VERTIV™

# Vertiv™ PowerGo Rack Power Distribution Unit

Installer/User Guide

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

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

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

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

### Technical Support Site

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

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

# TABLE OF CONTENTS

# 1 Important Safety Instructions

## Regulatory Compliance

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

## CE

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

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

## Federal Communications Commission (FCC)

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

The FCC standards specific to this equipment are:

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

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

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

This page intentionally left blank

# 2 Overview

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

Vertiv engineers took the robust Vertiv™ PowerGo rPDU design and incorporated an Interchangeable Monitoring Device (IMD). PDUs last for many years with the IMD design.

## 2.1 Environmental

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

**Table 2.1 Temperature Limits**

| Description | Minimum | Maximum |
|---|---|---|
| Operating | 0 °C (32 °F) | 45 °C (113 °F) |
| Storage | -40 °C (-40 °F) | 70 °C (158 °F) |

**Table 2.2 Humidity Limits**

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

**Table 2.3 Elevation Limits**

| Description | Minimum | Maximum |
|---|---|---|
| Operating | 0 m (0 ft) | 3050 m (10000 ft) |
| Storage | 0 m (0 ft) | 12200 m (40000 ft) |

## 2.2 Electrical

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

**Table 2.4 Receptacle Ratings**

| Type | Ratings |
|---|---|
| German Schuko | 250 VAC, 16 A |
| IEC-60320 C13 | 250 VAC, 10 A (UL & CSA 12 A, 250 VAC) |
| IEC-60320 C19 | 250 VAC, 16 A (UL & CSA 16 A, 250 VAC) |

## 2.3 Networking

The product communications requirements are defined in the next sections.

### 2.3.1 Ethernet

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

### 2.3.2 Protocols

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

### 2.3.3 User interfaces

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

# 3 Installation

Using the images in the mounting section, install the Vertiv™ PowerGo rPDU.

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

**To install unit:**

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

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

## 3.1 Mounting

Optional brackets are sold separately.

Figure 3.1 Toolless Mounting Hardware

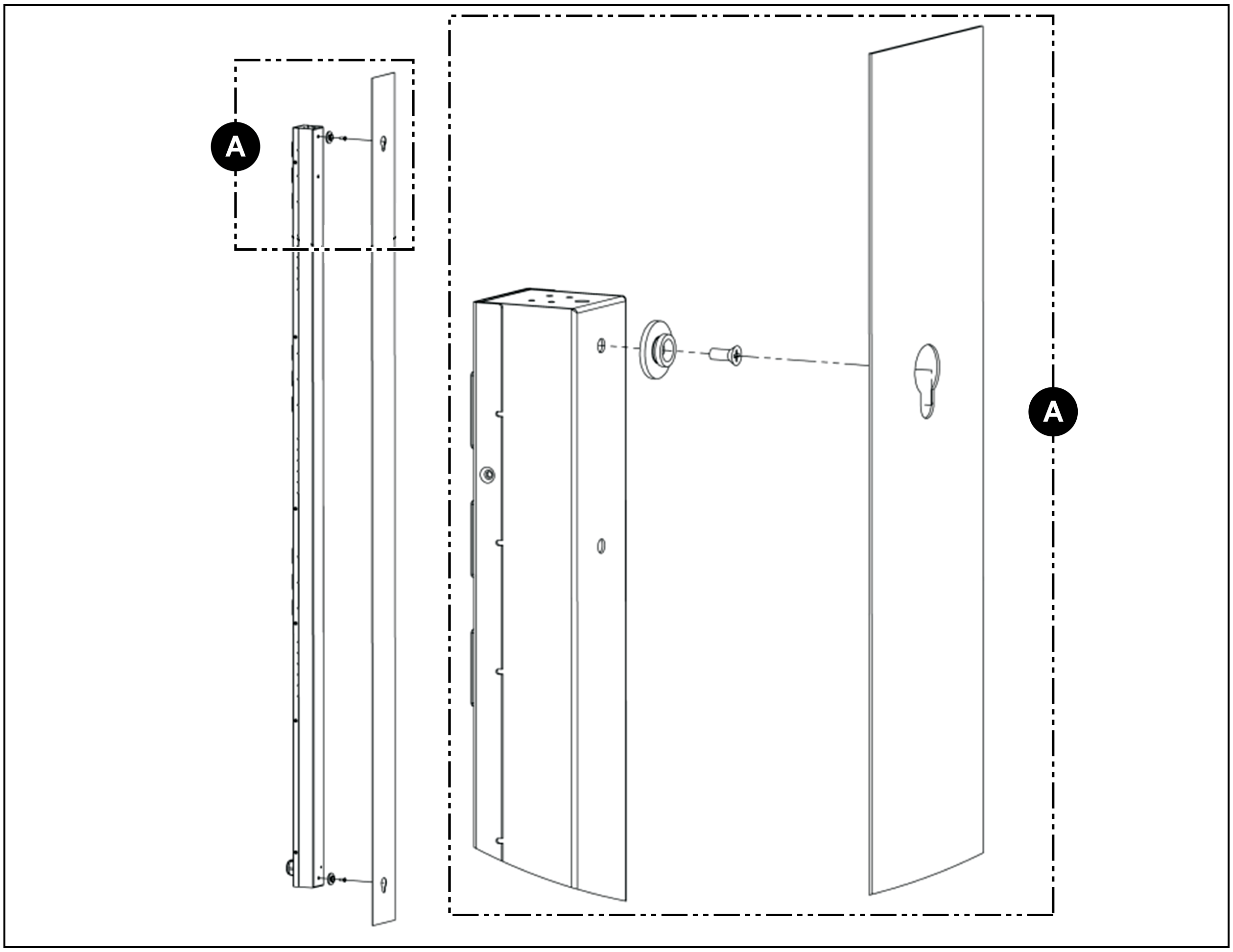


**Figure 3.2 Single Side Mount Two Units Brackets**

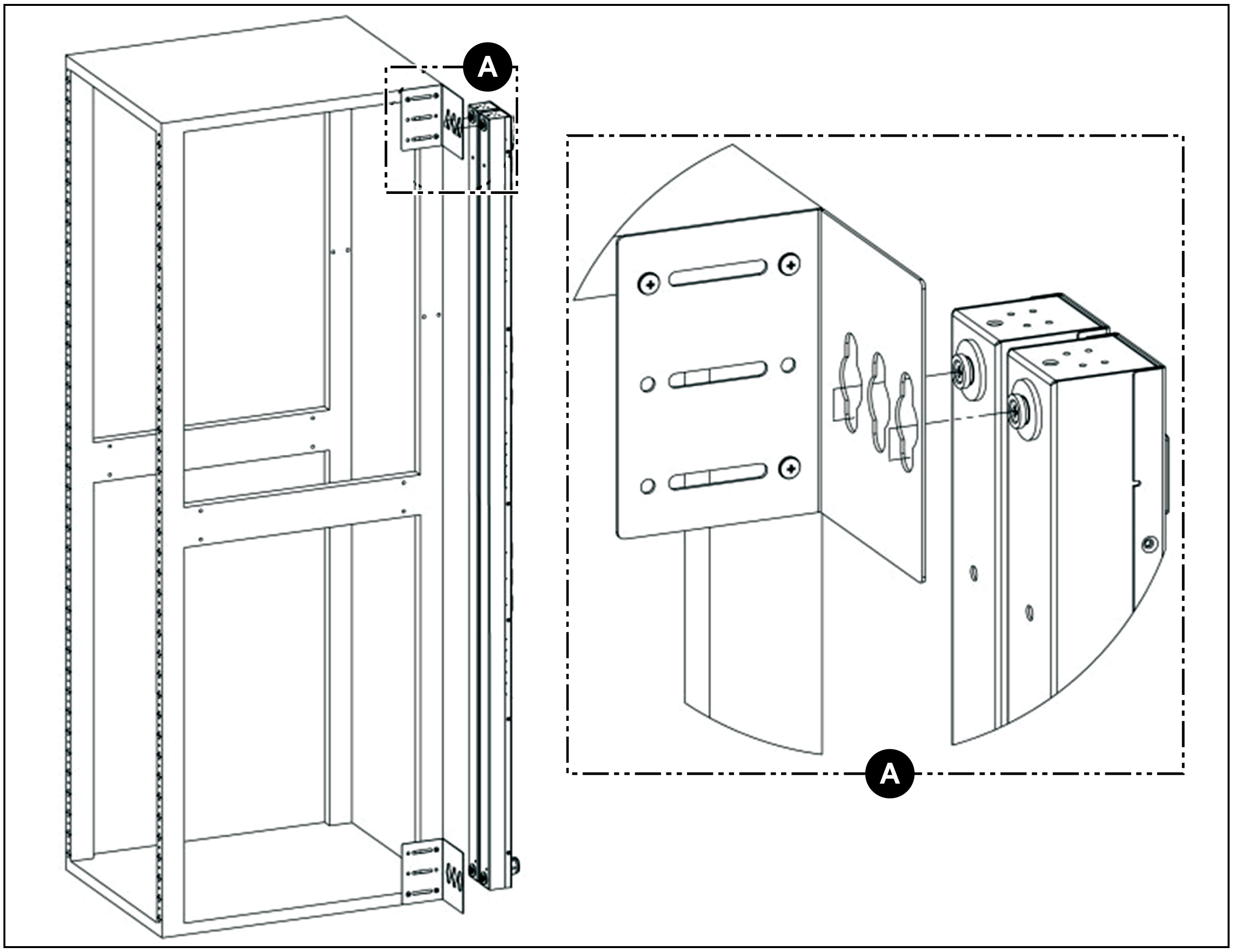


**Figure 3.3 Adjustable Mount Bracket**

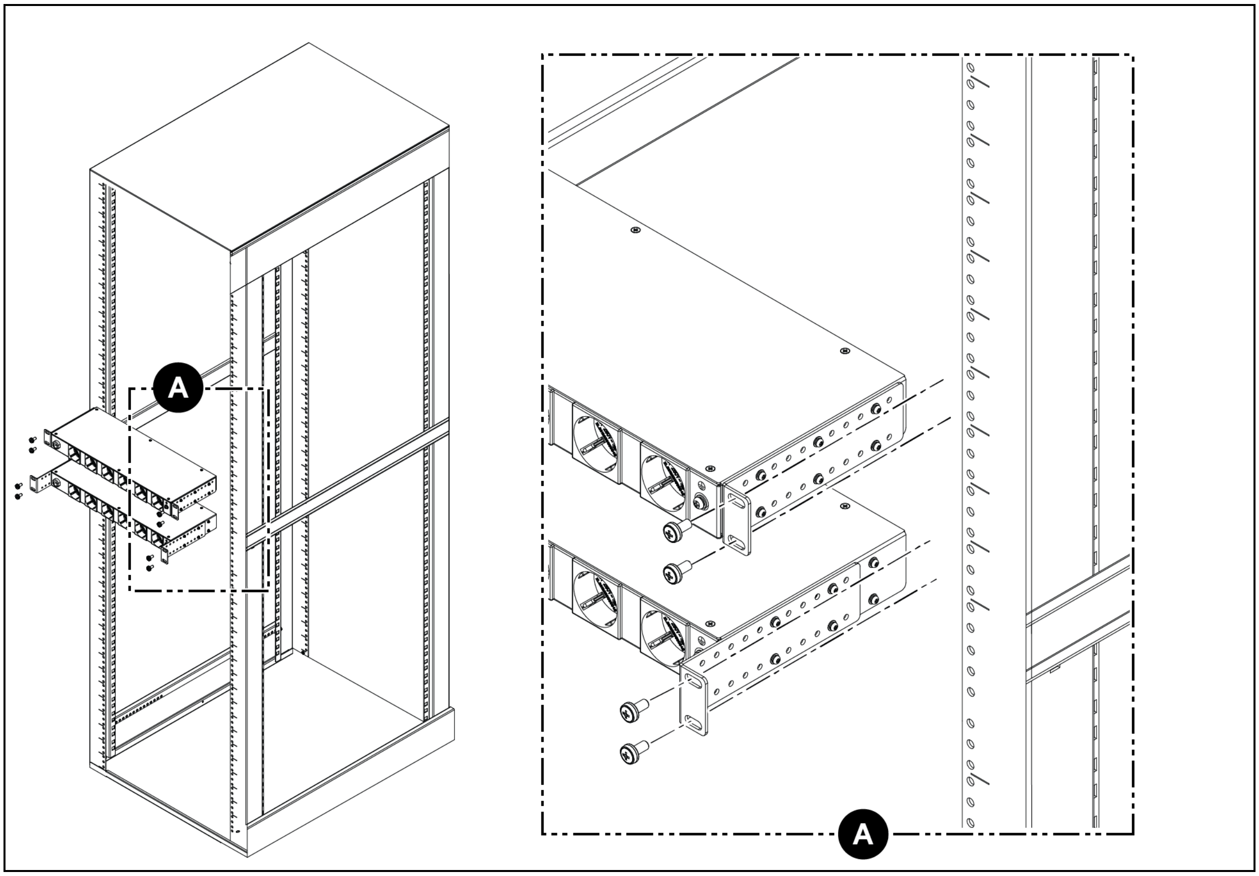
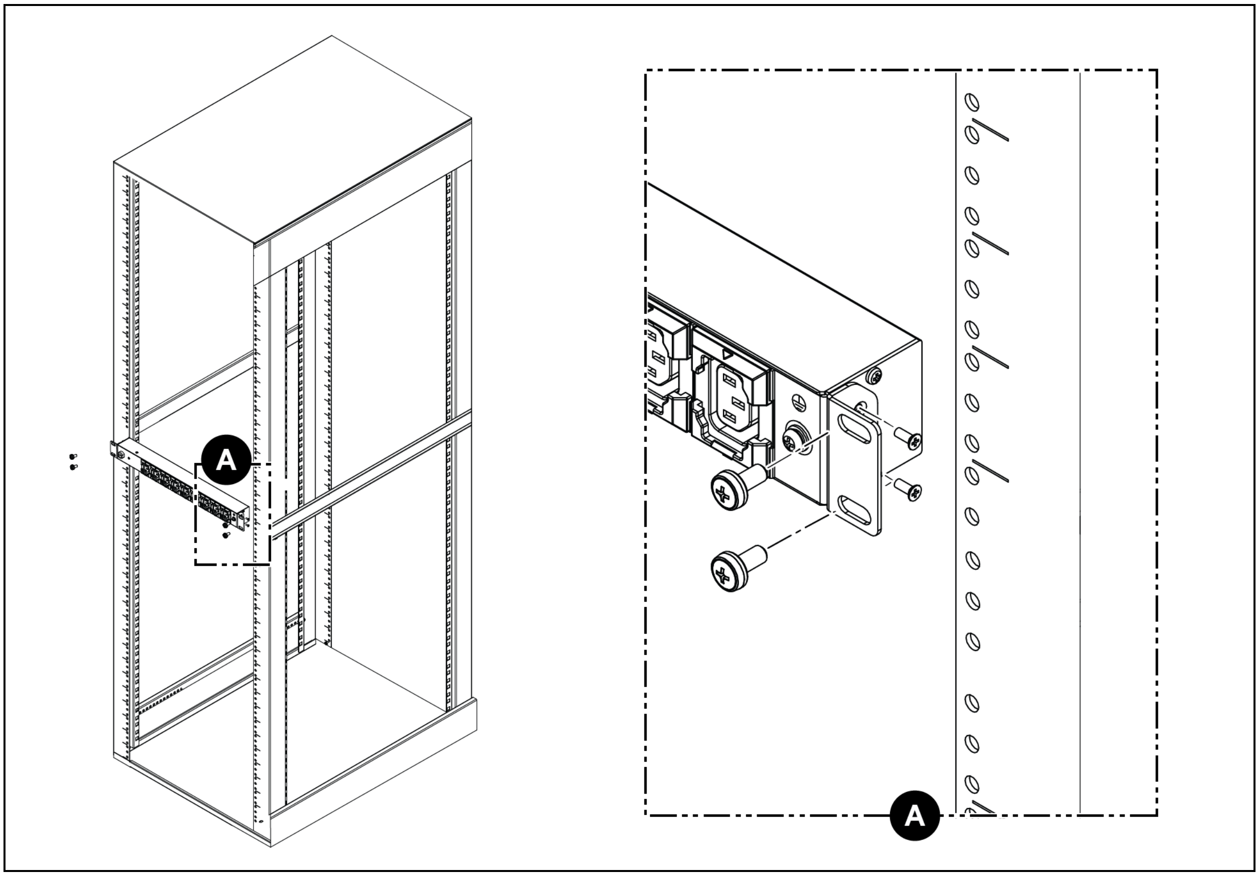


**Figure 3.4 19" (inch) Horizontal/Panel-Mount Brackets**



This page intentionally left blank

# 4 Security Best Practices

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

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

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

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

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

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

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

| Item | Description | Reference |
|---|---|---|
| Accounts and Passwords | Change the admin and user account names and passwords immediately to eliminate default credential access. | See Users on page 40. |
| IP Network Access | Enable/disable IPV4 and IPV6 network access to the card - disable unused network access. | See Network on page 44 . |
| SSHv2 Access | Enable/disable SSHv2 access for diagnostic and configuration support - disable when not in use. | See SSH on page 60. |
| Web Service Protocol | Select HTTPS to use SSL encryption when accessing data through the web user interface. | See Web server on page 53. |
| TLS Certificates | When using HTTPS, install your own TLS Certificates from a trusted certificate authority or generate alternative self-signed certificates. | See SSL Certificate: Allows you to upload your own signed SSL Certificate file to replace the default one. The certificate can be either self-signed or signed from a Certification Authority. SSL Certificate must be in either PEM or PFX (PKCS12) format. on page 53. |
| Remote Write Web Access | To control/write through web interface, you must log in remotely and have either an admin level or control level user account.<br>To prohibit remote access, disable both HTTP and HTTPS. | See Web server on page 53. |

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

| Item | Description | Reference |
|---|---|---|
| | ⚠ **WARNING! Disabling both HTTP and HTTPS will immediately terminate this connection and remote access will only be available using SSH.** | |
| Communication Protocols | Enable/disable SNMP - disable unused protocols. | See SNMP on page 62. |
| SNMP Version Settings | Enable/disable the desired SNMP versions, consider using SNMPv3 with user authentication and encryption. | See SNMP on page 62. |
| SNMP Access Table Settings | For each SNMPv1/v2c Access table entry, set the SNMP Access Type to Read-Only to prevent changes to the device from the hosts identified in the table entry. | See SNMP on page 62. |
| SNMP Community Strings | Use suitably strong values for SNMP communication in line with your organizations password policy. | See SNMP on page 62. |
| SNMPv3 Settings | Use suitable hashing and encryption algorithms for SNMPv3 Authentication and Privacy settings to make SNMPv3 communications more secure. | See SNMP on page 62. |
| Guest user account | This account should remain disabled, unless required. As it provides read-only access to device and may give additional context to device settings if enabled. | See Users on page 40. |

For added security, the local network firewall and gateway may be restricted to allow only the necessary traffic on the required network ports.

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

## 4.1 Risk Assessment

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

## 4.2 Physical Security

The IMD-3X is designed and intended to be deployed and operated in a physically secure location. Vertiv recommends a review of the physical security and operating environment of the unit. Since an attacker or insider threat can cause serious disruption, below are some recommended best practices that include, but are not limited to:

- Restrict access to areas, racks, and units with encrypted card RFID/badges, unique multi-factor passcode authentication for access, man traps, and biometric scanners for physical access to the equipment.
- Trusted and background checked security guards with 24x7x365 physical presence and written logs to help document and note physical access to a data center, building and rack.
- Restricted physical access to telecommunications equipment and network cabling. Physical access to the telecommunication lines and network cabling should be restricted to protect against attempts to intercept or sabotage communications. Best practices include uses of metal conduits for the network cabling running between equipment cabinets.

## 4.3 Account Access

The IMD-3X account access privileges should be administered to provide the least account functions that still enables the end-user to perform their job functions. Login to the IMD-3X should be restricted to legitimate users. Some of the following best practices should be adopted by an organization's written procedures for network and equipment access:

- First login to the IMD-3X requires credentials to be created.
- No account/logon sharing. Each user should have their own specific account and password. Logging functions of the IMD-3X expect each account to be a unique non-shared user.
- Admins should restrict access and privileges to only the required functions of the user's job function.
- Restrict all admin-level privileges (Such as firmware updates, protocol enablement/disablement.) to only approved administrators.
- Ensure password strength, complexity, and length requirements are enforced at the highest level per company IT policy.
- Ensure terminated employees instantly are removed from accessing the unit. Some examples include the user of a AAA, TACACS+ user authentication process.
- Enforce session time-out after a period of inactivity.
- Use the remote syslog facility to alert you to system and network events, security threats, and visibility into the device to troubleshoot problems. (This may also be required in your environment for PCI-DSS/SOX/HIPAA compliance).

This page intentionally left blank

# 5 Setup

## 5.1 Interchangeable Monitoring Device

The Interchangeable Monitoring Device (IMD) is the core behind the Vertiv™ PowerGo rPDU line of power products. Installing the wrong IMD for replacement in an rPDU can lead to damage to the IMD.

### 5.1.1 Basic

The Basic Vertiv™ PowerGo rPDU is the baseline for the GU line of products.

### 5.1.2 Unit monitored

Vertiv™ PowerGo rPDUs are shipped with the IMD-3X module.

**Figure 5.1 IMD-3X Module**

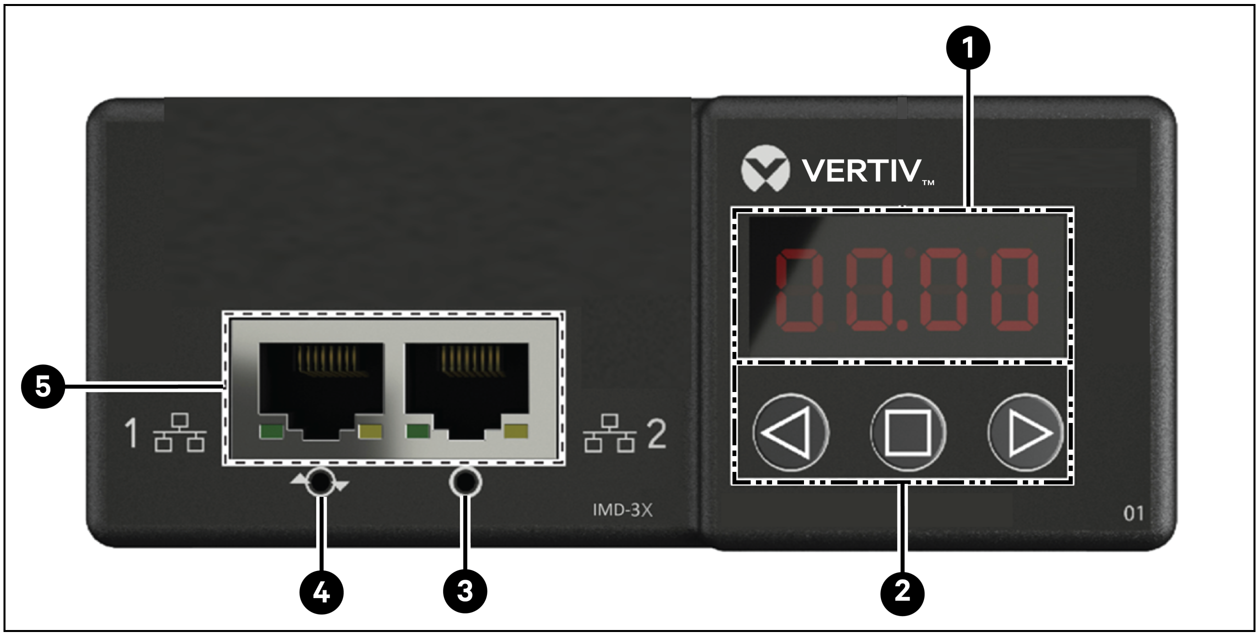


**Table 5.1 IMD-3X Module Descriptions**

| Number | Name | Description |
|---|---|---|
| 1 | Local Display | The local display shows the phase, line and circuit current values (in amperes). |
| 2 | Display Buttons | There are three buttons near the IMD display: a back button, a forward button and a center button. The functions of these buttons are described in the Table 5.2 on the next page. |
| 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 | Hard-Reboot | Pressing the hard-reboot button reboots the IMD. This acts as a power-cycle for the IMD; it does not change or remove any user information. |

**Table 5.1 IMD-3X Module Descriptions (continued)**

| Number | Name | Description |
|---|---|---|
| | Button | |
| 5 | Dual Ethernet Ports | The dual Ethernet ports act as a two-port Ethernet switch, allowing for multiple devices to be daisy- chained. The dual Ethernet ports can be independently configured dual Ethernet network interfaces, allowing the rPDU to connect to two different networks. |

**Table 5.2 Display Button Functions**

| Button | Symbol | Description |
|---|---|---|
| Back Button | ◁ | Press to decrement to previous channel.<br>Holding the button for 3 seconds initiates a configuration backup. The display will show a **bcup** message while the backup is being generated and will then go back to normal operation. The backup is stored on available web storage devices and the operation will do nothing if no such drives are available. |
| Forward Button | ▷ | Press to increment to next channel.<br>Holding this button for 3 seconds initiates a configuration restore. The display will show a **load** message followed by a **conf** message and then a 3 second countdown. Once the countdown expires, a **8888** message is displayed and the backup will be applied. The backup will be read from web storage devices. If the button is released at any time during this sequence, the restore is aborted. Once the backup is applied, or if there are no backup images or no web storage device attached, the display will then go back to normal operation. |
| Center Button | □ | Toggle between scrolling and static display modes. Holding this button for 3 seconds initiates a parameter reset sequence. This sequence consists of an **rset** message, followed by a **dflt** message and then a 3 second countdown. Once the countdown expires, an **8888** message is displayed and the network, *http* user accounts and *LDAP/RADIUS* information is reset to default values. If the button is released at any time during this sequence, the reset will be aborted. |
| Center Button x3 | □ | Pressing this button 3 times within 2 seconds enables VLC mode. Pressing the button while VLC mode is active returns the unit to the standard current display . |
| Back and Forward Buttons | ◁ and ▷ | Pressing both buttons at the same time flips the display 180 degrees. |
| Back and Center Buttons | ◁ and □ | Pressing both buttons at the same time displays the primary IPv4 address for the unit. |

## 5.1.3 Switched and unit level monitored

Vertiv™ PowerGo Switched unit level monitored are shipped with the IMD-3X module.

Figure 5.2 IMD-3X Module

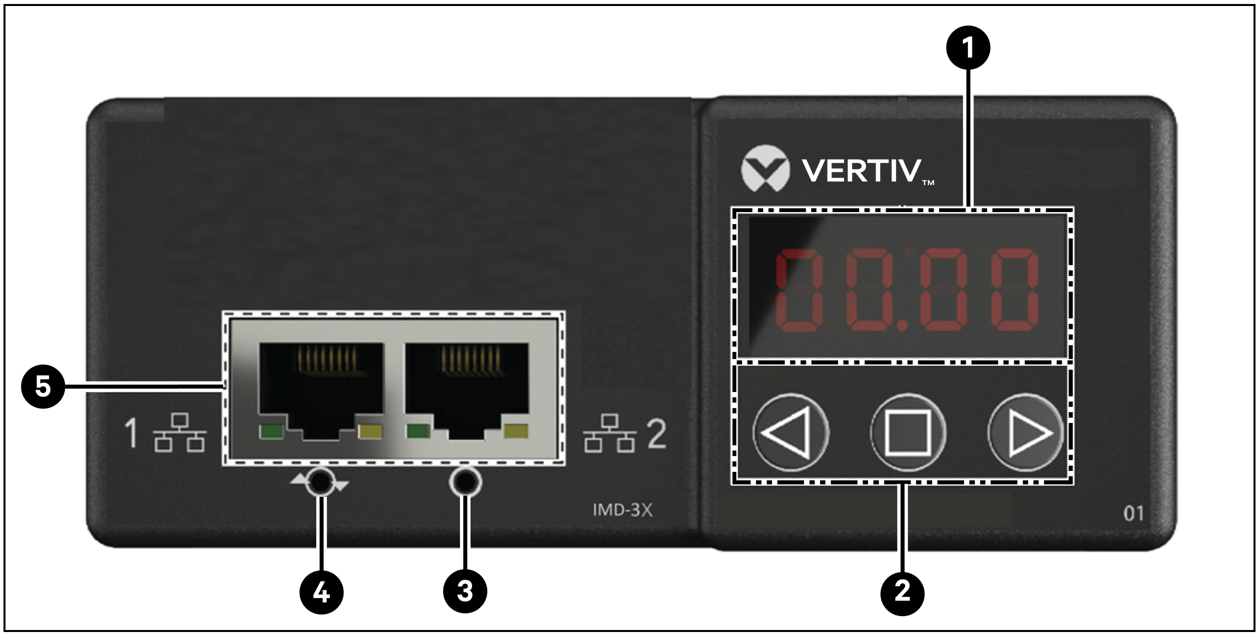


Table 5.3 IMD-3X Module Descriptions

| Number | Name | Description |
|---|---|---|
| 1 | Local Display | The local display shows the phase, line and circuit current values (in amperes). |
| 2 | Display Buttons | There are three buttons near the IMD display: a back button, a forward button and a center button. The functions of these buttons are described in the Table 5.4 on the next page. |
| 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 | Hard-Reboot Button | Pressing the hard-reboot button reboots the IMD. This acts as a power-cycle for the IMD; it does not change or remove any user information. |
| 5 | Dual Ethernet Ports | The dual Ethernet ports act as a two-port Ethernet switch, allowing for multiple devices to be daisy- chained. The dual Ethernet ports can be independently configured dual Ethernet network interfaces, allowing the rPDU to connect to two different networks. |

## Display Buttons

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

**Table 5.4 Display Button Functions**

| Button | Symbol | Description |
|---|---|---|
| Back Button | ◁ | Press to decrement to previous channel.<br>Holding this button for 3 seconds initiates a configuration backup. The display will show a **bcup** message while the backup is being generated and will then go back to normal operation. The backup is stored on available web storage devices and the operation will do nothing if no such drives are available. |
| Forward Button | ▷ | Press to increment to next channel.<br>Holding this button for 3 seconds initiates a configuration restore. The display will show a **load** message followed by a **conf** message and then a 3 second countdown. Once the countdown expires, a **8888** message is displayed and the backup will be applied. The backup will be read from web storage devices. If the button is released at any time during this sequence, the restore is aborted. Once the backup is applied, or if there are no backup images or no web storage device attached, the display will then go back to normal operation. |
| Center Button | □ | Toggle between scrolling and static display modes. Holding this button for 3 seconds initiates a parameter reset sequence. This sequence consists of an **rset** message, followed by a **dflt** message and then a 3 second countdown. Once the countdown expires, an **8888** message is displayed and the network, http, user accounts and LDAP/RADIUS information are reset to default values. If the button is released at any time during this sequence, the reset will be aborted. |
| Center Button x3 | □ | Pressing this button three times within 2 seconds enables VLC mode. Pressing the button while VLC mode is active returns the unit to the standard current display. |
| Back and Forward Buttons | ◁ and ▷ | Pressing both buttons at the same time flips the display 180 degrees. |
| Back and Center Buttons | ◁ and □ | Pressing both buttons at the same time displays the primary IPv4 address of the unit. |

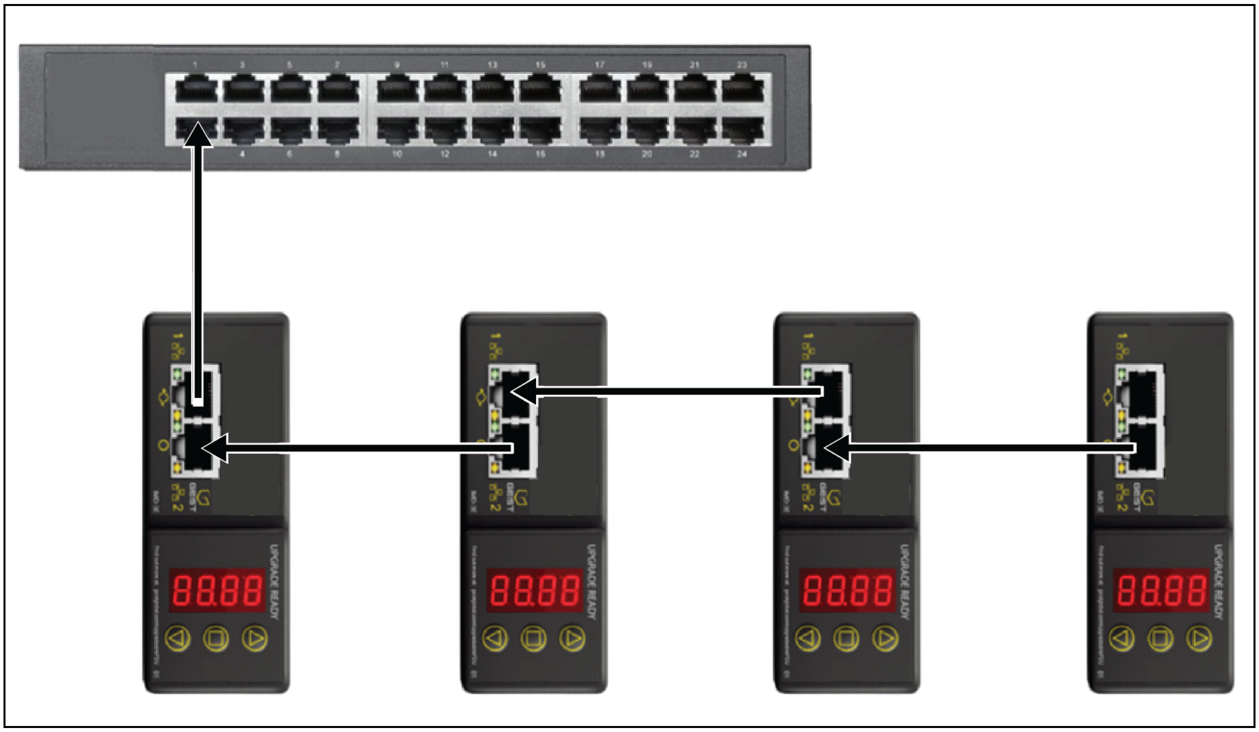
## 5.1.4 Rapid Spanning Tree Protocol (RSTP)

Monitored devices, built with the IMD-3X, include two Ethernet Ports that work together as an internal Ethernet Bridge. One of these ports can be used to connect the IMD to an existing network or both ports can be used at the same time to connect one IMD to another in a daisy chain configuration.

### Daisy-Chaining

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

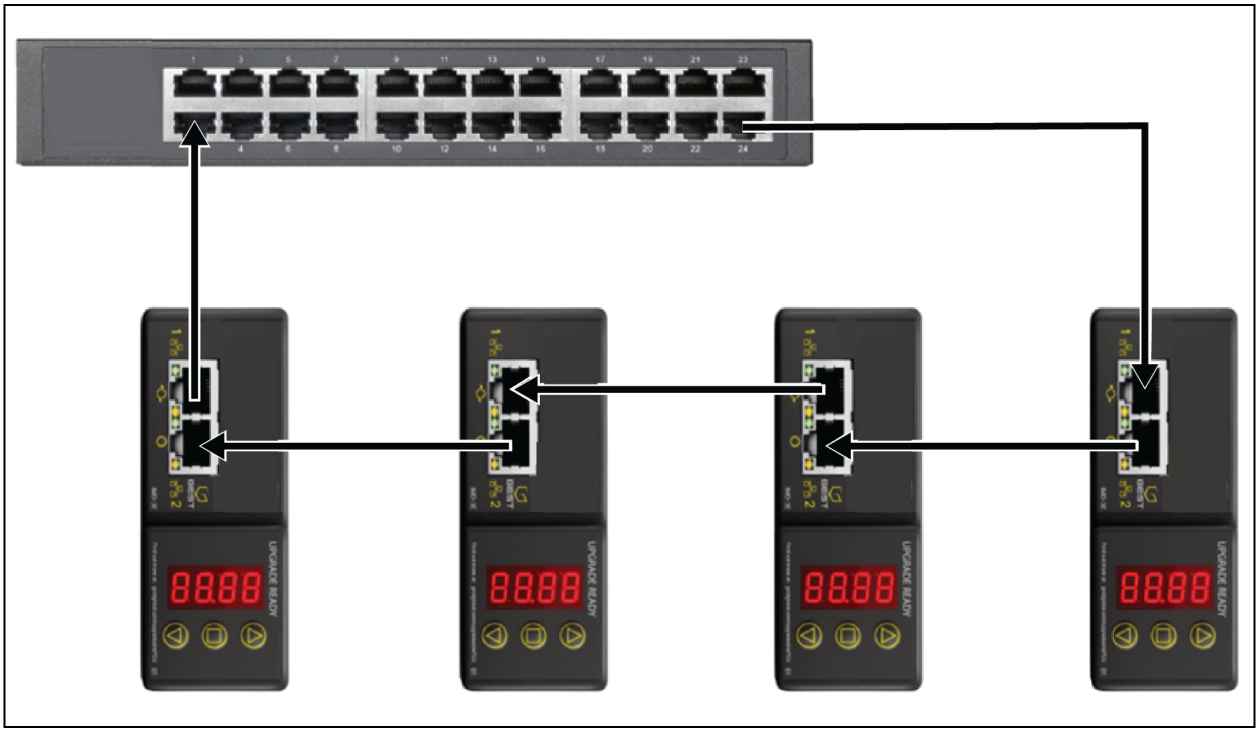
**Figure 5.3 Daisy-Chaining**



## Fault Tolerant Daisy-Chaining

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

**Figure 5.4 Fault Tolerant Daisy Chaining**



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

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

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

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

## 5.2 Network Setup

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

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

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

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

- **IP Address:** *192.168.123.123*

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

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

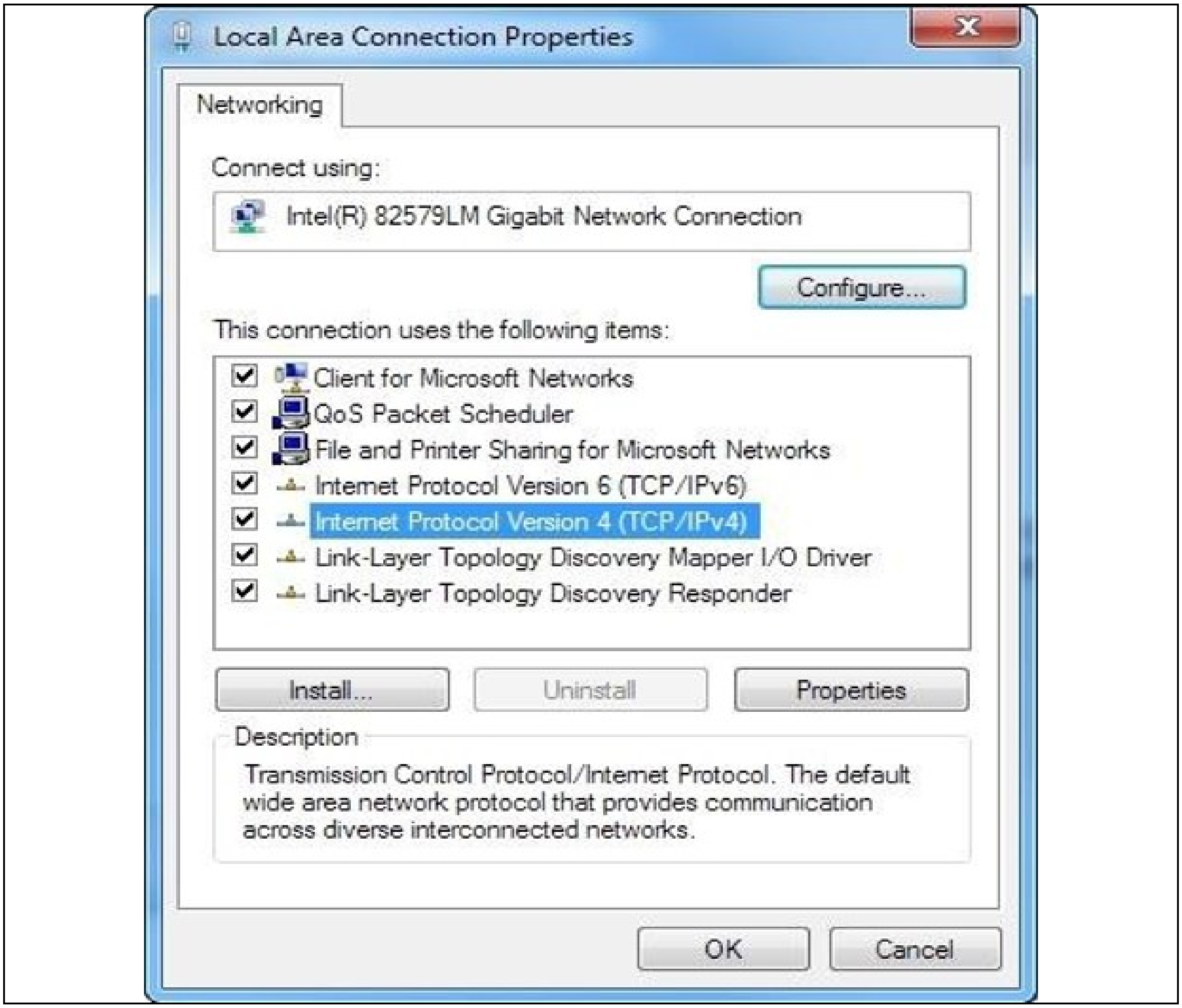
**To set up the network for a Windows operating system:**

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

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

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

**Figure 5.5 Local Area Connection Properties**



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82579LM Gigabit Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

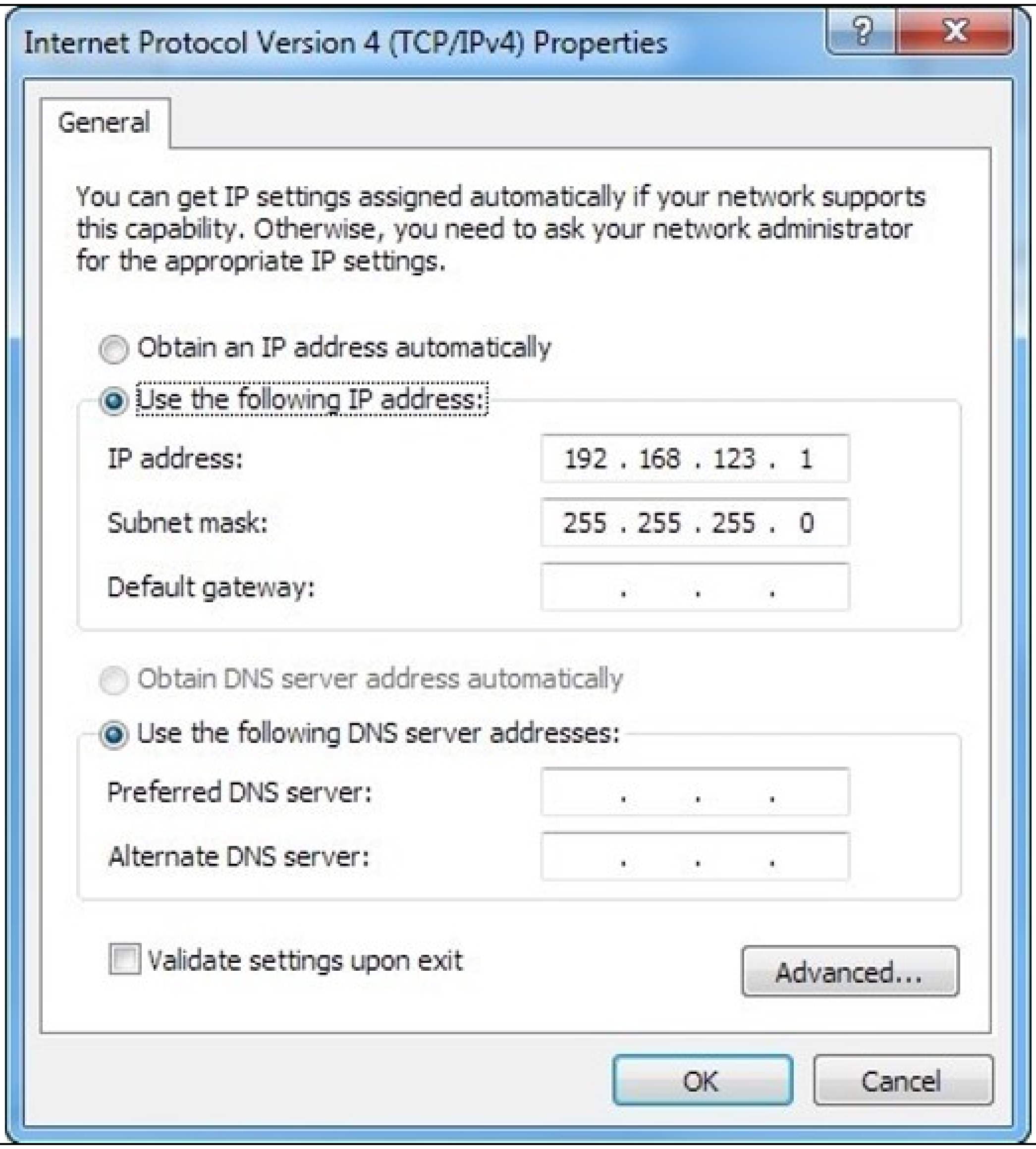
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

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

**Figure 5.6 Internet Protocol Version 4**



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 123 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

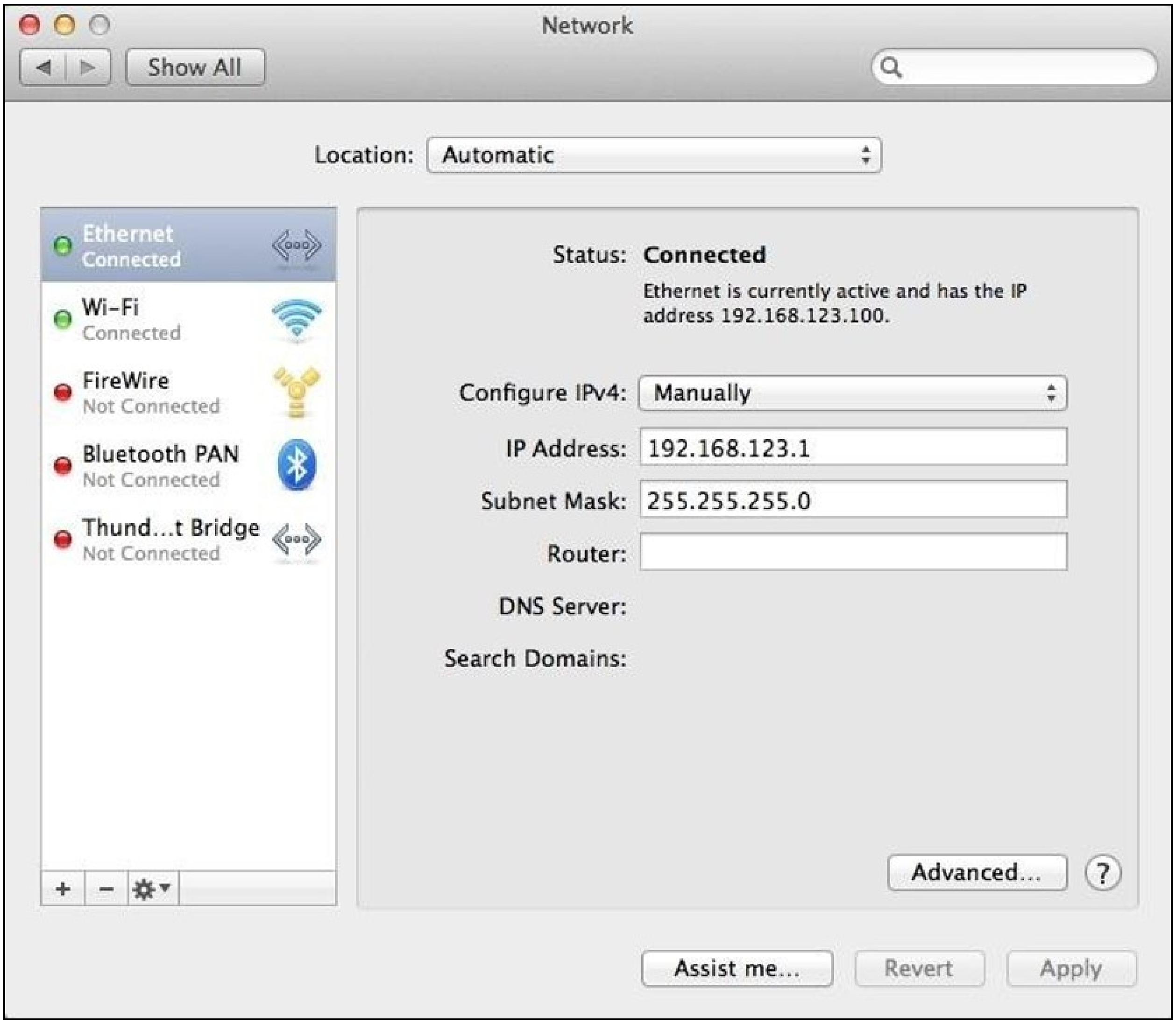
5. Choose *Use the following IP address*, set IP address to **192.168.123.1** and Subnet Mask to **255.255.255.0** . For initial setup, Default Gateway and the DNS Server entries can be left blank. Select *OK* - *OK* to close both the Internet Protocol Properties and Local Properties windows.
6. In a web browser, enter **http://192.168.123.123** to access the unit. If you are setting up the unit for the first time, the unit requires you to create an Admin account and password before you can proceed.
7. After the Admin account is created, login to the unit.

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

**To set up the network for a MAC:**

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

**Figure 5.7 MAC System Preferences**



Location: Automatic

Ethernet
Connected

Wi-Fi
Connected

FireWire
Not Connected

Bluetooth PAN
Not Connected

Thund...t Bridge
Not Connected

Status: **Connected**

Ethernet is currently active and has the IP address 192.168.123.100.

Configure IPv4: Manually

IP Address: 192.168.123.1

Subnet Mask: 255.255.255.0

Router:

DNS Server:

Search Domains:

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

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

4. After the Admin account is created, login to the unit.

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

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

## 5.3 Web User Interface

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

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

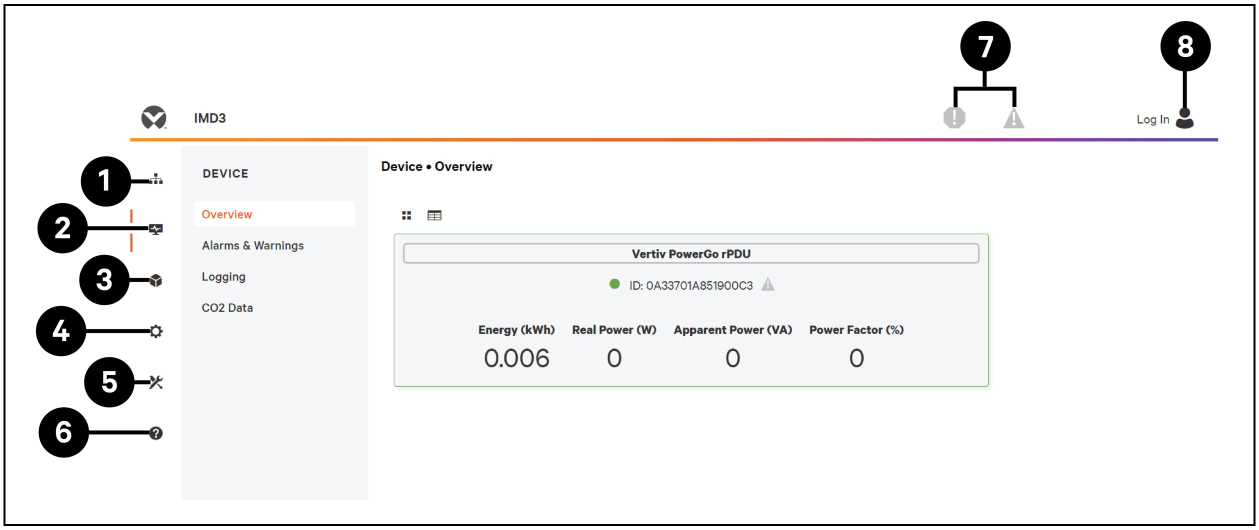
**NOTE: If Clock not set. appears at the bottom right of the page, follow procedures in Time on page 59.**

### 5.3.1 Main menu

The Main Menu is located vertically on the far left side. See Figure 5.8 below for Main Menu.

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

Figure 5.8 Main Menu



| Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) |
|---|---|---|---|
| 0.006 | 0 | 0 | 0 |

**Table 5.5 Main Menu Descriptions**

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

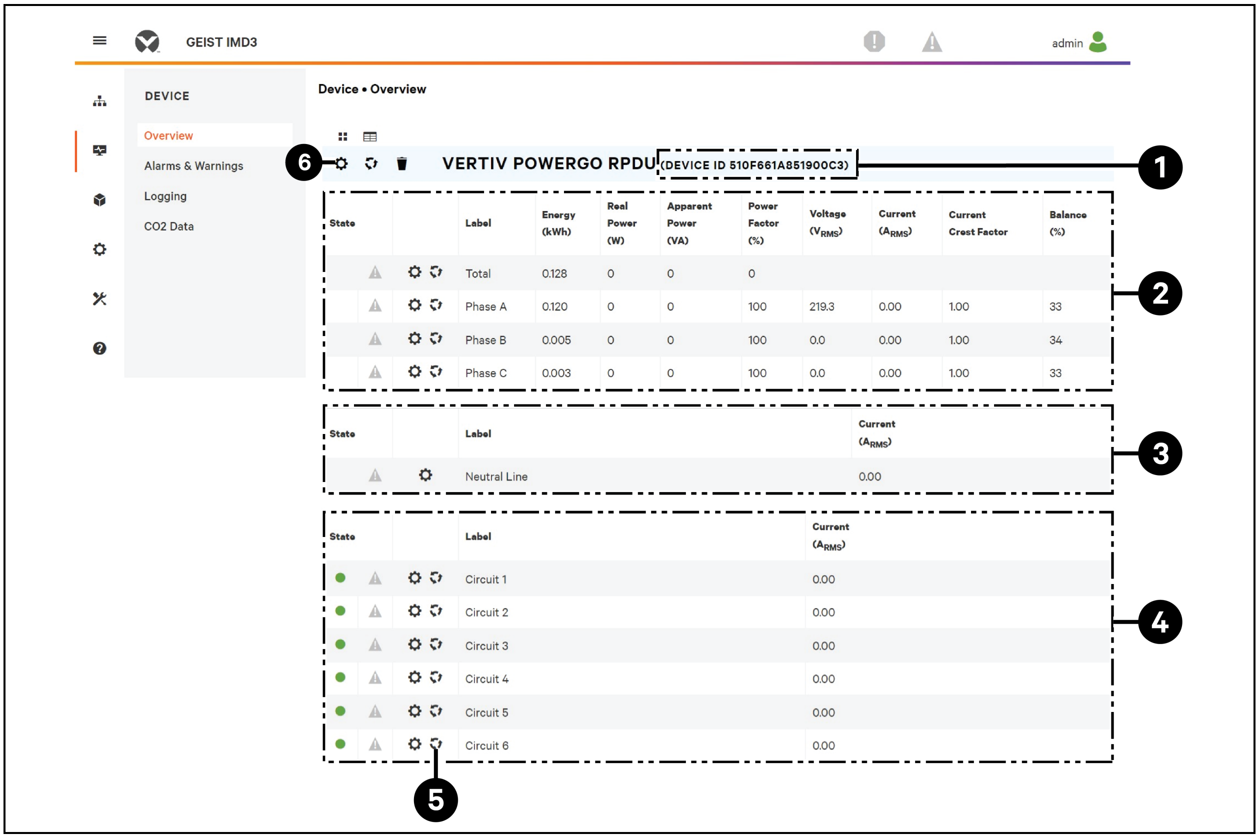
## 5.4 Device Sub Menu

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

### 5.4.1 Overview

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

**Figure 5.9 Device Overview Sub Menu Descriptions**



Device • Overview

VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Current Crest Factor | Balance (%) |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Total | 0.128 | 0 | 0 | 0 | | | | |
| | | Phase A | 0.120 | 0 | 0 | 100 | 219.3 | 0.00 | 1.00 | 33 |
| | | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 | 34 |
| | | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 | 33 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| | | Neutral Line | 0.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ● | | Circuit 1 | 0.00 |
| ● | | Circuit 2 | 0.00 |
| ● | | Circuit 3 | 0.00 |
| ● | | Circuit 4 | 0.00 |
| ● | | Circuit 5 | 0.00 |
| ● | | Circuit 6 | 0.00 |

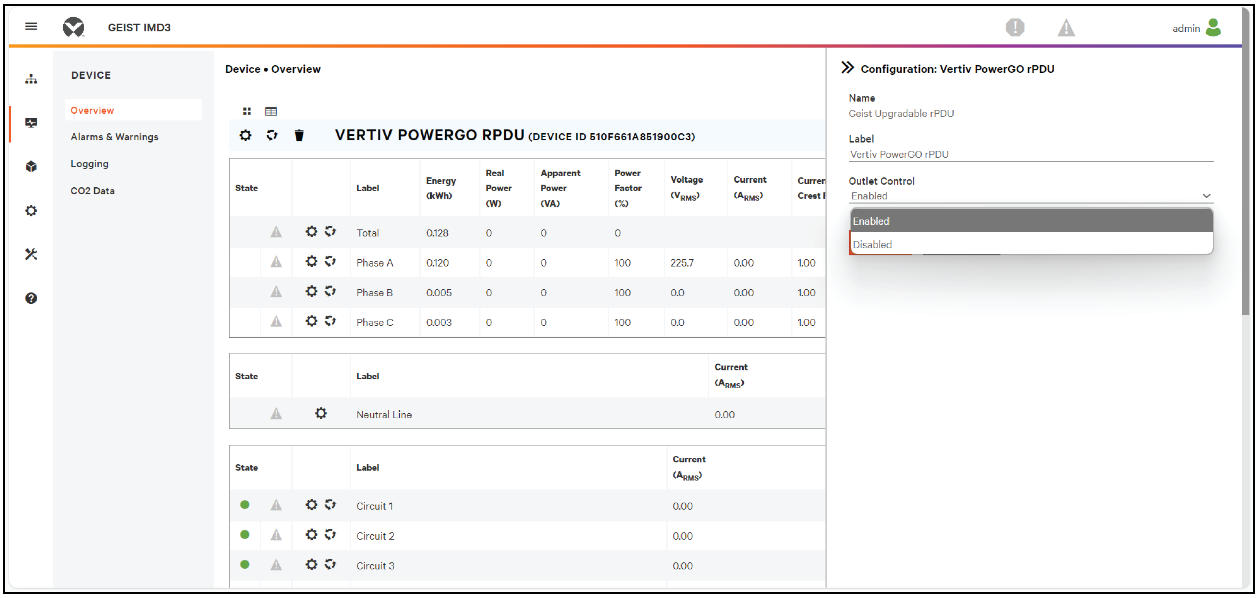
### Table 5.6 Device Overview Sub Menu Descriptions

| Number | Name | Description |
|---|---|---|
| 1 | Device ID | Unique product identification and cannot be changed. May be required for technical support. |
| 2 | Total and Individual Phase Monitor | Displays AC current, voltage, and power statistics for each individual phase and for the total of all phases combined. Current Crest Factor and Phase Balance (%) are also indicated. |
| 3 | Line | Displays the current (in Amps RMS) on 3-phase Wye units. This is not shown on single phase and 3-phase Delta units. |
| 4 | Current Monitor | Displays AC current draw statistics for each individual circuit on the rPDU. |
| 5 | Operation Icon | Applies to Outlet Switched rPDUs ONLY - Modify settings. |
| 6 | Configuration Icon | Applies to Outlet Switched rPDUs ONLY - Modify label name. |

### To change a device label:

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

### Figure 5.10 Changing Device Label



Device • Overview

VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Curren Crest F |
|---|---|---|---|---|---|---|---|---|---|
| | | Total | 0.128 | 0 | 0 | 0 | | | |
| | | Phase A | 0.120 | 0 | 0 | 100 | 225.7 | 0.00 | 1.00 |
| | | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |
| | | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| | | Neutral Line | 0.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ● | | Circuit 1 | 0.00 |
| ● | | Circuit 2 | 0.00 |
| ● | | Circuit 3 | 0.00 |

Configuration: Vertiv PowerGO rPDU

Name
Geist Upgradable rPDU

Label
Vertiv PowerGO rPDU

Outlet Control
Enabled

### To change device operation:

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

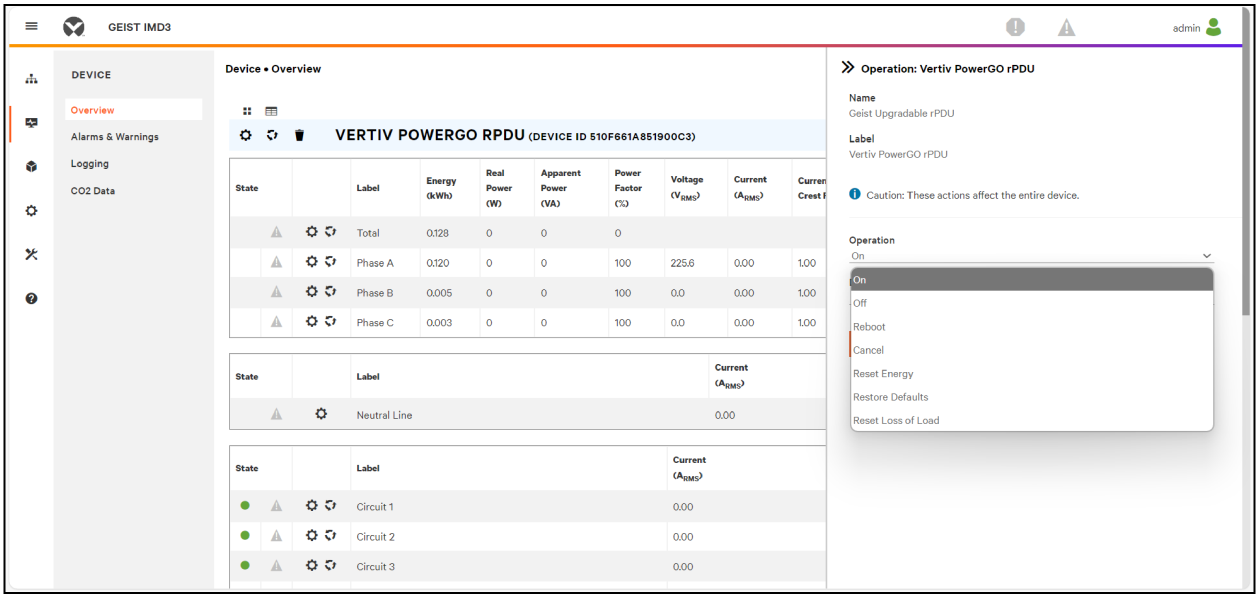
**NOTE: These actions affect the entire device.**

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

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

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

**Figure 5.11 Device Change Operation**



Device • Overview

VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Curren Crest F |
|---|---|---|---|---|---|---|---|---|---|
| | ⚠ ⚙ ⟳ | Total | 0.128 | 0 | 0 | 0 | | | |
| | ⚠ ⚙ ⟳ | Phase A | 0.120 | 0 | 0 | 100 | 225.6 | 0.00 | 1.00 |
| | ⚠ ⚙ ⟳ | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |
| | ⚠ ⚙ ⟳ | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| | ⚠ ⚙ | Neutral Line | 0.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ● | ⚠ ⚙ ⟳ | Circuit 1 | 0.00 |
| ● | ⚠ ⚙ ⟳ | Circuit 2 | 0.00 |
| ● | ⚠ ⚙ ⟳ | Circuit 3 | 0.00 |

Operation: Vertiv PowerGO rPDU

Name
Geist Upgradable rPDU

Label
Vertiv PowerGO rPDU

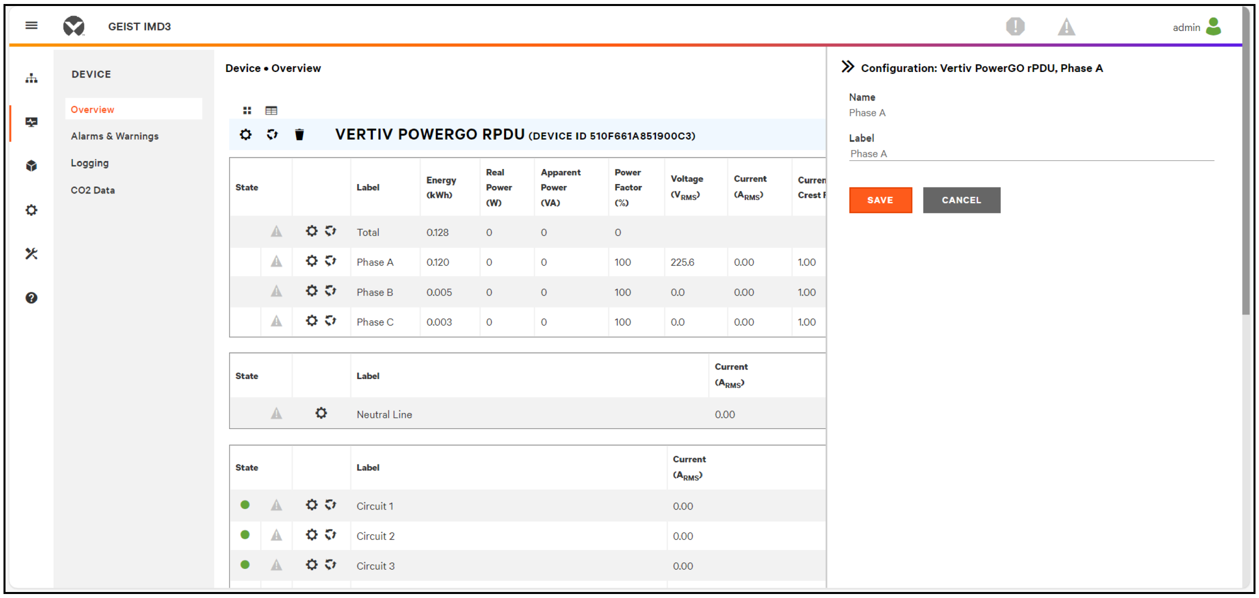
Caution: These actions affect the entire device.

Operation
On

### To change a phase or circuit label:

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

### Figure 5.12 Changing Phase or Circuit Label



VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Curren Crest F |
|---|---|---|---|---|---|---|---|---|---|
| ⚠ | ⚙ ⚙ | Total | 0.128 | 0 | 0 | 0 | | | |
| ⚠ | ⚙ ⚙ | Phase A | 0.120 | 0 | 0 | 100 | 225.6 | 0.00 | 1.00 |
| ⚠ | ⚙ ⚙ | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |
| ⚠ | ⚙ ⚙ | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ⚠ | ⚙ | Neutral Line | 0.00 |

| State | | | Label | Current ($A_{RMS}$) |
|---|---|---|---|---|
| ● | ⚠ | ⚙ ⚙ | Circuit 1 | 0.00 |
| ● | ⚠ | ⚙ ⚙ | Circuit 2 | 0.00 |
| ● | ⚠ | ⚙ ⚙ | Circuit 3 | 0.00 |

Configuration: Vertiv PowerGO rPDU, Phase A

Name
Phase A

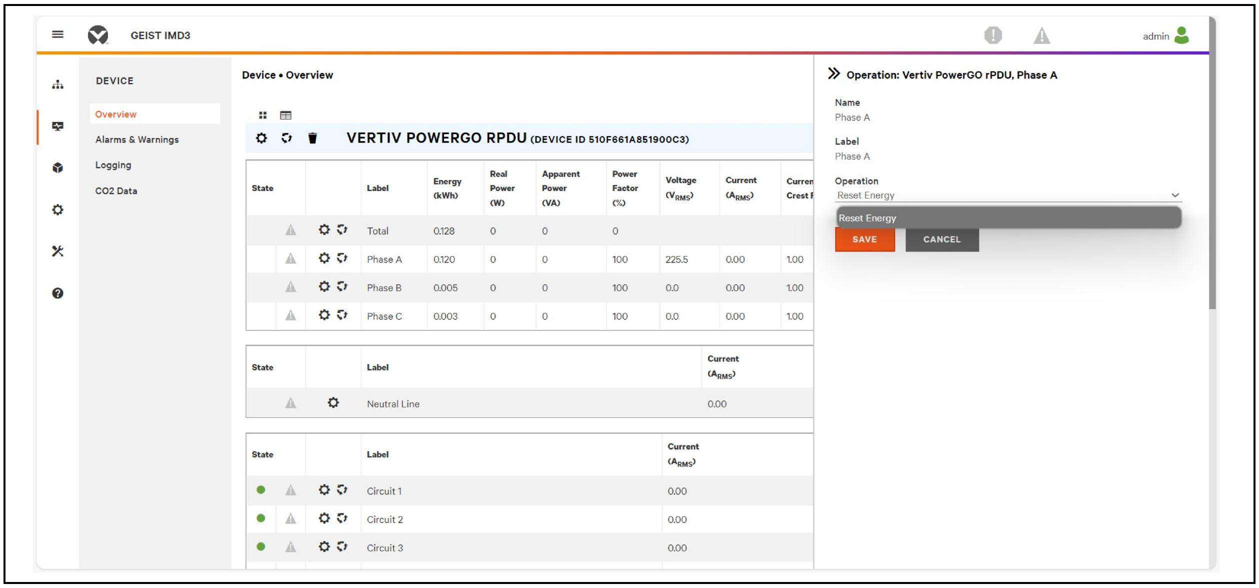
Label
Phase A

SAVE CANCEL

### To change phase operation:

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

### Figure 5.13 Changing Phase Operation



VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Curren Crest F |
|---|---|---|---|---|---|---|---|---|---|
| ⚠ | ⚙ ⚙ | Total | 0.128 | 0 | 0 | 0 | | | |
| ⚠ | ⚙ ⚙ | Phase A | 0.120 | 0 | 0 | 100 | 225.5 | 0.00 | 1.00 |
| ⚠ | ⚙ ⚙ | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |
| ⚠ | ⚙ ⚙ | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ⚠ | ⚙ | Neutral Line | 0.00 |

| State | | | Label | Current ($A_{RMS}$) |
|---|---|---|---|---|
| ● | ⚠ | ⚙ ⚙ | Circuit 1 | 0.00 |
| ● | ⚠ | ⚙ ⚙ | Circuit 2 | 0.00 |
| ● | ⚠ | ⚙ ⚙ | Circuit 3 | 0.00 |

Operation: Vertiv PowerGO rPDU, Phase A

Name
Phase A

Label
Phase A

Operation
Reset Energy

Reset Energy

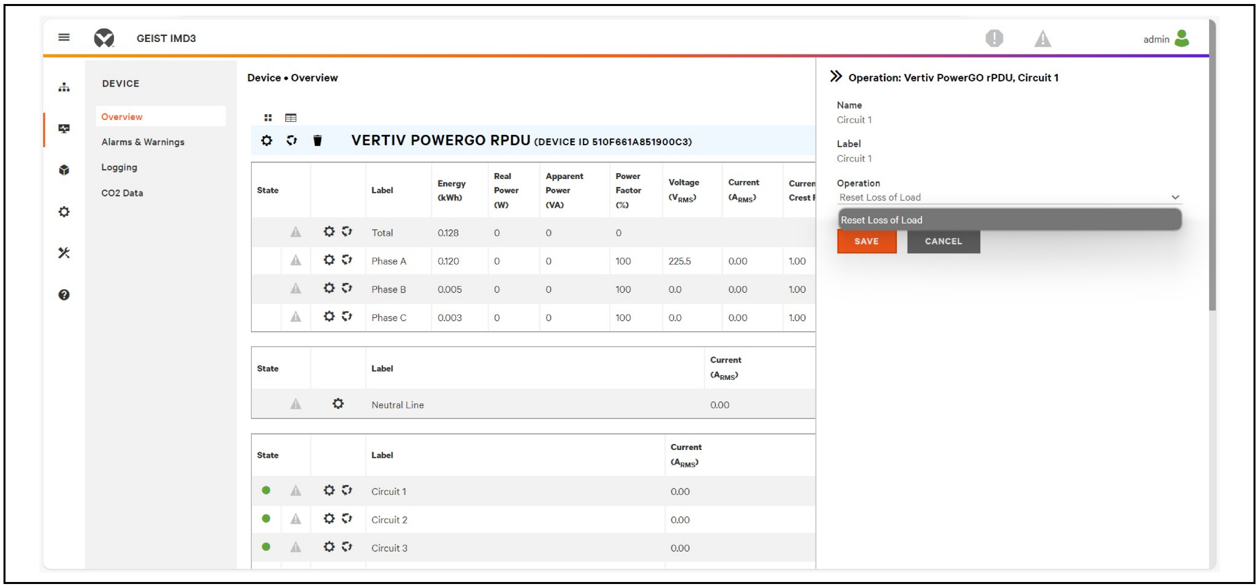
SAVE CANCEL

### To change circuit operation:

1. Click the Operation ⚙ icon.
2. Select *Reset Loss of Load* to reset the Loss of Load alarm.

3. Click *SAVE* to issue the action.

**Figure 5.14 Changing Circuit Operation**



VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| State | | Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Curren Crest F |
|---|---|---|---|---|---|---|---|---|---|
| | | Total | 0.128 | 0 | 0 | 0 | | | |
| | | Phase A | 0.120 | 0 | 0 | 100 | 225.5 | 0.00 | 1.00 |
| | | Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |
| | | Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| | | Neutral Line | 0.00 |

| State | | Label | Current ($A_{RMS}$) |
|---|---|---|---|
| ● | | Circuit 1 | 0.00 |
| ● | | Circuit 2 | 0.00 |
| ● | | Circuit 3 | 0.00 |

Operation: Vertiv PowerGO rPDU, Circuit 1

Name
Circuit 1

Label
Circuit 1

Operation
Reset Loss of Load

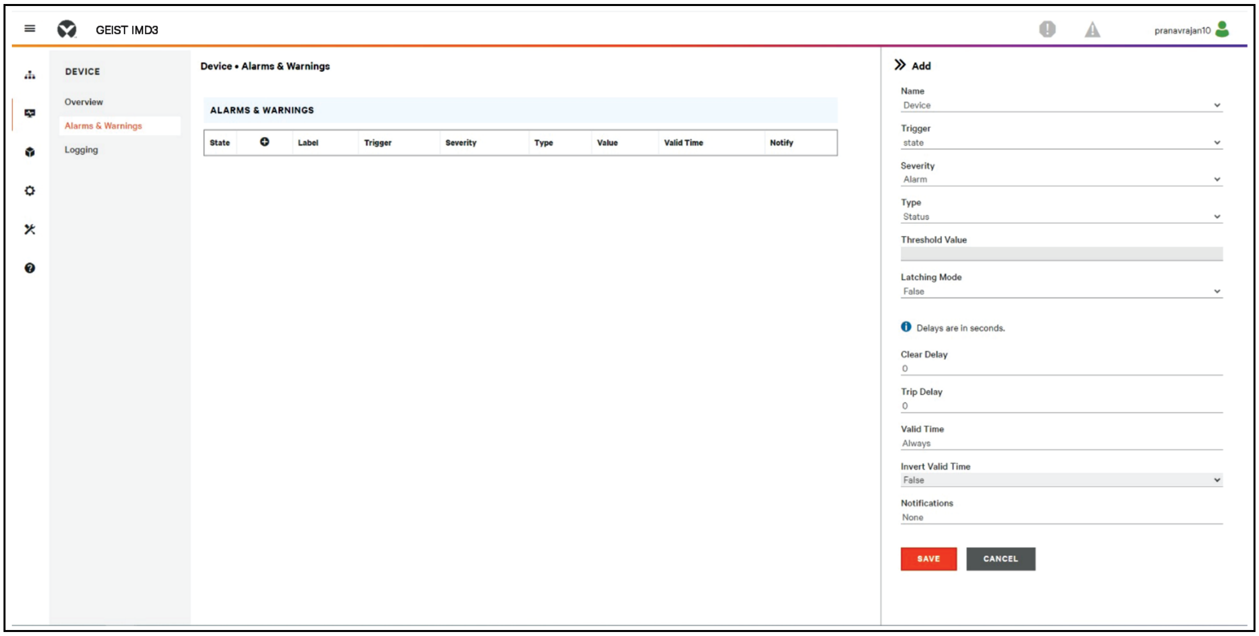
Reset Loss of Load

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

## 5.4.2 Alarms & Warnings

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

### Figure 5.15 Alarms & Warnings Page



Name: Device

Trigger: state

Severity: Alarm

Type: Status

Threshold Value:

Latching Mode: False

Delays are in seconds.

Clear Delay: 0

Trip Delay: 0

Valid Time: Always

Invert Valid Time: False

Notifications: None

### Table 5.7 Alarms & Warnings Descriptions

| Number | Description | Symbol | Description |
|---|---|---|---|
| 1 | Status of each event. | ! | Warning symbol. Event is displayed in orange. |
| | | ▲ | Alarm symbol. Alarm is displayed in red. |
| | | ✓ | Acknowledged event symbol. Symbol remains until the condition measured returns to normal. |
| 2 | Add/Delete/Modify alarms and warnings. | ⊕ | Add new alarms and warnings. |
| | | ✎ | Modify existing alarms and warnings. |
| | | 🗑 | Delete existing alarms and warnings. |
| 3 | Notify user of tripped Events and request acknowledgment. | N/A | Empty, if there is no alert condition. |
| | | ✓ | When a warning or alarm event occurs, you can click on this symbol to acknowledge the event and stop the unit from sending any more notifications about it.<br>**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 Email on page 60.
      - Or, when an outlet number is selected as the target, the outlet state switches when an event is tripped and remains in the switched state until the event resets or is acknowledged. For this option, the outlet mode must be configured for Alarm Control, see Alarms & Warnings on page 30.

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

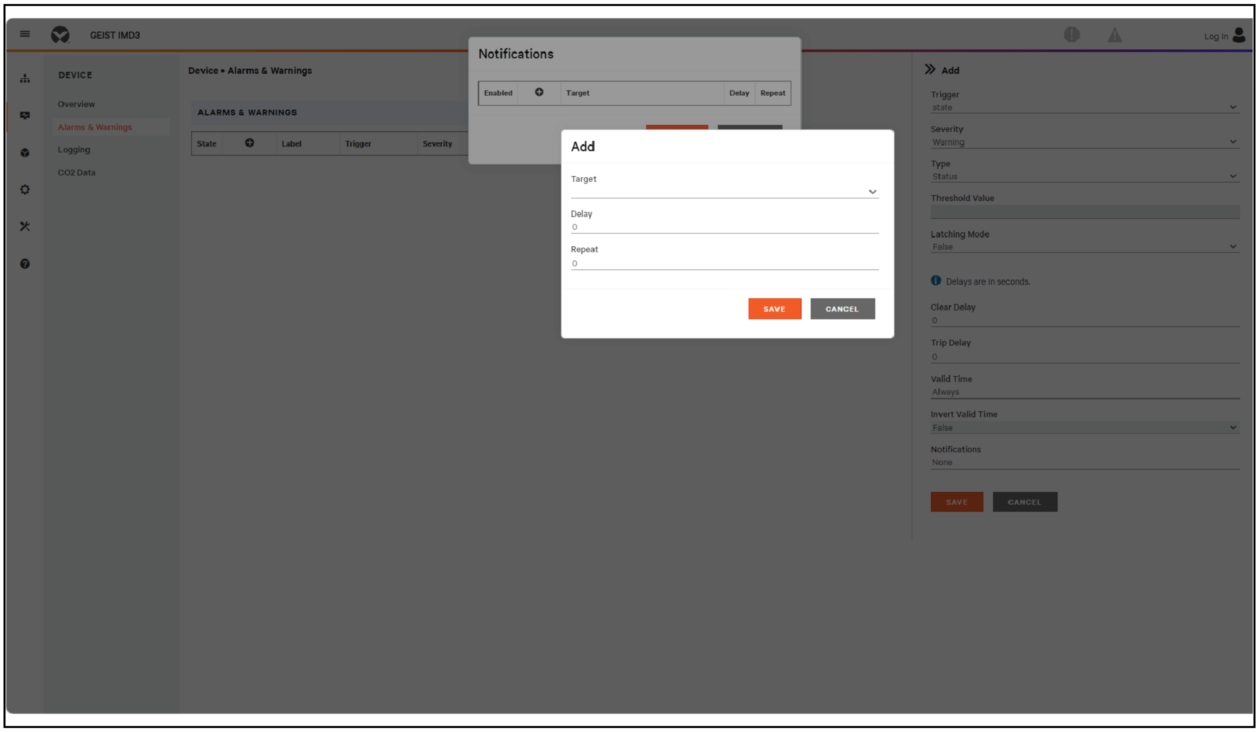
**NOTE: Applies to Outlet Switched Vertiv™ PowerGo rPDUs only.**

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

3. Click *SAVE* to save this notification action.

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

### Figure 5.16 Adding Alarms & Warnings Window



Add

Target

Delay
0

Repeat
0

Add

Trigger
state

Severity
Warning

Type
Status

Threshold Value

Latching Mode
False

Delays are in seconds.

Clear Delay
0

Trip Delay
0

Valid Time
Always

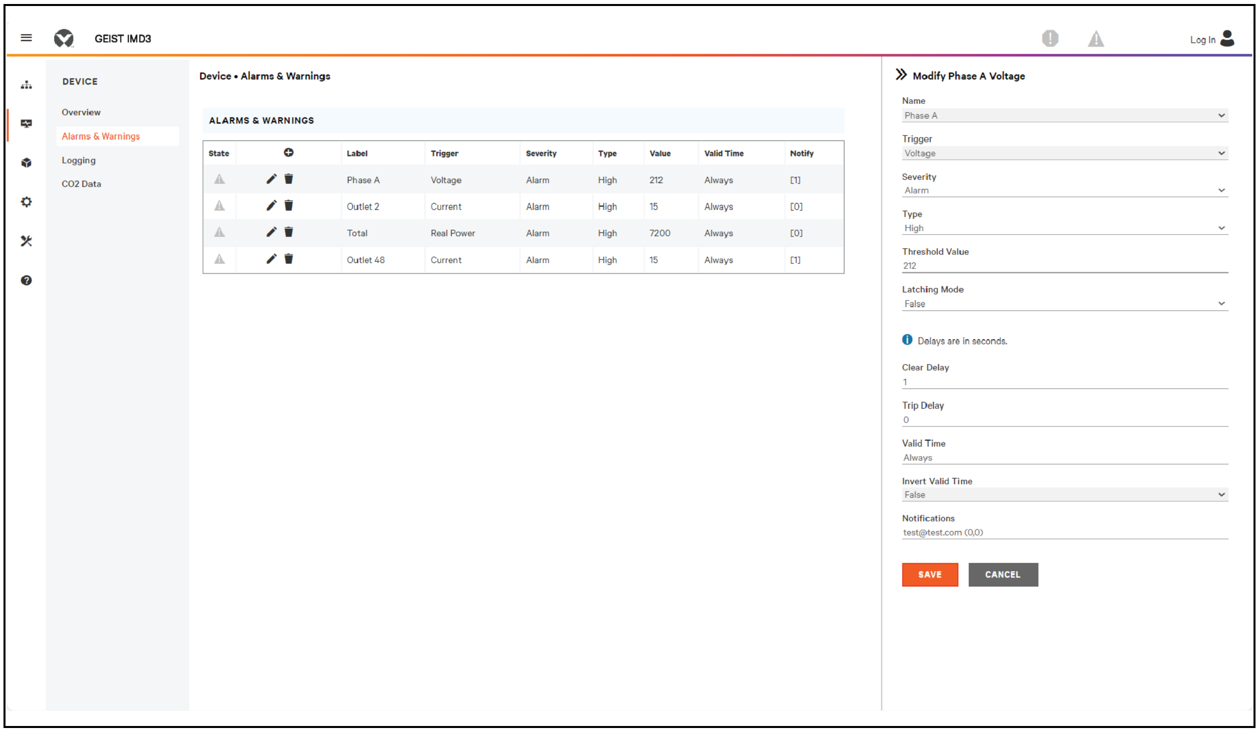
Invert Valid Time
False

Notifications
None

### To change an existing alarm or warning event:

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

### Figure 5.17 Changing Alarms & Warning Window



| State | ⊕ | Label | Trigger | Severity | Type | Value | Valid Time | Notify |
|---|---|---|---|---|---|---|---|---|
| ⚠ | ✎ 🗑 | Phase A | Voltage | Alarm | High | 212 | Always | [1] |
| ⚠ | ✎ 🗑 | Outlet 2 | Current | Alarm | High | 15 | Always | [0] |
| ⚠ | ✎ 🗑 | Total | Real Power | Alarm | High | 7200 | Always | [0] |
| ⚠ | ✎ 🗑 | Outlet 48 | Current | Alarm | High | 15 | Always | [1] |

Modify Phase A Voltage

Name: Phase A

Trigger: Voltage

Severity: Alarm

Type: High

Threshold Value: 212

Latching Mode: False

Delays are in seconds.

Clear Delay: 1

Trip Delay: 0

Valid Time: Always

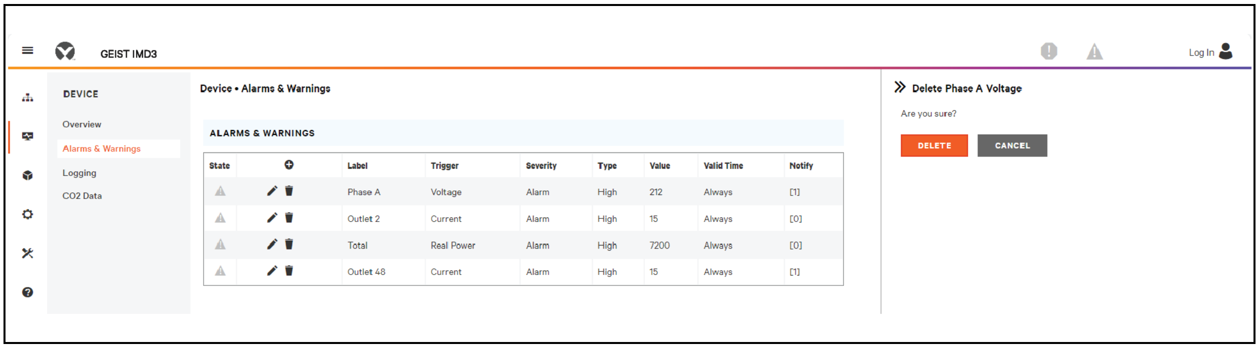
Invert Valid Time: False

Notifications: test@test.com (0,0)

### To delete an existing alarm or warning event:

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

### Figure 5.18 Deleting Alarms & Warning Event



| State | ⊕ | Label | Trigger | Severity | Type | Value | Valid Time | Notify |
|---|---|---|---|---|---|---|---|---|
| ⚠ | ✎ 🗑 | Phase A | Voltage | Alarm | High | 212 | Always | [1] |
| ⚠ | ✎ 🗑 | Outlet 2 | Current | Alarm | High | 15 | Always | [0] |
| ⚠ | ✎ 🗑 | Total | Real Power | Alarm | High | 7200 | Always | [0] |
| ⚠ | ✎ 🗑 | Outlet 48 | Current | Alarm | High | 15 | Always | [1] |

Delete Phase A Voltage

Are you sure?

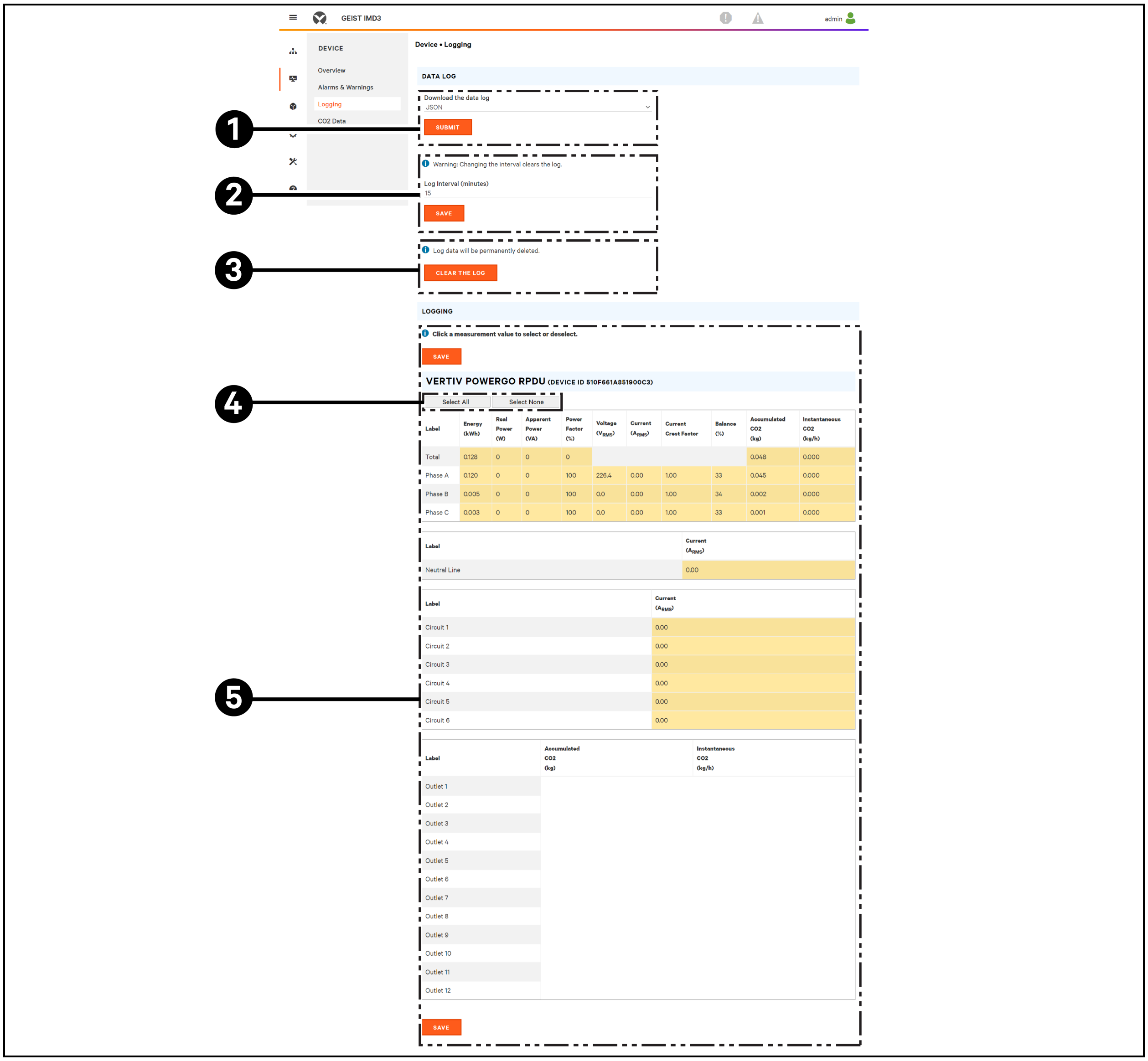
### 5.4.3 Logging

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

**To select or deselect the measurement value:**

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

**Figure 5.19 Logging Page**



Download the data log: JSON

Warning: Changing the interval clears the log.

Log Interval (minutes): 15

Log data will be permanently deleted.

Click a measurement value to select or deselect.

VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| Label | Energy (kWh) | Real Power (W) | Apparent Power (VA) | Power Factor (%) | Voltage ($V_{RMS}$) | Current ($A_{RMS}$) | Current Crest Factor | Balance (%) | Accumulated CO2 (kg) | Instantaneous CO2 (kg/h) |
|---|---|---|---|---|---|---|---|---|---|---|
| Total | 0.128 | 0 | 0 | 0 | | | | | 0.048 | 0.000 |
| Phase A | 0.120 | 0 | 0 | 100 | 226.4 | 0.00 | 1.00 | 33 | 0.045 | 0.000 |
| Phase B | 0.005 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 | 34 | 0.002 | 0.000 |
| Phase C | 0.003 | 0 | 0 | 100 | 0.0 | 0.00 | 1.00 | 33 | 0.001 | 0.000 |

| Label | Current ($A_{RMS}$) |
|---|---|
| Neutral Line | 0.00 |

| Label | Current ($A_{RMS}$) |
|---|---|
| Circuit 1 | 0.00 |
| Circuit 2 | 0.00 |
| Circuit 3 | 0.00 |
| Circuit 4 | 0.00 |
| Circuit 5 | 0.00 |
| Circuit 6 | 0.00 |

| Label | Accumulated CO2 (kg) | Instantaneous CO2 (kg/h) |
|---|---|---|
| Outlet 1 | | |
| Outlet 2 | | |
| Outlet 3 | | |
| Outlet 4 | | |
| Outlet 5 | | |
| Outlet 6 | | |
| Outlet 7 | | |
| Outlet 8 | | |
| Outlet 9 | | |
| Outlet 10 | | |
| Outlet 11 | | |
| Outlet 12 | | |

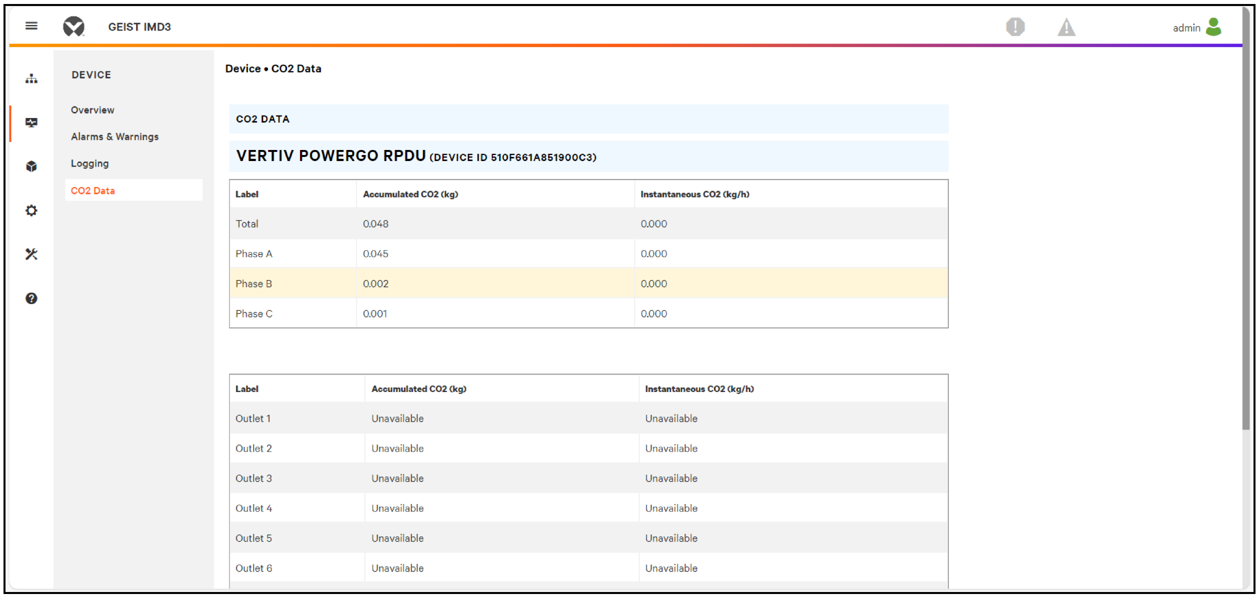
### Table 5.8 Logging Page Descriptions

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

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

## 5.4.4 CO2 Data

### Figure 5.20 CO2 Home Page



Device • CO2 Data

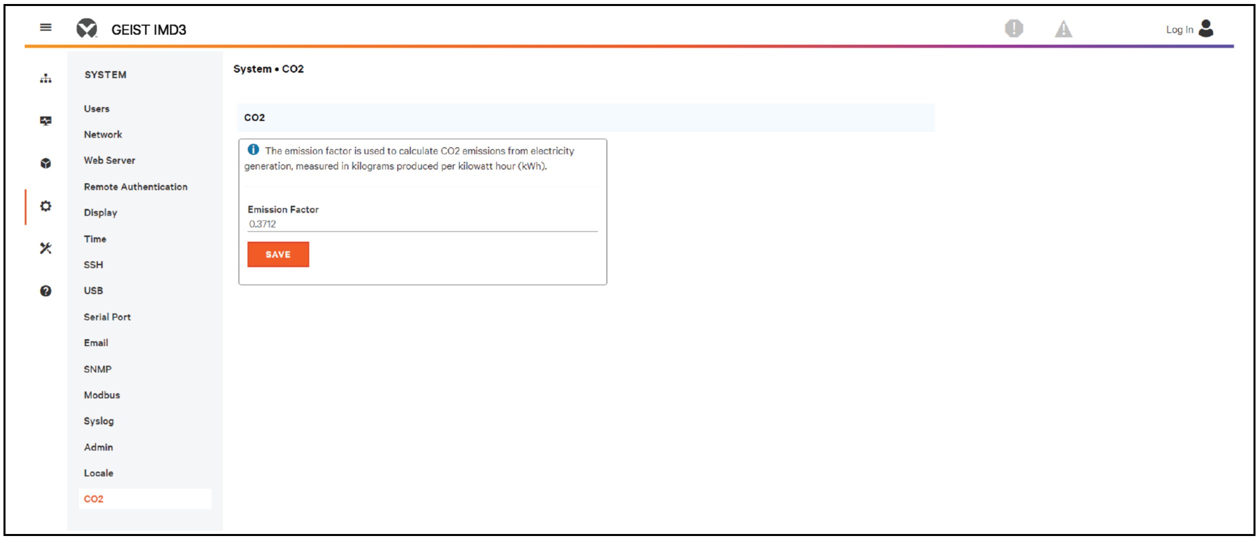
CO2 DATA

VERTIV POWERGO RPDU (DEVICE ID 510F661A851900C3)

| Label | Accumulated CO2 (kg) | Instantaneous CO2 (kg/h) |
|---|---|---|
| Total | 0.048 | 0.000 |
| Phase A | 0.045 | 0.000 |
| Phase B | 0.002 | 0.000 |
| Phase C | 0.001 | 0.000 |

| Label | Accumulated CO2 (kg) | Instantaneous CO2 (kg/h) |
|---|---|---|
| Outlet 1 | Unavailable | Unavailable |
| Outlet 2 | Unavailable | Unavailable |
| Outlet 3 | Unavailable | Unavailable |
| Outlet 4 | Unavailable | Unavailable |
| Outlet 5 | Unavailable | Unavailable |
| Outlet 6 | Unavailable | Unavailable |

Figure 5.21 System Tab of CO2



The emission factor is used to calculate CO2 emissions from electricity generation, measured in kilograms produced per kilowatt hour (kWh).

Emission Factor
0.3712

**NOTE: There are three pages associated with CO2 page. The first page is the CO2 data page under Device (Figure 5.20 on the previous page), which shows accumulated and instantaneous calculations for the phases and outlets. The second page is CO2 page under System where you set the Emission Factor to calculate CO2 per kWH. The default CO2 Emission Factor will be set to 0.3172. The third page is on the help-info page; The Lifetime CO2 is based on the Lifetime Energy. If a user does a reset on the energy usage on a PDU or a specific outlet, the value will return to 0. However, the Lifetime Energy of that component will not get reset to 0.**

## 5.5 Provisioner Sub Menu

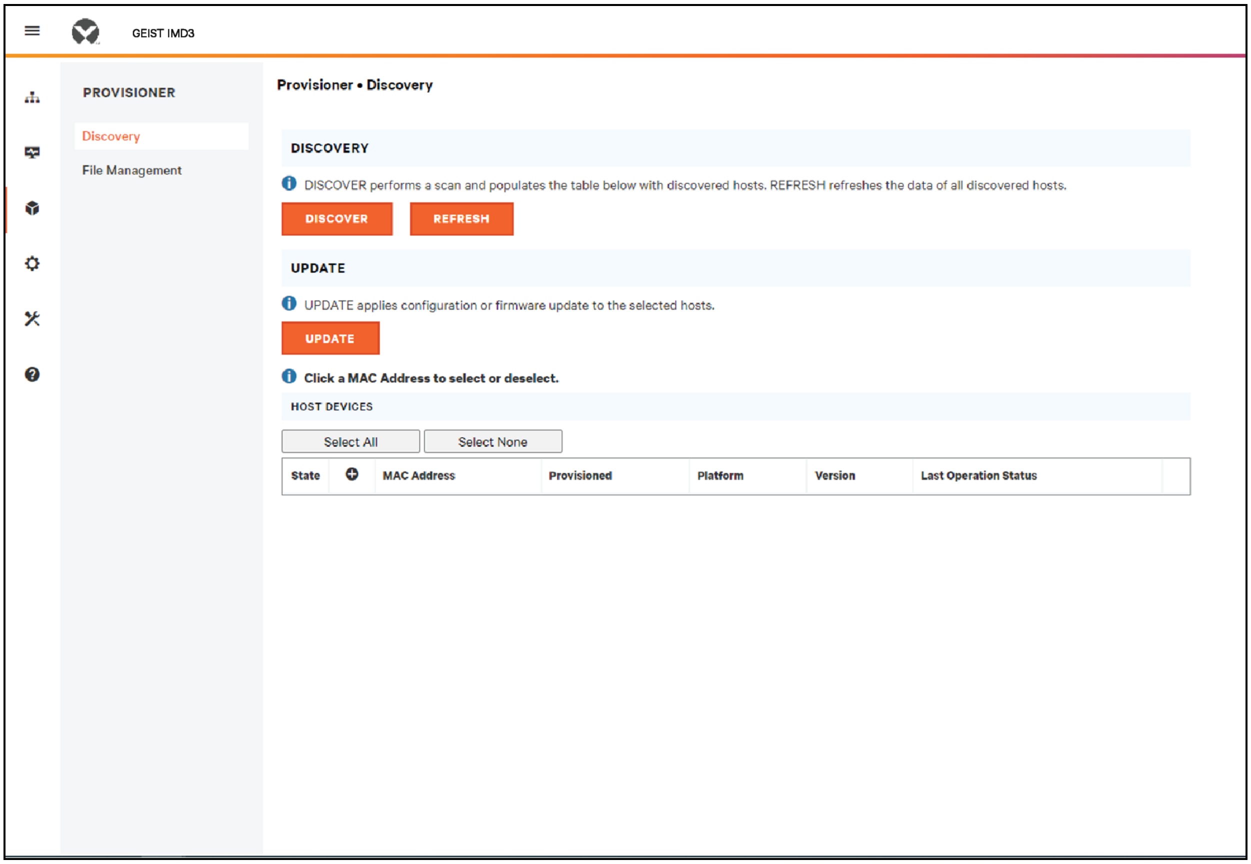
The Provisioner sub menu allows the user to discover locally connected Vertiv™ PowerGo rPDUs. The user can update their firmware and configure them by uploading a configuration settings file.

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

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

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

**Figure 5.22 Provisioner Sub Menu Page**



DISCOVER performs a scan and populates the table below with discovered hosts. REFRESH refreshes the data of all discovered hosts.

UPDATE applies configuration or firmware update to the selected hosts.

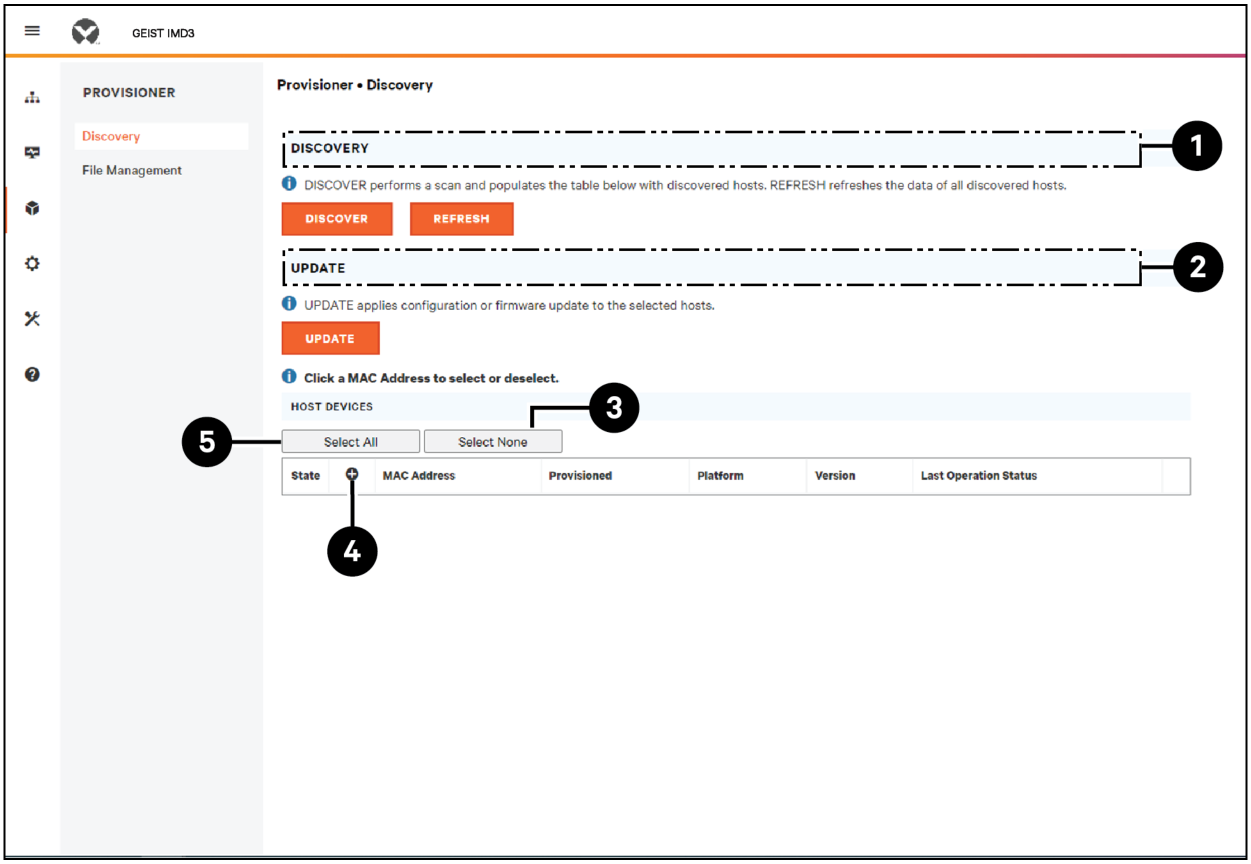
**Click a MAC Address to select or deselect.**

| State | ⊕ | MAC Address | Provisioned | Platform | Version | Last Operation Status |
|---|---|---|---|---|---|---|

## 5.5.1 Discovery

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

**Figure 5.23 Discovery**


GEIST IMD3
PROVISIONER
Discovery
File Management
Provisioner • Discovery
DISCOVERY
DISCOVER performs a scan and populates the table below with discovered hosts. REFRESH refreshes the data of all discovered hosts.
DISCOVER
REFRESH
UPDATE
UPDATE applies configuration or firmware update to the selected hosts.
UPDATE
Click a MAC Address to select or deselect.
HOST DEVICES
Select All
Select None
State
MAC Address
Provisioned
Platform
Version
Last Operation Status
1
2
3
4
5

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

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

## 5.5.2 File management

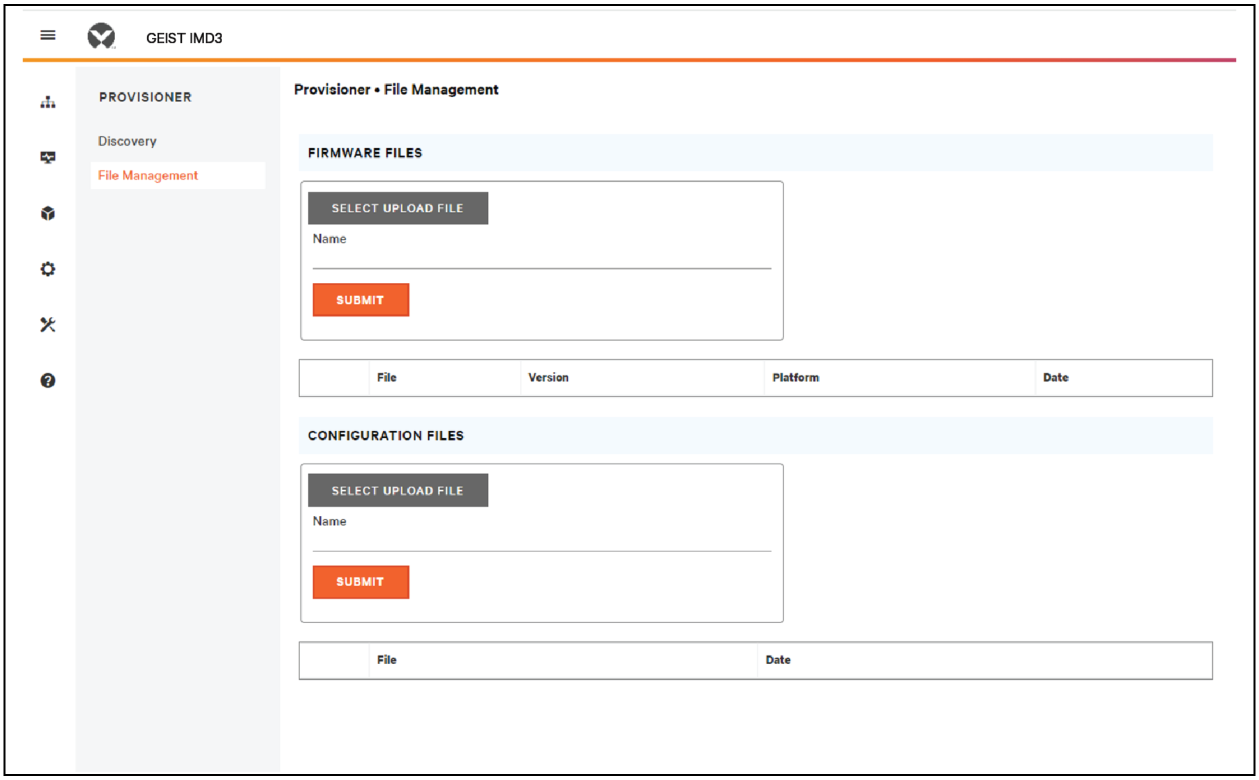
Firmware Files:

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

Configuration Files:

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

Figure 5.24 File Management Page



| | File | Version | Platform | Date |
|---|---|---|---|---|

| | File | Date |
|---|---|---|

See Provisioner - Format of the configuration settings file on page 93 for examples of configuration setting files used by the Provisioner and the necessary format for the file.

## 5.6 System Sub Menu

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

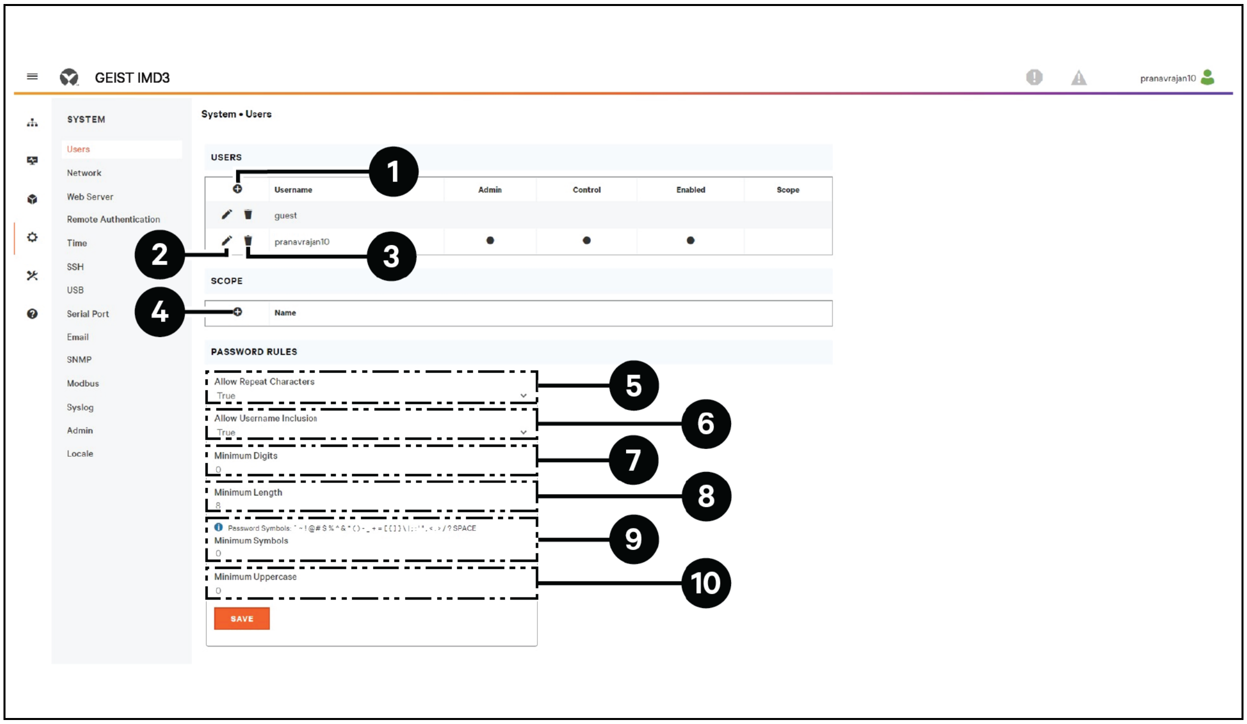
### 5.6.1 Users

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

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

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

### Figure 5.25 User Page



| | Username | Admin | Control | Enabled | Scope |
|---|---|---|---|---|---|
| | guest | | | | |
| | pranavrajan10 | ● | ● | ● | |

Scope: Name

Allow Repeat Characters: True

Allow Username Inclusion: True

Minimum Digits: 0

Minimum Length: 8

Password Symbols: ` ~ ! @ # $ % ^ & * ( ) - _ + = [ { ] } \ | ; : ' " , < . > / ? SPACE

Minimum Symbols: 0

Minimum Uppercase: 0

### Table 5.9 User Page Descriptions

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

**NOTE: *Only visible when logged in as an Administrator.**

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

**To add or modify a user account:**

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

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

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

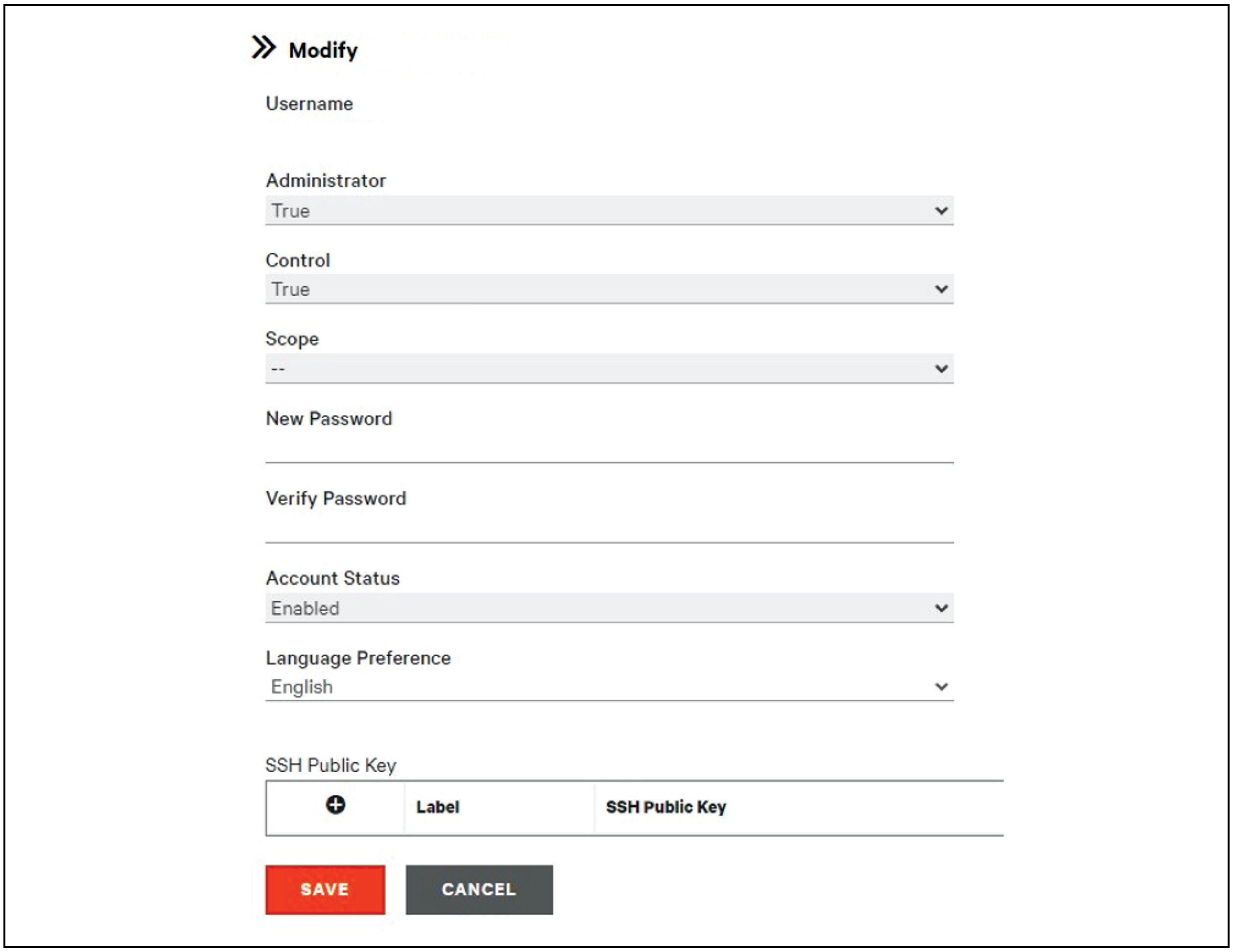
## User Account Types

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

**To change a user password:**

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

Figure 5.26 Change User Password Page



Modify

Username

Administrator: True

Control: True

Scope: --

New Password

Verify Password

Account Status: Enabled

Language Preference: English

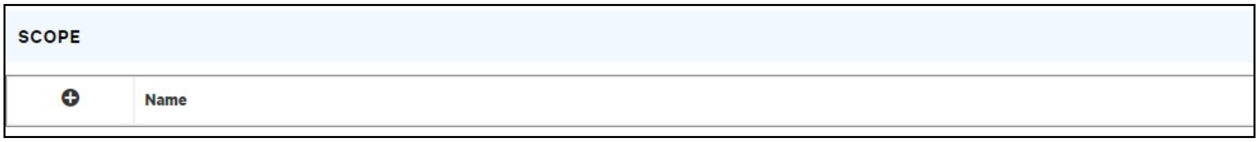
SSH Public Key

| ⊕ | Label | SSH Public Key |
|---|---|---|

**To add or modify a user scope:**

1. Click the Add or Modify Scope icon. Refer **Figure 5.27** below.
2. Create or modify the scope information as needed.
    a. **Label:** Enter the desired name of the selected scope.
    b. **Remote Authentication Attribute:** Used for all remote authentication types.
    c. Click applicable Outlets for a specified User. (Highlight in Green)
3. Click *OK* to save changes.

Figure 5.27 Add Scope



SCOPE

| ⊕ | Name |
|---|---|

## Password rules and account policy settings

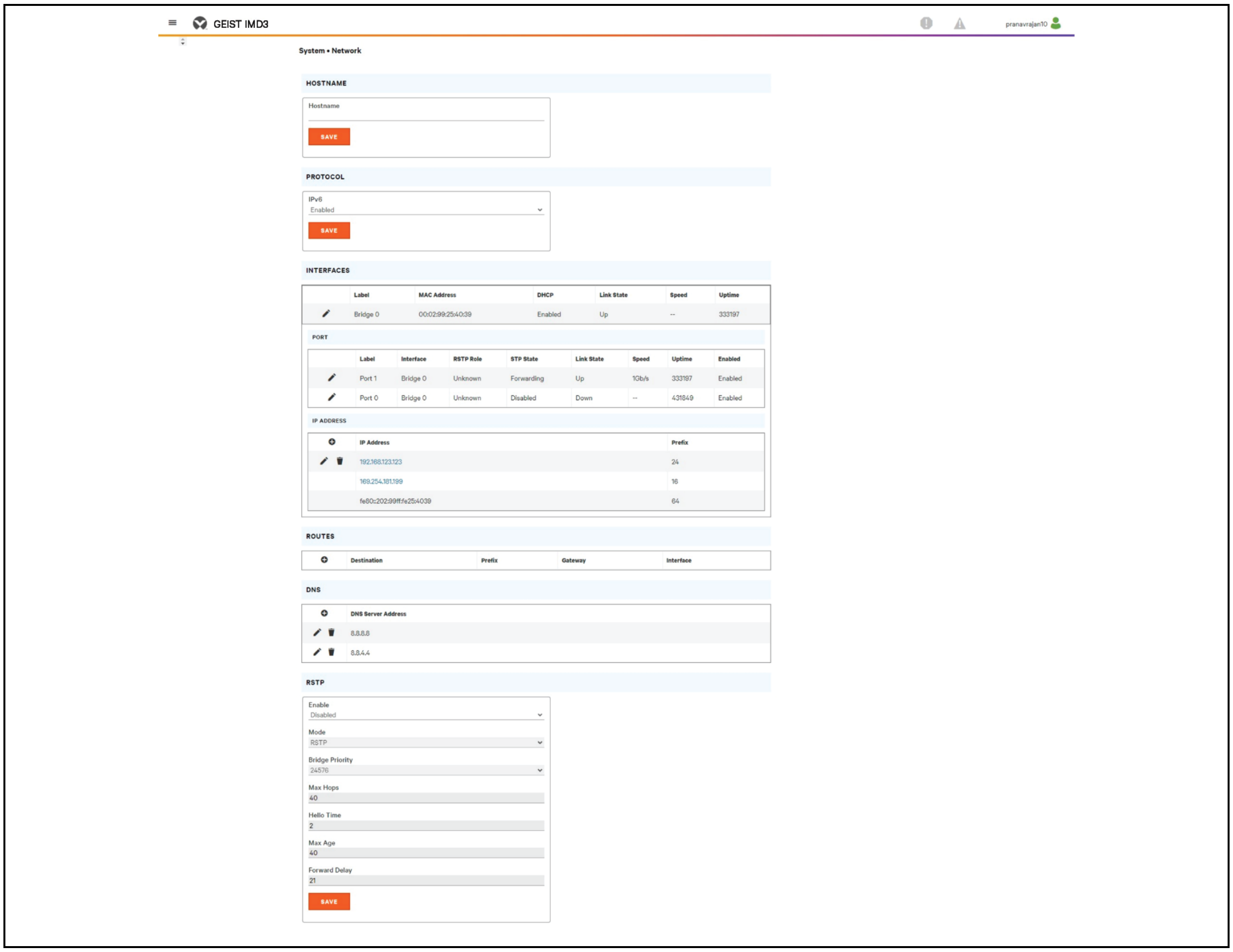
**NOTE: A user will be logged out automatically after 10 minutes of inactivity.**

### 5.6.2 Network

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

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

**Figure 5.28 Network Configuration Page**



System • Network

HOSTNAME

Hostname

PROTOCOL

IPv6: Enabled

INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed | Uptime |
|---|---|---|---|---|---|---|
| | Bridge 0 | 00:02:99:25:40:39 | Enabled | Up | -- | 333197 |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptime | Enabled |
|---|---|---|---|---|---|---|---|---|
| | Port 1 | Bridge 0 | Unknown | Forwarding | Up | 1Gb/s | 333197 | Enabled |
| | Port 0 | Bridge 0 | Unknown | Disabled | Down | -- | 431849 | Enabled |

IP ADDRESS

| | IP Address | Prefix |
|---|---|---|
| | 192.168.123.123 | 24 |
| | 169.254.181.199 | 16 |
| | fe80::202:99ff:fe25:4039 | 64 |

ROUTES

| | Destination | Prefix | Gateway | Interface |
|---|---|---|---|---|

DNS

| | DNS Server Address |
|---|---|
| | 8.8.8.8 |
| | 8.8.4.4 |

RSTP

Enable: Disabled

Mode: RSTP

Bridge Priority: 24576

Max Hops: 40

Hello Time: 2

Max Age: 40

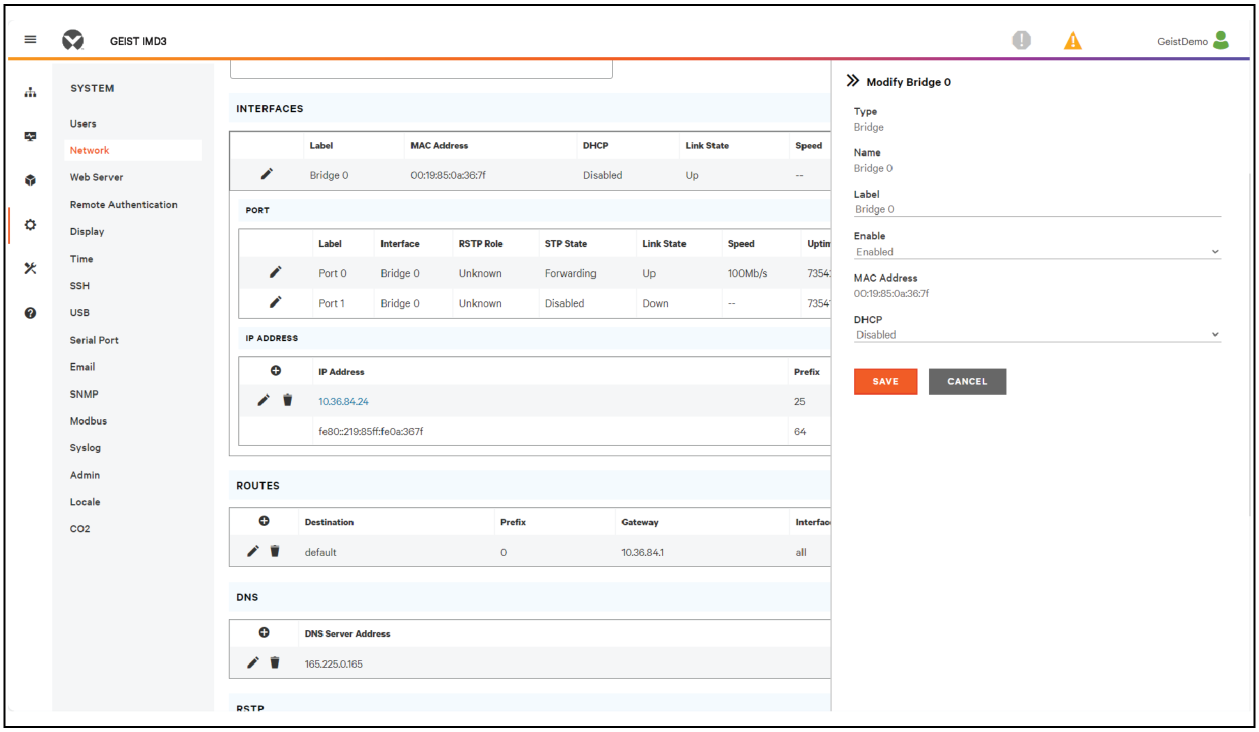
Forward Delay: 21

**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.**

**Figure 5.29 Interface Parameters**



INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|---|
| ✎ | Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|---|
| ✎ | Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 7354 |
| ✎ | Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 7354 |

IP ADDRESS

| ⊕ | IP Address | Prefix |
|---|---|---|
| ✎ 🗑 | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| ⊕ | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| ✎ 🗑 | default | 0 | 10.36.84.1 | all |

DNS

| ⊕ | DNS Server Address |
|---|---|
| ✎ 🗑 | 165.225.0.165 |

RSTP

Modify Bridge 0

Type
Bridge

Name
Bridge 0

Label
Bridge 0

Enable
Enabled

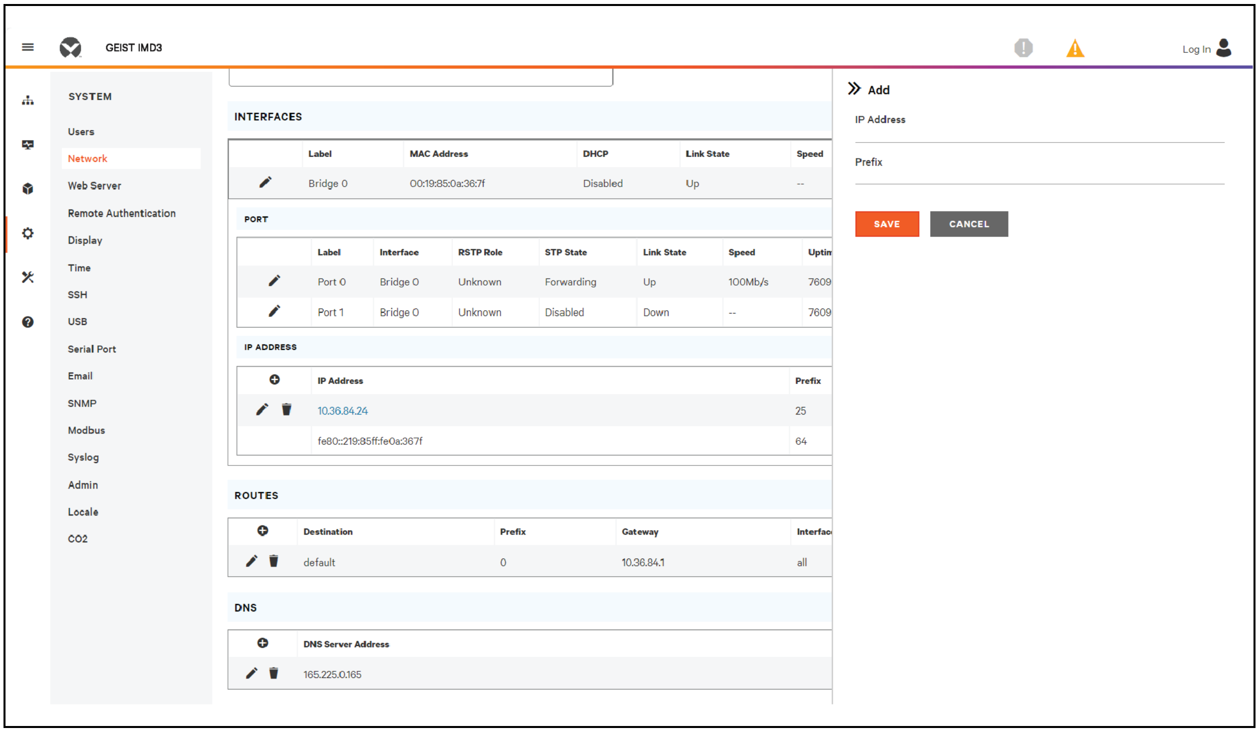
MAC Address
00:19:85:0a:36:7f

DHCP
Disabled

**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*.

**Figure 5.30 Add New IP Address**



INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|---|
| | Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|---|
| | Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 7609 |
| | Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 7609 |

IP ADDRESS

| | IP Address | Prefix |
|---|---|---|
| | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| | default | 0 | 10.36.84.1 | all |

DNS

| | DNS Server Address |
|---|---|
| | 165.225.0.165 |

IP Address

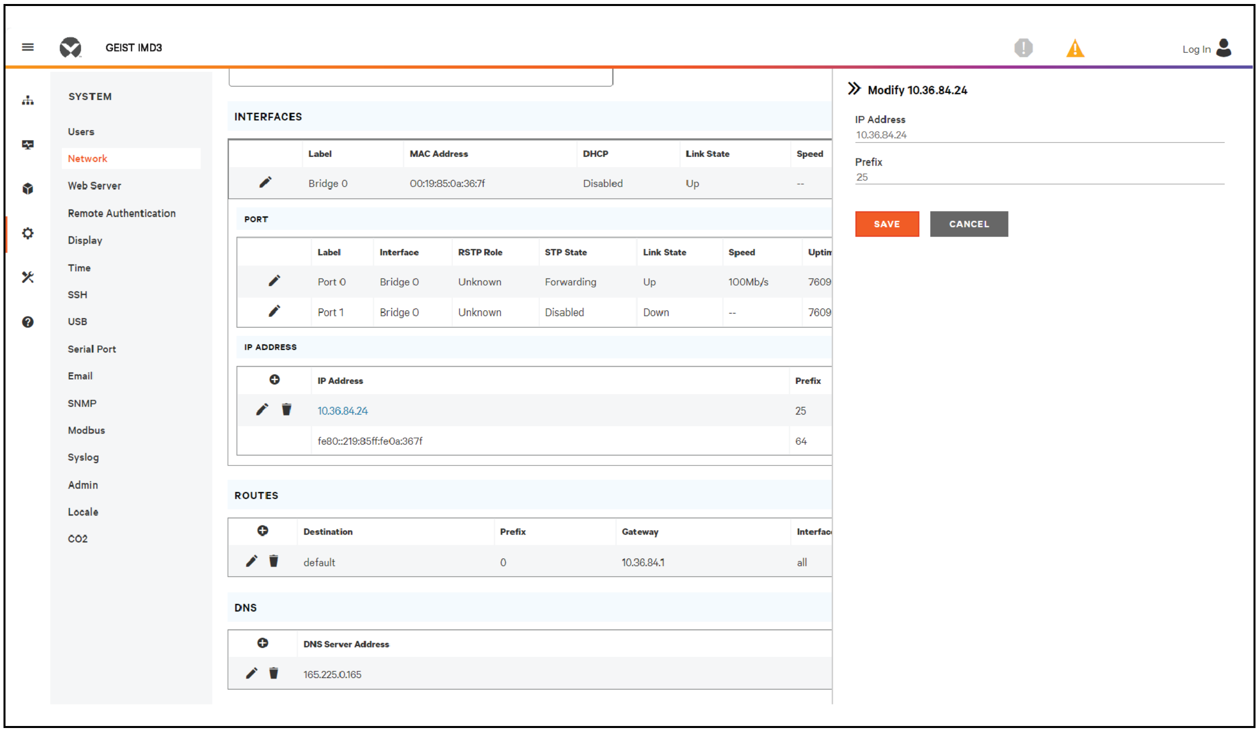
Prefix

### 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*.

**NOTE: After changing the IP, you need to disconnect the primary-secondary network cable and then reconnect it.**

### Figure 5.31 Modifying IP Address



INTERFACES

| Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|
| Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|
| Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 7609 |
| Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 7609 |

IP ADDRESS

| IP Address | Prefix |
|---|---|
| 10.36.84.24 | 25 |
| fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| Destination | Prefix | Gateway | Interfac |
|---|---|---|---|
| default | 0 | 10.36.84.1 | all |

DNS

| DNS Server Address |
|---|
| 165.225.0.165 |

Modify 10.36.84.24

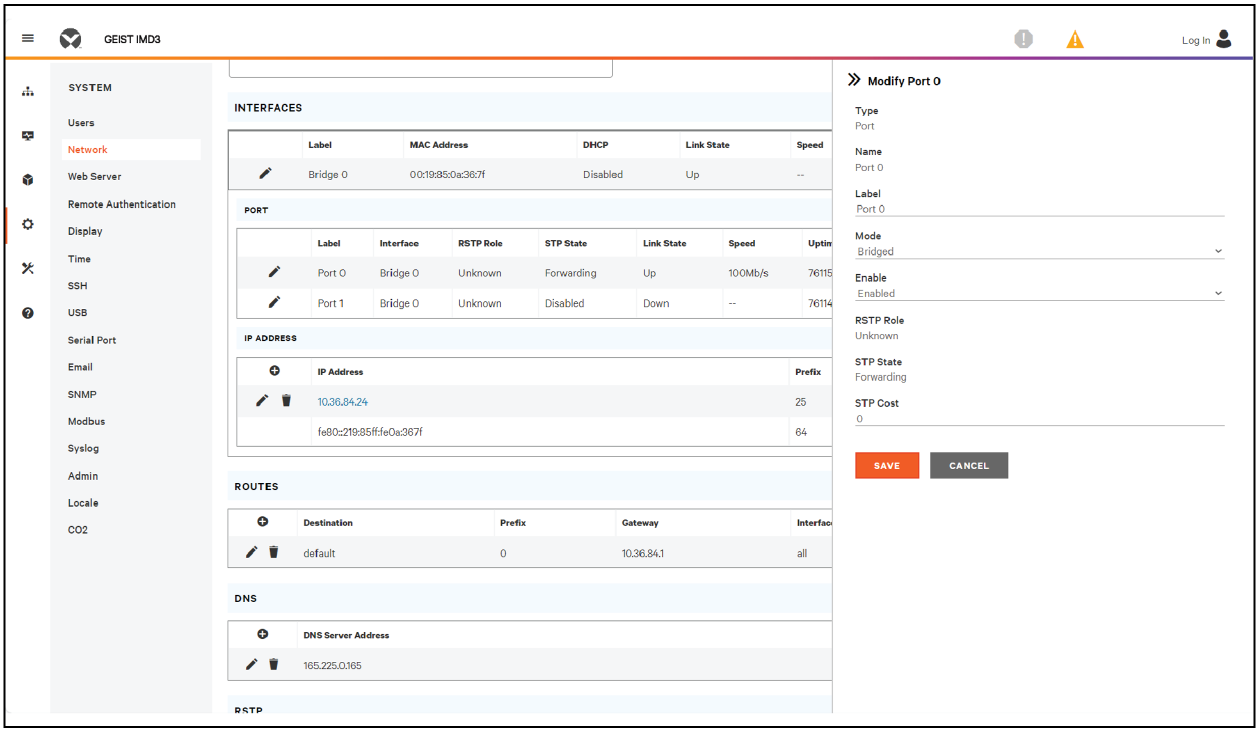
IP Address
10.36.84.24

Prefix
25

**To modify port settings:**

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

### Figure 5.32 Modifying Port Setting



INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|---|
| | Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|---|
| | Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 76115 |
| | Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 76114 |

IP ADDRESS

| | IP Address | Prefix |
|---|---|---|
| | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| | default | 0 | 10.36.84.1 | all |

DNS

| | DNS Server Address |
|---|---|
| | 165.225.0.165 |

RSTP

Modify Port 0

Type
Port

Name
Port 0

Label
Port 0

Mode
Bridged

Enable
Enabled

RSTP Role
Unknown

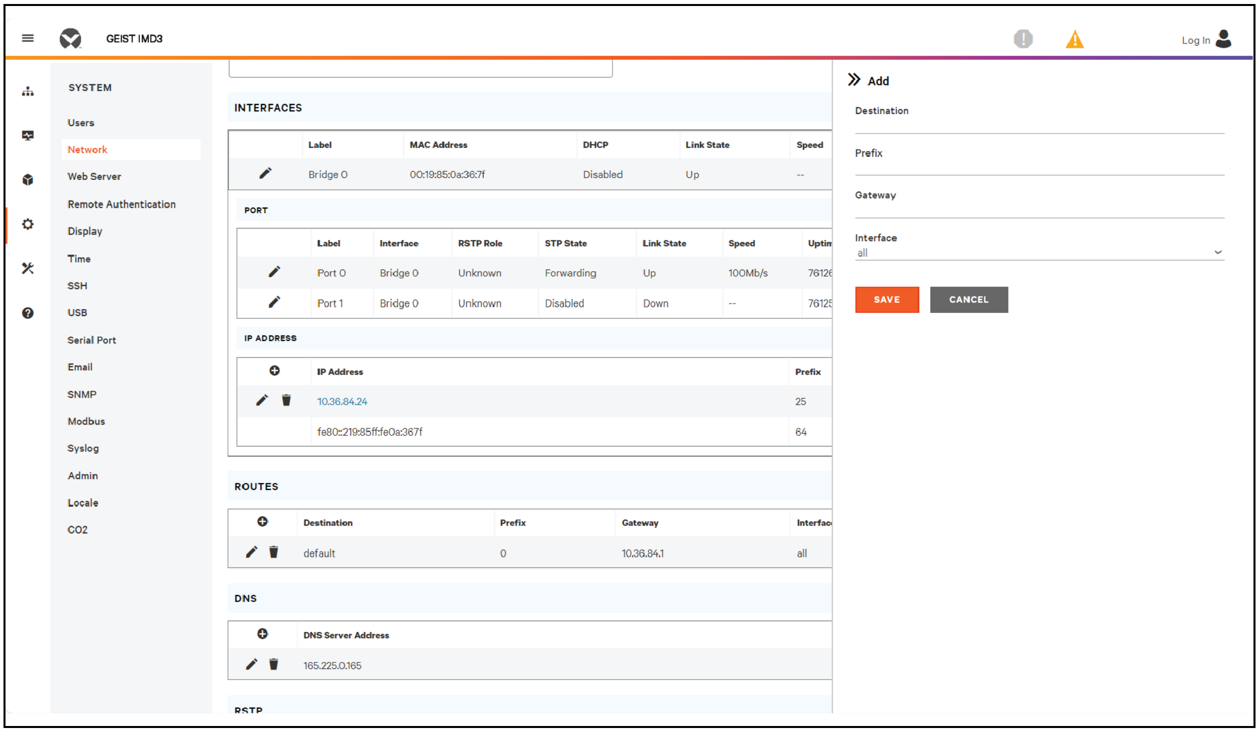
STP State
Forwarding

STP Cost
0

### 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*.

### Figure 5.33 Adding Route



INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|---|
| | Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|---|
| | Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 76126 |
| | Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 76125 |

IP ADDRESS

| | IP Address | Prefix |
|---|---|---|
| | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| | default | 0 | 10.36.84.1 | all |

DNS

| | DNS Server Address |
|---|---|
| | 165.225.0.165 |

RSTP

Add

Destination

Prefix

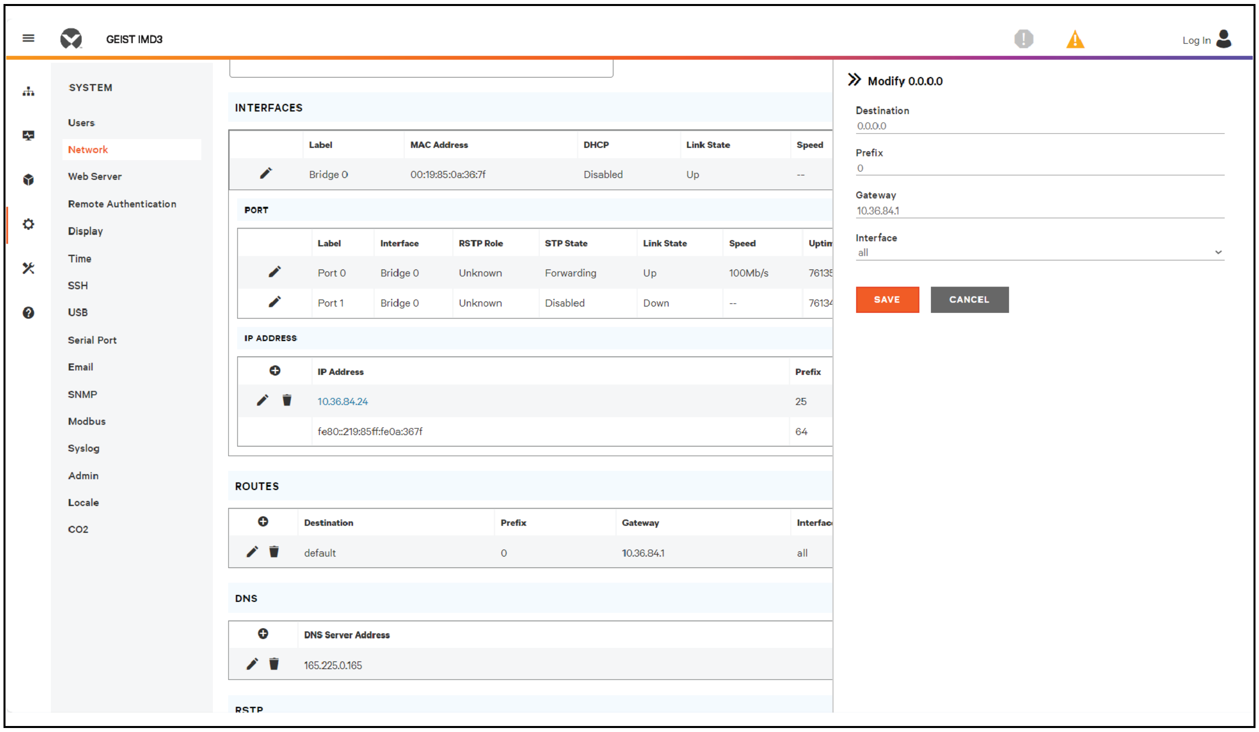
Gateway

Interface
all

**To modify an existing route:**

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

**Figure 5.34 Modifying Route**



INTERFACES

| | Label | MAC Address | DHCP | Link State | Speed |
|---|---|---|---|---|---|
| ✎ | Bridge 0 | 00:19:85:0a:36:7f | Disabled | Up | -- |

PORT

| | Label | Interface | RSTP Role | STP State | Link State | Speed | Uptim |
|---|---|---|---|---|---|---|---|
| ✎ | Port 0 | Bridge 0 | Unknown | Forwarding | Up | 100Mb/s | 76135 |
| ✎ | Port 1 | Bridge 0 | Unknown | Disabled | Down | -- | 76134 |

IP ADDRESS

| ⊕ | IP Address | Prefix |
|---|---|---|
| ✎ 🗑 | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| ⊕ | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| ✎ 🗑 | default | 0 | 10.36.84.1 | all |

DNS

| ⊕ | DNS Server Address |
|---|---|
| ✎ 🗑 | 165.225.0.165 |

RSTP

» Modify 0.0.0.0

Destination
0.0.0.0

Prefix
0

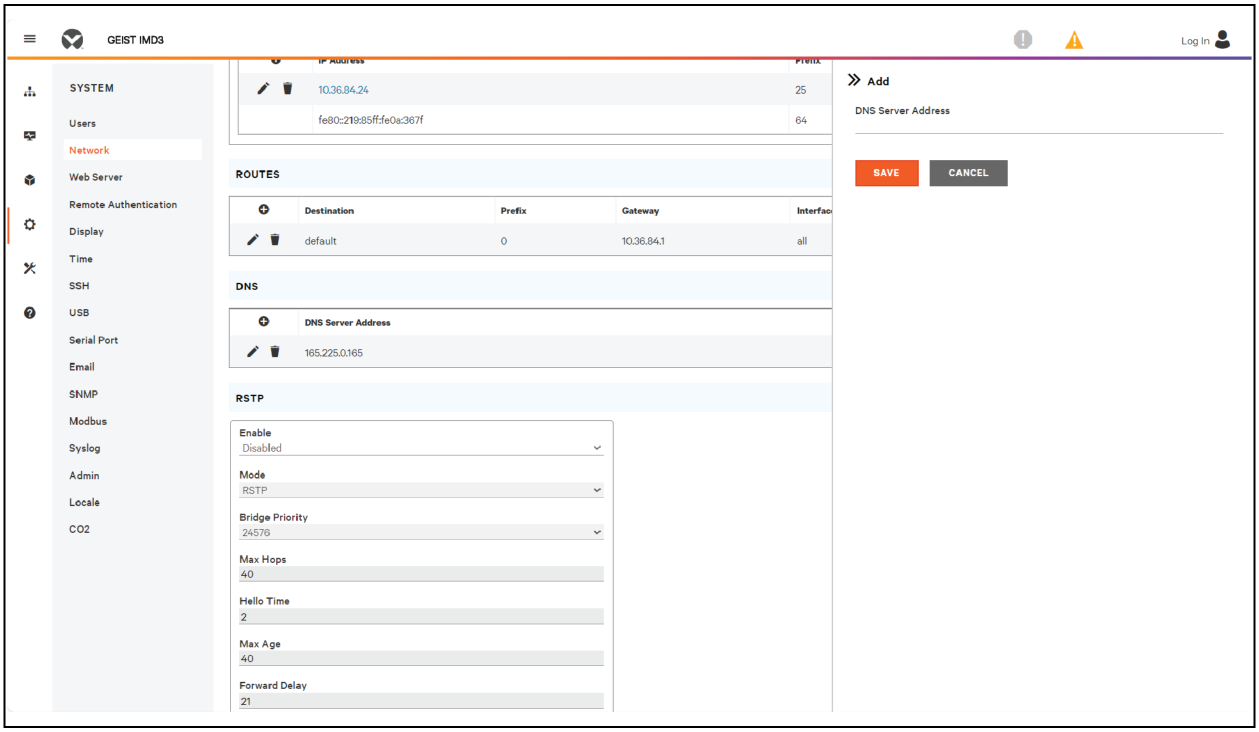
Gateway
10.36.84.1

Interface
all

**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*.

Figure 5.35 Adding DNS Server Address



| | IP Address | Prefix |
|---|---|---|
| | 10.36.84.24 | 25 |
| | fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| | Destination | Prefix | Gateway | Interfac |
|---|---|---|---|---|
| | default | 0 | 10.36.84.1 | all |

DNS

| | DNS Server Address |
|---|---|
| | 165.225.0.165 |

RSTP

Enable: Disabled

Mode: RSTP

Bridge Priority: 24576

Max Hops: 40

Hello Time: 2

Max Age: 40

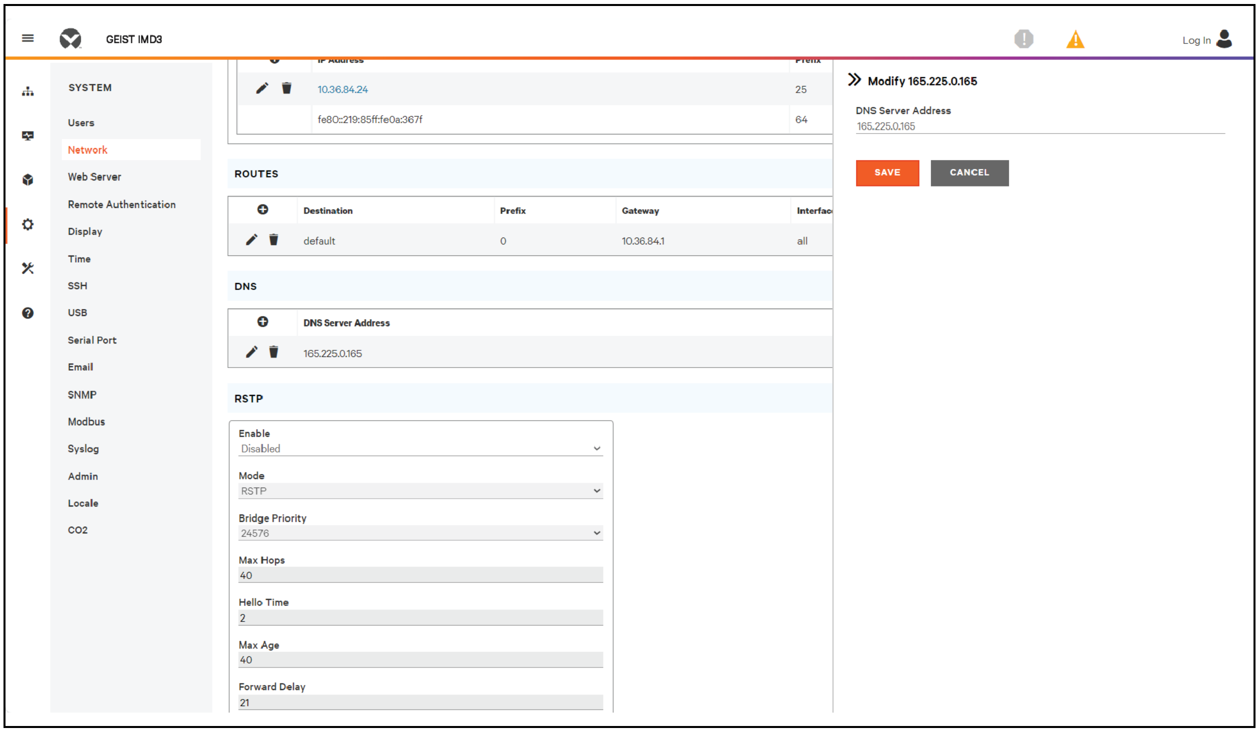
Forward Delay: 21

DNS Server Address

### To modify an existing DNS Server address:

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

### Figure 5.36 Modifying DNS Server Address



| IP Address | Prefix |
|---|---|
| 10.36.84.24 | 25 |
| fe80::219:85ff:fe0a:367f | 64 |

ROUTES

| Destination | Prefix | Gateway | Interface |
|---|---|---|---|
| default | 0 | 10.36.84.1 | all |

DNS

| DNS Server Address |
|---|
| 165.225.0.165 |

RSTP

Enable: Disabled

Mode: RSTP

Bridge Priority: 24576

Max Hops: 40

Hello Time: 2

Max Age: 40

Forward Delay: 21

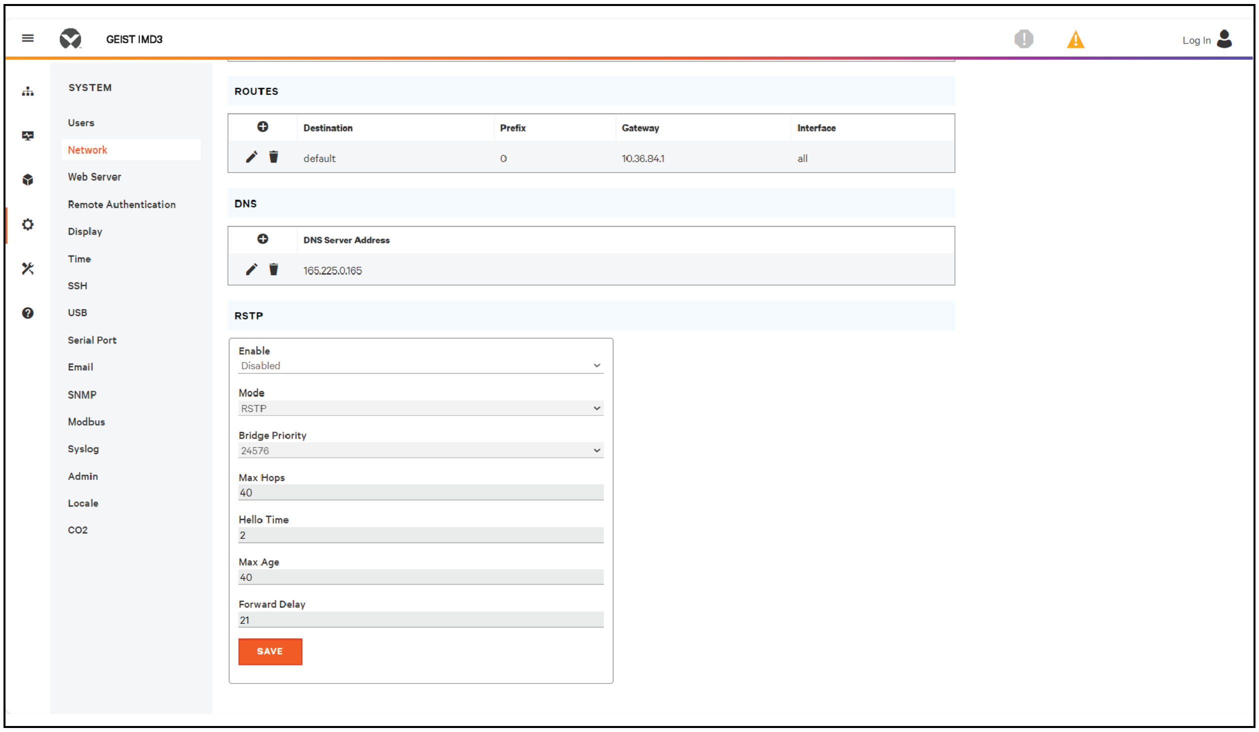
Modify 165.225.0.165

DNS Server Address: 165.225.0.165

### 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*.

Figure 5.37 Changing RSTP Setting



ROUTES

| Destination | Prefix | Gateway | Interface |
|---|---|---|---|
| default | 0 | 10.36.84.1 | all |

DNS

| DNS Server Address |
|---|
| 165.225.0.165 |

RSTP

Enable: Disabled
Mode: RSTP
Bridge Priority: 24576
Max Hops: 40
Hello Time: 2
Max Age: 40
Forward Delay: 21

## 5.6.3 Web server

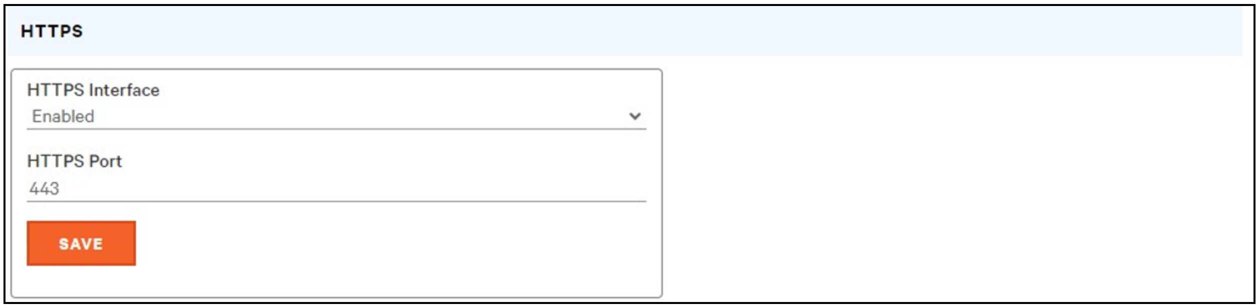
The unit's Web Server configuration can be updated on the Web Server tab of the System menu.

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

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

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

Figure 5.38 HTTP Configuration Page

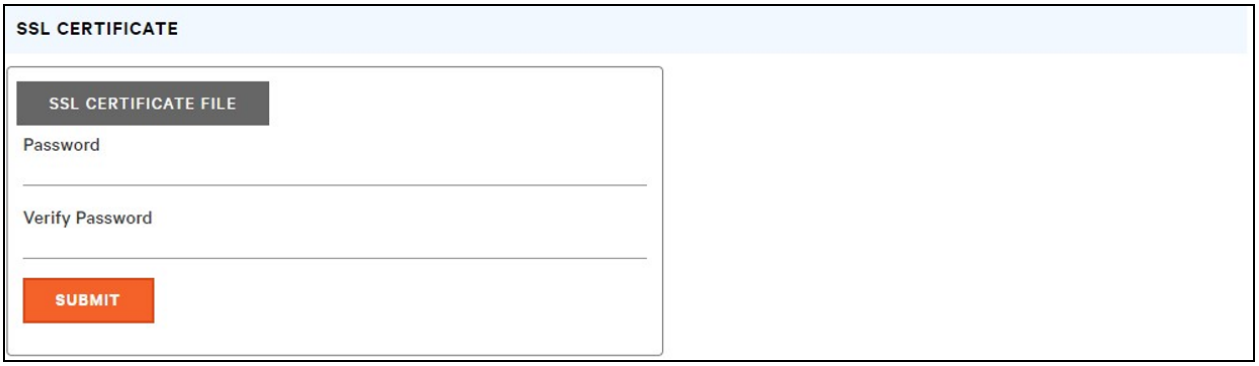


HTTPS

HTTPS Interface: Enabled
HTTPS Port: 443

- 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 5.39 SSL Certificate**


SSL CERTIFICATE

SSL CERTIFICATE FILE

Password

Verify Password

SUBMIT

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

## 5.6.4 Remote authentication

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

**To change Remote Authentication settings:**

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

### LDAP

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

**NOTE: Knowledge of your LDAP server settings is required to set up the Vertiv™ PowerGo 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 (Such as *[2001:0DB8:AC10:FE01::]*) or a hostname.
- **LDAP Server Port:** Used to set the LDAP port number. The default port for LDAP is *389* - use for Security Type *None* or *StartTLS*. Use *636* for Security Type *SSL*.
- **LDAP Mode:** From the drop-down menu, select *Active Directory* or **OpenLDAP**. See An Example of Configuring LDAP for Active Directory Credentials on page 117.
- **Security Type:** From the drop-down menu, select *None*, *SSL* or *StartTLS*.
- **Bind DN:** Distinguished Name used to bind to the directory server. Blank string for Bind DN and Password implies anonymous bind.
- **Bind Password:** Password used to bind to the directory server.
- **Base DN:** DN to use for the search base.

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

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

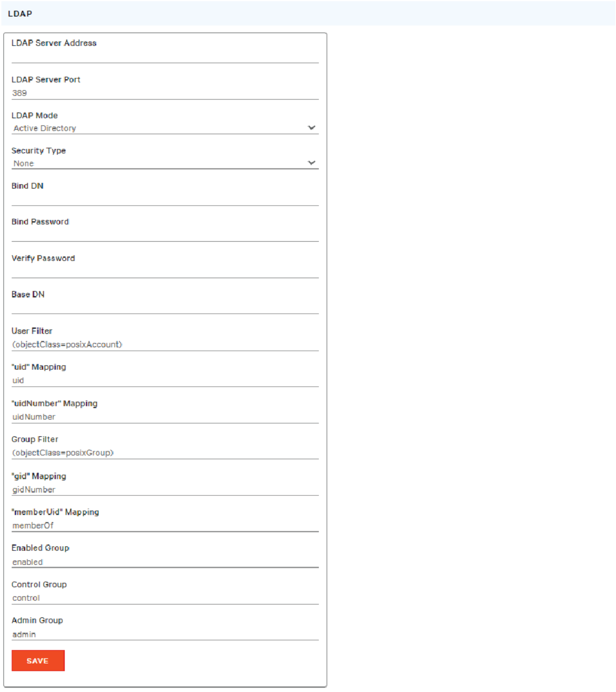
**NOTE: Users *must* populate uidNumber. A null or missing value will cause a valid login to fail. The user's uidNumber *must* be 1000 or greater. A value lower than 1000 will cause a valid login to fail.**

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

Click *SAVE*.

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

**Figure 5.40 LDAP Menu**



LDAP

LDAP Server Address

LDAP Server Port
389

LDAP Mode
Active Directory

Security Type
None

Bind DN

Bind Password

Verify 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

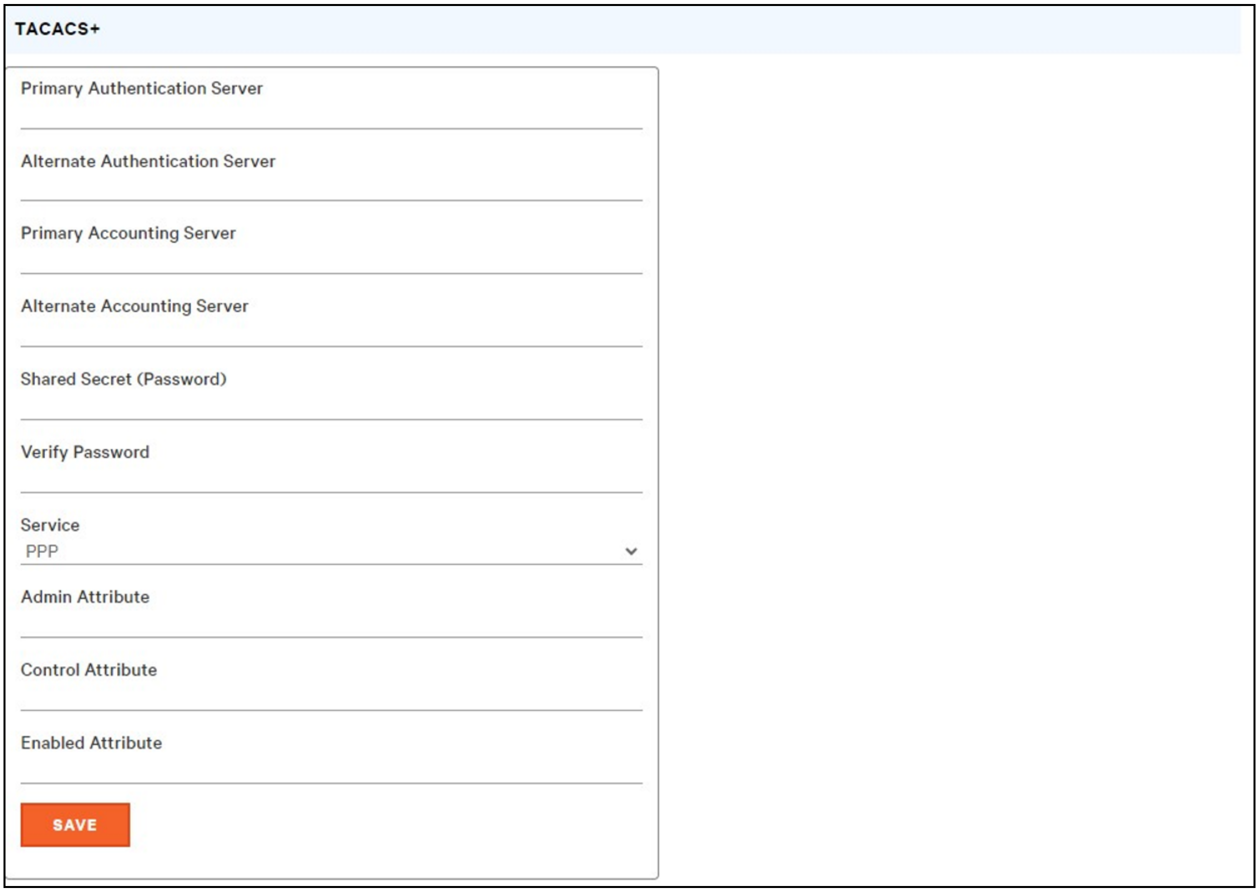
### TACACS+

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

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

Configuration for remote authentication using TACACS+.

**Figure 5.41 TACACS+ Menu**


TACACS+

Primary Authentication Server

Alternate Authentication Server

Primary Accounting Server

Alternate Accounting Server

Shared Secret (Password)

Verify Password

Service
PPP

Admin Attribute

Control Attribute

Enabled Attribute

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

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

Click *SAVE*.

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

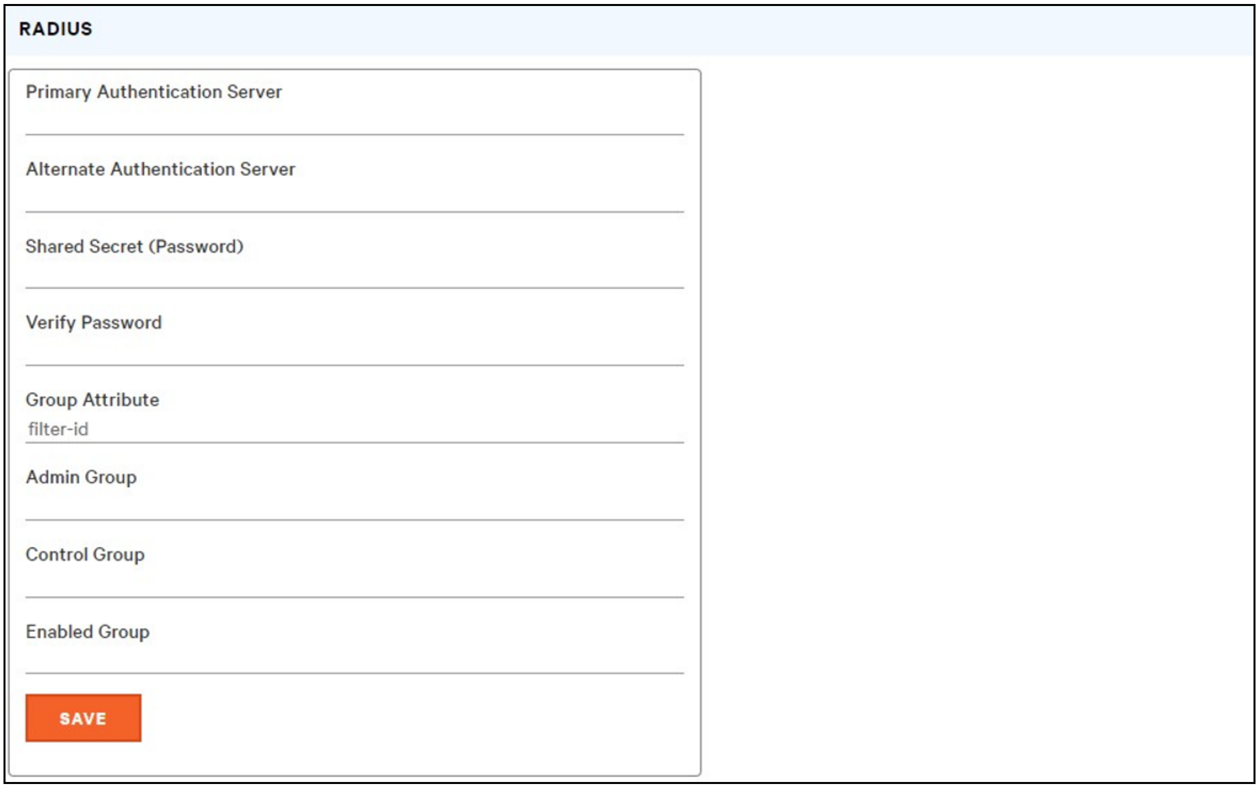
### RADIUS

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

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

Configuration for remote authentication using RADIUS.

**Figure 5.42 RADIUS Menu**



RADIUS

Primary Authentication Server

Alternate Authentication Server

Shared Secret (Password)

Verify Password

Group Attribute
filter-id

Admin Group

Control Group

Enabled Group

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

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

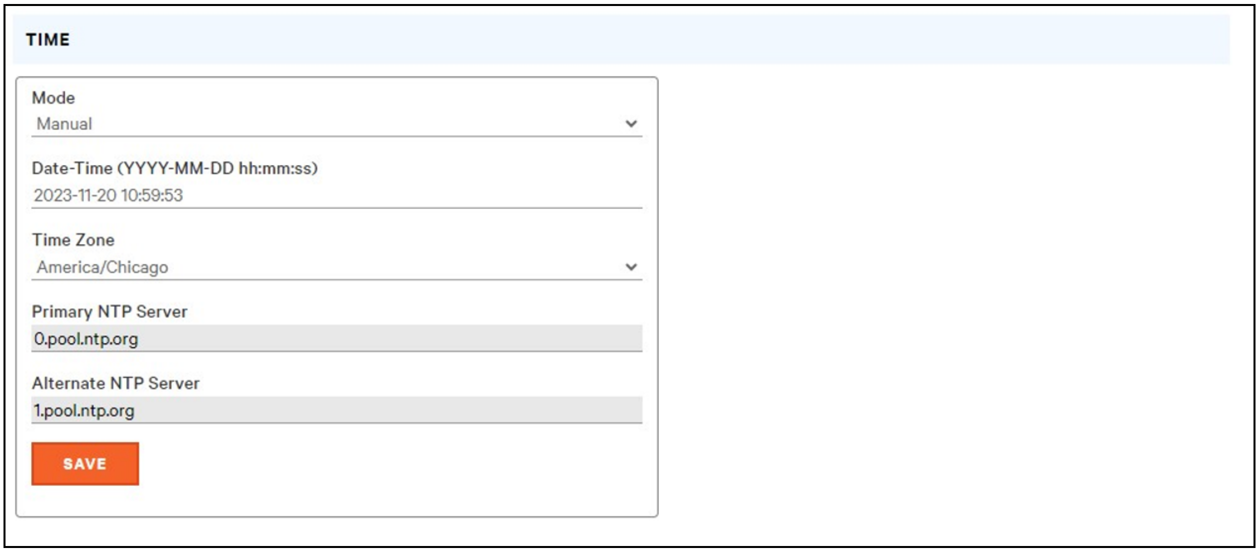
Click *SAVE*.

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

## 5.6.5 Time

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

**Figure 5.43 Time Configuration Page**



TIME

Mode
Manual

Date-Time (YYYY-MM-DD hh:mm:ss)
2023-11-20 10:59:53

Time Zone
America/Chicago

Primary NTP Server
0.pool.ntp.org

Alternate NTP Server
1.pool.ntp.org

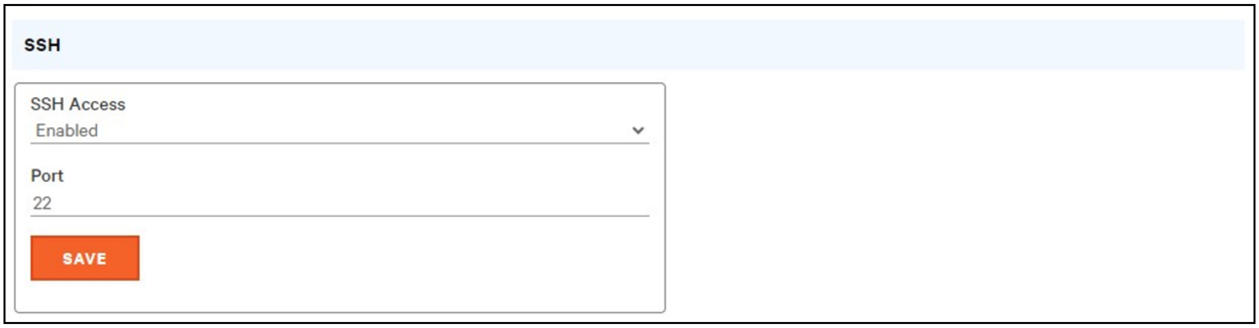
Two modes are available:

- **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.

### 5.6.6 SSH

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

**Figure 5.44 SSH Configuration Page**



SSH

SSH Access: Enabled

Port: 22

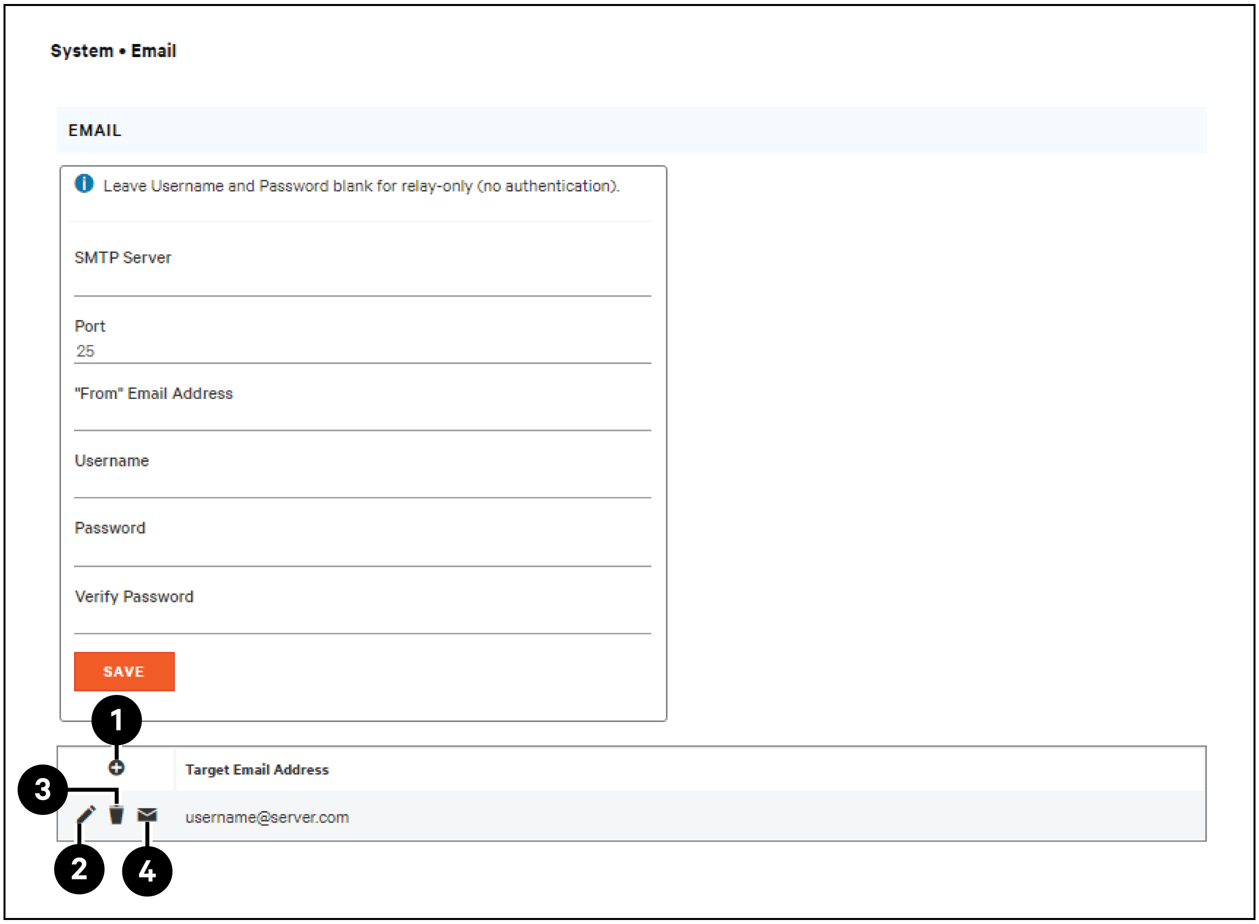
- **SSH Access:** Enables or disables access via SSH.
- **SSH Port:** Allows you to change the port that the SSH service listens to for incoming connections. The default is Port 22.

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

### 5.6.7 Email

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

### Figure 5.45 Email Configuration Page



System • Email

EMAIL

Leave Username and Password blank for relay-only (no authentication).

SMTP Server

Port
25

"From" Email Address

Username

Password

Verify Password

| | Target Email Address |
|---|---|
| | username@server.com |

### Table 5.10 Email Configuration Page Descriptions

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

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

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

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

**To add or modify a target email address:**

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

**To delete a target email address:**

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

**To send a test email:**

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

### 5.6.8 SNMP

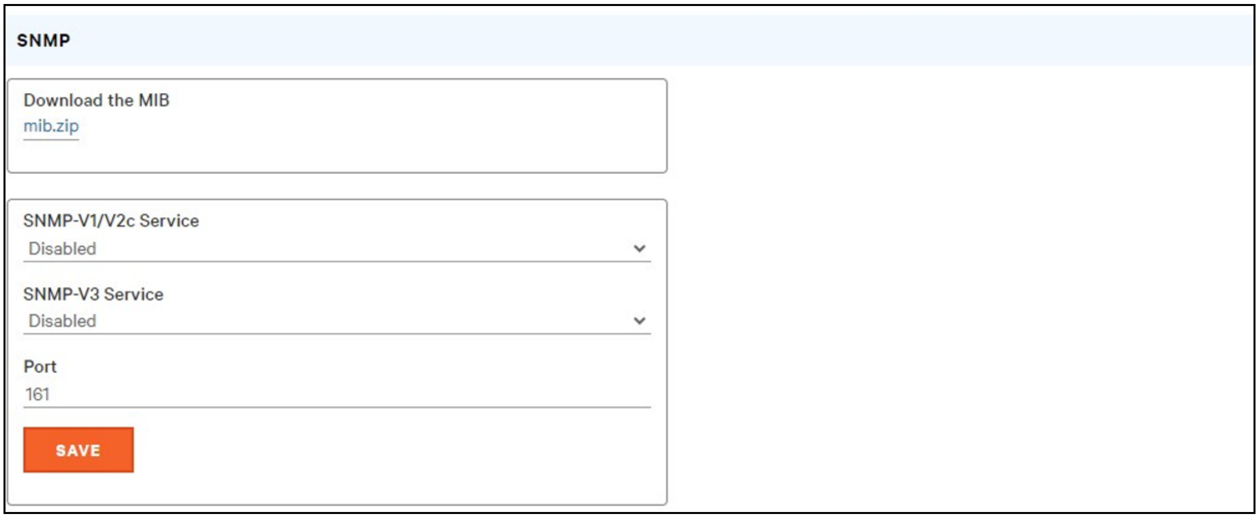
Simple Network Management Protocol (SNMP) can be used to monitor the unit's measurements and status. SNMP V1, V2c and V3 are supported. In addition, alarm traps can be sent to up to ten IP addresses.

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

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

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

Figure 5.46 SNMP Configuration Page



SNMP

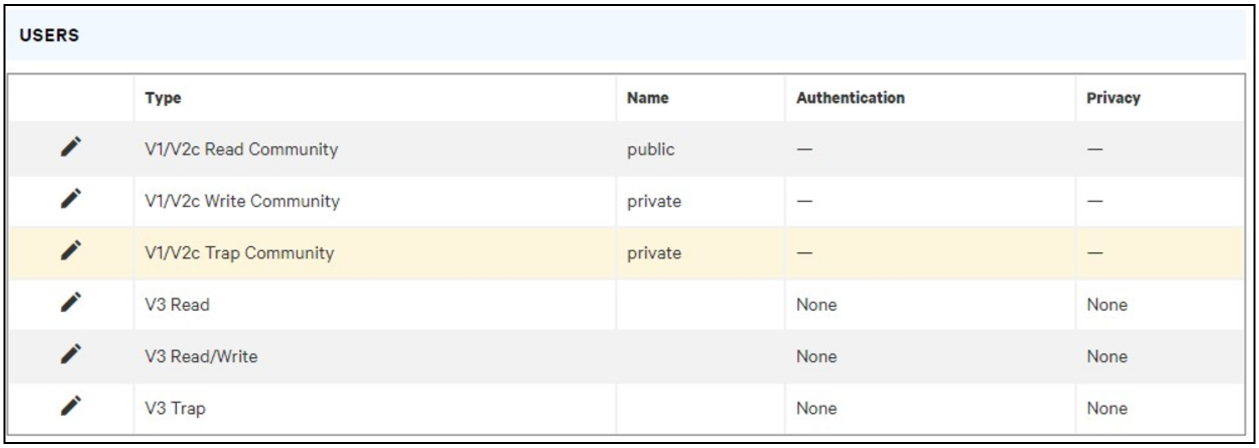
Download the MIB
mib.zip

SNMP-V1/V2c Service
Disabled

SNMP-V3 Service
Disabled

Port
161

Figure 5.47 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.

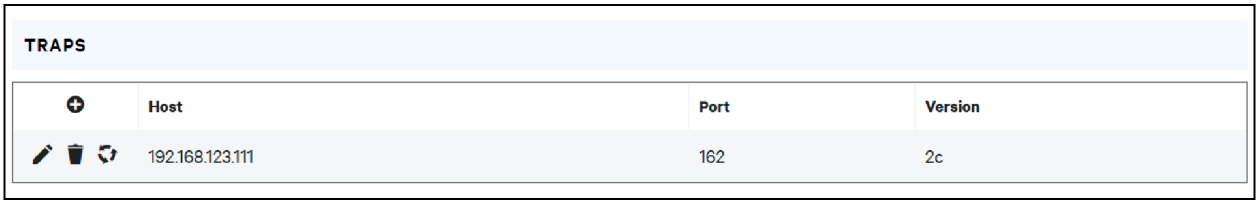
Traps allow defining the SNMP types that you wish to be sent and the IP addresses of recipients.

**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.

**Figure 5.48 Trap**



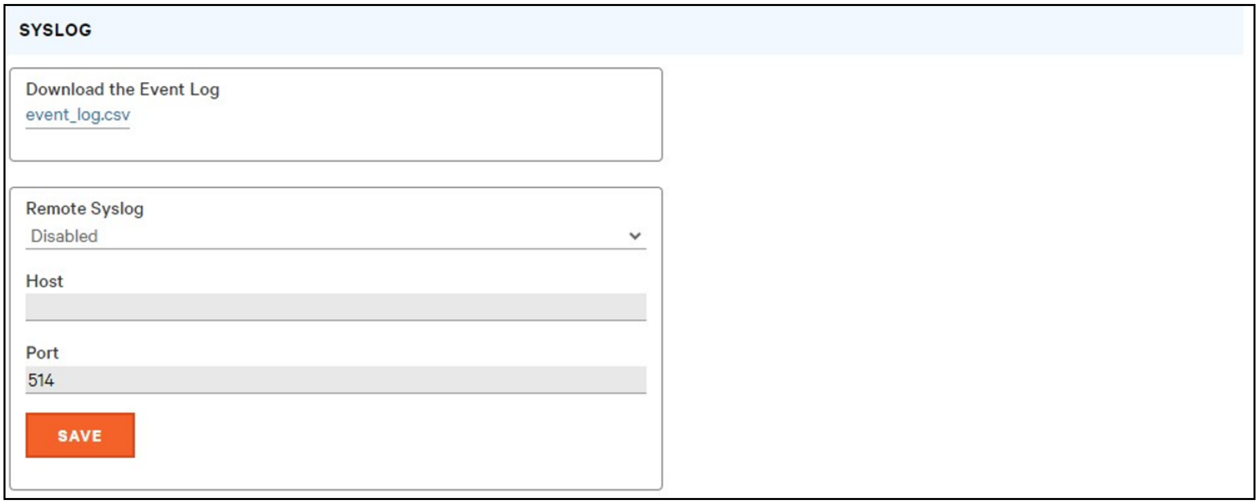
TRAPS

| ⊕ | Host | Port | Version |
|---|---|---|---|
| ✎ 🗑 ↻ | 192.168.123.111 | 162 | 2c |

## 5.6.9 SYSLOG

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

**Figure 5.49 SYSLOG**



SYSLOG

Download the Event Log
event_log.csv

Remote Syslog
Disabled

Host

Port
514

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

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

## 5.6.10 Admin

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

### 5.6.11 Locale

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

## 5.7 Utilities Sub Menu

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

### 5.7.1 Configuration Backup and Restore

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

**Table 5.11 Backup and Restore Options**

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

**To save current configuration settings:**

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

**NOTE: Saving configuration does not require user authentication.**

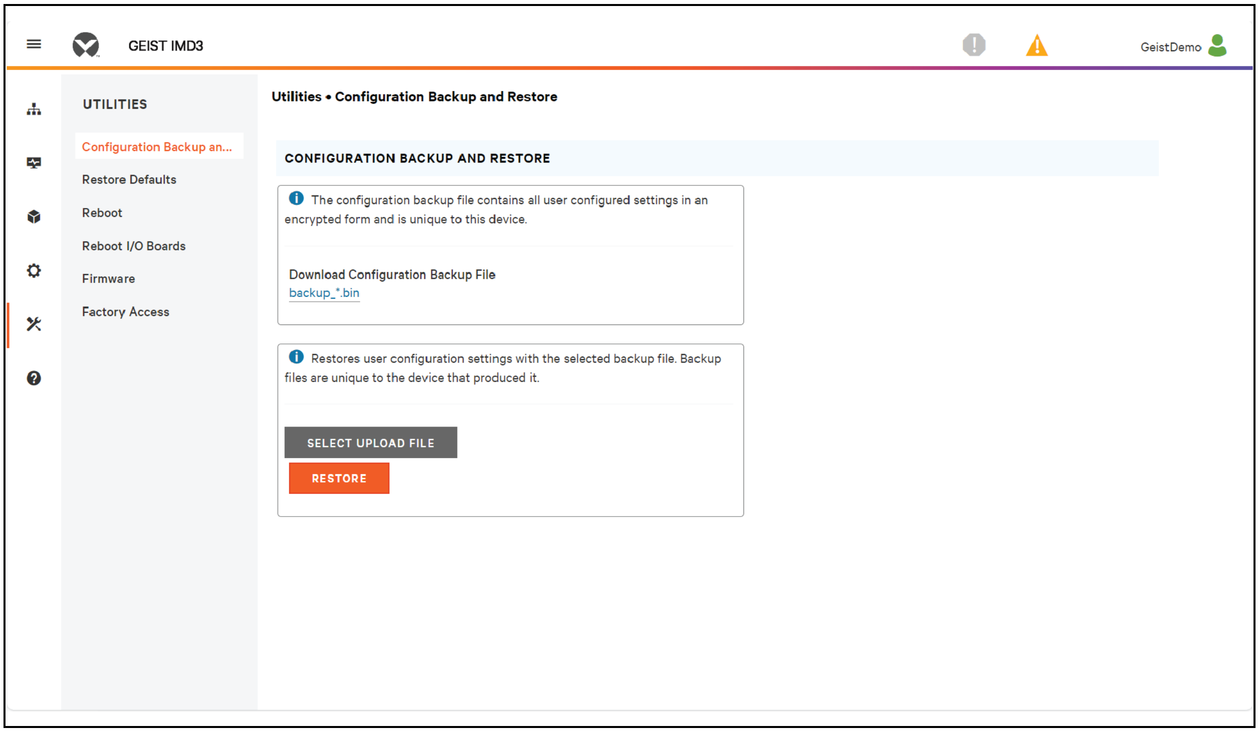
**To restore a previous configuration setting:**

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

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

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

Figure 5.50 Configuration Backup and Restore Overview



The configuration backup file contains all user configured settings in an encrypted form and is unique to this device.

Download Configuration Backup File
backup_*.bin

Restores user configuration settings with the selected backup file. Backup files are unique to the device that produced it.

## 5.7.2 Restore defaults

Restore the default settings.

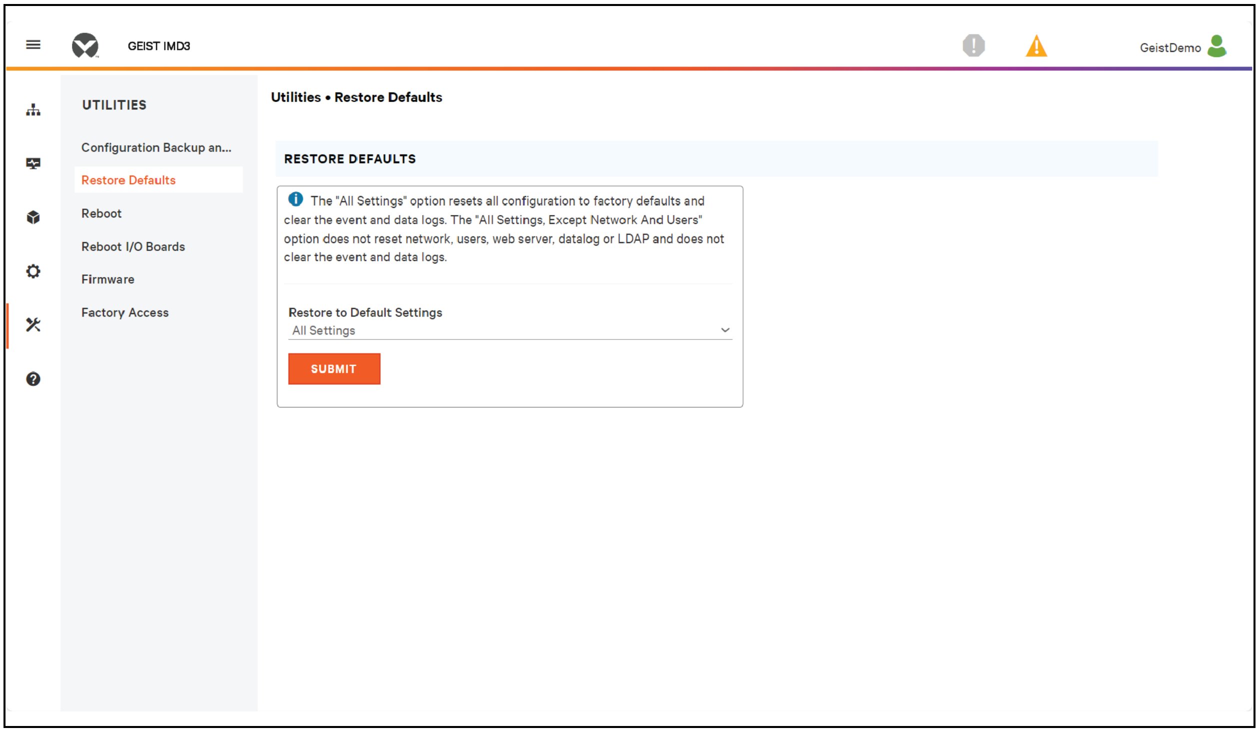
Table 5.12 Restore Default Options

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

**To restore default settings:**

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

**Figure 5.51 Restore Defaults Overview**



The "All Settings" option resets all configuration to factory defaults and clear the event and data logs. The "All Settings, Except Network And Users" option does not reset network, users, web server, datalog or LDAP and does not clear the event and data logs.

Restore to Default Settings: All Settings

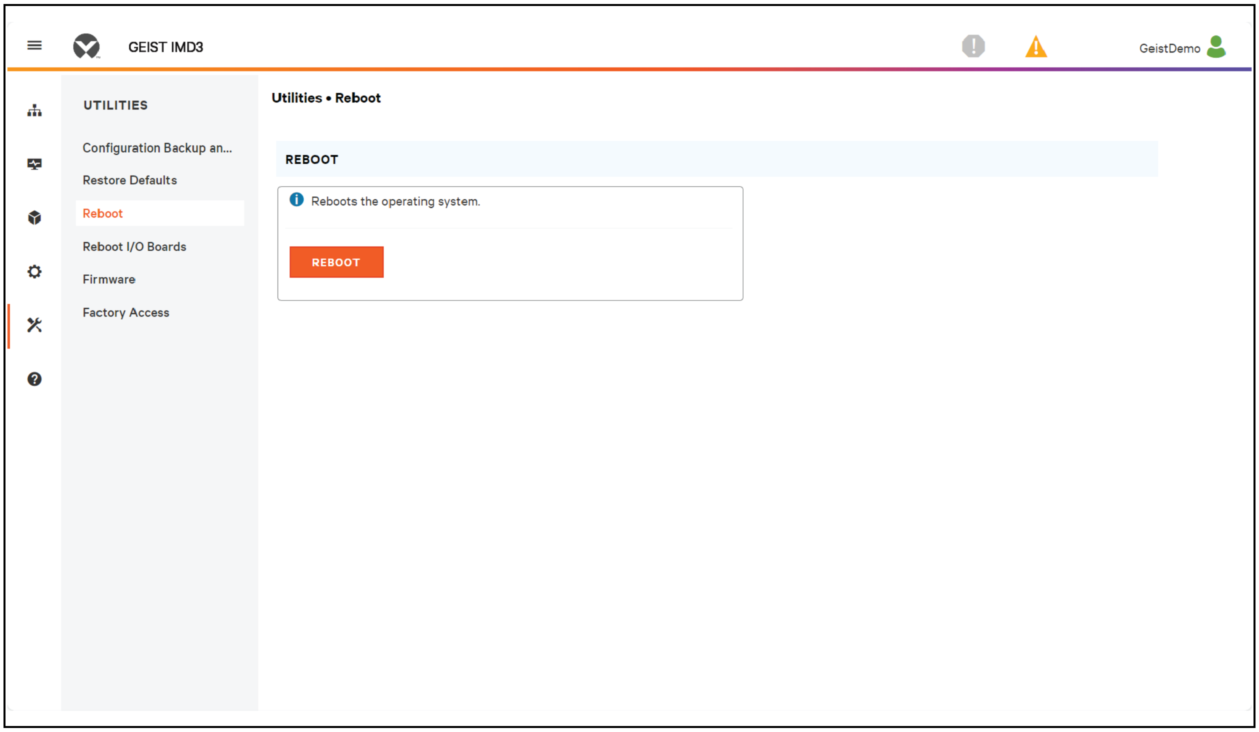
## 5.7.3 Reboot

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

Click *REBOOT* to reboot the operating system.

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

**Figure 5.52 Rebootc Overview**



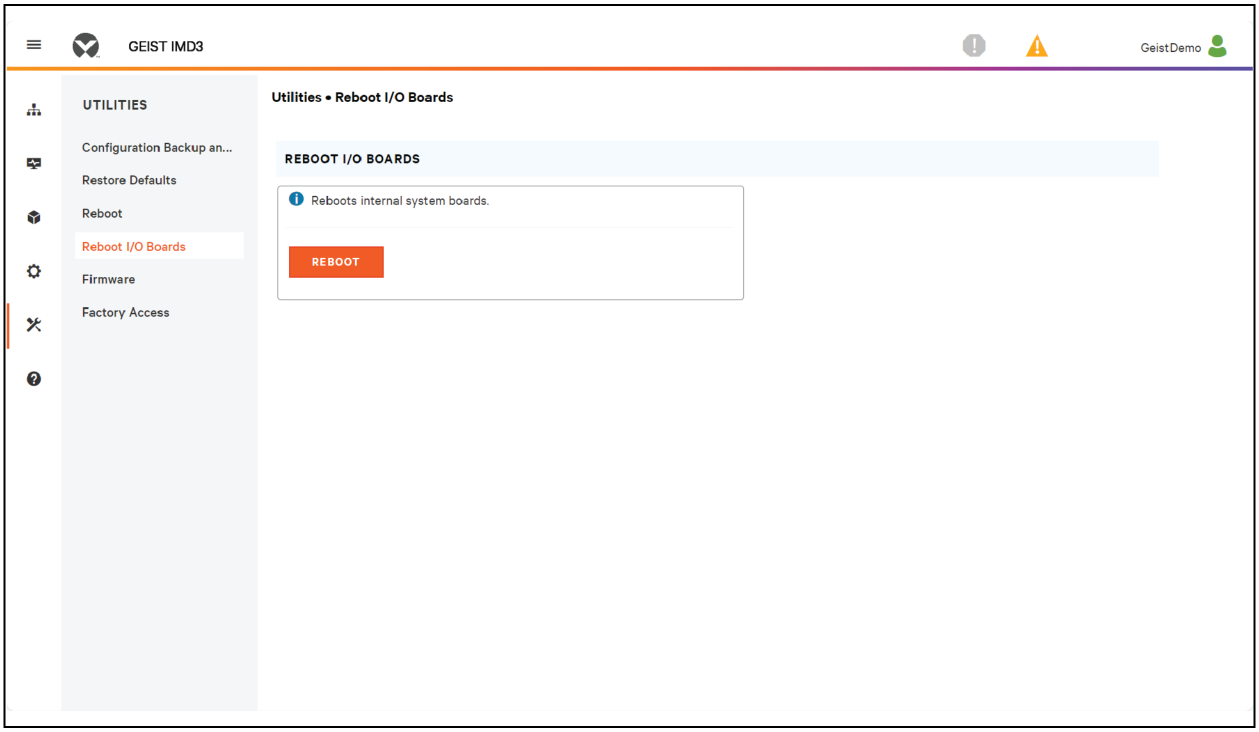
## 5.7.4 Reboot I/O Boards

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

Click *REBOOT* to reboot the internal system boards.

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

**Figure 5.53 Reboot I/O Boards Overview**



Reboots internal system boards.

## 5.7.5 Firmware Updates

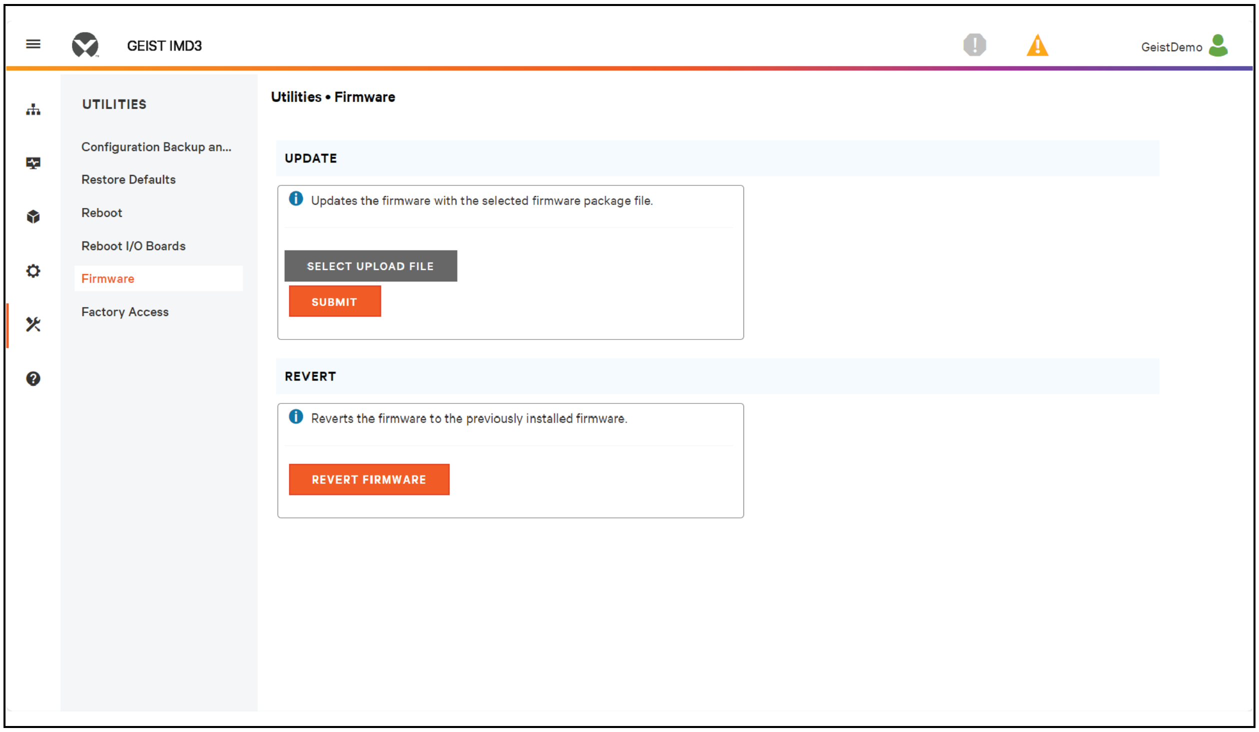
Uploads a firmware file that updates the system. This action requires user authentication and the user must have administrator privileges. Firmware updates typically comes in a .zip archive file containing several files including the firmware package itself, a copy of the SNMP MIB, a readme text file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

**To update Firmware via Firmware Package File:**

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

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.

Figure 5.54 Firmware Overview



Updates the firmware with the selected firmware package file.

Reverts the firmware to the previously installed firmware.

## 5.7.6 Factory Access

Factory Access Provides information for technical support.

Table 5.13 Factory Access Options

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

### To download a factory support package:

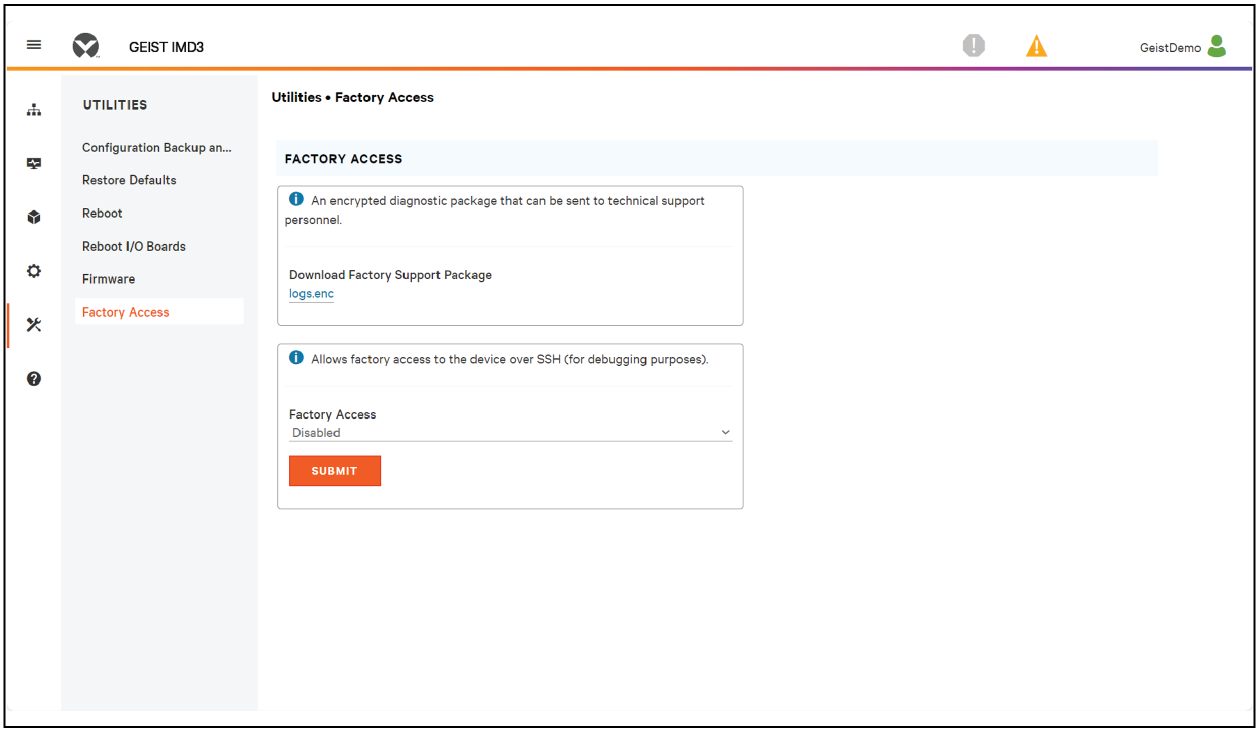
1. Click *Download Factory Support Package*.
2. Click *ENC*.

### To enable/disable factory access:

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

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

**Figure 5.55 Factory Access Overview**



Utilities • Factory Access

FACTORY ACCESS

An encrypted diagnostic package that can be sent to technical support personnel.

Download Factory Support Package
logs.enc

Allows factory access to the device over SSH (for debugging purposes).

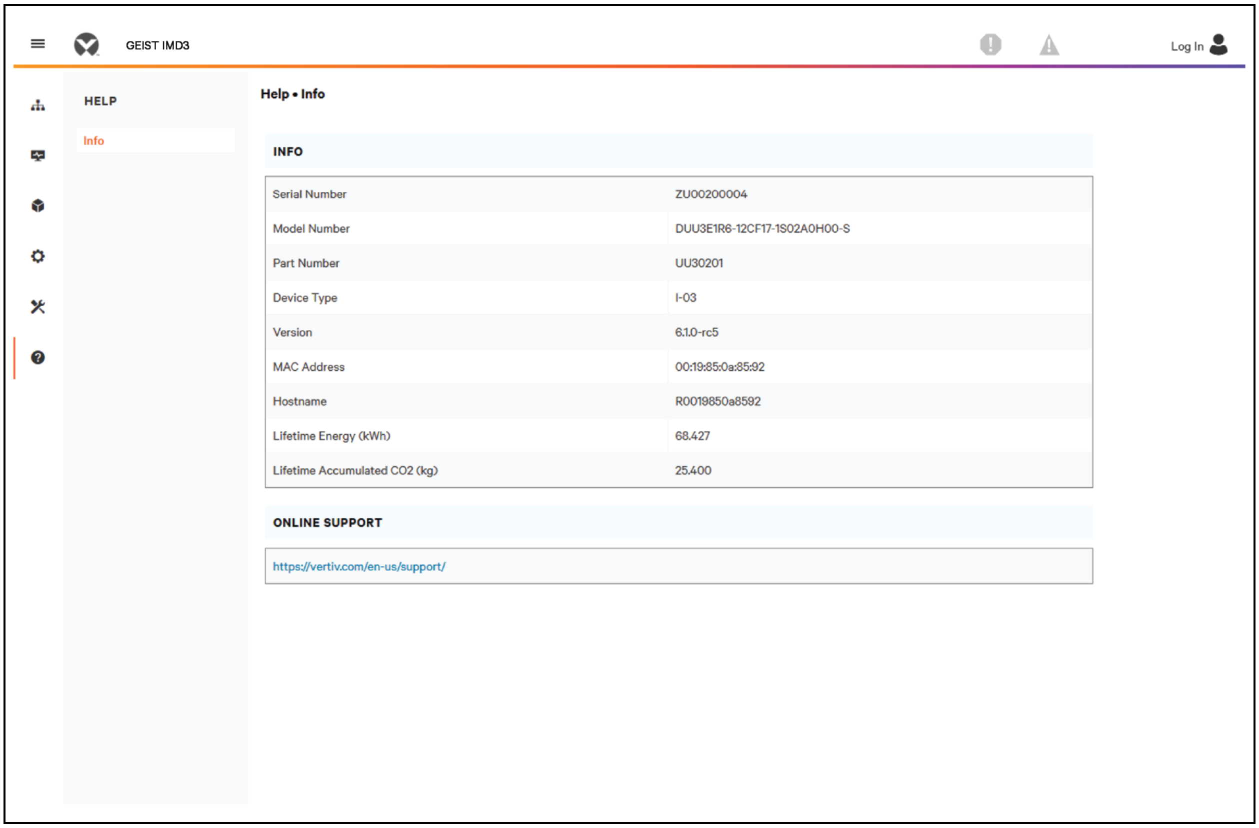
Factory Access
Disabled

## 5.8 Help Sub Menu

### Info Page

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

**Figure 5.56 Info Page**



Help • Info

INFO

| | |
|---|---|
| Serial Number | ZU00200004 |
| Model Number | DUU3E1R6-12CF17-1S02A0H00-S |
| Part Number | UU30201 |
| Device Type | I-03 |
| Version | 6.1.0-rc5 |
| MAC Address | 00:19:85:0a:85:92 |
| Hostname | R0019850a8592 |
| Lifetime Energy (kWh) | 68.427 |
| Lifetime Accumulated CO2 (kg) | 25.400 |

ONLINE SUPPORT

https://vertiv.com/en-us/support/

# 6 Vertiv™ Intelligence Director

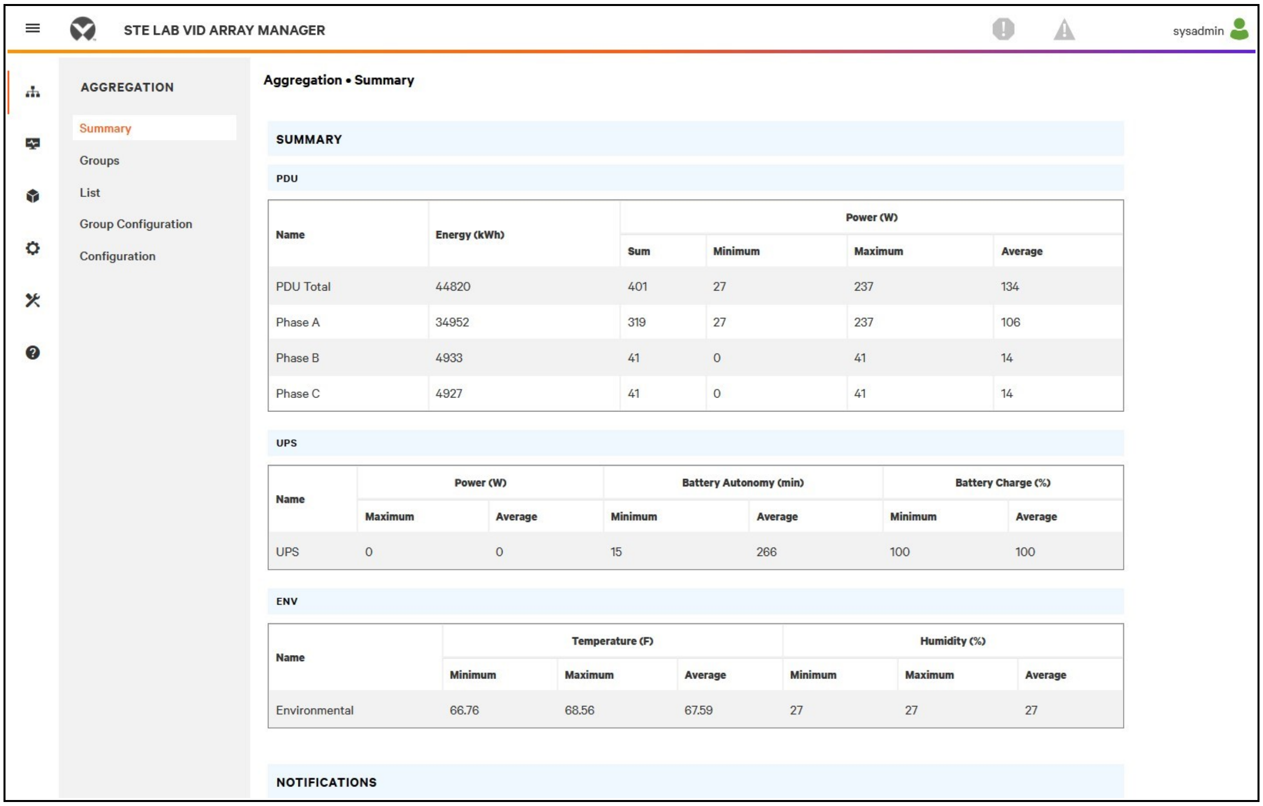
Vertiv Intelligence Director brings a single, unified viewing layer for small deployments of the Vertiv™ PowerGo rPDUs, Vertiv™ UPSs. When deployed, Vertiv Intelligence Director offers enhanced functionality, using the Vertiv™ PowerGo rPDU not as a stand-alone device but as a gateway to understand the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

## 6.1 Aggregation

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

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

## Figure 6.1 Aggregation Tab



Aggregation • Summary

SUMMARY

PDU

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

UPS

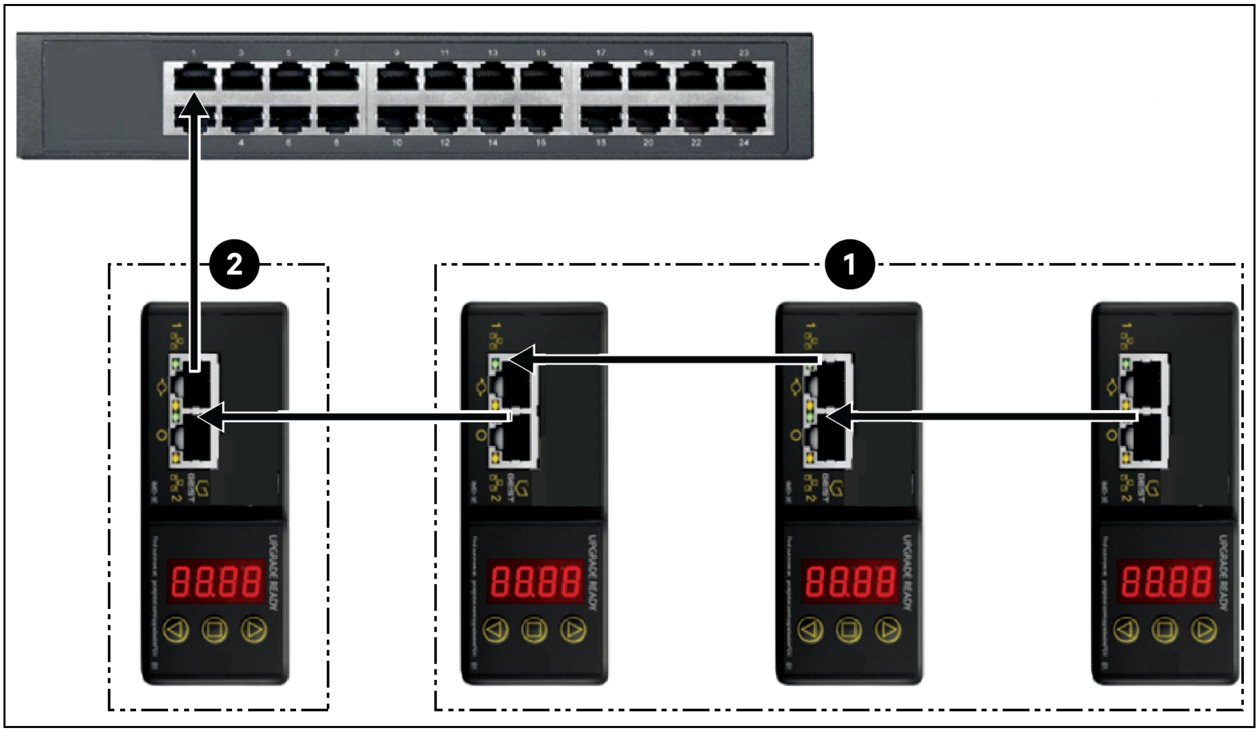
| Name | Power (W) | | Battery Autonomy (min) | | Battery Charge (%) | |
|---|---|---|---|---|---|---|
| | Maximum | Average | Minimum | Average | Minimum | Average |
| UPS | 0 | 0 | 15 | 266 | 100 | 100 |

ENV

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

NOTIFICATIONS

## Figure 6.2 Aggregation



| Item | Description |
|---|---|
| 1 | Array device |
| 2 | Array manager |

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

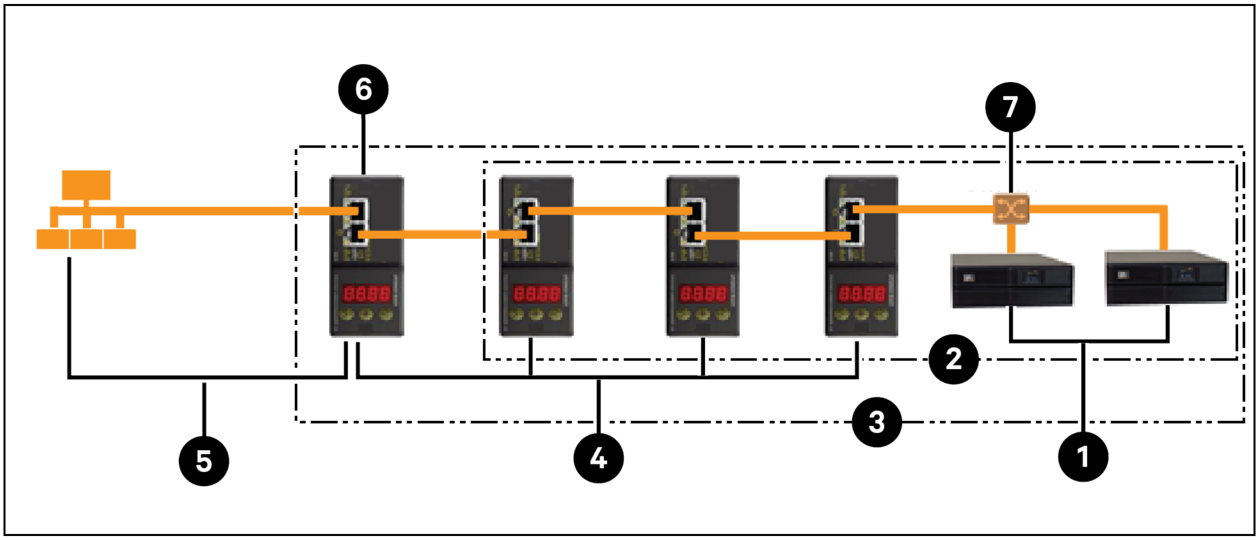
- Provide the ability for power off, power on or power cycle the group of outlets with a single commend (with Vertiv™ PowerGo rPDUs that support outlet switching).

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

## 6.2 Array Manager

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

**Figure 6.3 Sample Configuration**



| Item | Description |
|---|---|
| 1 | Vertiv™ Liebert® GXT4 |
| 2 | Downstream devices |
| 3 | Device network |
| 4 | GU |

| Item | Description |
|---|---|
| 5 | Management network |
| 6 | Master device (GU2) |
| 7 | Ethernet switch |

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

## 6.3 Network Configuration

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

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

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

**To commission the array manager:**

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

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

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

## Array devices

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

**To set up a new installation with one array manager:**

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

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

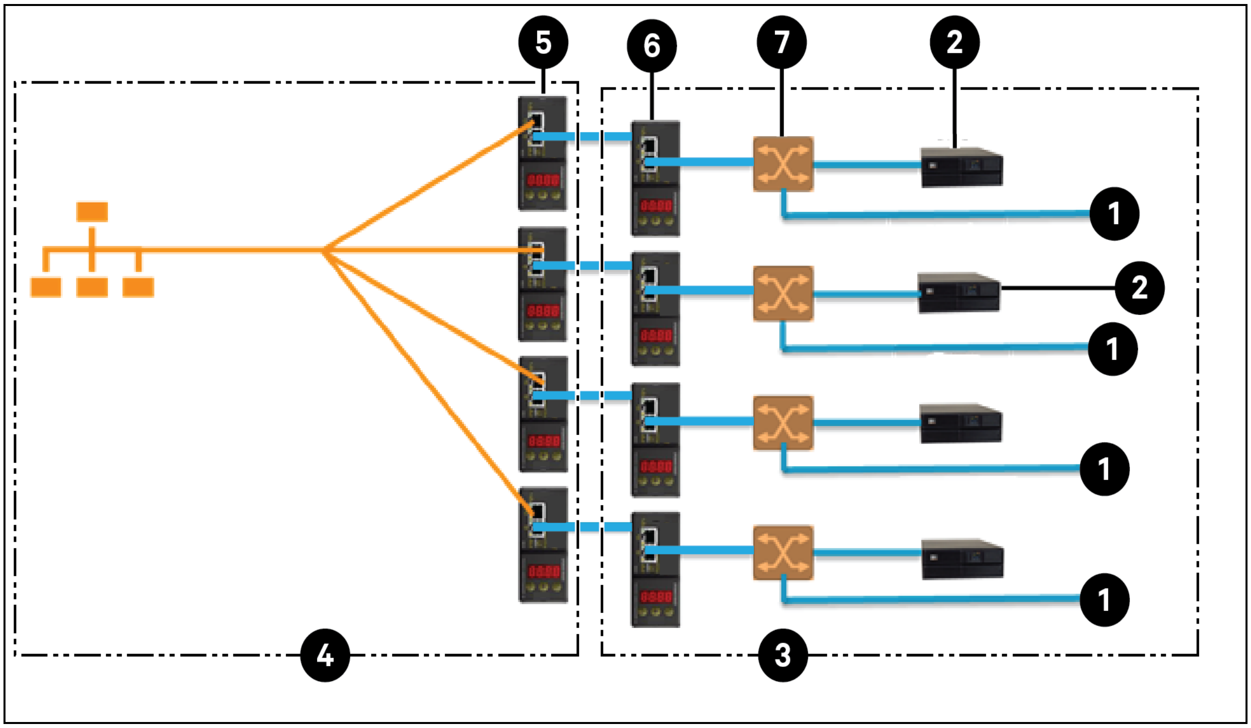
**NOTE: Use the following instructions if existing Vertiv™ PowerGo rPDUs are connected in a daisy-chain.**

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

## Multiple Array Managers

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

Figure 6.4 Sample Network Configuration



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

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

## 6.4 Views

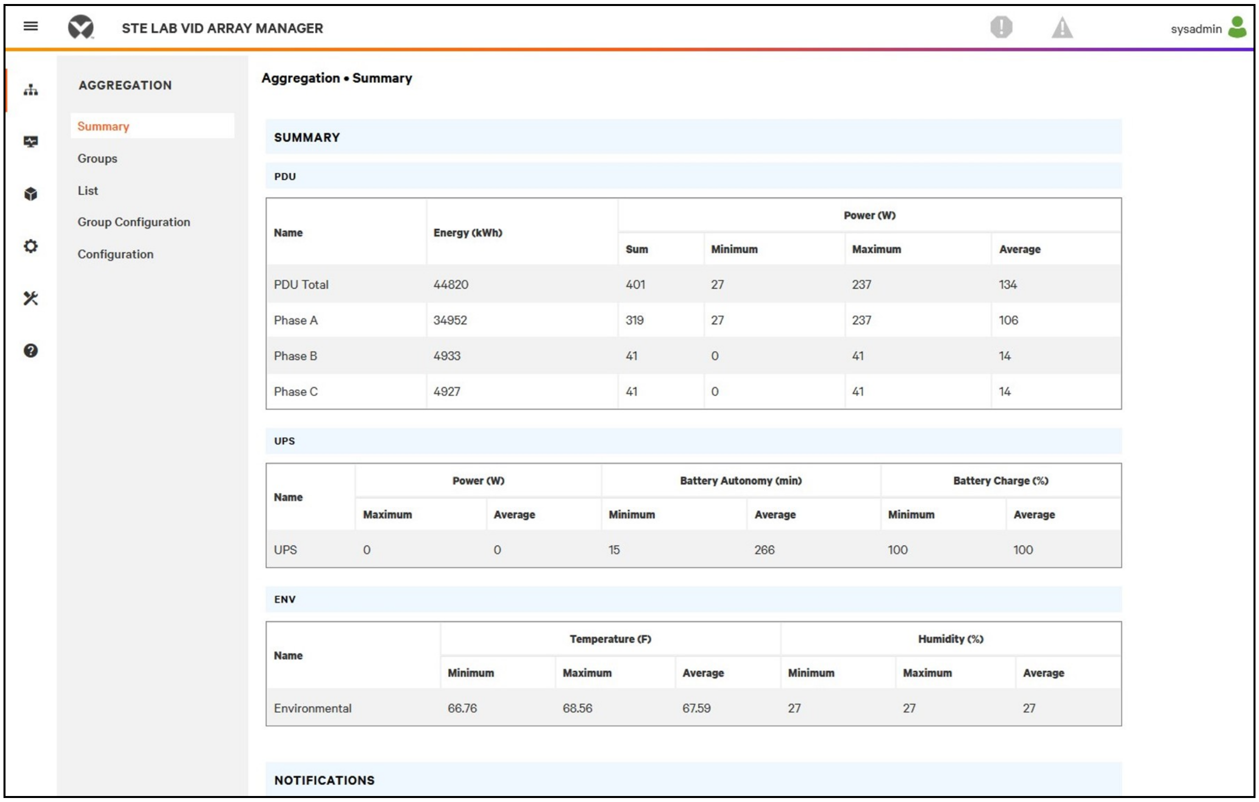
When communication is established between the array manager and array devices, several views are automatically populated in the user interface. The new views under the Device tab in the top navigation bar are:

- Summary
- Groups
- List
- Group Configuration
- Configuration

## 6.4.1 Summary

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

**Figure 6.5 Summary Tab**



Aggregation • Summary

SUMMARY

PDU

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

UPS

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

ENV

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

NOTIFICATIONS

## Rack PDUs

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

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

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

### UPS

The UPS network is summarized by the following data points:

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

### Thermal Cooling

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

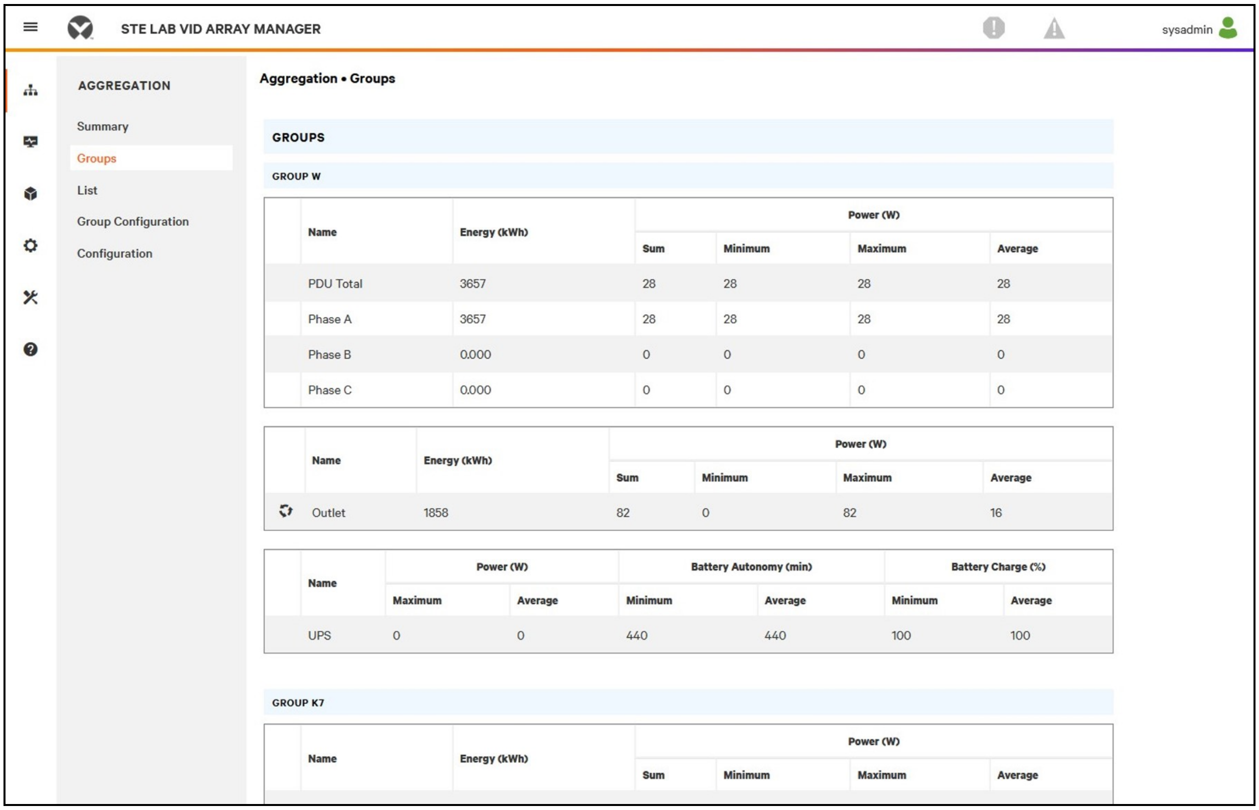
### Notifications

Notifications shows outstanding alarms from devices in the device network.

## 6.4.2 Groups

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

Figure 6.6 Groups Tab



Aggregation • Groups

GROUPS

GROUP W

| Name | Energy (kWh) | Power (W) | | | |
|---|---|---|---|---|---|
| | | Sum | Minimum | Maximum | Average |
| PDU Total | 3657 | 28 | 28 | 28 | 28 |
| Phase A | 3657 | 28 | 28 | 28 | 28 |
| Phase B | 0.000 | 0 | 0 | 0 | 0 |
| Phase C | 0.000 | 0 | 0 | 0 | 0 |

| Name | Energy (kWh) | Power (W) | | | |
|---|---|---|---|---|---|
| | | Sum | Minimum | Maximum | Average |
| Outlet | 1858 | 82 | 0 | 82 | 16 |

| Name | Power (W) | | Battery Autonomy (min) | | Battery Charge (%) | |
|---|---|---|---|---|---|---|
| | Maximum | Average | Minimum | Average | Minimum | Average |
| UPS | 0 | 0 | 440 | 440 | 100 | 100 |

GROUP K7

| Name | Energy (kWh) | Power (W) | | | |
|---|---|---|---|---|---|
| | | Sum | Minimum | Maximum | Average |

The available data points are:

## Group rPDU

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

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

## Group UPS

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

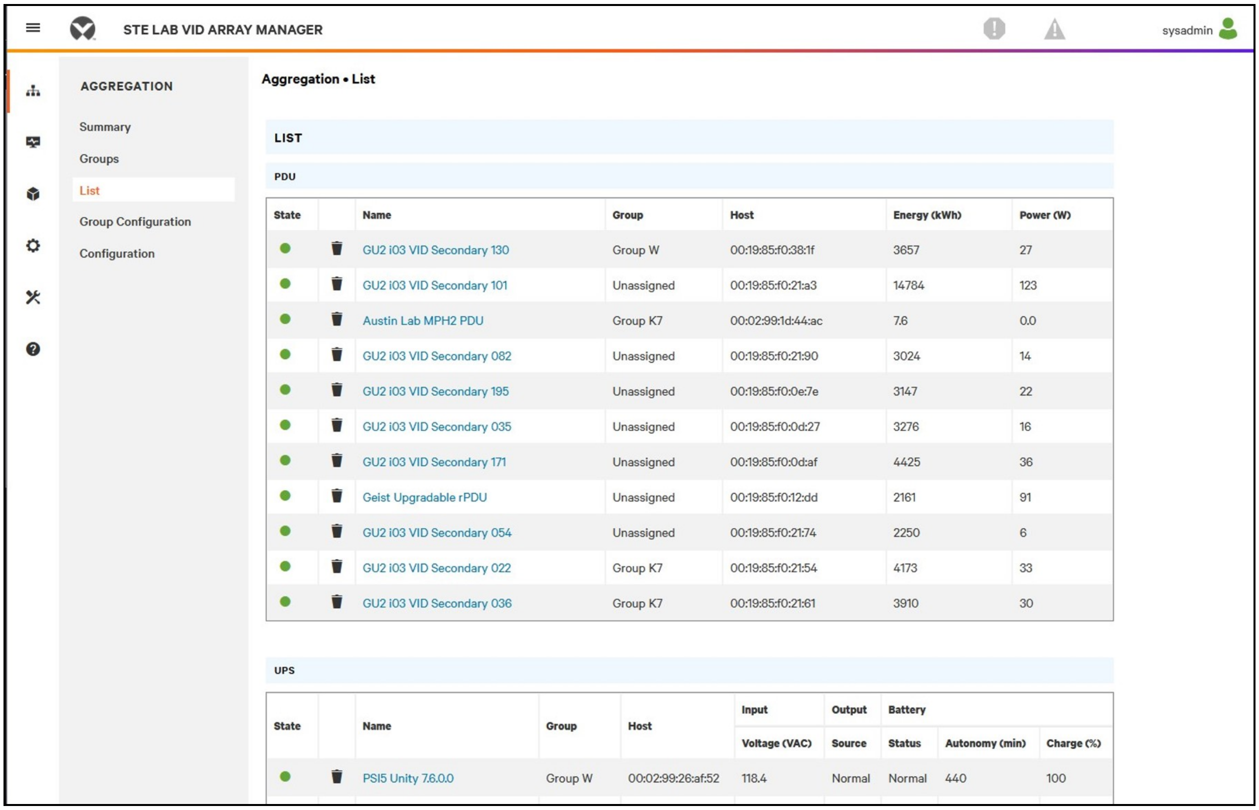
### Group Thermal Cooling

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

## 6.4.3 List

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

**Figure 6.7 List Tab**



Aggregation • List

LIST

PDU

| State | | Name | Group | Host | Energy (kWh) | Power (W) |
|---|---|---|---|---|---|---|
| ● | 🗑 | GU2 i03 VID Secondary 130 | Group W | 00:19:85:f0:38:1f | 3657 | 27 |
| ● | 🗑 | GU2 i03 VID Secondary 101 | Unassigned | 00:19:85:f0:21:a3 | 14784 | 123 |
| ● | 🗑 | Austin Lab MPH2 PDU | Group K7 | 00:02:99:1d:44:ac | 7.6 | 0.0 |
| ● | 🗑 | GU2 i03 VID Secondary 082 | Unassigned | 00:19:85:f0:21:90 | 3024 | 14 |
| ● | 🗑 | GU2 i03 VID Secondary 195 | Unassigned | 00:19:85:f0:0e:7e | 3147 | 22 |
| ● | 🗑 | GU2 i03 VID Secondary 035 | Unassigned | 00:19:85:f0:0d:27 | 3276 | 16 |
| ● | 🗑 | GU2 i03 VID Secondary 171 | Unassigned | 00:19:85:f0:0d:af | 4425 | 36 |
| ● | 🗑 | Geist Upgradable rPDU | Unassigned | 00:19:85:f0:12:dd | 2161 | 91 |
| ● | 🗑 | GU2 i03 VID Secondary 054 | Unassigned | 00:19:85:f0:21:74 | 2250 | 6 |
| ● | 🗑 | GU2 i03 VID Secondary 022 | Group K7 | 00:19:85:f0:21:54 | 4173 | 33 |
| ● | 🗑 | GU2 i03 VID Secondary 036 | Group K7 | 00:19:85:f0:21:61 | 3910 | 30 |

UPS

| State | | Name | Group | Host | Input | Output | Battery | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voltage (VAC) | Source | Status | Autonomy (min) | Charge (%) |
| ● | 🗑 | PSI5 Unity 7.6.0.0 | Group W | 00:02:99:26:af:52 | 118.4 | Normal | Normal | 440 | 100 |

The inventory is subdivided into the following categories:

### Rack PDUs

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

- **State:** The status of the Vertiv™ PowerGo rPDU. Status is either normal or unavailable (loss of connectivity).

- **Name:** Vertiv™ PowerGo 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:** Vertiv™ PowerGo rPDU energy.
- **Power:** Total Vertiv™ PowerGo 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.

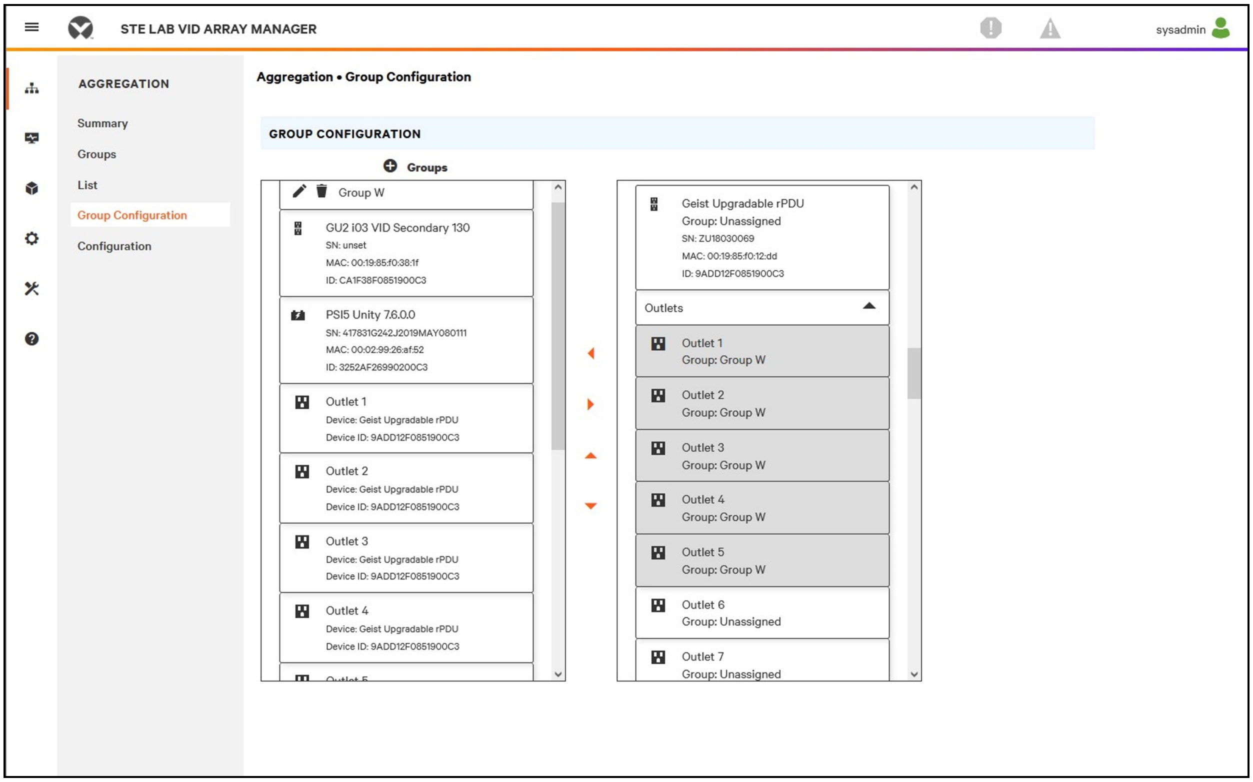
### Thermal Cooling

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

## 6.4.4 Group Configuration

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

**Figure 6.8 Group Configuration**



Group W

GU2 i03 VID Secondary 130
SN: unset
MAC: 00:19:85:f0:38:1f
ID: CA1F38F0851900C3

PSI5 Unity 7.6.0.0
SN: 417831G242J2019MAY080111
MAC: 00:02:99:26:af:52
ID: 3252AF26990200C3

Outlet 1
Device: Geist Upgradable rPDU
Device ID: 9ADD12F0851900C3

Outlet 2
Device: Geist Upgradable rPDU
Device ID: 9ADD12F0851900C3

Outlet 3
Device: Geist Upgradable rPDU
Device ID: 9ADD12F0851900C3

Outlet 4
Device: Geist Upgradable rPDU
Device ID: 9ADD12F0851900C3

Geist Upgradable rPDU
Group: Unassigned
SN: ZU18030069
MAC: 00:19:85:f0:12:dd
ID: 9ADD12F0851900C3

Outlet 1
Group: Group W

Outlet 2
Group: Group W

Outlet 3
Group: Group W

Outlet 4
Group: Group W

Outlet 5
Group: Group W

Outlet 6
Group: Unassigned

Outlet 7
Group: Unassigned

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

- One or more icons defining the type of device such as, Vertiv™ PowerGo rPDU and 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.

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

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

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

To remove devices from a group:

Highlight the devices and click the *Right Arrow*.

To delete a group:

Click the Trash icon next to the group name.

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

## 6.5 Interfaces

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

**To access the Array Device User Interface:**

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

   -or-

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

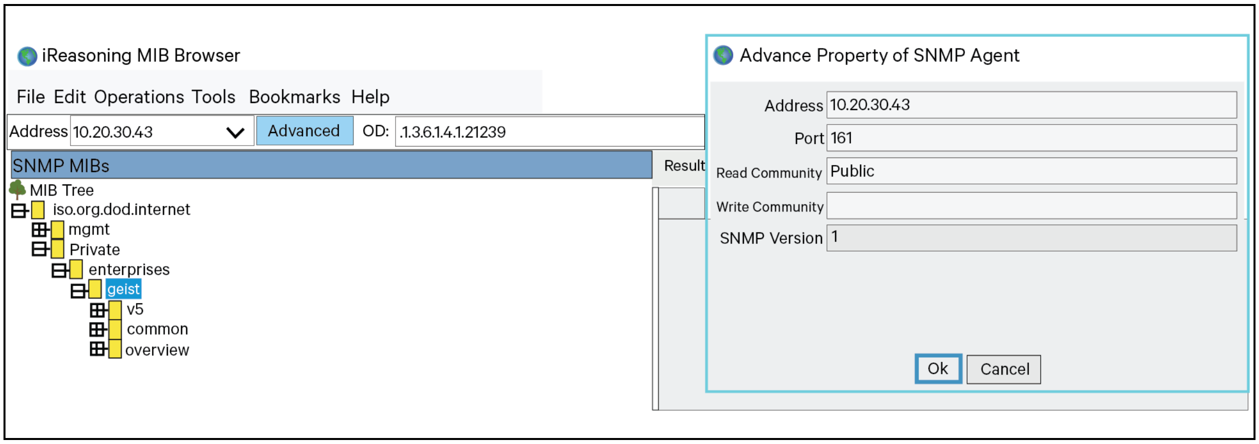
**To access Array Device SNMP Data:**

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

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

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

**Figure 6.9 MIB Browser**



Address 10.20.30.43

OD: .1.3.6.1.4.1.21239

Advance Property of SNMP Agent

Address 10.20.30.43

Port 161

Read Community Public

Write Community

SNMP Version 1

### 6.5.1 Group SNMP data

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

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

### 6.5.2 Tips and troubleshooting

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

# Appendices

## Appendix A: Technical Support

### A.1 Resetting a Vertiv™ PowerGo rPDU

If a Vertiv™ PowerGo rPDU loses communication, the processor may be manually rebooted without affecting power to the outlets. Pressing the reboot button on the face of the IMD will reboot the processor. The web interface will remain offline during boot-up. For more information, see Interchangeable Monitoring Device on page 15.

### A.2 Service and Maintenance

No service or maintenance is required. Opening the Vertiv™ PowerGo rPDU may void the warranty. There are no user-serviceable parts inside the Vertiv™ PowerGo rPDU other than the field-replaceable Interchangeable Monitoring Device (IMD). Vertiv 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 Vertiv™ PowerGo rPDU is still connected to utility power. Refer the Vertiv™ PowerGo 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:** https://www.vertiv.com/en-us/contacts2/support/#?country=198
- **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 Vertiv™ PowerGo 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 Vertiv™ PowerGo 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 Vertiv™ PowerGo 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 Vertiv™ PowerGo 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 Vertiv™ PowerGo 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 Vertiv™ PowerGo 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 Vertiv™ PowerGo rPDU still cannot connect to the Exchange server, the account probably did not properly inherit the new permissions when you enabled them as above. This tends to happen more often on Exchange servers that have been upgraded since the account you are trying to use were created, but can sometimes happen with accounts when new connectors and plug-ins are added, regardless of the Exchange version. Delete the user accounts, then create a new one for the monitoring unit to use and the new account should inherit the SMTP authentication and mail-relaying permissions correctly.

If none of the above suggestions succeed in getting your IMD Vertiv™ PowerGo 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: Outlet LEDs

**NOTE: This appendix applies to Outlet Switched Vertiv™ PowerGo rPDUs only.**

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

**Table B.1 LED Outlets**

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

**Table B.2 LED Status Description**

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

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

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

### Error Code

LEDs illuminate in Solid Amber during the following:

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

This page intentionally left blank

# Appendix C: IMD Display Codes

### Table C.1 IMD Display Codes

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

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

This page intentionally left blank

# Appendix D: Provisioner - Format of the configuration settings file

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

1. In the examples below, the text in blue can be copied to a text file and updated as required. The text file can then be uploaded to the provisioning tool.
2. When editing configuration files, use a text editor such as notepad which can save files in .txt format.
3. The indentations shown in the examples can be omitted.
4. Ensure the correct double quote is used when editing configuration.
5. If a setting is omitted from the settings file, the value of that setting will remain unchanged.
6. When configuring a previously unconfigured (factory fresh) Vertiv™ PowerGo rPDU, the first configuration setting should be the definition of an admin user, See Local Users below.
7. To combine several settings (other than local users) into one file (see also Example 1 on page 104 at the end of this document):
    - Append together the required settings into one file.
    - Delete all occurrences of {"conf":{ except for the first line of the file.
    - Replace all lines that contain only }} by a , (comma) except for the last line of the file.
8. If combining local user settings with other settings in one file, refer to Example 2 on page 104 at the end of this document.
9. After selecting *Provisioner>Discovery>Update*, enter the user name and password only when configuring previously configured Vertiv™ PowerGo rPDUs (the user name and password being that of the Vertiv™ PowerGo rPDUs being provisioned). Do not enter a user and password when configuring factory fresh units (identified by Provisioned attribute equalling False).

### Local Users

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

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

### LDAP

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

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

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

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

**Radius**

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

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

### Network Hostname and IP Addresses

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

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

### Network Ports

```
{"conf":{
"network": {
"port0": {
"label": "Port 0",
"enabled": true,
"stp": {"cost": 0}},
"port1": {
"label": "Port 1",
"enabled": true,
"stp": {"cost": 0}}}
}}
```

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

#### Network Routes

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

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

#### Network DNS

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

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

#### Network RSTP

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

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

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

### Web Server

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

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

### Reports

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

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

**Display**

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

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

**Time**

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

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

### SSH

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

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

### Email

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

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

### SNMP v1 or v2c

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

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

### SNMP v3

```
{"conf":{
"snmp": {
"v3Enabled": true,
"port": 161,
"user": {
"0": {
"privPassword": "password",
"type": "read",
"username": "name",
"privType": "aes",
"authPassword": "password",
"authType": "sha1"},
"1": {
```

```
"privPassword": "password",
"type": "write",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"},
"2": {
"privPassword": "password",
"type": "trap",
"username": "name",
"privType": "none",
"authPassword": "password",
"authType": "none"}}}
}}
```

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

**Syslog**

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

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

**Admin**

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

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

### Locale

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

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

### Data Logging Interval

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

| | |
|---|---|
| **interval** | The interval in minutes for data logging |

### Aggregation

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

**enabled** Options are true or false, determines whether aggregation is enabled

**username** User name (in quotes) to be set array devices

**password** Password (in quotes) to set for array devices (null deletes password)

**Example 1**

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

```
{"conf":{
"system": {
"hostname": "hostname1"},
"network": {
"ethernet": {
"dhcpOn": false,
"address": {
"0": {"address": "10.20.30.40","prefix": 24}}}}
,
"network": {
"ethernet": {
"route": {
"0": {
"gateway": "10.20.30.254",
"prefix": 0,
"destination": "0.0.0.0"}}}}
,
"network": {
"ethernet": {
"dns": {
"0": {"address": "8.8.8.8"},
"1": {"address": "8.8.4.4"}}}}
,
"snmp": {
"v1v2cEnabled": true,
"port": 161,
"readCommunity": "public",
"writeCommunity": "private",
"trapCommunity": "private",
"target": {
"0": {
"port": 162,
"name": "10.20.30.60",
"trapVersion": "1"}}}
,
"locale": {
"defaultLang": "en",
"units": "metric"}
}}
```

**Example 2**

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

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

### Sensor Settings and Alarms

```
{"dev": {
    "0000000000000000": {
        "label": "PDU 22A",
        "type": "i03",
        "conf": {"outletControlEnabled": true},
        "outlet": {
            "0": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.25,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 1"
            },
            "1": {
                "poaAction": "last",
                "rebootHoldDelay": 10,
                "rebootDelay": 5,
                "poaDelay": 1.50,
                "onDelay": 5,
                "mode": "manual",
                "offDelay": 5,
                "label": "Outlet 2"
            }
        },
        "entity": {
            "total0": {"label": "Total"},
            "breaker0": {"label": "Circuit 1"},
            "breaker1": {"label": "Circuit 2"},
            "phase0": {"label": "Phase A"},
            "phase1": {"label": "Phase B"},
            "phase2": {"label": "Phase C"},
            "line3": {"label": "Neutral Line"}
        }
    }
},
"alarm": {
    "action": {
        "0": {
            "target": "trap0",
            "delay": 0,
            "repeat": 0
        },
        "1": {
            "target": "email0",
            "delay": 0,
            "repeat": 0
        }
   },
    "trigger": {
        "0": {
            "path": "0000000000000000/entity/phase0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 222.0,
            "tripDelay": 0,
            "clearDelay": 1,
            "latching": false,
            "selectedActions": ["0","1"]
        },
        "1": {
            "path": "0000000000000000/outlet/0/measurement/0",
            "severity": "alarm",
            "type": "low",
            "threshold": 55.0,
            "tripDelay": 2,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "2": {
            "path": "0000000000000000/entity/breaker0/measurement/4",
            "severity": "alarm",
            "type": "high",
            "threshold": 12.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        },
        "3": {
            "path": "0000000000000000/entity/total0/measurement/0",
            "severity": "alarm",
            "type": "high",
            "threshold": 7200.0,
            "tripDelay": 0,
            "clearDelay": 0,
            "latching": false,
            "selectedActions": ["0"]
        }
    }
}}
```

**0000000000000000** The device-id (found on the sensors>overview page) of the rPDU to be configured. If this device-id does not match any of the selected devices being provisioned, all selected devices will be provisioned. Setting device-id to 0000000000000000 ensures all selected devices are configured.

**label** The rPDU label (shown on the sensors>overview page)

**type** For setting alarms on the internal PDU measurements, the “type” must match the IMD being used on the PDU.

For setting alarms on external sensors, “type” must be the external sensor’s type. Valid values are “remotetemp”, “afht3”, “thd”, “t3hd”, “a2d”, “snt”, “snh”, “snd”.

If omitted, prevents any selected rPDUs being configured when the device-id does not match that of any rPDU.

**outletControlEnabled** Applies to outlet switched rPDUs only and determines whether it is possible to control outlets on an outlet switched rPDU. The value true allows outlets to be controlled, the value false prevents outlets from being controlled.

**outlet** The outlet section applies to outlet switched rPDUs only and defines settings for each rPDU outlet. Note that outlet numbering starts with 0 (rPDU outlet number 1). Individual outlets (or the entire Outlet section) can be omitted if these settings do not require change.

**poaAction** Defines the state the outlet will start when powered on ("on", "off" or "last").

**rebootHoldDelay** Time, in seconds, the unit waits after switching the outlet off, before switching an outlet back on during a reboot. Can be any whole number between 0 and 14400.

**rebootDelay** Time, in seconds, the unit waits before rebooting an outlet. Can be any whole number between 0 and 14400.

**poaDelay** Time, in seconds, the unit waits after being powered on before powering on the outlet. Can be any whole number between 0 and 14400.

**onDelay** Time, in seconds, the unit waits before switching an outlet on. Can be any whole number between 0 and 14400.

**mode** Should have the value "manual" for user-controlled outlets.

**offDelay** Time, in seconds, the unit waits before switching an outlet off. Can be any whole number between 0 and 14400.

**label** The outlet label.

**entity** The entity section is used to label non-outlet measurements on the sensors>overview page.

**total0 label** Label for the rPDU total on the sensors>overview page

**breaker0 label** Label for the first circuit (if present). Further circuits if present can be labelled using breaker1, breaker2 etc.

**phase0 label**

Label for the first phase. Further phases if present can be labelled using phase1 and phase2.

**line3 label**

Label for the neutral line.

**alarm**

The alarm section defines the methods that can be used to send alarms. Each method is numbered starting from 0 defines:

**target**

For SNMP trap alarm delivery the target can have the values "trap0", "trap1" etc. which refers to the first, second etc. SNMP traps defined on the System>SNMP page.

For email alarm delivery the target can have the values "email0", "email1" etc. which refers to the first, second etc. target email defined on the System>Email page.

Note that the target must not specifies SNMP traps or email targets that have not been configured.

**delay**

Determines how long this event must remain tripped before this action's firstvertical notification is sent.

**repeat**

Determines whether multiple notifications will be sent for this event action.

**trigger**

This section defines which alarms have been configured, starting with the first alarm which is numbered 0.

**Path**

Defines the measurement to be alarmed upon. The format of this field is:

"0000000000000000/entity/phase0/measurement/0" defines alarms for rPDU inlet phase measurements, where phase0 refers to the first rPDU input phase, phase1 refers to the second phase (if present) etc. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below:

0: Voltage

4: Current

8: Real power

9: Apparent power

10: Power Factor

11: Energy

14: Current crest factor

"0000000000000000/outlet/0/measurement/0" defines outlet alarms for rPDUs with outlet monitoring where the number immediately following outlet specifies the outlet number (starting at zero). The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below:

0: Voltage

4: Current

8: Real power

9: Apparent power

10: Power Factor

11: Energy

12: Balance

14: Current crest factor

"0000000000000000/entity/total0/measurement/0" defines alarms for rPDU phase total inlet measurements. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below:

0: Real power

1: Apparent power

2: Power Factor

3: Energy

"0000000000000000/entity/breaker0/measurement/4" defines alarms for rPDU circuit alarms where the first circuit is indicated by breaker0, second by breaker1 etc. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below:

4: Current

"0000000000000000/entity/line3/measurement/4" defines alarms for rPDU neutral current alarms. The number immediately following measurement indicates the type of measurement to be alarmed upon as defined below:

0: Current

**severity** Can be "warning" or "alarm" describing the severity of the generated alarm.

**type** Can be "high" or "low" which defines whether this is a high or low threshold.

**threshold** Threshold value which can be any number between -999.0 through 999.0. Neutral line current can be specified with up to two decimal places.

**tripDelay** The measurement must exceed the threshold for this many seconds before the event will be tripped, can be any whole number between 0 and 14400.

**clearDelay** The measurement must return to normal for this many seconds before the event will clear and reset. can be any whole number between 0 and 14400.

**latching** Can be true or false. If true, the event and its associated actions remain active until the event is acknowledged, even if the measurement subsequently returns to normal.

**selectedActions** Defines which actions defined above to use to send the alarm. Such as ["0","1"] defines actions 0 and 1 which are defined as actions using trap0 and email0 in the example above.

This page intentionally left blank

# Appendix E: API / CLI Error Codes

## E.1 Success

| Code | Explanation |
|---|---|
| Success | Operation has succeeded |

### Authentication Errors

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

### JSON Format Errors

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

### Path Errors

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

### Data Validation Errors

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

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

### Other Errors

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

### Data Consistency Errors

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

### Upload Errors

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

This page intentionally left blank

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

## F.1 Overview

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

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

## F.2 General Requirements and Notes

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

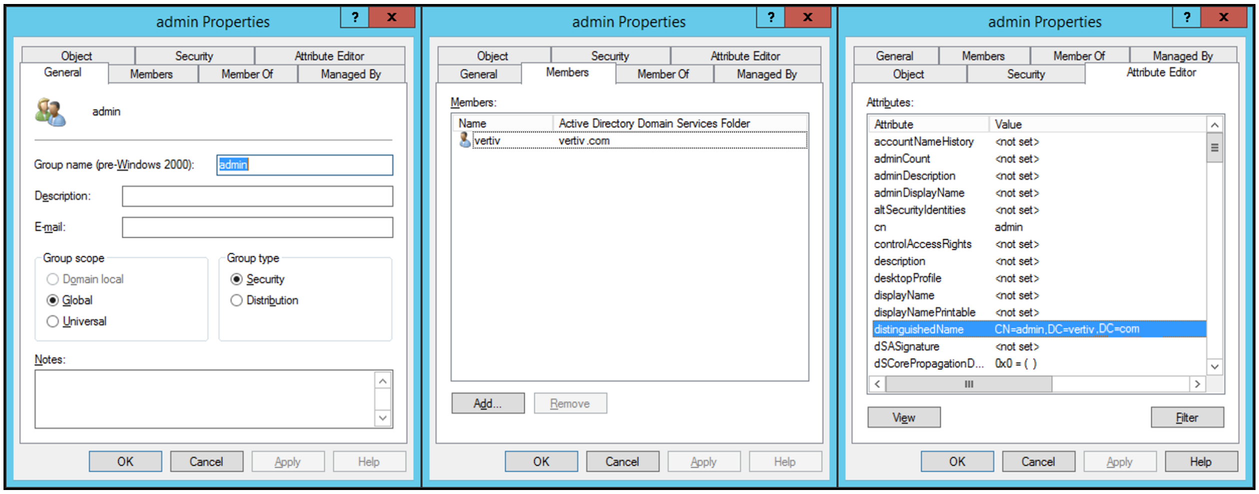
## F.3 Active Directory Configuration Procedure

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

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

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

### Figure F.1 Admin Properties Settings



admin

Group name (pre-Windows 2000): admin

Description:

E-mail:

Group scope

○ Domain local
● Global
○ Universal

Group type

● Security
○ Distribution

Notes:

Members:

| Name | Active Directory Domain Services Folder |
|---|---|
| vertiv | vertiv.com |

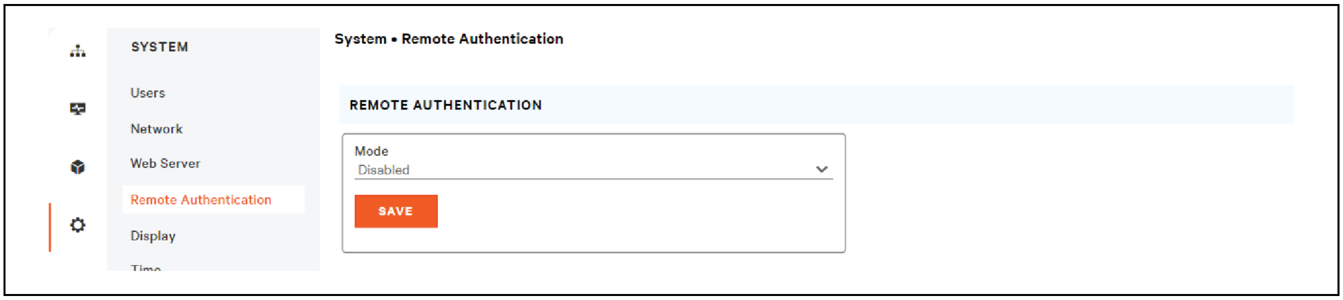
Attributes:

| Attribute | Value |
|---|---|
| accountNameHistory | <not set> |
| adminCount | <not set> |
| adminDescription | <not set> |
| adminDisplayName | <not set> |
| altSecurityIdentities | <not set> |
| cn | admin |
| controlAccessRights | <not set> |
| description | <not set> |
| desktopProfile | <not set> |
| displayName | <not set> |
| displayNamePrintable | <not set> |
| distinguishedName | CN=admin,DC=vertiv,DC=com |
| dSASignature | <not set> |
| dSCorePropagationD... | 0x0 = ( ) |

## F.4 IMD Configuration Procedure (Web Interface)

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

### Figure F.2 Remote Authentication



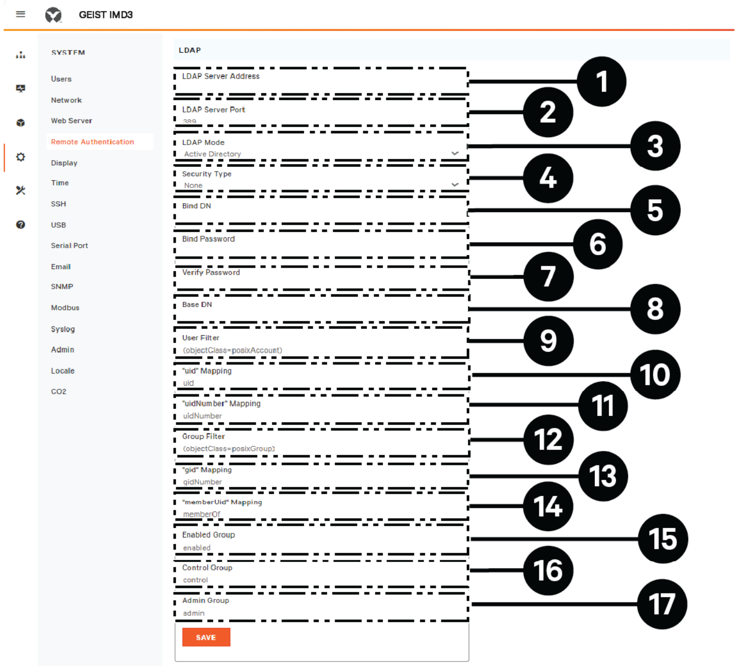
System • Remote Authentication

REMOTE AUTHENTICATION

Mode
Disabled

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

### Figure F.3 LDAP Setting



LDAP

LDAP Server Address

LDAP Server Port
389

LDAP Mode
Active Directory

Security Type
None

Bind DN

Bind Password

Verify 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

### Table F.1 LDAP Setting

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

**Table F.1 LDAP Setting (continued)**

| Item | Description |
|---|---|
| 10 | AD User Account Name Filter<br>samaccountname |
| 11 | "uidNumber" Mapping<br>uidNumber |
| 12 | AD Group ObjectClass Attribute Filter<br>(objectClass=group) |
| 13 | "gid" Mapping<br>gidNumber |
| 14 | Required Setting<br>memberOf |
| 15 | AD Security Group Map to Enabled Role<br>Must be in full DN path notation<br>CN=enabled, DC=vertiv, DC=com |
| 16 | AD Security Group Map to Control Role<br>Must be in full DN path notation<br>CN=control, DC=vertiv, DC=com |
| 17 | AD Security Group Map to Admin Role<br>Must be in full DN path notation<br>CN=admin, DC=vertiv, DC=com |

**NOTE: [1]Best practice is to reduce the scope of AD domain traversal to search for authenticated users. Try to avoid just specifying the base domain when there is a large and nested AD schema.**

- Ideal: OU=Enabled Users, OU=User Accounts, DC=vertiv, DC=com
- Not Ideal: DC=vertiv, DC=com

**NOTE: [2]StartTLS uses TCP port 389. It initially establishes the session unencrypted but will encrypt the session from that point forward ifthe LDAP_START_TLS_OID request is accepted by the Active Directory server.**

## Connect with Vertiv on Social Media

https://www.facebook.com/vertiv/

https://www.instagram.com/vertiv/

https://www.linkedin.com/company/vertiv/

https://www.x.com/Vertiv/

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