Hyper-V Installation Guide

FortiSIEM 7.2.7

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

10/06/2025
FortiSIEM 7.2.7 Hyper-V Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
06/05/2023	Release of FortiSIEM - Hyper-V Installation Guide for 7.0.0.
08/01/2023	Changed Local Disk specifications for Manager Node in Pre-Installation Checklist table.
11/06/2023	Release of FortiSIEM - Hyper-V Installation Guide for 7.1.0.
12/13/2023	Release of FortiSIEM - Hyper-V Installation Guide for 7.1.1.
01/12/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.1.2.
01/24/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.1.3.
03/05/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.1.4.
06/07/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.0.
06/26/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.1.
08/14/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.2.
09/12/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.3.
11/04/2024	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.4.
02/03/2025	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.5.
03/31/2025	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.6.
10/06/2025	Release of FortiSIEM - Hyper-V Installation Guide for 7.2.7.

Fresh Installation

Pre-Installation Checklist

Before you begin, check the following:

- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and can respond to a ping. The host can either be an internal host or a public domain host like google.com.
- Choose deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Determine whether FIPS should be enabled
- Choose install type:
  - All-in-one with FortiSIEM Manager
  - Cluster with Manager, Supervisor and Workers
  - All-in-one with Supervisor only, or
  - Cluster with Supervisor and Workers
- Choose storage type for Supervisor, Worker, and/or Collector
  - Online storage - There are 4 choices
    - ClickHouse - Recommended for most deployments. Please see ClickHouse Reference Architecture for more information.

      If you plan to use ClickHouse cluster, the Worker nodes will be defined as Keeper, Data or Query nodes. The Supervisor and Worker nodes can operate as a Keeper, Data or Query nodes. This is discussed in the ClickHouse Reference Architecture, Supervisor/Worker Nodes Running ClickHouse Functions and Configuring ClickHouse Topology.
    - EventDB on local disk
    - EventDB on NFS
    - Elasticsearch
  - Archive storage – There are 2 choices
    - EventDB on NFS
    - HDFS
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum • 24GB Recommended • 32GB	OS – 25GB OPT – 200GB CMDB – 100GB SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

- If your Online event database is external (e.g. EventDB on NFS or Elasticsearch), then you must configure external storage before proceeding to FortiSIEM deployment.
  - For NFS deployment, see here.
  - For Elasticsearch deployment, see here.
- If your Online event database is internal, that is, inside Supervisor or Worker nodes, then you need to determine the size of the disks based on your EPS and event retention needs.
  - For EventDB on local disk, see here.
  - For ClickHouse, see here.
- For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

All-in-one Installation

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- Download Compressed FortiSIEM VHDX File
- Create FortiSIEM VM in Hyper-V
- Start FortiSIEM from Hyper-V Manager

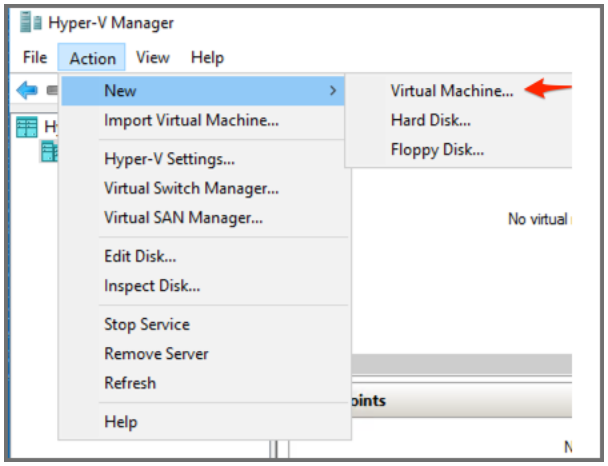
- Configure FortiSIEM
- Upload the FortiSIEM License
- Configure an Event Database
- Final Check

Download Compressed FortiSIEM VHDX File

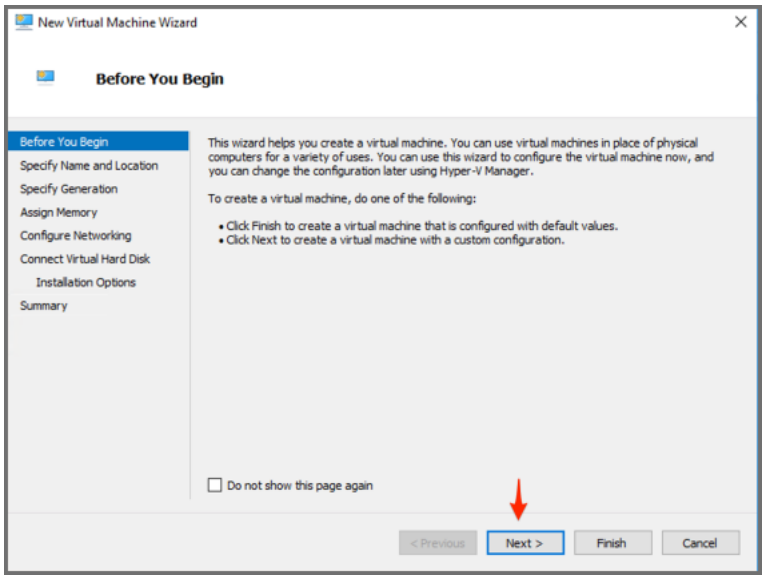
1. Go to the Fortinet Support website https://support.fortinet.com to download the Hyper-V package `FSM_Full_All_HYPERV_7.2.7_build0285.zip`. See Downloading FortiSIEM Products for more information on downloading products from the support website.
2. Download and uncompress the all-in-one package used for Super/Worker and Collector (using 7-Zip tool) to the location where you want to install the image.

Create FortiSIEM VM in Hyper-V

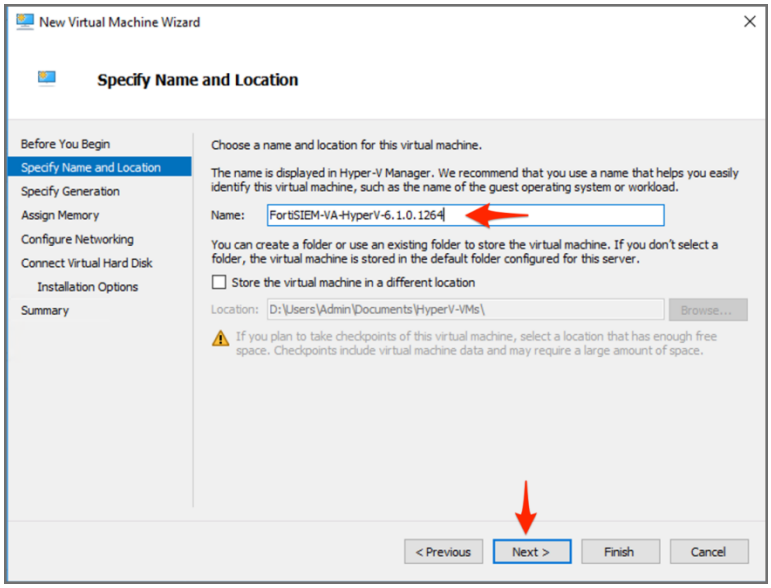
1. Launch Hyper-V Manager on your Microsoft Windows 2012 R2, 2016 or 2019 Server with Hyper-V installed.
2. Click **Action > New > Virtual Machine**, then Click **Next**.



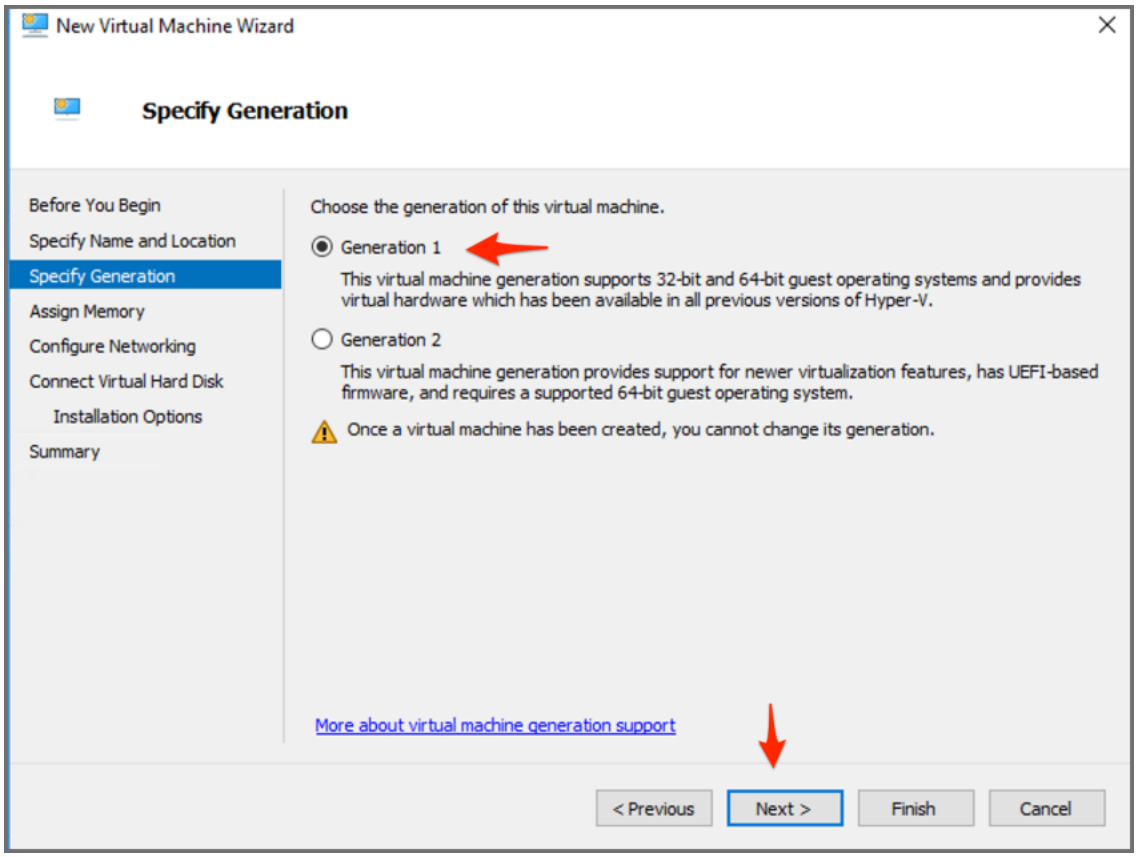
3. In the Before You Begin screen, click **Next**.



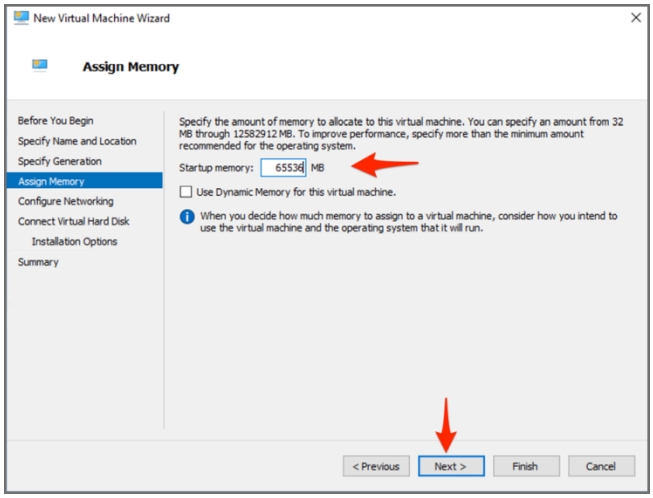
4. Specify the **Name** of the Virtual Machine, for example:



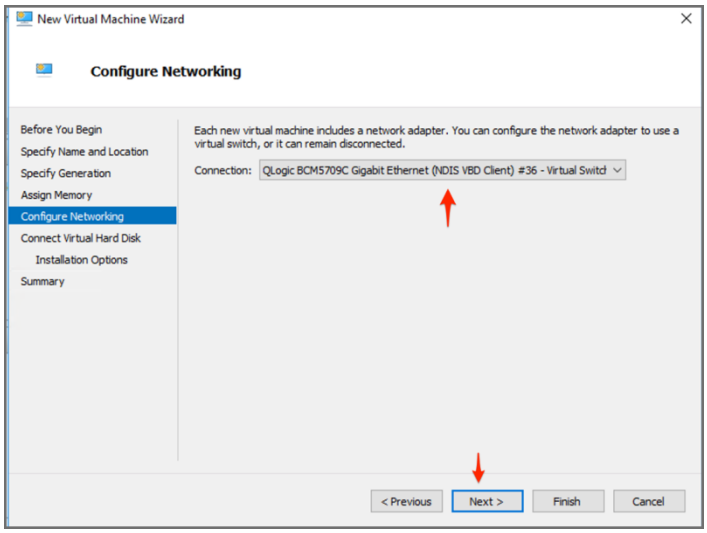
5. Specify the **Generation** type (choose **Generation 1**), for example:



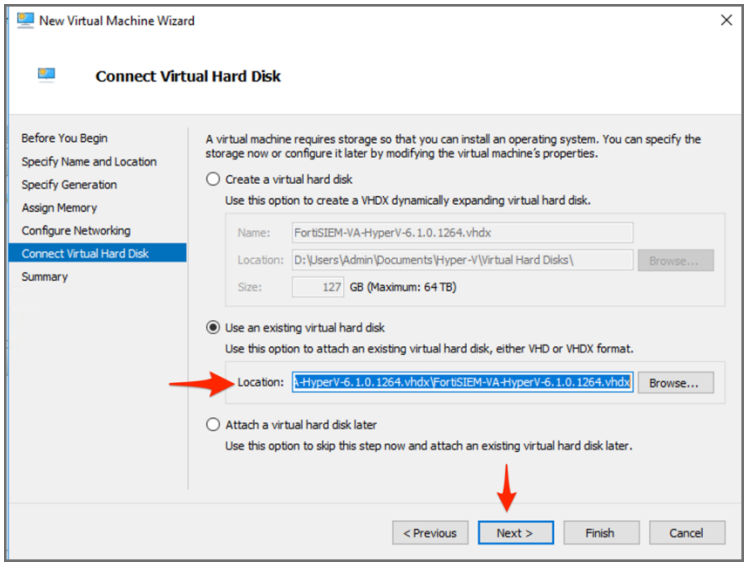
6. Add the amount of memory as per hardware requirements, then click **Next**.



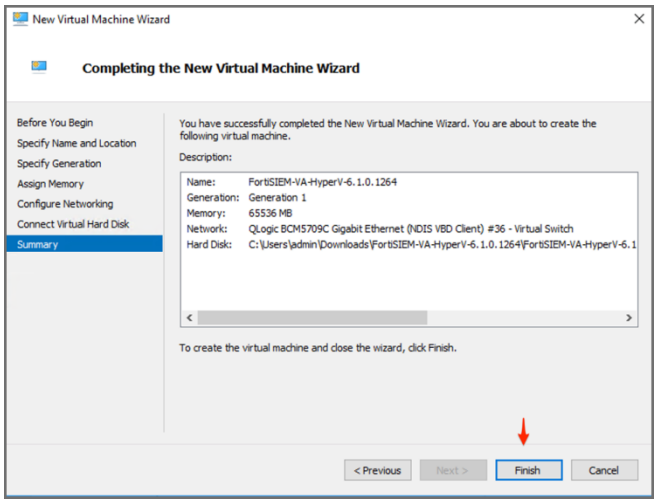
7. Configure Networking and select the virtual switch in your Hyper-V environment. Click **Next**.



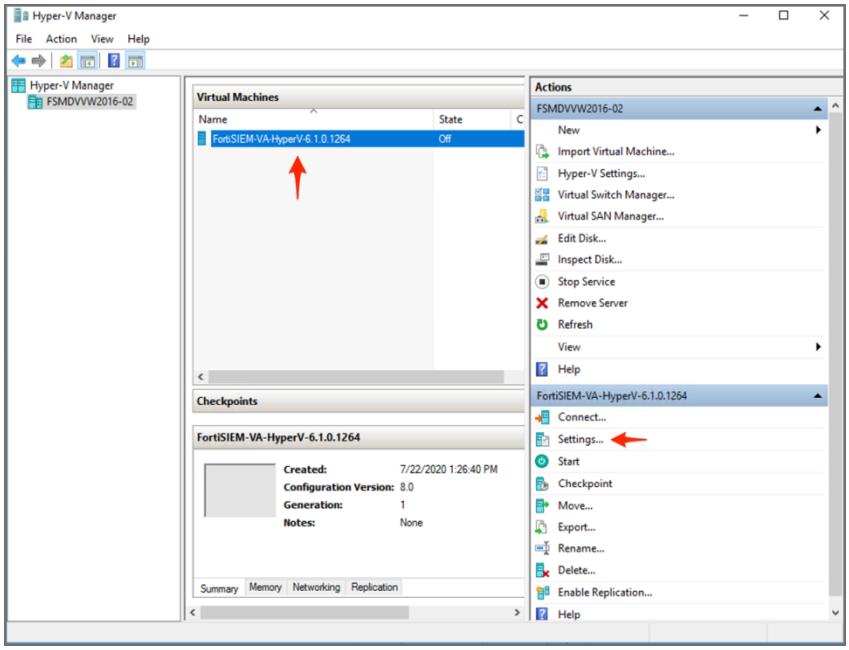
8. In Connect Virtual Hard Disk, select **Use an existing hard disk**, and choose the FortiSIEM VHDX you downloaded earlier, click **Next**:



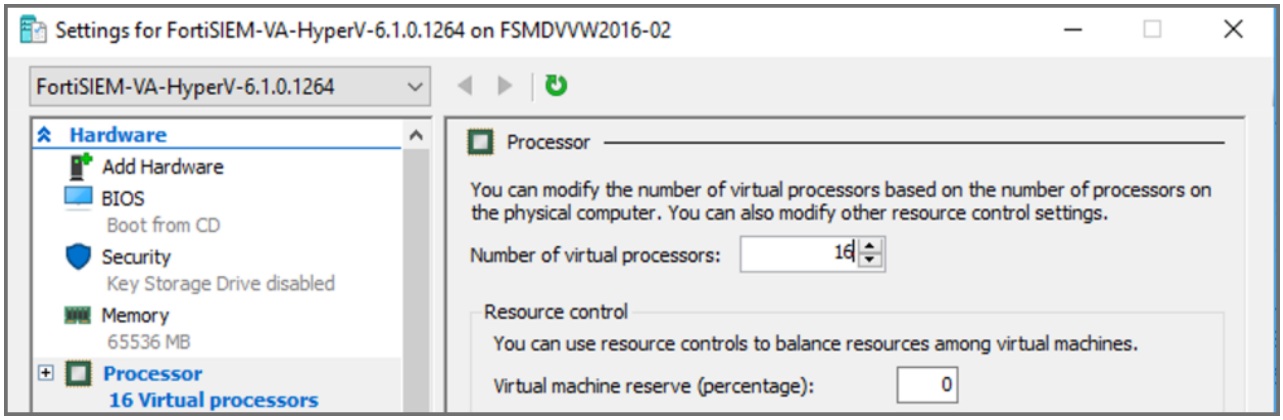
9. In Completing the New Virtual Machine Wizard, click **Finish**, for example:



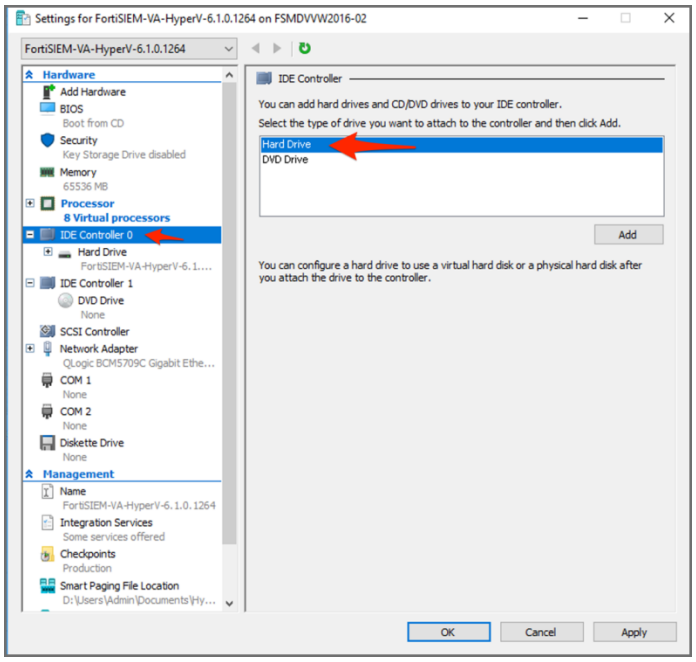
10. In Hyper-V Manager, select the virtual machine that you just created and click **Settings**, for example:



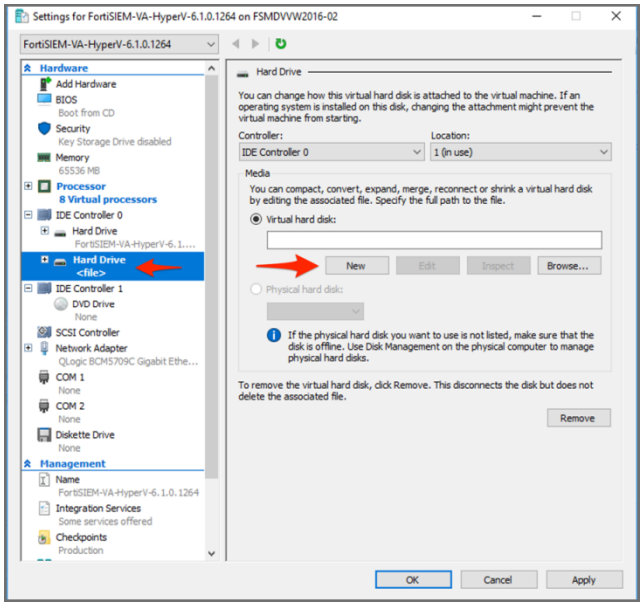
11. In Settings, select the **Processor** line in the navigation panel. Increase the number of virtual processors to **16**.



12. Navigate to **IDE Controller 0**, click on **Hard Drive**, then click **Add**, for example:



13. Select the Hard Drive you just created, Click **New**.



14. Click **Next** on the Before You Begin screen. You will add new hard disks using this method. The following is the list of disks you will need to add:

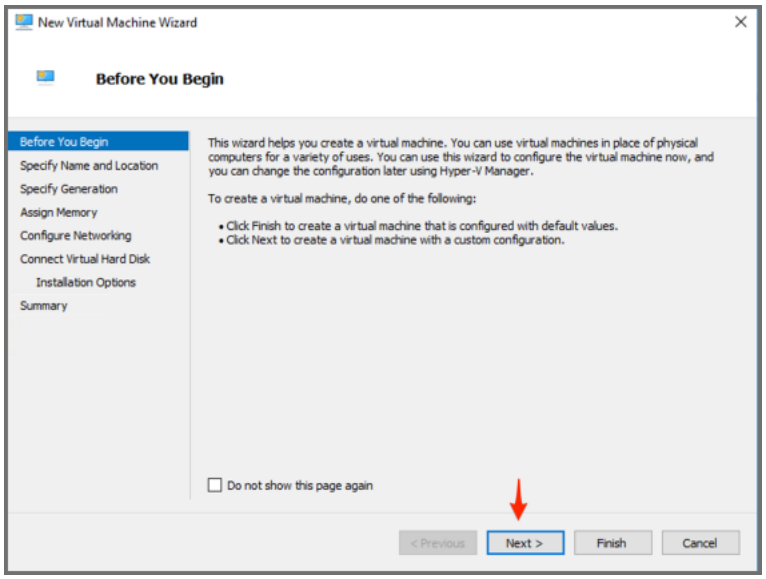
Disk	Size	Disk Name
Hard Disk 2	100GB	/opt

Disk	Size	Disk Name
		For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.
Hard Disk 3	60GB	/svn
Hard Disk 4	60GB	/cmdb
Hard Disk 5	60GB+	/data (see the following note)

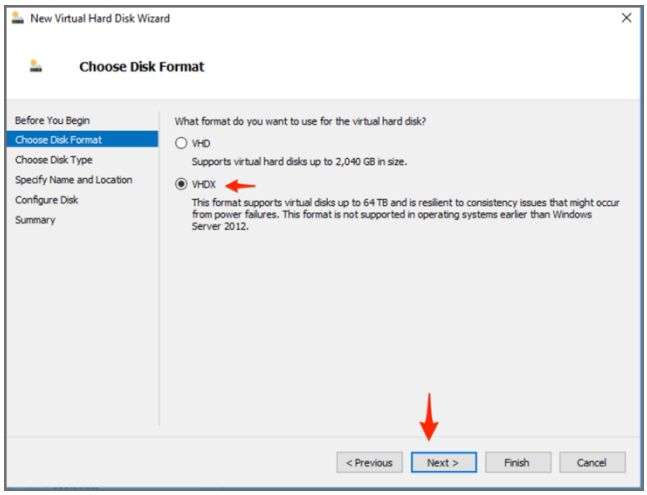
The **60GB CMDB disk** and **60GB SVN disk** should be assigned to **IDE Controller 1**.

Note on Hard Disk 5:

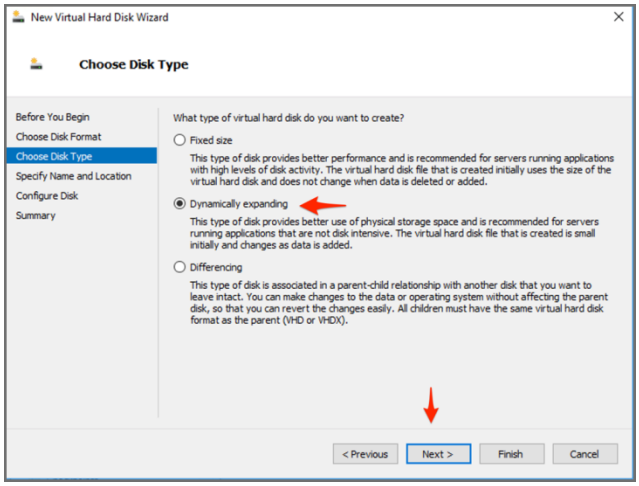
- Add the 5th disk only if using EventDB on local storage or ClickHouse. In all other cases, this disk is not required. ClickHouse is recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- For EventDB on local disk, choose a disk based on your EPS and event retention policy. See EventDB Sizing Guide for guidance. 60GB is the minimum.
- For ClickHouse, choose disks based on the number of Tiers and disks on each Tier. These depend on your EPS and event retention policy. See ClickHouse Sizing Guide for guidance. For example, you can choose 1 large disk for Hot Tier. Or you can choose 2 Tiers - Hot Tier comprised of one or more SSD disks and Warm Tier comprised of one or more magnetic hard disks.



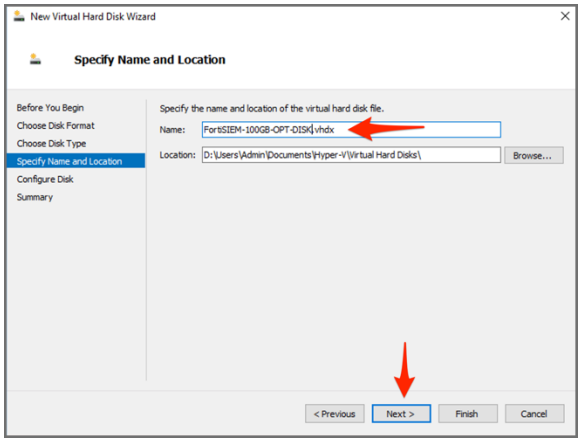
15. Choose a disk format (VHDX) and click **Next**.



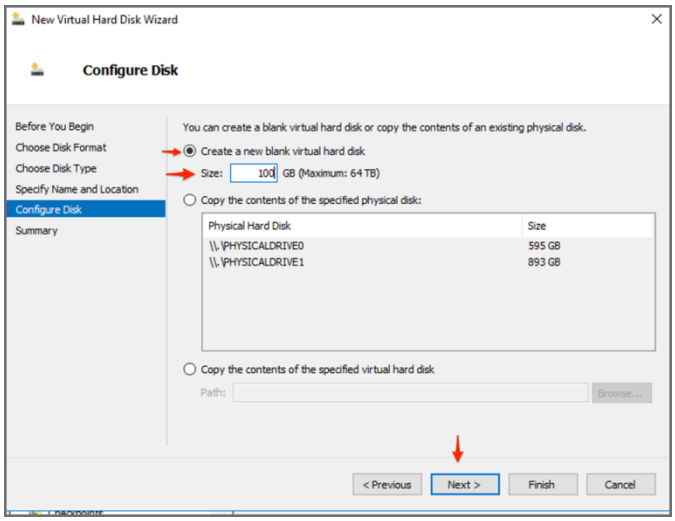
16. Choose Disk Type (**Dynamically expanding**) and click **Next**.



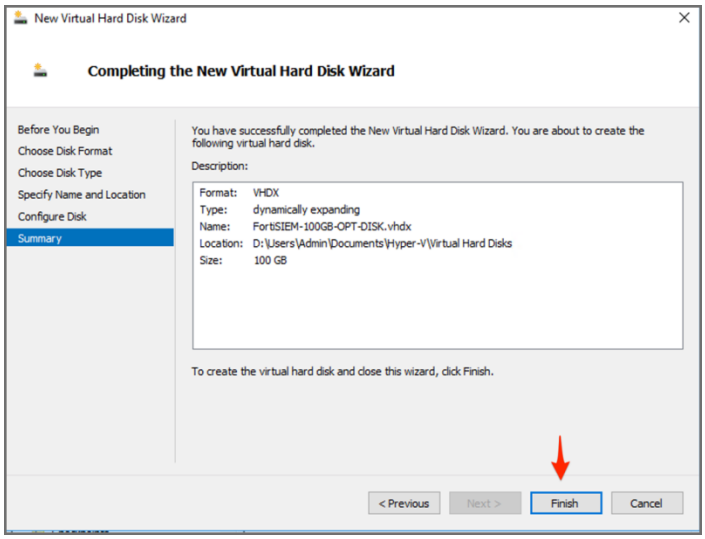
17. Specify the **Name** and **Location** of the disk. Click **Next**.



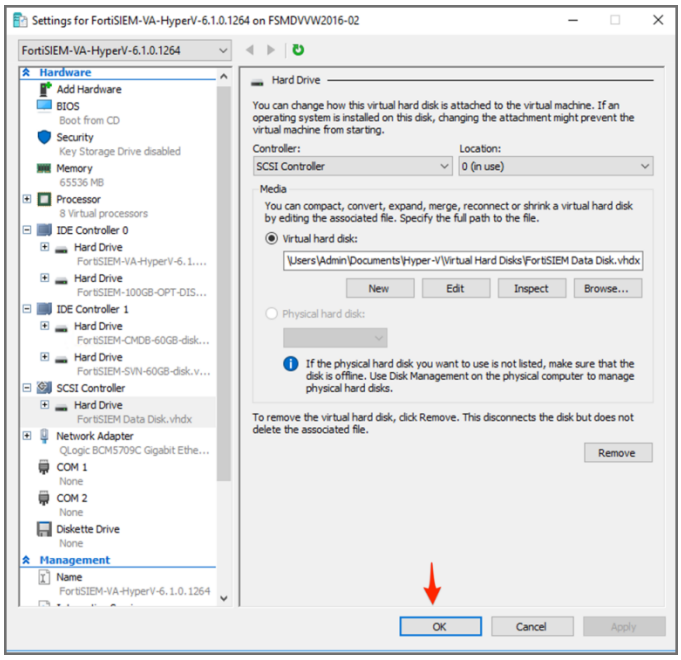
18. Specify 100GB as the size of the disk (for `/opt`). For other disks, specify size accordingly. Click **Next**.



19. Click **Finish**.

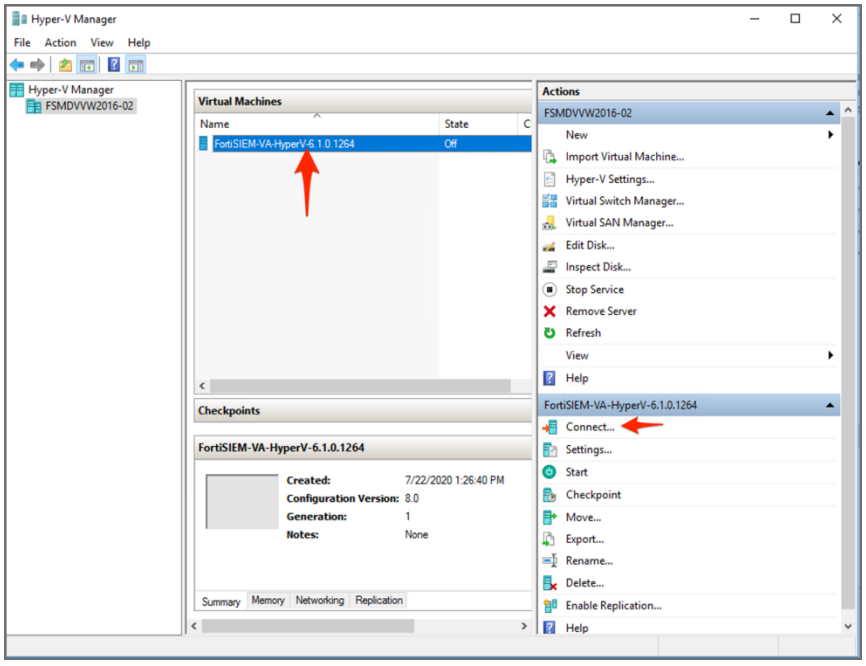


20. **IMPORTANT**: Similarly, add a 60GB CMDB disk, a 60GB SVN disk to **IDE Controller 1**. Delete the CD Drive that was added by default. If you need to use local data disk, then add a Hard Disk on the SCSI Controller of the appropriate size. Once all this is done, click **OK**.

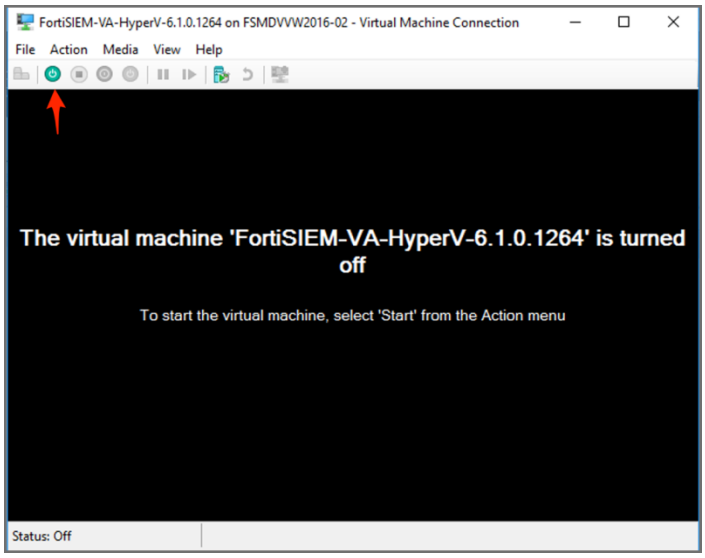


Start FortiSIEM from Hyper-V Manager

1. In Hyper-V Manager, select the Supervisor, Worker, or Collector virtual machine.
2. Click **Connect**.



3. Click the **Power On Icon** as illustrated.



4. The system will boot up. When the command prompt window opens, log in with the default login credentials: User `root` and Password `ProspectHills`.
5. You will be required to change the password. Remember this password for future use.

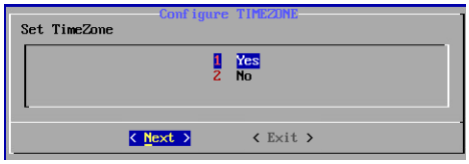
At this point, you can continue configuring FortiSIEM by using the GUI.

Configure FortiSIEM

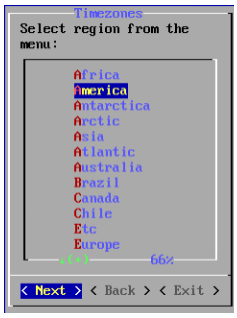
At no stage of the installation process is it required that users manually format the disks. FortiSIEM will provision the file system on disks as needed.

Follow these steps to configure FortiSIEM by using a simple GUI.

1. Log in as user `root` with the password you set in **Start FortiSIEM from Hyper-V Manager** Step 5 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
   `# configFSM.sh`
3. In VM console, select **1 Set Timezone** and then press **Next**.

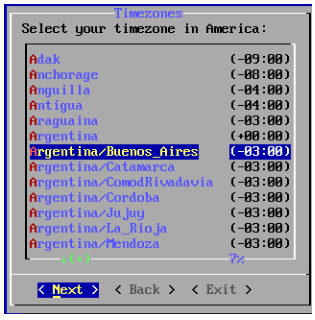


4. Select your **Region**, and press **Next**.



5. Select your **Country**, and press **Next**.

6. Select the **Country** and **City** for your timezone, and press **Next**.



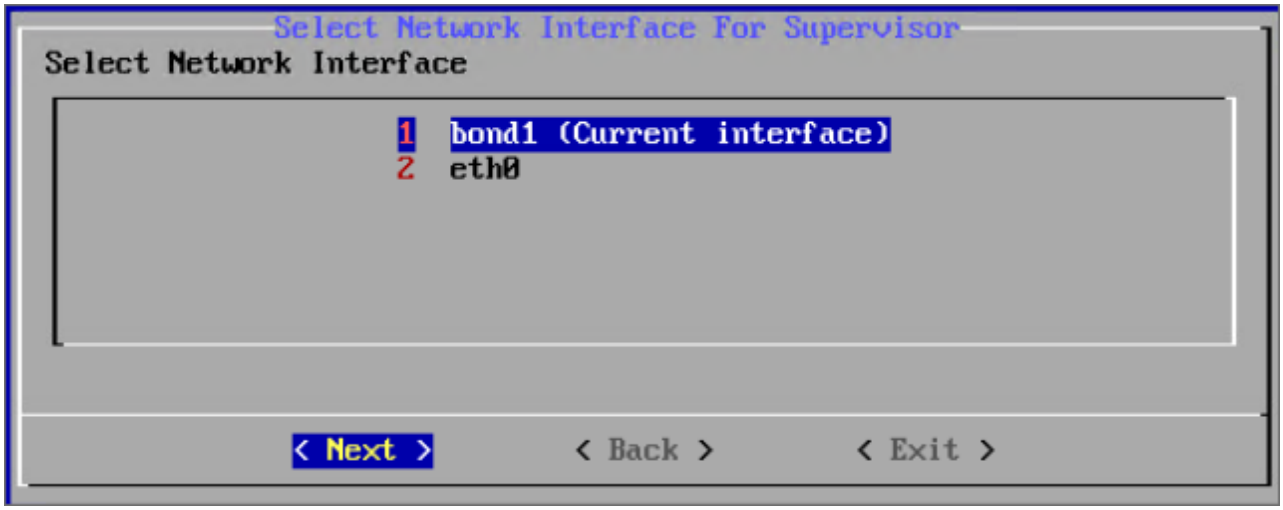
7. If installing a Supervisor, select **1 Supervisor** and press **Next**.
   If installing a Worker, select **2 Worker**, and press **Next**.
   If installing a Collector, select **3 Collector**, and press **Next**.
   If Installing FortiSIEM Manager, select **4 FortiSIEM Manager**, and press **Next**.
   If Installing FortiSIEM Supervisor Follower, select **5 Supervisor Follower** and press **Next**.
   Note: The appliance type cannot be changed once it is deployed, so ensure you have selected the correct option.

Regardless of whether you select **FortiSIEM Manager**,**Supervisor**, **Supervisor Follower**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

A dedicated ClickHouse Keeper uses a Worker, so first install a Worker and then in later steps configure the Worker as a ClickHouse Keeper.

8. Select the **Network Interface** you wish to use, and press **Next**.

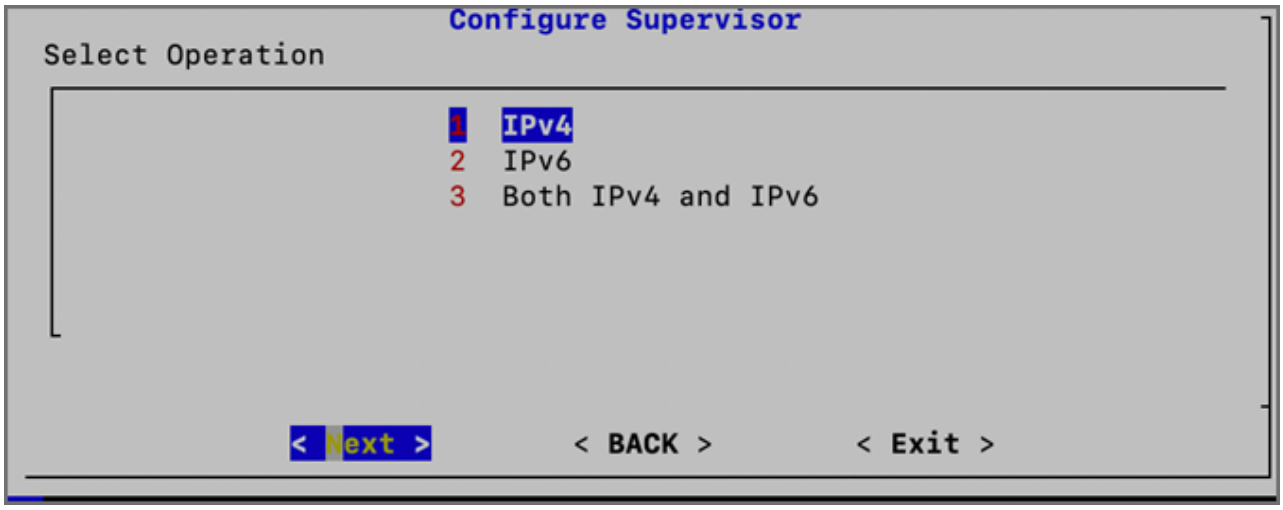
   Note: If a bond interface is configured, it will appear in the **Select Network Interface** window.



9. If you want to enable FIPS, then choose **2**. Otherwise, choose **1**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.

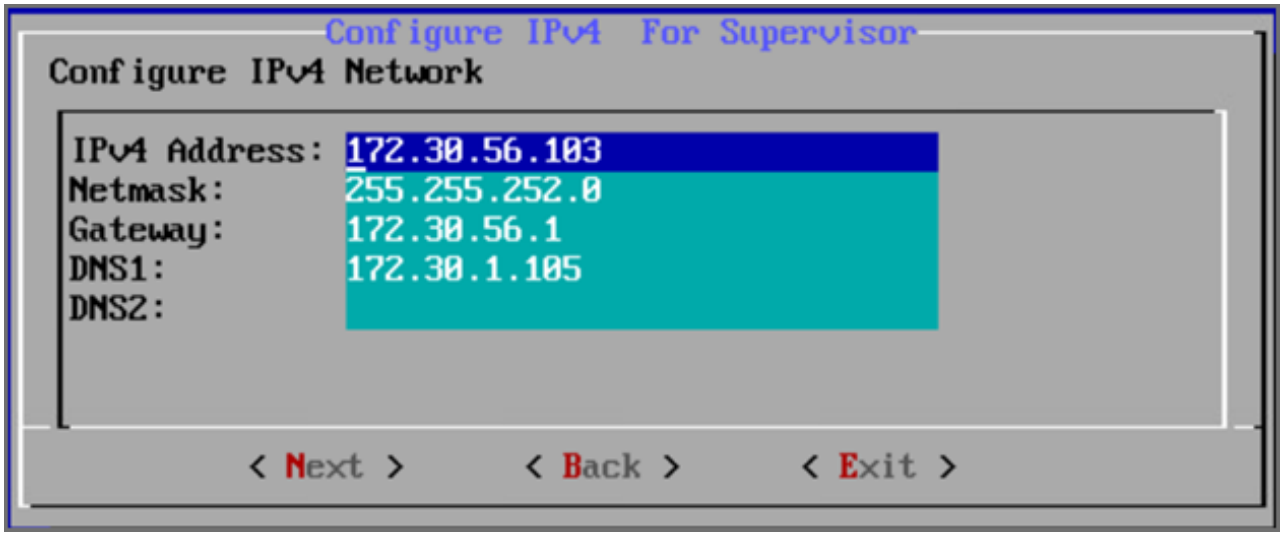
   Note: After Installation, a 5th option to change your network configuration (**5 change_network_config**) is available. This allows you to change your network settings and/or host name.

10. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



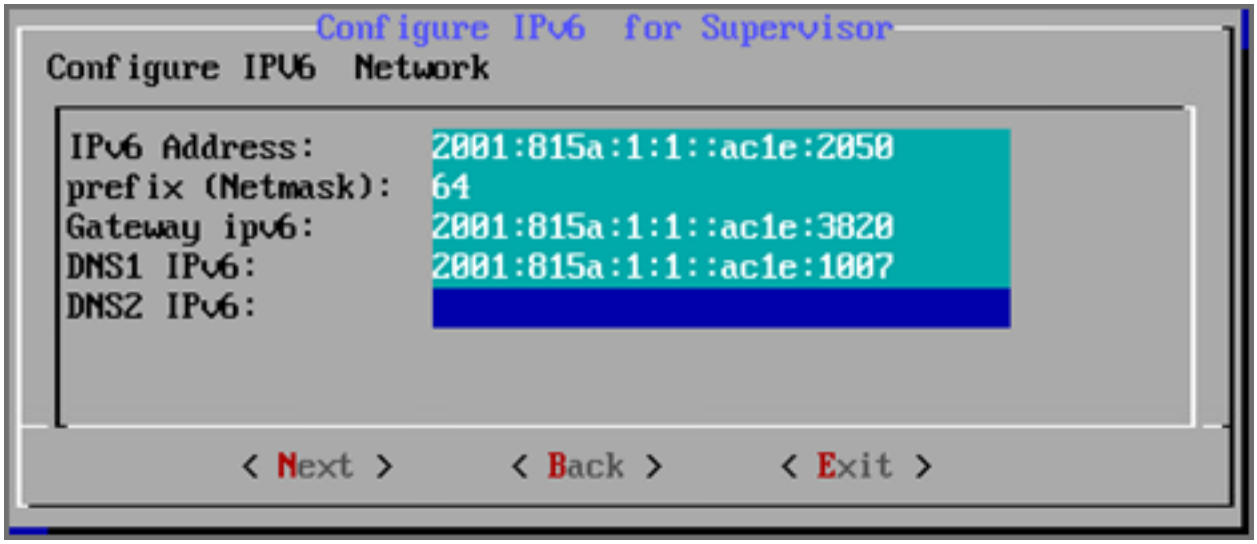
11. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 12. If you choose **2** (IPv6), and press **Next**, then skip to step 13.
12. Configure the network by entering the following fields. Press **Next**.

Option	Description
IPv4 Address	The Manager/Supervisor/Worker/Collector's IPv4 address
NetMask	The Manager/Supervisor/Worker/Collector's subnet
Gateway	Network gateway address
DNS1, DNS2	Addresses of the DNS servers



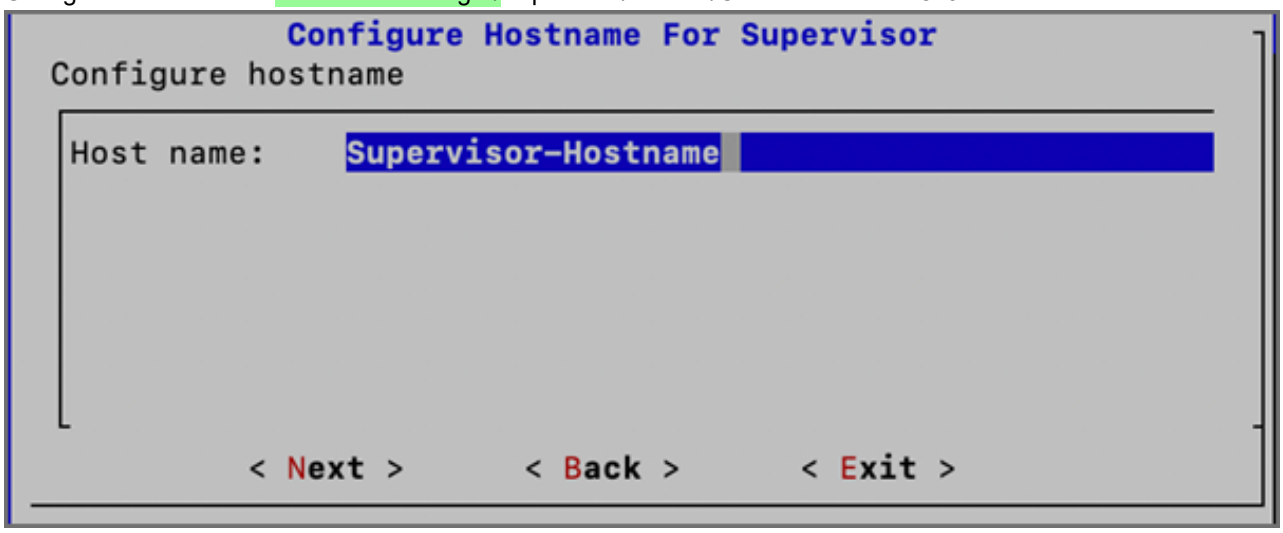
13. If you chose **1** in step 10, then you will need to skip to step 14. If you chose **2** or **3** in step 10, then you will configure the IPv6 network by entering the following fields, then press **Next**.

Option	Description
IPv6 Address	The Manager/Supervisor/Worker/Collector's IPv6 address
prefix (Netmask)	The Manager/Supervisor/Worker/Collector's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2



Note: If you chose option **3** in step 10 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration.
Note: In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

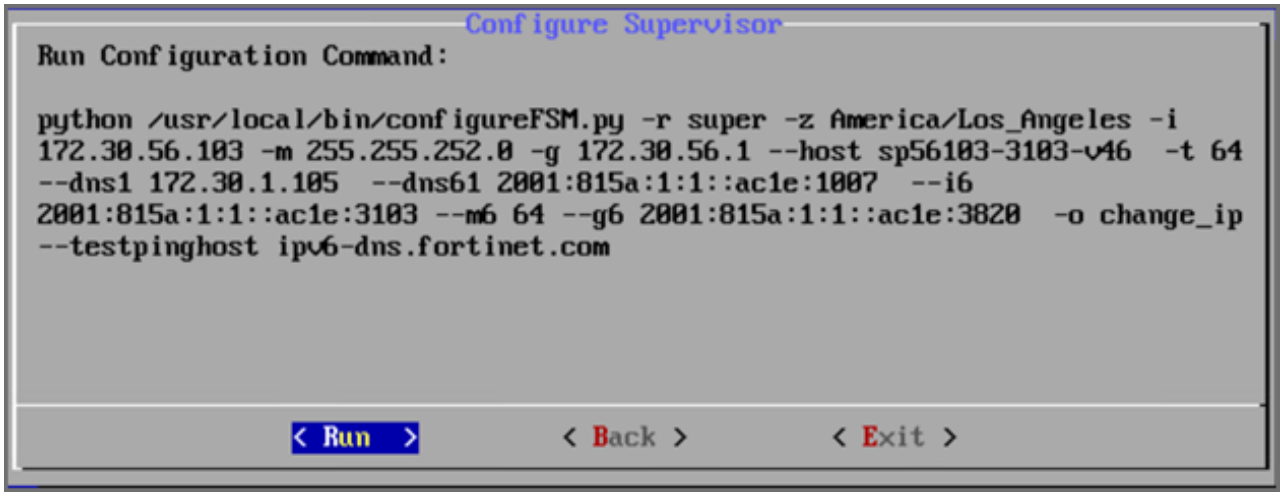
14. Configure Hostname for FortiSIEM Manager/Supervisor/Worker/Collector. Press **Next**.



Note: FQDN is no longer needed.

15. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.
Note: By default, “google.com” is shown for the connectivity test, but if configuring IPv6, you must enter an accessible internally approved IPv6 DNS server, for example: “ipv6-dns.fortinet.com"
Note: When configuring both IPv4 and IPv6, only testing connectivity for the IPv6 DNS is required because the IPV6 takes higher precedence. So update the host field with an approved IPv6 DNS server.

16. The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.



The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name

Option	Description
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either **4** (for **ipv4**) or **6** (for **v6**) or **64** (for both **ipv4** and **ipv6**). .
--dns1, --dns2	Addresses of the DNS servers
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (**install_without_fips**, **install_with_fips**, **enable_fips**, **disable_fips**, **change_network_config***) *Option only available after installation.)
--testpinghost	The URL used to test connectivity

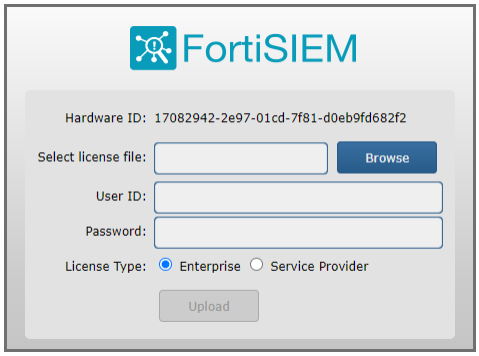
17. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

Upload the FortiSIEM License

Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the Licensing Guide.

You will now be asked to input a license.

1. Open a Web browser and log in to the FortiSIEM UI. Use link https://<*supervisor-ip*> to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input https://[*IPv6 address*] on the browser tab.
2. The License Upload dialog box will open.



3. Click **Browse** and upload the license file.
Make sure that the **Hardware ID** shown in the License Upload page matches the license.

4. For **User ID** and **Password**, choose any **Full Admin** credentials.
   For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
5. Choose **License type** as **Enterprise** or **Service Provider**.
   This option is available only for a first time installation. Once the database is configured, this option will not be available.
   For FortiSIEM Manager, **License Type** is not an available option, and will not appear. At this point, FortiSIEM Manager installation is complete. You will not be taken the Event Database Storage page, so you can skip **Configure an Event Database**.
   Note: The FortiSIEM Manager license allows a certain number of instances that can be registered to FortiSIEM Manager.
6. Proceed to Configure an Event Database.

Configure an Event Database

Choose the event database.

If the Event Database is one of the following options, additional disk configuration is required.

- **ClickHouse**: See Case 2 in Creating ClickHouse Online Storage.
  Recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- **EventDB on Local Disk**: See Case 2 in Creating EventDB Online Storage.

Final Check

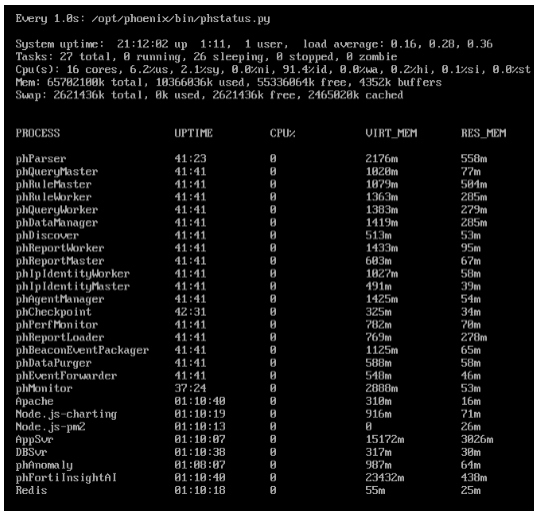
FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` if you encounter any issues during FortiSIEM installation.

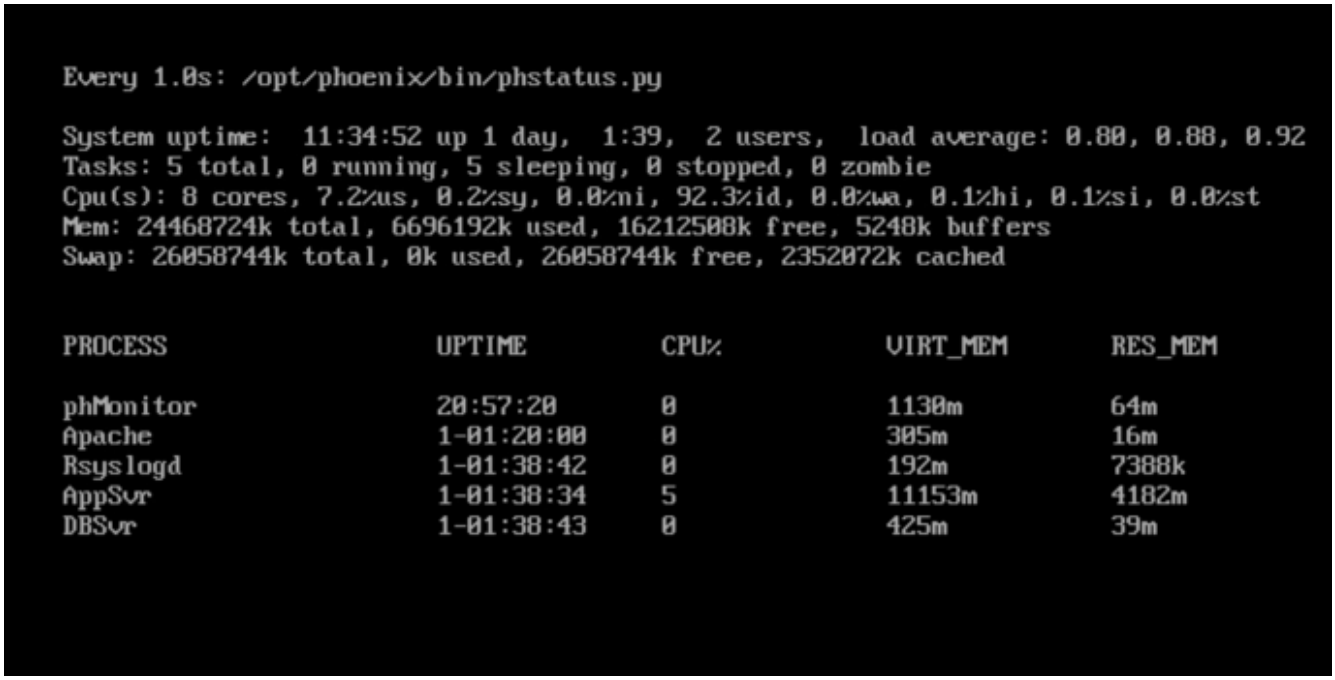
After installation completes, ensure that the `phMonitor` is up and running, for example:

```
# phstatus
```

For the Supervisor, Supervisor Follower, Worker and Collector, the response should be similar to the following.



For FortiSIEM Manager, the response should look similar to the following.



Cluster Installation

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS, ClickHouse, or Elasticsearch).

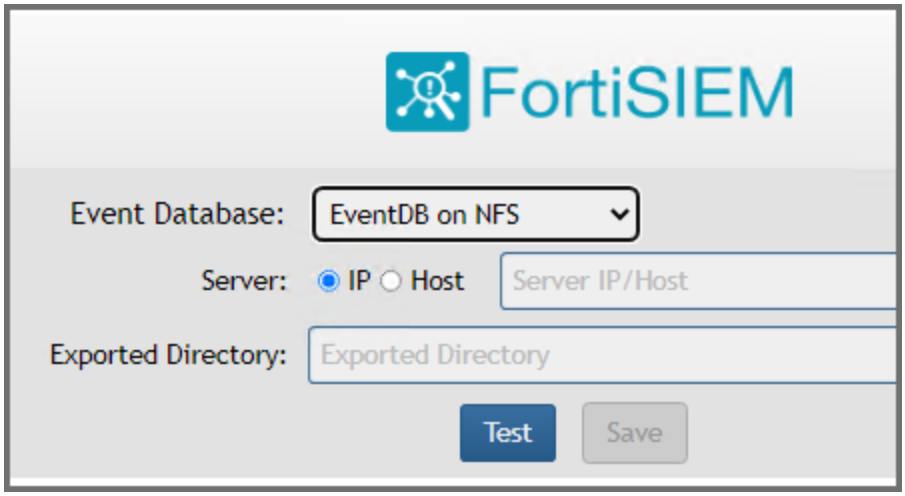
- Install Supervisor
- Install Workers
- Register Workers
- Create ClickHouse Topology (Optional)

- Install Collectors
- Register Collectors
- Install Manager
- Register Instances to Manager

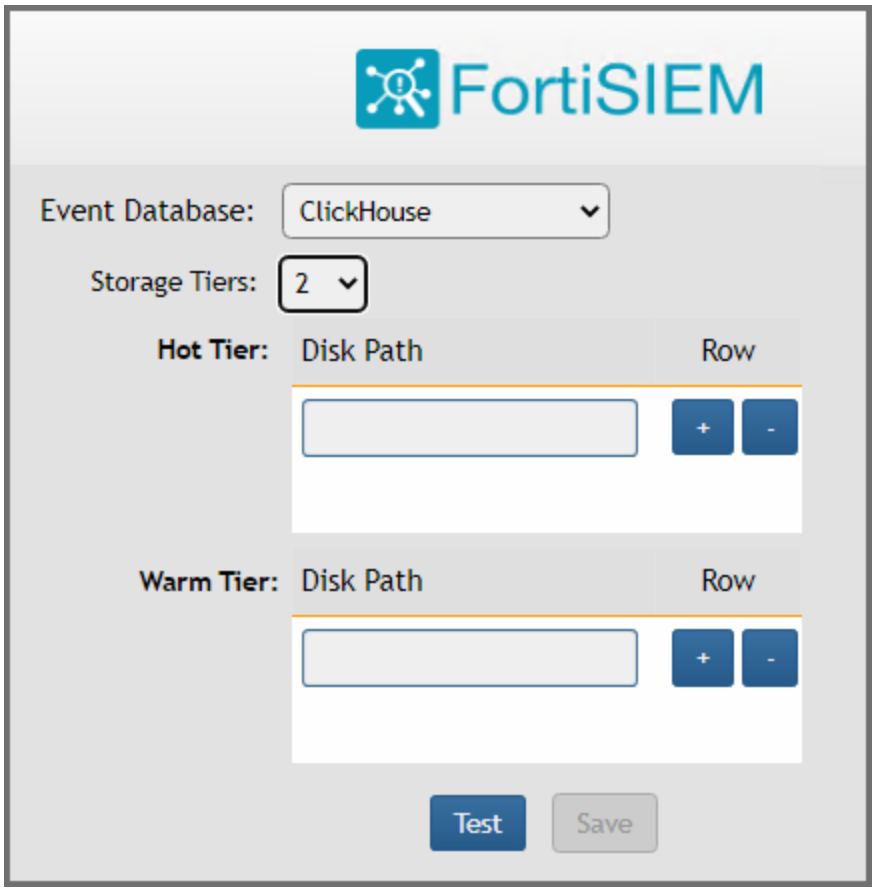
Install Supervisor

Follow the steps in All-in-one Installation, except with the following differences.

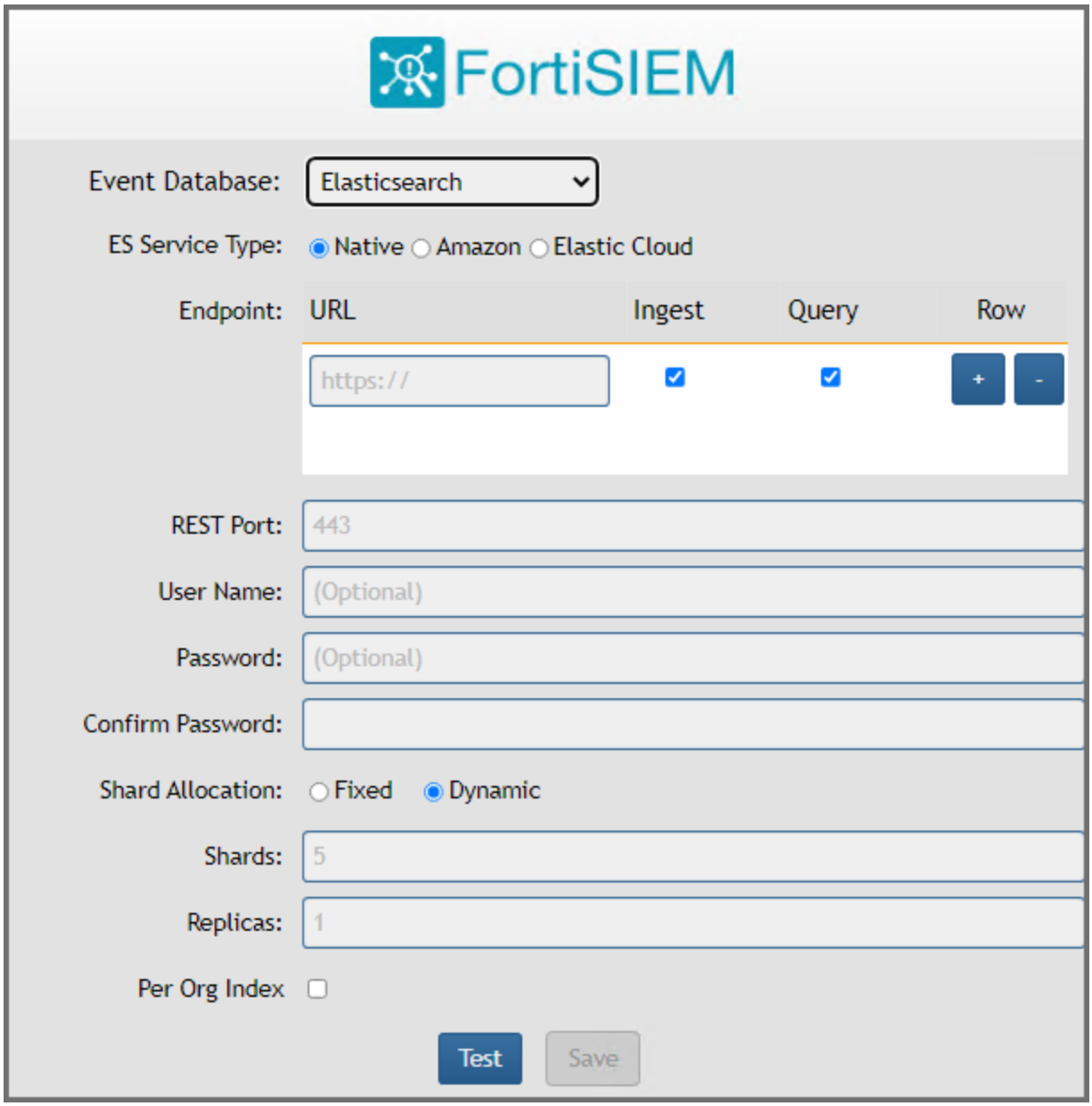
1. Event Database choices are **EventDB on NFS**, **ClickHouse**, or **Elasticsearch**.
2. If you choose **EventDB on NFS**
   a. Disk 5 is not required (From Create FortiSIEM VM in Hyper-V Step 14).
   b. You need to configure NFS after license upload.



3. If you choose **ClickHouse**
   a. You need to create disks during Create FortiSIEM VM in Hyper-V Step 14 based on the role of the Supervisor node in the ClickHouse cluster. See the ClickHouse Sizing Guide for details.
   b. You need to configure disks after license upload.



4. If you choose **Elasticsearch**, define Elasticsearch endpoints after license upload. See the Elasticsearch Sizing Guide for details.



Install Workers

Once the Supervisor is installed, take the same steps in All-in-one Installation to install a Worker with the following differences.

1. Choose appropriate CPU and memory for the Worker nodes based on Sizing guide.
2. Two hard disks for Operating Systems and FortiSIEM Application:
   - OS – 25GB
   - OPT – 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

3. If you are running ClickHouse, then create additional data disks based on the role of the Worker in ClickHouse topology. If it is a Keeper node, then a smaller disk is needed. If it is a data node, then a bigger disk is needed based on your EPS and retention policy. See ClickHouse Sizing Guide for details.

Sizing Guide References:

- ClickHouse Sizing Guide
- EventDB Sizing Guide
- Elasticsearch Sizing Guide

Register Workers

Once the Worker is up and running, add the Worker to the Supervisor node.

1. Go to **ADMIN > License > Nodes**.
2. Select Worker from the **Mode** drop-down list and enter the following information:
   a. In the **Host Name** field, enter the Worker's host name.
   b. In the **IP Address** field, enter the Worker's IP address.
   c. If you are running ClickHouse, then select the number for Storage Tiers from the **Storage Tiers** drop-down list, and input disk paths for disks in each Tier in the **Disk Path** fields.

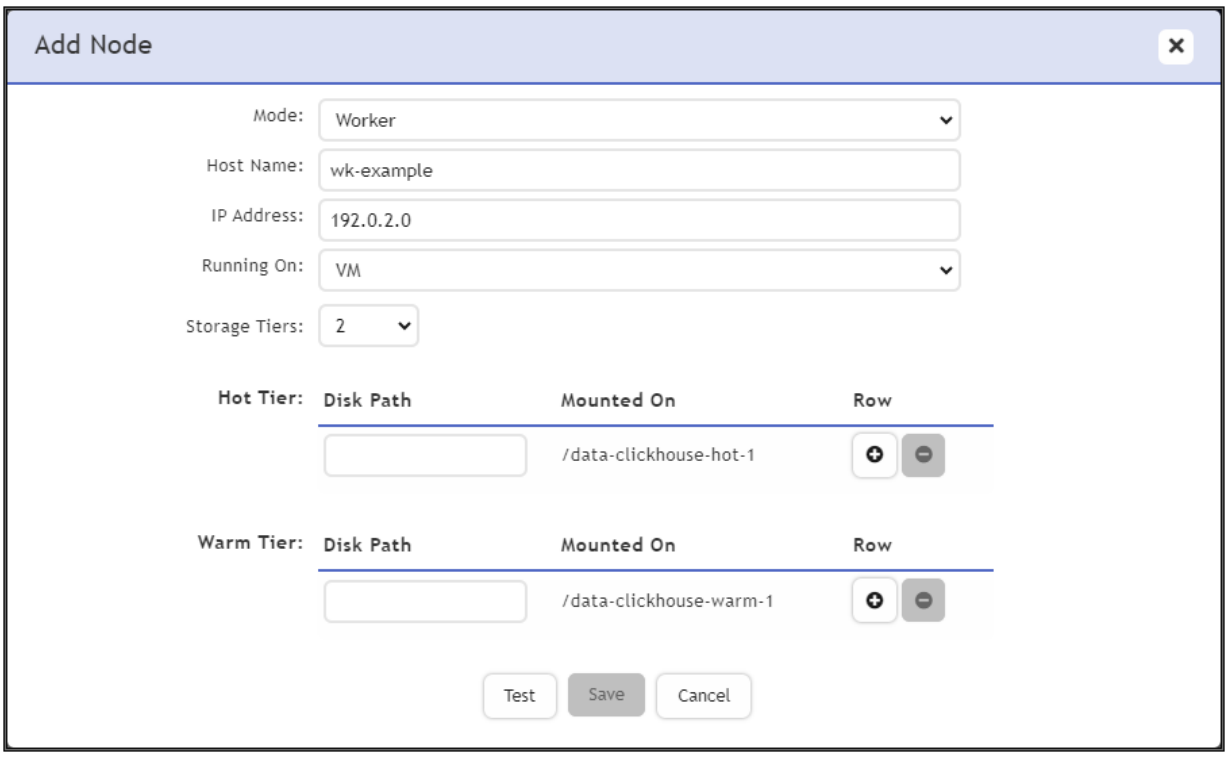
      For **Disk Path**, use one of the following CLI commands to find the disk names.

      `fdisk -l`

      or

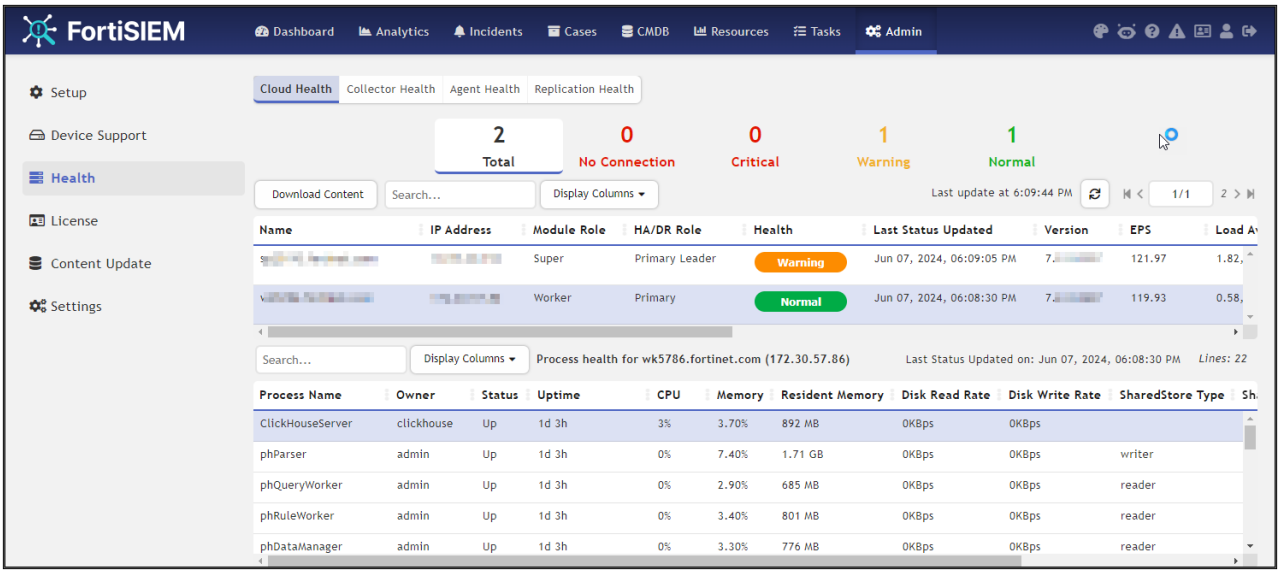
      `lsblk`

      When using `lsblk` to find the disk name, please note that the path will be `/dev/<disk>`. As an example, `/dev/vdc`.
   d. Click **Test**.



e. If the test succeeds, then click **Save**.

3. See **ADMIN > Health > Cloud Health** to ensure that the Workers are up, healthy, and properly added to the system.



Create ClickHouse Topology (Optional)

If you are running ClickHouse, you need to configure ClickHouse topology by specifying which nodes belong to ClickHouse Keeper and Data Clusters. Follow the steps in Configuring ClickHouse Topology.

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in All-in-one Install to install a Collector except in Edit FortiSIEM Hardware Settings, you need to only choose OS and OPT disks. The recommended settings for Collector node are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
  - OS – 25GB
  - OPT – 100GB
    For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

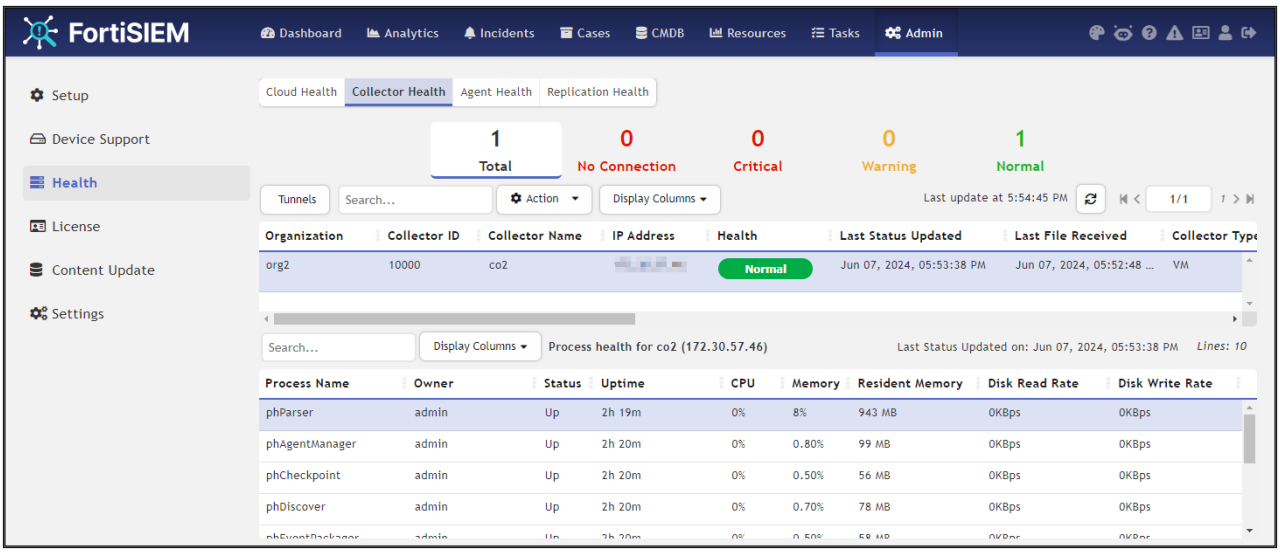
- Enterprise Deployments
- Service Provider Deployments

Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Under **Event Upload Workers**, enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **OK**.
3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>`
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.
   a. Set `user` and `password` using the admin user name and password for the Supervisor.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization`. For Enterprise deployments, the default name is Super.
   d. Set `CollectorName` from Step 3a.
   The Collector will reboot during the Registration.

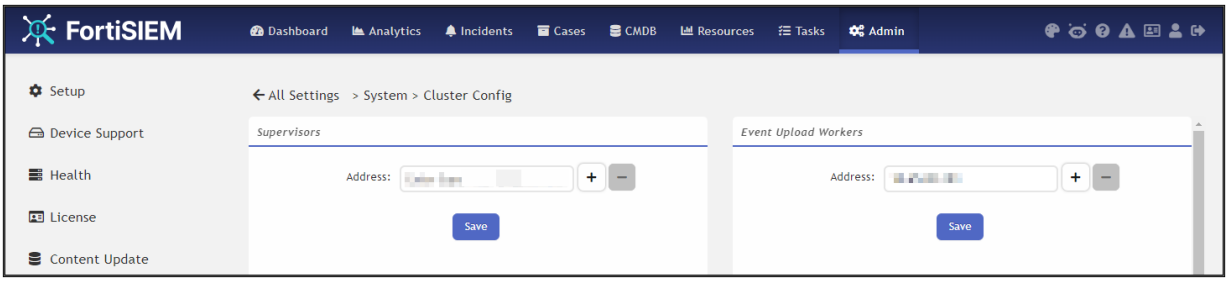
5. Go to **ADMIN > Health > Collector Health** for the status.



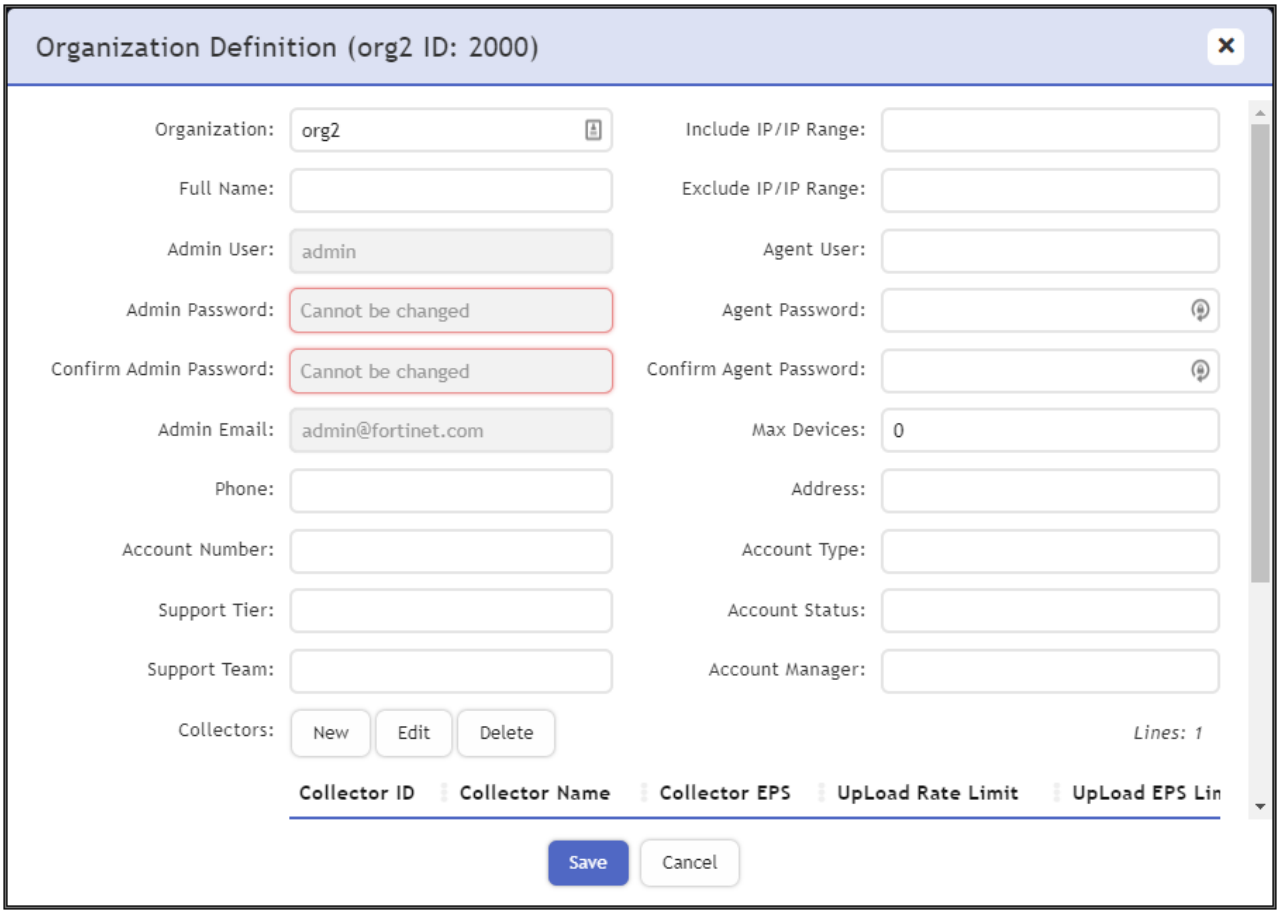
Service Provider Deployments

For Service Provider deployments, follow these steps.

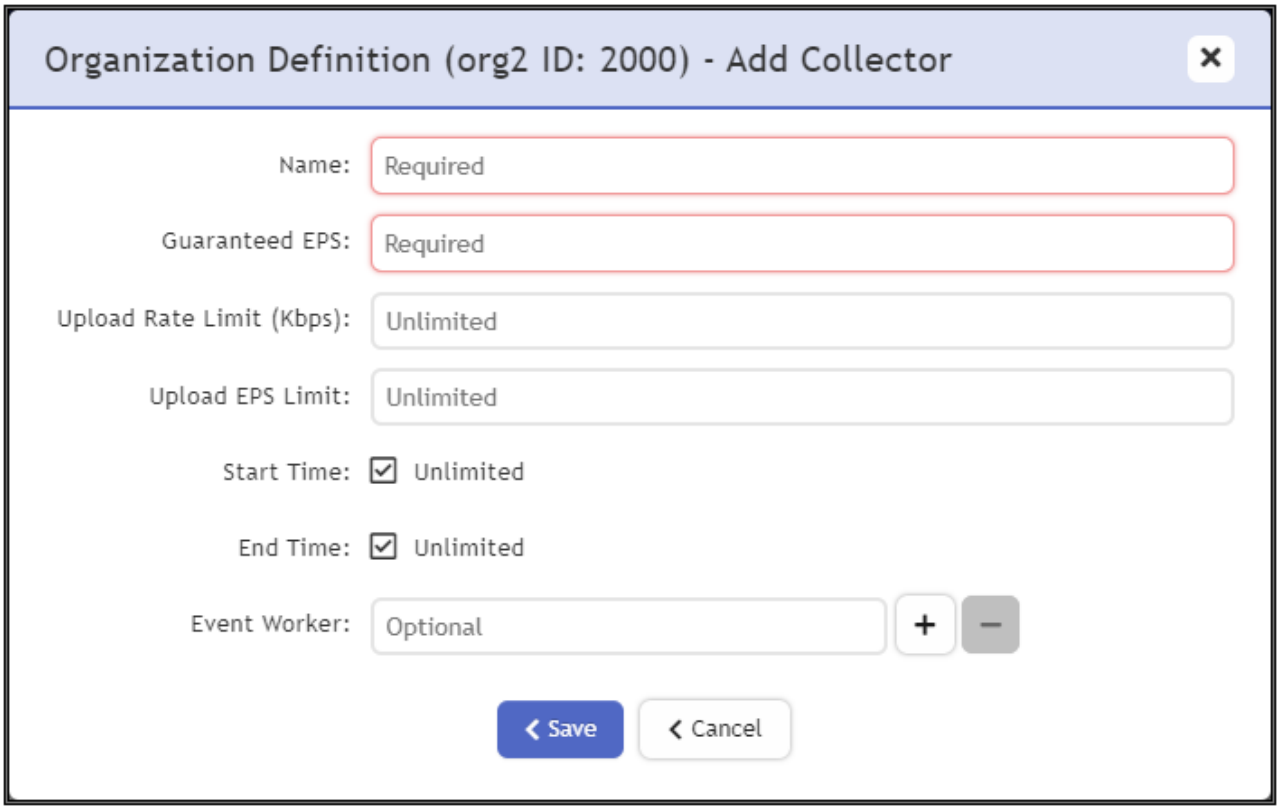
1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Under **Event Upload Workers**, enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.
   Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
   b. Click **OK**.



3. Go to **ADMIN > Setup > Organizations** and click **New** to add an Organization.



4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.



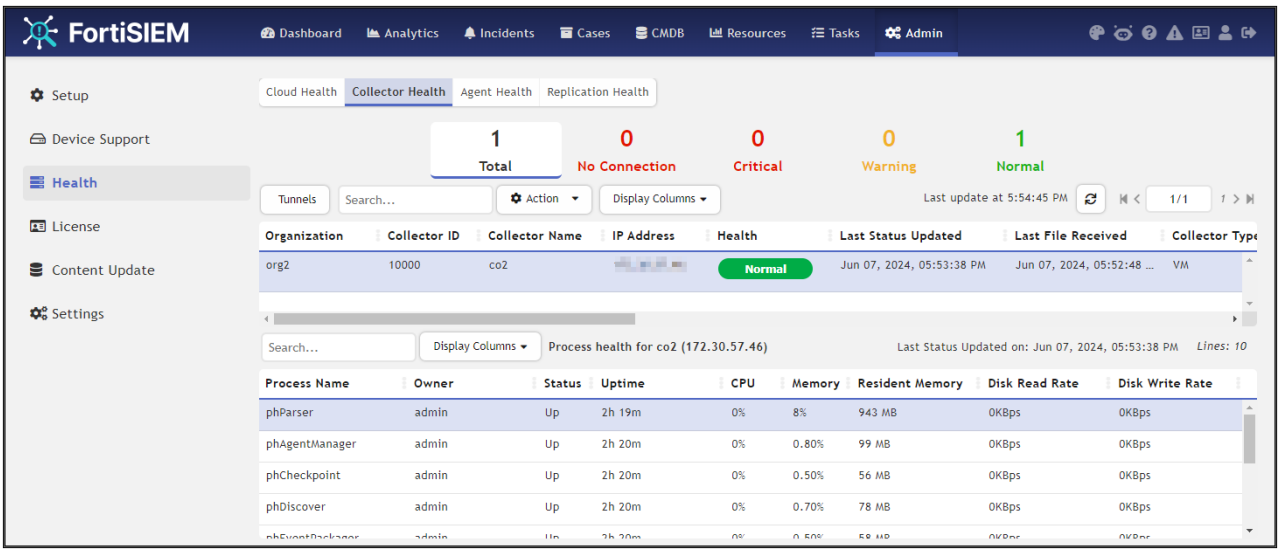
7. SSH to the Collector and run following script to register Collectors:
   `phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>`

   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.
   a. Set `user` and `password` using the admin User Name and password for the Organization that the Collector is going to be registered to.
   b. Set `Super IP or Host` as the Supervisor's IP address.
   c. Set `Organization` as the name of an organization created on the Supervisor.
   d. Set `CollectorName` from Step 6.

   ```
   [root@co574 ~]# phProvisionCollector
   Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
   [root@co574 ~]# phProvisionCollector --add admin Admin#11 172.30.57.2  ORG CO-ORG
   Continuing to provision the Collector
   This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
   [root@co574 ~]# _
   ```

   The Collector will reboot during the Registration.

8. Go to **ADMIN > Health > Collector Health** and check the status.



Install Manager

Starting with release 6.5.0, you can install FortiSIEM Manager to monitor and manage multiple FortiSIEM instances. An instance includes a Supervisor and optionally, Workers and Collectors. The FortiSIEM Manager needs to be installed on a separate Virtual Machine and requires a separate license. FortiSIEM Supervisors must be on 6.5.0 or later versions.

Follow the steps in All-in-one Install to install Manager. After any Supervisor, Workers, and Collectors are installed, you add the Supervisor instance to Manager, then Register the instance to Manager. See Register Instances to Manager.

Register Instances to Manager

To register your Supervisor instance with Manager, you will need to do two things in the following order.

- First, add the instance to Manager
- Then register the instance itself to Manager

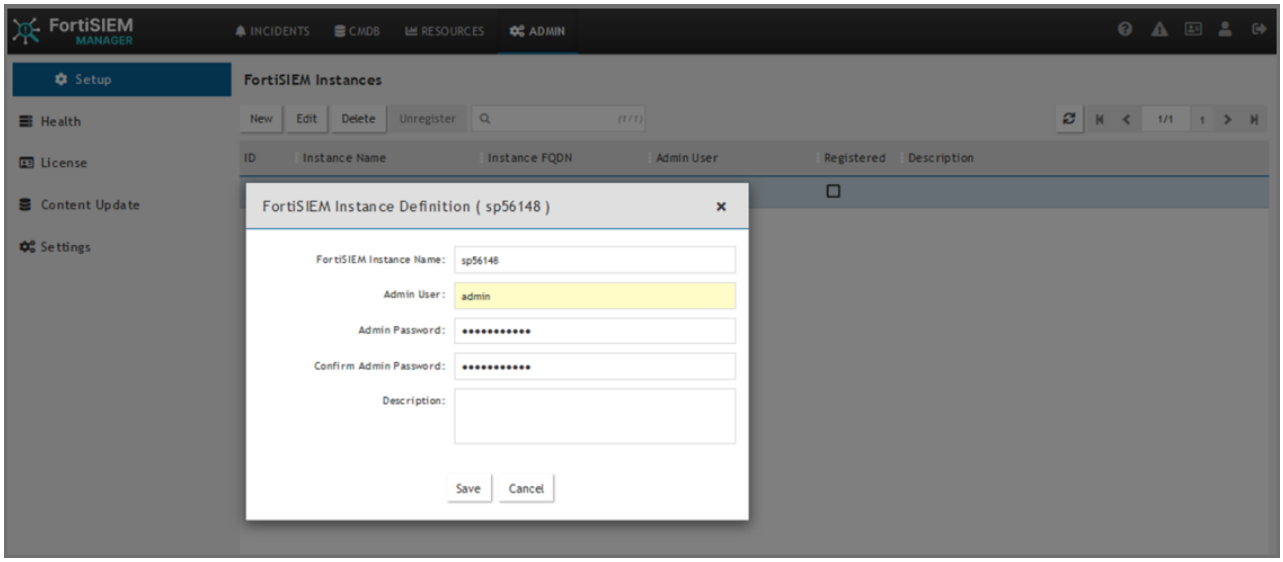
Note that Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

Adding Instance to Manager

You can add an instance to Manager by taking the following steps.
Note: Make sure to record the FortiSIEM Instance Name, Admin User and Admin Password, as this is needed when you register your instance.

1. Login to FortiSIEM Manager.
2. Navigate to **ADMIN > Setup**.
3. Click **New**.
4. In the **FortiSIEM Instance** field, enter the name of the Supervisor instance you wish to add.
5. In the **Admin User** field, enter the Account name you wish to use to access Manager.
6. In the **Admin Password** field, enter the Password that will be associated with the Admin User account.

7. In the **Confirm Admin Password** field, re-enter the Password.
8. (Optional) In the **Description** field, enter any information you wish to provide about the instance.
9. Click **Save**.

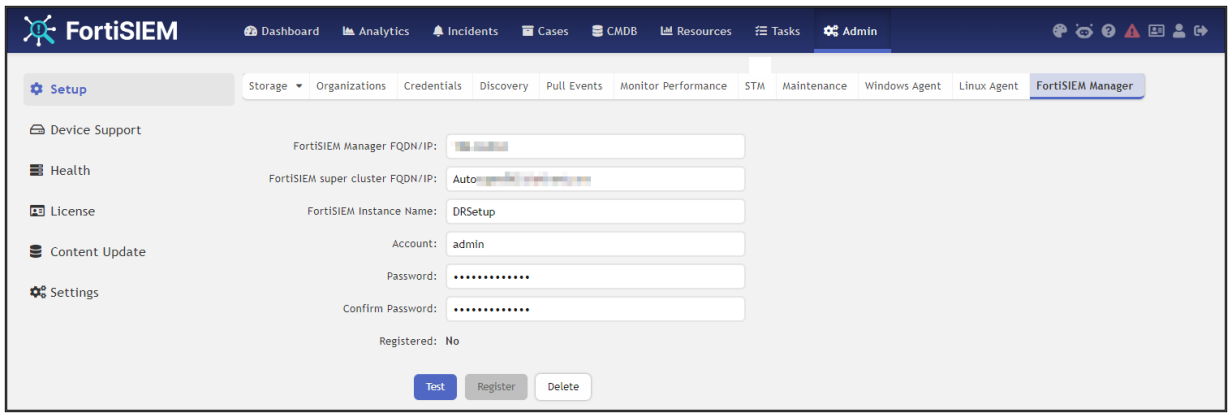


10. Repeat steps 1-9 to add any additional instances to Manager.
    Now, follow the instructions in Register the Instance Itself to Manager for each instance.

Register the Instance Itself to Manager

To register your instance with Manager, take the following steps.

1. From your FortiSIEM Supervisor/Instance, navigate to **ADMIN > Setup > FortiSIEM Manager**, and take the following steps.
   a. In the **FortiSIEM Manager FQDN/IP** field, enter the FortiSIEM Manager Fully Qualified Domain Name (FQDN) or IP address.
   b. If the Supervisor is under a Supervisor Cluster environment, in the **FortiSIEM super cluster FQDN/IP** field, enter the Supervisor Cluster Fully Qualified Domain Name (FQDN) or IP address.
   c. In the **FortiSIEM Instance Name** field, enter the instance name used when adding the instance to Manager.
   d. In the **Account** field, enter the Admin User name used when adding the instance to Manager.
   e. In the **Password** field, enter your password to be associated with the Admin User name.
   f. In the **Confirm Password** field, re-enter your password.
   g. Click **Test** to verify the configuration.
   h. Click **Register**.
   A dialog box displaying "Registered successfully" should appear if everything is valid.



i. Login to Manager, and navigate to any one of the following pages to verify registration.
   - **ADMIN > Setup** and check that the box is marked in the **Registered** column for your instance.
   - **ADMIN > Health**, look for your instance under FortiSIEM Instances.
   - **ADMIN > License**, look for your instance under FortiSIEM Instances.

Install Log

The install ansible log file is located here: `/usr/local/fresh-install/logs/ansible.log`.

Errors can be found at the end of the file.

www.fortinet.com