Vertiv™ Next Predict Security

Best Practices, Certificates, and Connections

Technical Note

JUNE 2026

Technical Note Section Outline

1. Overview

Vertiv™ Next Predict and Vertiv™ Next Response are proprietary API algorithms that run on aggregated data collected and sent to the Vertiv™ Service Cloud by either the Vertiv Services Gateway or via Vertiv communication cards (Direct IoT). This document provides essential security details for Vertiv™ Next Predict, Vertiv™ Next Response, and the Vertiv™ Service Cloud, including information on network connection best practices, certificate details, API connections, and answers to key security questions for the Americas

Helpful Contacts

- For more information on security concerns or for assistance with support issues, contact
  - monitoring.support@vertiv.com for the Americas
  - EMEADigitalOpseRequest@vertiv.com for the EMEA region
- For more information on configurations or for assistance with order issues, contact
  - rsd@vertiv.com for the Americas
  - EMEADigitalOpseRequest@vertiv.com for the EMEA region
- To request security enhancements, complete this form: Vertiv Voice of Customer Form. Feedback received is used to prioritize and implement security enhancements in our products.

2. Network Security Best Practices

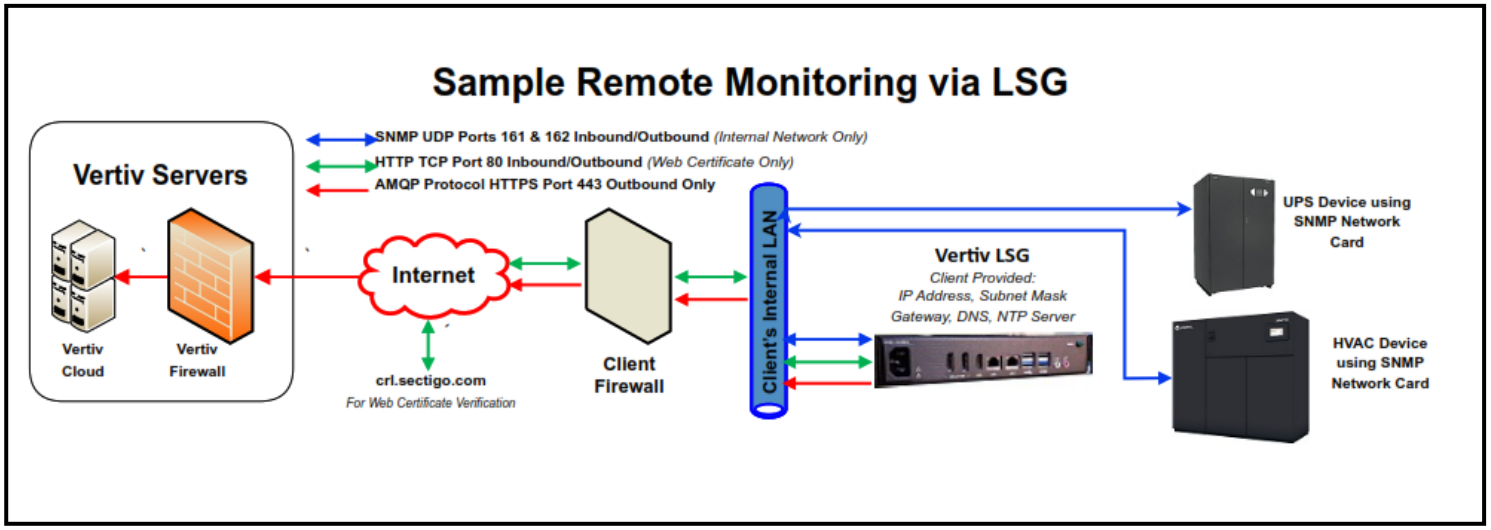
When setting up your Vertiv Services Gateway to the cloud service portal for Vertiv™ Next Predict or Vertiv™ Next Response services, please follow these recommendations:

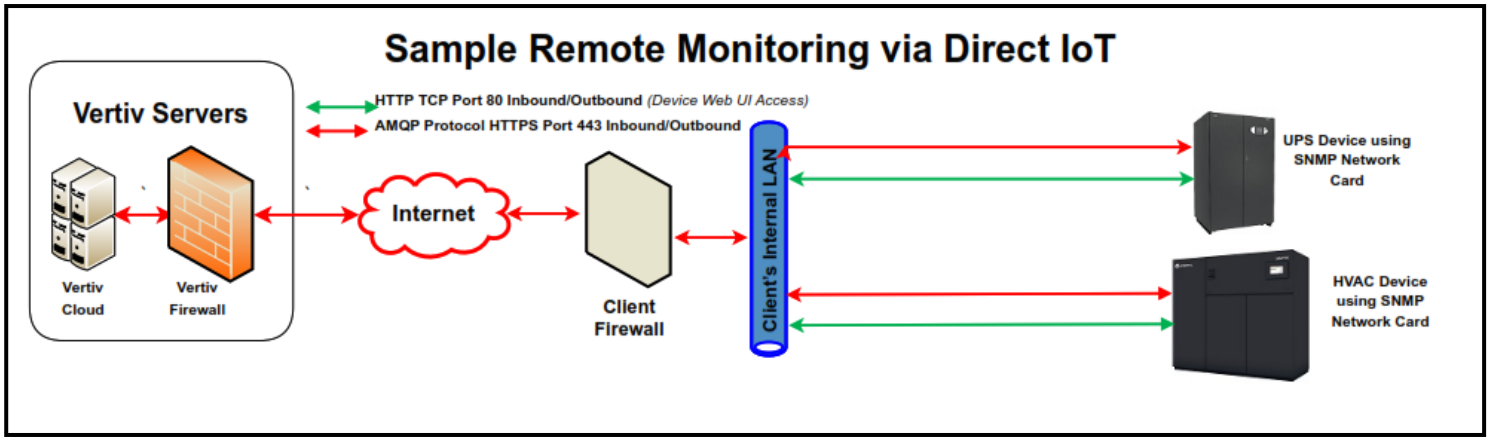
- Implement VLAN segmentation best practices:
  - Create MAC address-based network objects.
  - Group similar devices together. For example, group SNMP managers (Vertiv Services Gateway) together, and group SNMP agents (communication cards) together. (SNMP v3 is the default communication method for devices connecting via the Vertiv Services Gateway)
  - Allow only the routes and protocols defined in the architecture diagrams, and apply the rule of least privilege to all inbound and outbound VLAN traffic through firewall configurations and policies.
- Configure Port 80 with an implicit deny rule, allowing only crl.sectigo.com.
- Set SNMP unique community strings for managers and agents.
- Set a complex password for the Admin on Vertiv Services Gateway.

PROPRIETARY AND CONFIDENTIAL. © 2026 Vertiv Group Corp.

- Disable all TLS versions below TLS 1.2.

The following diagrams show sample network connections to the Vertiv™ Service Cloud from a Vertiv Services Gateway and from communication cards (Direct IoT).





3. Certificate Details

Certificates can be generated in both non-VPN and VPN configurations.

- Non-VPN certificates: Vertiv Services Gateway non-VPN certificates are generated in the Cloud Service Portal. The package is encrypted using a PKI public key registered by the Vertiv Services Gateway when it first connects to the cloud. This encrypted key is then sent to the Vertiv Services Gateway for decryption (the Vertiv Services Gateway has a private key that is never shared).
- VPN certificates: On the VPN configuration, a client certificate is given to the customer. This certificate contains the public key to access the Production VPN in the Vertiv cloud environment. The private key is stored in the cloud, and only Vertiv engineers/service support engineers have access to the environment and the private key.

PROPRIETARY AND CONFIDENTIAL. © 2026 Vertiv Group Corp.

Handshake Algorithms

For public or private key TLS handshakes by the Vertiv Services Gateway to the cloud service portal, the following cryptographic algorithms are approved in accordance with NIST 131a Rev2 and NIST 800 052 Rev 2.

DESCRIPTION	ALGORITHM
Block cipher encryption for information protection	AES-128
	AES-192
	AES-256
Asymmetrical algorithm used for key establishment	Elliptic Curve Diffie-Hellman Key Exchange (ECDH):
	• Curves P-224, P-256, P-384, P-521
	• Curves K-233, K-283, K-409, K-571
	• Curves B-233, B-283, B-409, B-571
	RSA: len (n) >= 2048
Asymmetrical algorithm used for key digital signature generation and verification	DSA >= 112 bits; DSA: (L, N)= (2048, 224, (2048, 256), or (3072, 256)
	ECDSA or EdDSA: len (n) ≥ 224
	RSA: len (n) ≥ 2048
Compute a condensed representation of data	SHA-2 Family
	SHA-3 Family
Message Authentication Codes (MAC)	HMAC; >= 112 bits
	CMAC; AES
	GMAC; AES
	KMAC; >= 112 bits
TSL/SSL Ciphers	RSA 2048
	ecdh_x25519

Outbound Encryption

For outbound connection encryption, use TLS 1.2 over HTTPS Port 443.

PROPRIETARY AND CONFIDENTIAL. © 2026 Vertiv Group Corp.

4. Key Security Questions

What are the security concerns or risks associated with connecting this service?

Vertiv™ Next Predict and Vertiv™ Next Response are proprietary API algorithms that run on aggregated data collected and sent to the Vertiv™ Service Cloud by a Vertiv Services Gateway or communication cards (Direct IoT). Vertiv uses internal metrics from product testing and feeds those values into the algorithms on the back end. This, however, does not increase any security risks, so the same risks associated with Vertiv Services Gateway are relevant here as well. Here are the Vertiv Services Gateway security risks:

- **Risk 1:** Outbound connection to Vertiv™ Service Cloud for some customers is an inherent risk they need to accept in their environment. Vertiv is actively working on an ISO 27001 Certification for this cloud environment and is committed to safeguarding your data and our products in your environment. Vertiv™ Next Predict only processes telemetry data, so no Personal Identification Information (PII) or Intellectual Property is at risk.
- **Risk 2:** SNMP v1 and v2 are susceptible and transmit clear text traffic due to their reliance on encrypted community strings and the lack of strong authentication methods. All traffic transmitted via SNMP is telemetry data sent from SNMP agents to the SNMP Manager, so no Personal Identification Information (PII) or Intellectual Property is at risk.
    - For SNMP v1 and v2 (Ports 161 and 162), it is recommended to place devices into dedicated VLANs and apply internal network segmentation. Use micro-segmentation within those VLANs to allow only the necessary SNMP traffic on Ports 161 and 162, and ensure that this traffic is restricted to specific, defined routes between authorized devices.
    - It is also recommended to change the community string from its default configuration of public and/or private to a unique community string across all devices.
    - For SNMP v3, it is highly recommended to configure a unique username and password for authentication and encryption

NOTE: To provide feedback, please complete the following form: Vertiv Voice of Customer Form.

What are the security concerns or risks associated with connecting to the cloud?

The only risk on the customer's side when connecting to the cloud is the outbound connection to the Vertiv™ Service Cloud, which uses HTTPS over Port 443 with TLS 1.2 and all known weak ciphers disabled. If you prefer stronger controls (such as TLS 1.3, Elliptic Curve key algorithms with Perfect Forward Secrecy, or mTLS), you can request these security enhancements through our Voice of Customer form. We use this feedback to prioritize and implement security improvements in our products. Vertiv is also actively working toward ISO 27001 Certification for our cloud environment to reassure you that your data security is our top priority.

NOTE: To provide feedback, please complete the following form: Vertiv Voice of Customer Form.

Who do we contact if we scan our environment and find a vulnerability?

All identified security vulnerabilities, including CVE, CVSS, CWE, or Nessus plug-in ID details, should be reported to monitoring.support@vertiv.com for the Americas, or *EMEADigitalOpseRequest@vertiv.com* for the EMEA region.

External vulnerabilities submitted will be incorporated into the next Delta Assessment for the affected product and reviewed in accordance with our SECURE 2.0 requirements, vulnerability triage Service Level Agreements (SLAs), and the "shall" statements outlined in NIST Special Publications 800-131A and 800-52 Revision 2.

How do I receive firmware and software updates for patching and security fixes?

Firmware and software updates are available here: Critical Equipment Software Downloads | Vertiv

What are the best practices for configuring our environment with other Vertiv monitoring products?

- **Best practice 1:** VLANs and network segmentation. Vertiv recommends grouping similar device types (such as SNMP managers with SNMP managers and SNMP agents with SNMP agents) into their own VLANs based on MAC address or device role. This allows you to control internal traffic, maintain predictable network paths, and move equipment as needed without disrupting the overall network design.
- **Best practice 2:** Apply the principle of least privilege. Only enable the protocols and ports required for Vertiv Services Gateway or Direct IoT to function, such as Port 443, Port 80 (Sectigo CRL), and Ports 161/162 for SNMP. Ensure appropriate routes and policies are applied to these VLANs so communication occurs only along defined, authorized paths.
- **Best practice 3:** Update SNMP community strings. Vertiv recommends using unique, complex community strings that align with your internal security and risk requirements.

© 2026 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.