



Geist™

Intelligent Rack PDU

Installer/User Guide

Switched, Unit and Outlet Monitored Upgradeable

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages resulting from use of this information or for any errors or omissions. Refer to other local practices or building codes as applicable for the correct methods, tools, and materials to be used in performing procedures not specifically described in this document.

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

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

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. Visit <https://www.Vertiv.com/en-us/support/> for additional assistance.

TABLE OF CONTENTS

1 Overview	1
1.1 Environmental	1
1.2 Electrical	1
1.3 Networking	2
1.3.1 Ethernet	2
1.3.2 Protocols	2
1.3.3 User interfaces	2
1.3.4 Regulatory compliance	2
2 Installation	5
2.1 Mounting	5
2.1.1 Power Connection	18
2.1.2 U-Lock Operation	18
3 Setup	19
3.1 Interchangeable Monitoring Device (IMD-3E)	19
3.1.1 Enhanced Switched Monitored	19
3.1.2 Enhanced Switched Monitored with RS-232	21
3.1.3 Rapid Spanning Tree Protocol (RSTP)	23
3.2 Network Setup	23
3.3 Web Interface	27
3.3.1 Home Page	27
3.3.2 Sensors Tab	28
3.3.3 System Tab	35
3.3.4 Help Tab	51
4 Vertiv™ Intelligence Director	53
4.1 Aggregation	53
4.2 Master rPDU	53
4.3 Network Configuration	54
4.3.1 Downstream Devices	54
4.4 Views	56
4.4.1 Summary	57
4.4.2 Groups	58
4.4.3 List	59
4.4.4 Group Configuration	60
4.5 Interfaces	61
4.5.1 Group SNMP Data	62
4.5.2 Tips and Troubleshooting	62
5 Appendices	63
Appendix A: Technical Support	63

Appendix B: Visible Light Communication (VLC)	64
Appendix C: Vertiv™ Mobile App	65
Appendix D: Available Sensors	72
Appendix E: Outlet LEDs	72
Appendix F: IMD Display Codes	74

1 OVERVIEW

The Upgradeable second generation (GU2) product is a high-tier, rack-level power distribution unit (rPDU) with input and output monitoring, outlet level switching, remote network access via an embedded Vertiv™ API and with external sensor support via built-in Enhanced Communications (EC) card. The embedded, web-based graphical user interface (GUI) provides access to user product configuration and data logging.

GU2 PDUs are available in a wide range of SKUs to support all standard global input voltages, enterprise and hyperscale rack loads of over 20 kVA and single-phase and three-phase Delta or Wye building wiring configurations.

Table 1.1 GU2 Families

	INPUT POWER MONITORING	OUTLET LEVEL POWER MONITORING	OUTLET LEVEL SWITCHING
Switched Input Level Monitoring EC	X	—	X
Outlet Level Monitoring EC	X	X	—
Switched Outlet Level Monitoring EC	X	X	X

1.1 Environmental

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

Table 1.2 Temperature Limits

DESCRIPTION	MINIMUM	MAXIMUM
Operating	10°C (50°F)	60°C (140°F) UL Listed Models 50°C (122°F) CE Marked Models
Storage	-40°C (-40°F)	70°C (158°F) max

Table 1.3 Humidity Limits

DESCRIPTION	MINIMUM	MAXIMUM
Operating	5%	95% (non-condensing)
Storage	5%	95% (non-condensing)

Table 1.4 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)

1.2 Electrical

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

Table 1.5 Receptacle Ratings

TYPE	RATINGS
NEMA 5-15R or L5-15R	125VAC, 12A
NEMA 5-20R or L5-20R	125VAC, 16A
NEMA 6-20R or L6-20R	250VAC, 16A
NEMA L5-30R	125VAC, 24A
NEMA L6-30R	250VAC, 24A
IEC-60320 C13	250VAC, 10A (UL & CSA 12A, 250VAC)
IEC-60320 C19	250VAC, 16A (UL & CSA 16A, 250VAC)
U-Lock Locking IEC-60320 C13	250VAC, 10A (UL & CSA 12A, 250VAC)
U-Lock Locking IEC -60320 C19	250VAC, 16A (UL & CSA 16A, 250VAC)

1.3 Networking

The product communications requirements are defined in the next sections.

1.3.1 Ethernet

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

1.3.2 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, DHCP, SNMP (V1/V2c/V3), LDAP, TACACS+, RADIUS, NTP, SSH, RS232 and Syslog.

1.3.3 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).

1.3.4 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:
 - i. This device may not cause harmful interference
 - ii. 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.

ROHS/WEEE

RoHS, also known as Lead-free, stands for Restriction of Hazardous Substances. RoHS, originated in the European Union and restricts the use of six hazardous materials found in electrical and electronic products. All applicable products in the EU market after July 1, 2006, must pass RoHS compliance. RoHS impacts the entire electronics industry and many electrical products as well.

WEEE stands for Waste from Electrical and Electronic Equipment. WEEE Directive 2002/96/EC mandates the treatment, recovery and recycling of electric and electronic equipment (90% ends up in landfills). All applicable products in the EU market must pass WEEE compliance and carry the Wheelie Bin sticker.

See product label for RoHS/WEEE compliance marks.

This page intentionally left blank

2 INSTALLATION

Using the images in the mounting section, install your rack PDU.

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

To install your unit:

1. Using appropriate hardware, attach the unit to the rack.
2. Plug the rPDU into an appropriately rated and protected branch circuit receptacle.
3. Plug in the devices to be powered by the rPDU.
4. Turn on each device connected to the rPDU.

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

2.1 Mounting

Optional brackets are sold separately.

Figure 2.1 Full-Length Brackets

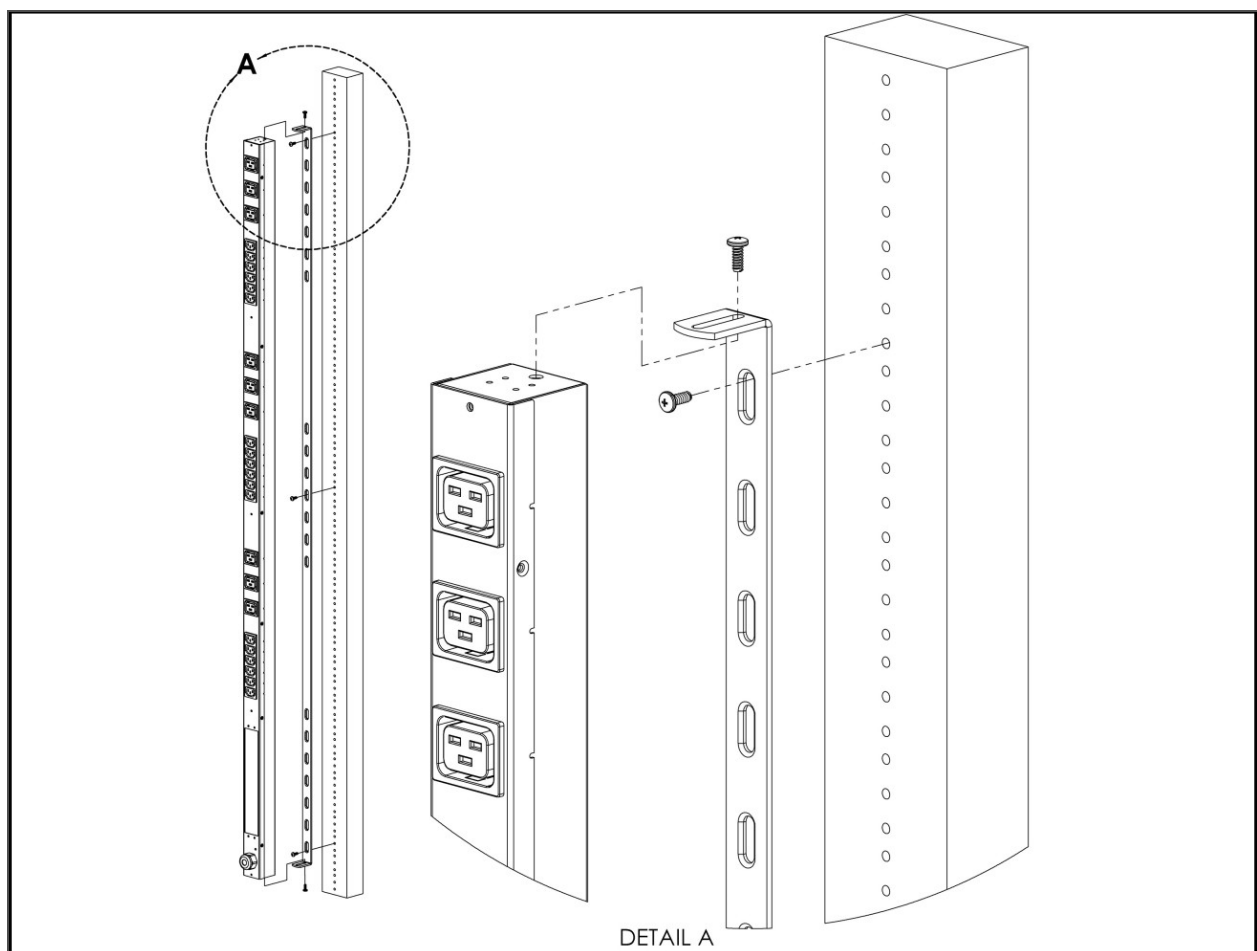


Figure 2.2 Mini L Brackets

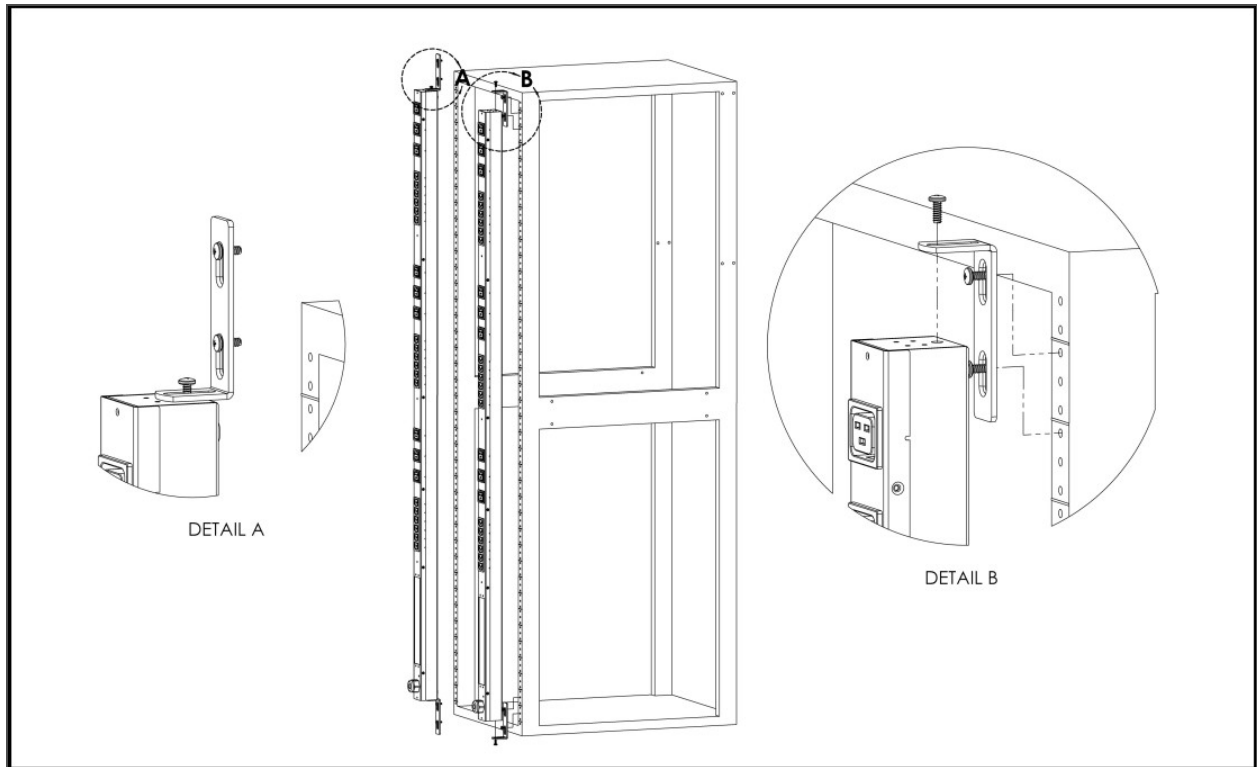


Figure 2.3 Vertical Extension Brackets

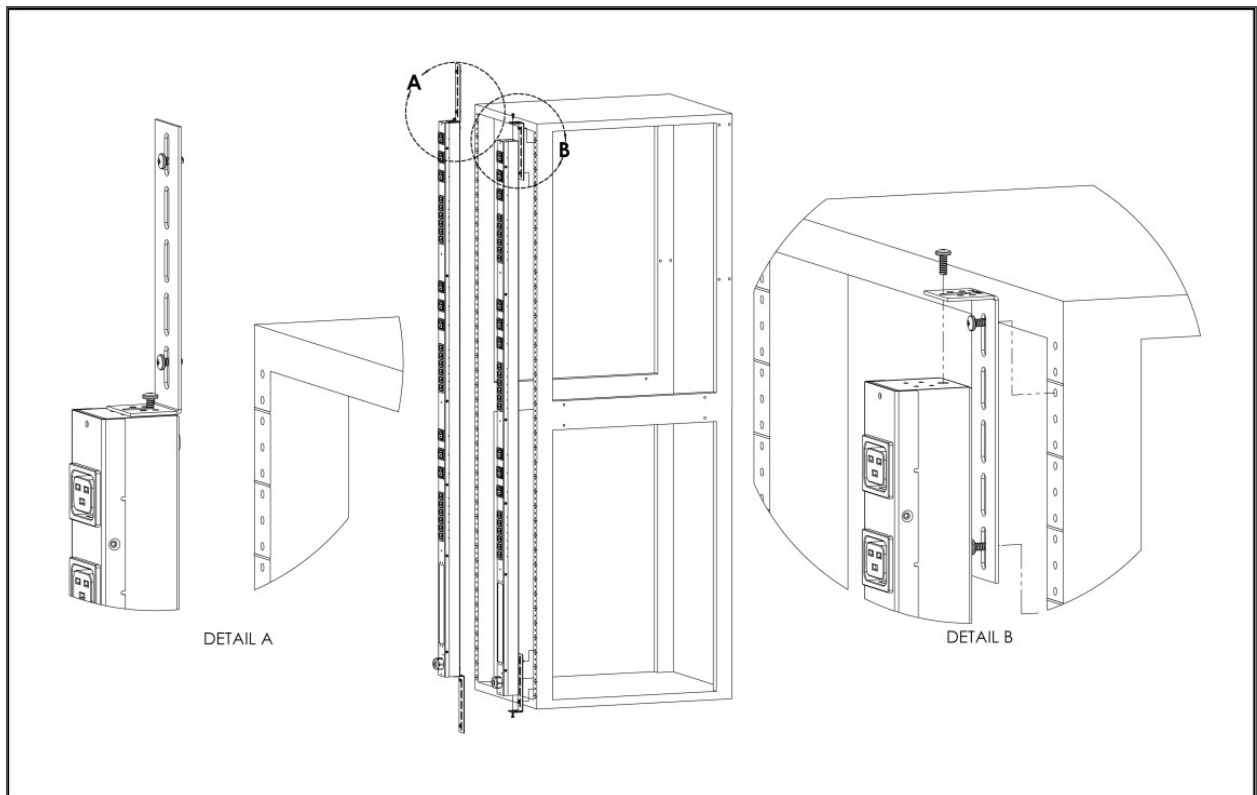


Figure 2.4 Toolless Mounting Hardware

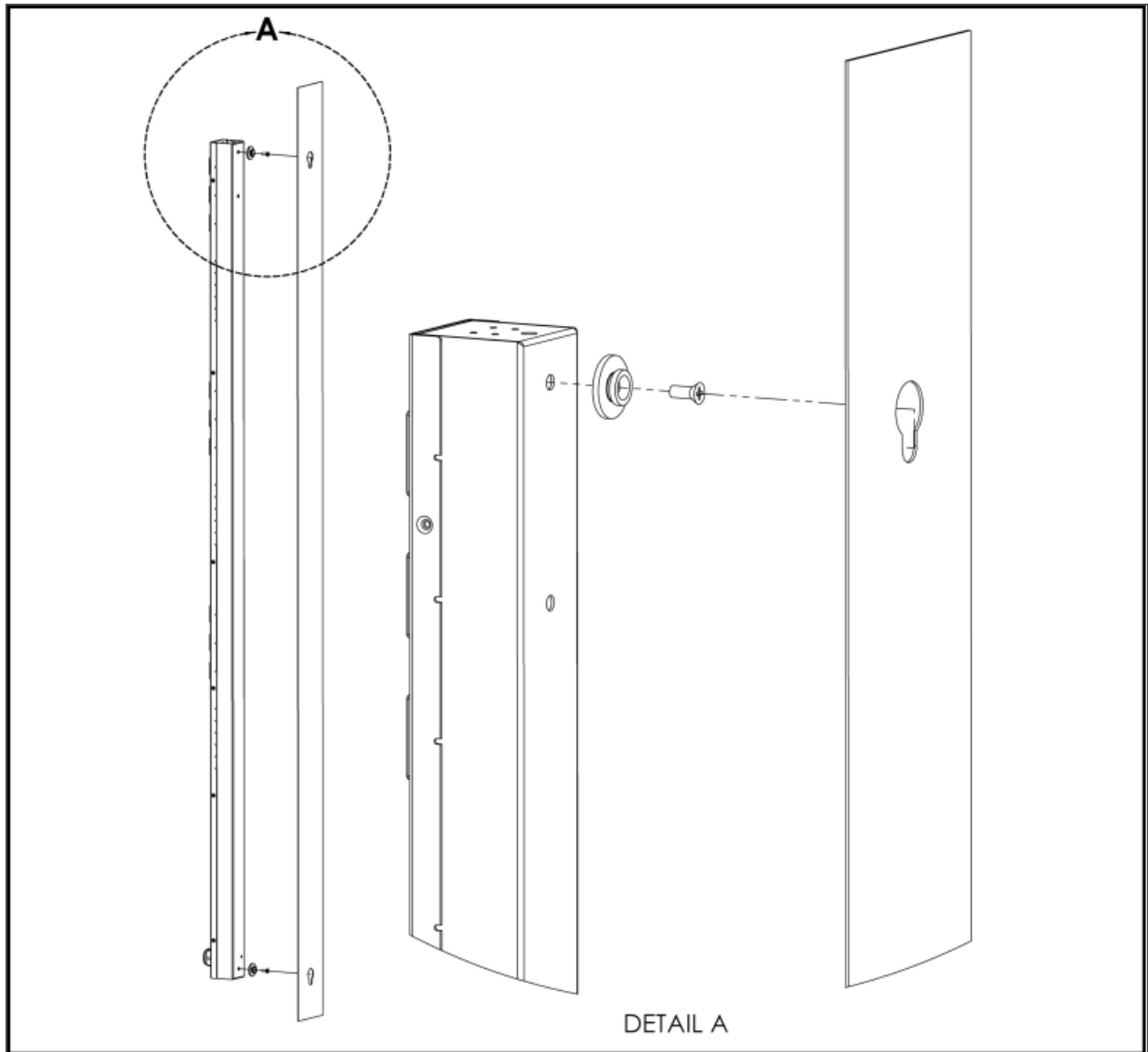


Figure 2.5 Toolless Full-Length Brackets

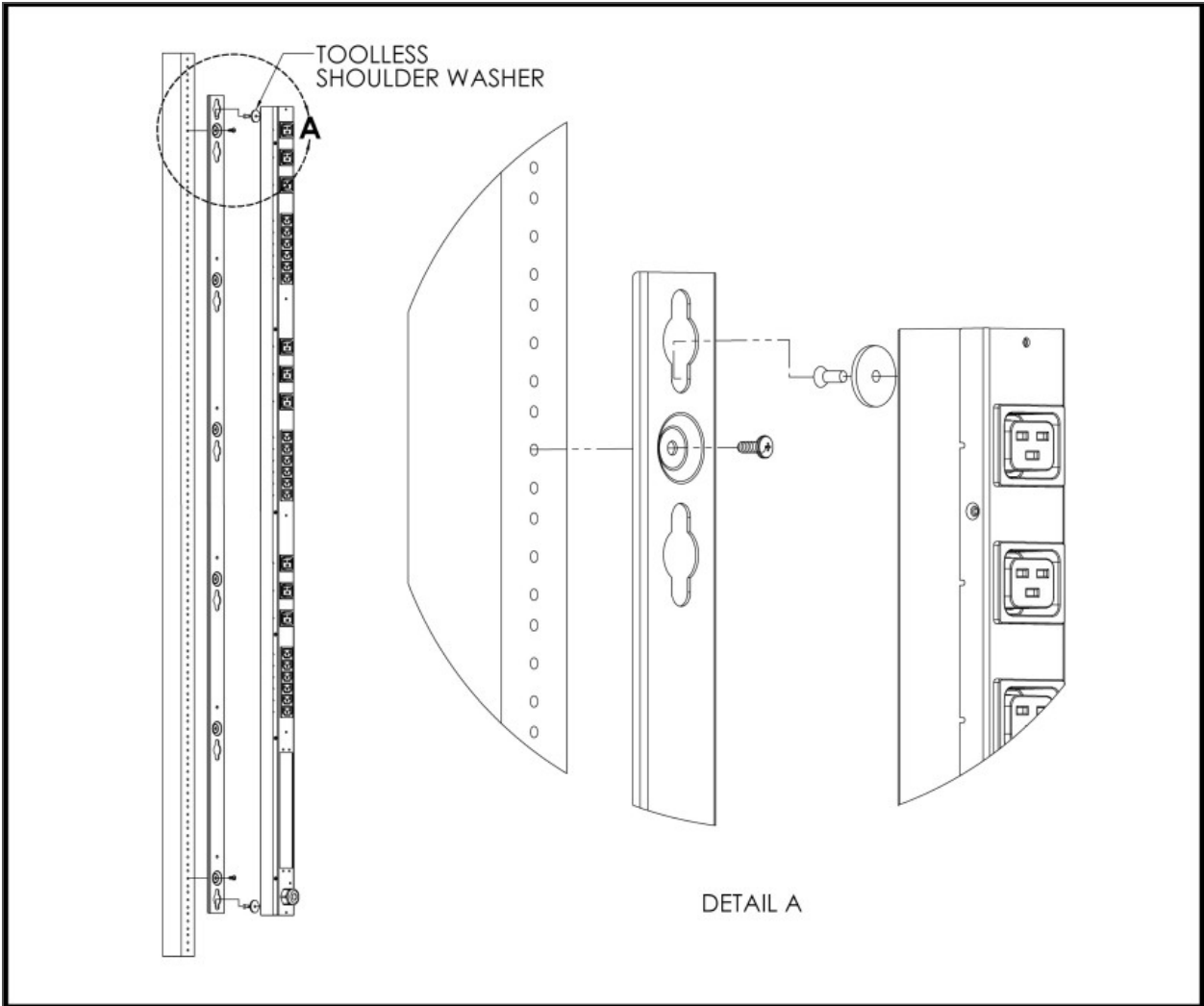


Figure 2.6 Single Side-Mount Two-Units Brackets

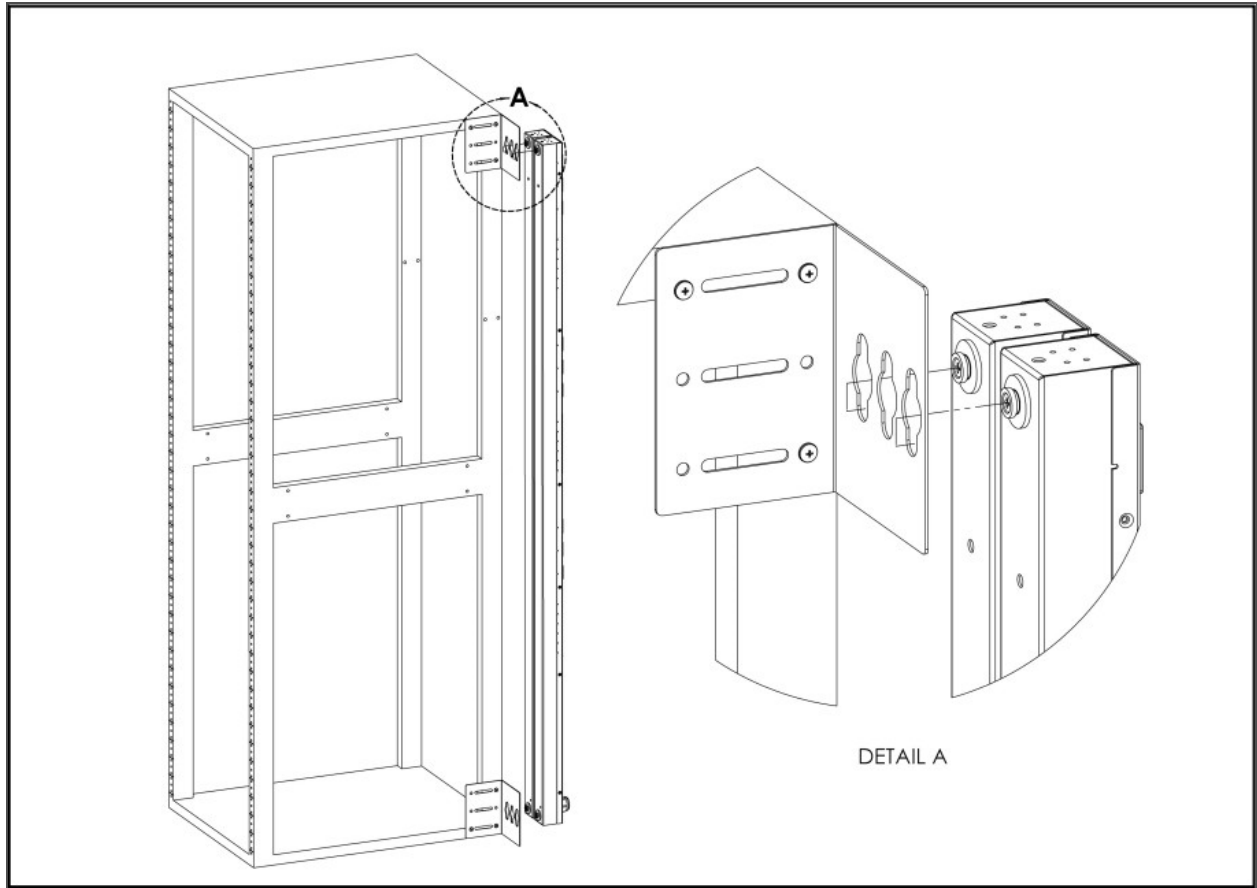


Figure 2.7 Offset/Side-Mount Brackets

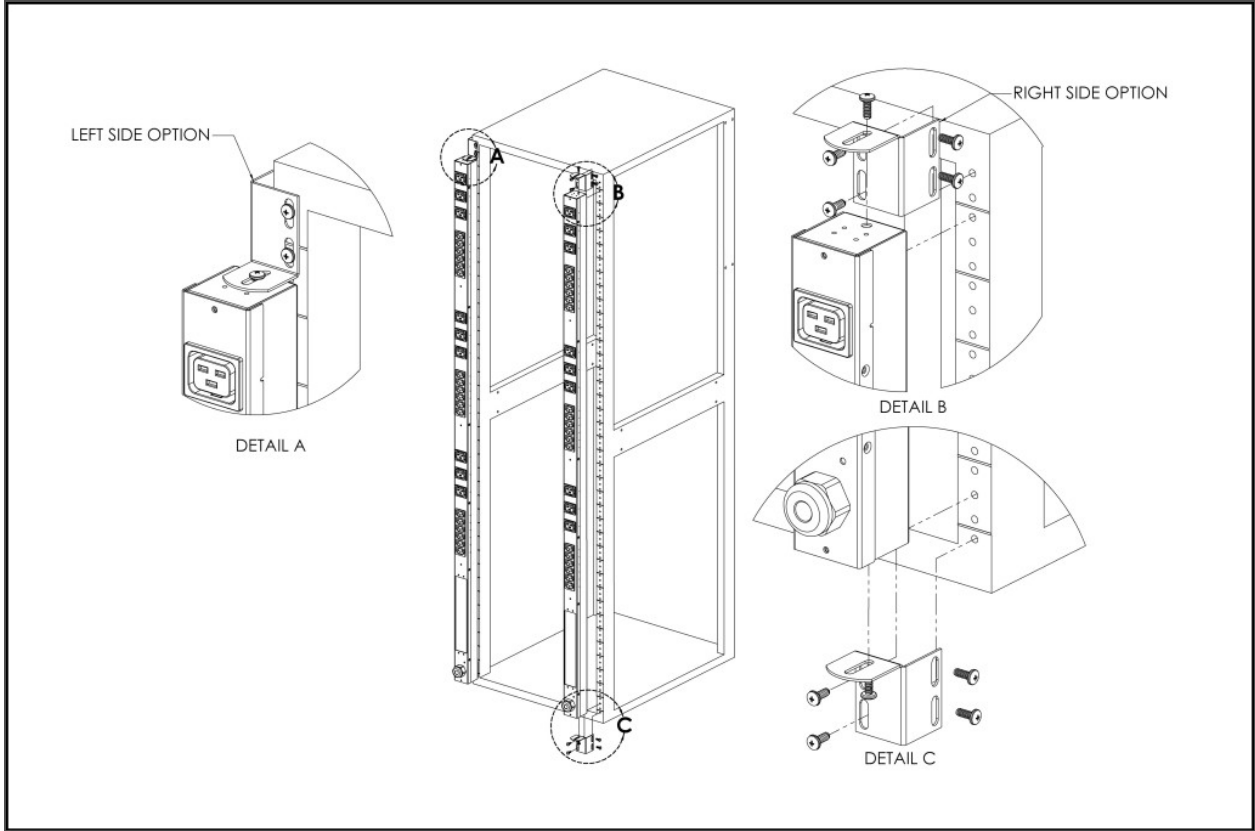


Figure 2.8 7" (inch) Extension Brackets

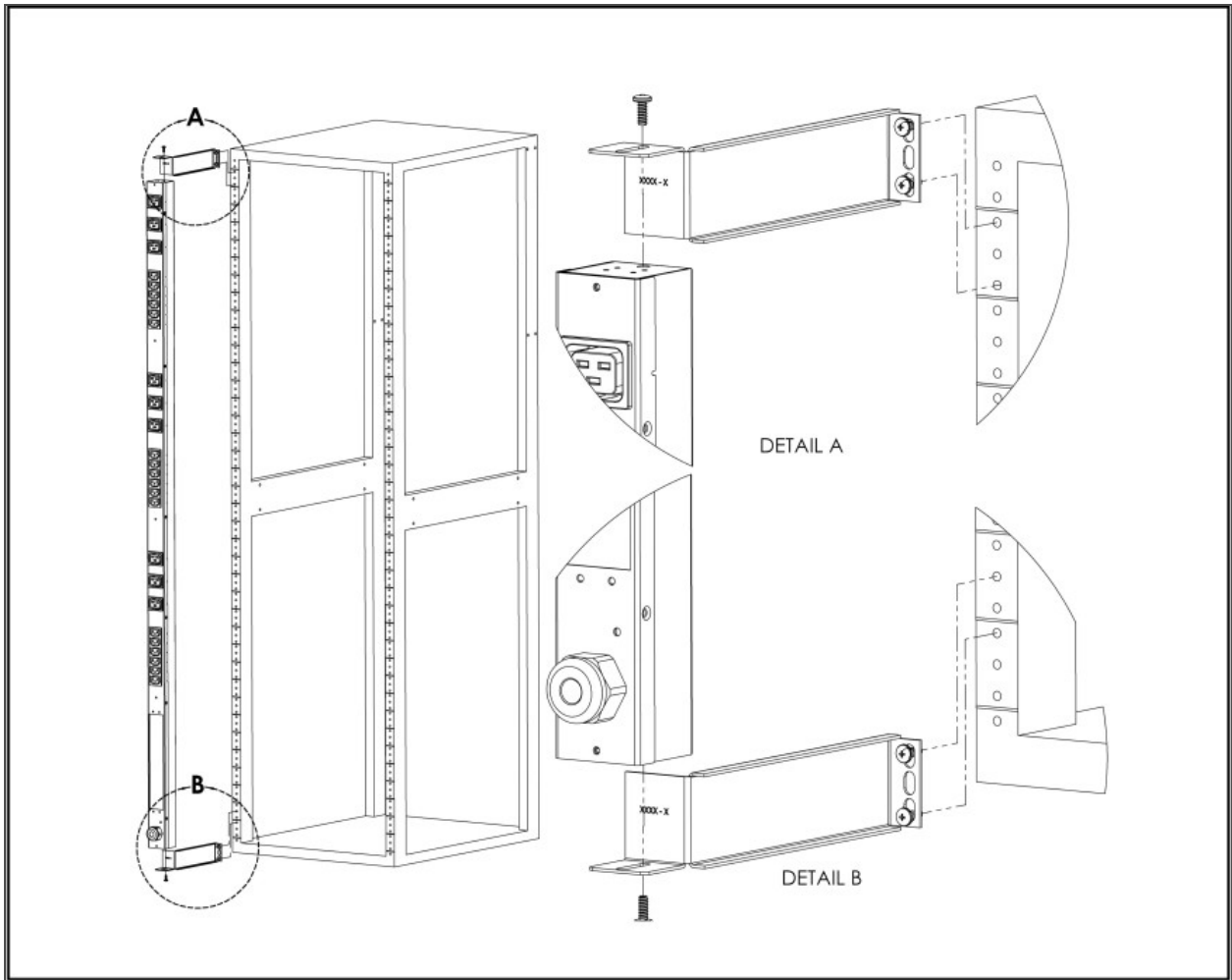


Figure 2.9 Flush-Mount Bracket

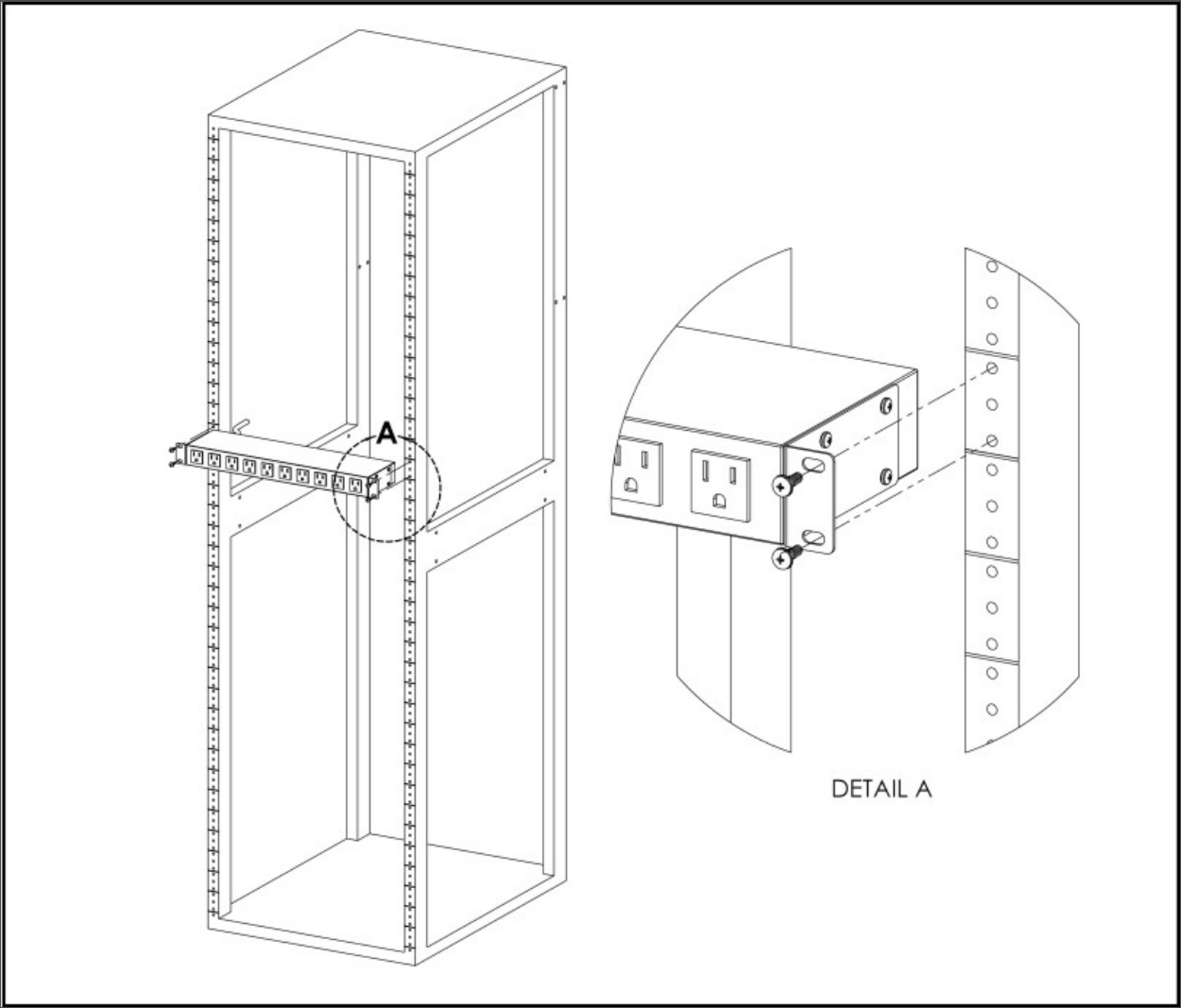


Figure 2.10 Adjustable-Mount Bracket

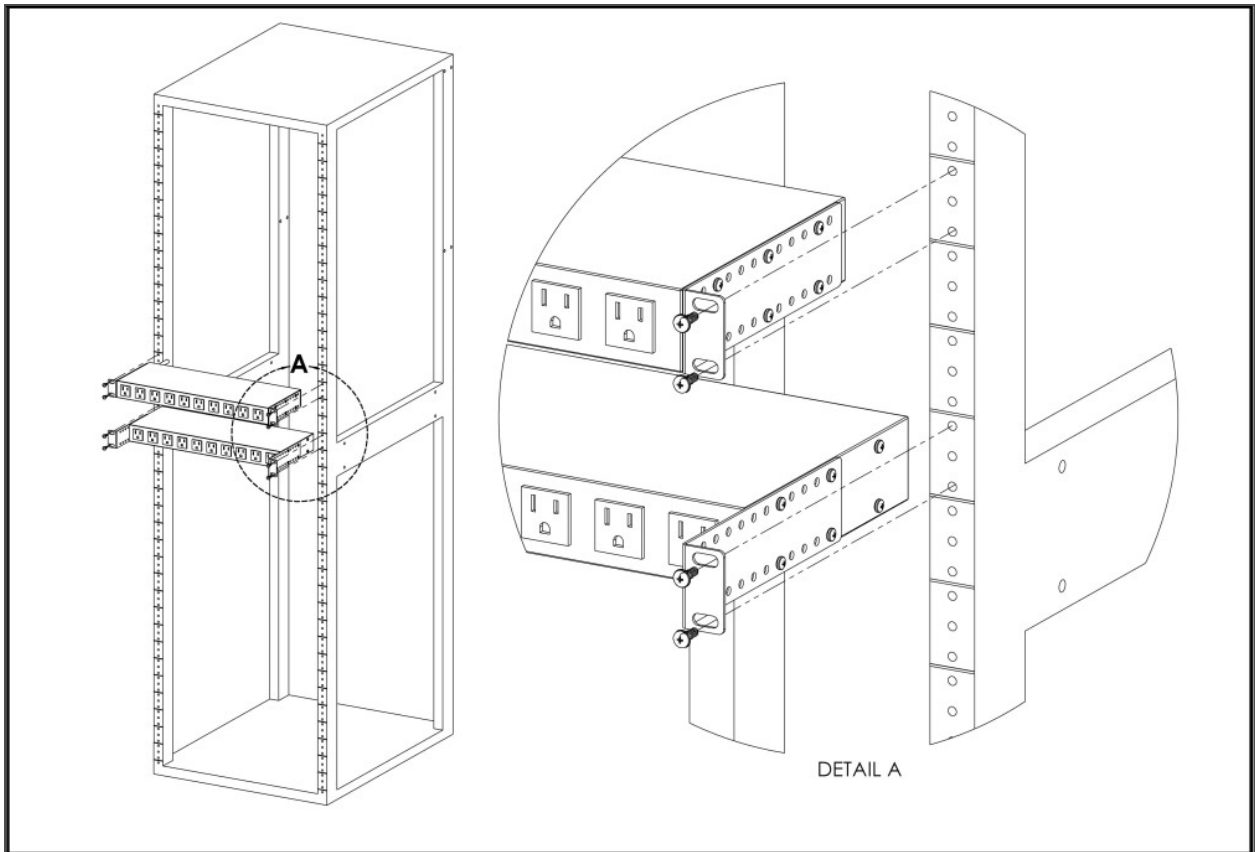
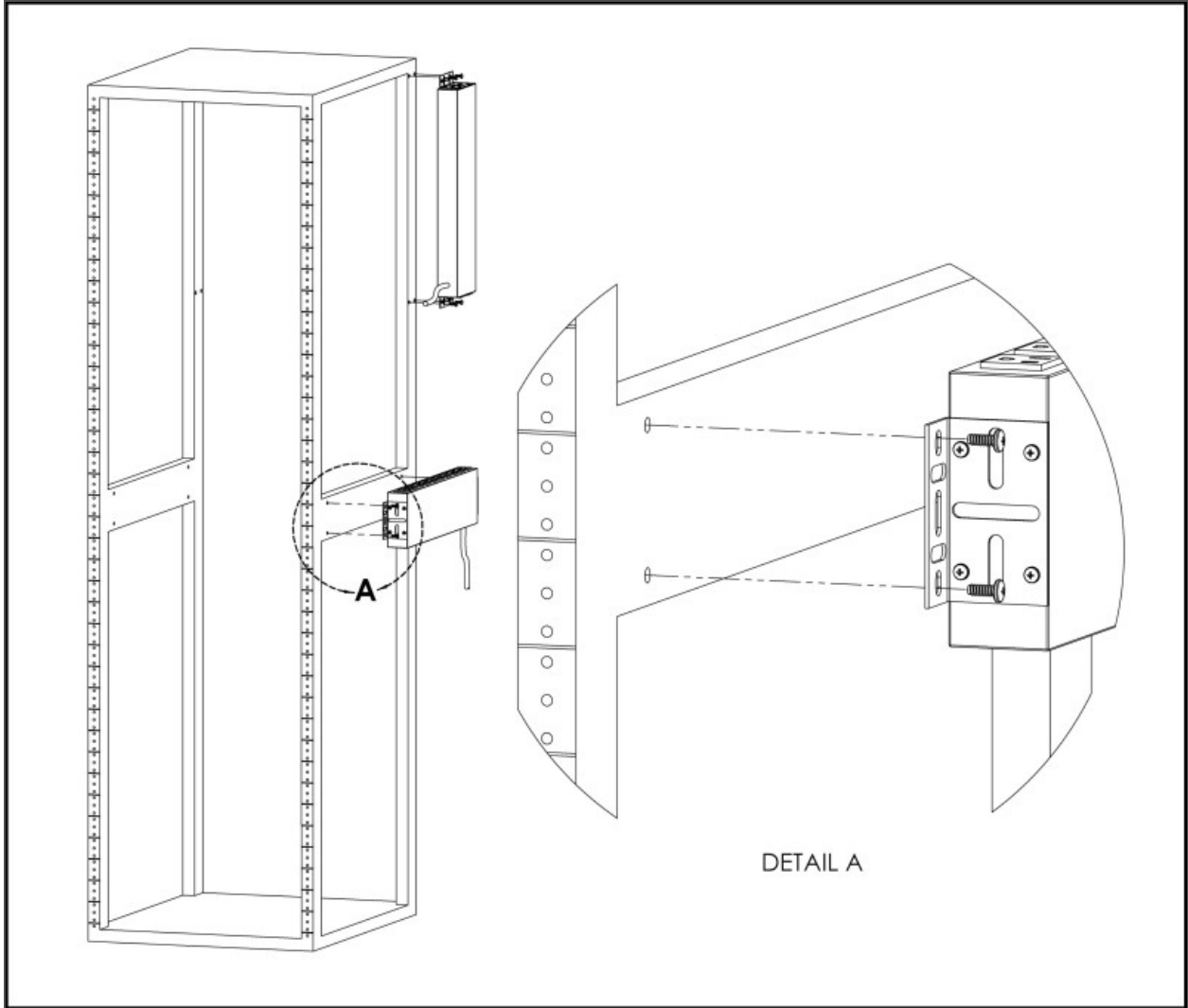


Figure 2.11 Panel-Mount Bracket



DETAIL A

Figure 2.12 23" (inch) Conversion-Mount Brackets

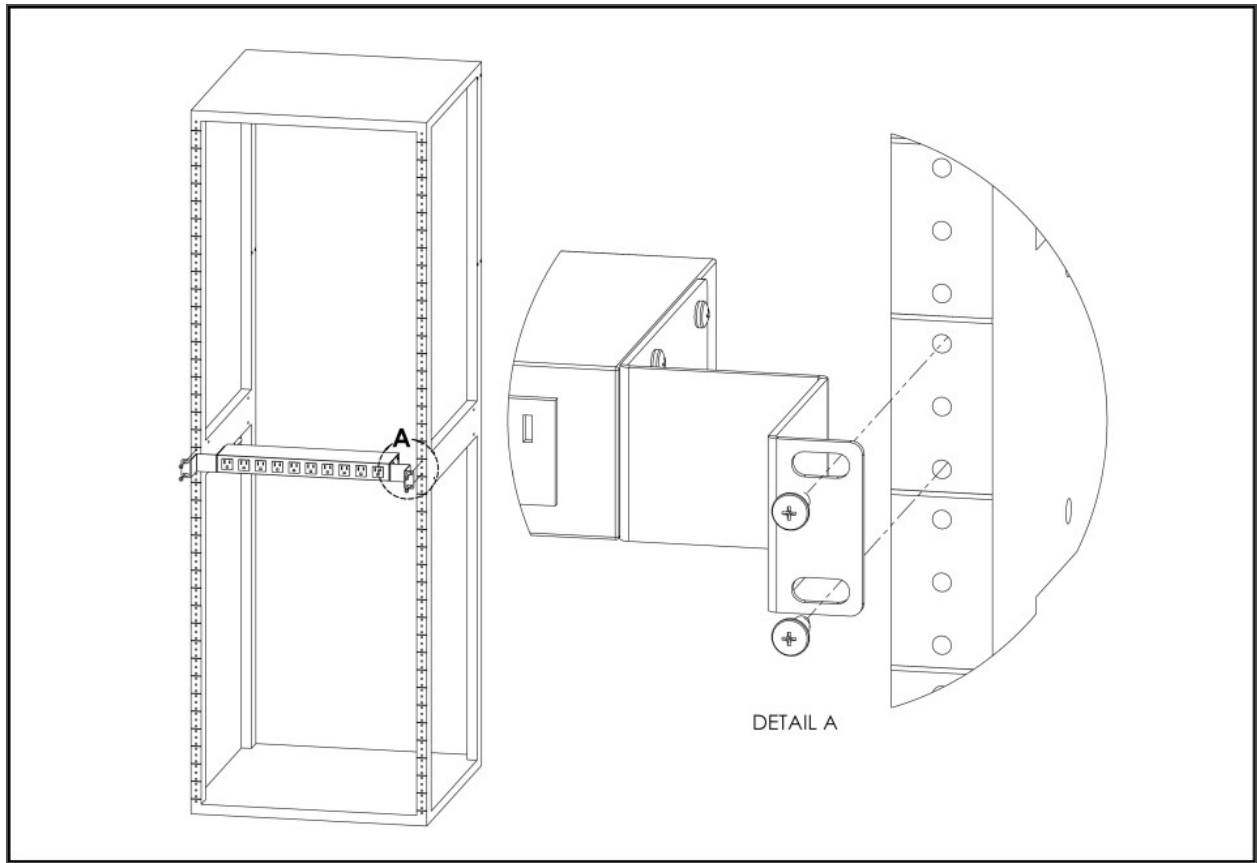


Figure 2.13 19" (inch) Horizontal/Panel-Mount Brackets

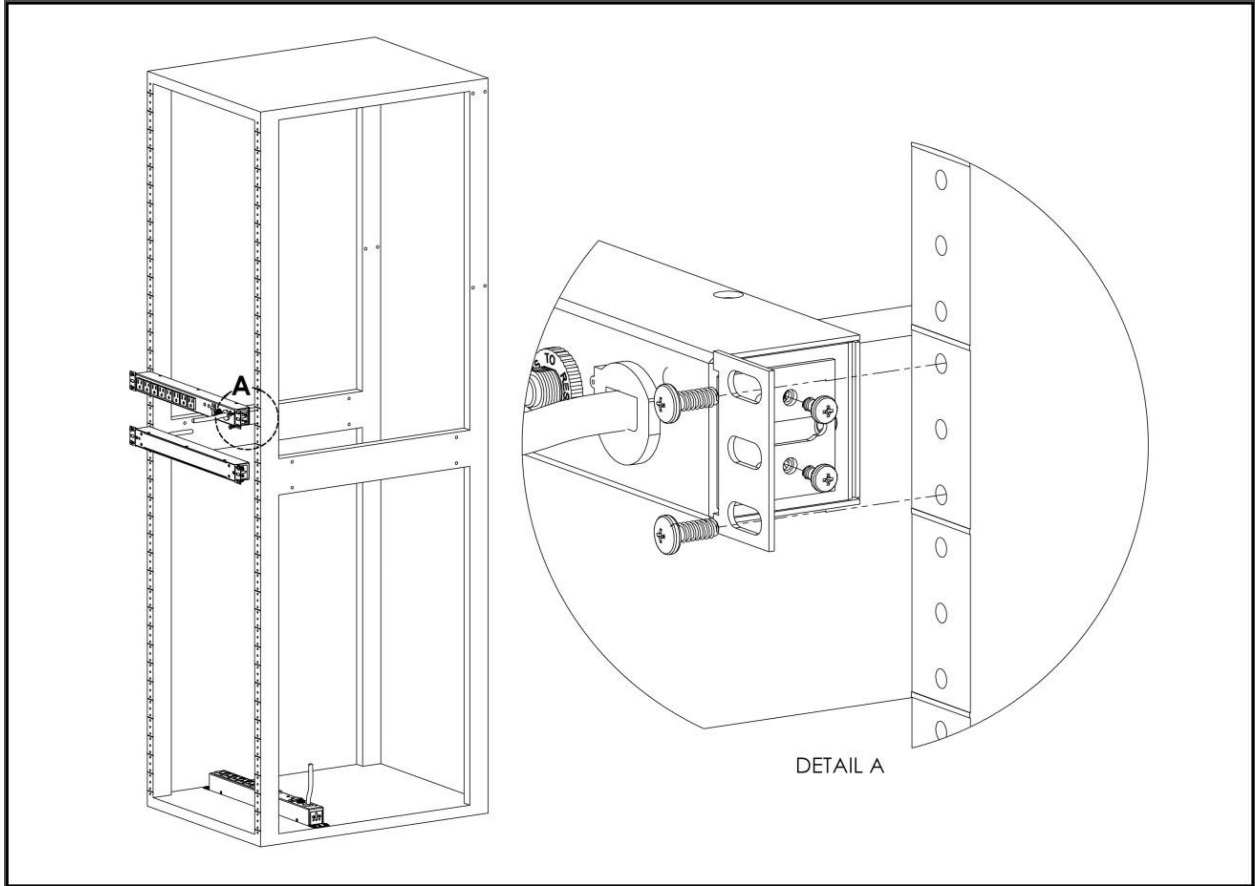
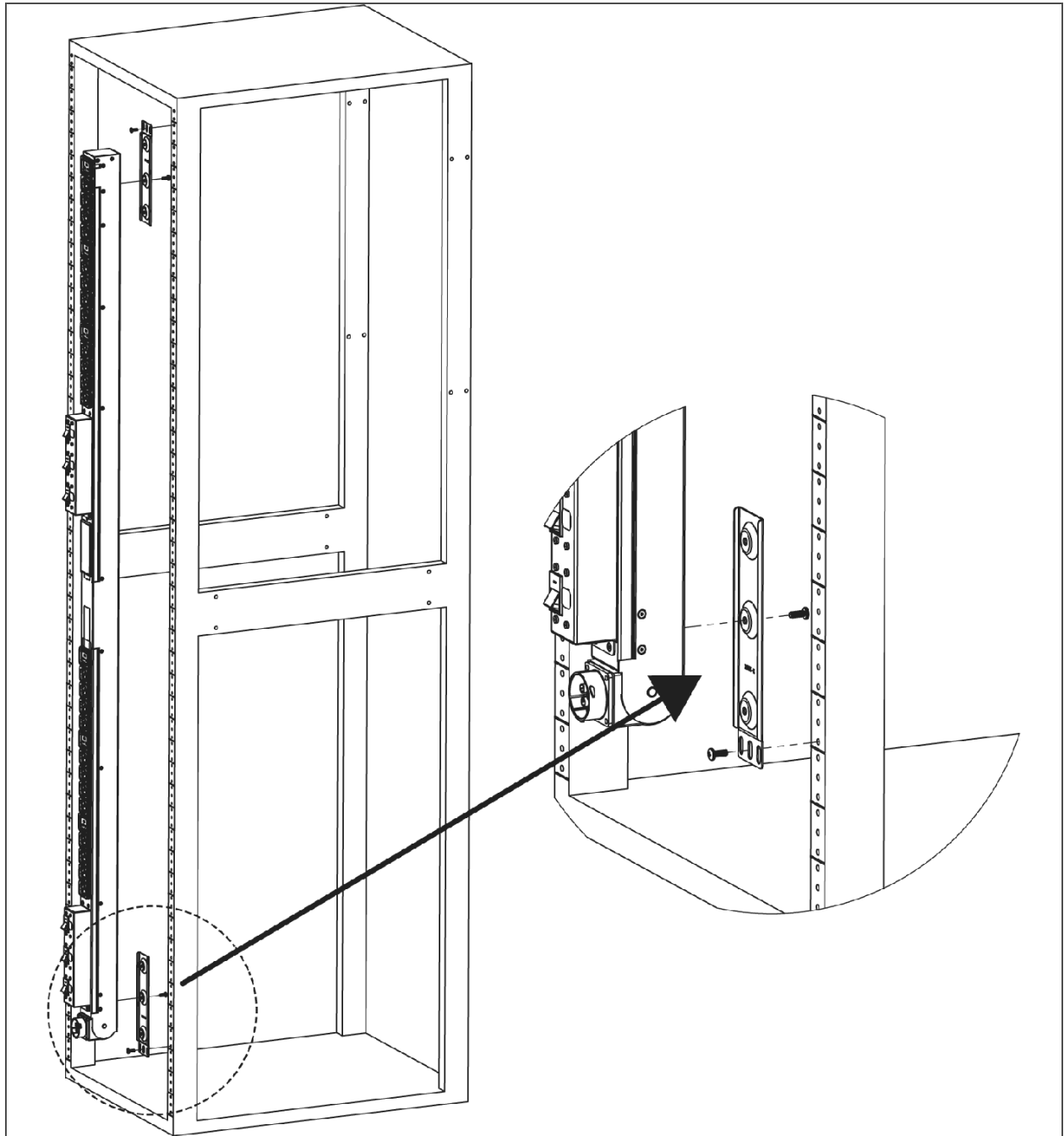


Figure 2.14 Mount Brackets for UPDU with Pivoting End



2.1.1 Power Connection

Plug the rPDU into an appropriately rated and protected branch circuit receptacle.

2.1.2 U-Lock Operation

Plug in the devices to be powered by the rPDU.

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

Figure 2.15 U-Lock Cord Retention Operation



3 SETUP

3.1 Interchangeable Monitoring Device (IMD-3E)

The Interchangeable Monitoring Device (IMD) is the controller for the GU2 line of power products. The IMD can be replaced and upgraded to allow data centers to future-proof their rPDU installation.

NOTE: The IMD-3E has been discontinued and replaced with the IMD-3E-S.

3.1.1 Enhanced Switched Monitored

The Enhanced Switched Monitored Vertiv™ Upgradeable rPDU is a more-advanced option for data centers that need full remote switching, monitoring, alarms and remote sensors. It is built with the IMD-3E module, which provides Dual Ethernet Ports, a local display, USB Port and an RJ-12 Port for remote sensors.

Figure 3.1 IMD-3E Module

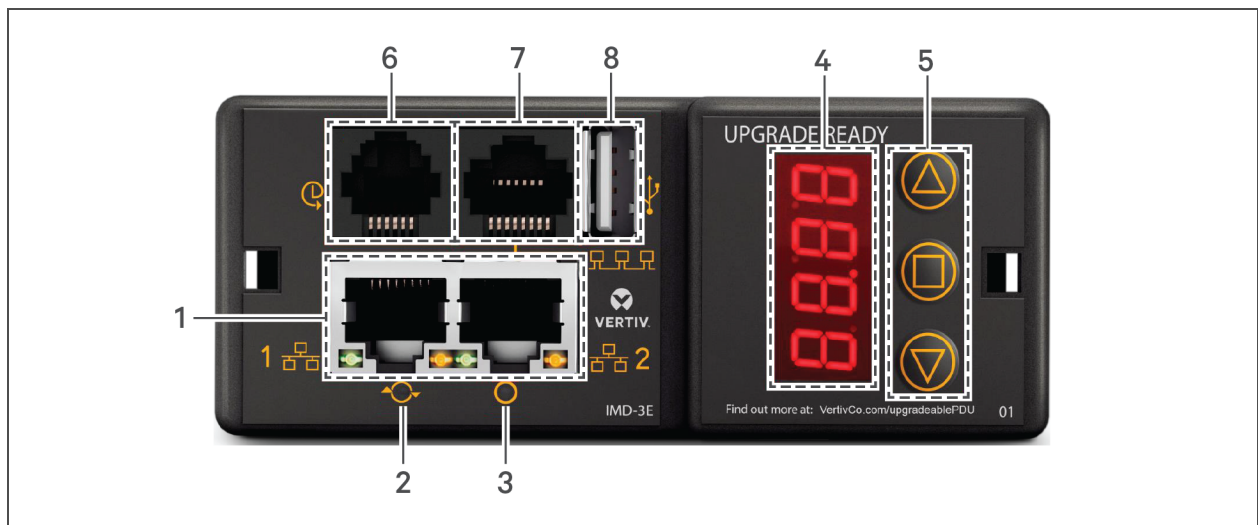


Table 3.1 IMD-3E Module Descriptions









NUMBER	NAME	DESCRIPTION
1	Dual Ethernet Ports	The dual ethernet ports act as a two-port ethernet switch, allowing 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 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 Display Button Functions on page 21
6	Remote Sensor Port	RJ-12 port for connecting a Vertiv™ plug-and-play remote digital sensors (sold separately). Each digital sensor has a unique serial number and is automatically discovered. GU2 PDUs support up to 16 sensors. The optional Vertiv A2D Converter can be added to support analog sensing. The optional SN-ADAPTER can be added to support Liebert® Integrated and Modular Sensors. See Available Sensors on page 72 for more information.
7	Proprietary Connectivity	RJ-45 port for future expansion.
8	USB Port	USB port used to upload firmware, backup/restore device configuration or expanded logging capacity via USB storage device. Provides up to 500mA power capacity for USB-connected devices.

NOTE: GU2 PDUs support the use of USB MSC devices such as thumb drives or external hard drives. USB storage devices must be formatted as FAT32.

Display Buttons

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

Table 3.2 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 3 seconds initiates a parameter reset sequence. This sequence consists of an <i>rset</i> message, followed by a <i>dflt</i> message and then a 3-second countdown. Once the countdown expires, an <i>8888</i> 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 Visible Light Communication (VLC) on page 64.
Back and Forward Buttons	 and 	Pressing both buttons at the same time flips the display 180 degrees.
Back and Center Buttons	 and 	Pressing both buttons at the same time displays the primary IPv4 address of the unit.

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

3.1.2 Enhanced Switched Monitored with RS-232

All Vertiv™ Geist™ Switched Unit Level Monitoring, Outlet Level Monitoring and Switched Outlet Level Monitoring 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 3.2 IMD-3E-S Module

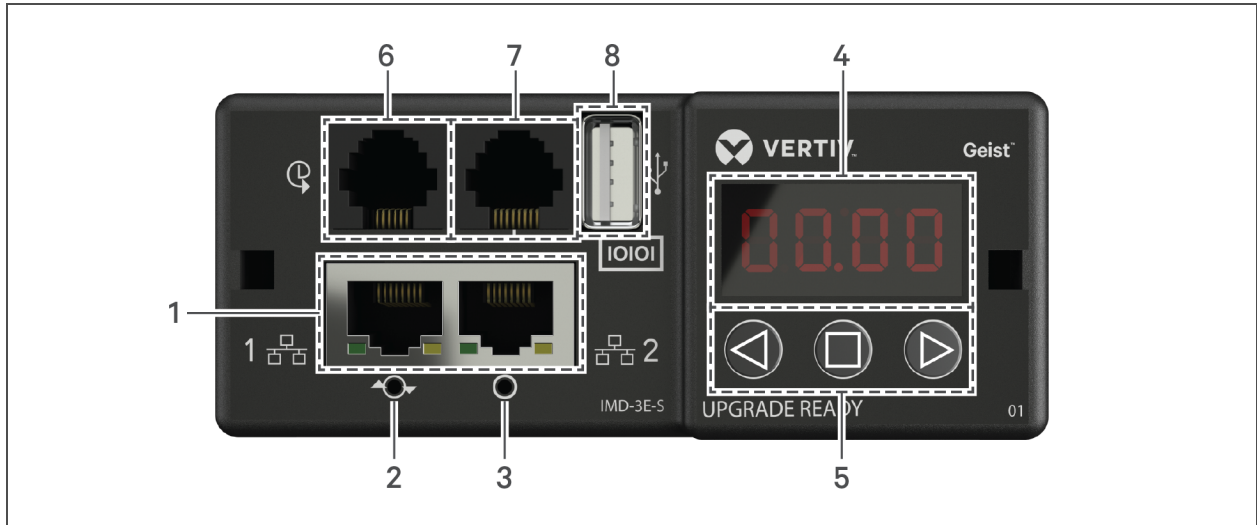


Table 3.3 IMD-3E-S Module Descriptions

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.
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 Display Button Functions on page 21.
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 Liebert® Integrated and Modular Sensors. For more information see, Available Sensors on page 72.
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 500mA power capacity for USB-connected devices.

NOTE: GU2 PDUs support the use of USB MSC devices such as thumb drives or external hard drives. USB storage devices must be formatted as FAT32.

3.1.3 Rapid Spanning Tree Protocol (RSTP)

GU2 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.

3.2 Network Setup

The Upgradeable IMD has a default IP address for initial setup and access. Once you have assigned an IP address, the default IP address is no longer active.

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.

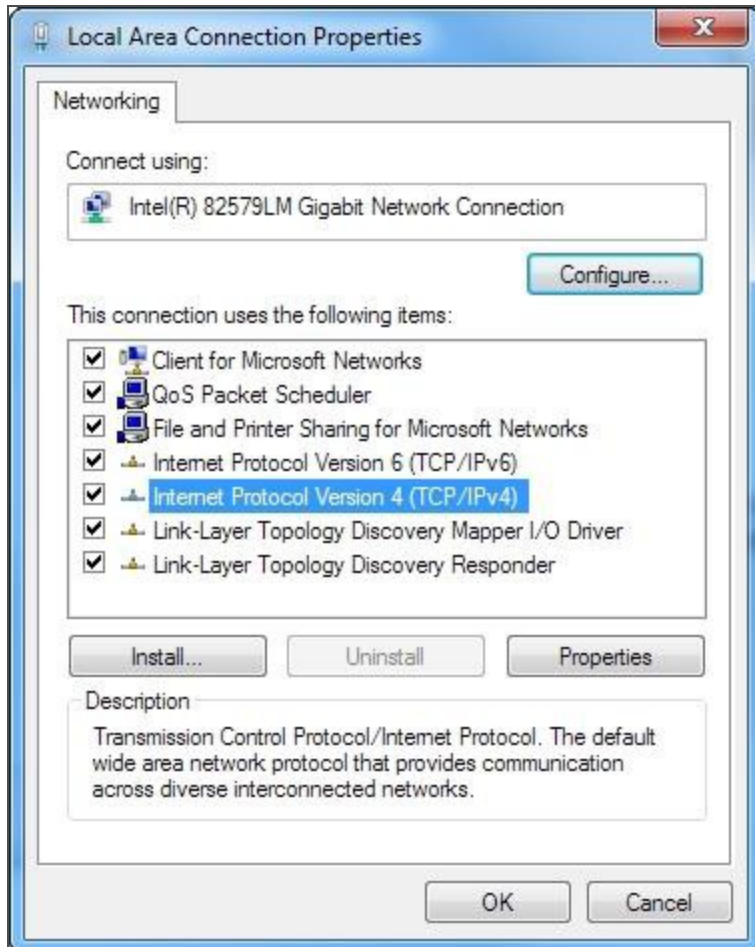
To set up the network for a Windows operating system:

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.

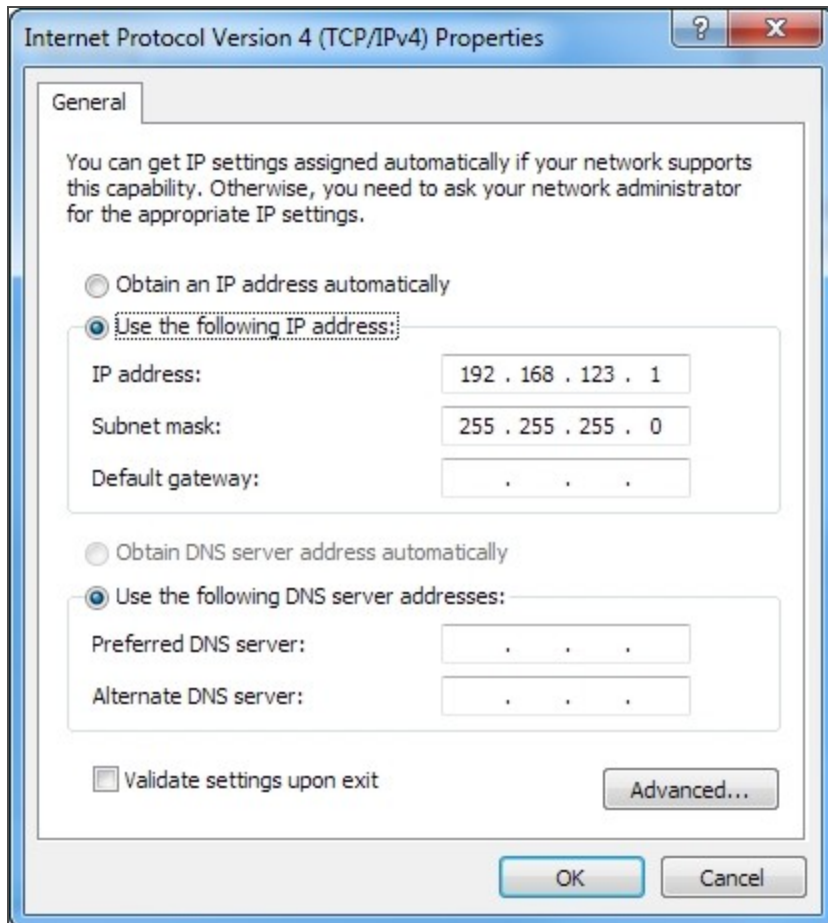
Figure 3.3 Local Area Connection Properties



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 3.4 Internet Protocol Version 4



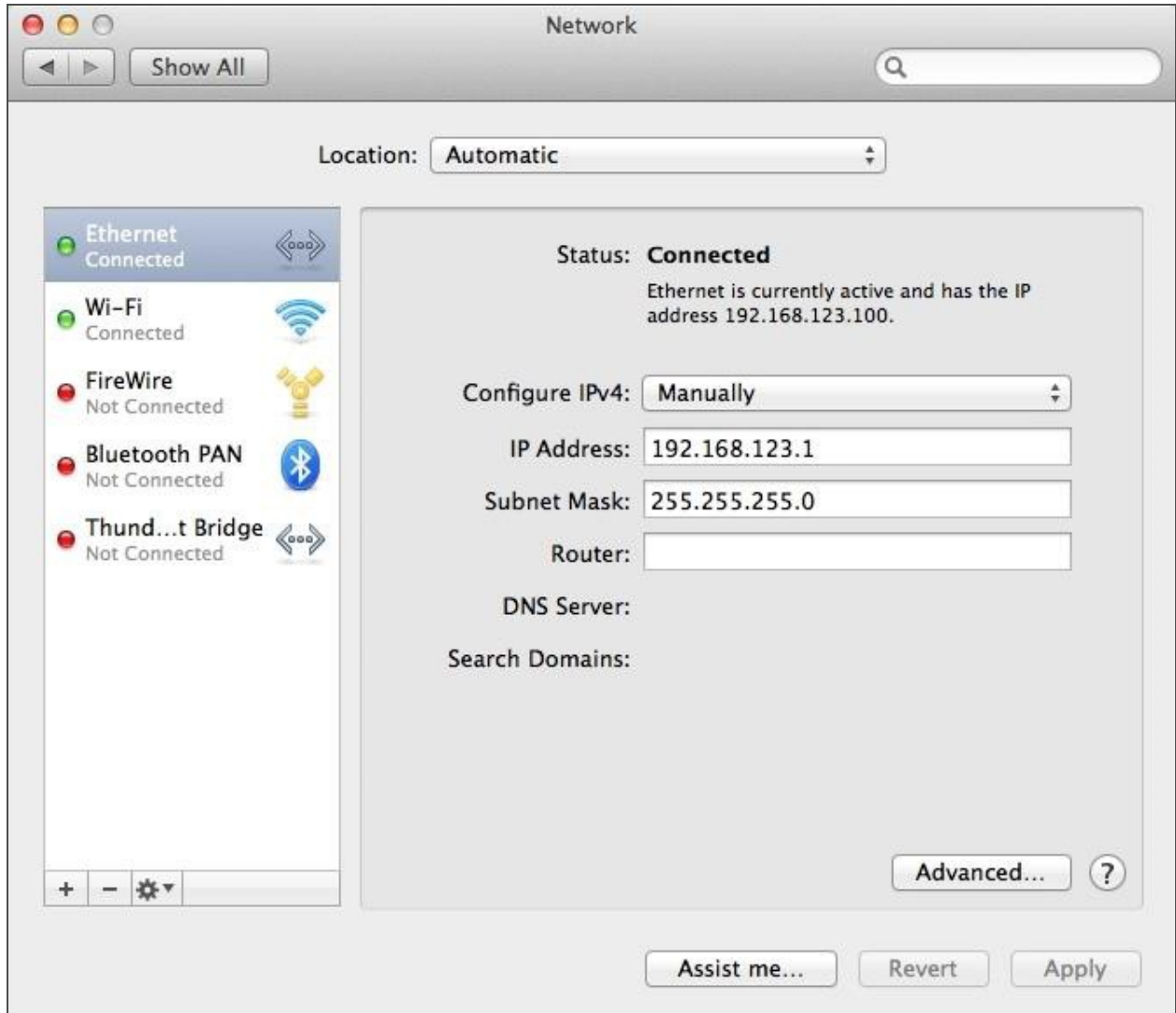
5. Choose *Use the following IP address*, set IP address to *192.168.123.1* and Subnet Mask to *255.255.255.0*. For initial setup, Default Gateway and the DNS Server entries can be left blank. Select *OK* - *OK* to close both the Internet Protocol Properties and Local Properties windows.
6. In a web 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* 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 3.5 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.

- 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.
- Click Save.

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

3.3 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.

3.3.1 Home Page

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

Figure 3.6 Home Page

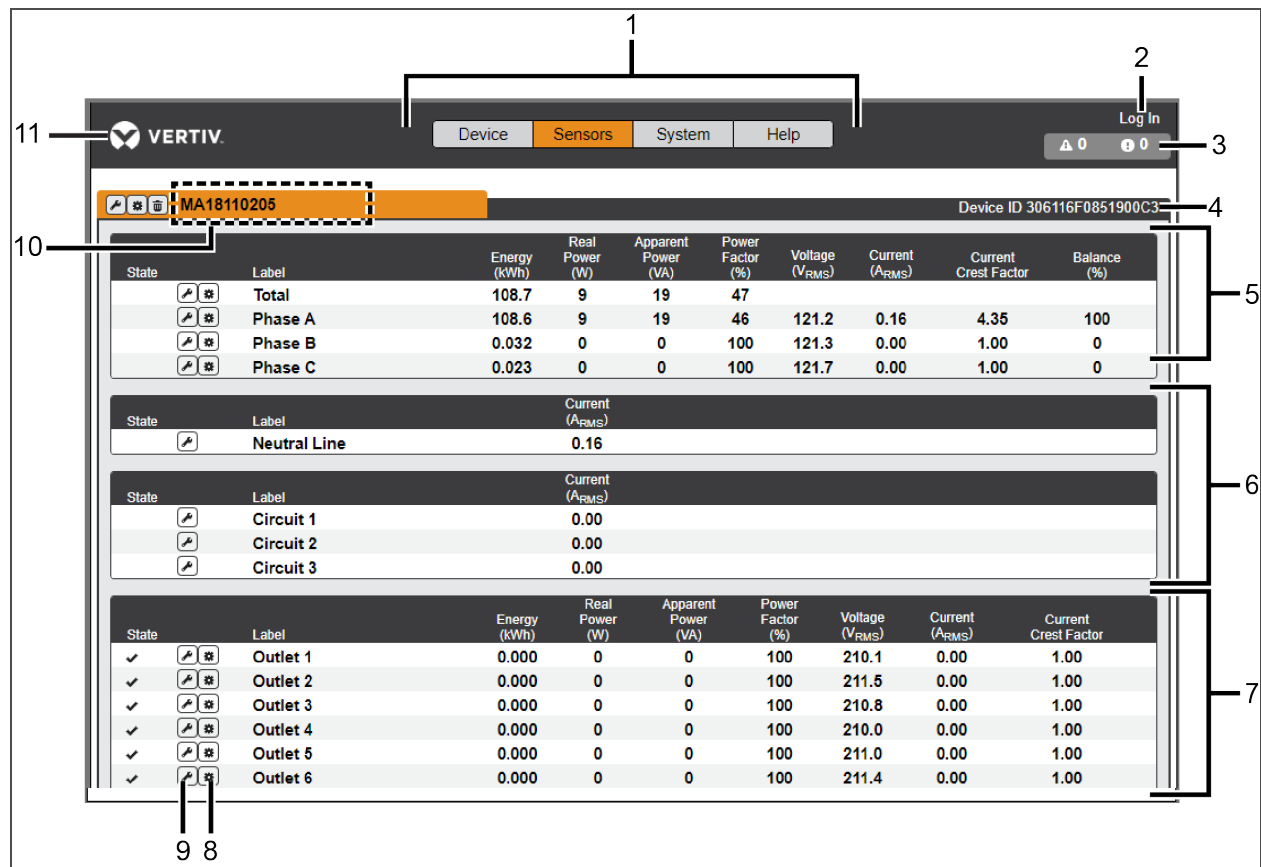


Table 3.4 Home Page Descriptions

NUMBER	NAME	DESCRIPTION
1	Device, Sensors, System and Help	Mouseover to show submenus: Device, Sensors, System and Help. NOTE: Device will only appear as a submenu when the unit is configured as a master rPDU. See the Vertiv™ Intelligence Director on page 53 section for further definition and configuration.
2	Log In/Log Out	Click to log in or log out of the unit. NOTE: Both username and password are case-sensitive and no spaces are allowed. Prohibited characters for username are: \$&`':<>[] { } "+%@/ ; = ? \ ^ ~ ,
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	Total and Individual Phase Monitor	Displays AC current, voltage and power statistics for each individual phase and for the total of all phases combined. Current Crest Factor and Phase Balance (%) are also indicated.
6	Neutral Line	Displays the current (in Amps RMS) on 3-phase Wye units. This is not shown on single phase and 3-phase Delta units.
6	Current Monitor	Displays AC current draw statistics for each individual circuit on the rPDU.
7	Outlet Monitor	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)
8	Operation Icon	Modify settings.
9	Configuration Icon	Modify label name.
10	Device Label	Displays the user-assigned label of this unit.
11	Vertiv™ Logo	Clicking on this logo from any page will reload the home page.

3.3.2 Sensors Tab

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

Overview

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

To change a device label:

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

NOTE: These actions affect the entire device.

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 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 configure an outlet:

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

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

- b. **State** - the outlet's current state (On or Off).
 - c. **Mode** - how the outlet will be controlled:
 - **Manual Control** - the outlet state is controlled using the web user interface, SNMP or the API.
 - **Alarm Control (normally Off, 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.
 3. Click *Save*.

To change outlet operation:

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.

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 3.7 Alarms and Warnings Page

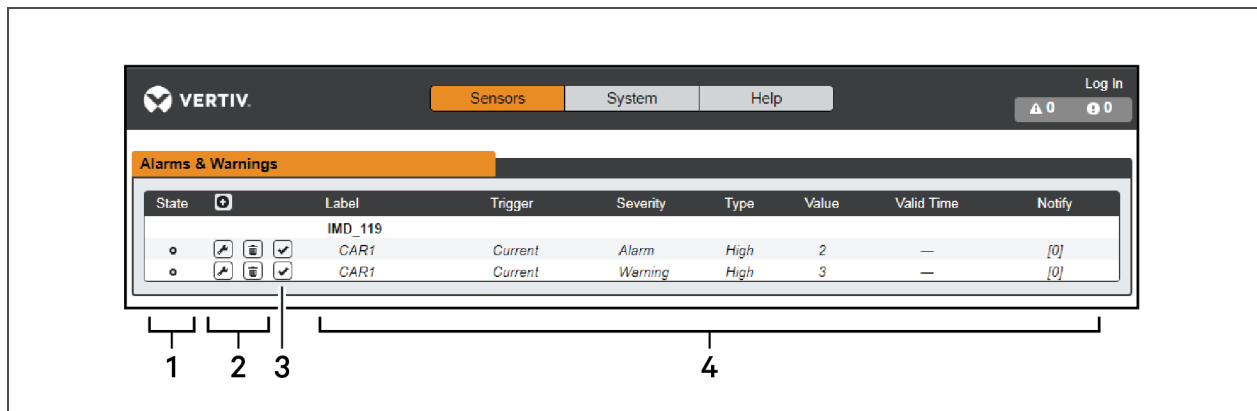


Table 3.5 Alarms and Warnings Descriptions

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

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 47.
 - 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 page 31.

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.

- 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.

Logging

The Logging page allows you to access the historical data recorded by the rPDU 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 3.8 Logging Page

The screenshot shows the VERTIV web interface for the 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 contains buttons for 'Download the data log JSON' and 'Download the data log CSV', a warning message, a 'Log Interval (minutes)' input field set to 15, and a 'Clear the Log' button. The 'Logging' section features a 'Save' button, a 'Select All' dropdown menu with a checked checkbox, and a table of PDU data. The table has three sections: Phase A, Circuit 1, and Outlet 1. The 'Outlet 1' row is selected with a checkmark in the 'State' column.

State	Label	Energy (kWh)	Real Power (W)	Apparent Power (VA)	Power Factor (%)	Voltage (V _{RMS})	Voltage Min (V _{RMS})	Voltage Max (V _{RMS})	Peak Voltage (V)	Current (A _{RMS})	Current Min (A _{RMS})	Current Max (A _{RMS})	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
	Circuit 1		0.00			0.00			0.00				0.00
✓	Outlet 1	0.047	0	0	100	121.2	120.9	121.3	172.8	0.00	0.00	0.00	0.00

Table 3.6 Logging Page Descriptions

NUMBER	NAME	DESCRIPTION
1	Data log download	Clicking the <i>JSON</i> link downloads the data log in <i>JSON</i> format. Clicking the <i>CSV</i> downloads the data log in <i>.csv</i> 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 <i>Select All</i> or <i>Select None</i> 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 <i>Save</i> 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.

3.3.3 System Tab

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

Users Account Page

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

Figure 3.9 User Account Page

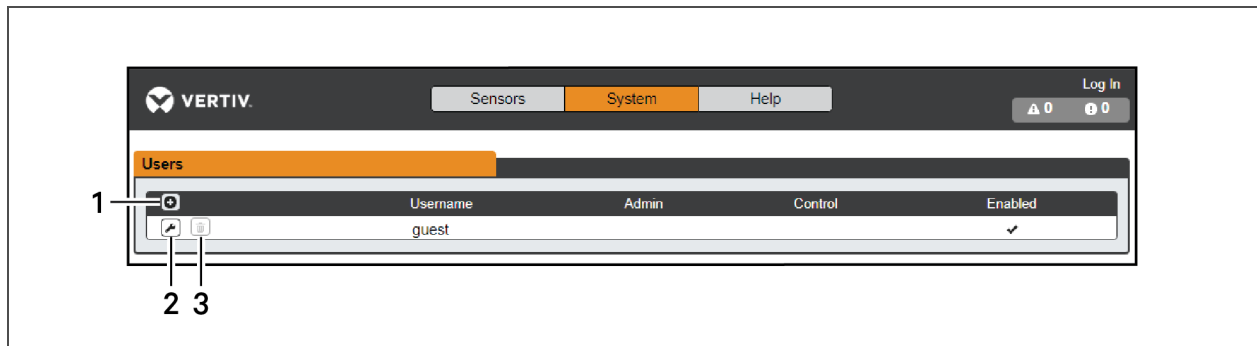


Table 3.7 User Account Page Descriptions

NUMBER	DESCRIPTIONS
1	Add new user account
2	Modify user account
3	Delete user account

NOTE: Only an Administrator-level account can add, modify or delete users. 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. **New Password:** Account password may be up to 24 characters long, are case-sensitive and may not contain spaces.
 - e. **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*.

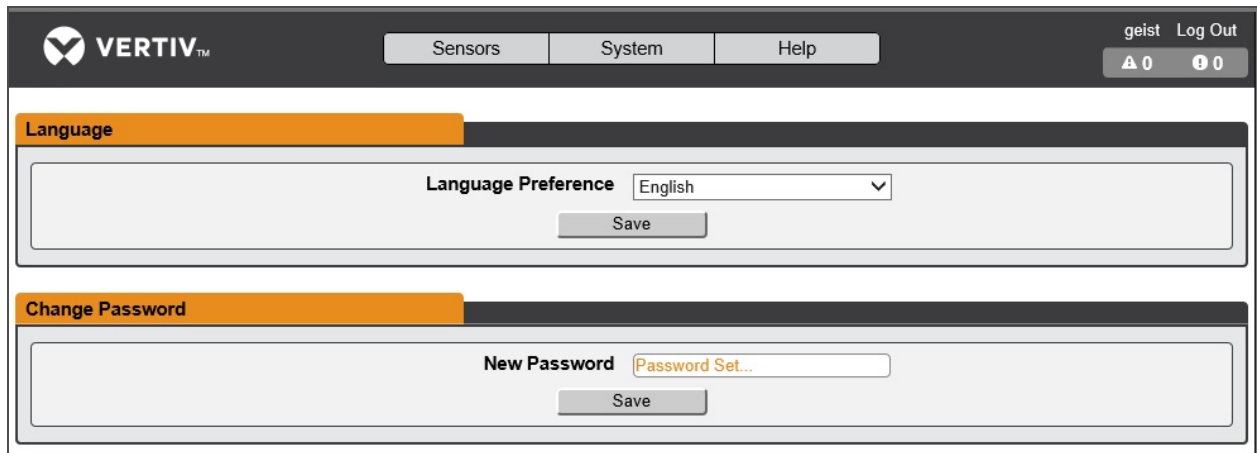
User Account Types

- **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, although the administrator can elevate the Guest account to control-level access, 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 3.10 Change User Password Page



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 rPDU, 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 rPDU.
- **Routes:** Displays configured routes and is where you will set your Gateway address for the rPDU. Default routes are distinguished by a *destination* of 0.0.0.0 or ":", with a Prefix of "0" and Interface of "all". Only one default route can exist for IPv4 and one for IPv6.
- **DNS:** Allows the unit to resolve hostnames for email, "NTP" and "SNMP" servers.

Figure 3.11 Network Configuration Page

Sensors
System
Help

Log In
▲ 0 ● 0

Hostname

Hostname

Protocol

IPv6

Interfaces

Label	MAC Address	DHCP	Link state	Uptime
Bridge 0	00:19:85:00:ad:32	Enabled	Up	157

IP Address	Prefix
<input type="text" value="192.168.123.123"/>	24
<input type="text" value="fe80::219:85ff:fe00:ad32"/>	64

Ports

Label	Interface	RSTP Role	STP State	Link state	Uptime	Enabled
Port 1	Bridge 0	Unknown	Disabled	Down	345276	Enabled
Port 0	Bridge 0	Designated	Forwarding	Up	159	Enabled

Routes

Destination	Prefix	Gateway	Interface

DNS

DNS Server Address
<input type="text" value="8.8.8.8"/>
<input type="text" value="8.8.4.4"/>

RSTP

Enable

Mode

Bridge Priority

Max Hops

Hello Time

Max Age

Forward Delay

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. Enable/Disable port.
 - c. 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:

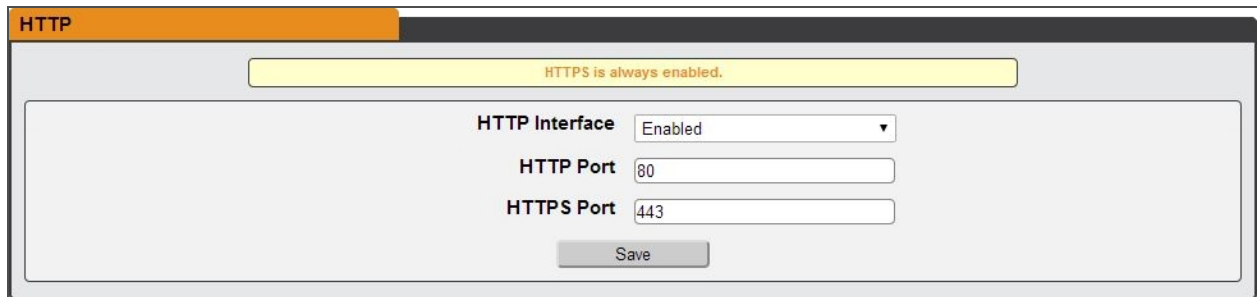
1. Change the settings, as desired.
 - a. **Enable:** Enable or Disable RSTP protocol.
 - b. **Mode:** RSTP mode supports falling back to STP when necessary.
 - c. **Bridge Priority:** Click the drop-down menu, select the appropriate value and click *Save*.
 - d. **Max Hops:** Used when mode enabled 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*.

Web Server

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

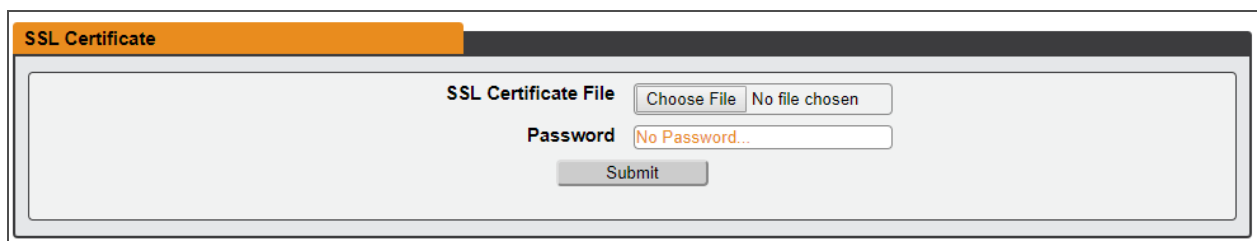
- **HTTP Interface:** Enables or disables access via HTTP. HTTPS interface is always enabled. Available options are *Enabled* and *Disabled*. It is not possible to disable the web interface completely.
- **HTTP/HTTPS Server Port:** Allows you to change the TCP ports that the HTTP and HTTPS services listen to for incoming connections. The defaults are Port 80 for HTTP and Port 443 for HTTPS.

Figure 3.12 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 3.13 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.

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.

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 Geist™ rPDU device for this remote authentication protocol. If you are not familiar with these settings, consult your LDAP server administrator.

Configuration for remote authentication using LDAP.

- **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".
- **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.

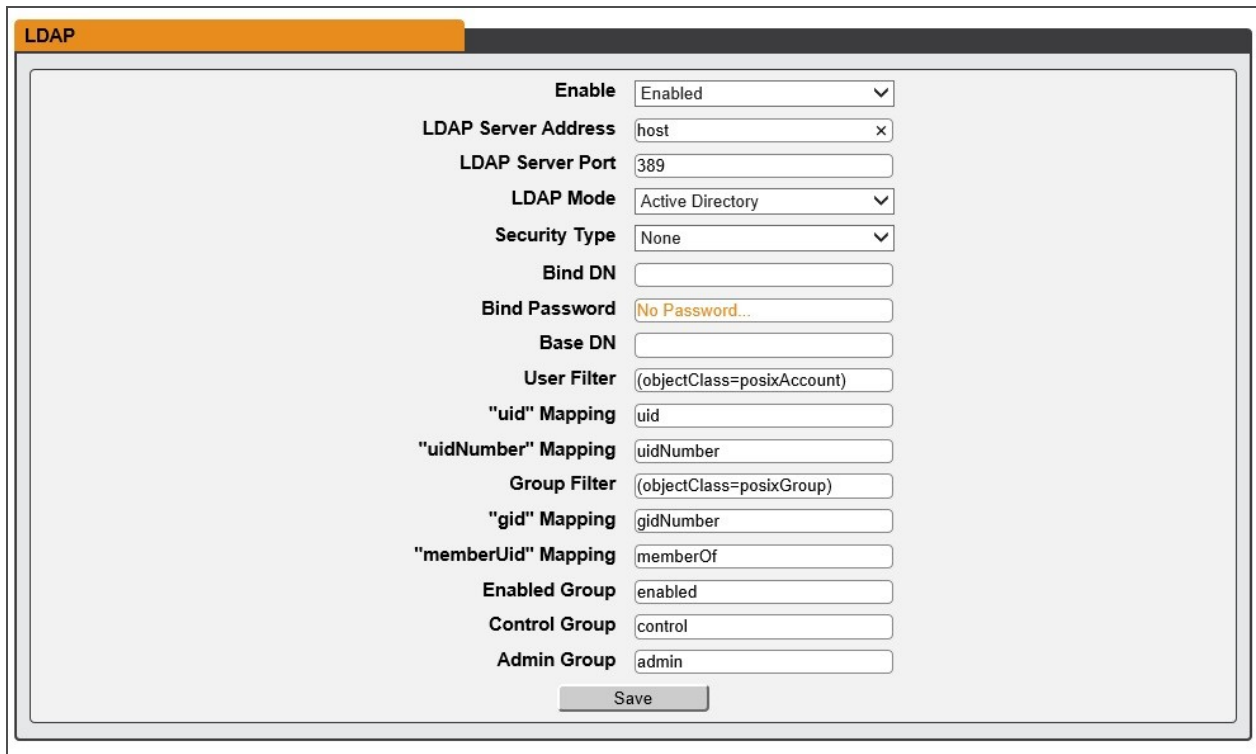
The remaining fields come from the NIS schema, defined in RFC2307. They are used to authenticate users in LDAP. Leaving them blank will use the default value.

- **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 3.14 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

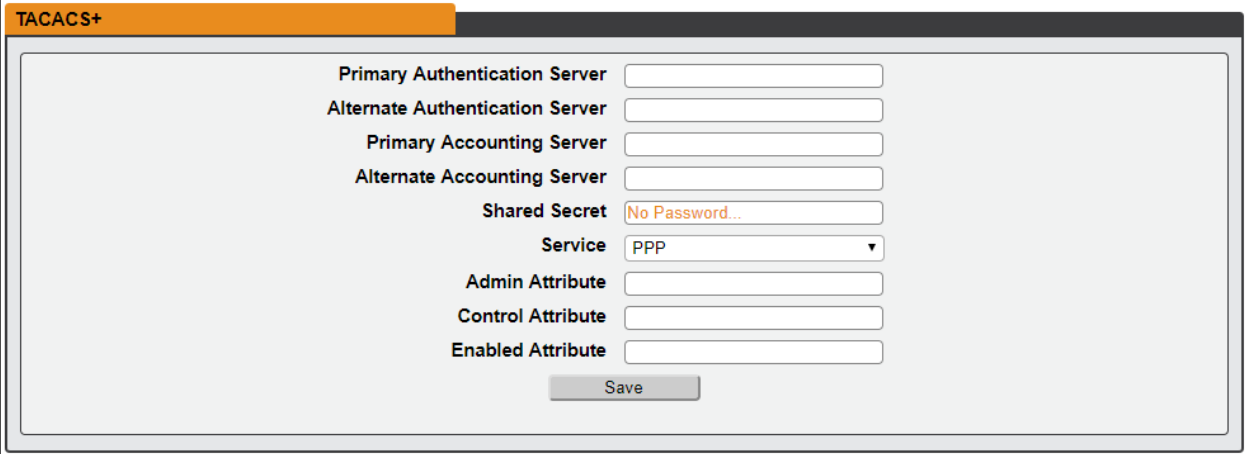
TACACS+

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 Geist™ rPDU 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 3.15 TACACS+ Menu



The screenshot shows a web-based configuration interface for TACACS+. The title bar is orange and labeled 'TACACS+'. Below it, there are several rows of labels and input fields:

- Primary Authentication Server: [Empty text box]
- Alternate Authentication Server: [Empty text box]
- Primary Accounting Server: [Empty text box]
- Alternate Accounting Server: [Empty text box]
- Shared Secret: [Text box containing 'No Password...']
- Service: [Dropdown menu showing 'PPP']
- Admin Attribute: [Empty text box]
- Control Attribute: [Empty text box]
- Enabled Attribute: [Empty text box]

A 'Save' button is centered at the bottom of the form area.

- **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 *radius*.
- **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.

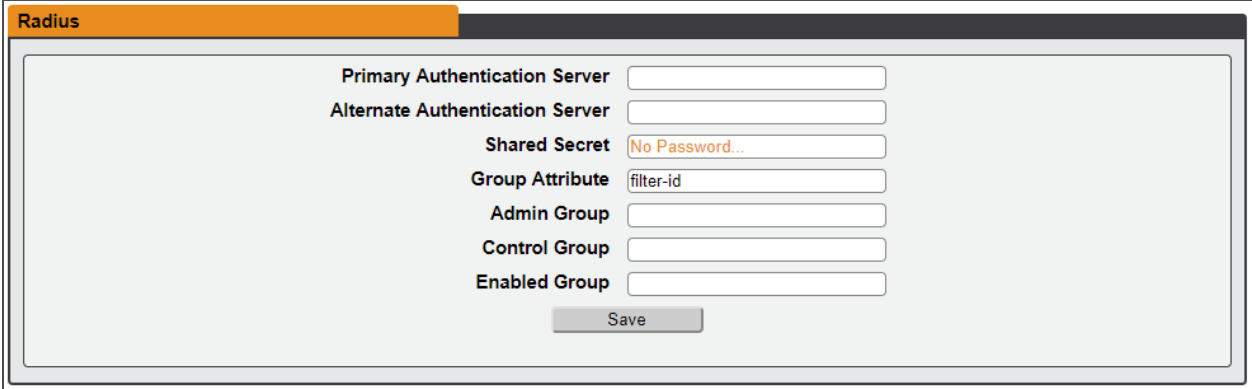
RADIUS

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 Geist™ rPDU device for this remote authentication protocol. If you are not familiar with these settings, consult your RADIUS server administrator.

Configuration for remote authentication using RADIUS.

Figure 3.16 RADIUS Menu



- **Primary Authentication Server:** Enter the IP address of the primary authentication/authorization/accounting server. The Primary Authentication Server can be an IPv4 address, an IPv6 address in square brackets (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.

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:

- **Display Mode:** Sets the unit to display current or total power (displayed as kW) on the local LED display.
- **VLC:** Allows user to enable or disable VLC mode from GUI (default is *disabled*).

Figure 3.17 Display Mode/VLC Configuration Page

The screenshot shows the VERTIV web interface with the 'System' menu selected. The 'Display Mode' section has a dropdown menu set to 'Current' and a 'Save' button. The 'VLC' section has a dropdown menu set to 'Disabled' and a 'Save' button.

Time

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

Figure 3.18 Time Configuration Page

The screenshot shows the 'Time' configuration page with the following fields: Mode (NTP), Date-Time (YYYY-MM-DD hh:mm:ss) (2014-09-17 08:50:20), Time Zone (America/Chicago), Primary NTP Server (0.pool.ntp.org), and Alternate NTP Server (1.pool.ntp.org). A 'Save' button is located at the bottom.

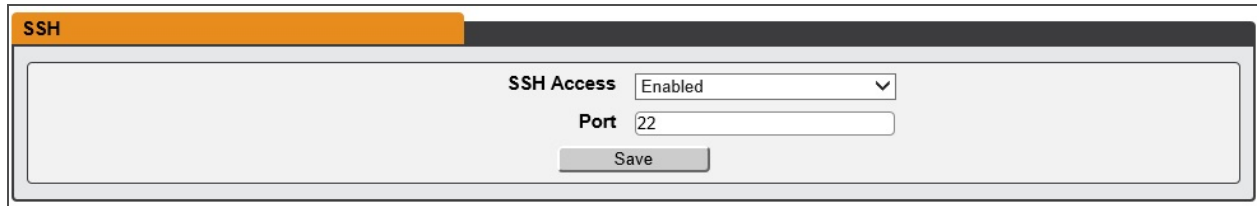
Two modes are available:

- **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.

SSH

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

Figure 3.19 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.

USB

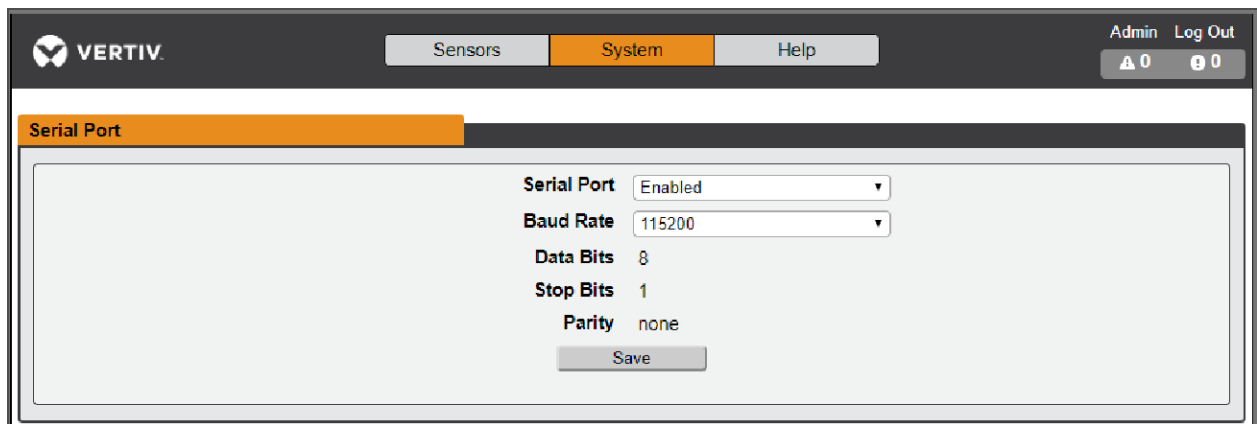
The USB menu allows you to configure settings for the USB port on the unit. It enables or disables the port.

Serial Port

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 3.20 System drop down, menu – Serial Port



Email

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

Figure 3.21 Email Configuration Page

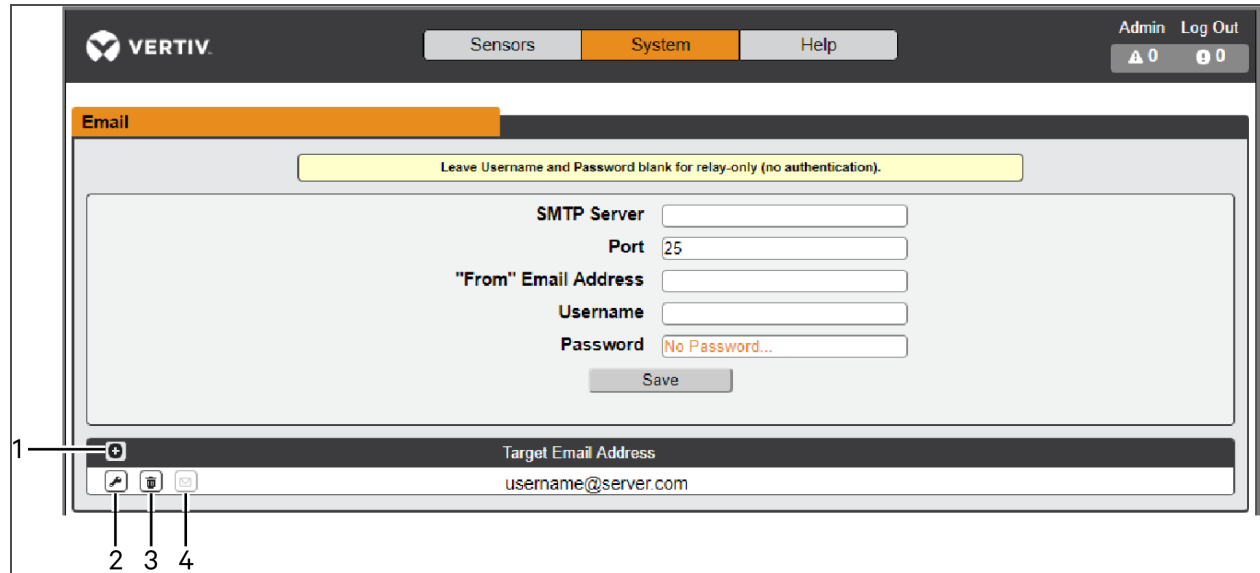


Table 3.8 Email Configuration Page Descriptions

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.
- **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:

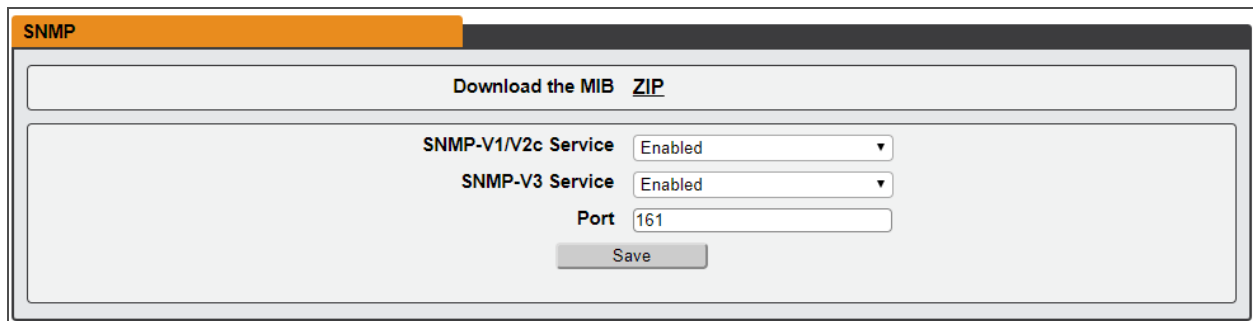
1. Click the *Test email* icon next to the address you wish to test.
2. A pop-up window indicates the test email is being sent, click *OK* to dismiss the pop-up.

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 3.22 SNMP Configuration Page



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 3.23 SNMP Users Configuration Page

Users				
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.

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.

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.

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.

Utilities

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

The Restore Defaults section allows you to restore the unit's settings to its factory defaults. There are two options:

- **All Settings:** Erases all of the unit's settings, including all network and the user accounts settings, effectively reverting the entire unit to its original, out-of-the-box state.
- **All Non-Network Settings:** Erases all settings except the network and user accounts.

The Reboot section allows the user to perform a system reboot. This function will not affect power delivery to connected equipment. Use the Firmware Update section to load firmware updates into the unit. Firmware updates, when available, can be found on the Vertiv™ website: Vertiv.com/Firmware-Support. You can also subscribe to a mailing list to be notified when firmware updates become available.

The Reboot I/O Boards section allows the user to reboot the I/O boards when one or both is not responsive.

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.

NOTE: Firmware updates can be performed via HTTP interface only. Updates over the HTTPS interface are not currently supported.

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.

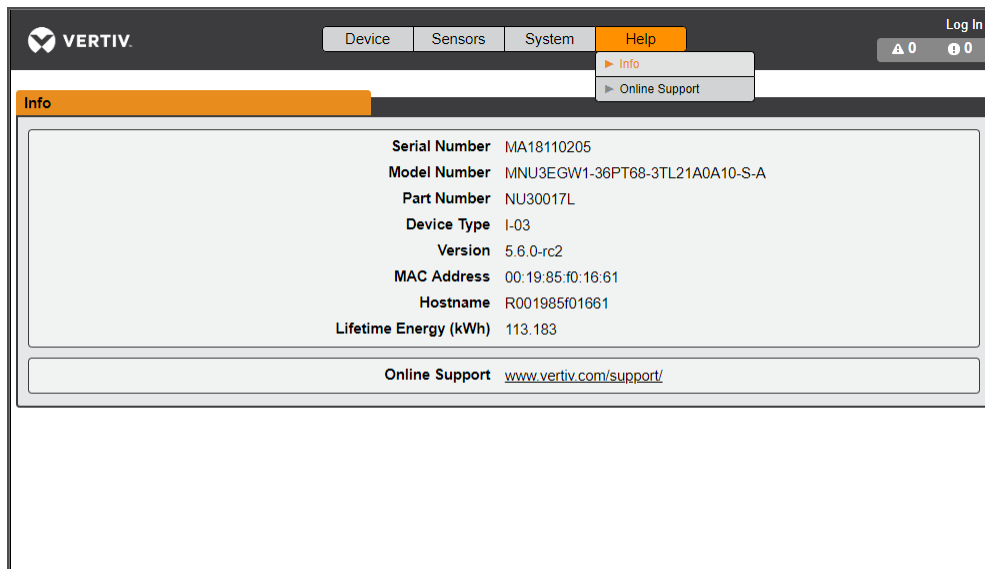
During the update, the IMD will stop scrolling data. After the update is complete, a boot message will appear on the display. After reboot is complete, the IMD will resume scrolling data on the display.

3.3.4 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 3.24 Info Page



This page intentionally left blank

4 VERTIV™ INTELLIGENCE DIRECTOR

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

4.1 Aggregation

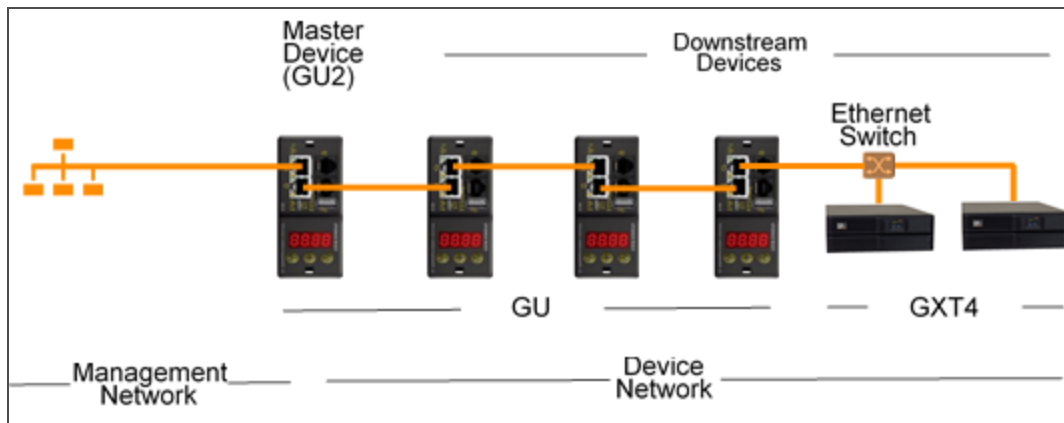
The initial element of Vertiv Intelligence Director, available with Vertiv™ Geist™ rPDUs running firmware 5.3.0 or later, is called Aggregation. This single element allows you to:

- Use a single IP address assigned to the Master rPDU to monitor up to 50 devices (the master and 49 downstream devices).
- Allow rPDUs downstream from the master to self-configure network settings.
- Create aggregated measurements like total rack power and total row power, including averages, minimums and maximums.

4.2 Master rPDU

Aggregation requires the designation of a Master rPDU, deployed with IMD model IMD-3E. The IMD of the master device facilitates and configures the device network, the interconnected array of Vertiv™ rPDUs, Vertiv™ UPS, Vertiv™ cooling and environmental sensors, while aggregating select data points from these devices. It also interacts with the management network for monitoring and management of itself and its downstream devices.

Figure 4.1 Sample Configuration



The IMD-3E is the default intelligence card for Vertiv™ Geist™ GU2 rPDUs, 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 Master rPDU, rPDUs with a legacy intelligence card must first be upgraded to the IMD-3E.

4.3 Network Configuration

In the initial release of aggregation, downstream devices are defined as rPDUs 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 master can support up to 49 downstream devices, so the number of masters depends on the overall size of the installation and the preferred network architecture.

The Master rPDU must be commissioned before it is connected to the primary management network or to the downstream 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 Master rPDU.

To commission the master rPDU:

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 downstream 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. **Managed Device Username:** Defines the username configured on all downstream devices.
 - c. **Managed Device Password:** Defines the password configured on all downstream devices.
5. Enter the new password, verify the password and click *OK*.
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 Master rPDU, configure the remaining Master rPDU settings. Connect the Master rPDU to management network (Port 1) on the IMD and the device network (Port 2).

NOTE: The Master rPDU has a built-in DHCP network to assign addresses to its downstream devices. This DHCP network uses 192.168.124.0/24 addresses and they cannot be used for the management network.

4.3.1 Downstream Devices

In the initial release of aggregation, downstream devices are defined as rPDUs 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 rPDUs must be running Version 5.3.0 or later. If the rPDUs are newly ordered and have never been configured with network settings, they are ready for aggregation out-of-the-box. If the rPDUs have been deployed in a computing environment and commissioned with local LAN settings and user accounts, each rPDU must be reset to its factory defaults using the Utilities page. The Master rPDU then pushes configuration data to the downstream devices, including:

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

To set up a new installation with one Master rPDU:

1. Install downstream rPDUs in racks and power-on the racks.

2. Daisy-chain the downstream rPDUs to each other where appropriate using ports labeled 1 and 2 on the IMD.
 - If daisy-chaining, ensure that no more than 100 rPDUs are chained together.
 - If connecting daisy-chains to a network switch, no daisy-chain should be longer than 20 rPDUs.
 - A star network or other design is also acceptable in lieu of a daisy-chain.
3. Install the Master rPDU in a rack. Using a laptop or a local machine, connect to Port 1 to configure Aggregation.
4. Connect the Master rPDU to the management network using Port 1.
5. Connect the Master rPDU to the downstream network using Port 2.

To set up an existing installation with one Master rPDU:

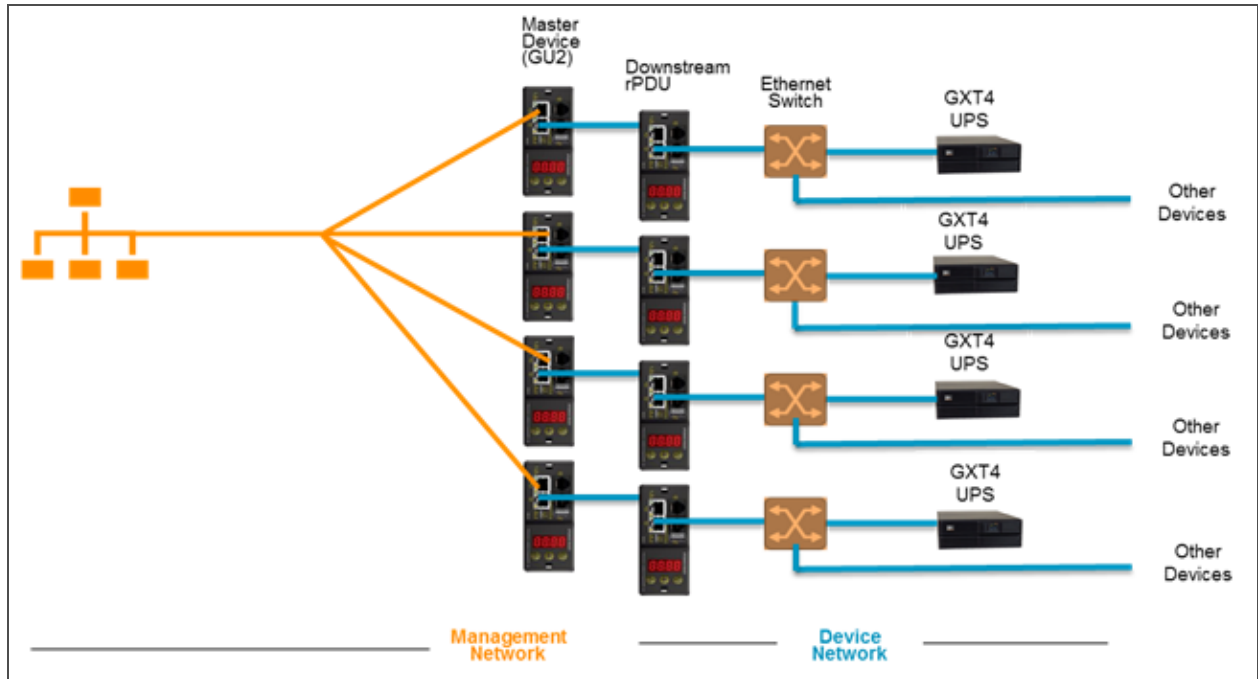
NOTE: Use the following instructions if existing Geist™ rPDUs are connected in a daisy-chain.

1. Designate a Master rPDU and disconnect it from the management network.
2. Reset all the downstream rPDUs 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 rPDU in the chain should be disconnected from the network switch.
3. Enable Aggregation on the Master rPDU.
4. Connect the Master rPDU to the management network using Port 1.
5. Connect the Master rPDU to the downstream network using Port 2.

Multiple Master rPDUs

For installations with multiple Master rPDUs, keep in mind that each device network must operate as a stand-alone, isolated network. Consider a 200 rPDU example, represented in the [Sample Network Configuration](#) on page 56. This installation would require a minimum of 4 master rPDUs, each operating its own stand-alone the device network. Each master is visible on the management network and acts as a DHCP server for its downstream devices. A user on the management network can navigate through each master rPDU to reach the interface of a downstream device. Other considerations may affect the quantity of master rPDUs. If you have a row network architecture, you may prefer 1 Master rPDU at the start of each row, as opposed to a master that traverses several rows. Depending on how these 200 cabinets are divided into rows, you may have more than 4 Master rPDUs. When the configuration is decided, follow the appropriate process for aggregation.

Figure 4.2 Sample Network Configuration



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

4.4 Views

When communication is established between the master and downstream 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 4.3 Device Tab

The screenshot shows the VERTIV Device Tab interface. At the top, there is a navigation bar with tabs for 'Device', 'Sensors', 'System', and 'Help'. The 'Device' tab is selected, and a dropdown menu is open showing options: 'Summary', 'Groups', 'List', and 'Group Configuration'. The 'Summary' option is highlighted. Below the navigation bar, there are three main sections:

- Summary:** A table showing aggregated data for Energy (kWh) and Power (W). The Power (W) section is further divided into Sum, Minimum, Maximum, and Average.
- Environmental:** A table showing Temperature (F) and Humidity (%) data. The Temperature (F) section is further divided into Minimum, Maximum, and Average.
- Notifications:** A table with columns for Severity, Name, and Event.

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

4.4.1 Summary

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

Rack PDUs

The rPDU network is summarized by the following data points:

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

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

Notifications

Notifications shows outstanding alarms from devices in the device network.

4.4.2 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

- **Energy:** The total rPDU energy within the group.
- **Power Sum:** The total rPDU power load within the group.
- **Power Minimum:** The lowest rPDU power load within the group.
- **Power Maximum:** The highest rPDU power load within the group.
- **Power Average:** The average rPDU power load within the group.

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

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.

4.4.3 List

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

The inventory is subdivided into the following categories:

Rack PDUs

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

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

UPS

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

- **State:** The status of the UPS. Status is either normal or unavailable (loss of connectivity).
- **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 rPDU 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 rPDUs to which they are connected. They are not stand-alone sensors with their own IP addresses. In this release, the only valid sensors are rPDU-connected Geist™ SRT, GTHD or GTHD3 sensors.

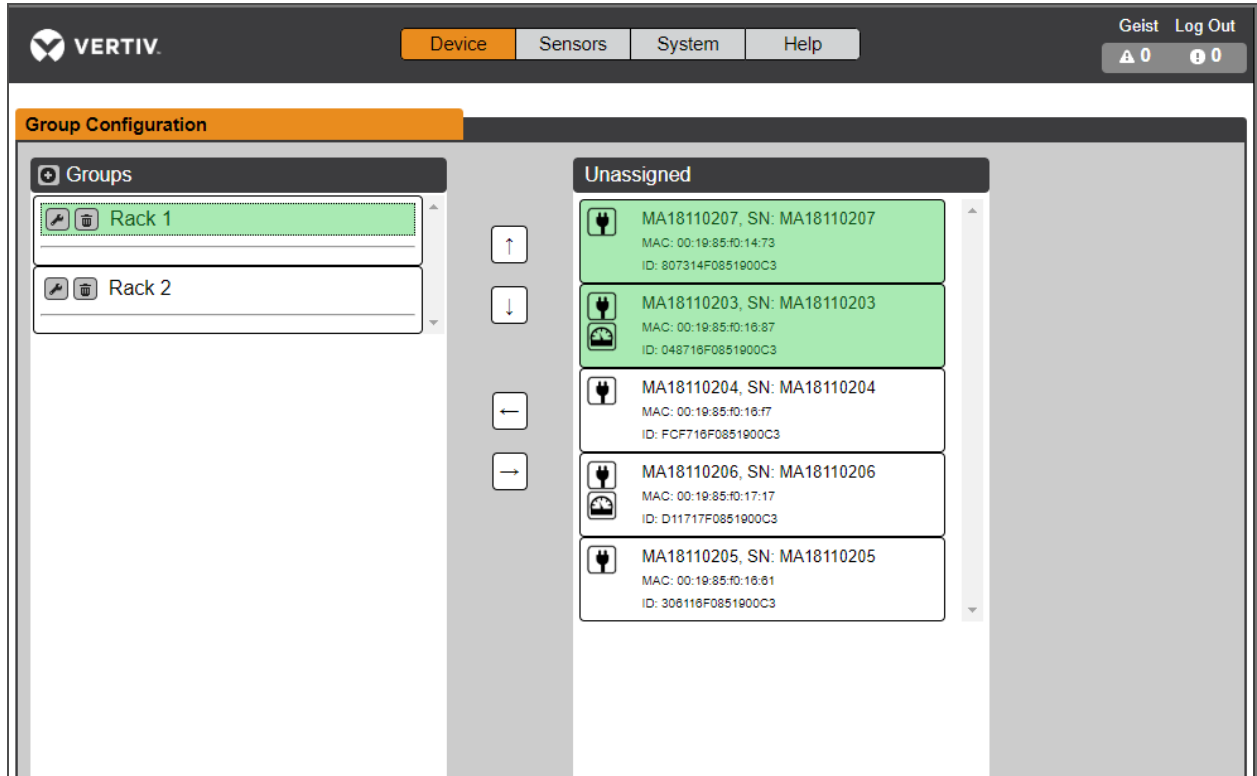
NOTE: The name of any device can be customized by logging into the device and editing through the Configuration icon.

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.

4.4.4 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 downstream devices, such as a rack with two rPDUs, UPS devices and environmental sensors or a row that includes multiple racks.

Figure 4.4 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, rPDU, Environmental Sensor or UPS.
- 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.
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.

4.5 Interfaces

Downstream Devices are combined to form groups; each device retains its own stand-alone user interface and SNMP data.

To access the Downstream 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-

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

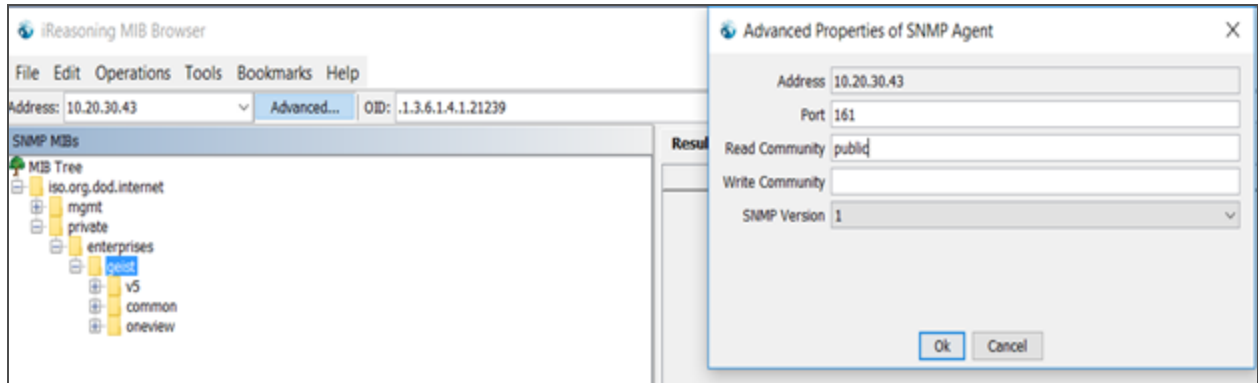
To access Downstream Device SNMP Data:

SNMP Data is available using port-mapped access through the master device IP address using the Geist™_v5 MIB. The MIB file is downloadable from the master device 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 downstream devices must be capable of accepting a unique SNMP port number per monitored device.

Figure 4.5 MIB Browser



4.5.1 Group SNMP Data

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

- **v5:** Contains data points for the individual Master rPDU.
- **Oneview:** Contains data points for aggregated data across all downstream devices.

4.5.2 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 a downstream device.
- SNMP traps and alarms are routed from a device to the management network through the master device.

5 APPENDICES

Appendix A: Technical Support

A.1 Resetting an rPDU

If an rPDU loses communication, the processor may be manually rebooted without affecting power to the outlets. Pressing the reboot button on the face of the IMD will reboot the processor. The web interface will remain offline during boot-up. For more information, see [Interchangeable Monitoring Device \(IMD-03X\)](#)

A.2 Service and Maintenance

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

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

A.3 More Technical Support

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

Americas

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

Europe and Middle East

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

Asia

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

A.4 Using Microsoft Exchange as an SMTP Server

If your facility uses a Microsoft Exchange email server, it can be used by the IMD rPDU to send Alarm and Warning notification emails. However, the Exchange server may need to be configured to allow SMTP connections from the unit first, as later versions of Exchange server often have SMTP services or basic authentication disabled by default. If you encounter difficulties in getting your IMD rPDU 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 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 rPDU cannot use IMAP or Microsoft's proprietary MAPI/RPC Exchange/Outlook protocols to send messages, you must enable SMTP by setting up an SMTP Send Connector in the Exchange server. More information on setting up an SMTP Send Connector in Exchange can be found at this Microsoft TechNet article: <http://technet.microsoft.com/en-us/library/aa997285.aspx>

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

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

To re-enable the AUTH LOGIN method:

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

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

Finally, once you have enabled SMTP, relaying and the AUTH LOGIN Basic Authentication method, you may also need to create a user account specifically for the IMD rPDU to log into. If you created an account prior to enabling the SMTP Send Connector or if you are trying to use an account created for another user and the IMD rPDU still cannot connect to the Exchange server, the account probably did not properly inherit the new permissions when you enabled them as above. This tends to happen more often on Exchange servers that have been upgraded since the account(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 rPDU to send mail through your Exchange server, then you may need to contact Microsoft's technical support for assistance in configuring your Exchange server to allow SMTP emails to be sent from a third-party, non-Windows device through your network.

Appendix B: Visible Light Communication (VLC)

The VLC feature on Upgradeable 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 rPDU power data to be obtained via the unit's display and all without physically connecting to the rPDU.

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.

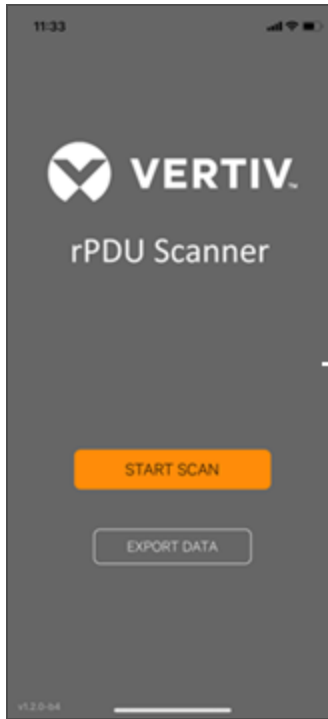
NOTE: With the release of firmware Version 3.3.0, Vertiv™ has added support for the VLC feature to all standard Metered and Monitored Upgradeable products, as well as a significant majority of its engineered-to-order range. Certain custom models of Upgradeable PDUs may not have VLC support within the 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.

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 rPDU.
- **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.

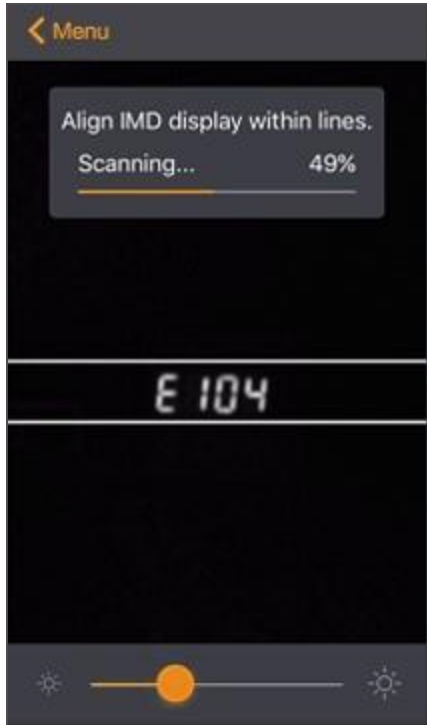
Figure A.1 Vertiv™ Mobile App Home Screen



To scan an rPDU

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

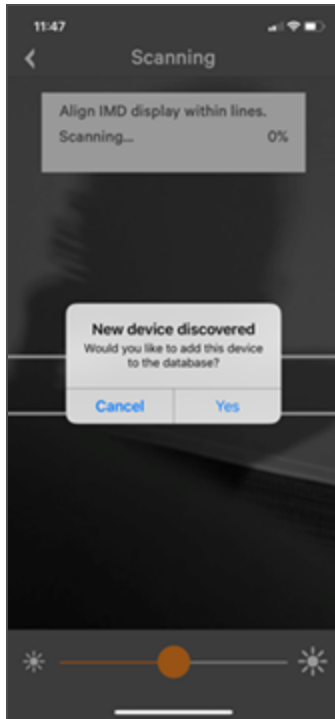
Figure A.2 Vertiv™ Mobile App Scanning Screen



- 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 A.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:

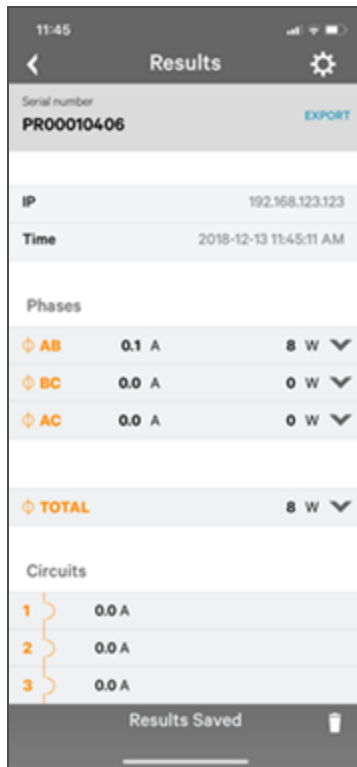
- **Scan failed:** Incorrect set of configuration.
- **Scan failed:** Incorrect data sequence.
- **Scan failed:** Adjust your position or the exposure and try again.

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 rPDU scanned using VLC.

Figure A.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 rPDU.

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.

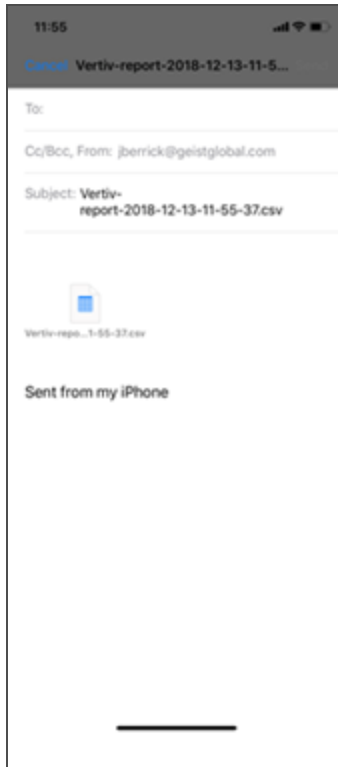
Figure A.5 Vertiv™ Mobile App Settings Screen



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 A.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 rPDU you scan adds a new entry to the database. There is no limit to the number of individual rPDU that can be added, but the database has a limit of 10 scans per rPDU. 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: rPDU Configuration and power data.

The rPDU Configuration Data includes:

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

The Power Data includes:

- Power Readings
- Totals

Table A.1 rPDU 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 A.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	2 va	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 A.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 A.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.

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.

Appendix E: Outlet LEDs

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 A.5 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 A.6 LED Status Description

MEASURED VOLTAGE	RELAY STATE	STATE	LED	
On	On or Unknown	Solid	Green	
Off	Off or Unknown	Solid	Red	
Off	On	Blinking ¹	Amber	Red
On	Off	Blinking ²	Amber	Green

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

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

Error Code

LEDs illuminate in Solid Amber during the following:

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

Appendix F: IMD Display Codes

Table A.7 IMD Display Codes

DISPLAY	IMD TYPE	EXPLANATION
<i>Err1</i>	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.
<i>8888</i>	IMD-02, IMD-03, IMD-3	IMD is booting and has yet to discover the simple display and shows <i>boot</i> on it. If this is displayed for more than a few seconds there is a problem the display board or with internal cabling.
<i>--</i> (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.
<i>boot</i>	IMD-01	IMD is booting and discovering the input board.
<i>boot</i>	IMD-02, IMD-03, IMD-3	Firmware is initializing. This will be displayed while firmware is being updated in slave boards.
<i>updt</i>	IMD-02, IMD-03, IMD-3	Firmware update in progress.
<i>rset dflt</i>	IMD-02, IMD-03, IMD-3	Following user action, <i>rset</i> (Reset) will appear during a parameter reset sequence. During a parameter reset, <i>dflt</i> (Default) will appear briefly.
<i>bcup</i>	IMD-02, IMD-03, IMD-3	<i>bcup</i> (Backup) will appear during a configuration backup.
<i>rest conf</i>	IMD-02, IMD-03, IMD-3	<i>rest</i> (Restore) and <i>Conf</i> (Configuration) will appear during a configuration restore .





Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA

© 2020 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 herein, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications are subject to change without notice.

VM1221_SL-70567_REV4_0520