ENDPOINT PROTECTOR APPLIANCE

User Manual Version 4.0.0.5

User Manual

A20 / A50 / A100 / A250 / A500 / A1000 / A2000 / A4000

COSOSYS

Table of Contents

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)

EndpointProtector.com
Working safe with portable devices
EndpointProtector.com
Working safe with portable devices

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.

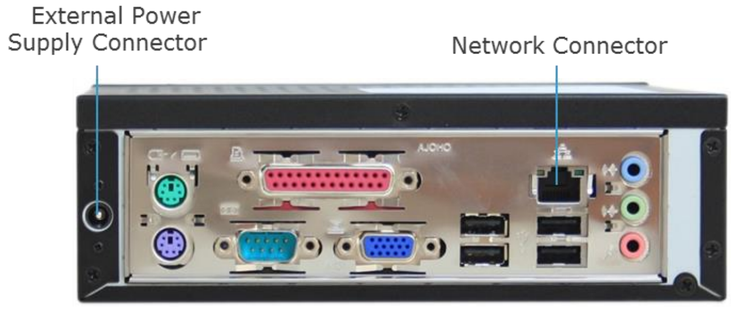
Your hardware appliance (models A50 to A4000) contains on the backside two network ports that are marked yellow for CONFIG (configuration connection) and blue for NET (network connection). The A20 hardware appliance has one network port.

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).

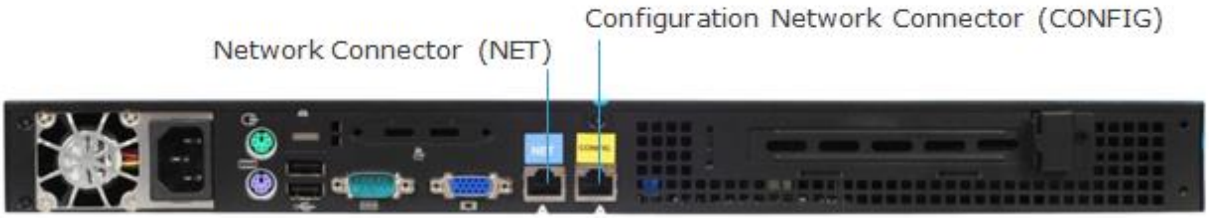
Start the Appliance by pushing the POWER button.

1.3. Hardware Appliance Back / Front Panel

1.3.1. A20 Appliance Back Panel



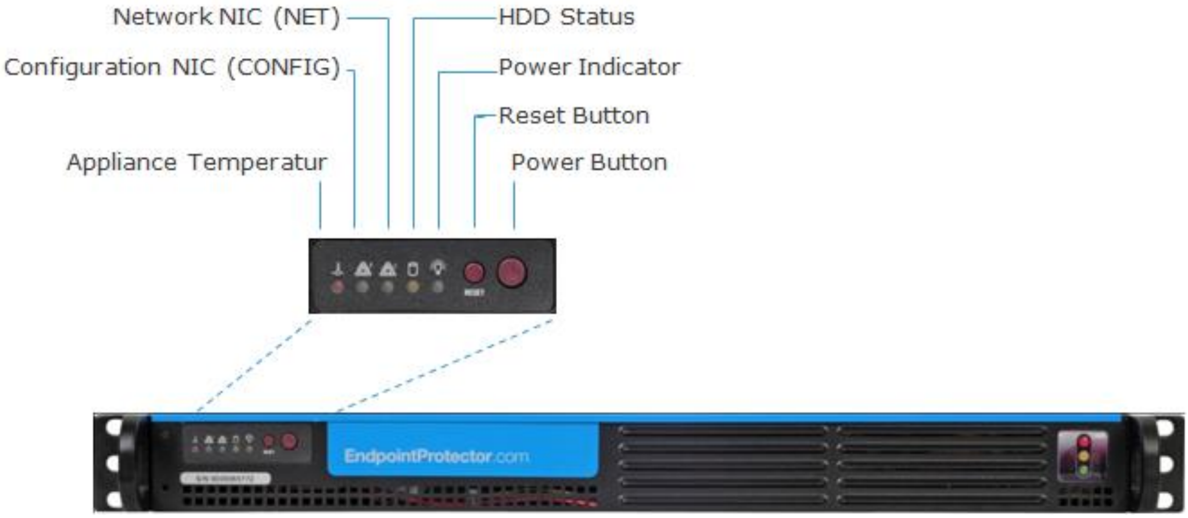
1.3.2. A50 and A100 Appliance Back Panel



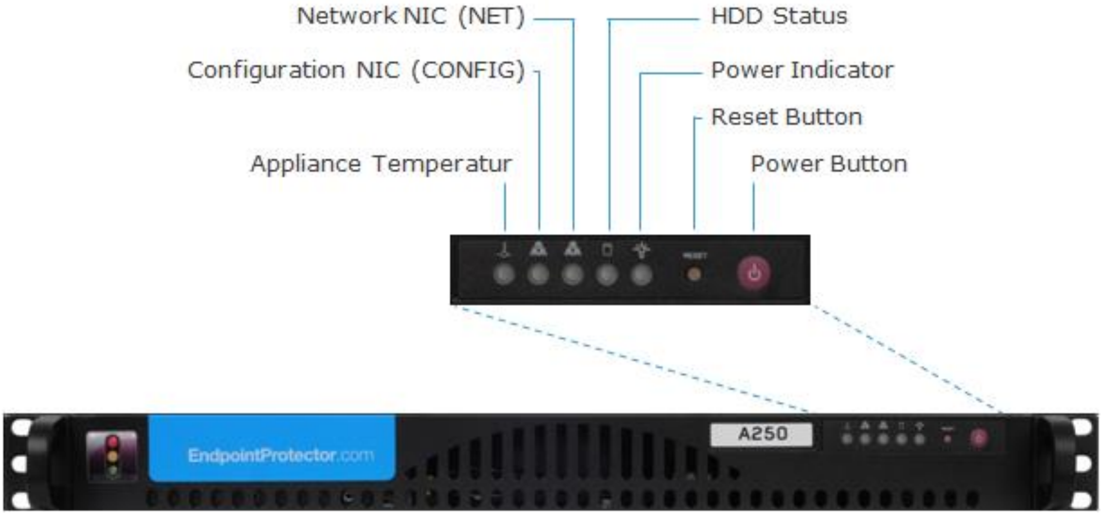
The back panels for Models A250 up to A4000 have marked network ports similar to the picture above for the A50 and A100 model.

1.3.3. A20 Appliance Front Panel

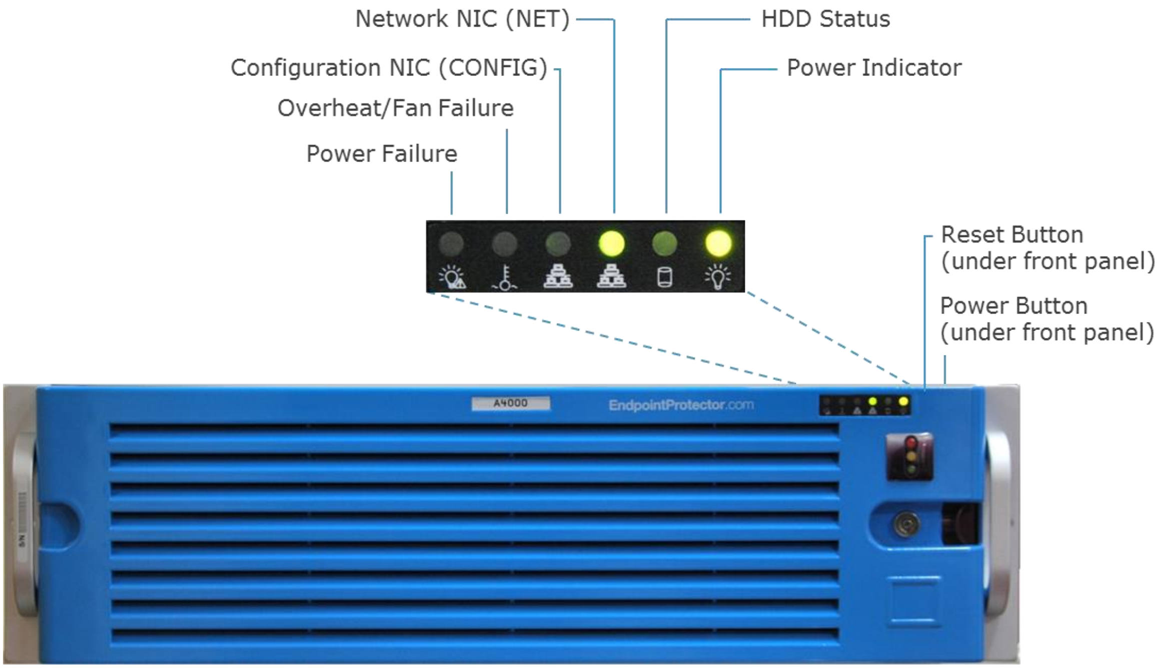
1.3.4. A50 and A100 Appliance Front Panel



1.3.5. A250, A500 and A1000 Appliance Front Panel

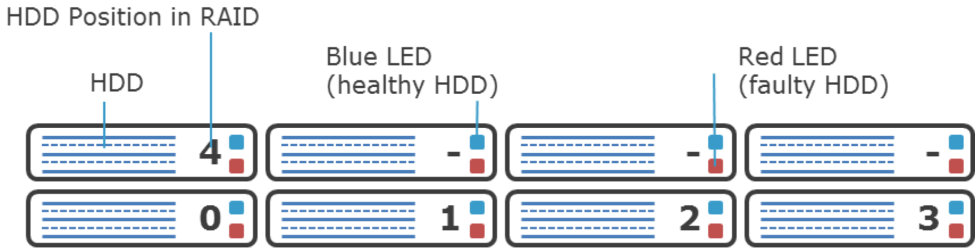


1.3.6. A2000 - A4000 Appliance Front Panel



1.4. A2000 / A4000 Appliance HDD Configuration

1.4.1. A2000 Appliance HDD Configuration

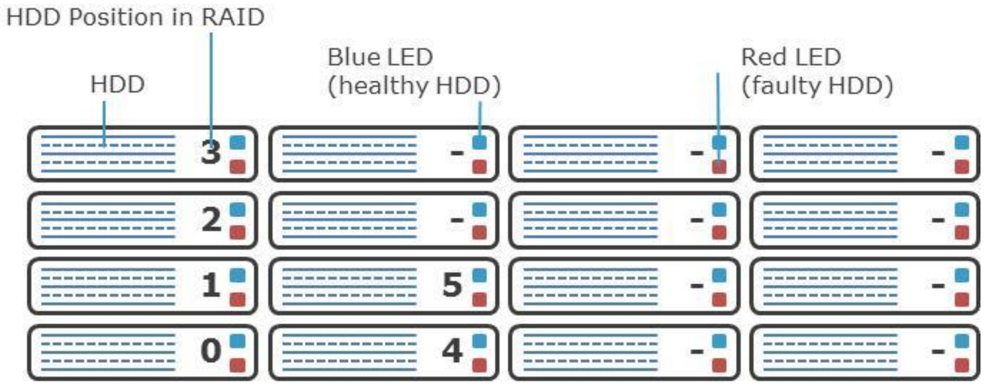


The A2000 Appliance comes with 4 HDDS in RAID 5 Configuration. The HDDs are installed in the number order 0-3.

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.

1.4.2. 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.

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."

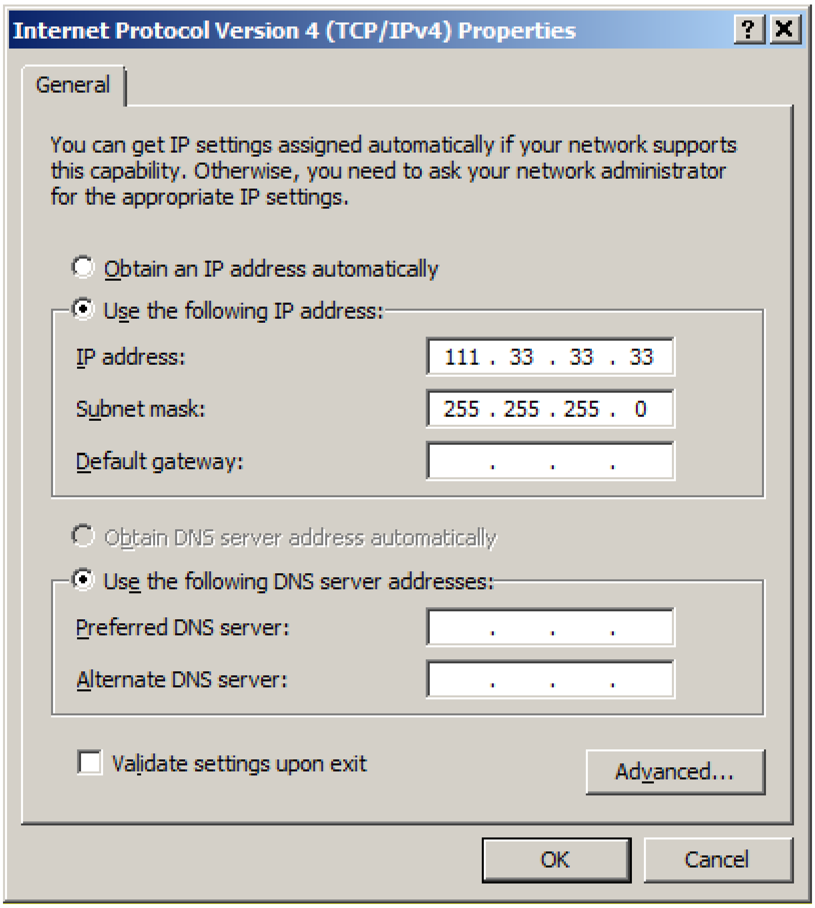
1.5. Access Appliance Setup Wizard with NORMAL Network Cable (only for A20)

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 111 . 33 . 33 . 33

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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

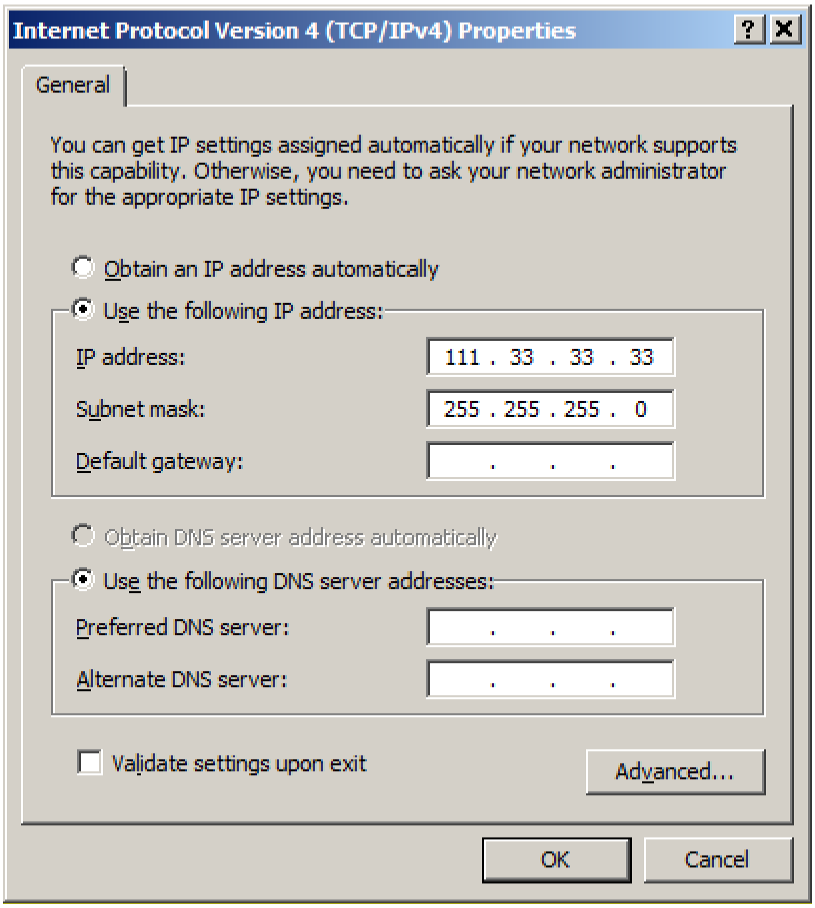
http://111.33.33.111 in the URL bar.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 111 . 33 . 33 . 33

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

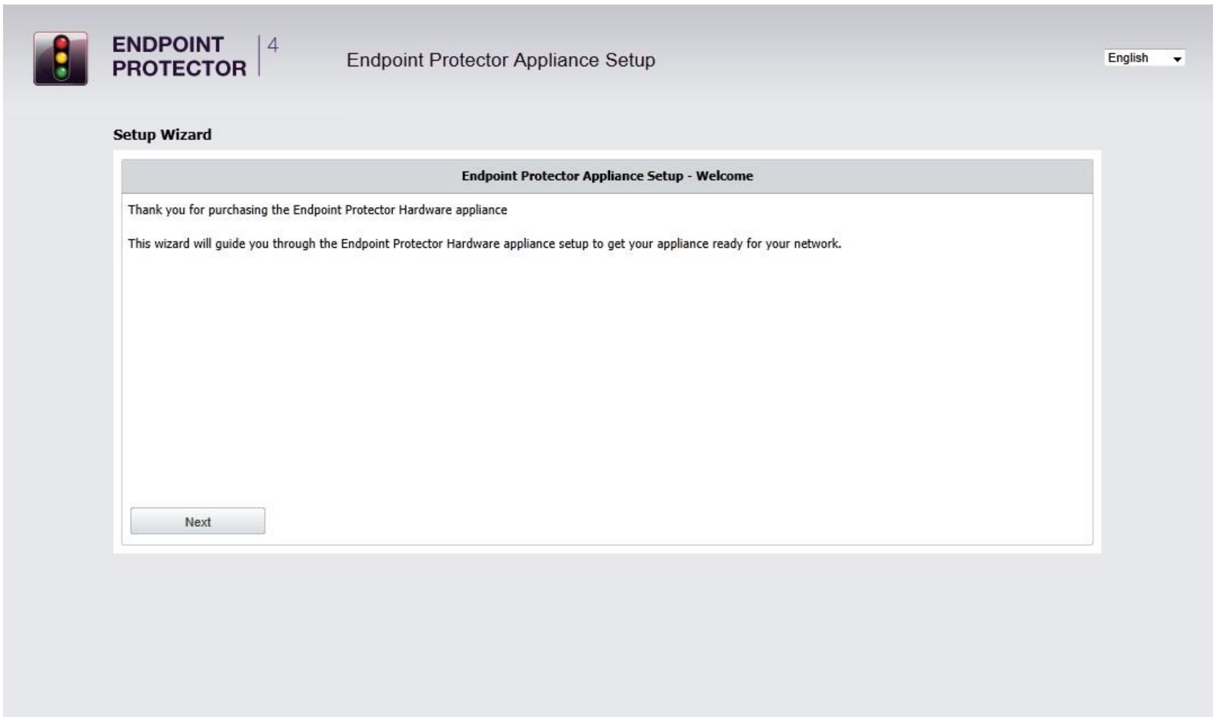
□ Validate settings upon exit

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

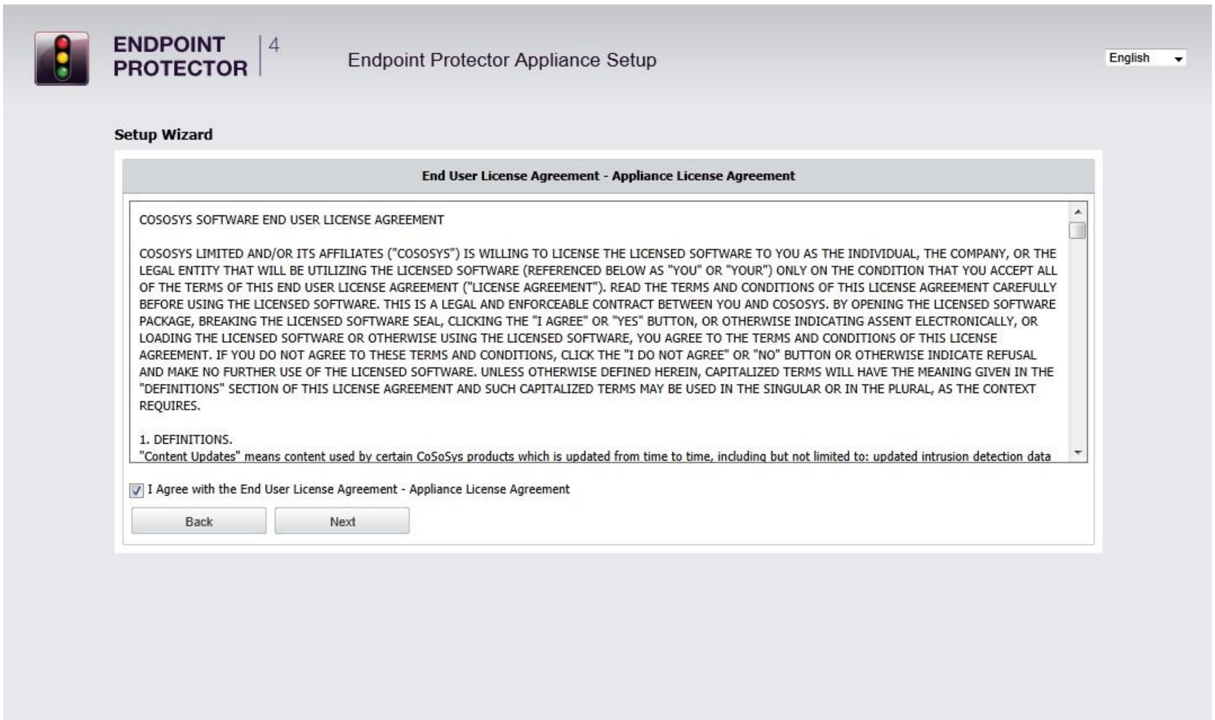
This wizard will guide you through the Endpoint Protector Hardware appliance setup to get your appliance ready for your network.


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector Appliance Setup - Welcome
Next

Thank you for purchasing the Endpoint Protector Hardware appliance

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


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
End User License Agreement - Appliance License Agreement
Back
Next

COSOSYS SOFTWARE END USER LICENSE AGREEMENT

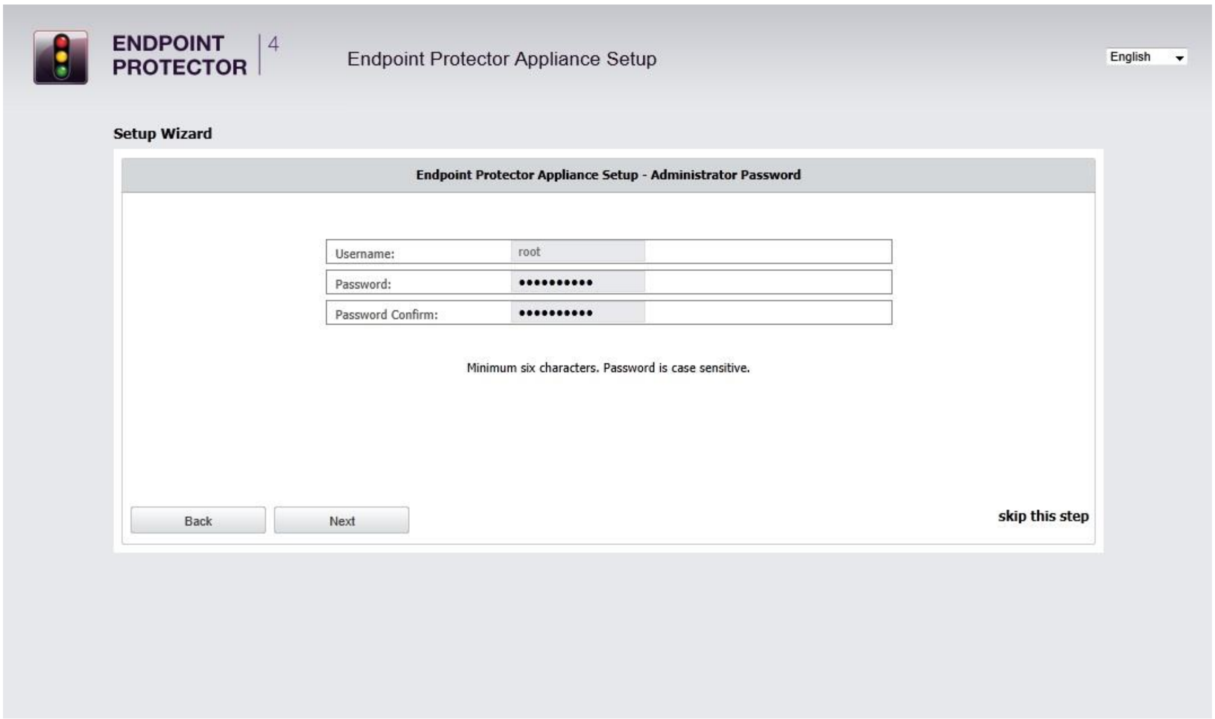
COSOSYS LIMITED AND/OR ITS AFFILIATES ("COSOSYS") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS END USER LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND COSOSYS. BY OPENING THE LICENSED SOFTWARE PACKAGE, BREAKING THE LICENSED SOFTWARE SEAL, CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE LICENSED SOFTWARE OR OTHERWISE USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE LICENSED SOFTWARE. UNLESS OTHERWISE DEFINED HEREIN, CAPITALIZED TERMS WILL HAVE THE MEANING GIVEN IN THE "DEFINITIONS" SECTION OF THIS LICENSE AGREEMENT AND SUCH CAPITALIZED TERMS MAY BE USED IN THE SINGULAR OR IN THE PLURAL, AS THE CONTEXT REQUIRES.

1. DEFINITIONS.
"Content Updates" means content used by certain CoSoSys products which is updated from time to time, including but not limited to: updated intrusion detection data

☑ I Agree with the 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


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector Appliance Setup - Administrator Password

Username: root
Password: ••••••••••
Password Confirm: ••••••••••

Minimum six characters. Password is case sensitive.

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

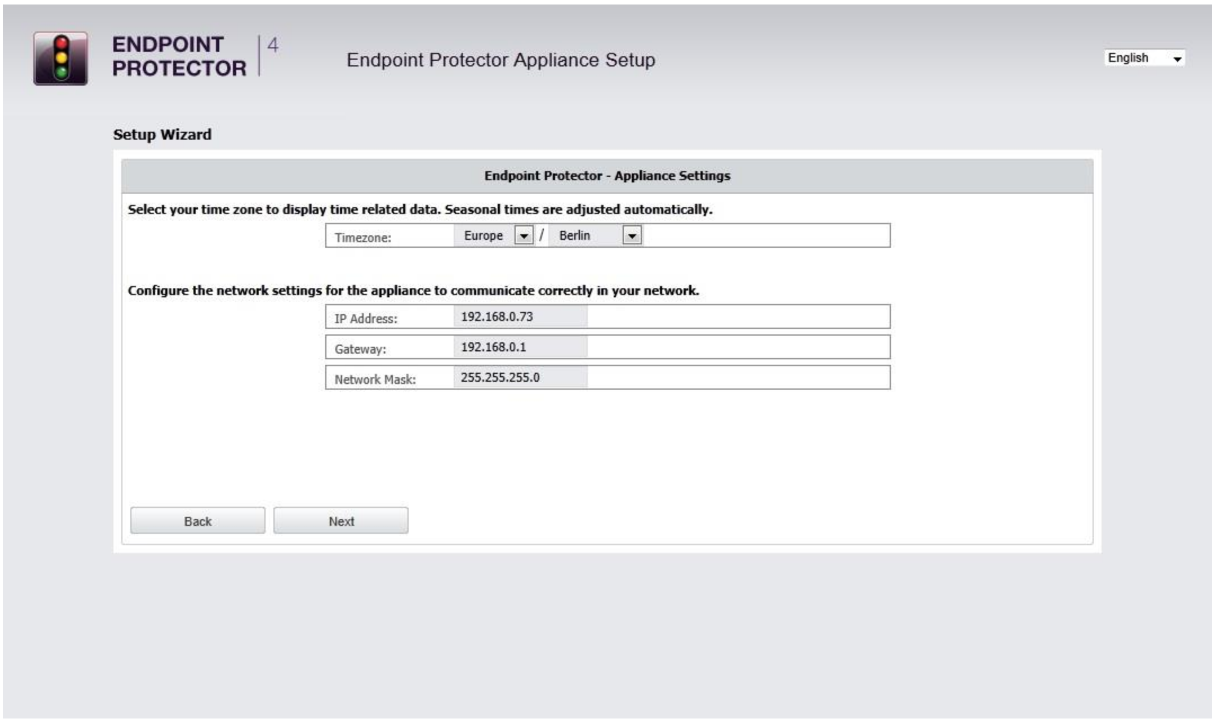
The default username and password for Endpoint Protector 4 Administration and Reporting Tool are:

USERNAME: root

PASSWORD: epp2011

After entering and confirming your administrator password click next to continue.

1.7.3. Set Time Zone



ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector - Appliance Settings
Back
Next

Select your time zone to display time related data. Seasonal times are adjusted automatically.

Timezone: Europe / Berlin

Configure the network settings for the appliance to communicate correctly in your network.

IP Address: 192.168.0.73

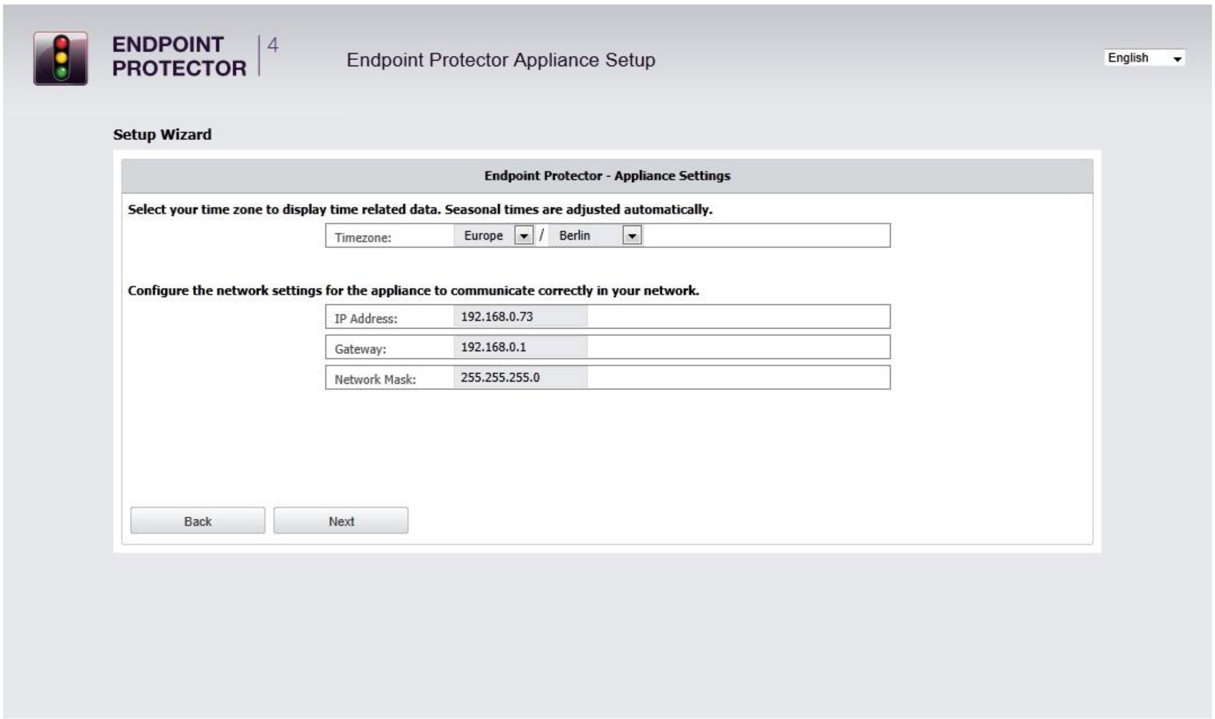
Gateway: 192.168.0.1

Network Mask: 255.255.255.0

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


ENDPOINT PROTECTOR | 4
Endpoint Protector Appliance Setup
English
Setup Wizard
Endpoint Protector - Appliance Settings
Back
Next

Select your time zone to display time related data. Seasonal times are adjusted automatically.

Timezone: Europe / Berlin

Configure the network settings for the appliance to communicate correctly in your network.

IP Address: 192.168.0.73

Gateway: 192.168.0.1

Network Mask: 255.255.255.0

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

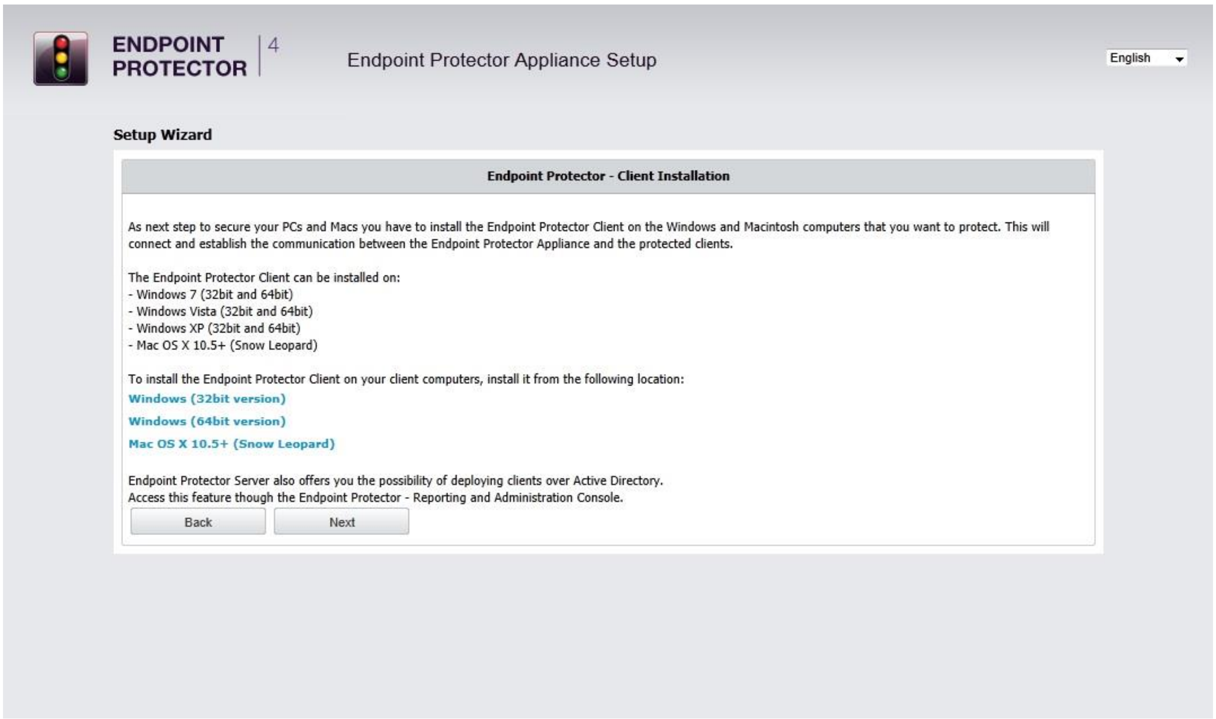
Gateway: 10.10.5.1

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



Setup Wizard

Endpoint Protector - Client Installation

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.

The Endpoint Protector Client can be installed on:
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)

To install the Endpoint Protector Client on your client computers, install it from the following location:

Windows (32bit version)

Windows (64bit version)

Mac OS X 10.5+ (Snow Leopard)

Endpoint Protector Server also offers you the possibility of deploying clients over Active Directory.
Access this feature though the Endpoint Protector - Reporting and Administration Console.

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.

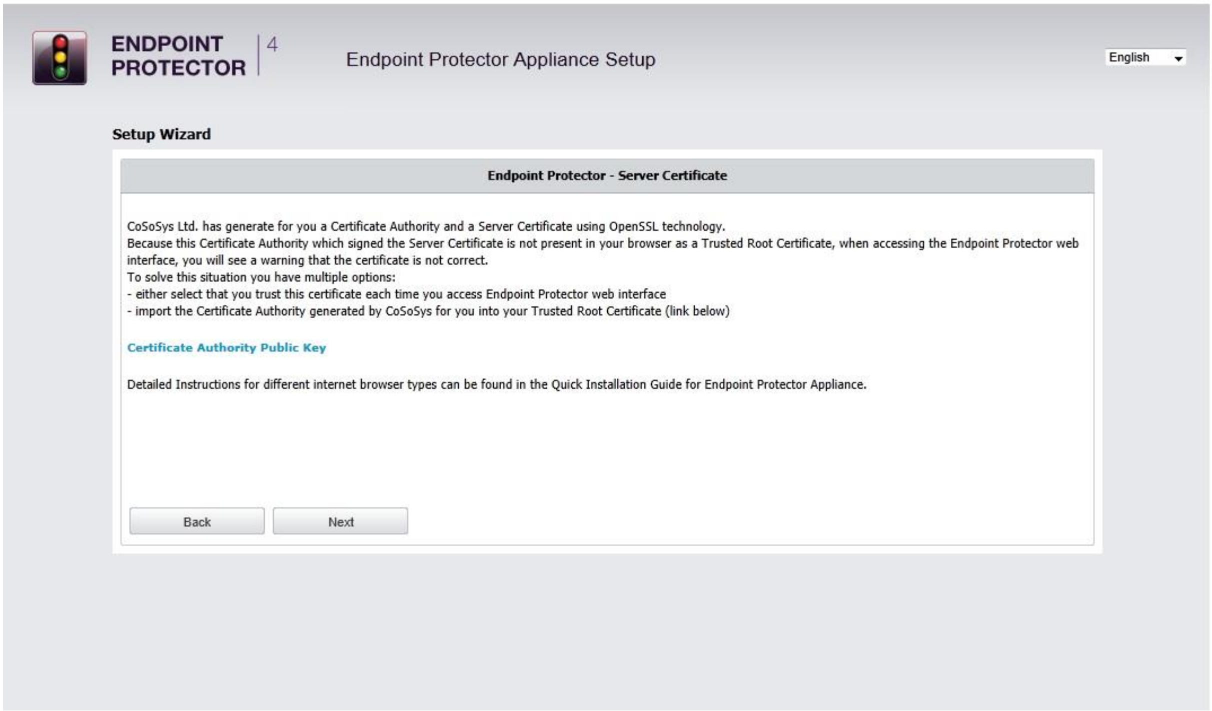
1.7.6. Appliance Server Certificate

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”.



Setup Wizard

Endpoint Protector - Server Certificate

CoSoSys Ltd. has generate for you a Certificate Authority and a Server Certificate using OpenSSL technology.
Because this Certificate Authority which signed the Server Certificate is not present in your browser as a Trusted Root Certificate, when accessing the Endpoint Protector web interface, you will see a warning that the certificate is not correct.
To solve this situation you have multiple options:
- either select that you trust this certificate each time you access Endpoint Protector web interface
- import the Certificate Authority generated by CoSoSys for you into your Trusted Root Certificate (link below)

Certificate Authority Public Key

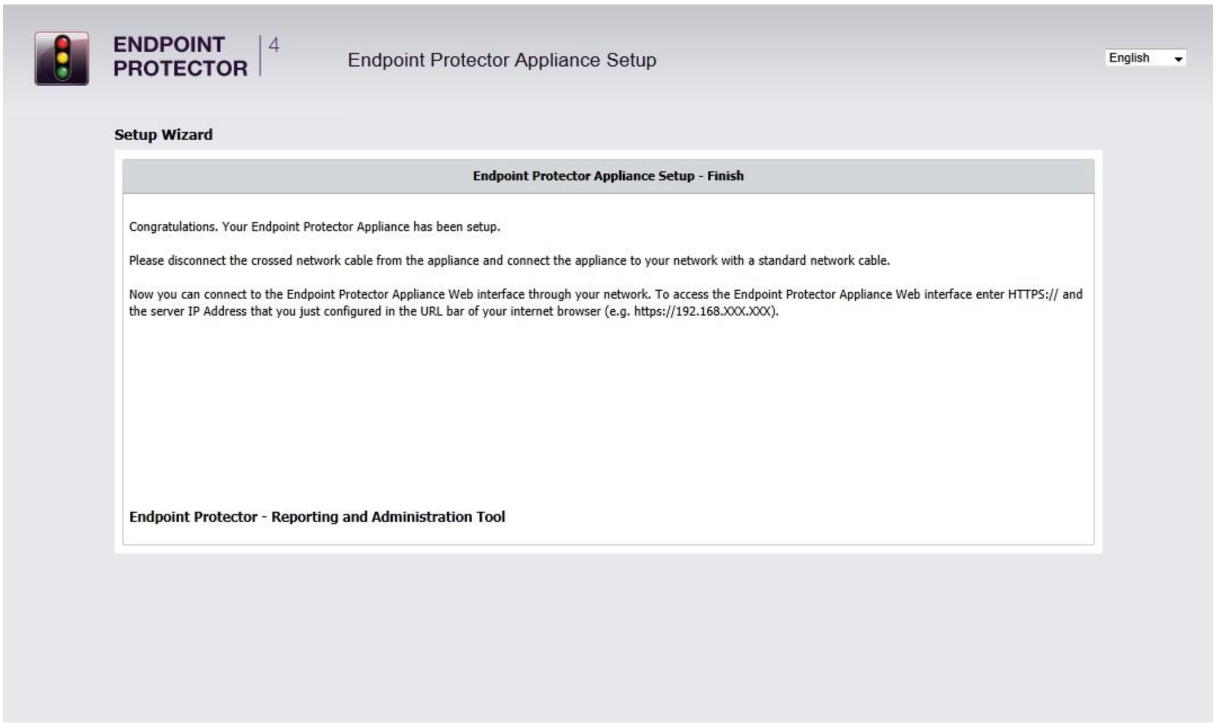
Detailed Instructions for different internet browser types can be found in the Quick Installation Guide for Endpoint Protector Appliance.

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 setup.

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



Endpoint Protector Appliance Setup - Finish

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.XXX.XXX).

Endpoint Protector - Reporting and Administration Tool

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

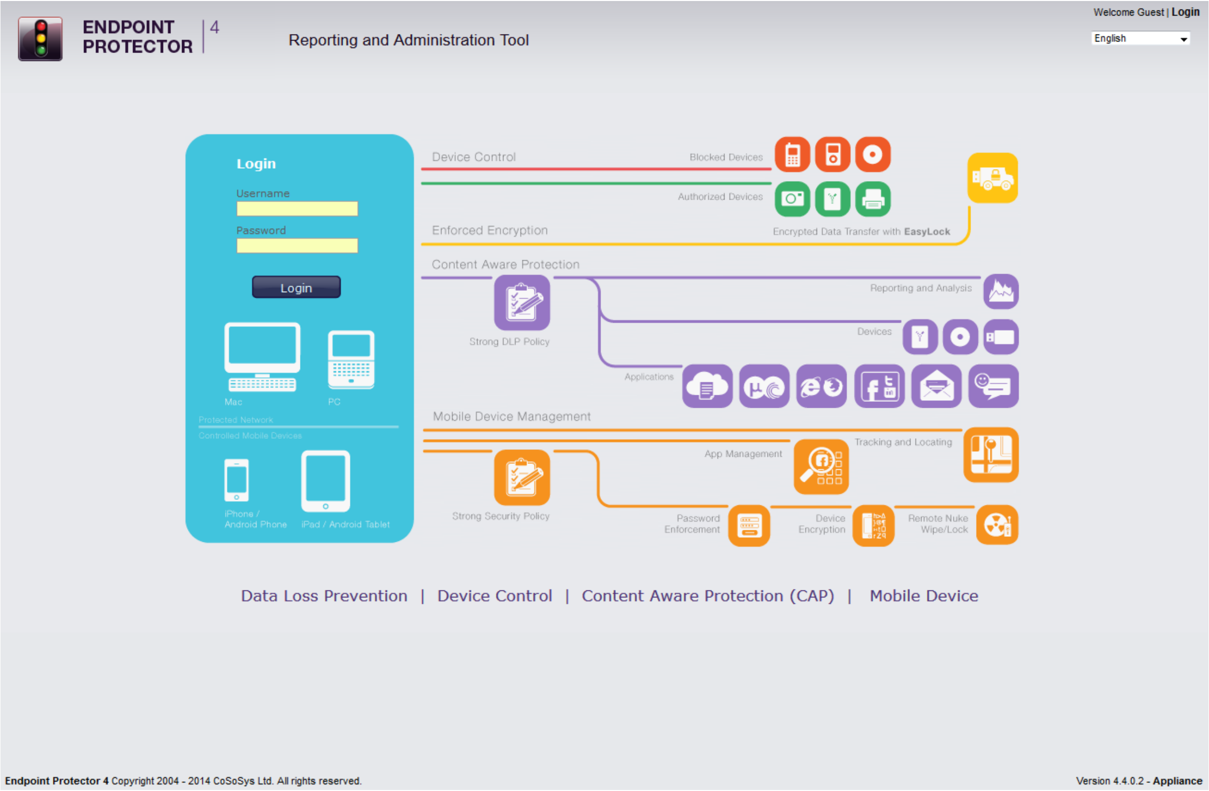
-Liveupdate: 80

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.

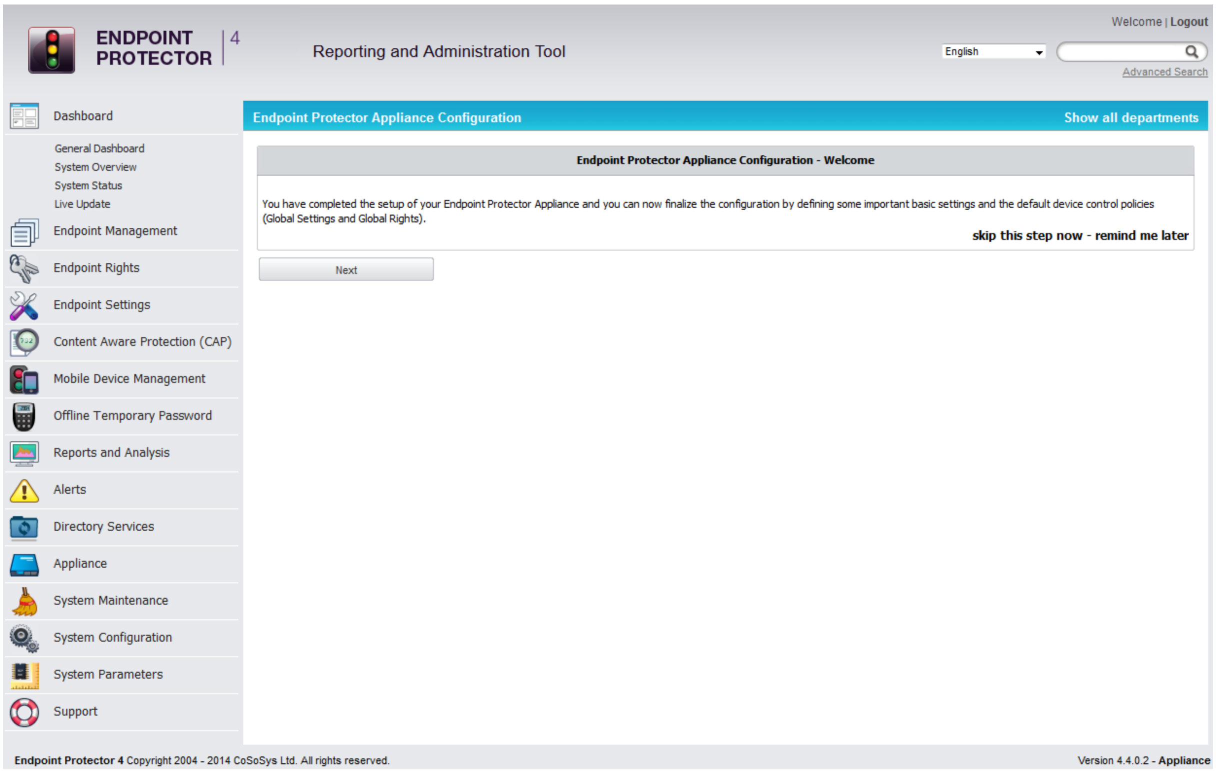


Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **Appliance**

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.



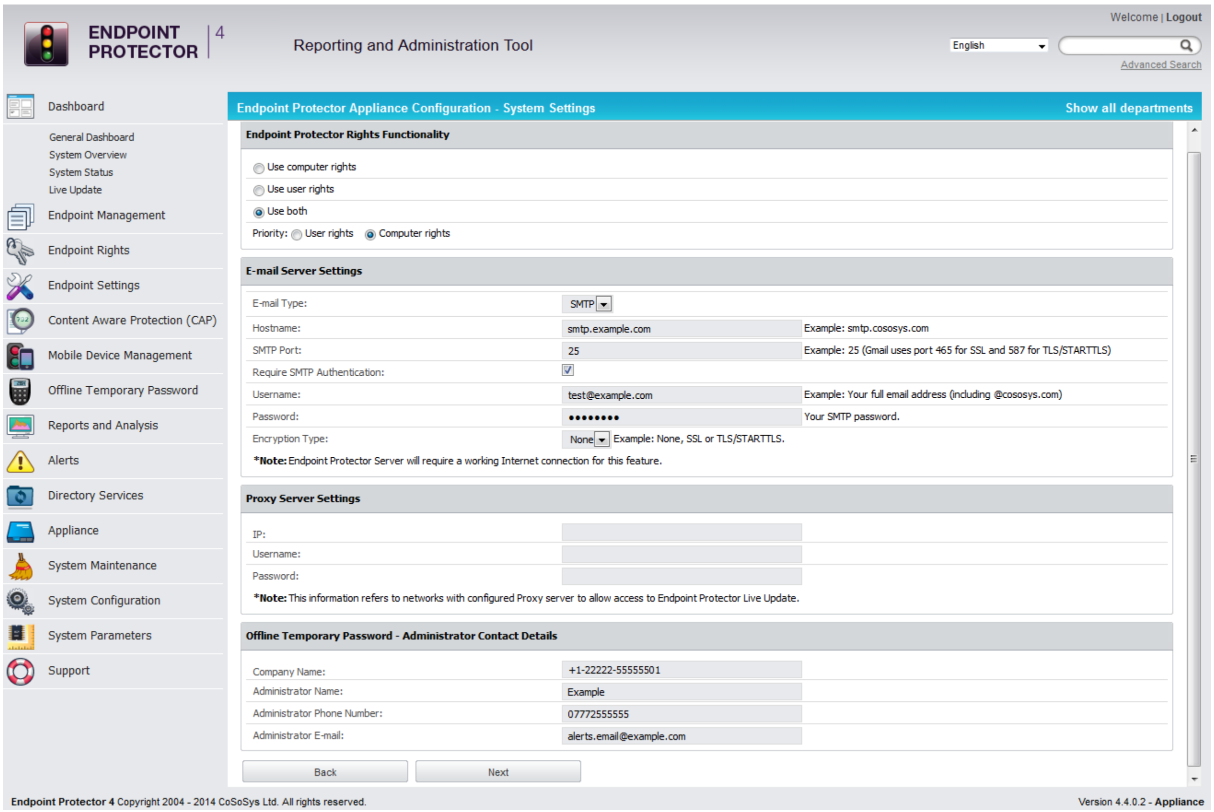
Endpoint Protector Appliance Configuration - Welcome

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 policies (Global Settings and Global Rights).

skip this step now - remind me later

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.



Endpoint Protector Appliance Configuration - System Settings

Endpoint Protector Rights Functionality

○ Use computer rights
○ Use user rights
● Use both
Priority: ○ User rights ● Computer rights

E-mail Server Settings

E-mail Type:	SMTP	
Hostname:	smtp.example.com	Example: smtp.cososys.com
SMTP Port:	25	Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:	☑	
Username:	test@example.com	Example: Your full email address (including @cososys.com)
Password:	••••••••	Your SMTP password.
Encryption Type:	None	Example: None, SSL or TLS/STARTTLS.

***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

Proxy Server Settings

IP:	
Username:	
Password:	

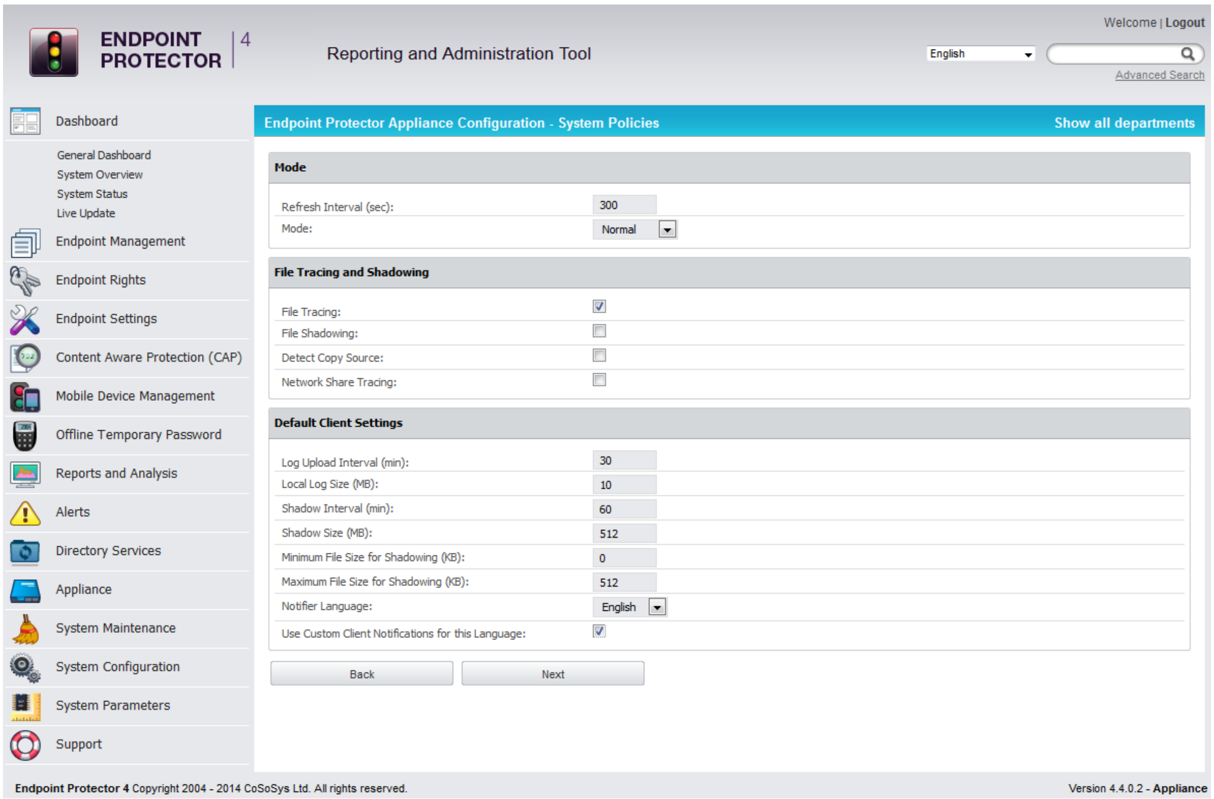
***Note:** This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.

Offline Temporary Password - Administrator Contact Details

Company Name:	+1-22222-55555501
Administrator Name:	Example
Administrator Phone Number:	07772555555
Administrator E-mail:	alerts.email@example.com

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Version 4.4.0.2 - **Appliance**

Additionally, you can select the Refresh Interval, activate/deactivate features such as File Tracing and File Shadowing and set default parameters for the generated logs.



Endpoint Protector Appliance Configuration - System Policies

Mode

Refresh Interval (sec):	300
Mode:	Normal

File Tracing and Shadowing

File Tracing:	☑
File Shadowing:	☐
Detect Copy Source:	☐
Network Share Tracing:	☐

Default Client Settings

Log Upload Interval (min):	30
Local Log Size (MB):	10
Shadow Interval (min):	60
Shadow Size (MB):	512
Minimum File Size for Shadowing (KB):	0
Maximum File Size for Shadowing (KB):	512
Notifier Language:	English
Use Custom Client Notifications for this Language:	☑

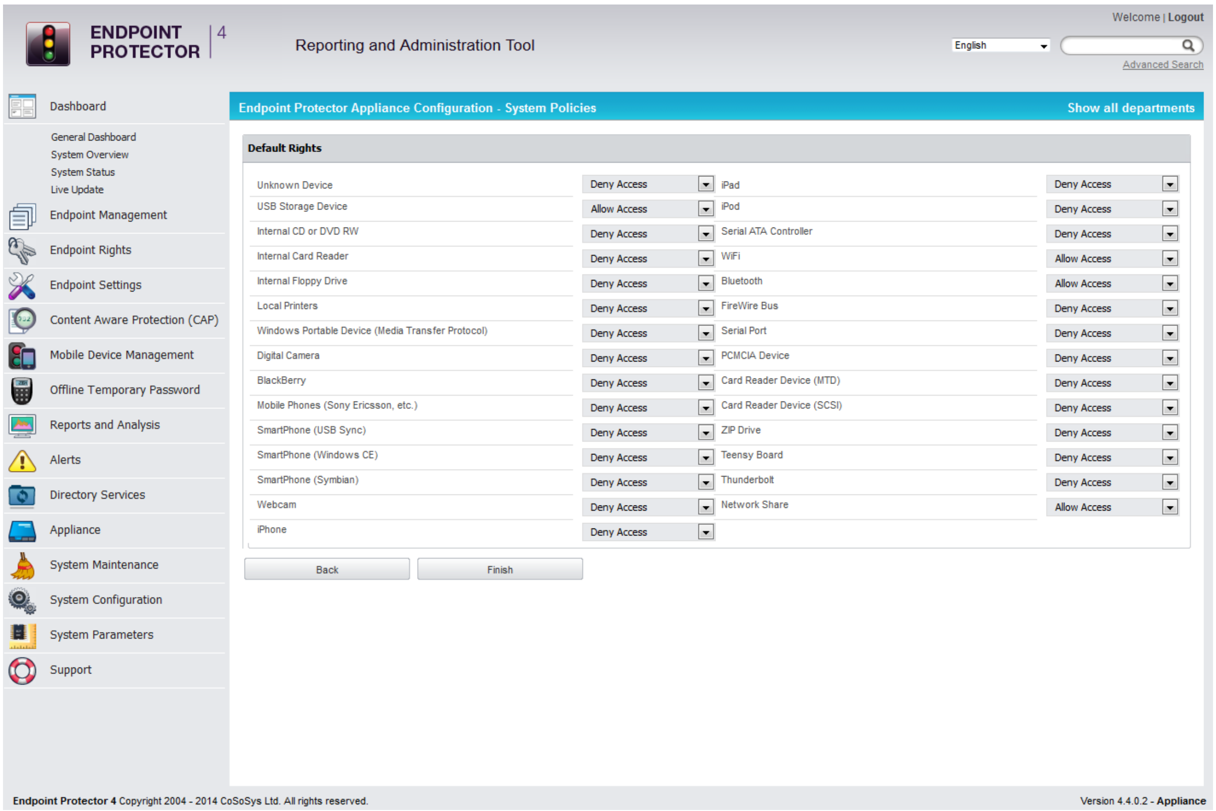
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **Appliance**

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 - System Policies

Default Rights

Unknown Device	Deny Access	iPad	Deny Access
USB Storage Device	Allow Access	iPod	Deny Access
Internal CD or DVD RW	Deny Access	Serial ATA Controller	Deny Access
Internal Card Reader	Deny Access	WiFi	Allow Access
Internal Floppy Drive	Deny Access	Bluetooth	Allow Access
Local Printers	Deny Access	FireWire Bus	Deny Access
Windows Portable Device (Media Transfer Protocol)	Deny Access	Serial Port	Deny Access
Digital Camera	Deny Access	PCMCIA Device	Deny Access
BlackBerry	Deny Access	Card Reader Device (MTD)	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access	Card Reader Device (SCSI)	Deny Access
SmartPhone (USB Sync)	Deny Access	ZIP Drive	Deny Access
SmartPhone (Windows CE)	Deny Access	Teensy Board	Deny Access
SmartPhone (Symbian)	Deny Access	Thunderbolt	Deny Access
Webcam	Deny Access	Network Share	Allow Access
iPhone	Deny Access		

2.8. Finishing the Endpoint Protector Appliance Configuration Wizard

You have now completed the setup and configuration of the Endpoint Protector Appliance.

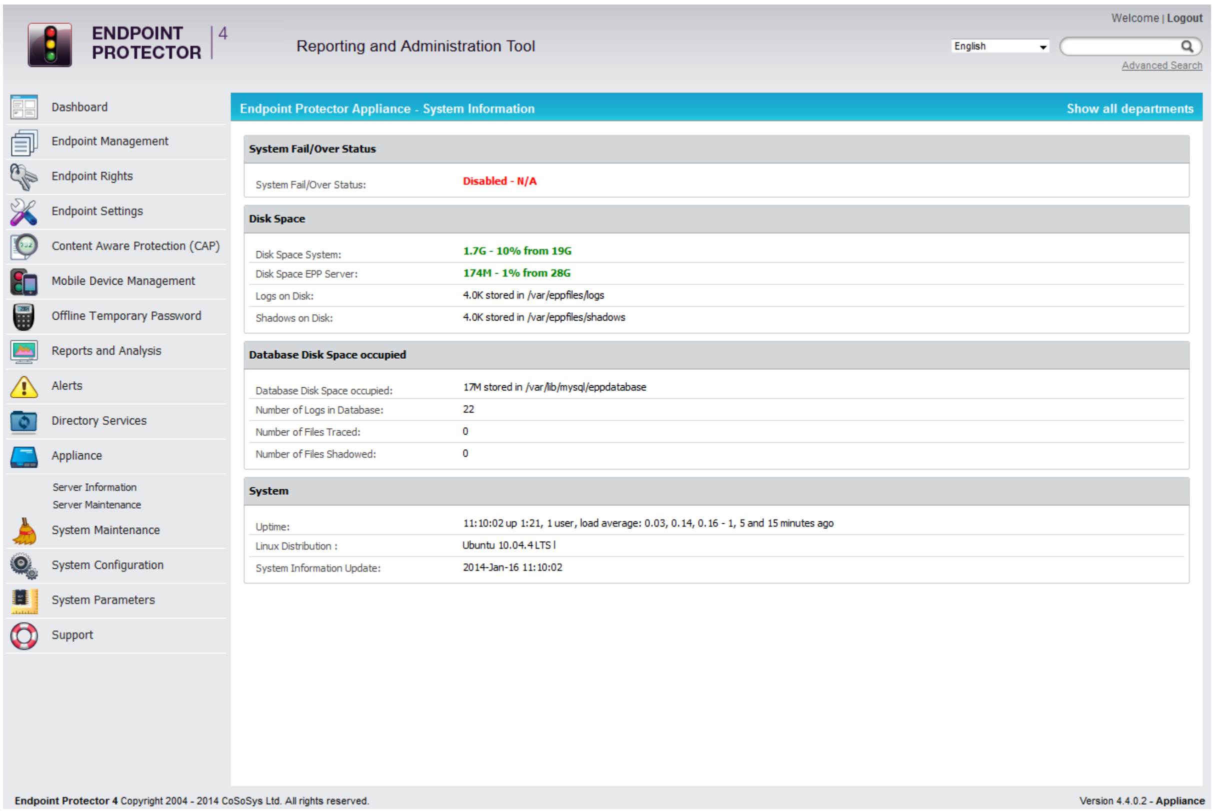
Now we recommend you to deploy the Endpoint Protector client to the Windows and Macintosh computers that you want to protect.

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.



System Fail/Over Status

System Fail/Over Status:	Disabled - N/A

Disk Space

Disk Space System:	1.7G - 10% from 19G
Disk Space EPP Server:	174M - 1% from 28G
Logs on Disk:	4.0K stored in /var/eppfiles/logs
Shadows on Disk:	4.0K stored in /var/eppfiles/shadows

Database Disk Space occupied

Database Disk Space occupied:	17M stored in /var/lib/mysql/eppdatabase
Number of Logs in Database:	22
Number of Files Traced:	0
Number of Files Shadowed:	0

System

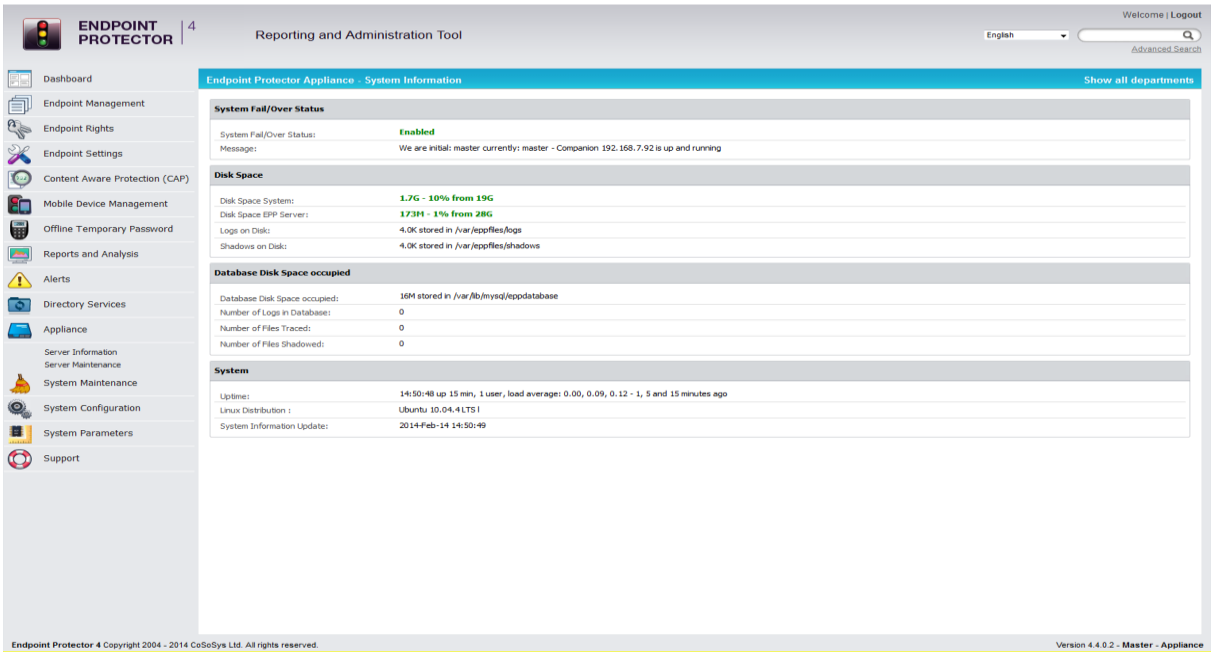
Uptime:	11:10:02 up 1:21, 1 user, load average: 0.03, 0.14, 0.16 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 10.04.4 LTS l
System Information Update:	2014-Jan-16 11:10:02

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **Appliance**

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.



Endpoint Protector Appliance - System Information

System Fail/Over Status

System Fail/Over Status:	**Enabled**
Message:	We are initial: master currently: master - Companion 192.168.7.92 is up and running

Disk Space

Disk Space System:	**1.7G - 10% from 19G**
Disk Space EPP Server:	**173M - 1% from 28G**
Logs on Disk:	4.0K stored in /var/eppfiles/logs
Shadows on Disk:	4.0K stored in /var/eppfiles/shadows

Database Disk Space occupied

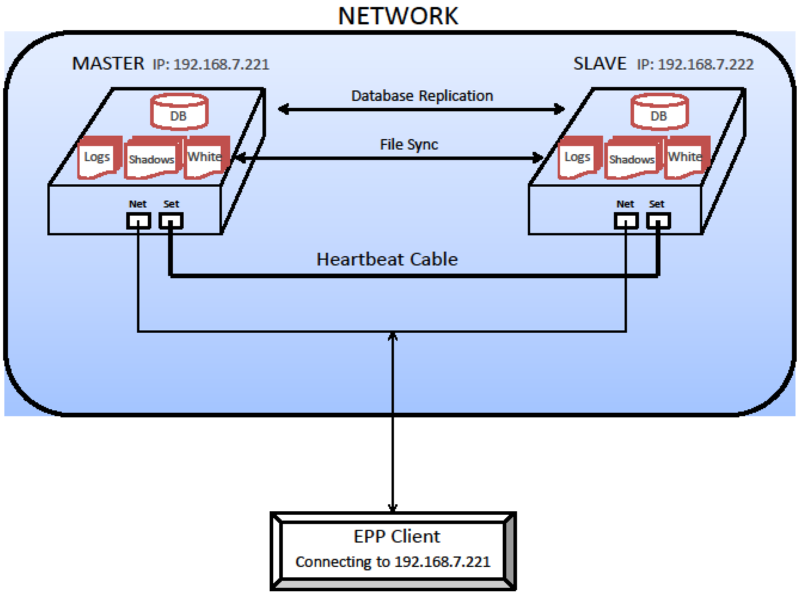
Database Disk Space occupied:	16M stored in /var/lib/mysql/eppdatabase
Number of Logs in Database:	0
Number of Files Traced:	0
Number of Files Shadowed:	0

System

Uptime:	14:50:48 up 15 min, 1 user, load average: 0.00, 0.09, 0.12 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 10.04.4 LTS l
System Information Update:	2014-Feb-14 14:50:49

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Version 4.4.0.2 - **Master** - **Appliance**

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

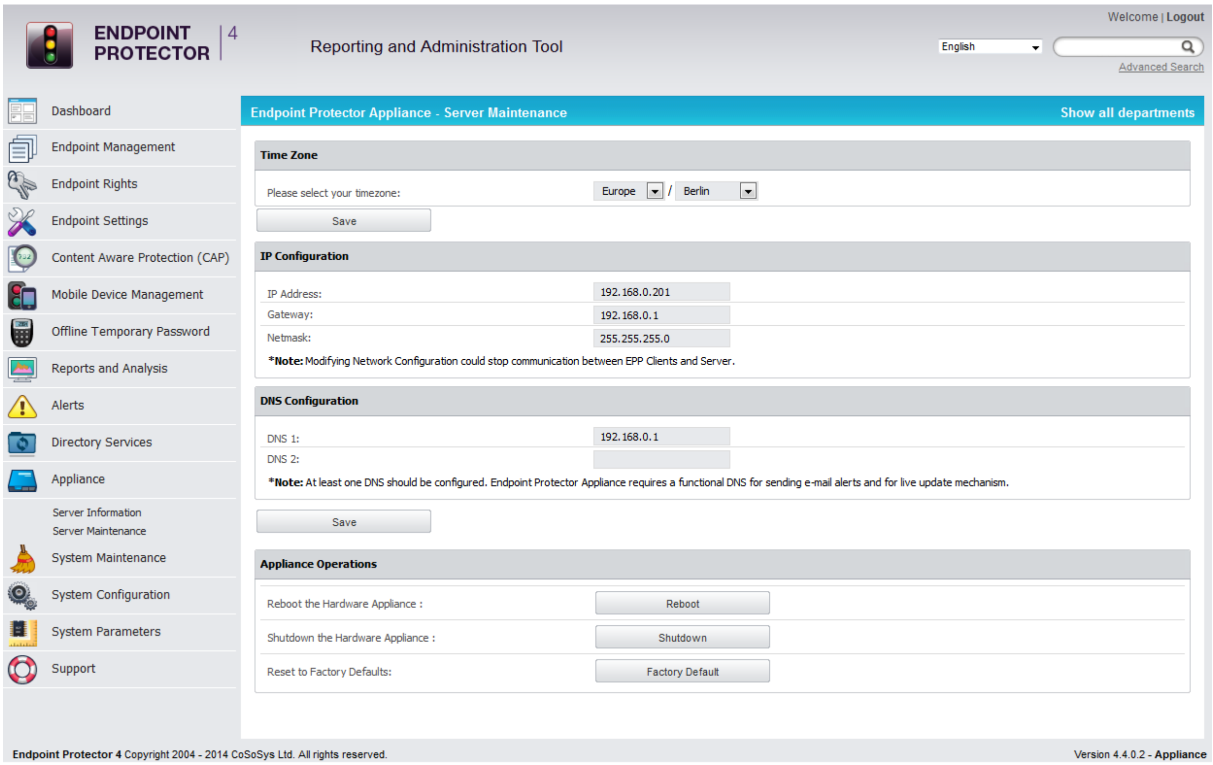
1. If **Master** is broken, it will try to heal itself first and if it fails will continue to step 2. If the selfheal went OK, the process will stop here and no role switch will occur;
2. **Slave** will check its own state to see if it's able to switch to **Master** role;
3. If OK, **Slave** will switch 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



Endpoint Protector Appliance - Server Maintenance

Time Zone

Please select your timezone: Europe / Berlin

IP Configuration

IP Address: 192.168.0.201
Gateway: 192.168.0.1
Netmask: 255.255.255.0

***Note:** Modifying Network Configuration could stop communication between EPP Clients and Server.

DNS Configuration

DNS 1: 192.168.0.1
DNS 2:

***Note:** At least one DNS should be configured. Endpoint Protector Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.

Appliance Operations

Reboot the Hardware Appliance :
Shutdown the Hardware Appliance :
Reset to Factory Defaults:

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **Appliance**

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.

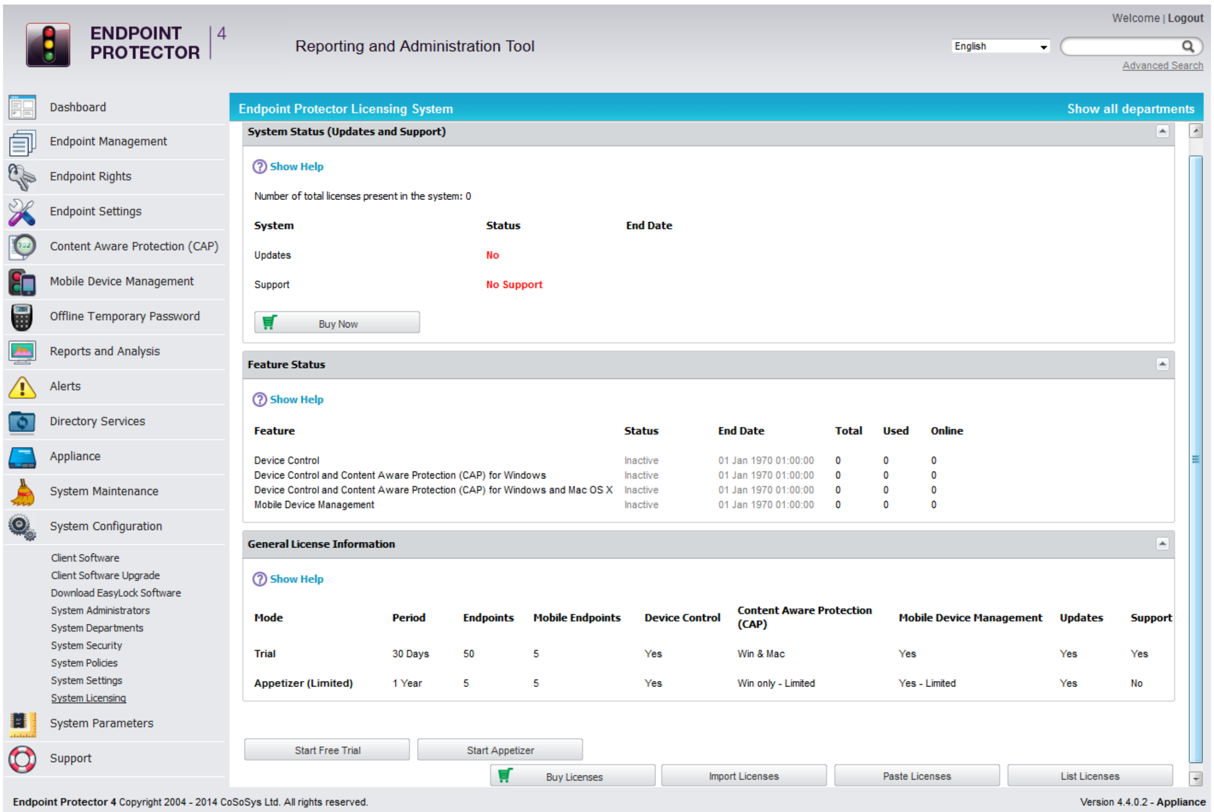
3.2.3. Reset Appliance to Factory Default

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.



System Status (Updates and Support)

Number of total licenses present in the system: 0

System	Status	End Date
Updates	No	
Support	No Support	

Feature Status

Feature	Status	End Date	Total	Used	Online
Device Control	Inactive	01 Jan 1970 01:00:00	0	0	0
Device Control and Content Aware Protection (CAP) for Windows	Inactive	01 Jan 1970 01:00:00	0	0	0
Device Control and Content Aware Protection (CAP) for Windows and Mac OS X	Inactive	01 Jan 1970 01:00:00	0	0	0
Mobile Device Management	Inactive	01 Jan 1970 01:00:00	0	0	0

General License Information

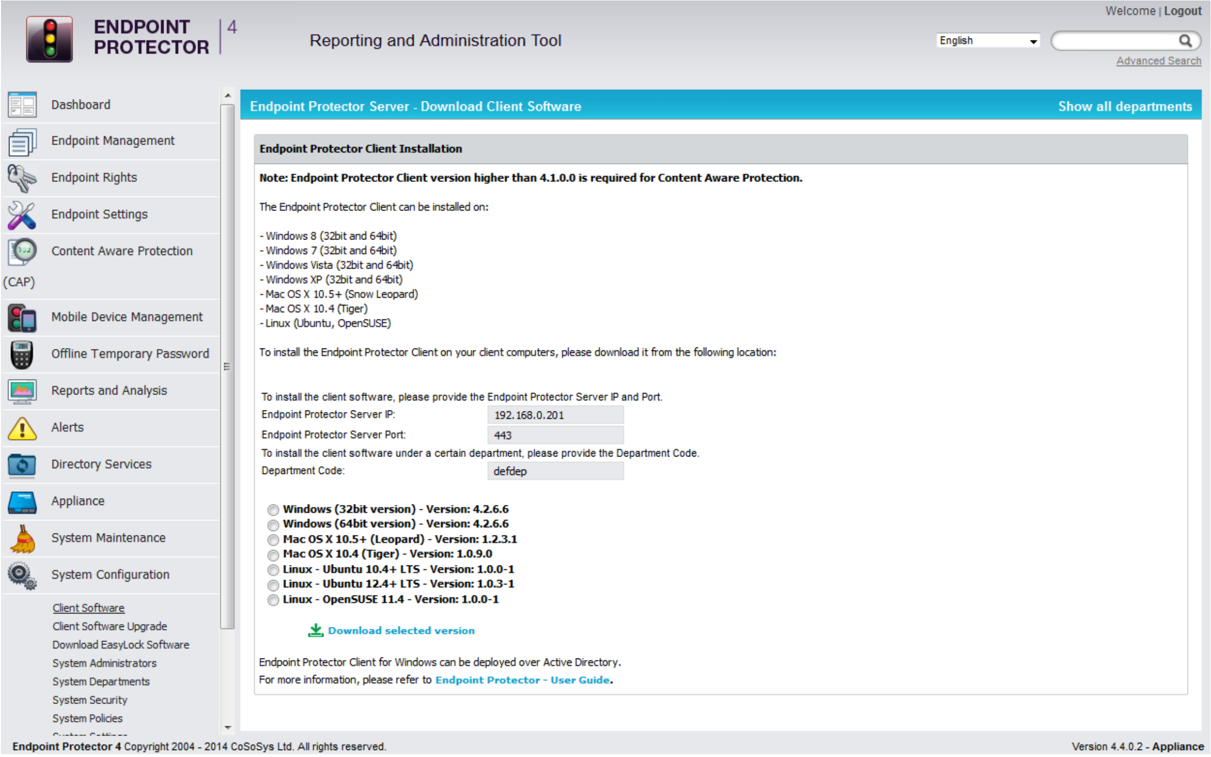
Mode	Period	Endpoints	Mobile Endpoints	Device Control	Content Aware Protection (CAP)	Mobile Device Management	Updates	Support
Trial	30 Days	50	5	Yes	Win & Mac	Yes	Yes	Yes
Appetizer (Limited)	1 Year	5	5	Yes	Win only - Limited	Yes - Limited	Yes	No

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **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 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.



Endpoint Protector Client Installation

Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.

The Endpoint Protector Client can be installed on:

- Windows 8 (32bit and 64bit)
- Windows 7 (32bit and 64bit)
- Windows Vista (32bit and 64bit)
- Windows XP (32bit and 64bit)
- Mac OS X 10.5+ (Snow Leopard)
- Mac OS X 10.4 (Tiger)
- Linux (Ubuntu, OpenSUSE)

To install the Endpoint Protector Client on your client computers, please download it from the following location:

To install the client software, please provide the Endpoint Protector Server IP and Port.

Endpoint Protector Server IP: 192.168.0.201

Endpoint Protector Server Port: 443

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

Department Code: defdep

○ **Windows (32bit version) - Version: 4.2.6.6**
○ **Windows (64bit version) - Version: 4.2.6.6**
○ **Mac OS X 10.5+ (Leopard) - Version: 1.2.3.1**
○ **Mac OS X 10.4 (Tiger) - Version: 1.0.9.0**
○ **Linux - Ubuntu 10.4+ LTS - Version: 1.0.0-1**
○ **Linux - Ubuntu 12.4+ LTS - Version: 1.0.3-1**
○ **Linux - OpenSUSE 11.4 - Version: 1.0.0-1**

Download selected version

Endpoint Protector Client for Windows can be deployed over Active Directory.
For more information, please refer to **Endpoint Protector - User Guide**.

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

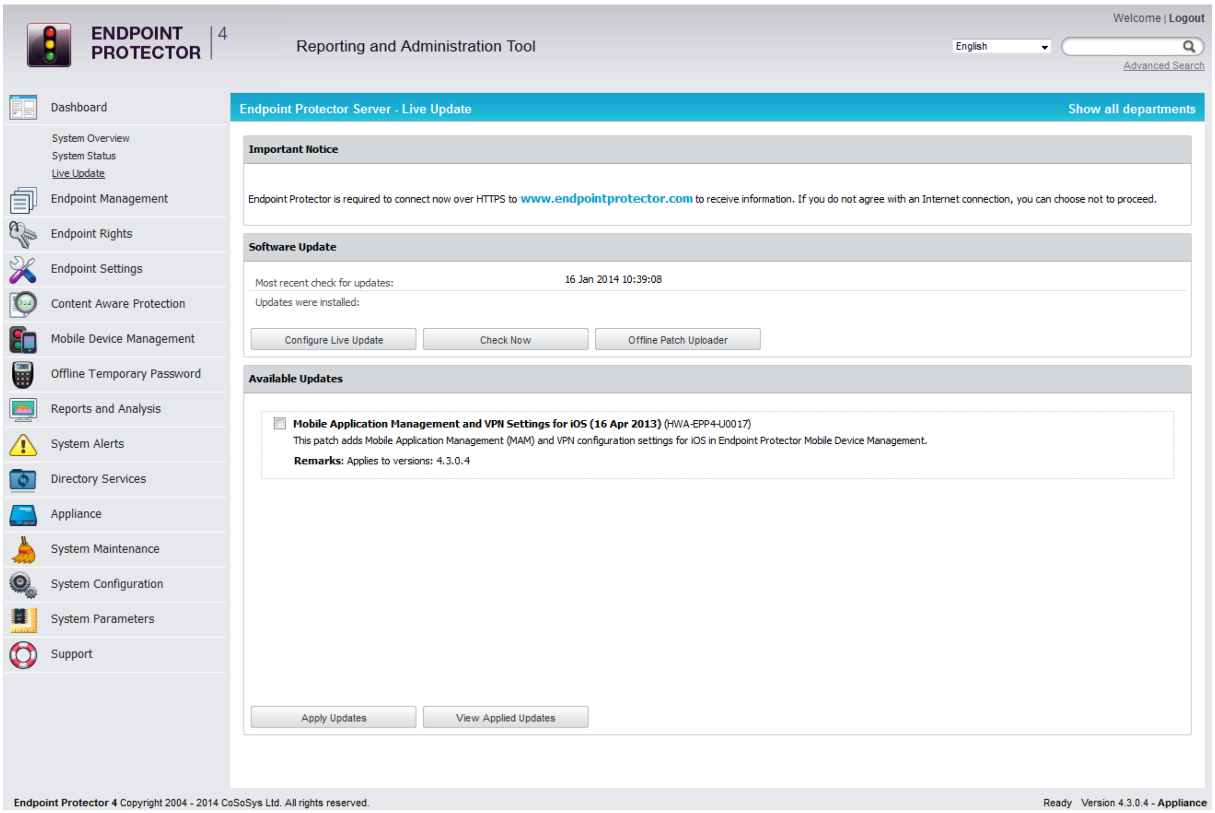
Version 4.4.0.2 - **Appliance**

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.



Endpoint Protector Server - Live Update

Important Notice

Endpoint Protector is required to connect now over HTTPS to www.endpointprotector.com to receive information. If you do not agree with an Internet connection, you can choose not to proceed.

Software Update

Most recent check for updates: 16 Jan 2014 10:39:08

Updates were installed:

Available Updates

☐ **Mobile Application Management and VPN Settings for iOS (16 Apr 2013)** (HWA-EPP4-U0017)
This patch adds Mobile Application Management (MAM) and VPN configuration settings for iOS in Endpoint Protector Mobile Device Management.
Remarks: Applies to versions: 4.3.0.4

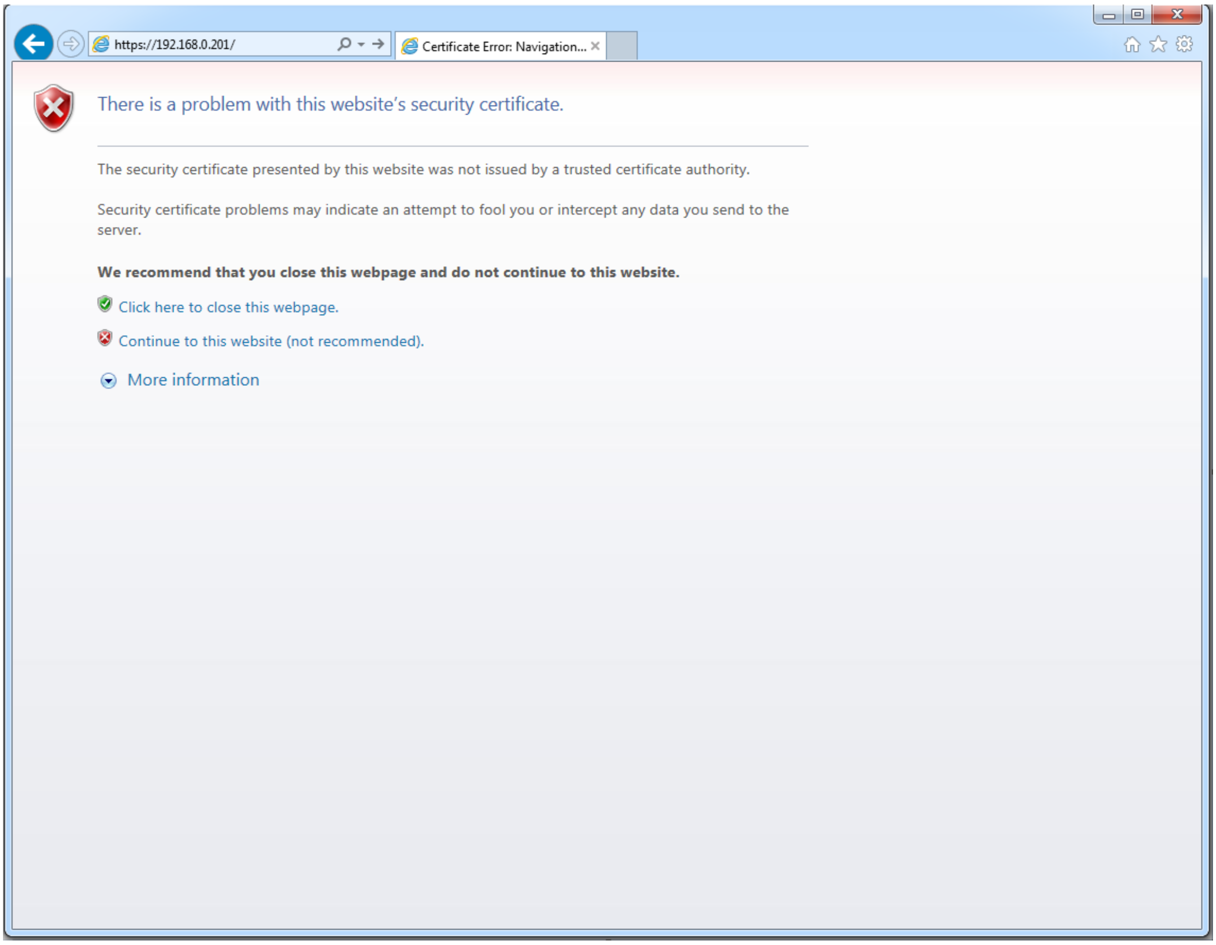
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.3.0.4 - **Appliance**

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.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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

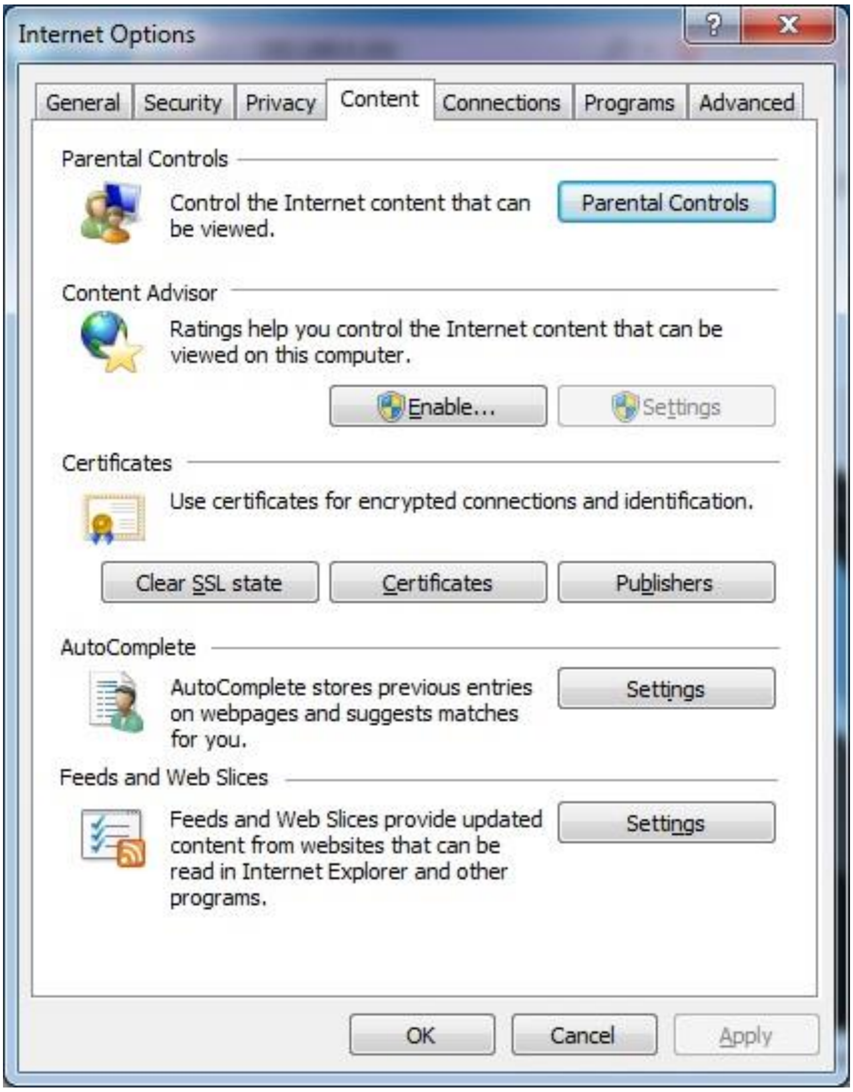
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

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.



Control the Internet content that can be viewed.

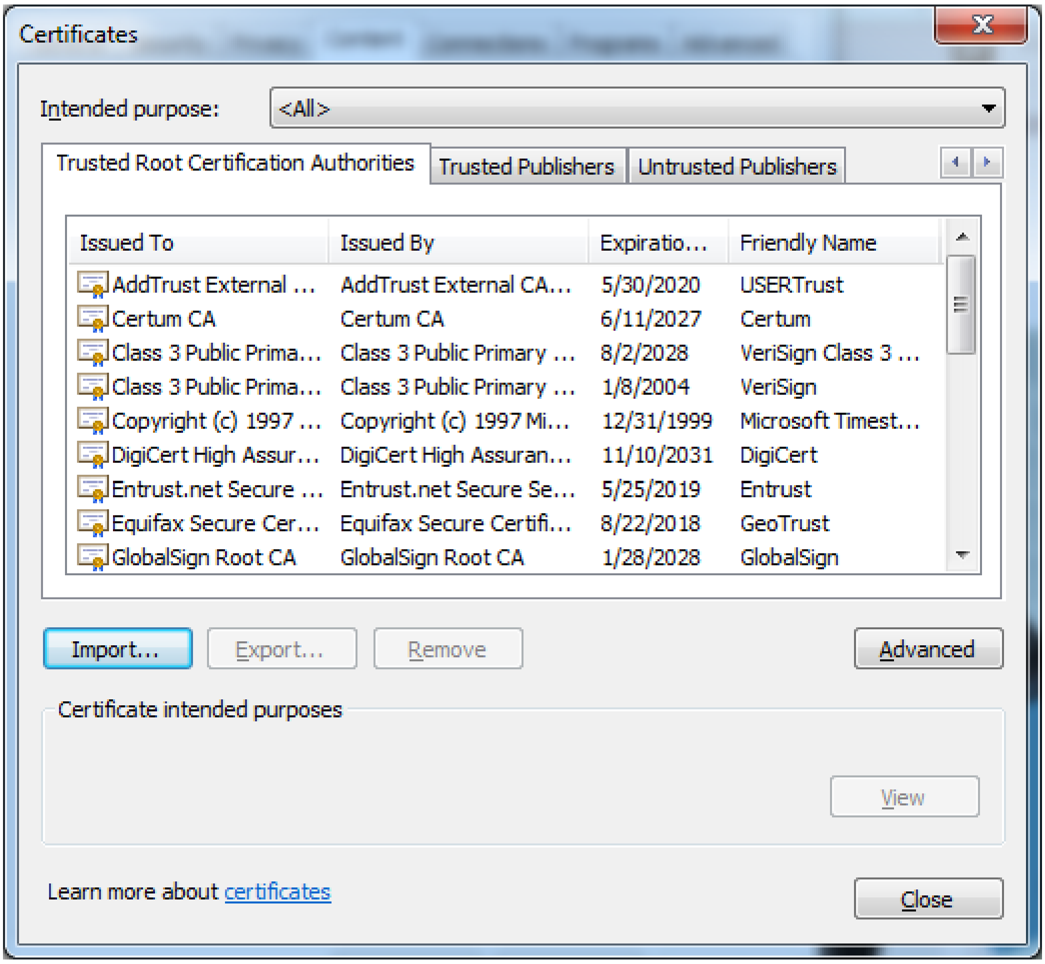
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.

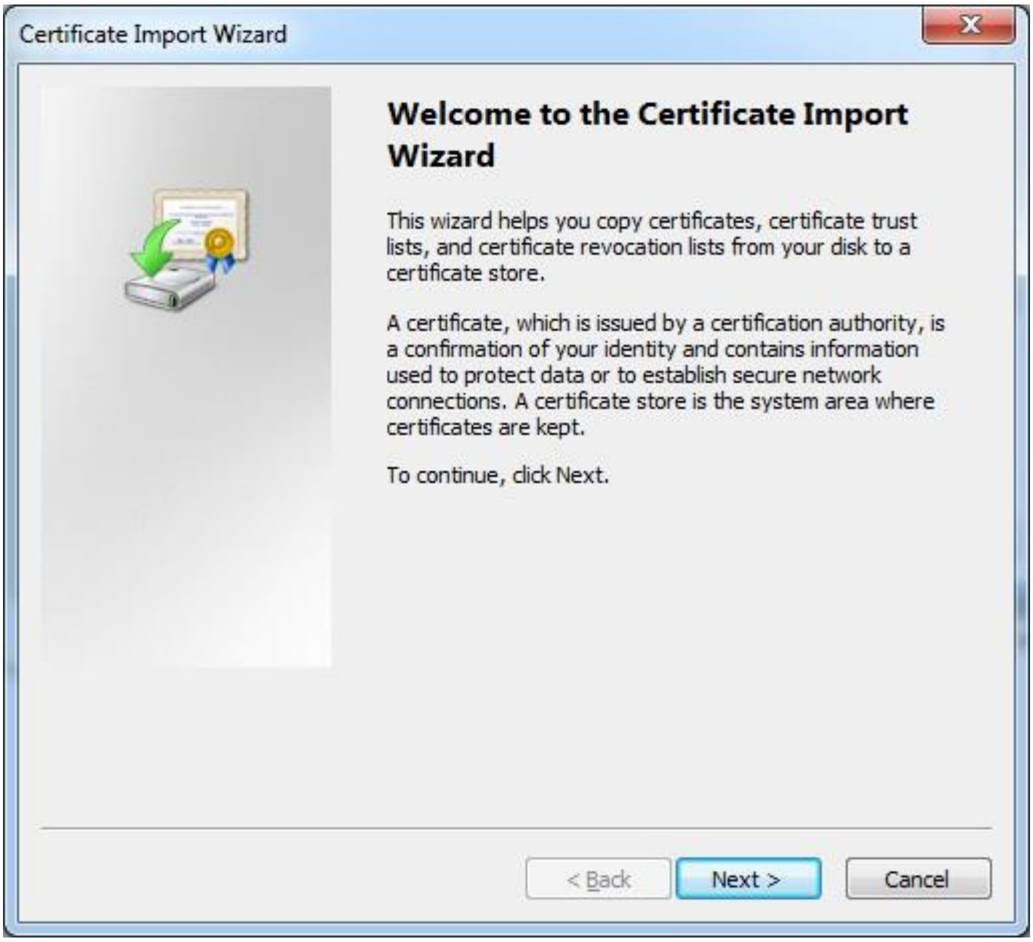
From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.


Certificates
Trusted Root Certification Authorities
Trusted Publishers
Untrusted Publishers
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Learn more about certificates
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	5/30/2020	USERTrust
Certum CA	Certum CA	6/11/2027	Certum
Class 3 Public Prima...	Class 3 Public Primary ...	8/2/2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	1/8/2004	VeriSign
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/31/1999	Microsoft Timest...
DigiCert High Assur...	DigiCert High Assuran...	11/10/2031	DigiCert
Entrust.net Secure ...	Entrust.net Secure Se...	5/25/2019	Entrust
Equifax Secure Cer...	Equifax Secure Certifi...	8/22/2018	GeoTrust
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	GlobalSign

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



Certificate Import Wizard

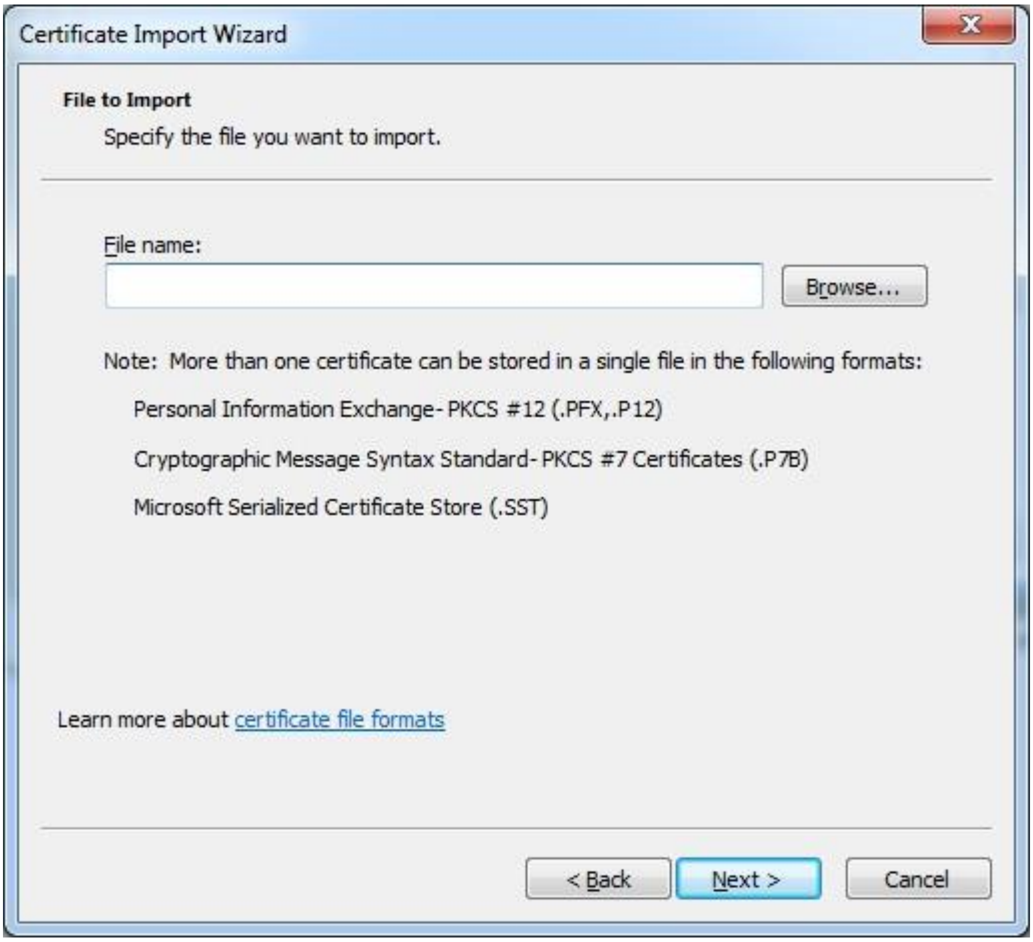
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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:

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

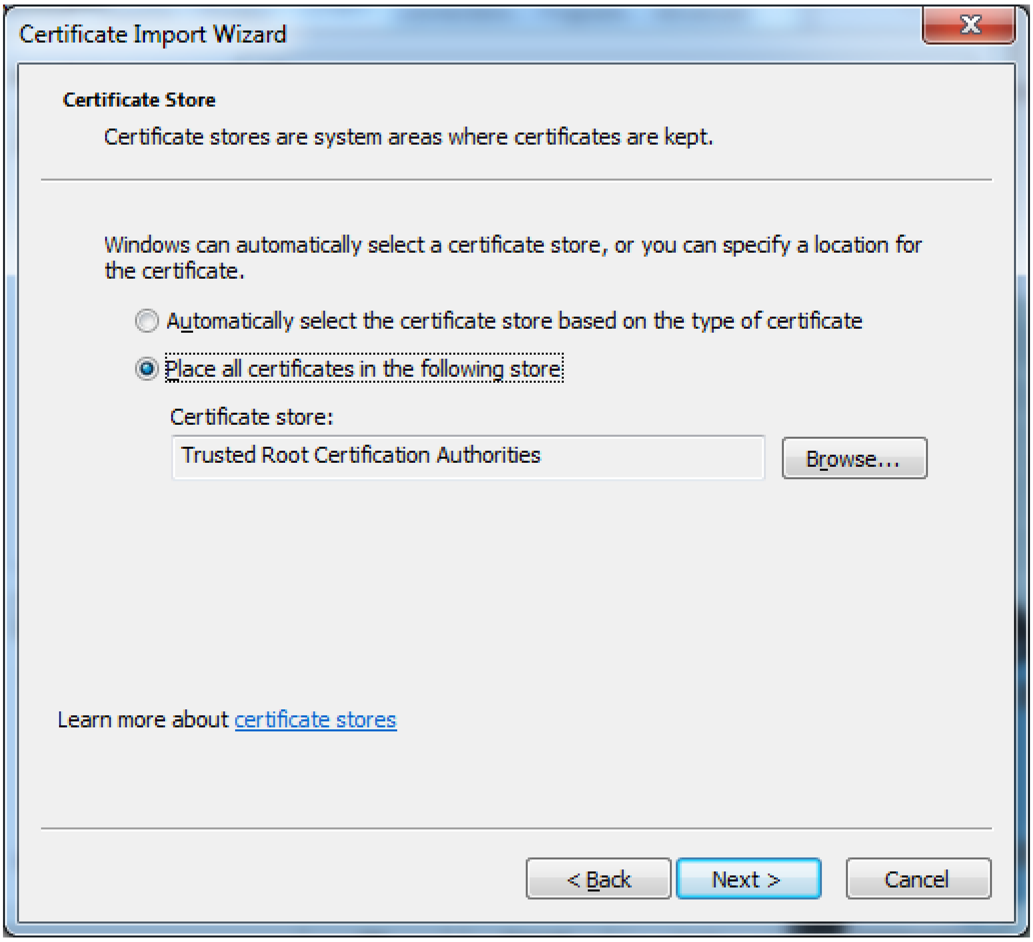
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

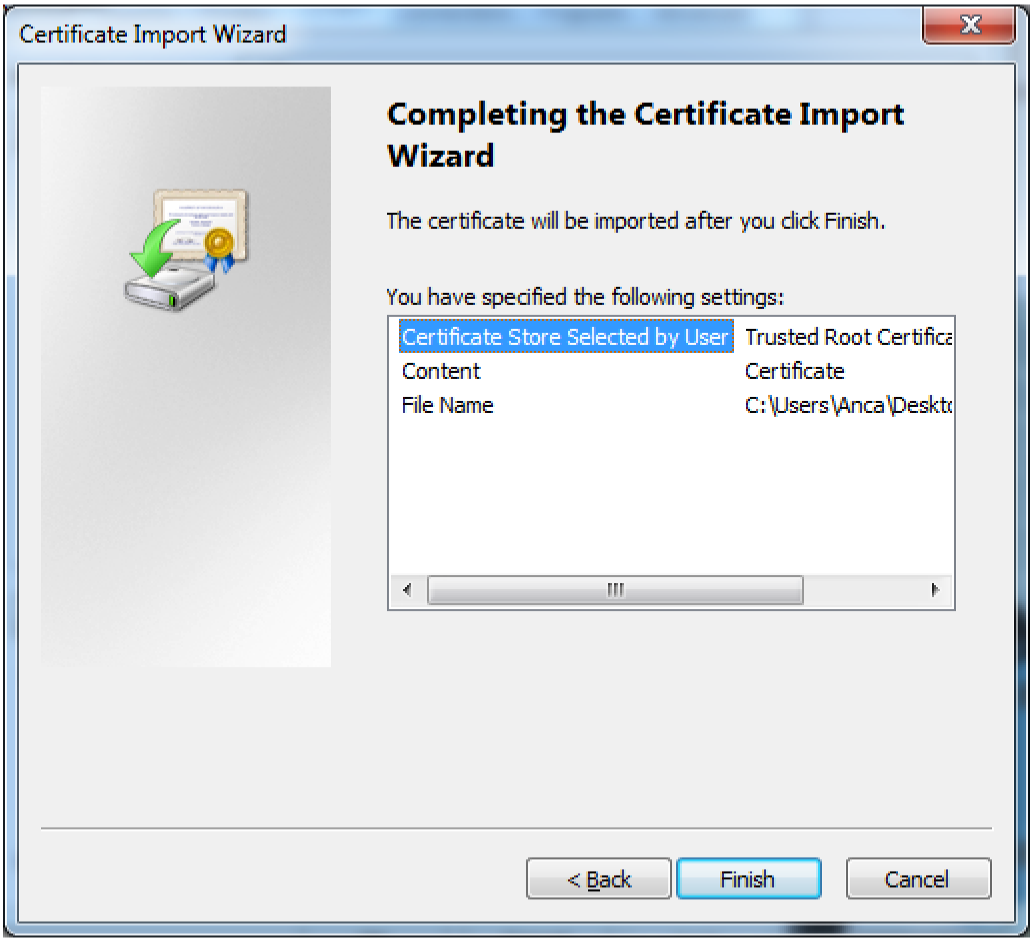
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Learn more about certificate stores

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



Certificate Import Wizard

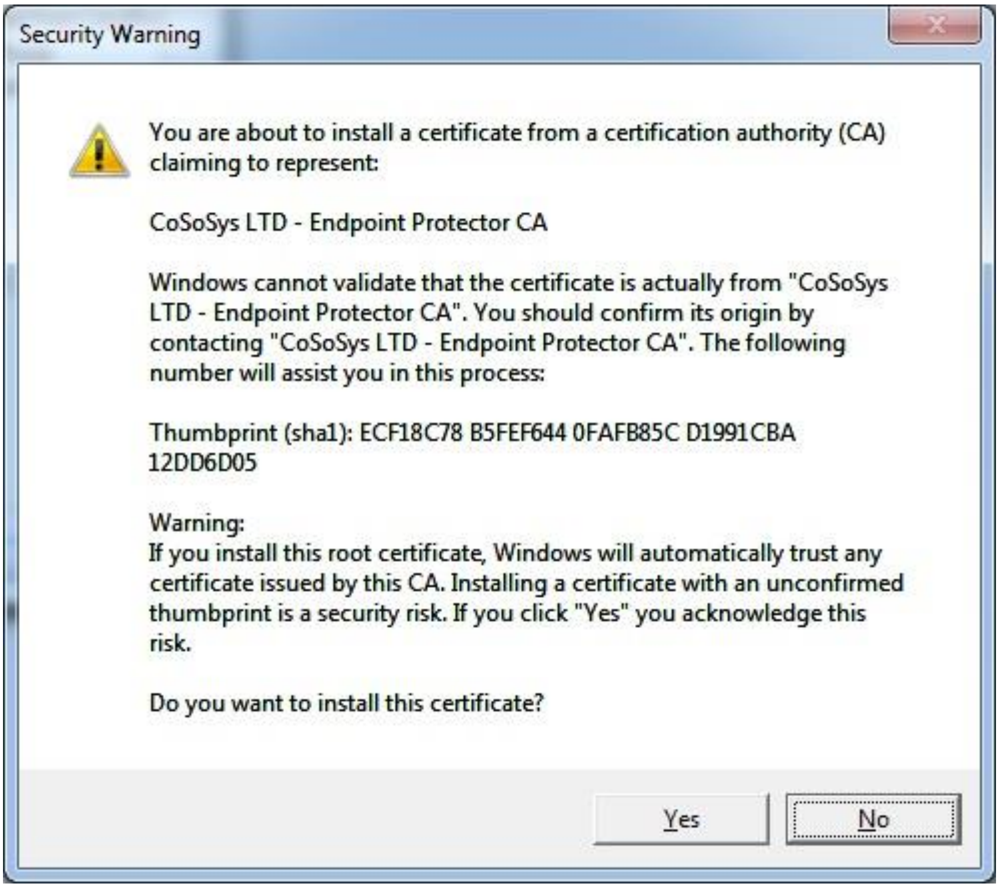
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate
File Name	C:\Users\Anca\Deskt

A Security Warning window pops up. Just click “Yes”.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CoSoSys LTD - Endpoint Protector CA

Windows cannot validate that the certificate is actually from "CoSoSys LTD - Endpoint Protector CA". You should confirm its origin by contacting "CoSoSys LTD - Endpoint Protector CA". The following number will assist you in this process:

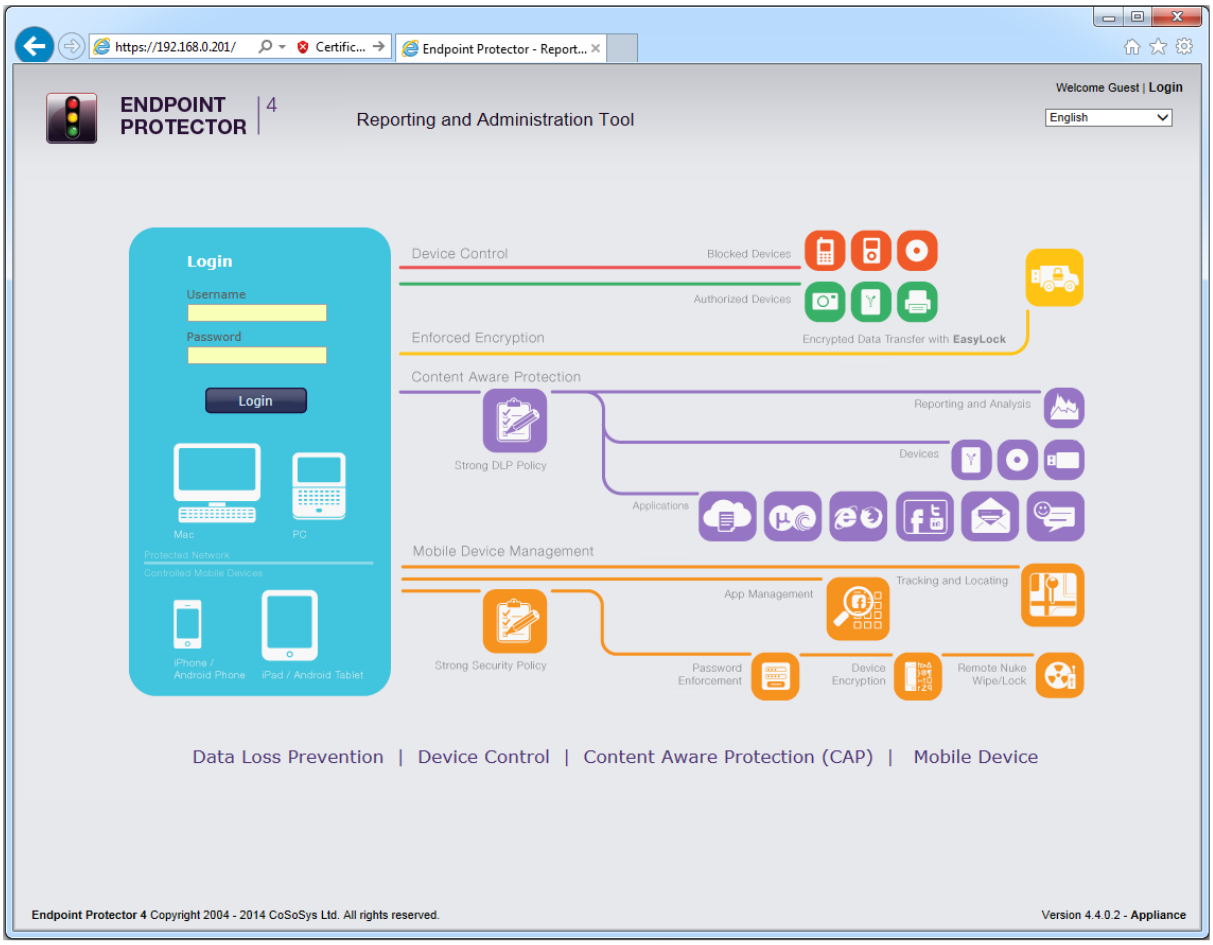
Thumbprint (sha1): ECF18C78 B5FEF644 0FAFB85C D1991CBA 12DD6D05

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

You have now successfully installed the Certificate.

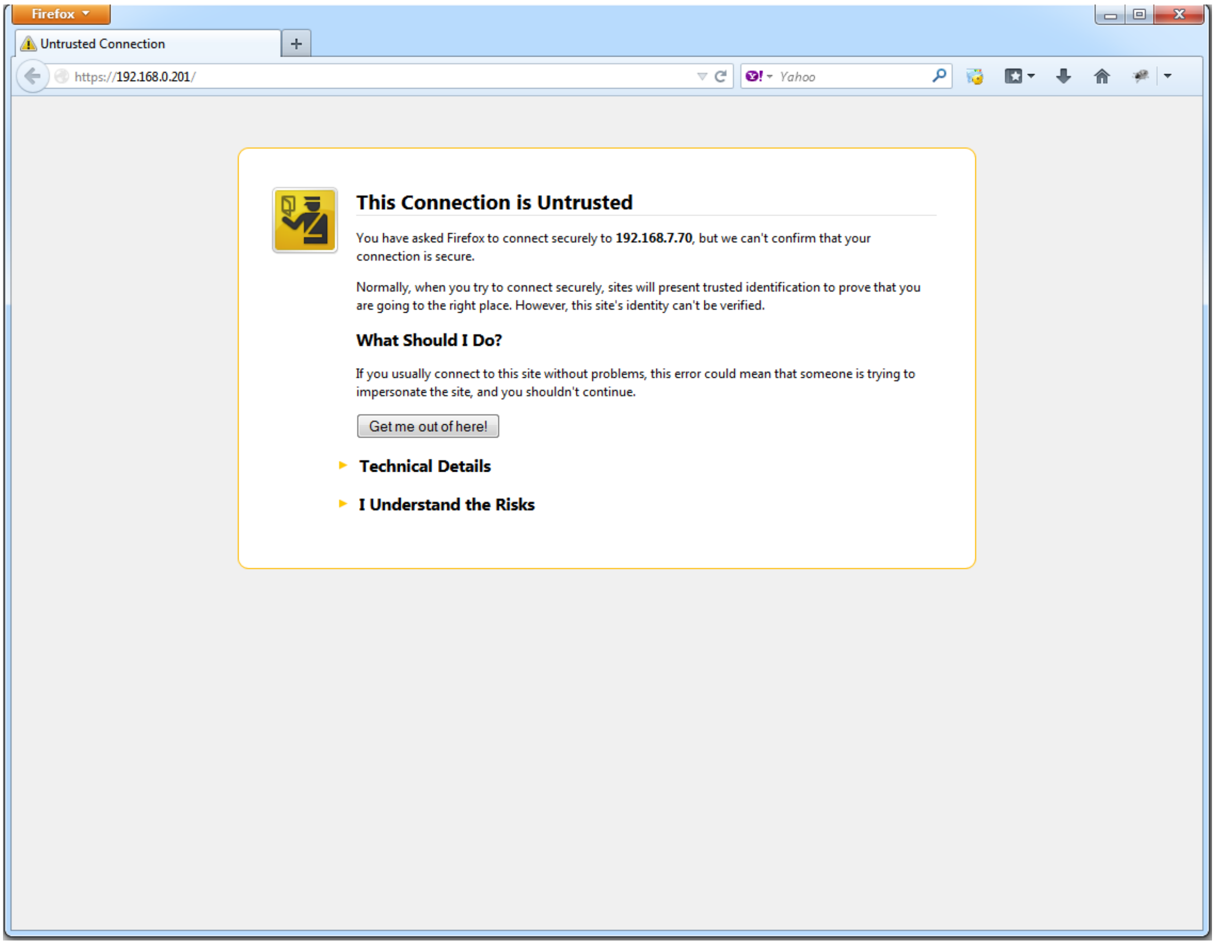
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



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).



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.7.70**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

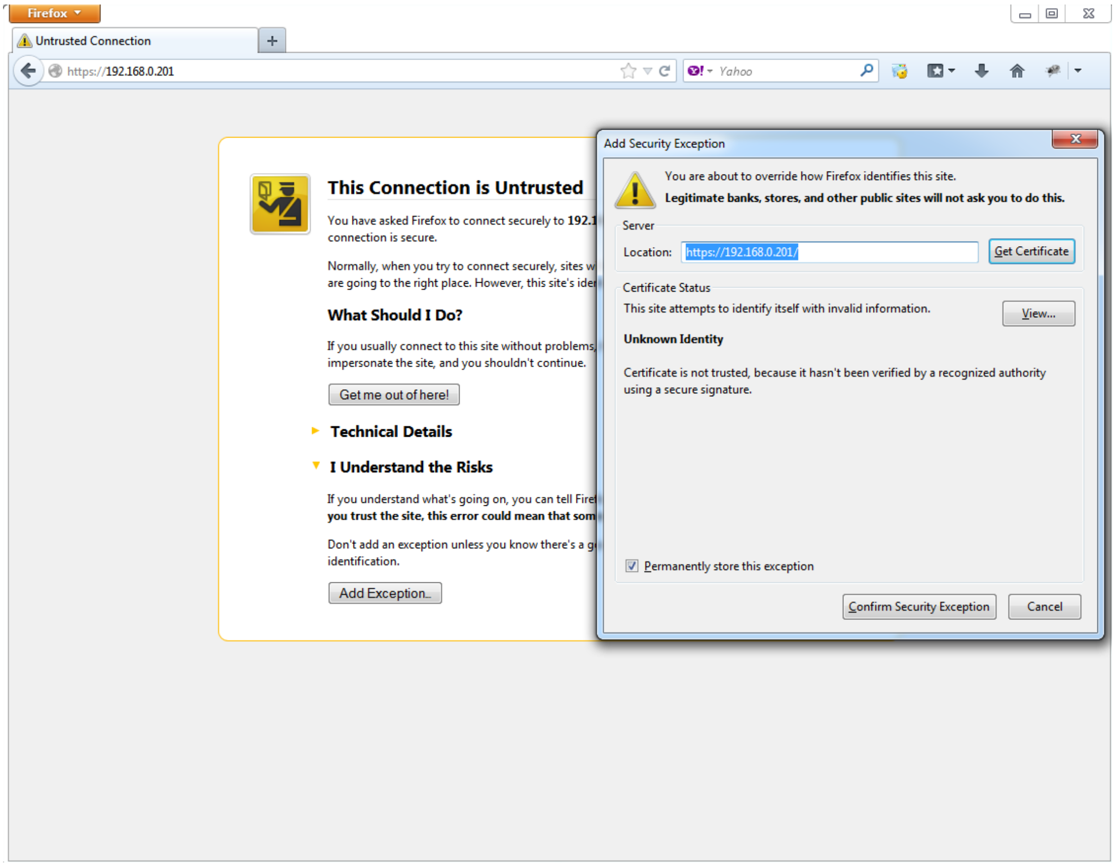
▸ **Technical Details**

▸ **I Understand the Risks**

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.



This Connection is Untrusted

You have asked Firefox to connect securely to 192.1
connection is secure.

Normally, when you try to connect securely, sites w
are going to the right place. However, this site's ide

What Should I Do?

If you usually connect to this site without problems,
impersonate the site, and you shouldn't continue.

Get me out of here!

Technical Details

I Understand the Risks

If you understand what's going on, you can tell Fire
you trust the site, this error could mean that som

Don't add an exception unless you know there's a g
identification.

Add Exception...

Add Security Exception

You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://192.168.0.201/ Get Certificate

Certificate Status

This site attempts to identify itself with invalid information. View...

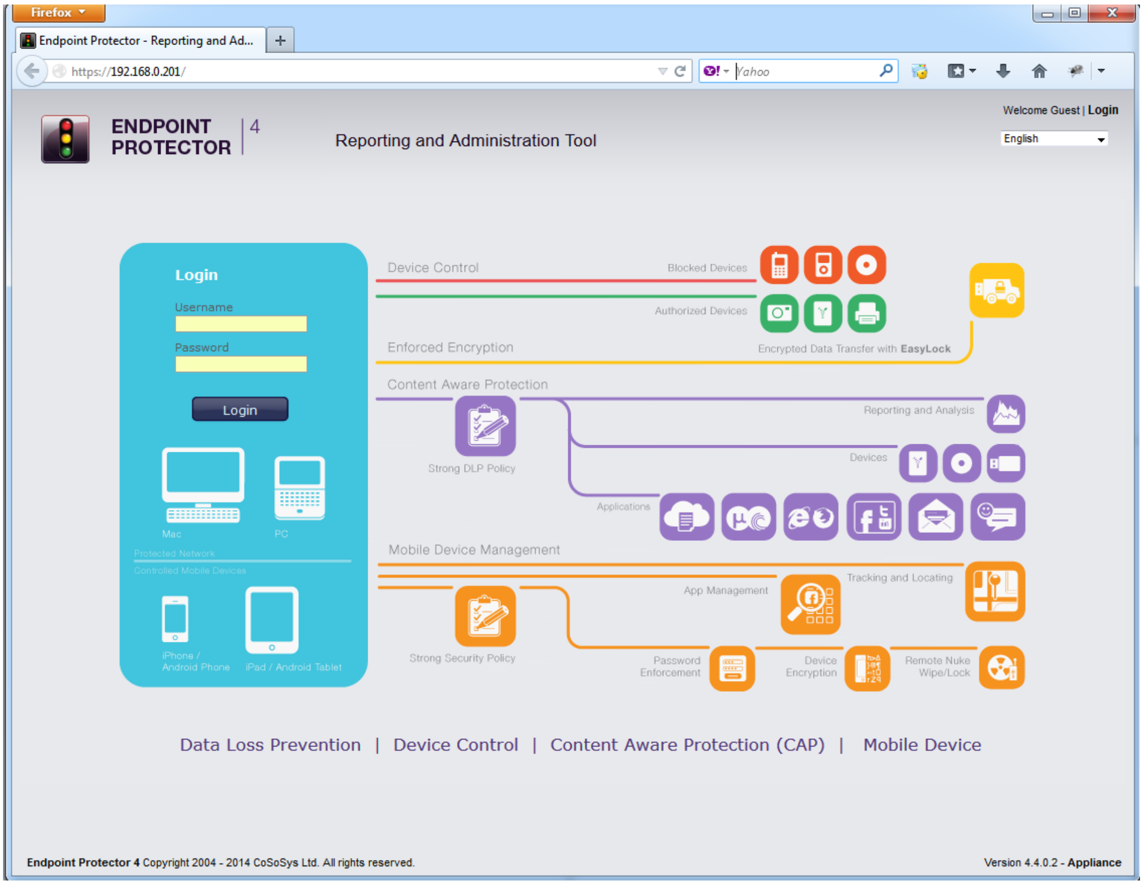
Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☑ Permanently store this exception

Confirm Security Exception Cancel

Close the browser and start it again.



Reporting and Administration Tool

Data Loss Prevention | Device Control | Content Aware Protection (CAP) | Mobile Device

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.

Version 4.4.0.2 - **Appliance**

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

6. Important Notice / Disclaimer

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.