FORTINET®

FortiInsight - VM Installation Guide

Version 6.2.0

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 17, 2020
FortiInsight 6.2.0 VM Installation Guide
52-600-543474-20190801

TABLE OF CONTENTS

Change log

Date	Change description
2020-09-17	First release of FortiInsight VM-installation guide.

Architecture

FortiInsight-VM is a virtual appliance version of FortiInsight. It is deployed in a virtual machine environment such as VMware ESX (or ESXi), MS Hyper-V, or KVM.

FortiInsight-VM requires the following connectivity for management. SSH is intended for initial configuration and diagnostics only. For more information, see the FortiInsight administration Guide.

Inbound management

Service	Port	Description
HTTPS	443	UI and API connection
HTTPS	8080	Collector Connection
SSH	22	SSH for initial configuration and diagnostics

Overview

This section provides an overview of FortiInsight VM-installation.

Licensing

Fortinet offers the FortiInsight-VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiInsight-VM, make sure to configure hardware settings as outlined in table three and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

FortiInsight VM Licensing

SKU	Description
FIN-VM-Base	Base FortiInsight-VM. Unlimited vCPU. Unlimited vRAM. User Licenses must be purchase separately.

FortiInsight VM User Licenses

Name	Description
FC1-10-FIN01-260-01-DD	25 User License Subscription for FortiInsight. Must be purchased with VM or Appliance. Includes 24/7 support.
FC2-10-FIN01- 260-01-DD	500 User License Subscription for FortiInsight. Must be purchased with VM or Appliance. Includes 24/7 support.
FC3-10-FIN01- 260-01-DD	10,000 User License Subscription for FortiInsight. Must be purchased with VM or Appliance. Includes 24/7 support.

System requirements

Prior to deploying the FortiInsight-VM virtual appliance, either VMware vSphere Hypervisor (ESX versions 4.0 or 4.1, ESXi versions 4/5/6), Microsoft Hyper-V Server (2010, 2012 R2, and 2016), or Virtual Machine Manager for KVM must be installed and configured. Note that VMWare ESXi was used for the purposes of this document. The installation instructions for FortiInsight-VM assume you are familiar with both VM platforms and their related terminology. For more details on all platforms, refer to:

- http://www.vmware.com/products/vsphere-hypervisor/overview.html
- https://www.microsoft.com/en-ca/server- cloud/solutions/virtualization.aspx
- https://virt-manager.org/

FortiInsight Virtual Machine Requirements

Resource	Min/Max
Virtual CPU	4 / 64
Virtual interfaces	1 / 4
Virtual Memory	16GB/1TB
Virtual Storage (Total)	180GB/6TB
Data Disk 1	60GB/2TB
Data Disk 2	60GB/2TB
Data Disk 3	60GB/2TB

Register FortiInsight-VM on FortiCloud

To obtain the FortiInsight-VM license file you must first register your FortiInsight-VM on FortiCloud.

1. Log in to FortiCloud using an existing support account or select Create an Account
2. In the toolbar select **Asset** > **Register/Activate**. The Registration Wizard opens.
3. Enter the license registration code from the FortiInsight-VM License Certificate that was emailed to you, and select **Next**.
4. Enter the support contract number, product description, Fortinet Partner, and IP address.
5. Select **Next** to continue.
6. Select the checkbox to indicate that you have read, understood, and accepted the service contract, and select Next to continue.
7. The verification page displays product entitlement. Select the checkbox to indicate that you accept the terms and select **Confirm** to submit the request.
8. In the Registration Completed page you can download the FortiInsight-VM license file. Select the License File Download link. You will be prompted to save the license file (.lic) to your management computer.

To edit the FortiInsight-VM IP address:

1. In the toolbar select **Asset > Manage/View** Products
2. Select the FortiInsight-VM serial number.
3. Select Edit to change the description, partner information, and IP address of your FortiInsight-VM.
4. Enter the new IP address and select Save.

> You can change the IP address five (5) times on a regular FortiInsight-VM license.

5. Select the License File Download link. You will be prompted to save the license file (.lic) to your management computer

Download the FortiInsight-VM software

Fortinet provides the FortiInsight-VM software for 64-bit environments in two formats:

Upgrades: Download this firmware image to upgrade your existing FortiInsight-VM installation.

- FIN_VM-vX.X.X.XXXX-FORTINET.out
- FIN_VM_HV-vX.X.X.XXXX-FORTINET.out
- FIN_VM_KVM-vX.X.X.XXXX-FORTINET.out

New Installations: Download for a new FortiInsight-VM installation. Choose the package relevant to your environment.

- FIN_VM-vX.X.X.XXXX-FORTINET.out.ovf.zip
- FIN_VM_HV-vX.X.X.XXXX-FORTINET.out.hyperv.zip
- FIN_VM_KVM-vX.X.X.XXXX-FORTINET.out.kvm.zip

MS Hyper-v deployment package contents

The FIN_VM_HV-vX.X.X.XXXX-FORTINET.out.hyperv.zip file contains:

1. Snapshots folder:
   - Optionally, Hyper-V stores snapshots of the FortiInsight-VM state here.
2. Virtual Hard Disks folder:
   - DATADRIVE.vhd: The FortiInsight-VM log disk1 in VHD format.
   - DATADRIVE2.vhd: The FortiInsight-VM log disk2 in VHD format.
   - DATADRIVE3.vhd: The FortiInsight-VM message processing disk3 in VHD format.
   - fin.vhd: The FortiInsight-VM system hard disk in VHD format.
3. Virtual Machines folder:
   - fortiinsight.xml: XML file containing virtual hardware configuration settings for Hyper-V.

VMware ESXI deployment package contents

The FIN_VM-vX.X.X.XXXX-FORTINET.out.ovf.zip file contains:

- datadrive.vmdk: The FortiInsight-VM log disk1 in VMDK format.
- datadrive2.vmdk: The FortiInsight-VM log disk2 in VMDK format.
- datadrive3.vmdk: The FortiInsight-VM message processing disk3 in VMDK format.
- fin.vmdk: The FortiInsight-VM system hard disk in VMDK format.
- FortiInsight-VM.ovf: OVF template file for VMware Hardware Type 10 (intel E1000 NIC Driver).

- FortiInsight-VM.hw04.ovf: OVF template file for VMware Hardware Type 04 (intel E1000 NIC Driver).
- FortiInsight-VM.hw07.ovf: OVF template file for VMware Hardware Type 07 (intel E1000 NIC Driver).

KVM deployment package contents

The FIN_VM_KVM-vX.X.X.XXXX-FORTINET.out.kvm.zip file contains:

- datadrive.qcow2: The FortiInsight-VM log disk1 in qcow2 format
- datadrive2.qcow2: The FortiInsight-VM log disk2 in qcow2 format
- datadrive3.qcow2: The FortiInsight-VM message processing disk3 in qcow2 format
- finkvm.file
- finkvm.xml
- finkvm.qcow2

FortiInsight-VM evaluation license

FortiInsight-VM includes a five-user evaluation license; no activation is required for the built-in evaluation license and there is no expiration of the license.

FortiInsight-VM deployment

FortiInsight-VM supports the following hypervisors:

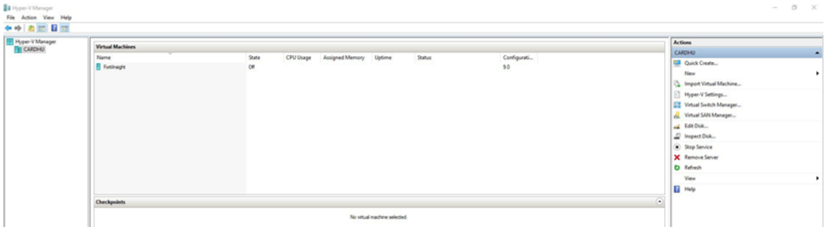
- VMware ESXI
- MS Hyper-V
- KVM

Deploying FortiInsight-VM on MS Hyper-V

Once you have downloaded the out.hyperv.zip file and extracted the package contents to a folder on your management computer, you can deploy the VHD package to your MS Hyper-V environment.

To deploy the FortiInsight VHD template:

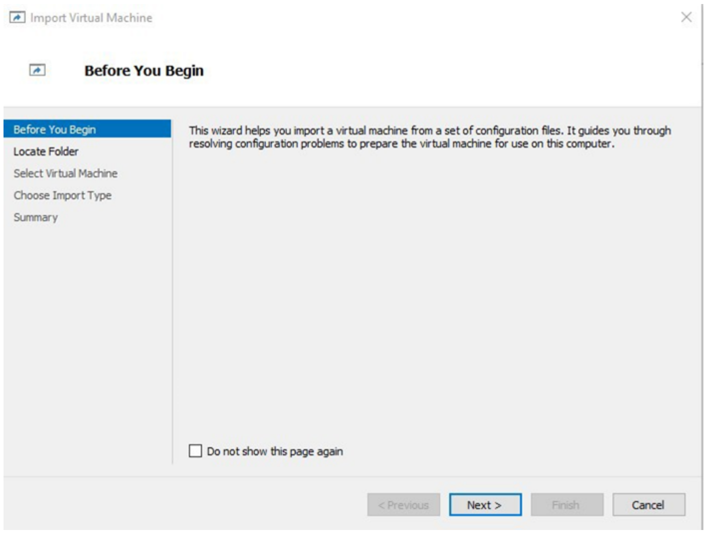
1. As an administrator, launch the Hyper-V Manager and connect to your Hyper-V Server.
2. Select the server in the right-hand menu and select **Import Virtual Machine.**



Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
FortiInsight	Off					9.0

No virtual machine selected.

Select Import Virtual Machine, and select next on the wizard "Before you begin"

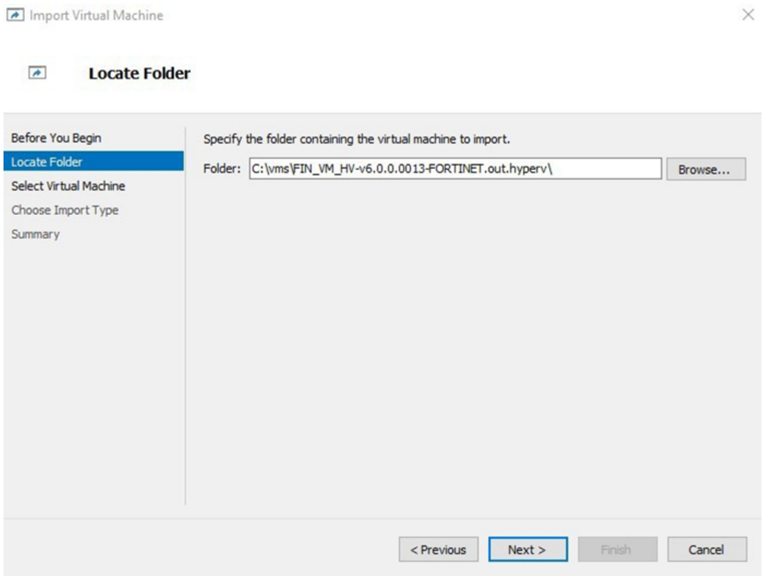


This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

☐ Do not show this page again

Before you begin warning message

3. Enter the location of the VM to be imported. This is the location of the folder that you extracted the FortiInsight hyperv.zip file to.

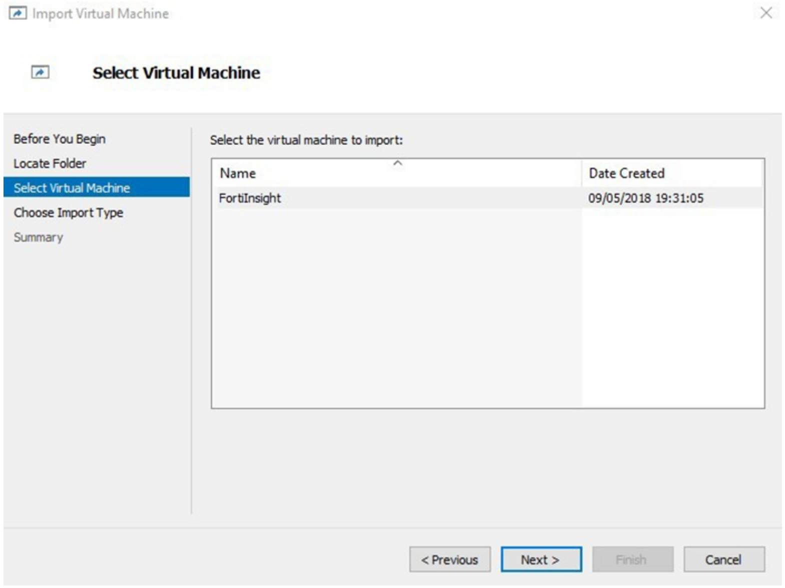


Specify the folder containing the virtual machine to import.

Folder: C:\vms\FIN_VM_HV-v6.0.0.0013-FORTINET.out.hyperv\

Select location of FortiInsight to import from

4. Select the FortiInsight-VM and select **Next**

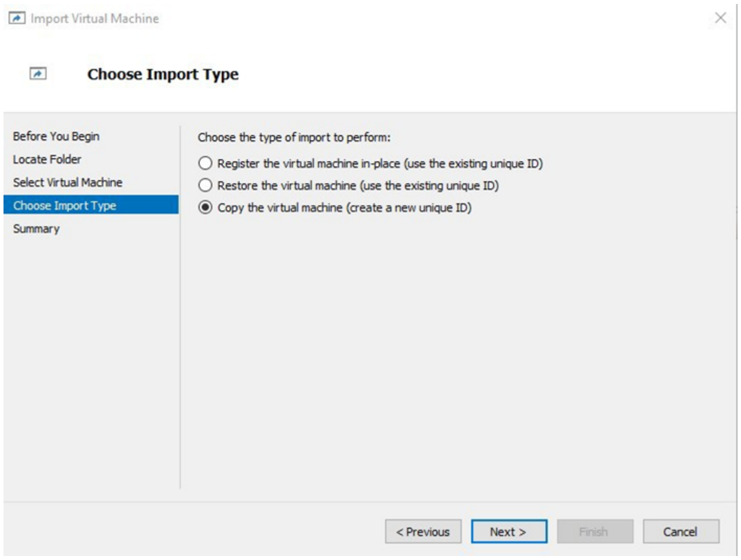


Select the virtual machine to import:

Name	Date Created
FortiInsight	09/05/2018 19:31:05

Select FortiInsight

5. For the import type, choose **Copy** the virtual machine and select **Next**.

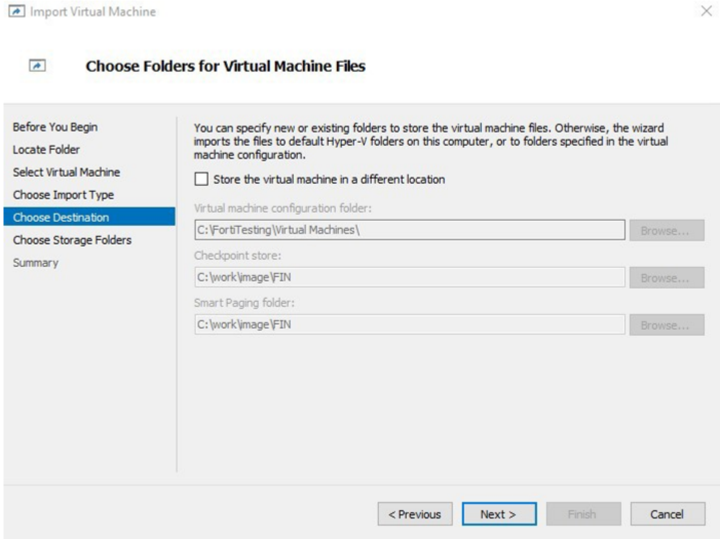


Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)
○ Restore the virtual machine (use the existing unique ID)
● Copy the virtual machine (create a new unique ID)

Copy the FortiInsight Virtual Appliance

6. Select **Next** if you wish to use the default storage location settings, or specify your own.



You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

□ Store the virtual machine in a different location

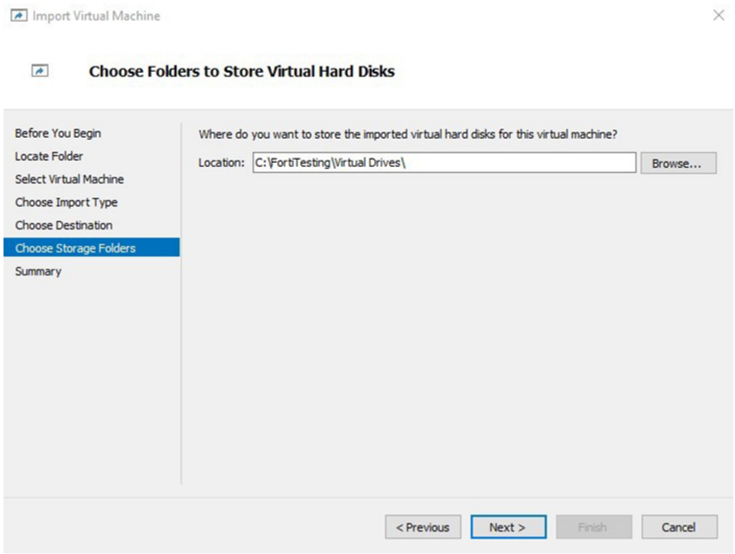
Virtual machine configuration folder: C:\FortiTesting\Virtual Machines\

Checkpoint store: C:\work\image\FIN

Smart Paging folder: C:\work\image\FIN

Choose default location, or customize

7. Select **Next** if you wish to use the default VM hard disk storage settings, or specify your own.



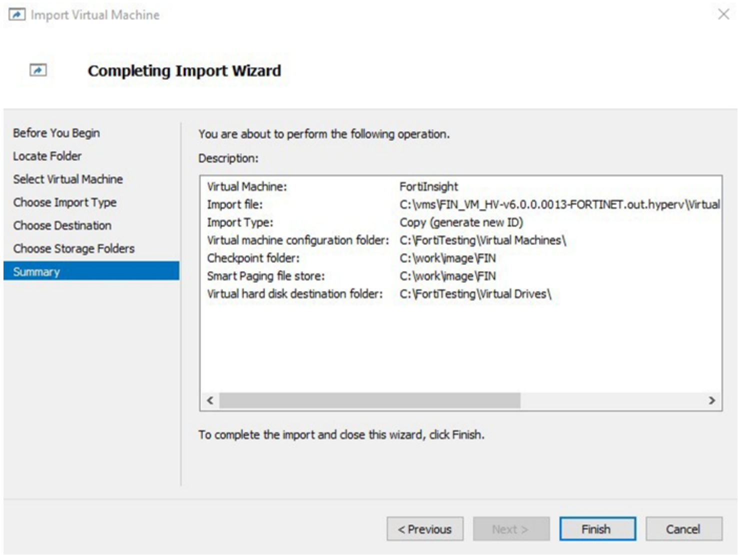
Choose Folders to Store Virtual Hard Disks

Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\FortiTesting\Virtual Drives\

Choose the default location or customize

8. Select **Finish** to accept the configuration and complete the VM installation.



Completing Import Wizard

You are about to perform the following operation.

Description:

```
Virtual Machine:                      FortiInsight
Import file:                          C:\vms\FIN_VM_HV-v6.0.0.0013-FORTINET.out.hyperv\Virtual
Import Type:                          Copy (generate new ID)
Virtual machine configuration folder: C:\FortiTesting\Virtual Machines\
Checkpoint folder:                    C:\work\image\FIN
Smart Paging file store:              C:\work\image\FIN
Virtual hard disk destination folder: C:\FortiTesting\Virtual Drives\
```

To complete the import and close this wizard, click Finish.

Review the summary before deploying the FortiInsight Virtual Appliance

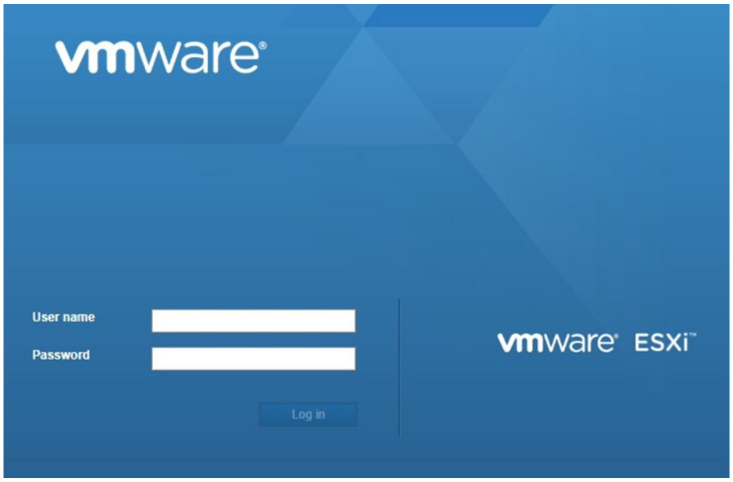
9. The VM will be installed and will be displayed in the Hyper-V Manager. Do not power on the VM; instead, configure the appliance settings as described in Configure FortiInsight-VM hardware settings on page 20

Deploying FortiInsight-VM on VMware

Once you have downloaded the out.ovf.zip file and extracted the package contents to a folder on your management computer, you can deploy it into your VMware environmnt.

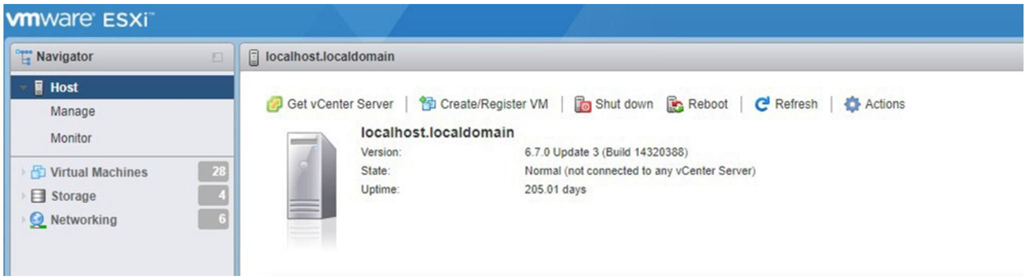
To deploy the FortiInsight-VM OVF template:

1. Connect to your VMware ESXi server by visiting its URL in your browser. Enter your username and password, and click **Log in**.



Login to your VMWare cluster

2. Select Create/Register VM



localhost.localdomain

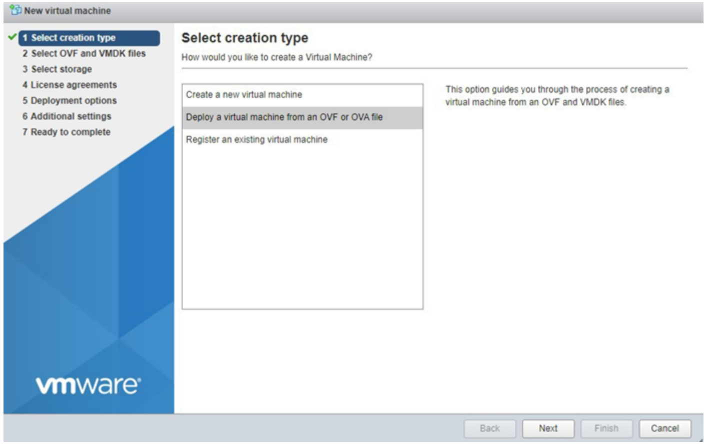
Version: 6.7.0 Update 3 (Build 14320388)

State: Normal (not connected to any vCenter Server)

Uptime: 205.01 days

Create/Register the FortiInsight Virtual Appliance Image

3. Select Deploy a virtual machine from an OVF or OVA file, and click Next.



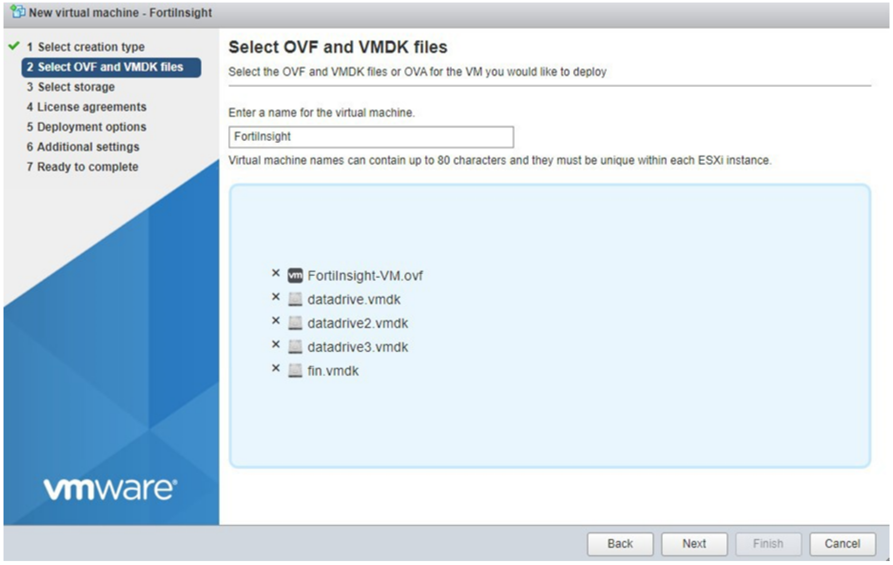
Select creation type

How would you like to create a Virtual Machine?

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

Deploy the FortiInsight virtual appliance image

4. Enter a name for your VM and select the OVF (FortiInsight-VM.ovf), firmware VMDK (fin.vmdk), and all datadrive* storage VMDK (datadrive*.vmdk) files previously extracted to your management computer, and click **Next**.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

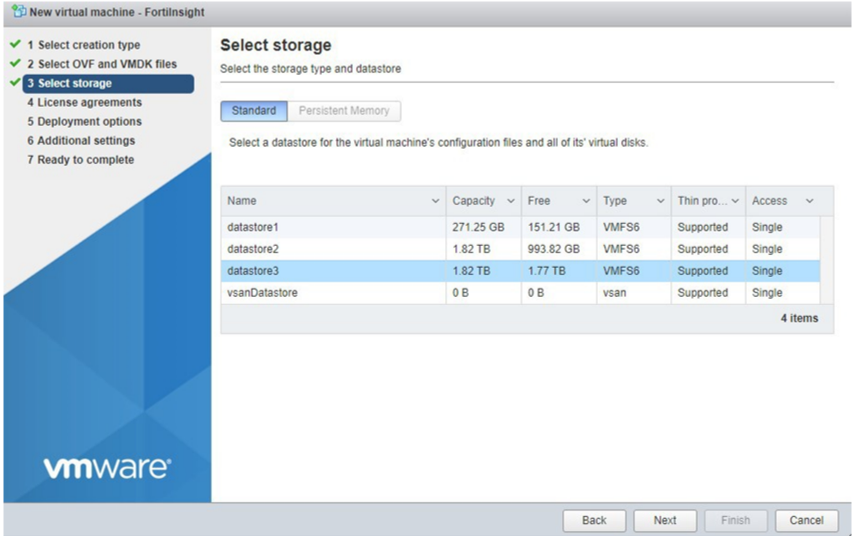
FortiInsight

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

- FortiInsight-VM.ovf
- datadrive.vmdk
- datadrive2.vmdk
- datadrive3.vmdk
- fin.vmdk

Select the FortiInsight OVF and all Data storage disks.

5. Select which ESXi server's datastore to use for the deployment of FortiInsight-VM, and click **Next**.



Select storage

Select the storage type and datastore

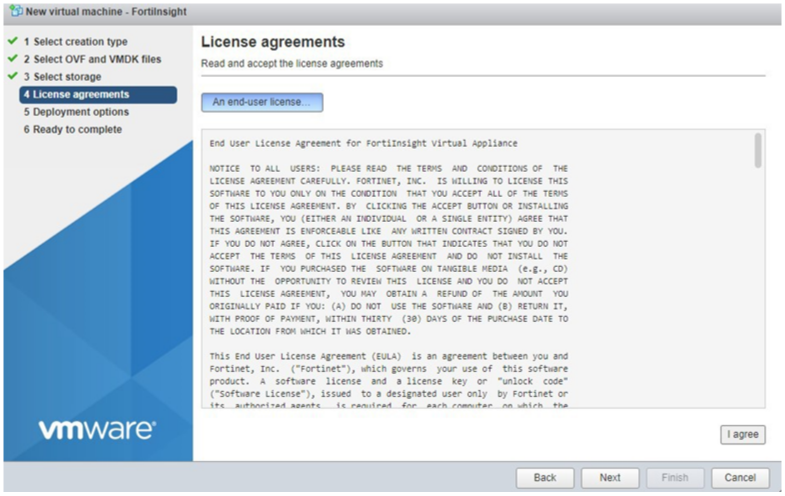
Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	271.25 GB	151.21 GB	VMFS6	Supported	Single
datastore2	1.82 TB	993.82 GB	VMFS6	Supported	Single
datastore3	1.82 TB	1.77 TB	VMFS6	Supported	Single
vsanDatastore	0 B	0 B	vsan	Supported	Single

4 items

Select which storage point to place the FortiInsight Virtual Appliance Image

6. Read the licensing terms and click **I agree** and **Next**.



License agreements

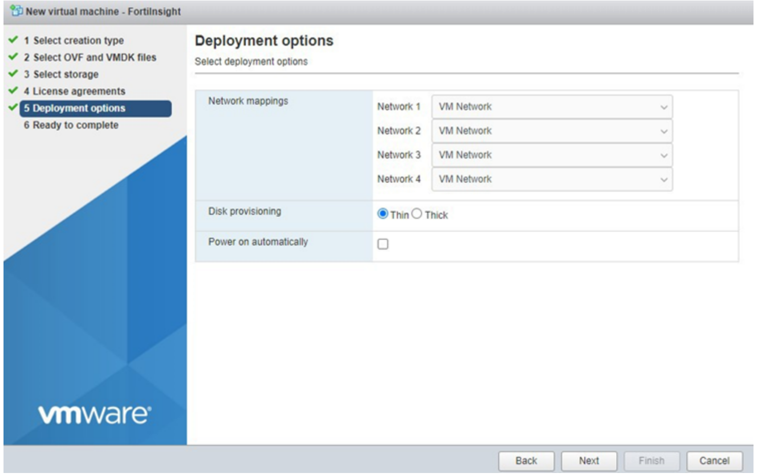
Read and accept the license agreements

```
End User License Agreement for FortiInsight Virtual Appliance

NOTICE  TO ALL  USERS:  PLEASE READ  THE TERMS  AND  CONDITIONS OF  THE
LICENSE AGREEMENT CAREFULLY. FORTINET, INC.  IS WILLING TO LICENSE THIS
SOFTWARE TO YOU ONLY ON THE CONDITION  THAT YOU ACCEPT ALL OF THE TERMS
OF THIS LICENSE AGREEMENT. BY  CLICKING THE ACCEPT BUTTON OR INSTALLING
THE SOFTWARE, YOU (EITHER AN INDIVIDUAL  OR A SINGLE ENTITY) AGREE THAT
THIS AGREEMENT IS ENFORCEABLE LIKE  ANY WRITTEN CONTRACT SIGNED BY YOU.
IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT
ACCEPT  THE TERMS  OF THIS  LICENSE AGREEMENT  AND DO  NOT INSTALL  THE
SOFTWARE. IF  YOU PURCHASED THE  SOFTWARE ON TANGIBLE MEDIA  (e.g., CD)
WITHOUT THE  OPPORTUNITY TO REVIEW THIS  LICENSE AND YOU DO  NOT ACCEPT
THIS  LICENSE AGREEMENT,  YOU MAY  OBTAIN A  REFUND OF  THE AMOUNT  YOU
ORIGINALLY PAID IF YOU: (A) DO NOT  USE THE SOFTWARE AND (B) RETURN IT,
WITH PROOF OF PAYMENT, WITHIN THIRTY  (30) DAYS OF THE PURCHASE DATE TO
THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA)  is an agreement between you and
Fortinet, Inc.  ("Fortinet"), which governs  your use of  this software
product.  A  software  license  and  a license  key  or  "unlock  code"
("Software License"), issued  to a designated user only  by Fortinet or
its  authorized agents   is required  for  each computer  on which  the
```

Agree to the license terms

7. Select the appropriate network mappings, disk provisioning, and power on options for your deployment, and click **Next**.

It's best to provision 'Thick Provisioning' as this will provide the best performance for your FortiInsight-VM.



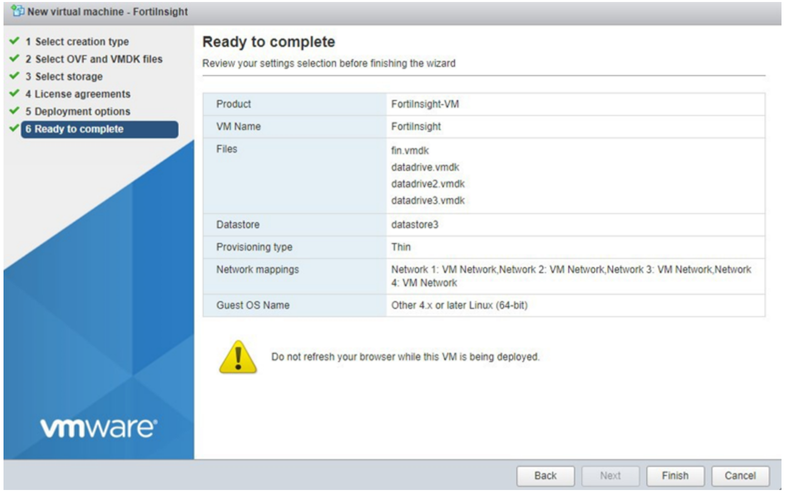
Deployment options

Select deployment options

Network mappings	Network 1	VM Network
	Network 2	VM Network
	Network 3	VM Network
	Network 4	VM Network
Disk provisioning	● Thin ○ Thick	
Power on automatically	□	

Choose deployment options for the FortiInsight Virtual Appliance Image

8. Review the summary of your VM settings, and click **Finish**.



Ready to complete

Review your settings selection before finishing the wizard

Product	FortiInsight-VM
VM Name	FortiInsight
Files	fin.vmdk datadrive.vmdk datadrive2.vmdk datadrive3.vmdk
Datastore	datastore3
Provisioning type	Thin
Network mappings	Network 1: VM Network,Network 2: VM Network,Network 3: VM Network,Network 4: VM Network
Guest OS Name	Other 4.x or later Linux (64-bit)

Do not refresh your browser while this VM is being deployed.

Review and deploy the FortiInsight Virtual Appliance Image to VMWare.

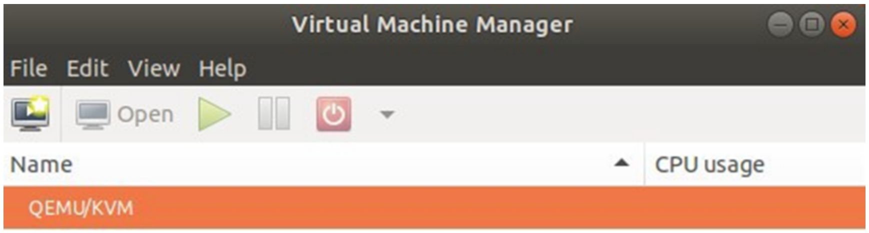
9. Continue with Configure FortiInsight-VM hardware settings on page 20.

Deploying FortiInsight-VM on KVM

Once you have downloaded the out.kvm.zip file and extracted the virtual hard drive image file finkvm.qcow2, you can create the virtual machine in your KVM environment.

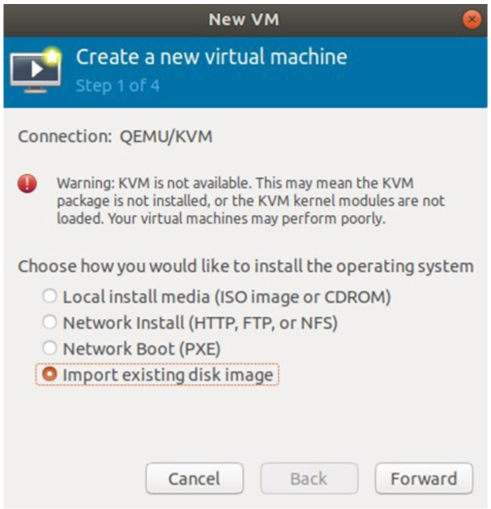
To deploy the FortiInsight-VM virtual machine:

1. Launch **Virtual Machine Manager** on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, select **Create a new virtual machine**.



Create a new FortiInsight Virtual Appliance

3. Select **Import existing** disk image and select Forward.



New VM

Create a new virtual machine

Step 1 of 4

Connection: QEMU/KVM

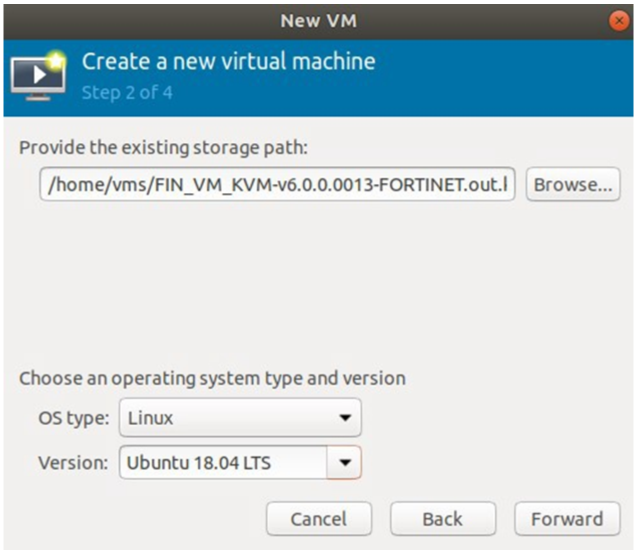
Warning: KVM is not available. This may mean the KVM package is not installed, or the KVM kernel modules are not loaded. Your virtual machines may perform poorly.

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

Import an existing disk image for FortiInsight

4. Select Browse. If you saved the finkvm.qcow2 file to */var/lib/libvirt/images*, it will be visible on the right. If you saved it somewhere else on your server, select **Browse Local**, find it, and select **Choose Volume**.
5. Select the **OS type** and **Version** you are running (in this case Linux Ubuntu 16.04), and select **Forward**.



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

/home/vms/FIN_VM_KVM-v6.0.0.0013-FORTINET.out.l

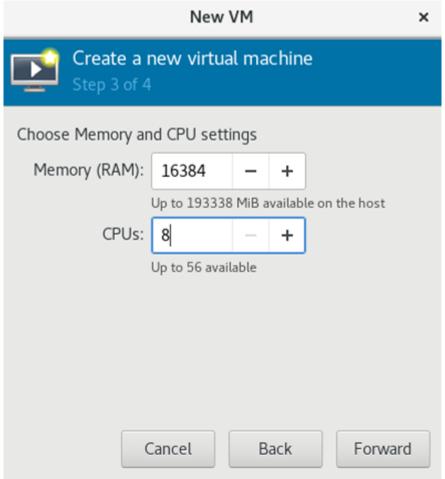
Choose an operating system type and version

OS type: Linux

Version: Ubuntu 18.04 LTS

Select required operating system

6. Specify the amount of memory and number of CPUs to allocate to this virtual machine. Select **Forward**.



New VM

Create a new virtual machine
Step 3 of 4

Choose Memory and CPU settings

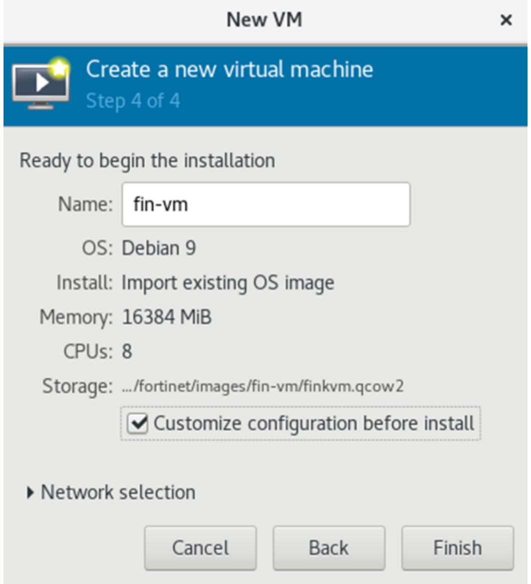
Memory (RAM): 16384

Up to 193338 MiB available on the host

CPUs: 8

Up to 56 available

7. Enter a suitable name for the FortiInsight-VM. Check ‘Customize configuration before install’ and click **Finish**.



New VM

Create a new virtual machine
Step 4 of 4

Ready to begin the installation

Name: fin-vm

OS: Debian 9

Install: Import existing OS image

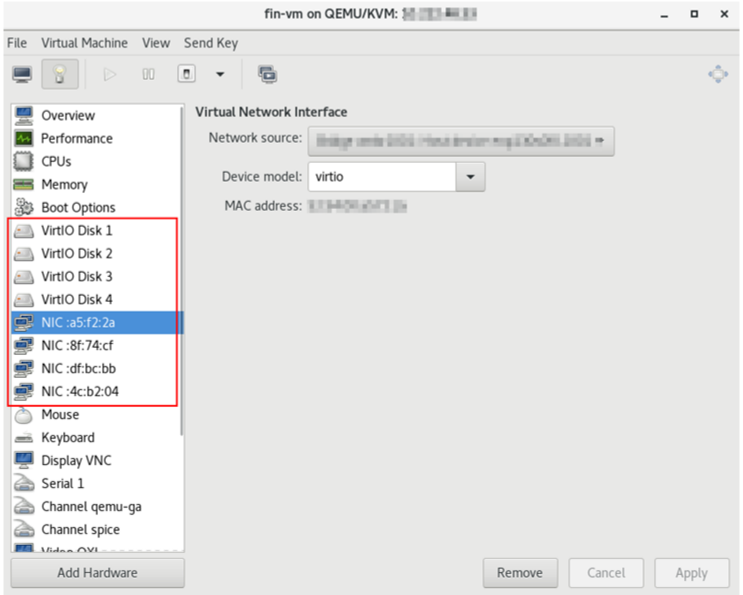
Memory: 16384 MiB

CPUs: 8

Storage: .../fortinet/images/fin-vm/finkvm.qcow2

☑ Customize configuration before install

8. Add the three additional data disks datadrive.qcow2, datadrive2.qcow2 and datadrive3.qcow2 in order. Add three additional vNICs, and associate the first vNIC with an appropriate virtual network. Select **Apply**.



Virtual Network Interface

Network source: [redacted]

Device model: virtio

MAC address: [redacted]

9. Continue with Configure FortiInsight-VM hardware settings on page 20.

Configure FortiInsight-VM hardware settings

Before powering on your FortiInsight-VM you must configure the virtual memory, virtual CPU, and virtual disks (VMDK) configuration, and map the virtual network adapters.

The instructions below are for VMware deployments. Refer to the hypervisor vendors documentation for instructions on how to perform similar configuration changes on KVM and Hyper-V.

These settings cannot be configured inside FortiInsight-VM, and must be configured in the VM environment. Some settings cannot be reconfigured after you power on the virtual appliance.

Resizing the virtual disk (vDisk)

If you configure the virtual appliance’s storage repository to be internal (i.e. local, on its own vDisk), resize the vDisk before powering on.

The FortiInsight-VM package that you downloaded includes pre-sized VMDK (Virtual Machine Disk Format) files of 1GB for disk 1 (for the OS) and 60GB for disk 2, and 3, and 4 data, which is large enough for most trial deployments.

Resize the vDisk before powering on the virtual machine.

The maximum disk size can be affected by the VM datastore block size. Consult VMware documentation for details. See http://communities.vmware.com/docs/DOC-11920.

Consider also that, depending on the size of your organization's network, you might require more or less storage for the FortiInsight data storage layer for anomalies, alerts and event telemetry.

To resize the vDisk:

1. In the VMware vSphere Client, right-click the name of the virtual appliance, and select **Edit Settings**. The Virtual Machine Properties page is displayed.
2. Select the Hardware tab and select **Hard Disk 2**.
3. Select **Remove**.
4. Select Add. The **Add Hardware** page is displayed.
5. In the list of device types, select **Hard Disk** and select **Next**.
6. Select **Create a new virtual disk** and select **Next**.
7. In **Disk Size**, enter the size of the vDisk in GB and select **Next**.
8. Select the bottom option in Virtual Device Node, select IDE (0:1) from the drop-down list, then select **Next**.
9. Select **Finish** to close the **Add Hardware** page and then select OK to save the settings to Virtual Machine Properties.
10. Repeat for Hard Disk 3, and 4.

All disks must be the same size, and Hard Disk 1 must not be resized.

Configuring the number of virtual CPUs (vCPUs)

By default, the virtual appliance is configured to use 4 vCPUs, which is sufficient for small deployments. Additional CPUs should be provisioned for larger deployments. FortiInsight-VM is not restricted to how many vCPUs can be configured so you can increase the number according to your requirements (e.g., you can allocate 2, 4, 8, 12, or 16 vCPUs).

Configuring virtual RAM (vRAM) limit

FortiInsight-VM comes pre-configured to use vRAM, which must be increased to at least 16GB before powering on FortiInsight. FortiInsight-Vm is not restricted to how much vRAM that can be assigned, so you can increase the number to your requirements (e.g 32GB, 64GB, 96GB, 128GB)

Mapping the virtual NICs (vNICs) to physical NICs

Assign the FortiInsight-VM vNICs to an appropriate virtual network. Only port 1 is used for FortiInsight communication.

Power on your FortiInsight-VM

You can now proceed to power on your FortiInsight-VM. Select the name of the FortiInsight-VM you deployed in the inventory list and select Power on the virtual machine in the **Getting Started** tab. Optionally, you can select the name of the FortiInsight-VM you deployed, right-click and select **Power > Power On**.

Initial configuration

Before you can connect to the FortiInsight-VM GUI you must configure basic network settings via the console tab in your vSphere client. Once configured, you can connect to the FortiInsight-VM GUI and upload the FortiInsight-VM license file that you downloaded from FortiCloud.

FortiInsight-VM console access

To enable GUI access to the FortiInsight-VM you must configure basic network settings of the FortiInsight-VM in the vSphere Client Console tab.

To configure basic network settings in FortiInsight-VM:

1. In the Inventory list, select the FortiInsight-VM that you deployed. In the Getting Started tab select **Power** on the virtual machine. Optionally, you can right-click the FortiInsight-VM, and select **Power > Power On**.
2. Select the **Console** tab. The Console window appears.
3. At the FortiInsight-VM login prompt enter the username **admin** and password.

Username	admin
Password	<blank>

   - You will be asked to reset the default password on first login.
4. The default **Port1** IP address is set to `192.168.1.99/24`. You can change this IP address with the following CLI command:

```
config system interface
   edit port1
      set ip <address_ipv4/netmask>
end
```

5. You can configure the static route for the default gateway using the following CLI command:

```
config router static
   edit 0
      set device port1
      set dst <destination_ipv4/netmask>
      set gateway <router_ipv4>
end
```

Connect to the FortiInsight-VM GUI

Once you have configured the port1 IP address, network mask, and default gateway, launch a web browser and enter the IP address you configured for port1.

Verify and accept the certificate, either permanently (the web browser will not display the self-signing warning again) or temporarily. You cannot log in until you accept the certificate.

For details on accepting the certificate, see the documentation for your web browser.

At the login page, enter the user name admin and password and select Login. This password will be the same as that set during the initial CLI configuration.