ESX Installation Guide

FortiSIEM 7.3.2

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

08/08/2025
FortiSIEM 7.3.2 ESX Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
12/16/2024	Release of FortiSIEM - ESX Installation Guide for 7.3.0.
03/04/2025	Release of FortiSIEM - ESX Installation Guide for 7.3.1.
03/21/2025	Release of FortiSIEM - ESX Installation Guide for 7.3.2.
07/15/2025	Release of FortiSIEM - ESX Installation Guide for 7.3.3.
07/29/2025	Release of FortiSIEM - ESX Installation Guide for 7.3.4.

Fresh Installation

Pre-Installation Checklist

Before you begin, check the following:

- Release 7.3.2 requires at least ESX 6.5, and ESX 6.7 Update 2 is recommended. To install on ESX 6.5, See Installing on ESX 6.5.
- 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 responds to 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 the 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 (Minimum Requirements)
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.

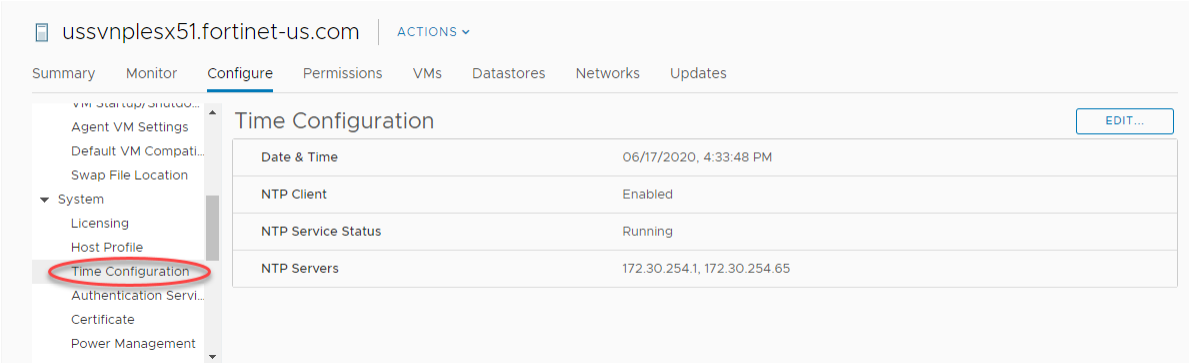
- Set Network Time Protocol for ESX
- Import FortiSIEM into ESX

- Edit FortiSIEM Hardware Settings
- Start FortiSIEM from the VMware Console
- Configure FortiSIEM
- Upload the FortiSIEM License
- Configure an Event Database
- Final Check

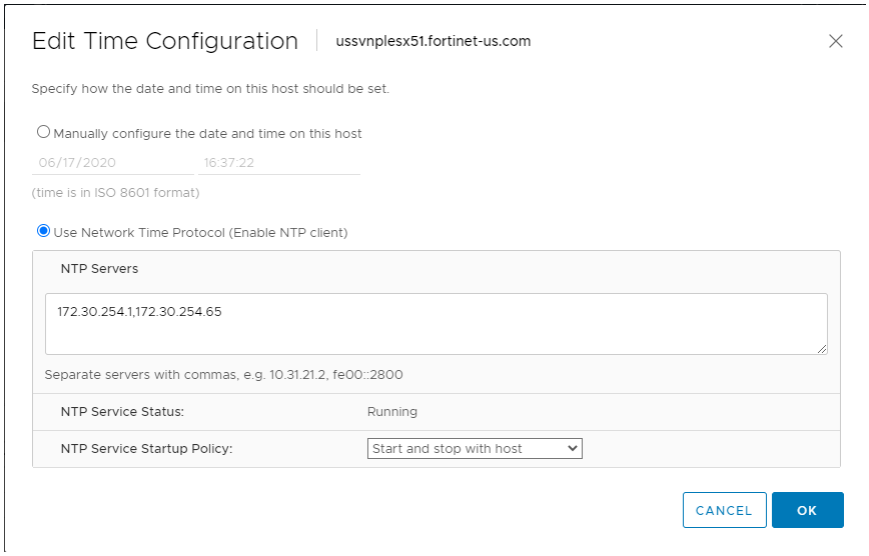
Set Network Time Protocol for ESX

FortiSIEM needs accurate time. To do this you must enable NTP on the ESX host which FortiSIEM Virtual Appliance is going to be installed.

1. Log in to your VCenter and select your ESX host.
2. Click the **Configure** tab.
3. Under **System**, select **Time Configuration**.



4. Click **Edit**.
5. Enter the time zone properties.

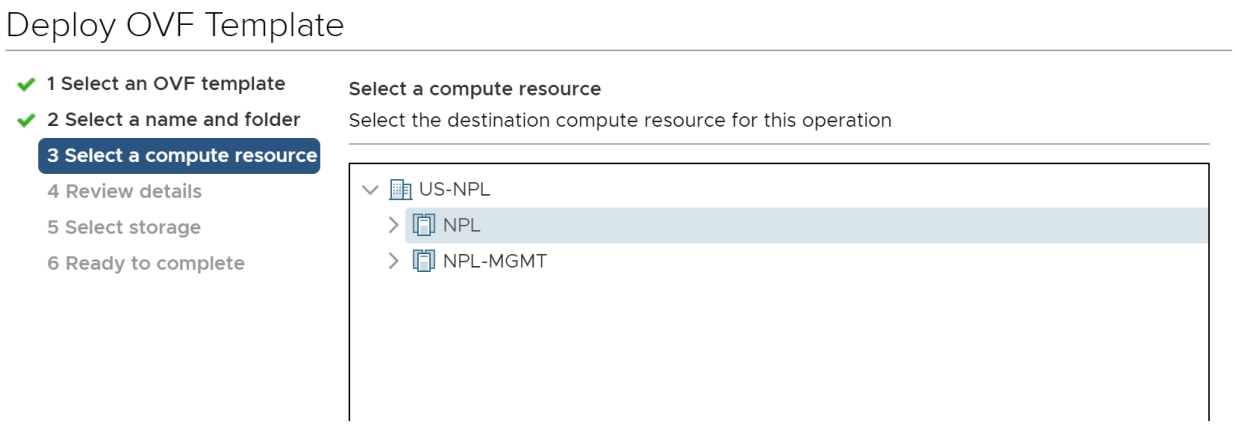


6. Enter the IP address of the NTP servers to use.
   If you do not have an internal NTP server, you can access a publicly available one at http://tf.nist.gov/tf-cgi/servers.cgi.

7. Choose an **NTP Service Startup Policy**.
8. Click **OK** to apply the changes.

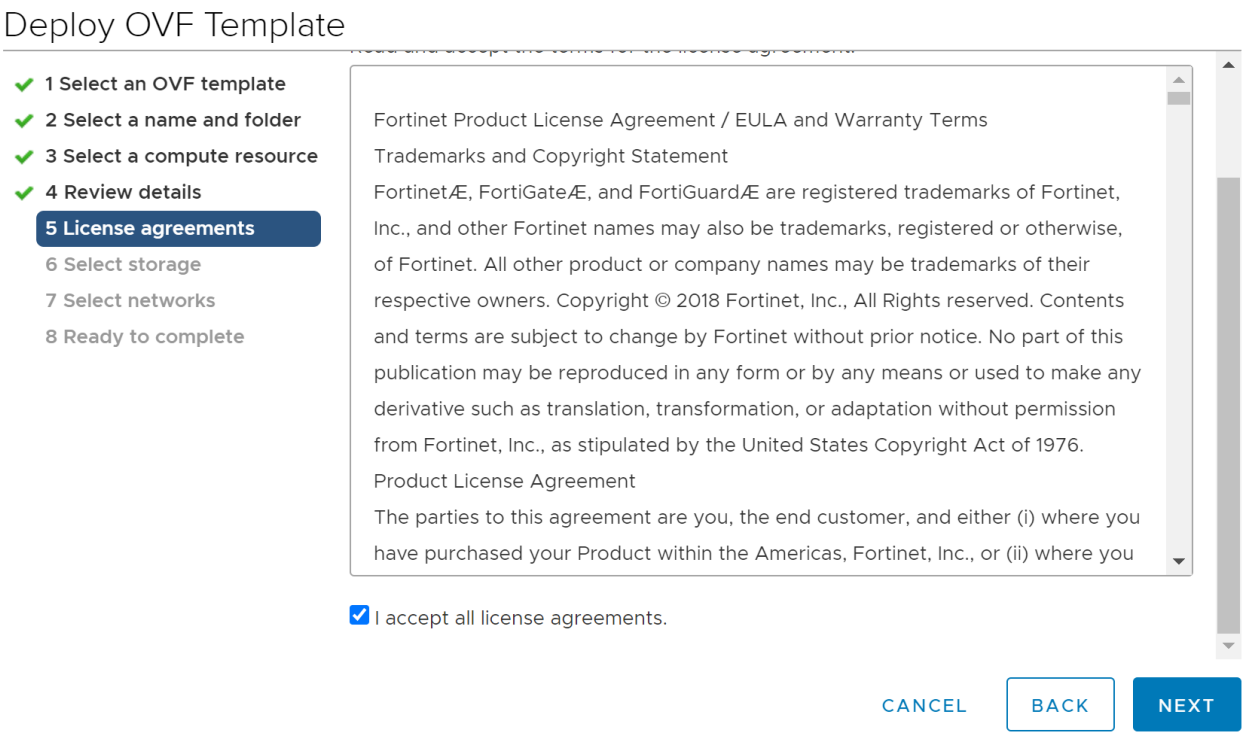
Import FortiSIEM into ESX

1. Go to the Fortinet Support website https://support.fortinet.com to download the ESX package `FSM_FULL_ALL_ESX_7.3.2_Build0374.zip`. See Downloading FortiSIEM Products for more information on downloading products from the support website.
2. Uncompress the packages for Super/Worker and Collector (using 7-Zip tool) to the location where you want to install the image. Identify the `.ova` file.
3. Right-click on your own host and choose **Deploy OVF Template**.
   The Deploy OVA Template dialog box appears.
4. In **1 Select an OVF template** select **Local file** and navigate to the `.ova` file. Click **Next**. If you are installing from a URL, select **URL** and paste the OVA URL into the field beneath **URL**.
5. In **2 Select a Name and Folder**, make any needed edits to the **Virtual machine name** field. Click **Next**.
6. In **3 Select a compute resource**, select any needed resource from the list. Click **Next**.

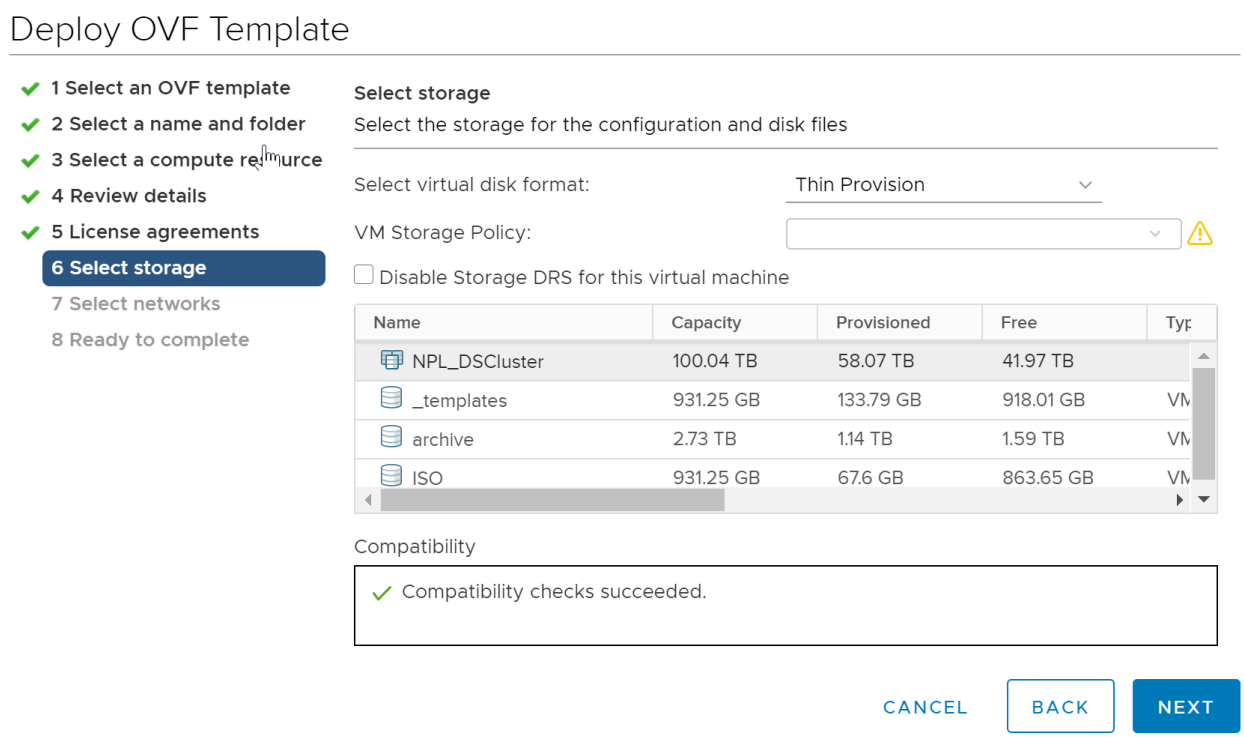


7. Review the information in **4 Review details** and click **Next**.

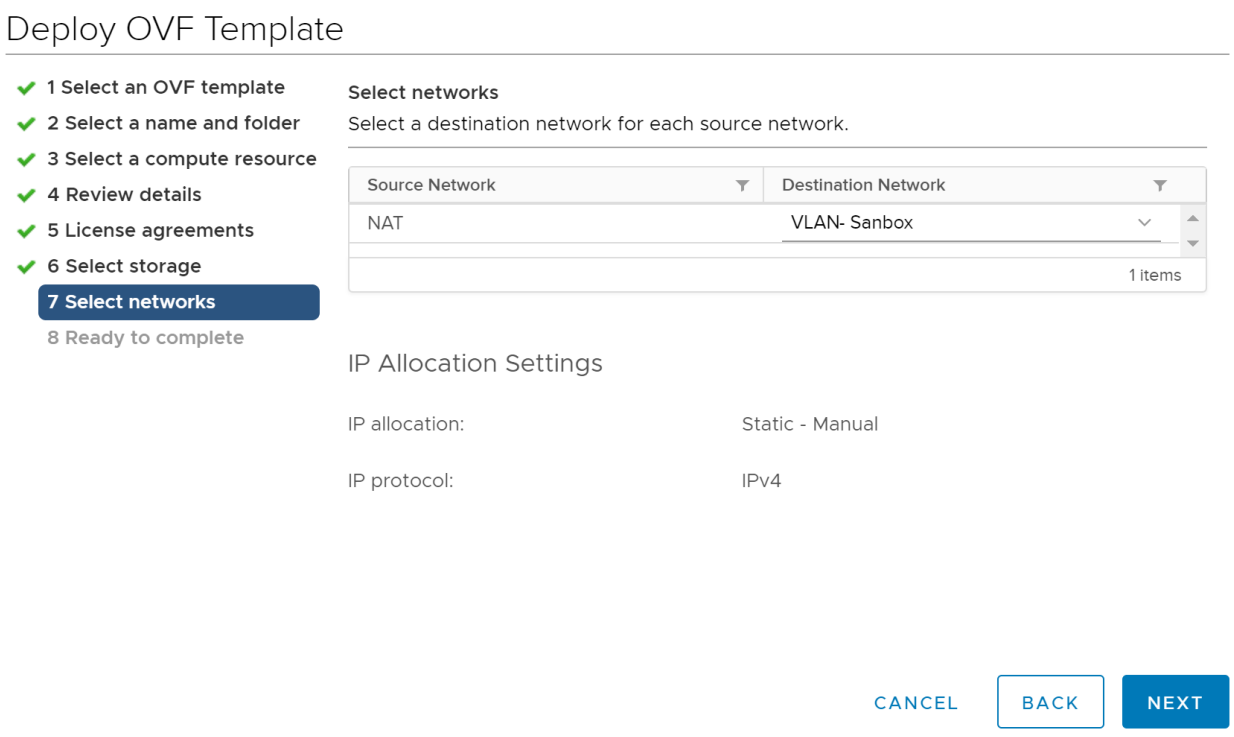
8. **5 License agreements**. Click **Next**.



9. In **6 Select Storage** select the following, then click **Next**:
   a. A disk format from the **Select virtual disk format** drop-down list. Select **Thin Provision**.
   b. A **VM Storage Policy** from the drop-down list.
   c. Select **Disable Storage DRS for this virtual machine**, if necessary, and choose the storage DRS from the table.



10. In **7 Select networks**, select the source and destination networks from the drop down lists. Click **Next**.



11. In **8 Ready to complete**, review the information and click **Finish**.

12. In the VSphere client, go to your installed OVA.

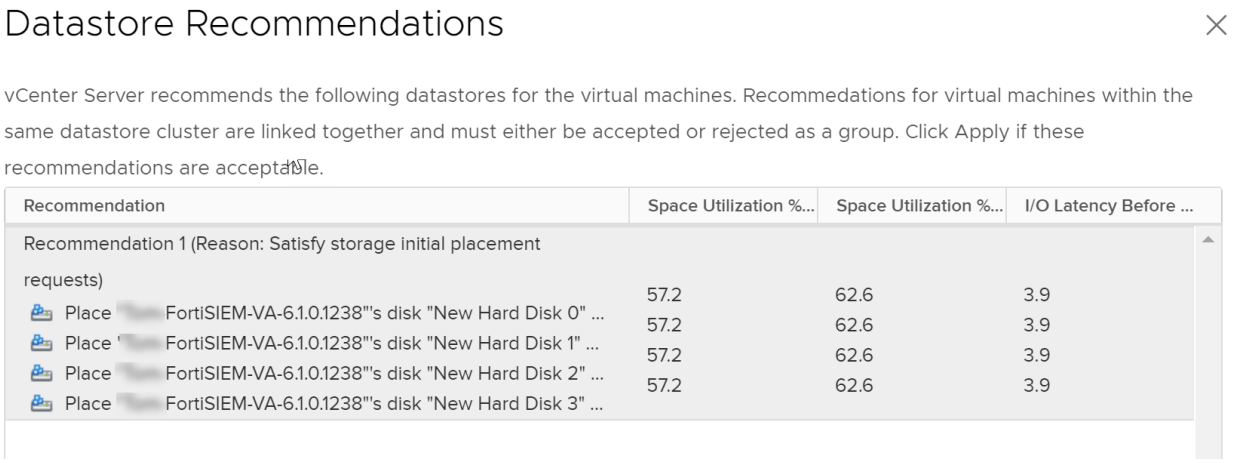
13. Right-click your installed OVA (example: `FortiSIEM-611.0374.ova`) and select **Edit Settings > VM Options > General Options** . Setup **Guest OS** and **Guest OS Version** (Linux and 64-bit).
14. Open the **Virtual Hardware** tab. Set **CPU** to 16 and **Memory** to 64GB.
15. Click **Add New Device** and create a device.
    Add additional disks to the virtual machine definition. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the following additional partitions.

Disk	Size	Disk Name
Hard Disk 2	100GB	/opt 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)

Note on Hard Disk 5:

a. 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.
b. 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.
c. 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.

16. After you click **OK**, a Datastore Recommendations dialog box opens. Click **Apply**.



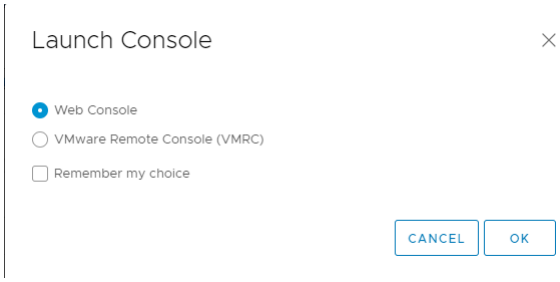
17. Do not turn off or reboot the system during deployment, which may take 7 to 10 minutes to complete. When the deployment completes, click **Close**.

Edit FortiSIEM Hardware Settings

1. In the VMware vSphere client, select the imported Supervisor.
2. Go to **Edit Settings > Virtual hardware**.
3. Set hardware settings as in Pre-Installation Checklist. The recommended settings for the Supervisor node are:
   - CPU = 16
   - Memory = 64 GB

Start FortiSIEM from the VMware Console

1. In the VMware vSphere client, select the Supervisor, Worker, or Collector virtual appliance.
2. Right-click to open the options menu and select **Power > Power On**.
3. Open the Summary tab for the , select **Launch Web Console**.
   Network Failure Message: When the console starts up for the first time you may see a `Network eth0 Failed` message, but this is expected behavior.
4. Select **Web Console** in the Launch Console dialog box.



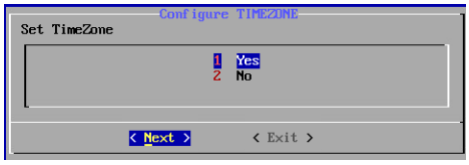
5. When the command prompt window opens, log in with the default login credentials – user: `root` and Password: `ProspectHills`.
6. You will be required to change the password. Remember this password for future use.

At this point, you can continue to Configure FortiSIEM.

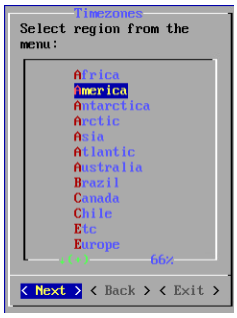
Configure FortiSIEM

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

1. Log in as user `root` with the password you set in Step 6 above.
2. At the command prompt, enter `configFSM.sh`, for example:
   `# configFSM.sh`
3. In VM console, select **1 Set Timezone** and then press **Next**.

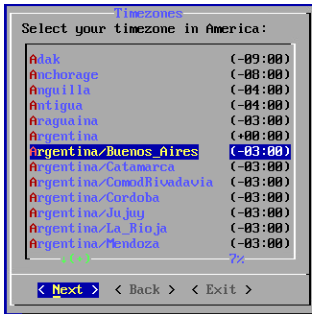


4. Select your **Region**, and press **Next**.

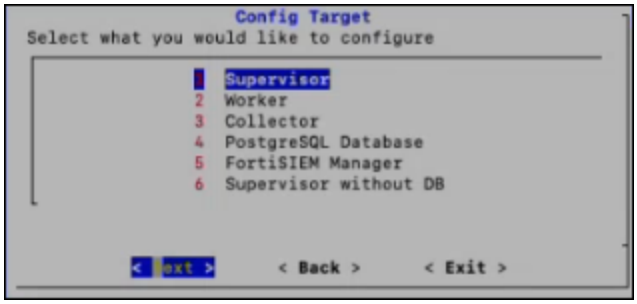


5. Select your **Country**, and press **Next**.

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



7. If installing a Supervisor, select **1 Supervisor**. Press **Next**.
   If installing a Worker, select **2 Worker**, and press **Next**.
   If installing a Collector, select **3 Collector**, and press **Next**.
   If Installing for automated High Availability, select **4 PostgreSQL Database**, and press **Next**.
   If Installing FortiSIEM Manager, select **5 FortiSIEM Manager**, and press **Next**.
   If Installing FortiSIEM Supervisor without DB (Follower), select **6 Supervisor without DB** and press **Next**.
   Note: The appliance type cannot be changed once it is deployed, so ensure you have selected the correct option.

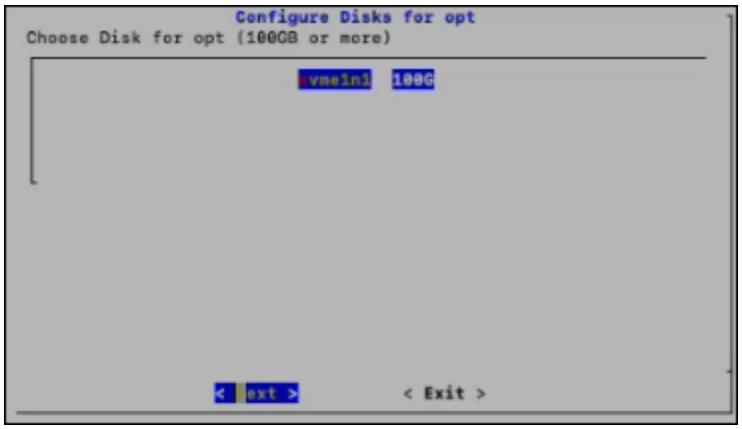


Regardless of whether you select **FortiSIEM Manager**,**Supervisor**, **Supervisor without DB**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

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

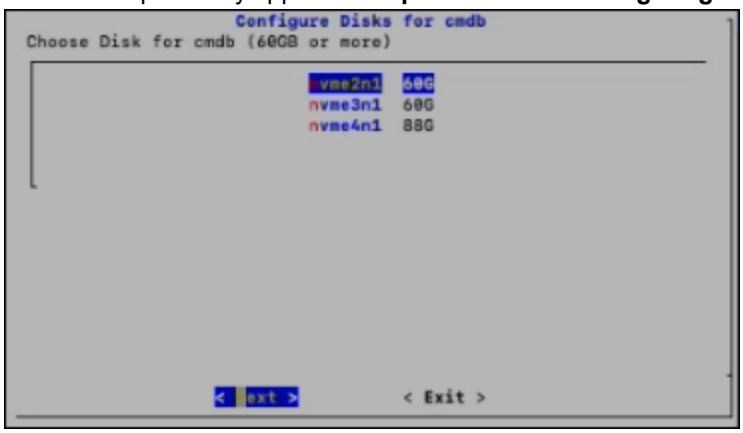
8. If you want to enable FIPS, then choose **2**. Otherwise, choose **1**. You have the option of enabling FIPS (option **3**) or disabling FIPS (option **4**) later.
   Note: After Installation, a 5th option to change your network configuration (**5 change_network_config**) is available. This allows you to change your network settings and/or host name.

9. Select the disk for opt and press **Next**.
   Note: This option only appears if **Supervisor**, **Worker** or **Collector** is selected as **Config Target**.



10. Select the disk for cmdb and press **Next**.

Note: This option only appears if **Supervisor** is the **Config Target**.



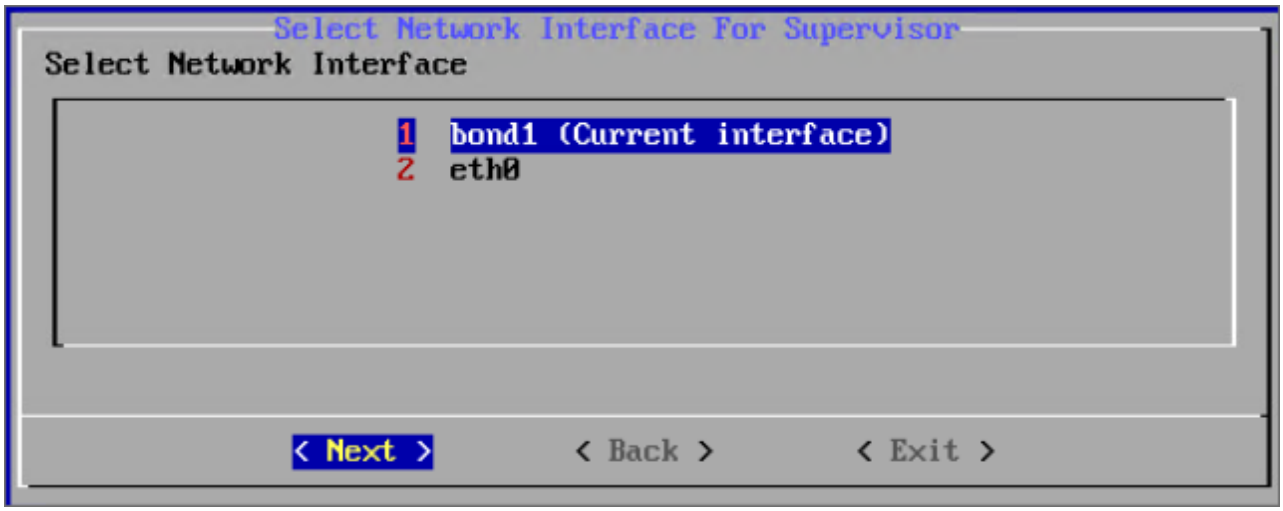
11. Confirm the disk for svn and press **Next**.

    Note: This option only appears if **Supervisor** is the **Config Target**.

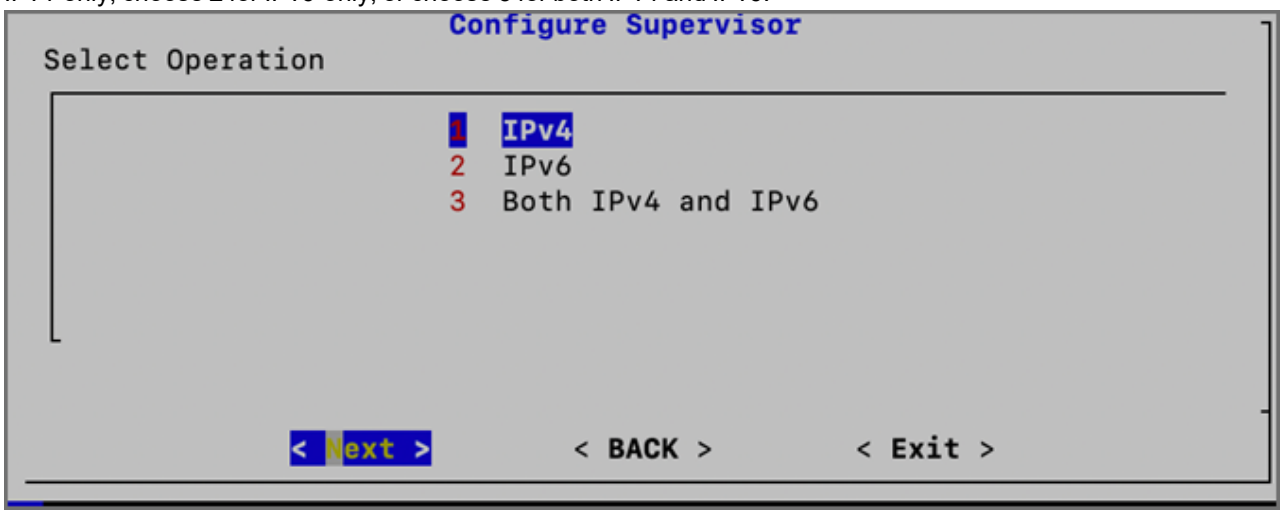
12. Confirm the selected disks (opt, cmdb, svn) for **Supervisor**, opt for **Worker** and **Collector**, and press **Next**, or press **Back** as needed to re-configure.

13. 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.

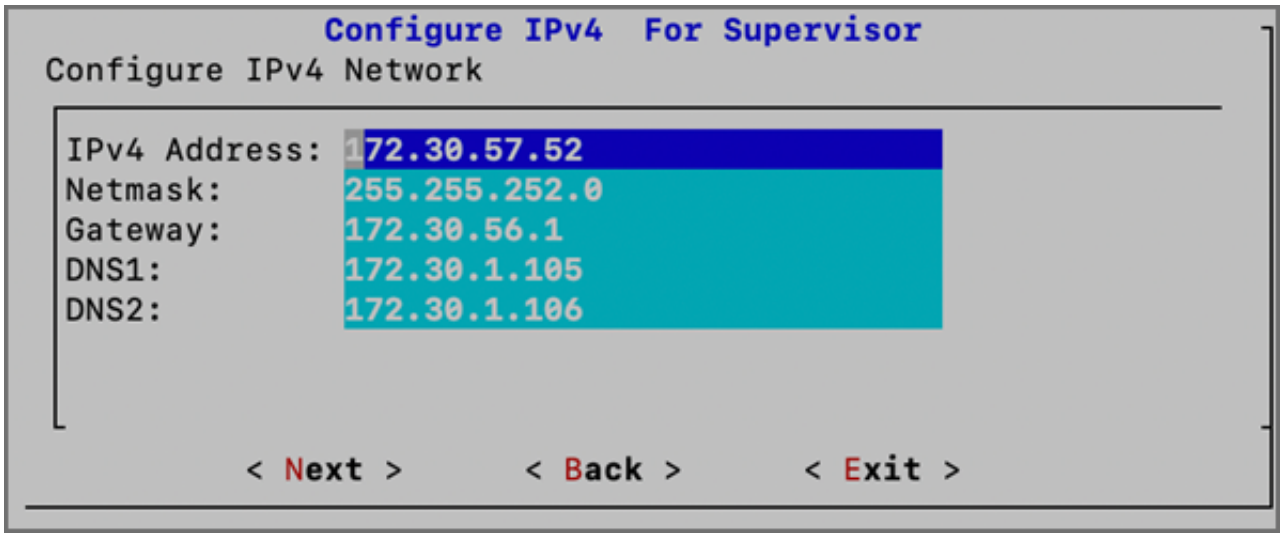


14. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



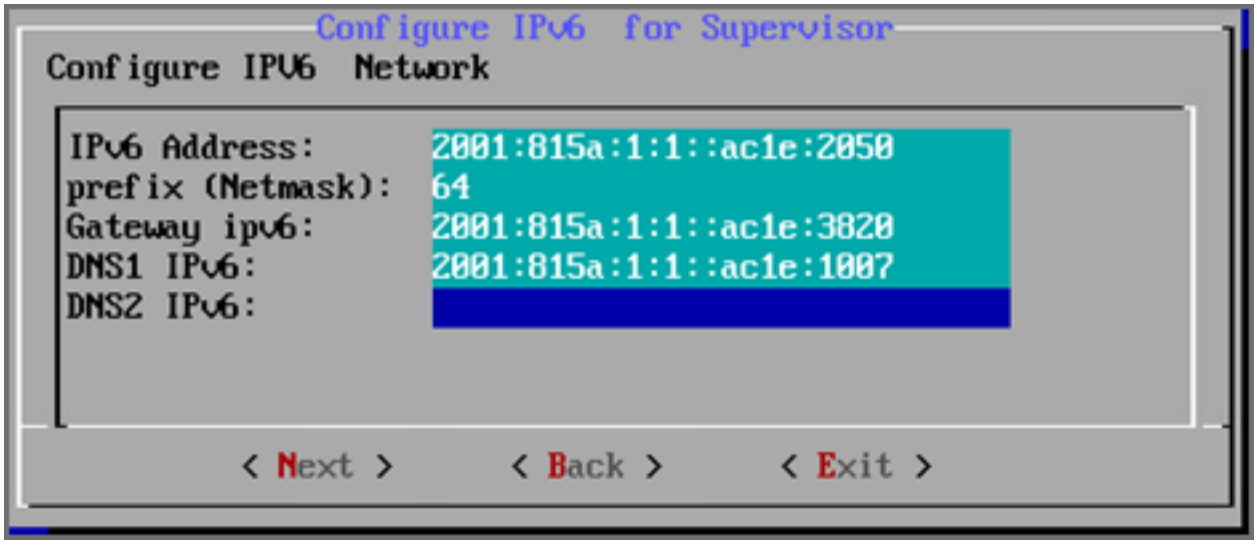
15. If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 16. If you choose **2** (IPv6), and press **Next**, then skip to step 17.
16. Configure the IPv4 network by entering the following fields, then press **Next**.

Option	Description
IPv4 Address	The Manager/Supervisor/Worker/Collector's IPv4 address
NetMask	The Manager/Supervisor/Worker/Collector's IPv4 subnet
Gateway	IPv4 Network gateway address
DNS1, DNS2	Addresses of the IPv4 DNS server 1 and DNS server2



17. If you chose **1** in step 14, then you will need to skip to step 18. If you chose **2** or **3** in step 14, then you will configure the IPv6 network by entering the following fields, then press **Next**.

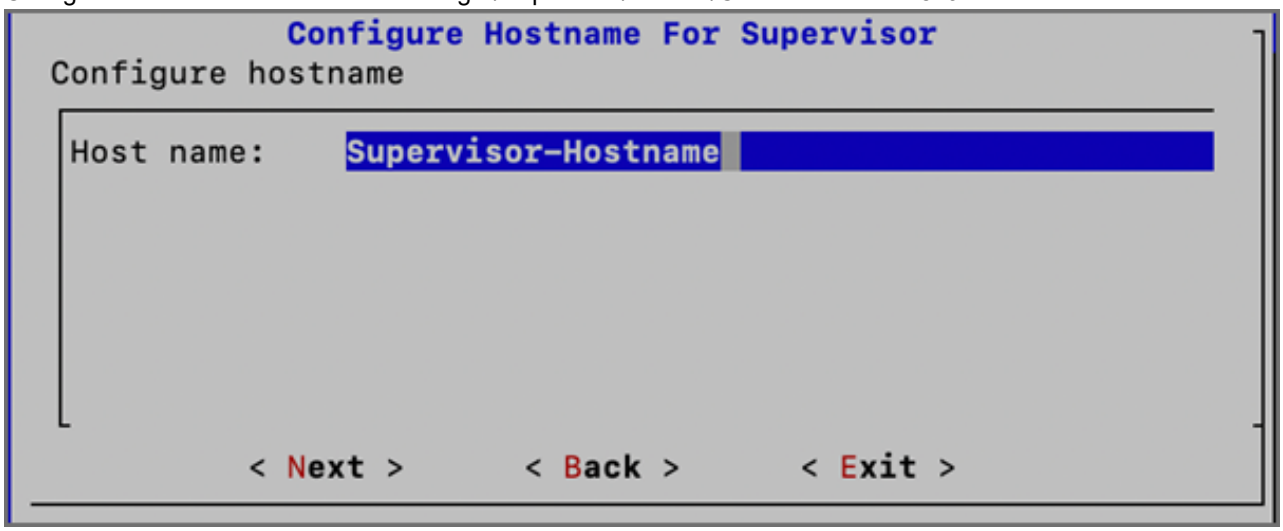
Option	Description
IPv6 Address	The Manager/Supervisor/Worker/Collector's IPv6 address
prefix (Netmask)	The Manager/Supervisor/Worker/Collector's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2



Note: If you chose option **3** in step 14 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

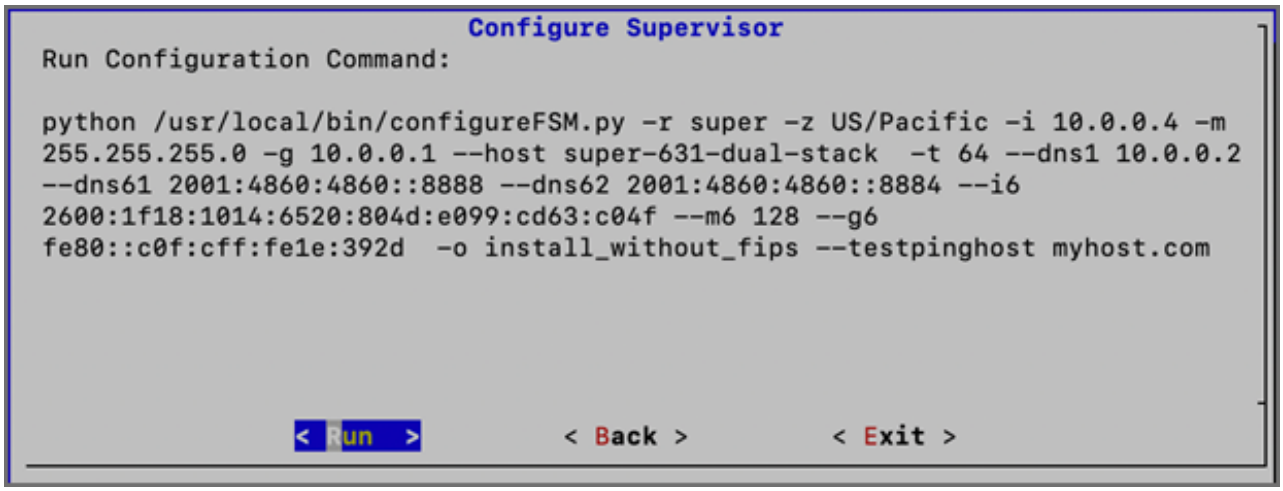
environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

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



19. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a 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.

20. 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 DNS server 1 and DNS server 2.
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (**install_without_fips**, **install_with_fips**, **enable_fips**, or **disable_fips**, **change_network_config***) *Option only available after installation.
--testpinghost	The URL used to test connectivity

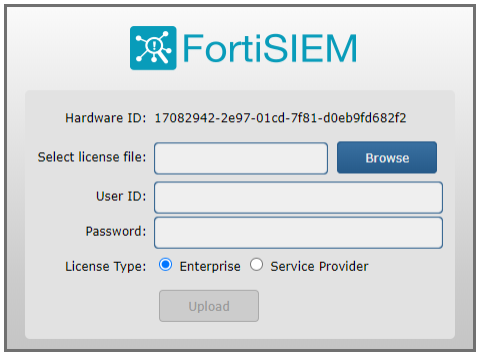
21. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the `ansible.log` file located at `/usr/local/fresh-install/logs` to try and identify the problem.

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.

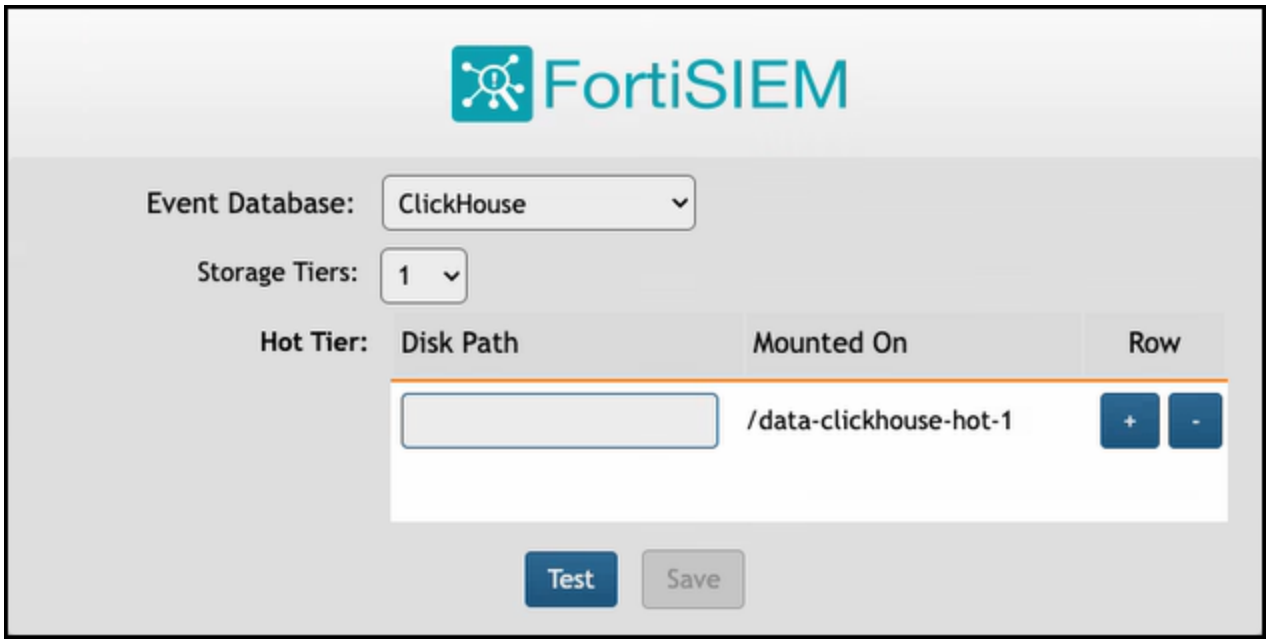
1. Open a Web browser and log in to the FortiSIEM UI. Use link `https://<supervisor-ip>` to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input `https://[IPv6 address]` on the browser tab.
2. The License Upload dialog box will open.



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 Configuring ClickHouse Storage.
  Recommended for most deployments. Please see ClickHouse Reference Architecture for more information.
- **EventDB on Local Disk**: See Configuring EventDB Storage.

Final Check

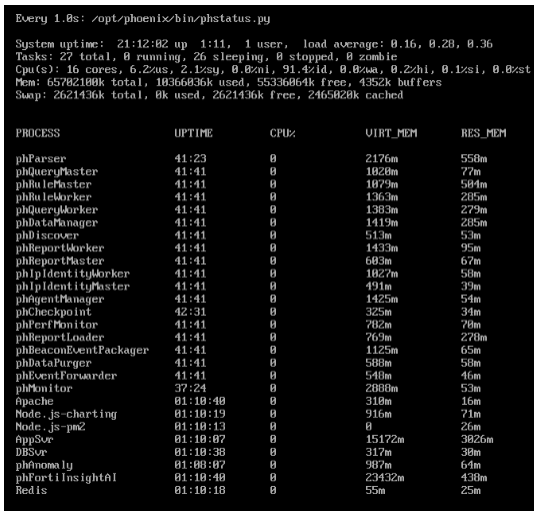
FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

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

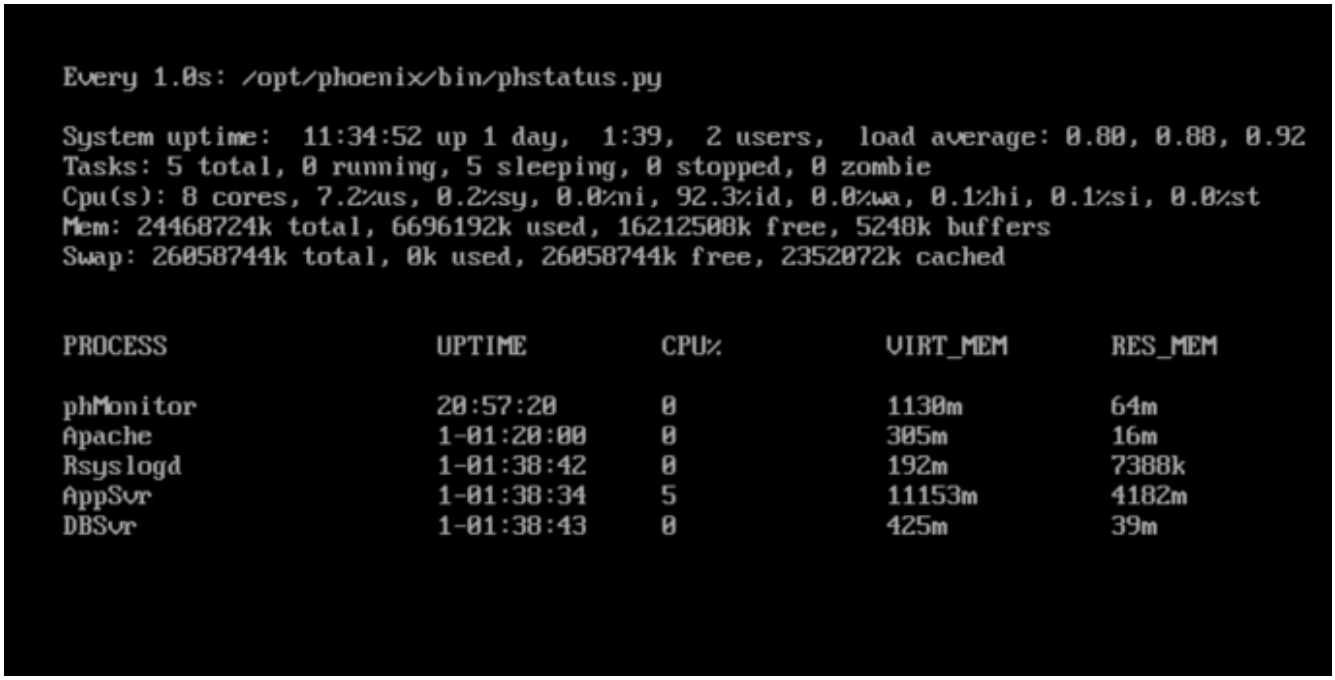
After installation completes, ensure that the `phMonitor` is up and running, for example:

```
# phstatus
```

For the Supervisor, Supervisor without DB (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).

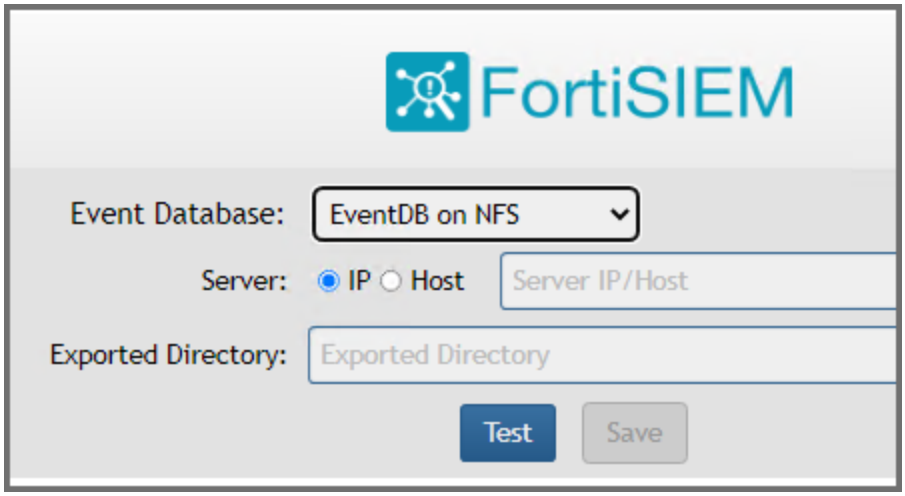
- Install Supervisor
- Install Workers
- Register Workers
- Create ClickHouse Topology (Optional)

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

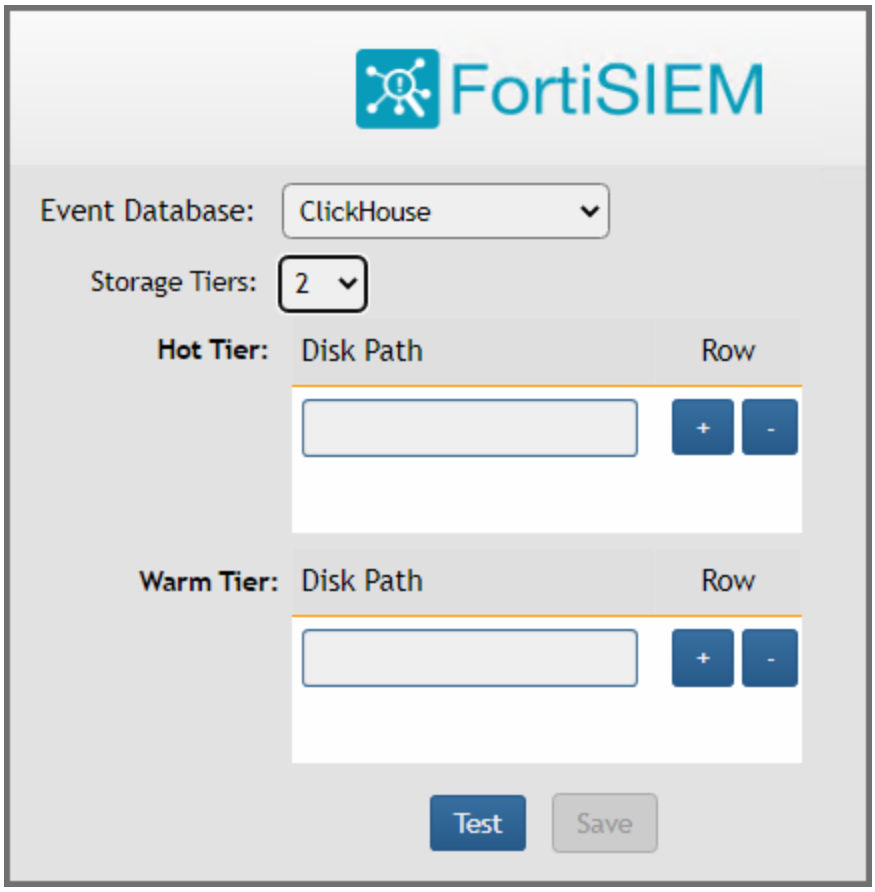
Install Supervisor

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

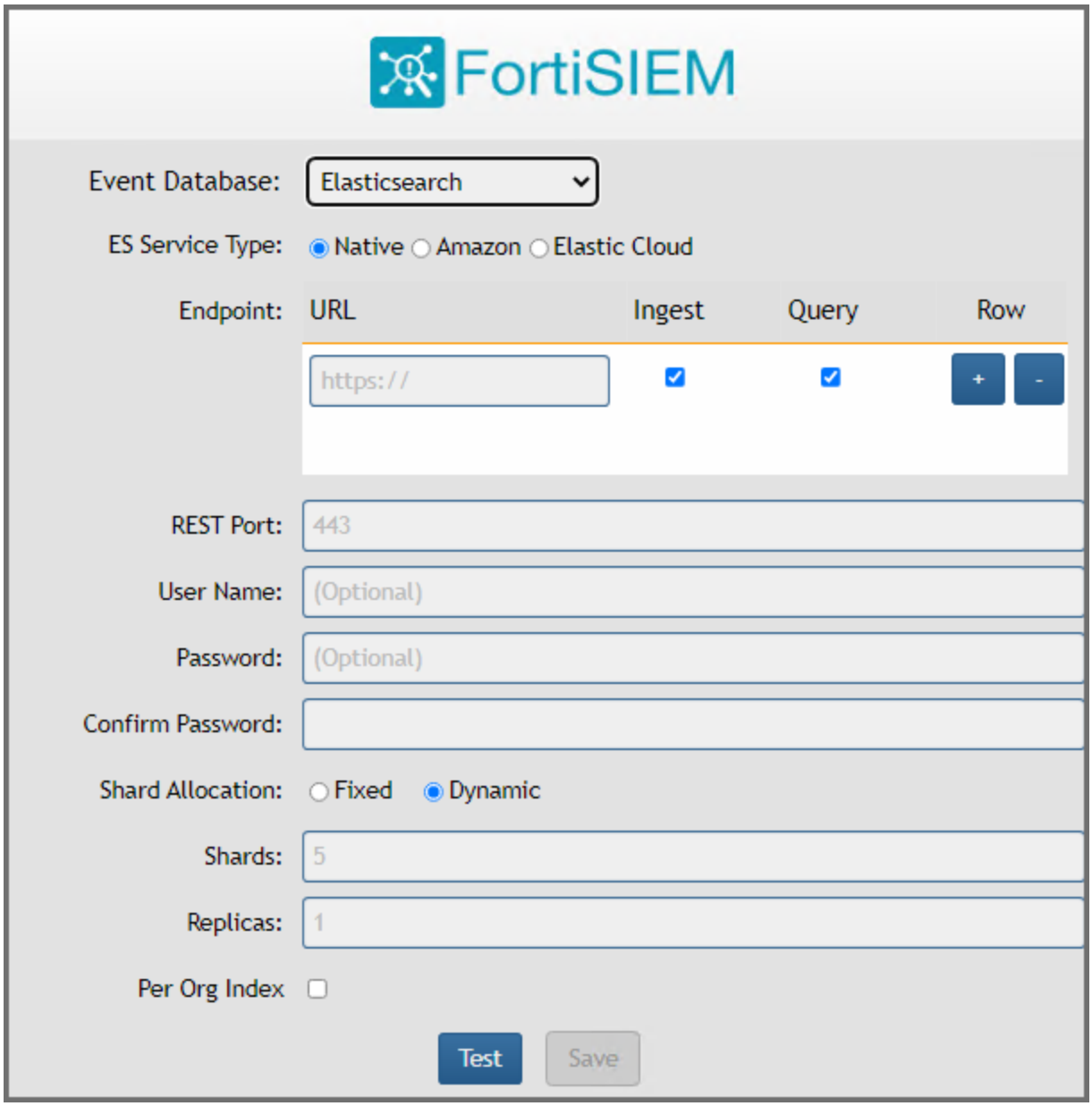
1. Event Database choices are **EventDB on NFS**, **ClickHouse**, or **Elasticsearch**.
2. If you choose **EventDB on NFS**
   a. Disk 5 is not required (From Import FortiSIEM into ESX Step 15).
   b. You need to configure NFS after license upload.



3. If you choose **ClickHouse**
   a. You need to create disks during Import FortiSIEM into ESX step 15 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.

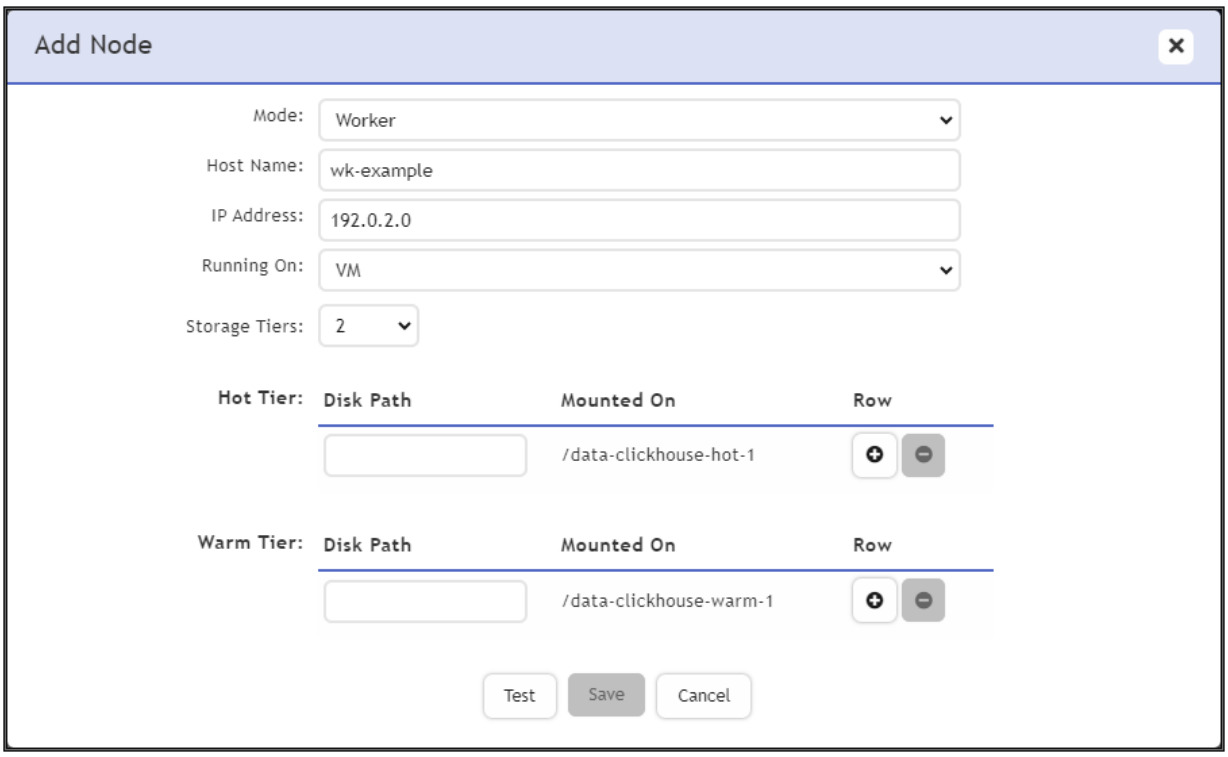
      For **Disk Path**, use one of the following CLI commands to find the disk names.

      ```
      fdisk -l
      ```

      or

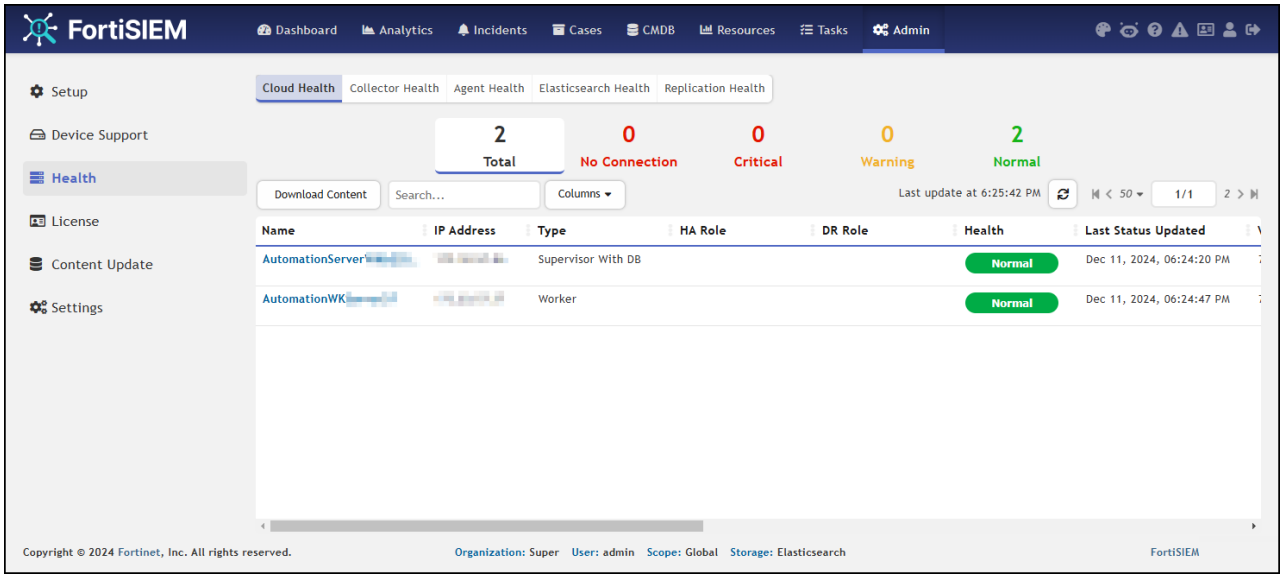
      ```
      lsblk
      ```

      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, only choose OS and OPT disks.

- Collector in Regular IT Environments
- Collector with Different OPT Disk Sizes

Collector in Regular IT Environments

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.

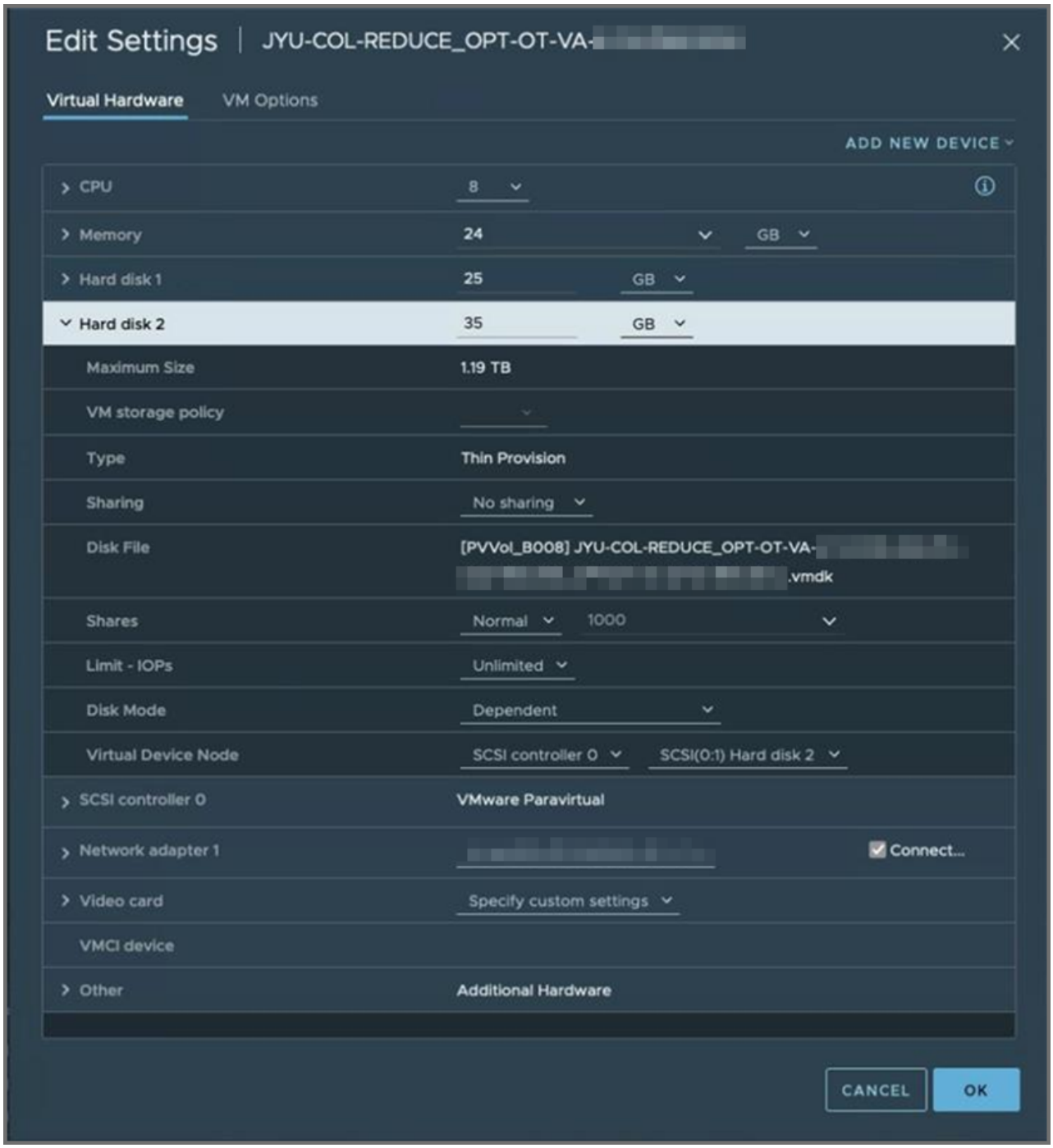
Collector with Different OPT Disk Sizes

FortiSIEM installations require the disk for OPT+SWAP to have exactly 100 GB. This is valid for all three node options (Supervisor, Worker and Collectors).

Depending on your situation, you may want to increase or decrease the size of the log collector. For example, an Operational Technology (OT) may find it difficult to dedicate 125 GB to a log collector, and want to decrease the size of the log collector. In another circumstance, a company may want to increase the event cache for their collectors, which usually means increasing the OPT disk size. For more information, see Increasing Collector Event Buffer Size in the Online Help.

The steps here explain how to bypass the requirement for Collector install. Be aware that reducing the size of the disk also reduces the size of the available cache when there is a connection interruption between Collector and Workers/Supervisor, and may result in loss of logs. Increasing the size of the disk provides a larger available cache.

1. Follow the installation guide but instead of adding a 100 GB disk for OPT, add a disk of whatever size you require.
2. In this example, we will assume the OPT disk is 35 GB, so in total, the Collector VM will have 70 GB (25 for OS + 35 for OPT).



3. After you boot the VM and change the password, you will be editing the following files.
   - /usr/local/syslib/config/disksConfig.json
   - /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml

   Note: You must make changes to these files **before** running the configureFSM.sh installer.
4. The `disksConfig.json` file contains a map of installation types and node types. It defines the required sizes of disks so that the installer can validate them. Since we are changing the KVM Collector opt disk requirement to 35 GB in this example, we must reflect that size in this file. Using a text editor, modify the "opt" line in the `disksConfig.json` file, shown in blue to your requirement.

```
"FSIEMVMWARE": {
  "SUPER": {
    "number": "3",
    "opt": "100",
    "svn": "60",
    "cmdb": "60"
  },
  "FSMMANAGER": {
    "number": "2",
    "opt": "100",
    "cmdb": "60"
  },
  "WORKER": {
    "number": "1",
    "opt": "100"
  },
  "COLLECTOR": {
    "number": "1",
    "opt": "35"
  }
},
```

5. Save the `disksConfig.json` file.
6. Load the `/usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml` file via a text editor. You can choose to adjust only the (step a) OPT disk or (step b) adjust the swap disk and OPT disk. To change only the OPT disk, proceed with step a, then skip to step 7. To adjust the swap disk and reduce the OPT disk, skip step a and proceed with step b.
   a. **ADJUST OPT DISK ONLY**

      Navigate to line 54 in the /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml file and change the line.

      Original line (The original line assumes the drive is 100 GB)

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
      100G && sleep 5
      ```

      Change this line to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

      ```
      parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
      35G && sleep 5
      ```

      Skip step b and c, and proceed to step 7.
   b. **ADJUST SWAP DISK and REDUCE OPT DISK**

      Reduce the Swap Disk by changing the following original line (The original line assumes swap disk to be 25GB).

      ```
      parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
      25G && sleep 5
      ```

      Change to (in this example 10G), marked in blue:

      ```
      parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
      10G && sleep 5
      ```
   c. Reduce /OPT disk: by changing the following line (The original line assumes the drive is 100 GB).

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
100G && sleep 5
```

Change to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 11G
35G && sleep 5
```

7. Save the `disks.yml` file.
8. Run configFSM.sh to install the collector. When it reboots, you can provision it using the `phProvisionCollector` command. Your partition output should appear similar to the following.

```
Partition Output of deployment:
sdb           8:16   0   35G  0 disk
├─sdb1        8:17   0  8.4G  0 part [SWAP]
└─sdb2        8:18   0 22.4G  0 part /opt

# df -h
Filesystem           Size  Used Avail Use% Mounted on
devtmpfs              12G     0   12G   0% /dev
tmpfs                 12G     0   12G   0% /dev/shm
tmpfs                 12G   17M   12G   1% /run
tmpfs                 12G     0   12G   0% /sys/fs/cgroup
/dev/mapper/rl-root   22G  8.1G   14G  38% /
/dev/sdb2             23G  4.3G   19G  19% /opt
/dev/sda1           1014M  661M  354M  66% /boot
tmpfs                2.4G     0  2.4G   0% /run/user/500
tmpfs                2.4G     0  2.4G   0% /run/user/0
```

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 **Save**.
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.

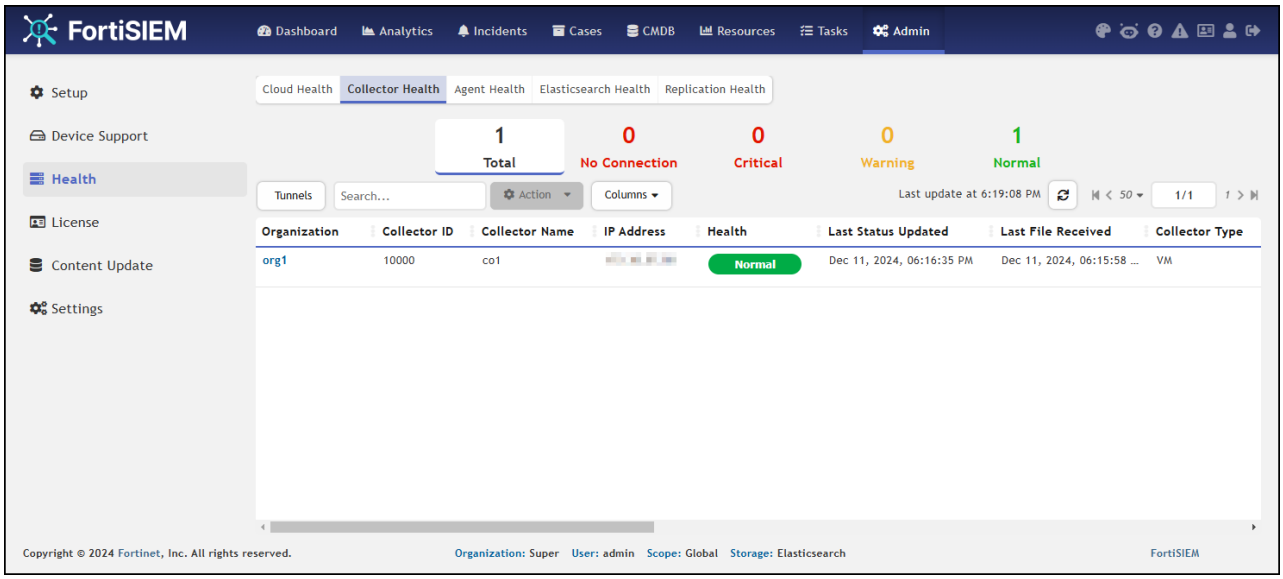
c. **Start Time** and **End Time** – set to **Unlimited**.

4. SSH to the Collector and run following script to register Collectors:
   `# /opt/phoenix/bin/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.



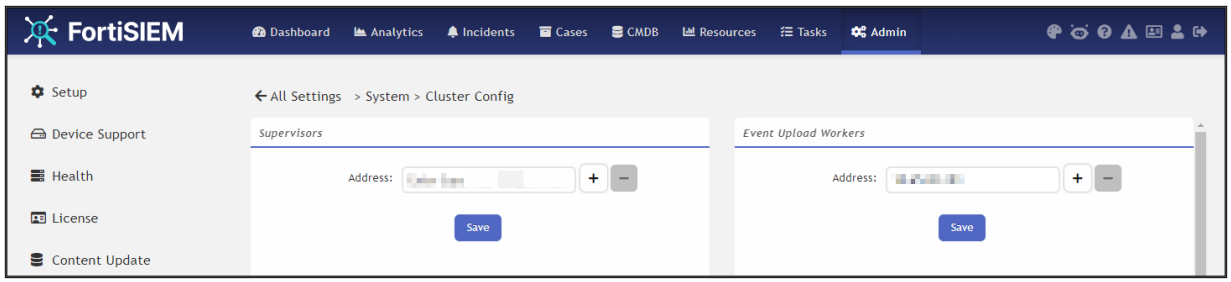
Service Provider Deployments

For Service Provider deployments, follow these steps.

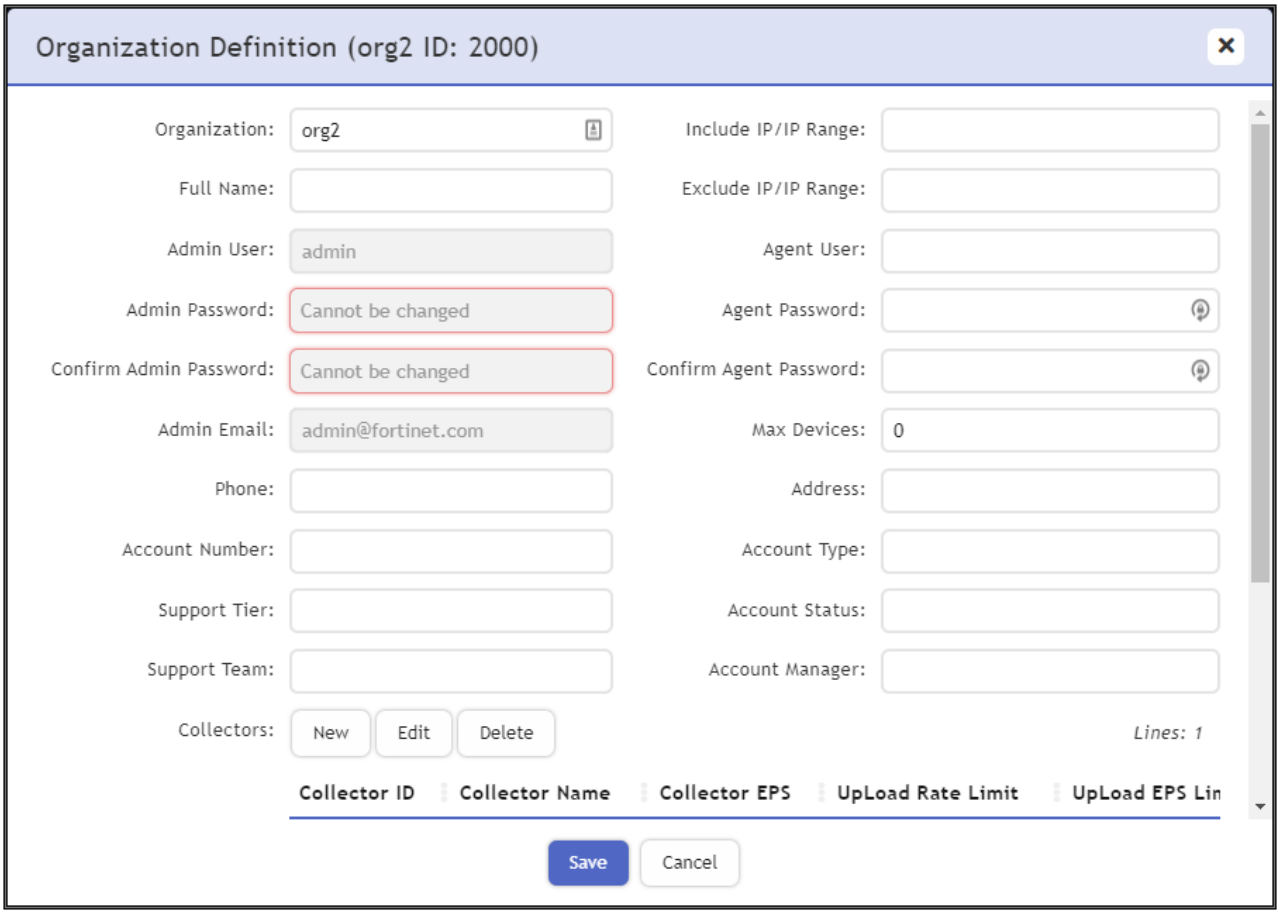
1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Cluster Config**.
   a. Under **Event Upload Workers**, enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate 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 **Save**.

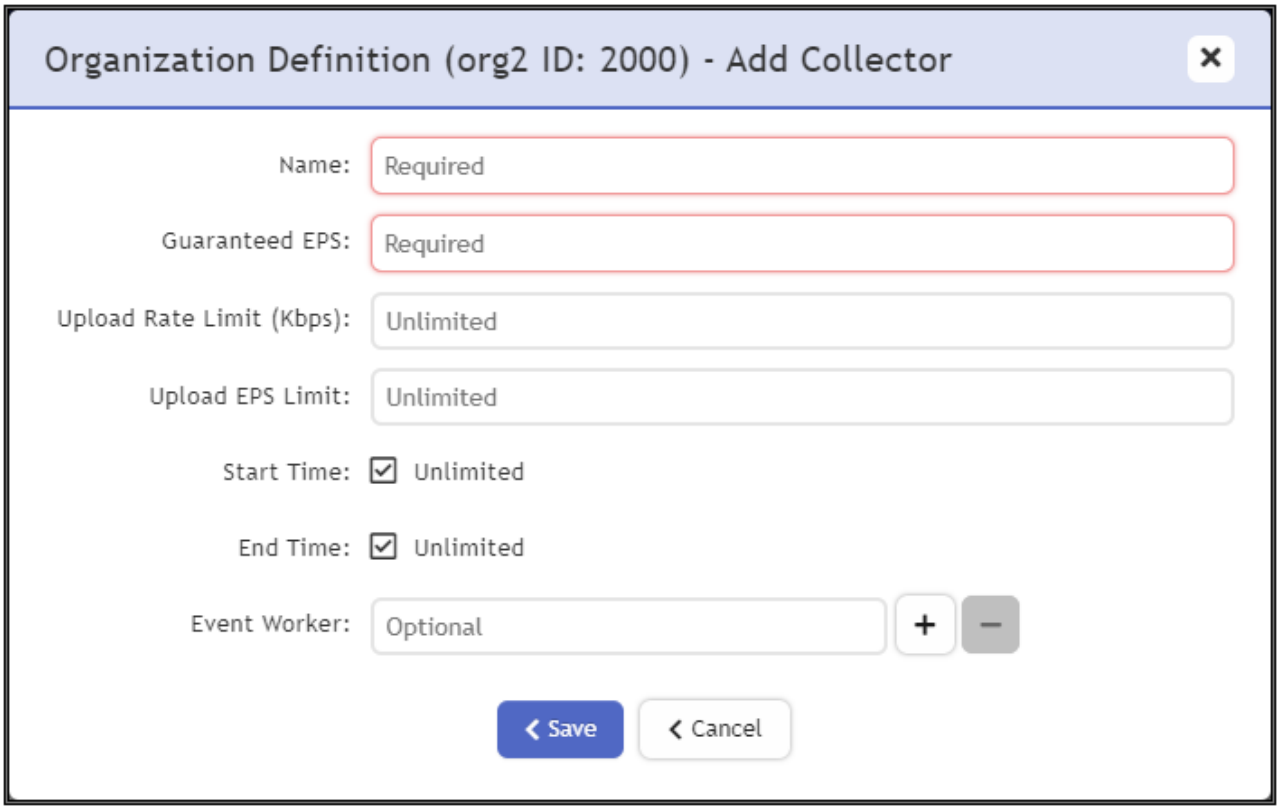
c.



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



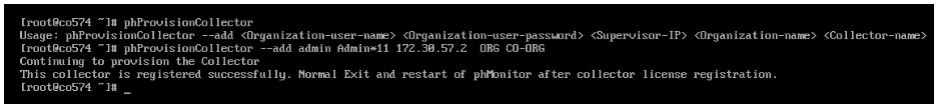
4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
5. Under **Collectors**, click **New**.
6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.
   The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS 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:
   `# /opt/phoenix/bin/phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization> <CollectorName>`

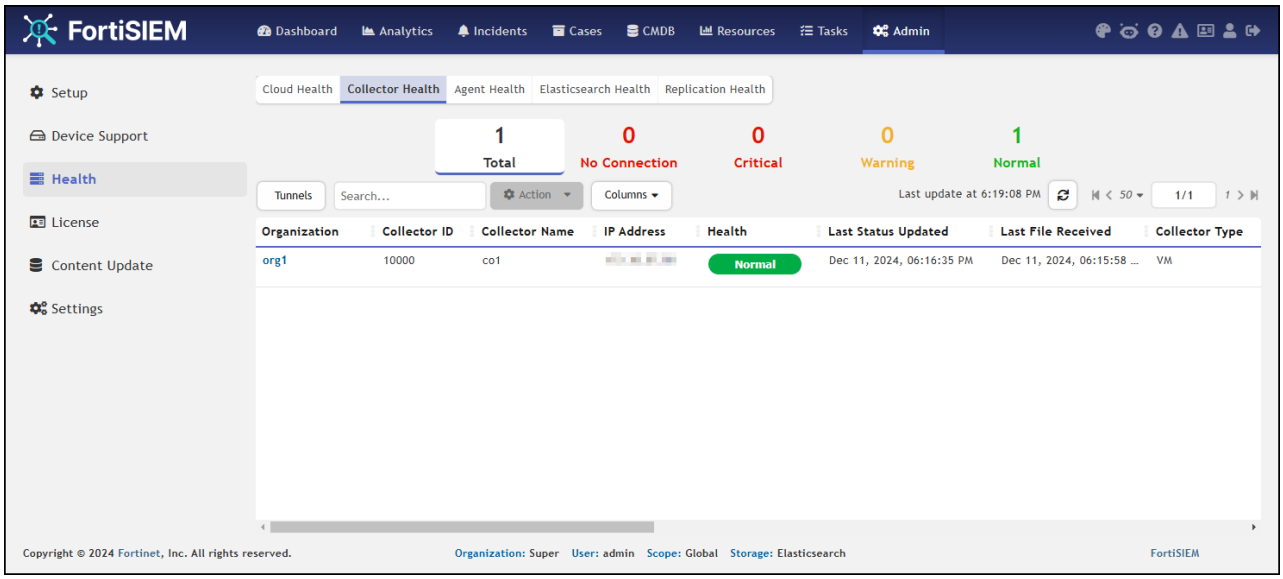
   The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

   a. Set `user` and `password` use the admin User Name and password for the 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.

   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 itself 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

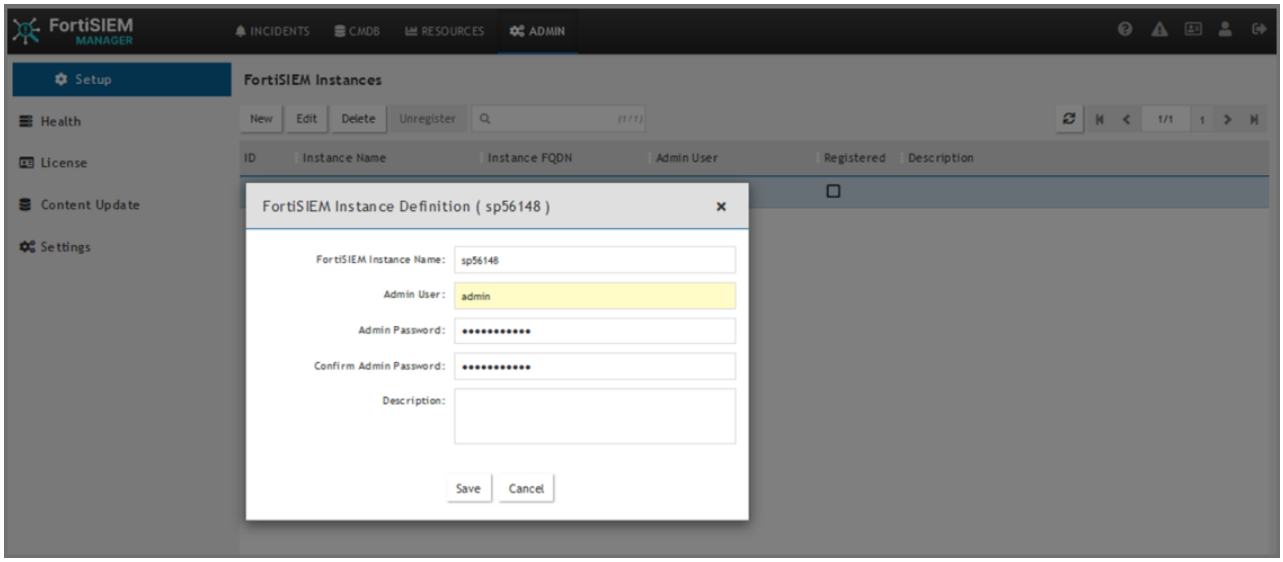
Note that Communication between FortiSIEM Manager and instances is via REST APIs over HTTP(S).

Add 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**.

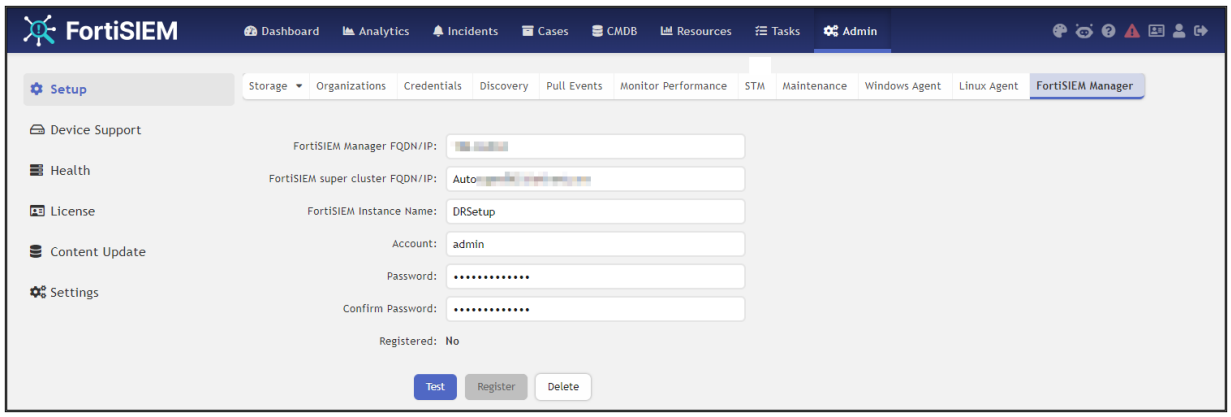


10. Repeat steps 1-9 to add any additional instances to Manager.
    Now, follow the instructions in Register the Instance Itself to Manager for each instance.

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.

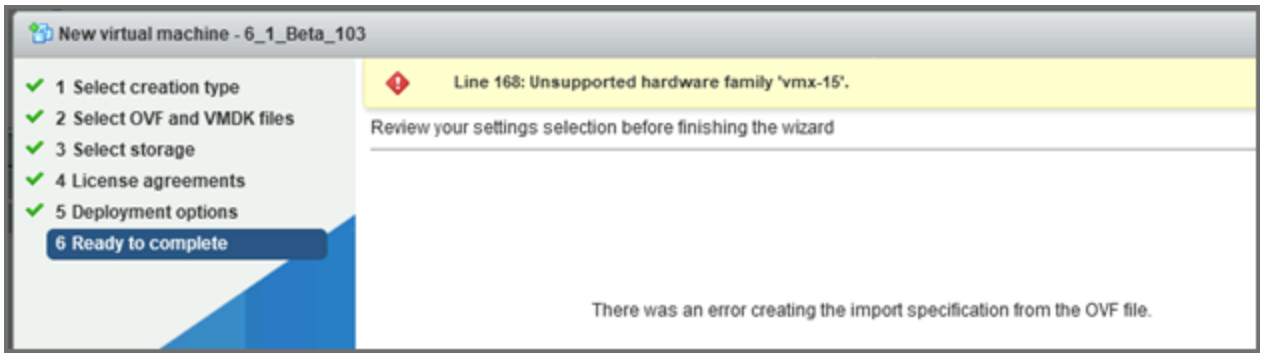


i. Login to Manager, and navigate to any one of the following pages to verify registration.
   - **ADMIN > Setup** and check that the box is marked in the **Registered** column for your instance.
   - **ADMIN > Health**, look for your instance under FortiSIEM Instances.
   - **ADMIN > License**, look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

Installing on ESX 6.5

Importing a 6.5 ESX Image

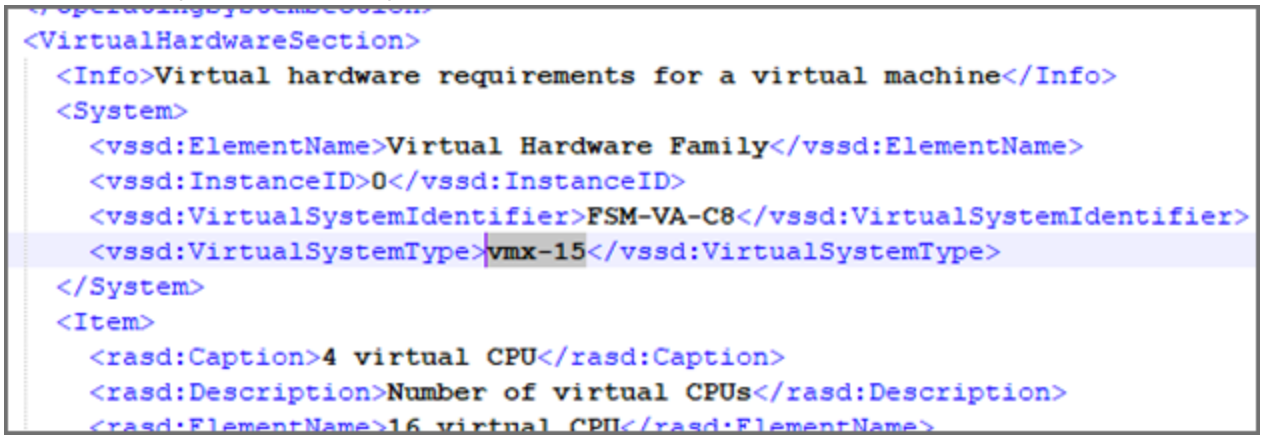
When installing with ESX 6.5, or an earlier version, you will get an error message when you attempt to import the image.



To resolve this import issue, you will need to take the following steps:

1. Install 7-Zip.
2. Extract the OVA file into a directory.

3. In the directory where you extracted the OVA file, edit the file `FortiSIEM-VA-7.3.2.0374.ovf`, and replace all references to `vmx-15` with your compatible ESX hardware version shown in the following table.
   Note: For example, for ESX 6.5, replace `vmx-15` with `vmx-13`.



   Note: For example, for ESX 6.5, replace `vmx-15` with `vmx-13`.

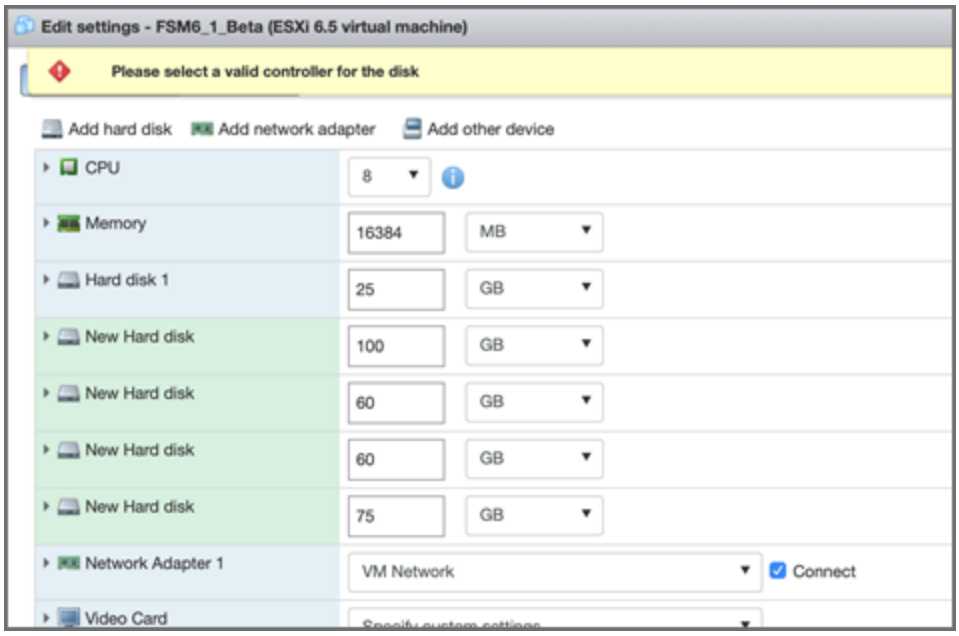
Compatibility	Description
EXSi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5.
EXSi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0 and ESXi 6.5.
EXSi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXSi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXSi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXI 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
ESX/EXSi 4.0 and later	This virtual machine (hardware version 7) is compatible with ESX/ESXi 4.0, ESX/ESXi 4.1, ESXI 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXS/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, ESXI 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5. It is also compatible with VMware Server 1.0 and later. ESXi 5.0 does not allow creation of virtual machines with ESX/ESXi 3.5 and later compatibility, but you can run such virtual machines if they were created on a host with different compatibility.
ESX Server 2.x and later	This virtual machine (hardware version 3) is compatible with ESX Server 2.x, ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, and ESXI 5.0. You cannot create, edit, turn on, clone, or migrate virtual machines with ESX Server 2.x compatibility. You can only register or upgrade them.

   Note: For more information, see here.
4. Right click on your host and choose **Deploy OVF Template**. The Deploy OVA Template dialog box appears.
5. In **1 Select an OVF template**, select **Local File**.
6. Navigate to the folder with the OVF file.
7. Select all the contents that are included with the OVF.

8. Click **Next**.

Resolving Disk Save Error

You may encounter an error message asking you to select a valid controller for the disk if you attempt to add an additional 4th disk (`/opt`, `/cmd`, `/svn`, and `/data`). This is likely due to an old IDE controller issue in VMware, where you are normally limited to 2 IDE controllers, 0, 1, and 2 disks per controller (Master/Slave).

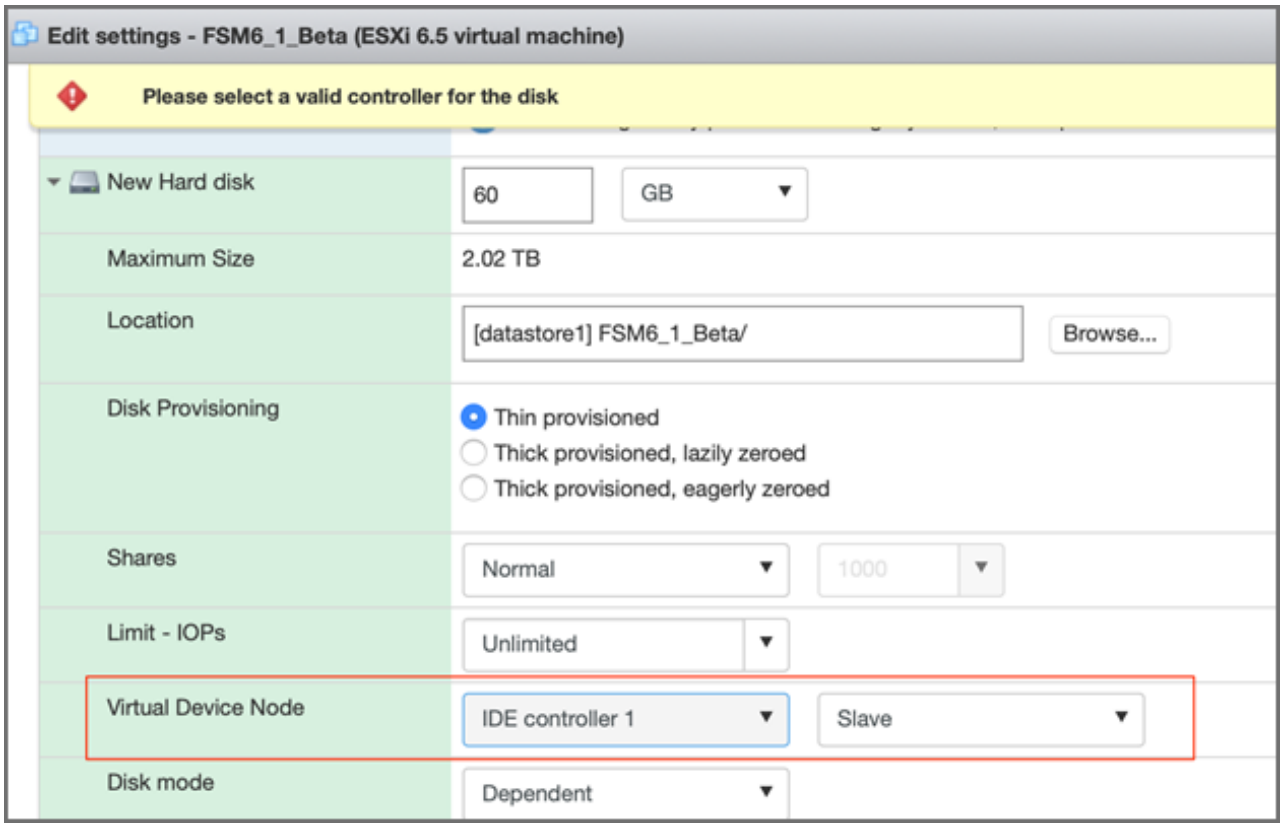


If you are attempting to add 5 disks in total, such as this following example, you will need to take the following steps:

Disk	Usage
1st	25GB default for image
2nd	100GB for `/opt` 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.
3rd	60GB for `/cmdb`
4th	60GB for `/svn`
5th	75GB for `/data` (optional, or use with NFS or ES storage)

1. Go to Edit settings, and add each disk individually, clicking save after adding each disk.
   When you reach the 4th disk, you will receive the "Please select a valid controller for the disk" message. This is because the software has failed to identify the virtual device node controller/Master or Slave for some unknown reason.
2. Expand the disk setting for each disk and review which IDE Controller Master/Slave slots are in use. For example, in one installation, there may be an attempt for the 4th disk to be added to IDE Controller 0 when the Master/Slave

slots are already in use. In this situation, you would need to put the 4th disk on IDE Controller 1 in the Slave position, as shown here. In your situation, make the appropriate configuration setting change.



3. Click save to ensure your work has been saved.

Adding a 5th Disk for /data

When you need to add a 5th disk, such as for `/data`, and there is no available slot, you will need to add a SATA controller to the VM by taking the following steps:

1. Go to Edit settings.
2. Select **Add Other Device**, and select **SCSI Controller** (or SATA).

You will now be able to add a 5th disk for `/data`, and it should default to using the additional controller. You should be able to save and power on your VM. At this point, follow the normal instructions for installation.

Note: When adding the local disk in the GUI, the path should be `/dev/sda` or `/dev/sdd`. You can use one of the following commands to locate:

```
# fdisk -l
```

or

```
# lsblk
```

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