

FortiDeceptor VM - Install Guide for KVM

Version 6.0.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



September 06, 2024

FortiDeceptor VM 6.0.0 Install Guide for KVM

50-600-809433-20240906

TABLE OF CONTENTS

Change Log	4
About FortiDeceptor VM on KVM	5
Licensing	5
Preparing for deployment	7
Minimum system requirements	7
CPU, network, memory and storage	7
Registering your FortiDeceptor VM	8
Editing FortiDeceptor VM IP addresses	8
Downloading deployment packages	9
Deployment package for KVM	9
Deployment	11
Deploying FortiDeceptor VM on KVM	11
Creating the virtual machine	11
Configuring initial settings	16
Enabling GUI access	16
Connecting to the GUI	16
Uploading the license file	17
Installing the Windows VM package	17
Activating Deception VMs	17
Configure the FortiDeceptor VM	19

Change Log

Date	Change Description
2024-07-16	Initial release.
2024-09-06	Added Minimum system requirements on page 7.

About FortiDeceptor VM on KVM

FortiDeceptor VM is a 64-bit virtual appliance version of FortiDeceptor. It is deployed in a virtual machine environment. Once the virtual appliance is deployed and set up, you can manage FortiDeceptor VM via its GUI in a web browser on your management computer.

This document provides information about deploying a FortiDeceptor VM in Linux KVM server environments.

This includes how to configure the virtual hardware settings of the virtual appliance. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For that information, see the [FortiDeceptor Administration Guide](#) in the [Fortinet Document Library](#).

Licensing

Fortinet offers the FortiDeceptor VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. For information on purchasing a FortiDeceptor VM license, contact your Fortinet Authorized Reseller, or visit https://www.fortinet.com/how_to_buy/.

When configuring your FortiDeceptor VM, ensure that you configure hardware settings as outlined in the following table and consider future expansion. Contact your Fortinet Authorized Reseller for more information.

Technical Specification	Details
Kernel Virtual Machine (KVM)	Linux Kernel 5.15 and lower have been tested. Higher versions are supported but are not tested.
Virtual CPUs (min / max)	12 / Unlimited*
Virtual Network Interfaces	6
Virtual Memory (min / max)	16GB / Unlimited**
Virtual Storage (min / max)	200GB / 16TB***



* Fortinet recommends that the number of virtual CPUs is two plus the number of Deception VMs when each Deception VM requires 2vCPU.

** Fortinet recommends that the size of virtual memory is 4GB plus 2GB for every Deception VM clone.

In addition, please adjust the requirements above if a custom decoy uses more than the default (2 vCPU/2G RAM).

*** Fortinet recommends that the size of virtual storage is 1TB for production environment.

For more information, see the FortiDeceptor product data sheet available on the Fortinet web site, <https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiDeceptor.pdf>.

After placing an order for FortiDeceptor VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiDeceptor VM with Customer Service & Support at <https://support.fortinet.com>.

Upon registration, you can download the license file. You will need this file to activate your FortiDeceptor VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded and validated, the CLI and GUI will be fully functional.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- [Minimum system requirements on page 7](#)
- [Registering your FortiDeceptor VM on page 8](#)
- [Deployment package for KVM on page 9](#)
- [Downloading deployment packages on page 9](#)

Minimum system requirements

Prior to deploying the FortiDeceptor VM virtual appliance, KVM must be installed and configured.

The installation instructions for FortiDeceptor VM assume you are familiar with your VM server and terminology.



Upgrade to the latest, stable update and patch release for your virtual environment.



FortiDeceptor VM has specific CPU requirements: Intel Virtualization Technology (VT-x/EPT) or AMD Virtualization (AMD-V/RVI).
Enter the BIOS to enable Virtualization Technology and 64-bit support.
Detailed information can be found at <https://communities.vmware.com/docs/DOC-8970>.

Ensure the following prerequisites are met before installing FortiDeceptor VM:

- A compatible Linux distribution, such as Ubuntu 16.04 with Kernel 4.6.7 and later and the qemu-kvm 2.5 and later packages, or CentOS 7.2 with Kernel 4.1.12 and later and the qemu-kvm 2.3 and later packages.
- virt-manager is installed on the management computer.

CPU, network, memory and storage

The following are the minimum system requirements for deploying decoys with FortiDeceptor VM for KVM:

Technical Specification	Details
Kernel Virtual Machine (KVM)	Linux Kernel 5.15 and lower have been tested. Higher versions are supported but are not tested.
Virtual CPUs (min / max)	4/ Unlimited
Virtual Network Interfaces	2-6

Technical Specification	Details
Virtual Memory (min / max)	8GB / Unlimited
Virtual Storage (min / max)	HDD 500GB/ 16TB

Registering your FortiDeceptor VM

To obtain the FortiDeceptor VM license file, you must first register your FortiDeceptor VM with [Fortinet Customer Service & Support](#).

To register your FortiDeceptor VM:

1. Log into the Fortinet Customer Service & Support portal using an existing support account, or select *Create an Account* to create a new account.
2. In the toolbar, select *Asset > Register/Renew*. The *Registration Wizard* opens.
3. Enter the registration code from the FortiDeceptor VM License Certificate that was emailed to you, then select *Next*. The *Registration Info* page is displayed.
4. Enter your support contract number, product description, Fortinet Partner, and IP address in the requisite fields, then select *Next*.



As a part of the license validation process, FortiDeceptor VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiDeceptor VM's IP address has been changed, the FortiDeceptor VM must be rebooted in order for the system to validate the change and operate with a valid license.



The [Customer Service & Support](#) portal currently does not support IPv6 for FortiDeceptor VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

5. On the *Fortinet Product Registration Agreement* page, select the check box to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
6. The verification page displays the product entitlement. Select the check box to indicate that you accept the terms then select *Confirm* to submit the request.
7. From the *Registration Completed* page, you can download the FortiDeceptor VM license file, select *Register More* to register another FortiDeceptor VM, or select *Finish* to complete the registration process. Select *License File Download* to save the license file (.lic) to your management computer. For instructions on uploading the license file to your FortiDeceptor VM via the GUI, see [Uploading the license file on page 17](#).

Editing FortiDeceptor VM IP addresses

To edit the FortiDeceptor VM IP address:

1. In the toolbar, select *Asset > Manage/View Products* to open the *View Products* page.
2. Select the FortiDeceptor VM serial number to open the *Product Details* page.

3. Click *Edit* to change the description, partner information, and IP address of your FortiDeceptor VM from the *Edit Product Info* page.
4. Enter the new IP address, then select *Save*.



You can change the IP address five (5) times on a regular FortiDeceptor VM license. There is no restriction on a full evaluation license.

5. Select *License File Download* to save the license file (.lic) to your management computer. For instructions on uploading the license file to your FortiDeceptor VM via the GUI, see [Uploading the license file on page 17](#).

Downloading deployment packages

Firmware images FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention, and each firmware image is specific to the device model.



You can download the *FortiDeceptor Release Notes* and FortiDeceptor and Fortinet core MIB files from this directory.



Download the .out file to upgrade your existing FortiDeceptor VM installation.

To download the firmware package:

1. Log in to the Fortinet Customer Service & Support portal at <https://support.fortinet.com>.
2. From the toolbar, select *Download > Firmware Images* to open the *Firmware Images* page.
3. Select *FortiDeceptor* from the *Select Product* dropdown list, then select *Download*.
4. Browse to the directory for the version that you want to download.
5. Download the firmware image and release notes to your management computer.
6. Extract the contents of the package to a new folder on you management computer.

Deployment package for KVM

FortiDeceptor VM deployment packages are included with firmware images on the [Customer Service & Support site](#).

Image File	Description
FDC_VM-v500-build0xxx-FORTINET.out	Download this firmware image to upgrade your existing FortiDeceptor VM installation.
FDC_VM-v500-build0xxx-FORTINET.out.kvm.zip	Download this package for a new FortiDeceptor VM installation on KVM.

The `out.kvm.zip` file contains:

- `image.out.qcow2`: The FortiDeceptor VM firmware.
- `datadrive.qcow2`: The data drive.
- `fdc-kvm.sh`: The installation script for easy installation.

Deployment

Before deploying FortiDeceptor VM, install and configure the VM platform so that it is ready to create virtual machines. The installation instructions for FortiDeceptor VM assume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example since you can use different ways to create a virtual machine, such as using command line tools, APIs, or alternative graphical user interface tools.

Before starting your FortiDeceptor VM appliance for the first time, you might need to adjust virtual disk sizes, network settings, and CPU configuration. The first time you start FortiDeceptor VM, you only have access through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiDeceptor VM GUI. For more information, see [Enabling GUI access on page 16](#).



Linux KVM server deployments have many variants with different Linux distributors. The FDC deployment is just to provide generic information instead of a step-by-step one like the VMware deployment guide.

Deploying FortiDeceptor VM on KVM

Once you have downloaded the `FDC_VM-v5xx-build0xxx-FORTINET.out.kvm.zip` file and extracted files, you can create the virtual machine in your KVM environment.

The Linux host must have at least two interfaces connected to different networks. One interface will be used by the FortiDeceptor VM Port1 as a management port.

Creating the virtual machine

You can create the virtual machine by executing the `fdc-kvm.sh` script in shell. Running `fdc-kvm.sh` to install FortiDeceptor VM for KVM is recommended. This is also the easiest way to create the virtual machine. This section describes how to manually create a virtual machine.



Important:

When successful the `fdc-kvm.sh` script will automatically create the FDC VM. However, if the required kernel module does not exist or is not configured properly, the `fdc-kvm.sh` script will report *kvm nested is not enabled!* Then, you will need to manually enable the feature by following the instruction in [To enable nested virtualization](#) and then run the script again.

The steps may vary between different Linux distributors (Ubuntu, Debian, RedHat, SuSE, etc.).

To enable nested virtualization

1. Check if nested virtualization is supported:

Intel processors	Check the <code>/sys/module/kvm_intel/parameters/nested</code> file.
AMD processors	Check the <code>/sys/module/kvm_amd/parameters/nested</code> file.

If you see `1` or `Y`, nested virtualization is supported; if you see `0` or `N`, nested virtualization is not supported.

2. Enable nested virtualization for Intel processors:

- a. Shut down all running VMs and unload the `kvm_probe` module:

```
sudo modprobe -r kvm_intel
```

- b. Activate the nesting feature:

```
sudo modprobe kvm_intel nested=1
```

- c. Nested virtualization is enabled until the host is rebooted. To enable it permanently, add the following line to the `/etc/modprobe.d/kvm.conf` file:

```
options kvm_intel nested=1
```

3. Enable nested virtualization for AMD processors:

- a. Shut down all running VMs and unload the `kvm_amd` module:

```
sudo modprobe -r kvm_amd
```

- b. Activate the nesting feature:

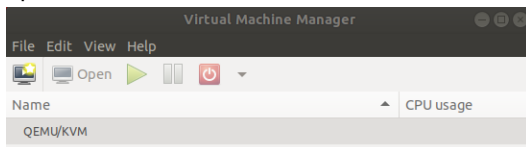
```
sudo modprobe kvm_amd nested=1
```

- c. Nested virtualization is enabled until the host is rebooted. To enable it permanently, add the following line to the `/etc/modprobe.d/kvm.conf` file:

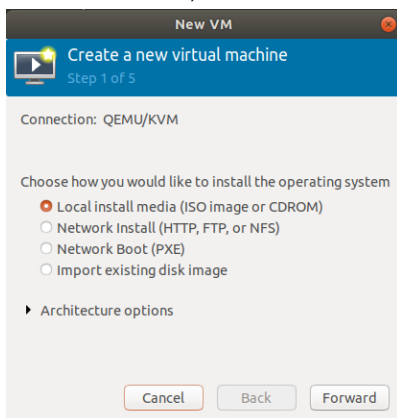
```
options kvm_amd nested=1
```

To create the virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server. The *Virtual Machine Manager* home page opens.

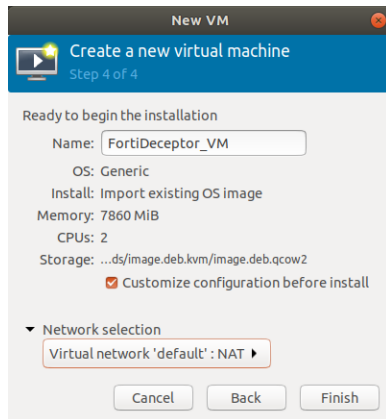


2. From the toolbar, click *Create a new virtual machine*.

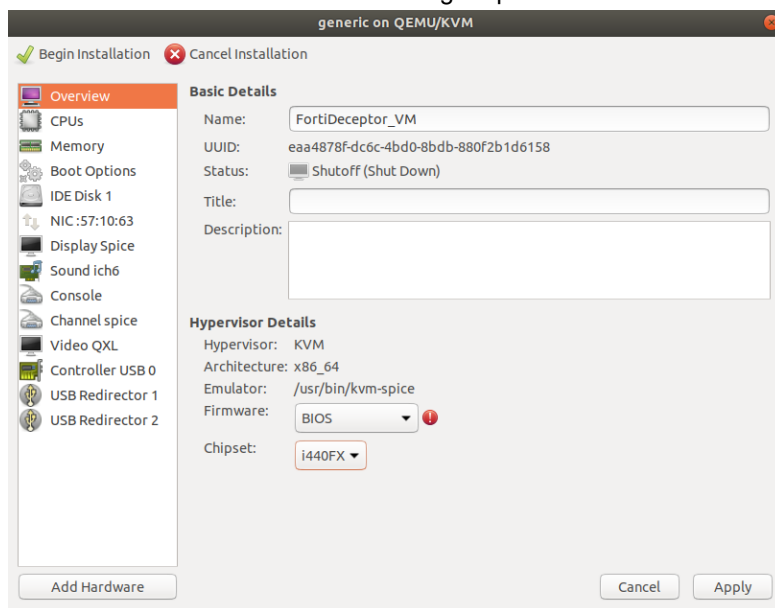


3. Select *Import existing disk image*, then click *Forward*.

4. Enter the full path to extract the `image.out.qcow2` file or click **Browse**. If you copied the file to `/var/lib/libvirt/images`, it will be shown on the right. If you saved it elsewhere on the server, select **Browse Local** to find it.
5. Click **Forward**.
6. Specify the amount of memory and the number of CPUs to allocate to this VM, then click **Forward**.
A minimum of 8GB of memory and two CPUs are required for the VM. Fortinet recommends that the number of CPU cores be four more than the number of Deception VMs, and 3GB of RAM per Deception VM.
 - a. Click **Forward** and set the name of your VM.
 - b. Select **Customize Configuration before install**.
 - c. Select the correct interface for the **Network Selection** field.

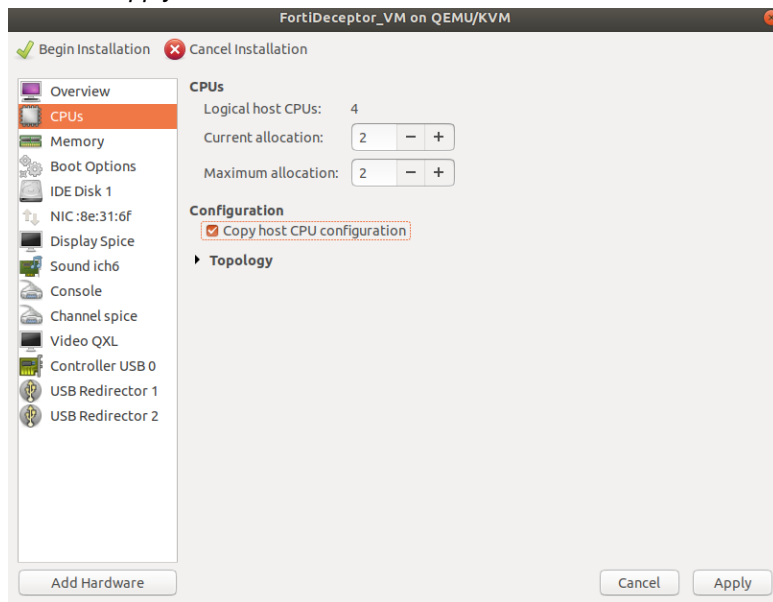


7. Click **Finish**. The Virtual Machine Manager opens.



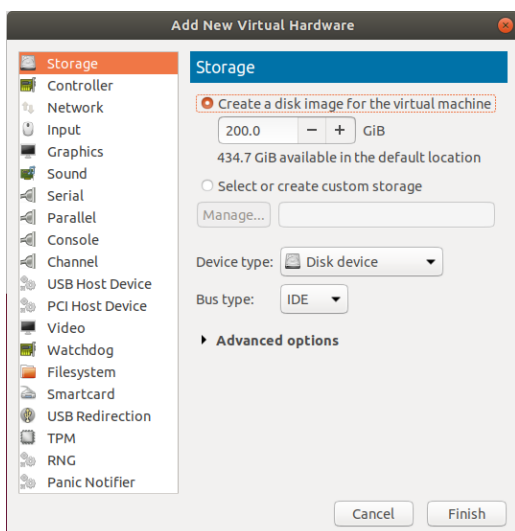
Before powering on your FortiDeceptor VM, you must configure the CPUs to copy the host configuration. You must also add a local hard drive of at least 200GB and add at least two more network interfaces.

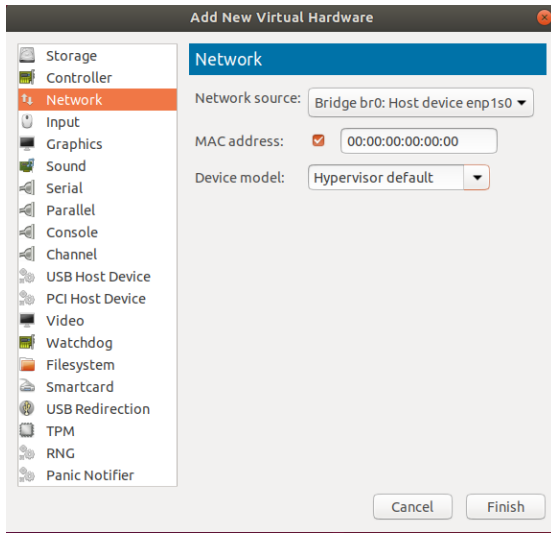
8. In the Virtual Machine Manager, set the following options:
 - a. From the list, select *CPUs*.
 - b. Select the *Copy host CPU configuration* check box.
 - c. Click *Apply*.



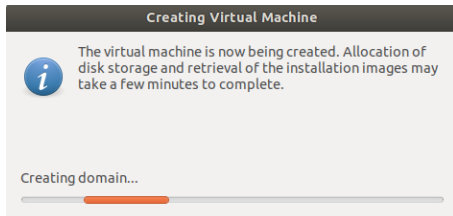
9. Add a second hard drive.
 - a. Click *Add Hardware > Storage*.
 - b. Configure the hard drive.

Option	Description
Create a disk image for the virtual machine	Enter <i>200</i> or a larger number in the disk size field, and then click <i>Finish</i> . Fortinet recommends making the virtual disk 1TB or larger. The disk is created and added to the hardware list as <i>IDE Disk 2</i> .
Select or create custom storage	a. Enter the full path to extract the <code>image.out.qcow2</code> file or click <i>Browse</i> . Click <i>Finish</i> .



10. Add more network interfaces:**a. Click *Add Hardware* > *Network*.****b. Edit the settings as required, then click *Finish* to create the interface.****c. Repeat these steps to create a third interface.**

FortiDeceptor VM requires a minimum of two network adapters to function and supports up to six. You can configure network adapters to connect to a virtual switch or to network adapters on the host computer.

11. Click *Begin Installation* to create the VM.

The FortiDeceptor VM is created and started. For information on configuring your FortiDeceptor VM, see [Configuring initial settings on page 16](#).

Configuring initial settings

Before you can connect to the FortiDeceptor VM, you must configure basic configuration via the CLI console. Once configured, you can connect to the FortiDeceptor VM GUI and upload the FortiDeceptor VM license file that you downloaded from the [Customer Service & Support](#) portal.

The following topics are included in this section:

- [Enabling GUI access](#)
- [Connecting to the GUI](#)
- [Uploading the license file](#)
- [Installing the Windows VM package](#)
- [Activating Deception VMs](#)

Enabling GUI access

To enable GUI access to the FortiDeceptor VM, you must configure the port1 IP address and network mask of the FortiDeceptor VM.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiDeceptor VM and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiDeceptor VM login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Configure the port1 IP address and netmask by using the following command:

```
set port1-ip <ip address>/<netmask>
```
4. Configure the static route for the default gateway by using the following command:

```
set default-gw <default gateway>
```



The Customer Service & Support portal does not currently support IPv6 for FortiDeceptor VM license validation. You must specify an IPv4 address in both the support portal and the port management interface.

Connecting to the GUI

Once you have configured the port1 IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. By default the GUI is accessible via HTTPS. At the login page, enter the user name *admin* and no password, then select *Login*.

Uploading the license file

Before using the FortiDeceptor VM, you must enter the license file that you downloaded from the [Customer Service & Support](#) portal upon registration.

To upload the license file:

1. Log into the FortiDeceptor VM GUI, and find the *System Information* widget on the dashboard.
2. In the *VM License* field, select *Upload License*. The *VM License Upload* page opens.
3. Select *Browse*, locate the VM license file (.lic) on your computer, then select *OK* to upload the license file. A reboot message will be shown, then the FortiDeceptor VM system will reboot and load the license file.
4. Refresh your browser and log back into the FortiDeceptor VM (username *admin*, no password). The VM registration status appears as valid in the *System Information* widget once the license has been validated.



As a part of the license validation process, FortiDeceptor VM compares its IP address with the IP information in the license file. If a new license has been imported or the FortiDeceptor's IP address has been changed, the FortiDeceptor VM must be rebooted in order for the system to validate the change and operate with a valid license.



If the IP address in the license file and the IP address configured in the FortiDeceptor VM do not match, you will receive an error message when you log back into the VM. If this occurs, you must change the IP address in the [Customer Service & Support](#) portal to match the management IP and re-download the license file. To change the management IP address, see [Editing FortiDeceptor VM IP addresses on page 8](#)

Installing the Windows VM package

To complete the installation, the VM package must be downloaded and installed either manually or automatically, and then activated.

For details, see the *Deploying FortiDeceptor in offline or air-gapped networks* section in the [FortiDeceptor Administration Guide](#) in the [Fortinet Document Library](#).

Activating Deception VMs

The Deception VMs must be activated before they can be used on the network.

To activate Deception VMs:

1. Download the Key license file from the [Fortinet Customer Service & Support](#) portal.
2. Log in to the FortiDeceptor VM GUI and find the *System Information* widget on the dashboard.
3. In the *Firmware License* field, select *Upload License*. The *Firmware License Upload* pane opens.
4. Browse to the license file on the management computer then click *Submit*. The Deception VM will reboot.

Once the license for the Deception VM is activated, the network must be set up with Internet access to activate the Windows Operating System license for the Windows Deception VM. Ubuntu Operating System for the Linux Deception VM does not need activation.

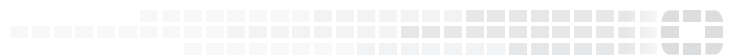
For details, see the *Deploying FortiDeceptor in offline or air-gapped networks* section in the [FortiDeceptor Administration Guide](#) in the [Fortinet Document Library](#).

Configure the FortiDeceptor VM

Once the FortiDeceptor VM license has been validated, you can configure your device. For more information on configuring your FortiDeceptor VM, see the [FortiDeceptor Administration Guide](#) in the [Fortinet Document Library](#).



FORTINET®



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.