



# ENDPOINT PROTECTOR

Virtual and Hardware Appliance User Manual - Version 4.5.0.2



## Table of Contents

<b>1.Endpoint Protector Virtual Appliance formats</b>	<b>1</b>
1.1. Virtualization software that support OVF and OVA .....	2
1.2. Virtualization software that supports VMX .....	2
1.3. Virtualization software that supports VHD .....	3
1.4. Virtualization software that support PVM .....	3
1.5. Virtualization software that supports XVA.....	3
<b>2.Using the OVF format .....</b>	<b>4</b>
2.1. Implementation using Oracle VM VirtualBox .....	4
2.2. Implementation using VMware vSphere .....	9
2.3. Implementing in Citrix XenServer 5.6 using OVF Format .....	14
<b>3.Using the VMX format.....</b>	<b>19</b>
3.1. Implementing using VMware Server .....	19
3.2. Implementing using VMware Player .....	21
3.3. Implementing using VMware Workstation.....	23
<b>4.Using the VHD format.....</b>	<b>25</b>
4.1. Implementing using Microsoft Hyper-V 2012 .....	25
<b>5.Virtual Appliance Setup Wizard.....</b>	<b>29</b>
5.1.1 Manual configuration .....	32
5.1.1. Automatic configuration .....	34
<b>6.Endpoint Protector Configuration .....</b>	<b>35</b>
6.1. Login to Endpoint Protector .....	35
6.2. Configuration Wizard .....	36
6.3. System Settings .....	36
6.4. Default Device Control Rights .....	37
6.5. Finishing the Endpoint Protector Configuration Wizard .....	38
<b>7.Server Information and Maintenance.....</b>	<b>39</b>
7.1. Server Information.....	39
7.2. Server Maintenance .....	39
7.3. Endpoint Protector Client Installation .....	40

7.4. Endpoint Protector Live Update .....	41
<b>8. Installing Root Certificate to Browsers .....</b>	<b>42</b>
8.1. For Microsoft Internet Explorer .....	42
8.2. For Mozilla Firefox .....	47
<b>9. Hardware Appliance Setup .....</b>	<b>49</b>
9.1. Endpoint Protector Appliance Delivery .....	49
9.2. Connecting Appliance for Initial Setup .....	50
9.3. Hardware Appliance Back and Front Panel .....	50
9.3.1. A20 Appliance Back Panel .....	50
9.3.2. A50 and A100 Appliance Back Panel .....	50
9.3.3. A20 Appliance Front Panel .....	51
9.3.4. A50 and A100 Appliance Front Panel .....	51
9.3.5. A250, A500 and A1000 Appliance Front Panel .....	51
9.3.6. A2000 - A4000 Appliance Front Panel .....	52
9.4. A2000 / A4000 Appliance HDD Configuration .....	52
9.4.1. A2000 Appliance HDD Configuration .....	52
9.4.2. A4000 Appliance HDD Configuration .....	53
9.4.3. A2000 and A4000 Appliance HDD RAID Additional Software .....	53
9.5. Hardware Appliance Setup Wizard .....	53
<b>10. Support .....</b>	<b>54</b>
<b>11. Disclaimer .....</b>	<b>55</b>

# 1. Endpoint Protector Virtual Appliance formats

The Endpoint Protector Virtual Appliance is available in different formats and for various platforms. The table below provides a quick overview.

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

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

## Note!

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

## 1.1. Virtualization software that support OVF and OVA

In addition to the information provided in the initial table, this formats are also supported by:

- 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

## 1.2. Virtualization software that supports VMX

In addition to the information provided in the initial table, this format is also supported by:

- 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 are required:

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

## 1.3. Virtualization software that supports VHD

In addition to the information provided in the initial table, this format is also supported by:

- Microsoft Hyper-V 6.1.7601.17514
- Microsoft Hyper-V 6.3.9600.16384

## 1.4. Virtualization software that support PVM

In addition to the information provided in the initial table, this format is also supported by:

- Parallels Desktop 10.2.1

## 1.5. Virtualization software that supports XVA

In addition to the information provided in the initial table, this format is also supported by:

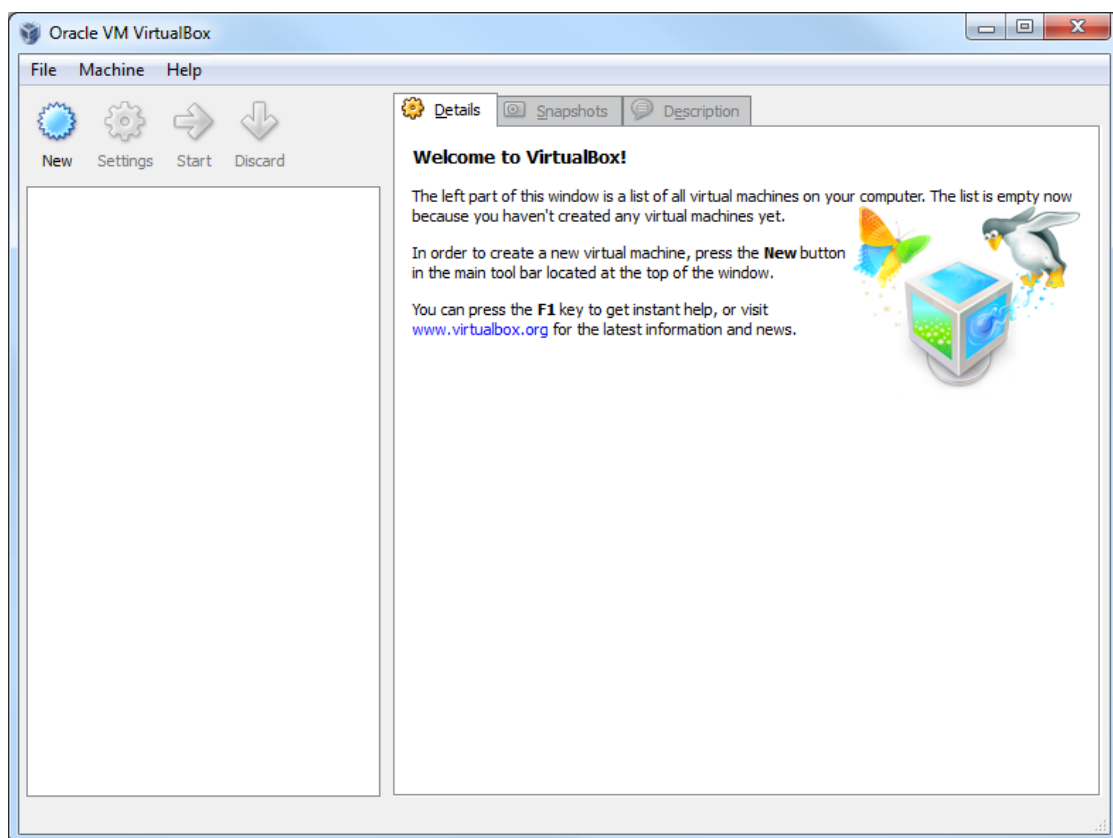
- Citrix XenServer 5.5
- Citrix XenServer 6.0

## 2. Using the OVF format

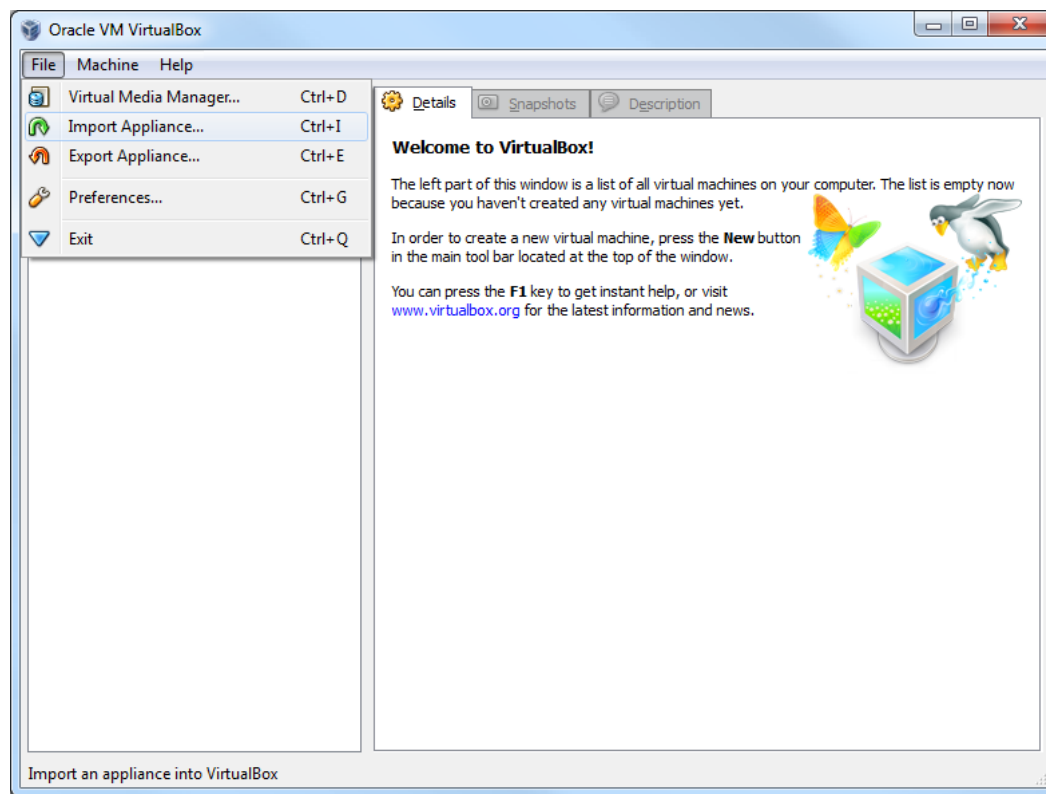
There are several options to implement the Endpoint Protector Virtual Appliance using the OVF format. The way to do this is explained below.

### 2.1. Implementation using Oracle VM VirtualBox

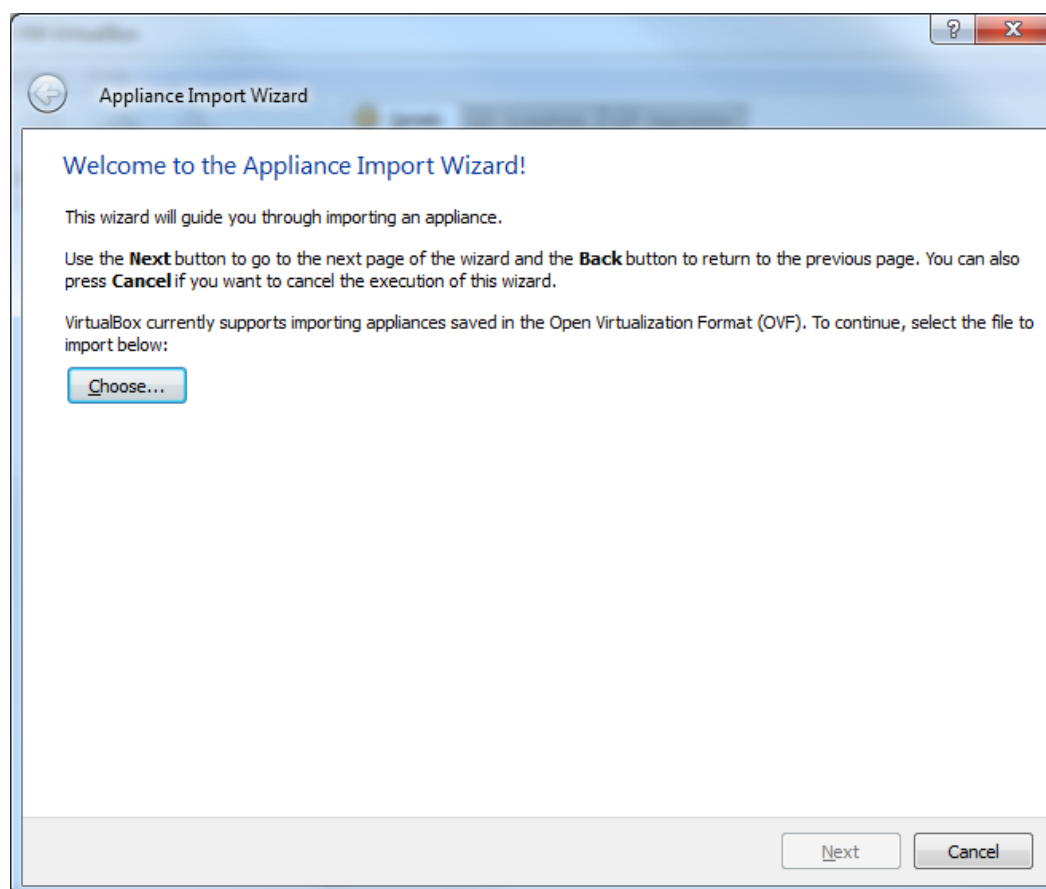
1. Unzip the downloaded package
2. Start VirtualBox



### 3. Go To File > Import Appliance

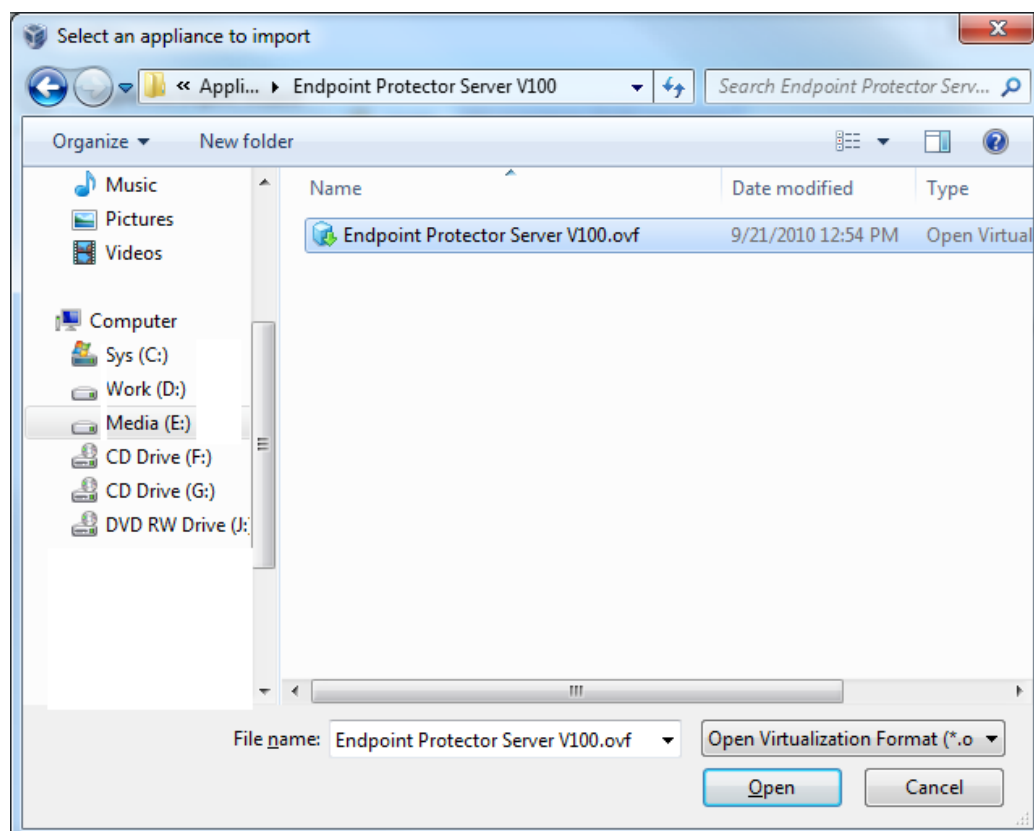


### 4. Press Choose button

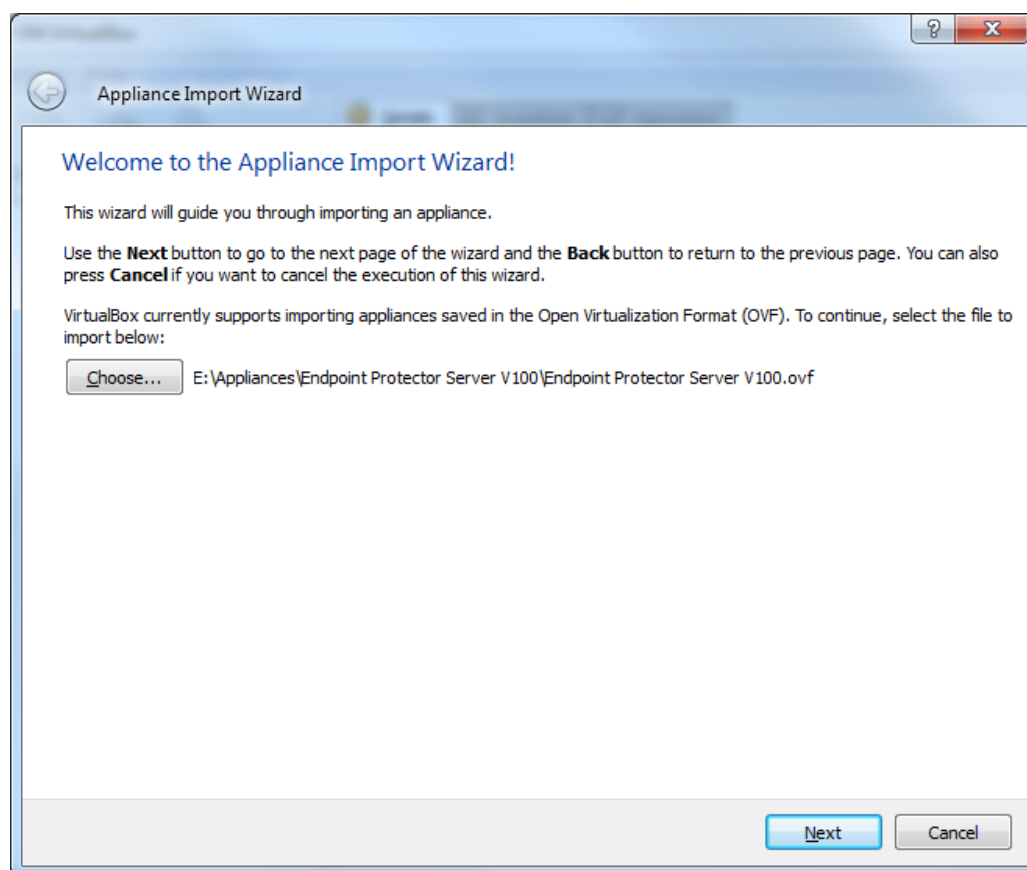




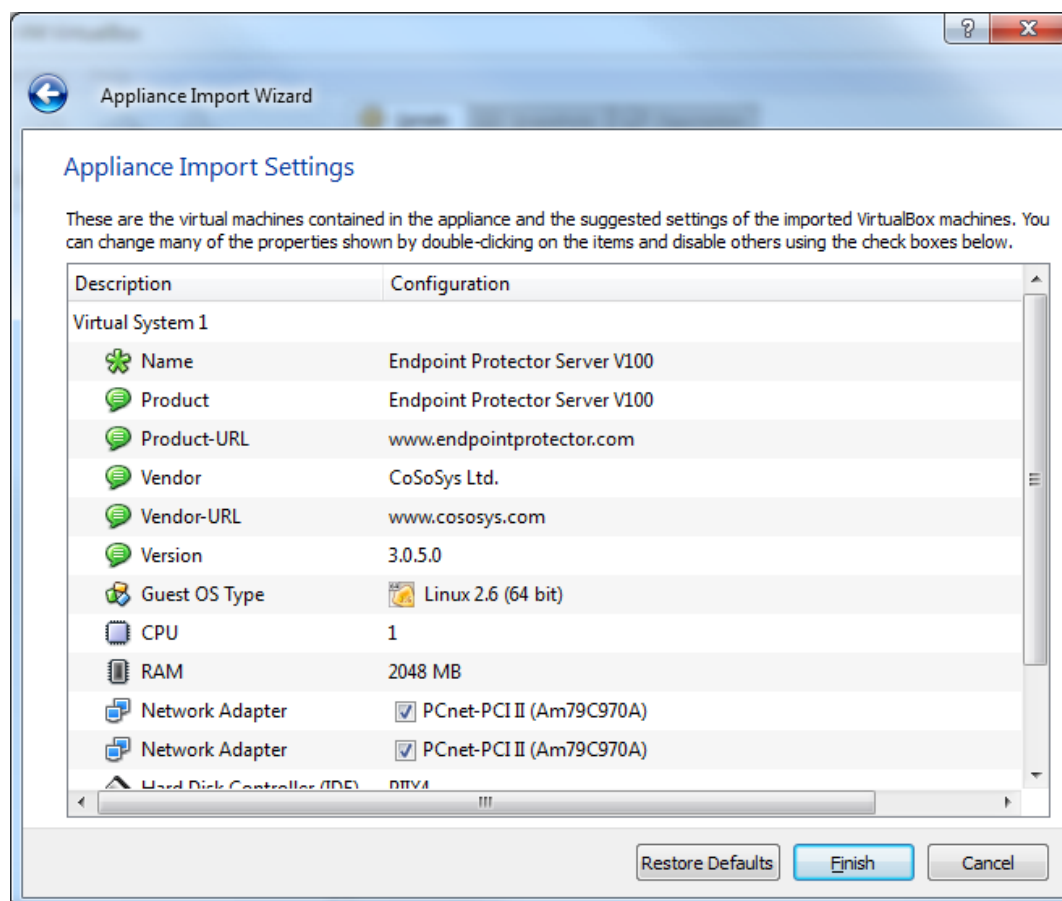
## 5. Browse and select the OVF file from the extracted zip file



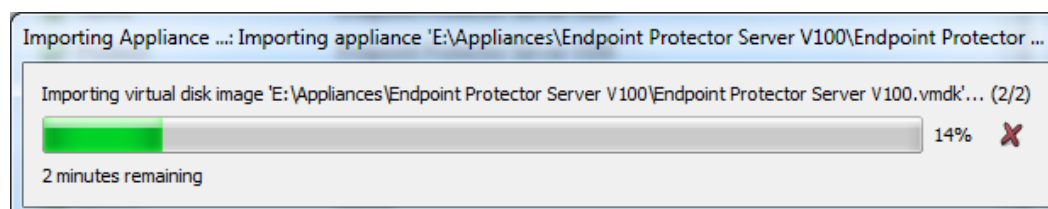
## 6. Press Next Button



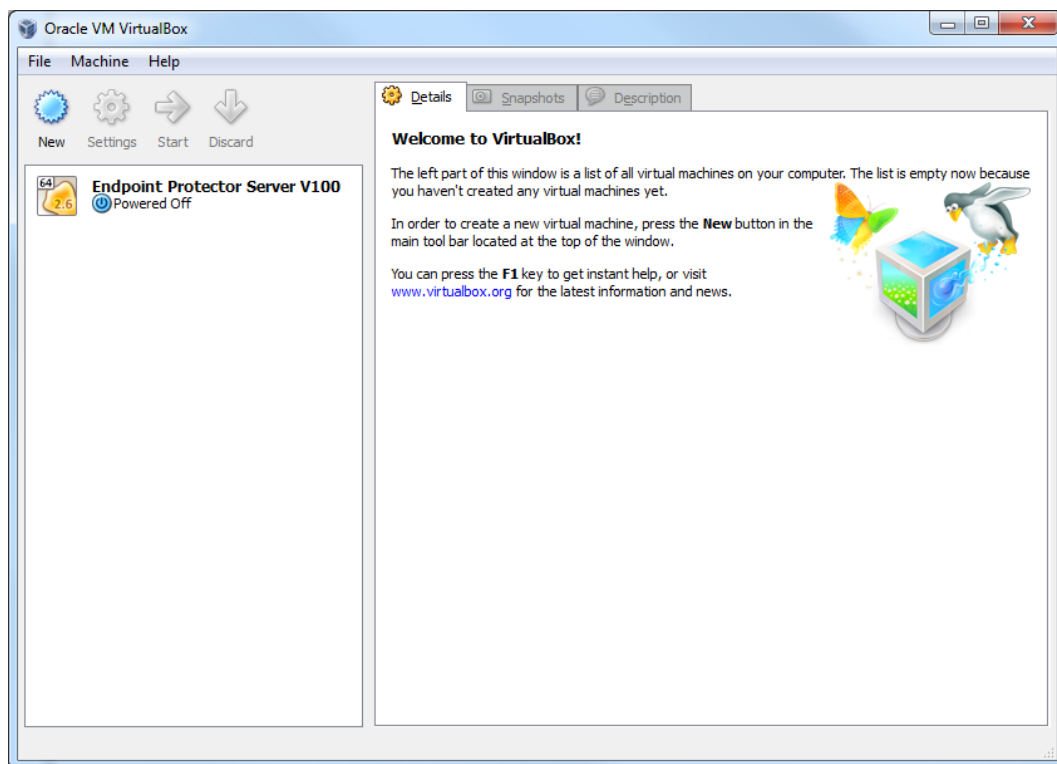
## 7. Press Finish Button



## 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

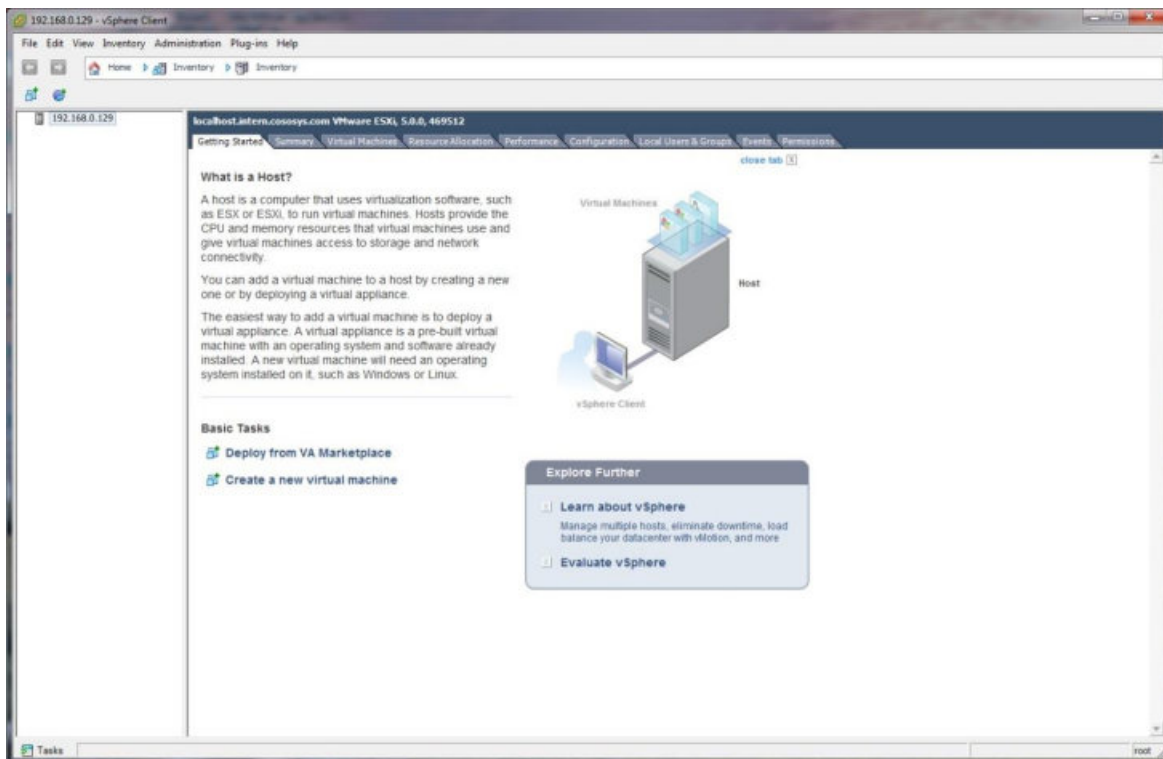


At this point the virtual machine is ready to be started.

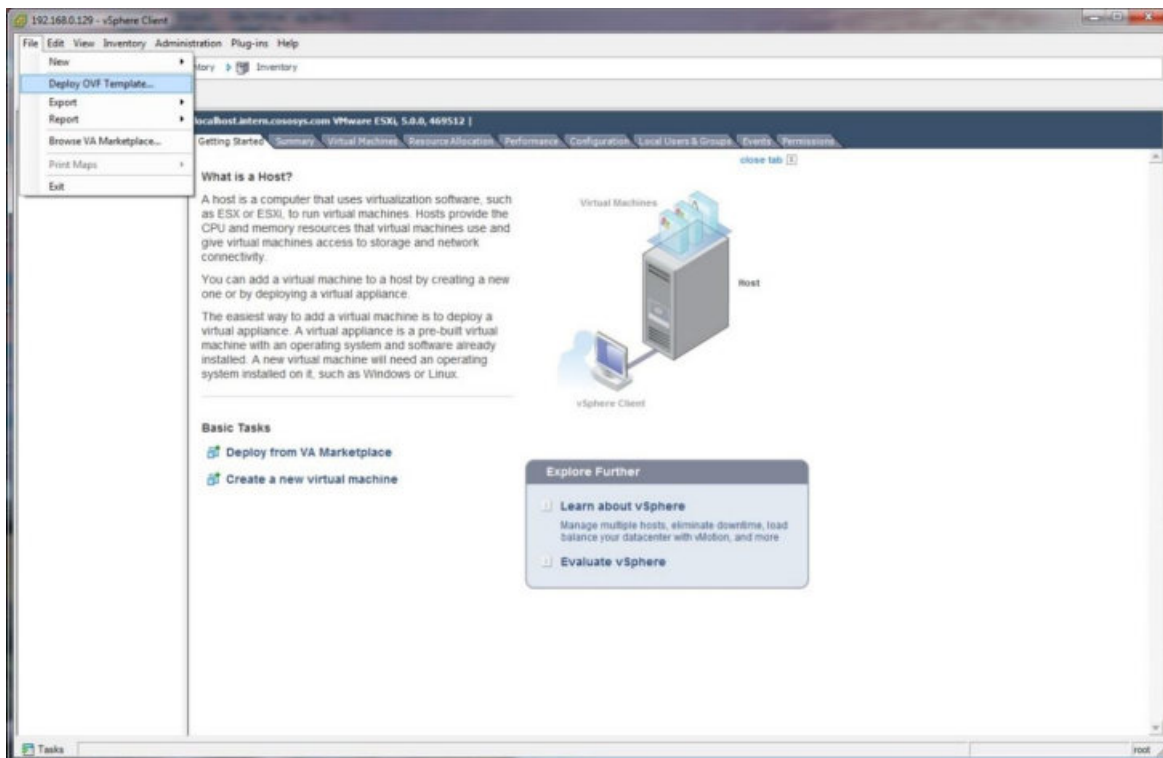
Please follow the Endpoint Protector Appliance User Manual from this point on.

## 2.2. Implementation using VMware vSphere

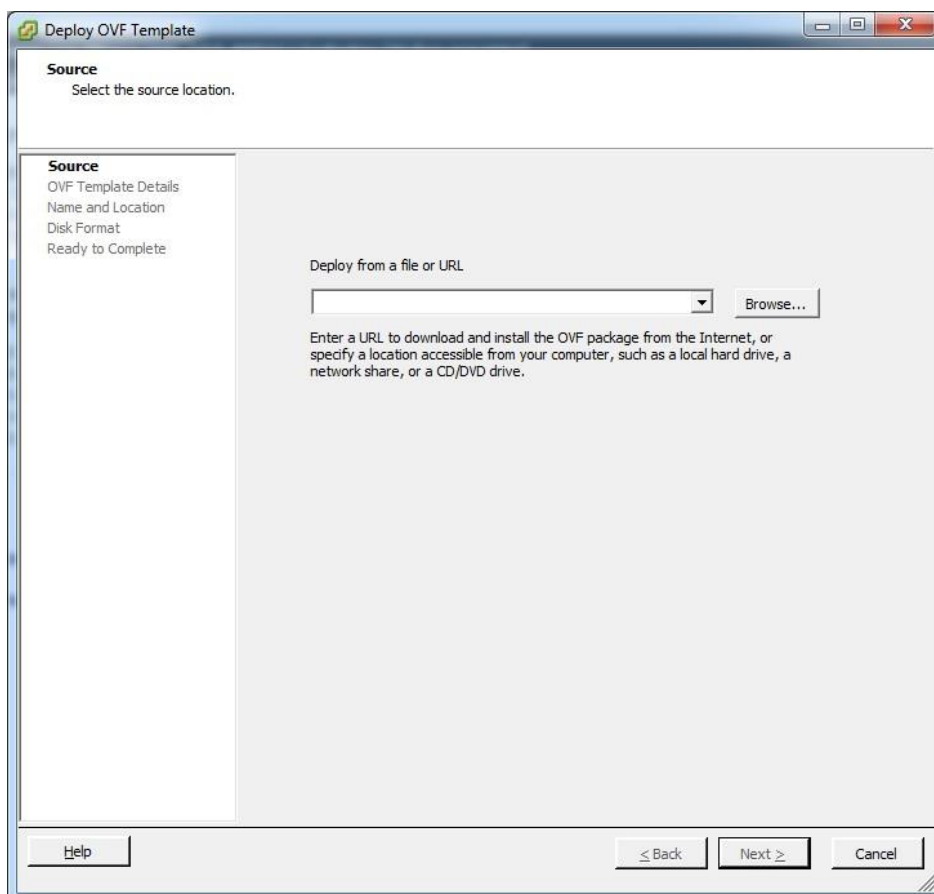
1. Unzip the downloaded package.
2. Start vSphere



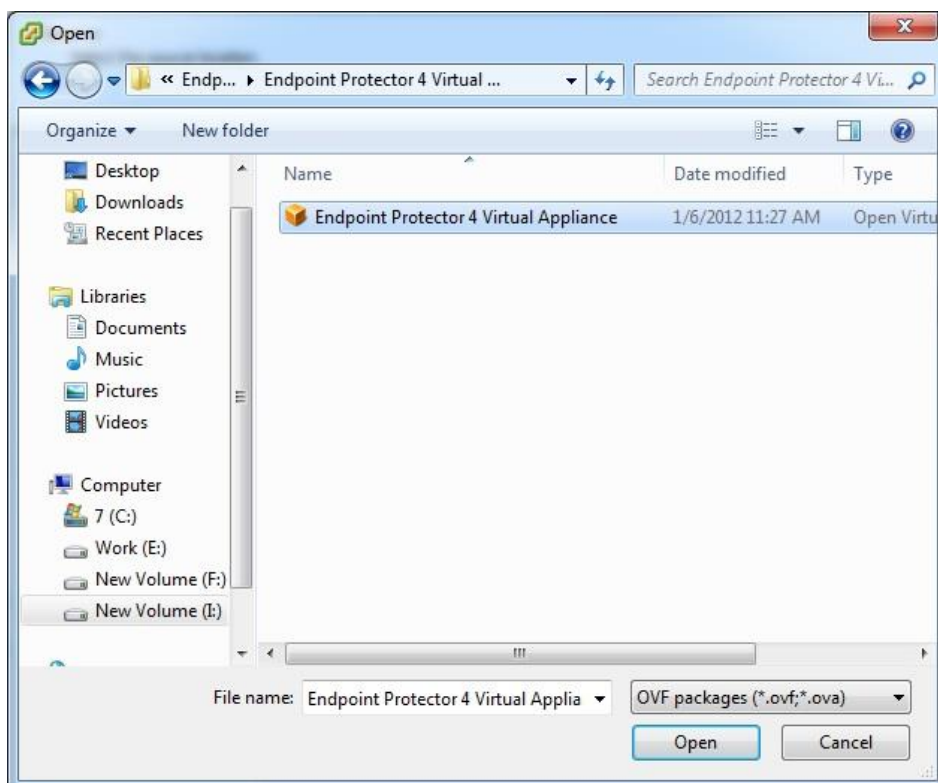
3. To File > Deploy OVF Template.



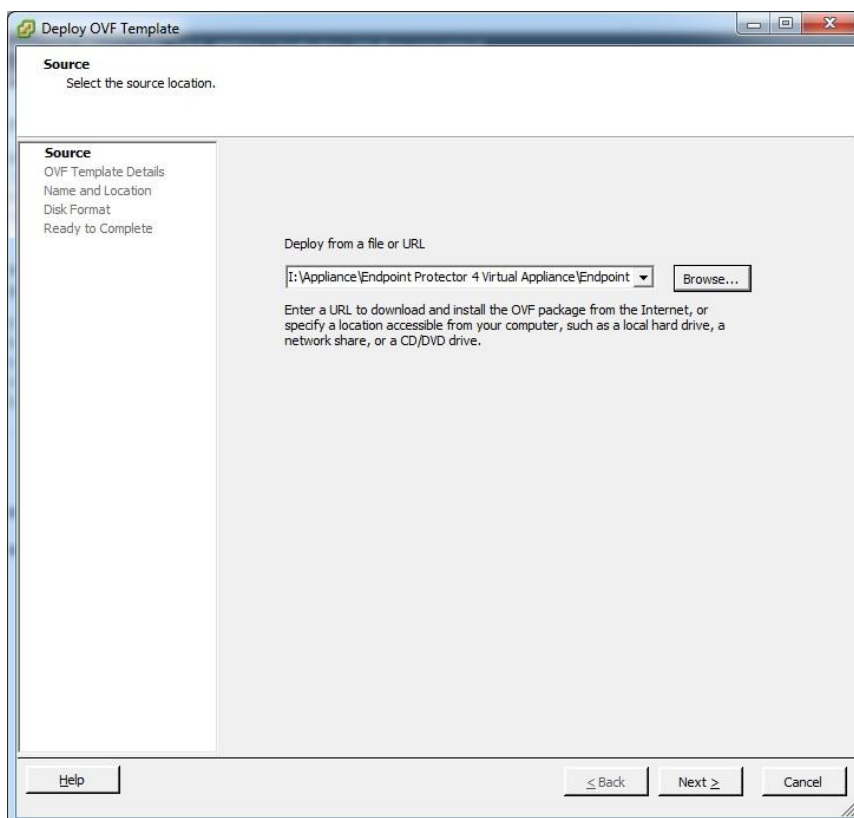
## 4. Press the Browse button.



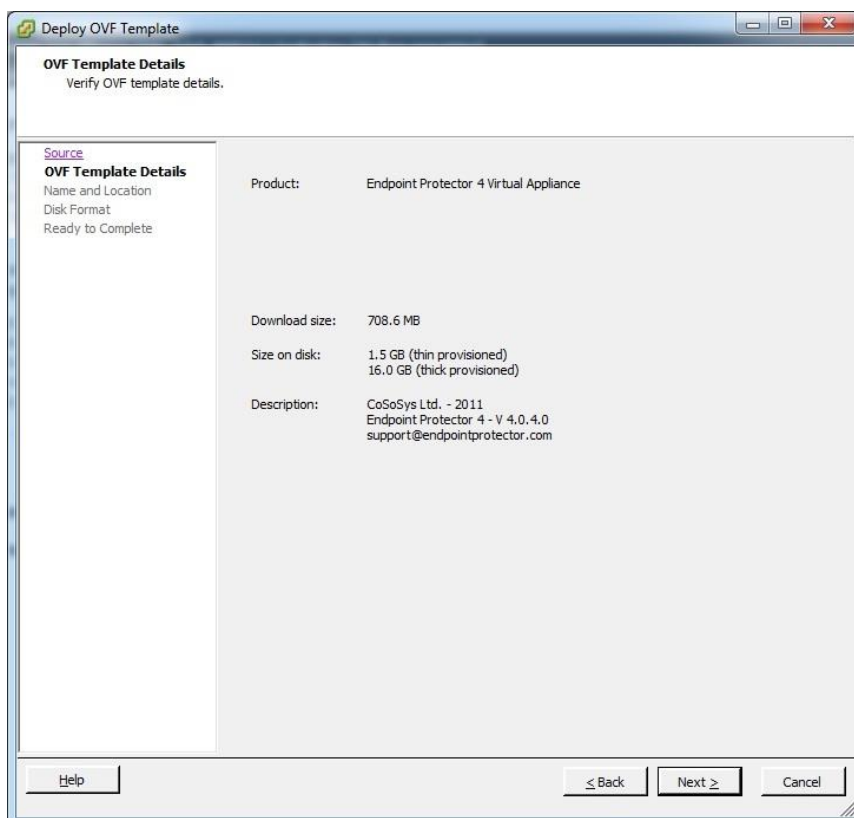
## 5. Browse and select the OVF file from the extracted zip file.



## 6. Press the Next button



## 7. Verify the OVF Template Details and press Next



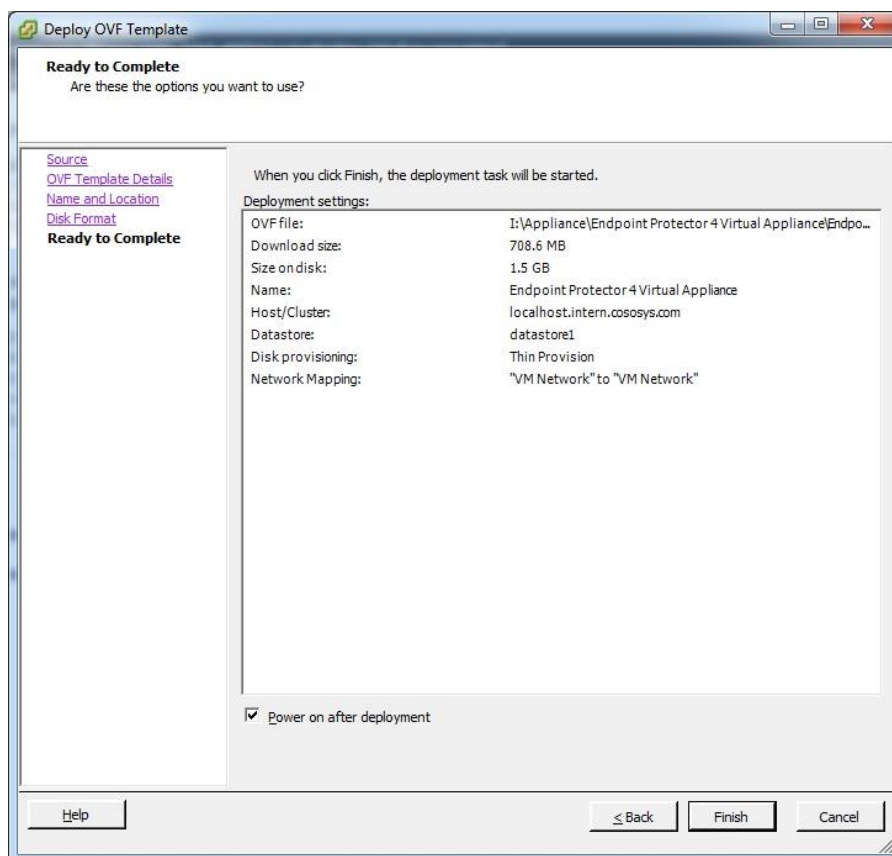
## 8. Specify the name of the OVF template and press Next.

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar says 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, there is a navigation pane with links: 'Source', 'OVF Template Details', 'Name and Location' (which is selected), 'Disk Format', and 'Ready to Complete'. The main area has a 'Name:' label followed by a text box containing 'Endpoint Protector 4 Virtual Appliance'. Below the text box, it says 'The name can contain up to 80 characters and it must be unique within the inventory folder.' At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button on the far right.

## 9. Select "Thin provision" as Disk Format option and press Next

The screenshot shows the 'Deploy OVF Template' wizard window at the 'Disk Format' step. The title bar says 'Deploy OVF Template'. The main heading is 'Disk Format' with the instruction 'In which format do you want to store the virtual disks?'. On the left, the navigation pane shows 'Source', 'OVF Template Details', 'Name and Location', 'Disk Format' (which is selected), and 'Ready to Complete'. The main area shows 'Datastore:' with a dropdown menu set to 'datastore 1'. Below that, 'Available space (GB):' is shown as '66.0'. There are three radio button options: 'Thick Provision Lazy Zeroed', 'Thick Provision Eager Zeroed', and 'Thin Provision' (which is selected). At the bottom, there are three buttons: 'Help', '< Back', and 'Next >', and a 'Cancel' button on the far right.

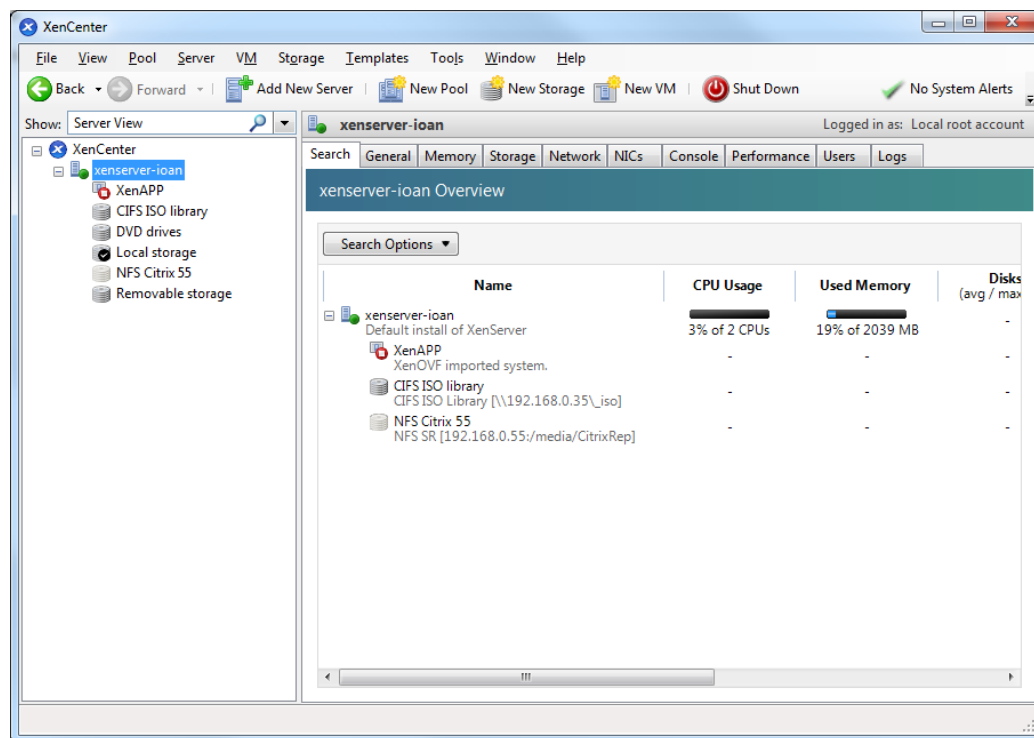
10. Press the Finish button to complete the installation.



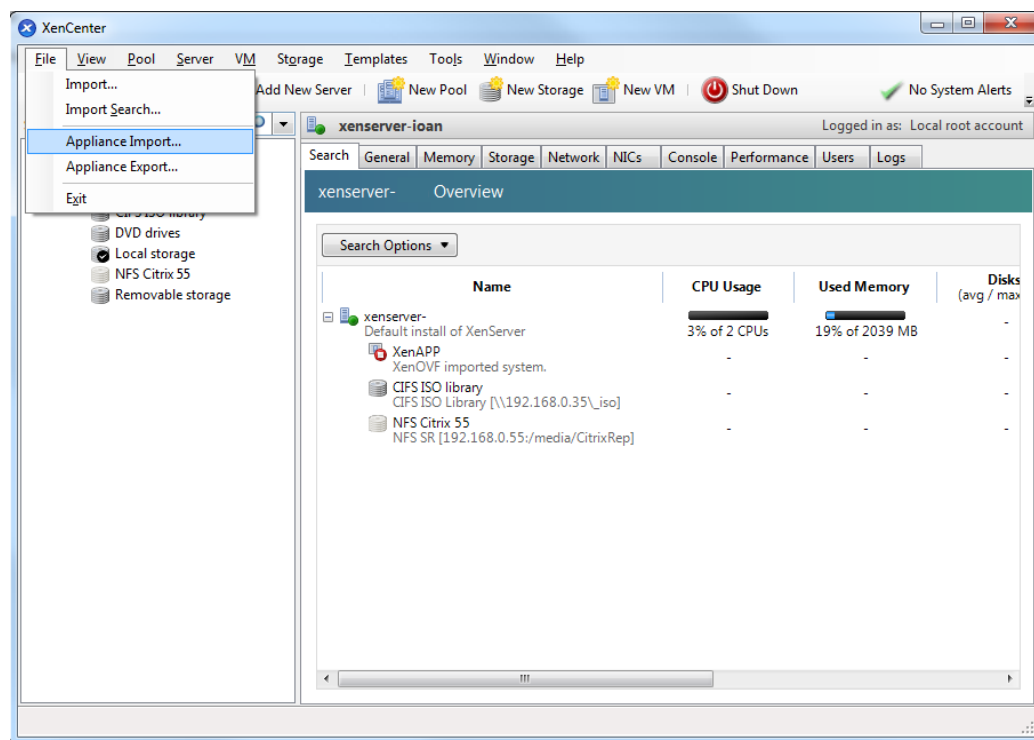


## 2.3. Implementing in Citrix XenServer 5.6 using OVF Format

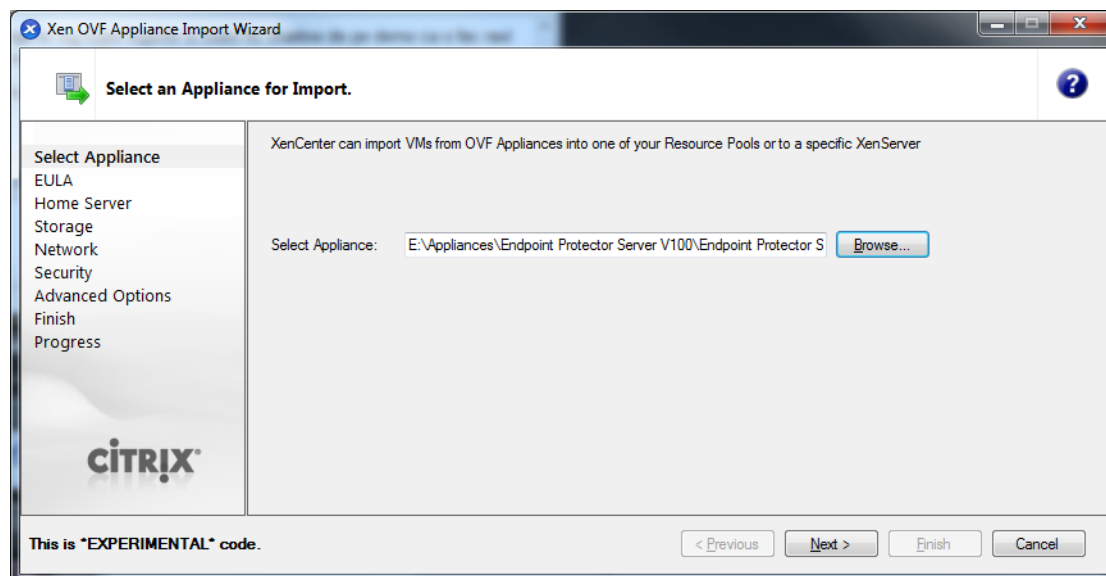
1. Unzip the downloaded package
2. Start XenCenter



3. Go To File > Appliance Import



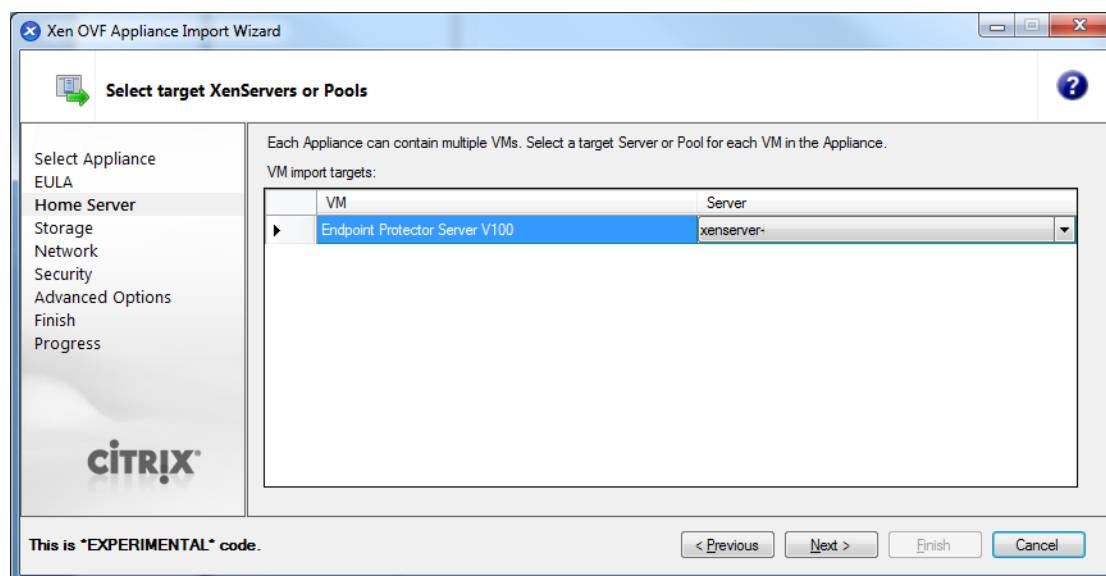
## 4. Select the OVF file



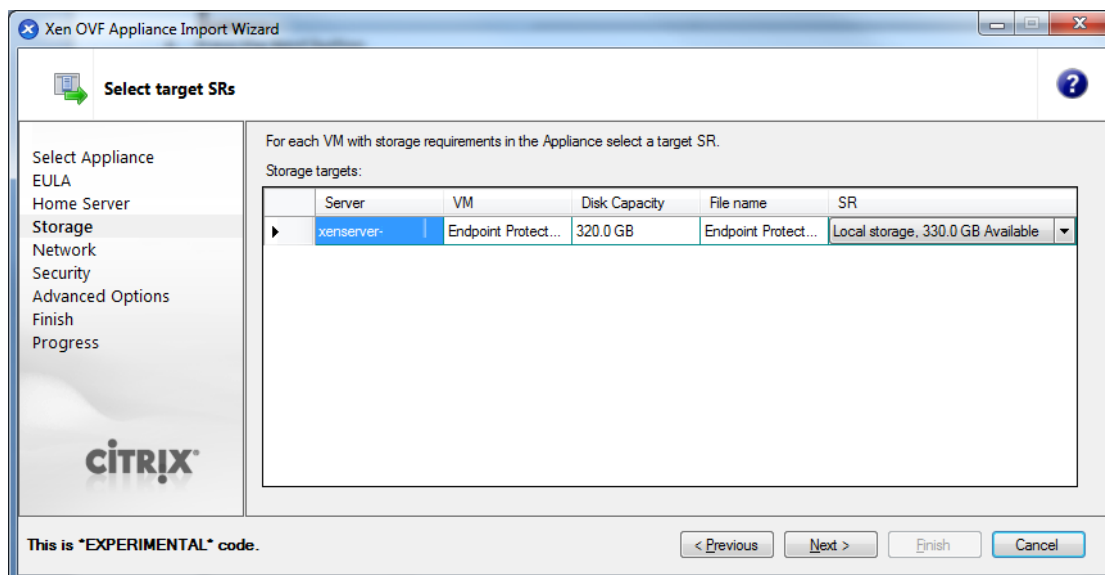
## 5. Press the Next button

## 6. Read and accept the EULA, then press Next

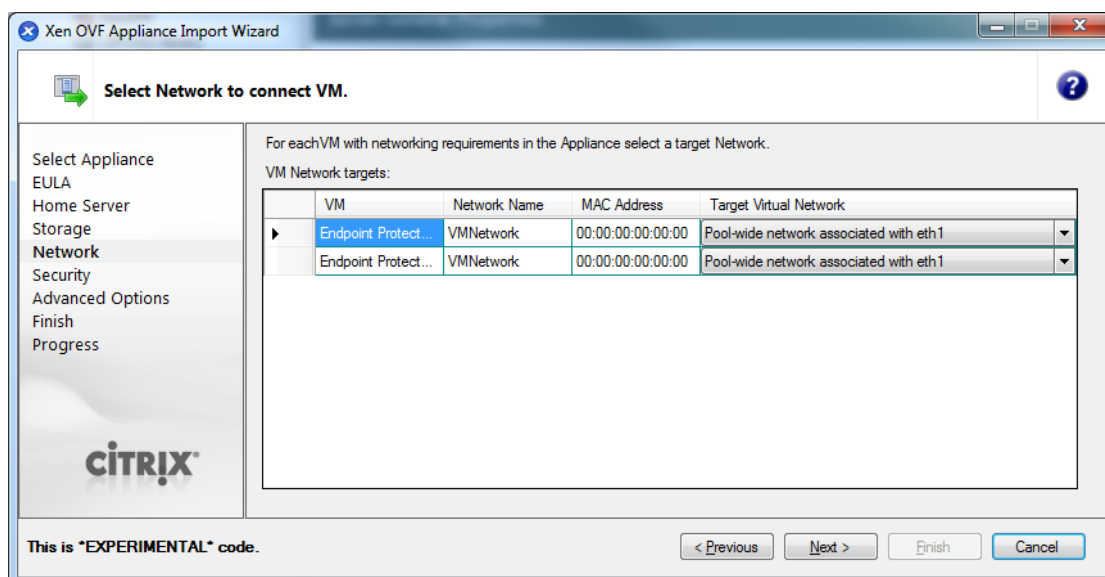
## 7. Select the target for this Virtual Appliance



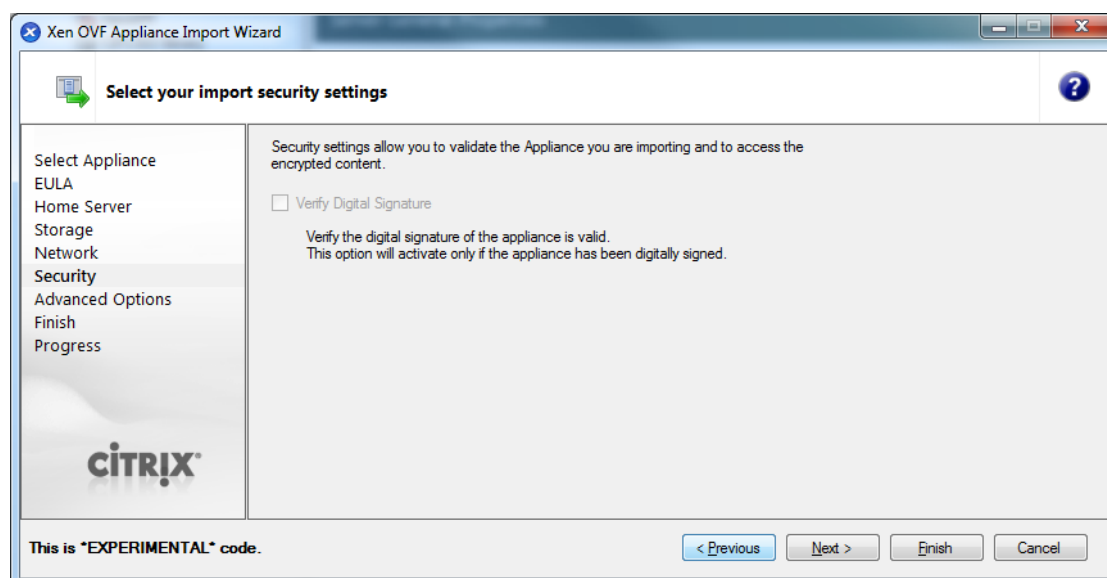
## 8. Select the storage location



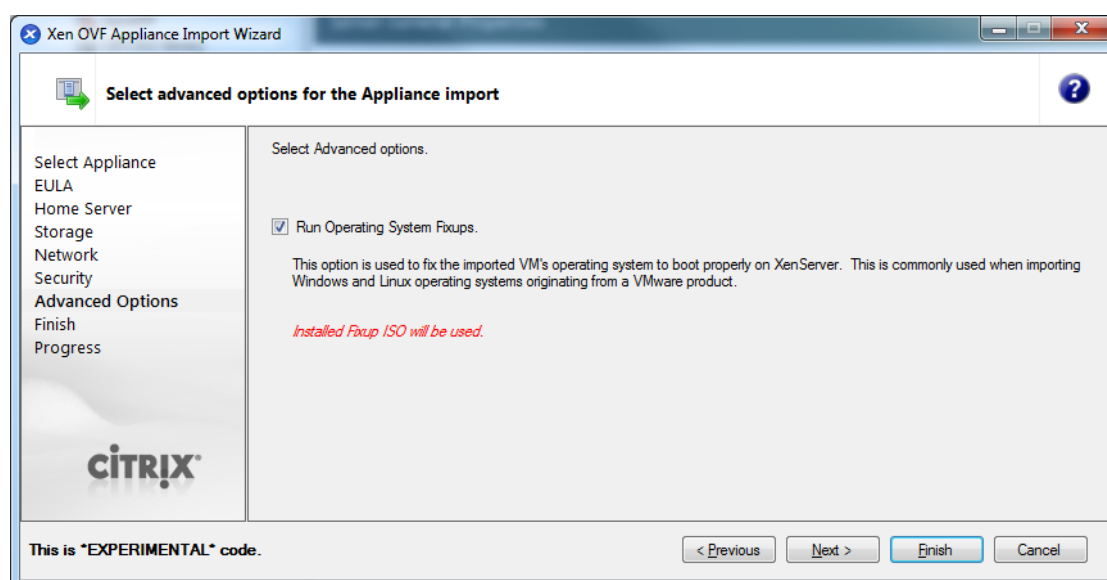
9. Select you network (keep default values)



10. On Security Screen click on Next button

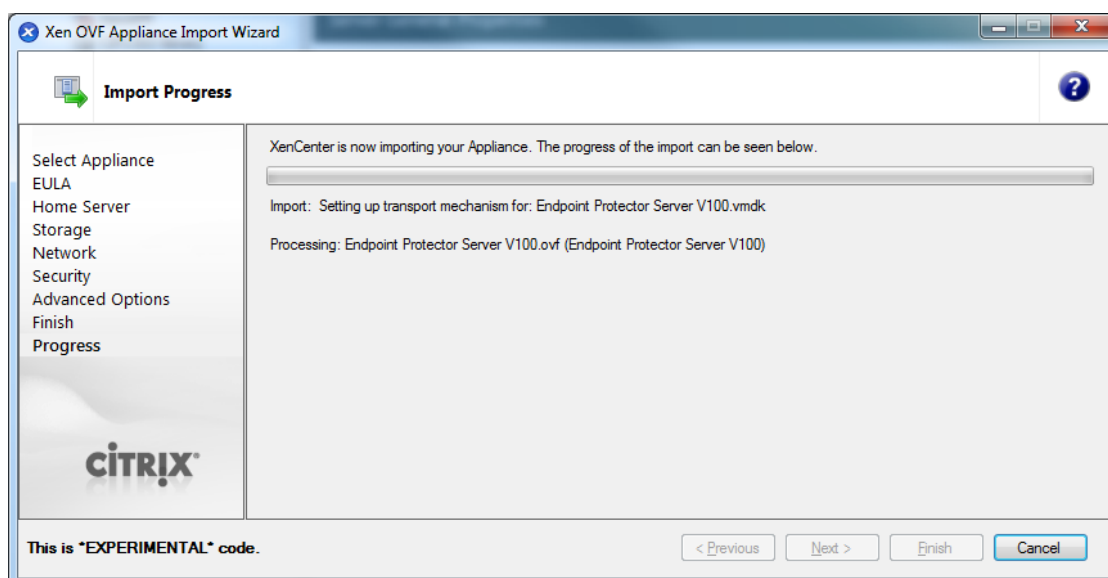


11. On Advanced Options screen click Next



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.

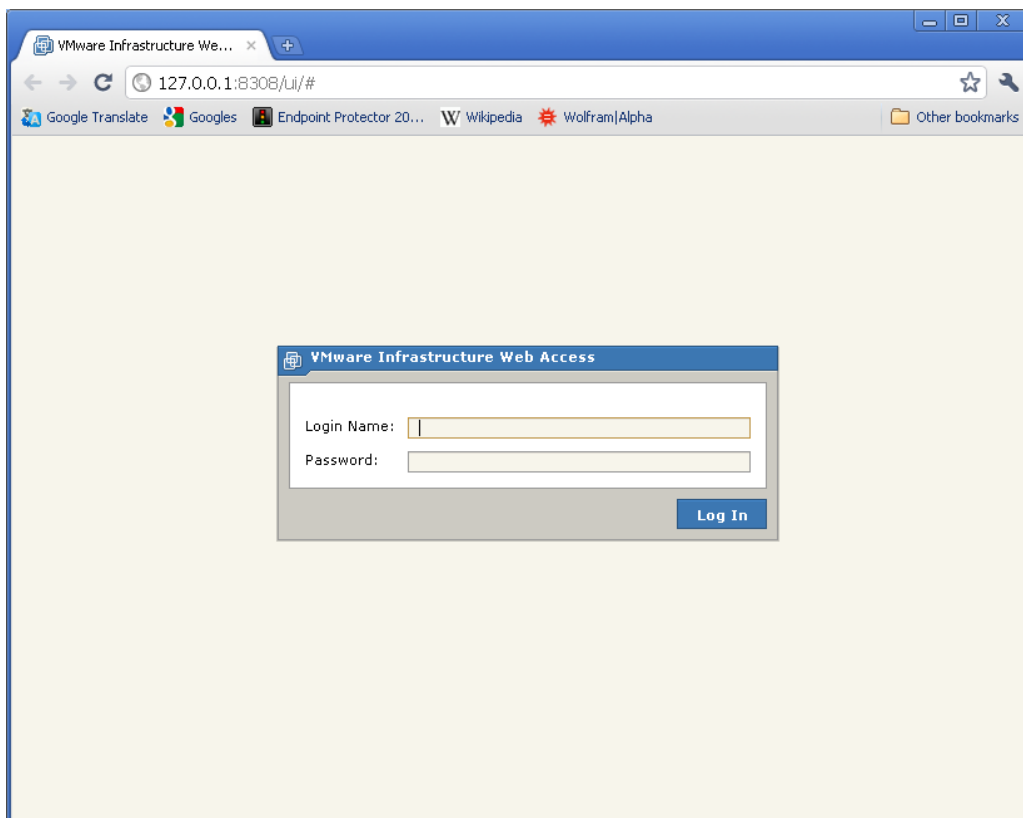
Please follow the Endpoint Protector Appliance User Manual from this point on.

# 3. Using the VMX format

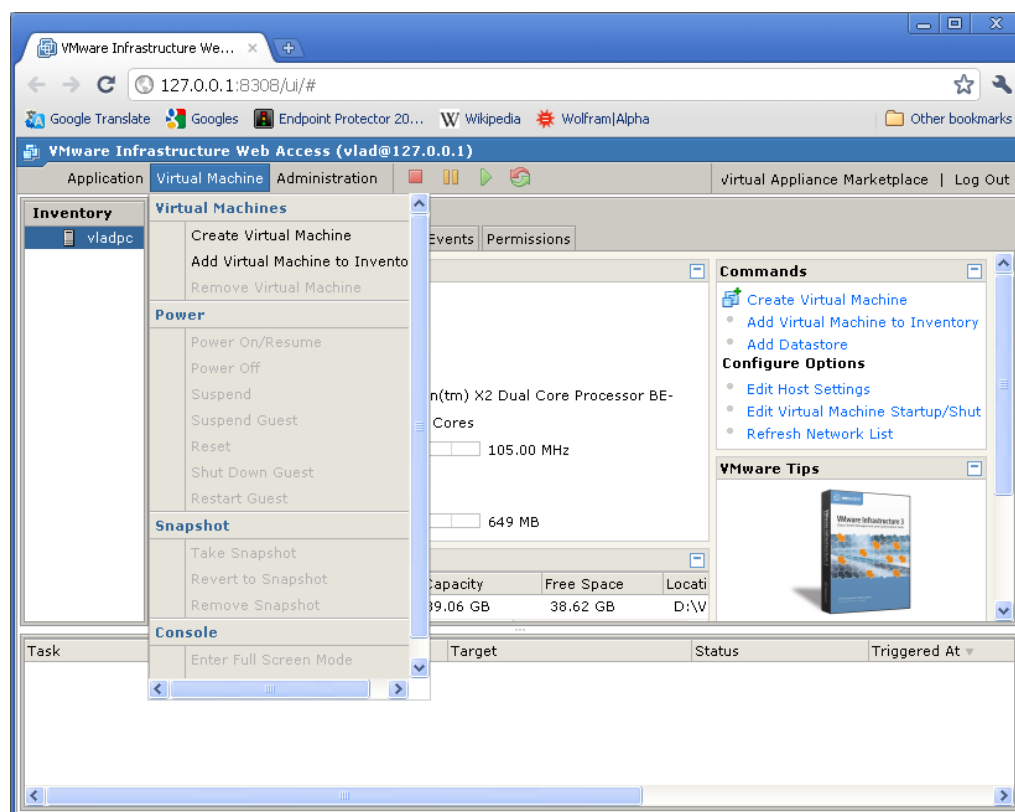
There are several options to implement the Endpoint Protector Virtual Appliance using the OVMX format. The way to do this is explained below.

## 3.1. Implementing using VMware Server

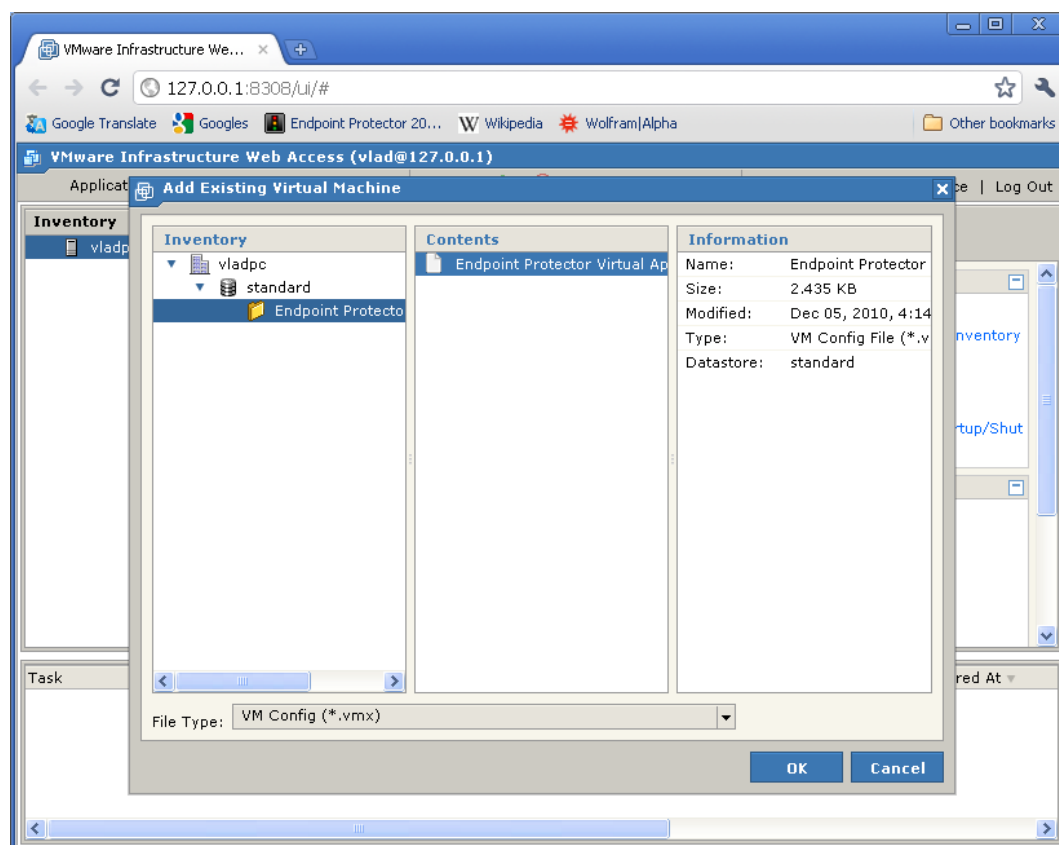
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored
2. Open your VMware Server web interface and login



### 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

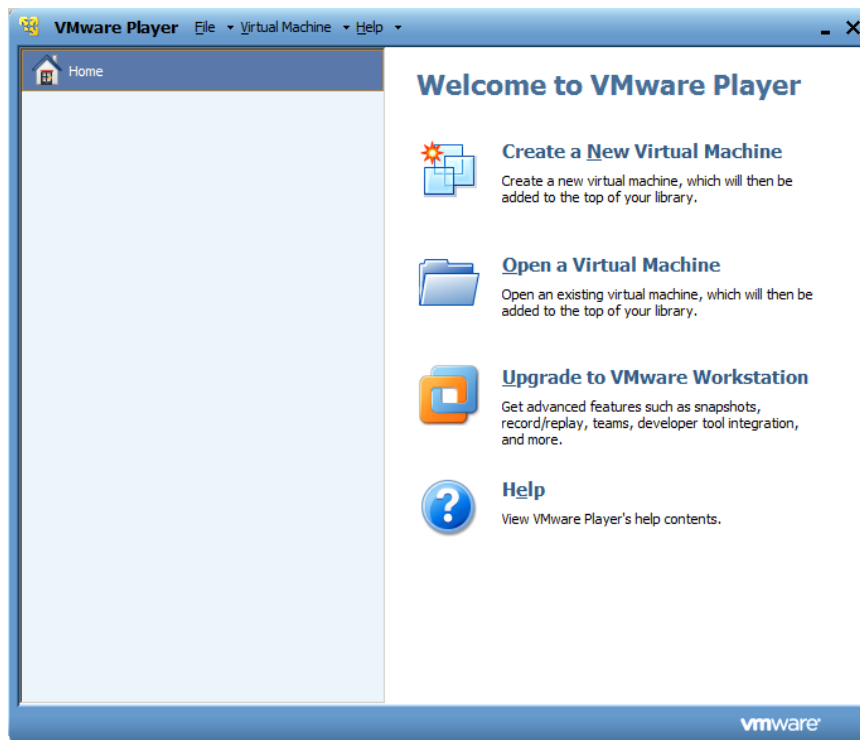


At this point the Virtual Machine is ready to be started.

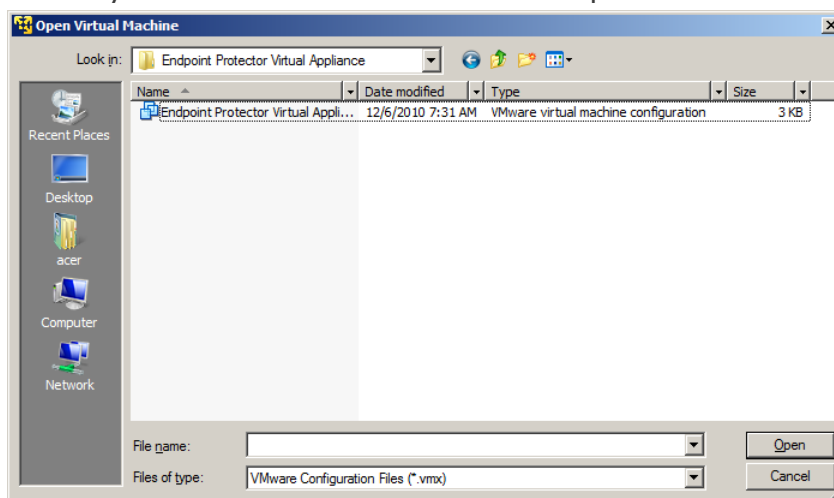
Please follow the Endpoint Protector Appliance User Manual from this point on.

## 3.2. Implementing using VMware Player

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

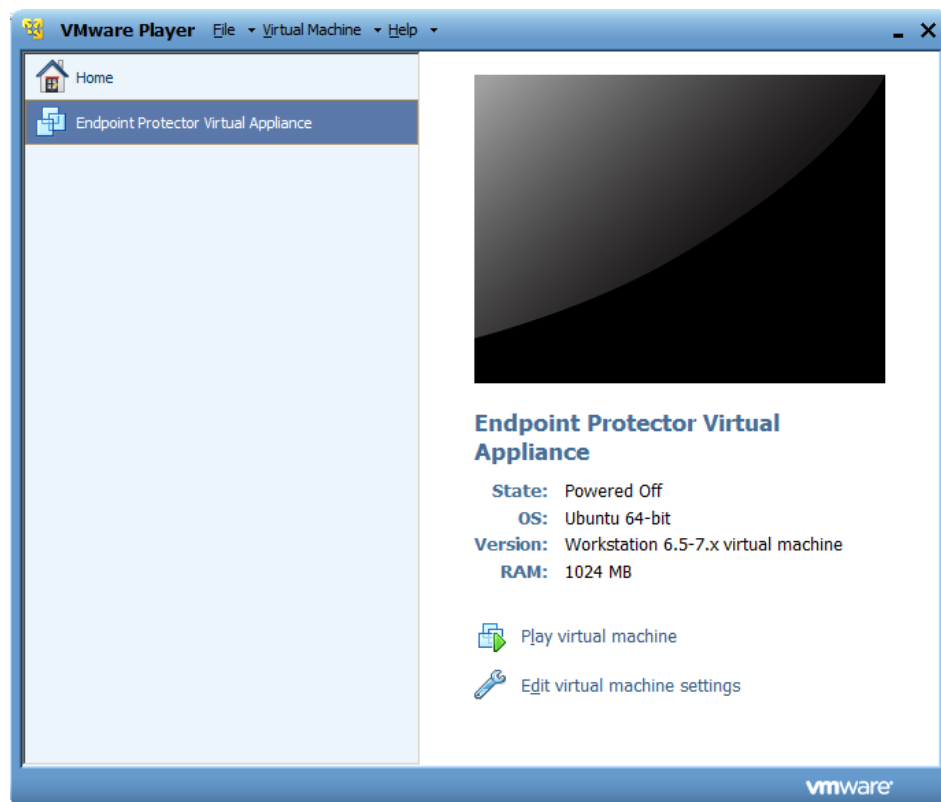


3. Select Open a Virtual Machine and select the VMX file from the location where you extracted it and then click Open





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.

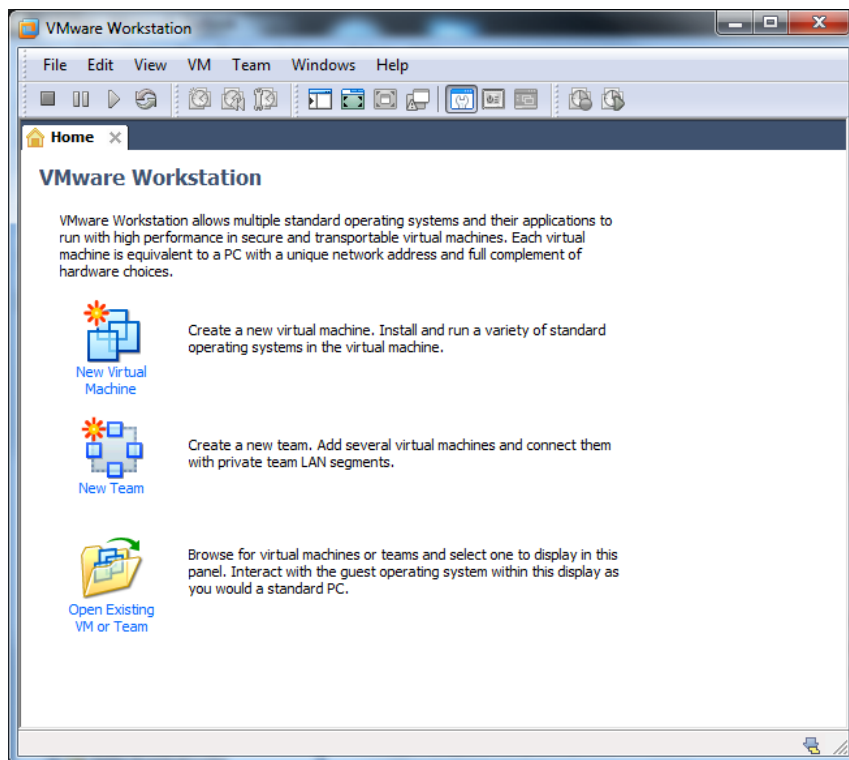
Please follow the Endpoint Protector Appliance User Manual from this point on.

### Note!

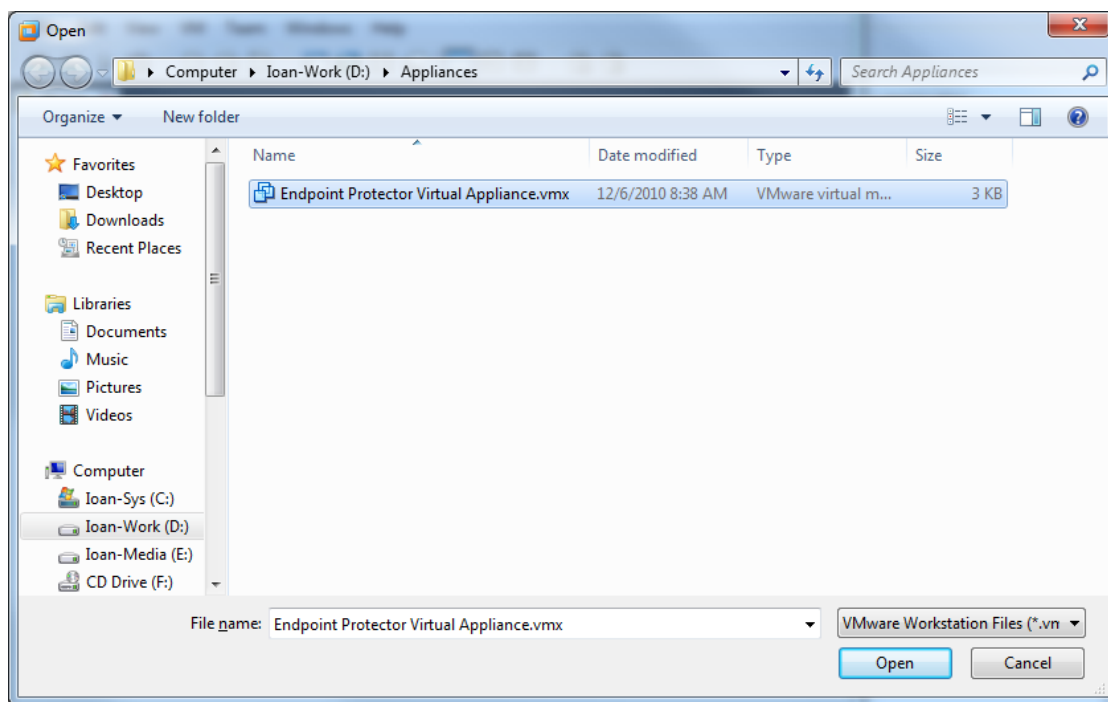
Do not suspend the VMware Player while Endpoint Protector Virtual Appliance is running! Also, do not shut down your computer while VMware Player is running.

### 3.3. Implementing using VMware Workstation

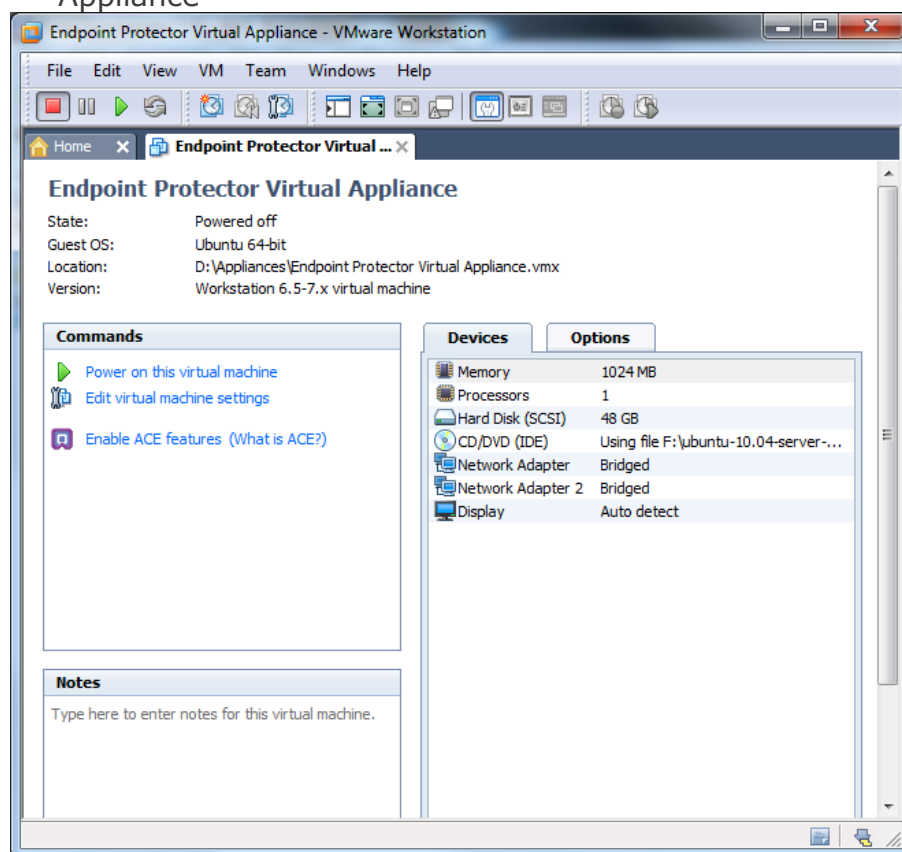
1. Extract the downloaded Endpoint Protector Virtual Appliance package and move the files to the path where your virtual machines are stored
2. Open VMWare Workstation



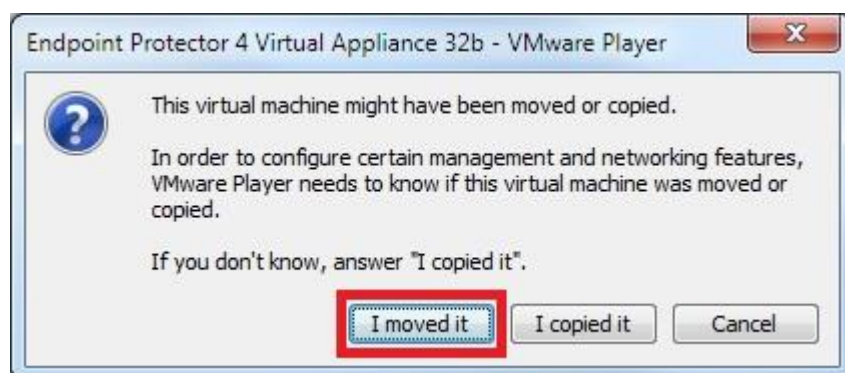
3. Select Open Existing VM or Team



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.

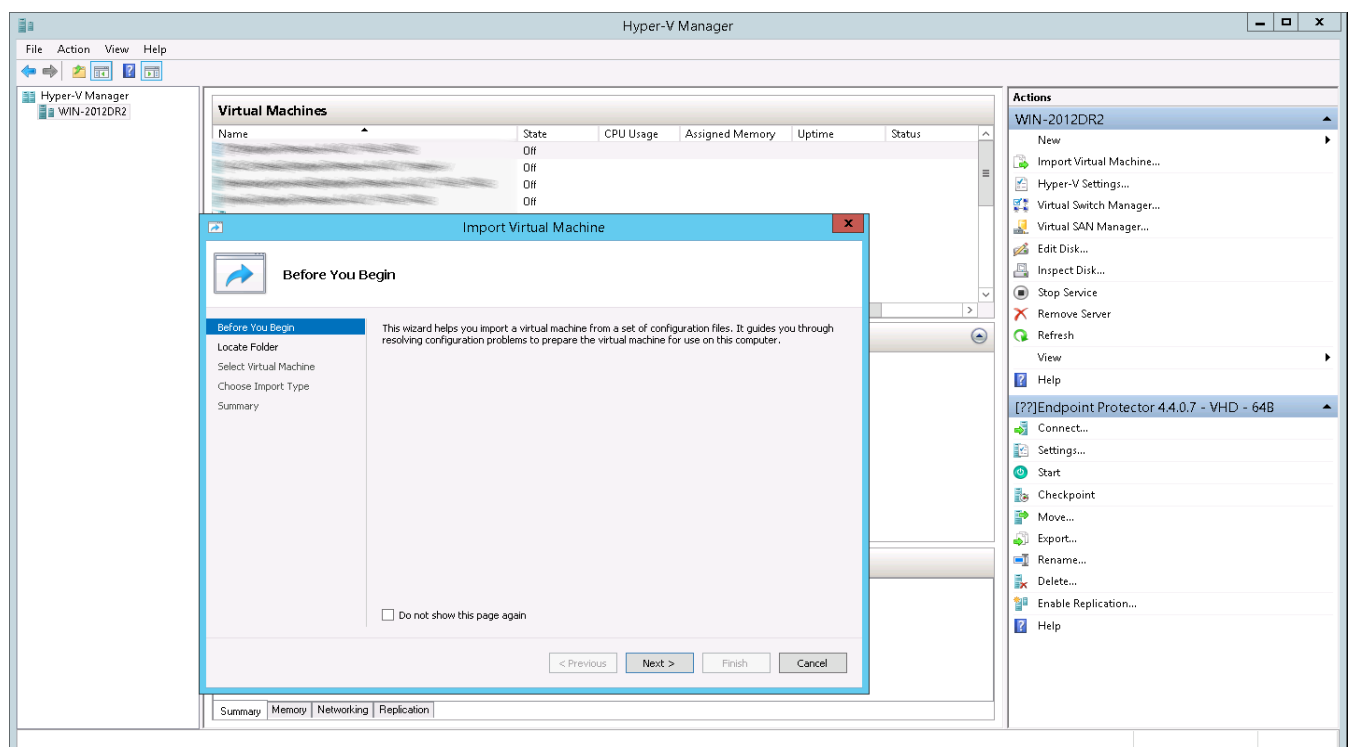
Please follow the Endpoint Protector Appliance User Manual from this point on.

# 4. Using the VHD format

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

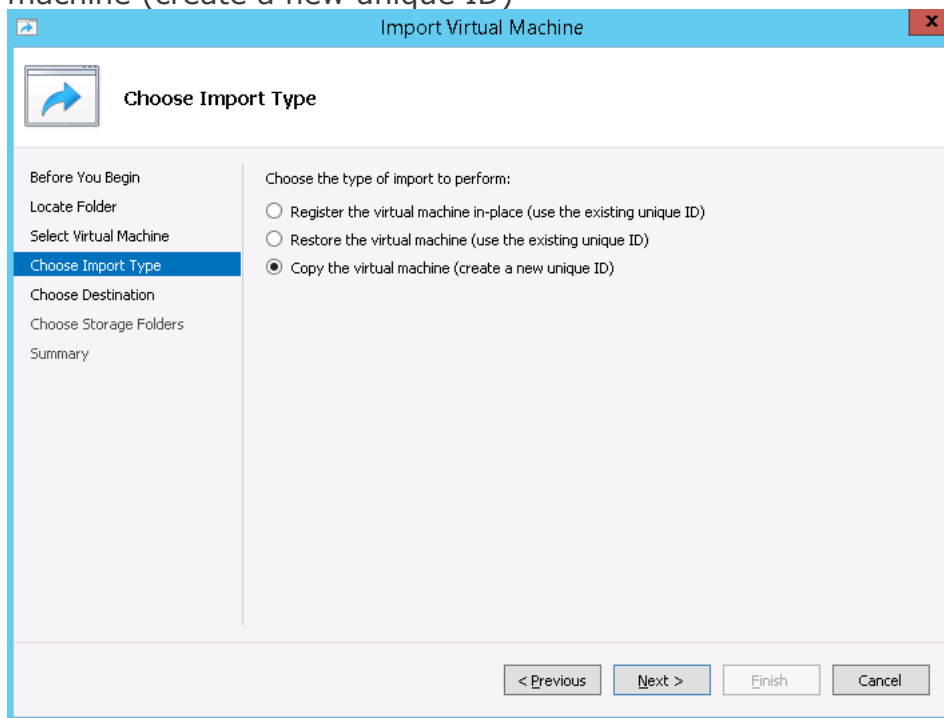
## 4.1. Implementing using Microsoft Hyper-V 2012

1. Extract the downloaded Endpoint Protector Virtual Appliance .zip package
2. Start Hyper-V Manager
3. Select from the right-side box the option to Import Virtual Machine

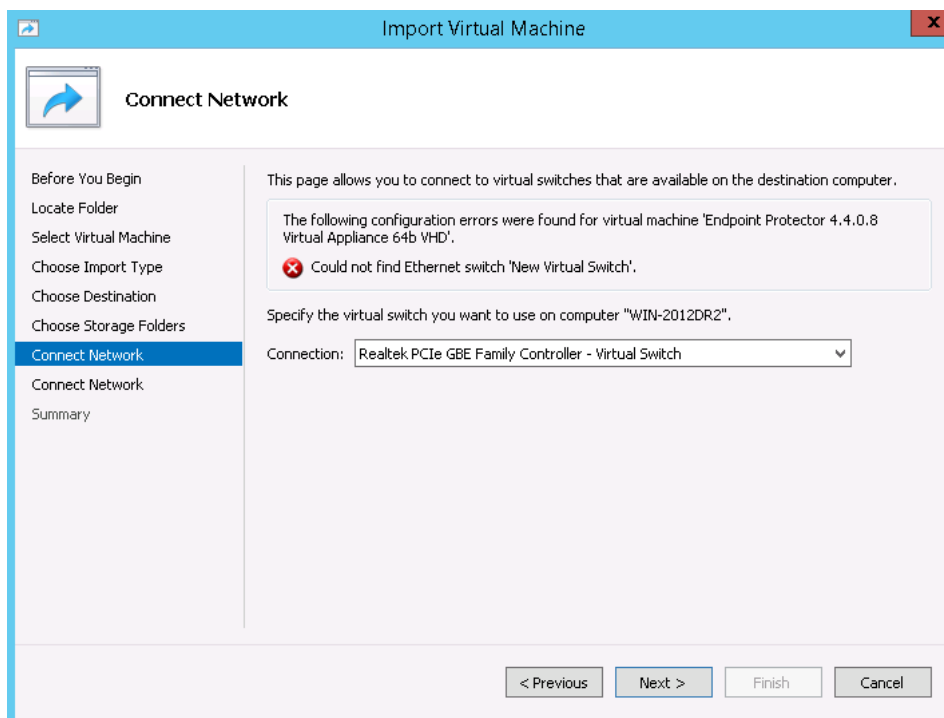


3.1 Select the folder containing the appliances' folders and files.

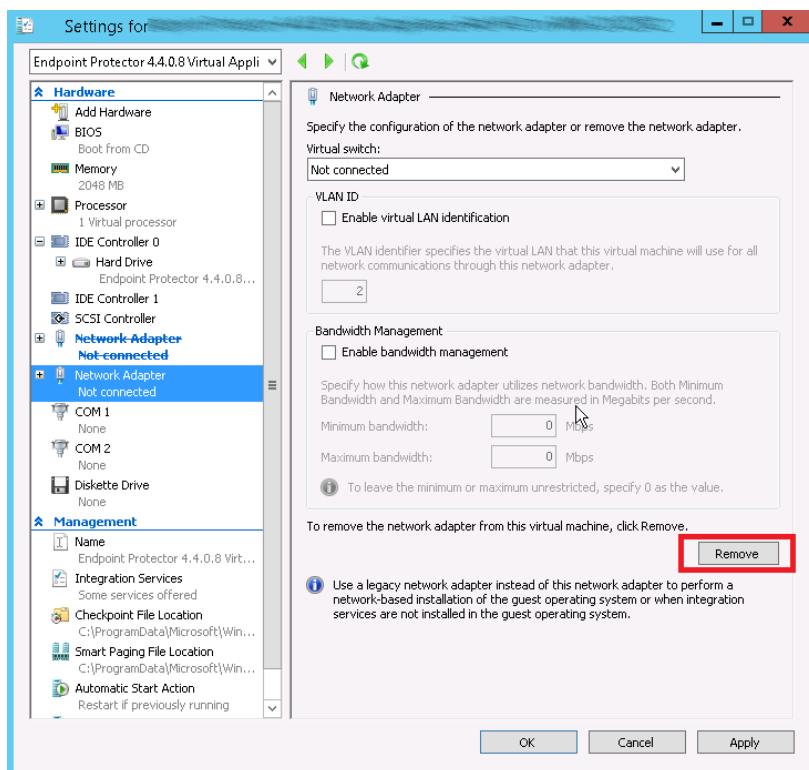
3.2 At the step "Choose Import Type" select the option to Copy the virtual machine (create a new unique ID)



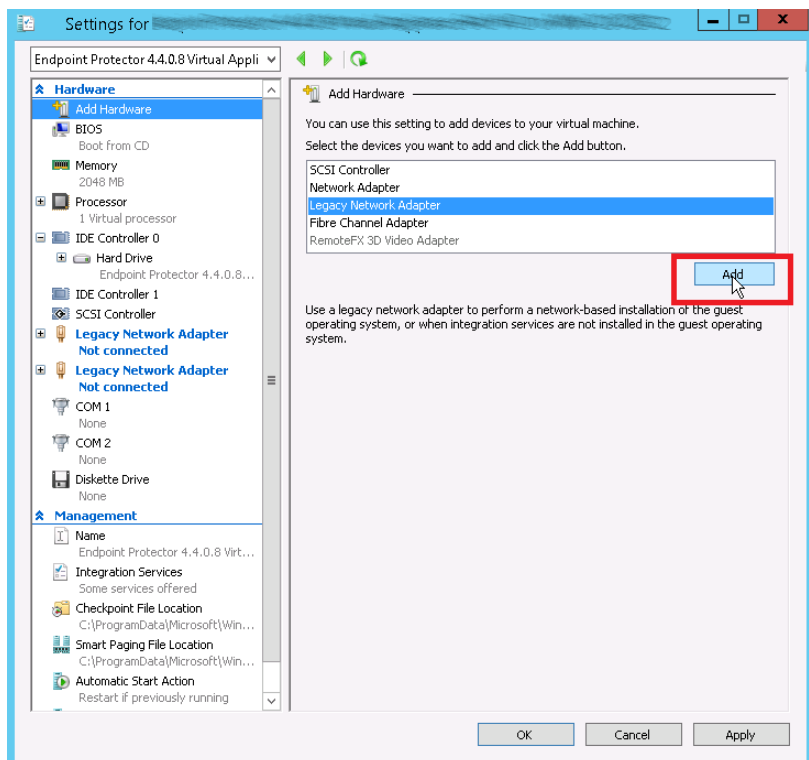
3.3 The "Connect Network" step will prompt with 2 errors, one for each Network Adapter. Ignore these and press Next, Next and then Finish.



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



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



**Note!**

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

8. Click on Apply.

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

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

# 5. Virtual Appliance Setup Wizard

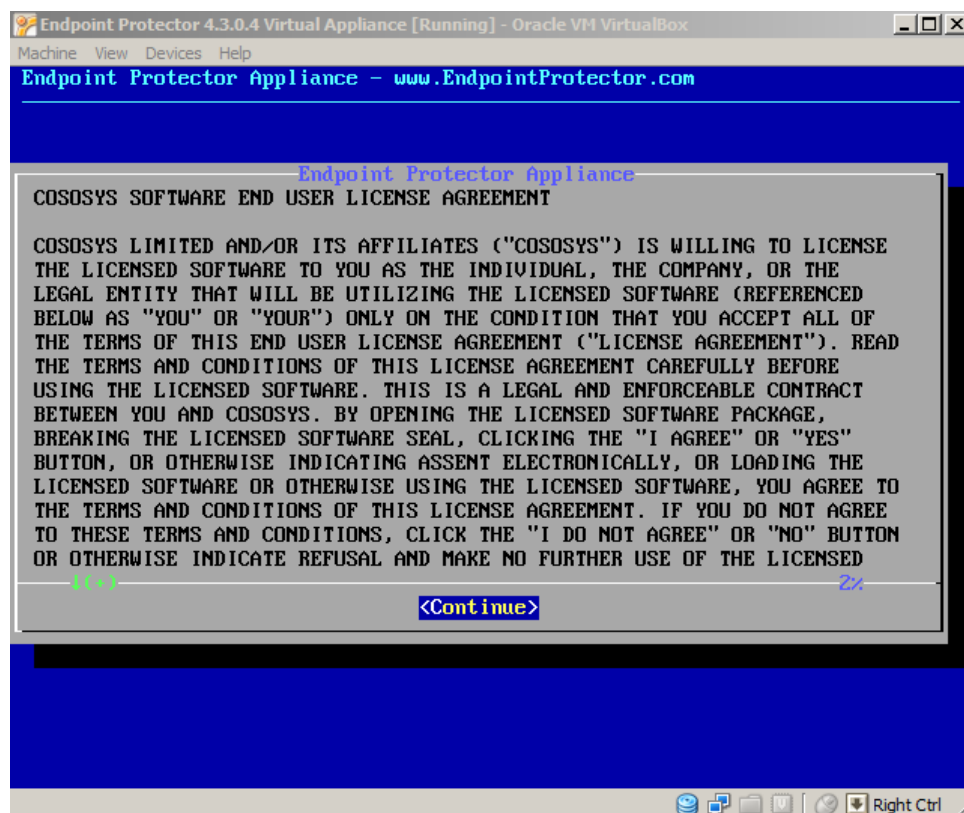
The Endpoint Protector Appliance (virtual or hardware) requires incoming traffic for ports 443 and 80 to be whitelisted from the firewall. They are used for:

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

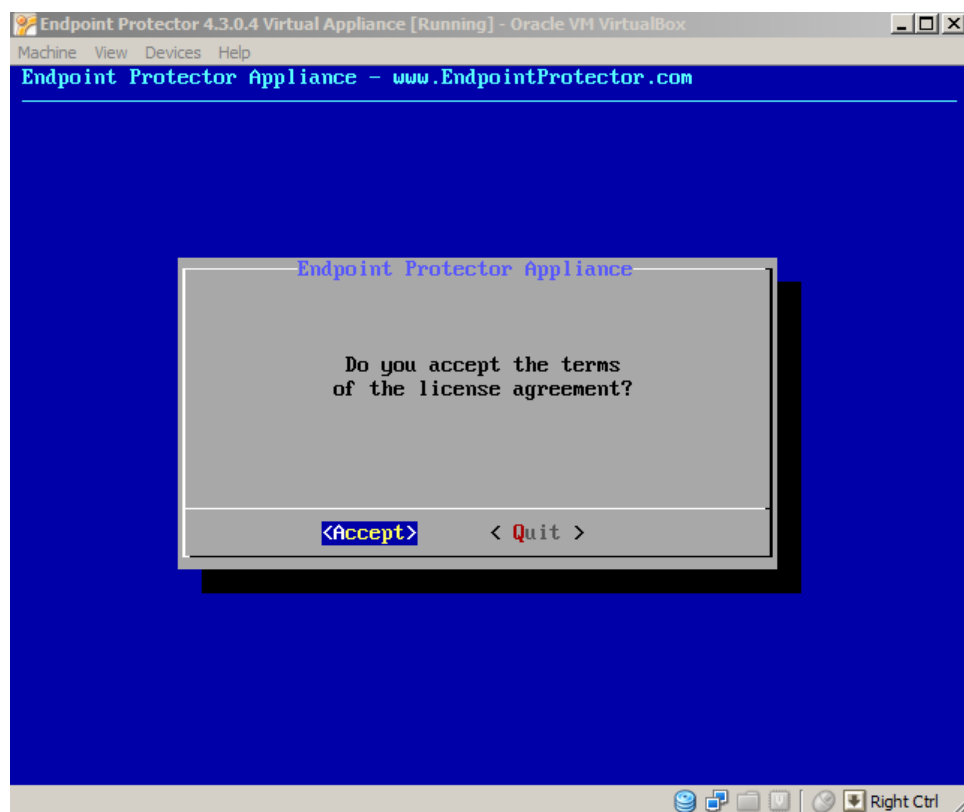
To configuring the Endpoint Protector Appliance for the first time, fallow the steps below.



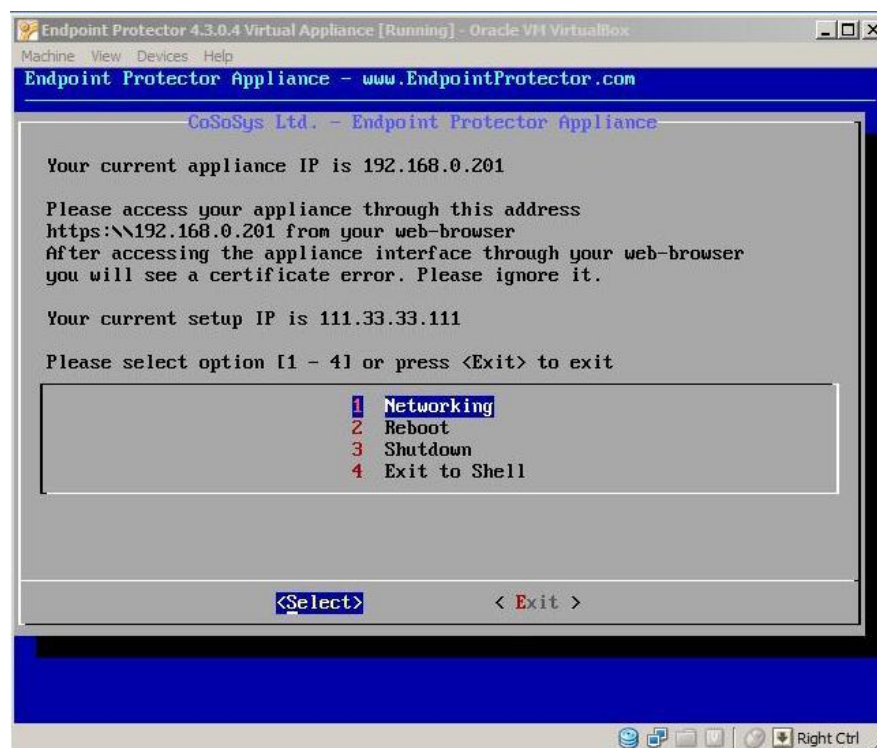
## 1. Press Continue when finished reading the End User License Agreement



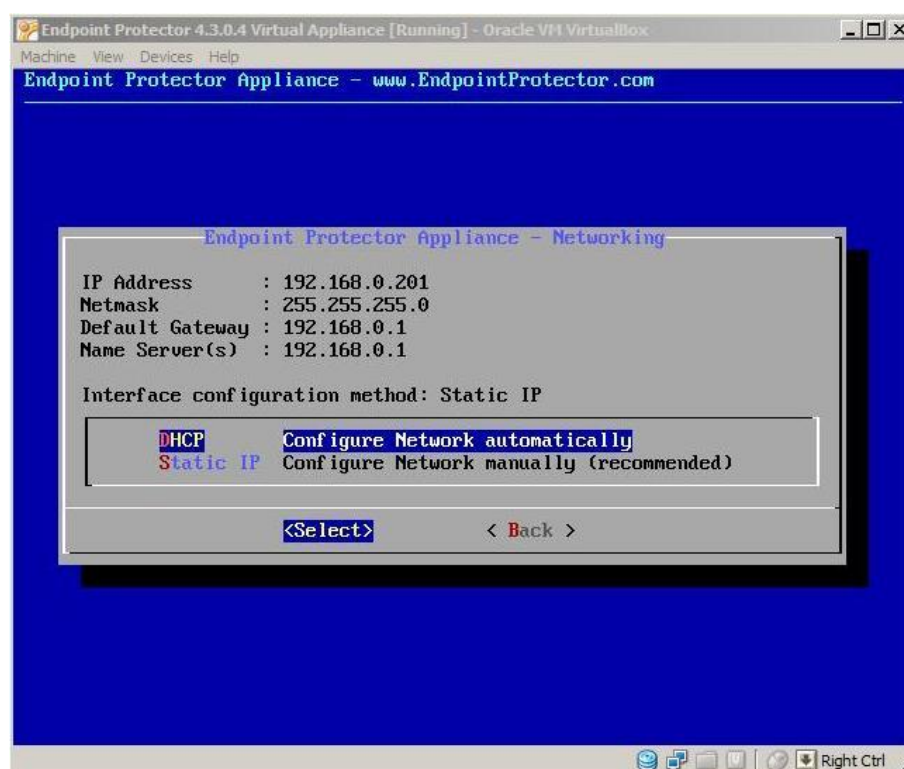
## 2. Press Accept



### 3. Select Networking



4. The configuration methods are now available.

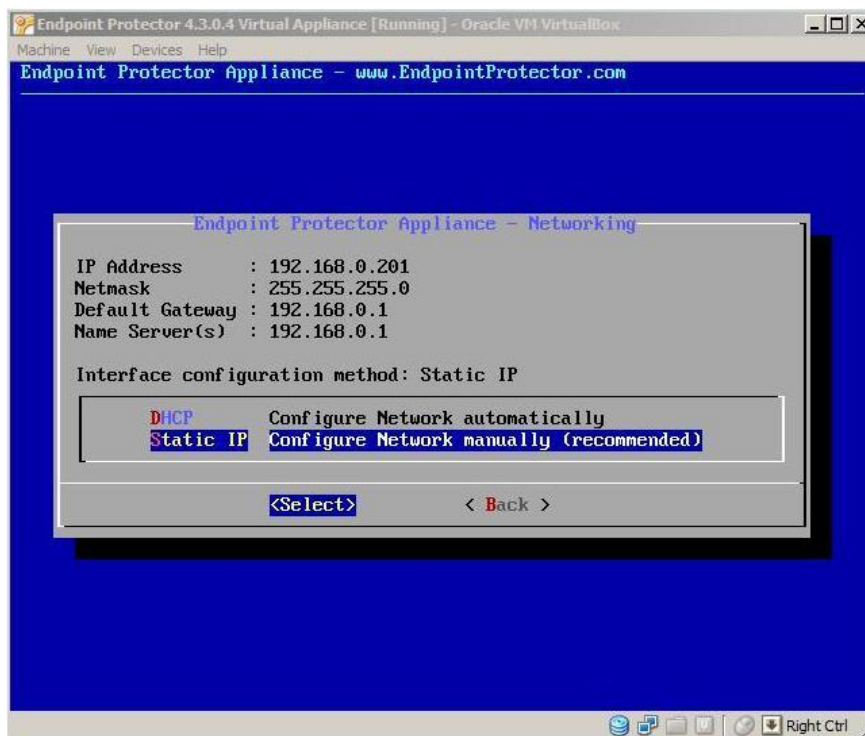


#### Note!

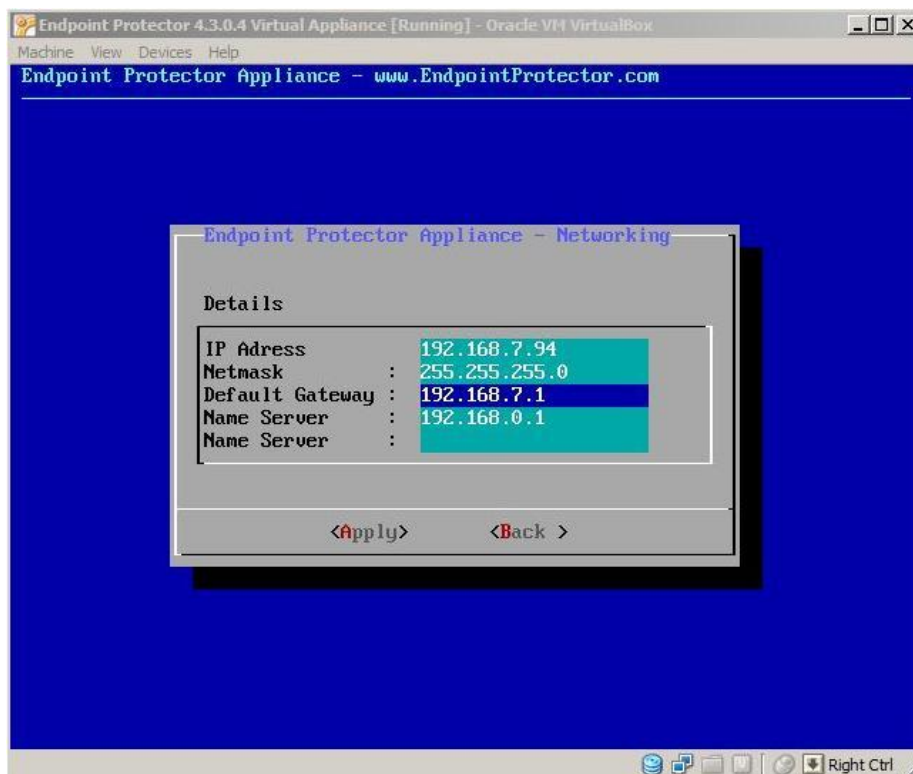
We recommend a manual configuration of the network settings.

### 5.1.1 Manual configuration

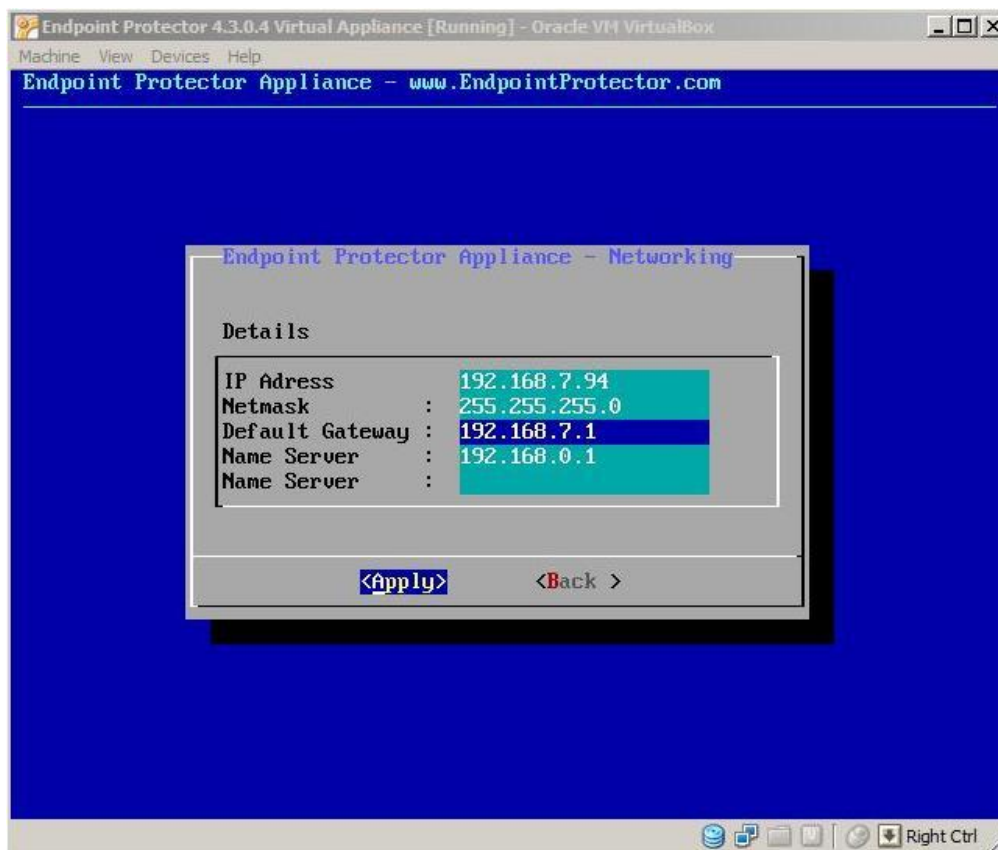
1. Select Configure Network manually (recommended)



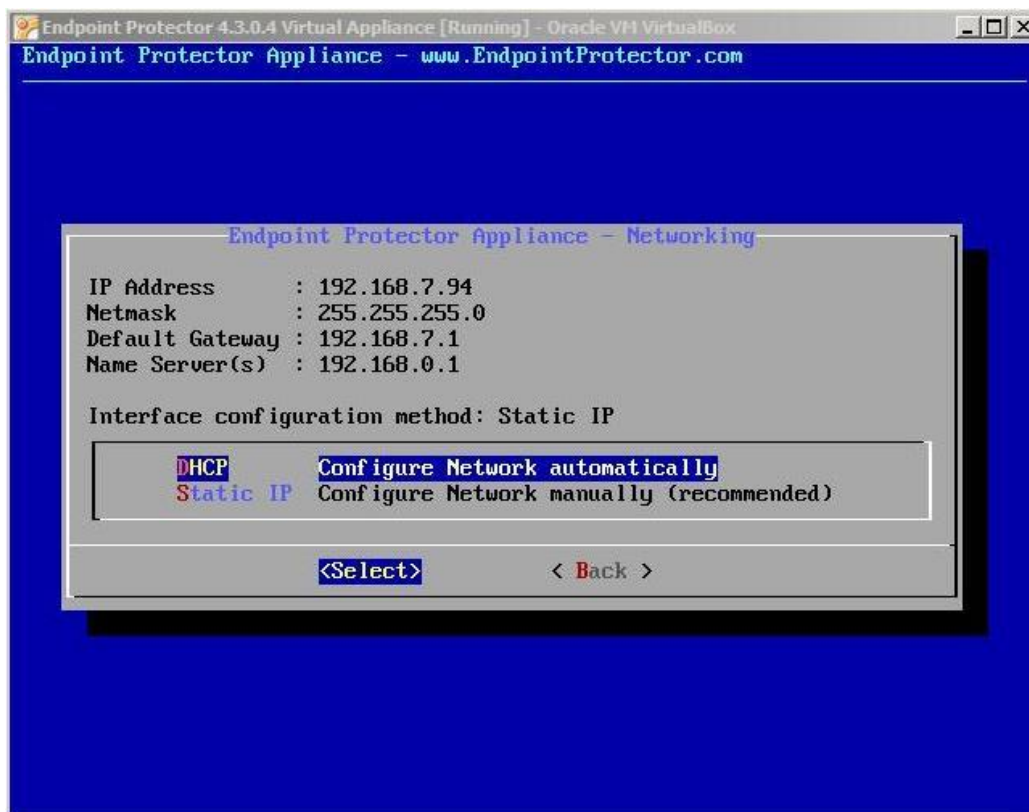
2. Set the IP Address, and Default Gateway (in our example we set the IP Address as 192.168.7.94 and the Default Gateway as 192.168.7.1).



### 3. Press Tab



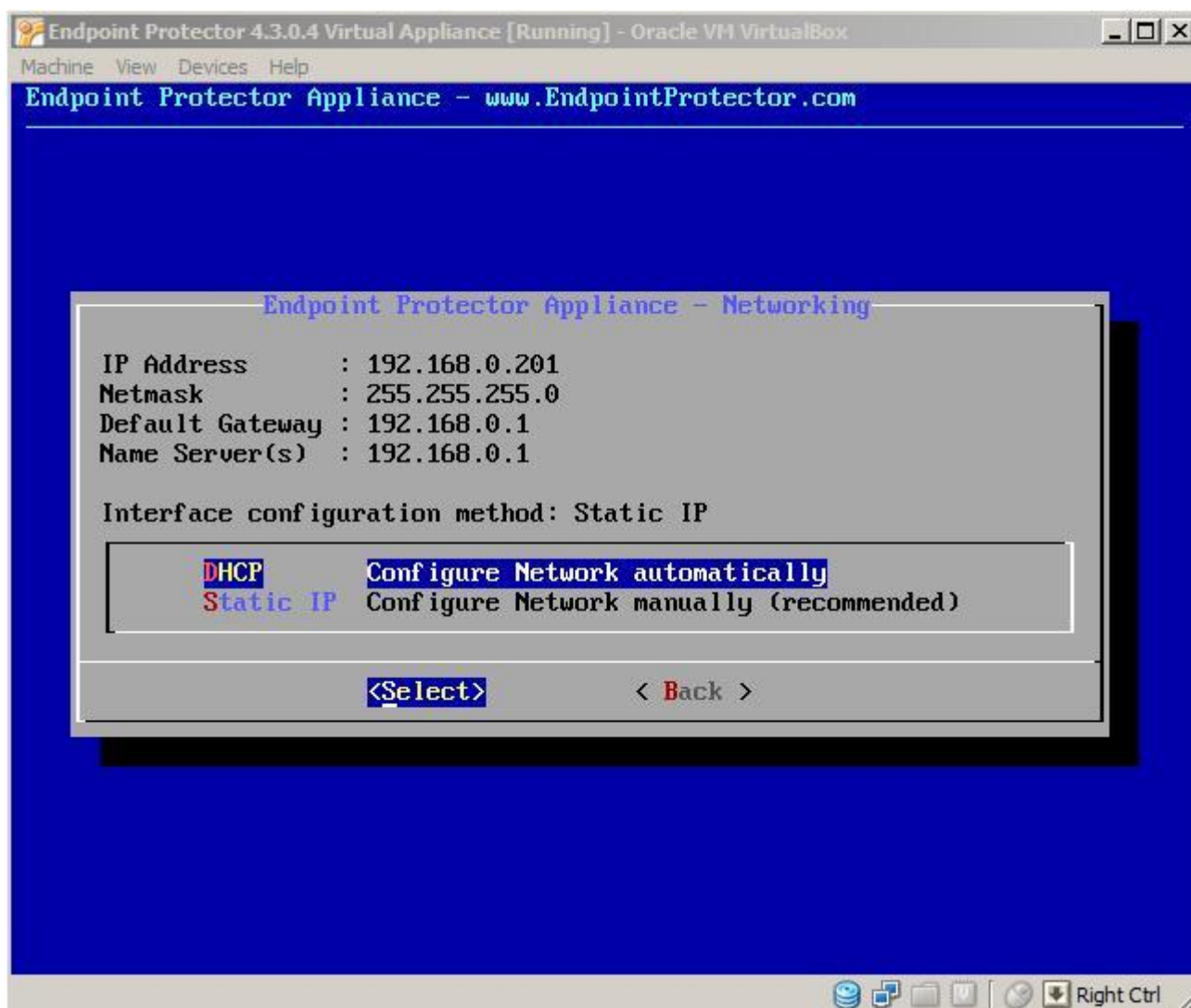
### 4. Press Enter



The virtual appliance now accessible from the configured IP Address. (in our example, [https:// 192.168.7.94](https://192.168.7.94))

### 5.1.1. Automatic configuration

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



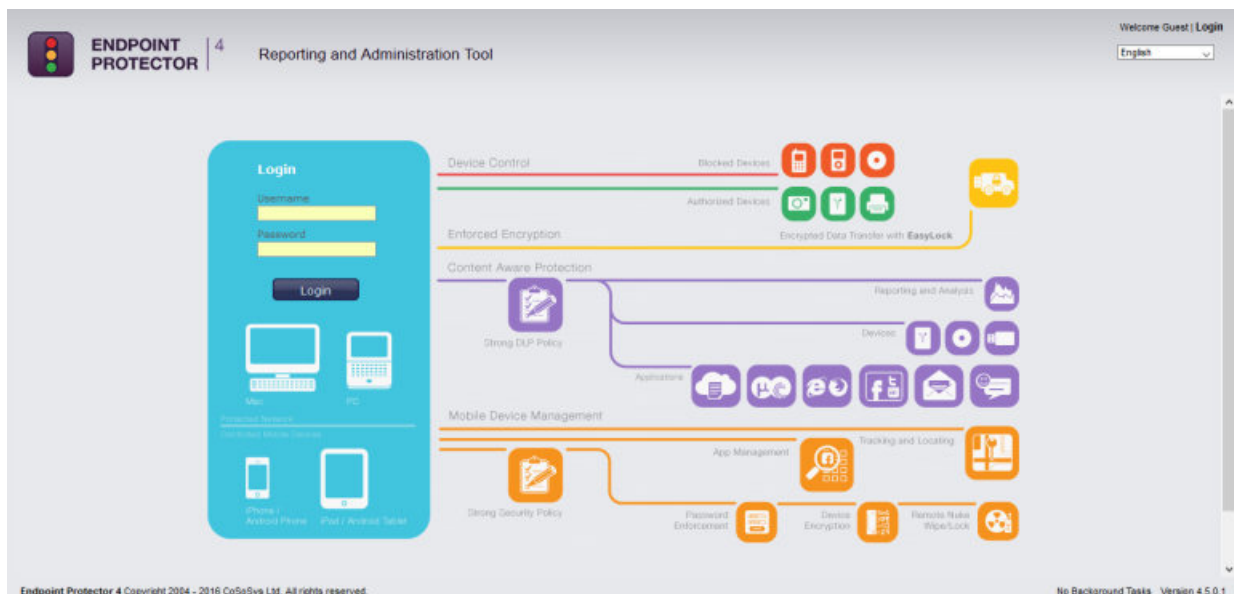
# 6. Endpoint Protector Configuration

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

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

## 6.1. Login to Endpoint Protector

Please enter the user name and password defined in the Endpoint Protector Setup Wizard.



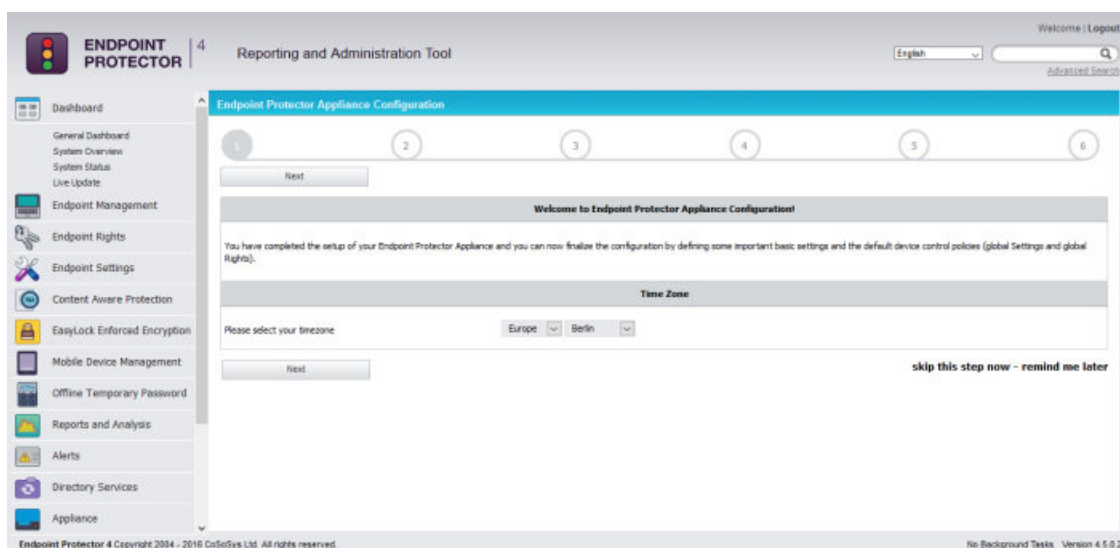
The default username and password for Endpoint Protector are:

**USERNAME:** root

**PASSWORD:** epp2011

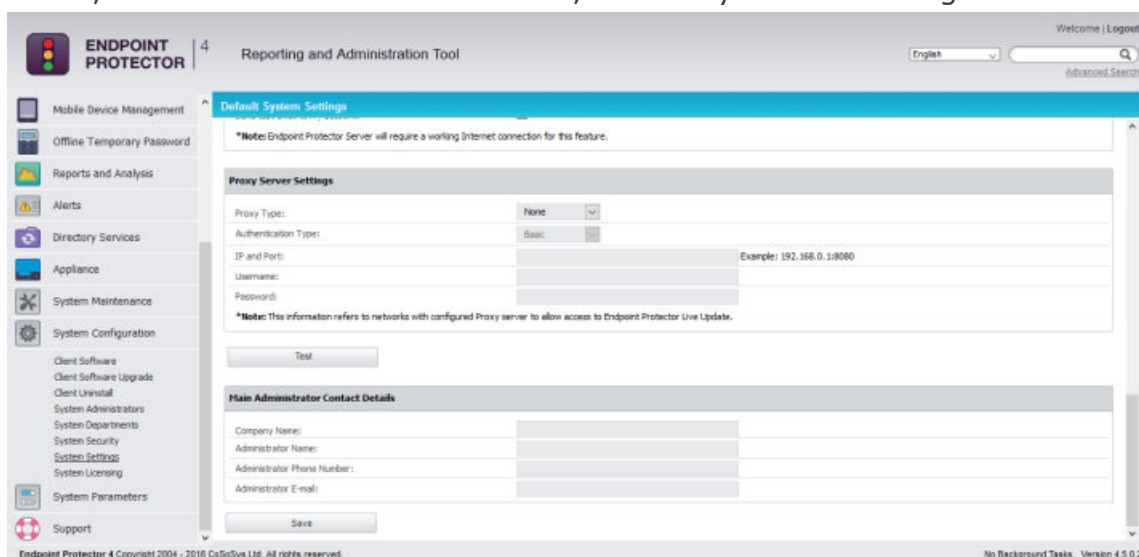
## 6.2. Configuration Wizard

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



## 6.3. System Settings

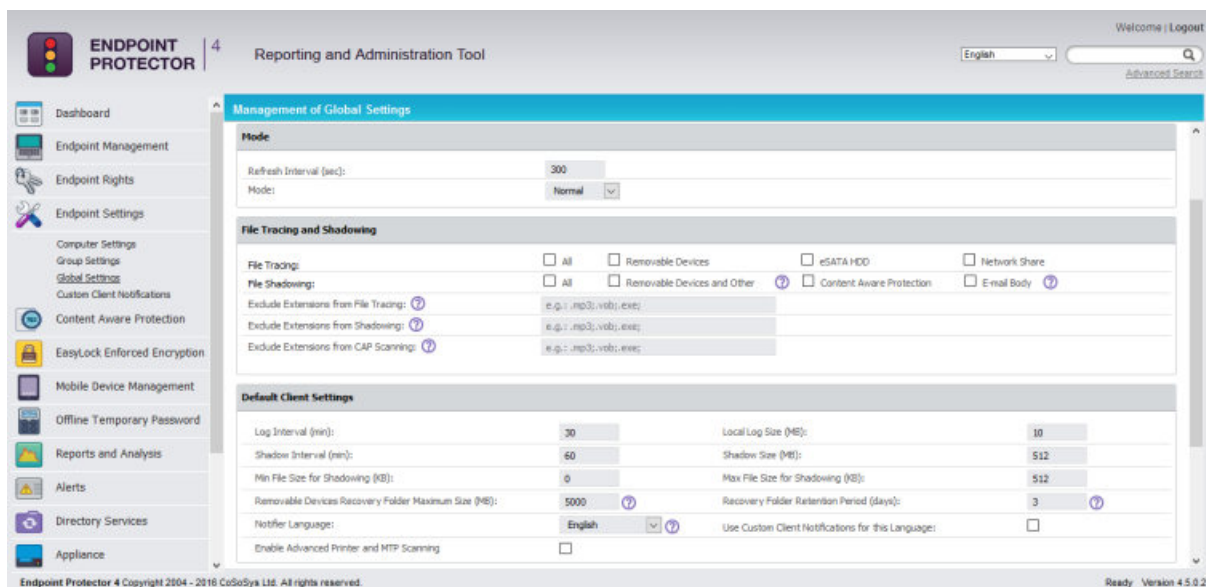
Some basic settings are required for the Endpoint Protector to function properly. Please choose what rights have priority, the E-mail address used to receive Alerts, the main Administrator contact, the Proxy Server Settings and more.





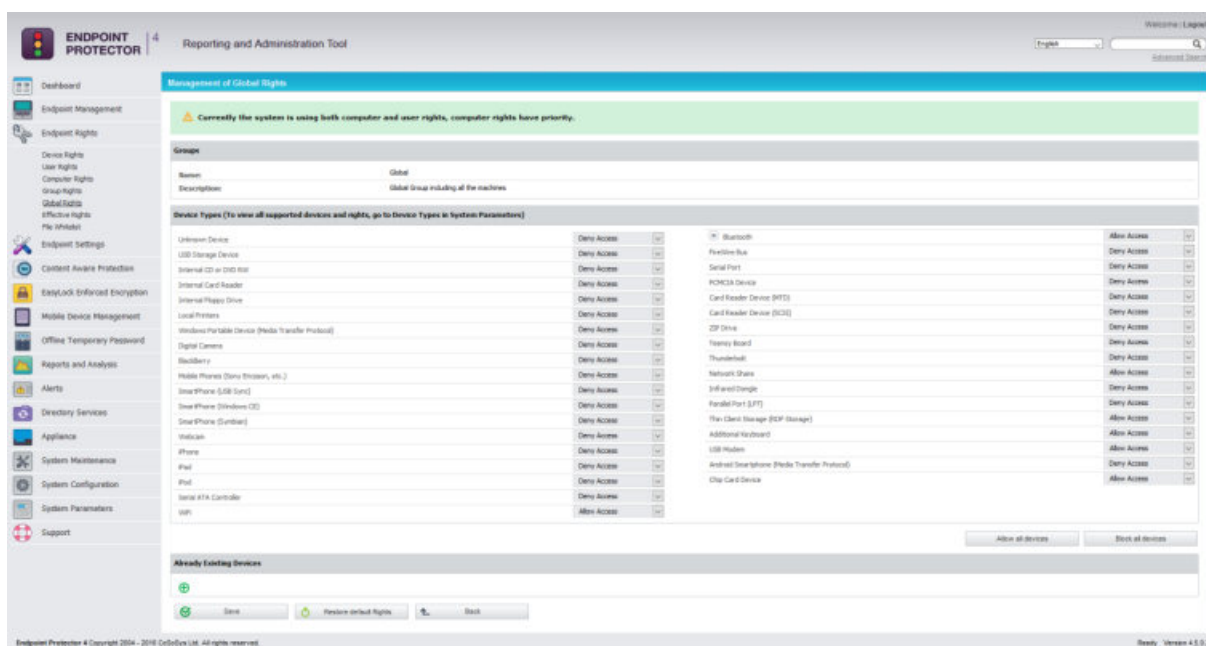
Additionally, the Endpoint Protector Client Refresh Interval, the activated or deactivate features such as File Tracing and File Shadowing and the default parameters for the generated logs can also be configured.

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



## 6.4. Default Device Control Rights

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





## 6.5. Finishing the Endpoint Protector Configuration Wizard

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

# 7. Server Information and Maintenance

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

## 7.1. Server Information

This section displays information about the Server current state.

The screenshot displays the 'Endpoint Protector Reporting and Administration Tool' interface. The left sidebar contains a menu with options: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, EasyLock Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, and Appliance. The 'Appliance' section is expanded, showing 'Server Information', 'Server Maintenance', and 'SIEM Integration'. The main content area is titled 'Endpoint Protector Appliance - System Information' and is divided into three sections: 'Disk Space', 'Info Disk Space', and 'Database Disk Space occupied'. The 'Disk Space' section shows: Disk Space System: 3.4G - 19% from 20G; Disk Space BPP Servers: 928M - 5% from 22G; Logs on Disk: 4.0K stored in /var/jepfiles/logs; Shadows on Disk: 8.0K stored in /var/jepfiles/shadows. The 'Info Disk Space' section provides instructions on how to manage disk space, including backing up logs and removing old logs. The 'Database Disk Space occupied' section shows: Database Disk Space occupied: 9.9M stored in /var/lib/mysql/jepdatabase; Number of Logs in Database: 0; Number of Files Traced: 0; Number of Files Shadowed: 0. The 'System' section shows: Uptime: 11:00:01 up 7 days, 22:54, 0 users, load average: 0.13, 0.18, 0.13 - 1, 5 and 15 minutes ago; Linux Distribution: Ubuntu 14.04.5 LTS; System Information Update: 2016-Dec-02 11:00:01. The footer of the interface includes 'Endpoint Protector 4 Copyright 2004 - 2016 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.5.0.2'.

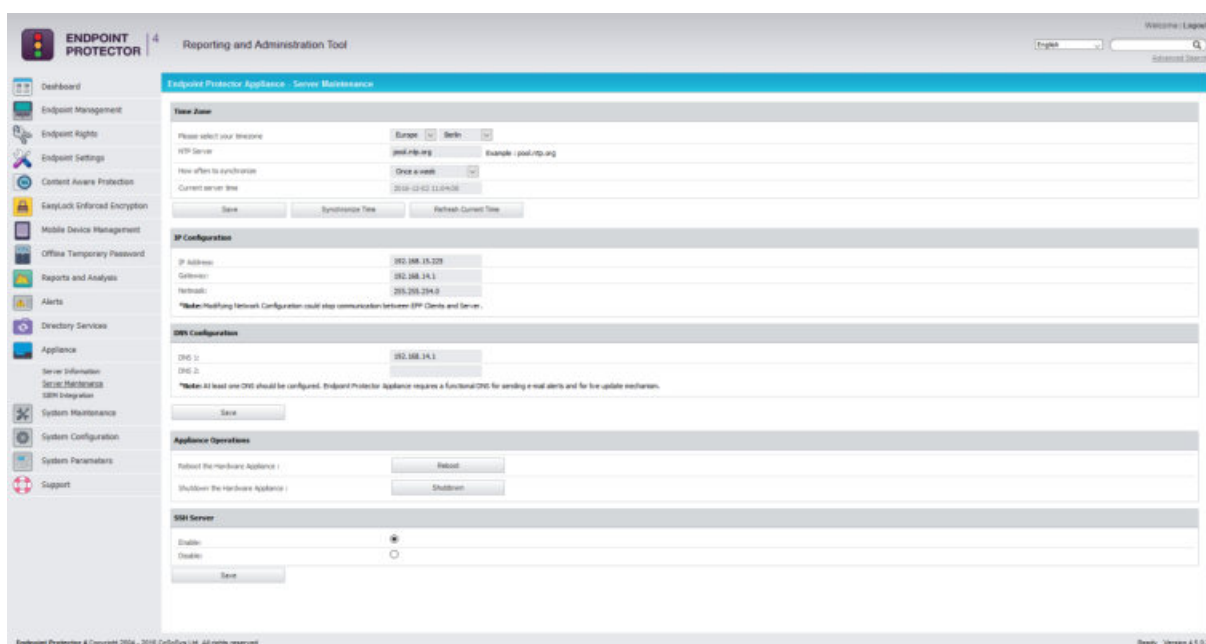
Disk Space	
Disk Space System:	3.4G - 19% from 20G
Disk Space BPP Servers:	928M - 5% from 22G
Logs on Disk:	4.0K stored in /var/jepfiles/logs
Shadows on Disk:	8.0K stored in /var/jepfiles/shadows

Database Disk Space occupied	
Database Disk Space occupied:	9.9M stored in /var/lib/mysql/jepdatabase
Number of Logs in Database:	0
Number of Files Traced:	0
Number of Files Shadowed:	0

System	
Uptime:	11:00:01 up 7 days, 22:54, 0 users, load average: 0.13, 0.18, 0.13 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 14.04.5 LTS
System Information Update:	2016-Dec-02 11:00:01

## 7.2. Server Maintenance

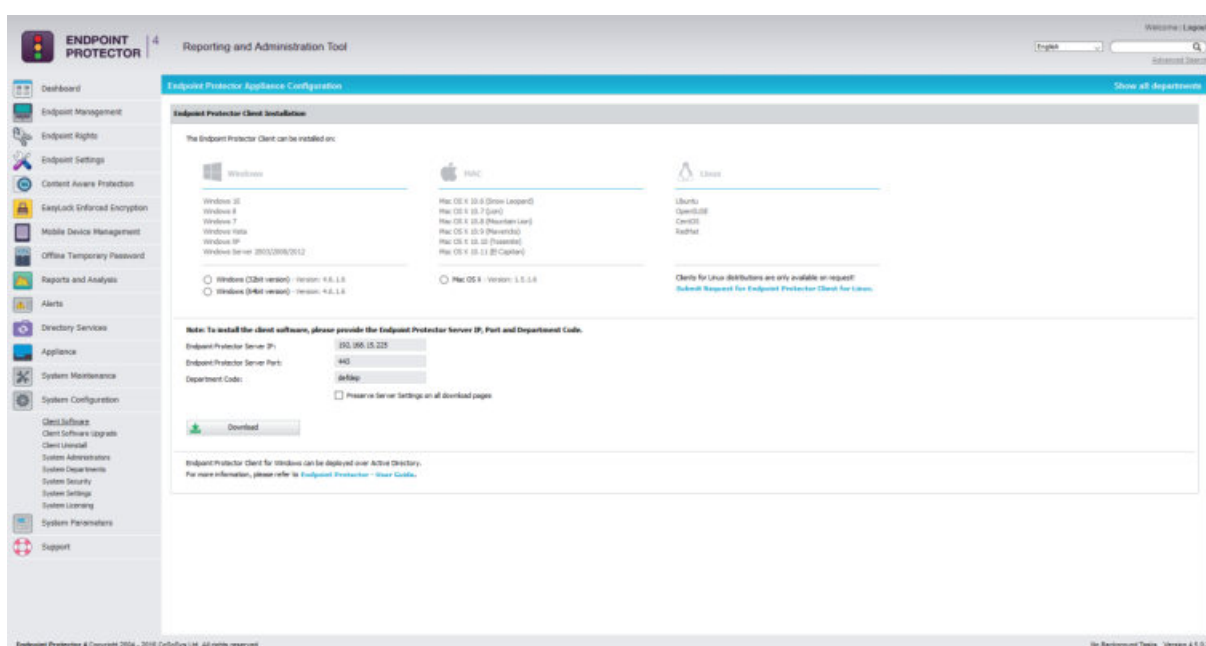
This section provides the option to configure the Appliance network settings, rebooting or shutting down the appliance and more.



## 7.3. Endpoint Protector Client Installation

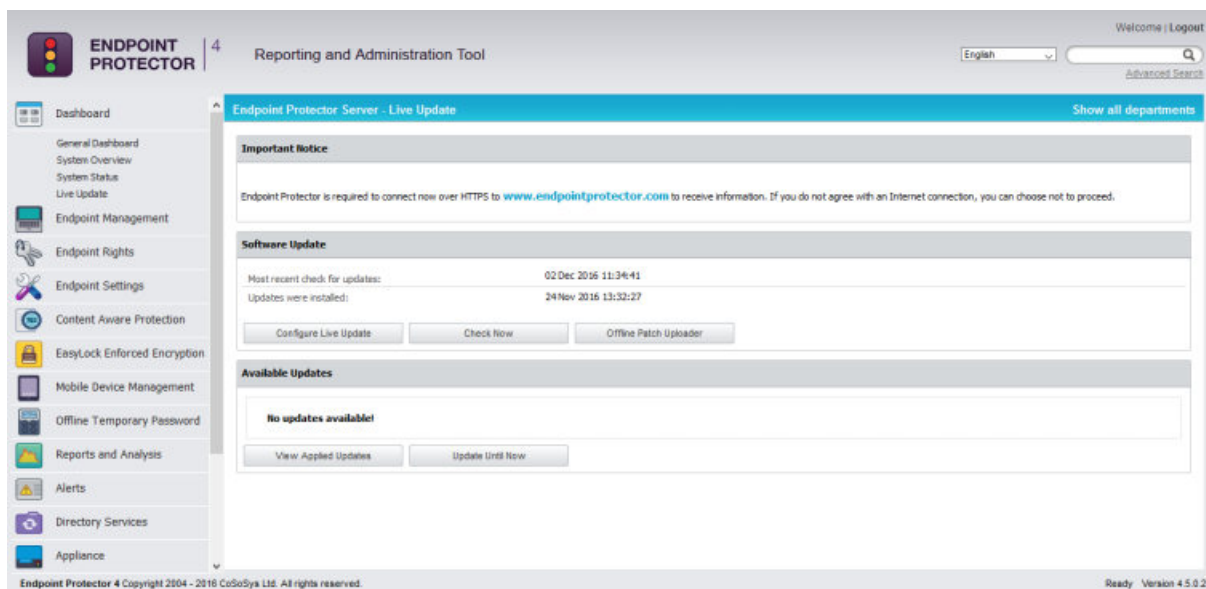
The Endpoint Protector Client needs to be deployed on the computers in the network. They can be downloaded directly from the Appliance by accessing the static IP Address in a browser (e.g.: <http://192.168.0.201>). The Endpoint Protector Download section can be accessed through both HTTPS and HTTP, allowing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

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



## 7.4. Endpoint Protector Live Update

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

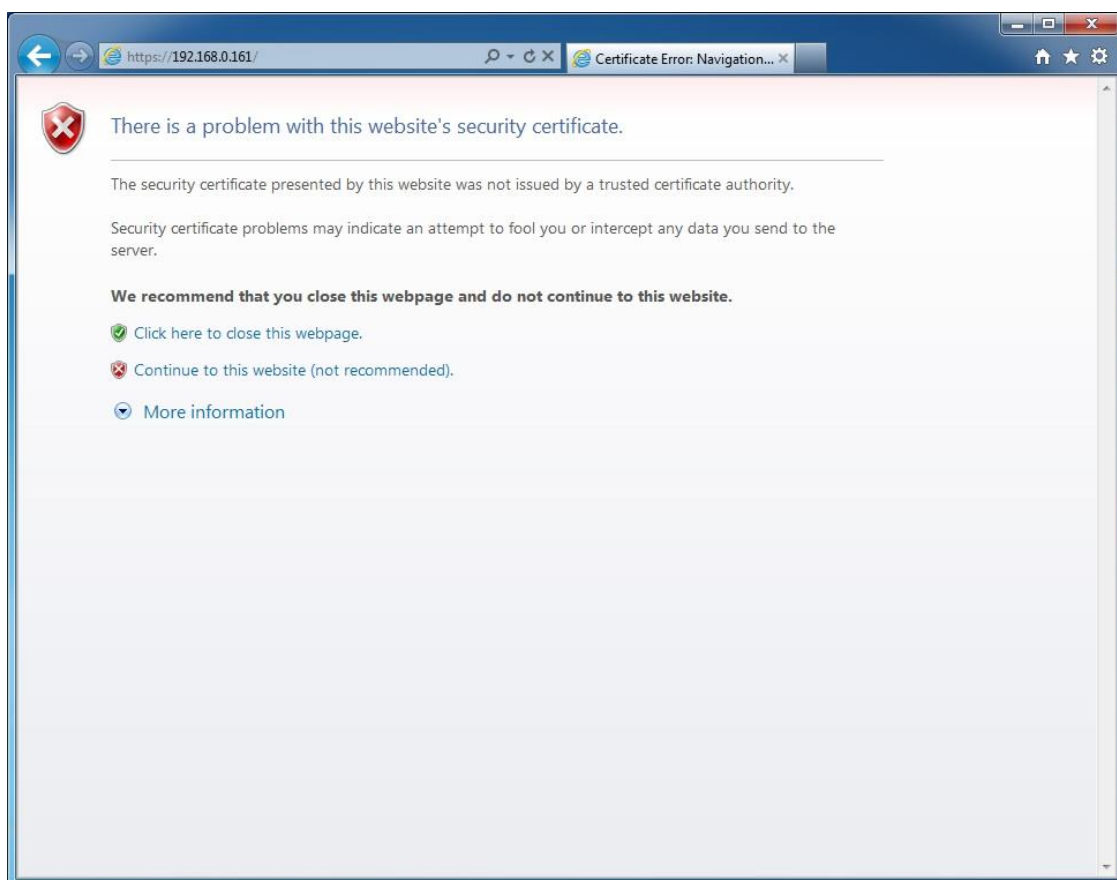



# 8. Installing Root Certificate to Browsers

## 8.1. For Microsoft Internet Explorer

Open Endpoint Protector User Interface by accessing the IP address. (e.g. <https://192.168.0.201/>).

If there is no certificate in your browser, the Certificate Error page will be prompted.



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

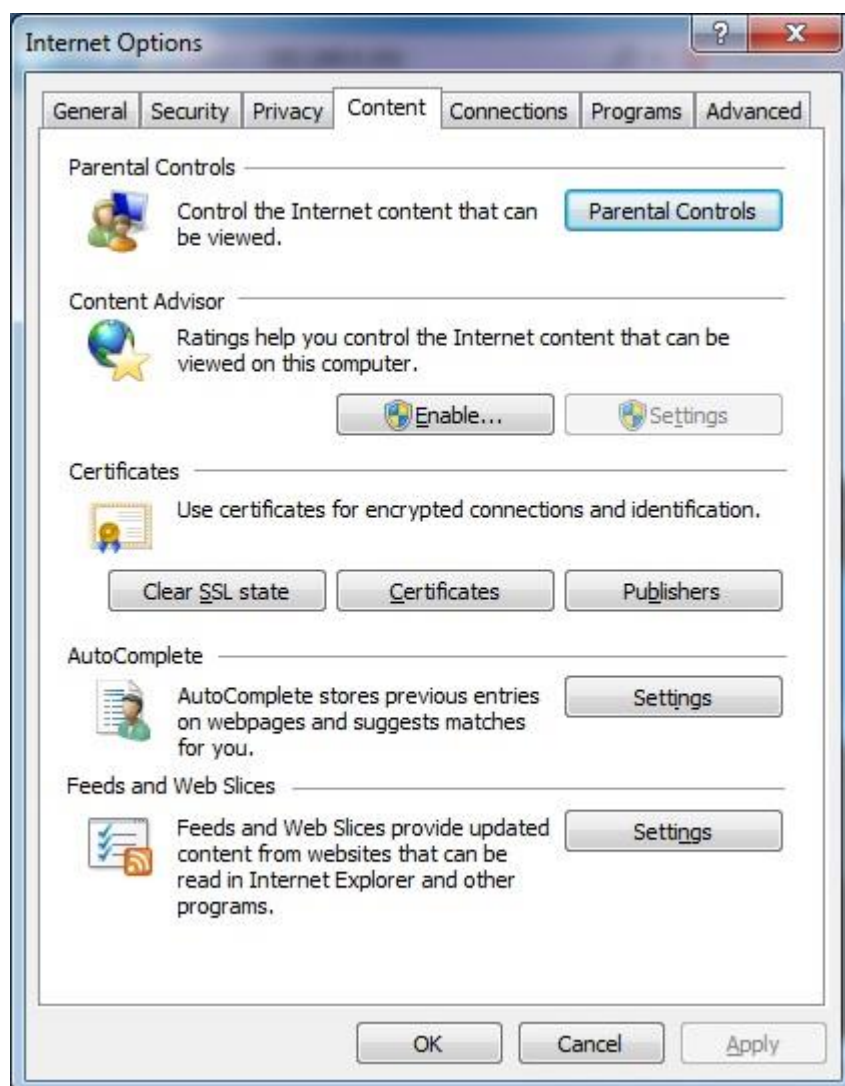
Go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate> and install the Certificate.

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

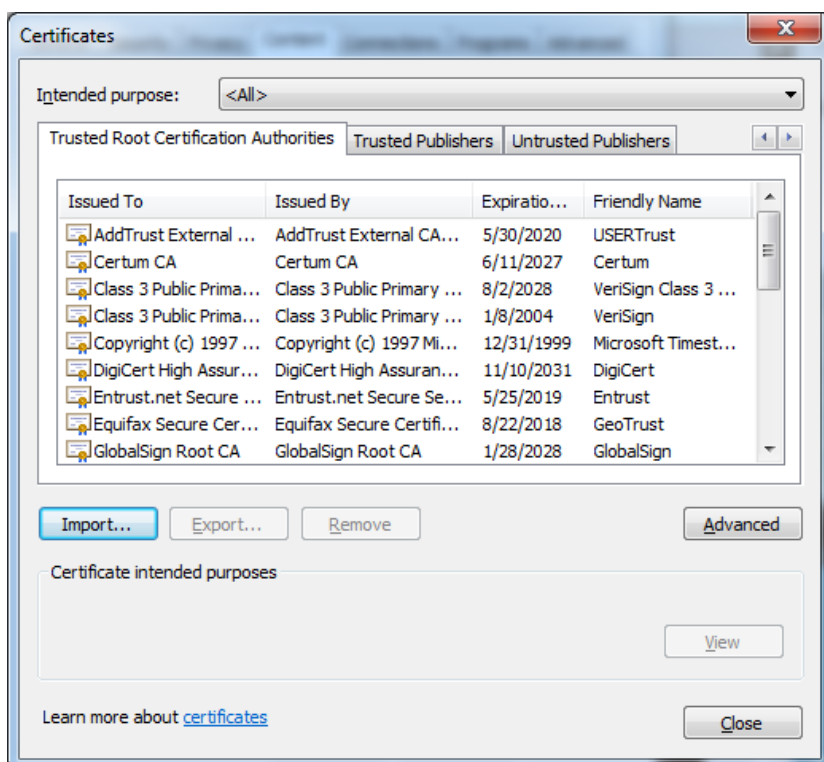
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

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.



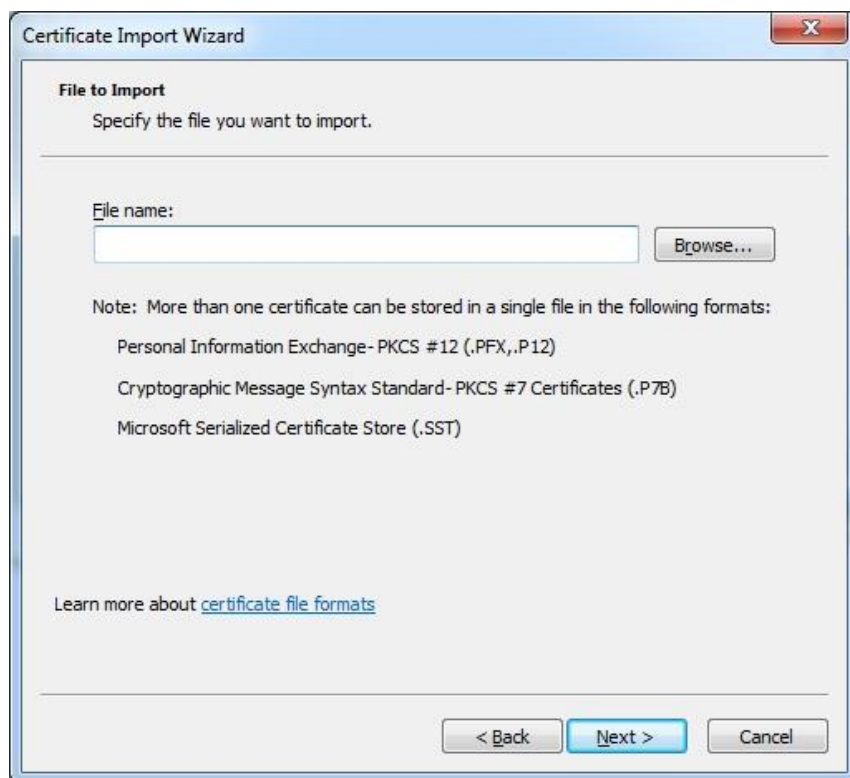
From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.



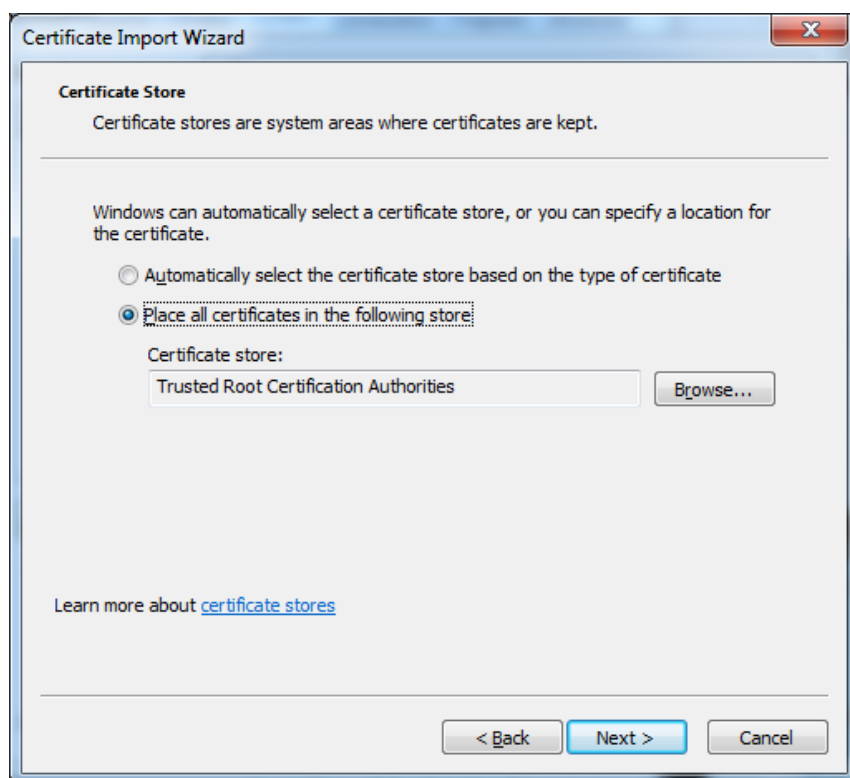
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.



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

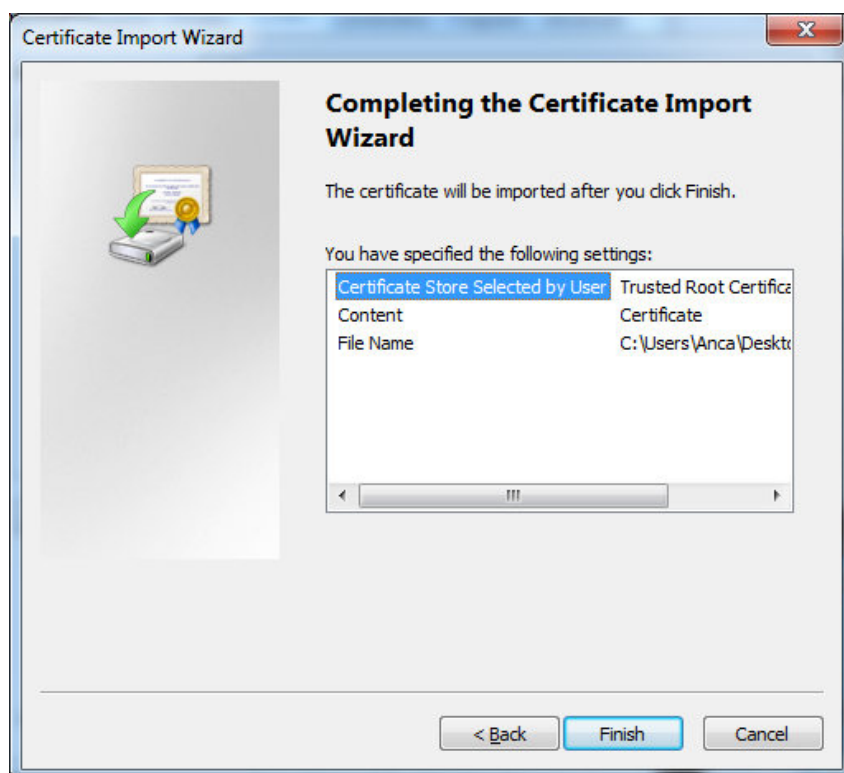


In the Certificate Store window, select "Place all certificates in the following store" radio button.

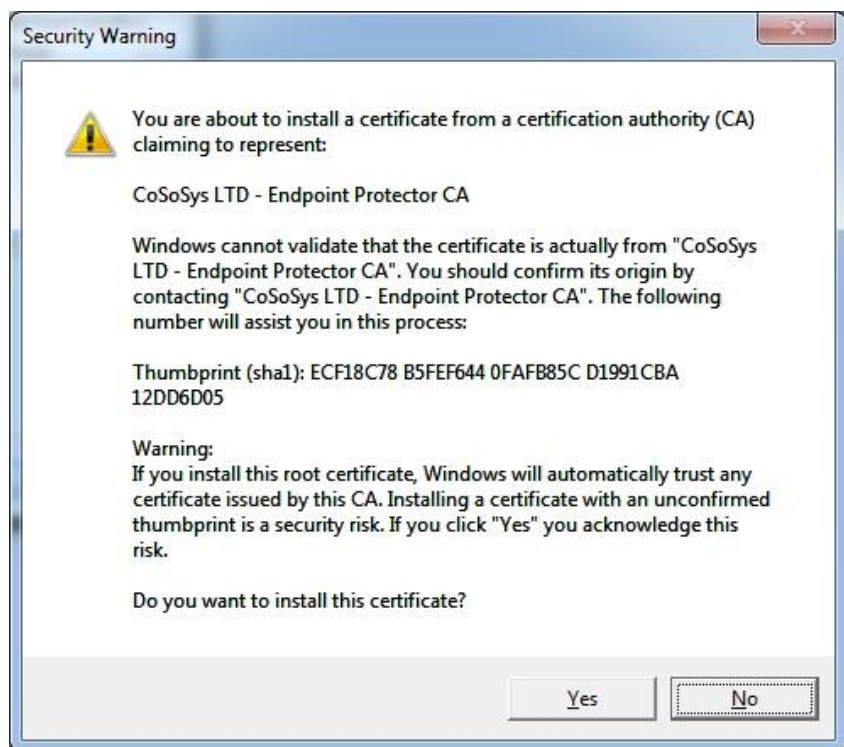




Another “Completing the Certificate Import Wizard” pops up. Just click the “Finish” button.



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 IP address again.

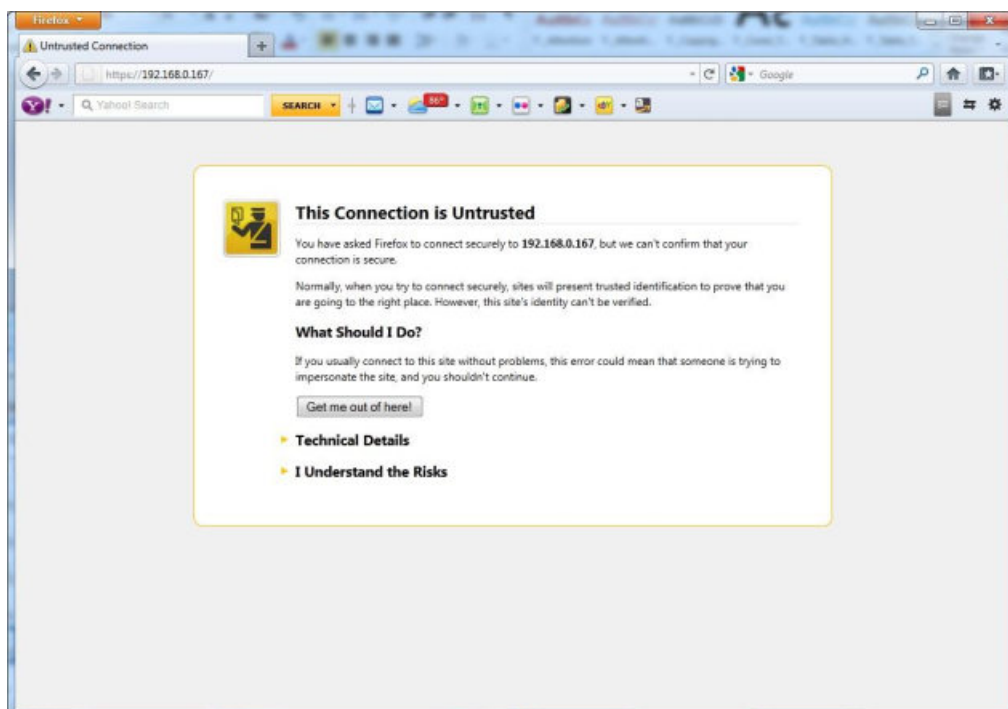


## 8.2. For Mozilla Firefox

Open the Browser.

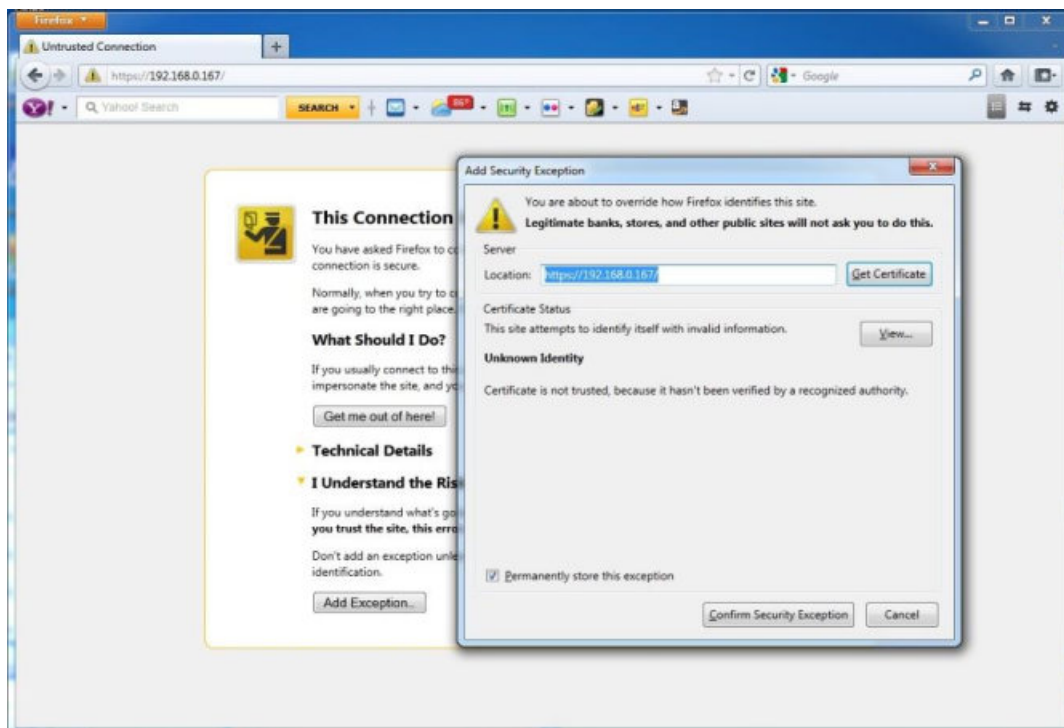
Open Endpoint Protector User Interface by accessing the IP address. (e.g. <https://192.168.0.201>).

If there is no certificate in your browser, the Certificate Error page will be prompted.

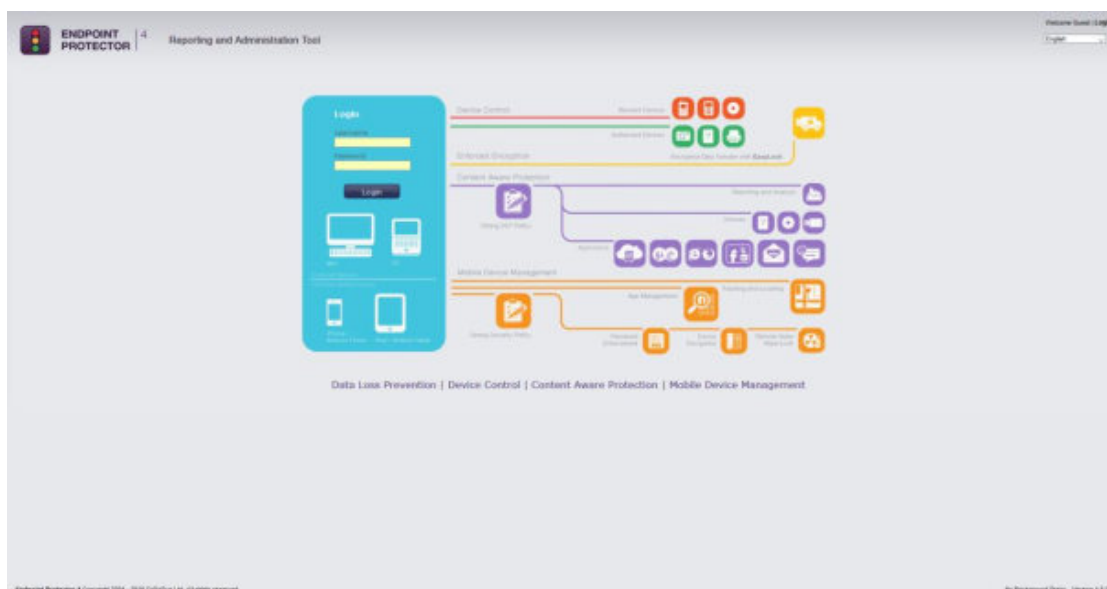


From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up. Click Get Certificate and then the Confirm Security Exception button.



Close the browser and start it again.



# 9. Hardware Appliance Setup

## 9.1. Endpoint Protector Appliance Delivery

When receiving the Endpoint Protector Appliance the package contains:

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



## 9.2. Connecting Appliance for Initial Setup

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

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

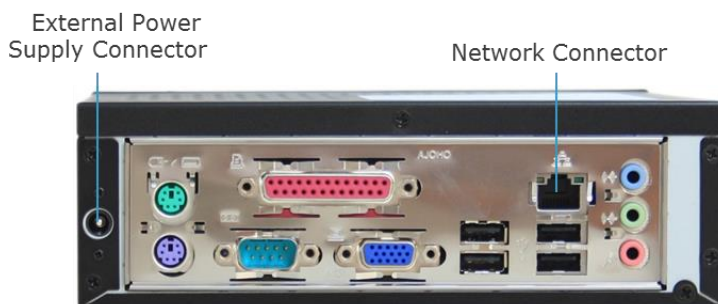
Your hardware appliance (models A50 to A4000) contains on the backside two network ports that are marked yellow for CONFIG (configuration connection) and blue for NET (network connection). The A20 hardware appliance has one network port.

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

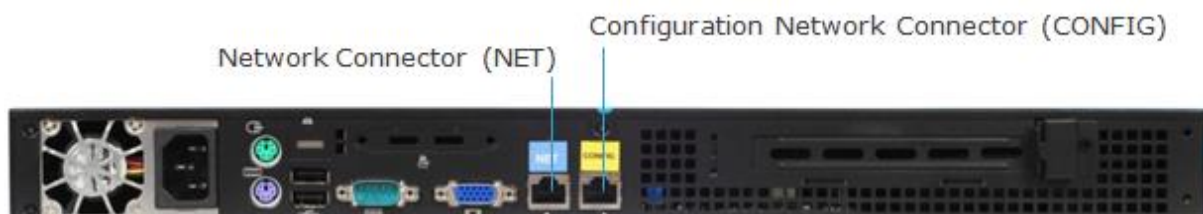
Start the Appliance by pushing the POWER button.

## 9.3. Hardware Appliance Back and Front Panel

### 9.3.1. A20 Appliance Back Panel



### 9.3.2. A50 and A100 Appliance Back Panel

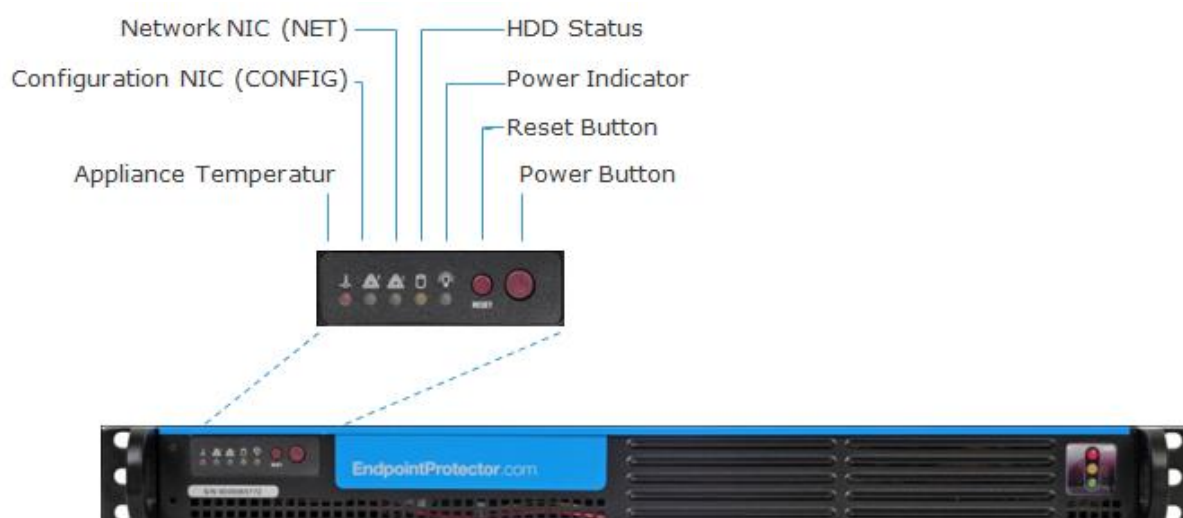


The back panels for Models A250 up to A4000 have marked network ports similar to the picture above for the A50 and A100 model.

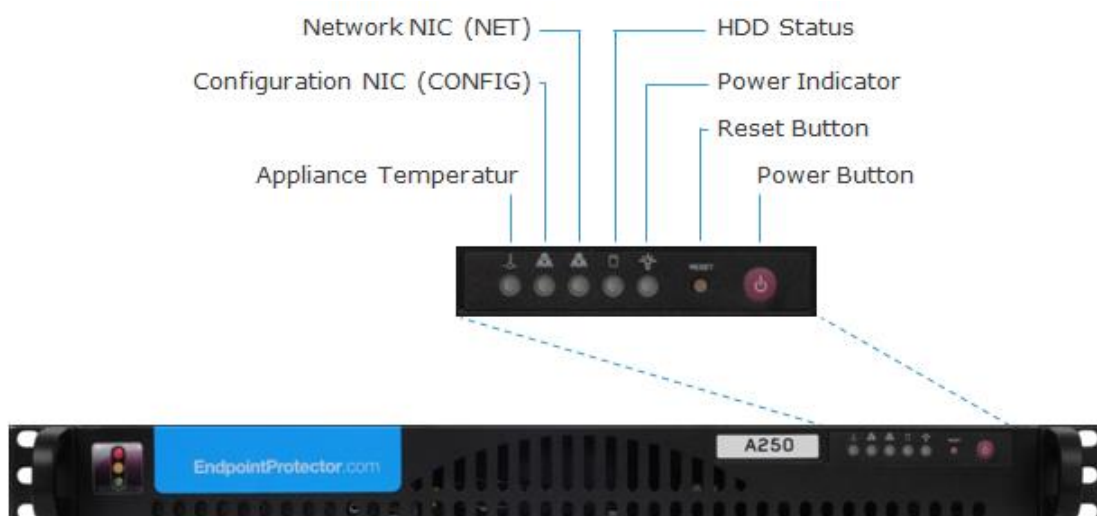
### 9.3.3. A20 Appliance Front Panel



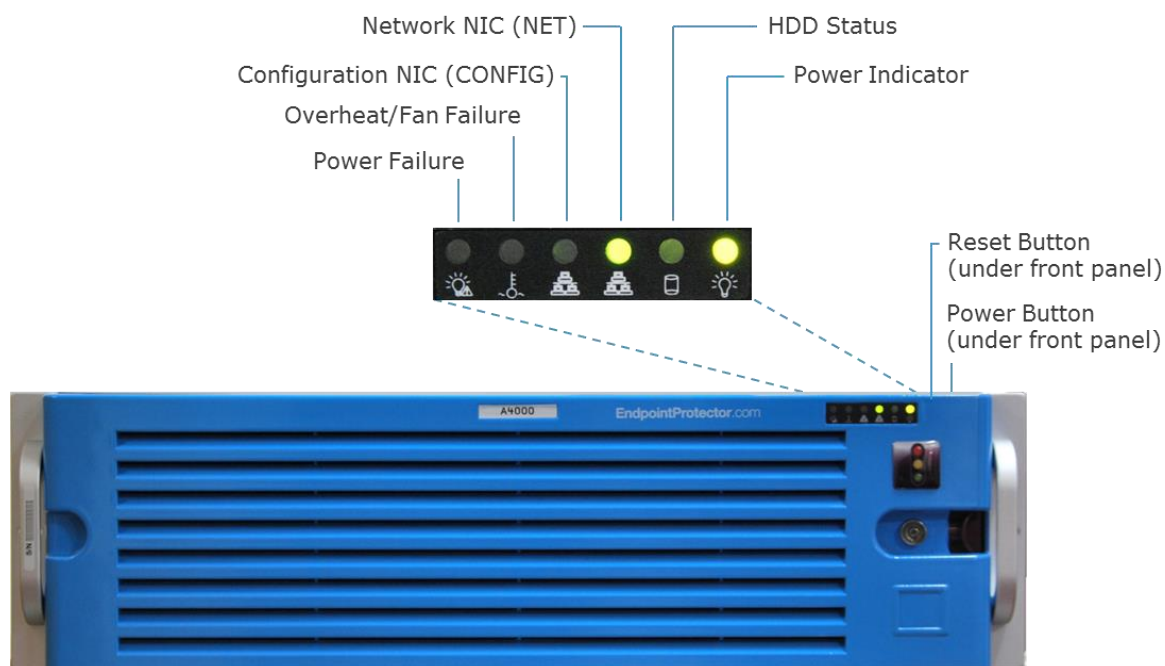
### 9.3.4. A50 and A100 Appliance Front Panel



### 9.3.5. A250, A500 and A1000 Appliance Front Panel

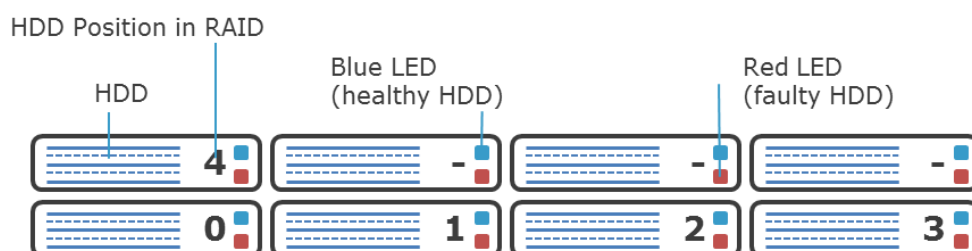


### 9.3.6. A2000 - A4000 Appliance Front Panel



## 9.4. A2000 / A4000 Appliance HDD Configuration

### 9.4.1. A2000 Appliance HDD Configuration



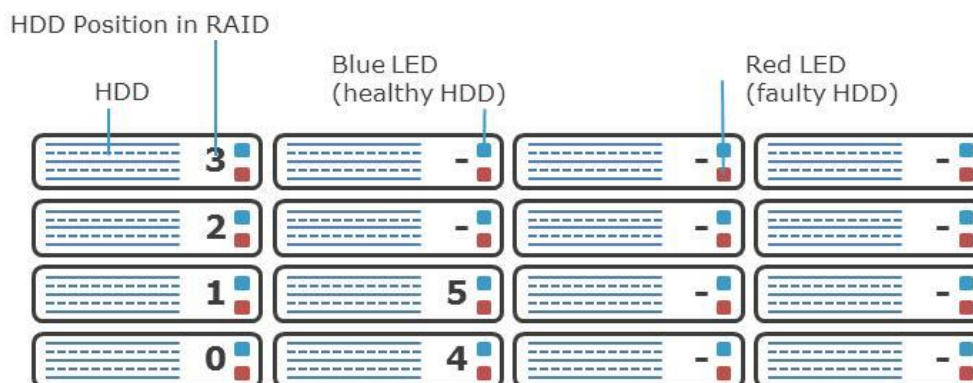
The A2000 Appliance comes with 4 HDDs in RAID 5 Configuration. The HDDs are installed in the number order 0-3.

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

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



### 9.4.2. A4000 Appliance HDD Configuration



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

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

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

### 9.4.3. A2000 and A4000 Appliance HDD RAID Additional Software

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

## 9.5. Hardware Appliance Setup Wizard

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

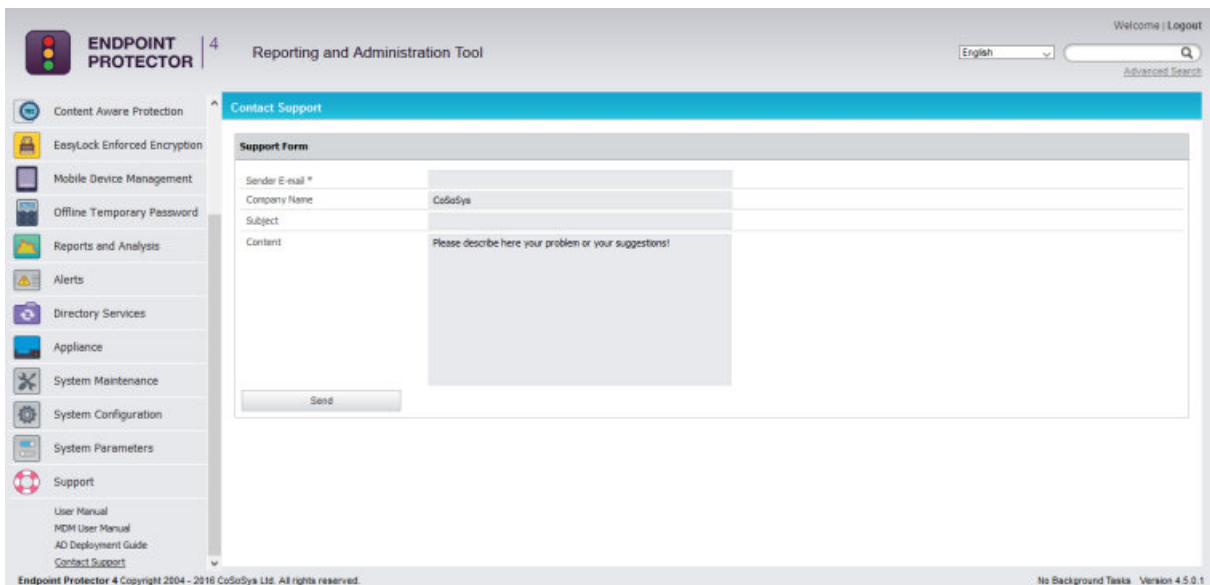
The easiest way to configure the Endpoint Protector Hardware Appliance is to connect a mouse, keyboard and monitor directly to it. This will prompt the same Setup Wizard as described in the chapter above Virtual Appliance Setup Wizard.



# 10. Support

Additional support resources as available. Please visit our website for more manuals, FAQs, videos and tutorials, direct e-mail support and more at [www.endpointprotector.com](http://www.endpointprotector.com)

Our Support department can also be contacted directly from the Endpoint Protector User Interface from the Support > Contact Support section. One of our team members will contact you in the shortest time possible.



The screenshot displays the Endpoint Protector 4 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 'Welcome | Logout' link. A left sidebar lists various system management options: Content Aware Protection, EasyLock Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The 'Support' section is expanded, showing links for User Manual, MDM User Manual, AD Deployment Guide, and 'Contact Support'. The main content area is titled 'Contact Support' and contains a 'Support Form'. The form fields are: 'Sender E-mail \*' (empty), 'Company Name' (filled with 'CodoSys'), 'Subject' (empty), and 'Content' (a large text area with the placeholder 'Please describe here your problem or your suggestions!'). A 'Send' button is located at the bottom of the form. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2018 CodoSys Ltd. All rights reserved.' on the left and 'No Background Tasks - Version 4.5.0.1' on the right.

Even if you do not have a problem but miss some feature or just want to leave us a general comment, we would love to hear from you.

# 11. Disclaimer

Endpoint Protector Appliance does not communicate outside of your network except with [liveupdate.endpointprotector.com](https://liveupdate.endpointprotector.com) and [cloud.endpointprotector.com](https://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 (eproot) 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 – 2017 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector, Endpoint Protector Basic and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows is a 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.