Vertiv™ Next Connect

Quick Installation Guide for Next Connect Local Agent on
Windows and Ubuntu Linux

Overview

This Quick Installation Guide provides step-by-step instructions to install the Vertiv™ Next Connect Local Agent on Windows 11, Server 2019, Server 2022, or Ubuntu Linux 22.04 LTS Desktop.

Prerequisites

- **Network and Firewall:** Ensure the required ports are open and the necessary cloud endpoints are accessible through the organization's firewall. For more details, refer to the Network and Firewall Configuration on page 1.
- **Internet Access:** Required for downloading, installing, registering, updating the agent, and for Vertiv Next Connect connectivity.
- **Vertiv Next Connect Account:** Make sure you have a Vertiv Next Connect account and a customer created for agent registration.

System Requirements

Requirement	Windows 11 or Server 2019/2022	Ubuntu Linux 22.04 LTS Desktop
Minimum free memory	2 GB (4 GB recommended)	2 GB (4 GB recommended)
Total memory	4 GB (8 GB recommended)	4 GB (8 GB recommended)
Total VM memory required (where applicable)	OS specified minimum + Agent minimum	
Minimum free disk space	27 GB (60 GB recommended)	27 GB (60 GB recommended)
Total disk space	60 GB (100 GB recommended)	60 GB (100 GB recommended)
CPU	2+ cores, Intel Xeon E5-2673 v3 or equivalent	2+ cores, Intel Xeon E5-2673 v3 or equivalent

Network and Firewall Configuration

The following table lists the inbound and outbound ports required for communication between the monitored devices and the Local Agent:

Port	Protocol	Transport	Description
0	ICMP	ICMP	Open to allow network connectivity verification over ICMP.
161	SNMP	UDP	Open to allow connectivity to SNMP based targets and clients.
162	SNMP	UDP	Open to send and receive SNMP traps.
22	SSH	TCP	Open to allow SSH sessions to the appliance.
80	HTTP	TCP	• Open to allow internet access to the Vertiv Next Connect portal. • Open to allow monitoring device discovery. • Open to allow communication to the monitoring device communication card. • Open to allow provisioning of the monitoring device card firmware. • REST-HTTPS for sending commands.
443	HTTPS	TCP	• Open to allow a web user interface. • REST-HTTPS for sending commands.
21000	HTTP	TCP	Local Web Application.
21001	HTTPS	TCP	Local Web Application.

Port	Protocol	Transport	Description
5671	AMQP	TCP	• Open for Azure IoT Hub. • Open for sending device data. • Open for Blob Storage Connection for device configuration.
8883	MQTT	TCP	• Device provisioning and communication with Azure IoT Hub. • Azure provision certificate. • Receiving commands. • Sending results. • Heartbeats.
6687	Geist™ Discovery Protocol	UDP	Geist™ device discovery protocol.

The following table lists the outbound endpoints required for the Local Agent to communicate securely with Vertiv™ Next Connect. These endpoints must be configured for outbound communication on your organization's firewall.

Service	Endpoint	Transport	Port Number	Description
IoT Hub MQTT / AMQP / HTTPS	*.azure-devices.net	TCP	8883, 5671, 443	Used for all IoT Hub communications.
Device provisioning service (DPS)	*.azure-devices-provisioning.net	TCP	443	Used during initial registration / reprovisioning.
Azure edge agent/hub updates	mcr.microsoft.com and *.data.mcr.microsoft.com	TCP	443	Microsoft Container Registry (MCR)—IoT Edge runtime modules.
Azure container registry	*.azurecr.io	TCP	443	Used for pulling custom container images.
Application specific API's	https://stfdtnpublicprdeastus002.blob.core.windows.net https://stfoundationprdeastus002.blob.core.windows.net https://next-connect.vertiv.com/* https://next-connect-api.vertiv.com/*			

Downloading the Agent Installer

1. Log in to the Vertiv™ Next Connect platform.
2. Select the *Local Agents* menu under the Equipment menu.
3. Click the *Add* icon to open the New Agent dialog.
4. Click the *DOWNLOAD AGENT INSTALLER* button and select the appropriate installer for your OS:
   - **Windows:** Choose either the standard Windows Agent or the bundled version. The standard version does not come bundled with Eflow and will download Eflow during the installation process.
   - **Ubuntu 22.04 Linux LTS Desktop:** Download the Linux Agent AppImage installer.

NOTE: *Vertiv recommends the use of Ubuntu for all installations whenever feasible.*

Windows Installation Steps

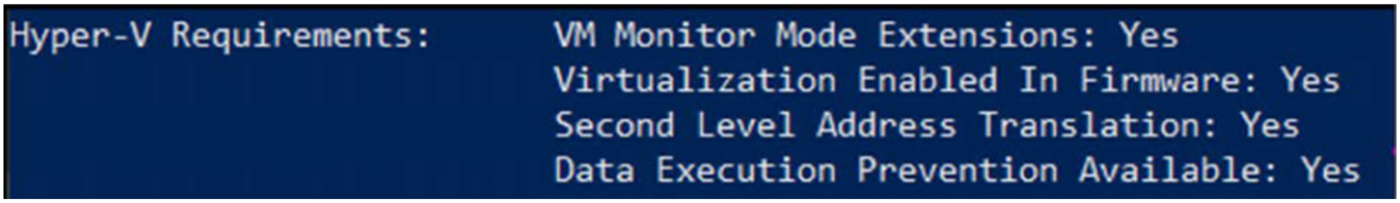
Preparation

IMPORTANT: *If you install the agent on a Windows virtual machine, refer to the VMWare and Hyper-V Additional Setup on page 5 section to enable nested virtualization on the VM host.*

1. Ensure Hyper-V compatibility. From an elevated PowerShell terminal, run the following command:

   systeminfo

2. This generates a report on the system's capabilities. The Hyper-V section is near the bottom of the report and appears as shown below.



```
Hyper-V Requirements:      VM Monitor Mode Extensions: Yes
                           Virtualization Enabled In Firmware: Yes
                           Second Level Address Translation: Yes
                           Data Execution Prevention Available: Yes
```

NOTE: *If all requirements show Yes, you can install Hyper-V on the system. If not, review the additional setup requirements in the System Requirements section, refer to the SL-71242 Vertiv™ Next Connect User Manual.*

3. Set PowerShell execution policy with the following PowerShell command:

   Set-ExecutionPolicy -ExecutionPolicy AllSigned

Run the Installer

1. Start the installation by double clicking the downloaded installer file.
2. As part of the installation process, the installer will check prerequisites and install dependencies. This includes Hyper-V and EFlow. During installation, your machine may restart as needed. After restarting, the installer will automatically launch and pick up the installation from the previous place.

Network Configuration

1. Select One NIC if your devices and internet are on the same network. Select Two NICs if you have separate devices and internet networks.
2. Choose to assign static or DHCP IPv4 addresses as appropriate. Each NIC must have a unique IP.
3. By default, the broadcast discovery scan is enabled. You can disable it by unselecting the Enable Broadcast Discovery Scans option. Vertiv recommends leaving this enabled whenever feasible. This functionality is used for discovering factory-fresh Vertiv Equipment and only performs a broadcast during a device search when broadcast discovery is selected by the user.
4. Confirm default gateway and DNS settings.

Agent Registration

1. The installer generates a temporary registration code that is valid for 15 minutes, which will allow you to register with Vertiv™ Next Connect.
2. Click the link provided during installation, or enter the code manually in the New Agent dialog on the Vertiv Next Connect platform.
3. Select your customer, and name the agent. Click *Save* to register.

Installer Completion and Post Installation

1. The agent will download additional components and updates, so allow 10 to 15 minutes.
2. Check the agent status in the Local Agents menu under Equipment. The agent may take a few minutes to show that it is communicating with the cloud.

NOTE: *Vertiv Next Connect Agent, EFlow, and Edge versions auto-update as needed.*

Ubuntu 22.04 Linux LTS Desktop Installation Steps

Preparation

1. Right-click on the *Installer*, select *Properties*, then select the *Permissions* header, and enable Allow executing file as a program, or from a terminal run:

   ```
   chmod a+x linux--local-agent-installer_ <Version>.AppImage
   ```

2. Edit the sudoers file to allow passwordless execution for your admin user. From a terminal run the following command:

   ```
   sudo nano /etc/sudoers
   ```

3. Append the following line at the end of the sudoers file:

   ```
   <<adminuser>> ALL=(ALL) NOPASSWD:ALL
   ```

4. Install libfuse2 if your Ubuntu uses FUSE3, from the terminal:

   ```
   sudo add-apt-repository universe
   sudo apt install libfuse2
   ```

5. Optionally, install net-tools for network commands:

   ```
   sudo apt-get install net-tools
   ```

6. Update your operating system before installing the agent.

Run the Installer and Register the Agent

1. Double-click or execute the AppImage installer in a terminal.
2. The installer generates a temporary registration code that is valid for 15 minutes, that will allow you to register with Vertiv Next Connect.
3. Click the provided link during installation or manually enter the code in the New Agent dialog on the Vertiv Next Connect platform.
4. Select your customer, and name the agent. Click *Save* to register.

Installer Completion and Post Installation

1. The agent downloads components and updates. Allow 10–15 minutes for this to take place.
2. Remove the passwordless execution from the sudoers file added in step 3 above for security purposes.
3. Check the agent status in the Local Agents menu under Equipment. The agent may take a few minutes to show that it is communicating with the cloud.

VMWare and Hyper-V Additional Setup

VMware and Hyper-V are supported for virtual environment installation and as a result there are additional setup items required on the host. This section is only necessary if you are installing the Vertiv™ Next Connect Agent on a Windows Virtual Machine.

Hyper-V Additional Setup

1. Enable nested virtualization on the Hyper V host by running the required PowerShell command on the physical host machine:

   ```
   Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
   ```

2. Enable MAC address spoofing on the first level (L1) virtual switch to allow network packets to pass through multiple virtual switch layers.

   ```
   Get-VMNetworkAdapter -VMName <VMName> | Set-VMNetworkAdapter -MacAddressSpoofing On
   ```

VMWare Additional Setup

NOTE: *These settings cannot be changed while the VM is running.*

Step 1: Enable Hardware Virtualization and Performance Counts

1. From the ESXi dashboard, navigate to the virtual machine for your agent and power it off.
2. After the VM has shutdown, edit the virtual machine settings.
3. Expand the CPU menu and select Hardware virtualization and Performance counters.
4. Click *Save* to save changes.

Step 2: Enable Promiscuous Mode and Related Settings

1. Select the virtual switch(es) used for the agent.
2. Expand security and select Promiscuous mode, MAC address changes, and Forged transmits.
3. Click *Save* to save the changes.

Step 3: Power on the Virtual Machine after all Changes Have Been Saved

Troubleshooting and Additional Notes

- Broadcast device discovery may not be supported in all environments.
- Wi-Fi adapters are not supported.
- If the registration code expires, restart the installer to generate a new one.
- Refer to the User Manual for advanced troubleshooting, supported hypervisors, and optional configurations.

Support

For further assistance, contact your Vertiv support contact at 1-800-543-2378 or refer to the SL-71242 Vertiv™ Next Connect User Manual.

THIS PAGE INTENTIONALLY
LEFT BLANK

THIS PAGE INTENTIONALLY
LEFT BLANK

To contact Vertiv Technical Support: visit www.Vertiv.com