



# Geist™ Rack Transfer Switch

**Installer/User Guide**

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages result from use of this information or for any errors or omissions.

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

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

### **Technical Support Site**

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit <https://www.vertiv.com/en-us/support/> for additional assistance.

# TABLE OF CONTENTS

<b>1 Important Safety Instructions</b> .....	<b>1</b>
<b>2 Overview</b> .....	<b>3</b>
2.1 Environmental .....	4
2.2 Electrical .....	4
2.3 Networking .....	5
2.3.1 Ethernet .....	5
2.3.2 Protocols .....	5
2.3.3 User interfaces .....	5
<b>3 Installation</b> .....	<b>7</b>
3.1 Mounting .....	8
3.1.1 4-Post Rack Mounting .....	8
3.1.2 2-Post Rack Mounting .....	8
3.2 Power Connection .....	9
3.2.1 P-Lock Operation .....	9
3.2.2 U-Lock Operation .....	10
<b>4 Setup</b> .....	<b>11</b>
4.1 Local HMI .....	11
4.2 Interchangeable Monitoring Device .....	13
4.2.1 Basic .....	13
4.2.2 Metered .....	14
4.2.3 Enhanced Monitored with RS-232 (IMD-03E-S) .....	14
4.2.4 Enhanced Switched Monitored with RS-232 .....	16
4.2.5 Rapid Spanning Tree Protocol (RSTP) .....	18
4.3 Network Setup .....	19
4.4 Web Interface .....	23
4.4.1 Home Page .....	23
4.5 Sensors Tab .....	25
4.5.1 Overview .....	25
4.5.2 Alarms and Warnings .....	28
4.5.3 Logging .....	30
4.6 System Tab .....	31
4.6.1 Users Page .....	31
4.6.2 Network .....	35
4.6.3 Web Server .....	38
4.6.4 Reports .....	39
4.6.5 Remote Authentication .....	40
4.6.6 Display .....	44

- 4.6.7 Time ..... 44
- 4.6.8 SSH ..... 45
- 4.6.9 USB ..... 45
- 4.6.10 Serial Port ..... 45
- 4.6.11 Email ..... 46
- 4.6.12 SNMP ..... 47
- 4.6.13 Modbus ..... 48
- 4.6.14 SYSLOG ..... 48
- 4.6.15 Admin ..... 49
- 4.6.16 Locale ..... 49
- 4.6.17 Utilities ..... 49
- 4.7 Provisioner Tab ..... 52
  - 4.7.1 Discovery ..... 53
  - 4.7.2 File Management ..... 53
- 4.8 Help Tab ..... 54
- 5 Vertiv™ Intelligence Director ..... 55**
- 5.1 Aggregation ..... 55
- 5.2 Array Manager ..... 55
- 5.3 Network Configuration ..... 56
  - 5.3.1 Array Devices ..... 57
- 5.4 Views ..... 58
  - 5.4.1 Summary ..... 59
  - 5.4.2 Groups ..... 60
  - 5.4.3 List ..... 62
  - 5.4.4 Group Configuration ..... 63
- 5.5 Interfaces ..... 65
  - 5.5.1 Group SNMP Data ..... 66
  - 5.5.2 Tips and Troubleshooting ..... 66
- Appendices ..... 67**
- Appendix A: Technical Support ..... 67
- Appendix B: Visible Light Communication (VLC) ..... 69
- Appendix C: Vertiv Mobile App ..... 71
- Appendix D: Available Sensors ..... 79
- Appendix E: Outlet LEDs ..... 81
- Appendix F: IMD Display Codes ..... 83
- Appendix G: Provisioner - Format of the Configuration Settings File ..... 85
- Appendix H: Provisioner Error Codes ..... 103
- Appendix I: An Example of Configuring LDAP for Active Directory Credentials ..... 107

# 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:** Please visit <http://www.Vertiv.com/ComplianceRegulatoryInfo> for important safety information prior to installation.

All safety statements in VM1227 referencing the Vertiv rack equipment apply to the Geist™ RTS.

Some loads may pull high inrush current when switching power sources. Do not overload RTS to prevent relay failure and tripping branch circuit protection.

If the RTS is installed in a cabinet, the ambient temperature of the rack should be no greater than 60°C.

The RTS relies on the building installation for protection from over-current conditions. A certified overcurrent protection device is required in the building installation. The overcurrent protection device should be sized according to the RTS's nameplate ratings and local/national electrical codes.

The RTS supports single-phase AC power distribution from sources connected to AC Mains of TN-S power distribution systems that provides separate protective earth and neutral circuits, if applicable, with a direct electrical connection of the equipment to the earthed point of the power distribution system per IEC 60364-3.

## 2 Overview

The Vertiv™ Geist™ Rack Transfer Switch (RTS) is used in the data center to facilitate switching or transfer of the rack space power distribution infrastructure between two independent power sources so that uninterrupted operation of the connected IT equipment is maintained. The transfer may occur automatically when suboptimal power quality conditions are detected on the active source or by manual intervention when maintenance of a source is required.

Refer to the table below for a list of transfer conditions that cause the power source to switch off.

**Table 2.1 Power Source Switch Off Conditions**

Parameter	Description
Voltage Shape	A distortion or anomaly of sinusoidal, complete loss of phase, or disconnect.
Voltage Peak	A sudden 1/2 line cycle drop below 85% peak of steady-state sinusoidal.
Voltage RMS	A gradual change exceeding $\pm 10\%$ RMS of nominal value.
Frequency	Line frequency exceeding $\pm 3.75\text{Hz}$ of nominal value.

The following are the major features of the RTS:

- 1U and 2U product variants with Combination outlets C13/C19 or NEMA outlets.
- Accuracy Class 1.0 metering of input, circuits, and outlets, including voltage & current (rms), real power (W), apparent power (VA), energy (kW-hr), power factor, and crest factor.
- Hybrid switching topology with typical total transfer time of 4-8ms.
- Break-before-make action with redundant switches and fail-safe fused thermistor to mitigate current surge during transfer.
- Soft start, i.e., output voltage ramping, at cold start to mitigate inrush current.
- Hot-standby controller for zero-down time during firmware update and processor reset.
- Redundant internal power supplies for resiliency to single point of failure.
- Internal diagnostic mode determines real-time health of inactive switch circuitry.
- Local HMI with touch key support and one-line graphic to support the change of retransfer mode, change of preferred source, initiate manual transfer, and report system status.
- IMD supports advanced configuration, remote control, and presentation of metering and log data, and system status.

## 2.1 Environmental

The operational environmental limits pertaining to temperature, humidity and elevation are as defined in **Table 2.2** below, **Table 2.3** below, **Table 2.4** below.

**Table 2.2 Temperature Limits**

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

**Table 2.3 Humidity Limits**

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

**Table 2.4 Elevation Limits**

Description	Minimum	Maximum
Operating	0 m (0 ft)	3,050 m (10,000 ft)
Storage	0 m (0 ft)	15,240 m (50,000 ft)

## 2.2 Electrical

Electrical product characteristics and performance are defined in the following table. Also, please see the product nameplate for additional rating limits.

**Table 2.5 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
German Schuko	250VAC, 16A
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	230VAC, 16A
NEMA 5-15R	125 VAC, 12 A
NEMA 6-15R	250VAC, 12A
NEMA 5-20R	125 VAC, 16 A
NEMA 6-20R	250 VAC, 16 A
NEMA L5-30R	125 VAC, 24 A
NEMA L6-30R	250 VAC, 24 A

**Table 2.5 Receptacle Ratings (continued)**

Type	Ratings
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	250VAC, 13A

## 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 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.

### 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).

This page intentionally left blank

## 3 Installation

Using the information in [Mounting](#) on the next page, install your Vertiv™ Geist™ RTS.

To install your unit:

1. Using appropriate hardware, mount *RTS* to rack (see to [Mounting](#) on the next page for additional instructions).
2. Plug *RTS* into de-energized *branch circuit* receptacles.
3. Connect devices into RTS output receptacles. It is recommended that the devices are turned off until all devices are connected to RTS.
4. Turn on *branch circuit* for Source A to energize RTS.
  - The unit sounder will beep once at startup.
5. Turn on *branch circuit* for Source B.
  - The unit will beep twice during startup after it locks onto the first available source line frequency.
6. Power on *devices*.

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

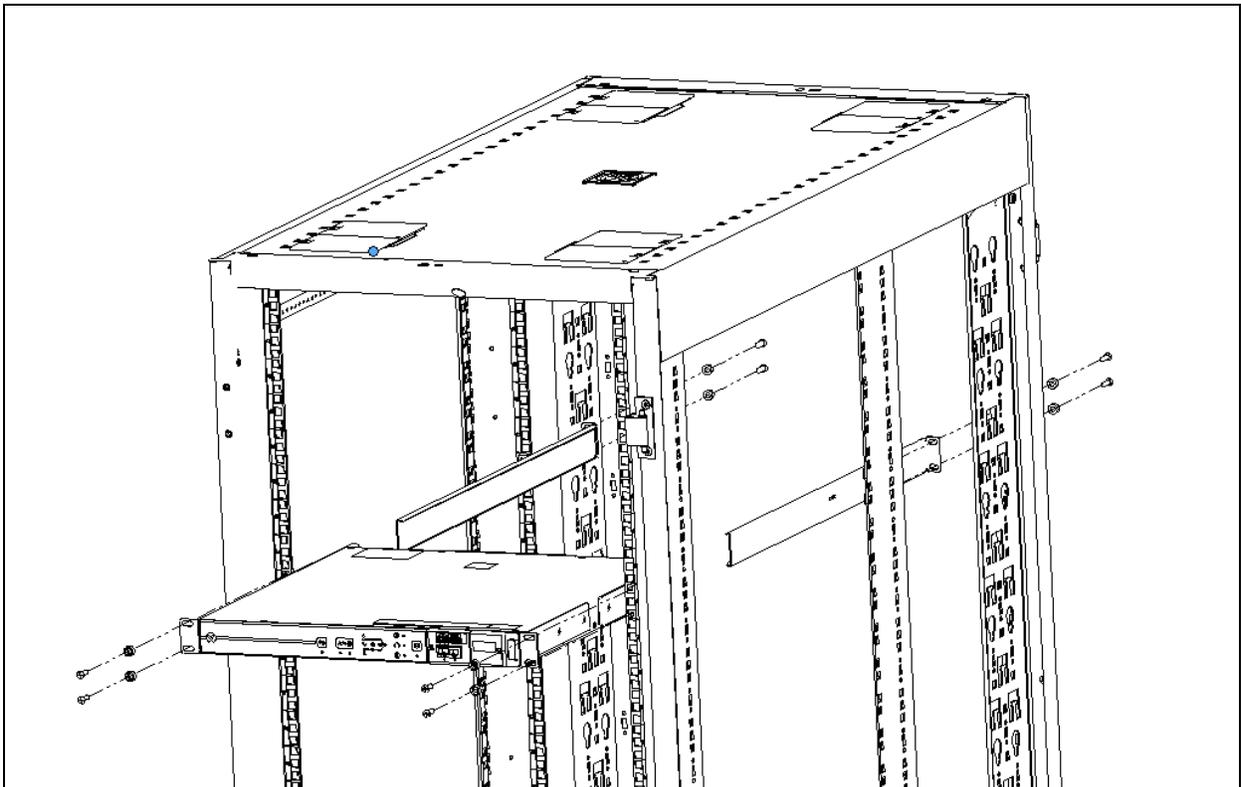
**NOTE: By factory default source A is designated as the preferred source and retransfer is enabled. On cold startup, if source B is connected and qualified first, power is enabled through source B. Once source A has been connected and qualified it will transfer power to source A.**

## 3.1 Mounting

### 3.1.1 4-Post Rack Mounting

1. Install the *mounting brackets* onto the RTS unit.
2. Install *sliding brackets* onto the rack.
3. Insert the *RTS unit* with brackets onto the sliding brackets. **Figure 3.1** below illustrates the installation of the RTS unit.

Figure 3.1 RTS Sliding Brackets



### 3.1.2 2-Post Rack Mounting

**NOTE:** Each mounting bracket can be used on the left or right side of the RTS unit. RTS unit can be mounted facing inward or outward from the 2-post rack.

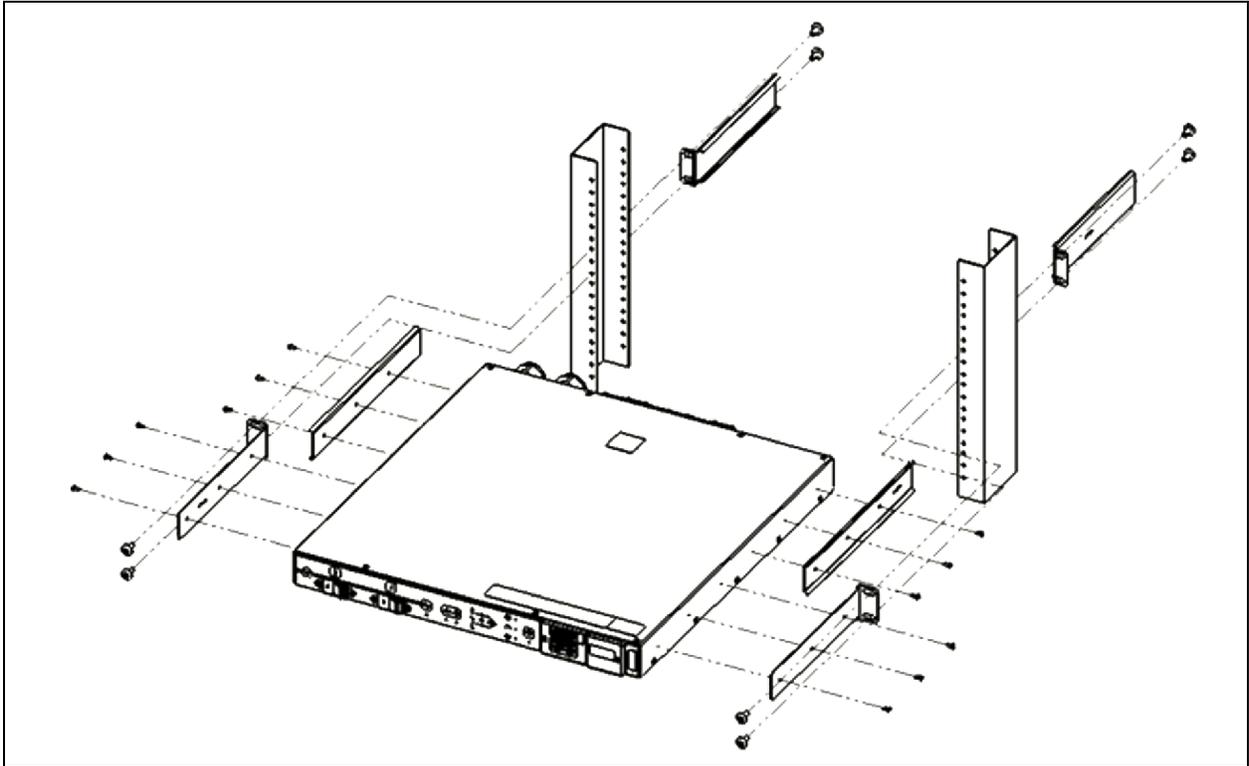
#### 1. Attaching the brackets to the RTS

- Align the U-bracket (without a 2-hole mounting fin) to the rear side of the RTS and secure the bracket to the RTS with two screws. Repeat for the other side of the RTS.
- Align the mounting bracket with 2-hole mounting fin to front side of the RTS and secure the bracket to the RTS with two screws. See orientation as shown in **Figure 3.2** on the facing page. Repeat for the other side of the RTS.
- Align the sliding bracket with 2-hole mounting fin from mounting kit to opposite side of the 2-post rack and secure the bracket to the rack with two screws (customer provided). Repeat for the other side of the rack.

## 2. Attaching the RTS to the 2-post rack

1. Insert the RTS with brackets onto the sliding brackets. **Figure 3.2** below illustrates the installation of the RTS unit.
2. Attach each side bracket to the rack with two screws (provided by the customer).

**Figure 3.2 RTS Sliding Brackets**



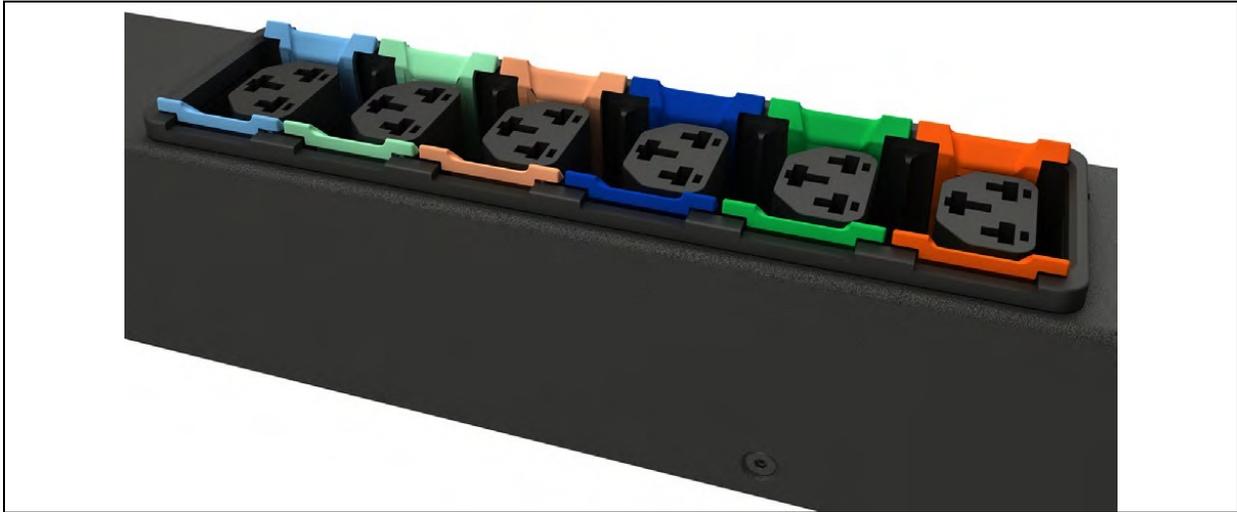
## 3.2 Power Connection

Plug the dual input power cords from the Vertiv™ Geist™ RTS into the appropriately rated and protected branch circuit receptacles.

### 3.2.1 P-Lock Operation

- Plug in the *devices* to be powered by the Geist™ RTS.
- 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 3.3 P-Lock Cord Retention Operation



### 3.2.2 U-Lock Operation

Plug in the devices to be powered by the Vertiv™ Geist™ RTS.

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

Figure 3.4 U-Lock Cord Retention Operation

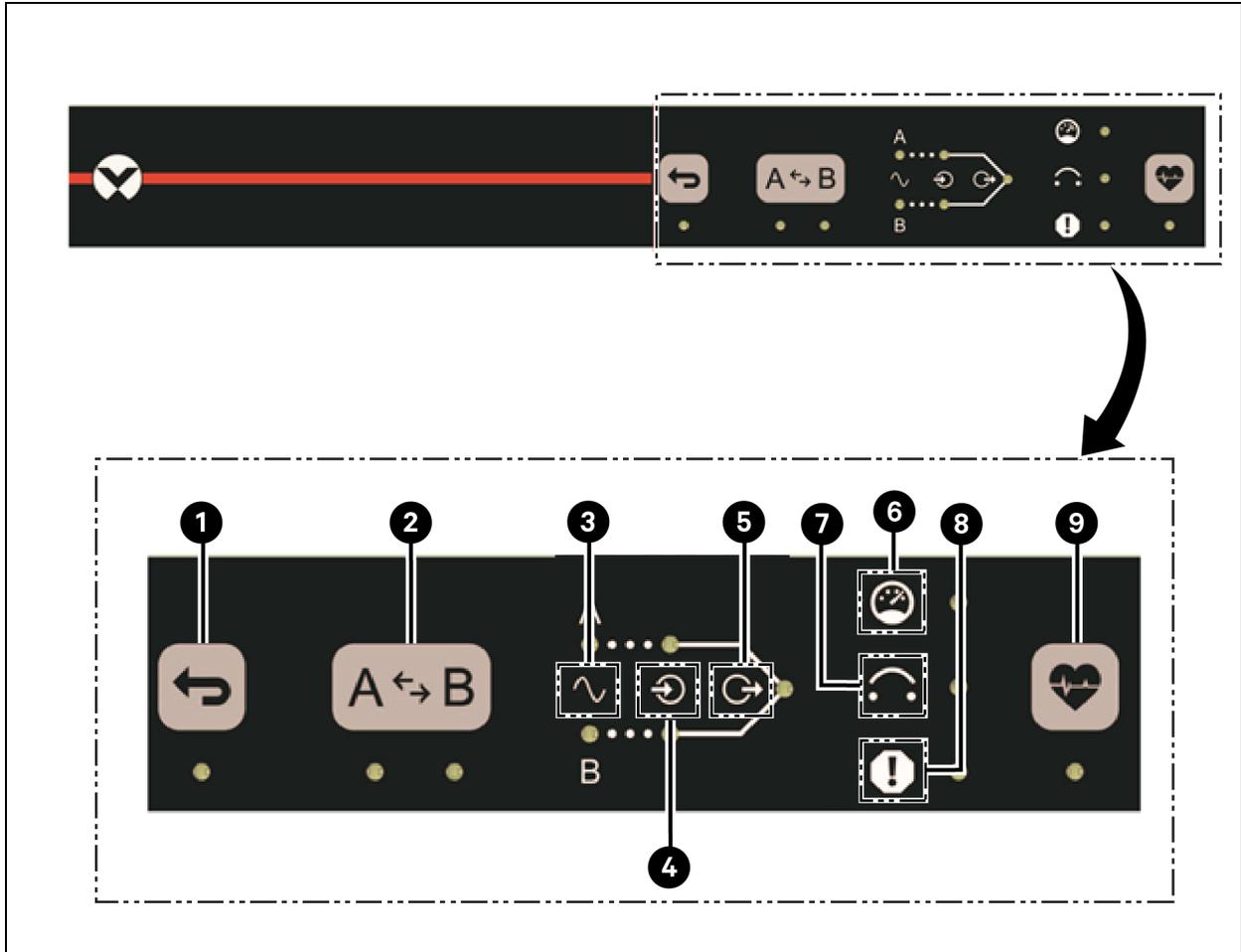


## 4 Setup

### 4.1 Local HMI

The Local Human Machine Interface (HMI) uses a touch key label to serve as the local means of control and convey operational state using its visual indicators. **Figure 4.1** below illustrates the layout of the HMI.

**Figure 4.1** Local HMI



Item	Description
1	Retransfer Enabled
2	Preferred Source
3	Source Qualified
4	Active Source
5	Active Output

Item	Description
6	Capacity Status
7	Over Current Protection Device (OCPD) Status
8	Internal Fault Status
9	Health Self-Test

The following elements' functionality are described in the context of **Figure 4.1** on the previous page.

## 1 - Retransfer Enabled

This key enables/disables the retransfer from the alternate source back to the preferred source. This key is inhibited if a lockout condition is configured by the IMD or if a Health Self-Test is pending. The LED indicates the enabled/disabled state of the retransfer mode. The LED is lit continuously when enabled and turned off when disabled. The LED flashes rapidly three (3) times and the sounder will beep rapidly three (3) times if the key is inhibited.

If retransfer is enabled prior to an automatic transfer from preferred to alternate source, then an automatic transfer back to the preferred source will occur after the retransfer delay time has expired and the preferred source has been qualified.

If retransfer is disabled prior to an automatic transfer from preferred to alternate source, then retransfer back to the preferred source shall be deferred until either the preferred source has been qualified and retransfer is enabled or the preferred source selection is toggled once.

**NOTE: The retransfer delay time starts to countdown from the moment of transfer.**

## 2 - Preferred Source

This key will toggle the selection of the preferred source.

If operating conditions allows:

- The RTS unit shall normally operate from the preferred source whenever both sources are qualified.
- This key will force a transfer to the newly selected preferred source.

**NOTE: If one or both sources are not qualified, changing the preferred source is allowed but does not elicit a transfer. This key may be inhibited if a lockout condition like a Health Self-Test is pending.**

The LED will indicate "A" or "B" source is preferred. The LED is lit continuously for the preferred source and turned off for the alternate source. The LED flashes rapidly three (3) times and the sounder will beep rapidly three (3) times if the key is inhibited.

## 3 - Source Qualified

The LED indicates that the source power is available and qualified, i.e. its electrical parameters are within acceptable limits to power ITE per section 6.2. The LED will be turned off while the source is unavailable or undetected. The LED flashes while the source is available, and its power quality determination is pending.

The LED is lit continuously while the source is deemed stable and suitable to power the IT devices.

## 4 - Active Source

These LEDs will indicate the active source providing power to the load. The LED is lit continuously for the active source and turned off for the inactive source.

## 5 - Active Output

The LED indicates active/inactive state of the output. The LED is lit continuously while the switching circuitry and circuit breakers (if equipped) are closed. The LED will turn off if all the circuit breakers are open.

## 6 - Capacity Status

The LED indicates over current warning/alarm condition. The LED flashes slowly while the current draw exceeds a threshold value of 80% of current rating and turned off while the current draw is less than this threshold.

## 7 - Over Current Protection Device (OCPD) Status

The LED indicates an open OCPD condition, caused by either an overcurrent condition exceeding the OCPD ratings or the actuator is manually opened. The LED is flashes slowly while the OCPD is tripped and turned off after the overcurrent condition has been corrected and the OCPD actuator is manually closed.

## 8 - Internal Fault Status

The LED indicates a faulted operating status of the Product. The LED flashes when an internal fault is diagnosed and turns off when the operating condition is normal.

## 9 - Health Self-Test

This key executes the Health Self-Test mode. When the enabled health touch key is pressed, the sounder will beep four (4) times. All HMI LEDs will flash continuously while the Health Self-Test mode is active. The active mode will persist for a few seconds. The LED is lit continuously when the Health Self-Testing schedule is overdue. The sounder beeps rapidly three (3) times if the key is inhibited.

**NOTE: This key will be inhibited if a persistent fault condition exists. If health mode can't execute at time of touch key press, then the sounder will beep four (4) times and all LEDs are momentarily lit solid, but no switching action occurs.**

## 4.2 Interchangeable Monitoring Device

The Interchangeable Monitoring Device (IMD) is the core behind the Vertiv™ Geist™ RTS line of power products. The IMD can be replaced and upgraded to allow data-centers to future-proof their locations.



**CAUTION: Installing the wrong IMD for replacement in an RTS unit can lead to damage to the IMD.**

### 4.2.1 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.

## 4.2.2 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 4.2 IMD-01D Module



Table 4.1 IMD-01D Module Descriptions

Number	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 following table <a href="#">Display Button Functions</a> below .

Table 4.2 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. For more information, see <a href="#">Visible Light Communication (VLC)</a> on page 69 .
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.

## 4.2.3 Enhanced Monitored with RS-232 (IMD-03E-S)

All Vertiv Unit Level Monitoring Vertiv™ Geist™ rPDUs ship with the IMD-03E-S module. This module provides all of the same features as the IMD-03E, with the addition of a RS232 serial port using RJ-45.

Figure 4.3 IMD-03E-S Module Descriptions

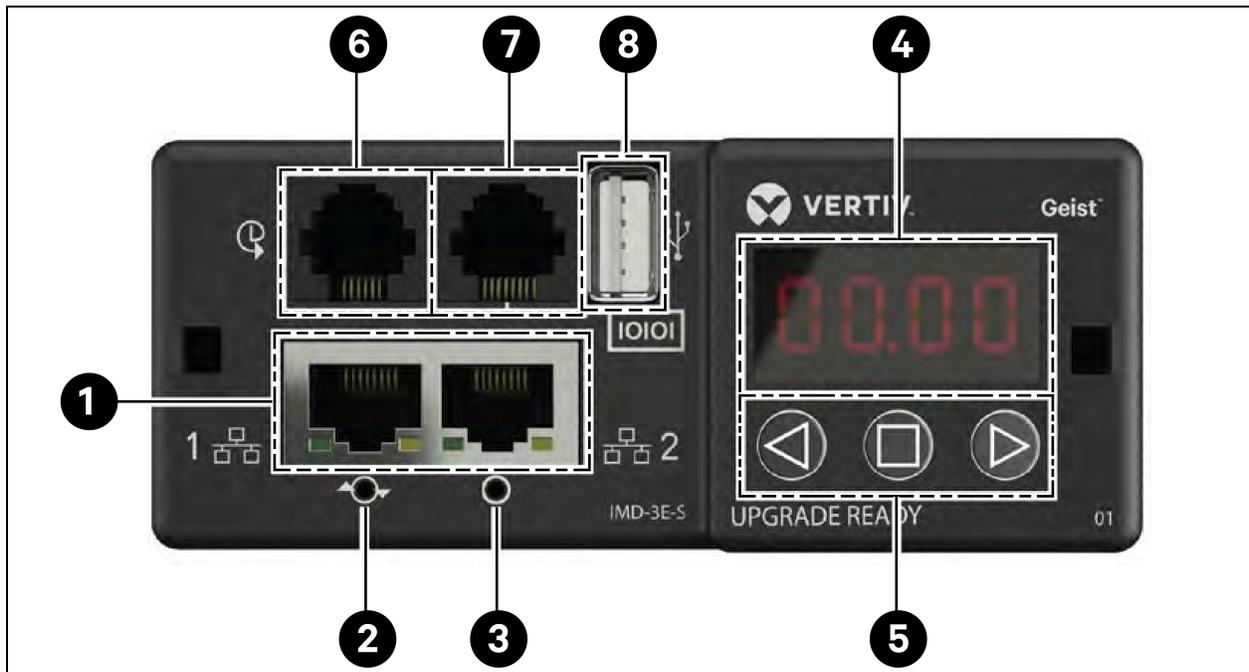


Table 4.3 IMD-03E-S Module Descriptions

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.
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 <a href="#">Display Button Functions</a> on the next page 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 Geist™ Integrated and Modular Sensors. For more information, see <a href="#">Available Sensors</a> on page 79 .
7	Serial Port	RS-232 via RJ-45 port.
8	USB Port	USB port used to upload firmware, backup/restore device configuration or expand logging capacity via USB storage device. Provides up to 100mA power capacity for USB- connected devices.

**NOTE:** Serial connection does not support flow control.

**Table 4.4 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 "rest" 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.
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.

**NOTE: Display Button functionality may vary based on unit configuration.**

#### 4.2.4 Enhanced Switched Monitored with RS-232

All Vertiv™ Geist™ Switched Unit Level Monitoring, Outlet Level Monitoring and Switched Outlet Level Monitoring Vertiv™ Geist™ rPDUs ship with the IMD-3E-S module. This module provides all of the same features as the IMD-3E, with the addition of a RS-232 serial port via RJ-45.

Figure 4.4 IMD-3E-S Module

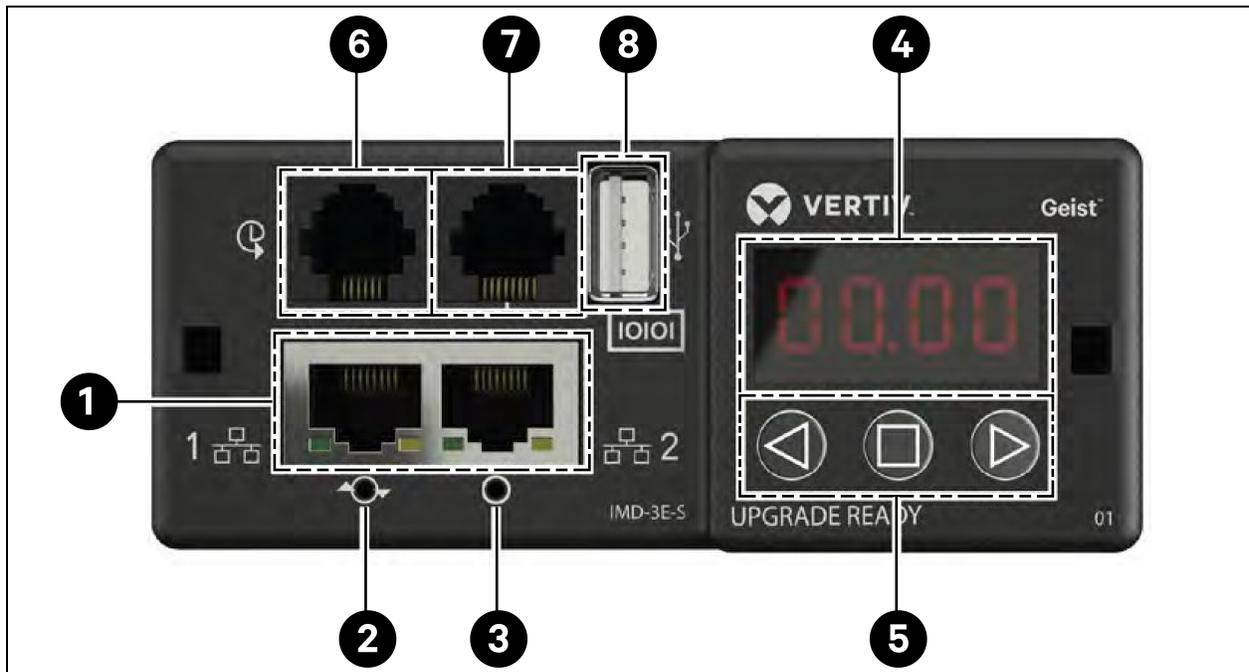


Table 4.5 IMD-3E-S Module Descriptions

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 RTS 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 and 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 <a href="#">Display Buttons</a> on the next page .
6	Remote Sensor Port	RJ-12 port for connecting a Vertiv plug-and-play remote digital sensor (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 Vertiv™ Integrated and Modular Sensors. For more information see <a href="#">Available Sensors</a> on page 79 .
7	Serial Port	RS-232 via RJ-45 port.
8	USB Port	USB port used to upload firmware, backup/restore device configuration or expanded logging capacity via USB storage device. Provides up to 1A 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.

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 "rest" 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.
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. For more information, see <a href="#">Visible Light Communication (VLC)</a> on page 69 .
Back and Forward Buttons		Pressing both buttons at the same time flips the display 180 degrees.
Back and Center Buttons		Pressing both buttons at the same time displays the primary IPv4 address of the unit.

### 4.2.5 Rapid Spanning Tree Protocol (RSTP)

Upgradeable monitored devices 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.

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.

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.**

## 4.3 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:

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. 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
- 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.

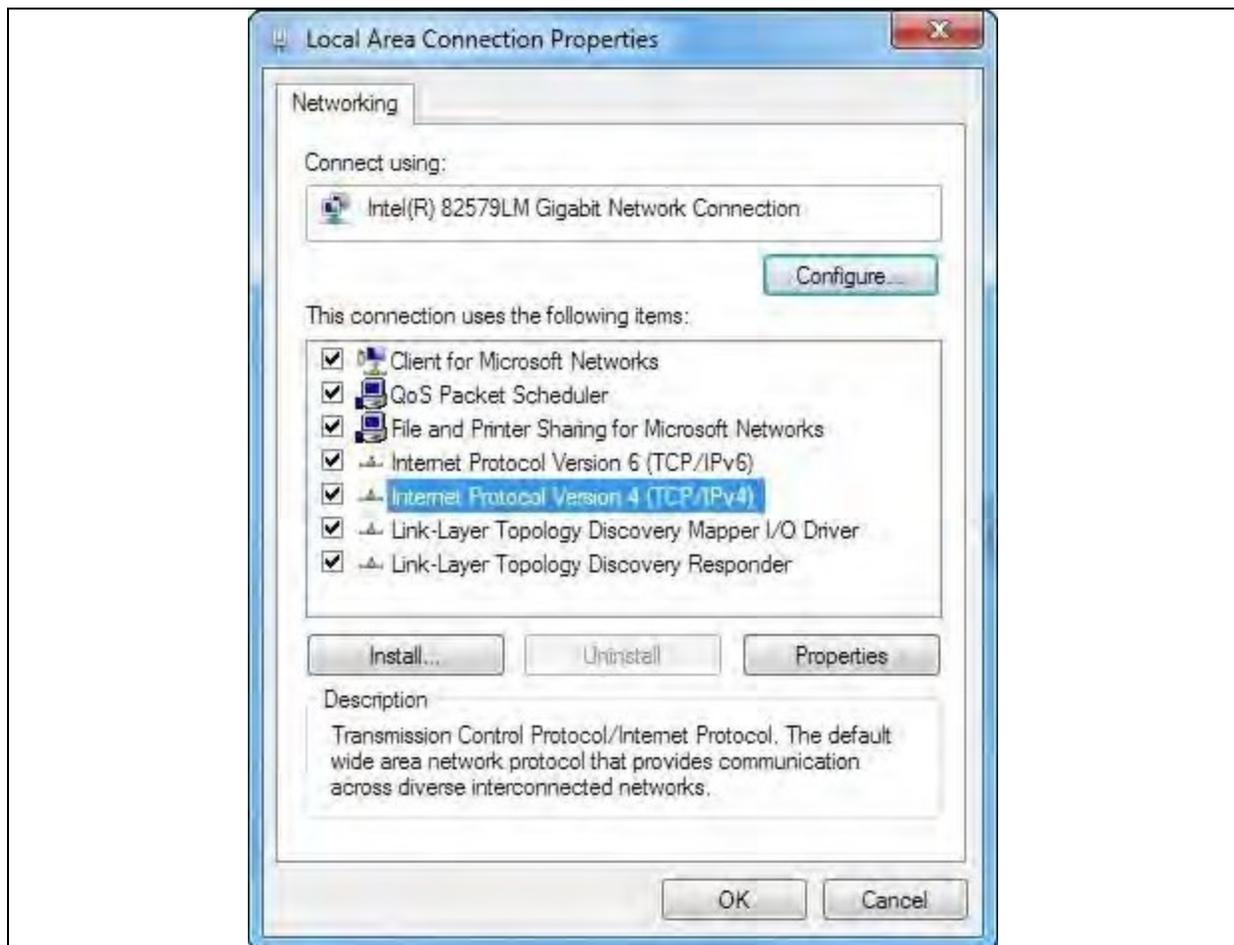
To set up the network for a Windows operating system:

1. Access the *network settings* for your operating system.
  - Using Microsoft Windows 2000, XP or Server 2003, click Start >Settings>Network Connections.
  - Using Microsoft Windows 7 or Server 2008, click Start>Control Panel>Adjust your Computer's Settings>View Network Status and Tasks>Change Adapter Settings or click Start>Settings>Control Panel>Network and Sharing Center>Change Adapter Settings.
  - Using Microsoft Windows 8 or Server 2012, move the mouse to the bottom or top right corner, click Settings>Control Panel>Large or Small Icons>Network and Sharing Center>Change Adapter Settings.
  - Using Microsoft Windows 10, 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 3G 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.

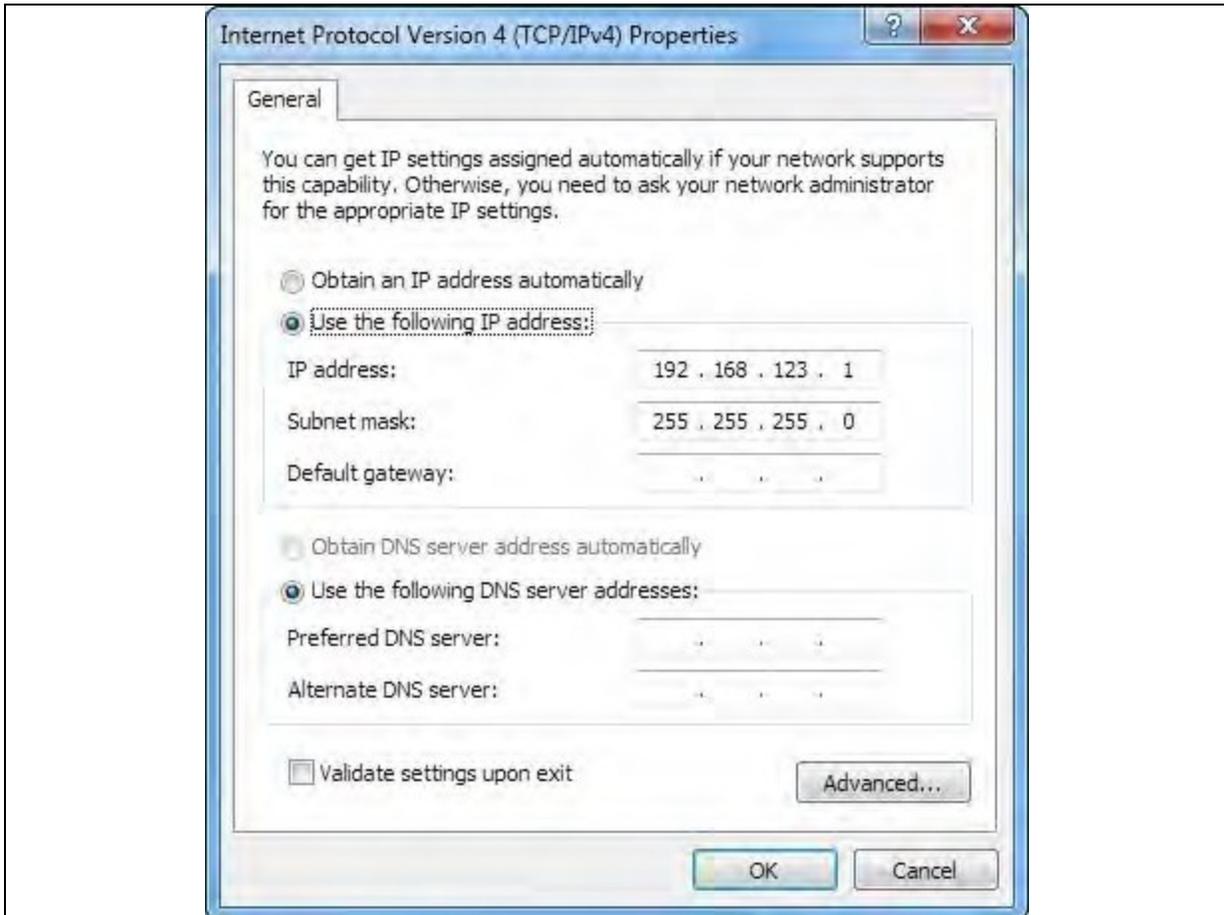
Figure 4.5 Local Area Connection Properties



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

Figure 4.6 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, log in 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*.

**NOTE:** After the changes are saved, the browser will no longer be able to reload the web page from the [192.168.123.123](http://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 4.7 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, then set IP address to 192.168.123.1 and Subnet Mask to 255.255.255.0 and click *Apply*.

**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, log in 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](http://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.

## 4.4 Web Interface

The unit is accessible via a standard, unencrypted HTTP connection as well as an encrypted HTTPS (TLS) connection.

**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 top of the page, please follow procedures in [Time](#) on page 44 .

### 4.4.1 Home Page

The Home Page gives both current and historical views of the unit's data. Real-time readings are provided for all Vertiv™ Geist™ RTS data and individual circuits' data.



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

Figure 4.8 Home Page

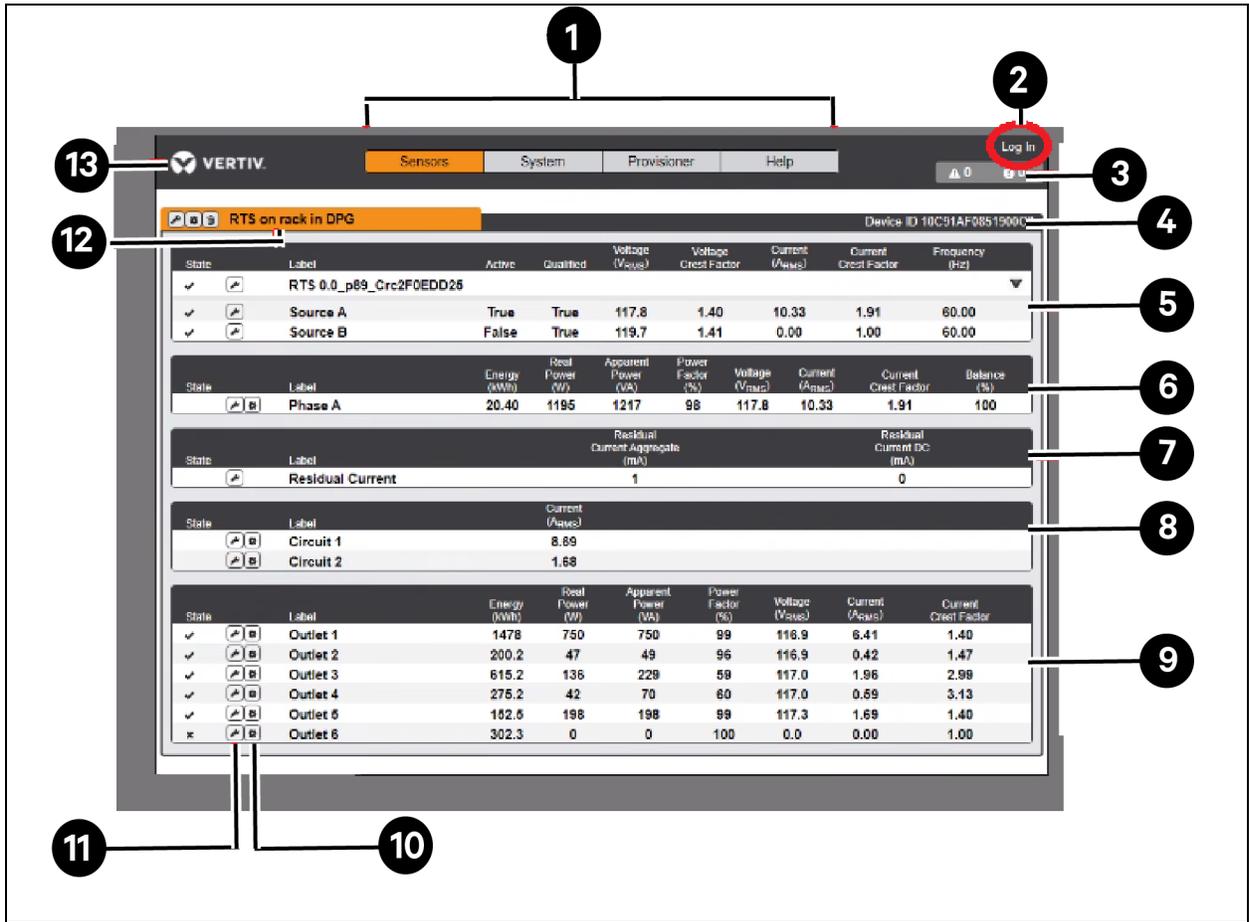


Table 4.6 Home Page Descriptions

Number	Name	Description
1	Device, Sensors, System and Help	Mouseover to show submenus: Device, Sensors, System, Provisioner and Help. <b>NOTE: Device will only appear as a sub menu when the unit is configured as an array manager. See the Vertiv™ Intelligence Director on page 55 for further definition and configuration.</b>
2	Log In/Log Out	Click to log in or log out of the unit. <b>NOTE: Both username and password are case-sensitive and no spaces are allowed. Prohibited characters for username are: \$&amp; `:&lt;&gt;[ ] { } * + % @ / ; = ? \ ^   - ,</b>
3	Alarms and Warnings	Indicates the number of alarms and warnings currently occurring, if any.
4	Device ID	Unique product identification and cannot be changed. May be required for technical support.
5	Rack Transfer Switch Power Sources A and B	Display status of both power sources including Active source (TRUE indicates active) and statistics for each source: Qualified (TRUE indicates source is qualified), Voltage, Voltage Crest Factor, Current, Current Crest Factor and Frequency
6	Total and Individual Phase	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.

**Table 4.6 Home Page Descriptions (continued)**

Number	Name	Description
	Monitor	
7	Residual Current	Only for rack devices with RCM-B Feature. Displays Residual Current Aggregate (mA) and Residual Current DC (mA). Where applicable, display Residual Current for each Phase.
8	Current Monitor	Displays AC current draw statistics for each individual circuit on the rack device.
9	Outlet Monitor	Applies to Outlet Monitored / Outlet Switched rack devices 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)
10	Operation Icon	Applies to Outlet Monitored / Outlet Switched rack devices ONLY - Modify settings.
11	Configuration Icon	Applies to Outlet Monitored / Outlet Switched rack devices ONLY - Modify label name.
12	Device Label	Displays the user-assigned label of this unit.
13	Vertiv Logo	Clicking on this logo from any page will reload the home page.

## 4.5 Sensors Tab

Click the *Sensors Tab* to access the Overview, Alarms and Warnings and Logging page from the drop-down menu.

### 4.5.1 Overview

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

#### To change device configuration:

1. Click the *Configuration icon* for the Vertiv™ Geist™ rack device and change the label. The Name is the rack device's factory name or model and cannot be changed.
2. Select *Outlet Control* for the Vertiv™ Geist™ rack device from dropdown to Enabled / Disabled.
3. Click *Save*.

#### 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.
  - Reset of Loss of Load - resets the Loss of Load alarm.

**NOTE:** These actions affect the entire device.

**NOTE:** On/Off and Reboot operations apply to Outlet Switched Geist™ rack devices 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. Select *Submit* 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.**

**To change the Rack Transfer Switch configuration:**

1. Click *Configuration icon* next to Rack Transfer Switch.
2. Change the *configurations*, as needed.
  - a. Label of the *Rack Transfer Switch*.
  - b. Select *Preferred Source* from dropdown.
  - c. Select *Auto Health Test* from dropdown to Enabled / Disabled.
  - d. Enter *Input Auto Health Self-Test Period (d)*, in days, the unit waits before Health Self-Test.
  - e. Select *Auto Retransfer* from dropdown to Disabled / Enabled.
  - f. Enter *Auto Retransfer Delay (s)*, in seconds, the unit waits before Retransfer.
3. Click *Save*.

**To change the Rack Transfer Switch source label:**

1. Click the *Configuration icon* for the source and change the label.
2. Click *Save*.

**To change a phase or circuit label:**

3. 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.
4. Click *Save*.

**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. Select *Submit* to issue the action.

**To change circuit operation:**

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

**NOTE: This step is required when State shows a loss of load alarm and the issue has been resolved.**

**To configure an outlet:****NOTE: Applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rack devices only**

4. Click the *Outlet Configuration icon*.
5. 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, trips On) - the outlet state is set normally Off and will be switched On when the outlet alarm event is tripped.
    - Alarm Control (normally on, trips off) – the outlet state is set normally on and will be switched off when the outlet alarm event is 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.
6. Click *Save*.

**To change outlet operation:****NOTE: Applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rack devices 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.
  - 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 *Submit* to issue the action.

## 4.5.2 Alarms and Warnings

The Alarms and 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.

Figure 4.9 Alarms and Warnings Page

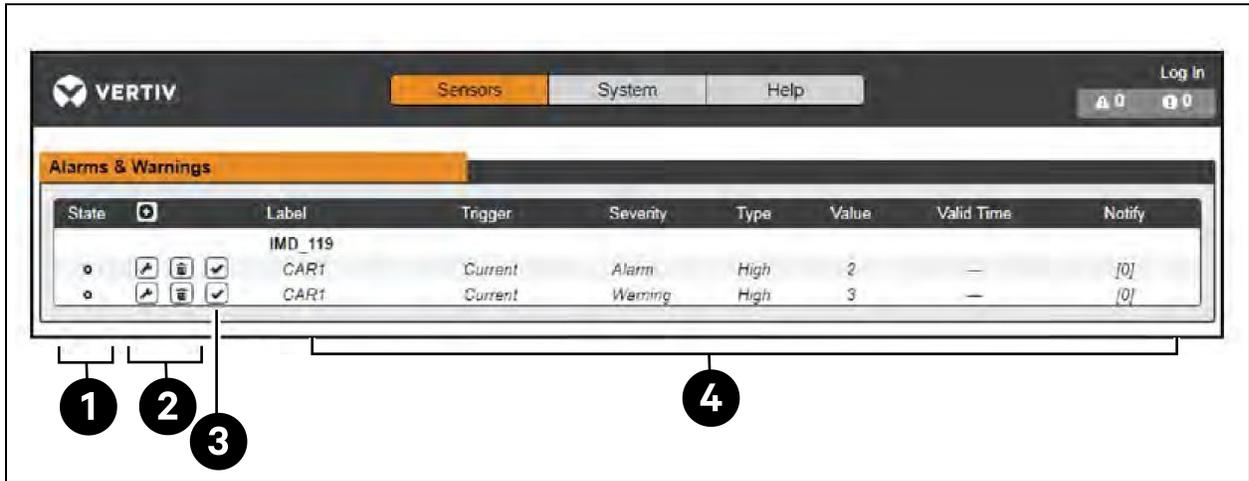


Table 4.7 Alarms and Warnings Descriptions

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. <b>NOTE: Clicking this symbol does not clear the warning or alarm event; it just stops the notifications from repeating.</b>
4	Displays the conditions for the alarms and warnings settings.		

**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 [Serial Port](#) on page 45 .
  - 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 and Warnings](#) on the previous page .

**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™ rack devices 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.**

**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.

**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.

### 4.5.3 Logging

The Logging page allows you to access the historical data recorded by the Vertiv™ Geist™ rack device by selecting the desired sensors and time range to be logged. The Logging page permits selecting all or selecting none. To do so, click on the drop-down menu, choose Select All or Select None and click on the appropriate check mark.

**Figure 4.10 Vertiv™ Geist™ RTS Logging Page**

The screenshot shows the Vertiv™ Geist™ RTS Logging Page. At the top, there are navigation tabs for 'Sensors', 'System', and 'Help', along with 'Admin' and 'Log Out' links. The 'Data Log' section includes buttons for 'Download the data log JSON' and 'Download the data log CSV', a warning message 'Warning: Changing the interval clears the log.', a 'Log Interval (minutes)' input field set to 15, and a 'Save' button. Below this is a 'Clear the Log' button. The 'Logging' section features a 'Click a measurement value to select or deselect.' message and a 'Save' button. A dropdown menu is set to 'Select All'. The main data table is titled 'Your PDU Name' and 'Device ID A532AD00651900C3'. It contains three tables of data:

State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (VRMS)	Voltage Min (VRMS)	Voltage Max (VRMS)	Peak Voltage (V)	Current (ARMS)	Current Min (ARMS)	Current Max (ARMS)	Peak Current (A)
	Phase A	41.321	5	10	51	125.6	125.3	125.7	179.0	0.08	0.07	0.08	0.35
State	Label	Current (ARMS)	Current Min (ARMS)	Current Max (ARMS)	Peak Current (A)								
	Circuit 1	0.00	0.00	0.00	0.00								
State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (VRMS)	Voltage Min (VRMS)	Voltage Max (VRMS)	Peak Voltage (V)	Current (ARMS)	Current Min (ARMS)	Current Max (ARMS)	Peak Current (A)
✓	Outlet 1	0.047	0	0	100	121.2	120.9	121.3	172.8	0.00	0.00	0.00	0.00

Table 4.8 Logging Page Descriptions

Number	Name	Description
1	Data log download	Clicking the JSON link downloads the data log in JSON format. Clicking the CSV downloads the data log in .csv format for use in spreadsheet software.
2	Log interval	The frequency at which data is written to the log file. The logging interval can be 1-600 minutes; the default setting is 15 minutes.
3	Clear log data	Delete the log file.
4	Select All/Select None	Click on the drop-down menu, select Select All or Select None and click on the check mark.
5	Logging	Click the measurement value to select or deselect desired logging parameters. By default, all measurements are selected. Press 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.

## 4.6 System Tab

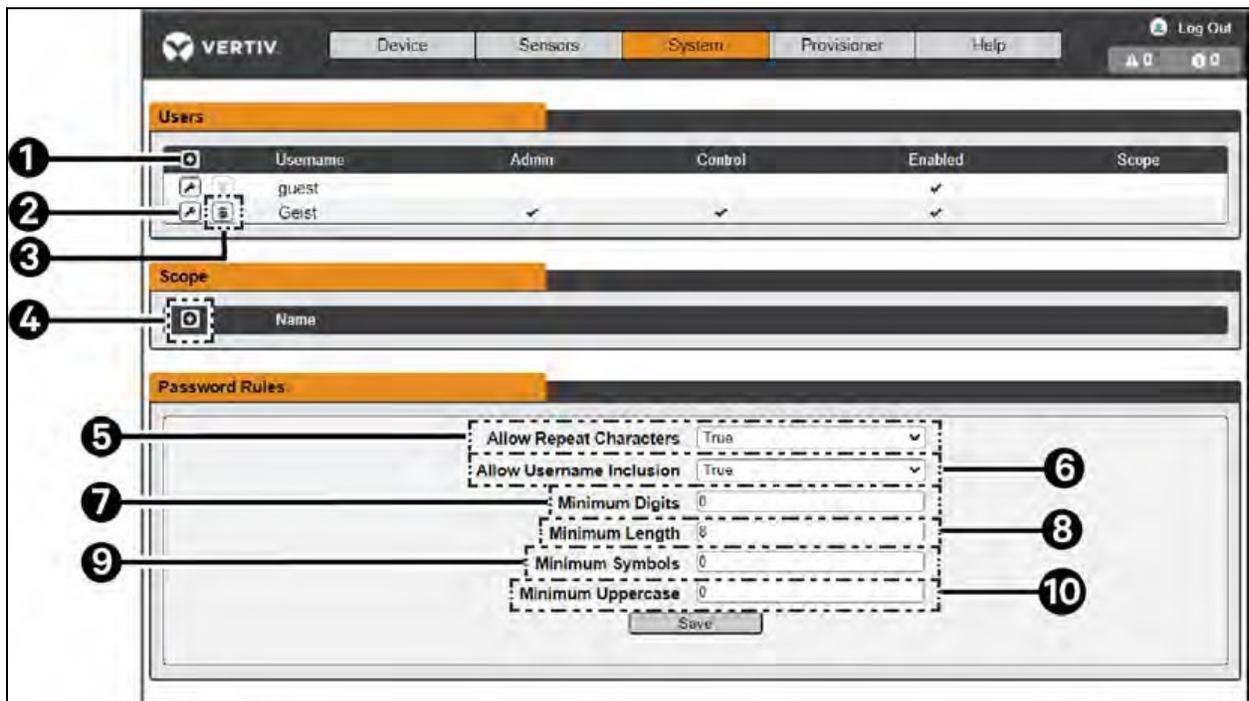
**NOTE:** You must be logged in as Administrator to modify settings in the System Tab.

### 4.6.1 Users Page

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.

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

Figure 4.11 User Page



**Table 4.9 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 an Administrator-level account can add, modify or delete users as well as add, modify or delete scopes. Control-level and Enabled 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.**

**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”.
  - 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.
- **Enabled:** If both administrator and control are set to False, the account is an Enabled account, which is view-only. The only changes an Enabled account is permitted to make are changing its own account's password and changing the preferred language for its own account. Enabled 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 your *Username* in the top right corner of the page.
3. Enter a *new password* and click *Save*.

Figure 4.12 Change User Password Page

### To add or modify a user scope:

1. Click the *Add or Modify Scope* icon. Refer to **Figure 4.13** on the next page for more details.
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 LDAP Remote Authentication
  - c. Click applicable Outlets for a specified User. (Highlight in Green)
3. Click *OK* to save changes.

Figure 4.13 Add Scope

**Add**

Label

Remote Authentication Attribute

Outlet 1 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 2 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 3 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 4 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 5 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 6 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 7 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 8 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 9 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 10 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 11 (Geist Upgradable rPDU, F4E16F0B851900C3)
Outlet 12 (Geist Upgradable rPDU, F4E16F0B851900C3)

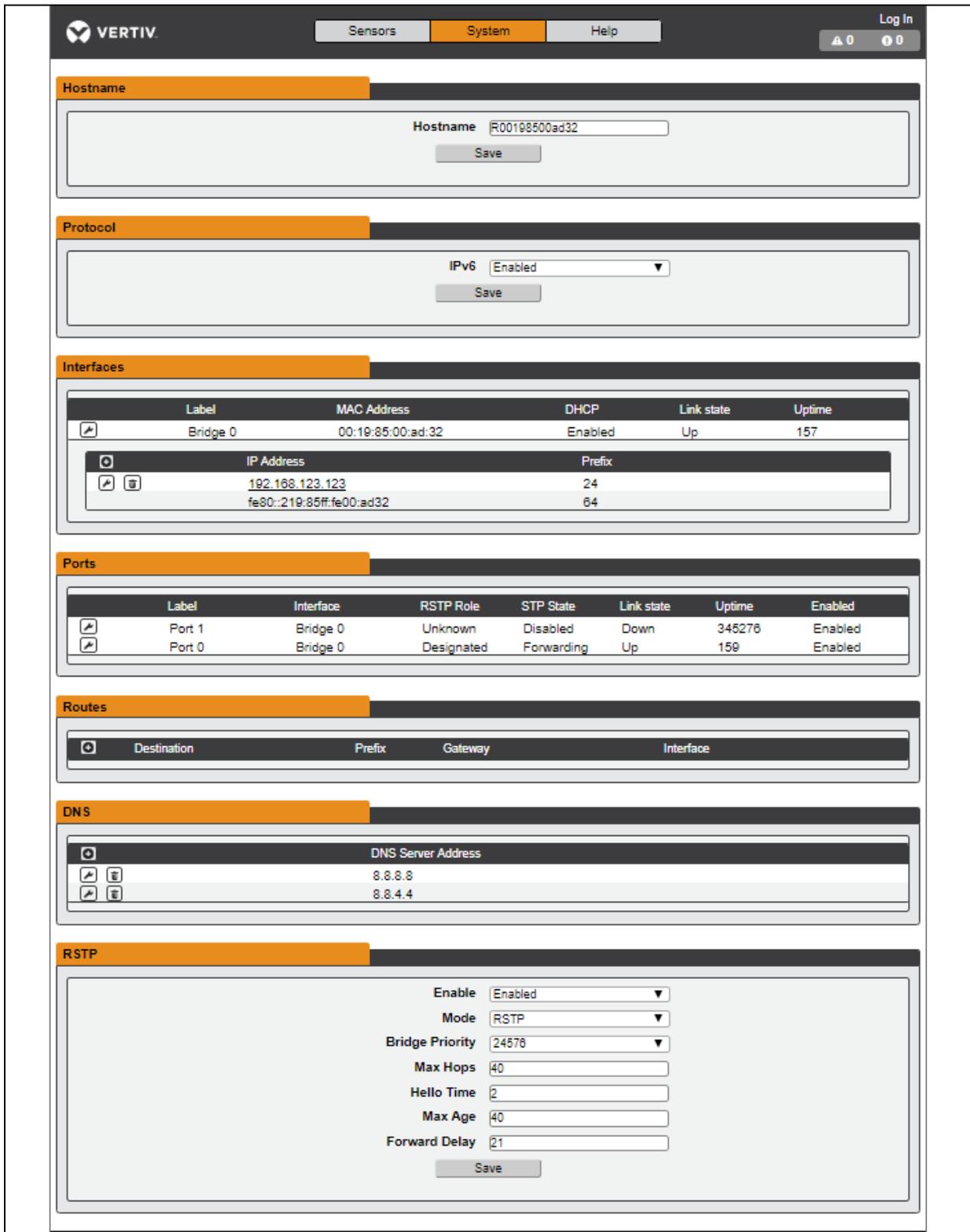
**NOTE:** A user will be logged out automatically after 10 minutes of inactivity.

## 4.6.2 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™ rack device, enable/disable DHCP and to view Link State 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 of each port on the Geist™ rack device.
- **Routes:** Displays configured routes and is where you will set your Gateway address for the Geist™ rack device. 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.

Figure 4.14 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*.

**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.**

**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*.

**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*.

**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 cost*. This designates this interface's contribution to the root path cost when it serves as the root port.
3. Click *Save*.

**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*.

**To modify an existing route:**

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

**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*.

**To modify an existing DNS Server address:**

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

**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*.

### 4.6.3 Web Server

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

- HTTP Interface: Enables or disables access via HTTP. HTTPS interface is always enabled. Available options are Enabled and Disabled. It is not possible to disable the web interface completely.
- 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 4.15 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.

Figure 4.16 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 the RSA algorithm and in PEM format.
- 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.

## 4.6.4 Reports

The Reports page allows you to schedule the device to send recurring status reports.

**NOTE: SMTP email must be set up on the device via the email page.**

**To Add or Modify a scheduled report:**

1. Click the *Add or Modify icon*.
2. Select the *Days* the report is to be sent.
3. Select the *time of the day* to Start sending reports.
4. Set the *interval (in hours)*.
5. Select the *Target email address* for the reports to be sent.
6. Click *OK* to save changes.

**To delete a scheduled report:**

1. Click on the *Delete icon* next to the report to delete.
2. Click *OK* on the pop-up window to confirm.

**4.6.5 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

**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™ rack 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.

- LDAP Server Address: Specify the host address for LDAP. The HOST can be an IPv4 address, an IPv6 address in brackets (e.g., [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 107.
- 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.
- 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.

Figure 4.17 LDAP Menu

Enable	Enabled
LDAP Server Address	host
LDAP Server Port	389
LDAP Mode	Active Directory
Security Type	None
Bind DN	
Bind Password	No Password...
Base DN	
User Filter	(objectClass=posixAccount)
"uid" Mapping	uid
"uidNumber" Mapping	uidNumber
Group Filter	(objectClass=posixGroup)
"gid" Mapping	gidNumber
"memberUid" Mapping	memberOf
Enabled Group	enabled
Control Group	control
Admin Group	admin

Save

## 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™ rack device for this remote authentication protocol. If you are not familiar with these settings, please consult your TACACS+ server administrator.

Configuration for remote authentication using TACACS+.

Figure 4.18 TACACS+ Menu

- Primary Authentication Server: The primary authentication/authorization server, which can be an IPv4 address, an IPv6 address in square brackets (e.g., [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: 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.
- 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.**

## Remote Authentication Dial-In User Service Protocol (RADIUS)

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

**NOTE: Knowledge of your RADIUS server settings is required to set up the Vertiv™ Geist™ rack 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 4.19 RADIUS Menu

The screenshot shows a configuration window titled "Radius". It contains the following fields and values:

- Primary Authentication Server: [Empty text box]
- Alternate Authentication Server: [Empty text box]
- Shared Secret: [No Password...]
- Group Attribute: [filter-id]
- Admin Group: [Empty text box]
- Control Group: [Empty text box]
- Enabled Group: [Empty text box]

A "Save" button is located at the bottom center of the form.

- 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 (e.g., [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: 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.**

## 4.6.6 Display

The unit's display configuration can be changed via the Display tab of the System menu. Settings pertaining to the unit's display are:

- Inverted: When true, the local display is flipped 180 degrees
- Total Power: Appears on local display when enabled (displayed as kW).
- Voltage: Appears on local display when enabled.
- Current: Appears on local display when enabled.
- VLC: Allows user to enable or disable VLC mode from GUI (default is disabled).

Figure 4.20 Display Mode/VLC Configuration Page

The screenshot shows the Vertiv web interface. At the top, there is a navigation bar with tabs for 'Device', 'Sensors', 'System' (selected), 'Provisioner', and 'Help'. A 'Log Out' button is in the top right corner. Below the navigation bar, the 'Display' configuration page is shown. It contains two sections: 'Inverted' with a dropdown set to 'False' and a 'Save' button; and 'Total Power', 'Voltage', and 'Current' each with a dropdown set to 'Disabled', 'Disabled', and 'Enabled' respectively, and a 'Save' button. Below this is the 'VLC' configuration page, which has a 'VLC Mode' dropdown set to 'Disabled' and a 'Save' button.

## 4.6.7 Time

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

Figure 4.21 Time Configuration Page

The screenshot shows the 'Time' configuration page. It features a 'Mode' dropdown set to 'NTP'. Below it are input fields for 'Date-Time (YYYY-MM-DD hh:mm:ss)' with the value '2014-09-17 08:50:20', 'Time Zone' dropdown set to 'America/Chicago', 'Primary NTP Server' input field with '0.pool.ntp.org', and 'Alternate NTP Server' input field with '1.pool.ntp.org'. A 'Save' button is located at the bottom of the configuration area.

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.

## 4.6.8 SSH

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

Figure 4.22 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.**

## 4.6.9 USB

To enable or disable the USB port:

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

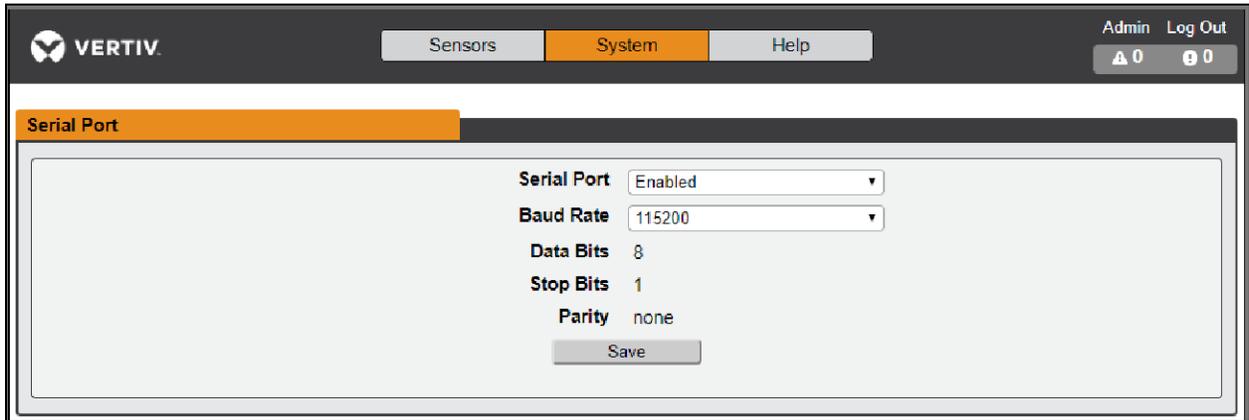
## 4.6.10 Serial Port

**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 4.23 Serial Port



### 4.6.11 Email

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

Figure 4.24 Email Configuration Page

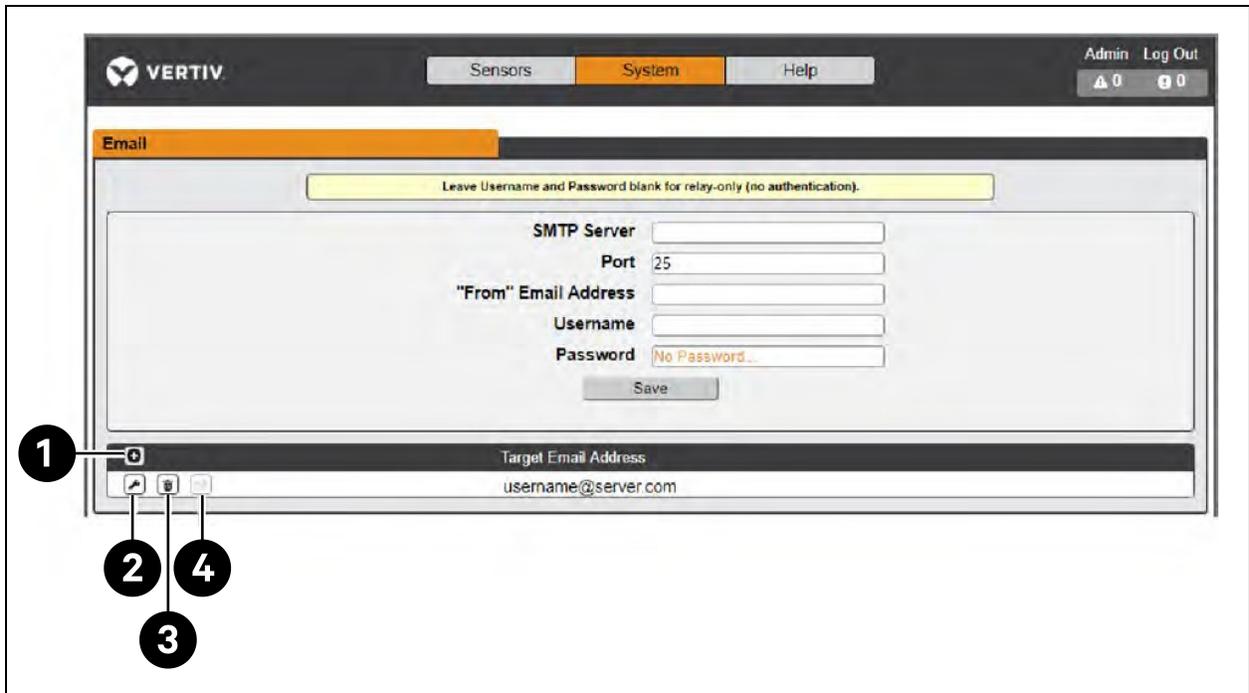


Table 4.10 Email Configuration Page Descriptions

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

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.
- **Enable SSL:** If Enabled, the unit will attempt to connect to the server using a fully encrypted TLS/SSL connection. Note that when this setting is enabled only fully encrypted sessions are supported; the StartTLS method, where the session starts out as unencrypted and then switches to encrypted part way through the session, is not supported. If using a service that utilizes StartTLS, such as Office365, leave this option disabled.
- **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.

## 4.6.12 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 two IP addresses.

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

**Figure 4.25 SNMP Configuration Page**

The screenshot shows the SNMP configuration interface. It features an orange header with the text "SNMP". Below the header is a white configuration area with a grey border. At the top of this area is a button labeled "Download the MIB ZIP". Below this button are two dropdown menus: "SNMP-V1/V2c Service" and "SNMP-V3 Service", both of which are currently set to "Enabled". Below the dropdowns is a text input field for "Port" with the value "161". At the bottom of the configuration area is a "Save" button.

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.

**Figure 4.26 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.

## 4.6.13 Modbus

Allows for Modbus TCP communication protocol support. The user is able to read Modbus TCP/IP data.

- Modbus: Enables or disables access via Modbus.
- Port: Allows you to change the port that the Modbus service listens to for incoming connections. The default is Port 502.

## 4.6.14 SYSLOG

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

**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.**

## 4.6.15 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 tab(s) currently viewing the device.

## 4.6.16 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.

## 4.6.17 Utilities

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

### Aggregation

Change *settings*, as desired. (See [Aggregation](#) on page 55 )

To change Aggregation setting:

1. Select *Enable or Disable* from dropdown menu
2. If Aggregation is enabled,
  - a. Array device Username: Defines the username configured on all array devices.
  - b. Array device Password: Defines the password configured on all array devices.
3. Click *Submit button*

### Configuration Backup and Restore

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

**Table 4.11 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 Choose 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.**

**Restore Defaults**

Restore the default settings.

**Table 4.12 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*.

**Reboot**

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

To reboot the operating system: Click Reboot.

**NOTE: The power to connected devices is not affected.**

**Reboot I/O Boards**

If the Vertiv™ Geist™ rack 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 board(s) causing them to restart.

To reboot the I/O boards: Click Reboot I/O Boards.

**NOTE: The power to connected devices is not affected.**

## 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 Choose File and select the .firmware file from the Open window.
2. Click Submit.
3. If a problem occurs, 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 (must 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.

## Factory Access

Provides information for technical support.

**Table 4.13 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.**

## 4.7 Provisioner Tab

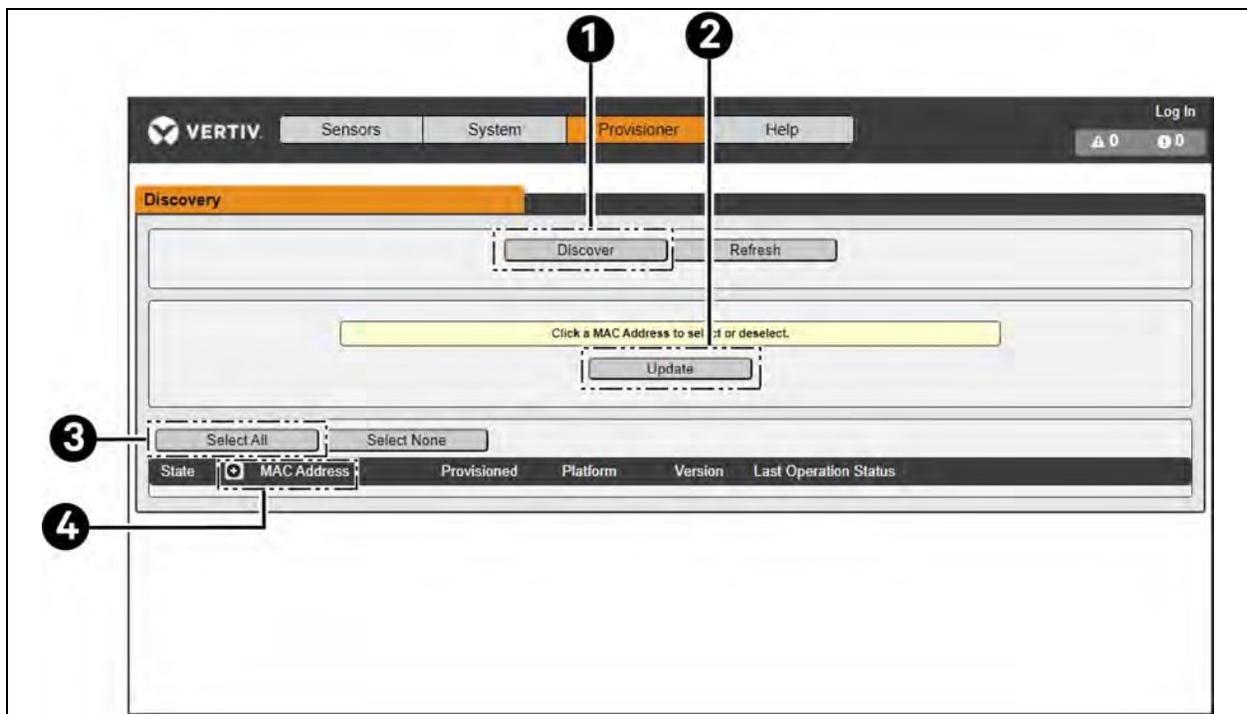
The Provisioner allows the user to discover locally connected Vertiv™ Geist™ rack devices. The user can update their firmware and configure them by uploading a configuration settings file.

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

- Geist™ rack devices running 3.x.x or 5.x.x firmware (IMD models 02, 02E, 3E, 03E, 3E-S and 03E-S)
- R-Series Geist™ rPDUs running 5.x.x firmware
- Factory fresh or previously configured Geist™ rack devices
- Rack PDUs and RTS units connected directly to the local network or connected as part of a Vertiv Intelligence Director (aggregation) network
- All or selected discovered Geist™ rack devices

**NOTE:** You must be logged in as Administrator-level user to utilize the Provisioner. IPV6 must be enabled on the Geist™ rack devices 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 4.27 Provisioner Page



Item	Name	Description
1	Discover	Identifies local and network connected rack PDUs
2	Update	Updates firmware and/or configuration of selected rack devices
3	Select All	Selects all connected rack devices
4	Add MAC address	Allows manually entered rack devices by MAC address

## 4.7.1 Discovery

1. Click *Discover icon* to identify locally connected Vertiv™ Geist™ rack devices.
2. Click *all the Geist™ rack devices* 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™ rack devices in listed.
3. Click *Update icon* to update all selected Geist™ rack devices with firmware file and/or configuration file.

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

## 4.7.2 File Management

### Firmware Files

1. Click *Choose File* and select the .firmware file from the Open window.
2. Click *Submit icon*. Firmware file will be listed

### Configuration Files

1. Click *Choose File* and select the .config file from the Open window.
2. Click *Submit icon*. Configuration file will be listed

**Figure 4.28 File Management Page**

The screenshot shows the 'Provisioner' tab of the Vertiv interface. It features a navigation bar with 'Sensors', 'System', 'Provisioner', and 'Help'. The 'Firmware Files' section includes an 'Upload File' area with a 'Choose File' button (showing 'No file chosen'), a 'Name' input field, and a 'Submit' button. Below this is a table with columns: File, Version, Platform, and Date. The 'Configuration Files' section has a similar 'Upload File' area and a table with columns: File and Date.

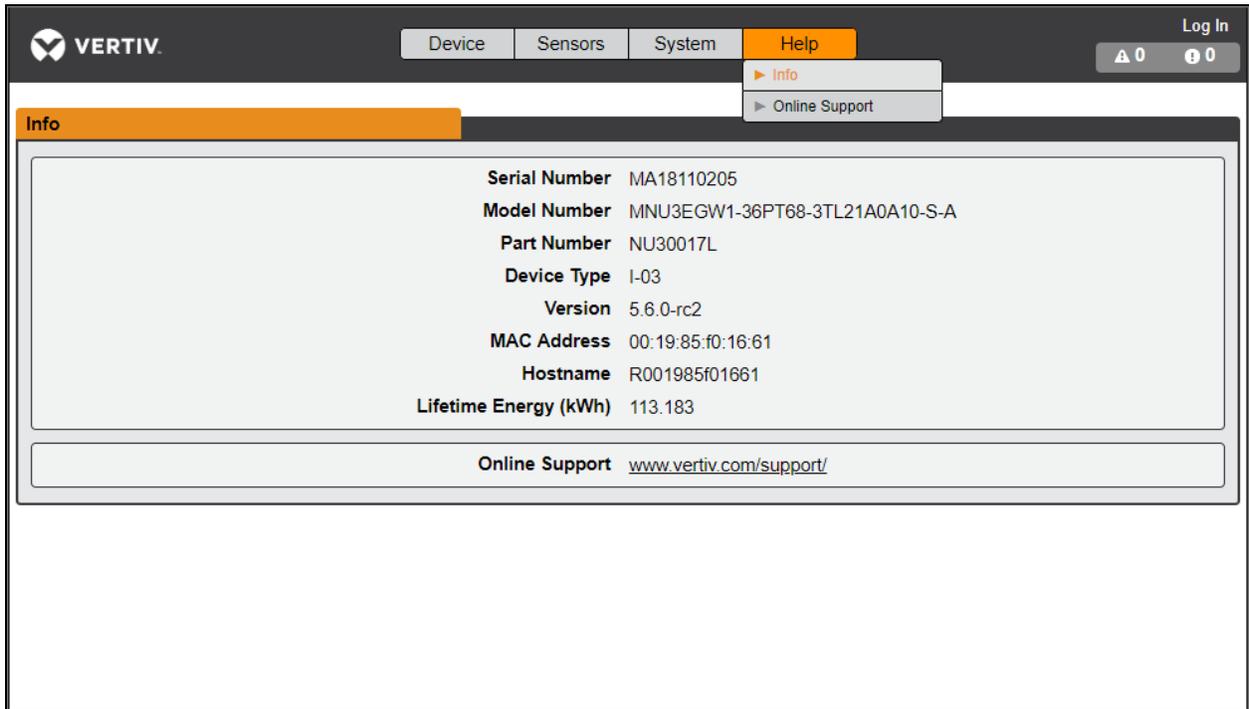
See [Provisioner - Format of the Configuration Settings File](#) on page 85 for examples of configuration setting files used by the Provisioner and the necessary format for the file.

## 4.8 Help Tab

### 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.

Figure 4.29 Info Page



## 5 Vertiv™ Intelligence Director

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

### 5.1 Aggregation

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

- This system consists of one array manager and one or more array devices. Use a single IP address assigned to the array manager to monitor up to 50 devices (the array manager and 49 array devices).
- Allow Geist™ rack devices array from the array manager to the self-configure network settings.
- Create aggregated measurements like total rack power and total row power, including averages, minimums and maximums.

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

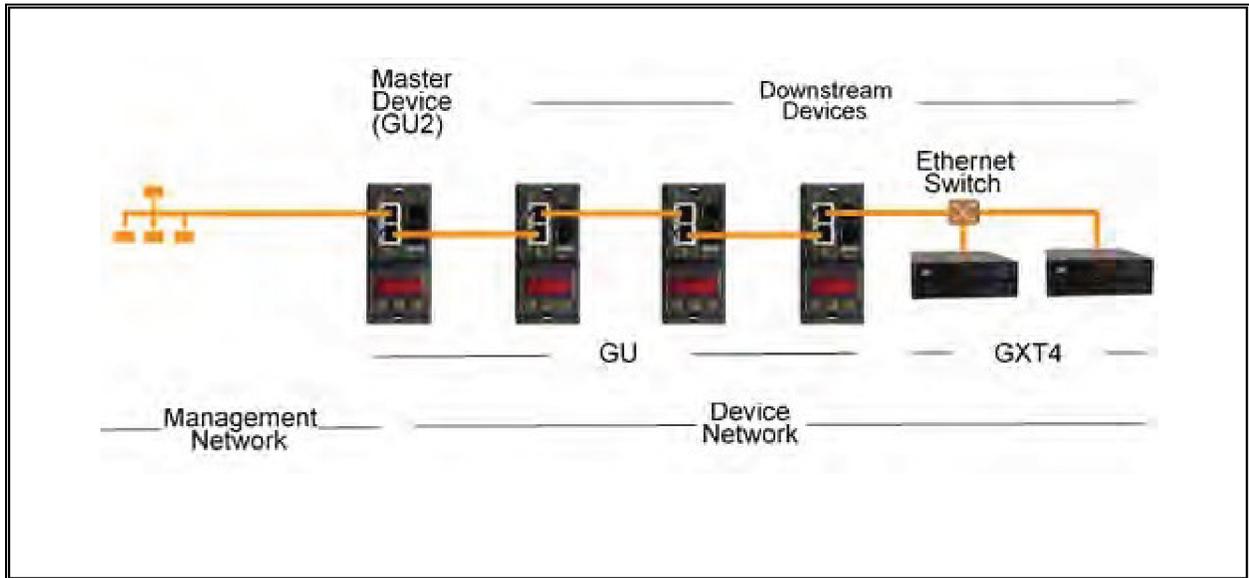
- Create groups of Geist™ rack device outlets spanning one or more Geist™ rack devices.
- Report on total power and energy for the outlet group (with Geist™ rack devices that report per outlet measurements).
- Provide the ability for power off, power on or power cycle the group of outlets with a single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

Visibility of Vertiv Intelligence Director (Aggregated) devices is available in read-only mode through SSH and serial port CLIs.

### 5.2 Array Manager

Aggregation requires the designation of an array manager, deployed with IMD model IMD-3E-S. The IMD of the array manager facilitates and configures the device network, the interconnected array of Geist™ rack devices, Vertiv™ UPSs, Vertiv™ cooling, environmental sensors and Geist™ rack device 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 5.1 Sample Configuration



The IMD-3E-S is the default intelligence card for Vertiv™ Geist™ GU2 rack devices, which include switched (model numbers beginning with MNS), outlet monitored (model numbers beginning with MNR) and switched plus outlet monitored (model numbers beginning with MNU) products. To serve as the array manager, Geist™ rack devices with a legacy intelligence card must first be upgraded to the IMD-3E-S.

## 5.3 Network Configuration

In the initial release of aggregation, array devices are defined as Geist™ rPDU / RTS units within the Geist™ GU1 and GU2 product platforms as well as Vertiv™ MPH2 and MPX rack PDUs, Vertiv™ GXT4, GXT5, PSI5, EXM, APM and ITA2 UPS, Vertiv™ CRV row cooling and USB-connected Vertiv™ 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. Use the *top drop-down menu* to navigate to System>Locale.
2. Select the *appropriate Default Language and Temperature Units* from the drop-down menus. These settings are pushed to the array devices in its network.
3. Browse to System>Network. In Protocol IPv6, choose Enabled from the drop-down menu.
4. Browse to System>Utilities. Change the settings as desired.
  - a. Aggregation: Choose Enabled from the drop-down menu.
  - b. Array device Username: Defines the username configured on all array devices.
  - c. Array device Password: Defines the password configured on all array devices.

5. Enter the *new password*, verify the *password* and click *OK*.  
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 Geist™ rack devices running 5.9.0 or later firmware.
6. Click *Submit*. If Aggregation is enabled, the Device Tab appears next to the Sensors Tab on the top navigation bar.

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.**

### 5.3.1 Array Devices

In the initial release of aggregation, array devices are defined as Geist™ rPDU/RTS units within the Geist™ GU1 and GU2 product platforms as well as Vertiv™ MPH2 and MPX rack PDUs, Vertiv™ GXT4, GXT5, PSI5, EXM, APM and ITA2 UPS, Vertiv™ CRV row cooling and USB-connected Vertiv™ VRC cooling. All Geist™ GU1 rPDUs must be running firmware Version 3.3.3 or later; Geist™ GU2 rack devices must be running Version 5.3.0 or later. If the Geist™ rack devices are newly ordered and have never been configured with network settings, they are ready for aggregation out-of-the-box. If the Geist™ rack devices have been deployed in a computing environment and commissioned with local LAN settings and user accounts, each Geist™ rack devices must be reset to its factory defaults using the Utilities page. The array manager then pushes configuration data to the array devices, including:

- Network settings
- Default Language and Temperature Units
- Username
- Password

#### 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 daisy-chaining, ensure that no more than 100 Vertiv™ Geist™ rack devices are chained together.
  - If connecting daisy-chains to a network switch, no daisy-chain should be longer than 20 Geist™ rack devices.
  - A star network or other design is also acceptable in lieu of a daisy-chain.
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 network using Port 2.

#### To set up an existing installation with one array manager:

**NOTE: Use the following instructions if existing Geist™ rPDU/RTS units are connected in a daisy-chain.**

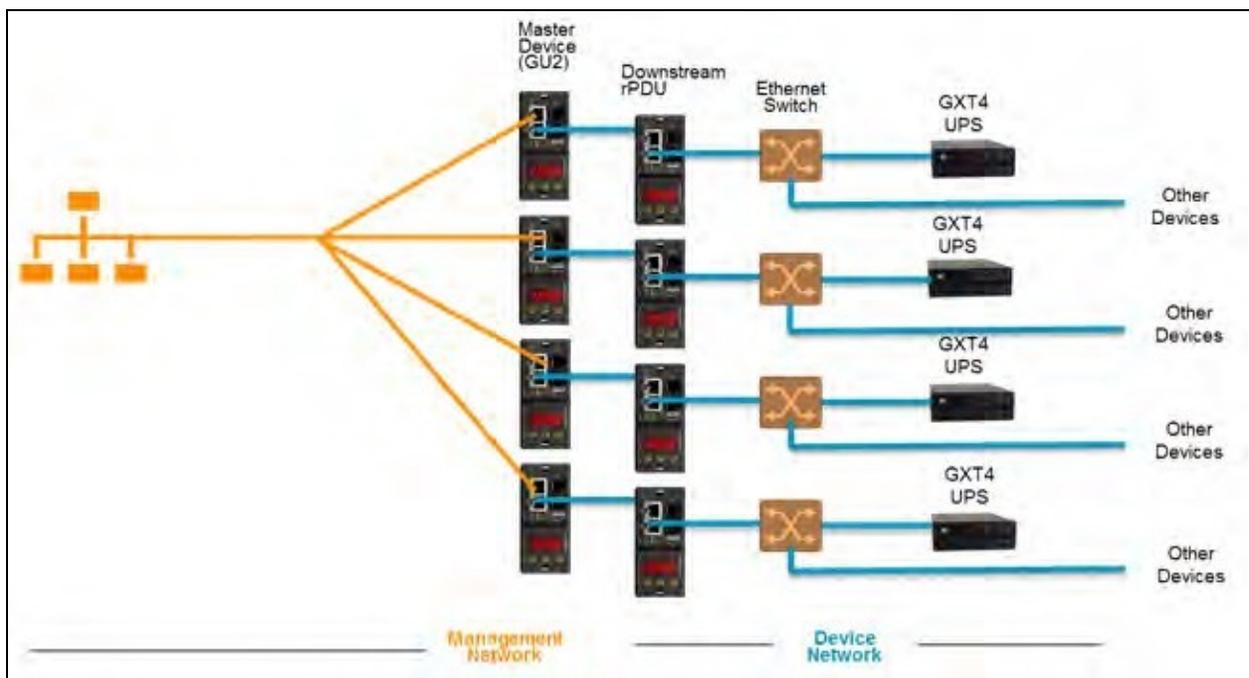
1. Designate an *array manager* and disconnect it from the management network.
2. Reset all the *array device* to factory default settings. The physical ETHERNET connections in the daisy-chain can remain the same; however, if previously connected in a looped configuration, the final Geist™ rPDU/RTS unit 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 rack device example, represented in the **Figure 5.2** below. This installation would require a minimum of four array managers, each operating its own stand-alone device on the 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.

**Figure 5.2 Sample Network Configuration**



**NOTE:** RSTP is disabled by default in Geist™ GU1 rPDUs running 3.4.0 or later and Geist™ GU2 rPDU/RTS units running 5.3.3 or later. In previous firmware, RSTP is enabled on both platforms. Aggregation does not support RSTP. Leaving RSTP enabled limits a rack device daisy-chain within aggregation to 40 devices. Disabling RSTP on array devices will remove the 40-device limitation.

## 5.4 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

Figure 5.3 Device Tab

Name	Energy (kWh)	Power (W)			
		Sum	Minimum	Maximum	Average
Total	174.9	44	17	27	22
Phase A	174.9	44	8	9	22
Phase B	0.000	0	0	0	0
Phase C	0.000	0	0	0	0

Name	Temperature (F)			Humidity (%)		
	Minimum	Maximum	Average	Minimum	Maximum	Average
Environmental	79.70	79.93	79.83			

Severity	Name	Event

### 5.4.1 Summary

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

#### Rack PDU/RTS Unit

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

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

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

#### UPS

The UPS network is summarized by the following data points:

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

The Environmental category is summarized by the following data points:

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

- Temperature Minimum: The lowest temperature within the device network.
- Temperature Maximum: The highest temperature within the device network.
- Temperature 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 Minimum: The lowest thermal device temperature within the device network.
- Temperature Maximum: The highest thermal device temperature within the device network.
- Temperature 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.

### 5.4.2 Groups

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

#### Group rPDU/RTS Unit

- Energy: The total Geist™ rack device energy within the group.
- Power Sum: The total Geist™ rack device power load within the group.
- Power Minimum: The lowest Geist™ rack device power load within the group.
- Power Maximum: The highest Geist™ rack device power load within the group.
- Power Average: The average Geist™ rack device power load within the group.

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

## Group rPDU/RTS Unit Outlet

- Energy: The total Geist™ rack device Outlet energy within the group.
- Power Sum: The total Geist™ rack device Outlet power load within the group.
- Power Minimum: The lowest Geist™ rack device Outlet power load within the group.
- Power Maximum: The highest Geist™ rack device Outlet power load within the group.
- Power Average: The average Geist™ rack device Outlet power load within the group.

These readings repeat for each group of Vertiv™ Geist™ rack device 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.

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 Operations 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 Maximum: The highest UPS power load within the group.
- Power Average: The average UPS power load within the group.
- Battery Autonomy Minimum: The lowest UPS battery run time within the group.
- Battery Autonomy 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 Minimum: The lowest temperature within the group.
- Temperature Maximum: The highest temperature within the group.
- Temperature 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 Minimum: The lowest thermal device temperature within the group.
- Temperature Maximum: The highest thermal device temperature within the group.
- Temperature Average: The average thermal device temperature within the group.
- Capacity (%) Minimum: The lowest thermal device capacity within the group.
- Capacity (%) Maximum: The highest thermal device capacity within the group.
- Capacity (%) Average: The average thermal device capacity within the group.

### 5.4.3 List

The List view presents an inventory of all devices within the array manager's Device network. The inventory is subdivided into the following categories:

#### Rack PDU / RTS Units

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

- State: The status of the Geist™ rack device. Status is either normal or unavailable (loss of connectivity).
- Name: Geist™ rack 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 name is Unassigned.
- Energy: Geist™ rack device energy.
- Power: Total Geist™ rack device 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).
- 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.

## ENV (Environmental 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™ rack device label and MAC address.
- Temperature: 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™ rack devices 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™ rack device-connected Geist™ SRT, GTHD or GTHD3 sensors.

**NOTE: The name 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 deletes the device and any Environmental Sensors connected to it.**

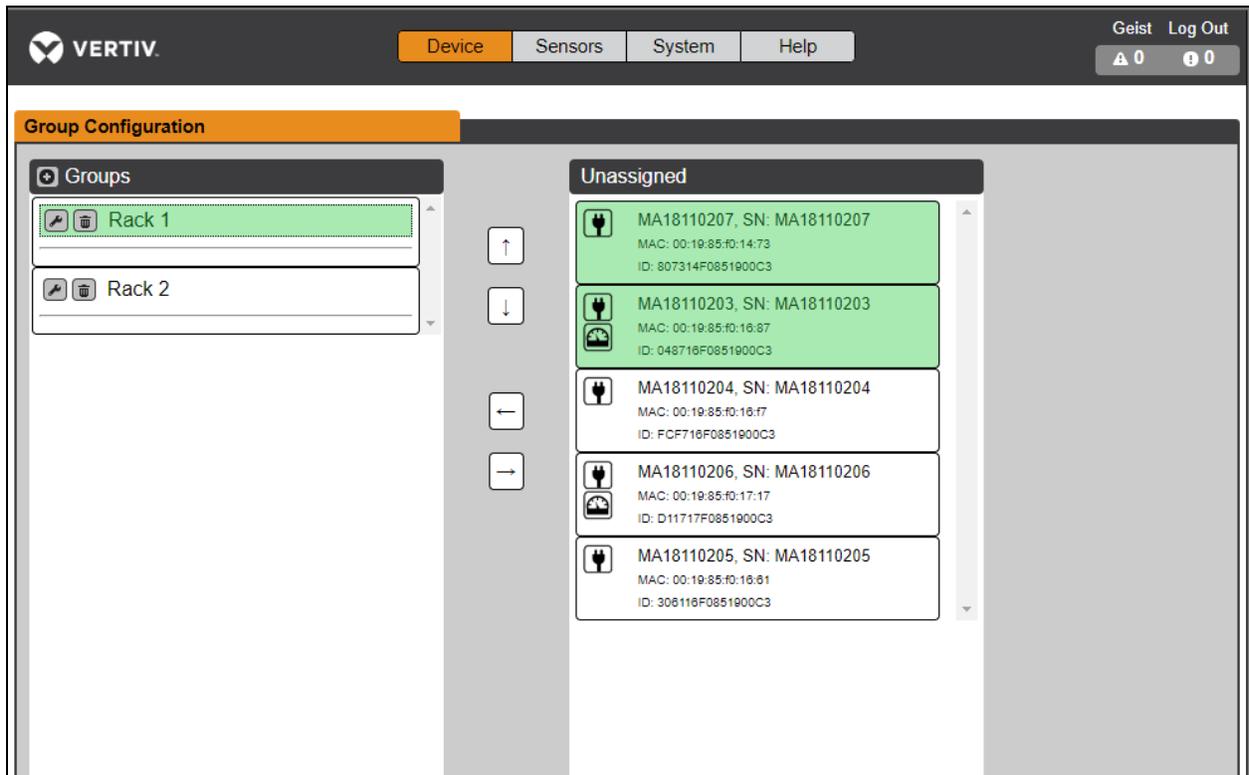
## Thermal Cooling

- 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: Thermal device temperature.
- Capacity (%): Thermal device capacity.

### 5.4.4 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.

Figure 5.4 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.**

**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.**

## 5.5 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.
2. Navigate to an *IP address* to access the web server interface of the device.  
-or-  
Click the *name of the device* to access the hyperlink to the web server.

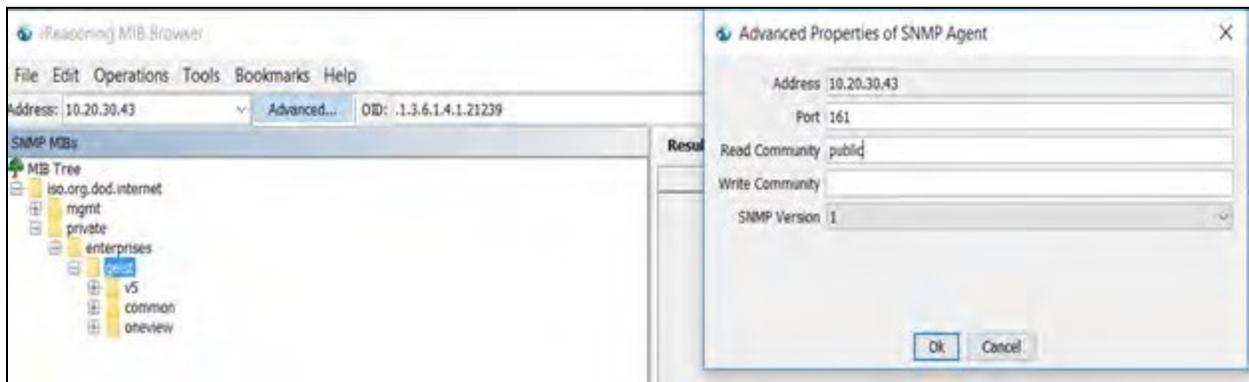
**To access Array Device SNMP Data:**

SNMP 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 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 5.5 MIB Browser**



## 5.5.1 Group SNMP Data

Aggregated data, both summary (such as total kWh and maximum kW) and group data, is available through the master Vertiv™ Geist™ rack device IP address and default SNMP Port 161. Within the MIB structure, the folders differentiate the data points available from the Master Geist™ rack device:

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

## 5.5.2 Tips and Troubleshooting

- 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 when logged into an array device.
- SNMP traps and alarms are routed from a device to the management network through the master device.

# Appendices

## Appendix A: Technical Support

### A.1 Resetting an Vertiv™ Geist™ rPDU / RTS Unit

If a Geist™ rack device 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 13.

### A.2 Service and Maintenance

No service or maintenance is required. Opening the Geist™ rack device may void the warranty. There are no user-serviceable parts inside the Geist™ rack device 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™ rack device is still connected to utility power. Refer the Geist™ rack device IMD Modules Replacement Guide for more information.

### A.3 More Technical Support

Technical support can be found at [www.Vertiv.com/support](http://www.Vertiv.com/support).

#### Americas

- Website: [www.Vertiv.com/geist](http://www.Vertiv.com/geist)
- Email: [geistsupport@vertiv.com](mailto:geistsupport@vertiv.com)
- Telephone: 1-888-630-4445

#### Europe and Middle East

- Technical Support: [www.Vertiv.com/en-emea/support](http://www.Vertiv.com/en-emea/support)
- Email: [eoc@Vertiv.com](mailto: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™ rack device 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™ rack device to send emails through your Exchange server, the following notes may help.

**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™ rack device 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™ rack device'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™ rack device 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™ rack device 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(s) 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 account, 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™ rack device 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.

## Appendix B: Visible Light Communication (VLC)

The VLC feature on Upgradeable Vertiv™ Geist™ PDUs allows the user to unobtrusively upload product information into a database management system via the embedded LED display. This product feature provides new opportunities to monitor and enable larger amounts of Geist™ rack device power data to be obtained via the unit's display and all without physically connecting to the Geist™ rack device.

Using a smart device, such as a smart phone or tablet with the Vertiv Mobile application installed, it is possible to capture data from the LED display when running in VLC mode, which can be enabled/disabled with the display buttons on the device or using the GUI on monitored units.

By default, the Upgradeable LED display will provide the current (Amps) per input and circuit breaker. By enabling the VLC feature, the LED display will scroll through a set of alphanumeric characters. Utilizing the Vertiv Mobile app, the user can scan the LED display and retrieve additional power metrics including Volts, Amps, Watts, Volt-Amps and Kilowatt Hours. Before VLC, the power data was available only on network-connected PDUs by viewing the GUI or using external software to collect and display the data. The VLC feature provides this data on local metered-only devices, as well as on monitored units without the need to connect them to the network.



**WARNING! This feature, when enabled, causes the unit to emit flashing lights, text or number sets at frequencies that can induce adverse reactions. Persons susceptible to adverse reactions as a result of such emissions or persons who have been diagnosed with epilepsy should not utilize or enable this feature.**

### To enable VLC:

Press the *center button* 3 times in less than 2 seconds.

**NOTE: With the release of firmware Version 3.3.0, Vertiv has added support for the VLC feature to all standard Metered and Monitored Upgradeable products, as well as a significant majority of its engineered-to-order range. Certain custom models of Upgradeable PDUs may not have VLC support within the Vertiv Mobile app. If your custom product is not supported by the Vertiv Mobile app it will be noted in the product specification sheet. Contact your sales representative if you would like assistance with this. The latest firmware updates can be found at [Vertiv.com/Firmware-Support](https://www.vertiv.com/Firmware-Support). Vertiv Mobile app is available in the App Store for iOS devices.**

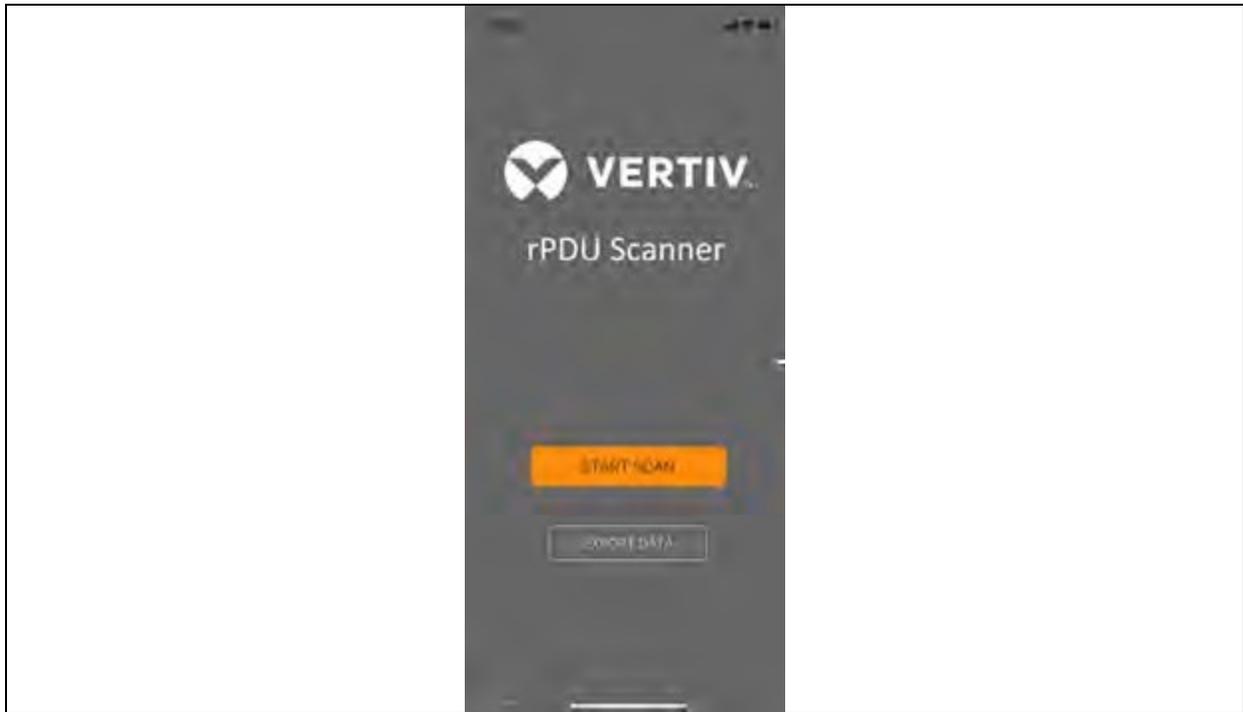
This page intentionally left blank

## Appendix C: Vertiv Mobile App

The Home screen allows the user to initiate a device scan or export data to a CSV file.

- Scan: Turns on scan mode to allow the app to capture VLC data from the Upgradeable Vertiv™ Geist™ rack device.
- Export: Pressing the Export button will launch the smart device's email app and attach the Database .csv file to be emailed to desired recipients.

Figure 8.1 Vertiv Mobile App Home Screen



### To scan a Geist™ rack device

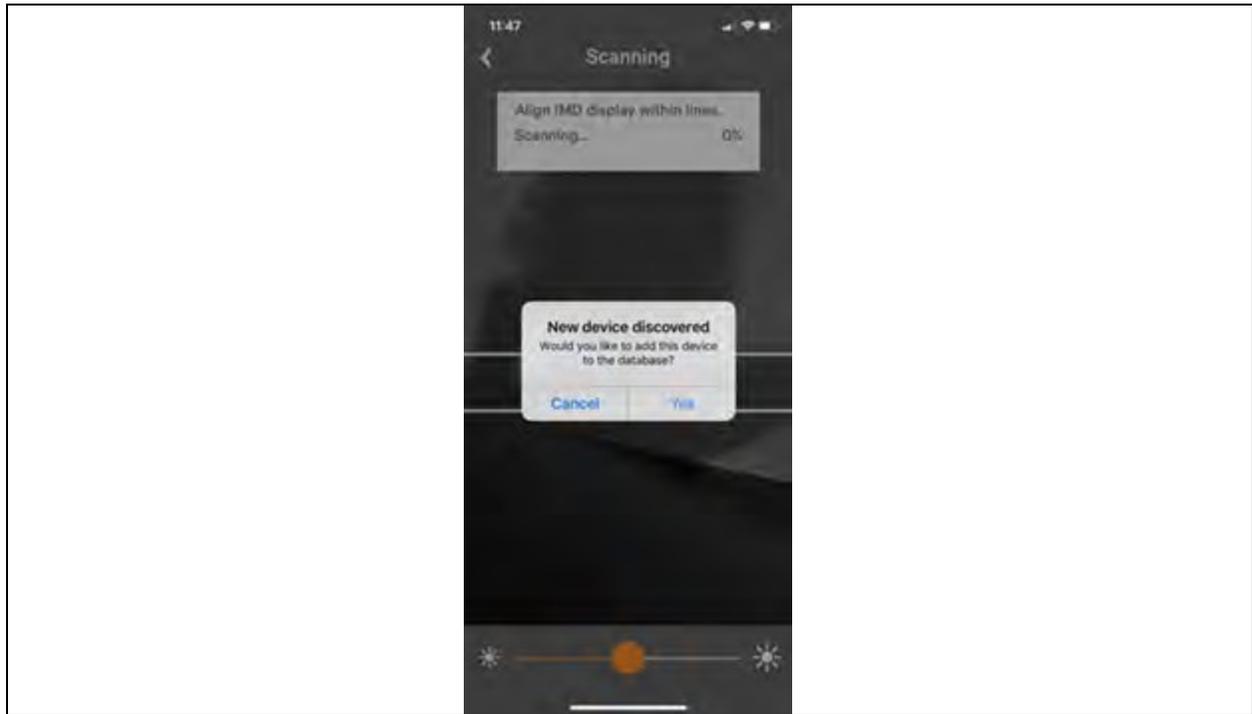
1. Press Scan on the Home screen to load the Vertiv Mobile App scanning engine.

**Figure 8.2 Vertiv Mobile App Scanning Screen**

2. Position the smart device so that the characters on the LED display are between the lines on the screen. The LED characters should be clear and in focus. If the characters appear too bright or too dark, the exposure setting can be adjusted with the sliding bar at the bottom of the screen. The app captures data as soon as it can see the LED characters inside the horizontal lines. Scan progress is displayed as a percentage. If the scan percentage is increasing slowly or resetting, the device has trouble in reading the data properly. In this case, try repositioning the device to improve results. After the scan reaches 100%, the app loads the Readings page.

**NOTE:** When a device is scanned for the first time, the Vertiv Mobile app recognizes the serial number as being new and asks if it should be added to the database as shown in the following image. If the device is added to the database, all future scanned data is added to the device serial number record.

Figure 8.3 Vertiv Mobile App New Device Screen



## C.1 Scanning Tips

The VLC feature relies on the light for its communication. If the lighting around the display or the lighting going through the lens of the smart device is not optimal, then the OCR (Optical Character Recognition) will struggle to capture the data. When looking at the smart device screen during capture, you can see if the characters of the LED display are in focus and bright. If they are blurred, with a surrounding glow or are faint, then the VLC capture will fail to work quickly and may be unable to scan at all.

### Proper capture methods

- High contrast between LED display and background
- No glow around LED display characters
- LED display characters between horizontal guidelines

### Improper capture methods

- Blurry image
- Overexposed image
- Glow around LED display characters
- LED display characters not between horizontal guidelines

## C.2 Failure Modes and Errors

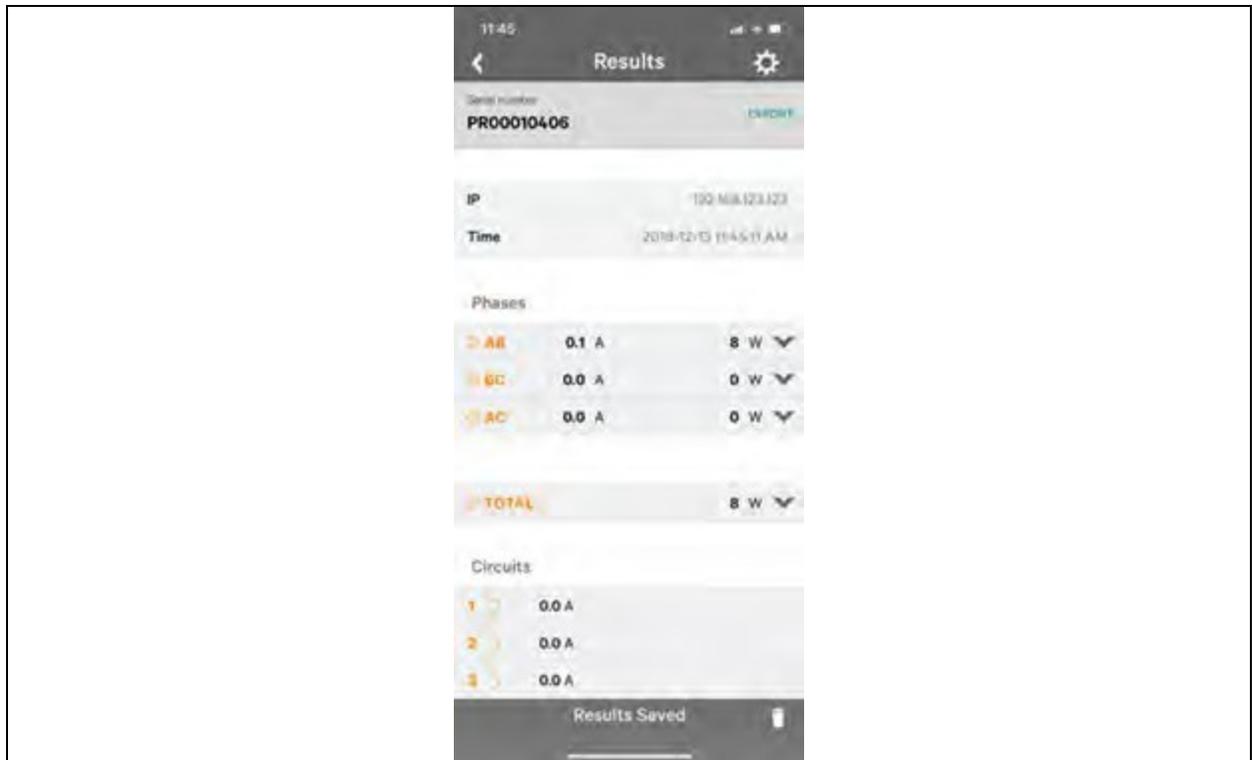
The Vertiv Mobile App retries a scan 2 times if the scan cannot be completed. The scan fails, if the smart device is unable to correctly capture all the VLC data correctly. One of the following messages is displayed:

- Scan failed: Incorrect set of configuration.
- Scan failed: Incorrect data sequence.
- Scan failed: Adjust your position or the exposure and try again. Press Cancel to return to the Home screen or Retry to return to the Scan page.

## C.3 Readings

The Readings screen displays scan results for each Vertiv™ Geist™ rack device scanned using VLC.

**Figure 8.4 Vertiv Mobile App Readings Screen**

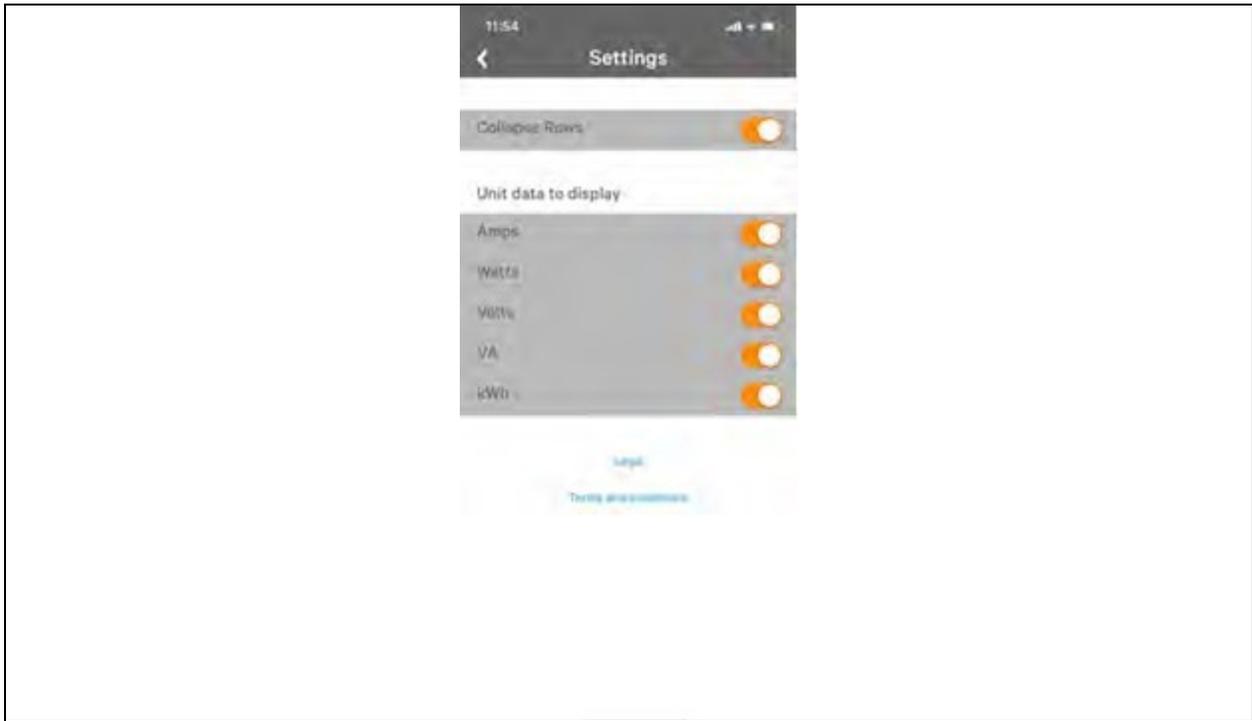


**NOTE:** The unit serial number is displayed in the title bar of the Readings screen. This serial number matches the serial number displayed on the surface of the Geist™ rack device.

Pressing the Settings icon enables the user to customized the data that is displayed in the scan results.

- Collapse Rows: Allows user to collapse or expand the Readings screen to help properly display data on smart devices with smaller screens.
- Unit Data to Display: Selects which data is shown on the Readings screen. All data is stored within the database regardless of settings here. These settings are global and will apply to any scanned unit.

Figure 8.5 Vertiv Mobile App Settings Screen



## C.4 Export

The Export button on the Home screen opens the smart device's default email app to send the database of scanned devices in .csv format to the desired recipients.

Figure 8.6 Vertiv Mobile App Export Screen



**NOTE: An email app must be properly configured on the smart device to utilize the Export function. The Vertiv™ Mobile App does not directly support email functionality. Vertiv cannot troubleshoot email errors as this could be an issue with either the device or with the email service being used.**

Each Vertiv™ Geist™ rack device you scan adds a new entry to the database. There is no limit to the number of individual Geist™ rack device that can be added, but the database has a limit of 10 scans per Geist™ rack device. Additional scans of the unit will overwrite the oldest data for that unit.

The .csv data output organizes data first by serial number and then by date and time. You can further organize the data by using the filter option in Microsoft Excel. The data structure is split into two sections: Geist™ rack device Configuration and power data.

The Geist™ rack device Configuration Data includes:

- Serial Number
- Frame Definition
- Date/Time stamp
- IPv4 address

The Power Data includes:

- Power Readings
- Totals

**Table 8.1 Geist™ Rack Device Configuration Data**

Serial number	FrameDef	yyyy-mm-dd-hh-mm-ss	IP add
Product's unique serial number. This is the same serial number present on the units label.	Part of the VLC configuration data and used for debugging.	Time stamp of when the scan occurred.	The IPv4 address of the unit. Locally Metered units will show Null IP address.

**Table 8.2 Power Data**

Volts	Amps	Watts	VA	kWh
1 Volt	1 Amp	1 Watt	1 VA	1 kWh
Input Phase for Single Phase units. Phase A or Phase AB if 3-Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours
2 Volts	2 Amps	2 Watts	2VA	2 kWh
Phase B or Phase BC if 3-Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours
3 Volts	3 Amps	3 watts	3 va	3 Kwh
Phase C or Phase AC if 3-Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours
4 Volts	4 Amps	4 Watts	4 VA	4 kWh
Secondary Input Phase for Single Phase units. Phase A or Phase AB if 3- Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours
5 Volts	5 Amps	5 Watts	5 VA	5 kWh
Secondary Phase B or Phase BC if 3-Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours
6 Volts	6 Amps	6 Watts	6 VA	6 kWh
Secondary Phase C or Phase AC if 3-Phase	Phase Amperes	Phase Real Power	Phase Apparent Power	Phase Kilowatt-Hours

**NOTE: Some Geist™ GU models have dual inputs with monitoring or dual Inline Monitoring; these units can have up to three additional power readings.**

**Table 8.3 Breakers/Circuits**

Breaker 1	Breaker 2	Breaker 3	Breaker 4	Breaker 5	Breaker 6
Breaker/Circuit 1 Amps	Breaker / Circuit 2 Amps	Breaker / Circuit 3 Amps	Breaker / Circuit 4 Amps	Breaker / Circuit 5 Amps	Breaker / Circuit 6 Amps

**Table 8.4 Totals**

Total Watts (Real Power)	Total VA (Apparent Power)	Total kWh
The total of Watts shown in sections 1-6	The total of VA shown in sections 1-6	The total kWh shown in sections 1-6

**NOTE: The tables above are an outline of data that is present in the database CSV file as is not representative of the actual format of the CSV file. Data stored will vary based on product configuration.**

This page intentionally left blank

## Appendix D: Available Sensors

### D.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.

### D.2 Analog I/O Sensors

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

### D.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.

### D.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 page.

**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. (180m) of sensor wire.**

This page intentionally left blank

## Appendix E: Outlet LEDs

**NOTE:** This appendix applies to Outlet Monitored / Outlet Switched Vertiv™ Geist™ rPDU / RTS Units 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 10.1 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 10.2 LED Status Description**

Measured voltage	Relay state	State	LED	
Measured voltage	Relay state	State	LED	
On	On or Unknown	Solid	Green	
Off	Off or Unknown	Solid	Red	
Off	On	Blinking <sup>1</sup>	Amber	Red
On	Off	Blinking <sup>2</sup>	Amber	Green
<sup>1</sup> Outlet is sensed to be Off but should be On.				
<sup>2</sup> 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

This page intentionally left blank

## Appendix F: IMD Display Codes

Table 11.1 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.

This page intentionally left blank

## Appendix G: 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™ rack device 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 (i.e. factory fresh) Geist™ rack device, 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 97 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, please refer to [Example 2](#) on page 98 at the end of this document.
9. After selecting Provisioner>Discovery>Update, enter the user name and password only when configuring previously configured Geist™ rack devices (the user name and password being that of the Geist™ rack devices being provisioned). Do not enter a user and password when configuring factory fresh units (identified by Provisioned attribute equaling False).

### Local Users

```

1 | { "auth": {
2 |   "username": {
3 |     "password": "userpw",
4 |     "enabled": true,
5 |     "control": false,
6 |     "admin": false,
7 |     "language": "en"}
8 | }}
9 |
```

Line Number	Description
2	The user name to be created (in quotes).
3	Password (in quotes).
4	Options true or false determines whether the user is enabled.
5	Options true or false determines whether the user will have control privileges.
6	Options true or false determines whether the user will have admin privileges.
7	Overrides default language for this user, valid options are "de", "en", "es", "fr", "ja", "ko", "pt", "zh".

## LDAP

```

1  {"conf":{
2  "remoteAuth": {
3  "mode":
4  "ldap", "ldap": {
5  "host": "192.168.123.1",
6  "port": 389,
7  "mode": "activeDirectory",
8  "securityType": "ssl",
9  "bindDn": "",
10 "password": null,
11 "baseDn": "",
12 "userFilter": "(objectClass=posixAccount)",
13 "userId": "uid",
14 "userIdNum": "uidNumber",
15 "groupFilter": "(objectClass=posixGroup)",
16 "groupId": "gidNumber",
17 "groupMemberUid": "memberOf",
18 "enabledGroup": "enabled",
19 "controlGroup": "control",
20 "adminGroup": "admin"}}
21 }}

```

Line Number	Description
5	LDAP URL (ref RFC4516 > RFC2255) (in quotes), required if LDAP is enabled.
6	Port for protocol communication.
7	Determines default compatibility among the different LDAP types, options are "openLdap or activeDirectory".
8	Encryption to be used in connecting to LDAP server, options are "ssl" and "starttls".
9	Distinguished Name (in quotes) (ref RFC4514 > RFC2253), used to bind to the directory server, blank string implies anonymous bind.
10	Password (in quotes) used to bind to the directory server.
11	Distinguished Name (in quotes) (ref RFC4514 > RFC2253) to use for the search base.
12	LDAP Search Filter (in quotes) (ref RFC4515 > RFC2254), objectClass equivalent to posixAccount (ref RFC2307).
13	Equivalent to attribute "uid" (in quotes) ref (RFC2307).
14	Equivalent to attribute "uidNumber" (in quotes) (ref RFC2307).
15	LDAP Search Filter (in quotes) (ref RFC4515 > RFC2254), objectClass equivalent to posixGroup (RFC2307).
16	Equivalent to attribute "gidNumber" (ref RFC2307) (in quotes).
17	Equivalent to attribute "memberUid" (ref RFC2307) (in quotes).
18	User (in quotes) in this group will have the "enabled" privilege.
19	User (in quotes) in this group will have the "control" privilege.
20	User (in quotes) in this group will have the "admin" privilege.

```

1  {"conf":{
2  "remoteAuth": {

```

```

3 | "mode": "tacacs",
4 | "tacacs": {
5 |   "authenticationServer1": "10.20.30.21",
6 |   "authenticationServer2": "10.20.30.70",
7 |   "accountingServer1": "10.20.30.21",
8 |   "accountingServer2": "10.20.30.70",
9 |   "sharedSecret": "secret",
10 |  "service": "raccess",
11 |  "adminAttribute": "admin=true",
12 |  "controlAttribute": "control=true",
13 |  "enabledAttribute": "enabled=true"}}
14 | }}

```

Line Number	Description
5	Primary authentication/authorization server (in quotes)
6	Alternate authentication/authorization server (in quotes)
7	Primary accounting server (in quotes)
8	Alternate accounting server (in quotes)
9	Secret (in quotes) shared by client and server (null deletes secret).
10	Value for the service field in TACACS requests. Options are "ppp" and "raccess"
11	User (in quotes) with this Attribute-Value Pair will have "admin" privilege.
12	User (in quotes) with this Attribute-Value Pair will have "control" privilege.
13	User (in quotes) with this Attribute-Value Pair will have "enabled" privilege.

## Radius

```

1 | {"conf":{
2 |   "remoteAuth": {
3 |     "mode": "radius",
4 |     "radius": {
5 |       "authenticationServer1": "",
6 |       "authenticationServer2": "",
7 |       "accountingServer1": "",
8 |       "accountingServer2": "",
9 |       "sharedSecret": "Secret",
10 |      "groupAttribute": "filter-id",
11 |      "adminGroup": "admin",
12 |      "controlGroup": "control",
13 |      "enabledGroup": "enabled"}}
14 |   }}

```

Line Number	Description
5	Primary authentication server (in quotes)
6	Alternate authentication server (in quotes)
7	Primary accounting server (in quotes)

Line Number	Description
8	Alternate accounting server (in quotes)
9	Secret shared by client and server in quotes).
10	Identifies the AVP that tells which access group the user belongs to, valid values are "filter-id" and "management-privilege-level".
11	User (in quotes) that belongs to this group has "admin" privilege.
12	User (in quotes) that belongs to this group has "control" privilege.
13	User (in quotes) that belongs to this group will have "enabled" privilege.

### Network Hostname and IP addresses

```

1  {"conf":{
2  "system": {
3  "hostname": "rPDUhostname",
4  "ip6Enabled": true},
5  "network": {
6  "ethernet": {
7  "label": "Bridge 0",
8  "enabled": true,
9  "dhcpOn": false,
10 "address": {
11 "0": {"address": "192.168.123.123", "prefix": 24},
12 "1": {"address": "10.20.30.43", "prefix": 24}}}}
13 }}

```

Line Number	Description
3	Name (in quotes) to identify the unit in a network
4	Options are true or false to enable or disable IPV6 support.
7	Bridge label (in quotes)
8	Options are true or false to enable or disable the network bridg.
9	Options are true or false to enable or disable DHCP.
10	IP address (in quotes) of the interface
11, 12	Prefix of the interface IP address

## Network Ports

```

1 | {"conf":{
2 |   "network": {
3 |     "port0": {
4 |       "label": "Port 0",
5 |       "enabled": true,
6 |       "stp": {"cost": 0}},
7 |     "port1": {
8 |       "label": "Port 1",
9 |       "enabled": true,
10 |      "stp": {"cost": 0}}}
11 | }}

```

Line Number	Description
4, 8	Port label (in quotes)
5, 9	Options are true or false to determine whether the port is enabled.
6, 10	Spanning tree cost for this port

## Network Routes

```

1 | {"conf":{
2 |   "network": {
3 |     "ethernet": {
4 |       "route": {
5 |         "0": {
6 |           "gateway": "10.20.30.254",
7 |           "prefix": 0,
8 |           "destination": "0.0.0.0"}}}}
9 | }}

```

Line Number	Description
6	Gateway address (in quotes) for the route
7	Network prefix, 0 for default gateway
8	Destination network address (in quotes), "0.0.0.0" for default network

## Network DNS

```

1 | {"conf":{
2 |   "network": {
3 |     "ethernet": {
4 |       "dns": {
5 |         "0": {"address": "8.8.8.8"},
6 |         "1": {"address": "8.8.4.4"}}}}
7 | }}

```

Line Number	Description
5, 6	The DNS server address (in quotes). Second occurrence is for the alternate DNS server.

## Network RSTP

```

1  {"conf":{
2  "network": {
3  "ethernet": {
4  "stp": {
5  "enabled": false,
6  "mode": "rstp",
7  "bridgePriority": 24576,
8  "helloTime": 2,
9  "maxAge": 40,
10 "maxHops": 40,
11 "forwardDelay": 21}}}
12 }}

```

Line Number	Description
5	Options are true or false, determines whether spanning tree protocol is enabled.
6	Options are "stp" or "rstp", RSTP mode supports falling back to STP when necessary.
7	This interface's spanning tree bridge priority.
8	The interval in seconds between periodic transmissions of configuration message.
9	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).
10	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".
11	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

```

1  {"conf":{
2  "http": {
3  "httpEnabled": true,
4  "httpPort": 80,
5  "httpsPort": 443}
6  }}

```

Line Number	Description
3	Options are true or false to allow unencrypted communications.
4	Port number for HTTP communication
5	Port number for HTTPS communication

## Reports

```

1  {"conf":{
2  "report": {
3  "0": {
4  "start": "00:00",
5  "days": "MTWTFSS",
6  "targets": ["1","2"],
7  "interval": 1},
8  "1": {
9  "start": "00:00",
10 "days": "MT   ",
11 "targets": ["1"],
12 "interval": 1}}
13 }}

```

Line Number	Description
4,9	Time of day from which interval is applied. Format is "(00-23):(00-59)" configurable in 15 minute increments.
5,10	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)
7,12	Number of hours between reports, can be 1, 2, 3, 4, 6, 8, 12, and 24.

## Display

```

1  {"conf":{
2  "display": {
3  "gmsd": {
4  "mode": "currentAndTotalPower",
5  "inverted": false,
6  "vlc": {"enabled": false}}}
7  }}

```

Line Number	Description
4	Selects a set of data to present on the display, options are "current", "totalPower", and "currentAndTotalPower".
5	Options are true or false to describe the current orientation of the display.
6	Options are true or false to determine rPDU / RTS Unit VLC display mode.

## Time

```

1  {"conf":{
2  "time": {
3  "mode": "ntp",
4  "datetime": "2021-03-09 12:05:36",
5  "zone": "UTC",
6  "ntpServer1": "0.pool.ntp.org",
7  "ntpServer2": "1.pool.ntp.org"}
8  }}

```

Line Number	Description
3	Mode, valid options are "ntp" and "manual".
4	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".
5	This must be a valid name (in quotes) from the tz database.
6	Primary NTP server address (in quotes), must only be used with mode="ntp".
7	Backup NTP server address (in quotes), must only be used with mode="ntp".

## SSH

```

1 | {"conf":{
2 |   "ssh": {
3 |     "enabled": true,
4 |     "port": 22}
5 |   }}

```

Line Number	Description
3	Options are true or false to enable or disable SSH.
4	Port number for SSH communication

## USB

```

1 | {"conf":{
2 |   "usb": {"enabled": true}
3 |   }}

```

Line Number	Description
2	Options are true or false, enables or disabled the USB port.

## Serial Port

```

1 | {"conf":{
2 |   "serial": {
3 |     "baudRate": 115200,
4 |     "dataBits": 8,
5 |     "enabled": true,
6 |     "parity": "none",
7 |     "stopBits": 1}
8 |   }}

```

Line Number	Description
3	Baud rate, options are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200.
4	Number of bits of data in one frame, options 7 and 8.
5	Options are true or false, enables or disabled the serial CLI on a device.
6	Parity bit type used in the frame, options "none", "even" and "odd".
7	Number of stop bits used to terminate each frame, options 1 and 2.

## Email

```

1  {"conf":{
2  "email": {
3  "server": "Example-server",
4  "port": 25,
5  "sender": "From email address",
6  "username": "username",
7  "password": "password",
8  "target": {
9  "0": {"name": "email1@domain.com"},
10 "1": {"name": "email2@domain.com"}}}
11 }}

```

Line Number	Description
3	SMTP sever address (in quotes)
4	SMTP port number
5	Senders email address (in quotes)
6	SMTP user name (in quotes)
7	SMTP password (in quotes)
9,10	Destination email address (in quotes)

## SNMP v1 or v2c

```

1  {"conf":{
2  "snmp": {
3  "v1v2cEnabled": true,
4  "port": 161,
5  "readCommunity": "public",
6  "writeCommunity": "private",
7  "trapCommunity": "private",
8  "target": {
9  "0": {
10 "port": 162,
11 "name": "10.20.30.10",
12 "trapVersion": "1"},
13 "1": {
14 "port": 162,
15 "name": "10.20.30.11",

```

```

16  "trapVersion": "1"},
17  "2": {
18  "port": 162,
19  "name": "10.20.30.12",
20  "trapVersion": "2c"}}}
21  }}

```

Line Number	Description
3	Options are true or false, enables or disables SNMP version 1 and 2c.
4	Port number for SNMP communication
5	Read community name (in quotes), must be different from writeCommunity
6	Write community name (in quotes), must be different from readCommunity
7	Trap community name (in quotes)
10, 14, 18	Port number for SNMP traps
11, 15, 19	Address (in quotes) for the SNMP trap destination
12, 16, 20	SNMP trap version, "1" or "2c"

### SNMP v3

```

1  {"conf":{
2  "snmp": {
3  "v3Enabled": true,
4  "port": 161,
5  "user": {
6  "0": {
7  "privPassword": "password",
8  "type": "read",
9  "username": "name",
10 "privType": "aes",
11 "authPassword": "password",
12 "authType": "sha1"},
13 "1": {
14 "privPassword": "password",
15 "type": "write",
16 "username": "name",
17 "privType": "none",
18 "authPassword": "password",
19 "authType": "none"},
20 "2": {
21 "privPassword": "password",
22 "type": "trap",
23 "username": "name",
24 "privType": "none",
25 "authPassword": "password",
26 "authType": "none"}}}
27 }}

```

Line Number	Description
3	Options are true or false, enable or disable SNMP version 1 and 2c.
4	Port number for SNMP communication
8, 15, 22	Permission type, possible values "read", "write" or "trap"
9, 16, 23	SNMPV3 user name (in quotes)
7, 14, 21	Privacy password (in quotes)
10, 17, , 24	Privacy encryption type, values "aes", "des" or "none"
11, 18, 25	Authentication password (in quotes)
12, 19, 26	Authentication type, values "sha1", "md5" or "none"

## Syslog

```

1 | {"conf":{
2 |   "syslog": {
3 |     "enabled": true,
4 |     "target": "10.20.30.40",
5 |     "port": 514}
6 |   }}

```

Line Number	Description
3	Options are true or false, enable the transmission of syslog messages to a remote destination.
4	Address (in quotes) of the remote destination for syslog messages
5	Destination port number for messages

## Admin

```

1 | {"conf":{
2 |   "contact": {
3 |     "description": " Geist GU PDU ",
4 |     "location": "Example Location",
5 |     "contactName": "Example Contact",
6 |     "contactEmail": "email@example.com",
7 |     "contactPhone": "123 456 789"},
8 |   "system": {"label": "System Label"}
9 |   }}

```

Line Number	Description
3	Unit description (in quotes)
4	Unit location (in quotes)
5	Unit contact name (in quotes)

Line Number	Description
6	Unit contact email (in quotes)
7	Unit contact phone number (in quotes)
8	Unit system label (in quotes)

## Locale

```

1 | {"conf":{
2 |   "locale": {
3 |     "defaultLang": "en",
4 |     "units": "metric"}
5 |   }}

```

Line Number	Description
3	Language, valid options are "de", "en", "es", "fr", "ja", "ko", "pt", "zh".
4	Units, valid options are "metric" and "imperial".

## Data Logging Interval

```

1 | {"conf":{
2 |   "datalog": {"interval": 15}
3 |   }}

```

Line Number	Description
2	The interval in minutes for data logging

## Aggregation

```

1 | {"conf":{
2 |   "oneview": {
3 |     "enabled": true,
4 |     "username": "x",
5 |     "password": "pass"}
6 |   }}

```

Line Number	Description
3	Options are true or false, determines whether aggregation is enabled.
4	User name (in quotes) to be set array devices.
5	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:

```
1  {"conf":{
2  "system": {
3  "hostname": "hostname1"},
4  "network": {
5  "ethernet": {
6  "dhcpOn": false,
7  "address": {
8  "0": {"address": "10.20.30.40","prefix": 24}}}}
9  ,
10 "network": {
11 "ethernet": {
12 "route": {
13 "0": {
14 "gateway": "10.20.30.254",
15 "prefix": 0,
16 "destination": "0.0.0.0"}}}}
17 ,
18 "network": {
19 "ethernet": {
20 "dns": {
21 "0": {"address": "8.8.8.8"},
22 "1": {"address": "8.8.4.4"}}}}
23 ,
24 "snmp": {
25 "v1v2cEnabled": true,
26 "port": 161,
27 "readCommunity": "public",
28 "writeCommunity": "private",
29 "trapCommunity": "private",
30 "target": {
31 "0": {
32 "port": 162,
33 "name": "10.20.30.60",
34 "trapVersion": "1"}}}
35 ,
36 "locale": {
37 "defaultLang": "en",
38 "units": "metric"}
39 }}
```

## Example 2

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

```

1  { "auth": {
2    "username": {
3      "password": "userpw",
4      "enabled": true,
5      "control": false,
6      "admin": false,
7      "language": "en"}
8  },
9  "conf":{
10   "http": {
11     "httpEnabled": false}
12  ,
13   "time": { "mode": "ntp",
14     "zone": "UTC",
15     "ntpServer1": "0.pool.ntp.org", "ntpServer2": "1.pool.ntp.org"} }}

```

## Sensor Settings and Alarms

```

1  {"dev": {
2    "0000000000000000": {
3      "label": "PDU 22A",
4      "type": "i03",
5      "conf": {"outletControlEnabled": true},
6      "outlet": {
7        "0": {
8          "poaAction": "last",
9          "rebootHoldDelay": 10,
10         "rebootDelay": 5,
11         "poaDelay": 1.25,
12         "onDelay": 5,
13         "mode": "manual",
14         "offDelay": 5,
15         "label": "Outlet 1"
16       }, "1": {
17         "poaAction": "last",
18         "rebootHoldDelay": 10,
19         "rebootDelay": 5,
20         "poaDelay": 1.50,
21         "onDelay": 5,
22         "mode": "manual",
23         "offDelay": 5,
24         "label": "Outlet 2"
25       }
26     },
27     "entity": {
28       "total0": {"label": "Total"},
29       "breaker0": {"label": "Circuit 1"},
30       "breaker1": {"label": "Circuit 2"},
31       "phase0": {"label": "Phase A"},
32       "phase1": {"label": "Phase B"},
33       "phase2": {"label": "Phase C"},
34       "line3": {"label": "Neutral Line"}

```

```

35 }
36 }
37 },
38 "alarm": {
39 "action": {
40 "0": {
41 "target": "trap0", "delay": 0,
42 "repeat": 0
43 }, "1": {
44 "target": "email0", "delay": 0,
45 "repeat": 0
46 }
47 },
48 "trigger": {
49 "0": {
50 "path": "0000000000000000/entity/phase0/measurement/0",
51 "severity": "alarm",
52 "type": "high",
53 "threshold": 222.0,
54 "tripDelay": 0,
55 "clearDelay": 1,
56 "latching": false,
57 "selectedActions": ["0","1"]
58 }, "1": {
59 "path": "0000000000000000/outlet/0/measurement/0",
60 "severity": "alarm",
61 "type": "low",
62 "threshold": 55.0,
63 "tripDelay": 2,
64 "clearDelay": 0,
65 "latching": false,
66 "selectedActions": ["0"]
67 }, "2": {
68 "path": "0000000000000000/entity/breaker0/measurement/4",
69 "severity": "alarm",
70 "type": "high",
71 "threshold": 12.0,
72 "tripDelay": 0,
73 "clearDelay": 0,
74 "latching": false,
75 "selectedActions": ["0"]
76 },
77 "3": {
78 "path": "0000000000000000/entity/total0/measurement/0",
79 "severity": "alarm",
80 "type": "high", "threshold": 7200.0,
81 "tripDelay": 0,
82 "clearDelay": 0,
83 "latching": false,
84 "selectedActions": ["0"]
85 }
86 }
87 }}

```

0000000000000000	The device-id (found on the sensors>overview page) of the rack device 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 rack device label (shown on the sensors>overview page).
type	Must have the value "i03". If omitted, prevents any selected rack devices being configured when the device-id does not match that of any rack device.
outletControlEnabled	Applies to outlet switched rack devices only and determines whether it is possible to control outlets on an outlet switched rack device. The value true allows outlets to be controlled, the value false prevents outlets from being controlled.
outlet	The outlet section applies to outlet switched rack devices only and defines settings for each rack device outlet. Note that outlet numbering starts with 0 (rack device 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 use-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 rack device 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.
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 rack device inlet phase measurements, where phase0 refers to the first rack device input phase, phase1 refers to the second phase (if present) etc. The number immediately following measurement indicates the type of measurement to alarmed as defined below: 0: Voltage 4: Current

	<p>8: Real power</p> <p>9: Apparent power</p> <p>10: Power Factor</p> <p>11: Energy</p> <p>14: Current crest factor</p> <p>"0000000000000000/outlet/0/measurement/0" defines outlet alarms for rack devices 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 alarmed as defined below:</p> <p>0: Voltage</p> <p>4: Current</p> <p>8: Real power</p> <p>9: Apparent power</p> <p>10: Power Factor</p> <p>11: Energy</p> <p>12: Balance</p> <p>14: Current crest factor</p> <p>"0000000000000000/entity/total0/measurement/0" defines alarms for rack device phase total inlet measurements. The number immediately following measurement indicates the type of measurement to alarmed as defined below:</p> <p>0: Real power</p> <p>1: Apparent power</p> <p>2: Power Factor</p> <p>3: Energy</p> <p>"0000000000000000/entity/breaker0/measurement/4" defines alarms for rack device 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 alarmed as defined below:</p> <p>4: Current</p> <p>"0000000000000000/entity/line3/measurement/4" defines alarms for rack device neutral current alarms. The number immediately following measurement indicates the type of measurement to alarmed as defined below:</p> <p>0: Current</p>
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.
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. E.g. ["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

## Appendix H: Provisioner Error Codes

### H.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
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, e.g. 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 Error

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.
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.
OneView missing credentials	Enabling OneView requires that a OneView username and password be set.
Time not settable	Setting date time requires manual time mode.

## 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

## Appendix I: An Example of Configuring LDAP for Active Directory Credentials

The following pages provide an example of configuring LDAP for active directory credentials.

### 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 be designated into one of the three IMD roles based on the user's Active Directory security group.

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.

### General Requirements and Notes

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

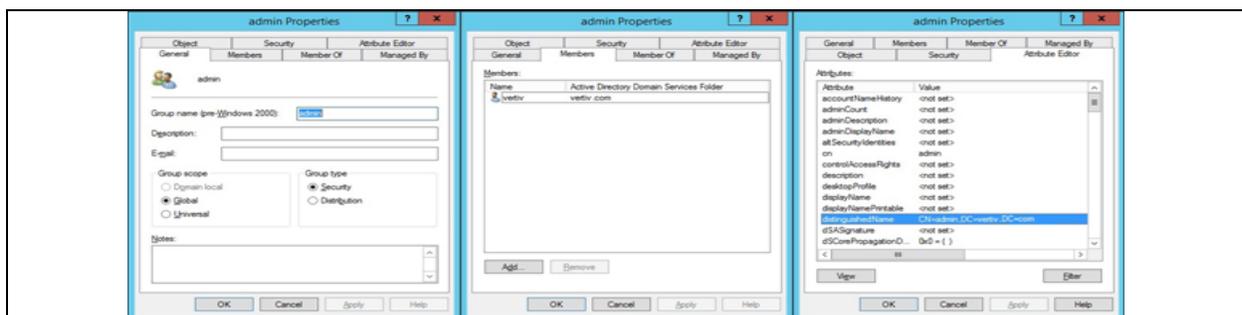
### Active Directory Configuration Procedure

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

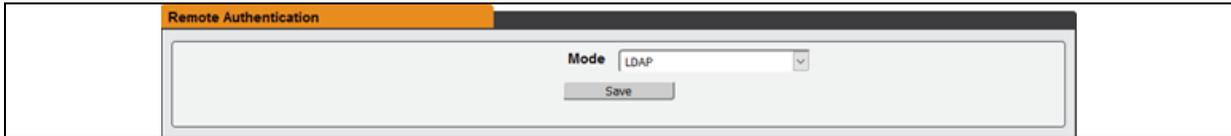
Figure 14.1 Setting of Admin Properties



### IMD Configuration Procedure (Web Interface)

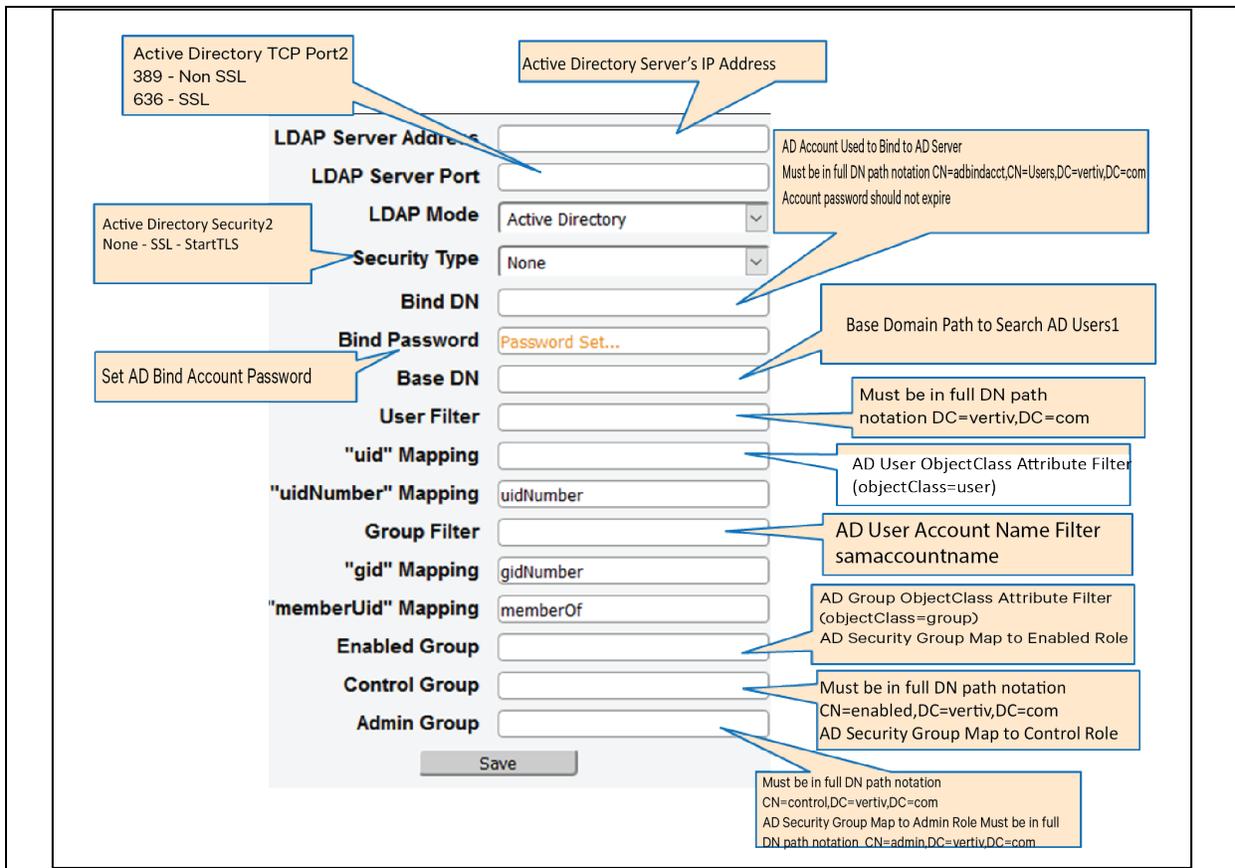
- Open a web browser to the IP or DNS name of the IMD and login as the local admin account.
- Navigate to System -> Remote Authentication.
- Set Remote Authentication Mode to "LDAP" and save.

Figure 14.2 Selection of Remote Authentication Mode



- Refer to Figure 14.3 below for descriptions of the LDAP section settings.

Figure 14.3 Overview of LDAP Section Settings



<sup>1</sup>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

<sup>2</sup>StartTLS uses TCP port 389. It initially establishes the session unencrypted but will encrypt the session from that point forward if the LDAP\_START\_TLS\_OID request is accepted by the Active Directory server.

### **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

©2023 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-70891\_REVB\_10-23