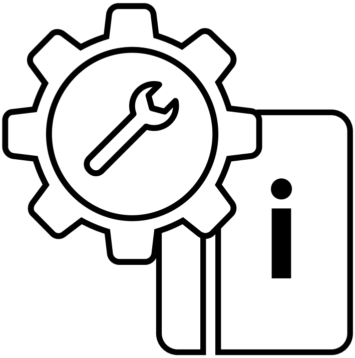
Installation Guide

LANCOM vFirewall



LANCOM
SYSTEMS

Copyright

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany

www.lancom-systems.com
Wuerselen, März 2025

Introduction

Thank you for purchasing a LANCOM vFirewall.
The LANCOM vFirewall is a software-based Unified Threat Management (UTM) firewall, which is operated on a virtual machine. And yet, it offers the same functionality as a real, appliance-based LANCOM R&S®Unified Firewall.
This installation guide describes the setup of the LANCOM vFirewall under VMware ESXi-Server, Oracle Virtual Box, and Microsoft Hyper-V Server.

Installation of the LANCOM vFirewall on a VMware ESXi server

Below, the prerequisites and single steps for a successful installation of the LANCOM vFirewall on a VMware ESXi server are described.

vFirewall files

The following files are available for the LANCOM vFirewall in the myLANCOM firewall license portal:
→ ISO image file

Prerequisites

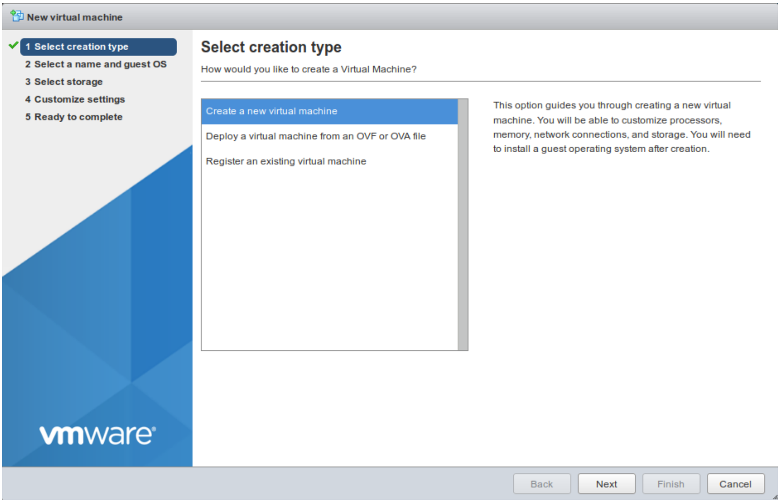
The following prerequisites are mandatory for a successful installation of the LANCOM vFirewall on a VMware ESXi server:
→ The LANCOM vFirewall software has to be available as an ISO image file
→ The VMware ESXI version ESXI 6.0.0 (VM version 11) or higher has to be installed on a server with an Intel processor.

The virtual machine has to meet the following minimum requirements:
→ 1 ×86 CPU (64 bit) processor
→ 4 GB RAM
→ 30 GB free harddisk space
→ 2 network interfaces

Creating and configuring the LANCOM vFirewall on a VMware ESXI server

Below, the necessary steps are described to put the LANCOM vFirewall into operation on a VMware ESXi server.
Start VMware ESXi, login and create a new virtual machine.

→ Select creation type - Create a new virtual machine



New virtual machine

✓ 1 Select creation type
2 Select a name and guest OS
3 Select storage
4 Customize settings
5 Ready to complete

Select creation type

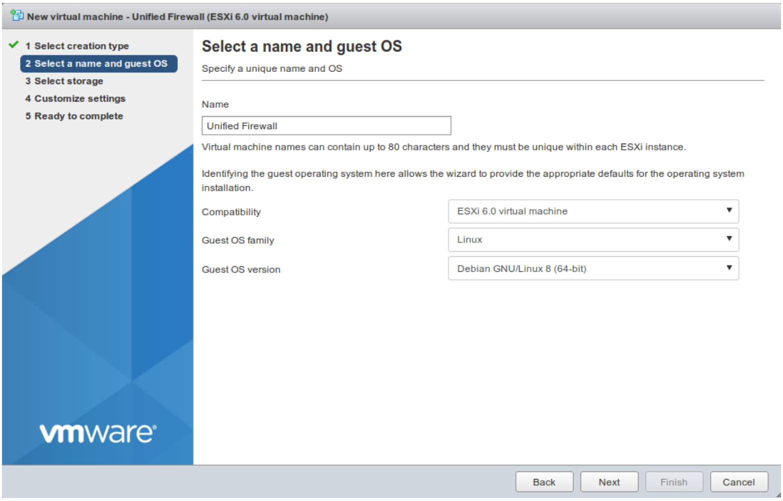
How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

Create a name for the virtual machine

→ Select a name and guest OS



New virtual machine - Unified Firewall (ESXi 6.0 virtual machine)

Select a name and guest OS

Specify a unique name and OS

Name: Unified Firewall

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

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 6.0 virtual machine

Guest OS family: Linux

Guest OS version: Debian GNU/Linux 8 (64-bit)

In the shown example, the name “Unified Firewall“ has been chosen. Further, please configure

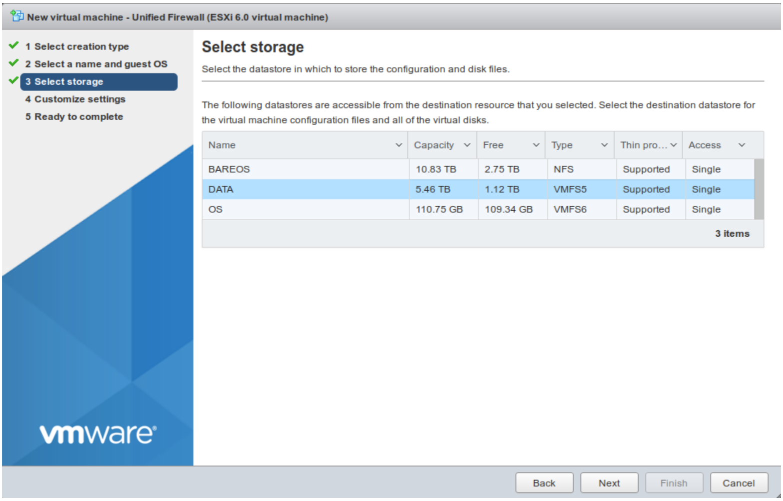
→ Compability: ESXI 6.0 virtual machine

→ Guest OS family: Linux

→ Guest OS version: Debian Linux 8 (64 bit)

Select the storage location for the virtual machine

→ Select storage



New virtual machine - Unified Firewall (ESXi 6.0 virtual machine)

- ✓ 1 Select creation type
- ✓ 2 Select a name and guest OS
- ✓ 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files.

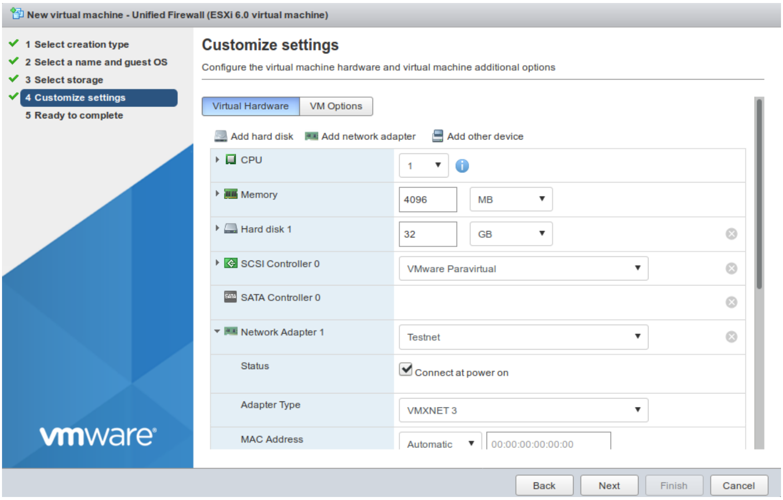
The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
BAREOS	10.83 TB	2.75 TB	NFS	Supported	Single
DATA	5.46 TB	1.12 TB	VMFS5	Supported	Single
OS	110.75 GB	109.34 GB	VMFS6	Supported	Single

3 items

Modify your settings

→ Customize settings



New virtual machine - Unified Firewall (ESXi 6.0 virtual machine)

- ✓ 1 Select creation type
- ✓ 2 Select a name and guest OS
- ✓ 3 Select storage
- ✓ 4 Customize settings
- 5 Ready to complete

Customize settings

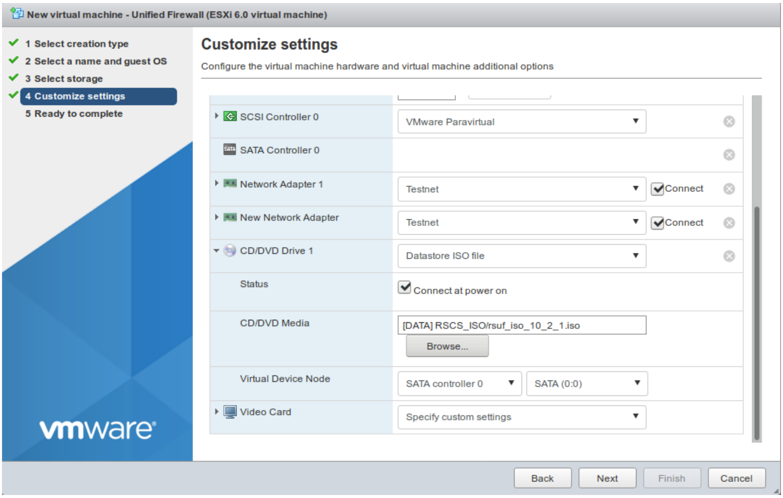
Configure the virtual machine hardware and virtual machine additional options

CPU	1
Memory	4096 MB
Hard disk 1	32 GB
SCSI Controller 0	VMware Paravirtual
SATA Controller 0	
Network Adapter 1	Testnet
Status	☑ Connect at power on
Adapter Type	VMXNET 3
MAC Address	Automatic 00:00:00:00:00:00

Configure as follows:

→ CPU: at least 1
→ Memory: at least 4096 MB
→ Hard disk 1: at least 32 GB
→ Adapter type: **VMXNET 3**

Select the ISO image file via the “Browse“ button.



New virtual machine - Unified Firewall (ESXi 6.0 virtual machine)

✓ 1 Select creation type
✓ 2 Select a name and guest OS
✓ 3 Select storage
✓ 4 Customize settings
5 Ready to complete

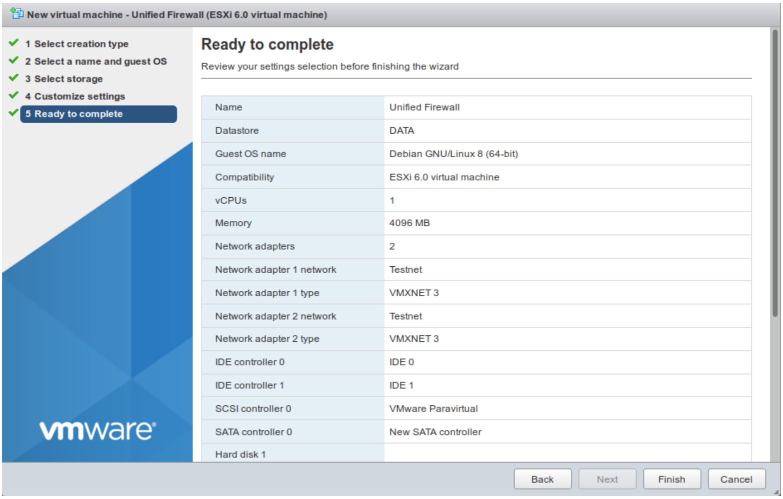
Customize settings

Configure the virtual machine hardware and virtual machine additional options

SCSI Controller 0	VMware Paravirtual	
SATA Controller 0		
Network Adapter 1	Testnet	☑ Connect
New Network Adapter	Testnet	☑ Connect
CD/DVD Drive 1	Datastore ISO file	
Status	☑ Connect at power on	
CD/DVD Media	[DATA] RSCS_ISO/rsuf_iso_10_2_1.iso	
Virtual Device Node	SATA controller 0	SATA (0:0)
Video Card	Specify custom settings	

Check your configuration.

→ Ready to complete



New virtual machine - Unified Firewall (ESXi 6.0 virtual machine)

✓ 1 Select creation type
✓ 2 Select a name and guest OS
✓ 3 Select storage
✓ 4 Customize settings
✓ 5 Ready to complete

Ready to complete

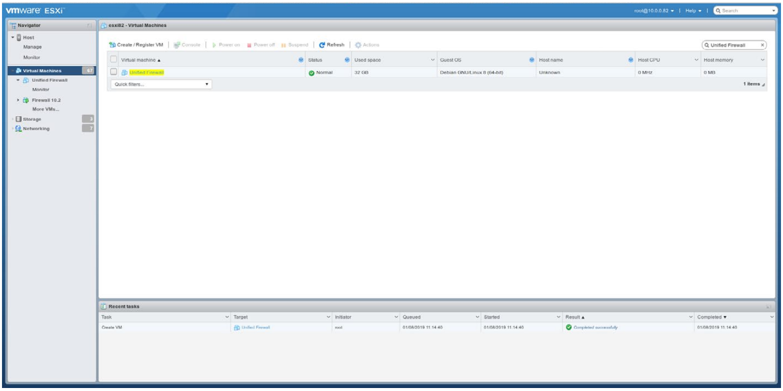
Review your settings selection before finishing the wizard

Name	Unified Firewall
Datastore	DATA
Guest OS name	Debian GNU/Linux 8 (64-bit)
Compatibility	ESXi 6.0 virtual machine
vCPUs	1
Memory	4096 MB
Network adapters	2
Network adapter 1 network	Testnet
Network adapter 1 type	VMXNET 3
Network adapter 2 network	Testnet
Network adapter 2 type	VMXNET 3
IDE controller 0	IDE 0
IDE controller 1	IDE 1
SCSI controller 0	VMware Paravirtual
SATA controller 0	New SATA controller
Hard disk 1	

Confirm the checked configuration using the “Finish“ button. Afterwards you can see your created virtual machine.

Starting the LANCOM vFirewall on a VMware ESXi server

Enter the name of the virtual machine in the search field, e.g. “Unified Firewall”.



esxi82 - Virtual Machines

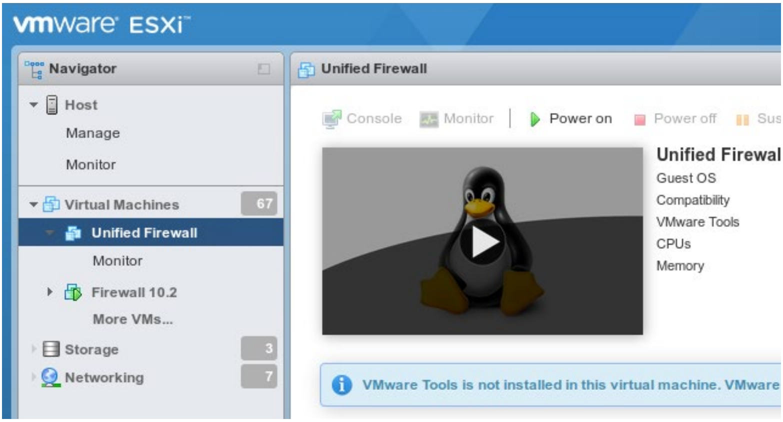
Search: Unified Firewall

Virtual machine ▲	Status	Used space	Guest OS	Host name	Host CPU	Host memory
Unified Firewall	Normal	32 GB	Debian GNU/Linux 8 (64-bit)	Unknown	0 MHz	0 MB

Recent tasks

Task	Target	Initiator	Queued	Started	Result ▲	Completed ▼
Create VM	Unified Firewall	root	01/08/2019 11:14:40	01/08/2019 11:14:40	Completed successfully	01/08/2019 11:14:40

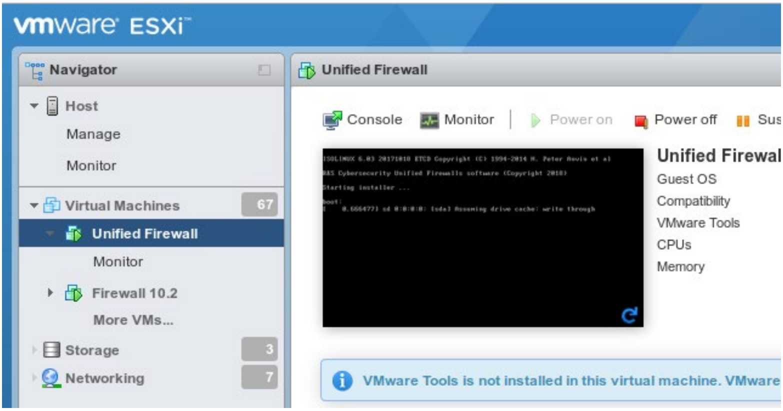
After selecting “Unified Firewall” you will see the following overview:



VMware Tools is not installed in this virtual machine. VMware

Select “Power on“ in the upper menu bar.

Select “Console“ in the upper menu bar, and in the following window “Open browser console“.



```
ISOLINUX 6.03 20171018 ETCD Copyright (C) 1994-2014 H. Peter Anvin et al
R&S Cybersecurity Unified Firewalls software (Copyright 2018)
Starting installer ...
boot:
[    0.666477] sd 0:0:0:0: [sda] Assuming drive cache: write through
```

VMware Tools is not installed in this virtual machine. VMware

The further configuration of the LANCOM vFirewall via console is described in the chapter „Final installation of the LANCOM vFirewall on the console“ on page 39.

The installation of the LANCOM vFirewall under Oracle VirtualBox

Below, the prerequisites and single steps for a successful installation of the LANCOM vFirewall under Oracle VirtualBox are described.

vFirewall files

The following files are available for the LANCOM vFirewall in the myLANCOM firewall license portal:

- ISO image file

Prerequisites

The following prerequisites are mandatory for a successful installation of the LANCOM vFirewall in the Oracle VM VirtualBox Manager:

- The LANCOM vFirewall software has to be available as an ISO image file
- Oracle VM VirtualBox Manager 5.0 or higher has to be installed on a server with an Intel processor.

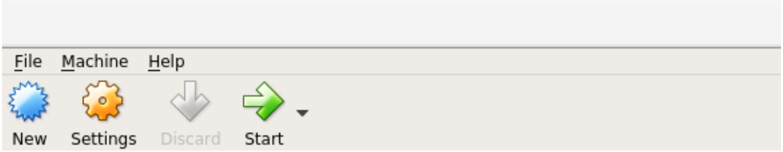
The virtual machine has to meet the following minimum requirements:

- 1 ×86 CPU (64 bit) processor
- 4 GB RAM
- 30 GB free hard disk space
- 2 network interfaces

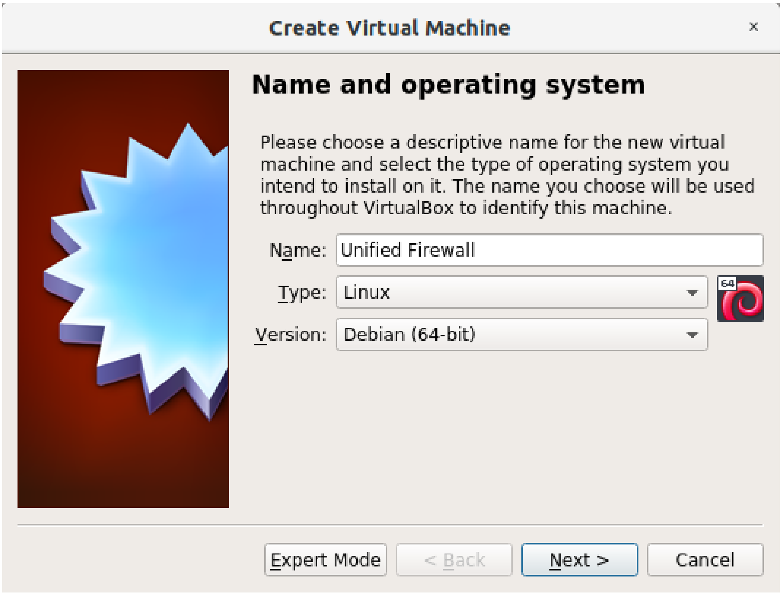
Creating and configuring the LANCOM vFirewall in the Oracle VirtualBox Manager

Below, the necessary steps are described to put the LANCOM vFirewall into operation in the Oracle Virtual Box Manager.

Start the Oracle VM Virtual Box Manager and select the “New“ button in the upper menu bar to create a new virtual machine.



In the upcoming window “Name and operating system“ allocate a name for the virtual machine.
In the shown example, the name ”Unified Firewall“ has been chosen.



Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Unified Firewall

Type: Linux

Version: Debian (64-bit)

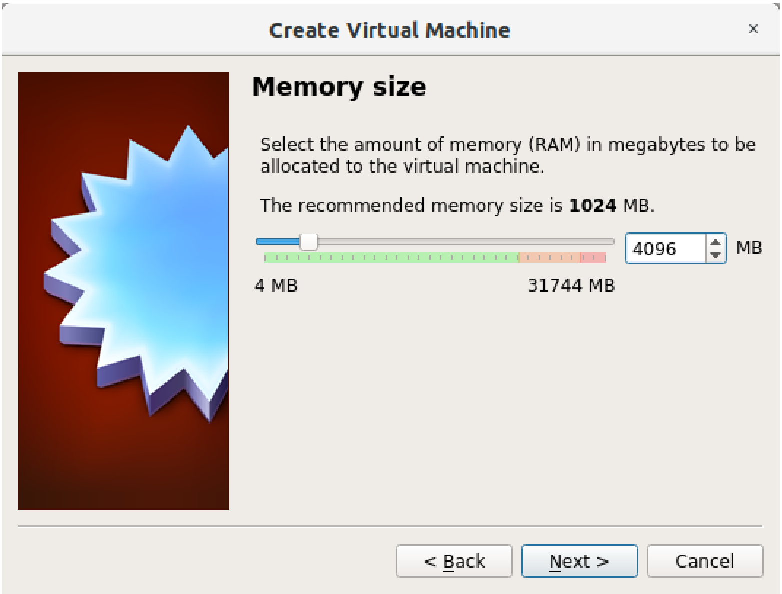
Further, please configure:

→ Type: Linux

→ Version: Debian (64-bit)

Click on “Next“.

In the window ”Memory size“ you configure the allocated memory for the virtual machine.



Create Virtual Machine

Memory size

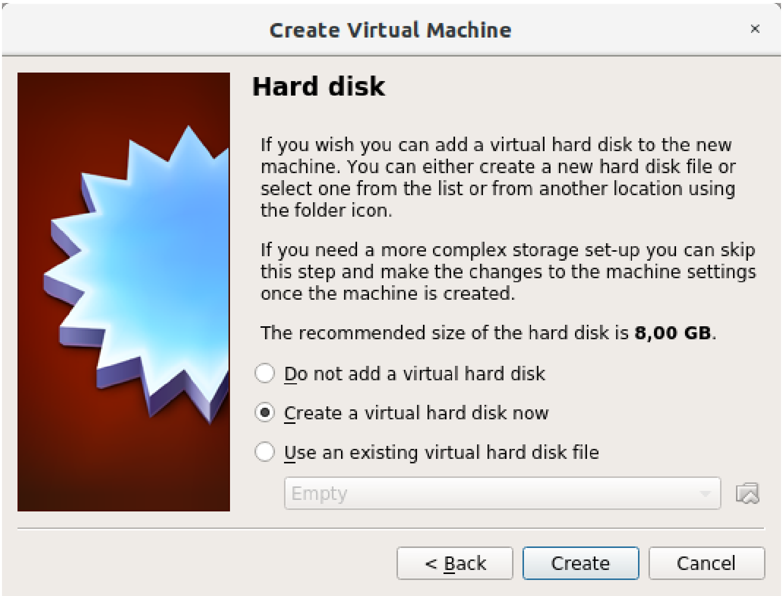
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024** MB.

4096 MB

Select 4096 MB as a minimum for full UTM and confirm with “Next“.

In the window “Hard disk“ you configure the virtual harddisk.



Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8,00 GB**.

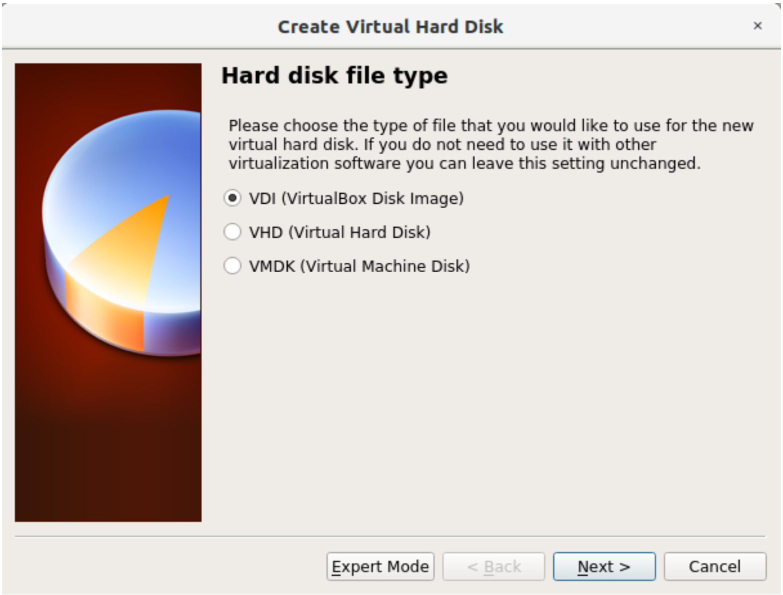
○ Do not add a virtual hard disk

● Create a virtual hard disk now

○ Use an existing virtual hard disk file

Select “Create a virtual hard disk now“ and confirm with “Create“.

In the next step “Hard disk file type“ you define the file type of the virtual harddisk.



Hard disk file type

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

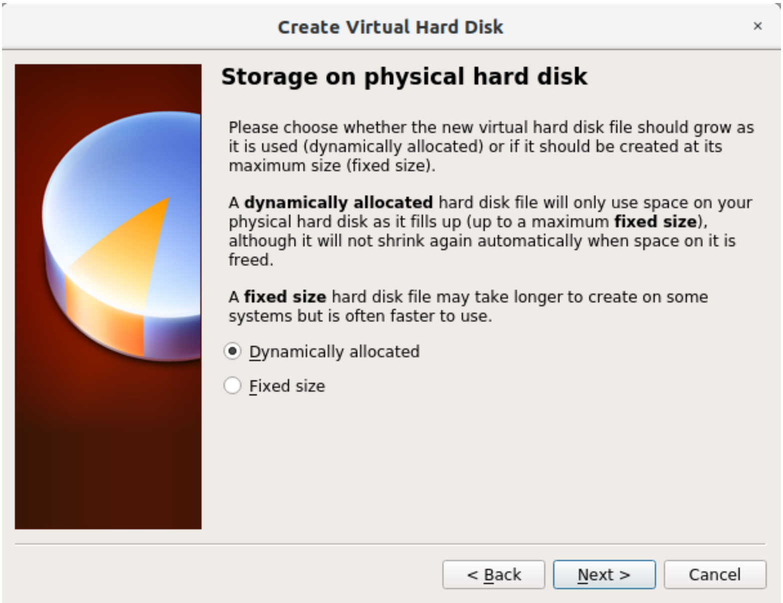
● VDI (VirtualBox Disk Image)

○ VHD (Virtual Hard Disk)

○ VMDK (Virtual Machine Disk)

Select “VDI (Virtual Box Disk Image)“ and confirm with “Next“.

In the next window ”Storage on physical hard disk“ you select the option to allocate memory for the virtual harddisk dynamically.



Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

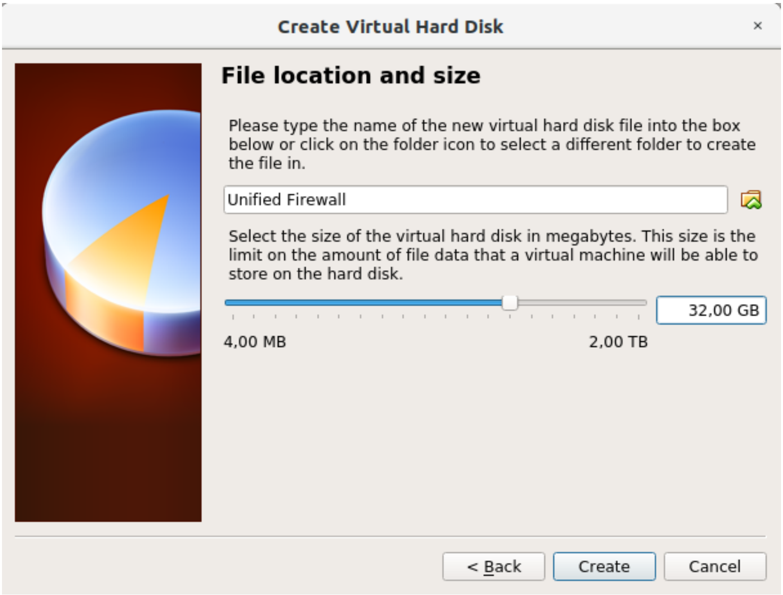
A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

● Dynamically allocated

○ Fixed size

Select “Dynamically allocated“ and confirm with “Next”.

In the next step ”File location and size“ you configure the name of the virtual harddisk, its storage location, and its minimum size.



File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

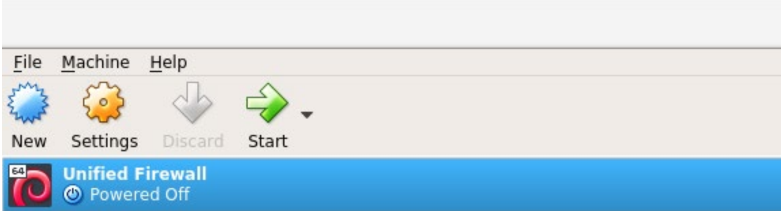
Unified Firewall

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

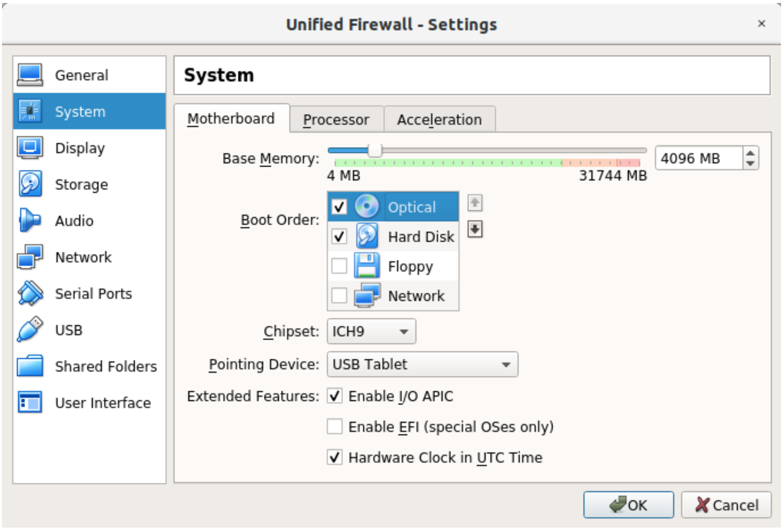
32,00 GB

Select a minimum size of 32 GB and proceed with “Create“.

Now, the entry for your previously created virtual machine appears in the main window of the Oracle VM Virtual Box Manager.
Select the virtual machine by a single click and choose “Settings“ in the upper menu bar.



In the “System” section, check the settings on the tab “Motherboard“, and adjust them according to the following screenshot.



Base Memory: 4096 MB

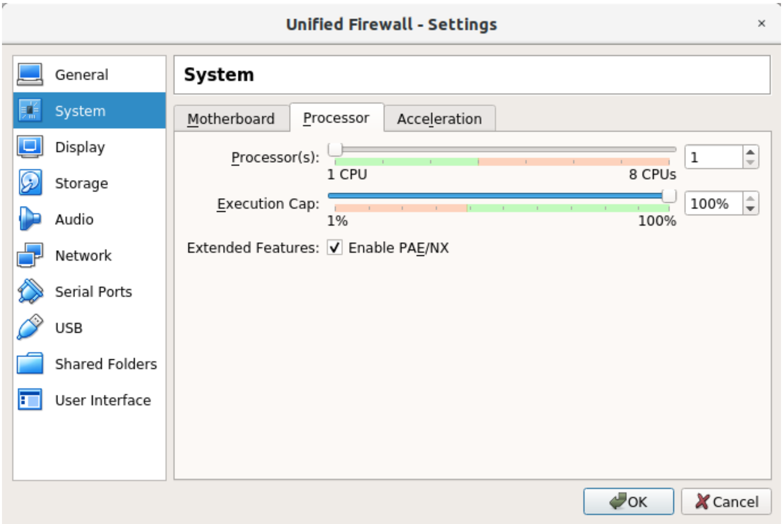
Boot Order:
☑ Optical
☑ Hard Disk
□ Floppy
□ Network

Chipset: ICH9

Pointing Device: USB Tablet

Extended Features:
☑ Enable I/O APIC
□ Enable EFI (special OSes only)
☑ Hardware Clock in UTC Time

Activate the option “Enable PAE/NX“ on the tab “Processor“.



Unified Firewall - Settings

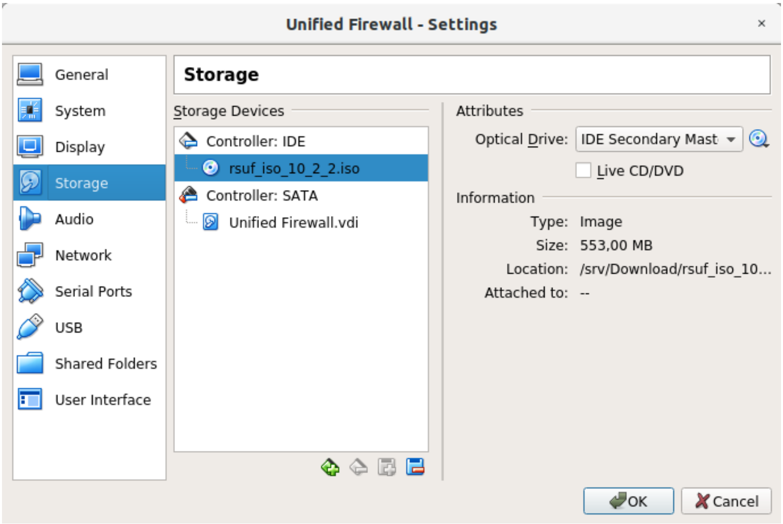
System

Processor(s): 1 (1 CPU – 8 CPUs)

Execution Cap: 100% (1% – 100%)

Extended Features: ☑ Enable PAE/NX

Select “Storage“ from the left menu bar and click on the disc icon under “Attributes“ to select “Virtual optical disk file“.



Unified Firewall - Settings

Storage

Storage Devices

- Controller: IDE
  - rsuf_iso_10_2_2.iso
- Controller: SATA
  - Unified Firewall.vdi

Attributes

Optical Drive: IDE Secondary Mast

□ Live CD/DVD

Information

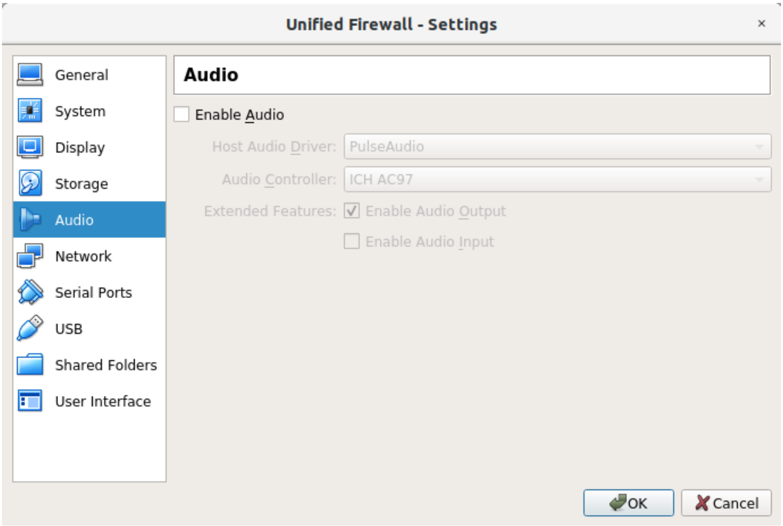
Type: Image

Size: 553,00 MB

Location: /srv/Download/rsuf_iso_10...

Attached to: --

In the menu”Audio“, untag “Enable Audio“.



Unified Firewall - Settings

Audio

□ Enable Audio

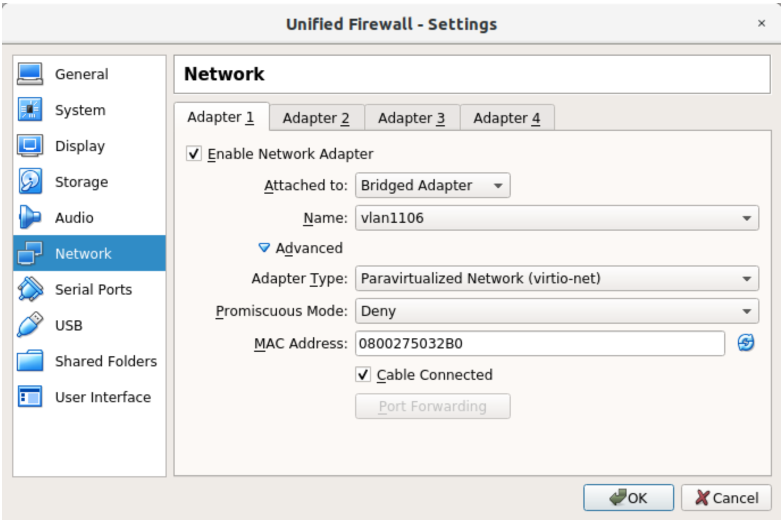
Host Audio Driver: PulseAudio

Audio Controller: ICH AC97

Extended Features: ☑ Enable Audio Output

□ Enable Audio Input

In the menu “network“, select ”Enable Network Adapter“ and configure as shown:



Unified Firewall - Settings

Network

☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: vlan1106

Advanced

Adapter Type: Paravirtualized Network (virtio-net)

Promiscuous Mode: Deny

MAC Address: 0800275032B0

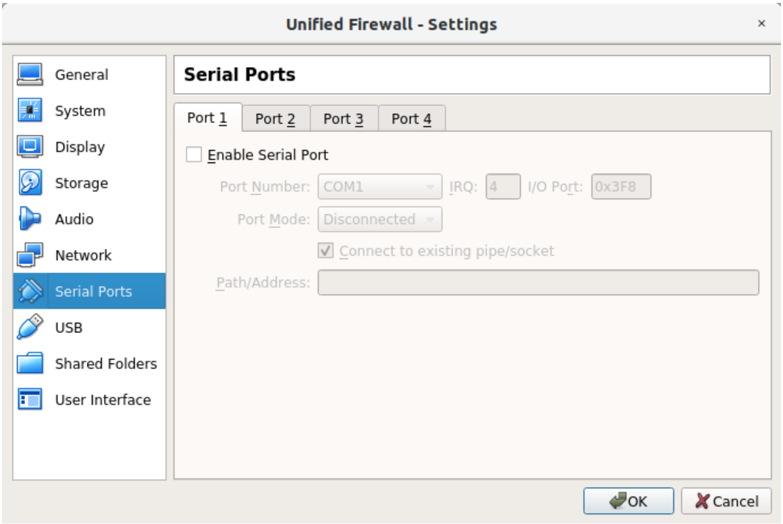
☑ Cable Connected

- → Attached to: user specific, e.g. “Bridged Adapter”
- → Name: user specific; if “Bridged Adapter” has been selected, please choose the appropriate interface.
- → Adapter Type: Paravirtualized Network (virtio-net)
- → Promiscous Mode: Deny
- → Cable Connected: enabled

The MAC address is automatically determined and filled in.

In the tab ”Adapter 2“ choose a name different from adapter 1 for “Attached to”. The remaining entries are configured identically.

In the menu ”Serial Ports“, disable any serial interfaces.



Unified Firewall - Settings

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

□ Enable Serial Port

Port Number: COM1 IRQ: 4 I/O Port: 0x3F8

Port Mode: Disconnected

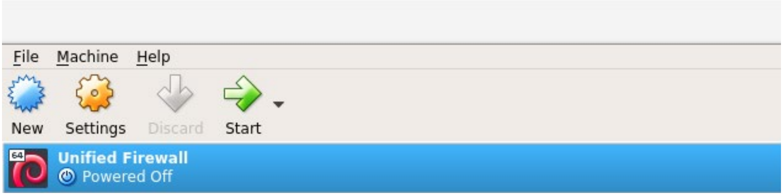
☑ Connect to existing pipe/socket

Path/Address:

In the menus ”USB“, “Shared Folders“, and “User Interface“ confirm the preselected default values.
Select “OK“ to apply the modified settings.

Start of the LANCOM vFirewall in the Oracle VirtualBox Manager

Start your virtual machine in the Oracle VM Virtual Box Manager by selecting the green "Start“ arrow icon.



The further configuration of the LANCOM vFirewall via console is described in the chapter „Final installation of the LANCOM vFirewall on the console“ on page 39.

Installation of the LANCOM vFirewall in Microsoft Hyper-V

Below, the prerequisites and single steps for a successful installation of the LANCOM vFirewall in Microsoft Hyper-V are described.

vFirewall files

The following files are available for the LANCOM vFirewall in the myLANCOM firewall license portal:

→ ISO image file

Prerequisites

The following prerequisites are mandatory for a successful installation of the LANCOM vFirewall under Microsoft Hyper-V:

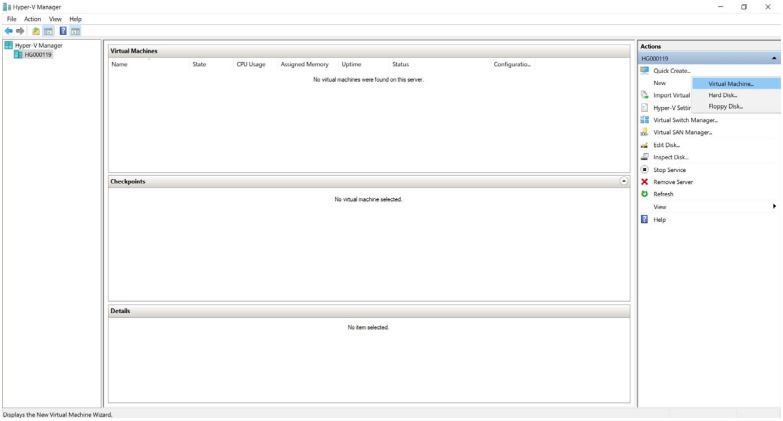
→ The LANCOM vFirewall software has to be available as an ISO image file.
→ Microsoft Hyper-V Manager 10.0 or higher has to be installed on a server with Intel processor.

The virtual machine has to meet the following minimum requirements:

→ 1 ×86 CPU (64 bit) processor
→ 4 GB RAM
→ 30 GB free harddisk space
→ 2 network interfaces

Creating and configuring the LANCOM vFirewall in the Microsoft Hyper-V Manager

Start the Microsoft Hyper-V Manager. On the right side of the screen in the “Actions“ area, first select “New“, then “Virtual Machine“.



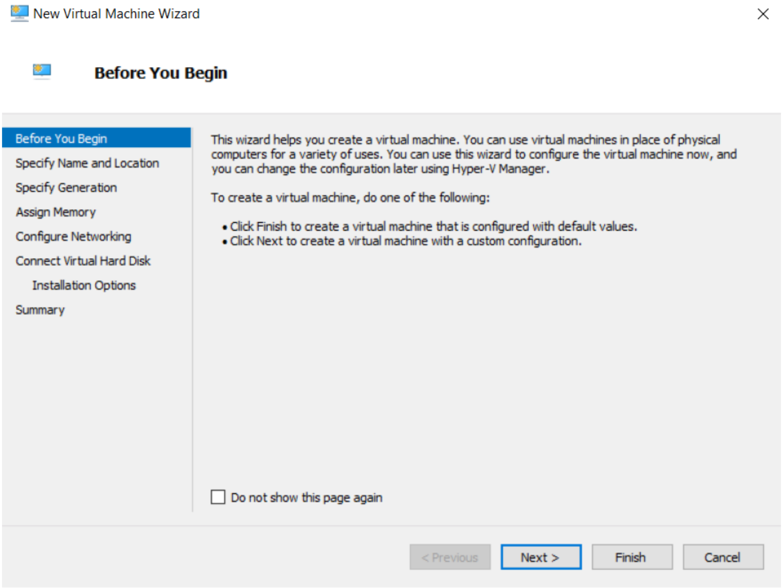
No virtual machines were found on this server.

No virtual machine selected.

No item selected.

Displays the New Virtual Machine Wizard.

The “New Virtual Machine Wizard“ is started. A new window “Before you begin“ opens.



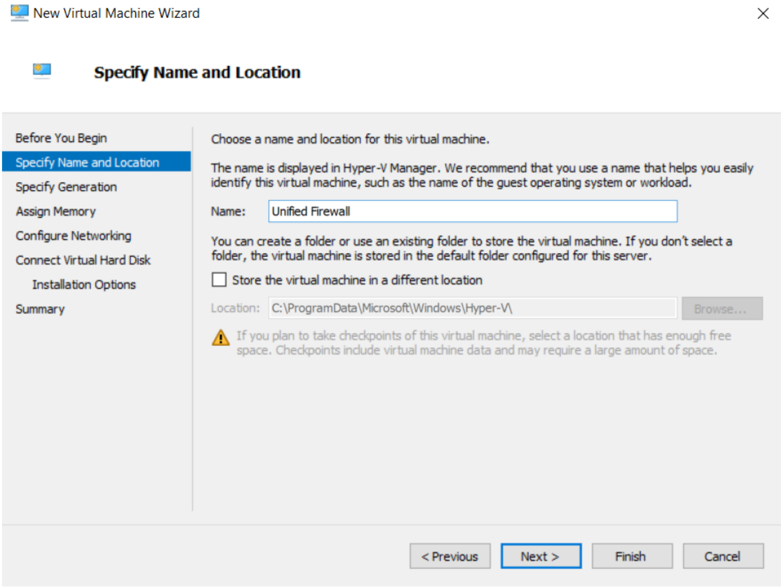
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

Click on “Next“ and choose a name for the virtual machine, e.g. “Unified Firewall“. Confirm with “Next“.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Unified Firewall

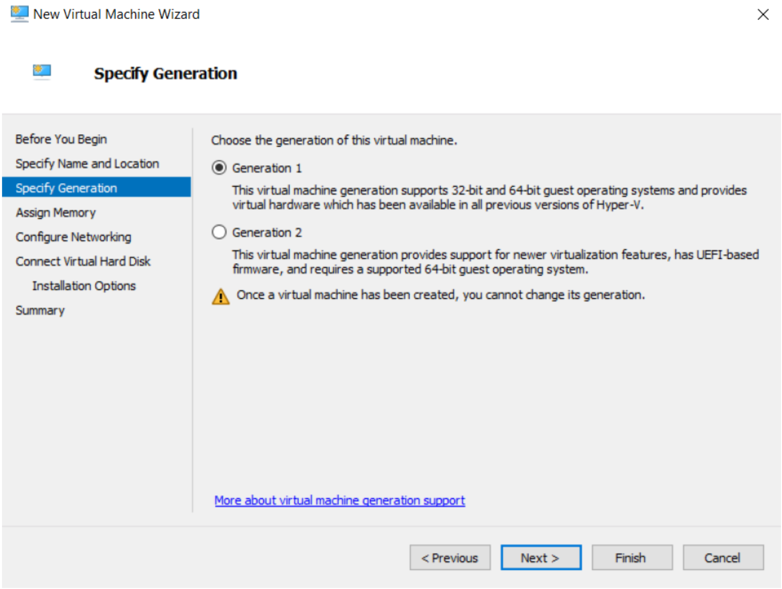
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

In the next step, select ”Generation 1“ and confirm with “Next“.



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

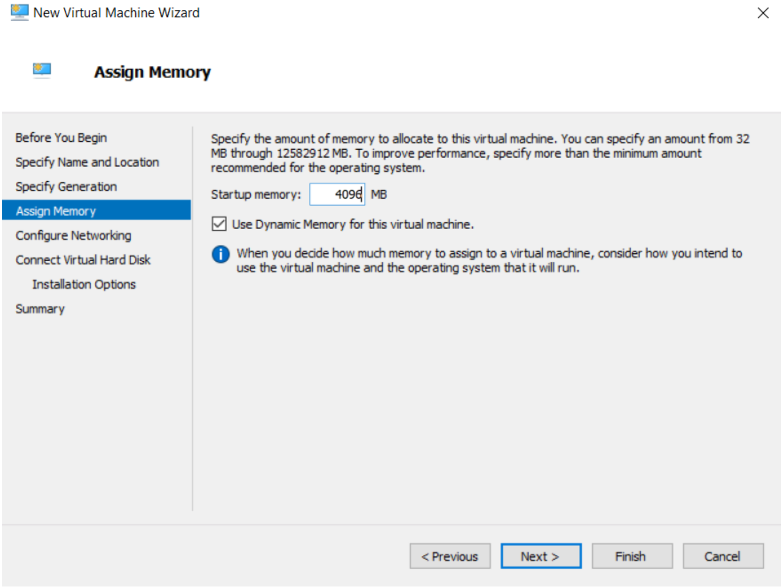
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

More about virtual machine generation support

In the window “Assign Memory“, specify a value of at least 4096 MB as “Startup memory”, and activate “Use Dynamic Memory for this virtual machine“. Confirm with “Next“.



New Virtual Machine Wizard

Assign Memory

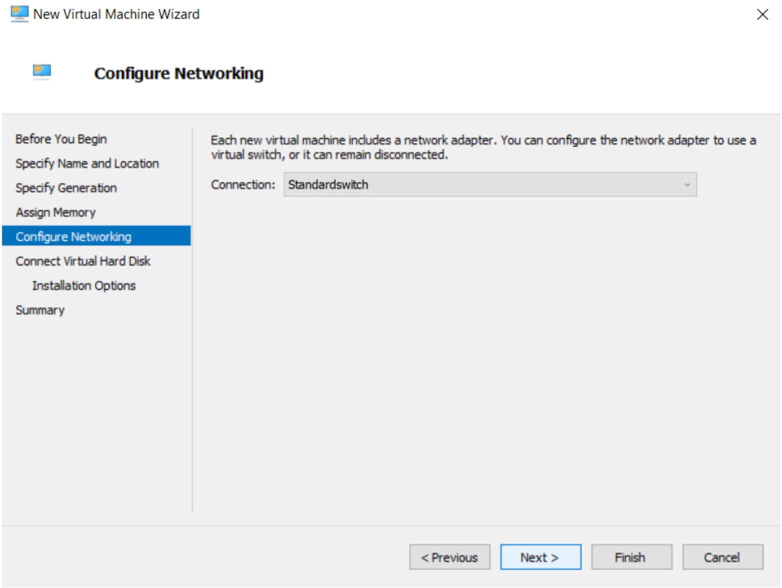
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 4096 MB

☑ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

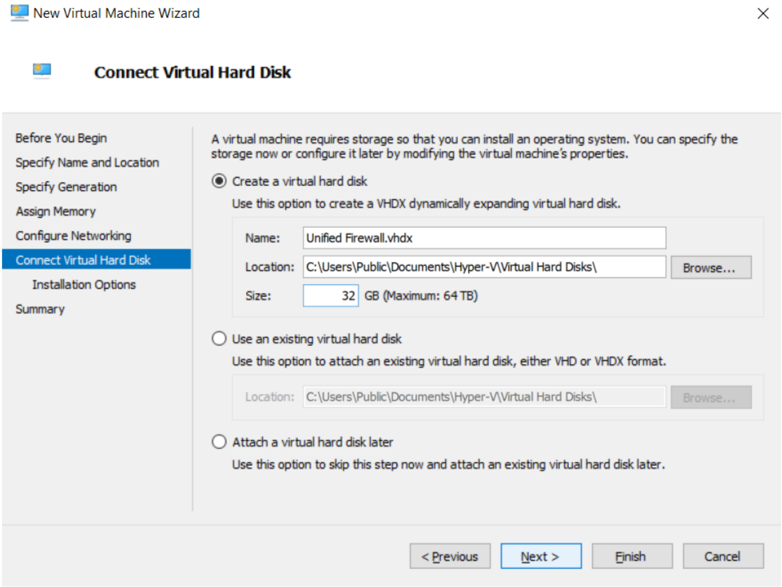
In the next step “Configure Networking“, specify the value “Standardswitch” for “Connection”. Confirm with “Next“.



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Standardswitch

Under “Connect Virtual Hard Disk“, select the option “Create a virtual hard disk“ and a size of 32 GB. Confirm with “Next“.



New Virtual Machine Wizard

Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

● Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: Unified Firewall.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 32 GB (Maximum: 64 TB)

○ Use an existing virtual hard disk

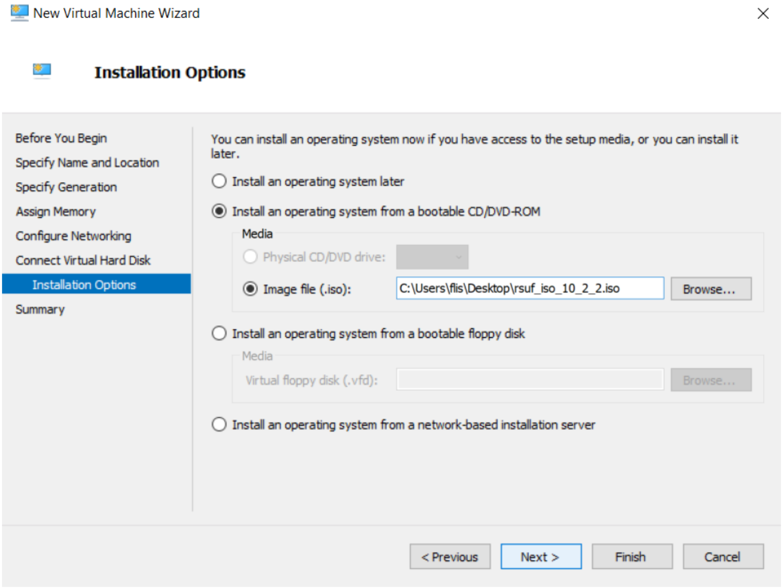
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

In the window ”Installation Options“, activate the option “Install an operating system from a bootable CD/DVD-ROM“ as well as the option ”Image file (.iso)“. Select or confirm the path to the vFirewall image file and confirm with “Next“.



New Virtual Machine Wizard

Installation Options

You can install an operating system now if you have access to the setup media, or you can install it later.

○ Install an operating system later

● Install an operating system from a bootable CD/DVD-ROM

Media

○ Physical CD/DVD drive:

● Image file (.iso): C:\Users\flis\Desktop\rsuf_iso_10_2_2.iso

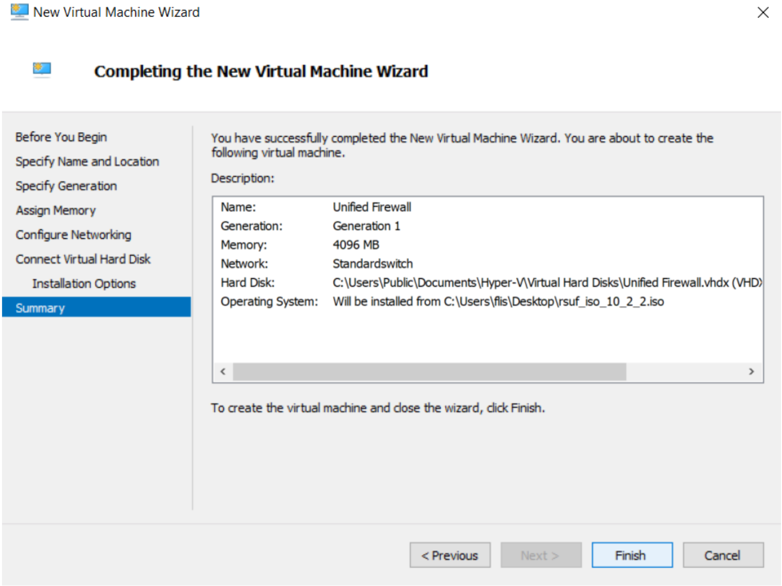
○ Install an operating system from a bootable floppy disk

Media

Virtual floppy disk (.vfd):

○ Install an operating system from a network-based installation server

The final page completes the wizard by displaying an overview of the so far configured parameters. Confirm with “Finish“.



Completing the New Virtual Machine Wizard

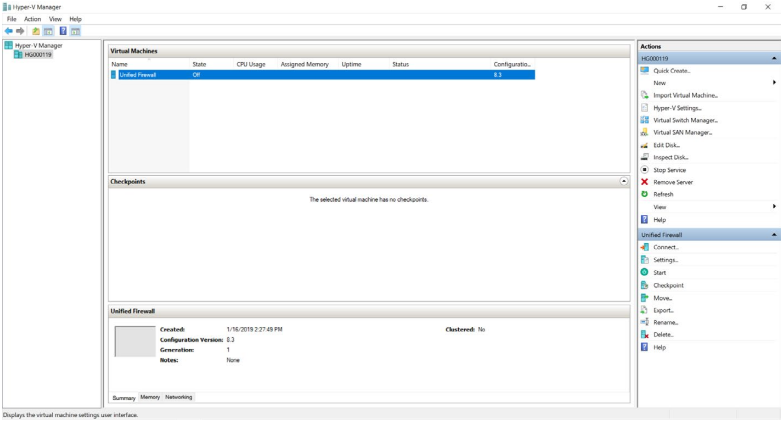
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name:	Unified Firewall
Generation:	Generation 1
Memory:	4096 MB
Network:	Standardswitch
Hard Disk:	C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\Unified Firewall.vhdx (VHD)
Operating System:	Will be installed from C:\Users\flis\Desktop\rsuf_iso_10_2_2.iso

To create the virtual machine and close the wizard, click Finish.

The virtual machine is now created and has to be configured subsequently. For this, select “Settings” in the “Actions“ area of the Hyper-V Manager under “Unified Firewall“.



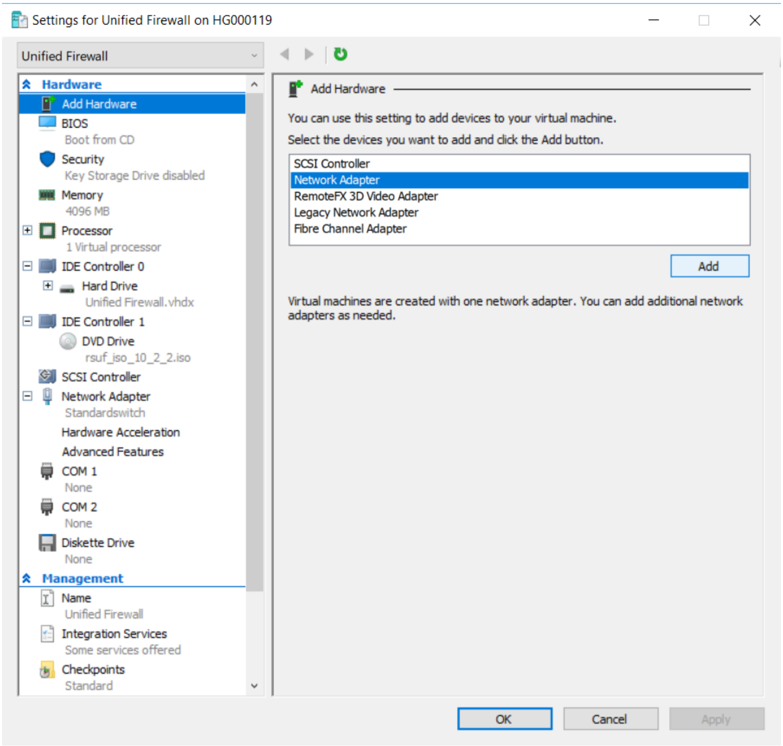
Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuratio...
Unified Firewall	Off					8.3

The selected virtual machine has no checkpoints.

Created: 1/16/2019 2:27:49 PM
Configuration Version: 8.3
Generation: 1
Notes: None
Clustered: No

Displays the virtual machine settings user interface.

The “Settings“ window opens. In the left area under “Hardware”, select the item ”Add Hardware“. Then, in the right area, select ”Network Adapter“. Confirm with “Add“.

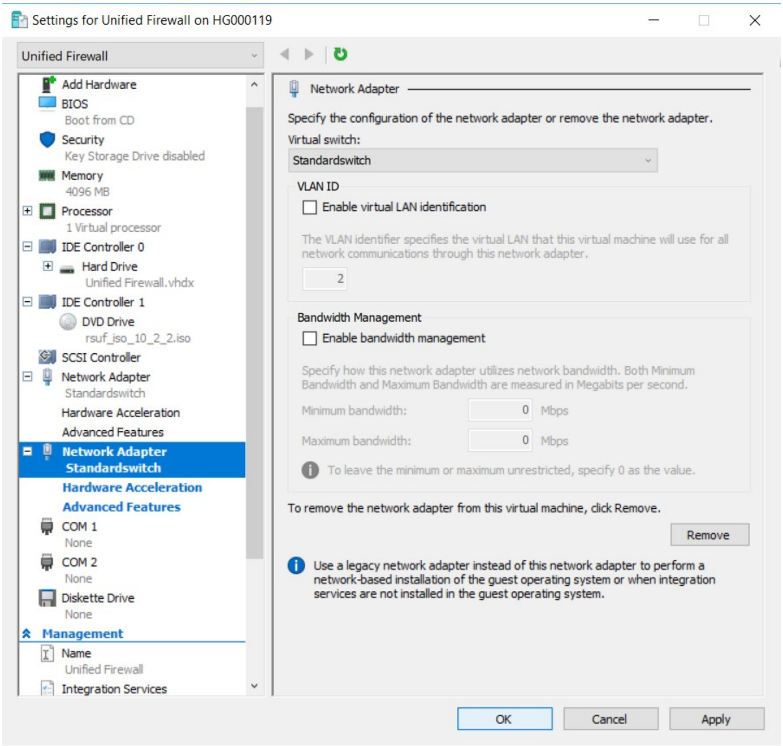


You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

Virtual machines are created with one network adapter. You can add additional network adapters as needed.

In the next window under “Virtual Switch“, select the item “Standardswitch“. A second network adapter shows up in the left area of the window. Confirm with “OK“.



Settings for Unified Firewall on HG000119

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: Standardswitch

VLAN ID

□ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

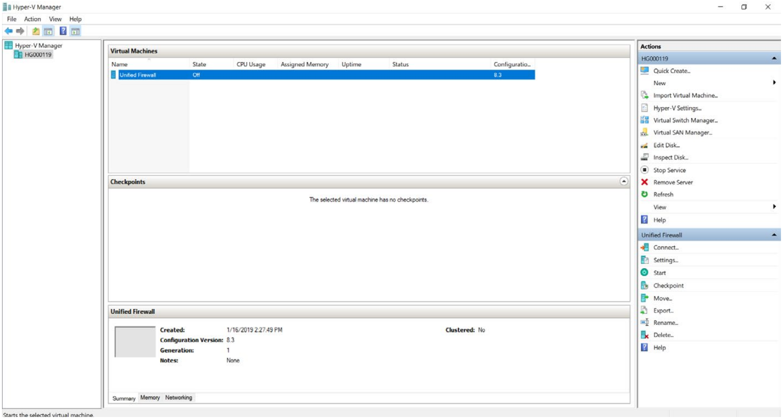
To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

Starting the LANCOM vFirewall in the Microsoft Hyper-V Manager

In the main window of the Microsoft Hyper-V Manager, under “Actions / Unified Firewall“, select the item “Start“, and then”Connect“.



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuratio...
Unified Firewall	Off					8.3

Checkpoints

The selected virtual machine has no checkpoints.

Unified Firewall

Created: 1/16/2019 2:27:49 PM
Configuration Version: 8.3
Generation: 1
Notes: None
Clustered: No

Starts the selected virtual machine.

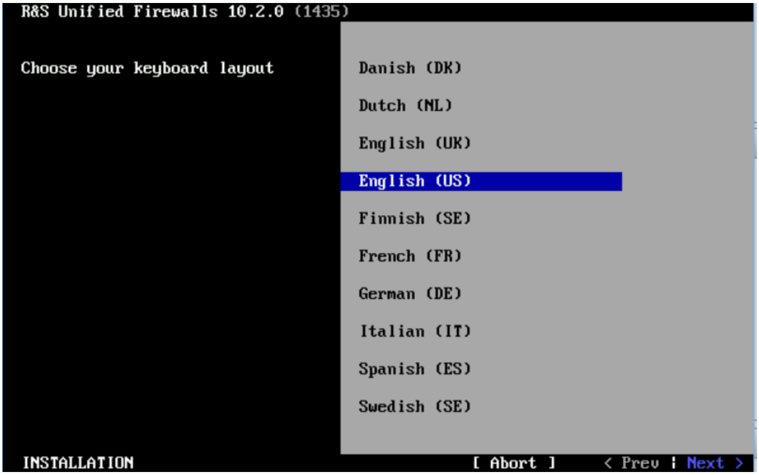
A separate console window pops up. Continue with the installation of the LANCOM vFirewall on the console as described in the next chapter.

Final installation of the LANCOM vFirewall on the console

The following menu navigation on the console is basically valid for all virtual environments described in this installation guide. Variations between these systems are marked by separate screenshots.

After the start of the console the following window appears:

Language selection

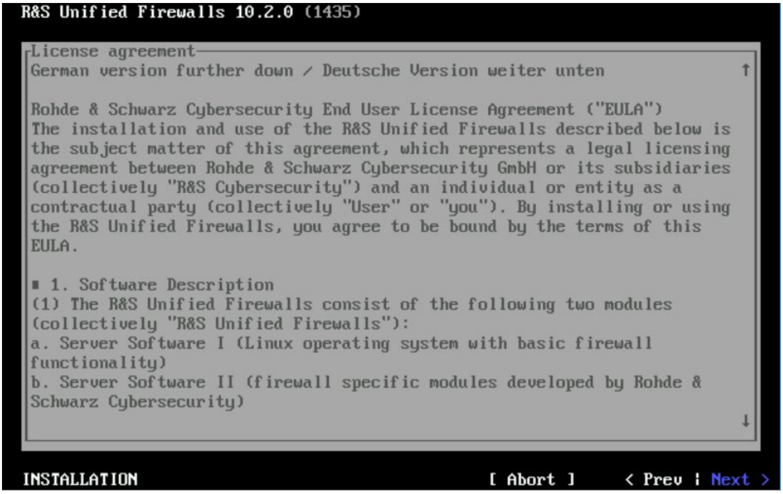


R&S Unified Firewalls 10.2.0 (1435)

Choose your keyboard layout

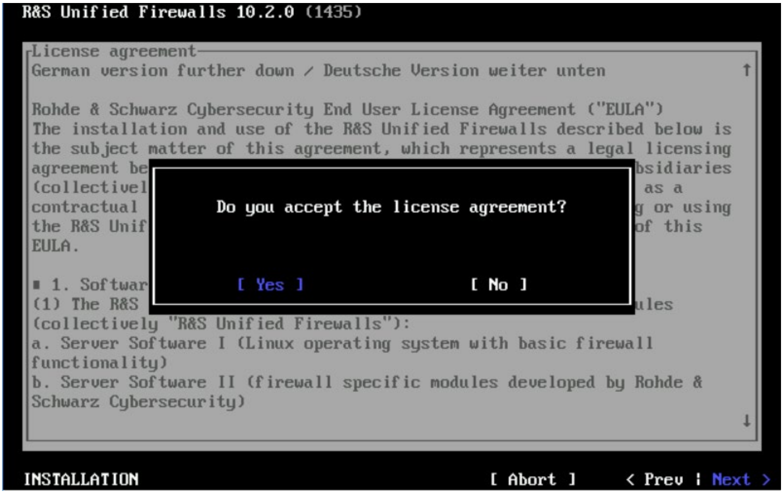
Choose your keyboard language and click on “Next“.

License agreement



```
R&S Unified Firewalls 10.2.0 (1435)

License agreement
German version further down / Deutsche Version weiter unten

Rohde & Schwarz Cybersecurity End User License Agreement ("EULA")
The installation and use of the R&S Unified Firewalls described below is
the subject matter of this agreement, which represents a legal licensing
agreement between Rohde & Schwarz Cybersecurity GmbH or its subsidiaries
(collectively "R&S Cybersecurity") and an individual or entity as a
contractual party (collectively "User" or "you"). By installing or using
the R&S Unified Firewalls, you agree to be bound by the terms of this
EULA.

▪ 1. Software Description
(1) The R&S Unified Firewalls consist of the following two modules
(collectively "R&S Unified Firewalls"):
a. Server Software I (Linux operating system with basic firewall
functionality)
b. Server Software II (firewall specific modules developed by Rohde &
Schwarz Cybersecurity)

INSTALLATION                                [ Abort ]     < Prev ¦ Next >
```

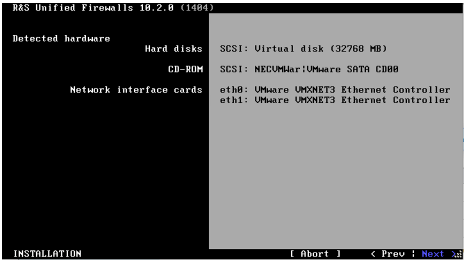
Confirm the license agreement with “Next“ and the following dialog with “Yes”.



```
Do you accept the license agreement?

        [ Yes ]                    [ No ]
```

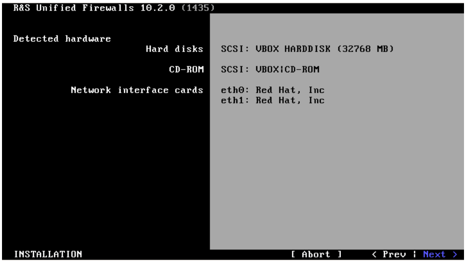
Overview of the detected hardware

→ VMware ESXi:



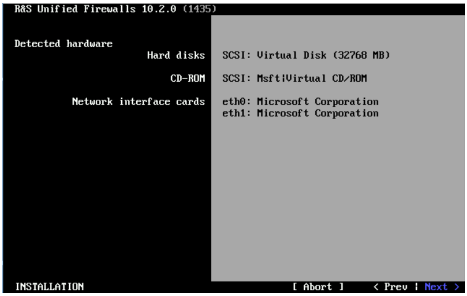
```
R&S Unified Firewalls 10.2.0 (1404)

Detected hardware
                  Hard disks    SCSI: Virtual disk (32768 MB)

                      CD-ROM    SCSI: NECVMWar|VMware SATA CD00

     Network interface cards    eth0: VMware VMXNET3 Ethernet Controller
                                eth1: VMware VMXNET3 Ethernet Controller

INSTALLATION                              [ Abort ]     < Prev | Next >
```

→ Oracle VirtualBox



```
R&S Unified Firewalls 10.2.0 (1435)

Detected hardware
                  Hard disks    SCSI: VBOX HARDDISK (32768 MB)

                      CD-ROM    SCSI: VBOX|CD-ROM

     Network interface cards    eth0: Red Hat, Inc
                                eth1: Red Hat, Inc

INSTALLATION                              [ Abort ]     < Prev | Next >
```

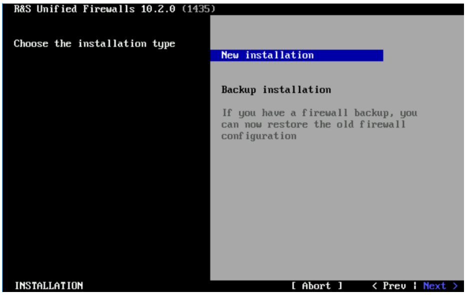
→ Microsoft Hyper-V



```
R&S Unified Firewalls 10.2.0 (1435)

Detected hardware
                  Hard disks    SCSI: Virtual Disk (32768 MB)

                      CD-ROM    SCSI: Msft|Virtual CD/ROM

     Network interface cards    eth0: Microsoft Corporation
                                eth1: Microsoft Corporation

INSTALLATION                              [ Abort ]     < Prev | Next >
```

Respectively, confirm with “Next“.

Selection of the installation type



R&S Unified Firewalls 10.2.0 (1435)

Choose the installation type

New installation

Backup installation

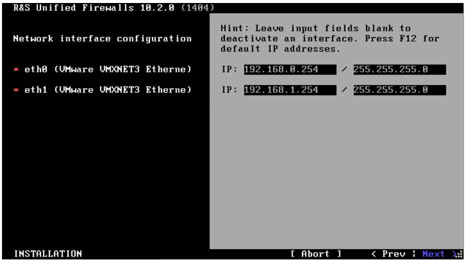
If you have a firewall backup, you can now restore the old firewall configuration

Confirm “New Installation“ with “Next“.

Configuration of the network interfaces

The default IP addresses are allocated to the network interfaces by pressing F12. The following screenshot appears:

→ VMware ESXi



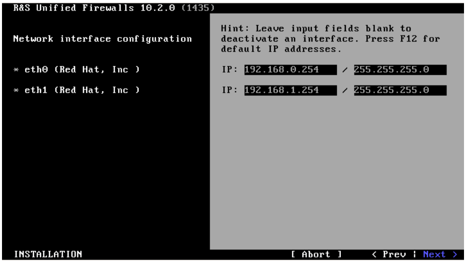
R&S Unified Firewalls 10.0.0 (1404)

Network interface configuration

Hint: Leave input fields blank to deactivate an interface. Press F12 for default IP addresses.

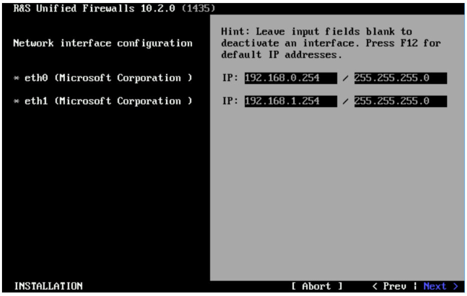
```
* eth0 (VMware VMXNET3 Etherne)    IP: 192.168.0.254 / 255.255.255.0
* eth1 (VMware VMXNET3 Etherne)    IP: 192.168.1.254 / 255.255.255.0
```

→ Oracle VirtualBox



```
R&S Unified Firewalls 10.2.0 (1435)

Network interface configuration        Hint: Leave input fields blank to
                                       deactivate an interface. Press F12 for
                                       default IP addresses.

* eth0 (Red Hat, Inc )                 IP: 192.168.0.254    / 255.255.255.0

* eth1 (Red Hat, Inc )                 IP: 192.168.1.254    / 255.255.255.0

INSTALLATION
```

→ Microsoft Hyper-V



```
R&S Unified Firewalls 10.2.0 (1435)

Network interface configuration        Hint: Leave input fields blank to
                                       deactivate an interface. Press F12 for
                                       default IP addresses.

* eth0 (Microsoft Corporation )        IP: 192.168.0.254    / 255.255.255.0

* eth1 (Microsoft Corporation )        IP: 192.168.1.254    / 255.255.255.0

INSTALLATION
```

Respectively, confirm with “Next“.

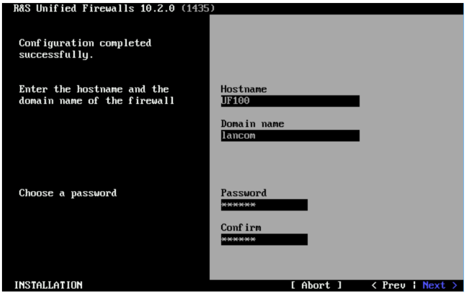
Input dialog for host- and domain name

Configure as follows:

→ Hostname: UF100

→ Domain name: lancom

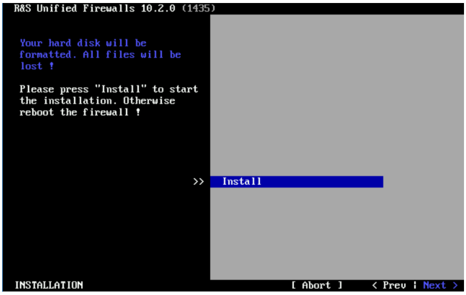
→ Password: freely selectable



```
R&S Unified Firewalls 10.2.0 (1435)

Configuration completed
successfully.

Enter the hostname and the        Hostname
domain name of the firewall       UF100

                                  Domain name
                                  lancom

Choose a password                 Password
                                  ******

                                  Confirm
                                  ******

INSTALLATION                      [ Abort ]   < Prev | Next >
```

Click on “Next“ to confirm your input.

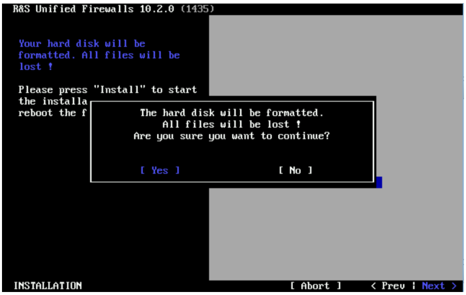
Start of the installation



```
R&S Unified Firewalls 10.2.0 (1435)

Your hard disk will be
formatted. All files will be
lost !

Please press "Install" to start
the installation. Otherwise
reboot the firewall !

                              >>  Install

INSTALLATION                      [ Abort ]   < Prev | Next >
```

Confirm with “Next“.

Confirm formatting of the virtual harddisk

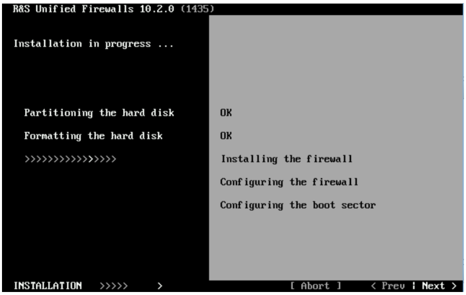


```
R&S Unified Firewalls 10.2.0 (1435)

Your hard disk will be
formatted. All files will be
lost !

Please press "Install" to start
the installa
reboot the f     The hard disk will be formatted.
                     All files will be lost !
                 Are you sure you want to continue?


                    [ Yes ]               [ No ]

INSTALLATION                         [ Abort ]     < Prev | Next >
```

Confirm the question to format the virtual harddisk with “Yes“.

Proceeding the installation

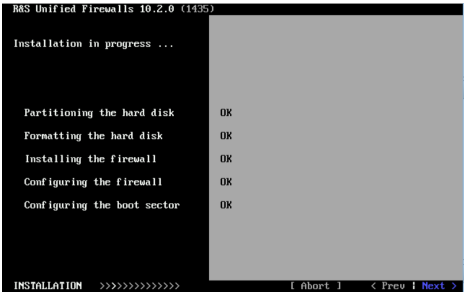
The installation is now executed and can take some time (up to 10 minutes), typically only a few minutes.



```
R&S Unified Firewalls 10.2.0 (1435)

Installation in progress ...



  Partitioning the hard disk           OK

  Formatting the hard disk             OK

  >>>>>>>>>>>>>>>>                     Installing the firewall

                                       Configuring the firewall

                                       Configuring the boot sector




INSTALLATION   >>>>>     >           [ Abort ]     < Prev | Next >
```

Finishing the installation

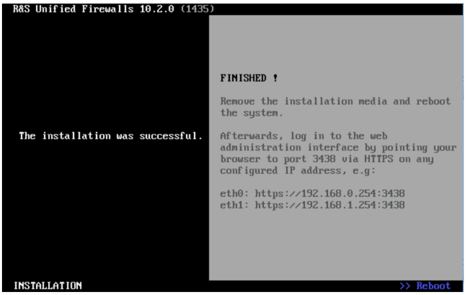
After successful installation you will notice the following screen:



```
R&S Unified Firewalls 10.2.0 (1435)

Installation in progress ...


  Partitioning the hard disk        OK
  Formatting the hard disk          OK
  Installing the firewall           OK
  Configuring the firewall          OK
  Configuring the boot sector       OK


INSTALLATION   >>>>>>>>>>>>>>            [ Abort ]     < Prev ¦ Next >
```

Confirm with „Next“ to get to the next screen.

Restart request

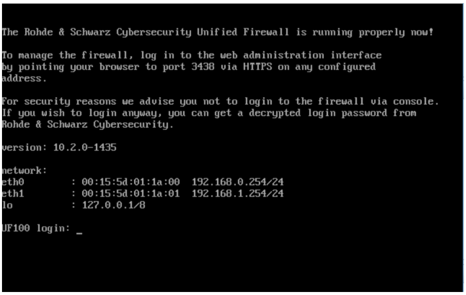


```
R&S Unified Firewalls 10.2.0 (1435)

                                    FINISHED !

                                    Remove the installation media and reboot
                                    the system.

 The installation was successful.   Afterwards, log in to the web
                                    administration interface by pointing your
                                    browser to port 3438 via HTTPS on any
                                    configured IP address, e.g:

                                    eth0: https://192.168.0.254:3438
                                    eth1: https://192.168.1.254:3438


INSTALLATION                                                      >> Reboot
```

Confirm the restart request with “Reboot“.

Completing the LANCOM vFirewall installation

After the restart the following screen occurs:

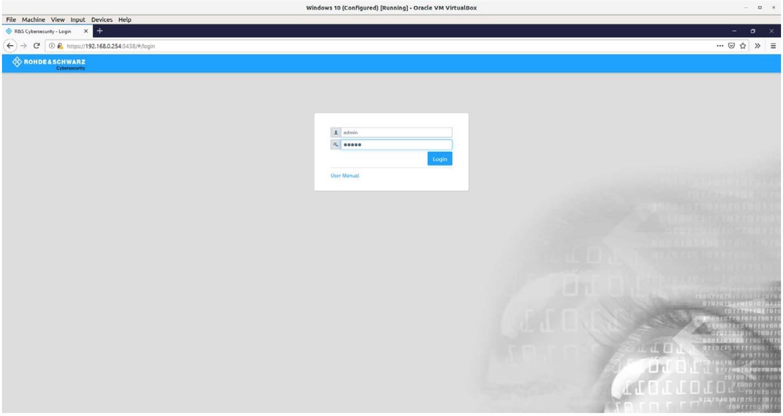


```
The Rohde & Schwarz Cybersecurity Unified Firewall is running properly now!

To manage the firewall, log in to the web administration interface
by pointing your browser to port 3438 via HTTPS on any configured
address.

For security reasons we advise you not to login to the firewall via console.
If you wish to login anyway, you can get a decrypted login password from
Rohde & Schwarz Cybersecurity.

version: 10.2.0-1435

network:
eth0          : 00:15:5d:01:1a:00  192.168.0.254/24
eth1          : 00:15:5d:01:1a:01  192.168.1.254/24
lo            : 127.0.0.1/8

UF100 login: _
```

The installation has now completed. A console login is not necessary. Follow the information according the user login in the browser via the predefined interfaces, as shown in the screenshot.

Logging in to the LANCOM vFirewall via web interface

Start a web browser on a computer which is located in the subnet of the vFirewall and invoke the LANCOM vFirewall web interface as follows:
For connecting to the network interface eth0 please enter:
https://192.168.0.254:3438
or for network interface eth1:
https://192.168.1.254:3438
The login window of your LANCOM vFirewall appears. Enter **admin** both for username and password.



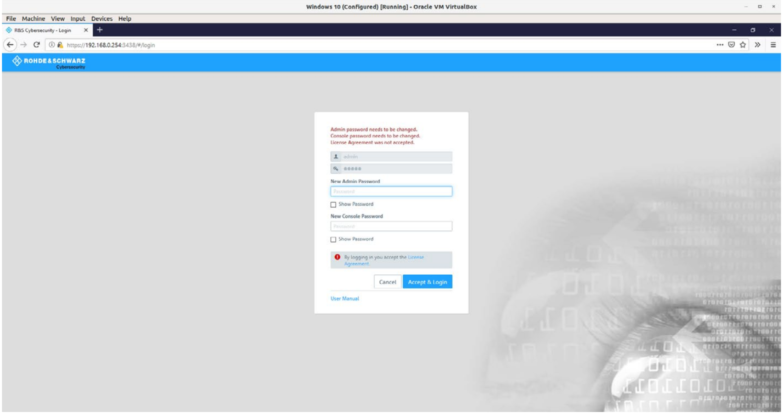
Windows 10 (Configured) [Running] - Oracle VM VirtualBox

https://192.168.0.254:3438/#/login

admin

●●●●●

You are asked to create a new password.


Windows 10 (Configured) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
R&S Cybersecurity - Login
https://192.168.0.254:3438/#/login
ROHDE&SCHWARZ Cybersecurity

Admin password needs to be changed.
Console password needs to be changed.
License Agreement was not accepted.

admin

●●●●●

New Admin Password

Password

□ Show Password

New Console Password

Password

□ Show Password

By logging in you accept the License Agreement.

Cancel
Accept & Login
User Manual

After creating the new password you are automatically logged in and the web interface of your LANCOM vFirewall shows up. Now you can continue with either the Setup Wizard or a manual setup.

Setup tutorials

Here are some helpful videos and tutorials to help you set up your LANCOM vFirewall:

https://www.lancom-systems.com/uf-tutorials

Alternatively, you can scan this QR code to view it on your smartphone:

LANCOM Service & Support

By choosing the LANCOM vFirewall you have opted for maximum reliability. In the unfortunate event that you should have a problem, you are in good hands with us!

LANCOM Support

Support from reseller or distributor
You can contact your reseller or distributor for support:
www.lancom-systems.com/how-to-buy

Online
The LANCOM Knowledge Base is always available via our website:
knowledgebase.lancom-systems.com
You will also find explanations of all the functions of your LANCOM device in the documentation of the operating system used (LCOS FX):
www.lancom-systems.com/publications

Firmware
The latest versions of the LCOS FX firmware, tools, and documentation are available for download in the myLANCOM firewall license portal. You can also manage, activate, and extend your firewall licenses there:
my.lancom-systems.com/mylancom/lizenzportal/downloads

Partner support
Our partners get additional support access according to their partner level. More information can be found on our website:
www.lancom-systems.com/lancommunity

LANCOM Service

Extras for your individual requirements
LANCOM Systems offers additional support as required to protect your devices in the long term. LANcare products, for example, provide increased protection during the entire product lifecycle in the form of manufacturer support with guaranteed service and response times as well as security updates. Find the right LANcare product here:
www.lancom-systems.com/products/services-support/lancare
For individual support, e.g. with network problems or configurations, you will find customized services directly from LANCOM Systems here:
www.lancom-systems.com/products/services-support/services

Your LANCOM Team

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Germany
info@lancom.de
www.lancom-systems.com