User Manual
A20 / A50 / A100 / A250 / A500 / A1000 / A2000 / A4000
# Table of Contents

1. Endpoint Protector Appliance Setup .......... 1
   1.1. Endpoint Protector Appliance Delivery ........................................ 1
   1.2. Connecting Appliance for Initial Setup ........................................ 2
   1.3. Hardware Appliance Back / Front Panel ...................................... 3
      1.3.1. A20 Appliance Back Panel .................................................... 3
      1.3.2. A50 and A100 Appliance Back Panel ....................................... 3
      1.3.3. A20 Appliance Front Panel .................................................... 3
      1.3.4. A50 and A100 Appliance Front Panel ....................................... 4
      1.3.5. A250, A500 and A1000 Appliance Front Panel ......................... 4
      1.3.6. A2000 - A4000 Appliance Front Panel .................................... 5
   1.4. A2000 / A4000 Appliance HDD Configuration ................................. 5
      1.4.1. A2000 Appliance HDD Configuration ........................................ 5
      1.4.2. A4000 Appliance HDD Configuration ........................................ 6
      1.4.3. A2000 and A4000 Appliance HDD RAID 3ware® 3DM® Additional Software ............................................................. 6
   1.5. Access Appliance Setup Wizard with NORMAL Network Cable (only for A20) ........................................................................ 7
   1.6. Access Appliance Setup Wizard directly with CROSSED Network Cable (Models A50 and larger) ......................................................... 7
   1.7. Appliance Setup Wizard .................................................................. 9
      1.7.1. End User License Agreement - Appliance License Agreement ........ 9
      1.7.2. Define your Appliance Administrator Password .......................... 10
      1.7.3. Set Time Zone ........................................................................ 11
      1.7.4. Set Appliance Network IP Address .......................................... 12
      1.7.5. Endpoint Protector Client – Automatic MSI Repackaging ......... 13
      1.7.6. Appliance Server Certificate ..................................................... 14
      1.7.7. Finishing the Endpoint Protector Appliance Setup ..................... 15

2. Endpoint Protector Appliance Configuration 16
   2.1. Connect Appliance to Network ..................................................... 16
   2.2. Firewall settings for the Appliance ............................................ 16
   2.3. Access to the Appliance Interface through your Network ............ 16
   2.4. Login to Appliance Interface ...................................................... 17
   2.5. Appliance Configuration Wizard .................................................. 18
II | Endpoint Protector Appliance | User Manual

2.6. Appliance Basic Settings ......................................................... 19
2.7. Appliance Default Policies......................................................... 21
2.8. Finishing the Endpoint Protector Appliance Configuration Wizard
21

3. Appliance Settings and Maintenance ........ 22
3.1. Server Information......................................................................... 22
   3.1.1. Fail Over ............................................................................ 23
3.2. Server Maintenance ........................................................................ 25
   3.2.1. Network Settings ................................................................. 25
   3.2.2. Reboot the Appliance ......................................................... 25
   3.2.3. Reset Appliance to Factory Default ....................................... 25
3.3. Endpoint Protector Client Installation for Appliance.................... 26
3.4. Appliance Online Live Update...................................................... 28

4. Installing Root Certificate to your Internet
   Browser .......................................................................................... 29
   4.1. For Microsoft Internet Explorer .............................................. 29
   4.2. For Mozilla Firefox ................................................................. 38

5. Support ......................................................................................... 40

6. Important Notice / Disclaimer .................... 41
1. Endpoint Protector Appliance Setup

1.1. 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)
1.2. 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.
1.3. Hardware Appliance Back / Front Panel

1.3.1. A20 Appliance Back Panel

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

1.3.2. 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.

1.3.3. A20 Appliance Front Panel
1.3.4. A50 and A100 Appliance Front Panel

1.3.5. A250, A500 and A1000 Appliance Front Panel
1.3.6. 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 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.
1.4.2. A4000 Appliance HDD Configuration

The A4000 Appliance comes with 6 HDSS in RAID 5 Configuration. The HDSS 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.

1.4.3. A2000 and A4000 Appliance HDD RAID 3ware® 3DM® 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."
1.5. Access Appliance Setup Wizard with NORMAL Network Cable (only for A20)

Connect the blue cable to the A20 network port and then to the network.

Check the TCP/IPv4 Settings to be:

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.

1.6. Access Appliance Setup Wizard directly with CROSSED Network Cable (Models A50 and larger)

With your computer connect now to the Appliance through the CROSSED cable. Check the TCP/IPv4 Settings to be:
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.
1.7. Appliance Setup Wizard

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

1.7.1. End User License Agreement - Appliance License Agreement

To continue with the setup process, please review the End User License Agreement – Appliance License Agreement.
1.7.2. Define your Appliance Administrator Password

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

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

USERNAME: root

PASSWORD: epp2011

After entering and confirming your administrator password click next to continue.
1.7.3. 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 Server Maintenance option.
1.7.4. Set Appliance Network IP Address

Provide an IP address for your appliance under which it will be reachable in your network. In case your network uses IPs of type 192.168.0.0, then 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.

**NOTE!**

The network configuration needs to fit your network topology. For example, if your network uses class A IPs (e.g. 10.10.5.10) and there are no subnets defined, then the following information must be entered:

**IP Address:** 10.10.5.10  
**Gateway:** 10.10.5.1  
**Network Mask:** 255.255.255.0

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 Server Maintenance option.
1.7.5. Endpoint Protector Client – Automatic MSI Repackaging

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

For the Macintosh installation file the Appliance IP Address has to entered manually in the installation process of the Endpoint Protector Client on a MAC OS X computer.
1.7.6. 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 4. “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.
1.7.7. Finishing the Endpoint Protector Appliance Setup

Your Endpoint Protector Appliance has been set up.

Please disconnect now the crossed network cable from the appliance and continue connecting the appliance to your network as described in the next step.

**NOTE!**

Skip this step for A20 models! Please keep the blue cable connected.
2. Endpoint Protector Appliance Configuration

2.1. Connect Appliance to Network

After assigning in the Setup process a static IP address for the Endpoint Protector Appliance, you can connect now the Appliance to your network. Connect the appliance with a standard network cable through the network connector on the back of the appliance marked with NET (blue) to your network.

2.2. Firewall settings for the Appliance

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

- Server and Client: 443
- Liveupdate: 80

2.3. 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.
2.4. Login to Appliance Interface

Please enter your user name and password that you have defined for the Endpoint Protector Appliance in the previous setup step.
2.5. 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.
2.6. Appliance Basic Settings

Please provide here all required settings for the Appliance to function properly, including the Proxy Server ones if necessary. 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.
2.7. Appliance Default Policies

In this step you can define the default Appliance Policy for portable device use. This Policy (Global Settings) can be later changed.

![Endpoint Protector Appliance Configuration Tool](image)

2.8. 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.
3. Appliance Settings and Maintenance

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

3.1. Server Information

Here you can view information about the Server current state.
3.1.1. Fail Over

The Fail Over solution is an automatic switching to a redundant or standby Slave EPP Server upon the failure or abnormal termination of the Master EPP Server. Fail Over is an automatic process and usually operates without warning or requiring any human intervention.

At server level, failover automation uses a "heartbeat" cable that connects two appliances using the second network port designated, in general, for configuration. As long as a regular "pulse" or "heartbeat" continues between the main server and the second server, the second server will not initiate its takeover. The second server takes over the work of the first as soon as it detects an alteration in the "heartbeat" of the first appliance and if its own status is Ok.
Defining a fail scenario for EPP Server:

On the Master appliance, one of the following components will fail to work properly;
- Web Server (nginx);
- Database Server (MySQL);
- PHP-FPM – scripting language for EPP Server;
- Network Connection;
- Power

Workflow

Assumptions:
- Both appliances, Master and Slave are connected to the network and also have an internal connection using a “heartbeat” cable.
- EPP Client is sending data and it is connected to Master IP;
- Master EPP Server is replicating database, logs, shadows and file whitelist information on the Slave EPP Server

Actions

1. If Master is broken, it will try to heal itself first and if it fails will continue to step 2. If the selfheal went OK, the process will stop here and no role switch will occur;
2. Slave will check its own state to see if it’s able to switch to Master role;
3. If OK, Slave will switch role to Master and will change IP with the one from the Master;
4. Web Interface is updated with information that the currently working appliance is the Slave;
5. Master will cede the role in favor of the Slave and will switch the IP to the IP of the Slave;
   
   Note: Since the Slave took the IP from the Master, the EPP Client will continue sending data to that IP and a continuous communication is assured.
6. New data from EPP Client will enter the same IP, but the server is the original Slave now;
7. Slave has the Master IP’s now and will continue working like this until the Master is working properly again;
8. If, at any point, the original Master is fully functional again and connected to the network, it will take over the role from the Slave, becoming Master and the original Slave will go back to Slave state.
9. At this point, when everything is back to “normal”, the data collected from the EPP Client in the original Slave, which became Master, will be replicated on the original Master, which is up and running.

Note: Insertion in the Database is made with odd IDs on the Master and even IDs on the Slave. This will ensure that replicated data won’t have the same ID for a certain entry, causing a huge mess in the database.
3.2. Server Maintenance

3.2.1. 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 1.7.4 “Set Appliance Network IP Address”.

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

3.2.3. 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.
3.3. Endpoint Protector Client Installation for Appliance

**NOTE!**

Please make sure you activate the Endpoint Protector licenses before the client installation. The licenses can be activated from System Configuration -> System Licensing.

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 System Configuration Client Software menu option by entering the Appliance static IP Address in a browser (example http://192.168.0.201). Note: access it through HTTP and not HTTPS.

Active Directory can be used for Endpoint Protector Client deployment as well. This feature can be found in the Endpoint Protector Directory Services menu.
3.4. 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 have the choice to have the appliance check automatically for updates or manually. If new updates are available they will only be installed when applied by the administrator.
4. Installing Root Certificate to your Internet Browser

4.1. For Microsoft Internet Explorer

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

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.
Continue your navigation by clicking “Continue to this website (not recommended)”.

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

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

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

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

Select the “General” tab and then click “Install Certificate...” button or go to Tools->Internet Options-> Content->Certificates.
From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.
Browse for the Certificate file you downloaded from the Appliance Setup Wizard -> Appliance Server Certificate.
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.
4.2. 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.
5. Support

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