Geist™ Rack Power Distribution Unit

Installer/User Guide

Upgradeable and Non-Upgradeable M-Series and D-Series (equipped with Firmware 6.x.x)

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 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.

Proprietary and Confidential ©2024 Vertiv Group Corp.

TABLE OF CONTENTS

1 Important Safety Instructions **1**
2 Overview **3**
2.1 Environmental 3
2.2 Electrical 4
2.3 Networking 4
2.3.1 ETHERNET 4
2.3.2 Protocols 4
2.3.3 User interfaces 5
3 Installation **7**
3.1 Mounting 7
3.2 Power Connection 19
3.2.1 U-Lock operation 19
3.2.2 P-Lock operation 21
4 Security Best Practices **23**
4.1 Risk Assessment 25
4.2 Physical Security 25
4.3 Account Access 25
5 Setup **27**
5.1 Interchangeable Monitoring Device 27
5.1.1 Basic 27
5.1.2 Metered 27
5.1.3 Unit monitored 28
5.1.4 Switched and outlet monitored 30
5.1.5 Monitored and switched (IMD-5M) 32
5.1.6 Rapid Spanning Tree Protocol (RSTP) 34
5.2 Network Setup 36
5.3 Web User Interface 41
5.3.1 Main menu 41
5.4 Device Sub Menu 42
5.4.1 Overview 43
5.4.2 Alarms & Warnings 50
5.4.3 Logging 55
5.4.4 CO2 Data 57
5.5 Provisioner Sub Menu 58
5.5.1 Discovery 59
5.5.2 File management 60
5.6 System Sub Menu 61

5.6.1 Users 61
5.6.2 Network 65
5.6.3 Web server 75
5.6.4 Remote authentication 76
5.6.5 Time 81
5.6.6 SSH 82
5.6.7 USB 82
5.6.8 Serial port 83
5.6.9 Email 83
5.6.10 SNMP 85
5.6.11 Modbus 87
5.6.12 SYSLOG 88
5.6.13 Admin 88
5.6.14 Locale 88
5.7 Utilities Sub Menu 88
5.7.1 Configuration Backup and Restore 88
5.7.2 Restore defaults 90
5.7.3 Reboot 90
5.7.4 Reboot I/O Boards 91
5.7.5 Firmware Updates 92
5.7.6 Factory Access 93
5.8 Help Sub Menu 94
6 Vertiv™ Intelligence Director 97
6.1 Aggregation 97
6.2 Array Manager 99
6.3 Network Configuration 100
6.4 Views 102
6.4.1 Summary 103
6.4.2 Groups 104
6.4.3 List 107
6.4.4 Group Configuration 108
6.5 Interfaces 110
6.5.1 Group SNMP data 111
6.5.2 Tips and troubleshooting 111
Appendices 113
Appendix A: Technical Support 113
Appendix B: Available Sensors 115
Appendix C: TP-Link Wireless USB adapters 116
Appendix D: Outlet LEDs 118
Appendix E: IMD Display Codes 119

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix F: Provisioner - Format of the configuration settings file 121
Appendix G: API / CLI Error Codes 141
Appendix H: An Example of Configuring LDAP for Active Directory Credentials 145

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

1 Important Safety Instructions

Regulatory Compliance

Vertiv products are regulated for safety, emissions and environment impact per the following agencies and policies.

Underwriters Laboratories (UL)

UL standards are used to assess products; test components, materials, systems and performance; and evaluate environmentally sustainable products, renewable energies, food and water products, recycling systems and other innovative technologies.

The UL standards specific to this equipment are as noted on the device nameplate.

CE

The placement of the CE mark on a product signifies that the product complies with the applicable European (EU) health, safety and environmental protection requirements, including EU legislation and product directives. The CE mark is required for products offered for sale within the European Economic Area (EEA).

The specific regulations, directives and standards applicable to each product are specified on the Declaration of Conformity.

Federal Communications Commission (FCC)

The Federal Communications Commission (FCC) regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the FCC is the United States primary authority for communications laws, regulation and technological innovation.

The FCC standards specific to this equipment are:

- This Class A device complies with part 15 of the FCC Rules.
- Operation is subject to the following two conditions:
  - This device may not cause harmful interference.
  - This device must accept any interference received, including interference that may cause undesired operation.
- This Class A digital apparatus complies with Canadian ICES-003.
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

WARNING! Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

NOTE: Visit *http://www.Vertiv.com/ComplianceRegulatoryInfo* for important safety information prior to installation.

Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

2 Overview

The Vertiv™ Geist™ Rack Power Distribution Unit (rPDU) gives data center managers the flexibility to install the intelligence required today. From basic power to power monitoring to outlet switching, the Geist™ rPDU product line adapts to a business needs now and in the future.

To establish this upgrade path, Vertiv engineers took the robust Geist™ rPDU design and incorporated an Interchangeable Monitoring Device (IMD). PDUs last for many years and with the IMD design, businesses are able to upgrade their PDUs to newer monitoring technologies in the future without having to replace the entire Geist™ rPDU. The hot swappable IMD is changed out in a few simple steps, without interrupting power to critical servers.

2.1 Environmental

The operational environmental limits pertaining to temperature, humidity, and elevation are as defined in the following tables.

Table 2.1 Temperature Limits

Description	Minimum	Maximum
Operating	10 °C (50 °F)	60 °C (140 °F)
Storage	-40 °C (-40 °F)	70 °C (158 °F)

Table 2.2 Humidity Limits

Description	Minimum	Maximum
Operating	5 %	95 % (non-condensing)
Storage	5 %	95 % (non-condensing)

Table 2.3 Elevation Limits

Description	Minimum	Maximum
Operating	0 m (0 ft)	3050 m (10000 ft)
Storage	0 m (0 ft)	15240 m (50000 ft)

Proprietary and Confidential ©2024 Vertiv Group Corp.

2.2 Electrical

Electrical product characteristics and performance are defined in the Table 2.4 below . Also, see the product nameplate for additional rating limits.

Table 2.4 Receptacle Ratings

Type	Ratings
Combination C13/C19	250 VAC, 16 A (UL & CSA 16 A, 250 VAC) with C20 cord 250 VAC, 10 A (UL & CSA 12 A, 250 VAC) with C14 cord **NOTE: Each Combination C13/C19 outlet bank is restricted to no more than 32 A per bank.**
German Schuko	250 VAC, 16 A
IEC-60320 C13	250 VAC, 10 A (UL & CSA 12 A, 250 VAC)
IEC-60320 C19	250 VAC, 16 A (UL & CSA 16 A, 250 VAC)
IEC309 PS6	230 VAC, 16 A
IEC309 PS56	230/400 VAC, 32 A
NEMA 5-15R or L5-15R	125 VAC, 12 A
NEMA 6-15R or L6-15R	250 VAC, 12 A
NEMA 5-20R or L5-20R	125 VAC, 16 A
NEMA 6-20R or L6-20R	250 VAC, 16 A
NEMA L5-30R	125 VAC, 24 A
NEMA L6-30R	250 VAC, 24 A
NEMA L7-15R	277 VAC, 12 A
NEMA L7-20R	277 VAC, 16 A
Saf-D-Grid	277 VAC, 16 A
U-Lock Locking IEC-60320 C13	250 VAC, 10 A (UL & CSA 12 A, 250 VAC)
U-Lock Locking IEC -60320 C19	250 VAC, 16 A (UL & CSA 16 A, 250 VAC)
United Kingdom BS1363	250 VAC, 13 A

2.3 Networking

The product communications requirements are defined in the next sections.

2.3.1 ETHERNET

The ETHERNET link speed for this product is: 10/100/1000 Mb; full duplex.

2.3.2 Protocols

The communications protocols supported by this product include: ARP, IPv4, IPv6, ICMP, ICMPv6, NDP, TCP, UDP, RSTP, STP, DNS, HTTP, HTTPS (TLSv1.3), SMTP, SMTPS, Modbus TCP/IP, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232, and Syslog.

Proprietary and Confidential ©2024 Vertiv Group Corp.

2.3.3 User interfaces

This product supports the following user interfaces: SNMP, JSON-based Web GUI, JSON API and Command line interface using SSH or serial (RS232).

Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

3 Installation

Using the images in the mounting section, install the Geist™ rPDU.

NOTE: Visit http://www.Vertiv.com/ComplianceRegulatoryInfo for important safety information prior to installation

To install unit:

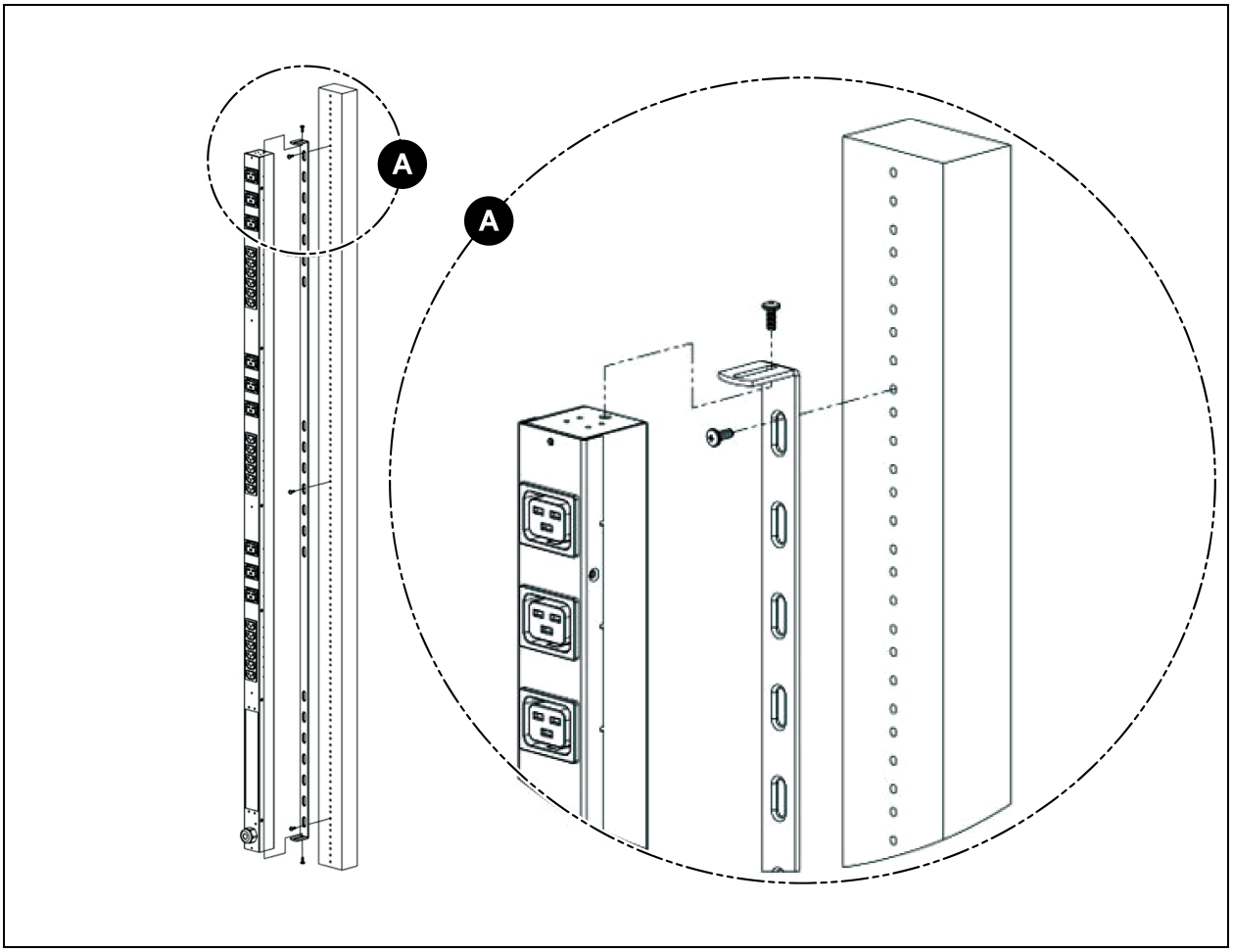
1. Wear all applicable Personal Protection Equipment (PPE).
2. Using appropriate hardware, attach the unit to the rack.
3. Plug the Geist™ rPDU into an appropriately rated and protected branch circuit receptacle.
4. Plug in the devices to be powered by the Geist™ rPDU.
5. Turn on each device connected to the Geist™ rPDU.

NOTE: Sequential power-up is recommended to avoid high inrush current.

3.1 Mounting

Optional brackets are sold separately.

Figure 3.1 Full Length Brackets



Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.2 Mini L Brackets

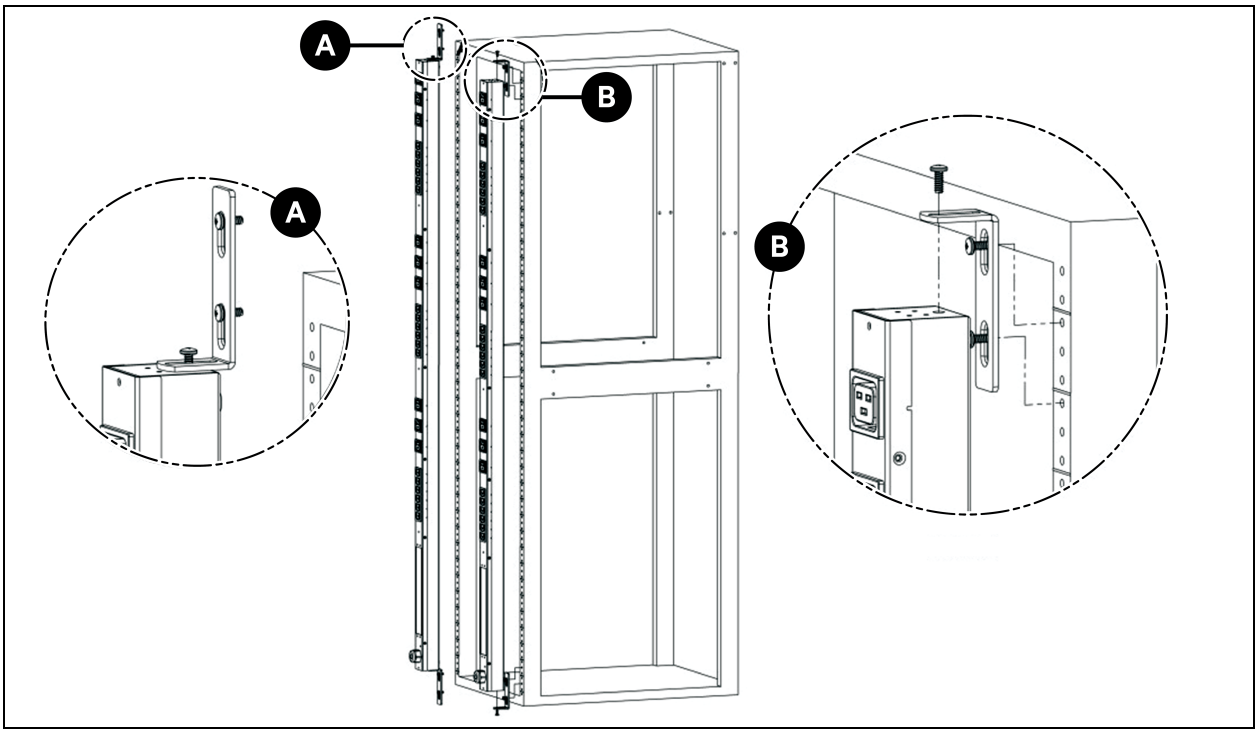
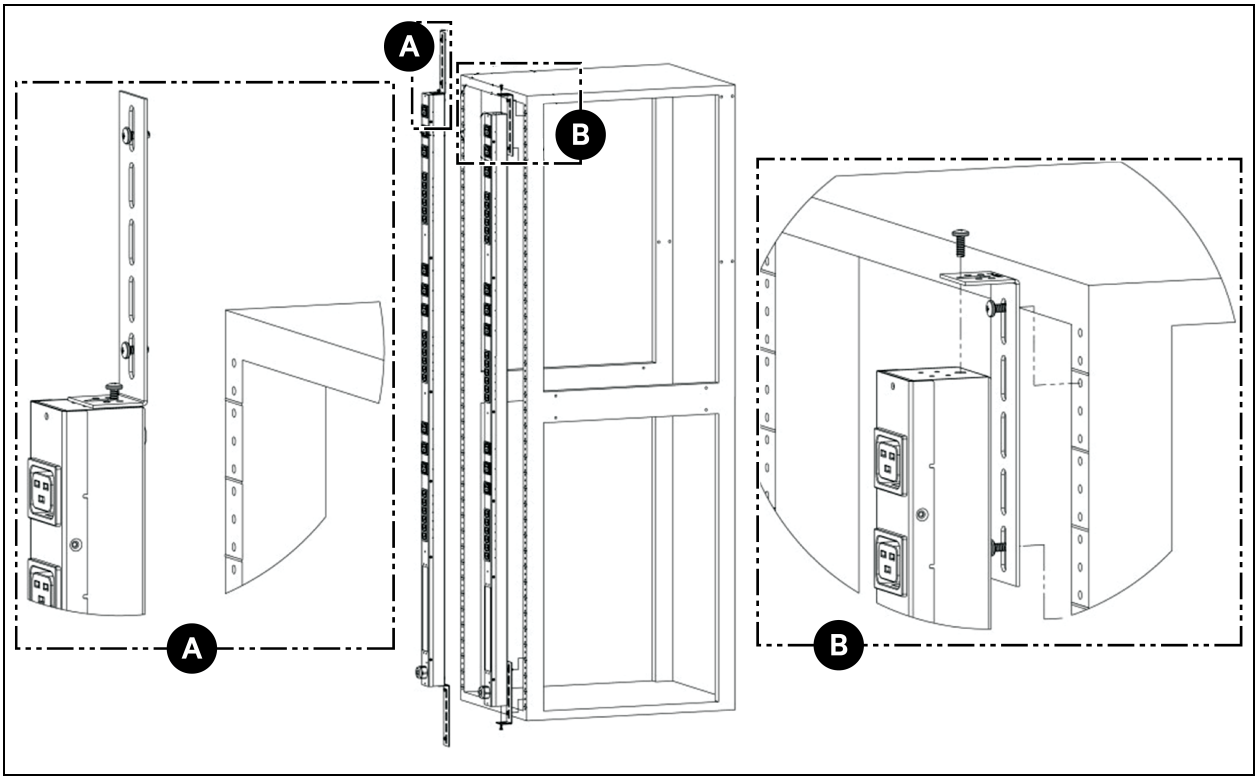
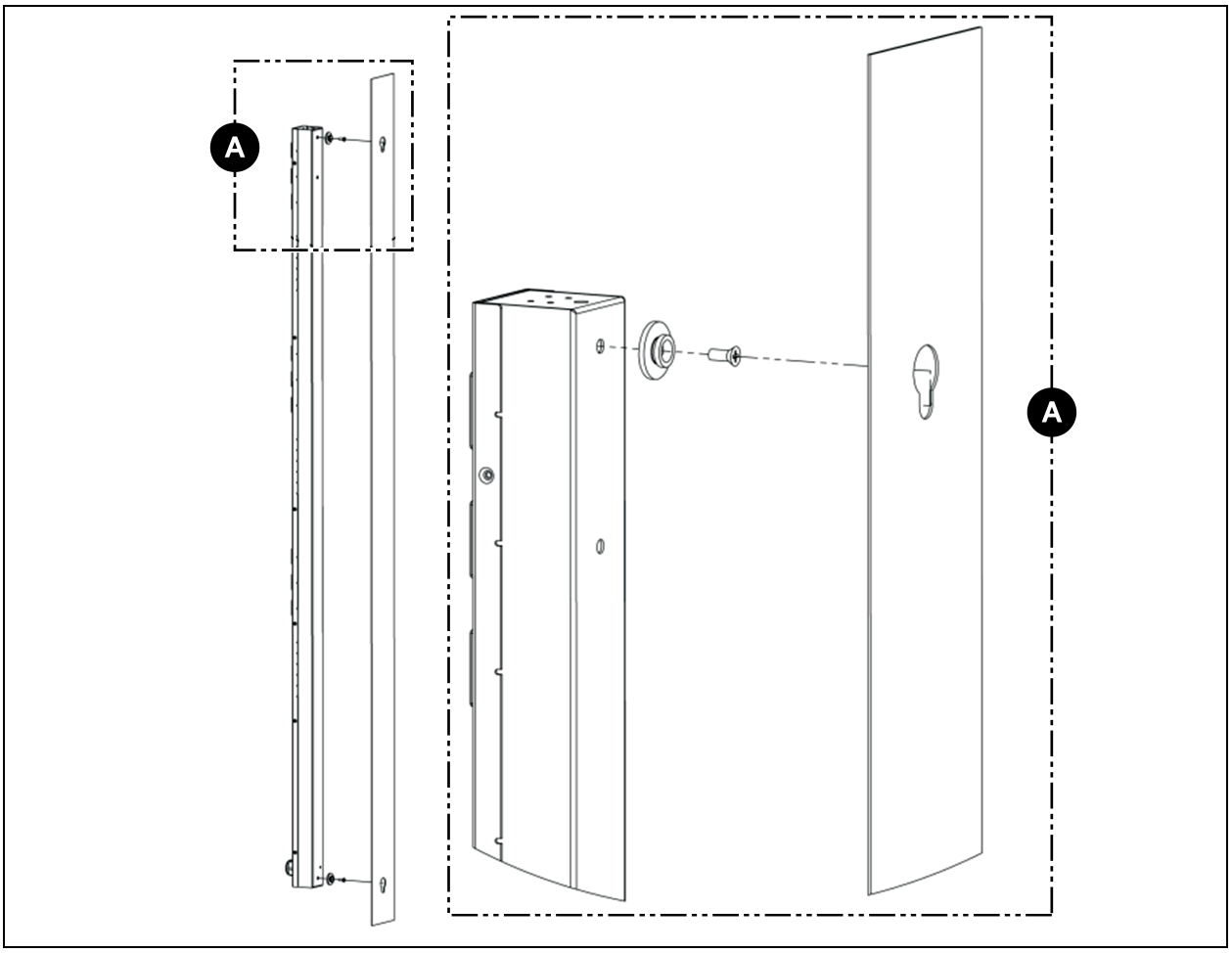


Figure 3.3 Vertical Extension Brackets



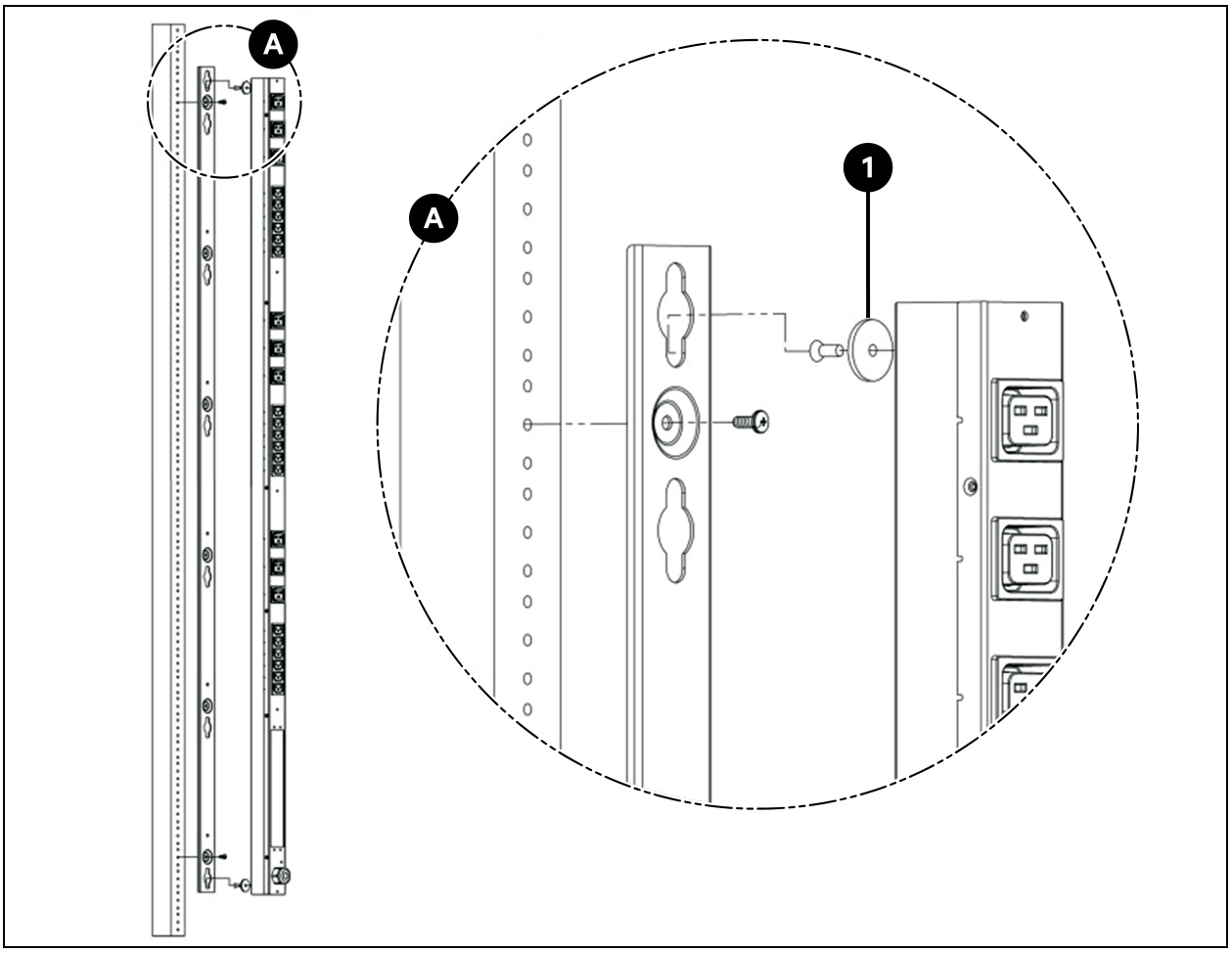
Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.4 Toolless Mounting Hardware



Proprietary and Confidential ©2024 Vertiv Group Corp.

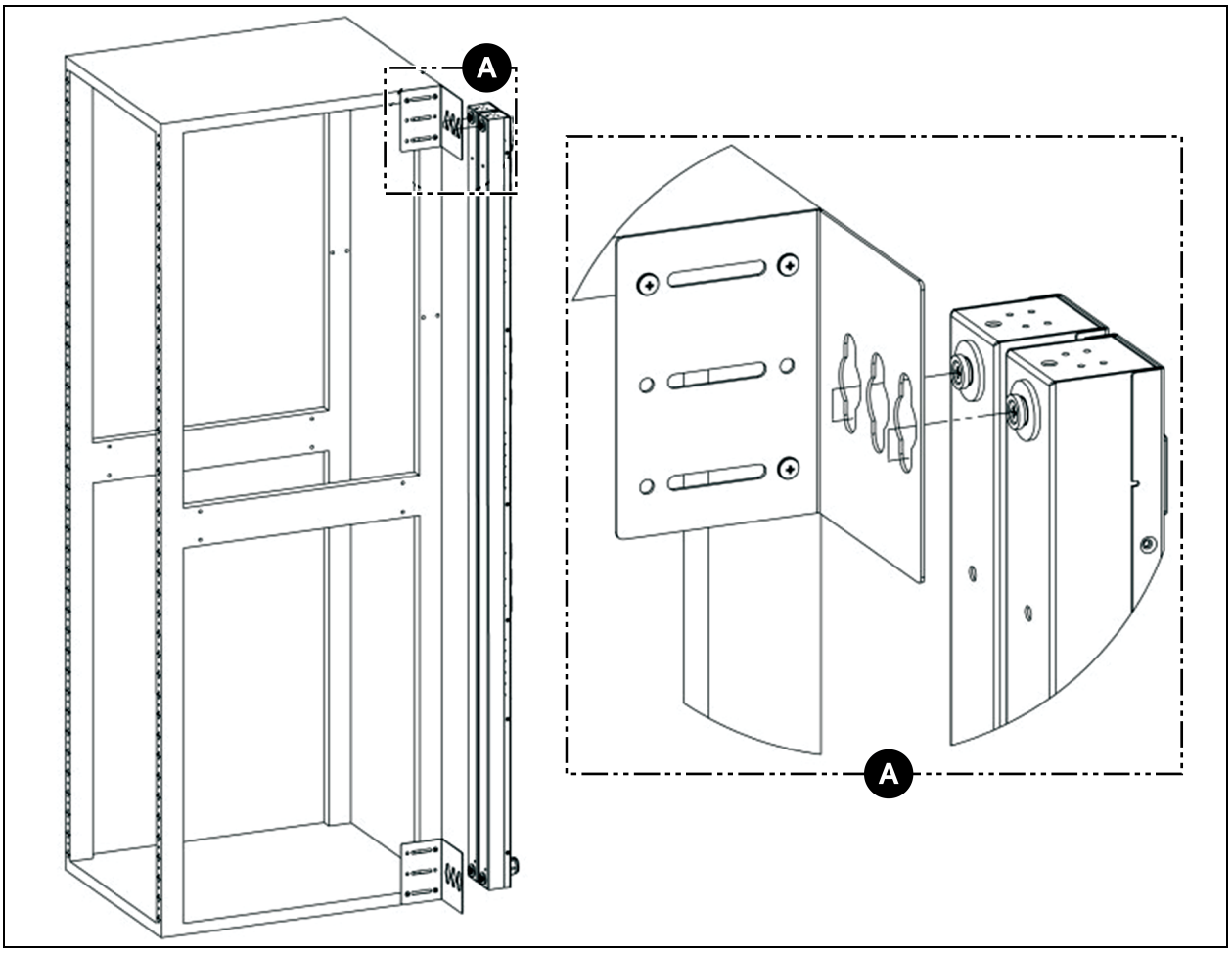
Figure 3.5 Toolless Full Length Brackets



Item	Description
1	Toolless shoulder washer

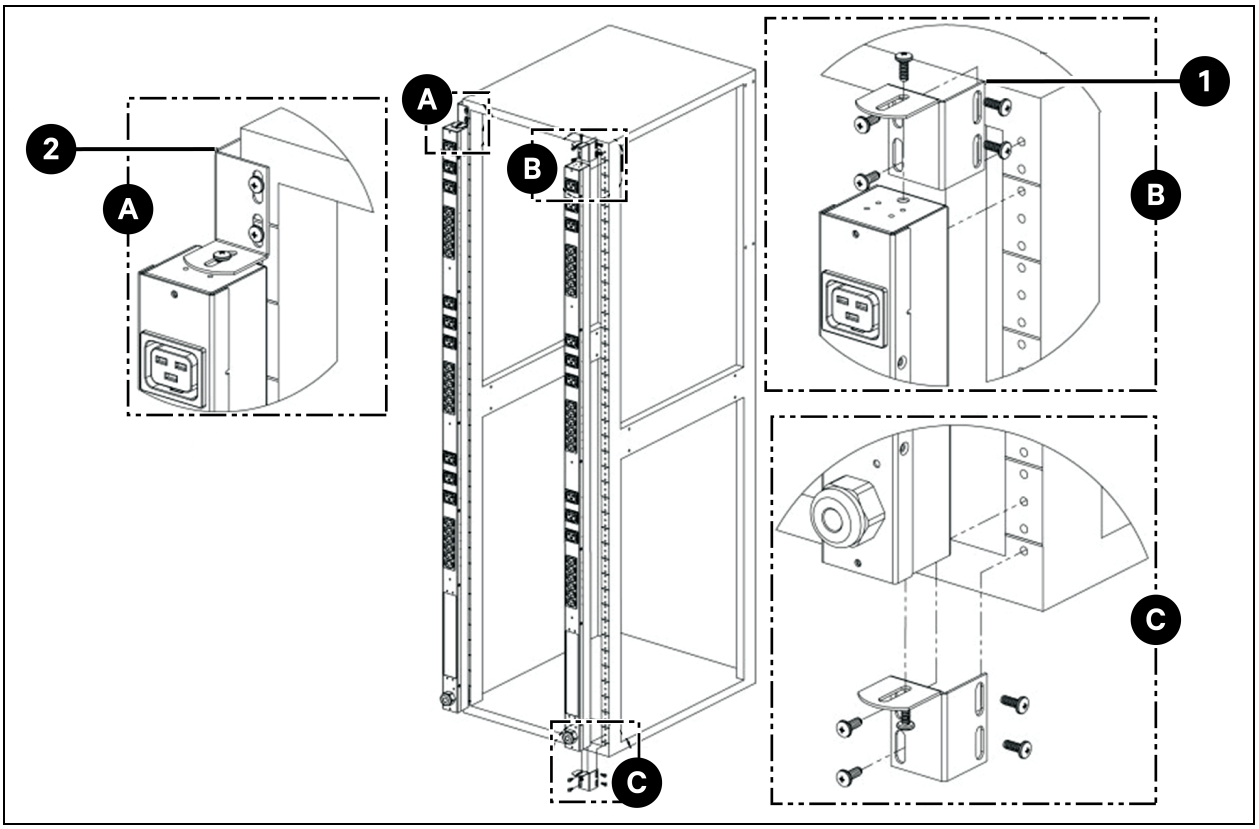
Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.6 Single Side Mount Two Units Brackets



Proprietary and Confidential ©2024 Vertiv Group Corp.

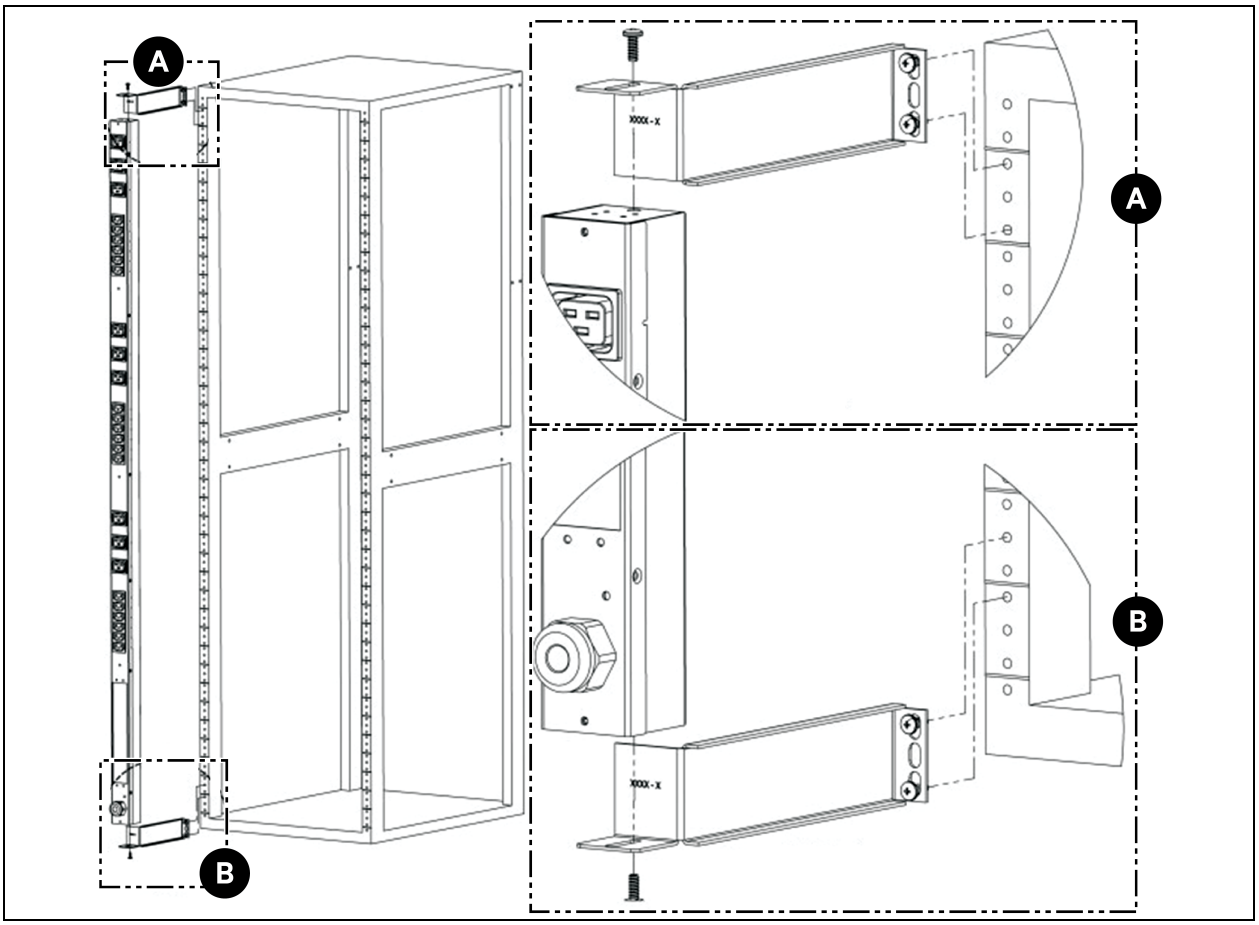
Figure 3.7 Offset/Side Mount Brackets



Item	Description
1	Right side option
2	Left side option

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.8 7" (inch) Extension Brackets



Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.9 Flush Mount Bracket

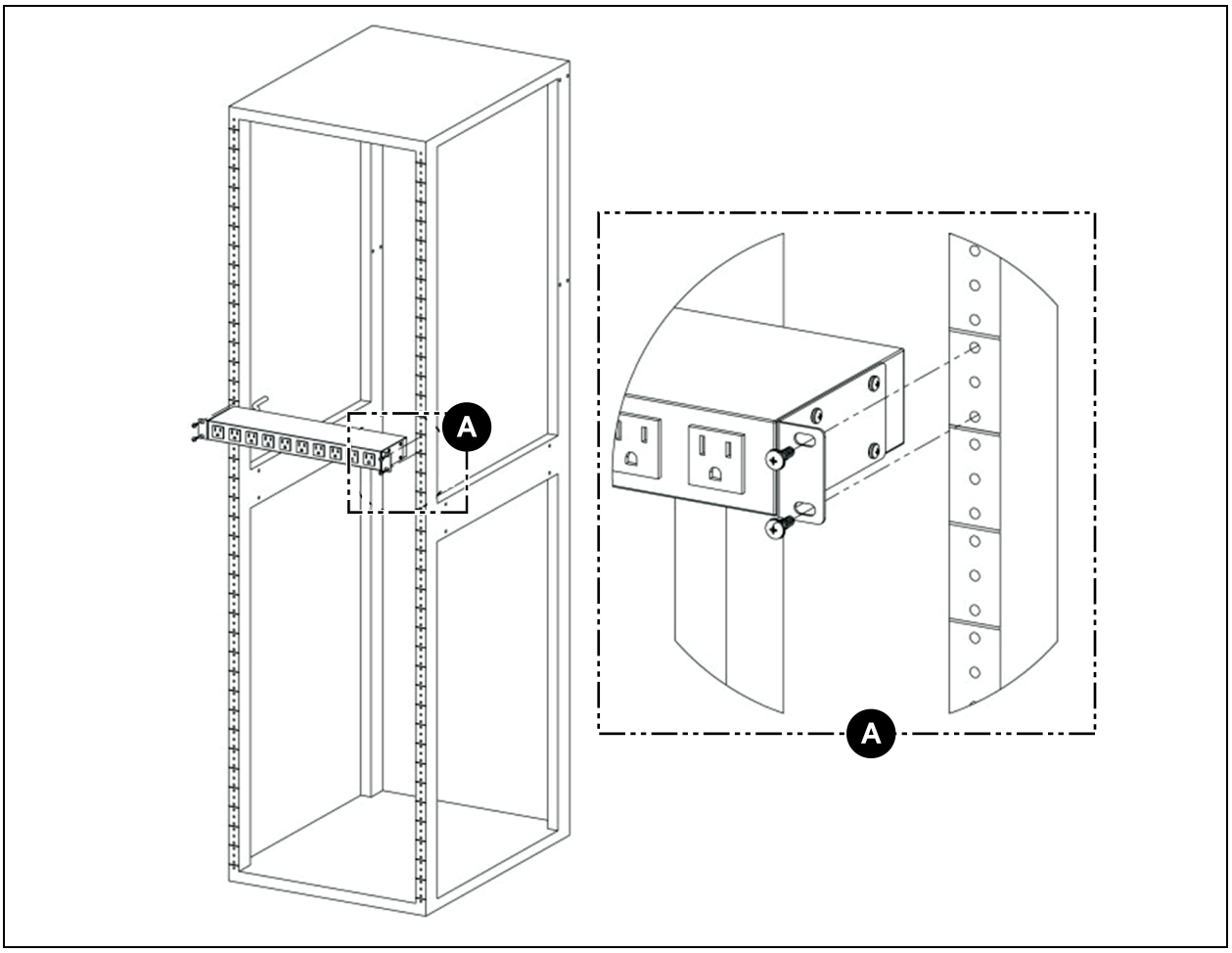
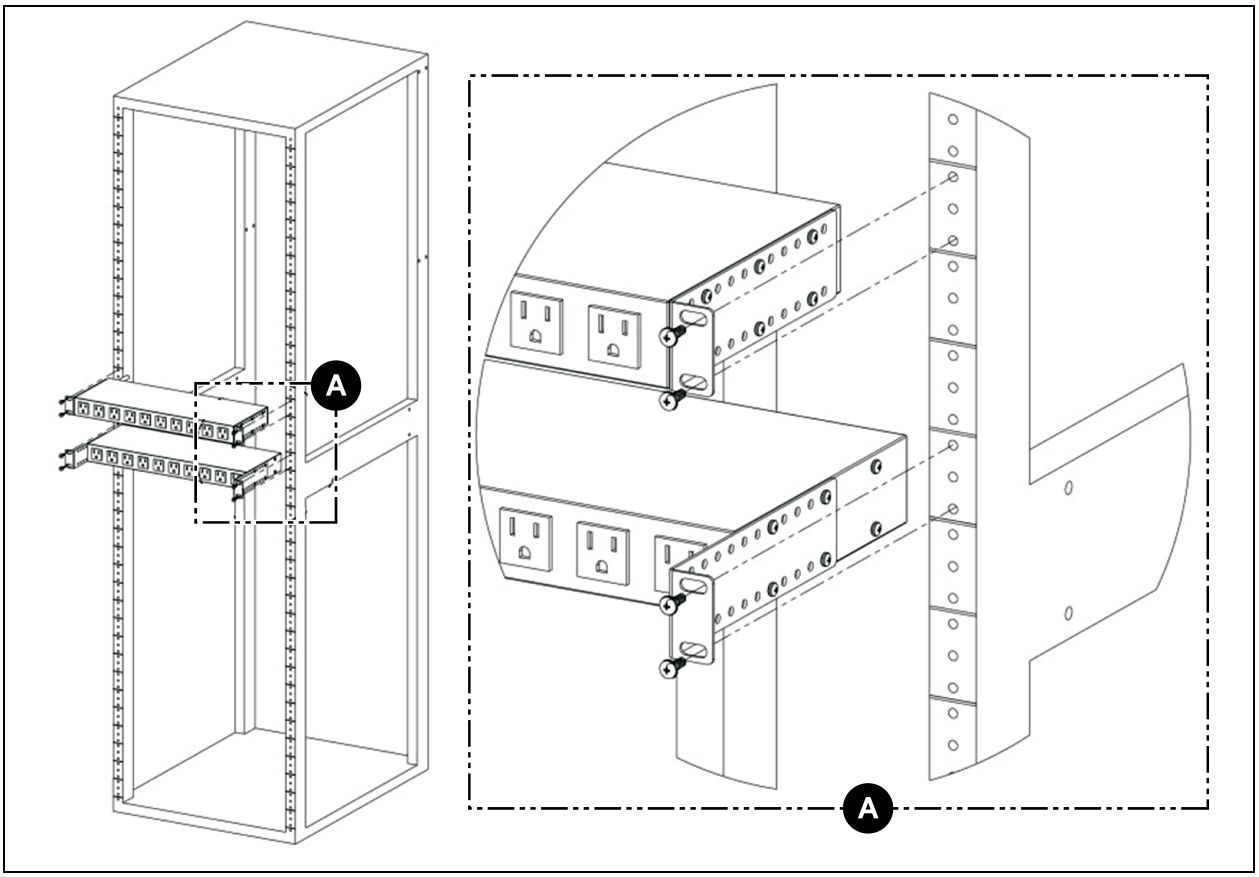


Figure 3.10 Adjustable Mount Bracket



Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.11 Panel Mount Bracket

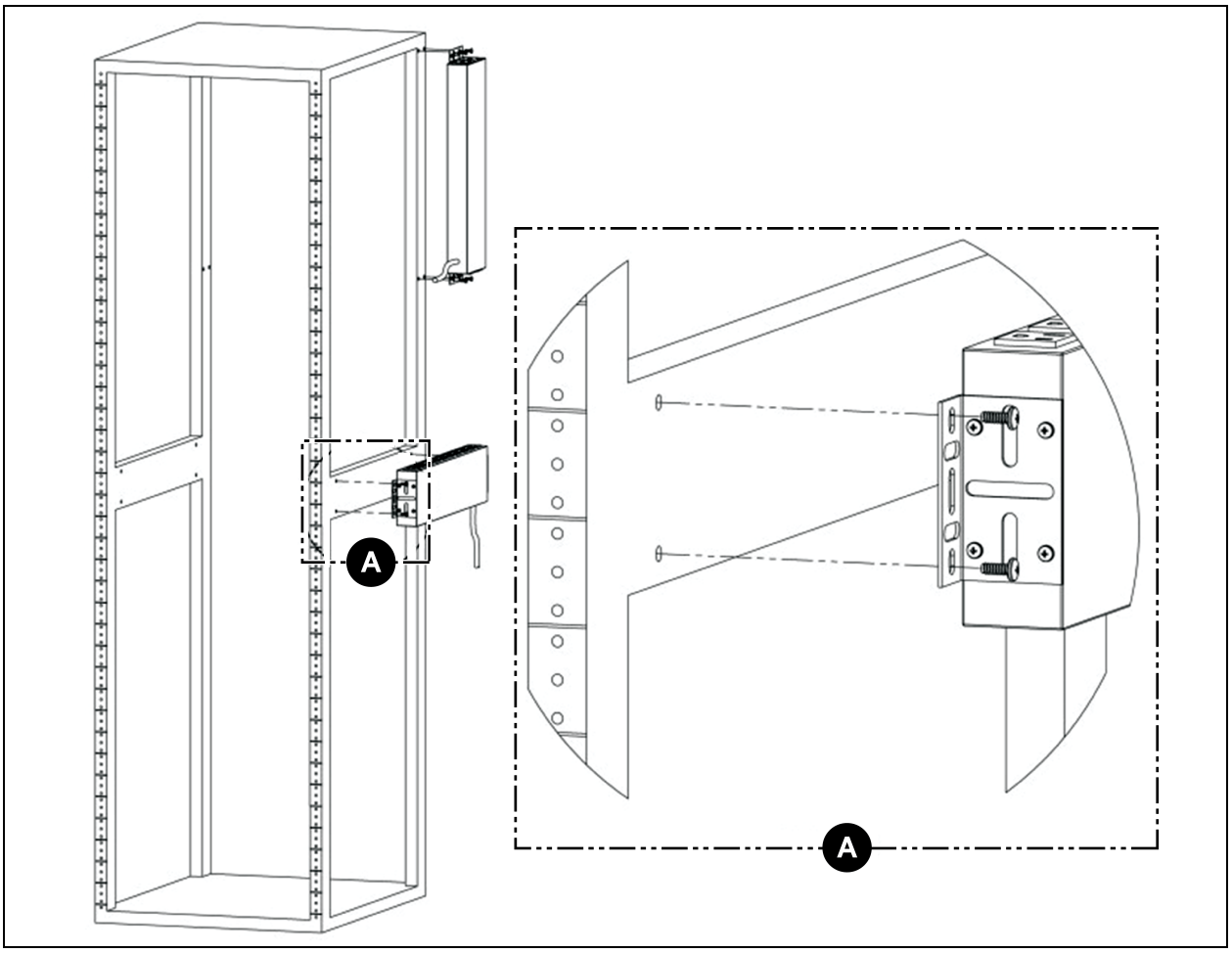
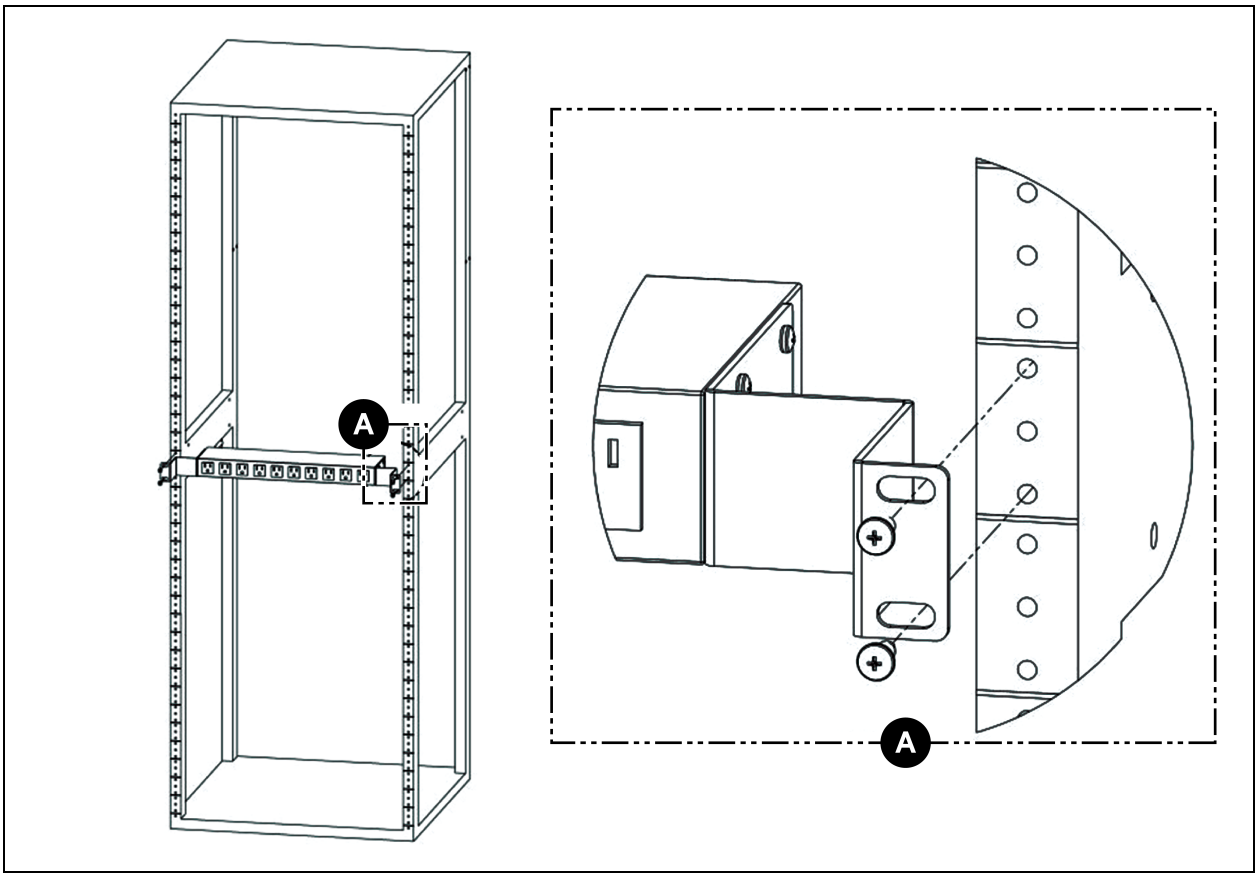


Figure 3.12 23" (inch) Conversion Mount Brackets



Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 3.13 19" (inch) Horizontal/Panel-Mount Brackets

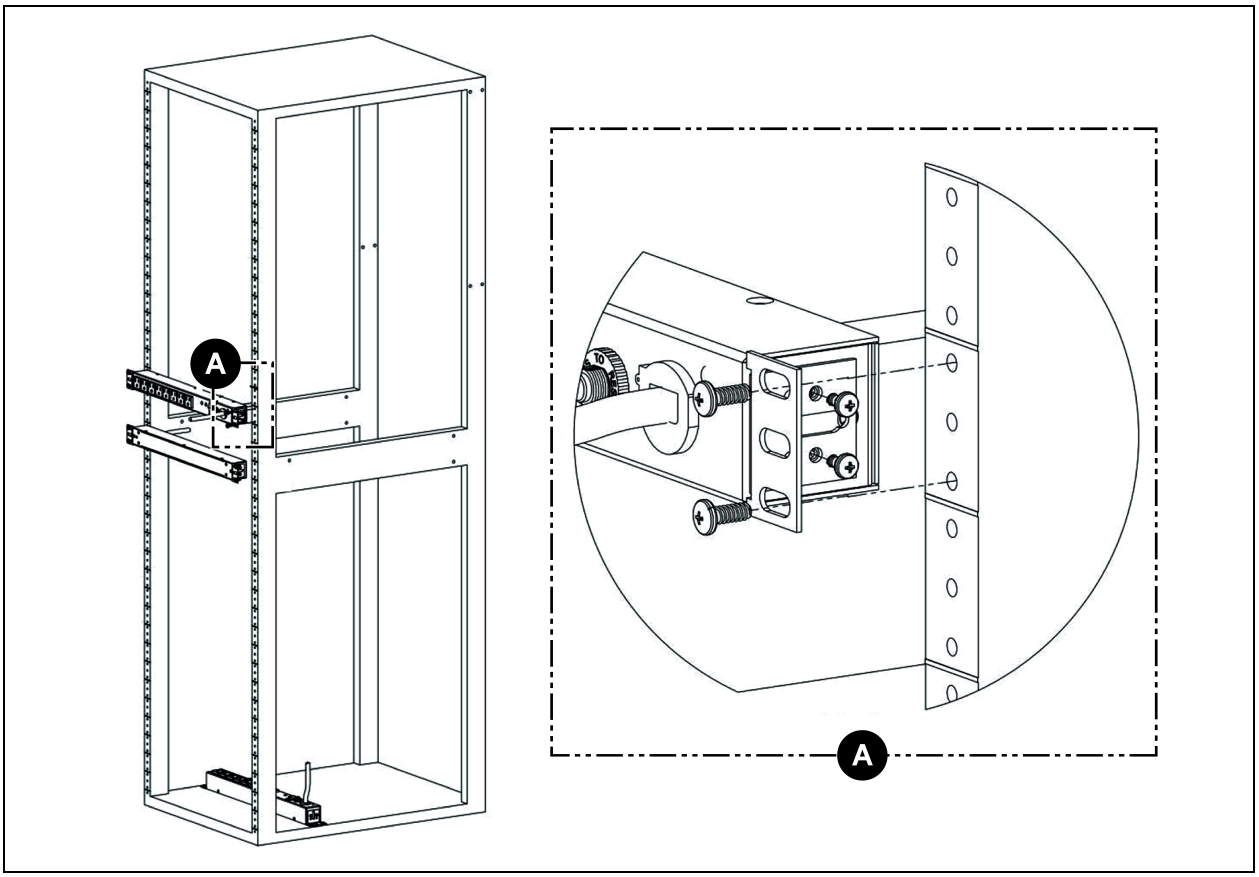
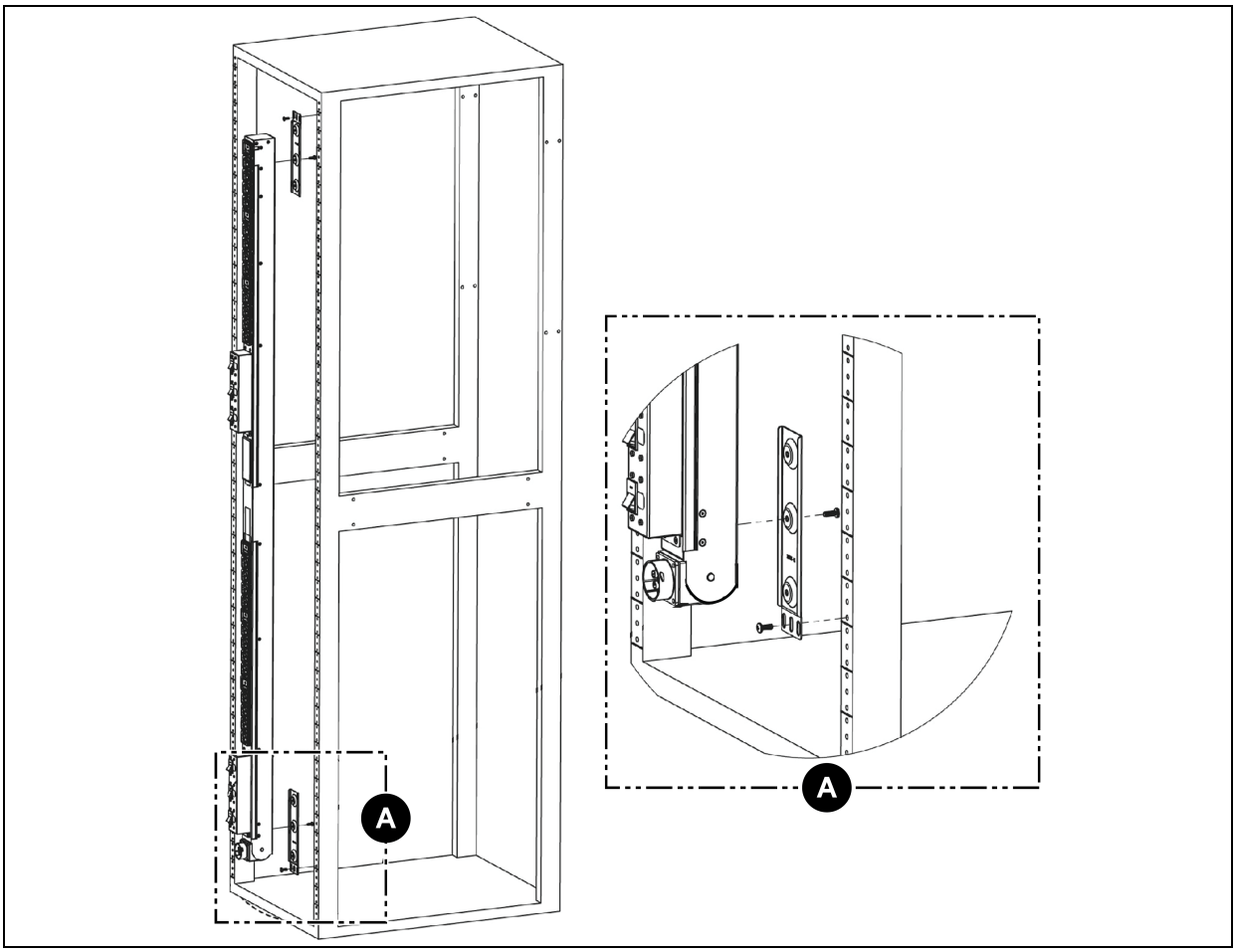


Figure 3.14 Mount Brackets for Vertiv™ Geist™ Universal Power Distribution Unit (UPDU) with Pivoting End



3.2 Power Connection

Plug the Vertiv™ Geist™ rPDU into an appropriately rated and protected branch circuit receptacle. Ensure the power cable does not exceed manufacture's bend radius (10X).

3.2.1 U-Lock operation

Plug in the devices to be powered by the Geist™ rPDU.

- Vertiv patented U-Lock power cord retention.
- Uses standard power cords.
- Cord insertion activated locking system.
- Easy push-and-hold bezel unlocking feature.

Proprietary and Confidential ©2024 Vertiv Group Corp.

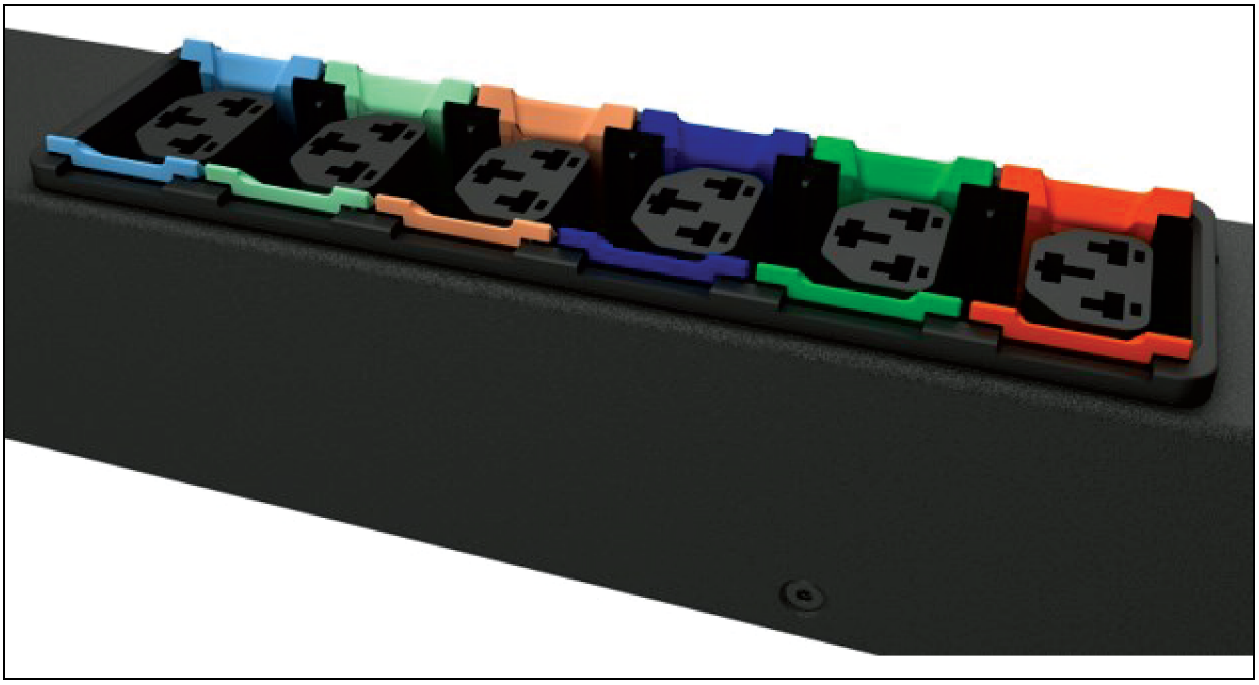
Figure 3.15 U-Lock Cord Retention Operation

Proprietary and Confidential ©2024 Vertiv Group Corp.

3.2.2 P-Lock operation

- Plug in the devices to be powered by the Geist™ rPDU.
- Vertiv™ Combination C13/C19 Outlet with P-Lock power cord retention.
- Compatible with P-Lock power cords.
- Use press-and-hold tabs on the P-Lock cord to release from outlet.

Figure 3.16 P-Lock Cord Retention Operation



Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

4 Security Best Practices

The default settings on the card support are defaulted for a secure configuration on deployment. Proper security of critical infrastructure equipment requires proper configuration of ALL communication services. This section summarizes the settings.

Through our Vertiv SECURE product life cycle, Vertiv is committed to minimizing cybersecurity risk in our products by deploying cybersecurity best practices across our engineering design of products and solutions, by making them more secure, reliable, and competitive for our customers.

Below are some life cycle cybersecurity recommendations. The cybersecurity recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement a customers existing cybersecurity programs. The following sites are available for more information on general cybersecurity best practices and guidelines:

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

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

Table 4.1 below , provides a list of items to review. Each should be reviewed, configured based on the operational needs for managing the equipment, and verified that the settings support the desired operational functionality without adding unnecessary or unauthorized access to critical infrastructure equipment. A reference to the proper section in this document is provided for configuring each item.

Table 4.1 Settings to Review and Verify to Reduce the Risk of Unauthorized Access

Item	Description	Reference
Accounts and Passwords	Change the admin and user account names and passwords immediately to eliminate default credential access.	See Users on page 61 .
IP Network Access	Enable/disable IPV4 and IPV6 network access to the card - disable unused network access.	See Network on page 65 .
SSHv2 Access	Enable/disable SSHv2 access for diagnostic and configuration support - disable when not in use.	See SSH on page 82 .
Web Service Protocol	Select HTTPS to use SSL encryption when accessing data through the web user interface.	See Web server on page 75 .
TLS Certificates	When using HTTPS, install your own TLS Certificates from a trusted certificate authority or generate alternative self-signed certificates.	See SSL Certificate: Allows you to upload your own signed SSL Certificate file to replace the default one. The certificate can be either self-signed or signed from a Certification Authority. SSL Certificate must be in either PEM or PFX (PKCS12) format. on page 75 .
Remote Write Web Access	To control/write through web interface, you must log in remotely and have either an admin level or control level user account. To prohibit remote access, disable both HTTP and HTTPS.	See Web server on page 75 .

Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 4.1 Settings to Review and Verify to Reduce the Risk of Unauthorized Access (continued)

Item	Description	Reference
	WARNING! Disabling both HTTP and HTTPS will immediately terminate this connection and remote access will only be available using SSH.	
Communication Protocols	Enable/disable SNMP - disable unused protocols.	See Modbus on page 87 .
SNMP Version Settings	Enable/disable the desired SNMP versions, consider using SNMPv3 with user authentication and encryption.	See SNMP on page 85 .
SNMP Access Table Settings	For each SNMPv1/v2c Access table entry, set the SNMP Access Type to Read-Only to prevent changes to the device from the hosts identified in the table entry.	See SNMP on page 85 .
SNMP Community Strings	Use suitably strong values for SNMP communication in line with your organizations password policy.	See SNMP on page 85 .
SNMPv3 Settings	Use suitable hashing and encryption algorithms for SNMPv3 Authentication and Privacy settings to make SNMPv3 communications more secure.	See SNMP on page 85 .
Guest user account	This account should remain disabled, unless required. As it provides read-only access to device and may give additional context to device settings if enabled.	See Users on page 61 .

For added security, the local network firewall and gateway may be restricted to allow only the necessary traffic on the required network ports. The ports used by the MRIC-RP card are listed in the following table. Some port settings may be changed by the administrator.

Table 4.2 Ports Used by the MRIC-RP Card (v6.1 or higher)

Network Service	Port used	Default	Modification Required
HTTP	TCP80	N	Y
HTTPS	TCP443	Y	Y
DNS	TCP&UDP 53	Y	N
NTP	TCP&UDP 123	Y	N
SMTP	TCP25	Y	Y
SSH	TCP UDP 22	Y	N
SNMP	UDP 161, 162	N	Only trap port 162 may be changed.
Modbus	TCP 502	N	Y
VID/VIP	GDP/HTTP	N	N
DHCP Client	UDP 68	Y	N
GDP (Geist Discovery Protocol)	UDP 6687	Y	N
LDAP	TCP 389	N	Y
RADIUS	UDP1812/1813/1645/1646	N	N
TACACS	TCP 49	N	N
Remote Syslog	TCP 514	N	Y

Details for configuration of all options are provided in the remainder of this guide.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

4.1 Risk Assessment

Vertiv recommends conducting a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, availability and integrity of the system and its environment. This exercise should be conducted in accordance with applicable technical and regulatory frameworks such as IEC 62443 and NERC-CIP. The risk assessment should be repeated periodically.

4.2 Physical Security

The IMD5 is designed and intended to be deployed and operated in a physically secure location. Vertiv recommends a review of the physical security and operating environment of the unit. Since an attacker or insider threat can cause serious disruption, below are some recommended best practices that include, but are not limited to:

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

4.3 Account Access

The IMD5 account access privileges should be administered to provide the least account functions that still enables the end-user to perform their job functions. Login to the IMD5 should be restricted to legitimate users. Some of the following best practices should be adopted by an organization's written procedures for network and equipment access:

- First login to the IMD5 requires credentials to be created.
- No account/logon sharing. Each user should have their own specific account and password. Logging functions of the IMD5 expect each account to be a unique non-shared user.
- Admins should restrict access and privileges to only the required functions of the user's job function.
- Restrict all admin-level privileges (Such as firmware updates, protocol enablement/disablement.) to only approved administrators.
- Ensure password strength, complexity, and length requirements are enforced at the highest level per company IT policy.
- Ensure terminated employees instantly are removed from accessing the unit. Some examples include the user of a AAA, TACACS+ user authentication process.
- Enforce session time-out after a period of inactivity.
- Use the remote syslog facility to alert you to system and network events, security threats, and visibility into the device to troubleshoot problems. (This may also be required in your environment for PCI-DSS/SOX/HIPAA compliance).

Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

5 Setup

5.1 Interchangeable Monitoring Device

The Interchangeable Monitoring Device (IMD) is the core behind the Upgradable Geist™ rPDU line of power products. The IMD can be replaced and upgraded to allow data centers to future proof their locations. Installing the wrong IMD for replacement in an rPDU can lead to damage to the IMD.

5.1.1 Basic

The Basic upgradeable Geist™ rPDU is the baseline for the GU line of products. It is built with the IMD-01X module, and provides low cost power distribution with the option to upgrade to add local metering and/or remote monitoring and other features in the future.

5.1.2 Metered

The Metered upgradable Geist™ rPDU is a locally metered option for the GU line of products. It is built with the IMD-01D module, and provides a local display for viewing current draw (Amps) with the option to upgrade to add monitoring and other features in the future.

Figure 5.1 IMD-01D Module

Table 5.1 IMD-01D Module Descriptions

Item	Name	Description
1	Local Display	The local display shows the phase, line, and circuit current values (in Amperes).
2	Display Buttons	There are three buttons near the IMD display; a back button, a forward button, and a center button. The functions of these buttons are described in the Table 5.2 on the next page .

Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 5.2 Display Button Functions

Button	Symbol	Description
Back Button	◁	Decrement to the previous channel.
Forward Button	▷	Increment to the next channel.
Center Button	□	Toggle between scrolling and static display modes. Holding this button for 10 seconds will perform a network reset, restoring the default IP address and resetting user account information.
Center Button x3	□	Pressing this button three times within two seconds enables VLC mode. Pressing the button while VLC mode is active returns the unit to the standard current display.
Back and Forward Buttons	◁ and ▷	Pressing both buttons at the same time flips the display 180 degrees.

NOTE: Display button functionality may vary based on unit configuration.

5.1.3 Unit monitored

Previous versions of the Vertiv™ Unit Level Monitoring Vertiv™ Geist™ rPDUs were shipped with the IMD-03E-G module.

Figure 5.2 IMD-03E-G Module

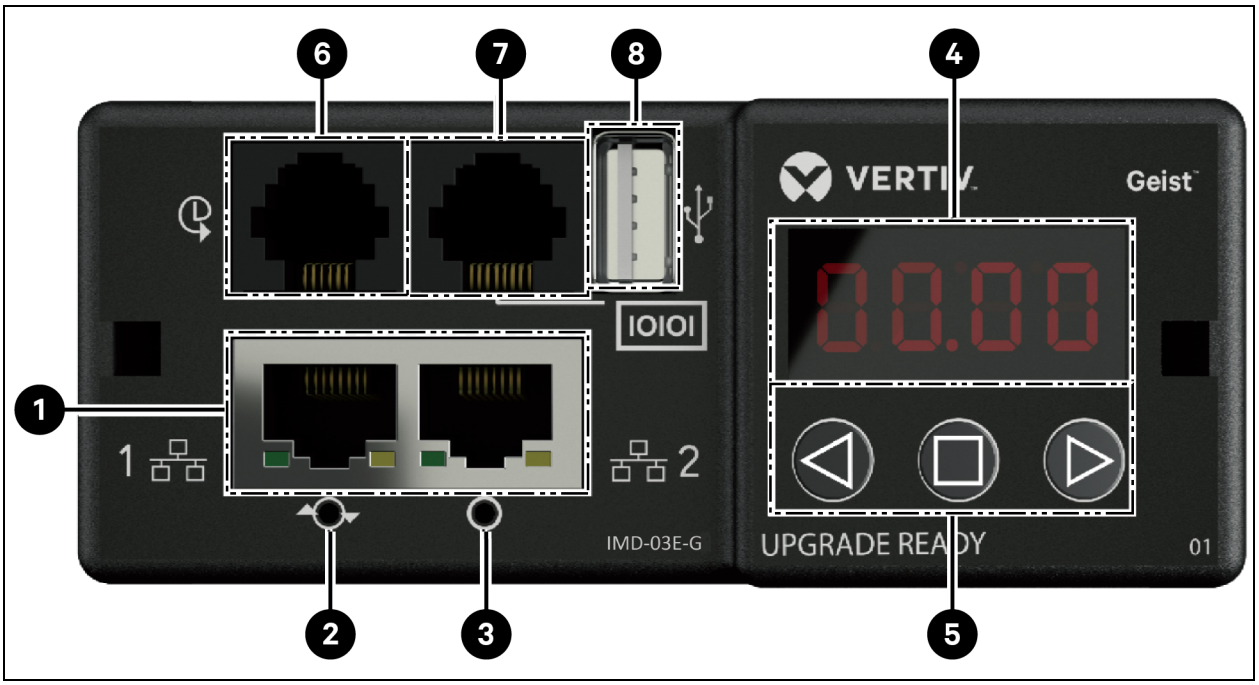


Table 5.3 IMD-03E-G Module Descriptions

Number	Name	Description
1	Dual ETHERNET Ports	The dual ETHERNET ports act as a two-port ETHERNET switch, allowing for multiple devices to be daisy- chained. The dual ETHERNET ports can be independently configured dual ETHERNET network interfaces, allowing the rPDU to connect to two different networks.
2	Hard-Reboot Button	Pressing the hard-reboot button reboots the IMD. This acts as a power-cycle for the IMD; it does not change or remove any user information.
3	Network Reset Button	Holding the network reset button for 5 seconds during normal operation will restore the default IP address and reset the user accounts.
4	Local Display	The local display shows the phase, line and circuit current values (in amperes).
5	Display Buttons	There are three buttons near the IMD display: a back button, a forward button and a center button. The functions of these buttons are described in the **Table 5.4** below .
6	Remote Sensor Port	RJ-12 port for connecting a Vertiv™ plug-and-play remote digital sensors (sold separately). Each digital sensor has a unique serial number and is automatically discovered. GU2 PDUs support up to 16 sensors. The optional Vertiv™ A2D Converter can be added to support analog sensing.The optional SN-ADAPTER can be added to support Liebert Integrated and Modular Sensors. For more information, see Available Sensors on page 115 .
7	Serial Port	RS-232 via RJ-45 port.
8	USB Port	USB port used to upload firmware, backup/restore device configuration, expand logging capacity via a USB storage device or support TP-Link wireless USB adapters. The USB port must be enabled - see USB on page 82 . Provides up to 100 mA power capacity for USB - connected devices.

NOTE: Serial connection does not support flow control.

Table 5.4 Display Button Functions

Button	Symbol	Description
Back Button		Press to decrement to previous channel. Holding the button for 3 seconds initiates a configuration backup. The display will show a **bcup** message while the backup is being generated and will then go back to normal operation. The backup is stored on available USB storage devices and the operation will do nothing if no such drives are available.
Forward Button		Press to increment to next channel. Holding this button for 3 seconds initiates a configuration restore. The display will show a **load** message followed by a **conf** message and then a 3 second countdown. Once the countdown expires, a **8888** message is displayed and the backup will be applied. The backup will be read from USB storage devices. If the button is released at any time during this sequence, the restore is aborted. Once the backup is applied, or if there are no backup images or no USB storage device attached, the display will then go back to normal operation.
Center Button		Toggle between scrolling and static display modes. Holding this button for 3 seconds initiates a parameter reset sequence. This sequence consists of an **rset** message, followed by a **dflt** message and then a 3 second countdown. Once the countdown expires, an **8888** message is displayed and the network, *http* user accounts and *LDAP/RADIUS* information is reset to default values. If the button is released at any time during this sequence, the reset will be aborted.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 5.4 Display Button Functions (continued)

Button	Symbol	Description
Center Button x3		Pressing this button 3 times within 2 seconds enables VLC mode. Pressing the button while VLC mode is active returns the unit to the standard current display .
Back and Forward Buttons	and	Pressing both buttons at the same time flips the display 180 degrees.
Back and Center Buttons	and	Pressing both buttons at the same time displays the primary IPv4 address for the unit.

5.1.4 Switched and outlet monitored

Previous versions of the Vertiv™ Geist™ Switched Unit Level Monitoring, Outlet Level Monitoring and Switched Outlet Level Monitoring rPDUs were shipped with the IMD-03E-G module.

Figure 5.3 IMD-03E-G Module

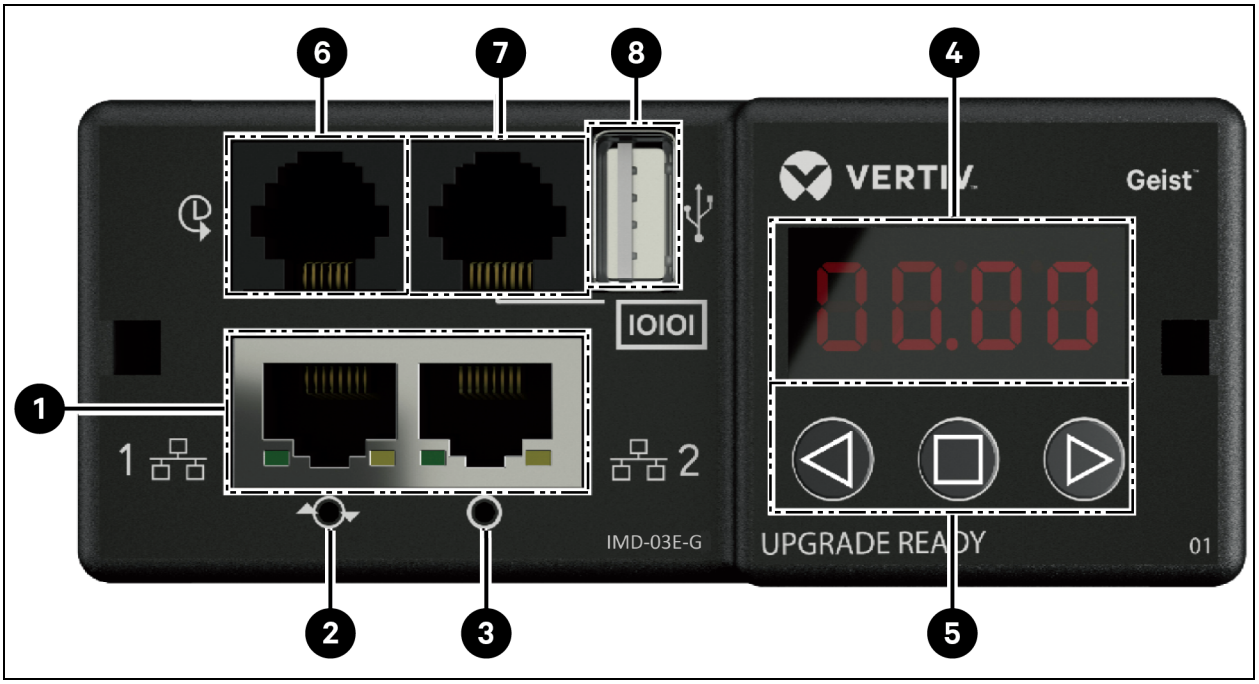


Table 5.5 IMD-03E-G Module Descriptions

Number	Name	Description
1	Dual ETHERNET Ports	The dual ETHERNET ports act as a two-port ETHERNET switch, allowing for multiple devices to be daisy- chained. The dual ETHERNET ports can be independently configured dual ETHERNET network interfaces, allowing the rPDU to connect to two different networks.
2	Hard-Reboot Button	Pressing the hard-reboot button reboots the IMD. This acts as a power-cycle for the IMD; it does not change or remove any user information.
3	Network Reset Button	Holding the network reset button for 5 seconds during normal operation will restore the default IP address and reset the user accounts.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 5.5 IMD-03E-G Module Descriptions (continued)

Number	Name	Description
4	Local Display	The local display shows the phase, line and circuit current values (in amperes).
5	Display Buttons	There are three buttons near the IMD display: a back button, a forward button and a center button. The functions of these buttons are described in the Display Button Functions below .
6	Remote Sensor Port	RJ-12 port for connecting a Vertiv plug-and-play remote digital sensors (sold separately). Each digital sensor has a unique serial number and is automatically discovered. GU2 PDUs support up to 16 sensors. The optional Vertiv™ A2D Converter can be added to support analog sensing.The optional SN-ADAPTER can be added to support Liebert Integrated and Modular Sensors. For more information, see Available Sensors on page 115 .
7	Serial Port	RS-232 via RJ-45 port.
8	USB Port	USB port used to upload firmware, backup/restore device configuration, expand logging capacity via a USB storage device or support TP-Link wireless USB adapters. The USB port must be enabled - see USB on page 82 . Provides up to 100 mA power capacity for USB - connected devices.

NOTE: USB MSC devices such as thumb drives or external hard drives are supported. USB storage devices must be formatted as FAT32.

NOTE: Serial connection does not support flow control.

Display Buttons

There are three buttons near the IMD display: a back button, a forward button and a center button. The functions of these buttons are described in the following table.

Table 5.6 Display Button Functions

Button	Symbol	Description
Back Button		Press to decrement to previous channel. Holding this button for 3 seconds initiates a configuration backup. The display will show a **bcup** message while the backup is being generated and will then go back to normal operation. The backup is stored on available USB storage devices and the operation will do nothing if no such drives are available.
Forward Button		Press to increment to next channel. Holding this button for 3 seconds initiates a configuration restore. The display will show a **load** message followed by a **conf** message and then a 3 second countdown. Once the countdown expires, a **8888** message is displayed and the backup will be applied. The backup will be read from USB storage devices. If the button is released at any time during this sequence, the restore is aborted. Once the backup is applied, or if there are no backup images or no USB storage device attached, the display will then go back to normal operation.
Center Button		Toggle between scrolling and static display modes. Holding this button for 3 seconds initiates a parameter reset sequence. This sequence consists of an **rset** message, followed by a **dflt** message and then a 3 second countdown. Once the countdown expires, an **8888** message is displayed and the network, http, user accounts and LDAP/RADIUS information are reset to default values. If the button is released at any time during this sequence, the reset will be aborted.

Proprietary and Confidential ©2024 Vertiv Group Corp.

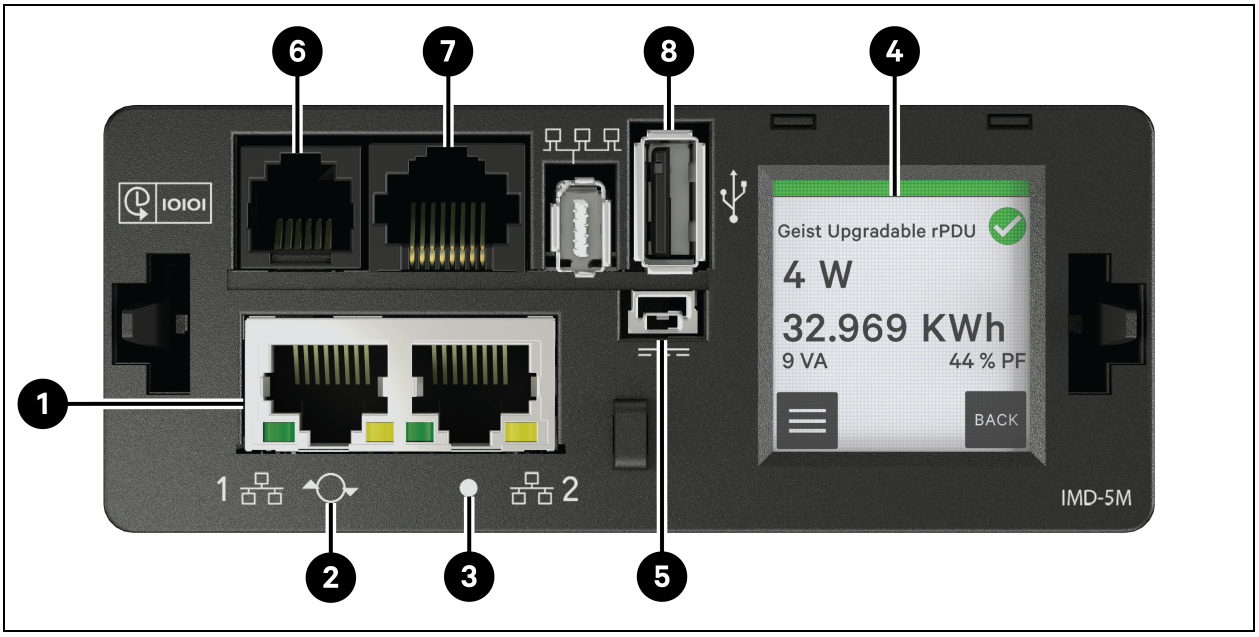
Table 5.6 Display Button Functions (continued)

Button	Symbol	Description
Center Button x3		Pressing this button three times within 2 seconds enables VLC mode. Pressing the button while VLC mode is active returns the unit to the standard current display.
Back and Forward Buttons	and	Pressing both buttons at the same time flips the display 180 degrees.
Back and Center Buttons	and	Pressing both buttons at the same time displays the primary IPv4 address of the unit.

5.1.5 Monitored and switched (IMD-5M)

All Vertiv™ Geist™ Monitored and Switched rPDUs are shipped with the IMD-5M module.

Figure 5.4 IMD-5M Module



Item	Name	Description
1	Dual ETHERNET ports	The dual ETHERNET ports act as a two-port ETHERNET switch, allowing for multiple devices to be daisy-chained. The dual ETHERNET ports can be independently configured dual ETHERNET network interfaces, allowing the rPDU to connect to two different networks.
2	Restart/Reset button	Press and hold the button for 10 seconds restarts the IMD. This acts as a power cycle for the IMD; it does not change or remove any user information. Press and hold the button for 25 seconds during normal operation will restore the default IP address and reset the user accounts.
3	RGB status LED	Green LED : Unit is up and running. Yellow LED : Unit is booting up.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Item	Name	Description
4	Touchscreen menu	Use the touchscreen menu to find the phase, line, and circuit current values (in amperes).
5	Redundant power input	If optional connection cable is plugged into second unit, the IMD will remain powered when rPDU loses power.
6	Remote Sensor Port	RJ-12 port for connecting a Vertiv™ plug-and-play remote digital sensors (sold separately). Each digital sensor has a unique serial number and is automatically discovered. GU2 PDUs support up to 16 sensors. The optional Vertiv™ A2D Converter can be added to support analog sensing.The optional SN-ADAPTER can be added to support Liebert® Integrated and Modular Sensors. For more information, see Available Sensors on page 115 .
7	Serial port	RS-232 via RJ-45 port.
8	USB port	USB port used to upload firmware, backup/restore device configuration, expand logging capacity via a USB storage device or support TP-Link wireless USB adapters. The USB port must be enabled - see USB on page 82 . Provides up to 0.5 watt for Unit Monitored Level and 5 watt for Monitored Outlet Level/Switched Unit Level/Switched Outlet Level.

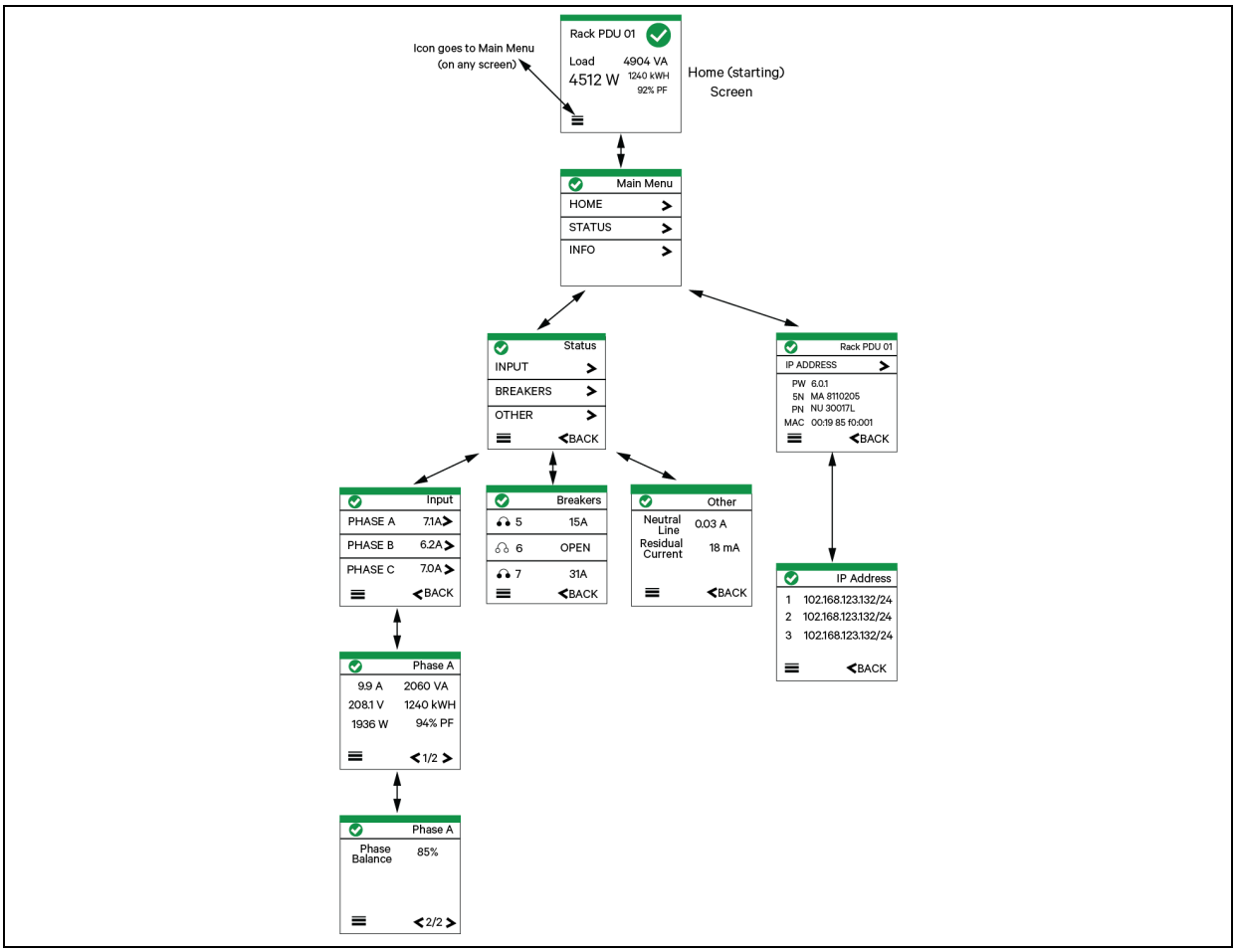
NOTE: Serial connection does not support flow control.

Touchscreen Menu Workflow

The home starting screen will show the wattage load, the voltage, kilowatts/hour, and the PF percentage. Clicking the bottom right hamburger button will direct to the main menu regardless of location in the flow. From the main menu, there are three options. Home will return to the first page with the aforementioned statistics. The status page will link to another menu page where there is navigation to pages with phase, breaker, or line information respectively. The INFO button will show the IP Address page.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.5 Touchscreen Menu Workflow Diagram



5.1.6 Rapid Spanning Tree Protocol (RSTP)

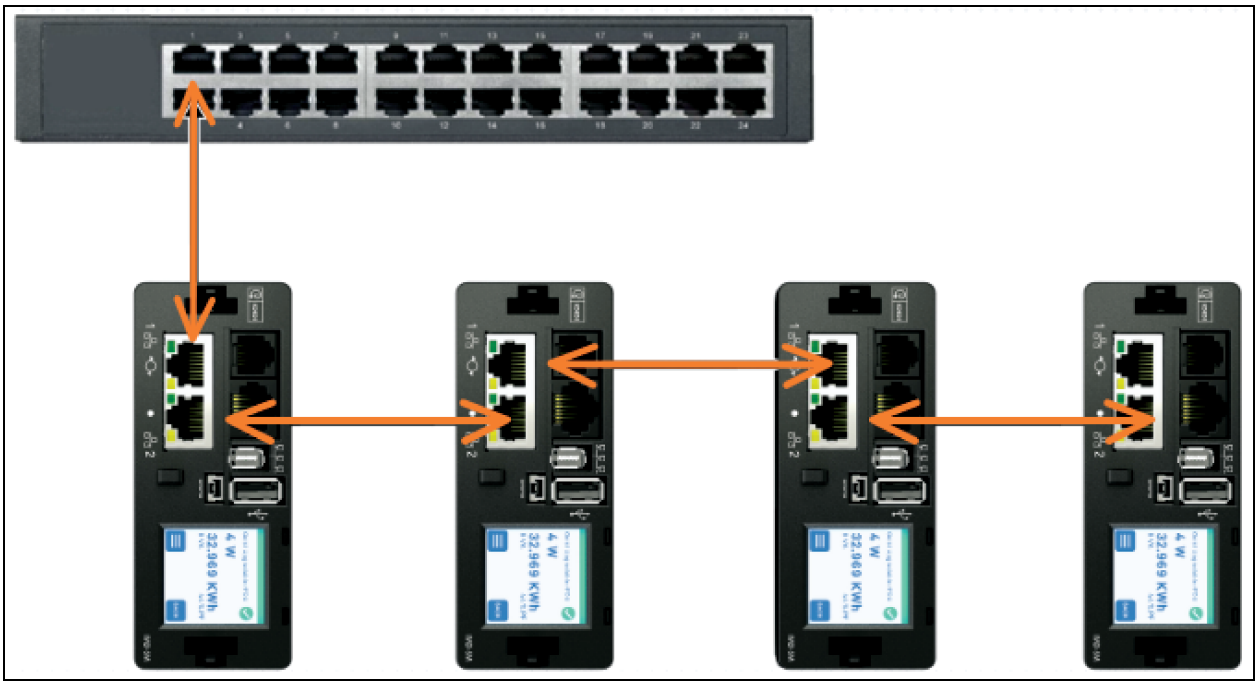
Upgradeable monitored devices, built with the IMD-5M, include two ETHERNET Ports that work together as an internal ETHERNET Bridge. One of these ports can be used to connect the IMD to an existing network or both ports can be used at the same time to connect one IMD to another in a daisy chain configuration.

Daisy-Chaining

- Use daisy chaining to reduce network switch port count.
- Rack PDUs are connected using an ETHERNET daisy chain.
- The head of the chain rack PDU connects to a network switch port.
- Each rack PDU has its own unique IP address.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.6 Daisy-Chaining

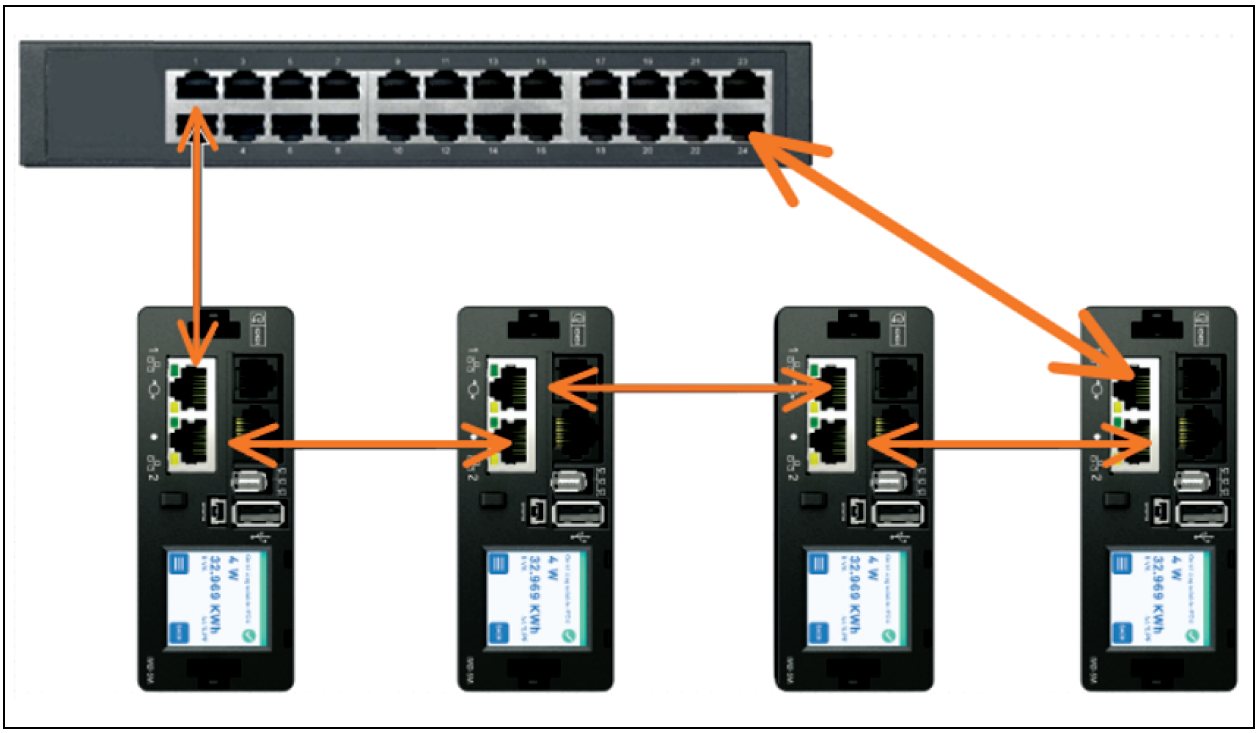


Fault Tolerant Daisy-Chaining

- Use fault tolerant daisy-chaining to provide resilient network connectivity.
- Rack PDUs are connected using an ETHERNET daisy chain.
- Both head and tail of the chain rack PDUs connect to network switch ports.
- Each rack PDU has its own unique IP address.
- Rapid Spanning Tree protocol (RSTP) must be configured to manage fault tolerance and maintain connectivity in the event of a cable fault or rack PDU power loss.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.7 Fault Tolerant Daisy Chaining



When both network interfaces are connected, the IMD implements a network bridging protocol called the Rapid Spanning Tree Protocol (RSTP). RSTP is an IEEE standard that is implemented by all managed bridges. Using RSTP, bridges in the network exchange information to find redundant paths or loops. IPv6 should be disabled when using redundant network connectivity.

When a loop is detected, the bridges in the network work together to temporarily disable the redundant paths. This allows the network to avoid broadcast storms caused by the loops. In addition, RSTP regularly checks for changes in the network topology. When a connection is lost, RSTP allows the bridges to quickly switch to a redundant path.

NOTE: RSTP protocol imposes a limit of 40 links between bridges, including IMDs.

NOTE: The Vertiv Intelligence Director cannot be used in conjunction with RSTP and redundant network connectivity.

5.2 Network Setup

The Upgradeable IMD has a default IP address for initial setup and access.

To restore the default IP address and reset all user-account information:

1. If the user-assigned address or passwords are lost or forgotten, press and hold the network reset button located below the ETHERNET Port for 15 seconds.
2. Holding the center button of the LED display for 10 seconds also resets the network and user account information.

The Network Page, located under the System tab, allows you to assign the network properties manually or use DHCP to connect to your network. Access to the unit requires the IP address to be known. Use of a static IP or a reserved DHCP is recommended. The default address is displayed on the front of the unit.

- IP Address: *192.168.123.123*

Proprietary and Confidential ©2024 Vertiv Group Corp.

- Subnet Mask: *255.255.255.0*
- Gateway: *192.168.123.1*

To access the unit for the first time, you must temporarily change your computer's network settings to match the 192.168.123.xxx subnet. To setup the unit, connect it to your computer's ETHERNET Port, then follow the appropriate instructions for your computer's operating system.

To set up the network for a Windows operating system:

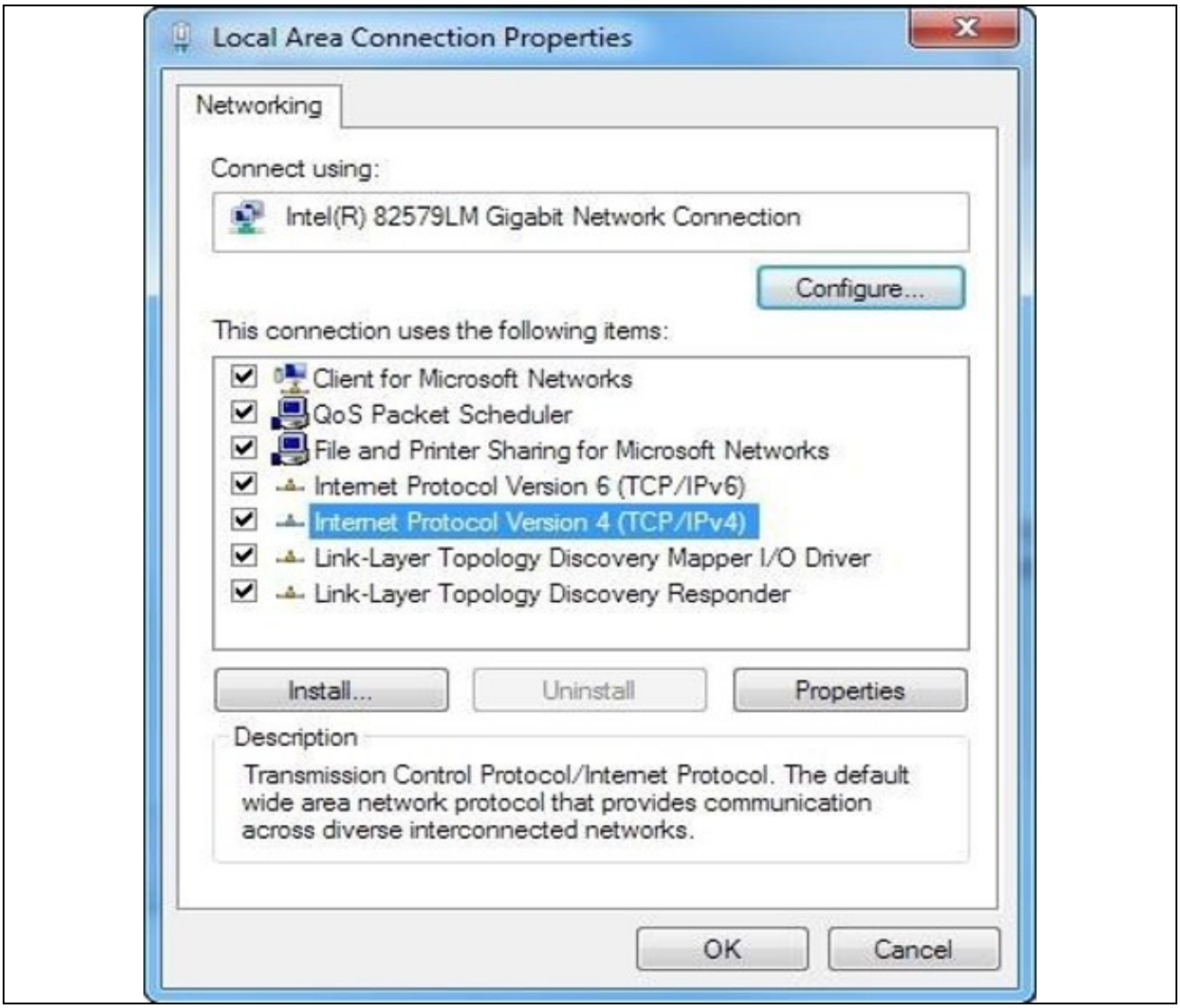
1. Access the network settings for your operating system.
   - Windows Server 2022 and 2019.
   - Using Microsoft Windows 10, click *Start>Network and Internet>Change Adapter Settings*.
   - Windows Microsoft Windows 11, click *Start>Network and Internet>Change Adapter Settings*.
2. Locate the entry under LAN, High Speed Internet or Local Area Connection that corresponds to the Network Card (NIC). Double click on the network adapter's entry in the Network Connections list.

NOTE: Most computers will have a single ETHERNET NIC installed, but a WiFi or cellular data adapter also shows as a NIC in this list. Be sure to choose the correct entry.

3. Click *Properties* to open the Local Properties window.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.8 Local Area Connection Properties

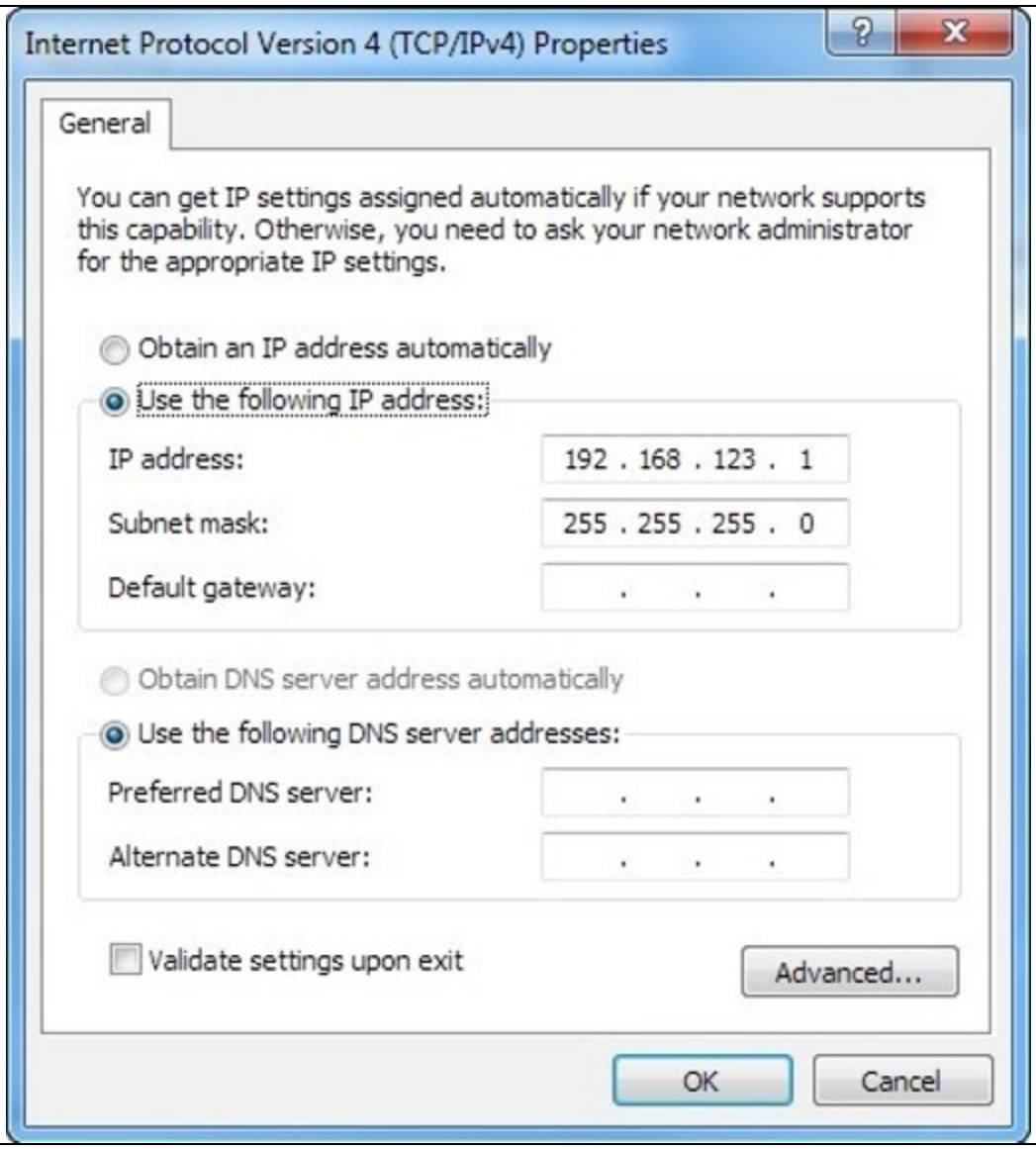


4. Select *Internet Protocol Version 4 (TCP/IPv4)* from the list, and click *Properties*.

NOTE: If you see more than one TCP/IP entry, as in the example above, the computer may be configured for IPv6 support as well as IPv4, make sure to select the entry for the IPv4 protocol. Write down the current NIC card settings so you can restore them to normal after you have completed the setup procedure.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.9 Internet Protocol Version 4



5. Choose *Use the following IP address*, set IP address to 192.168.123.1 and Subnet Mask to 255.255.255.0 . For initial setup, Default Gateway and the DNS Server entries can be left blank. Select *OK - OK* to close both the Internet Protocol Properties and Local Properties windows.
6. In a web browser, enter http://192.168.123.123 to access the unit. If you are setting up the unit for the first time, the unit requires you to create an Admin account and password before you can proceed.
7. After the Admin account is created, login to the unit.
8. By default, the default sensors page is displayed. Navigate to the *System tab*, then the *Network Page* to configure the device's network properties. The unit's IP address, Subnet Mask, Gateway and DNS settings can either be assigned manually or acquired via DHCP.
9. Click *Save*.

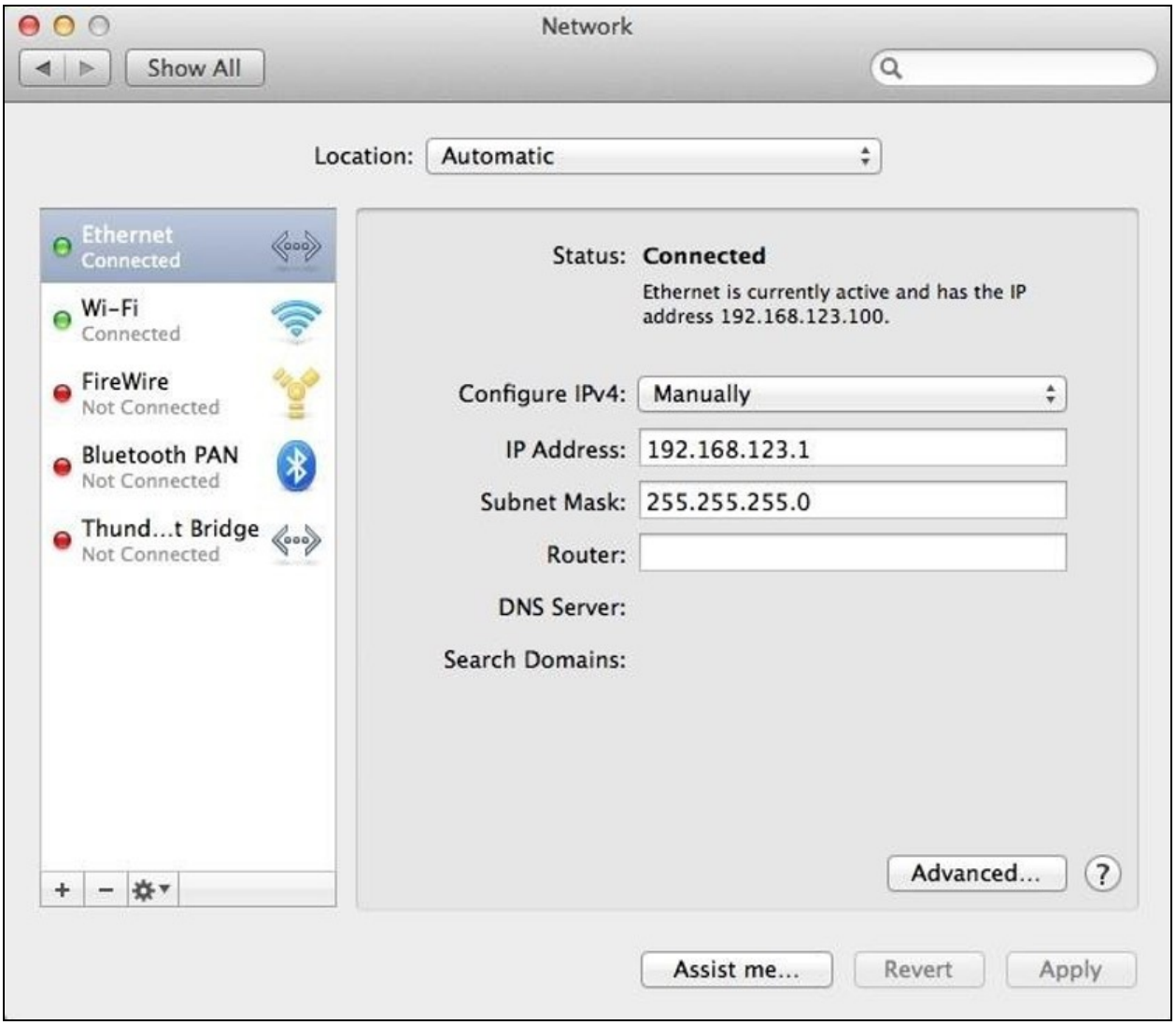
Proprietary and Confidential ©2024 Vertiv Group Corp.

NOTE: After the changes are saved, the browser will no longer be able to reload the web page from the 192.168.123.123 address and displays Page not Found or Host Unavailable message, this is normal. After you are finished configuring the unit's IP address, repeat the steps above, changing the computer's ETHERNET NIC card settings to the ones you wrote down prior to changing them.

To set up the network for a MAC:

1. Click the System Preferences icon on the Dock and choose *Network*.

Figure 5.10 MAC System Preferences



2. Ensure ETHERNET is highlighted on the left side of the NIC window. In most cases, there will be one ETHERNET entry on a Mac. Write down the current settings so you can restore them to normal after you have completed the setup procedure.
3. Select *Manually* from the Configure IPv4 drop-down list, set IP address to 192.168.123.1 and Subnet Mask to 255.255.255.0 and click *Apply*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

NOTE: The Router and DNS Server settings can be left blank for this initial setup. In a web browser, enter http://192.168.123.123 to access the unit. If you are setting up the unit for the first time, the unit requires you to create an Admin account and password before you can proceed.

4. After the Admin account is created, login to the unit.
5. By default, the default sensors page is displayed. Navigate to the *System* tab, then the *Network* page to configure the device's network properties. The unit's IP Address, Subnet Mask, Gateway and DNS settings can either be assigned manually or acquired via DHCP.
6. Click *Save*.

NOTE: After the changes are saved, the browser will no longer be able to reload the web page from the 192.168.123.123 address and displays Page not Found or Host Unavailable message; this is normal. After you are finished configuring the unit's IP address, repeat the steps above, changing the computer's ETHERNET NIC card settings to the ones you wrote down prior to changing them.

5.3 Web User Interface

The unit is accessible via a standard, unencrypted HTTP connection as well as an encrypted HTTPS (TLS) connection. Units will default to HTTP redirected to HTTPS unless the admin explicitly enables HTTP.

NOTE: An administrator account (username and password) must be created when logging in to the device the first time.

NOTE: If Clock not set. appears at the bottom right of the page, follow procedures in Time on page 81 .

5.3.1 Main menu

The Main Menu is located vertically on the far left side. See Figure 5.11 on the next page for Main Menu.

WARNING! Do not connect electric heaters, electric heating appliances or other electric appliances which may cause fire, electric shock, injuries when operated unattended.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.11 Main Menu

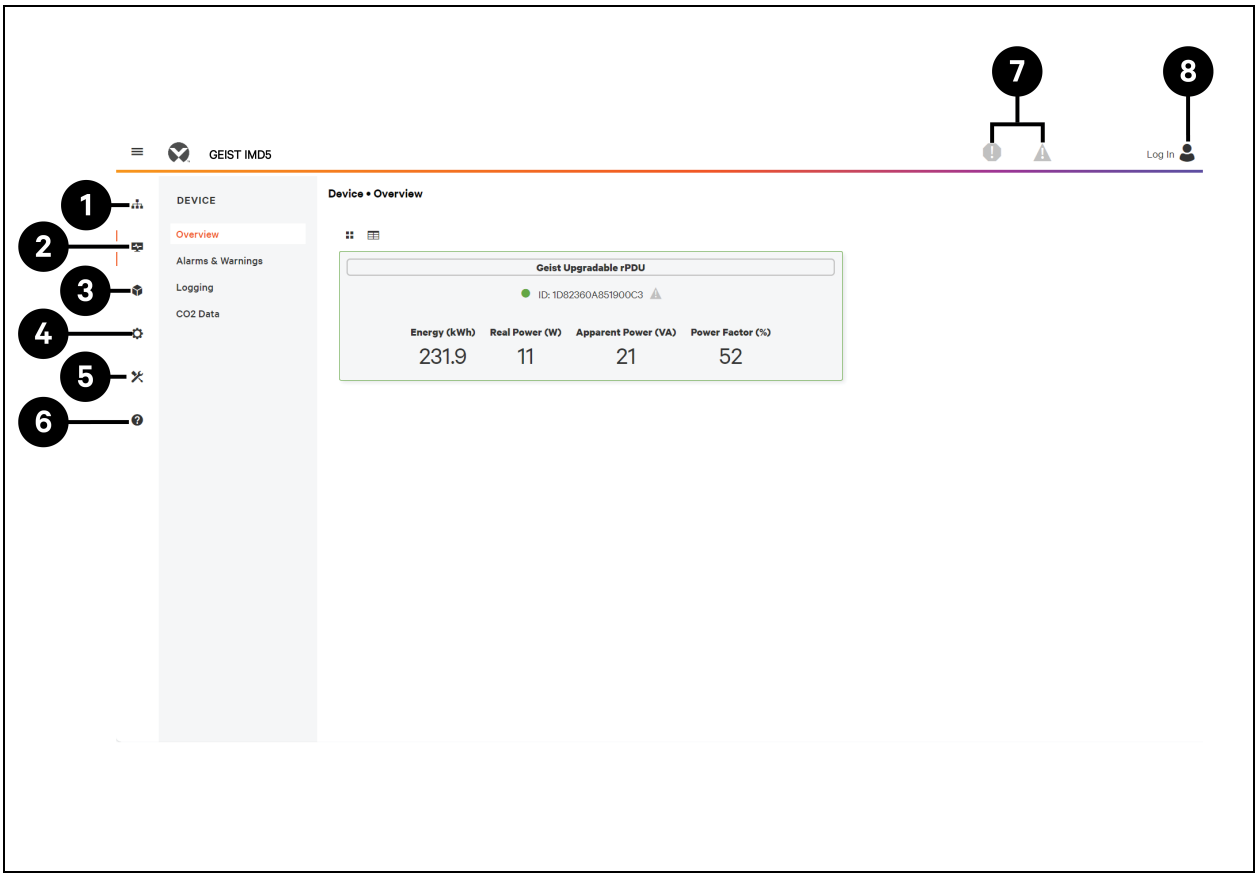


Table 5.7 Main Menu Descriptions

Item	Decription
1	Aggregation
2	Device
3	Provisioner
4	System
5	Utilities
6	Help
7	Alarms & Warnings
8	Log In/Log Out

5.4 Device Sub Menu

Click the Device Sub Menu to access *Overview, Alarms & Warnings, Logging* and *CO2 Data* menus.

Proprietary and Confidential ©2024 Vertiv Group Corp.

5.4.1 Overview

You must login before making any changes. Only users with control-level or higher authorizations have access to these settings.

Figure 5.12 Device Overview Sub Menu Descriptions

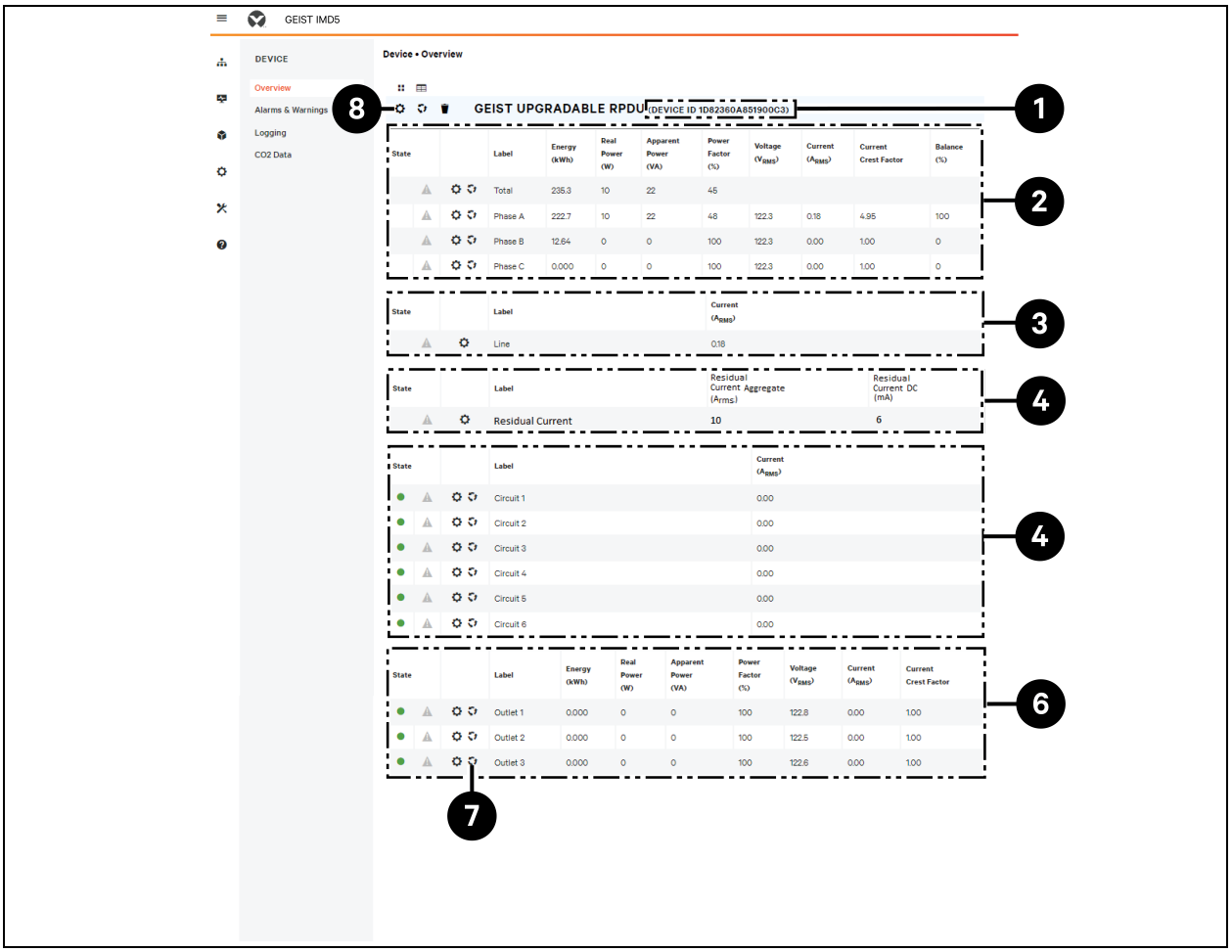


Table 5.8 Device Overview Sub Menu Descriptions

Number	Name	Description
1	Device ID	Unique product identification and cannot be changed. May be required for technical support.
2	Total and Individual Phase Monitor	Displays AC current, voltage, and power statistics for each individual phase and for the total of all phases combined. Current Crest Factor and Phase Balance (%) are also indicated.
3	Line	Displays the current (in Amps RMS) on 3-phase Wye units. This is not shown on single phase and 3-phase Delta units.
4	Residual Current	Only for rPDUs with RCM-B Feature. Displays Residual Current Aggregate (mA) and Residual Current DC (mA). Where applicable, display Residual Current for each Phase.
5	Current Monitor	Displays AC current draw statistics for each individual circuit on the rPDU.

Proprietary and Confidential ©2024 Vertiv Group Corp.

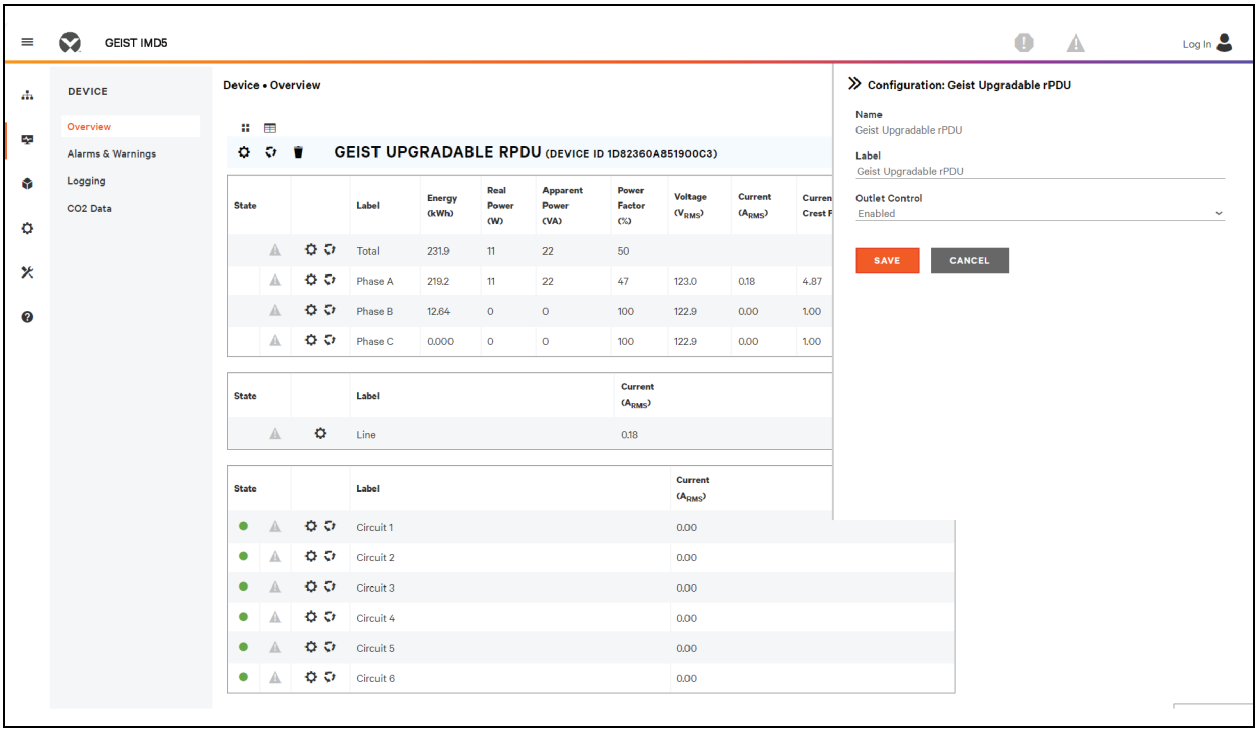
Table 5.8 Device Overview Sub Menu Descriptions (continued)

Number	Name	Description
6	Outlet Monitor	Applies to Outlet Monitored/Outlet Switched rPDUs ONLY - Displays AC current, voltage, and power statistics for each circuit and outlet. Current Crest Factor also indicated. (Outlet Level Power Monitoring and Switched Outlet Level Monitoring Only). Displays outlet status. (Switched and Switched Outlet Level Monitoring Only).
7	Operation Icon	Applies to Outlet Monitored/Outlet Switched rPDUs ONLY - Modify settings.
8	Configuration Icon	Applies to Outlet Monitored/Outlet Switched rPDUs ONLY - Modify label name.

To change a device label:

1. Click the Configuration icon to change label for the Vertiv™ Geist™ rPDU and change the label. The Name is the rPDU's factory name or model and cannot be changed.
2. Click *SAVE* .

Figure 5.13 Changing Device Label



Proprietary and Confidential ©2024 Vertiv Group Corp.

To change device operation:

1. Click the Operation icon.
2. Select the operation to perform:
   - **On/Off:** Turns all outlets On or Off.
   - **Reboot:** For outlets currently On, reboot cycles the outlets Off, then back On after the reboot hold delay. For outlets currently Off, reboot turns the outlets On.
   - **Cancel:** Cancels the current operation if it has not been completed.
   - **Reset Energy:** Resets the total energy measured in kWH.
   - **Restore Defaults:** Restores device settings to their factory default. This includes Labels, Delays and Power-on Actions for the device.

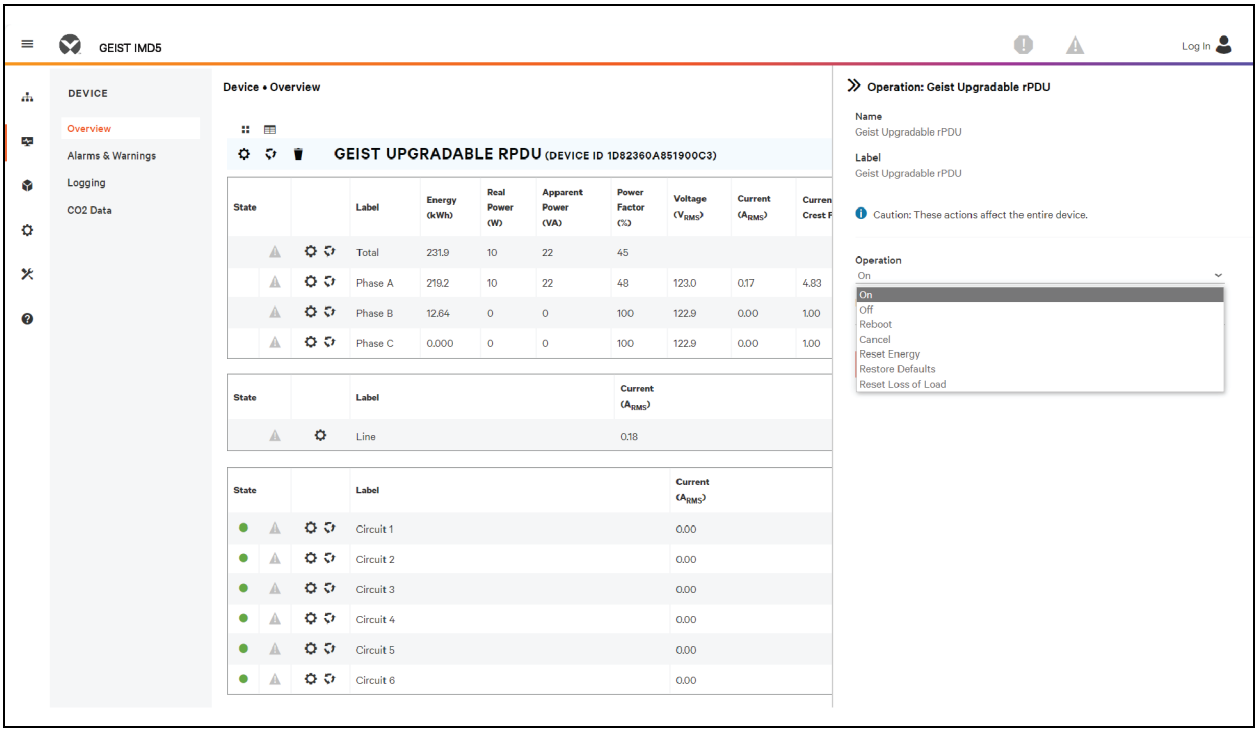
NOTE: These actions affect the entire device.

NOTE: On/Off and Reboot operations apply to Outlet Switched Geist™ rPDUs only.

3. For operations involving the state of the outlets, setting Delay to *True* uses the current Delay configuration for each outlet when performing the selected operation.
4. Click *SAVE* to issue the action.

NOTE: Power-on action delays refer to the time since the unit was plugged in, not the time since it fully booted. They may execute before the unit fully boots.

Figure 5.14 Device Change Operation

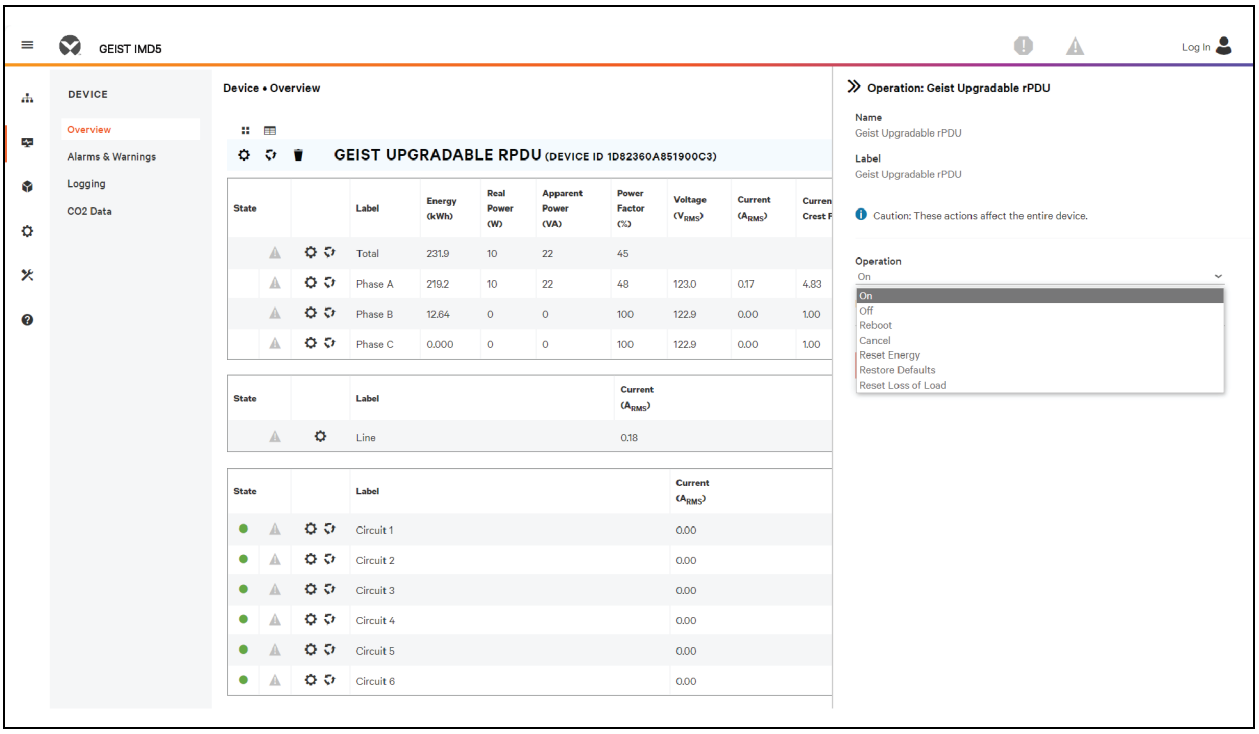


Proprietary and Confidential ©2024 Vertiv Group Corp.

To change a phase or circuit label:

1. Click the Configuration icon for the phase or circuit and change the label. The Name is the physical phase or circuit name and cannot be changed.
2. Click *SAVE*.

Figure 5.15 Changing Phase or Circuit Label

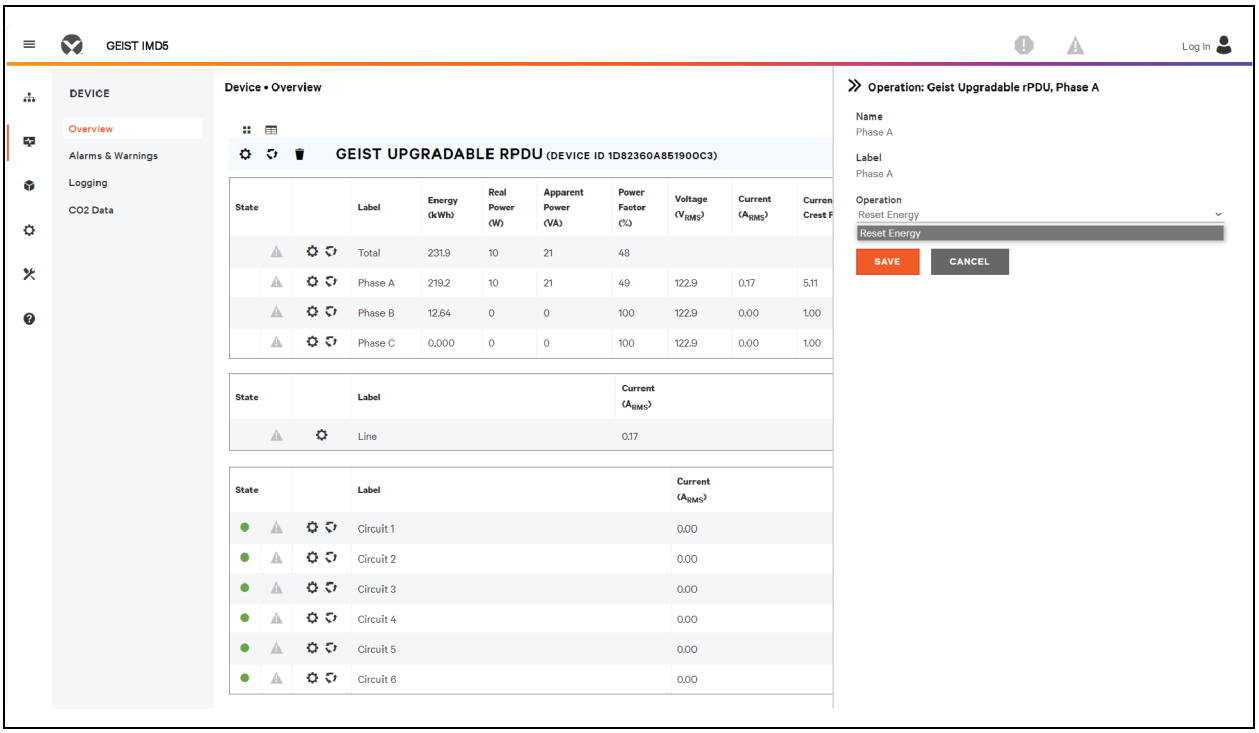


To change phase operation:

1. Click the Operation icon.
2. Select *Reset Energy* to reset the total energy measured in kWH for the selected phase.
3. Click *SAVE* to issue the action.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.16 Changing Phase Operation

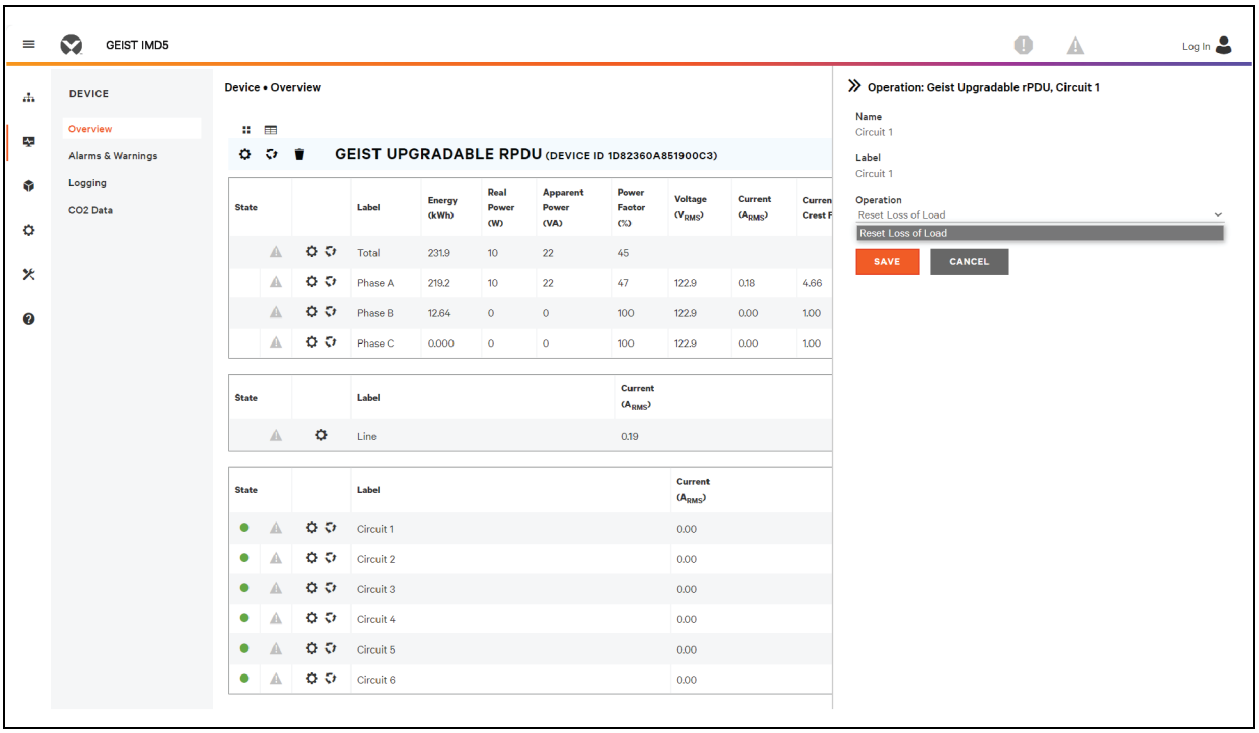


To change circuit operation:

1. Click the Operation icon.
2. Select *Reset Loss of Load* to reset the Loss of Load alarm.
3. Click *SAVE* to issue the action.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.17 Changing Circuit Operation



NOTE: This step is required when state shows a loss of load alarm and the issue has been resolved. Loss of load alarm is triggered by a sudden drop of current detected by the circuit breaker's current measuring transducer when operating close to the circuit load limit. For the Switched Upgradeable horizontal units, the loss of load alarm is additionally triggered by circuit breaker loss of voltage (regardless of circuit load).

To configure an outlet:

NOTE: Applies to Outlet Monitored/Outlet Switched Vertiv™ Geist™ rPDUs only.

1. Click the Outlet Configuration icon.
2. Change the configurations, as needed.
   a. Label of the outlet.

NOTE: Steps 2b through 2k apply only to switched outlets.

   b. State: The outlet's current state (On or Off).
   c. Mode: How the outlet will be controlled:
      - Manual Control: The outlet state is controlled using the web user interface, SNMP or the API.
      - Alarm Control (normally off, on when any associated alarm trips): The outlet state is set normally Off and will be switched On when any outlet alarm event is tripped.
      - Alarm Control (normally on, off when any associated alarm trips): The outlet state is set normally On and will be switched Off when any outlet alarm event is tripped.
      - Alarm Control (normally Off, on when all associated alarm trips): The outlet state is set normally Off and will be switched On when all outlet alarm events are tripped.

Proprietary and Confidential ©2024 Vertiv Group Corp.

- **Alarm Control (normally on, off when all associated alarm trips):** The outlet state is set normally On and will be switched Off when all outlet alarm events are tripped.

d. **Pending State:** The state the outlet is currently transitioning to.

e. **Time To Action:** The time left before the pending action takes place. This is adjusted using Delays.

f. **On Delay:** The time, in seconds, the unit waits before switching an outlet On.

g. **Off Delay:** The time, in seconds, the unit waits before switching an outlet Off.

h. **Reboot Delay:** The time, in seconds, the unit waits before rebooting an outlet.

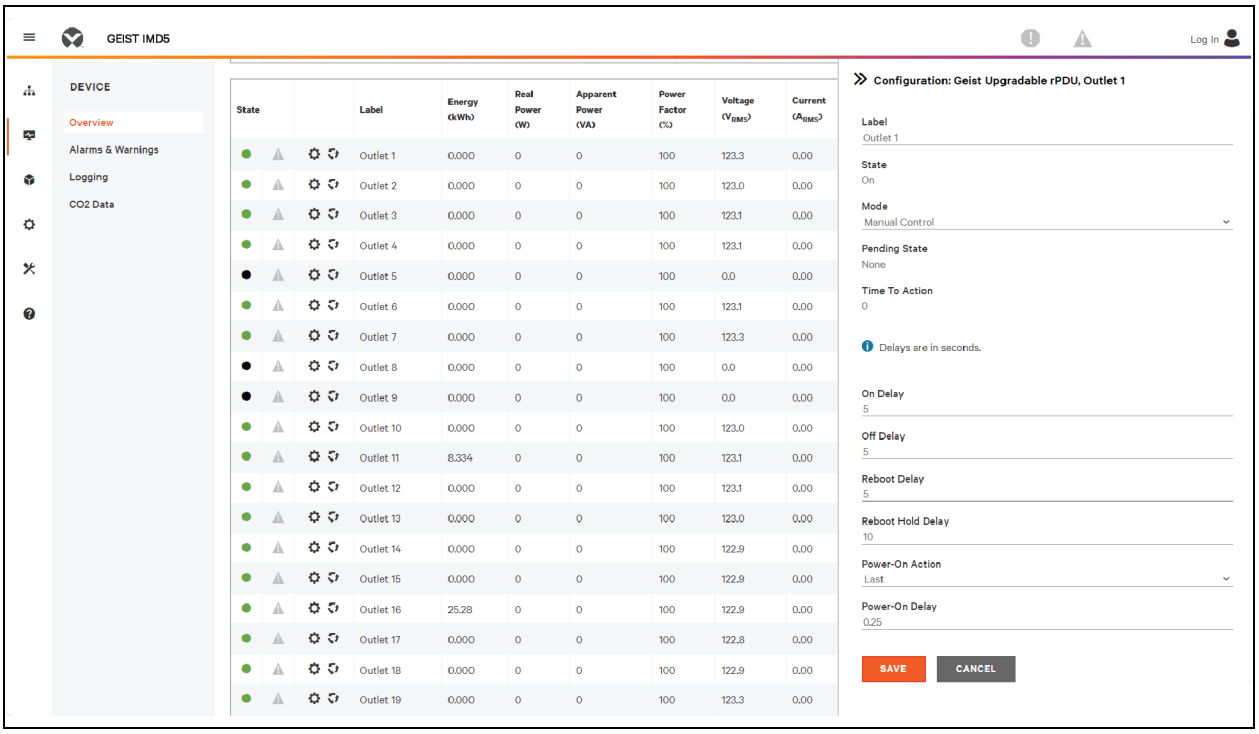
i. **Reboot Hold Delay:** The time, in seconds, the unit waits after switching the outlet Off, before switching an outlet back On during a reboot.

j. **Power-On Action:** Describes the state the outlet will start when powered On (On, Off or Last).

k. **Power-On Delay:** The time, in seconds, the unit waits after being powered On before powering On the outlet.

3. Click *SAVE*.

Figure 5.18 Outlet Configuration



To change outlet operation:

NOTE: Applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rPDUs only.

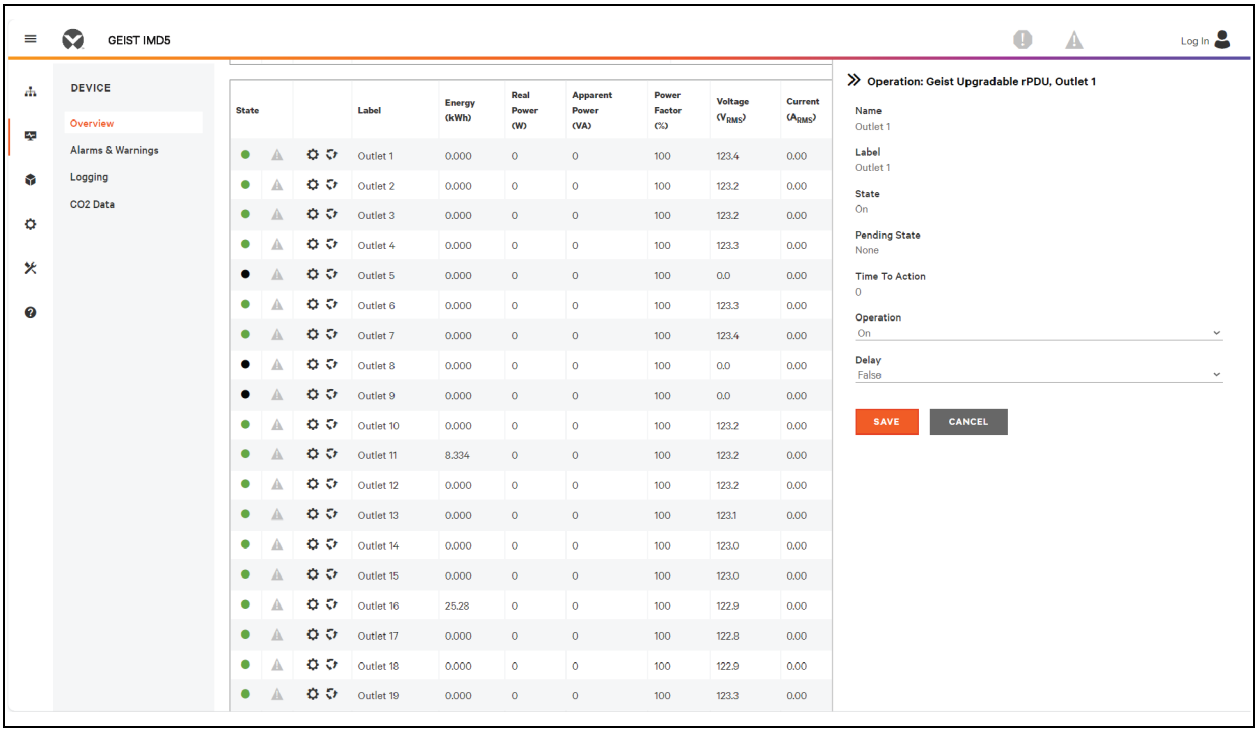
1. Click the desired Outlet Operation icon.
2. Select the operation to perform:
   - **On/Off:** Turns the selected outlet On or Off.
   - **Reboot:** For outlets currently On, reboot cycles the outlets off, then back On after the reboot hold delay. For outlets currently Off, reboot turns the outlets On.
   - **Cancel:** Cancels the current operation if it has not been completed.

Proprietary and Confidential ©2024 Vertiv Group Corp.

- **Reset Energy:** Resets the total energy measured in kWH for the selected outlet.

3. For operations involving the state of the outlets, setting Delay to *True* uses the current Delay configuration for each outlet when performing the selected operation.
4. Select *SAVE* to issue the action.

Figure 5.19 Changing Outlet Operation



5.4.2 Alarms & Warnings

The Alarms & Warnings page allows you to establish alarm or warning conditions (events) for each power and circuit reading. Events are triggered when a measurement exceeds a user-defined threshold, either going above the threshold (high-trip) or below it (low-trip). Events are displayed in different sections, based on the device or measurement the event is associated with. Each event can have one or more actions to be taken when the event occurs.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.20 Alarms & Warnings Page

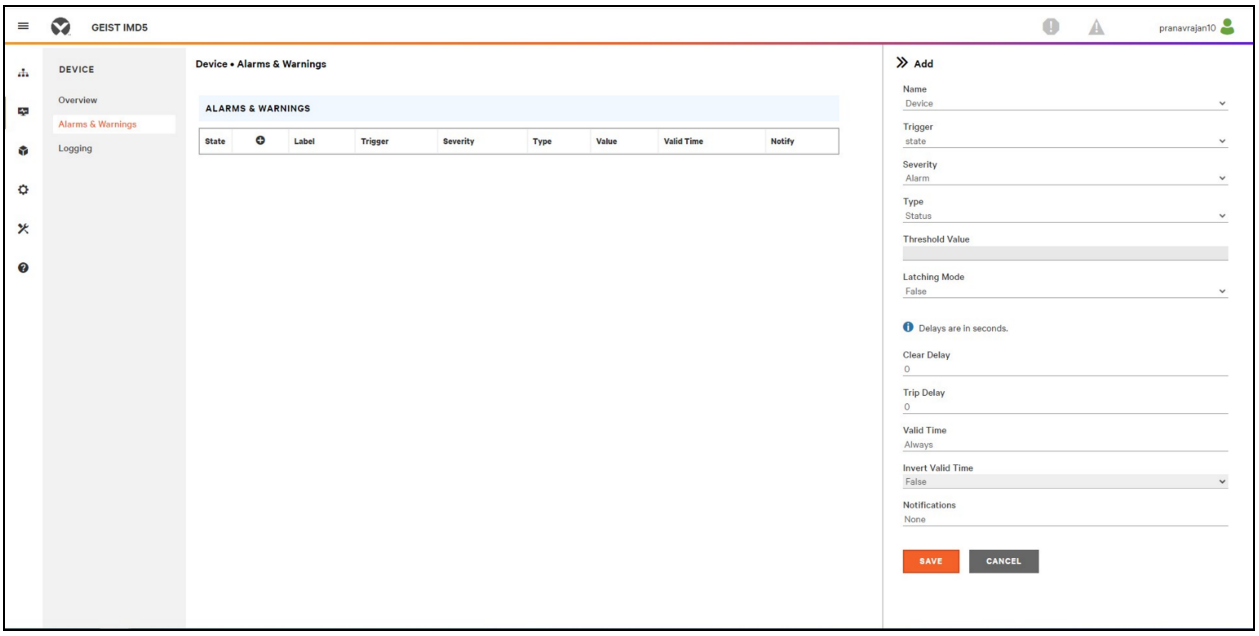


Table 5.9 Alarms & Warnings Descriptions

Number	Description	Symbol	Description
1	Status of each event.		Warning symbol. Event is displayed in orange.
			Alarm symbol. Alarm is displayed in red.
			Acknowledged event symbol. Symbol remains until the condition measured returns to normal.
2	Add/Delete/Modify alarms and warnings.		Add new alarms and warnings.
			Modify existing alarms and warnings.
			Delete existing alarms and warnings.
3	Notify user of tripped Events and request acknowledgment.	N/A	Empty, if there is no alert condition.
			When a warning or alarm event occurs, you can click on this symbol to acknowledge the event and stop the unit from sending any more notifications about it. **NOTE: Clicking this symbol does not clear the warning or alarm event; it just stops the notifications from repeating.**
4	Displays the conditions for the alarms and warnings settings.		

Proprietary and Confidential ©2024 Vertiv Group Corp.

To add a new Alarm or Warning Event:

1. Click the *Add/Modify Alarms* and *Warnings* button.
2. Set the desired conditions for this event as follows:
   a. From the drop-down lists, select the name of the phase or circuit, the trigger measurement, the severity and the type.

NOTE: High trips if the measurement goes above the threshold and low trips if the measurement goes below the threshold.

   b. Enter the desired Threshold Value (any number between -999.0 through 999.0).
   c. Enter the desired Clear Delay time in seconds. Any value other than *0* means once this event is tripped, the measurement must return to normal for this many seconds before the event will clear and reset. Clear Delay can be up to 14,400 seconds (4 hours).
   d. Enter the desired Trip Delay time in seconds. Any value other than *0* means that the measurement must exceed the threshold for this many seconds before the Event will be tripped. Trip Delay can be up to 14,400 seconds (4 hours).
   e. Latching Mode, if enabled, this event and its associated actions remain active until the event is acknowledged, even if the measurement subsequently returns to normal.
   f. To specify where the alert notifications are sent when this alarm or warning event occurs, click the Add icon to create a new action.
   g. Select the desired options from the drop-down menu:
      - Target is the email address or SNMP manager where the notifications are sent when the event is tripped. For more information on configuring a target email address, see Email on page 83 .
      - Or, when an outlet number is selected as the target, the outlet state switches when an event is tripped and remains in the switched state until the event resets or is acknowledged. For this option, the outlet mode must be configured for Alarm Control, see Alarms & Warnings on page 50 .

NOTE: Target Delays and Repeats are shared across all alarms. If multiple delay or repeat values are needed for specific targets, each one must be added to the target list and then the appropriate Enabled box must be checked on each alarm.

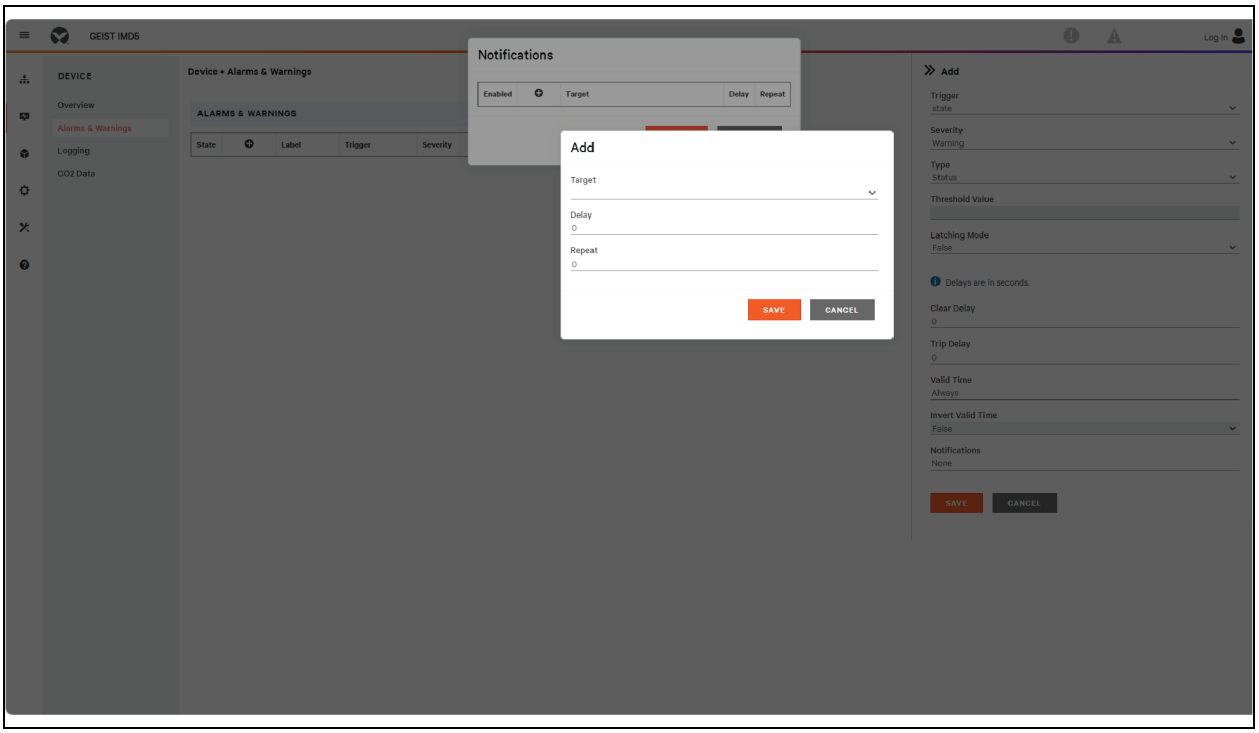
NOTE: Applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rPDUs only.

      - Delay determines how long this Event must remain tripped before this Action's first notification is sent. This is different from the Trip Delay above. Trip Delay determines how long the threshold value has to be exceeded before the Event itself is tripped. This delay determines how long the Event must remain tripped before this Action occurs. Delay can be up to 14,400 seconds (4 hours). A Delay of *0* will send the notification immediately.
      - Repeat determines whether multiple notifications will be sent for this Event Action. Repeat notifications are sent at the specified intervals until the Event is acknowledged or until the Event is cleared and reset. The Repeat interval can be up to 14,400 seconds (4 hours). A Repeat of *0* disables this feature and only one notification will be sent.
3. Click *SAVE* to save this notification action.

NOTE: More than one action can be set for an alarm or warning. To add multiple actions, just click the Add icon again and set each one as desired. Each alert can have up to 32 Actions associated with it.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.21 Adding Alarms & Warnings Window

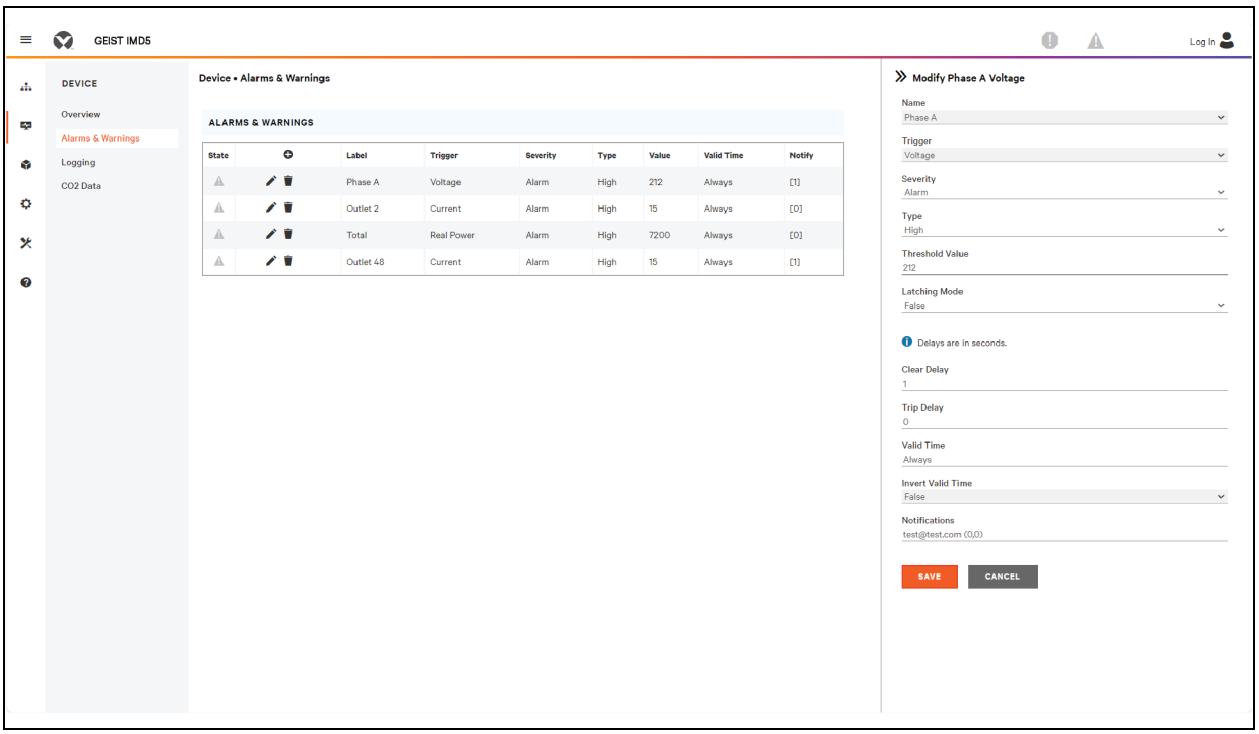


Proprietary and Confidential ©2024 Vertiv Group Corp.

To change an existing alarm or warning event:

1. Click the Modify icon next to the alarm or warning event you wish to change.
2. Modify the settings as needed and click *SAVE*.
3. After an action is added, it has a checkbox in the enabled column at the far left. By default, when an action is added it is unchecked (disabled). Click the *checkbox* to enable it. This allows you to selectively turn different actions On and Off for testing.

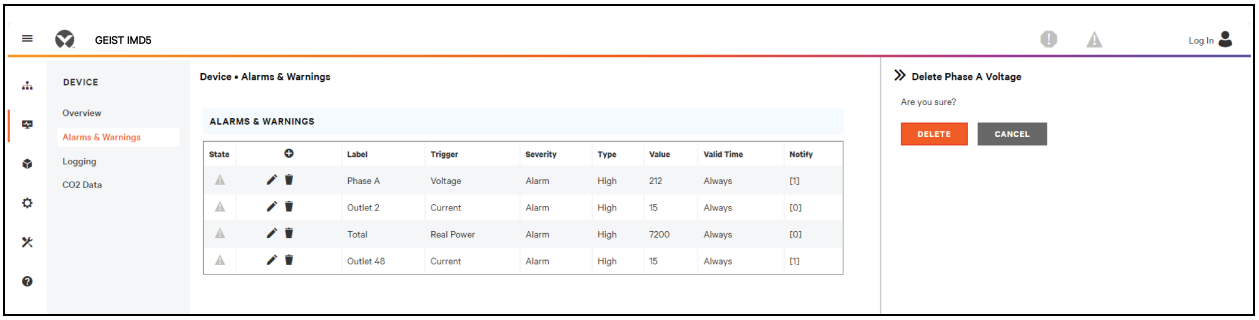
Figure 5.22 Changing Alarms & Warning Window



To delete an existing alarm or warning event:

1. Click the Delete icon next to the alarm or warning event you wish to remove.
2. Click *DELETE* and *SAVE* to confirm.

Figure 5.23 Deleting Alarms & Warning Event



Proprietary and Confidential ©2024 Vertiv Group Corp.

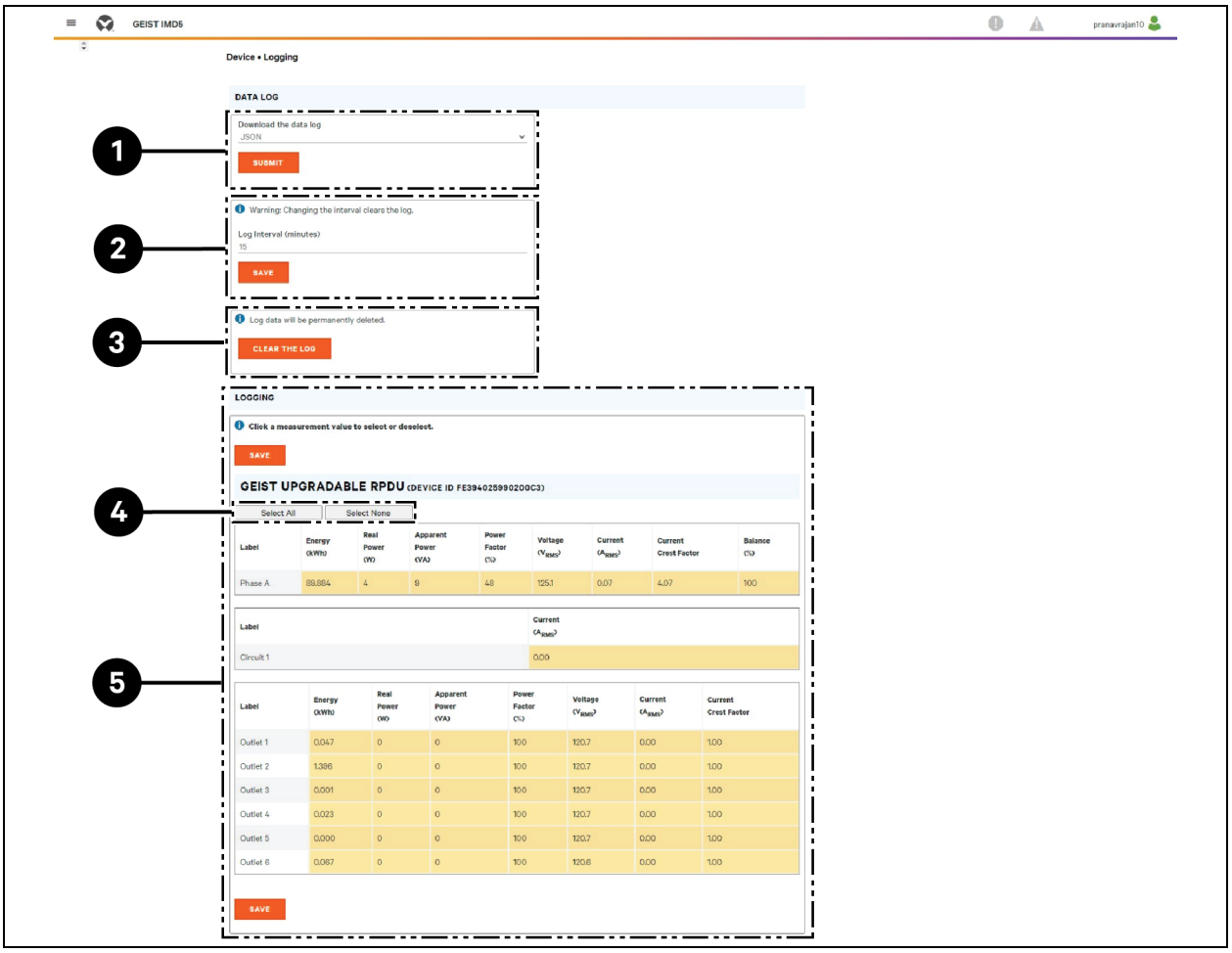
5.4.3 Logging

The Logging page allows you to access the historical data recorded by the Vertiv™ Geist™ rPDU by selecting the desired sensors and time range to be logged. The Logging page permits selecting all or selecting none.

To select or deselect the measurement value:

1. Click the Device icon and click on the Logging sub menu.
2. From Logging page, click *Select All* to select the measurement value and click *Select None* to deselect the measurement value.

Figure 5.24 Logging Page



Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 5.10 Logging Page Descriptions

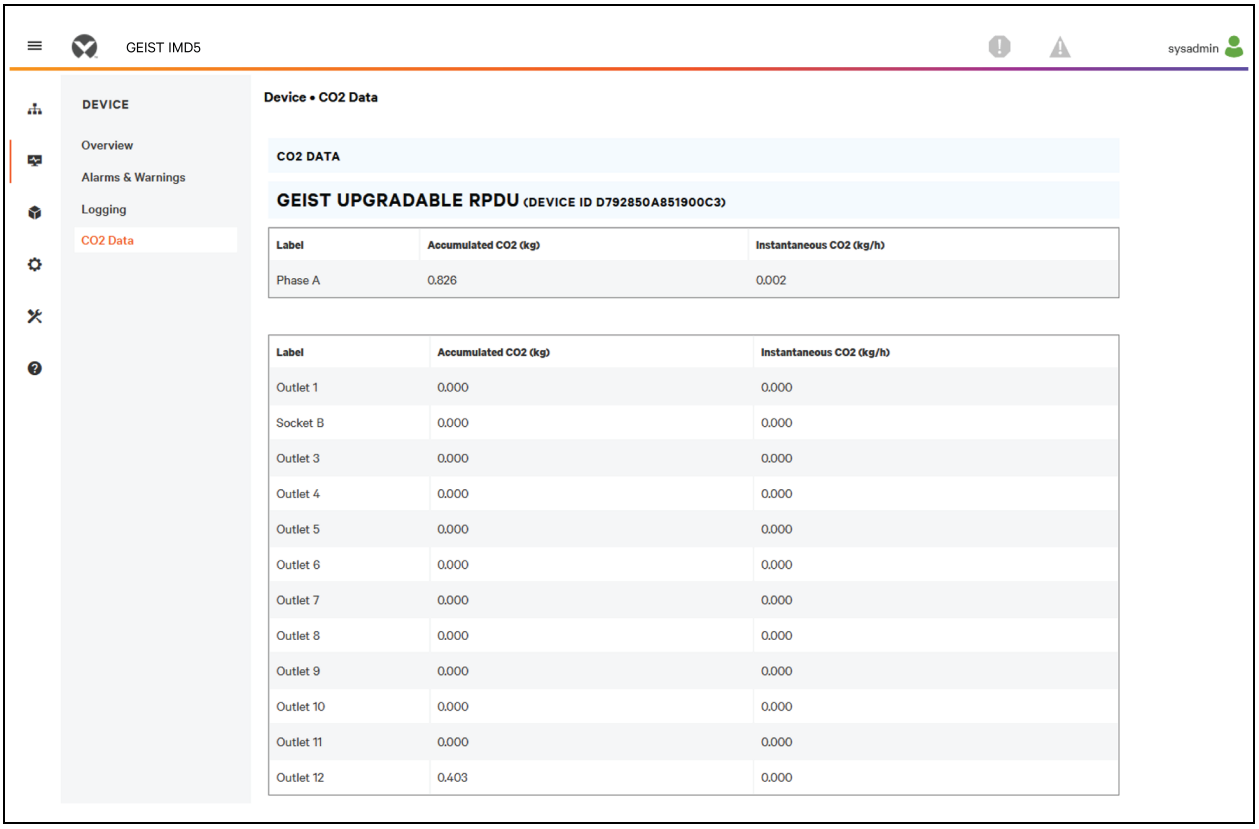
Item	Name	Description
1	Download the data log	Click the drop down menu and select one of the options : *JSON* for the *JSON* format. CSV for the .csv format in spreadsheet software. Click *SUBMIT* button to download the data log.
2	Log interval	The frequency at which data is written to the log file. The logging interval can be 1 to 600 minutes; the default setting is 15 minutes. **WARNING! Log data will be permanently deleted.**
3	Clear the log	Delete the log file. **WARNING! Log data will be permanently deleted.**
4	Select All/Select None	Click *Select All* to select the measurement value and click *Select None* to deselect the measurement value.
5	Logging	Click the measurement value to select or deselect desired logging parameters. By default, all measurements are selected. Click *SAVE* to save changes.

NOTE: The maximum loggable time frame is determined by number of measurements being logged and the interval at which data is written to the log file.

Proprietary and Confidential ©2024 Vertiv Group Corp.

5.4.4 CO2 Data

Figure 5.25 CO2 Home Page

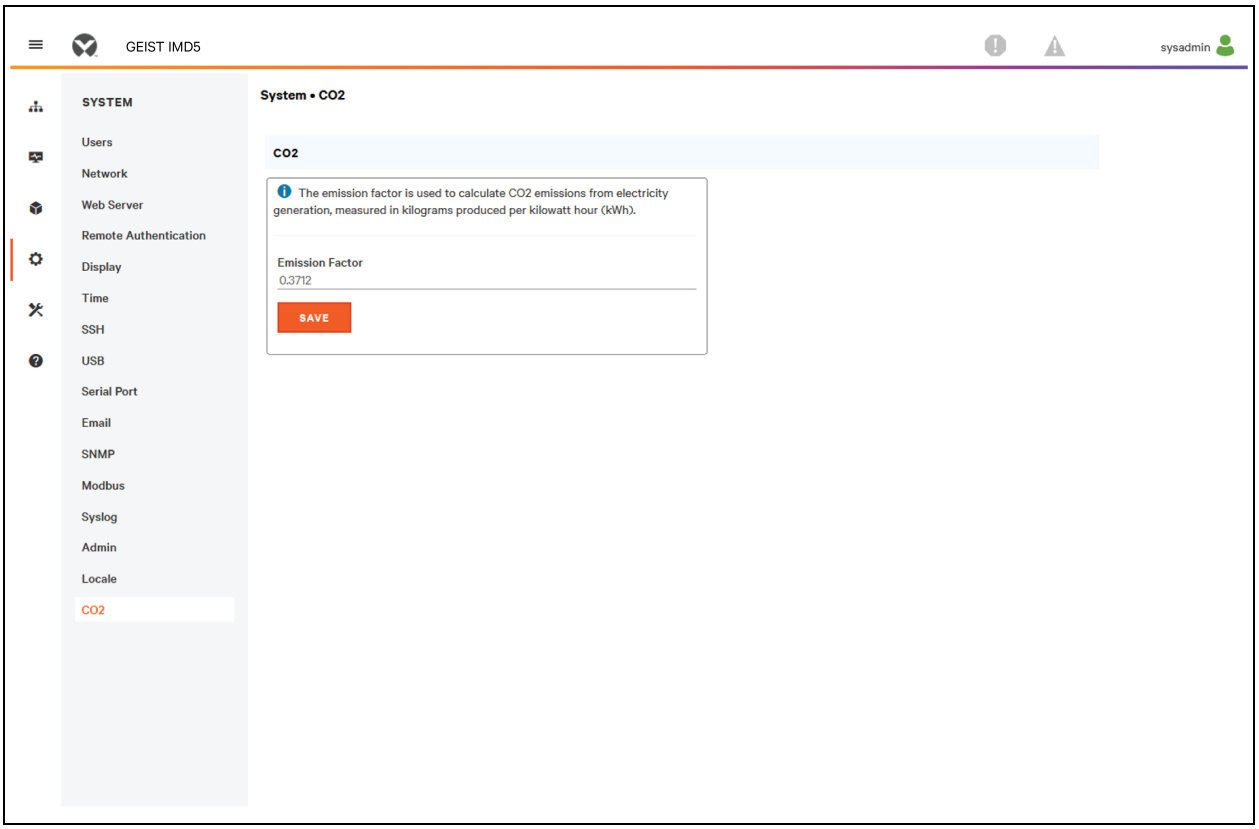


Label	Accumulated CO2 (kg)	Instantaneous CO2 (kg/h)
Phase A	0.826	0.002

Label	Accumulated CO2 (kg)	Instantaneous CO2 (kg/h)
Outlet 1	0.000	0.000
Socket B	0.000	0.000
Outlet 3	0.000	0.000
Outlet 4	0.000	0.000
Outlet 5	0.000	0.000
Outlet 6	0.000	0.000
Outlet 7	0.000	0.000
Outlet 8	0.000	0.000
Outlet 9	0.000	0.000
Outlet 10	0.000	0.000
Outlet 11	0.000	0.000
Outlet 12	0.403	0.000

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.26 System Tab of CO2



NOTE: There are three pages associated with CO2 page. The first page is the CO2 data page under Device (Figure 5.25 on the previous page), which shows accumulated and instantaneous calculations for the phases and outlets. The second page is CO2 page under System where you set the Emission Factor to calculate CO2 per kWH. The default CO2 Emission Factor will be set to 0.3172. The third page is on the help-info page; The Lifetime CO2 is based on the Lifetime Energy. If a user does a reset on the energy usage on a PDU or a specific outlet, the value will return to 0. However, the Lifetime Energy of that component will not get reset to 0.

5.5 Provisioner Sub Menu

The Provisioner sub menu allows the user to discover locally connected Vertiv™ Geist™ rPDUs. The user can update their firmware and configure them by uploading a configuration settings file.

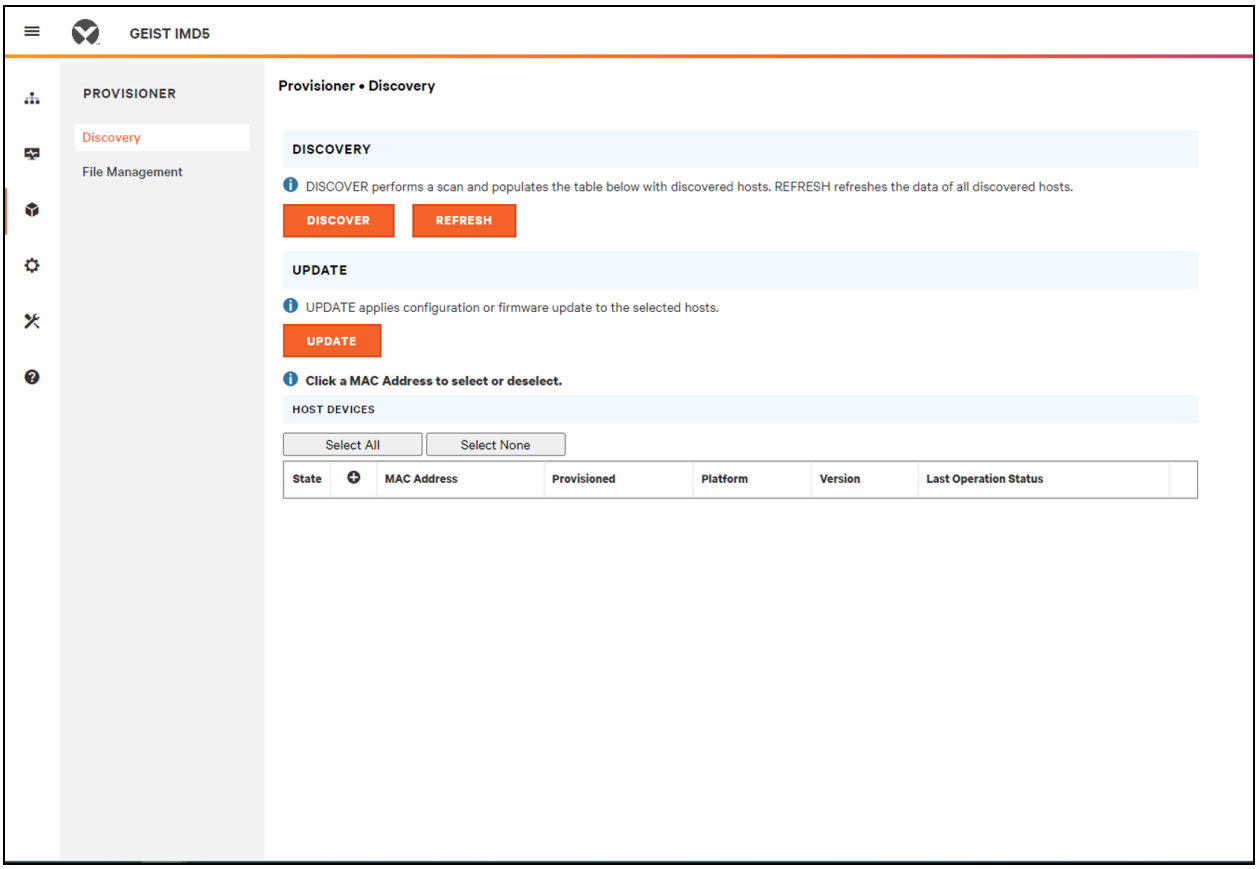
The Provisioner sub menu provides the ability to configure device settings (example, alarms) and system settings. This functionality can provision:

- IMD-5M running 6.x.x Firmware.
- rPDUs running 5.x.x firmware (IMD models 3E, 03E, 3E-S and 03E-S).
- Factory fresh or previously configured Geist™ rPDUs with 6.1.0.
- Rack PDUs connected directly to the local network or connected as part of a Vertiv Intelligence Director (aggregation) network.
- All or selected discovered Geist™ rPDUs.

Proprietary and Confidential ©2024 Vertiv Group Corp.

NOTE: You must be logged in as Administrator-level user to utilize the Provisioner. IPV6 must be enabled on the Geist™ rPDUs being discovered It is possible to configure most items in the System user interface menu. Other settings such as sensor settings and alarms cannot be configured with this version of the provisioning tool.

Figure 5.27 Provisioner Sub Menu Page

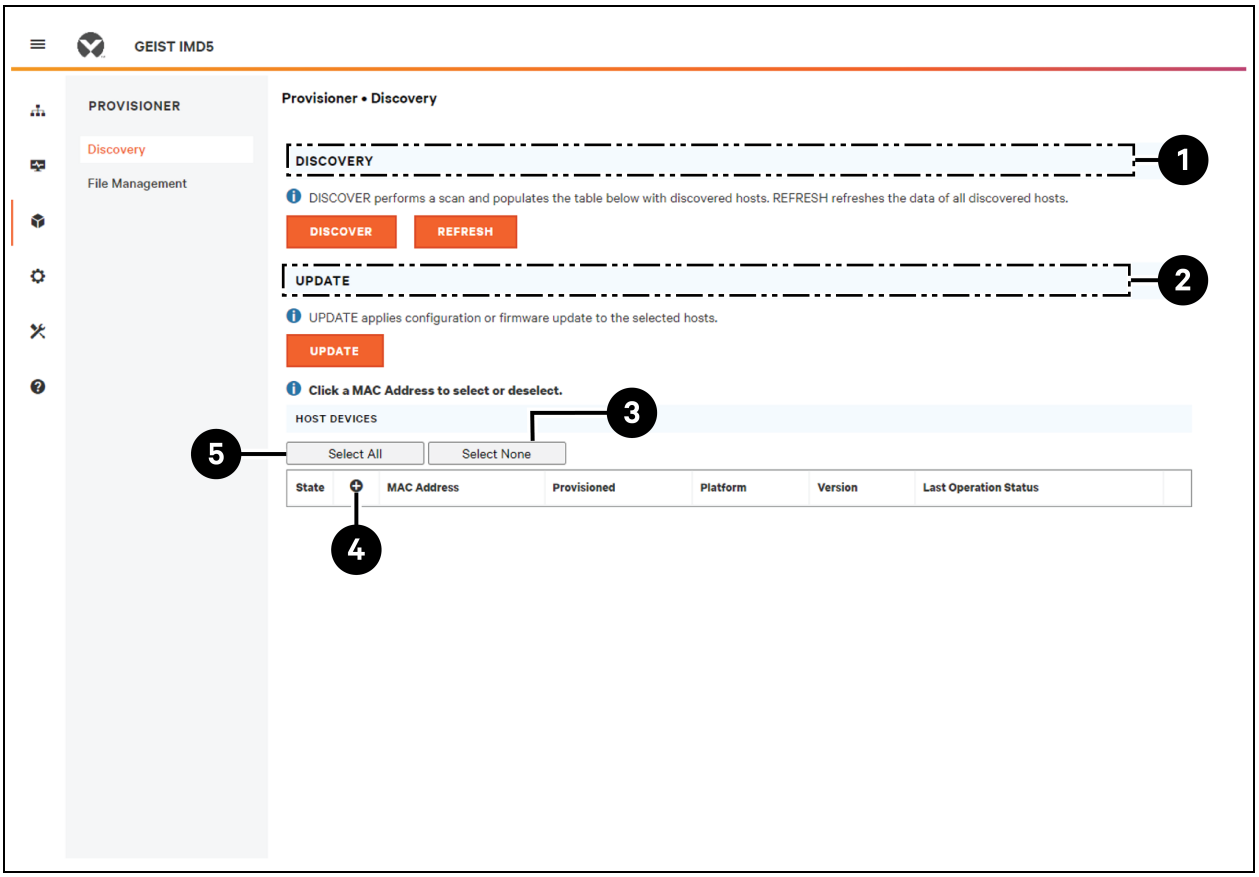


5.5.1 Discovery

1. Click on *DISCOVER* to identify locally connected Vertiv™ Geist™ rPDUs.
2. Click all the Geist™ rPDUs in the listing that you would like to update firmware and/or configuration. Those units selected will be highlighted in green. You may also click the *Select All* to update all Geist™ rPDUs in listed.
3. Click on *UPDATE* to update all selected Geist™ rPDUs with firmware file and/or configuration file.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.28 Discovery



Number	Name	Description
1	Discover	Identifies local and network connected rack PDUs
2	Update	Updates firmware and/or configuration of selected rPDUs
3	Select None	Select none to unselect all selections
4	Add MAC address	Allows manually entered rPDUs by MAC address
5	Select All	Selects all connected rPDUs

NOTE: You must load the firmware and configuration files before performing this step in the File Management TAB.

5.5.2 File management

Firmware Files:

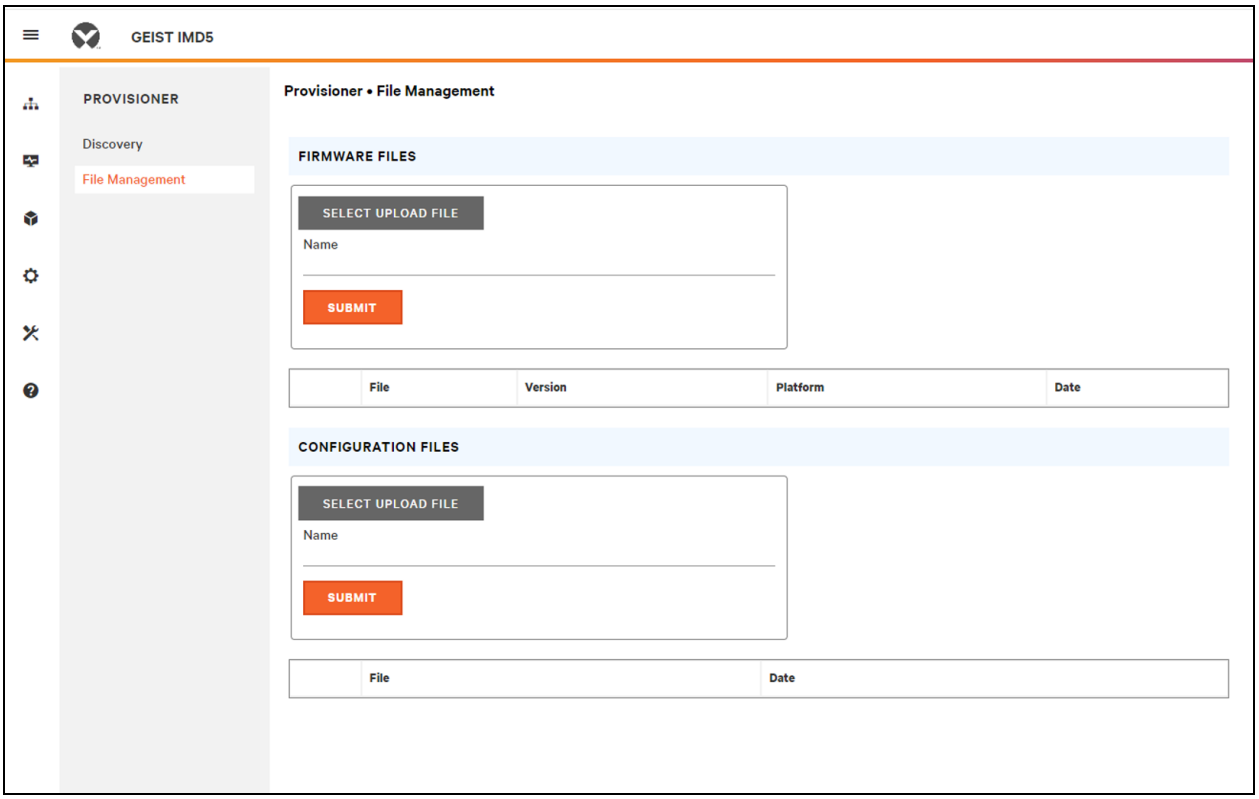
1. Click *SELECT UPLOAD FILE* and select the *.firmware file* from the Open window.
2. Click *SUBMIT*. Firmware file will be listed.

Configuration Files:

1. Click *SELECT UPLOAD FILE* and select the *.config file* from the Open window.
2. Click *SUBMIT*. Configuration file will be listed.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.29 File Management Page



See Provisioner - Format of the configuration settings file on page 121 for examples of configuration setting files used by the Provisioner and the necessary format for the file.

5.6 System Sub Menu

NOTE: You must be logged in as Administrator to modify settings in the System tab.

5.6.1 Users

The Users page in the System menu allows you to manage or restrict access to the unit's features by creating accounts for different users.

NOTE: Web/SSH/CLI account lockout policy: An account is locked for 30 minutes when 10 sequential unsuccessful login attempts are made within 60 minutes. This can be edited with the latest firmware version.

Scope allows an Administrator-level account to restrict Users to the visibility of specified Outlet information.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.30 User Page

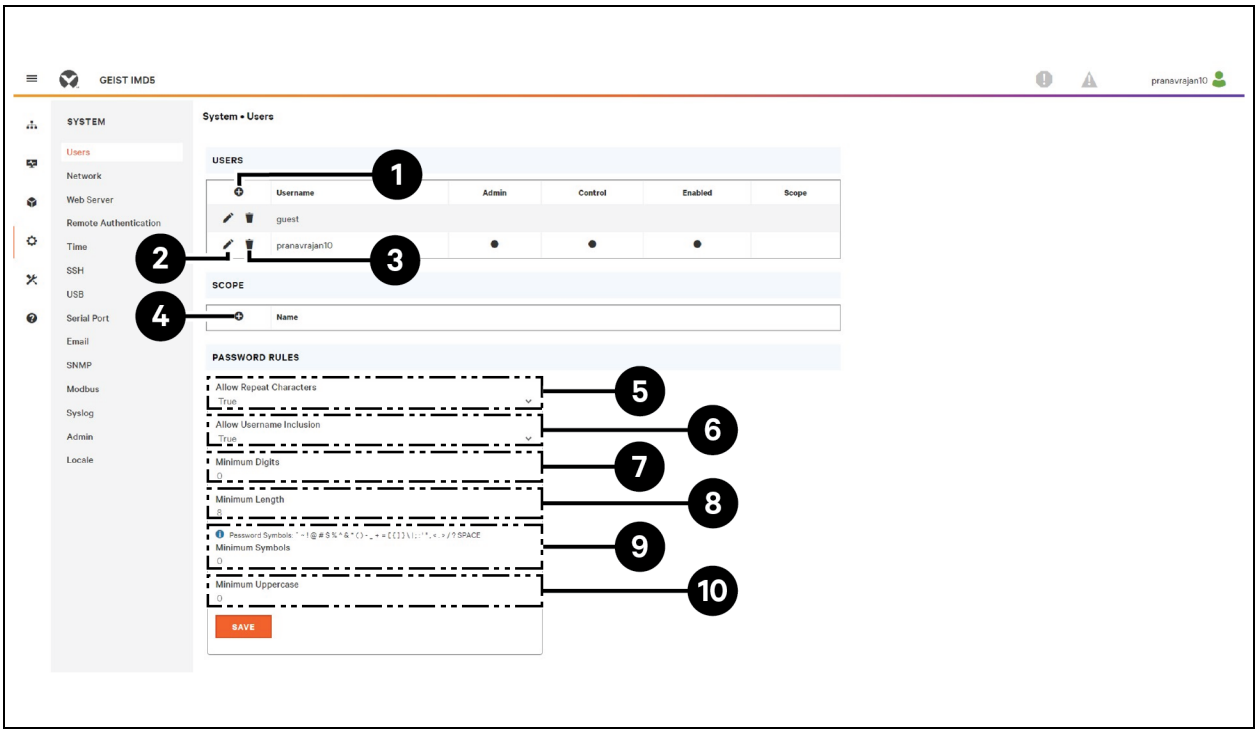


Table 5.11 User Page Descriptions

Number	Descriptions
1	Add new user account
2	Modify user account
3	Delete user account
4	Add user scope : Only visible when logged in as an Administrator*
5	Allow Repeat Characters: restrict the use of more than 2 repeat characters (default false)*
6	Allow Username Inclusion: restrict the inclusion of the user name in the password (default false)*
7	Minimum Digits: enter the minimum numerical digit characters (default 0)*
8	Minimum Length: enter the minimum number of password characters (default 8, minimum 6)*
9	Minimum Symbols: enter the minimum symbol characters (default 0)*
10	Minimum Uppercase: enter the minimum uppercase characters (default 0)*
NOTE: *Only visible when logged in as an Administrator.	

NOTE: Only an Administrator-level account can add, modify or delete users as well as add, modify or delete scopes. Control-level and View-Only accounts can change their own passwords using the Modify User icon, but cannot add, delete or modify other accounts. The Guest account cannot add, delete or modify any account, not even itself.

Proprietary and Confidential ©2024 Vertiv Group Corp.

To add or modify a user account:

1. Click the Add or Modify User icon.
2. Create or modify the account information as needed.
   a. **Username:** The name of the account. User names may be up to 24 characters long, are case-sensitive and may not contain spaces or any of these prohibited characters: $& `:<>[ ] { }"+%@/ ; =?\^|~'.,

NOTE: A username cannot be changed after the account is created.

   b. **Administrator:** If set to *True*, this account has Administrator level access to the unit and can change any setting.
   c. **Control:** If set to *True*, this account has Control-level access. Setting Administrator to *True* will automatically set Control to *True* as well. Setting this to *False* makes the account an Enabled account, which is view-only.
   d. **Scope:** If a user scope has been created, select applicable scope for the account. See step To add or modify a user scope: on the next page .
   e. **New Password:** Account password may be up to 24 characters long, are case-sensitive and may not contain spaces.
   f. **Account Status:** Set the account to *Enabled* or *Disabled*. Disabling an account prevents it from being used to log in, but does not delete it from the account list.
3. Click *SAVE*.

User Account Types

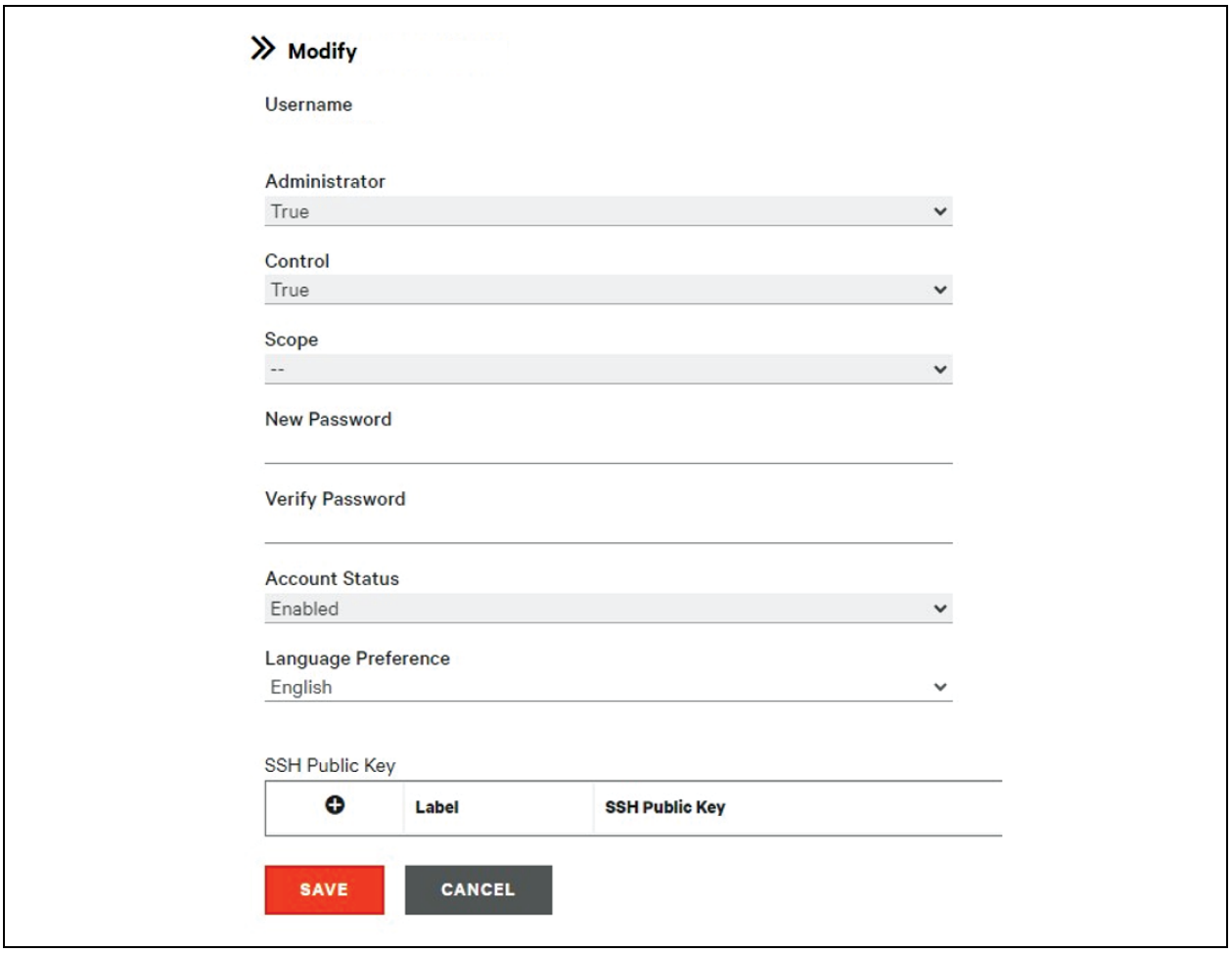
- **Administrator:** Administrator accounts (accounts with both administrator and control authority set to *True*, as above) have full control over all available functions and settings on the device, including the ability to modify system settings and add, modify or delete other users accounts.
- **Control:** Control accounts (accounts with only control set to *True*) have control over all settings pertaining to the device's sensors. They can add, modify or delete alarms and warning events and notification actions and can change the names or labels of the device and its sensors. Control accounts cannot modify system settings or make changes to other users' accounts.
- **View-Only:** If both administrator and control are set to *False*, the account is a View-Only account. The only changes, a View-Only account is permitted to make are changing its own account's password and changing the preferred language for its own account. View-Only accounts cannot change any device or system settings.
- **Guest:** Any user that views the unit's web page without logging in is automatically viewing the unit as Guest. By default, the Guest account is a View-only account and cannot make changes to any settings, allowing anyone to make changes to names, labels, alarm events and notifications without logging in. The Guest account cannot be deleted but can be disabled to require log in for viewing system status.

To change a user password:

1. Log in to your account.
2. Click the Modify User icon.
3. Click on Username in the top right corner of the page.
4. Enter a new password and Verify new password by re-entering In Verify password field.
5. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

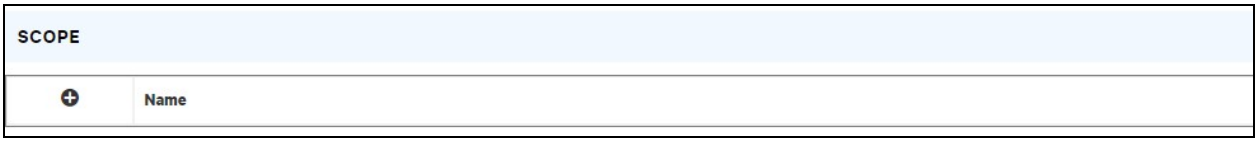
Figure 5.31 Change User Password Page



To add or modify a user scope:

1. Click the Add or Modify Scope icon. Refer Figure 5.32 below .
2. Create or modify the scope information as needed.
   a. Label: Enter the desired name of the selected scope.
   b. Remote Authentication Attribute: Used for all remote authentication types.
   c. Click applicable Outlets for a specified User. (Highlight in Green)
3. Click *OK* to save changes.

Figure 5.32 Add Scope



Password rules and account policy settings

NOTE: A user will be logged out automatically after 10 minutes of inactivity.

Proprietary and Confidential ©2024 Vertiv Group Corp.

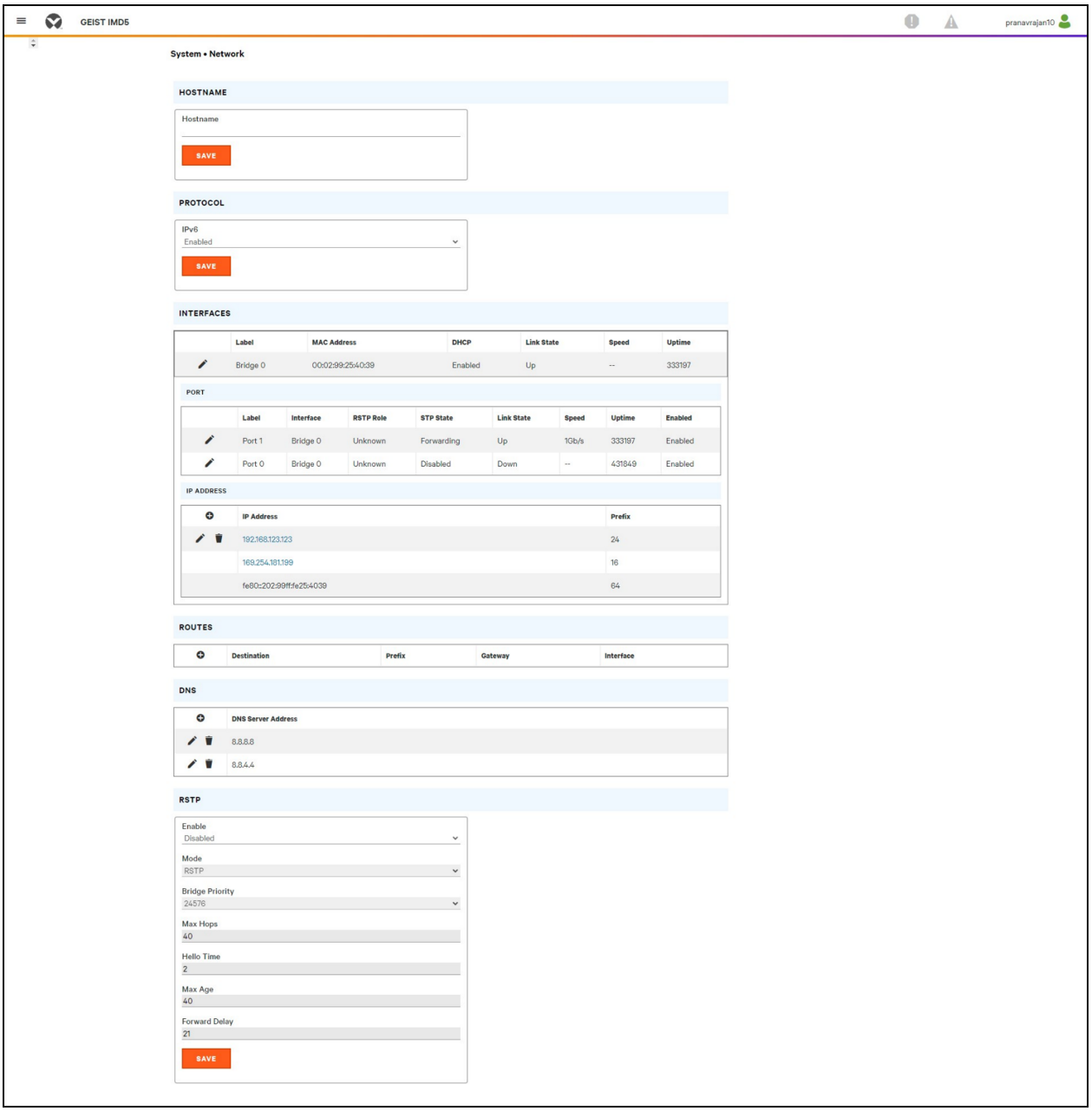
5.6.2 Network

The unit's network configuration is set on the *Network tab* of the System menu. Settings pertaining to the unit's network connection are:

- Hostname: The hostname may be used as a method for device identification on the network.
- Protocol: Click on the IPv6 drop-down menu, select *Enabled* or *Disabled* and click on *Save*.
- Interfaces: Used to configure the IP address of the Vertiv™ Geist™ rPDU, enable/disable DHCP and to view Link State, Speed and Uptime. The device supports up to eight user-configured IP address entries.
- Ports: Used to view and/or modify ETHERNET Port settings and RSTP status, Interface, STP State, Link State Speed , Uptime, Enabled of each port on the Geist™ rPDU.
- IP Address: Used to add or modify the IP Addresses.
- Routes: Displays configured routes and is where you will set your Gateway address for the Geist™ rPDU. Default routes are distinguished by a *destination* of 0.0.0.0 or ::, with a Prefix of 0 and Interface of all. Only one default route can exist for IPv4 and one for IPv6.
- DNS: Allows the unit to resolve hostnames for email, NTP and SNMP servers.
- RSTP: Used for to view and modify the state of RSTP, mode, Bridge priority, Max Hops, Hello time Maximum age (Max) and forward delay.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.33 Network Configuration Page



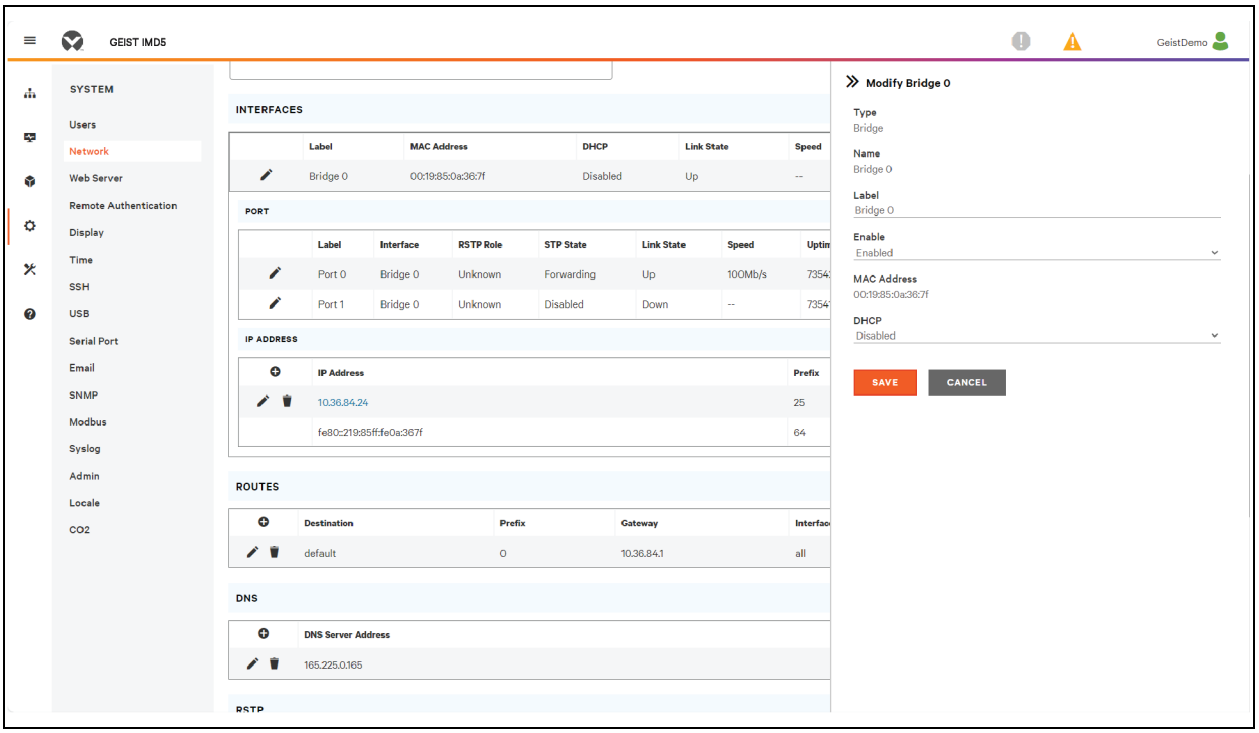
To edit the interface parameters:

1. Click the Modify icon.
2. Modify the desired fields.
   a. **Label:** *Change* the desired name of the selected interface.
   b. **Enable:** *Enable/Disable* the selected interface. If only one interface is available, disabling the interface restricts access to the device requiring a network reset.
   c. **DHCP:** *Enable/Disable* DHCP on the selected interface.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

NOTE: Any changes made to the network interface settings take effect once the *Save* button is clicked. If you have changed the IP address, it will appear as if the unit is no longer responding because the browser will not be able to reload the web page. Close the browser window, type the new IP address into the browser's address bar and the unit will be accessible.

Figure 5.34 Interface Parameters



To add an interface for a wireless USB adapter:

1. Insert the wireless USB adapter into the USB port. (The rPDU will be inaccessible for a few seconds while the network stack reconfigures itself.)
2. After the adapter is auto detected, a Wi-Fi interface will appear.
3. Click the Modify icon. Select the applicable SSID from the Detected SSIDs drop-down menu.

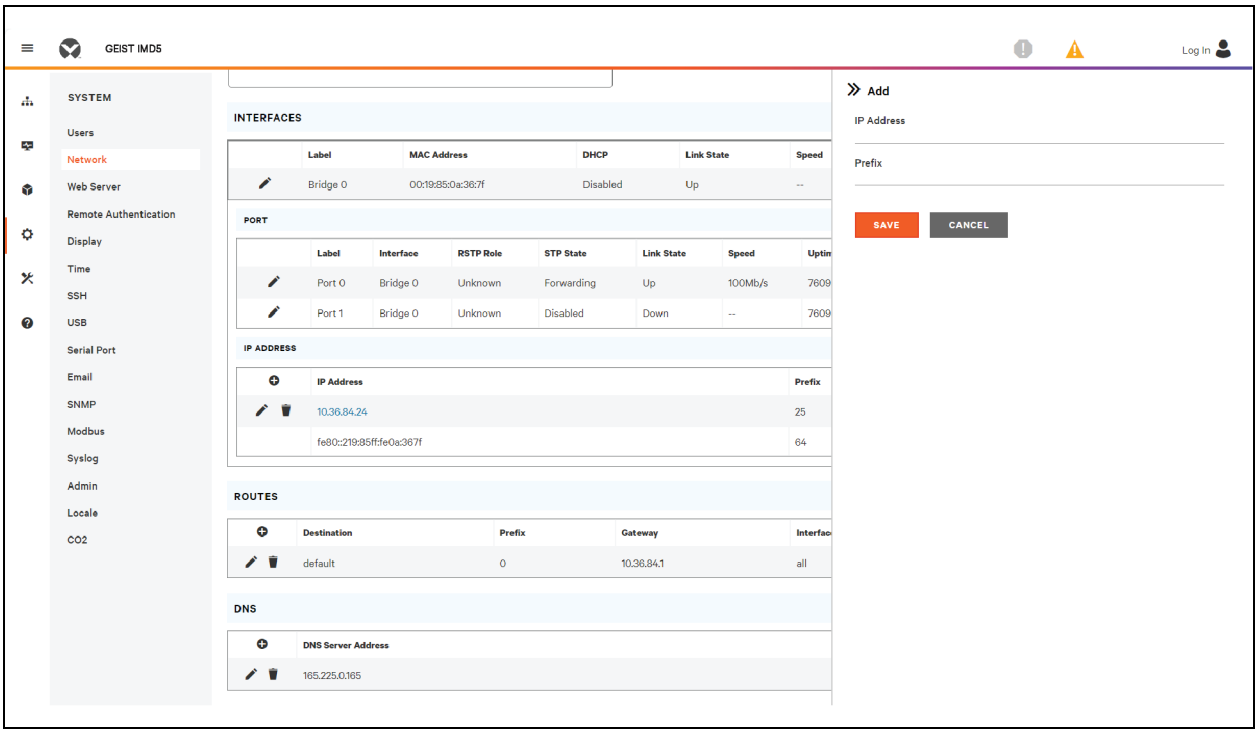
NOTE: See TP-Link Wireless USB adapters on page 116 for listing of TP-Link wireless.

To add a new IP Address:

1. Click the Add icon.
2. Enter the IPv4 or IPv6 address and Prefix/Subnet Mask into appropriate fields. Up to eight IP addresses can be statically assigned.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.35 Add New IP Address

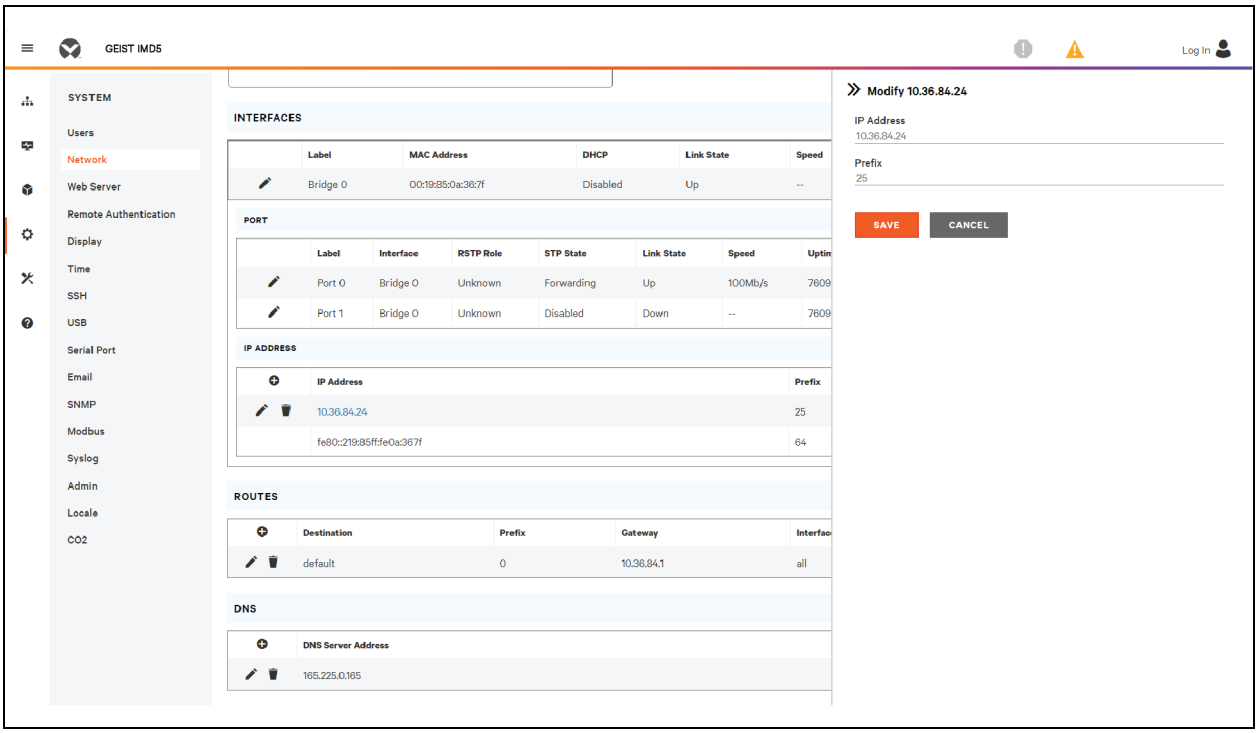


To modify an existing IP address:

1. Click the Modify icon.
2. Edit the IP address and Prefix/Subnet Mask fields as needed.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.36 Modifying IP Address

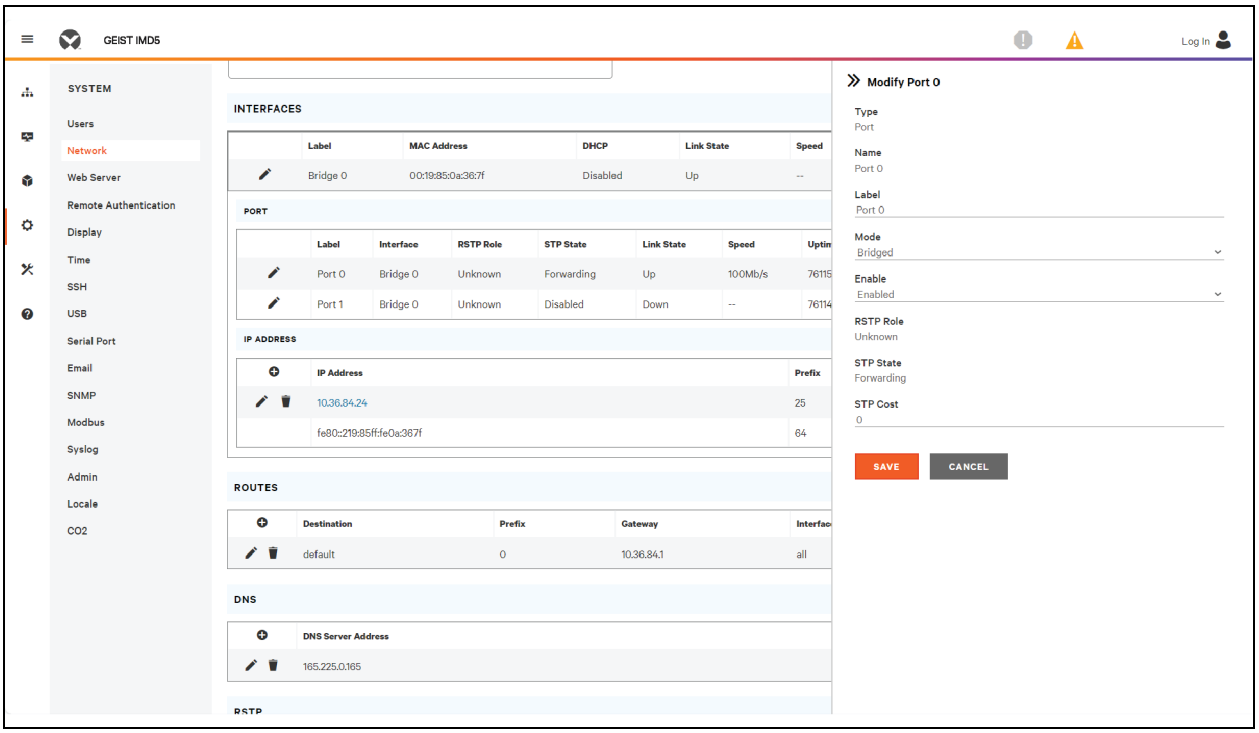


To modify port settings:

1. Click the Modify icon.
2. Enter the appropriate information.
   a. Change port label if desired.
   b. Select either Bridged/Independent Mode.
   c. Enable/Disable port.
   d. Assign STP State. This designates this interface's contribution to the root path cost when it serves as the root port.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.37 Modifying Port Setting

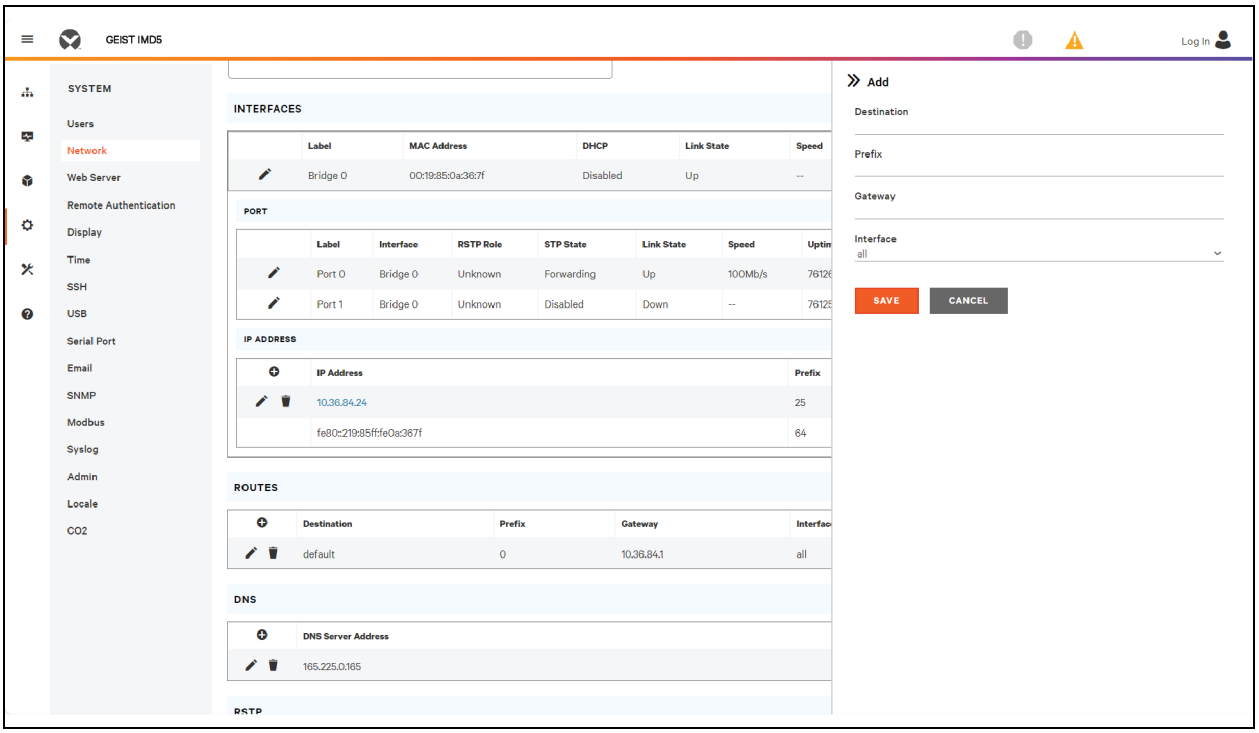


To add a new route:

1. Click the Add icon.
2. Enter the appropriate information.
   a. Destination IP address for desired route.
   b. Enter *Prefix* for the desired route.
   c. Enter the Gateway IP address.
   d. Select the *Interface* that route applies.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.38 Adding Route

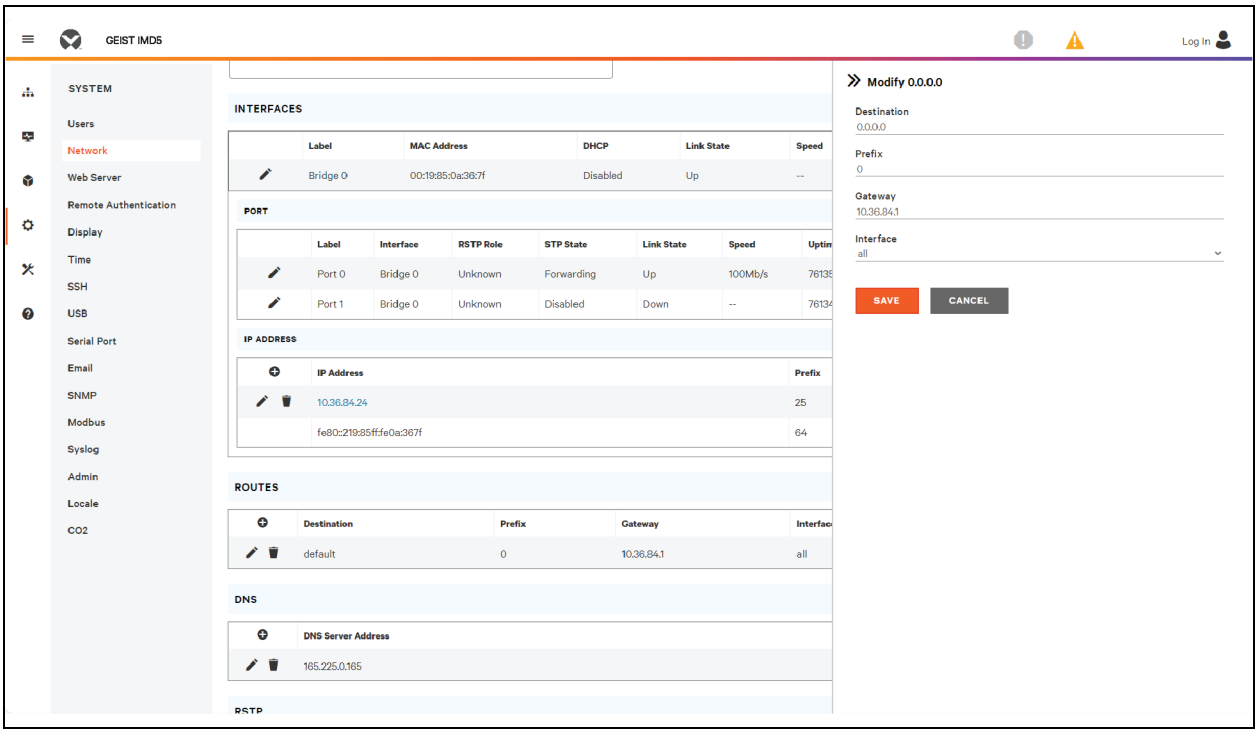


Proprietary and Confidential ©2024 Vertiv Group Corp.

To modify an existing route:

1. Click the Modify icon.
2. Edit the desired fields.
3. Click *SAVE*.

Figure 5.39 Modifying Route

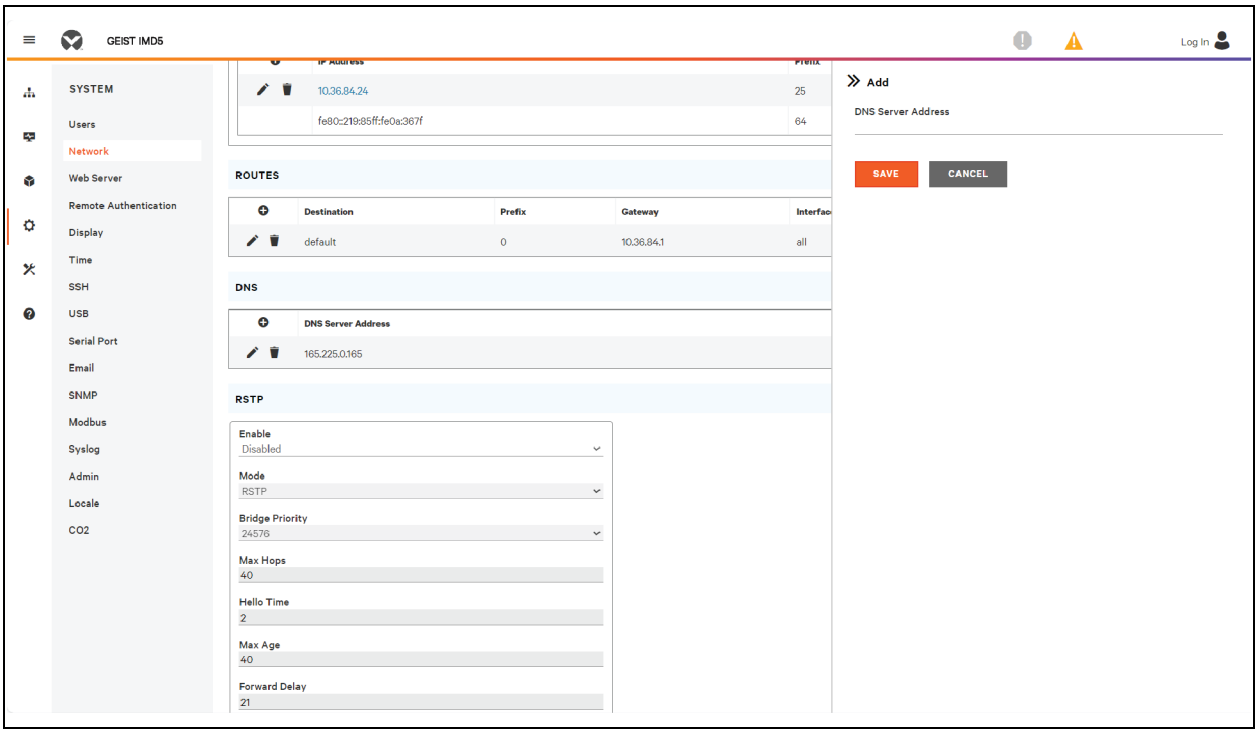


To add a new DNS Server Address:

1. Click the Add icon.
2. Enter the IP of the desired DNS server. Up to two DNS servers can be added.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.40 Adding DNS Server Address

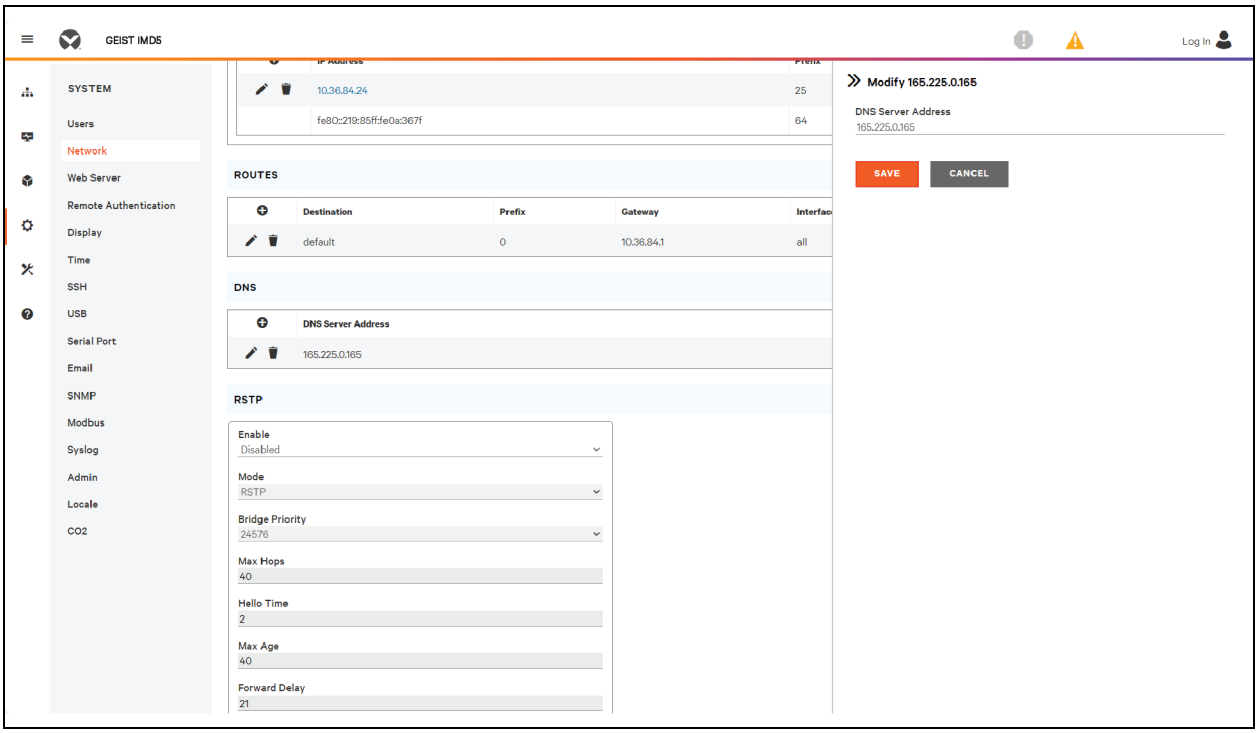


To modify an existing DNS Server address:

1. Click the Modify icon.
2. Edit the DNS Server Address field as required.
3. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.41 Modifying DNS Server Address

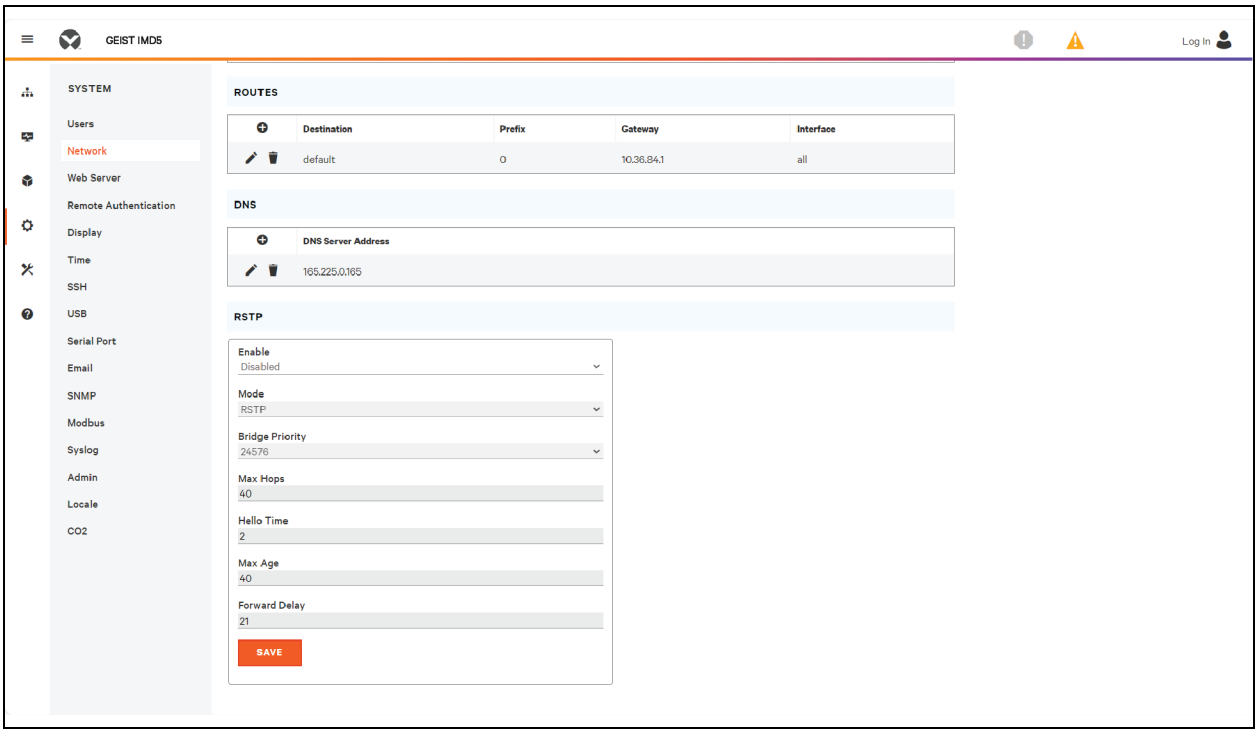


To change RSTP settings:

1. Change the settings, as desired.
   a. **Enable:** Enable or Disable RSTP protocol.
   b. **Mode:** RSTP mode supports falling back to STP when necessary.
   c. **Bridge Priority:** Click the drop-down menu, select the appropriate value and click *Save*.
   d. **Max Hops:** Used when mode enabled to RSTP.
   e. **Hello Time:** The interval, in seconds, between periodic transmissions of configuration messages by designated ports.
   f. **Max Age:** The maximum age, in seconds, of the information transmitted by this interface, when it serves as the root bridge. Set at 2 seconds.
   g. **Forward Delay:** The delay, in seconds, used by bridges to transition the root bridge and designated ports into forwarding mode. Set at 21 seconds.
2. Click *SAVE*.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.42 Changing RSTP Setting



5.6.3 Web server

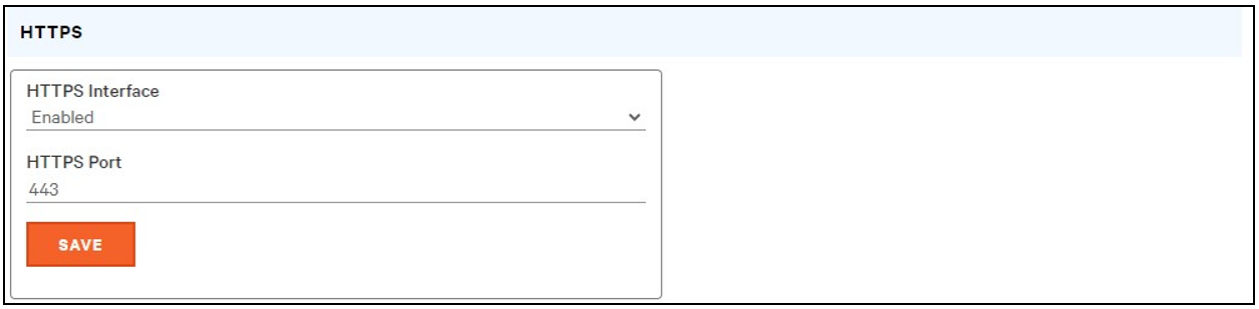
The unit's Web Server configuration can be updated on the Web Server tab of the System menu.

- HTTP Interface: Enabled or redirected to HTTPS, whilst the HTTPS interface can be enabled or disabled. When the HTTP interface is redirected to HTTPS and the HTTPS interface is disabled, the HTTP interface will be effectively disabled too.

NOTE: Note it is not possible to disable HTTP, HTTPS and SSH protocols at the same time.

- HTTP/HTTPS Server Port: Allows you to change the TCP ports that the HTTP and HTTPS services listen to for incoming connections. The defaults are Port 80 for HTTP and Port 443 for HTTPS.

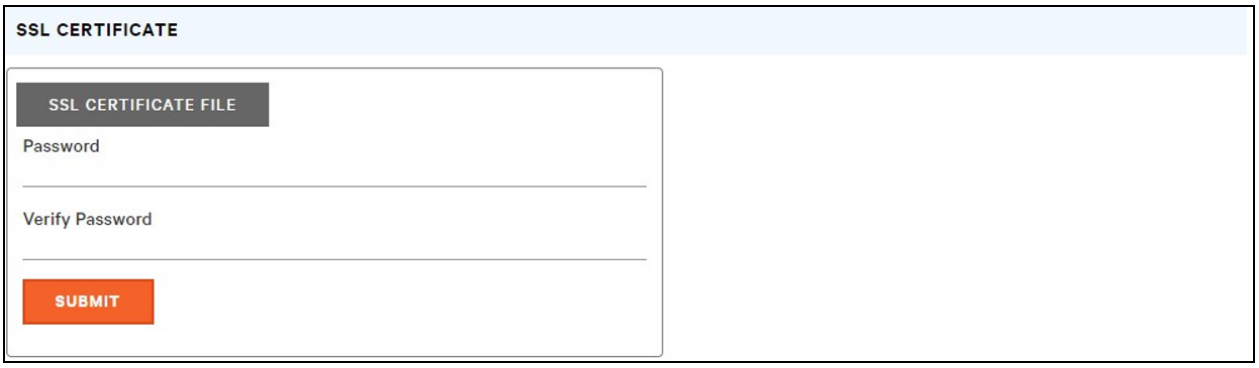
Figure 5.43 HTTP Configuration Page



- SSL Certificate: Allows you to upload your own signed SSL Certificate file to replace the default one. The certificate can be either self-signed or signed from a Certification Authority. SSL Certificate must be in either *PEM* or *PFX* (PKCS12) format.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.44 SSL Certificate



- *PEM* Format:
  - The public certificate and private key must reside in the same file.
  - The certificate must follow standard x.509.
  - The private key must be generated with either the RSA algorithm or the ECDSA algorithm. It must be in *PEM* format.
    - 2048-bit RSA or smaller is not supported.
    - P-384 is the supported key size for ECDSA.
  - The *PEM RSA* private key may be password-secured.
- *PFX* Format: Support is also available for the PKCS12 standard (*.pfx*), which is a binary encrypted combination of a *PEM* public certificate and its *PEM* private key. When generating a *PFX* certificate you are prompted for an optional password.

5.6.4 Remote authentication

The Remote Authentication page allows you to designate one of three authentication protocols for remote access to the device. By default, the device uses the local database to authenticate users. Remote authentication allows the device to authenticate a user with a remote server. If remote authentication fails, then it will revert to local authentication.

To change Remote Authentication settings:

1. Select the required mode from the drop-down menu.
   - Disabled: Local Authentication.
   - LDAP: Lightweight Directory Access Protocol.
   - TACACS+: Terminal Access Controller Access Control System Plus.
   - RADIUS: Remote Authentication Dial-In User Service.
2. Click *SAVE*.

LDAP

The Lightweight Directory Access Protocol (LDAP) can be set up through this menu.

NOTE: Knowledge of your LDAP server settings is required to set up the Vertiv™ Geist™ rPDU device for this remote authentication protocol. If you are not familiar with these settings, consult your LDAP server administrator.

Configuration for remote authentication using LDAP.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

- **LDAP Server Address:** Specify the host address for LDAP. The *HOST* can be an IPv4 address, an IPv6 address in brackets (Such as *[2001:0DB8:AC10:FE01::]*) or a hostname.
- **LDAP Server Port:** Used to set the LDAP port number. The default port for LDAP is *389* - use for Security Type *None* or *StartTLS*. Use *636* for Security Type *SSL*.
- **LDAP Mode:** From the drop-down menu, select *Active Directory* or **OpenLDAP**. See An Example of Configuring LDAP for Active Directory Credentials on page 145 .
- **Security Type:** From the drop-down menu, select *None*, *SSL* or *StartTLS*.
- **Bind DN:** Distinguished Name used to bind to the directory server. Blank string for Bind DN and Password implies anonymous bind.
- **Bind Password:** Password used to bind to the directory server.
- **Base DN:** DN to use for the search base.

The remaining fields come from the NIS schema, defined in RFC2307. They are used to authenticate users in LDAP. Leaving them blank will use the default value.

- **User Filter:** LDAP filter for selecting users.
- **"uid" Mapping:** Name of the server attribute that corresponds to the *uid* attribute in the schema.
- **"uidNumber"Mapping:** Name of the server attribute that corresponds to the *uidNumber* attribute in the schema.
- **Group Filter:** LDAP filter for selecting groups.
- **"gid" Mapping:** Name of the server attribute that corresponds to the *gid* attribute in the schema.
- **"memberUid" Mapping:** Name of the server attribute that corresponds to the *memberUid* attribute in the schema.

NOTE: Users *must* populate uidNumber. A null or missing value will cause a valid login to fail. The user's uidNumber *must* be 1000 or greater. A value lower than 1000 will cause a valid login to fail.

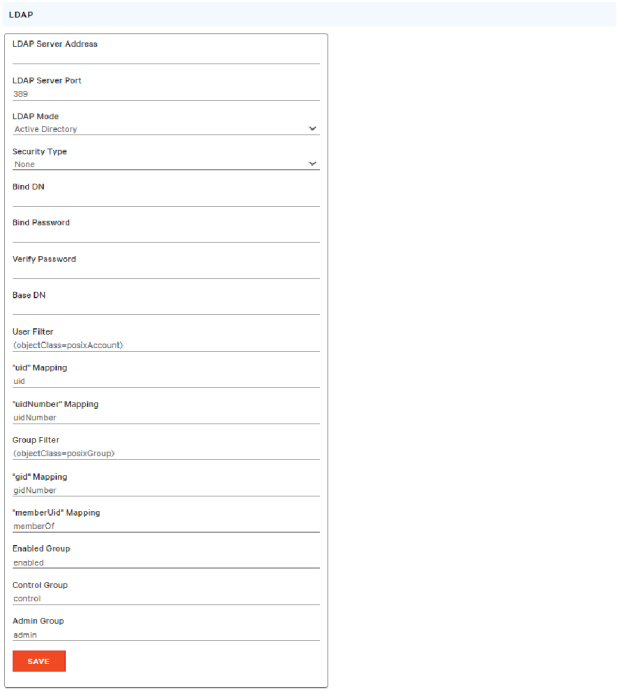
- **Enabled Group:** Users in this group have view-only privileges as described in the Users section of this manual.
- **Control Group:** Users in this group have control privileges as described in the Users section of this manual.
- **Admin Group:** Users in this group have admin privileges as described in the Users section of this manual. LDAP users do not count toward the minimum number of required admin users.

Click *SAVE*.

The Enabled Group, Control Group and Admin Group fields tell how to map groups to user permissions. A user must belong to one of these groups to access the device. If a user belongs to more than one group, then the group with the highest permission is used.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.45 LDAP Menu



TACACS+

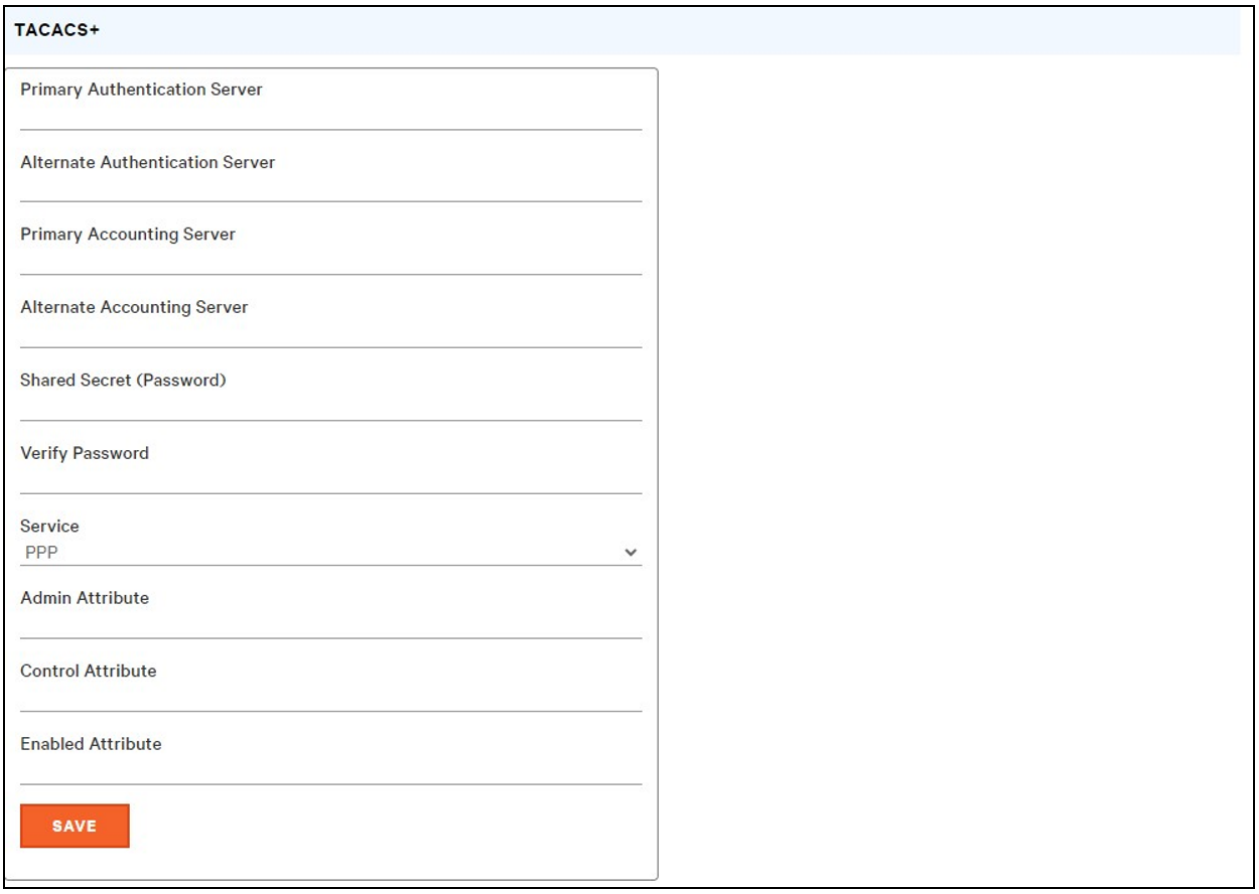
The Terminal Access Controller Access-Control Plus Protocol (TACACS+) can be set up through this menu.

NOTE: Knowledge of your TACACS+ server settings is required to set up the Vertiv™ Geist™ rPDU device for this remote authentication protocol. If you are not familiar with these settings, consult TACACS+ server administrator.

Configuration for remote authentication using TACACS+.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.46 TACACS+ Menu



- Primary Authentication Server: The primary authentication/authorization server, which can be an IPv4 address, an IPv6 address in square brackets (Such as *[2001:0DB8:AC10:FE01::]*) or a host name. The Primary Authentication Server is used for both authentication and authorization. This AA server address/host name is required.
- Alternate Authentication Server: The alternate authentication/authorization server, which can be an IPv4 address, an IPv6 address in square brackets or a host name. The Secondary Authentication Server is used for both authentication and authorization.
- Primary Accounting Server: The primary accounting server, which can be an IPv4 address, an IPv6 address in square brackets or a host name. The Primary Accounting Server is optional. If configured, the server is notified when a user is authorized.
- Alternate Accounting Server: The alternate accounting server, which can be an IPv4 address, an IPv6 address in square brackets or a host name. The Secondary Accounting Server is optional. If configured, the server is notified when a user is authorized.
- Shared Secret (Password): Enter a secret word or passphrase in the Shared Secret field (applies to both primary and secondary authentication and accounting servers).
- Service: The value to use for the service field in TACACS+ requests. Valid options are *PPP* and *raccess*.
- Admin Attribute: A user with this attribute will have *admin* privileges as described in the Users section of this manual. TACACS+ users do not count toward minimum number of required admin users.
- Control Attribute: Users with this attribute will have control privileges as described in the Users section of this manual.

Proprietary and Confidential ©2024 Vertiv Group Corp.

- Enabled Attribute: Users with this attribute will have view-only privileges as described in the Users section of this manual.

Click *SAVE*.

NOTE: The Attribute-Value Pairs (AVPs) returned by the server during authentication/authorization determine the user permissions. The Group Attribute field tells the system which AVP contains the user's access group. If the AVP value matches the Admin Group field, then the user has Admin (full) access. If the AVP value matches the Control Group field, the user has control access. If the AVP matches the Enabled Group field, the user has view-only access. If no matches are found, then the user will not have access to the unit. A blank Group field will not match any AVP.

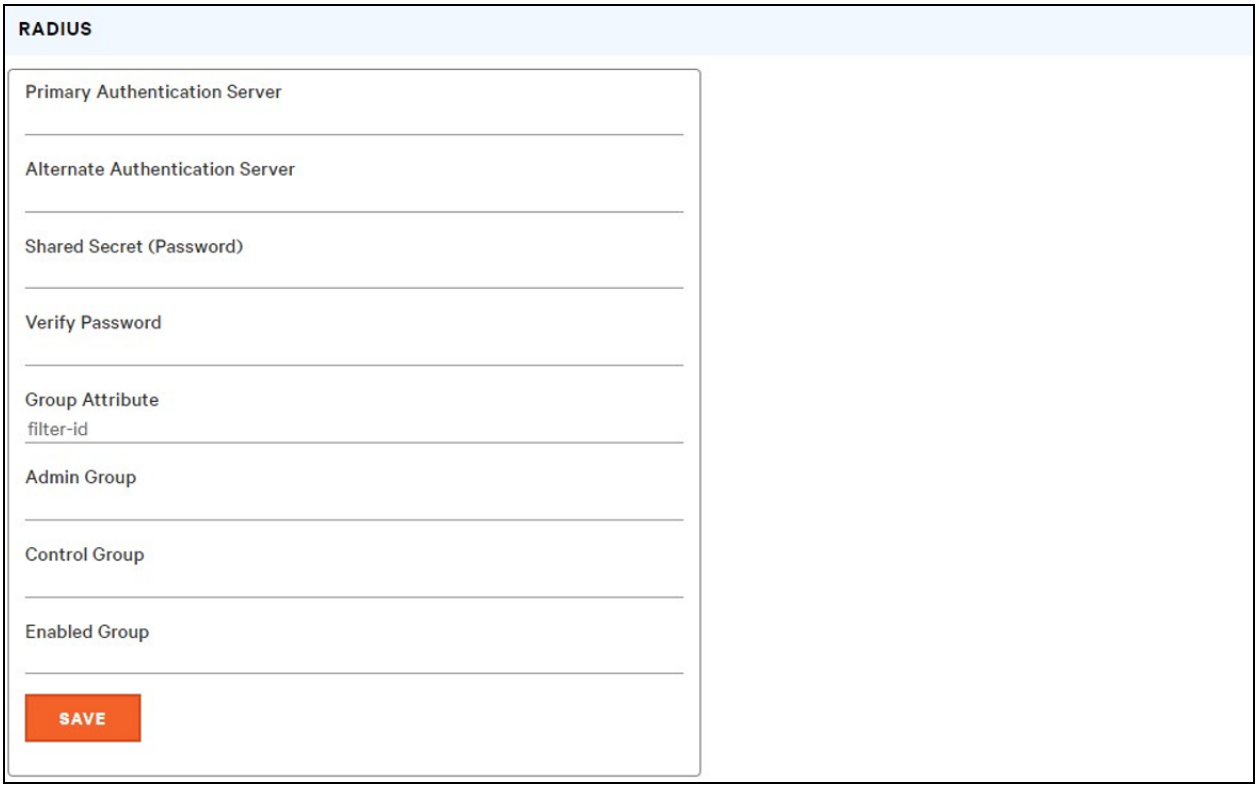
RADIUS

The Remote Authentication Dial-In User Service Protocol (RADIUS) can be set up through this menu.

NOTE: Knowledge of RADIUS server settings is required to set up the Vertiv™ Geist™ rPDU device for this remote authentication protocol. If you are not familiar with these settings, consult your RADIUS server administrator.

Configuration for remote authentication using RADIUS.

Figure 5.47 RADIUS Menu



- Primary Authentication Server: Enter the IP address of the primary authentication/authorization/accounting server. The Primary Authentication Server can be an IPv4 address, an IPv6 address in square brackets (Such as *[2001:0DB8:AC10:FE01::]*) or a host name. The Primary Authentication Server is used for authentication, authorization and accounting. This AA server is required.

- **Alternate Authentication Server:** If applicable, enter the IP address of the alternate authentication/authorization/accounting server. The Alternate Authentication Server can be an IPv4 address, an IPv6 address in square brackets or a host name. The Secondary Authentication Server is used for authentication, authorization and accounting.
- **Shared Secret (Password):** Enter a secret word or passphrase in the Shared Secret field (applies to both primary and secondary authentication and accounting servers).
- **Group Attribute:** Identifies the Attribute-Value Pair (AVP) that tells which access group the user belongs to. Valid values are *filter-id* and *management-privilege-level*.
- **Admin Group:** A user belonging to this group has Admin privileges as described in the Users section of the manual.
- **Control Group:** A user belonging to this group has Control privileges as described in the Users section of the manual.
- **Enabled Group:** A user belonging to this group has **Enabled** view-only privileges as described in the Users section of the manual.

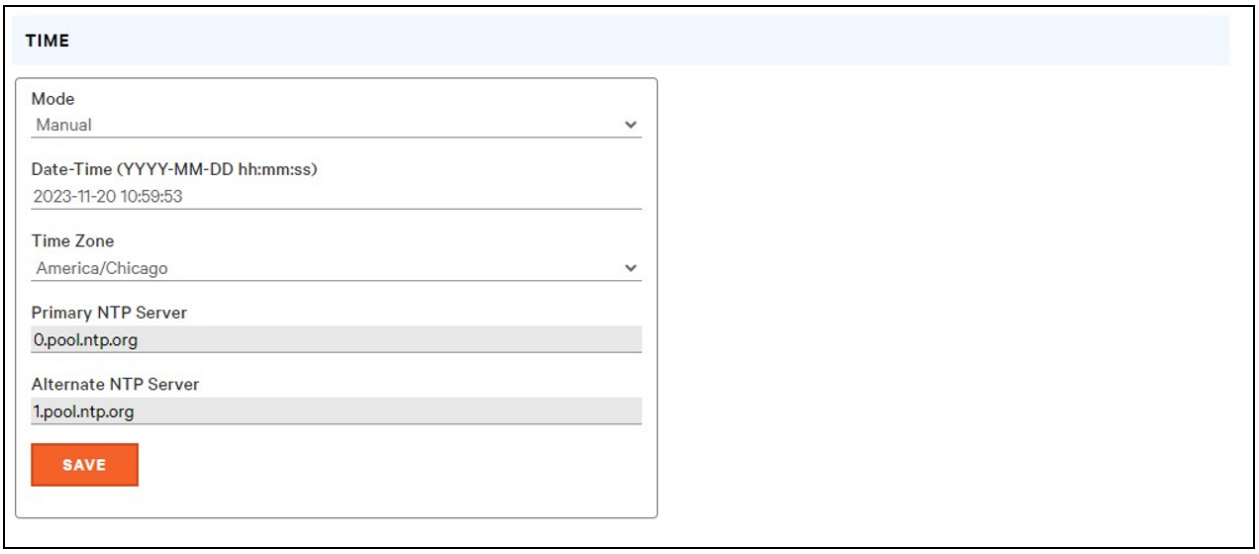
Click *SAVE*.

NOTE: The Attribute-Value Pairs (AVPs) returned by the server during authentication / authorization determine the user permissions. The Group Attribute field tells the system which AVP contains the user's access group. If the AVP value matches the Admin Group field, then the user has Admin (full) Access. If the AVP value matches the Control Group field, the user has Control Access. If the AVP matches the Enabled Group field, the user has view-only access. If no matches are found, then the user will not have access to the unit. A blank Group field will not match any AVP.

5.6.5 Time

The unit's time and date are set on this page.

Figure 5.48 Time Configuration Page



Two modes are available:

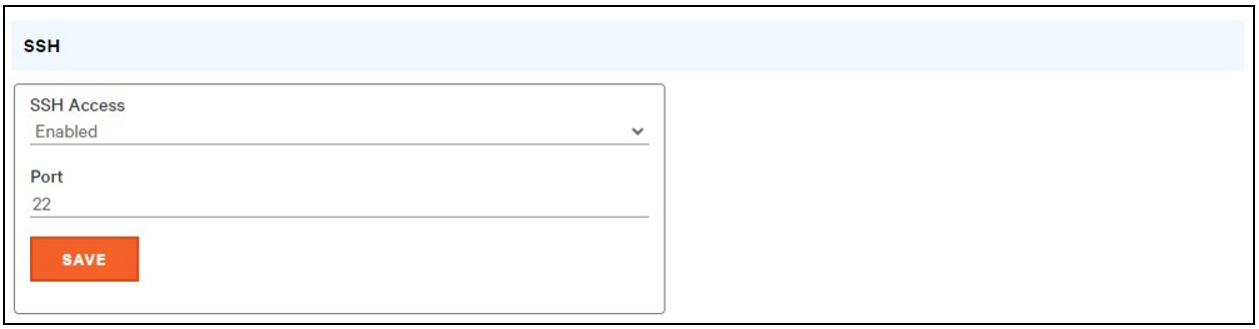
- **Network Time Protocol (NTP):** Synchronizes the unit's time and date to the specified time zone using listed NTP Servers. NTP servers can be reconfigured.
- **Manual:** In this mode, the date and time must be typed as indicated on the left of the field.

Proprietary and Confidential ©2024 Vertiv Group Corp.

5.6.6 SSH

The SSH menu allows you to configure settings for SSH access to the device.

Figure 5.49 SSH Configuration Page



- SSH Access: Enables or disables access via SSH.
- SSH Port: Allows you to change the port that the SSH service listens to for incoming connections. The default is Port 22.

NOTE: An SSH user will be logged out automatically after 10 minutes of inactivity.

5.6.7 USB

To enable or disable the USB port:

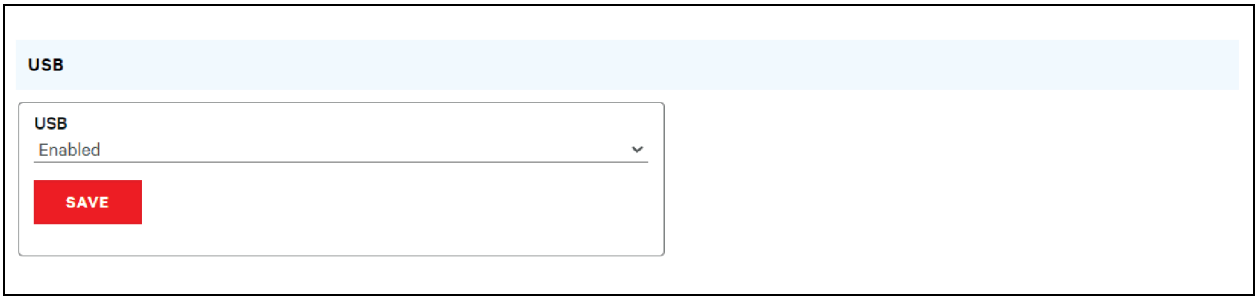
1. Select Enable or Disable from drop-down menu.
2. Click *SAVE* button.

When USB port is enabled, the attached USB devices are displayed on the web interface.

NOTE: The USB device must be formatted as FAT32.

If a valid USB storage device is detected and historic data is being logged, this data is also stored in a file on the USB storage drive. If it does not already exist, a file called log-1.csv is created under a log directory at the top level of the file system. If log files already exist, the one with the highest number identifier in the title is used as a starting point. Every log period, new data is appended to this file in the same format as the CSV retrieval. If data points are created or removed relative to the ones listed in the CSV header, a new file is created named with the next sequential number. If the file system becomes full, this logging will cease.

Figure 5.50 USB



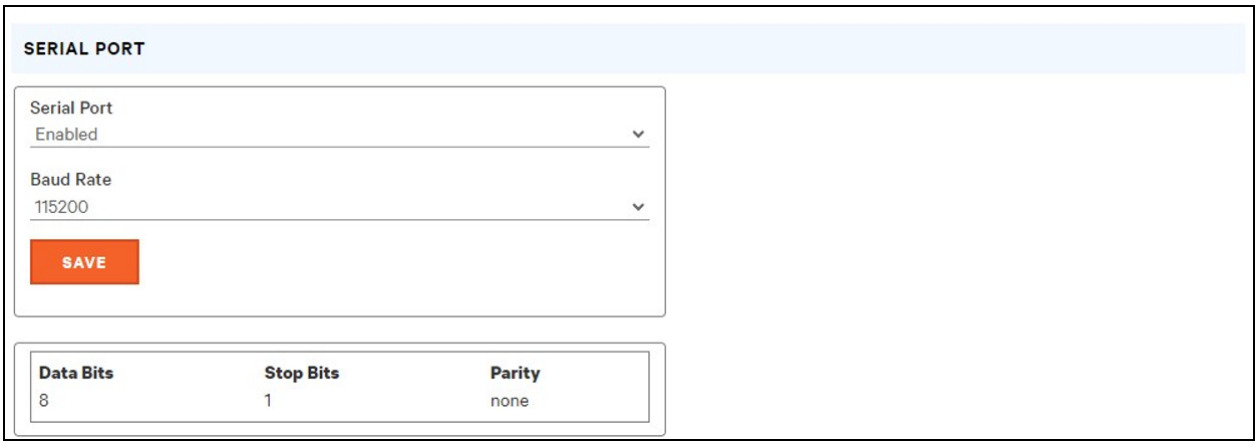
5.6.8 Serial port

NOTE: Serial connection does not support flow control.

The Serial Port menu allows configuring settings for the serial port, enabling or disabling the port and setting the baud rate.

1. Click on the Serial Port drop-down menu, select *Enabled/Disabled*.
2. Click on Baud Rate drop-down menu, select *Baud Rate* value.
3. Click on *SAVE*.

Figure 5.51 System drop-down, Menu – Serial Port



5.6.9 Email

The unit is capable of sending email notifications to up to ten (10) email addresses when an alarm or warning event occurs.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.52 Email Configuration Page

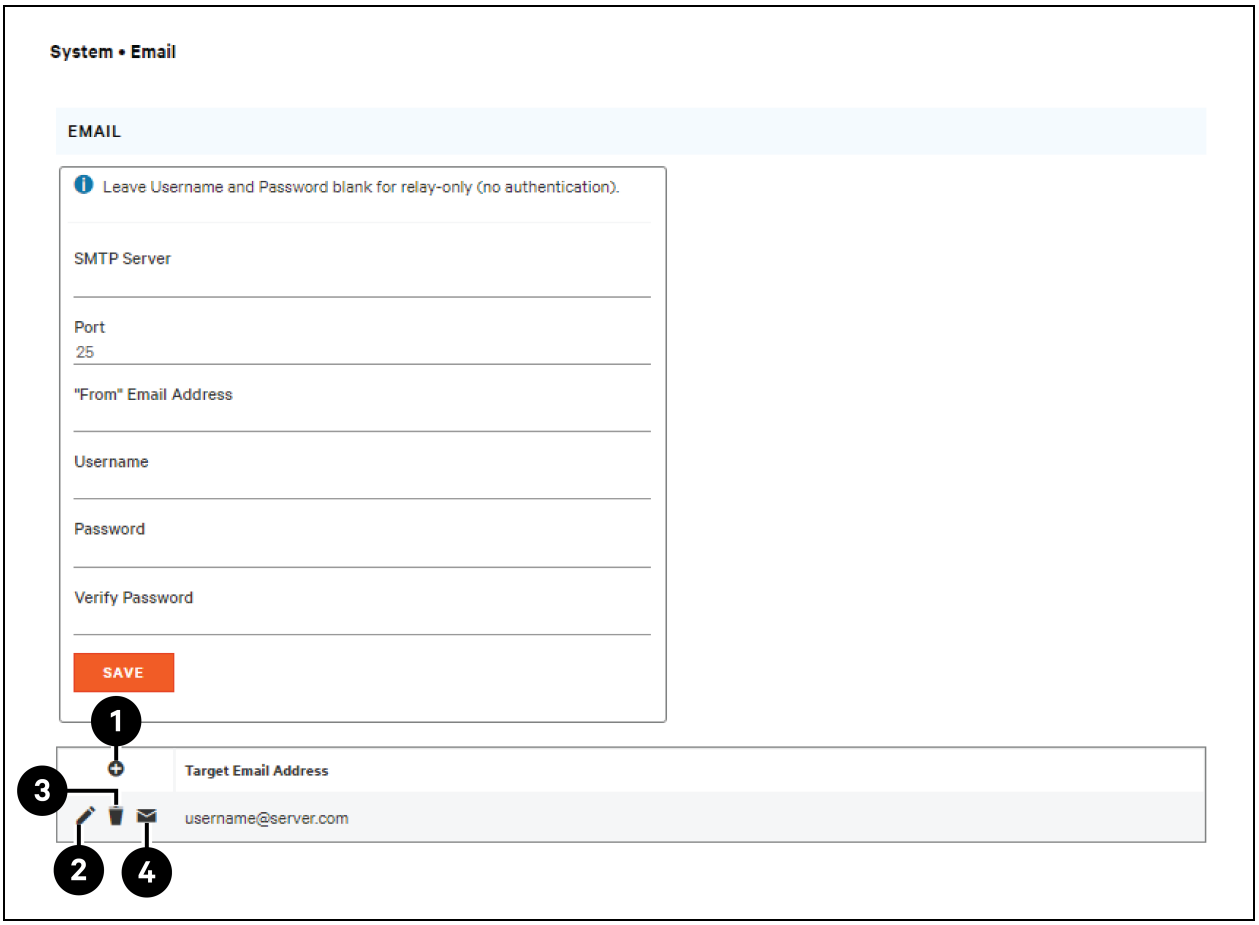


Table 5.12 Email Configuration Page Descriptions

Item	Description
1	Add new target email address.
2	Modify existing target email address.
3	Delete existing target email address.
4	Send test email.

Proprietary and Confidential ©2024 Vertiv Group Corp.

To send emails, the unit must be configured to access the mail server, as follows:

- SMTP Server: The name or IP address of a suitable SMTP or ESMTP server.
- Port: The TCP port that the SMTP Server uses to provide mail services. Typical values would be Port 25 for an unencrypted connection or 465 and 587 for a TLS/SSL-encrypted connection, but these may vary depending on the mail server's configuration.
- From Email Address: The address that the unit's emails appear to come from. Many hosted email services, such as Gmail, require this to be the email account of a valid user.
- Username and Password: The login credentials for the email server. If your server does not require authentication (open relay), these can be left blank.

Microsoft Exchange servers must be set to allow SMTP relay from the IP address of the unit. In addition, the Exchange server must be set to allow Basic Authentication, so the unit is able to log in with the AUTH LOGIN method of sending its login credentials. Other methods, such as AUTH PLAIN and AUTH MD5 are not supported.

To add or modify a target email address:

1. Click the Add or Modify icon.
2. Enter the email address and then click *Save*.

To delete a target email address:

1. Click the Delete icon next to the address you wish to delete.
2. Click *Delete* on the pop-up window to confirm.

To send a test email:

1. Click the Test email icon next to the address you wish to test.
2. A pop-up window indicates the test email is being sent, click *OK* to dismiss the pop-up.

5.6.10 SNMP

Simple Network Management Protocol (SNMP) can be used to monitor the unit's measurements and status. SNMP V1, V2c and V3 are supported. In addition, alarm traps can be sent to up to ten IP addresses.

Click on *ZIP* to download the *mib.zip* file containing both the MIB file and the CSV-formatted spreadsheet.

The SNMP-V1/V2c and SNMP-V3 Service can be enabled or disabled independently. The service listens for data-read requests on Port 161, which is the usual default for SNMP services; this can also be changed.

The Management Information Base (MIB) can be downloaded from the unit, via the ZIP link at the top of the web page. Clicking this link, downloads a .Zip archive containing both the MIB file and a CSV format spreadsheet describing the available OIDs in a human-readable form to assist you in setting up your SNMP manager to read data from the unit.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.53 SNMP Configuration Page

Figure 5.54 SNMP Users Configuration Page

	Type	Name	Authentication	Privacy
	V1/V2c Read Community	public	—	—
	V1/V2c Write Community	private	—	—
	V1/V2c Trap Community	private	—	—
	V3 Read		None	None
	V3 Read/Write		None	None
	V3 Trap		None	None

The Users section allows you to configure the various Read, Write and Trap communities for SNMP services. You can also configure the authentication types and encryption methods used for the SNMP V3 if desired. Click the Modify icon to change settings.

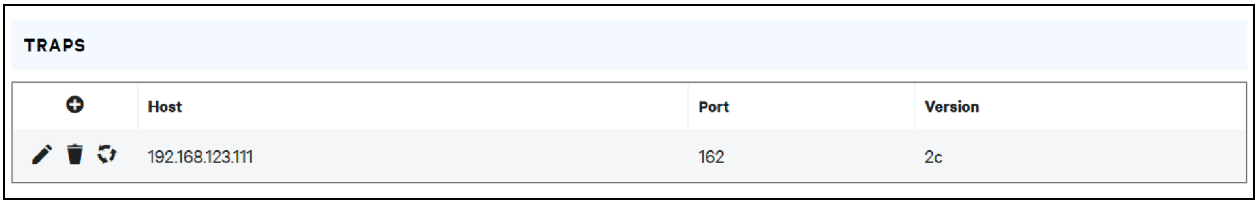
Traps allow defining the SNMP types that you wish to be sent and the IP addresses of recipients.

To configure a Trap Destination:

1. Locate the *Traps* section of the SNMP page and click the Add icon.
2. Enter the IP Address where the trap should be sent in the Host field.
3. Change the port number if required.
4. Select the trap version to be used (V1, V2c or V3) and click *SAVE*.

A test trap may be sent by clicking on the Test icon next to the Host IP address. You can also update/change the Trap settings. Click the Modify icon next to the Host IP address.

Figure 5.55 Trap



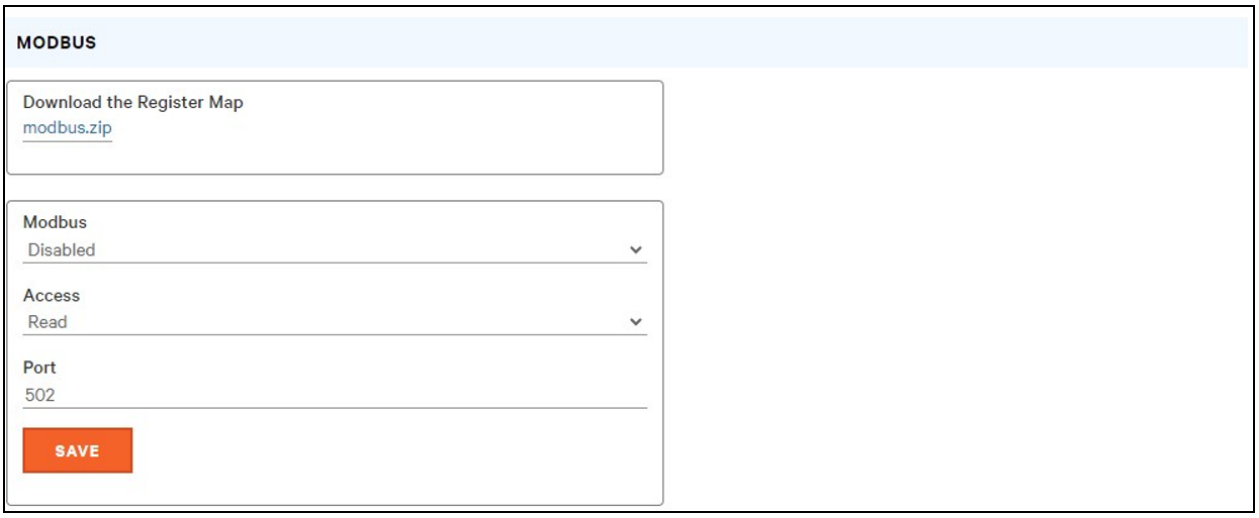
5.6.11 Modbus

Modbus TCP communication protocol can be used to monitor the unit's measurements and status. It also allows the user to adjust the unit's settings.

The register map can be downloaded from the unit, via the ZIP link at the top of the web page. Clicking this link, downloads a .zip archive containing a CSV format spreadsheet describing the Modbus mapping in a human-readable form to assist you in setting up your Modbus manager to read/write data to the unit.

The Modbus communication protocol can be enabled or disabled. Modbus access to the unit can be either *Read* or *Read/Write*. Data-read or data-write requests are made on Port 502, which is the usual default for Modbus protocol; this port can also be changed.

Figure 5.56 Modbus

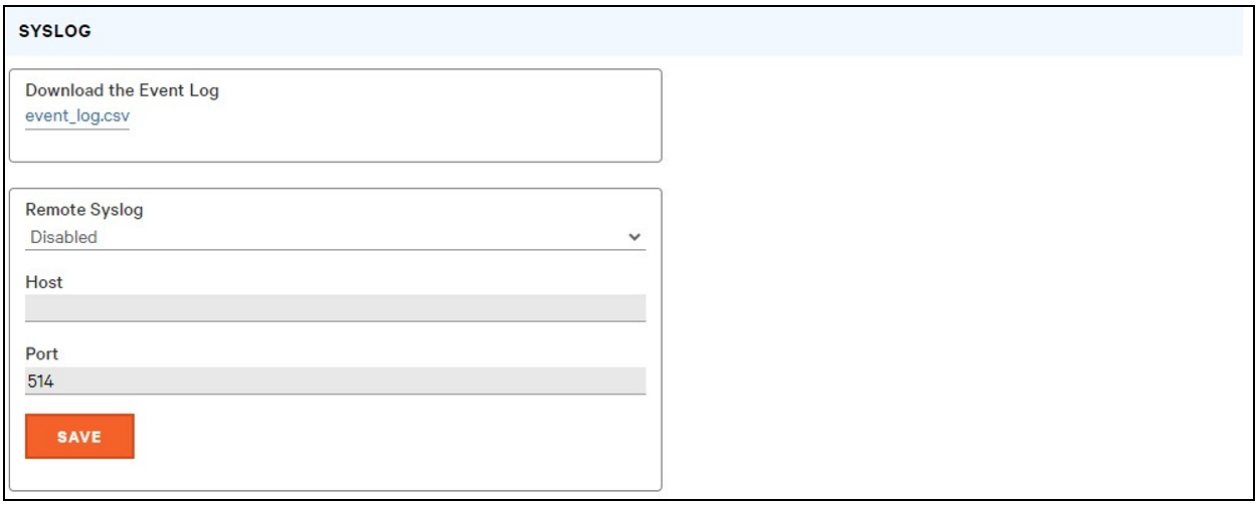


Proprietary and Confidential ©2024 Vertiv Group Corp.

5.6.12 SYSLOG

Syslog data can be captured remotely but must first be set up and enabled via the SYSLOG page.

Figure 5.57 SYSLOG



NOTE: This function is primarily useful for diagnostic purposes and should normally be left disabled unless advised to enable it by Vertiv™ technical support for troubleshooting a specific issue.

The use of the Download the Event Log CSV button requires the user to have admin access.

5.6.13 Admin

The Admin page allows the administrator of the device to save their contact information along with the device description and location. Once the information is saved by an administrator, other (non-administrator) users can view it. Also, the System Label can be modified on this page. This label is typically shown in the title bar of the web browser's window and/or on the browser tabs currently viewing the device.

5.6.14 Locale

The Locale page sets the default language and temperature units for the device. These settings will become the default viewing options for the device, although individual users can change these options for their own accounts. The guest account will only be able to view the device with the options set here.

5.7 Utilities Sub Menu

The Utilities sub menu in the System menu provides the ability to restore defaults, reboot the communication system and perform firmware updates.

5.7.1 Configuration Backup and Restore

Save current configuration settings and restore previous configuration settings as needed.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Table 5.13 Backup and Restore Options

Option	Description
Download Configuration Backup File	Downloads do not require user authentication. The name of the downloaded file is **backup_XXX.bin** where XXX represents a string representation of the MAC address for the **ETHERNET** interface of the unit without the **:** characters.
Backup File	Uploads the configuration backup file. This requires user authentication and the user must have administrator privileges. A backup file can only be used to load configuration on units with the same model number.

To save current configuration settings:

1. Select *Download Configuration Backup File*.
2. Click *BIN*.

NOTE: Saving configuration does not require user authentication.

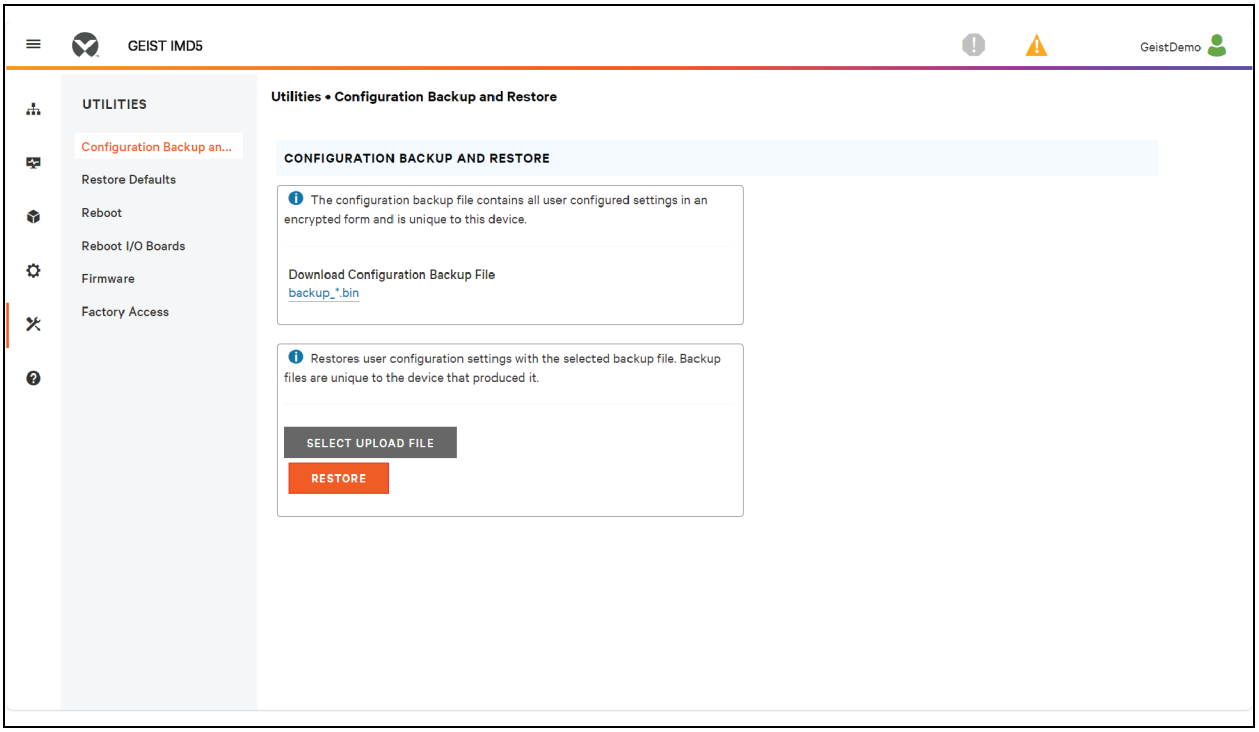
To restore a previous configuration setting:

1. Click *Backup File*.
2. Click *SELECT UPLOAD FILE*.
3. Select the Backup File.
4. Click *RESTORE*.

NOTE: Restoring configurations requires user authentication and the user must have administrator privileges.

NOTE: A backup file can only be used to load configuration on units with the same model number.

Figure 5.58 Configuration Backup and Restore Overview



Proprietary and Confidential ©2024 Vertiv Group Corp.

5.7.2 Restore defaults

Restore the default settings.

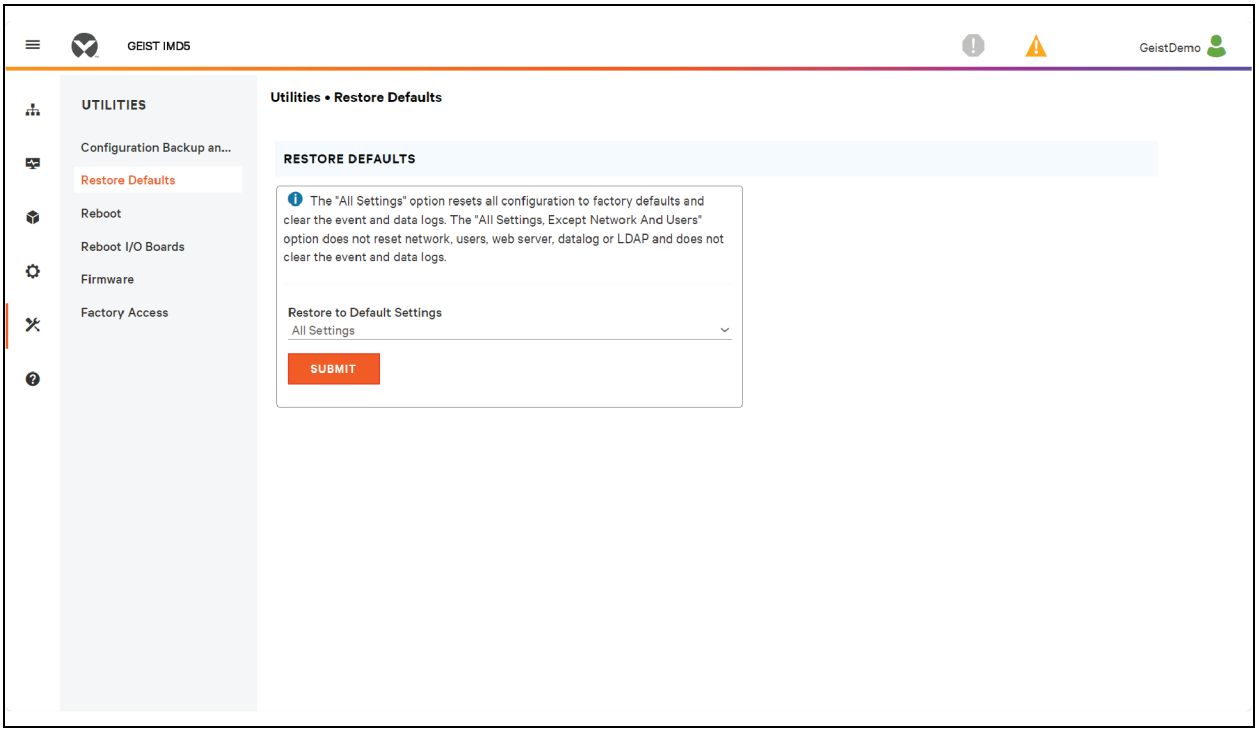
Table 5.14 Restore Default Options

Option	Description
All Settings	Resets all configuration on /conf, /alarm, and /dev to factory defaults. Will also clear the event log, data log, and execute the delete command on any devices with a state of **unavailable**. This will cause portions of the system to reinitialize. It will return success and then be followed by a short period where access to the system will be unavailable.
All Settings, Except Networks And Users	As the **defaults** option above but does not reset /conf/network, /conf/http, /conf/datalog, /auth, or /conf/ldap and does not clear the event log or data log. This will cause portions of the system to reinitialize. It will return success and then be followed by a short period where access to the system will be unavailable.

To restore default settings:

1. Select from either *All Settings* or *All Settings, Except Networks And Users* from the drop-down menu.
2. Click *SUBMIT*.

Figure 5.59 Restore Defaults Overview



5.7.3 Reboot

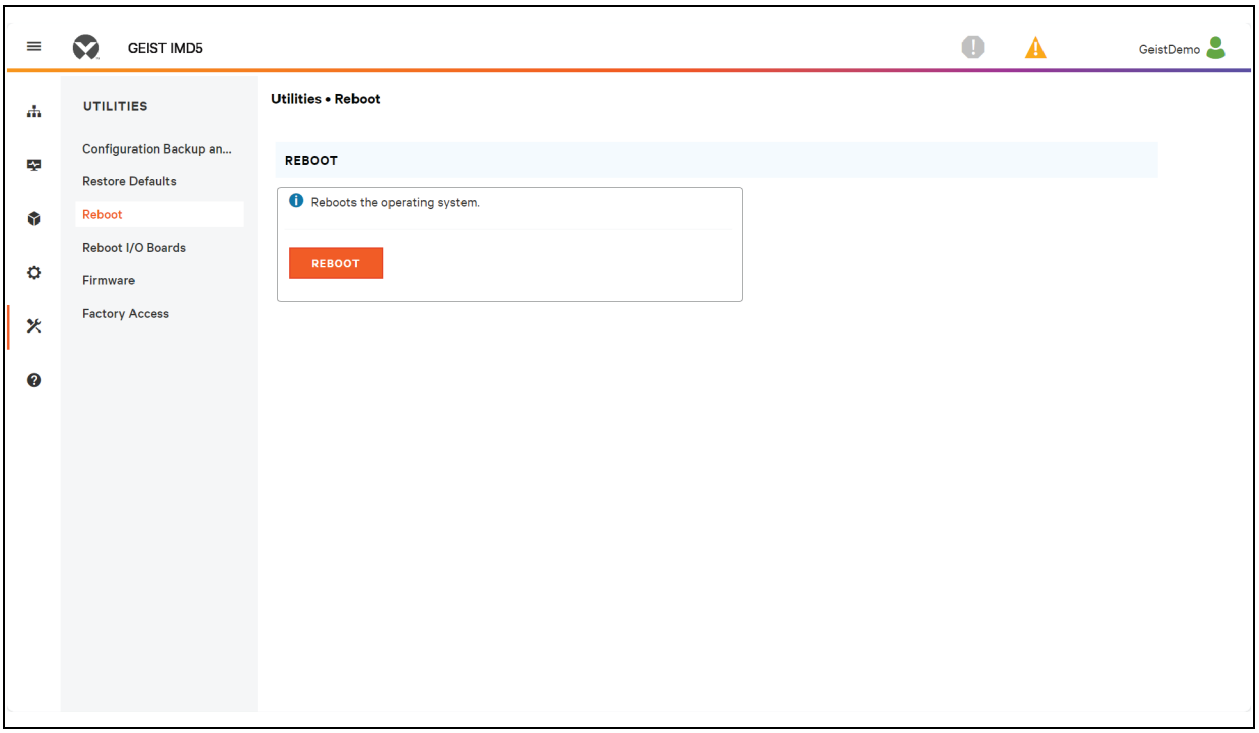
Reboots the operating system. Resets the IMD processor causing the IMD to reboot.

Click *REBOOT* to reboot the operating system.

NOTE: The power to connected devices is not affected.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.60 Rebootc Overview



5.7.4 Reboot I/O Boards

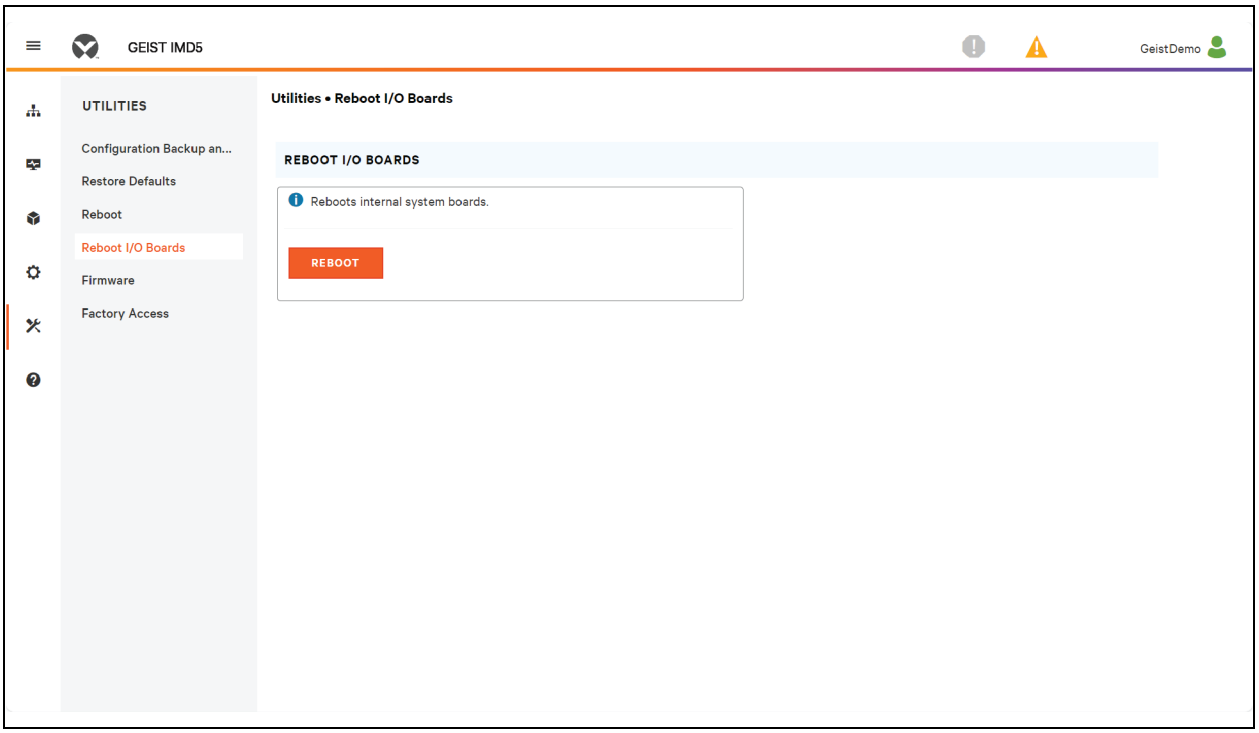
If the Vertiv™ Geist™ rPDU is not responding or not displaying all values, rebooting the internal boards will reinitialize the system. This will reset the processors on the internal input board and the outlet boards causing them to restart.

Click *REBOOT* to reboot the internal system boards.

NOTE: The power to connected devices is not affected.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.61 Reboot I/O Boards Overview



5.7.5 Firmware Updates

Uploads a firmware file that updates the system. This action requires user authentication and the user must have administrator privileges. Firmware updates typically comes in a .zip archive file containing several files including the firmware package itself, a copy of the SNMP MIB, a readme text file explaining how to install the firmware and various other support files as needed. Be sure to unzip the archive and follow the included instructions.

To update Firmware via Firmware Package File:

1. Click *SELECT UPLOAD FILE* and select the *.firmware* file from the *Open* window.
2. Click *SUBMIT*.
3. If an issue is discovered (the unit is not behaving correctly) after the firmware has been successfully installed, click *REVERT FIRMWARE*.

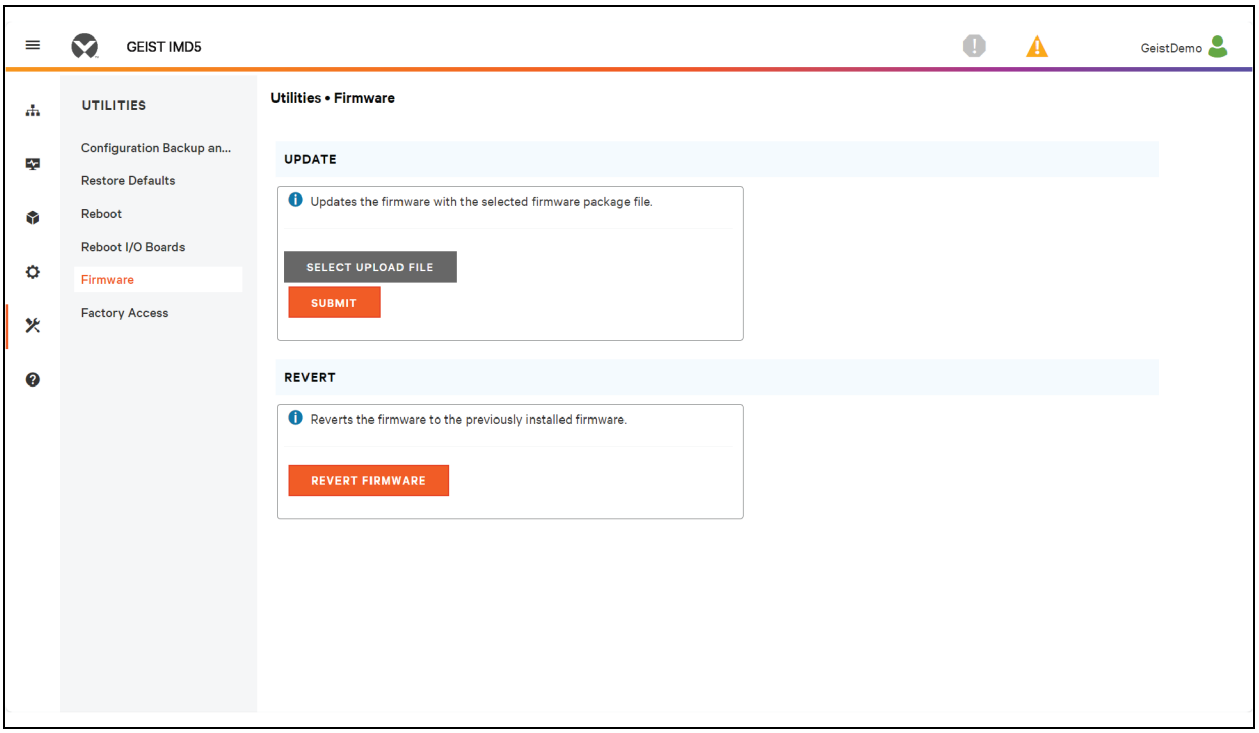
To update Firmware via a USB flash drive:

1. Download the latest firmware from *https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/* and unzip the folder.
2. Get a USB flash drive and format it as FAT32.
3. Create a directory on the USB flash drive called *FIRMWARE* (does not need to be uppercase).
4. Open the unzipped firmware folder and copy the .firmware file.
5. Paste this file into the *FIRMWARE* folder on the flash drive.
6. Plug the USB flash drive into the PDU.

During the update, the IMD will stop scrolling data. After the update is complete, a boot message will appear on the display. After reboot is complete, the IMD will resume scrolling data on the display.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.62 Firmware Overview



5.7.6 Factory Access

Factory Access Provides information for technical support.

Table 5.15 Factory Access Options

Option	Description
Download Factory Support Package	Downloads an encrypted diagnostic package that can be sent to technical support personnel.
Factory Access	Allows factory access to unit over SSH (for debugging purposes).

To download a factory support package:

1. Click *Download Factory Support Package*.
2. Click *ENC*.

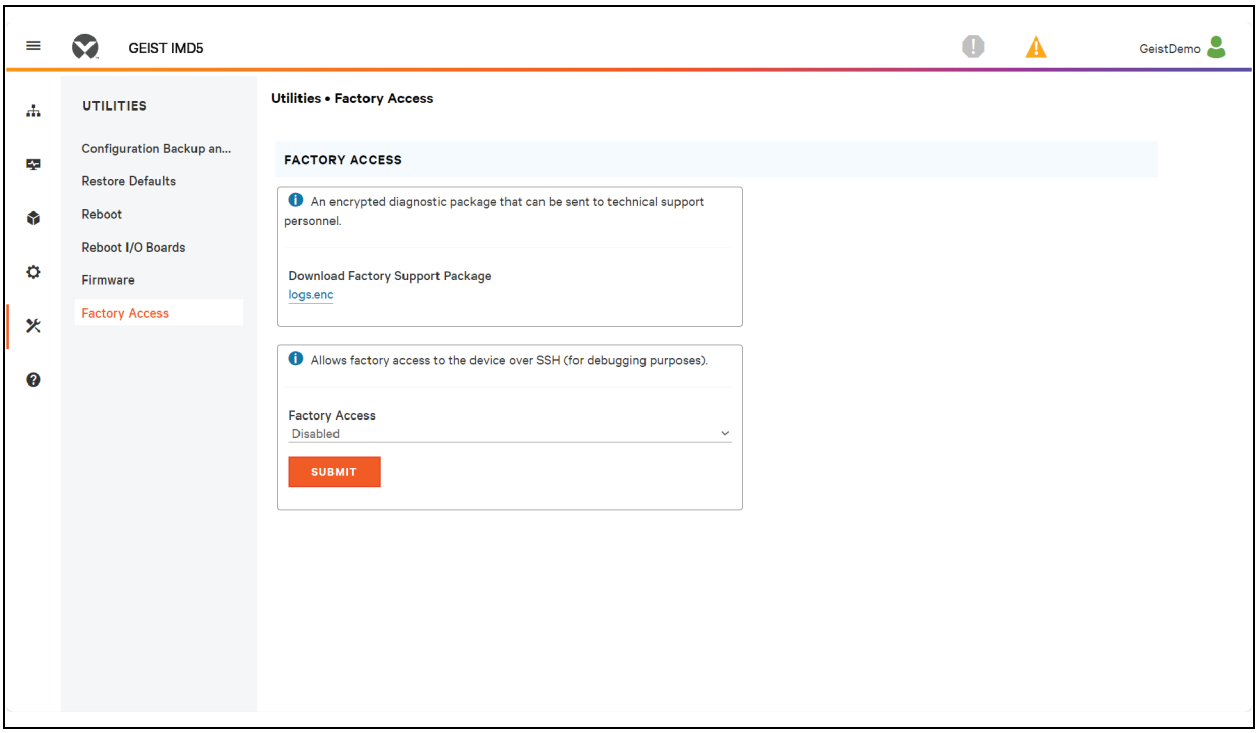
To enable/disable factory access:

1. Select either *Enable* or *Disable* from the drop-down menu.
2. Click *SUBMIT*.

NOTE: This requires user authentication and the user must have administrator privileges.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.63 Factory Access Overview



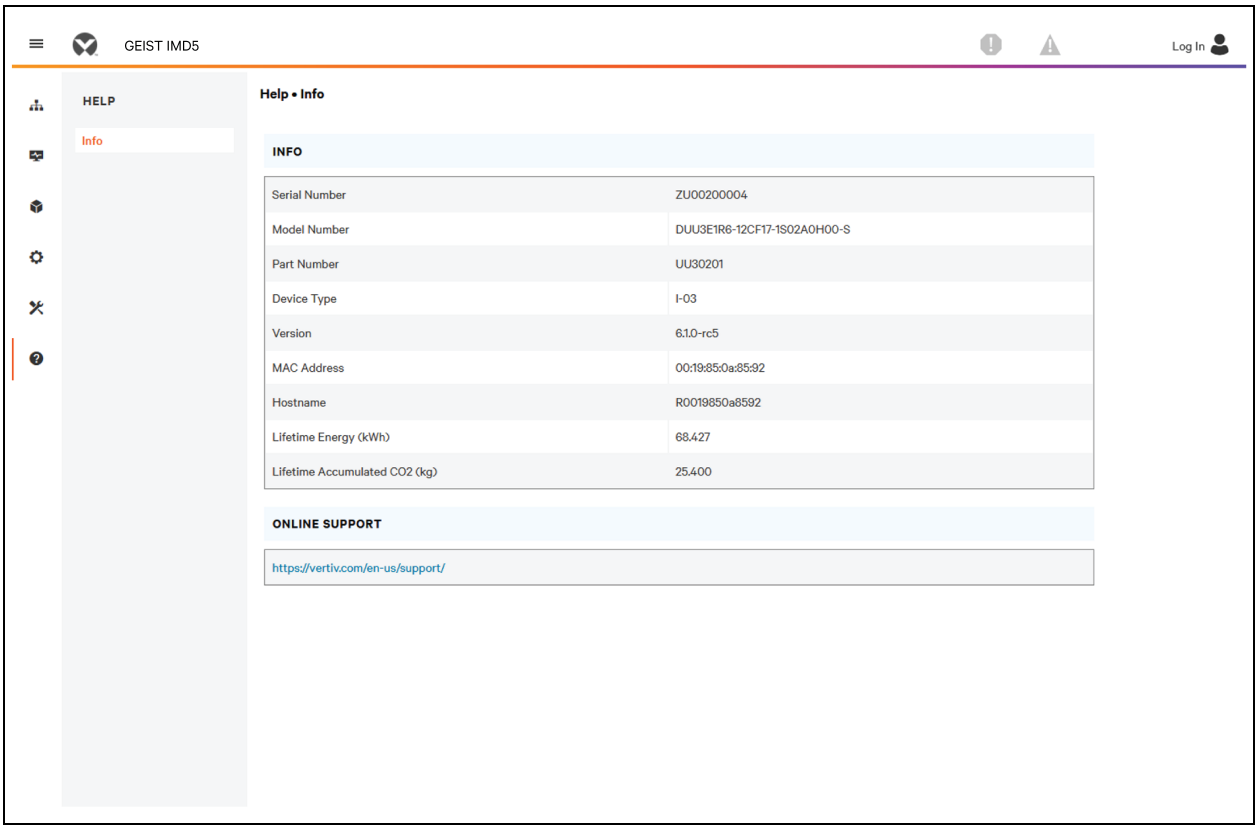
5.8 Help Sub Menu

Info Page

The Info Page displays the unit's current configuration information, including the device name and ID, the type of IMD installed, the unit's current firmware versions and network information. Manufacturer support information is also here.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 5.64 Info Page



Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

6 Vertiv™ Intelligence Director

Vertiv Intelligence Director brings a single, unified viewing layer for small deployments of the Vertiv™ Geist™ rPDUs, Vertiv™ UPSs, environmental sensors and Geist™ rPDU outlets. When deployed, Vertiv Intelligence Director offers enhanced functionality, using the Geist™ rPDU not as a stand-alone device but as a gateway to understand the broader device ecosystem in which it is installed.

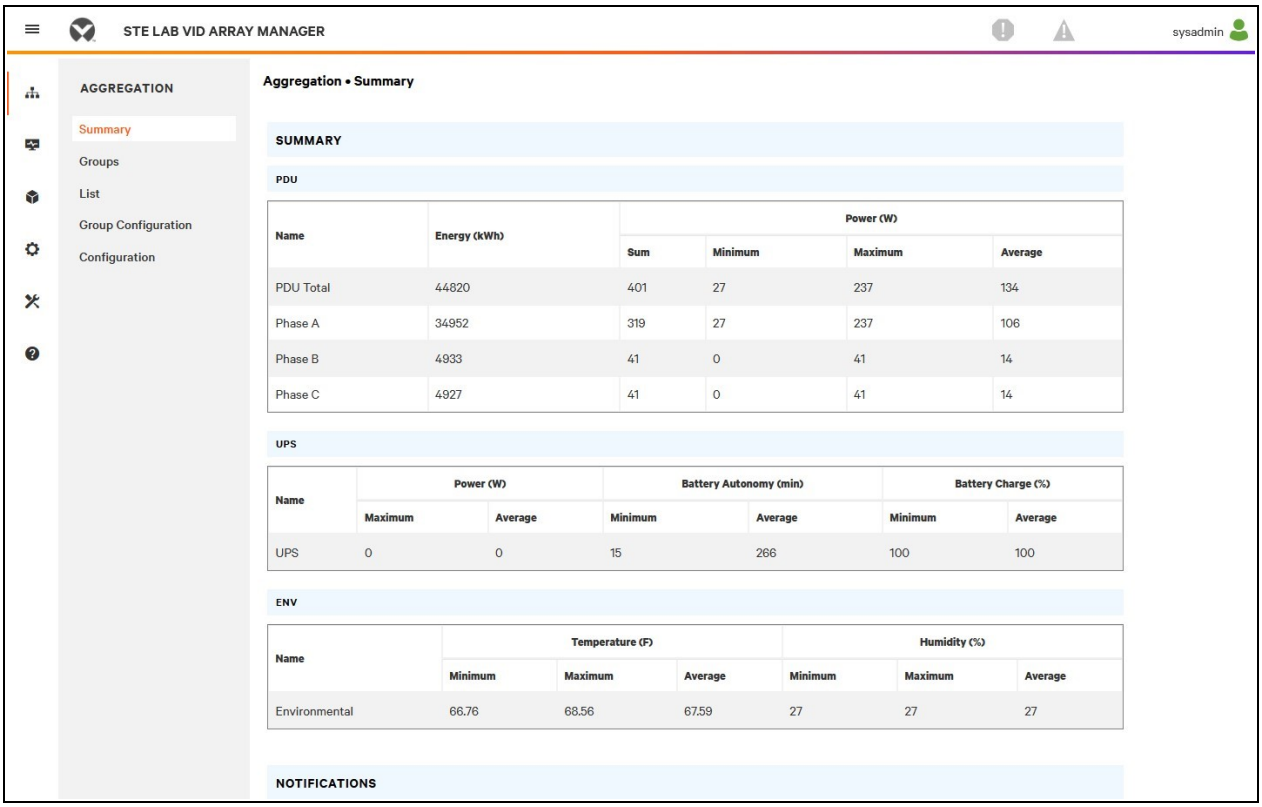
6.1 Aggregation

The initial element of Vertiv Intelligence Director, available with Geist™ rPDUs running firmware 5.3.0 or later, is called Aggregation. This single element allows you to:

- Use aggregation to reduce IP address count, aggregate data from multiple rack PDUs, and enable management of rack PDU outlet groups.
- Rack PDUs are connected using an ETHERNET daisy chain as in the daisy-chaining example above.
- The head of the chain rack PDU is configured as the array manager.
- The array device network can include network switches.
- A single IP address assigned to the array manager can be used to access up to 50 devices (the array manager and 49 array devices).
- Array device network settings are automatically configured.
- Array devices are accessed using the array manager IP address and a port number. The port number can be obtained by navigating the *Device>List page* and hovering over the device.
- Users can define groups of devices. Example, representing racks.
- The array manager generates aggregated measurements like total group power and total power, including averages, minimums, and maximums.
- Fault tolerant daisy chaining is not permitted when using Vertiv Intelligence Director.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 6.1 Aggregation Tab

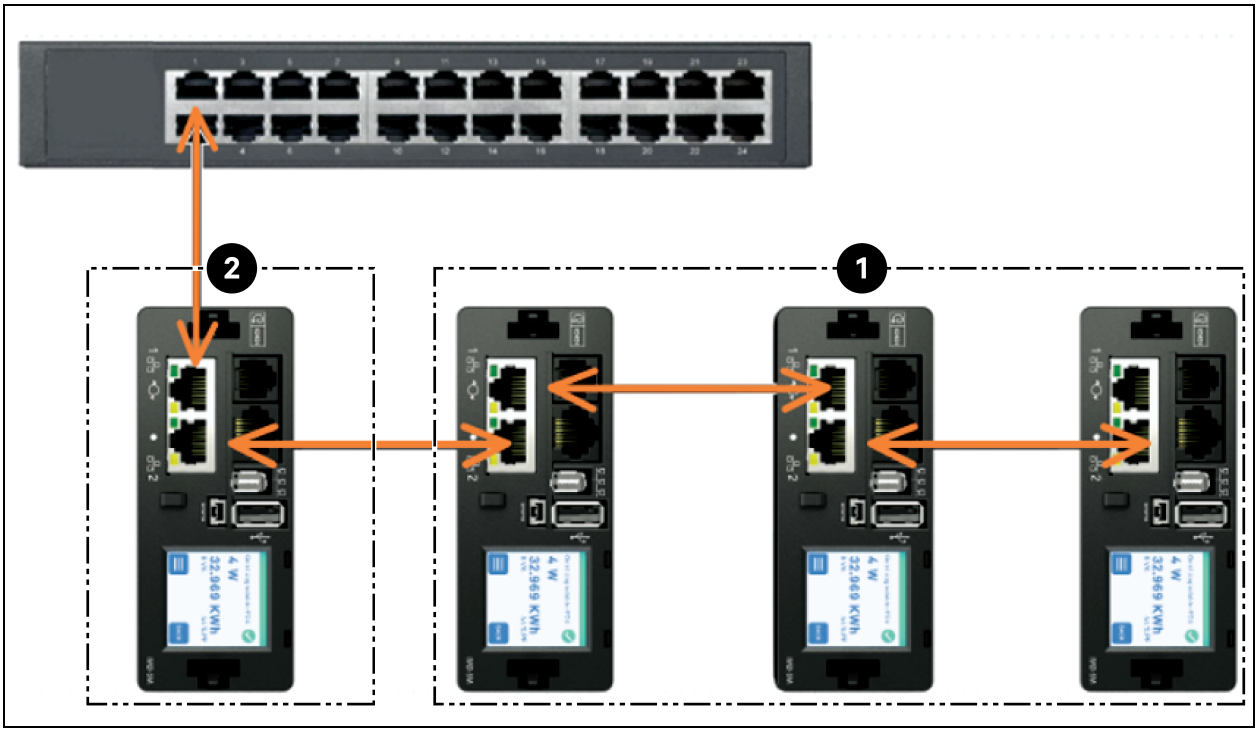


Name	Energy (kWh)	Power (W)			
		Sum	Minimum	Maximum	Average
PDU Total	44820	401	27	237	134
Phase A	34952	319	27	237	106
Phase B	4933	41	0	41	14
Phase C	4927	41	0	41	14

Name	Power (W)		Battery Autonomy (min)		Battery Charge (%)	
	Maximum	Average	Minimum	Average	Minimum	Average
UPS	0	0	15	266	100	100

Name	Temperature (F)			Humidity (%)		
	Minimum	Maximum	Average	Minimum	Maximum	Average
Environmental	66.76	68.56	67.59	27	27	27

Figure 6.2 Aggregation



Item	Description
1	Array device
2	Array manager

An additional element of Vertiv Intelligence Director, available with Vertiv™ Geist™ rPDUs running firmware 5.7.0 or later, is Rack PDU Outlet Grouping. This element allows you to:

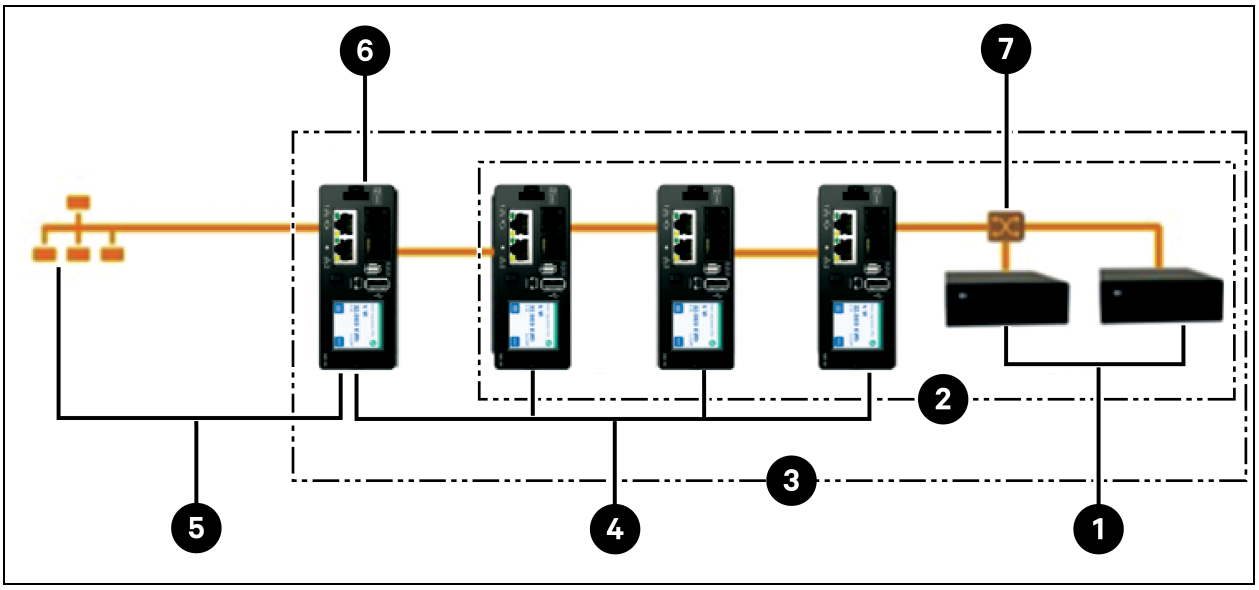
- Create groups of Geist™ rPDU outlets spanning one or more Geist™ rPDUs.
- Report on total power and energy for the outlet group (with Geist™ rPDUs that report per outlet measurements).
- Provide the ability for power off, power on or power cycle the group of outlets with a single commend (with Geist™ rPDUs that support outlet switching).

With firmware 5.10.1 or later, full visibility of Vertiv Intelligence Director (Aggregated) devices is available through SSH and serial port CLIs.

6.2 Array Manager

Aggregation requires the designation of an array manager, deployed with Geist™ rack PDUs equipped with IMD models 5M running firmware version 6.1.0 or newer or IMD models 3E, 03E, 3E (-S or -G), 03 E(-S or -G), or 5M which are currently running firmware versions 5.3.0 and newer (though the latest firmware version is strongly recommended). The IMD of the array manager facilitates and configures the device network, the interconnected array of Geist™ rPDUs, Vertiv™ UPSs, Vertiv™ cooling, environmental sensors, and Geist™ rPDU outlets, while aggregating select data points from these devices. It also interacts with the management network for monitoring and management of itself and its array devices.

Figure 6.3 Sample Configuration



Proprietary and Confidential ©2024 Vertiv Group Corp.

Item	Description
1	Vertiv™ Liebert® GXT4
2	Downstream devices
3	Device network
4	GU
5	Management network
6	Master device (GU2)
7	ETHERNET switch

It is no longer possible to onboard new IMD-02x rack PDUs when using an array manager running firmware 6.1.0 or newer.

6.3 Network Configuration

In the initial release of aggregation, array devices are defined as Vertiv™ Geist™ rPDUs within the Vertiv™ Geist™ GU2 product platforms as well as Vertiv™ MPH2™ and Vertiv™ MPX™ rack PDUs, Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM and Vertiv™ Liebert® ITA2 UPS, Vertiv™ Liebert® CRV Row Cooling and USB-connected Vertiv™ Liebert® VRC cooling. Each array manager can support up to 49 array devices, so the number of managers depends on the overall size of the installation and the preferred network architecture.

The array manager must be commissioned before it is connected to the primary management network or to the array device network. This commissioning is typically accomplished using a laptop or local machine connected directly to Port 1 on the IMD.

After local connectivity is established, you can commission the array manager.

To commission the array manager:

1. Browse to *System>Locale*. Select the appropriate Default Language and Temperature Units from the drop-down menus. These settings are pushed to the array devices in its network.
2. Browse to *System>Network*. In Protocol IPv6, choose *Enabled* from the drop-down menu.
3. Browse to *Aggregation>Configuration* Change the settings as desired.
   a. Aggregation: Choose *Enabled* from the drop-down menu.
   b. Array device Username: Defines the username to be configured on all array devices.
   c. Array device Password: Defines the password to be configured on all array devices.
   - Enter the new password, verify the password and click *Submit*. When configuring Aggregation, ensure the Managed Device Password meets all array device password complexity rules. Unless changed by the user, these require a minimum password length of 8 characters with rPDUs running 5.9.0 or later firmware.
4. Click *Submit*.

After Aggregation is enabled on the array manager, configure the remaining array manager settings. Connect the array manager to management network (Port 1) on the IMD and the device network (Port 2).

NOTE: The array manager has a built-in DHCP network to assign addresses to its array devices. This DHCP network uses *192.168.123 / 192.168.124* addresses and they cannot be used for the management network.

Array devices

In the initial release of aggregation, array devices are defined as Vertiv™ Geist™ rPDUs within the Vertiv™ Geist™ GU2 product platforms as well as Vertiv™ MPH2™ and Vertiv™ MPX™ rack PDUs, Vertiv™ Liebert® GXT4, Vertiv™ Liebert® GXT5, Vertiv™ Liebert® PSI5, Vertiv™ Liebert® EXM, Vertiv™ Liebert® APM, and Vertiv™ Liebert® ITA2 UPS, Vertiv™ Liebert® CRV Row Cooling and USB-connected Vertiv™ Liebert® VRC cooling. All Geist™ GU1 rPDUs must be running firmware Version 3.4 or later; Geist™ GU2 rPDUs must be running firmware version 5.3.0 or later. GU1 array devices cannot be onboarded with 6.1.0 or newer firmware array controllers. In all cases it is strongly recommended that all rPDUs are updated to the latest available firmware version. If the Geist™ rPDUs are newly ordered and have never been configured, they are ready for aggregation out-of-the-box. If the Geist™ rPDUs have been deployed in a computing environment and commissioned with local LAN settings and user accounts, each Geist™ rPDU must be reset to its factory defaults using the *Utilities>Restore Defaults*. Select *All Settings* and click *Submit*. The array manager will then push the configuration data to the array devices.

To set up a new installation with one array manager:

1. Install array devices in racks and power-on the racks.
2. Daisy-chain the array devices to each other where appropriate using ports labeled 1 and 2 on the IMD.
   - If using daisy chained rPDU connections ensure no daisy-chain is longer that 20 rPDUs.
   - Array devices may be networked using daisy chained connections, star connections, or a combination of both.
3. Install the array manager in a rack. Using a laptop or a local machine, connect to Port 1 to configure Aggregation.
4. Connect the array manager to the management network using Port 1.
5. Connect the array manager to the array device network using Port 2.

To set up an existing installation with one array manager:

NOTE: Use the following instructions if existing Geist™ rPDUs are connected in a daisy-chain.

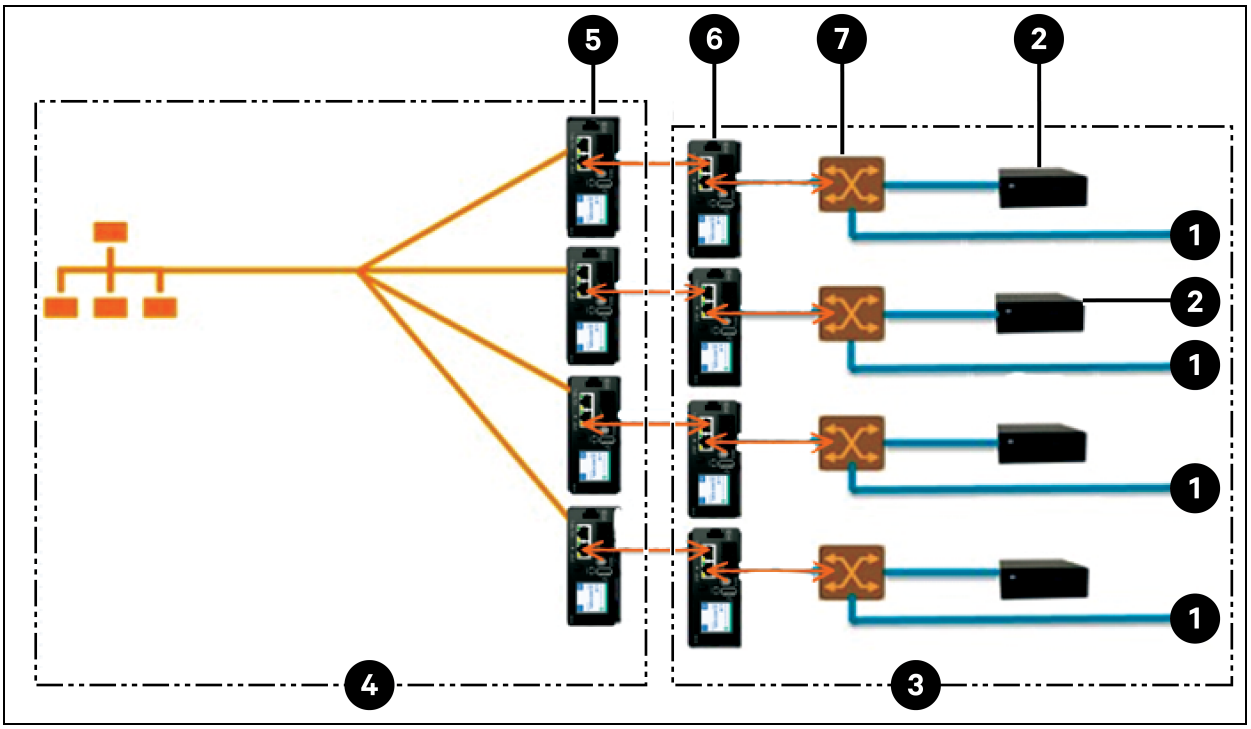
1. Designate an array manager and disconnect it from the management network.
2. Reset all the array device to factory default settings. The physical ETHERNET connections in the daisy-chain can remain the same; however, if previously connected in a looped configuration, the final Geist™ rPDU in the chain should be disconnected from the network switch.
3. Enable Aggregation on the array manager.
4. Connect the array manager to the management network using Port 1.
5. Connect the array manager to the array network using Port 2.

Multiple Array Managers

For installations with multiple array managers, keep in mind that each device network must operate as a stand-alone, isolated network. Consider a 200 rPDU example, represented in the Figure 6.4 on the next page . This installation would require a minimum of four array managers, each operating its own stand-alone the device network. Each array manager is visible on the management network and acts as a DHCP server for its array devices. A user on the management network can navigate through each array manager to reach the interface of an array device. Other considerations may affect the quantity of array managers. If you have a row network architecture, you may prefer one array manager at the start of each row, as opposed to an array manager that traverses several rows. Depending on how these 200 cabinets are divided into rows, you may have more than four array managers. When the configuration is decided, follow the appropriate process for aggregation.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 6.4 Sample Network Configuration



Item	Description
1	Other devices
2	UPS
3	Device network
4	Management network
5	Master device (GU2)
6	Downstream rPDU
7	ETHERNET switch

NOTE: A device network ETHERNET switch will only be required when connecting more than one single network port device to the end of a rPDU daisy chain or when not using daisy chained connections.

6.4 Views

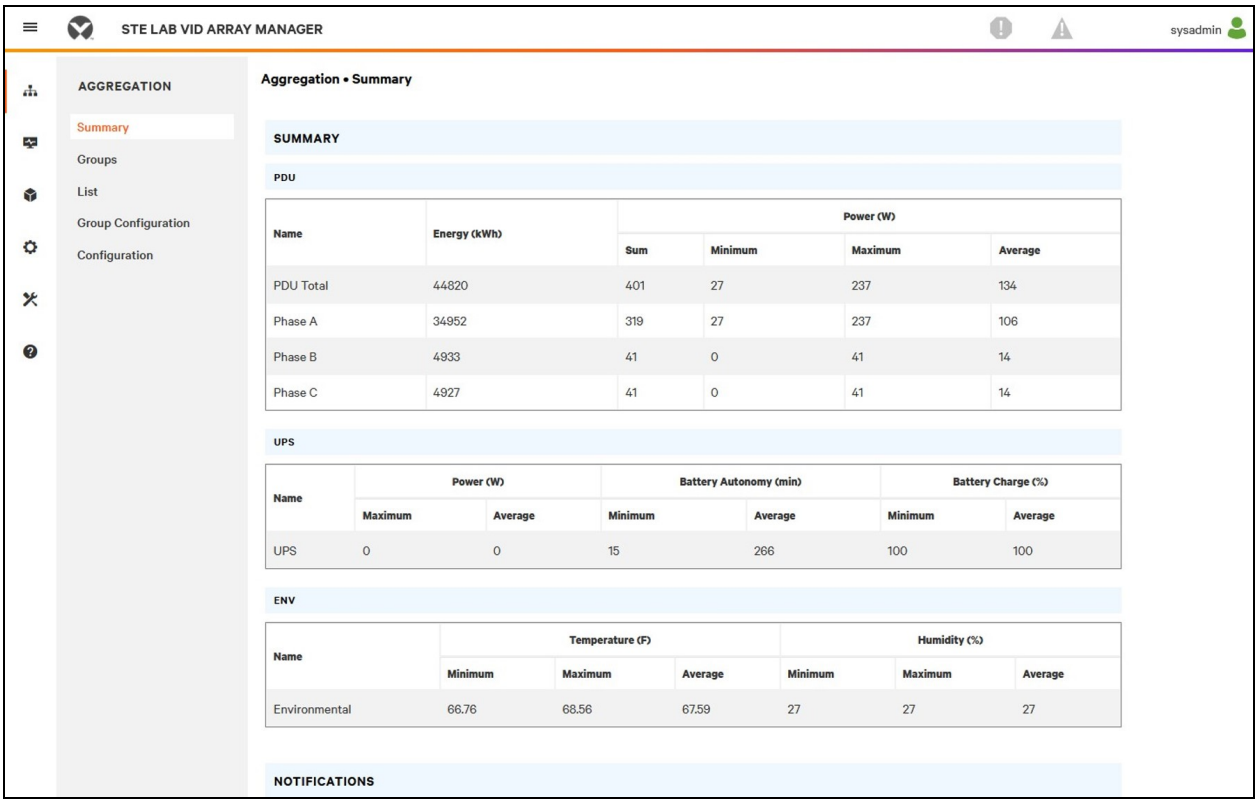
When communication is established between the array manager and array devices, several views are automatically populated in the user interface. The new views under the Device tab in the top navigation bar are:

- Summary
- Groups
- List
- Group Configuration
- Configuration

6.4.1 Summary

The Summary view aggregates data from all array devices, presenting a concise outline of relevant power, environmental, and alarm details.

Figure 6.5 Summary Tab



Name	Energy (kWh)	Power (W)			
		Sum	Minimum	Maximum	Average
PDU Total	44820	401	27	237	134
Phase A	34952	319	27	237	106
Phase B	4933	41	0	41	14
Phase C	4927	41	0	41	14

Name	Power (W)		Battery Autonomy (min)		Battery Charge (%)	
	Maximum	Average	Minimum	Average	Minimum	Average
UPS	0	0	15	266	100	100

Name	Temperature (F)			Humidity (%)		
	Minimum	Maximum	Average	Minimum	Maximum	Average
Environmental	66.76	68.56	67.59	27	27	27

Rack PDUs

The Vertiv™ Geist™ rPDU network is summarized by the following data points:

- Energy (kWh): The total Geist™ rPDU energy within the device network.
- Power (W) Sum: The total Geist™ rPDU power load within the device network.
- Power (W) Minimum: The lowest group Geist™ rPDU power load within the device network.
- Power (W) Maximum: The highest group Geist™ rPDU power load within the device network.
- Power (W) Average: The average group Geist™ rPDU power load within the device network.

NOTE: These readings are repeated per phase (shown when only 3-phase Geist™ rPDUs present).

Proprietary and Confidential ©2024 Vertiv Group Corp.

UPS

The UPS network is summarized by the following data points:

- Power (W) Maximum: The highest group UPS power load within the device network.
- Power (W) Average: The average group UPS power load within the device network.
- Battery Autonomy (min) Minimum: The lowest UPS battery run time within the device network.
- Battery Autonomy (min) Average: The average UPS battery run time within the device network.
- Battery Charge (%) Minimum: The lowest UPS battery charge within the device network.
- Battery Charge (%) Average: The average UPS battery charge within the device network.

Environmental (ENV) Sensors

The Environmental category is summarized by the following data points:

NOTE: Humidity values will be blank when temperature-only sensors are used.

- Temperature (F) Minimum: The lowest temperature within the device network.
- Temperature (F) Maximum: The highest temperature within the device network.
- Temperature (F) Average: The average temperature within the device network.
- Humidity (%) Minimum: The lowest humidity within the device network.
- Humidity (%) Maximum: The highest humidity within the device network.
- Humidity (%) Average: The average humidity within the device network.

Thermal Cooling

- Fan Speed (%) Minimum: The lowest thermal device fan speed within the device network.
- Fan Speed (%) Maximum: The highest thermal device fan speed within the device network.
- Fan Speed (%) Average: The average thermal device fan speed within the device network.
- Temperature (F) Minimum: The lowest thermal device temperature within the device network.
- Temperature (F) Maximum: The highest thermal device temperature within the device network.
- Temperature (F) Average: The average thermal device temperature within the device network.
- Capacity (%) Minimum: The lowest thermal device capacity within the device network.
- Capacity (%) Maximum: The highest thermal device capacity within the device network.
- Capacity (%) Average: The average thermal device capacity within the device network.

Notifications

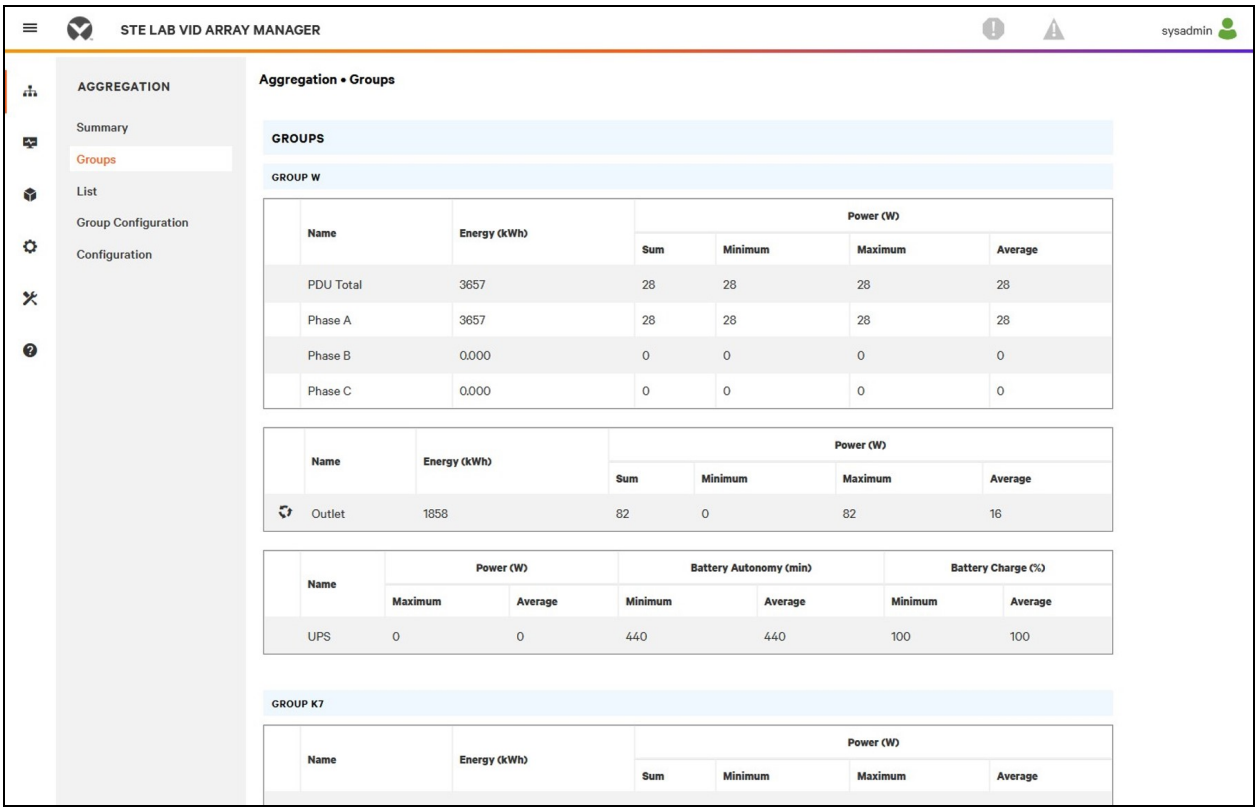
Notifications shows outstanding alarms from devices in the device network.

6.4.2 Groups

After the groups are established within the Group Configuration, the Groups view summarizes power and environmental data.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 6.6 Groups Tab



The available data points are:

Group rPDU

- Energy (kWh): The total Vertiv™ Geist™ rPDU energy within the group.
- Power (W) Sum: The total Geist™ rPDU power load within the group.
- Power (W) Minimum: The lowest Geist™ rPDU power load within the group.
- Power (W) Maximum: The highest Geist™ rPDU power load within the group.
- Power (W) Average: The average Geist™ rPDU power load within the group.

NOTE: These readings are repeated per phase (shown when only 3-phase rPDUs present).

Group rPDU Outlet

- Energy (kWh) : The total Geist™ rPDU Outlet energy within the group.
- Power (W) Sum: The total Geist™ rPDU Outlet power load within the group.
- Power (W) Minimum: The lowest Geist™ rPDU Outlet power load within the group.
- Power (W) Maximum: The highest Geist™ rPDU Outlet power load within the group.
- Power (W) Average: The average Geist™ rPDU Outlet power load within the group.

These readings repeat for each group of Vertiv™ Geist™ rPDU outlets present in the group when at least one monitored outlet is present. If a combination of outlet monitored and non-outlet monitored rack PDUs are present in the group, the readings will be the total of the outlet monitored rack PDUs only.

Proprietary and Confidential ©2024 Vertiv Group Corp.

These readings repeated for each phase (shown when only 3-phase PDUs present).

NOTE: The energy readings reflect the sum of outlet energy readings and resetting each outlet energy reading will also reset the total energy for the outlet group.

The Operation icon is shown for each group that includes at least one rack PDU outlet with switching capability.

To change outlet group operation:

1. Click the Operation icon.
2. Select the operation to perform (applies to only switching capable Rack PDU outlets assigned to the group):
   - On/Off: Turns all outlets On or Off.
   - Reboot: For outlets currently On, reboot cycles the outlets Off, then back On after the reboot hold delay.

     For outlets currently Off, reboot turns the outlets On.
   - Cancel: Cancels the current operation if it has not been completed.
3. For operations involving the state of the outlets, setting Delay to True uses the current Delay configuration for each outlet.
4. Select *Submit* to issue the action.

Group UPS

- Power (W) Maximum: The highest UPS power load within the group.
- Power (W) Average: The average UPS power load within the group.
- Battery Autonomy (min) Minimum: The lowest UPS battery run time within the group.
- Battery Autonomy (min) Average: The average UPS battery run time within the group.
- Battery Charge (%) Minimum: The lowest UPS battery charge within the group.
- Battery Charge (%) Average: The average UPS battery charge for the group.

Group Environmental

- Temperature (F) Minimum: The lowest temperature within the group.
- Temperature (F) Maximum: The highest temperature within the group.
- Temperature (F) Average: The average temperature within the group.
- Humidity (%) Minimum: The lowest humidity within the group.
- Humidity (%) Maximum: The highest humidity within the group.
- Humidity (%) Average: The average humidity within the group.

Group Thermal Cooling

- Fan Speed (%) Minimum: The lowest thermal device fan speed within the group.
- Fan Speed (%) Maximum: The highest thermal device fan speed within the group.
- Fan Speed (%) Average: The average thermal device fan speed within the group.
- Temperature (F) Minimum: The lowest thermal device temperature within the group.
- Temperature (F) Maximum: The highest thermal device temperature within the group.
- Temperature (F) Average: The average thermal device temperature within the group.
- Capacity (%) Minimum: The lowest thermal device capacity within the group.

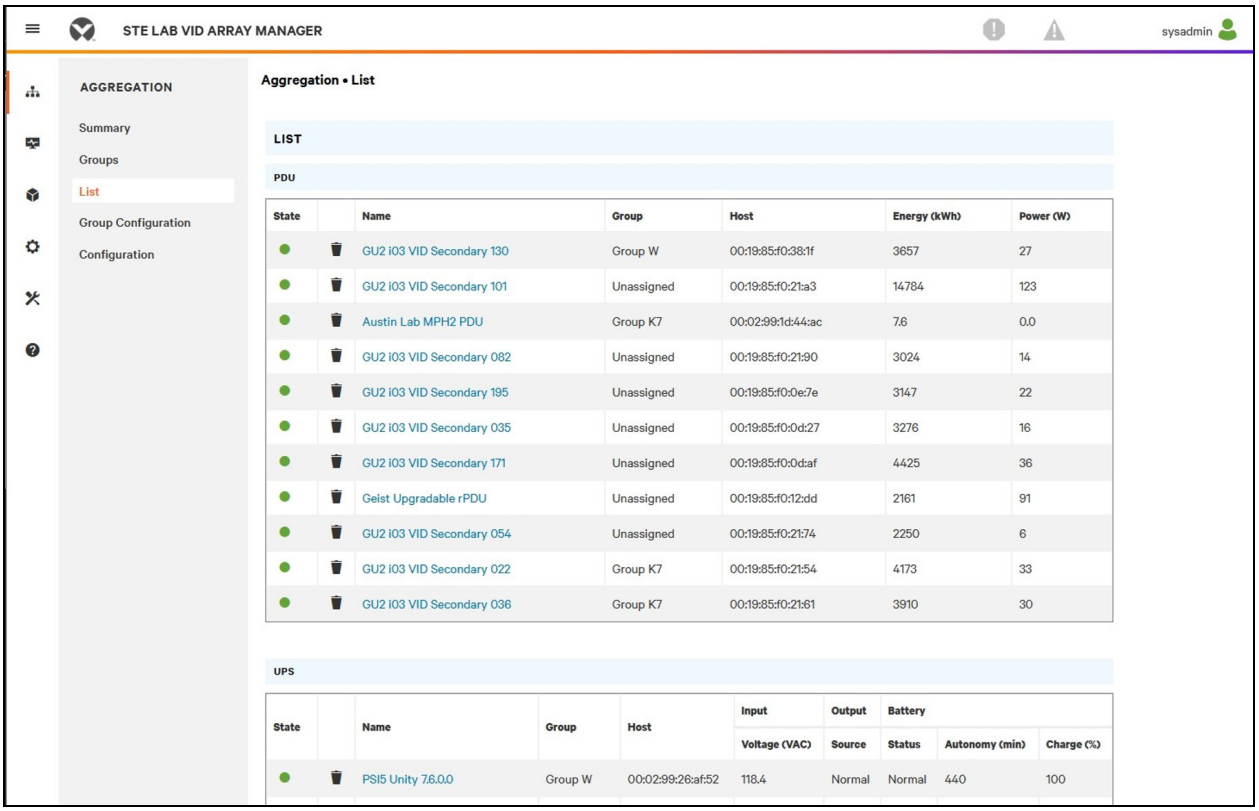
 Proprietary and Confidential ©2024 Vertiv Group Corp.

- **Capacity (%) Maximum:** The highest thermal device capacity within the group.
- **Capacity (%) Average:** The average thermal device capacity within the group.

6.4.3 List

The List view presents an inventory of all devices within the array manager's Device network.

Figure 6.7 List Tab



The inventory is subdivided into the following categories:

Rack PDUs

All Vertiv™ Geist™ rPDUs in the device network roll into this category and present the following data points:

- **State:** The status of the Geist™ rPDU. Status is either normal or unavailable (loss of connectivity).
- **Name:** Geist™ rPDU label. Clicking on the name opens a browser tab for device access.
- **Group:** The group name. If there is no user created group, the group name is Unassigned.
- **Energy:** Geist™ rPDU energy.
- **Power:** Total Geist™ rPDU power load.

UPS

All UPS devices in the device network roll into this category and present the following data points:

- **State:** The status of the UPS. Status is either normal or unavailable (loss of connectivity).

 Proprietary and Confidential ©2024 Vertiv Group Corp.

- **Name:** UPS label. Clicking on the name opens a browser tab for device access.
- **Group:** The group name. If there is no user-created group, the group name is Unassigned.
- **Input Voltage:** UPS input voltage.
- **Output Source:** The UPS operating mode, which can be: Normal, Bypass, Battery, Booster, Reducer, Off, or Other.
- **Status:** The battery status, which can be: Normal , Low, Depleted, or Unknown.
- **Battery Autonomy:** UPS battery run time.
- **Charge:** UPS battery charge.

Environmental (ENV) Sensors

All Environmental Sensors in the device network roll into this category and present the following data points:

- **State:** The status of the Sensor. Status is either normal or unavailable (loss of connectivity).
- **Name:** Sensor label. Clicking on the name opens a browser tab for device access.
- **Group:** The group name. If there is no user-created group, the group name is Unassigned.
- **Device:** Displays the sensor parent Vertiv™ Geist™ rPDU label and MAC address.
- **Temperature (F):** Temperature reading (main temperature only with GT3HD sensors).
- **Humidity (%):** Humidity reading. This field is blank if only SRT temperature sensors are deployed.

Environmental sensors, report their values through the MIB of the Geist™ rPDUs to which they are connected. They are not stand-alone sensors with their own IP addresses. In this release, the only valid sensors are Geist™ rPDU-connected Geist™ SRT, GTHD or GTHD3 sensors.

NOTE: The label of any device can be customized by logging into the device and editing through the Configuration icon.

NOTE: To delete a device which has been removed from the network, select the Trash icon next to the device. Selecting Delete icon deletes the device and any Environmental Sensors connected to it.

Thermal Cooling

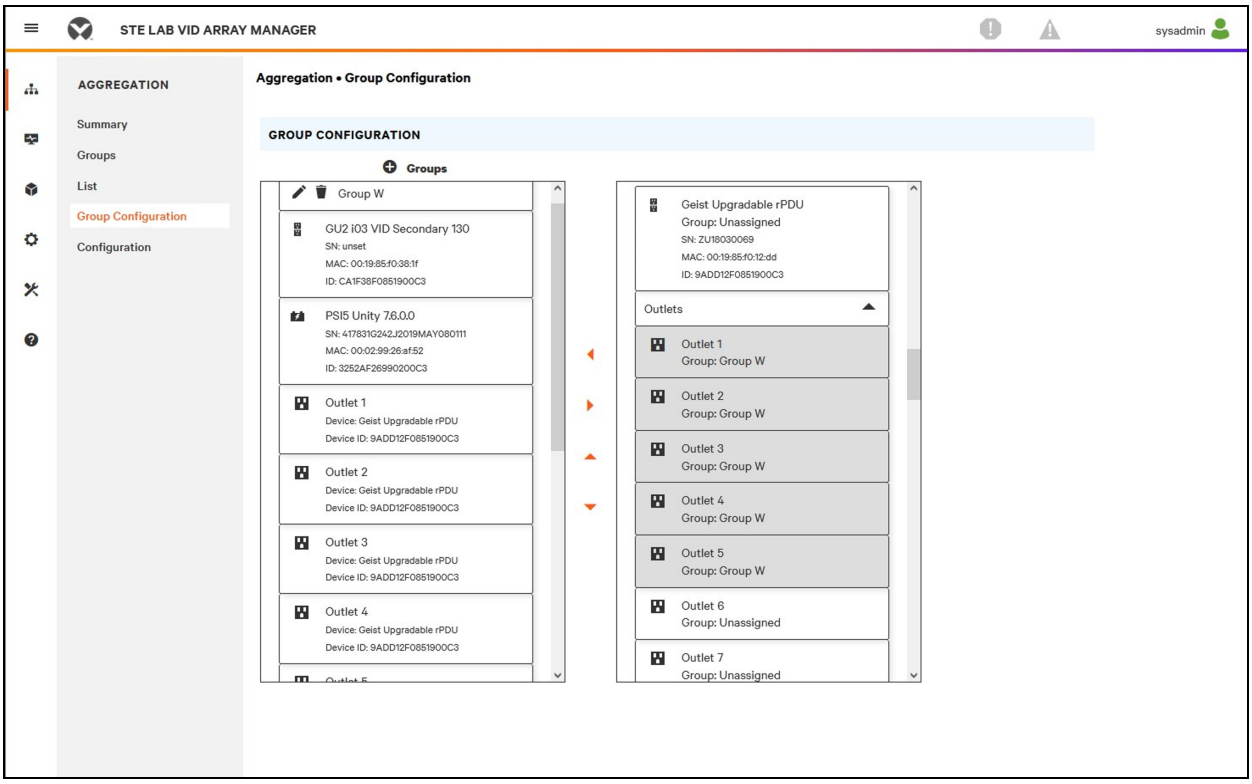
- **State:** The status of the cooling. Status is either Normal or Unavailable (loss of connectivity).
- **Name:** Thermal cooling device label. Clicking on the name opens a browser tab for device access.
- **Group:** The group name. If there is no user created group, the group is Unassigned.
- **Host:** MAC address.
- **Fan Speed (%):** Thermal device fan speed.
- **Temperature (F):** Thermal device temperature.
- **Capacity (%):** Thermal device capacity.

6.4.4 Group Configuration

On the Group Configuration page, you can define groups of devices for data aggregation and analytic purposes. A group often refers to a unit of measure within a computing environment that includes multiple array devices, such as a rack with two Geist™ rPDUs, UPS devices and environmental sensors or a row that includes multiple racks.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure 6.8 Group Configuration



The Group Configuration page lists the automatically discovered devices under the *Unassigned* column showing:

- One or more icons defining the type of device such as, Vertiv™ Geist™ rPDU, Environmental Sensor, UPS or Geist™ rPDU Outlet.
- Device label
- Serial number
- MAC address
- ID

Configured groups of devices (typically representing racks) are shown on the left.

To create a new group:

1. Click the *plus sign (+)* to the left of Groups, to add a new group, under Groups.
2. Click the Configuration icon to change the name of the group label.
3. Edit the label, if desired, and click *Save*.
4. To assign devices to the group, highlight the desired group (within Groups category) and highlight the desired devices within the Unassigned category.

NOTE: You must click on the down arrow below the PDU to see the list of its outlets.

5. Click the *Right Arrow* to assign the devices to the group.
6. Repeat the process for other groups, as needed.

NOTE: Groups can be reordered by clicking the up or down arrows.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

To remove devices from a group:

Highlight the devices and click the *Right Arrow*.

To delete a group:

Click the Trash icon next to the group name.

NOTE: Deleting a group returns all of its devices to the Unassigned group

6.5 Interfaces

Array devices are combined to form groups; each device retains its own stand alone user interface and SNMP data.

To access the Array Device User Interface:

1. From the List View, use your mouse to hover over the entries in the table. A yellow highlight and text box appear as you pause on the devices. The text box reveals the IP address of the device and port number of the device.
2. Navigate to an IP address and port number to access the web server interface of the device.

   -or-

3. Click the name of the device to access the hyperlink to the device web interface.

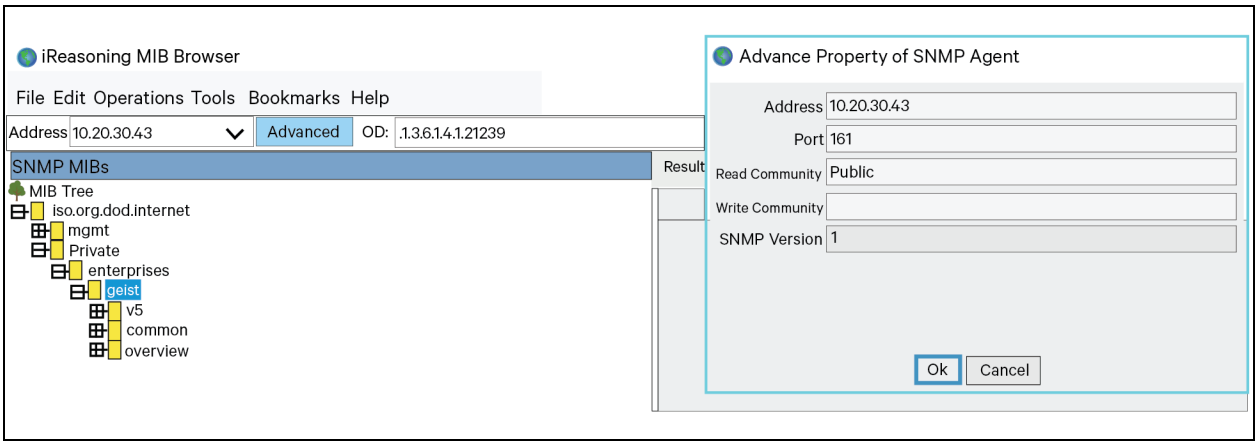
To access Array Device SNMP Data:

SNMP Geist Rack PDU Data is available using port-mapped access through the array manager device IP address using the Geist™ v5 MIB. The MIB file is downloadable from the array manager SNMP page.

1. From the List view, use your mouse to hover over the entries in the table. As you pause over a device, a yellow highlight and text box appear with the SNMP port of the device.
2. In the MIB browser, enter the SNMP port listed.

NOTE: Software to monitor individual array devices must be capable of accepting a unique SNMP port number per monitored device.

Figure 6.9 MIB Browser



6.5.1 Group SNMP data

Aggregated data, both summary (such as total kWH and maximum kW) and group data, is available through the master Vertiv™ Geist™ rPDU IP address and default SNMP Port 161. Two MIBS are available for the Array Controller Geist rack PDU:

- v5: Contains data points for the individual Master Geist™ rPDU.
- Oneview: Contains data points for aggregated data across all array devices.

6.5.2 Tips and troubleshooting

- It is recommended that all devices are updated to the latest firmware version before configuring aggregation.
- Ensure that the rack PDU nominated as the array manager is fully configured and aggregation is enabled before connecting any array devices.
- Ensure all array devices are in a factory default state before connecting them to the array manager. If settings have previously been changed or if any users have been defined on a device, the device must be reset to factory defaults before the device is connected to the array manager.
- If resetting a rack PDU to the factory default settings, ensure you use the *Utilities>Restore defaults>All Settings* function. Using the IMD center button or pinhole reset switch under network port 2 to reset settings does not reset all settings and may cause array devices to not be identified correctly.
- After resetting a rack PDU to factory default settings and before connecting it as an array device, disconnect the rack PDU from the network and restart it using the button beneath network port 1. This ensures any DHCP address allocated during the reset to factory defaults procedure is released.
- It can take up to 20 minutes for array device devices to be recognized after initial setup.
- Summary and group aggregated data cannot be alarmed upon.
- The Provisioner Tool (*Provisioner>Discovery and Provisioner>File Management*) can be used to easily update array manager and array device rack PDU firmware.
- Summary and Group aggregated data cannot be used to generate SNMP traps.
- SNMP community names are configured on each device. Follow the device links displayed on the List page under the Devices menu and logging into each device to configure SNMP.
- Do not change the default SNMP port number, Network settings or Web Server settings when logged into an array device.
- SNMP traps and alarms are routed from a device to the management network through the master device.

Proprietary and Confidential ©2024 Vertiv Group Corp.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendices

Appendix A: Technical Support

A.1 Resetting a Vertiv™ Geist™ rPDU

If a Geist™ rPDU loses communication, the processor may be manually rebooted without affecting power to the outlets. Pressing the reboot button on the face of the IMD will reboot the processor. The web interface will remain offline during boot-up. For more information, see Interchangeable Monitoring Device on page 27 .

A.2 Service and Maintenance

No service or maintenance is required. Opening the Geist™ rPDU may void the warranty. There are no user-serviceable parts inside the Geist™ rPDU other than the field-replaceable Interchangeable Monitoring Device (IMD). Geist™ recommends removing power from the unit before installing or removing any equipment.

The IMD is designed to be field-replaceable by properly trained and qualified service personnel only. The IMD is designed to be replaced while the Geist™ rPDU is still connected to utility power. Refer the Geist™ rPDU IMD Modules Replacement Guide for more information.

A.3 More Technical Support

Technical support can be found at *www.Vertiv.com/support*.

Americas

- **Website:** *www.Vertiv.com/geist*
- **Email:** geistsupport@vertiv.com
- **Telephone:** 1-888-630-4445

Europe and Middle East

- **Technical Support:** *www.Vertiv.com/en-emea/support*
- **Email:** eoc@Vertiv.com
- **Telephone:** 44 1823 275100

Asia

- **Telephone (English):** 1-888-630-4445 (US number)
- **Telephone (Chinese):** +86 755 23546462

A.4 Using Microsoft Exchange as an SMTP Server

If your facility uses a Microsoft Exchange email server, it can be used by the IMD Geist™ rPDU to send Alarm and Warning notification emails. However, the Exchange server may need to be configured to allow SMTP connections from the unit first, as later versions of Exchange server often have SMTP services or basic authentication disabled by default. If you encounter difficulties in getting your IMD Geist™ rPDU to send emails through your Exchange server, the following notes may help.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

NOTE: These suggestions apply only if you are using your own, physical Exchange server. Microsoft's hosted Office 365 service is not compatible with the IMD Vertiv™ Geist™ rPDU using firmware versions prior to v3.0.0, as Office 365 requires a StartTLS connection. Firmware versions 3.0.0 and beyond have support for StartTLS and are compatible with Office 365.

First, since the IMD Geist™ rPDU cannot use IMAP or Microsoft's proprietary MAPI/RPC Exchange/Outlook protocols to send messages, you must enable SMTP by setting up an SMTP Send Connector in the Exchange server. More information on setting up an SMTP Send Connector in Exchange can be found at this Microsoft TechNet article: *http://technet.microsoft.com/en-us/library/aa997285.aspx*

Second, you may need to configure your Exchange server to allow messages to be relayed from the monitoring unit. Typically, this will involve turning on the *Reroute incoming SMTP mail* option in the Exchange server's Routing properties, then adding the IMD Geist™ rPDU's IP address as a domain that is permitted to relay mail through the Exchange server. More information about enabling and configuring SMTP relaying in Exchange can be found at this Microsoft TechNet article: *http://technet.microsoft.com/en- us/library/dd277329.aspx*

The SMTP AUTH PLAIN and AUTH LOGIN authentication methods for logging in to the server are often no longer enabled by default in Exchange Server; only Microsoft's proprietary NTLM authentication method is enabled.

To re-enable the AUTH LOGIN method:

1. In the Exchange console, select *Server Configuration - Hub Transport*.
2. Right-click the *Client Server* and select *Properties*.
3. Select the *Authentication* tab and click the *Basic Authentication* checkbox.
4. Deselect the *Offer Basic only after TLS* checkbox.
5. *Apply* or *Save* and click *Exit*.

NOTE: You may need to restart the Exchange service after making these changes.

Finally, once you have enabled SMTP, relaying and the AUTH LOGIN Basic Authentication method, you may also need to create a user account specifically for the IMD Geist™ rPDU to log into. If you created an account prior to enabling the SMTP Send Connector or if you are trying to use an account created for another user and the IMD Geist™ rPDU still cannot connect to the Exchange server, the account probably did not properly inherit the new permissions when you enabled them as above. This tends to happen more often on Exchange servers that have been upgraded since the account you are trying to use were created, but can sometimes happen with accounts when new connectors and plug-ins are added, regardless of the Exchange version. Delete the user accounts, then create a new one for the monitoring unit to use and the new account should inherit the SMTP authentication and mail-relaying permissions correctly.

If none of the above suggestions succeed in getting your IMD Geist™ rPDU to send mail through your Exchange server, then you may need to contact Microsoft's technical support for assistance in configuring your Exchange server to allow SMTP emails to be sent from a third-party, non-Windows device through your network.

 Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix B: Available Sensors

B.1 Remote Sensors

- **SRT:** Stainless Remote Temperature.
- **GTHD:** Temperature/Humidity/Dew Point.
- **GT3HD:** Temperature/Humidity/Dew Point with two SRT sensors.
- **RTAFHD3:** Temperature/Air Flow/Humidity/Dew Point.
- **A2D:** Converts Analog I/O Sensors to Remote Digital Sensors.

B.2 Analog I/O Sensors

- **FS-15:** Flood (Water) Sensor.
- **PFS-100 US / PFS-100 UN:** Power Failure Sensor.
- **RPDS:** Door Switch Kit.

B.3 Liebert® Integrated and Modular Sensors

NOTE: An adapter is required to use any of the following sensors.

- **SN-T:** One Temperature Probe.
- **SN-TH:** One Temperature Probe and one Humidity Probe.
- **SN-Z01:** Integrated Cable with one Temperature Probe.
- **SN-Z02:** Integrated Cable with three Temperature Probes.
- **SN-Z03:** Integrated Cable with four Probes (three Temperature and one Humidity).
- **SN-2D:** Two-Door Switch Monitor Sensor.

B.4 Connecting Remote Sensors

Up to 16 plug-and-play remote sensors can be attached to the unit at any time via the RJ-12 connectors on the front of the unit. In some cases, splitters may be required to add additional sensors. Each sensor has a unique serial number and is automatically discovered and added to the web page. The sensors serial number determines their display order on the web. Sensor names can be customized on the Sensors Overview age.

NOTE: Sensors use Cat 5, CMP wire and RJ-12 connectors. Wiring must be straight-through. Reverse polarity temporarily disables all of the sensors until corrected. Sensors use a serial communication protocol and are subject to network signaling constraints dependent on shielding, environmental noise and length of wire. Typical installations allow runs of up to 600 ft. (180 m) of sensor wire.

Appendix C: TP-Link Wireless USB adapters

- Archer T2U Nano (AC600 Nano Wireless USB Adapter)
- Archer T2U Plus (AC600 High Gain Wireless Dual Band USB Adapter)
- Archer T2U v3 (AC600 Wireless Dual Band USB Adapter)
- Archer T3U (AC1300 Mini Wireless MU-MIMO USB Adapter)
- Archer T3U Plus (AC1300 High Gain Wireless Dual Band USB Adapter)
- Archer T4U v3 (AC1300 Wireless Dual Band USB Adapter)

NOTE: These devices are auto detected when connected and can be configured as an additional network interface.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix D: Outlet LEDs

NOTE: This appendix applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rPDUs only.

Outlet LEDs provide a visual indication of outlet power status (On, Off or Error). The LEDs are sequentially numbered with easy-to-read white numbers on a black background. Depending on outlet power status, the LEDs illuminate in solid colors or blinking colors.

Table D.1 LED Outlets

LED	Description
Green	Outlet voltage is present and above minimum threshold limit
Red	Outlet voltage is not present
Amber	Power output error condition has been detected

Table D.2 LED Status Description

Measured voltage	Relay state	State	LED	
On	On or Unknown	Solid	Green	
Off	Off or Unknown	Solid	Red	
Off	On	Blinking [1]	Amber	Red
On	Off	Blinking [2]	Amber	Green

[1] Outlet is sensed to be Off but should be On.

[2] Outlet is sensed to be On but should be Off.

Error Code

LEDs illuminate in Solid Amber during the following:

- Power failure (all relays are forced open in the event of power failure to allow for power-on sequencing)
- Circuit breaker open
- No input voltage detected

Appendix E: IMD Display Codes

Table E.1 IMD Display Codes

Display	IMD Type	Explanation
Err1	IMD-01 (Metered only)	The IMD discovered either none or more than one input board. This may be caused by internal cabling issues or an unresponsive input board. This is also displayed if there is a measurement error reported by the input board.
8888	IMD-02, IMD-03, IMD-3	IMD is booting and has yet to discover the simple display and shows *boot* on it. If this is displayed for more than a few seconds there is a problem the display board or with internal cabling.
-- (Two dashes on the right-most display position)	IMD-02, IMD-03, IMD-3	The IMD cannot communicate with the input board. This may also be shown intermittently for individual measurements. There is a problem with the input board or with internal cabling.
boot	IMD-01	IMD is booting and discovering the input board.
boot	IMD-02, IMD-03, IMD-3	Firmware is initializing. This will be displayed while firmware is being updated in internal boards.
updt	IMD-02, IMD-03, IMD-3	Firmware update in progress.
rset dflt	IMD-02, IMD-03, IMD-3	Following user action, *rset* (Reset) will appear during a parameter reset sequence. During a parameter reset, *dflt* (Default) will appear briefly.
bcup	IMD-02, IMD-03, IMD-3	*bcup* (Backup) will appear during a configuration backup.
rest conf	IMD-02, IMD-03, IMD-3	*rest* (Restore) and *Conf* (Configuration) will appear during a configuration restore .
____ (Four underscores on the bottom of the display)	IMD-03 IMD-3	The IMD display has been configured such that Total Power, Voltage and Current has been disabled.

NOTE: The IMD-5M does not have Display Codes; the touchscreen displays status information.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix F: Provisioner - Format of the configuration settings file

NOTE: The following describes the format of the configuration settings file used by the Provisioner. The examples broadly follow the settings available in the Vertiv™ Geist™ rPDU web user interface.

1. In the examples below, the text in blue can be copied to a text file and updated as required. The text file can then be uploaded to the provisioning tool.
2. When editing configuration files, use a text editor such as notepad which can save files in .txt format.
3. The indentations shown in the examples can be omitted.
4. Ensure the correct double quote is used when editing configuration.
5. If a setting is omitted from the settings file, the value of that setting will remain unchanged.
6. When configuring a previously unconfigured (factory fresh) Geist™ rPDU, the first configuration setting should be the definition of an admin user, See Local Users below .
7. To combine several settings (other than local users) into one file (see also Example 1 on page 132 at the end of this document):
   - Append together the required settings into one file.
   - Delete all occurrences of {"conf":{ except for the first line of the file.
   - Replace all lines that contain only }} by a , (comma) except for the last line of the file.
8. If combining local user settings with other settings in one file, refer to Example 2 on page 133 at the end of this document.
9. After selecting *Provisioner>Discovery>Update*, enter the user name and password only when configuring previously configured Geist™ rPDUs (the user name and password being that of the Geist™ rPDUs being provisioned). Do not enter a user and password when configuring factory fresh units (identified by Provisioned attribute equalling False).

Local Users

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
}}
```

username	The user name to be created (in quotes)
password	Password (in quotes)
enabled	Options true or false determines whether the user is enabled
control	Options true or false determines whether the user will have control privileges
admin	Options true or false determines whether the user will have admin privileges
language	Overrides default language for this user, valid options are "de", "en", "es", "fr", "ja", "ko", "pt", "zh"

LDAP


```
{"conf":{
"remoteAuth": {
"mode": "ldap",
"ldap": {
"host": "192.168.123.1",
"port": 389,
"mode": "activeDirectory",
"securityType": "ssl",
"bindDn": "",
"password": null,
"baseDn": "",
"userFilter": "(objectClass=posixAccount)",
"userId": "uid",
"userIdNum": "uidNumber",
"groupFilter": "(objectClass=posixGroup)",
"groupId": "gidNumber",
"groupMemberUid": "memberOf",
"enabledGroup": "enabled",
"controlGroup": "control",
"adminGroup": "admin"}}
}}
```


host	LDAP URL (ref RFC4516 > RFC2255) (in quotes), required if LDAP is enabled.
port	Port for protocol communication
mode	Determines default compatibility among the different LDAP types, options are “openLdap or activeDirectory”
securityType	Encryption to be used in connecting to LDAP server, options are “ssl” and “starttls”
bindDn	Distinguished Name (in quotes) (ref RFC4514 > RFC2253), used to bind to the directory server, blank string implies anonymous bind
password	Password (in quotes) used to bind to the directory server
baseDn	Distinguished Name (in quotes) (ref RFC4514 > RFC2253) to use for the search base
userFilter	LDAP Search Filter (in quotes) (ref RFC4515 > RFC2254), objectClass equivalent to posixAccount (ref RFC2307)
userId	Equivalent to attribute "uid" (in quotes) ref (RFC2307)
userIdNum	Equivalent to attribute "uidNumber" (in quotes) (ref RFC2307)
groupFilter	LDAP Search Filter (in quotes) (ref RFC4515 > RFC2254), objectClass equivalent to posixGroup (RFC2307)
groupId	Equivalent to attribute "gidNumber" (ref RFC2307) (in quotes)
groupMemberUid	Equivalent to attribute "memberUid" (ref RFC2307) (in quotes)
enabledGroup	User (in quotes) in this group will have the "enabled" privilege
controlGroup	User (in quotes) in this group will have the "control" privilege
adminGroup	User (in quotes) in this group will have the "admin" privilege

Proprietary and Confidential ©2024 Vertiv Group Corp.

```
{"conf":{
"remoteAuth": {
"mode": "tacacs",
"tacacs": {
"authenticationServer1": "10.20.30.21",
"authenticationServer2": "10.20.30.70",
"accountingServer1": "10.20.30.21",
"accountingServer2": "10.20.30.70",
"sharedSecret": "secret",
"service": "raccess",
"adminAttribute": "admin=true",
"controlAttribute": "control=true",
"enabledAttribute": "enabled=true"}}
}}
```

authenticationServer1	Primary authentication/authorization server (in quotes)
authenticationServer2	Alternate authentication/authorization server (in quotes)
accountingServer1	Primary accounting server (in quotes)
accountingServer2	Alternate accounting server (in quotes)
sharedSecret	Secret (in quotes) shared by client and server (null deletes secret)
service	Value for the service field in TACACS requests. Options are "ppp" and "raccess"
adminAttribute	User (in quotes) with this Attribute-Value Pair will have "admin" privilege
controlAttribute	User (in quotes) with this Attribute-Value Pair will have "control" privilege
enabledAttribute	User (in quotes) with this Attribute-Value Pair will have "enabled" privilege

Radius

```
{"conf":{
"remoteAuth": {
"mode": "radius",
"radius": {
"authenticationServer1": "",
"authenticationServer2": "",
"accountingServer1": "",
"accountingServer2": "",
"sharedSecret": "Secret",
"groupAttribute": "filter-id",
"adminGroup": "admin",
"controlGroup": "control",
"enabledGroup": "enabled"}}
}}
```

authenticationServer1	Primary authentication server (in quotes)
authenticationServer2	Alternate authentication server (in quotes)
accountingServer1	Primary accounting server (in quotes)
accountingServer2	Alternate accounting server (in quotes)
sharedSecret	Secret shared by client and server in quotes)
groupAttribute	Identifies the AVP that tells which access group the user belongs to, valid values are "filter-id" and "management-privilege-level".
adminGroup	User (in quotes) that belongs to this group has "admin" privilege
controlGroup	User (in quotes) that belongs to this group has "control" privilege
enabledGroup	User (in quotes) that belongs to this group will have "enabled" privilege

Network Hostname and IP Addresses


```
{"conf":{
"system": {
"hostname": "rPDUhostname",
"ip6Enabled": true},
"network": {
"ethernet": {
"label": "Bridge 0",
"enabled": true,
"dhcpOn": false,
"address": {
"0": {"address": "192.168.123.123","prefix": 24},
"1": {"address": "10.20.30.43","prefix": 24}}}}
}}
```


Hostname	Name (in quotes) to identify the unit in a network
ip6Enabled	Options are true or false to enable or disable IPV6 support
label	Bridge label (in quotes)
enabled	Options are true or false to enable or disable the network bridge
dhcpOn	Options are true or false to enable or disable DHCP
address	IP address (in quotes) of the interface
prefix	Prefix of the interface IP address

Network Ports


```
{"conf":{
"network": {
"port0": {
"label": "Port 0",
```


Proprietary and Confidential ©2024 Vertiv Group Corp.

```
"enabled": true,
"stp": {"cost": 0}},
"port1": {
"label": "Port 1",
"enabled": true,
"stp": {"cost": 0}}}
}}
```

label	Port label (in quotes)
enabled	Options are true or false to determine whether the port is enabled
cost	Spanning tree cost for this port

Network Routes

```
{"conf":{
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
}}
```

gateway	Gateway address (in quotes) for the route
prefixDestination	Network prefix, 0 for default gateway
destination	Destination network address (in quotes), “0.0.0.0” for default network

Network DNS

```
{"conf":{
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
}}
```

address	The DNS server address (in quotes). Second occurrence is for the alternate DNS server.

Network RSTP

```
{"conf":{
"network": {
```

```
"ethernet": {
"stp": {
"enabled": false,
"mode": "rstp",
"bridgePriority": 24576,
"helloTime": 2,
"maxAge": 40,
"maxHops": 40,
"forwardDelay": 21}}}
}}
```

enabled	Options are true or false, determines whether spanning tree protocol is enabled
mode	Options are "stp" or "rstp", RSTP mode supports falling back to STP when necessary
bridgePriority	This interface's spanning tree bridge priority
helloTime	The interval in seconds between periodic transmissions of configuration message
maxAge	The maximum age of the information transmitted by this interface, when it serves as the root bridge. Used when "mode" is set to "stp". Should be at least 2 * (helloTime + 1)
maxHops	The maximum number of bridge traversals of the information transmitted by this interface when it serves as the root bridge, used when "mode" is set to "rstp"
forwardDelay	The delay used by bridges to transition the root bridge and designated ports into forwarding mode, should be at least (maxAge / 2) + 1

Web Server

```
{"conf":{
"http": {
"httpEnabled": true,
"httpPort": 80,
"httpsPort": 443}
}}
```

httpEnabled	Options are true or false to allow unencrypted communications
httpPort	Port number for HTTP communication
httpsPort	Port number for HTTPS communication

Reports

```
{"conf":{
"report": {
"0": {
"start": "00:00",
"days": "MTWTFSS",
"targets": ["1","2"],
```


Proprietary and Confidential ©2024 Vertiv Group Corp.

```
"interval": 1},
"1": {
"start": "00:00",
"days": "MT-----",
"targets": ["1"],
"interval": 1}}
}}
```

start	Time of day from which interval is applied. Format is “(00-23):(00-59)” configurable in 15 minute increments
days	First letter of selected days (in quotes) in order Monday - Sunday. A '-' is used to represent unselected days targets
	List of keys referencing email targets (in quotes)
interval	Number of hours between reports, can be 1, 2, 3, 4, 6, 8, 12, and 24

Display

```
{"conf":{
"display": {
"gmsd": {
"mode": "currentAndTotalPower",
"inverted": false,
"vlc": {"enabled": false}}}
}}
```

mode	Selects a set of data to present on the display, options are “current”, “totalPower”, and “currentAndTotalPower”
inverted	Options are true or false to describe the current orientation of the display
enabled	Options are true or false to determine rPDU VLC display mode

Time

```
{"conf":{
"time": {
"mode": "ntp",
"datetime": "2021-03-09 12:05:36",
"zone": "UTC",
"ntpServer1": "0.pool.ntp.org",
"ntpServer2": "1.pool.ntp.org"}
}}
```

mode	Mode, valid options are "ntp" and "manual"
datetime	Date and time, format is "YYYY-MM-DD HH:MM:SS" with hours ranging from 0-23 (This field is displayed in local time), must only be used with mode=”manual”
Zone	This must be a valid name (in quotes) from the tz database
ntpServer1	Primary NTP server address (in quotes), must only be used with mode=”ntp”
ntpServer2	Backup NTP server address (in quotes) , must only be used with mode=”ntp”

SSH

```
{"conf":{
"ssh": {
"enabled": true,
"port": 22}
}}
```

enabled	Options are true or false to enable or disable SSH
port	Port number for SSH communication

USB

```
{"conf":{
"usb": {"enabled": true}
}}
```

enabled	Options are true of false, enables or disabled the USB port

Serial Port

```
{"conf":{
"serial": {
"baudRate": 115200,
"dataBits": 8,
"enabled": true,
"parity": "none",
"stopBits": 1}
}}
```

baudRate	Baud rate, options are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200
dataBits	Number of bits of data in one frame, options 7 and 8
enabled	Options are true of false, enables or disabled the serial CLI on a device
parity	Parity bit type used in the frame, options “none”, “even” and “odd”
stopBits	Number of stop bits used to terminate each frame, options 1 and 2

Proprietary and Confidential ©2024 Vertiv Group Corp.

Email

```
{"conf":{
"email": {
"server": "Example-server",
"port": 25,
"sender": "From email address",
"username": "username",
"password": "password",
"target": {
"0": {"name": "email1@domain.com"},
"1": {"name": "email2@domain.com"}}}
}}
```

Server	SMTP sever address (in quotes)
port	SMTP port number
sender	Senders email address (in quotes)
username	SMTP user name (in quotes)
password	SMTP password (in quotes)
name	Destination email address (in quotes)

SNMP v1 or v2c

```
{"conf":{
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.10",
"trapVersion": "1"},
"1": {
"port": 162,
"name": "10.20.30.11",
"trapVersion": "1"},
"2": {
"port": 162,
"name": "10.20.30.12",
"trapVersion": "2c"}}}
}}
```

v1v2cEnabled	Options are true or false, enables or disables SNMP version 1 and 2c
port	Port number for SNMP communication
readCommunity	Read community name (in quotes), must be different from writeCommunity
writeCommunity	Write community name (in quotes), must be different from readCommunity
trapCommunity	Trap community name (in quotes)
port	Port number for SNMP traps
name	Address (in quotes) for the SNMP trap destination
trapVersion	SNMP trap version, "1" or "2c"

SNMP v3


```
{"conf":{
"snmp": {
"v3Enabled": true,
"port": 161,
"user": {
"0": {
"privPassword": "password",
"type": "read",
"username": "name",
"privType": "aes",
"authPassword": "password",
"authType": "sha1"},
"1": {
"privPassword": "password",
"type": "write",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"},
"2": {
"privPassword": "password",
"type": "trap",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"}}}
}}
```


Proprietary and Confidential ©2024 Vertiv Group Corp.

v3Enabled	Options are true or false, enable or disable SNMP version 1 and 2c
port	Port number for SNMP communication
type	Permission type, possible values "read", "write" or "trap"
username	SNMPv3 user name (in quotes)
privPassword	Privacy password (in quotes)
privType	Privacy encryption type, values "aes", “des” or "none"
authPassword	Authentication password (in quotes)
authType	Authentication type, values "sha1", “md5” or "none"

Syslog

```
{"conf":{
"syslog": {
"enabled": true,
"target": "10.20.30.40",
"port": 514}
}}
```

enabled	Options are true or false, enable the transmission of syslog messages to a remote destination
target	Address (in quotes) of the remote destination for syslog messages
port	Destination port number for messages

Admin

```
{"conf":{
"contact": {
"description": " Geist GU PDU ",
"location": "Example Location",
"contactName": "Example Contact",
"contactEmail": "email@example.com",
"contactPhone": "123 456 789"},
"system": {"label": "System Label"}
}}
```

description	Unit description (in quotes)
location	Unit location (in quotes)
contactName	Unit contact name (in quotes)
contactEmail	Unit contact email (in quotes)
contactPhone	Unit contact phone number (in quotes)
label	Unit system label (in quotes)

Locale

```
{"conf":{
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

defaultLang	Language, valid options are "de", "en", "es", "fr", "ja", "ko", "pt", "zh"
units	Units, valid options are "metric" and "imperial"

Data Logging Interval

```
{"conf":{
"datalog": {"interval": 15}
}}
```

interval	The interval in minutes for data logging

Aggregation

```
{"conf":{
"oneview": {
"enabled": true,
"username": "x",
"password": "pass"}
}}
```

enabled	Options are true or false, determines whether aggregation is enabled
username	User name (in quotes) to be set array devices
password	Password (in quotes) to set for array devices (null deletes password)

Example 1

File to configure a hostname, IP address, gateway, SNMP v1 community names and locale:

```
{"conf":{
"system": {
"hostname": "hostname1"},
"network": {
"ethernet": {
"dhcpOn": false,
"address": {
"0": {"address": "10.20.30.40","prefix": 24}}}}
```


Proprietary and Confidential ©2024 Vertiv Group Corp.

```
,
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
,
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
,
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.60",
"trapVersion": "1"}}}
,
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

Example 2

File to configure an admin user, disable HTTP, and configure a NTP server:

```
{ "auth": {
"username": {
"password": "userpw",
"enabled": true,
"control": false,
"admin": false,
"language": "en"}
},
"conf":{
"http": {
"httpEnabled": false}
,
"time": {
"mode": "ntp",
"zone": "UTC",
"ntpServer1": "0.pool.ntp.org", "ntpServer2": "1.pool.ntp.org"} }}
```

Sensor Settings and Alarms


```
{"dev": {
    "0000000000000000": {
        "label": "PDU 22A",
        "type": "i03",
        "conf": {"outletControlEnabled": true},
        "outlet": {
            "0": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.25,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 1"
            },
            "1": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.50,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 2"
            }
        },
        "entity": {
            "total0": {"label": "Total"},
            "breaker0": {"label": "Circuit 1"},
            "breaker1": {"label": "Circuit 2"},
            "phase0": {"label": "Phase A"},
            "phase1": {"label": "Phase B"},
            "phase2": {"label": "Phase C"},
            "line3": {"label": "Neutral Line"}
        }
    }
},
"alarm": {
    "action": {
        "0": {
            "target": "trap0",
            "delay": 0,
            "repeat": 0
        },
        "1": {
            "target": "email0",
            "delay": 0,
            "repeat": 0
        }
   },
    "trigger": {
        "0": {
```


Proprietary and Confidential ©2024 Vertiv Group Corp.

```
            "path": "0000000000000000/entity/phase0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 222.0,
            "tripDelay": 0,
            "clearDelay": 1,
            "latching": false,
            "selectedActions": ["0","1"]
        },
        "1": {
            "path": "0000000000000000/outlet/0/measurement/0",
            "severity": "alarm",
            "type": "low",
            "threshold": 55.0,
            "tripDelay": 2,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "2": {
            "path": "0000000000000000/entity/breaker0/measurement/4",
            "severity": "alarm",
            "type": "high",
            "threshold": 12.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "3": {
            "path": "0000000000000000/entity/total0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 7200.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        }
    }
}}
```

0000000000000000	The device-id (found on the sensors>overview page) of the rPDU to be configured. If this device-id does not match any of the selected devices being provisioned, all selected devices will be provisioned. Setting device-id to 0000000000000000 ensures all selected devices are configured.
label	The rPDU label (shown on the sensors>overview page)
type	For setting alarms on the internal PDU measurements, the “type” must match the IMD being used on the PDU, so it must be “i03” for PDUs using any IMD-03x or IMD-3x, and “i05” for PDUs using the IMD-5M. For setting alarms on external sensors, “type” must be the external sensor’s type. Valid values are “remotetemp”, “afht3”, “thd”, “t3hd”, “a2d”, “snt”, “snh”, “snd”. If omitted, prevents any selected rPDUs being configured when the device-id does not match that of any rPDU.
outletControlEnabled	Applies to outlet switched rPDUs only and determines whether it is possible to control outlets on an outlet switched rPDU. The value true allows outlets to be controlled, the value false prevents outlets from being controlled.
outlet	The outlet section applies to outlet switched rPDUs only and defines settings for each rPDU outlet. Note that outlet numbering starts with 0 (rPDU outlet number 1). Individual outlets (or the entire Outlet section) can be omitted if these settings do not require change.
poaAction	Defines the state the outlet will start when powered on ("on", "off" or "last").
rebootHoldDelay	Time, in seconds, the unit waits after switching the outlet off, before switching an outlet back on during a reboot. Can be any whole number between 0 and 14400.
rebootDelay	Time, in seconds, the unit waits before rebooting an outlet. Can be any whole number between 0 and 14400.
poaDelay	Time, in seconds, the unit waits after being powered on before powering on the outlet. Can be any whole number between 0 and 14400.
onDelay	Time, in seconds, the unit waits before switching an outlet on. Can be any whole number between 0 and 14400.
mode	Should have the value "manual" for user-controlled outlets.
offDelay	Time, in seconds, the unit waits before switching an outlet off. Can be any whole number between 0 and 14400.
label	The outlet label.
entity	The entity section is used to label non-outlet measurements on the sensors>overview page.
total0 label	Label for the rPDU total on the sensors>overview page
breaker0 label	Label for the first circuit (if present). Further circuits if present can be labelled using breaker1, breaker2 etc.

Proprietary and Confidential ©2024 Vertiv Group Corp.

phase0 label	Label for the first phase. Further phases if present can be labelled using phase1 and phase2.
line3 label	Label for the neutral line.
alarm	The alarm section defines the methods that can be used to send alarms. Each method is numbered starting from 0 defines: For SNMP trap alarm delivery the target can have the values "trap0", "trap1" etc. which refers to the first, second etc. SNMP traps defined on the System>SNMP page.
target	For email alarm delivery the target can have the values "email0", "email1" etc. which refers to the first, second etc. target email defined on the System>Email page. Note that the target must not specifies SNMP traps or email targets that have not been configured.
delay	Determines how long this event must remain tripped before this action's firstvertical notification is sent.
repeat	Determines whether multiple notifications will be sent for this event action.
trigger	This section defines which alarms have been configured, starting with the first alarm which is numbered 0.
Path	Defines the measurement to be alarmed upon. The format of this field is: "0000000000000000/entity/phase0/measurement/0" defines alarms for rPDU inlet phase measurements, where phase0 refers to the first rPDU input phase, phase1 refers to the second phase (if present) etc. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below: 0: Voltage 4: Current 8: Real power 9: Apparent power 10: Power Factor 11: Energy 14: Current crest factor "0000000000000000/outlet/0/measurement/0" defines outlet alarms for rPDUs with outlet monitoring where the number immediately following outlet specifies the outlet number (starting at zero). The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below: 0: Voltage

	4: Current 8: Real power 9: Apparent power 10: Power Factor 11: Energy 12: Balance 14: Current crest factor "0000000000000000/entity/total0/measurement/0" defines alarms for rPDU phase total inlet measurements. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below: 0: Real power 1: Apparent power 2: Power Factor 3: Energy "0000000000000000/entity/breaker0/measurement/4" defines alarms for rPDU circuit alarms where the first circuit is indicated by breaker0, second by breaker1 etc. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below: 4: Current "0000000000000000/entity/line3/measurement/4" defines alarms for rPDU neutral current alarms. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below: 0: Current
severity	Can be "warning" or "alarm" describing the severity of the generated alarm.
type	Can be "high" or "low" which defines whether this is a high or low threshold.
threshold	Threshold value which can be any number between -999.0 through 999.0. Neutral line current can be specified with up to two decimal places.
tripDelay	The measurement must exceed the threshold for this many seconds before the event will be tripped, can be any whole number between 0 and 14400.

Proprietary and Confidential ©2024 Vertiv Group Corp.

clearDelay	The measurement must return to normal for this many seconds before the event will clear and reset. can be any whole number between 0 and 14400.
latching	Can be true or false. If true, the event and its associated actions remain active until the event is acknowledged, even if the measurement subsequently returns to normal.
selectedActions	Defines which actions defined above to use to send the alarm. Such as ["0","1"] defines actions 0 and 1 which are defined as actions using trap0 and email0 in the example above.

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix G: API / CLI Error Codes

G.1 Success

Code	Explanation
Success	Operation has succeeded

Authentication Errors

Code	Explanation
No Admin user configured	At least one Admin user must be configured on the system
Not Authorized	The current user is not authorized
Not Authorized: Session expired	The token used is no longer valid
Not Authorized: Not enough permissions	The current user does not have enough permissions to perform the operation
Invalid credential combination	Both username/password and token were provided or only one of username or password was provided
Must have at least one admin user	At least one Admin user must be configured on the system

JSON Format Errors

Code	Explanation
Malformed JSON	Received JSON is not valid or corrupt
Missing field	An expected field was not found in the JSON structure
Duplicate fields	The same field was set multiple times, such as in the HTTP body and query string

Path Errors

Code	Explanation
Invalid path	Supplied path does not fulfill system requirements
Path not found	Supplied path was not found
Identifier not found	One of the fields in the received JSON structure does not exist
Field not applicable	A field in the JSON structure exists but should not have been sent

Data Validation Errors

Code	Explanation
Invalid input	An input field is invalid but does not fit in other data validation categories
Input too long	An input field exceeds the maximum allowed length
Invalid characters	An input field contains invalid characters for the field

Code	Explanation
Invalid serial	An input field is an invalid serial number
Invalid Boolean	An input field is an invalid Boolean value
Out of range	An input field falls outside the valid range for the field
Invalid integer	An input field is not an integer when one is expected
Invalid number	An input field is not a number when one is expected
Invalid URL	An input field is not a valid URL when one is expected
Invalid IP	An input field is not a valid IP address when one is expected
Paths not allowed	An input field contains a path when one is not expected
Invalid username	An input field is an unsupported user name
Invalid email address	An input field is not a valid email address when one is expected
Invalid option	An input field contains an invalid option selection
Invalid datetime	An input field is not a valid date or time when one is expected
Out of bounds	An input field is out of the allowed bounds for the field
Invalid week	An input field represents an invalid days of the week selection
Duplicate entry	An input field would create a duplicate when one is not allowed
Invalid Route	A network route was misconfigured

Other Errors

Code	Explanation
Unknown error	A system error occurred for which no other error code applies
Command not allowed	The received command is not allowed at the specified path
System busy	The action attempted cannot be currently executed and should be retried

Data Consistency Errors

Code	Explanation
Inconsistent state	The command will leave the system in an inconsistent state, so it is rejected
Syslog enabled requires target	Enabling remote syslog requires a target host be specified
NTP mode requires servers	Enabling NTP requires servers to query
Start time must come before end time	Time was received for which the end came before the start
Invalid SNMPv3 auth/priv combination	SNMPv3 privacy cannot be used without authentication
Port not available	There was an attempt to set a port number to one already in use
Vertiv Intelligence Director missing credentials	Enabling Vertiv Intelligence Director requires that a username and password be set
Time not settable	Setting datetime requires manual time mode

Proprietary and Confidential ©2024 Vertiv Group Corp.

Upload Errors

Code	Explanation
Invalid firmware package	The package is formatted incorrectly or corrupt
Invalid file key	The package specifies a wrong OEM key and cannot be used with this unit
Invalid version	The version is too old or otherwise unsupported
Invalid product	The package is meant for a different hardware architecture
Invalid certificate file	The SSL certificate provided could not be parsed
Invalid certificate password	The password did not work with the SSL certificate provided

This page intentionally left blank

Proprietary and Confidential ©2024 Vertiv Group Corp.

Appendix H: An Example of Configuring LDAP for Active Directory Credentials

H.1 Overview

Active Directory integration with the Vertiv-branded and Geist-branded Interchangeable Monitoring Device (IMD) allows users to authenticate and authorize at the IMD's web and CLI interface using their enterprise Active Directory credentials. The user will also be authorized into one of three IMD roles based upon an Active Directorysecurity group the user is a member of. These roles are:

- Admin: Full configuration rights including Control role permissions.
- Control: Ability to control outlet state if applicable, change device names and alarm/event settings.
- Enabled: Read-only of the configuration settings and no outlet control rights.

H.2 General Requirements and Notes

- IMD v5.3.3 or new firmware can be used for this procedure.
- Examples are represented in green.

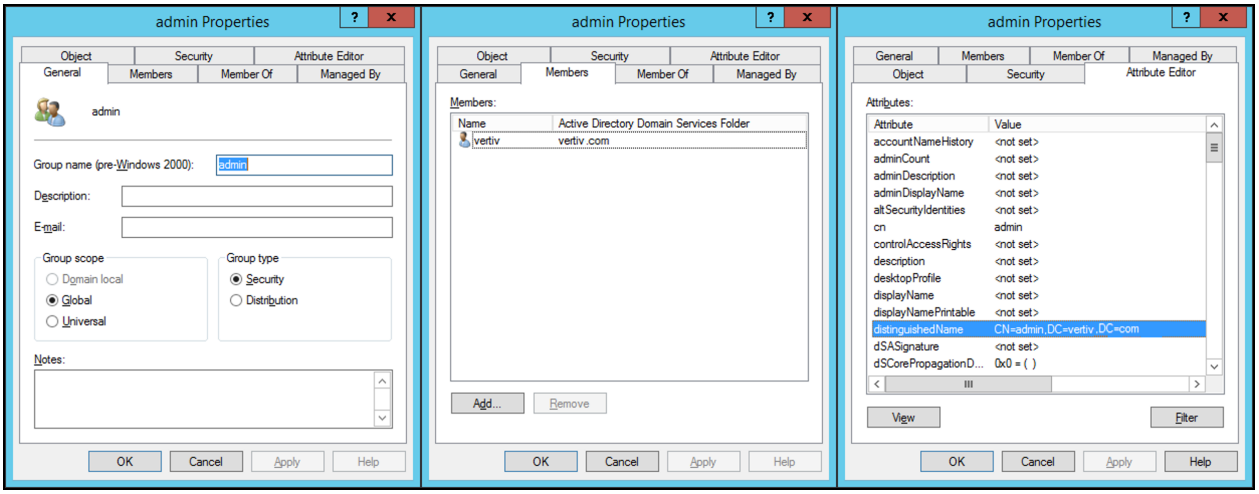
H.3 Active Directory Configuration Procedure

- Create or utilize an existing AD bind account for the IMD. This account will be used by the IMD to search the AD domain and authenticate users. The password for this account should be set to never expire.
- Create one or more AD security groups to represent the Admin, Control and Enabled IMD roles.
- Make the AD user a member of the applicable security group.
    - AD account "vertiv" has been assigned a member of security group "admin" in example shown below. As a result, the "vertiv" AD user account will assume the IMD Admin role upon login.

NOTE: The naming of the security group is at your discretion. The security group name and DN should match what is defined in the IMD's LDAP "Group" section.

NOTE: An AD user belonging to more than one of these IMD role mapped security groups will inherit the highest role privileges.

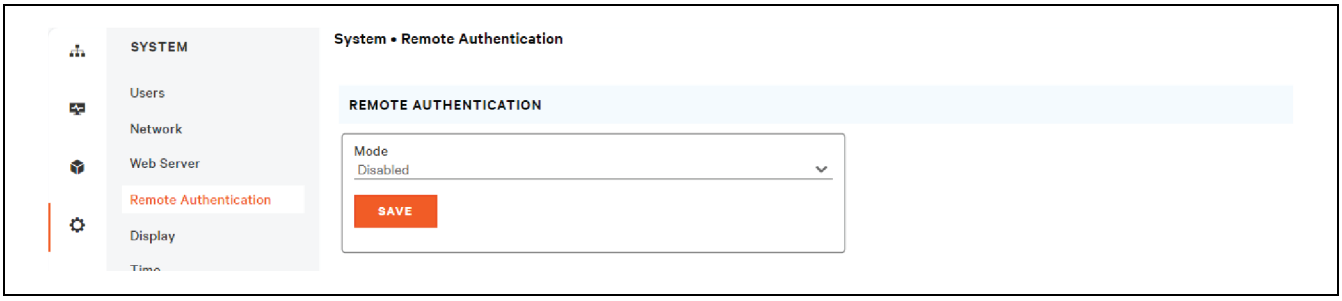
Figure H.1 Admin Properties Settings



H.4 IMD Configuration Procedure (Web Interface)

- Open a web browser to the IP or DNS name of the IMD and login as the local admin account.
- Navigate to *System >Remote Authentication.*
- Set Remote Authentication Mode to LDAP and save.

Figure H.2 Remote Authentication



- Refer to the illustration below for descriptions of the LDAP section settings.

Proprietary and Confidential ©2024 Vertiv Group Corp.

Figure H.3 LDAP Setting

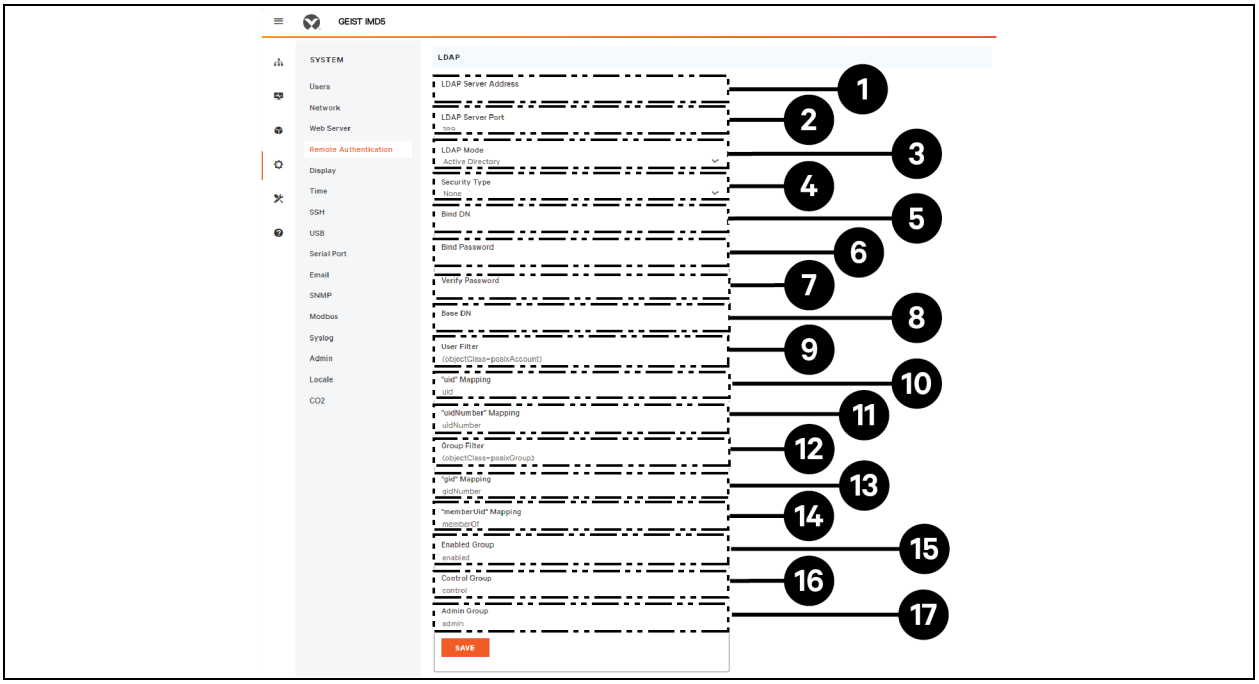


Table H.1 LDAP Setting

Item	Description
1	Active Directory Server's IP Address
2	Active Directory TCP Port[2] 389 - Non SSL 636 - SSL
3	LADAP Mode OpenLDAP - Active Directory
4	Active Directory Security[2] None - SSL - StartTLS
5	AD Account Used to Bind to AD Server Must be in full DN path notation CN=adbindacct,CN=Users,DC=vertiv,DC=com Account password should not expire
6	Set AD Bind Account Password
7	Verify Password
8	Base Domain Path to Search AD Users[1] Must be in full DN path notation DC=vertiv, DC=com
9	AD User ObjectClass Attribute Filter (objectClass=user)

Table H.1 LDAP Setting (continued)

Item	Description
10	AD User Account Name Filter samaccountname
11	"uidNumber" Mapping uidNumber
12	AD Group ObjectClass Attribute Filter (objectClass=group)
13	"gid" Mapping gidNumber
14	Required Setting memberOf
15	AD Security Group Map to Enabled Role Must be in full DN path notation CN=enabled, DC=vertiv, DC=com
16	AD Security Group Map to Control Role Must be in full DN path notation CN=control, DC=vertiv, DC=com
17	AD Security Group Map to Admin Role Must be in full DN path notation CN=admin, DC=vertiv, DC=com
NOTE: [1]Best practice is to reduce the scope of AD domain traversal to search for authenticated users. Try to avoid just specifying the base domain when there is a large and nested AD schema. • Ideal: OU=Enabled Users, OU=User Accounts, DC=vertiv, DC=com • Not Ideal: DC=vertiv, DC=com	
NOTE: [2]StartTLS uses TCP port 389. It initially establishes the session unencrypted but will encrypt the session from that point forward ifthe LDAP_START_TLS_OID request is accepted by the Active Directory server.	

Proprietary and Confidential ©2024 Vertiv Group Corp.

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

©2024 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.

SL-71211_REVA_03-24