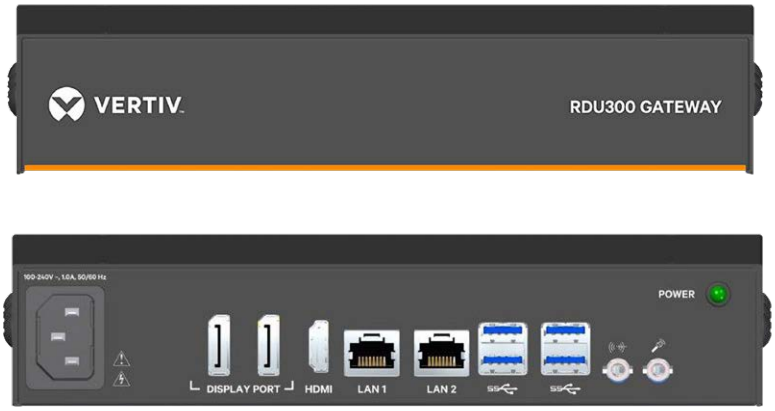
LSG – Life Services Gateway

Version 4

Overview

The **LSG (LIFE Services Gateway)** is used to deliver monitoring services and is an aggregator of device data. It is a network appliance installed on site and communicates with equipment (both Vertiv and 3rd party).

The Vertiv IoT Gateway appliance is a physical device with the LSG software running on it.



Technical Specifications

Dimensions (W x D x H)	8.5 x 9.5 x 1.5 in (22 x 25 x 4 cm) – with the included rack mount kit installed, fits in a 1U slot of a standard 19-inch (48.3 cm) rack*
Ethernet (LAN1)	1 Gigabit
Ethernet (LAN2)	LAN2 is used for configuration only and should not be connected to a network
Power Requirements	100-240V – 1A, 50/60Hz

** If a different configuration is desired, please work with your Vertiv remote monitoring contact to make alternate arrangements.*

Requirements for Configuration

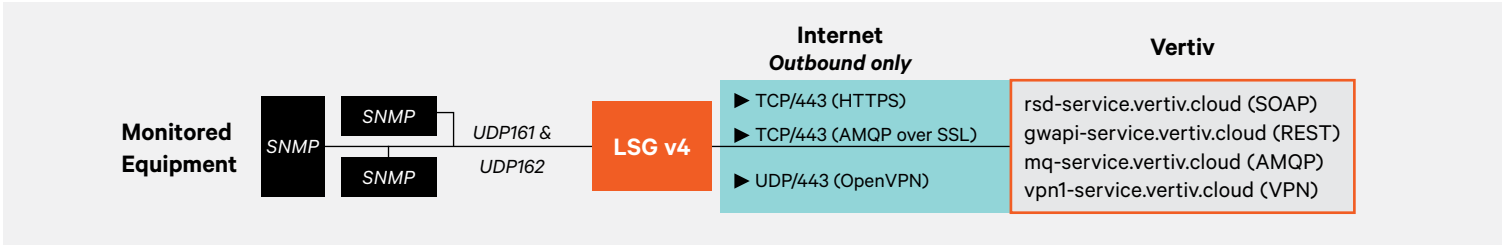
- Static IP address for Gateway
- Subnet Mask
- Default Gateway IP Address
- SNMP Community String (default: public)
- Internal or External DNS access
  - Primary DNS Server IP Address
  - Secondary DNS Server IP Address (optional)
- Internal or External NTP access (optional)
  - Primary NTP Server IP Address
  - Secondary NTP Server IP Address
- By default, the LSG will try to access following NTP servers:
  - 0.centos.pool.ntp.org
  - 1.centos.pool.ntp.org
  - 2.centos.pool.ntp.org
  - 3.centos.pool.ntp.org
- Internal SNMP v1/2 Access on UDP ports 161/162
- Contact for Card Configuration
  - We will need to get all monitored units configured for SNMP access. Please let us know if we can work with someone internally to do this quickly, or if we need to make alternate arrangement such as sending a technician out.
- LSG shipping details
  - Attention:
  - Address:
  - City:
  - State:
  - Zip Code:

Networking Requirements

The LSG should be installed in a secure location within your network. Only the LAN1 interface should be connected and should be protected from the general internet. It should also be firewalled from the rest of the network. However, LAN1 must have an open path to the equipment it is intended to monitor or connect to. It must have access to the following addresses and protocols/ports in the Vertiv cloud via its LAN1 Ethernet interface to perform its primary functions:

- **Messaging Service:** mq-service.vertiv.cloud – AMQP over TCP/443
- **Provisioning Service:** rsd-service.vertiv.cloud – HTTPS web services (SOAP) over TCP/443
- **Authentication Service:** gwapi-service.vertiv.cloud – HTTPS web services (REST) over TCP/443
- **VPN Service:** vpn1-service.vertiv.cloud – OpenVPN protocol over UDP/443

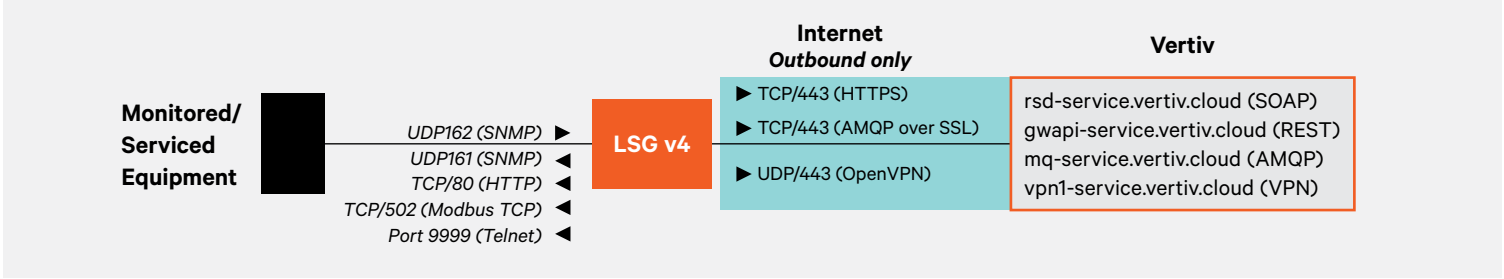
For general remote monitoring or Life services with an LSG, the gateway must be allowed to query equipment via SNMP (UDP/161) and receive SNMP traps (UDP/162) from the monitored device. In this configuration the VPN connection is optional:



The gateway performs several critical functions from translating SNMP protocols to encrypting, processing, managing, and filtering data. It does this by optimizing system performance through the collected operational data gathered and processed in real-time. SNMP is primary protocol supported for remotely monitoring devices. The collected data is normalized and then sent to the Vertiv cloud securely over the internet via AMQP over SSL.

When connected to a production network, the gateway uses the SNMP v1/2 protocol to poll information from the device via UDP port 161, and to receive SNMP Traps via UDP port 162. The SNMP community is typically set to public (all lowercase) by default but can be changed as desired. Additionally, the LSG will need to access a DNS server to resolve the Vertiv Hostnames, and a NTP Server to ensure the LSG has the correct time for its web certificates.

For preferred monitoring of Alber units and remote service support of SiteScan and Environent systems, the VPN connection is required for report generation, remote system support, and system maintenance. Additional ports between the LSG and monitored/service equipment also need to be opened depending on the system. For example, TCP port 80 (HTTP), TCP port 502 (Modbus), and potentially Port 9999 (for changing configurations and setpoints) need to be opened for Alber BDS40, BDS256, MPM100, and UXTM units. The diagram above would change to the following for those Alber units under a preferred remote monitoring contract:



VPN Information

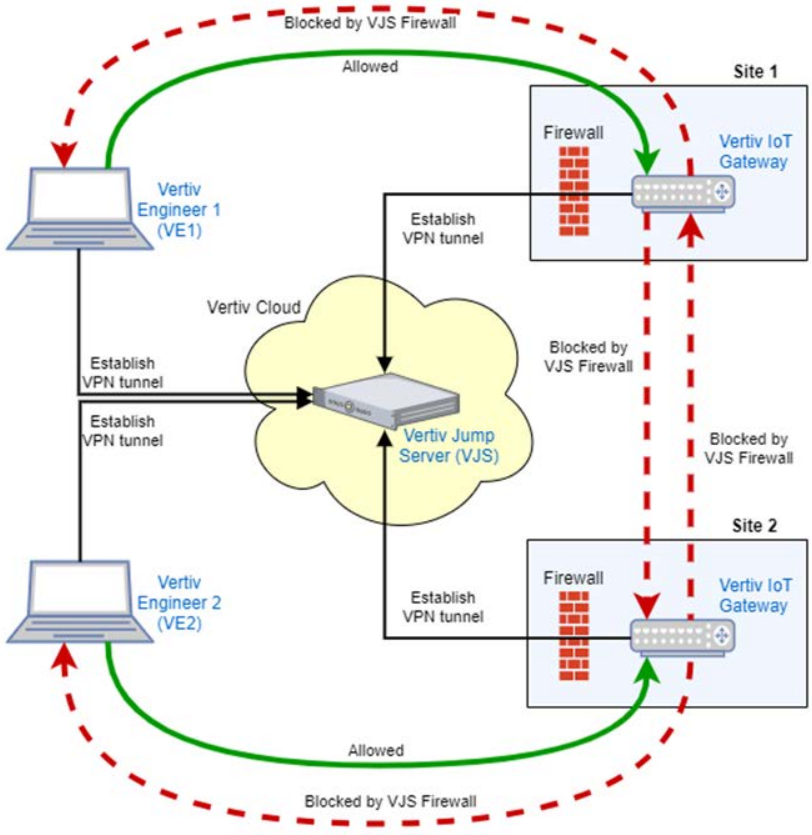
The LSG includes a feature that allows it to securely connect to a Virtual Private Network (VPN) hosted by an OpenVPN server in the Vertiv cloud (vpn1-service.vertiv.cloud). This VPN allows Vertiv service engineers to remotely access the gateway and connected equipment.

VPN connections are authenticated using industry standard X509 certificate technology. The client certificate and associated private key are protected from disclosure using strong passwords and industry standard encryption technologies. The certificate and private key pair are used by an OpenVPN server in the Vertiv cloud and allows the server to authenticate VPN clients. The server is completely administered by Vertiv. SSH access to the OpenVPN server is blocked from the internet and is controlled by a private key which is only available to select Vertiv administrators. A Vertiv certificate administrator will only issue certificates to Vertiv engineers authorized to connect to the VPN.

VPN clients consist of LSGs in the field and Vertiv employed engineers. Contractors, vendors, or anyone else external to Vertiv is not eligible to have a VPN client. Each Vertiv service engineer and LSG authorized to connect to the OpenVPN server has their own dedicated certificate. LSGs must be individually authorized to connect, which is only possible when VPN is enabled on the LSG's web application. Even if VPN is enabled on the LSG, an authorized Vertiv service engineer still must enable the LSG for VPN and request a certificate for it in the Vertiv cloud. The VPN client certificate is manually requested. If the VPN tunnel is left open and unused for 120 minutes, the VPN tunnel is automatically closed.

The LSG's VPN certificate and private key pair is generated at the time it is authorized to connect to the Vertiv cloud (which it does via mq-service.vertiv.cloud). The package is encrypted using a PKI public key registered by the LSG when it first connects to the cloud. This encrypted package is then sent to the LSG. Only the LSG can decrypt it because it alone has the corresponding PKI private key. The LSG generates the PKI public and private key pair the first time it starts up. It never publishes the private key, which is kept in a protected area with access limited to only the application that decrypts the OpenVPN certificate package. In the cloud, the files used to generate the encrypted certificate package are immediately deleted. Once the encrypted package is generated, only the target LSG can decrypt it.

The VPN is designed to only allow access from Vertiv Services technicians. Gateways cannot initiate connections to Vertiv or initiate connections to other gateways. The following diagram illustrates the virtual connections that are allowed via the VPN tunnel (solid green lines), as well as those that are prevented (dashed red lines).



Note: VJS is the OpenVPN server in the Vertiv cloud (vpn1-service.vertiv.cloud)

Security Features

The LSG is a secure appliance and is outbound only over port 443. All communications to the Vertiv Cloud are initiated by the gateway using the AMQP protocol and are encrypted using industry standard technologies. Security features include:

- TLS 1.2 with uniquely generated symmetric encryption keys.
- Public key bit length: 2048
- Hash algorithm: SHA-1 (256 bit)
- Cipher suite: Negotiated between the client and server during the connection handshake
- Only the following ports are open on the LAN1 Ethernet interface:
  - SNMP Trap (UDP/162) - Listens for SNMP Traps, doesn't respond to other protocols, and all invalid messages are dropped
  - HTTPS (TCP/443) - Access is protected by a username/password configured in the Vertiv cloud. Even when logged in, no Personally Identifiable Information (PII) or any other sensitive data is accessible via the web application listening on this port.
- Communications between the LSG and the cloud are all outbound – they are all initiated by the gateway. (The only exception to this is when the gateway is enabled for and connected to the VPN. However, there still is no requirement for inbound firewall exceptions).
- The only configuration done on the gateway itself is to register it with an account in the Vertiv Cloud
- The VPN must be enabled from the LSG's Web Application
- The only outbound exceptions required are noted above.

Additional Gateway Features

- Downloads updated configuration daily from the Vertiv cloud
- Sends a heartbeat message every 5 minutes back to Vertiv
  - This allows Vertiv to know the gateway is communicating
  - Part of the response also includes a timestamp to keep the hardware-based gateways synced
- Supports remotely specified commands, including Full Firmware Update, Application Update, Download of LogicX Scripts, Force Configuration Download, and Upload Log Files
  - Commands are downloaded as part of the heartbeat