Micro-FortiGuard Server for FortiClient - Install Guide

Version 6.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET COOKBOOK
https://cookbook.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: techdocs@fortinet.com

November 2, 2018
Micro-FortiGuard Server for FortiClient 6.0 Install Guide
04-600-504219-20181102

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-07-23	Initial release.
2018-09-07	VM deployment package versions updated.
2018-11-02	VM deployment package names changed for Micro-FortiGuard Server for FortiClient 6.0.3 and later.

About Micro-FortiGuard Server for FortiClient on VMware

This document provides information about deploying a Micro-FortiGuard Server for FortiClient using VMware vSphere or Player. 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.

The minimum system requirements for Micro-FortiGuard Server for FortiClient is 2 CPUs and 4GB or RAM.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Registering your Micro-FortiGuard Server for FortiClient
- Downloading deployment packages

Registering your Micro-FortiGuard Server for FortiClient

After placing an order for Micro-FortiGuard Server for FortiClient, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the Micro-FortiGuard Server for FortiClient 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 Micro-FortiGuard Server for FortiClient. 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.

To register your Micro-FortiGuard Server for FortiClient:

1. Ensure that you have the following items needed to complete the procedure:
   - License registration code that was emailed to you after you placed an order for Micro-FortiGuard Server for FortiClient
   - Support contract number
   - IPv4 address for the Micro-FortiGuard Server for FortiClient
2. Log into the Fortinet Customer Service & Support portal at https://support.fortinet.com/ using an existing support account, or click *Create an Account* to create a new account.
3. In the toolbar, select *Asset* > *Register/Renew*. The *Registration Wizard* opens.
4. Enter the registration code from the Micro-FortiGuard Server for FortiClient License Certificate that was emailed to you, select the end user type, and then click *Next*. The *Registration Info* page is displayed.
5. 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, Micro-FortiGuard Server for FortiClient compares its configured IP addresses with the IP information in the license file. The license must be associated with an IP address assigned to one of the interfaces on the Micro-FortiGuard Server for FortiClient. If a new license has been imported or the Micro-FortiGuard Server for FortiClient's associated IP address has been changed, the Micro-FortiGuard Server for FortiClient 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 Micro-FortiGuard Server for FortiClient license validation. You must specify an IPv4 address in both the support portal and the port management interface.

6. On the *Fortinet Product Registration Agreement* page, select the checkbox to indicate that you have read, understood, and accepted the service contract, then select *Next* to continue to the *Verification* page.
7. The verification page displays the product entitlement. Select the checkbox to indicate that you accept the terms then select *Confirm* to submit the request.
8. From the *Registration Completed* page, you can download the Micro-FortiGuard Server for FortiClient license file, select *Register More* to register another Micro-FortiGuard Server for FortiClient, 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 Micro-FortiGuard Server for FortiClient via the GUI, see Uploading the license file on page 17 .

Editing Micro-FortiGuard Server for FortiClient IP addresses

To edit the Micro-FortiGuard Server for FortiClient IP address:

1. In the toolbar, select *Asset* > *Manage/View Products* to open the *View Products* page.
2. Select the Micro-FortiGuard Server for FortiClient serial number to open the *Product Details* page.
3. Click *Edit* to change the description, partner information, and IP address of your Micro-FortiGuard Server for FortiClient 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 Micro-FortiGuard Server for FortiClient 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 Micro-FortiGuard Server for FortiClient via the GUI, see Uploading the license file on page 17.

Deployment package

Micro-FortiGuard Server for FortiClient deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment package.

VM Platform	Deployment File

VMware ESXi 5.0, 5.5, 6.0, 6.5, and 6.7	ESX/ESXi server:
	`FMG_VM64_MFGD-vX-buildxxxx-FORTINET.out.ovf.zip`
	VMware Player:
	`FMG_VM64_MFGD-vX-buildxxxx-FORTINET.out.vmware.zip`

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

- `fmg.vmdk`: The Micro-FortiGuard Server for FortiClient system hard disk in Virtual Machine Disk (VMDK) format.
- `Micro-FortiGuard-Server.ovf`: The VMware virtual hardware configuration file.

- `Micro-FortiGuard-Server.vapp.ovf`
- `DATADRIVE.vmdk`: The Micro-FortiGuard Server for FortiClient log disk in VMDK format

The `.out.vmware.zip` file, for use with VMware Player, contains:

- `fmg.vmdk`: The Micro-FortiGuard Server for FortiClient system hard disk in VMDK format.
- `Micro-FortiGuard-Server.vmx`: The VMware virtual hardware configuration file.
- `DATADRIVE.vmdk`: The Micro-FortiGuard Server for FortiClient log disk in VMDK format
- `DATADRIVE-S0XX.vmdk`: 41 VMDK files used during deployment.

Downloading deployment packages

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

You can download the *Micro-FortiGuard Server for FortiClient Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the Micro-FortiGuard Server for FortiClient 6.0.0 directory.

Download the `.out` file to upgrade your existing Micro-FortiGuard Server for FortiClient installation.

To download deployment packages:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiManager* from the *Select Product* drop-down list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Deployment

Prior to deploying the Micro-FortiGuard Server for FortiClient, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for Micro-FortiGuard Server for FortiClient presume 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 because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your Micro-FortiGuard Server for FortiClient appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start Micro-FortiGuard Server for FortiClient, you will have access only 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 GUI (see Enabling GUI access on page 16).

Deploying Micro-FortiGuard Server for FortiClient on VMware vSphere

Once you have downloaded the `FMG_MFGD-v5-buildxxxx-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.

Prior to deploying the Micro-FortiGuard Server for FortiClient, ensure that the following are configured and functioning properly:

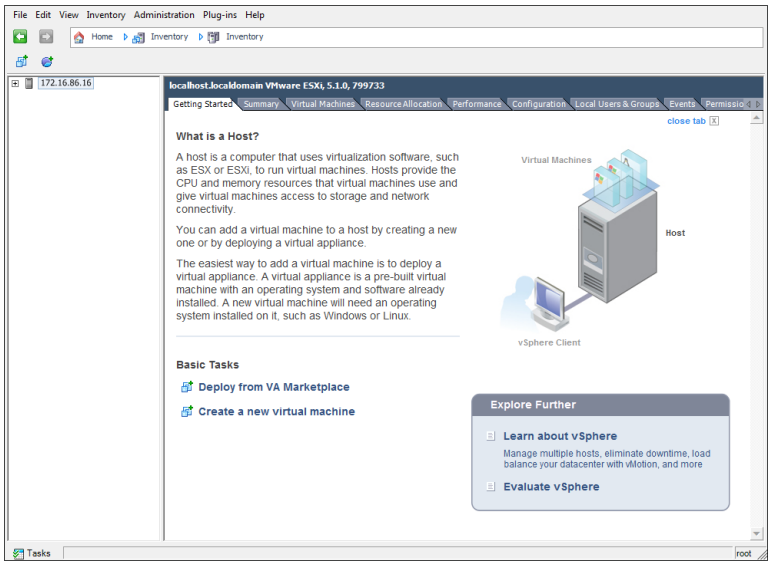
- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server and updated to the latest patch release prior to installing Micro-FortiGuard Server for FortiClient. Go to https://www.vmware.com/products/vsphere-hypervisor.html for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the Micro-FortiGuard Server for FortiClient.

The following topics are included in this section:

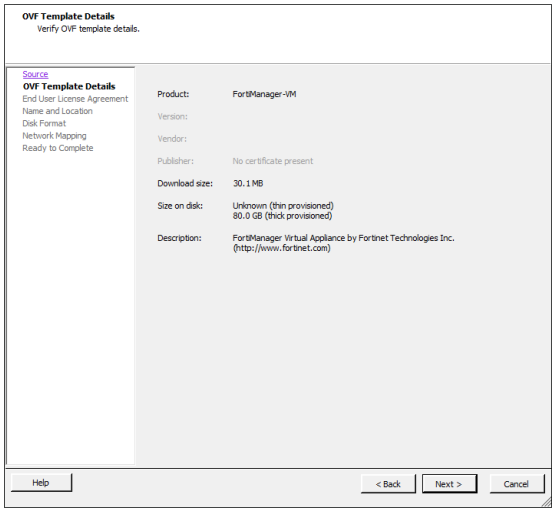
Deploying the OVF file

To deploy the OVF file template:

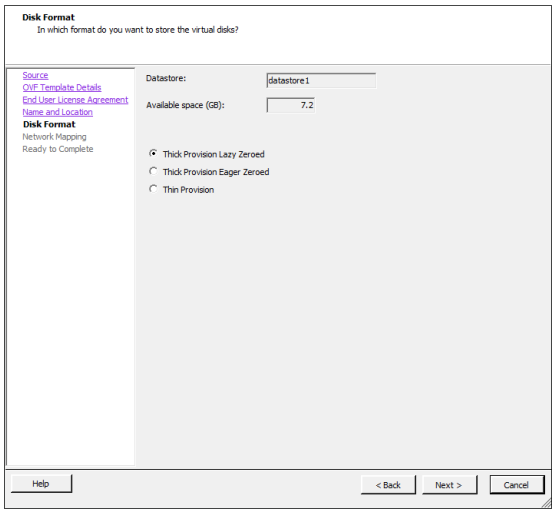
1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then click *Login*. The vSphere client home page opens.



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 click *Next* to continue. The OVF Template *Details* page opens.



4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Click *Next* to continue. The OVF Template *End User License Agreement* page opens.
5. Read the end user license agreement, then click *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 must be unique within the inventory folder. Click *Next* to continue. The OVF Template *Disk Format* page opens.

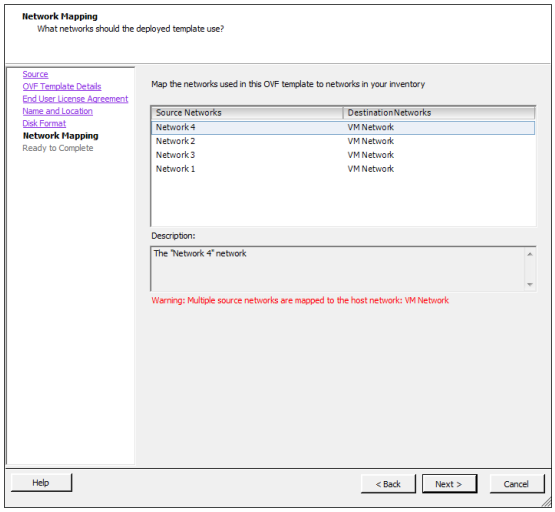


7. Select one of the following:
   - *Thick Provision Lazy Zeroed*: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - *Thick Provision 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 Micro-FortiGuard Server for FortiClient base 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. Click *Next* to continue. The OVF Template *Network Mapping* page opens.



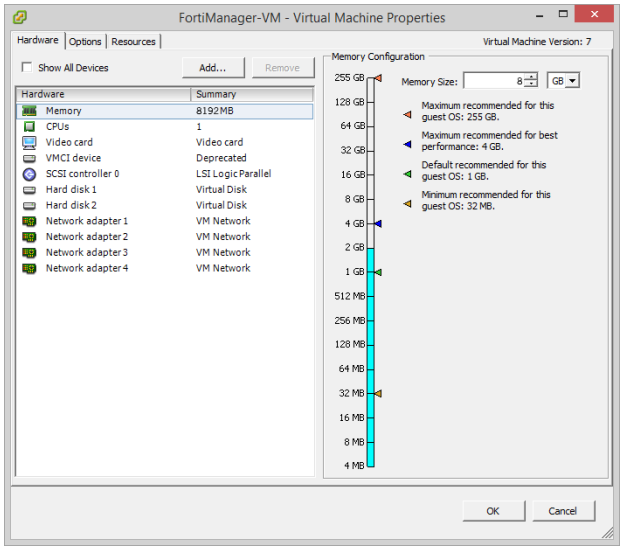
9. Map the networks used in this OVF template to networks in your inventory. Network 1 maps to port1 of the Micro-FortiGuard Server for FortiClient. You must set the destination network for this entry to access the device console. Click *Next* to continue. The OVF Template *Ready to Complete* page opens.
10. Review the template configuration.
    Ensure that *Power on after deployment* is not enabled. You might need to configure the Micro-FortiGuard Server for FortiClient hardware settings prior to powering on the VM.
11. Click *Finish* to deploy the OVF template. A *Deployment Completed Successfully* dialog box is displayed once the Micro-FortiGuard Server for FortiClient OVF template wizard has finished.

Configuring hardware settings

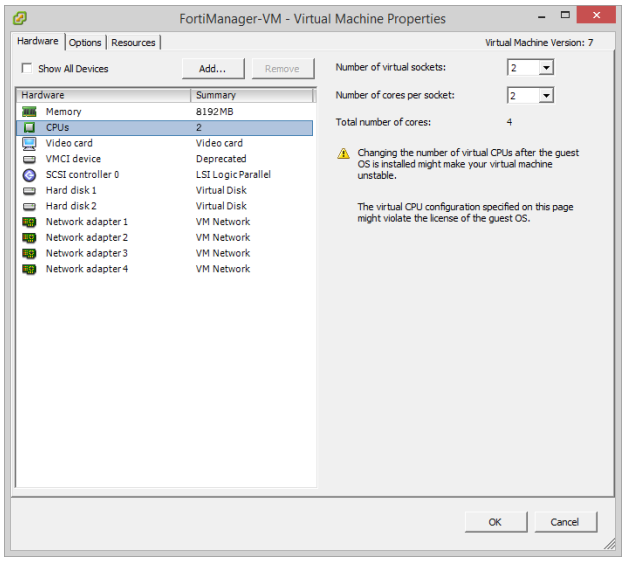
Before powering on your Micro-FortiGuard Server for FortiClient, you must configure the virtual memory, virtual CPU, and virtual disk.

To configure hardware settings:

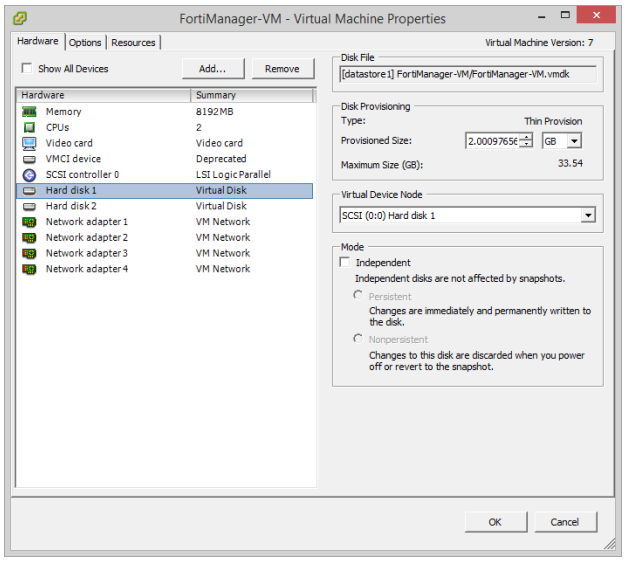
1. In the vSphere Client, right-click on the Micro-FortiGuard Server for FortiClient in the left pane, and select *Edit Settings* to open the *Virtual Machine Properties* window.
2. Select *Memory* from the *Hardware* list, then adjust the *Memory Size* as required.



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



4. Select *Hard disk 2*, the log disk, from the *Hardware* list, and configure it as required. *Hard disk 1* should not be edited.



The Micro-FortiGuard Server for FortiClient allows for 12 virtual log disks to be added to a deployed instance. When adding additional hard disks use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

5. Click *OK* to apply your changes.

Powering on the virtual machine

You can now proceed to power on your Micro-FortiGuard Server for FortiClient.

- Select the Micro-FortiGuard Server for FortiClient in the left pane, then click *Power on the virtual machine* in the *Getting Started* tab.
- Select the VM in the left pane, then click *Power On* in the toolbar.
- Right-click the VM in the left pane, then select *Power > Power On* from the right-click menu.

Once the VM has started, proceed with the initial configuration. See Configuring initial settings on page 16.

Deploying Micro-FortiGuard Server for FortiClient on VMware Player

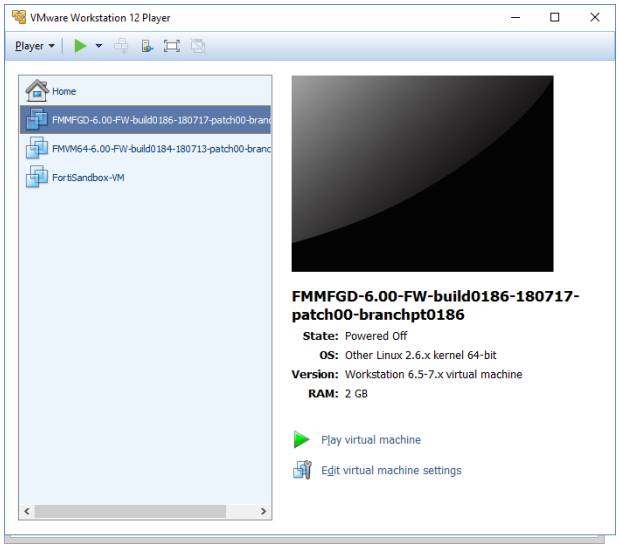
Once you have downloaded the `FMG_MFGD-vX-buildxxxx-FORTINET.out.vmware.zip` file and extracted the package contents to a folder on your management computer, you can deploy the package.

Before powering on your Micro-FortiGuard Server for FortiClient you must configure the virtual memory, CPU, and disk configuration to match your Micro-FortiGuard Server for FortiClient VM license.

The default IP address and netmask of the Micro-FortiGuard Server for FortiClient is **192.168.1.99 255.255.255.0**.

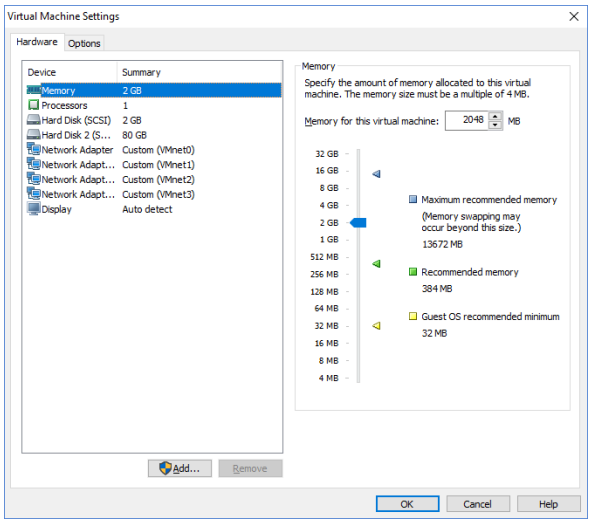
To deploy and configure the VM:

1. Launch the VMware Player, then select *Open a Virtual Machine*.
2. Browse to the location of the *FortiManager-MFGD.vmx* file, select it, then select *Open*.

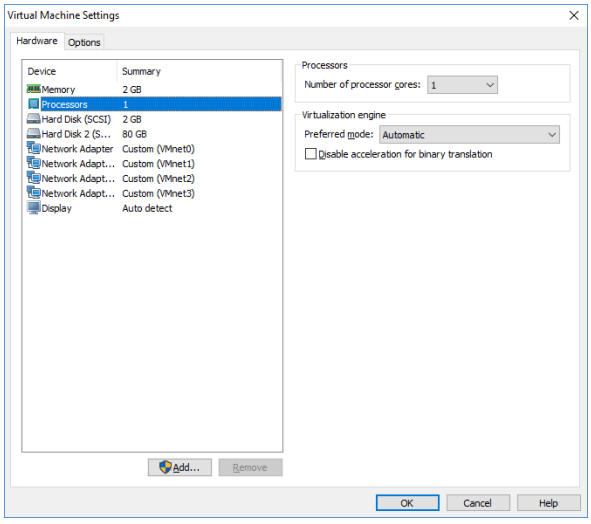


3. Select *Edit virtual machine settings* to open the *Virtual Machine Settings* window.

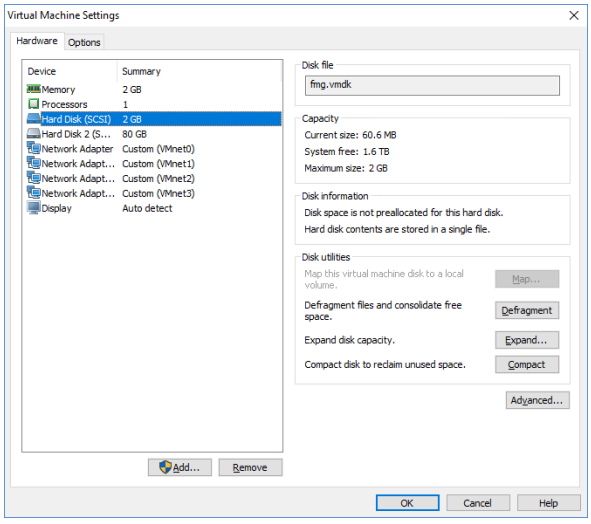
4. Select *Memory*, then adjust the *Memory for this virtual machine* as required.



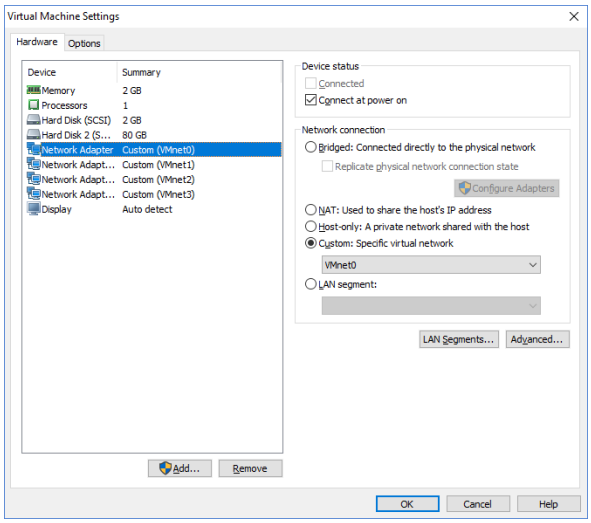
5. Select *Processors*, then adjust the *Number of processor cores* as required.



6. Select *Hard Disk* and *Hard disk 2* to configure the disks as required.



7. Configure the network adapters as required.



8. To add new hardware, such as another hard disk or network adapter, select *Add* then follow the steps in the *Add Hardware Wizard*.
9. Once the VM is configured as required, select *OK*, then select *Play virtual machine* to start the VM.
   The Micro-FortiGuard Server for FortiClient CLI console will open in VMware Player.

Once the VM has started, proceed with the initial configuration. See Configuring initial settings on page 16.

Configuring initial settings

Before you can connect to the Micro-FortiGuard Server for FortiClient, you must configure basic network settings via the CLI console. Once configured, you can connect to the Micro-FortiGuard Server for FortiClient GUI and upload the Micro-FortiGuard Server for FortiClient 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

Enabling GUI access

To enable GUI access to the Micro-FortiGuard Server for FortiClient, you must configure the IP address and network mask of the appropriate port on the Micro-FortiGuard Server for FortiClient. The following instructions use port 1.

The appropriate port can be determined by matching the MAC address of the network adapter and the `HWaddr` provided by the CLI command `diagnose fmnetwork interface list`.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the Micro-FortiGuard Server for FortiClient and access the console window. You might need to press *Enter* to see the login prompt.
2. At the Micro-FortiGuard Server for FortiClient login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
config system interface
   edit port1
      set ip <IP address> <netmask>
end
```

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor virtual machine settings.

4. To configure the default gateway, enter the following commands:

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

The Customer Service & Support portal does not currently support IPv6 for Micro-FortiGuard Server for FortiClient 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 a port's IP address and network mask, launch a web browser and enter the IP address you configured for the port management interface. At the login page, enter the user name `admin` and no password, then select *Login*.

The GUI will open with an *Evaluation License* dialog box.

Uploading the license file

Micro-FortiGuard Server for FortiClient includes a free, full featured 15 day trial.

Before using the Micro-FortiGuard Server for FortiClient, you must enter the license file that you downloaded from the Customer Service & Support portal when you registered your Micro-FortiGuard Server for FortiClient. See Registering your Micro-FortiGuard Server for FortiClient on page 6.

To upload the license via the CLI:

1. Open the license file in a text editor and copy the VM license string.
2. In a Micro-FortiGuard Server for FortiClient console window, enter the following:

```
execute add-vm-license <"vm license string">
```

To upload the license file via the GUI:

1. In the *Evaluation License* dialog box, select *Enter License*.
   Optionally, you can also select *Upload License* in the *License Information* dashboard widget.
2. In the license upload page, click *Browse*, locate the VM license file (`.lic`) on your computer, then click *OK* to upload the license file.
   A reboot message will be shown, then the Micro-FortiGuard Server for FortiClient system will reboot and load the license file.
3. Refresh your browser and log back into the Micro-FortiGuard Server for FortiClient with username *admin* and no password.
   The VM registration status appears as valid in the *License Information* widget once the license has been validated.

As a part of the license validation process, Micro-FortiGuard Server for FortiClient compares its IP address with the IP information in the license file. If a new license has been imported or the Micro-FortiGuard Server for FortiClient's IP address has been changed, the Micro-FortiGuard Server for FortiClient 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 Micro-FortiGuard Server for FortiClient do not match, you will receive an error message when you log back into the VM.

If this occurs, you will need to 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 Micro-FortiGuard Server for FortiClient IP addresses on page 7

After an invalid license file has been loaded onto the Micro-FortiGuard Server for FortiClient, the GUI will be locked until a valid license file is uploaded. A new license file can be uploaded via the CLI.

Configuring your Micro-FortiGuard Server for FortiClient

Once the Micro-FortiGuard Server for FortiClient license has been validated, you can configure your device.

If the amount of memory or number of CPUs are too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages will be shown in the GUI in the *System Resources* widget on the dashboard.

Index