FortiDeceptor VM - Install Guide for VMware

Version 4.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE 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

December 29, 2021
FortiDeceptor VM 4.0 Install Guide for VMware
50-400-733528-20211229

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-07-30	Initial release.
2021-10-26	Updated Deployment package for VMware on page 8.
2021-12-29	Added Virtual Switch Configuration on page 16.

About FortiDeceptor VM on VMware

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 VMware VSphere Hypervisor (ESX/ESCi) and VMware vShpere Client 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
Hypervisor Support	VMware ESXi version 5.1, 5.5, or 6.0 and later Kernel Virtual Machine (KVM)
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 7
- Deployment package for VMware on page 8
- Downloading deployment packages on page 9

Minimum system requirements

Prior to deploying the FortiDeceptor VM virtual appliance, VMware vSphere Hypervisor 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:

- The VMware vSphere ESXi hypervisor software must be installed and configured.
  - ESXi version 5.1: Hardware version 9
  - ESXi version 5.5: Hardware version 9 or 10
  - ESXi version 6.0, 6.5, and 6.7: Hardware version 9, 10, or 11
- The VMware vSphere client is installed on the management computer.

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 19.

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 19.

Deployment package for VMware

FortiDeceptor VM deployment packages are included with firmware images on the Customer Service & Support site.

- FDC_VM-v400-build0xxx-FORTINET.out: Download this firmware image to upgrade your existing FortiDeceptor VM installation.

- FDC_VM-v400-build0xxx-FORTINET.out.ovf.zip: Download this package for a new FortiDeceptor VM installation on ESXi server.

The `.out.ovf.zip` file contains:

- `fdc.vmdk`: The FortiDeceptor VM system hard disk in Virtual Machine Disk (VMDK) format.
- `FortiDeceptor-VM.ovf`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The FortiDeceptor VM log disk in VMDK format

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

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 17.

Deploying FortiDeceptor VM on VMware

When you have downloaded the `FDC_VM-v3xx-build0xxx-FORTINET.out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Before deploying the FortiDeceptor VM, ensure that the following are configured and functioning properly:

- VMware vSphere Hypervisor (ESX/ESXi) software must be installed on a server prior to installing FortiDeceptor VM. Go to http://www.vmware.com/products/vsphere-hypervisor/index.html for installation details.
- VMware vSphere Client must be installed on the computer that you will be using for managing the FortiDeceptor VM.

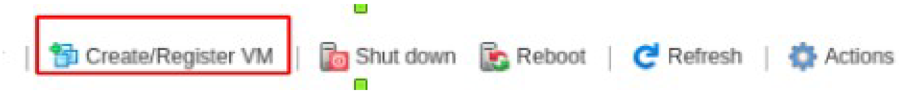
The following topics are included in this section:

- Deploying the OVF file using ESXi web GUI
- Deploying the OVF file using VMware vSphere client
- Configuring hardware settings
- Powering on the virtual machine

Deploying the OVF file using ESXi web GUI

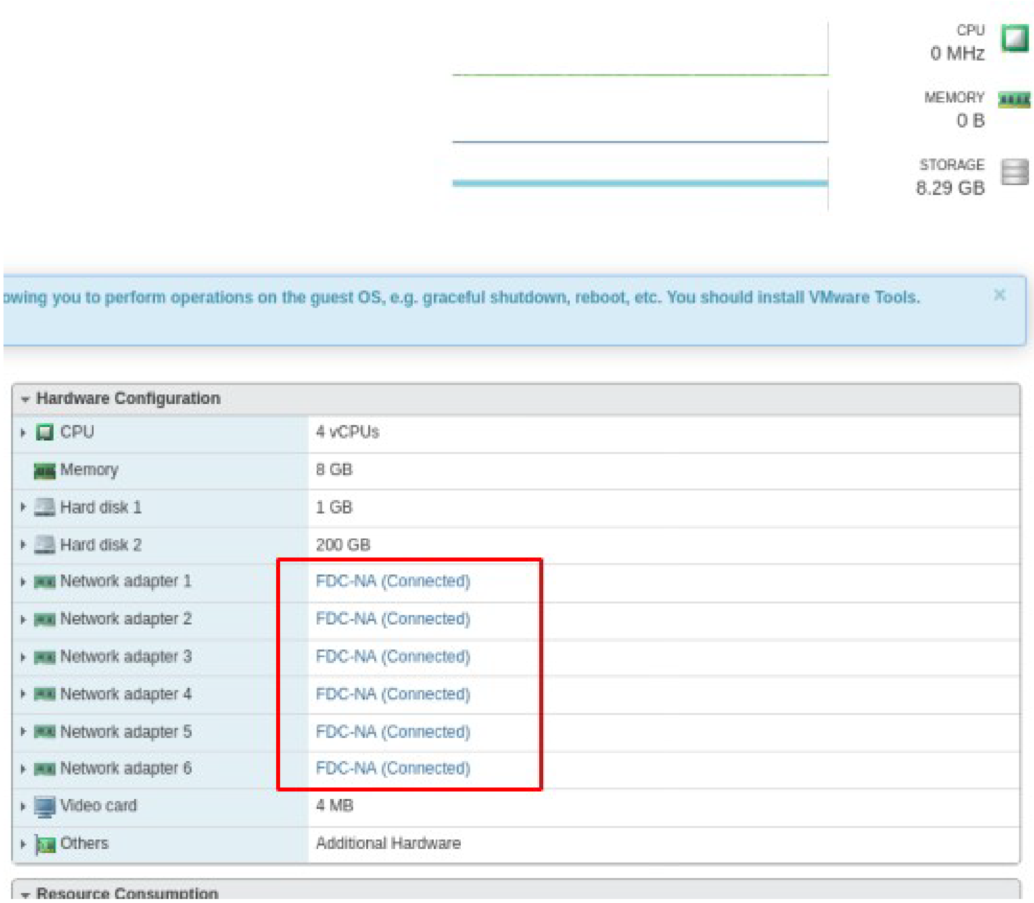
To deploy the OVF file using ESXi web GUI:

1. In a web browser, go to the URL or IP address of the vCenter server or host, and log in.
2. Click *Create/Register VM* to launch the wizard.



3. In the *Select creation type* dialog box, click *Deploy a virtual machine from an OVF or OVA file*. Click *Next*.
4. Enter a name for the VM and then select the OVF and VMDK files. Click *Next*.

5. Select the datastore. Click *Next*.
6. Read and accept the license agreements. Click *Next*.
7. Select one of the following:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks, until the first write takes place to that block during runtime (which includes a full disk format).
   - *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data.
8. Finish creating the VM.
9. Go to the Dashboard and select the VM you created.
10. Select the network adapters you require.
    To use sniffer mode, promiscuous mode must be enabled on a port.



CPU
0 MHz

MEMORY
0 B

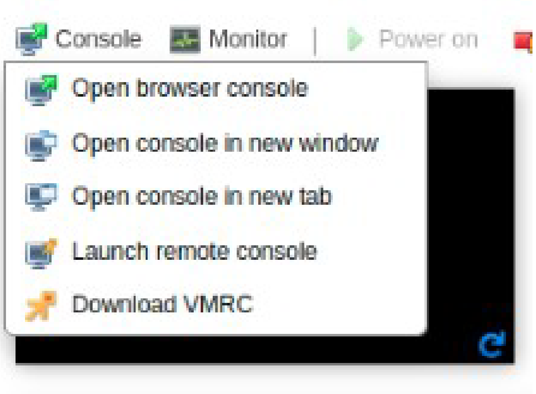
STORAGE
8.29 GB

owing you to perform operations on the guest OS, e.g. graceful shutdown, reboot, etc. You should install VMware Tools.

Hardware Configuration	
CPU	4 vCPUs
Memory	8 GB
Hard disk 1	1 GB
Hard disk 2	200 GB
Network adapter 1	FDC-NA (Connected)
Network adapter 2	FDC-NA (Connected)
Network adapter 3	FDC-NA (Connected)
Network adapter 4	FDC-NA (Connected)
Network adapter 5	FDC-NA (Connected)
Network adapter 6	FDC-NA (Connected)
Video card	4 MB
Others	Additional Hardware

Resource Consumption

11. Use the console to do basic configuration.

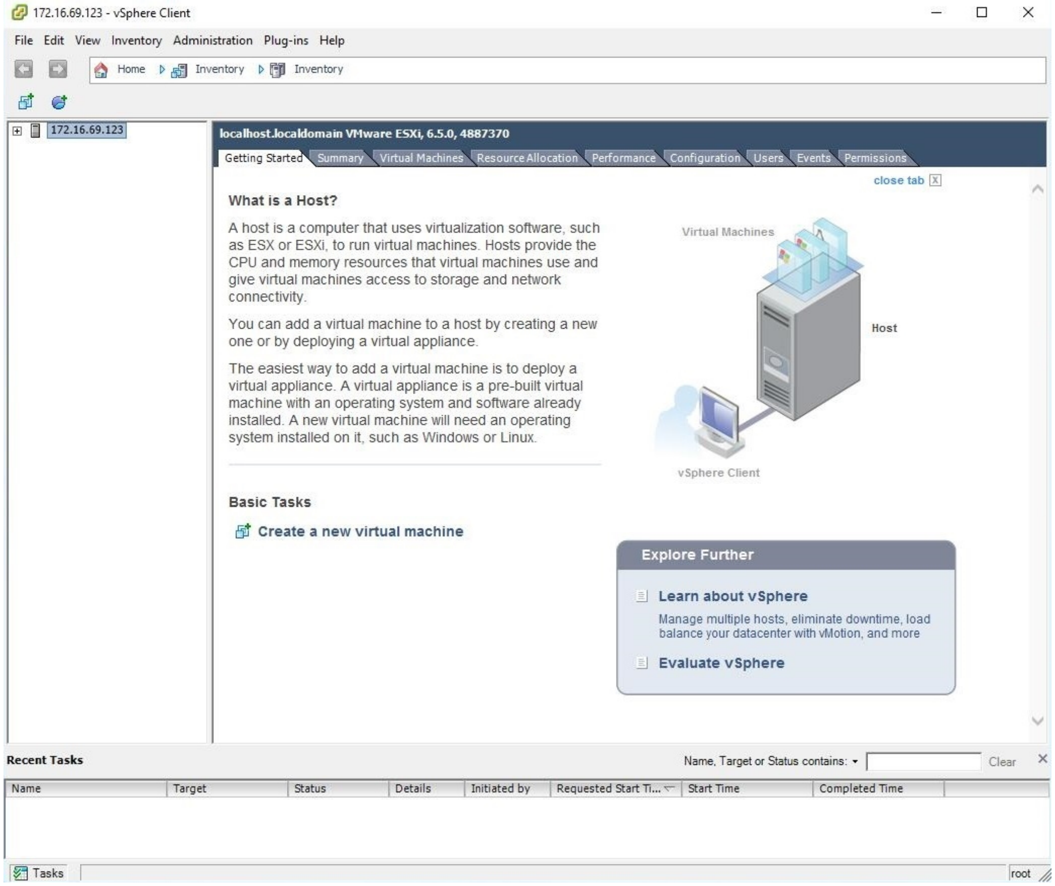


12. Complete the configuration following the instructions in Configuring initial settings on page 17.

Deploying the OVF file using VMware vSphere client

To deploy the OVF file template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then select *Login*. The vSphere client home page opens.


172.16.69.123 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
172.16.69.123
localhost.localdomain VMware ESXi, 6.5.0, 4887370
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Users Events Permissions
close tab
Virtual Machines
Host
vSphere Client

What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

You can add a virtual machine to a host by creating a new one or by deploying a virtual appliance.

The easiest way to add a virtual machine is to deploy a virtual appliance. A virtual appliance is a pre-built virtual machine with an operating system and software already installed. A new virtual machine will need an operating system installed on it, such as Windows or Linux.

Basic Tasks

Create a new virtual machine

Explore Further

Learn about vSphere

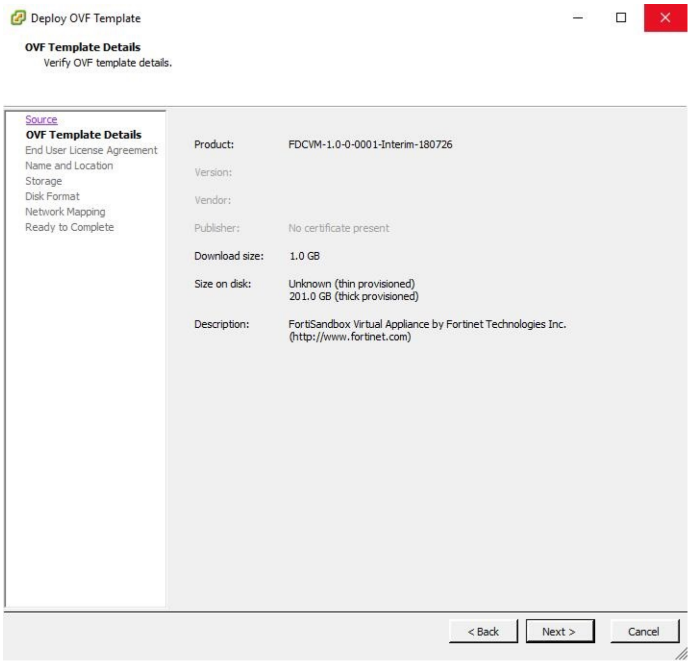
Manage multiple hosts, eliminate downtime, load balance your datacenter with vMotion, and more

Evaluate vSphere

Recent Tasks
Name, Target or Status contains:
Clear
Name Target Status Details Initiated by Requested Start Ti... Start Time Completed Time
Tasks
root

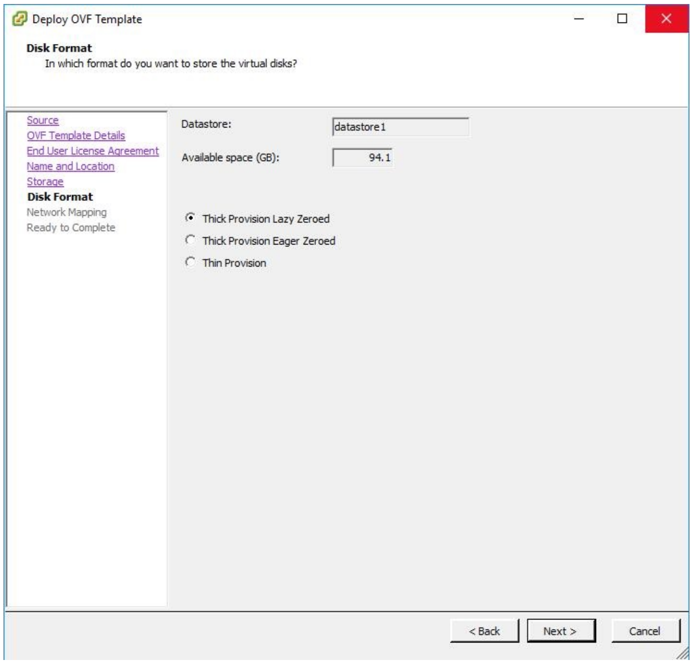
2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard. The OVF Template *Source* page opens.

3. Click *Browse*, locate the OVF file on your computer, then select *Next* to continue. The OVF Template *Details* page opens.



Product: FDCVM-1.0-0-0001-Interim-180726
Version:
Vendor:
Publisher: No certificate present
Download size: 1.0 GB
Size on disk: Unknown (thin provisioned)
201.0 GB (thick provisioned)
Description: FortiSandbox Virtual Appliance by Fortinet Technologies Inc.
(http://www.fortinet.com)

4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select *Next* to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then select *Accept* then *Next* to continue. The OVF Template *Name and Location* page opens.
6. Enter a name for this OVF template. The name can contain up to 80 characters, and it must be unique within the inventory folder. Click *Next* to continue. The OVF Template *Disk Format* page opens.



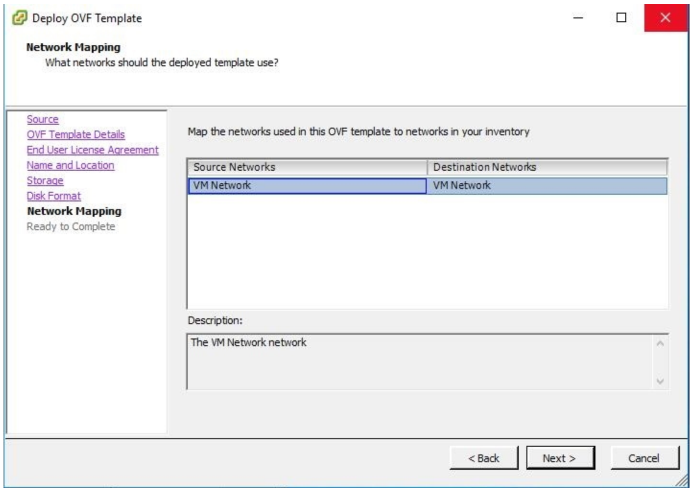
Datastore: datastore1
Available space (GB): 94.1

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

7. Select one of the following:
    - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks, until the first write takes place to that block during runtime (which includes a full disk format).
    - *Thick Provision Eager Zeroed*: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
    - *Thin Provision*: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data.

If you know your environment will expand in the future, it is recommended to add hard disks larger than the 200GB FortiDeceptor VM license requirement and utilize Thin Provision when setting the OVF Template disk format. This will allow your environment to expand as required while not taking up more space in the SAN than is needed.

8. Select *Next* to continue. The OVF Template *Network Mapping* page opens.



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
VM Network	VM Network

Description:

The VM Network network

9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the FortiDeceptor VM. You must set the destination network for this entry to access the device console. Select *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.

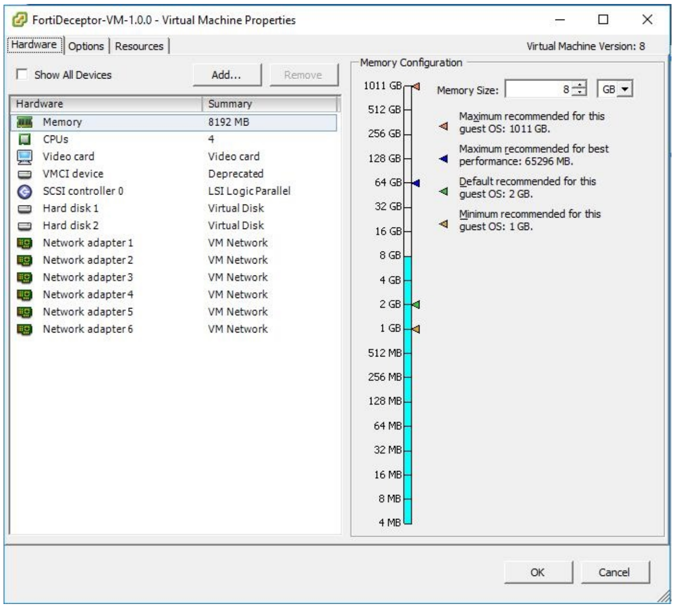
    Ensure that *Power on after deployment* is not enabled. You need to configure the FortiDeceptor VM hardware settings prior to powering on the VM.
11. Select *Finish* to deploy the OVF template. A *Deployment Completed Successfully* dialog box is displayed once the FortiDeceptor VM OVF template wizard has finished.

Configuring hardware settings

Before powering on your FortiDeceptor VM, you must configure the virtual memory, virtual CPU, and virtual disk.

To configure hardware settings:

1. In the vSphere Client, right-click on the FortiDeceptor VM in the left pane, and select *Edit Settings* to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required. 3GB of RAM per Deception VM is recommended.



FortiDeceptor-VM-1.0.0 - Virtual Machine Properties

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Memory Size: 8 GB

Maximum recommended for this guest OS: 1011 GB.

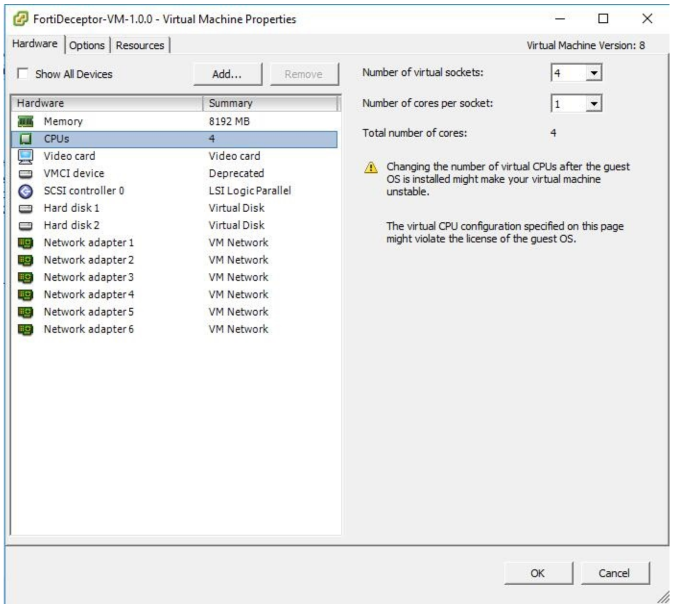
Maximum recommended for best performance: 65296 MB.

Default recommended for this guest OS: 2 GB.

Minimum recommended for this guest OS: 1 GB.

3. Select *CPUs* from the *Hardware* list, then adjust the *Number of virtual sockets* and *Number of cores per socket* as required.

If you need to change the vCPUs after the initial boot, power off FortiDeceptor VM. Fortinet recommends that the number of vCPUs be four more than the number of Deception VMs.



FortiDeceptor-VM-1.0.0 - Virtual Machine Properties

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Number of virtual sockets: 4

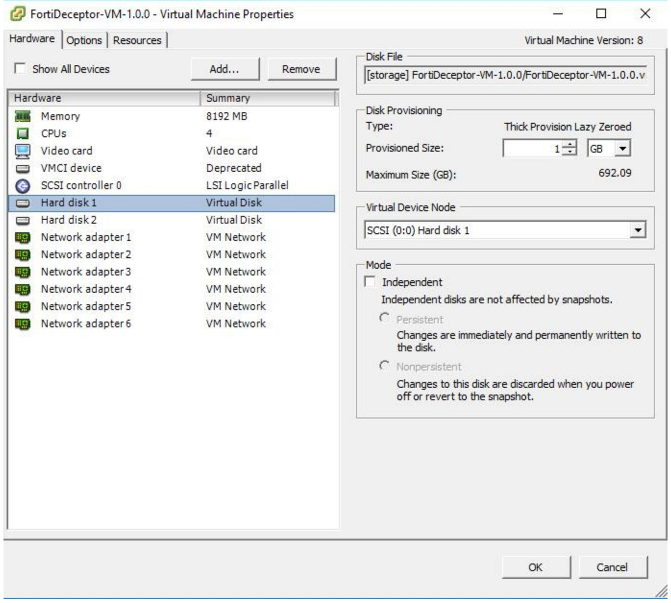
Number of cores per socket: 1

Total number of cores: 4

⚠ Changing the number of virtual CPUs after the guest OS is installed might make your virtual machine unstable.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

4. Select *Hard disk 2*, the data disk, from the *Hardware* list, and configure it as required. Fortinet recommends making the virtual disk 1TB or larger. *Hard disk 1* should not be edited.



FortiDeceptor-VM-1.0.0 - Virtual Machine Properties

Virtual Machine Version: 8

□ Show All Devices

Hardware	Summary
Memory	8192 MB
CPUs	4
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
Hard disk 1	Virtual Disk
Hard disk 2	Virtual Disk
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Network adapter 4	VM Network
Network adapter 5	VM Network
Network adapter 6	VM Network

Disk File

[storage] FortiDeceptor-VM-1.0.0/FortiDeceptor-VM-1.0.0.v

Disk Provisioning

Type: Thick Provision Lazy Zeroed

Provisioned Size: 1 GB

Maximum Size (GB): 692.09

Virtual Device Node

SCSI (0:0) Hard disk 1

Mode

□ Independent

Independent disks are not affected by snapshots.

○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

5. From the *Hardware* list, select a network adapter, then adjust the virtual network mapping as required by your network configuration. To use sniffer mode, promiscuous mode must be enabled on a port.

By default, six bridging virtual network adapters are created and automatically mapped to a port group on a virtual switch (vSwitch) in the virtual server. Each of the network adapters can be used by one of the six network interfaces in the FortiDeceptor VM. The default mappings are appropriate when each of the host's guest virtual machines have their own IP address on your network.

6. Select *OK* to apply your changes.

Virtual Switch Configuration

The virtual switch requires the following configurations to be enabled:

- Promiscuous mode
- MAC address changes
- Forged transmits

For each network connection, we highly recommend creating a new virtual switch and enabling the configurations above.

Powering on the virtual machine

You can now proceed to power on your FortiDeceptor VM.

- In the left pane, select the FortiDeceptor VM, and select *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then select *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power* > *Power On* from the right-click menu.

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:

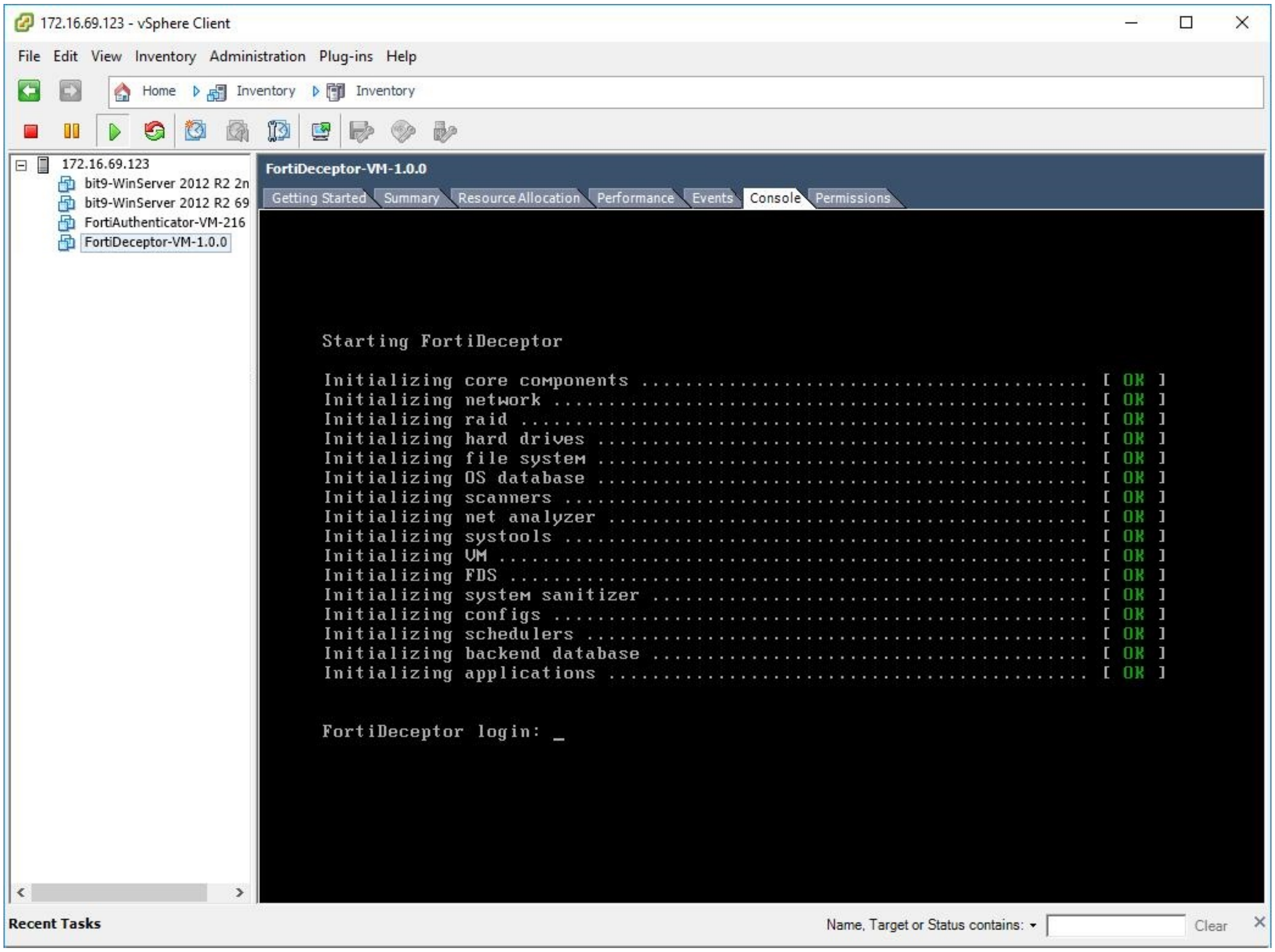
- Enabling GUI access
- Connecting to the GUI
- Uploading the license file
- Installing the Windows VM package
- Activating Deception VMs

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.


172.16.69.123 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
172.16.69.123
bit9-WinServer 2012 R2 2n
bit9-WinServer 2012 R2 69
FortiAuthenticator-VM-216
FortiDeceptor-VM-1.0.0
FortiDeceptor-VM-1.0.0
Getting Started
Summary
Resource Allocation
Performance
Events
Console
Permissions
Recent Tasks
Name, Target or Status contains: ▾
Clear

```
Starting FortiDeceptor

Initializing core components ........................................ [ OK ]
Initializing network ................................................ [ OK ]
Initializing raid ................................................... [ OK ]
Initializing hard drives ............................................ [ OK ]
Initializing file system ............................................ [ OK ]
Initializing OS database ............................................ [ OK ]
Initializing scanners ............................................... [ OK ]
Initializing net analyzer ........................................... [ OK ]
Initializing systools ............................................... [ OK ]
Initializing VM ..................................................... [ OK ]
Initializing FDS .................................................... [ OK ]
Initializing system sanitizer ....................................... [ OK ]
Initializing configs ................................................ [ OK ]
Initializing schedulers ............................................. [ OK ]
Initializing backend database ....................................... [ OK ]
Initializing applications ........................................... [ OK ]


FortiDeceptor login: _
```

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.

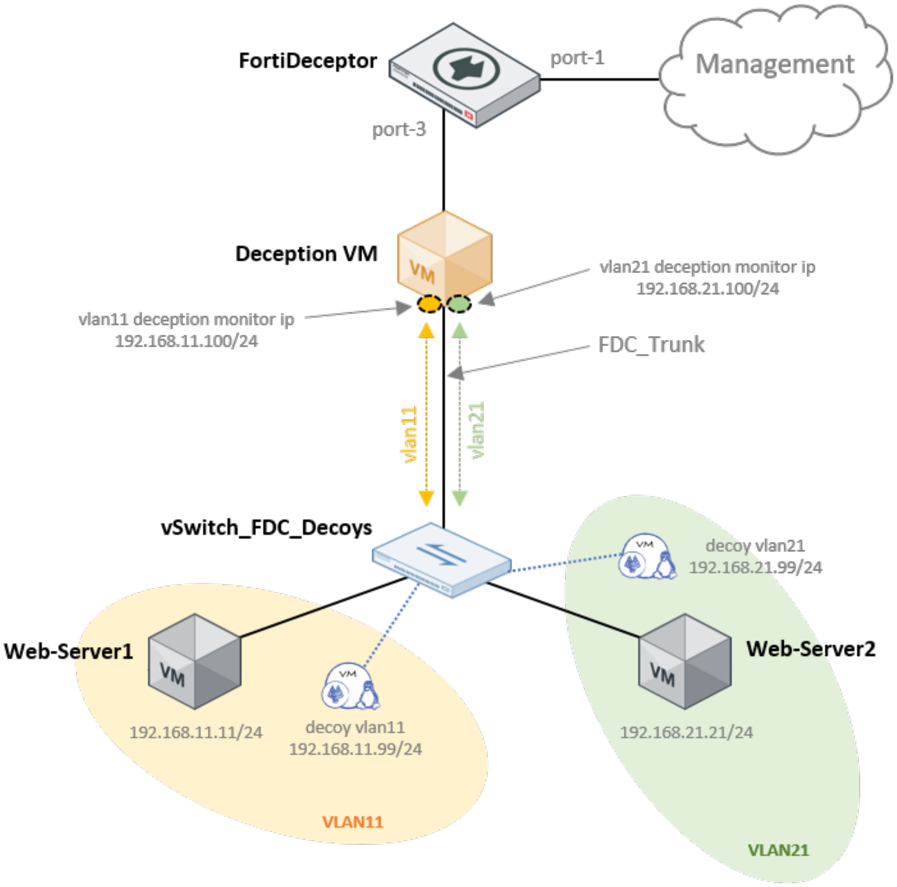
Once the license for the Deception VM is activated, the network must be set up with Internet access to activate the Windows Operating System license for the Windows Deception VM. Ubuntu Operating System for the Linux Deception VM does not need activation.

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

Configuring FortiDeceptor VM networking

To simplify configuration, we recommend using a dedicated vSwitch for the decoy and monitored segments.

The following diagram shows the vSwitch ports relationship.

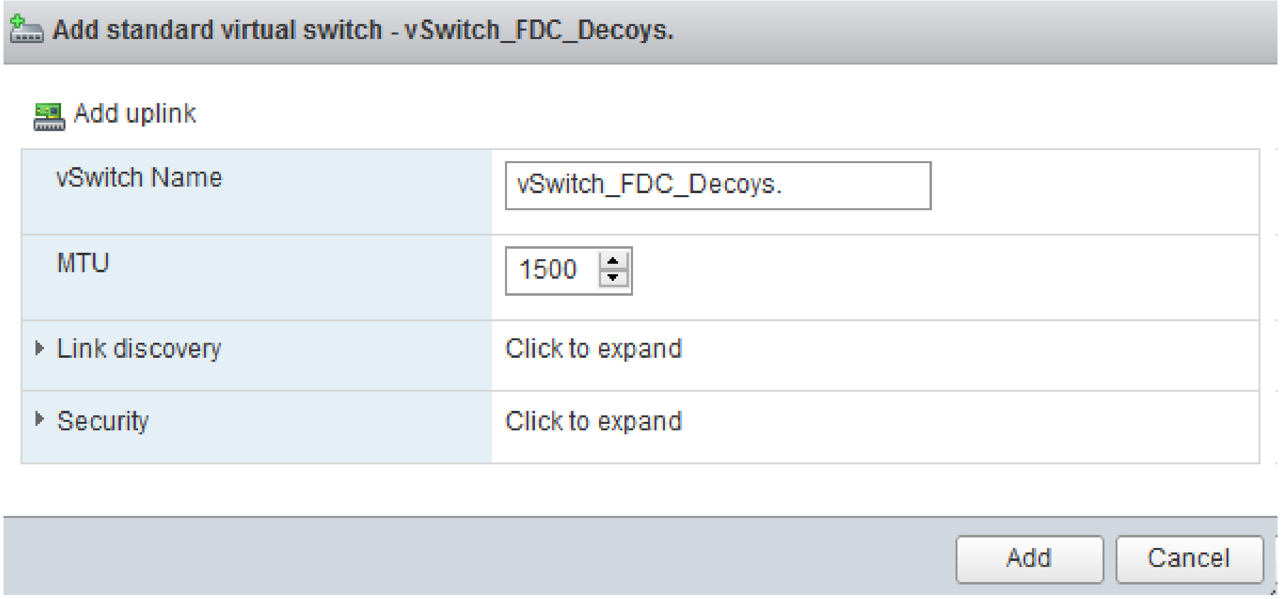


On ESXi, configure the *vSwitch_ FDC_Decoys* vSwitch to connect both VLANs to FortiDeceptor VM. Then configure three network port-groups:

1. *FDC_Trunk* – Port-group for the actual trunk interface between FortiDeceptor VM and vSwitch.
2. *VLAN11* – Port-group to connect VLAN11 to vSwitch.
3. *VLAN21* – Port-group to connect VLAN21 to vSwitch.

To configure the vSwitch:

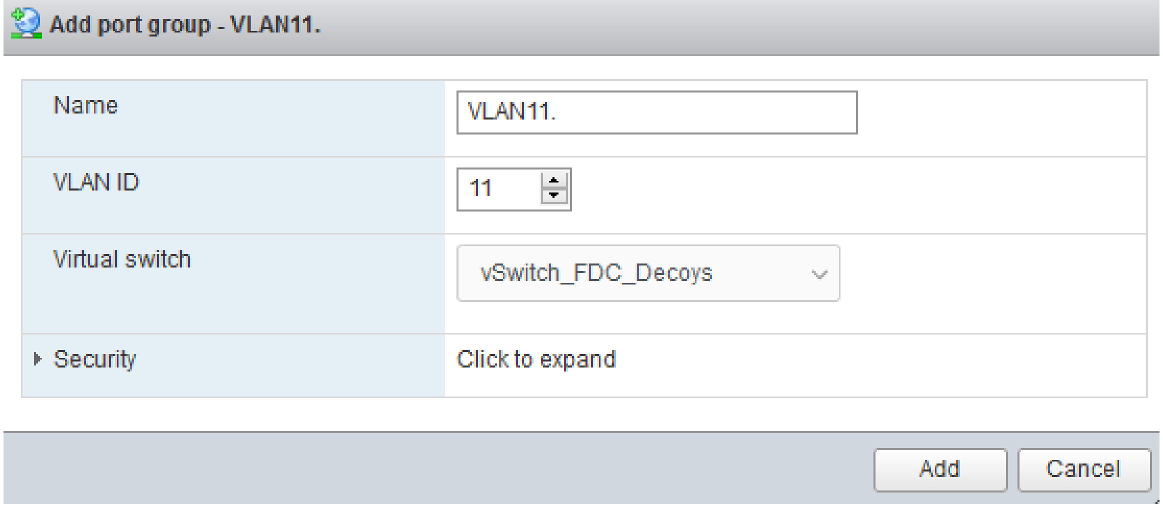
1. On the ESXi client, go to *Networking* > *Virtual Switches* and add a standard virtual switch.
   Just configure the *vSwtich Name*, remove the uplink (unless you need it), and use default values for the other options.



Add standard virtual switch - vSwitch_FDC_Decoys.

vSwitch Name	vSwitch_FDC_Decoys.
MTU	1500
Link discovery	Click to expand
Security	Click to expand

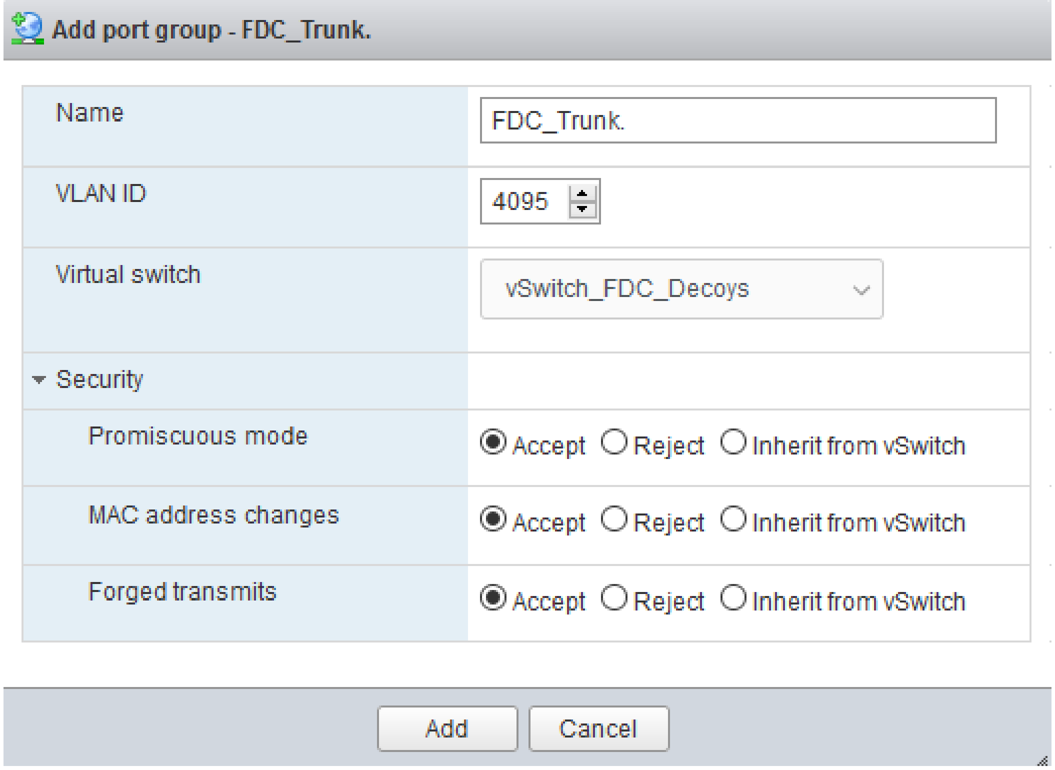
2. Go to *Networking* > *Port groups* and add the port groups.
   Port groups for VLAN11 and VLAN21 are similar. For each port group, specify a *Name*, configure the *VLAN ID*, and select the *Virtual switch*.



Add port group - VLAN11.

Name	VLAN11.
VLAN ID	11
Virtual switch	vSwitch_FDC_Decoys
Security	Click to expand

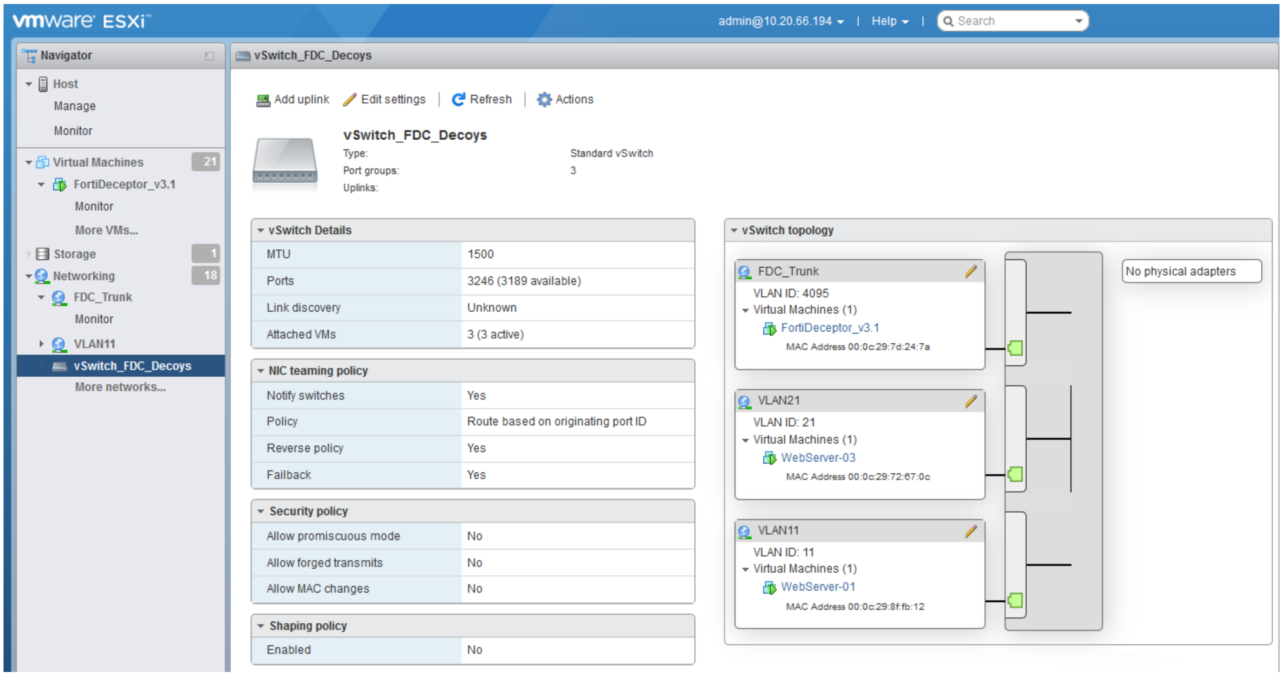
3. For the FDC Trunk port, configure a special port-group.
   On ESXi, you do not need to configure 802.1Q. You only need to set the port group to be a promiscuous interface and specify *4095* for the *VLAN ID* so the vSwitch can send and receive traffic from the VLANs configured on FortiDeceptor VM.
   Select the *Virtual switch* and set all *Security* options to *Accept*.



Add port group - FDC_Trunk.

Name	FDC_Trunk.
VLAN ID	4095
Virtual switch	vSwitch_FDC_Decoys
Security	
Promiscuous mode	● Accept ○ Reject ○ Inherit from vSwitch
MAC address changes	● Accept ○ Reject ○ Inherit from vSwitch
Forged transmits	● Accept ○ Reject ○ Inherit from vSwitch

4. To verify the configuration, check the vSwitch topology and ensure all devices are connected to this switch.



vSwitch_FDC_Decoys

Type: Standard vSwitch
Port groups: 3
Uplinks:

vSwitch Details	
MTU	1500
Ports	3246 (3189 available)
Link discovery	Unknown
Attached VMs	3 (3 active)

NIC teaming policy	
Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Failback	Yes

Security policy	
Allow promiscuous mode	No
Allow forged transmits	No
Allow MAC changes	No

Shaping policy	
Enabled	No

vSwitch topology

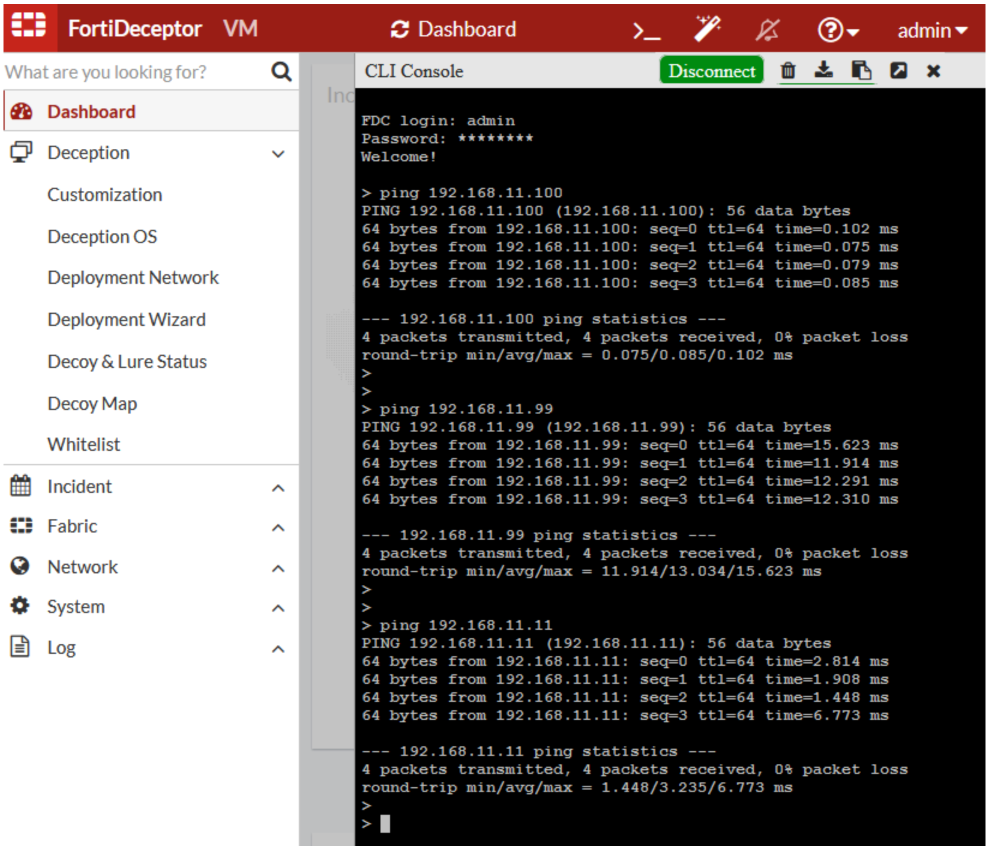
FDC_Trunk
VLAN ID: 4095
Virtual Machines (1)
FortiDeceptor_v3.1
MAC Address 00:0c:29:7d:24:7a

VLAN21
VLAN ID: 21
Virtual Machines (1)
WebServer-03
MAC Address 00:0c:29:72:67:0c

VLAN11
VLAN ID: 11
Virtual Machines (1)
WebServer-01
MAC Address 00:0c:29:8f:fb:12

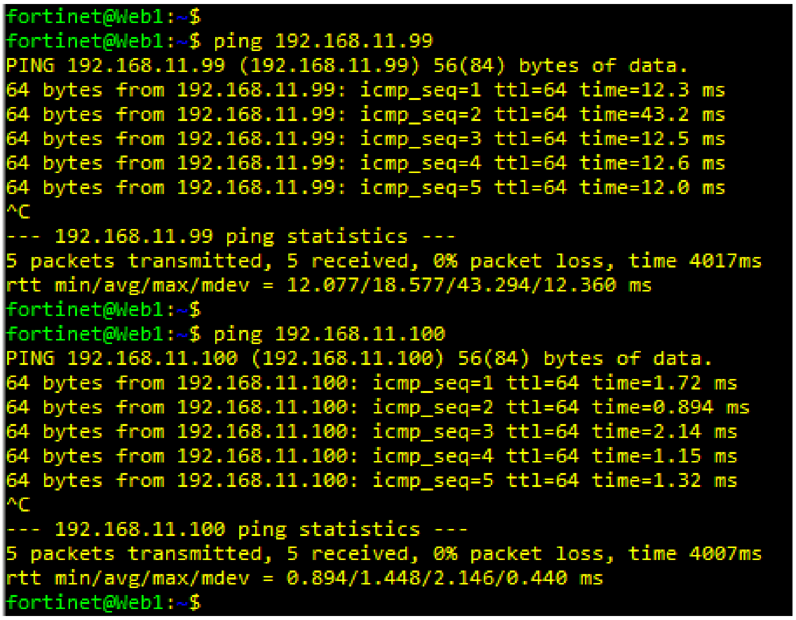
No physical adapters

5. Test connectivity from FortiDeceptor VM to the web servers, and from each web server to the decoys connected to the same VLAN.
   - From FortiDeceptor VM.



```
FDC login: admin
Password: ********
Welcome!

> ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100): 56 data bytes
64 bytes from 192.168.11.100: seq=0 ttl=64 time=0.102 ms
64 bytes from 192.168.11.100: seq=1 ttl=64 time=0.075 ms
64 bytes from 192.168.11.100: seq=2 ttl=64 time=0.079 ms
64 bytes from 192.168.11.100: seq=3 ttl=64 time=0.085 ms

--- 192.168.11.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.075/0.085/0.102 ms
>
>
> ping 192.168.11.99
PING 192.168.11.99 (192.168.11.99): 56 data bytes
64 bytes from 192.168.11.99: seq=0 ttl=64 time=15.623 ms
64 bytes from 192.168.11.99: seq=1 ttl=64 time=11.914 ms
64 bytes from 192.168.11.99: seq=2 ttl=64 time=12.291 ms
64 bytes from 192.168.11.99: seq=3 ttl=64 time=12.310 ms

--- 192.168.11.99 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 11.914/13.034/15.623 ms
>
>
> ping 192.168.11.11
PING 192.168.11.11 (192.168.11.11): 56 data bytes
64 bytes from 192.168.11.11: seq=0 ttl=64 time=2.814 ms
64 bytes from 192.168.11.11: seq=1 ttl=64 time=1.908 ms
64 bytes from 192.168.11.11: seq=2 ttl=64 time=1.448 ms
64 bytes from 192.168.11.11: seq=3 ttl=64 time=6.773 ms

--- 192.168.11.11 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.448/3.235/6.773 ms
>
>
```

   - From web server 1.



```
fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.99
PING 192.168.11.99 (192.168.11.99) 56(84) bytes of data.
64 bytes from 192.168.11.99: icmp_seq=1 ttl=64 time=12.3 ms
64 bytes from 192.168.11.99: icmp_seq=2 ttl=64 time=43.2 ms
64 bytes from 192.168.11.99: icmp_seq=3 ttl=64 time=12.5 ms
64 bytes from 192.168.11.99: icmp_seq=4 ttl=64 time=12.6 ms
64 bytes from 192.168.11.99: icmp_seq=5 ttl=64 time=12.0 ms
^C
--- 192.168.11.99 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4017ms
rtt min/avg/max/mdev = 12.077/18.577/43.294/12.360 ms
fortinet@Web1:~$
fortinet@Web1:~$ ping 192.168.11.100
PING 192.168.11.100 (192.168.11.100) 56(84) bytes of data.
64 bytes from 192.168.11.100: icmp_seq=1 ttl=64 time=1.72 ms
64 bytes from 192.168.11.100: icmp_seq=2 ttl=64 time=0.894 ms
64 bytes from 192.168.11.100: icmp_seq=3 ttl=64 time=2.14 ms
64 bytes from 192.168.11.100: icmp_seq=4 ttl=64 time=1.15 ms
64 bytes from 192.168.11.100: icmp_seq=5 ttl=64 time=1.32 ms
^C
--- 192.168.11.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 0.894/1.448/2.146/0.440 ms
fortinet@Web1:~$
```

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.