

3.5.16 Locale

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

3.5.17 Utilities

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

Aggregation

Change settings, as desired. (See [Aggregation](#) on page 67)

To change Aggregation setting:

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

Configuration Backup and Restore

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

Table 3.12 Backup and Restore Options

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

To save current configuration settings:

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

NOTE: Saving configuration does not require user authentication.

To restore a previous configuration setting:

1. Click *Backup File*.
2. Click *Choose File*.
3. Select the Backup File.
4. Click *Restore*.

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

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

Restore Defaults

Restore the default settings.

Table 3.13 Restore Default Options

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

To restore default settings:

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

Reboot

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

To reboot the operating system: Click *Reboot*.

NOTE: The power to connected devices is not affected.

Reboot I/O Boards

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

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

NOTE: The power to connected devices is not affected.

Firmware Updates

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

To update Firmware via Firmware Package File:

1. Click *Choose File* and select the .firmware file from the *Open* window.
2. Click *Submit*.
3. If a problem occurs, click *Revert Firmware*.

To update Firmware via a USB flash drive:

1. Download the latest firmware from <https://www.vertiv.com/en-us/support/software-download/power-distribution/geist-upgradeable-series-v5-firmware/> and unzip the folder.
2. Get a USB flash drive and format it as FAT32.

3. Create a directory on the USB flash drive called *FIRMWARE* (must be uppercase).
4. Open the unzipped firmware folder and copy the *.firmware* file.
5. Paste this file into the *FIRMWARE* folder on the flash drive.
6. Plug the USB flash drive into the PDU.

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

Factory Access

Provides information for technical support.

Table 3.14 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.

3.6 Provisioner Tab

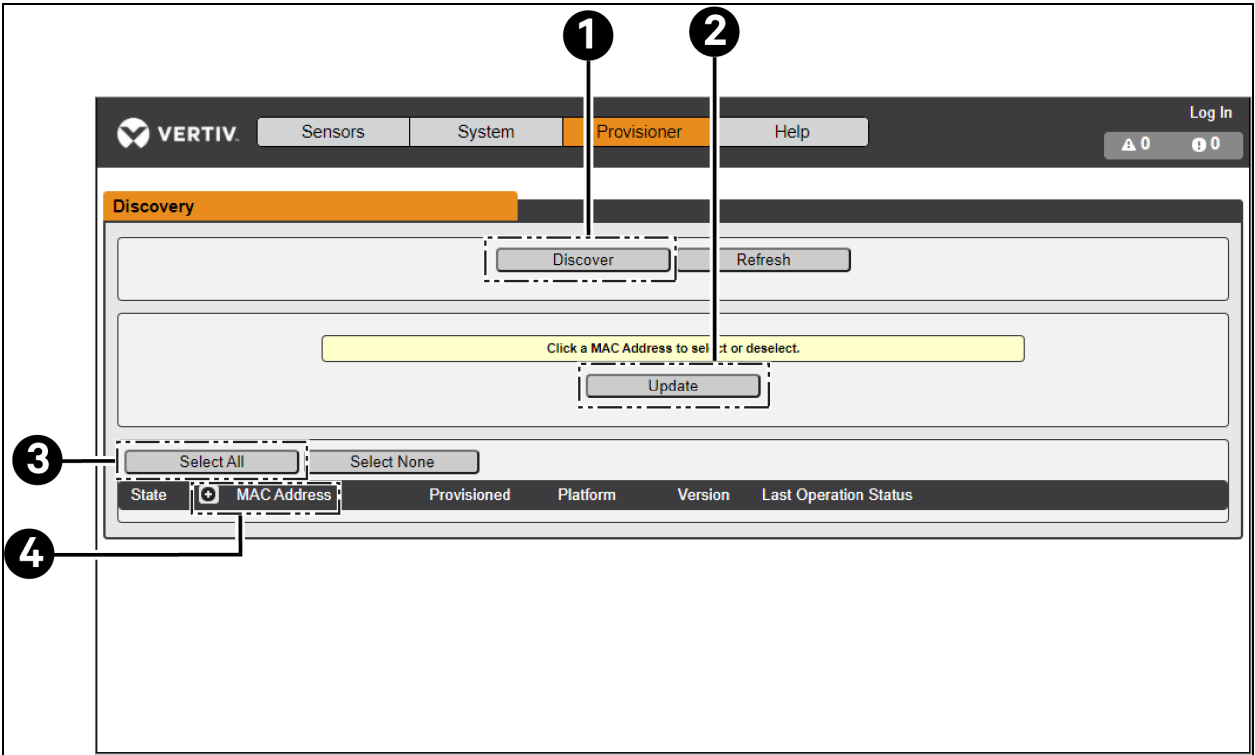
The Provisioner allows the user to discover locally connected Vertiv™ Geist™ rPDUs. The user can update their firmware and configure them by uploading a configuration settings file.

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

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

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

Figure 3.30 Provisioner Page



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

3.6.1 Discovery

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

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

3.6.2 File management

Firmware Files

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

Configuration Files

1. Click *Choose File* and select the .config file from the Open window.

2. Click Submit icon. Configuration file will be listed

Figure 3.31 File Management Page

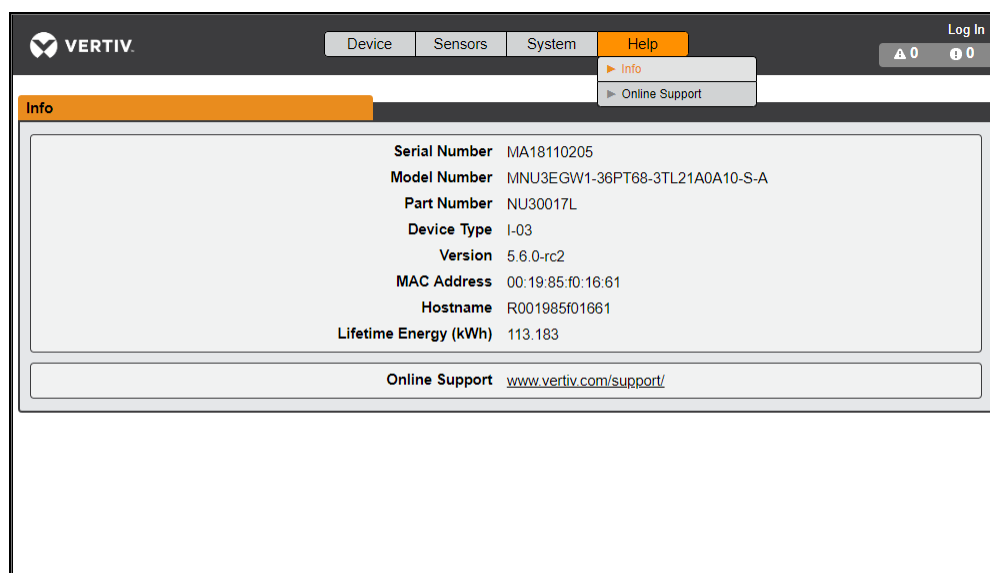
See [Provisioner - Format of the configuration settings file](#) on page 97 for examples of configuration setting files used by the Provisioner and the necessary format for the file.

3.7 Help Tab

Info Page

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

Figure 3.32 Info Page



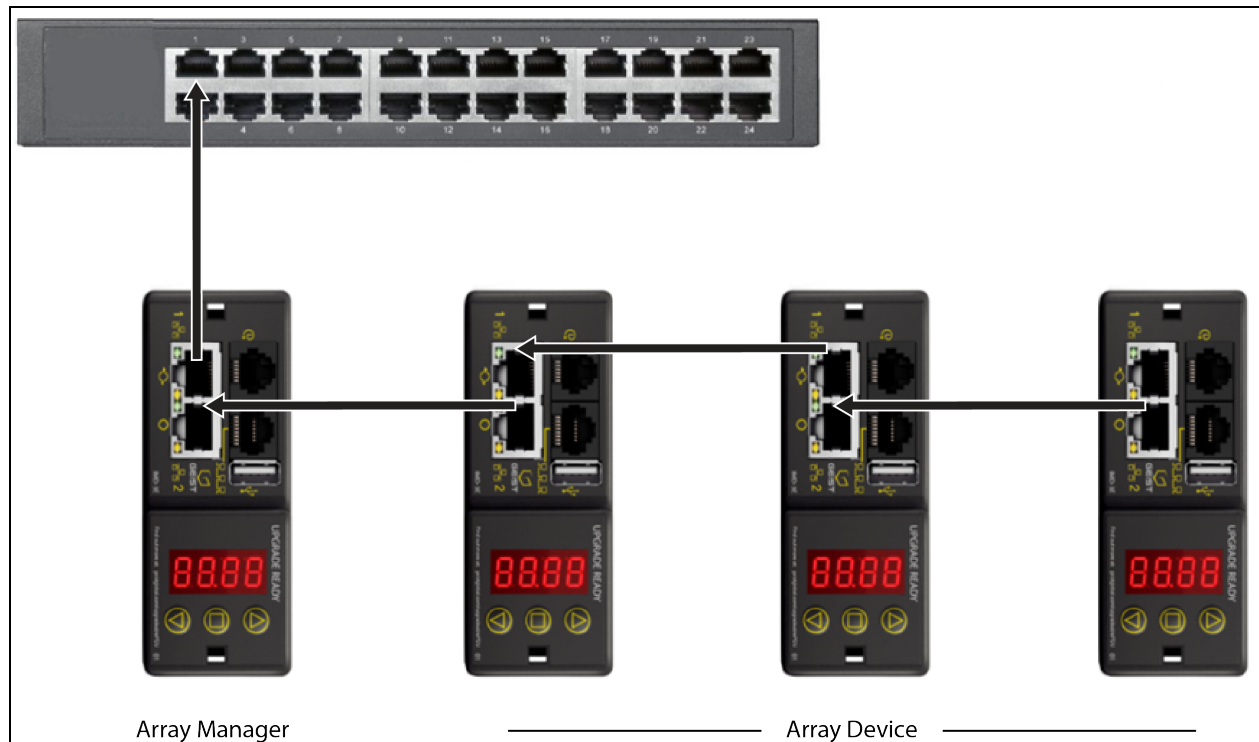
4 Vertiv™ Intelligence Director

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

4.1 Aggregation

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

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

Figure 4.1 Aggregation

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

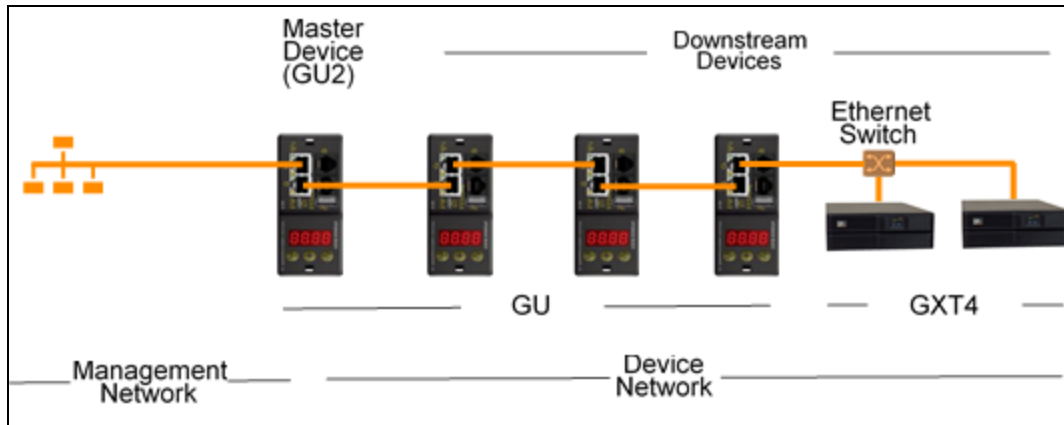
- Create groups of Geist™ rPDU outlets spanning one or more Geist™ rPDUs.
- Report on total power and energy for the outlet group (with Geist™ rPDUs that report per outlet measurements).
- Provide the ability for power off, power on or power cycle the group of outlets with a single command (with Geist™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

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

4.2 Array Manager

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

Figure 4.2 Sample Configuration



If you wish to use an IMD-02X or IMD-02E equipped rPDU as an array manager, you must first upgrade it to an IMD-3E-S or IMD-3E-G.

4.3 Network Configuration

In the initial release of aggregation, array devices are defined as Geist™ rPDUs within the Geist™ GU1 and GU2 product platforms as well as Vertiv™ MPH2 and MPX rack PDUs, Vertiv™ GXT4, GXT5, PSI5, EXM, APM and ITA2 UPS, Vertiv™ CRV row cooling and USB-connected Vertiv™ VRC cooling.. Each array manager can support up to 49 array devices, so the number of managers depends on the overall size of the installation and the preferred network architecture.

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

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

To commission the array manager:

1. Use the top drop-down menu to navigate to *System>Locale*.
2. Select the appropriate Default Language and Temperature Units from the drop-down menus. These settings are pushed to the array devices in its network.
3. Browse to *System>Network*. In Protocol IPv6, choose *Enabled* from the drop-down menu.
4. Browse to *System>Utilities*. Change the settings as desired.
 - a. **Aggregation:** Choose *Enabled* from the drop-down menu.
 - b. **Array device Username:** Defines the username configured on all array devices.
 - c. **Array device Password:** Defines the password configured on all array devices.
5. Enter the new password, verify the password and click *OK*.

When configuring Aggregation, ensure the Managed Device Password meets all array device password complexity rules. Unless changed by the user, these require a minimum password length of 8 characters with rPDUs running 5.9.0 or later firmware.

6. Click *Submit*. If Aggregation is enabled, the Device Tab appears next to the Sensors Tab on the top navigation bar.

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

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

4.3.1 Array devices

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

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

To set up a new installation with one array manager:

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

To set up an existing installation with one array manager:

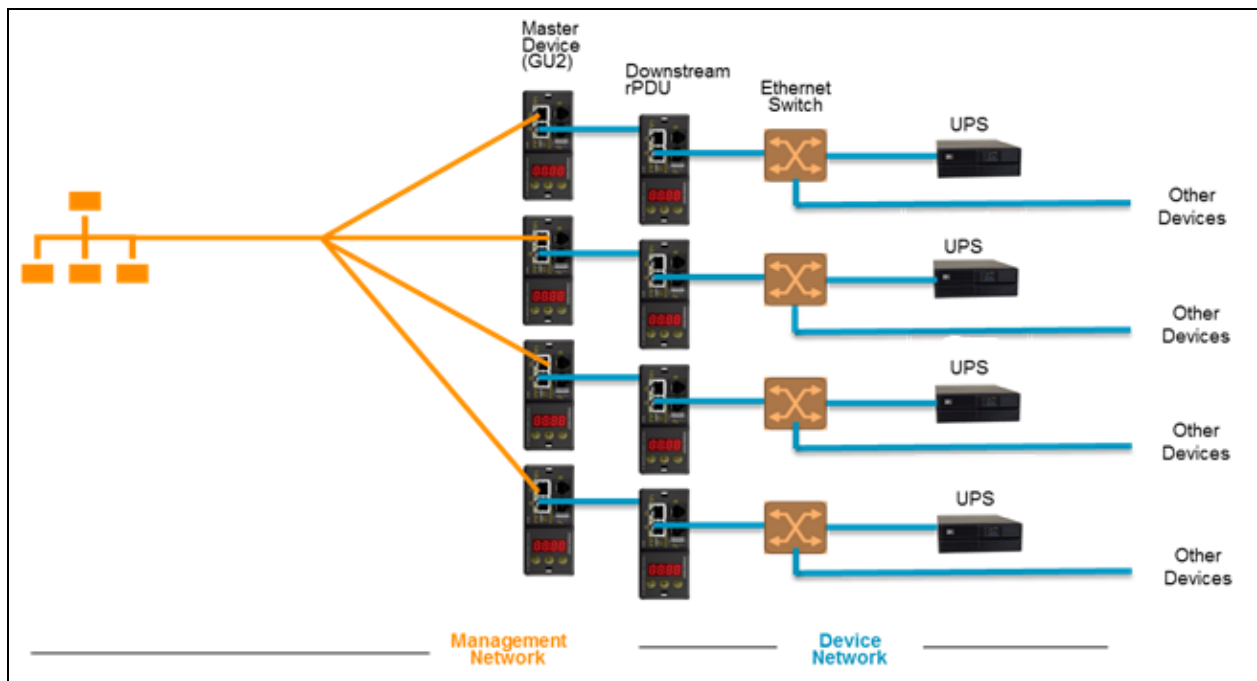
NOTE: Use the following instructions if existing Geist™ rPDUs are connected in a daisy-chain.

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

Multiple Array Managers

For installations with multiple array managers, keep in mind that each device network must operate as a stand-alone, isolated network. Consider a 200 rPDU example, represented in the [Sample Network Configuration](#) below. 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 4.3 Sample Network Configuration



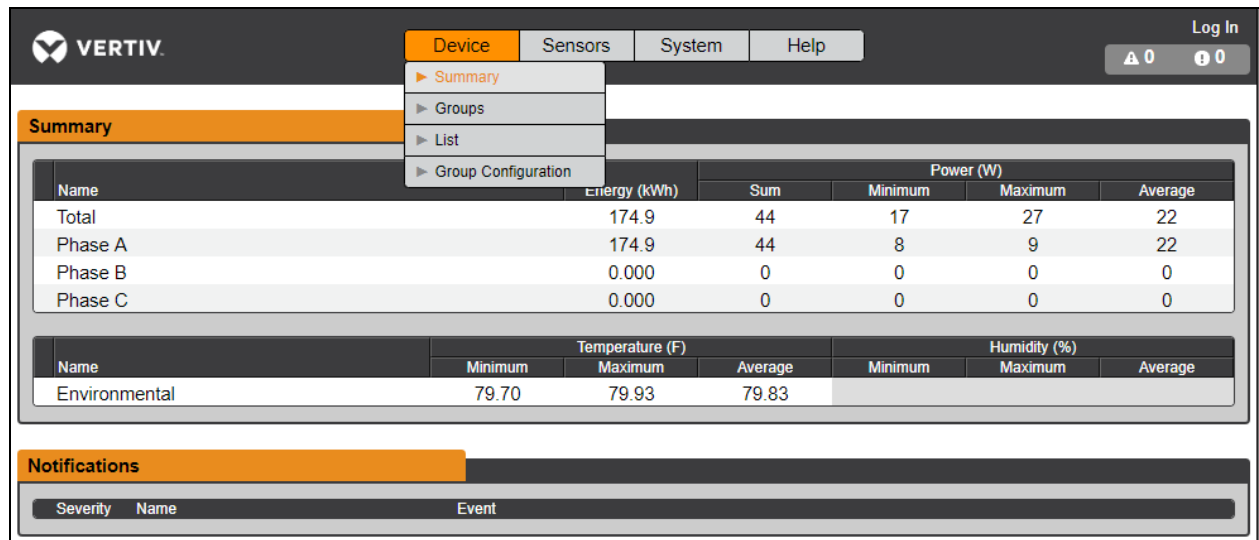
NOTE: A device network Ethernet switch will only be required when connecting more than one single network port device to the end of a rPDU daisy chain or when not using daisy chained connections.

4.4 Views

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

- Summary
- Groups
- List
- Group Configuration

Figure 4.4 Device Tab



4.4.1 Summary

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

Rack PDUs

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

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

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

UPS

The UPS network is summarized by the following data points:

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

Environmental (Sensors)

The Environmental category is summarized by the following data points:

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

- **Temperature Minimum:** The lowest temperature within the device network.
- **Temperature Maximum:** The highest temperature within the device network.
- **Temperature Average:** The average temperature within the device network.
- **Humidity Minimum:** The lowest humidity within the device network.
- **Humidity Maximum:** The highest humidity within the device network.
- **Humidity Average:** The average humidity within the device network.

Thermal Cooling

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

Notifications

Notifications shows outstanding alarms from devices in the device network.

4.4.2 Groups

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

Group rPDU

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

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

Group rPDU Outlet

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

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

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

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

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

To change outlet group operation:

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

For outlets currently Off, reboot turns the outlets On.

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

Group UPS

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

Group Environmental

- **Temperature Minimum:** The lowest temperature within the group.
- **Temperature Maximum:** The highest temperature within the group.
- **Temperature Average:** The average temperature within the group.
- **Humidity Minimum:** The lowest humidity within the group.
- **Humidity Maximum:** The highest humidity within the group.
- **Humidity Average:** The average humidity within the group.

Group Thermal Cooling

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

4.4.3 List

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

The inventory is subdivided into the following categories:

Rack PDUs

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

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

UPS

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

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

- **Charge:** UPS battery charge.

ENV (Environmental Sensors)

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

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

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

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

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

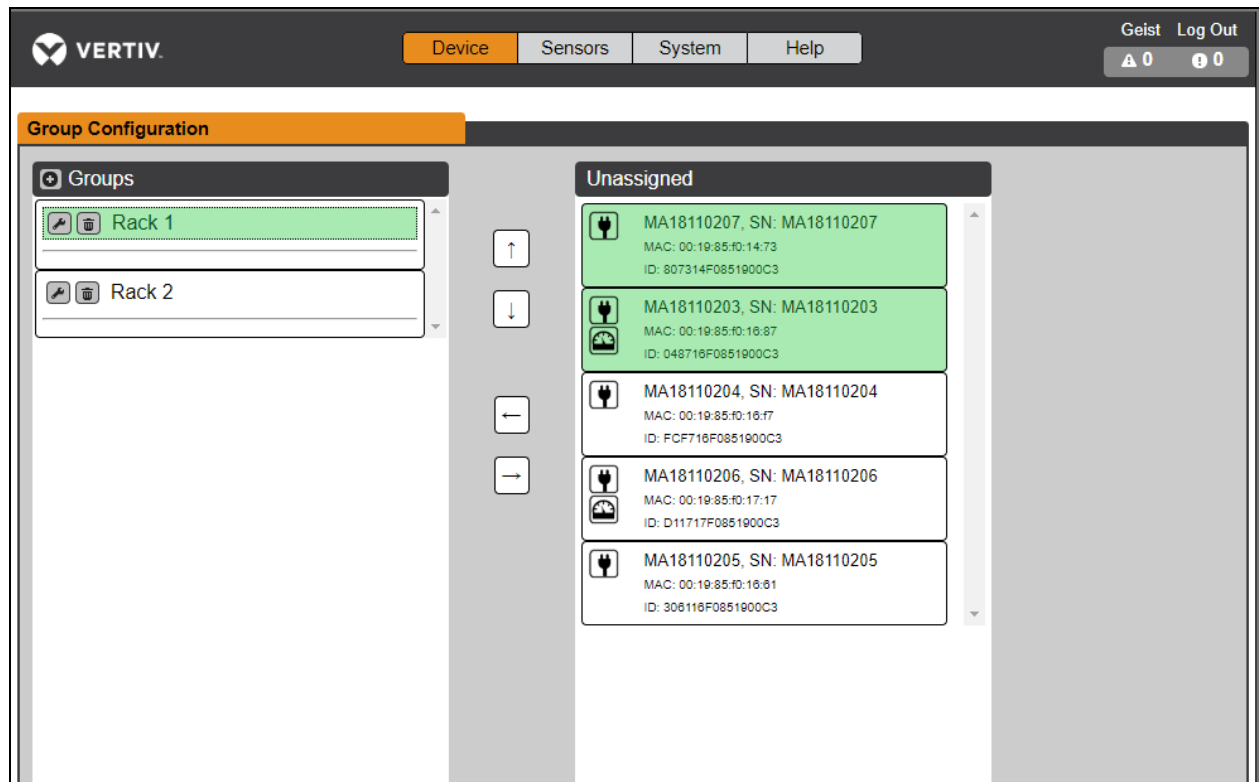
Thermal Cooling

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

4.4.4 Group configuration

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

Figure 4.5 Group Configuration



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

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

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

To create a new group:

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

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

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

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

To remove devices from a group:

Highlight the devices and click the *Right Arrow*.

To delete a group:

Click the *Trash* icon next to the group name.

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

4.5 Interfaces

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

To access the Array Device User Interface:

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

-or-

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

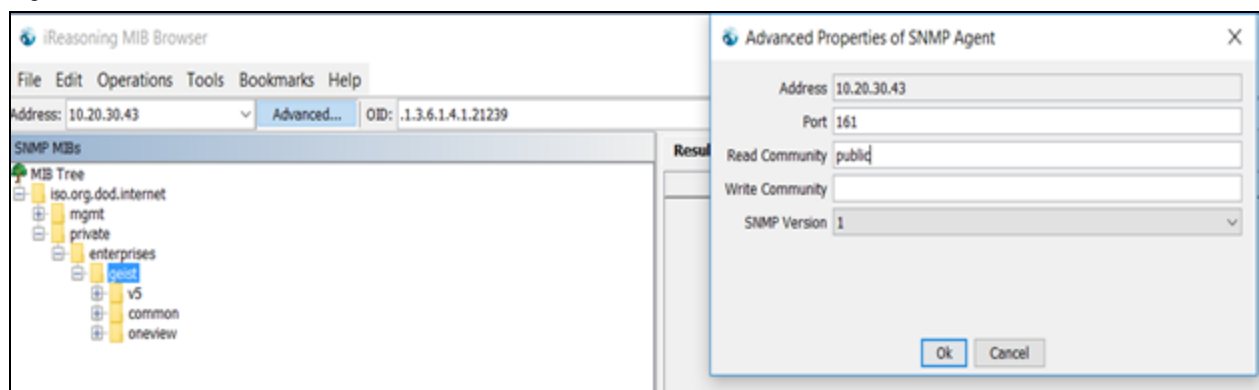
To access Array Device SNMP Data:

SNMP Data is available using port-mapped access through the array manager device IP address using the Geist™_v5 MIB. The MIB file is downloadable from the array manager SNMP page.

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

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

Figure 4.6 MIB Browser



4.5.1 Group SNMP data

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

- **v5:** Contains data points for the individual Master Geist™ rPDU.

- **Oneview:** Contains data points for aggregated data across all array devices.

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

This page intentionally left blank

Appendices

Appendix A: Technical Support

A.1 Resetting an Vertiv™ Geist™ rPDU

If a Geist™ rPDU loses communication, the processor may be manually rebooted without affecting power to the outlets. Pressing the reboot button on the face of the IMD will reboot the processor. The web interface will remain offline during boot-up. For more information, see [Interchangeable Monitoring Device](#) on page 21

A.2 Service and Maintenance

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

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

A.3 More Technical Support

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

Americas

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

Europe and Middle East

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

Asia

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

A.4 Using Microsoft Exchange as an SMTP Server

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

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

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

<http://technet.microsoft.com/en-us/library/aa997285.aspx>

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

<http://technet.microsoft.com/en-us/library/dd277329.aspx>

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

To re-enable the AUTH LOGIN method:

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

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

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

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

Appendix B: Visible Light Communication (VLC)

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

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

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



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

To enable VLC:

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

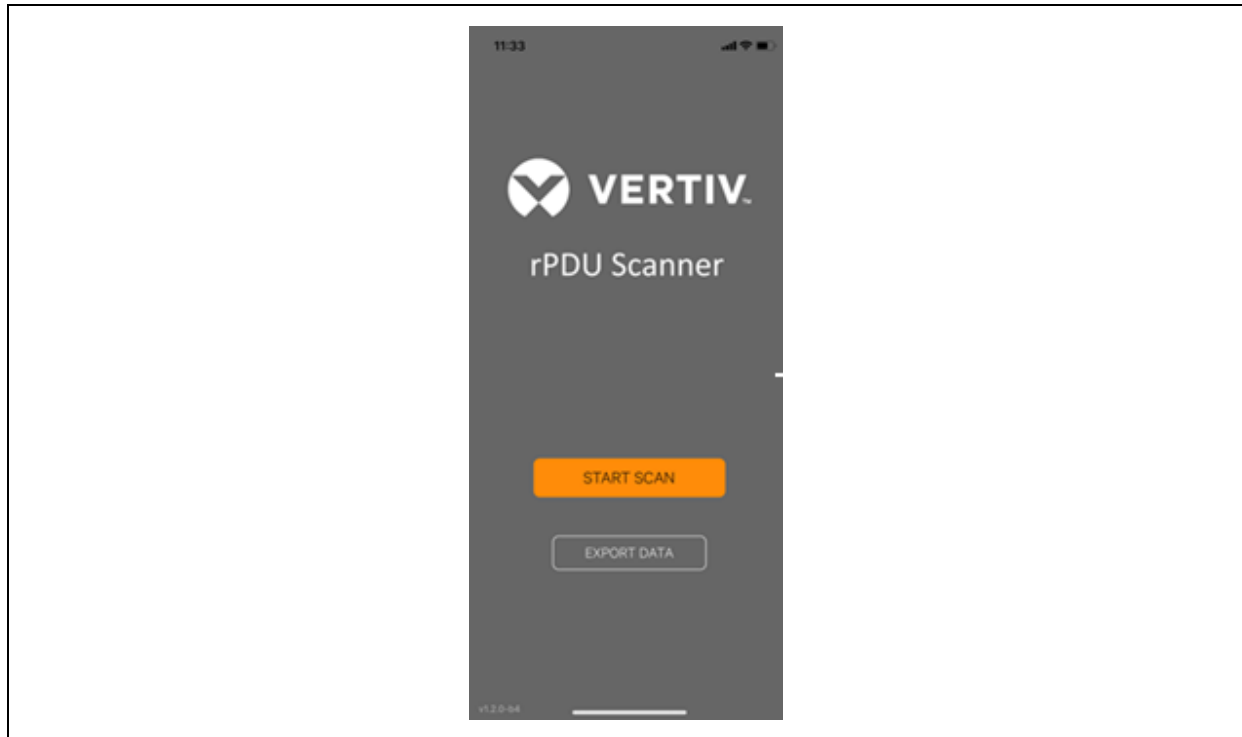
NOTE: With the release of firmware Version 3.3.0, Vertiv™ has added support for the VLC feature to all standard Metered and Monitored Upgradeable products, as well as a significant majority of its engineered-to-order range. Certain custom models of Upgradeable PDUs may not have VLC support within the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

Appendix C: Vertiv™ Mobile App

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

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

Figure C.1 Vertiv™ Mobile App Home Screen



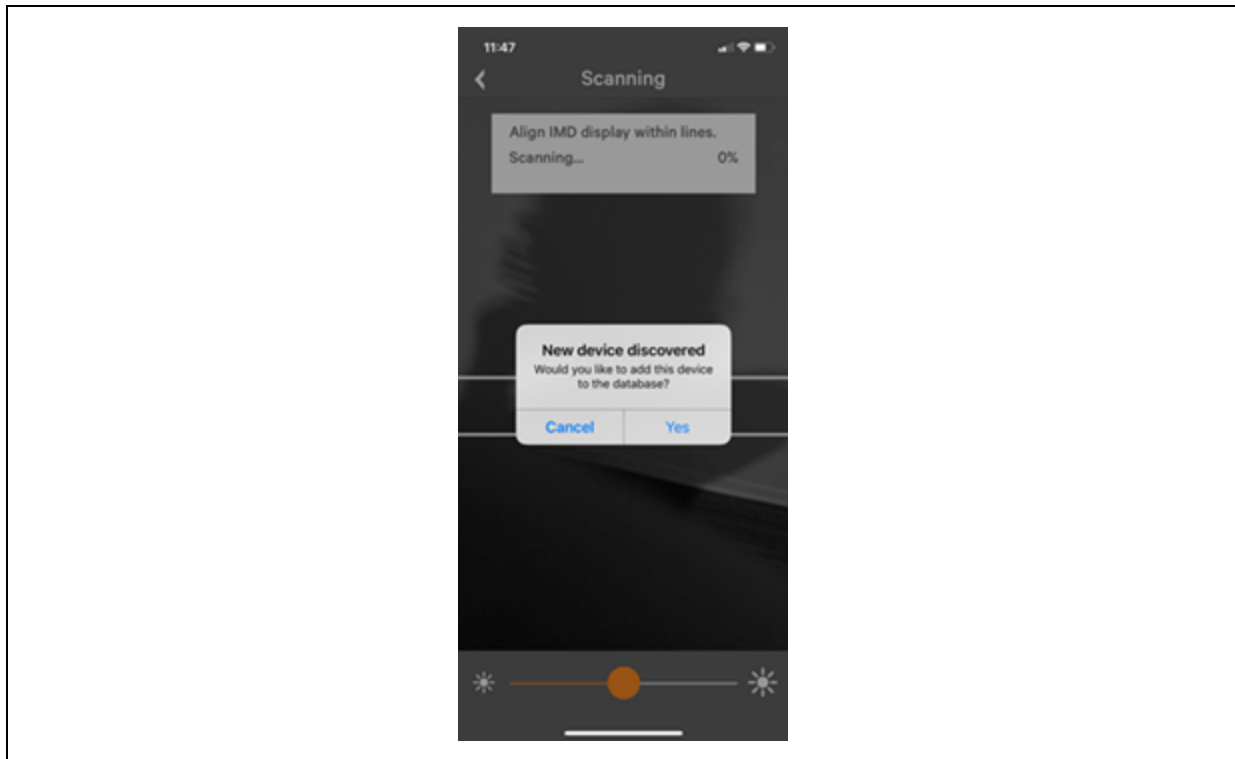
To scan a Geist™ rPDU

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

Figure C.2 Vertiv™ Mobile App Scanning Screen

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

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

Figure C.3 Vertiv™ Mobile App New Device Screen

C.1 Scanning Tips

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

Proper capture methods

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

Improper capture methods

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

C.2 Failure Modes and Errors

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

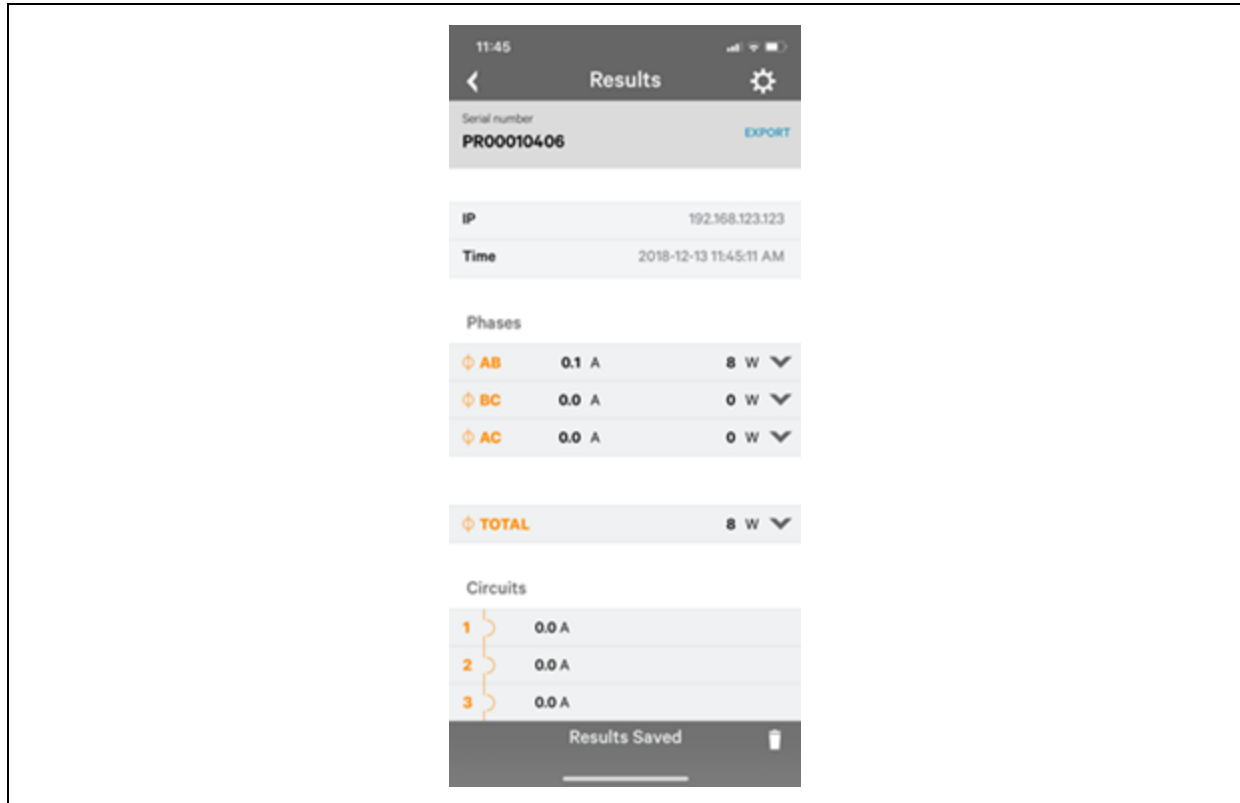
- **Scan failed:** Incorrect set of configuration.
- **Scan failed:** Incorrect data sequence.
- **Scan failed:** Adjust your position or the exposure and try again.

Press *Cancel* to return to the Home screen or *Retry* to return to the Scan page.

C.3 Readings

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

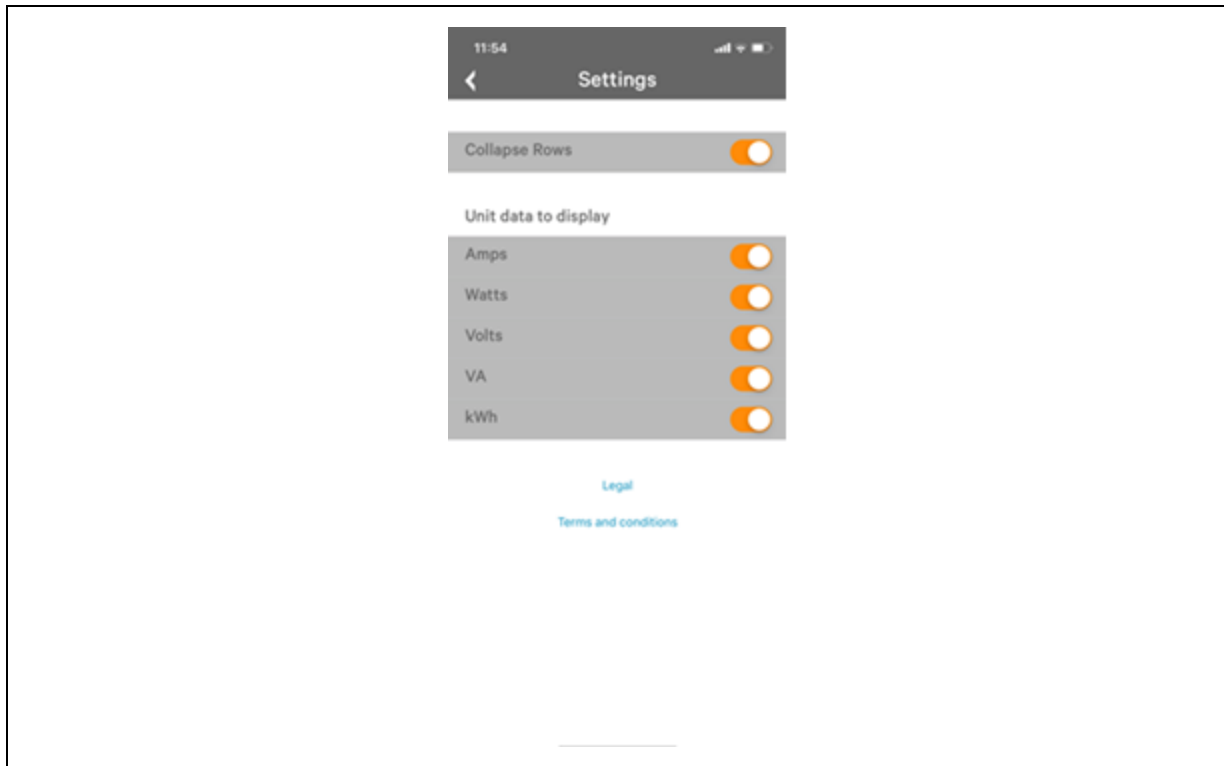
Figure C.4 Vertiv™ Mobile App Readings Screen



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

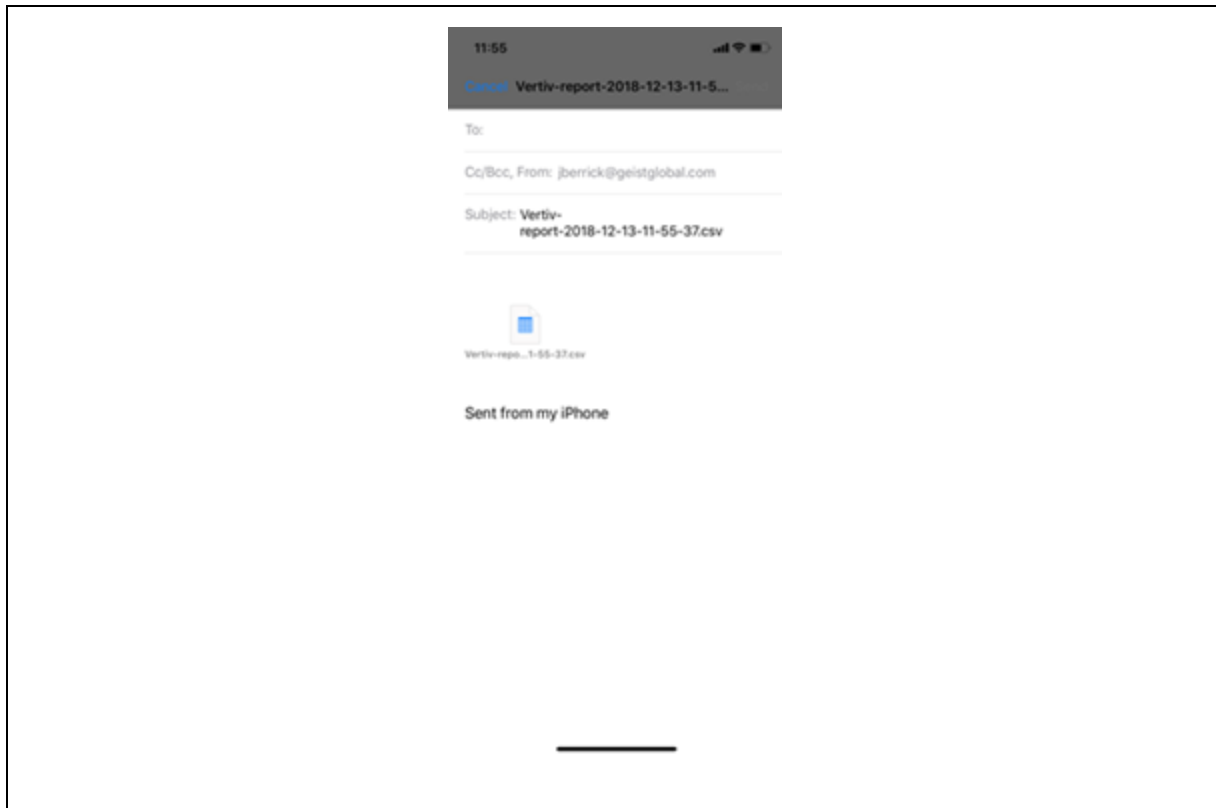
Pressing the *Settings* icon enables the user to customized the data that is displayed in the scan results.

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

Figure C.5 Vertiv™ Mobile App Settings Screen

C.4 Export

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

Figure C.6 Vertiv™ Mobile App Export Screen

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

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

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

The Geist™ rPDU Configuration Data includes:

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

The Power Data includes:

- Power Readings
- Totals

Table C.1 Geist™ rPDU Configuration Data

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

Table C.2 Power Data

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

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

Table C.3 Breakers/Circuits

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

Table C.4 Totals

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

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

Appendix D: Available Sensors

D.1 Remote Sensors

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

D.2 Analog I/O Sensors

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

D.3 Liebert® Integrated and Modular Sensors

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

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

D.4 Connecting Remote Sensors

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

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

Appendix E: TP-Link Wireless USB adapters

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

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

This page intentionally left blank

Appendix F: Outlet LEDs

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

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

Table F.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 F.2 LED Status Description

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

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

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

Error Code

LEDs illuminate in Solid Amber during the following:

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

Appendix G: IMD Display Codes

Table G.1 IMD Display Codes

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

This page intentionally left blank

Appendix H: Provisioner - Format of the configuration settings file

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

1. In the examples below, the text in blue can be copied to a text file and updated as required. The text file can then be uploaded to the provisioning tool.
2. When editing configuration files, use a text editor such as notepad which can save files in .txt format.
3. The indentations shown in the examples can be omitted.
4. Ensure the correct double quote is used when editing configuration.
5. If a setting is omitted from the settings file, the value of that setting will remain unchanged.
6. When configuring a previously unconfigured (i.e. factory fresh) Geist™ rPDU, the first configuration setting should be the definition of an admin user, See [Local Users](#) below .
7. To combine several settings (other than local users) into one file (see also [Example 1](#) on page 108 at the end of this document):
 - Append together the required settings into one file
 - Delete all occurrences of `{ "conf": {` except for the first line of the file
 - Replace all lines that contain only `}}` by a `,` (comma) except for the last line of the file
8. If combining local user settings with other settings in one file, please refer to [Example 2](#) on page 109 at the end of this document.
9. After selecting Provisioner>Discovery>Update, enter the user name and password only when configuring previously configured Geist™ rPDUs (the user name and password being that of the Geist™ rPDUs being provisioned). Do not enter a user and password when configuring factory fresh units (identified by Provisioned attribute equalling False).

Local Users

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

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

LDAP

```

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

```

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

```
{
  "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 $2 * (\text{helloTime} + 1)$
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 $(\text{maxAge} / 2) + 1$

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

USB

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

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

Serial Port

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

baudRate Baud rate, options are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200

dataBits Number of bits of data in one frame, options 7 and 8

enabled Options are true or false, enables or disabled the serial CLI on a device

parity Parity bit type used in the frame, options "none", "even" and "odd"

stopBits Number of stop bits used to terminate each frame, options 1 and 2

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": "000000000000000/outlet/0/measurement/0",
  "severity": "alarm",
  "type": "low",
  "threshold": 55.0,
  "tripDelay": 2,
  "clearDelay": 0,
  "latching": false,
  "selectedActions": ["0"]
},
"2": {
  "path": "000000000000000/entity/breaker0/measurement/4",
  "severity": "alarm",
  "type": "high",
  "threshold": 12.0,
  "tripDelay": 0,
  "clearDelay": 0,
  "latching": false,
  "selectedActions": ["0"]
},
"3": {
  "path": "000000000000000/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	Must have the value "i03". 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 use-controlled outlets.
offDelay	Time, in seconds, the unit waits before switching an outlet off. Can be any whole number between 0 and 14400.
label	The outlet label.
entity	The entity section is used to label non-outlet measurements on the sensors>overview page.
total0 label	Label for the 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: For SNMP trap alarm delivery the target can have the values "trap0", "trap1" etc. which refers to the first, second etc. SNMP traps defined on the System>SNMP page.
target	For email alarm delivery the target can have the values "email0", "email1" etc. which refers to the first, second etc. target email defined on the System>Email page. Note that the target must not specifies SNMP traps or email targets that have not been configured.
delay	Determines how long this event must remain tripped before this action's first vertical 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 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 alarmed 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 alarmed 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 alarmed 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 alarmed 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. E.g. ["0","1"] defines actions 0 and 1 which are defined as actions using trap0 and email0 in the example above.

This page intentionally left blank

Appendix I: Provisioner Error Codes

I.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, e.g. in the HTTP body and query string

Path Errors

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

Data Validation 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
OneView missing credentials	Enabling OneView requires that a OneView 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 J: An Example of Configuring LDAP for Active Directory Credentials

J.1 Overview

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

J.2 General Requirements and Notes

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

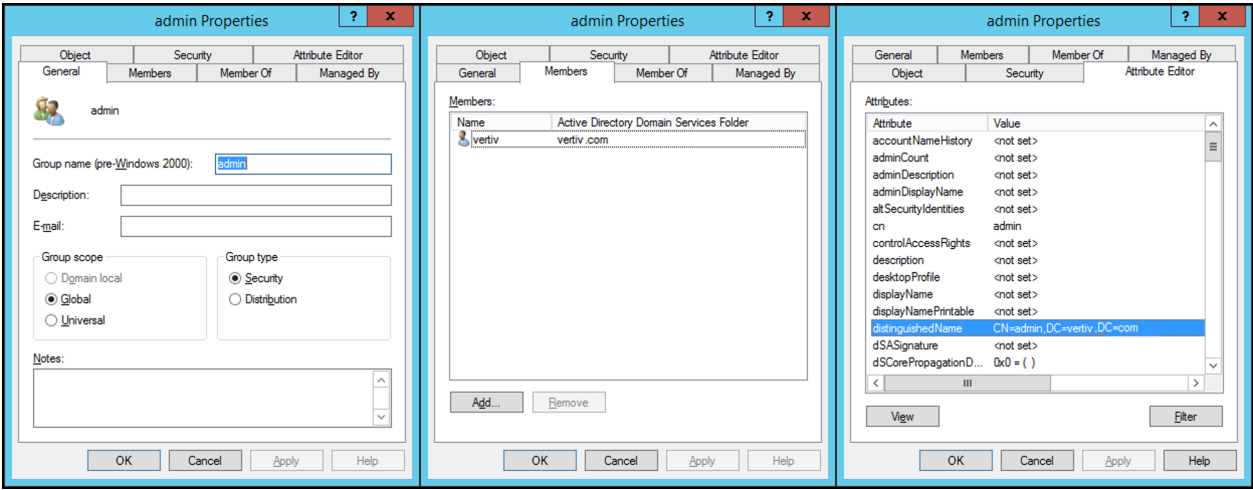
J.3 Active Directory Configuration Procedure

- 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.

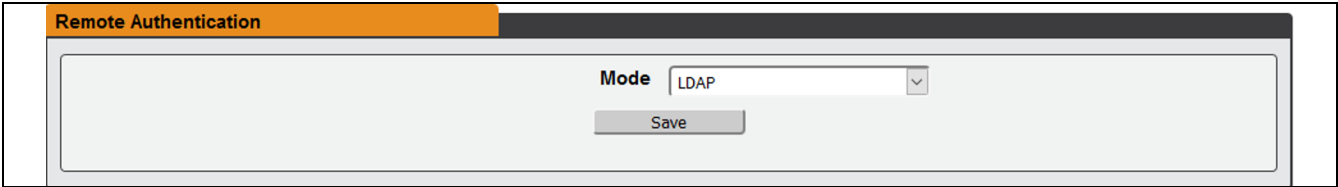
Figure J.1 Admin Properties Settings



J.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 J.2 Remote Authentication



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

Figure J.3 LDAP Setting

The image shows a web-based configuration interface for LDAP settings. It consists of a list of fields with labels on the left and input areas on the right. Numbered callouts (1-13) point to specific fields: 1 points to 'LDAP Server Address', 2 to 'LDAP Server Port', 3 to 'LDAP Mode' (set to 'Active Directory'), 4 to 'Security Type' (set to 'None'), 5 to 'Bind Password' (showing 'Password Set...'), 6 to 'Base DN', 7 to 'User Filter', 8 to '"uid" Mapping', 9 to 'Group Filter', 10 to '"gid" Mapping' (set to 'gidNumber'), 11 to '"memberUid" Mapping' (set to 'memberOf'), 12 to 'Enabled Group', and 13 to 'Admin Group'. A 'Save' button is at the bottom.

Item	Description
1	LDAP Server Address
2	LDAP Server Port
3	LDAP Mode (Active Directory)
4	Security Type (None)
5	Bind Password (Password Set...)
6	Base DN
7	User Filter
8	"uid" Mapping
9	Group Filter
10	"gid" Mapping (gidNumber)
11	"memberUid" Mapping (memberOf)
12	Enabled Group
13	Admin Group

Table J.1 LDAP Setting

Item	Description
1	Active Directory Server's IP Address
2	Active Directory TCP Port ² 389 - Non SSL 636 - SSL
3	Active Directory Security ² None - SSL - StartTLS
4	AD Account Used to Bind to AD Server Must be in full DN path notation CN=adbindacct,CN=Users,DC=vertiv,DC=com Account password should not expire
5	Set AD Bind Account Password
6	Base Domain Path to Search AD Users ¹ Must be in full DN path notation

Table J.1 LDAP Setting (continued)

Item	Description
	DC=vertiv,DC=com
7	AD User ObjectClass Attribute Filter (objectClass=user)
8	AD User Account Name Filter samaccountname
9	AD Group ObjectClass Attribute Filter (objectClass=group)
10	Required Setting memberOf
11	AD Security Group Map to Enabled Role Must be in full DN path notation CN=enabled,DC=vertiv,DC=com
12	AD Security Group Map to Control Role Must be in full DN path notation CN=control,DC=vertiv,DC=com
13	AD Security Group Map to Admin Role Must be in full DN path notation CN=admin,DC=vertiv,DC=com
NOTE: ¹Best 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: ²StartTLS uses TCP port 389. It initially establishes the session unencrypted but will encrypt the session from that point forward if the LDAP_START_TLS_OID request is accepted by the Active Directory server.	

Connect with Vertiv on Social Media



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



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



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



<https://www.twitter.com/Vertiv/>



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

© 2022 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice.

VM1221/SL-70567_REV10_10-22