ENDPOINT PROTECTOR

User Manual for Version 4.4.0.8

COSOSYS

Table of Contents

1. Endpoint Protector Virtual Appliance Formats

1.1. Available Formats of the Virtual Appliance

The Endpoint Protector Virtual Appliance is distributed in different formats and for different platforms. This table summarizes them:

Supported Virtual Environments	Version	.OVF	.OVA	.VMX	.VHD	.PVM	.XVA
VMware Player	5.0.0	✓		✓			
	6.0.5	✓	✓	✓			
	7.1.0	✓	✓	✓			
VMware Workstation	9.0.0			✓			
	11.1.0	✓	✓	✓			
Oracle VM VirtualBox	4.3.26	✓	✓				
vSphere Client VMware ESXi	5.1.0	✓	✓				
	5.5.0	✓	✓				
	6.0.0	✓	✓				
VMware Fusion Professional	7.1.2	✓	✓				
Hyper-V Manager 2008 R2	6.1.7601.17514				✓		
Hyper-V Manager 2012 R2	6.3.9600.16384				✓		
Parallels Desktop	10.2.1					✓	
Citrix XenCenter	6.2						✓

Endpoint Protector makes available these formats in order to help customers test and implement Endpoint Protector in different virtualized environments.

Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual appliances.

1.1.1. The Virtualization software that supports OVF and OVA Format is:

- VMWare Workstation 11.1, VMware Player 5.0 or higher, VMware Fusion 7.1.2 and VMware ESXi 5.1 or higher
- Oracle VM VirtualBox
- Citrix XenCenter 6.2

1.1.2. The Virtualization software that supports VMX Format is:

- 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 on the latest VMware Player version (v7.x.x). In order to run these virtual appliances on older VMware Workstation / VMware Player versions, the following actions need to be done:

1. Extract the .zip archive
2. Go to the extract location
3. Click to edit the .VMX file using a text editor; 4. Search for the "virtualHW.version" field; 5. Replace the default version (default = 11) to the desired version

Examples:
- if you want to run the .VMX virtual appliance on VMware Workstation v9.x.x or VMware Player v5.x.x, than virtualHW.version = "9"
- if you want to run the .VMX virtual appliance on VMware Workstation v10.x.x or VMware Player v6.x.x, than virtualHW.version = "10"

6. Save the changes and close the text editor
7. Import the virtual image
8. Play the virtual machine

1.1.3. The Virtualization software that supports VHD Format is:

- Microsoft Hyper-V

1.1.4. The Virtualization software that supports PVM Format is:

- Parallels Desktop

1.1.5. The Virtualization software that supports XVA Format is:

- Citrix XenServer 5.5
- Citrix XenServer 6.0

Note!

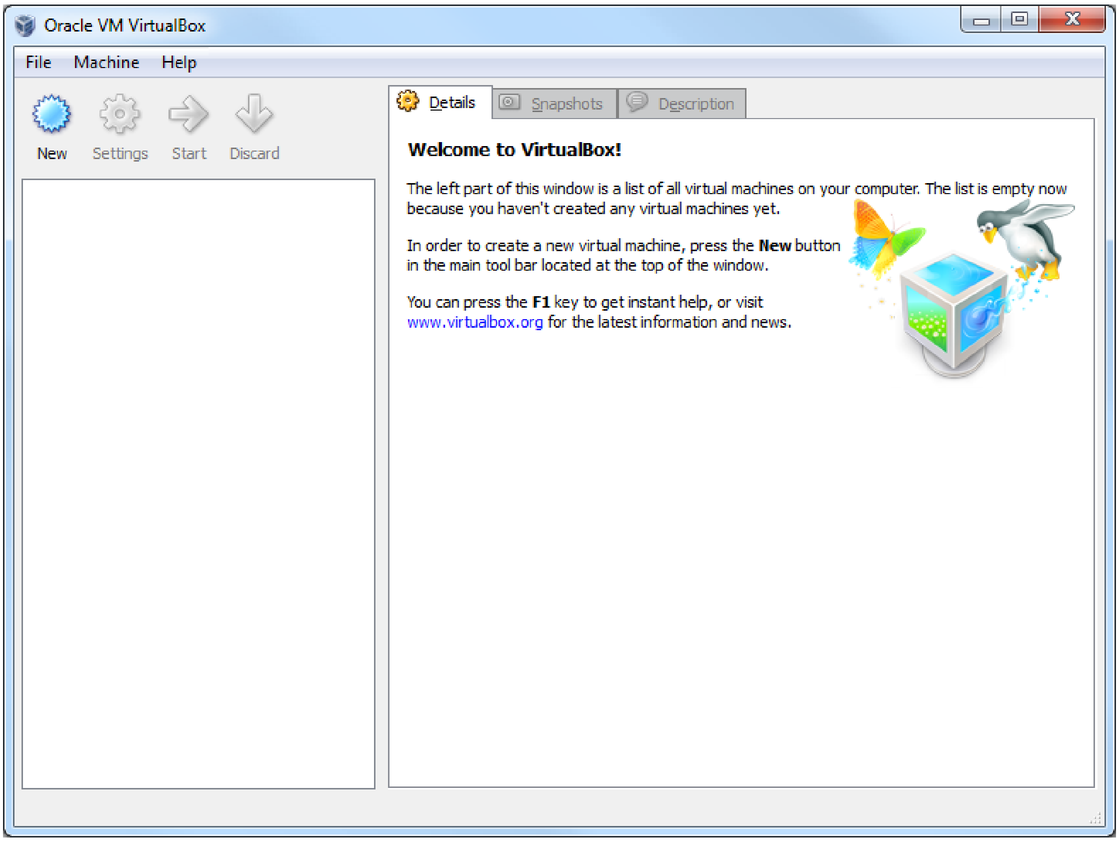
In case of a power failure or any other event that causes the host computer to shut down unexpectedly, the Endpoint Protector Virtual Appliance can be corrupted. In such a situation, we recommend starting it by booting the Ubuntu operating system in Safe Mode.

2. Implementing using OVF Format

2.1. Implementing in Oracle VM VirtualBox using OVF Format

1. Unzip the downloaded package

2. Start VirtualBox



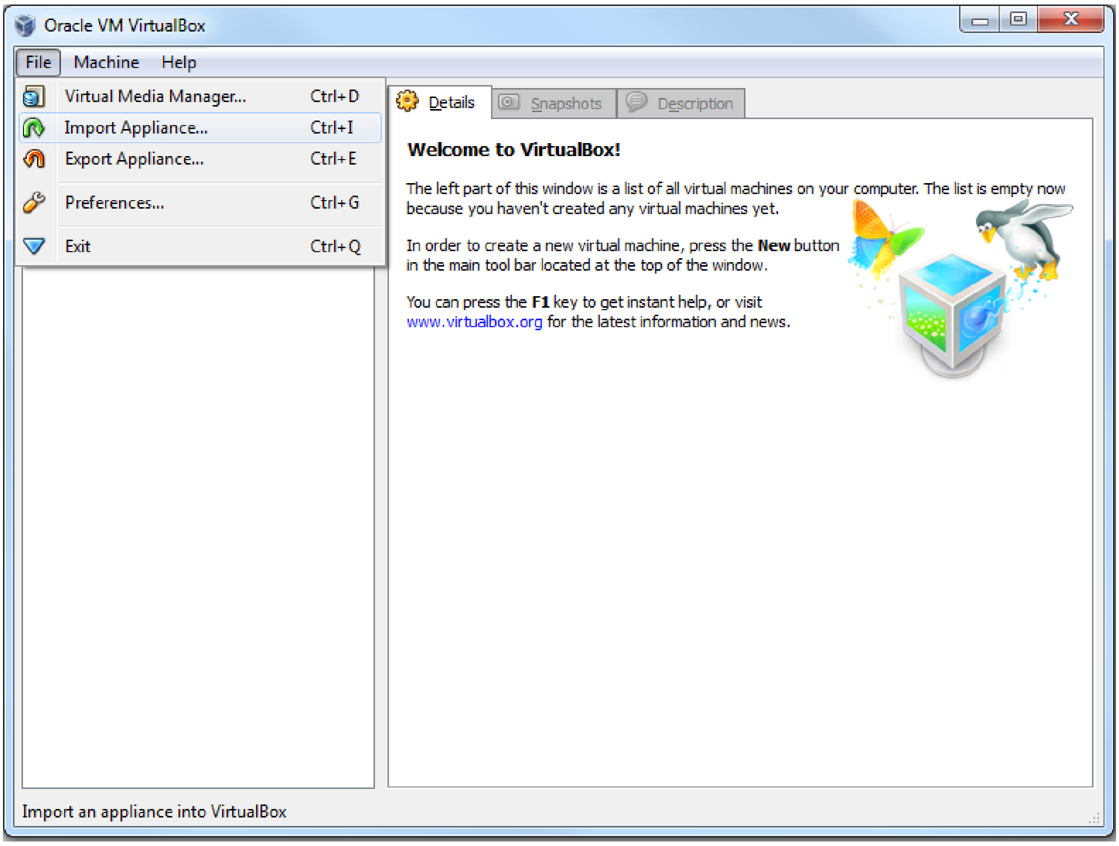
Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

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

3. Go To File > Import Appliance



Oracle VM VirtualBox

File
Machine
Help
Virtual Media Manager... Ctrl+D
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Preferences... Ctrl+G
Exit Ctrl+Q
Details
Snapshots
Description

Welcome to VirtualBox!

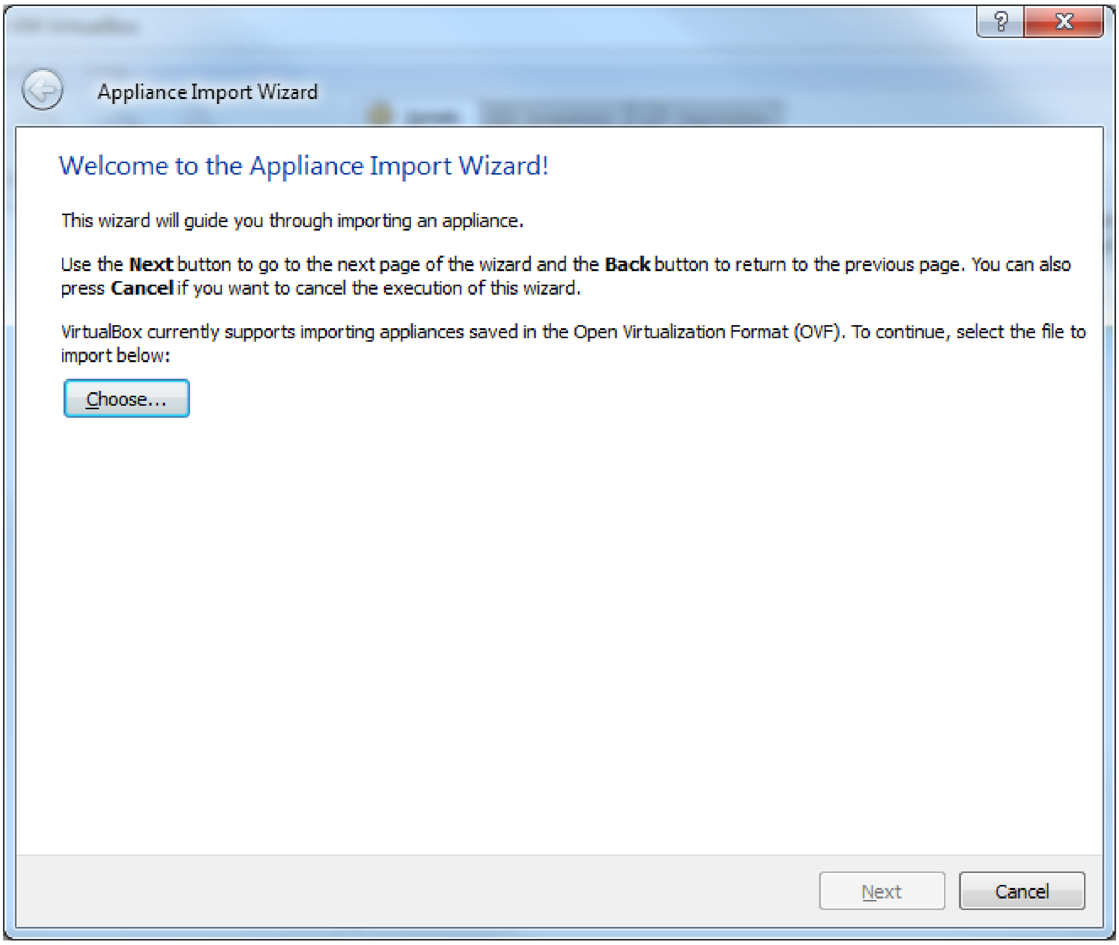
The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

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

Import an appliance into VirtualBox

4. Press Choose button



Appliance Import Wizard

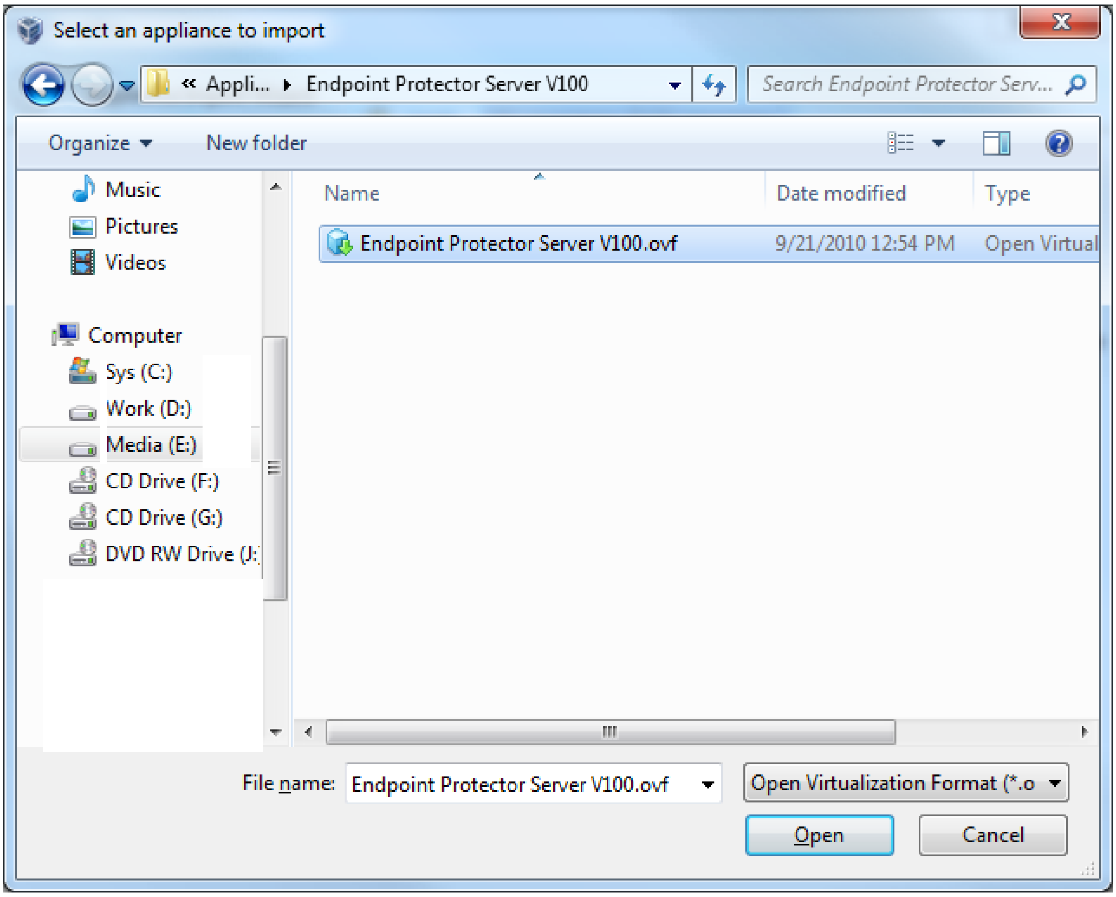
Welcome to the Appliance Import Wizard!

This wizard will guide you through importing an appliance.

Use the **Next** button to go to the next page of the wizard and the **Back** button to return to the previous page. You can also press **Cancel** if you want to cancel the execution of this wizard.

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below:

5. Browse and select the OVF file from the extracted zip file

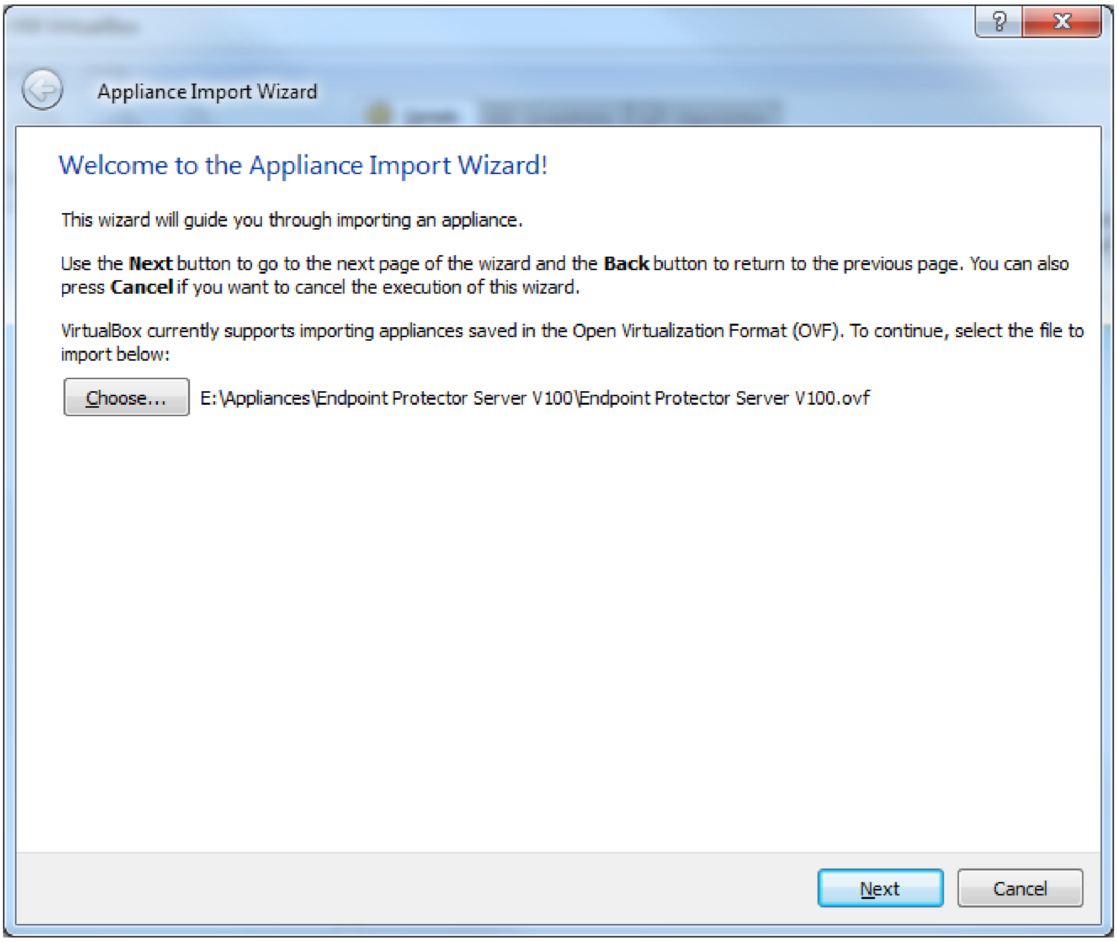


Select an appliance to import

File name: Endpoint Protector Server V100.ovf

Open Virtualization Format (*.o

6. Press Next Button



Welcome to the Appliance Import Wizard!

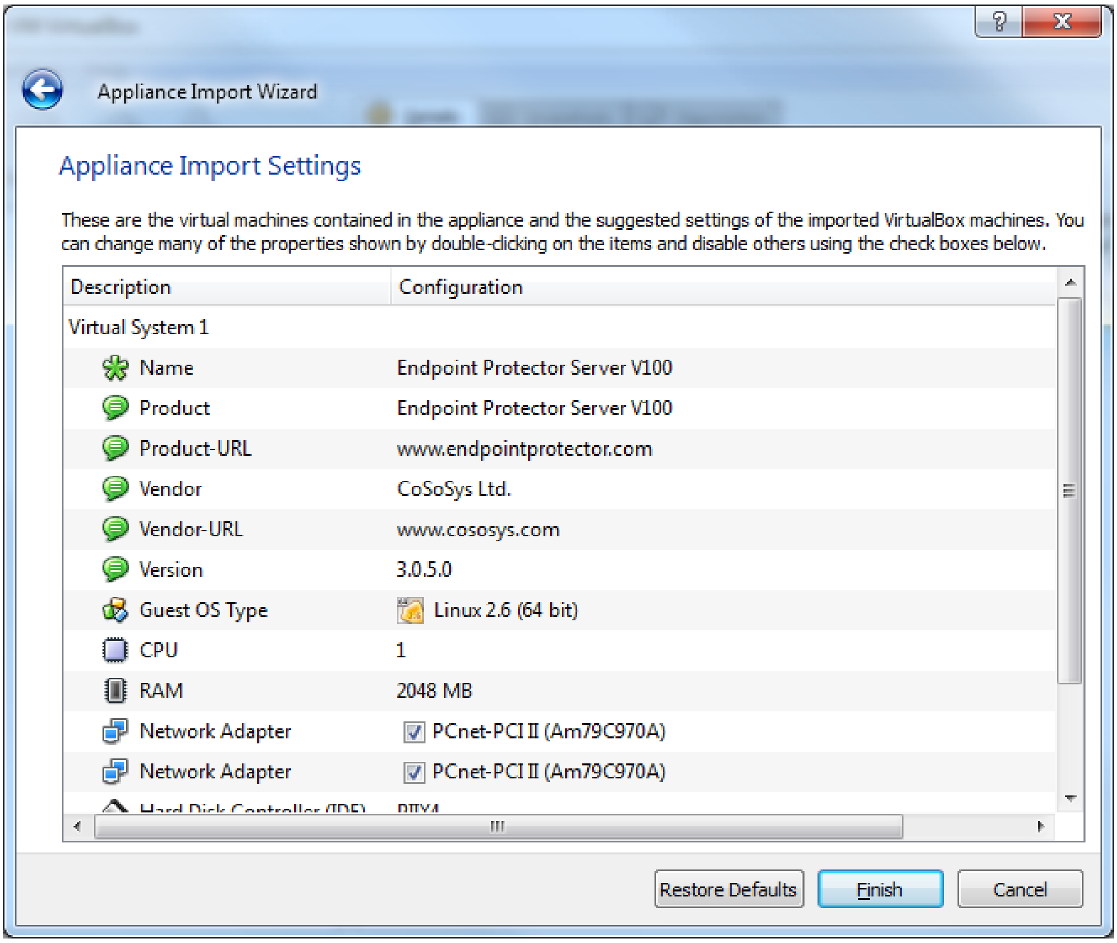
This wizard will guide you through importing an appliance.

Use the **Next** button to go to the next page of the wizard and the **Back** button to return to the previous page. You can also press **Cancel** if you want to cancel the execution of this wizard.

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below:

Choose... E:\Appliances\Endpoint Protector Server V100\Endpoint Protector Server V100.ovf

7. Press Finish Button

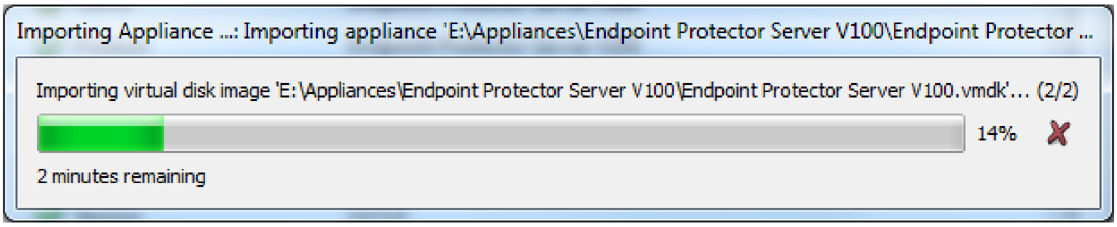


Appliance Import Settings

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.

Description	Configuration
Virtual System 1	
Name	Endpoint Protector Server V100
Product	Endpoint Protector Server V100
Product-URL	www.endpointprotector.com
Vendor	CoSoSys Ltd.
Vendor-URL	www.cososys.com
Version	3.0.5.0
Guest OS Type	Linux 2.6 (64 bit)
CPU	1
RAM	2048 MB
Network Adapter	☑ PCnet-PCI II (Am79C970A)
Network Adapter	☑ PCnet-PCI II (Am79C970A)
Hard Disk Controller (IDE)	PIIX4

8. Wait for the import displayed by the progress bar



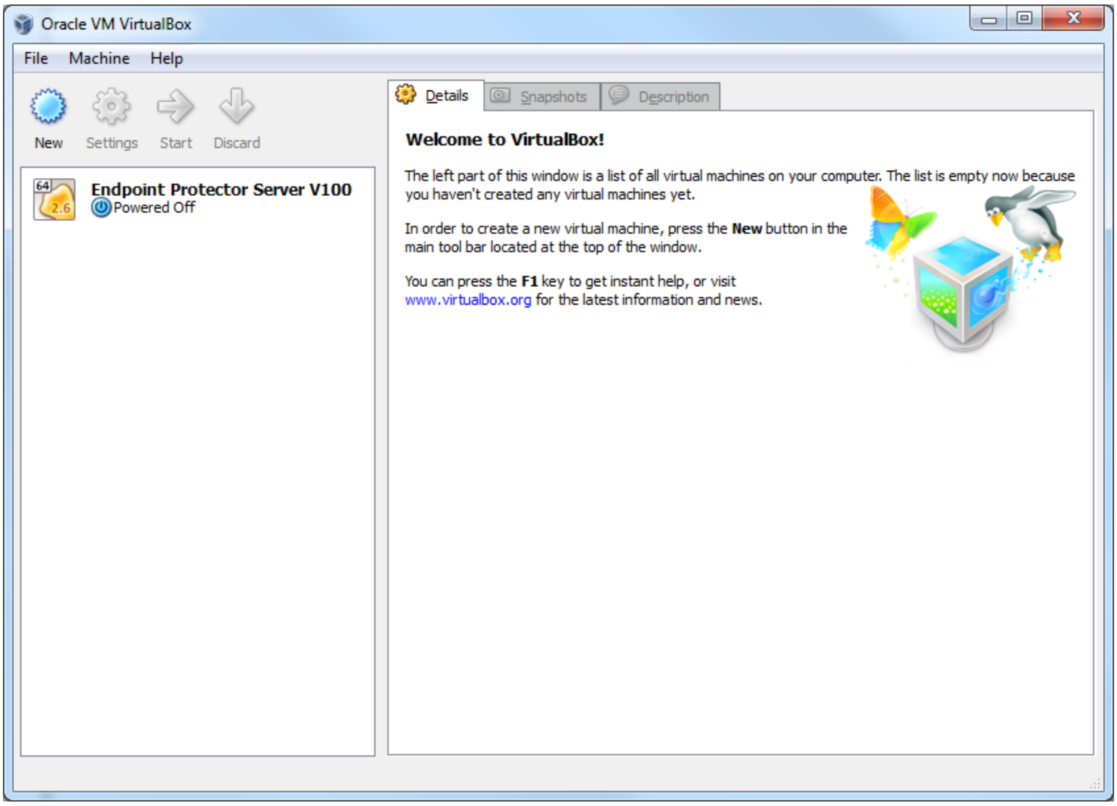
Importing Appliance ...: Importing appliance 'E:\Appliances\Endpoint Protector Server V100\Endpoint Protector ...

Importing virtual disk image 'E:\Appliances\Endpoint Protector Server V100\Endpoint Protector Server V100.vmdk'... (2/2)

14%

2 minutes remaining

9. At the end the new virtual machine will appear on the left container as displayed bellow



Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

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

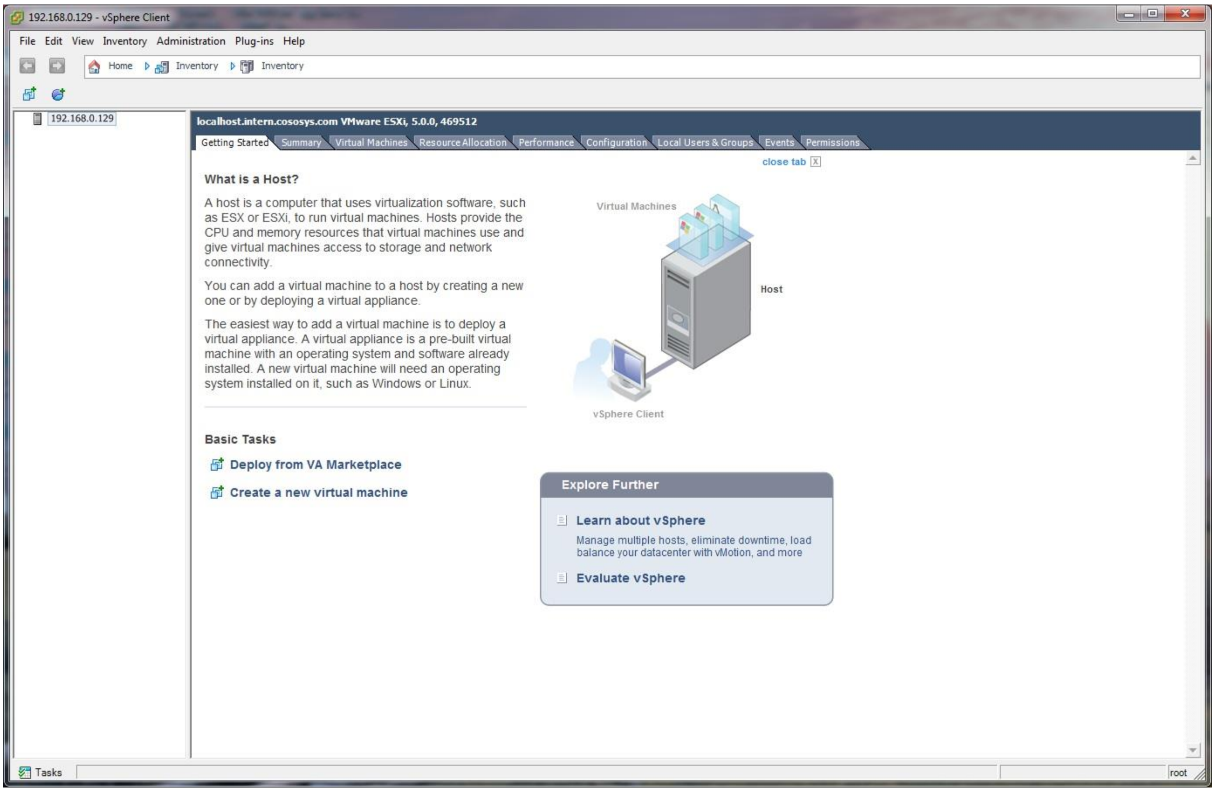
At this point the virtual machine is ready to be started.

Please follow the Endpoint Protector Appliance User Manual from this point on.

2.2. Implementing in VMware vSphere using OVF Format

1. Unzip the downloaded package.

2. Start vSphere.



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

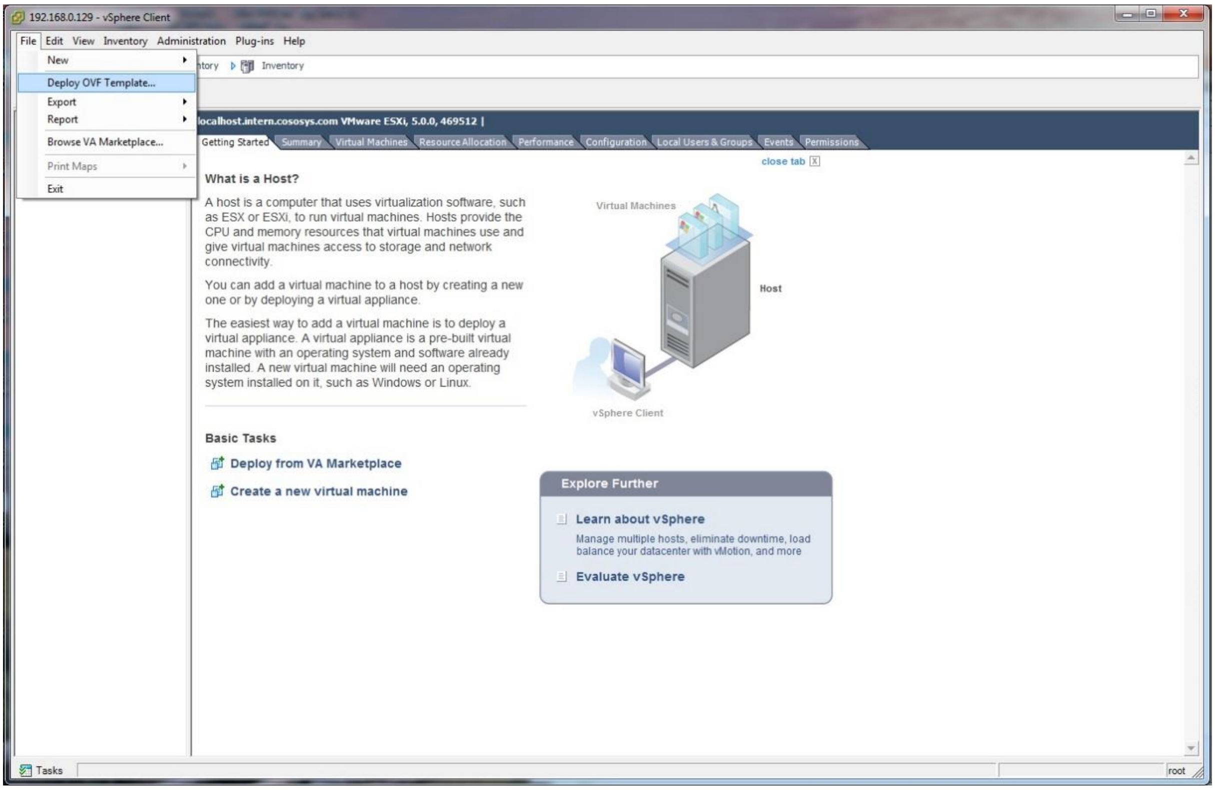
Explore Further

Learn about vSphere

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

Evaluate vSphere

3. Go To File > Deploy OVF Template.



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

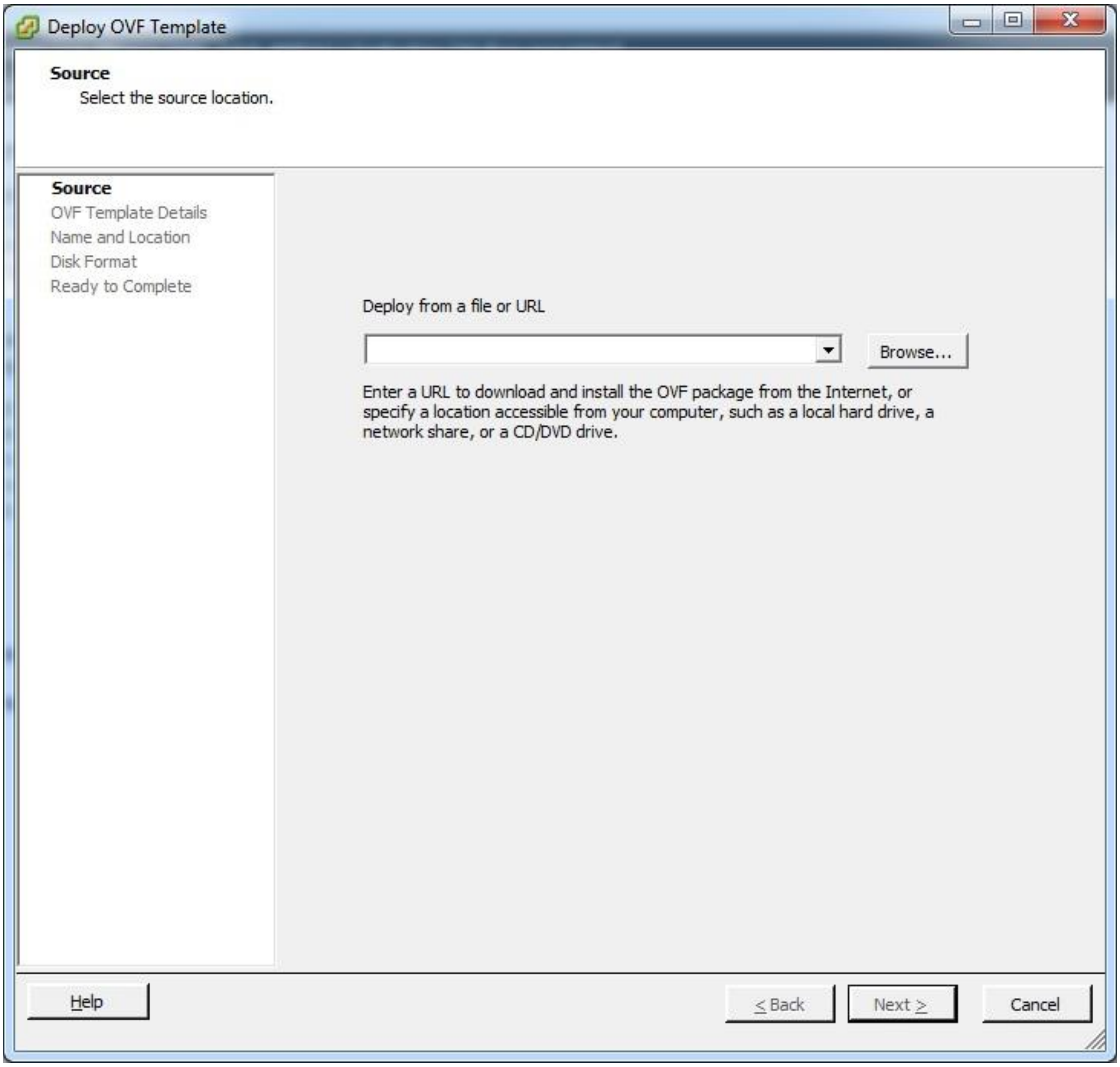
Explore Further

Learn about vSphere

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

Evaluate vSphere

4. Press the Browse button.



Deploy OVF Template

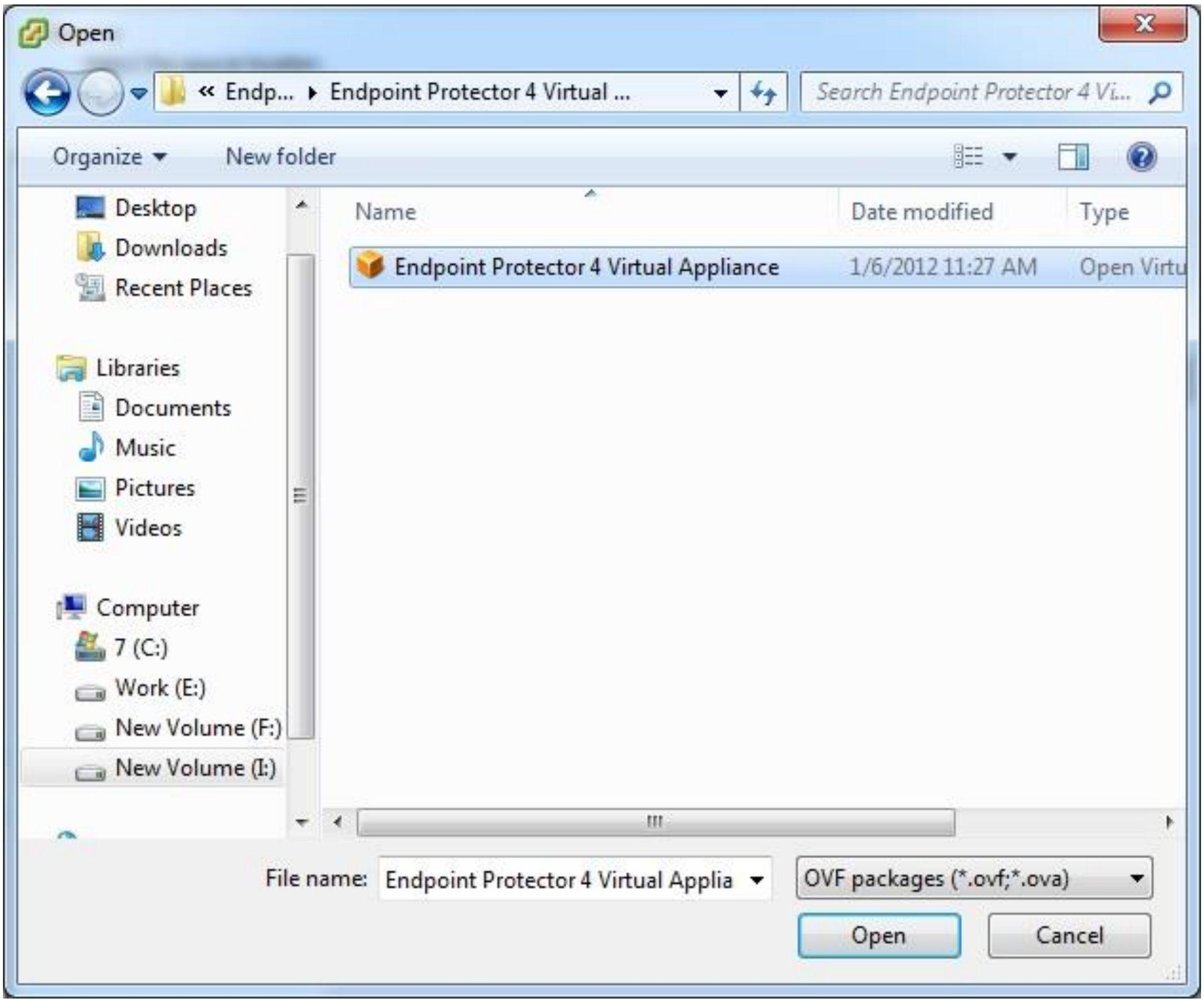
Source

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. Browse and select the OVF file from the extracted zip file.

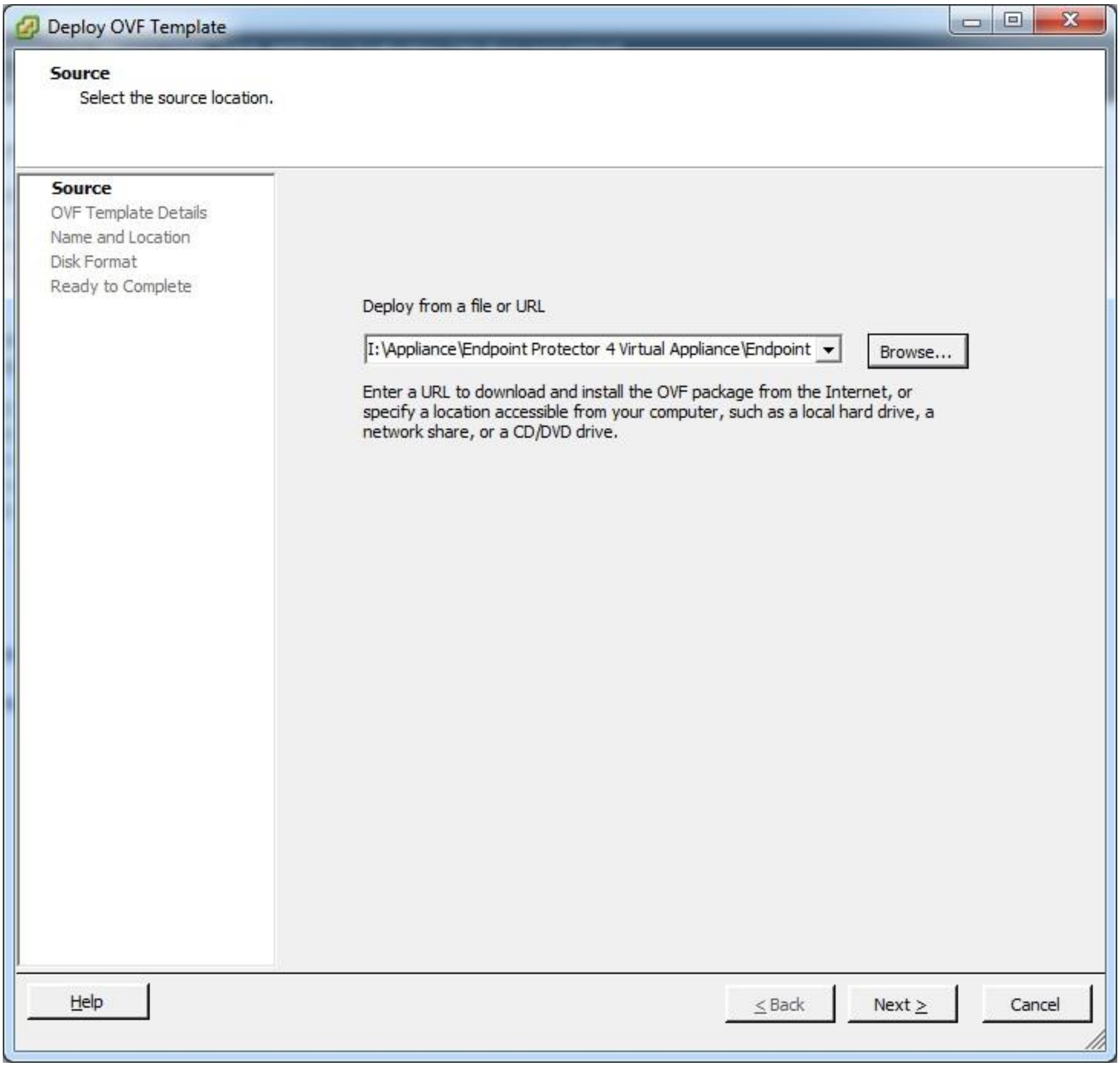


Name	Date modified	Type
Endpoint Protector 4 Virtual Appliance	1/6/2012 11:27 AM	Open Virtu

File name: Endpoint Protector 4 Virtual Applia

OVF packages (*.ovf;*.ova)

6. Press the Next button.

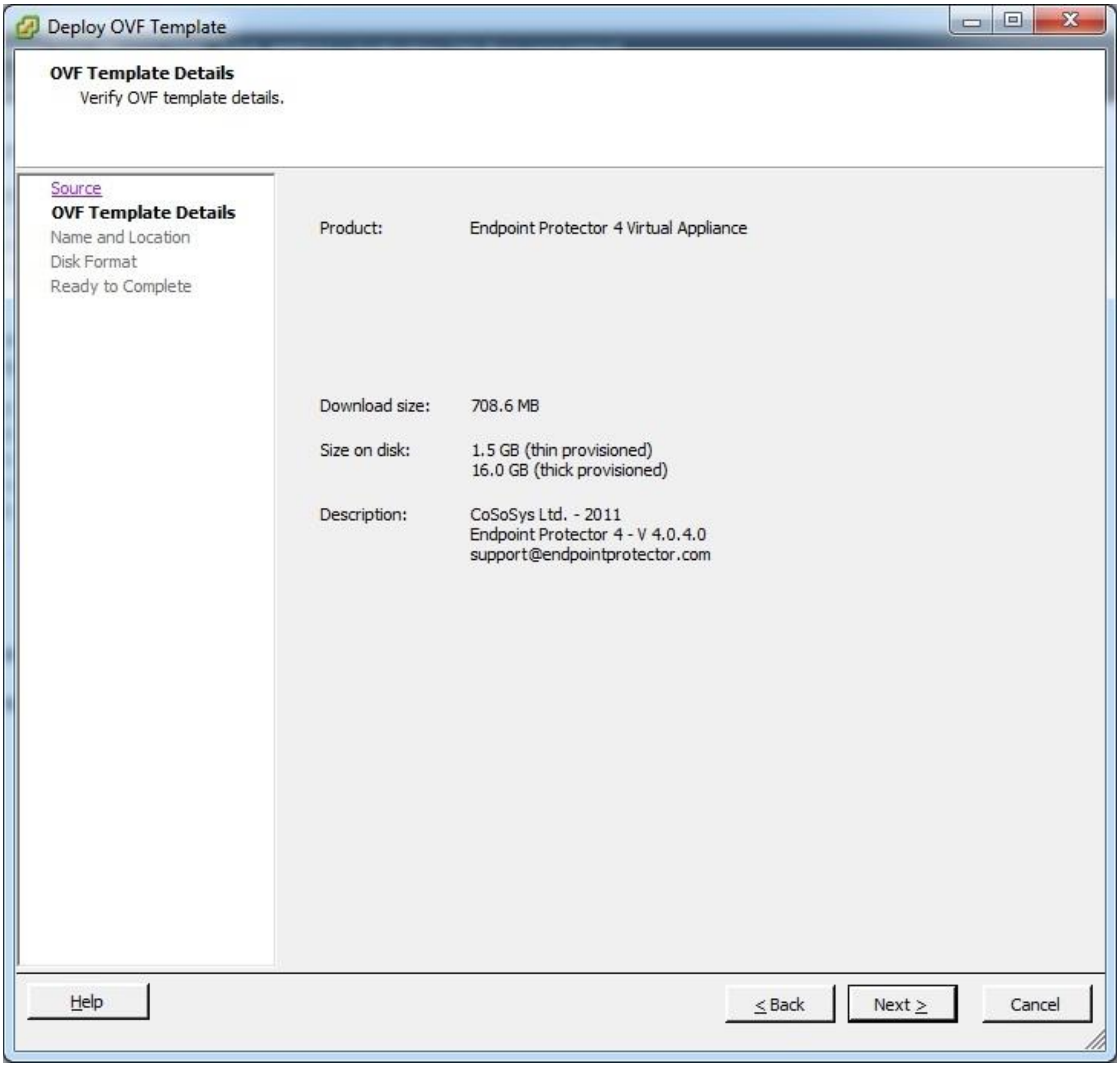


Deploy from a file or URL

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. Verify the OVF Template Details and press Next.



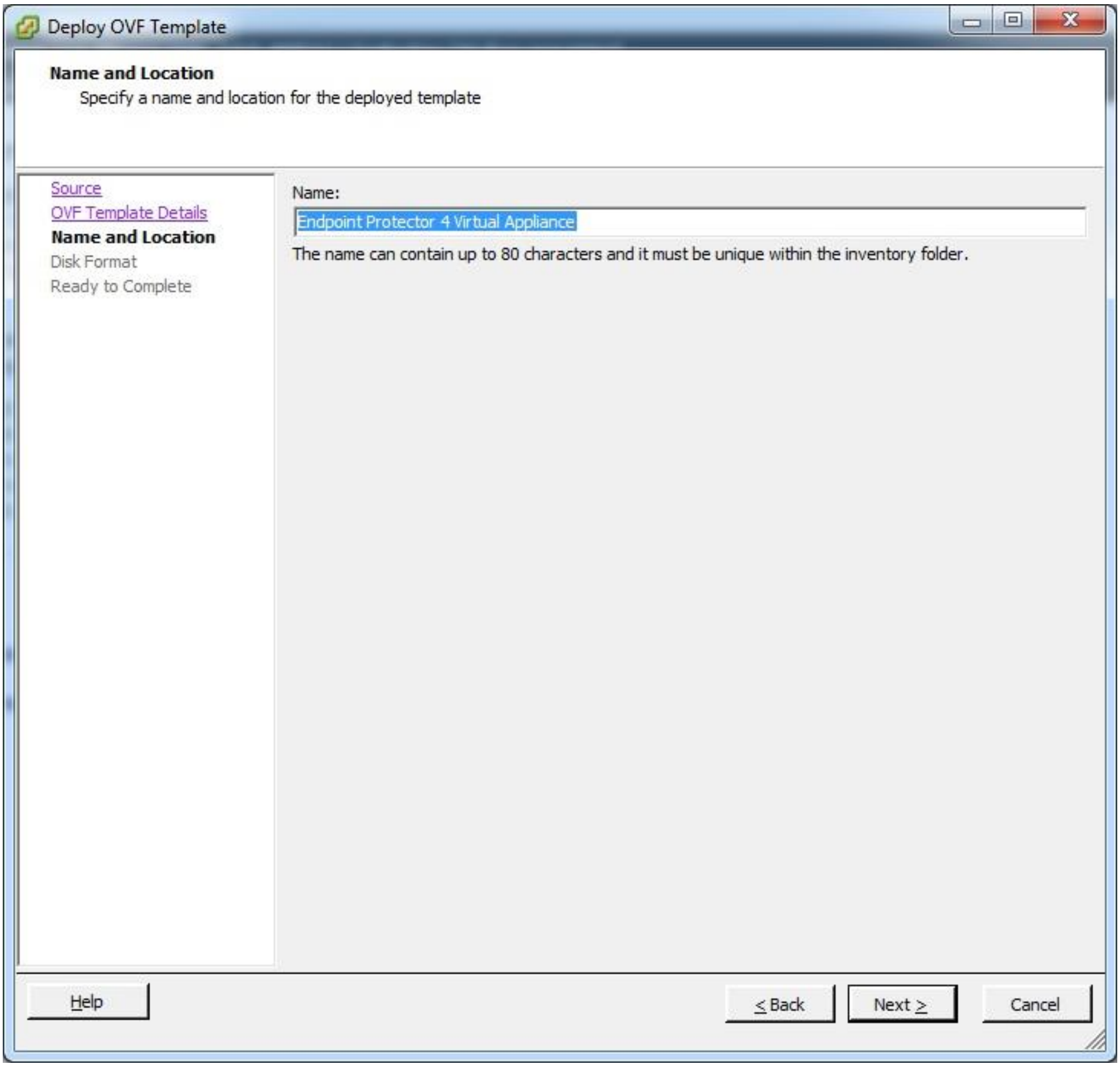
Product: Endpoint Protector 4 Virtual Appliance

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 press Next.



Deploy OVF Template

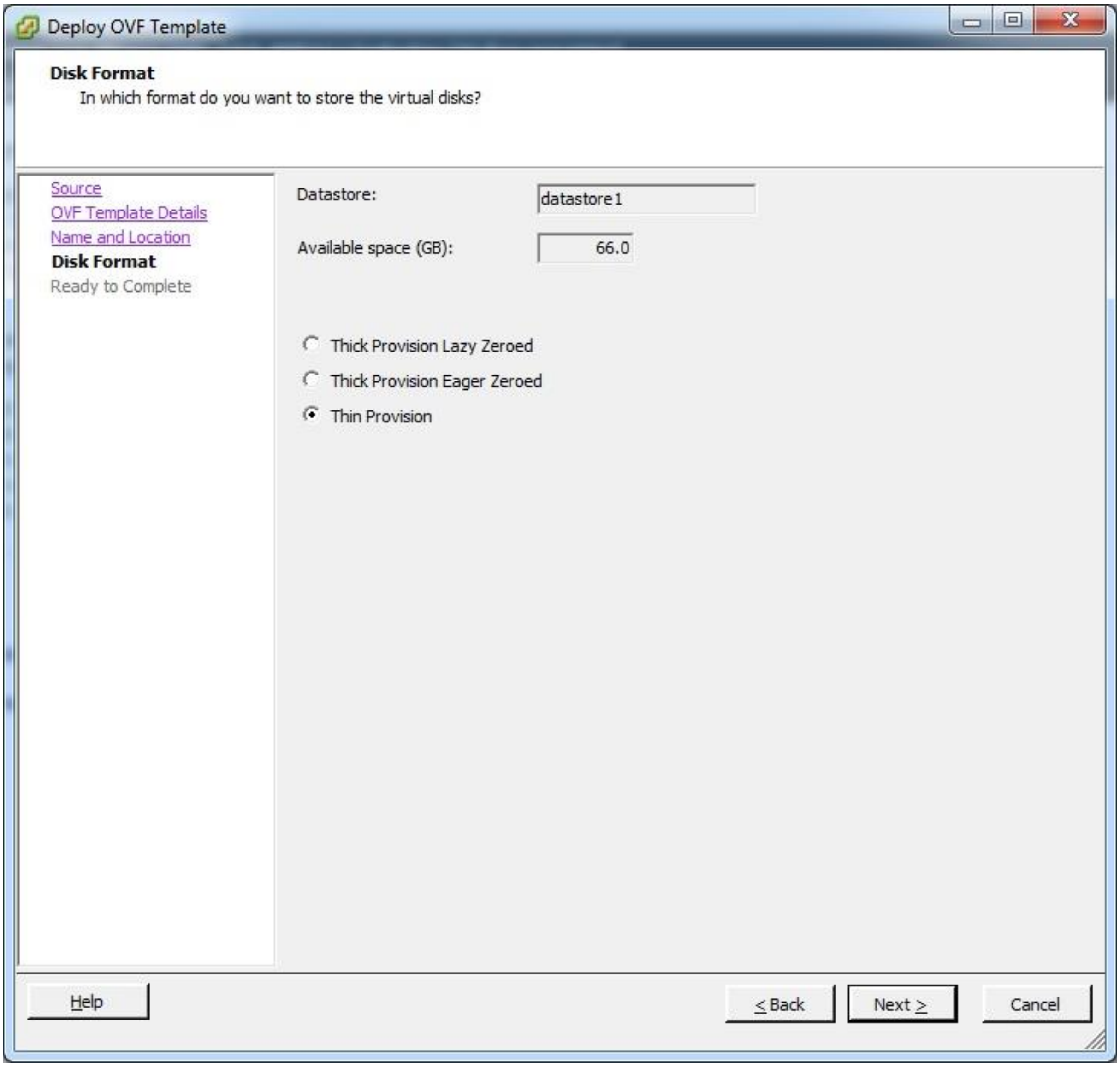
Name and Location

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 “Thin provision” as Disk Format option and press Next.



Deploy OVF Template

Disk Format

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

Datastore: datastore1

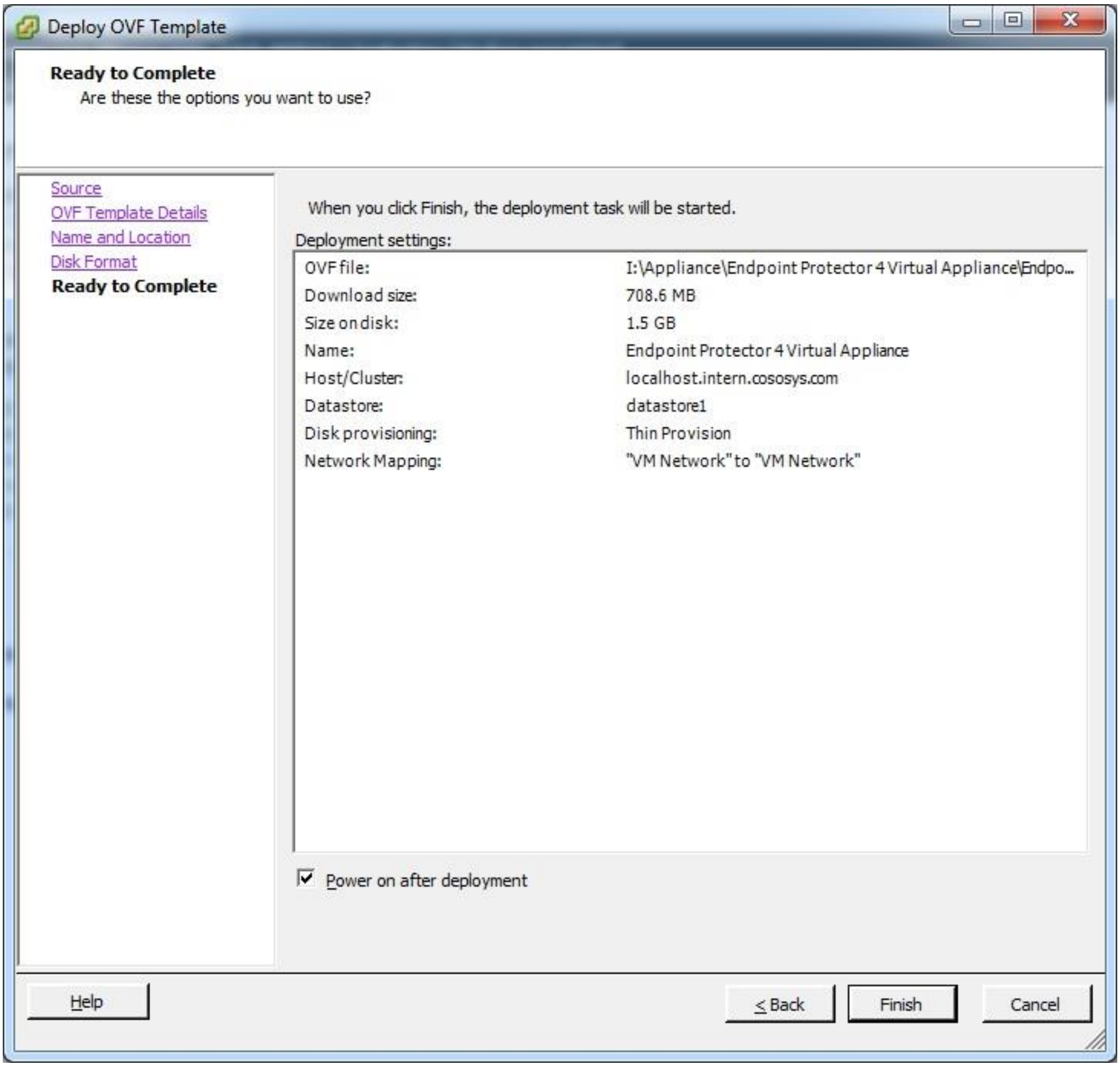
Available space (GB): 66.0

○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

10. Press the Finish button 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:

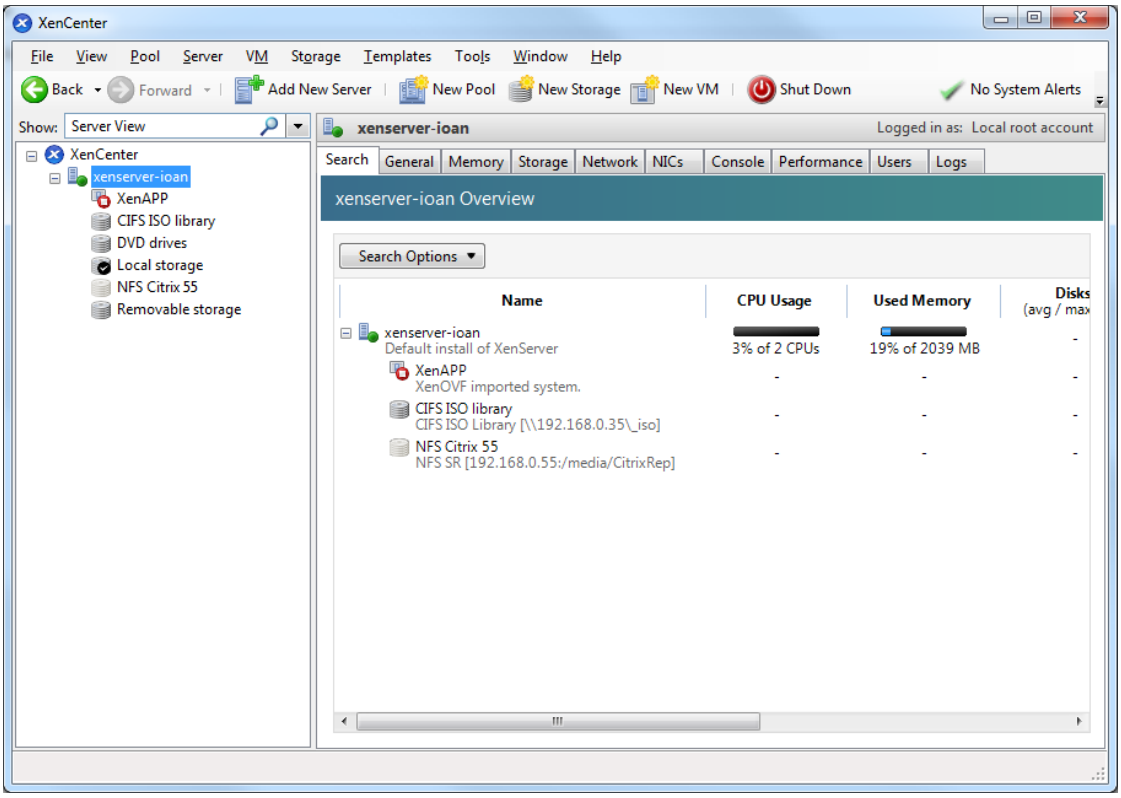
OVF file:	I:\Appliance\Endpoint Protector 4 Virtual Appliance\Endpo...
Download size:	708.6 MB
Size on disk:	1.5 GB
Name:	Endpoint Protector 4 Virtual Appliance
Host/Cluster:	localhost.intern.cososys.com
Datastore:	datastore1
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

☑ Power on after deployment

2.3. Implementing in Citrix XenServer 5.6 using OVF Format

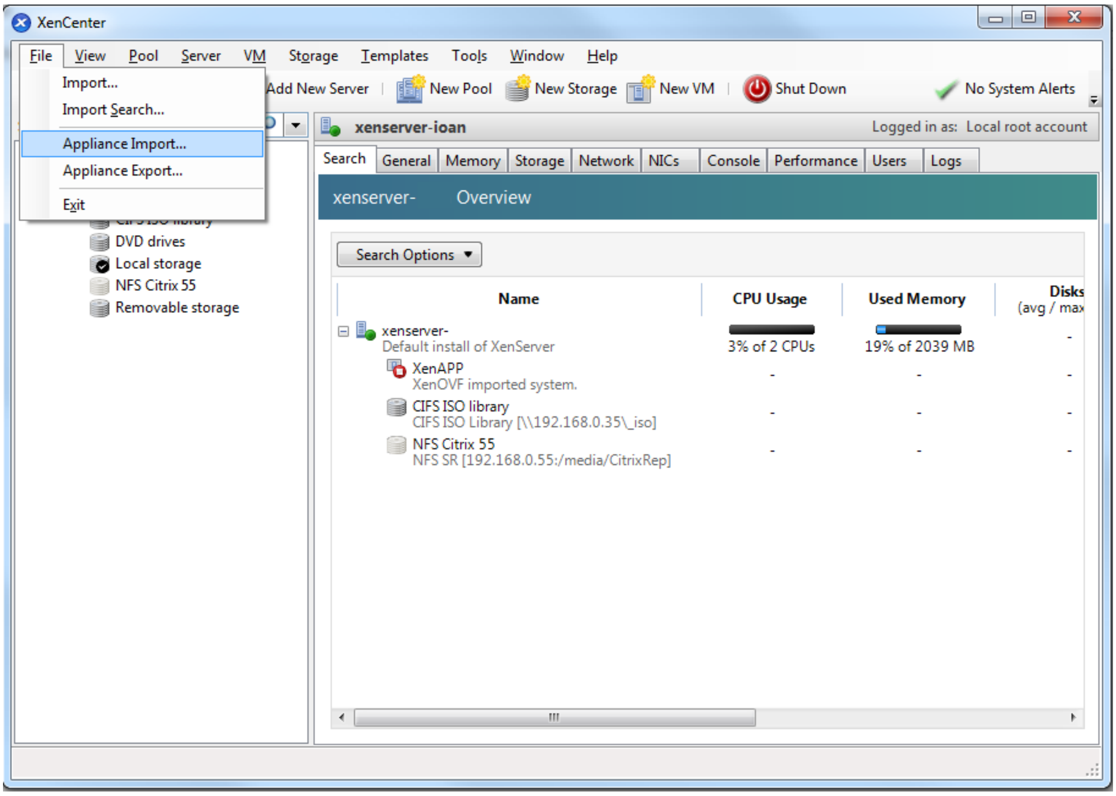
1. Unzip the downloaded package

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

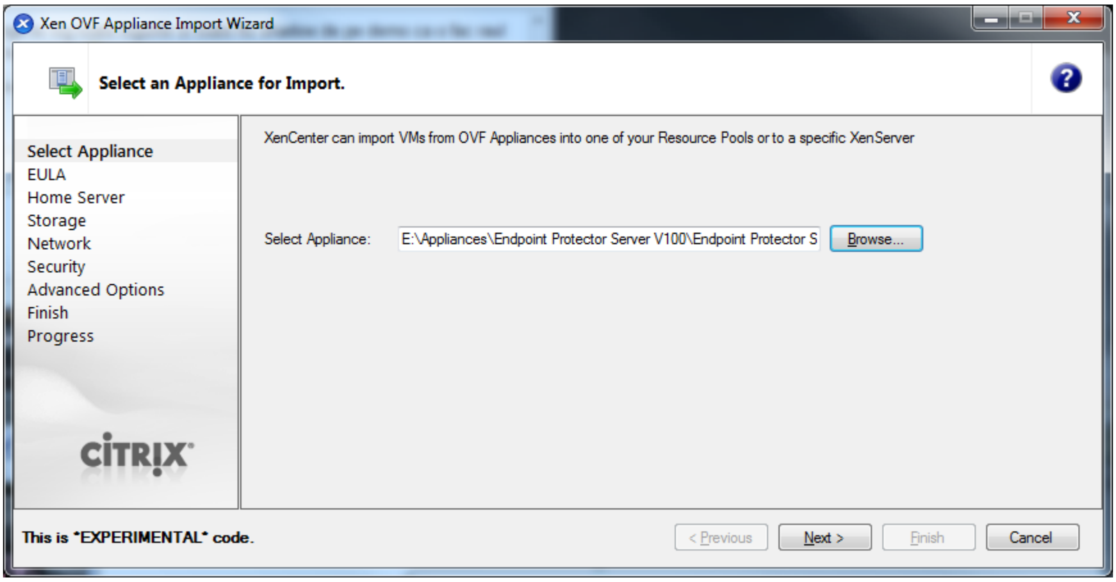
Name	CPU Usage	Used Memory	Disks (avg / max
xenserver-ioan Default install of XenServer	3% of 2 CPUs	19% of 2039 MB	-
XenAPP XenOVF imported system.	-	-	-
CIFS ISO library CIFS ISO Library [\\192.168.0.35_iso]	-	-	-
NFS Citrix 55 NFS SR [192.168.0.55:/media/CitrixRep]	-	-	-

3. Go To File > Appliance Import



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



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

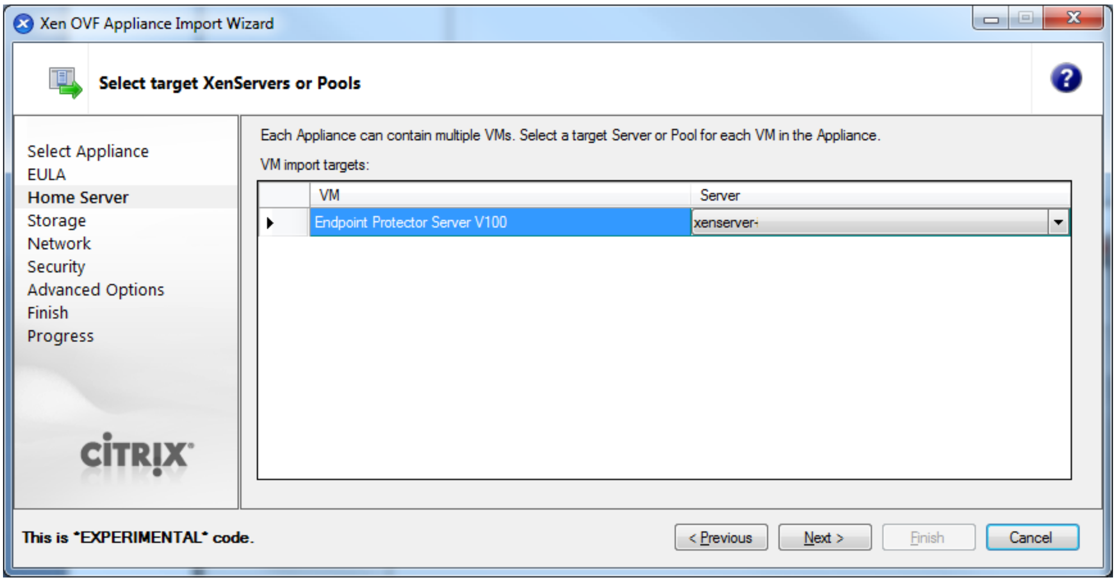
Select Appliance: E:\Appliances\Endpoint Protector Server V100\Endpoint Protector S

This is "EXPERIMENTAL" code.

5. Press the Next button

6. Read and accept the EULA, then press Next

7. Select the target for this Virtual Appliance



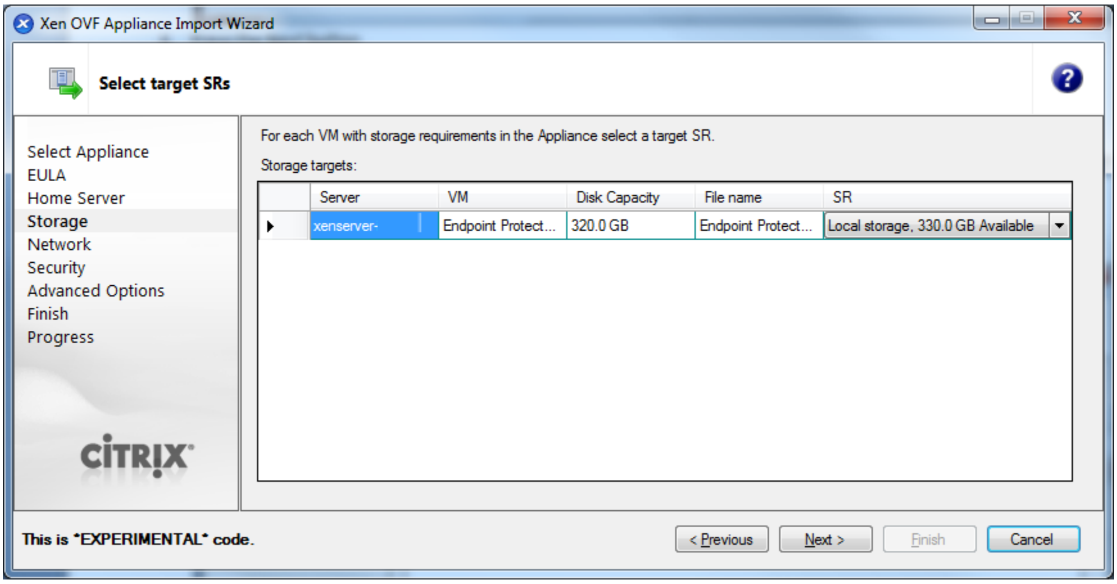
Each Appliance can contain multiple VMs. Select a target Server or Pool for each VM in the Appliance.

VM import targets:

	VM	Server
▶	Endpoint Protector Server V100	xenserver-

This is *EXPERIMENTAL* code.

8. Select the storage location



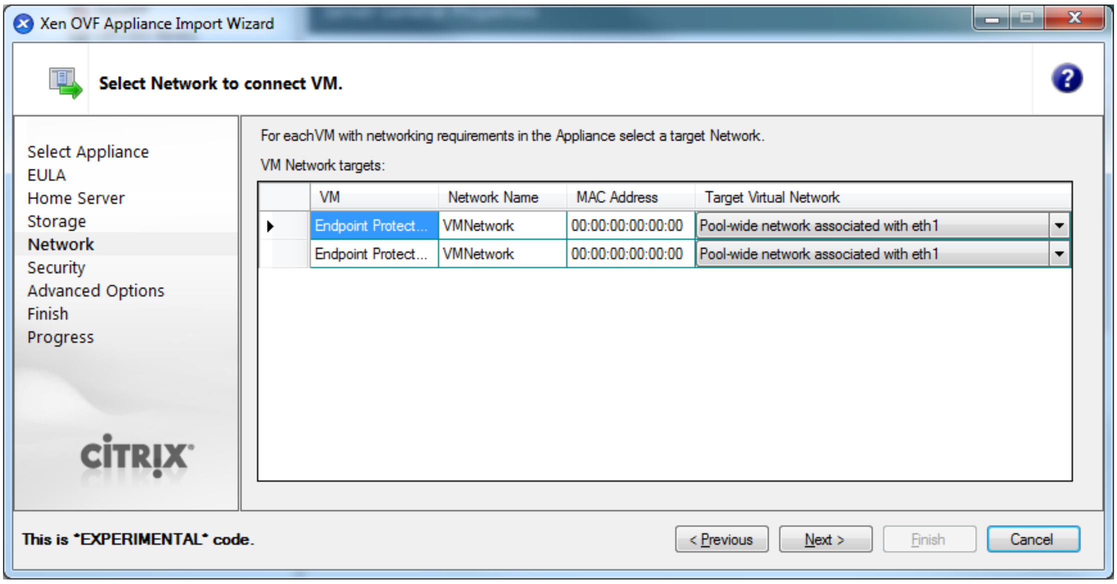
For each VM with storage requirements in the Appliance select a target SR.

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.

9. Select you network (keep default values)



Select Network to connect VM.

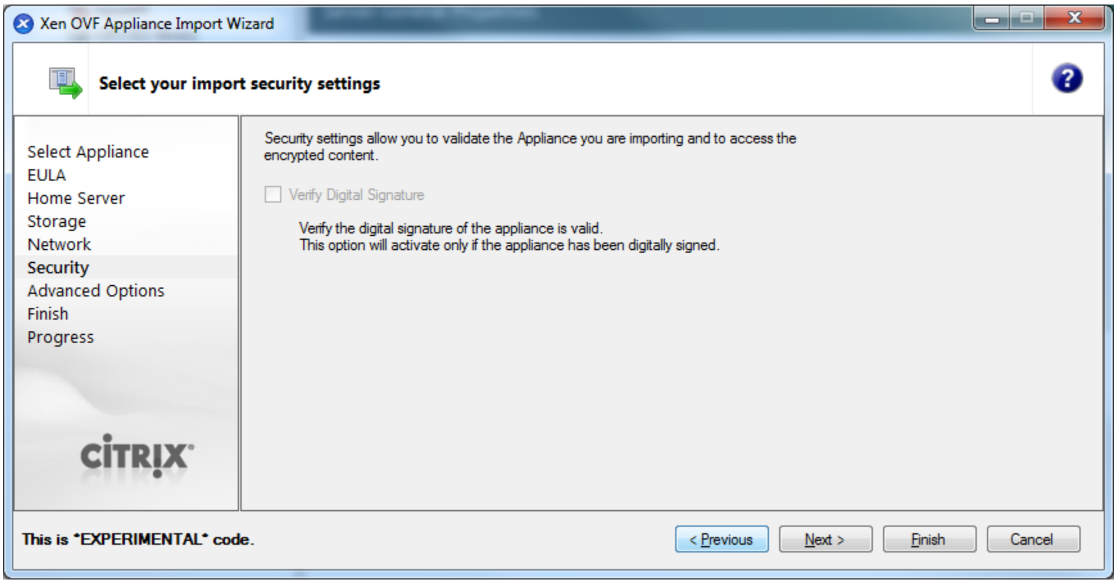
For each VM with networking requirements in the Appliance select a target Network.

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.

10. On Security Screen click on Next button



Select your import security settings

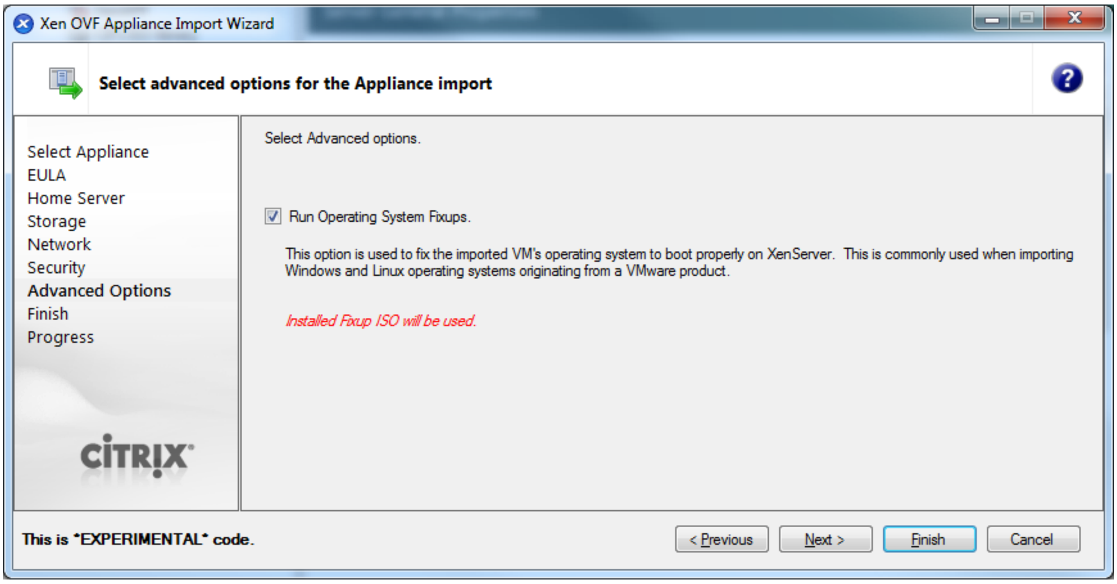
Security settings allow you to validate the Appliance you are importing and to access the encrypted content.

□ 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.

11. On Advanced Options screen click Next



Select advanced options for the Appliance import

Select Advanced options.

☑ Run Operating System Fixups.

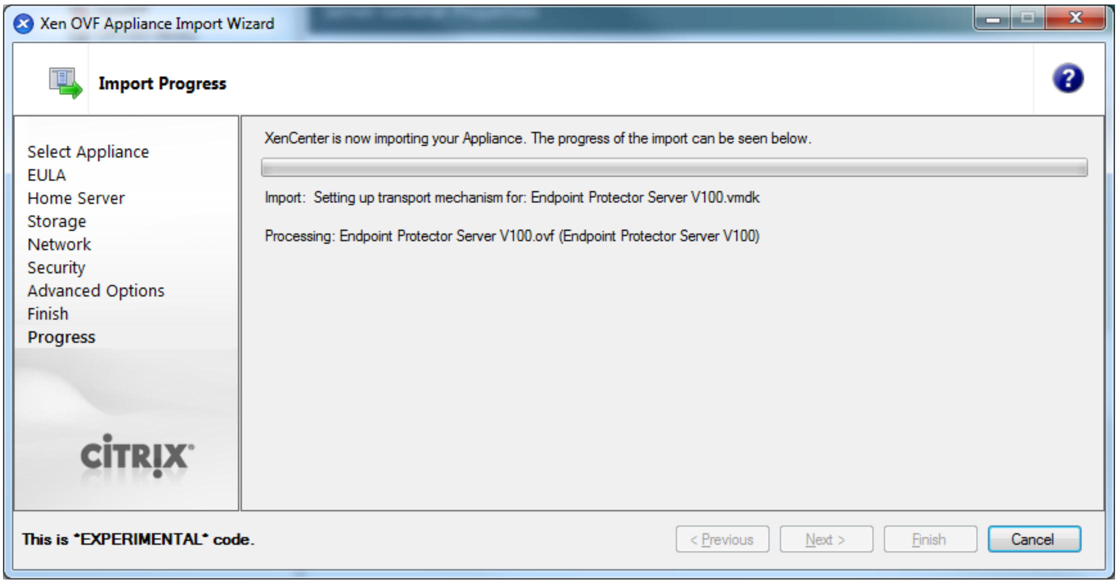
This option is used to fix the imported VM's operating system to boot properly on XenServer. This is commonly used when importing Windows and Linux operating systems originating from a VMware product.

Installed Fixup ISO will be used.

This is *EXPERIMENTAL* code.

12. On the Finish Screen, review this configuration and click Finish

13. Wait for the import to be completed



Import Progress

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.

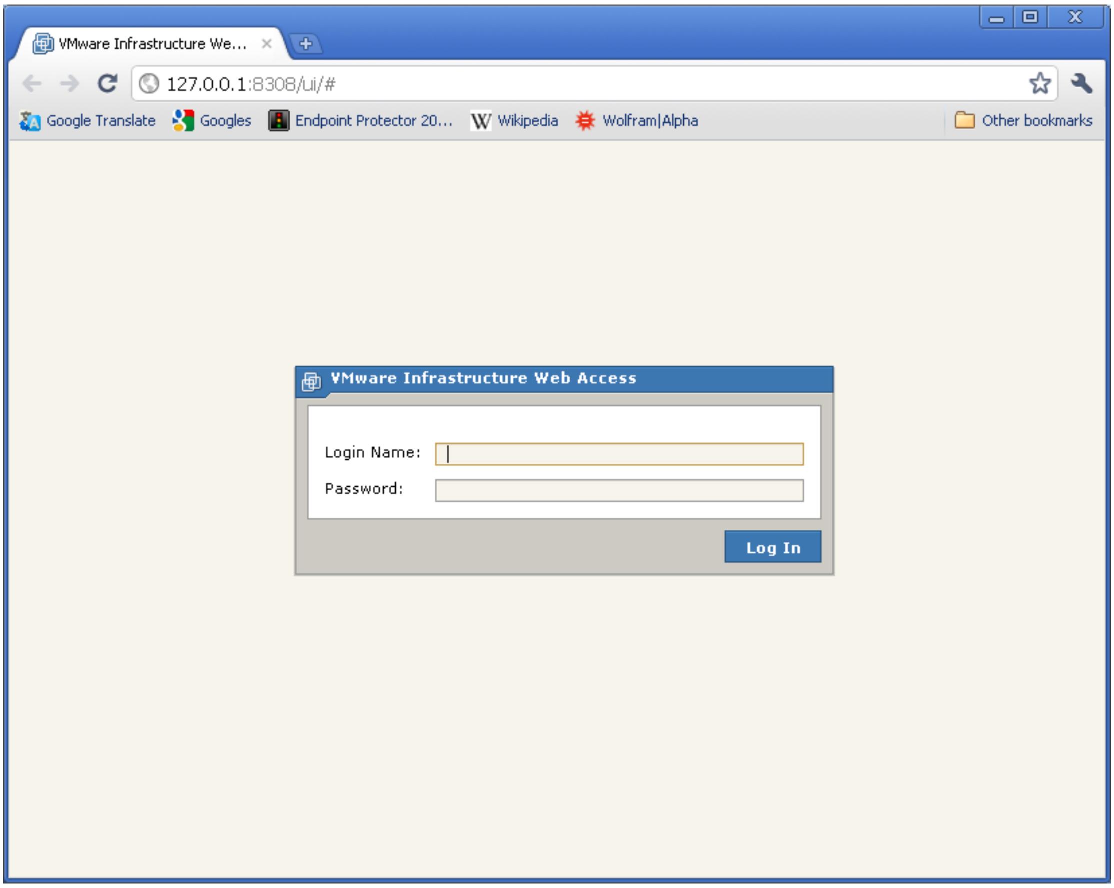
Please follow the Endpoint Protector Appliance User Manual from this point on.

3. Implementing using VMX Format

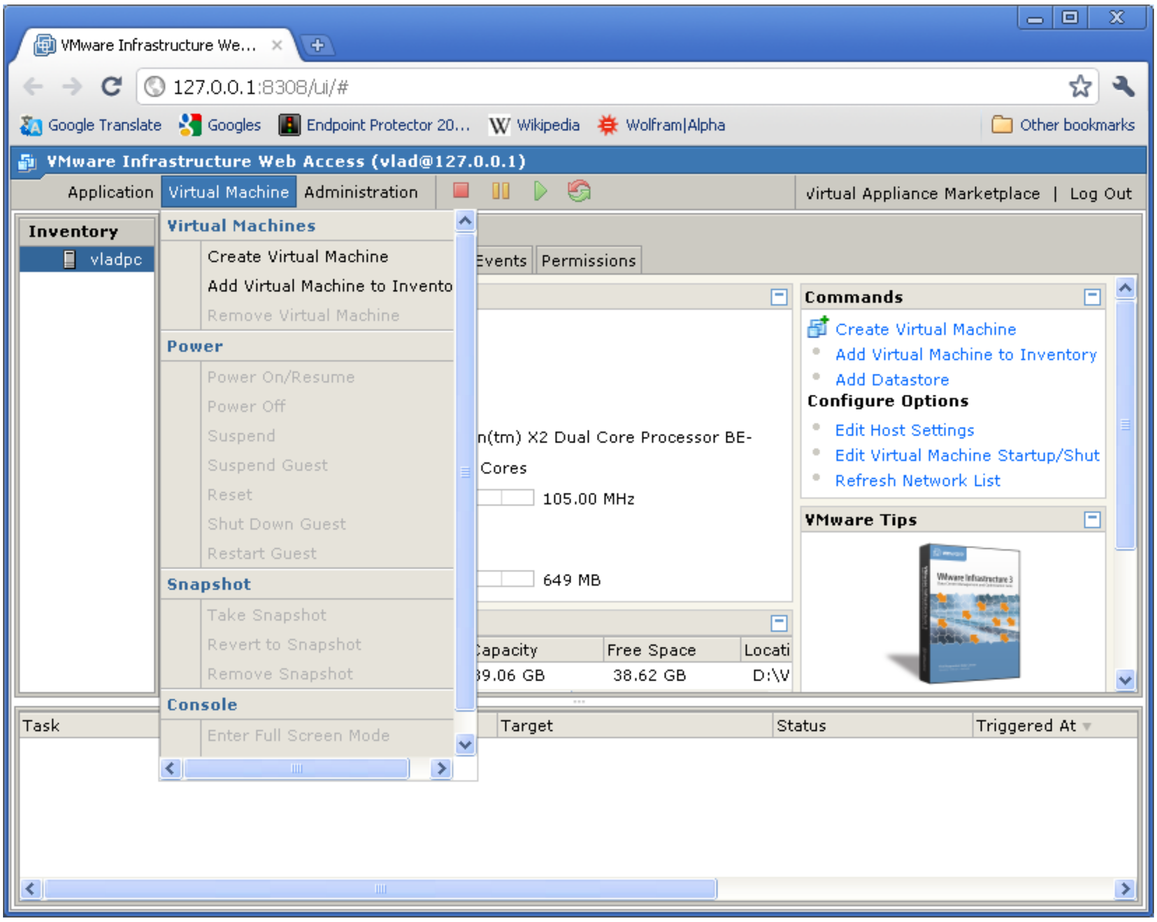
3.1. Implementing in VMware Server 2.0 using VMX Format

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

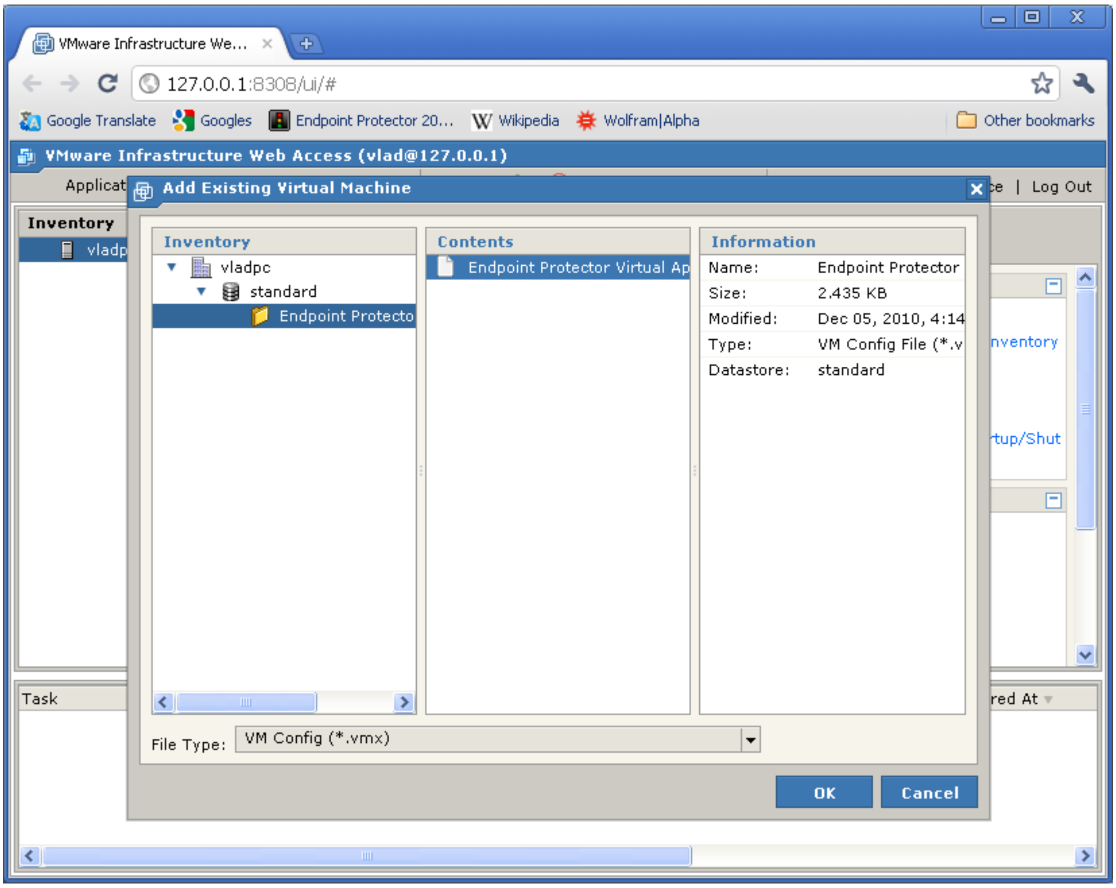
2. Open your WMware Server web interface and login



3. Select Add Virtual Machine to inventory



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



Add Existing Virtual Machine

Information	
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)

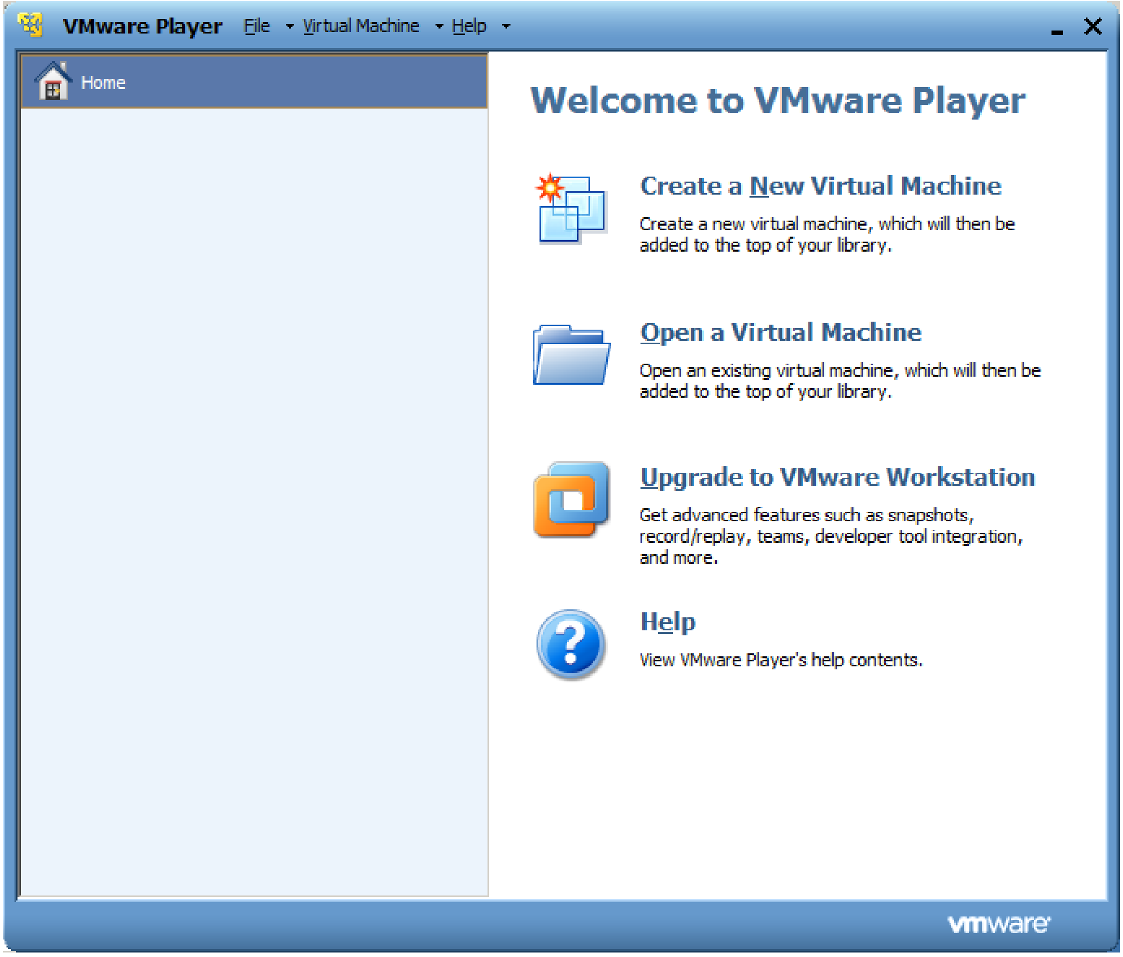
At this point the Virtual Machine is ready to be started.

Please follow the Endpoint Protector Appliance User Manual from this point on.

3.2. Implementing in VMware Player 3.0 using VMX Format

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



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.

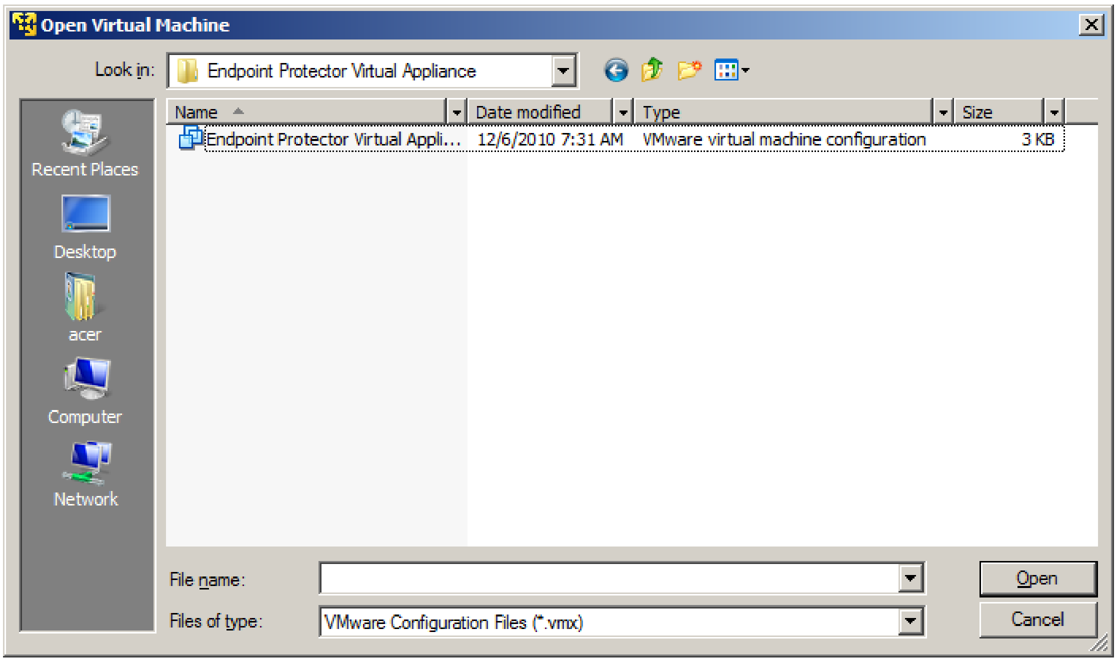
Upgrade to VMware Workstation

Get advanced features such as snapshots, record/replay, teams, developer tool integration, and more.

Help

View VMware Player's help contents.

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

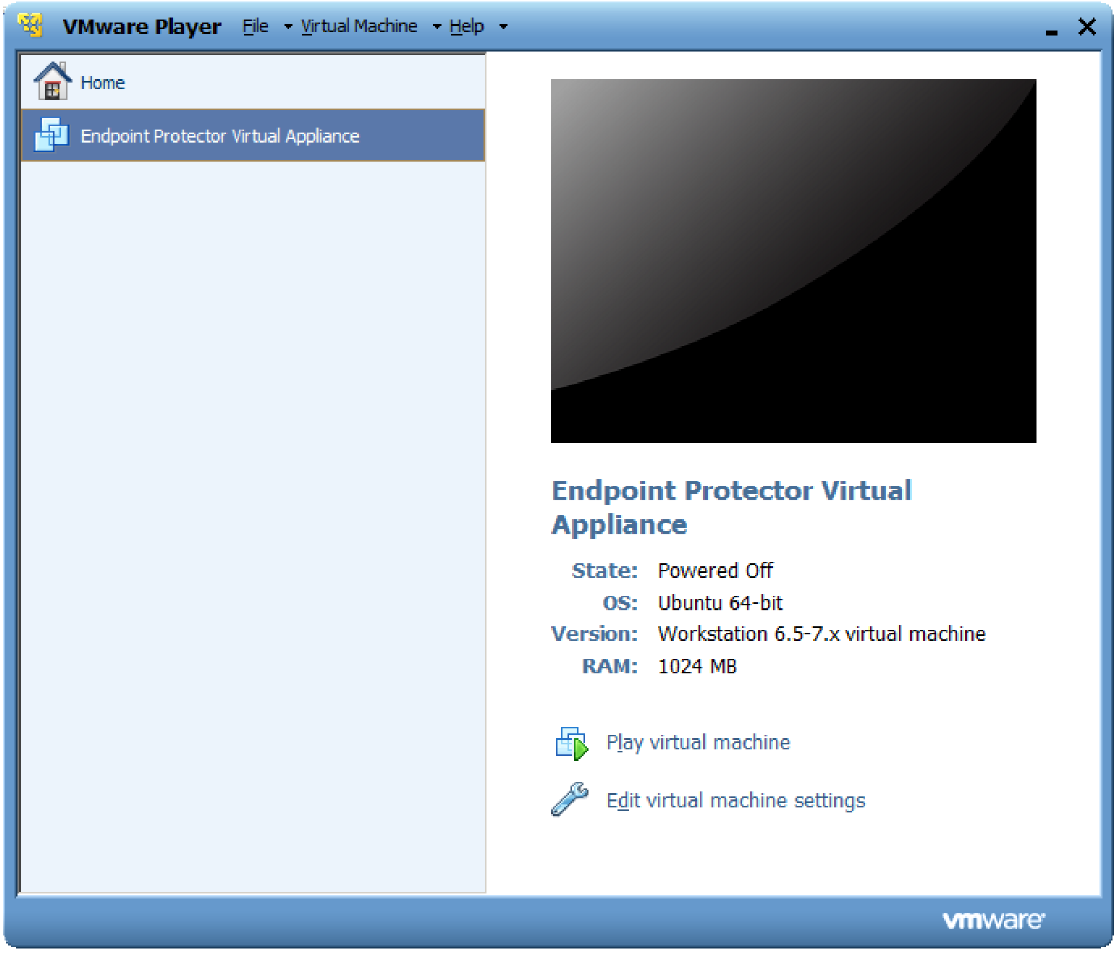


Name	Date modified	Type	Size
Endpoint Protector Virtual Appli…	12/6/2010 7:31 AM	VMware virtual machine configuration	3 KB

File name:

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

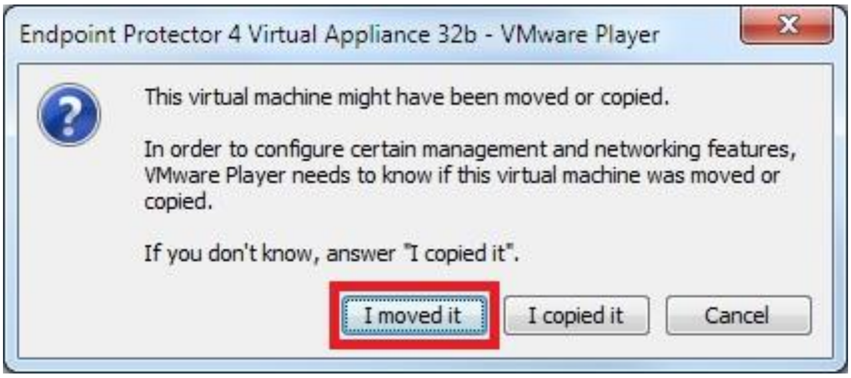
4. After the Virtual Machine is in your inventory click Play Virtual Machine



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.

Please follow the Endpoint Protector Appliance User Manual from this point on.

Note!

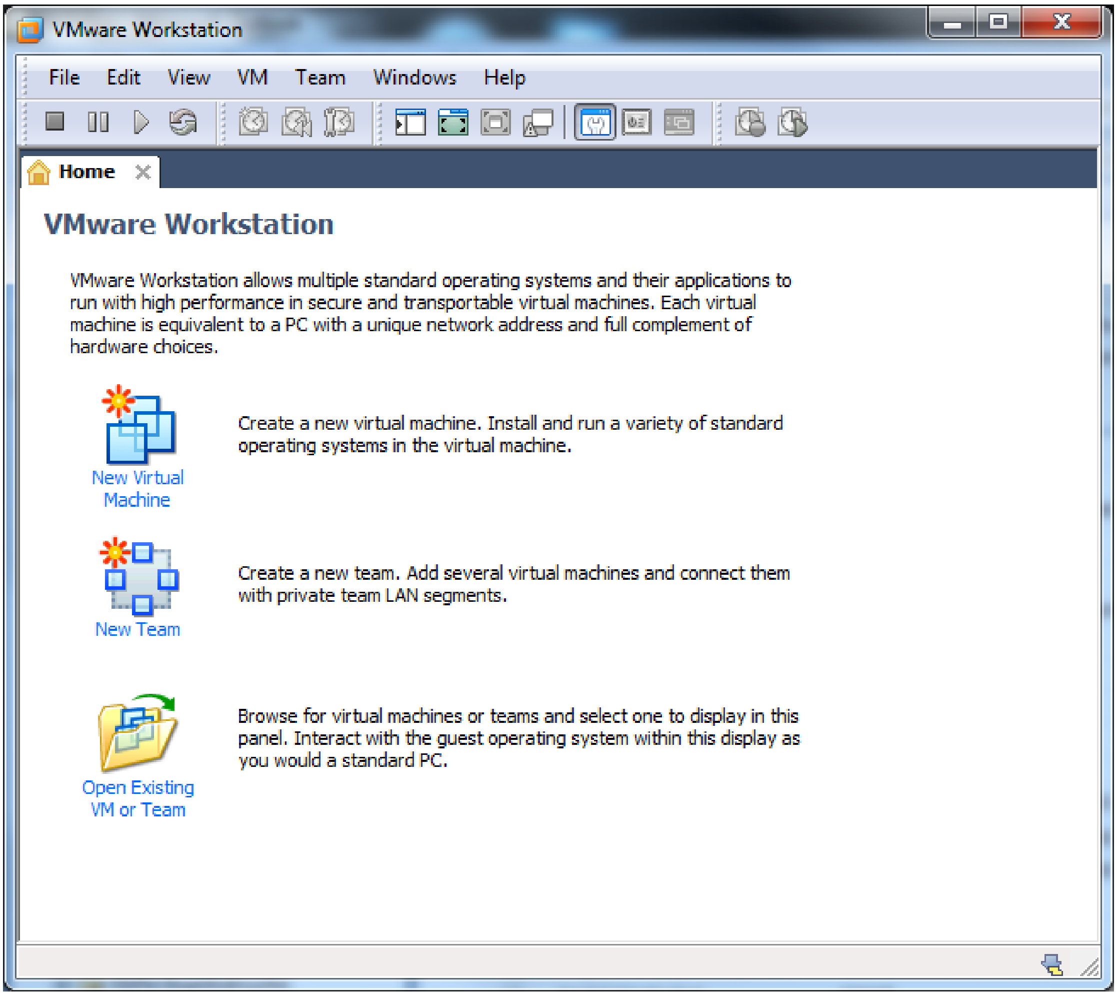
Do not suspend the VMware Player while Endpoint Protector Virtual Appliance is running!

Do not shut down your computer while VMware Player is running.

3.3. Implementing in VMware Workstation 6.5 using VMX Format

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

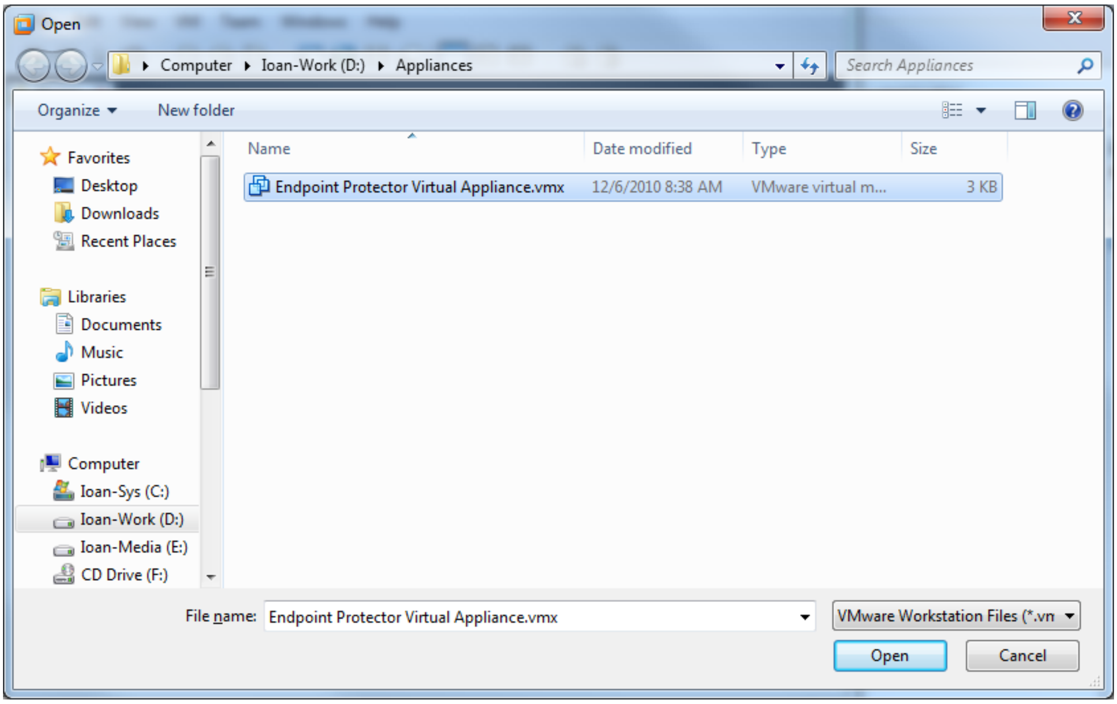
VMware Workstation allows multiple standard operating systems and their applications to run with high performance in secure and transportable virtual machines. Each virtual machine is equivalent to a PC with a unique network address and full complement of hardware choices.

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

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

Open Existing VM or Team — 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

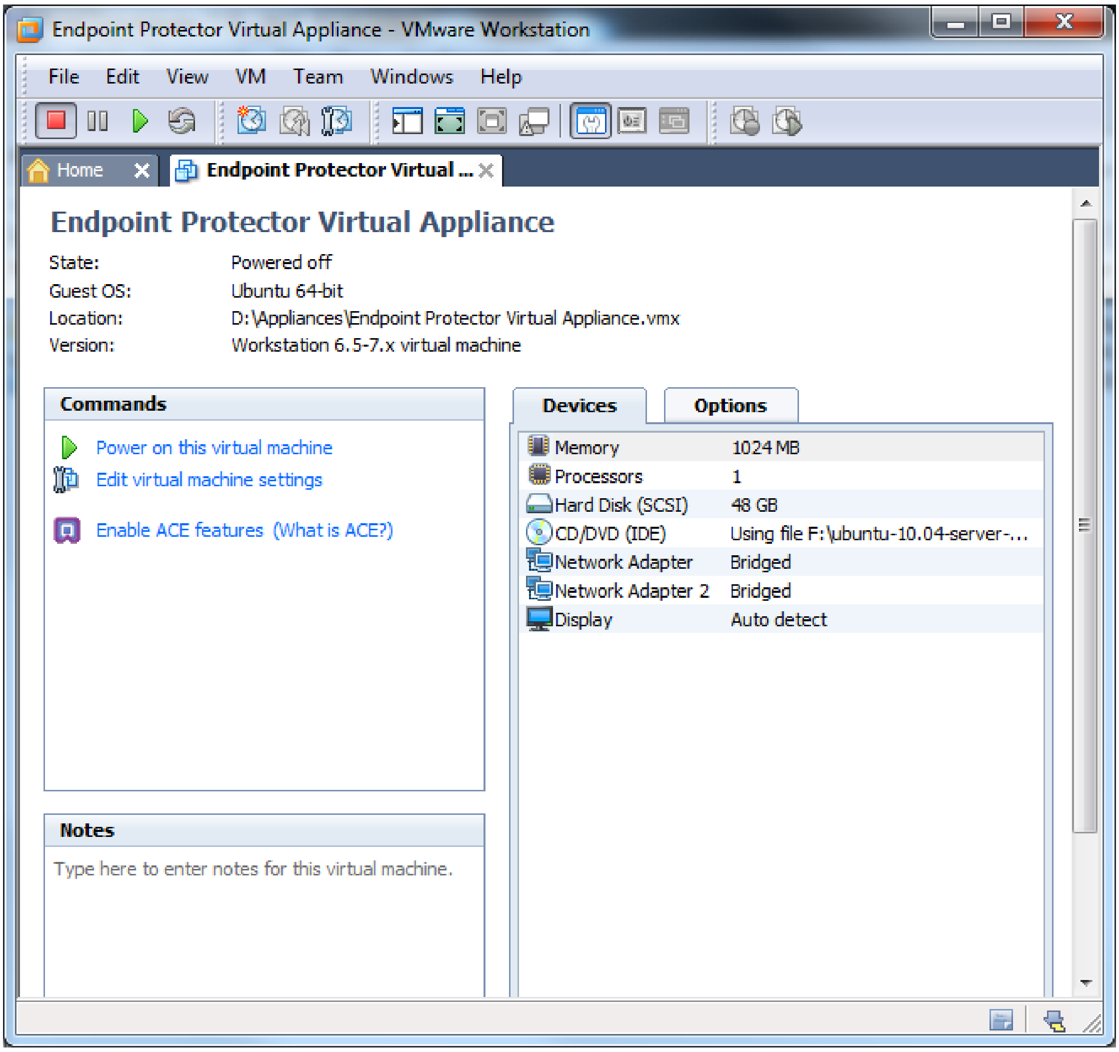


Name	Date modified	Type	Size
Endpoint Protector Virtual Appliance.vmx	12/6/2010 8:38 AM	VMware virtual m...	3 KB

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 ...

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

Commands

- Power on this virtual machine
- Edit virtual machine settings
- Enable ACE features (What is ACE?)

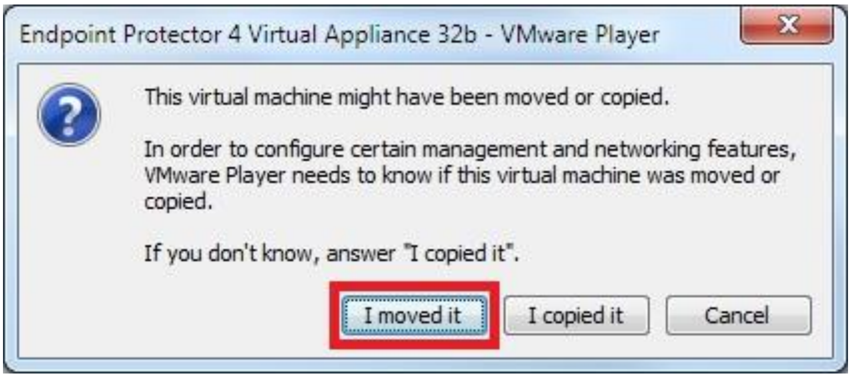
Notes

Type here to enter notes for this virtual machine.

Devices | Options

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)



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".

The Virtual Machine is started and ready for use.

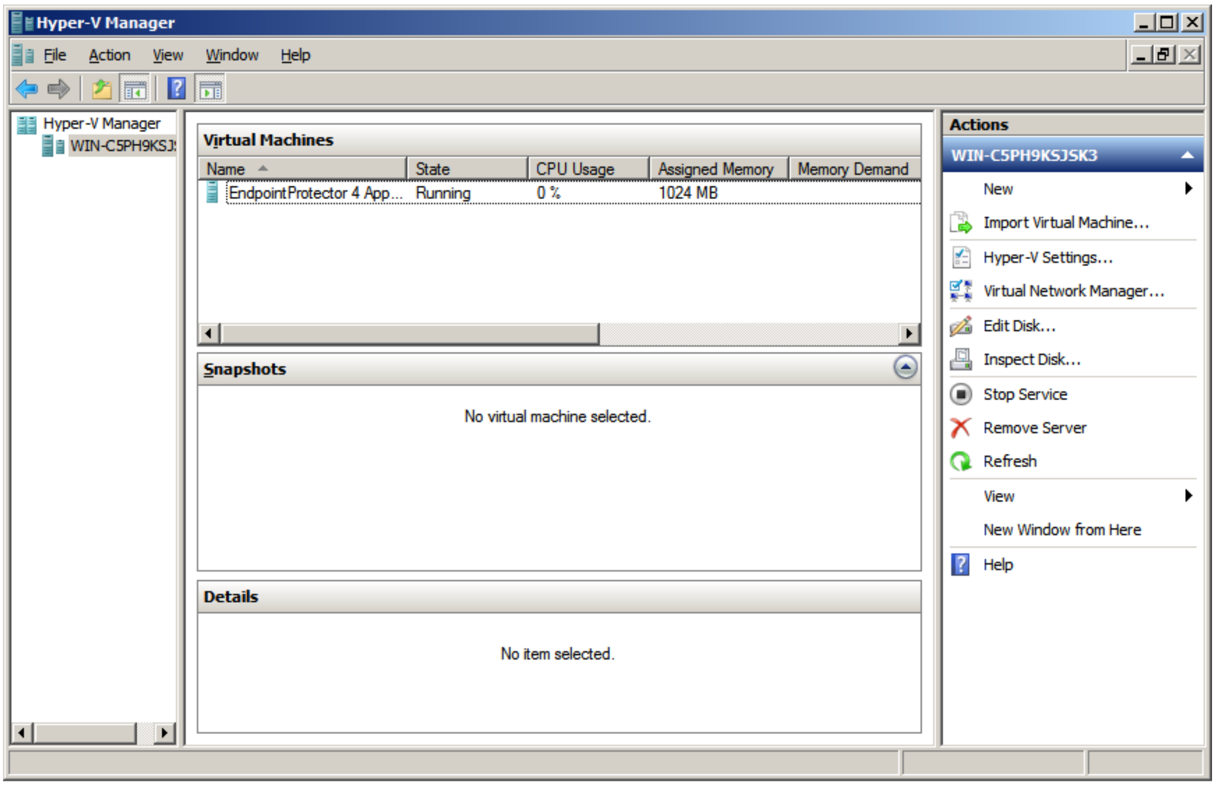
Please follow the Endpoint Protector Appliance User Manual from this point on.

4. Implementing using VHD Format

4.1. Implementing in Microsoft Hyper-V 2008 using VHD Format

1. Extract the downloaded Endpoint Protector Virtual Appliance zip package

2. Start Hyper-V Manager

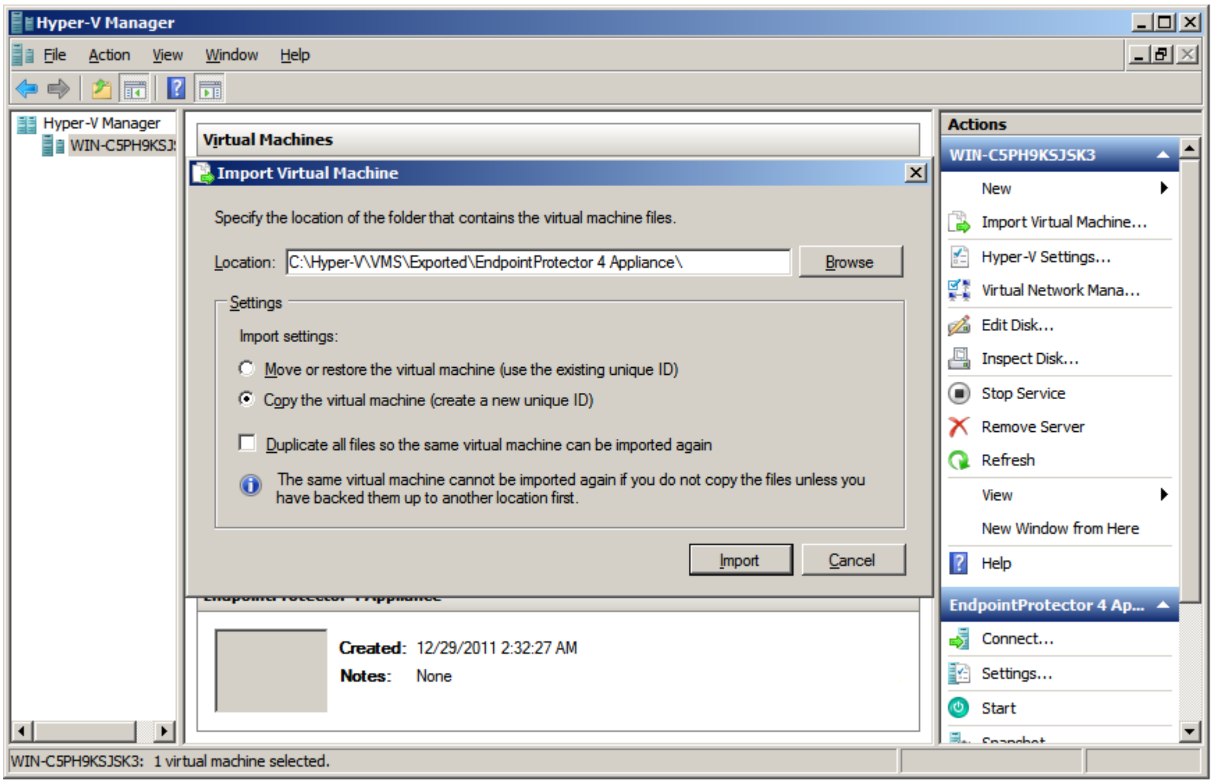


Name	State	CPU Usage	Assigned Memory	Memory Demand
EndpointProtector 4 App...	Running	0 %	1024 MB	

No virtual machine selected.

No item selected.

3. Select Import Virtual Machine Option from right side box



Specify the location of the folder that contains the virtual machine files.

Location: C:\Hyper-V\VMS\Exported\EndpointProtector 4 Appliance\

Settings

Import settings:

○ Move or restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

□ Duplicate all files so the same virtual machine can be imported again

The same virtual machine cannot be imported again if you do not copy the files unless you have backed them up to another location first.

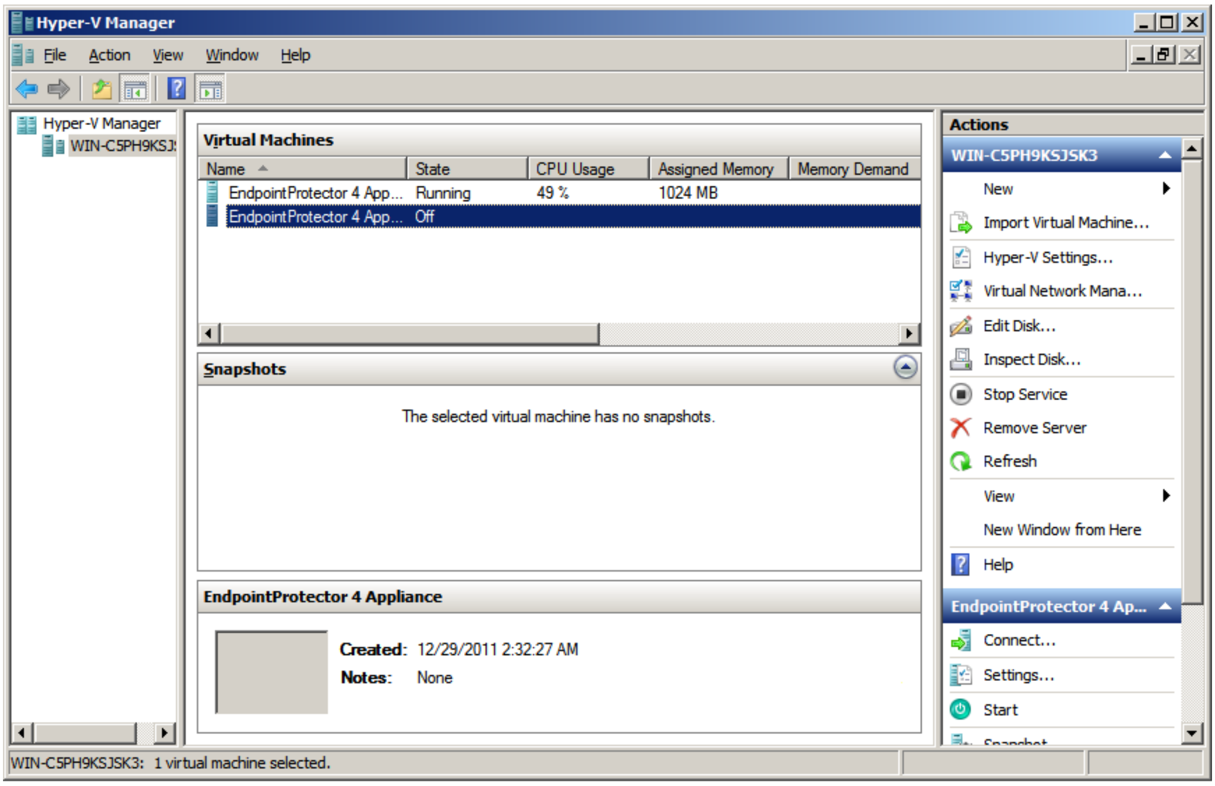
Created: 12/29/2011 2:32:27 AM

Notes: None

WIN-C5PH9KSJSK3: 1 virtual machine selected.

Select the folder which contains the Appliance folders/files.
Choose Copy the virtual machine as Import Settings.

4. Press Import button



Name	State	CPU Usage	Assigned Memory	Memory Demand
EndpointProtector 4 App...	Running	49 %	1024 MB	
EndpointProtector 4 App...	Off			

The selected virtual machine has no snapshots.

EndpointProtector 4 Appliance

Created: 12/29/2011 2:32:27 AM
Notes: None

WIN-C5PH9KSJSK3: 1 virtual machine selected.

5. The new Virtual Machine will appear in the Virtual Machines list.

The Virtual Machine is started and ready for use.

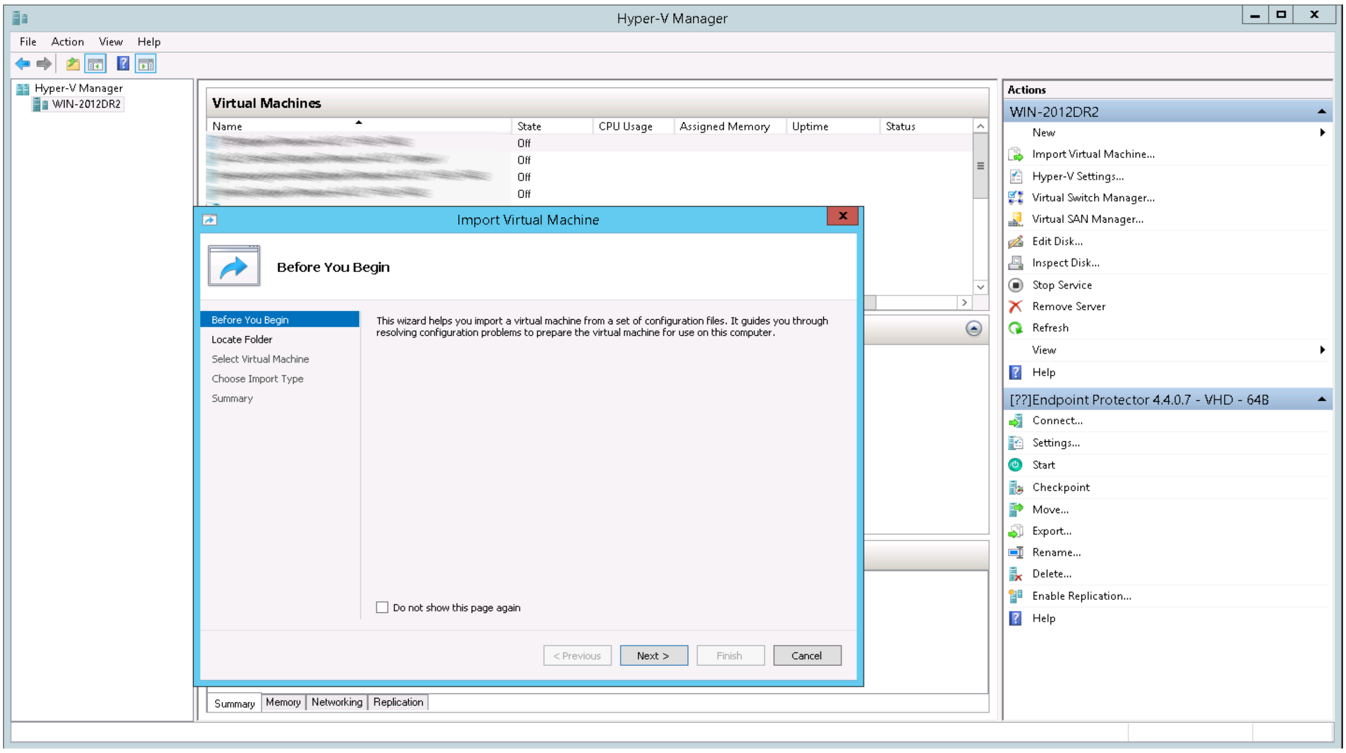
Please follow the Endpoint Protector Appliance User Manual from this point on.

4.2. Implementing in Microsoft Hyper-V 2012 using VHD Format

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

2. Start **Hyper-V Manager**

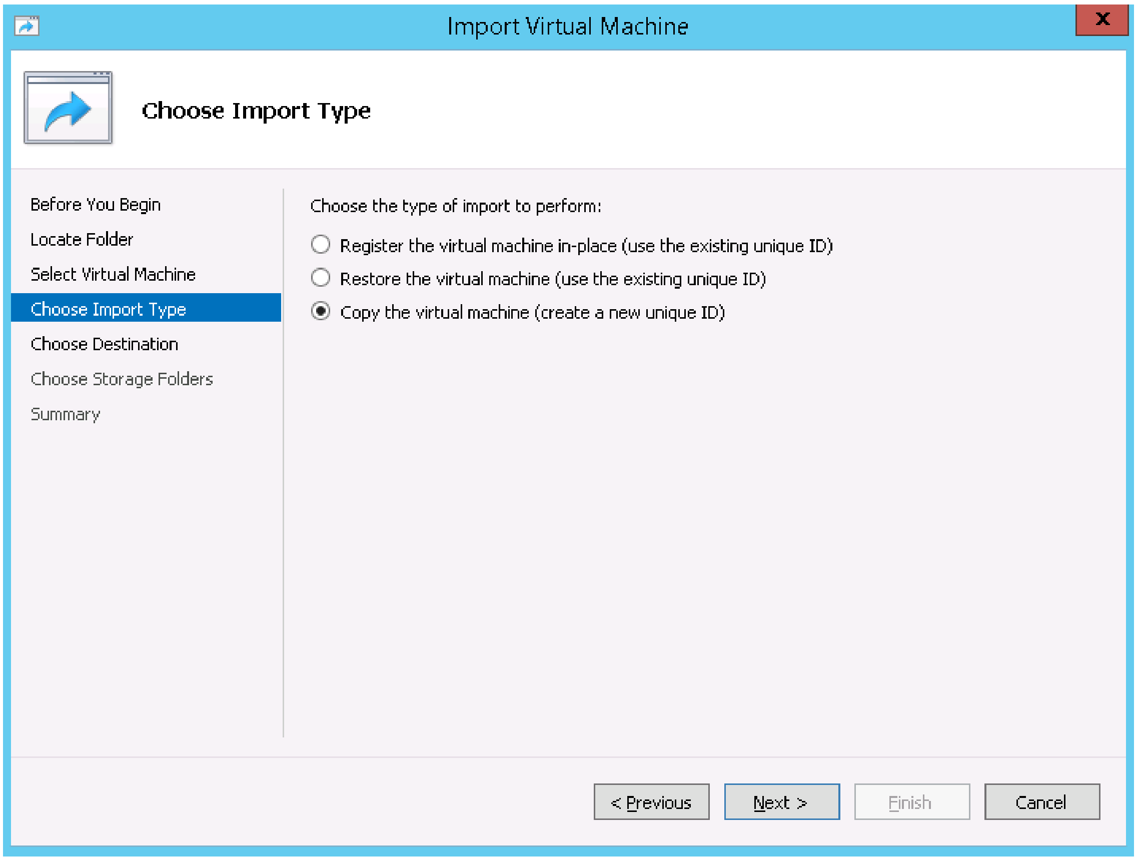
3. Select the option to **Import Virtual Machine...** from the right-side box



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.

3.1 Select the folder containing the appliances' folders and files.

3.2 At the step "Choose Import Type" select the option to **Copy the virtual machine (create a new unique ID)**



Choose Import Type

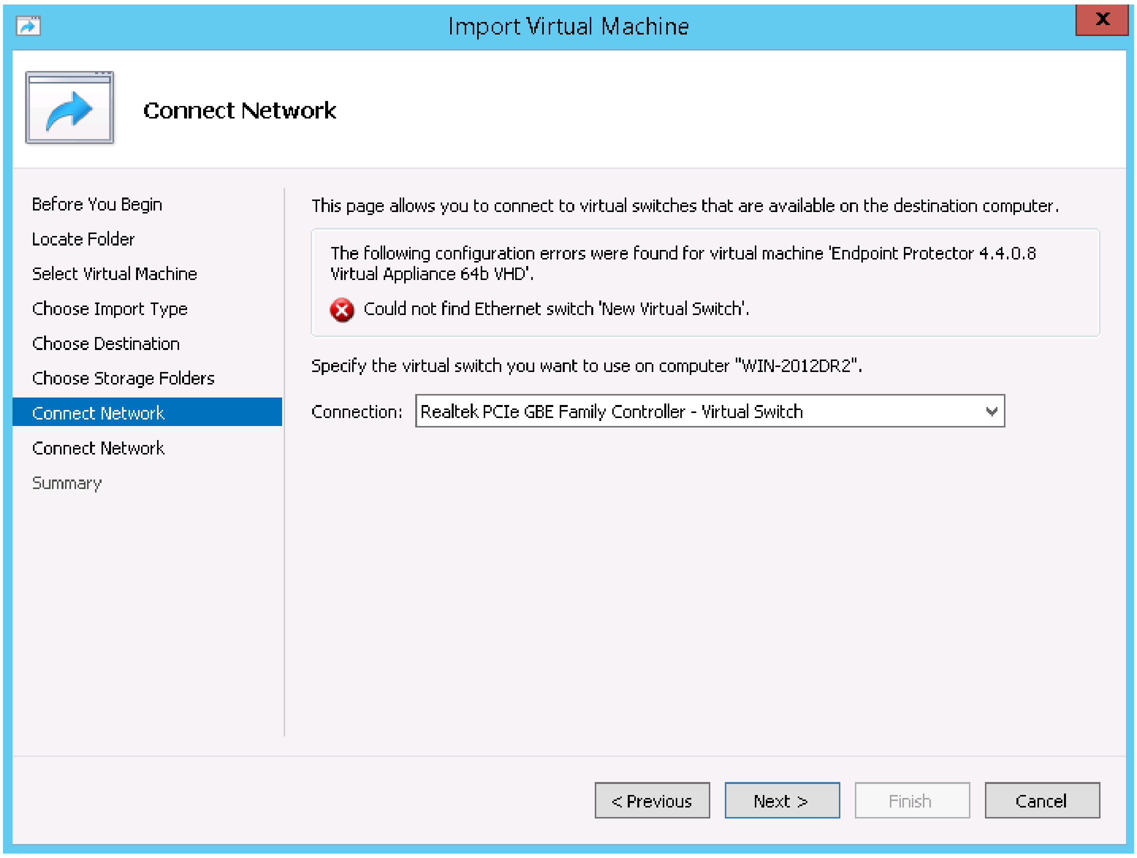
Choose the type of import to perform:

○ 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)

3.3 The “Connect Network” step will prompt with 2 errors, one for each Network Adapter. Ignore these and press **Next, Next** and then **Finish**.



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 4.4.0.8 Virtual Appliance 64b VHD'.

☒ Could not find Ethernet switch 'New Virtual Switch'.

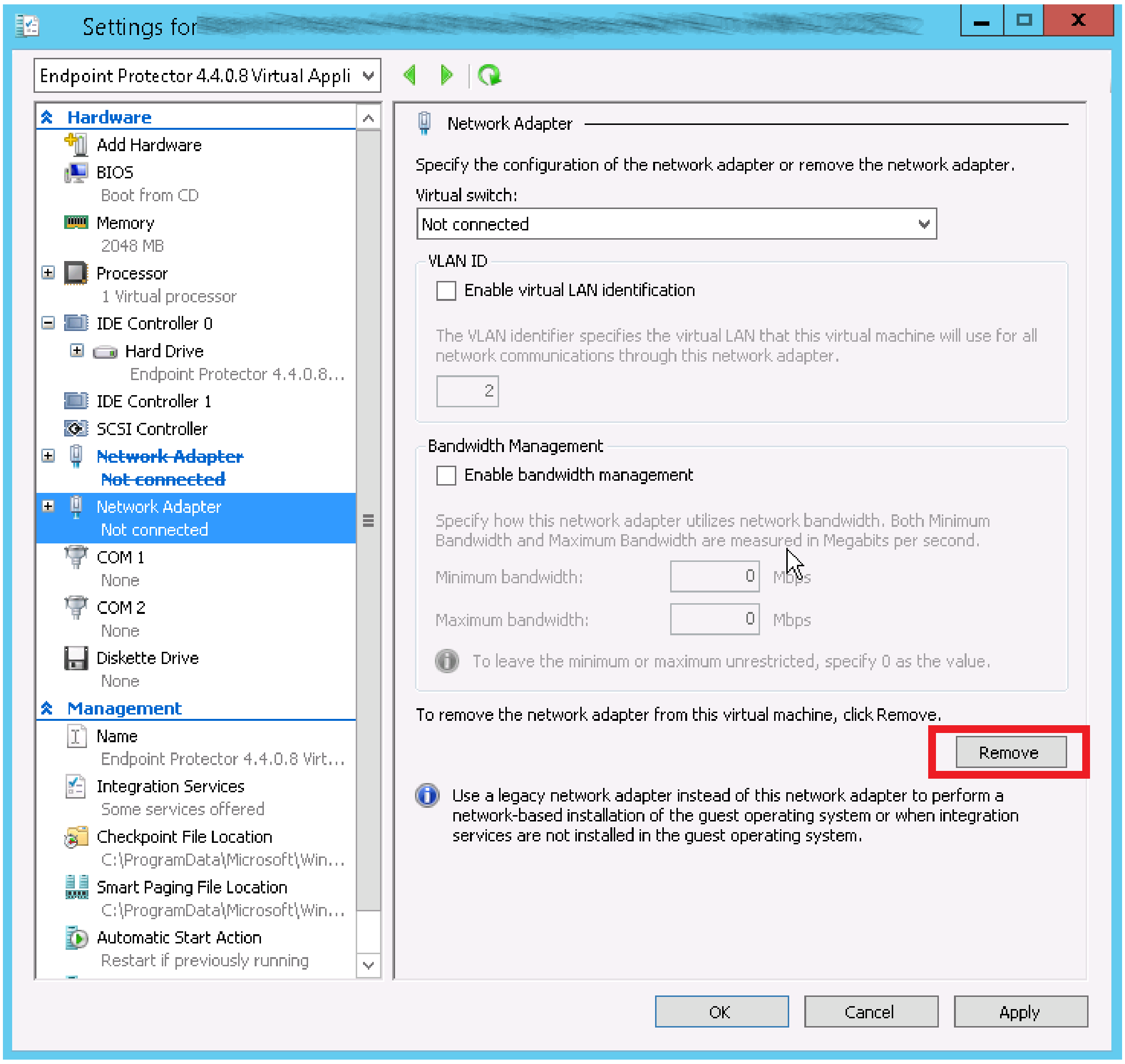
Specify the virtual switch you want to use on computer "WIN-2012DR2".

Connection: Realtek PCIe GBE Family Controller - Virtual Switch

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

5. Right click on the newly created Virtual Machine and select **Settings…**

6. **Remove** the two existing network adapters from the left side box



Settings for [redacted]

Endpoint Protector 4.4.0.8 Virtual Appli

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  2048 MB
- ⊞ Processor
  1 Virtual processor
- ⊟ IDE Controller 0
  - ⊞ Hard Drive
    Endpoint Protector 4.4.0.8…
- IDE Controller 1
- SCSI Controller
- ⊞ ~~Network Adapter~~
  ~~Not connected~~
- ⊞ Network Adapter
  Not connected
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  Endpoint Protector 4.4.0.8 Virt…
- Integration Services
  Some services offered
- Checkpoint File Location
  C:\ProgramData\Microsoft\Win…
- Smart Paging File Location
  C:\ProgramData\Microsoft\Win…
- Automatic Start Action
  Restart if previously running

Network Adapter

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

Virtual switch:
Not connected

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

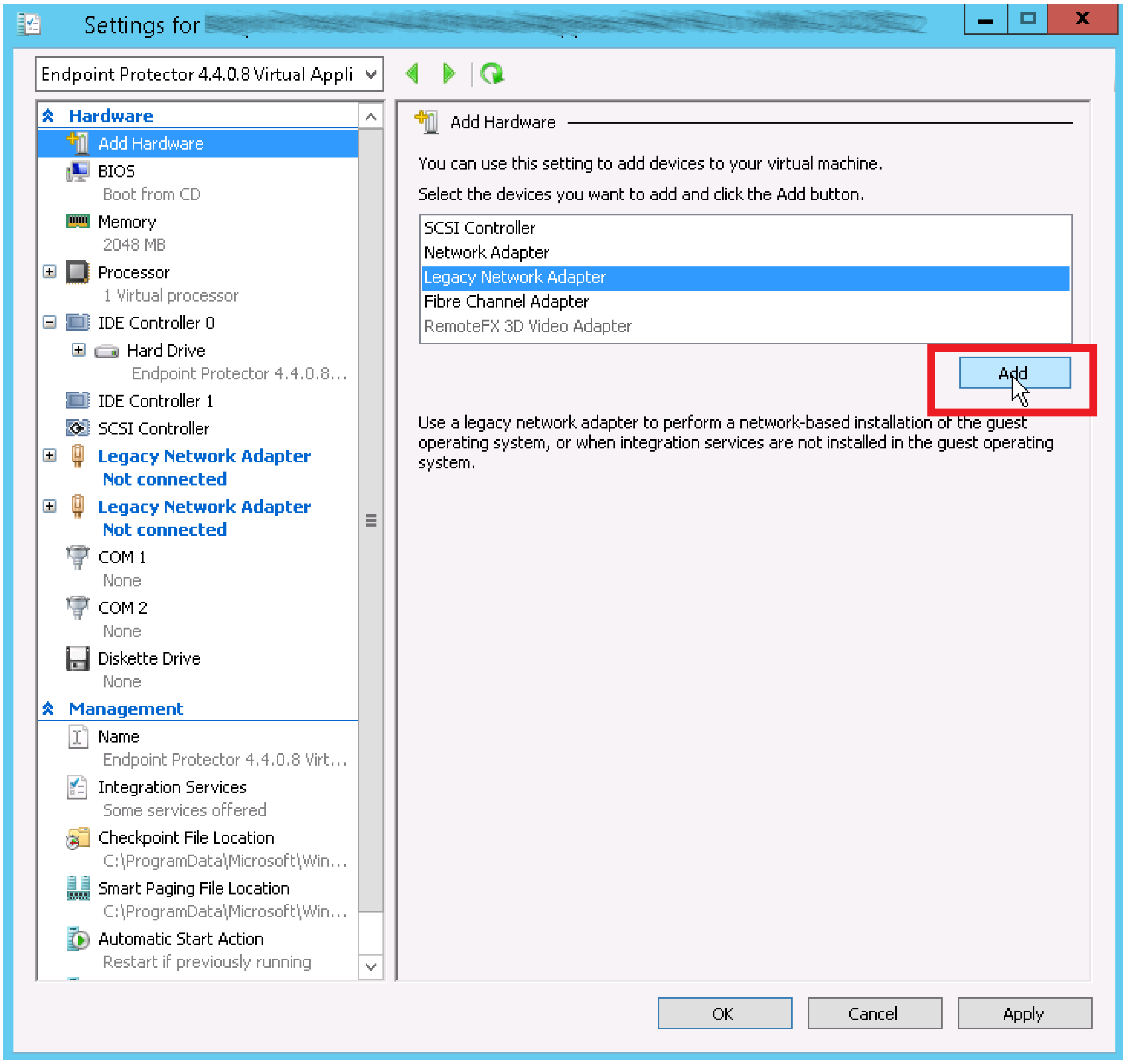
To leave the minimum or maximum unrestricted, specify 0 as the value.

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

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.

7. Add two **Legacy Network Adapters** with the **Add Hardware** command.



Settings for [redacted]

Endpoint Protector 4.4.0.8 Virtual Appli

Hardware
Add Hardware
BIOS
Boot from CD
Memory
2048 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
Endpoint Protector 4.4.0.8...
IDE Controller 1
SCSI Controller
Legacy Network Adapter
Not connected
Legacy Network Adapter
Not connected
COM 1
None
COM 2
None
Diskette Drive
None

Management
Name
Endpoint Protector 4.4.0.8 Virt...
Integration Services
Some services offered
Checkpoint File Location
C:\ProgramData\Microsoft\Win...
Smart Paging File Location
C:\ProgramData\Microsoft\Win...
Automatic Start Action
Restart if previously running

Add Hardware

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

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

SCSI Controller
Network Adapter
Legacy Network Adapter
Fibre Channel Adapter
RemoteFX 3D Video Adapter

Use a legacy 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.

Note!

Remember to specify the configurations of the two Legacy Network Adapters so that their status will be changed from “Not Connected”.

9. Click on **Apply**.

10. The Virtual Machine is now imported and ready to to be configured.

Please follow the Endpoint Protector Appliance User Manual from this point on.

Note!

In case you experience difficulties using Microsoft Hyper-V 2012 please contact support@endpointprotector.com

5. Access Appliance Setup Wizard

5.1. Appliance network configuration from console

Endpoint Protector Appliance console gives you the possibility to manage your network configuration, reboot or shut down your Virtual Appliance.

To allow access through your firewall you need to allow the following ports:

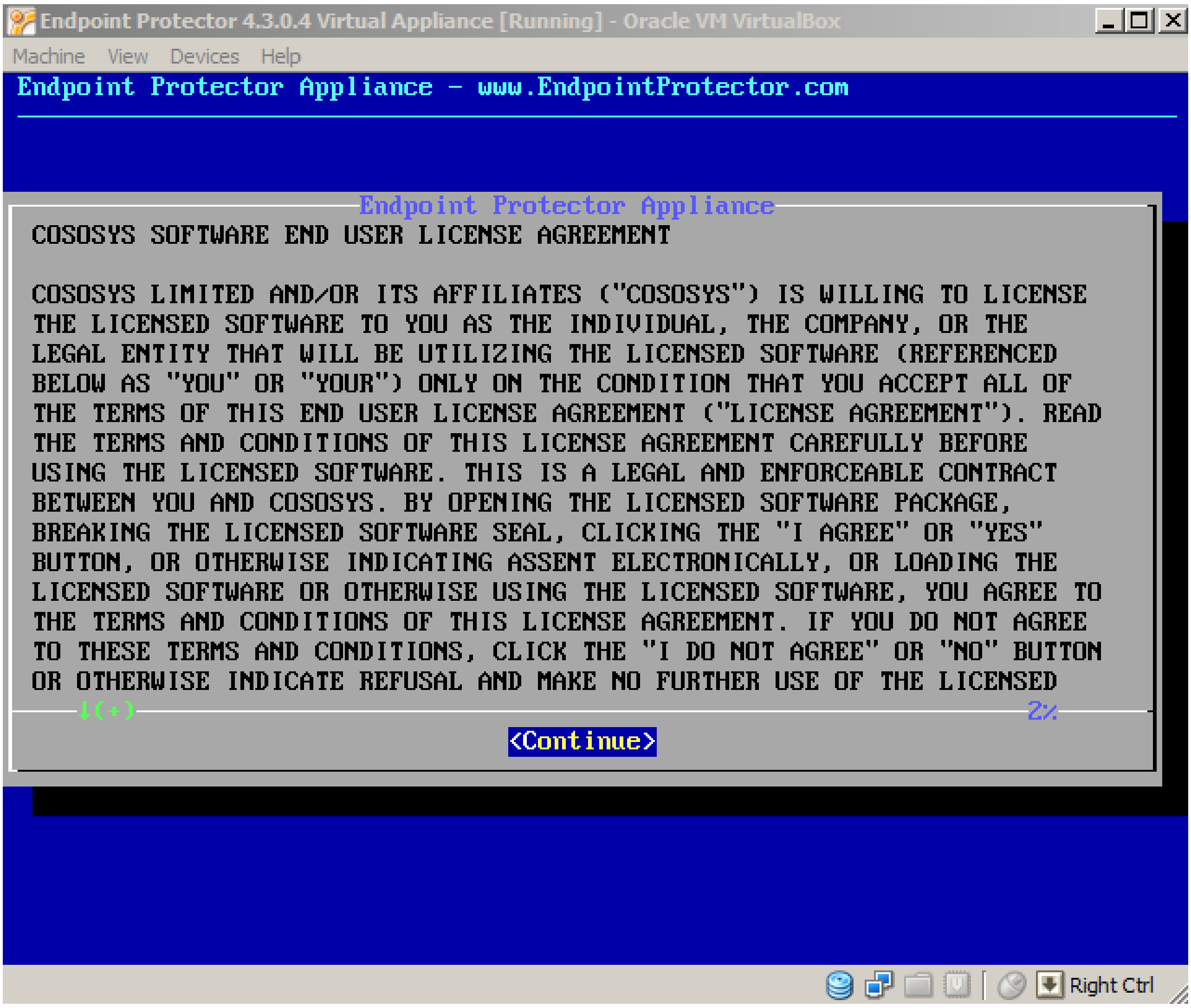
-Server and Client: 443

-Live Update (liveupdate.endpointprotector.com): 80 & 443

-MDM Cloud (cloud.endpointprotector.com): 443

To configure the Virtual Appliance's network it is required to follow the steps below.

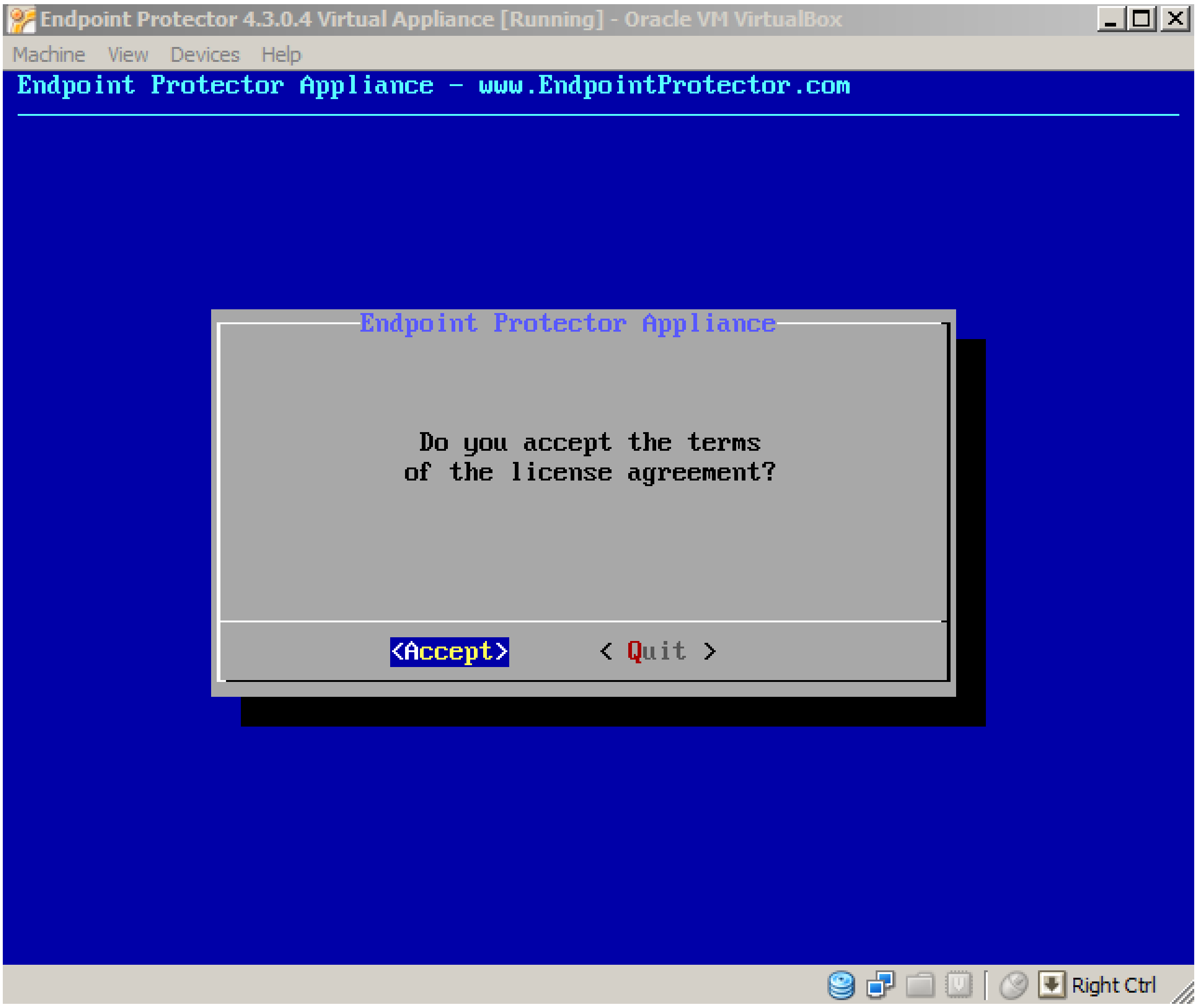
1. Press Continue when finished reading the End User License Agreement



Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help
Endpoint Protector Appliance - www.EndpointProtector.com
Endpoint Protector Appliance

```
COSOSYS SOFTWARE END USER LICENSE AGREEMENT

COSOSYS LIMITED AND/OR ITS AFFILIATES ("COSOSYS") IS WILLING TO LICENSE
THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE
LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED
BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF
THE TERMS OF THIS END USER LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ
THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE
USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT
BETWEEN YOU AND COSOSYS. BY OPENING THE LICENSED SOFTWARE PACKAGE,
BREAKING THE LICENSED SOFTWARE SEAL, CLICKING THE "I AGREE" OR "YES"
BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE
LICENSED SOFTWARE OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO
THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE
TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON
OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE LICENSED
↓(+)                                                              2%
```

2. Press Accept

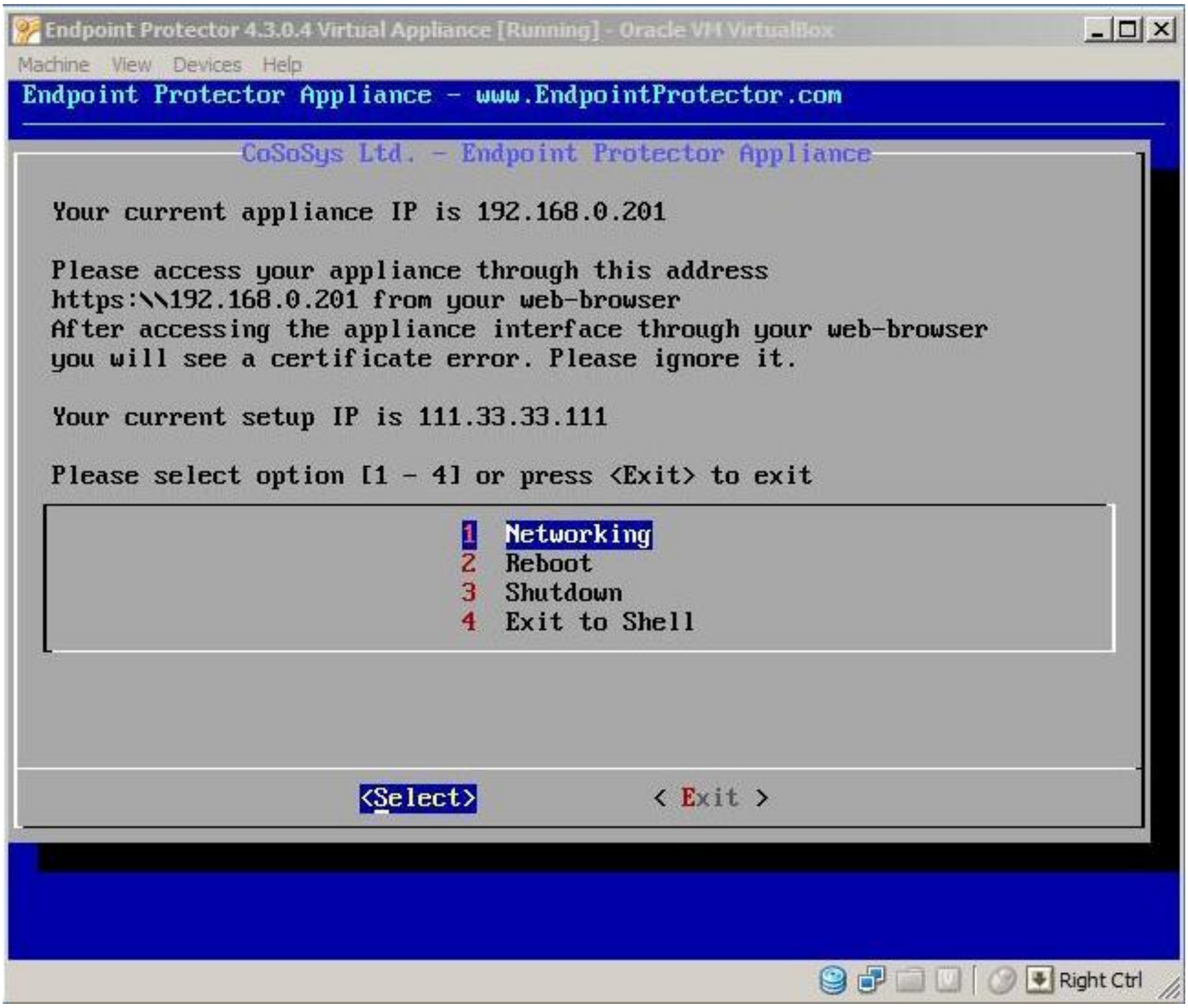

Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

Endpoint Protector Appliance - www.EndpointProtector.com

Endpoint Protector Appliance

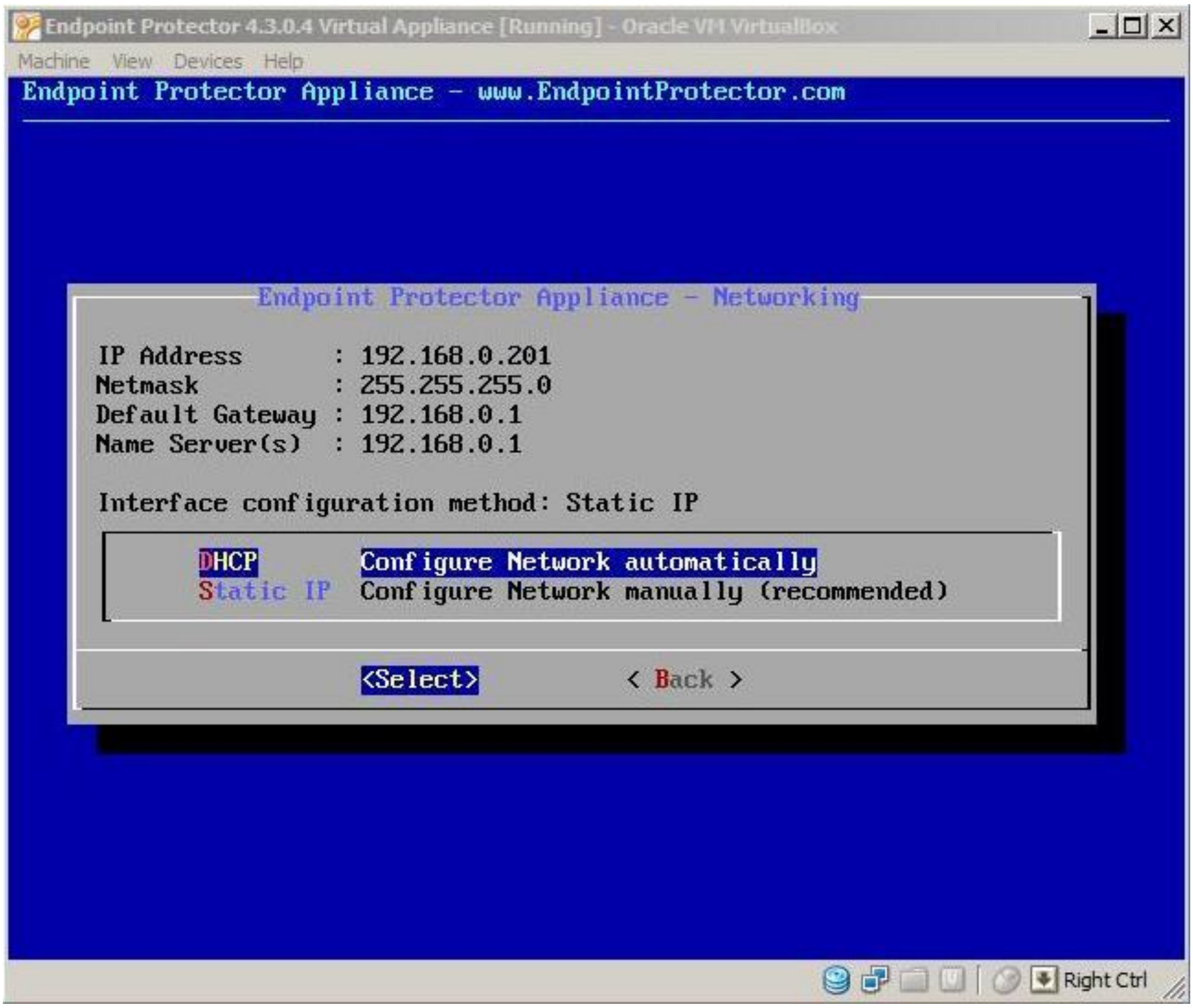
Do you accept the terms
of the license agreement?

3. Select Networking


Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

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

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 - 4] or press <Exit> to exit

                    1  Networking
                    2  Reboot
                    3  Shutdown
                    4  Exit to Shell

            <Select>              < Exit >
```

4. The configuration methods are now available.


Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine
View
Devices
Help
Right Ctrl

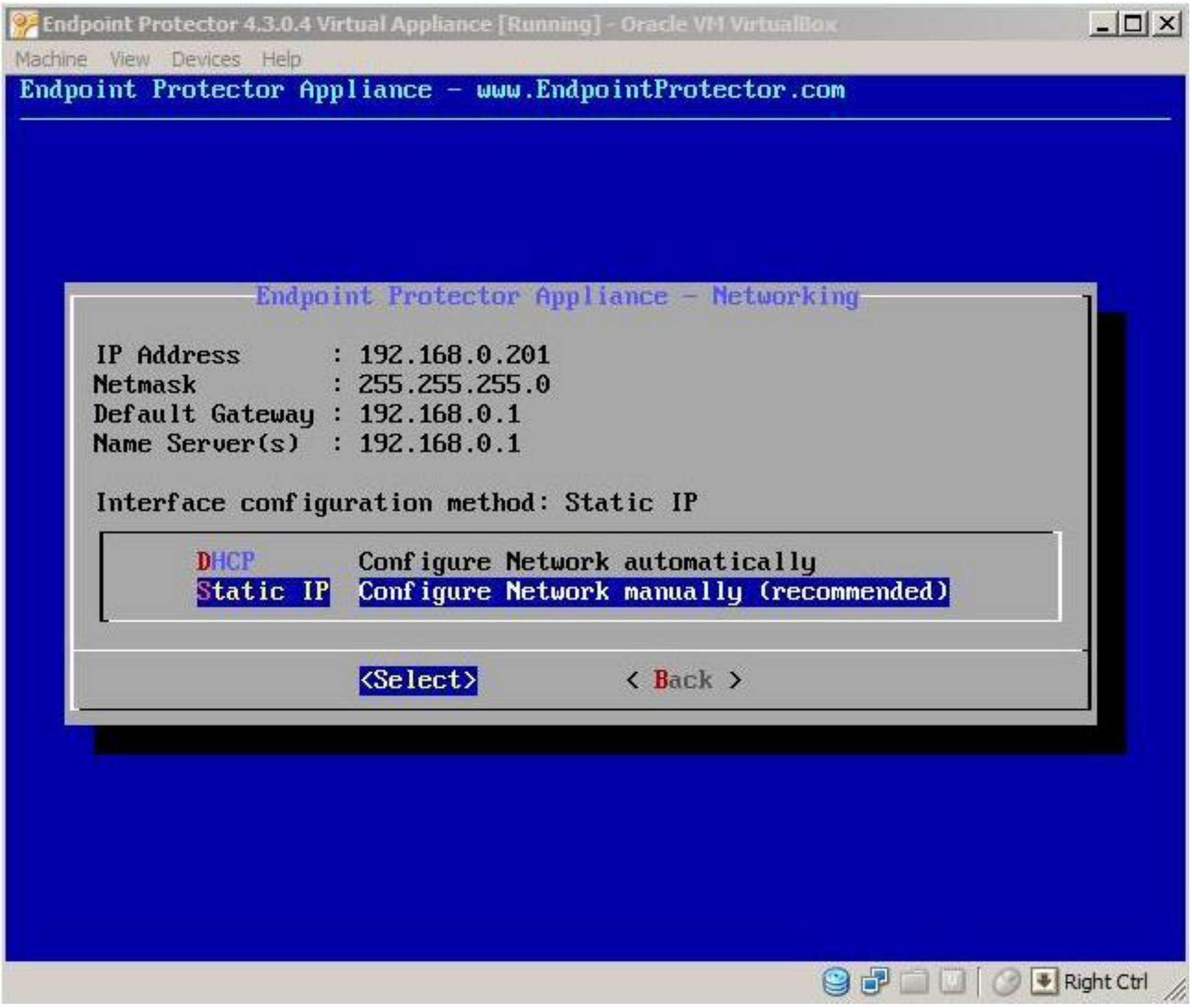
```
Endpoint Protector Appliance - www.EndpointProtector.com

Endpoint Protector Appliance - Networking

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

Interface configuration method: Static IP

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

             <Select>              < Back >
```

Note!

We recommend a manual configuration of the network settings.

5.1.1 Manual configuration

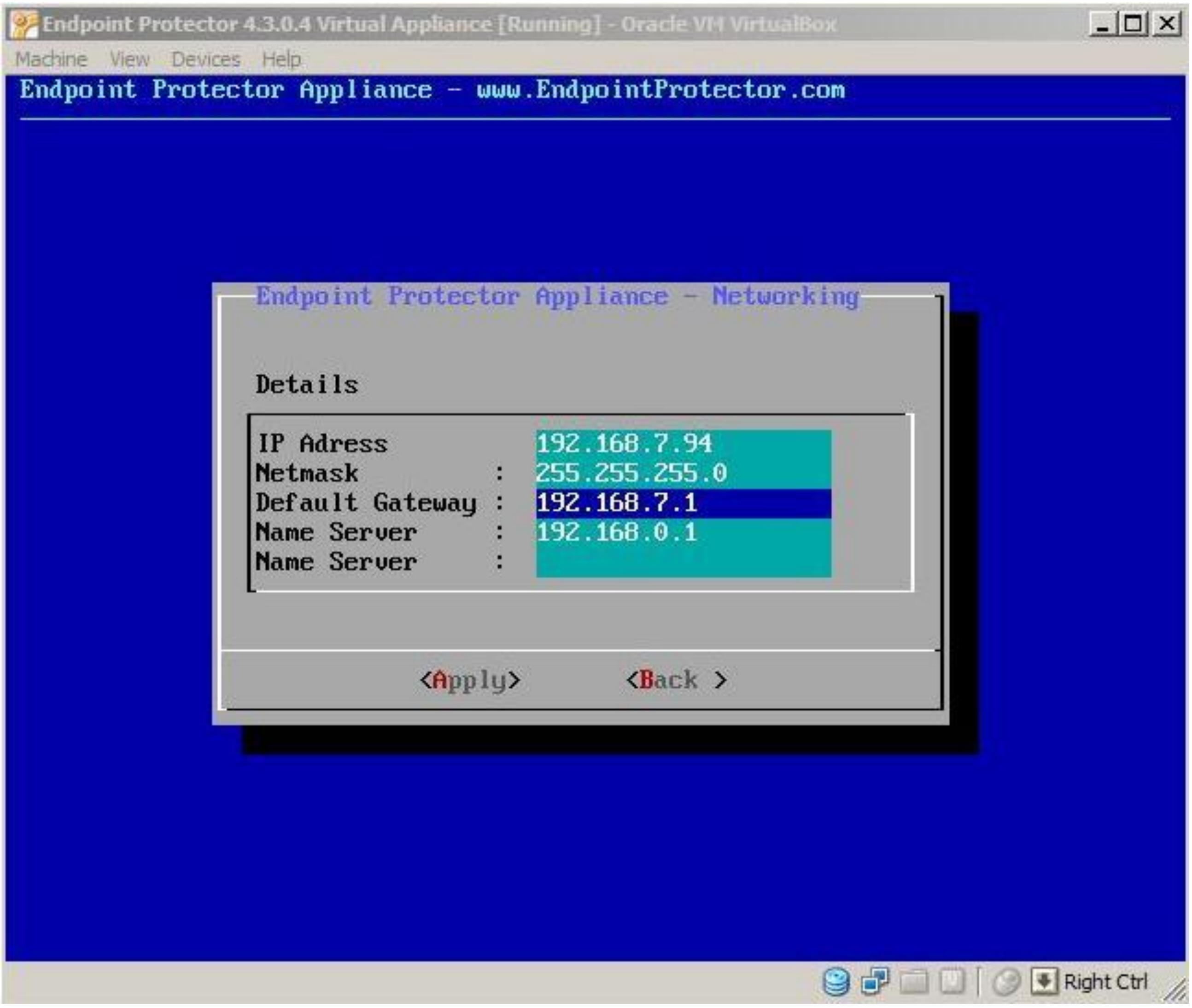
1. Select Configure Network manually (recommended)



Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help

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

        Endpoint Protector Appliance - Networking

IP Address      : 192.168.0.201
Netmask         : 255.255.255.0
Default Gateway : 192.168.0.1
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 up 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 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine
View
Devices
Help
Right Ctrl

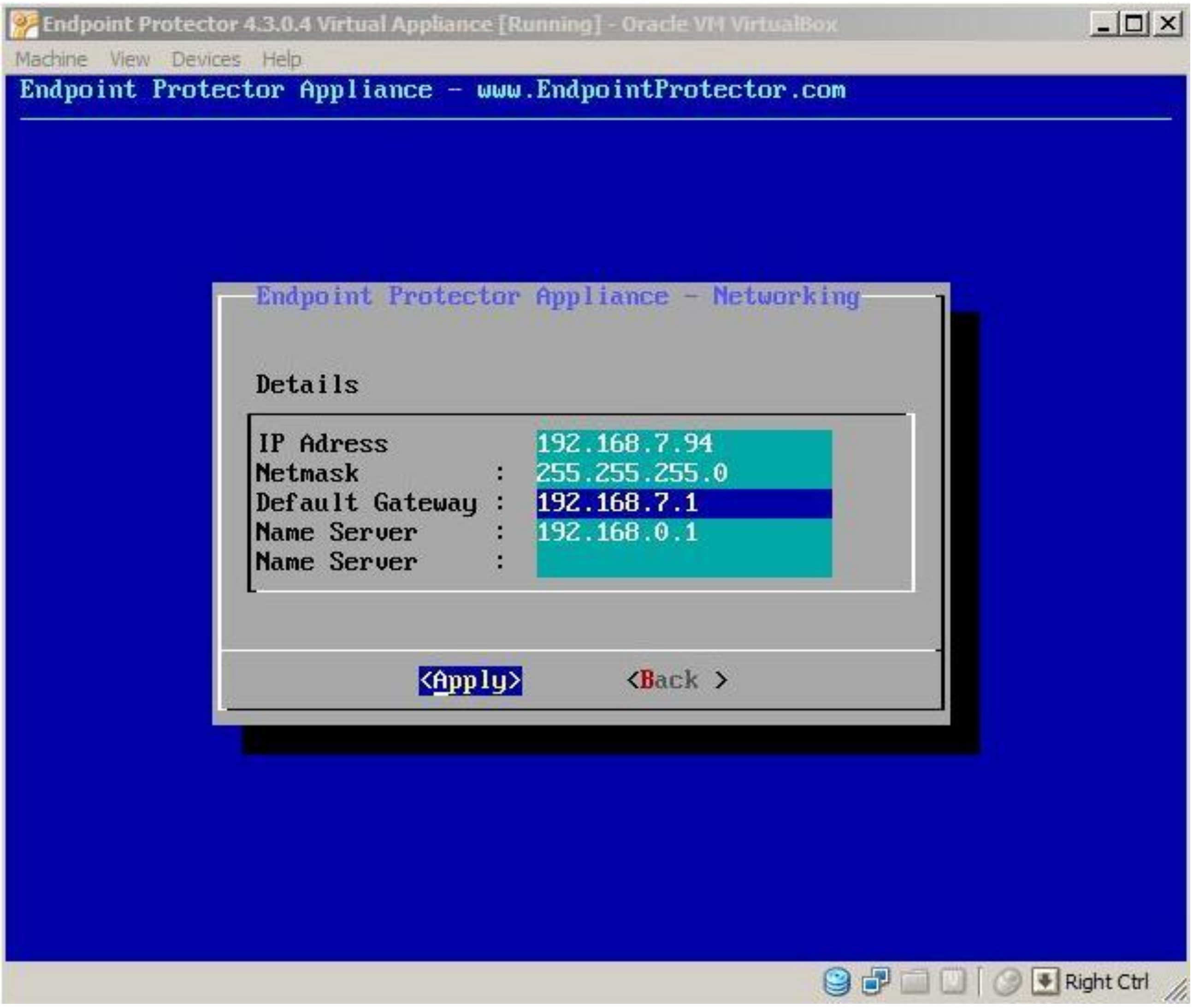
Endpoint Protector Appliance - www.EndpointProtector.com

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     :
```

3. Press Tab



Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

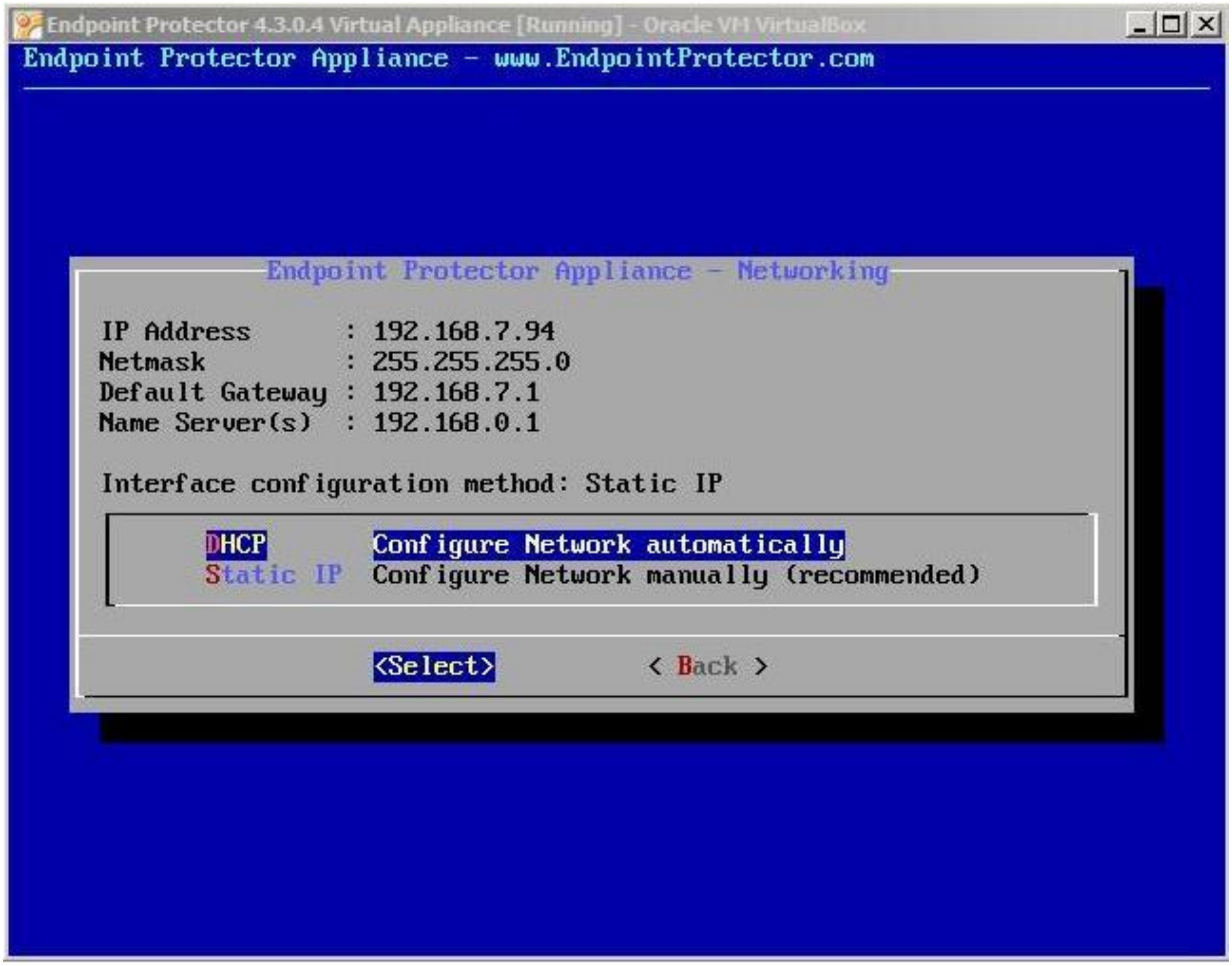
Endpoint Protector Appliance - www.EndpointProtector.com

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       :
```

4. Press Enter



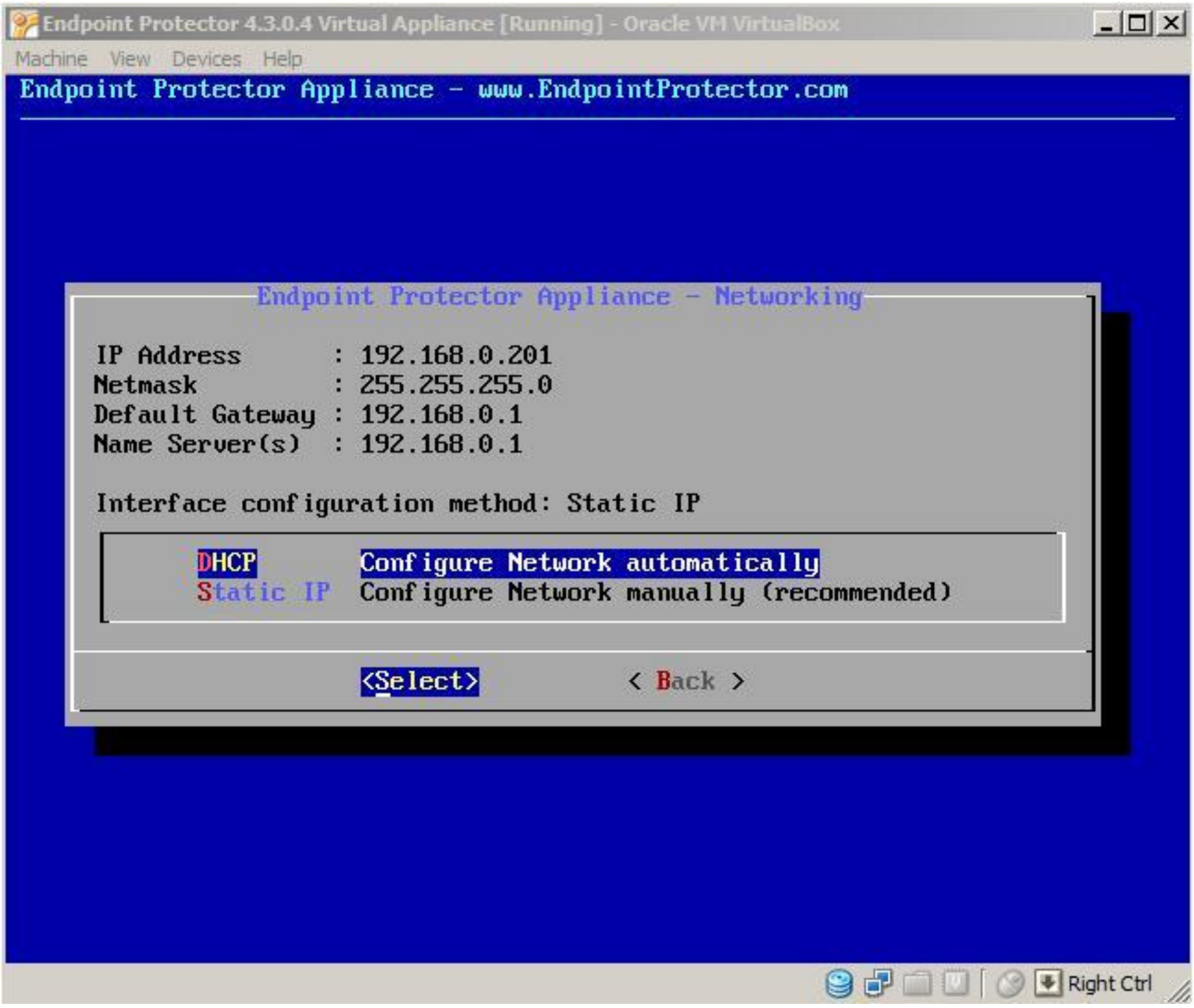
Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox

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

Endpoint Protector Appliance - Networking

IP Address      : 192.168.7.94
Netmask         : 255.255.255.0
Default Gateway : 192.168.7.1
Name Server(s)  : 192.168.0.1

Interface configuration method: Static IP

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

               <Select>          < Back >
```

The virtual appliance now will work on the configured IP Address. You can access you appliance through the configured address (192.168.7.94 in the example given above)

5.1.2. Automatic configuration

Select configure network automatically, and press Enter. IP Address and Default Gateway will be configured automatically.



Endpoint Protector 4.3.0.4 Virtual Appliance [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

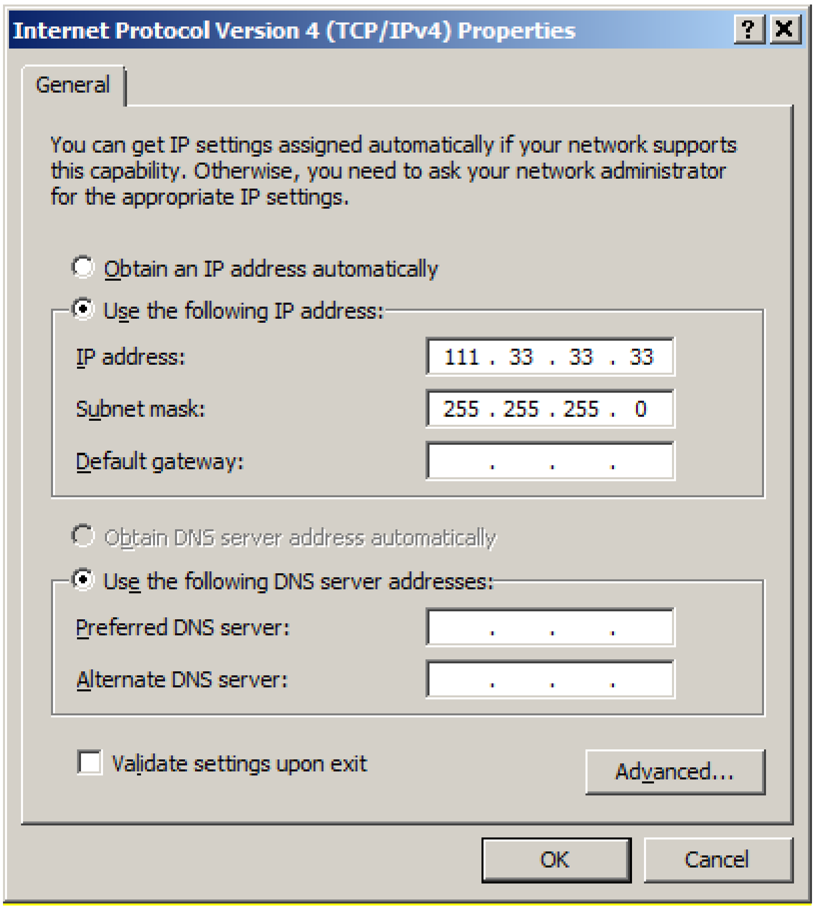
```
Endpoint Protector Appliance - www.EndpointProtector.com

            Endpoint Protector Appliance - Networking

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

Interface configuration method: Static IP

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

                   <Select>             < Back >
```

5.2. Hardware Appliance Setup Wizard

With your computer that is in the same local network as your virtual appliance, connect now to the virtual appliance.
Check the TCP/IPv4 Settings to be on your PC:

IP Address 111.33.33.33

Subnet Mask 255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	111 . 33 . 33 . 33
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

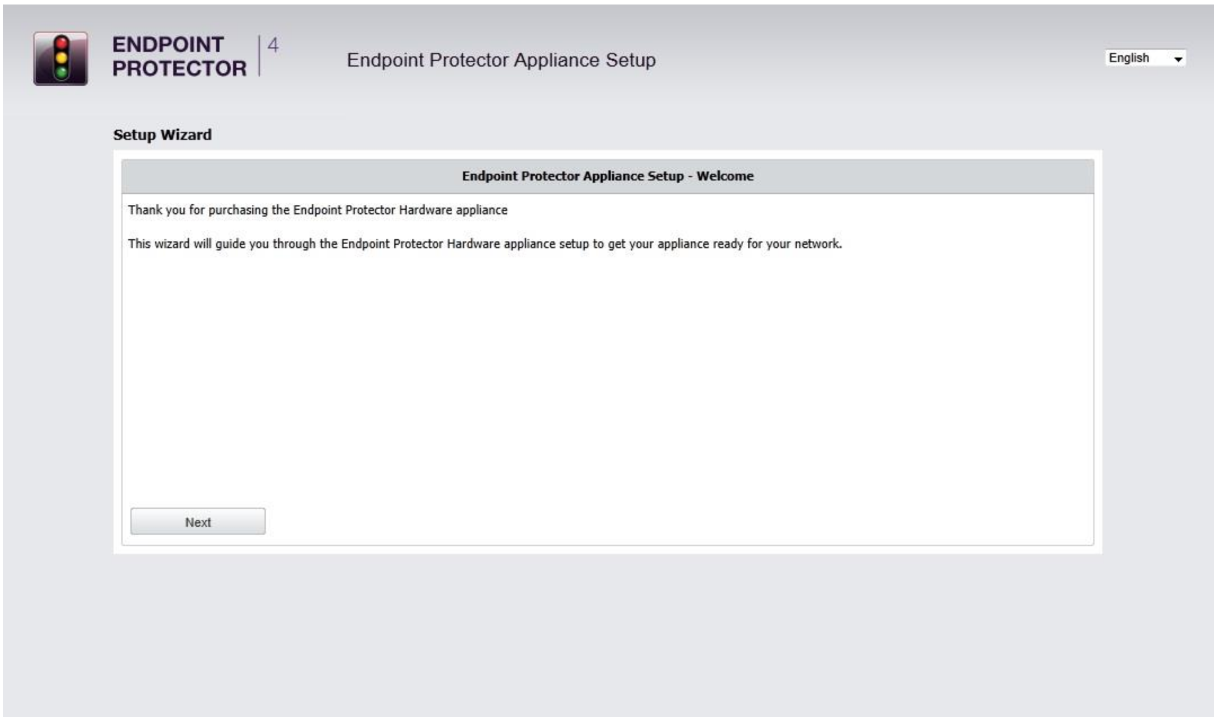
□ Validate settings upon exit

Then access it through your internet browser by typing the following IP

http://111.33.33.111 in the URL bar.

There are two possibilities for configuration of your virtual appliance’s network

This wizard will guide you through the Endpoint Protector Appliance setup to get your Appliance ready for your network.



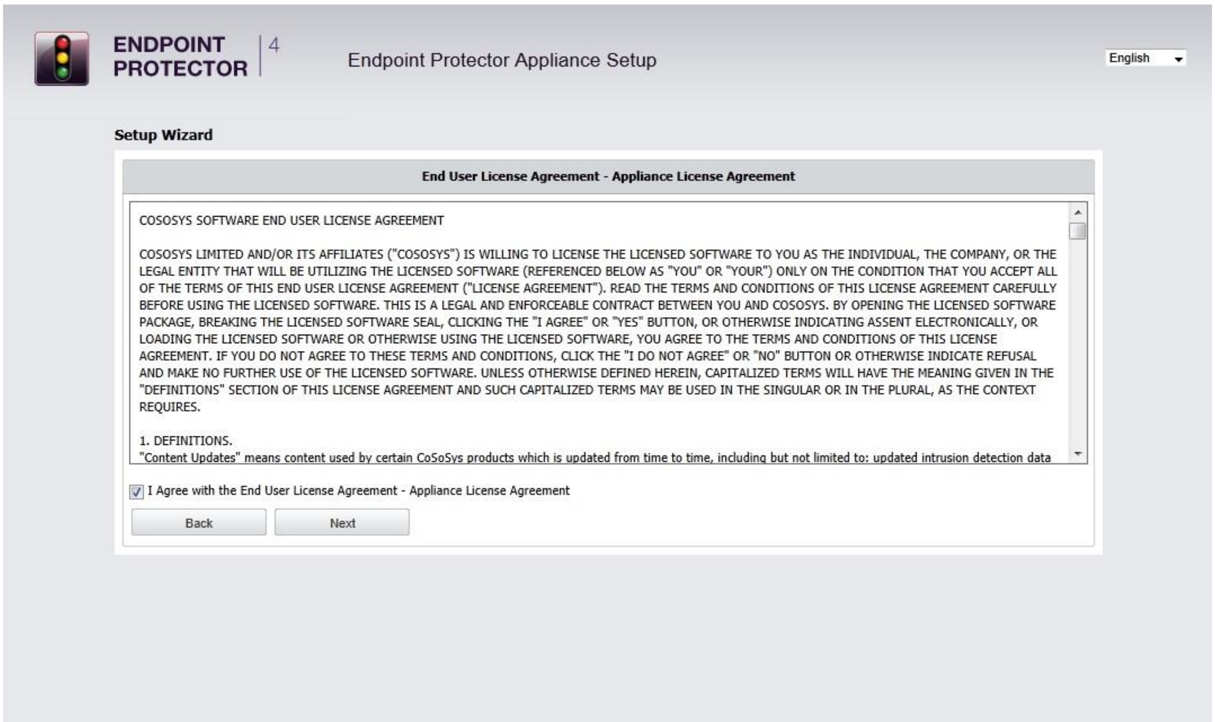
Setup Wizard

Endpoint Protector Appliance Setup - Welcome

Thank you for purchasing the Endpoint Protector Hardware appliance

This wizard will guide you through the Endpoint Protector Hardware appliance setup to get your appliance ready for your network.

5.2.1. End User License Agreement - Appliance License Agreement



Setup Wizard

End User License Agreement - Appliance License Agreement

COSOSYS SOFTWARE END USER LICENSE AGREEMENT

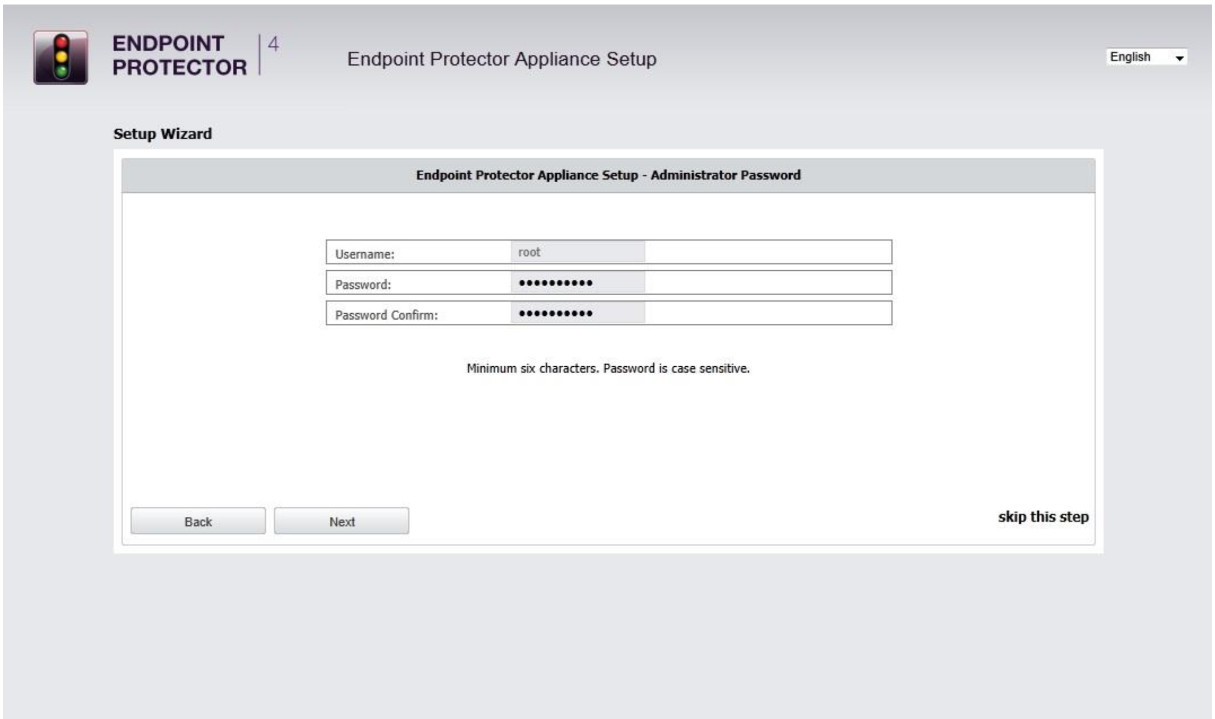
COSOSYS LIMITED AND/OR ITS AFFILIATES ("COSOSYS") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS END USER LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND COSOSYS. BY OPENING THE LICENSED SOFTWARE PACKAGE, BREAKING THE LICENSED SOFTWARE SEAL, CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE LICENSED SOFTWARE OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE LICENSED SOFTWARE. UNLESS OTHERWISE DEFINED HEREIN, CAPITALIZED TERMS WILL HAVE THE MEANING GIVEN IN THE "DEFINITIONS" SECTION OF THIS LICENSE AGREEMENT AND SUCH CAPITALIZED TERMS MAY BE USED IN THE SINGULAR OR IN THE PLURAL, AS THE CONTEXT REQUIRES.

1. DEFINITIONS.
"Content Updates" means content used by certain CoSoSys products which is updated from time to time, including but not limited to: updated intrusion detection data

☑ I Agree with the End User License Agreement - Appliance License Agreement

To continue with the setup process, please review the End User License Agreement – Appliance License Agreement.

5.2.2. Define your Appliance Administrator Password



ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector Appliance Setup - Administrator Password

Username: root
Password: ••••••••••
Password Confirm: ••••••••••

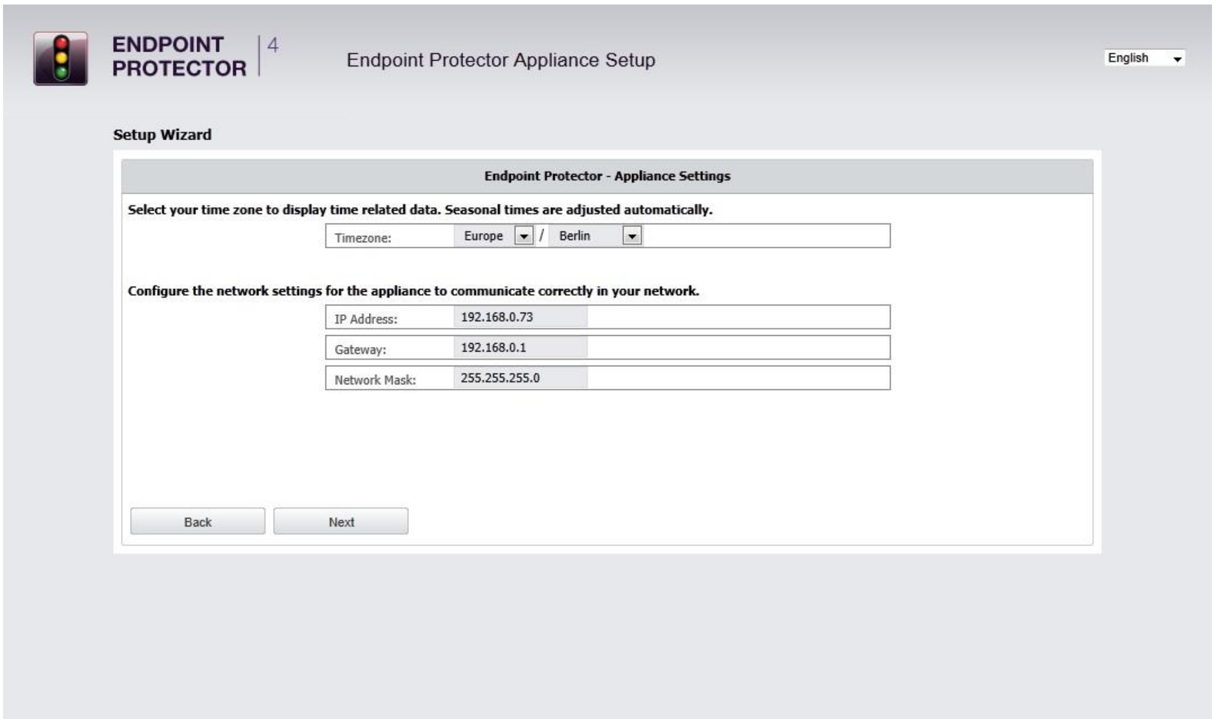
Minimum six characters. Password is case sensitive.

Enter and confirm your administrator password. The minimum length is 6 characters and the password is case sensitive.

The default administrator user name is root.

After entering and confirming your administrator password click next to continue.

5.2.3. Set Time Zone


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector - Appliance Settings
Back
Next

Select your time zone to display time related data. Seasonal times are adjusted automatically.

Timezone: Europe / Berlin

Configure the network settings for the appliance to communicate correctly in your network.

IP Address: 192.168.0.73

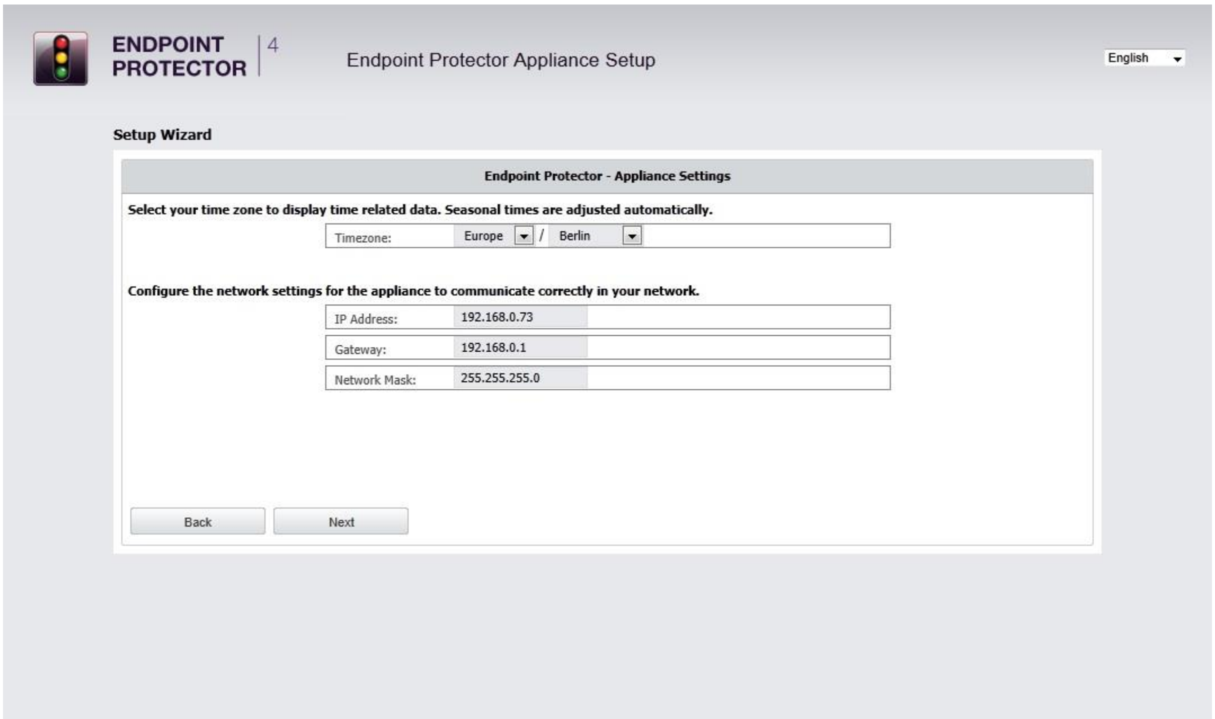
Gateway: 192.168.0.1

Network Mask: 255.255.255.0

Select your time zone to correctly display time related data. Seasonal time changes are adjusted automatically.

You can change this setting later from Appliance menu, by selecting System Maintenance option.

5.2.4. Set Appliance Network IP Address



Endpoint Protector Appliance Setup

Setup Wizard

Endpoint Protector - Appliance Settings

Select your time zone to display time related data. Seasonal times are adjusted automatically.

Timezone: Europe / Berlin

Configure the network settings for the appliance to communicate correctly in your network.

IP Address: 192.168.0.73

Gateway: 192.168.0.1

Network Mask: 255.255.255.0

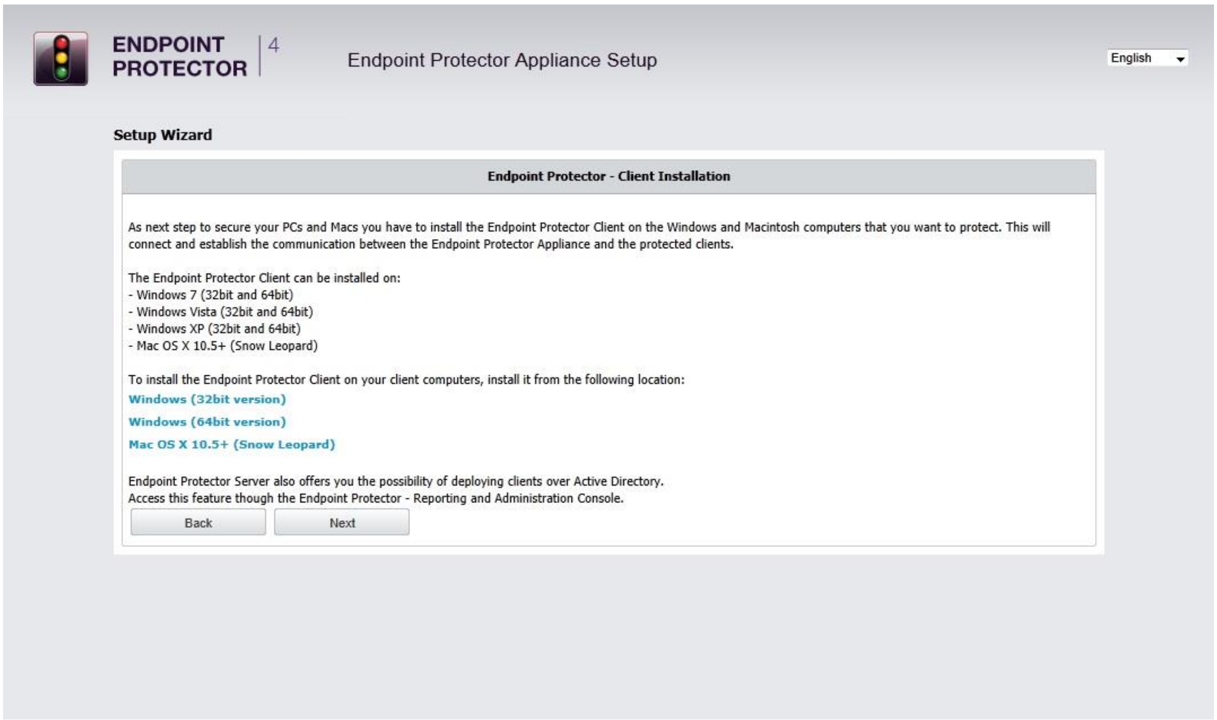
Provide an IP address for your appliance under which it will be reachable in your network. The default IP Address assigned to the Endpoint Protector Appliance in your network is 192.168.0.201. If this IP Address is not assigned in your network this setting does not require a change.

A static IP for the Endpoint Protector Appliance is required for a stable and functional communication between the Appliance and the protected clients. Therefore DHCP is not offered since the IP Address of the Appliance must be a static one.

Please provide also Gateway, Network Mask, Network and Broadcast settings if default values require to be changed.

You can change this setting later from Appliance menu, by selecting System Maintenance option.

5.2.5. Endpoint Protector Client – Automatic Repackaging



Endpoint Protector - Client Installation

As next step to secure your PCs and Macs you have to install the Endpoint Protector Client on the Windows and Macintosh computers that you want to protect. This will connect and establish the communication between the Endpoint Protector Appliance and the protected clients.

The Endpoint Protector Client can be installed on:
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)

To install the Endpoint Protector Client on your client computers, install it from the following location:
Windows (32bit version)
Windows (64bit version)
Mac OS X 10.5+ (Snow Leopard)

Endpoint Protector Server also offers you the possibility of deploying clients over Active Directory.
Access this feature though the Endpoint Protector - Reporting and Administration Console.

After setting the Appliance server static IP Address, the installation files for the Endpoint Protector client have been automatically repackaged. Your server IP Address has been added to the Client package.

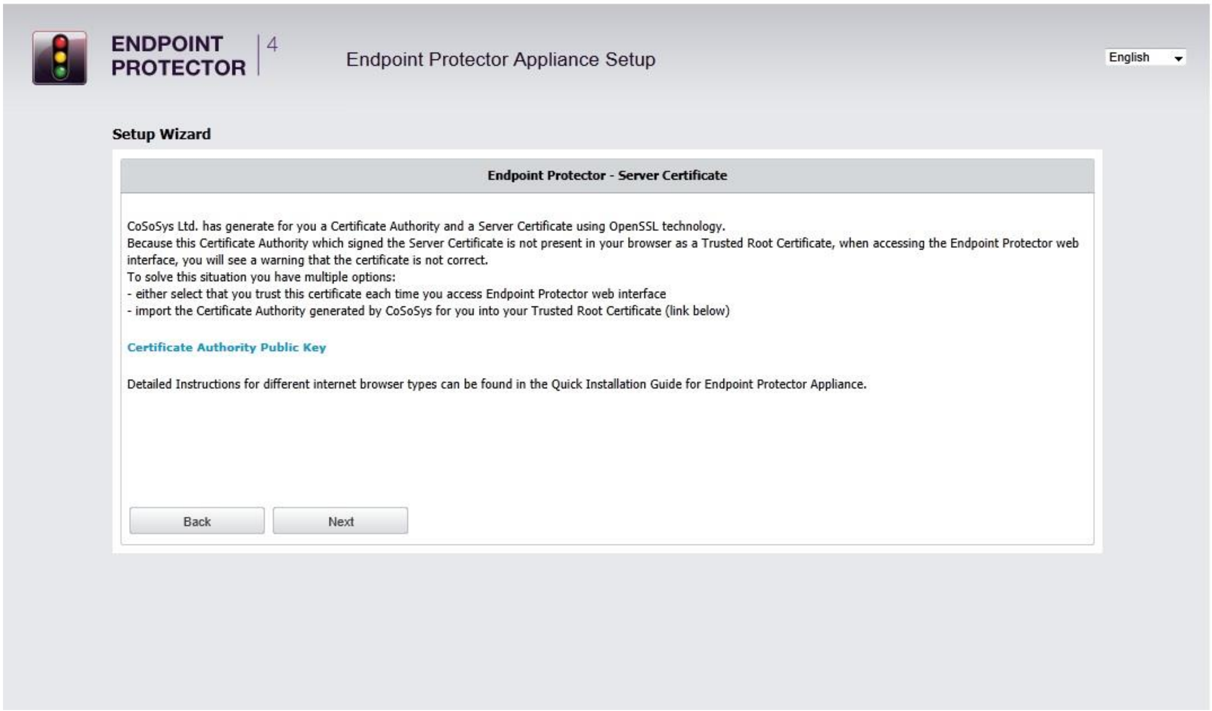
5.2.6. Appliance Server Certificate

After you have set a static IP address the Endpoint Protector Appliance has created for your Appliance a Certificate Authority using OpenSSL technology. This will enable you to connect securely over your network to the Web-based administration interface of the appliance and it also provides a secure and encrypted communication between the Appliance and the protected Client computers.

We recommend you to add the Root Certificate of the Endpoint Protector Appliance to your Trusted Root Certificates store of your internet browser.

If not, then when prompted by your internet browser, please accept the invalid certificate.

Detailed instructions on how to add the Root Certificate for different Internet browser types can be found in Chapter 8. "Installing Root Certificate to your Internet Browser".


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector - Server Certificate

CoSoSys Ltd. has generate for you a Certificate Authority and a Server Certificate using OpenSSL technology.
Because this Certificate Authority which signed the Server Certificate is not present in your browser as a Trusted Root Certificate, when accessing the Endpoint Protector web interface, you will see a warning that the certificate is not correct.
To solve this situation you have multiple options:
- either select that you trust this certificate each time you access Endpoint Protector web interface
- import the Certificate Authority generated by CoSoSys for you into your Trusted Root Certificate (link below)

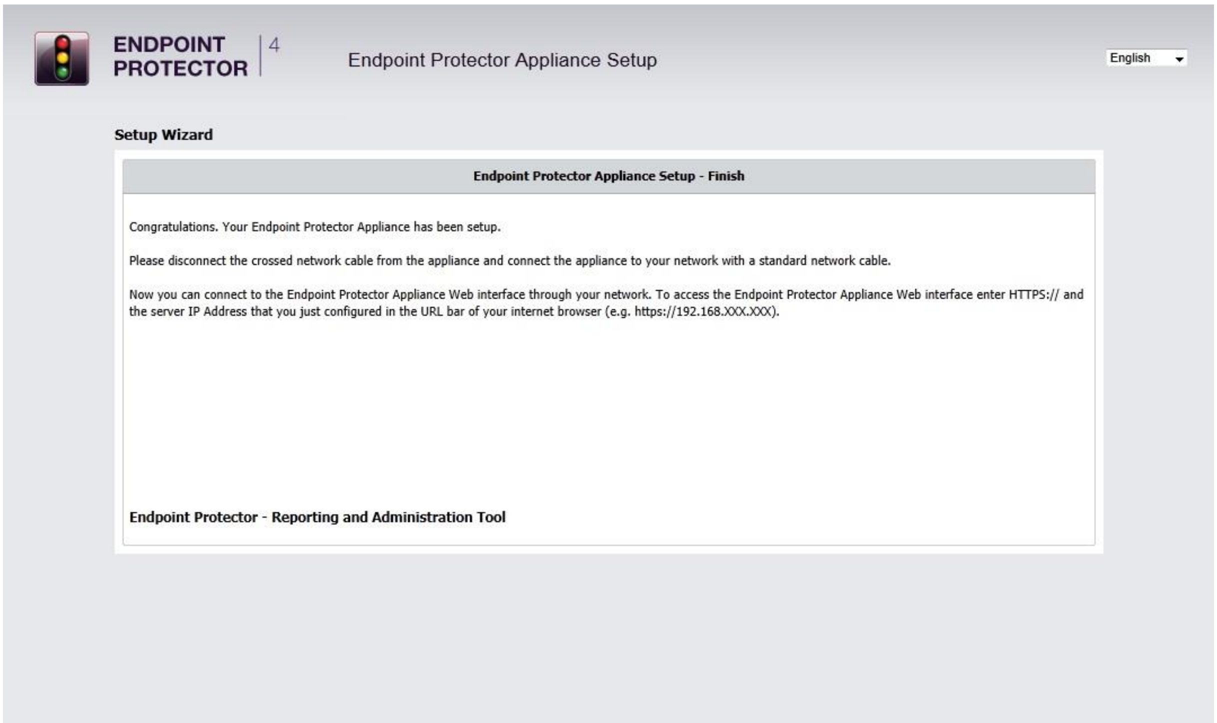
Certificate Authority Public Key

Detailed Instructions for different internet browser types can be found in the Quick Installation Guide for Endpoint Protector Appliance.

If using Internet Explorer with Enhanced Security Configuration enabled, you need to add Endpoint Protector site to the browser's trusted Sites list.

5.2.7. Finishing the Endpoint Protector Appliance Setup

Your Endpoint Protector Appliance has been setup.



Setup Wizard

Endpoint Protector Appliance Setup - Finish

Congratulations. Your Endpoint Protector Appliance has been setup.

Please disconnect the crossed network cable from the appliance and connect the appliance to your network with a standard network cable.

Now you can connect to the Endpoint Protector Appliance Web interface through your network. To access the Endpoint Protector Appliance Web interface enter HTTPS:// and the server IP Address that you just configured in the URL bar of your internet browser (e.g. https://192.168.XXX.XXX).

Endpoint Protector - Reporting and Administration Tool

6. Endpoint Protector Appliance Configuration

6.2 Connect Appliance to Network

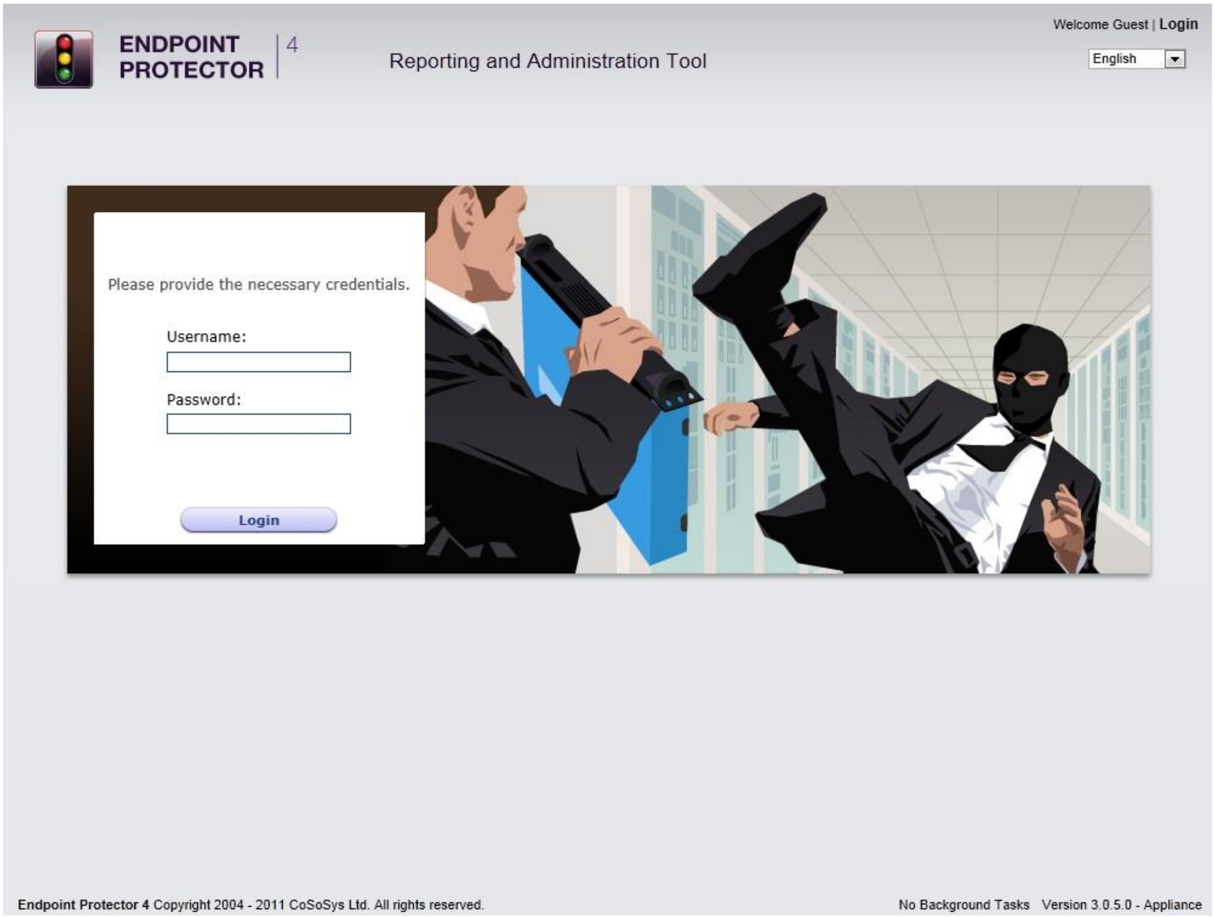
After assigning in the Setup process a static IP address for the Endpoint Protector Appliance, you can connect the Appliance to your network.

6.3 Access to the Appliance Interface through your Network

Now you can connect to the Endpoint Protector Appliance Web interface through your network. To access the Appliance connect to the static IP address that you have defined before through https. Example default: https://192.168.0.201.

6.4 Login to Endpoint Protector

Please enter your user name and password that you have defined for the Endpoint Protector installation in the previous setup step.

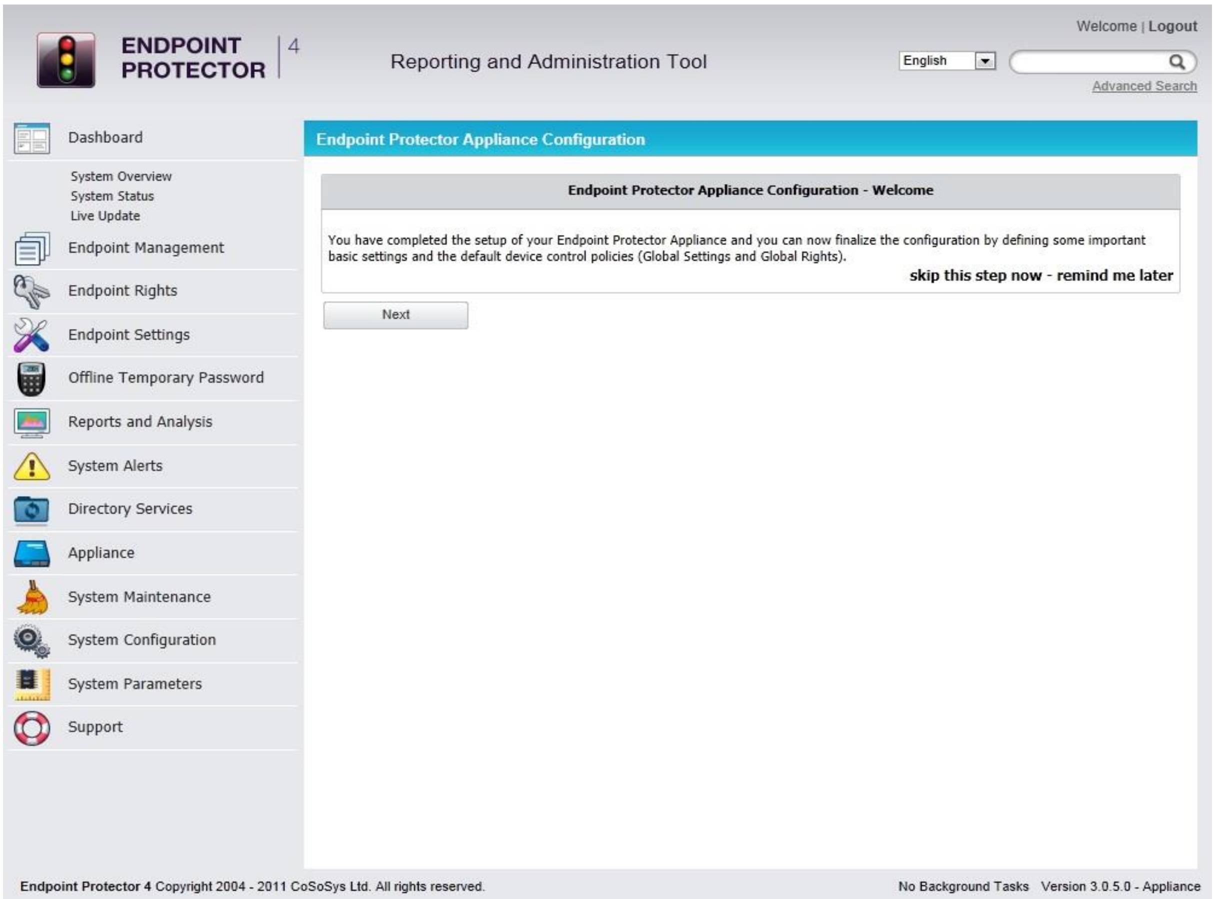

ENDPOINT PROTECTOR | 4
Reporting and Administration Tool
Welcome Guest | Login
English
Please provide the necessary credentials.
Username:
Password:
Login
Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.
No Background Tasks Version 3.0.5.0 - Appliance

The default username and password for Endpoint Protector 4 Administration and Reporting Tool are:

USERNAME:	root
PASSWORD:	epp2011

6.5 Appliance Configuration Wizard

You have completed the setup of your Endpoint Protector Appliance and you can now finalize the configuration by defining some important basic settings and the default device control policy (Global Settings) by following the steps of the Configuration Wizard.



Endpoint Protector Appliance Configuration

Endpoint Protector Appliance Configuration - Welcome

You have completed the setup of your Endpoint Protector Appliance and you can now finalize the configuration by defining some important basic settings and the default device control policies (Global Settings and Global Rights).

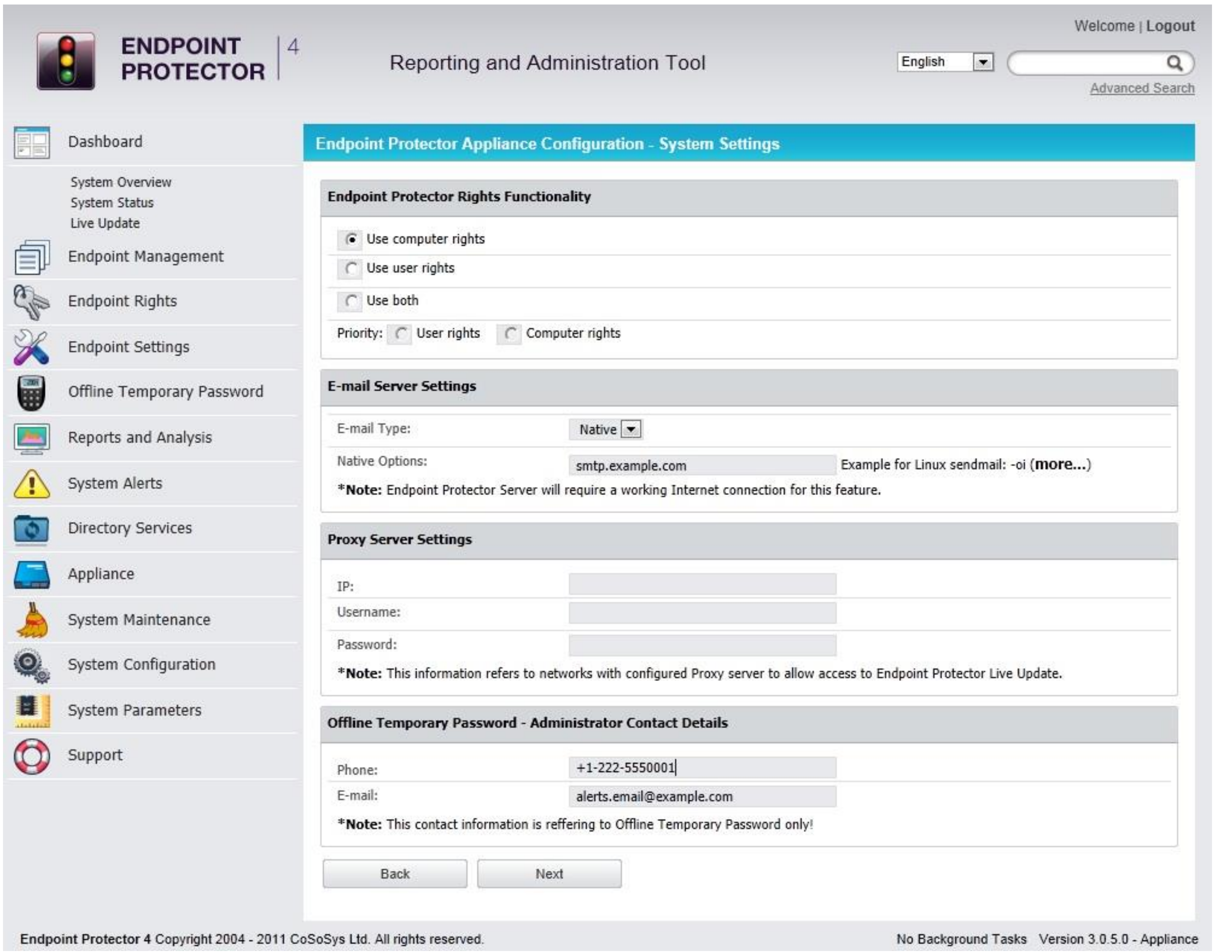
skip this step now - remind me later

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

No Background Tasks Version 3.0.5.0 - Appliance

6.6 Appliance Basic Settings

Please provide here all required settings for the Appliance to function properly. Choose what later defined right will have priority, what E-mail address is used to receive System Alerts and what contact information is shown to users in the Offline Temporary Password system tray dialog.



Endpoint Protector Appliance Configuration - System Settings

Endpoint Protector Rights Functionality

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

E-mail Server Settings

E-mail Type: Native
Native Options: smtp.example.com Example for Linux sendmail: -oi (more...)
***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

Proxy Server Settings

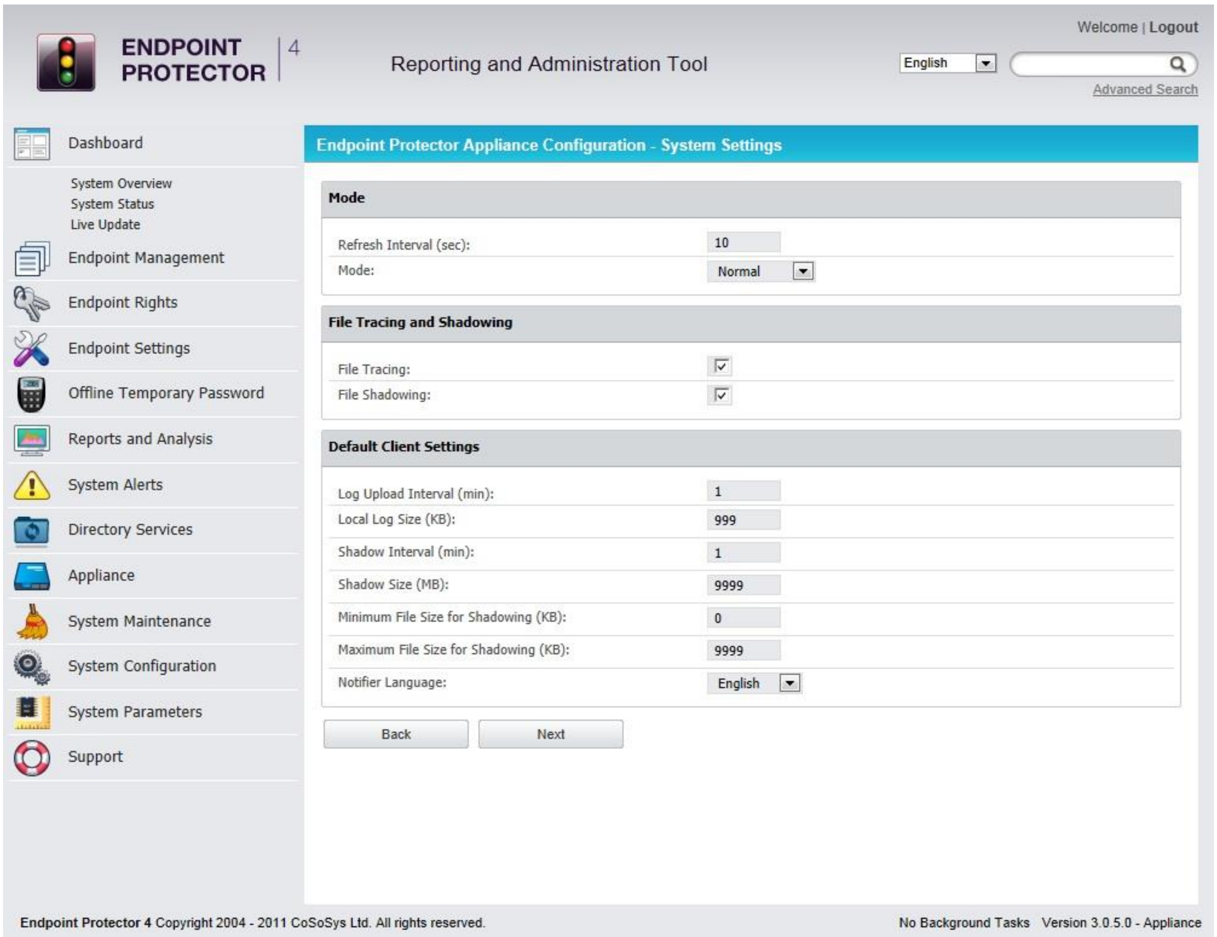
IP:
Username:
Password:
***Note:** This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.

Offline Temporary Password - Administrator Contact Details

Phone: +1-222-5550001
E-mail: alerts.email@example.com
***Note:** This contact information is reffering to Offline Temporary Password only!

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.
No Background Tasks Version 3.0.5.0 - Appliance

Additionally, you can select the Refresh Interval, activate/deactivate features such as File Tracing and File Shadowing and set default parameters for the generated logs.



Endpoint Protector Appliance Configuration - System Settings

Mode

Refresh Interval (sec):	10
Mode:	Normal

File Tracing and Shadowing

File Tracing:	☑
File Shadowing:	☑

Default Client Settings

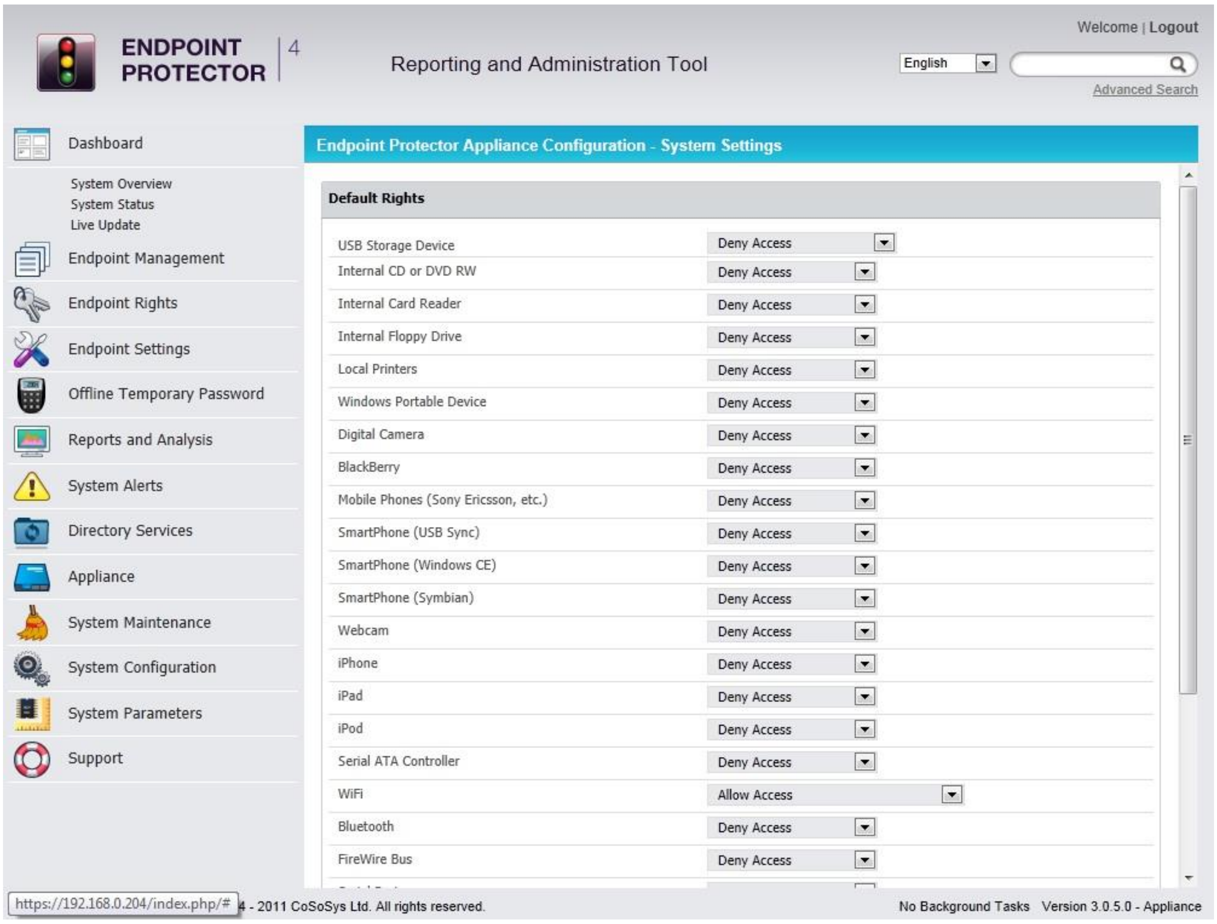
Log Upload Interval (min):	1
Local Log Size (KB):	999
Shadow Interval (min):	1
Shadow Size (MB):	9999
Minimum File Size for Shadowing (KB):	0
Maximum File Size for Shadowing (KB):	9999
Notifier Language:	English

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

6.7 Appliance Default Policies

In this step you can define the default Appliance Policy for portable device use.

This Policy (Global Settings) can be later changed.



Endpoint Protector Appliance Configuration - System Settings

Default Rights

USB Storage Device	Deny Access
Internal CD or DVD RW	Deny Access
Internal Card Reader	Deny Access
Internal Floppy Drive	Deny Access
Local Printers	Deny Access
Windows Portable Device	Deny Access
Digital Camera	Deny Access
BlackBerry	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access
SmartPhone (USB Sync)	Deny Access
SmartPhone (Windows CE)	Deny Access
SmartPhone (Symbian)	Deny Access
Webcam	Deny Access
iPhone	Deny Access
iPad	Deny Access
iPod	Deny Access
Serial ATA Controller	Deny Access
WiFi	Allow Access
Bluetooth	Deny Access
FireWire Bus	Deny Access

6.8 Finishing the Endpoint Protector Appliance Configuration Wizard

You have now completed the setup and configuration of the Endpoint Protector Appliance.

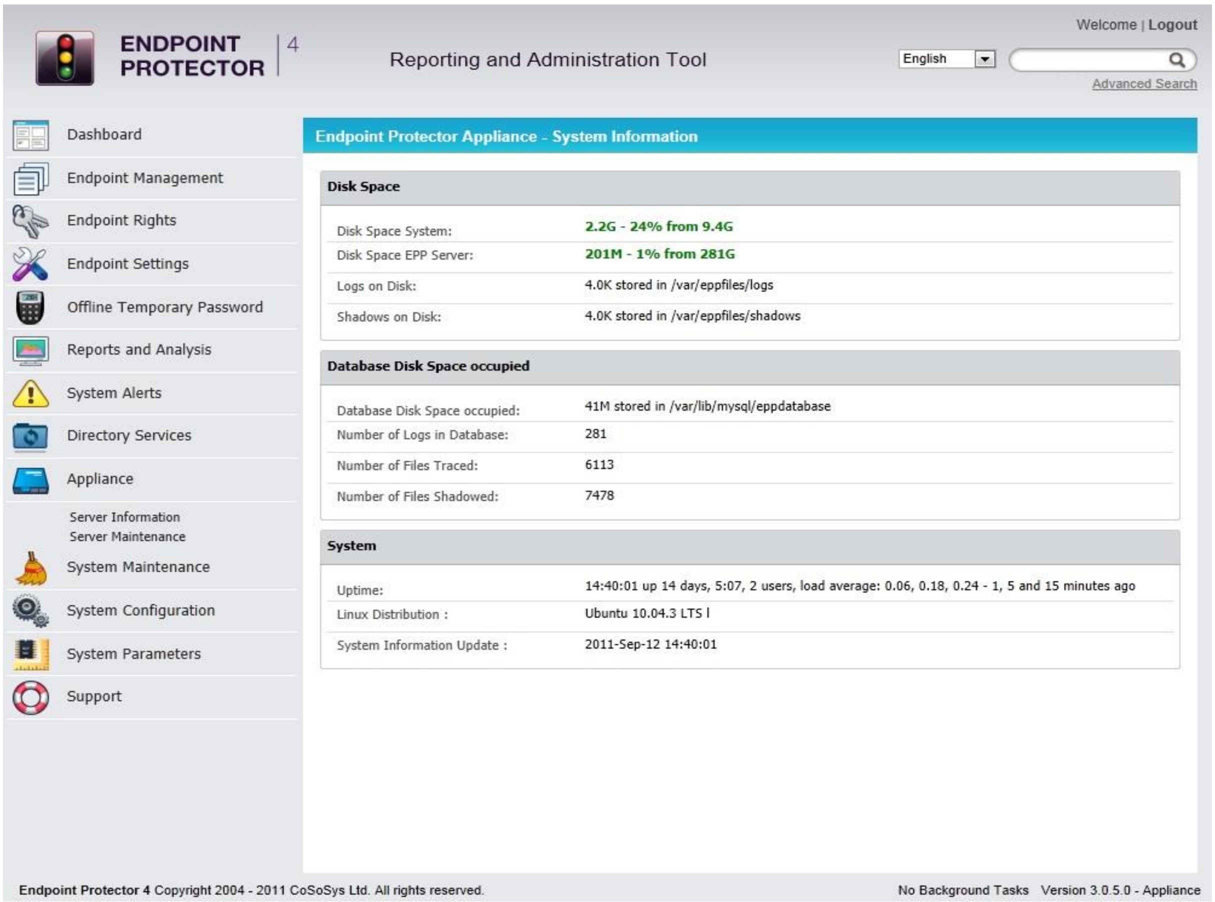
Now we recommend you to deploy the Endpoint Protector client to the Windows and Macintosh computers that you want to protect.

7. Appliance Settings and Maintenance

The Endpoint Protector Appliance Settings can be accessed through the main menu item Appliance in the Administration and Reporting Tool.

7.2 Server Information

Here you can view information about the Server current state.



Endpoint Protector Appliance - System Information

Disk Space

Disk Space System:	2.2G - 24% from 9.4G
Disk Space EPP Server:	201M - 1% from 281G
Logs on Disk:	4.0K stored in /var/eppfiles/logs
Shadows on Disk:	4.0K stored in /var/eppfiles/shadows

Database Disk Space occupied

Database Disk Space occupied:	41M stored in /var/lib/mysql/eppdatabase
Number of Logs in Database:	281
Number of Files Traced:	6113
Number of Files Shadowed:	7478

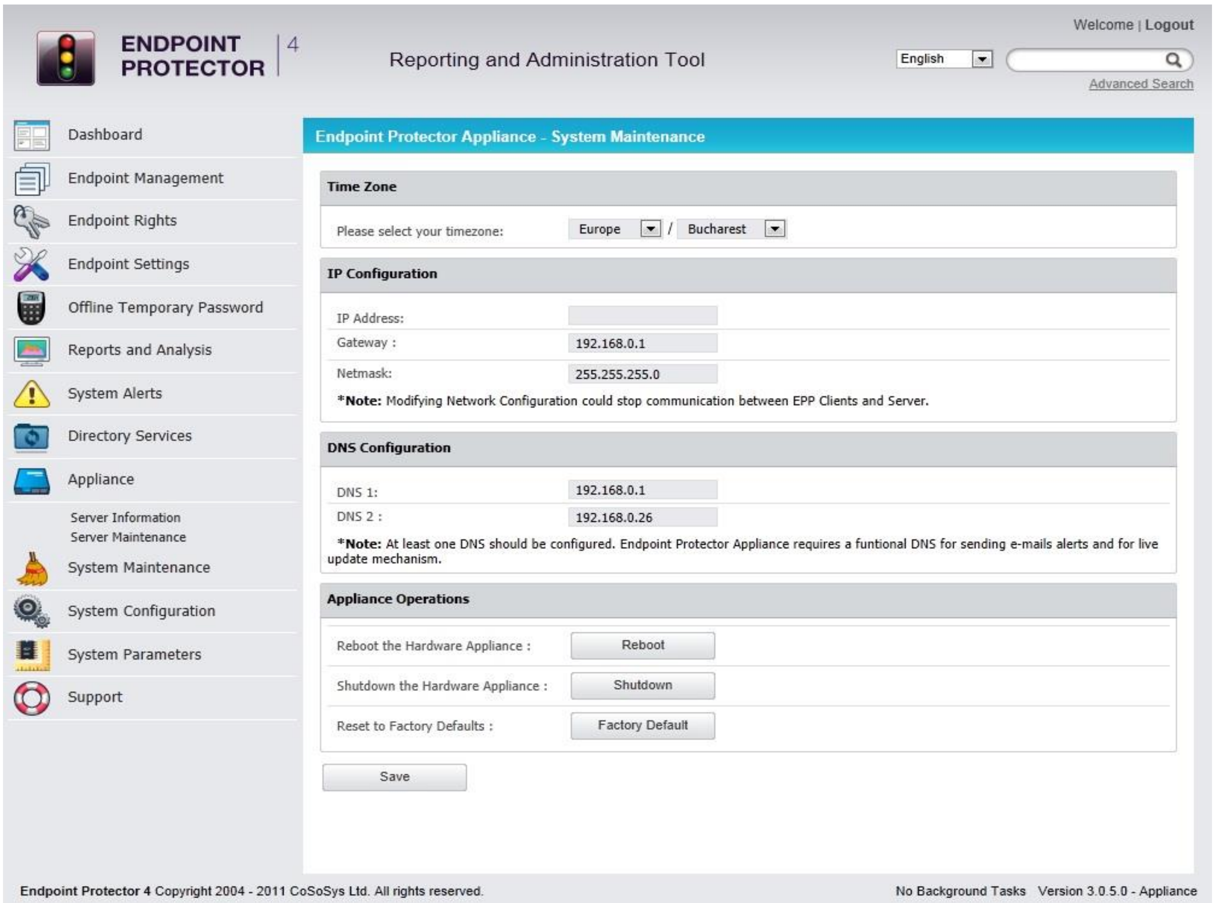
System

Uptime:	14:40:01 up 14 days, 5:07, 2 users, load average: 0.06, 0.18, 0.24 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 10.04.3 LTS l
System Information Update :	2011-Sep-12 14:40:01

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

No Background Tasks Version 3.0.5.0 - Appliance

7.3 Server Maintenance



Endpoint Protector Appliance - System Maintenance

Time Zone

Please select your timezone: Europe / Bucharest

IP Configuration

IP Address:

Gateway : 192.168.0.1

Netmask: 255.255.255.0

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

DNS Configuration

DNS 1: 192.168.0.1

DNS 2 : 192.168.0.26

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

Appliance Operations

Reboot the Hardware Appliance :

Shutdown the Hardware Appliance :

Reset to Factory Defaults :

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

No Background Tasks Version 3.0.5.0 - Appliance

7.3.1 Network Settings

Here you can change the network settings for the appliance to communicate correctly in your network. Detailed description can be found in Chapter 5.2.4 “Set Appliance Network IP Address”.

Attention!

Close the Internet browser, then reopen a new instance of your Internet browser. Now try to access the Endpoint Protector Administration and Reporting Tool with the NEW IP address!

7.3.2 Reboot the Appliance

You have the option to reboot the Appliance by clicking the Reboot button.

7.3.3 Reset Appliance to Factory Default

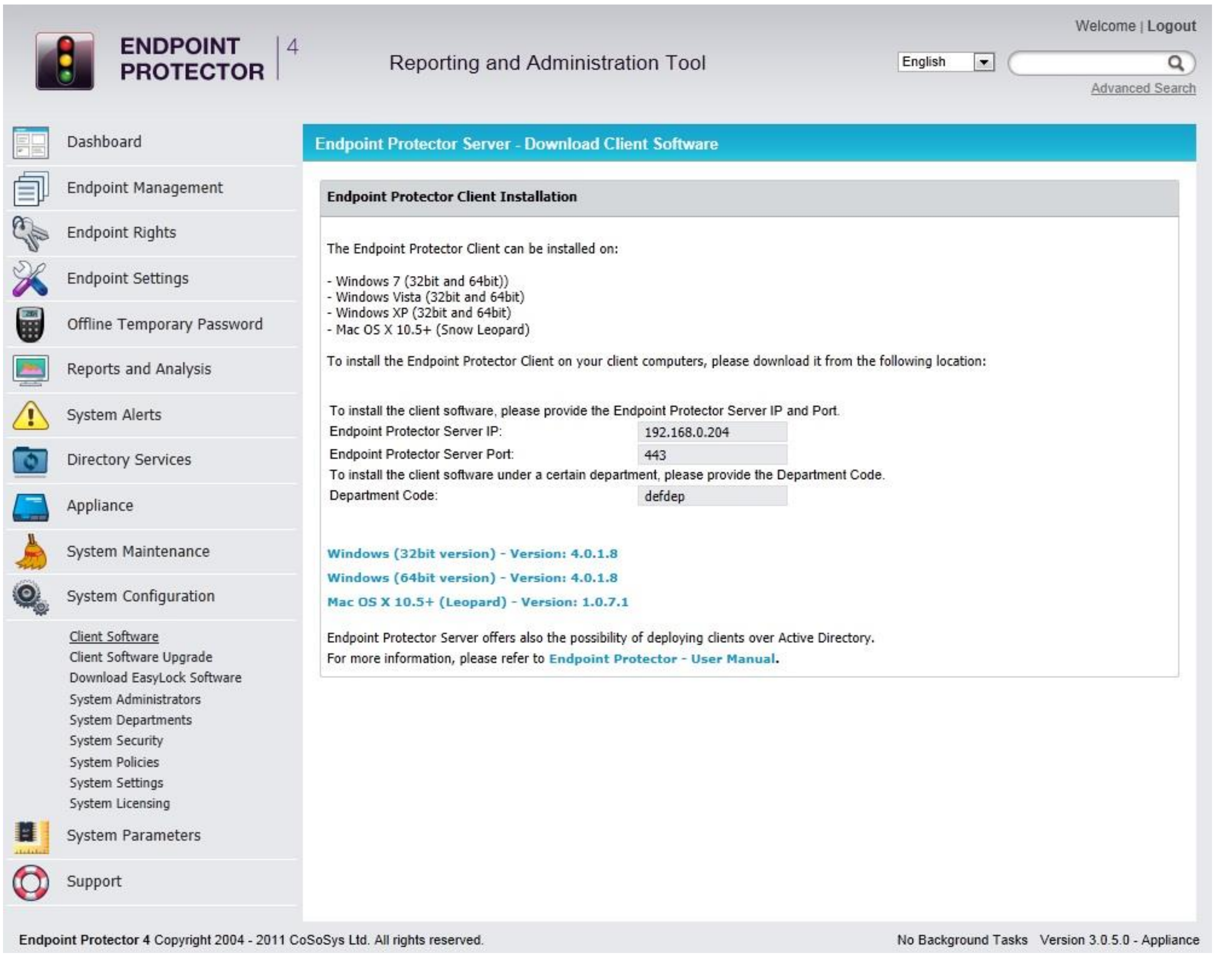
A reset to Factory will erase all settings, policies, certificates and other data on the Appliance. If you reset to factory default, all settings and the communication between Appliance and Endpoint Protector Clients will be interrupted. A complete new installation of all Endpoint Protector Clients will be also required when setting up the Appliance again.

7.4 Endpoint Protector Client Installation for Appliance

As next step to secure your PCs and MACs you have to install the Endpoint Protector Client on the Windows and Macintosh computers that you want to protect. This will connect and establish the communication between the Endpoint Protector Appliance and the protected clients.

To install the Endpoint Protector Client on your client computers, download it directly from the Appliance by entering the Appliance static IP Address in a browser (example http://192.168.0.201). Note: access it through HTTP and not HTTPS.

Note: You need to "Save" the Endpoint Protector Client on a location and then install it from there. Do not run it directly from the browser!



Endpoint Protector Server - Download Client Software

Endpoint Protector Client Installation

The Endpoint Protector Client can be installed on:

- Windows 7 (32bit and 64bit))
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)

To install the Endpoint Protector Client on your client computers, please download it from the following location:

To install the client software, please provide the Endpoint Protector Server IP and Port.

Endpoint Protector Server IP:	192.168.0.204
Endpoint Protector Server Port:	443

To install the client software under a certain department, please provide the Department Code.

Department Code:	defdep

Windows (32bit version) - Version: 4.0.1.8
Windows (64bit version) - Version: 4.0.1.8
Mac OS X 10.5+ (Leopard) - Version: 1.0.7.1

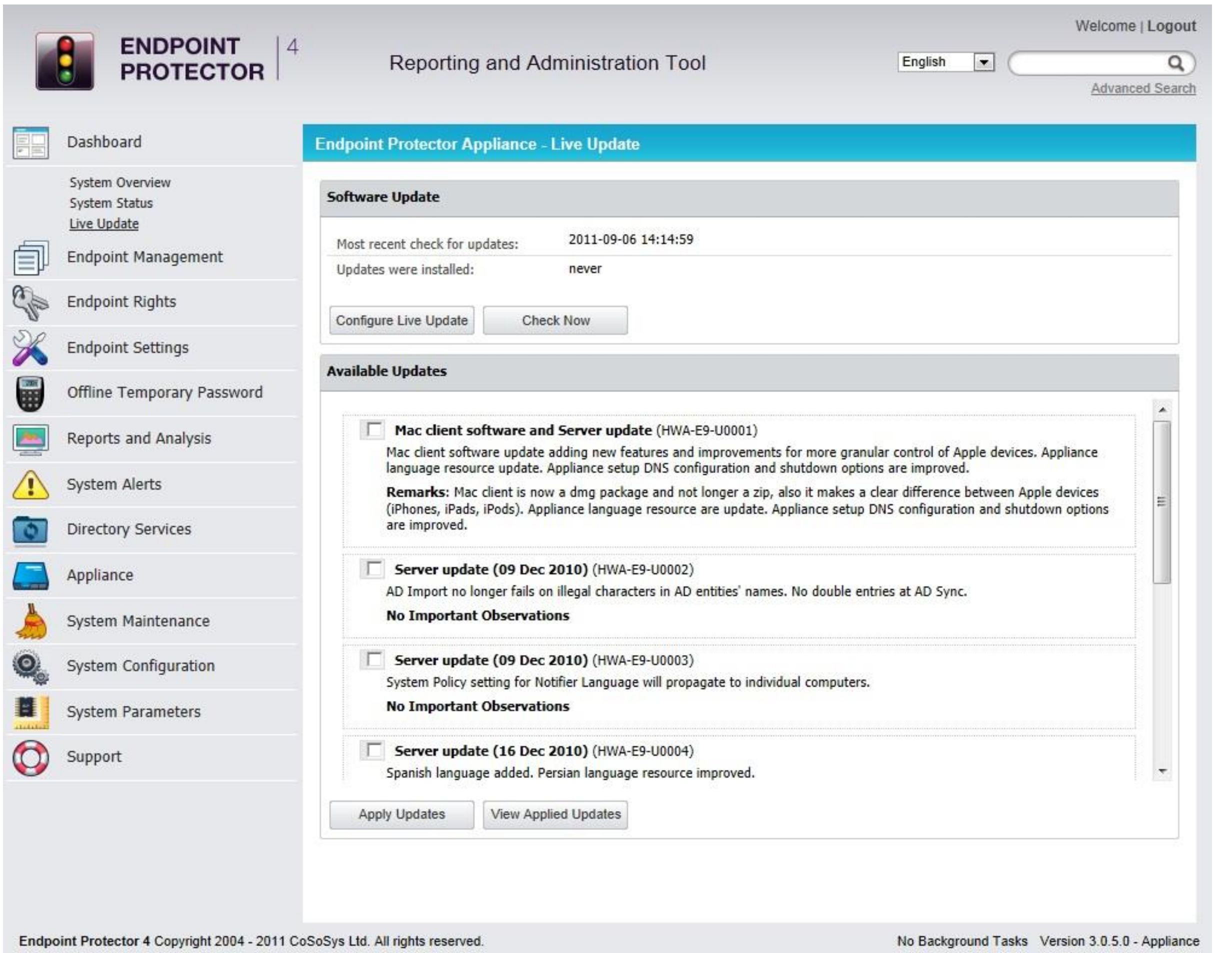
Endpoint Protector Server offers also the possibility of deploying clients over Active Directory.
For more information, please refer to **Endpoint Protector - User Manual.**

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.   No Background Tasks   Version 3.0.5.0 - Appliance

7.5 Appliance Online Live Update

The Live Update feature is checking online if updates for the Appliance and the Endpoint Protector Client software are available.

You can check manually/automatically for updates. If new updates are available they will only be installed when applied by the administrator.



Endpoint Protector Appliance - Live Update

Software Update

Most recent check for updates: 2011-09-06 14:14:59

Updates were installed: never

Available Updates

□ **Mac client software and Server update** (HWA-E9-U0001)
Mac client software update adding new features and improvements for more granular control of Apple devices. Appliance language resource update. Appliance setup DNS configuration and shutdown options are improved.
Remarks: Mac client is now a dmg package and not longer a zip, also it makes a clear difference between Apple devices (iPhones, iPads, iPods). Appliance language resource are update. Appliance setup DNS configuration and shutdown options are improved.

□ **Server update (09 Dec 2010)** (HWA-E9-U0002)
AD Import no longer fails on illegal characters in AD entities' names. No double entries at AD Sync.
No Important Observations

□ **Server update (09 Dec 2010)** (HWA-E9-U0003)
System Policy setting for Notifier Language will propagate to individual computers.
No Important Observations

□ **Server update (16 Dec 2010)** (HWA-E9-U0004)
Spanish language added. Persian language resource improved.

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

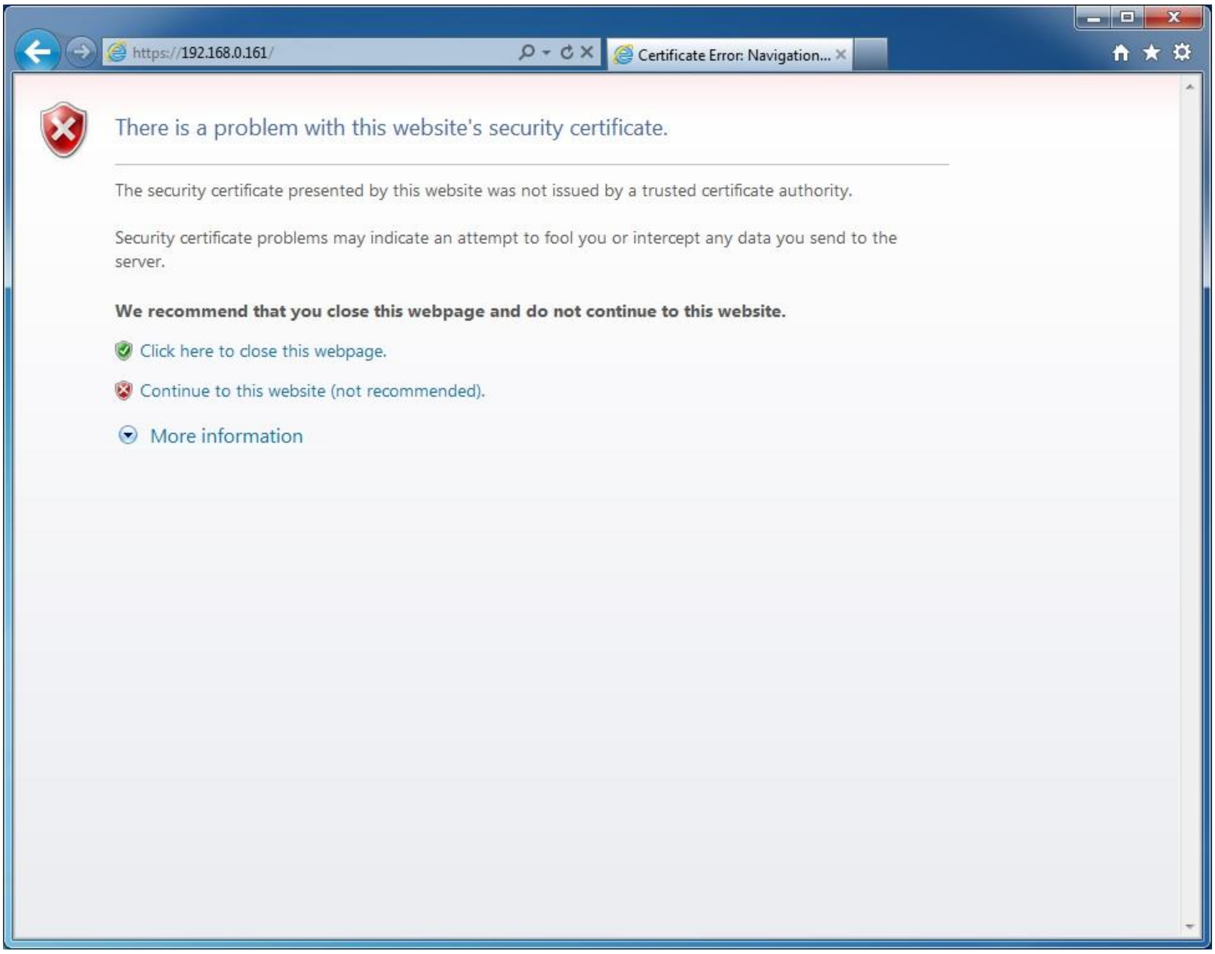
No Background Tasks Version 3.0.5.0 - Appliance

8. Installing Root Certificate to your Internet Browser

8.2 For Microsoft Internet Explorer

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Continue your navigation by clicking 🛡 "Continue to this website (not recommended)".

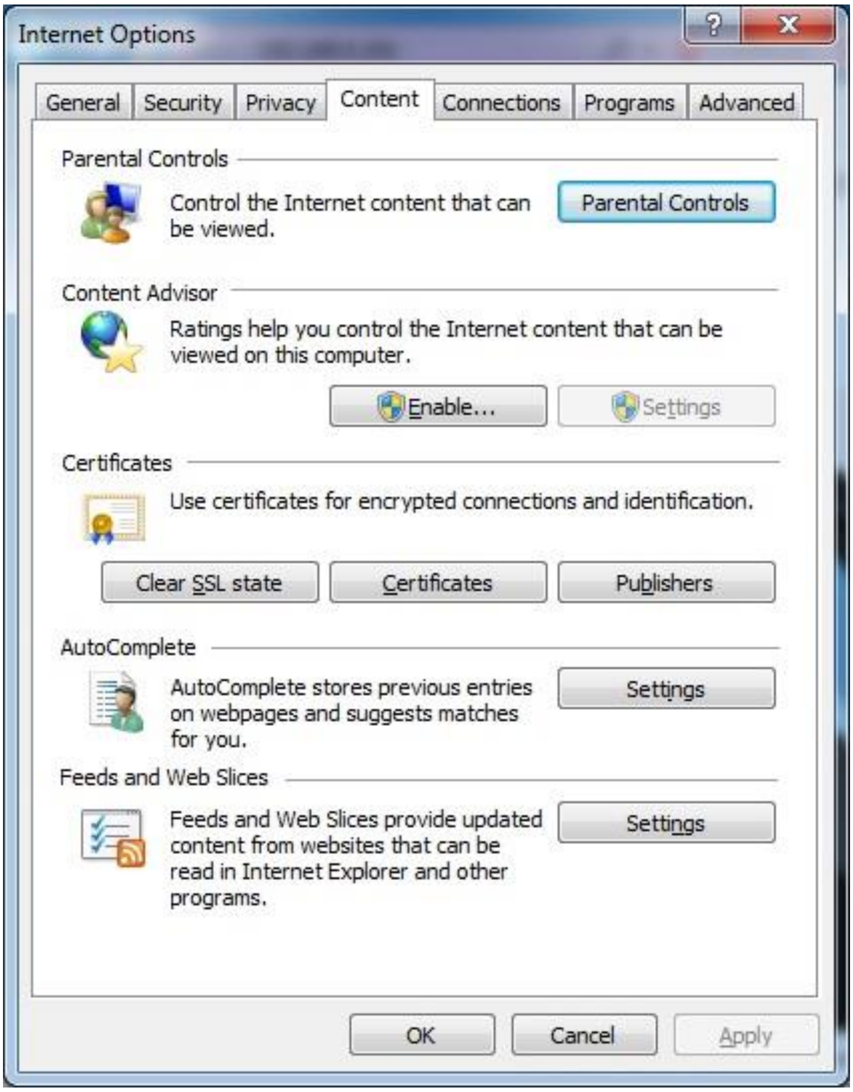
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

Click the Certificate Error button just next to the IE address bar as shown.

By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

Another pop-up Certificate window will appear with three tabs namely "General", "Details" and "Certification Path".

Select the "General" tab and then click "Install Certificate..." button or go to Tools->Internet Options-> Content->Certificates.



Control the Internet content that can be viewed.

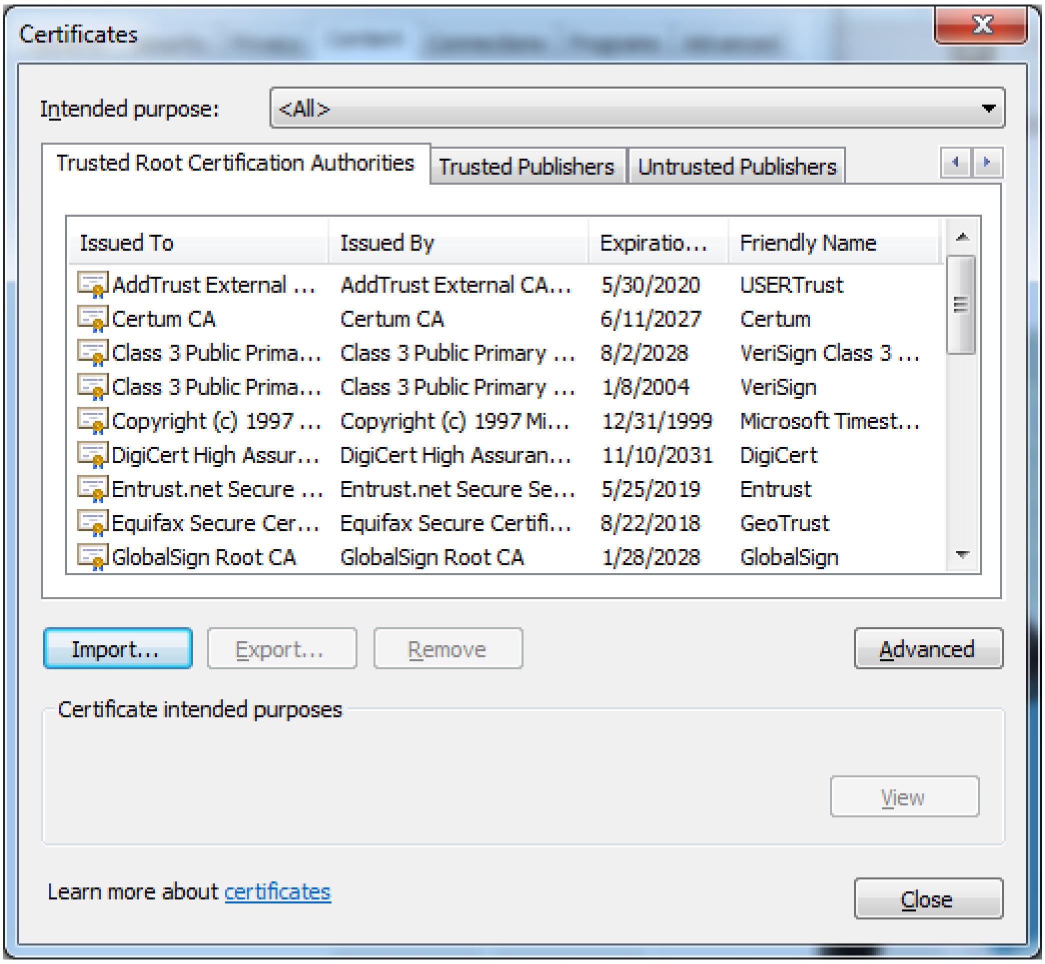
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.



Certificates

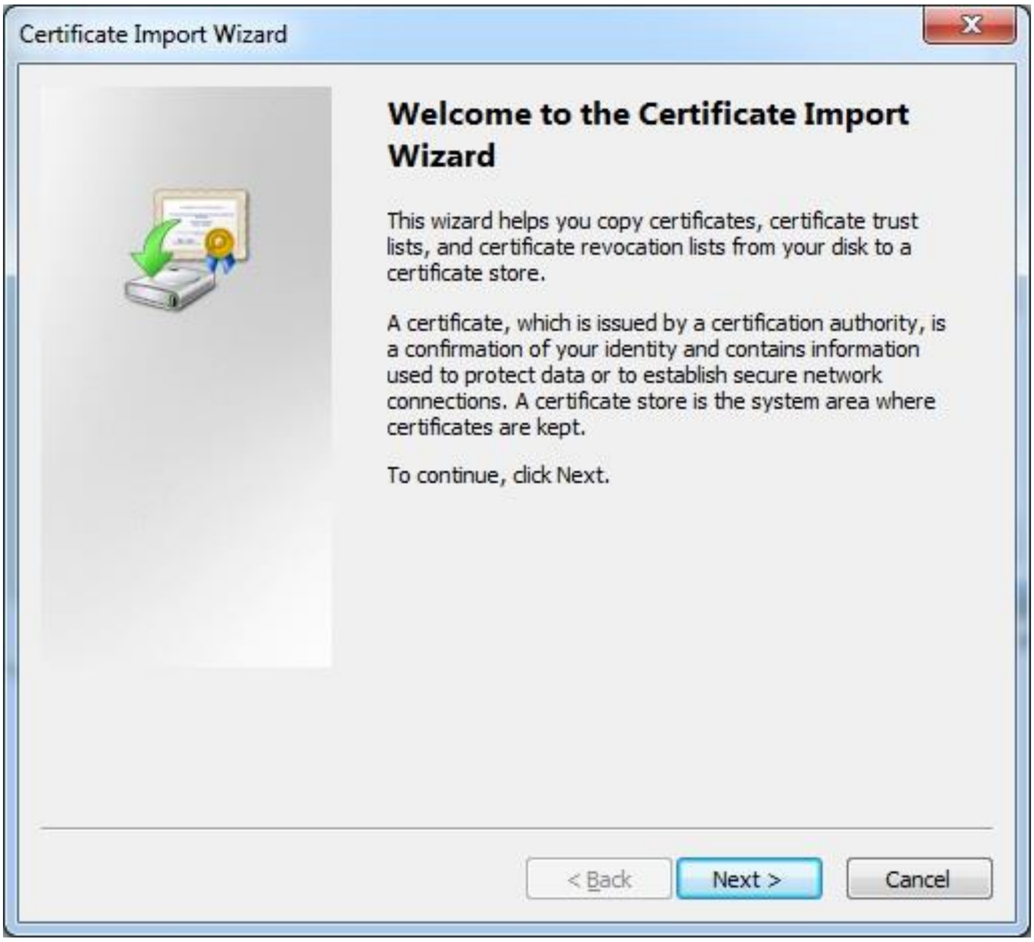
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	5/30/2020	USERTrust
Certum CA	Certum CA	6/11/2027	Certum
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	1/8/2004	VeriSign
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/31/1999	Microsoft Timest...
DigiCert High Assur...	DigiCert High Assuran...	11/10/2031	DigiCert
Entrust.net Secure ...	Entrust.net Secure Se...	5/25/2019	Entrust
Equifax Secure Cer...	Equifax Secure Certifi...	8/22/2018	GeoTrust
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	GlobalSign

Certificate intended purposes

Learn more about certificates

A Welcome to the Certificate Import Wizard pops up. Just click the Next button.



Certificate Import Wizard

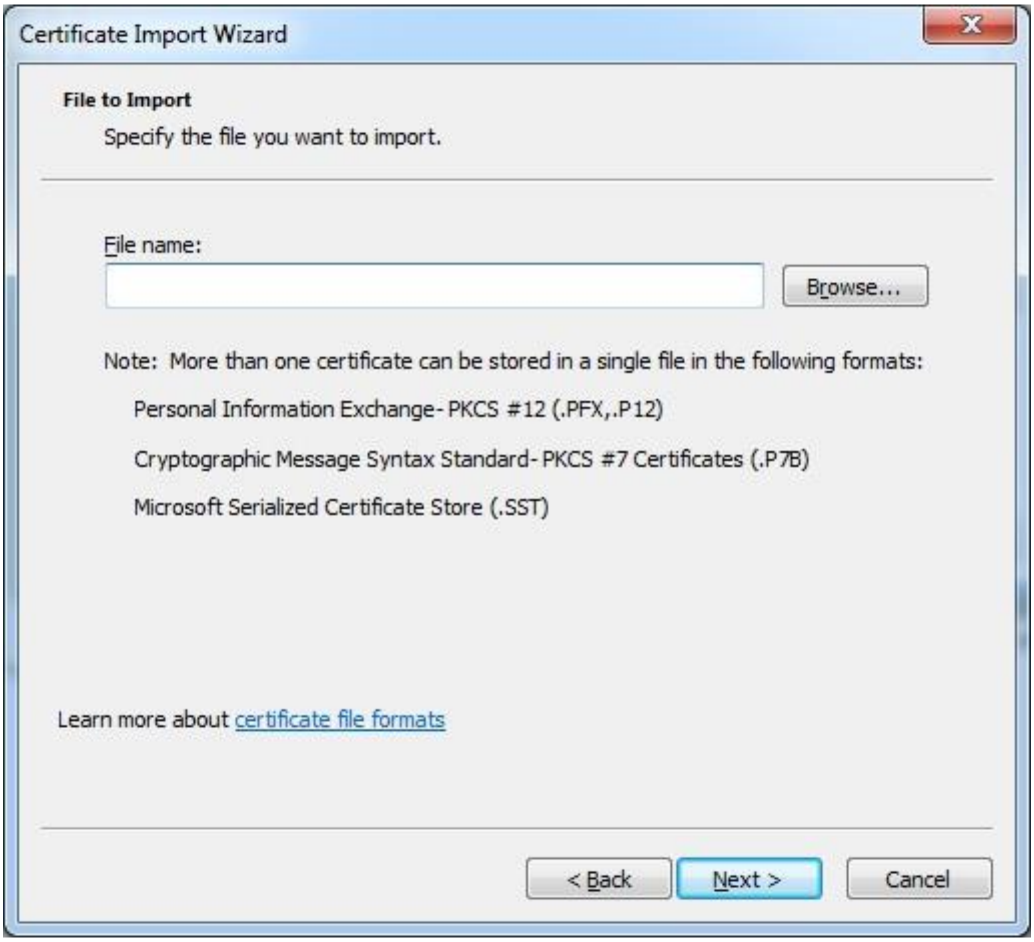
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Browse for the Certificate file you downloaded from the Appliance Setup Wizard ->Appliance Server Certificate.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

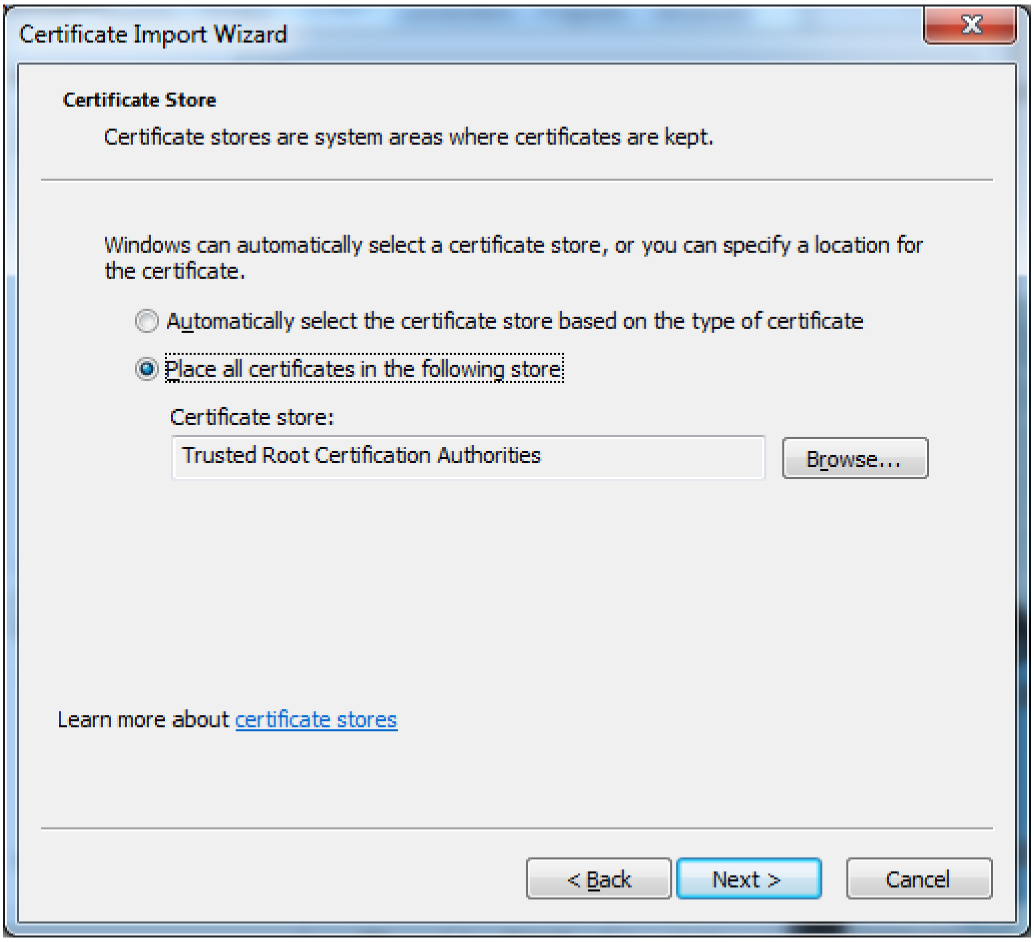
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

In the Certificate Store window, select “Place all certificates in the following store” radio button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

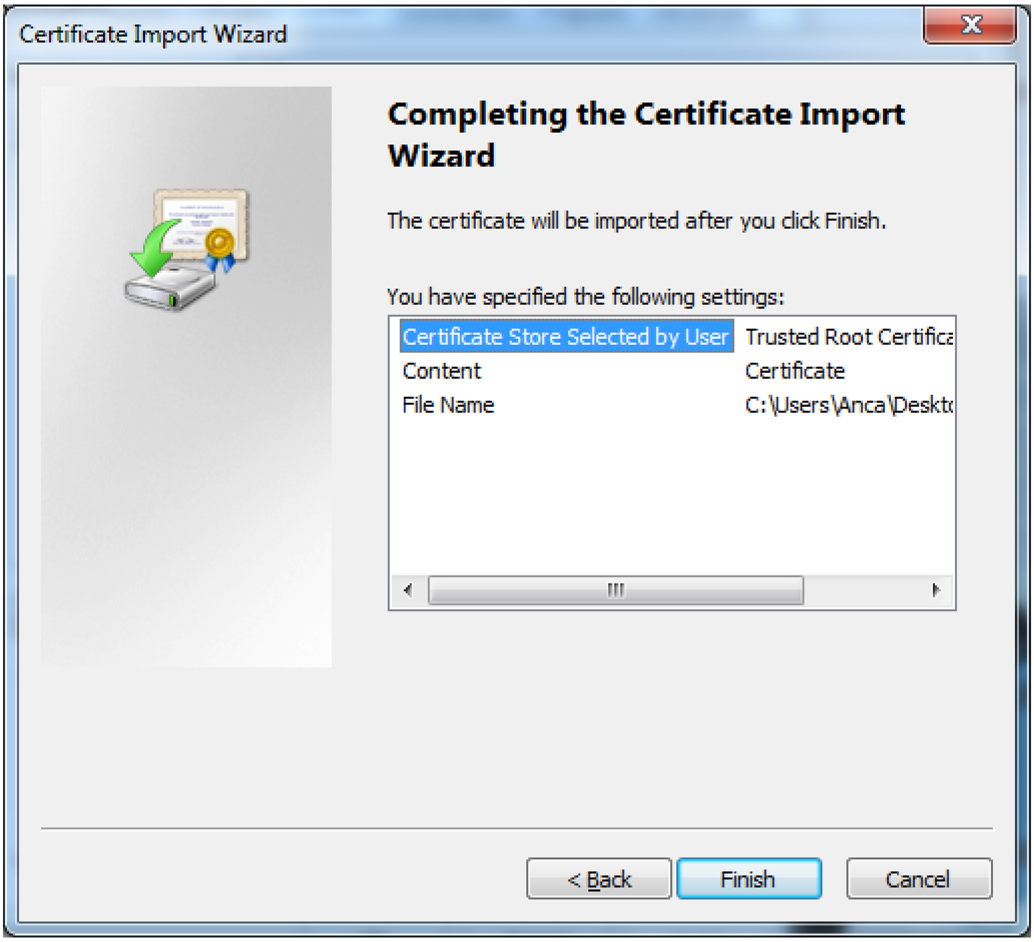
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

Another “Completing the Certificate Import Wizard” pops up. Just click the “Finish” button.



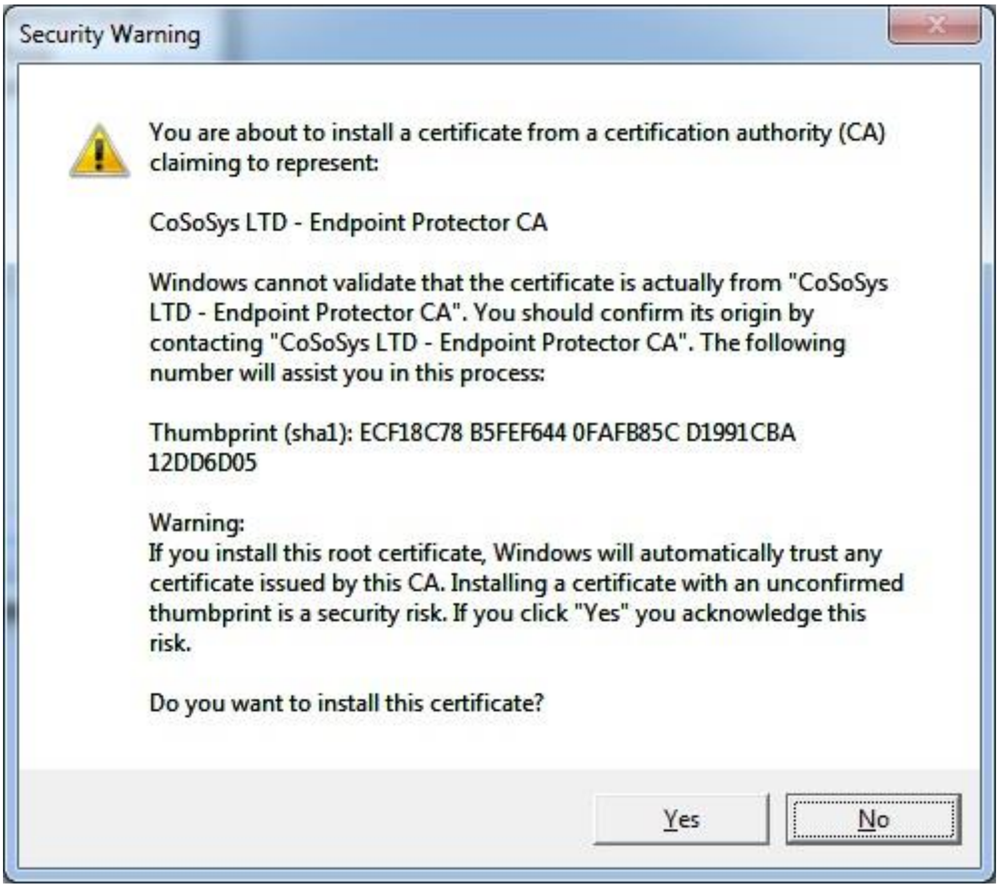
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate
File Name	C:\Users\Anca\Deskt

A Security Warning window pops up. Just click “Yes”.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CoSoSys LTD - Endpoint Protector CA

Windows cannot validate that the certificate is actually from "CoSoSys LTD - Endpoint Protector CA". You should confirm its origin by contacting "CoSoSys LTD - Endpoint Protector CA". The following number will assist you in this process:

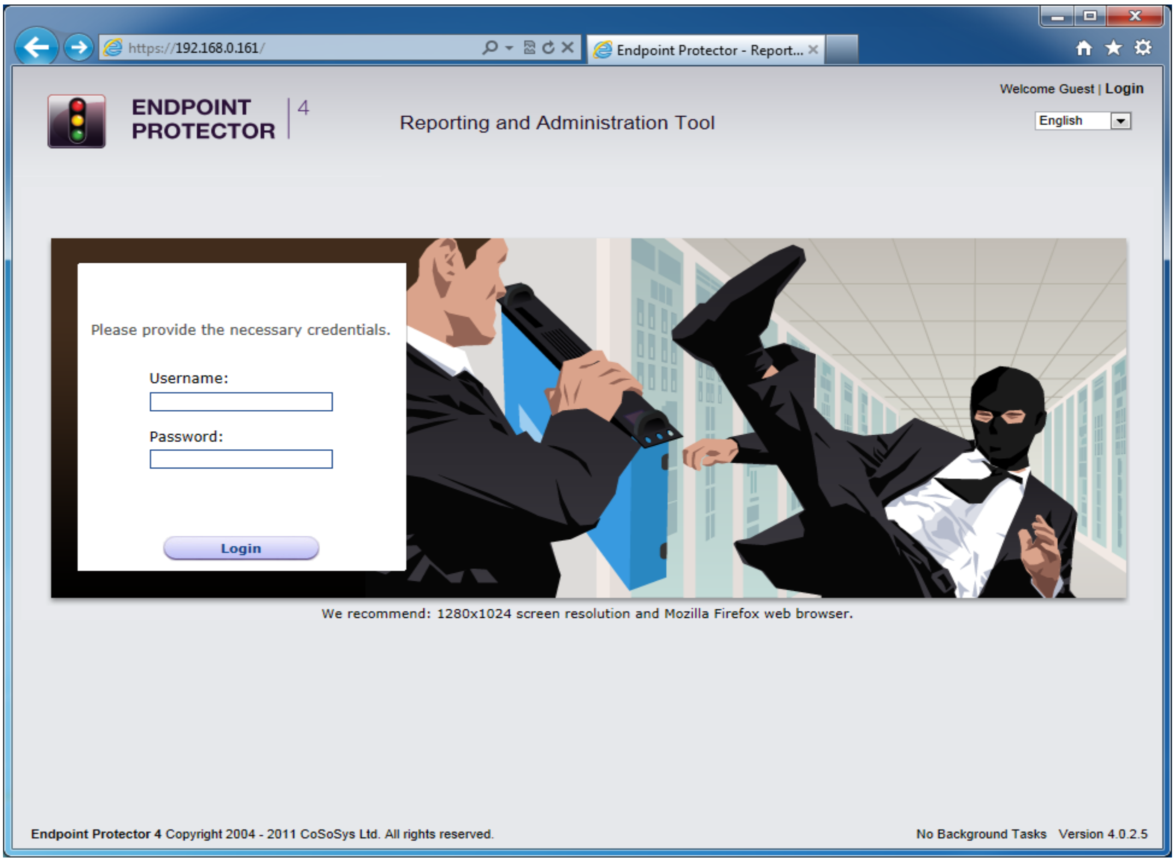
Thumbprint (sha1): ECF18C78 B5FEF644 0FAFB85C D1991CBA 12DD6D05

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

You have now successfully installed the Certificate.

Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



Please provide the necessary credentials.

Username:

Password:

We recommend: 1280x1024 screen resolution and Mozilla Firefox web browser.

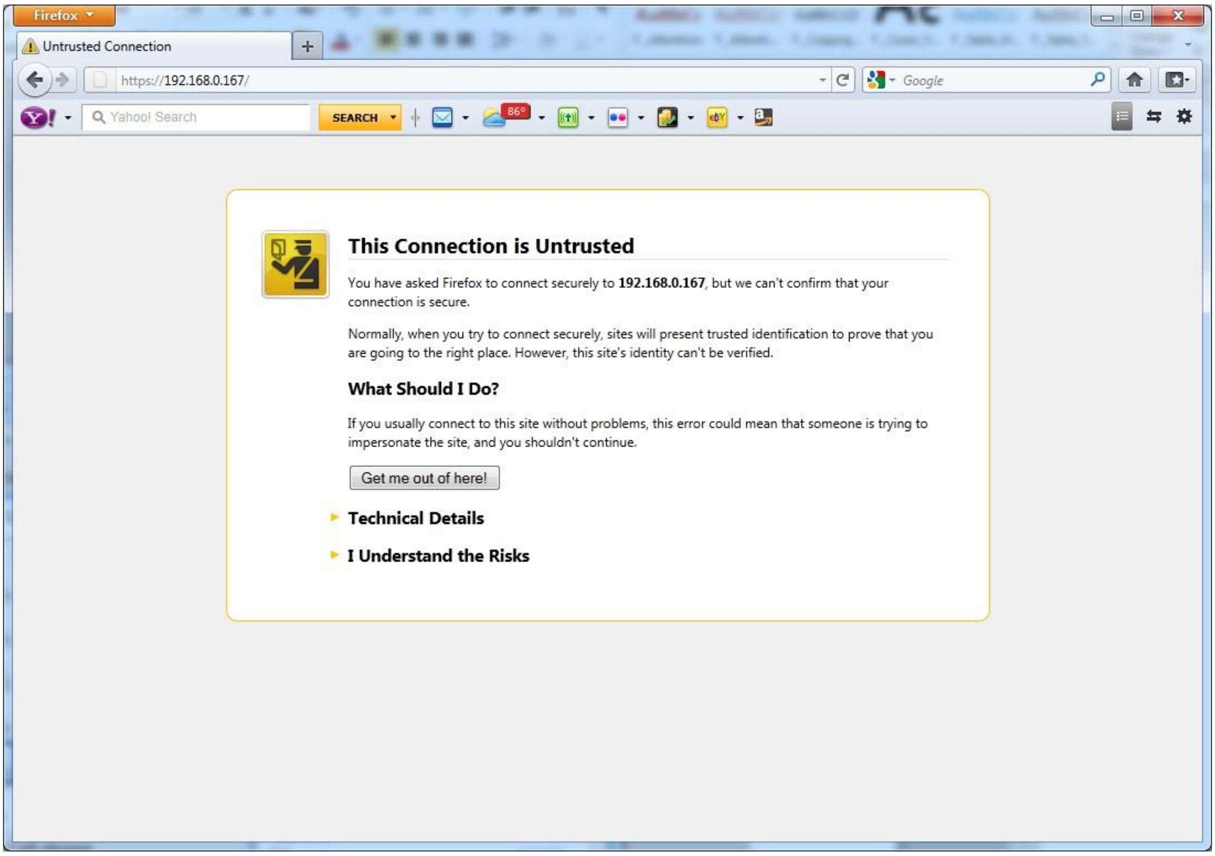
Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

No Background Tasks Version 4.0.2.5

8.3 For Mozilla Firefox

Open the Browser.

Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example https://192.168.0.201).



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.0.167**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

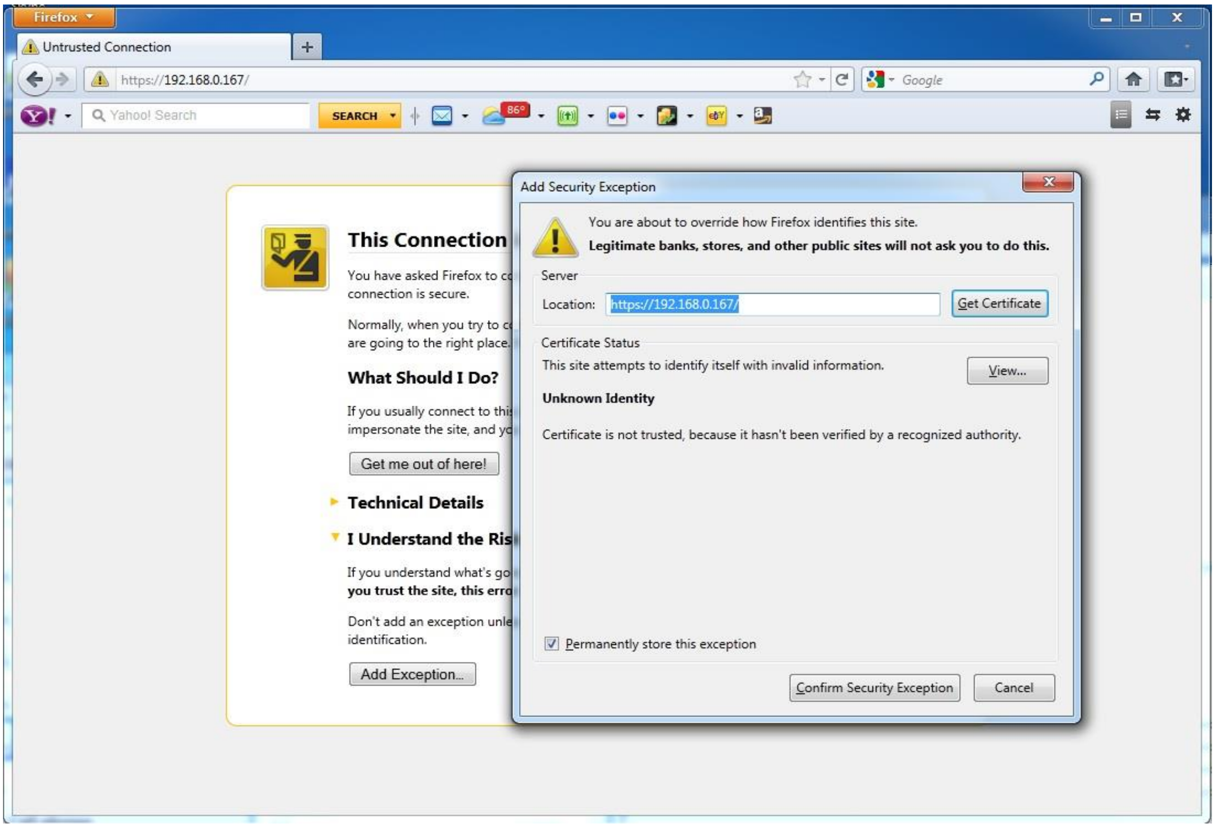
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

Just click Get Certificate button and then the Confirm Security Exception button.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://192.168.0.167/

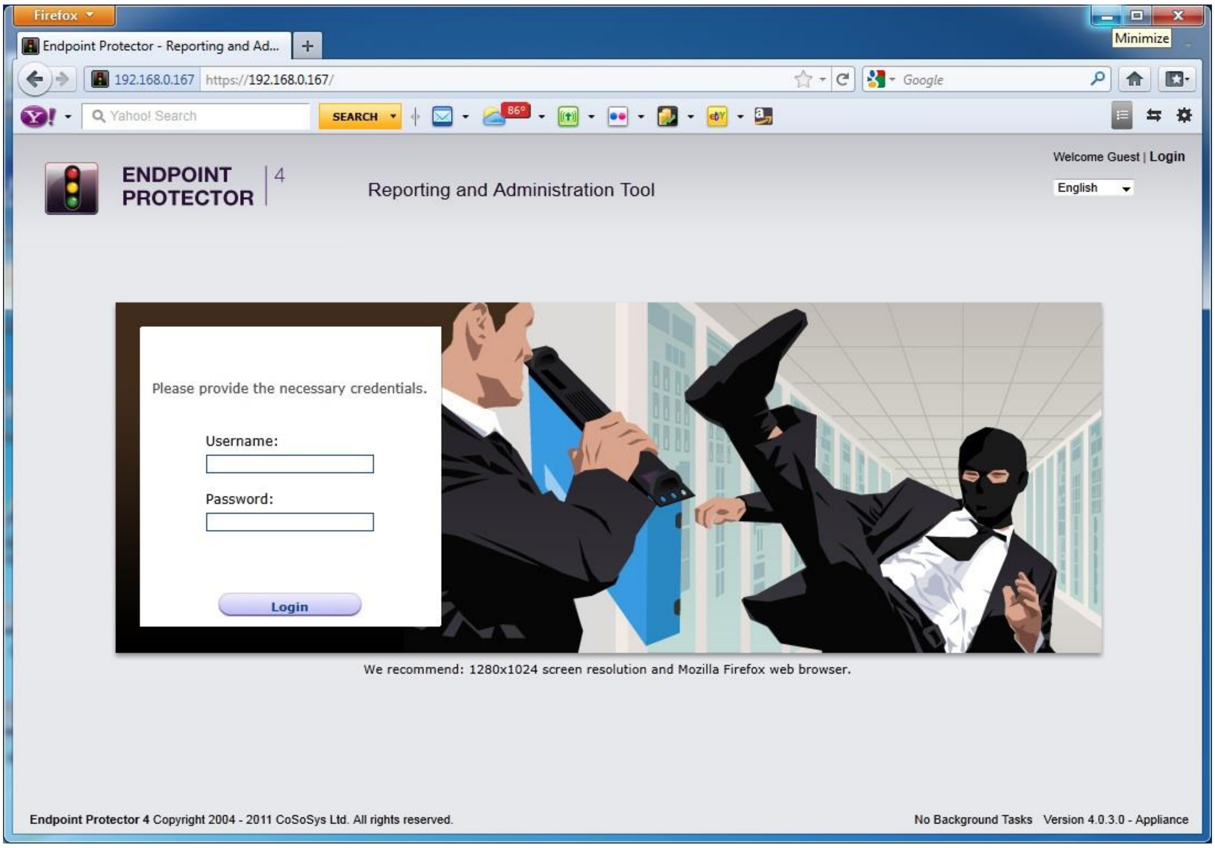
This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

Close the browser and start it again.



Welcome Guest | Login

English

ENDPOINT PROTECTOR | 4

Reporting and Administration Tool

Please provide the necessary credentials.

Username:

Password:

Login

We recommend: 1280x1024 screen resolution and Mozilla Firefox web browser.

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.

No Background Tasks Version 4.0.3.0 - Appliance

Firefox
Endpoint Protector - Reporting and Ad...
192.168.0.167 https://192.168.0.167/
Google
Minimize
Yahoo! Search
SEARCH
86°

9. Support

In case additional help is required, such as the FAQs or e-mail support, please visit the support website directly at http://www.cososys.com/help.html

10. Important Notice / Disclaimer

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of you private information (if Automatic Live Update Reporting is DISABLED).

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.

© 2004 – 2014 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.