Table of Contents

1. Endpoint Protector Virtual Appliance Formats 1
   1.1. Available Formats of the Virtual Appliance ............................. 1
      1.1.1. The Virtualization software that supports OVF Format is: 2
      1.1.2. The Virtualization software that supports VMX Format is: 2
      1.1.3. The Virtualization software that supports VHD Format is: 2
      1.1.4. The Virtualization software that supports XVA Format is: 3

2. Implementing using OVF Format ............... 4
   2.1. Implementing in Oracle VM VirtualBox using OVF Format .... 4
   2.2. Implementing in VMware vSphere using OVF Format .......... 11
   2.3. Implementing in Citrix XenServer 5.6 using OVF Format .... 20

3. Implementing using VMX Format .......... 25
   3.1. Implementing in VMware Server 2.0 using VMX Format .... 25
   3.2. Implementing in VMware Player 3.0 using VMX Format .... 28
   3.3. Implementing in VMware Workstation 6.5 using VMX Format 31

4. Implementing using VHD Format .......... 35
   4.1. Implementing in Microsoft Hyper-V 2008 using VHD Format 35
   4.2. Implementing in Microsoft Hyper-V 2012 using VHD Format 38

5. Access Appliance Setup Wizard ............... 42
   5.1. Appliance network configuration from console ............... 42
      5.1.1. Manual configuration .............................................. 47
      5.1.2. Automatic configuration ......................................... 51
   5.2. Hardware Appliance Setup Wizard ............................... 52
      5.2.1. End User License Agreement - Appliance License Agreement 53
      5.2.2. Define your Appliance Administrator Password ........ 54
      5.2.3. Set Time Zone .................................................... 55
      5.2.4. Set Appliance Network IP Address .......................... 56
      5.2.5. Endpoint Protector Client – Automatic Repackaging .... 57
      5.2.6. Appliance Server Certificate ..................................... 58
      5.2.7. Finishing the Endpoint Protector Appliance Setup .... 59

6. Endpoint Protector Appliance Configuration 60
   6.2. Connect Appliance to Network ................................. 60
6.3 Access to the Appliance Interface through your Network ...... 60
6.4 Login to Endpoint Protector ........................................ 61
6.5 Appliance Configuration Wizard .................................... 62
6.6 Appliance Basic Settings ............................................. 63
6.7 Appliance Default Policies ........................................... 65
6.8 Finishing the Endpoint Protector Appliance Configuration Wizard 65

7. Appliance Settings and Maintenance ........... 66
   7.2 Server Information .................................................. 66
   7.3 Server Maintenance ............................................... 67
       7.3.1 Network Settings ........................................... 67
       7.3.2 Reboot the Appliance .................................... 67
       7.3.3 Reset Appliance to Factory Default .................. 68
   7.4 Endpoint Protector Client Installation for Appliance .... 69
   7.5 Appliance Online Live Update ................................ 70

8. Installing Root Certificate to your Internet Browser ........................................ 71
   8.2 For Microsoft Internet Explorer ................................. 71
   8.3 For Mozilla Firefox .............................................. 81

9. Support ................................................................. 84

10. Important Notice / Disclaimer ............... 85
1. Endpoint Protector Virtual Appliance Formats

1.1. Available Formats of the Virtual Appliance

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

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

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

Open Virtualization Format (OVF) is an open standard for packaging and distributing virtual appliances.
1.1.1. The Virtualization software that supports OVF and OVA Format is:

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

1.1.2. The Virtualization software that supports VMX Format is:

- VMware Player 5.0 or higher
- VMware Workstation 9.0 or higher

**Note!**

The .VMX virtual appliance is set to run on the latest VMware Workstation version (v11.x.x) and on the latest VMware Player version (v7.x.x). In order to run these virtual appliances on older VMware Workstation / VMware Player versions, the following actions need to be done:

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

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

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

1.1.3. The Virtualization software that supports VHD Format is:

- Microsoft Hyper-V

1.1.4. The Virtualization software that supports PVM Format is:

- Parallels Desktop
1.1.5. The Virtualization software that supports XVA Format is:

- Citrix XenServer 5.5
- Citrix XenServer 6.0

Note!

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

2.1. Implementing in Oracle VM VirtualBox using OVF Format

1. Unzip the downloaded package

2. Start VirtualBox
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

![Appliance Import Settings](image1)

8. Wait for the import displayed by the progress bar

![Importing Appliance](image2)
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.
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.
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 your 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.
4.2. Implementing in Microsoft Hyper-V 2012 using VHD Format

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

2. Start **Hyper-V Manager**

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

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**.

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”.

9. Click on **Apply**.

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

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

**Note!**

In case you experience difficulties using Microsoft Hyper-V 2012 please contact support@endpointprotector.com
5. Access Appliance Setup Wizard

5.1. Appliance network configuration from console

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

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

- Server and Client: 443
- Live Update (liveupdate.endpointprotector.com): 80 & 443
- MDM Cloud (cloud.endpointprotector.com): 443

To configure the Virtual Appliance’s network it is required to follow the steps below.
1. Press Continue when finished reading the End User License Agreement
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 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.
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

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

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.
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.

Congratulations. Your Endpoint Protector Appliance has been setup.

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

Now you can connect to the Endpoint Protector Appliance Web interface through your network. To access the Endpoint Protector Appliance Web interface enter HTTPS:// and the server IP Address that you just configured in the URL bar of your internet browser (e.g., https://192.168.100.100).
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.

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.
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.
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.

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.
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.
7.3 Server Maintenance

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!
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.
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](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.
### Certificates

#### Intended purpose:
- <All>

<table>
<thead>
<tr>
<th>Trusted Root Certification Authorities</th>
<th>Trusted Publishers</th>
<th>Untrusted Publishers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued To</td>
<td>Issued By</td>
<td>Expiration</td>
</tr>
<tr>
<td>AddTrust External CA</td>
<td>AddTrust External CA</td>
<td>5/30/2020</td>
</tr>
<tr>
<td>Certum CA</td>
<td>Certum CA</td>
<td>6/11/2027</td>
</tr>
<tr>
<td>Class 3 Public Primary</td>
<td>Class 3 Public Primary</td>
<td>8/2/2028</td>
</tr>
<tr>
<td>Class 3 Public Primary</td>
<td>Class 3 Public Primary</td>
<td>1/8/2004</td>
</tr>
<tr>
<td>Copyright (c) 1997 Microsoft</td>
<td>Copyright (c) 1997 Microsoft</td>
<td>12/31/1999</td>
</tr>
<tr>
<td>DigiCert High Assurance</td>
<td>DigiCert High Assurance</td>
<td>11/10/2011</td>
</tr>
<tr>
<td>Entrust.net Secure</td>
<td>Entrust.net Secure</td>
<td>5/25/2019</td>
</tr>
<tr>
<td>Equifax Secure Cer</td>
<td>Equifax Secure Cer</td>
<td>8/22/2018</td>
</tr>
<tr>
<td>GlobalSign Root CA</td>
<td>GlobalSign Root CA</td>
<td>1/28/2028</td>
</tr>
</tbody>
</table>

#### Certificate intended purposes

Learn more about [certificates](#)
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.

Certificate Import Wizard

File to Import
Specify the file you want to import.

File name: [blank]
Browse...

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)
- MicrosoftSerialized Certificate Store (.SST)

Learn more about certificate file formats
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.
Please provide the necessary credentials.

Username: 
Password: 

Login

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

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

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

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

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

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

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