



FortiSIEM - Hyper-V Installation and Migration Guide

Version 6.1.0

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 6.1.0 Hyper-V Installation and Migration 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	21
Choose an Event Database	21
Cluster Installation	22
Install Supervisor	22
Install Workers	23
Register Workers	24
Install Collectors	24
Register Collectors	25
Migrating from FortiSIEM 5.3.0, 5.3.1, or 5.3.2	29
Pre-Migration Checklist	29
Create the Directories	29
Download the Backup Script	29
Run the Backup Script and Shutdown System	30
Migrate All-in-one Installation	30
Download and Uncompress the 6.1.0 Hyper-V Root VHDX	31
Modify the 5.3.0, 5.3.1, or 5.3.2 Instance to use new VHDX	31
Migrate to FortiSIEM 6.1.0	34
Migrate Cluster Installation	38
Delete Workers	39
Migrate Supervisor	39
Install New Worker(s)	39
Register Workers	39
Set Up Collector-to-Worker Communication	39
Working with Pre-6.1.0 Collectors	39
Install 6.1.0 Collectors	40
Register 6.1.0 Collectors	40

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: Updated Migration.
20/04/2021	Revision 3: Updated Migration - Download the Backup Script.
20/05/2021	Revision 4: Updated Create FortiSIEM VM in Hyper-V section for 6.1.0 and 6.1.1 releases.
11/19/2021	Revision 5: Updated Register Collectors section for 6.1.0 and 6.1.1 releases.
08/18/2022	Revision 6: Updated All-in-one Installation section.
10/20/2022	Revision 7: 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.

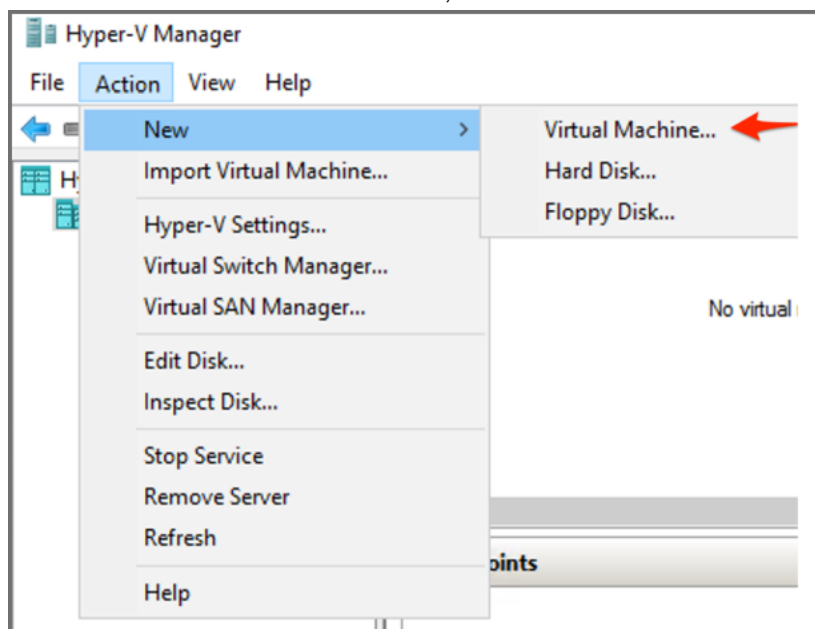
- [Download Compressed FortiSIEM VHDX File](#)
- [Create FortiSIEM VM in Hyper-V](#)
- [Start FortiSIEM from Hyper-V Manager](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

Download Compressed FortiSIEM VHDX File

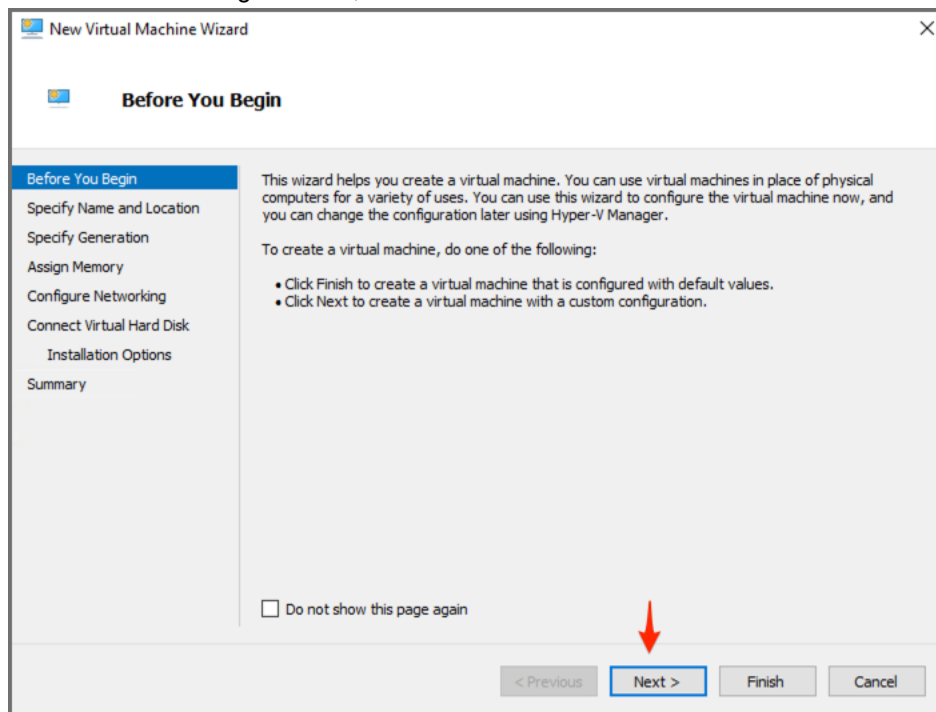
1. Go to the Fortinet Support website <https://support.fortinet.com> to download the Hyper-V package `FSM_Full_All_HYPERV_6.1.0_build0112.zip`. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Download and uncompress the all-in-one package 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

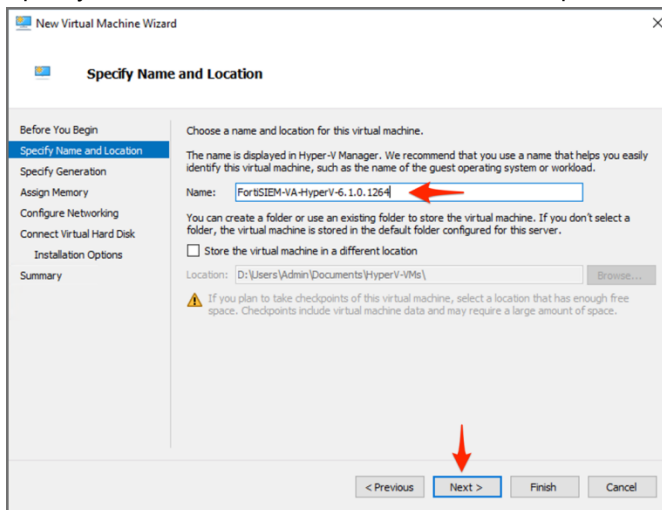
1. Launch Hyper-V Manager on your Microsoft Windows 2012 R2, 2016 or 2019 Server with Hyper-V installed.
2. Click **Action > New > Virtual Machine**, then Click **Next**.



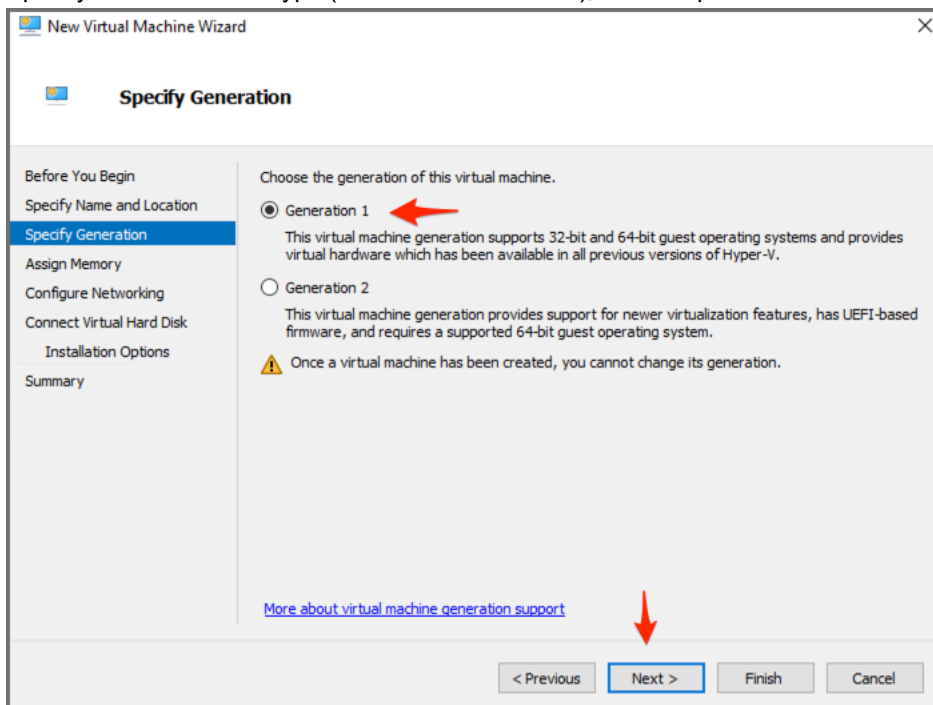
3. In the Before You Begin screen, click **Next**.



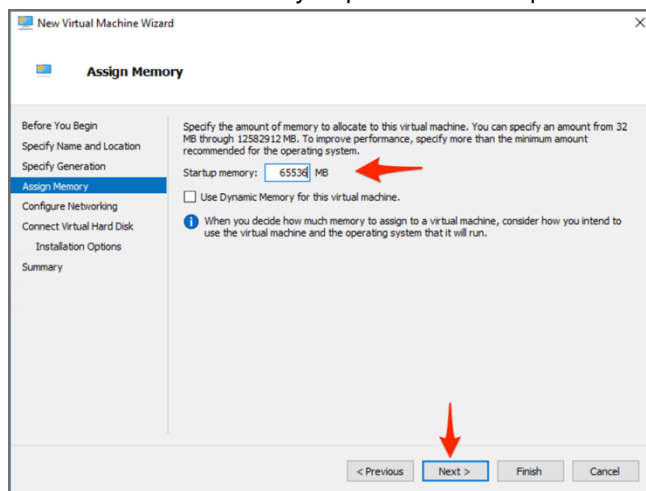
4. Specify the **Name** of the Virtual Machine, for example:



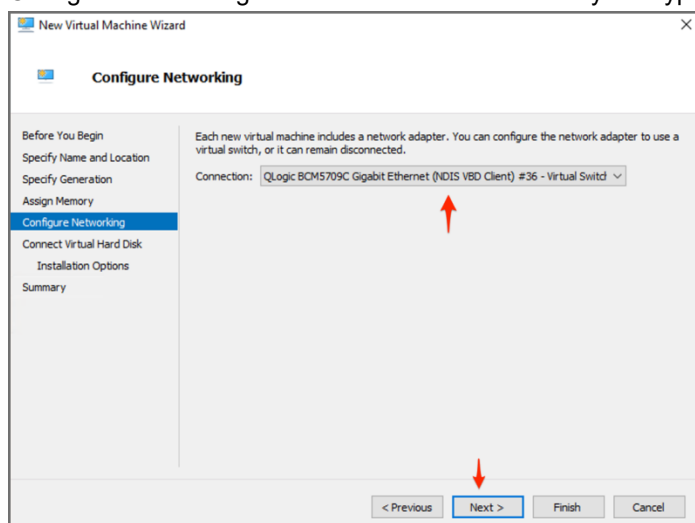
5. Specify the **Generation** type (choose **Generation 1**), for example:



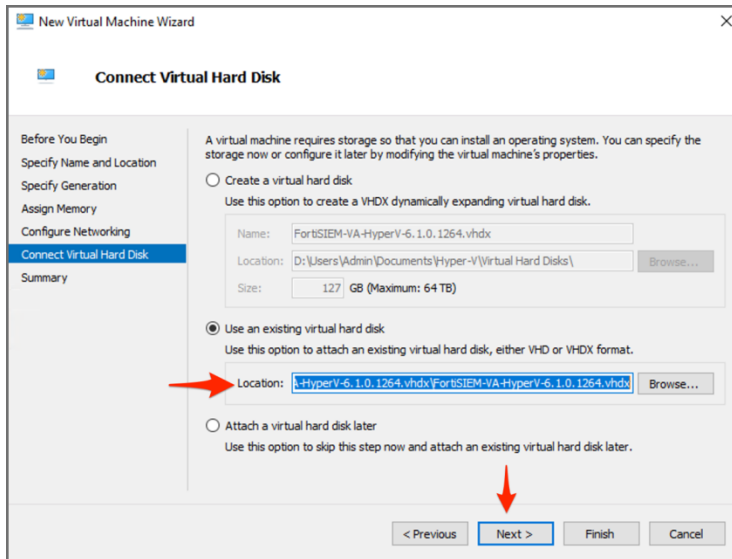
6. Add the amount of memory as per hardware requirements, then click **Next**.



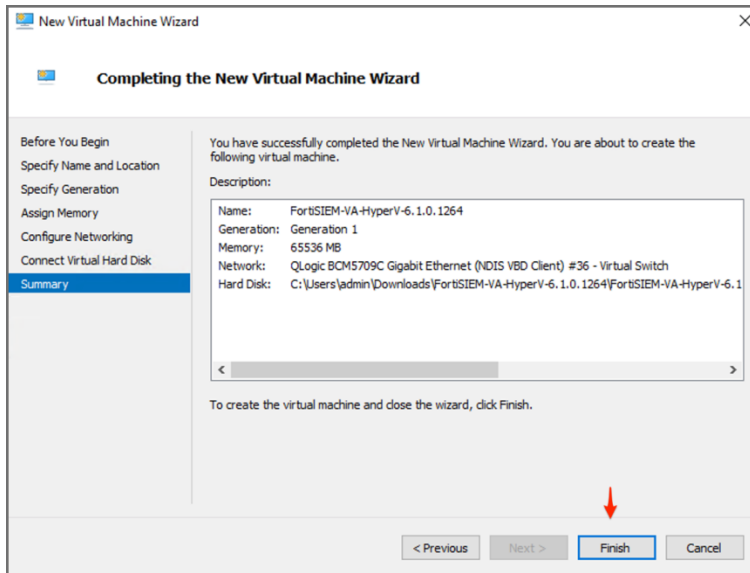
7. Configure Networking and select the virtual switch in your Hyper-V environment. Click **Next**.



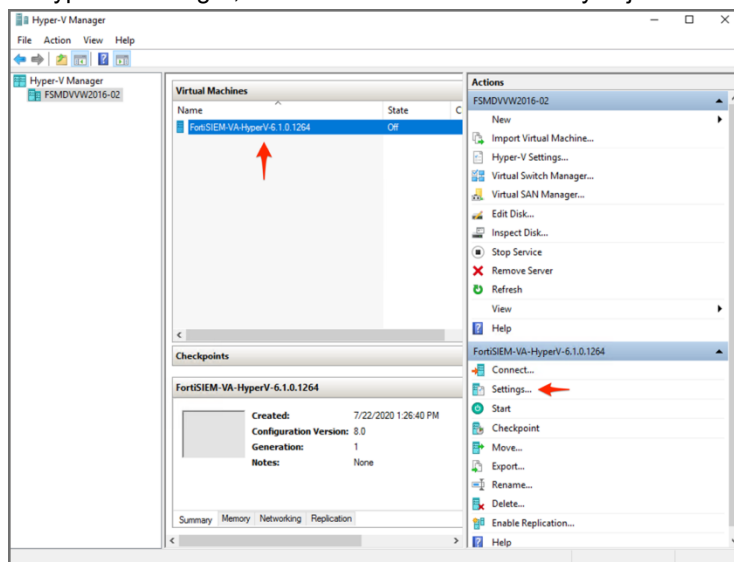
8. In Connect Virtual Hard Disk, select **Use an existing hard disk**, and choose the FortiSIEM VHDX you downloaded earlier, click **Next**:



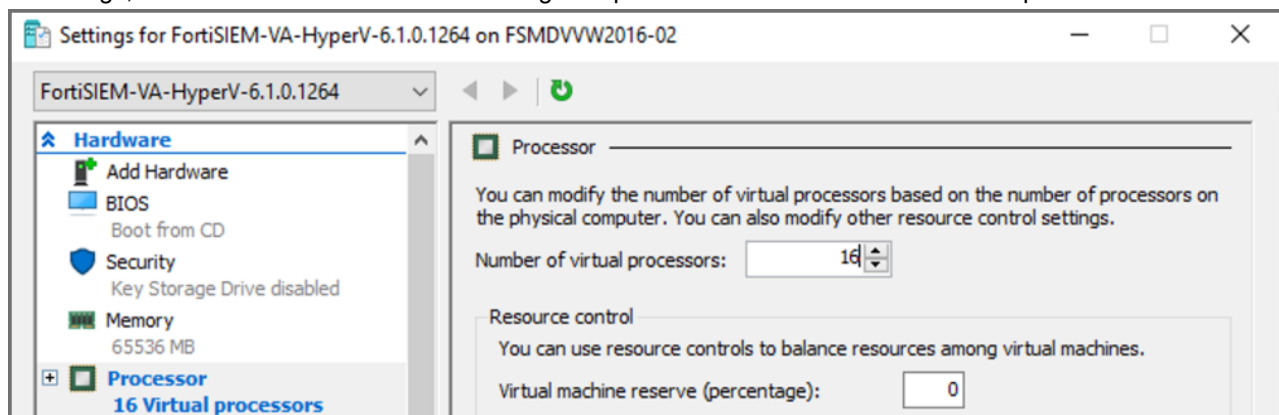
9. In Completing the New Virtual Machine Wizard, click **Finish**, for example:



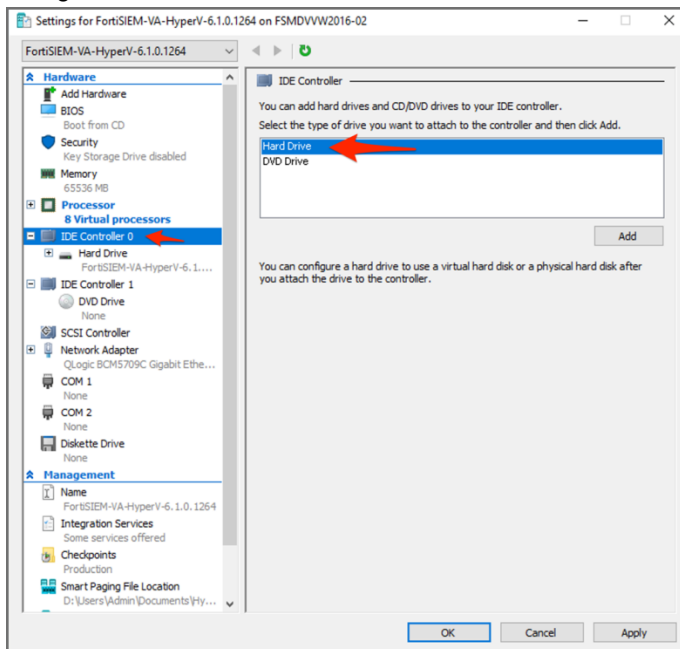
10. In Hyper-V Manager, select the virtual machine that you just created and click **Settings**, for example:



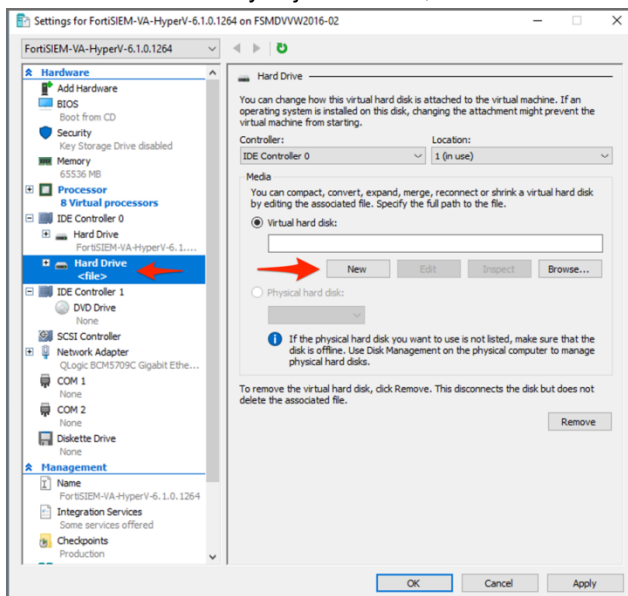
11. In Settings, select the **Processor** line in the navigation panel. Increase the number of virtual processors to **16**.



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:

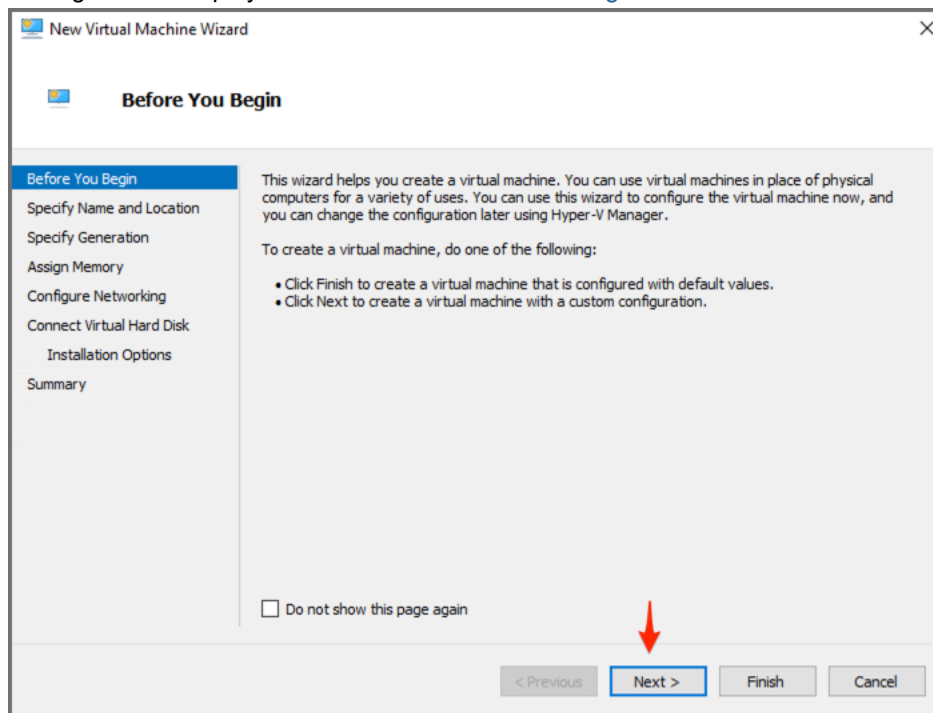
Disk	Size	Disk Name
Hard Disk 2	100GB	/opt

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 <code>configFSM.sh</code> runs.		
Hard Disk 3	60GB	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk 5	60GB+	/data (see the following note)

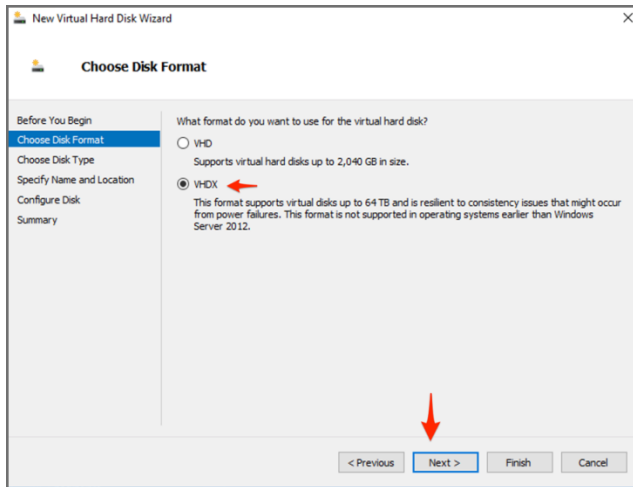
The **60GB CMDDB** disk and **60GB SVN** disk should be assigned to **IDE Controller 1**.

Note on Hard Disk 5:

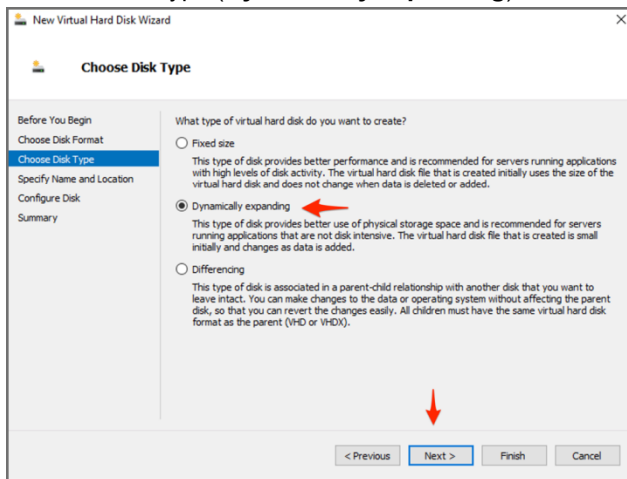
- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the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



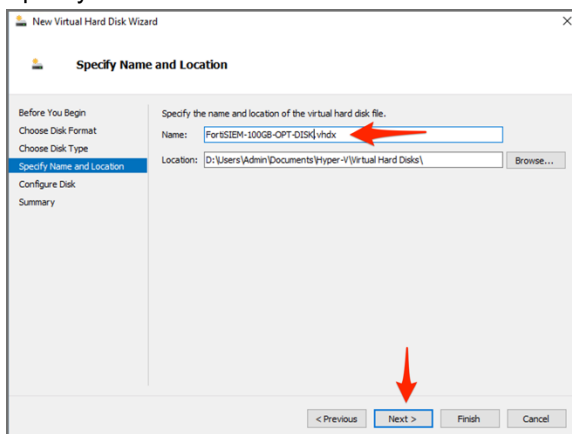
15. Choose a disk format (VHDX) and click **Next**.



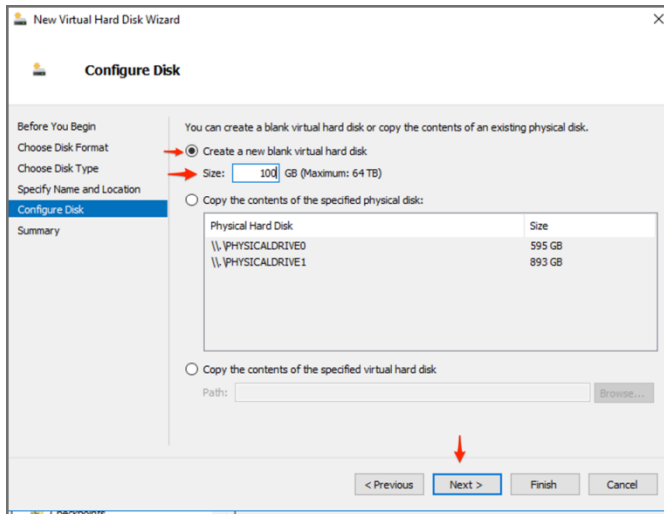
16. Choose Disk Type (**Dynamically expanding**) and click **Next**.



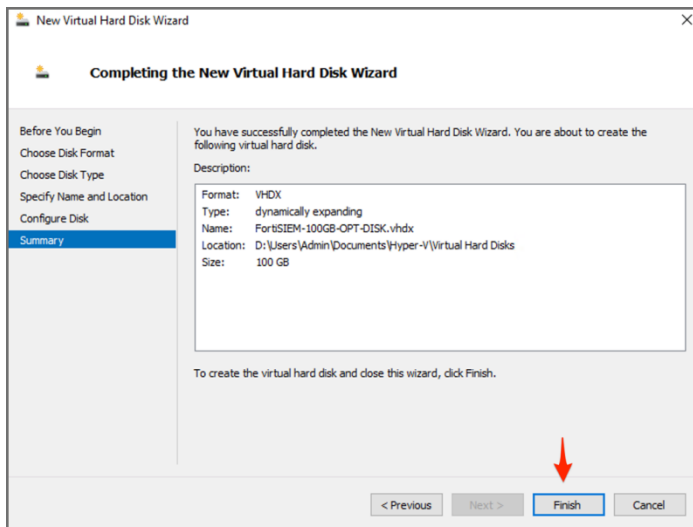
17. Specify the **Name** and **Location** of the disk. Click **Next**.



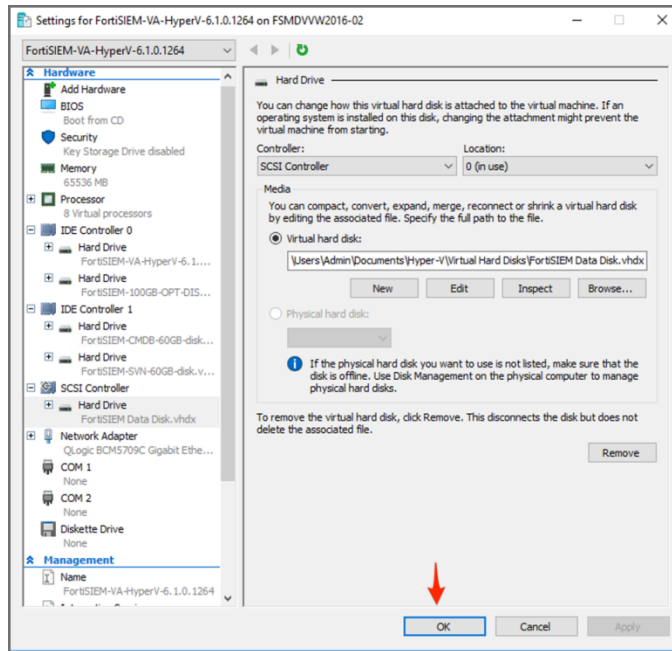
18. Specify 100GB as the size of the disk (for /opt). For other disks, specify size accordingly. Click **Next**.



19. Click **Finish**.

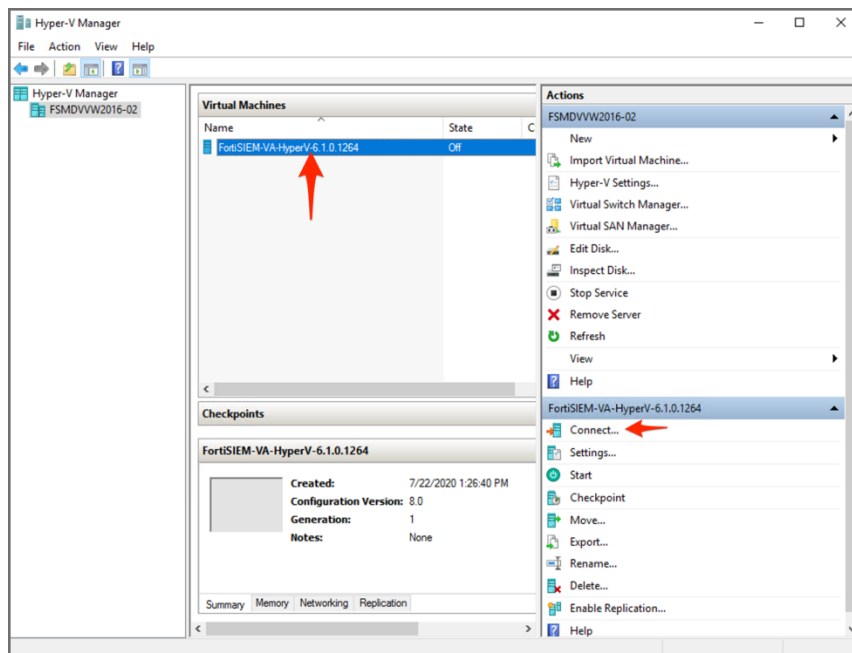


20. **IMPORTANT:** Similarly, add a 60GB CMDB disk, a 60GB SVN disk to IDE Controller 1. Delete the CD Drive that was added by default. If you need to use local data disk, then add a Hard Disk on the SCSI Controller of the appropriate size. Once all this is done, click **OK**.

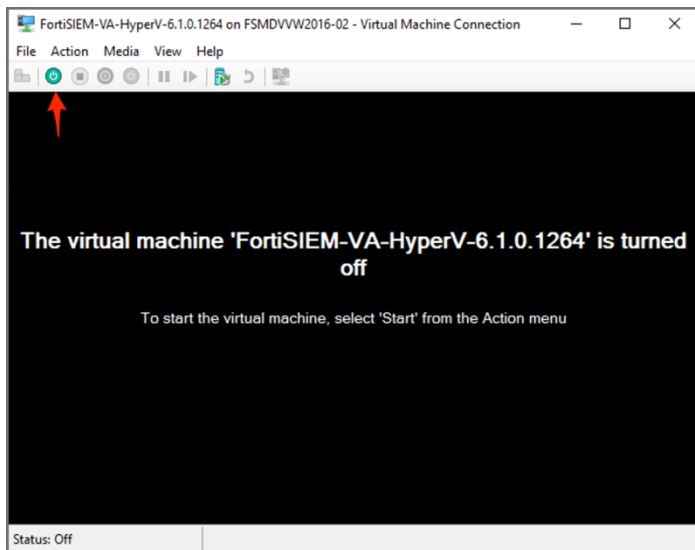


Start FortiSIEM from Hyper-V Manager

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



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



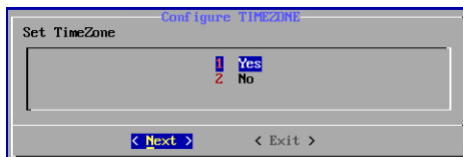
- The system will boot up. When the command prompt window opens, log in with the default login credentials: User `root` and Password `ProspectHills`.
- You will be required to change the password. Remember this password for future use.

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

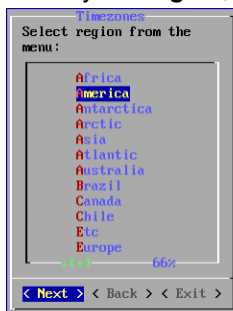
Configure FortiSIEM via GUI

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

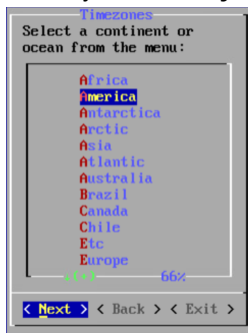
- Log in as user `root` with the password you set in [Step 5](#) above.
- At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`configFSM.sh`
- In VM console, select **1 Set Timezone** and then press **Next**.



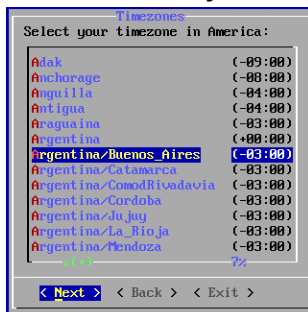
- Select your **Region**, and press **Next**.



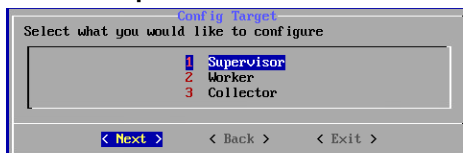
5. Select your **Country**, and press **Next**.



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

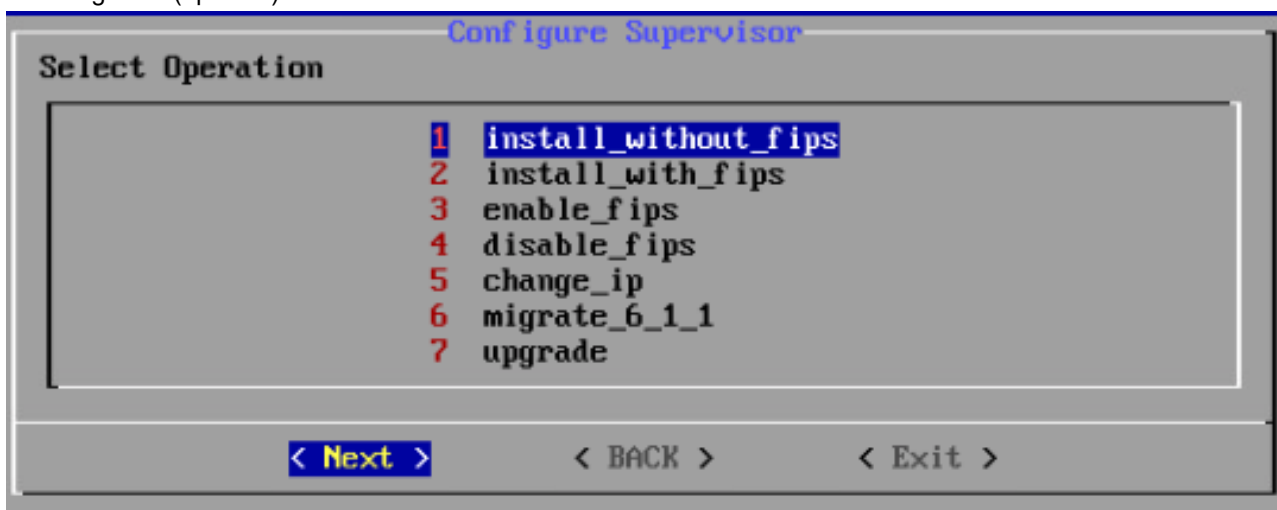


7. Select **1 Supervisor**. Press **Next**.



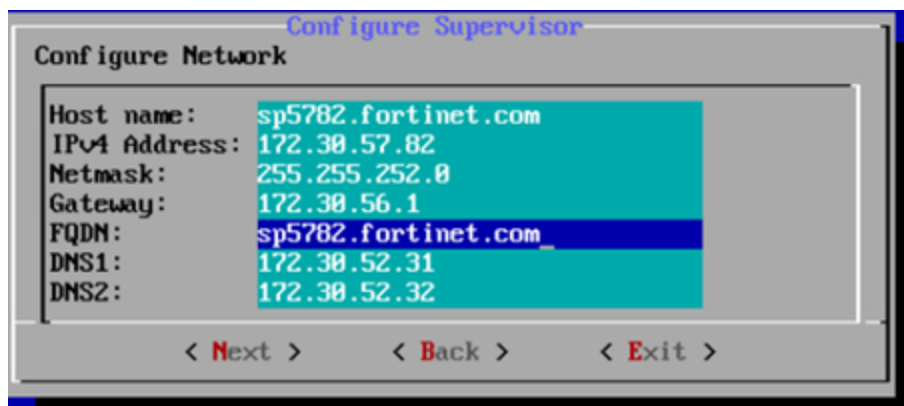
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

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.

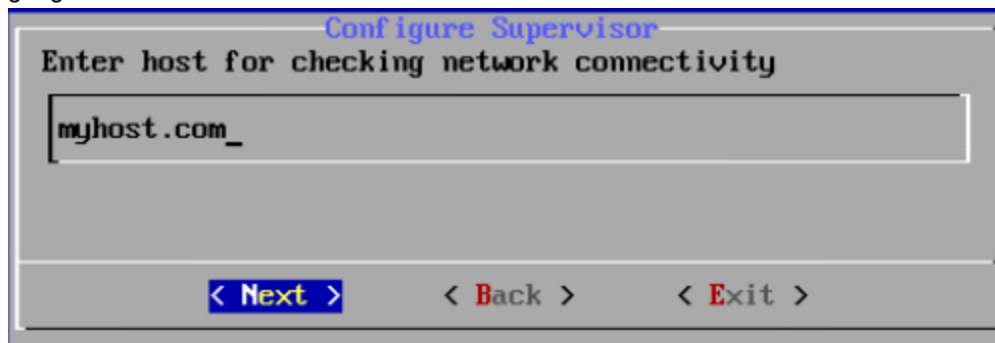


9. Configure the network by entering the following fields. Press **Next**.

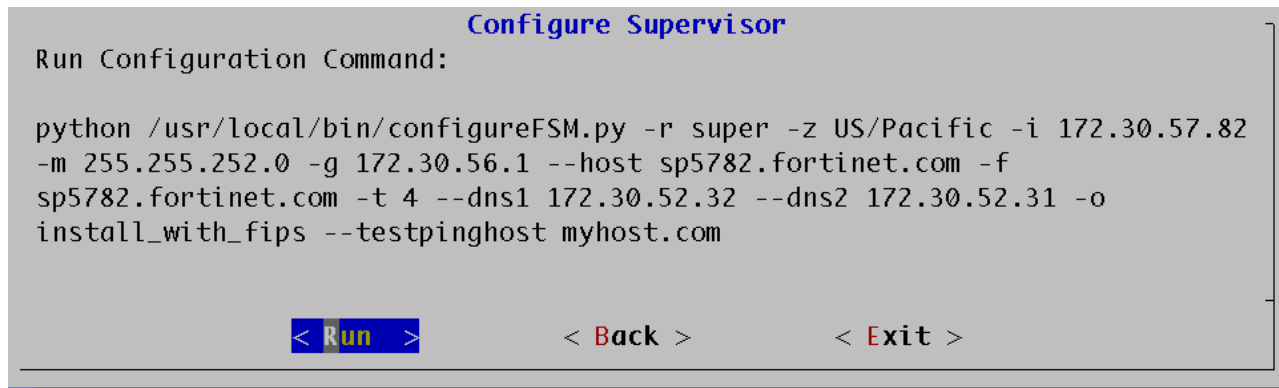
Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers



10. 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**.



11. 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) Note: the 6 value is not currently supported.
--dns1, --dns2	Addresses of the DNS servers
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_ip , or migrate_6_1_0 .)
-Z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

12. 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.
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).

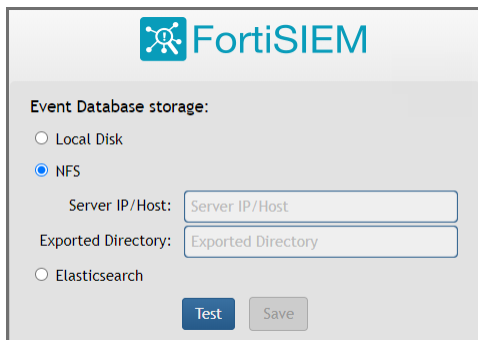
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

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



FortiSIEM

Event Database storage:

☐ Local Disk

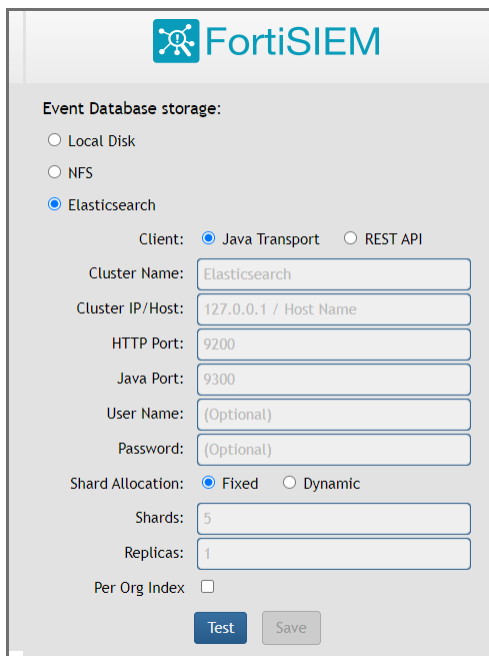
☒ NFS

Server IP/Host:

Exported Directory:

☐ Elasticsearch

Elasticsearch



FortiSIEM

Event Database storage:

☐ Local Disk

☐ NFS

☒ Elasticsearch

Client: ☒ Java Transport ☐ REST API

Cluster Name:

Cluster IP/Host:

HTTP Port:

Java Port:

User Name:

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:

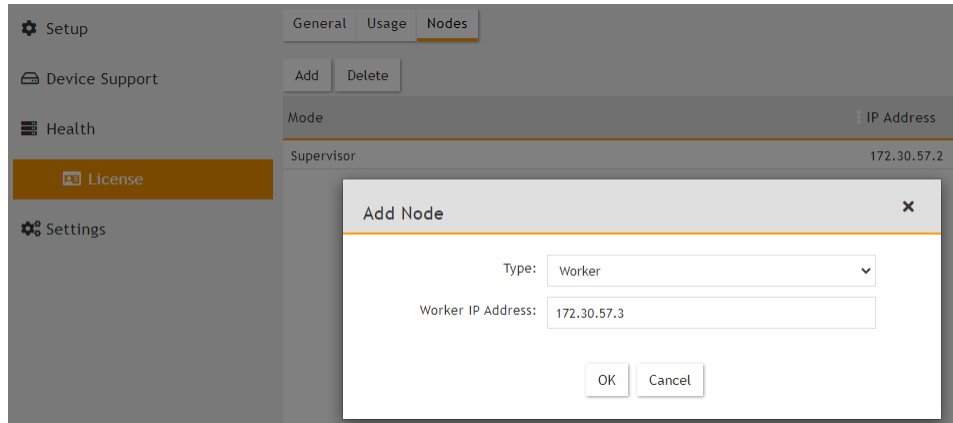
- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

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. Click **Add**.



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

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		
phDataManager	Up	14m 6s	0%	103 MB	1229 MB	1	126108

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:

```
phpProvisionCollector --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 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	10.10.10.1	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.

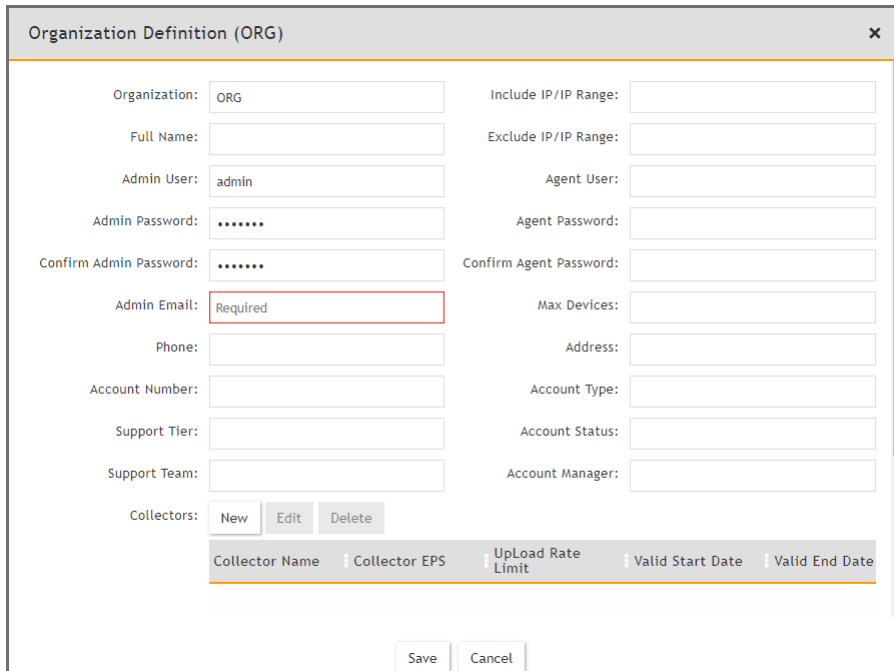
1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
 - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors 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

Worker Address: 10.10.10.3

Save

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



The screenshot shows the 'Organization Definition (ORG)' form. It contains the following fields:

- Organization:
- Full Name:
- Admin User:
- Admin Password:
- Confirm Admin Password:
- Admin Email:
- Phone:
- Account Number:
- Support Tier:
- Support Team:
- Collectors: New Edit Delete
- Include IP/IP Range:
- Exclude IP/IP Range:
- Agent User:
- Agent Password:
- Confirm Agent Password:
- Max Devices:
- Address:
- Account Type:
- Account Status:
- Account Manager:

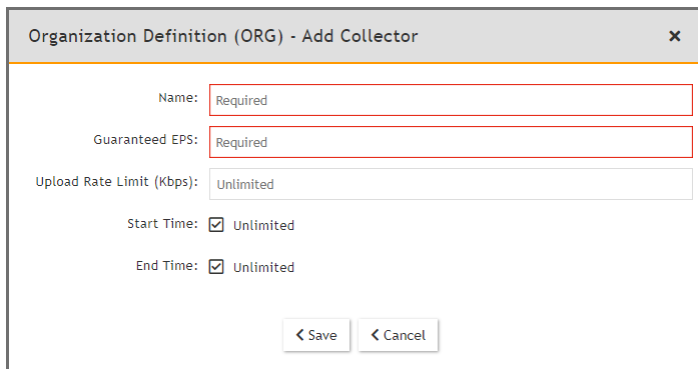
At the bottom, there is a table with the following headers: Collector Name, Collector EPS, UpLoad Rate Limit, Valid Start Date, Valid End Date. Below the table are 'Save' and 'Cancel' buttons.

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.



The screenshot shows the 'Organization Definition (ORG) - Add Collector' form. It contains the following fields:

- Name:
- Guaranteed EPS:
- Upload Rate Limit (Kbps):
- Start Time: ☒ Unlimited
- End Time: ☒ Unlimited

At the bottom are '< Save' and '< Cancel' buttons.

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.

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 0B6 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 displays the FortiSIEM web interface. On the left is a navigation menu with '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', shows the overall status of the collector. It has columns for Organization, Name, IP Address, Status, Health, Up Time, CPU, Memory, Allocated EPS, Incoming EPS, Version, and Col. The data row shows: Organization: Super, Name: CO-ORG, IP Address: 172.30.57.2, Status: up, Health: Normal, Up Time: 3m 4s, CPU: 65%, Memory: 5%, Allocated EPS: 200, Incoming EPS: 0, Version: 6.1.0.0, Col: 100.

The second table, 'Processes', shows the status of individual collector processes. It has columns for Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. The data rows are:

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		

Migrating from FortiSIEM 5.3.0, 5.3.1, or 5.3.2

WARNING: FortiSIEM 5.3.3 and 5.4.0 cannot be upgraded to FortiSIEM 6.1.0. You must upgrade to FortiSIEM 6.1.1.

This section describes how upgrade from FortiSIEM 5.3.0, 5.3.1, or 5.3.2 to FortiSIEM 6.1.0.

- [Pre-Migration checklist](#)
- [Migrate All-in-one Installation](#)
- [Migrate Cluster](#)

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met:

- [Create the Directories](#)
- [Download the Backup Script](#)
- [Run the Backup Script and Shutdown System](#)

Create the Directories

1. Delete the Worker from the Super GUI.
2. Stop/Shutdown the Worker.
3. Create a `/svn/53x-settings` directory and symlink it to `/images`. For FSM running on Hyper-V, you only need a tiny amount of space to backup 5.3.0, 5.3.1, or 5.3.2 system settings, so use the `/svn` partition (a partition other than `root`) instead of a new disk. The following screen shot illustrates this:

```
[root@fsm-hyperv-531-to-610 ~]# cat /opt/phoenix/bin/VERSION
Version: 5.3.1.1671
DSVersion: 5.3.1.1671
CommitHash:de812f1ef
Built on: 1592428994
Local time: Wed Jun 17 14:23:14 PDT 2020
[root@fsm-hyperv-531-to-610 ~]#
[root@fsm-hyperv-531-to-610 ~]# mkdir /svn/53x-settings
[root@fsm-hyperv-531-to-610 ~]# ln -sf /svn/53x-settings /images
[root@fsm-hyperv-531-to-610 ~]# █
```

Download the Backup Script

Download the FortiSIEM Hyper-V backup script to start migration. Follow these steps:

1. Download the file `FSM_Backup_5.3_Files_6.1.0_build0112.zip` from the [support site](#).
2. Copy the file to the 5.3.0, 5.3.1, or 5.3.2 Hyper-V instance (for example, `/svn/53x-settings`) that you are planning to migrate to 6.1.0.
3. Unzip the `.zip` file:

```
# cd /svn/53x-settings  
# unzip FSM_Backup_5.3_Files_6.1.0_build0112.zip
```

```
[root@testsup 53x-settings]# unzip FSM_Backup_5.3_Files_6.1.0_build0112.zip  
Archive:  FSM_Backup_5.3_Files_6.1.0_build0112.zip  
  inflating: FSM_Backup_5.3_Files_6.1.0_build0112/backup  
  inflating: FSM_Backup_5.3_Files_6.1.0_build0112/network_params.json  
  inflating: FSM_Backup_5.3_Files_6.1.0_build0112/pwd_backup  
[root@testsup 53x-settings]#
```

Run the Backup Script and Shutdown System

Follow these steps to run the backup script:

1. Go to the directory that contains the `backup-config` file, for example:

```
# cd /svn/53x-settings/fsm-53x-backup-config
```
2. Run the `sh backup` script to backup the 5.3.0, 5.3.1, or 5.3.2 settings that will be migrated later into the new 6.1 OS.

```
# sh backup
```

```
[root@fsm-hyperv-531-to-610 53x-settings]# cd /svn/53x-settings/fsm-53x-backup-config  
[root@fsm-hyperv-531-to-610 fsm-53x-backup-config]# sh backup  
backing up DataBases  
backing Up Network Parameters  
[root@fsm-hyperv-531-to-610 fsm-53x-backup-config]#
```

3. Shutdown the system.

```
# shutdown -h now  
[root@fsm-hyperv-531-to-610 fsm-53x-backup-config]# shutdown -h now  
  
Broadcast message from root@fsm-hyperv-531-to-610  
      (/dev/pts/0) at 22:48 ...  
  
The system is going down for halt NOW!  
[root@fsm-hyperv-531-to-610 fsm-53x-backup-config]# Connection to 172.30.53.135 closed by remote host.  
Connection to 172.30.53.135 closed.
```

Migrate All-in-one Installation

- [Download and Uncompress 6.1.0 Hyper-V Root VHDX](#)
- [Modify the 5.3.0, 5.3.1, or 5.3.2 Instance to Use the New VHDX](#)
- [Migrate to FortiSIEM 6.1.0](#)

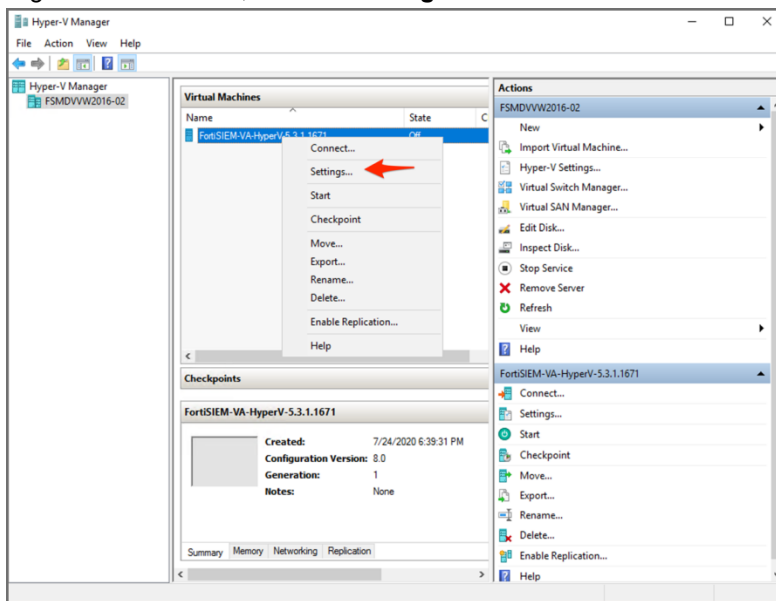
Download and Uncompress the 6.1.0 Hyper-V Root VHDX

Download the compressed FortiSIEM Hyper-V root VHDX migration. Follow these steps:

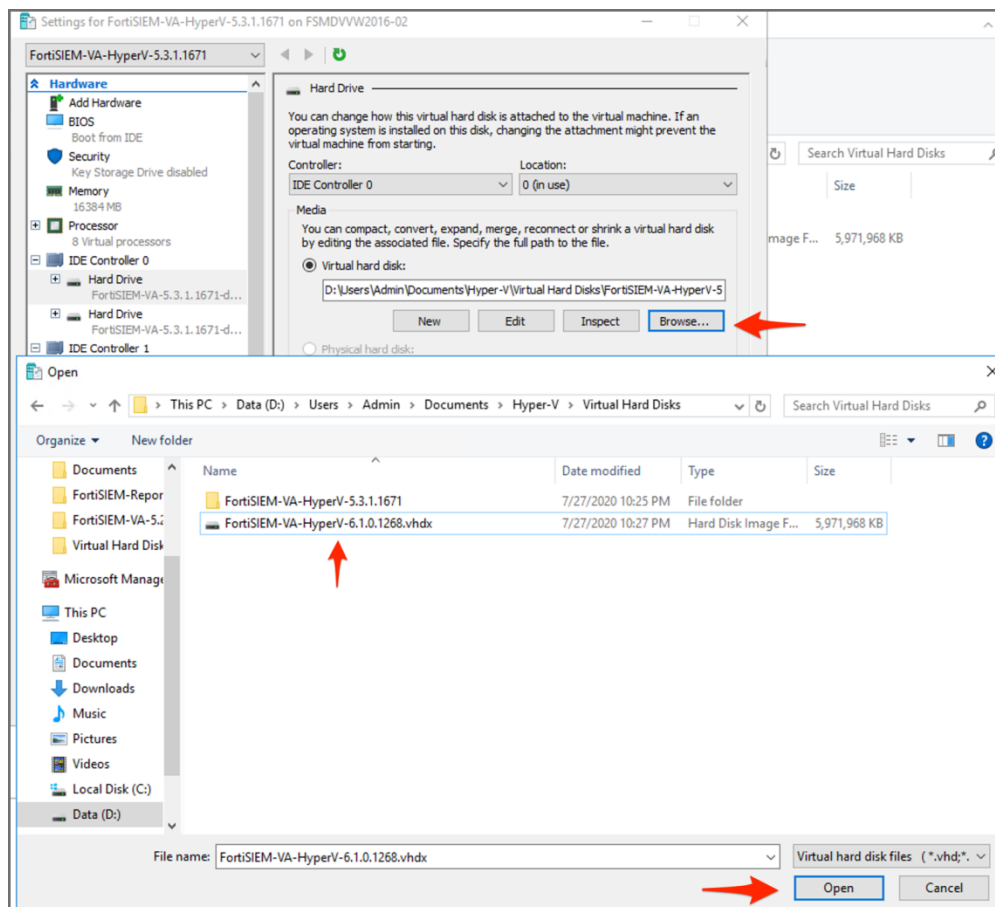
1. Download the file `FortiSIEM-HyperV-6.1.0.0112.zip` from the [support site](#).
2. Copy the file to your 5.3.0, 5.3.1, or 5.3.2 Hyper-V host that is currently running the 5.3.0, 5.3.1, or 5.3.2 instance.
3. Use unzip tools to uncompress the `.zip` file to obtain the `FortiSIEM-HyperV-6.1.0.0112.zip` file. Store it in the same folder where you have your 5.3.0, 5.3.1, or 5.3.2 disks.

Modify the 5.3.0, 5.3.1, or 5.3.2 Instance to use new VHDX

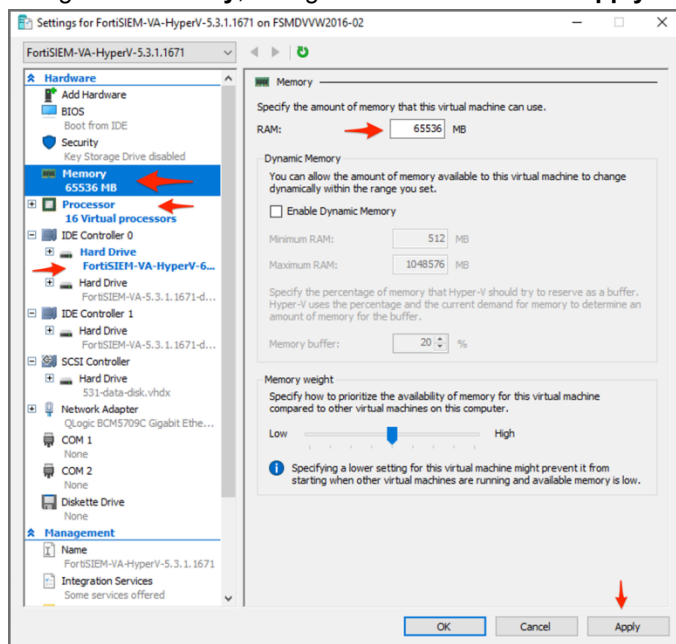
1. Open the Hyper-V Manager and select your 5.3.0, 5.3.1, or 5.3.2 VM.
2. Right-click on the VM, then click **Settings**.



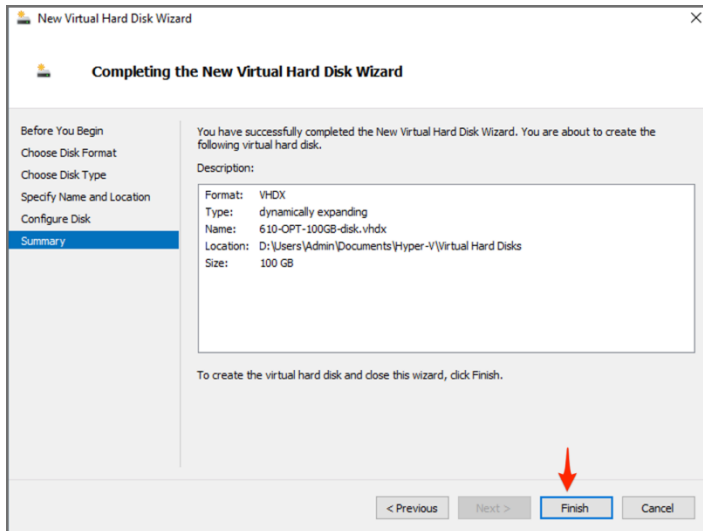
3. Navigate to the first hard drive under **IDE Controller 0**. Click **Browse** and select the new 6.1 VHDX you just uncompressed. Click **Open**.



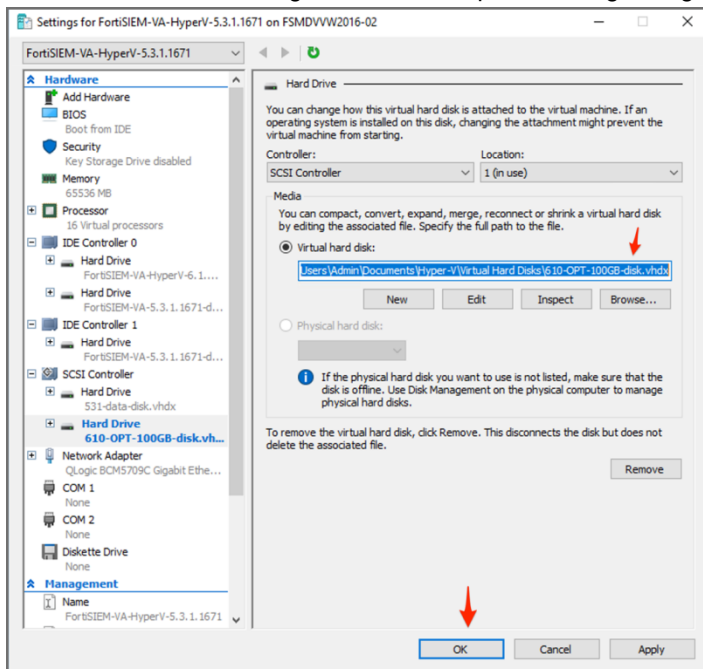
4. Navigate to **Processor**, change **8 vCPUs** to **16**.
5. Navigate to **Memory**, change **16GB** to **64GB**. Click **Apply**.



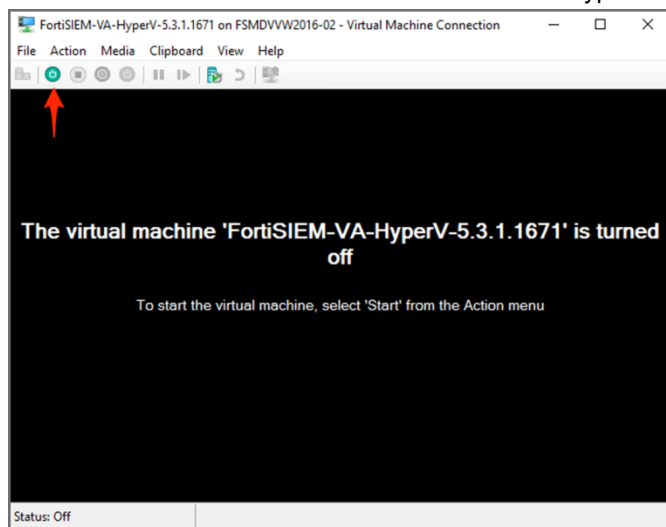
- Click **SCSI Controller**, Hard Drive, Click **Add**. Similar to Fresh Install [steps 12- 19](#), add a new hard drive of size **100GB** for the /opt partition. Below is a screen shot of the final screen of **Add new hard drive**.



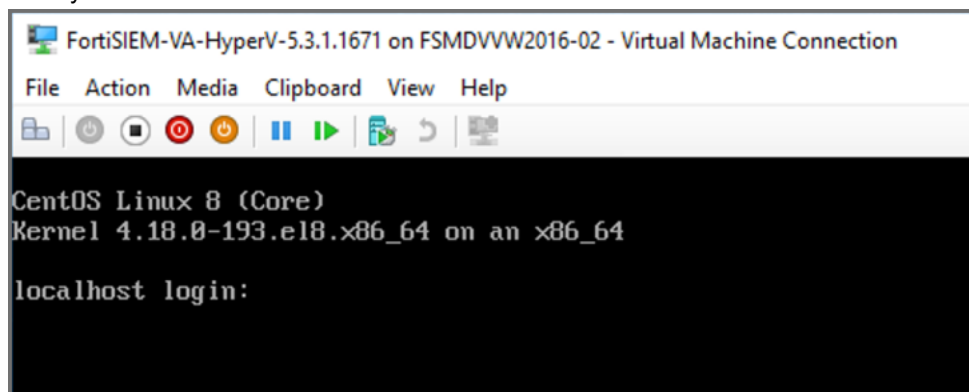
- Click **OK** on the VM settings screen to complete making changes to the VM for migration.



8. Connect to the VM Console and Start the VM from Hyper-V Manager.



9. The system will start with the FortiSIEM 6.1 OS.



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

Migrate to FortiSIEM 6.1.0

1. Find the device name of the original 5.3.0, 5.3.1, or 5.3.2 SVN volume using `fdisk -l` and mount it to `/mnt`. This contains the backup of 5.3.0, 5.3.1, or 5.3.2 system settings that will be used during migration. Copy the 5.3.0, 5.3.1, or 5.3.2 settings that were previously backed up and then `umount /mnt`, for example:

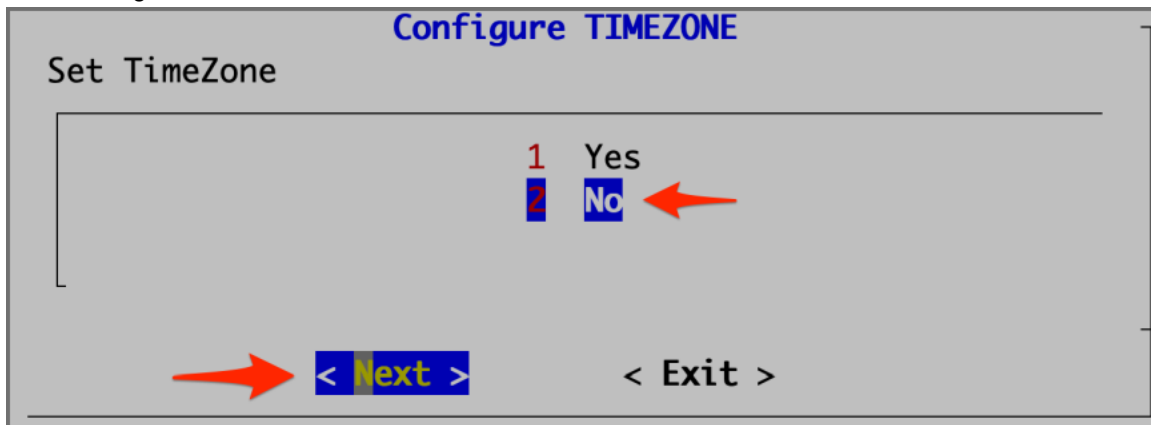
```
# mount /dev/sdb1 /mnt
# mkdir /restore-53x-settings
# cd /restore-53x-settings
# rsync -av /mnt/53x-settings/. .
# ln -sf /restore-53x-settings /images
# umount /mnt
```

```
[root@localhost ~]# mount /dev/sdb1 /mnt
[root@localhost ~]# ls -ld /mnt/53x-settings/
drwxr-xr-x 5 root root 4096 Jul 28 00:45 /mnt/53x-settings/
[root@localhost ~]# mkdir /restore-53x-settings
[root@localhost ~]# cd /restore-53x-settings
[root@localhost restore-53x-settings]# rsync -av /mnt/53x-settings/. .
sending incremental file list
./
.fortisiem4x0
VERSION
ao_login.png
ao_upload.png
bg.png
fsm-53x-backup-config.tgz
grub_base
login.png
network_params.json
network_params.json.bak
orig_UUID
origdisks
origdisks.bak
passwd
phoenix_config.txt
pwd_backup
pwd_backup.bak
upload.png
wl_login.png
wl_upload.png
backup/
backup/accelopslogo.png
backup/companylogo.png
backup/companylogo.svg
backup/ph_entry_id.seq
backup/ph_event_id.seq
backup/phoenix_config.txt
backup/header/
backup/header/login.png
backup/header/logo.png
backup/header/wl_login.png
backup/image/
backup/image/login.png
backup/image/upload.png
backup/image/wl_login.png
backup/image/wl_upload.png
fsm-53x-backup-config/
fsm-53x-backup-config/backup
fsm-53x-backup-config/fstab_base
fsm-53x-backup-config/grub_base
fsm-53x-backup-config/grub.bl.tmpl
fsm-53x-backup-config/network_params.json
fsm-53x-backup-config/pwd_backup
org/
org/1
org/2

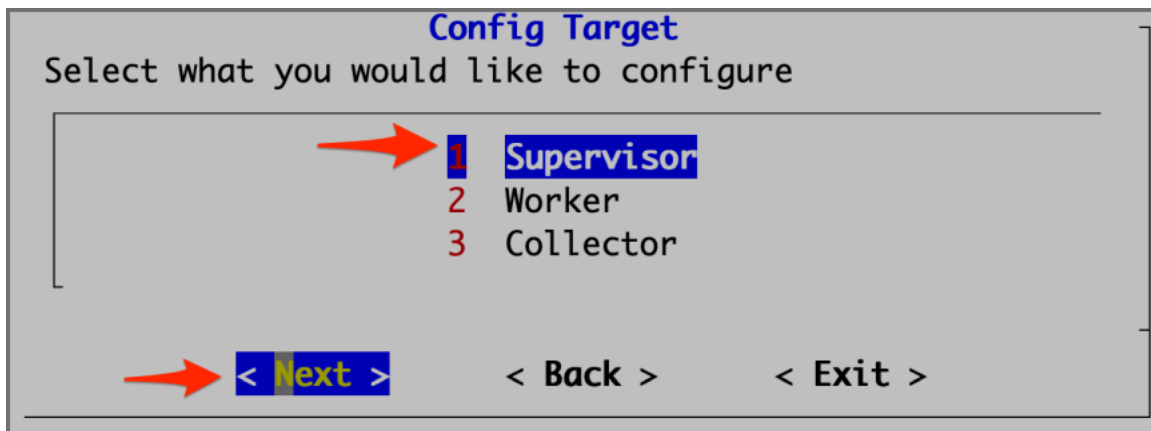
sent 219,713 bytes  received 830 bytes  441,086.00 bytes/sec
total size is 216,757  speedup is 0.98
[root@localhost restore-53x-settings]#
[root@localhost restore-53x-settings]# ln -sf /restore-53x-settings /images
[root@localhost restore-53x-settings]# umount /mnt
[root@localhost restore-53x-settings]#
```

2. Run the `configFSM.sh` command to configure the migration via a GUI, for example:
`configFSM.sh`

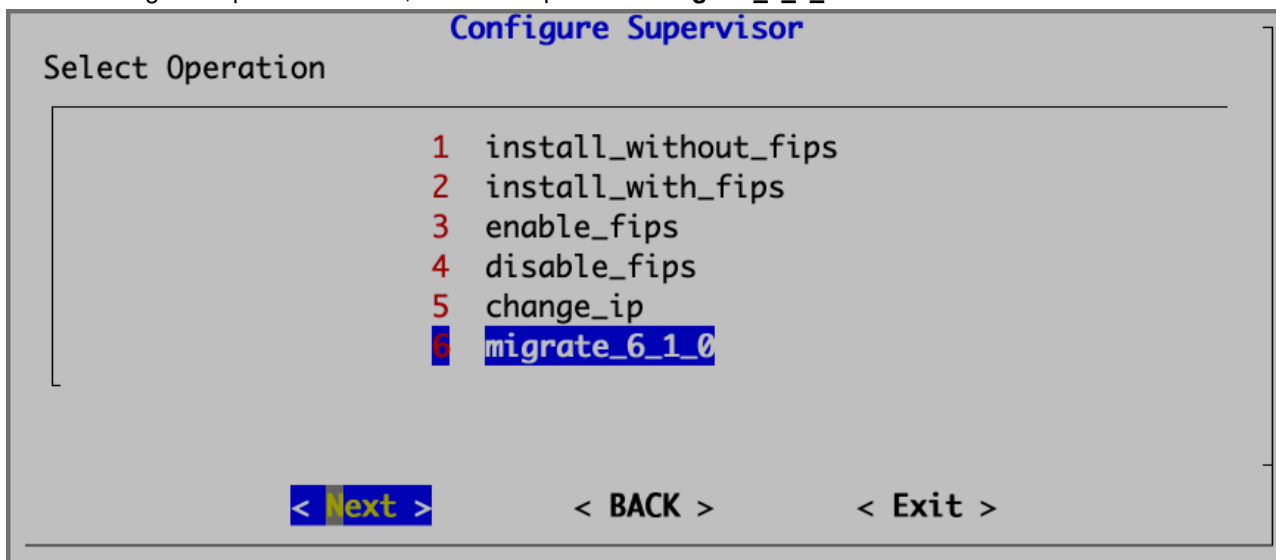
3. In the Configure TIMEZONE screen of the GUI select **2 No**. Press **Next**.



4. Select your node type: **Supervisor**, **Worker**, or **Collector**. This step is usually performed on **Supervisor**. Press **Next**.



5. On the Configure Supervisor screen, select the operation **6 migrate_6_1_0**. Press **Next**.



6. 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**.

Configure Supervisor

Enter host for checking network connectivity

myhost.com_

< Next >
< Back >
< Exit >

7. Click **Run** on the confirmation page once you make sure all the values are correct. The options for the `configureFSM.py` script are described in the table [here](#).

Configure Supervisor

Run Configuration Command:

```
python /usr/local/bin/configureFSM.py -r super -z US/Pacific -i
172.30.57.83 -m 255.255.252.0 -g 172.30.56.1 --host sp5783 -f
sp5783.fortinet.com -t 4 --dns1 172.30.52.32 --dns2 172.30.52.31 -o migrate
--testpinghost myhost.com
```

< Run >
< Back >
< Exit >

8. Wait for the operations to complete, and system to reboot.

```
TASK [Execute GlassFish Tasks] *****
TASK [appserver : GLASSFISH | Remove Passwd File] *****
changed: [localhost]

PLAY RECAP *****
localhost                : ok=115  changed=87  unreachable=0    failed=0    skipped=21   rescued=0    ignored=3

('ansible running result=', 0)
Connection to 172.30.53.135 closed by remote host.
Connection to 172.30.53.135 closed.
$
```

9. Login to the system after a few minutes. Wait several more minutes for all processes to start up. Execute the `phstatus` command, for example:
`phstatus`

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

```
System uptime: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.28, 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%ni, 91.4%id, 0.0%wa, 0.2%hi, 0.1%si, 0.0%st
Mem: 65702100k total, 10366036k used, 55336064k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465020k cached
```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	41:23	0	2176m	558m
phQueryMaster	41:41	0	1020m	77m
phRuleMaster	41:41	0	1079m	504m
phRuleWorker	41:41	0	1363m	285m
phQueryWorker	41:41	0	1383m	279m
phDataManager	41:41	0	1419m	285m
phDiscover	41:41	0	513m	53m
phReportWorker	41:41	0	1433m	95m
phReportMaster	41:41	0	603m	67m
phIpIdentityWorker	41:41	0	1027m	58m
phIpIdentityMaster	41:41	0	491m	39m
phAgentManager	41:41	0	1425m	54m
phCheckpoint	42:31	0	325m	34m
phPerfMonitor	41:41	0	702m	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	2000m	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
AppSvr	01:10:07	0	15172m	3026m
DBSvr	01:10:38	0	317m	30m
phAnomaly	01:00:07	0	907m	64m
phFortiInsightAI	01:10:40	0	23432m	430m
Redis	01:10:10	0	55m	25m

- Remove the restored settings directories because you no longer need them, for example:

```
# rm -rf /restore-53x-settings
# rm -rf /svn/53x-settings
# rm -f /images
```

Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- [Delete Workers](#)
- [Migrate Supervisor](#)

- [Install New Worker\(s\)](#)
- [Register Workers](#)
- [Set Up Collector-to-Worker Communication](#)
- [Working with Pre-6.1.0 Collectors](#)
- [Install 6.1.0 Collectors](#)
- [Register 6.1.0 Collectors](#)

Delete Workers

1. Login to the Supervisor.
2. Go to **Admin > License > Nodes** and delete the Workers one-by-one.
3. Go to the **Admin > Cloud Health** page and make sure that the Workers are not present.
Note that the Collectors will buffer events while the Workers are down.
4. Shutdown the Workers.
SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in [Migrate All-in-one Installation](#) to migrate the supervisor node. **Note:** FortiSIEM 6.1.0 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in [Cluster Installation > Install Workers](#) to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in [Cluster Installation > Register Workers](#) to register the newly created 6.1.0 Workers to the 6.1.0 Supervisor. The 6.1.0 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

1. Go to **Admin > Systems > Settings**.
2. Add the Workers to the Event Worker or Query Worker as appropriate.
3. Click **Save**.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.0 Supervisor and Workers. You can install 6.1.0 collectors at your convenience.

Install 6.1.0 Collectors

FortiSIEM does not support Collector migration to 6.1.0. You can install new 6.1.0 Collectors and register them to 6.1.0 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

1. Copy the http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector.
2. Disconnect the pre-6.1.0 Collector.
3. Install the 6.1.0 Collector with the old IP address by the following the steps in [Cluster Installation > Install Collectors](#).
4. Copy the saved http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector to the 6.1.0 Collector.

This step is needed for Agents to work seamlessly with 6.1.0 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.0 migration, this password is lost.

Register 6.1.0 Collectors

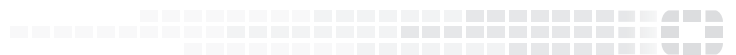
Follow the steps in [Cluster Installation > Register Collectors](#), with the following difference: in the `phProvisionCollector` command, use the `--update` option instead of `--add`. Other than this, use the exactly the same parameters that were used to register the pre-6.1.0 Collector. Specifically, use this form of the

`phProvisionCollector` command to register a 6.1.0 Collector and keep the old associations:

```
# /opt/phoenix/bin/phProvisionCollector --update <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.

Re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.