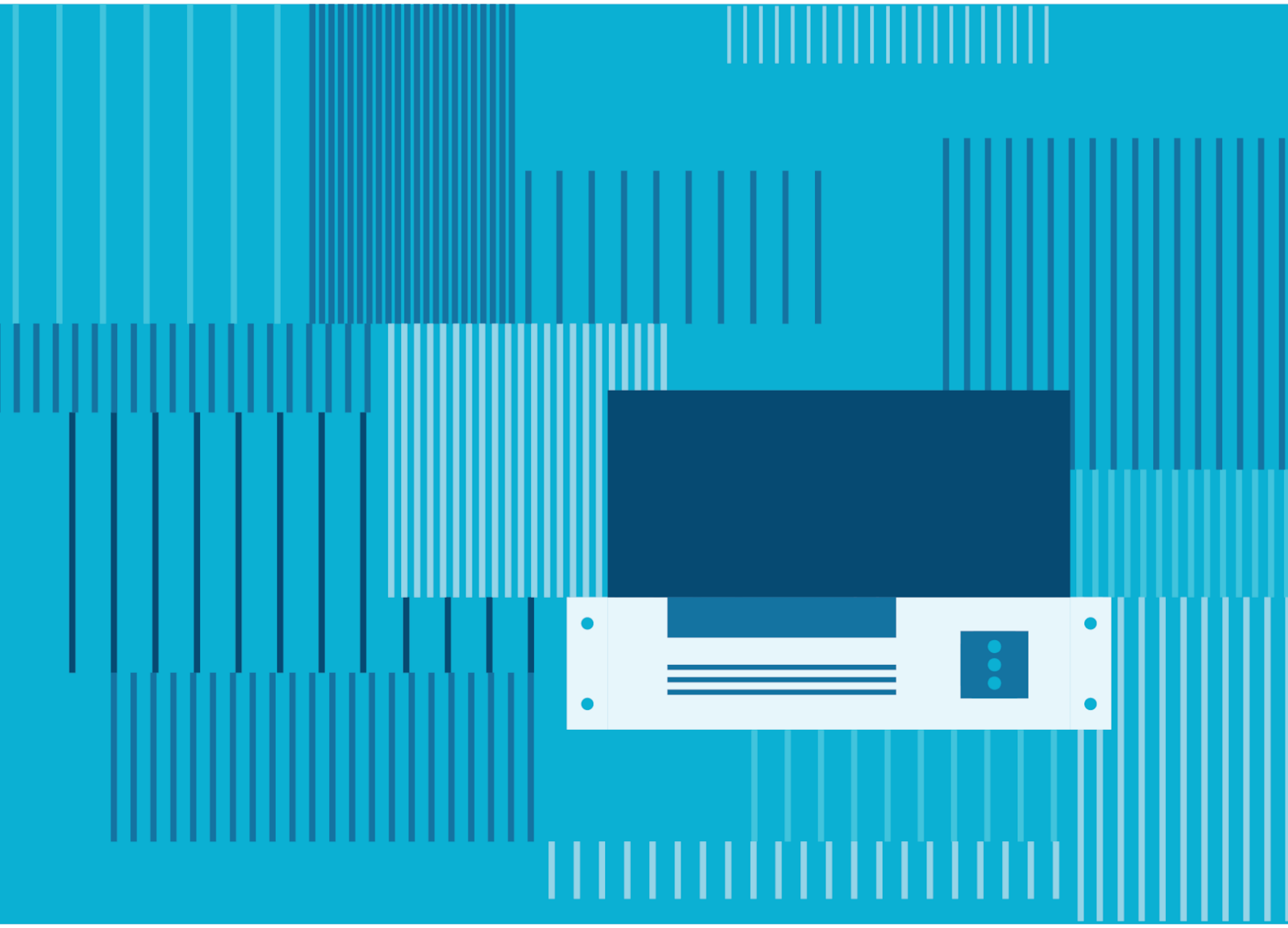
ENDPOINT PROTECTOR | by CoSoSys

Virtual and Hardware Appliance

User Manual



Version: 5.0
28 November 2023

Table of Contents

Document Changelog

Version	Date	Notes
1.0	2020	The document was created.
2.0	16 May 2022	The document was updated with the current template.
3.0	19 Jul 2022	Images from chapters Endpoint Protector Configuration, Server Information, and Maintenance and Support were updated.
4.0	11 Nov 2022	Deleted the Installing Root Certificate to Browsers chapter.
5.0	28 Nov 2023	Revised chapter 4 (Genius Chando) Legal approved

1. Endpoint Protector Virtual Appliance formats

The Endpoint Protector Virtual Appliance is available in different formats and for various platforms. The table below provides a list of supported virtual environments, versions, and main formats.

1.1. Table

In addition to the Virtual Environments mentioned above, the Endpoint Protector Virtual Appliance can also be run on older versions of the virtualization software. This makes testing and implementation as easy as possible. Additional information can be found in the following chapters.

Supported Virtual Environments	Version	.OVF	.OVA	.VMX	.VHD	.PVM	.XVA
VMware Player	7.1.0	●	●	●			
VMware Workstation	11.1.0	●	●	●			
Oracle VM VirtualBox	5.0.28	●	●				
VMware vSphere (ESXi)	6.0.0	●	●				
VMware Fusion Professional	7.1.3	●	●				
Hyper-V Manager Windows Server 2016	10.0.14393.0				●		
Parallels Desktop	11.1.3					●	
Citrix XenCenter	6.2						●

Note: The most commonly used format is **OVF** (Open Virtualization Format) as it is compatible with the majority of the virtualization software.

1.2. Format supported by Virtualization Software

In addition to the virtualization software listed in the previous table, these formats are also supported by the following:

1. **OVF and OVA**
   - VMware Workstation 11.1
   - VMware Player 5.0 (or higher)
   - VMware Fusion 7.1.2
   - VMware ESXi 5.1 (or higher)
   - Oracle VM VirtualBox
   - Citrix XenCenter 6.2
2. **VHD**
   - Microsoft Hyper-V 6.1.7601.17514
   - Microsoft Hyper-V 6.3.9600.16384
3. **PVM**
   - Parallels Desktop 10.2.1
4. **XVA**
   - Citrix XenServer 5.5
   - Citrix XenServer 6.0
5. **VMX**
   - VMware Player 5.0 (or higher)
   - VMware Workstation 9.0 (or higher)

Note: The .VMX virtual appliance is set to run on the latest VMware Workstation version (v11.x.x) and the latest VMware Player version (v7.x.x).

To run the virtual appliances on older VMware Workstation / VMware Player versions, follow these steps:

1. Extract the .zip archive and go to the extract location;
2. Click to edit the .VMX file using a text editor;
3. Search for the "virtualHW.version" field;
4. Replace the default version (default = 11) to the new version
   - if you want to run the .VMX virtual appliance on VMware Workstation v9.x.x or VMware Player v5.x.x, then virtualHW.version = "9"
   - if you want to run the .VMX virtual appliance on VMware Workstation v10.x.x or VMware Player v6.x.x, then virtualHW.version = "10"
5. Save the changes and close the text editor;
6. Import the virtual image;
7. Play the virtual machine.

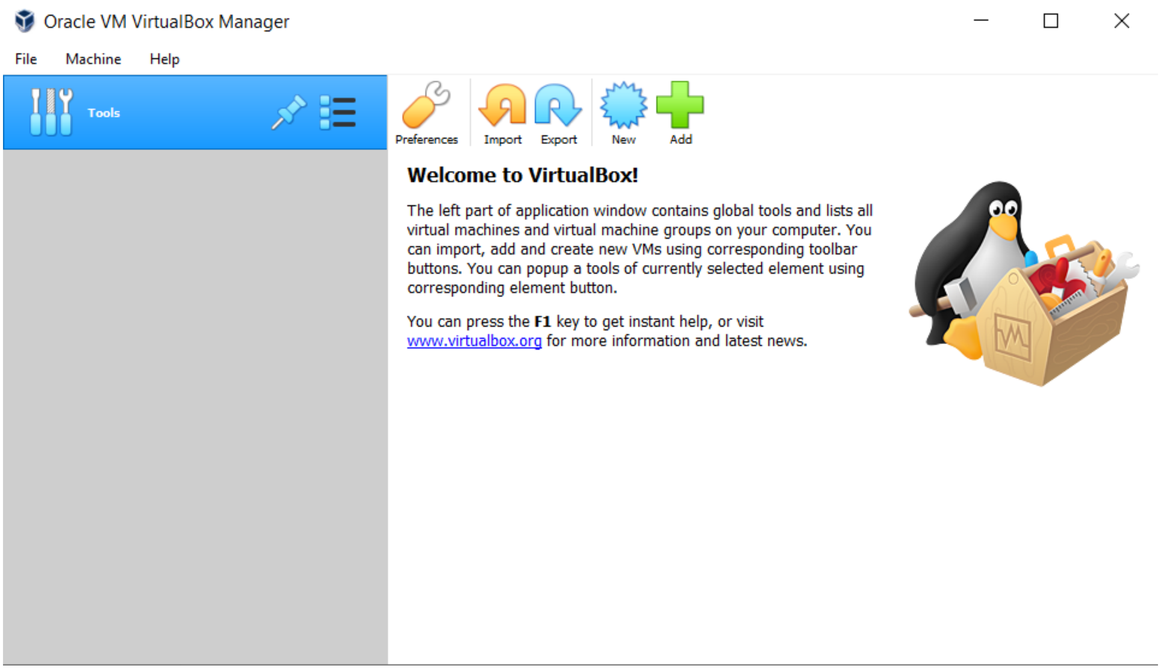
2. Implement using the OVF format

There are several options to implement the Endpoint Protector Virtual Appliance using the OVF format.

2.1. Oracle VM VirtualBox

To implement using the Oracle VM VirtualBox, follow these steps:

1. Unzip the downloaded package;
2. Open **VirtualBox;**

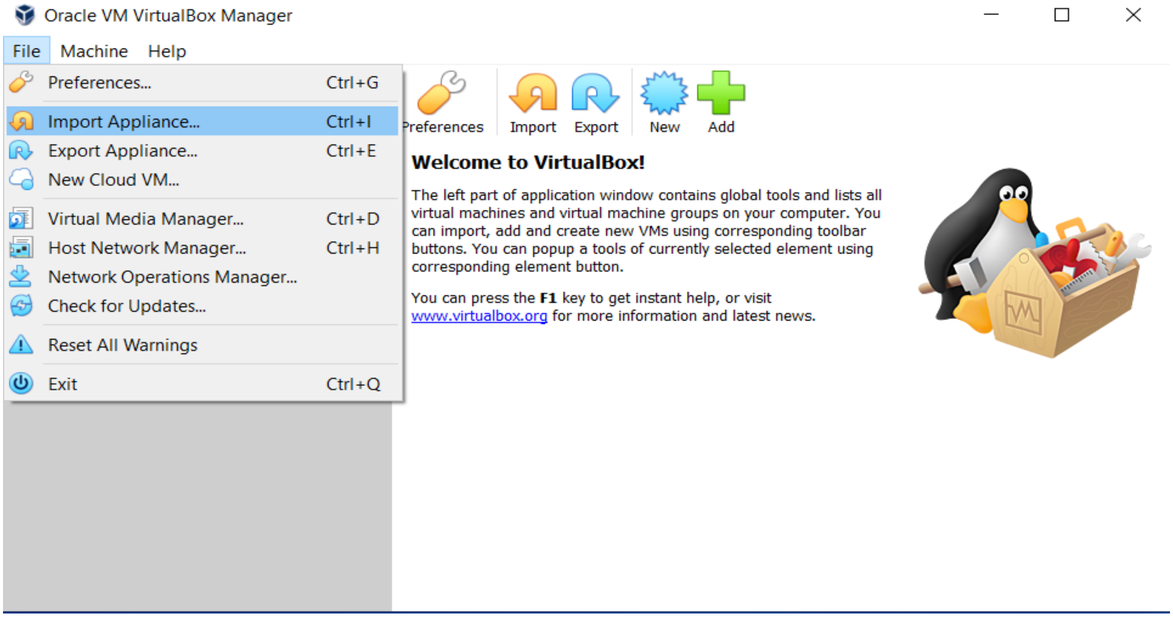


Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

3. Go to **File** and select **Import Appliance**;



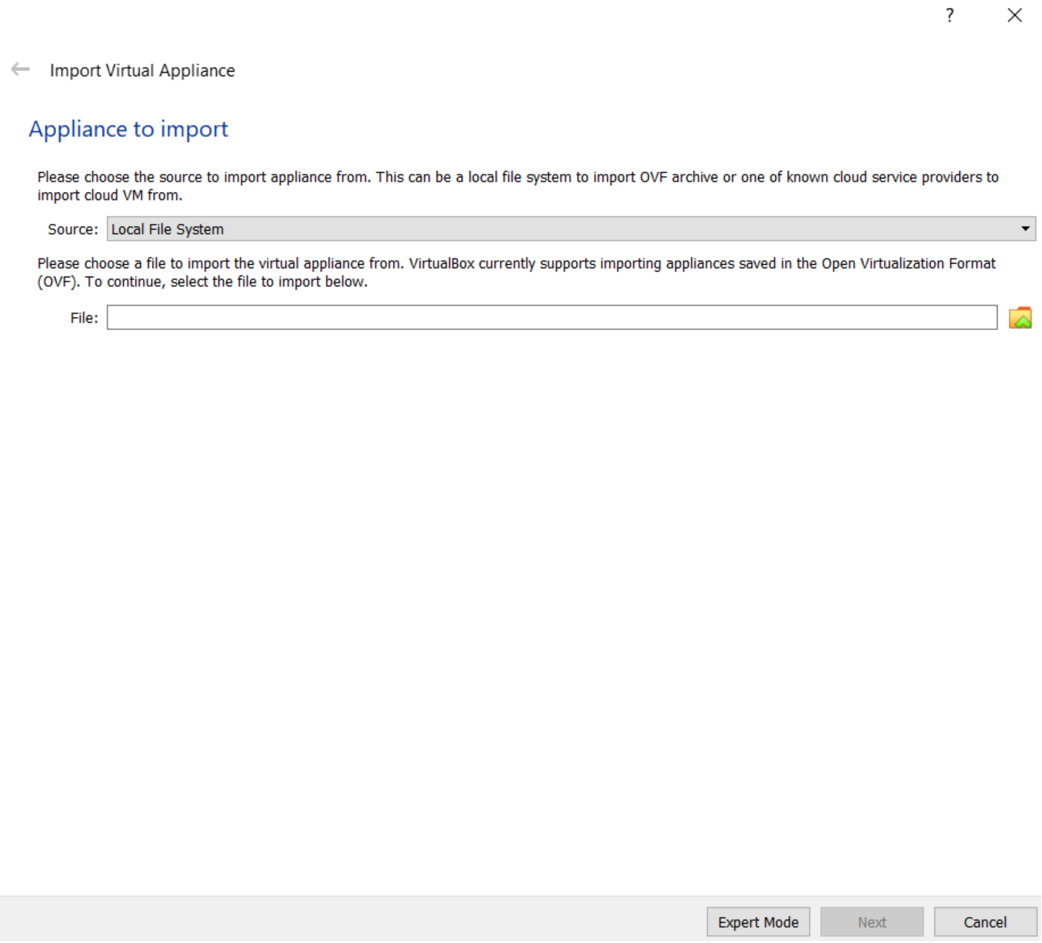
Welcome to VirtualBox!

The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
New Cloud VM...
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+H
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Preferences
Import
Export
New
Add

4. On the **Appliance to import** page, click the **File icon**, browse and select the OVF file from the extracted zip;



Import Virtual Appliance

Appliance to import

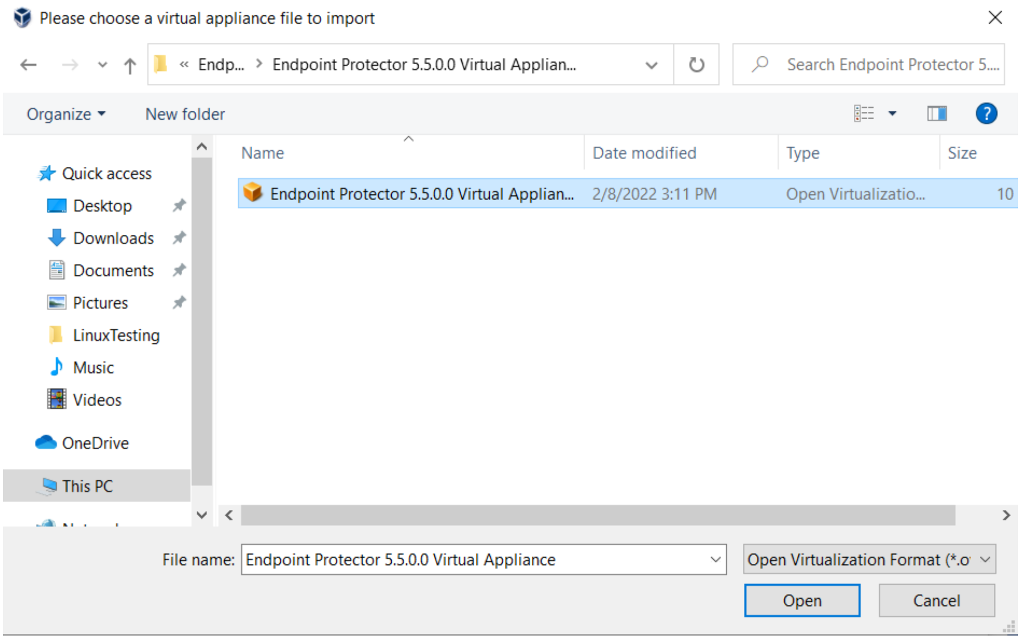
Please choose the source to import appliance from. This can be a local file system to import OVF archive or one of known cloud service providers to import cloud VM from.

Source: Local File System

Please choose a file to import the virtual appliance from. VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

File:

5. Click **Open;**



Please choose a virtual appliance file to import

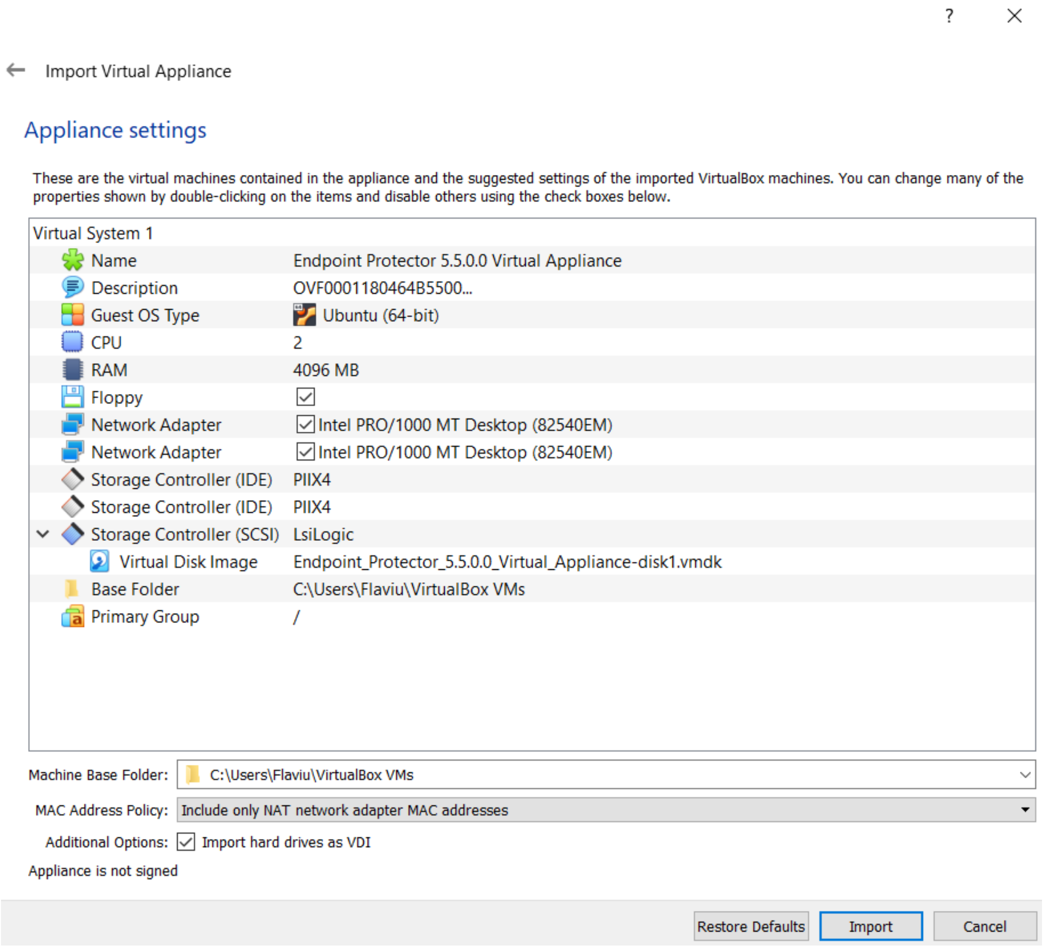
« Endp... › Endpoint Protector 5.5.0.0 Virtual Applian...

Name	Date modified	Type	Size
Endpoint Protector 5.5.0.0 Virtual Applian...	2/8/2022 3:11 PM	Open Virtualizatio...	10

File name: Endpoint Protector 5.5.0.0 Virtual Appliance

Open Virtualization Format (*.o

6. Click **Import;**



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	Endpoint Protector 5.5.0.0 Virtual Appliance
Description	OVF0001180464B5500...
Guest OS Type	Ubuntu (64-bit)
CPU	2
RAM	4096 MB
Floppy	☑
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Network Adapter	☑ Intel PRO/1000 MT Desktop (82540EM)
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SCSI)	LsiLogic
Virtual Disk Image	Endpoint_Protector_5.5.0.0_Virtual_Appliance-disk1.vmdk
Base Folder	C:\Users\Flaviu\VirtualBox VMs
Primary Group	/

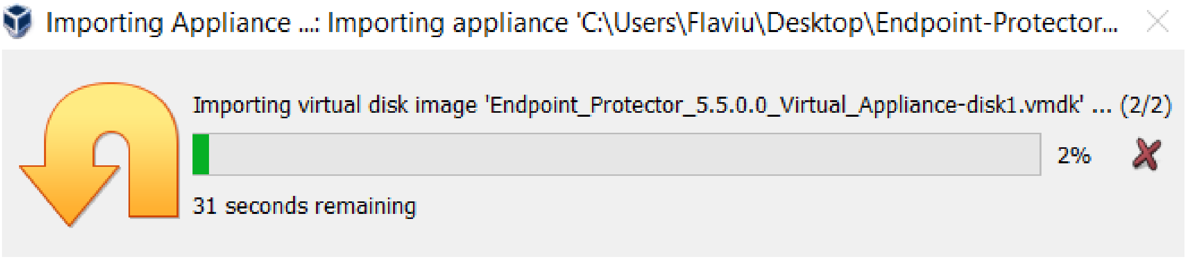
Machine Base Folder: C:\Users\Flaviu\VirtualBox VMs

MAC Address Policy: Include only NAT network adapter MAC addresses

Additional Options: ☑ Import hard drives as VDI

Appliance is not signed

7. Wait for the import displayed by the progress bar;



Importing Appliance ...: Importing appliance 'C:\Users\Flaviu\Desktop\Endpoint-Protector...

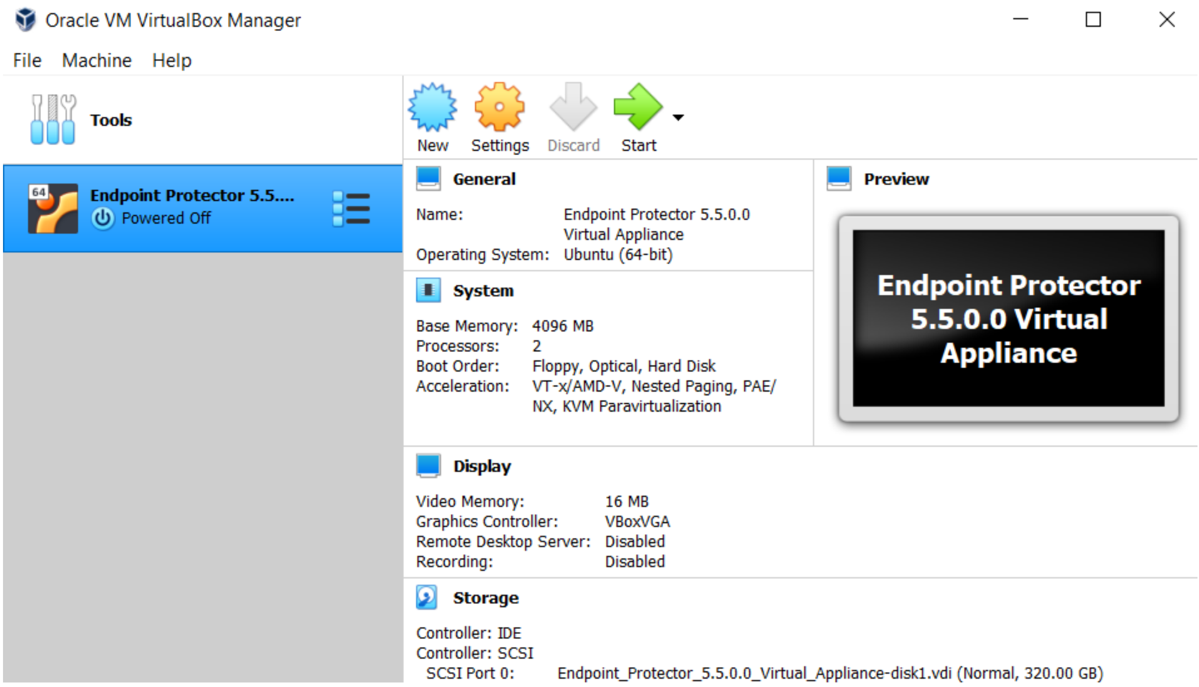
Importing virtual disk image 'Endpoint_Protector_5.5.0.0_Virtual_Appliance-disk1.vmdk' ... (2/2)

2%

31 seconds remaining

At this point, the virtual machine is ready for use.

Follow the Endpoint Protector Appliance User Manual from this point on.



Oracle VM VirtualBox Manager
File
Machine
Help
Tools
New
Settings
Discard
Start
Endpoint Protector 5.5....
Powered Off

General

Name: Endpoint Protector 5.5.0.0 Virtual Appliance
Operating System: Ubuntu (64-bit)

System

Base Memory: 4096 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Preview

Endpoint Protector 5.5.0.0 Virtual Appliance

Display

Video Memory: 16 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

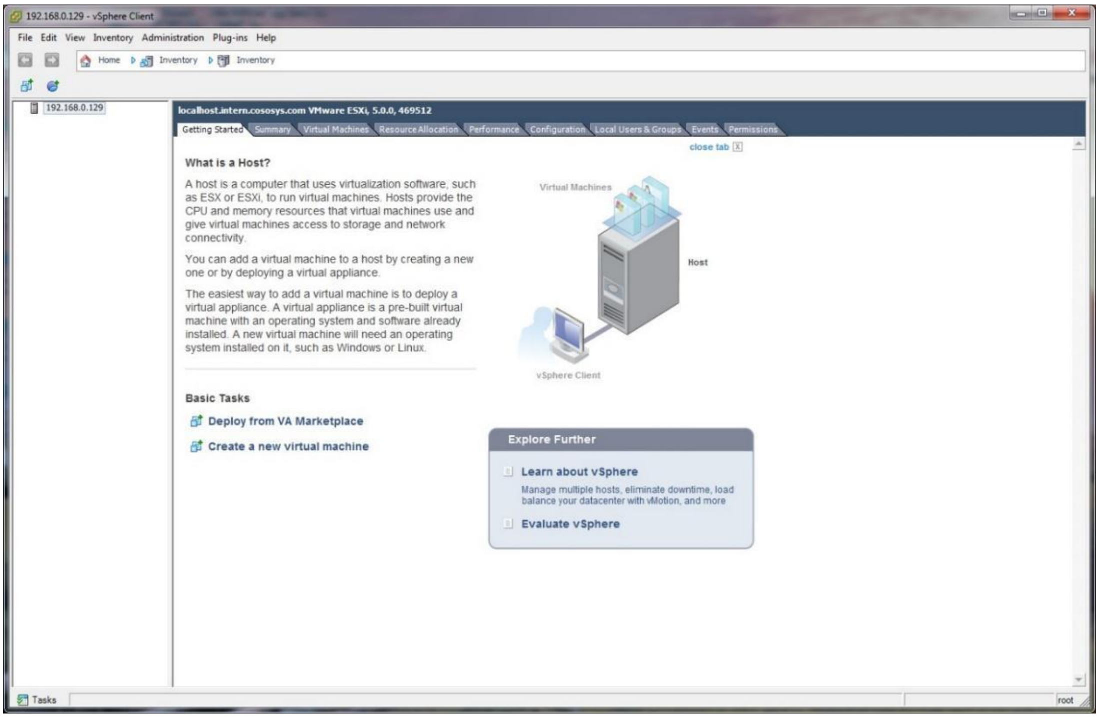
Storage

Controller: IDE
Controller: SCSI
SCSI Port 0: Endpoint_Protector_5.5.0.0_Virtual_Appliance-disk1.vdi (Normal, 320.00 GB)

2.2. VMware vSphere

To implement using the VMware vShpere, follow these steps:

1. Unzip the downloaded package;
2. Start **vSphere**;


192.168.0.129 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
192.168.0.129
localhost.intern.cososys.com VMware ESXi, 5.0.0, 469512
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
close tab
Virtual Machines
Host
vSphere Client
Tasks
root

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

Deploy from VA Marketplace

Create a new virtual machine

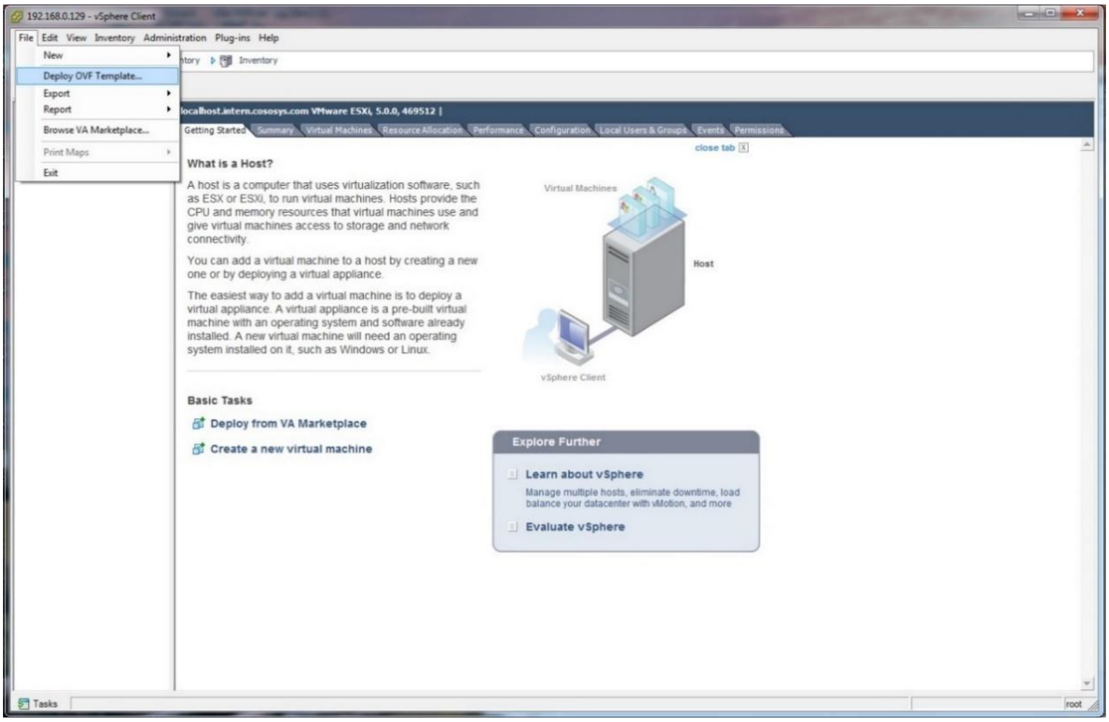
Explore Further

Learn about vSphere

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

Evaluate vSphere

3. Go to **File** and select **Deploy OVF Template**;


192.168.0.129 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
New
Deploy OVF Template...
Export
Report
Browse VA Marketplace...
Print Maps
Exit
Inventory
localhost.intern.cososys.com VMware ESXi, 5.0.0, 469512
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions
close tab
Virtual Machines
Host
vSphere Client
Tasks
root

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

Deploy from VA Marketplace

Create a new virtual machine

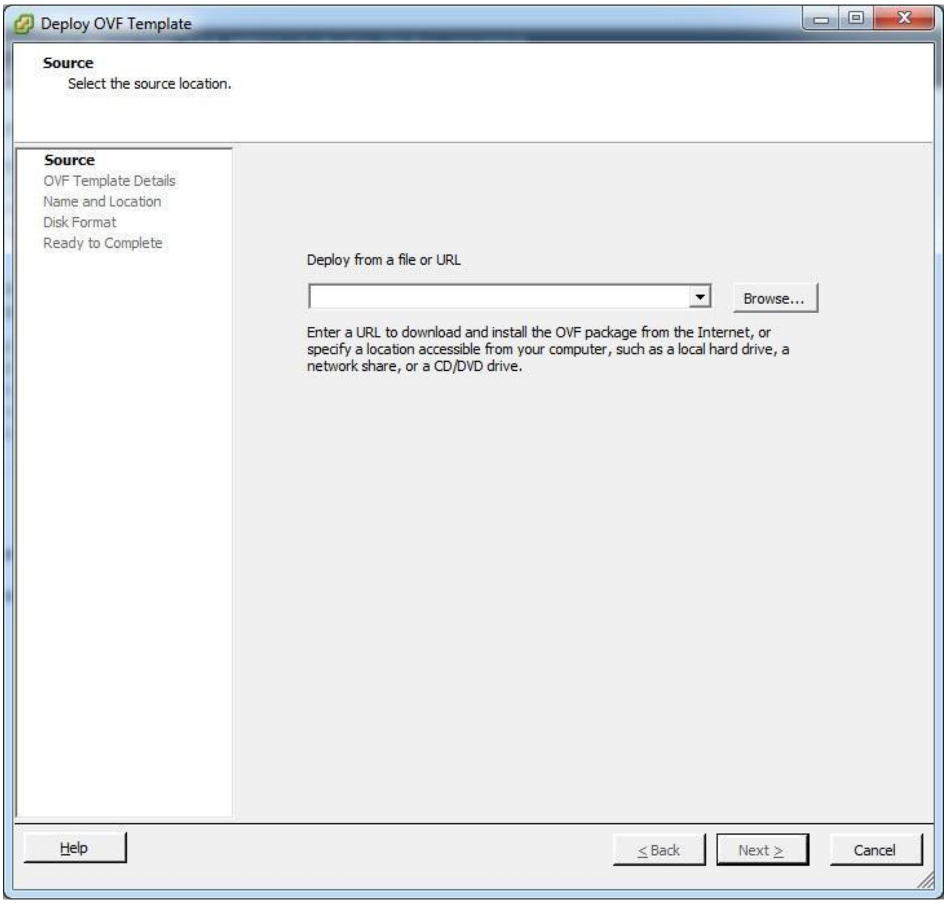
Explore Further

Learn about vSphere

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

Evaluate vSphere

4. Click **Browse;**



Deploy OVF Template

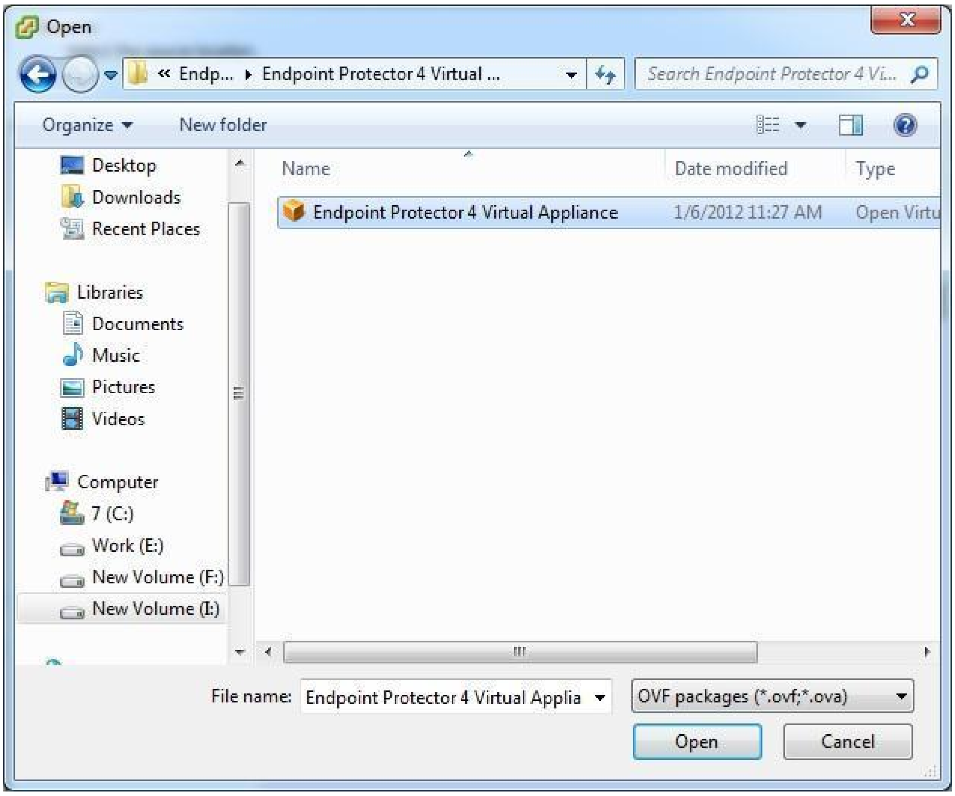
Source

Select the source location.

Deploy from a file or URL

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

5. Select the OVF file from the extracted zip file;



Open

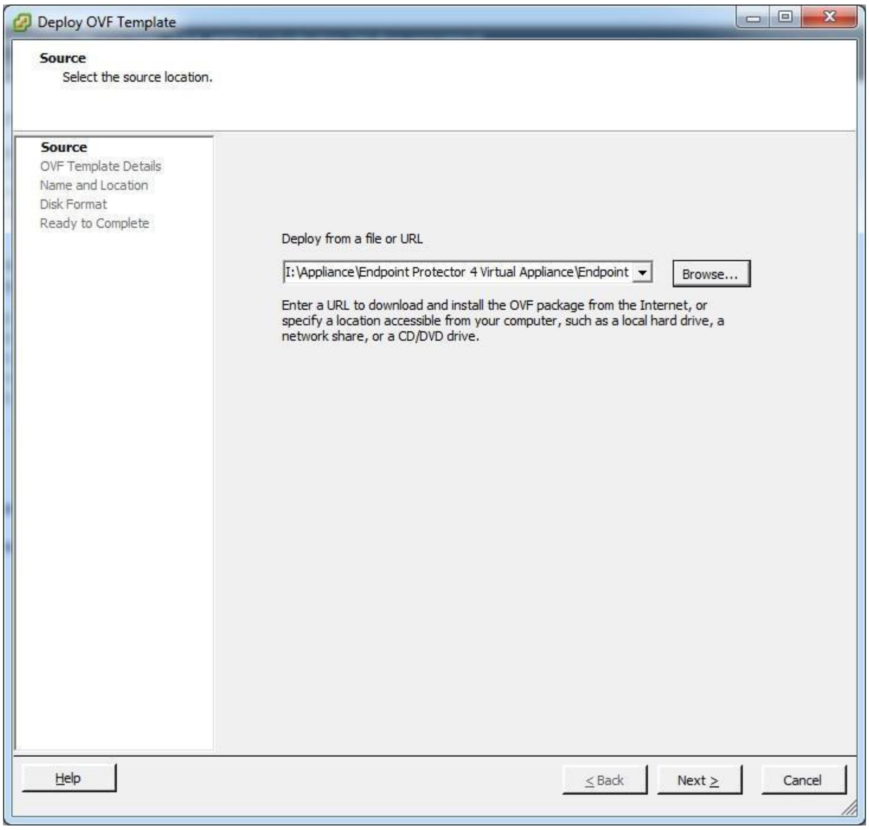
« Endp... ▸ Endpoint Protector 4 Virtual ...

Name	Date modified	Type
Endpoint Protector 4 Virtual Appliance	1/6/2012 11:27 AM	Open Virtu

File name: Endpoint Protector 4 Virtual Applia

OVF packages (*.ovf;*.ova)

6. Click **Next**;

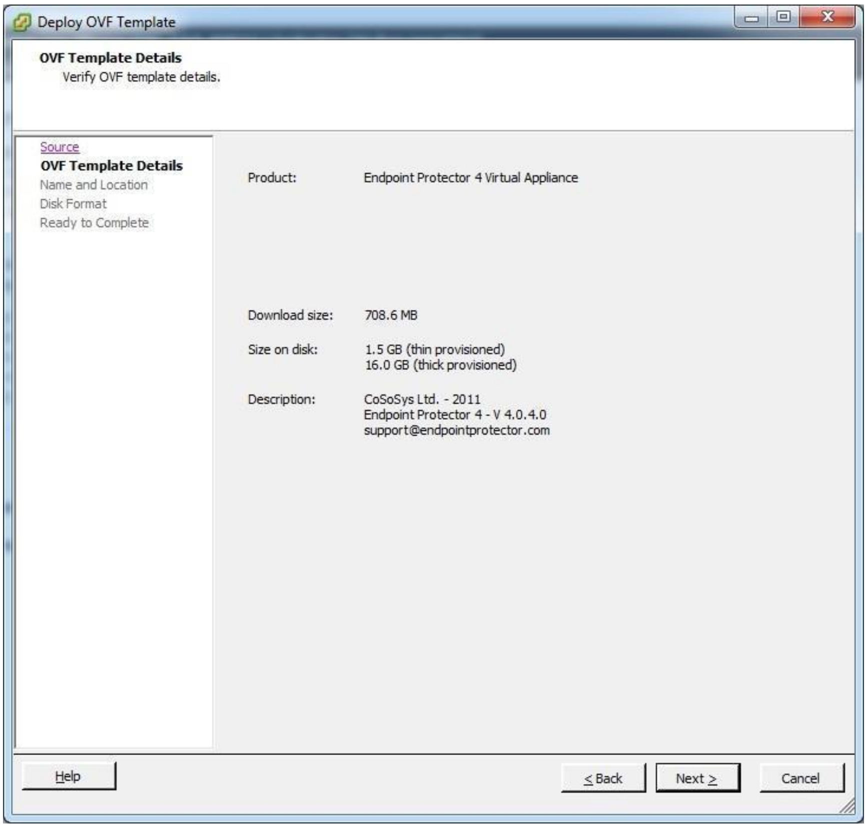


Deploy from a file or URL

I:\Appliance\Endpoint Protector 4 Virtual Appliance\Endpoint

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

7. Check the OVF Template Details and then click **Next;**



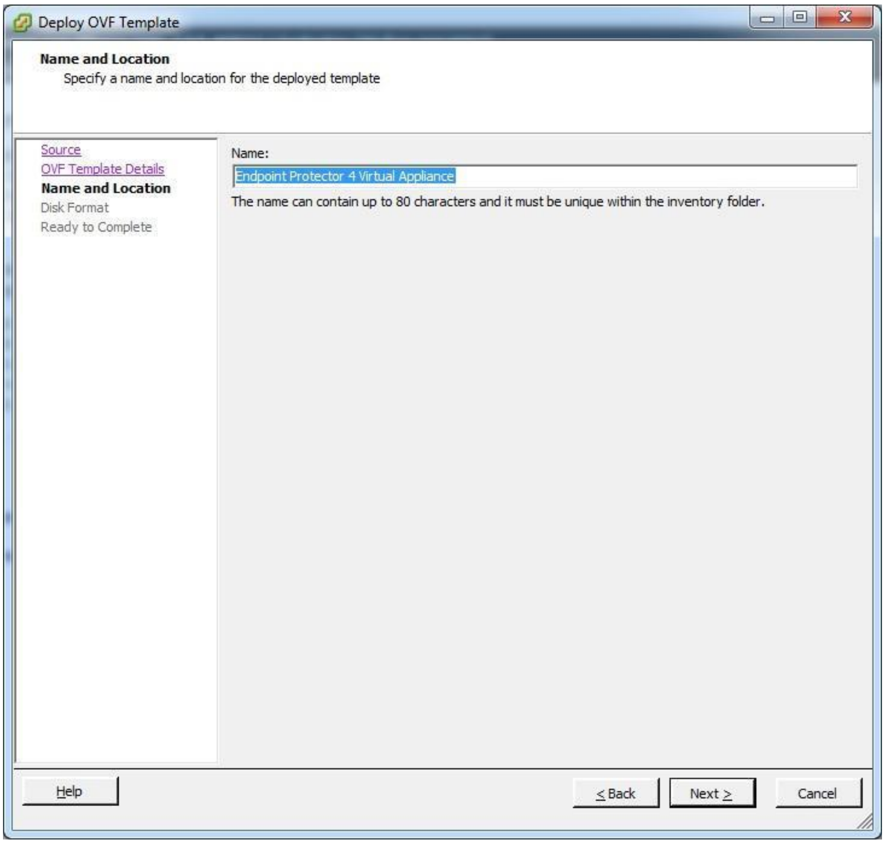
Product: Endpoint Protector 4 Virtual Appliance

Download size: 708.6 MB

Size on disk: 1.5 GB (thin provisioned)
16.0 GB (thick provisioned)

Description: CoSoSys Ltd. - 2011
Endpoint Protector 4 - V 4.0.4.0
support@endpointprotector.com

8. Specify the name of the OVF template and click **Next**;



Deploy OVF Template

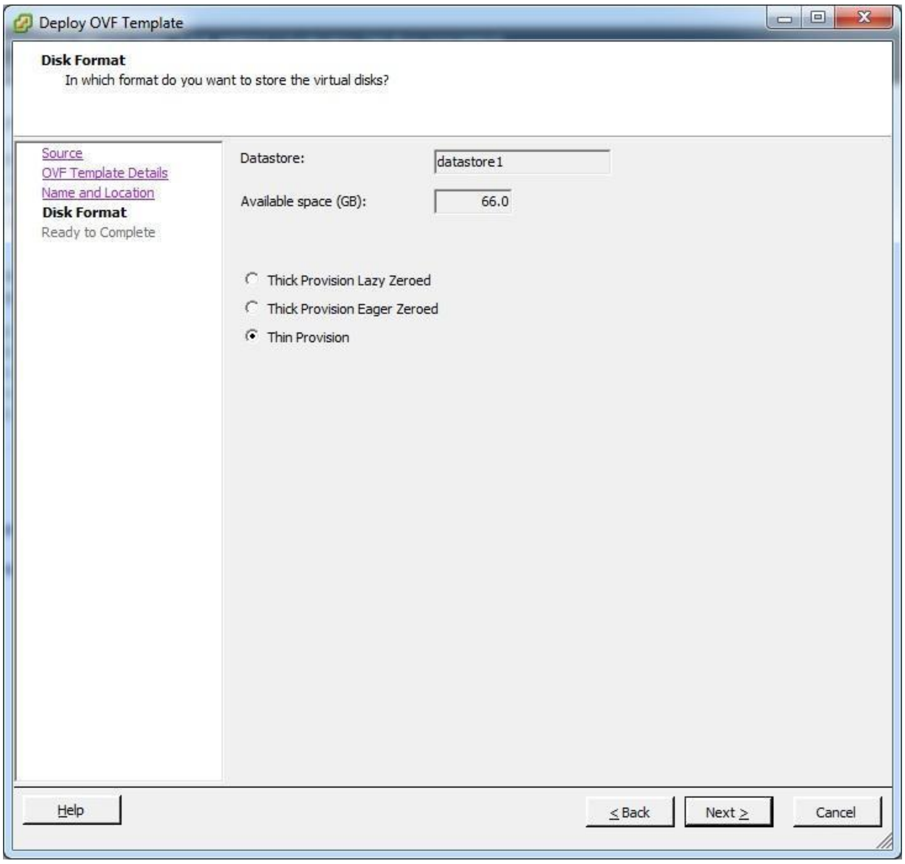
Name and Location

Specify a name and location for the deployed template

Name: Endpoint Protector 4 Virtual Appliance

The name can contain up to 80 characters and it must be unique within the inventory folder.

9. Select the **Thin provision** Disk Format option and click **Next;**



Deploy OVF Template

Disk Format

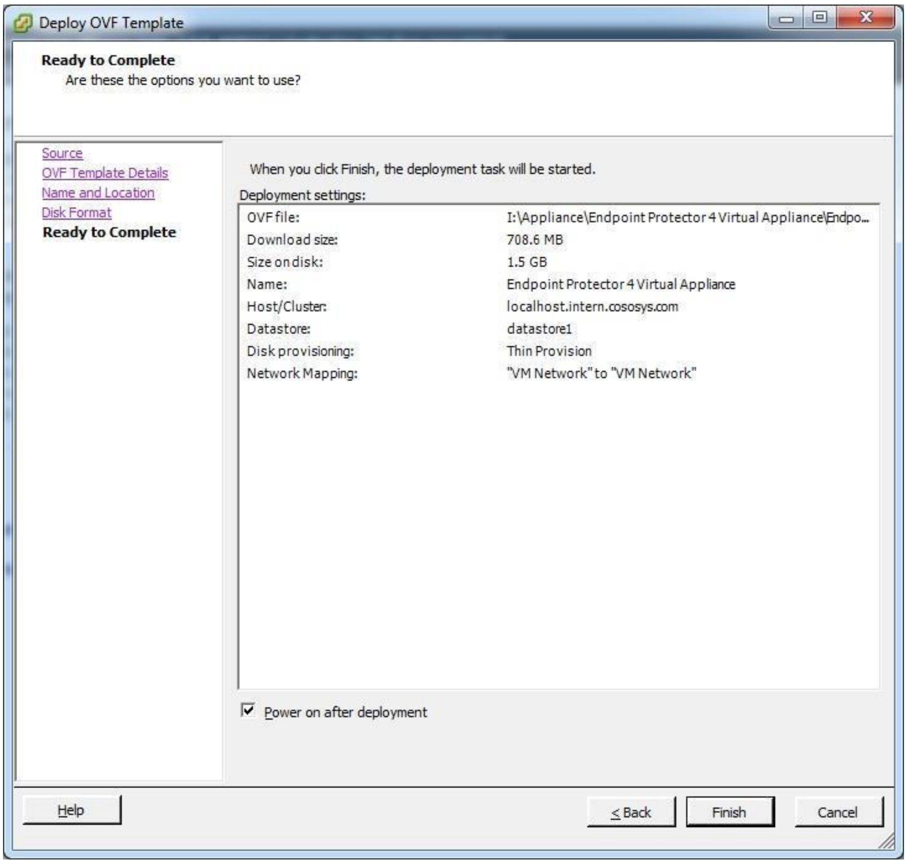
In which format do you want to store the virtual disks?

Datastore: datastore1

Available space (GB): 66.0

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

10. Click **Finish** to complete the installation.



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

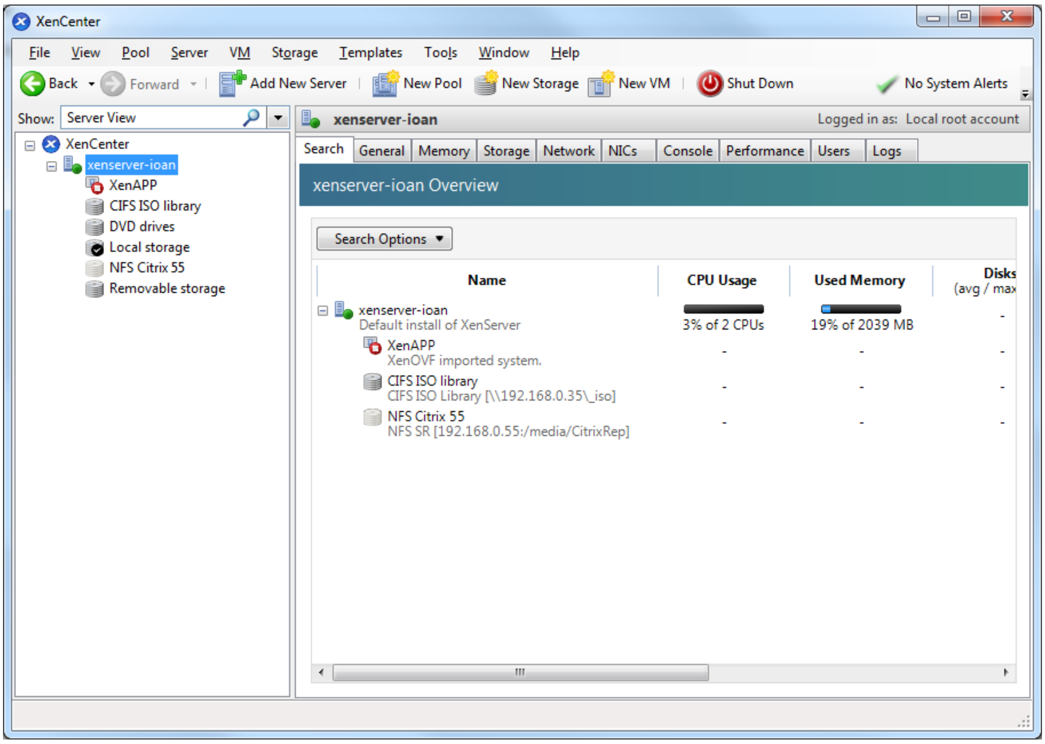
Deployment settings:

```
OVF file:            I:\Appliance\Endpoint Protector 4 Virtual Appliance\Endpo...
Download size:       708.6 MB
Size on disk:        1.5 GB
Name:                Endpoint Protector 4 Virtual Appliance
Host/Cluster:        localhost.intern.cososys.com
Datastore:           datastore1
Disk provisioning:   Thin Provision
Network Mapping:     "VM Network" to "VM Network"
```

☑ Power on after deployment

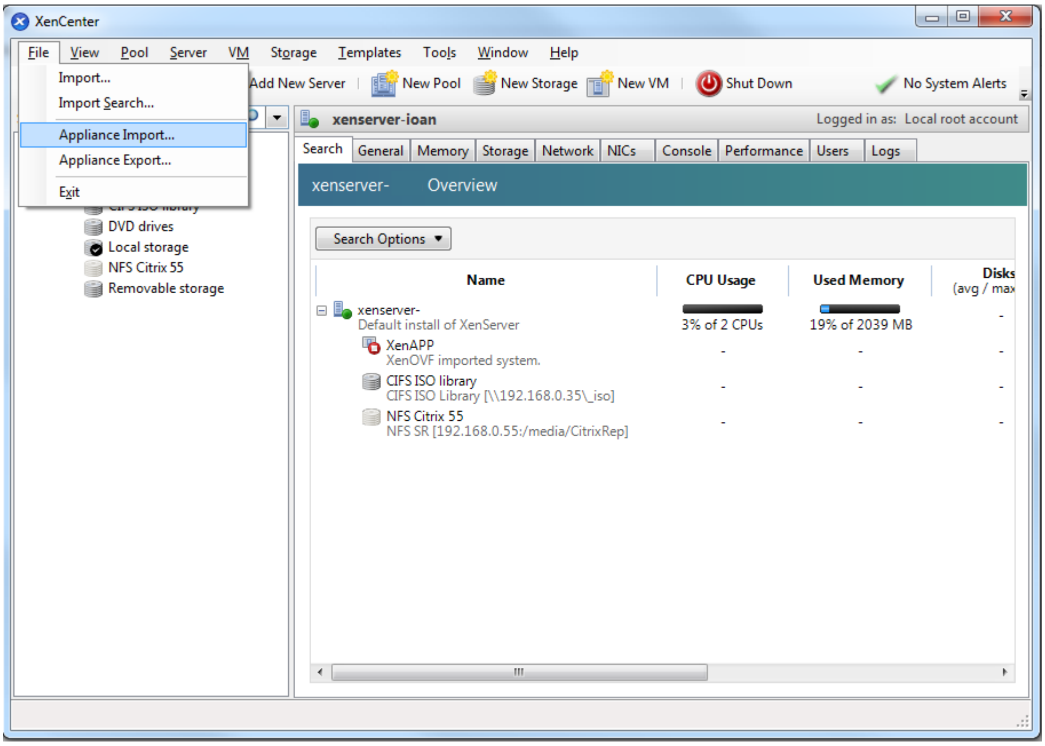
2.3. Citrix XenServer 5.6

1. Unzip the downloaded package;
2. Start **XenCenter;**


XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Back Forward Add New Server New Pool New Storage New VM Shut Down No System Alerts
Show: Server View
XenCenter
xenserver-ioan
XenAPP
CIFS ISO library
DVD drives
Local storage
NFS Citrix 55
Removable storage
xenserver-ioan
Logged in as: Local root account
Search General Memory Storage Network NICs Console Performance Users Logs
xenserver-ioan Overview
Search Options

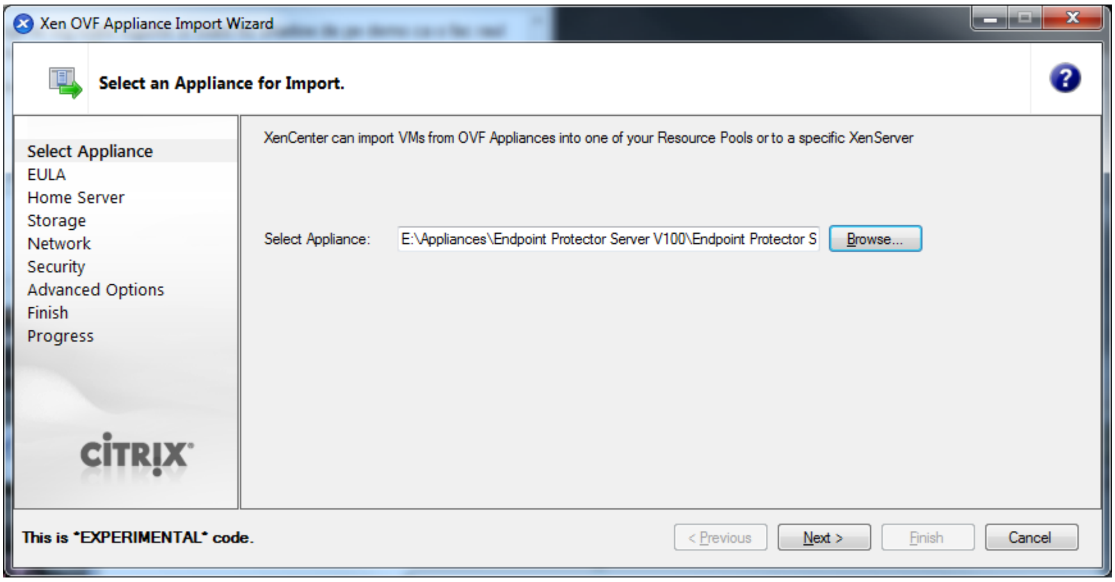
Name	CPU Usage	Used Memory	Disks (avg / max
xenserver-ioan Default install of XenServer	3% of 2 CPUs	19% of 2039 MB	-
XenAPP XenOVF imported system.	-	-	-
CIFS ISO library CIFS ISO Library [\\192.168.0.35_iso]	-	-	-
NFS Citrix 55 NFS SR [192.168.0.55:/media/CitrixRep]	-	-	-

3. Go to **File** and select **Appliance Import;**


XenCenter
File View Pool Server VM Storage Templates Tools Window Help
Import...
Import Search...
Appliance Import...
Appliance Export...
Exit
Add New Server New Pool New Storage New VM Shut Down No System Alerts
DVD drives
Local storage
NFS Citrix 55
Removable storage
xenserver-ioan
Logged in as: Local root account
Search General Memory Storage Network NICs Console Performance Users Logs
xenserver- Overview
Search Options

Name	CPU Usage	Used Memory	Disks (avg / max
xenserver- Default install of XenServer	3% of 2 CPUs	19% of 2039 MB	-
XenAPP XenOVF imported system.	-	-	-
CIFS ISO library CIFS ISO Library [\\192.168.0.35_iso]	-	-	-
NFS Citrix 55 NFS SR [192.168.0.55:/media/CitrixRep]	-	-	-

4. Select the OVF file and then click **Next;**



Select an Appliance for Import.

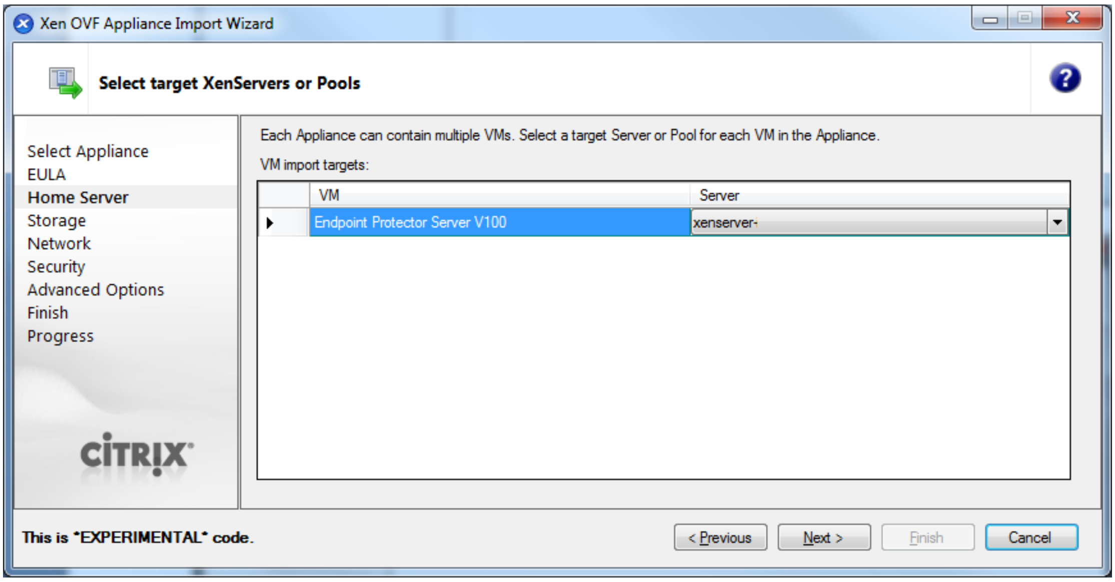
XenCenter can import VMs from OVF Appliances into one of your Resource Pools or to a specific XenServer

Select Appliance: E:\Appliances\Endpoint Protector Server V100\Endpoint Protector S

This is "EXPERIMENTAL" code.

5. Read and accept the EULA, then click **Next;**

6. Select the target for the Virtual Appliance;



Select target XenServers or Pools

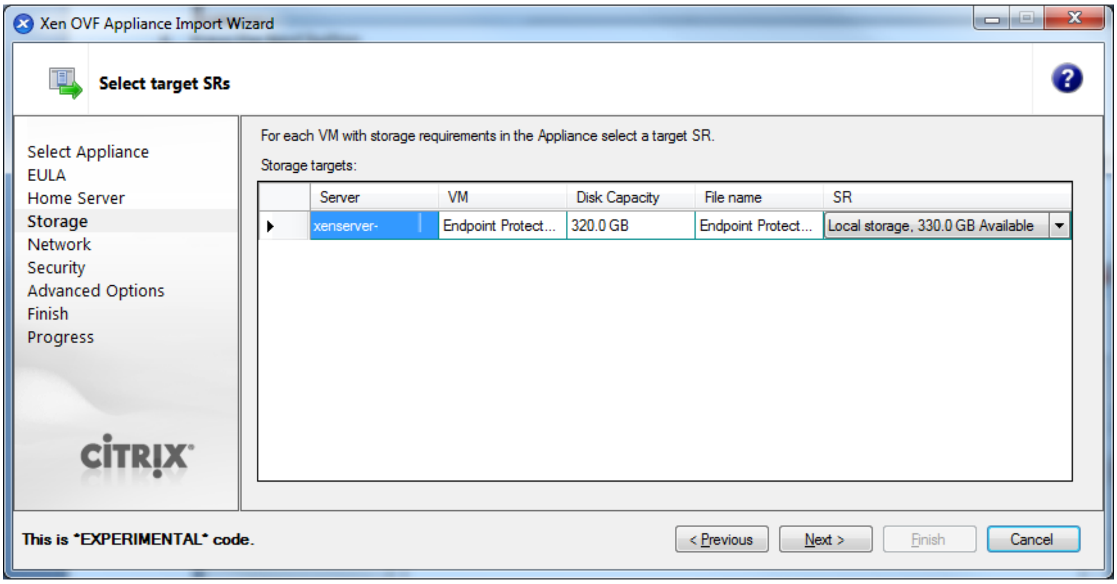
Each Appliance can contain multiple VMs. Select a target Server or Pool for each VM in the Appliance.

VM import targets:

VM	Server
Endpoint Protector Server V100	xenserver-

This is "EXPERIMENTAL" code.

7. Select the storage location;



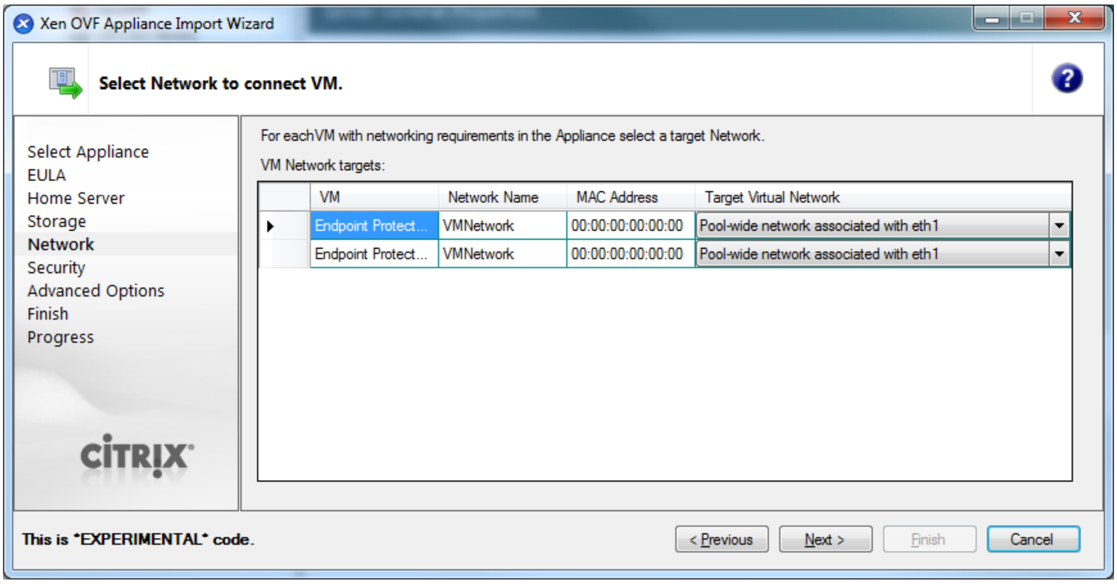
For each VM with storage requirements in the Appliance select a target SR.

Storage targets:

Server	VM	Disk Capacity	File name	SR
xenserver-	Endpoint Protect...	320.0 GB	Endpoint Protect...	Local storage, 330.0 GB Available

This is "EXPERIMENTAL" code.

8. Select the network (keep default values);



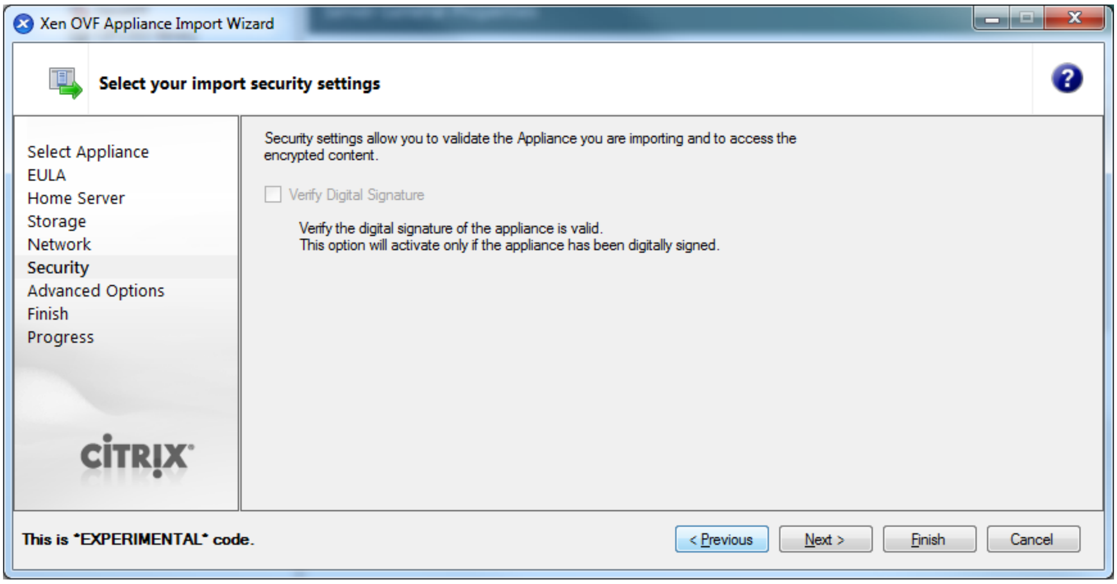
For eachVM with networking requirements in the Appliance select a target Network.

VM Network targets:

VM	Network Name	MAC Address	Target Virtual Network
Endpoint Protect...	VMNetwork	00:00:00:00:00:00	Pool-wide network associated with eth1
Endpoint Protect...	VMNetwork	00:00:00:00:00:00	Pool-wide network associated with eth1

This is "EXPERIMENTAL" code.

9. On the Security screen click **Next**;



Select your import security settings

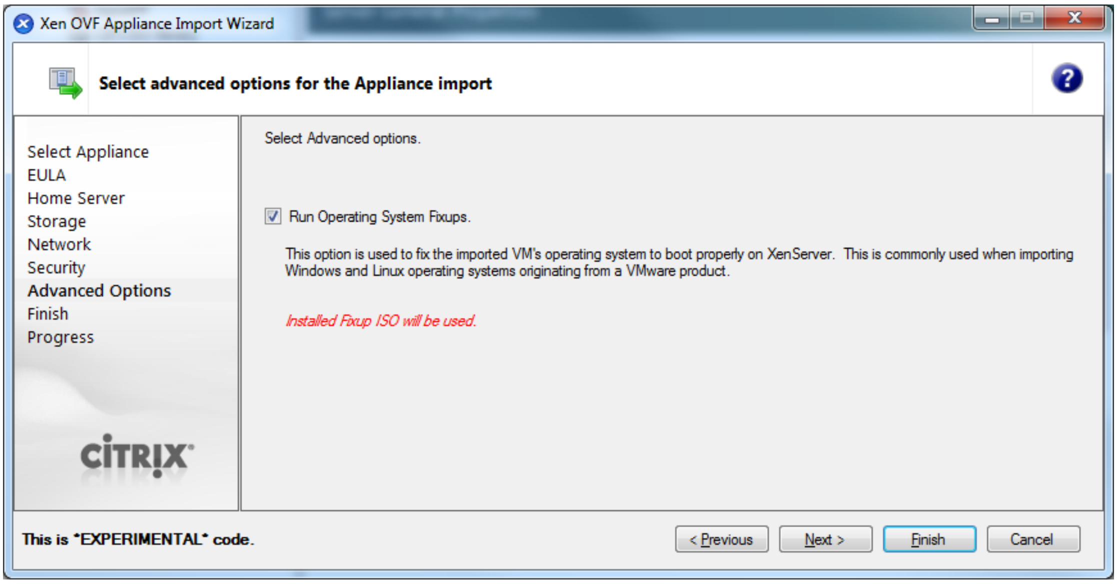
Security settings allow you to validate the Appliance you are importing and to access the encrypted content.

□ Verify Digital Signature

Verify the digital signature of the appliance is valid.
This option will activate only if the appliance has been digitally signed.

This is "EXPERIMENTAL" code.

10. On the Advanced Options screen click **Next;**



Select advanced options for the Appliance import

Select Advanced options.

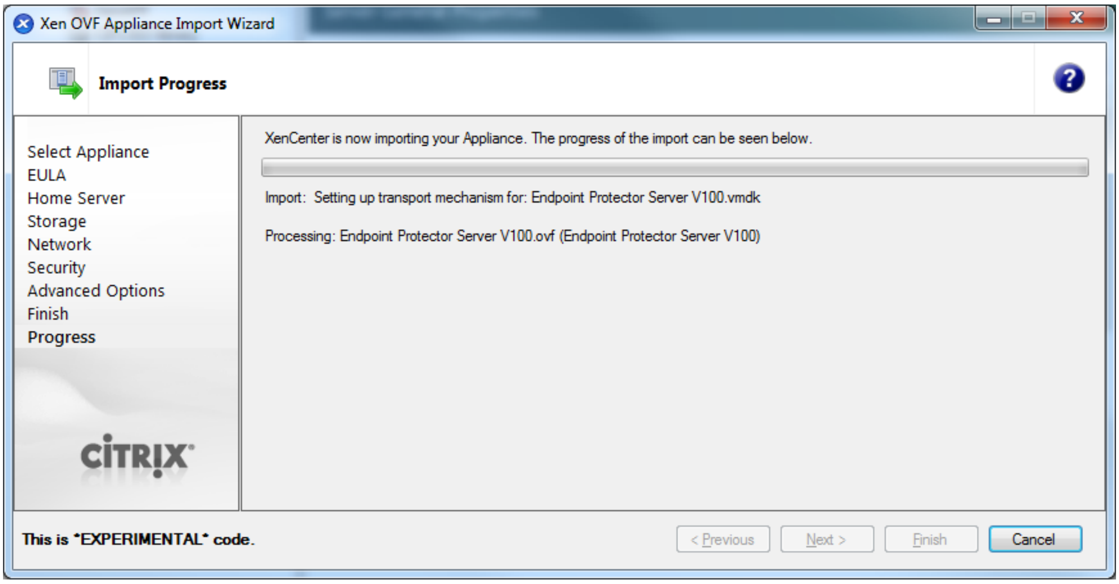
☑ Run Operating System Fixups.

This option is used to fix the imported VM's operating system to boot properly on XenServer. This is commonly used when importing Windows and Linux operating systems originating from a VMware product.

Installed Fixup ISO will be used.

This is "EXPERIMENTAL" code.

11. On the **Finish** screen, review the configuration, click **Finish** and wait for the import to be completed.



XenCenter is now importing your Appliance. The progress of the import can be seen below.

Import: Setting up transport mechanism for: Endpoint Protector Server V100.vmdk

Processing: Endpoint Protector Server V100.ovf (Endpoint Protector Server V100)

This is *EXPERIMENTAL* code.

At this point, the virtual machine is ready to be started.

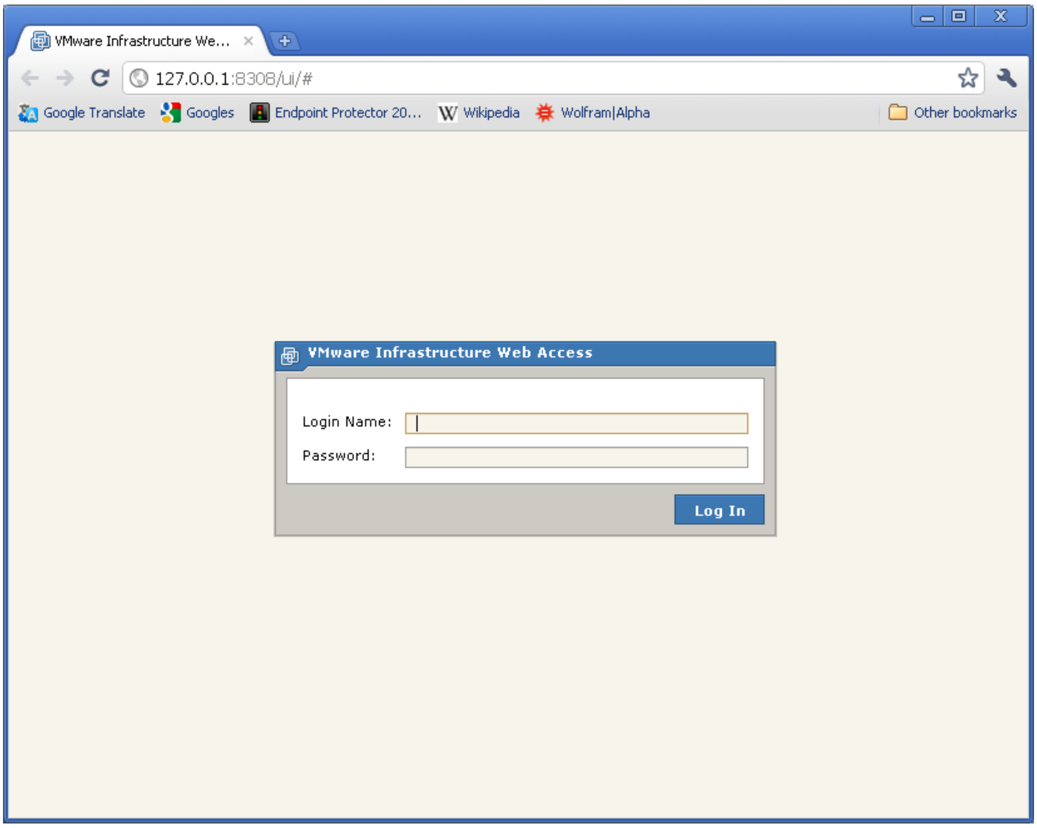
Follow the Endpoint Protector Appliance User Manual from this point on.

3. Implement using the VMX format

There are several options to implement the Endpoint Protector Virtual Appliance using the OVMX format.

3.1. Implementing using VMware Server

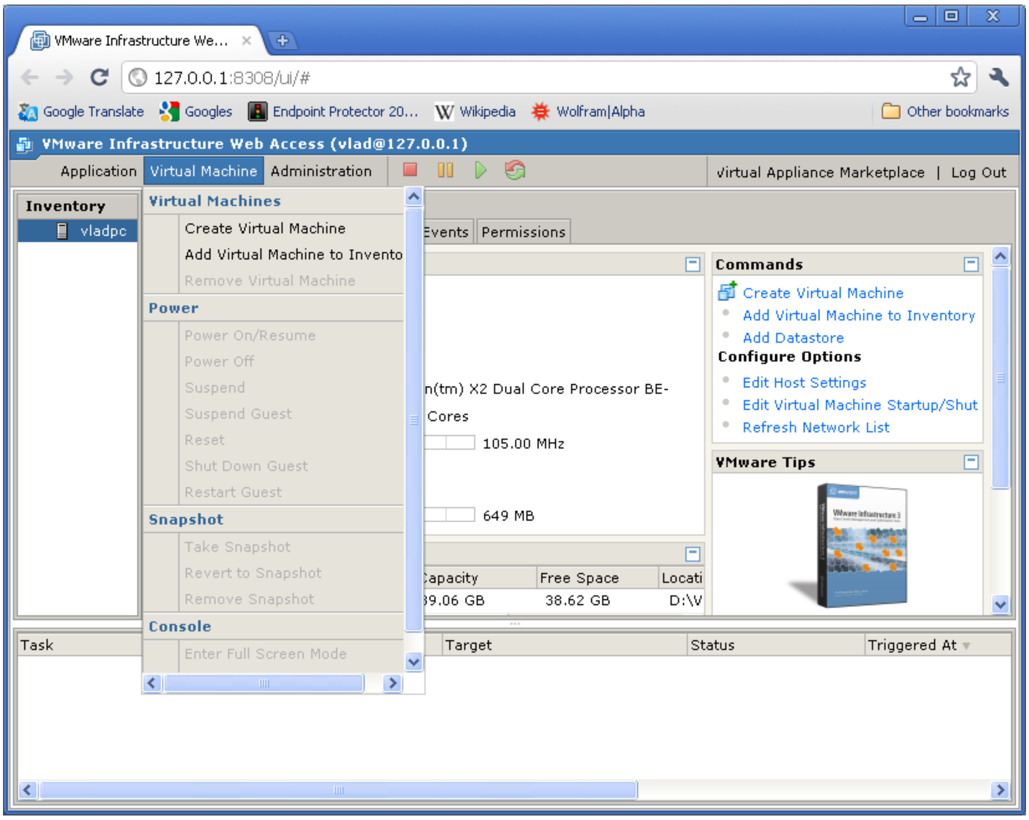
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored;
2. Open your VMware Server web interface and log in;



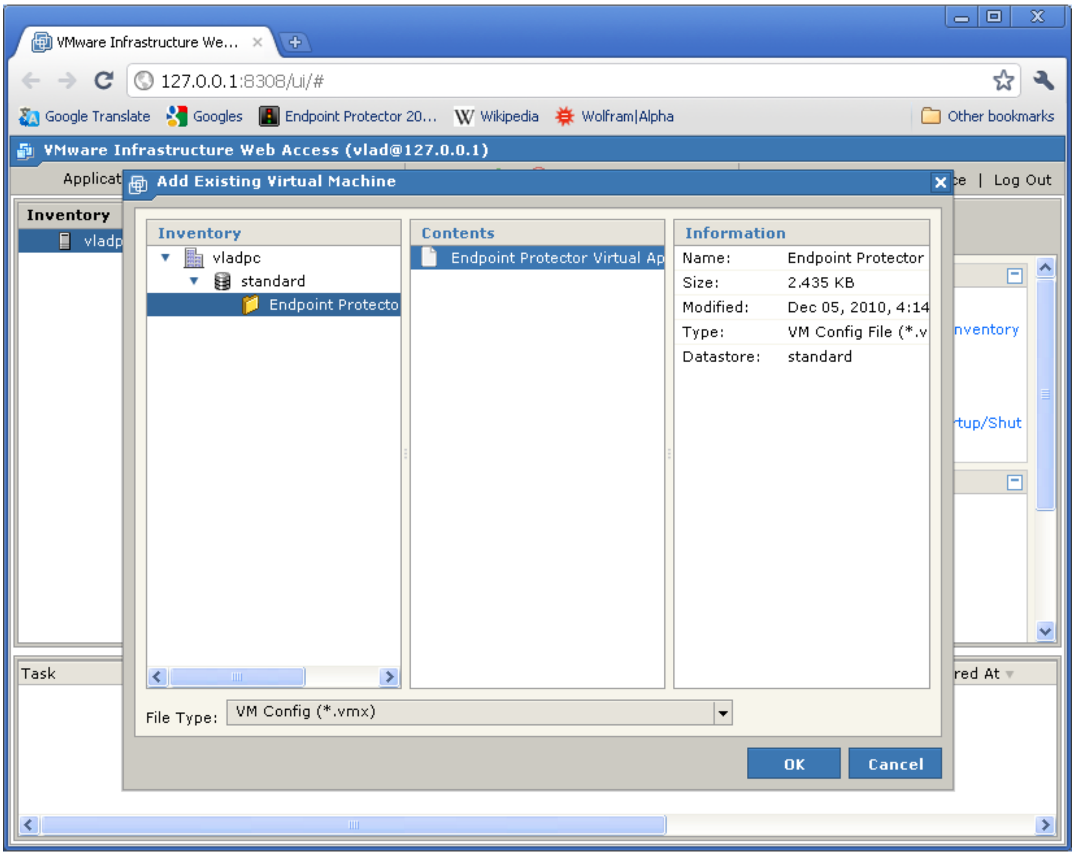
Login Name:

Password:

3. Select **Add Virtual Machine to inventory;**



4. Browse in the inventory for Endpoint Protector Virtual Appliance and select the VMX file and click **OK;**



Name: Endpoint Protector
Size: 2.435 KB
Modified: Dec 05, 2010, 4:14
Type: VM Config File (*.v
Datastore: standard

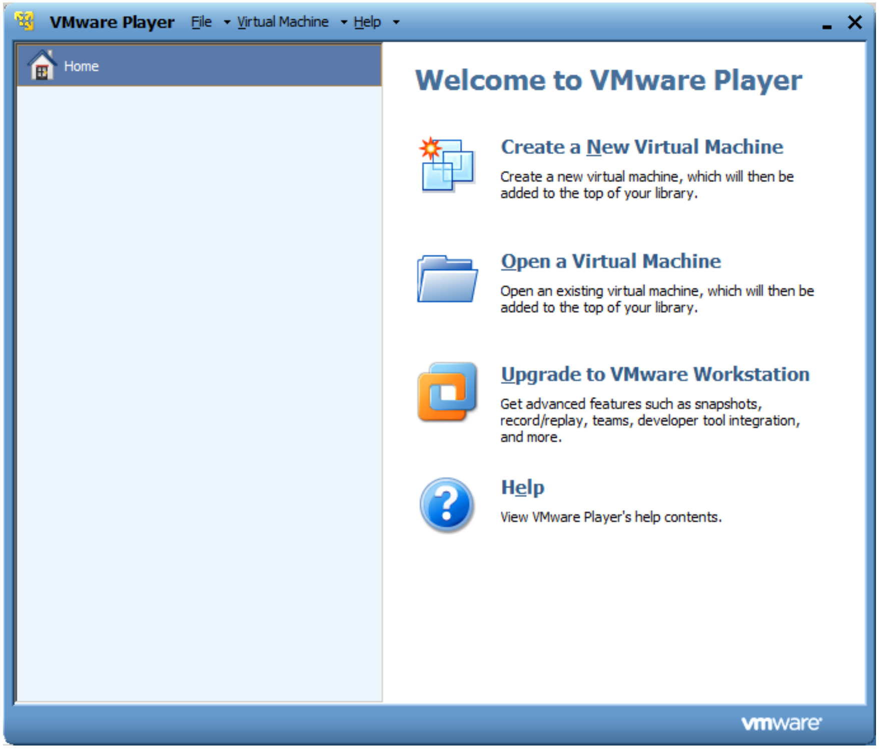
File Type: VM Config (*.vmx)

At this point, the Virtual Machine is ready to be started.

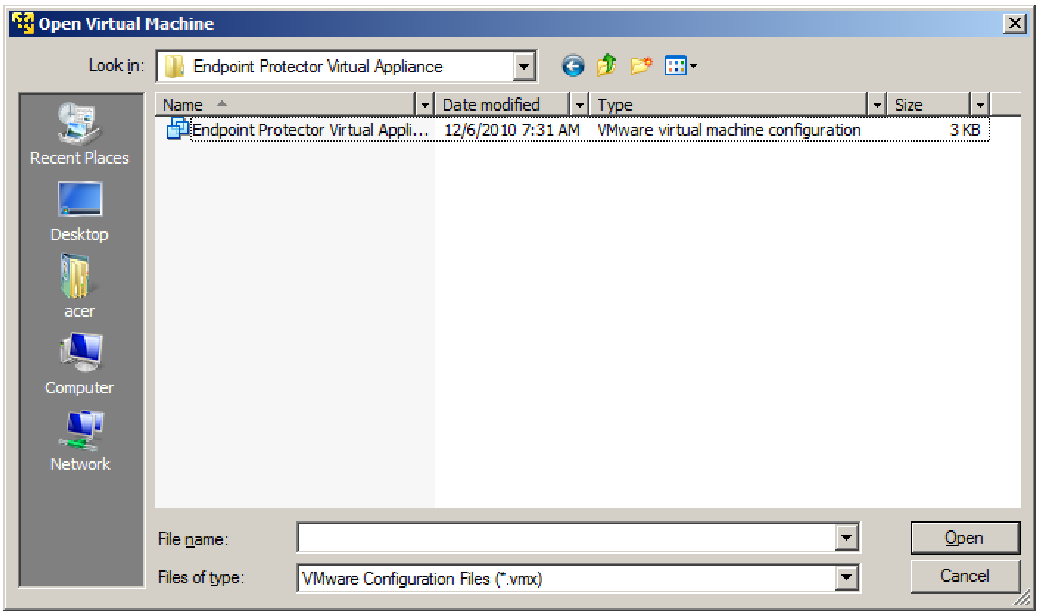
Follow the Endpoint Protector Appliance User Manual from this point on.

3.2. Implementing using VMware Player

1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored;
2. Open VMware Player;


VMware Player
File
Virtual Machine
Help
Home
Welcome to VMware Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation
Get advanced features such as snapshots, record/replay, teams, developer tool integration, and more.
Help
View VMware Player's help contents.
vmware

3. Select **Open a Virtual Machine** and select the VMX file from the location where you extracted it and then click **Open**;



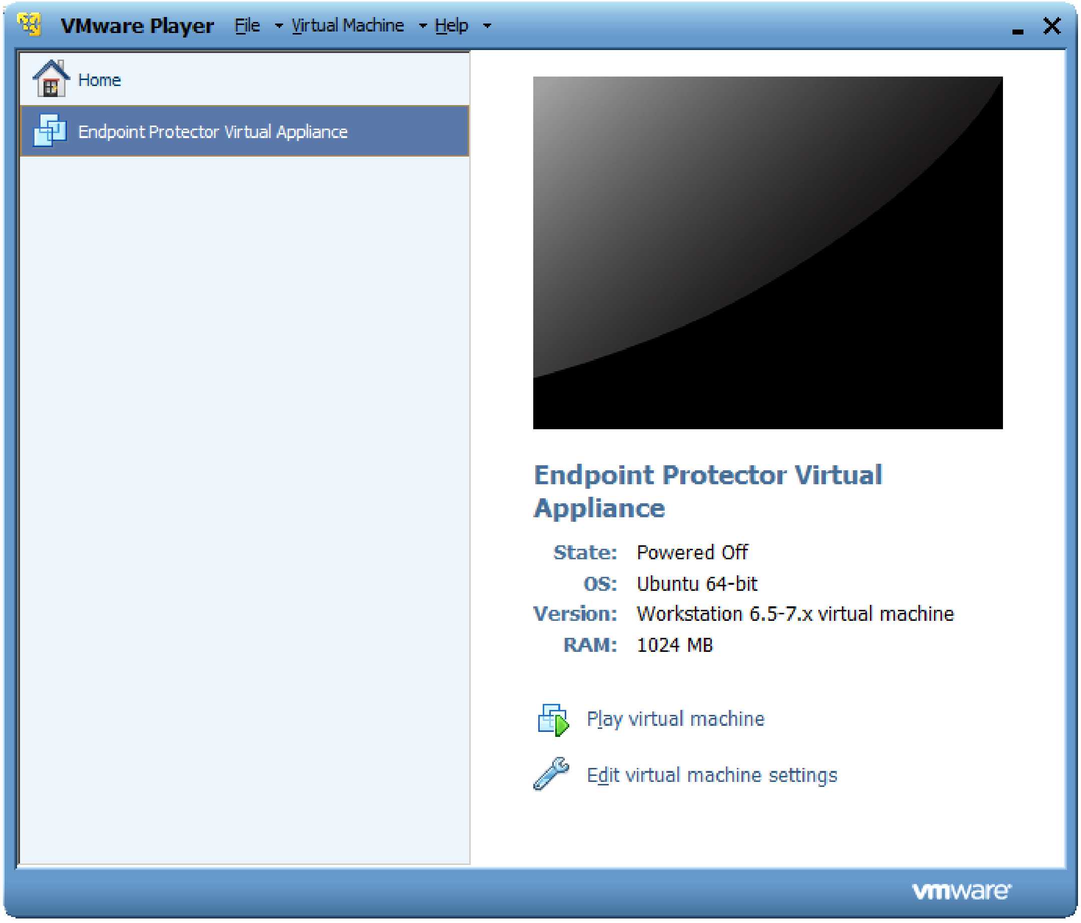
Look in: Endpoint Protector Virtual Appliance

Name	Date modified	Type	Size
Endpoint Protector Virtual Appli...	12/6/2010 7:31 AM	VMware virtual machine configuration	3 KB

File name:

Files of type: VMware Configuration Files (*.vmx)

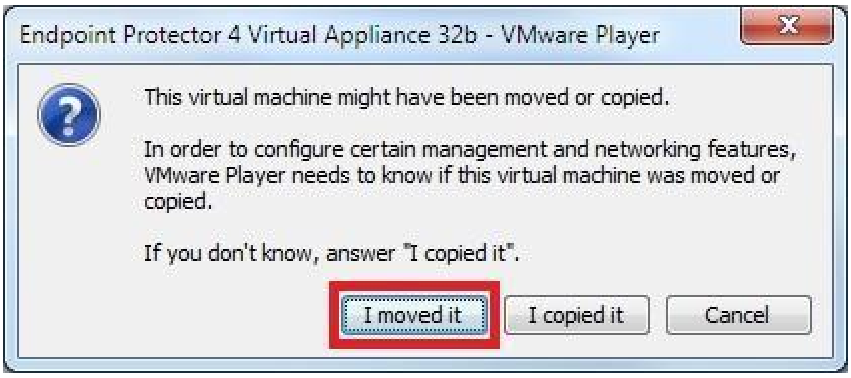
4. After the Virtual Machine is in your inventory click **Play Virtual Machine;**



Endpoint Protector Virtual Appliance

State: Powered Off
OS: Ubuntu 64-bit
Version: Workstation 6.5-7.x virtual machine
RAM: 1024 MB

5. If asked if the Virtual Machine was copied or moved, select moved (if it is the only Endpoint Protector Virtual Appliance in your network);



Endpoint Protector 4 Virtual Appliance 32b - VMware Player

This virtual machine might have been moved or copied.

In order to configure certain management and networking features, VMware Player needs to know if this virtual machine was moved or copied.

If you don't know, answer "I copied it".

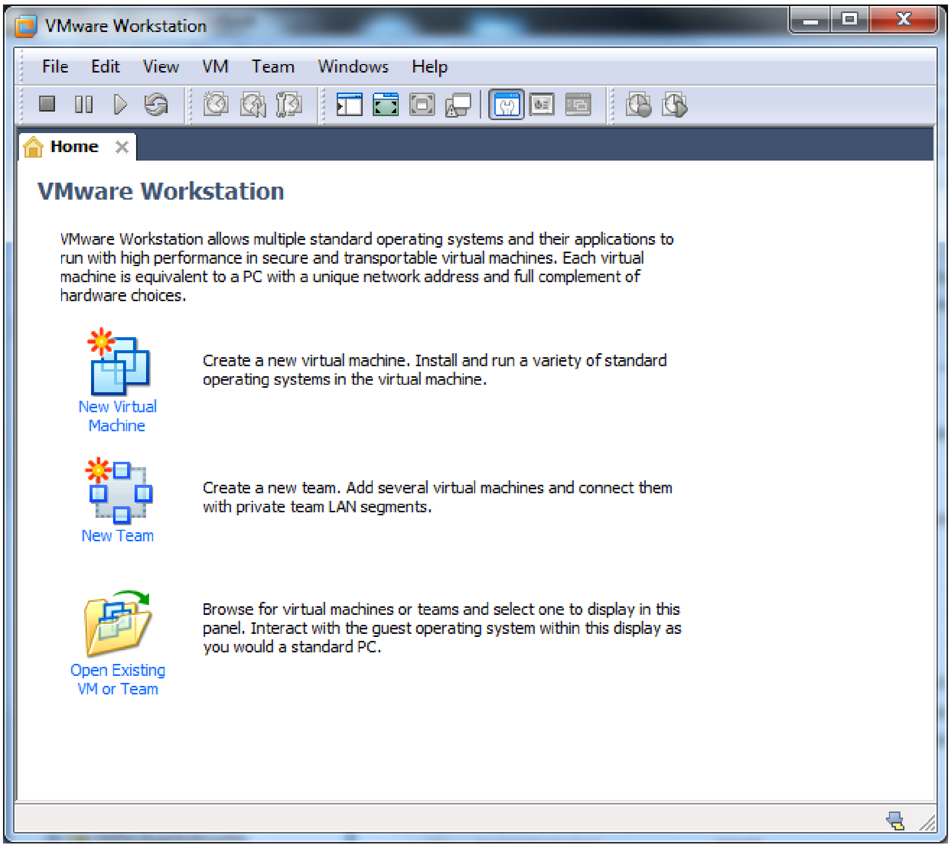
At this point, the Virtual Machine is ready to be started.

Follow the Endpoint Protector Appliance User Manual from this point on.

Important: Do not suspend the VMware Player while Endpoint Protector Virtual Appliance is running! Also, do not shut down your computer while VMware Player is running.

3.3. Implementing using VMware Workstation

1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored;
2. Open VMWare Workstation;



VMware Workstation

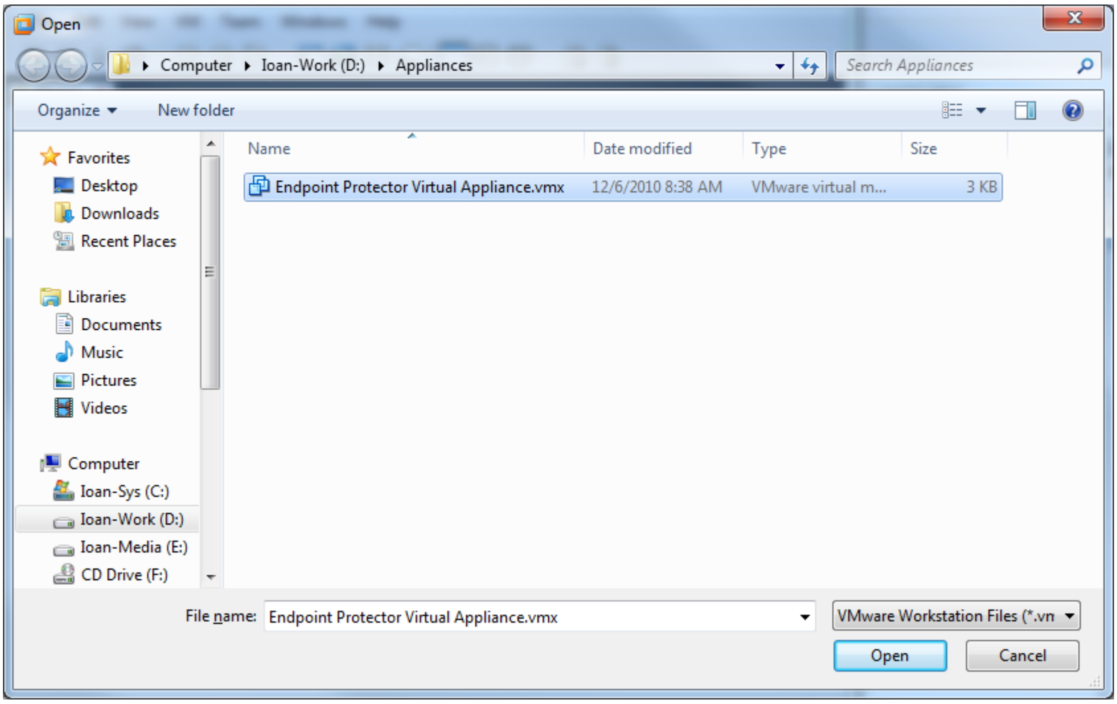
VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.

Create a new virtual machine. Install and run a variety of standard operating systems in the virtual machine.

Create a new team. Add several virtual machines and connect them with private team LAN segments.

Browse for virtual machines or teams and select one to display in this panel. Interact with the guest operating system within this display as you would a standard PC.

3. Select Open Existing VM or Team;

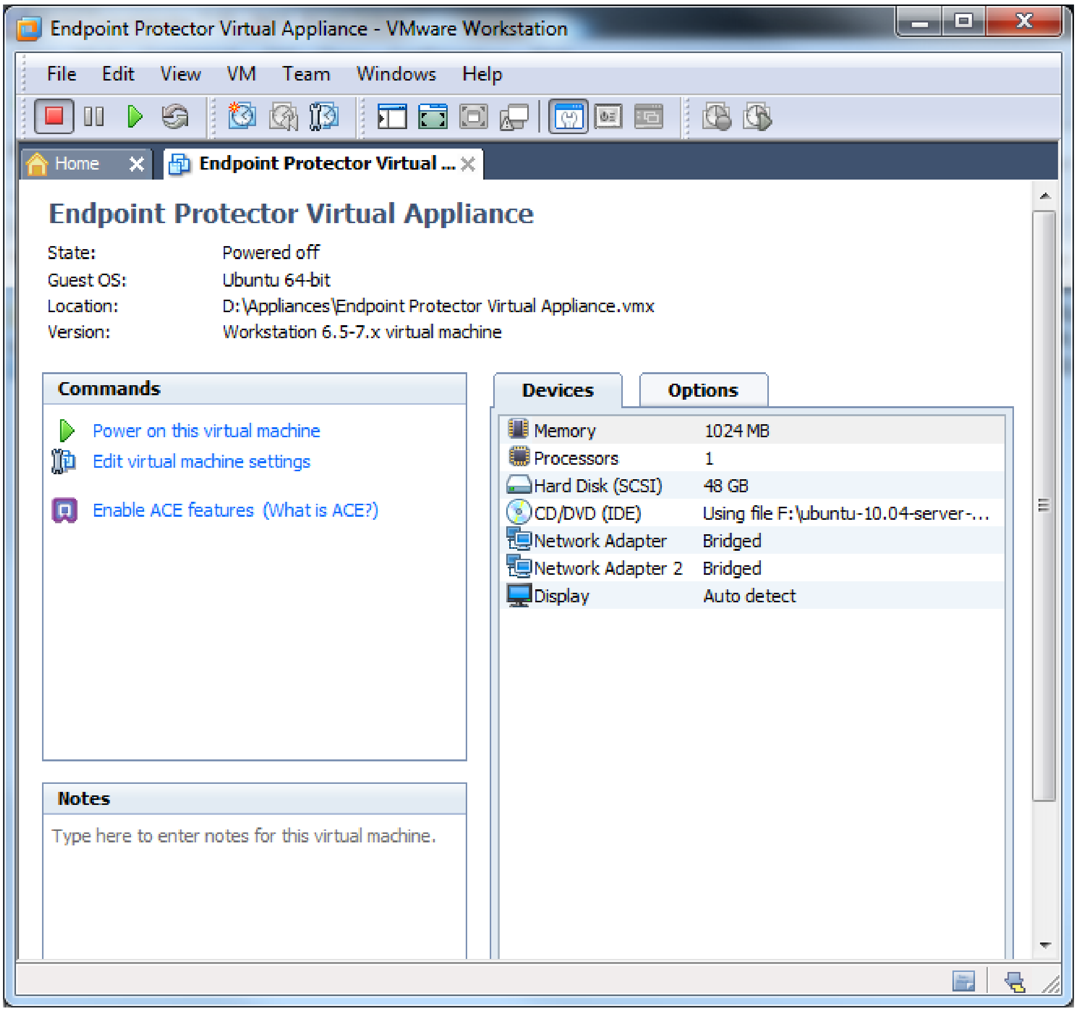


Name	Date modified	Type	Size
Endpoint Protector Virtual Appliance.vmx	12/6/2010 8:38 AM	VMware virtual m...	3 KB

File name: Endpoint Protector Virtual Appliance.vmx

VMware Workstation Files (*.vn

4. After the Virtual Appliance is in your inventory power on the Virtual Appliance;



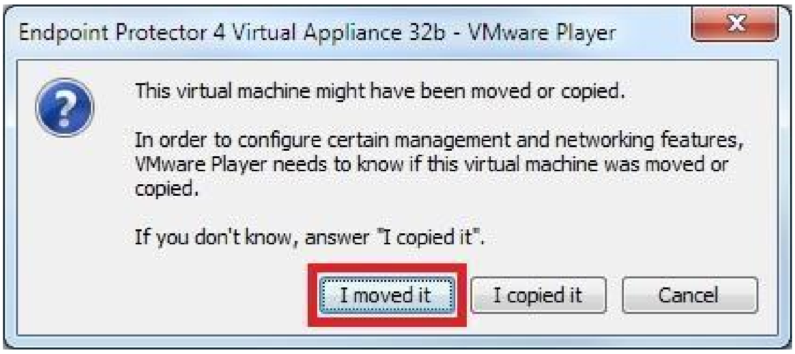
Endpoint Protector Virtual Appliance - VMware Workstation
File Edit View VM Team Windows Help
Home
Endpoint Protector Virtual ...
Commands
Power on this virtual machine
Edit virtual machine settings
Enable ACE features (What is ACE?)
Notes
Type here to enter notes for this virtual machine.
Devices
Options

Endpoint Protector Virtual Appliance

State: Powered off
Guest OS: Ubuntu 64-bit
Location: D:\Appliances\Endpoint Protector Virtual Appliance.vmx
Version: Workstation 6.5-7.x virtual machine

Memory	1024 MB
Processors	1
Hard Disk (SCSI)	48 GB
CD/DVD (IDE)	Using file F:\ubuntu-10.04-server-...
Network Adapter	Bridged
Network Adapter 2	Bridged
Display	Auto detect

5. If asked if the Virtual Machine was copied or moved, select moved (if it is the only Endpoint Protector Virtual Appliance in your network).



This virtual machine might have been moved or copied.

In order to configure certain management and networking features, VMware Player needs to know if this virtual machine was moved or copied.

If you don't know, answer "I copied it".

The Virtual Machine is started and ready for use.

Follow the Endpoint Protector Appliance User Manual from this point on.

4. Using the VHD format

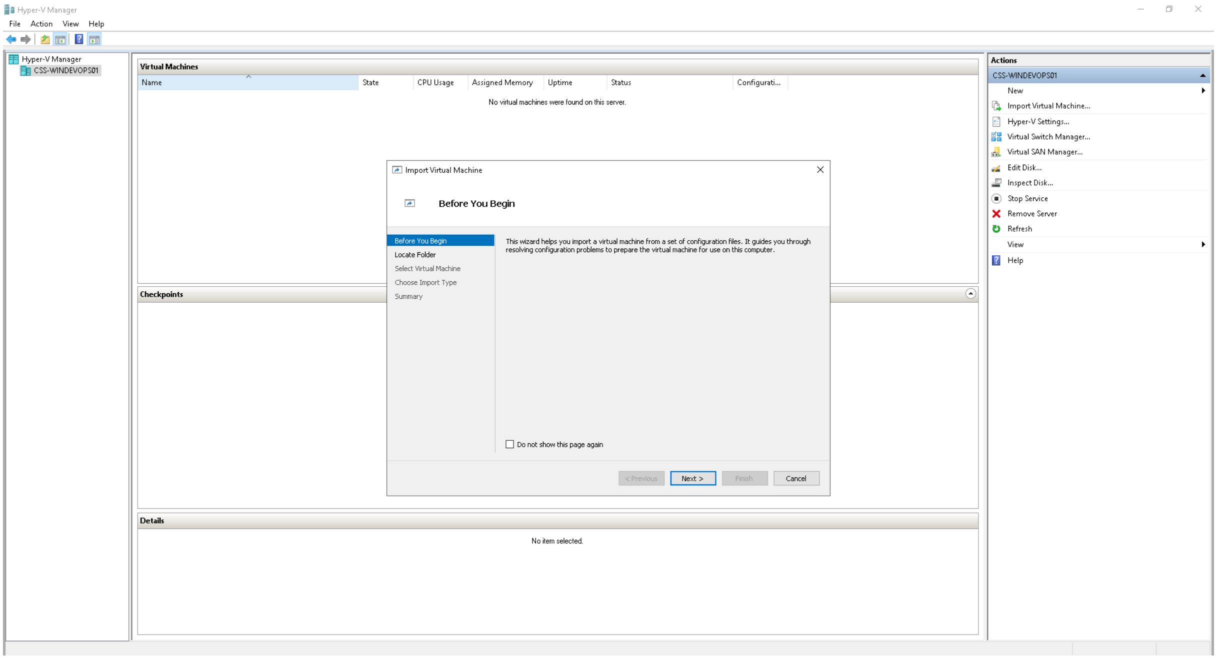
There are several options to implement the Endpoint Protector Virtual Appliance using the VHD format. The way to do this is explained below.

4.1. Implementing using Microsoft Hyper-V 2022

1. Extract the downloaded Endpoint Protector Virtual Appliance .zip package;

2. Start Hyper-V Manager;

3. Select from the right-side box the option to **Import Virtual Machine**;



No virtual machines were found on this server.

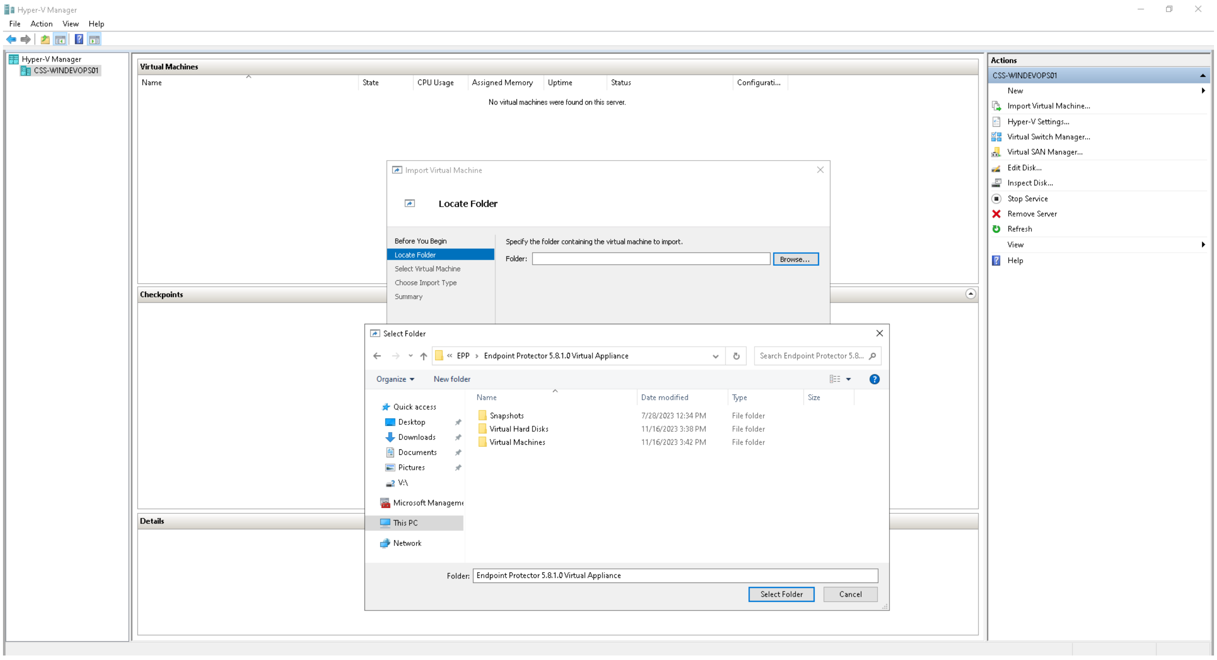
This wizard helps you import a virtual machine from a set of configuration files. It guides you through resolving configuration problems to prepare the virtual machine for use on this computer.

No item selected.

Click ‘Next’ at the **Before You Begin** step.

3.1 Select the Endpoint Protector Virtual Appliance folder, containing:

- Snapshots
- Virtual Hard Disks
- Virtual Machines

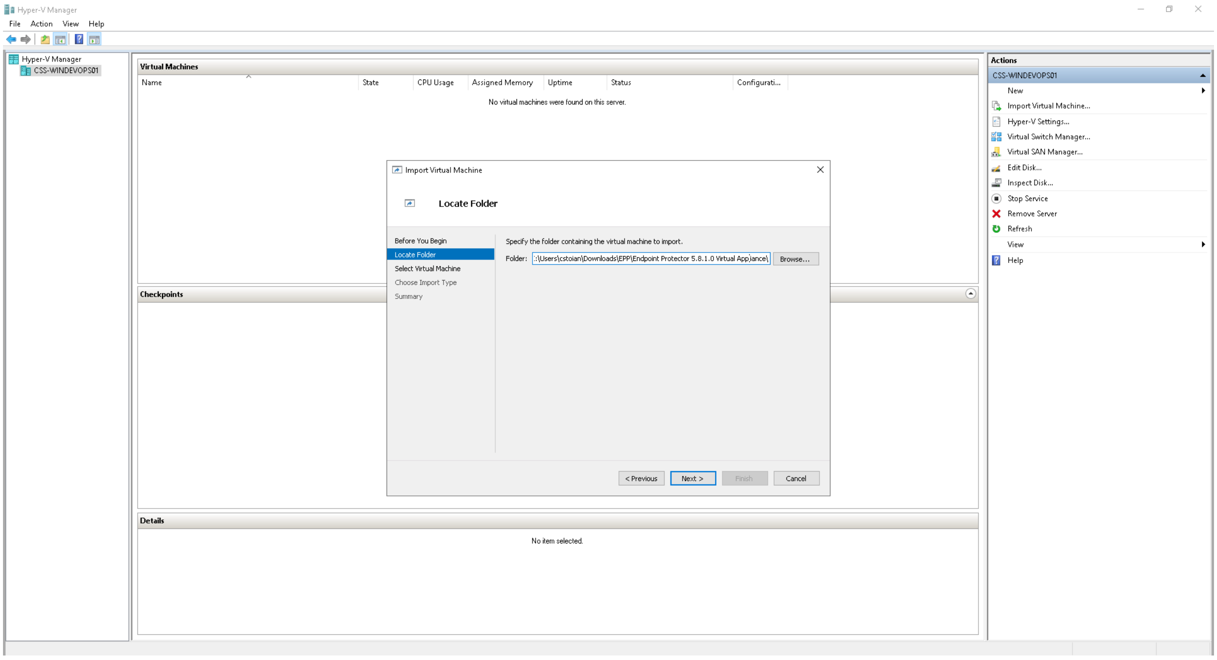


Specify the folder containing the virtual machine to import.

Folder:

Name	Date modified	Type	Size
Snapshots	7/28/2023 12:34 PM	File folder	
Virtual Hard Disks	11/16/2023 3:38 PM	File folder	
Virtual Machines	11/16/2023 3:42 PM	File folder	

Folder: Endpoint Protector 5.8.1.0 Virtual Appliance

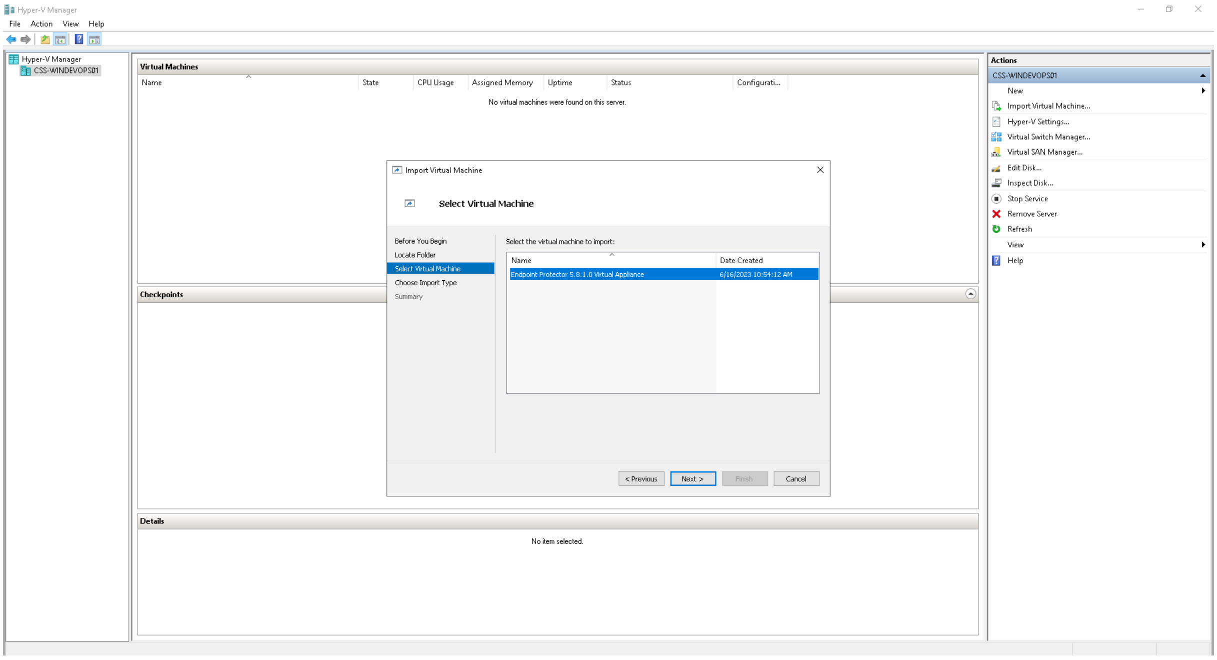


Specify the folder containing the virtual machine to import.

Folder: :\Users\cstoian\Downloads\EPP\Endpoint Protector 5.8.1.0 Virtual Appliance\

Then click ‘Next’.

3.2 On the **Select Virtual Machine** section, select the Endpoint Protector Virtual Appliance, then click ‘Next’.



No virtual machines were found on this server.

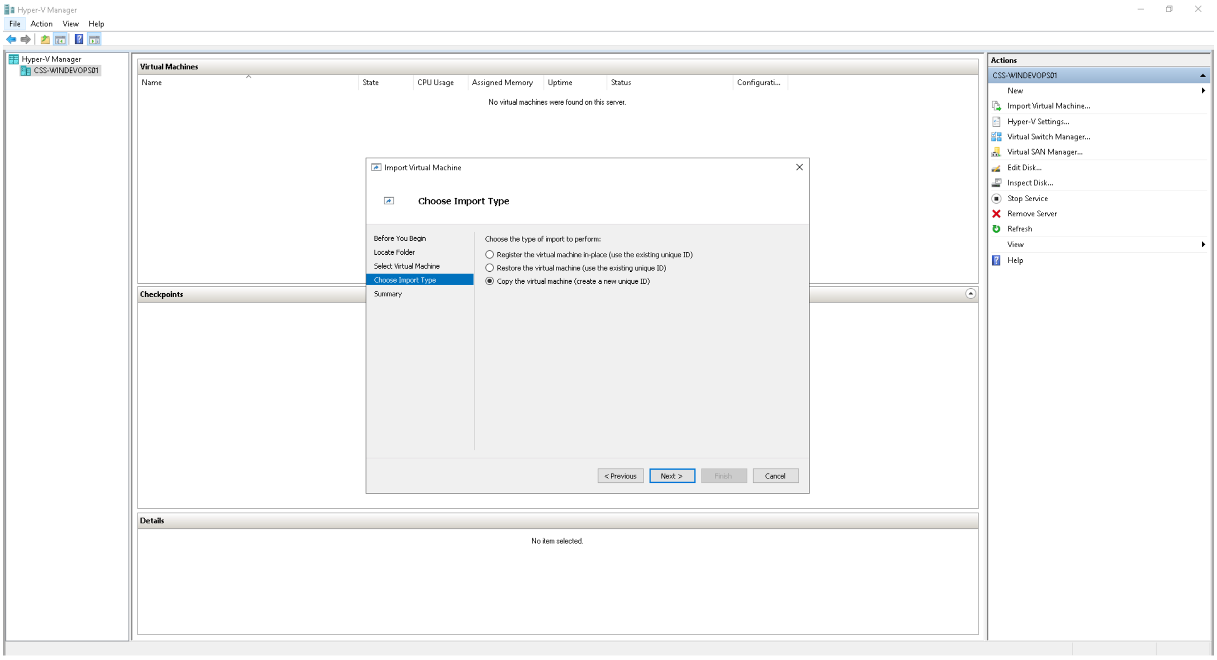
Select Virtual Machine

Select the virtual machine to import:

Name	Date Created
Endpoint Protector 5.8.1.0 Virtual Appliance	6/16/2023 10:54:12 AM

No item selected.

3.3. On the Choose Import Type section, select the **Copy the virtual machine (create a new unique ID)** option. Then click 'Next'.



No virtual machines were found on this server.

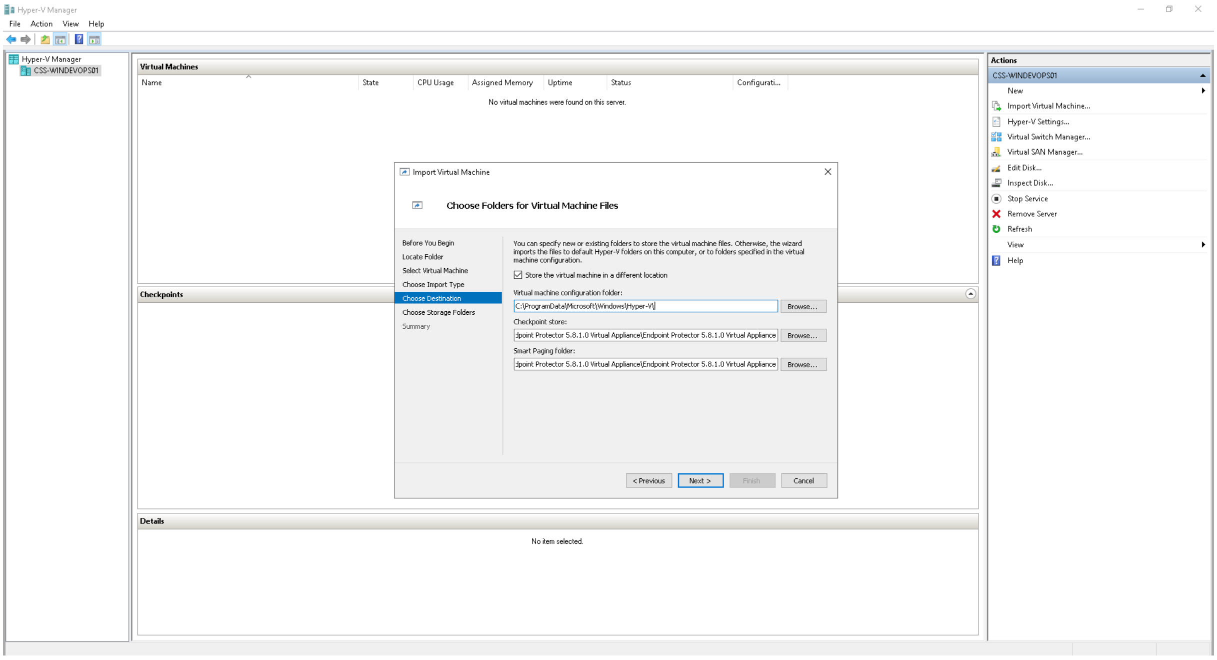
Choose Import Type

Choose the type of import to perform:

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

No item selected.

3.4. On the **Choose Folders for Virtual Machine Files** section, tick 'Store the virtual machine in a different location' and then set desired paths inside the three input fields. Click 'Next'.



No virtual machines were found on this server.

No item selected.

Choose Folders for Virtual Machine Files

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

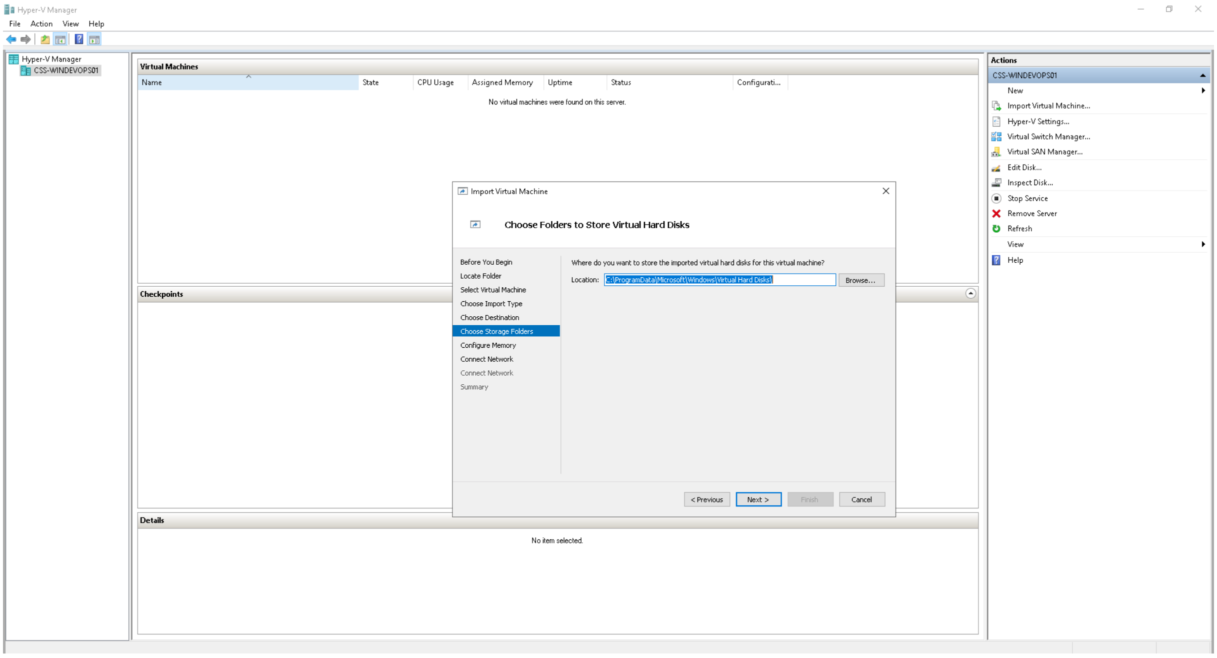
☑ Store the virtual machine in a different location

Virtual machine configuration folder: C:\ProgramData\Microsoft\Windows\Hyper-V\

Checkpoint store: dpoint Protector 5.8.1.0 Virtual Appliance\Endpoint Protector 5.8.1.0 Virtual Appliance

Smart Paging folder: dpoint Protector 5.8.1.0 Virtual Appliance\Endpoint Protector 5.8.1.0 Virtual Appliance

3.5 On the **Choose Folders to Store Virtual Hard Disks** section, set the desired path for storing imported virtual hard disk. Click Next.



No virtual machines were found on this server.

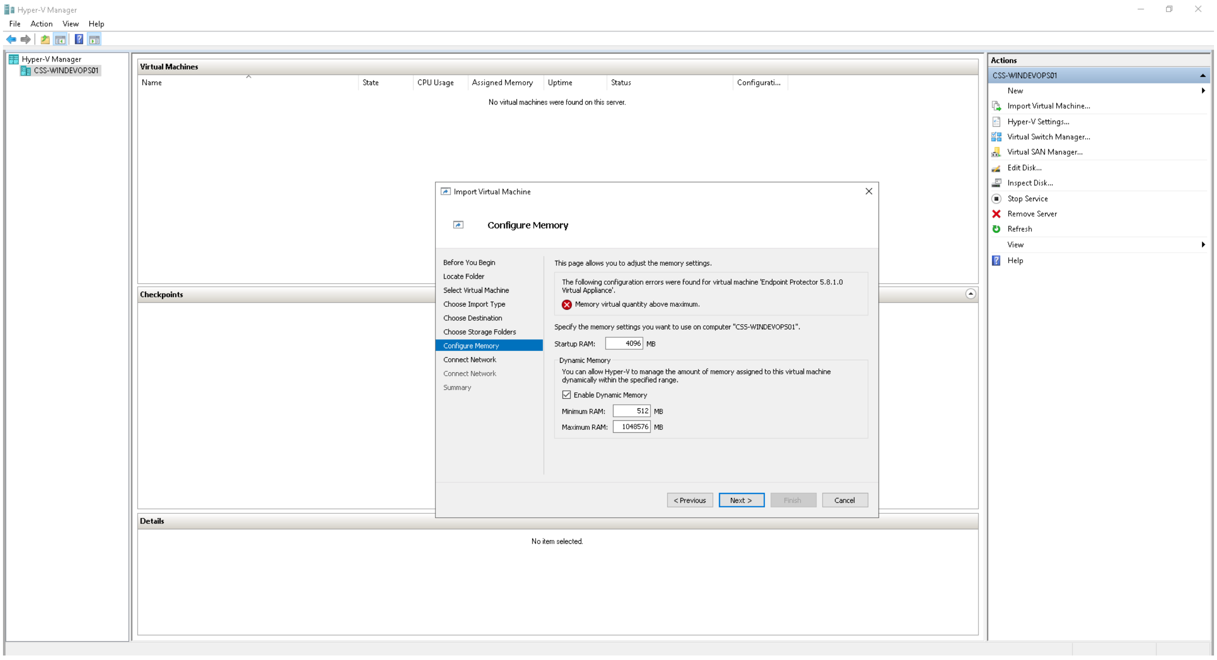
No item selected.

Choose Folders to Store Virtual Hard Disks

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

Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\

3.6 If you get to the **Get Memory** step, it means you have insufficient memory on the Hyper-V Host. Please abort the process here and either increase memory on the Host or choose another Host to import the Endpoint Protector Virtual Appliance on.



No virtual machines were found on this server.

No item selected.

This page allows you to adjust the memory settings.

The following configuration errors were found for virtual machine 'Endpoint Protector 5.8.1.0 Virtual Appliance'.

Memory virtual quantity above maximum.

Specify the memory settings you want to use on computer "CSS-WINDEVOPS01".

Startup RAM: 4096 MB

Dynamic Memory

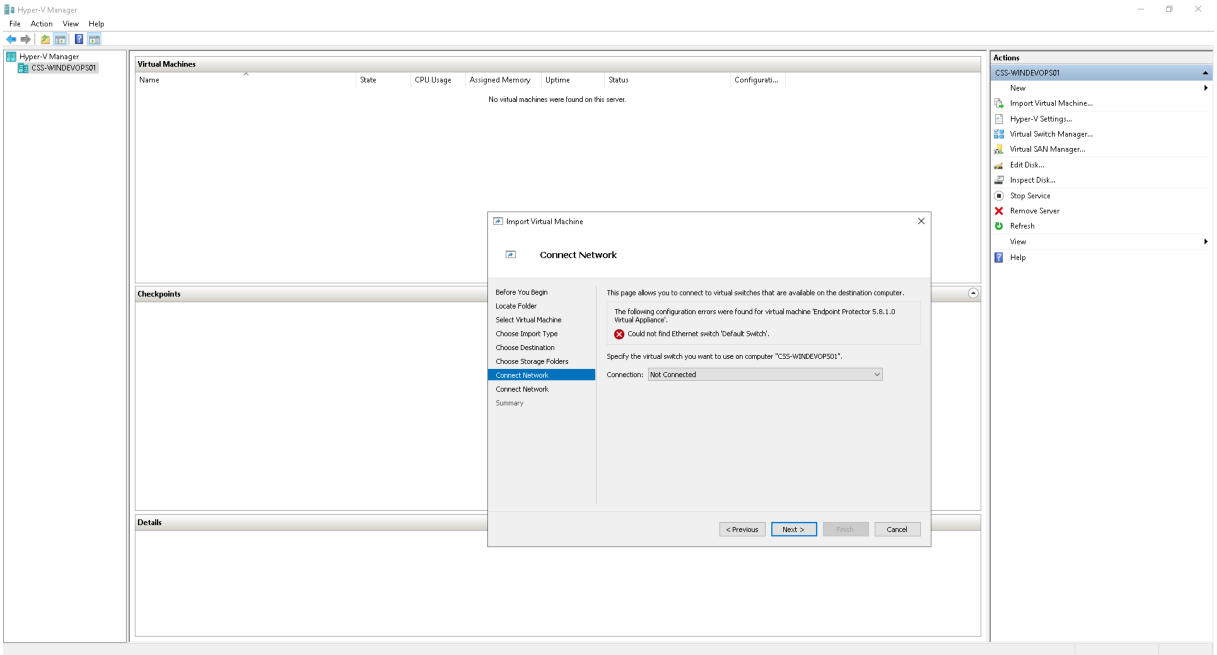
You can allow Hyper-V to manage the amount of memory assigned to this virtual machine dynamically within the specified range.

☑ Enable Dynamic Memory

Minimum RAM: 512 MB

Maximum RAM: 1048576 MB

3.7 On the first **Connect Network** step, please mention the virtual switch you want to use for the first virtual network interface, changing it from 'Not Connected' to desired one. Click 'Next'.



No virtual machines were found on this server.

This page allows you to connect to virtual switches that are available on the destination computer.

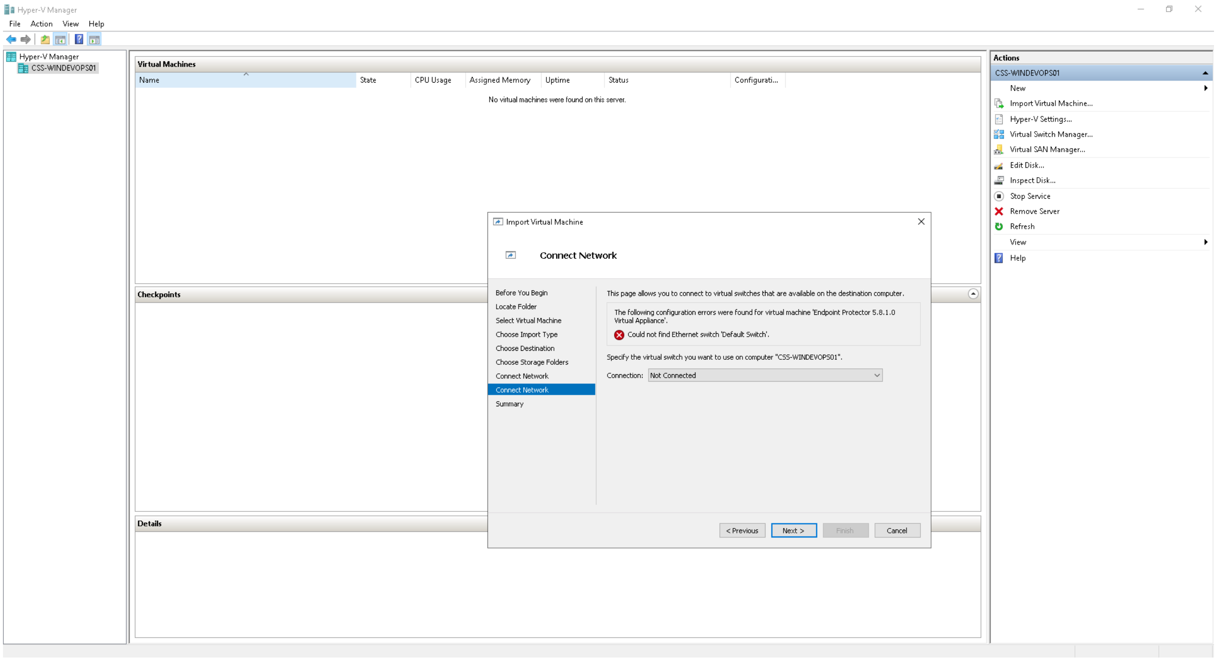
The following configuration errors were found for virtual machine 'Endpoint Protector 5.8.1.0 Virtual Appliance'.

Could not find Ethernet switch 'Default Switch'.

Specify the virtual switch you want to use on computer "CSS-WINDEVOPS01".

Connection: Not Connected

3.8 On the second **Connect Network** step, please mention the virtual switch you want to use for the second virtual network interface. You may use the same one you have used at the previous step. Click 'Next'.



No virtual machines were found on this server.

Connect Network

This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'Endpoint Protector 5.8.1.0 Virtual Appliance'.

Could not find Ethernet switch 'Default Switch'.

Specify the virtual switch you want to use on computer "CSS-WINDEVOPS01".

Connection: Not Connected

3.9 On the **Completing Import Wizard** step, check that the settings are the ones wanted, and press ‘Finish’.

4. The new Virtual Machine will appear in the Virtual Machines list;

Follow the Endpoint Protector Appliance User Manual from this point on.

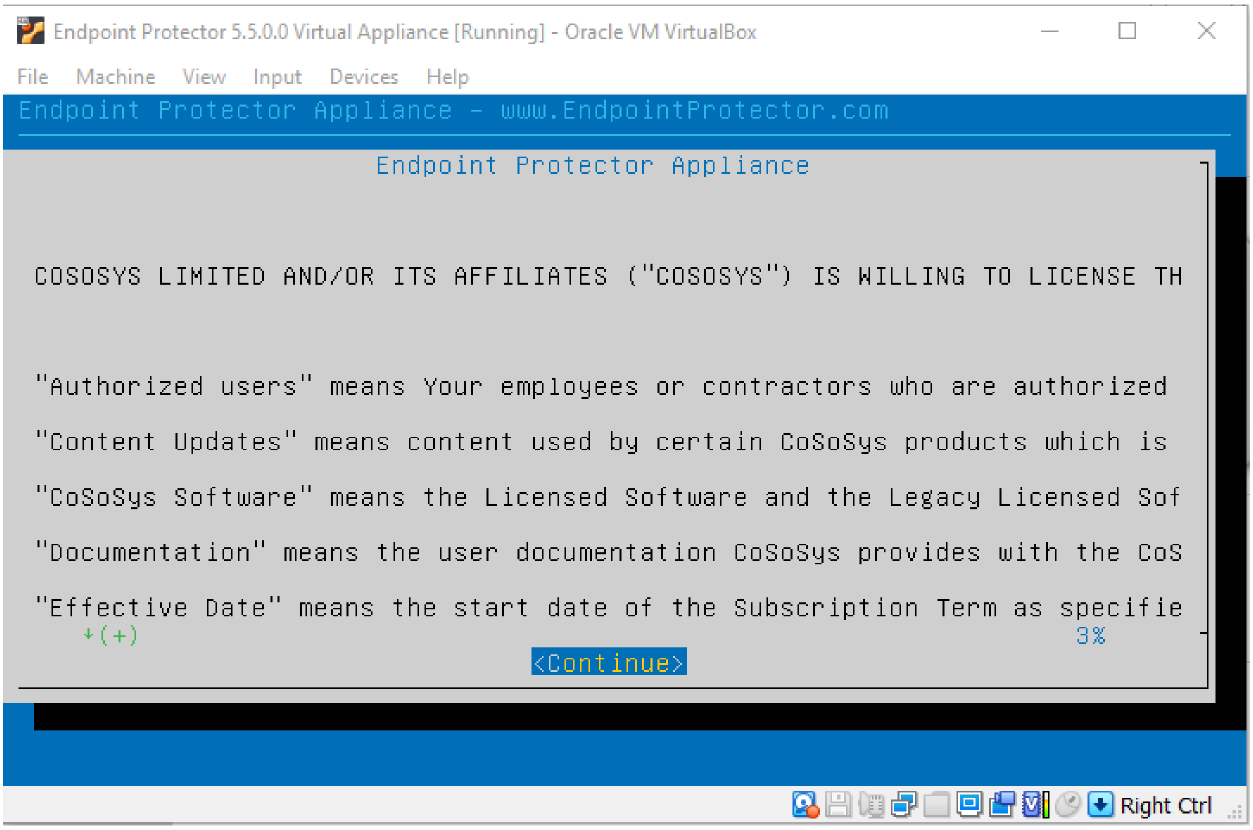
5. Virtual Appliance Setup Wizard

The Endpoint Protector Appliance (virtual or hardware) requires incoming traffic for ports 443 and 80 to be whitelisted from the firewall. They are used for:

- Endpoint Protector Server and Client communication: 443
- Mobile Device Management Cloud (cloud.endpointprotector.com): 443
- Live Update (liveupdate.endpointprotector.com): 80 & 443

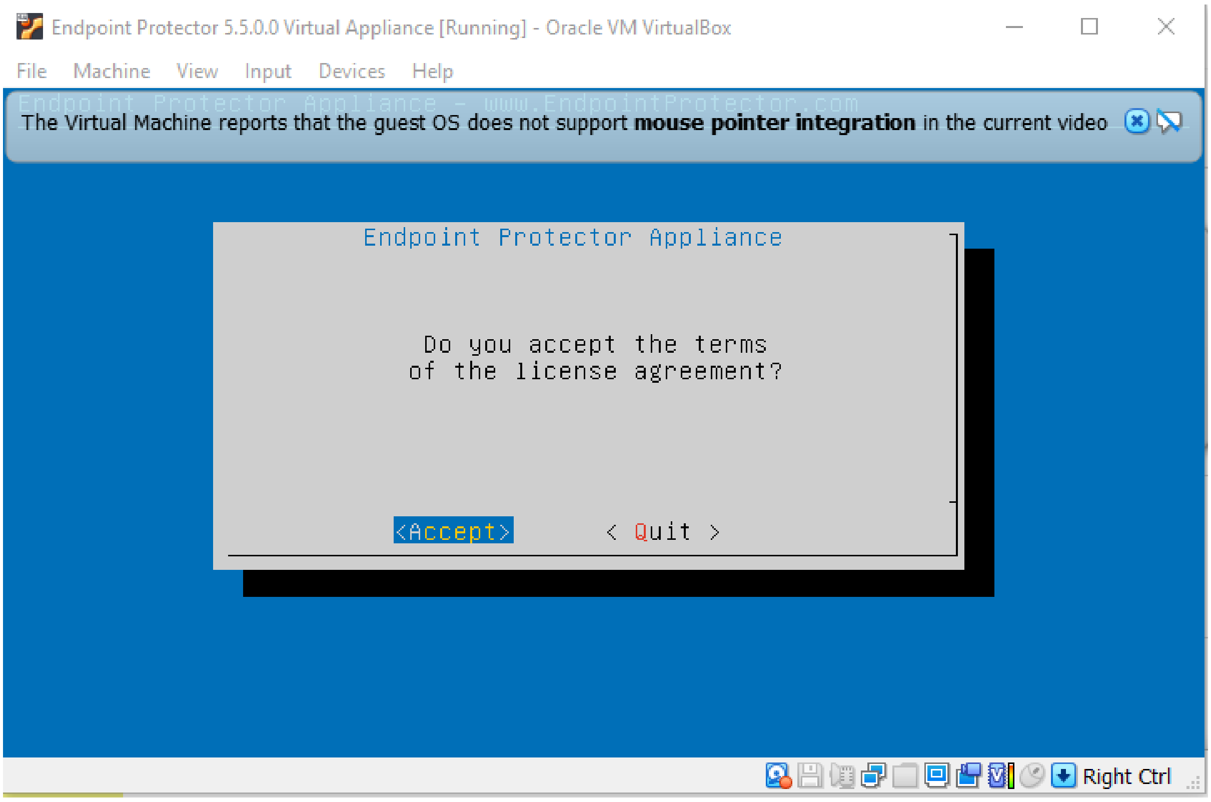
To configure the Endpoint Protector Appliance for the first time, follow the steps below.

1. Select **Continue** when finished reading the End User License Agreement;


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

                 Endpoint Protector Appliance


COSOSYS LIMITED AND/OR ITS AFFILIATES ("COSOSYS") IS WILLING TO LICENSE TH


"Authorized users" means Your employees or contractors who are authorized
"Content Updates" means content used by certain CoSoSys products which is
"CoSoSys Software" means the Licensed Software and the Legacy Licensed Sof
"Documentation" means the user documentation CoSoSys provides with the CoS
"Effective Date" means the start date of the Subscription Term as specifie
   ↓(+)                                                          3%
                          <Continue>
```

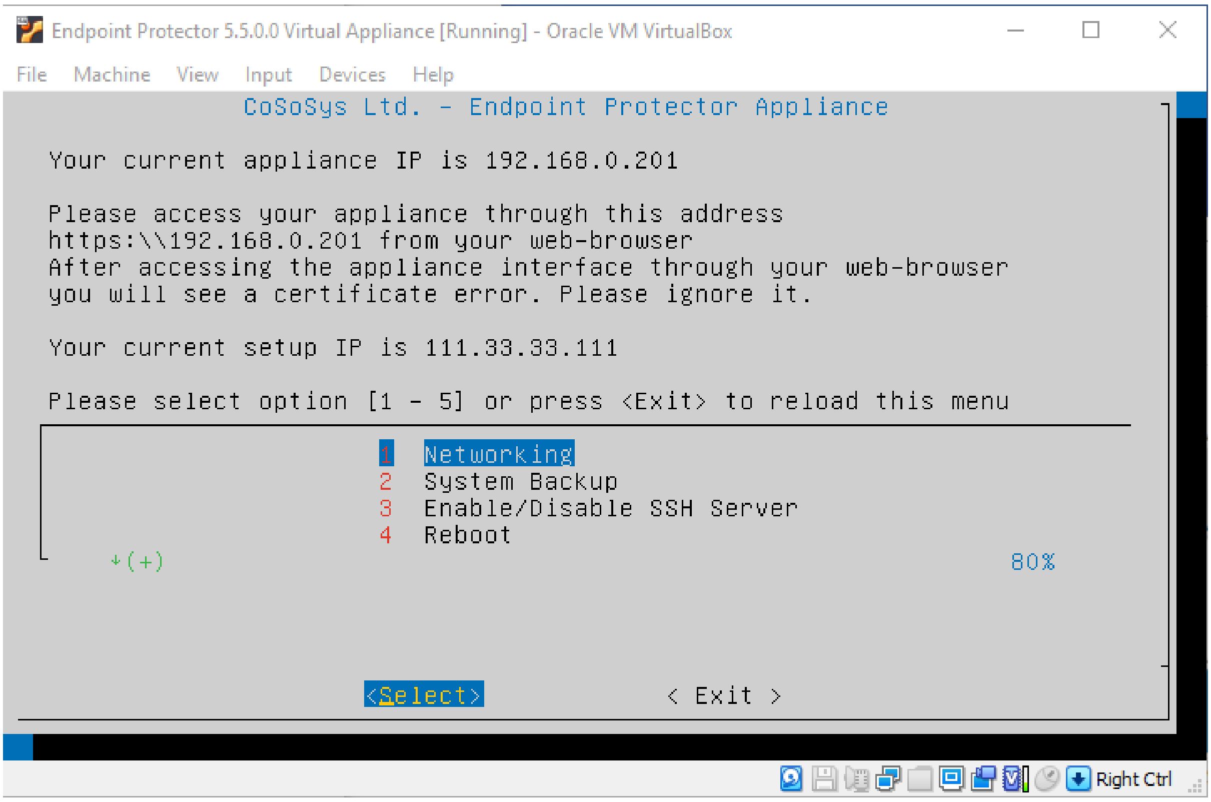
2. Select **Accept;**


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

The Virtual Machine reports that the guest OS does not support **mouse pointer integration** in the current video

```
Endpoint Protector Appliance - www.EndpointProtector.com

                    Endpoint Protector Appliance


                        Do you accept the terms
                       of the license agreement?



                   <Accept>        < Quit >
```

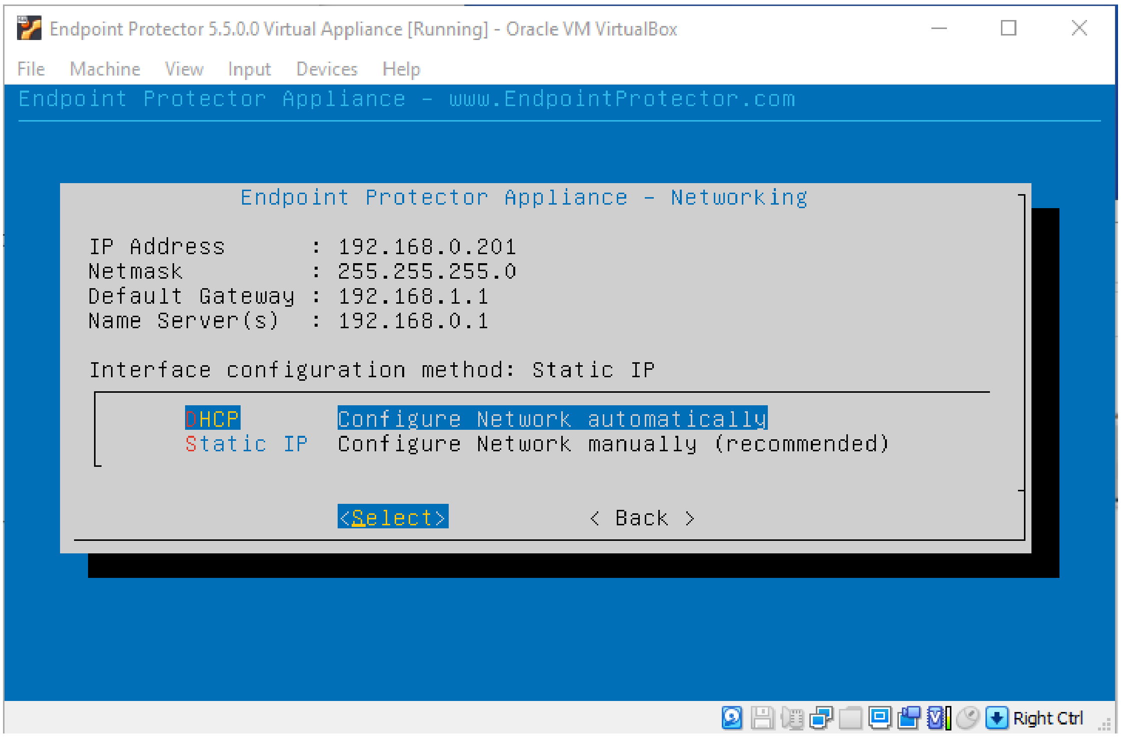
3. Select **Networking;**


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
              CoSoSys Ltd. - Endpoint Protector Appliance

 Your current appliance IP is 192.168.0.201

 Please access your appliance through this address
 https:\\192.168.0.201 from your web-browser
 After accessing the appliance interface through your web-browser
 you will see a certificate error. Please ignore it.

 Your current setup IP is 111.33.33.111

 Please select option [1 - 5] or press <Exit> to reload this menu

                      1  Networking
                      2  System Backup
                      3  Enable/Disable SSH Server
                      4  Reboot
     ↓(+)                                                 80%



                  <Select>          < Exit >
```

4. The configuration methods are now available.

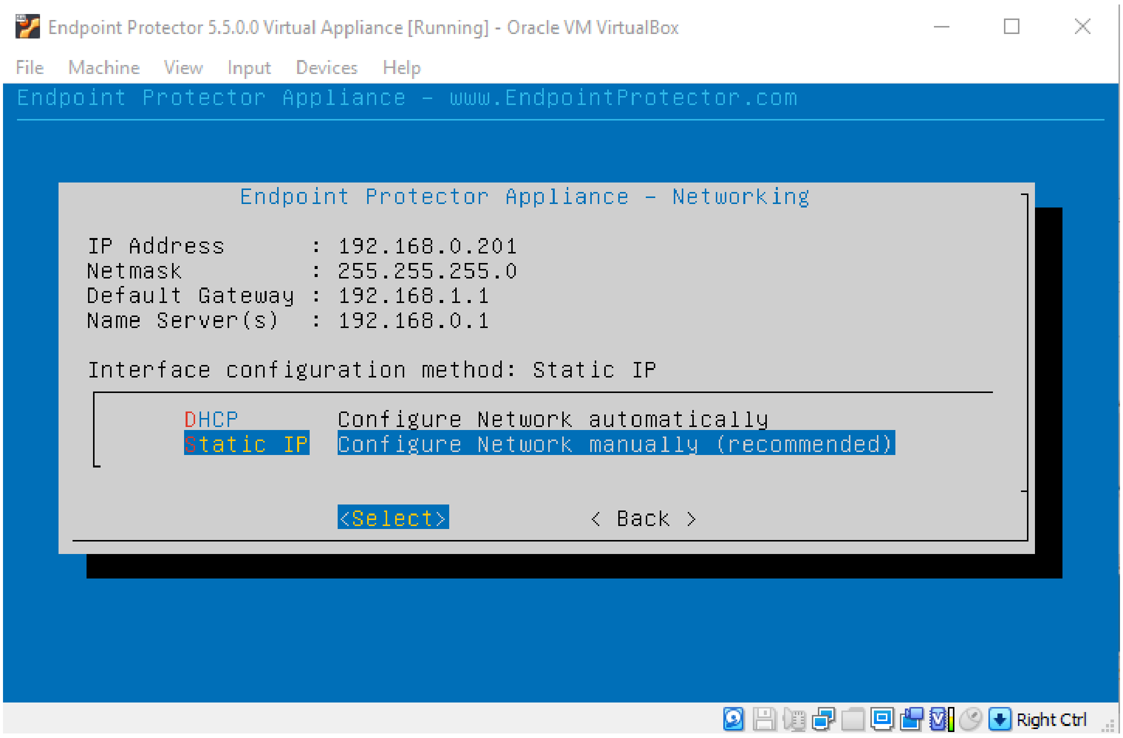
Important: We recommend a manual configuration of the network settings.


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

              Endpoint Protector Appliance - Networking

  IP Address      : 192.168.0.201
  Netmask         : 255.255.255.0
  Default Gateway : 192.168.1.1
  Name Server(s)  : 192.168.0.1

  Interface configuration method: Static IP

        DHCP        Configure Network automatically
        Static IP   Configure Network manually (recommended)

                    <Select>            < Back >
```

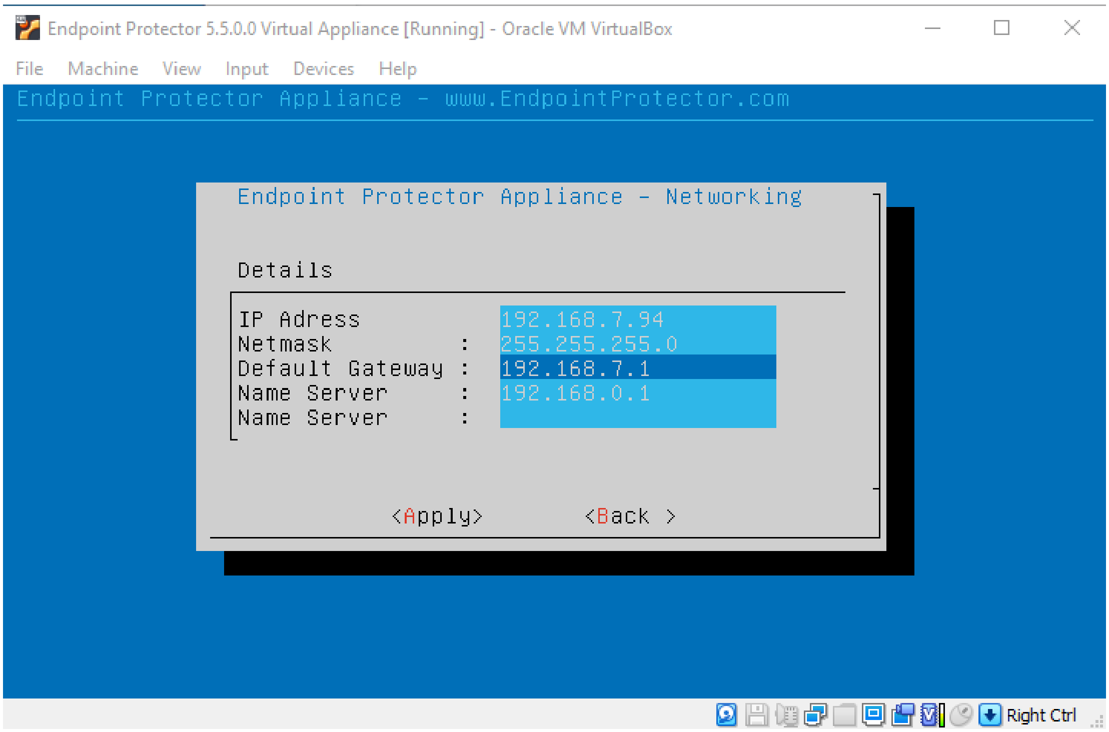
5.1.1 Manual configuration

1. Select **Configure Network manually (recommended);**


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

              Endpoint Protector Appliance - Networking

  IP Address      : 192.168.0.201
  Netmask         : 255.255.255.0
  Default Gateway : 192.168.1.1
  Name Server(s)  : 192.168.0.1

  Interface configuration method: Static IP

        DHCP        Configure Network automatically
        Static IP   Configure Network manually (recommended)

                    <Select>            < Back >
```

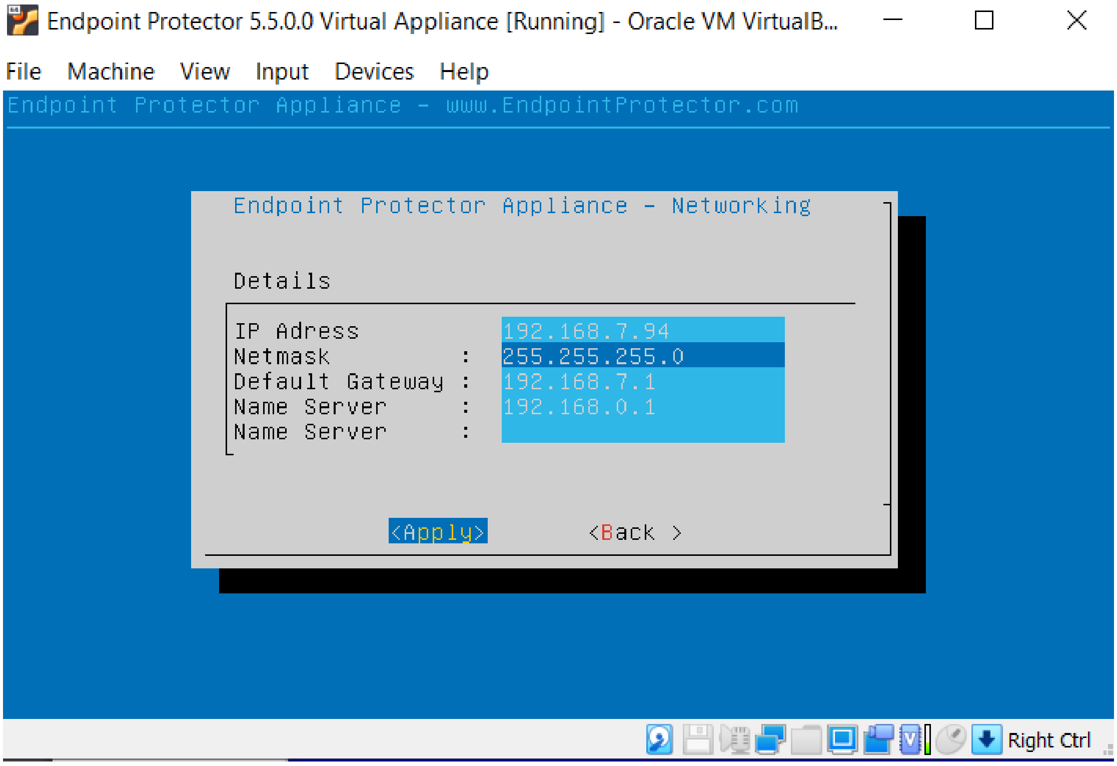
2. Set the IP Address, and Default Gateway (in our example we set the IP Address as 192.168.7.94 and the Default Gateway as 192.168.7.1);



Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

Endpoint Protector Appliance - Networking

Details
IP Adress              192.168.7.94
Netmask         :      255.255.255.0
Default Gateway :      192.168.7.1
Name Server     :      192.168.0.1
Name Server     :

        <Apply>        <Back >
```

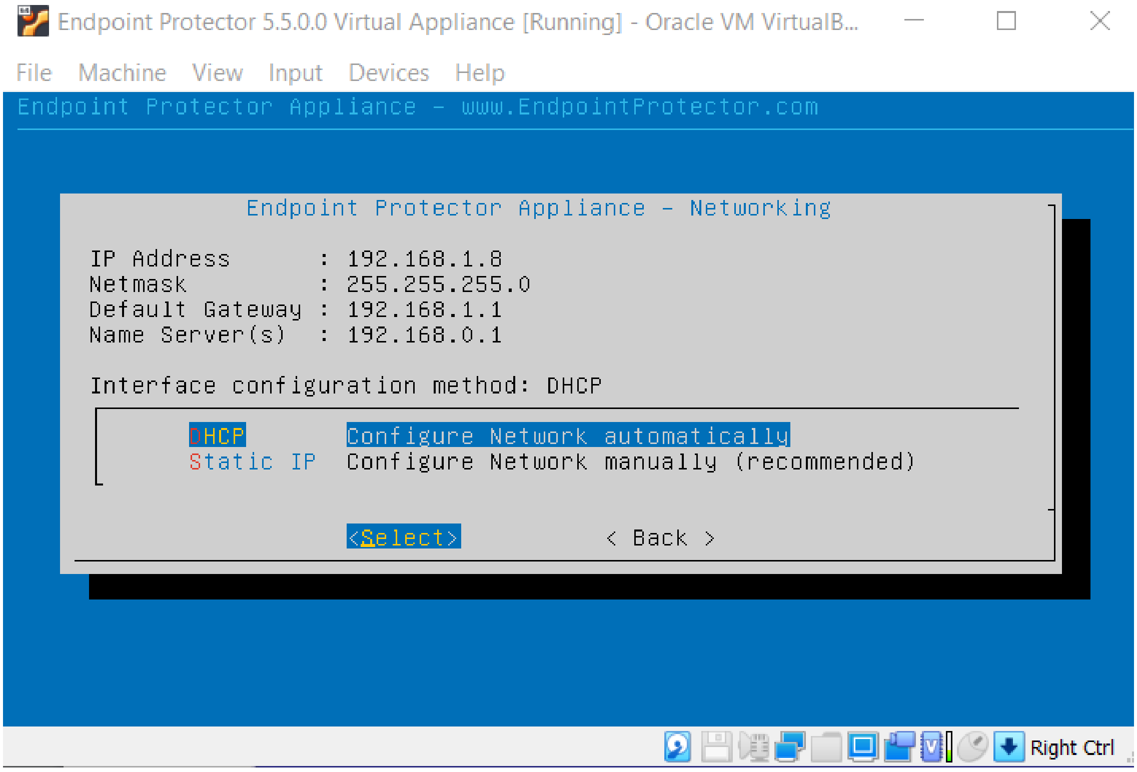
3. Press **Tab;**



Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualB...
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

Endpoint Protector Appliance - Networking

Details
IP Adress              192.168.7.94
Netmask         :      255.255.255.0
Default Gateway :      192.168.7.1
Name Server     :      192.168.0.1
Name Server     :

        <Apply>        <Back >
```

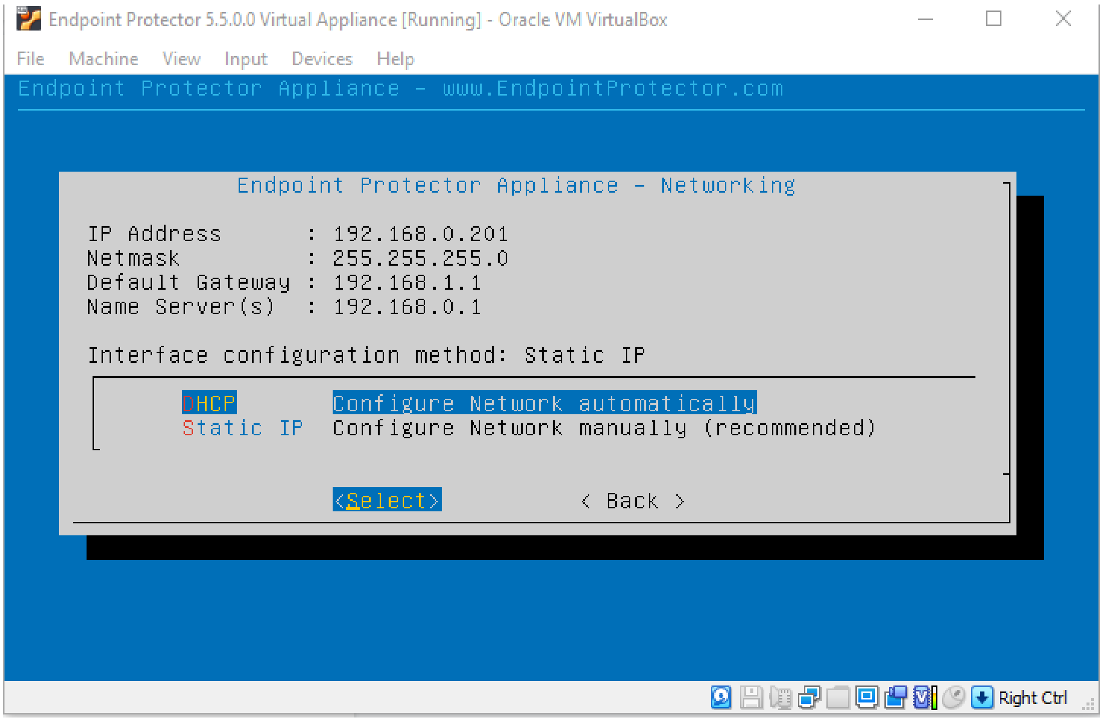
4. Select **Apply -** the virtual appliance is now accessible from the configured IP Address. (in our example, https:// 192.168.7.94)


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualB...
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

          Endpoint Protector Appliance - Networking

 IP Address      : 192.168.1.8
 Netmask         : 255.255.255.0
 Default Gateway : 192.168.1.1
 Name Server(s)  : 192.168.0.1

 Interface configuration method: DHCP

       DHCP       Configure Network automatically
       Static IP  Configure Network manually (recommended)

                  <Select>             < Back >
```

5.1.1. Automatic configuration

Select configure network automatically, and select **Enter**. The IP Address and Default Gateway will be configured automatically.


Endpoint Protector 5.5.0.0 Virtual Appliance [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Endpoint Protector Appliance - www.EndpointProtector.com

          Endpoint Protector Appliance - Networking

 IP Address      : 192.168.0.201
 Netmask         : 255.255.255.0
 Default Gateway : 192.168.1.1
 Name Server(s)  : 192.168.0.1

 Interface configuration method: Static IP

       DHCP       Configure Network automatically
       Static IP  Configure Network manually (recommended)

                  <Select>             < Back >
```

6. Endpoint Protector Configuration

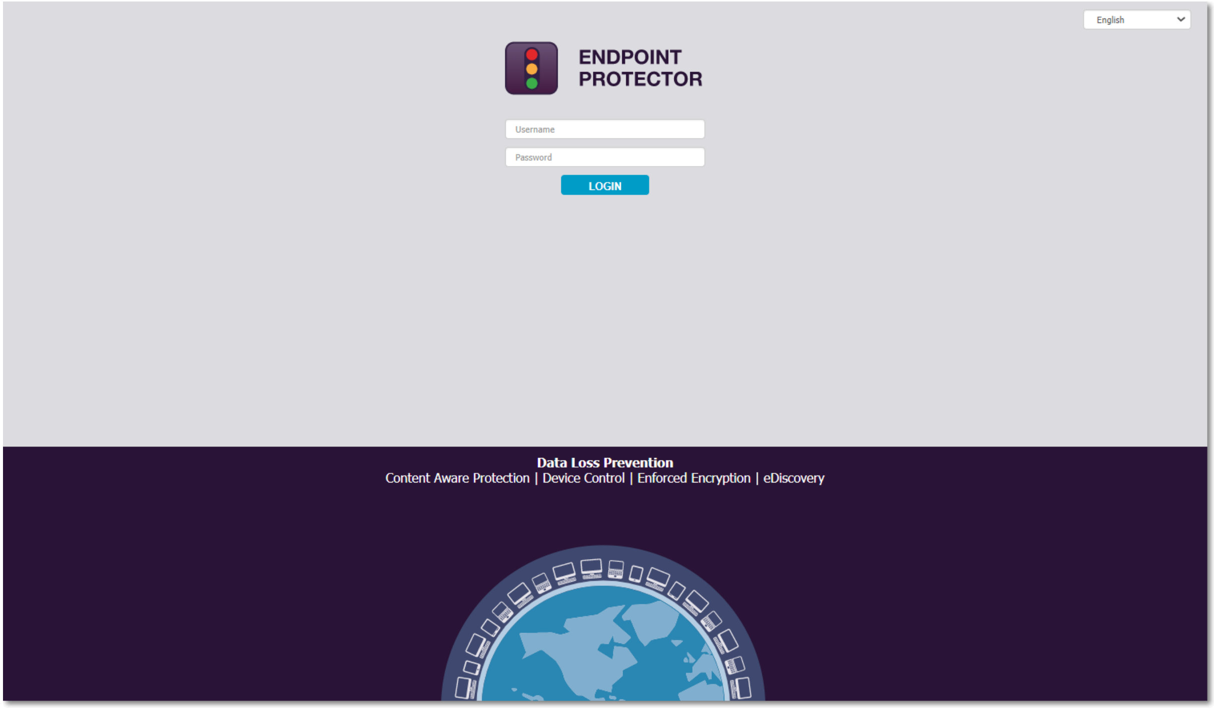
After assigning a static IP in the Endpoint Protector Setup Wizard, you can connect the Appliance to your network.

The Endpoint Protector User Interface can be accessed by going to the defined HTTPS address (e.g. default: https://192.168.0.201).

6.1. Login to Endpoint Protector

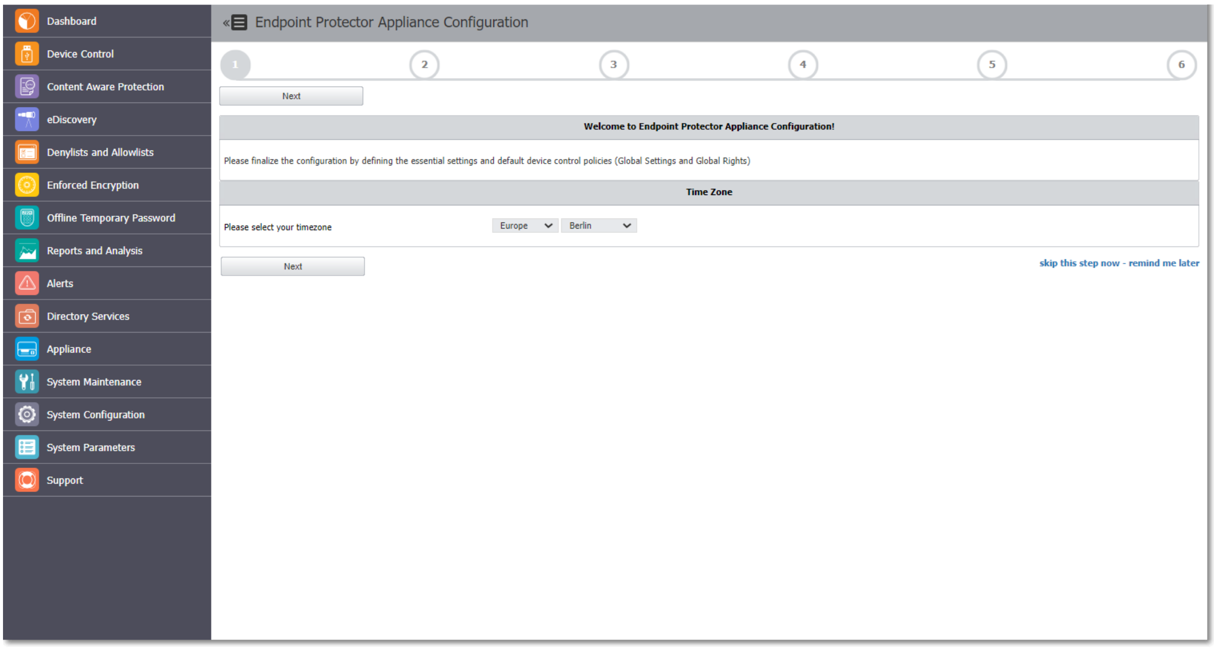
Enter the username and password defined in the Endpoint Protector Setup Wizard.

Use the default Endpoint Protector credentials for the root account.


English
ENDPOINT PROTECTOR
Username
Password
LOGIN
Data Loss Prevention
Content Aware Protection | Device Control | Enforced Encryption | eDiscovery

6.2. Configuration Wizard

To finalize the Endpoint Protector Configuration, some important basic settings and the default device control policy (Global Settings) have to be defined by following the steps in the Configuration Wizard.



Endpoint Protector Appliance Configuration

Welcome to Endpoint Protector Appliance Configuration!

Please finalize the configuration by defining the essential settings and default device control policies (Global Settings and Global Rights)

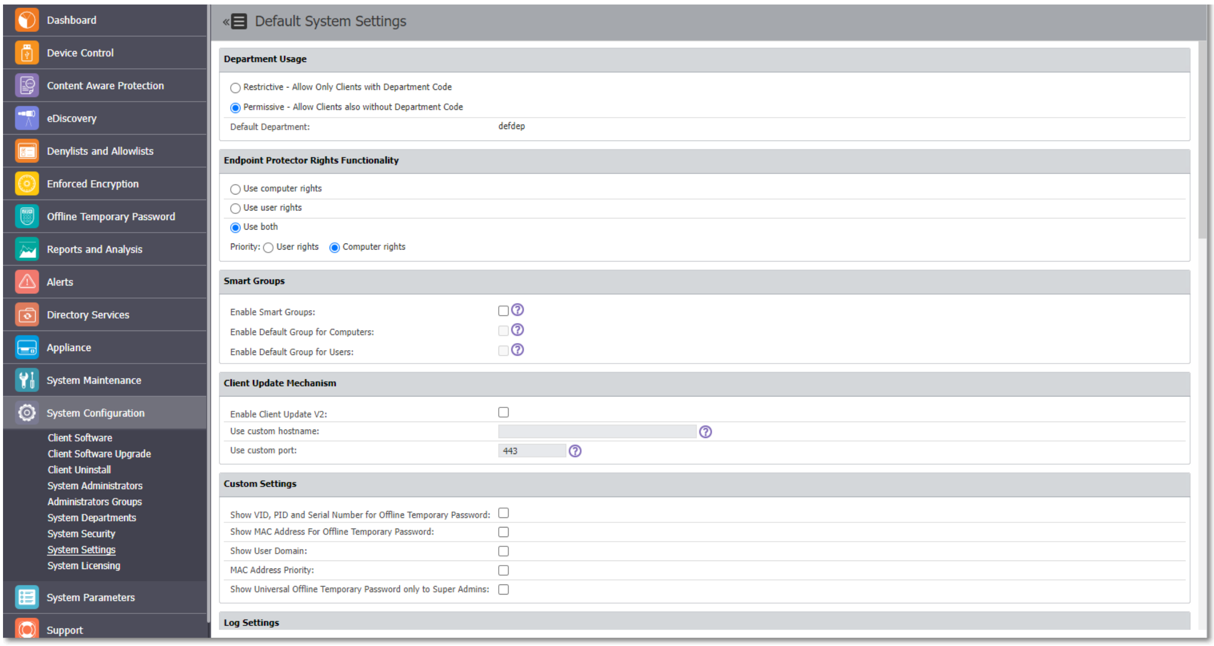
Time Zone

Please select your timezone: Europe, Berlin

skip this step now - remind me later

6.3. System Settings

Some basic settings are required for the Endpoint Protector to function properly. Select what rights have priority, the E-mail address used to receive Alerts, the main Administrator contact, the Proxy Server Settings, and more.



Default System Settings

Department Usage

○ Restrictive - Allow Only Clients with Department Code
● Permissive - Allow Clients also without Department Code
Default Department: defdep

Endpoint Protector Rights Functionality

○ Use computer rights
○ Use user rights
● Use both
Priority: ○ User rights ● Computer rights

Smart Groups

Enable Smart Groups: □
Enable Default Group for Computers: □
Enable Default Group for Users: □

Client Update Mechanism

Enable Client Update V2: □
Use custom hostname:
Use custom port: 443

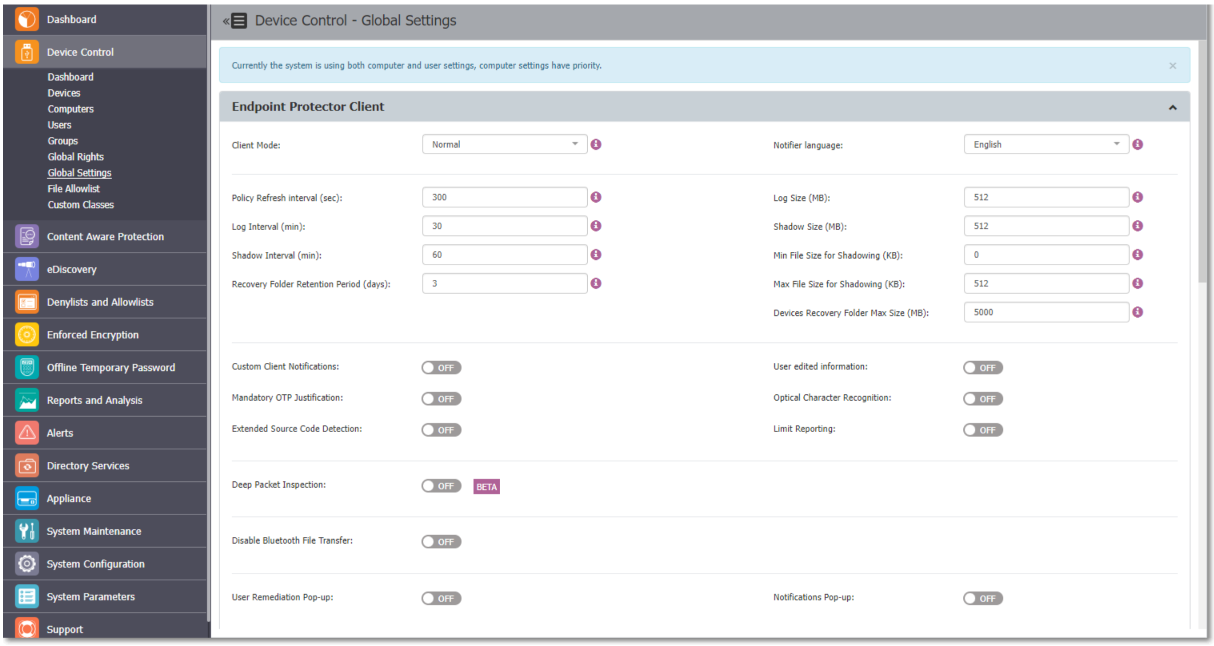
Custom Settings

Show VID, PID and Serial Number for Offline Temporary Password: □
Show MAC Address For Offline Temporary Password: □
Show User Domain: □
MAC Address Priority: □
Show Universal Offline Temporary Password only to Super Admins: □

Log Settings

Additionally, the Endpoint Protector Client Refresh Interval, the activated or deactivated features such as File Tracing and File Shadowing, and the default parameters for the generated logs can also be configured.

By default, the recommended settings are already configured and they apply globally throughout the entire network.



Device Control - Global Settings

Currently the system is using both computer and user settings, computer settings have priority.

Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Policy Refresh interval (sec): 300

Log Interval (min): 30

Shadow Interval (min): 60

Recovery Folder Retention Period (days): 3

Log Size (MB): 512

Shadow Size (MB): 512

Min File Size for Shadowing (KB): 0

Max File Size for Shadowing (KB): 512

Devices Recovery Folder Max Size (MB): 5000

Custom Client Notifications: OFF

Mandatory OTP Justification: OFF

Extended Source Code Detection: OFF

User edited information: OFF

Optical Character Recognition: OFF

Limit Reporting: OFF

Deep Packet Inspection: OFF BETA

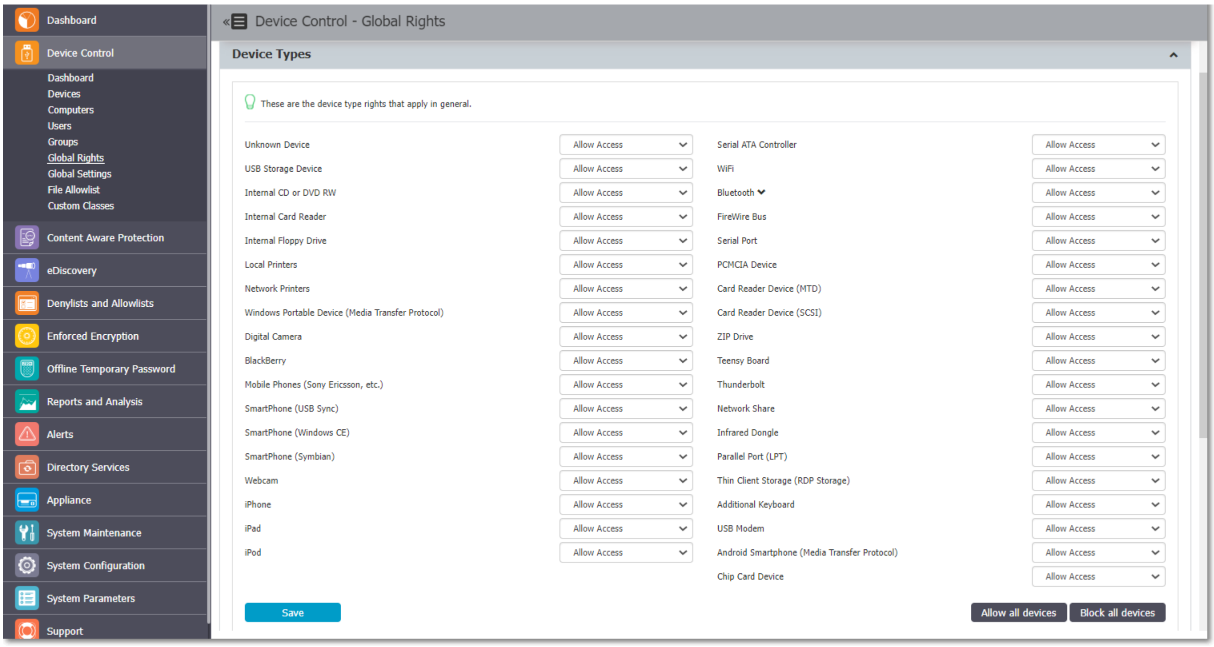
Disable Bluetooth File Transfer: OFF

User Remediation Pop-up: OFF

Notifications Pop-up: OFF

6.4. Default Device Control Rights

As Endpoint Protector provides the Device Control module enabled by default, the use of USB devices and peripheral ports have the Global Rights preconfigured. They can be changed later at any time or they can be applied more granularly (per device, computer, user, or group).



Device Control - Global Rights

Device Types

These are the device type rights that apply in general.

Unknown Device	Allow Access	Serial ATA Controller	Allow Access
USB Storage Device	Allow Access	WiFi	Allow Access
Internal CD or DVD RW	Allow Access	Bluetooth	Allow Access
Internal Card Reader	Allow Access	FireWire Bus	Allow Access
Internal Floppy Drive	Allow Access	Serial Port	Allow Access
Local Printers	Allow Access	PCMCIA Device	Allow Access
Network Printers	Allow Access	Card Reader Device (MTD)	Allow Access
Windows Portable Device (Media Transfer Protocol)	Allow Access	Card Reader Device (SCSI)	Allow Access
Digital Camera	Allow Access	ZIP Drive	Allow Access
BlackBerry	Allow Access	Teensy Board	Allow Access
Mobile Phones (Sony Ericsson, etc.)	Allow Access	Thunderbolt	Allow Access
SmartPhone (USB Sync)	Allow Access	Network Share	Allow Access
SmartPhone (Windows CE)	Allow Access	Infrared Dongle	Allow Access
SmartPhone (Symbian)	Allow Access	Parallel Port (LPT)	Allow Access
Webcam	Allow Access	Thin Client Storage (RDP Storage)	Allow Access
iPhone	Allow Access	Additional Keyboard	Allow Access
iPad	Allow Access	USB Modem	Allow Access
iPod	Allow Access	Android Smartphone (Media Transfer Protocol)	Allow Access
		Chip Card Device	Allow Access

6.5. Finishing the Endpoint Protector Configuration Wizard

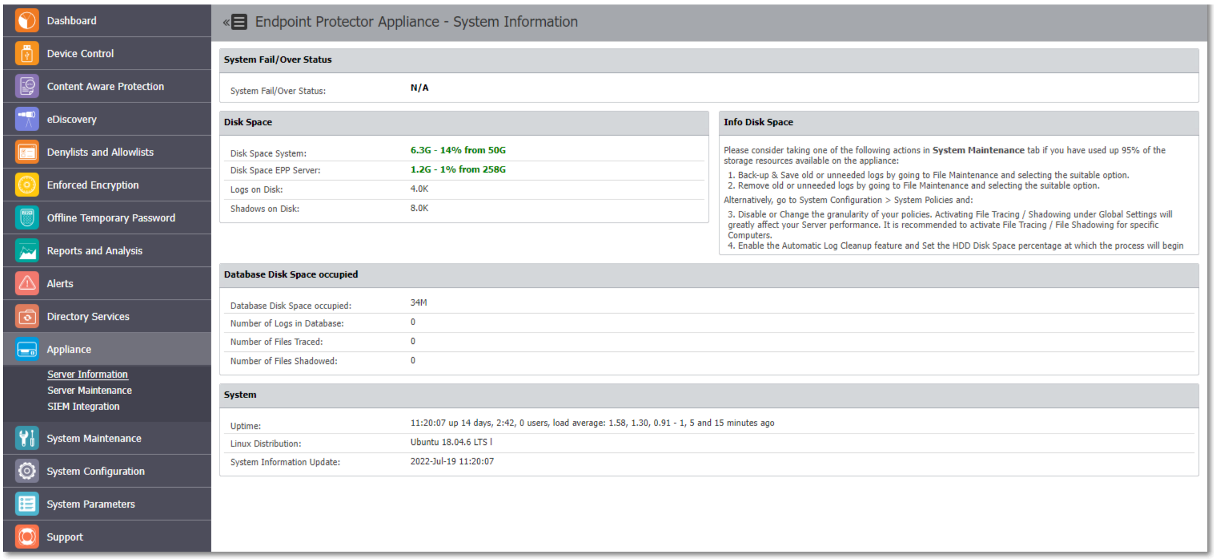
After following the above steps, the Endpoint Protector setup and configuration are completed. The next step is to deploy the Endpoint Protector Clients to the Windows, Mac, and Linux computers that need to be protected.

7. Server Information and Maintenance

The Endpoint Protector Server Information and Maintenance Settings can be accessed from the Appliance section in the main menu.

7.1. Server Information

This section displays information about the Server’s current state.



Endpoint Protector Appliance - System Information

System Fail/Over Status

System Fail/Over Status:	**N/A**

Disk Space

Disk Space System:	**6.3G - 14% from 50G**
Disk Space EPP Server:	**1.2G - 1% from 258G**
Logs on Disk:	4.0K
Shadows on Disk:	8.0K

Info Disk Space

Please consider taking one of the following actions in **System Maintenance** tab if you have used up 95% of the storage resources available on the appliance:

1. Back-up & Save old or unneeded logs by going to File Maintenance and selecting the suitable option.
2. Remove old or unneeded logs by going to File Maintenance and selecting the suitable option.

Alternatively, go to System Configuration > System Policies and:

3. Disable or Change the granularity of your policies. Activating File Tracing / Shadowing under Global Settings will greatly affect your Server performance. It is recommended to activate File Tracing / File Shadowing for specific Computers.
4. Enable the Automatic Log Cleanup feature and Set the HDD Disk Space percentage at which the process will begin

Database Disk Space occupied

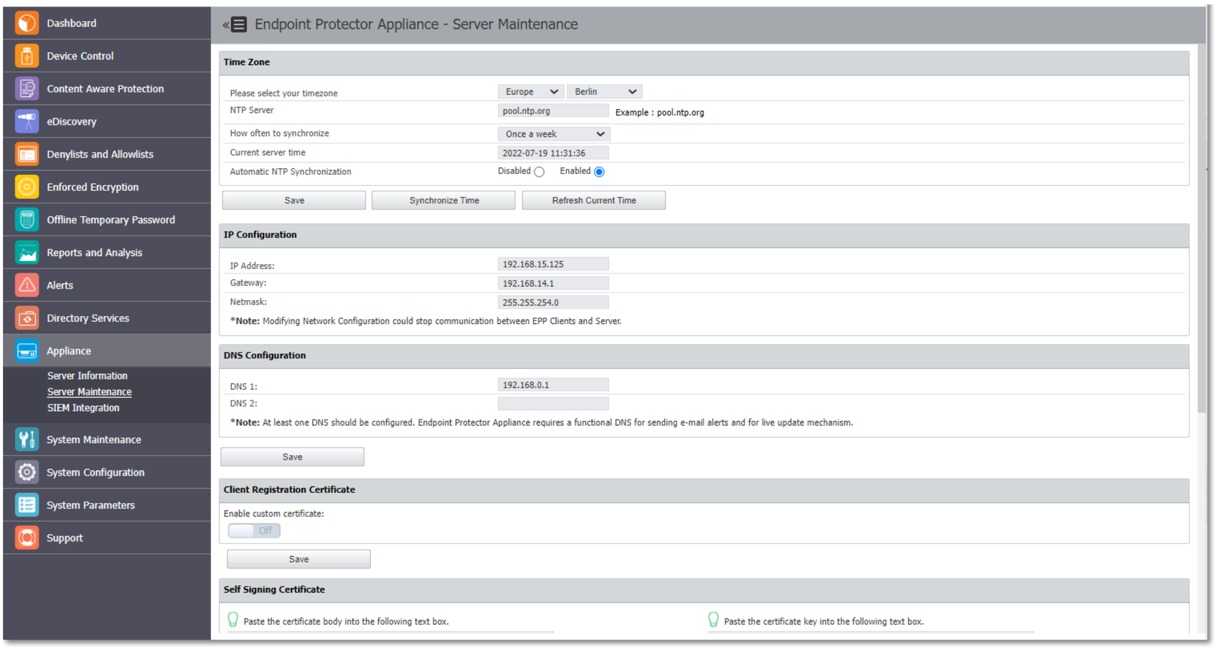
Database Disk Space occupied:	34M
Number of Logs in Database:	0
Number of Files Traced:	0
Number of Files Shadowed:	0

System

Uptime:	11:20:07 up 14 days, 2:42, 0 users, load average: 1.58, 1.30, 0.91 - 1, 5 and 15 minutes ago
Linux Distribution:	Ubuntu 18.04.6 LTS l
System Information Update:	2022-Jul-19 11:20:07

7.2. Server Maintenance

This section provides the option to configure the Appliance network settings, reboot or shut down the appliance, and more.



Endpoint Protector Appliance - Server Maintenance

Time Zone

Please select your timezone: Europe, Berlin
NTP Server: pool.ntp.org Example : pool.ntp.org
How often to synchronize: Once a week
Current server time: 2022-07-19 11:31:36
Automatic NTP Synchronization: Disabled ○ Enabled ●

IP Configuration

IP Address: 192.168.15.125
Gateway: 192.168.14.1
Netmask: 255.255.254.0

***Note:** Modifying Network Configuration could stop communication between EPP Clients and Server.

DNS Configuration

DNS 1: 192.168.0.1
DNS 2:

***Note:** At least one DNS should be configured. Endpoint Protector Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.

Client Registration Certificate

Enable custom certificate: Off

Self Signing Certificate

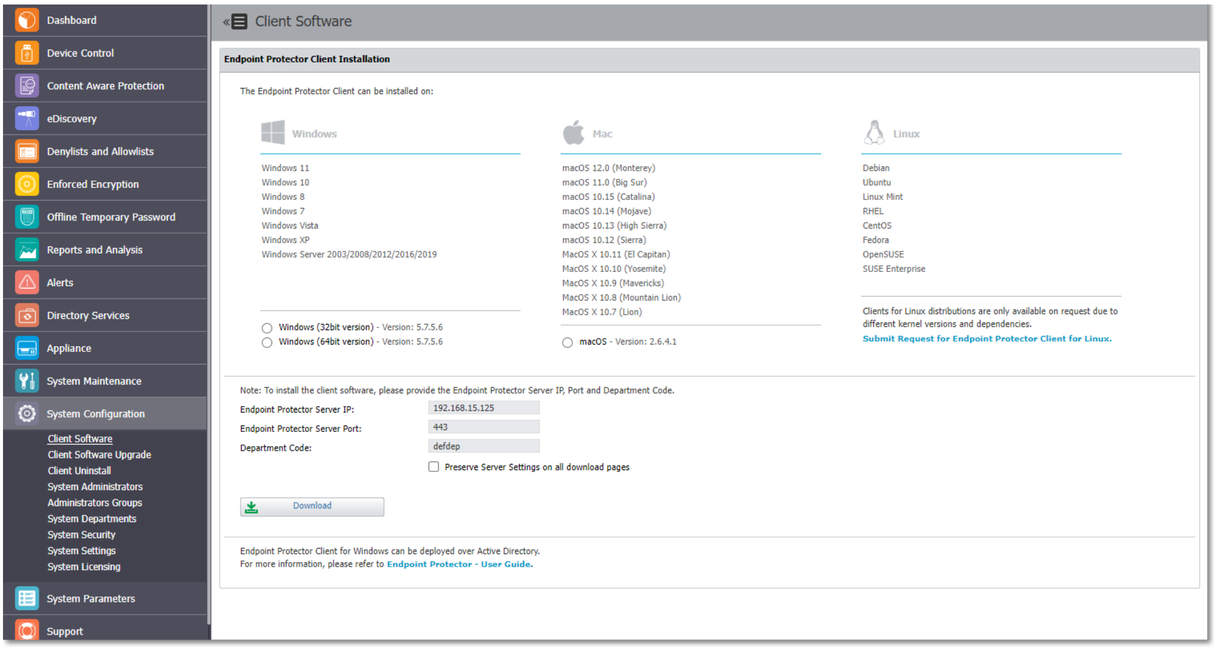
Paste the certificate body into the following text box.

Paste the certificate key into the following text box.

7.3. Endpoint Protector Client Installation

The Endpoint Protector Client needs to be deployed on the computers in the network. They can be downloaded directly from the Appliance by accessing the static IP Address in a browser (e.g.: http://192.168.0.201). The Endpoint Protector Download section can be accessed through both HTTPS and HTTP, allowing a user that is not an Endpoint Protector Administrator to deploy it themselves.

If the Endpoint Protector Administrator is going to deploy the Client on the network computers, it needs to be saved on a location. Solutions like Active Directory or Apple Remote Desktop can be used to make the deployment easier.



Client Software

Endpoint Protector Client Installation

The Endpoint Protector Client can be installed on:

Windows	Mac	Linux
Windows 11 Windows 10 Windows 8 Windows 7 Windows Vista Windows XP Windows Server 2003/2008/2012/2016/2019	macOS 12.0 (Monterey) macOS 11.0 (Big Sur) macOS 10.15 (Catalina) macOS 10.14 (Mojave) macOS 10.13 (High Sierra) macOS 10.12 (Sierra) MacOS X 10.11 (El Capitan) MacOS X 10.10 (Yosemite) MacOS X 10.9 (Mavericks) MacOS X 10.8 (Mountain Lion) MacOS X 10.7 (Lion)	Debian Ubuntu Linux Mint RHEL CentOS Fedora OpenSUSE SUSE Enterprise
○ Windows (32bit version) - Version: 5.7.5.6 ○ Windows (64bit version) - Version: 5.7.5.6	○ macOS - Version: 2.6.4.1	Clients for Linux distributions are only available on request due to different kernel versions and dependencies. **Submit Request for Endpoint Protector Client for Linux.**

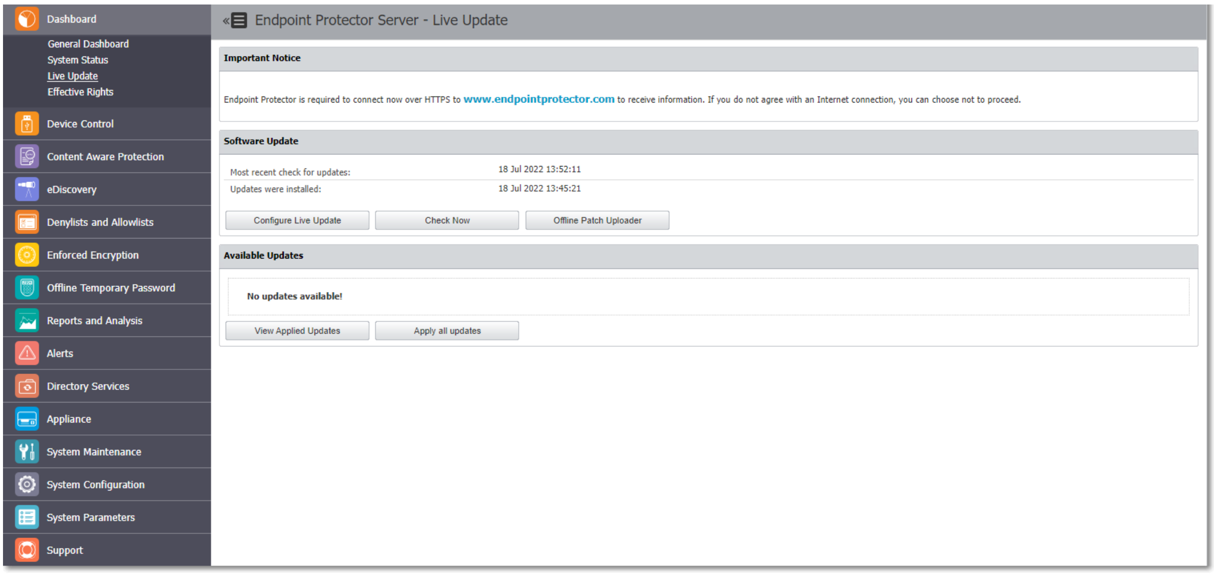
Note: To install the client software, please provide the Endpoint Protector Server IP, Port and Department Code.

Endpoint Protector Server IP: 192.168.15.125
Endpoint Protector Server Port: 443
Department Code: defdep
□ Preserve Server Settings on all download pages

Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to **Endpoint Protector - User Guide.**

7.4. Endpoint Protector Live Update

The Live Update feature allows checking online if Endpoint Protector updates are available. The process can be done manually or, if enabled, automatically. However, installing any available updates need to be done by the Endpoint Protector Administrator.



Endpoint Protector Server - Live Update

Important Notice

Endpoint Protector is required to connect now over HTTPS to www.endpointprotector.com to receive information. If you do not agree with an Internet connection, you can choose not to proceed.

Software Update

Most recent check for updates: 18 Jul 2022 13:52:11
Updates were installed: 18 Jul 2022 13:45:21

Available Updates

No updates available!

8. Hardware Appliance Setup

8.1. Endpoint Protector Appliance Delivery

When receiving the Endpoint Protector Appliance, the package contains:

- Endpoint Protector Appliance
- Power Cable
- Crossed Network Cable for the initial Appliance Setup (yellow sticker)
  (not included with the A20 model)
- Network Cable for connection of Appliance with your network
- Rack Mount Screws
  (not included with the A20 model)
- Extractable assembly rails (included in A250, A500, A1000, and A4000 models only)
- External power supply (only included and required for A20)

EndpointProtector.com
Working safe with portable devices
EndpointProtector.com
Working safe with portable devices

8.2. Connecting Appliance for Initial Setup

Connect the power cable to the appliance and a power outlet.

For the A20 appliance connect the external power supply to the A20 and the power outlet. Next, connect the blue cable to the A20 network port and then to the network.

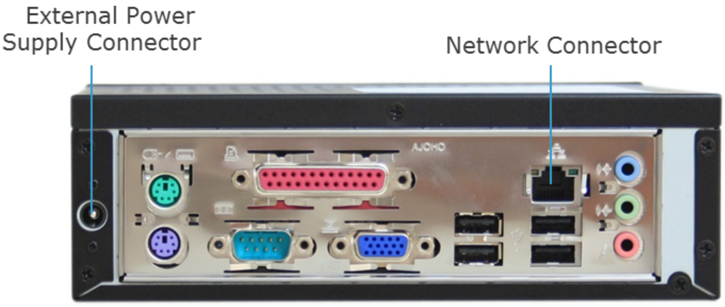
Your hardware appliance (models A50 to A4000) contains on the backside two network ports that are marked yellow for CONFIG (configuration connection) and blue for NET (network connection). The A20 hardware appliance has one network port.

Connect the CROSSED Network Cable (yellow sticker) to the configuration network port CONFIG (yellow marked) on the back of the appliance and connect it directly to a PC (a Laptop, PC, Netbook).

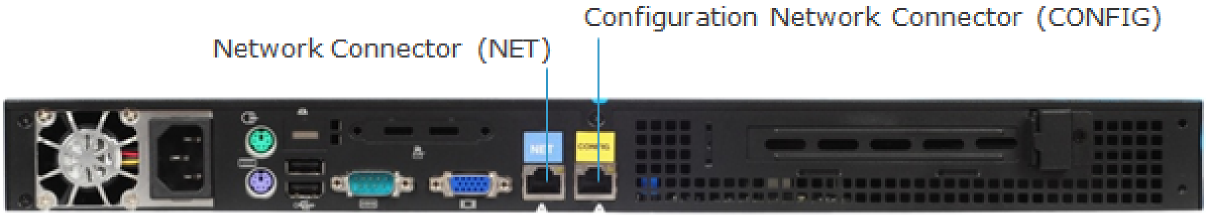
Start the Appliance by pushing the POWER button.

8.3. Hardware Appliance Back and Front Panel

8.3.1. A20 Appliance Back Panel

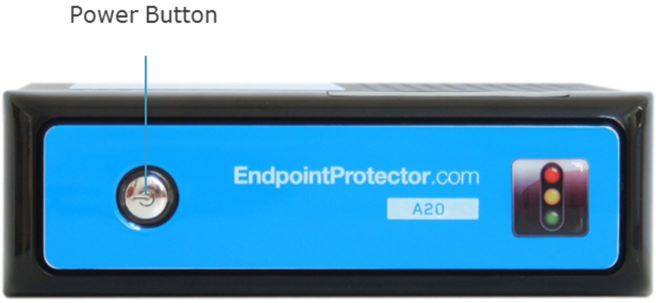


8.3.2. A50 and A100 Appliance Back Panel

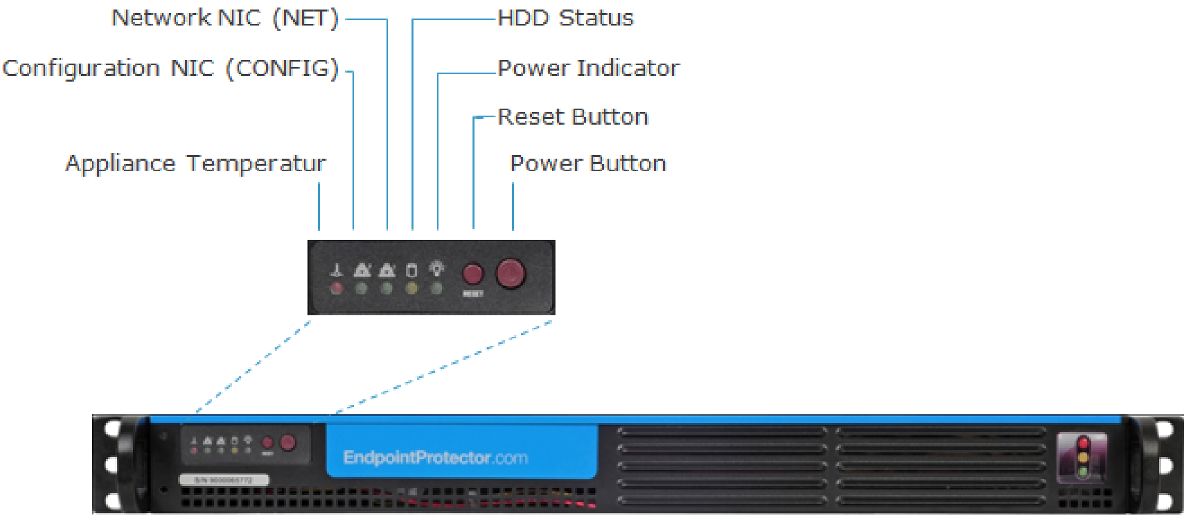


The back panels for Models A250 up to A4000 have marked network ports similar to the picture above for the A50 and A100 model.

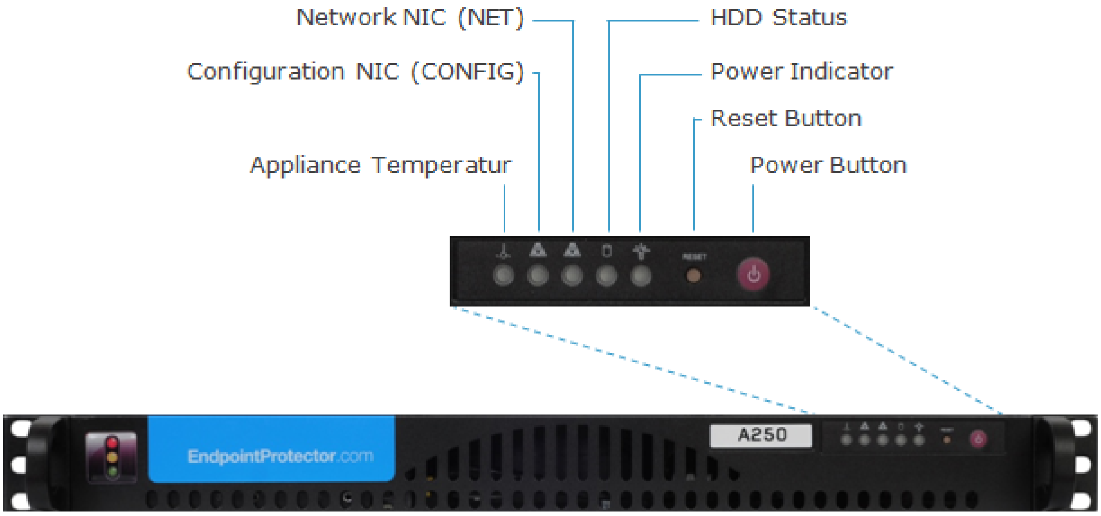
8.3.3. A20 Appliance Front Panel



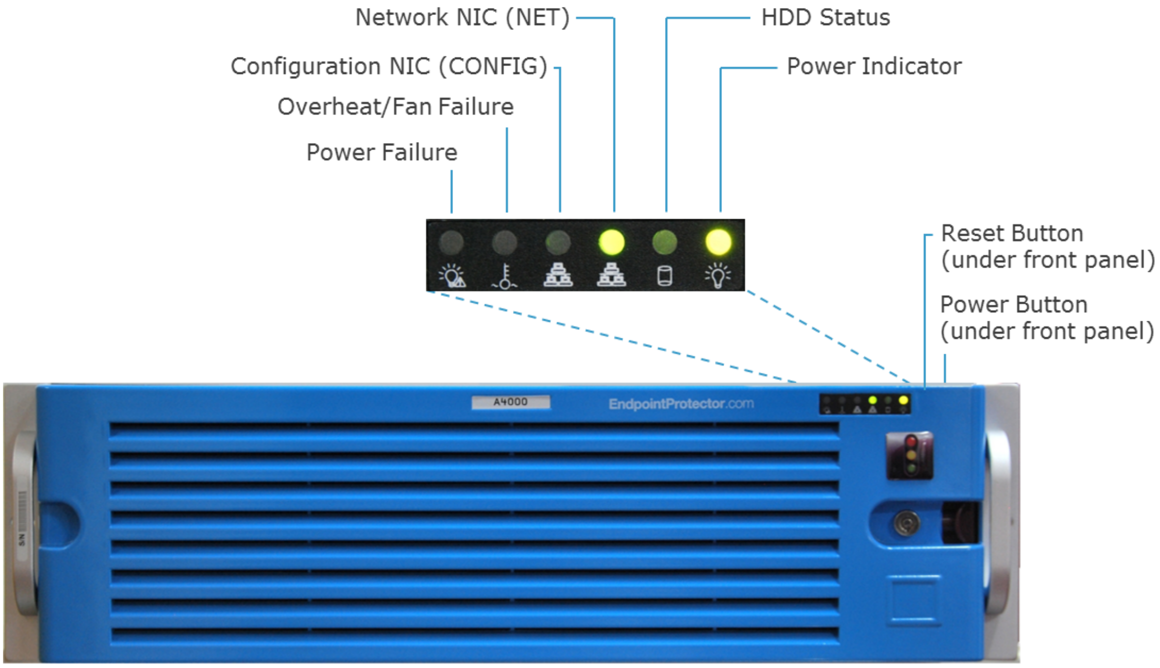
8.3.4. A50 and A100 Appliance Front Panel



8.3.5. A250, A500, and A1000 Appliance Front Panel

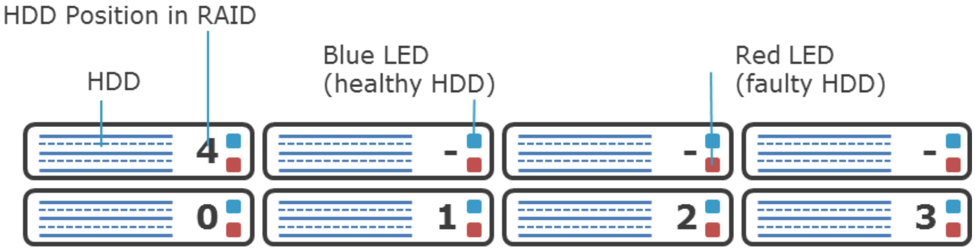


8.3.6. A2000 - A4000 Appliance Front Panel



8.4. A2000 / A4000 Appliance HDD Configuration

8.4.1. A2000 Appliance HDD Configuration

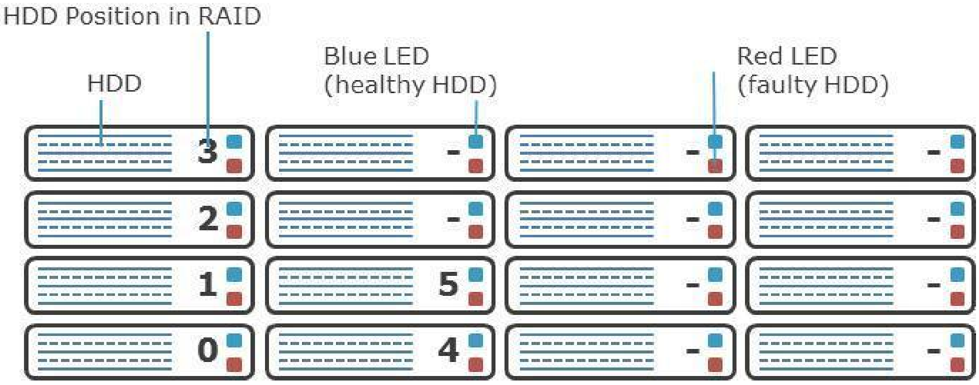


The A2000 Appliance comes with 4 HDDs in RAID 5 Configuration. The HDDs are installed in the number order 0-3.

In case of an HDD failure, the HDD can be replaced by changing it with the same model HDD.

Each HDD bay features a blue and red LED to indicate drive status. A blue indicator symbolizes a healthy hard drive, and a red indicator a bad hard drive. A faulty hard drive should be replaced immediately by an identical model.

8.4.2. A4000 Appliance HDD Configuration



The A4000 Appliance comes with 6 HDDs in RAID 5 Configuration. The HDDs are installed in the number order 0-5.

In case of an HDD failure, an HDD can be replaced by changing it with the same model HDD.

Each HDD bay features a blue and red LED to indicate drive status. A blue indicator symbolizes a healthy hard drive, and a red indicator a bad hard drive. A faulty hard drive should be replaced immediately by an identical model.

8.4.3. A2000 and A4000 Appliance HDD RAID Additional Software

The A2000 and A4000 appliance have additional configurable software from 3Ware ® preinstalled which you can use as an administrator to be warned of possible errors on one HDD by e-mail notification. More information on configuring this additional software can be found in the Appendix to this User Manual for the "3ware 3DM ® 2 ® User Manual.

8.5. Hardware Appliance Setup Wizard

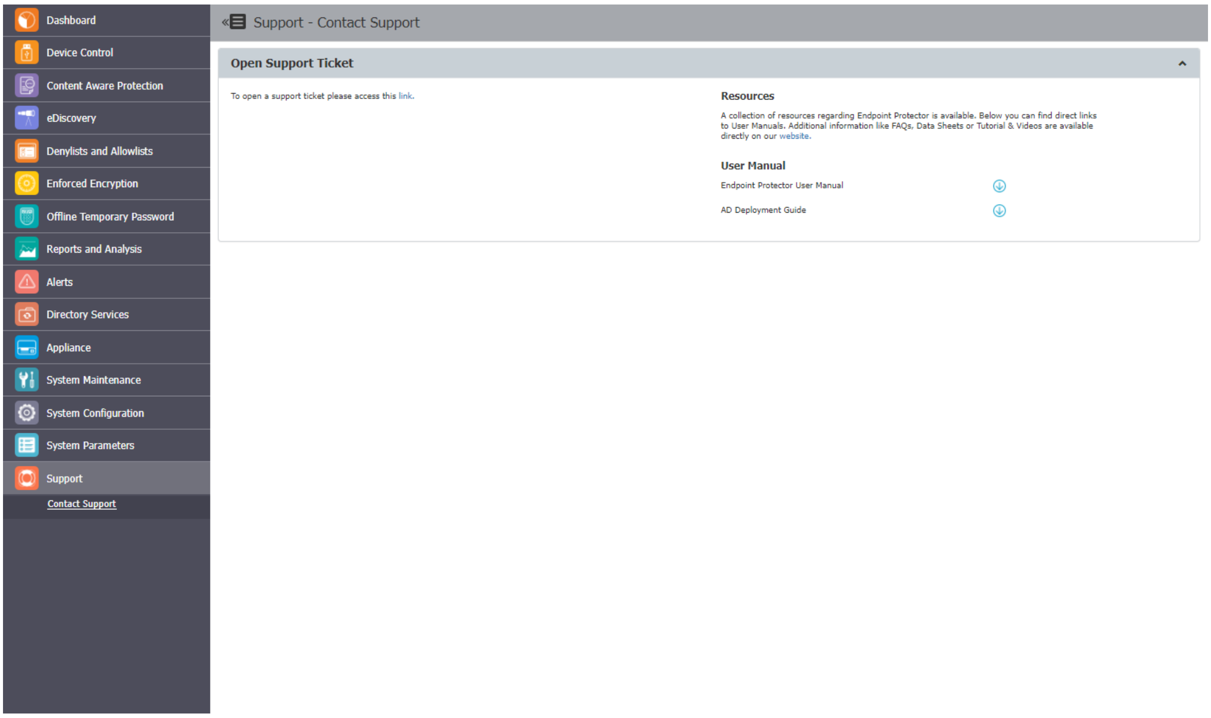
The Hardware Appliance Setup Wizard will guide you through the Endpoint Protector Hardware appliance setup.

The easiest way to configure the Endpoint Protector Hardware Appliance is to connect a mouse, keyboard, and monitor directly to it. This will prompt the same Setup Wizard as described in the chapter above Virtual Appliance Setup Wizard.

9. Support

For additional support resources, please visit our website where you can read manuals, FAQs, watch videos and tutorials, direct E-mail support, and much more.

Our Technical Support Department can also be contacted from Endpoint Protector, the Support section by using the **Open Support Ticket** option. One of our team members will contact you in the shortest time possible.



Open Support Ticket

To open a support ticket please access this link.

Resources

A collection of resources regarding Endpoint Protector is available. Below you can find direct links to User Manuals. Additional information like FAQs, Data Sheets or Tutorial & Videos are available directly on our website.

User Manual

Endpoint Protector User Manual

AD Deployment Guide

10. Disclaimer

The information in this document is provided on an "AS IS" basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, including but not limited to fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the customer's use of Endpoint Protector.

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions, and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers' request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

.

EndpointProtector.com