



# ENDPOINT PROTECTOR

User Manual for Version 4.5.0.1

# User Manual



## Table of Contents

<b>1. Introduction</b>	<b>1</b>
1.1. What is Endpoint Protector?	2
1.2. Main Features	4
1.2.1. Centralized web based Device Management / Dashboard	4
1.2.2. Control your data flow: File Tracing / File Shadowing	4
1.2.3. Audit Trail – Device Activity Logging	5
1.2.4. Audit Trail – Reporting and Analysis Tools	5
1.2.5. Sensitive Content Filtering	5
1.2.6. File Whitelist	5
1.2.7. Easy Enforcement of Your Security Policies	5
1.2.8. Network "Offline" Mode to Support Your Field Employees	5
1.2.9. Enforced Encryption - protecting sensitive data in transit / Trusted Device	6
1.2.10. Client Uninstall Protection	6
1.2.11. Client Stop Protection / Tamper Protection	6
1.2.12. Backup Scheduler	6
1.3. Controlled Device Types / Ports	7
1.4. Conclusions	9
<b>2. Server Functionality / Server Components</b>	<b>10</b>
2.1. Endpoint Protector – Web Service	11
2.2. Administration and Reporting Tool	11
2.3. Accessing the Administration and Reporting Tool	14
2.4. Login Credentials (Username and Password)	15
2.5. General Dashboard	15
2.6. System Status	16
2.7. Live Update	17
<b>3. Endpoint Management</b>	<b>19</b>
3.1. Devices	19
3.2. Device Functionality	20
3.2.1. Give / Deny Access to Devices	21
3.2.2. Enable Device Read-Only Access	23
3.2.3. TrustedDevice Level 1 to Level 4	23

3.2.4. WiFi - Block if wired network is present.....	23
3.3. Computers .....	24
3.4. Groups .....	25
3.5. Users .....	26
3.6. Custom Classes .....	27
3.7. Terminal Servers and Thin Clients .....	31
3.7.1. Initial Configuration.....	31
<b>4.Endpoint Rights .....</b>	<b>34</b>
4.1. Device Rights .....	35
4.2. User Rights .....	36
4.3. Computer Rights.....	37
4.4. Group Rights .....	38
4.5. Global Rights.....	39
4.6. Effective Rights.....	40
4.7. File Whitelist .....	40
<b>5.Offline Temporary Password .....</b>	<b>42</b>
5.1. Generating the Offline Temporary Password .....	43
5.2. Using the Offline Temporary Password to authorize a device	44
5.3. Setting the Administrator Contact Information .....	44
<b>6.Endpoint Settings.....</b>	<b>45</b>
6.1. Computer Settings .....	46
6.2. Group Settings .....	47
6.3. Global Settings .....	47
6.4. Custom Client Notifications .....	48
6.5. File Tracing .....	49
6.6. File Shadowing .....	50
<b>7.Content Aware Protection .....</b>	<b>51</b>
7.1. Activation of Content Aware Protection .....	52
7.2. Content Aware Policies .....	53
7.2.1. Creating new policies.....	54
7.2.2. Predefined policies .....	55

7.2.3.	Priorities for Content Aware Policies.....	55
7.2.4.	How Content Aware Policies Work .....	56
7.2.5.	Setting up Content Aware Policies .....	57
7.2.6.	The Threshold Number .....	62
7.3.	File Size Threshold .....	63
7.4.	Custom Content Dictionary Blacklists.....	63
7.5.	Custom Content Filename Blacklists .....	64
7.6.	Content Aware URL Whitelists.....	65
7.7.	Content Aware File Whitelists .....	66
7.8.	Content Aware Domain Whitelists .....	67
7.9.	Network Share Whitelists .....	67
7.10.	Content Aware Regex Blacklists .....	68
7.11.	Content Aware Type Whitelist.....	69
7.12.	Content Aware File Location Whitelist .....	70
7.13.	Content Aware File Location Blacklist.....	71
7.14.	How Content Aware Protection works for monitored Applications / Online Services .....	72
7.15.	HIPAA compliant Content Aware Protection .....	73
7.15.1.	How Endpoint Protector is HIPAA compliant.....	73
7.15.2.	Use Case Nr. 1.....	74
7.15.3.	Use Case Nr. 2.....	75
<b>8.</b>	<b>Reports and Analysis .....</b>	<b>77</b>
8.1.	Logs Report.....	78
8.2.	File Tracing .....	79
8.3.	File Shadowing .....	80
8.4.	Content Aware Report .....	81
8.5.	Content Aware File Shadowing.....	82
8.6.	Admin Actions .....	83
8.7.	Online Computers .....	84
8.8.	Online Users.....	84
8.9.	Online Devices.....	86
8.10.	Computer History.....	87

8.11. User History .....	88
8.12. Device History .....	89
8.13. Statistics.....	90
<b>9. Alerts .....</b>	<b>91</b>
9.1. Define System Alerts .....	93
9.2. Define Alerts (Device Control Alerts) .....	95
9.3. Define Content Aware Alerts.....	96
9.4. Define MDM Alerts .....	97
9.5. System Alerts History .....	98
9.6. Alerts History .....	99
9.7. Content Aware Alerts History .....	100
9.8. MDM Alerts History.....	101
<b>10. Directory Services .....</b>	<b>102</b>
10.1. Active Directory Import .....	102
10.2. Active Directory Sync .....	105
<b>11. Appliance .....</b>	<b>109</b>
11.1. Server Information.....	109
11.2. Server Maintenance .....	110
11.2.1. Time Zone Settings .....	110
11.2.2. Network Settings .....	111
11.2.3. Reset Appliance to Factory Default .....	111
11.2.4. SSH Server .....	111
11.3. SIEM Integration.....	111
<b>12. System Maintenance .....</b>	<b>114</b>
12.1. File Maintenance .....	114
12.2. System Snapshots .....	115
12.3. Log Backup .....	117
12.3.1. Backup Scheduler (Automatic Log Backup).....	118
12.4. Content Aware Log Backup.....	119
12.4.1. Automatic Scheduler (Automatic CAP Log Backup) .....	120
12.5. Audit Log Backup .....	121

12.5.1. Audit Log Backup Scheduler .....	122
12.6. External Storage .....	123
12.6.1. FTP Server .....	123
12.6.2. Samba / Network Share .....	124
12.6.3. From the Web Interface .....	125
12.6.4. From the Console .....	128
<b>13. System Configuration .....</b>	<b>130</b>
13.1. Client Software .....	130
13.2. Client Software Upgrade .....	131
13.3. Client Uninstall .....	132
13.4. System Administrators .....	133
13.5. System Departments .....	135
13.6. System Security / Client Uninstall Protection .....	137
13.7. System Security .....	138
13.8. System Settings .....	139
13.8.1. Rights Functionality .....	139
13.8.2. Proxy Settings .....	139
13.9. System Licensing .....	140
13.9.1. Appetizer Mode .....	142
13.9.2. Trial Mode .....	143
13.9.3. Import Licenses .....	143
<b>14. System Parameters .....</b>	<b>146</b>
14.1. Device Types .....	146
14.2. Rights .....	148
14.3. Events .....	149
14.4. File Types .....	150
<b>15. Setting up Policies .....</b>	<b>151</b>
<b>16. Modes for Users, Computers and Groups</b>	<b>153</b>
16.1. Transparent Mode .....	154
16.2. Stealth Mode .....	154
16.3. Panic Mode .....	154

16.4. Hidden Icon Mode .....	155
16.5. Silent Mode .....	155
15.6. Adding new administrator(s) .....	156
16.7. Working with logs and reports .....	158
<b>17. Enforced Encryption with Trusted Devices</b>	
<b>159</b>	
17.1. Managing Trusted Devices from Endpoint Protector .....	160
17.2. Trusted Device Level 1 and Enforced Encryption with EasyLock	161
17.2.1. Deploying EasyLock.....	161
17.2.2. EasyLock Enforced Encryption Settings and Clients.....	162
17.2.3. File Tracing on EasyLock Trusted Devices.....	164
<b>18. Endpoint Protector Client .....</b>	<b>165</b>
18.1. Endpoint Protector Client Installation .....	165
18.2. Endpoint Protector Client Security .....	166
18.3. Client Notifications (Notifier) .....	167
18.4. Client Policy Update .....	167
18.5. Offline Functionality for Endpoint Protector Client.....	168
18.6. DHCP / Manual IP address.....	168
18.7. Client Removal .....	168
18.7.1. Client Removal on Windows OS .....	168
18.7.2. Client removal on MAC OS X.....	168
18.7.3. Client removal on Linux OS .....	168
<b>19. Installing Root Certificates to your Internet</b>	
<b>Browser .....</b>	<b>169</b>
19.1. For Microsoft Internet Explorer .....	169
19.2. For Mozilla Firefox .....	178
<b>20. Terms and Definitions .....</b>	<b>180</b>
20.1. Server Related.....	180
20.2. Client Related.....	181
<b>21. Support .....</b>	<b>183</b>

22. Important Notice / Disclaimer..... 184



# 1. Introduction

Portable storage devices such as USB flash drives, external HDDs, digital cameras and MP3 players/iPods are virtually everywhere and are connected to a Windows PC, Macintosh or Linux computer via plug and play within seconds.

With virtually every Windows, Mac or Linux workstation having easily accessible USB, FireWire and other ports, the theft of data or accidental loss of data is for individuals a mere child's play.

Data theft or data loss or infecting companies' computers or network through a simple connection is easy and doesn't take more than a minute. Network administrators have little chance to prevent this from happening or to catch the responsible user(s). Now Endpoint Protector, through its Device Control module, helps companies to stop these threats.

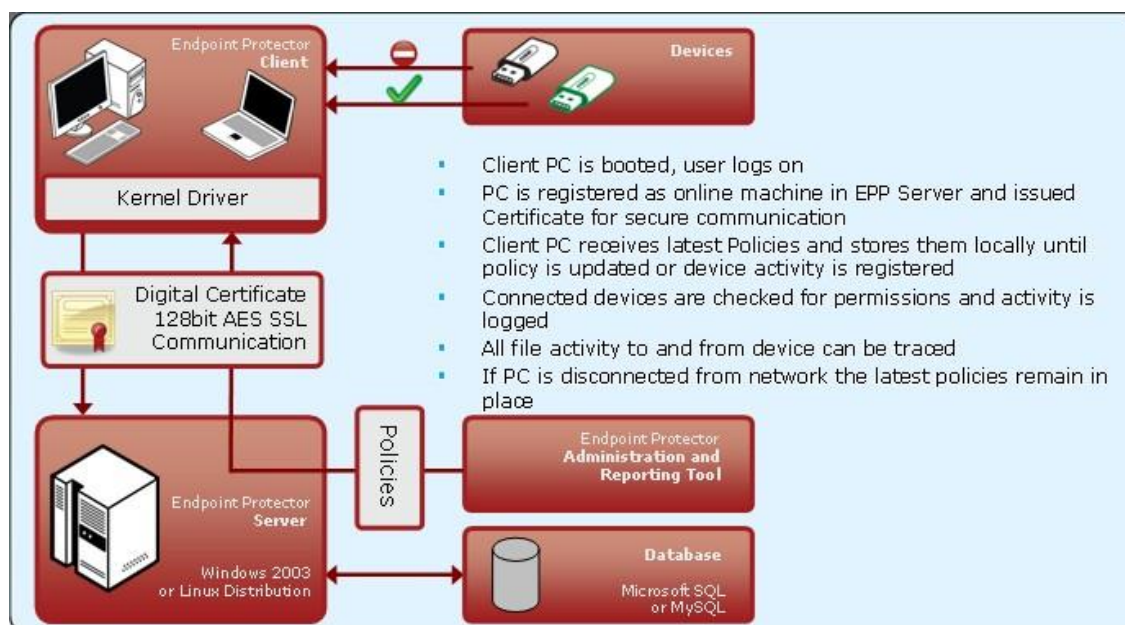
As a complete Data Loss Prevention solution, Endpoint Protector not only controls all device activity at endpoints, but monitors and scans all possible exit points for sensitive content detection. Its second module, Content Aware Protection, ensures that no critical business data leaves the internal network either by being copied on devices or sent via the Internet without authorization, reporting all sensitive data incidents.

## 1.1. What is Endpoint Protector?

Endpoint Protector will help you secure your PCs endpoints within your network and screen all possible exit ways for sensitive content detection. You will be able to restrict the use of both internal and external devices which can be used for data storage and transfer and to manage Windows Mac and Linux ports.

Endpoint Protector, through its two main modules, Device Control and Content Aware Protection gives network administrators the control needed to keep network endpoints safe:

- Control use of all USB and other storage devices
- Tracking of what data is saved to storage devices
- Tracking of what data is copied from and to storage devices
- Scanning of all data transfers for sensitive content detection
- Complete monitoring of all possible data exit points
- Authorize the use of USB storage devices
- Securing data on USB storage devices
- Powerful reporting tool and audit



The modular and intuitive Web-based administration interface has been designed to offer fast access to controlling computer, devices and user behavior in a large network. It also offers several ways to track any kind of portable device related activity registered on the system. A detailed report including timestamps, file

names, action(s) taken, logged user, etc. allows for pin-pointing malicious behavior and users.

The system's design also allows the CoSoSys team to perform easy customizations and extensions requested by clients. Better automation and express reports can be developed accordingly to customer demands. In the same time this structure is easy to update and maintain, making the usability even greater.

Endpoint Protector is the only solution that gives companies of any size the ability to let users take advantage of the increasingly important functionality of USB and other ports without losing control over data and compliance.

This endpoint security device control solution is designed to control usage of all portable storage and to keep track of what data users are taking from and to their work computers on any kind of portable storage devices.

Furthermore, Endpoint Protector enables network administrators to monitor and report what data is introduced into the corporate network from a portable storage device such as prohibited materials (MP3s, movies or games) or harmful data like a virus that could jeopardize the networks integrity.

As not all portable storage devices are used with the intent to harm the company, many legitimate reasons commonly justify the need of such devices to increase network users' productivity. Thus, Endpoint Protector allows authorized use of certain device types or specific devices such as the companies' own USB Flash Drives to handle and transfer confidential data.

To ensure the protection of data carried by users on authorized devices, the Endpoint Protector administrator can allow users to copy work data only to a password protected / encrypted area of an authorized device, a so called "Trusted Device". In this way confidential corporate data is protected in case of hardware loss.

Endpoint Protector creates an audit trail that shows the use and activity of portable storage devices in corporate networks. Thus, administrators have the possibility to trace and track file transfers through endpoints and then use the audit trail as legal evidence for data theft. For more details on Endpoint Protector, please see the Data Sheet available on the company's website.

<http://www.EndpointProtector.com>

## 1.2. Main Features

Your confidential sensitive data is only as safe as your endpoints are. Designed for medium and large enterprises, Endpoint Protector offers powerful features in order to control, monitor and enforce network and endpoint security.

Endpoint Security for Windows, Macintosh and Linux Workstations, Notebooks and Netbooks.

Endpoint Protectors full feature set is available for Windows. A reduced feature set is available for Macintosh (OS X) and Linux - Ubuntu 10.04 LTS and openSUSE 11.4.

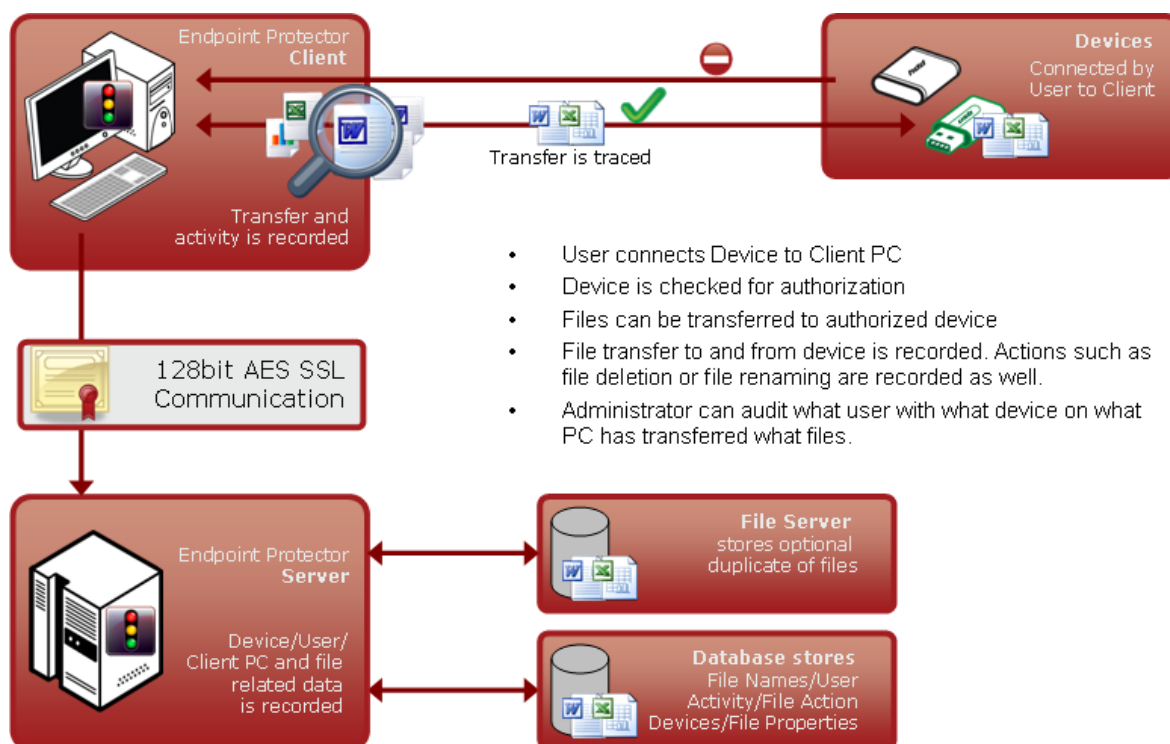
Protects PCs from threats posed by removable portable storage and endpoint devices like USB Flash Drives, MP3 Players, iPods, digital cameras and other devices that could be intentionally or accidentally used to leak, steal, lose, virus or malware infect your data. Even self-executing devices like a USB Flash Drive with a CD-ROM autorun feature such as U3 Drives will not be accessible and thereby pose no threats.

### 1.2.1. Centralized web based Device Management / Dashboard

Network administrators have the ability to centrally manage and authorize the use of devices. The Endpoint Protector 4 Dashboard is designed to meet the needs of both management and security staff and offer access to real-time information, charts and reports about organization wide controlled device and data transfer activity. All in an integrated single view and Web based Administration and Reporting Tool.

### 1.2.2. Control your data flow: File Tracing / File Shadowing

This thorough record of information streams at the network's endpoints is supporting audits of data flow and controlling the impact of data leakage. The File Tracing feature will track all data that was copied to and from prior authorized portable storage devices. The File Shadowing feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.



### 1.2.3. Audit Trail – Device Activity Logging

A device activity log is recorded for all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

### 1.2.4. Audit Trail – Reporting and Analysis Tools

Endpoint Protector 4 is equipped with powerful reporting and analysis tools to make the data audit process easy and straightforward.

### 1.2.5. Sensitive Content Filtering

Scans and reports all transfers of sensitive data on and from any removable media or via the Internet.

### 1.2.6. File Whitelist

Allows only previously authorized files to be copied to portable storage devices.

### 1.2.7. Easy Enforcement of Your Security Policies

Simplified device management policies with customizable templates for defining User Group permissions allow easy enforcement and maintenance of your latest security policies across your network.

### 1.2.8. Network "Offline" Mode to Support Your Field Employees

"Offline Temporary Password" to allow time limited access to a specific device or to file transfers, when the client computer is disconnected from the network.

Protected computers that are temporary or frequently disconnected from the network stay protected based on the last locally saved policy. All notifications are transmitted at the next network connection.

### 1.2.9. Enforced Encryption - protecting sensitive data in transit / Trusted Device

The technology behind Trusted Devices is designed to certify that in the corporate environment all the endpoint devices are not only authorized and controlled via endpoint software and security policies but also certified and trusted for protecting sensitive and confidential data in transit (in case of a Trusted Device). This will assure that in the event a device is stolen or lost all the data stored on it is encrypted and therefore not accessible for other parties.

### 1.2.10. Client Uninstall Protection

Endpoint Protector 4 offers a password-based solution that prevents the users from uninstalling the Endpoint Protector Clients, thus ensuring continuous data protection.

### 1.2.11. Client Stop Protection / Tamper Protection

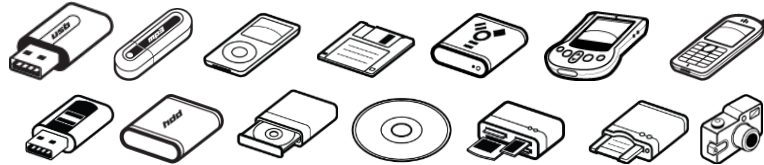
Endpoint Protector 4 prevents users from stopping the Endpoint Protector Clients at any time.

### 1.2.12. Backup Scheduler

Endpoint Protector 4 provides an automatic log backup solution in order to prevent the server from overloading.

## 1.3. Controlled Device Types / Ports

Endpoint Protector supports a wide range of device types which represent key sources of security breaches. These devices can be authorized which makes it possible for the users to view, create or modify their content and for administrators to view the data transferred to and from the authorized devices.



- Removable Storage Devices
  - Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
  - USB 1.1, USB 2.0, USB 3.0
  - Wireless USB
  - LPT/Parallel ports
    - By controlling the Parallel ports of a PC using Endpoint Protector, the network administrator can deny or allow users access to storage devices connected to these ports.
    - \* APPLIES ONLY TO STORAGE DEVICES
  - Floppy disk drives
    - Access to floppy disk drives can be managed through Endpoint Protector and can be turned on/off completely.
  - Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.
    - These devices can be enabled / disabled via Endpoint Protector.
  - Card Readers - internal and external
    - These devices can be enabled / disabled via Endpoint Protector.
  - CD/DVD-Player/Burner - internal and external
    - These devices can be enabled / disabled via Endpoint Protector.
  - Digital Cameras
    - These devices can be enabled / disabled via Endpoint Protector.

- **Smartphones / Handhelds / PDAs**  
This category includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.
- **iPods / iPhones / iPads**  
These devices can be enabled / disabled via Endpoint Protector.
- **MP3 Player / Media Player Devices**  
These devices can be enabled / disabled via Endpoint Protector.
- **External HDDs / portable hard disks**  
These devices can be enabled / disabled via Endpoint Protector.
- **FireWire Devices**  
These devices can be enabled / disabled via Endpoint Protector.
- **PCMCIA Devices**  
These devices can be enabled / disabled via Endpoint Protector.
- **Biometric Devices**  
These devices can be enabled / disabled via Endpoint Protector.
- **Bluetooth**  
These devices can be enabled / disabled via Endpoint Protector.  
For Mac OS X, a more granular way to manage Bluetooth devices is also available, providing the option to enable / disable Smartphones, Tablets, Keyboards, Mice and Others.
- **Printers**  
Applies to serial, USB and LPT connection methods. These devices can be enabled / disabled via Endpoint Protector.
- **ExpressCard (SSD)**  
These devices can be enabled / disabled via Endpoint Protector.



## 1.4. Conclusions

As information theft and data leakage are a reality of today's business world, effectively preventing all possible security breaches is becoming an ultimate concern for enterprise security experts. Endpoint security comes to complete your existing security policies, aiming to render it full proof.

As new circumvention and data compromising techniques come to diminish the benefits of new devices and gadgets, Endpoint Protector secures your company's technologically enabled mobility. Thus, by easily protecting all exposed endpoints from inbound and outbound threats, you can enjoy enhanced portability, efficiency and productivity.

As it enables your employees to use devices you have already invested in and it protects your company from losses generated by attacks from outside and within, all financial costs entailed by implementing Endpoint Protector, such as purchase, implementation and usage training expenses, are fully justified by the yielded return on investment.

## 2. Server Functionality / Server Components

The functionality is designed to be around several physical entities:

- Computers (PCs, MACs and Linux workstations with Endpoint Protector Client installed)
- Devices (the devices which are currently supported by Endpoint Protector. e.g.: USB devices, digital photo cameras, USB memory cards etc)
- Client user (the user who will use the devices and the computers)

The server side of Endpoint Protector has different parts working close together:

- Web Service – responsible of communicating with the clients and storing the information received from them
- The Administration and Reporting Tool – responsible for managing the existing devices, computers, users, groups and their behavior in the entire system
- Endpoint Protector Appliance Hardware (Only applies if you have purchased the Endpoint Protector Hardware Appliance) – is the hardware running the Endpoint Protector Server containing Operating System, Database, etc.

## 2.1. Endpoint Protector – Web Service

The Web Service of Endpoint Protector is responsible for the communication between Endpoint Protector Server and the Client computers. Starting with the registration of the client computers, the Web Service sends the settings and rights of each computer and also receives the log information from each client and stores that information in the database.

The Web Service is started as long as the Web server is running, and it is ready to respond to each client request.

## 2.2. Administration and Reporting Tool

This part of the Server is designated as a tool for customizing the behavior of the entire system (Server and Clients) and to offer the administrator(s) (the person handling this tool) the necessary information regarding the activity on the system.

Access to this part of the Web server is restricted by a username/password pair. The users accessing the Web application are referred to as Administrator in this document. This administrator can be a regular administrator or super administrator. The difference between the two is the level of access to some administrative parts of the application. The regular administrator cannot change critical system parameters, cannot create/delete other administrators and has restricted access to some areas of Endpoint Protector.

**Dashboard** – Lets you view statistics of the server such as the number of clients and devices currently connected, total number of computers, log and shadow size, last logged action, newest added client, latest news about the product and the company, licensing status, etc. and also provides shortcuts to the essential management tools.

The screenshot displays the Endpoint Protector Reporting and Administration Tool dashboard. The interface is divided into a sidebar on the left and a main content area. The sidebar includes navigation options such as System Overview, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'System Overview' and contains several panels: 'System Information' showing system statistics (Computers total: 24/20, Devices total: 105/14), 'Recently Added' listing new devices and users, 'Latest Logs' showing a table of events (Computer, Device / Destination, User, Event), 'Latest News' with recent updates, and 'Statistics (most active)' showing active counts for Computers, Devices, and Users. The bottom of the dashboard includes copyright information and version details.

**Endpoint Management** – Used for administration of Devices, Computers, Groups, and Client Users.



In this module, the administrator can edit, manage rights and settings for or even delete devices, computers or groups. He can also create groups and add or remove client users.

**Endpoint Rights** – Used to determine and define rules of access. Six subsections are found here: Devices Rights, User Rights, Computers Rights, Group Rights, Global Rights, Effective Rights and File Whitelist.



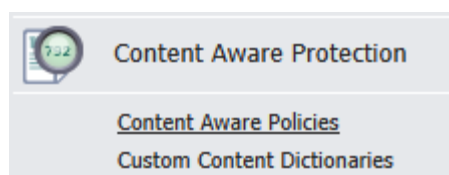
This is the most important module of Endpoint Protector. In this module the administrator can set up and enforce security policies by assigning specific rights to devices, computers, computer groups and global device access. Please refer to section 4 “Endpoint Rights” for more information.

**Endpoint Settings** – Used for setting the behavior of computers, groups of computers or all the computers.

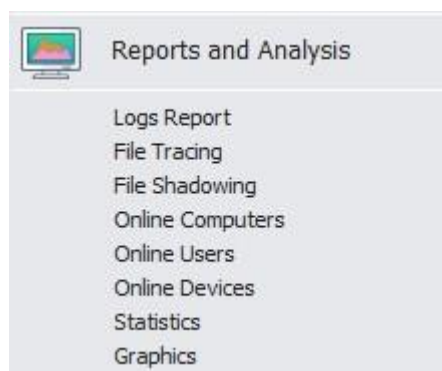


In this module the administrator can modify global settings such as the log upload interval, local log and shadow size, as well as manage computer and computer group’s settings. The functionality mode (Normal, Stealth, Transparent, etc) can also be set from here.

**Content Aware Protection** – Separate module, which allows creating and enforcing strong content aware policies for a better control of what data leaves the company network via any removable media or the Internet.

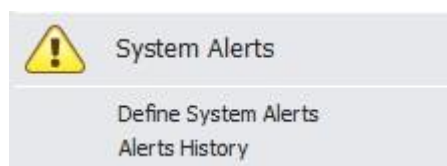


**Reports and Analysis** – Designed to offer the administrator information regarding the past and current activity on the system (Server and Clients). It includes several sections such as Online Computers, Online Users, Statistics, Graphics, etc. Several information formats are available for view and export.



Similar to the Dashboard, this module displays usage statistics on past and current activities, but with more details.

**System Alerts** – Allows the creation of System Alerts – notifications, set up by administrators, which will alert them if a certain device was connected or accessed, a certain user performed a certain action, etc. Please see paragraph 8 “Alerts” for more details.



**System Parameters** – Here you can determine the functionality of the entire system. This module includes sections such as Device and File Types, Rights and Events.



## 2.3. Accessing the Administration and Reporting Tool

To access the Administration and Reporting Tool, simply open a browser and enter the IP address of the Endpoint Protector Server, the Endpoint Protector Appliance IP or the Server Host Name.

In case you enter the IP address, please note that you must use the HTTPS (Hypertext Transfer Protocol Secure) prefix, followed by the IP address of the Endpoint Protector Server.

Example: <https://127.0.0.1/index.php>.

(In case of using the Endpoint Protector Appliance the default IP address is <https://192.168.0.201>).

If you use Internet Explorer, we recommend that you add this page to Internet Explorer’s trusted sites. To do this, follow the steps in paragraph 19 “Installing Root Certificates to your Internet Browser”.

## 2.4. Login Credentials (Username and Password)

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

**USERNAME:** root  
**PASSWORD:** epp2011

To change the username and password and to create additional administrators, please see paragraph 11.2 “System Administrators”.

## 2.5. General Dashboard

Some of the most important activities logged by EPP can be monitored under this tab. The image below is self-explanatory.

The screenshot displays the Endpoint Protector 4 Reporting and Administration Tool dashboard. The interface includes a sidebar with navigation options like Dashboard, General Dashboard, Endpoint Management, and Alerts. The main content area is titled 'Endpoint Protector - Dashboard GENERAL' and features several charts and a table.

**Endpoints and Mobile Devices:** A bar chart showing the number of devices for different operating systems: Windows (2), Mac (1), Linux (1), iOS (1), and Android (2).

**Most Active Users (# of connected devices):** A bar chart showing the number of active users for different systems: Windows (6) and Mac (2).

**Most Active Users (# of transfers blocked):** A bar chart showing the number of transfers blocked for different systems: Windows (14) and Mac (8).

**Passcode Protected Mobile Devices:** A pie chart showing the distribution of mobile devices: 67% No passcode, 33% Passcode preset, and 0% Unmanaged.

**Latest News:** A section with a news item dated 18 Nov 2013: 'Endpoint Protector releases support for OS X their network prevent data losses and data. Upgrade to our newest version if you are u...'. A 'Check all news' link is provided.

**Device Control Logs Table:**

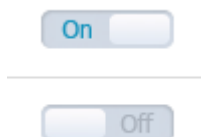
Event name	Client Computer	IP Address	Domain Name	Client User	Device Type	Device	Date/Time
Device not TD					USB Storage Device	DataTraveler 2.0	2013-12-09 13:41:28
Blocked					USB Storage Device	DataTraveler 2.0	2013-12-09 13:41:18
Connected					USB Storage Device	DataTraveler 2.0	2013-12-09 13:41:18
Disconnected					USB Storage Device	DataTraveler 2.0	2013-12-09 13:41:12
Device not TD					USB Storage Device	DataTraveler 2.0	2013-12-09 13:38:45
Blocked					USB Storage Device	DataTraveler 2.0	2013-12-09 13:38:36
Connected					USB Storage Device	DataTraveler 2.0	2013-12-09 13:38:36

Endpoint Protector 4 Copyright 2004 – 2013 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.2 - Appliance

More specific dashboards are available at Endpoint Management, Content Aware Protection and Mobile Device Management.

## 2.6. System Status

Under the System Status tab from the Dashboard module, you can access the "System Lockdown", "Endpoint Protector ON/OFF" , "Content Aware Protection ON/OFF".



**System Lockdown** - Pressing this button will cause Endpoint Protector to instantly deny access to all devices in the system, stopping also ongoing data transfers (depending on device type). Log files are still created of what was accessed or modified before the Lockdown button was pushed.

### Note!

The following device types are not blocked in the event of a System Lockdown: Wi-Fi, Keyboards, Bluetooth and USB Modems.

**Endpoint Protector ON/OFF** – Pressing this button (OFF) will stop all Endpoint Protector related activities completely. This means that all devices, even those previously blocked, will now be usable, logging of traffic will stop as well as file shadowing.

**Content Aware Protection ON/OFF** – Pressing this button (OFF) will stop all Content Aware Protection related activities completely. This means that all files that are sensitive or are containing sensitive data will not be detected and will not be reported.

The "**Re-read**" command will force all computers to re-read their rights at the next refresh interval.



## 2.7. Live Update

This section allows checking and applying the latest Endpoint Protector Server updates. Please note that this feature communicates through port 80.

The two options available are:

- Configure Live Update – allows selecting one of the two options for performing the live update check: manually or automatically and enabling or disabling the Automatic Reporting to the Live Update Server

**Live Update Settings**

Check Automatically for Updates:

Check Manually for Updates:

---

**Live Update Reporting**

**\*Note:** Endpoint Protector Server will report each night the current system status to our Live Update Server

Enable Automatic Report:

Disable Automatic Report:

- Check Now – searches for the latest Endpoint Protector Server updates.

The screenshot displays the 'Endpoint Protector Server - Live Update' page within the Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, System Overview, System Status, Live Update, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection, Mobile Device Management, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area features an 'Important Notice' about connecting over HTTPS, a 'Software Update' section showing the most recent check for updates on 24 Feb 2013 14:25:01 and updates installed on 06 Feb 2013 15:45:01, and an 'Available Updates' section indicating 'No updates available!'. Buttons for 'Configure Live Update', 'Check Now', 'Offline Patch Uploader', and 'View Applied Updates' are visible. The footer shows 'Endpoint Protector 4 Copyright 2004 - 2013 CoSeSys Ltd. All rights reserved.' and 'Ready Version 4.3.0.3 - Appliance'.

In case that new updates are found, they are displayed under the Available Updates window section and can be directly installed by pressing on the “Apply Updates” button. The latest installed updates can be checked by pressing on the “View Applied Updates” button.

- Offline Patch Uploader - offers the possibility to upload updates in offline mode, without an internet connection

**Note!**

Contact [support@endpointprotector.com](mailto:support@endpointprotector.com) to request the Offline Patch.

# 3. Endpoint Management

## 3.1. Devices

In this module the administrator can manage all devices in the system. Endpoint Protector has an automatic system implemented meaning that it will automatically add any unknown devices connected to client computers to the database, thus making them manageable.

When an unknown device is connected to one of the client computers, the device's parameters are stored in the system database as: device data (Vendor ID, Product ID, and Serial Number). The user who first used the device is stored as the default user of the device. This, however, can be changed anytime, later.

The screenshot shows the 'List of Devices' page in the Endpoint Protector interface. The page title is 'Reporting and Administration Tool'. The interface includes a sidebar with navigation options and a main content area displaying a table of devices. The table has the following columns: Status, TD, Device Type, Device Name (Identification), Description, Department, and Last Location. The table lists various hardware components such as Serial ATA Controller, Internal CD or DVD RW, Webcam, WFI, Additional Keyboard, USB Storage Device, Local Printers, Bluetooth, and USB Modem.

Status	TD	Device Type	Device Name (Identification)	Description	Department	Last Location	Last User
All							
<input type="checkbox"/>		Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller ...	Default Department	-	-
<input type="checkbox"/>		Internal CD or DVD RW	MATSHITA DVD-RAM UJ8C2 S ATA Device	MATSHITA DVD-RAM UJ8C2 S ATA Device / (S...	Default Department	-	-
<input type="checkbox"/>		Webcam	USB2.0 HD UVC WebCam	USB2.0 HD UVC WebCam / Chicony Electron...	Default Department	-	-
<input type="checkbox"/>		WFI	Microsoft Virtual WiFi Miniport Adapter	Microsoft Virtual WiFi Miniport Adapter ...	Default Department	-	-
<input type="checkbox"/>		WFI	Atheros AR9485WB-EG Wireless Network Ada...	Atheros AR9485WB-EG Wireless Network Ada...	Default Department	-	-
<input type="checkbox"/>		Additional Keyboard	HD Keyboard Device	HD Keyboard Device / (Standard keyboard...	Default Department	-	-
<input type="checkbox"/>		Additional Keyboard	PC/AT Enhanced PS/2 Keyboard (101/102-Ke...	PC/AT Enhanced PS/2 Keyboard (101/102-Ke...	Default Department	-	-
<input type="checkbox"/>		USB Storage Device	DATATRAVELER_3.0	DATATRAVELER_3.0 / KINGSTON	Default Department	-	-
<input type="checkbox"/>		USB Storage Device	USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	Default Department	-	-
<input type="checkbox"/>		USB Storage Device	VOYAGER_LS	VOYAGER_LS / CORSAIR	Default Department	-	-
<input type="checkbox"/>		USB Storage Device	2307_FRAM	2307_FRAM / Kingston Technology Company ...	Default Department	-	-
<input type="checkbox"/>		Local Printers	Canon MP210 series	Canon MP210 series /	Default Department	-	-
<input type="checkbox"/>		Local Printers	HP LaserJet P1005, 1.6.0	HP LaserJet P1005, 1.6.0 /	Default Department	-	-
<input type="checkbox"/>		Bluetooth	Bluetooth Device	Bluetooth Device / Broadcom	Default Department	-	-
<input type="checkbox"/>		WFI	Wireless Network Adapter (802.11 a/b/g/n...	Wireless Network Adapter (802.11 a/b/g/n...	Default Department	-	-
<input type="checkbox"/>		Local Printers	Remote Printer	Remote Printer /	Default Department	-	-
<input type="checkbox"/>		Local Printers	Remote Printer	Remote Printer /	Default Department	-	-
<input type="checkbox"/>		Local Printers	Remote Printer	Remote Printer /	Default Department	-	-
<input type="checkbox"/>		Local Printers	Remote Printer	Remote Printer /	Default Department	-	-
<input type="checkbox"/>		Serial ATA Controller	Standard SATA AHCI Controller	Standard SATA AHCI Controller / Intel Co...	Default Department	-	-
<input type="checkbox"/>		USB Storage Device	VOYAGER_VEGA	VOYAGER_VEGA / CORSAIR	Default Department	-	-
<input type="checkbox"/>		Parallel Port (LPT)	Printer Port (LPT1)	Printer Port (LPT1) / (Standard port typ...	Default Department	-	-
<input type="checkbox"/>		Serial Port	Communications Port (COM1)	Communications Port (COM1) / (Standard p...	Default Department	-	-
<input type="checkbox"/>		Internal CD or DVD RW	HL-DT-ST DVDROM GH24NSC0	HL-DT-ST DVDROM GH24NSC0 / (Standard CD...	Default Department	-	-
<input type="checkbox"/>		USB Modem	SAMSUNG Mobile USB Modem	SAMSUNG Mobile USB Modem / SAMSUNG Elect...	Default Department	-	-

These are the actions available to the administrator in this module:



### **Edit, Manage Rights, Device History, Export Device History, Delete**

Manage Rights and Device History are actually shortcuts to the Devices Rights and Logs Report modules, and will be explained in one of the following chapters.

The status column indicates the current rights for the devices.



Red means that the device is blocked in the system.



Green means that the device is allowed on computers or users.



Yellow means that device is allowed on some users or computers with restrictions.

## 3.2. Device Functionality

Endpoint Protector can handle a wide variety of devices and device types and offers several methods of usage for each device in particular. These can be found by accessing the “Endpoint Rights” module of Endpoint Protector and selecting one of the relevant Rights tabs. The Endpoint Rights module contains the following sections: Device Rights, User Rights, Computer Rights, Group Rights, Global Rights, Effective Rights and File Whitelist.



Depending on the network policy, administrators can use the following settings:

- Preserve Global settings
- Deny access to devices
- Allow access to devices
- Enable read-only access
- Trusted Device Level 1 to Level 4
- Block WiFi if wired Internet connection is present



### 3.2.1. Give / Deny Access to Devices

With this option the administrator can give or deny complete access to a certain device making it usable or obsolete for a certain group, computer or user.

The administrator can configure these settings for each device individually and can also choose for what computer(s), user(s) and group(s) they will apply to.

The File Whitelisting feature allows the super administrator to control the transfer of only authorized files to previously authorized portable storage devices.

To configure File Whitelisting, please see paragraph 4.7 "File Whitelist".

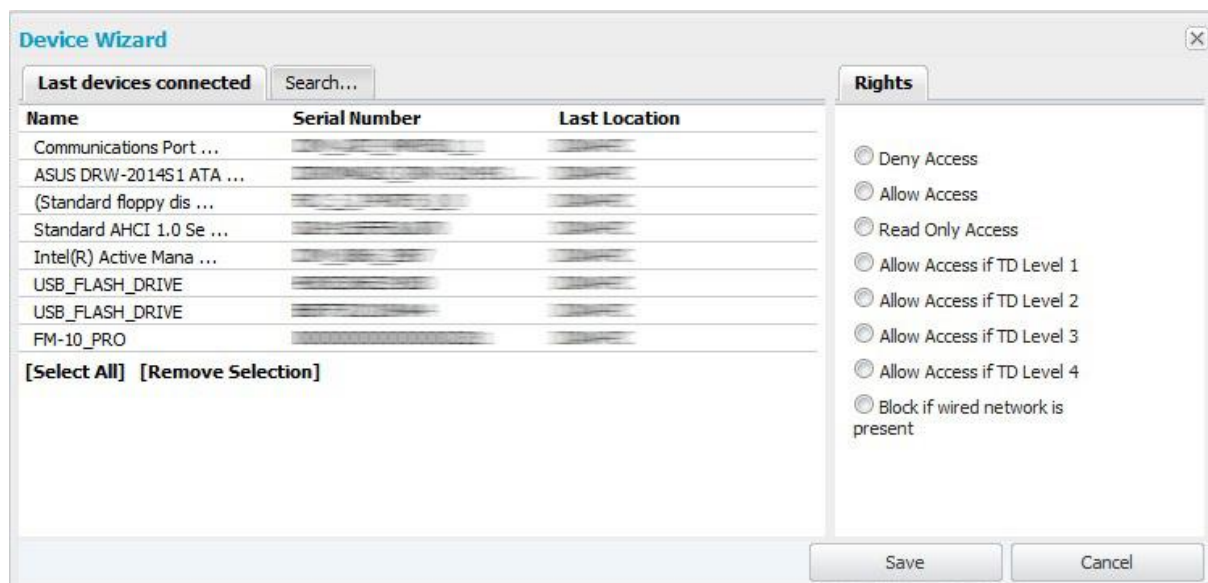
Once configured, you can enable this feature for devices, users, computers and groups. To do this, simply access the Endpoint Rights module and select device, computer, user or group rights, depending on the rights priority configuration of your server.



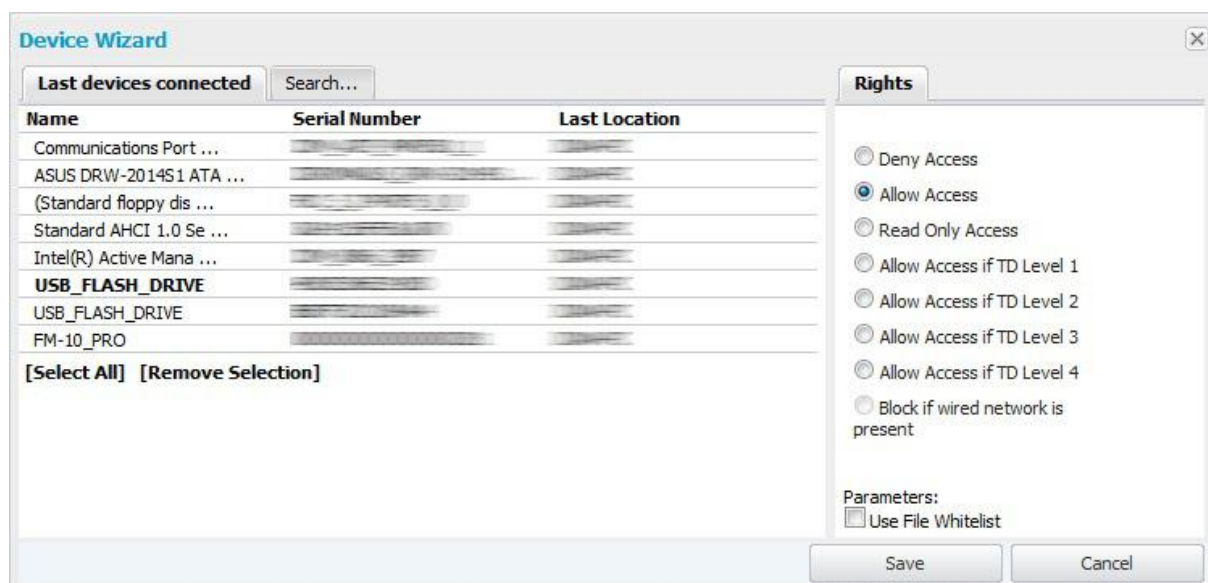
Select the device, user, computer or group you wish to manage rights for and click the + (plus) button at the bottom of the page, under "Already Existing Devices"



Once you do that, the Device Wizard will appear, allowing you to select the device(s) you wish to manage. Please note that you need to allow access to the storage device in order to enable the File Whitelisting for it.



Selecting a device will allow you to select one of the rights for that device.



Once you select a portable device, and choose “Allow Access” for it, you will also have the option to enable File Whitelisting for that device.

Click “Save” to store your changes.

The device(s) you selected will appear in the “Already Existing Devices” section.



To add more devices, simply repeat the steps mentioned above.

To change or delete added devices use either “Rights Wizard” or “Remove” action buttons.



### 3.2.2. Enable Device Read-Only Access

With this option the administrator can enable read-only access to devices preventing the deletion or alteration of data on the device(s).

The administrator can configure each device individually and can also choose for what computer(s), user(s) and group(s) it will apply to.

### 3.2.3. TrustedDevice Level 1 to Level 4

The TrustedDevices™ technology integrated within Endpoint Protector is available in four security levels, depending on the degree of protection offered by a device (devices using EasyLock™ are TD level 1).

For more information on TrustedDevices™ and EasyLock™, refer to section 15. “Enforced Encryption with TrustedDevice” in this user manual.

### 3.2.4. WiFi - Block if wired network is present

With this option the administrator can disable the WiFi connection, while a wired network connection is present. The WiFi connection will be available when the wired network is not present.

### 3.3. Computers

This is the module responsible for managing the client computers.

The screenshot shows the 'List of Computers' page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and Reports and Analysis. The main content area displays a table of registered computers with the following columns: Computer Name, IP, Department, Workgroup, Domain, Mac Address, Default User, Location, Last Time Online, Version, License, Modified at, and Modified by. The table contains several rows of data, including entries for 'intern.cososys.com' and 'ad4cososys.com'. Below the table, there are controls for 'Create', 'Export', 'Delete', and 'Back'.

Computer Name	IP	Department	Workgroup	Domain	Mac Address	Default User	Location	Last Time Online	Version	License	Modified at	Modified by
	192.168.0.125	Default Department	tony00-21-5D-27-4A-DE-1000	intern.cososys.com	00-21-5D-27-4A-DE			07-May-2015 13:42		Offline		
	81.196.156.53	Default Department		intern.cososys.com	00-21-5D-27-4A-DE			07-May-2015 13:42	1.0.5.1 - (Linux)	Offline		
	192.168.0.199	Default Department	WORKGROUP		e0-3f-49-33-38-16			07-May-2015 13:38	4.4.2.4 - (PC)	Offline		
	81.196.156.53	Default Department		intern.cososys.com	00-0C-29-C6-41-06			06-May-2015 21:39	1.0.4.1 - (Linux)	Offline		
	81.196.156.53	Default Department	WORKGROUP		c8-2a-14-0f-8b-92			29-Apr-2015 19:44	1.4.3.1 - (Macintosh)	Offline	29-Apr-2015 14:57:40	root
		Default Department		ad4cososys.com						Unlicensed		
		Default Department		ad4cososys.com						Unlicensed		
		Default Department		ad4cososys.com						Unlicensed		

The client computers have a registration mechanism. This self-registration mechanism is run once after the Endpoint Protector Client software is installed on a client computer. The client software will then communicate to the server its existence in the system. The server will store the information regarding the client computer in the system database and it will assign a license to the client computer (if none available, a demo license will be created and assigned, which will expire after 30 days).

#### NOTE!

The self-registration mechanism acts whenever a change in the computer licensing module is made, and also each time the application client is reinstalled. The owner of the computer is not saved in the process of self-registration.

Computers can also be imported into Endpoint Protector from Active Directory using the Active Directory Plug-in.

For details, please see paragraph 10.1 "Active Directory Import".

The available actions here are:





**Edit, Manage Rights, Manage Settings, Offline Temporary Password, Computer History, Export Computer History and Delete.** The Manage Rights, Manage Settings, Offline Temporary Password and Computer History are links to their respective modules, which will be explained in their own chapter.

For a better organization and manageability, a computer can be assigned as belonging to a Group (several computers within the same office, a group of computers which will have same access rights or settings) or to a Department (an alternative organization to groups). For more details about departments, please see paragraph 11.3 "System Departments".

## 3.4. Groups

This module is responsible for editing groups. **Edit, Manage Rights, Manage Settings** and **Delete** are the commands available from this section.

The screenshot shows the 'List of Groups' interface in the Endpoint Protector 4 Reporting and Administration Tool. The interface includes a sidebar with navigation options and a main content area displaying a table of groups. The table has the following columns: Name, Description, Domain, Department, Modified at, Modified by, and Actions. The table shows 5 results, all belonging to the 'Default Department'. Below the table are buttons for 'Create', 'Delete', and 'Back'.

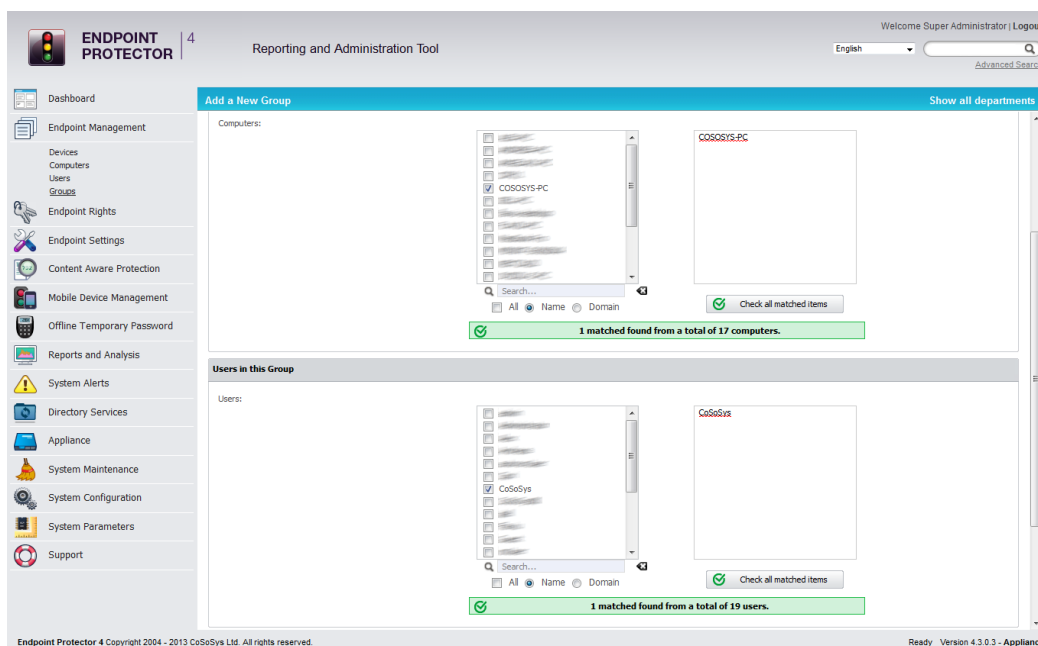
All	Name	Description	Domain	Department	Modified at	Modified by	Actions
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	Default Department	18-Jan-2016 21:37:46	root	[Edit] [Delete] [Back]
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	Default Department			[Edit] [Delete] [Back]
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	Default Department			[Edit] [Delete] [Back]
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	Default Department			[Edit] [Delete] [Back]
<input type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	Default Department			[Edit] [Delete] [Back]

5 results [ 20 per page]

Buttons: Create, Delete, Back

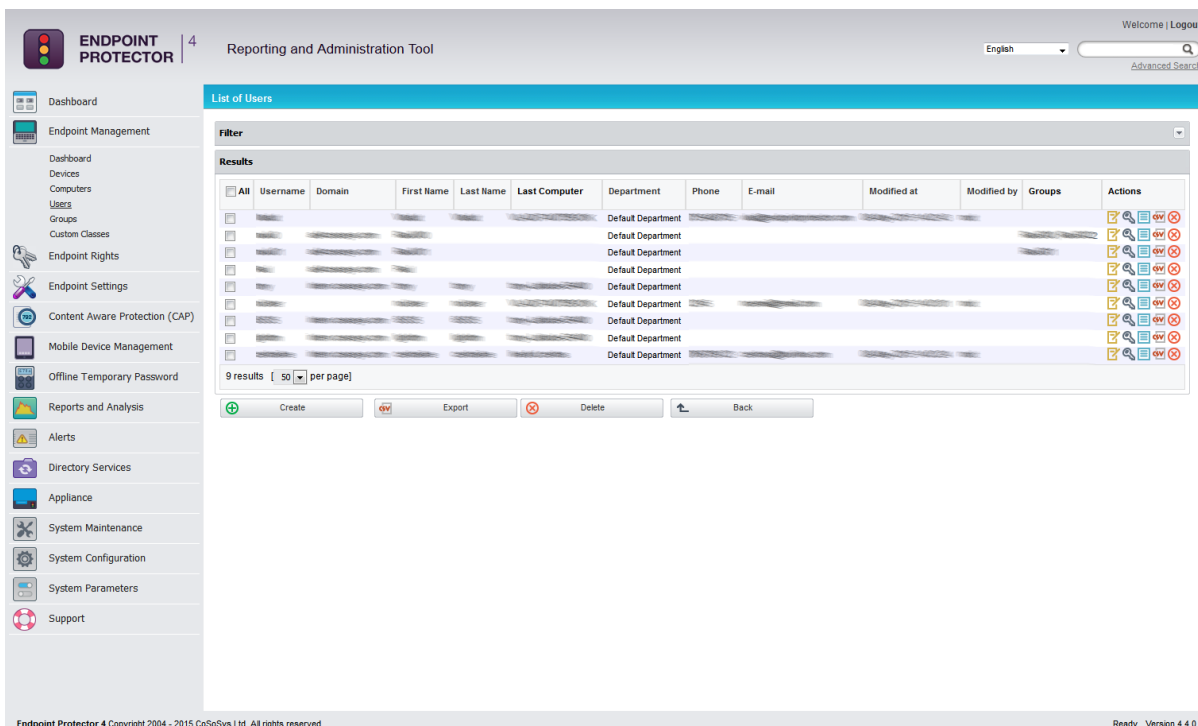
Grouping computers and client users will help the administrator to manage the rights, or settings for these entities in an efficient way. This can be done from the Group Rights and Group Settings tabs.

When creating a new group there is the possibility to add multiple users / computers simultaneously, by using the checkboxes and the option "Check all matched items".



### 3.5. Users

The client users are the end users who are logged on a computer on which the Endpoint Protector Client software is installed.



This module has a self-completing mechanism: as soon as a user has some activity on the system and he is new in the system, he will be added to the system database.



Actions available in this group are: **Edit, Manage Rights, User History, Export User History** and **Delete**.

There are two users created by default during the installation process of Endpoint Protector.

**noUser** – is the user linked to all events performed while no user was logged in to the computer. Remote users' names who log into the computer will not be logged and their events will be stored as events of noUser. Another occurrence of noUser events would be to have an automated script/software which accesses a device when no user is logged in to the specific computer.

**autorunUser** – indicates that an installer has been launched by Windows from the specific device. It is the user attached to all events generated by the programs launched from the specific device when Autoplay is enabled in the Operating System.

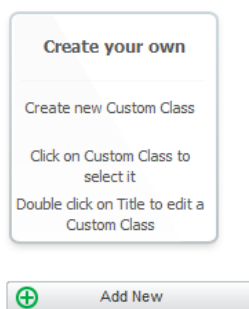
The users can be arranged in groups for easier management at a later point. Users can also be imported into Endpoint Protector from Active Directory through the Active Directory Plug-in.

For details, please see paragraph 10.1 "Active Directory Import".

## 3.6. Custom Classes

This section provides the option to create new classes of devices for an easier management. It is a powerful feature, especially for devices belonging to the same vendor and/or being the same product (same VID and/or PID).

A new Custom Class can be created by pressing on the *Add New* button or double clicking on the *Create your own* policy.



Before adding devices to a Custom Class, the Name, Description and Rights (Deny Access, Allow Access, Read Only Access, etc.) need to be provided and saved.

**Custom Class Description**

**Note:** Please provide and save the Name and Description before adding devices to the Custom Class.

Name:

Description:

Rights: Deny Access ▼

Once this is done, there are multiple ways of adding devices to a Custom Class:

- **Add new device** – will open a pop-up, allowing for each device to be added based on Vendor ID, Product ID and Serial Number. Pressing on the green plus button will provide the option to continue adding devices.

**Add new device** ✕

▼
Vendor ID
Product ID
Serial Number
Description
+

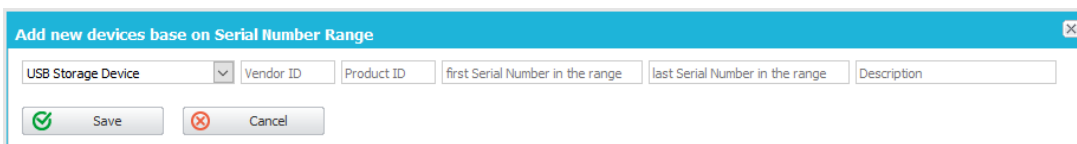
- **Add existing device** – will open a pop-up, allowing the selection of devices previously connected to protected computers and subsequently already available in the Endpoint Protector database.

**Add existing devices** ✕

All Device Types
▼
Name
Vendor ID
Product ID
Serial Number
🔍

<input type="checkbox"/> All	Name	Vendor ID	Product ID	Serial Number	Last Location
<input type="checkbox"/>	HID Keyboard Device	2101	20f	HID-VID_2101&PID_020F&REV_0	CRISTIB
<input type="checkbox"/>	HID Keyboard Device	0	0	HID-MLIT_HID&Col01/HID_DEVIC	CRISTIB
<input type="checkbox"/>	Communications Port (COM1)	0	0	COM_ACPI_PNP0501_1_1VR.32D!	CRISTIB
<input type="checkbox"/>	HL-DT-ST DVDROM GH24NSB0	0	0	CDROM&VEN_HL-	CRISTIB
<input type="checkbox"/>	STORAGE_MEDIA	54c	9c2	5C071058DF9B156A86	CRISTIB
<input type="checkbox"/>	HID Keyboard Device	2101	20f	HID-VID_2101&PID_020F&REV_0	CRISTIB

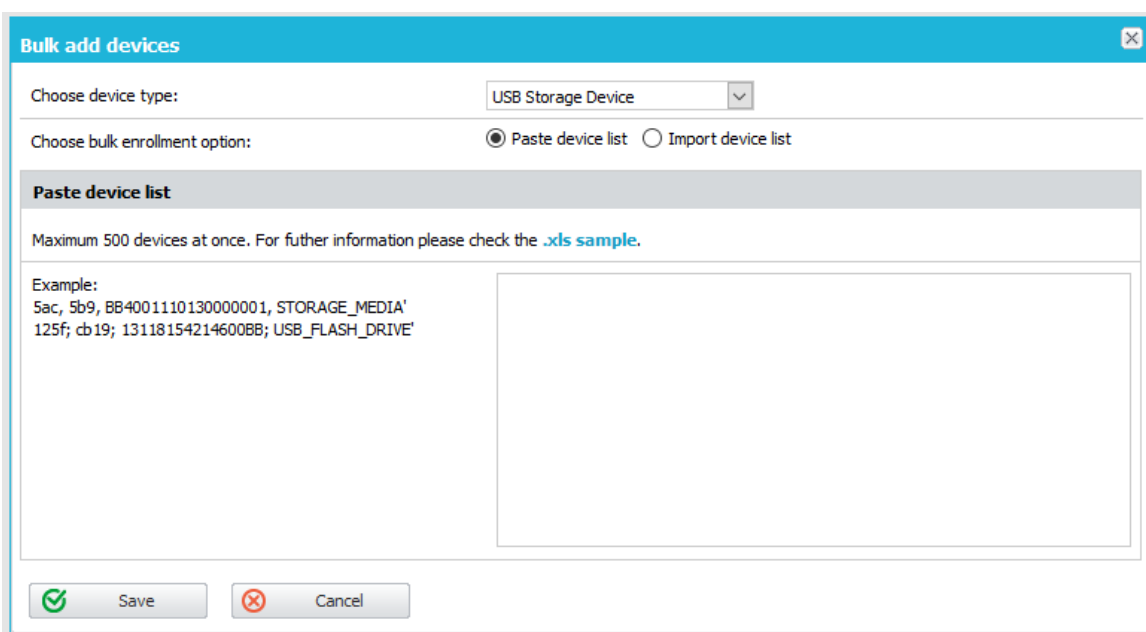
- **Add Serial Number range** – will open a pop-up, allowing multiple devices to be added at the same time, by specifying the first and last Serial Number in the range. The recommended use for this feature is for devices that have a consecutive range, with a clear, noticeable pattern.



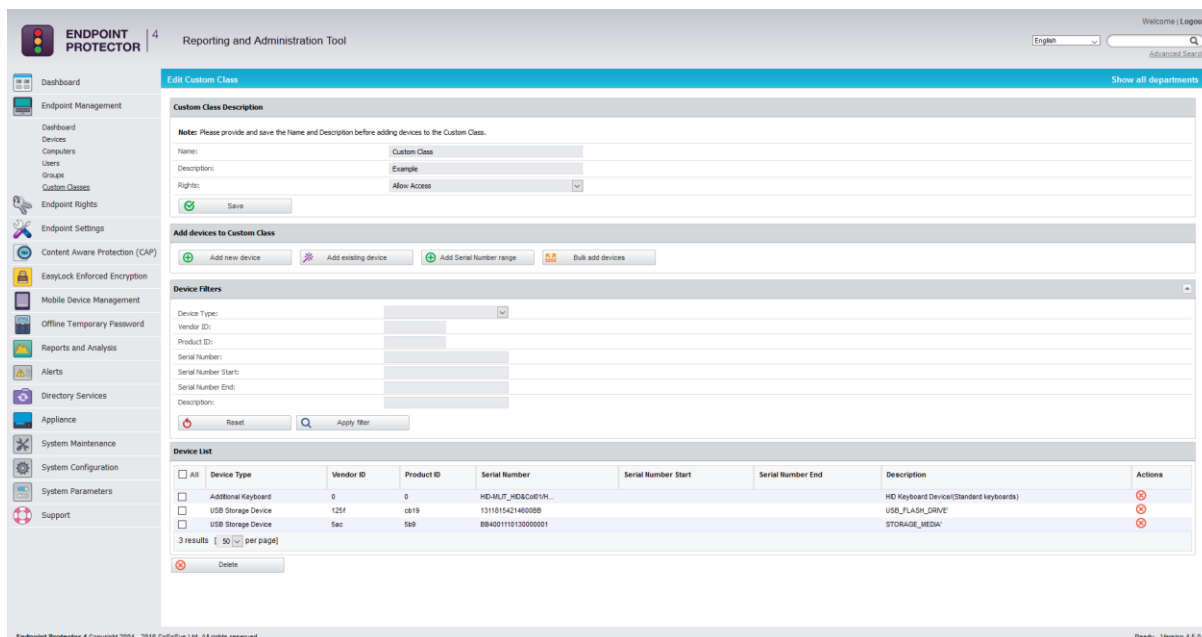
**Note!**

Although this feature can actually work in situations where the Serial Number range does not follow a noticeable pattern, it is not recommended. In these type of situations, some devices will be ignored by Endpoint Protector and the Custom Class will not have the desired effect.

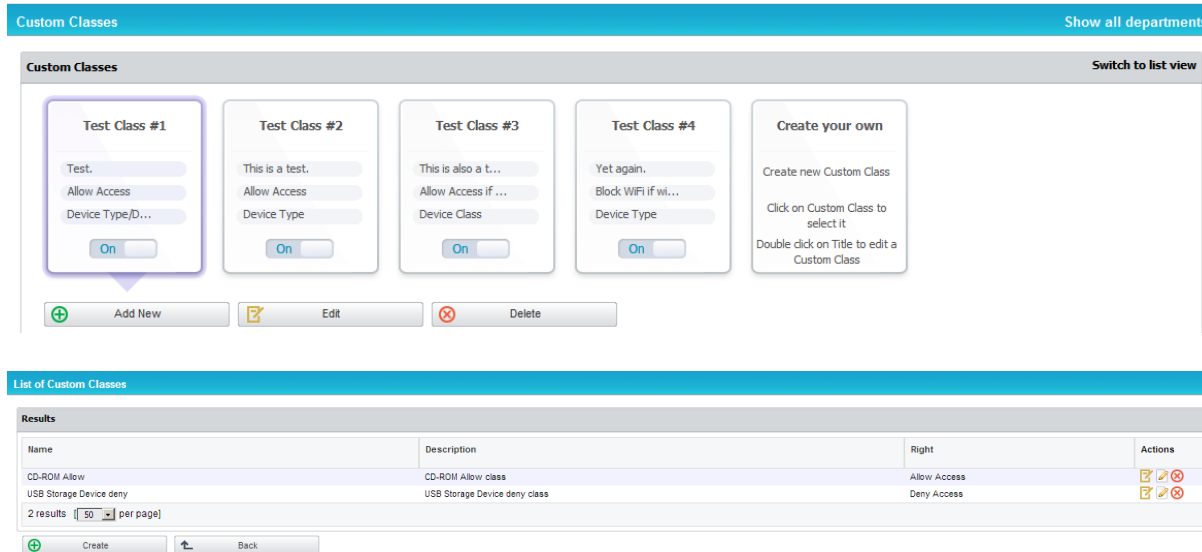
- **Add bulk devices** – will open a pop-up, allowing up to 500 devices with the same type to be added. There are two methods to choose from, either importing a list or by simply pasting the information.



Once the devices have been added, the inside of a Custom Class will look similar to the below image.



When multiple Custom Classes have been created, the user interface for this section is set by default to resemble the below shown. However, a list view is also available by clicking the *Switch to list view* button.



For a better understanding of how rights are assigned to Custom Classes, please see the example below:

Eg. For the case above, we created a Custom Class *CD-ROM Allow* and set "Allow access" rights to devices of type CD-ROM /DVD-ROM. Let's say that CD-ROMs have "Deny access" rights set on Client PC CIP0. Once the custom class *CD-ROM Allow* is created and Custom Classes is enabled, all the CD-ROMs/DVD-ROMs will have access, even if on the Client PC CIP0 they have "Deny access".


## 3.7. Terminal Servers and Thin Clients

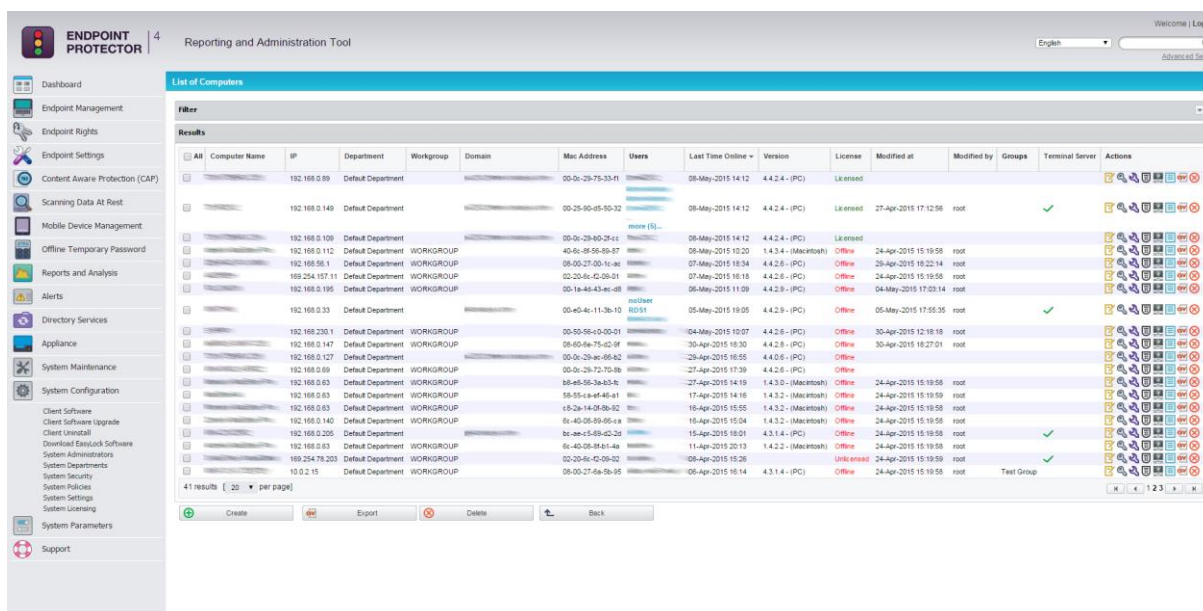
The capability to control file transfers on RDP storage between thin clients and Windows Terminal servers can be enforced through Endpoint Protector, as detailed below.

### 3.7.1. Initial Configuration

The process starts with the menu view from Endpoint Management ->

Computers, namely the action to **Mark as Terminal Server** .

After successfully marking the computer present in the system as a Terminal Server, a distinctive  will be displayed for ease of identification, as seen below:



The screenshot shows the 'List of Computers' page in the Endpoint Protector interface. The table lists various computers with columns for Computer Name, IP, Department, Workgroup, Domain, Mac Address, Users, Last Time Online, Version, License, Modified at, Modified by, Groups, Terminal Server, and Actions. The 'Terminal Server' column for the selected computer (IP: 192.168.0.149) shows a green checkmark, indicating it has been successfully marked as a Terminal Server.

#### Note!

The computers that can be targeted by this action are strictly Windows Servers with Terminal Server roles properly configured.

Make sure that there is at least one (1) Terminal Server license available when the action **Mark as Terminal Server** is performed.

If the terminal server is successfully marked, a new device type will appear when choosing to Edit it under Endpoint Rights -> Computer Rights.

The settings for the Terminal Server specific Device Types are: Preserve Global Settings, Allow Access, Deny Access and Read Only Access.

#### Terminal Server Specific Device Types

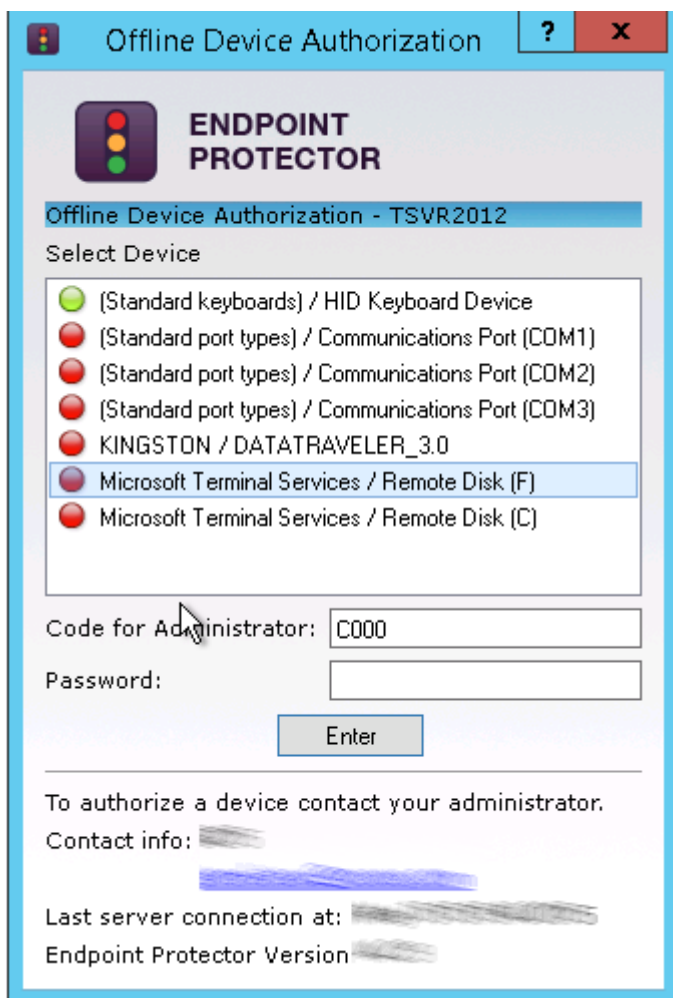
Thin Client Storage (RDP Storage)

Allow Access





On a Windows Terminal server, the Endpoint Protector client will display RDP Storage disks shared by one or multiple thin clients as seen below.



# 4. Endpoint Rights

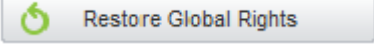
The modules in this area will allow the administrator to define which device can be used on computers, groups and which client users have access to them.

The screenshot displays the 'Management of Rights per Devices' interface in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, and Endpoint Settings. The main content area features a 'Filter' section with fields for Device Name, Device Type (set to 'USB Storage Device'), VID, PID, and Serial Number. Below the filter is a 'Results' table listing various USB storage devices with columns for Device Name, Device Description, Device Type, VID, PID, Serial Number, and Actions. The table shows 9 results, with a pagination control set to 50 per page.

Device Name	Device Description	Device Type	VID	PID	Serial Number	Actions
USB_SD_READER	USB_SD_READER / GENERIC	USB Storage Device				
USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device				
USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device				
USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device				
USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device				
USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device				
Port_#0004.Hub_#0004	Port_#0004.Hub_#0004 / Ironkey Inc.	USB Storage Device				
FREEAGENT	FREEAGENT / SEAGATE	USB Storage Device				
DISK	DISK / EASY	USB Storage Device				

The rule of inheritance is as follows (from most important to least important): Computer Rights -> Group Rights -> Global Rights. The rights are overwritten in this order.

Example: If global rights indicate that no computer on the system has access to a specific device, and for one computer that device has been authorized, then that computer will have access to that device.

“Restore Global Rights” (  ) button can be used to revert to a lower level of rights. Once this button is pushed all rights on that level will be set to “preserve global settings” and the system will use the next level of rights.

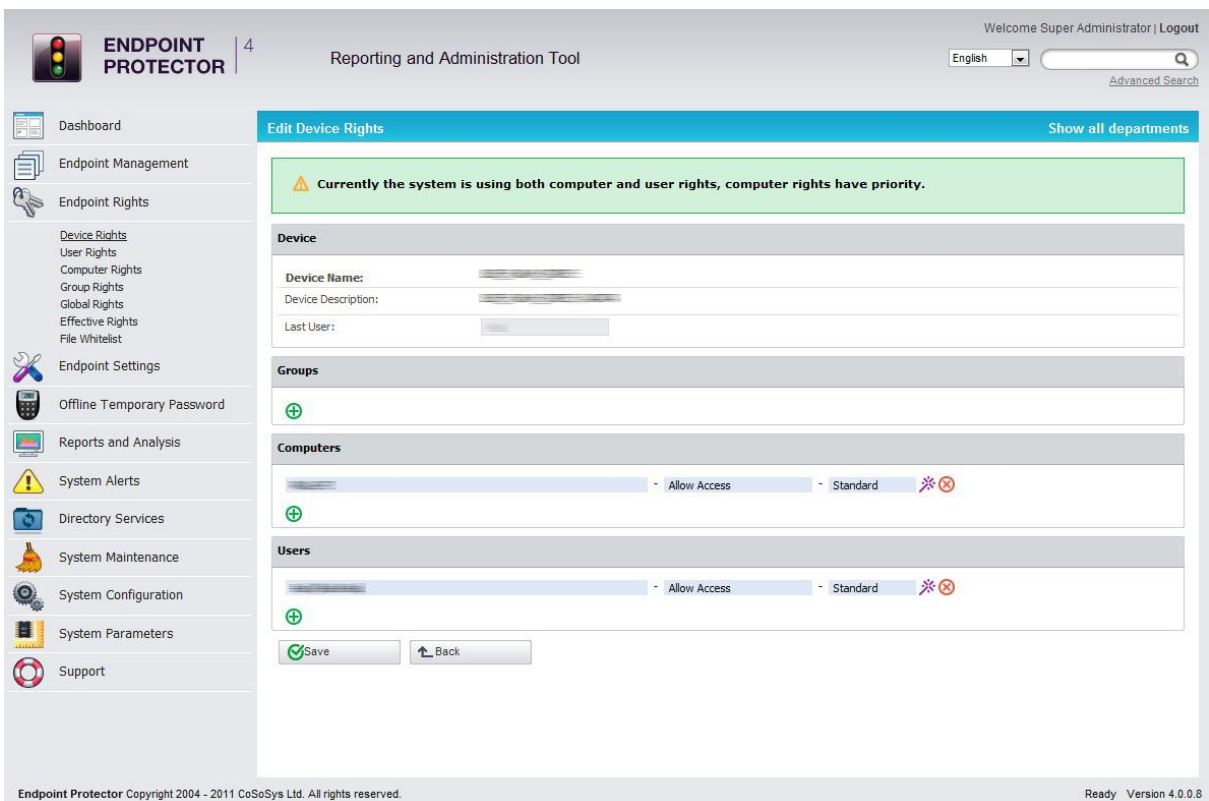
Example: If the action is done on group rights, the entities from that group will use from that point onwards the global rights.

### Note!

All “already existing devices” that were added on that level will be deleted when the restore is used.

## 4.1. Device Rights

This section is built around the devices, allowing the administrator to enable or disable them for specific computers, groups or users.



The screenshot displays the 'Edit Device Rights' interface in the Endpoint Protector administration tool. The top navigation bar includes the logo, 'Reporting and Administration Tool', and user information. The left sidebar lists various management options. The main content area features a warning banner and sections for configuring rights for a specific device, including groups, computers, and users. Each section shows a list of entities with their current rights settings and control icons.

After selecting a computer, you select the computers and group of computers for which the device has specified rights.

## 4.2. User Rights

This module is built around the user, allowing administrators to manage rights of access to devices per users.

The screenshot displays the 'Edit User Rights' interface within the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Device Rights, User Rights, Computer Rights, Group Rights, Global Rights, Effective Rights, File Whitelist, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support.

The main content area is titled 'Edit User Rights' and features a green warning banner: 'Currently the system is using both computer and user rights, computer rights have priority.' Below this, there are input fields for 'User Name', 'First Name', and 'Last Name'. A section titled 'Device Types (To view all supported devices and rights, go to Device Types in System Parameters)' contains a table of device categories and their associated rights settings.

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

At the bottom of the device list, there is an 'Already Existing Devices' section with a plus icon and a 'Save' button. Below this are buttons for 'Restore Global Rights' and 'Back'. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.6'.

## 4.3. Computer Rights

This module will allow administrators to specify what device types and also what specific device(s) can be accessible from a single or all computers.

**ENDPOINT PROTECTOR** | 4 Reporting and Administration Tool Welcome | Logout English  Advanced Search

**Edit Computer Rights**

**Warning:** Currently the system is using both computer and user rights, computer rights have priority.

**Computer**

Computer Name:

Location:

**Device Types (To view all supported devices and rights, go to Device Types in System Parameters)**

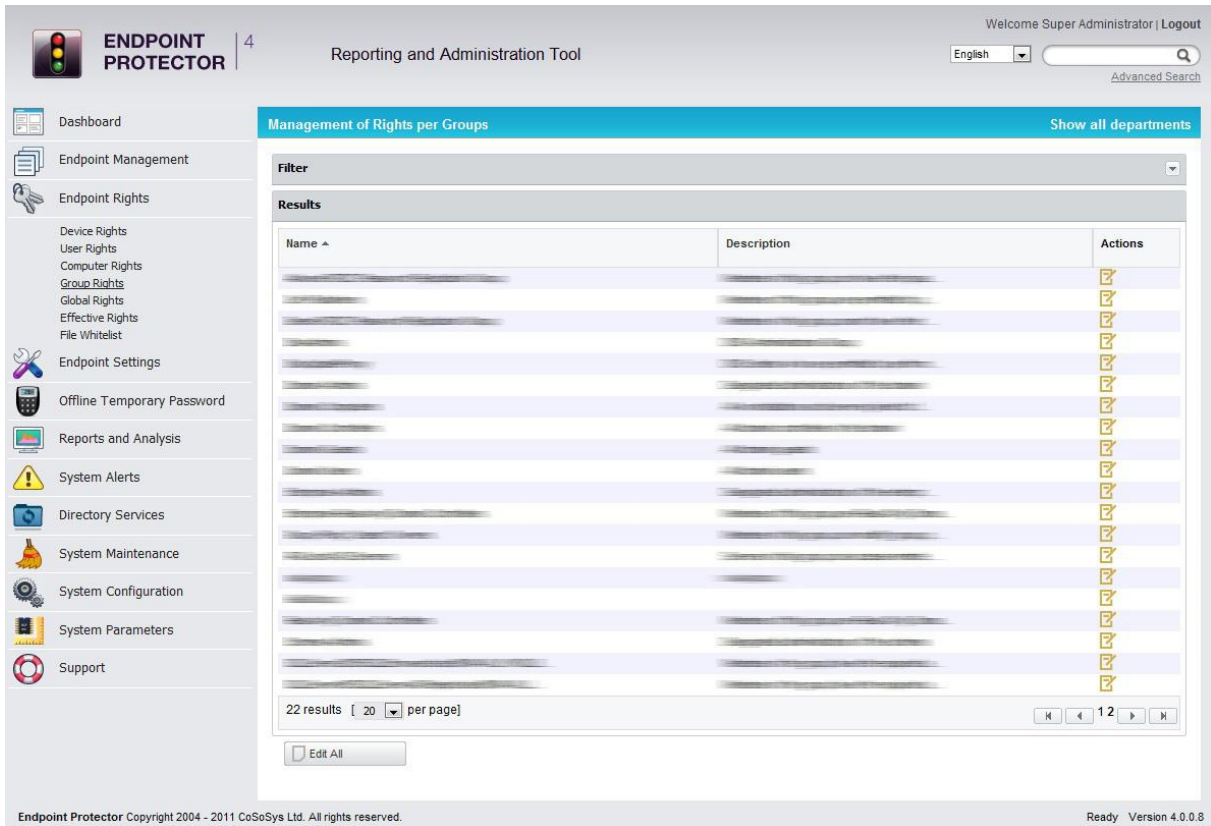
Unknown Device	Preserve global setting	Serial ATA Controller	Preserve global setting
USB Storage Device	Allow Access	WiFi	Preserve global setting
Internal CD or DVD RW	Preserve global setting	Bluetooth	Preserve global setting
Internal Card Reader	Preserve global setting	FireWire Bus	Preserve global setting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

**Already Existing Devices**

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.6

## 4.4. Group Rights

This module is similar to the previous one, only difference is that the rights here are applied to a group instead of a single computer.



The administrator can use the “Edit All” action here to edit rights for all groups at once.



## 4.5. Global Rights

This module applies rights to computers in the entire system.

**ENDPOINT PROTECTOR 4** Reporting and Administration Tool

Welcome | Logout

English

Advanced Search

**Management of Global Rights**

⚠ **Currently the system is using both computer and user rights, computer rights have priority.**

**Groups**

Name: Global  
Description: Global Group including all the machines

**Device Types (To view all supported devices and rights, go to Device Types in System Parameters)**

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

**Already Existing Devices**

Save Back

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.6

## 4.6. Effective Rights

This section displays the Device Control or Content Aware Protection policies applied at that time.

Depending on the options selected from the drop-down menus, information can be displayed based on rights, users, computers, device types, specific devices and more.

The screenshot shows the 'Effective Rights' configuration page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and Endpoint Rights. The main content area has a header indicating the system is using both computer and user rights, with computer rights having priority. Below this is an 'Effective Rights Filter' section with several dropdown menus for selecting rights, computers, users, device types, and specific devices. A 'Results' section follows, displaying a table of rights applied to various device types.

Device Type	Device	Right	Using File Whitelist	Observation	Defined On
Unknown Device		Deny Access	No	Inherited from Global Policies	Global
USB Storage Device		Deny Access	No	Inherited from Global Policies	Global
Digital Camera		Deny Access	No	Inherited from Global Policies	Global
SmartPhone (USB Sync)		Deny Access	No	Inherited from Global Policies	Global
SmartPhone (Windows CE)		Deny Access	No	Inherited from Global Policies	Global
SmartPhone (Symbian)		Deny Access	No	Inherited from Global Policies	Global
Internal Card Reader		Deny Access	No	Inherited from Global Policies	Global
PCMCIA Device		Deny Access	No	Inherited from Global Policies	Global
FireWire Bus		Deny Access	No	Inherited from Global Policies	Global
ZIP Drive		Deny Access	No	Inherited from Global Policies	Global
Internal CD or DVD RW		Deny Access	No	Inherited from Global Policies	Global
Internal Floppy Drive		Deny Access	No	Inherited from Global Policies	Global
Card Reader Device (MTD)		Deny Access	No	Inherited from Global Policies	Global
Card Reader Device (SCSI)		Deny Access	No	Inherited from Global Policies	Global
Windows Portable Device (Media Transfer Protocol)		Deny Access	No	Inherited from Global Policies	Global
Mobile Phones (Sony Ericsson, etc.)		Deny Access	No	Inherited from Global Policies	Global
Local Printers		Deny Access	No	Inherited from Global Policies	Global
Bluetooth		Allow Access	No	Inherited from Global Policies	Global

## 4.7. File Whitelist

This module allows the super administrator to control the transfer of only authorized files to previously authorized portable storage devices.



The screenshot shows the 'File Whitelist' configuration page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and Endpoint Rights. The main content area is titled 'File Whitelist' and features a 'Folder containing Whitelist files' section with a text input field set to 'c:/TempWeb'. Below this, there are 'Refresh' and 'Upload Files' buttons. A table lists files found in the folder, with columns for Status, Filename, File Path, File Extension, Last Modified, and Size. The table contains four entries, with the first one checked. At the bottom of the table, there are 'Check All' and 'Uncheck All' buttons, and a 'Save' button.

Status	Filename	File Path	File Extension	Last Modified	Size
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	doc	1 June 2011 16:13:25 EEST	38.5 kB
<input type="checkbox"/>	[Redacted]	[Redacted]	log	2 June 2011 16:12:16 EEST	12.02 MB
<input type="checkbox"/>	[Redacted]	[Redacted]	log	1 June 2011 10:52:25 EEST	0 B
<input type="checkbox"/>	[Redacted]	[Redacted]	test	1 June 2011 09:30:14 EEST	8 B

The super administrator can manage exactly what files can be copied to removable devices, and which cannot. In order to use this feature, the administrator must create a folder in which the authorized files will be kept and he must set this address in the "Folder" field.

This is a close-up view of the 'File Whitelist' configuration page. It shows the 'Folder containing Whitelist files' section with the 'Folder' field set to 'c:/TempWeb'. Below the field, there are 'Refresh' and 'Upload Files' buttons. A table lists files found in the folder, with columns for Status, Filename, File Path, File Extension, Last Modified, and Size. The table contains four entries, with the first one checked. At the bottom of the table, there are 'Check All' and 'Uncheck All' buttons, and a 'Save' button.

Status	Filename	File Path	File Extension	Last Modified	Size
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	doc	1 June 2011 16:13:25 EEST	38.5 kB
<input type="checkbox"/>	[Redacted]	[Redacted]	log	2 June 2011 16:12:16 EEST	12.02 MB
<input type="checkbox"/>	[Redacted]	[Redacted]	log	1 June 2011 10:52:25 EEST	0 B
<input type="checkbox"/>	[Redacted]	[Redacted]	test	1 June 2011 09:30:14 EEST	8 B

After copying the required files into the previously created folder, he must simply press the "Refresh" button for a list to be generated.

Finally, he must check the box next to each file to enable it, and click the "Save" button. The files will be hashed and will receive permission to be copied.

This feature is only available to the Super Administrator user and cannot be modified by regular administrators.

### Note!

This only works for outbound transfers. Files copied from external sources onto client (protected) computers will still be processed using the existing system policy.

# 5. Offline Temporary Password

This module allows the Super Administrator or the Offline Temporary Access Administrator to generate a password and grant temporary access to:

- a specific device on a computer
- the Content Aware Protection feature on a computer
- the entire computer

It can be used when there is no network connection between the client computer and the Server.

## **Note!**

Once a device is temporarily authorized, any other rights/settings saved afterwards for this device will not take immediate effect, until the time period has passed and the connection with the Server is re-established.

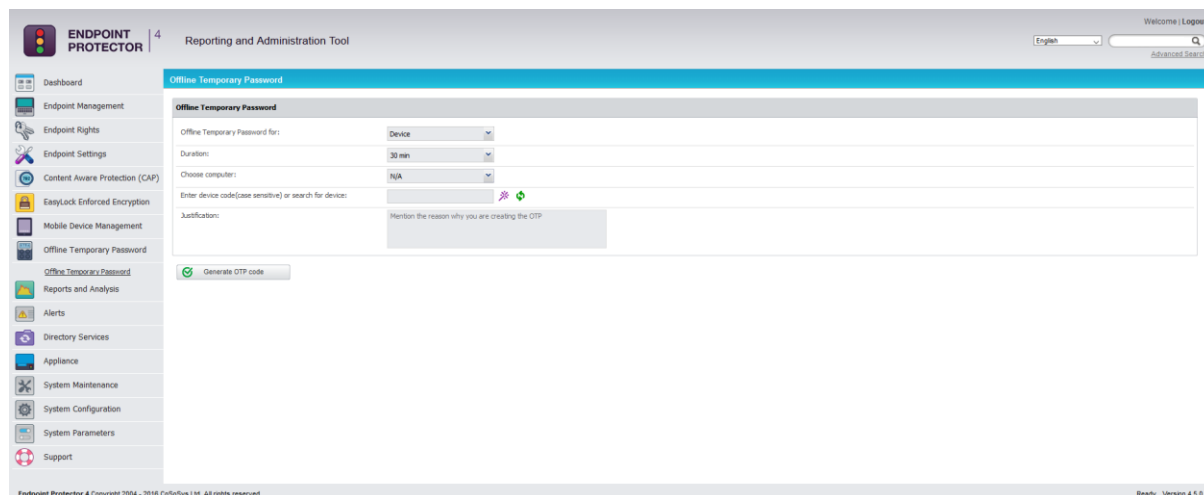
A password is unique for a certain device and time period. This means the same password cannot be used for a different device or for the same device twice.


The password will give permission to the device, computer or sensitive data transfer for the specified amount of time. The time intervals which can be selected are: 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days and 30 days.


The administrator also has the option to add a justification, mentioning the reason why the password was created. This can later be used for a better overview or various audit purposes.

## 5.1. Generating the Offline Temporary Password

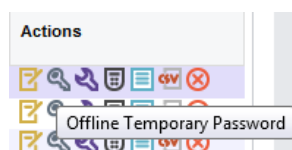
Depending on the options selected from the drop-down menus, the Offline Temporary Password (or OTP) can be generated for the exact device or computer needed.



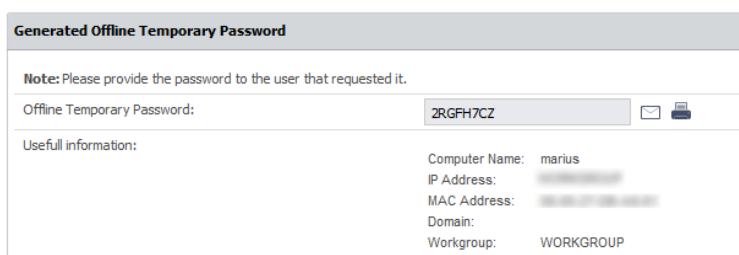
When generating an OTP for a Device, the administrator can either introduce the device code communicated by the user or search the Endpoint Protector database for an existing device, using the wizard .

For additional verification, the administrator can check the authenticity of a given device code by using the “Refresh Device Codes” option . This will only work if it was previously listed in the Endpoint Management > Devices list.

Another way to generate a password is by right clicking on a managed computer or device (from the Endpoint Management tab) and select the “Offline Temporary Password” action.



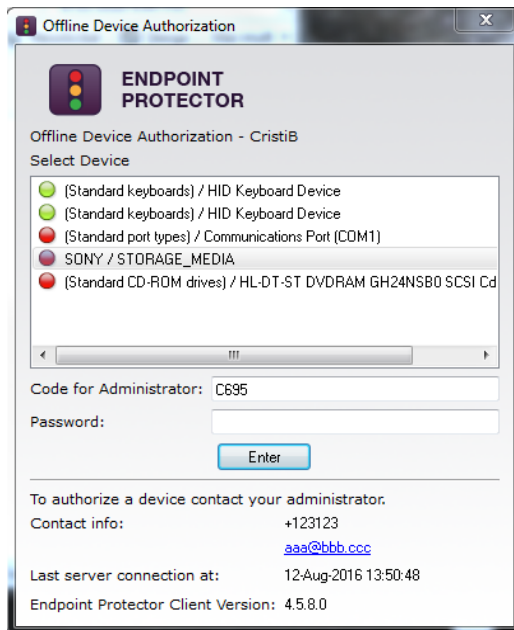
Once the OTP code has been generated, it will be displayed as below, and it needs to be provided to the user that made the request. Endpoint Protector offers two quick ways of doing this, either by sending a direct email or by printing it out.



## 5.2. Using the Offline Temporary Password to authorize a device

In order to select a device and enter a password, the user needs to click on the Endpoint Protector icon from the system tray.

The user will select the device from the list and contact the administrator at the displayed contact information. The administrator will generate the OTP based on the device code (see above paragraph).



Once the code has been generated and is in the user's possession, the password will be inserted in the correspondent field and applied by clicking "Enter".

For Content Aware Protection or full Computer authorization, the administrator just simply needs to provide the user with password previously generated.

## 5.3. Setting the Administrator Contact Information

The Administrator contact information can be edited under System Configuration > System Settings, in the "Main Administrator Contact Details" section.

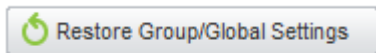
Main Administrator Contact Details	
Phone:	<input type="text" value="+{(40)0740000001"/>
E-mail:	<input type="text" value="Administrator@example.com"/>
<p><b>*Note:</b> This contact information is referring to Offline Temporary Password only! For Alerts, you must setup the e-mail address from System Administrators &gt; Edit info.</p>	
<input type="button" value="Save"/>	

# 6. Endpoint Settings

The settings are attributes which are inherited. Settings are designed to be applied on computers, groups or globally (to all computers). The rule of inheritance is the following (from the most important to the least important):

- Computer Settings (settings applied to exactly one computer)
- Group Settings (settings applied on a group)
- Global Settings (settings applied for all the computers)

Reverting the settings for an entity to the higher level settings can be done by using the *Restore Group/Global Settings* button.



Example: If the action is done on group settings, the entities in the group will use the global settings from that point onwards.

The settings available in this section are listed below:

**Refresh Interval** (in seconds) – represents the time interval at which the client will send a notification to the server with the intent to inform the server of its presence in the system. The server will respond by checking the settings and rights and updating them if needed, so the client can behave accordingly.

**Log Upload Interval** (in minutes) – represents the maximum time interval at which the client will send the locally stored log information to the server. This time interval can be smaller than the default value in case the log size is greater than the Local Log Size setting.

**Local Log Size** (in kilobytes) – represents the maximum size of the log which can be stored by the client on the client pc. If this value is reached then the client will send this information to the server.

This mechanism is optimal when a client computer has a lot of activity, because

it will send the information very quickly to the server, so the administrator can be informed almost instantly about the activities on that computer.

**Shadow Upload Interval** (in minutes) – represents the maximum time interval at which the client will send the locally stored shadow information to the server.

**Local Shadow Size** (in megabytes) – represents the maximum size of shadowed files stored by the client on a client PC. When this value is reached, the client will start overwriting existing files in order for it to not exceed the specified limit.

**Minimum File Size for Shadowing** (in kilobytes) – represents the minimum file size that should be shadowed. If a value is set here than files smaller in size than that value will not be shadowed.

**Maximum File Size for Shadowing** (in kilobytes) – represents the maximum file size that should be shadowed. If a value is set here, then files larger in size than that value will not be shadowed.

Additionally, File Tracing, File Shadowing and enabling Custom Client Notifications are also powerful features that can be set from this section. They will be explained in their own subsections below, due to their importance.

## 6.1. Computer Settings

This section will allow the administrator to edit the settings for each computer.

The screenshot shows the 'Edit Settings for Computer' page in the Endpoint Protector Reporting and Administration Tool. The page is organized into several sections:

- Computer:** Fields for Default User, IP, MAC Address, Computer Name, and Location.
- Mode:** Refresh Interval (set to 0) and Mode (set to Normal).
- File Tracing and Shadowing:** Checkboxes for File Tracing, File Shadowing, and Exclude Extensions from Shadowing. A text input for Exclude Extensions from CAP Scanning.
- Client Settings:** A table of settings for Log Interval, Shadow Interval, Min File Size, Removable Devices Recovery Folder Maximum Size, and Recovery Folder Retention Period.
- Logging:** Fields for Created at, Created by, Modified at, and Modified by.

At the bottom of the page, there are buttons for Save, Restore Group/Global Settings, and Back. The footer of the page reads 'Endpoint Protector 4 Copyright 2004 - 2016 CofSISys Ltd. All rights reserved. Ready Version 4.4.1.0'.

Defining custom settings for all computers is not necessary, since a computer is perfectly capable of functioning correctly without any manual settings defined. It will do this by either inheriting the settings of a group it's in or, if not possible,

the global settings, which are mandatory and exist in the system with default values from installation.

## 6.2. Group Settings

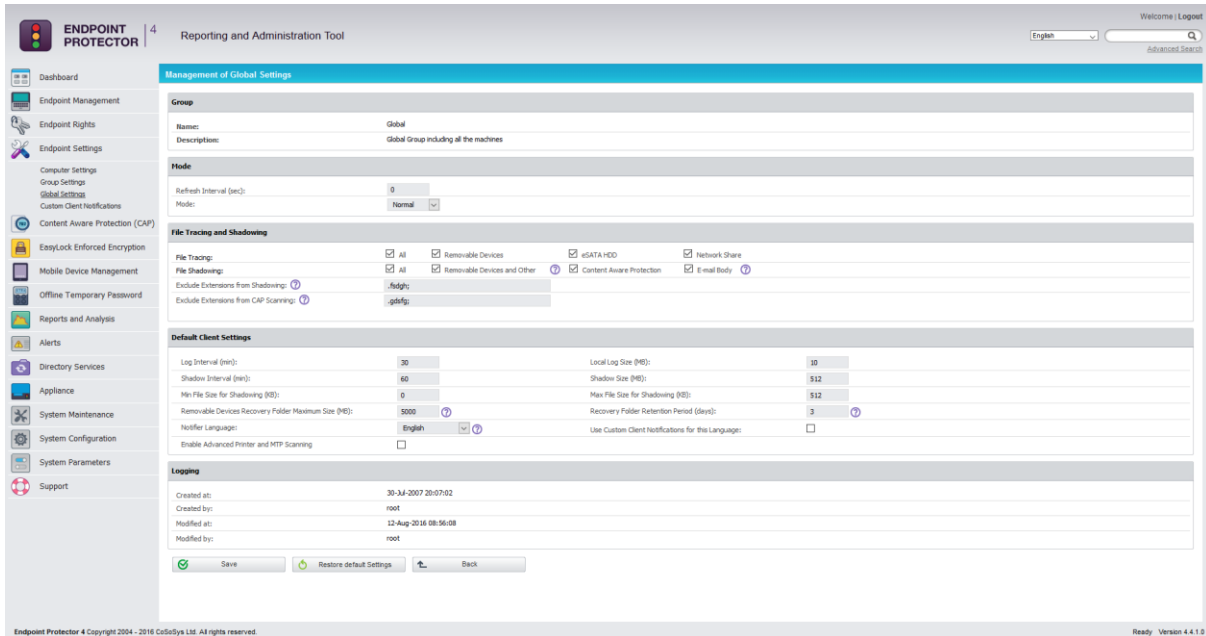
This section will allow the administrator to edit the settings for each group.

The screenshot displays the 'Management of Global Settings' page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Computer Settings, Group Settings, Global Settings, Custom Client Notifications, Content Aware Protection (CAP), EasyLock Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Management of Global Settings' and shows the configuration for a group named 'Global'. The group description is 'Global Group including all the machines'. The settings are organized into several sections: 'Group' (Name: Global, Description: Global Group including all the machines), 'Mode' (Refresh Interval: 0, Mode: Normal), 'File Tracing and Shadowing' (File Tracing: All, Removable Devices, eSATA/HDD, Network Share; File Shadowing: All, Removable Devices and Other, Content Aware Protection, E-mail Body; Exclude Extensions from Shadowing: .hdg; Exclude Extensions from CAP Scanning: .gdf;), 'Default Client Settings' (Log Interval: 30, Local Log Size: 10, Shadow Interval: 60, Shadow Size: 512, Min File Size for Shadowing: 0, Max File Size for Shadowing: 512, Removable Devices Recovery Folder Maximum Size: 5000, Recovery Folder Retention Period: 3, Notifier Language: English, Use Custom Client Notifications for this Language: unchecked), and 'Logging' (Created at: 30-Jul-2007 20:07:02, Created by: met, Modified at: 12-Aug-2016 08:56:08, Modified by: met). At the bottom, there are buttons for 'Save', 'Restore default Settings', and 'Back'.

We mentioned earlier that computers can be grouped in order to make editing the settings easier and more logical.

## 6.3. Global Settings

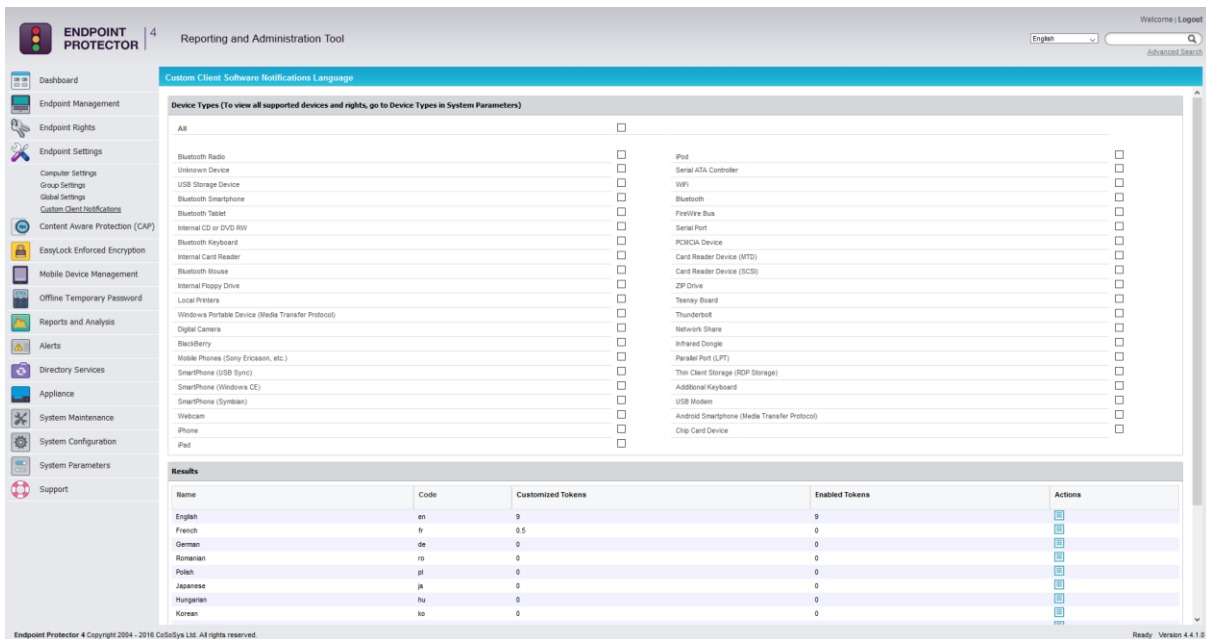
This section holds the global settings, which influence all computers within the system. If there are no settings defined for a computer, and it does not belong to a group, these are the settings it will inherit. If the computer belongs to a group, then it will inherit the settings of that group.



## 6.4. Custom Client Notifications

This section allows the administrator to edit the notification messages that appear from the Endpoint Protector Client. Custom Client Notifications can be globally enabled from Endpoint Settings > Global Settings. It can also be individually checked on computers or groups, as per the sections mentioned above.

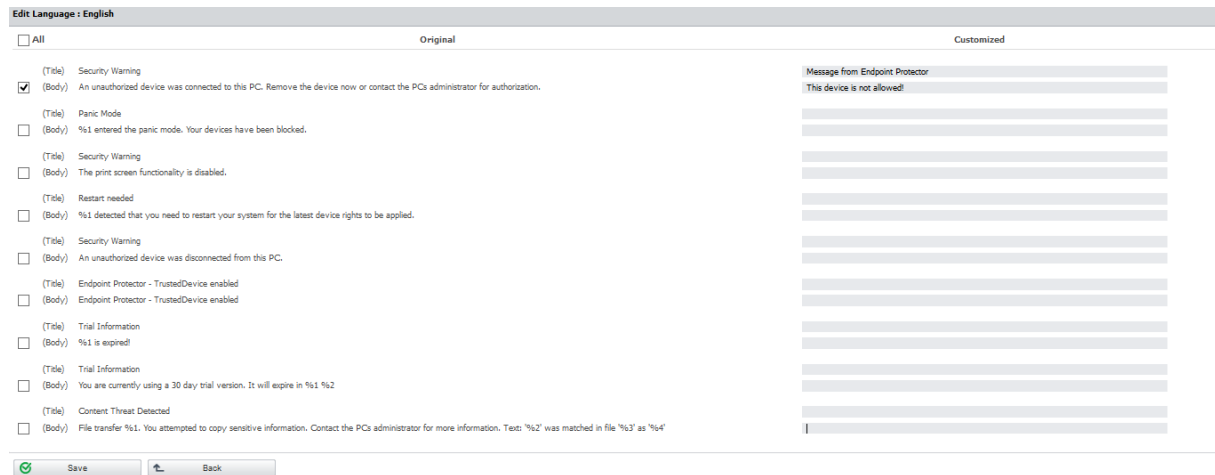
By selecting a Device Type, the Results section will display the editable languages available.



To edit the messages for a specific language, click on Actions.



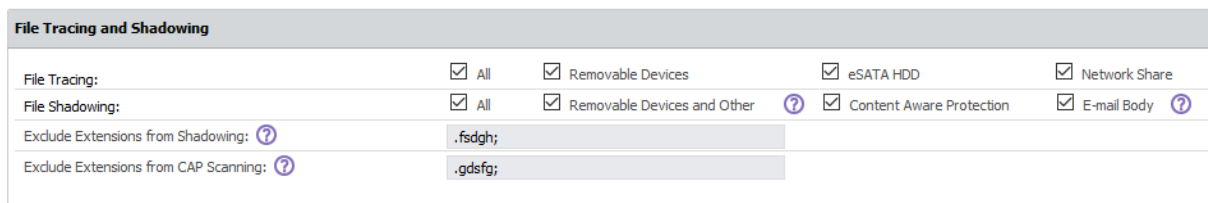
In the example below we set the message as “Message from Endpoint Protector – This device is not allowed!”



Some administrators might want not to display some notifications, while showing others. This can be done by (not) ticking the box for the specific message.

## 6.5. File Tracing

The File Tracing feature allows monitoring of data traffic between protected clients and portable devices. It shows what files were copied, to which location, at what time and by which user. It also shows other actions that took place, such as file renamed, deleted, accessed, modified, etc. It can be enabled from Endpoint Settings > Global settings, or granularly for Groups or Computers.



File Tracing is an essential feature for administrators since they can keep track of all data that is being transferred to and from devices. All traffic is recorded and logged for later auditing. Depending on each administrator’s needs, File Tracing can be enabled on all supported Removable Devices (including or not eSATA HDDs) or Network Shares.

### Note!

Prior to Endpoint Protector 4.5.0.1, the Detect Copy Source option needed to be checked. It is now enabled by default, however, we recommend using the related Endpoint Protector Client versions.

## 6.6. File Shadowing

The File Shadowing feature extends the information provided by File Tracing, creating exact copies of files accessed by users. The creation of shadow copies can be triggered by the following events: file copy, file write, and file read. Events such as file deleted, file renamed, etc. do not trigger the function.

Similar to File Tracing, shadowing of files can be enabled from the Endpoint Settings section. Please note, however, that this feature cannot be used without enabling the File Tracing feature.

Depending on each administrator's needs, File Shadowing can be enabled on all supported Removable Devices (including eSATA HDDs and Network Shares, if selected) or Content Aware Protection (file transfers through various exist points such as online applications, printers, clipboard, etc.) and E-mail Body.

File Shadowing can be disabled for specific file types using the "Exclude Extensions from Shadowing" option.

File Tracing and Shadowing				
File Tracing:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> Removable Devices	<input checked="" type="checkbox"/> eSATA HDD	<input checked="" type="checkbox"/> Network Share
File Shadowing:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> Removable Devices and Other <span>?</span>	<input checked="" type="checkbox"/> Content Aware Protection	<input checked="" type="checkbox"/> E-mail Body <span>?</span>
Exclude Extensions from Shadowing: <span>?</span>	<input type="text" value=".fsdgh;"/>			
Exclude Extensions from CAP Scanning: <span>?</span>	<input type="text" value=".gdsfg;"/>			

Advanced settings such as minimum file size to be shadowed and shadowing upload interval can also be configured.

Default Client Settings			
Log Interval (min):	<input type="text" value="30"/>	Local Log Size (MB):	<input type="text" value="10"/>
Shadow Interval (min):	<input type="text" value="60"/>	Shadow Size (MB):	<input type="text" value="512"/>
Min File Size for Shadowing (KB):	<input type="text" value="0"/>	Max File Size for Shadowing (KB):	<input type="text" value="512"/>
Removable Devices Recovery Folder Maximum Size (MB):	<input type="text" value="5000"/> <span>?</span>	Recovery Folder Retention Period (days):	<input type="text" value="3"/> <span>?</span>
Notifier Language:	<input type="text" value="English"/> <span>?</span>	Use Custom Client Notifications for this Language:	<input type="checkbox"/>
Enable Advanced Printer and MTP Scanning	<input type="checkbox"/>		

### Note!

File Shadowing can be delayed due to network traffic and Endpoint Protector Settings for different computers or file sizes. Shadowed files are usually available after a few minutes.

For large base installations (such as 250-1000 endpoints) we strongly advise to activate File Shadowing for up to 15% of your virtual or hardware appliance total endpoint capacity. (E.g. for an A1000 Hardware Appliance, File Shadowing should be set to a maximum of 150 endpoints for optimal performance).

# 7. Content Aware Protection

This module allows the administrator to setup and enforce strong content filtering policies for selected users, computers, groups or departments and take control over the risks posed by accidental or intentional file transfers of sensitive company data, such as:

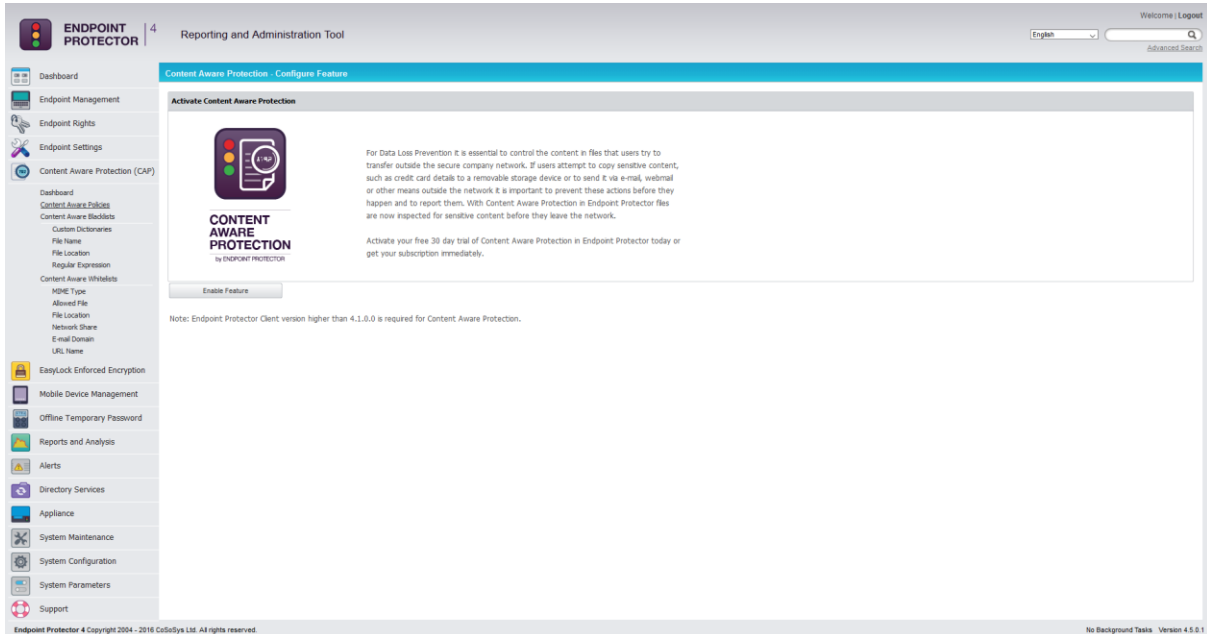
- Personally Identifiable Information (PII): social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.
- Financial and credit card information: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Dinners Club, bank account numbers etc.
- Confidential files: sales and marketing reports, technical documents, accounting documents, customer databases etc.

To prevent sensitive data leakage, Endpoint Protector closely monitors all activity at various exit points:

- Transfers on portable storage and other media devices (USB Drives, external HDDs, CDs, DVDs, SD cards etc.), either directly or through encryption software (e.g. EasyLock)
- Transfers on local networks (Network Share)
- Transfers via Internet (E-mail clients, file sharing application, Web Browsers, Instant Messaging, Social Media)
- Transfers to the cloud (iCloud, Google Drive, Dropbox, Microsoft SkyDrive)
- Transfers through Copy & Paste / Cut & Paste
- Print screens
- Printers and others

## 7.1. Activation of Content Aware Protection

Content Aware Protection comes as an optional feature with Endpoint Protector. The module is displayed but will require a simple activation by pressing the *Enable Feature* button and providing contact details for the Main Administrator.



The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector. The main content area is titled 'Content Aware Protection - Configure Feature' and contains the following elements:

- Activate Content Aware Protection** header with a logo icon.
- Text:** 'For Data Loss Prevention it is essential to control the content in files that users try to transfer outside the secure company network. If users attempt to copy sensitive content, such as credit card details to a removable storage device or to send it via e-mail, webmail or other means outside the network it is important to prevent these actions before they happen and to report them. With Content Aware Protection in Endpoint Protector files are now inspected for sensitive content before they leave the network.'
- Text:** 'Activate your free 30 day trial of Content Aware Protection in Endpoint Protector today or get your subscription immediately.'
- Enable Feature** button.
- Note:** 'Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.'

The left sidebar contains a navigation menu with items such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), EasyLock Enforced Encryption, Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The footer of the interface includes 'Endpoint Protector 4 Copyright 2004 - 2016 CoSibys Ltd. All rights reserved.' and 'No Background Task Version 4.5.0.1'.

### Note!

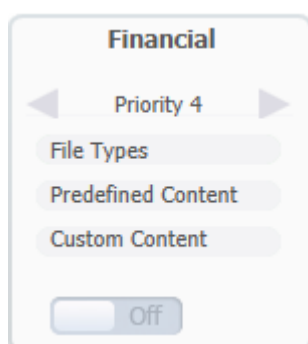
The Content Aware Protection module is separate from Device Control, and requires separate licensing.

## 7.2. Content Aware Policies

Content Aware Policies are sets of rules for sensitive content detection and they enforce file transfers management on selected entities (users, computers, groups, departments). A content aware policy is made up of four elements:

- Policy Type: defines the OS type for which it applies – Windows, Mac OS X or Linux
- Policy Action: defines the type of action to be performed – reporting only or blocking and reporting of sensitive content transfers
- Policy Filter: specifies the content to be detected – it includes file type filtering, predefined content filtering, custom content filtering, file whitelists, regular expressions and domain whitelists.
- Exit Points: establishes the transfer destinations to be monitored

For example, a policy can be setup for the Financial Department of the company to block Excel reports sent via E-mail or to report all transfers of files containing personally identifiable and financial information (e.g. credit card numbers, E-mail, phone numbers, social security numbers etc.).



Additionally, each company can define its own sensitive content data lists as Custom Content Dictionaries corresponding to their specific domain of activity, targeted industry and roles. To ease this task, the Content Aware Protection module comes with a Predefined Content Dictionary that covers the most used sets of confidential terms and expressions.

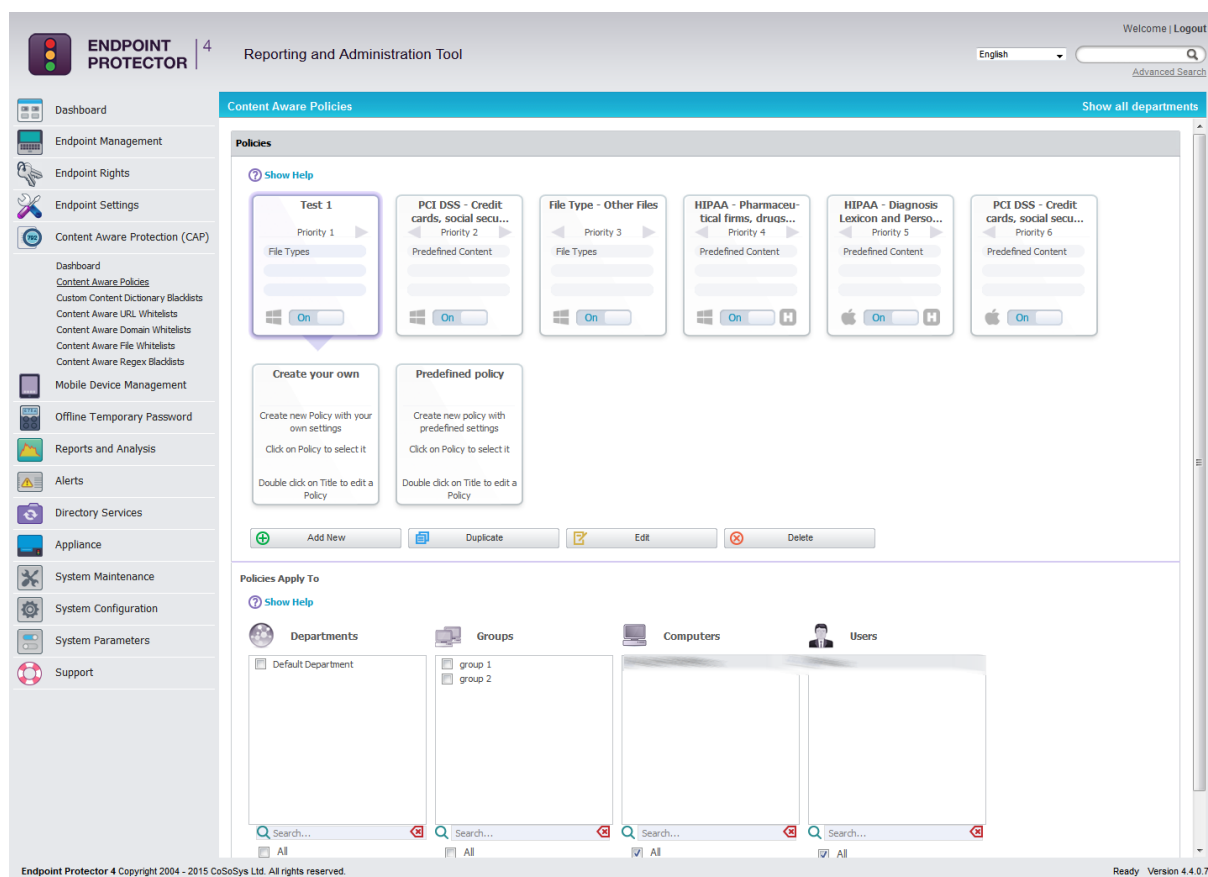
### Note!

Content Aware Policies also apply to File Whitelist (Endpoint Rights > File Whitelist). This means that all files that were previously whitelisted will be inspected for sensitive content detection, reported and / or blocked, according to the defined policy.

Exactly like Device Control policies, the Content Aware policies continue to be enforced on a computer even after it is disconnected from the company network.

### 7.2.1. Creating new policies

The administrator can easily create and manage Content Aware Policies from the Content Aware Protection > Content Aware Policies submenu option.



The available actions are: **Add New**, **Duplicate**, **Edit** and **Delete**. A new policy can be created also by clicking on the **Create your own** policy icon. An existing policy can be edited also by double-clicking the upper part of the policy icon.

By selecting a policy, the departments, groups, computers and users on which the selected policy applies, will be highlighted for an easier policy management. The administrator can then uncheck previously enabled entities for monitoring or check new ones. All the changes performed on the page are applied after clicking **Save**.

## 7.2.2. Predefined policies

A second option is to use the *Predefined policy* button. This redirects the administrator to two lists of predefined policies that come with Action set to “Block and Report” by default, for both Windows and OS X. The administrator can select by the description a policy of interest and press the “Create Policy” button for it to be displayed in the list of active policies.

These policies are named as per the information found in the column “Name” and have different Threshold values defined, as per the information found inside the column “Threshold”.

The screenshot shows the 'Content Aware Policies' section of the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main area displays a table of predefined policies for Windows and Mac OS X. The table has three columns: Name, Description, and Threshold. The 'Create Policy' button is visible at the bottom of the table.

Name	Description	Threshold
<input checked="" type="radio"/> File Type - Archive Files	Block archive file transfers to all destinations	3 Global
<input type="radio"/> File Type - Graphic Files	Block graphic file transfers to all destinations	3 Global
<input type="radio"/> File Type - Office Files	Block office file transfers to all destinations	3 Global
<input type="radio"/> File Type - Other Files	Block other file transfers to all destinations	3 Global
<input type="radio"/> File Type - Programming Files	Block programming file transfers to all destinations	3 Global
<input type="radio"/> File Type - Media Files	Block media file transfers to all destinations	3 Global
<input type="radio"/> HIPAA - Diagnosis Lexicon	Block ICD-9 codes and diagnosis lexicon transfers to all destinations	5 Global
<input type="radio"/> HIPAA - Diagnosis Lexicon and Personal Information	Block ICD-9 codes, diagnosis lexicon and personally identifiable information transfers to all destinations	10 Global
<input type="radio"/> HIPAA - Personal Information	Block personally identifiable information transfers to all destinations	5 Global
<input type="radio"/> HIPAA - Pharmaceutical firms	Block FDA recognised pharmaceutical firm transfers to all destinations	5 Global
<input type="radio"/> HIPAA - Pharmaceutical firms, drugs and diagnosis	Block FDA recognised pharmaceutical drug, firm and ICD diagnosis lexicon transfers to all destinations	10 Global
<input type="radio"/> HIPAA - Pharmaceutical firms and Personal Information	Block FDA recognised pharmaceutical firm and personally identifiable information transfers to all destinations	10 Global
<input type="radio"/> HIPAA - Prescription Drugs	Block FDA recognised prescription drug and personally identifiable information transfers to all destinations	5 Global
<input type="radio"/> HIPAA - Prescription Drugs and Personal Information	Block FDA recognised prescription drug and personally identifiable information transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit Cards	Block credit number transfers to all destinations	5 Global
<input type="radio"/> PCI DSS - Credit Cards and e-mail addresses	Block credit card number and e-mail address transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit Cards and IBAN	Block credit card number and IBAN transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit Cards and phone numbers	Block credit card number and telephone number transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit Cards and postal addresses (US)	Block credit card number and postal address (US) transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit Cards and Social Security Numbers	Block credit card number and social security number transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit cards, social security numbers and addresses (US)	Block credit card number, social security number and postal address (US) transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit cards, social security numbers and e-mail addresses	Block credit card number, social security number and email address transfers to all destinations	10 Global
<input type="radio"/> PCI DSS - Credit cards, social security numbers and phone numbers	Block credit card number, social security number and phone number transfers to all destinations	10 Global

## 7.2.3. Priorities for Content Aware Policies

One or more Content Aware Policy can be enforced on the same computer, user, group or department. To avoid any conflicts between the applied rules, a prioritization of policies is performed through a left-to-right ordering. The leftmost policy has the highest priority (Priority 1), while the rightmost policy has the lowest priority. Changing priorities for one or more policies can be performed by moving the policy to the right or to the left with a simple click on the left arrow for higher priority or on the right arrow for lower priority.

### 7.2.4. How Content Aware Policies Work

Content Aware Protection is a very versatile tool, where granular implementation of the desired actions regarding report and/or block and report of files can be performed.

A Content Aware Policy is a set of rules for reporting or blocking & reporting the selected information. All the other options left unchecked will be considered as Ignored by Endpoint Protector.

When applying two policies to the same PC, it is possible to block one type of file, for example PNG files, when they are uploaded through Mozilla Firefox, while with a second policy to report only PNG files when they are uploaded through Internet Explorer. In the same way it is possible to report only files that contain confidential words from a selected dictionary that are sent through Skype, while with the second policy to block the same files if they are sent through Yahoo Messenger. Similarly, it is possible to create combinations that block a file type or a file that contains predefined content/custom content/regular expression for one application, while letting it through and report it only for another.

The following rules are used in the application of one or more Content Aware Policies on a computer/user/group/department for each separately selected item (e.g. a specific file type, predefined information or a custom content dictionary):

Policy A with Priority 1	Policy B with Priority 2	Policy C with Priority 3	Endpoint Protector Action
IGNORED	IGNORED	IGNORED	Information will not be blocked or reported.
IGNORED	IGNORED	<i>REPORTED</i>	Information will be reported.
IGNORED	<i>REPORTED</i>	<i>REPORTED</i>	Information will be reported.
<i>REPORTED</i>	<i>REPORTED</i>	<i>REPORTED</i>	Information will be reported.
IGNORED	IGNORED	<b>BLOCKED</b>	Information will be blocked.
IGNORED	<b>BLOCKED</b>	<b>BLOCKED</b>	Information will be blocked.
<b>BLOCKED</b>	<b>BLOCKED</b>	<b>BLOCKED</b>	Information will be blocked.
IGNORED	<i>REPORTED</i>	<b>BLOCKED</b>	Information will be reported.
IGNORED	<b>BLOCKED</b>	<i>REPORTED</i>	Information will be blocked.



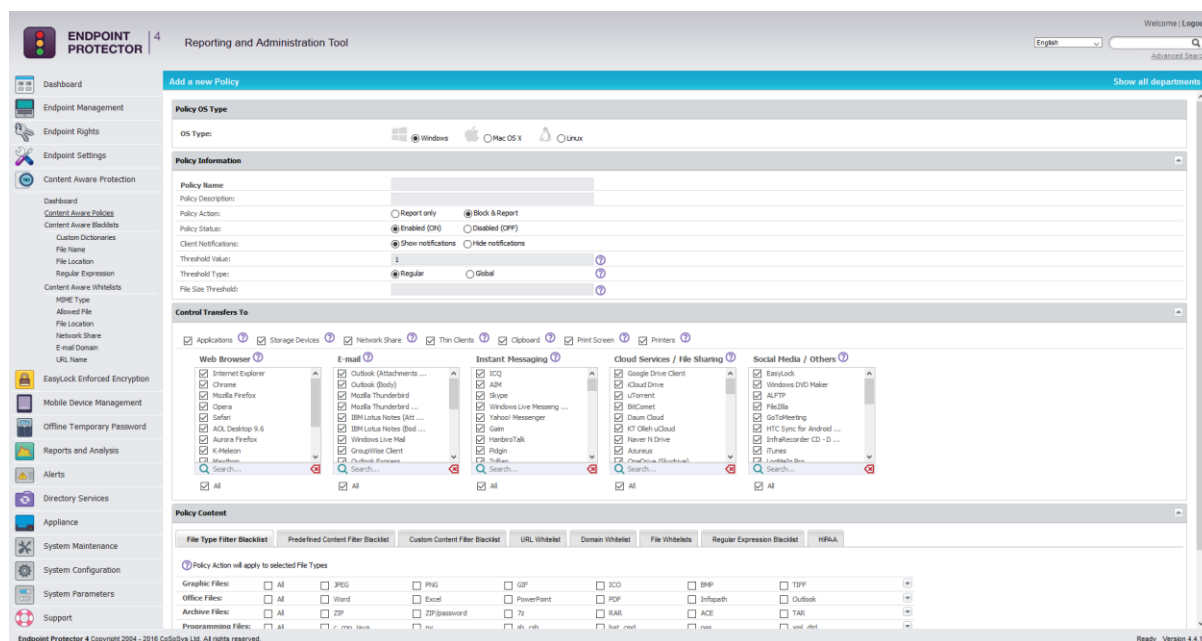
<i>REPORTED</i>	IGNORED	<b>BLOCKED</b>	Information will be reported.
<b>BLOCKED</b>	IGNORED	<i>REPORTED</i>	Information will be blocked.
<i>REPORTED</i>	<b>BLOCKED</b>	IGNORED	Information will be reported.
<b>BLOCKED</b>	<i>REPORTED</i>	IGNORED	Information will be blocked.

## Note!

The information left unchecked when creating a policy will be considered as Ignored by Endpoint Protector and **NOT AS ALLOWED**.

### 7.2.5. Setting up Content Aware Policies

To setup a Content Aware Policy, go to Content Aware Protection > Content Aware Policies and click on the Create Your Own Policy icon or push the *Add Policy* button. This will open the Add a new Policy window, which will allow setting the parameters of the newly created policy.



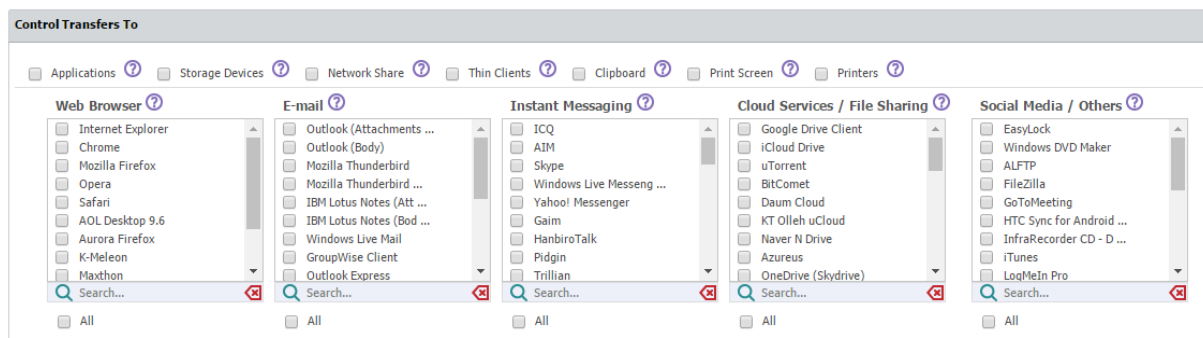
A policy can be enforced to detect and report all transfers of sensitive content data and/or block all transfers:

**Block & Report**    **Report only**

## Note!

We recommend using the “Report only” action initially to detect but not block data transfers. This way, no activity will be interrupted and you can gain a better view of data use across your network.

The next step in defining a policy is selecting the transfer destinations to be monitored.



Below is the main categories list of transfer destinations to control:

- Applications (Web Browser, E-mail, Instant Messaging, etc.)

Type	List of Applications
Web Browsers	Internet Explorer, Mozilla Firefox, Chrome, Opera, Safari, SeaMonkey, Maxthon, AOL Destop 9.6, K-Meleon, Aurora Firefox, Adobe Flash Player*
E-mail Clients	Microsoft Office Outlook, Mozilla Thunderbird, Windows Live Mail, Outlook Express, Windows Mail, AOL Mail, Opera Mail, SeaMonkey Mail, Courier, IBM Lotus Notes, GroupWise Client,
Instant Messaging	AIM, eBuddy, MySpace IM, ICQ, Google Talk, Skype, Windows Live Messenger, Yahoo! Messenger, mIRC, Trillian, MyChat, LingoWare, Chit Chat For Facebook, Nimbuzz, Facebook Messenger, Microsoft Communicator 2007, Facemoods, Gaim, LAN Chat Enterprise, OpenTalk, TurboIRC, WinSent Messenger, Pink Notes Plus, fTalk, XChat, ooVoo, TweetDeck, Pidgin Instant Messenger, NateOn Messenger, QQ International, Twihirl, Daum MyPeople, Mail.Ru
Cloud Services / File Sharing	Google Drive Client, iCloud, Dropbox, Microsoft SkyDrive, eMule, Kazaa, Shareaza, Morpheus, eDonkey, DC++, BitTorrent, Azureus, BitComet, uTorrent, iMesh, Daum Cloud, KT Olleh uCloud, Naver N Drive, Microsoft Skydrive client, Limewire, FTP Command, ownCloud client, Pogoplug Backup, Pruna P2P, Sendspace, Evernote, FileCloud Sync client, GitHub, Remote Desktop Connection, Mega, Yandex Disk
Social Media / Others	InfraRecorder, iTunes, Nokia PC Suite 2008 / 2011, Samsung Kies, Sony Ericsson PC Companion, TeamViewer, HTC Sync for Android phones, Total Commander, LogMeIn, EasyLock, GoToMeeting, Windows DVD Maker, FileZilla, ALFTP, GoToMeeting, Windows Store Apps

### Note!

Adobe Flash Player must be checked inside the Web Browser category in order to block sites that use Adobe Flash Active X.

- Storage Devices (all controlled device types; the list can be viewed at System Parameters > Device Types > Content Aware Protection)

### Note!

For Storage Devices for Windows policies, Endpoint Protector will monitor file transfers both to and from removable media.

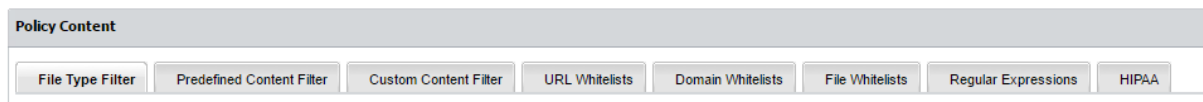
- Network Share

### Note!

For Network Share for Mac OS X, Endpoint Protector will report all the events for “Report Only” policies. For “Block & Report” policies the transfer from a Local Share towards the Local Disk, Controlled Storage Device Types and Controlled Applications is blocked.

- Thin Clients
- Clipboard (refers to all content captured through Copy & Paste or Cut & Paste operations)
- Print Screen (refers to the screen capture options)
- Printers (refers to both local and network shared printers)

The last step in defining a new policy consists in selecting the content to be detect and the type of filters.



The File Type Filter contains a list of supported file types grouped in six categories:

- Graphic Files: JPEG, PNG, GIF, ICO, BMP, TIFF, EPS, CorelDraw etc.
- Office Files: Word (.DOC, .DOCX), Excel (.XLS, .XLSX), PowerPoint (.PPT, .PPTX), PDF, Infopath (.XSN), RTF, OneNote (.ONE), Outlook (.PST, .OST) etc.
- Archive Files: ZIP, 7z, RAR, ACE, TAR, XAR etc.
- Programming Files: C, CPP, JAVA, PY, SH, CSH, BAT, CMD, PAS, XML, DTD, TEX, F, PHP, Ruby (.RB), Perl (.PL) etc.
- Media Files: MP3, M4A, WAV, WMA, AVI, AIF, M3U, MPA etc.
- Other Files: TXT, EXE, SYS, DLL, SO, DRM, SolidWorks, Nasca-Drm, Ideas-3D-CAD, etc.

For each category, the most common file types are displayed. To be able to view and select more file types, click on the More File Types option at the end of each file type enumeration.

File Type Filter	Predefined Content Filter	Custom Content Filter	URL Whitelists	Domain Whitelists			
Policy Action will apply to selected File Types							
Graphic Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> JPEG	<input checked="" type="checkbox"/> PNG	<input checked="" type="checkbox"/> GIF	<input checked="" type="checkbox"/> ICO	<input checked="" type="checkbox"/> BMP	<input checked="" type="checkbox"/> TIFF <a href="#">More File Types</a>
Office Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> Word	<input checked="" type="checkbox"/> Excel	<input checked="" type="checkbox"/> PowerPoint	<input checked="" type="checkbox"/> PDF	<input checked="" type="checkbox"/> Infopath	<input checked="" type="checkbox"/> Outlook <a href="#">More File Types</a>
Archive Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> ZIP	<input checked="" type="checkbox"/> ZIP/password	<input checked="" type="checkbox"/> 7z	<input checked="" type="checkbox"/> RAR	<input checked="" type="checkbox"/> ACE	<input checked="" type="checkbox"/> TAR <a href="#">More File Types</a>
Programming Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> c, cpp, java	<input checked="" type="checkbox"/> py	<input checked="" type="checkbox"/> sh, csh	<input checked="" type="checkbox"/> bat, cmd	<input checked="" type="checkbox"/> pas	<input checked="" type="checkbox"/> xml, dtd <a href="#">More File Types</a>
Other Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> AutoCAD files	<input checked="" type="checkbox"/> Text files	<input checked="" type="checkbox"/> DRM Files	<input checked="" type="checkbox"/> exe, sys, dll	<input checked="" type="checkbox"/> so	<input checked="" type="checkbox"/> Unidentified <a href="#">More File Types</a>
Media Files:	<input checked="" type="checkbox"/> All	<input checked="" type="checkbox"/> mov	<input checked="" type="checkbox"/> mp3	<input checked="" type="checkbox"/> m4a	<input checked="" type="checkbox"/> wav	<input checked="" type="checkbox"/> wma	<input checked="" type="checkbox"/> avi <a href="#">More File Types</a>
<input checked="" type="button" value="Save"/> <input type="button" value="Back"/> <input type="button" value="Delete"/>							

## Note!

As many files (e.g. Programming Files) are actually .TXT files, we recommend more precaution when selecting this file type to avoid any undesired effects.

The “Predefined Content Filter” displays a list of predefined items to detect, from credit card information to Personal Identifiable Information. The Content Aware Protection module offers the option of Localization, meaning that you can select specific formats for a list of countries for information such as Driving License, ID, Phone Number and Social Security Number. By leaving unchecked this option, all formats will be detected by the Content Aware Protection agent.

File Type Filter Blacklist	Predefined Content Filter Blacklist	Custom Content Filter Blacklist	URL Whitelist	Domain Whitelist	File Whitelists	Regular Expression Blacklist	HIPAA
Policy Action will apply to selected Predefined Content for ALL File Types (regardless of the selected File Type Filter).							
The below filters help ensure compliance with various regulations like PCI DSS and HIPAA.							
<input checked="" type="checkbox"/> Credit Cards:		<input checked="" type="checkbox"/> Amex <input checked="" type="checkbox"/> Diners <input checked="" type="checkbox"/> Discover <input checked="" type="checkbox"/> JCB <input checked="" type="checkbox"/> Mastercard <input checked="" type="checkbox"/> Visa					
<input checked="" type="checkbox"/> Personal Identifiable Information:		<input checked="" type="checkbox"/> IBAN <input checked="" type="checkbox"/> Date <input checked="" type="checkbox"/> E-mail <input checked="" type="checkbox"/> Address <a href="#">?</a>					
<input checked="" type="checkbox"/> Country Specific:		<input checked="" type="checkbox"/> SSN <input checked="" type="checkbox"/> ID <input checked="" type="checkbox"/> Passport <input checked="" type="checkbox"/> Phone Number <input checked="" type="checkbox"/> Tax ID <input checked="" type="checkbox"/> Driving License <input checked="" type="checkbox"/> Health Insurance Number					
<input checked="" type="checkbox"/> SSN:		<input checked="" type="checkbox"/> Austria <input checked="" type="checkbox"/> Canada <input checked="" type="checkbox"/> France <input checked="" type="checkbox"/> Germany <input checked="" type="checkbox"/> Japan <input checked="" type="checkbox"/> Korea <input checked="" type="checkbox"/> Netherlands <input checked="" type="checkbox"/> Poland <input checked="" type="checkbox"/> Romania <input checked="" type="checkbox"/> Spain <input checked="" type="checkbox"/> Switzerland <input checked="" type="checkbox"/>					
<input checked="" type="checkbox"/> ID:		<input checked="" type="checkbox"/> Germany <input checked="" type="checkbox"/> Poland <input checked="" type="checkbox"/> Singapore <input checked="" type="checkbox"/> South Africa <input checked="" type="checkbox"/> Turkey <input checked="" type="checkbox"/> China ( <input checked="" type="checkbox"/> Mainland <input checked="" type="checkbox"/> Macau <input checked="" type="checkbox"/> Hong Kong)					
<input checked="" type="checkbox"/> Passport:		<input checked="" type="checkbox"/> Japan <input checked="" type="checkbox"/> Korea <input checked="" type="checkbox"/> China ( <input checked="" type="checkbox"/> Mainland <input checked="" type="checkbox"/> Macau <input checked="" type="checkbox"/> Hong Kong)					
<input checked="" type="checkbox"/> Phone Number:		<input checked="" type="checkbox"/> International <input checked="" type="checkbox"/> Japan <input checked="" type="checkbox"/> Korea <input checked="" type="checkbox"/> Turkey <input checked="" type="checkbox"/> China ( <input checked="" type="checkbox"/> Mainland <input checked="" type="checkbox"/> Macau <input checked="" type="checkbox"/> Hong Kong)					
<input checked="" type="checkbox"/> Tax ID:		<input checked="" type="checkbox"/> International <input checked="" type="checkbox"/> Italy <input checked="" type="checkbox"/> Poland <input checked="" type="checkbox"/> United States					
<input checked="" type="checkbox"/> Driving License:		<input checked="" type="checkbox"/> Korea					
<input checked="" type="checkbox"/> Health Insurance Number:		<input checked="" type="checkbox"/> Australia <input checked="" type="checkbox"/> Korea <input checked="" type="checkbox"/> United Kingdom					
<input checked="" type="checkbox"/> Internet Protocol Addresses:		<input checked="" type="checkbox"/> Internet Protocol Version 4 (IPv4) <input checked="" type="checkbox"/> Internet Protocol Version 6 (IPv6)					
<input checked="" type="button" value="Save"/> <input type="button" value="Back"/> <input type="button" value="Delete"/>							

The “Custom Content Filter” displays a list of Content Aware dictionaries. By selecting one or more dictionaries, the Content Aware Protection agent will detect any occurrence of one, more or all terms contained in the Dictionary list.

File Type Filter    Predefined Content Filter    **Custom Content Filter**    URL Whitelists    Domain Whitelists

**?** Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).

Case Sensitive     Whole Words Only

All     Confidential Dictionary

To add, delete and edit Dictionaries: [Go to Custom Content Dictionaries](#)

By checking the Case Sensitive option, the agent can differentiate the uppercase and lowercase letters when inspecting the content.

If the Whole Words Only option is marked, terms from the inspected content are detected only if they are an identical match with the ones that appear in the dictionary (e.g. „age“ is in the Dictionary; variations like „aged“, „agent“, „agency“ etc. won't be reported/blocked).

The “URL Whitelist” displays a list of URL whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan uploads or attachments to the web addresses present in the whitelists. Whitelisting works for Internet Explorer.

File Type Filter    Predefined Content Filter    Custom Content Filter    **URL Whitelists**    Domain Whitelists

**?** Policy Action will apply only to the following applications, if selected: Internet Explorer

All     Default URL Whitelist

To add, delete and edit URL Whitelists: [Go to Content Aware URL Whitelists](#)

The “Domain Whitelist” displays a list of domain whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan mails sent to the recipients or domains present in the whitelists. Whitelisting works for Microsoft Outlook and Mozilla Thunderbird.

**Policy Content**

File Type Filter    Predefined Content Filter    Custom Content Filter    URL Whitelists    **Domain Whitelists**    Regular Expressions

**?** Policy Action will apply only to the following applications, if selected: Outlook and Thunderbird

All     Default Domain Whitelist

To add, delete and edit Domain Whitelists: [Go to Content Domain URL Whitelists](#)

The “Regular Expressions” shows the list of the created regular expressions and the administrator can select up to five (5) expressions.

**Policy Content**

File Type Filter    Predefined Content Filter    Custom Content Filter    URL Whitelists    Domain Whitelists    **Regular Expressions**

**?** Policy Action will apply to selected Custom Content for ALL File Types (regardless of the selected File Type Filter).

All     Default Regular Expression

To add, delete and edit Regular Expression: [Go to Regular Expressions](#)

Once a policy is created, it will be displayed inside the Policies List. To enforce a content aware policy inside the network, one must select the specific policy that they want to apply by clicking on it and check the corresponding boxes to the network entity on which they want to apply the content rules. If a Content Aware Policy was already enforced on a computer, user, group or department, when clicking on it, the corresponding network entities on which it was applied will be highlighted.

The administrator can be notified of each occurrence of an event described in a newly created policy by setting up a Content Aware alert for that specific policy from System Alerts -> Content Aware Alerts.

### 7.2.6. The Threshold Number


A powerful Content Aware Policy option consists of setting up a threshold. A threshold is defined by the maximum number of allowed content violation for a file transfer. This means that the policy does not block or report a file transfer.

There are two types of thresholds to choose from: Regular or Global.

Threshold Value:	<input type="text" value="1"/>	
Threshold Type:	<input checked="" type="radio"/> Regular	<input type="radio"/> Global 

Suppose that you have set up a "Block & Report" policy on the transfer of Social Security Numbers (SSN) on some types of Internet browsers. A Regular Threshold setup of four (4) will block all transfers - on those browsers - which contain four or more individual SSN numbers, but not 1, 2, 3 x SSN appearances. A set value of four (4) will permit and only report those transfers.

In contrast to the Regular Threshold which blocks 4 or more threats of the same type, the Global Threshold blocks 4 or more threats of different types combined. In another example, two (2) threats, one being a Social Security Number and the other being a Phone number, will not be blocked by a policy with a Regular Threshold of 2, only by one with a Global Threshold. On the other hand, two (2) Social Security Numbers will be blocked by policies with both types of thresholds set at two (2).

The info button  next to the options provides more examples related to the differences between the Regular and the Global Threshold.

#### Note!

The Threshold option applies only to multiple filters, including Predefined Content, Custom Content and Regular Expressions. As a general rule, it is recommended that "Block & Report" policies that use the Threshold should be placed with higher priority than "Report Only" policies.

## 7.3. File Size Threshold

Not linked to the Regular and Global Threshold mentioned above, The File Size Threshold value defines the size (in MB) starting from which the file transfer is either blocked or reported.

File Size Threshold:

99



To **Enable** the File Size Threshold in a Policy, a value bigger than 0 must be set.  
To **Disable** the File Size Threshold in a Policy, 0 or no value must be set.




### Note!

If a File Size Threshold is set, it will be applied to the whole policy, regardless of what file types or custom contents are checked inside the policy.

The value used in the File Size Threshold must be a positive, whole number.

## 7.4. Custom Content Dictionary Blacklists




Custom Content Dictionary Blacklists are custom defined lists of terms and expressions to be detected as sensitive content by Endpoint Protector. The list of custom content dictionaries is available under Content Aware Protection -> Custom Content Dictionary Blacklists.


The available actions for each dictionary are: **Edit**, **Export Dictionary** and **Delete**.   

A new dictionary can be created by clicking on the "Add New" button. To populate the content of a newly created dictionary, items of at least three characters might be entered either manually separated by comma, semicolon or new line or directly imported from an Excel file by pressing the Import Dictionary button.

An example of a Custom Content Dictionary with financial terms is shown below:

**List of Dictionaries**

Dictionary Name ^	Dictionary Description	Created at	Created by	Modified at	Modified by	Words/Items	Actions
Confidential Dictionary	List of Confidential Terms		root		root	102	  

 Add New

---






**Dictionary Information**

Dictionary Name: Confidential Dictionary

Dictionary Description: List of Confidential Terms

Dictionary Content (separated by new line, comma or semicolon):

Agak Rahasia  
 Arme intern od. dienstlich/Interne au service  
 Begrenset  
 Beperkte Verspreiding  
 Bizalmas  
 Classified information  
 Clearance  
 Confidential  
 Confidential  
 Confidential défense  
 Diffusion restreinte

 Save
  Import Dictionary
  Export As
  Delete
  Back

Once a new dictionary is created, it will be automatically displayed inside the Custom Content tab when creating a new or editing an existing Content Aware Policy. The Content Aware Protection module comes with a predefined set of dictionaries.

## 7.5. Custom Content Filename Blacklists




























Custom Content Filename Blacklists are custom defined lists of filenames (with extensions included) to be detected by Endpoint Protector. The list of custom content filenames is available under Content Aware Protection -> Custom Content Filename Blacklists.


The available actions for each dictionary are: **Edit**, **Export** and **Delete**.   

A new filename blacklist can be created by clicking the "Add New" button. To populate the content of a newly created filename blacklist, items of at least two characters can be entered, separated by a comma, semicolon or a new line. Also, items can be directly imported from an Excel file by pressing the "Import List" button.

**Custom Content Filename Blacklists**

**List of Filename Blacklists**

Dictionary Name ^	Dictionary Description	Created at	Created by	Modified at	Modified by	Words/Items	Actions
asa	asa	15 October 2015 17:18	root	17 November 2015 11:14	root	3	  
Cris9	For Test	17 November 2015 10:08	root	17 November 2015 11:06	root	10	  
marus	do not delete me	6 November 2015 12:31	root	17 November 2015 11:15	root	3	  
test	test	15 October 2015 12:07	root	15 October 2015 17:27	avidu	3	  
Test1	Test1 Description	15 October 2015 10:41	root	15 October 2015 17:17	avidu	7	  
test123	test2	18 November 2015 13:41	root	18 November 2015 13:41	root	0	  
test2	test2	18 October 2015 10:39	root	18 October 2015 10:39	root	1	  
test3	test3	18 October 2015 10:46	root	18 October 2015 10:46	root	1	  
test4	test4	18 October 2015 10:51	root	18 October 2015 10:51	root	15	  

 Add New






---

**Filename Blacklist Information**

Filename Blacklist Name: FileName Blacklist 1

Filename Blacklist Description: Test

example.pdf  
 .app

 Save
  Import List
  Export As
  Delete
  Back



Once a new filename blacklist is created, it will automatically be displayed inside the Custom Content Filter Blacklist tab when creating a new or editing an existing Content Aware Policy.

### Note!

The Filename Blacklists work only for Block & Report type of Content Aware Policies.

The Case Sensitive and Whole Words Only checkboxes do not apply to Filename Blacklists.

Examples of how Filename Blacklists work:

#### Example 1

If "example.pdf" filename is used then all files that end in example.pdf will be blocked (i.e. example.pdf, myexample.pdf, test1example.pdf).

#### Example 2

If ".epp" extension is used then all files that have the .epp extension will be blocked (i.e. test.epp, mail.epp, 123.epp).

## 7.6. Content Aware URL Whitelists

URL Whitelists are custom defined lists of web addresses where uploading of confidential information will be allowed by the Endpoint Protector. This feature works on Internet Explorer.

The defined URL should not only contain the name and the domain and not any prefixes like www.\*, www2.\* or en.\*.

Example: endpointprotector.com (not www.endpointprotector.com)

Content Aware URL Whitelists Show all departments

URL Whitelist Name ^	URL Whitelist Description	Created at	Created by	Modified at	Modified by	Words/Items	Actions
Default URL Whitelist	Default URL Whitelist	root	root	root	root	0	

+ Add New

---

**Edit Dictionary Information**

URL Whitelist Name:

URL Whitelist Description:

URL Whitelist Content (separated by new line, comma or semicolon):

Save

 Export As
 Delete

Once a new URL whitelist is added, it will be automatically displayed inside the URL Whitelists tab.

## 7.7. Content Aware File Whitelists

Content Aware File Whitelists are custom groups of files which the administrator wishes to exclude from the enforced Content Aware policies.

The screenshot displays the 'Content Aware File Whitelists' management interface. It features a sidebar with navigation options such as Dashboard, Endpoint Management, and Content Aware Protection (CAP). The main content area is divided into three sections:

- File Whitelists:** A table listing existing whitelists.
 

File Whitelist Name	File Whitelist Description	Created at	Created by	Modified at	Modified by	Files	Actions
Default File Whitelist	Default File Whitelist		root		root	0	[Edit] [Delete]
Test		20 February 2015 14:35	root	20 February 2015 14:35	root	0	[Edit] [Delete]
Test 1		20 February 2015 14:35	root	20 February 2015 14:35	root	3	[Edit] [Delete]
- File Whitelist - Information:** A form for adding a new whitelist, with fields for 'File Whitelist Name' (Default File Whitelist) and 'File Whitelist Description' (Default File Whitelist). A 'Save Whitelist' button is present.
- File Whitelist - Manage Files:** A section for managing files associated with the selected whitelist. It includes a 'Results' table:
 

All	File Name	Hash	File Extension	File Size	Modified by	Last Modified	Actions
<input type="checkbox"/>	Confidential.docx	c44f91a2ba2d2be91114ea6294d9bc3e	docx	11 kB	root	20 February 2015 14:35	[Delete]
<input type="checkbox"/>	image001.png	de946a8a5f672d5452a0754fbbd8aec	png	15 kB	root	20 February 2015 14:35	[Delete]
<input type="checkbox"/>	photo.PNG	4a7a785272085096215b89ec67a59808	PNG	107 kB	root	20 February 2015 14:35	[Delete]

 Below the table are buttons for 'Add Files To Whitelist', 'Upload Files', 'Remove From Whitelist', and 'Delete Selected'.

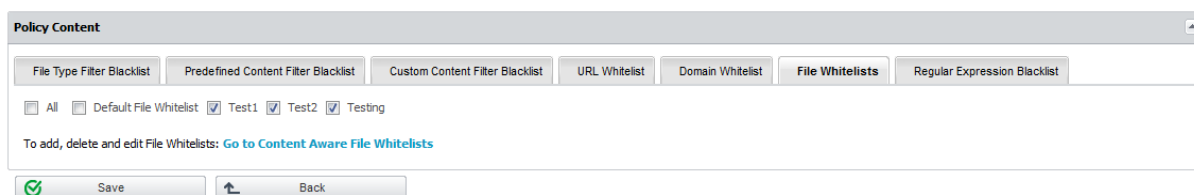
The first step requires the files to be uploaded on the Endpoint Protector application by using the **Upload Files** button.

The second step is to use **Add New Whitelist** which will prompt with an empty File Whitelist – Information section. After the name and description of the whitelist are set, they can be saved using the **Save Whitelist** button.

After the File Whitelists section is populated with the wanted lists, the administrator can use the **Edit** [Edit] button to select one of the lists - and enable the selection of one or multiple files from the Manage Files section - and populate it with files recently uploaded.

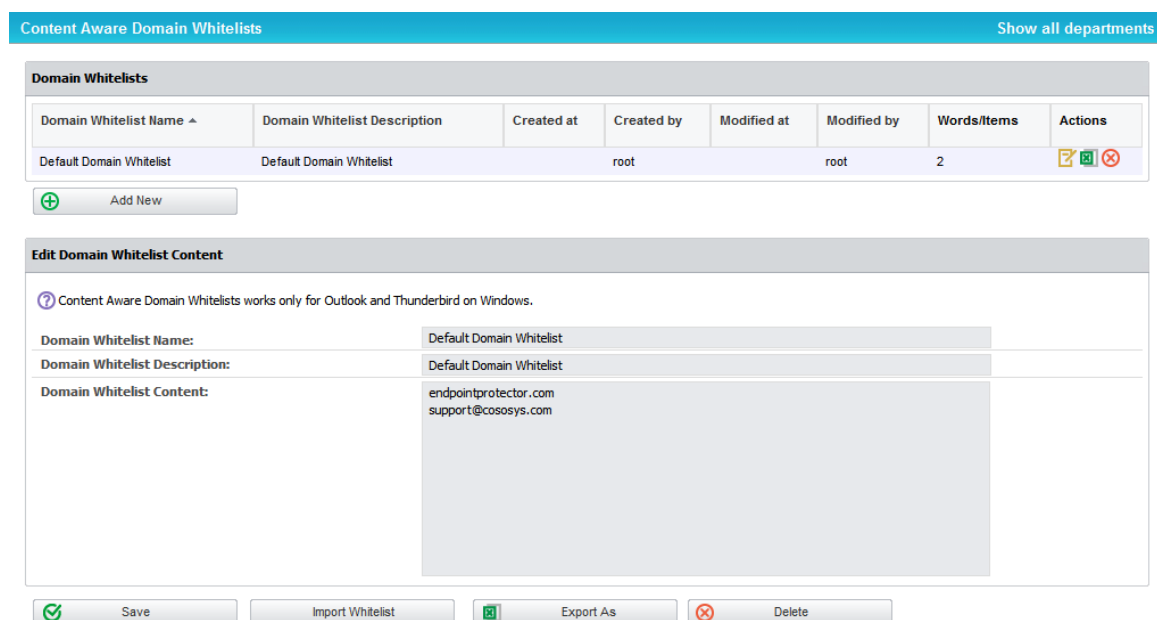
The final step required is to press the button **Add Files To Whitelist**, which will save all the modifications made to the most recently edited list.

From here on, navigating to the below shown menu will allow an administrator to whitelist one or multiple file whitelists for any Content Aware policy enforced on the network.



## 7.8. Content Aware Domain Whitelists

Domain Whitelists are custom defined e-mail addresses to which sending of confidential information will be allowed by the Endpoint Protector. This feature works on Microsoft Outlook and Mozilla Thunderbird.



Once a new domain whitelist is added, it will be automatically displayed inside the Domain Whitelists tab.

## 7.9. Network Share Whitelists

Network Share Whitelists are custom defined lists of network share addresses where transfers of confidential information will be allowed by the Endpoint Protector.

In order for this feature to work accordingly, the Network Share must be set to Allow Access and Scan Network Share must be checked inside a Content Aware Policy.

**Network Share Whitelists** Show all departments

**Results**

Network Share Whitelist Name ^	Whitelist Description	Created at	Created by	Modified at	Modified by	Items	Actions
Default Network Share Whitelist	Default Network Share Whitelist	24 November 2015 13:01	root	24 November 2015 15:28	root	Default Network Share Whitelist	
Test	Share	24 November 2015 13:06	root	24 November 2015 13:06	root	192.168.0.1\public\users\test fileserver\documents\examples	
test2	share	24 November 2015 13:06	root	24 November 2015 13:06	root		

3 results [ 10 per page]

[Add New](#)

**Network Share Information**

Network Share Whitelist Name:

Network Share Whitelist Description:

Network Share Whitelist Content (separated by new line, comma or semicolon):

Network Share Whitelist Computers:

- CRISTIB
- Test's iMac

The server name or IP address can be used to define a network share path within a whitelist. The network share path should not begin with backslashes (\\).

Examples: 192.168.0.1\public\users\test; fileserver\documents\example

Upon creating a new or editing an already existing whitelist, it must be assigned to the desired computers by marking them inside of each whitelist.

## 7.10. Content Aware Regex Blacklists

By definition, Regular Expressions are sequences of characters that form a search pattern, mainly for use in pattern matching with strings. An administrator can create a regular expression in order to find a certain recurrence in the data that is transferred across the protected network.

**Content Aware Regular Expressions** Show all departments

**Regular Expressions**

Name ^	Description	Expression	Created at	Created by	Modified at	Modified by	Actions
Default Regular Expression	Expression To Verify An E-mail Address	[-0-9a-zA-Z.+_]+@[[-0-9a-zA-Z.+_]+\.[a-zA-Z]{2,4}		root		root	

[Add New](#)

**Edit Regular Expression Information**

Regular Expression Name:

Regular Expression Description:

Regular Expression Content:

Example that matches an e-mail: **[-0-9a-zA-Z.+\_]+@[[-0-9a-zA-Z.+\_]+\.[a-zA-Z]{2,4}**

Example that matches an IP: **(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(\.|(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)){3}**

### Note!

If possible, avoid using Regular Expressions, as their complexity typically increases the resources usage. Using a large number of regular expressions as filtering criteria typically increases CPU usage. Also, improper regular expressions or improper use can have negative implications.

This feature is provided “as is” and requires advanced knowledge of the Regular Expression syntax.

The regular expressions feature is provided with no direct support and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.

Regular Expressions can be tested for accuracy. Insert into the “Add Content for Testing Regular Expression” box a general example of something on which the regex applies to, and press the “Test” button. If the Regular Expression has no errors inside of it, then the same content should appear into the “Matched Regular Expression” box, as shown below:

Edit Regular Expression Information	
Regular Expression Name:	Default Regular Expression
Regular Expression Description:	Expression To Verify An E-mail Address
Regular Expression Content:	<code>[-0-9a-zA-Z. +_]+@[-0-9a-zA-Z. +_]+\.[a-zA-Z]{2,4}</code>
Add Content For Testing Regular Expression:	test@test.com
Matched Regular Expression:	test@test.com

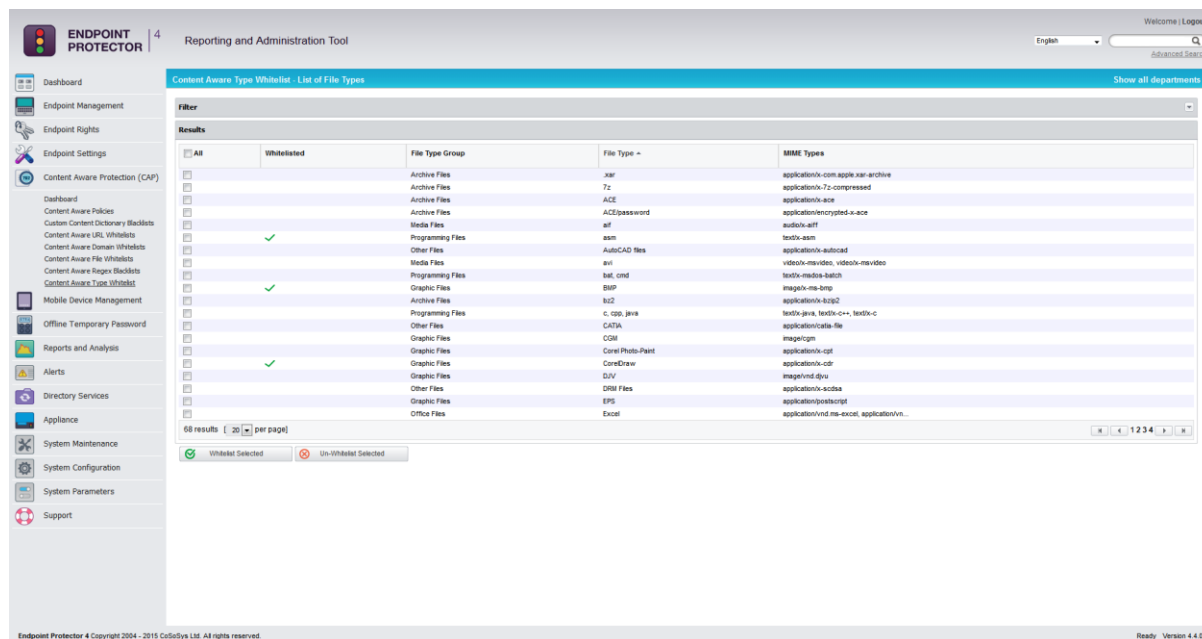
## 7.11. Content Aware Type Whitelist

Content Aware Type Whitelist allows the administrator to skip scanning the content of certain MIME types. This applies to Custom Content Dictionary, Predefined Content Dictionary and Regular Expressions Filter.

The purpose of this action would be to reduce false positive incidents such as Personal Identification Information (SSN, etc.) threats detected in metadata of some file types where the risk is very low (e.g. .dll, .exe).

First, when using this feature, a Content Aware Policy that uses a Custom Content Filter Blacklist has to be set up.

The next step is to navigate to “Content Aware Type Whitelist” and choose the exceptions that are required.



To select and apply the exceptions for the file type, simply tick the box to the left of each extension name, then save by clicking the button.

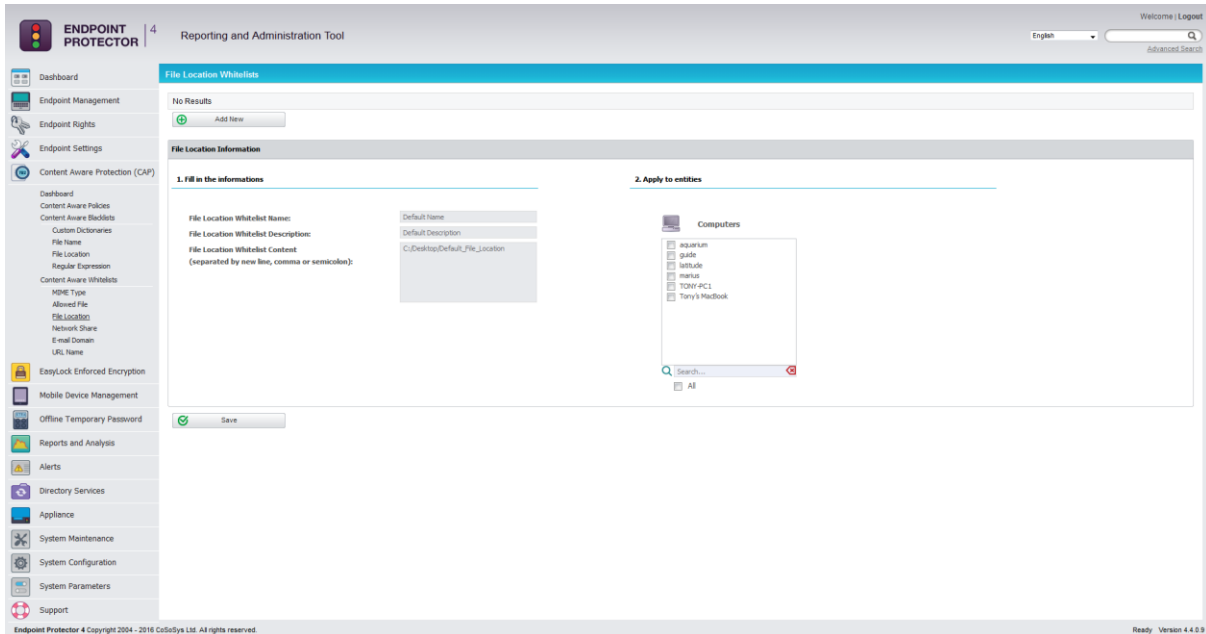
If the configuration is saved successfully, the symbol will be displayed to the left of the file type.

To remove the file type, simply select it and click on the button.

This is a simple to use yet efficient feature that allows the system administrator more flexibility and also better filtration of data.

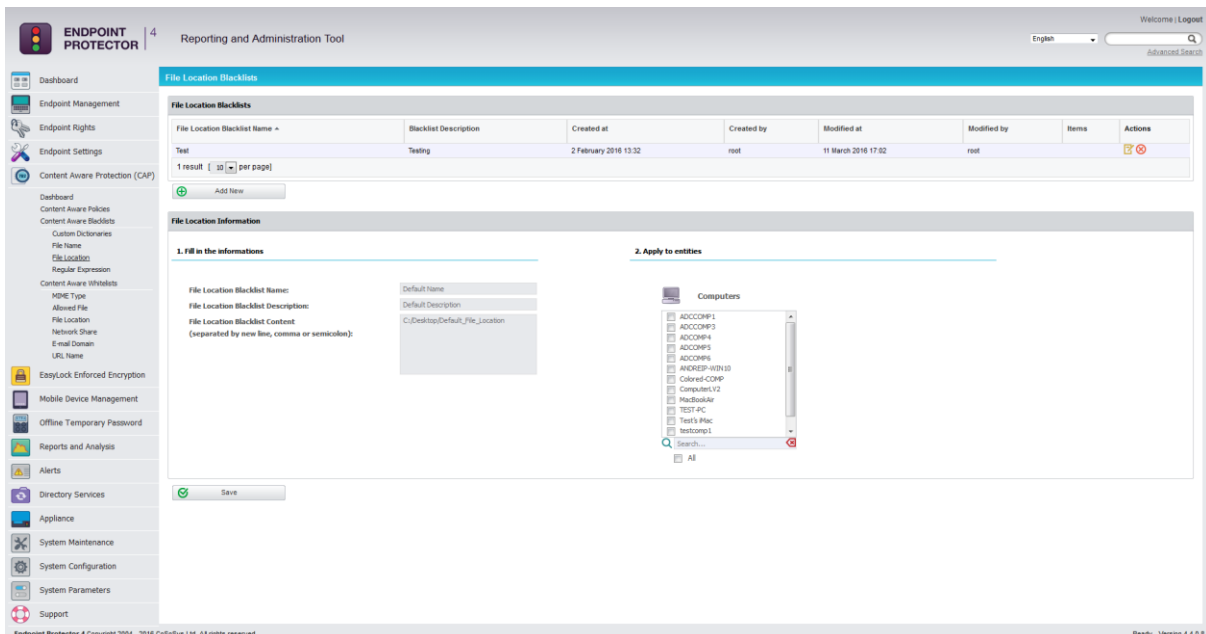
## 7.12. Content Aware File Location Whitelist

Content Aware File Location Whitelists allows the administrator to skip the scanning the content of certain files based on their location. This applies to all files located in the specific folder but does not apply to the files containing subfolders. The users will be able to transfer the files in the defined File Location regardless of the Content Aware Policies restrictions.



## 7.13. Content Aware File Location Blacklist

Content Aware File Location Blacklists allows the administrator to block file transfers of certain files based on their location. This applies to all files located in the specific folder but does not apply to the files containing subfolders. The users will not be able to transfer the files in the defined File Location regardless of the Content Aware Policies permissions.



## 7.14. How Content Aware Protection works for monitored Applications / Online Services

The following table shows a list of actions and content that are screened/inspected or left unscreened/uninspected by the Content Aware Protection feature.

APPLICATION	SCREENED	NOT SCREENED
Web Browsers	Uploaded Files	Webpage Content
	Webmail Attachments	Downloaded Content
		Blog Posts
E-MAIL Clients	File Attachments	E-MAIL Content for other E-MAIL Services
	Microsoft Outlook E-MAIL Content	Forwarded Attachments
	Microsoft Outlook Forwarded and Saved Attachments	Saved Attachments
	Microsoft Outlook E-mailed directly from Windows Explorer	Attachments e-mailed directly from Windows Explorer
	Microsoft Outlook Copied Attachments from one E-MAIL to another	Copied Attachments from one E-MAIL to another
Instant Messaging	File Transfers	IM Message Content
	Shared Picture Files	Sent Files
File Sharing	File Uploads	Saved Files
Social Media/Other	File Transfers	Blog Posts

\*Other limitations may apply.



## 7.15. HIPAA compliant Content Aware Protection

The Health Insurance Portability and Accountability Act (HIPAA) is a set of standards created to safeguard protected health information (PHI) by regulating healthcare providers. HIPAA was created in 1996 by the US Congress but it took the creation of a new act called HITECH (The Health Information Technology for Economic and Clinical Health Act) to ensure its effectiveness, starting from February 2010.

When it comes to audits, some requirement may be subject to interpretation but from an IT department point of view, compliance means setup of processes and controls that ensure security and integrity of PHI.

As HIPAA / HITECH compliancy also relate to things like employee trainings and physical access to the facilities (keys, access cards, tokens) data backup and disposal, Data Loss Prevention and Mobile Device Management solutions cannot solely ensure compliance.

### 7.15.1. How Endpoint Protector is HIPAA compliant

Any Content Aware Protection policy automatically becomes a HIPAA policy if any options from the HIPAA tab are selected. The available options refer to FDA approved lists and ICD codes.

**Policy Content**

File Type Filter Blacklist | Predefined Content Filter Blacklist | Custom Content Filter Blacklist | URL Whitelist | Domain Whitelist | File Whitelists | Regular Expression Blacklist | **HIPAA**

**Note:** A HIPAA Policy should include PII's like addresses, phone and fax numbers, emails and custom dictionaries. Please make sure you include them from the previous tabs.

<input type="checkbox"/> FDA recognised pharmaceutical firms	8.00 KB	↓
<input type="checkbox"/> FDA recognised pharmaceutical prescription drugs (branded)	12.00 KB	↓
<input type="checkbox"/> FDA recognised pharmaceutical prescription drugs (generic)	74.00 KB	↓
<input type="checkbox"/> ICD-10 codes and diagnosis lexicon	429.50 KB	↓
<input type="checkbox"/> ICD-9 codes and diagnosis lexicon	1.01 MB	↓

Save | Back | Delete

However, in order for a HIPAA policy to be affective, Predefined Content and Custom Content filters should also be enabled. These will automatically report or block transfer files containing PII like Health Insurance Numbers, Social Security Numbers, Addresses and much more.

File Type Filter Blacklist | **Predefined Content Filter Blacklist** | Custom Content Filter Blacklist | URL Whitelist | Domain Whitelist | File Whitelists | Regular Expression Blacklist | HIPAA

Policy Action will apply to selected Predefined Content for ALL File Types (regardless of the selected File Type Filter).

The below filters help ensure compliance with various regulations like PCI DSS and HIPAA.

**Credit Cards:**  Amex  Diners  Discover  JCB  Mastercard  Visa

**Personal Identifiable Information:**  IBAN  Date  E-mail  Address  ?

**Country Specific:**  SSN  ID  Passport  Phone Number  Tax ID  Driving License  Health Insurance Number

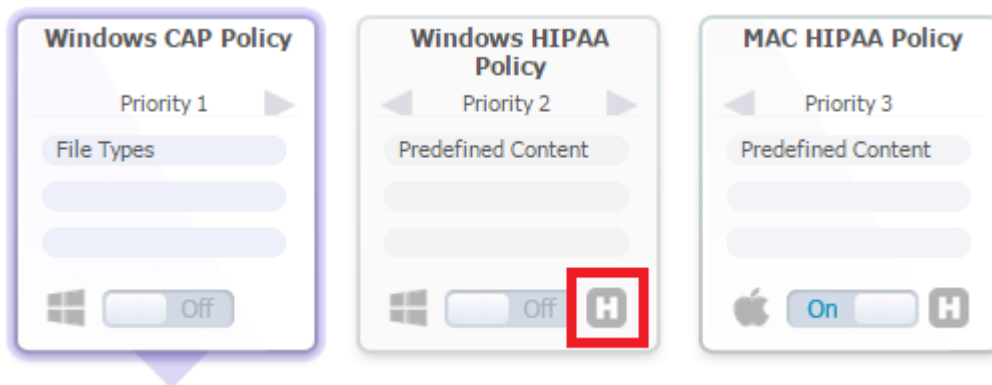
**Internet Protocol Addresses:**  Internet Protocol Version 4 (IPv4)  Internet Protocol Version 6 (IPv6)

Save | Back | Delete

A recommended HIPAA should be considered a Content Aware Policy that, besides the options in the HIPAA tab, also has the below configuration:

- All the File Types recognized should be included.
- All Personal Identifiable Information should be Country Specific to the United States (Address, Phone/Fax and Social Security Numbers)
- Both Internet Protocol Addresses Access should be selected
- The URL and Domain Whitelists options should also be checked

HIPAA policies can be created and used on their own or in combination with regular policies, for a better control of the data inside the network. These policies are available for Windows, Mac OS X or Linux computers. They are marked in the bottom right corner of the policy tab with a distinctive H.



### 7.15.2. Use Case Nr. 1

Suppose that Company X handles patient medical records that come in electronic formats and which contain generic information such as: Patient Name, Address, Birthdate, Phone number, Social Security Number and E-Mail address. The company would like to block the transfer of this data through all the common Windows desktop applications.

Knowing that the sensitive data comes in the format of a profile per patient, the administrator can create a HIPAA policy like the one shown below:

The screenshot displays the 'Edit Policy' configuration in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and Content Aware Protection (CAP). The main area shows the following settings:

- Policy Os Type:** Windows
- Policy Name:** Company X HPAIA Policy
- Policy Description:** Policy through which Patient Information leaks are blocked.
- Policy Action:** Report only, Block & Report (selected), Hide CAP Client Notifications
- Policy Status:** Enabled (ON), Disabled (OFF)
- Threshold:** 4
- Control Transfers To:**
  - Controlled Storage Device Types:  Clipboard,  Disable Print Screen,  Scan Network Share,  Printers
  - Applications / Online Services (Attachments / File Transfers):
    - Web Browser:** Internet Explorer, Chrome, Mozilla Firefox, Opera, Safari, AOL Desktop 9.6, Aurora Firefox, K-Melcon, Maxthon
    - E-mail:** Outlook (Attachments ...), Outlook (Body), Mozilla Thunderbird, Mozilla Thunderbird ..., IBM Lotus Notes v.6..., IBM Lotus Notes v.7, IBM Lotus Notes v.8..., IBM Lotus Notes v.8..., IBM Lotus Notes v.9...
    - Instant Messaging:** ICQ, AIM, Skype, Windows Live Messeng..., Yahoo! Messenger, Gaim, Pidgin, Trillian, NextOn Messenger
    - Cloud Services / File Sharing:** Google Drive Client, iCloud Client, uTorrent, BitComet, Daim Cloud, KT Client uCloud, Navier N Drive, Azarous, OneDrive (SkyDrive)
    - Social Media / Others:** EasyLock, Windows DVD Maker, ALFTP, FileZilla, GoToMeeting, HTC Sync for Android ..., InfraRecorder CD - D ..., iTunes, LionMain Bro...
- Policy Content:**
  - Personal Information:**
    - Contact Details:** Policy Action will apply to selected Custom Content for ALL File Types.  All,  E-mail Address,  Phone/Fax Numbers,  Address
    - Personal Details:** Policy Action will apply to selected Custom Content for ALL File Types.  All,  Social Security Numbers,  Dates
  - Custom Content:** Policy Action will apply to selected Custom Content for ALL File Types.

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.6

This policy is set on Block & Report with a Global Threshold of 4. It scans the Controlled Storage Device Types (which can be inspected from the System Parameters -> Device Types), the Clipboard and the Network Share as well as all the database of applications recognized by Endpoint Protector. This policy will ONLY block the transfer of those files which contain 4 or more of the PII's selected inside the policy. All the files which happen to contain just 1 Address or 2 Phone Numbers or 2 E-mails will be transferred

### 7.15.3. Use Case Nr. 2

Company Y has a large database of patients' sensitive information. This information is stored in individual office files which contain ten (10) or even more Personally Identifiable Information (PII) items per patient. Other than these files, the company's staff regularly uses some file which contain three (3) of the same PII's per file. Company Y would like to block the leakage of the files database from its database that contain 10 or more items yet only report the transfer of the files containing 3 items.

The administrator can setup a policy which will block the transfer of files containing 10 PII's by using a Global Threshold of 10, like in the policy shown below:

Policy Information	
Policy Name	Policy Y
Policy Description:	Policy that blocks 10 or more PIIs
Policy Action:	<input type="radio"/> Report only <input checked="" type="radio"/> Block & Report <input type="checkbox"/> Hide CAP Client Notifications <a href="#">?</a>
Policy Status:	<input checked="" type="radio"/> Enabled (ON) <input type="radio"/> Disabled (OFF)
Threshold:	10 <input type="checkbox"/> <a href="#">?</a>

Another HIPAA policy can be used to report the transfer of files which contain 3 items of the same kind by using a Regular Threshold set at 3, like the below shown example:

Policy Information	
Policy Name	Policy Y
Policy Description:	Policy that reports 3 or more of the same PIIs
Policy Action:	<input checked="" type="radio"/> Report only <input type="radio"/> Block & Report <input type="checkbox"/> Hide CAP Client Notifications <a href="#">?</a>
Policy Status:	<input checked="" type="radio"/> Enabled (ON) <input type="radio"/> Disabled (OFF)
Threshold:	3 <input type="checkbox"/> <a href="#">?</a>

Following our recommendations from subchapter 7.2.5, the Block & Report policy will have the 1st priority while the Report Only policy will be the 2nd.

# 8. Reports and Analysis

This section is designed to offer the administrator feedback regarding system functionality, logs and information related to devices, users and computers in the entire system.

The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector. The left sidebar contains navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main area shows a 'Logs Report' with a 'Filter' section and a table of results. The table has columns for Event name, Client Computer, IP Address, Domain Name, Client User, Device Type, Device, Files, Date/Time(Server), Date/Time(Client), OS Type, and Actions. The table lists various events like 'Blocked', 'Unblocked', and 'Connected' for different devices and users, with corresponding timestamps and OS types. At the bottom of the table, it shows '18 results' and '50 per page'.

Event name	Client Computer	IP Address	Domain Name	Client User	Device Type	Device	Files	Date/Time(Server)	Date/Time(Client)	OS Type	Actions
Blocked		192.168.0.198			Internal CD or DVD RW	MATSHITA DVD-RAM U8C2 S ATA Device	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55	Windows	
Blocked		192.168.0.198			Webcam	USB2.0 HD UVC WebCam	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55	Windows	
Unblocked		192.168.0.198			WIFI	Atheros AR9485WB-EG Wireless Network Ada...	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55	Windows	
Unblocked		192.168.0.198			WIFI	Atheros AR9485WB-EG Wireless Network Ada...	0	10-Sep-2014 10:57:25	10-Sep-2014 12:00:54	Windows	
Blocked		192.168.0.198			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	10-Sep-2014 10:57:23	10-Sep-2014 12:00:52	Windows	
Connected		192.168.0.198			Webcam	USB2.0 HD UVC WebCam	0	10-Sep-2014 10:57:23	10-Sep-2014 12:00:52	Windows	
Connected		192.168.0.198			Internal CD or DVD RW	MATSHITA DVD-RAM U8C2 S ATA Device	0	10-Sep-2014 10:57:23	10-Sep-2014 12:00:52	Windows	
Connected		192.168.0.198			WIFI	Atheros AR9485WB-EG Wireless Network Ada...	0	10-Sep-2014 10:57:22	10-Sep-2014 12:00:51	Windows	
Connected		192.168.0.198			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	10-Sep-2014 10:57:22	10-Sep-2014 12:00:51	Windows	
Blocked		192.168.0.198			Internal CD or DVD RW	MATSHITA DVD-RAM U8C2 S ATA Device	0	04-Sep-2014 09:27:30	04-Sep-2014 10:30:59	Windows	
Blocked		192.168.0.198			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:30	04-Sep-2014 10:30:59	Windows	
Blocked		192.168.0.198			Webcam	USB2.0 HD UVC WebCam	0	04-Sep-2014 09:27:30	04-Sep-2014 10:30:59	Windows	
Unblocked		192.168.0.198			WIFI	Atheros AR9485WB-EG Wireless Network Ada...	0	04-Sep-2014 09:27:30	04-Sep-2014 10:30:59	Windows	
Connected		192.168.0.198			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:24	04-Sep-2014 10:30:53	Windows	
Connected		192.168.0.198			Webcam	USB2.0 HD UVC WebCam	0	04-Sep-2014 09:27:21	04-Sep-2014 10:30:50	Windows	
Connected		192.168.0.198			Internal CD or DVD RW	MATSHITA DVD-RAM U8C2 S ATA Device	0	04-Sep-2014 09:27:21	04-Sep-2014 10:30:50	Windows	
Connected		192.168.0.198			WIFI	Atheros AR9485WB-EG Wireless Network Ada...	0	04-Sep-2014 09:27:21	04-Sep-2014 10:30:50	Windows	
Connected		192.168.0.198			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:21	04-Sep-2014 10:30:50	Windows	

All tabs described below will have a filter option at the beginning of each table. This will add or remove columns based on the content considered relevant.

This close-up shows the 'Logs Report' section with a 'Filter' button and a 'Results' table. The table has a dropdown menu for 'Event name' and a 'Show/Hide Columns' button.

## 8.1. Logs Report

This section allows the administrator to see exactly what actions took place and at what time. The information provided contains the computer name, user and device used and also the action taken and the files accessed.

The granular filter available is designed to make finding information quick and easy.

The screenshot shows a 'Logs Report' window with a 'Filter' section. The filter section contains the following fields:

- Event: [Dropdown menu]
- Computer: [Text input field]
- IP Address: [Text input field]
- Domain Name: [Text input field]
- User: [Text input field]
- Device Type: [Dropdown menu]
- Device: [Text input field]
- Date/Time(Server): [Text input field with calendar icon]
- Date/Time(Client): [Text input field with calendar icon]
- OS Type: [Dropdown menu with 'All' selected]

At the bottom of the filter section, there are two buttons: 'Reset' (with a refresh icon) and 'Apply filter' (with a magnifying glass icon).

The administrator has the possibility of exporting either the search results or the entire log report as a .CSV file, which can later be printed out for detailed analysis.

As an additional data security measure, this module may be protected by an additional password set by the Super Administrator.

The screenshot shows a 'Protected Area' dialog box. It contains a text input field labeled 'Additional Password Protection:'. Below the input field are two buttons: 'Unlock' and 'Close'.

The additional security password can be set from the System Configuration module, under the System Security tab and it applies to all the Reports and Analysis sections.

The screenshot shows a form titled 'Additional Security Password for Sensitive Data Protection'. It contains three text input fields:

- Current Password:
- New Password:
- New Password (confirm):

Below the input fields is a 'Save' button.

## 8.2. File Tracing

This section displays information about traced files that have been transferred from a protected computer to a portable device or to another computer on the network, and vice versa. It also displays the original location of the transferred files, as a Detect Source Copy feature is activated by default.

The screenshot shows the 'File Tracing' section of the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options and a main area displaying a table of file tracing results. The table has the following columns: Event, Computer, IP Address, Device, User, Device Type, File Name, File Hash, File Size, and File Type. The results show various file operations such as File Read, File Delete, and File Copy, with corresponding file hashes and sizes. At the bottom, there are buttons for Export and Back, and a footer indicating 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.0.4'.

Event	Computer	IP Address	Device	User	Device Type	File Name	File Hash	File Size	File Type
File Read		192.168.0.108	NT LAN Manager		Network Share		0e006eac634d3308bad77101e1ebee08	532.2 KB	VLC media
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				java file
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		3d74e350e6797b7dca1f121f7645eab	3.43 KB	java file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				Python File
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		af1839a10c85cb23da6097339f13939b	19 B	Python File
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				java file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				Python File
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		e26cac7b75af15e8c089f334f0f3eaa	7.47 KB	Python File
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		3d74e350e6797b7dca1f121f7645eab	3.43 KB	java file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				.ace file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				Python File
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		e26cac7b75af15e8c089f334f0f3eaa	7.47 KB	Python File
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		80f572ee491e457ffc94b1c4e8fa670	224 B	.ace file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				.ace file
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		80f572ee491e457ffc94b1c4e8fa670	224 B	.ace file
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		07e06f04179f2485c90a9a1dc47203f	216 B	.ace file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		65853869e8417352d09d25a66b243f4e	571 B	.ace file
File Copy		192.168.0.198	DATATRAVELER_2.0		USB Storage Device		75f1125bd481db684e89449c0fc8164	7.26 KB	.ace file
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				Python File
File Delete		192.168.0.198	DATATRAVELER_2.0		USB Storage Device				Python File

Similar to the Logs Reports section, you may need to enter an additional password set by the administrator in order to be able to access the list of files.

A special mention is given here to the "File Hash" column. The Endpoint Protector application computes an MD5 hash for most of the files on which the File Tracing feature applies to. This way, mitigating threats coming from the changing the file content is ensured.

## 8.3. File Shadowing

This section displays information about shadowed files that have been transferred from a protected computer to a portable device. The list of files may be protected by an additional password set by the administrator. In this case, you will be prompted to insert the additional password when entering this section.

Additionally, the shadowed files can be saved locally on the Server by the Endpoint Protector administrator.

The screenshot shows the 'File Shadowing' section of the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main area displays a table of shadowed files with the following columns: File Name, File Size, File Type, Users, Computer, IP Address, Date/Time(Client), Date/Time(Server), OS Type, and Actions. The table contains 20 rows of data, including files like PNG images, data files, and .icns files, with various file sizes and types. The footer of the interface indicates 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.3 - Appliance'.

File Name	File Size	File Type	Users	Computer	IP Address	Date/Time(Client)	Date/Time(Server)	OS Type	Actions
[Redacted]	73.32 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	121.16 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	94.95 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	108.33 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	67.26 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	14.24 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	[Icons]
[Redacted]	67.26 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:30	2014-03-11 16:29:35	Windows	[Icons]
[Redacted]	94.95 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:22	2014-03-11 16:29:28	Windows	[Icons]
[Redacted]	121.16 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:20	2014-03-11 16:29:26	Windows	[Icons]
[Redacted]	73.32 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:19	2014-03-11 16:29:25	Windows	[Icons]
[Redacted]	108.33 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:17	2014-03-11 16:29:23	Windows	[Icons]
[Redacted]	14.24 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.96	2014-03-11 17:29:11	2014-03-11 16:29:17	Windows	[Icons]
[Redacted]	106.85 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.21	2014-03-11 14:59:40	2014-03-11 13:59:44	Windows	[Icons]
[Redacted]	226.28 KB	PNG Image	[Redacted]	[Redacted]	192.168.0.21	2014-03-11 14:58:30	2014-03-11 13:58:34	Windows	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 12:06:27	2014-03-11 11:06:30	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 12:03:12	2014-03-11 11:03:14	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 12:02:03	2014-03-11 11:02:06	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 12:00:19	2014-03-11 11:00:21	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 11:58:28	2014-03-11 10:58:30	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 11:40:35	2014-03-11 10:40:37	Macintosh	[Icons]
[Redacted]	205 B	data	[Redacted]	[Redacted]	192.168.0.115	2014-03-11 11:39:19	2014-03-11 10:39:19	Macintosh	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-11 11:37:27	2014-03-11 10:37:30	Macintosh	[Icons]
[Redacted]	46.63 KB	.icns file	[Redacted]	[Redacted]	192.168.0.21	2014-03-11 11:35:16	2014-03-11 10:35:20	Windows	[Icons]
[Redacted]	9 B		[Redacted]	[Redacted]	192.168.0.21	2014-03-11 11:35:15	2014-03-11 10:35:19	Windows	[Icons]
[Redacted]	784 B		[Redacted]	[Redacted]	192.168.0.21	2014-03-11 11:35:09	2014-03-11 10:35:13	Windows	[Icons]
[Redacted]	613 B	QuickTime Preferences	[Redacted]	[Redacted]	192.168.0.21	2014-03-11 11:35:09	2014-03-11 10:35:13	Windows	[Icons]
[Redacted]	28 B		[Redacted]	[Redacted]	192.168.0.21	2014-03-11 11:35:09	2014-03-11 10:35:13	Windows	[Icons]
[Redacted]	36 B		[Redacted]	[Redacted]	192.168.0.20	2014-03-10 17:33:49	2014-03-10 16:33:50	Macintosh	[Icons]
[Redacted]	14.23 KB	png	[Redacted]	[Redacted]	192.168.0.89	2014-03-10 16:23:40	2014-03-10 15:23:40	Macintosh	[Icons]
[Redacted]	205 B	data	[Redacted]	[Redacted]	192.168.0.115	2014-03-10 15:24:15	2014-03-10 14:24:15	Macintosh	[Icons]



## 8.4. Content Aware Report

This module provides detailed logs of all Content Aware activity. It allows the administrator to see exactly what data incidents were detected corresponding to the Content Aware Policies applied and at what time. This information also contains the computer name, user and transfer destination type, the action taken and the file inspected. The included granular filter is designed to make finding information quick and easy.

The screenshot shows the 'Content Aware Report' interface. At the top, there's a navigation bar with 'ENDPOINT PROTECTOR 4' and 'Reporting and Administration Tool'. A sidebar on the left contains menu items like 'Dashboard', 'Endpoint Management', 'Endpoint Rights', 'Endpoint Settings', 'Content Aware Protection (CAP)', 'Mobile Device Management', 'Offline Temporary Password', 'Reports and Analysis', 'Alerts', 'Directory Services', 'Appliance', 'System Maintenance', 'System Configuration', 'System Parameters', and 'Support'. The main content area is titled 'Content Aware Report' and includes a 'Filter' section and a 'Results' table. The table has the following columns: Content Policy, Destination Type, Destination, File Name, File Hash, File Size, and Matched Item. The results list various incidents, such as 'screen-capture', 'Web Browser', and 'test for exceptions from sys policies', with associated file hashes and sizes.

Content Policy	Destination Type	Destination	File Name	File Hash	File Size	Matched Item
Undefined Policy	screen-capture		screen-capture-image			
RO	Web Browser	Mozilla Firefox	[Redacted]	80f48c1f435fe040d336850307f19132	7.77 MB	application/x-dosexec
RO	Web Browser	Mozilla Firefox	[Redacted]	f3e7a015c1d541528085d39581ab41f	220 KB	application/x-dosexec
RO	Web Browser	Mozilla Firefox	[Redacted]	46860396033a0d38326cbcb8a8719577a	245.5 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	f3e7a015c1d541528085d39581ab41f	220 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	f3e7a015c1d541528085d39581ab41f	220 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	f3e7a015c1d541528085d39581ab41f	220 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	732a2aad77e65d56e7a534086881e230	9.58 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	83a7340778e7c353b9a2d2a788c3a13a	132 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	6368baa2c6d3ae01ce29106c48847def	3.9 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	414b5bb94da8e1250a9d43cfd7ac5053	7 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	732a2aad77e65d56e7a534086881e230	9.58 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	83a7340778e7c353b9a2d2a788c3a13a	132 KB	application/x-dosexec
RO	file-type	explorer	[Redacted]	1f23ae997ee575de679e6f37c317462	15.3 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	be25009e663442f0d0512bffc050a7	20.59 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	84e6b1d544f91c4d2f98ac0d66d3ab00	9.07 MB	application/x-dosexec
RO	file-type	explorer	[Redacted]	6368baa2c6d3ae01ce29106c48847def	3.9 MB	application/x-dosexec
test for exceptions from sys policies	E-mail	Mozilla Thunderbird	[Redacted]	79fb3436099fe00467bc874fd0313d13	19.33 KB	image/x-icon
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			text/x-c++
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	0b4c5b394dfb23ee1a92a8ce9e6530bf	22.34 KB	text/x-tex
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	69d0ba69f5ce6f14d10f40dedc8abfd	10.72 KB	text/x-shellscript
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	7e861912881c4ee67787865f5648bf2	3.98 KB	text/x-tex
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	730dd0fe402efc1d41f33e574f6c08d	3.08 KB	text/x-tex
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	3d74e350e6797b7dca1f121764568ab	3.43 KB	text/x-c++
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	cbd5c5895eb6336e15312eb128427d21	1.22 MB	application/x-ace
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	ca2dbdece6e29101b9f7bc06893b39	1013 KB	image/gif
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	0de7cc7a79396fdb6d08cc27c0f09895	140.65 KB	image/gif
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	730dd0fe402efc1d41f33e574f6c08d	3.08 KB	text/x-tex
test for exceptions from sys policies	Web Browser	Mozilla Firefox	[Redacted]	69d0ba69f5ce6f14d10f40dedc8abfd	10.72 KB	text/x-shellscript
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			text/x-python
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			text/x-python
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			text/x-c++
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			text/x-python
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			application/encrypted-x-act
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]			application/encrypted-x-act
test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	[Redacted]	65853869e8417352d09d25a666243f4e	571 B	application/encrypted-x-act

The administrator has the possibility of exporting both the search results and the entire log report as a .CSV file, which can later be printed out for detailed auditing.

As an additional data security measure, this module may be protected by an additional password set by the Super Administrator. For more details, please see section 8.1. Logs Report.

Content Aware Report
Show all departments

**Filter**

Event Name:

Client Computer:

Client User:

Destination Type:

Destination:

File Name:

Content Policy:

Item Type:

Matched Item:

Item Details:

Date/Time(Server):

Date/Time(Client):

## 8.5. Content Aware File Shadowing

Displays the list of file shadows and files that have been detected by a Content Aware policy. The list of files may be protected by the additional password set by the administrator for all the Reports and Analysis sections. In this case, you will be prompted to insert the additional password when entering this section.

**ENDPOINT PROTECTOR** | 4

Reporting and Administration Tool

Welcome | Logout

English

Advanced Search

Content Aware File Shadowing

**Filter**

**Results**

<input type="checkbox"/>	File Name	File Size	User	Computer	IP Address	Date/Time(Client)	Date/Time(Server)	OS Type	Actions
<input type="checkbox"/>	...	12.89 KB	...	...	192.168.0.20	2014-09-10 16:31:52	2014-09-06 12:38:23	Macintosh	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	220 KB	...	...	192.168.56.1	2014-09-10 10:12:22	2014-09-06 06:15:20	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	245.5 KB	...	...	192.168.56.1	2014-09-10 10:12:22	2014-09-06 06:15:20	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	220 KB	...	...	192.168.56.1	2014-09-10 09:52:33	2014-09-06 05:55:31	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	220 KB	...	...	192.168.56.1	2014-09-09 18:01:19	2014-09-05 14:04:18	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	220 KB	...	...	192.168.56.1	2014-09-09 17:53:31	2014-09-05 13:56:31	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	132 KB	...	...	192.168.0.198	2014-09-09 16:05:58	2014-09-05 12:08:58	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	132 KB	...	...	192.168.56.1	2014-09-09 16:05:58	2014-09-05 12:08:58	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	19.33 KB	...	...	192.168.56.1	2014-09-09 14:22:46	2014-09-05 10:25:46	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	10.72 KB	...	...	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	10.72 KB	...	...	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	3.98 KB	...	...	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	3.08 KB	...	...	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	3.43 KB	...	...	192.168.56.1	2014-09-09 13:16:53	2014-09-05 09:19:53	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	140.65 KB	...	...	192.168.56.1	2014-09-09 13:16:31	2014-09-05 09:19:32	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	3.08 KB	...	...	192.168.56.1	2014-09-09 13:16:23	2014-09-05 09:19:24	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	10.72 KB	...	...	192.168.56.1	2014-09-09 13:16:15	2014-09-05 09:19:16	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	10.72 KB	...	...	192.168.56.1	2014-09-09 12:54:32	2014-09-05 08:57:32	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	10.72 KB	...	...	192.168.56.1	2014-09-09 12:18:35	2014-09-05 08:21:36	Windows	<input type="button" value=""/> <input type="button" value=""/>
<input type="checkbox"/>	...	30.46 KB	...	...	192.168.56.1	2014-09-09 12:18:14	2014-09-05 08:21:14	Windows	<input type="button" value=""/> <input type="button" value=""/>

44 results [ 20 per page]

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.4

## 8.6. Admin Actions

Every important action performed by administrators in the interface is recorded. Clicking the “view details” button will open the “Admin Actions Details” page where further details about the specific event is shown, with the status of the modified feature before and after the change took place.

The screenshot displays the 'Admin Actions' page in the Endpoint Protector interface. The page title is 'Reporting and Administration Tool' and it shows 'Showing departments: Default Department'. A sidebar on the left contains navigation options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area features a table of administrative actions.

Administrator	Section	Action Type	Before	After	Created at
root	Computer Settings	EDIT	IP...	IP...	07-Mar-2014 15:35:1
root	Computer Rights	EDIT	Computer Name...	Computer Name...	07-Mar-2014 15:34:5
root	Content Aware Policies	POLICY APPLIED TO	Policy Name	Policy Name...	07-Mar-2014 15:31:4
root	Content Aware Protection (CAP)	CREATE	...	...	07-Mar-2014 15:30:4
root	User Authentication	SIGN OUT	...	User Sign Out...	07-Mar-2014 15:27:5
root	Administrators	CREATE	...	Username...	07-Mar-2014 15:27:4
root	System Security	SET DATA SECURITY PRIVILEGES	Restrict Sensitive Data Access only to s...	Restrict Sensitive Data Access only to s...	07-Mar-2014 15:27:2
root	Device Rights	EDIT	Device Name...	Device Name...	07-Mar-2014 15:10:5
root	Device Rights	EDIT	Device Name...	Device Name...	07-Mar-2014 15:10:4
root	Device Rights	EDIT	Device Name...	Device Name...	07-Mar-2014 15:10:3
root	Content Aware Regex	CREATE	...	Regular Expression Name...	07-Mar-2014 15:00:4
root	Client Software	DOWNLOAD	...	Downloaded Endpoint Protector Client Sof...	07-Mar-2014 14:59:2
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 14:58:5
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 14:35:1
root	Content Aware Regex	DELETE	Domain Whitelist Name...	...	07-Mar-2014 14:32:0
root	Content Aware Regex	DELETE	Domain Whitelist Name...	...	07-Mar-2014 14:32:0
root	Client Software	DOWNLOAD	...	Downloaded Endpoint Protector Client Sof...	07-Mar-2014 14:16:0
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 14:14:3
root	Content Aware Regex	EDIT	Regular Expression Name...	Regular Expression Name...	07-Mar-2014 14:08:2
root	Content Aware Regex	EDIT	Regular Expression Name...	Regular Expression Name...	07-Mar-2014 14:08:2
root	Content Aware Regex	CREATE	...	Regular Expression Name...	07-Mar-2014 14:08:2
root	Content Aware Protection (CAP)	EDIT	...	...	07-Mar-2014 14:02:2
root	Configuration	signedEnvelope	...	Certificate Signing Request (CSR)...	07-Mar-2014 14:01:2
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 13:55:5
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 13:50:2
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 13:40:3
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 13:37:0
root	Administrators	EDIT	First Name...	Email...	07-Mar-2014 06:20:5
root	User Authentication	SIGN IN	...	User Logging...	07-Mar-2014 06:20:2
root	User Authentication	SIGN OUT	...	User Sign Out...	07-Mar-2014 06:20:2

The logs can be exported in a .csv file, while the filter can help find the desired information quickly and easily.

## 8.7. Online Computers

The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The top navigation bar includes the logo, the text "Reporting and Administration Tool", and a user greeting "Welcome Super Administrator | Logout" with a language dropdown set to "English" and a search bar. A left sidebar contains a menu with categories like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Offline Temporary Password, Reports and Analysis, System Alerts, Directory Services, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled "Online Computers" and features a "Show all departments" link. Below this is a "Results" section with a table listing online computers. The table has columns for Name, User Logged, Domain, Workgroup, IP, MAC Address, Location, Status, and Actions. Two rows of data are visible, both with a status of "Online". Below the table, it indicates "2 computers online" and a pagination control set to "20 per page". The footer of the interface shows "Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved." and "Ready Version 4.0.0.8".

Offers real time\* monitoring of the client computers registered on the system which have an established connection with the server.

\*depends on the Refresh Interval; if the Refresh Interval for computer X is 1 minute, than the computer X was communicating with the server in the last 1 minute.


The administrator has the possibility of accessing the log for a certain computer by pressing the "View Logs" action button.



Pressing this button will take you to the logs report where it will only display the actions of that specific computer for which the button was pushed.

## 8.8. Online Users

Shows a list of users that are connected to the Endpoint Protector Server in real time.

 **ENDPOINT PROTECTOR** | 4 Reporting and Administration Tool Welcome Super Administrator | [Logout](#)

English  [Advanced Search](#)

- Dashboard
- Endpoint Management
- Endpoint Rights
- Endpoint Settings
- Offline Temporary Password
- Reports and Analysis
  - Logs Report
  - File Tracing
  - File Shadowing
  - Online Computers
  - Online Users**
  - Online Devices
  - Statistics
  - Graphics
- System Alerts
- Directory Services
- System Maintenance
- System Configuration
- System Parameters
- Support

**Online Users** Show all departments

**Results**

Username	Name ^	Computer Name	IP	Connected Device
██████████	██████████	██████████	██████████	none
██████████	██████████	██████████	██████████	none

2 users online [ 20 per page]

Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved.Ready Version 4.0.0.8

## 8.9. Online Devices

Offers information regarding the devices connected to the computers on the system.

The screenshot shows the 'Connected Devices' section of the Endpoint Protector interface. The interface includes a sidebar with navigation options and a main content area displaying a table of connected devices. The table has the following columns: Computer Name, User Logged, IP, Device Type, Device Name, VID, PID, Serial No, and Actions. The table lists 9 devices connected, including a Card Reader Device (SCSI), Internal Floppy Drive, Serial Port, and several USB Storage Devices. The interface also shows a 'Show all departments' link and a 'Results' header.

Computer Name	User Logged	IP	Device Type	Device Name	VID	PID	Serial No	Actions
			Card Reader Device (SCSI)	NVIDIA nForce Serial ATA Controller				[View Logs] [Manage Rights]
			Internal Floppy Drive	(Standard floppy disk drives)				[View Logs] [Manage Rights]
			Serial Port	Communications Port (COM3)				[View Logs] [Manage Rights]
			Serial Port	Communications Port (COM1)				[View Logs] [Manage Rights]
			USB Storage Device	TS1GJFV30				[View Logs] [Manage Rights]
			USB Storage Device	USB_SD_READER				[View Logs] [Manage Rights]
			Internal CD or DVD RW	ASUS DRW-1814BL				[View Logs] [Manage Rights]
			USB Storage Device	USB_FLASH_DRIVE				[View Logs] [Manage Rights]
			USB Storage Device	Port_#0004.Hub_#0004				[View Logs] [Manage Rights]

9 devices connected [ 20 ] per page

The administrator can see which devices are connected to what computers and also the client user who is accessing them. The administrator can also use the action buttons "View Logs" and "Manage Rights" to quickly administer the device.



## 8.10. Computer History

This module shows all computers that were at least once connected to the server. With the help of the "Export" button the logs can be saved to a .csv file, while pressing the "View Machine log" will show the Logs Report page filtered for the respective Computer.

The screenshot shows the 'Computers History' page in the Endpoint Protector Reporting and Administration Tool. The page title is 'Computers History' and it indicates 'Showing departments: Default Department'. A 'Filter' section is present above the results table. The table contains the following data:

Computer Name	Domain	WorkGroup	IP	Computer Location	Last Time Online	Actions
[Redacted]		WORKGROUP	192.168.0.21		07-Mar-2014 17:17	[Export] [View Log]
[Redacted]		WORKGROUP	192.168.0.20		07-Mar-2014 17:05	[Export] [View Log]
[Redacted]		WORKGROUP	192.168.0.89		07-Mar-2014 16:52	[Export] [View Log]
[Redacted]		WORKGROUP	192.168.0.20		07-Mar-2014 05:32	[Export] [View Log]
[Redacted]		WORKGROUP	192.168.0.20		07-Mar-2014 05:32	[Export] [View Log]

Below the table, it shows '5 results [ 20 per page]'. The sidebar on the left includes options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Admin Actions, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The top navigation bar shows 'Endpoint Protector 4', 'Reporting and Administration Tool', and 'Welcome | Logout'.





## 8.12. Device History

Similar to Computer and User history, all devices that were at least once connected to the server can be found here. Logs can be exported to a .csv file by pressing the "Export" button, while "View Device Log" will show the Logs Report page filtered for the respective device.

The screenshot shows the 'Devices History' page in the Endpoint Protector 4 Reporting and Administration Tool. The page title is 'Reporting and Administration Tool' and it shows 'Showing departments: Default Department'. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area displays a table of device connection logs with the following columns: Device Type, Device Name (identification), Last User, Last Computer, Description, TD, VID, PID, Serial Number, Last Connection, and Actions. The table contains 10 rows of data, including entries for USB Storage Devices, Serial Port, Internal CD or DVD RW, Internal CD or DVD RW, Local Printers, and Local Printers. Below the table, there is a filter section, a '10 results [ 20 ] per page' indicator, and an 'Export' button.

Device Type	Device Name (identification)	Last User	Last Computer	Description	TD	VID	PID	Serial Number	Last Connection	Actions
USB Storage Device	Security Pack			Security Pack / Verbatim	13fe	3327	070007A814070680BA39		07-Mar-2014 16:12	<a href="#">View</a>
USB Storage Device	DataTraveler 2.0			DataTraveler 2.0 / Kingston	951	1665	60A44C3FB294FD412968...		07-Mar-2014 15:11	<a href="#">View</a>
USB Storage Device	ADATA USB Flash Drive			ADATA USB Flash Drive / ADATA	125f	c08a	132212022221001D		07-Mar-2014 03:45	<a href="#">View</a>
USB Storage Device	ADATA USB Flash Drive			ADATA USB Flash Drive / ADATA	125f	cb10	1373113251469A45		07-Mar-2014 03:17	<a href="#">View</a>
Serial Port	Communications Port (COM1)			Communications Port (COM1) / (Standard p...	0	0	COM_ACPL_PNP0501_1_6...		07-Mar-2014 03:00	<a href="#">View</a>
Internal CD or DVD RW	ASUS CB-5216A ATA Device			ASUS CB-5216A ATA Device / (Standard CD-...	0	0	CDROMASUS_CB-5216A_1...		07-Mar-2014 03:00	<a href="#">View</a>
Internal CD or DVD RW	Security Pack Media			Security Pack Media / Verbatim	0	0	Verbatim Security Pa...		07-Mar-2014 01:58	<a href="#">View</a>
Local Printers	HP LaserJet P1005, 1.4.0			HP LaserJet P1005, 1.4.0 /	0	0	usb://Hewlett-Packar...		07-Mar-2014 01:38	<a href="#">View</a>
Internal Card Reader	SDXC Card Reader			SDXC Card Reader / Apple	14e4	16bc	c82a140f8b52		07-Mar-2014 01:38	<a href="#">View</a>
Local Printers	HP Officejet 5600 series			HP Officejet 5600 series /	0	0	usb://HP/Officejet%2...		06-Mar-2014 10:09	<a href="#">View</a>

10 results [ 20 ] per page

[Export](#)

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.3 - Appliance

## 8.13. Statistics

The Statistics module will allow you to view system activity regarding data traffic and device connections. The integrated filter makes generating reports easy and fast. Simply select the field of interest and click the "Apply filter" button.

The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The top navigation bar includes the logo, version number (4), and user information (Welcome Super Administrator | Logout). The sidebar on the left lists various system management options, with 'Reports and Analysis' selected. The main content area shows the 'Statistics' module with a search criteria section and a results table.

**Search Criteria**

Report: Most Active (Device Connections) [v]  
 Period: Last Week [v]  
 On: Computers [v]  
 [Apply filter]

**Results**

Computer Name	Default User	Group	IP	Total Connections
[Redacted]	[Redacted]	[Redacted]	[Redacted]	13
[Redacted]	[Redacted]	[Redacted]	[Redacted]	3

2 results

Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved. System Statistics! Version 4.0.0.8

# 9. Alerts

Endpoint Protector allows you to set notifications (Alerts) for Sensitive Content Transfers, Devices, Computers, Groups and Users making monitoring them easier. An Alert will trigger an E-MAIL that will be sent to the selected administrator(s) that are intended to receive the alerts. You can set up device related activity alerts in the System Alerts-> Define System Alerts module in Endpoint Protector. The Define Content Aware Alerts option will allow administrators to set special alerts for sensitive content detection and transfer blocking.

Before you can create an E-MAIL alert, you must configure the server host and provide a user name and password to that mail server. You can do that by accessing "System Settings" in the "System Configuration" module.

E-mail Server Settings	
<b>*Note:</b> The test e-mail will be sent to <input type="text"/>	
Hostname:	<input type="text" value="smtp.gmail.com"/> Example: smtp.cososys.com
SMTP Port:	<input type="text" value="465"/> Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:	<input checked="" type="checkbox"/>
Username:	<input type="text"/> Example: Your full email address (including @cososys.com).
Password:	<input type="password" value="••••••••"/> Your SMTP password.
Encryption Type:	SSL <input type="button" value="v"/> Example: None, SSL or TLS/STARTTLS.
Send test e-mail to my account:	<input checked="" type="checkbox"/>

Proxy Server Settings	
IP:	<input type="text"/>
Username:	<input type="text"/>

You can also verify if your settings are correct by checking the box next to "Send test E-MAIL to my account".

You also have to configure the E-MAIL of your current user with which you are accessing Endpoint Protector; by default, "root". To do this, go to "System Configuration" > "System Administrators".

The screenshot shows the Endpoint Protector Reporting and Administration Tool interface. The top navigation bar includes the logo, the title "Reporting and Administration Tool", and a user greeting "Welcome Super Administrator | Logout". A search bar is also present. The left sidebar contains a menu with various system management options. The main content area displays a table titled "List of Administrators" with columns for "User Name", "Created at", "Last Login", and "Actions". The table contains five rows of administrator data. Below the table, there is a "Create" button and a footer with copyright information.

User Name	Created at	Last Login	Actions
[Redacted]	[Redacted]	01-Jul-2011 11:11	[Edit] [Info] [Delete]
[Redacted]	8 June 2011 12:53	08-Jun-2011 12:55	[Edit] [Info] [Delete]
[Redacted]	8 June 2011 12:59	08-Jun-2011 13:02	[Edit] [Info] [Delete]
[Redacted]	8 June 2011 16:25	[Redacted]	[Edit] [Info] [Delete]
[Redacted]	23 June 2011 15:28	23-Jun-2011 15:34	[Edit] [Info] [Delete]

5 results [ 50 per page]

Create

Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved. Ready Version 4.0.2.1

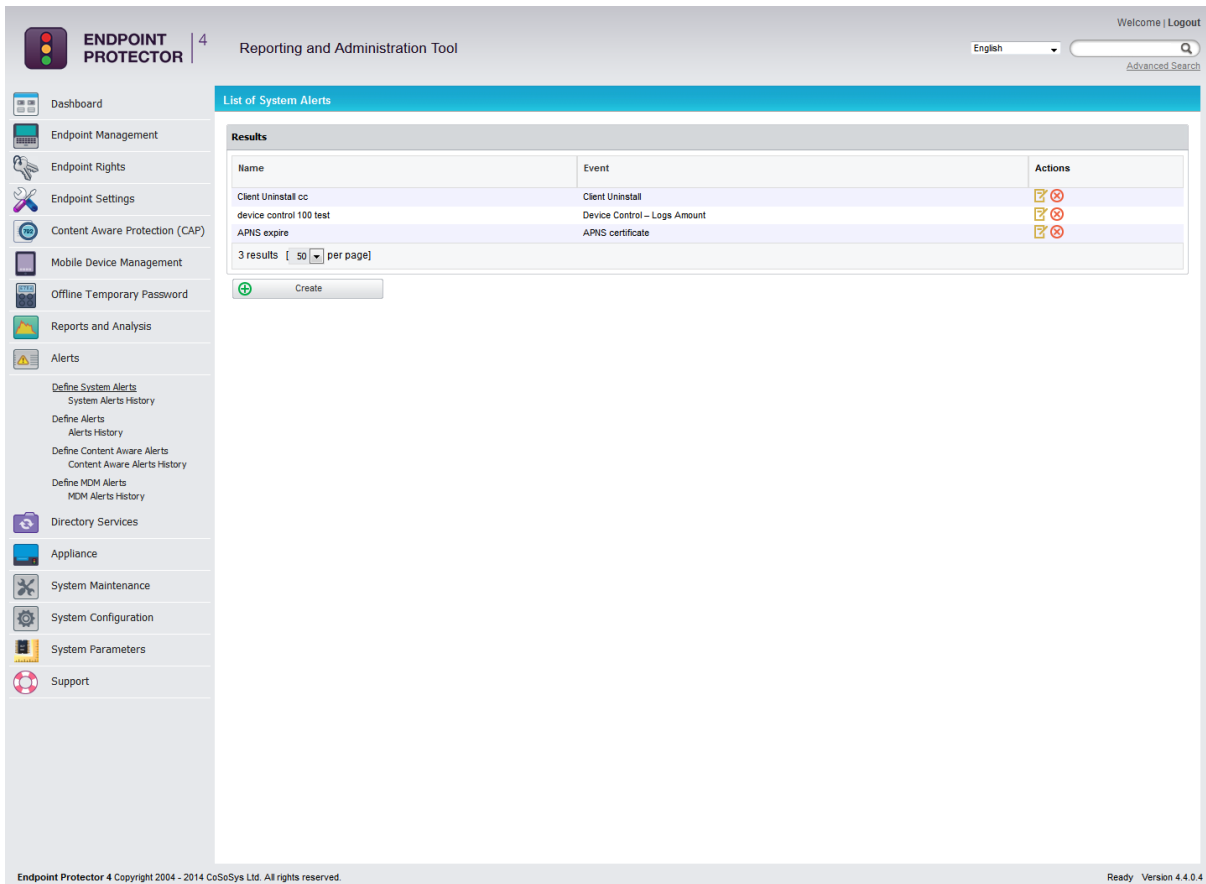
The actions available here are Edit, Edit Info and Delete.



Select the option "Edit info" for the desired user and complete the required fields. After you are done, click "Save".

Now you are set up to receive E-MAIL alerts.

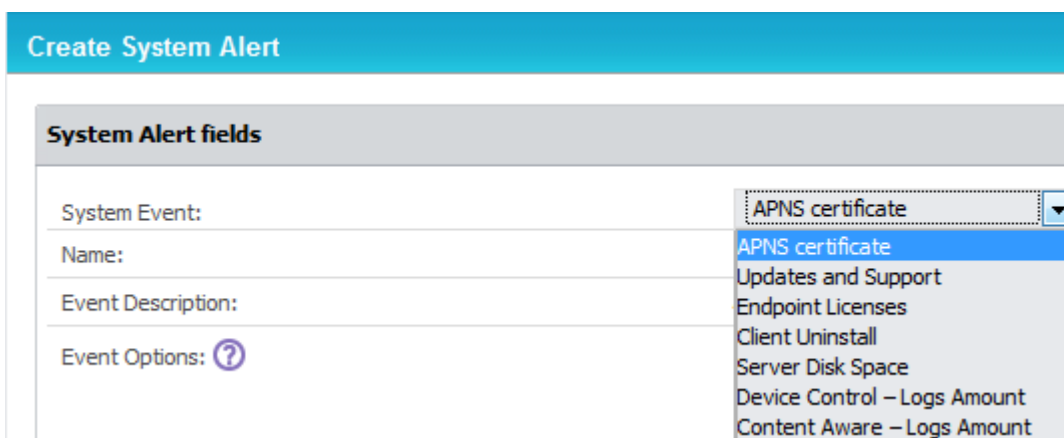
## 9.1. Define System Alerts



To create a new system alert, go to “Define System Alerts” and click “Create”.



There are several types of alerts available as shown below:



**APNS certificate** – APNS certificates expire and have to be renewed on a regular basis. These alerts eliminates the risks of having to re-enroll all the mobile devices by sending an e-mail reminder 60, 30 or 10 days prior.

**Updates and Support** – To ensure the Endpoint Protector Appliance is up to date, a reminder can be sent regarding each module maintenance status (Device Control, Content Aware Protection and Mobile Device Management).

**Endpoint Licenses** – As each network is constantly growing, to eliminate the risks of having unprotected endpoints, an alert can be generated. It can be defined if the percentage of already used Endpoint Licenses reaches 70%, 80% or 90%.

**Client Uninstall** – For a better management of a large network, an alert can be sent each time an Endpoint Protector Client is uninstalled. This is particularly helpful when there are several assigned Administrators.

**Server Disk Space** – Ensuring Server Disk Space remains available for logs to be stored and policies are properly applied, and alert can be setup when disk space reaches 70%, 80% or 90%.

**Device Control – Logs Amount** – An alert can be sent each time the Number of Device Control Logs Stored reaches a specific amount. The option to choose either from an interval between 10,000 rows or 10,000,000 rows or define a desired value are available.

**Content Aware – Logs Amount** – An alert can be sent each time the Number of Content Aware Logs Stored reaches a specific amount. The option to choose either from an interval between 10,000 rows or 10,000,000 rows or define a desired value are available.

**Note!**

Both the APNS Certificate and Update and Support system alerts can be disabled from General Dashboard -> System Status

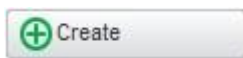
## 9.2. Define Alerts (Device Control Alerts)

The screenshot shows the 'List of Alerts' page in the Endpoint Protector interface. The page title is 'Reporting and Administration Tool'. The sidebar on the left contains various navigation options, including 'Alerts' which is currently selected. The main content area shows a table with the following data:

Client	Computer	Group	Device Type	Device	Event	Actions
Any	My testing Computer 1	Any	Any	Any	Connected	[Icons]
Any	My testing Computer 2	Any	Any	Any	Blocked	[Icons]

Below the table, there are '2 results' and a 'per page' dropdown. A 'Create' button is located at the bottom left of the table area.

To create a new alert, go to “Define Alerts” and click “Create”.



The 'Create Alert' form is shown with the following details:

- Alert Name:** Alert Test
- Alert Entities:**
  - Groups: Any
  - Computers: Any
  - Users: Any
- Alert fields:**
  - Device type: Internal CD or DVD RW
  - Device: SDA Standard Compliant SD Host Controller
  - Event: Connected

Then select the Group, User, Computer, Device type or Device - depending if you mean a single device or all devices of a certain type - and the event that will trigger the notification. The filters shown above designed to make finding information quick and easy.

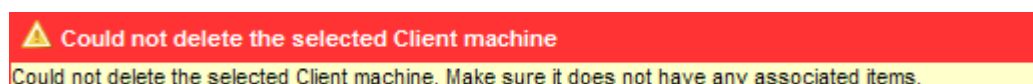
You can also select one or more administrators to receive the same notification(s). This is useful in case there is more than one administrator for Endpoint Protector.

Example: if you want to be notified when a certain device is connected to a certain computer you must set up an alert choosing the specific device and

computer that you wish to be notified of and selecting the “Connected” event from the events list.

In this case, the “Client” and “Group” fields do not influence the triggering of the alert so there is no need to fill them out. Setting up a value for the “Group” field means that the alert will be triggered when the selected event occurs for any clients or computers in that group.

If you try to delete any items (Users, Groups, Computers etc.) that have been used in setting up an alert, you will receive a notification, and you will not be able to delete them.



### 9.3. Define Content Aware Alerts

To create a new Content Aware Alert corresponding to the policies defined in the Content Aware Protection module, go to Define Content Aware Alerts submenu option and click “Create”.



The screenshot shows the 'Create Alert' form with the following sections:

- Create Alert** (header) with a 'Show all departments' link on the right.
- Content Aware Alert Name**: A text field containing 'Alert Test #2'.
- Content Aware Alert Entities**: Three selection fields:
  - Groups**: A dropdown menu with 'Any' selected.
  - Computers**: A dropdown menu with 'Any' selected.
  - Users**: A dropdown menu with 'Any' selected.
- Content Aware Alerts fields**: Three dropdown menus:
  - Department**: 'Default Department'.
  - Content Policy**: 'PDF Test'.
  - Event**: 'Content Threat Detected'.
- Alert administrators**: A checkbox labeled '(root)' which is checked.

Then select the Group, Computer, User that you want to monitor, the Content Aware Policy to be considered, and the event that will trigger the notification. The filter is designed to make finding information quick and easy.

Example: if you want to be notified when a file containing credit card information is attached to an E-MAIL on one of the Financial Departments computers, you must set up an alert choosing the Financial Department as the monitored entity, the Content Aware Policy that inspects documents for that type of information and, finally, selecting the “Content Threat Detected” event from the events list.



**Note!**

Before creating the alert, you must make sure that the selected Content Aware Policy is enabled on the chosen Computer, User, Group or Department.

## 9.4. Define MDM Alerts

To create a new MDM alert go to the “Define MDM Alerts” tab and press the “Create” button.

The screenshot displays the Endpoint Protector web interface. The top navigation bar includes the logo, version number '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar. The left sidebar contains a menu with categories like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The 'Alerts' section is expanded to show 'Define Alerts', 'Define Content Aware Alerts', 'Define MDM Alerts', 'Alerts History', 'Content Aware Alerts History', and 'MDM Alerts History'. The main content area is titled 'Create Mobile Device Management Alert' and features a 'Show all departments' link. Under 'Alert fields', there are three dropdown menus: 'Type' (Any), 'Device Name' (Any), and 'Event' (Uninstall App). The 'Alert administrators' section contains a list of administrators with checkboxes: (root), (Marketing-admin), and (Financial-admin). A note below states: '\*Note: In order to have a complete list, please make sure administrators have their e-mail addresses set up from System Configuration > System Administrators > Edit Info.' At the bottom of the form are three buttons: 'Save', 'Save Add', and 'Back'. The footer shows 'Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.1 - Appliance'.

Alerts can be created for IOS MDM profile removal, Android application removal, SIM card changed and carrier changed.

## 9.5. System Alerts History

A history of the system alerts is kept in this tab for later auditing. Each event that triggers a system alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing the "Delete History" button.

The screenshot displays the 'System Alerts History' interface. At the top left is the 'ENDPOINT PROTECTOR' logo and the version number '4'. The main header reads 'Reporting and Administration Tool'. On the right, there is a language dropdown set to 'English' and a search bar with a magnifying glass icon and the text 'Advanced Search'. The left sidebar contains a list of navigation items: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Define System Alerts, System Alerts History, Define Alerts, Alerts History, Define Content Aware Alerts, Content Aware Alerts History, Define MDM Alerts, MDM Alerts History, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'System Alerts History' and features a 'Filter' section with a dropdown arrow. Below the filter is a table with the following data:

System Alert Name	System Event	System Event Option	Created at
Client Uninstall cc	Client Uninstall	-	8 September 2014 12:00
device control 100 test	Device Control - Logs Amount	100 rows	5 September 2014 0:00
Client Uninstall cc	Client Uninstall	-	4 September 2014 12:00
Client Uninstall cc	Client Uninstal	-	2 September 2014 0:00

Below the table, it shows '4 results' and a dropdown menu set to '50 per page'. A 'Delete History' button with a red 'X' icon is located below the table. At the bottom of the page, the footer contains 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' on the left and 'Ready Version 4.4.0.4' on the right.

## 9.6. Alerts History

A history of the alerts is kept in this tab for later auditing. Each event that triggers an alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing "Delete History" the button.

The screenshot shows the 'Alerts History' page in the Endpoint Protector interface. The page includes a sidebar with navigation options, a top navigation bar with the product name and version, and a main content area displaying a table of alert results. The table has columns for User, Computer, Device Type, Device, Event, and Created at. Below the table, there are buttons for 'Delete History' and 'Back', along with a pagination control showing '208 results' and '20 per page'.

User	Computer	Device Type	Device	Event	Created at
		USB Storage Device	Mass Storage Device	Connected	10 September 2014 16:29
		Serial ATA Controller	Intel(R) 7 Series/C216 Chipset Family SA...	Connected	10 September 2014 15:50
		Serial ATA Controller	Intel(R) 7 Series/C216 Chipset Family SA...	Connected	10 September 2014 15:50
		WiFi	Wireless Network Adapter (802.11 a/b/g/n...	Connected	10 September 2014 15:37
		Bluetooth	Bluetooth Device	Connected	10 September 2014 15:37
		Local Printers	HP Officejet 5600 series	Connected	10 September 2014 15:24
		Bluetooth	Bluetooth Device	Connected	10 September 2014 15:24
		WiFi	Wireless Network Adapter (802.11 a/b/g/n...	Connected	10 September 2014 15:24
		iPad	iPad	Connected	10 September 2014 11:42
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40
		iPad	iPad	Connected	10 September 2014 11:40



## 9.8. MDM Alerts History

A history of the MDM alerts is kept in this tab for later auditing. Each event that triggers an MDM alert will be saved here. Administrators can search for data more easily with the implemented filter, while if not needed anymore the logs can be deleted by pressing the "Delete History" button.

The screenshot shows the Endpoint Protector interface. The top header includes the logo, version number '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Advanced Search' link. The sidebar on the left lists various management categories like Dashboard, Endpoint Management, Alerts, etc. The main content area is titled 'Mobile Device Management Alerts History' and features a 'Filter' section above a table of results. The table lists three 'Uninstal App' events with their respective OS types, device names, and creation timestamps. Below the table are 'Delete History' and 'Back' buttons.

Event Name	Type OS	Device Name	Created at
Uninstal App	Any	Any	12 March 2014 13:02
Uninstal App	Any	Any	12 March 2014 9:35
Uninstal App	Any	Any	11 March 2014 16:35

3 results [ 20 per page]

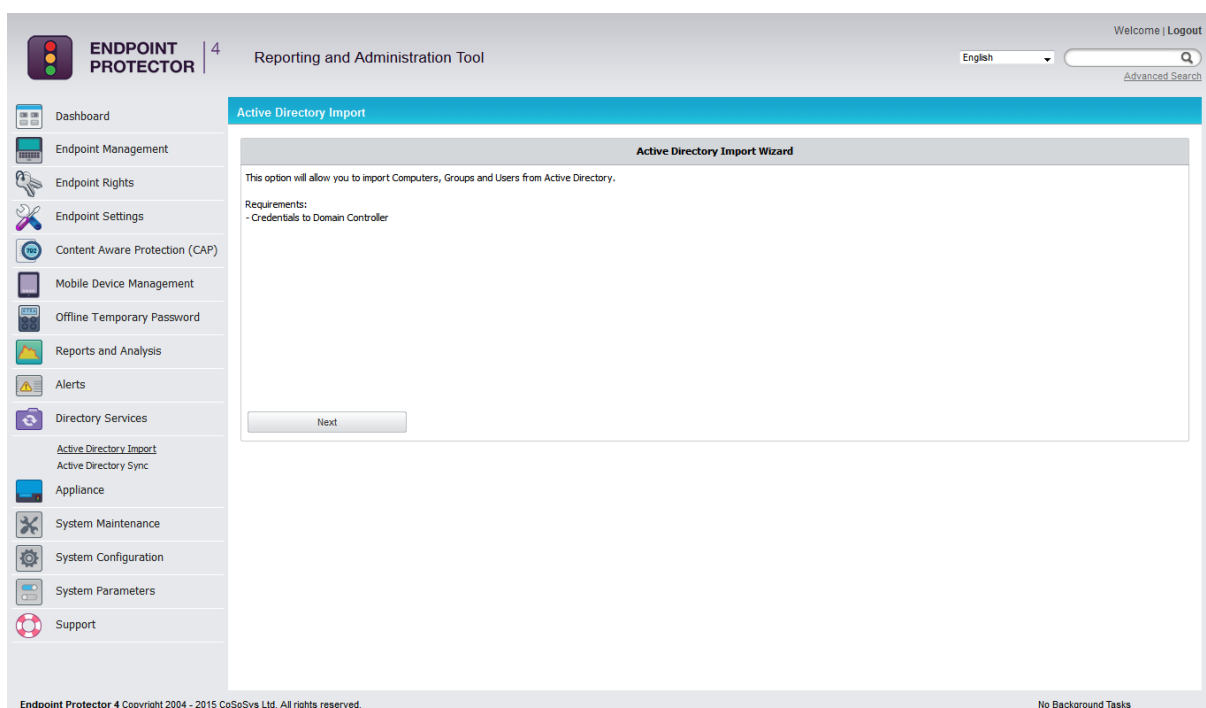
Buttons: Delete History, Back

Footer: Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.3 - Appliance

# 10. Directory Services

## 10.1. Active Directory Import

This module allows you to import Computers, Groups and Users from Active Directory (where available).



The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. The top navigation bar includes the logo, version number '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Advanced Search' and 'Welcome | Logout' links. A left-hand sidebar lists various management options: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services (with sub-items for Active Directory Import and Active Directory Sync), Appliance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Active Directory Import' and features a wizard box. The wizard box contains the text: 'This option will allow you to import Computers, Groups and Users from Active Directory.' followed by 'Requirements: - Credentials to Domain Controller'. A 'Next' button is located at the bottom of the wizard box. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2015 CoSoSys Ltd. All rights reserved.' on the left and 'No Background Tasks' on the right.

If you have the requirements, simply click **Next**.

The screenshot shows the 'Active Directory Import' configuration page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and Directory Services. The main content area shows a green success message: 'Connection is valid. Standard Connection.' Below this is a form titled 'Active Directory Import. Step 1: Define Connection' with the following fields and values:

Field	Value	Example
Domain Controller Server Name:	w2003server	Example: w2003server
Domain Controller Port:	389	Default: 389 (Global Catalog: 3268)
Domain/Search In:	example.cososys.com	Example: example.cososys.com
User:	admin	Example: admin@example.cososys.com
Password:	*****	

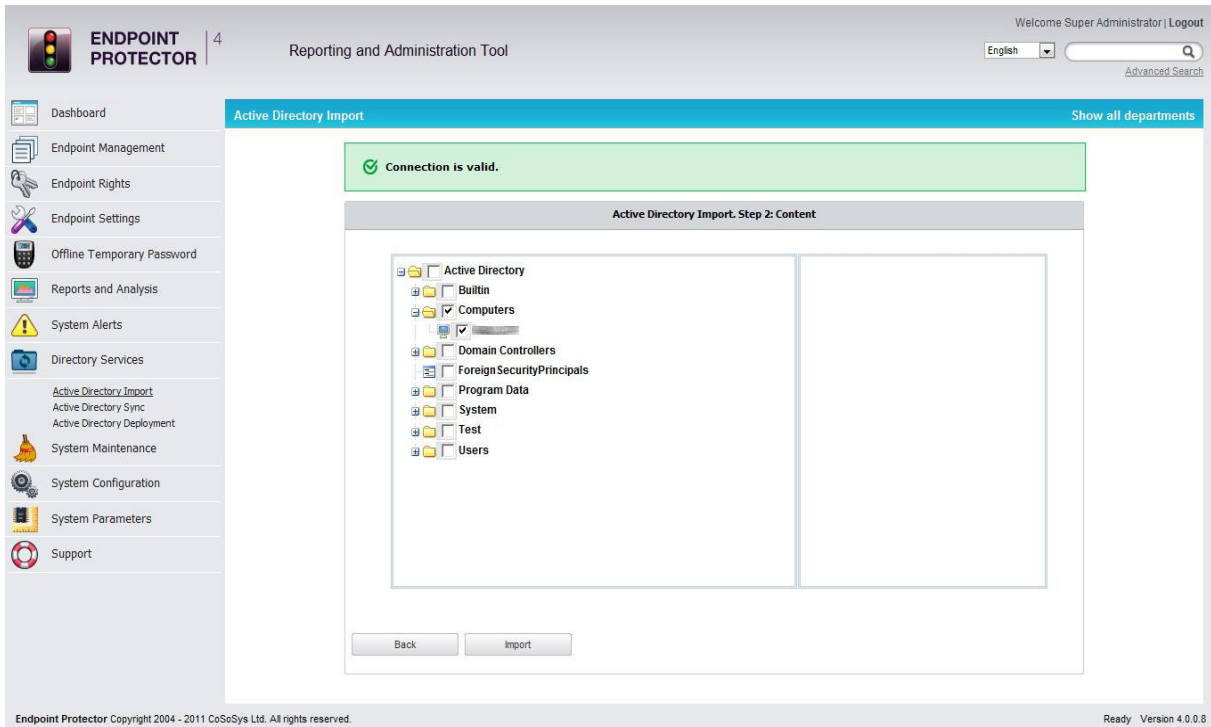
At the bottom of the form are three buttons: 'Back', 'Next', and 'Test Connection'. The footer of the page reads 'Endpoint Protector 4 Copyright 2004 - 2015 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks'.

Enter the Active Directory domain controller server name, the domain name and a username and password in the format as in the examples presented in the form. First, you can push the "Test Connection" button to test if the connection is established successfully. If the connection is valid, push the "Next" button. This operation might take some time, depending on the volume of data that needs to be imported.

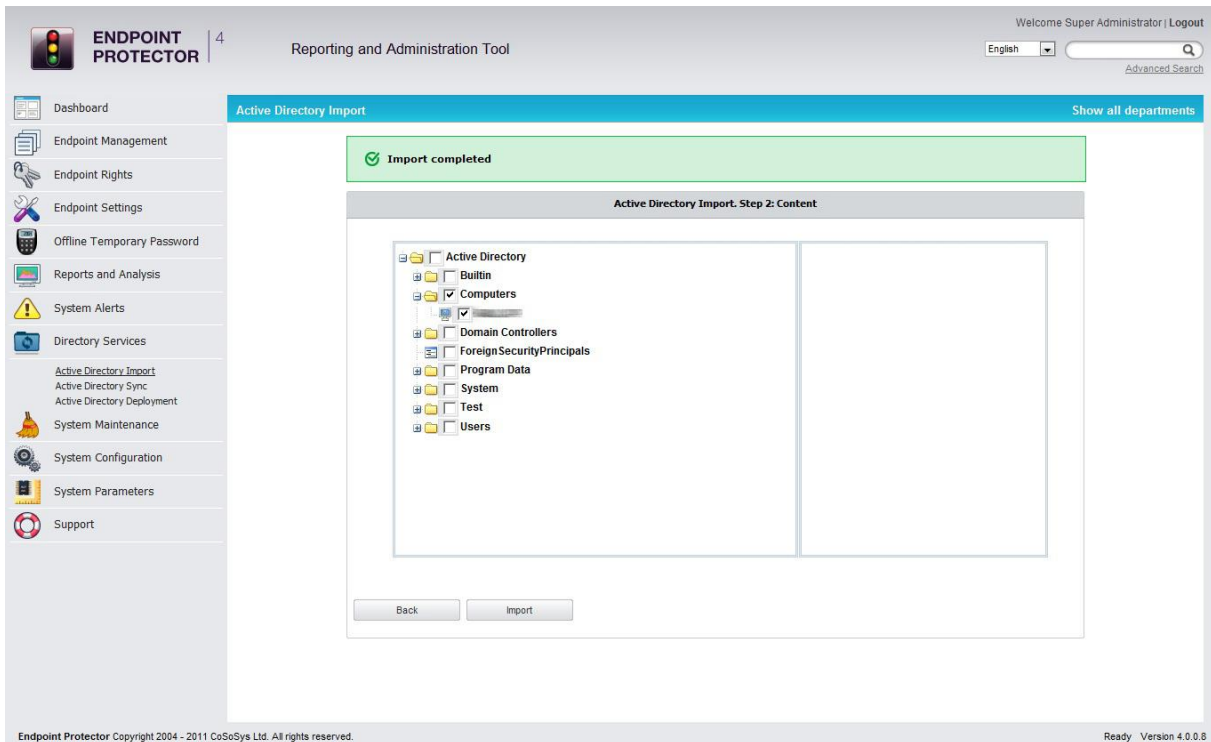
### Note!

When having to import a very large number of entities from the Active Directory, we recommend using the "Domain/Search In" filter from the AD Import page in order to get only the relevant information displayed for import. Due to browser limitations, importing the whole AD structure may impede the display of the import tree if it contains a very large number of entities.

In the next step, simply select what items you would like to import by clicking the checkbox next to them and finally, select "Import".



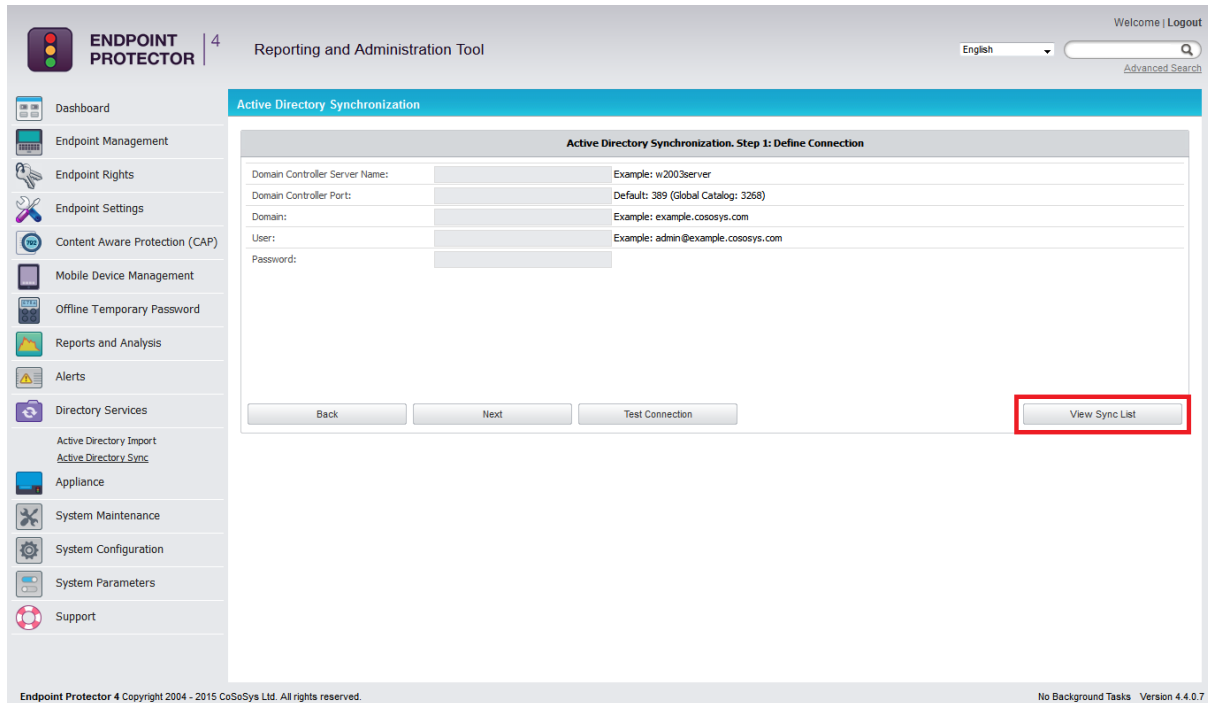
If the import procedure was successful, you will see the message "Import completed".



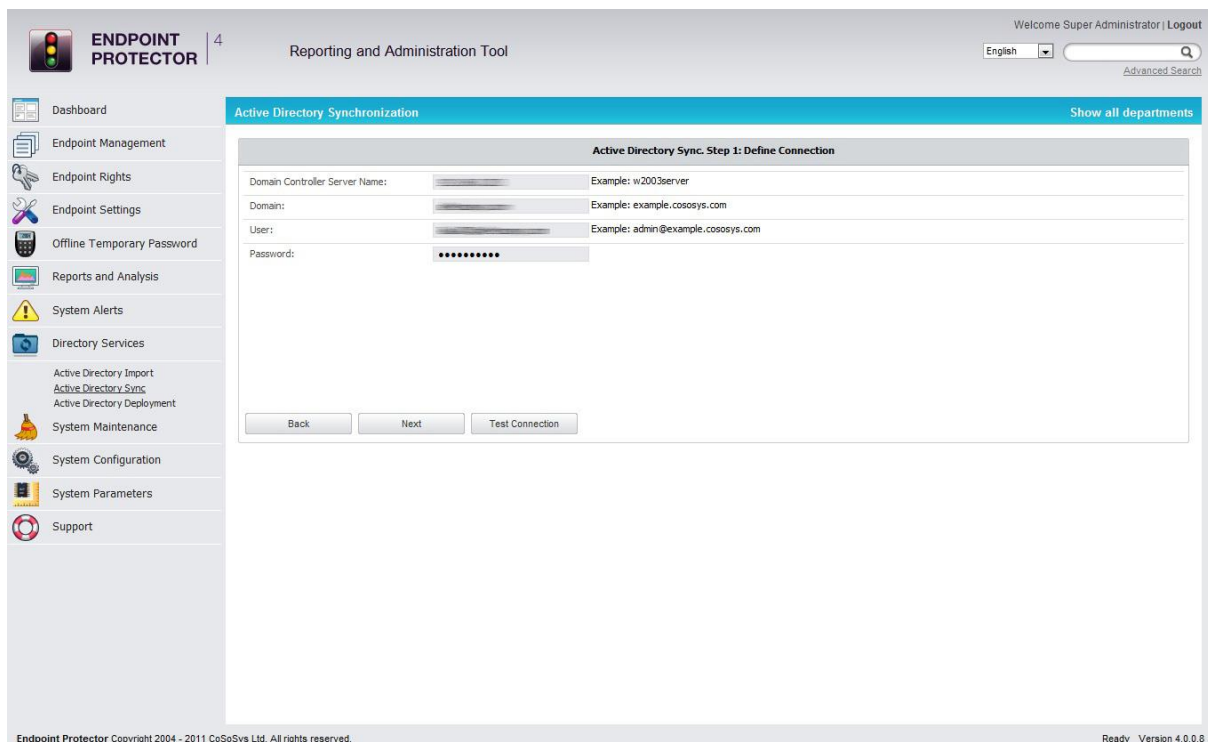


## 10.2. Active Directory Sync

This module allows you to synchronize the entities in Endpoint Protector with the entities in Active Directory (Computers, Users, and Groups).

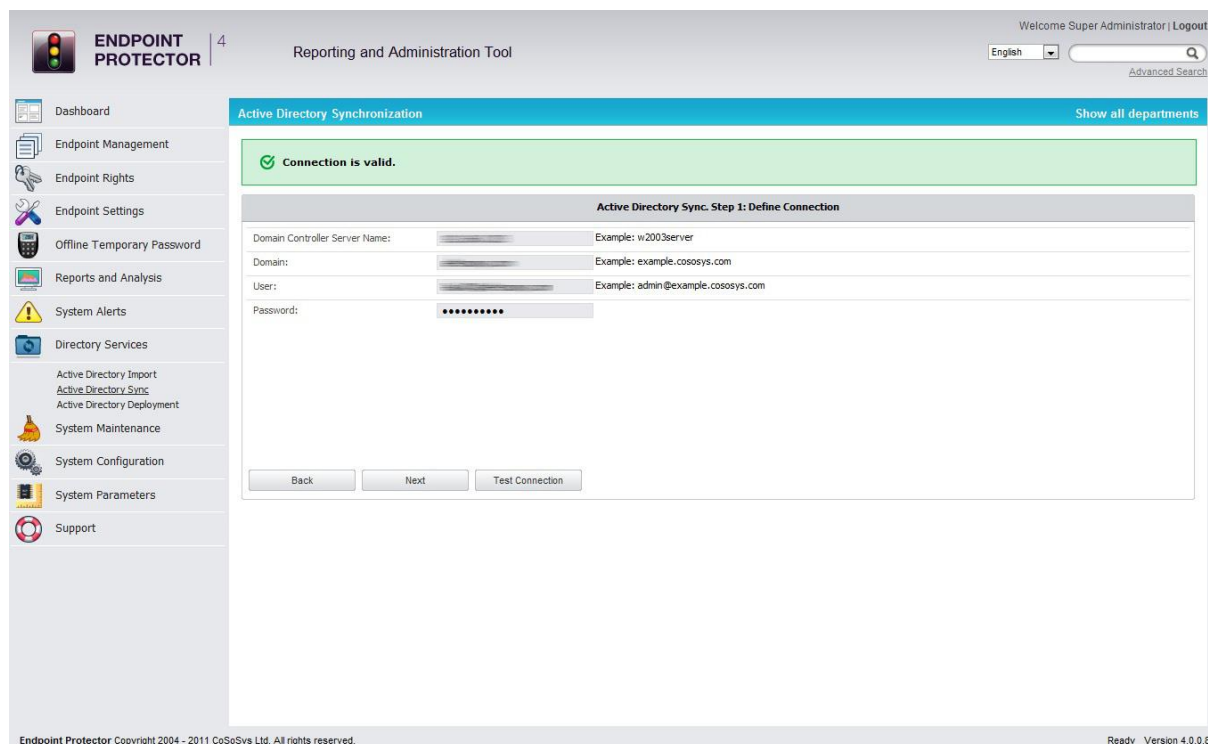


You can either examine existing synchronizations by clicking **View Sync List** or, if you have the requirements, simply click "Next" to set up your synchronization settings.



Enter the Active Directory domain controller server name, the domain name and a username and password in the format as in the examples presented in the form.

You can also check if your settings are correct by clicking the “Test Connection” button.



The screenshot shows the Endpoint Protector Reporting and Administration Tool interface. The main content area is titled "Active Directory Synchronization" and displays a green message: "Connection is valid." Below this, the "Active Directory Sync. Step 1: Define Connection" form is visible. The form contains the following fields and values:

Field	Value
Domain Controller Server Name:	Example: w2003server
Domain:	Example: example.cososys.com
User:	Example: admin@example.cososys.com
Password:	*****

At the bottom of the form, there are three buttons: "Back", "Next", and "Test Connection". The "Test Connection" button is highlighted.

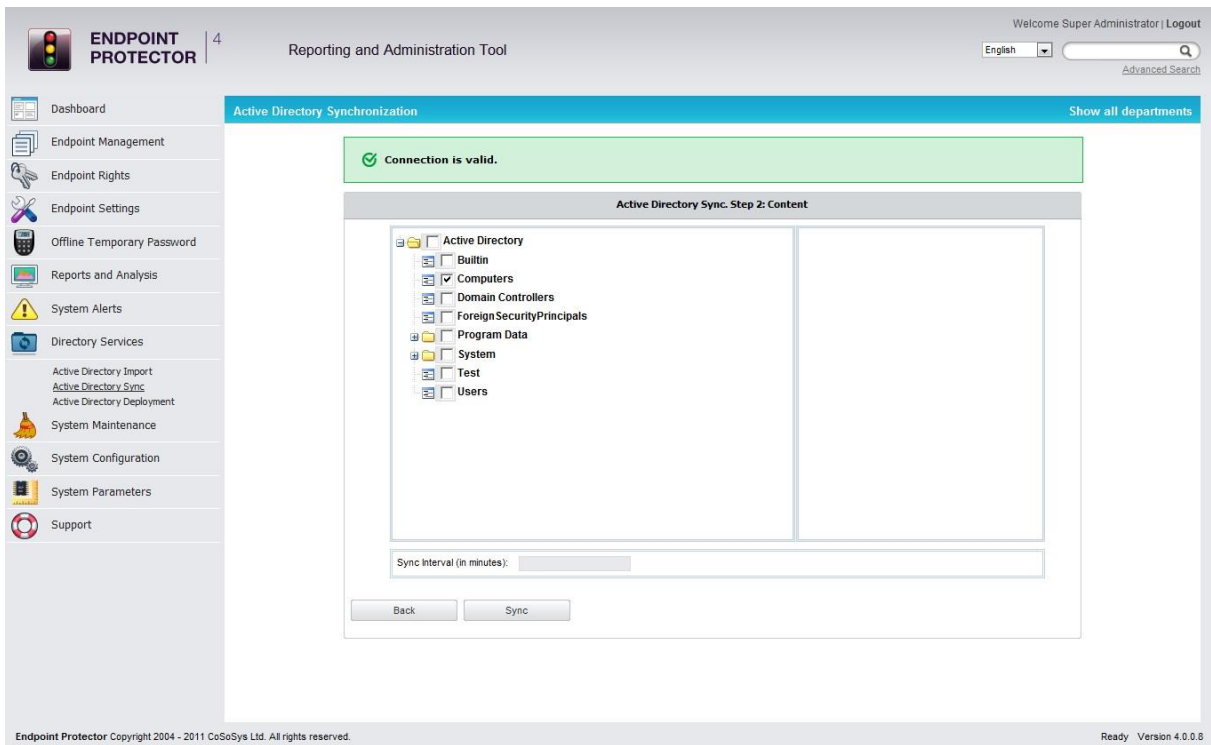
You should see a message “Connection is valid” on the top of the page.

Click “Next” to continue.

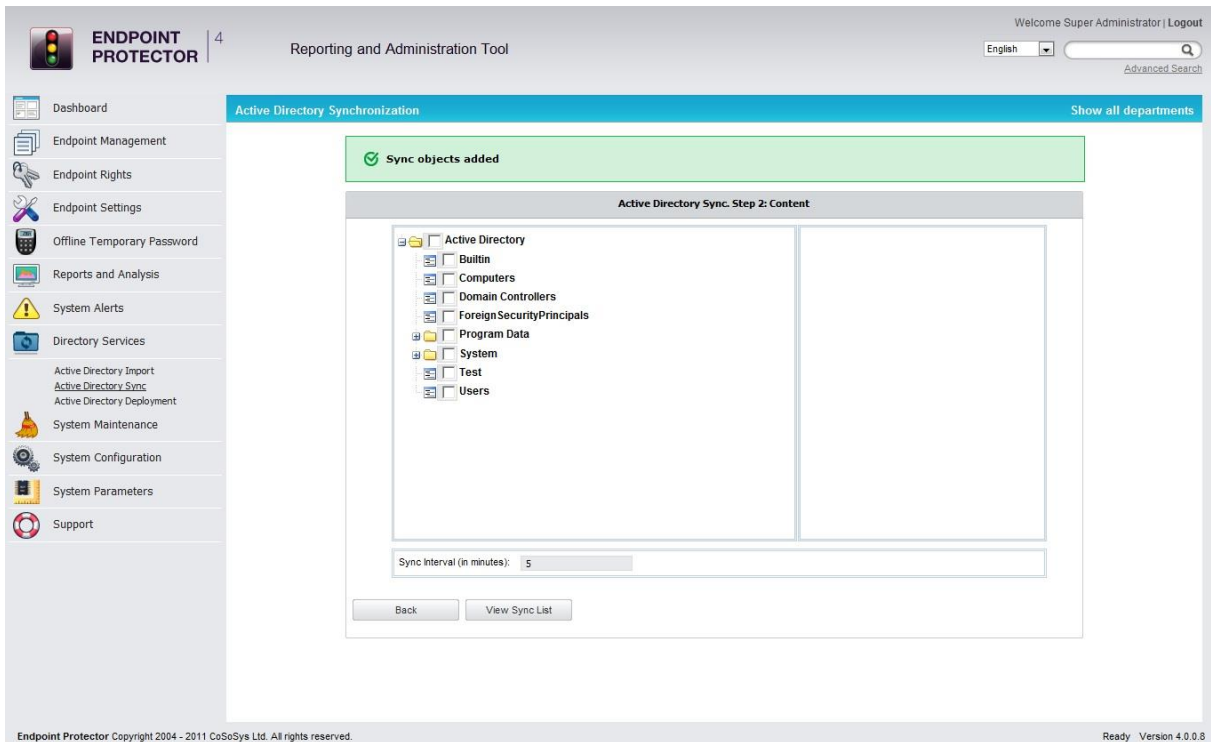
### Note!

This operation might take some time, depending on the volume of data that needs to be synchronized.

In the next step, simply select what items you would like to synchronize by clicking the checkbox next to them, define a sync interval and select “Sync”.



You will see the message "Sync object added".



You can set up multiple synchronizations from multiple locations at once. These can be viewed and canceled in the "View Sync List".

The screenshot displays the 'Active Directory Synchronization' page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, and System Alerts. The main content area features a green notification banner stating 'Sync objects added'. Below this is a table titled 'Active Synchronizations' with columns for Sync Interval, Domain Controller, User, Last Sync, and Actions. The table contains one entry with a sync interval of 5 minutes and a last sync time of 2011-06-07 11:08:00. A 'Back' button is located at the bottom left, and a 'Refresh' button is at the bottom right. The footer contains copyright information and the version number 4.0.0.8.

Endpoint Protector Reporting and Administration Tool

Welcome Super Administrator | Logout

English

Advanced Search

Active Directory Synchronization

Show all departments

Sync objects added

Sync Interval	Domain Controller	User	Last Sync	Actions
5 minutes			2011-06-07 11:08:00	

Back Refresh

Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved. Ready Version 4.0.0.8

# 11. Appliance

## 11.1. Server Information

This view offers the administrator general information about the Server, the Fail/Over function, the total Disk Usage and the Uptime.

The screenshot displays the 'Endpoint Protector Appliance - System Information' page. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, Server Information, Server Maintenance, System Maintenance, System Configuration, System Parameters, and Support. The main content area is titled 'Endpoint Protector Appliance - System Information' and contains several sections:

- System Fail/Over Status:** System Fail/Over Status: **Disabled - N/A**
- Disk Space:**

Disk Space System:	<b>2.0G - 12% from 19G</b>
Disk Space EPP Server:	<b>708M - 3% from 28G</b>
Logs on Disk:	4.0K stored in /var/epfiles/logs
Shadows on Disk:	4.0K stored in /var/epfiles/shadows
- Info Disk Space:**

Please consider taking one of the following actions in **System Maintenance** tab if you have used up 95% of the storage resources available on the appliance:

  1. Back-up & Save old or unneeded logs by going to File Maintenance and selecting the suitable option.
  2. Remove old or unneeded logs by going to File Maintenance and selecting the suitable option.

Alternatively, go to System Configuration > System Policies and:

  3. Disable or Change the granularity of your policies. Activating File Tracing / Shadowing under Global Settings will greatly affect your Server performance. It is recommended to activate File Tracing / File Shadowing for specific Computers.
  4. Enable the Automatic Log Cleanup feature and Set the HDD Disk Space percentage at which the process will begin
- Database Disk Space occupied:**

Database Disk Space occupied:	20M stored in /var/lib/mysql/epdatabase
Number of Logs in Database:	16
Number of Files Traced:	0
Number of Files Shadowed:	0
- System:**

Uptime:	13:20:02 up 26 min, 0 users, load average: 0.00, 0.00, 0.00 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 10.04-4LTS1
System Information Update:	2014-Nov-28 13:20:02

Footer: Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. No Background Tasks Version 4.4.0.6

## 11.2. Server Maintenance

From this view the administrator can: setup a preferential time zone and NTP synchronization server, configure his IP and DNS, perform routine operations such as Reboot and Shutdown as well as Enable/Disable the SSH access.

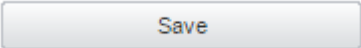
The screenshot displays the 'Endpoint Protector Appliance - Server Maintenance' configuration page. It features a sidebar on the left with navigation options such as Dashboard, Endpoint Management, and System Configuration. The main content area is organized into several sections:

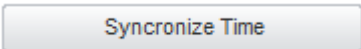
- Time Zone:** Includes a dropdown for 'Please select your timezone' (set to Europe / Bucharest), an NTP Server field (pool.ntp.org), a frequency dropdown (Once a week), and a 'Current server time' field (2014-11-28 13:26:28). Buttons for 'Save', 'Synchronize Time', and 'Update current Time' are present.
- IP Configuration:** Fields for IP Address (192.168.7.159), Gateway (192.168.7.1), and Netmask (255.255.255.0). A note states: '\*Note: Modifying Network Configuration could stop communication between EPP Clients and Server.'
- DNS Configuration:** Fields for DNS 1 (192.168.0.1) and DNS 2. A note states: '\*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:** Buttons for 'Reboot the Hardware Appliance', 'Shutdown the Hardware Appliance', and 'Reset to Factory Defaults'.
- SSH Server:** Radio buttons for 'Enable' (selected) and 'Disable'.

The footer of the interface includes 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks Version 4.4.0.6'.

### 11.2.1. Time Zone Settings

This menu allows the administrator to set a preferential time zone and/or sync the appliance to a NTP source.

Pressing the  button will save all the changes, but it will not trigger the synchronization process!

Pressing the  button will trigger the synchronization, which will occur in the next 5 minutes. The Alerts and Logs will be reported after the 5 minutes in a format of your choice.

Pressing the  button will update the display below.

Current server time

2014-11-28 13:54:51

### Note!

The appliances come preset to sync once a week with [pool.ntp.org](http://pool.ntp.org).

## 11.2.2. Network Settings

Here you can change the network settings for the appliance to communicate correctly in your network.

### Attention!

After you change the IP address, close the Internet browser, then reopen a new instance of your browser. Afterwards try to access the Endpoint Protector Administration and Reporting Tool with the NEW IP address!

## 11.2.3. 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.

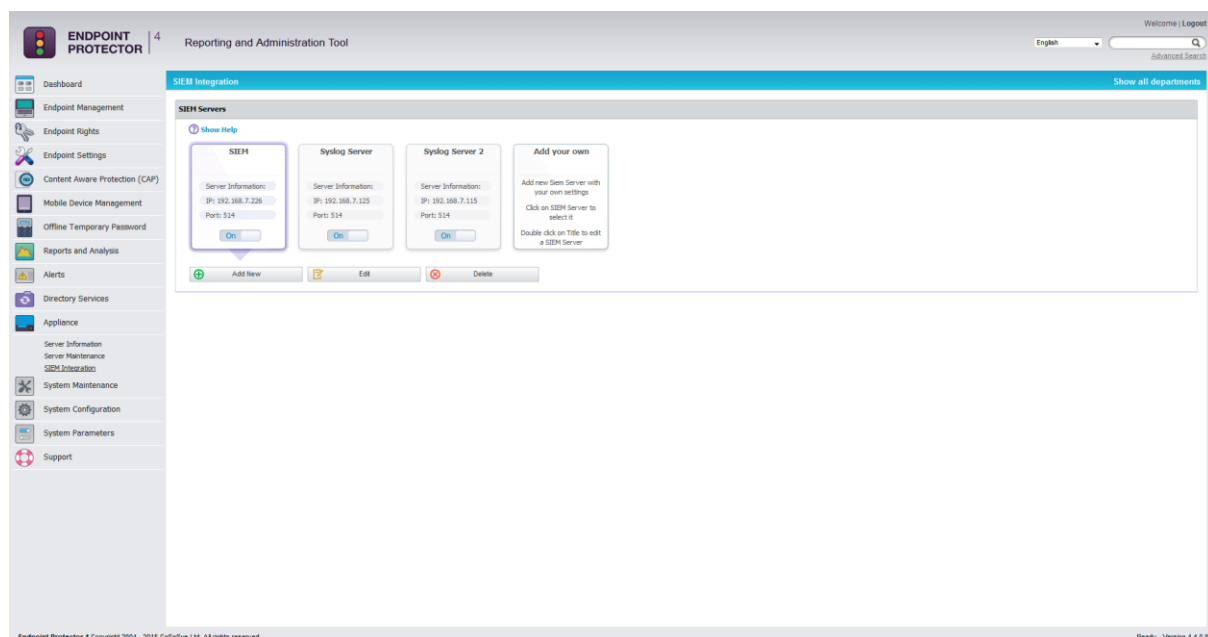
## 11.2.4. SSH Server

This option will either enable or disable the access to the Appliance through the SSH protocol. It is recommended to be set on **Enable** before requesting Support access.

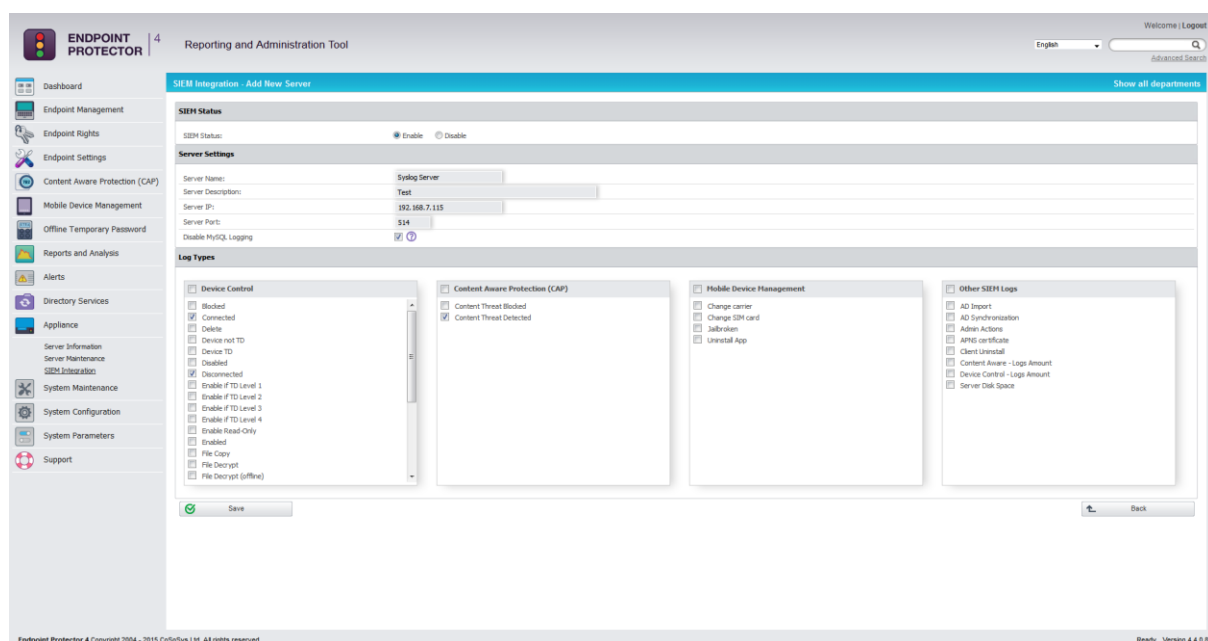
## 11.3. SIEM Integration

Third-party security information and event management (SIEM) tools allow the logging and analysis of logs generated by network devices and software. Integration with SIEM technology allows Endpoint Protector to transfer activity events to a SIEM server for analysis and reporting.

Administrators can access SIEM Integration from the sub-menu at Appliance -> SIEM Integration.



The available actions are: **Add New**, **Edit** and **Delete**. A new SIEM server can be added also by clicking on the **Add your own** icon. An existing server address can be edited also by double-clicking the upper part of the policy icon.



## Note!

The maximum number of SIEM hosts configured at one any given time is four (4). The menu for each SIEM address consists of the following settings and parameters: **Server Name**, **Server Description**, **Server IP**, **Server Port** and **Disable MySQL Logging**.

## Note!

Checking the option to Disable MySQL Logging will set the system to record logs only on the SIEM target and not inside Endpoint Protector itself.



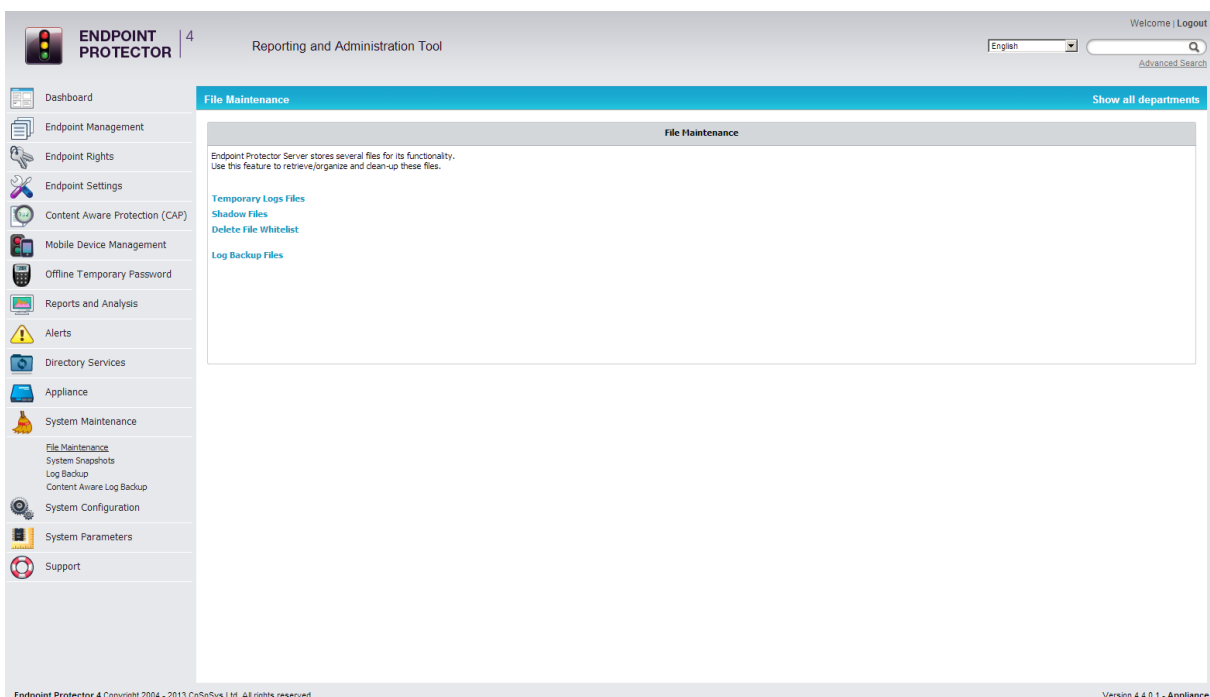
The TCP ports used by rsyslog are by default 513 and 514.

After all the above parameters are set to point to a valid SIEM server, the administrator must choose from Log Types which events in particular to send to the SIEM target.

# 12. System Maintenance

## 12.1. File Maintenance

This module allows the administrator to retrieve/organize and clean-up files used by Endpoint Protector Server.



The available options are:

- **Temporary Log Files:** allows archiving and deleting log files from a selected client computer
- **Shadow Files:** allows archiving and deleting shadowed files from a selected client computer
- **Log Backup Files:** allows archiving and deleting previously backed up log files

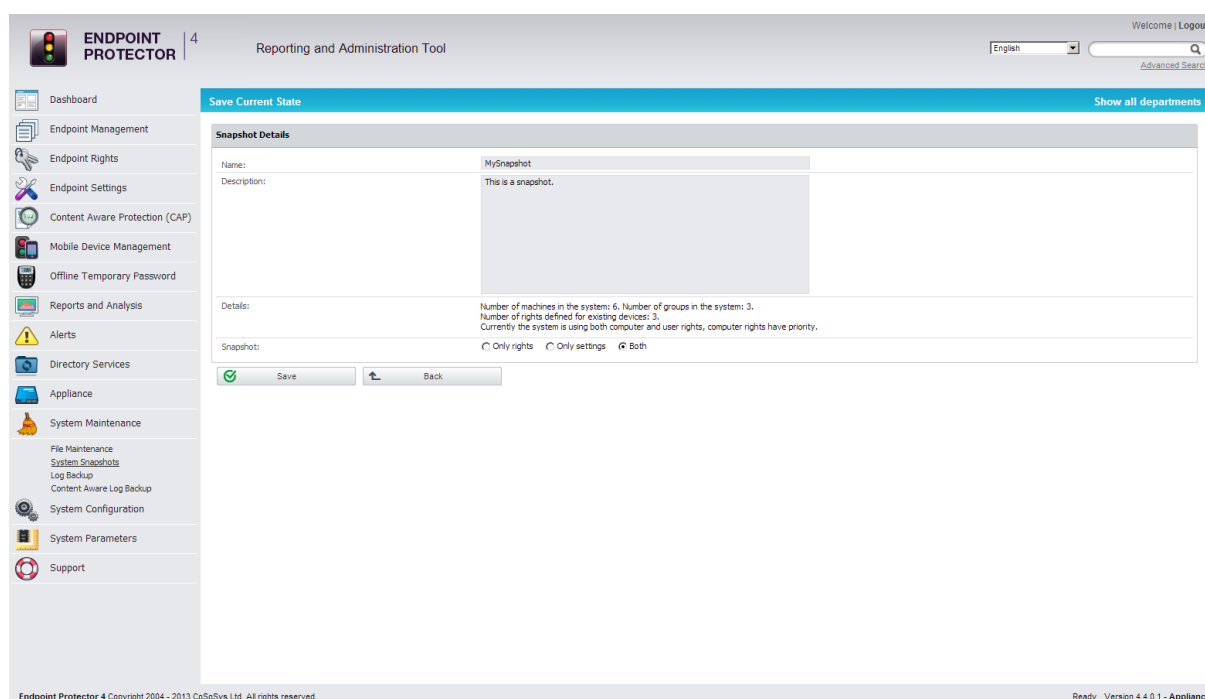
To archive a previously selected set of files, click the “Save as Zip” button, while to permanently remove a set of files from the Endpoint Protector Server use the “Delete” button.

## 12.2. System Snapshots

The System Snapshots module allows you to save all device control rights and settings in the system and restore them later, if needed.

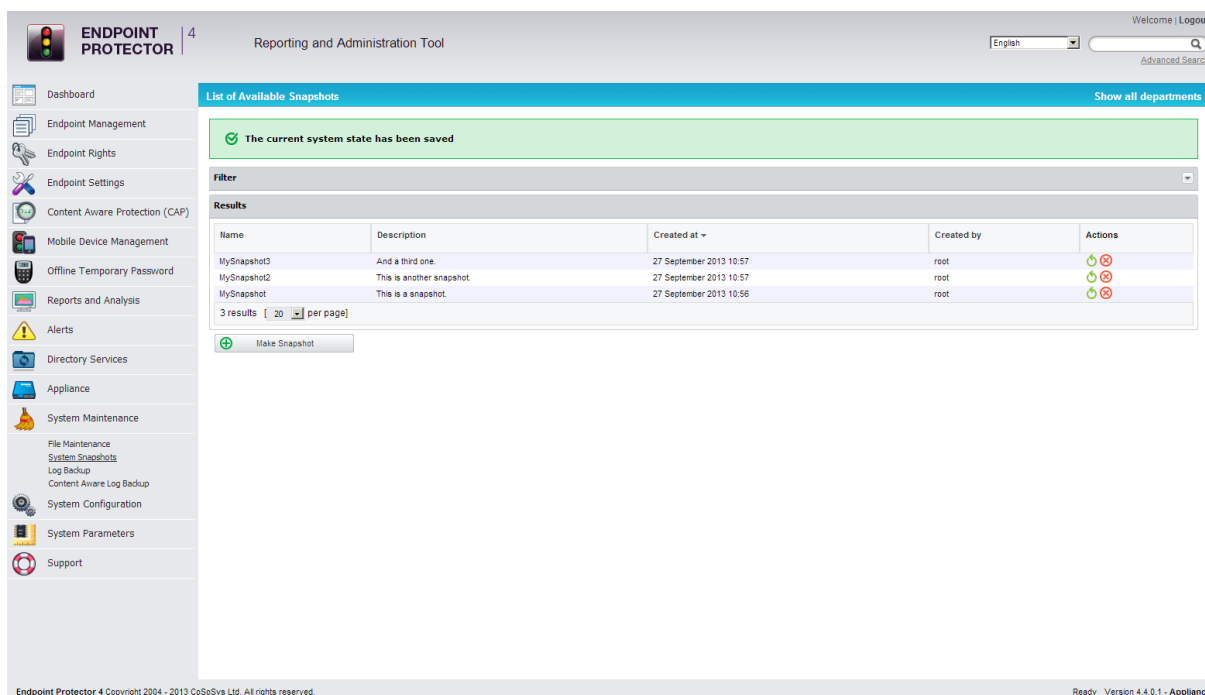
After installing the Endpoint Protector 4 Server, we strongly recommend that you create a System Snapshot before modifying anything. In this case you can revert back to the original settings if you configure the server incorrectly.

To create a System Snapshot, access the module from System Configuration and click “Make Snapshot”.



Enter a name for the snapshot, and a description. Select also what you wish to store in the snapshot, Only Rights, Only Settings, or Both.

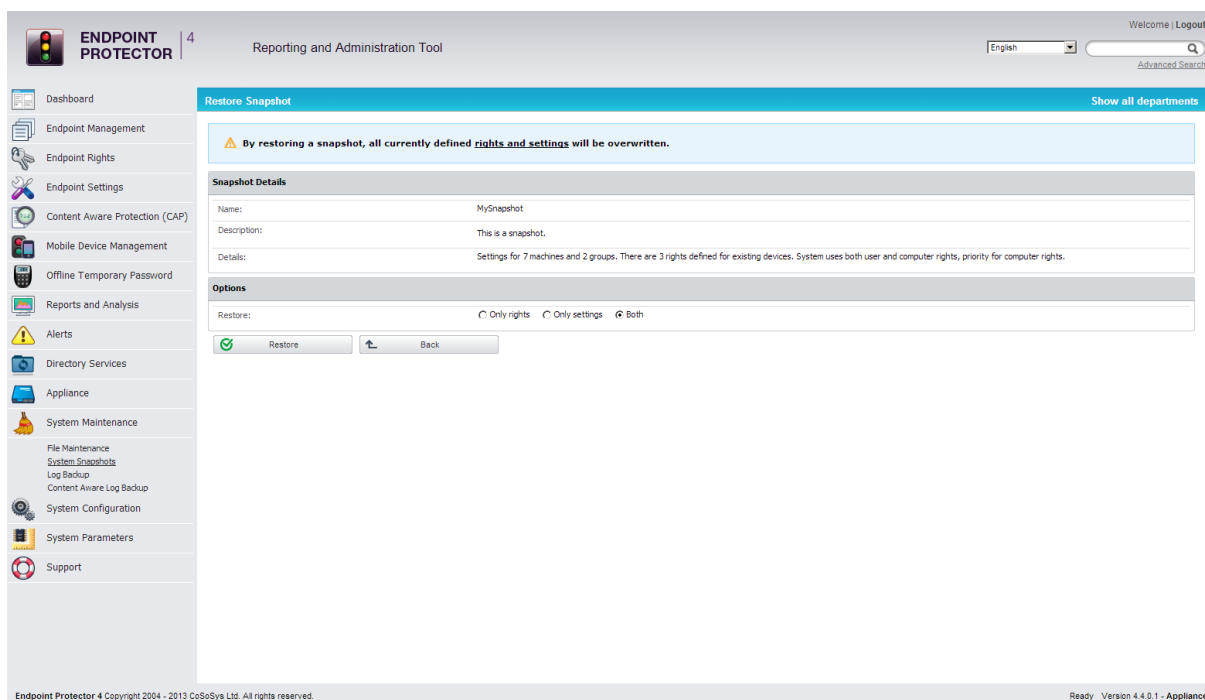
Finally, click “Save”.



Your snapshot will appear in the list of System Snapshots.

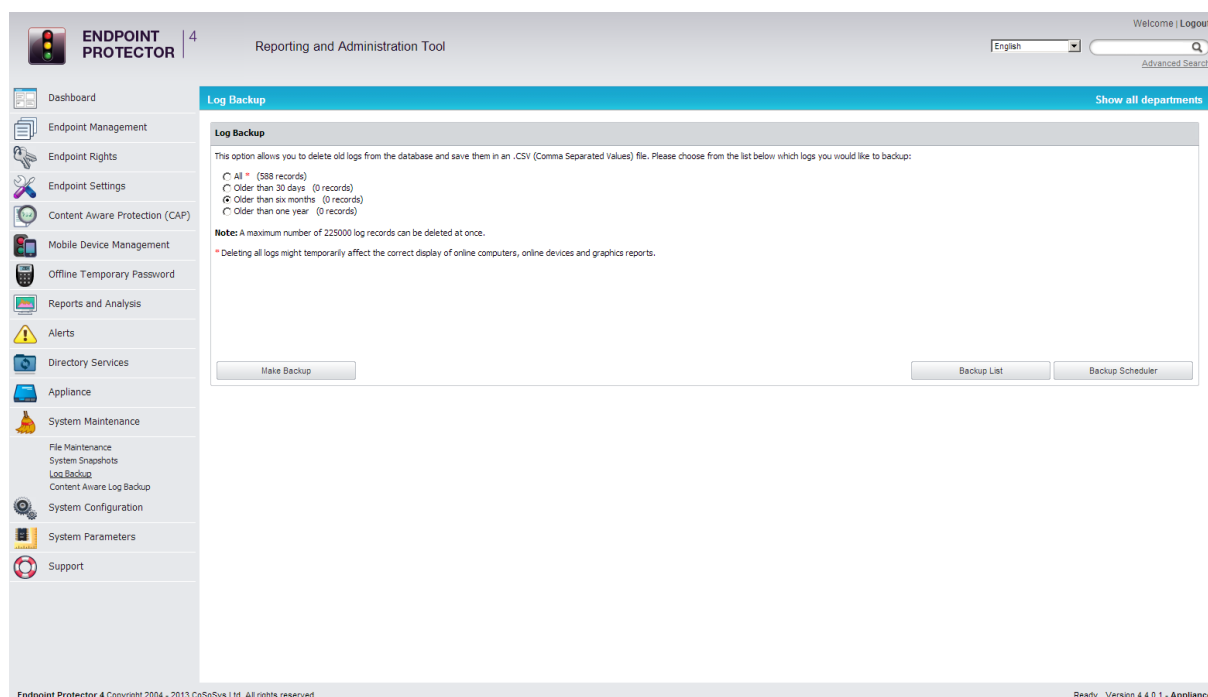
To restore a previously created snapshot click the "Restore" button next to the desired snapshot. - Restore

Confirm the action by clicking the "Restore" button again in the next window.

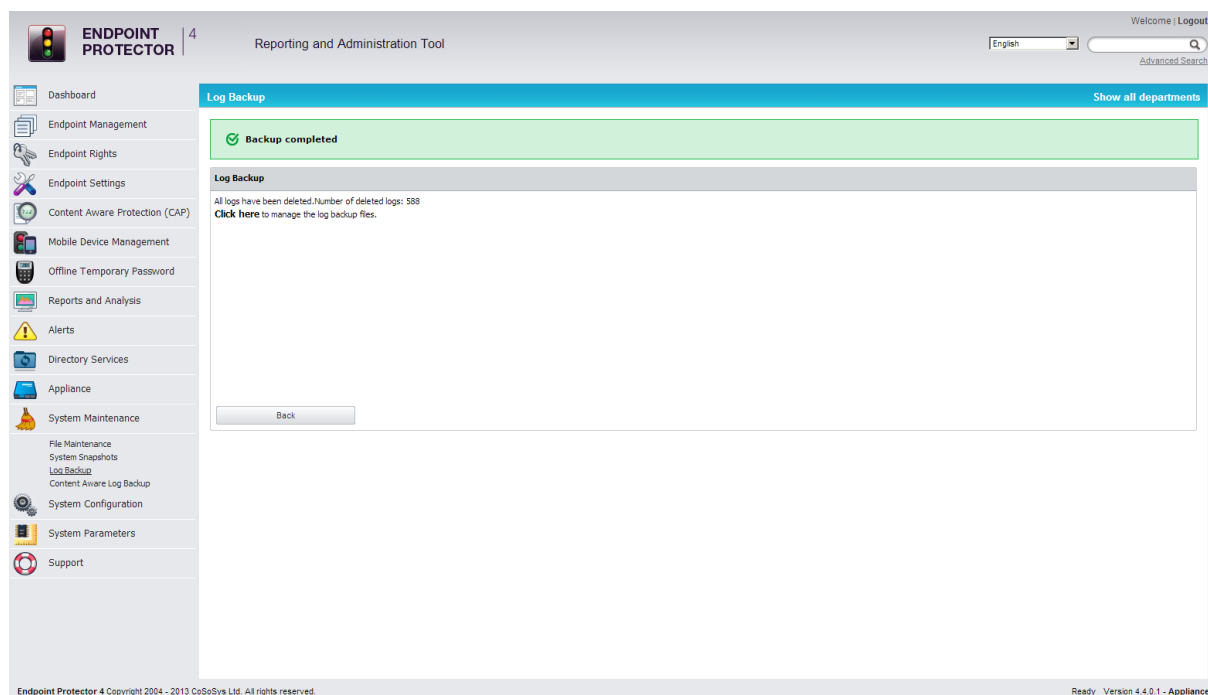


## 12.3. Log Backup

This module allows you to delete old logs from the database and save them in a .CSV document.



Here you can select the logs you wish to back-up. Simply select an option and click "Make Backup".

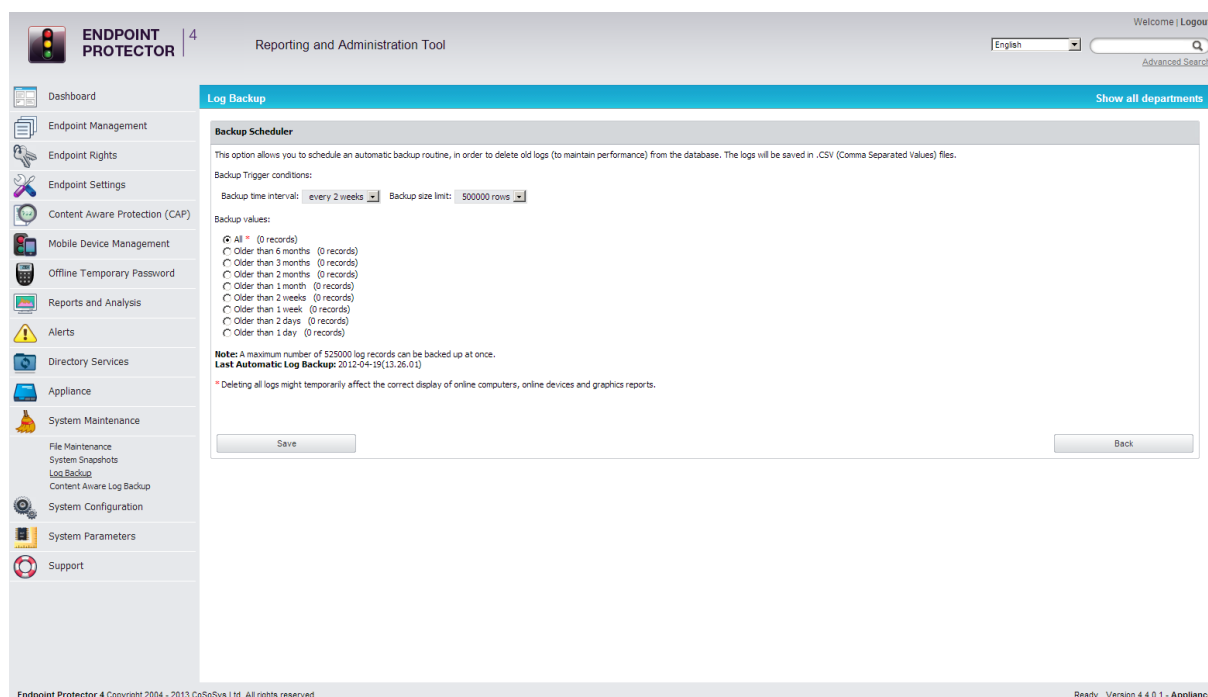


You should see the message "Backup Completed" in the top-center of your browser.

You can download and view the logs by selecting the "click here" link.

### 12.3.1. Backup Scheduler (Automatic Log Backup)

You can back up your log files also automatically by using the Backup Scheduler option.



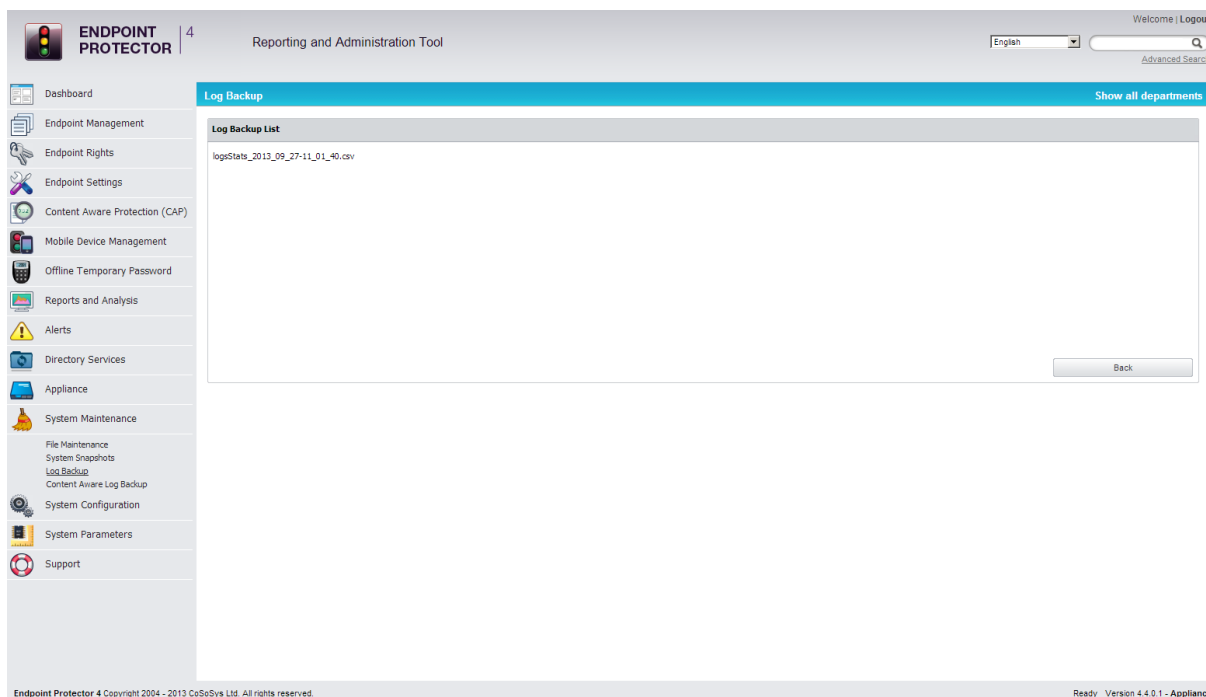
Here you can schedule an automatic backup routine by setting two trigger conditions:

**Backup time interval** - allows you to select a certain time interval for repeating the backup operation

**Backup size limit** - allows you to select a maximum size for the logs to be backed up

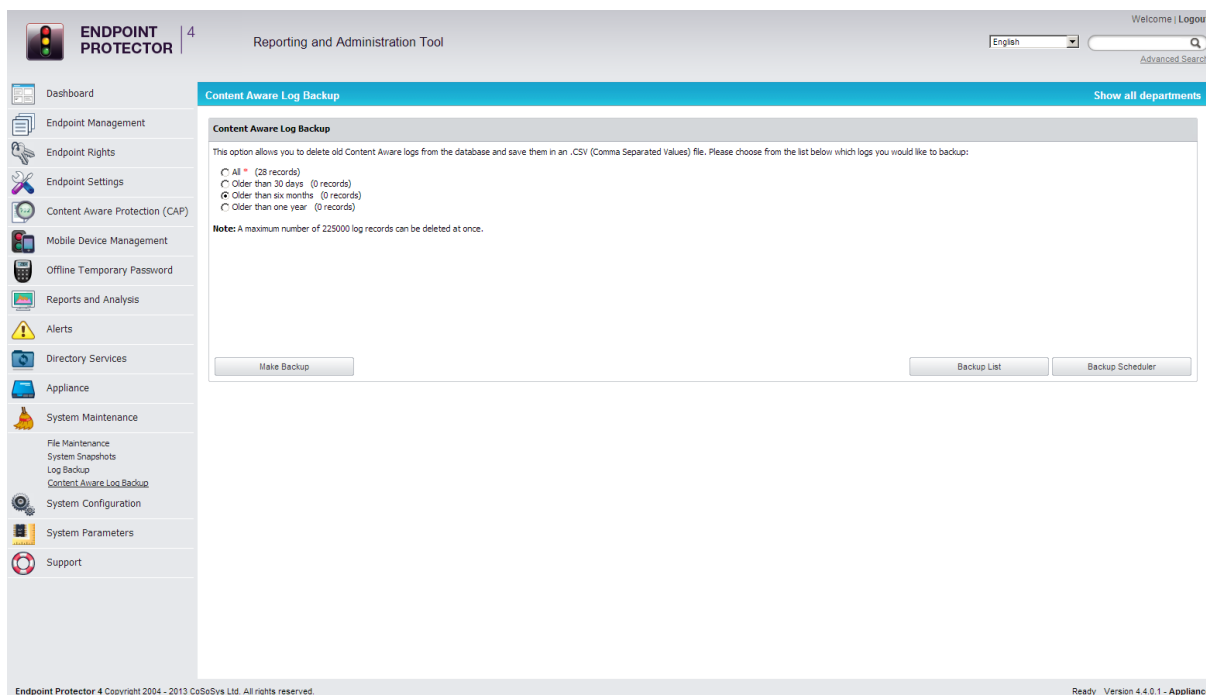
In case that you don't wish to set a specific value for one or both of these options, please leave the specific field(s) blank. After specifying the logs to be backed up automatically based on their creation time, please click "Save" in order for your options to be applied.

You can view the created backups by using the Backup List option.

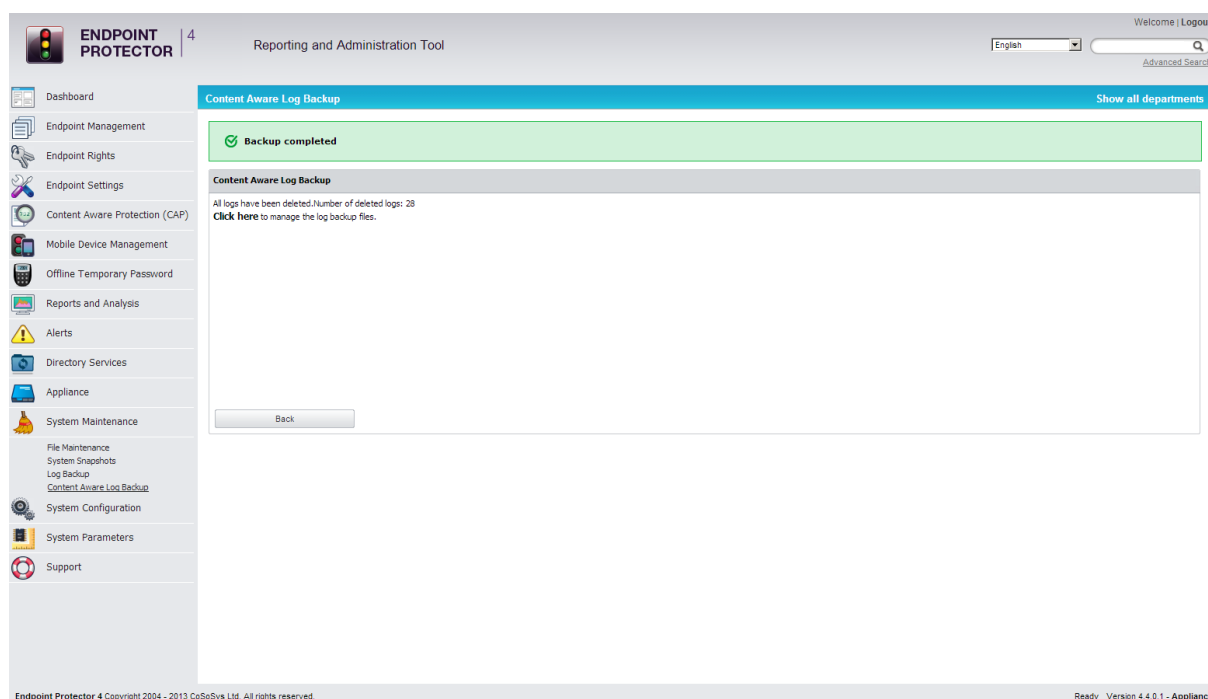


## 12.4. Content Aware Log Backup

This module allows you to delete old content aware logs from the database and save them in a .CSV document.



Here you can select the logs you wish to backup. Simply select an option and click "Make Backup".

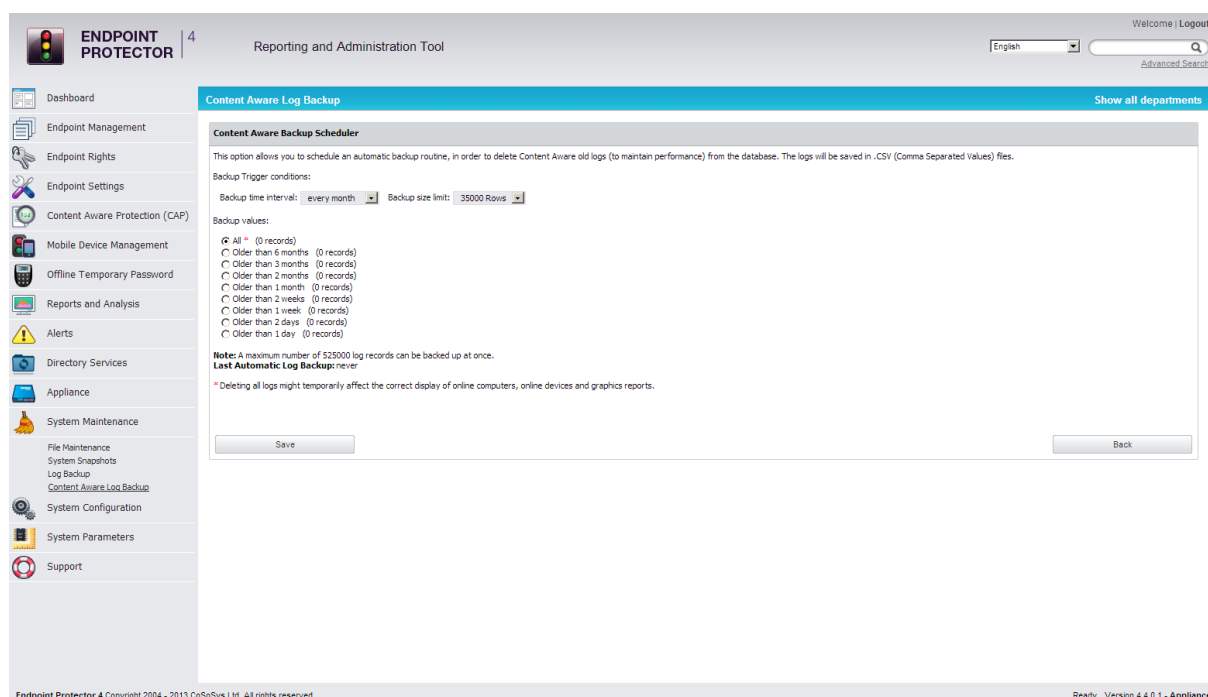


You should see the message “Backup Completed” in the top-center of your browser.

You can download and view the logs by selecting the “click here” link.

### 12.4.1. Automatic Scheduler (Automatic CAP Log Backup)

You can back up your log files also automatically by using the Backup Scheduler option.



Here you can schedule an automatic backup routine by setting two trigger conditions:

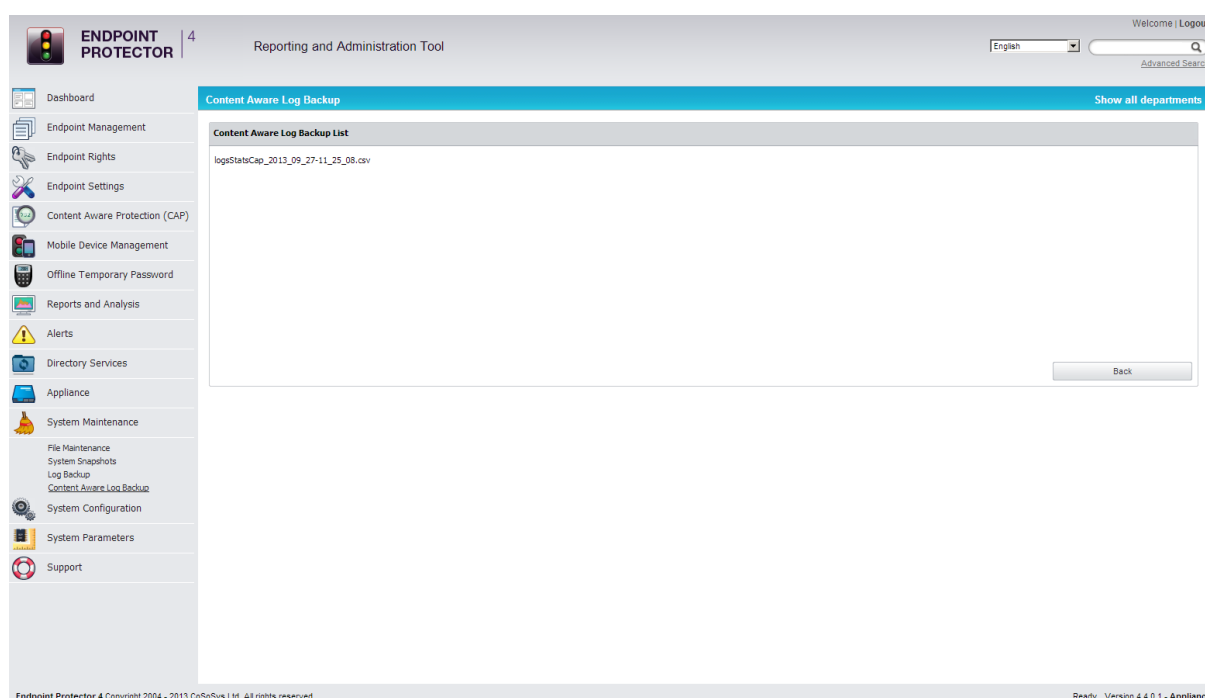


Backup time interval - allows you to select a certain time interval for repeating the backup operation

Backup size limit - allows you to select a maximum size for the logs to be backed up

In case that you don't wish to set a specific value for one or both of these options, please leave the specific field(s) blank. After specifying the logs to be backed up automatically based on their creation time, please click "Save" in order for your options to be applied.

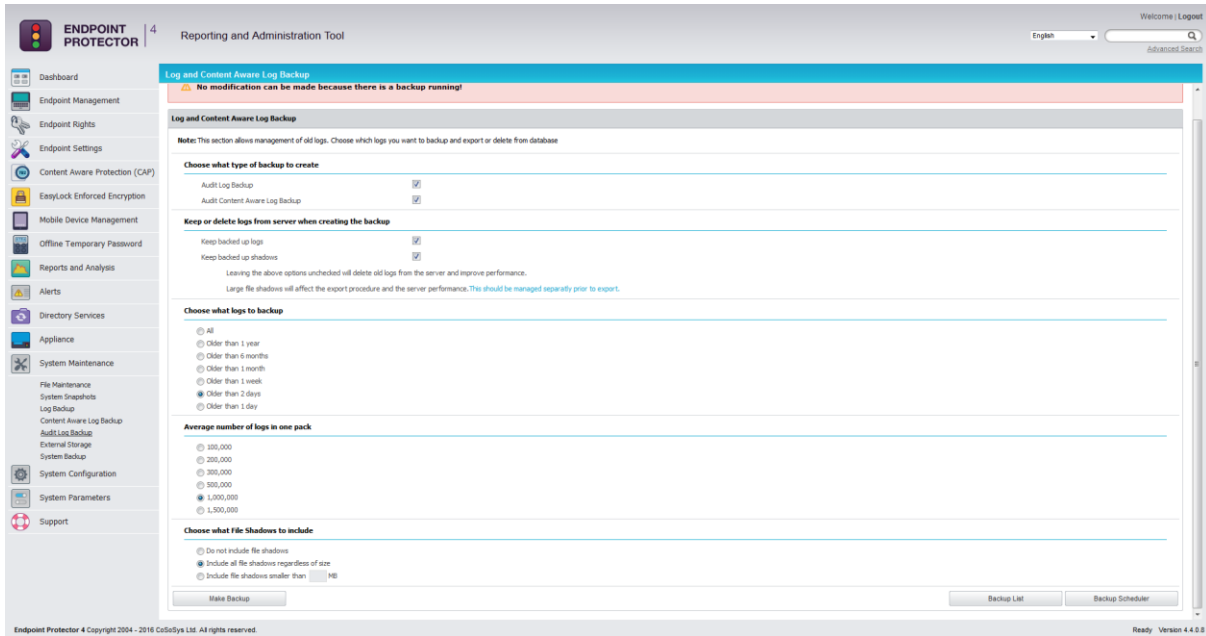
You can view the created backups by using the Backup List option.



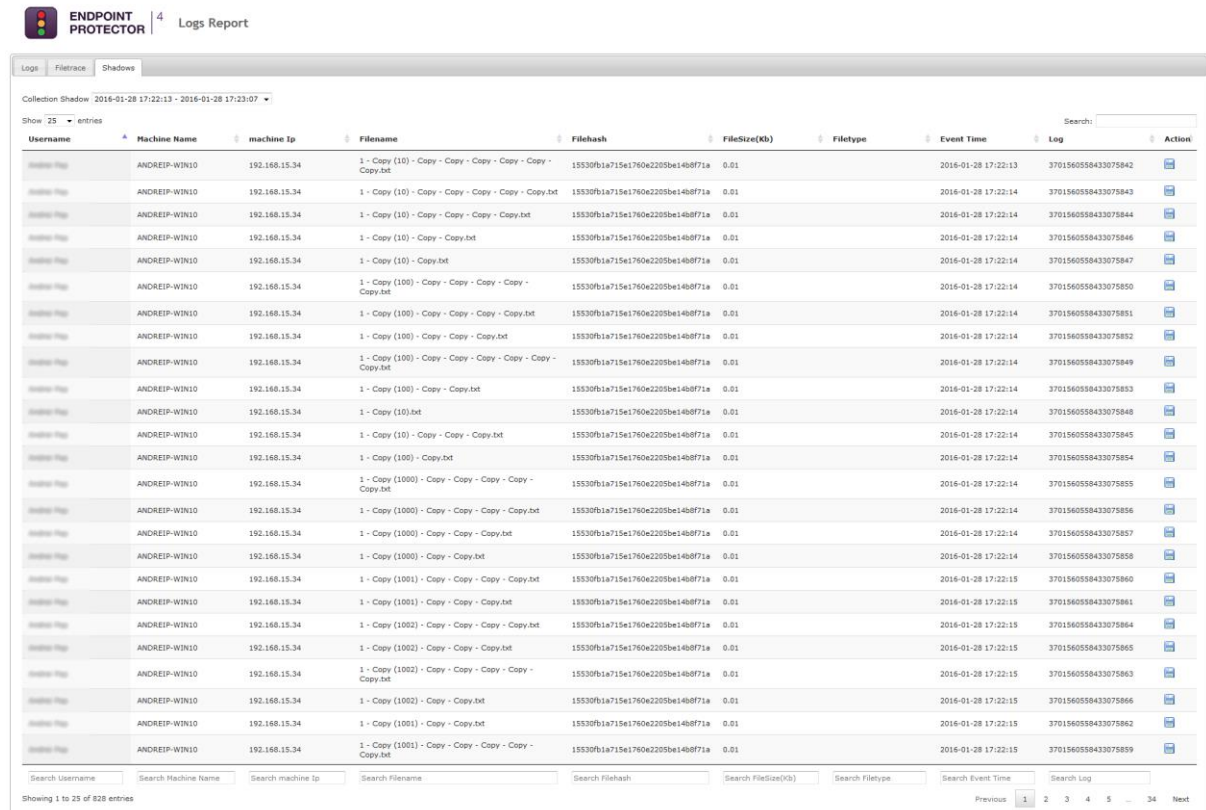
## 12.5. Audit Log Backup

Similar to the Log Backup and Content Aware Log Backup, this section allows old logs to be saved and exported. The options to select the number of logs to be exported, period and file size are available, as well as the option to view a Backup List or set a Backup Scheduler.

Both the Audit Log Backup and Audit Backup Scheduler offer several options like what type of logs to backup, how old should the included logs be, to keep or delete them from the server, to include file shadows or not, etc.

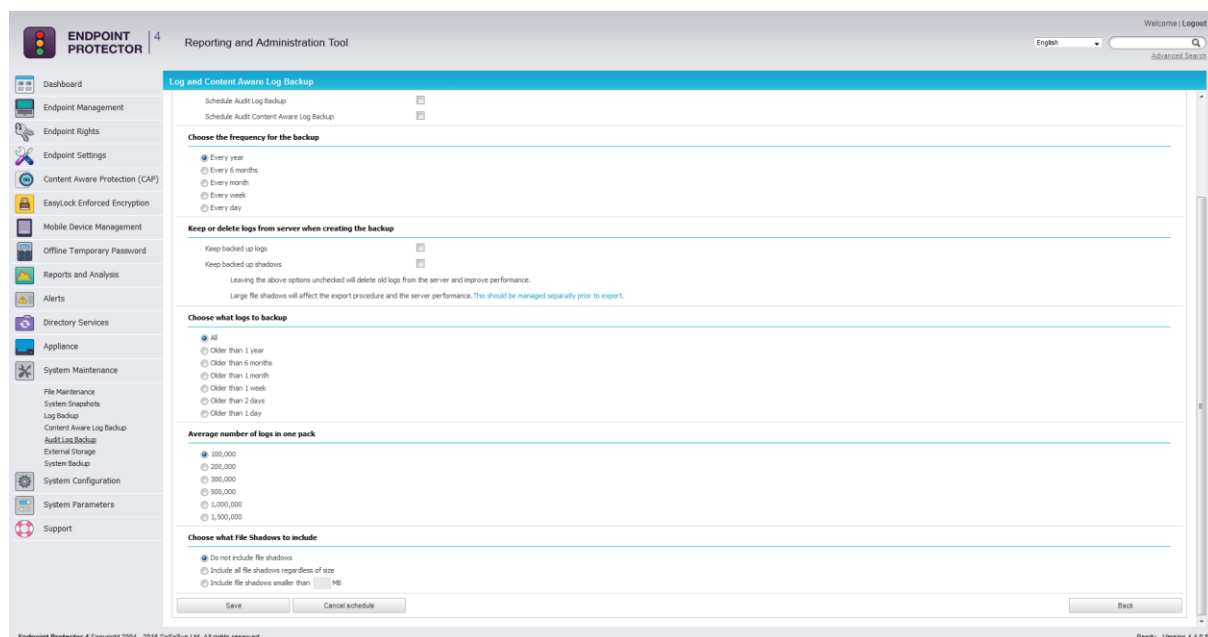


However, the main difference comes from the fact that the exported logs come in an improved visual mode, making things easier to audit or to create reports for executives.



### 12.5.1. Audit Log Backup Scheduler

While the Audit Log Backup starts the backup instantly, the Audit Log Backup Scheduler provides the option to set the procedure for a specific time and the frequency of the backup (every day, every week, every month, every year, etc.).



## 12.6. External Storage

The External Storage option allows the administrator to save the Log Backup files and Shadowed files generated by Endpoint Protector to a particular storage disk from his network. The two mediums supported are FTP and Samba / Network shares.

### 12.6.1. FTP Server

The configuration parameters which enable the backup of these files on an existent FTP share are shown below:

Endpoint Protector Server - External Storage Settings

**External Storage Settings**

External Storage Type: FTP Server

Enable FTP Storage:

Keep copy on EPP Server:

Server Address: 192.168.0.3 ?

Remote Directory: /DLP/logbackup/ ?

Server Port: 21 ?

Passive Connection:

Anonymous Login:

Username: Anonymous

Password:  

Actions: Test Connection Before testing the connection, it is required to save the current settings to the database.

Test Result:

**\*Note:** This feature allows the saving of Shadow Files and Log Backup Files to a network share or FTP server.

Save

**Enable FTP Storage:** This button must be checked for the external storage process to run

**Keep Copy on the EPP Server:** This option enables the administrator to choose whether the logs should be mirrored on both the external storage and on the application.

Server Address: A regular IP ie. 192.168.0.10

Remote Directory: The directory path on the FTP share where the logs will be stored. Trailing directory separators are needed i.e /DLP/logbackup/

Server Port: By default, the FTP application port is 21.

### Note!

The parameter values must be saved before the "Test Connection" option is checked.

Inside the path provided for the storage of backups, Endpoint Protector will create a number of files as seen below.

logbackup	3/2/2015 7:27 PM	File folder	
shadows	3/2/2015 7:27 PM	File folder	
sysbackup	3/2/2015 7:27 PM	File folder	
eppftptest.txt	3/2/2015 7:27 PM	Text Document	1 KB

- Logbackup – inside it all the backups will be stored, both for Device Control and Content Aware Protection
- Shadows – it is the folder in which the shadowed files will be stored, both for Device Control and Content Aware Protection
- Sysbackup – inside it all the created system backups can be stored
- eppftptest.txt – it is created to test the connection between the FTP share and the appliance.

## 12.6.2. Samba / Network Share

The configuration parameters which enable the backup of these files on an existent Samba / Network Share are shown below:

Endpoint Protector Server - External Storage Settings

**External Storage Settings**

External Storage Type: Samba / Network Share

Enable Network Share Storage:

Keep copy on EPP Server:

Network Share Path: //192.168.0.52/epp ⓘ

Remote Directory: /epp/tmp/test/ ⓘ

Username: root

Password: ●●●●●●●●

Actions: Test Connection Before testing the connection, it is required to save the current settings to the database.

Test Result: Connection Successful!

**\*Note:** This feature allows the saving of Shadow Files and Log Backup Files to a network share or FTP server.

Save

Enable Network Share Storage: This button must be checked for the external storage option to run

**Keep Copy on the EPP Server:** This option enables the administrator to choose whether the files should be mirrored on both the external storage and on the application.

**Network Share Path:** A path to the shared directory i.e //192.168.0.10/epp

**Remote Directory:** The directory path on the Network Share where the files will be stored. Trailing directory separators are needed i.e /epp/tmp/logs

### Note!

The parameter values must be saved before the "Test Connection" option is checked.

In the same way as presented for FTP storage, inside the path provided for the storage of backups, Endpoint Protector will create those folders meant for different storage of logs, shadows or system backups and the file eppnstest.txt.System Backup

## 12.6.3. From the Web Interface


This module allows the administrator to make complete system backups.

The screenshot shows the Endpoint Protector web interface. The top navigation bar includes the logo, version number (4), and the title 'Reporting and Administration Tool'. A sidebar on the left contains various menu items such as 'Dashboard', 'Endpoint Management', 'Endpoint Rights', 'Endpoint Settings', 'Content Aware Protection (CAP)', 'Mobile Device Management', 'Offline Temporary Password', 'Reports and Analysis', 'Alerts', 'Directory Services', 'Appliance', 'System Maintenance', 'System Configuration', 'System Parameters', and 'Support'. The main content area is titled 'List of Available Backups' and features a 'Filter' dropdown and a 'Results' table. The table has the following data:

Name	Version	Content	Description	Created at	Actions
Backup for crash recovery	4.4.0.5	Database Content	Just a test.	17-Oct-2014 11:24:02	[Restore] [Download] [Delete]
Test Backup 171014	4.4.0.5	Database Content, Application Sources	For safety reasons.	17-Oct-2014 11:18:02	[Restore] [Download] [Delete]
141014 b4 update bckp	4.4.0.4	Database Content, Application Sources	www	14-Oct-2014 11:44:01	[Restore] [Download] [Delete]
auto_backup_10Oct2014	4.4.0.4	Database Content, Application Sources	Scheduled System Backup on 10-Oct-2014	10-Oct-2014 13:39:18	[Restore] [Download] [Delete]

Below the table, there are 4 results and a 'per page' dropdown set to 20. At the bottom of the main content area, there are buttons for 'Make Backup', 'Status', 'Upload', 'Backup Scheduler', and 'Back'. The footer of the page contains the text 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.5'.

From the menu at **System Maintenance -> System Backup** one can view in a list the current existing backups. The administrative actions available are: **Restore, Download** and **Delete**.

To restore the system to an earlier state, simply click the **Restore** button  next to the desired backup. Confirm the action by clicking the button again in the next window.

The Download button will prompt the administrator to save the **.eppb** backup file on the local drive. It is recommended to keep a good record of where these files are saved.

### Note!

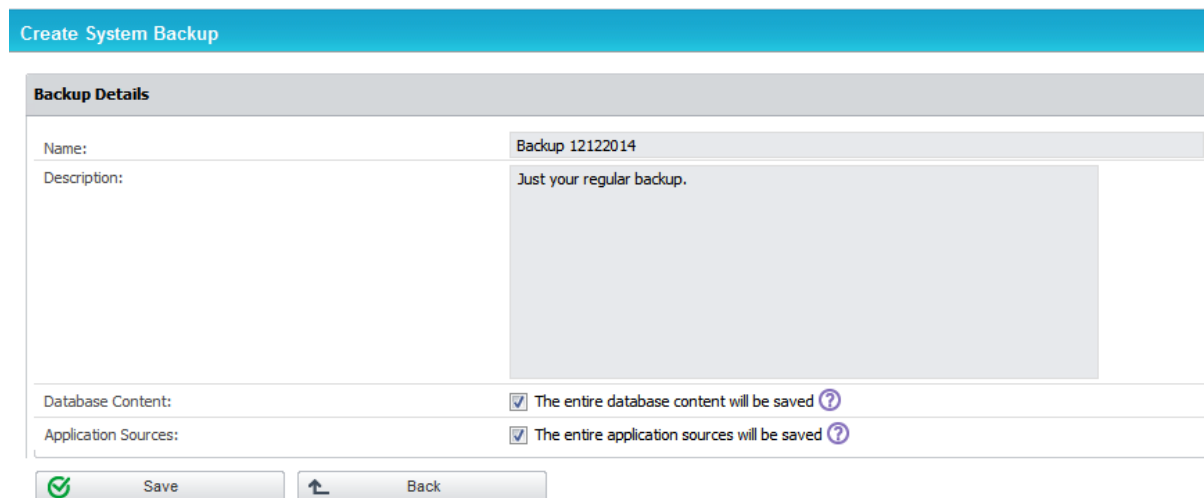
We recommend asking for Support assistance at [support@endpointprotector.com](mailto:support@endpointprotector.com) when using the Restore Backup feature.

### Note!

Once deleted, a backup cannot be recovered.

The sub-menus available from **System Maintenance -> System Backup** are: **Make Backup, Status, Upload** and **Backup Scheduler**.

The first options, **Make Backup**, opens the following menu:



**Create System Backup**

**Backup Details**

Name: Backup 12122014

Description: Just your regular backup.

Database Content:  The entire database content will be saved ?

Application Sources:  The entire application sources will be saved ?

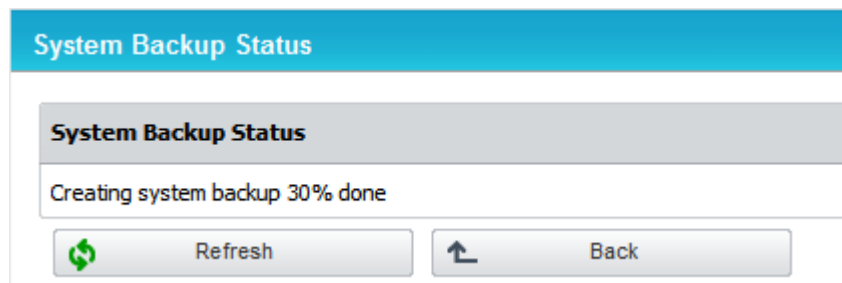
The administrator is presented here with two options:

- To save the **Database content**. This option will make the backup file contain all the devices, rights, logs, settings and policies present on the EPP server at the making of the backup.
- To save the **Application sources**. This option will make the backup contain files such as the EPP clients and others related to the proper functioning of the server.

**Note!**

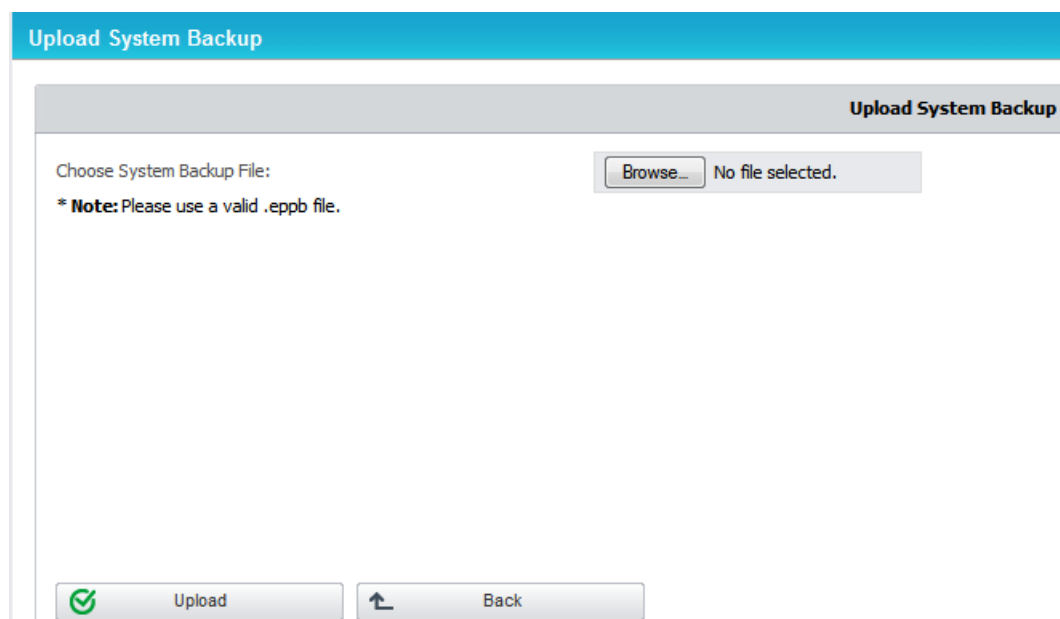
The System Backup will not contain nor preserve the IP Address, File Shadowing copies or the Temporary Logs Files.

The second menu, **Status**, returns the state of the system. If a backup creation is in progress, it will be reported as seen below.



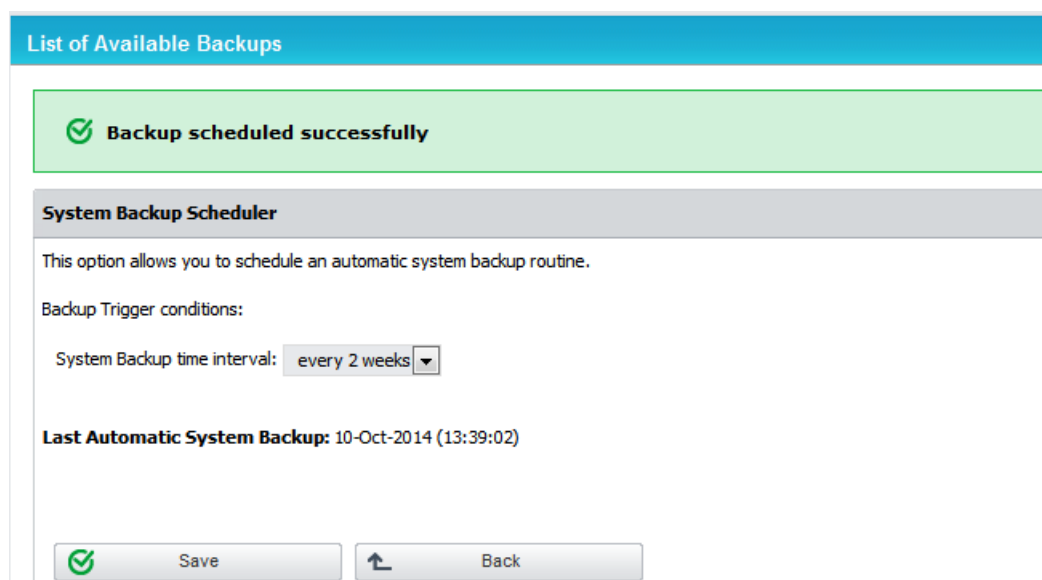
If the system is idle, the button will return the last known status, which by default is set at 100% done.

The next menu, **Upload**, allows the administrator to populate the backup list with **.eppb** files from the local filesystem. This functionality is useful in cases of server migration or crash recovery. The view is as seen below:

**Note!**

Endpoint Protector Backup Files (.eppb) that are larger than 200 MB can only be uploaded from the console of the appliance. We recommend that you contact Support when a created .eppb file exceeds this 200 MB limit.

The final menu is the **Backup Scheduler**.



The screenshot shows a web interface with a blue header bar containing the text "List of Available Backups". Below the header is a green notification box with a checkmark icon and the text "Backup scheduled successfully". Underneath is a grey header bar for the "System Backup Scheduler" section. The main content area contains the text "This option allows you to schedule an automatic system backup routine." followed by "Backup Trigger conditions:". A dropdown menu is set to "every 2 weeks". Below this, it displays "Last Automatic System Backup: 10-Oct-2014 (13:39:02)". At the bottom, there are two buttons: "Save" with a checkmark icon and "Back" with an upward-pointing arrow icon.

From this view the administrator can schedule an automatic backup routine by setting a trigger condition, the **System Backup time interval**. The routine can be set to run daily, weekly, monthly and so forth.

The Scheduler will also prompt the administrator with the **Last Automatic System Backup reminder**.

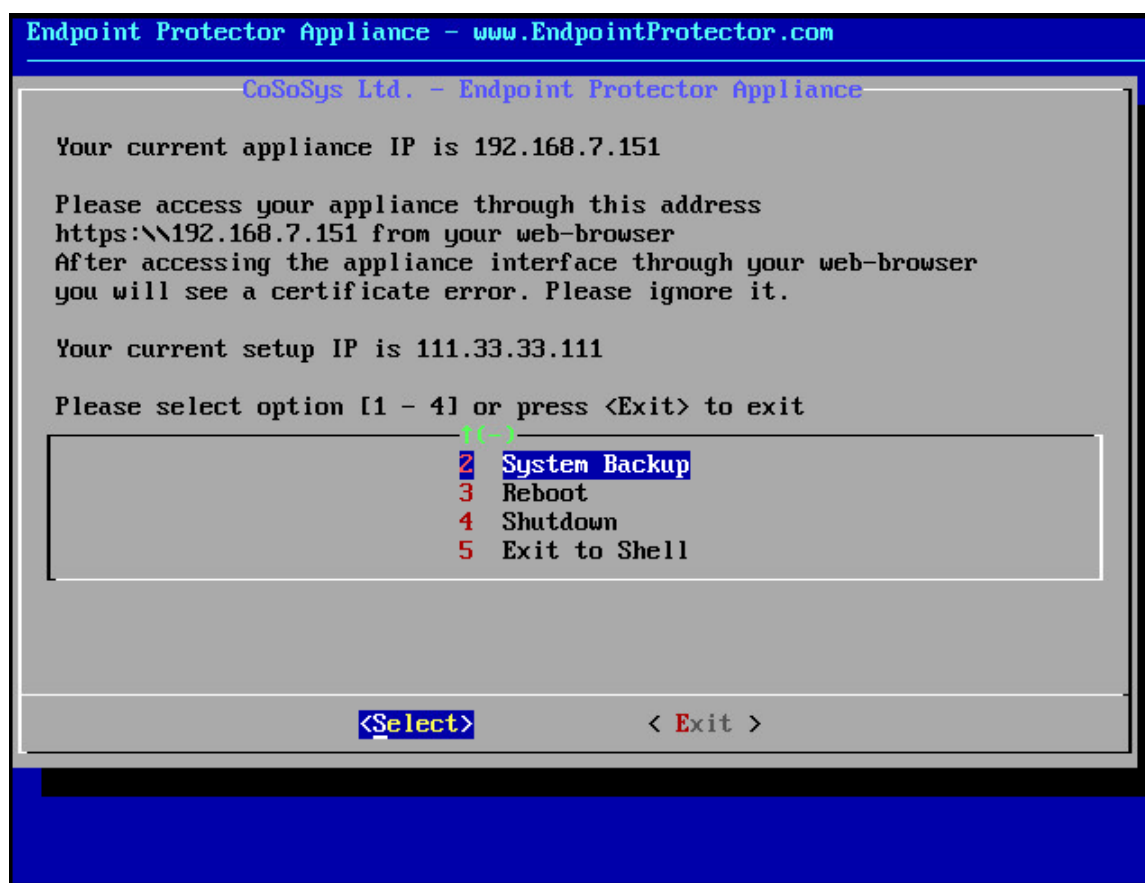
### Note!

A scheduled routine is recommended in order to prevent unwanted loss.

#### 12.6.4. From the Console

Endpoint Protector offers the option to revert the system to a previous state from the administrative console on which the initial configuration occurs.



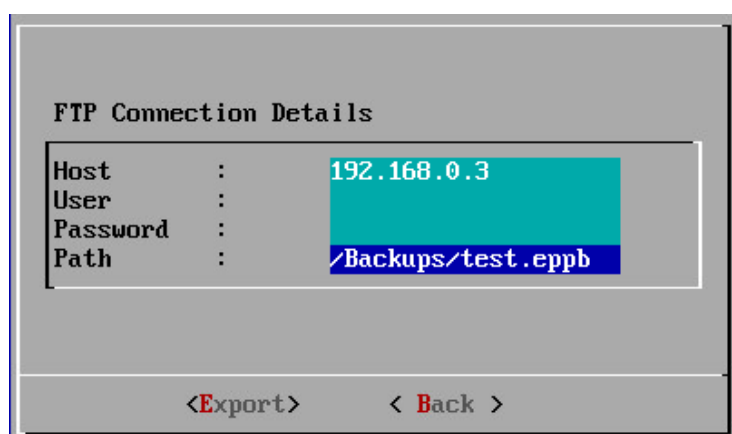


The #2 menu presents the administrator with the following options:

1. **System Restore** – can be performed if a system backup has been performed prior to the event, using the web interface
2. **Import** – can be performed if a **.eppb** file has been downloaded and saved on a FTP server
3. **Export** – can be performed in order to save existing backups on an existant FTP server

To either import or export the **.eppb** files, an administrator will need to provide the system a valid FTP IP address and the path inside its filesystem to the **.eppb** file.

An example is shown below:

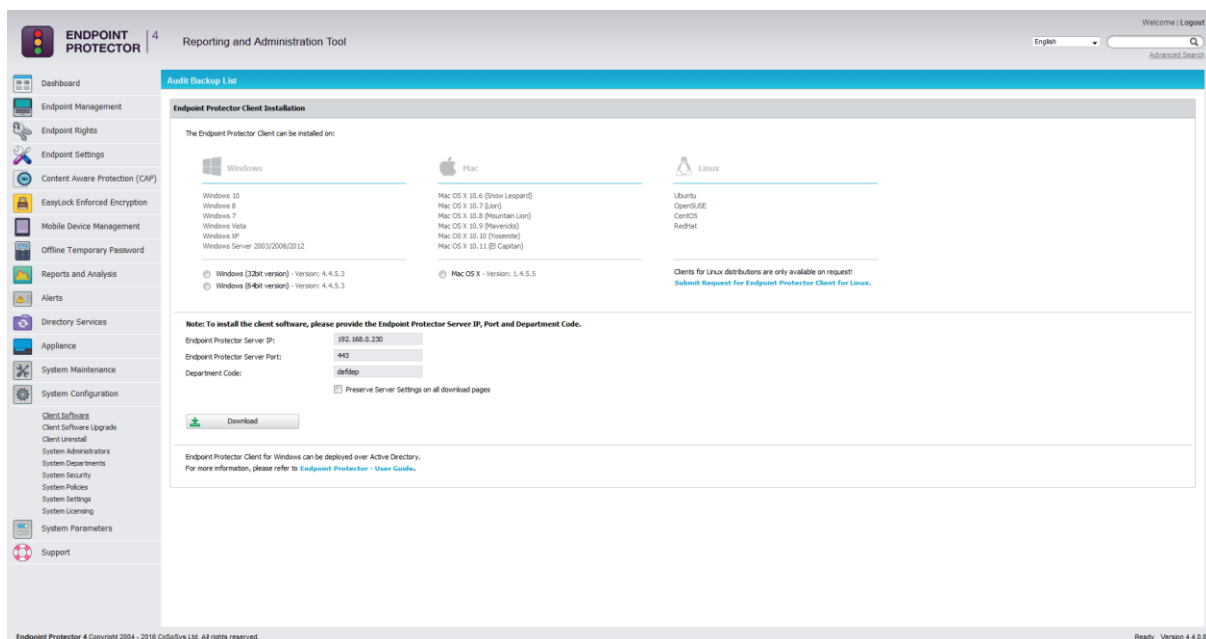


# 13. System Configuration

This module also contains advanced settings, which influence the functionality and stability of the system.

## 13.1. Client Software

In this section, the administrator can download and install the Endpoint Protector Client corresponding to the used operating system. Please note that our Server and Client are communicating through port 443.



The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector. The main content area is titled 'Audit Backup List' and 'Endpoint Protector Client Installation'. It provides instructions on where the client can be installed: Windows, Mac, and Linux. Under Windows, it lists versions 10, 8, 7, Vista, XP, and Server 2003/2008/2012, with radio buttons for 32-bit and 64-bit versions (both version 4.4.5.3). Under Mac, it lists OS X 10.6 (Snow Leopard), 10.7 (Lion), 10.8 (Mountain Lion), 10.9 (Mavericks), 10.10 (Yosemite), and 10.11 (El Capitan), with a radio button for version 1.4.5.5. Under Linux, it lists Ubuntu, CentOS, CentOS, and Redhat, with a note that clients for Linux distributions are only available on request. Below the installation options, there is a 'Note: To install the client software, please provide the Endpoint Protector Server IP, Port and Department Code.' with input fields for IP (192.168.0.230), Port (443), and Department Code (defsp). There is also a checkbox for 'Preserve Server Settings on all download pages' and a 'Download' button. At the bottom, it states 'Endpoint Protector Client for Windows can be deployed over Active Directory. For more information, please refer to Endpoint Protector - User Guide.'

### Note!

The Windows 32-bit and 64-bit client installers both offer the option to download the package with or without a Microsoft Outlook add-on. This option fixes any incompatibility that may arise between Microsoft Outlook and Endpoint Protector.

## 13.2. Client Software Upgrade

This section allows selecting and performing an automatic update of the installed Endpoint Protector Client version. Starting with Windows Client Version 4.2.3.0 a restart PC is mandatory in case of Client Software Upgrade is performed from Web UI.

The screenshot shows the 'Software Update' section of the Endpoint Protector Web UI. The page title is 'Reporting and Administration Tool'. The sidebar on the left contains various navigation options. The main content area is titled 'Step 1: Select the update you want to apply' and displays a table of available updates for the Endpoint Protector Client. The table has the following columns: OS Type, Default, Version, Release Notes, Applicable on versions, and Actions. The 'Actions' column contains a star icon (✳) for each update. A 'Next' button is located at the bottom of the table.

OS Type	Default	Version	Release Notes	Applicable on versions	Actions
<input type="radio"/> Windows	Yes	4.2.9.2		4.0.1.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	Yes	1.4.0.6		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.4 (Tiger)	Yes	1.0.9.0		none	✳
<input type="radio"/> Ubuntu 14.4 LTS	Yes	1.0.5-1		none	✳
<input type="radio"/> Ubuntu 12.4 LTS	Yes	1.0.3-1		none	✳
<input type="radio"/> Ubuntu 10.4 LTS	Yes	1.0.0-1		none	✳
<input type="radio"/> OpenSUSE 11.4	Yes	1.0.0-1		none	✳
<input checked="" type="radio"/> Windows	No	4.2.8.1		4.0.1.5	✳
<input type="radio"/> Windows	No	4.2.6.6		4.0.1.5	✳
<input type="radio"/> Windows	No	4.2.5.7		4.0.1.5	✳
<input type="radio"/> Windows	No	4.2.3.0		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.7.0		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.4.4		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.3.7		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.2.3		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.1.4		4.0.1.5	✳
<input type="radio"/> Windows	No	4.1.0.7		4.0.1.5	✳
<input type="radio"/> Windows	No	4.0.6.0		4.0.1.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.3.0.4		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.2.3.1		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.2.2.6		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.2.1.6		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.1.1.0		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.1.0.4		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.1.0.0		1.0.9.5	✳
<input type="radio"/> Mac OS X 10.5+ (Snow Leopard)	No	1.0.9.1		none	✳

The ✳ button under the Actions column allows setting the default Endpoint Protector Client version that will be available for download under the Client Software section.

### Note!

Downgrading from a currently installed Endpoint Protector Client version to an older one cannot be performed automatically.

## 13.3. Client Uninstall

The EPP Clients installed on the computers can be remotely uninstalled from this tab. The computers will receive the uninstall command at the same time they receive the next set of commands from the server. If the computer is offline it will receive the uninstall command the first time it will come online. When the uninstall button is pressed the computer(s) will be greyed out until the action will be performed. The uninstall command can be cancelled if it was not already executed.

The screenshot shows the 'Client Uninstall - List of Computers' page in the Endpoint Protector Reporting and Administration Tool. The page features a sidebar with navigation options, a top navigation bar, and a main content area displaying a table of installed clients. The table has the following columns: Computer Name, IP, Department, Workgroup, Domain, Default User, Location, Last Time Online, Version, License, Modified at, and Modified by. The table shows 7 results, with the last two rows highlighted in blue. The interface includes a sidebar with navigation options, a top navigation bar, and a footer with copyright information.

Computer Name	IP	Department	Workgroup	Domain	Default User	Location	Last Time Online	Version	License	Modified at	Modified by
	192.168.0.21	Default Department	WORKGROUP				26-Feb-2014 11:49	4.2.7.6 - (PC)	Offline	14-Mar-2014 15:32:02	root
	192.168.0.60	Default Department	WORKGROUP				17-Jan-2014 09:45	4.2.6.6 - (PC)	Offline	14-Mar-2014 15:32:02	root
	192.168.0.215	Default Department	WORKGROUP				10-Dec-2013 13:00	4.2.7.3 - (PC)	Offline	14-Mar-2014 15:32:02	root
	192.168.0.20	Default Department	WORKGROUP				25-Nov-2013 09:42	4.2.6.7 - (PC)	Offline	14-Mar-2014 15:32:02	root
	192.168.0.106	Default Department	WORKGROUP				19-Nov-2013 12:59	4.2.6.6 - (PC)	Offline	14-Mar-2014 15:32:02	root
	192.168.0.96	Default Department	WORKGROUP				17-Mar-2014 08:59	4.2.7.9 - (PC)	Licensed	14-Mar-2014 16:57:01	root
	192.168.0.69	Default Department	WORKGROUP				14-Mar-2014 17:01	4.2.7.9 - (PC)	Unlicensed	14-Mar-2014 17:01:02	root

7 results [ 20 per page]

Client Uninstall Back

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

### Note!

The uninstall command works for Windows client version 4.2.8.1 or newer.

## 13.4. System Administrators

This section allows the creation of new administrators. Once administrators are created, a lists containing all the administrators will be displayed. Options to editing details and settings or delete unwanted administrators are also available. One of the most important distinction is that the administrators can be: regular administrators, which have some limitations and super administrators which have full access to the system, including advanced features.

The screenshot displays the 'List of Administrators' page in the Endpoint Protector 4 Reporting and Administration Tool. The interface includes a sidebar with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, and System Configuration. The main content area shows a table of administrators with columns for User Name, Created at, Last Login, Super Admin, and Actions. Two administrators are listed: 'root' and 'viadul - root'. The 'root' user is a Super Admin, while 'viadul - root' is not. A 'Create' button is visible below the table.

User Name	Created at	Last Login	Super Admin	Actions
root		11-Sep-2014 09:16	✓	
viadul - root	4 September 2014 13:03		✓	

2 results [ 50 per page]

Create

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready! Version 4.4.0.4

While creating an Administrator, there are several Administrator Details and Administrator Settings can be configured. Among them, whether e-mail alerts are received, managed departments, IP login restrictions and Default UI Language can be mentioned. All of these settings can be changed at a later time.

The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector. The top navigation bar includes the logo, version '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with 'Advanced Search' and a 'Logout' link. A left sidebar contains a menu with categories like 'Dashboard', 'Endpoint Management', 'Endpoint Rights', 'Endpoint Settings', 'Content Aware Protection (CAP)', 'EasyLock Enforced Encryption', 'Mobile Device Management', 'Offline Temporary Password', 'Reports and Analysis', 'Alerts', 'Directory Services', 'Appliance', 'System Maintenance', 'System Configuration', 'Client Software', 'Client Software Upgrade', 'Client Uninstall', 'System Administrators', 'System Departments', 'System Policies', 'System Settings', 'System Licensing', 'System Parameters', and 'Support'. The main content area is titled 'Administrator: User' and features a 'Show all departments' link. It is divided into two sections: 'Administrator Details' and 'Administrator Settings'. The 'Administrator Details' section includes fields for 'User Name' (root), 'Password', 'Password Confirmation', 'First Name', 'Last Name', 'E-mail', and 'Phone'. The 'Administrator Settings' section includes checkboxes for 'Super Administrator', 'Receive E-mail Alerts', 'Account is active', and 'Enforce login IP restrictions'. A 'Managed Departments' list shows 'Default Department' (checked), 'test dep', 'nume foarte lung de departament', and 'sf\_guvern\_ghid@mead'. Other settings include 'Default UI Language' (English), 'Last Login' (22-Mar-2016 11:19), and 'Current password set on:'. At the bottom of the settings section are buttons for 'Save', 'Save Add', 'Back', and 'Delete'. The footer contains 'Endpoint Protector 4 Copyright 2004 - 2016 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.8'.

## 13.5. System Departments

This module allows creating System Departments. The available options are **Edit** and **Delete**.



The main reason for using this feature is to target Large Installation where one Super Administrator cannot handle the Endpoint Protector Server configuration and maintenance. Even further, one Regular administrator should only be responsible for his entities.

The screenshot shows the 'Reporting and Administration Tool' interface. The main content area is titled 'List of Departments' and contains a table with the following data:

Department Name	Description	Department Code	Actions
Default Department	New entities will belong to this depart...	defdep	
Secret Department	Secret	secdep	
Public Department	public	pubdep	

Below the table, there is a 'Create' button and a 'Show all departments' link in the top right corner of the table area.

A new department can be defined by using the "Create" button.

The screenshot shows the 'Add a New Department' form. The fields are filled with the following information:

- Department Name:** Testing
- Description:** This is the Testing Department.
- Unique Code:** 335efr

At the bottom of the form, there are three buttons: 'Save', 'Save Add', and 'Back'.

Even if the term Department is simple, if we want to make a similarity between Endpoint Protector and Active Directory (or any other Director Service software) the equivalent of this term is Organization Unit. Of course Organization Unit is not identical with Department, and again Endpoint Protector leaves the power to the actual Super Administrator to virtually link one or more Organization Units to an Endpoint Protector Department. For more details, please see paragraph "10.1. AD Deployment".

Several aspects regarding departments are detailed below:

1. Each main entity must belong to a department, except with the scenario when the super administrator deletes the Default Department. At computer registration, the Department Code is provided. If a department having the given code is found, then the computer will register and it will belong to that department. All the main entities information received from a computer in department X will also belong to department X.

Example: Computer Test-PC is registered to department "developers". In this case, user Test logged on that computer will be assigned to the same department together with the devices connected on the computer Test-PC.

**Note!**

In case that, at registration, no department code is provided or a wrong department code is provided, the department code is considered invalid and that computer will be assigned to the default department (defdep).

2. Super Administrators (example root) will still have access to all the main entities regardless of their departments and will be able to change departments. When logged on as Super Administrator, the text "Show all departments" will be displayed on the right top part of the main content layout of the Web interface.

3. As only the Super Administrator has the possibility to create regular users, he is also responsible for assigning regular administrators to handle one or more departments. Regular Administrator will see and manage in the Web interface only the main entities belonging to the assigned departments.

4. From a security stand point of view:

A Regular Administrator should only see his department's entities and nothing more.



A Regular Administrator should only control his department's entities and nothing more.

## IMPORTANT!

If you do not want to have any departments based organization within the Endpoint Protector deployment, please make sure that you always assign the default Department to all new created Regular Administrators within the Endpoint Protector Web Interface.

## 13.6. System Security / Client Uninstall Protection

The Client Uninstall Protection feature protects the Endpoint Protector Client from being uninstalled by using a password-based mechanism. The Administrator of the system defines this password from within the Reporting and Administration Tool of Endpoint Protector 4. When somebody tries to uninstall the Endpoint Protector Client, they will be prompted for the password. If they do not know the password, the Client removal cannot continue.

This password can be set by accessing "System Configuration" – "System Security", entering a password in the "Password" field and clicking on "Save".

The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector 4. The main content area is titled 'System Security' and includes the following sections:

- System Security** (Header)
- Alerts:**
  - You do not have an uninstall password defined.
  - You do not have a security password for sensitive data defined.
- Security Password for Uninstall Protection:**
  - Field: Password: [masked]
  - Button: Save
- Data Security Privileges:**
  - Field: Restrict Sensitive Data Access only to super administrators:
  - Button: Save
- Additional Security Password for Sensitive Data Protection:**
  - Field: Current Password: [masked]
  - Field: New Password: [masked]
  - Field: New Password (confirm): [masked]
  - Button: Save

The left sidebar contains a navigation menu with items such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, Client Software, Client Software Upgrade, Client Uninstall, Download EasyLock Software, System Administrators, System Departments, System Security, System Policies, System Settings, System Licensing, System Parameters, and Support.

At the bottom of the page, the footer text reads: 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.4'.

The second option, “**Data Security Privileges**”, allows you to restrict Sensitive Data sections access only to Super Administrators. If this option is selected, then only super administrators are able to view the “Reports and Analysis” section. If this option is not selected, then super administrators and also administrators are able to view the “Reports and Analysis” section.

## 13.7. System Security

This module enables the administrator to set a number of security policies such as: set a client uninstall password, restrict the access to sensitive information to super administrators and set a password protection on that sensitive data.

The screenshot displays the 'System Security' configuration page in the Endpoint Protector 4 interface. The page is titled 'Reporting and Administration Tool' and includes a search bar and a language dropdown set to 'English'. The left sidebar contains a navigation menu with categories like 'Dashboard', 'Endpoint Management', 'Endpoint Rights', 'Endpoint Settings', 'Content Aware Protection (CAP)', 'Mobile Device Management', 'Offline Temporary Password', 'Reports and Analysis', 'Alerts', 'Directory Services', 'Appliance', 'System Maintenance', 'System Configuration', 'Client Software', 'System Parameters', and 'Support'. The main content area is divided into three sections:

- System Security**: Contains two warning messages: 'You do not have an uninstall password defined.' and 'You do not have a security password for sensitive data defined.'
- Security Password for Uninstall Protection**: A form with a 'Password:' field (masked with dots) and a 'Save' button.
- Data Security Privileges**: A form with a checkbox for 'Restrict Sensitive Data Access only to super administrators:' and a 'Save' button.
- Additional Security Password for Sensitive Data Protection**: A form with three password fields: 'Current Password:', 'New Password:', and 'New Password (confirm):' (all masked with dots), and a 'Save' button.

At the bottom of the page, the footer text reads: 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.4'.

## 13.8. System Settings

### 13.8.1. Rights Functionality

In the System Settings module, you can modify Endpoint Protector 4 Server Rights functionalities by giving priority to either User Rights or Computer Rights.

Scroll down to the **Setting up policies** chapter of this document for more information on the subject.

### 13.8.2. Proxy Settings

Endpoint Protector offers configuration options for a proxy, as seen below:

Proxy Server Settings	
IP:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
*Note: This information refers to networks with configured Proxy server to allow access to Endpoint Protector Live Update.	

The necessary configuration details are:

- IP – the Proxy Server IP
- Username/Password – Proxy access credentials (not mandatory)

#### Note!

If these details are not filled in, Endpoint Protector will connect directly to [liveupdate.endpointprotector.com](http://liveupdate.endpointprotector.com). Data sent to this server is not security sensitive, being limited only to your version/language.

## 13.9. System Licensing

This module allows the administrator to manage the licensing of Endpoint Protector and offers a complete overview of the current licenses status.

The screenshot shows the 'Endpoint Protector Licensing System' interface. It features a sidebar on the left with navigation options such as Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, Client Software, Client Software Upgrade, Client Uninstall, Download EasyLock Software, System Administrators, System Departments, System Security, System Policies, System Settings, System Licensing, System Parameters, and Support. The main content area is titled 'Endpoint Protector Licensing System' and includes a 'Show all departments' link. It is divided into three sections: 'System Status (Updates and Support)', 'Feature Status', and 'General License Information'.

**System Status (Updates and Support)**

Number of total licenses present in the system: 55

System	Status	End Date
Updates	Yes	
Device Control		02 Oct 2014 10:54:01
Content Aware Protection (CAP)		02 Oct 2014 10:54:01
Mobile Device Management		02 Oct 2014 10:54:01

**Feature Status**

Feature	Status	End Date	Total	Used	Online
Device Control	Trial Mode	02 Oct 2014 10:54:01	50	7	2
Device Control and Content Aware Protection (CAP) for Windows	Trial Mode	02 Oct 2014 10:54:01	50	7	2
Device Control and Content Aware Protection (CAP) for Windows and Mac OS X	Trial Mode	02 Oct 2014 10:54:01	50	7	2
Mobile Device Management	Trial Mode	02 Oct 2014 10:54:01	5	2	2

**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

Buttons: Buy Licenses, Import Licenses, Paste Licenses, List Licenses

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.4

The Endpoint Protector licensing system comprises three types of licenses: Endpoint licenses for Mobile and Fixed endpoints, Feature licenses and Updates & Support licenses.

**Endpoint licenses** are used for registering the Endpoint Protector Client, enabling the communication with the Endpoint Protector Server. They are available as either 30 days Trial licenses or perpetual (permanent) licenses. Once registered with a valid Endpoint license, the Endpoint Protector Client remains active for an unlimited period of time regardless of the status of the other license types.

**Feature licenses** are used for activating one of the three Endpoint Protector modules: Device Control, Content Aware Protection, respectively Mobile Device Management. Each of these modules can be used in Trial Mode for a period of up to 30 days. Then, a perpetual (permanent) license is required to be purchased

and imported for the feature to remain active. Although the Device Control module appears by default as active in the Web Administration Interface, a license is required to enable the communication between Server and Client. The Content Aware Protection and Mobile Device Management features are displayed as blocked by default and require an additional Activation request to be performed by the administrator. The Features Status section offers an overview of the current features licensing status.

**Updates & Support licenses** are optional licenses that once purchased and imported into the system allow access to the latest Updates available for both Client and Server side and enable premium Support and Technical Assistance. The Updates and Support licenses can be purchased for a period varying from 1 month up to 36 months, with a separate option for 120 months. As opposed to Endpoint and Feature licenses, Updates & Support licenses are not permanent and they require periodic renewal for being able to get access to our Live Update Server.

### Note!

When first activating one or more features, an Updates & Support license for a period of minimum 1 year is required. After the Updates & Support license expires, the feature remains active and purchasing additional Updates & Support licenses becomes optional.

For example, if you wish to license Endpoint Protector for 100 workstations and use the Content Aware Protection module for 1 year, you will require:

- 100 Endpoint licenses
- 1 Content Aware Protection license, which includes an Updates & Support license for Device Control and Content Aware Protection valid for 1 year. After the validity period expires, the feature remains active, while any updates and support services are not available anymore.

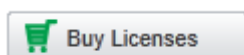
If you wish to manage also a fleet of 10 devices for 6 months, you will additionally require:

- 10 Mobile Endpoint licenses
- 1 Mobile Device Management license, which includes an Updates & Support license for Mobile Device Management for 6 months

### Note!

As opposed to Device Control and Content Aware Protection, a valid Updates & Support license for Mobile Device Management is required for the feature to remain active as the Mobile Device Management service requires a working connection to our Cloud.

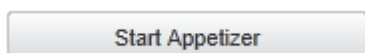
All license types can be purchased directly by using the “Buy Licenses” option.



A separate free licensing option, called **Appetizer Mode**, is available for small networks of up to 5 computers and / or 5 iOS and Android devices. Appetizer licenses enable access to each of the three Endpoint Protector modules for a period of 1 year.

### 13.9.1. Appetizer Mode

The Appetizer Mode can be activated by pushing the “Start Appetizer” button, which will automatically assign 1 year Device Control and Content Aware Protection licenses for up to 5 computers. Additionally, it will enable a 1 year subscription for Mobile Device Management by Endpoint Protector for up to 5 iOS and Android smartphones and tablets.



The Appetizer license is a limited license valid for 1 year with automatic renewal, which includes also 1 year of updates with automatic renewal. The following limitations apply:

- **No Support Included!**
- **Device Control:** no limitations
- **Content Aware Protection:** The options for E-mail, Web Browsers and Cloud Services/File Sharing, Clipboard Monitor and Print Screen Monitor are disabled. Mac OS X compatibility is also disabled.
- **Mobile Device Management:** mobile device tracking is disabled.

#### **Note!**

License terms may change without prior notice.

Several Requirements are necessary for using Appetizer Licenses:

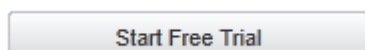
- Licensee has to be small business or registered professional (e.g. a company such as a Ltd. or a registered professional such as a law firm or architectural association).
- Valid company e-mail address
- Online activation of virtual appliance after setup in your network

- Online self-enrollment of MDM services (e.g. for Apple Push Notification Certificate)

### 13.9.2. Trial Mode

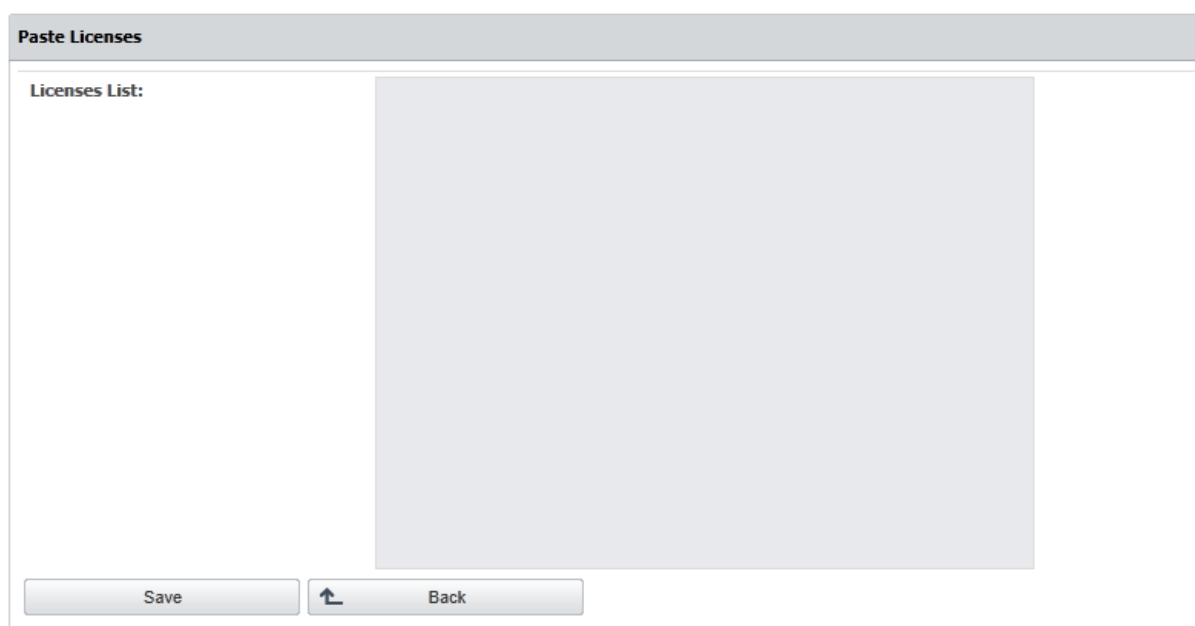
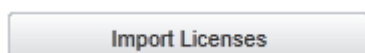
The trial period can be activated by pushing the “Start Free Trial” button, which will automatically assign 30 days trial licenses for up to 50 computers.

The trial licenses are assigned on a “first-in-first-served” basis. In case that one or more computers with assigned trial licenses are inactive for a certain interval of time, the administrator can manually release those licenses, which will automatically be reassigned to other online computers.



### 13.9.3. Import Licenses

The Import Licenses option gives you the possibility to browse for an Excel file that contains licenses. After you have selected the file, click Upload.

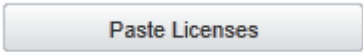


#### **Attention!**

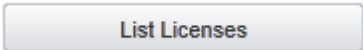
The Excel document has to be formatted in a specific way. Only the first column in the excel sheet is taken into consideration and the first line in the excel sheet is ignored.

	A	C	D
1	<b>Endpoint Protector Client License Keys for Import</b>	<b>License Type</b>	<b>Software</b>
2	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
3	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
4	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
5	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
6	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
7	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
8	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
9	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
10	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
11	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
12	ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint License
13	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Mobile Device Management
14	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Device Control & Content Aware Protection
15	YYYY-YYYY-YYYY-YYYY	1 Year	Updates & Support for Device Control
16			
17			
18			
19			
20			

Licenses can be imported also by using the “Paste Licenses” option, which allows to manually copy&paste licenses into the system. This option is recommended for online purchases, when licenses are delivered directly in your e-mail.



The List Licenses button displays the list of imported license keys, including the computers to which they were assigned and the validity period.





**ENDPOINT PROTECTOR** | 4

Reporting and Administration Tool

Welcome | Logout

English

[Advanced Search](#)

List of Available Licenses
Show all departments

**Filter**

**List of Licenses**

<input type="checkbox"/> All	Order Number	License Validity	License Key	Valid until	License Type	Assigned Computer	Assigned Mobile Device	Actions
<input type="checkbox"/>	1	<span style="color: green;">●</span>	TRIA-L000-0794-0118	02 Oct 2014 10:54:01	Updates & Support (Trial)			<span style="color: red;">⊗</span>
<input type="checkbox"/>	2	<span style="color: green;">●</span>	TRIA-LMDM-0367-0393	Active	Mobile Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	3	<span style="color: green;">●</span>	TRIA-LMDM-0878-0730	Active	Mobile Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	4	<span style="color: green;">●</span>	TRIA-LMDM-0128-0543	Active	Mobile Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	5	<span style="color: green;">●</span>	TRIA-LMDM-0991-0650	Active	Mobile Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	6	<span style="color: green;">●</span>	TRIA-LMDM-0446-0446	Active	Mobile Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	7	<span style="color: green;">●</span>	TRIA-LCAP-0024-0958	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	8	<span style="color: green;">●</span>	TRIA-LCAP-0565-0321	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	9	<span style="color: green;">●</span>	TRIA-LCAP-0510-0789	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	10	<span style="color: green;">●</span>	TRIA-LCAP-0397-0112	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	11	<span style="color: green;">●</span>	TRIA-LCAP-0783-0973	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	12	<span style="color: green;">●</span>	TRIA-LCAP-0742-0830	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	13	<span style="color: green;">●</span>	TRIA-LCAP-0748-0572	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	14	<span style="color: green;">●</span>	TRIA-LCAP-0251-0995	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	15	<span style="color: green;">●</span>	TRIA-LCAP-0297-0836	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	16	<span style="color: green;">●</span>	TRIA-LCAP-0532-0668	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	17	<span style="color: green;">●</span>	TRIA-LCAP-0453-0689	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	18	<span style="color: green;">●</span>	TRIA-LCAP-0463-0532	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	19	<span style="color: green;">●</span>	TRIA-LCAP-0321-0379	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	20	<span style="color: green;">●</span>	TRIA-LCAP-0418-0040	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	21	<span style="color: green;">●</span>	TRIA-LCAP-0776-0000	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	22	<span style="color: green;">●</span>	TRIA-LCAP-0585-0801	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	23	<span style="color: green;">●</span>	TRIA-LCAP-0959-0150	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	24	<span style="color: green;">●</span>	TRIA-LCAP-0122-0469	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	25	<span style="color: green;">●</span>	TRIA-LCAP-0940-0520	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	26	<span style="color: green;">●</span>	TRIA-LCAP-0582-0703	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	27	<span style="color: green;">●</span>	TRIA-LCAP-0494-0324	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	28	<span style="color: green;">●</span>	TRIA-LCAP-0534-0242	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	29	<span style="color: green;">●</span>	TRIA-LCAP-0897-0786	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	30	<span style="color: green;">●</span>	TRIA-LCAP-0237-0194	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	31	<span style="color: green;">●</span>	TRIA-LCAP-0623-0769	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	32	<span style="color: green;">●</span>	TRIA-LCAP-0863-0076	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	33	<span style="color: green;">●</span>	TRIA-LCAP-0459-0326	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	34	<span style="color: green;">●</span>	TRIA-LCAP-0609-0780	Active	Endpoint License			<span style="color: red;">⊗</span>
<input type="checkbox"/>	35	<span style="color: green;">●</span>	TRIA-LCAP-0706-0027	Active	Endpoint License			<span style="color: red;">⊗</span>

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.
Ready Version 4.0.4

# 14. System Parameters

This module of Endpoint Protector is designed for super administrators. The advanced settings available here determine the functionality of the entire system. Introducing wrong or new values can limit the functionality and performance of the entire system.

## 14.1. Device Types

Here is a list of all device types currently supported through Device Control by Endpoint Protector, along with a short description for all of the items.

The screenshot shows the Endpoint Protector Reporting and Administration Tool interface. The main content area displays the 'Device Types' configuration page, which is divided into two tabs: 'Device Control' (selected) and 'Content Aware Protection (CAP)'. The 'Device Control' tab contains a table listing various device types and their supported operating systems.

Name	Description	Windows	Mac	Linux
Unknown Device	Unknown Device	✓	✓	✓
USB Storage Device	USB Storage Device (USB Flash Drives, U3 Drives, ExpressCard, Biometric USB Storage Devices, etc.)	✓	✓	✓
Internal CD or DVD RW	Internal CD or DVD RW	✓	✓	✓
Internal Card Reader	Internal Card Reader (SD Cards, Memory Cards, Compact Flash, etc.)	✓	✓	✓
Internal Floppy Drive	Internal Floppy Drive	✓	✓	✓
Local Printers	Local Printers connected to Computer	✓	✓	✓
Windows Portable Device (Media Transfer Protocol)	Windows Portable Device (Media Transfer Protocol)	✓	✓	✓
Digital Camera	Digital Camera	✓	✓	✓
BlackBerry	BlackBerry hand held Device	✓	✓	✓
Mobile Phones (Sony Ericsson, etc.)	Mobile Phones (Sony Ericsson, etc.)	✓	✓	✓
SmartPhone (USB Sync)	SmartPhone connected through USB	✓	✓	✓
SmartPhone (Windows CE)	Windows CE Device	✓	✓	✓
SmartPhone (Symbian)	Nokia N Series	✓	✓	✓
Webcam	Web Camera	✓	✓	✓
iPhone	iPhone	✓	✓	✓
iPad	iPad	✓	✓	✓
iPod	iPod	✓	✓	✓
Serial ATA Controller	Serial ATA Controller	✓	✓	✓
WiFi	Wireless Network	✓	✓	✓
Bluetooth	Bluetooth Devices	✓	✓	✓
FireWire Bus	FireWire Bus	✓	✓	✓
Serial Port	Serial Port	✓	✓	✓
PCMCIA Device	PCMCIA Device	✓	✓	✓
Card Reader Device (MTD)	Card Reader Device based on Memory Technology Driver	✓	✓	✓
Card Reader Device (SCSI)	Card Reader Device based on SCSI Adapter	✓	✓	✓
ZIP Drive	ZIP Drive	✓	✓	✓
Teensy Board	USB-based Microcontroller Development System	✓	✓	✓
Thunderbolt	Thunderbolt	✓	✓	✓
Network Share	Network Share	✓	✓	✓
Infrared Dongle	Infrared Dongle	✓	✓	✓
Parallel Port (LPT)	Parallel Port (LPT)	✓	✓	✓
Additional Keyboard	Additional Keyboard	✓	✓	✓
USB Modem	USB Modem	✓	✓	✓

The interface also includes a sidebar with navigation options like Dashboard, Endpoint Management, and System Parameters. The footer contains copyright information for Endpoint Protector 4 and version details.

Here is a list of all device types currently supported through Content Aware Protections' option for Controlled Storage Device Types, along with a short description for all of the items.

The screenshot shows the 'Reporting and Administration Tool' interface. On the left is a navigation menu with options like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, and System Parameters. The main area is titled 'Device Types' and contains a table with columns for Name, Description, Windows, and Mac. The table lists various device types such as Unknown Device, USB Storage Device, Internal CD or DVD RW, Internal Card Reader, Internal Floppy Drive, Local Printers, Windows Portable Device (Media Transfer Protocol), Digital Camera, BlackBerry, Mobile Phones (Sony Ericsson, etc.), SmartPhone (USB Sync), SmartPhone (Windows CE), SmartPhone (Symbian), Webcam, iPhone, iPad, iPod, Serial ATA Controller, WiFi, Bluetooth, FireWire Bus, Serial Port, PCMCIA Device, Card Reader Device (MTD), Card Reader Device (SCSI), ZIP Drive, Teensy Board, Thunderbolt, Network Share, Infrared Dongle, Parallel Port (LPT), Additional Keyboard, and USB Modem. Checkmarks in the Windows and Mac columns indicate supported operating systems.

Name	Description	Windows	Mac
Unknown Device	Unknown Device		
USB Storage Device	USB Storage Device (USB Flash Drives, U3 Drives, ExpressCard, Biometric USB Storage Devices, etc.)	✓	✓
Internal CD or DVD RW	Internal CD or DVD RW		
Internal Card Reader	Internal Card Reader (SD Cards, Memory Cards, Compact Flash, etc.)	✓	✓
Internal Floppy Drive	Internal Floppy Drive		
Local Printers	Local Printers connected to Computer	✓	
Windows Portable Device (Media Transfer Protocol)	Windows Portable Device (Media Transfer Protocol)		
Digital Camera	Digital Camera		
BlackBerry	BlackBerry hand held Device		
Mobile Phones (Sony Ericsson, etc.)	Mobile Phones (Sony Ericsson, etc.)		
SmartPhone (USB Sync)	SmartPhone connected through USB		
SmartPhone (Windows CE)	Windows CE Device		
SmartPhone (Symbian)	Nokia N Series		
Webcam	Web Camera		
iPhone	iPhone		
iPad	iPad		
iPod	iPod		
Serial ATA Controller	Serial ATA Controller	✓	
WiFi	Wireless Network		
Bluetooth	Bluetooth Devices		
FireWire Bus	FireWire Bus	✓	✓
Serial Port	Serial Port		
PCMCIA Device	PCMCIA Device		
Card Reader Device (MTD)	Card Reader Device based on Memory Technology Drive	✓	
Card Reader Device (SCSI)	Card Reader Device based on SCSI Adapter	✓	
ZIP Drive	ZIP Drive	✓	
Teensy Board	USB-based Microcontroller Development System		
Thunderbolt	Thunderbolt	✓	✓
Network Share	Network Share	✓	
Infrared Dongle	Infrared Dongle		
Parallel Port (LPT)	Parallel Port (LPT)		
Additional Keyboard	Additional Keyboard		
USB Modem	USB Modem		

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. No Background Tasks Version 4.4.0.6

## 14.2. Rights

This list contains the access rights which can be assigned on the system for devices at any time.

The screenshot shows the 'Reporting and Administration Tool' interface. The left sidebar contains a navigation menu with items like Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, Device Types, Rights, Events, File Types, and Support. The main content area is titled 'List of Possible Rights' and includes a 'Show all departments' link. Below this is a table with the following data:

Name	Description
Deny Access	Deny Access
Allow Access	Allow Access
Read Only Access	Read Only Access
Allow Access if TD Level 1	Allow Access if device is Trusted Device Level 1
Allow Access if TD Level 2	Allow Access if device is Trusted Device Level 2
Allow Access if TD Level 3	Allow Access if device is Trusted Device Level 3
Allow Access if TD Level 4	Allow Access if device is Trusted Device Level 4
Block WiFi if wired network is present	Block WiFi if wired network connection is present

At the bottom of the table, it indicates '8 results [ 50 per page]'.

Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.4

## 14.3. Events

This list contains the events which will be logged for further reference.

The screenshot shows the 'List of Events' page in the Endpoint Protector 4 Reporting and Administration Tool. The interface includes a sidebar with navigation options, a top navigation bar with 'Welcome | Logout' and a search bar, and a main content area displaying a table of events. The table has the following columns: Event Name, Description, Logging, Quick Logging, and Actions. The table lists 32 events, each with a green checkmark in the 'Logging' and 'Quick Logging' columns and a yellow icon in the 'Actions' column. At the bottom of the table, it shows '32 results' and a dropdown menu set to '50 per page'.

Event Name	Description	Logging	Quick Logging	Actions
Connected	Device Connected	✓	✓	🔗
Disconnected	Device Disconnected	✓	✓	🔗
Enabled	Device Enabled	✓	✓	🔗
Disabled	Device Disabled	✓	✓	🔗
File Read	File read from device	✓	✓	🔗
File Write	File written to device	✓	✓	🔗
File Read-Write	File read and write from device	✓	✓	🔗
File Rename	File from device renamed	✓	✓	🔗
File Delete	File deleted from device	✓	✓	🔗
Device TD	Device is trusted	✓	✓	🔗
Device not TD	Device is not trusted	✓	✓	🔗
Delete	Delete an item	✓	✓	🔗
Enable Read-Only	Device Read-Only Enabled	✓	✓	🔗
Enable if TD Level 1	Device Enabled if TD Level 1	✓	✓	🔗
Enable if TD Level 2	Device Enabled if TD Level 2	✓	✓	🔗
Enable if TD Level 3	Device Enabled if TD Level 3	✓	✓	🔗
Enable if TD Level 4	Device Enabled if TD Level 4	✓	✓	🔗
AD Import	AD Import	✓	✓	🔗
AD Synchronization	AD Synchronization	✓	✓	🔗
Blocked	Blocked on the client side	✓	✓	🔗
Unblocked	Allowed on the client side	✓	✓	🔗
Offline Temporary Password used	Offline Temporary Password used	✓	✓	🔗
User Login	User Login	✓	✓	🔗
File Encrypt	File Encrypt using EasyLock v2	✓	✓	🔗
File Decrypt	File Decrypt using EasyLock v2	✓	✓	🔗
File Encrypt (offline)	File Encrypt (offline) using Easy Lock v...	✓	✓	🔗
File Decrypt (offline)	File Decrypt (offline) using Easy Lock v...	✓	✓	🔗
Content Threat Detected	Content Aware Protection - Threat Detect...	✓	✓	🔗
Content Threat Blocked	Content Aware Protection - Threat Blocke...	✓	✓	🔗
File Copy	A file was copied to or from a removable ...	✓	✓	🔗
Scanning Data at Rest	Found Object from Scanning Data at Rest	✓	✓	🔗
User Logout	User Logout	✓	✓	🔗

32 results [ 50 per page]

### Note!

Changing this list without CoSoSys' acknowledgement can limit system functionality and performance; however, such customizations/implementations can be performed by request by one of our specialists as part of our Professional Services offered to customers.

## 14.4. File Types

This list contains common file type extensions and a description for each of them making them easier to recognize when creating audits.

The screenshot shows the 'List of File Types' page in the Endpoint Protector 4 Reporting and Administration Tool. The page features a sidebar on the left with navigation options: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, Device Types, Rights, Events, File Types, and Support. The main content area is titled 'List of File Types' and includes a 'Show all departments' link. Below the title is a 'Results' section with a table of file types. The table has four columns: Extension, Mime Type, Description, and Actions. The Actions column contains a checkbox and a delete icon for each row. At the bottom of the table, it shows '24 results ( 50 per page)' and a 'Create' button. The footer of the page contains the text 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.4'.

Extension	Mime Type	Description	Actions
.doc		Microsoft Word Document	<input checked="" type="checkbox"/>
PNG image		PNG image	<input checked="" type="checkbox"/>
OpenDocument Text		OpenDocument Text	<input checked="" type="checkbox"/>
Setup Information		Setup Information	<input checked="" type="checkbox"/>
Application		Application	<input checked="" type="checkbox"/>
.Identifier file		.Identifier file	<input checked="" type="checkbox"/>
.data file		.data file	<input checked="" type="checkbox"/>
.Hp3948 file		.Hp3948 file	<input checked="" type="checkbox"/>
Configuration Settings		Configuration Settings	<input checked="" type="checkbox"/>
Microsoft Word-Dokument		Microsoft Word-Dokument	<input checked="" type="checkbox"/>
.tmp file		.tmp file	<input checked="" type="checkbox"/>
.ace file		.ace file	<input checked="" type="checkbox"/>
.oft file		.oft file	<input checked="" type="checkbox"/>
.p file		.p file	<input checked="" type="checkbox"/>
.pas file		.pas file	<input checked="" type="checkbox"/>
.tex file		.tex file	<input checked="" type="checkbox"/>
QIF image		QIF image	<input checked="" type="checkbox"/>
Python File		Python File	<input checked="" type="checkbox"/>
.rar file		.rar file	<input checked="" type="checkbox"/>
.sh file		.sh file	<input checked="" type="checkbox"/>
.java file		.java file	<input checked="" type="checkbox"/>
VLC media file (.bin)		VLC media file (.bin)	<input checked="" type="checkbox"/>
docx		docx	<input checked="" type="checkbox"/>

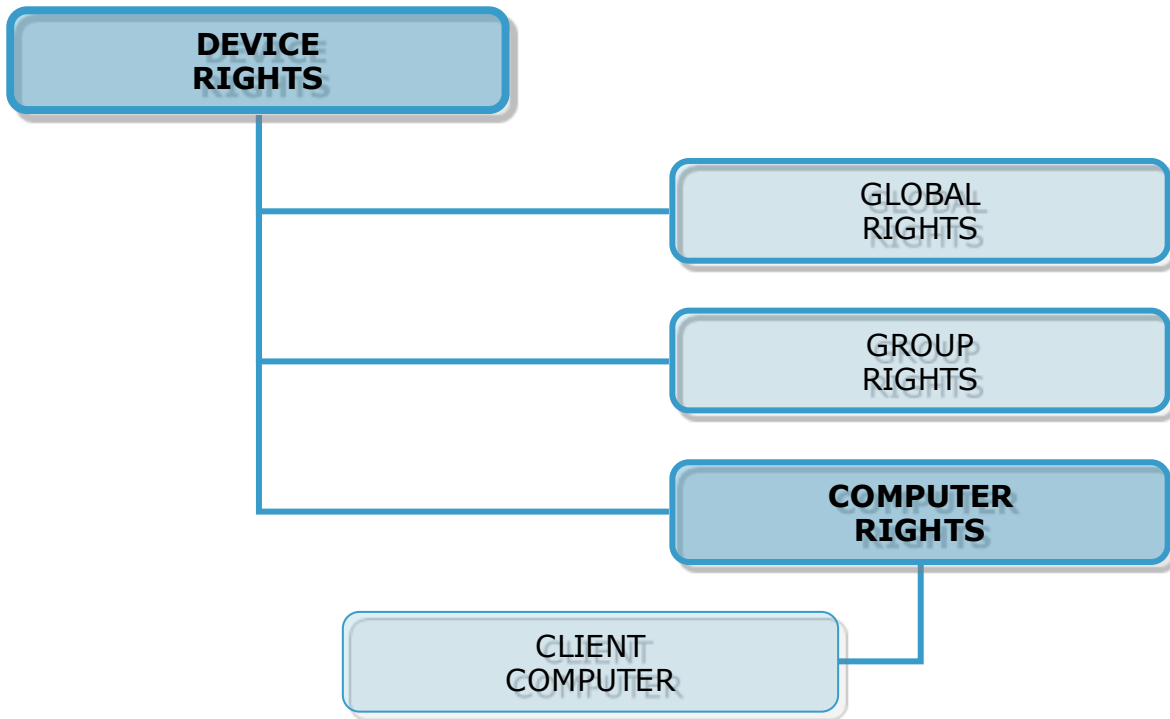
# 15. Setting up Policies

Most companies like to limit their employee's access to data, especially if it is confidential. Through Endpoint Protector you can enforce your security policies and keep confidential data away from the hands of curious employees. You can start setting your policies in the Rights section of Endpoint Protector. There are four sections here that need to be mentioned.

Device Rights, Computer Rights, Group Rights and Global Rights. You can find descriptions of these items in the previous paragraphs. Before configuring computers and devices, there are certain aspects of Endpoint Protector you should be aware of.

Computer Rights, Group Rights and Global Rights form a single unit and they inherit each-others settings, meaning that changes to any one of these modules affect the other ones. There are three levels of hierarchy: Global Rights, Group Rights and Computer Rights, the latter being the deciding factor in rights management.

The Device Rights module surpasses all settings from Computer Rights, Group Rights and Global Rights. If you give permission to a device to be available to clients, it will be usable under any circumstances.



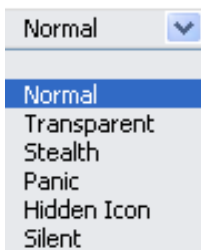
For example: in Global Rights, assign Allow for device X. If in Computer Rights, the same device does not have permission to be used; the device will not be usable. Same applies vice-versa: if the device lacks permission to be used in Global Rights, and has permission under Computer Rights, the device will be usable to the client. The same applies for Global Rights and Group Rights: if under Global Rights the device does not have permission to be used, and under Group Rights permission exists, the device will be available to the client.

	DEVICE 1	DEVICE 2	DEVICE 3	DEVICE 4	DEVICE 5	DEVICE 6
GLOBAL RIGHTS	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED
GROUP RIGHTS	NOT ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED
COMPUTER RIGHTS	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED
CLIENT COMPUTER	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED



# 16. Modes for Users, Computers and Groups

Endpoint Protector features several functionality modes for users, computers and groups. These modes are accessible for each item (users, computers, groups) from the System Policies module of Endpoint Protector using the "Edit" button.



You can change these at any given time.

There are six modes from which you can choose:

- Normal Mode (default setting of Endpoint Protector)
- Transparent Mode
- Stealth Mode
- Panic Mode
- Hidden Icon Mode
- Silent Mode

## 16.1. Transparent Mode

This mode is used if you want to block all devices but you don't want the user to see and know anything about EPP activity.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is blocked regardless if authorized or not
- Administrator receives alerts (dashboard also shows alerts) for all activities

## 16.2. Stealth Mode

Similar to Transparent mode, Stealth mode allows the administrator to monitor all of the users and computers activities and actions with all devices allowed.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is allowed (nothing is blocked regardless of what activity)
- file shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts (dashboard shows also alerts) for all activities

## 16.3. Panic Mode

Under special circumstances, Panic Mode can be set manually by the administrator in order to block all access to devices.

- system tray icon is displayed
- notifications are displayed
- everything is blocked regardless if authorized or not
- Administrator receives alert (dashboard also shows alerts) when PCs are going in and out of Panic mode

## 16.4. Hidden Icon Mode

The Hidden Icon Mode is similar to the Normal mode, the difference consisting in the fact that the Agent is not visible to the user.

- no system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

## 16.5. Silent Mode

The Silent Mode is similar to the Normal mode, the difference consisting in the fact that the notifications do not pup-up to the user.

- system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied

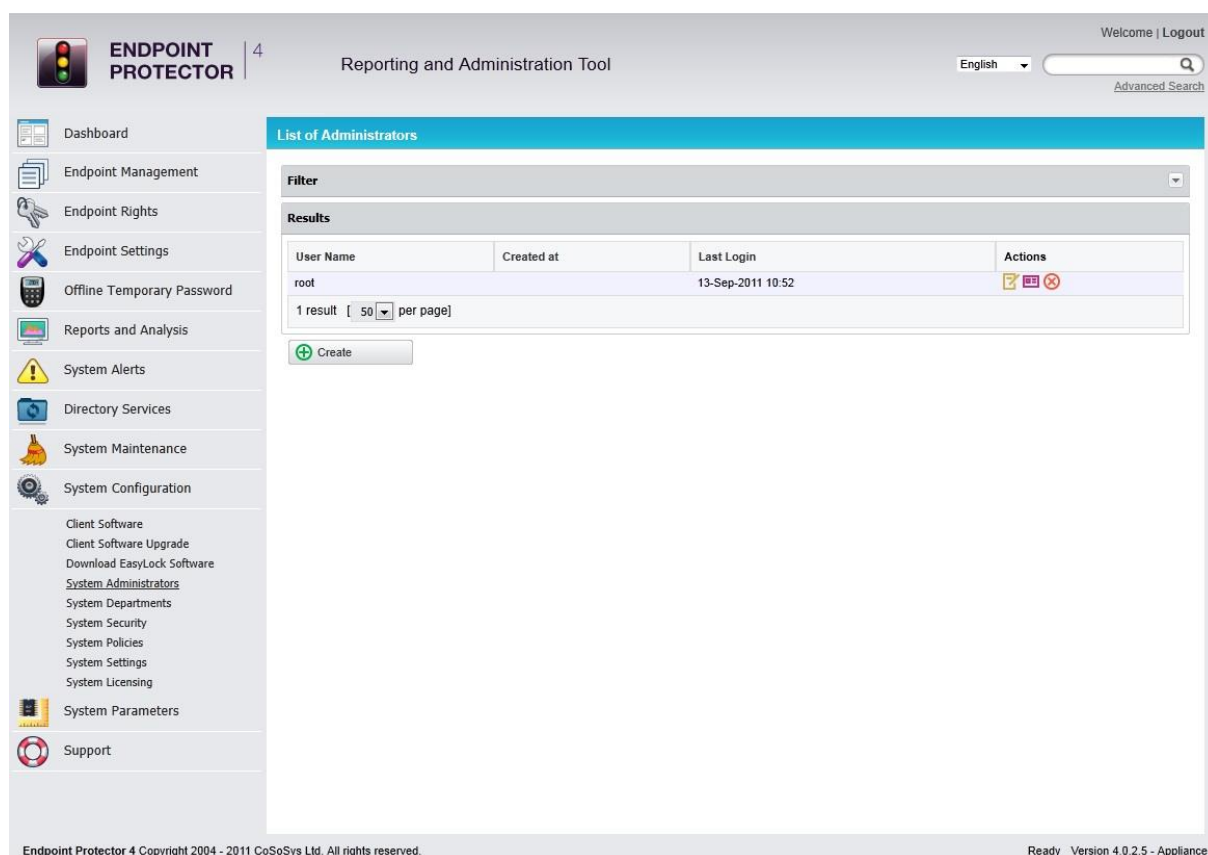
## 15.6. Adding new administrator(s)

You can add an unlimited number of system administrators, depending on the size and manageability of your network.



While fewer administrators are recommended for easier data loss prevention, it is easier to manage a large network with more.

To add an administrator or Super Administrator in Endpoint Protector, you must login as a super administrator and access the "System Configuration" module then the "Administrators" panel.

Here you can see a list of current Administrator and Super Administrators.



The screenshot shows the Endpoint Protector web interface. The top navigation bar includes the logo, version number '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar. The left sidebar contains a menu with categories like 'Dashboard', 'Endpoint Management', 'Endpoint Rights', 'Endpoint Settings', 'Offline Temporary Password', 'Reports and Analysis', 'System Alerts', 'Directory Services', 'System Maintenance', 'System Configuration', 'Client Software', 'Client Software Upgrade', 'Download EasyLock Software', 'System Administrators', 'System Departments', 'System Security', 'System Policies', 'System Settings', 'System Licensing', 'System Parameters', and 'Support'. The main content area is titled 'List of Administrators' and features a 'Filter' dropdown, a 'Results' table, and a 'Create' button. The table contains one entry for the user 'root'.

User Name	Created at	Last Login	Actions
root		13-Sep-2011 10:52	 

1 result [ 50 per page]

[+ Create](#)

Endpoint Protector 4 Copyright 2004 - 2011 CoSoSys Ltd. All rights reserved. Ready Version 4.0.2.5 - Appliance

To add another Administrator or Super Administrator, click the "Create" button.

**Administrator User**

**User Information**

User Name:	<input type="text" value="My Admin"/>
Password:	<input type="password" value="••••••••"/>
Password Confirmation:	<input type="password" value="••••••••"/>

**Permissions and Departments**

Is active:	<input checked="" type="checkbox"/>
Is super admin:	<input type="checkbox"/>
Departments:	<input type="checkbox"/> Default Department

**Information**

Last Login:	
-------------	--

Enter the desired user name and password for the new account, then set if the account is active or not or whether is a super admin or not.

**Permissions and groups**

Is active:	<input checked="" type="checkbox"/>
Is super admin:	<input type="checkbox"/>

**Is active** – if this option is not enabled the selected user cannot log in to the Endpoint Protector console. Use this option in case you want to create temporary admin or super admin privileges to a certain user and then remove them or if you want to disable an administrator but do not want to delete his credentials from the server.

**Is Super Admin** – Super Administrators have more rights than administrators. Super Administrator can create, delete and modify administrator and super administrator settings, while standard administrators do not have this right. The most important difference is that only super administrators are able to view the "Reports and Analysis" section if the option "Data Security Privileges" is selected.

## 16.7. Working with logs and reports

Endpoint Protector creates a device activity log in which it records actions from all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

**Logs Report** - The most powerful and detailed representation of activity recording can be achieved using this module. This allows the administrator to see exactly which device, computer a user used on a specific time interval, and whether the shadowing for that user/device is enabled or not. There is a special filter designed to make it easier to find this information.

**Online Users** – Online users are end users who have logged on to a client computer.

**Online Computers** – Online Computers are client computers which have been set up to communicate with the Endpoint Protector server by installing the Endpoint Protector Client. Here you can see a list of computers which are currently powered on and you can view the actions they have taken.

**Online Devices** – Connected Devices are devices which are currently plugged-in to one of the (online) client computers. Here again you have the possibility to view an activity log, this time, of the device.

**Statistics** – The statistics module can generate reports on registered computers, devices and users based on traffic, connections or overall activity. You can set a period for this report (last week, month or year).

# 17. Enforced Encryption with Trusted Devices

Protecting Data in Transit is essential to ensure no third party has access to data in case a device is lost or stolen. The Enforced Encryption solution gives administrators the possibility to protect confidential data on portable devices in case of loss or theft.

Ensuring only encrypted devices can be used on computers where Endpoint Protector is present can be done by utilizing Trusted Devices. Trusted Devices must receive authorization from the Endpoint Protector 4 Server, otherwise they will be unusable. There are four levels of security for Trusted Devices.

- **Level 1** - Minimum security for office and personal use with a focus on software based encryption for data security. Any USB Flash Drive and most other portable storage devices can be turned into a Trusted Device Level 1. It does not require any specific hardware but it does need an encryption solution such as EasyLock  
<http://www.endpointprotector.com/en/index.php/products/easylock>
- **Level 2** - Medium security level with biometric data protection or advanced software based data encryption. It requires special hardware that includes security software and has been tested for Trusted Device Level 2.
- **Level 3** - High security level with strong hardware based encryption that is mandatory for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC. It requires special hardware that includes advanced security software and hardware based encryption that has been tested for Trusted Device Level 3.
- **Level 4** - Maximum security for military and government use. Level 4 Trusted Devices include strong hardware based encryption for data

protection and are independently certified (e.g. FIPS 140). These devices have successfully undergone rigorous testing for software and hardware. It requires special hardware that is available primarily through security focused resellers.

- **Level 1+** - Derived from Level 1, it will ensure that EasyLock 2 with Master Password will be automatically deployed on USB storage devices plugged into computers where the Endpoint Protector Client is present.

The table below provides a comprehensive list of TrustedDevices:


Device Names	TrustedDevices Level
UT169, UT176	2
Trek ThumbDrive	2
AT1177	2
Verbatim: V-Secure, Secure Data USB Drive	3
Kanguru: Defender Elite, Elite 30, Elite 200, Defender Elite 2000, Flashtrust	3
IronKey Secure Drive	3
Buffalo Secure Lock	3
Stealth MXP Bio	4
SafeStick BE	4

## 17.1. Managing Trusted Devices from Endpoint Protector

Access Rights to Trusted Devices can be configured from the Endpoint Rights > Global Rights section. The drop-down box next to the USB Storage Device allows the desired Trusted Device Level to be selected and enforced.



**Management of Global Rights**

 **Currently the system is using both computer and user rights, user rights have priority .**

**Groups**

**Name:** Global


**Description:** Global Group including all the entities

**Device Types**

USB Storage Device	Allow Access	iPhone
Internal CD or DVD RW	Preserve global setting	iPad
Internal Card Reader	Deny Access	iPod
Internal Floppy Drive	Allow Access	Serial ATA Controller
Local Printers	Read Only Access	WiFi
Windows Portable Device	Allow Access if TD Level 1	Bluetooth
Digital Camera	Allow Access if TD Level 2	FireWire Bus
BlackBerry	Allow Access if TD Level 3	Serial Port
Mobile Phones (Sony Ericsson, etc.)	Allow Access if TD Level 4	PCMCIA Device
SmartPhone (USB Sync)	Deny Access	Card Reader Device (MTD)
SmartPhone (Windows CE)	Deny Access	Card Reader Device (SCSI)
SmartPhone (Symbian)	Deny Access	ZIP Drive
Webcam	Deny Access	

**Already existing devices**

+

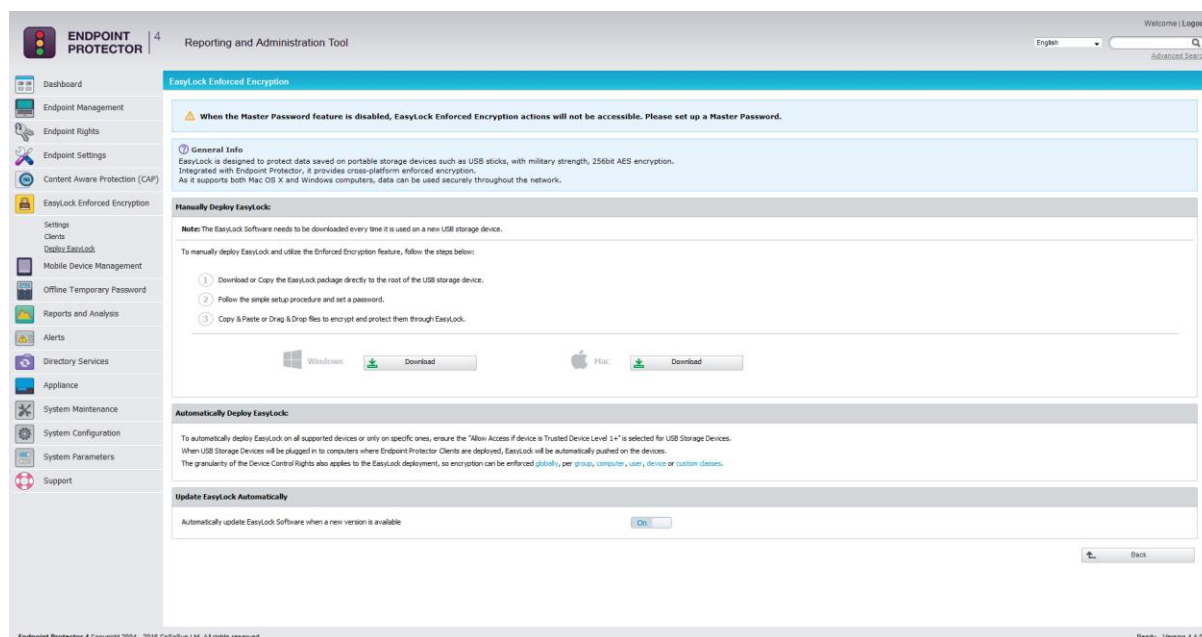
 Save

## 17.2. Trusted Device Level 1 and Enforced Encryption with EasyLock

EasyLock allows USB storage devices to be identified as Trusted Devices Level 1 and protects the stored data on the device with government-approved 256bit AES CBC-mode encryption. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device. Accessing data stored on the device can be done via the password the user configured or via a Master Password set by the Endpoint Protector administrator. The encrypted data can be opened by any user only after it is decrypted, therefore requiring the user to copy the information out of EasyLock

### 17.2.1. Deploying EasyLock

EasyLock is a cross-platform encryption solution, supporting both Mac OS X and Windows computers. Deploying the software can be done from the EasyLock Enforced Encryption section in the Endpoint Protector interface.



Deployment can be done automatically if "Allow Access if Trusted Device Level 1+" is selected for the USB Storage Devices. This can be done by going to Endpoint Rights > Global Rights section or using the quick links provided, as per the image above.

Manual deployment is also available. Download links for both Windows and the Mac OS X are available in this section. The downloaded EasyLock file must be copied onto the USB storage device and executed from the root of the device. Due to extended security features for manual deployment, EasyLock will have to be redownloaded from the Endpoint Protector interface each time it will be used to encrypt a new USB storage device.

Both EasyLock deployments are straight forward and require the user only to configure a password.

### Note!

USB storage devices with multiple partitions are not supported by EasyLock and Trusted Devices Level 1 on Mac OS X.

## 17.2.2. EasyLock Enforced Encryption Settings and Clients

This sections allow the Endpoint Protector administrator a way to remotely manage EasyLock encrypted devices. Before being able to take advantage of the features provided, the administrator must configure a Master Password.

The screenshot displays the 'EasyLock Enforced Encryption - Settings' page in the Endpoint Protector Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Endpoint Management, and EasyLock Enforced Encryption. The main content area is divided into several sections:

- EasyLock Master Password:** Fields for Old Master Password, New Master Password, and Confirm New Master Password, with a 'Save Master Password' button.
- EasyLock Security Details:** Fields for User Maximum Password Retries (10), User Minimum Password Length (6), and Device Status becomes 'Inactive' after (30 days).
- EasyLock Installation and Execution:** A checkbox to allow EasyLock to be installed and run only on computers where the Endpoint Protector Client is present, with a 'Save Settings' button.
- EasyLock File Tracing:** Checkboxes for File Tracing and Offline File Tracing, with a 'Save File Tracing' button.
- EasyLock License:** A field for EasyLock Site License with a green checkmark indicating it is active.

At the bottom right, there is a 'Back' button. The footer shows 'Endpoint Protector 4 Copyright 2004 - 2016 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.9'.

In the Settings section, the Master Password can be configured, EasyLock File Tracing enabled, as well as defining the installation and execution of EasyLock only on computers where the Endpoint Protector Client is present.

In the Clients section, all EasyLock enforced devices are listed. By selecting the Manage Client Action a list of Actions History is displayed, as well as the option to manage them by sending a message, changing user's password, resetting the device, resending the master password and more.

The screenshot displays the 'EasyLock Enforced Encryption - Manage Client' page. It shows details for a specific client named 'test' and a table of its actions history.

**Client Details:**

- Name: test
- Device Name (Identification): -
- Description: [Redacted]
- Status: Active
- Last Location IP: 192.168.0.153
- Last Seen: 03-Feb-2016 13:39:12
- Created at: 03-Feb-2016 13:39:12
- Created by: user
- Username: [Redacted]
- Computer Name: [Redacted]
- Vendor ID: [Redacted]
- Product ID: [Redacted]
- Serial Number: [Redacted]
- Modified at: [Redacted]
- Modified by: [Redacted]

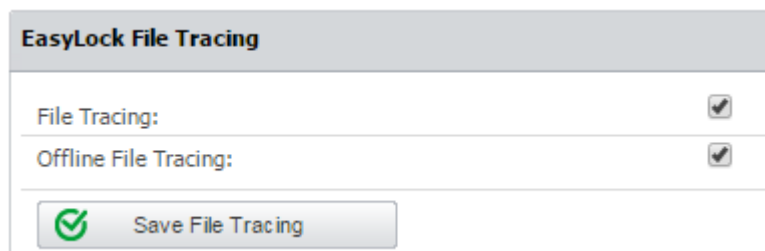
**Actions History Table:**

Type	Status	Details	Created at	Modified at	Created by	Modified by	Actions
Re-deploy Client	Completed		3 February 2016 15:39	3 February 2016 15:39	auto	auto	
Reset Device	Cancelled		2 February 2016 17:42	2 February 2016 17:42	root	root	
Reset Device	Failed		2 February 2016 17:42	2 February 2016 17:42	root	root	
Change Master Password			2 February 2016 17:41	2 February 2016 17:41	root	root	
Change User Password			2 February 2016 17:39	2 February 2016 17:39	root	root	
Send Message			2 February 2016 17:39	2 February 2016 17:39	root	root	
Send Message			2 February 2016 17:38	2 February 2016 17:38	root	root	
Send Message			2 February 2016 16:32	2 February 2016 16:32	root	root	
Change Settings - Installation and Execution			2 February 2016 16:30	2 February 2016 16:30	root	root	
Change Master Password			2 February 2016 15:47	2 February 2016 15:47	root	root	
Send Message			2 February 2016 15:22	2 February 2016 15:22	root	root	
Send Message			2 February 2016 15:22	2 February 2016 15:22	root	root	
Send Message			2 February 2016 15:21	2 February 2016 15:21	root	root	
Change Settings - Installation and Execution			2 February 2016 11:28	2 February 2016 11:28	root	root	
Re-deploy Client			1 February 2016 12:44	1 February 2016 12:44	auto	auto	

At the bottom, there are 'Export' and 'Refresh List' buttons, and a 'Back' button. The footer shows 'Endpoint Protector 4 Copyright 2004 - 2016 CoSoSys Ltd. All rights reserved.' and 'Ready Version 4.4.0.9'.

### 17.2.3. File Tracing on EasyLock Trusted Devices

Endpoint Protector 4 allows tracing of files copied and encrypted on portable devices using EasyLock. This option can be activated from inside the Settings windows located under the EasyLock Enforced Encryption tab.



By checking the File Tracing option, all data transferred to and from devices using EasyLock is recorded and logged for later auditing. The logged information is automatically sent to the Endpoint Protector Server if Endpoint Protector Client is present on that computer. This action takes place regardless of the File Tracing option being enabled or not for that specific computer through the Device Control module.

In case that Endpoint Protector Client is not present, the information is stored locally in an encrypted format on the device and it will be sent at a later time from any other computer with Endpoint Protector Client installed.

The additional "Offline File Tracing" option is an extension to the first option, offering the possibility to store information directly on the device, before being sent to the Endpoint Protector Server. The list of copied files is sent only next time the device is plugged in and only if Endpoint Protector Client is present and communicates with the Endpoint Protector Server.

Additionally, Easy Lock performs File Shadowing for the files that are transferred, if Endpoint Protector Client is present and the File Shadowing option is enabled on the computer on which the events occur – through the Device Control module. This is a real time event and no shadowing information is stored on the device at any given time.

#### **Note!**

Enabling global File Tracing will not automatically activate the File Tracing option on EasyLock Trusted Devices and vice versa.

# 18. Endpoint Protector Client

The Endpoint Protector Client is the application which once installed on the client Computers (PC's), communicates with the Endpoint Protector Server and blocks or allows devices to function, as well as sends out notifications in case of unauthorized access.

## 18.1. Endpoint Protector Client Installation

To install the Endpoint Protector Client on your client computers, you can download it directly from the Endpoint Protector Server Web interface, under the System Configuration -> Client Software tab.

### Note!

You need to "Save" the Endpoint Protector Client first on a location and then install it from there. Do not run it directly from the browser!



Before downloading the Endpoint Protector Client, please make sure that you specify the IP of your Endpoint Protector Server and the unique code of the Department in which you want to include it. In case that no unique code is entered, the client will be assigned to the Default Department.

The screenshot shows the 'Endpoint Protector Server - Download Client Software' page. The main content area is titled 'Endpoint Protector Client Installation'. It includes a note: 'Note: Endpoint Protector Client version higher than 4.1.0.0 is required for Content Aware Protection.' Below this, it lists the operating systems where the client can be installed: Windows 8 (32bit and 64bit), Windows 7 (32bit and 64bit), Windows Vista (32bit and 64bit), Windows XP (32bit and 64bit), Windows Server 2003/2008 (32bit and 64bit), Mac OS X 10.5+ (Snow Leopard), Mac OS X 10.4 (Tiger), and Linux (Ubuntu, OpenSUSE). It then provides a form to specify the Endpoint Protector Server IP (192.168.7.70), Endpoint Protector Server Port (443), and Department Code (defdep). Below the form, there are radio buttons for selecting the client version: Windows (32bit version) - Version: 4.2.9.2, Windows (64bit version) - Version: 4.2.9.2, Mac OS X 10.5+ (Leopard) - Version: 1.4.0.6, 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 - Ubuntu 14.4 LTS - Version: 1.0.5-1, and Linux - OpenSUSE 11.4 - Version: 1.0.0-1. A 'Download selected version' button is located below the radio buttons. At the bottom of the page, it says 'Endpoint Protector Client for Windows can be deployed over Active Directory. For more information, please refer to Endpoint Protector - User Guide.'

Active Directory can be used for Endpoint Protector Client deployment as well. This feature can be used by accessing the Endpoint Protector **Directory Services** menu. The manual containing the instructions for importing and synchronizing Active Directory with Endpoint Protector can be accessed from the Support Menu, at **AD Deployment Guide**.

### Note!

For Linux clients, please consult the **readmeLinux.txt** file available under the "Read this before installing" link for exact installation instructions corresponding to the previously selected Linux distribution!

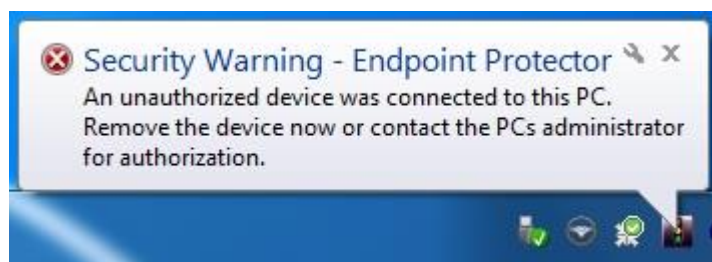
## 18.2. Endpoint Protector Client Security

The Endpoint Protector Client has a built in security system which makes stopping the service nearly impossible.

This mechanism has been implemented to prevent the circumvention of security measures enforced by then network administrator.

### 18.3. Client Notifications (Notifier)

The Endpoint Protector Client, depending in the mode it is currently running on, will display a notification from the taskbar icon when an unauthorized device is connected to the PC. Not only does it log any attempts to forcefully access the system, it can also trigger the Panic mode.

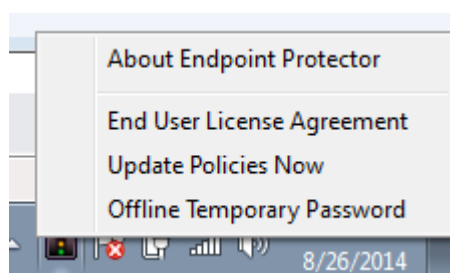


In case of a Mac, the notification will look like bellow:



### 18.4. Client Policy Update

The Client has a built in feature to ensure the latest policies are received. The "Update Policies Now" is available by right clicking on the Endpoint Protector system tray icon, as shown below:



## 18.5. Offline Functionality for Endpoint Protector Client

Depending on the global settings the Endpoint Protector Client will store a local file tracing history and a local file shadow history that will be submitted and synchronized with the Endpoint Protector Server upon next connection to the network.

## 18.6. DHCP / Manual IP address

Endpoint Protector Client automatically recognizes changes in the network's configuration and updates settings accordingly, meaning that you can keep your laptop protected at the office (DHCP) and at home (Manual IP address) too without having to reinstall the client or modify any changes.

## 18.7. Client Removal

### 18.7.1. Client Removal on Windows OS

The Endpoint Protector Client cannot be uninstalled without specifying the password set by the administrator(s) in the Reporting and Administration Tool.

There is also the option to remotely uninstall clients from the

### 18.7.2. Client removal on MAC OS X

To remove the Endpoint Protector Client you need to run (double click in Finder) the "remove-epp.command" file that was attached to the "Endpoint Protector" client package that you downloaded.

You will be prompted to enter the root password to perform administrative tasks.

### 18.7.3. Client removal on Linux OS

To remove the Endpoint Protector Client you need to run from the console/terminal the "uninstall.sh" file that was attached to the "Endpoint Protector" client package that you downloaded.

#### **Note!**

For exact uninstall instructions corresponding to your Linux distribution, please consult the readme file available in the System Configuration – Client Installation window by clicking the "Read this before installing" link!

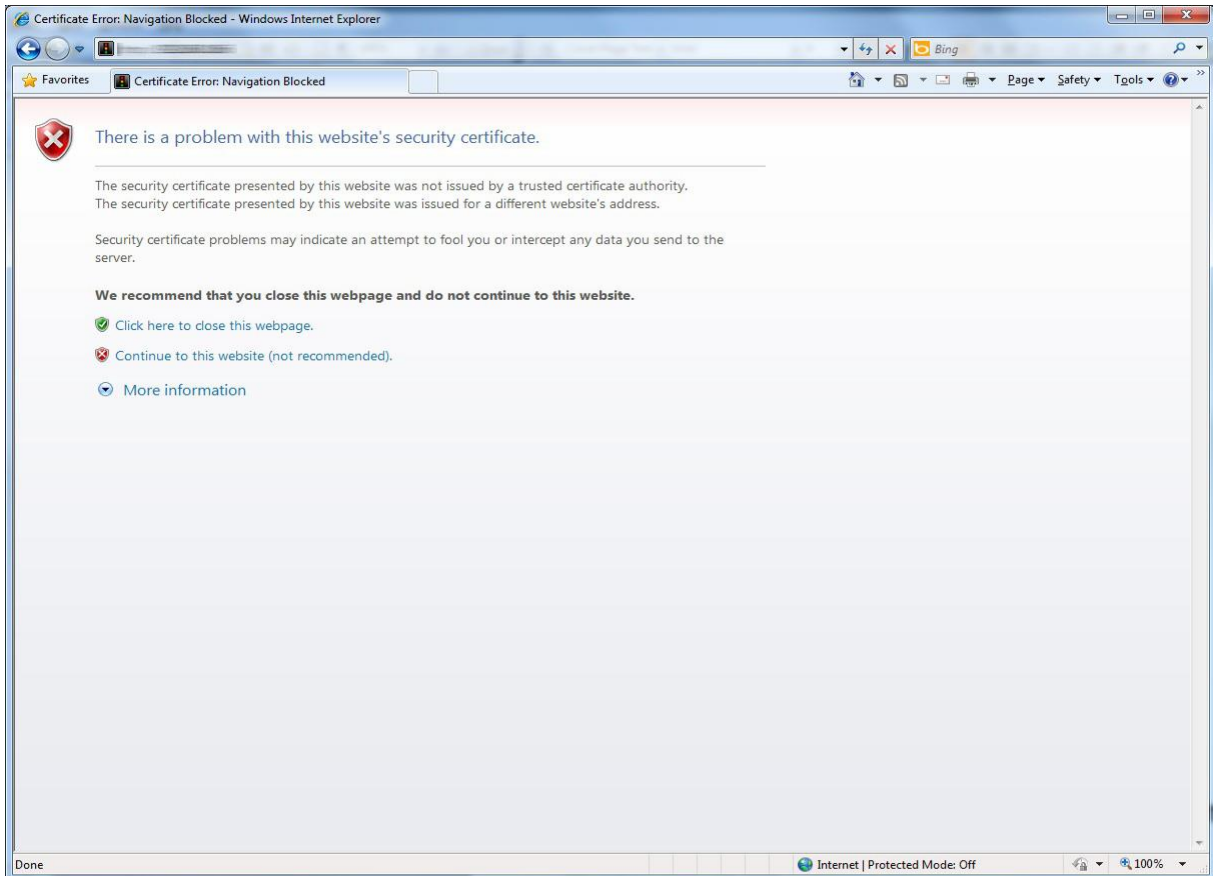



# 19. Installing Root Certificates to your Internet Browser

## 19.1. 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)".

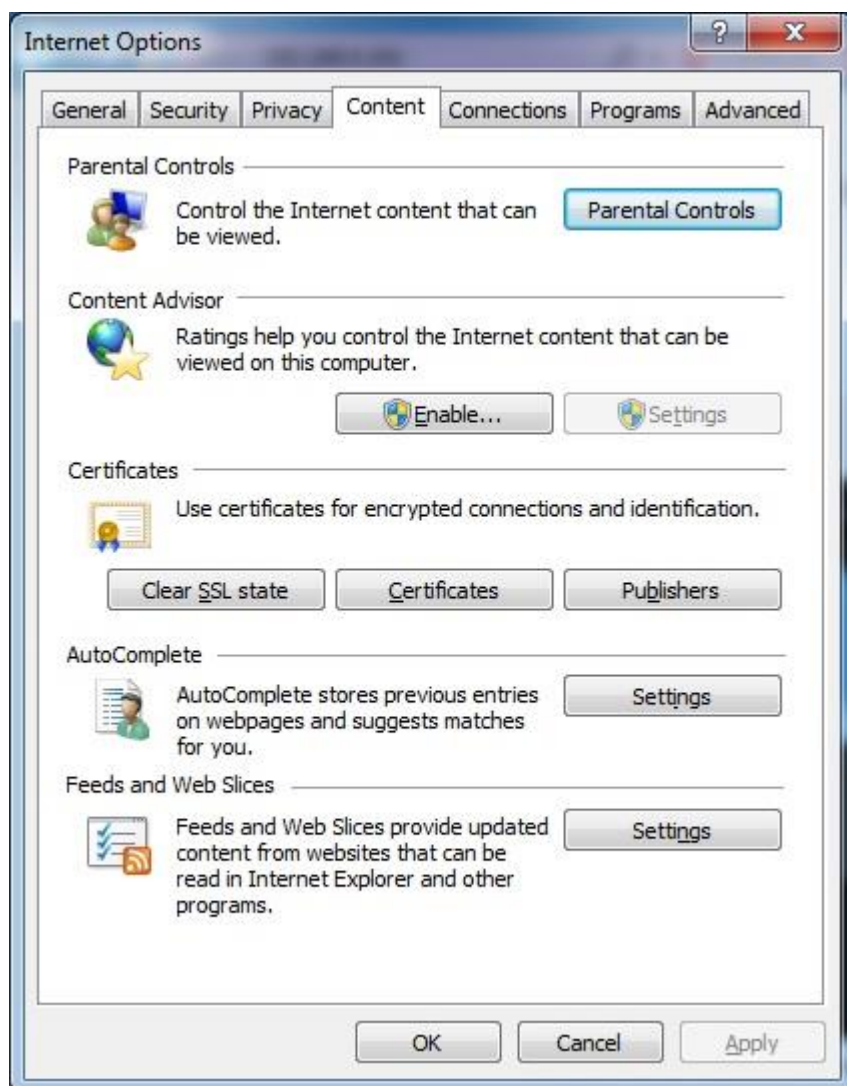
Now, go to the Certificate file you downloaded from the Appliance Setup Wizard->Appliance Server Certificate-> and install the Certificate.

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

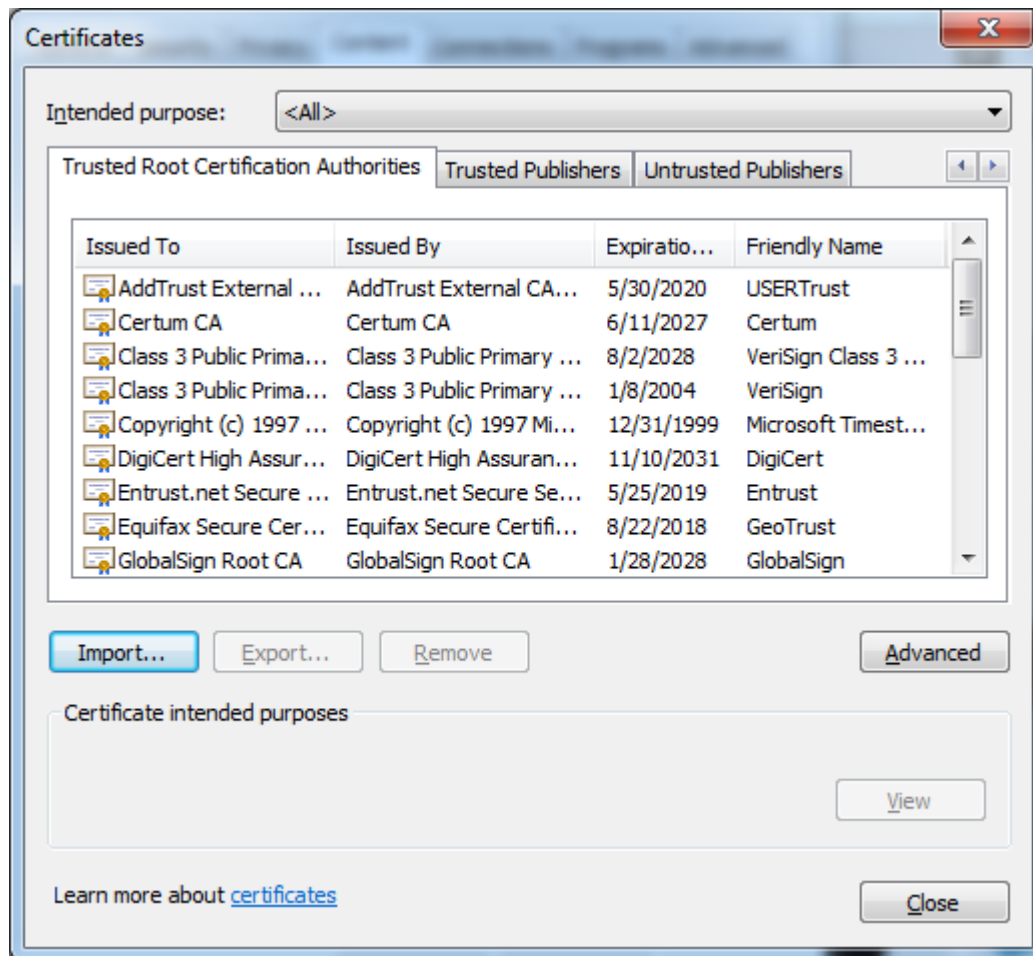
By clicking the "Certificate Error" button, a pop-up window appears. Just click the "View certificates" in that pop-up window.

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.



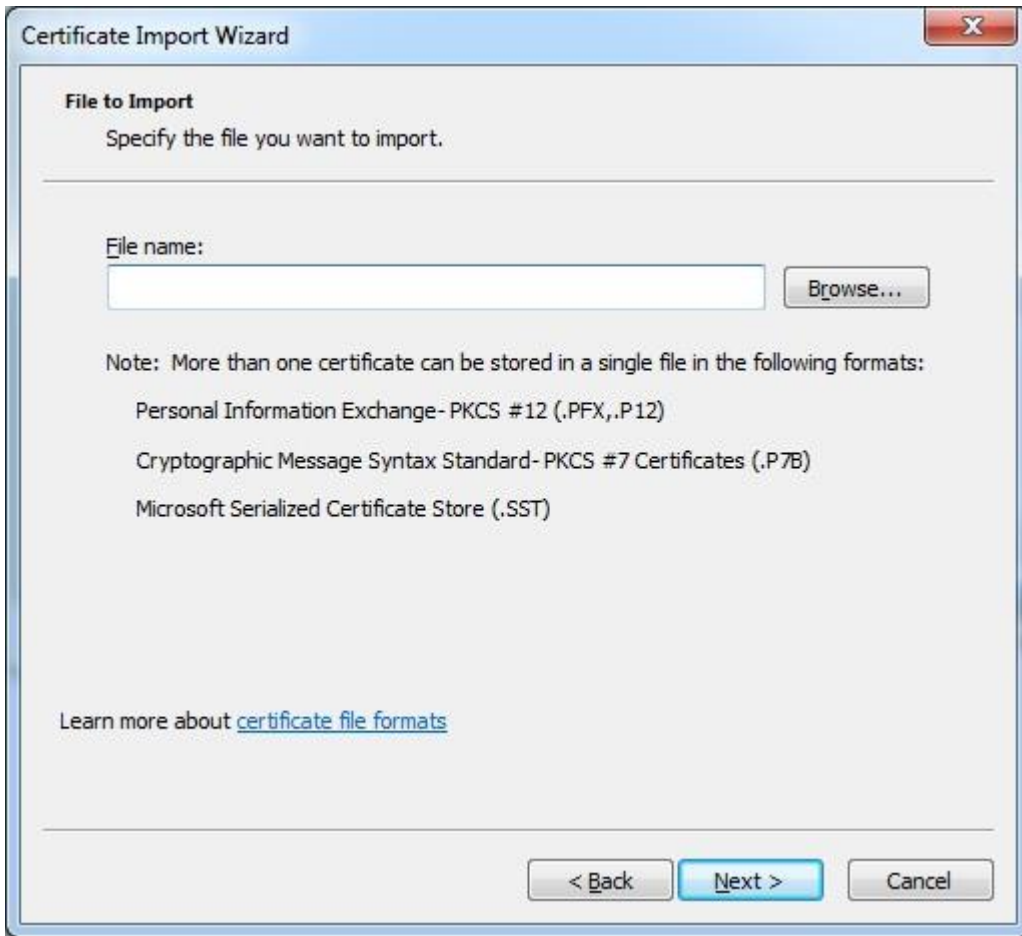
From the Certificates list, select “Trusted Root Certification Authorities” and click on the “Import” button.



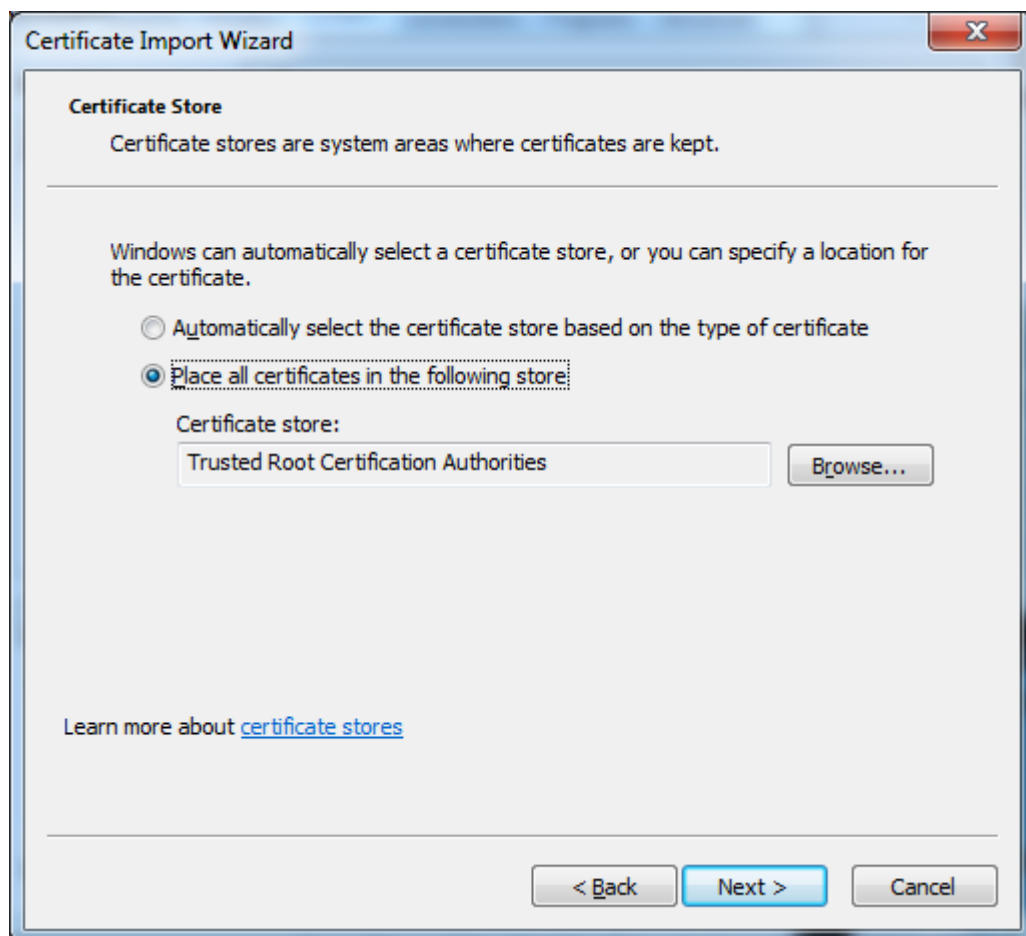
A Welcome to the Certificate Import Wizard pops up. Just click the Next button.



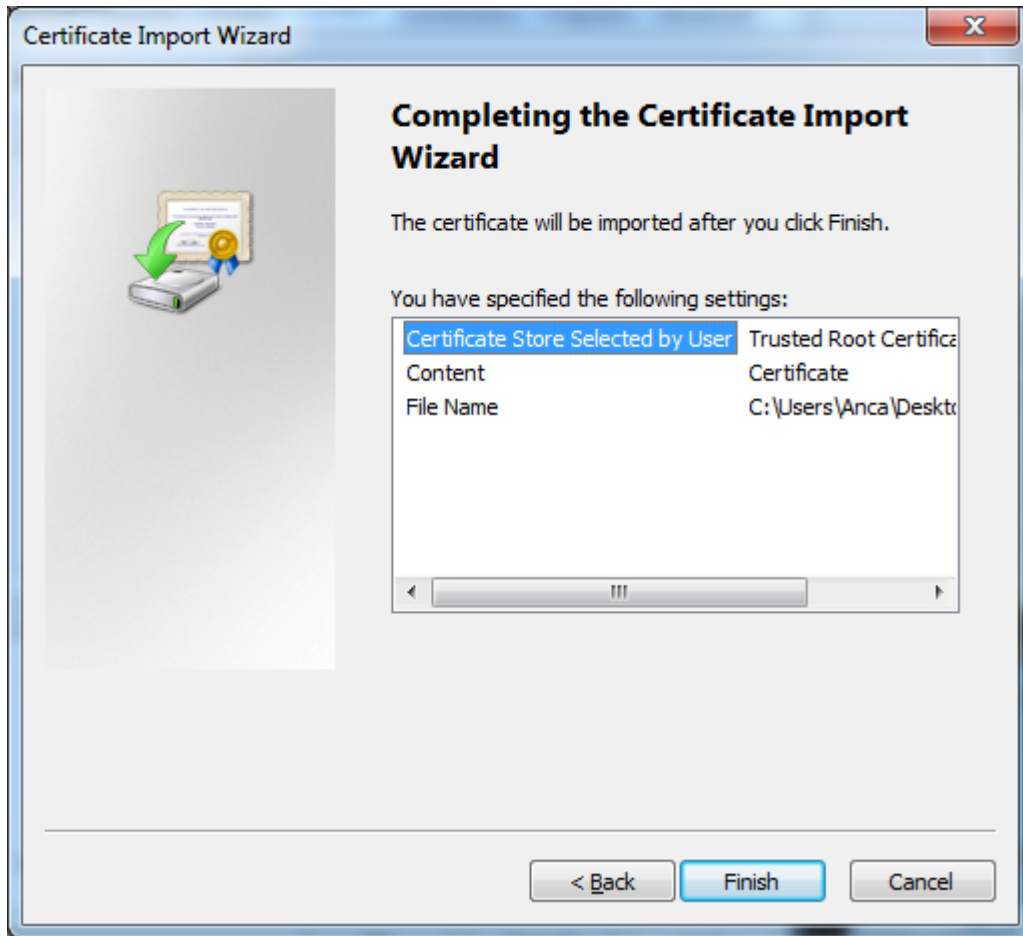
Browse for the Certificate file you downloaded from the Appliance Setup Wizard  
->Appliance Server Certificate.



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.

The screenshot displays the Endpoint Protector Reporting and Administration Tool interface. At the top left, the logo for Endpoint Protector 4 is visible, along with the text 'Reporting and Administration Tool'. In the top right corner, there is a 'Welcome Guest | Login' link and a language dropdown menu set to 'English'. The main content area is divided into several sections:

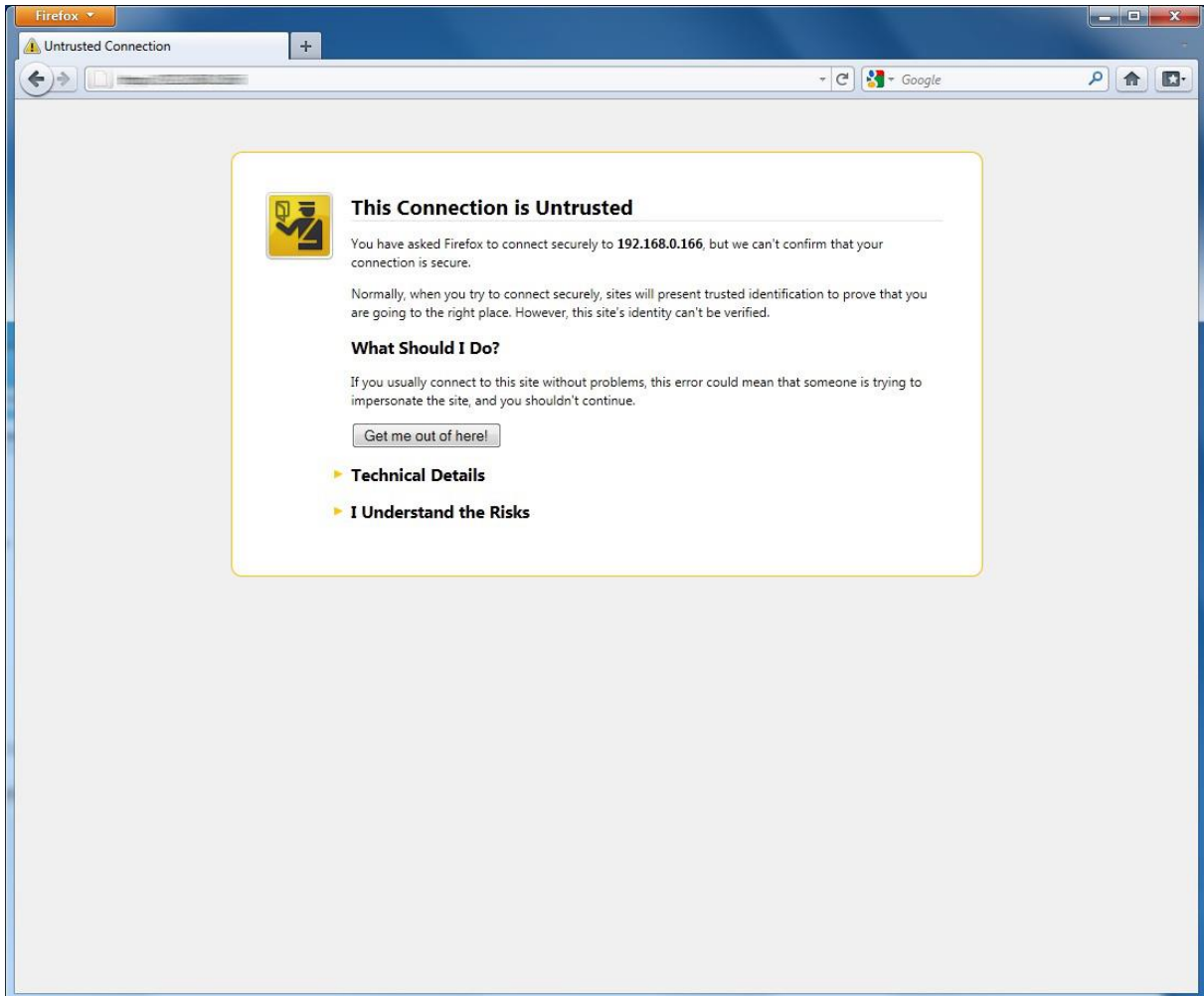
- Login:** A blue sidebar on the left contains a login form with fields for 'Username' and 'Password', a 'Login' button, and icons for 'Mac' and 'PC'. Below this, it lists 'Protected Network' and 'Controlled Mobile Devices' with icons for 'iPhone / Android Phone' and 'iPad / Android Tablet'.
- Device Control:** Features 'Blocked Devices' (with icons of a smartphone, tablet, and laptop) and 'Authorized Devices' (with icons of a smartphone, tablet, and laptop).
- Enforced Encryption:** Includes 'Encrypted Data Transfer with EasyLock'.
- Content Aware Protection:** Contains 'Strong DLP Policy', 'Applications' (with icons for various apps), 'Reporting and Analysis', and 'Devices'.
- Mobile Device Management:** Includes 'Strong Security Policy', 'App Management', 'Tracking and Locating', 'Password Enforcement', 'Device Encryption', and 'Remote Wipe/Lock'.

At the bottom of the interface, there is a navigation bar with the following links: 'Data Loss Prevention | Device Control | Content Aware Protection (CAP) | Mobile Device'. The footer contains the text 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks Version 4.4.0.4'.

## 19.2. 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 and restart the browser.

# 20. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

## 20.1. Server Related

Appliance – Appliance refers to the Endpoint Protector Appliance which is running the Endpoint Protector Server, Operating System, Databases, etc.

Computers – refers to PC's, workstations, thin clients, notebooks which have Endpoint Protector Client installed.

File Tracing - this feature will track all data that was copied to and from prior authorized portable storage devices.

File Shadowing – this feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.

Devices – refers to a list of known portable storage devices, ranging from USB storage devices to digital cameras, LTP storage devices and biometric devices.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

Departments – an alternative way to Groups to organize main entities (devices, users or computers), which involves also the administrators of Endpoint Protector.

## 20.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

Trusted Devices – portable storage devices that carry a seal of approval from the Endpoint Protector Server and can be utilized according to their level (1-4). For more information please see “Enforced Encryption with Trusted Devices” section.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC’s, Workstations and/or Notebooks which have Endpoint Protector Client installed and are currently running and are connected to the Endpoint Protector server.

Connected devices – are devices which are connected to online computers.

Events – are a list of actions that hold major significance in Endpoint Protector. There are currently 17 events that are monitored by Endpoint Protector:

- Connected – the action of connecting a device to a computer running Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File read - a file located on a portable device was opened by a user or the file was automatically opened if the portable device was autorun by the operating system.
- File copy – a file was copied onto or from a portable device.
- File write – a file located on a portable device was opened and edited; changes were saved to the file.
- File renamed – a file located on a portable device has been renamed.

- File delete – a file located on a portable device has been deleted.
- Device TD – means that a device is registered as a Trusted Device and has access to files accordingly
- Device not TD – means that a device is not trusted and does not have automatic access to files
- Delete – refers to computers, users, groups, alerts and devices; the action of removing any of these items from the list
- Enable read-only – refers to devices; the action of allowing access to devices but disabling the ability to write on them. User(s) can copy files from device(s) but cannot write anything onto the device.
- Enable if TD Level 1-4 – refers to Trusted Devices; grants the device access if the device is a level one, two, three or four Trusted Device.
- Offline Temporary Password used – refers to computers, the action of temporarily allowing access to a specific device on a certain client computer.

# 21. Support

In case additional help, such as the FAQs or E-MAIL support is required, please visit our support website directly at <http://www.cososys.com/help.html>.

You can also write an E-MAIL to our Support Department under the Contact Us tab from the Support module.

The screenshot displays the 'Reporting and Administration Tool' interface for Endpoint Protector. The top navigation bar includes the 'ENDPOINT PROTECTOR' logo, a version indicator '4', the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a 'Welcome | Logout' link. A search bar with 'Advanced Search' is also present. The left sidebar contains a menu of system management options: Dashboard, Endpoint Management, Endpoint Rights, Endpoint Settings, Content Aware Protection (CAP), Mobile Device Management, Offline Temporary Password, Reports and Analysis, Alerts, Directory Services, Appliance, System Maintenance, System Configuration, System Parameters, and Support. The 'Support' option is selected, leading to a 'Contact Support' page. This page features a 'Support Form' with the following fields: 'Sender E-mail \*', 'Company Name' (pre-filled with 'CSS'), 'Subject', and 'Content' (with a placeholder text 'Please describe here your problem or your suggestions!'). A 'Send' button is located at the bottom of the form. The footer of the interface shows 'Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved.' and 'No Background Tasks Version 4.4.0.4'.

One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

# 22. 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.