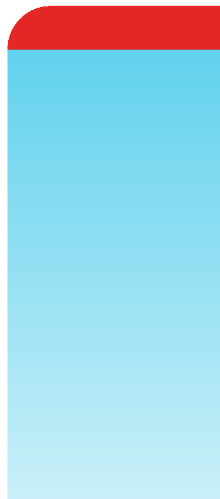


Hyper-V Installation Guide

FortiSIEM 6.3.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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 CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



10/04/2023

FortiSIEM 6.3.2 Hyper-V Installation Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Download Compressed FortiSIEM VHDX File	6
Create FortiSIEM VM in Hyper-V	7
Start FortiSIEM from Hyper-V Manager	16
Configure FortiSIEM via GUI	17
Upload the FortiSIEM License	23
Choose an Event Database	23
Cluster Installation	24
Install Supervisor	24
Install Workers	26
Register Workers	26
Install Collectors	27
Register Collectors	27
Install Log	31

Change Log

Date	Change Description
05/09/2018	Initial version of FortiSIEM - Hyper-V Installation Guide
03/29/2019	Revision 1: updated instructions for registering on a Supervisor node.
08/20/2019	Revision 2: Updated the location of the image download site.
09/13/2019	Revision 3: FortiSIEM now supports Hyper-V on Microsoft Windows 2012 R2.
11/20/2019	Release of FortiSIEM - Hyper-V Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - Hyper-V Installation Guide for 5.3.0.
08/15/2020	Release of FortiSIEM - HyperV Installation and Migration Guide for 6.1.0.
11/05/2020	Release of FortiSIEM - HyperV Installation and Migration Guide for 6.1.1.
12/07/2020	Revision 1: Small addition to Register Collectors.
02/04/2021	Revision 2: Migration update.
03/23/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.2.0.
04/22/2021	Revision 1: Added Install Log section.
05/07/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.2.1.
05/20/2021	Updated Create FortiSIEM VM in Hyper-V section for 6.2.x Hyper-V Installation Guides.
06/07/2021	Updated Elasticsearch screenshot for 6.2.x guides.
07/06/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.3.0.
08/26/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.3.1.
10/15/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.3.2.
11/17/2021	Updated Register Collectors instructions for 6.x guides.
12/22/2021	Release of FortiSIEM - Hyper-V Installation Guide for 6.3.3.
08/18/2022	Updated All-in-one Installation section.
10/20/2022	Updated Register Collectors instructions for 6.x guides.

Fresh Installation

- [Pre-Installation Checklist](#)
- [All-in-one Installation](#)
- [Cluster 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.
- Deployment type – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Storage type
 - Online – Local or NFS or Elasticsearch
 - Archive – NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• 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

Node	vCPU	RAM	Local Disks
Collector	Minimum – 4 Recommended – 8 (based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

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.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

- For NFS deployment, see *FortiSIEM - NFS Storage Guide* [here](#).
- For Elasticsearch deployment, see *FortiSIEM - Elasticsearch Storage Guide* [here](#).

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.

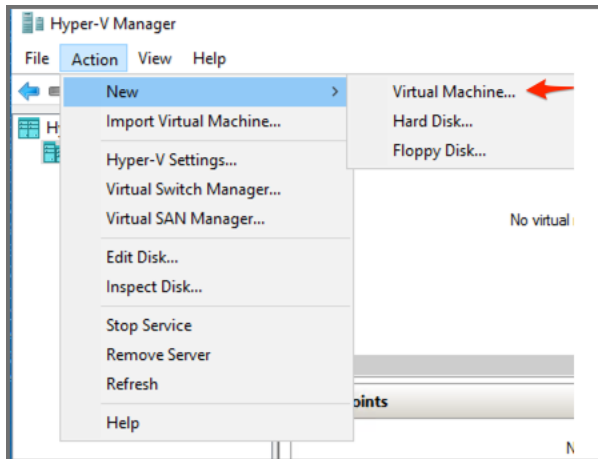
- [Download Compressed FortiSIEM VHDX File](#)
- [Create FortiSIEM VM in Hyper-V](#)
- [Start FortiSIEM from Hyper-V Manager](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Download Compressed FortiSIEM VHDX File

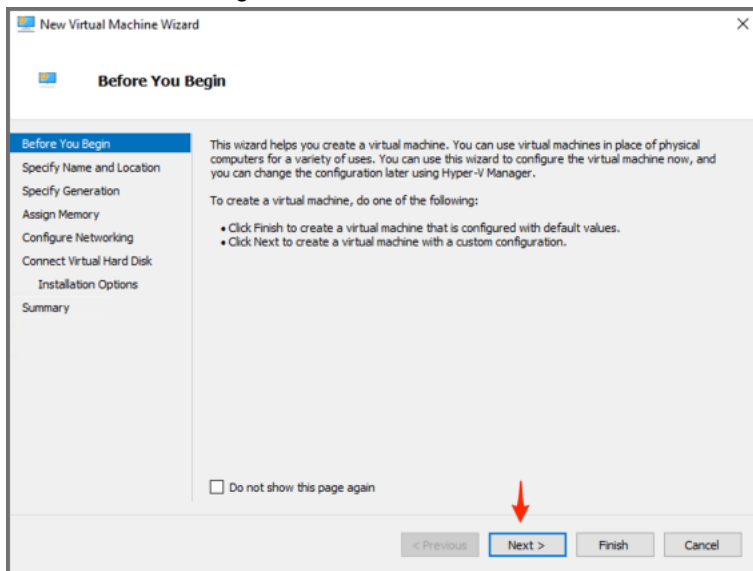
1. Go to the Fortinet Support website <https://support.fortinet.com> to download the Hyper-V package `FSM_Full_All_HYPERV_6.3.2_build0343.zip`. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Download and uncompress the all-in-one package 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

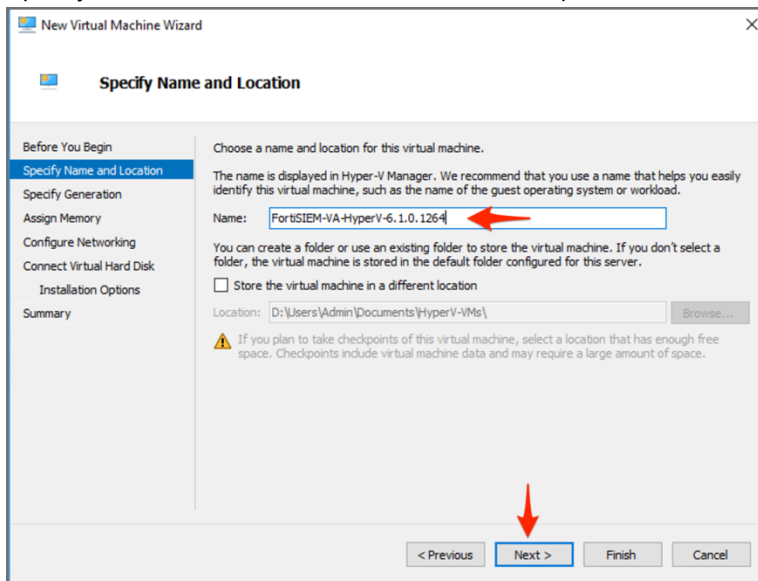
1. Launch Hyper-V Manager on your Microsoft Windows 2012 R2, 2016 or 2019 Server with Hyper-V installed.
2. Click **Action > New > Virtual Machine**, then Click **Next**.



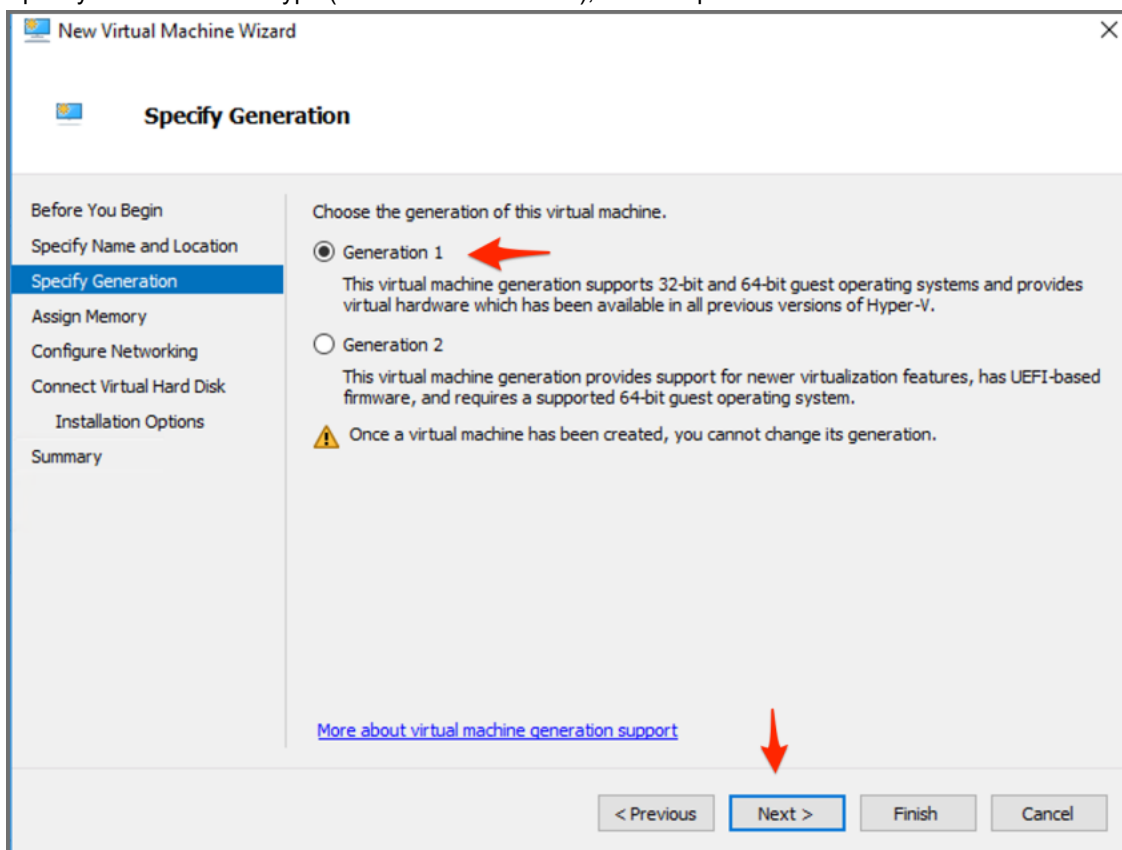
3. In the Before You Begin screen, click **Next**.



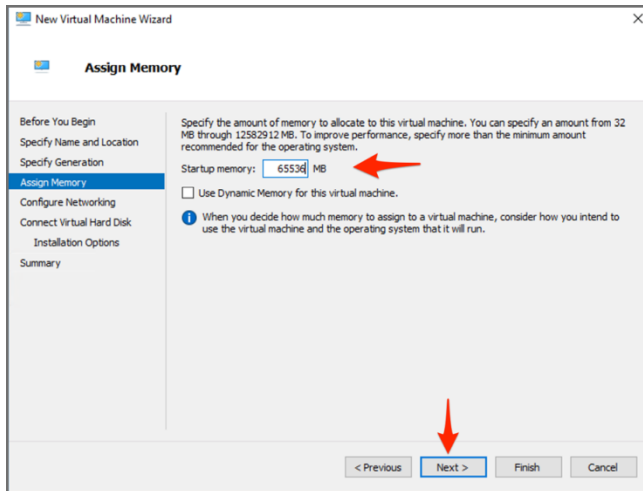
4. Specify the **Name** of the Virtual Machine, for example:



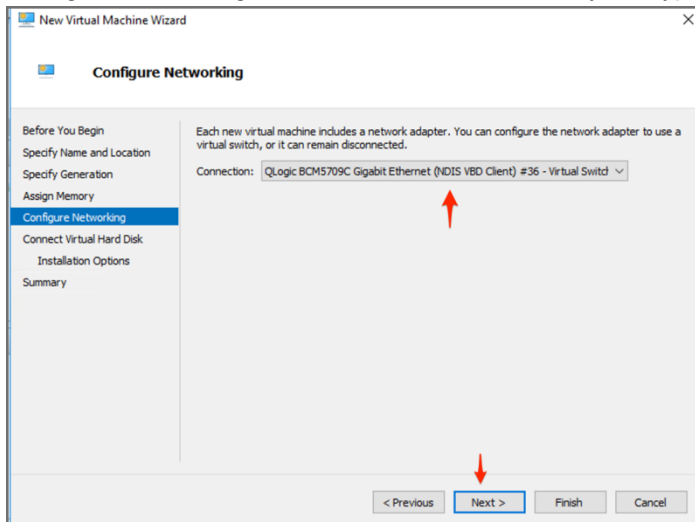
5. Specify the **Generation** type (choose **Generation 1**), for example:



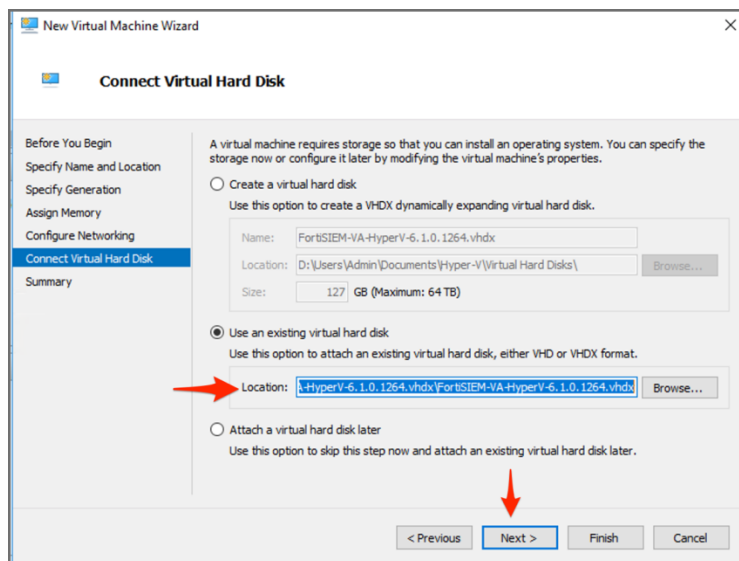
6. Add the amount of memory as per hardware requirements, then click **Next**.



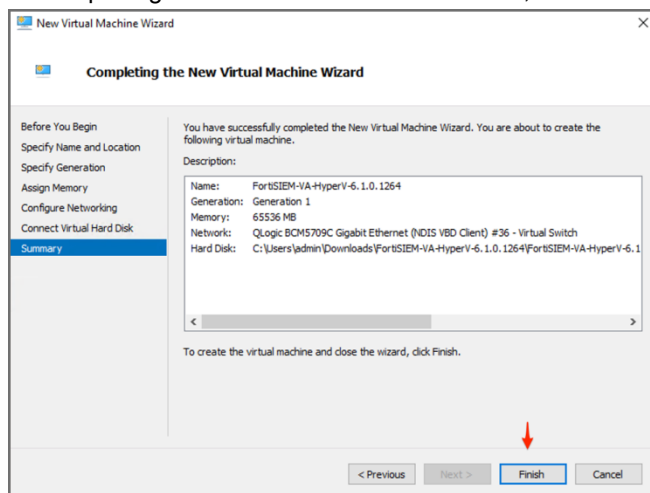
7. Configure Networking and select the virtual switch in your Hyper-V environment. Click **Next**.



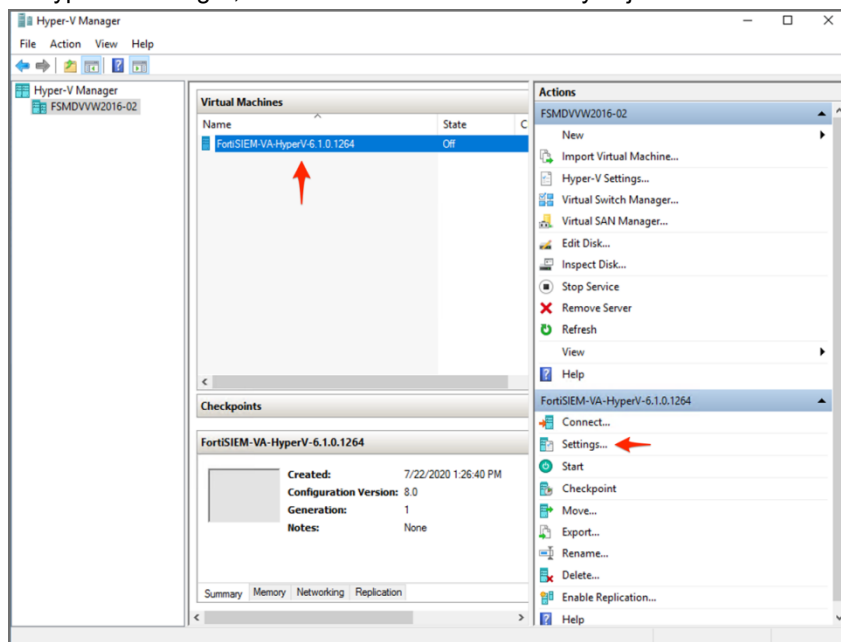
8. In Connect Virtual Hard Disk, select **Use an existing hard disk**, and choose the FortiSIEM VHDX you downloaded earlier, click **Next**:



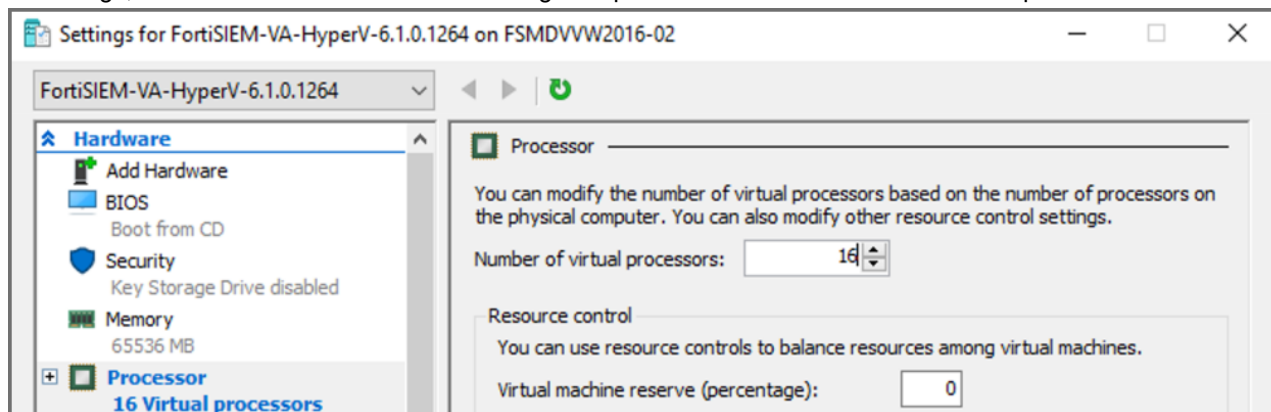
9. In Completing the New Virtual Machine Wizard, click **Finish**, for example:



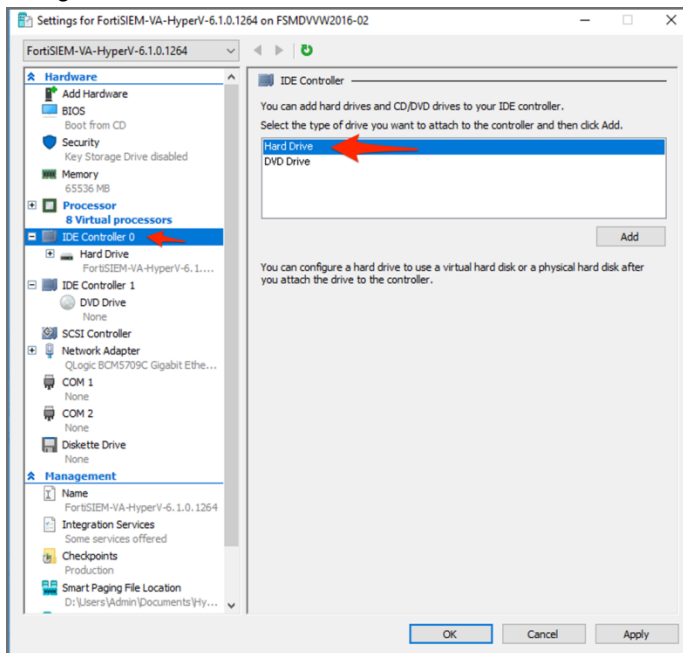
10. In Hyper-V Manager, select the virtual machine that you just created and click **Settings**, for example:



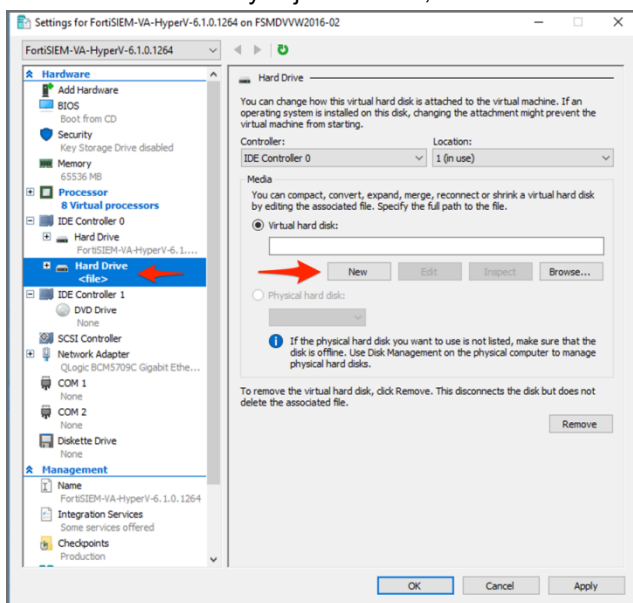
11. In Settings, select the **Processor** line in the navigation panel. Increase the number of virtual processors to **16**.



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:

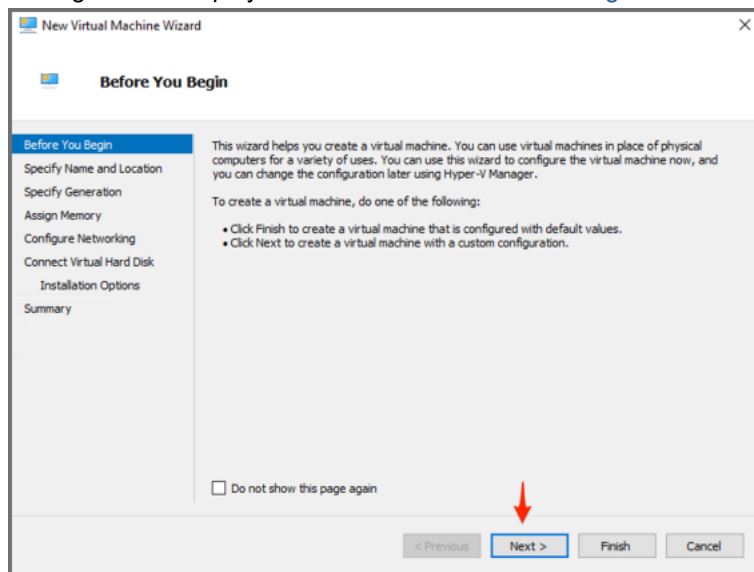
Disk	Size	Disk Name
Hard Disk 2	100GB	/opt

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	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk 5	60GB+	/data (see the following note)

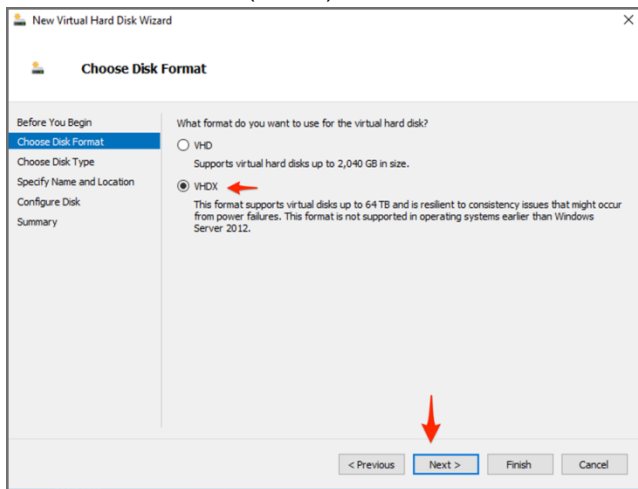
The **60GB CMDDB disk** and **60GB SVN disk** should be assigned to **IDE Controller 1**.

Note on Hard Disk 5:

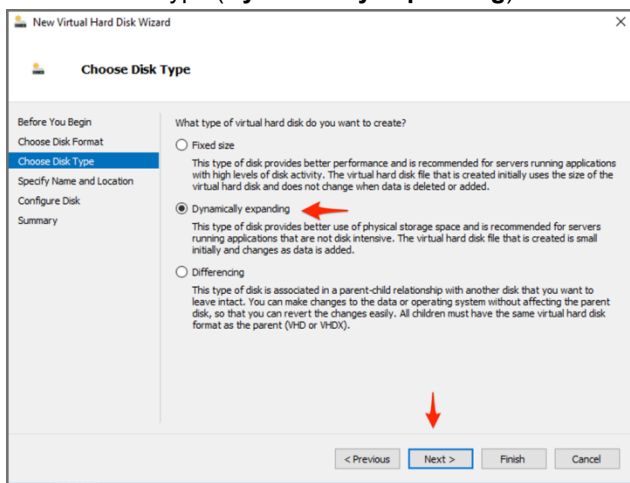
- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the [FortiSIEM Sizing Guide](#) for additional information.



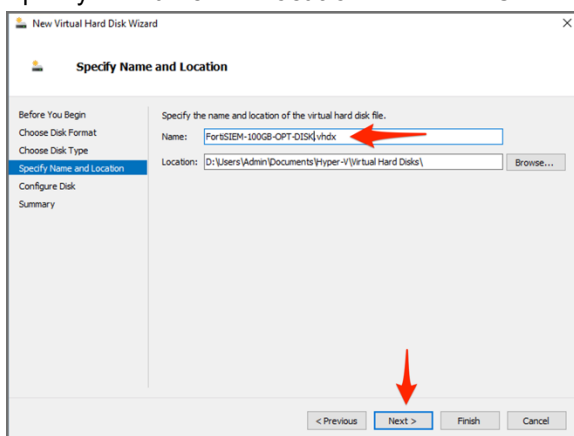
15. Choose a disk format (VHDX) and click **Next**.



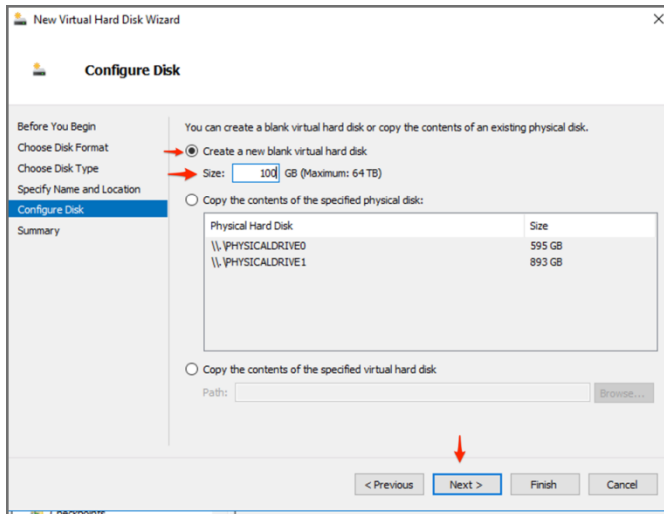
16. Choose Disk Type (**Dynamically expanding**) and click **Next**.



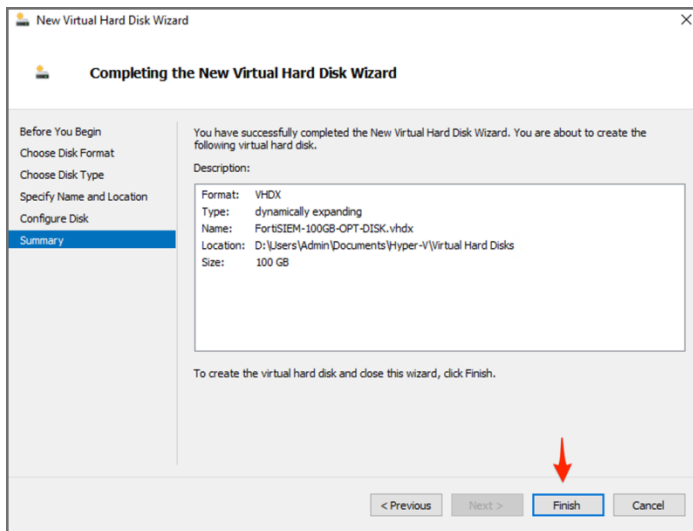
17. Specify the **Name** and **Location** of the disk. Click **Next**.



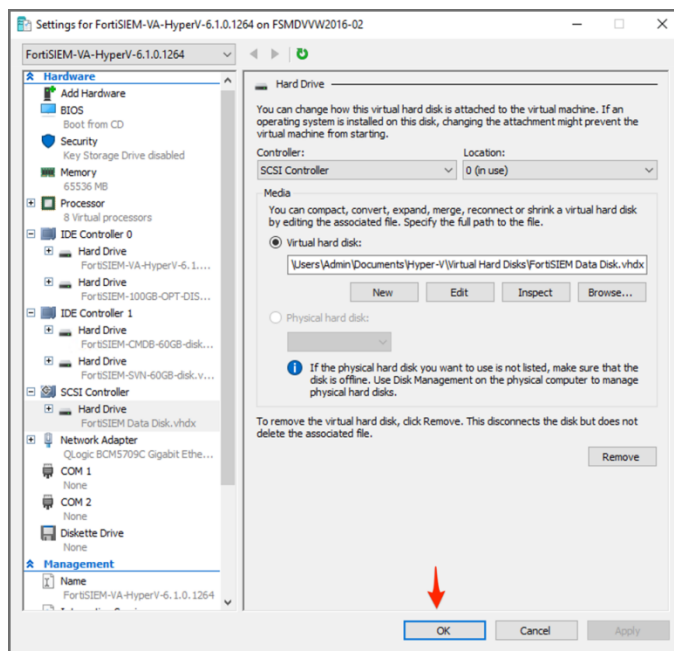
18. Specify 100GB as the size of the disk (for /opt). For other disks, specify size accordingly. Click **Next**.



19. Click **Finish**.

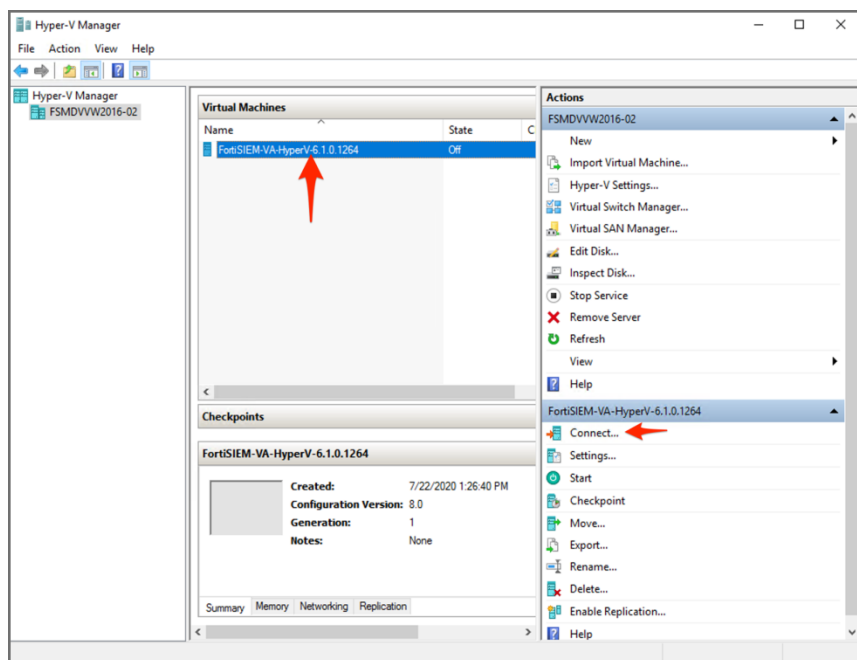


20. **IMPORTANT:** Similarly, add a 60GB CMDB disk, a 60GB SVN disk to **IDE Controller 1**. Delete the CD Drive that was added by default. If you need to use local data disk, then add a Hard Disk on the SCSI Controller of the appropriate size. Once all this is done, click **OK**.

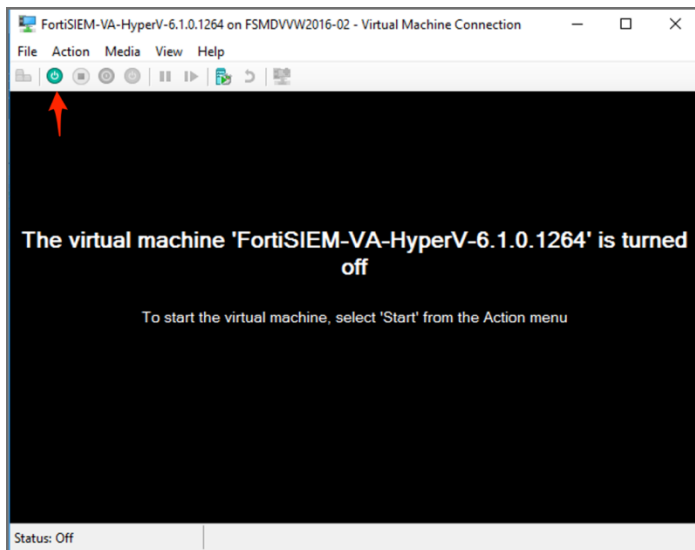


Start FortiSIEM from Hyper-V Manager

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



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



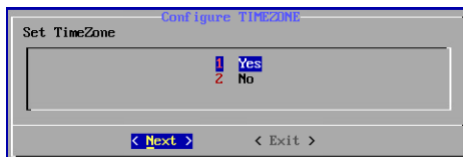
- The system will boot up. When the command prompt window opens, log in with the default login credentials: User `root` and Password `ProspectHills`.
- You will be required to change the password. Remember this password for future use.

At this point, you can continue configuring FortiSIEM by [using the GUI](#).

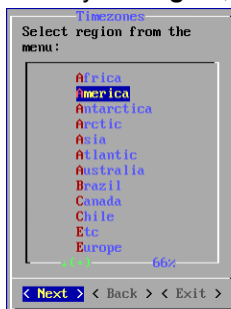
Configure FortiSIEM via GUI

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

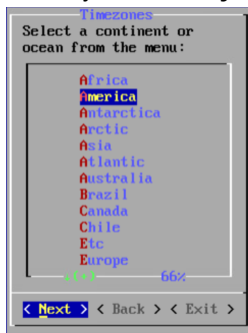
- Log in as user `root` with the password you set in **Start FortiSIEM from Hyper-V Manager** Step 5 above.
- At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`configFSM.sh`
- In VM console, select **1 Set Timezone** and then press **Next**.



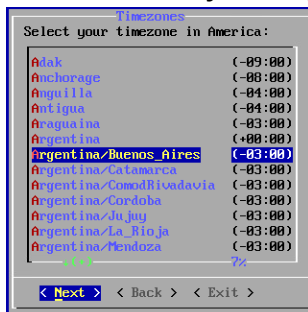
- Select your **Region**, and press **Next**.



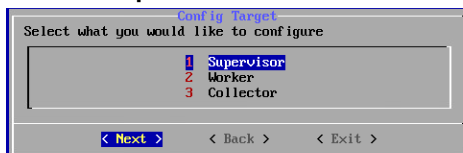
5. Select your **Country**, and press **Next**.



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



7. Select **1 Supervisor**. Press **Next**.



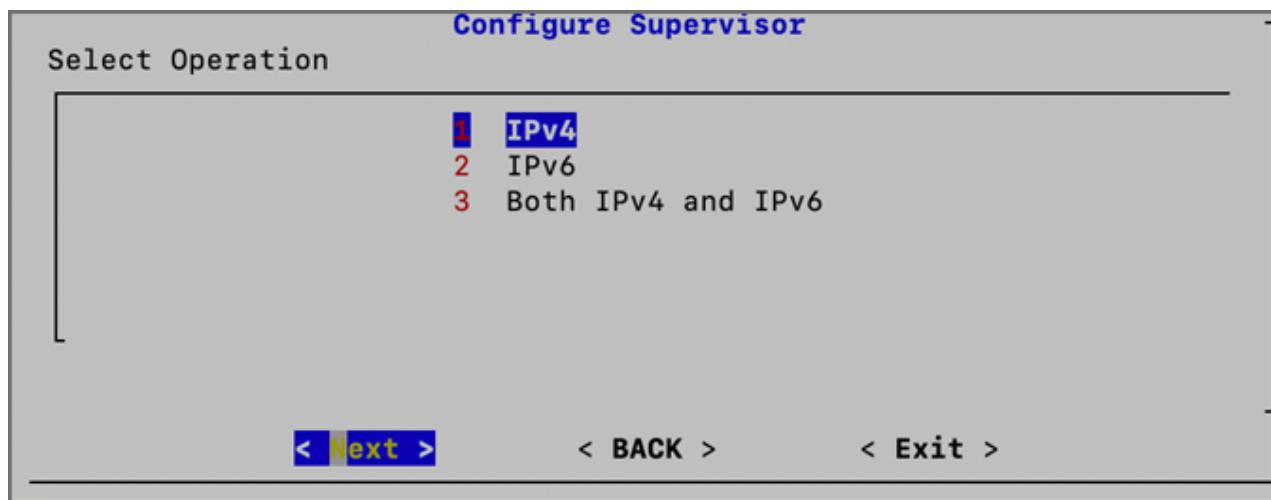
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

8. 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.



9. 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.



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

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

Configure IPv4 For Supervisor

Configure IPv4 Network

IPv4 Address: 172.30.56.103
 Netmask: 255.255.252.0
 Gateway: 172.30.56.1
 DNS1: 172.30.1.105
 DNS2:

< **Next** > < **Back** > < **Exit** >

12. If you chose **1** in step 9, then you will need to skip to step 13. If you chose **2** or **3** in step 9, then you will configure the IPv6 network by entering the following fields, then press **Next**.

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

Configure IPv6 for Supervisor

Configure IPV6 Network

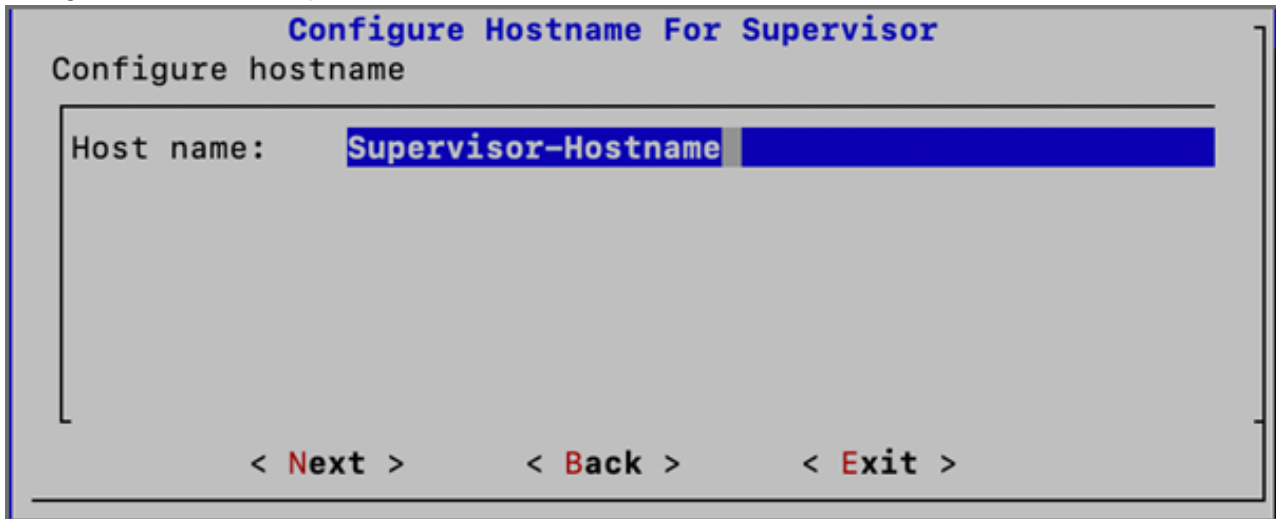
IPv6 Address: 2001:815a:1:1::ac1e:2050
 prefix (Netmask): 64
 Gateway ipv6: 2001:815a:1:1::ac1e:3820
 DNS1 IPv6: 2001:815a:1:1::ac1e:1007
 DNS2 IPv6:

< **Next** > < **Back** > < **Exit** >

Note: If you chose option **3** in step 9 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.

13. Configure Hostname for Supervisor. Press **Next**.



Configure Hostname For Supervisor

Configure hostname

Host name: **Supervisor-Hostname**

< **Next** > < **Back** > < **Exit** >

Note: FQDN is no longer needed.

14. 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.



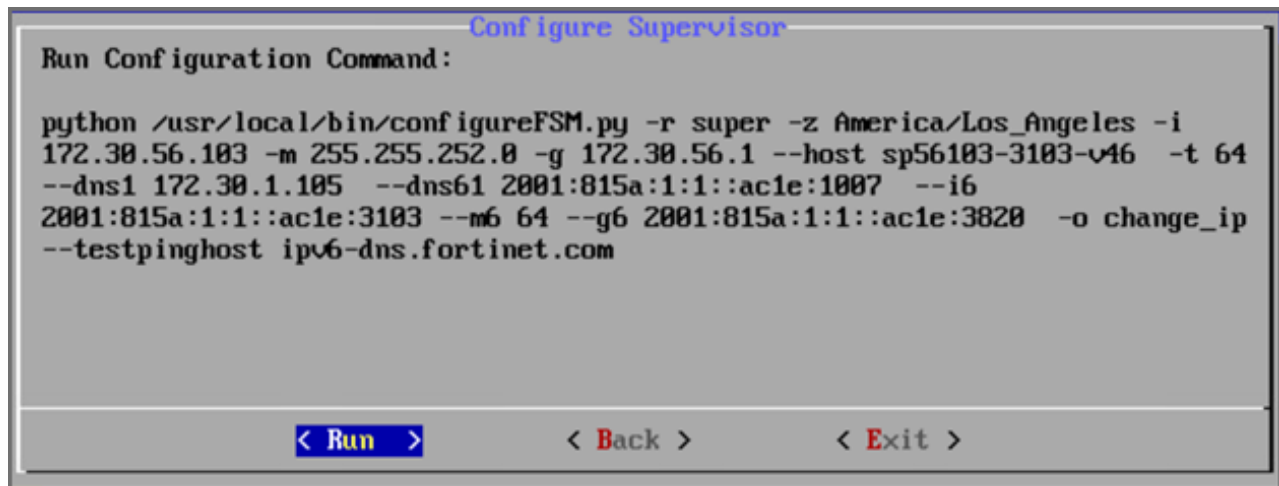
Configure Supervisor

Enter host for checking network connectivity

ipv6-dns.fortinet.com

< **Next** > < **Back** > < **Exit** >

15. 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
-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.)
-z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

16. 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.
6. Proceed to [Choose an Event Database](#).

Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see [Configuring Storage](#).

After the License has been uploaded, and the Event Database Storage setup is configured, 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
```

The response should be similar to the following.

```
Every 1.0s: /opt/phoenix/bin/phstatus.py

System uptime: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16 cores, 6.2%us, 2.1%sy, 0.0%zi, 91.4%id, 0.8%wa, 0.2%hi, 0.1%si, 0.8%st
Mem: 65782180k total, 10366836k used, 5533684k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465820k cached
```

PROCESS	UPTIME	CPU%	UPT_MEM	RES_MEM
phParser	41:23	0	2176m	550m
phQueryMaster	41:41	0	1820m	77m
phRuleMaster	41:41	0	1079m	594m
phRuleWorker	41:41	0	1363m	205m
phQueryWorker	41:41	0	1303m	279m
phDataManager	41:41	0	1419m	205m
phDiscover	41:41	0	513m	53m
phReportWorker	41:41	0	1433m	95m
phReportMaster	41:41	0	683m	67m
phIdentityWorker	41:41	0	1827m	50m
phIdentityMaster	41:41	0	491m	39m
phAgentManager	41:41	0	1425m	54m
phCheckpoint	42:31	0	325m	34m
phPerfMonitor	41:41	0	782m	70m
phReportLoader	41:41	0	769m	270m
phBeaconEventPackager	41:41	0	1125m	65m
phDataPurger	41:41	0	580m	58m
phEventForwarder	41:41	0	540m	46m
phMonitor	37:24	0	2080m	53m
apache	01:10:40	0	310m	16m
node.js-charting	01:10:19	0	916m	71m
node.js-pm2	01:10:13	0	0	26m
AppSvc	01:10:07	0	15172m	3826m
DBSvc	01:10:38	0	317m	30m
phnomaly	01:00:07	0	307m	64m
phFortiInsightAI	01:10:40	0	22432m	430m
Redis	01:10:10	0	55m	25m

Cluster Installation

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


- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

Install Supervisor

Follow the steps in [All-in-one Install](#) with two differences:

- Setting up hardware - you do not need an event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

NFS



Event Database storage:

☐ Local Disk


☒ NFS

Server IP/Host:

Exported Directory:

☐ Elasticsearch

Elasticsearch



Event Database storage:

☐ Local Disk

☐ NFS

☒ Elasticsearch

ES Service Type: ☒ Native ☐ Amazon ☐ Elastic Cloud

URL:

REST Port:

User Name:

Password:

Confirm Password:

Shard Allocation: ☐ Fixed ☒ Dynamic

Shards:

Replicas:

Per Org Index ☐

You must choose external storage listed in [Choose an Event Database](#).

Install Workers

Once the Supervisor is installed, follow the same steps in [All-in-one Install](#) to install a Worker except you need to only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

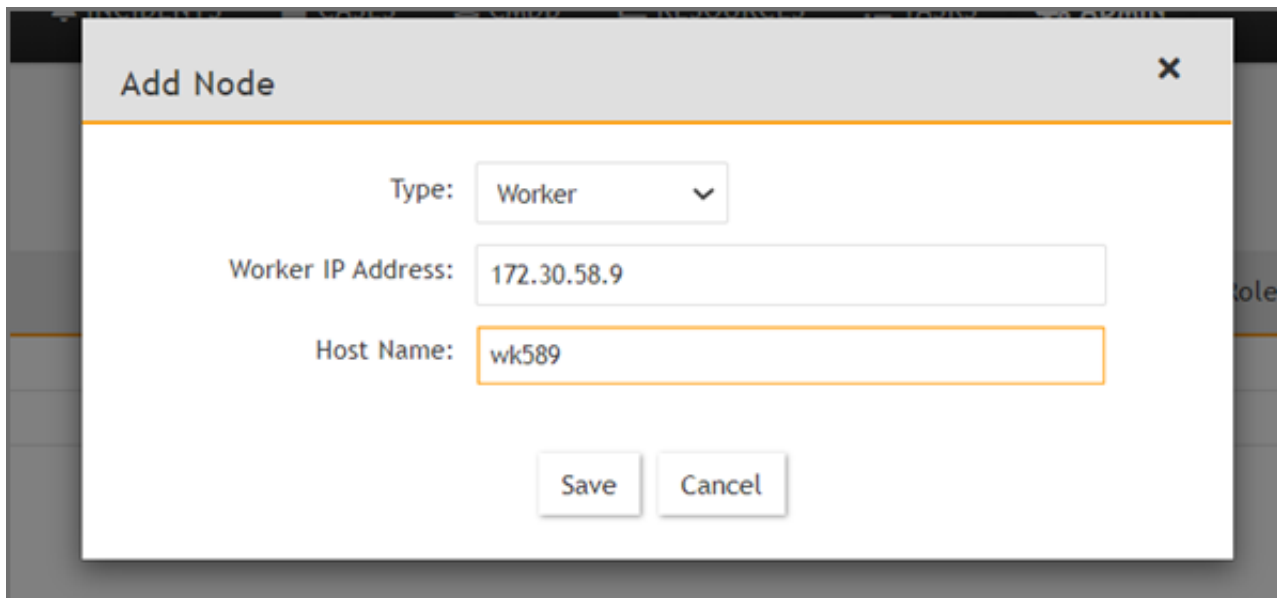
- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

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 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 drop-down list and enter the Worker's IP address and hostname. Click **Add**.



The screenshot shows a modal window titled "Add Node" with a close button (X) in the top right corner. Inside the window, there are three input fields: "Type" with a dropdown menu showing "Worker", "Worker IP Address" with the value "172.30.58.9", and "Host Name" with the value "wk589". At the bottom of the window are two buttons: "Save" and "Cancel".

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

system.

The screenshot displays the FortiSIEM Health page. On the left is a sidebar with navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area is divided into two sections. The top section, titled 'Cloud Health' and 'Collector Health', shows a table of system components. The bottom section, titled 'Process level metrics for wk573.fortinet.com (172.30.57.3)', shows a table of running processes.

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
sp572.fortinet.com	172.30.57.2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	172.30.57.3	Worker	Normal	6.1.0.1238	0.1,0.2,0.16	2%	0 KB

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
Node.js-charting	Up	1h 3m	0%	70 MB	916 MB		
httpd	Up	14m 6s	0%	16 MB	310 MB		
Redis	Up	14m 6s	0%	22 MB	51 MB		
Node.js-pm2	Up	1h 3m	0%	44 MB	899 MB		
rsyslogd	Up	1h 3m	0%	7 MB	189 MB		
phDataMaanaer	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM

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 CPU and memory settings for Collector node, and required hard disk settings 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 > Event Worker**.
 - a. 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` use 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 2a](#).

The Collector will reboot during the Registration.

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

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	172.30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Service Provider Deployments

For Service Provider deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.

2. Go to **ADMIN > Settings > System > Event Worker**.

a. 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**.

Setup ← All Settings > System > Event Worker

Device Support

Health

License

Settings

Worker Address: 172.30.57.3

Save

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

Organization Definition (ORG)

Organization: ORG Include IP/IP Range:

Full Name: Exclude IP/IP Range:

Admin User: admin Agent User:

Admin Password: Agent Password:

Confirm Admin Password: Confirm Agent Password:

Admin Email: Required Max Devices:

Phone: Address:

Account Number: Account Type:

Support Tier: Account Status:

Support Team: Account Manager:

Collectors: New Edit Delete

Collector Name	Collector EPS	UpLoad Rate Limit	Valid Start Date	Valid End Date
----------------	---------------	-------------------	------------------	----------------

Save Cancel

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.

Organization Definition (ORG) - Add Collector

Name: Required

Guaranteed EPS: Required

Upload Rate Limit (Kbps): Unlimited

Start Time: ☒ Unlimited

End Time: ☒ Unlimited

< Save < Cancel

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.

- Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
- Set `Super IP` or `Host` as the Supervisor's IP address.
- Set `Organization` as the name of an organization created on the Supervisor.
- 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.

The screenshot shows the FortiSIEM web interface. On the left is a sidebar with navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area is titled 'Collector Health' and contains two tables.

The first table, 'Collector Health', has columns: Organization, Name, IP Address, Status, Health, Up Time, CPU, Memory, Allocated EPS, Incoming EPS, Version, and Col. It shows one entry for 'Super' with 'CO-ORG' as the name, IP '172.30.57.4', status 'up', and health 'Normal'.

The second table, 'Processes', is expanded below the first. It has columns: Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. It lists several processes: phMonitorAgent, phParser, phPerfMonitor, phEventForwarder, and phDiscover, all with status 'Up'.

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

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.