Table of Contents

Document Changelog 3

1. Endpoint Protector Virtual Appliance formats 1
   1.1. Table 1
   1.2. Format supported by Virtualization Software 1

2. Implement using the OVF format 3
   2.1. Oracle VM VirtualBox 3
   2.2. VMware vSphere 7
   2.3. Citrix XenServer 5.6 12

3. Implement using the VMX format 17
   3.1. Implementing using VMware Server 17
   3.2. Implementing using VMware Player 19
   3.3. Implementing using VMware Workstation 21

4. Using the VHD format 23
   4.1. Implementing using Microsoft Hyper-V 2012 23

5. Virtual Appliance Setup Wizard 26
   5.1.1. Manual configuration 28
   5.1.2. Automatic configuration 30

6. Endpoint Protector Configuration 31
   6.1. Login to Endpoint Protector 31
   6.2. Configuration Wizard 31
   6.3. System Settings 32
   6.4. Default Device Control Rights 33
   6.5. Finishing the Endpoint Protector Configuration Wizard 33

7. Server Information and Maintenance 34
   7.1. Server Information 34
   7.2. Server Maintenance 34
   7.3. Endpoint Protector Client Installation 35
   7.4. Endpoint Protector Live Update 36

8. Hardware Appliance Setup 37
   8.1. Endpoint Protector Appliance Delivery 37
   8.2. Connecting Appliance for Initial Setup 37
   8.3. Hardware Appliance Back and Front Panel 38
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.1.</td>
<td>A20 Appliance Back Panel</td>
<td>38</td>
</tr>
<tr>
<td>8.3.2.</td>
<td>A50 and A100 Appliance Back Panel</td>
<td>38</td>
</tr>
<tr>
<td>8.3.3.</td>
<td>A20 Appliance Front Panel</td>
<td>38</td>
</tr>
<tr>
<td>8.3.4.</td>
<td>A50 and A100 Appliance Front Panel</td>
<td>39</td>
</tr>
<tr>
<td>8.3.5.</td>
<td>A250, A500, and A1000 Appliance Front Panel</td>
<td>39</td>
</tr>
<tr>
<td>8.3.6.</td>
<td>A2000 - A4000 Appliance Front Panel</td>
<td>40</td>
</tr>
<tr>
<td>8.4.</td>
<td>A2000 / A4000 Appliance HDD Configuration</td>
<td>40</td>
</tr>
<tr>
<td>8.4.1.</td>
<td>A2000 Appliance HDD Configuration</td>
<td>40</td>
</tr>
<tr>
<td>8.4.2.</td>
<td>A4000 Appliance HDD Configuration</td>
<td>41</td>
</tr>
<tr>
<td>8.4.3.</td>
<td>A2000 and A4000 Appliance HDD RAID Additional Software</td>
<td>41</td>
</tr>
<tr>
<td>8.5.</td>
<td>Hardware Appliance Setup Wizard</td>
<td>41</td>
</tr>
<tr>
<td>9.</td>
<td>Support</td>
<td>42</td>
</tr>
<tr>
<td>10.</td>
<td>Disclaimer</td>
<td>43</td>
</tr>
</tbody>
</table>
## Document Changelog

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>2020</td>
<td>The document was created.</td>
</tr>
<tr>
<td>2.0</td>
<td>16.05.2022</td>
<td>The document was updated with the current template.</td>
</tr>
<tr>
<td>3.0</td>
<td>19.07.2022</td>
<td>Images from chapters <a href="#">Endpoint Protector Configuration</a>, <a href="#">Server Information, and Maintenance</a> and <a href="#">Support</a> were updated.</td>
</tr>
<tr>
<td>4.0</td>
<td>11.11.2022</td>
<td>Deleted the Installing Root Certificate to Browsers chapter.</td>
</tr>
</tbody>
</table>
1. Endpoint Protector Virtual Appliance formats

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

<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>7.1.0</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware Workstation</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>5.0.28</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VMware vSphere (ESXi)</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>7.1.3</td>
<td>●</td>
<td></td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyper-V Manager Windows Server 2016</td>
<td>10.0.14393.0</td>
<td></td>
<td></td>
<td></td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parallels Desktop</td>
<td>11.1.3</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>

1.1. Table

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

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

1.2. Format supported by Virtualization Software

In addition to the virtualization software listed in the previous table, these formats are also supported by the following:
1. **OVF and OVA**
   - VMware Workstation 11.1
   - VMware Player 5.0 (or higher)
   - VMware Fusion 7.1.2
   - VMware ESXi 5.1 (or higher)
   - Oracle VM VirtualBox
   - Citrix XenCenter 6.2

2. **VHD**
   - Microsoft Hyper-V 6.1.7601.17514
   - Microsoft Hyper-V 6.3.9600.16384

3. **PVM**
   - Parallels Desktop 10.2.1

4. **XVA**
   - Citrix XenServer 5.5
   - Citrix XenServer 6.0

5. **VMX**
   - VMware Player 5.0 (or higher)
   - VMware Workstation 9.0 (or higher)

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

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

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

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

2.1. Oracle VM VirtualBox

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

1. Unzip the downloaded package;

2. Open VirtualBox;
3. Go to File and select Import Appliance;

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

6. Click Import;

Appliance settings

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

<table>
<thead>
<tr>
<th>Virtual System 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Endpoint Protector 5.5.0.0 Virtual Appliance</td>
</tr>
<tr>
<td>Description</td>
<td>OVF0001180464B5500...</td>
</tr>
<tr>
<td>Guest OS Type</td>
<td>Ubuntu (64-bit)</td>
</tr>
<tr>
<td>CPU</td>
<td>2</td>
</tr>
<tr>
<td>RAM</td>
<td>4096 MB</td>
</tr>
<tr>
<td>Floppy</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter</td>
<td>Intel PRO/1000 MT Desktop (82540EM)</td>
</tr>
<tr>
<td>Storage Controller (IDE)</td>
<td>PIX4</td>
</tr>
<tr>
<td>Storage Controller (SCSI)</td>
<td>LiLogic</td>
</tr>
<tr>
<td>Virtual Disk Image</td>
<td>Endpoint Protector_5.5.0.0_Virtual_Appliance-disk1.vmdk</td>
</tr>
<tr>
<td>Base Folder</td>
<td>C:\Users\Flaviu\VirtualBox VMs</td>
</tr>
<tr>
<td>Primary Group</td>
<td>/</td>
</tr>
</tbody>
</table>

7. Wait for the import displayed by the progress bar;
At this point, the virtual machine is ready for use.

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

To implement using the VMware vSphere, follow these steps:

1. Unzip the downloaded package;
2. Start vSphere;
3. Go to File and select Deploy OVF Template;
4. Click Browse;
5. Select the OVF file from the extracted zip file;

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

8. Specify the name of the OVF template and click **Next**;
9. Select the **Thin provision** Disk Format option and click **Next**;

10. Click **Finish** to complete the installation.
2.3. Citrix XenServer 5.6

1. Unzip the downloaded package;
2. Start XenCenter;
3. Go to File and select Appliance Import;
4. Select the OVF file and then click **Next**;

![Select an Appliance for Import](image1)

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

6. Select the target for the Virtual Appliance;

![Select target XenServers or Pools](image2)
7. Select the storage location;

8. Select the network (keep default values);
9. On the Security screen click **Next**;

10. On the Advanced Options screen click **Next**;
11. On the **Finish** screen, review the configuration, click **Finish** and wait for the import to be completed.

   ![Import Progress](image)

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

   Follow the Endpoint Protector Appliance User Manual from this point on.
3. Implement using the VMX format

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

3.1. Implementing using VMware Server

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

4. Browse in the inventory for Endpoint Protector Virtual Appliance and select the VMX file and click **OK**;
At this point, the Virtual Machine is ready to be started.
Follow the Endpoint Protector Appliance User Manual from this point on.

3.2. Implementing using VMware Player

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

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;

![VMware Player interface]

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);

![Virtual Machine dialog]

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

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

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

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

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 On the Choose Import Type section, select Copy the virtual machine (create a new unique ID) option;
3.3. To ignore the Connect Network errors for Network Adapter, click 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;

8. Click **Apply** - the Virtual Machine is now imported and ready to be configured.

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

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

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

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

2. Select **Accept**;
3. Select **Networking**;

4. The configuration methods are now available.

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

5.1.1. **Automatic configuration**

Select configure network automatically, and select **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

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

Use the default Endpoint Protector credentials for the root account.

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. Select 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 deactivated features such as File Tracing and File Shadowing, and the default parameters for the generated logs can also be configured.

By default, the recommended settings are already configured and they apply globally throughout the entire network.
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 are completed. The next step is to deploy the Endpoint Protector Clients to the Windows, Mac, and Linux computers that need to be protected.
7. Server Information and Maintenance

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

7.1. Server Information

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

7.2. Server Maintenance

This section provides the option to configure the Appliance network settings, reboot or shut 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. Hardware Appliance Setup

8.1. Endpoint Protector Appliance Delivery

When receiving the Endpoint Protector Appliance, the package contains:

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

8.2. Connecting Appliance for Initial Setup

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

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

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

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

8.3. Hardware Appliance Back and Front Panel

8.3.1. A20 Appliance Back Panel

![A20 Appliance Back Panel Diagram]

8.3.2. A50 and A100 Appliance Back Panel

![A50 and A100 Appliance Back Panel Diagram]

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

8.3.3. A20 Appliance Front Panel

![A20 Appliance Front Panel Diagram]
8.3.4. A50 and A100 Appliance Front Panel

8.3.5. A250, A500, and A1000 Appliance Front Panel
8.3.6. A2000 - A4000 Appliance Front Panel

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

In case of an HDD failure, the HDD can be replaced by changing it with the same model HDD. Each HDD bay features a blue and red LED to indicate drive status. A blue indicator symbolizes a healthy hard drive, and a red indicator a bad hard drive. A faulty hard drive should be replaced immediately by an identical model.

8.4. A2000 / A4000 Appliance HDD Configuration

8.4.1. A2000 Appliance HDD Configuration

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

In case of an HDD failure, the HDD can be replaced by changing it with the same model HDD. Each HDD bay features a blue and red LED to indicate drive status. A blue indicator symbolizes a healthy hard drive, and a red indicator a bad hard drive. A faulty hard drive should be replaced immediately by an identical model.
8.4.2. A4000 Appliance HDD Configuration

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

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

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

8.4.3. A2000 and A4000 Appliance HDD RAID Additional Software

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

8.5. Hardware Appliance Setup Wizard

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

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

For additional support resources, please visit our [website](#) where you can read manuals, FAQs, watch videos and tutorials, direct e-mail support, and much more.

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

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

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

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