Digital Services Connectivity

Connecting Devices Via the Vertiv Services Gateway and Direct IoT

Technical Note

JUNE 2026

Technical Note Section Outline

1. Overview

This document explains the onboarding process for customers to connect devices to Vertiv's Digital Service for monitoring. This process begins when the customer has selected the desired offering and the offering contract has been signed. Onboarding consists of seven phases: Connection Type Selection, Information Gathering, Data Entry and Pre-Configuration, Firewall Exceptions, Vertiv Services Gateway Shipping and Installation, Device Configuration, and Verification. During these phases, both the customer and Vertiv must fulfill their specified responsibilities to ensure the devices are configured and connected correctly. For more information, please refer to the subsequent sections that describe each phase.

2. Connection Type Selection

Two options are available for connecting to Vertiv's Digital Service:

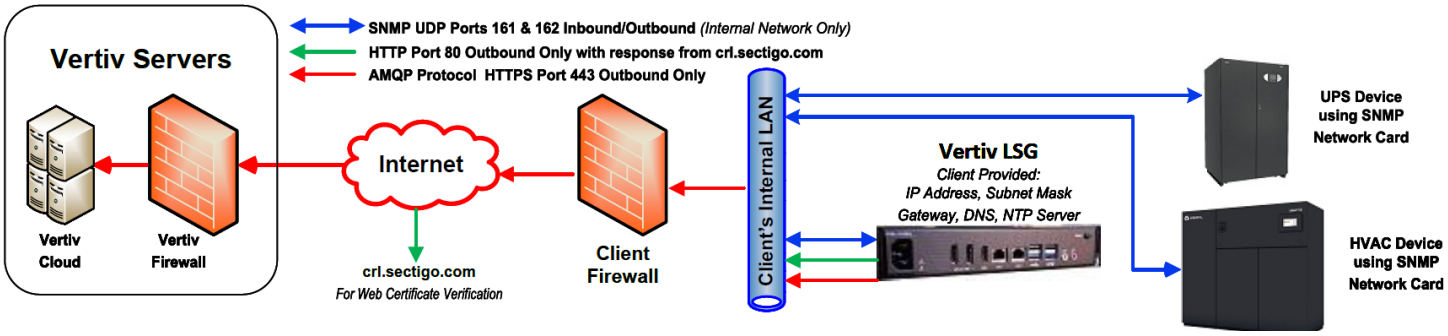
1. **Vertiv Services Gateway:** Ideal for customers who will permit SNMP v1/2/3 traffic on their internal network and require only a single point of communication through their network firewall to the Vertiv Cloud. SNMP v3 is the default communication method for devices connecting via the Vertiv Services Gateway.

   The gateway operates as an aggregator for all devices being monitored. To achieve this functionality, the gateway utilizes the following protocols:

   - **SNMP v1/2/3 protocol on UDP port 161**: Used to send a request for information to the SNMP agent via the SNMP manager.
   - **SNMP v1/2/3 protocol on UDP port 162**: Used to send trap notifications by the SNMP agent to the SNMP manager.
   - **AMQP protocol via TLS 1.2 on HTTPS port 443**: Used to encrypt and transmit data to the Vertiv Cloud.

   The gateway can be installed as a rack-mounted appliance or on a Windows 2019 Server or later. For additional technical information, please refer to the Vertiv Services Gateway Data Sheet Version 4 on this webpage: Life™ Services - Remote Monitoring| Vertiv Maintenance Services.

Sample Remote Monitoring via Vertiv™ LSG

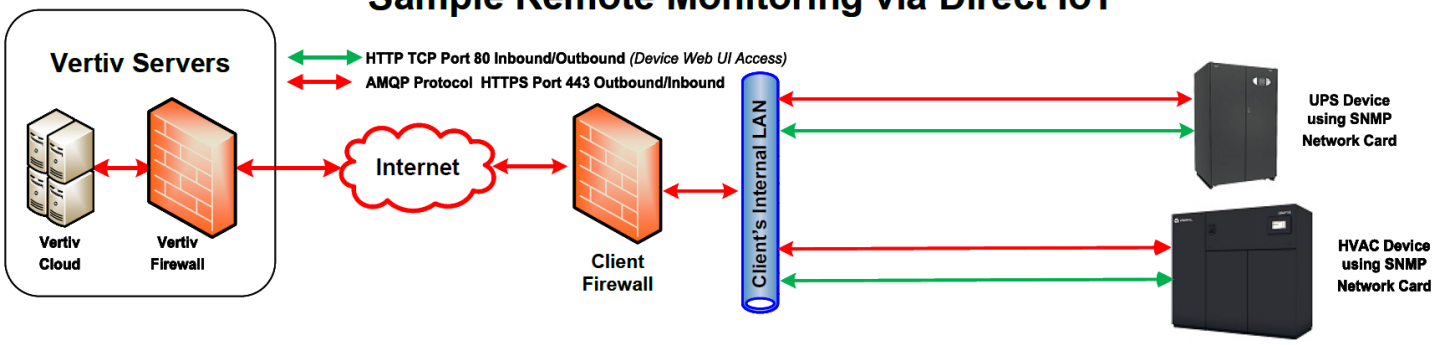


2. **Direct IoT:** Ideal for customers that will not permit SNMP v1/2 traffic on their internal network and require only one or two devices to be monitored on remote sites.

   Direct IoT is a communication protocol within the monitored device's network card. It communicates directly through the customer's Internet firewall to the Vertiv Cloud using the AMQP Protocol via TLS 1.2 on HTTPS port 443.

   NOTE: This option is only available for devices equipped with either the Vertiv™ Liebert® IntelliSlot™ Unity Communications Card or the Vertiv™ Liebert® IntelliSlot™ RDU Communications Card.

Sample Remote Monitoring via Direct IoT



3. Information Gathering

After selecting a connection option, the customer must provide Vertiv with the following items:

- A list of all sites and street addresses where the monitored devices and Vertiv Services Gateway are located.
- A call and email escalation list of all individuals in the customer's organization that are to be contacted in the event of an alarm, and the order in which they are to be contacted.
- Any information required for network configurations. The network requirements for the Vertiv Services Gateway and direct IoT options are listed below.

Vertiv Services Gateway Appliance Requirements

For Vertiv to properly pre-configure and ship the gateway, the customer must provide the following:

Device Information

- IP Address
- Subnet Mask
- Gateway
- Primary DNS
- Secondary DNS (Optional)
- Primary NTP
- Secondary NTP (Optional)
- Device Name
- Vertiv Services Gateway Site Location

Shipping Information

- Attn
- Address 1
- Address 2
- City, State, Postal Code

Vertiv Services Gateway Windows Server Requirements

To install the gateway software, internet access and a configured Windows server is required. The server should meet the following minimum requirements:

Minimum Recommended Server Requirements

- Windows Server 2019 or later
- Processor: 2.8GHz 64-bit, dual processors
- RAM: 16GB
- Disk Space: 30GB allocated exclusively for the Vertiv Services Gateway - not including any space required by the operating system
- Network Adaptor: An Ethernet adapter capable of at least gigabit throughput
- Installed on C: Drive

NOTE: No other SNMP service or program that uses SNMP to monitor the Windows server can be installed on the server, as they will conflict with Vertiv Digital Services.

Vertiv Service Gateway Device Requirements

For devices that will be monitored by Vertiv, the customer must provide the following:

Device Information

- IP Address
- Subnet Mask
- Gateway
- Primary DNS
- Secondary DNS (Optional)
- Primary NTP
- Secondary NTP (Optional)
- Community String for SNMP
- Device Name
- Serial Number
- Device Site Location

NOTE: To use DHCP with reservations, please provide Vertiv with the reserved IP address, community string for SNMP, and hostname (optional).

Direct IoT Requirements

Only Vertiv™ Liebert® IntelliSlot™ Unity Communications Cards or the Vertiv™ Liebert® IntelliSlot™ RDU101 Communications Cards can use the direct IoT option. Customers must provide the following:

Device Information

- IP Address
- Subnet Mask
- Gateway
- Primary DNS
- Secondary DNS (Optional)
- Primary NTP
- Secondary NTP (Optional)
- Device Name
- Serial Number
- Vertiv Services Gateway Location

NOTE: To use DHCP with reservations, please provide Vertiv with the reserved IP address and hostname (optional).

4. Data Entry and Pre-Configuration

During this phase, Vertiv completes the following tasks:

- Generates the internal tracking number for each monitored device and Vertiv Services Gateway.
- Enters the customer-provided information into the Vertiv Cloud Service Portal.
- Configures any items that are to be shipped to the customer, such as Vertiv Services Gateways, network cards, dry contact monitors, etc.

5. Firewall Exceptions

While the Vertiv team works on the Data Entry and Pre-Configuration phase, the customer should begin configuring their network to accommodate for the firewall exceptions for their connection type. Depending on your connection type, please refer to the appropriate table for descriptions of the firewall exceptions.

Vertiv Services Gateway Firewall Exceptions

External Firewall Exceptions - From the gateway IP address to the specified URLs		
Type	**Exception**	**Description**
URL	mq-service.vertiv.cloud	Uses AMQP over TCP/443 (Outbound Only)
	rsd-service.vertiv.cloud	Uses HTTPS web services (SOAP) over TCP/443 (Outbound Only)
	gwapi-service.vertiv.cloud	Uses HTTPS web services (REST) over TCP/443 (Outbound Only)
	crl.sectigo.com	Uses HTTP on port 80 for Web Certificate verification (Outbound with a response from the Server)
Protocol	Network Time Protocol (NTP)	Only applicable if the Vertiv Services Gateway is configured to use External Time Servers
Service	Domain Name Service (DNS)	Only applicable if the Vertiv Services Gateway is configured to use External DNS Servers

Internal Firewall Exceptions – Between the gateway and monitored devices		
Type	**Exception**	**Description**
Port	UDP Port 161	For SNMP communications
	UDP Port 162	For SNMP traps sent by the monitored device to the Vertiv Services Gateway
Protocol	HTTPS (Enable HTTPS Only Option)	For accessing the web UI of the card for network configuration
	Network Time Protocol (NTP)	Only applicable if the Vertiv Services Gateway is configured to use Internal Time Servers
Service	Domain Name Service (DNS)	Only applicable if the Vertiv Services Gateway is configured to use Internal DNS Servers

Direct IoT Firewall Exceptions

External Firewall Exceptions		
Type	**Exception**	**Description**
URL	mq-service.vertiv.cloud	Uses AMQP over TCP/443 (Outbound Only)
Protocol	Network Time Protocol (NTP)	Only applicable if the network card is configured to use External Time Servers
Service	Domain Name Service (DNS)	Only applicable if the network card is configured to use External DNS Servers

Internal Firewall Exceptions		
Type	**Exception**	**Description**
Protocol	HTTPS (Enable HTTPS Only Option)	For accessing the web UI of the card for network configuration
	Network Time Protocol (NTP)	Only applicable if the network card is configured to use Internal Time Servers
Service	Domain Name Service (DNS)	Only applicable if the network card is configured to use Internal DNS Servers

6. Vertiv Services Gateway Shipping and Installation

Gateway Rack Mounting Installation

For installing the gateway on a rack, a pre-configured gateway unit is shipped to the customer for them to install on their network. The customer should notify Vertiv when the installation is complete. Vertiv will then verify the gateway is online and functioning properly. If the gateway is malfunctioning, Vertiv Tier 2 support will assist the customer in determining if there are issues related to the firewall or internet connections.

Gateway Server Installation

For installing the gateway on a Windows server, a download link is provided to the customer that directs them to all required files and documentation for installation. If necessary, a Vertiv Support engineer can assist with the installation via remote sessions. The customer should notify Vertiv when installation is complete. Vertiv will then verify the gateway is online and functioning properly. If the gateway is malfunctioning, Vertiv Tier 2 support will assist the customer in determining if there are issues related to the firewall or internet connections.

7. Device Configuration

The next phase in the on-boarding process is configuring the devices that will be communicating with the Vertiv Services Gateway and/or directly to Vertiv via the direct IoT. There are three options for completing this phase:

Option 1

Customer preforms the configurations.
Instructions are sent to the customer for them to configure all devices on their timetable.

Option 2

Customer preforms the configurations with Vertiv assistance.
Same as Option 1 with the exception that a Vertiv Support engineer is available via remote sessions to assist the customer.

Option 3

Vertiv Certified Engineer performs the configurations.
Vertiv arranges a day and time for a Vertiv Certified Engineer to perform on-site configurations for the customer's network card(s). Networking contact must be resent during a site visit.

8. Verification

In the final phase, Vertiv verifies the following:

- All monitored devices are properly communicating with the Vertiv Cloud.
- Vertiv Cloud is receiving data and alarms from the monitored devices.
- The customer is receiving alarm notifications from Remote Monitoring as specified in the contract.

9. Frequently Asked Questions

Can Vertiv Digital Services monitor third-party devices?

This is dependent on the offering and connection type selected by the customer. While the Vertiv Services Gateway can support most third-party devices, the customer must provide a current MIB file and MIB Walk of the device if there is no current template for the device.

NOTE: The direct IoT communication option only supports Vertiv devices that use a Vertiv™ Liebert® IntelliSlot™ IS-UNITY-DP Communications Card, a Vertiv™ Liebert® IntelliSlot™ RDU101 Communications Card, or a Vertiv™ Liebert® IntelliSlot™ RDU120 Communications Card.

Does the Vertiv Gateway Services support DHCP?

Yes. While the Vertiv Services Gateway supports DHCP, the customer must provide the reserved IP address to Vertiv. This is due to the gateway requiring an IP address to access the monitored devices, as well as the SNMP settings requiring an IP address to use for their Access and Trap target settings.

Can the same device use both direct IoT and Vertiv Services Gateway?

No. A single device can use only one method of communication. However, customers can use the direct IoT option for certain devices and the Vertiv Services Gateway option for others. This is useful for scenarios where one or two devices at a remote location are monitored using direct IoT, while additional devices at a different location are monitored using the gateway.

Is it an issue if the customer's firewall only supports firewall exceptions using an IP address?

While the Vertiv Services Gateway and network cards only use URLs to transmit data to the Vertiv Cloud, an IP address can be used in the customer's firewall rules. Vertiv can provide the customer with the IP address(es), or the customer can verify the current address(es) using nslookup. However, if these IP addresses change in the future, the customer's firewall rules would have to be updated.

Is it required to use the customer's company network for these connection options?

The devices can be hosted on the customer's own network or VLAN. When devices are on different networks or VLANs, the customer must ensure that all devices can communicate properly to the gateway or via an internet connection for the direct IoT option.

Can the ports used by the Vertiv Services Gateway or direct IoT be changed?

At this time, the port used for communication cannot be changed.

Can a proxy server be used with either option?

Proxy support is only available with the Virtual Server option.

Is on-site support available for these options?

The scope of support is limited to Vertiv devices and further determined by the customer's service contract.

10. Contact Information

For technical support or configuration assistance, please contact

- rsd@vertiv.com for the Americas
- *EMEADigitalOpseRequest@vertiv.com* for the EMEA region

For security concerns (CVE, CWE, and CVSS), please contact both

- monitoring.support@vertiv.com and product.vulnerability@vertiv.com for the Americas
- *EMEADigitalOpseRequest@vertiv.com* for the EMEA region