



ENDPOINT PROTECTOR

VIRTUAL APPLIANCE

User Manual Version 4.1.0.2

User Manual



Table of Contents

1.Endpoint Protector Virtual Appliance Formats1

- 1.1. Available Formats of the Virtual Appliance.....1
 - 1.1.1. The Virtualization software that supports OVF Format is: 1
 - 1.1.2. The Virtualization software that supports VMX Format is: 1
 - 1.1.3. The Virtualization software that supports VHD Format is: 2
 - 1.1.4. The Virtualization software that supports XVA Format is: 2

2.Implementing using OVF Format3

- 2.1. Implementing in Oracle VM VirtualBox using OVF Format.....3
- 2.2. Implementing in VMware vSphere using OVF Format..... 10
- 2.3. Implementing in Citrix XenServer 5.6 using OVF Format..... 19

3.Implementing using VMX Format..... 24

- 3.1. Implementing in VMware Server 2.0 using VMX Format 24
- 3.2. Implementing in VMware Player 3.0 using VMX Format..... 27
- 3.3. Implementing in VMware Workstation 6.5 using VMX Format 30

4.Implementing using VHD Format 34

- 4.1. Implementing in Microsoft Hyper-V 2008 using VHD Format. 34

5.Access Appliance Setup Wizard 44

- 5.1. Appliance network configuration from console 44
 - 5.1.1 Manual configuration 49
 - 5.1.2. Automatic configuration 53
- 5.2. Hardware Appliance Setup Wizard..... 54
 - 5.2.1. End User License Agreement - Appliance License Agreement55
 - 5.2.2. Define your Appliance Administrator Password..... 56
 - 5.2.3. Set Time Zone 57
 - 5.2.4. Set Appliance Network IP Address 58
 - 5.2.5. Endpoint Protector Client – Automatic Repackaging 59
 - 5.2.6. Appliance Server Certificate..... 60
 - 5.2.7. Finishing the Endpoint Protector Appliance Setup 61

6.Endpoint Protector Appliance Configuration62

- 6.2 Connect Appliance to Network 62
- 6.3 Access to the Appliance Interface through your Network..... 62

6.4	Login to Endpoint Protector	63
6.5	Appliance Configuration Wizard.....	64
6.6	Appliance Basic Settings	65
6.7	Appliance Default Policies.....	67
6.8	Finishing the Endpoint Protector Appliance Configuration Wizard	67
7. Appliance Settings and Maintenance		68
7.2	Server Information.....	68
7.3	Server Maintenance	69
7.3.1	Network Settings	69
7.3.2	Reboot the Appliance.....	69
7.3.3	Reset Appliance to Factory Default	70
7.4	Endpoint Protector Client Installation for Appliance.....	71
7.5	Appliance Online Live Update.....	73
8. Installing Root Certificate to your Internet Browser		74
8.2	For Microsoft Internet Explorer	74
8.3	For Mozilla Firefox	84
9. Support		87
10. Important Notice / Disclaimer.....		88

1. Endpoint Protector Virtual Appliance Formats

1.1. Available Formats of the Virtual Appliance

The Endpoint Protector Virtual Appliance is distributed in different formats:

- As OVF package
- As VMX package
- As XVA package
- As VHD package

Endpoint Protector makes available these formats in order to help customer 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 Format is:

- VMWare Workstation 7.1 and VMware Player 3.1
- Oracle VM Virtual Box
- Citrix XenServer 5.6

1.1.2. The Virtualization software that supports VMX Format is:

- VMware Server 2.0 or higher
- VMware Player 3.0 or higher
- VMware Workstation 6.5 or higher

Note! Some of the images might be incompatible with some versions of certain virtualization media. Please contact support@endpointprotector.com or try another image format.

1.1.3. The Virtualization software that supports VHD Format is:

- Microsoft Hyper-V

1.1.4. The Virtualization software that supports XVA Format is:

- Citrix XenServer 5.5
- Citrix XenServer 6.0

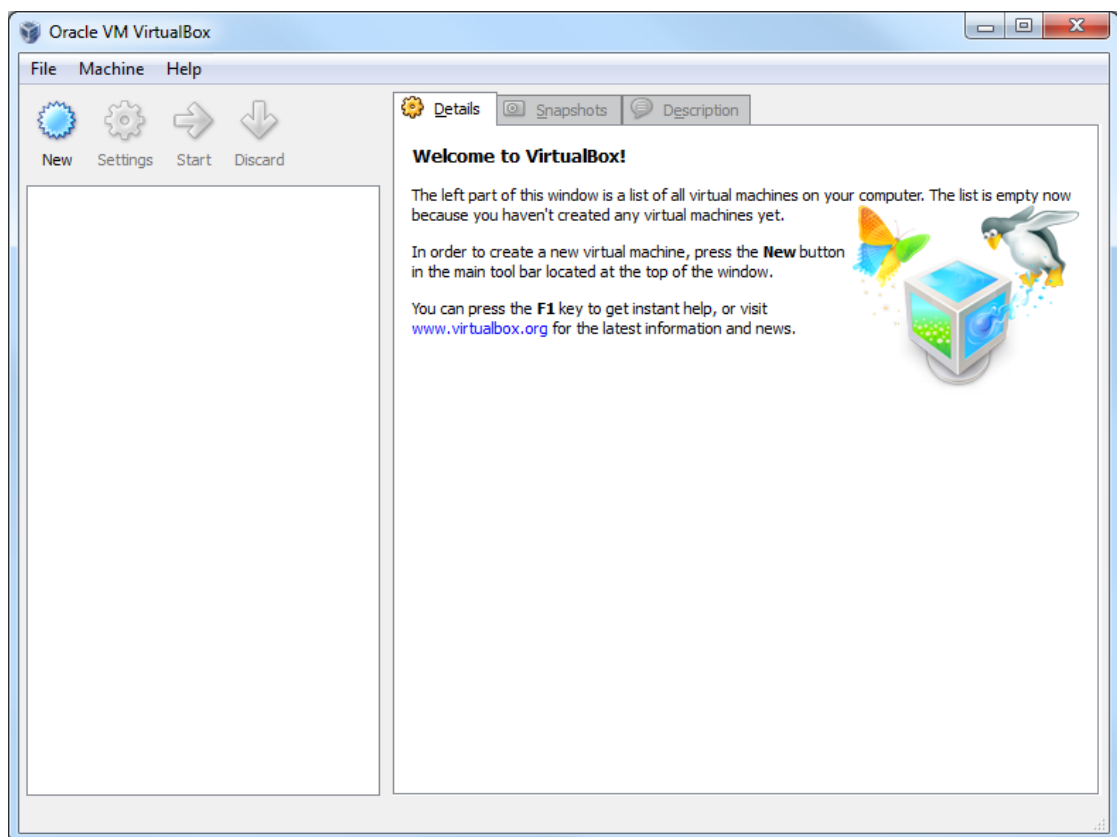
Note!

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.

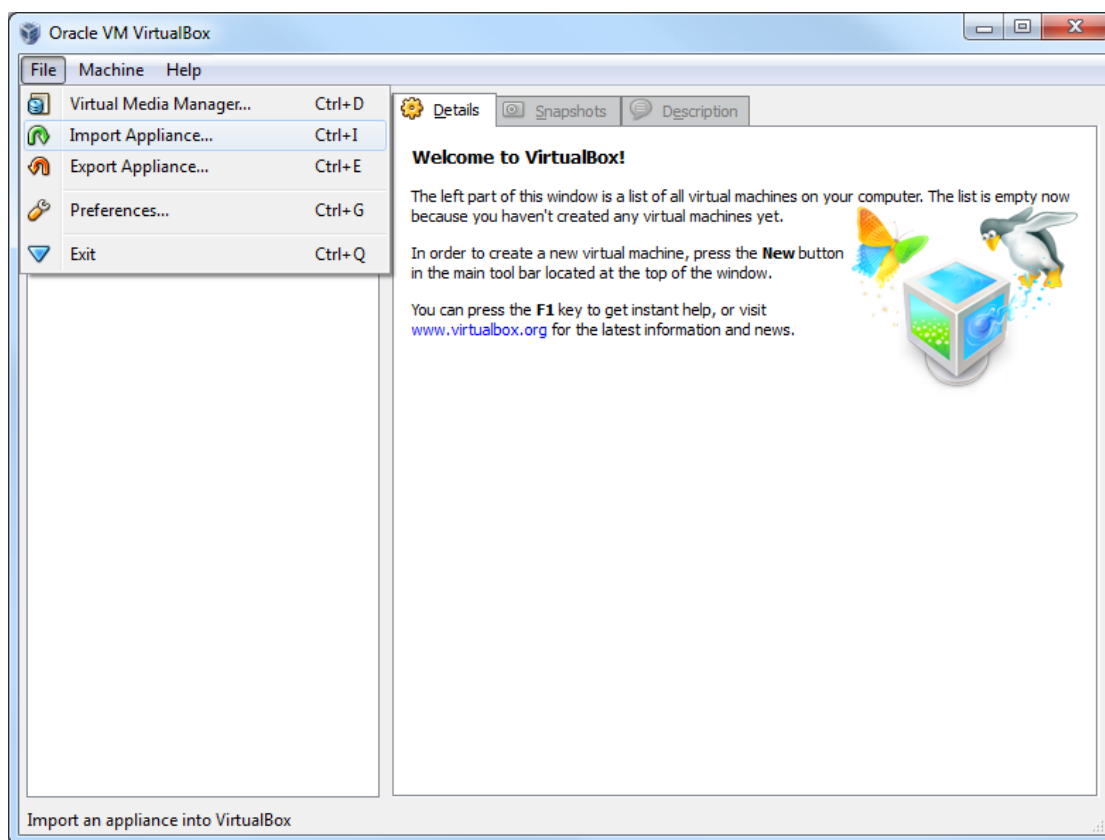
2. Implementing using OVF Format

2.1. Implementing in Oracle VM VirtualBox using OVF Format

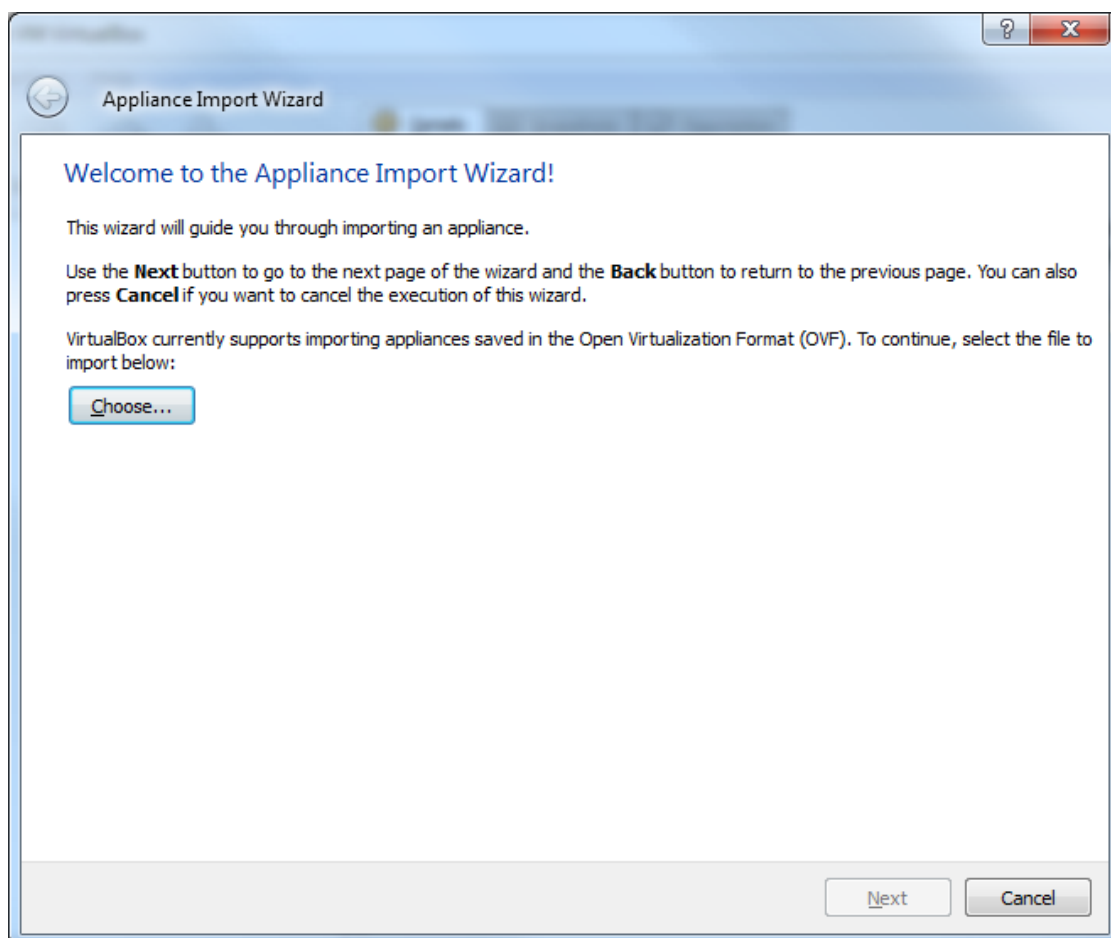
1. Unzip the downloaded package
2. Start VirtualBox



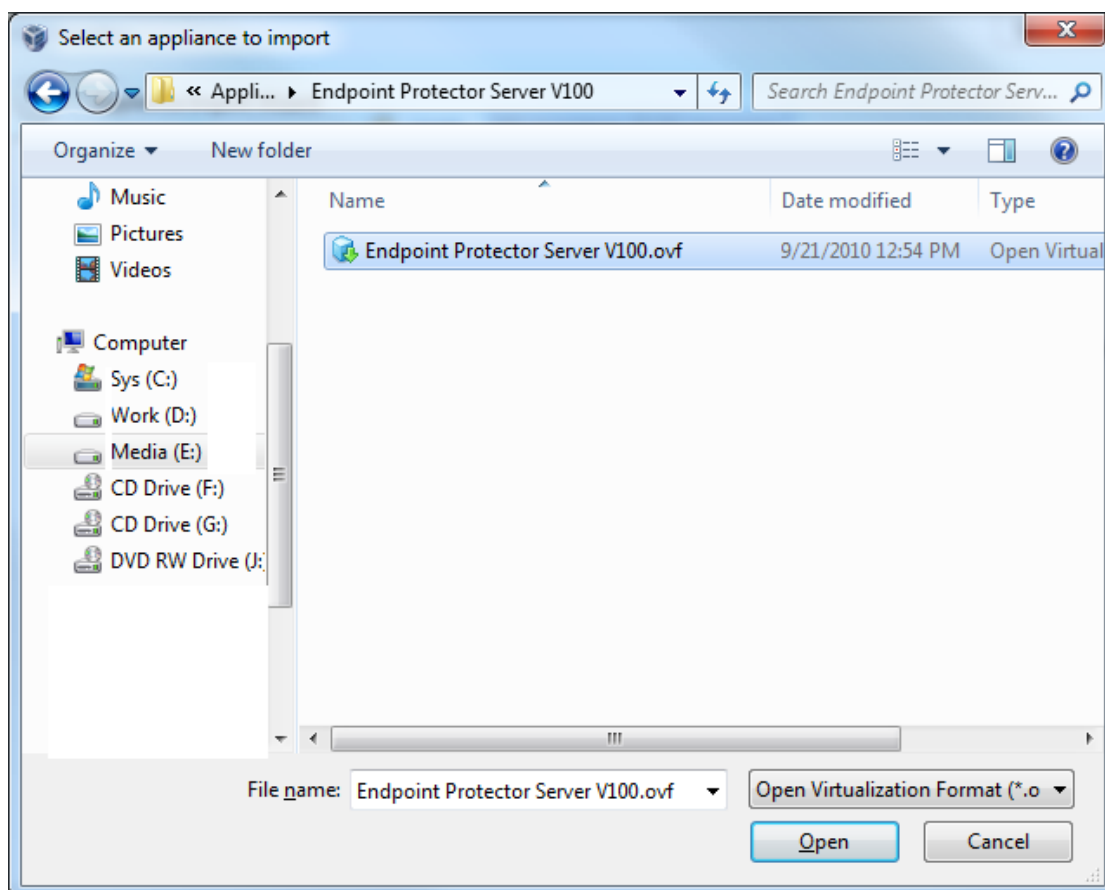
3. Go To File > Import Appliance



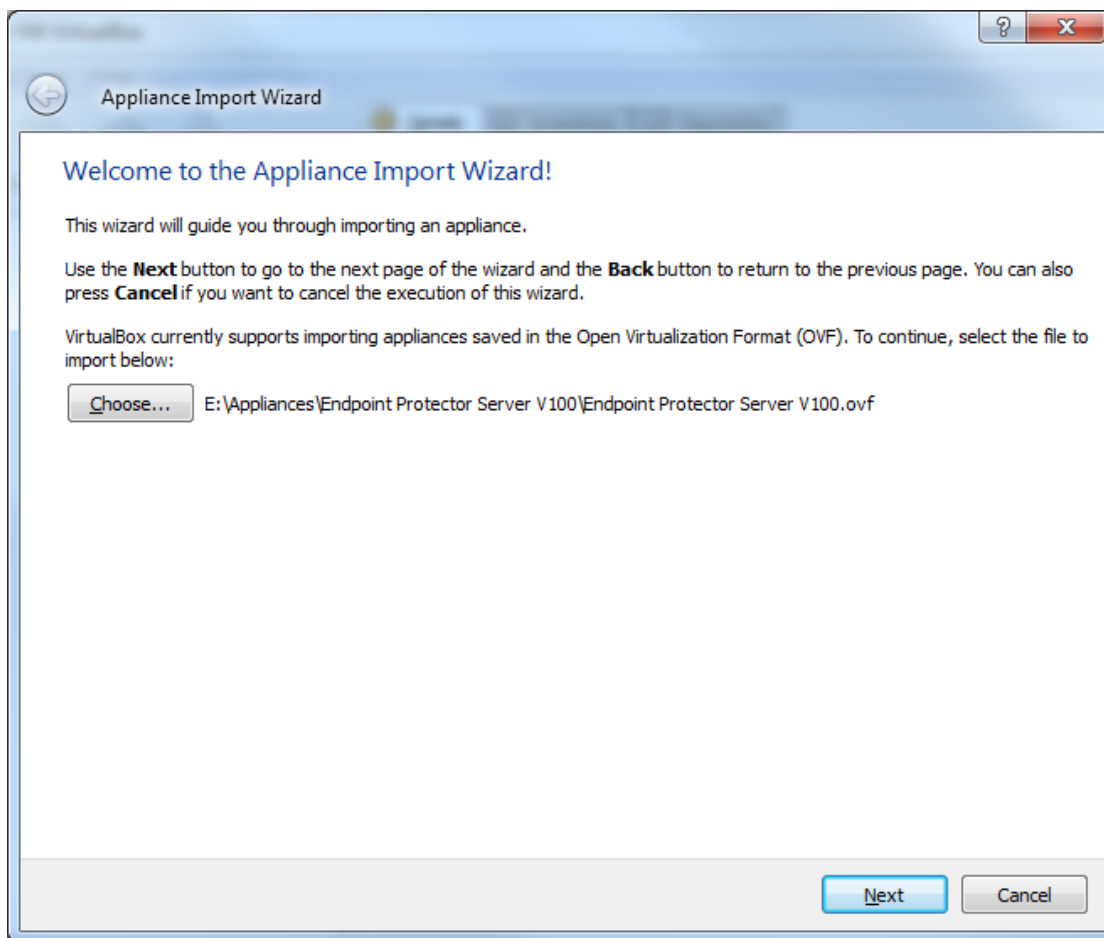
4. Press Choose button



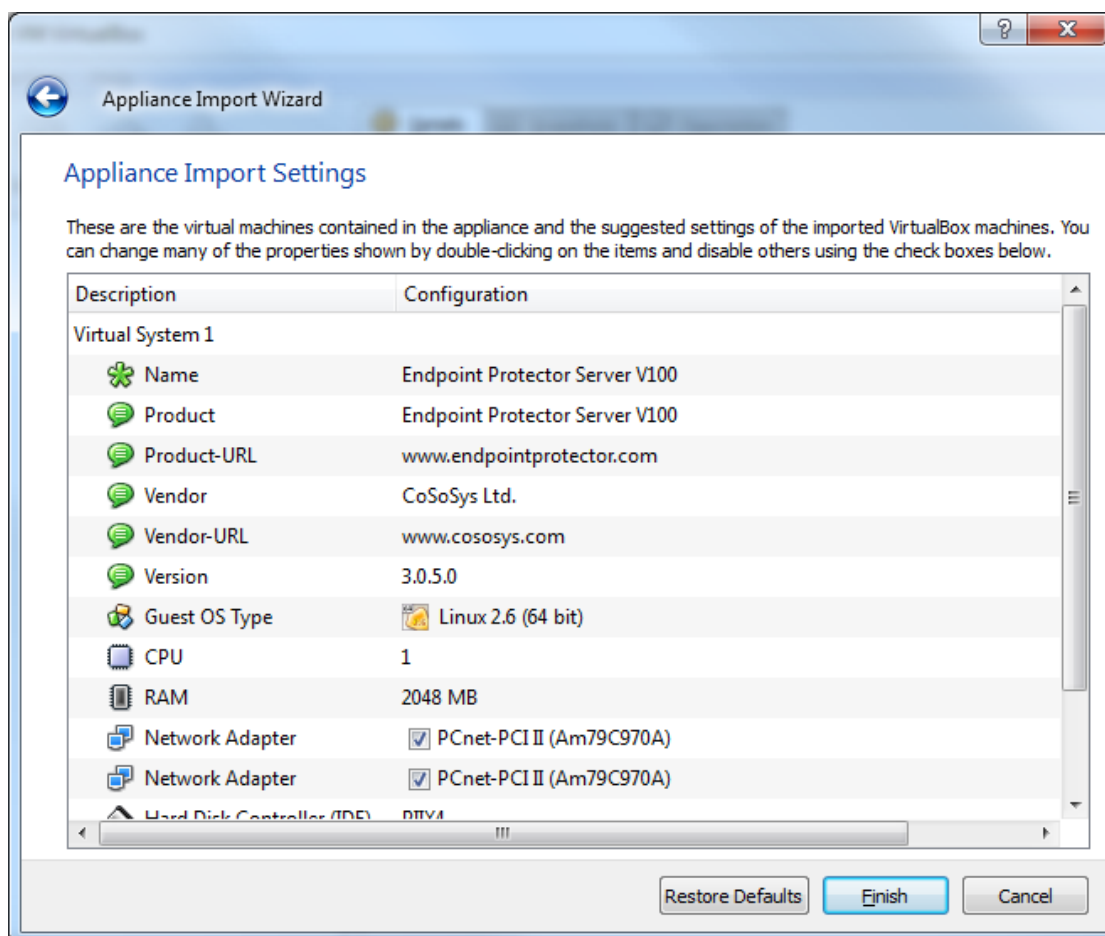
5. Browse and select the OVF file from the extracted zip file



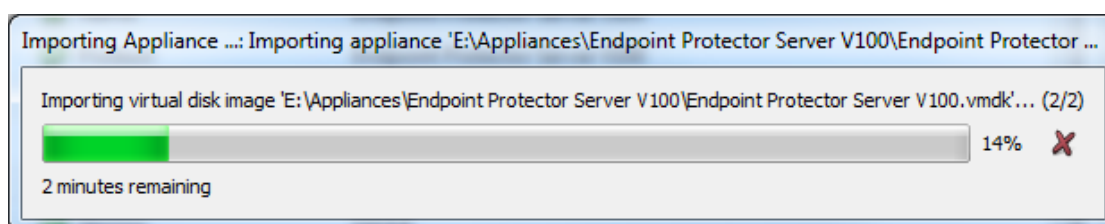
6. Press Next Button



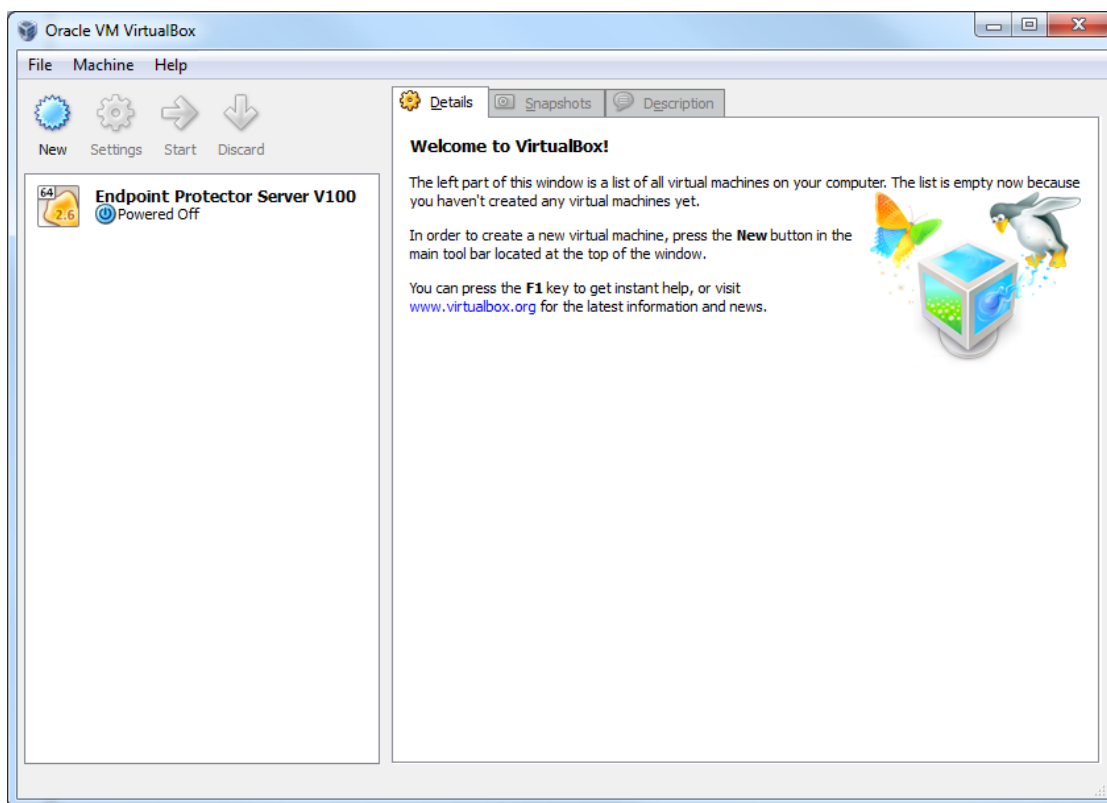
7. Press Finish Button



8. Wait for the import displayed by the progress bar



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

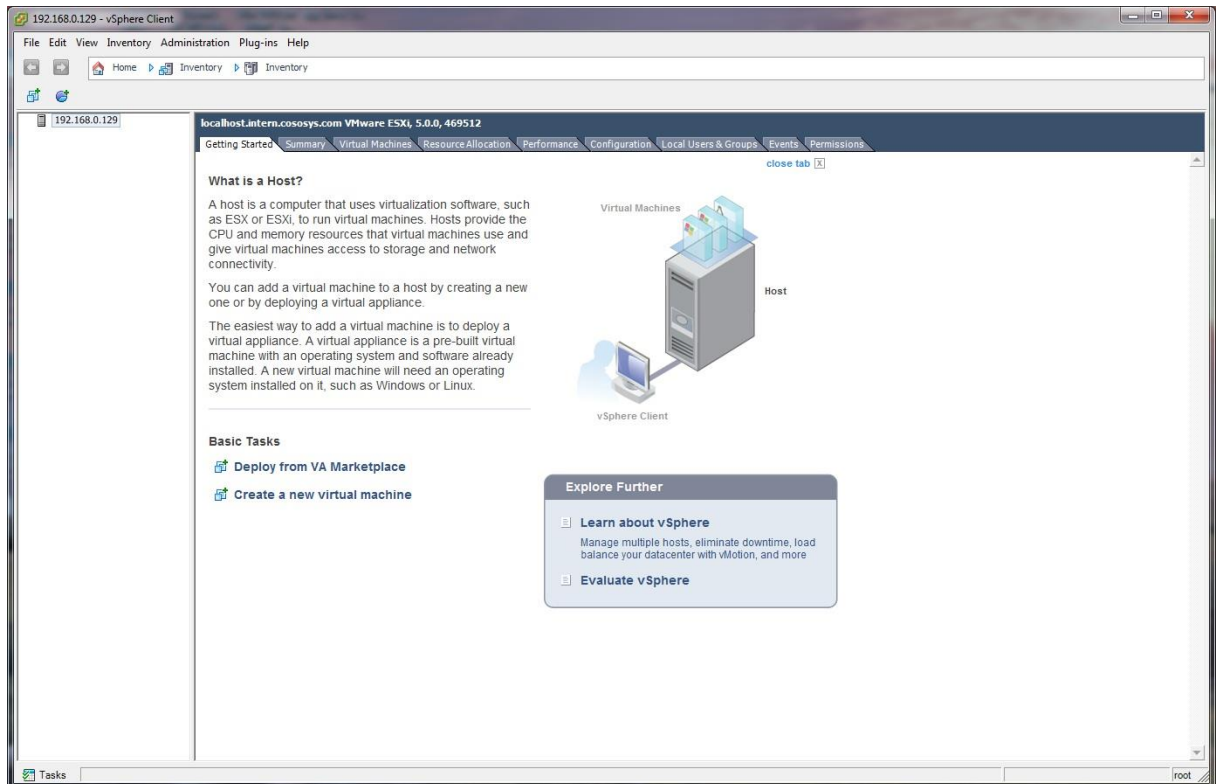


At this point the virtual machine is ready to be started.

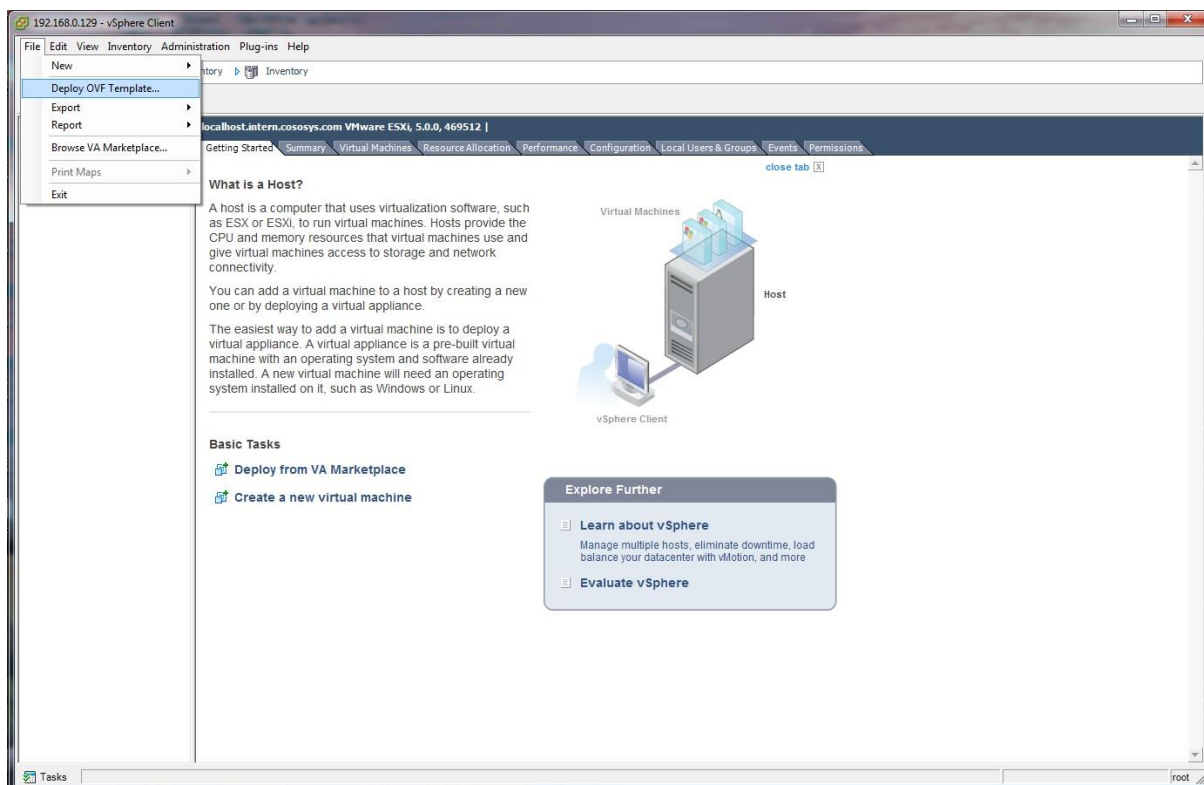
Please follow the Endpoint Protector Appliance User Manual from this point on.

2.2. Implementing in VMware vSphere using OVF Format

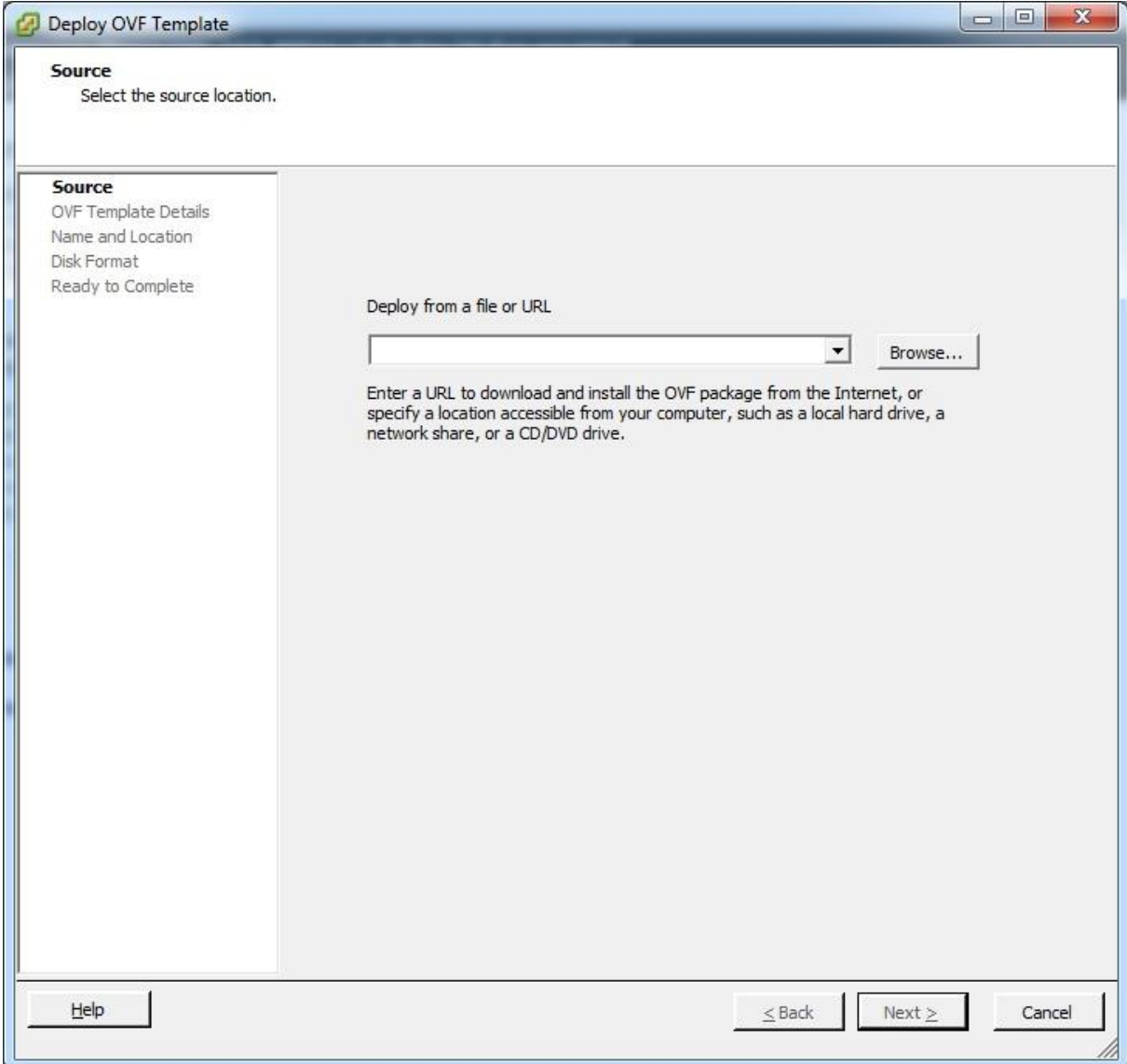
1. Unzip the downloaded package.
2. Start vSphere.



3. Go To File > Deploy OVF Template.



4. Press the Browse button.



The image shows a Windows-style dialog box titled "Deploy OVF Template". It has a standard title bar with minimize, maximize, and close buttons. The main area is divided into two panes. The left pane, titled "Source", contains a list of steps: "OVF Template Details", "Name and Location", "Disk Format", and "Ready to Complete". The right pane, also titled "Source", contains the instruction "Select the source location." and a section labeled "Deploy from a file or URL". This section features a text input field with a dropdown arrow and a "Browse..." button. Below the input field, there is a paragraph of text: "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." At the bottom of the dialog, there are three buttons: "Help" on the left, and "< Back", "Next >", and "Cancel" on the right.

Deploy OVF Template

Source
Select the source location.

Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete

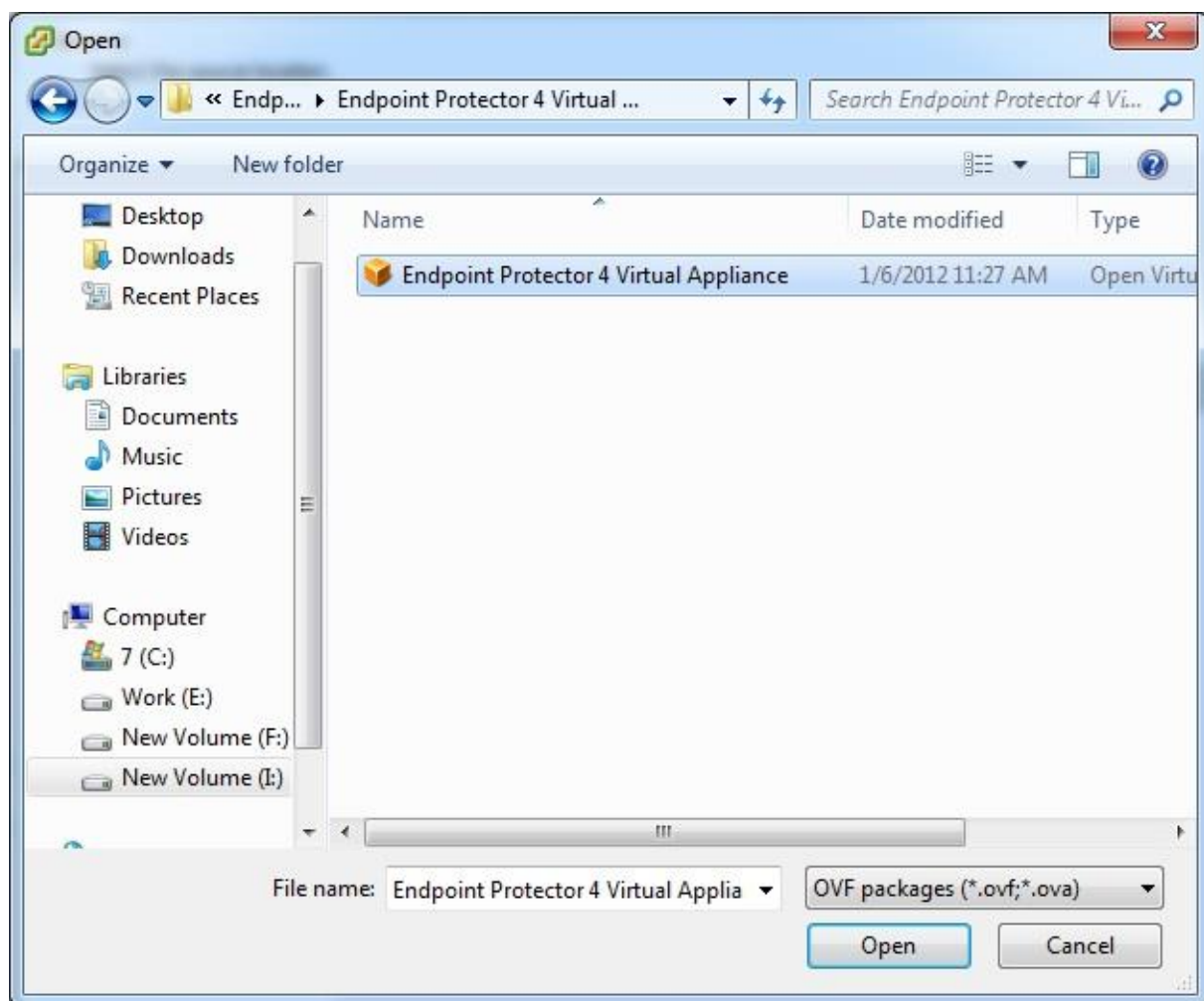
Deploy from a file or URL

Browse...

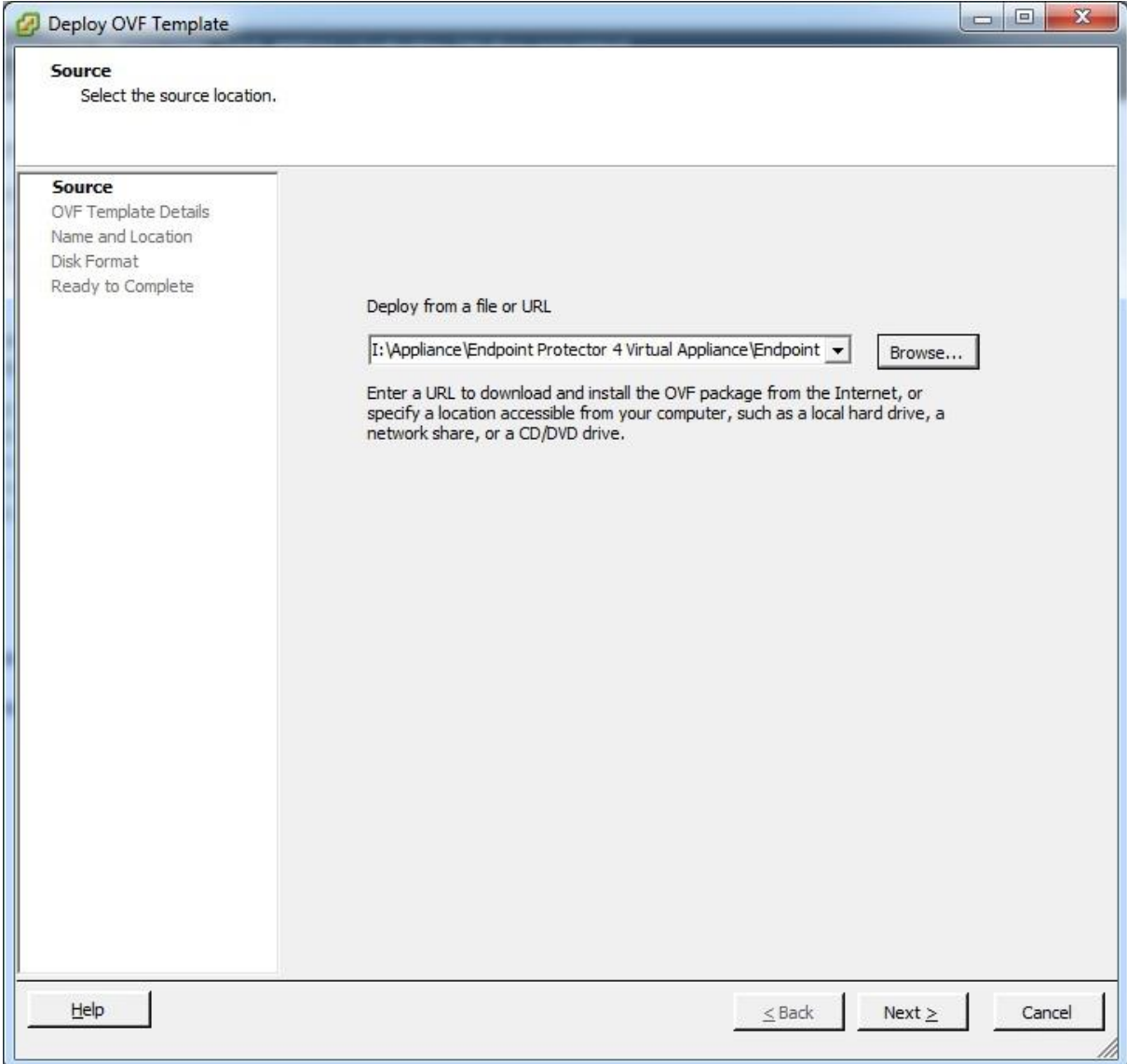
Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Help **< Back** **Next >** **Cancel**

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



6. Press the Next button.



The image shows a Windows-style dialog box titled "Deploy OVF Template". The dialog has a standard title bar with minimize, maximize, and close buttons. The main content area is divided into two sections. The top section, labeled "Source", contains the instruction "Select the source location." Below this is a list of steps: "Source", "OVF Template Details", "Name and Location", "Disk Format", and "Ready to Complete". The "Source" step is currently selected. The main area of the dialog is titled "Deploy from a file or URL" and contains a text input field with the path "I:\Appliance\Endpoint Protector 4 Virtual Appliance\Endpoint" and a "Browse..." button. Below the input field, there is a paragraph of text: "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." At the bottom of the dialog, there are three buttons: "Help", "< Back", and "Next >", and a "Cancel" button on the far right.

Deploy OVF Template

Source
Select the source location.

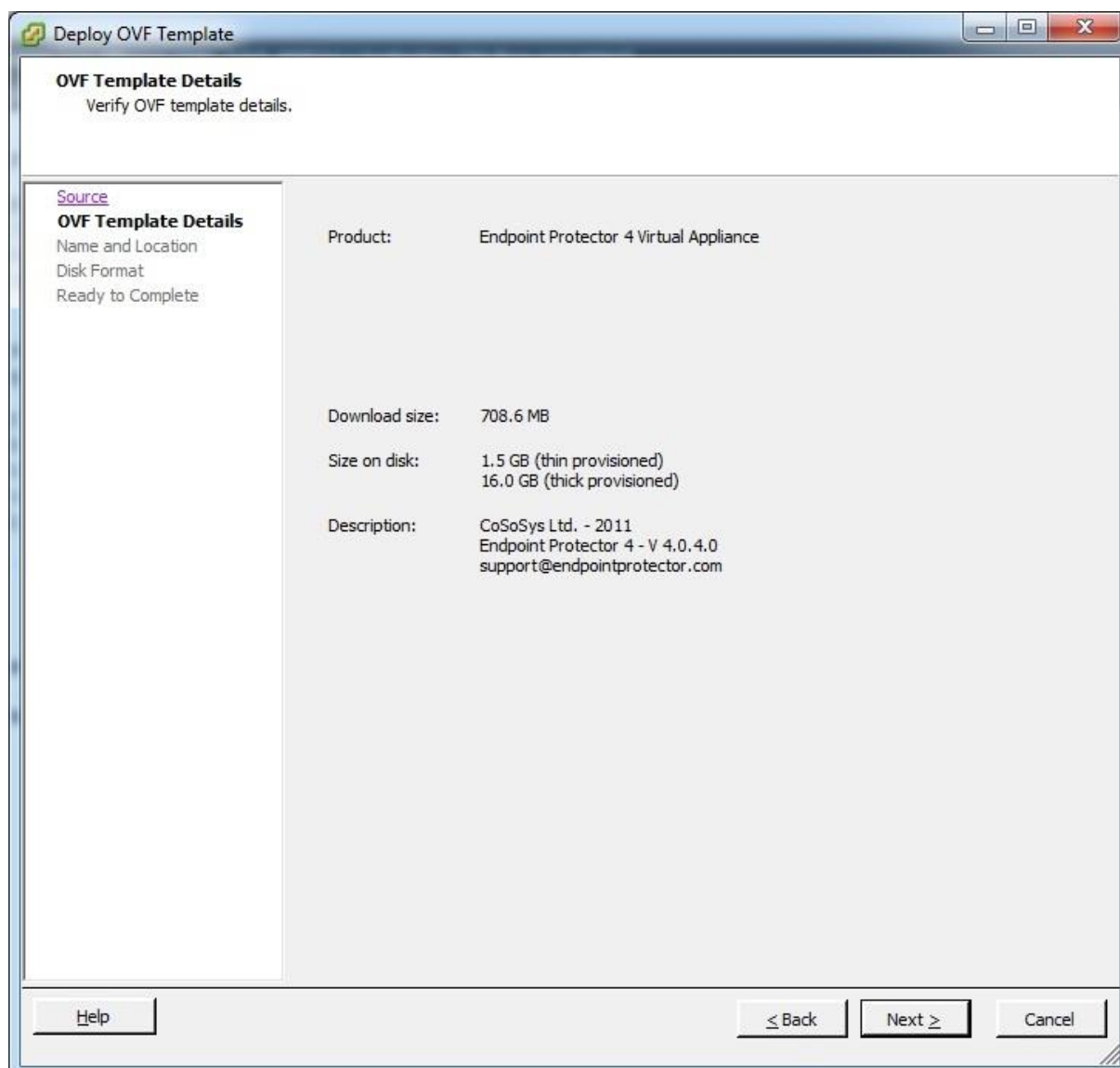
Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete

Deploy from a file or URL

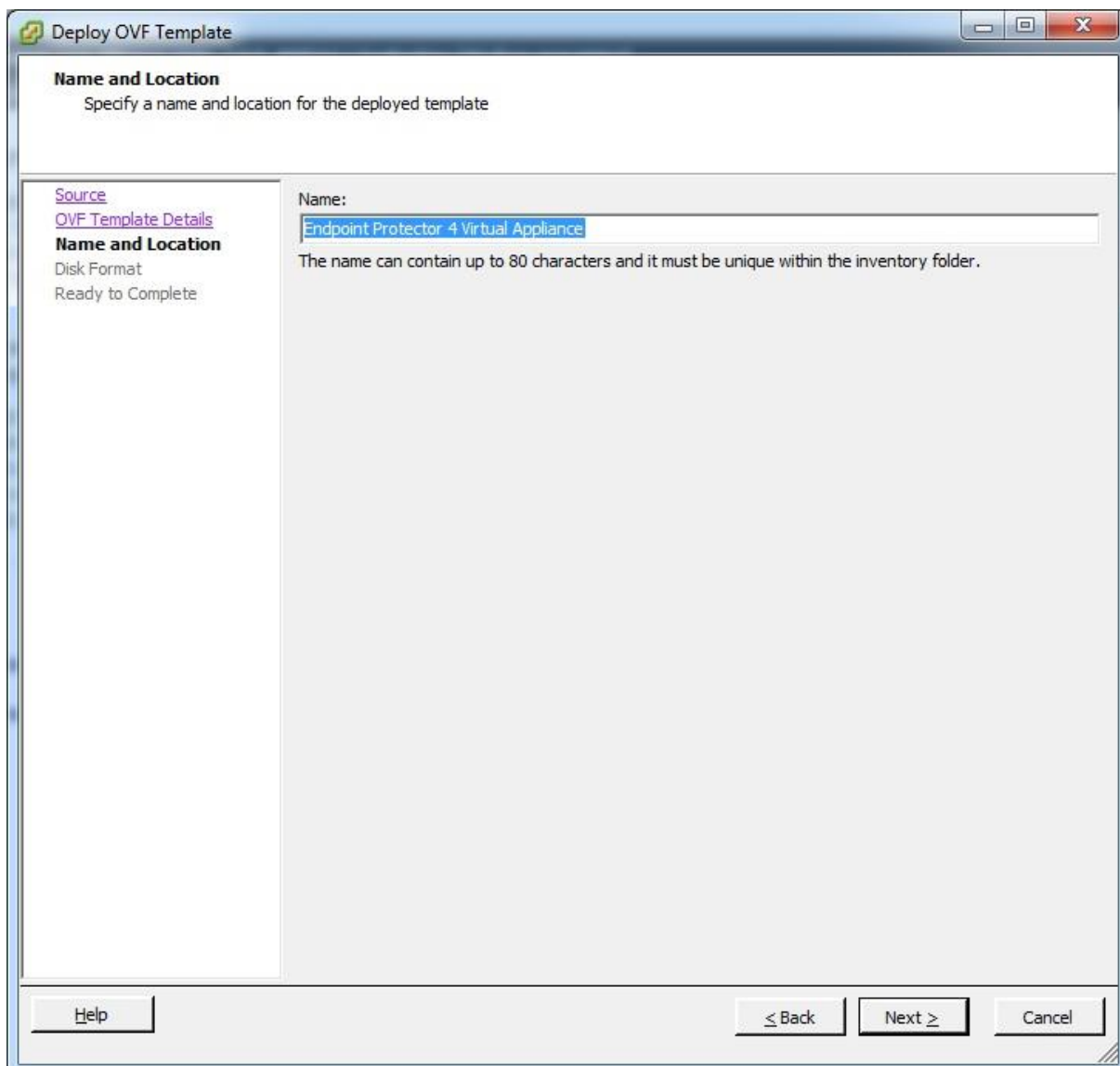
I:\Appliance\Endpoint Protector 4 Virtual Appliance\Endpoint

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.



8. Specify the name of the OVF template and press Next.



The image shows a Windows-style dialog box titled "Deploy OVF Template". It has a standard title bar with minimize, maximize, and close buttons. The main content area is divided into two panes. The left pane contains a list of steps: "Source", "OVF Template Details", "Name and Location" (which is currently selected and bolded), "Disk Format", and "Ready to Complete". The right pane is titled "Name and Location" and contains the instruction "Specify a name and location for the deployed template". Below this, there is a "Name:" label followed by a text input field containing "Endpoint Protector 4 Virtual Appliance". A note below the input field states: "The name can contain up to 80 characters and it must be unique within the inventory folder." At the bottom of the dialog, there are three buttons: "Help", "< Back", and "Next >", and a "Cancel" button on the far right.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

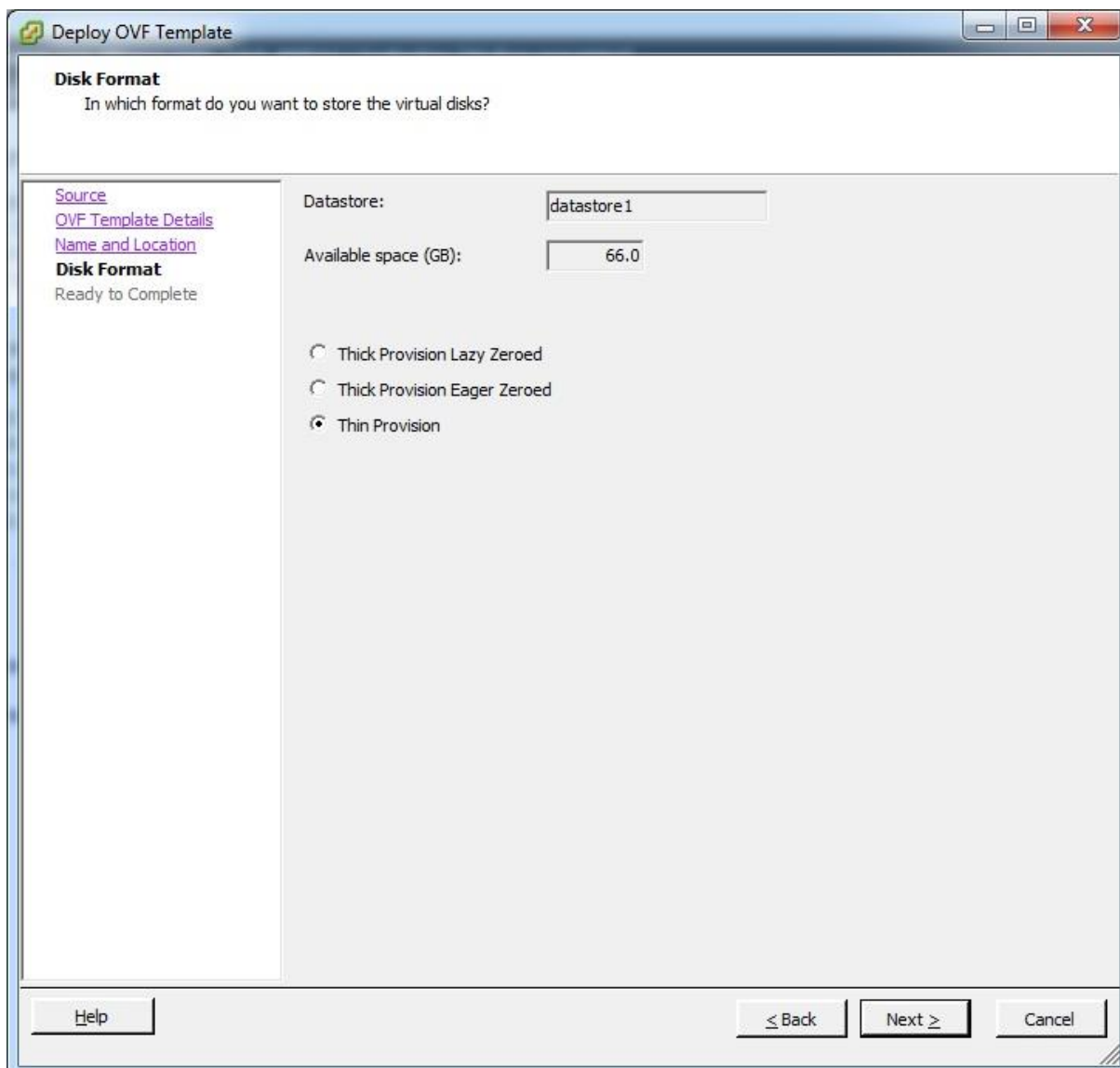
[Source](#)
[OVF Template Details](#)
Name and Location
[Disk Format](#)
[Ready to Complete](#)

Name:
Endpoint Protector 4 Virtual Appliance

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

Help < Back Next > Cancel

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



The screenshot shows a window titled "Deploy OVF Template" with a standard Windows-style title bar. The main content area is titled "Disk Format" and contains the question "In which format do you want to store the virtual disks?". On the left side, there is a sidebar with a list of steps: "Source", "OVF Template Details", "Name and Location", "Disk Format" (which is currently selected and bolded), and "Ready to Complete". The main area displays the "Datastore:" field with the value "datastore 1" and the "Available space (GB):" field with the value "66.0". Below these fields, there are three radio button options: "Thick Provision Lazy Zeroed", "Thick Provision Eager Zeroed", and "Thin Provision" (which is selected). At the bottom of the window, there are three buttons: "Help", "< Back", and "Next >", and a "Cancel" button on the far right.

Deploy OVF Template

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

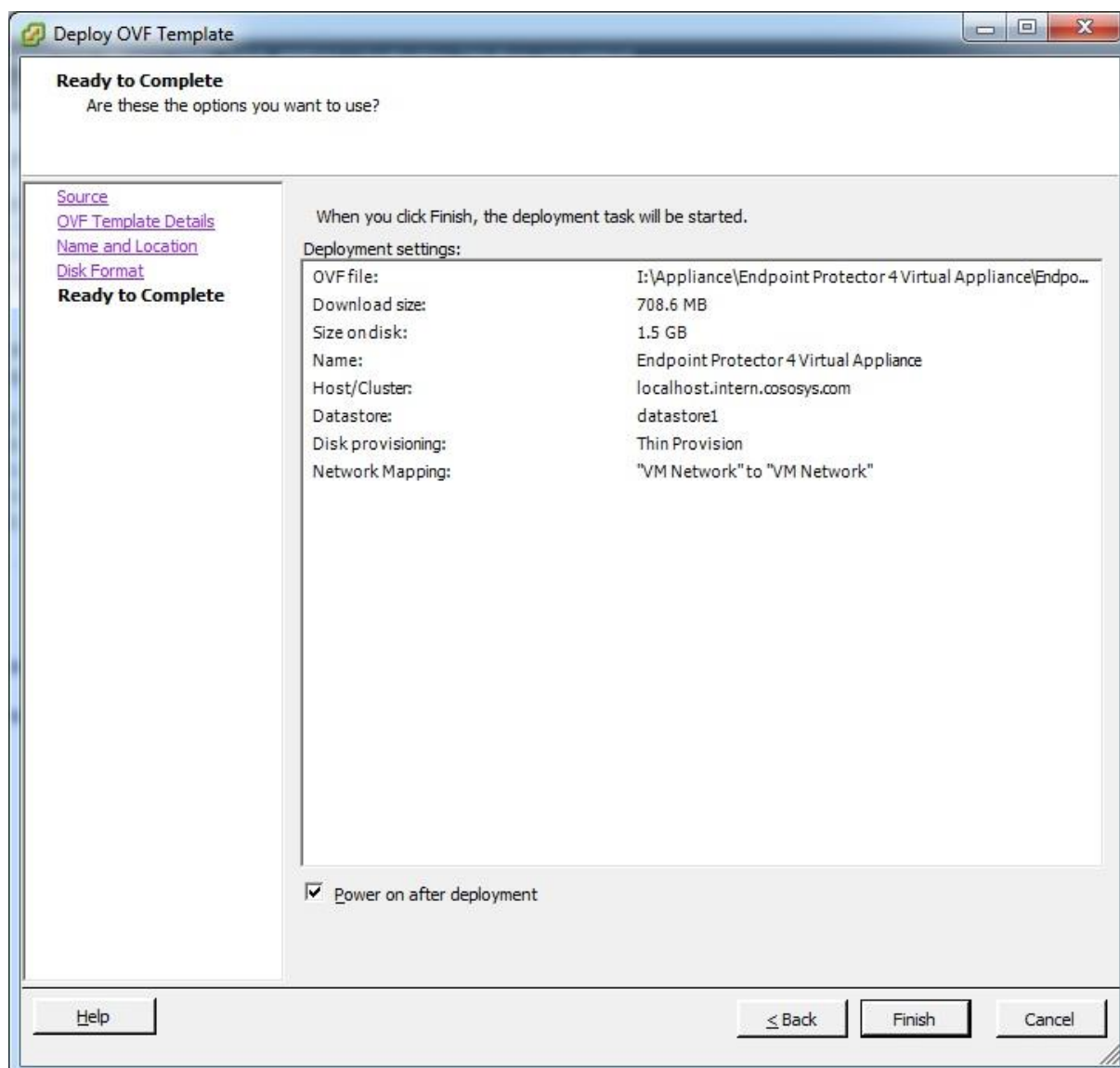
[Source](#)
[OVF Template Details](#)
[Name and Location](#)
Disk Format
Ready to Complete

Datastore:

Available space (GB):

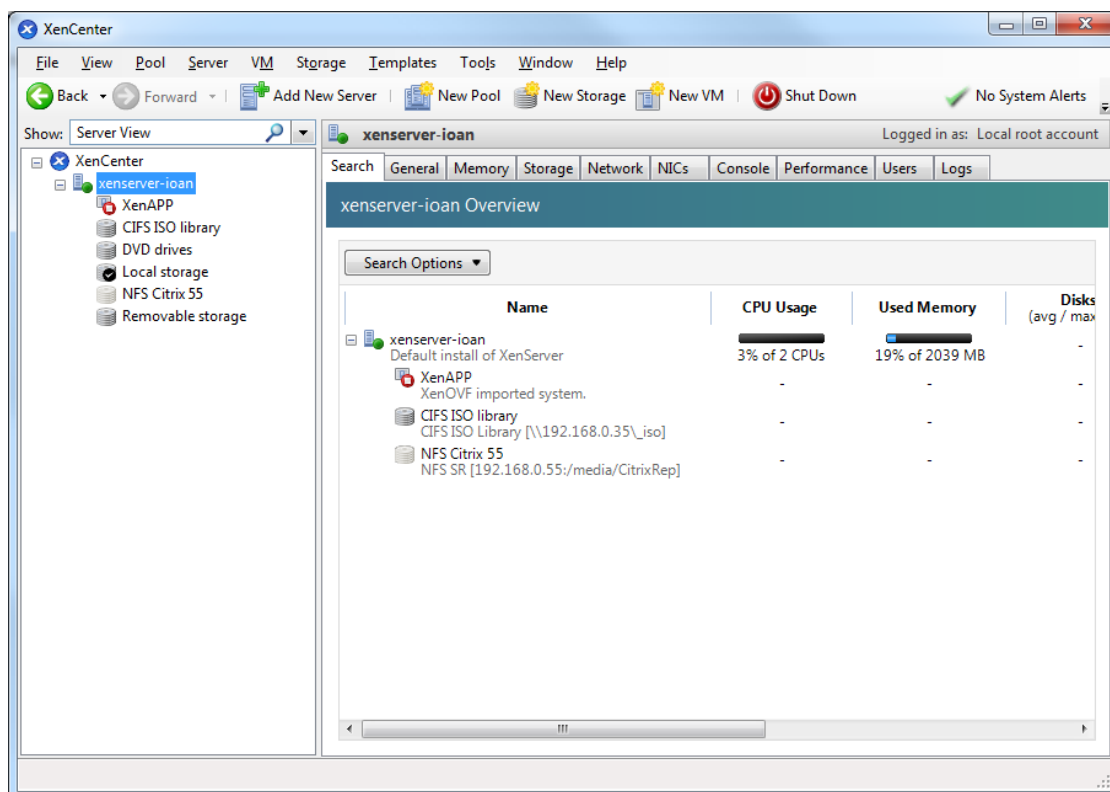
☐ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☒ Thin Provision

10. Press the Finish button to complete the installation.

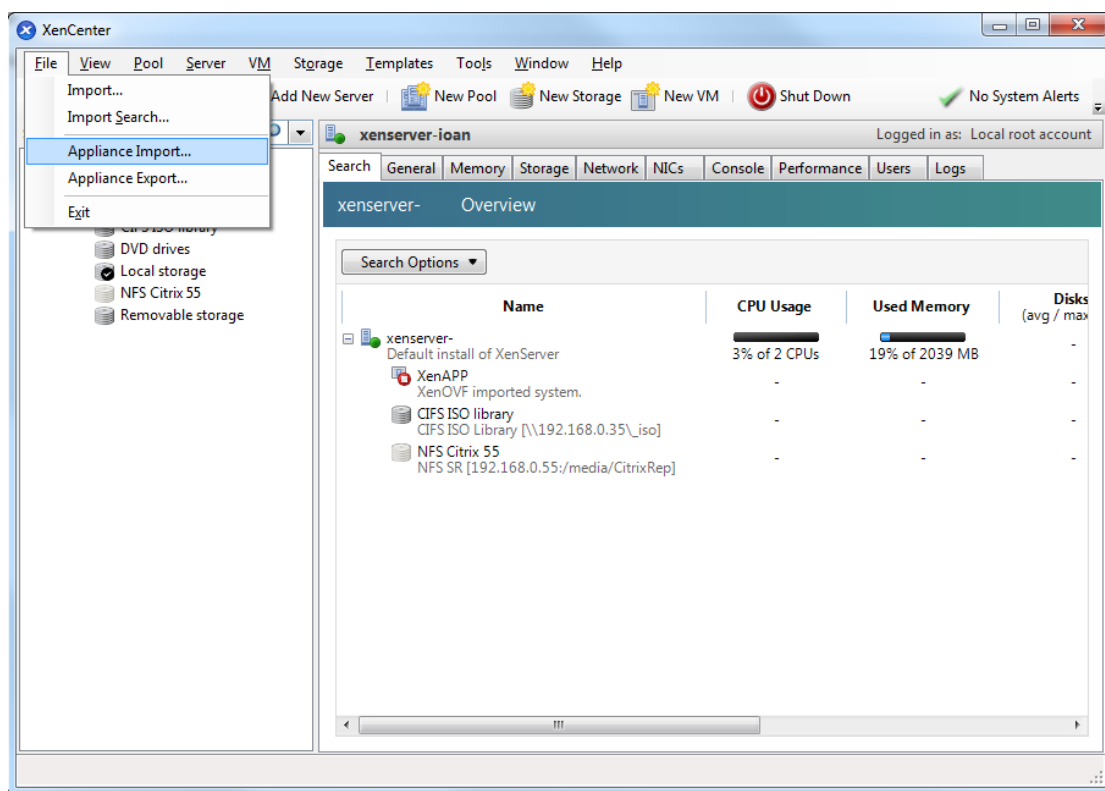


2.3. Implementing in Citrix XenServer 5.6 using OVF Format

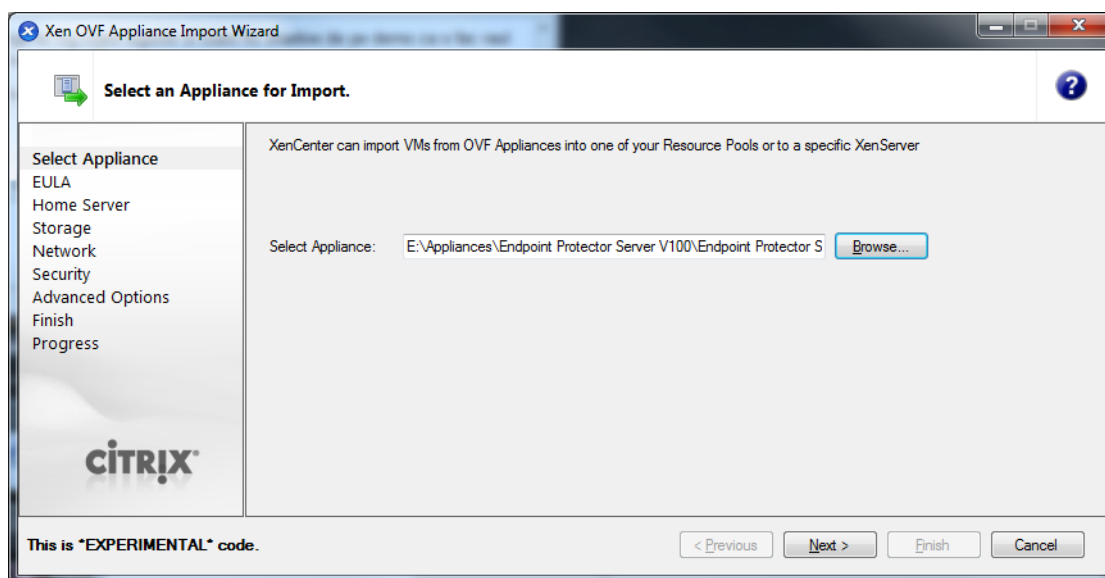
1. Unzip the downloaded package
2. Start XenCenter



3. Go To File > Appliance Import



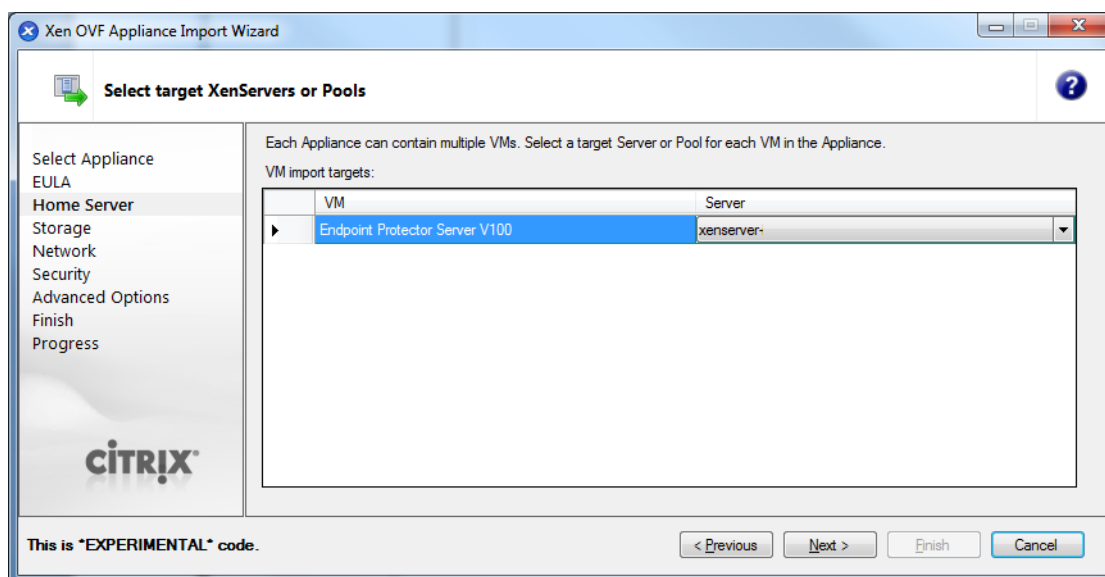
4. Select the OVF file



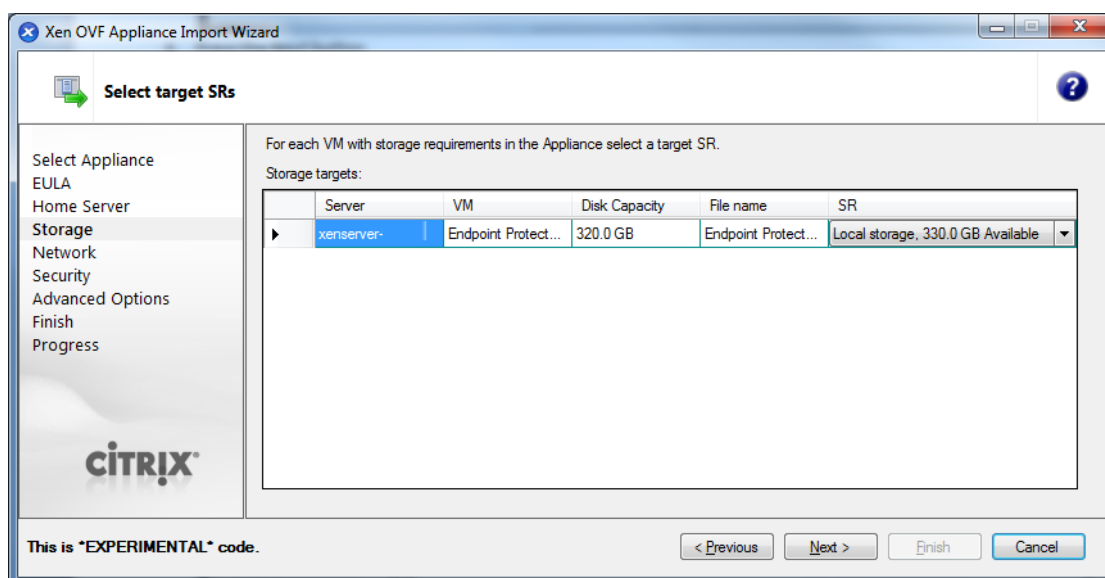
5. Press the Next button

6. Read and accept the EULA, then press Next

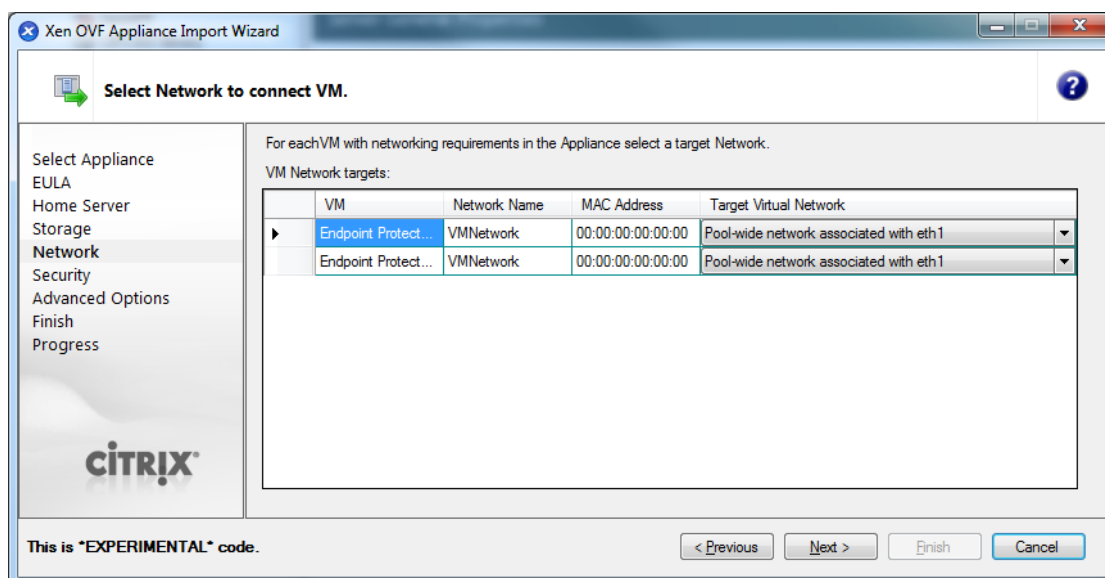
7. Select the target for this Virtual Appliance



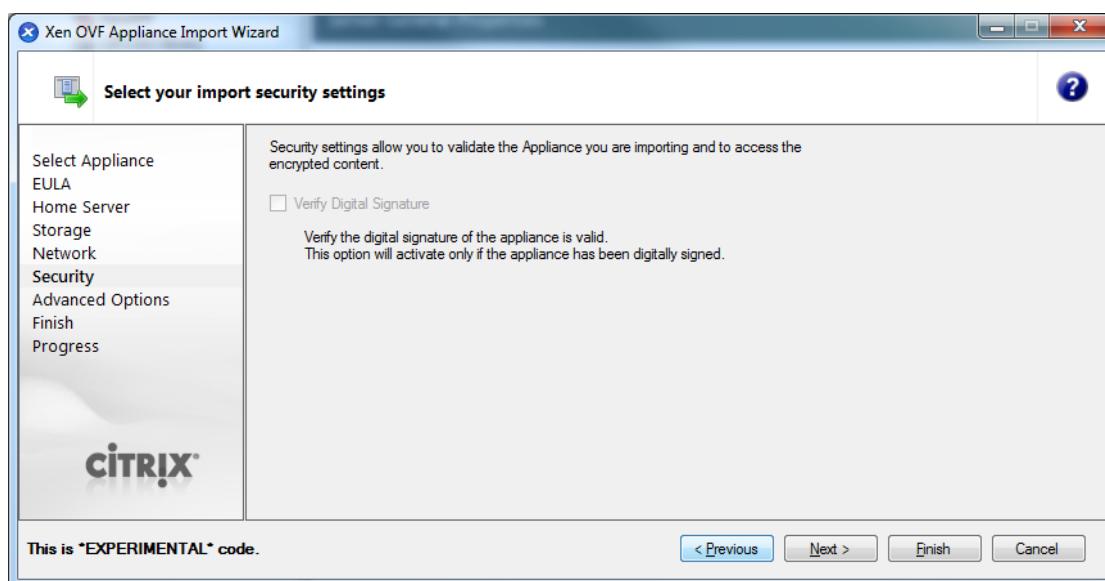
8. Select the storage location



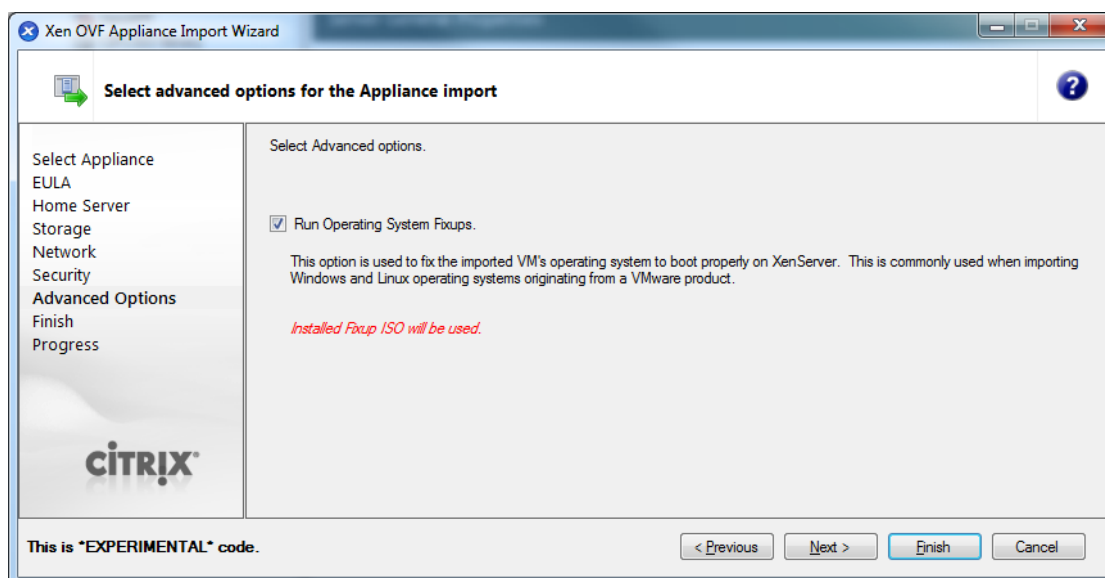
9. Select you network (keep default values)



10. On Security Screen click on Next button

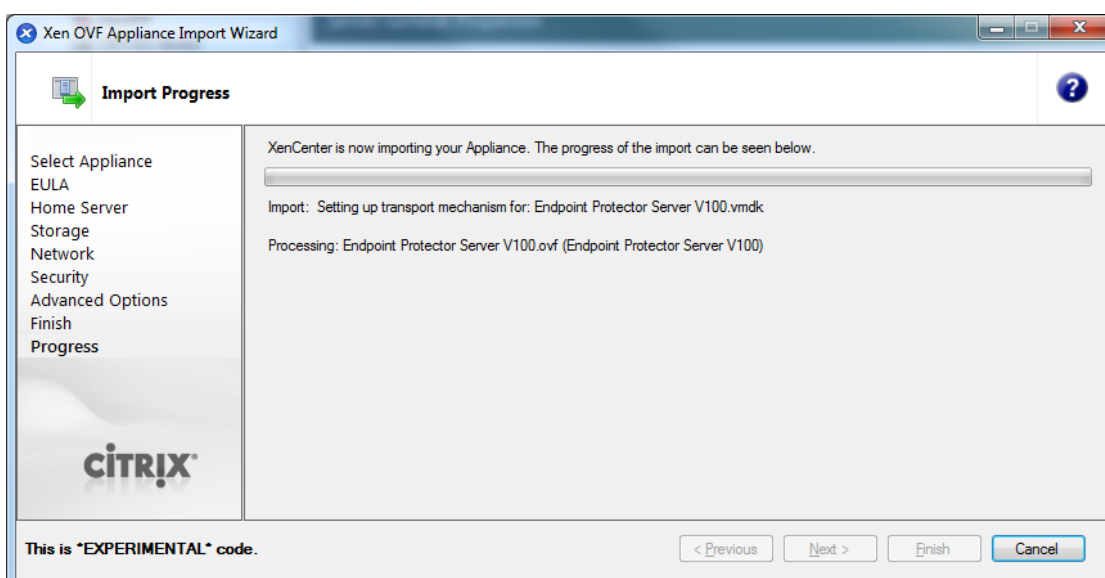


11. On Advanced Options screen click Next



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

13. Wait for the import to be completed



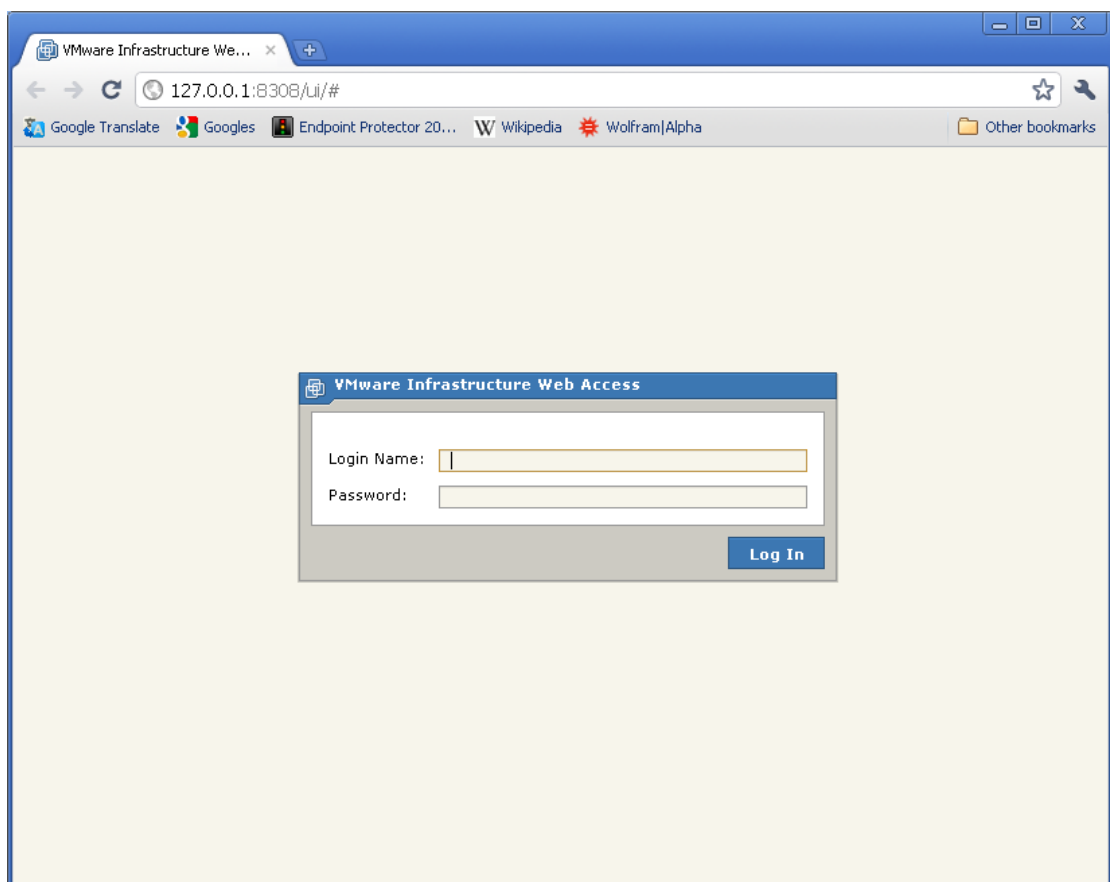
At this point the virtual machine is ready to be started.

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

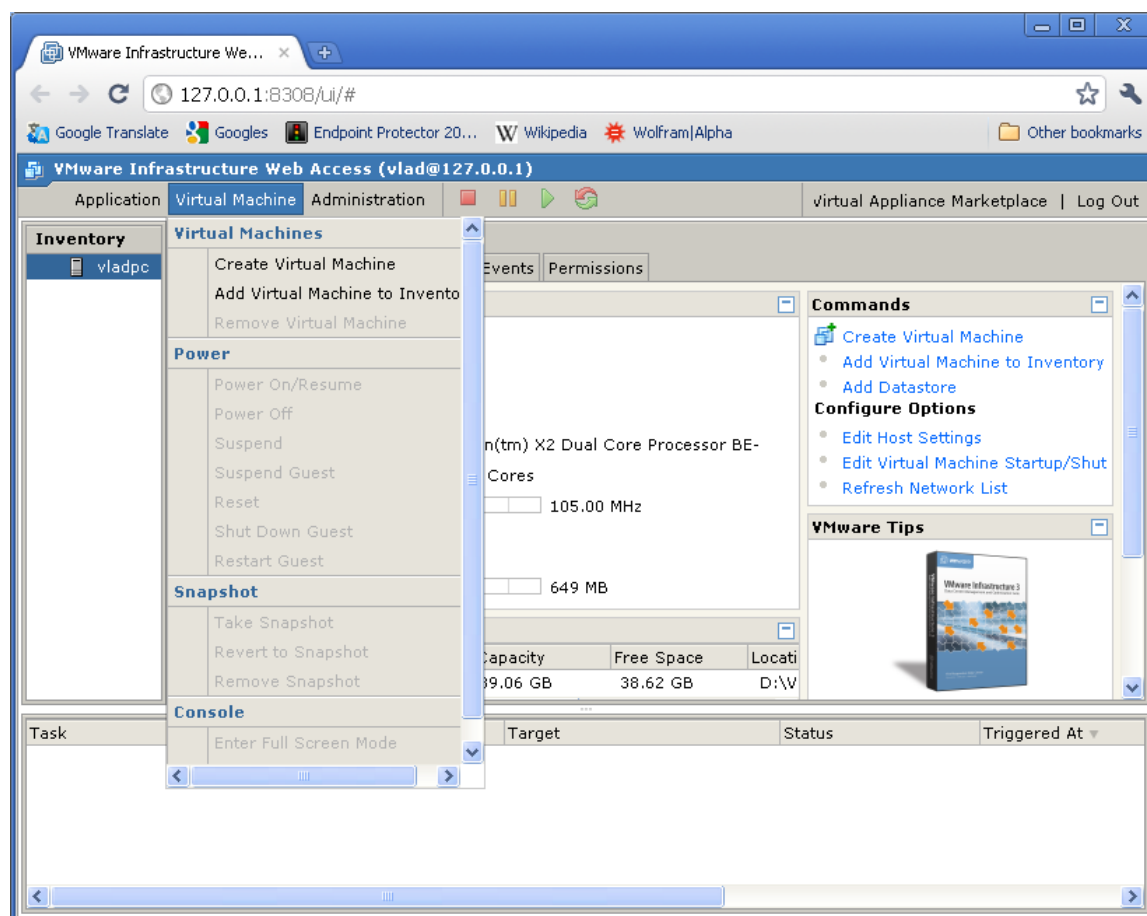
3. Implementing using VMX Format

3.1. Implementing in VMware Server 2.0 using VMX Format

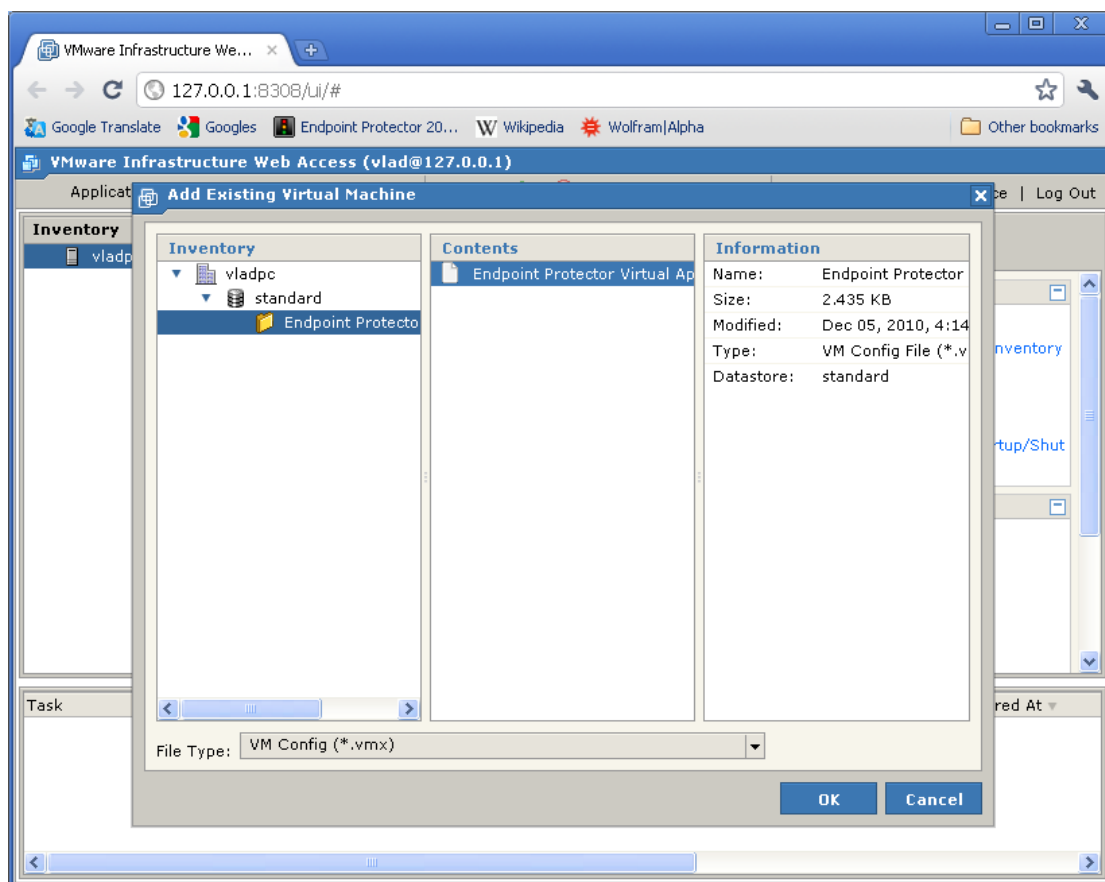
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored
2. Open your VMware Server web interface and login



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



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

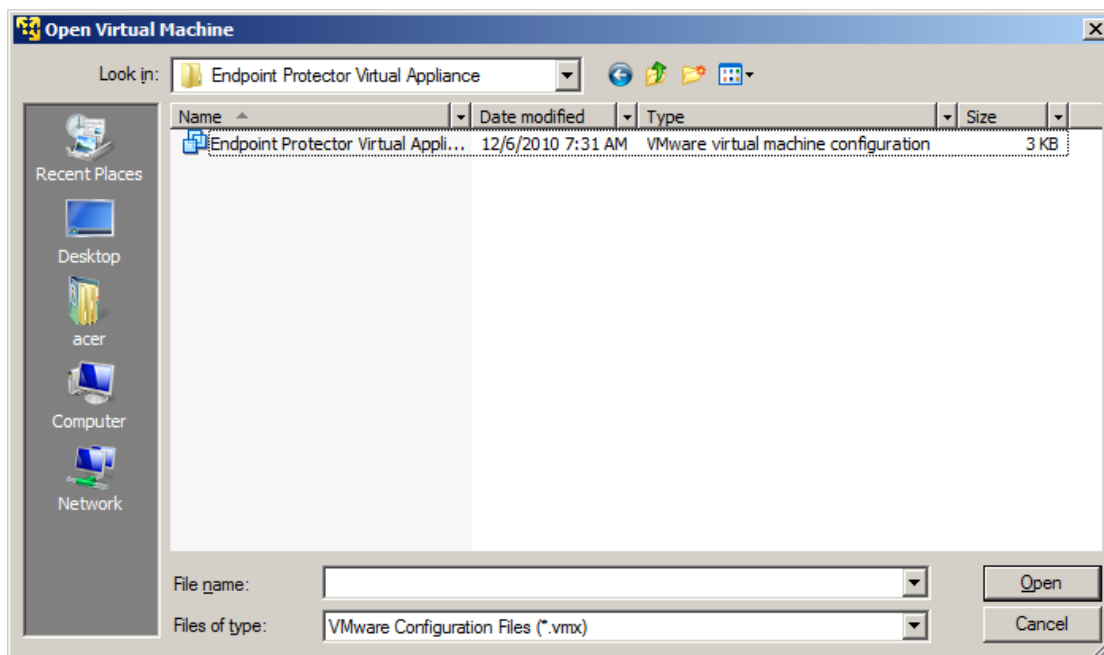
Please follow the Endpoint Protector Appliance User Manual from this point on.

3.2. Implementing in VMware Player 3.0 using VMX Format

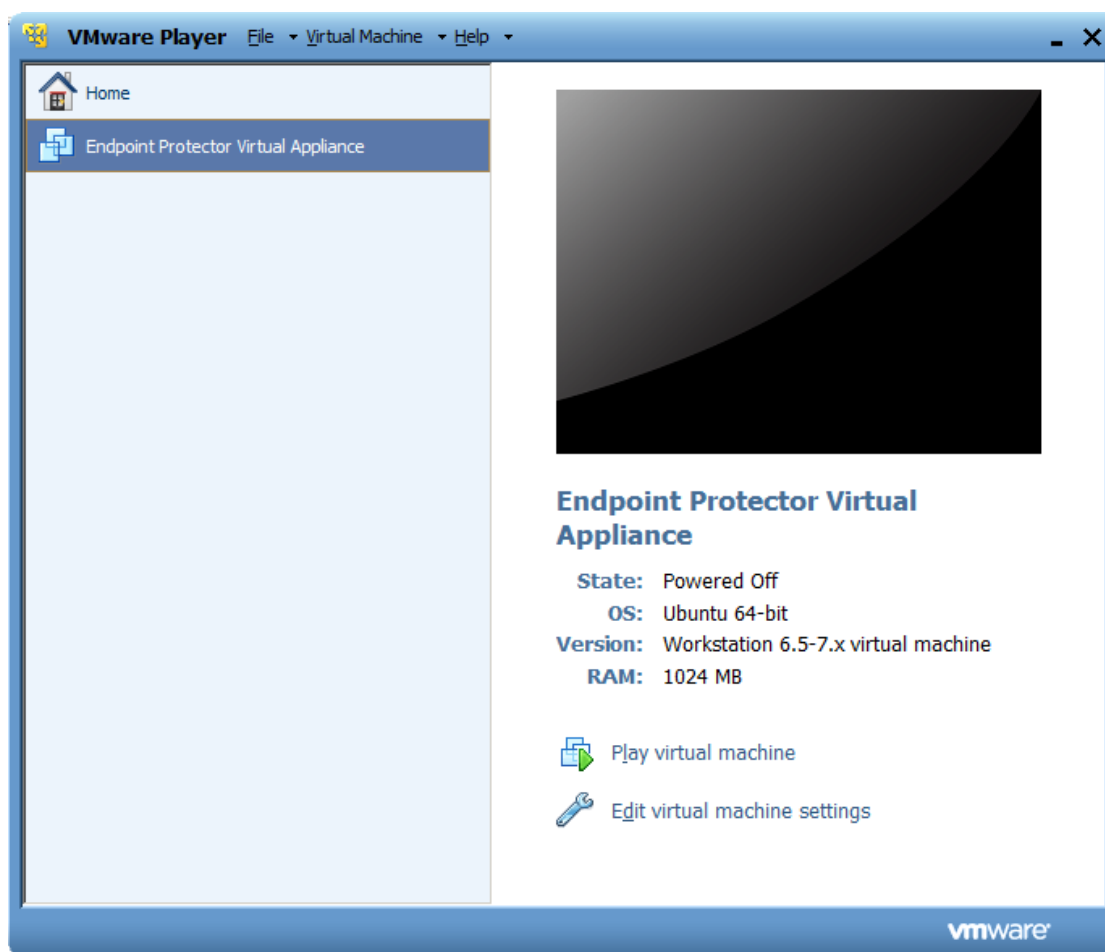
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored
2. Open VMware Player



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



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



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)



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

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

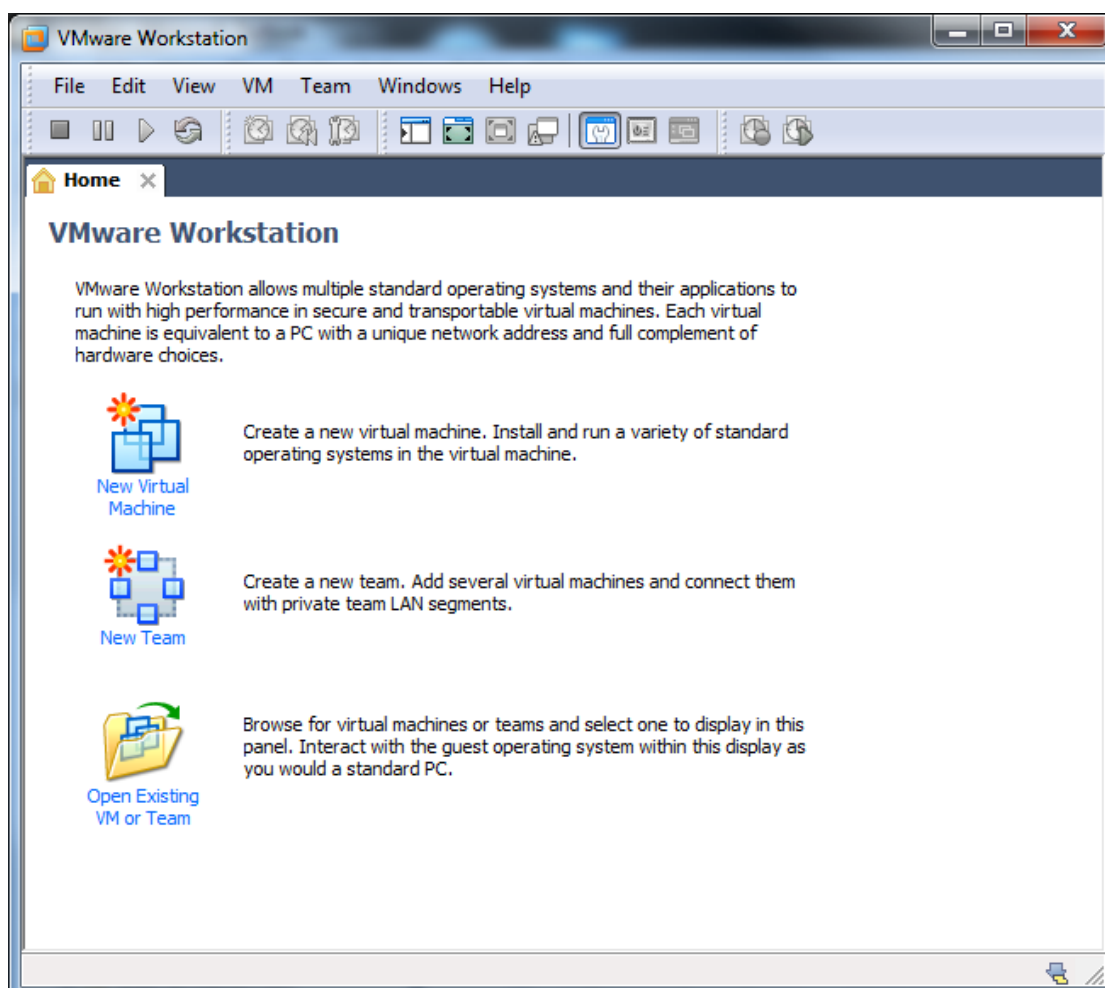
Note!

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

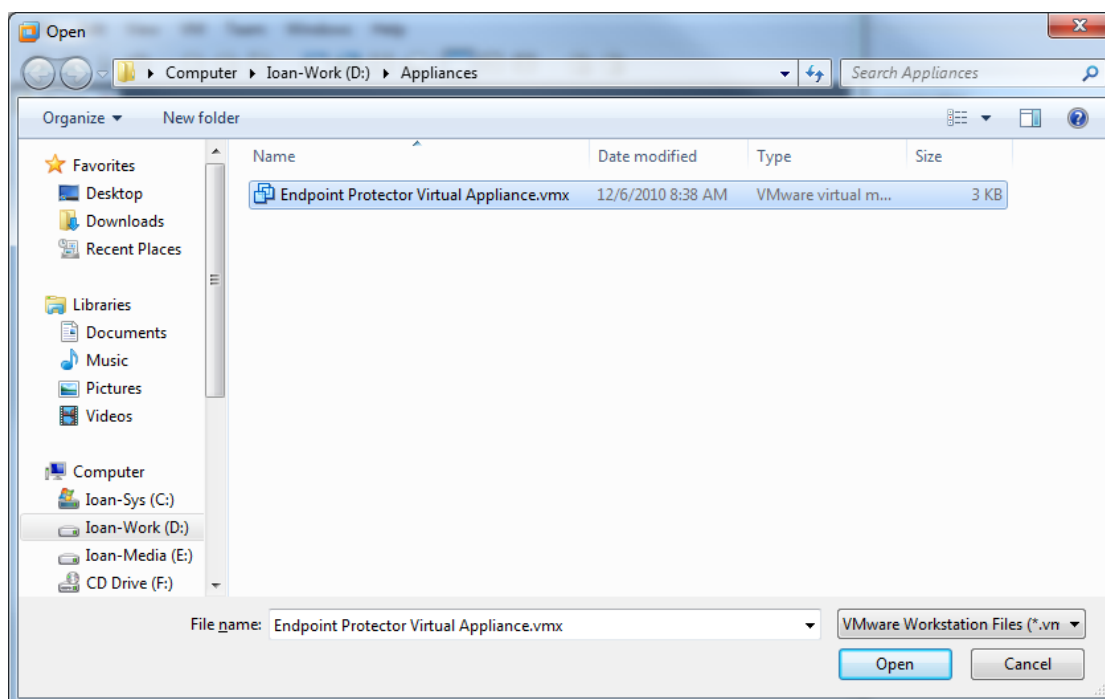
Do not shut down your computer while VMware Player is running.

3.3. Implementing in VMware Workstation 6.5 using VMX Format

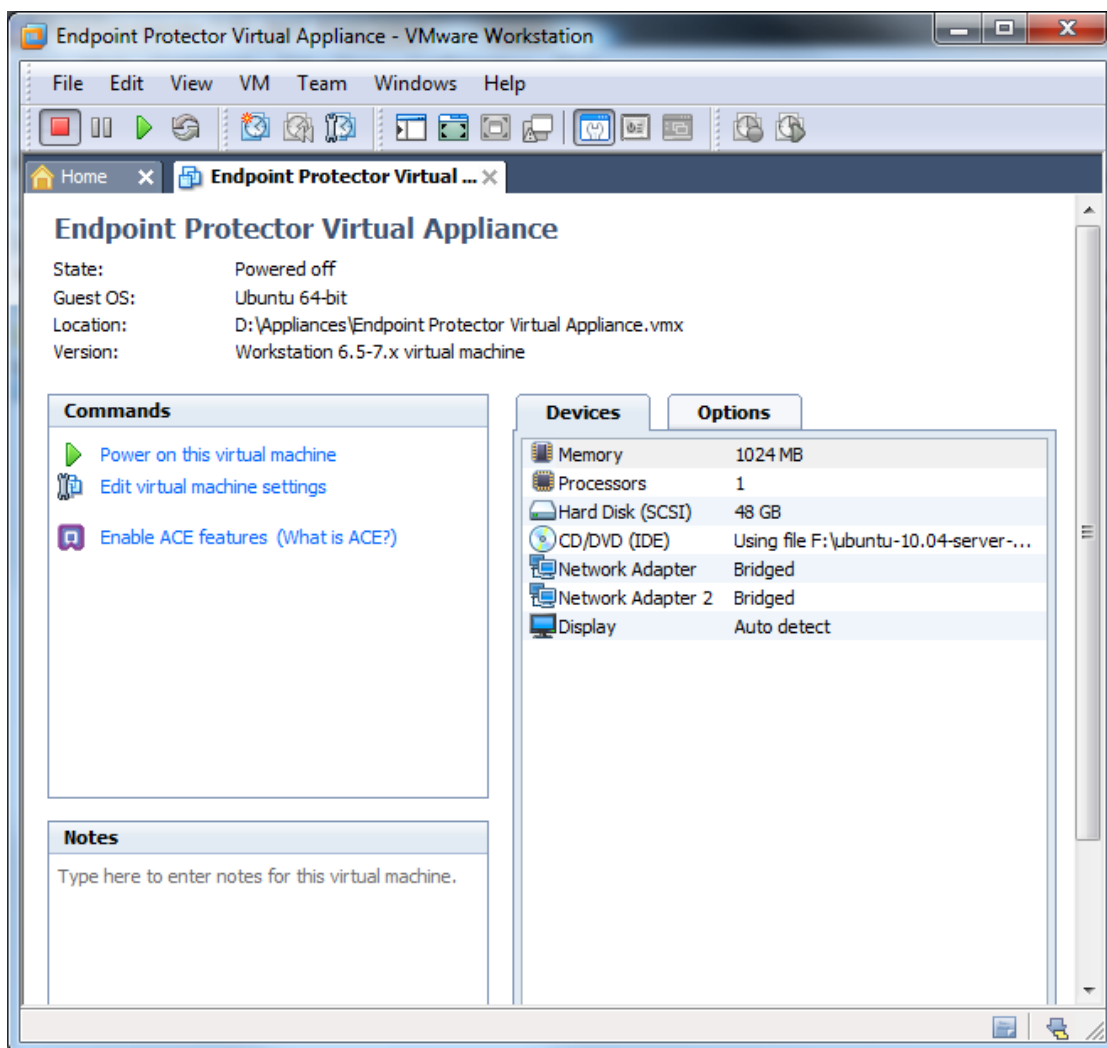
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored
2. Open VMWare Workstation



3. Select Open Existing VM or Team



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



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)



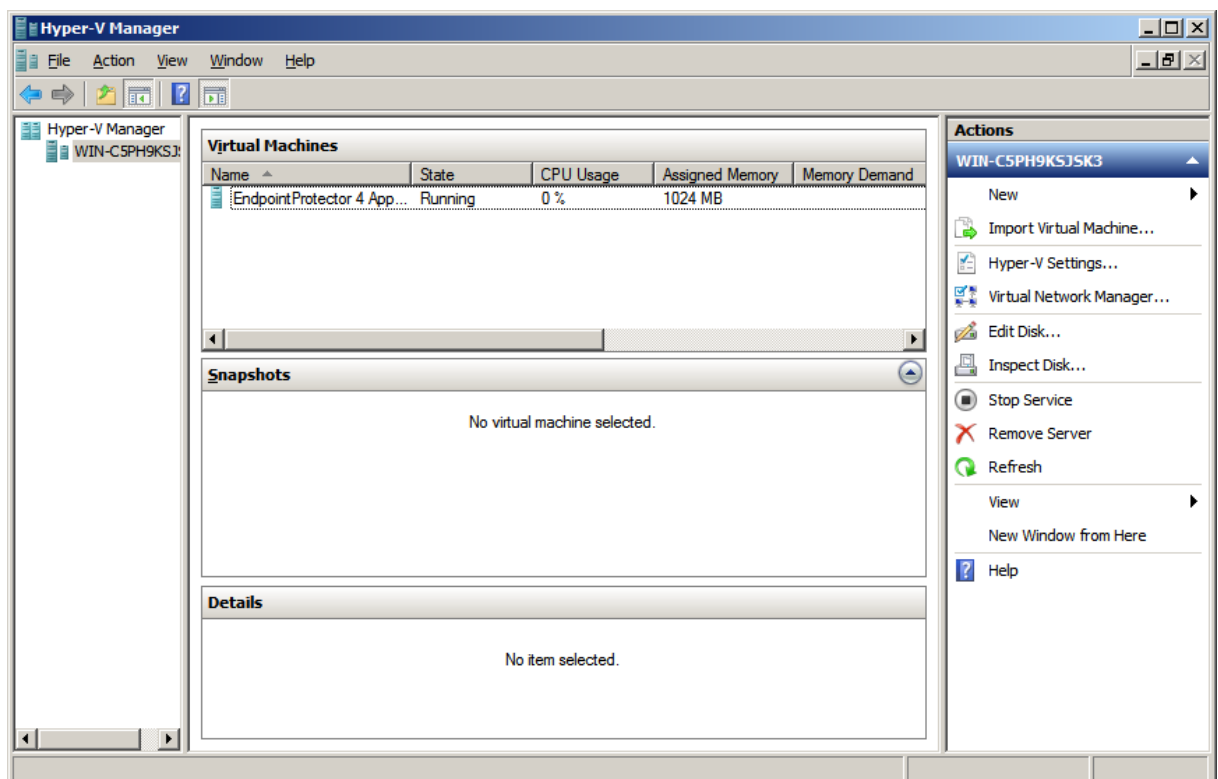
The Virtual Machine is started and ready for use.

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

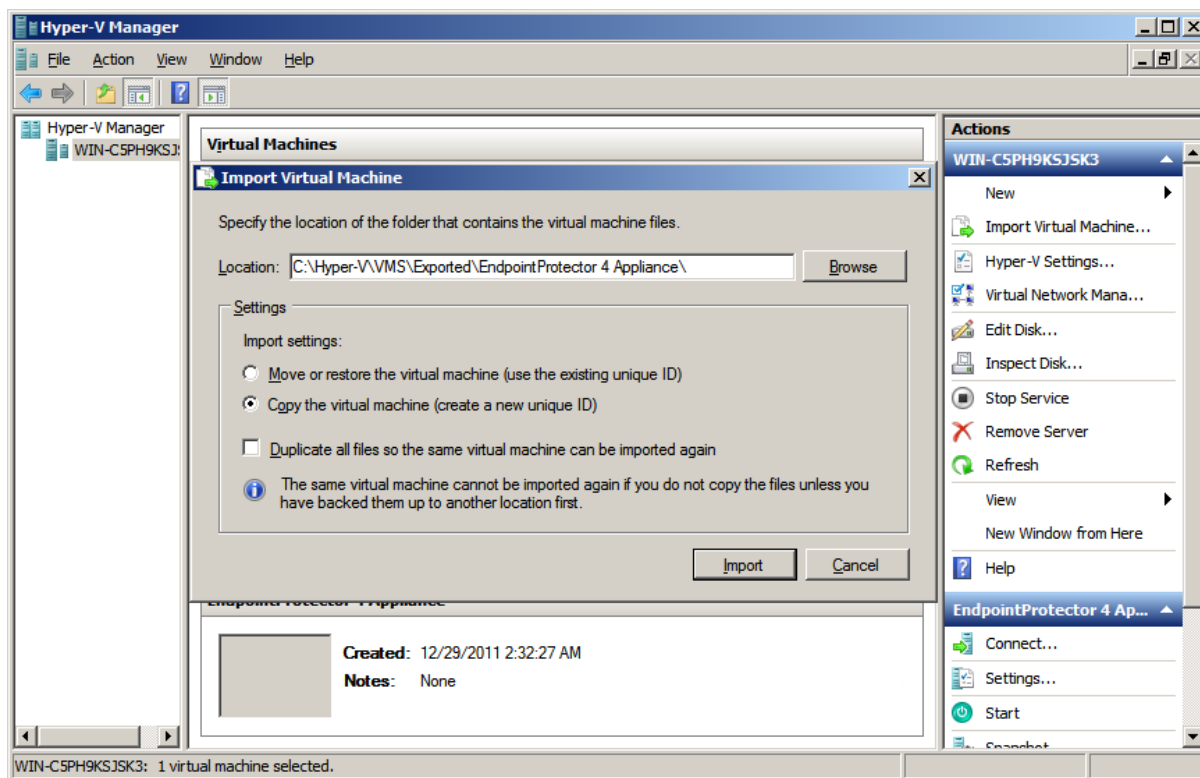
4. Implementing using VHD Format

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

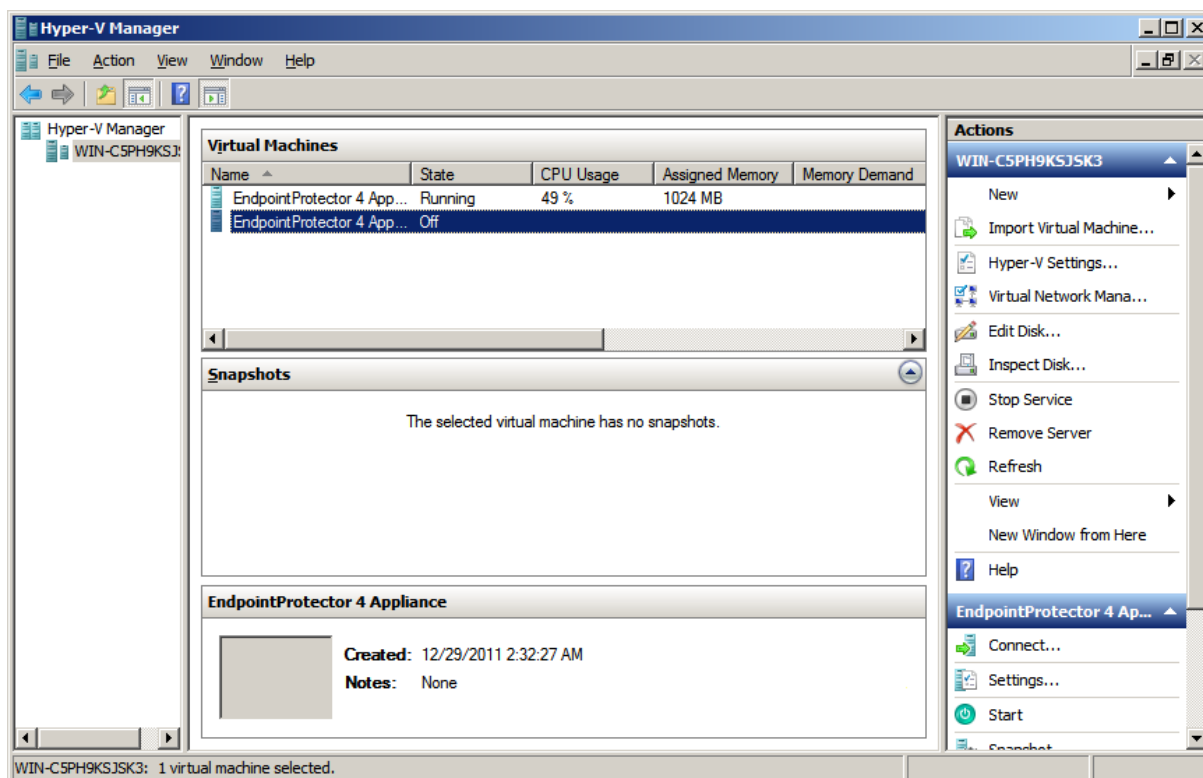


3. Select Import Virtual Machine Option from right side box



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

4. Press Import button



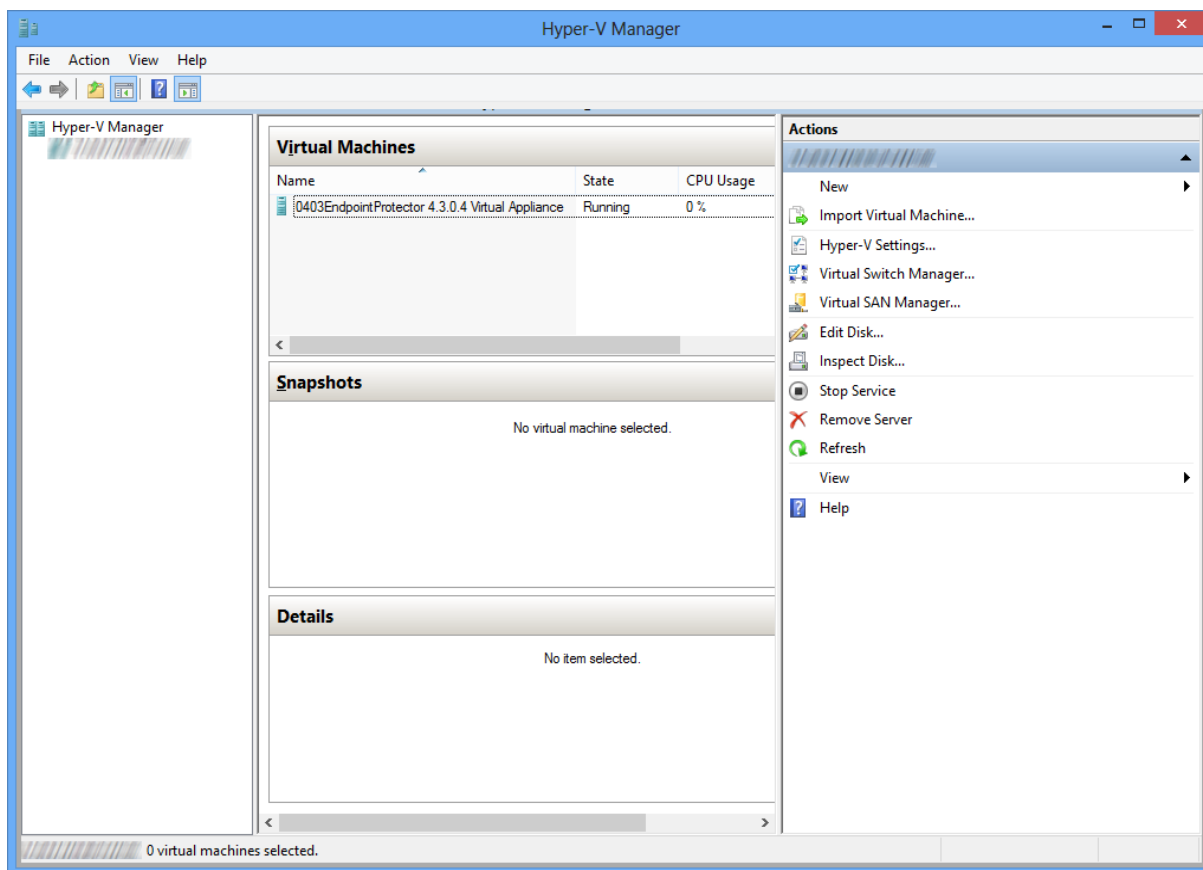
5. The new Virtual Machine will appear in the Virtual Machines list.

The Virtual Machine is started and ready for use.

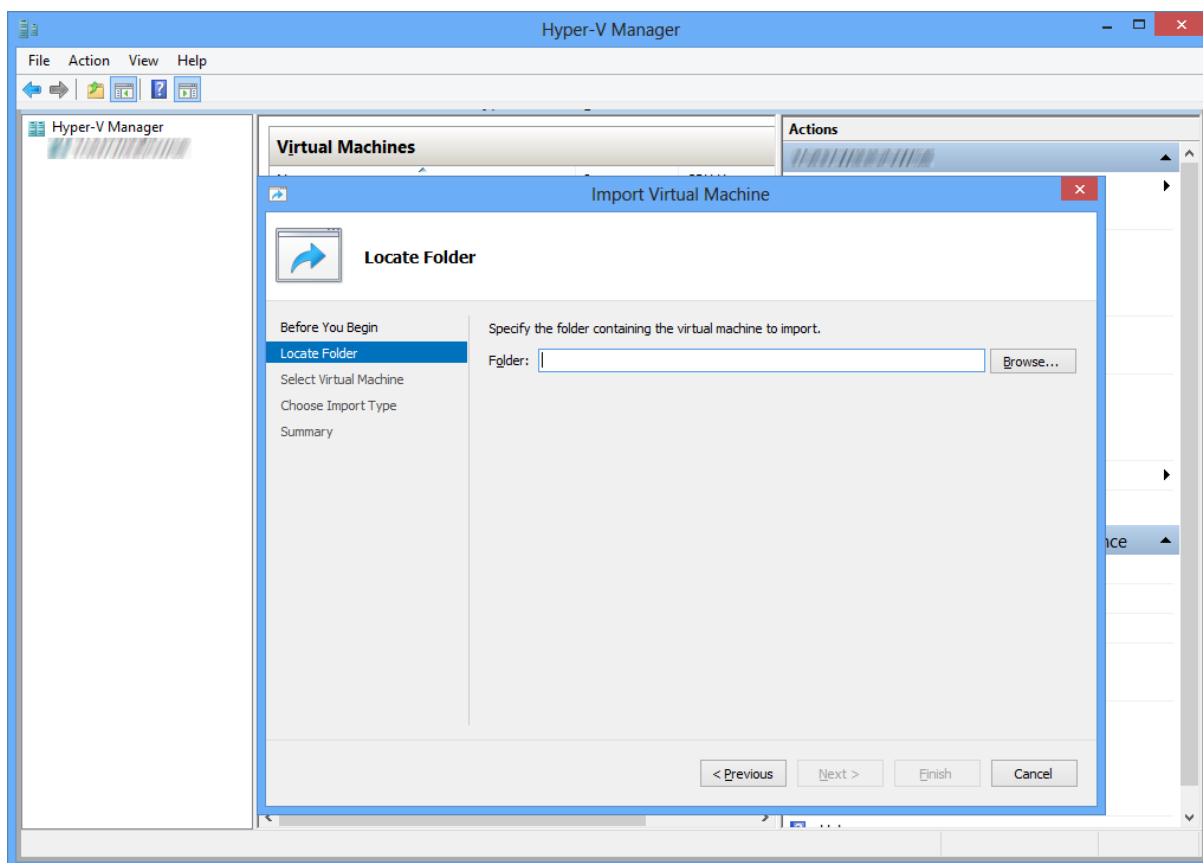
Please follow the Endpoint Protector Appliance User Manual from this point on.

Microsoft Hyper-V 2012 using VHD Format (not officially supported)

1. Extract the downloaded Endpoint Protector Virtual Appliance zip package
2. Start Hyper-V Manager

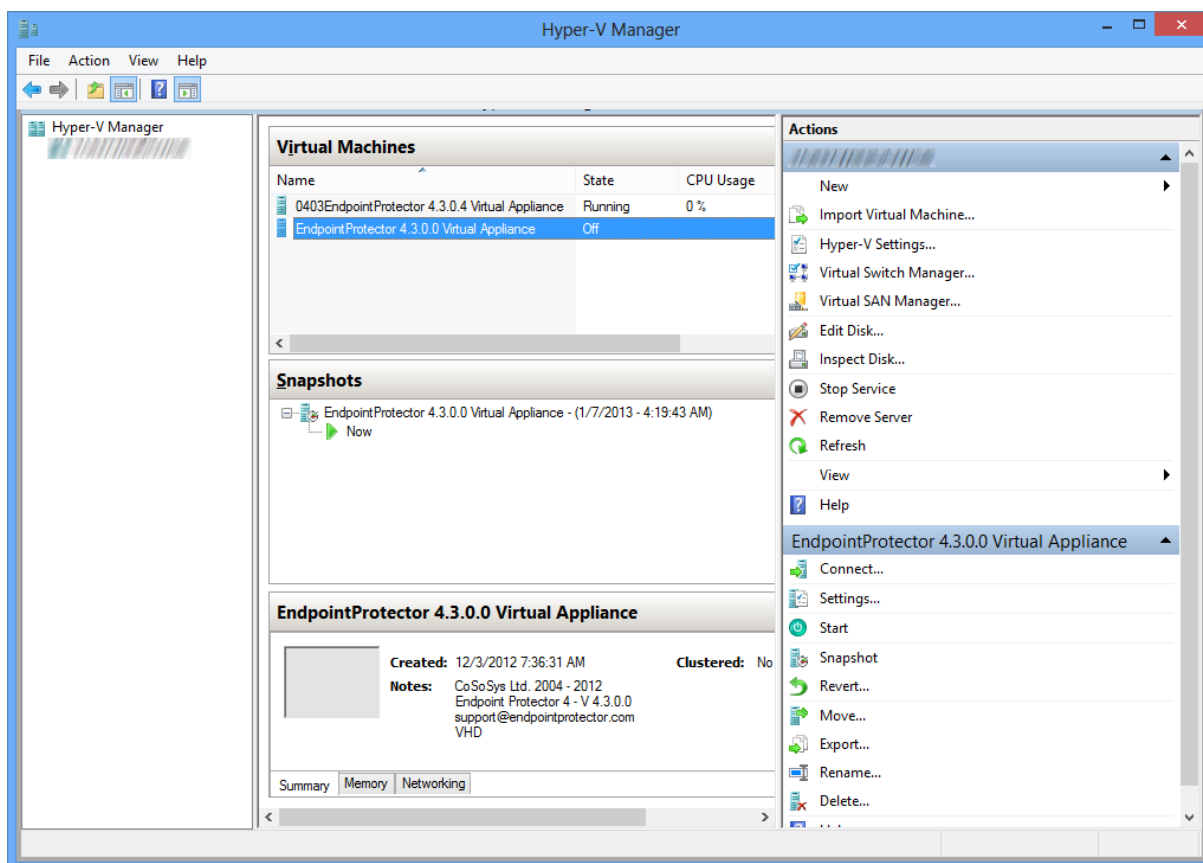


3. Select Import Virtual Machine Option from right side box



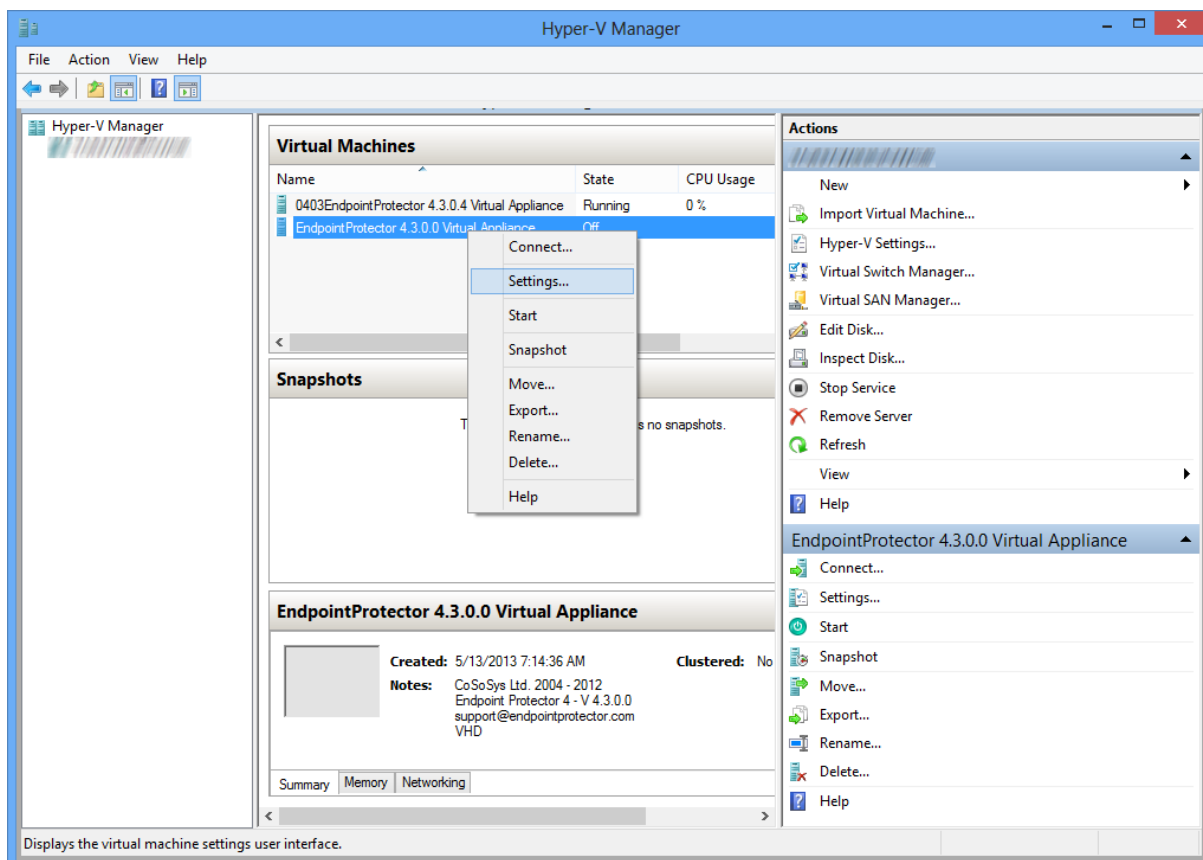
Select the folder which contains the Appliance folders/files.
Choose Copy the virtual machine as Import Type.

4. Go through the importing options, then press Finish button

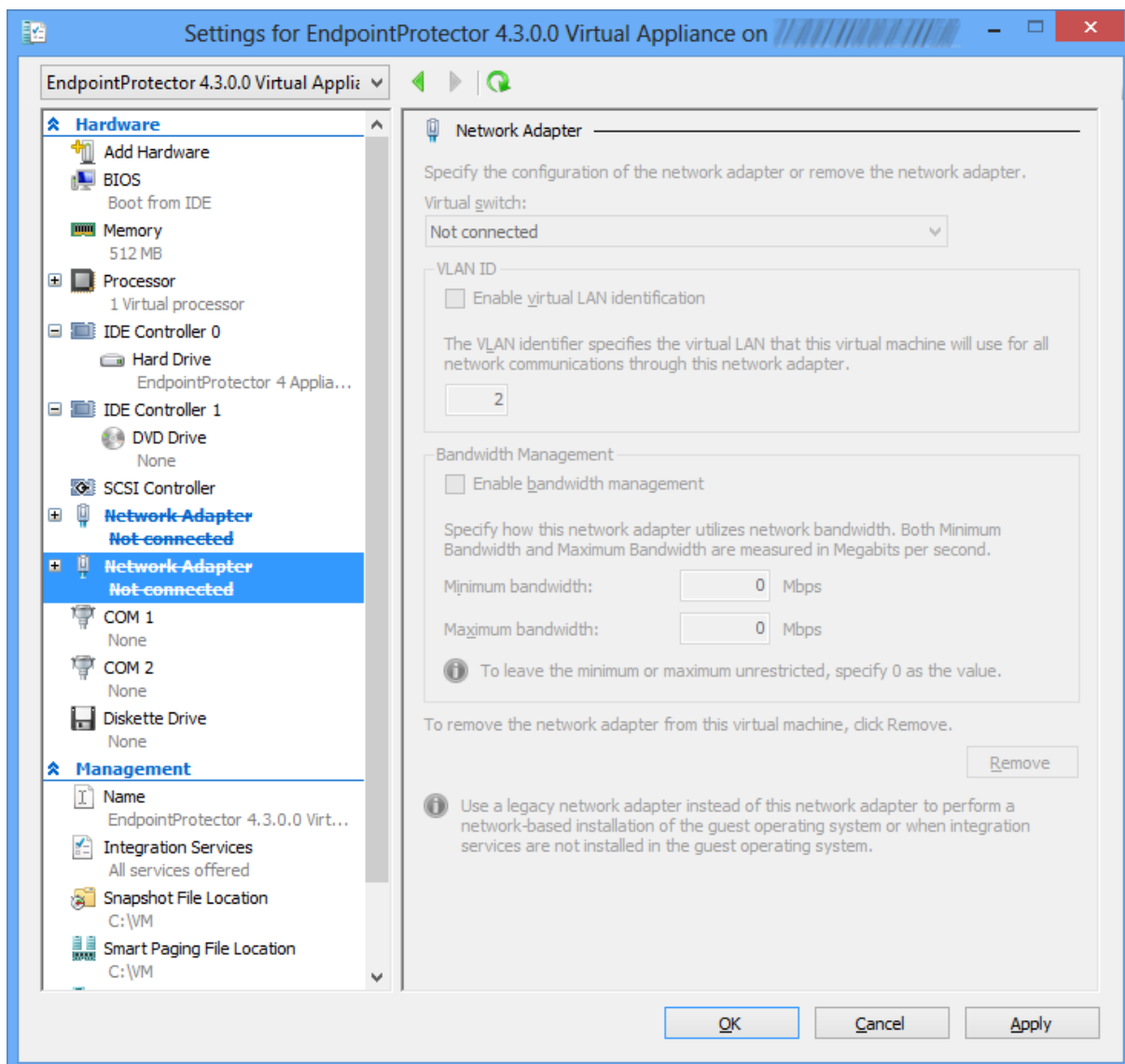


The new Virtual Machine will appear in the Virtual Machines list.

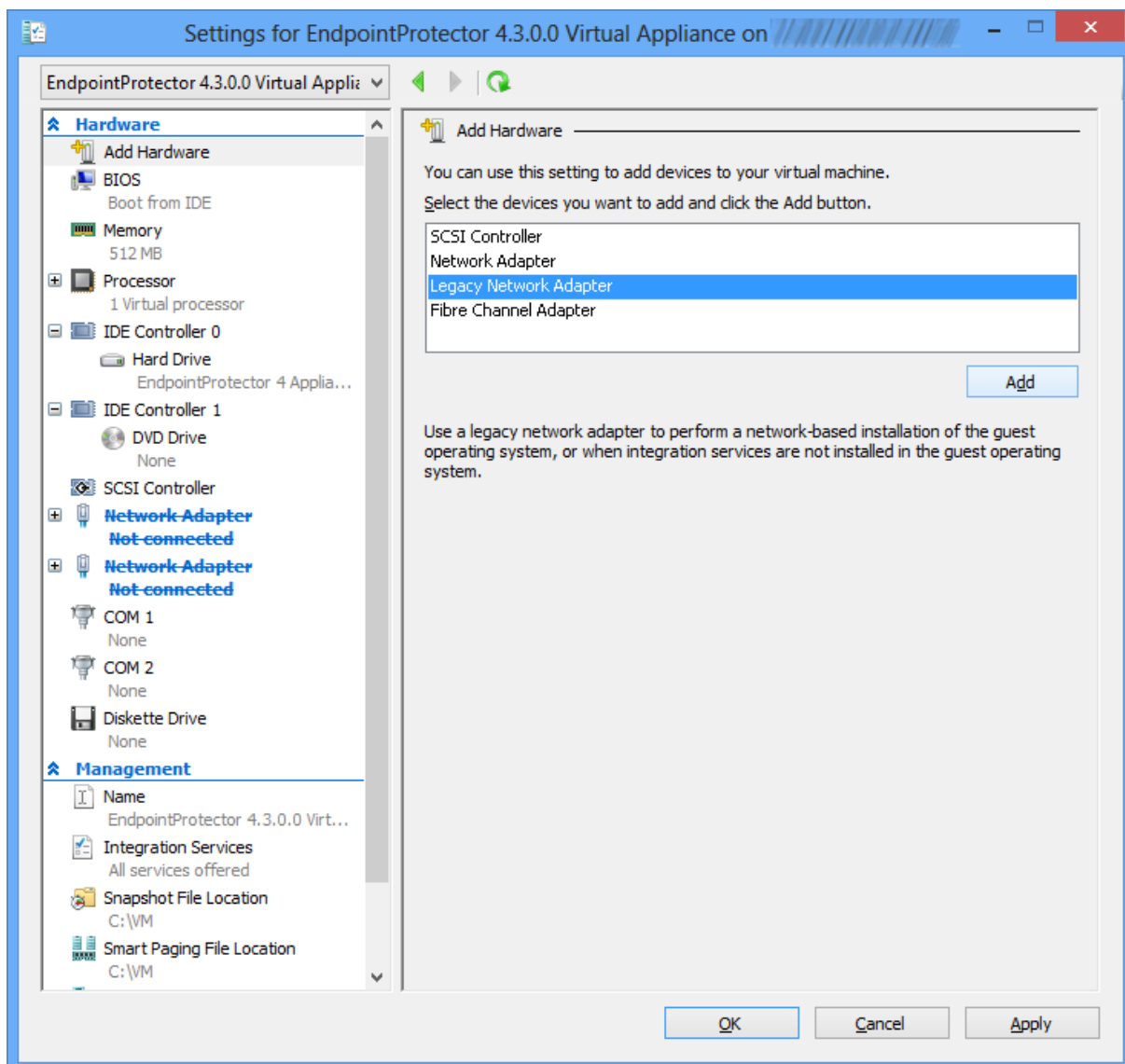
5. Right click on the new Virtual Machine and select settings...



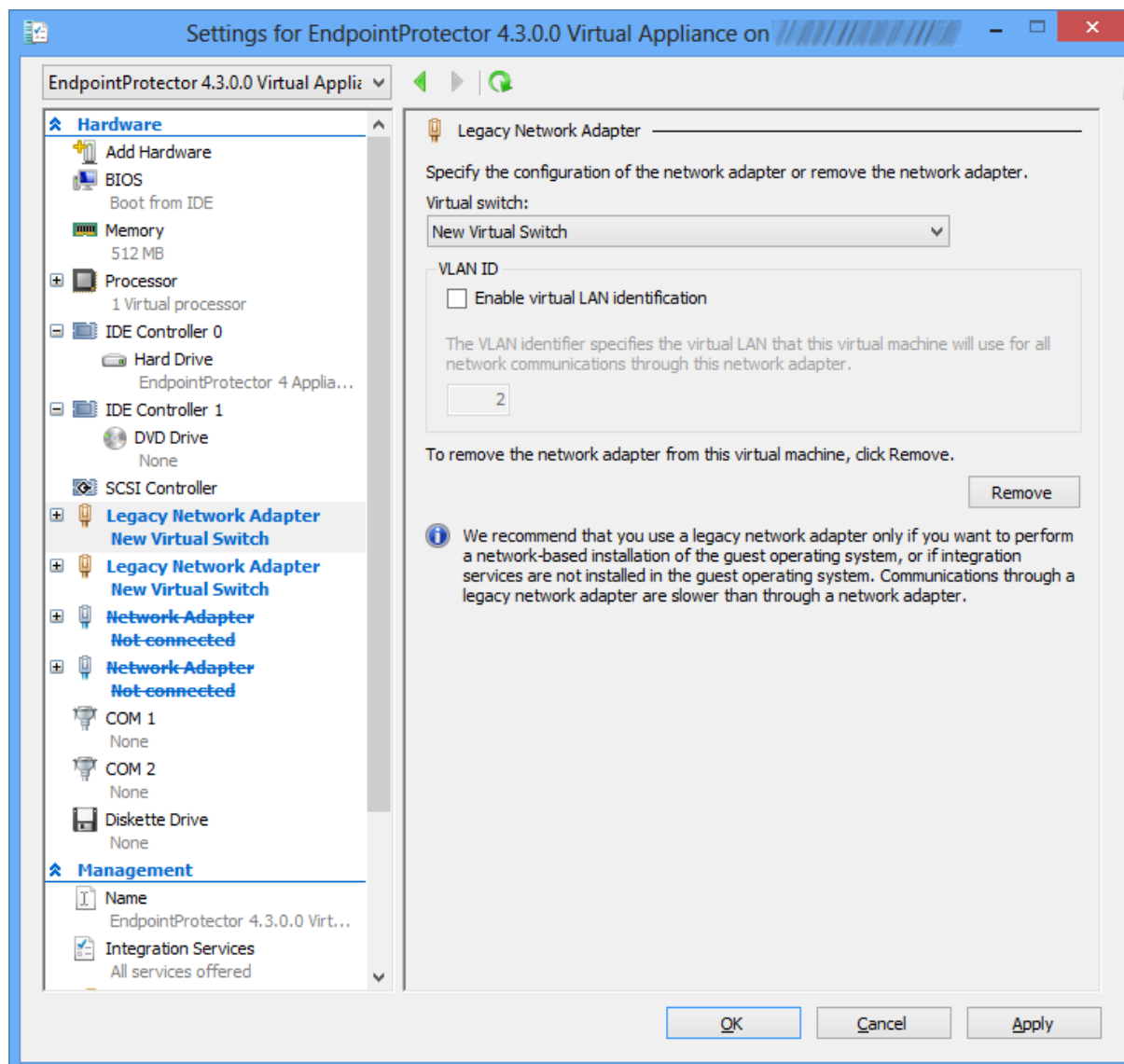
6. Remove the two existing network adapters from the left side box



7. Add two Legacy Network Adapters from the add hardware command.



8. Select from virtual switch field, "new virtual switch" for both adapters.



9. Click on OK.

The Virtual Machine is now imported and ready to use.

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

Note! In case you experience problems 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:

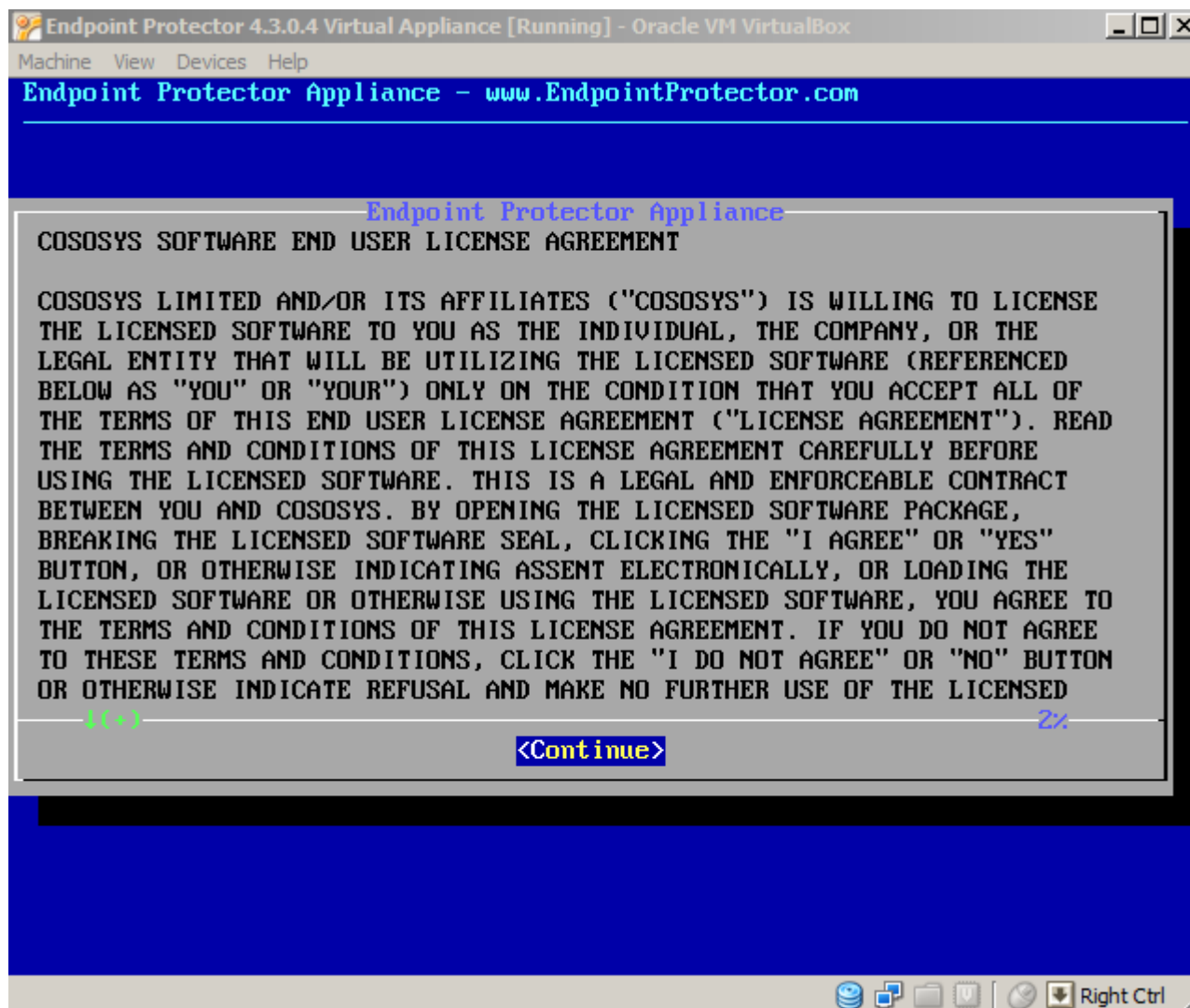
- Server and Client: 443

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

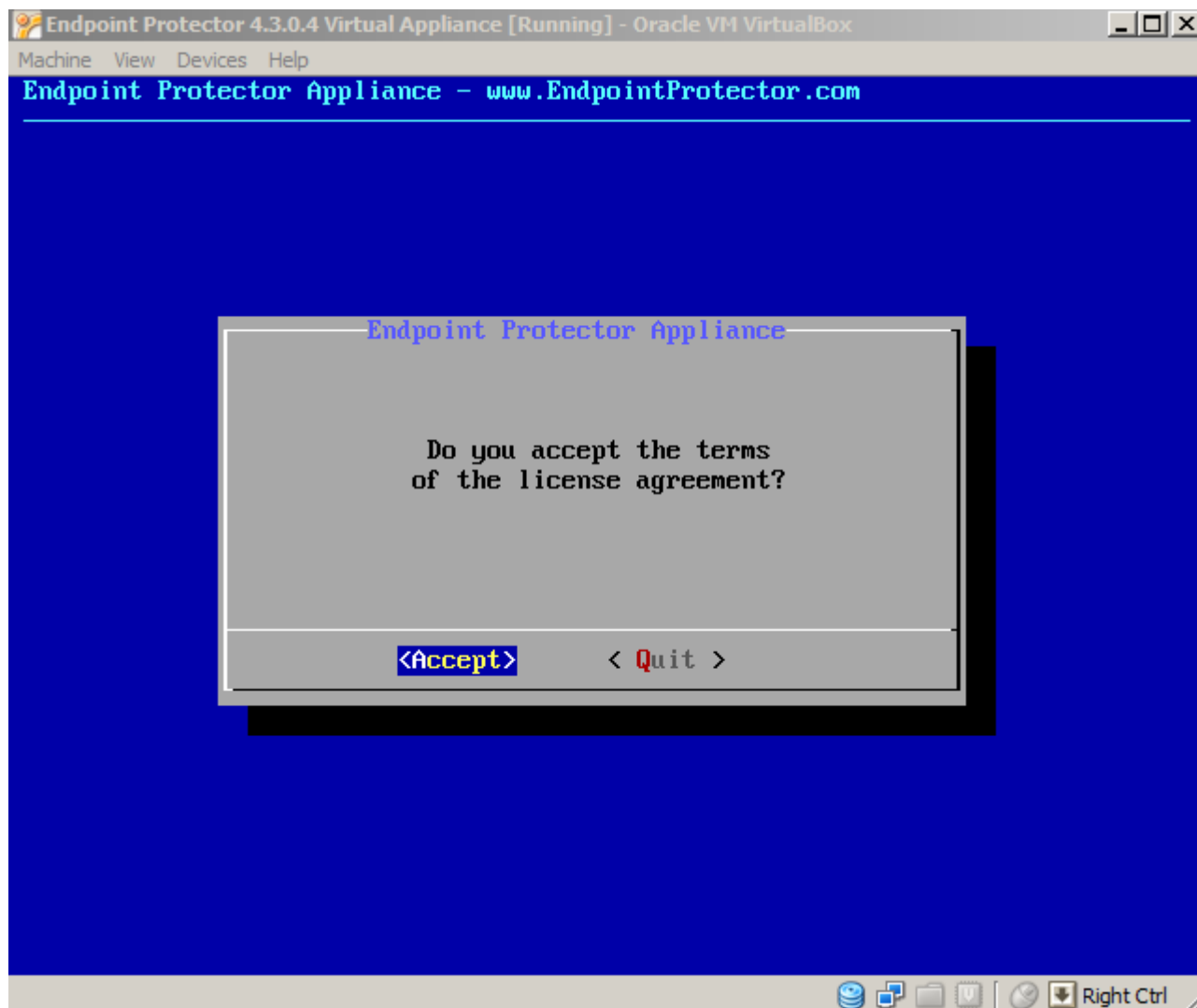
- MDM Cloud (cloud.endpointprotector.com): 443

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

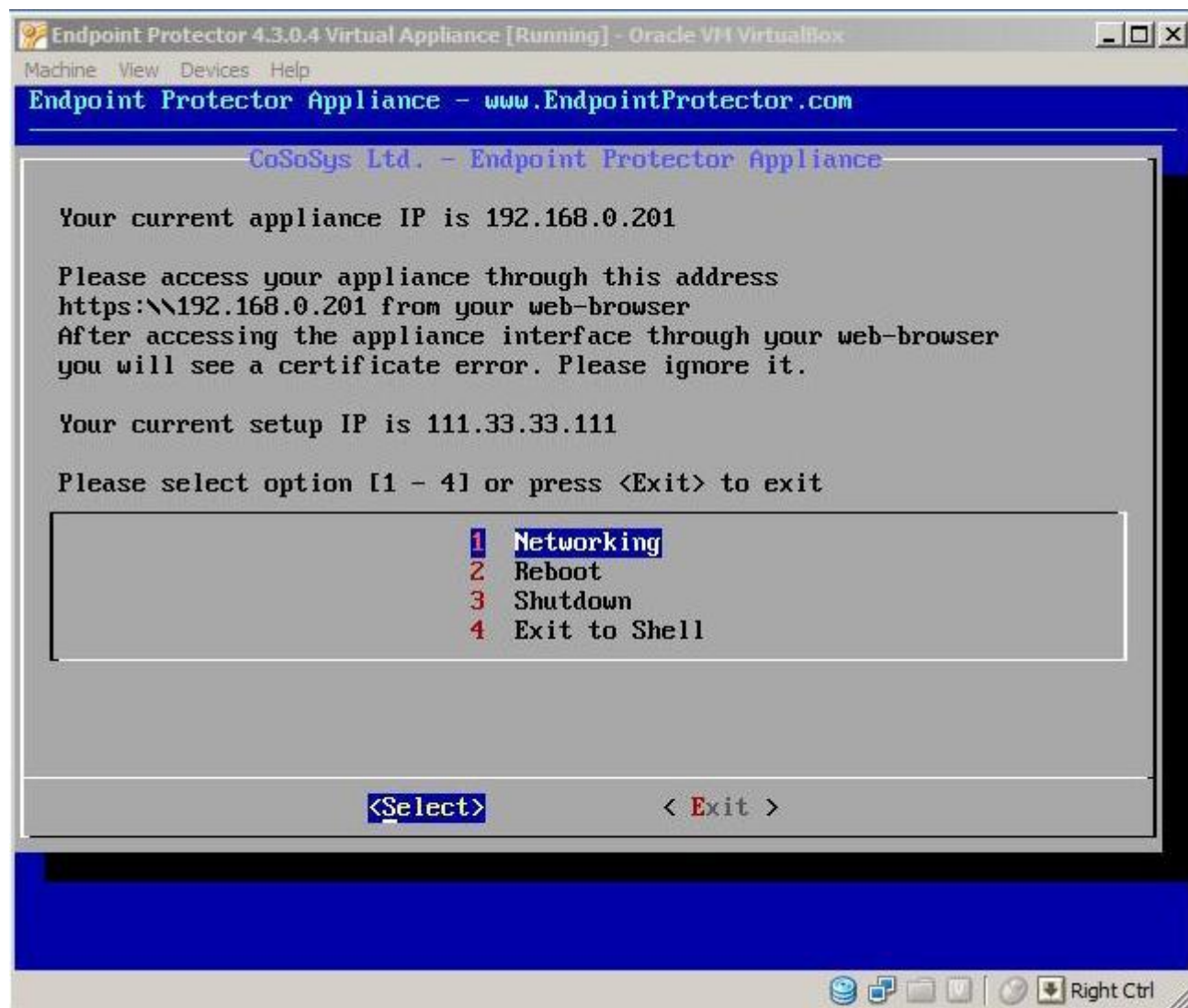
1. Press Continue when finished reading the End User License Agreement



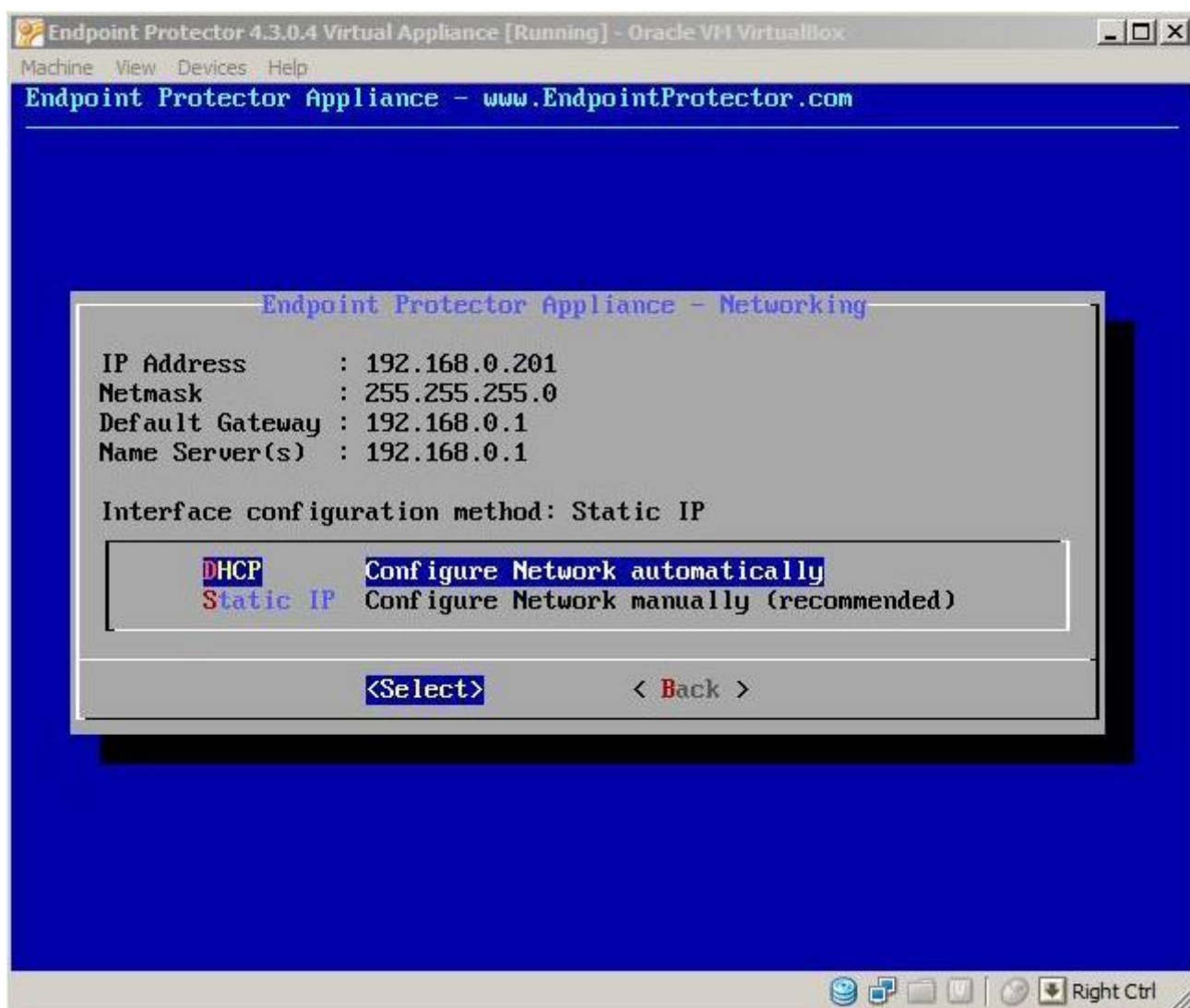
2. Press Accept



3. Select Networking



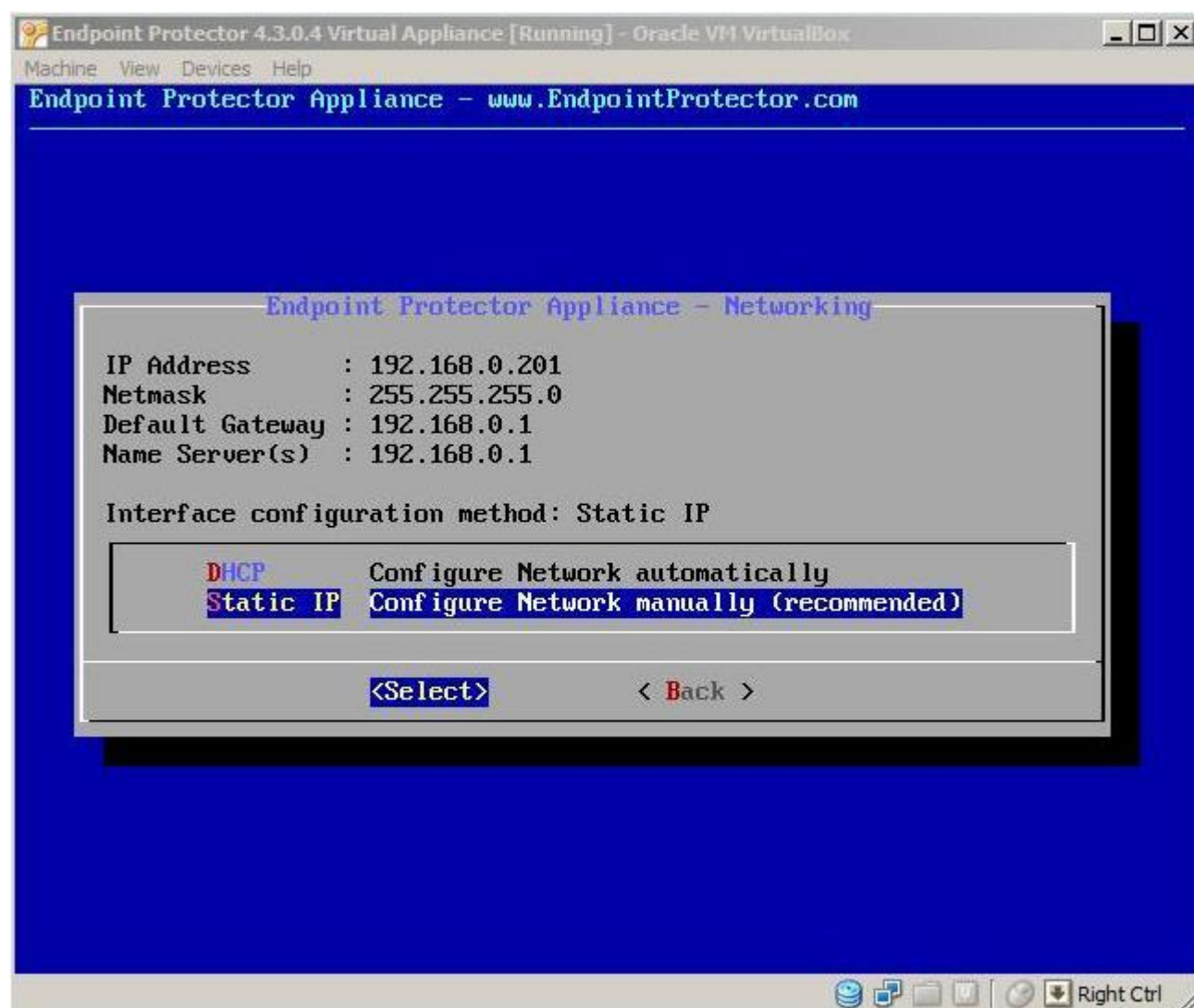
4. The configuration methods are now available.



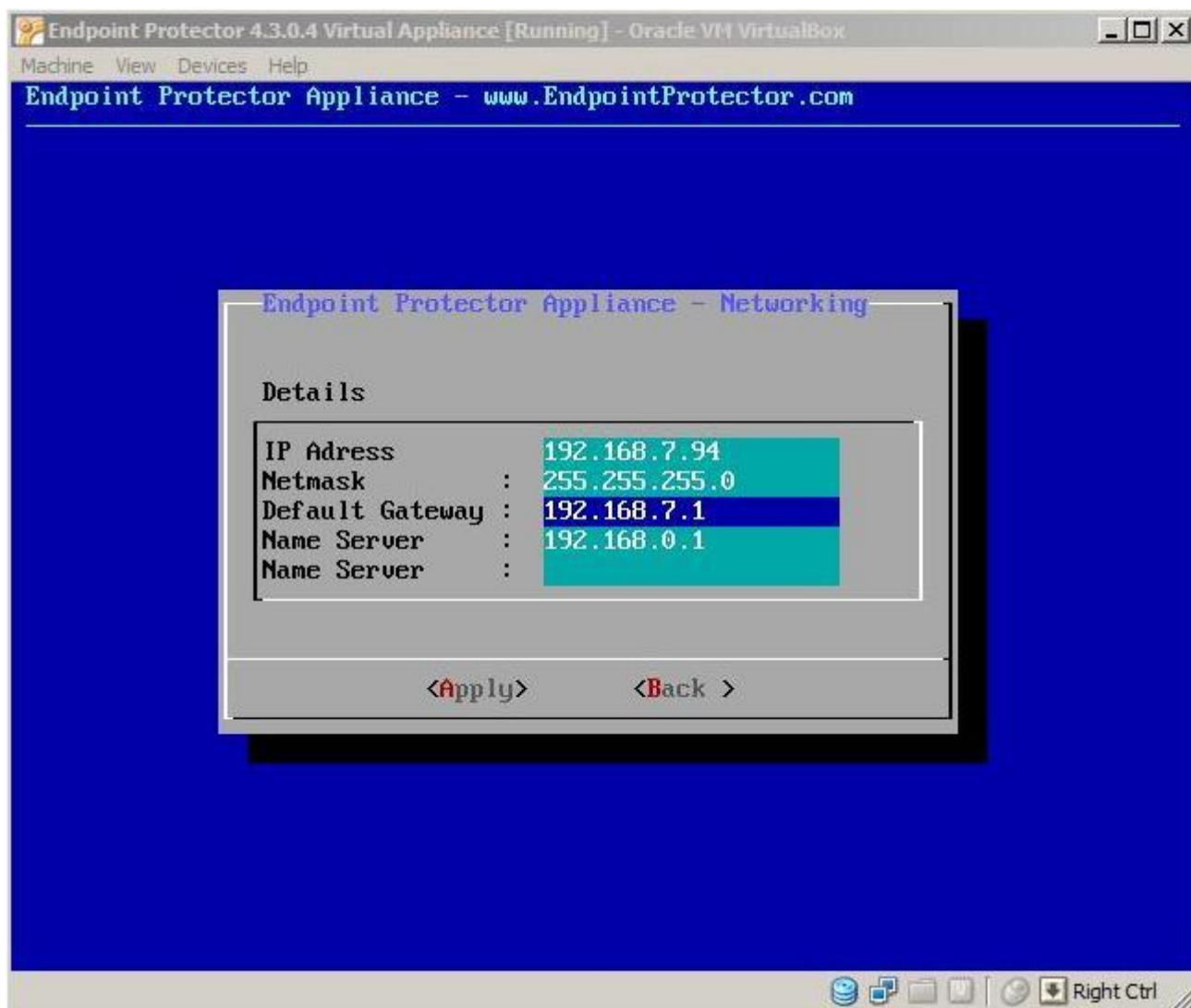
Note! We recommend to configure your network manually!

5.1.1 Manual configuration

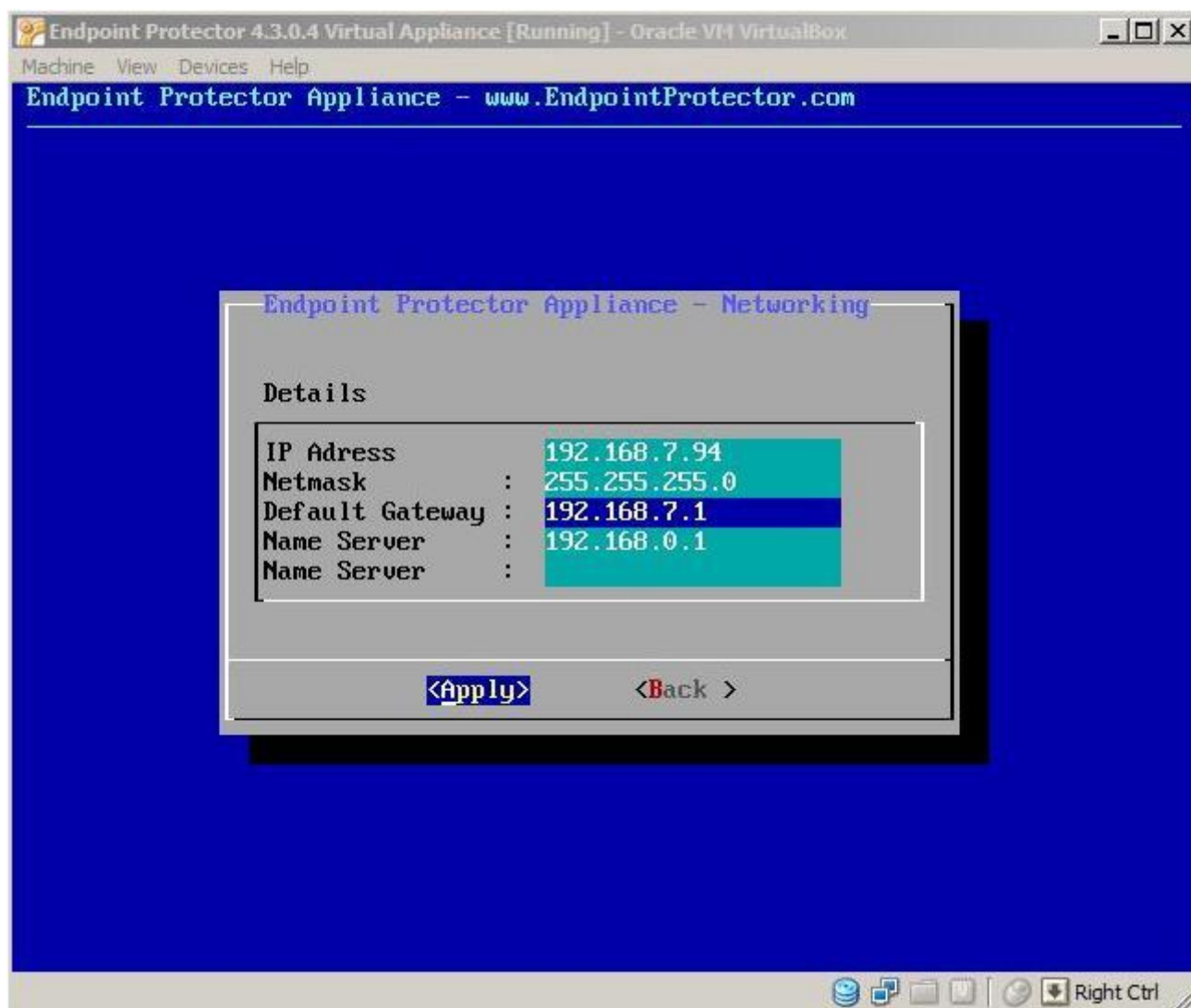
1. Select Configure Network manually(recommended)



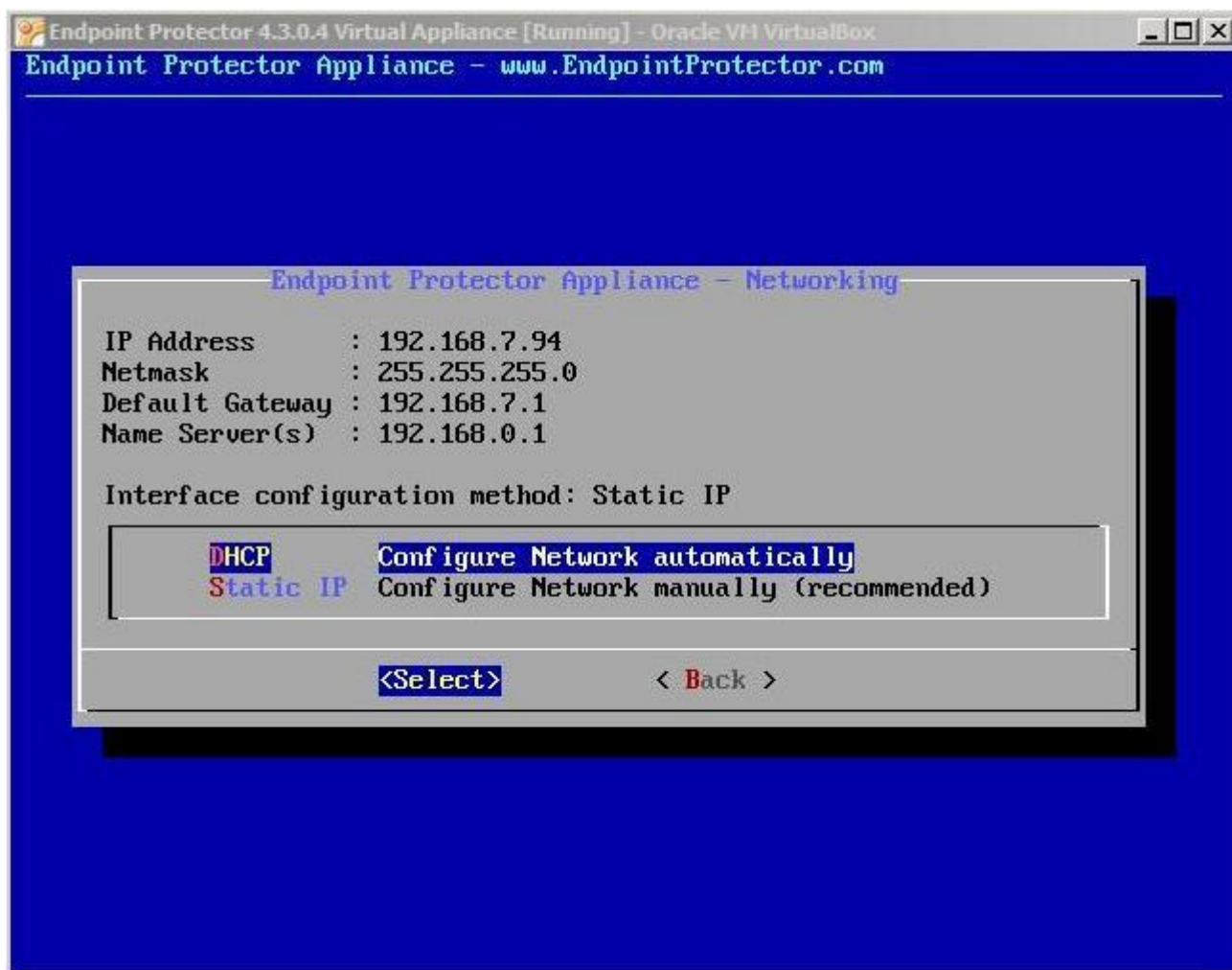
2. Set up the IP Address, and Default Gateway (in our example we set the IP Address as 192.168.7.94 and the Default Gateway as 192.168.7.1).



3. Press Tab



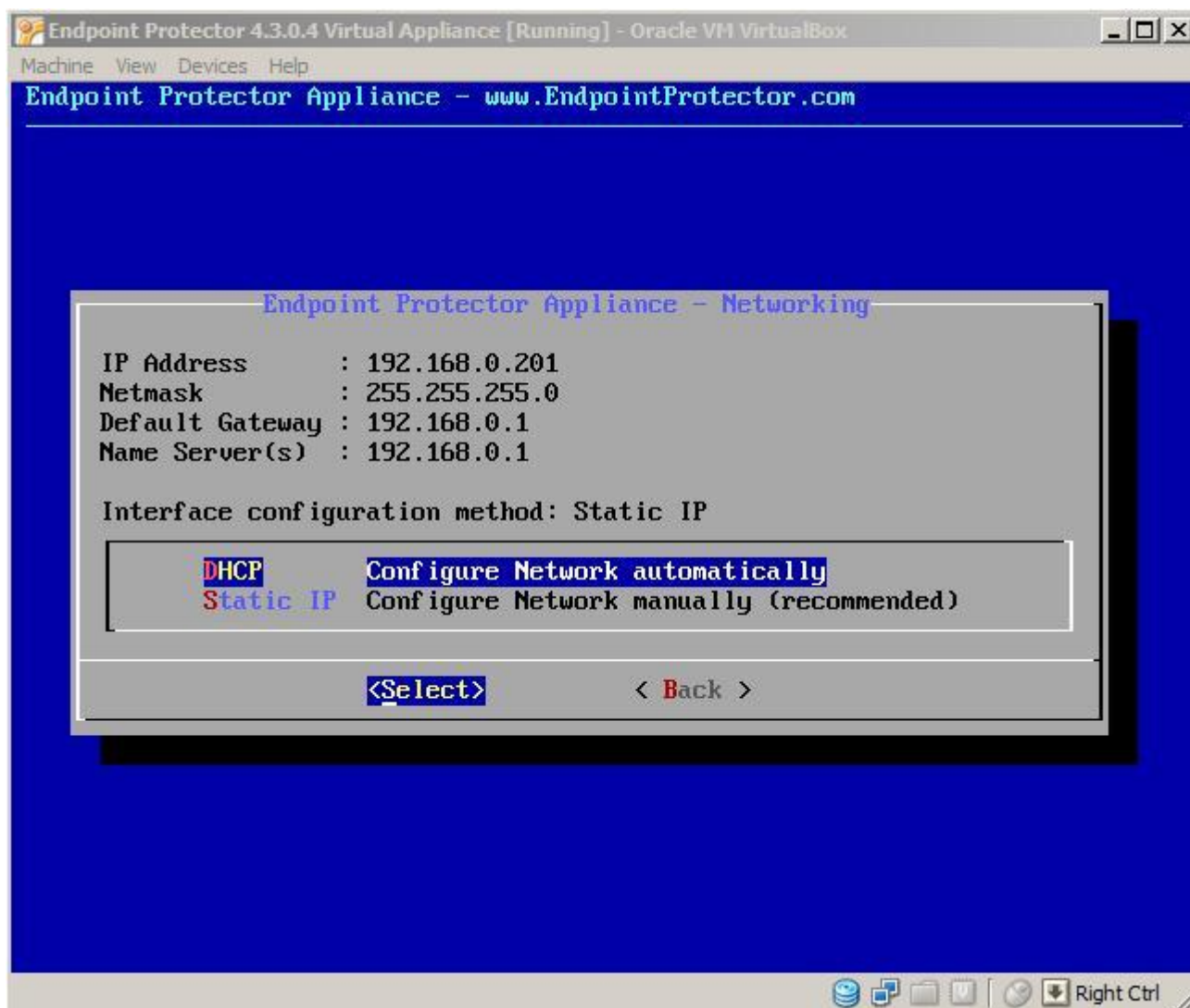
4. Press Enter



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.



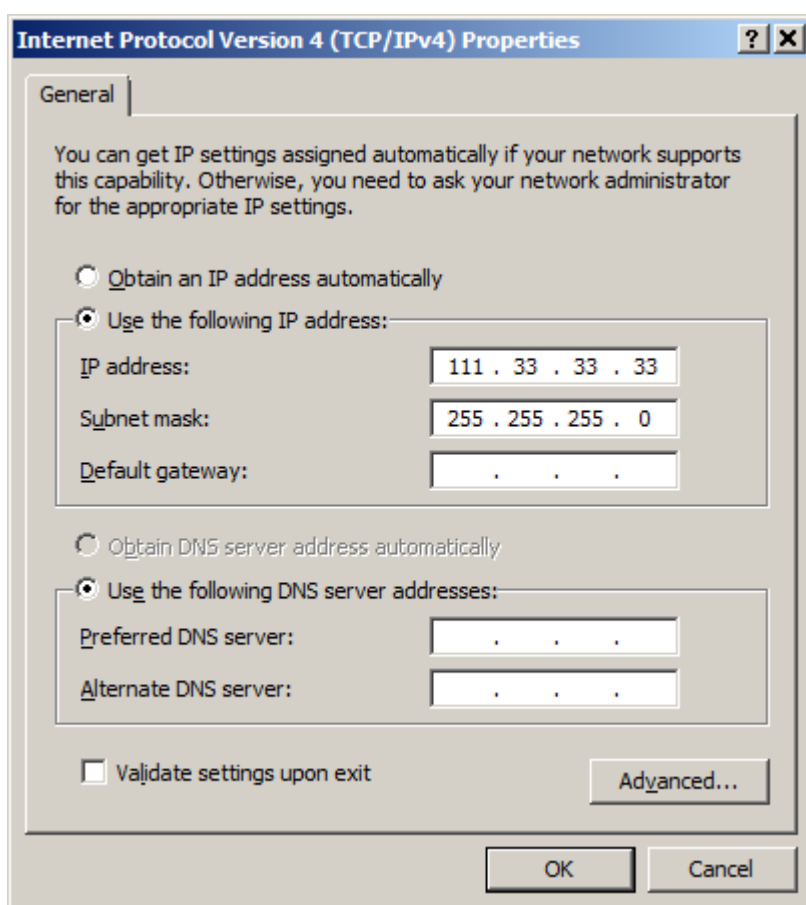
5.2. Hardware Appliance Setup Wizard

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

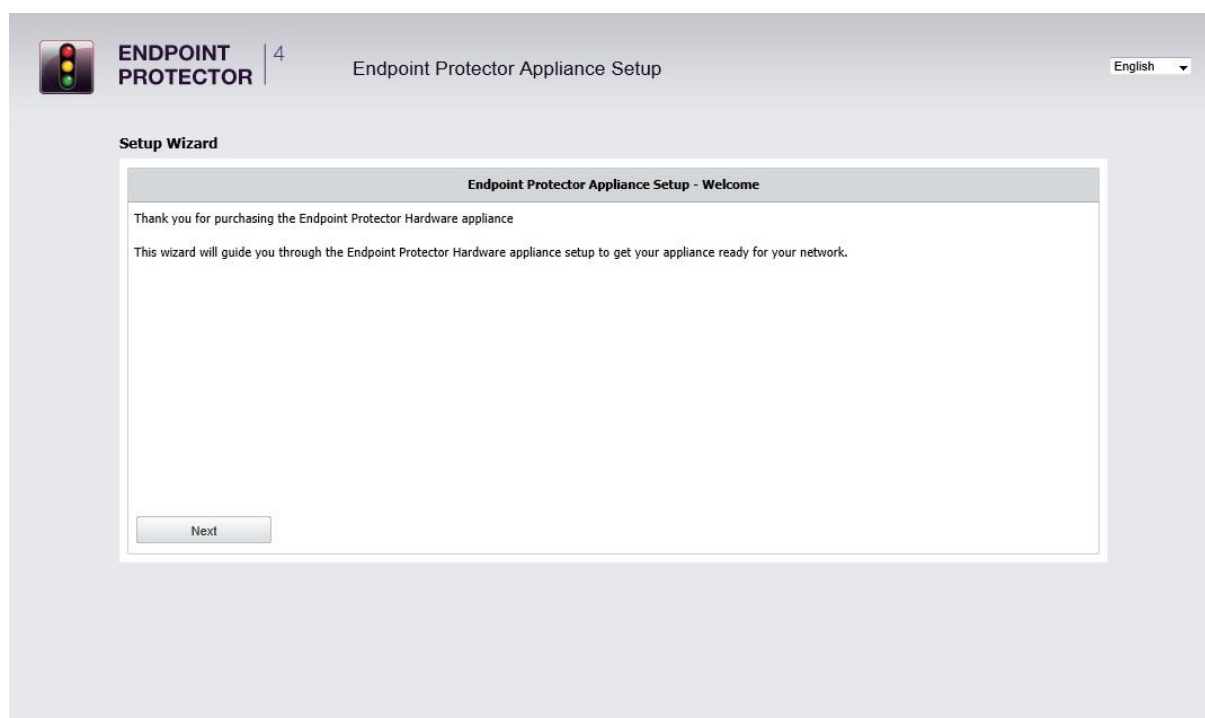


Then access it through your internet browser by typing the following IP

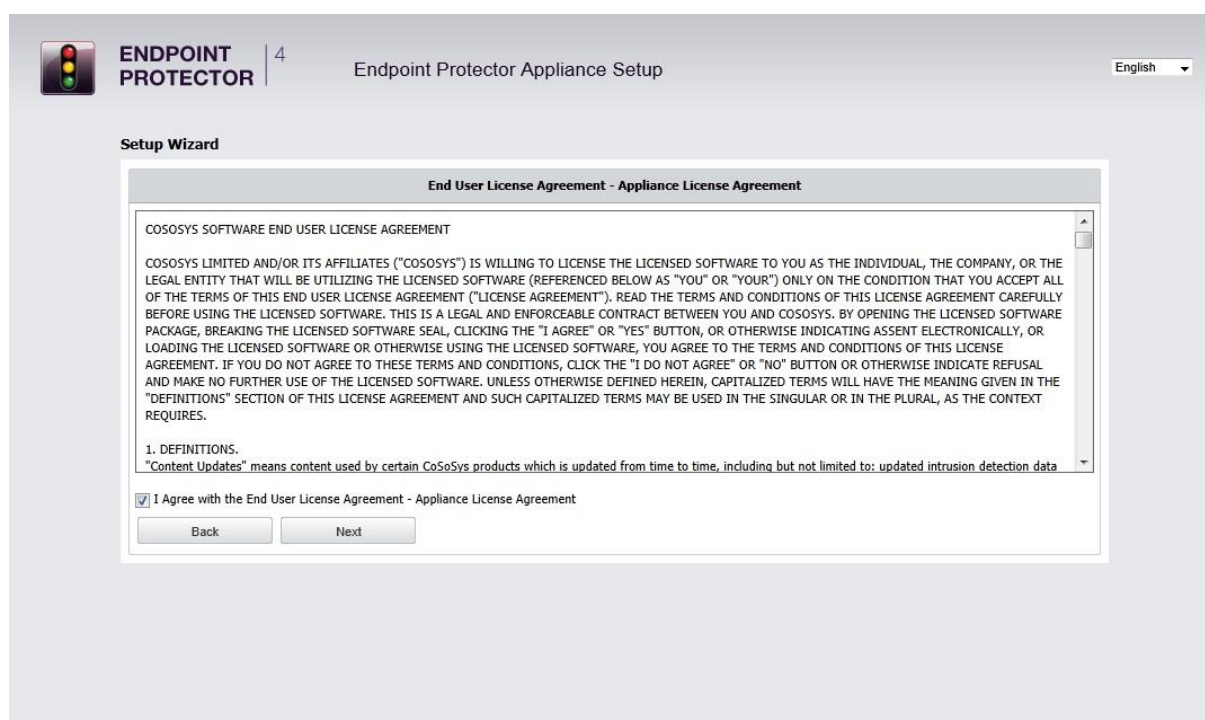
http://111.33.33.111 in the URL bar.

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.

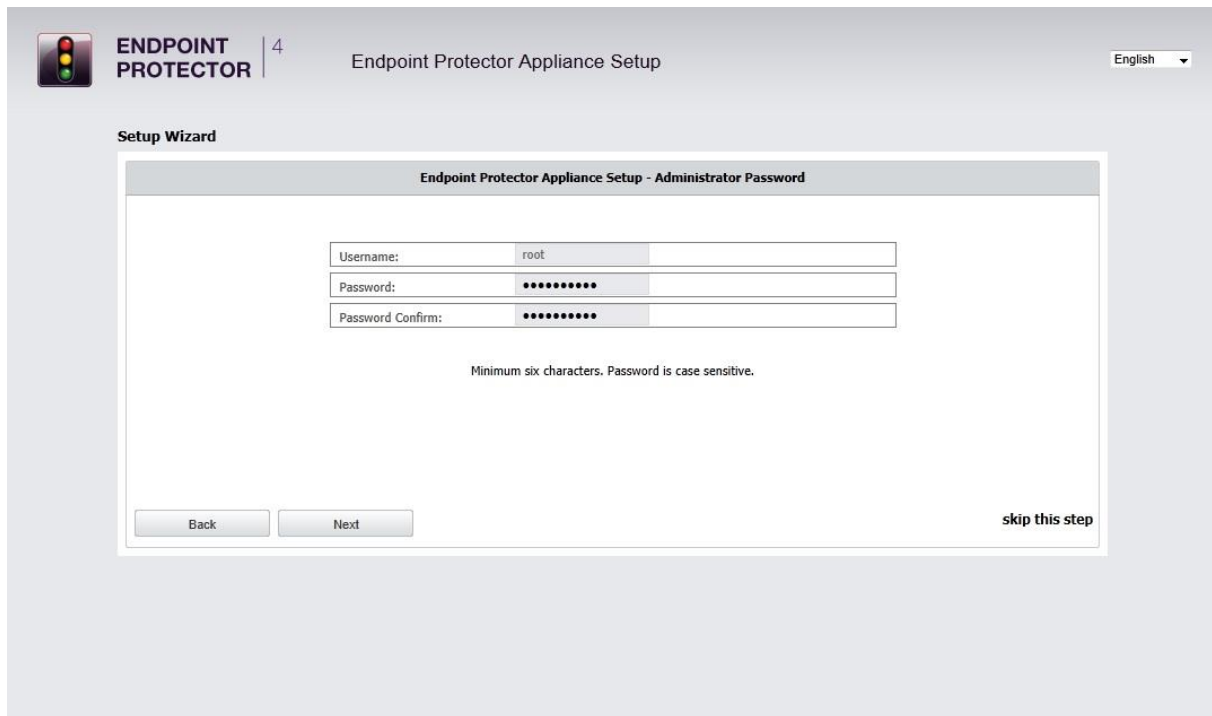


5.2.1. End User License Agreement - Appliance License Agreement



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

5.2.2. Define your Appliance Administrator Password



The screenshot shows the 'Endpoint Protector Appliance Setup - Administrator Password' window. At the top left is the 'ENDPOINT PROTECTOR' logo with a step indicator '4'. The title bar reads 'Endpoint Protector Appliance Setup'. In the top right corner, there is a language dropdown menu set to 'English'. Below the title bar, the text 'Setup Wizard' is visible. The main content area contains three input fields: 'Username:' with the value 'root', 'Password:' with masked characters '*****', and 'Password Confirm:' with masked characters '*****'. Below these fields, a note states: 'Minimum six characters. Password is case sensitive.' At the bottom left are 'Back' and 'Next' buttons. At the bottom right is a link that says 'skip this step'.

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

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

Back Next

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

The screenshot displays the 'Endpoint Protector - Appliance Settings' window within a 'Setup Wizard' interface. The window is titled 'Endpoint Protector - Appliance Settings' and contains the following elements:

- Header:** 'Endpoint Protector' logo, a vertical line with the number '4', and the text 'Endpoint Protector Appliance Setup'. A language dropdown menu is set to 'English'.
- Section Header:** 'Setup Wizard'.
- Instructions:** 'Select your time zone to display time related data. Seasonal times are adjusted automatically.'
- Timezone Selection:** A dropdown menu showing 'Europe' and a sub-menu showing 'Berlin'.
- Instructions:** 'Configure the network settings for the appliance to communicate correctly in your network.'
- Network Settings:** Three input fields with pre-filled values:
 - IP Address: 192.168.0.73
 - Gateway: 192.168.0.1
 - Network Mask: 255.255.255.0
- Navigation:** 'Back' and 'Next' buttons at the bottom.

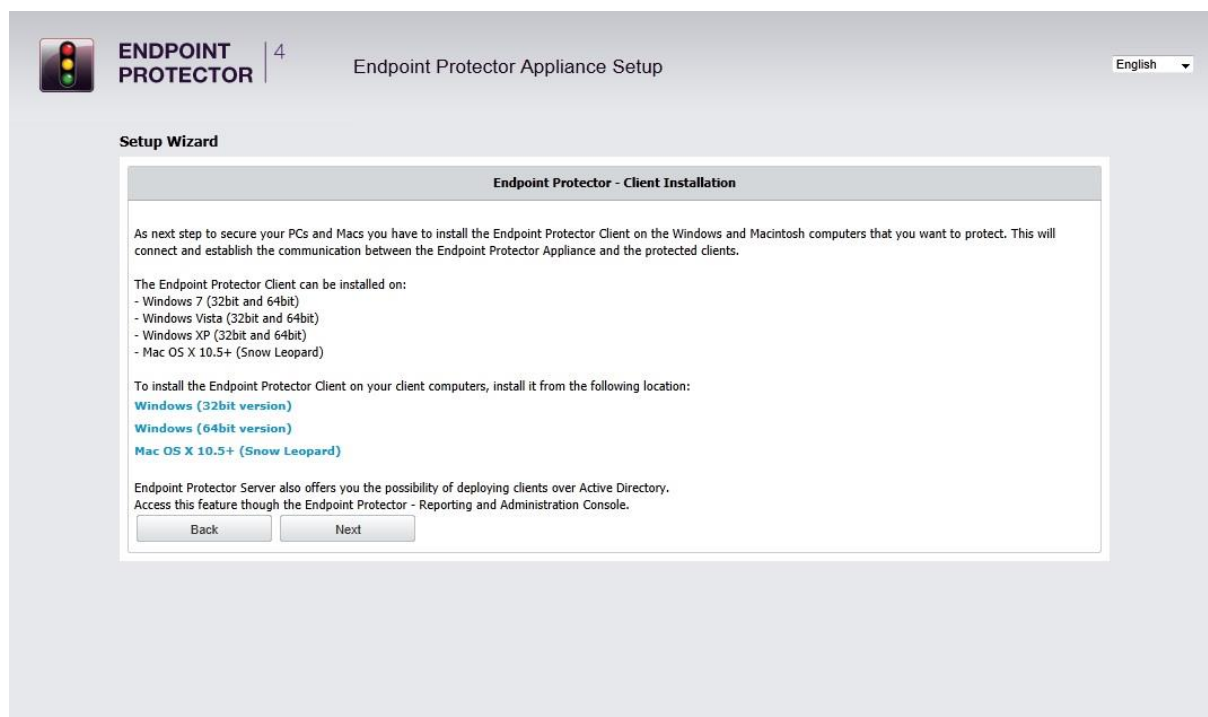
Provide an IP address for your appliance under which it will be reachable in your network. The default IP Address assigned to the Endpoint Protector Appliance in your network is 192.168.0.201. If this IP Address is not assigned in your network this setting does not require a change.

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



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.

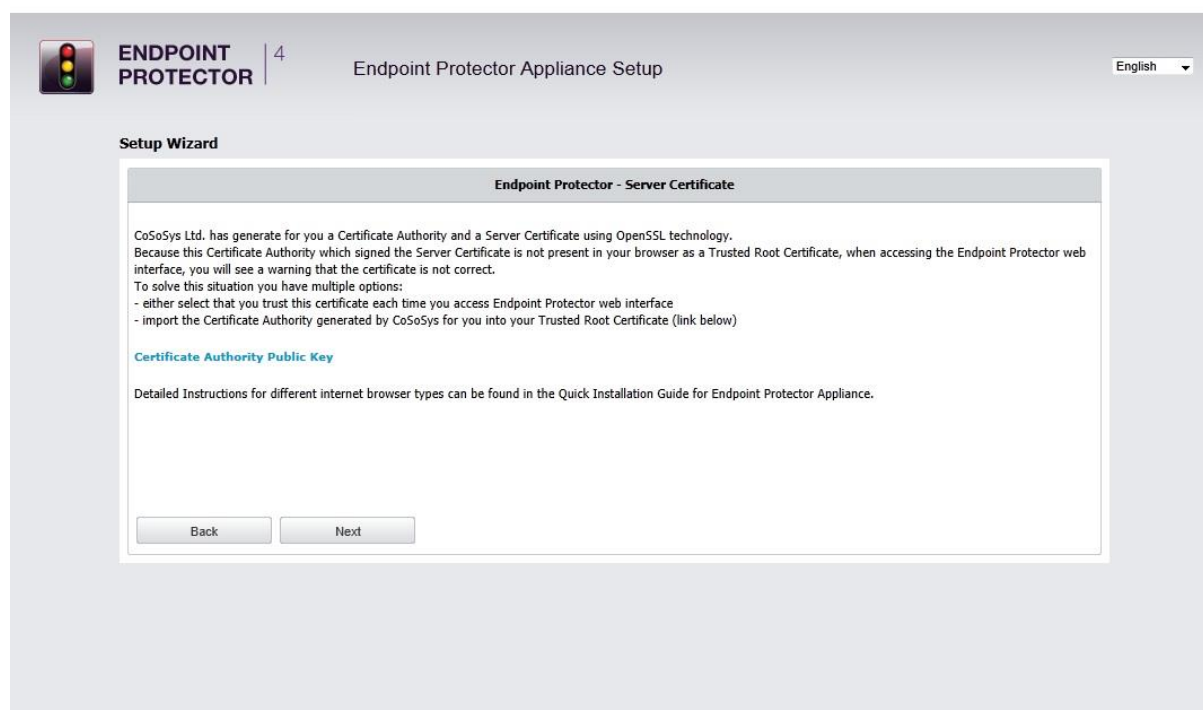
5.2.6. Appliance Server Certificate

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.

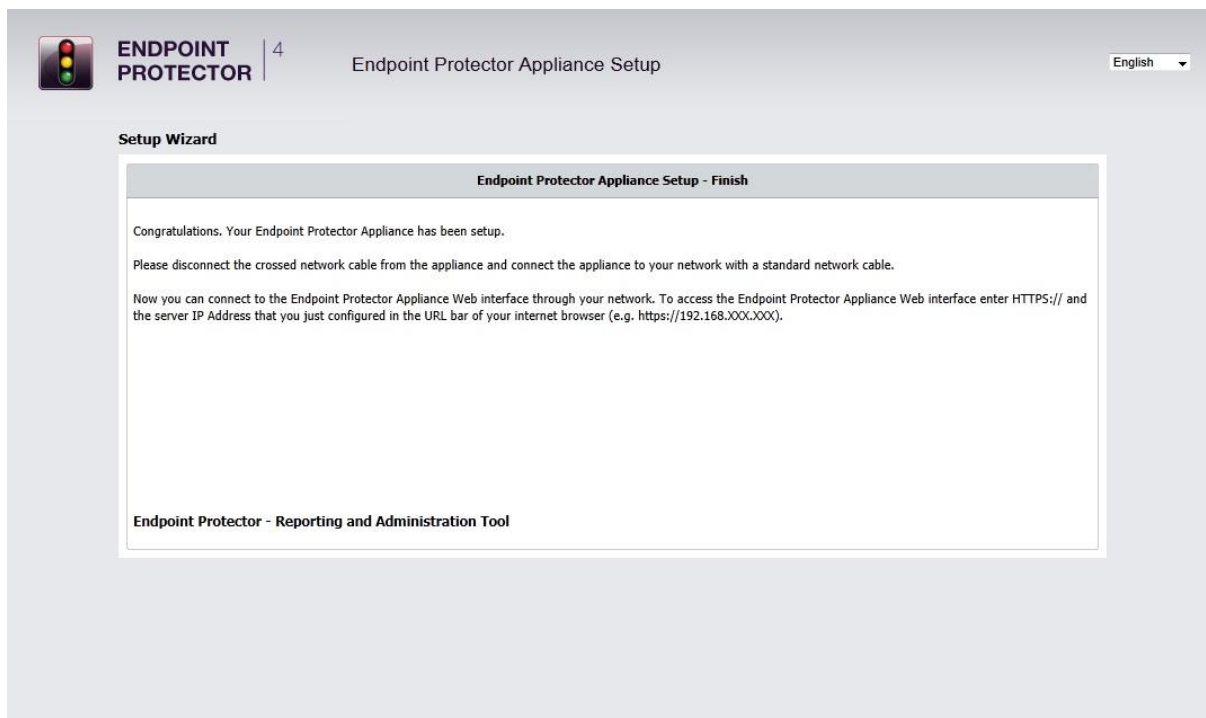
Detailed instructions on how to add the Root Certificate for different Internet browser types can be found in Chapter 8. "Installing Root Certificate to your Internet Browser".



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.



6. Endpoint Protector Appliance Configuration

6.2 Connect Appliance to Network

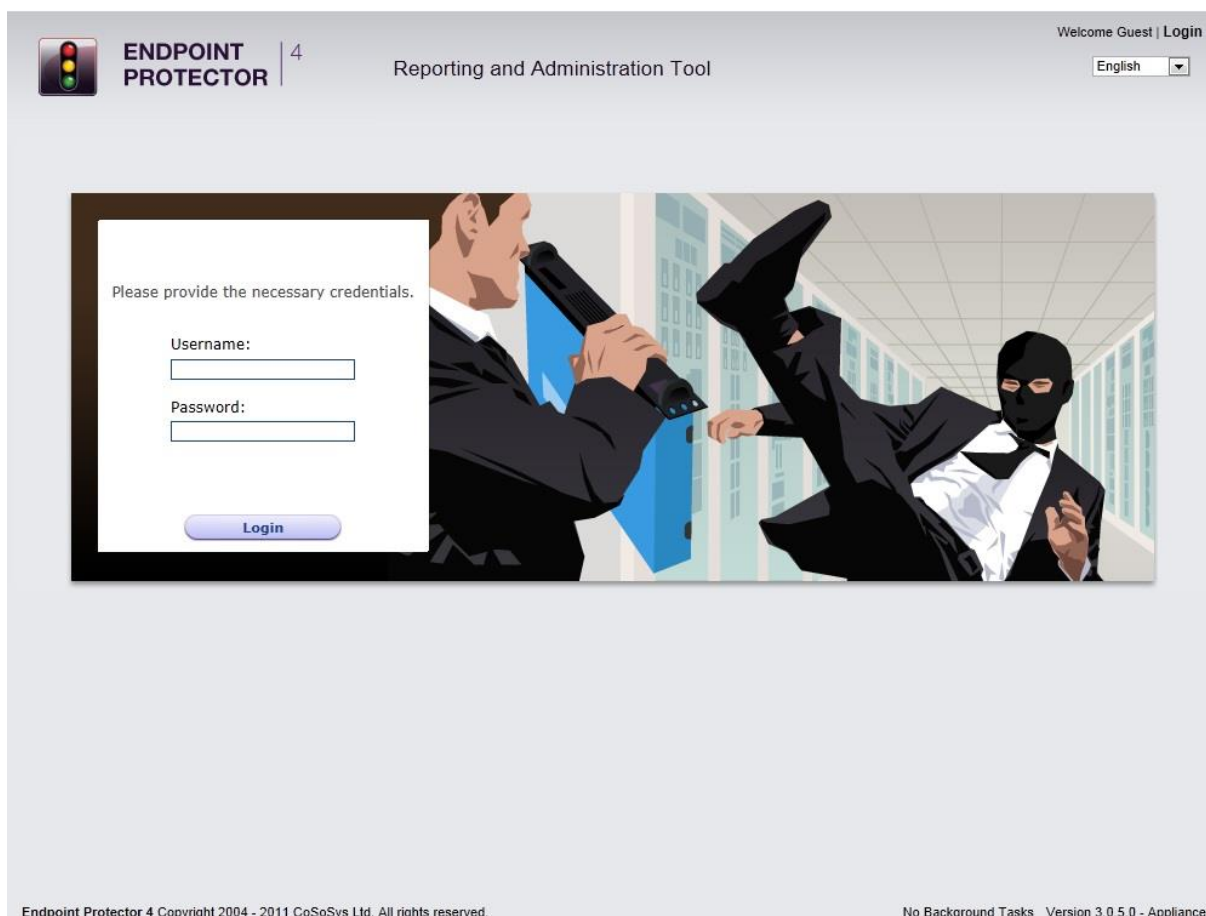
After assigning in the Setup process a static IP address for the Endpoint Protector Appliance, you can connect the Appliance to your network.

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

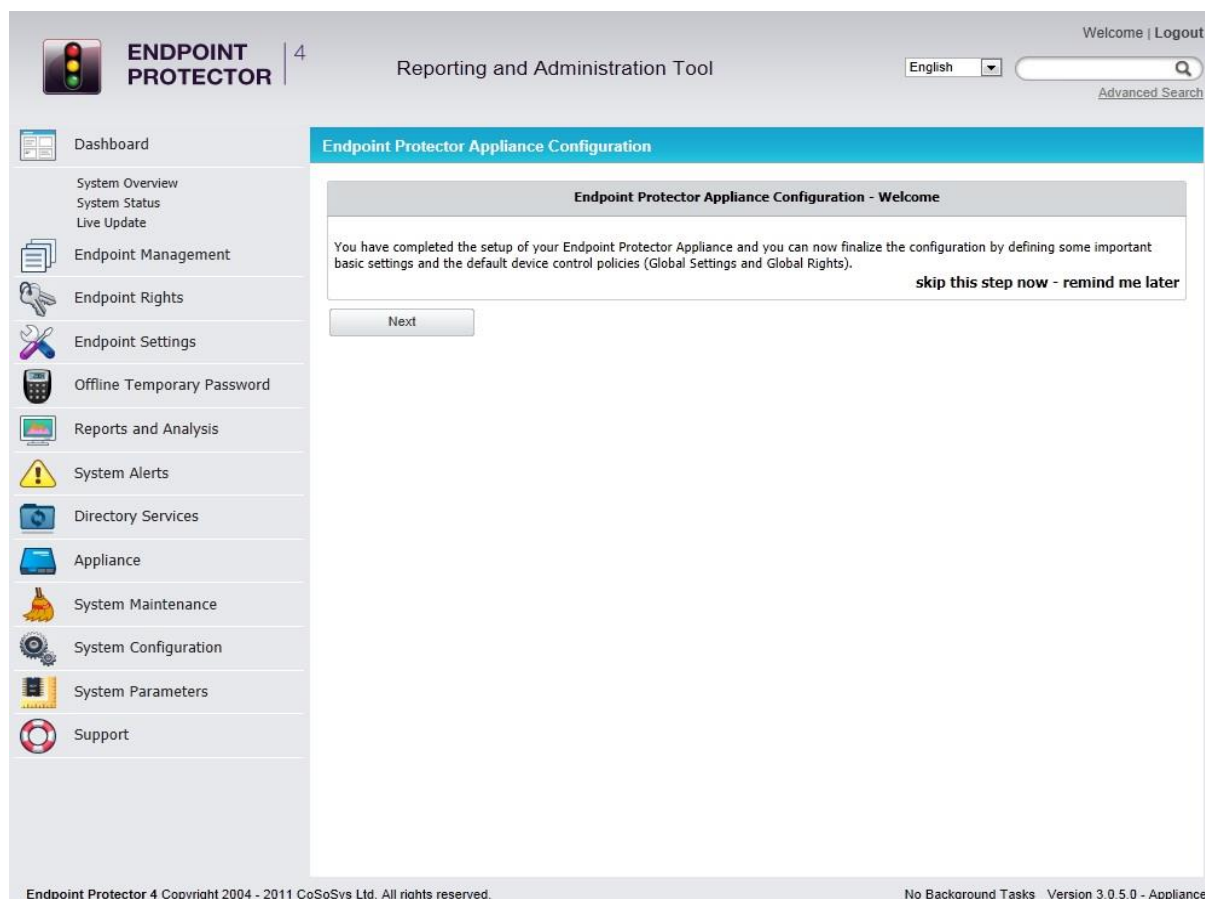
The default username and password for Endpoint Protector 4 Administration and Reporting Tool are:

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.



6.6 Appliance Basic Settings

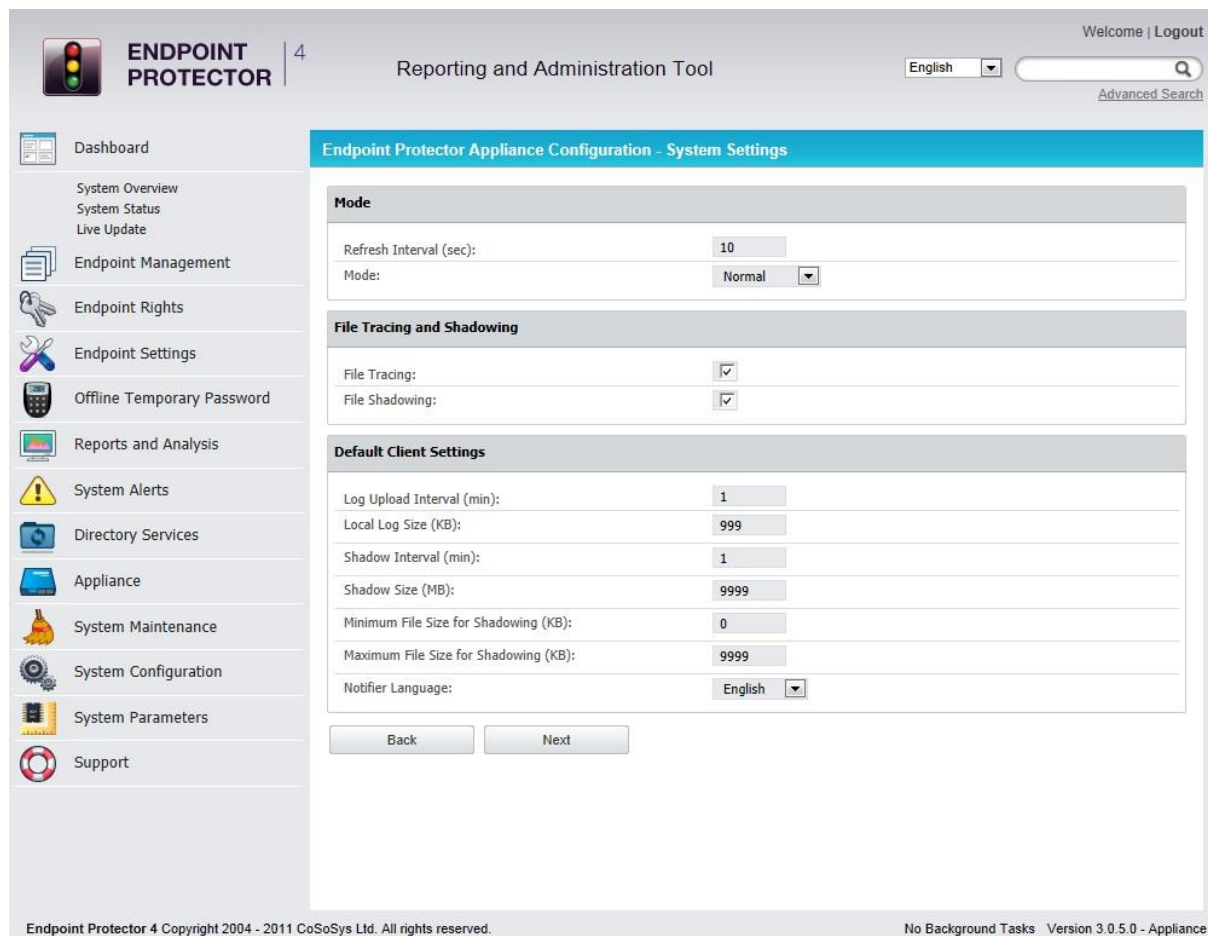
Please provide here all required settings for the Appliance to function properly. Choose what later defined right will have priority, what E-mail address is used to receive System Alerts and what contact information is shown to users in the Offline Temporary Password system tray dialog.

The screenshot displays the 'Endpoint Protector 4' Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance Configuration - System Settings' and is divided into several sections:

- Endpoint Protector Rights Functionality:** Includes radio buttons for 'Use computer rights' (selected), 'Use user rights', and 'Use both'. Below these are checkboxes for 'User rights' and 'Computer rights' under a 'Priority' label.
- E-mail Server Settings:** Features a dropdown for 'E-mail Type' set to 'Native', a text field for 'Native Options' containing 'smtp.example.com', and a note: '*Note: Endpoint Protector Server will require a working Internet connection for this feature.' An example for Linux sendmail is provided: '-oi (more...)'.
- Proxy Server Settings:** Includes text fields for 'IP:', 'Username:', and 'Password:'. A note states: '*Note: This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.'
- Offline Temporary Password - Administrator Contact Details:** Includes text fields for 'Phone:' (containing '+1-222-5550001') and 'E-mail:' (containing 'alerts.email@example.com'). A note states: '*Note: This contact information is referring to Offline Temporary Password only!'.

At the bottom of the configuration area are 'Back' and 'Next' buttons. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.' and '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.



The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The top header includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with a magnifying glass icon and the text 'Advanced Search'. The top right corner shows 'Welcome | Logout'.

The left sidebar contains a navigation menu with the following items: Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support.

The main content area is titled 'Endpoint Protector Appliance Configuration - System Settings'. It is divided into three sections:

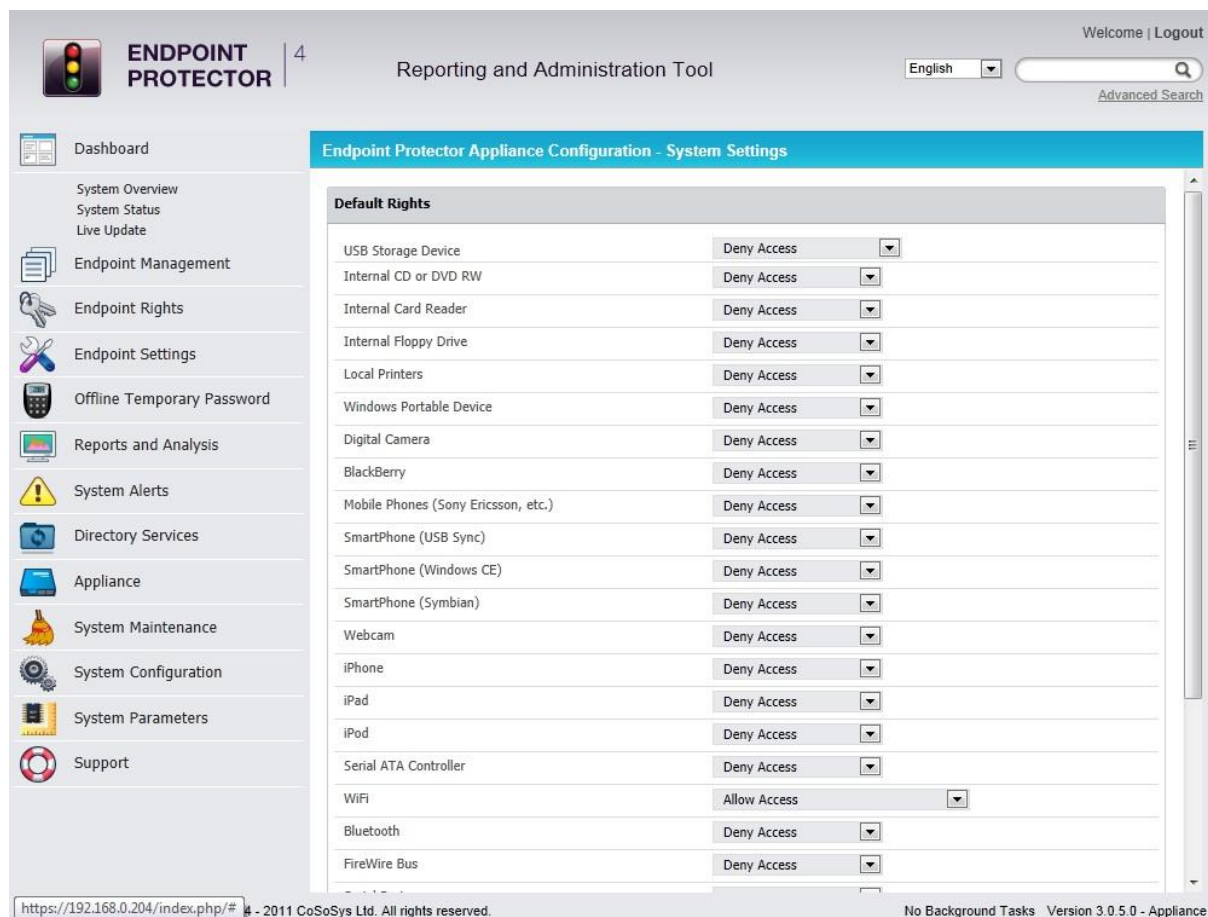
- Mode**: Contains 'Refresh Interval (sec):' set to '10' and 'Mode:' set to 'Normal' with a dropdown arrow.
- File Tracing and Shadowing**: Contains 'File Tracing:' and 'File Shadowing:', both with checked checkboxes.
- Default Client Settings**: Contains several settings with input fields:
 - Log Upload 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 (with a dropdown arrow)

At the bottom of the configuration area are 'Back' and 'Next' buttons. The footer of the page contains the text 'Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.' on the left and 'No Background Tasks Version 3.0.5.0 - Appliance' on the right.

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.



The screenshot shows the 'Endpoint Protector Appliance Configuration - System Settings' page. The left sidebar contains a navigation menu with options: Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance Configuration - System Settings' and contains a table of 'Default Rights'.

Device	Access Policy
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

The footer of the interface shows the URL 'https://192.168.0.204/index.php/#', copyright information '© 2011 CoSoSys Ltd. All rights reserved.', and system status 'No Background Tasks Version 3.0.5.0 - Appliance'.

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.

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Welcome | Logout' and 'Advanced Search' links.

The left sidebar contains a menu with the following items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, Server Information, Server Maintenance, System Maintenance, System Configuration, System Parameters, and Support.

The main content area is titled 'Endpoint Protector Appliance - System Information' and contains three sections:

- 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 I
System Information Update :	2011-Sep-12 14:40:01

The footer of the interface contains the text: 'Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks Version 3.0.5.0 - Appliance'.

7.3 Server Maintenance

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The left sidebar contains a navigation menu with items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, Server Information, Server Maintenance, System Maintenance (highlighted), System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance - System Maintenance' and contains three sections: 'Time Zone' with a dropdown for 'Europe' and 'Bucharest'; 'IP Configuration' with input fields for IP Address (192.168.0.1), Gateway (192.168.0.1), and Netmask (255.255.255.0), followed by a note about network configuration; and 'DNS Configuration' with input fields for DNS 1 (192.168.0.1) and DNS 2 (192.168.0.26), followed by a note about DNS requirements. Below these is the 'Appliance Operations' section with buttons for 'Reboot', 'Shutdown', and 'Factory Default', and a 'Save' button at the bottom.

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!

The screenshot displays the 'Endpoint Protector Server - Download Client Software' page within the 'Reporting and Administration Tool' interface. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and System Alerts. The main content area is titled 'Endpoint Protector Client Installation' and provides instructions for installing the client software. It lists supported operating systems: Windows 7 (32bit and 64bit), Windows Vista (32bit and 64bit), Windows XP (32bit and 64bit), and Mac OS X 10.5+ (Snow Leopard). It also provides the Endpoint Protector Server IP (192.168.0.204) and Port (443). The page includes a section for downloading the client software for different operating systems and versions, and a link to the user manual for more information.

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:

Endpoint Protector Server Port:

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

Department Code:

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

Active Directory can be used for Endpoint Protector Client deployment as well. This feature can be found in the Endpoint Protector System Configuration menu Active Directory.

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.

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Advanced Search' link. A sidebar on the left lists various system management options: Dashboard, System Overview, System Status, Live Update (highlighted), Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support.

The main content area is titled 'Endpoint Protector Appliance - Live Update'. It is divided into two sections:

- Software Update:** This section shows the 'Most recent check for updates' as '2011-09-06 14:14:59' and 'Updates were installed' as 'never'. It includes two buttons: 'Configure Live Update' and 'Check Now'.
- Available Updates:** This section lists three updates, each with a checkbox for selection:
 - Mac client software and Server update (HWA-E9-U0001):** Description: '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):** Description: 'AD Import no longer fails on illegal characters in AD entities' names. No double entries at AD Sync.' Remarks: 'No Important Observations'.
 - Server update (09 Dec 2010) (HWA-E9-U0003):** Description: 'System Policy setting for Notifier Language will propagate to individual computers.' Remarks: 'No Important Observations'.
 - Server update (16 Dec 2010) (HWA-E9-U0004):** Description: 'Spanish language added. Persian language resource improved.'
 At the bottom of this section are buttons for 'Apply Updates' and 'View Applied Updates'.

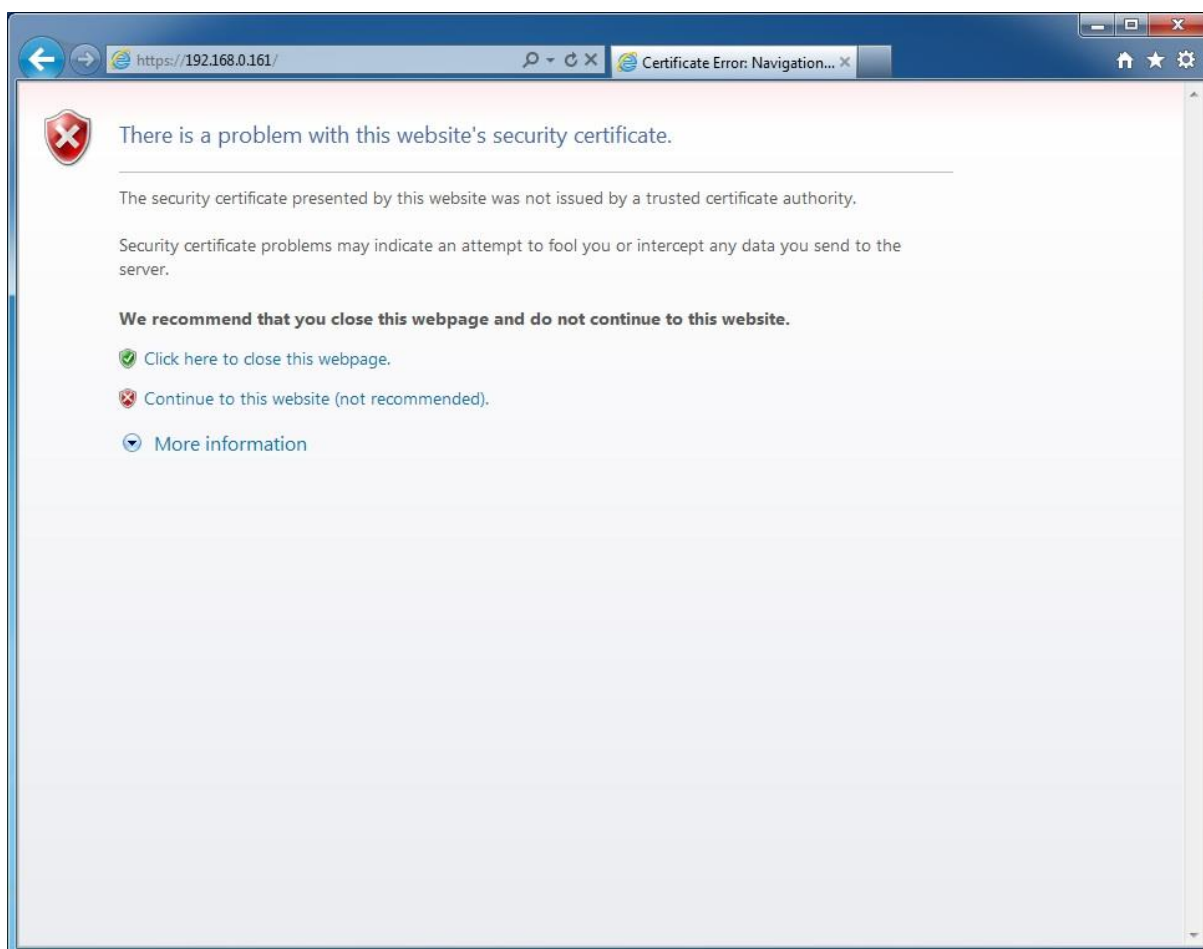
The footer of the interface contains the text: 'Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks Version 3.0.5.0 - Appliance'.


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.



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

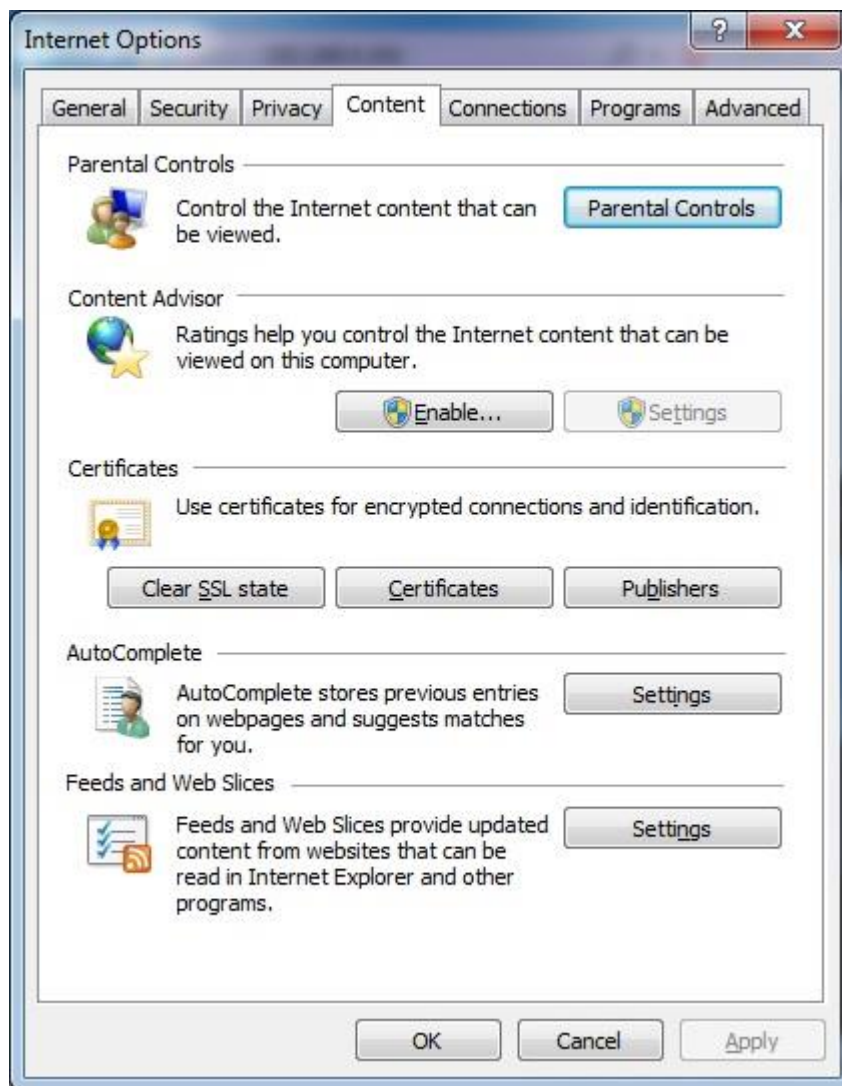
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

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

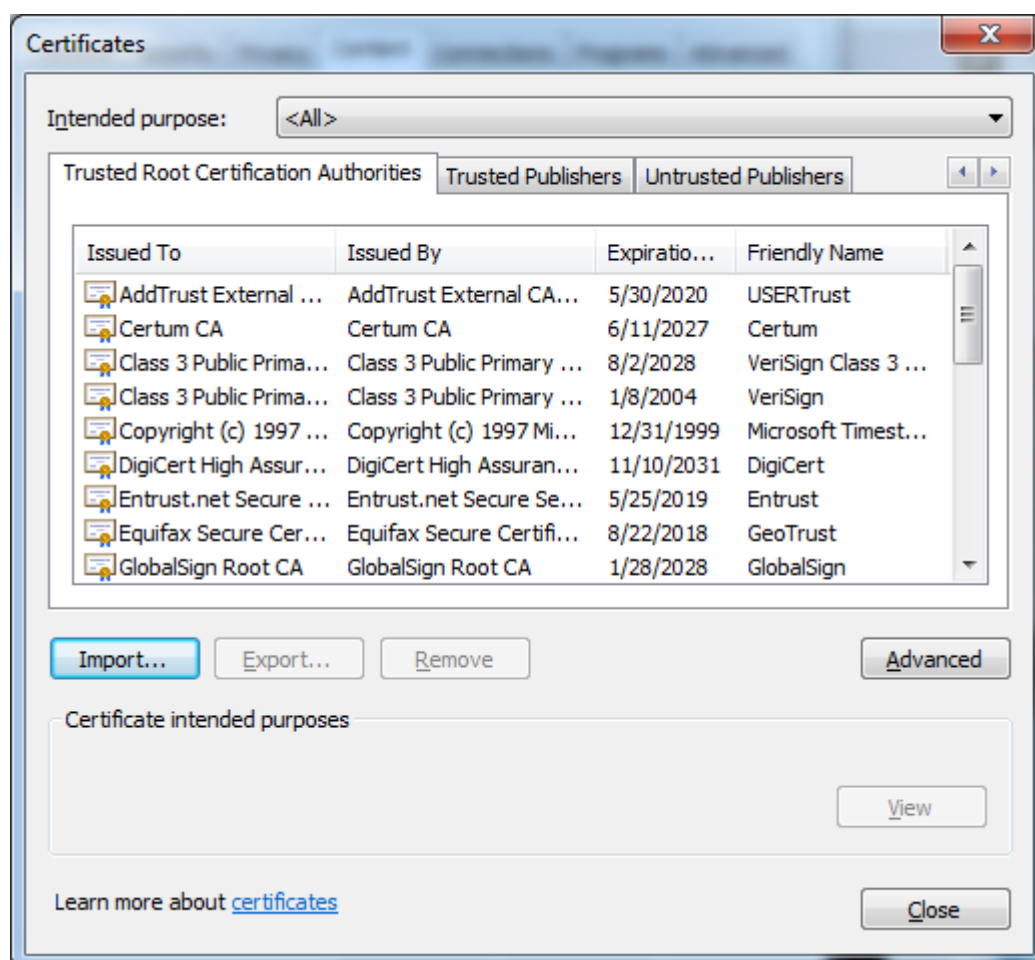
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

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.



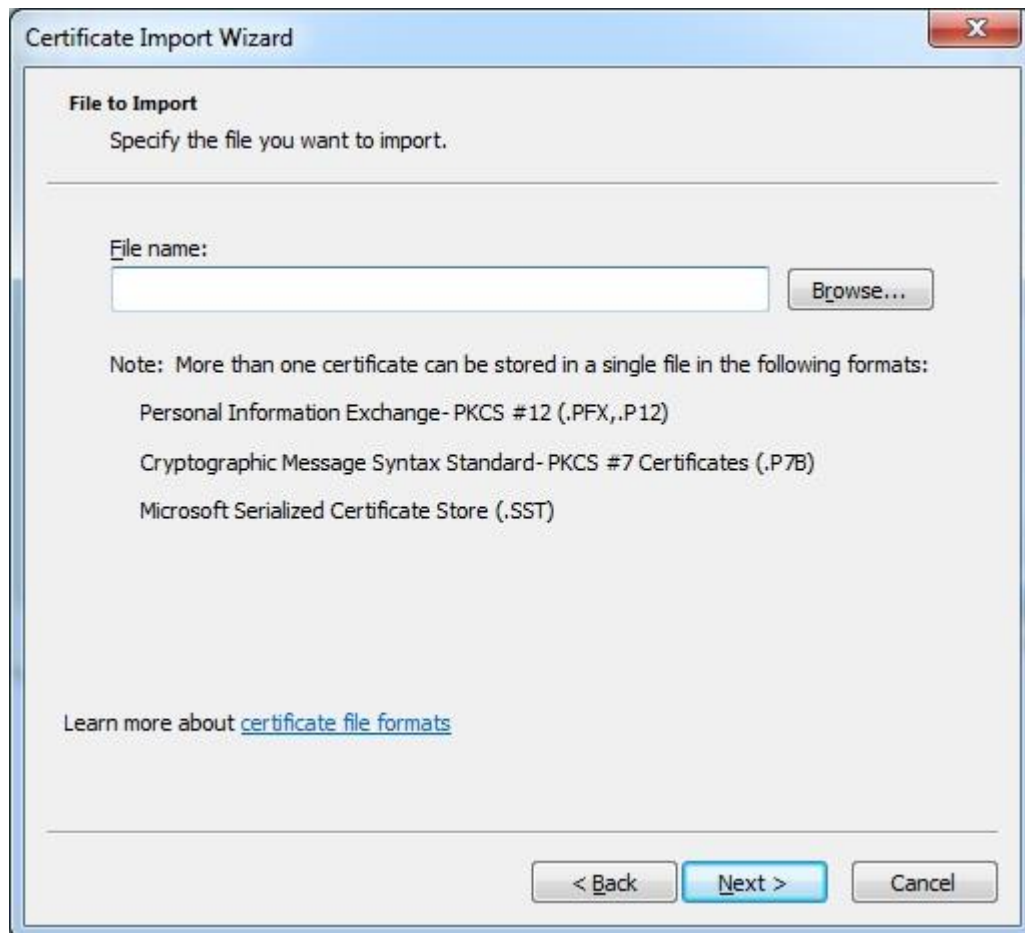
From the Certificates list, select "Trusted Root Certification Authorities" and click on the "Import" button.



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



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



The image shows a 'Certificate Import Wizard' dialog box. The title bar is blue with a close button (X) in the top right corner. The main area is light gray. At the top, it says 'File to Import' and 'Specify the file you want to import.' Below this is a horizontal line. Under the line, there is a label 'File name:' followed by a text input field and a 'Browse...' button. Below the input field, there is a 'Note' section stating: 'Note: More than one certificate can be stored in a single file in the following formats:'. This is followed by three bullet points: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom left, there is a link: 'Learn more about [certificate file formats](#)'. At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted in blue), and 'Cancel'.

File to Import
Specify the file you want to import.

File name:

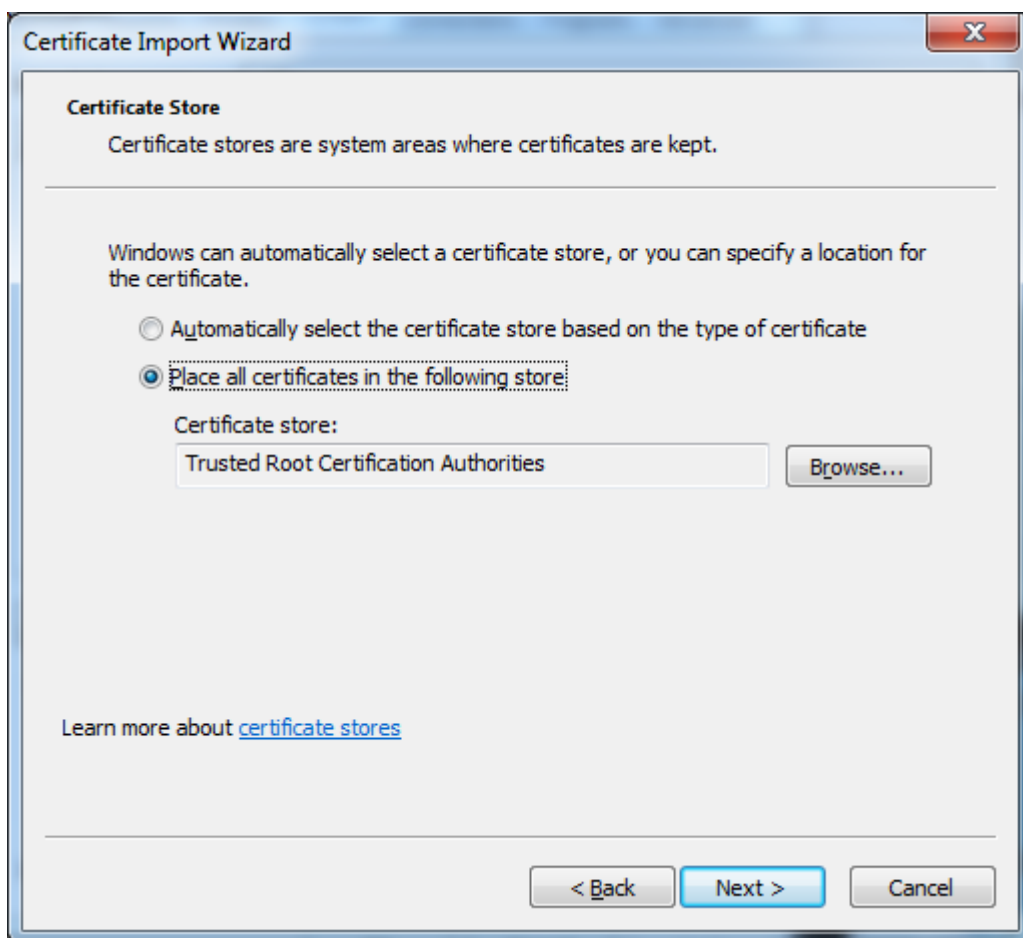
Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

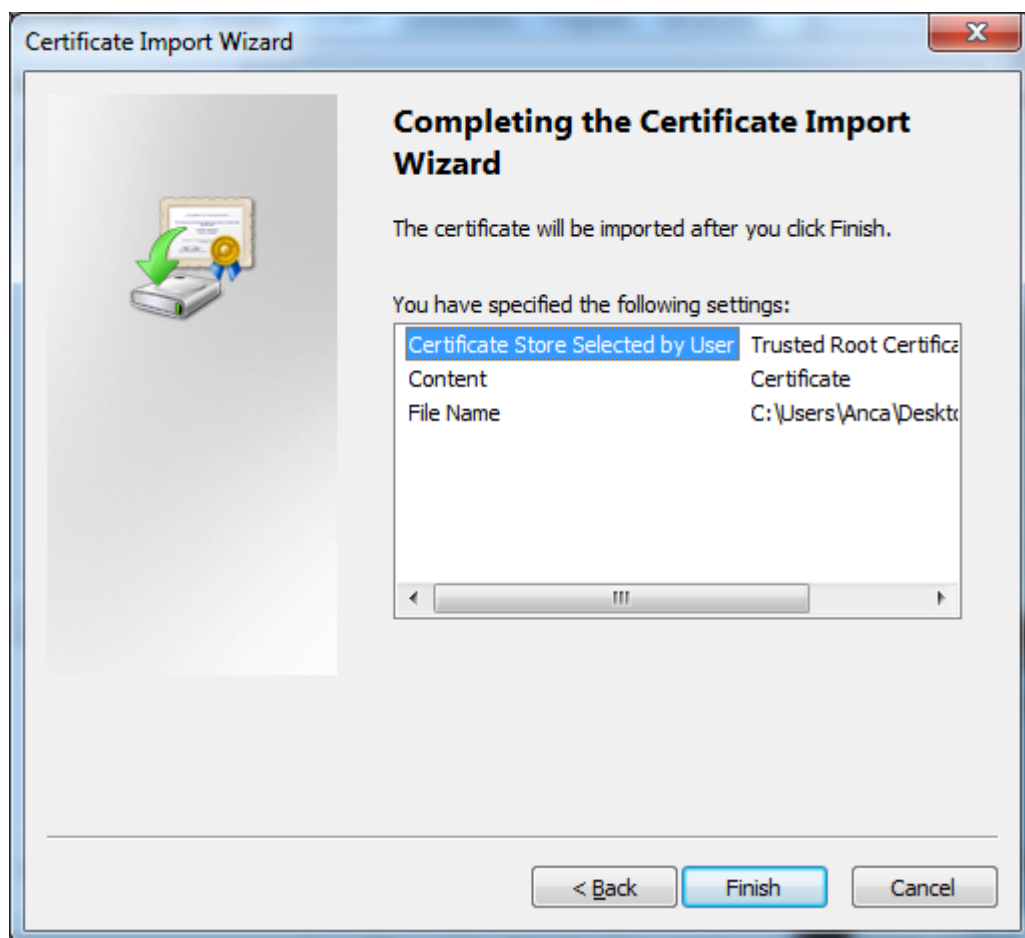
Learn more about [certificate file formats](#)

< Back Next > Cancel

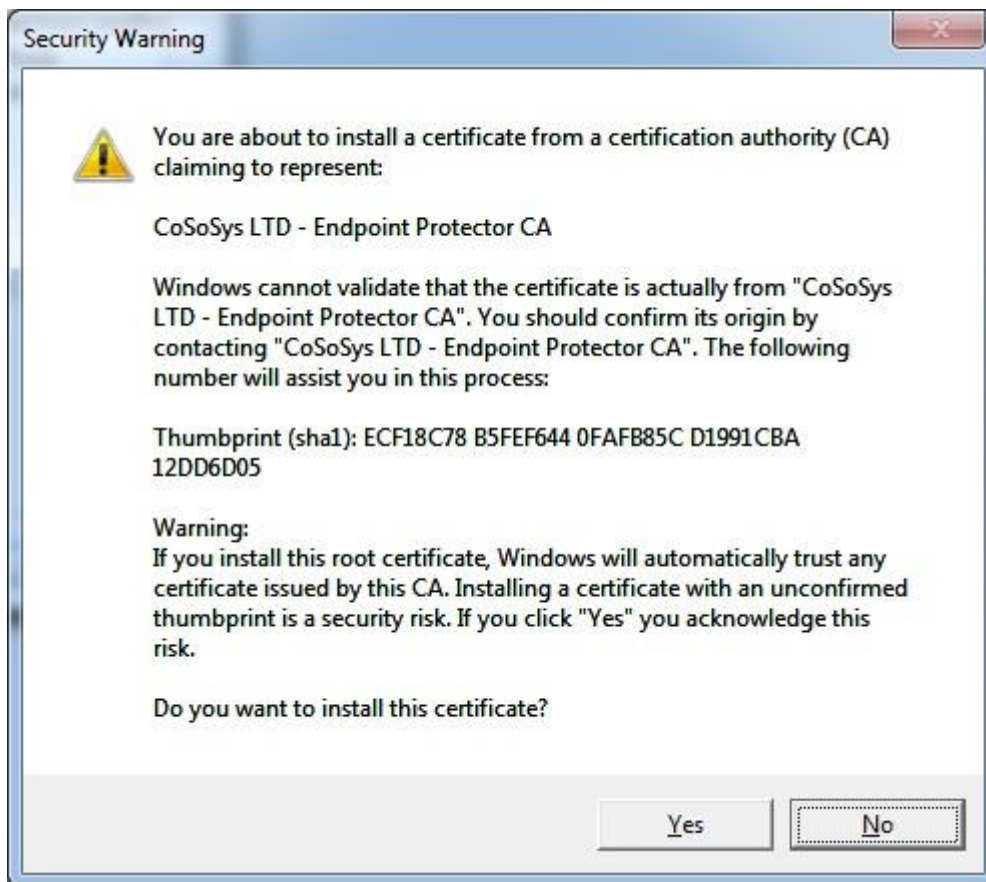
In the Certificate Store window, select “Place all certificates in the following store” radio button.



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

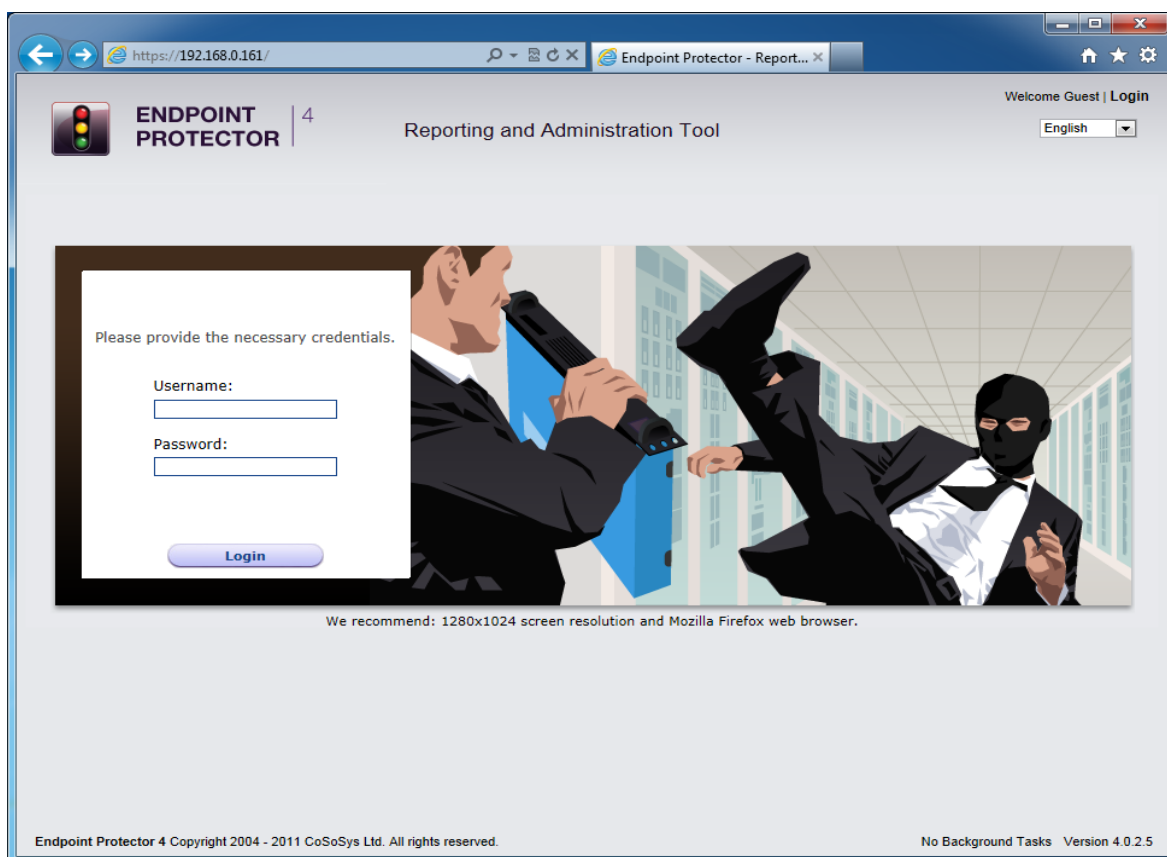


A Security Warning window pops up. Just click "Yes".



You have now successfully installed the Certificate.

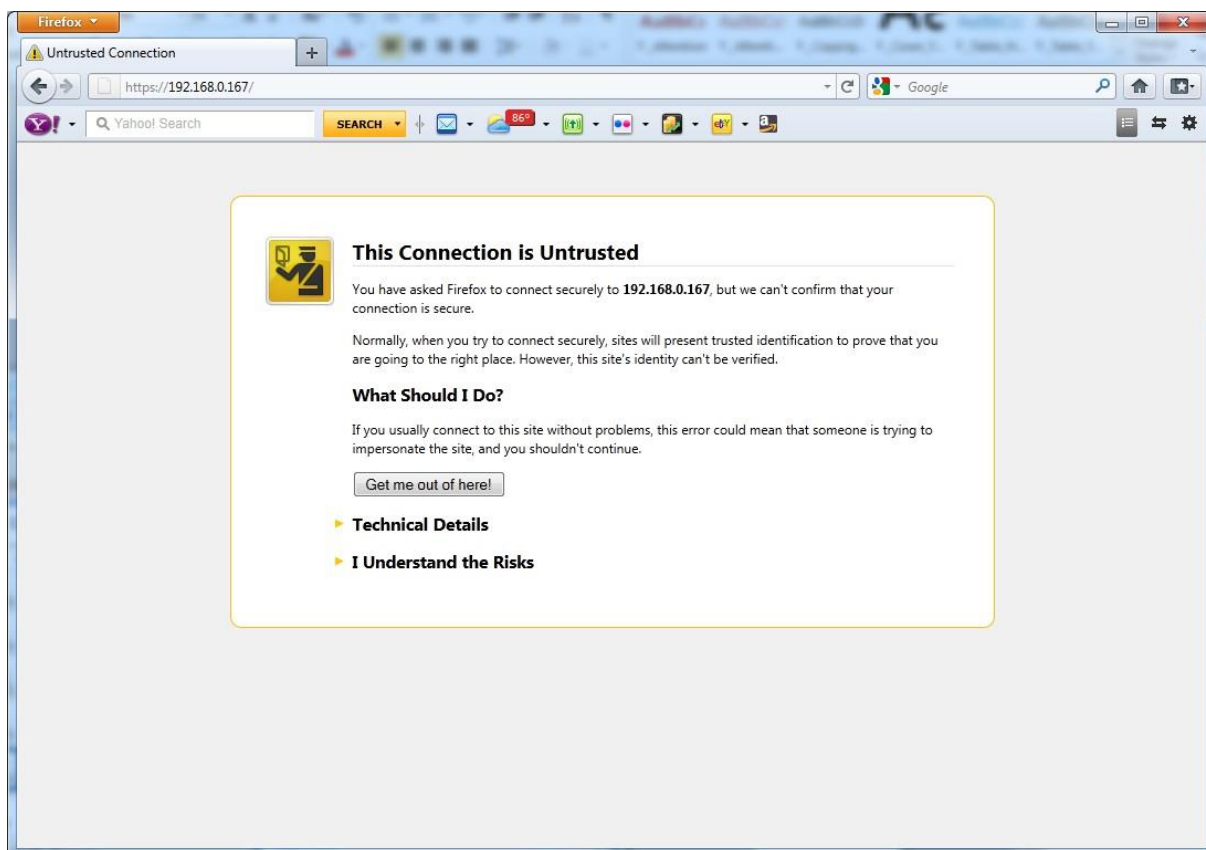
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



8.3 For Mozilla Firefox

Open the Browser.

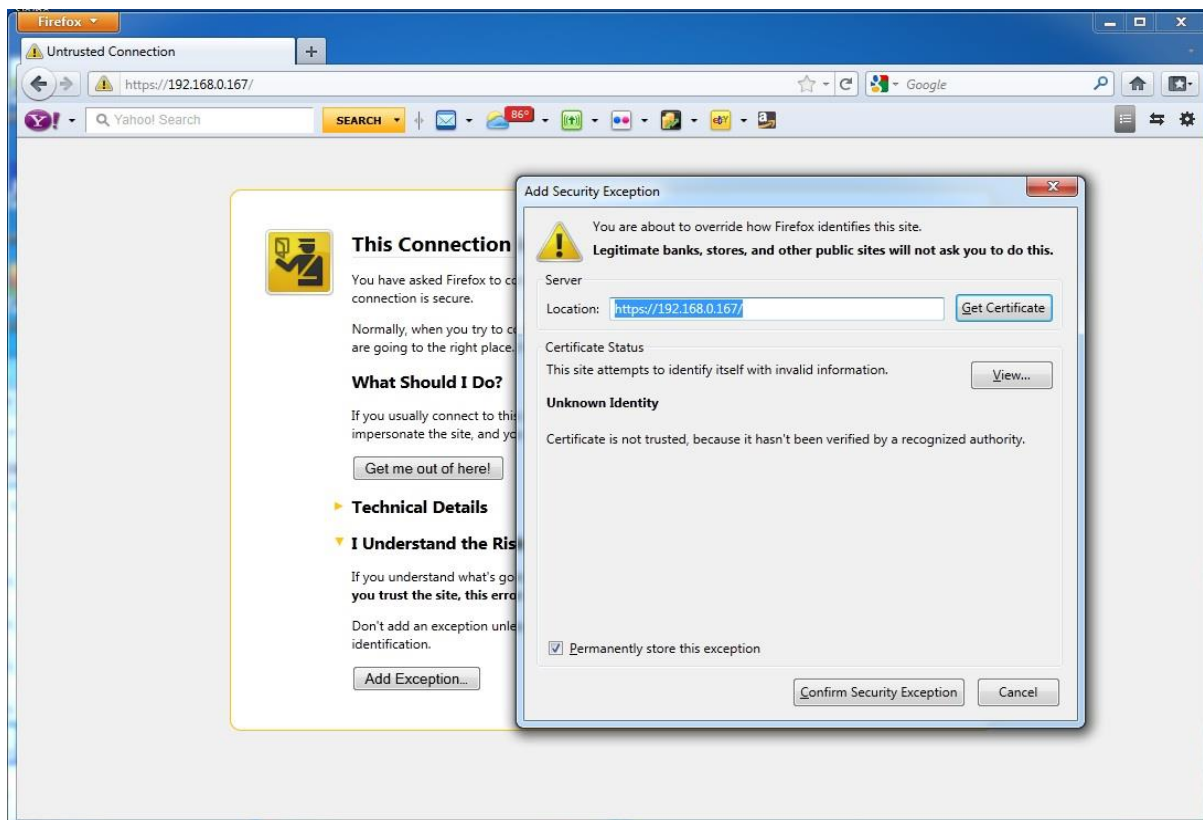
Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example <https://192.168.0.201>).



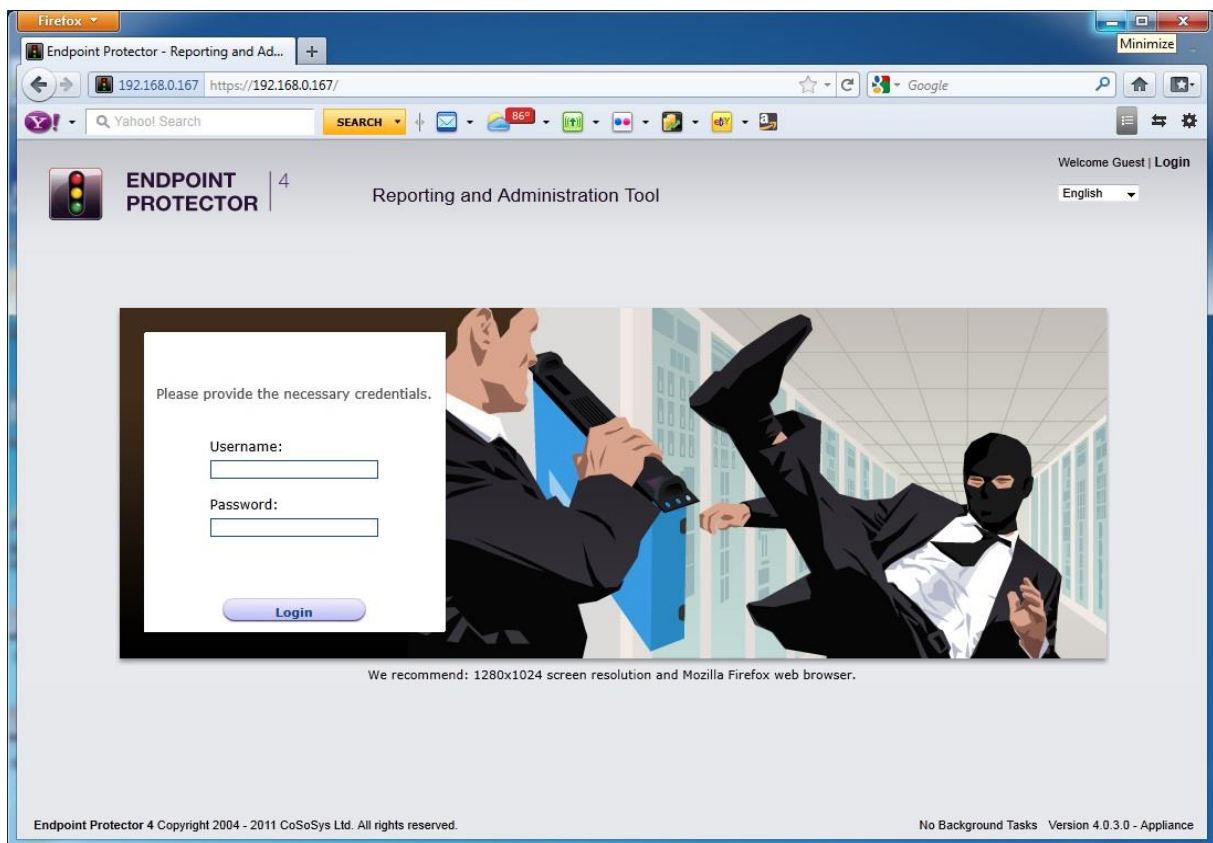
From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

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



Close the browser and start it again.



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 your 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.