



KVM Installation Guide

FortiSIEM 7.3.0



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



12/16/2024

FortiSIEM 7.3.0 KVM Installation Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Import FortiSIEM into KVM	7
Configure FortiSIEM	15
Upload the FortiSIEM License	23
Configure an Event Database	23
Final Check	24
Cluster Installation	25
Install Supervisor	26
Install Workers	28
Register Workers	29
Create ClickHouse Topology (Optional)	30
Install Collectors	31
Register Collectors	35
Install Manager	39
Register Instances to Manager	39
Install Log	42

Change Log

Date	Change Description
12/16/2024	Release of FortiSIEM - KVM Installation Guide for 7.3.0.

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 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
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Choose storage type for Supervisor, Worker, and/or Collector
 - Online storage - There are 4 choices
 - ClickHouse – Recommended for most deployments. Please see the [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 CMDDB – 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 CMDDB – 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 CMDDB – 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.

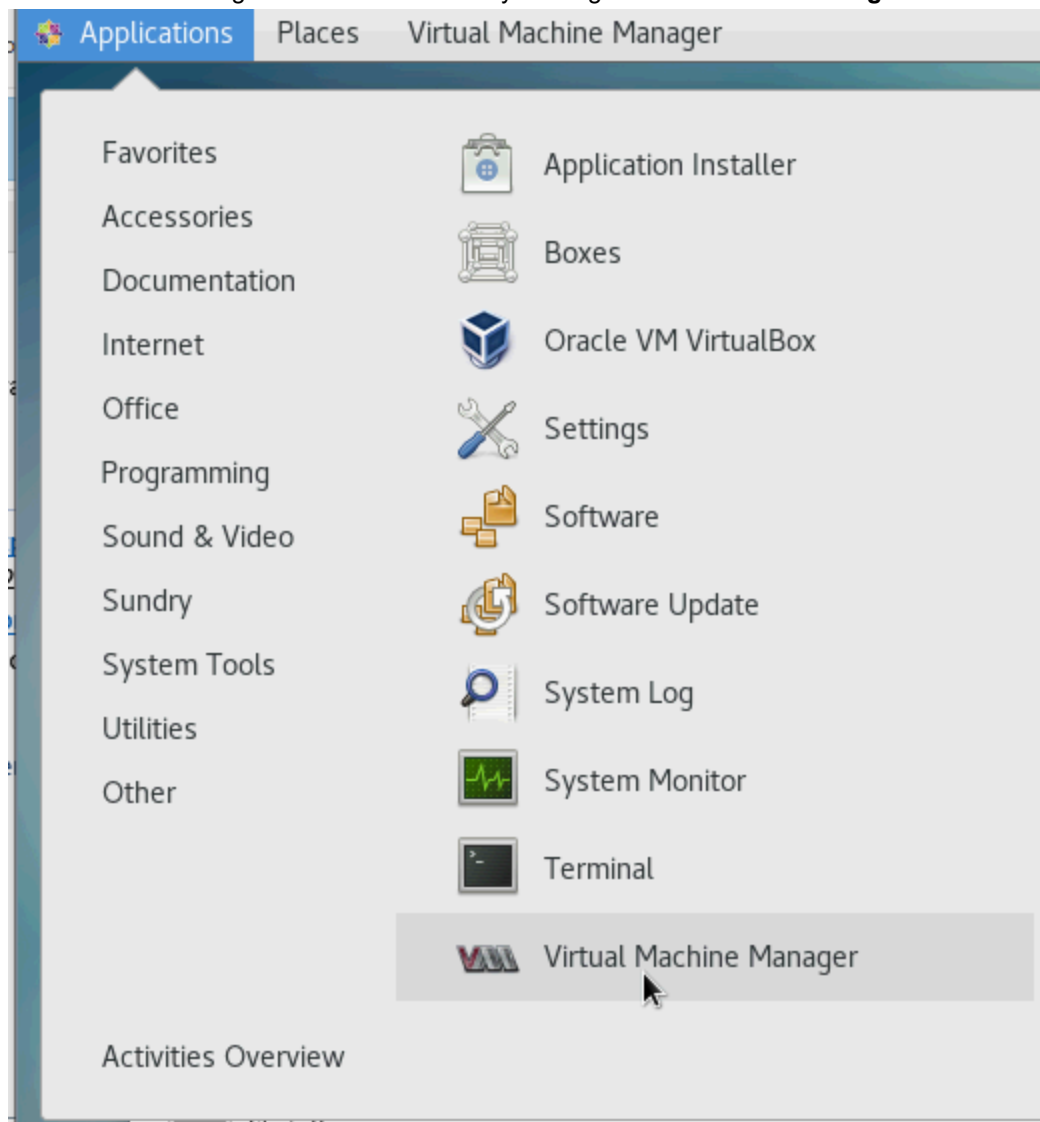
- [Import FortiSIEM into KVM](#)
- [Configure FortiSIEM](#)

- [Upload the FortiSIEM License](#)
- [Configure an Event Database](#)
- [Final Check](#)

Import FortiSIEM into KVM

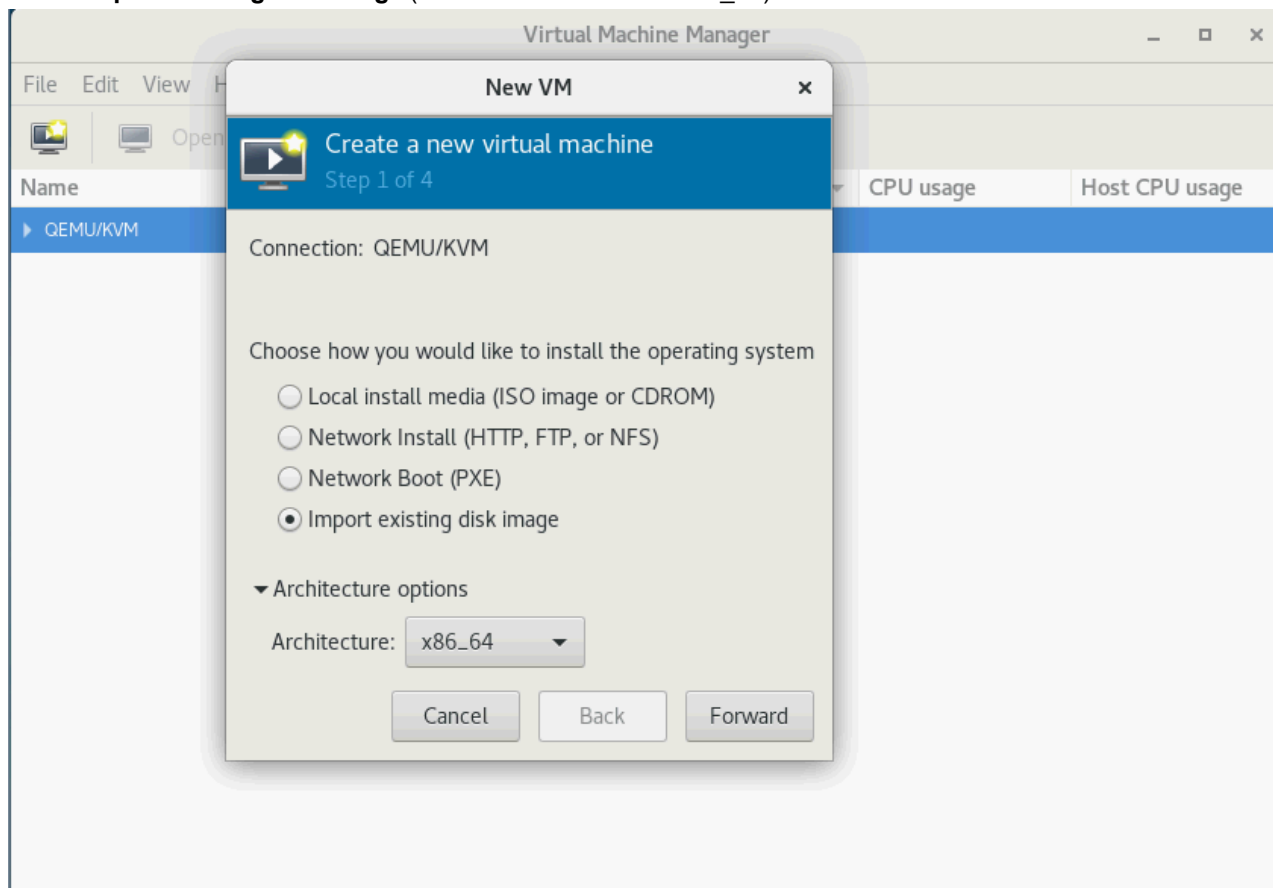
1. Go to the Fortinet Support website <https://support.fortinet.com> to download the KVM package `FSM_Full_All_KVM_7.3.0_build0338.zip`. See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Download the packages for Super/Worker and Collector to the location where you want to install the image. For example: `FSM_Full_All_KVM_7.3.0_build0338.zip`.
3. Unzip the `.zip` file to get the `FortiSIEM-7.3.0.0338.qcow2` file.
4. Copy the above unzipped `qcow2` file into the storage image location separately for the installation of super, worker, and collector. For example:
`/var/lib/libvirt/images/super/FortiSIEM-7.3.0.0338.qcow2`
`/var/lib/libvirt/images/worker/FortiSIEM-7.3.0.0338.qcow2`
`/var/lib/libvirt/images/collector/FortiSIEM-7.3.0.0338.qcow2`

5. Start the KVM Manager for the KVM server by clicking **Virtual Machine Manager**.

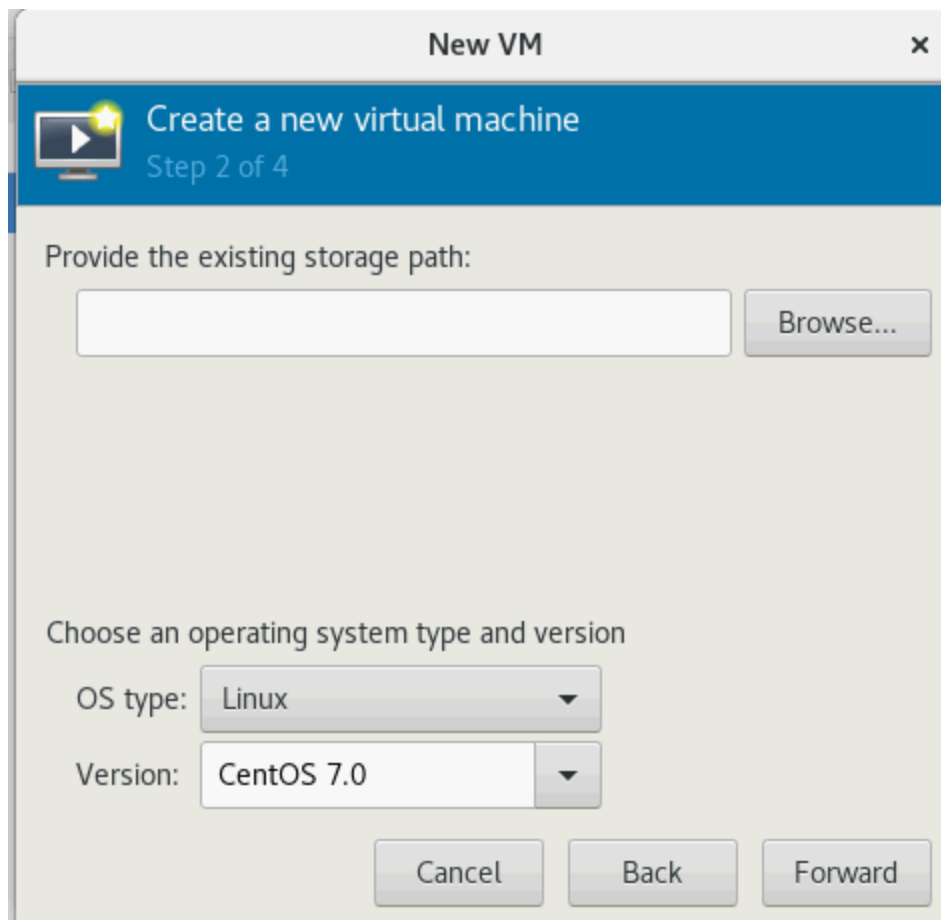


6. Click **Create a new virtual machine** from the **Virtual Machine Manager**.

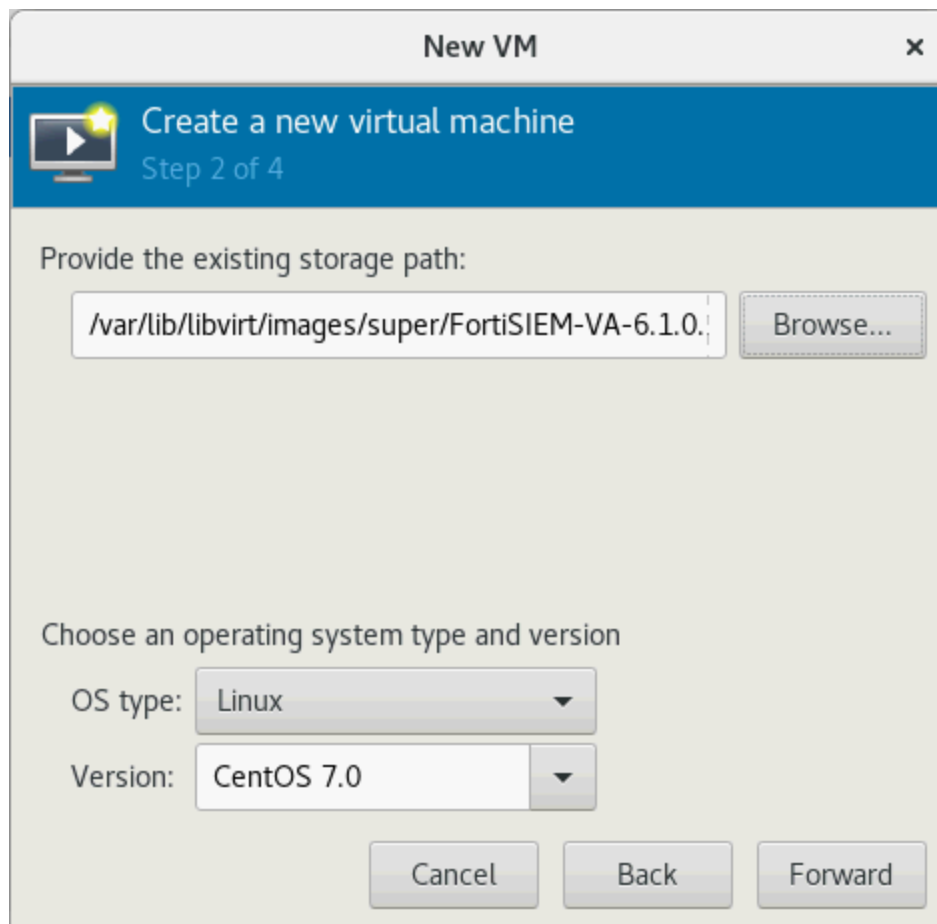
7. Select **Import existing disk image** (Architecture defaults to x86_64).



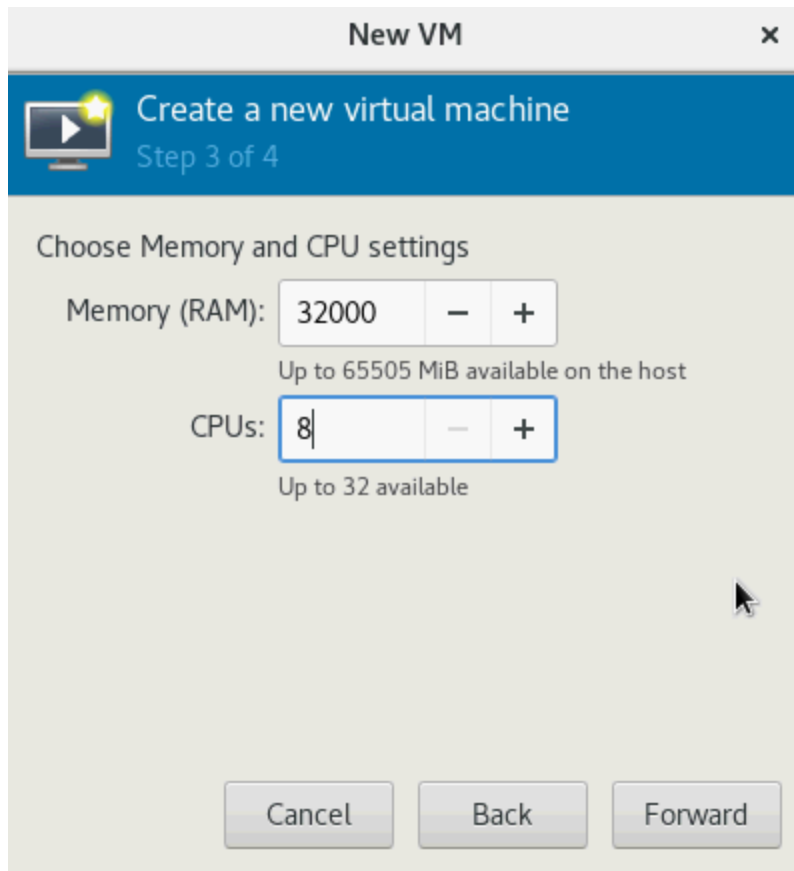
8. Click **Forward** from the above step, and select the OS type as **Linux** and Version to **CentOS 7.0**, then click **Forward**.



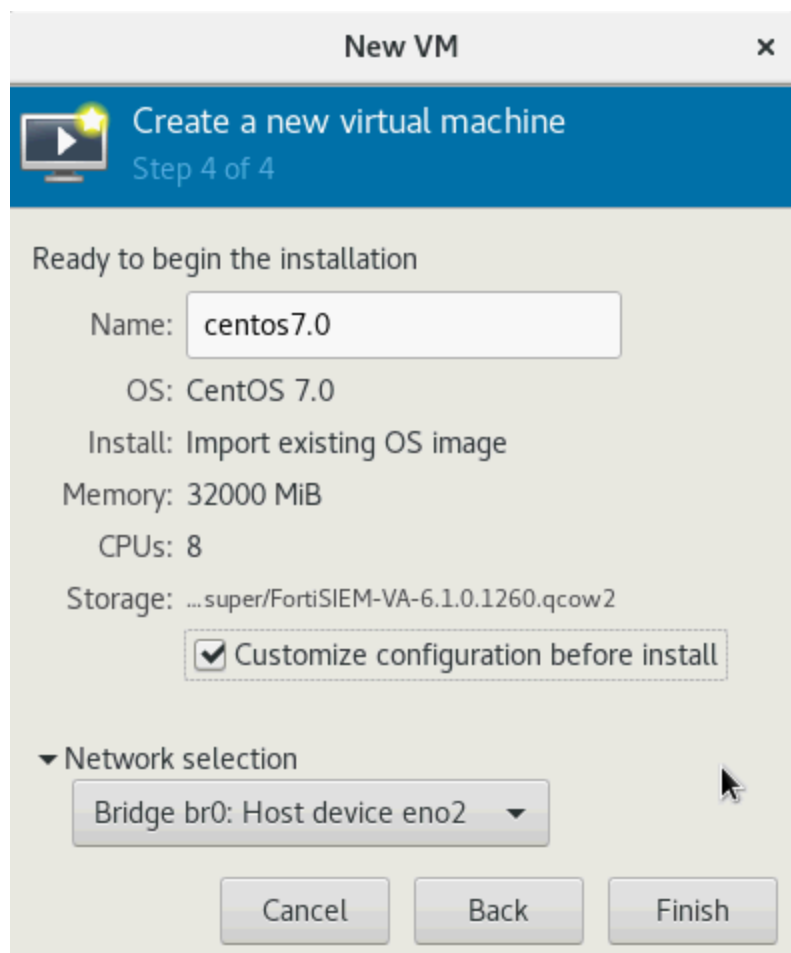
9. Click **Browse...** from the **New VM** dialog box to find the location for the file (for example, `FortiSIEM-7.3.0.0338.qcow2`). Or, you can directly copy the path and the `qcow2` file name under **Provide the existing storage path**. Click **Forward**.



10. In the New VM dialog box, change **Memory** from **1024** to **32000 (32 GB)**. Change the **CPUs** from **1** to **8**. Click **Forward**.



11. Before clicking **Finish**, make sure to check that the **Network selection** is a **Bridge**, and **Customize configuration before install** is selected. Then, click **Finish**.



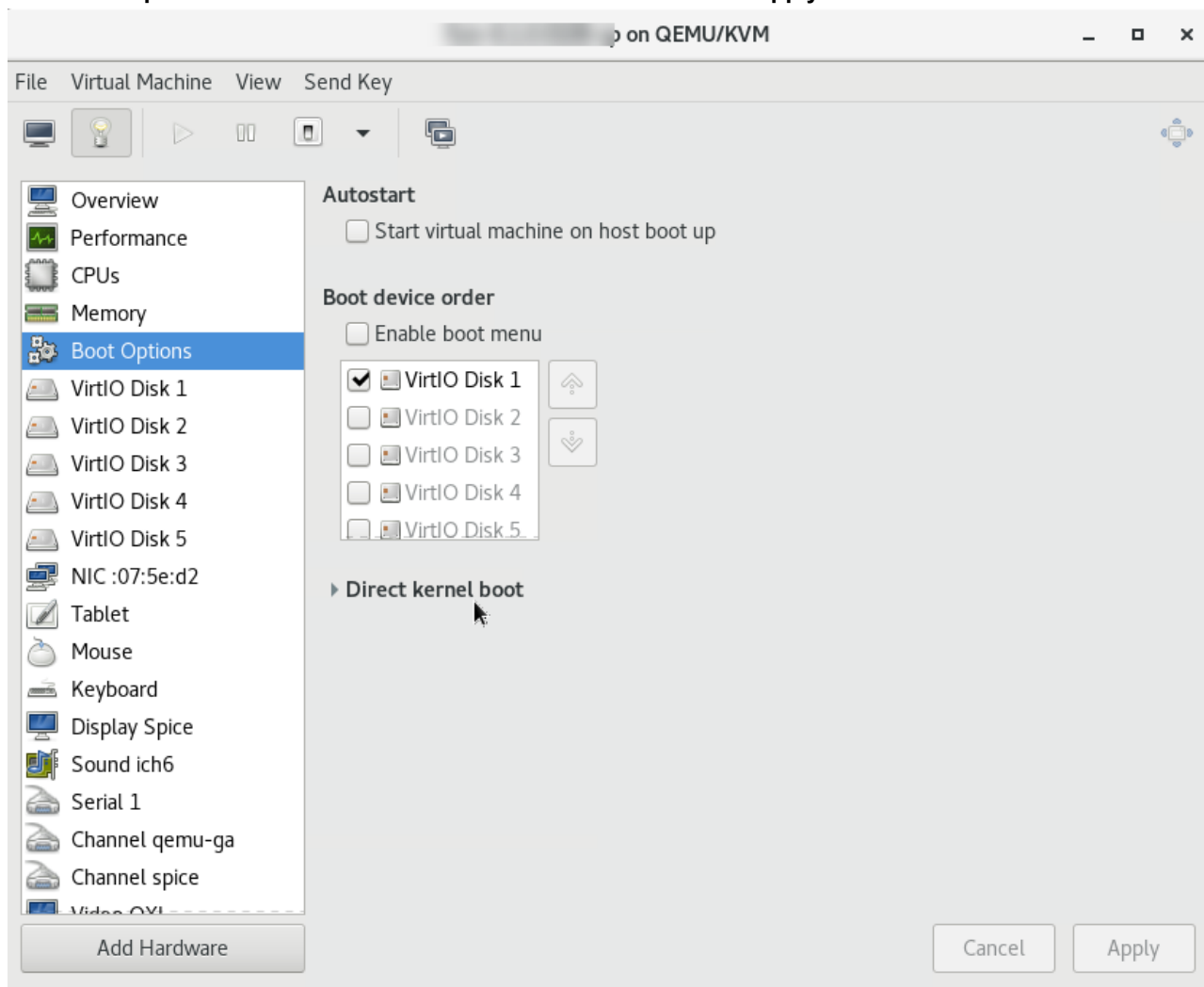
12. Start to make the configuration. This is the place where you change the name from the default name centos 7.0 in the Overview.



In every step in this configuration, you must click **Apply** to save your changes.

13. Click **VirtIO Disk 1** (the default disk) and check that the **Source** path is correct. Click **Apply**.

14. Click **Boot Options** and make sure that **VirtIO Disk 1** is checked. Click **Apply**.



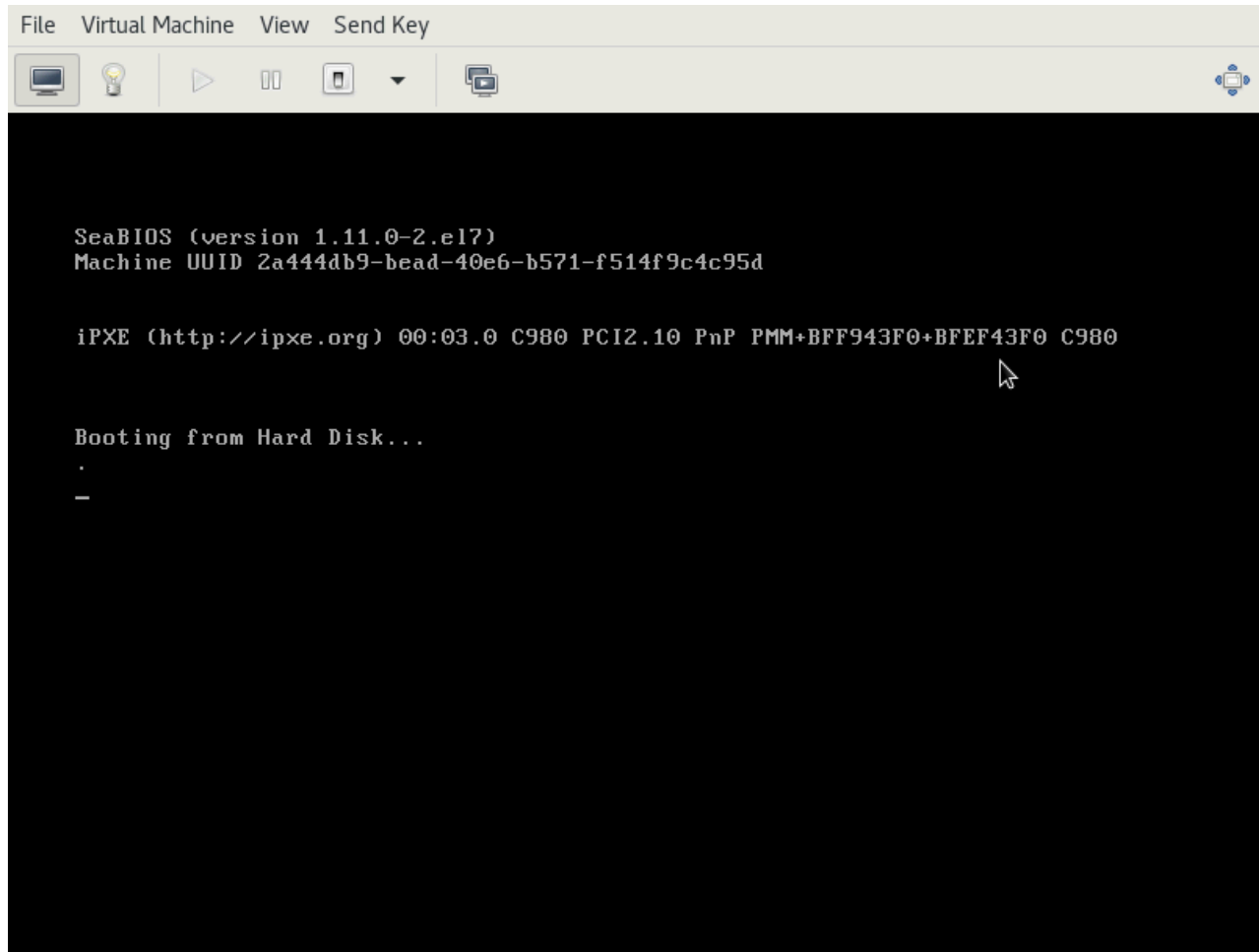
15. Add an extra three disks by clicking **Add Hardware**. Assign to them the disk image size to 100GB, 60GB, and 60GB respectively with the same Bus type of **VirtIO**. Click **Finish** to save the result.

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:

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

16. Click **Begin Installation** at the top of the dialog box to start the installation process.



17. At the end of booting, log in with the default login credentials: User: `root` and Password: `ProspectHills`.
18. You will be required to change the password. Remember this password for future use.
- At this point, you can continue configuring FortiSIEM by [using the GUI](#).

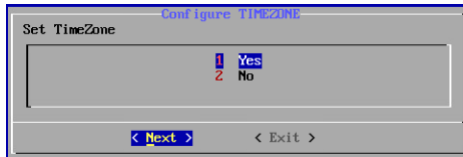
Configure FortiSIEM



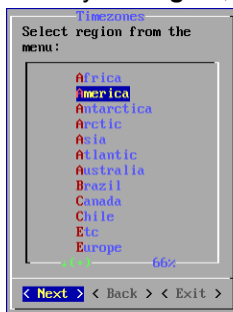
At no stage of the installation process is it required that users manually format the disks. FortiSIEM will provision the file system on disks as needed.

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

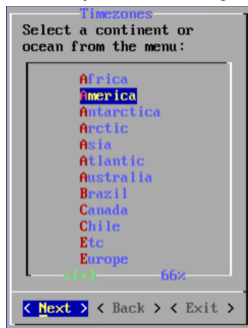
1. Log in as user `root` with the password you set in Step 18 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`configFSM.sh`
3. In VM console, select **1 Set Timezone** and then press **Next**.



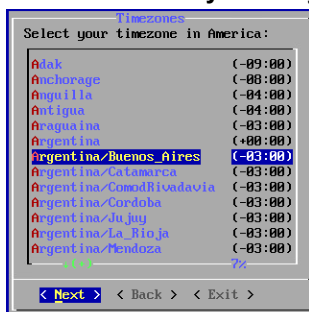
4. Select your **Region**, and press **Next**.



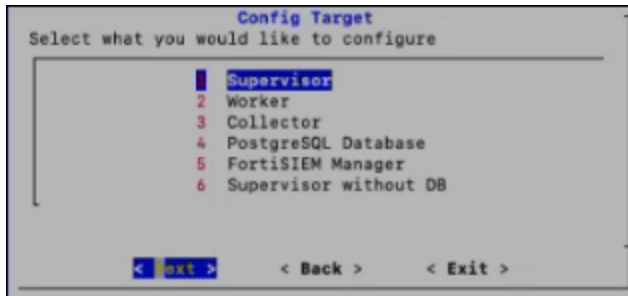
5. Select your **Country**, and press **Next**.



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



7. If installing a Supervisor, select **1 Supervisor**. 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.



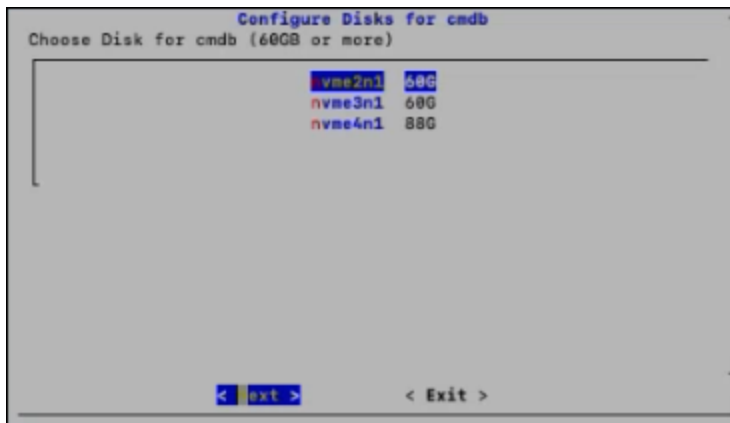
9. Select the disk for opt and press **Next**.

Note: This option only appears if **Supervisor**, **Worker** or **Collector** is selected as **Config Target**.



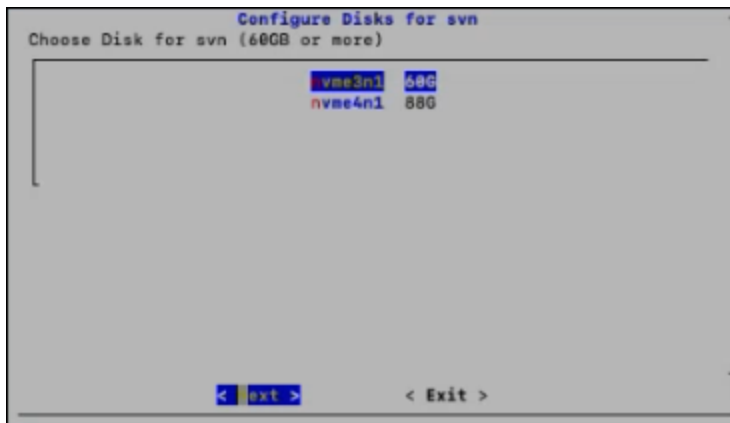
10. Select the disk for cmdb and press **Next**.

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

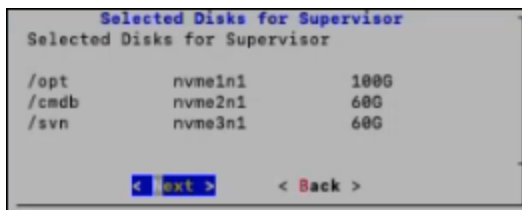


11. Confirm the disk for svn and press **Next**.

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

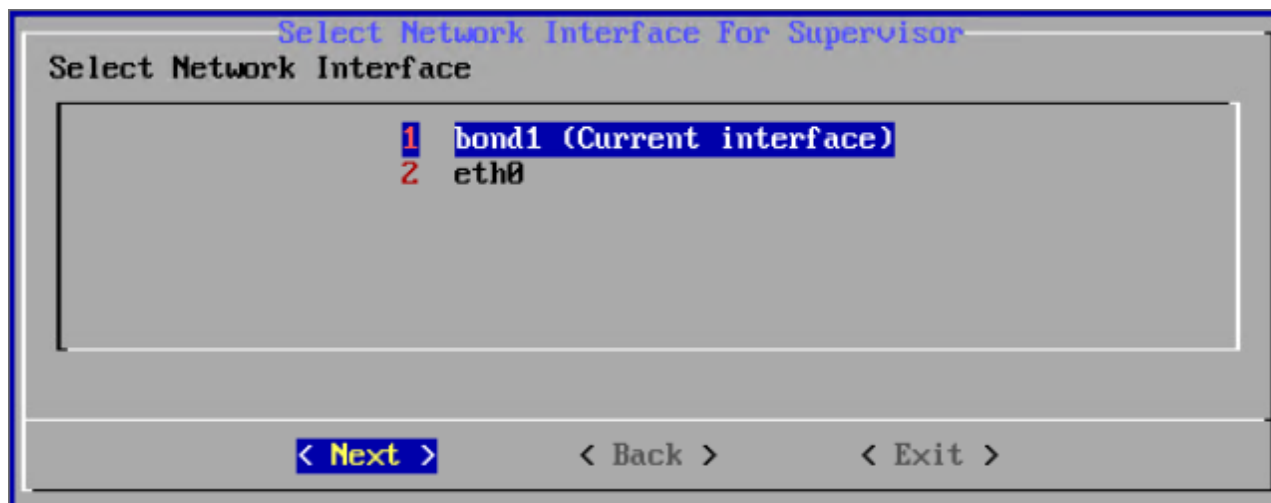


12. Confirm the selected disks (opt, cmdb, svn) for **Supervisor**, opt for **Worker** and **Collector**, and press **Next**, or press **Back** as needed to re-configure.

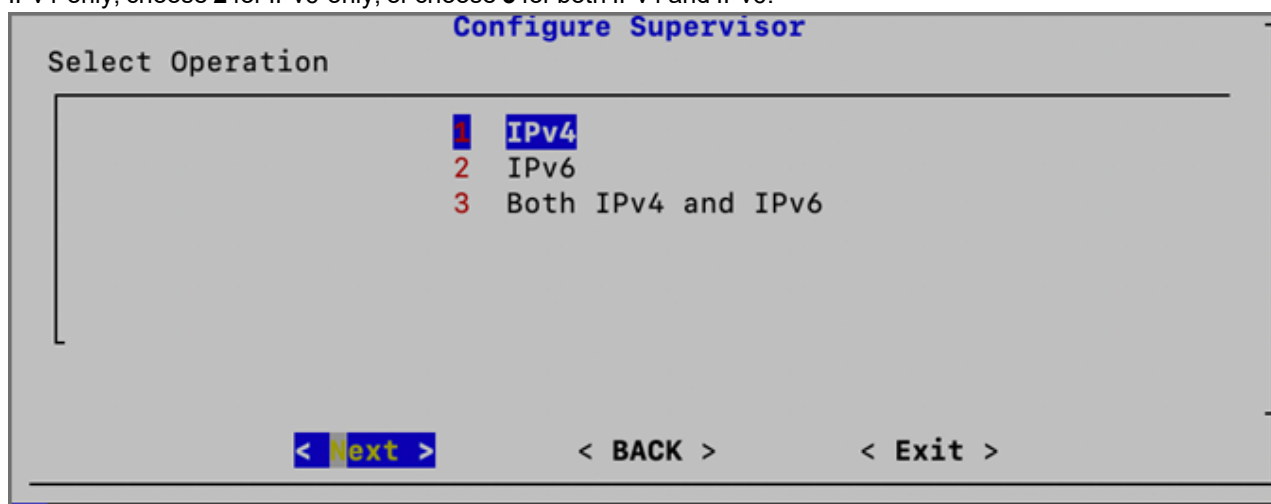


13. Select the **Network Interface** you wish to use, and press **Next**.

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

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

```

Configure IPv4 For Supervisor
Configure IPv4 Network

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

< Next >      < Back >      < Exit >

```

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

```

Configure IPv6 for Supervisor
Configure IPv6 Network

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

< Next >      < Back >      < Exit >

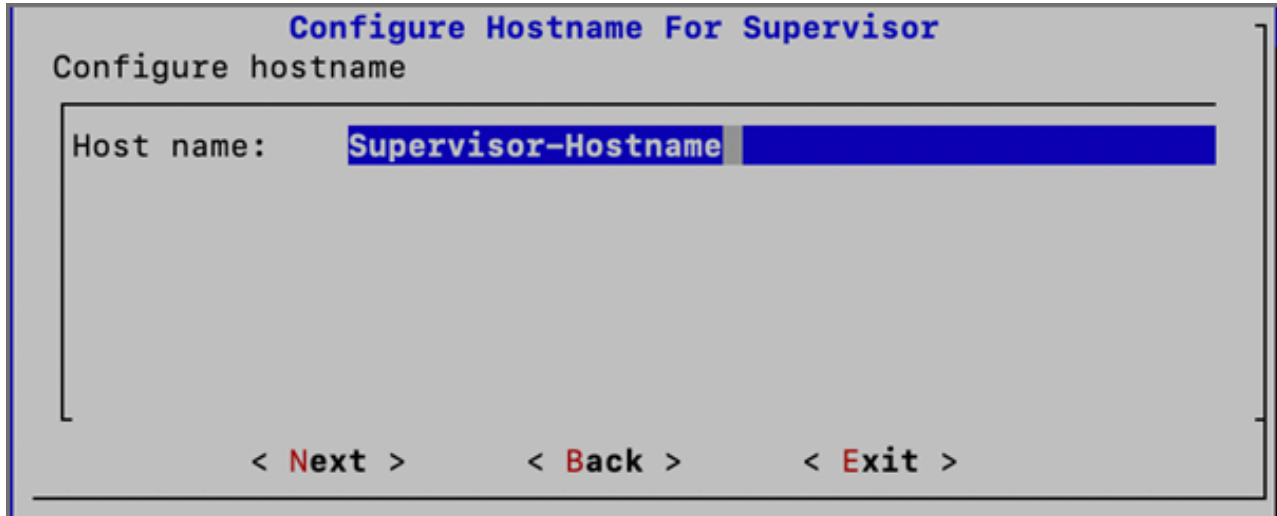
```

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



Configure Hostname For Supervisor

Configure hostname

Host name: **Supervisor-Hostname**

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

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.



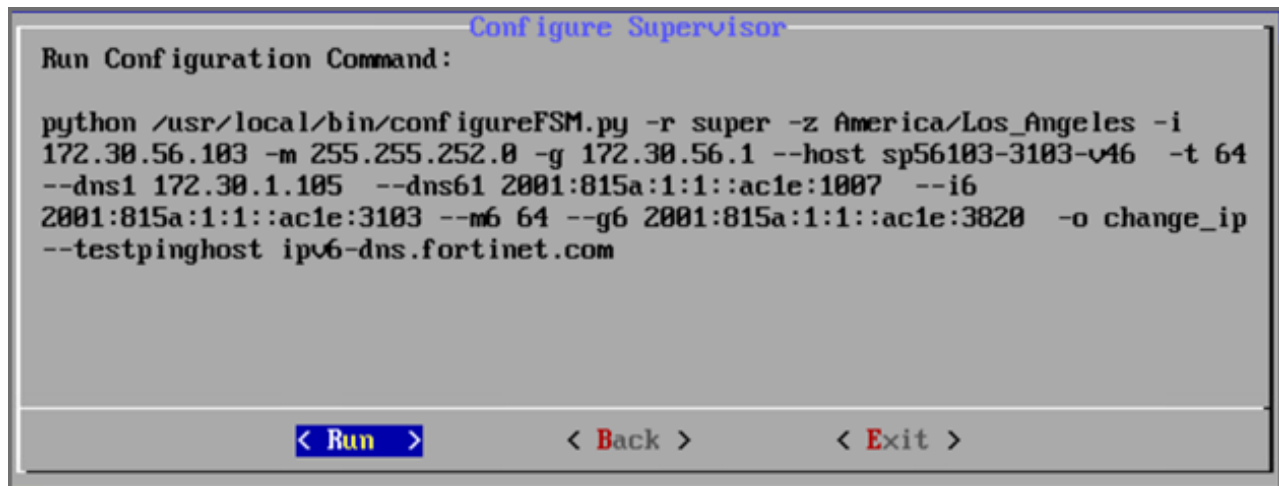
Configure Supervisor

Enter host for checking network connectivity

ipv6-dns.fortinet.com

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

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

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](#).

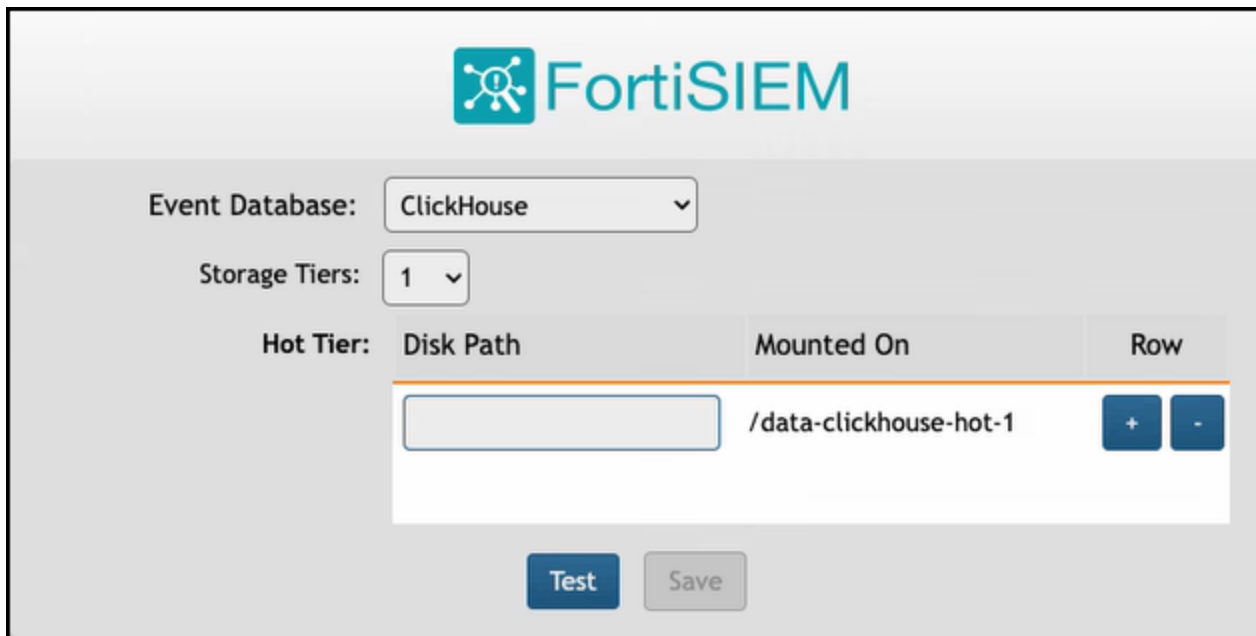
You will now be asked to input a license.

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.



The screenshot shows the FortiSIEM configuration interface. At the top is the FortiSIEM logo. Below it, the 'Event Database' is set to 'ClickHouse'. The 'Storage Tiers' are set to '1'. The 'Hot Tier' configuration table is shown below:

Hot Tier:	Disk Path	Mounted On	Row
		/data-clickhouse-hot-1	+ -

At the bottom of the form are 'Test' and 'Save' buttons.

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.


```

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%ni, 91.4%id, 0.6%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                550m
phQueryMaster           41:41                0                1820m                77m
phAlertMaster           41:41                0                1879m                504m
phAlertWorker           41:41                0                1363m                205m
phQueryWorker           41:41                0                1383m                279m
phDataManager           41:41                0                1419m                205m
phDiscover              41:41                0                513m                53m
phReportWorker          41:41                0                1433m                95m
phReportMaster          41:41                0                600m                67m
phIdentityWorker        41:41                0                1027m                50m
phIdentityMaster        41:41                0                491m                39m
phAgentManager          41:41                0                1425m                54m
phCheckpoint            42:31                0                325m                39m
phEventManager          41:41                0                702m                70m
phReportLoader          41:41                0                769m                270m
phBeaconEventPackager   41:41                0                1125m                65m
phDataPurger            41:41                0                588m                50m
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
AppSvc                  01:10:07            0                15172m               3026m
DBSvc                   01:10:30            0                317m                30m
phAnomaly               01:00:07            0                907m                64m
phFortiInsightAI        01:10:40            0                23432m               430m
Redis                   01:10:10            0                55m                25m

```

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

```

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

System uptime: 11:34:52 up 1 day, 1:39, 2 users, load average: 0.00, 0.00, 0.92
Tasks: 5 total, 0 running, 5 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 7.2%us, 0.2%sy, 0.0%ni, 92.3%id, 0.0%wa, 0.1%hi, 0.1%si, 0.0%st
Mem: 244687224k total, 6696192k used, 162125088k free, 5248k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2352072k cached

PROCESS                UPTIME                CPU%                VIRT_MEM            RES_MEM
phMonitor              20:57:20                0                1130m                64m
Apache                 1-01:20:00            0                305m                16m
Rsyslogd               1-01:38:42            0                192m                7380k
AppSvc                 1-01:38:34            5                11153m               4182m
DBSvc                  1-01:38:43            0                425m                39m

```

Cluster Installation

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

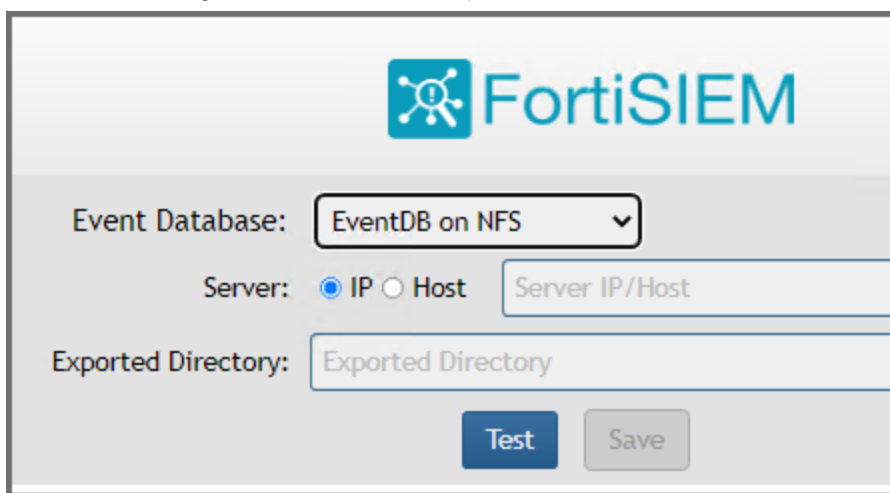
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Create ClickHouse Topology \(Optional\)](#)

- [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 KVM Step 15](#)).
 - b. You need to configure NFS after license upload.



The screenshot shows the FortiSIEM configuration interface. At the top is the FortiSIEM logo. Below it, the 'Event Database' is set to 'EventDB on NFS' in a dropdown menu. Under 'Server', the 'IP' radio button is selected, and the 'Server IP/Host' field is empty. The 'Exported Directory' field is also empty. At the bottom are 'Test' and 'Save' buttons.

3. If you choose **ClickHouse**
 - a. You need to create disks during [Import FortiSIEM into KVM 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.



Event Database: ClickHouse ▼

Storage Tiers: 2 ▼

Hot Tier:

Disk Path	Row
	+ -

Warm Tier:

Disk Path	Row
	+ -

4. If you choose **Elasticsearch**, define Elasticsearch endpoints after license upload. See the [Elasticsearch Sizing Guide](#) for details.


FortiSIEM

Event Database: Elasticsearch ▼

ES Service Type: ☒ Native ☐ Amazon ☐ Elastic Cloud

Endpoint: URL	Ingest	Query	Row
https://	☒	☒	+ -

REST Port: 443

User Name: (Optional)

Password: (Optional)

Confirm Password:

Shard Allocation: ☐ Fixed ☒ Dynamic

Shards: 5

Replicas: 1

Per Org Index ☐

Test
Save

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 KVM, the 3rd disk (hot) will be `/dev/vdc` and the 4th disk (warm) will be `/dev/vdc`.
 - d. Click **Test**.

Add Node
✕

Mode: Worker ▼

Host Name:

IP Address:

Running On: VM ▼

Storage Tiers: 2 ▼

Hot Tier:

Disk Path	Mounted On	Row
	/data-clickhouse-hot-1	+ -

Warm Tier:

Disk Path	Mounted On	Row
	/data-clickhouse-warm-1	+ -

Test
Save
Cancel

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.

FortiSIEM Admin > Health > Cloud Health

Summary: 2 Total, 0 No Connection, 0 Critical, 0 Warning, 2 Normal

Name	IP Address	Type	HA Role	DR Role	Health	Last Status Updated
AutomationServer		Supervisor With DB			Normal	Dec 11, 2024, 06:24:20 PM
AutomationWK		Worker			Normal	Dec 11, 2024, 06:24:47 PM

Copyright © 2024 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global Storage: Elasticsearch FortiSIEM

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 you need to only choose OS and OPT disks.

- [Collector in Regular IT Environments](#)
- [Collector with Reduced Disk in OT Environments](#)

Collector in Regular IT Environments

The recommended settings for Collector node are:

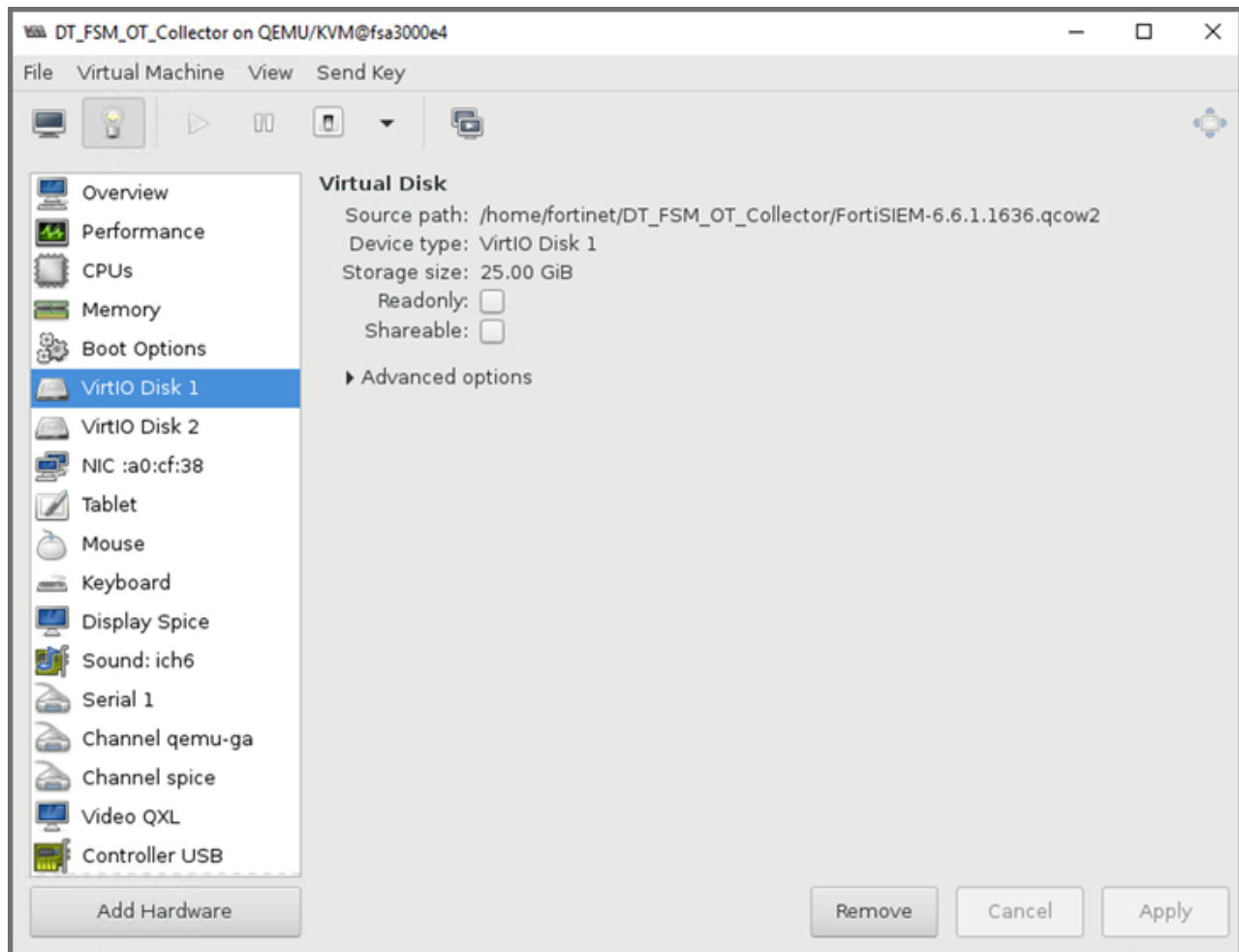
- CPU = 4
 - Memory = 8GB
 - Two hard disks:
 - OS – 25GB
 - OPT – 100GB
- For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

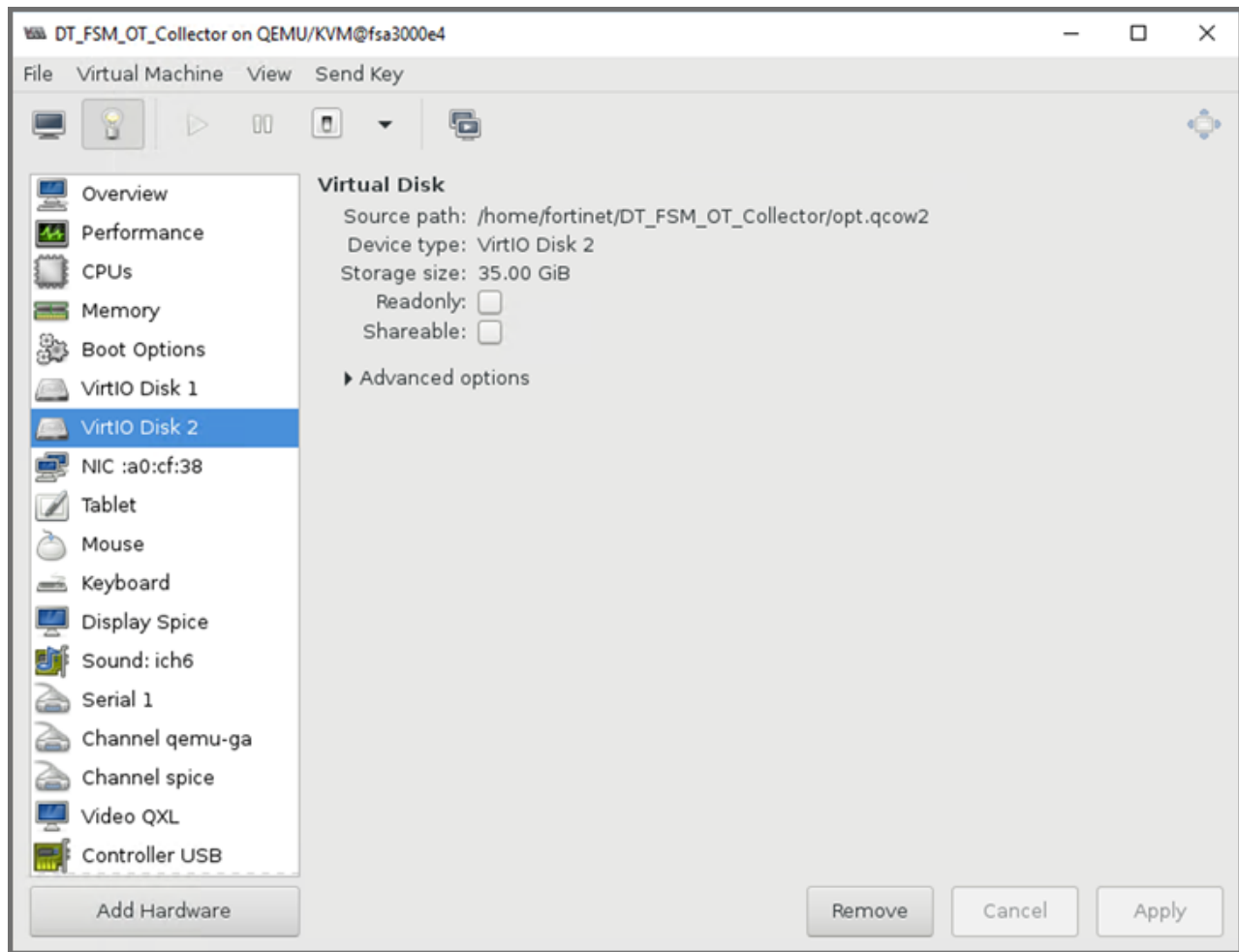
Collector with Reduced Disk in OT Environments

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).

Certain environments such as Operational Technology (OT) may find it difficult to dedicate 125 GB to a log collector. 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.

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.

```
"FSIEMKVM": {
  "SUPER": {
    "number": "3",
    "opt": "100",
    "svn": "60",
    "cddb": "60"
  },
  "FSMMANAGER": {
    "number": "2",
    "opt": "100",
    "cddb": "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:


```
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.

FortiSIEM Admin - Collector Health

Summary:

- Total: 1
- No Connection: 0
- Critical: 0
- Warning: 0
- Normal: 1

Last update at 6:19:08 PM

Organization	Collector ID	Collector Name	IP Address	Health	Last Status Updated	Last File Received	Collector Type
org1	10000	co1		Normal	Dec 11, 2024, 06:16:35 PM	Dec 11, 2024, 06:15:58 ...	VM

Copyright © 2024 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global Storage: Elasticsearch FortiSIEM

Service Provider Deployments

For Service Provider deployments, follow these steps.

- Log in to Supervisor with 'Admin' privileges.
- Go to **ADMIN > Settings > System > Cluster Config**.
 - 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.
 - Click **Save**.

FortiSIEM Admin - Cluster Config

← All Settings > System > Cluster Config

Supervisors

Address: + -

Save

Event Upload Workers

Address: + -

Save

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

Organization Definition (org2 ID: 2000) ✕

Organization: org2	Include IP/IP Range:
Full Name:	Exclude IP/IP Range:
Admin User: admin	Agent User:
Admin Password: Cannot be changed	Agent Password:
Confirm Admin Password: Cannot be changed	Confirm Agent Password:
Admin Email: admin@fortinet.com	Max Devices: 0
Phone:	Address:
Account Number:	Account Type:
Support Tier:	Account Status:
Support Team:	Account Manager:

Collectors: Lines: 1

Collector ID	Collector Name	Collector EPS	UpLoad Rate Limit	UpLoad EPS Lin
Save Cancel				

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

Organization Definition (org2 ID: 2000) - Add Collector

Name: Required

Guaranteed EPS: Required

Upload Rate Limit (Kbps): Unlimited

Upload EPS Limit: Unlimited

Start Time: ☒ Unlimited

End Time: ☒ Unlimited

Event Worker: Optional + -

< Save < Cancel

7. SSH to the Collector and run following script to register Collectors:

```
phProvisionCollector --add <user> '<password>' <Super IP or Host> <Organization>
<CollectorName>
```

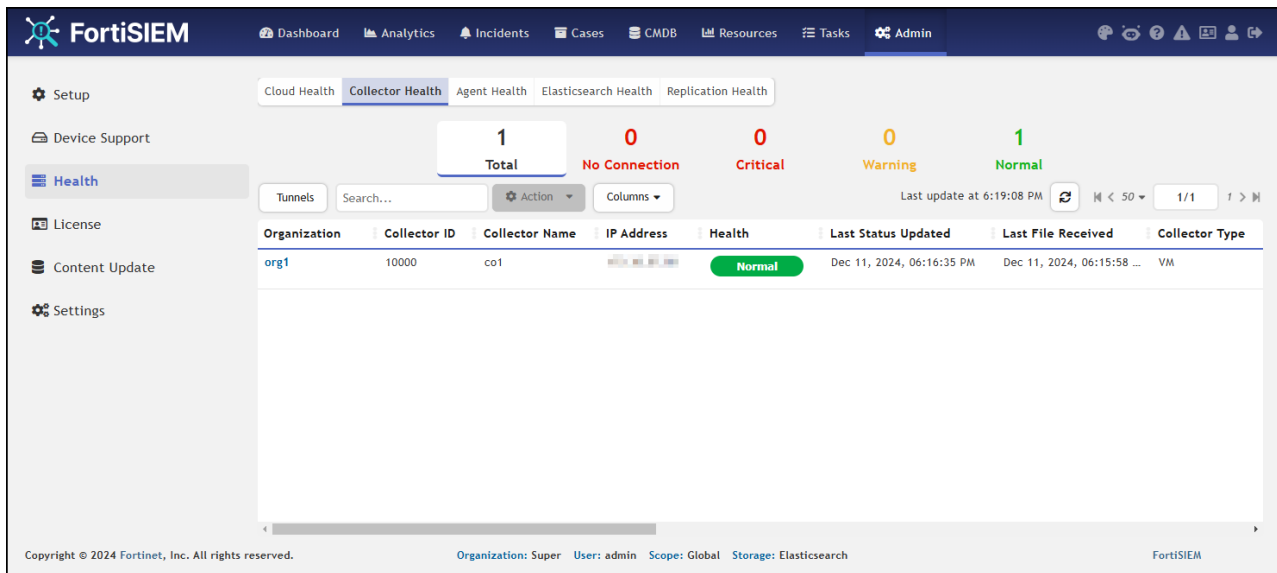
The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
- Set `Super IP or Host` as the Supervisor's IP address.
- Set `Organization` as the name of an organization created on the Supervisor.
- Set `CollectorName` from [Step 6](#).

```
root@ec574 ~# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@ec574 ~# phProvisionCollector --add admin Admin@11 172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@ec574 ~# _
```

The Collector will reboot during the Registration.

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



Install Manager

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

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

Register Instances to Manager

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

- First, [add the instance to Manager](#)
- Then [register the instance itself to Manager](#)

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

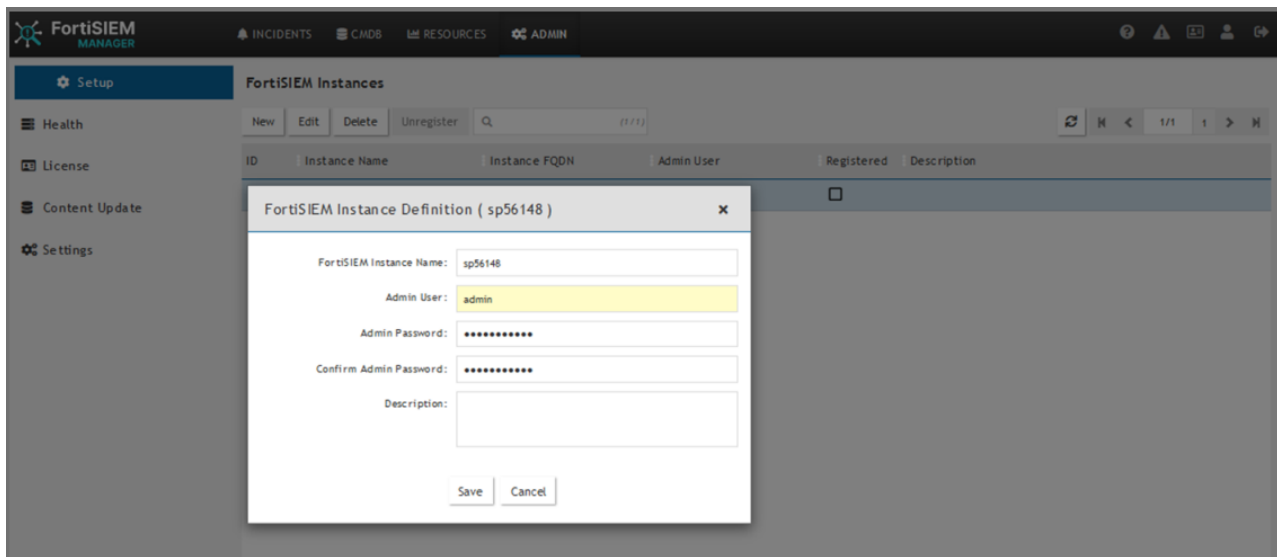
Adding Instance to Manager

You can add an instance to Manager by taking the following steps.

Note: Make sure to record the FortiSIEM Instance Name, Admin User and Admin Password, as this is needed when you register your instance.

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

6. In the **Admin Password** field, enter the Password that will be associated with the Admin User account.
7. In the **Confirm Admin Password** field, re-enter the Password.
8. (Optional) In the **Description** field, enter any information you wish to provide about the instance.
9. Click **Save**.

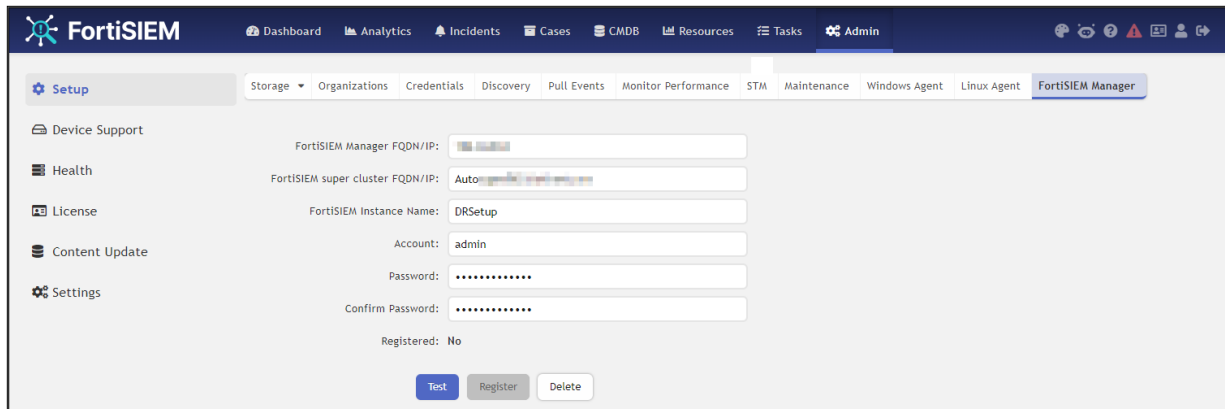


10. Repeat steps 1-9 to add any additional instances to Manager.
Now, follow the instructions in [Register the Instance Itself to Manager](#) for each instance.

Register the Instance Itself to Manager

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

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



The screenshot shows the FortiSIEM Manager registration interface. The top navigation bar includes 'Dashboard', 'Analytics', 'Incidents', 'Cases', 'CMDB', 'Resources', 'Tasks', and 'Admin'. The 'Admin' tab is active, and the 'FortiSIEM Manager' sub-tab is selected. The left sidebar contains 'Setup', 'Device Support', 'Health', 'License', 'Content Update', and 'Settings'. The main form area contains the following fields and controls:

- FortiSIEM Manager FQDN/IP: [Text input field]
- FortiSIEM super cluster FQDN/IP: Auto [Text input field]
- FortiSIEM Instance Name: DRSetup [Text input field]
- Account: admin [Text input field]
- Password: [Password input field]
- Confirm Password: [Password input field]
- Registered: No
- Buttons: Test, Register, Delete

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

Install Log

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

Errors can be found at the end of the file.



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.