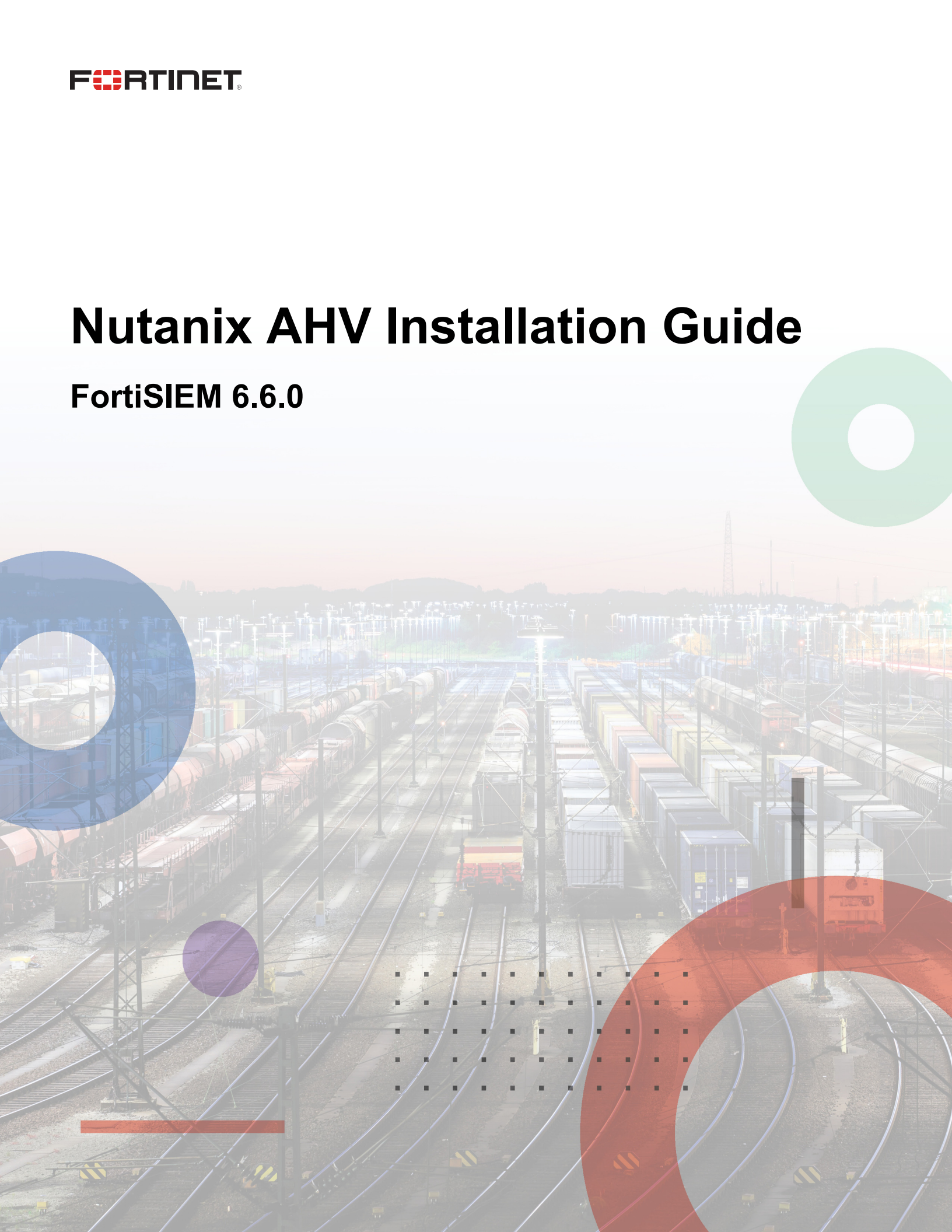


# Nutanix AHV Installation Guide

**FortiSIEM 6.6.0**



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



10/03/2023

FortiSIEM 6.6.0 Nutanix AHV Installation Guide

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Fresh Installation</b>	<b>5</b>
Pre-Installation Checklist	5
All-in-one Installation	6
Import FortiSIEM into Nutanix AHV Prism Console	6
Configure FortiSIEM via GUI	18
Upload the FortiSIEM License	24
Choose an Event Database	25
Cluster Installation	26
Install Supervisor	27
Install Workers	29
Register Workers	30
Install Collectors	31
Register Collectors	31
Install Manager	34
Register Instances to Manager	34
<b>Install Log</b>	<b>37</b>

# Change Log

Date	Change Description
04/08/2019	Initial version of FortiSIEM Nutanix AHV Installation Guide.
11/20/2019	Release of FortiSIEM Nutanix AHV Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM Nutanix AHV Installation Guide for 5.3.0.
03/17/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.1.x
03/19/2021	Revision 1: Added Migration section.
03/25/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.2.0.
04/22/2021	Revision 2: Added Install Log section.
05/07/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.2.1.
06/07/2021	Updated Elasticsearch screenshot for 6.2.x guides.
07/06/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.3.0.
08/26/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.3.1.
10/15/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.3.2.
11/17/2021	Updated Register Collectors instructions for 6.x guides.
12/22/2021	Release of FortiSIEM Nutanix AHV Installation Guide for 6.3.3.
01/18/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.4.0.
05/09/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.5.0.
07/26/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.6.0.
08/18/2022	Updated All-in-one Installation section.
09/12/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.5.1.
09/14/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.6.1.
09/19/2022	Release of FortiSIEM Nutanix AHV Installation Guide for 6.6.2.
10/20/2022	Updated Register Collectors instructions for 6.x guides.
01/03/2023	Release of FortiSIEM Nutanix AHV Installation Guide for 6.6.3.
08/31/2023	Release of FortiSIEM Nutanix AHV Installation Guide for 6.6.4.

# 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.
- Deployment type for Supervisor, Worker, and Collector – Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
  - All-in-one with FortiSIEM Manager  
**Note:** FortiSIEM Manager installation has slight differences from the Supervisor/Worker/Collector installation.
  - Cluster with Manager, Supervisor and Workers
  - Cluster with Manager, Supervisor and Workers
  - All-in-one with Supervisor only, or
  - Cluster with Supervisor and Workers
- Storage type for Supervisor, Worker, and/or Collector
  - Online – Local or NFS or ClickHouse or Elasticsearch
  - Archive – NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage, excluding FortiSIEM Manager.
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum <ul style="list-style-type: none"><li>• 24GB</li></ul> Recommended <ul style="list-style-type: none"><li>• 32GB</li></ul>	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none"><li>• without UEBA – 24GB</li><li>• with UEBA - 32GB</li></ul> Recommended <ul style="list-style-type: none"><li>• without UEBA – 32GB</li><li>• with UEBA - 64GB</li></ul>	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need

Node	vCPU	RAM	Local Disks
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none"> <li>without UEBA – 24GB</li> <li>with UEBA - 32GB</li> </ul> Recommended <ul style="list-style-type: none"> <li>without UEBA – 32GB</li> <li>with UEBA - 64GB</li> </ul>	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

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

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

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

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

## All-in-one Installation

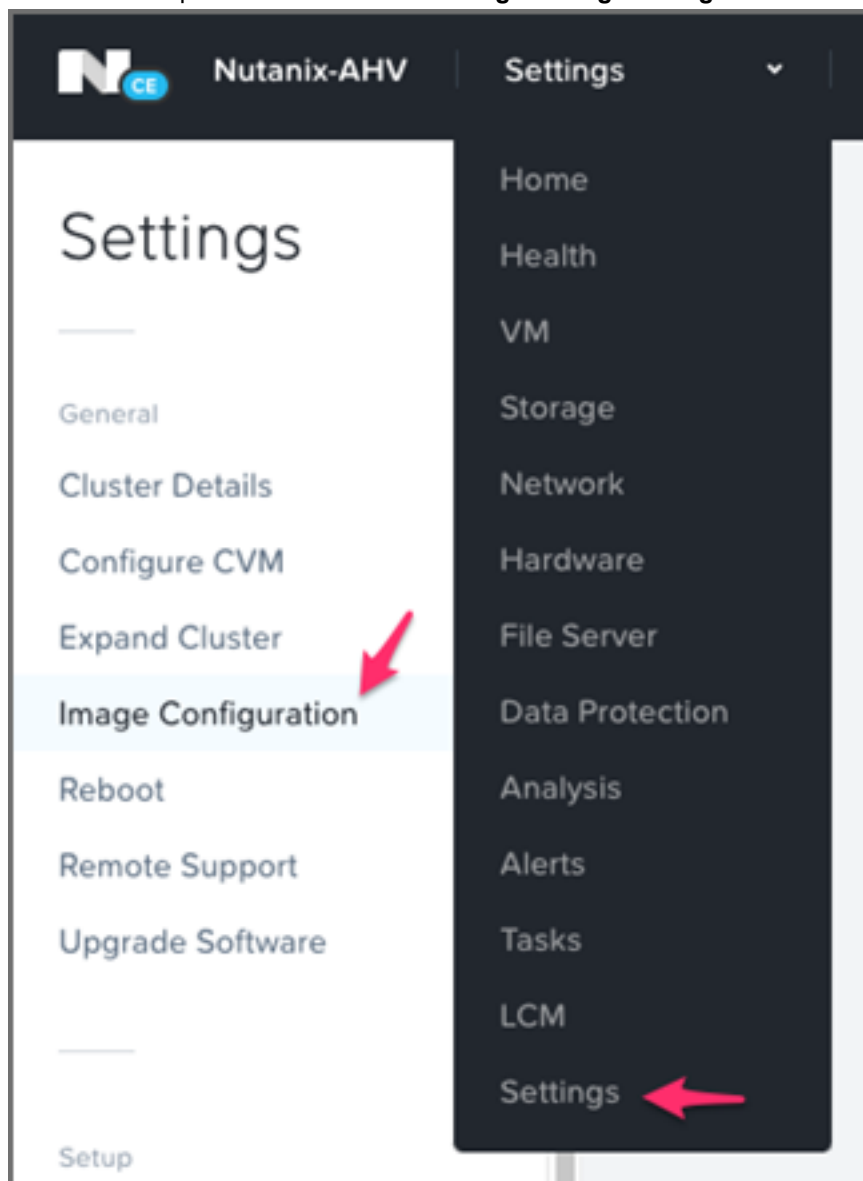
This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- [Import FortiSIEM into Nutanix AHV Prism Console](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

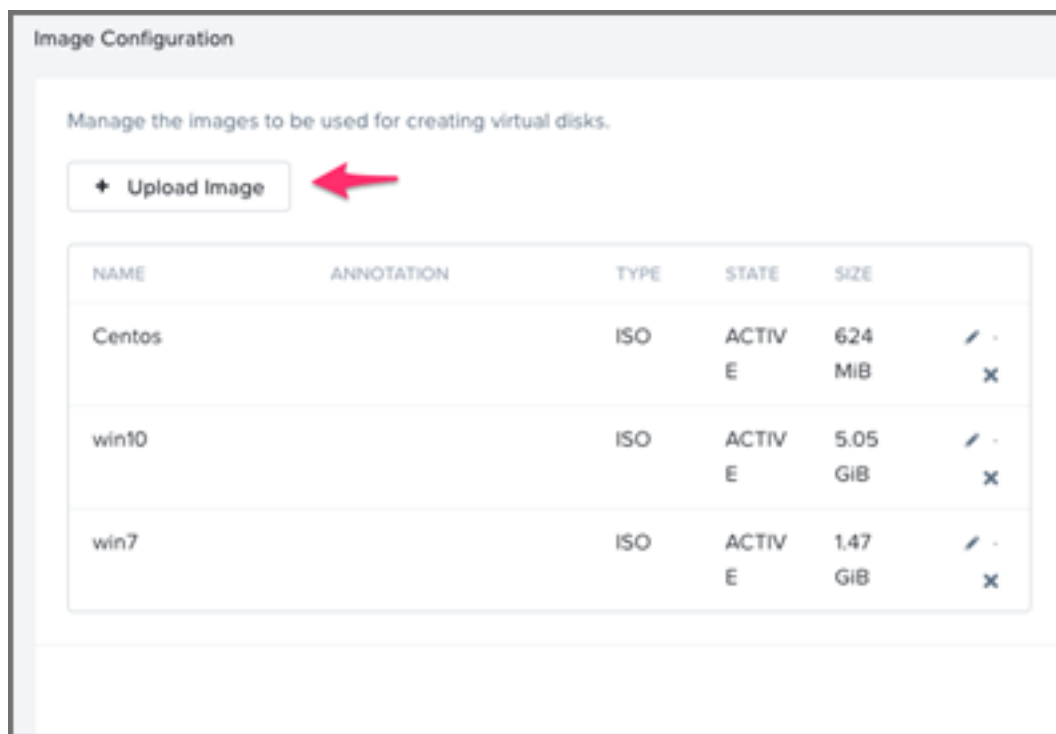
## Import FortiSIEM into Nutanix AHV Prism Console

1. Go to the Fortinet Support website <https://support.fortinet.com> to download the KVM package `FSM_Full_All_KVM_6.6.0_build1633.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_6.6.0_build1633.zip`.
3. Unzip the `.zip` file to get the `FortiSIEM-6.6.0.1633.qcow2` file.
4. Login to the Nutanix AHV Prism Console.

5. Click on the drop-down list and select **Settings > Image Configuration**.



6. Click **Upload Image** from the **Image Configuration** page.



7. Select Upload a file, click on Choose File, and browse to the `FortiSIEM-6.6.0.1633.qcow2` file.
- From the **Storage Container** drop-down list, select a storage container.
  - From the **Image Type** drop-down list, select **DISK**.
  - In the **Name** field, provide the name of the image.
  - Click **Save**.

- e. Wait for the image upload to complete before proceeding to the next step.

**Create Image**

Name: FortiSIEM-6.1.1.0118 c

Annotation:

Image Type: DISK b

Storage Container: default-container-43082970730805 a

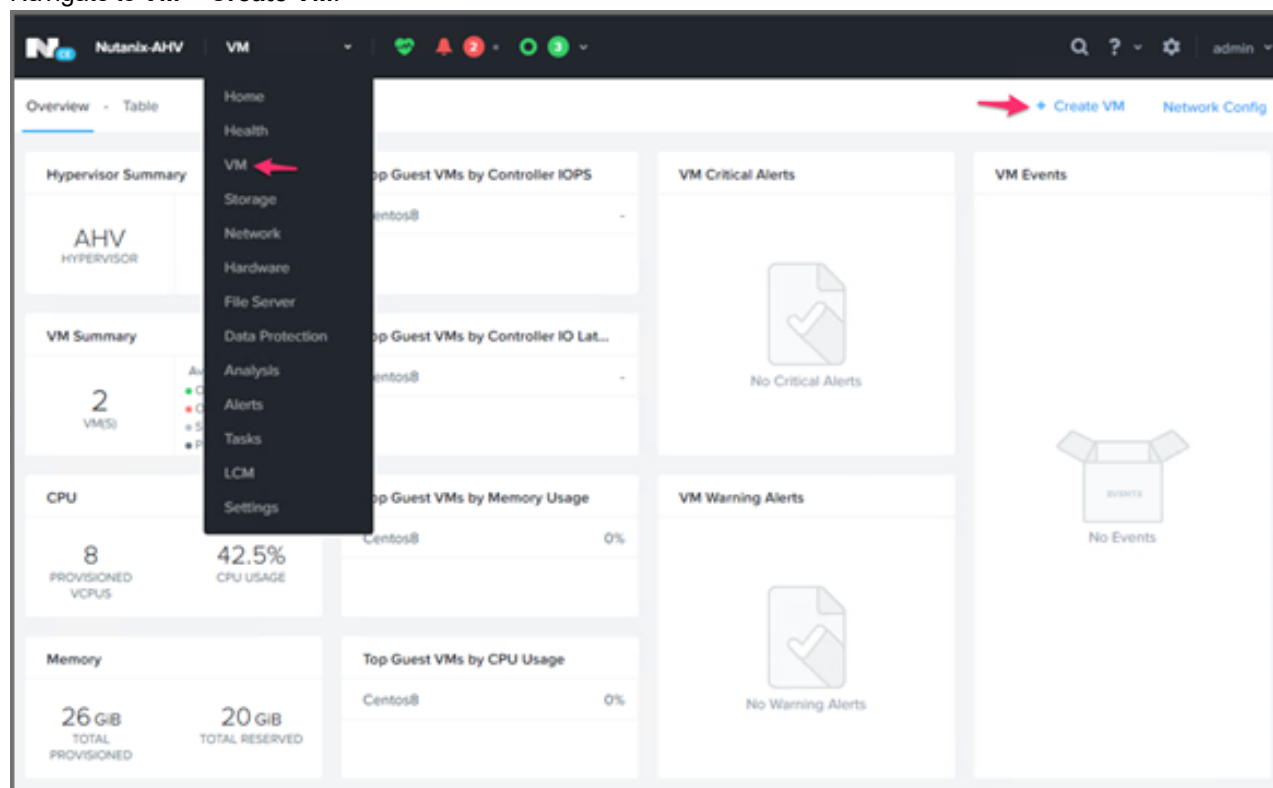
Image Source:

☐ From URL

☒ Upload a file 7 Choose File FortiSIEM-6.1.1.0118.qcow2

Back Cancel Save d

8. Navigate to **VM > Create VM**.



**Create VM** ? X

Name  
fsm-super-611

Description  
Optional

Timezone  
(UTC) UTC Cluster ▾

☐ Use this VM as an agent VM

---

**Compute Details**

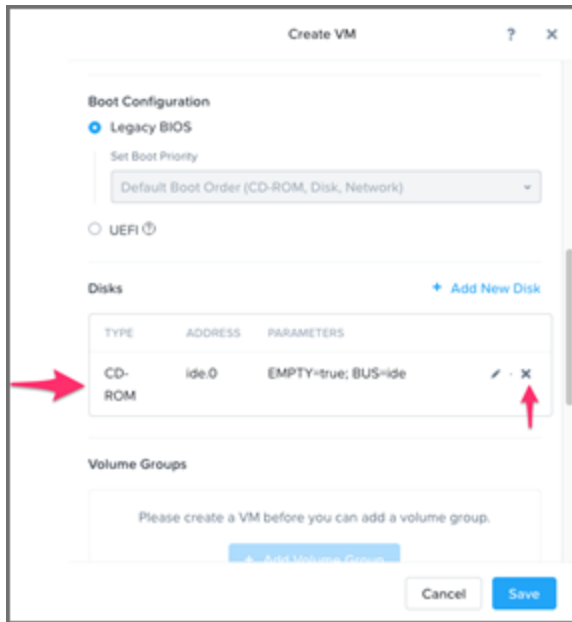
vCPU(s)  
8

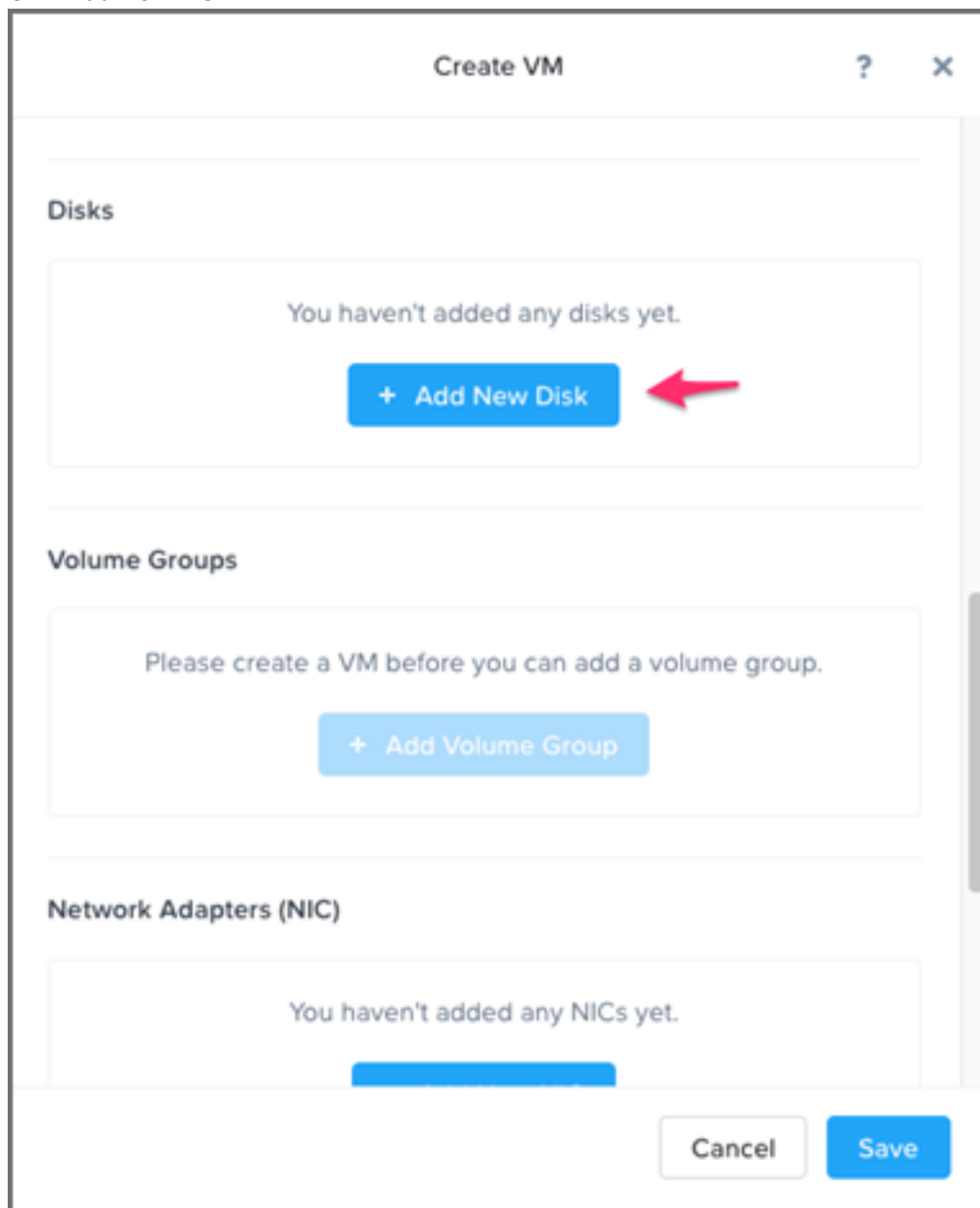
Number Of Cores Per vCPU  
1

Memory ⓘ  
32 GiB

Cancel Save

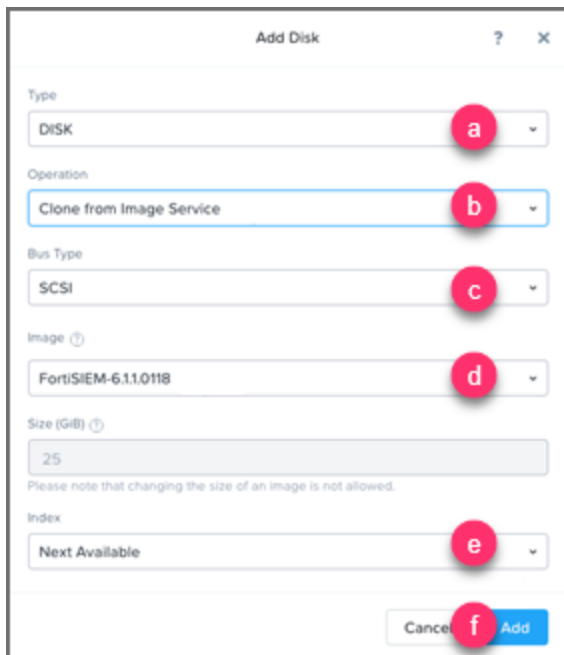
9. Scroll down in the Create VM window, continue to select Legacy BIOS, and at CD-ROM, click "X" to remove.



**10. Click Add New Disk.****11. In the Add Disk dialog, take the following steps:**

- a. From the **Type** drop-down list, select **DISK**.
- b. From the **Operation** drop-down list, select **Clone from Image Service**.
- c. From the **Bus Type** drop-down list, select **SCSI**.
- d. From the **Image** drop-down list, select the FortiSIEM image you created earlier (FortiSIEM-6.6.0.1633).
- e. From the **Index** drop-down list, select **Next Available**.

f. Click **Add**.



The screenshot shows the 'Add Disk' dialog box with the following fields and annotations:

- Type:** A dropdown menu with 'DISK' selected. A red circle with the letter 'a' is next to it.
- Operation:** A dropdown menu with 'Clone from Image Service' selected. A red circle with the letter 'b' is next to it.
- Bus Type:** A dropdown menu with 'SCSI' selected. A red circle with the letter 'c' is next to it.
- Image:** A dropdown menu with 'FortiSIEM-6.11.0118' selected. A red circle with the letter 'd' is next to it.
- Size (GiB):** A text input field with '25' entered. A red circle with the letter 'e' is next to it.
- Index:** A dropdown menu with 'Next Available' selected. A red circle with the letter 'e' is next to it.
- Buttons:** At the bottom right, there are 'Cancel' and 'Add' buttons. A red circle with the letter 'f' is next to the 'Add' button.

You will now see the OS disk 25GiB in the list of disks shown.

**Create VM**

**Boot Configuration**

☒ Legacy BIOS

Set Boot Priority

Default Boot Order (CD-ROM, Disk, Network) ▼

☐ UEFI ?

**Disks** [+ Add New Disk](#)

TYPE	ADDRESS	PARAMETERS	
DISK	scsi.0	SIZE=25GiB; BUS=scsi	

**Volume Groups**

Please create a VM before you can add a volume group.

[+ Add Volume Group](#)

[Cancel](#) [Save](#)

12. For the Supervisor, you will need to add the 100GB /opt disk. Click **Add New Disk**, and take the following steps:
- From the **Operation** drop-down list, select **Allocate on Storage Container**.
  - In the **Size (GiB)** field, enter "100".

- c. Click **Add**.

13. Similar to the previous step, add an extra two disks by taking the following steps **twice**:
- Click **Add New Disk** for each new disk.
  - In the **Size** field, enter "60".
  - From the **Operation** drop-down list, select **Allocate on Storage Container**.
  - Click **Add**.

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

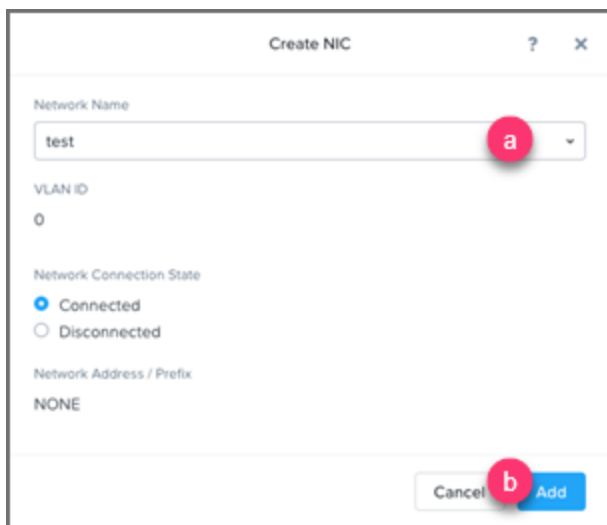
**Note on Hard Disk 5:**

- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.

- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the [FortiSIEM Sizing Guide](#) for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.

14. Click on **Add New NIC**, and take the following steps:

- a. From the **Network Name** drop-down list, select the correct network.
- b. Click **Add**.
- c. Click **Save**.

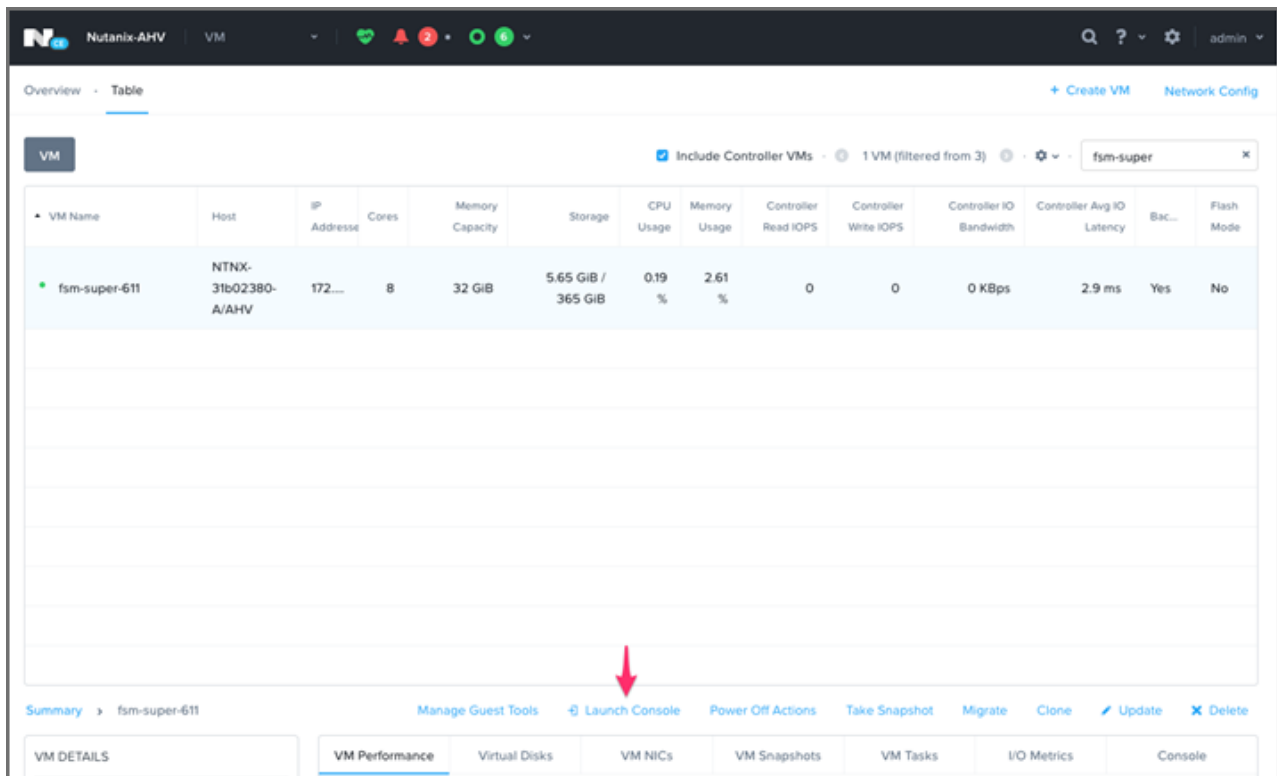


15. Navigate to **VM > Table** to find your newly created fsm-super-6## VM, then click **Power On**.

The screenshot shows the Nutanix AHV VM console interface. At the top, the 'Table' tab is selected, indicated by a red arrow. Below the tab, a search filter 'fsm-super' is applied, also indicated by a red arrow. The table lists VMs with columns for Name, Host, IP Address, Cores, Memory Capacity, Storage, CPU Usage, Memory Usage, Controller Read IOPS, Controller Write IOPS, Controller IO Bandwidth, Controller Avg IO Latency, Backing Store, and Flash Mode. The VM 'fsm-super-611' is highlighted, with a red arrow pointing to its name. Below the table, the 'Summary' section for 'fsm-super-611' is visible. In the 'VM DETAILS' section, the Name is 'fsm-super-611' and the ID is 'c173e331-6b81-481a-a8a5-4ff52ca6dba5'. In the 'VM Performance' section, there are graphs for CPU Usage and Memory Usage, both showing 0% usage. A red arrow points to the 'Launch Console' button in the 'Manage Guest Tools' section.

VM Name	Host	IP Address	Cores	Memory Capacity	Storage	CPU Usage	Memory Usage	Controller Read IOPS	Controller Write IOPS	Controller IO Bandwidth	Controller Avg IO Latency	Back...	Flash Mode
fsm-super-611			8	32 GiB	5.62 GiB / 365 GiB	0%	0%	-	-	-	-	Yes	No

16. Click on **Launch Console** to open the console.



17. After the VM has booted up to the login prompt, log in with the default login credentials:

User: root

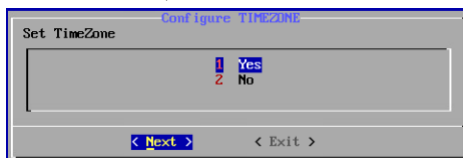
Password: ProspectHills

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](#).

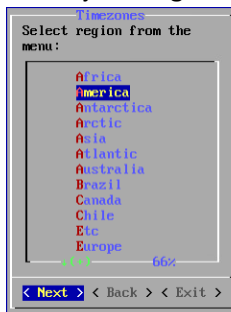
## Configure FortiSIEM via GUI

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

1. Log in as user `root` with the password you set in **Import FortiSIEM into Nutanix AHV Prism Console** Step 17 above.
2. At the command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:  
`# configFSM.sh`
3. In VM console, select **1 Set Timezone** and then press **Next**.



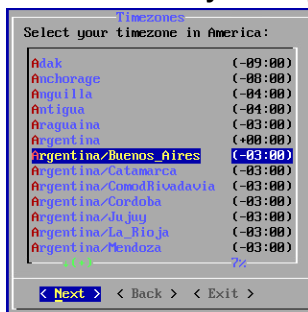
4. Select your **Region**, and press **Next**.



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



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



7. If installing a Supervisor, select **1 Supervisor**, and press **Next**.

If installing a Worker, select **2 Worker**, and press **Next**.

If installing a Collector, select **3 Collector**, and press **Next**.

If installing FortiSIEM Manager, select **4 FortiSIEM Manager**, and press **Next**.

**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**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

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

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



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

The screenshot shows a terminal window titled "Configure Supervisor". Inside, there's a section "Select Operation" with three numbered options: 1 IPv4, 2 IPv6, and 3 Both IPv4 and IPv6. At the bottom, there are three navigation buttons: "< Next >", "< BACK >", and "< Exit >". The "Next" button is highlighted with a blue cursor.

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

Option	Description
IPv4 Address	The 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

The screenshot shows a terminal window titled "Configure IPv4 For Supervisor". Inside, there's a section "Configure IPv4 Network" with five fields: IPv4 Address, Netmask, Gateway, DNS1, and DNS2. Each field has a value entered: 172.30.56.103, 255.255.252.0, 172.30.56.1, 172.30.1.105, and an empty field for DNS2. At the bottom, there are three navigation buttons: "< Next >", "< Back >", and "< Exit >". The "Next" button is highlighted with a blue cursor.

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

Option	Description
IPv6 Address	The 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 9 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration.

**Note:** In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

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

**Configure Hostname For Supervisor**

Configure hostname

Host name: Supervisor-Hostname

< Next >      < Back >      < Exit >

**Note:** FQDN is no longer needed.

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

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

The options are described in the following table.

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

Option	Description
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either <b>4</b> (for <b>ipv4</b> ) or <b>6</b> (for <b>v6</b> ) or <b>64</b> (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 ( <b>install_without_fips</b> , <b>install_with_fips</b> , <b>enable_fips</b> , <b>disable_fips</b> , <b>change_network_config*</b> ) *Option only available after installation.
-Z	Time zone. Possible values are <b>US/Pacific</b> , <b>Asia/Shanghai</b> , <b>Europe/London</b> , or <b>Africa/Tunis</b>
--testpinghost	The URL used to test connectivity

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

## Upload the FortiSIEM License



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

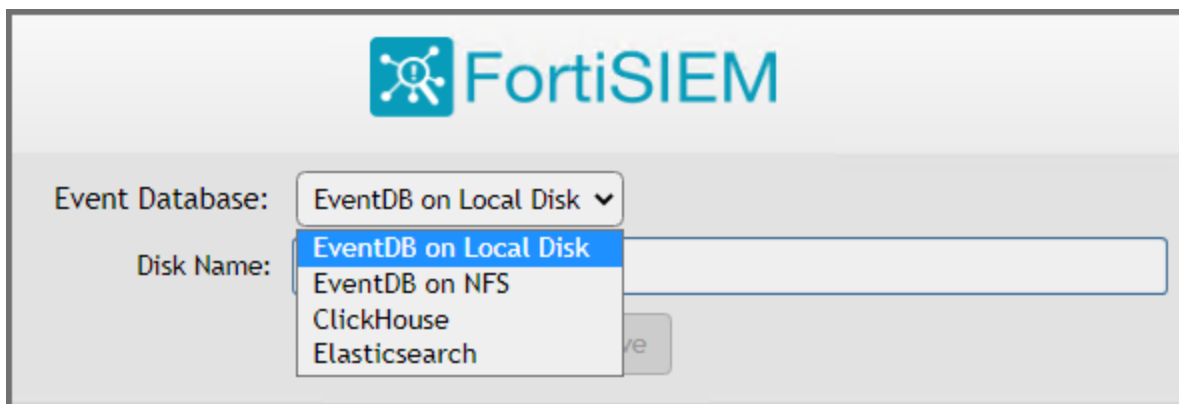
You will now be asked to input a license.

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

3. Click **Browse** and upload the license file.  
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
4. For **User ID** and **Password**, choose any **Full Admin** credentials.  
For the first time installation, enter `admin` as the user and `admin*1` as the password. You will then be asked to create a new password for GUI access.
5. Choose **License type** as **Enterprise** or **Service Provider**.  
This option is available only for a first time installation. Once the database is configured, this option will not be available.  
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 **Choose an Event Database**.  
**Note:** The FortiSIEM Manager license allows a certain number of instances that can be registered to FortiSIEM Manager.
6. Proceed to [Choose an Event Database](#).

## Choose an Event Database

For a fresh installation, you will be taken to the Event Database Storage page. From the **Event Database** drop-down list, choose **EventDB on Local Disk**, **EventDB on NFS**, **ClickHouse**, or **Elasticsearch**. For more details, see [Configuring Storage](#).



The screenshot shows the FortiSIEM web interface for configuring the Event Database. At the top is the FortiSIEM logo. Below it, there is a section titled 'Event Database:' with a dropdown menu currently showing 'EventDB on Local Disk'. Underneath, there is a 'Disk Name:' label followed by a text input field. A dropdown menu is open below the input field, listing four options: 'EventDB on Local Disk' (highlighted in blue), 'EventDB on NFS', 'ClickHouse', and 'Elasticsearch'. To the right of the input field, there is a 'Save' button.

After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

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

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

```
# phstatus
```

For the Supervisor, 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                  603m                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: 24468724k total, 6696192k used, 16212508k 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](#)
- [Install Collectors](#)

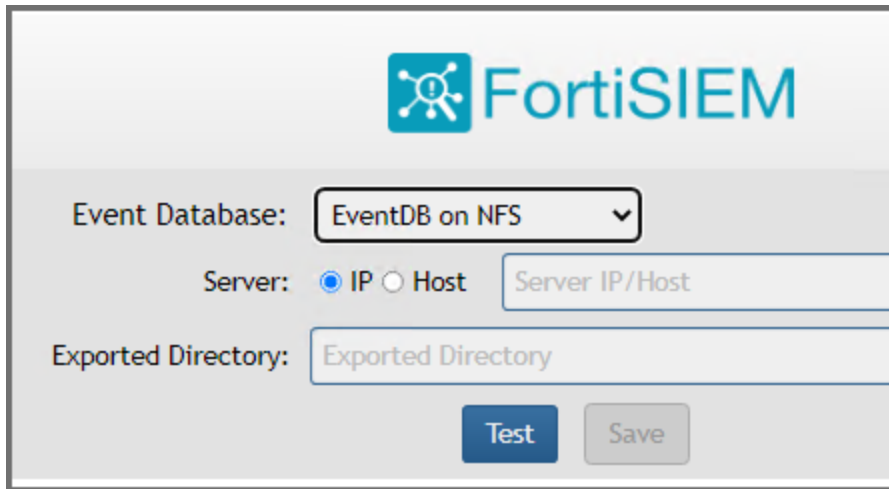
- [Register Collectors](#)
- [Install Manager](#)
- [Register Instances to Manager](#)

## Install Supervisor

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


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

### NFS



The image shows a web-based configuration interface for FortiSIEM. At the top, there is a logo consisting of a blue square with a white network icon and the text "FortiSIEM" in blue. Below the logo, the "Event Database:" label is followed by a dropdown menu currently showing "EventDB on NFS". Underneath, the "Server:" label is followed by two radio buttons: "IP" (which is selected) and "Host". To the right of these radio buttons is a text input field containing the placeholder text "Server IP/Host". Below this, the "Exported Directory:" label is followed by a text input field containing the placeholder text "Exported Directory". At the bottom right of the form, there are two buttons: a blue "Test" button and a grey "Save" button.

### ClickHouse



Event Database:

ClickHouse

Storage Tiers:

2

Hot Tier:

Disk Path

Row

+

-

Warm Tier:

Disk Path

Row


+

-

Test

Save

Elasticsearch



Event Database: Elasticsearch

ES Service Type: ☒ Native ☐ Amazon ☐ Elastic Cloud

Endpoint:	URL	Ingest	Query	Row
<input type="text" value="https://"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="button" value="+"/>	<input type="button" value="-"/>

REST Port:

User Name:

Password:

Confirm Password:

Shard Allocation: ☐ Fixed ☒ Dynamic

Shards:

Replicas:

Per Org Index ☐

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

## Install Workers

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

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

- OPT – 100GB

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

## Register Workers

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

1. Go to **ADMIN > License > Nodes**.
2. Select **Worker** from the drop-down list and enter the Worker's IP address and host name. Click **Add**.

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

Setup

Device Support

Health

License

Settings

Cloud Health

Collector Health

Search...

Columns

Lines: 2

Last update at 8:49:17 PM

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

Search...

Columns

Process level metrics for wk573.fortinet.com (172.30.57.3)

Lines: 17

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

Copyright © 2020 Fortinet, Inc. All rights reserved.

Organization: Super

User: admin

Scope: Global

FortiSIEM

## Install Collectors

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

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

## Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

- [Enterprise Deployments](#)
- [Service Provider Deployments](#)

### Enterprise Deployments

For Enterprise deployments, follow these steps.

1. Log in to Supervisor with 'Admin' privileges.
2. Go to **ADMIN > Settings > System > Event Worker**.
  - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.  
**Note:** Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.
  - b. Click **OK**.
3. Go to **ADMIN > Setup > Collectors** and add a Collector by entering:
  - a. **Name** – Collector Name
  - b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
  - c. **Start Time** and **End Time** – set to **Unlimited**.
4. SSH to the Collector and run following script to register Collectors:

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

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

  - a. Set `user` and `password` using the admin user name and password for the Supervisor.
  - b. Set `Super IP or Host` as the Supervisor's IP address.
  - c. Set `Organization`. For Enterprise deployments, the default name is Super.

- d. Set `CollectorName` from [Step 2a](#).

The Collector will reboot during the Registration.

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

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

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

## Service Provider Deployments

For Service Provider deployments, follow these steps.

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

← All Settings > System > Event Worker

Worker Address: 172.30.57.3 + -

Save

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

4. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.

5. Under **Collectors**, click **New**.

6. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**.

The last two values could be set as **Unlimited**. **Guaranteed EPS** is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

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

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

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

- 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@cc574 ~]# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
[root@cc574 ~]# phProvisionCollector --add admin Admin=11.172.38.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
[root@cc574 ~]# _
```

The Collector will reboot during the Registration.

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

The screenshot shows the 'Collector Health' page in the FortiSIEM interface. It includes a sidebar with navigation options like Setup, Device Support, Health, License, and Settings. The main content area has tabs for Cloud Health and Collector Health. Below the tabs, there's a table showing collector information and a detailed process list.

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

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

## 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).

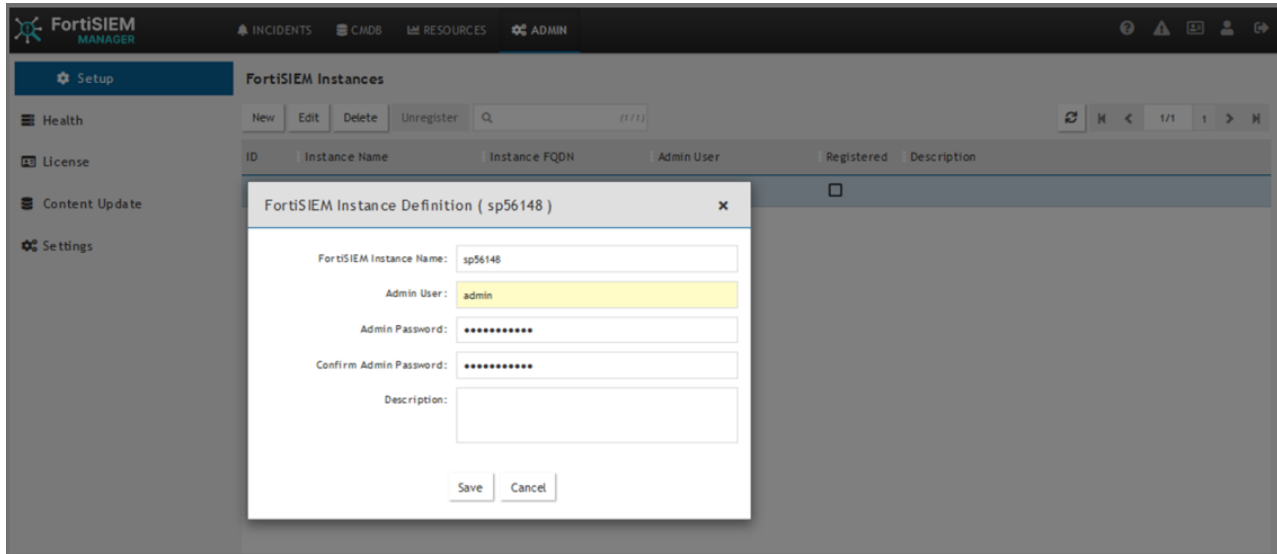
## Adding Instance to Manager

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. In the **FortiSIEM Instance Name** field, enter the instance name used when adding the instance to Manager.
  - c. In the **Account** field, enter the Admin User name used when adding the instance to Manager.
  - d. In the **Password** field, enter your password to be associated with the Admin User name.
  - e. In the **Confirm Password** field, re-enter your password.
  - f. Click **Test** to verify the configuration.
  - g. Click **Register**.  
A dialog box displaying "Registered successfully" should appear if everything is valid.

The screenshot shows the FortiSIEM Setup page under the ADMIN tab. The left sidebar contains links for Device Support, Health, License, Content Update, and Settings. The main content area has a 'Setup' sub-tab selected. It contains the following fields:

- FortiSIEM Manager FQDN/IP: [Empty field]
- FortiSIEM Instance FQDN/IP: [Empty field with '.com' placeholder]
- FortiSIEM Instance Name: DRSetup
- Account: admin
- Password: [Masked with dots]
- Confirm Password: [Masked with dots]
- Registered: No

At the bottom, there are three buttons: Test, Register, and Delete.

- h. 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](http://www.fortinet.com)

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