

Azure Installation Guide

FortiSIEM 6.3.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



10/04/2023

FortiSIEM 6.3.1 Azure Installation Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Find the FortiSIEM Offer in Azure Using the Azure Marketplace	7
Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image	8
Configure FortiSIEM	19
Upload the FortiSIEM License	25
Configure an Event Database	25
Final Check	26
Cluster Installation	27
Install Supervisor	27
Install Workers	28
Register Workers	29
Create ClickHouse Topology (Optional)	30
Install Collectors	30
Register Collectors	30
Install Log	34

Change Log

Date	Change Description
10/06/2020	Initial release of Azure Installation and Migration Guide.
11/03/2020	Revision 1: Release of Azure Installation and Migration Guide for 6.1.1.
12/07/2020	Revision 2: Small addition to Register Collectors.
02/05/2021	Revision 3: Migration update.
03/23/2021	Revision 4: Release of Azure Installation Guide for 6.2.0.
04/22/2021	Revision 5: Added Install Log section.
05/07/2021	Revision 6: Release of Azure Installation Guide for 6.2.1.
06/07/2021	Revision 7: Updated Elasticsearch screenshot for 6.2.x guides.
07/06/2021	Revision 8: Release of Azure Installation Guide for 6.3.0.
08/26/2021	Revision 9: Release of Azure Installation Guide for 6.3.1.
10/15/2021	Revision 10: Release of Azure Installation Guide for 6.3.2.
11/17/2021	Revision 11: Updated Register Collectors instructions for 6.x guides.
12/22/2021	Revision 12: Release of Azure Installation Guide for 6.3.3.
08/18/2022	Revision 13: Updated All-in-one Installation section.
10/20/2022	Revision 14: Updated Register Collectors instructions for 6.x guides.
05/18/2023	Revision 15: Updated steps in Create a VM Using a FortiSIEM ### Azure Marketplace Image.

Fresh Installation

This section describes how to install FortiSIEM for the current release.

- [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
 - Cluster with Manager, Supervisor and Workers
 - All-in-one with Supervisor only, or
 - Cluster with Supervisor and Workers
- Choose the storage type for Supervisor, Worker, and/or Collector
 - Online - There are 4 choices
 - EventDB on local disk
 - EventDB on NFS
 - ClickHouse
 - Elasticsearch
 - Archive – There are 2 choices
 - EventDB on NFS
 - HDFS
- Determine hardware requirements and choose the Azure instance type accordingly:

Node	vCPU	RAM	Local Disks
Manager	Minimum – 16 Recommended - 32	Minimum • 24GB Recommended • 32GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB	OS – 25GB OPT – 100GB

Node	vCPU	RAM	Local Disks
		<ul style="list-style-type: none"> with UEBA - 32GB Recommended <ul style="list-style-type: none"> without UEBA – 32GB with UEBA - 64GB 	CMDb – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none"> without UEBA – 24GB with UEBA - 32GB Recommended <ul style="list-style-type: none"> without UEBA – 32GB with UEBA - 64GB 	OS – 25GB OPT – 100GB CMDb – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB
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.

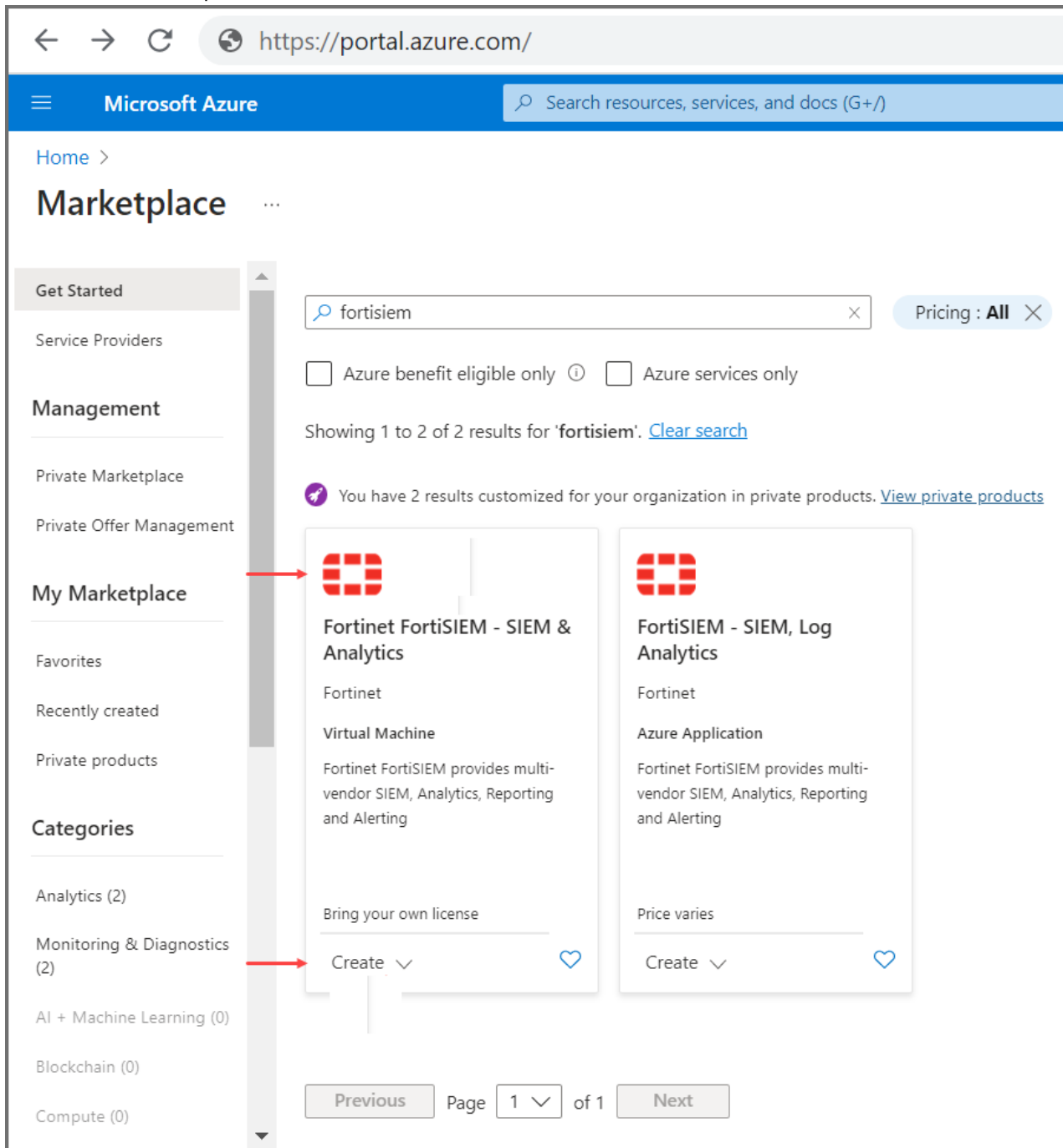
All-in-one Installation

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

- [Find the FortiSIEM Offer in Azure Using the Azure Marketplace](#)
- [Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image](#)
- [Configure FortiSIEM](#)
- [Upload the FortiSIEM License](#)
- [Configure an Event Database](#)
- [Final Check](#)

Find the FortiSIEM Offer in Azure Using the Azure Marketplace

1. On the Azure portal, search for Marketplace and navigate to **Azure Marketplace**.
2. Search for the keyword "fortisiem".
3. Select the **Create** drop-down, and choose **Fortinet FortiSIEM for Azure**.



At this point, Azure will take you through the steps to create a virtual machine by first taking you to the **Create a virtual machine** page. Follow the steps in [Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image](#) to continue.

Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image

From the **Create a virtual machine** page, take the following steps:

1. From the **Resource group** drop-down list, select a resource group.
2. In the **Virtual machine name** field, enter a name for your virtual machine.
3. From the **Image** drop-down list, select the image.

portal.azure.com/#create/Microsoft.VirtualMachine-ARM

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ [Redacted]

Resource group * ⓘ (New) test [Create new](#)

Instance details

Virtual machine name * ⓘ fsm-super ✓

Region * ⓘ (US) West US

Availability options ⓘ No infrastructure redundancy required

Security type ⓘ Standard

Image * ⓘ Fortinet FortiSIEM for Azure - x64 Gen1 [See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64 x64

[Review + create](#) < Previous Next : Disks >

4. From the **Size** drop-down list, select a size based on your node type and hardware requirements.

5. Under **Administrator account**, select **SSH public key** for Authentication type.
6. The **Username** field is specified as `azureuser`.
7. From the **Key pair name** drop-down list, select your existing key pair. If needed, generate a new key pair, then select it here.

The screenshot shows the 'Create a virtual machine' page in the Azure portal. The configuration is as follows:

- Image:** Fortinet FortiSIEM for Azure - x64 Gen1
- VM architecture:** x64 (selected)
- Run with Azure Spot discount:**
- Size:** Standard_B8ms - 8 vcpus, 32 GiB memory (\$289.81/month)
- Administrator account:**
 - Authentication type:** SSH public key (selected)
 - Username:** azureuser
 - SSH public key source:** Generate new key pair
 - Key pair name:** fsm-super_key

A blue information box states: "Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine."

8. When done with this step for configuration , click **Next: Disks >**.
9. On the **Create a new disk** page, you will need to create disks based on the following table.

Volume Name	Size	Disk Name
Data Disk LUN 0	100GB	/opt

Volume Name	Size	Disk Name
		For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when <code>configFSM.sh</code> runs.
Data Disk LUN 1	60GB for FortiSIEM Supervisor or 200GB for FortiSIEM Manager	/cmdb
Data Disk LUN 2	60GB	/svn
Data Disk LUN 3	60GB+	/data (see the following note)

Note on Data Disk LUN 3:

- Add the 4th Data Disk only if using EventDB on local storage or ClickHouse. In all other cases, this disk is not required.
 - 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.
 - Choose Standard SSD volume type for all volumes. For the CMDB partition, you can choose to modify your volume type to Premium SSD or Ultra SSD based on your system workload if you see the consistently high IOPS requirement in your deployment.
- a. In the **Name** field, enter the name of the disk.
 - b. In the **Source** type drop-down list, leave as **None (empty disk)**.
 - c. In the **Size** drop-down list, select **Change size**, select the **Custom disk size (GiB)** option, and enter the disk size in the available field.
 - d. Click **OK**.
 - e. For each new disk, click **Create and attach a new disk** and repeat steps a-d until all the necessary disks have

been created.

portal.azure.com/#view/Microsoft_Azure_Compute/CreateDataDiskBlade/

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine >

Create a new disk ...

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name * fsm-super_opt_disk ✓

Source type * ① None (empty disk) ▼

Size * ① **100 GiB**
Standard SSD LRS
[Change size](#)

Key management ① Platform-managed key ▼

Enable shared disk Yes No

Delete disk with VM

OK

10. After entering your disk partition values, click **Next: Networking >**.

Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host

i Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

OS disk

OS disk type *

If performance is critical for your workloads, choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. [Learn more](#)

Delete with VM

Key management

Enable Ultra Disk compatibility

Data disks for fsm-super

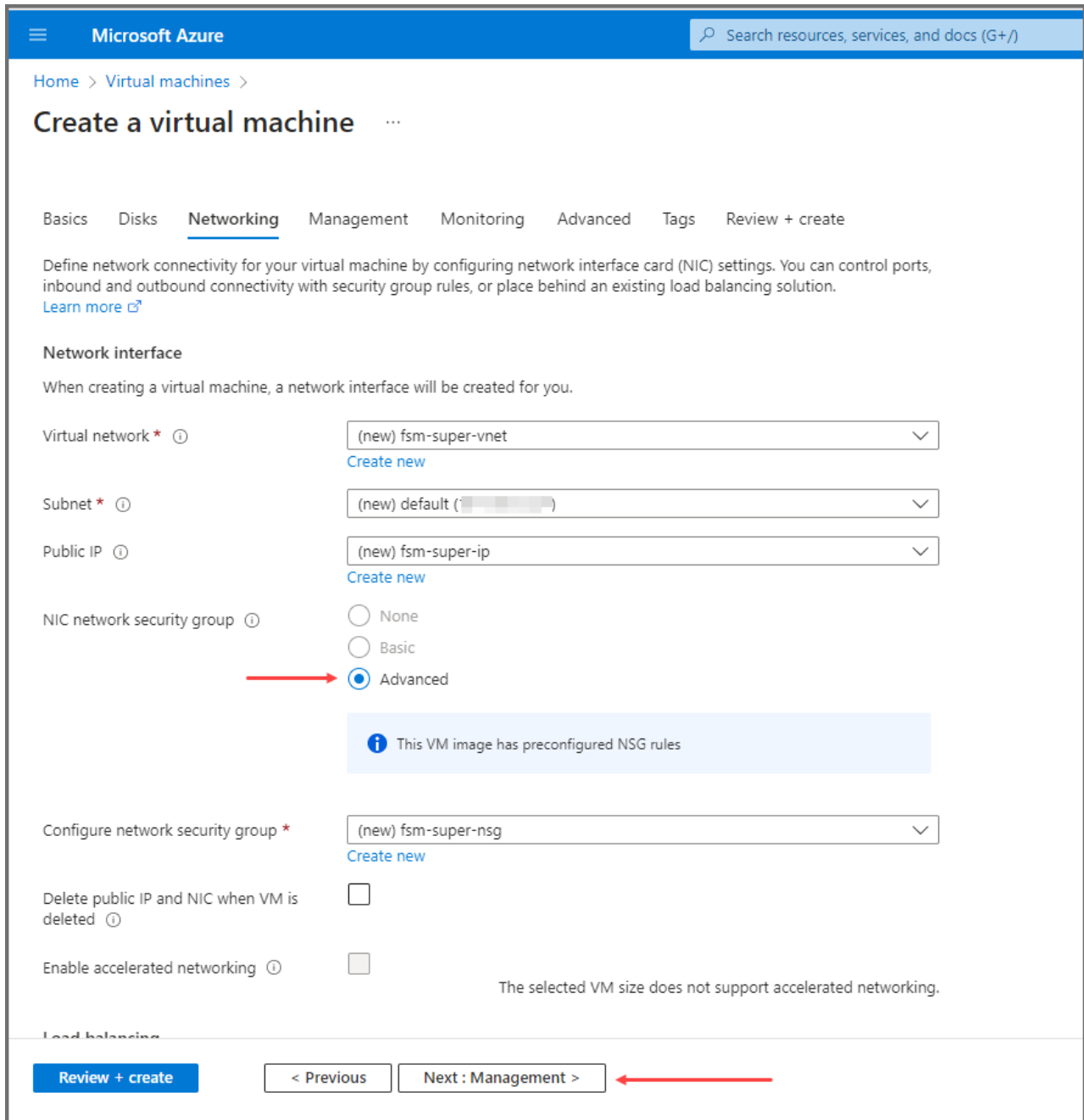
You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
<input type="text" value="0"/>	fsm-super_opt_disk	100	Standard SSD LRS	None	<input checked="" type="checkbox"/>
<input type="text" value="1"/>	fsm-super_cmdb_disk	60	Standard SSD LRS	None	<input checked="" type="checkbox"/>
<input type="text" value="2"/>	fsm-super_svn-lite_disk	60	Standard SSD LRS	None	<input checked="" type="checkbox"/>
<input type="text" value="3"/>	fsm-super_DataDisk_3	120	Standard SSD LRS	None	<input checked="" type="checkbox"/>

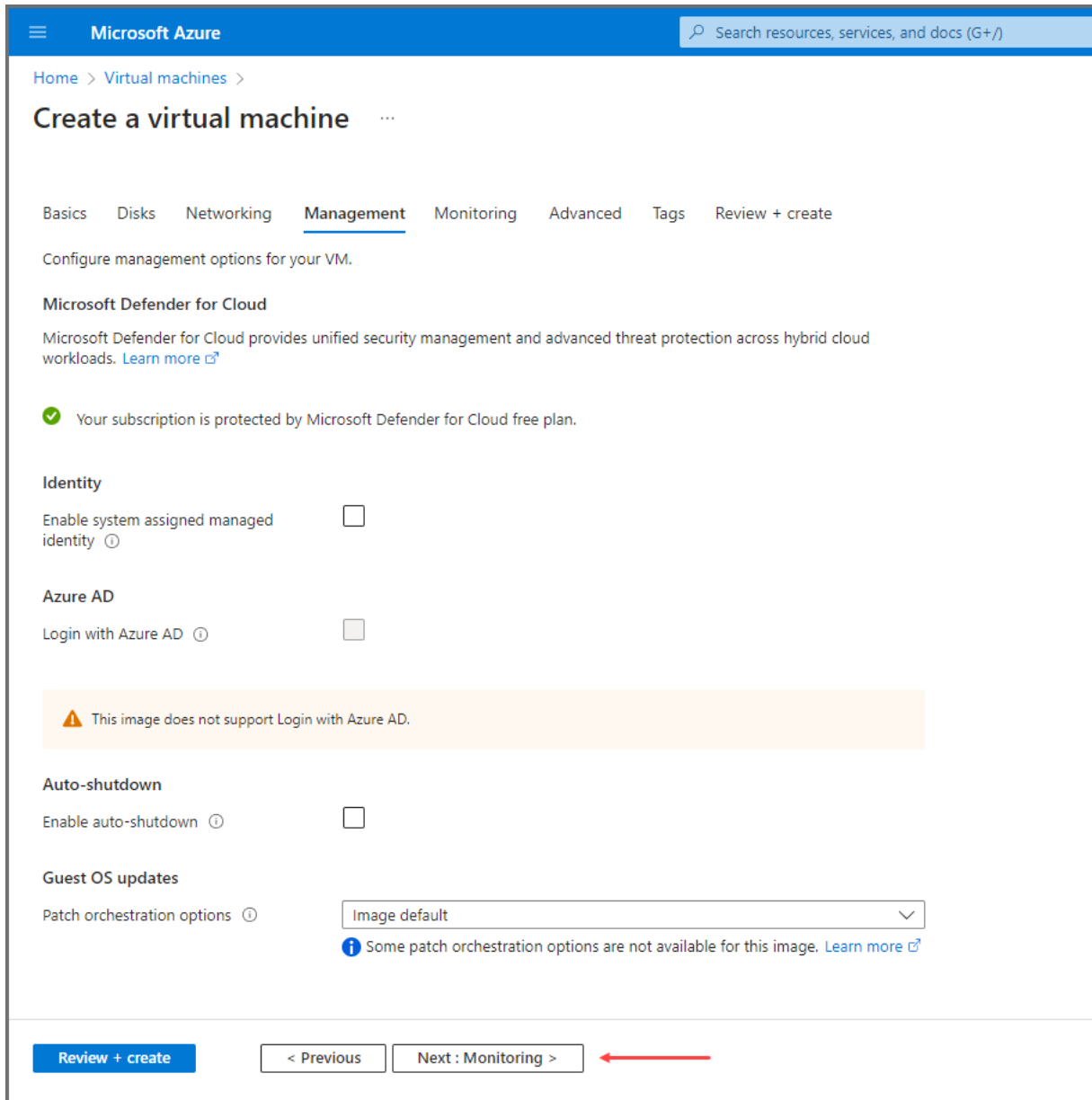
[Create and attach a new disk](#) [Attach an existing disk](#)

[Review + create](#) [< Previous](#) [Next: Networking >](#)

- From the Networking page (Networking tab), accept the defaults except for **NIC network security groups**. For production, choose **Advanced** and configure the required inbound ports and IP addresses (refer to [Azure documentation](#)).



12. Click **Next: Management >**.
13. From the Management page (Management tab), accept the defaults provided or change them as needed per the [Azure documentation](#).
14. Click **Next: Monitoring**.



- From the Monitoring page (Monitoring tab), under **Diagnostics**, select **Enable with managed storage account (recommended)**.
Click **Next: Advanced >**.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Monitoring' tab. The breadcrumb navigation is 'Home > Virtual machines >'. The title is 'Create a virtual machine'. The tabs are 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring' (selected), 'Advanced', 'Tags', and 'Review + create'. Below the tabs, it says 'Configure monitoring options for your VM.' There are two sections: 'Alerts' and 'Diagnostics'. Under 'Alerts', there is a checkbox for 'Enable recommended alert rules' which is unchecked. Under 'Diagnostics', there is a section for 'Boot diagnostics' with three radio button options: 'Enable with managed storage account (recommended)' (selected), 'Enable with custom storage account', and 'Disable'. A red arrow points to the selected option. Below this is a checkbox for 'Enable OS guest diagnostics' which is unchecked. At the bottom, there are three buttons: 'Review + create' (blue), '< Previous', and 'Next : Advanced >' (with a red arrow pointing to it).

16. Leave Advanced settings alone, and click **Next: Tags >**.
17. From the Tags page (Tags tab), add a Name tag and any other tags as needed.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Basics Disks Networking Management Monitoring Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
name ←	fsm-super ←	13 selected ↓
		13 selected ↓

Review + create < Previous Next : Review + create > ←

18. Click **Next: Review + create >**.

19. From the Review + create page tab, verify that all the information is correct. Click **Create**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Validation passed

Basics

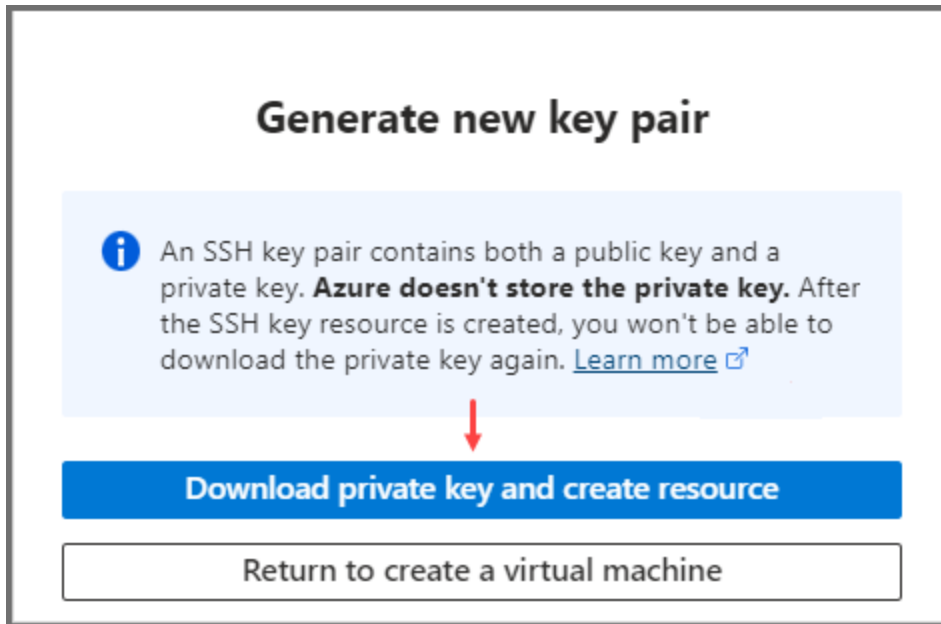
Subscription	Software Development/Engineering
Resource group	(new) test
Virtual machine name	fsm-super
Region	West US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Fortinet FortiSIEM for Azure - Gen1
VM architecture	x64
Size	Standard B8ms (8 vcpus, 32 GiB memory)
Authentication type	SSH public key
Username	azureuser
Key pair name	fsm-super_key
Azure Spot	No

Disks

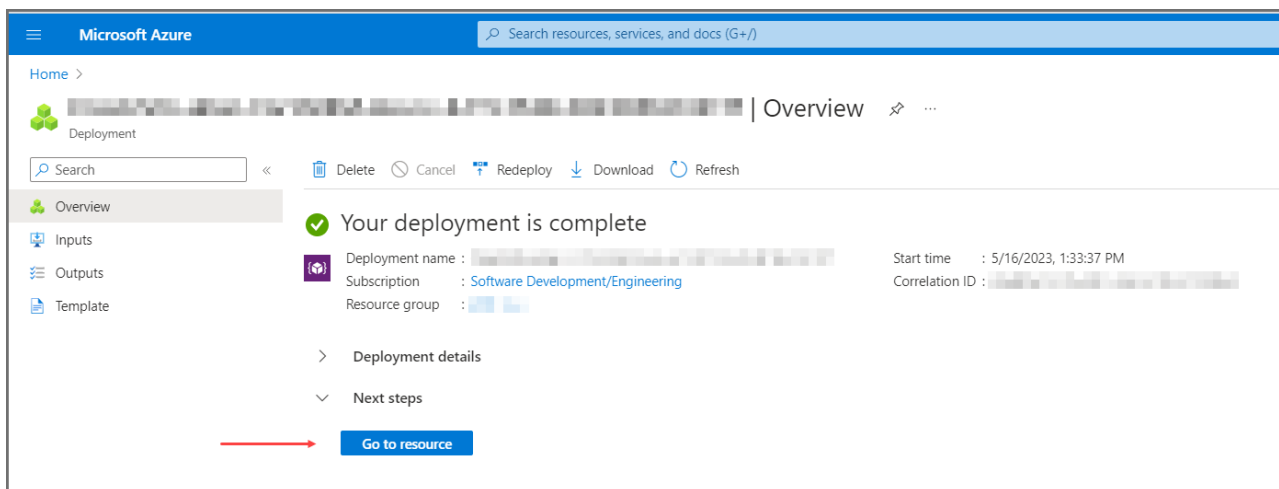
OS disk type	Standard SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Data disks	4

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#)

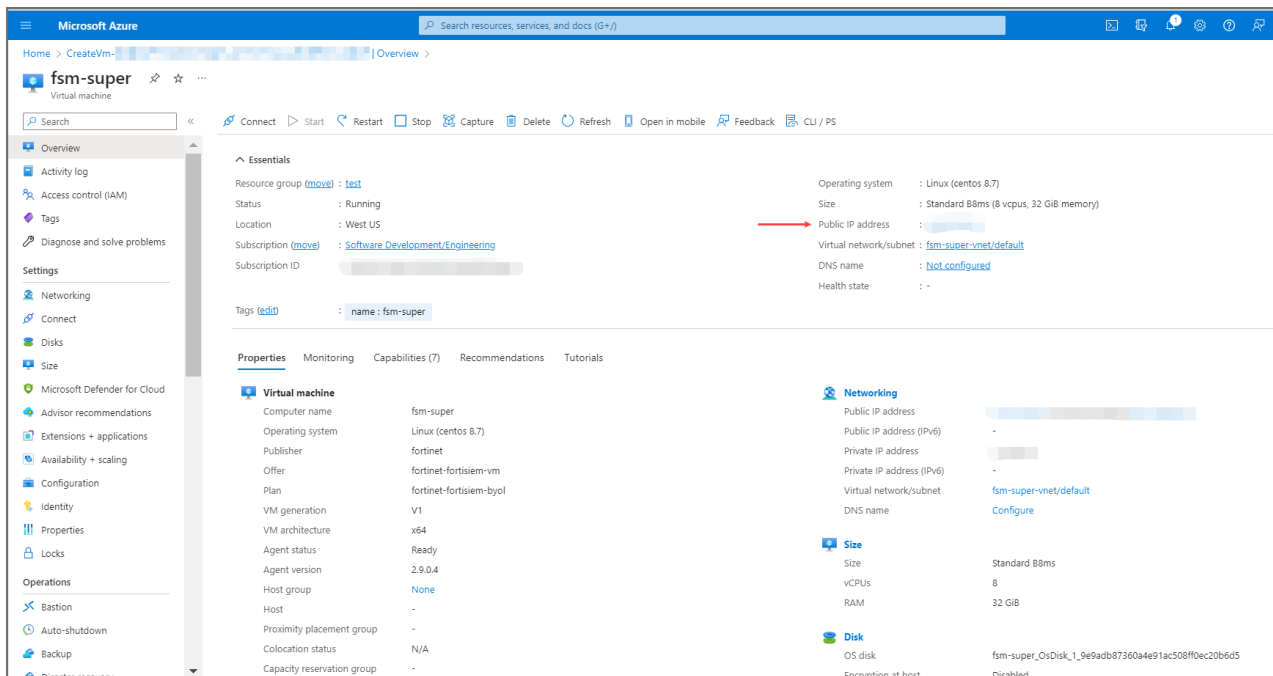
20. If you chose to create a new SSH key, then you will be asked to download the private key and create the resource. Click **Download private key and create resource**.



21. Wait for deployment to succeed. Click **Go to resource**.



22. Note the **Public IP address** and copy it to the clipboard.



- 23. (Optional) Configure the DNS name according to [Azure documentation](#).
- 24. SSH to the FortiSIEM VM with user `azureuser` (as specified [here](#)) and the downloaded SSH key. Run `sudo su -` to become user `root`. Run `configFSM.sh`.

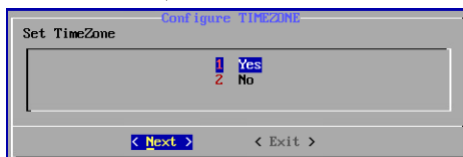
```

$ ssh -i ~/.ssh/fsm-westus-ssh-key.pem azureuser@104.42.55.107
Last login: Tue Sep 22 17:55:11 2020 from 69.181.213.37
[azureuser@super-611-1302 ~]$ sudo su -
Last login: Tue Sep 22 17:55:15 CDT 2020 on pts/0
[root@super-611-1302 ~]# configFSM.sh
    
```

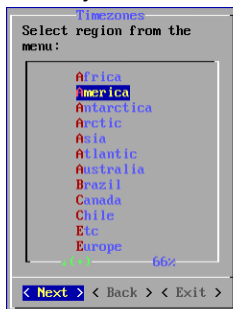
Configure FortiSIEM

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

1. At the `root` command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`# configFSM.sh`
2. In VM console, select **1 Set Timezone** and then press **Next**.



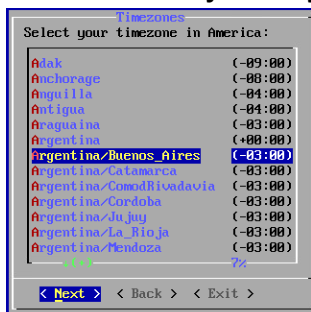
3. Select your **Location**, and press **Next**.



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

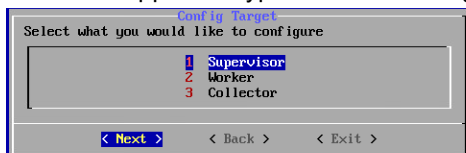


5. Select the **Country** and **City** for your timezone, and press **Next**.



6. 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 FortiSIEM Manager, select **4 FortiSIEM Manager**, and press **Next**.
 If installing FortiSIEM Supervisor Follower, select **5 Supervisor Follower** and press **Next**.

Note: The appliance type cannot be changed once it is deployed, so ensure you have selected the correct option.



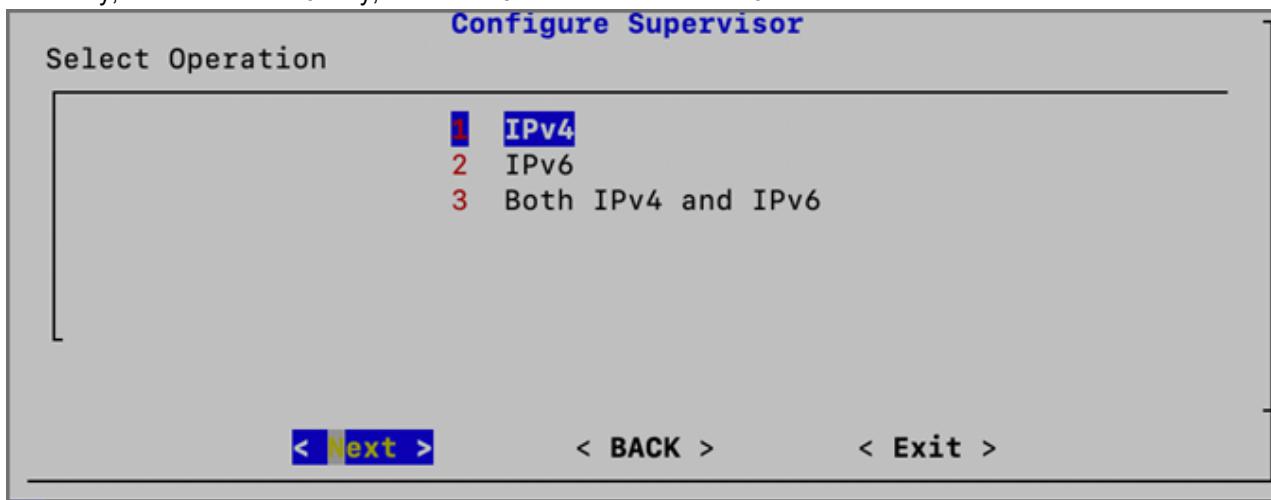
Regardless of whether you select **FortiSIEM Manager**, **Supervisor**, **Supervisor Follower**, **Worker**, or **Collector**, you will see the same series of screens with only the header changed to reflect your target installation, unless noted otherwise.

7. If you want to enable FIPS, then choose **2 install_with_fips**. Otherwise, choose **1 install_without_fips**. 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.

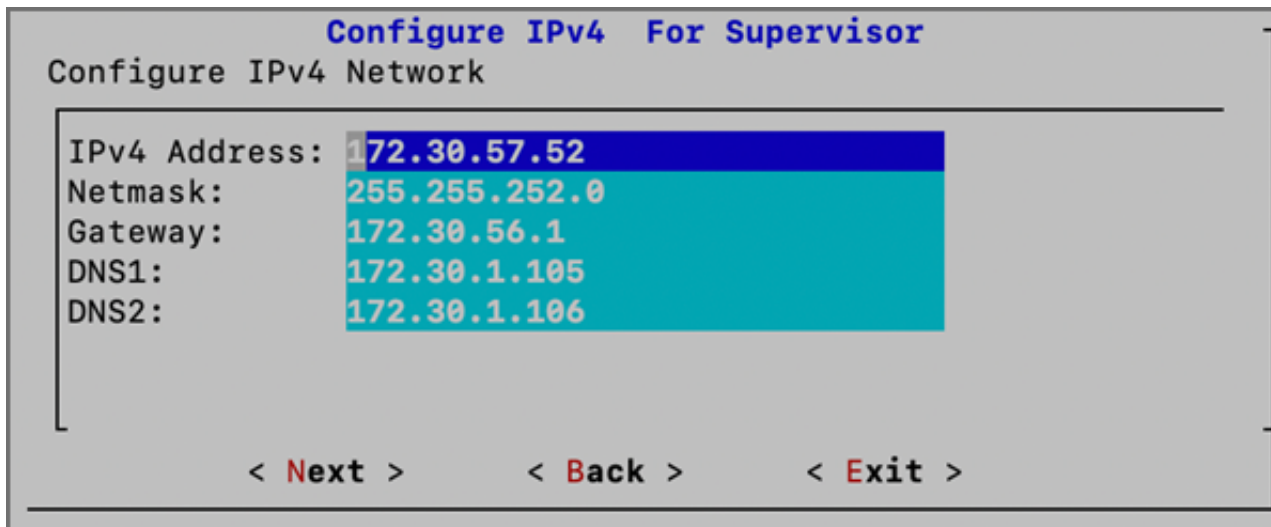


- Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose **1** for IPv4-only, choose **2** for IPv6-only, or choose **3** for both IPv4 and IPv6.



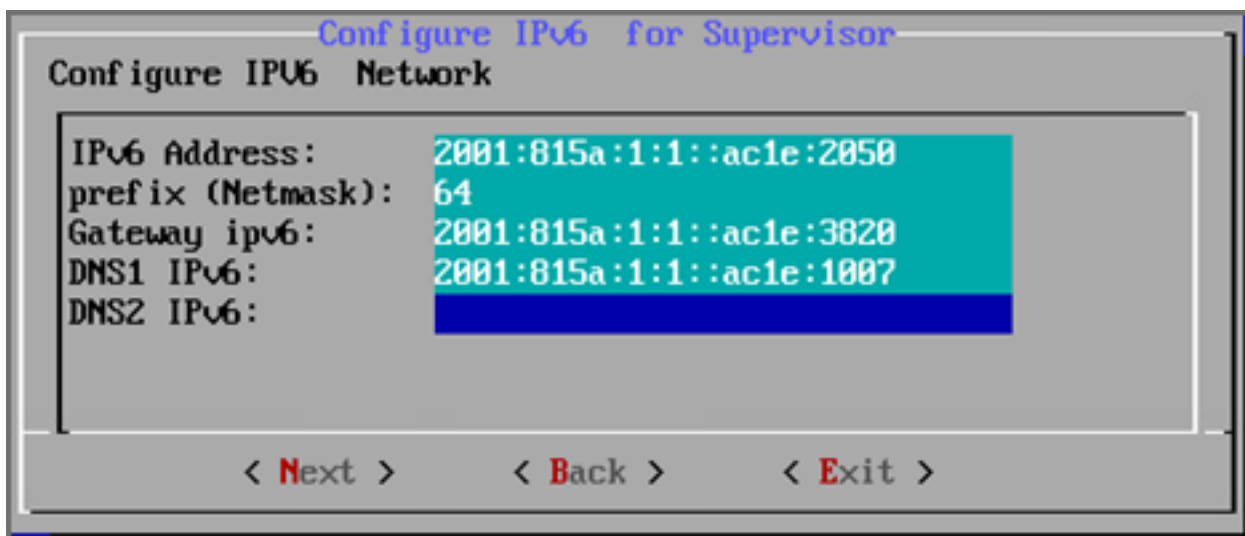
- If you choose **1** (IPv4) or choose **3** (Both IPv4 and IPv6), and press **Next**, then you will move to step 10. If you choose **2** (IPv6), and press **Next**, then skip to step 11.
- Configure the IPv4 network by entering the following fields. Press **Next**.

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



11. If you chose 1 in step 8, then you will need to skip to step 12. If you chose 2 or 3 in step 8, then you will configure the IPv6 network by entering the following fields, then press **Next**.

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



Note: If you chose option 3 in step 8 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.

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

Configure Hostname For Supervisor

Configure hostname

Host name:

< Next >
 < Back >
 < Exit >

Note: FQDN is no longer needed.

13. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. In order for the migration to complete, the system still needs https connectivity to FortiSIEM OS update servers - `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-c8.fortisiem.fortinet.com`. Then, click **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

< Next >
 < Back >
 < Exit >

14. 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**.

```

Configure Supervisor
Run Configuration Command:

python /usr/local/bin/configureFSM.py -r super -z America/Los_Angeles -i
172.30.56.103 -m 255.255.252.0 -g 172.30.56.1 --host sp56103-3103-v46 -t 64
--dns1 172.30.1.105 --dns61 2001:815a:1:1::ac1e:1007 --i6
2001:815a:1:1::ac1e:3103 --m6 64 --g6 2001:815a:1:1::ac1e:3820 -o change_ip
--testpinghost ipv6-dns.fortinet.com

< Run >      < Back >      < Exit >

```

The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
--host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either 4 (for ipv4) or 6 (for v6) or 64 (for both IPv4 and IPv6).
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
--i6	IPv6-formatted address
--m6	IPv6 prefix
--g6	IPv6 gateway
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_network_config*) *Option only available after installation.
-z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

- 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](#).

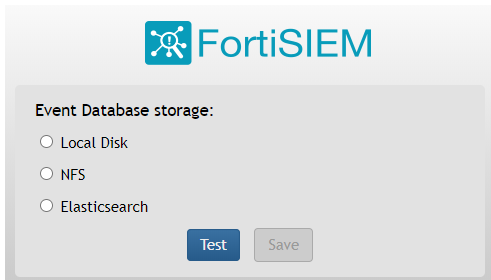
You will now be asked to input a license.

- 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.
- The License Upload dialog box will open.

- Click **Browse** and upload the license file.
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
- 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.
- For Supervisor, Worker, or Collector, choose **License type** as **Enterprise** or **Service Provider**. The following option will be available for first time installations. 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.
- Proceed to [Configure an Event Database](#).

Configure an Event Database

Choose the event database.



If the Event Database is one of the following options, additional disk configuration is required.

- **EventDB on Local Disk:** See Case 2 in [Creating EventDB Online Storage](#).
- **ClickHouse:** See Case 2 in [Creating ClickHouse Online 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 Follower, Worker and Collector, the response should be similar to the following.

```
Every 1.8s: /opt/phenix/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, 6.22us, 2.12sq, 0.02nl, 0.43id, 0.03aw, 0.22hl, 0.12sl, 0.02st
Mem: 6592180k total, 10366836k used, 5533694k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465820k cached

PROCESS           UPTIME          CPU%           VIRT_MEM       RES_MEM
phParser           41:23           0              2176m          550m
phQueryMaster     41:41           0              1020m          77m
phUserMaster     41:41           0              1079m          504m
phUserWorker     41:41           0              1303m          295m
phQueryWorker    41:41           0              1303m          273m
phDataManager    41:41           0              1419m          285m
phDiscover       41:41           0              513m           53m
phReportWorker   41:41           0              1433m          95m
phReportMaster   41:41           0              603m           67m
phIdentityWorker 41:41           0              1027m          58m
phIdentityMaster 41:41           0              491m           39m
phAgentManager   41:41           0              1425m          54m
phCheckpoint     42:31           0              325m           34m
phMonitor        41:41           0              702m           70m
phReportLoader   41:41           0              769m          220m
phBeaconEventPackager 41:41           0              1125m          65m
phDataPurger     41:41           0              588m           58m
phEventForwarder 41:41           0              540m           46m
phMonitor        37:24           0              2030m          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           36m
phenomally      01:00:07        0              987m           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.

Cluster Installation

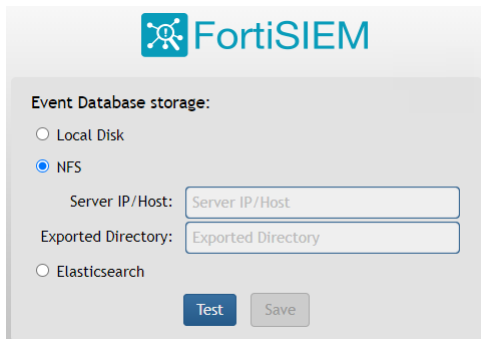
For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS, ClickHouse, or Elasticsearch).

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

Install 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 4 is not required (From [Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image Step 8](#)).
 - b. You need to configure NFS after license upload.



The screenshot shows the FortiSIEM configuration interface for Event Database storage. The title is "Event Database storage:". There are three radio button options: "Local Disk", "NFS", and "Elasticsearch". The "NFS" option is selected. Below the "NFS" option, there are two input fields: "Server IP/Host:" and "Exported Directory:". At the bottom of the form, there are two buttons: "Test" and "Save".

3. If you choose **ClickHouse**
 - a. You need to create disks during [Create a VM Using a FortiSIEM 6.3.1 Azure Marketplace Image Step 8](#) based on the role of the Supervisor node in the ClickHouse cluster. See the [ClickHouse Sizing Guide](#) for details.
 - b. You need to configure disks after license upload.
4. If you choose **Elasticsearch**, define Elasticsearch endpoints after license upload. See the [Elasticsearch Sizing](#)

[Guide](#) for details.



The screenshot shows the FortiSIEM configuration interface for Event Database storage. At the top is the FortiSIEM logo. Below it, the section is titled "Event Database storage:". There are three radio button options: "Local Disk", "NFS", and "Elasticsearch", with "Elasticsearch" selected. Under "Elasticsearch", there are three radio button options for "ES Service Type": "Native", "Amazon", and "Elastic Cloud", with "Native" selected. The "URL:" field contains "https://" and has plus and minus buttons. The "REST Port:" field contains "443". The "User Name:" field contains "(Optional)". The "Password:" field contains "(Optional)". The "Confirm Password:" field is empty. Below these, there are three radio button options for "Shard Allocation": "Fixed", "Dynamic", and "Dynamic" is selected. The "Shards:" field contains "5". The "Replicas:" field contains "1". At the bottom, there is a "Per Org Index" checkbox which is unchecked. There are "Test" and "Save" buttons at the bottom right.

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 – 100GBFor 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.

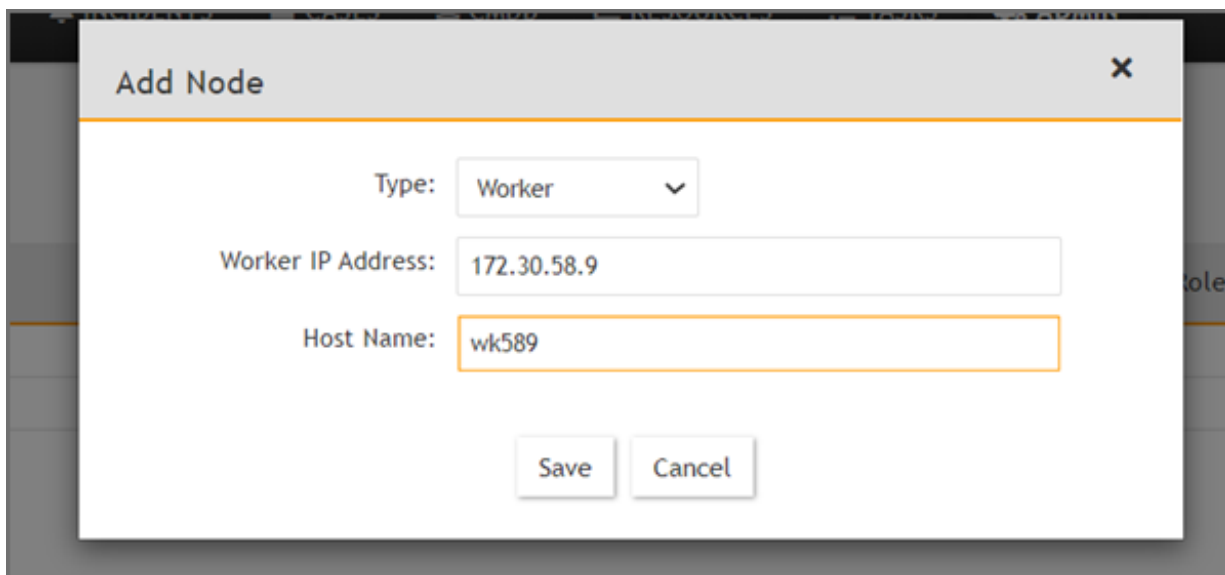
Sizing Guide References:

- [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.
 - d. Click **Test**.



The screenshot shows a modal window titled "Add Node" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Type:** A dropdown menu with "Worker" selected.
- Worker IP Address:** A text input field containing "172.30.58.9".
- Host Name:** A text input field containing "wk589".
- Buttons:** "Save" and "Cancel" buttons at the bottom center.

- 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.

The screenshot displays the FortiSIEM Cloud Health interface. On the left is a navigation sidebar with options: Setup, Device Support, Health (selected), License, and Settings. The main content area is divided into two sections. The top section, titled 'Cloud Health', shows a table with columns: Name, IP Address, Module Role, Health, Version, Load Average, CPU, and Swap Used. It lists two nodes: 'sp572.fortinet.com' (Supervisor, Normal, 6.1.0.1238) and 'wk573.fortinet.com' (Worker, Normal, 6.1.0.1238). The bottom section, titled 'Process level metrics for wk573.fortinet.com (172.30.57.3)', shows a table with columns: Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. It lists processes like Node.js-charting, httpd, Redis, Node.js-pm2, rsyslogd, and chDataManaaer. At the bottom, there is a footer with copyright information and system details: 'Copyright © 2020 Fortinet, Inc. All rights reserved. Organization: Super User: admin Scope: Global FortiSIEM'.

4.

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 when adding disks, you need to only add a data disk for OPT. The recommended CPU and memory settings for Collector node, and required hard disk settings are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

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

Register Collectors

Collectors can be deployed in Enterprise or Service Provider environments.

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

Enterprise Deployments

For Enterprise deployments, follow these steps.

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

The Collector will reboot during the Registration.
5. Go to **ADMIN > Health > Collector Health** for the status.

The screenshot shows the 'Collector Health' page in FortiSIEM. It features 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 are search and action controls. The primary table lists collector details:

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

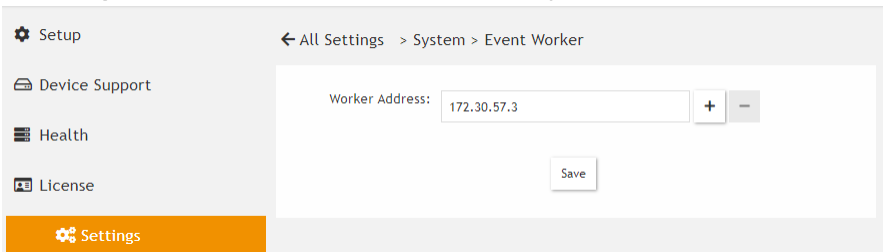
Below this table is a 'Close Panel' section with a search bar and a 'Columns' dropdown. It displays a detailed view of system processes:

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**.
 - c. In the **Supervisors** column, enter the IP of the Supervisor node and click **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.

Organization Definition (ORG) - Add Collector ✕

Name:

Guaranteed EPS:

Upload Rate Limit (Kbps):

Start Time: Unlimited

End Time: Unlimited

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.

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

```
root@co574 ~# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@co574 ~# phProvisionCollector --add admin Admin=11.172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@co574 ~# _
```

The Collector will reboot during the Registration.

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

- Setup
- Device Support
- Health
- License
- Settings

Cloud Health
Collector Health

Show Processes
Tunnels
Action
Search...
Columns
Lines: 1 Last update at 8:54:17 PM

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

Close Panel
Search...
Columns
Lines: 9 Last update at 8:54:24 PM

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 Log

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

Errors can be found at the end of the file.



www.fortinet.com

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