

User Manual for Version 4.5.0.1

# User Manual



# Table of Contents

1.In	trodu	uction1
1.1.	What	is Endpoint Protector?2
1.2.	Main	Features4
	1.2.1.	Centralized web based Device Management / Dashboard 4
	1.2.2.	Control your data flow: File Tracing / File Shadowing
	1.2.3.	Audit Trail – Device Activity Logging
	1.2.4.	Audit Trail – Reporting and Analysis Tools
	1.2.5.	Sensitive Content Filtering5
	1.2.6.	File Whitelist5
	1.2.7.	Easy Enforcement of Your Security Policies
	1.2.8.	Network "Offline" Mode to Support Your Field Employees 5
	1.2.9. Device	Enforced Encryption - protecting sensitive data in transit / Trusted 6
	1.2.10.	Client Uninstall Protection
	1.2.11.	Client Stop Protection / Tamper Protection
•	1.2.12.	Backup Scheduler
1.3.	Contr	olled Device Types / Ports7
1.4.	Concl	usions9
2.Se	erver	Functionality / Server Components 10
2.1.	Endpo	pint Protector – Web Service11
2.2.	Admir	nistration and Reporting Tool11
2.3.	Acces	sing the Administration and Reporting Tool
2.4.	Login	Credentials (Username and Password)15
2.5.	Gener	al Dashboard15
2.6.	Syste	m Status16
2.7.	Live L	Jpdate17
3.En	dpoi	nt Management19
	-	es
3.2.	Devic	e Functionality20
	3.2.1.	Give / Deny Access to Devices 21
	3.2.2.	Enable Device Read-Only Access
	3.2.3.	TrustedDevice Level 1 to Level 4

3	3.2.4. WiFi - Block if wired network is present	23
3.3.	Computers	24
3.4.	Groups	25
3.5.	Users	
3.6.	Custom Classes	
3.7.	Terminal Servers and Thin Clients	
3	3.7.1. Initial Configuration	31
4.En	dpoint Rights	34
4.1.	Device Rights	
4.2.	User Rights	
4.3.	Computer Rights	
4.4.	Group Rights	
4.5.	Global Rights	
4.6.	Effective Rights	40
4.7.	File Whitelist	40
5.Off	fline Temporary Password	42
	Generating the Offline Temporary Password	
5.2.	Using the Offline Temporary Password to authorize a de	evice 44
5.3.	Setting the Administrator Contact Information	
6.En	dpoint Settings	45
	Computer Settings	
6.2.	Group Settings	
6.3.	Global Settings	
6.4.	Custom Client Notifications	
6.5.	File Tracing	
6.6.	File Shadowing	50
7.Co	ntent Aware Protection	51
7.1.	Activation of Content Aware Protection	52
7.2.	Content Aware Policies	53
7	7.2.1. Creating new policies	54
7	7.2.2. Predefined policies	55

7.2.3. Priorities for Content Aware Policies
7.2.4. How Content Aware Policies Work
7.2.5. Setting up Content Aware Policies
7.2.6. The Threshold Number
7.3. File Size Threshold63
7.4. Custom Content Dictionary Blacklists
7.5. Custom Content Filename Blacklists
7.6. Content Aware URL Whitelists65
7.7. Content Aware File Whitelists66
7.8. Content Aware Domain Whitelists67
7.9. Network Share Whitelists
7.10. Content Aware Regex Blacklists
7.11.Content Aware Type Whitelist
7.12. Content Aware File Location Whitelist
7.13. Content Aware File Location Blacklist
7.14.How Content Aware Protection works for monitored Applications / Online Services
7.15. HIPAA compliant Content Aware Protection
7.15.1. How Endpoint Protector is HIPAA compliant
7.15.2. Use Case Nr. 1
7.15.3. Use Case Nr. 2
8. Reports and Analysis
8.1. Logs Report78
8.2. File Tracing79
8.3. File Shadowing80
8.4. Content Aware Report81
8.5. Content Aware File Shadowing82
8.6. Admin Actions83
8.7. Online Computers
8.8. Online Users
8.9. Online Devices
8.10. Computer History

8.11.User History	
8.12. Device History	89
8.13. Statistics	90
9.Alerts	91
9.1. Define System Alerts	
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
10. Directory Services	. 102
10.1.Active Directory Import	
10.2. Active Directory Sync	105
11. Appliance	. 109
11.1.Server Information	
11.2.Server Maintenance	110
11.2.1. Time Zone Settings	110
11.2.2. Network Settings	
11.2.3. Reset Appliance to Factory Default	
11.2.4. SSH Server 11.3.SIEM Integration	
12. System Maintenance	
12.1. File Maintenance	
12.2.System Snapshots	
12.3.Log Backup	
12.3.1. Backup Scheduler (Automatic Log Backup) 12.4.Content Aware Log Backup	
12.4.Content Aware Log Backup	
12.4.1. Automatic Scheduler (Automatic CAP Log Backup) 12.5.Audit Log Backup	

12.5.1. Audit Log Backup Scheduler122
12.6. External Storage 123
12.6.1. FTP Server123
12.6.2. Samba / Network Share124
12.6.3. From the Web Interface125
12.6.4. From the Console128
13. System Configuration
13.1.Client Software 130
13.2. Client Software Upgrade 131
13.3. Client Uninstall 132
13.4. System Administrators 133
13.5.System Departments135
13.6.System Security / Client Uninstall Protection
13.7.System Security138
13.8.System Settings 139
13.8.1. Rights Functionality139
13.8.2. Proxy Settings139
13.9.System Licensing 140
13.9.1. Appetizer Mode142
13.9.2. Trial Mode143
13.9.3. Import Licenses143
14. System Parameters 146
14.1. Device Types 146
14.2.Rights148
14.3. Events
14.4. File Types 150
15. Setting up Policies 151
16. Modes for Users, Computers and Groups153
16.1.Transparent Mode
16.2. Stealth Mode154
16.3. Panic Mode154

16.4. Hidden Icon Mode 1	L55
16.5. Silent Mode 1	L55
15.6.Adding new administrator(s)1	156
16.7. Working with logs and reports1	158

# 17. Enforced Encryption with Trusted Devices 159

17.1. Managing Trusted Devices from Endpoint Protector
17.2. Trusted Device Level 1 and Enforced Encryption with EasyLock161
17.2.1. Deploying EasyLock
<b>18. Endpoint Protector Client165</b> 18.1.Endpoint Protector Client Installation165
18.2. Endpoint Protector Client Security 166
18.3. Client Notifications (Notifier) 167
18.4. Client Policy Update167
18.5. Offline Functionality for Endpoint Protector Client
18.6.DHCP / Manual IP address168
18.7.Client Removal168
18.7.1. Client Removal on Windows OS168
18.7.2. Client removal on MAC OS X168
18.7.3. Client removal on Linux OS168
19. Installing Root Certificates to your Internet
Browser
20. Terms and Definitions
20.1.Server Related
20.2. Client Related
21. Support 183

# 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.

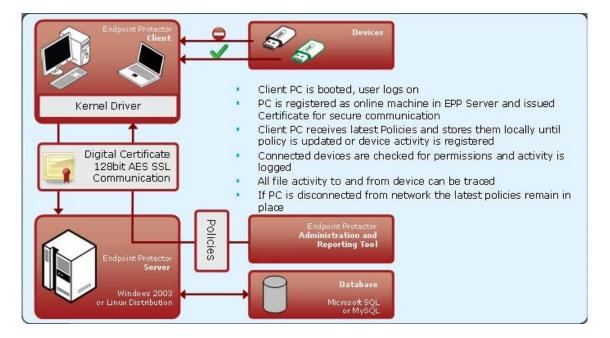
As a complete Data Loss Prevention solution, Endpoint Protector not only controls all device activity at endpoints, but monitors and scans all possible exit points for sensitive content detection. Its second module, Content Aware Protection, ensures that no critical business data leaves the internal 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.

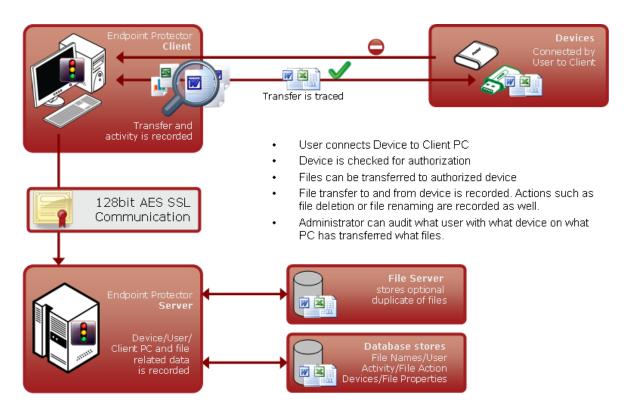
## 1.2.1. Centralized web based Device Management / Dashboard

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.

#### 5 | Endpoint Protector | User Manual



## 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

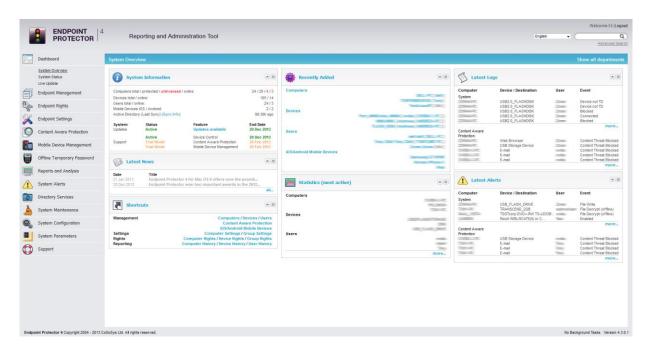
The Web Service of Endpoint Protector is responsible for the communication between Endpoint Protector Server and the Client computers. Starting with the registration of the client computers, the Web Service sends the settings and rights of each computer and also receives the log information from each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



**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.

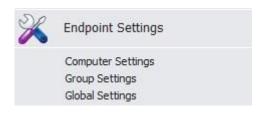
**Endpoint Rights** – Used to determine and define rules of access. Six subsections are found here Devices Rights, User Rights, Computers Rights, Group Rights, Global Rights, Effective Rights and File Whitelist.

#### 13 | Endpoint Protector | User Manual



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.

#### 14 | Endpoint Protector | User Manual



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 Alerts
Define System Alerts Alerts History

**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: <u>https://127.0.0.1/index.php</u>.

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

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.

	<b>ENDPOINT</b> <b>PROTECTOR</b> 4	Reporting	and Administration Too						English 👻		Re   Logout
	Dashboard	Endpoint Protector - D	ashboard GENERAL							Show all dep	artments
	<u>General Dashboard</u> System Overview System Status	Endpoints and Mobi	ile Devices		Most	Active Users (# of con	nnected devices)		General		Î
í	Live Update Endpoint Management	2	2			6			Status Updates	Active	Featur No upc Device
3	Endpoint Rights		1 1 1			2			Support	Trial Mode	Conter Mobile
$\frac{\times}{2}$	Endpoint Settings								Active Directory	(Last Sync): ement CAP Policier	N/A
0	Content Aware Protection (CAP)	Windows M	acs Linux iOS Androi	1							
	Mobile Device Management	•			m						Þ
	Offline Temporary Password	Most Active Users (	# of transfers blocked)		Passo	ode Protected Mobile	Devices		Latest News		
	Reports and Analysis	14							18 Nov 2013		E
	Alerts		3			2			Endpoint Protector releases support f Endpoint Protector is now ready for OS X their network prevent data losses and data		r OS X
Ø	Directory Services	67% No passode					u are u				
	Appliance						- ore official ages		Check all news		
۵	System Maintenance	_				-					
0	System Configuration	٠ [									Þ
Ħ	System Parameters Device Control Logs Device Control Alerts CAP Logs CAP Alerts MDM Profile Removed Devices MDM Devices not connected for long time										
0	Support	Event name	Client Computer	IP Address	Domain Name	Client User	Device Type	Device	Date/Time		
		Device not TD	To a second s				USB Storage Device	DataTraveler 2.0	2013-12-09 13:	41:28	
		Blocked				_	USB Storage Device	DataTraveler 2.0	2013-12-09 13:		
		Connected					USB Storage Device	DataTraveler 2.0	2013-12-09 13:		
		Disconnected					USB Storage Device	DataTraveler 2.0	2013-12-09 13:		
		Device not TD					USB Storage Device	DataTraveler 2.0	2013-12-09 13:		
		Blocked					USB Storage Device USB Storage Device	DataTraveler 2.0 DataTraveler 2.0	2013-12-09 13: 2013-12-09 13:		-
	pint Protector 4 Copyright 2004 - 2013 Co						USD Storage Device	Data HaVeler 2.0		38:36 dv Version 4.4.0.2	

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

ive Update Settings		
Check Automatically for Updates:	0	
Check Manually for Updates:	۲	
the second states and the second	ch night the current curters status to our Live	
*Note: Endpoint Protector Server will report ea	ch hight the current system status to our live	Update Serv
Enable Automatic Report:		Update Serv
*Note: Endpoint Protector Server will report ea Enable Automatic Report: Disable Automatic Report:	-	Update Serv

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

		Welcome Super Administrator   Logout		
PROTECTOR	* Reporting and Administration Tool	English  C Advanced Sea		
Dashboard	Endpoint Protector Server - Live Update	Show all department		
System Overview System Status Live Update	Important Notice			
Endpoint Management	Endpoint Protector is required to connect now over HTTPS to www.endpointprotector.com to receive information. If you do not	gree with an Internet connection, you can choose not to proceed.		
Endpoint Rights	Software Update			
Endpoint Settings				
Content Aware Protection	Most recent check for updates:         24 Feb 2013 14:25:01           Updates were installed:         06 Feb 2013 15:45:01			
Mobile Device Management	Configure Live Update Check Now Offline Patch Uploader			
Offline Temporary Password	Available Updates			
Reports and Analysis				
System Alerts	No updates available!			
Directory Services	View Applied Updates			
Appliance				
System Maintenance				
System Configuration				
System Parameters				
Support				
adpoint Protector 4 Copyright 2004 - 2013	CoSoSys I Id. All rights reserved	Ready Version 4.3.0.3 - Applia		

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 <a href="mailto:support@endpointprotector.com">support@endpointprotector.com</a> 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.

8	<b>ENDPOINT</b> 4 <b>PROTECTOR</b> 4	Re	porting a	and Administration Too	I		English 👻	Adva	nced
Da	ashboard	List of	Devices						
En	ndpoint Management	Filter							T
	ashboard	Resul	ts						
Co	evices omputers sers	All	Status TD	Device Type	Device Name (Identification)	Description	Department	Last Location	La
	oups			Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	Default Department		
Ou	ustom Classes			Internal CD or DVD RW	MATSHITA DVD-RAM UJ8C2 S ATA Device	MATSHITA DVD-RAM UJ8C2 S ATA Device / (S	Default Department		100
En	ndpoint Rights			Webcam	USB2.0 HD UVC WebCam	USB2.0 HD UVC WebCam / Chicony Electroni	Default Department		1000
	lupoine regnes		-	WFi	Microsoft Virtual WiFi Miniport Adapter	Microsoft Virtual WiFi Miniport Adapter	Default Department		100
En	ndpoint Settings		-	WFi	Atheros AR9485WB-EG Wireless Network Ada	Atheros AR9485WB-EG Wireless Network Ada	Default Department		1000
				Additional Keyboard	HID Keyboard Device	HD Keyboard Device / (Standard keyboard	Default Department		
Co	ontent Aware Protection		-	Additional Keyboard	PC/AT Enhanced PS/2 Keyboard (101/102-Ke	PC/AT Enhanced PS/2 Keyboard (101/102-Ke	Default Department		1000
	-		0	USB Storage Device	DATATRAVELER_3.0	DATATRAVELER_3.0 / KINGSTON	Default Department		1000
				USB Storage Device	USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	Default Department		
M	obile Device Management		-	USB Storage Device	VOYAGER LS	VOYAGER LS/CORSAIR	Default Department		
			-	USB Storage Device	2307_PRAM	2307_PRAM / Kingston Technology Company	Default Department		
Of	ffline Temporary Password			Local Printers	Canon MP210 series	Canon MP210 series /	Default Department	ACCOUNT OF ALL	1000
				Local Printers	HP LaserJet P1005, 1.6.0	HP LaserJet P1005, 1.6.0 /	Default Department	ALCONO DE L	10000
Re	eports and Analysis			Bluetooth	Bluetooth Device	Bluetooth Device / Broadcom	Default Department	ACCOUNT OF ALL	1000
Al	erts			WFi	Wireless Network Adapter (802.11 a/b/g/n	Wireless Network Adapter (802.11 a/b/g/n	Default Department	Martin Martin	10001
				Local Printers	Remote Printer	Remote Printer /	Default Department	The state of the s	1000
Di	rectory Services			Local Printers	Remote Printer	Remote Printer /	Default Department	The state of the second second	10001
				Local Printers	Remote Printer	Remote Printer /	Default Department	The state of the s	1000
Ap	ppliance		-	Serial ATA Controller	Standard SATA AHCI Controller	Standard SATA AHCI Controller / Intel Co	Default Department		
				USB Storage Device	V0YAGER_VEGA	VOYAGER_VEGA / CORSAIR	Default Department		1000
Sy	/stem Maintenance		-	Parallel Port (LPT)	Printer Port (LPT1)	Printer Port (LPT1) / (Standard port typ	Default Department	-	-
SV	stem Configuration			Serial Port	Communications Port (COM1)	Communications Port (COM1) / (Standard p	Default Department	-	-
3	uton conngaration			Internal CD or DVD RW	HL-DT-ST DVDRAM GH24NSC0	HL-DT-ST DVDRAM GH24NSC0 / (Standard CD	Default Department	-	-
Su	stem Parameters			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.

 $\blacksquare$  Red means that the device is blocked in the system.

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

Vellow 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"

Already Existing	Devices	
Ð		
Save	▲ Back	

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.

Last devices connected	Search		Rights	
Name	Serial Number	Last Location		
Communications Port	TRACE PROPERTY	100001CT	Deny Access	
ASUS DRW-2014S1 ATA	Transferrer (Compared)		and the second sec	
(Standard floppy dis	HEC-1 22475-0 0	CONTRACTOR OF THE OWNER O	C Allow Access	
Standard AHCI 1.0 Se	1041-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1	1.	Read Only Acce	SS
Intel(R) Active Mana	TRUM Store - Award		O Allow Access if	TD Level 1
USB_FLASH_DRIVE		and the second sec	Allow Access if	
USB_FLASH_DRIVE		and the second se		SANTA MARK
FM-10_PRO	000000000000000000000000000000000000000	and the second se	C Allow Access if	TD Level 3
Select All] [Remove Sele	ection]		C Allow Access if	TD Level 4
			Block if wired ne present	twork is
			Save	Cancel

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

Last devices connected	Search		Rights	
Name	Serial Number	Last Location		
Communications Port	TRANSIT PARTS 1	COMPARENT.	Deny Access	
ASUS DRW-2014S1 ATA	Second Se			
(Standard floppy dis		and the second se	Allow Access	
Standard AHCI 1.0 Se			Read Only Acce	ess
Intel(R) Active Mana	TROM COT	and the second sec	O Allow Access if	TD Level 1
USB_FLASH_DRIVE			Allow Access if	
USB_FLASH_DRIVE				
FM-10_PRO		and the second s	C Allow Access if	TD Level 3
[Select All] [Remove Sele	ction]		C Allow Access if	TD Level 4
			Block if wired ne present	etwork is
			Parameters:	t
			Save	Cancel

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.

Already Existing Devices				
USB_FLASH_DRIVE	-	Allow Access	Standard	<u>*8</u>
$\oplus$				

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

For more information on TrustedDevices<sup>™</sup> and EasyLock<sup>™</sup>, 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.

	ENDPOINT 4 PROTECTOR													4	Advanced Si
	Dashboard	List of Computers													
	Endpoint Management	Filter													
	Dashboard Devices	Results													
	Computers Users	Computer Name	IP	Department	Workgroup		Domain	Mac Address	Default User	Location	Last Time Online 👻	Version	License	Modified at	Modified
	Groups	101-10802-0540	192.168.0.125	Default Department	tony/00-21-5D-27-	4A-DE-1000	intern.cososys.com	00-21-5D-27-4A-DE			07-May-2015 13:42		Offline		
	Custom Classes	Tre-Linkson Could	81.196.156.53	Default Department			intern.cososys.com	00-21-5D-27-4A-DE	May .		07-May-2015 13:42	1.0.5.1 - (Linux)	Offline		
3	Endpoint Rights	1244207744077555078	K 192.168.0.199	Default Department	WORKGROUP			e0-3f-49-33-38-f6	Web:		07-May-2015 13:38	4.4.2.4 - (PC)	Offline		
-	Lindpoint rugino	100000000000000000000000000000000000000	81.196.156.53	Default Department			intern.cososys.com	00-0C-29-C6-41-06	distance.		06-May-2015 21:39	1.0.4.1 - (Linux)	Offline		
	Endpoint Settings	BACHNERT	81.196.156.53	Default Department	WORKGROUP			c8-2a-14-0f-8b-92	May		29-Apr-2015 19:44	1.4.3.1 - (Macintosh)	Offline	29-Apr-2015 14:57:40	root
		844.001		Default Department			ad4cososys.com						Unlicensed		
)	Content Aware Protection (CAP)	R44.000		Default Department			ad4cososys.com						Unlicensed		
	Mobile Device Management	1000jillte:		Default Department			ad4cososys.com						Unlicensed		
	Offline Temporary Password	esults [ 20 💌 pe	er page]				m								
	Reports and Analysis	Creat	e	ØV Đ	rport	8	Delete	<b>≜</b> B	ack						
	Alerts														
	Directory Services														
	Appliance														
	System Maintenance														
	System Configuration														
	System Parameters														
	Support														

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:

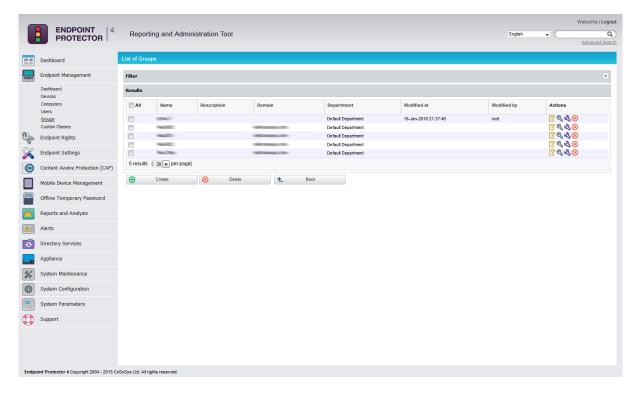


Edit, Manage Rights, Manage Settings, Offline Temporary Password, Computer History, Export Computer History and Delete. The Manage Rights, Manage Settings, Offline Temporary Password and Computer History are links to their respective modules, which will be explained in their own chapter.

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.



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".

ENDF PROT	OINT   4 ECTOR   Reporting and Administra	ation Tool	Welcome Super Administrator   Log English C Advanced Sea
Dashboard	Add a New Group		Show all departmen
Endpoint Manage Devices Computers Users Groups Endpoint Rights Chapoint Setting		C050615.PC	
Content Aware F		Q Search G Check all matched	terre
Offline Tempora		Al  Name Domain  Check all matched i  Check all mat	
System Alerts	Users in this Group		
Directory Service	S Users:	Coductions	
System Maintena	ince		
System Configur	ation	CoSoSys	
System Paramet	ers		
Support		Q Search All Name Doman C Check all matched	tems
Endpoint Protector 4 Cop	rright 2004 - 2013 CoSoSys Ltd. All rights reserved.		Ready Version 4.3.0.3 - Applia

# 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.

		List of U	eore										_	Advanced Se
	Dashboard	LISCOLO	5015											
	Endpoint Management	Filter												
	Dashboard Devices	Results												
	Computers Users	E All	Username	Domain	First Name	Last Name	Last Computer	Department	Phone	E-mail	Modified at	Modified by	Groups	Actions
	Groups		Intellor:		Viewicz	Totals:	144420744075550914	Default Department	1155440770	and the second second second	CONTRACTOR OF CONTRACTOR			29.00
	Custom Classes		NAME:		Real CO.			Default Department					ABROAT ABROAT	
n	Endpoint Rights		TENGLET 1	100000000000000000000000000000000000000	- Resolution			Default Department					- RESERVED 1	
, P	Endpoint Settings		Real I			CORE I	The states of the	Default Department						79.848
	Endpoint Settings		NOTE:			10000000	1.4.2.1.2.2.1.7.4.6.7.0.1	Default Department	17426-	Concession of the local division of the loca	Contraction of the local distance	- mailer		
	Content Aware Protection (CAP)		185355	Telesconder (Contra		18535-	1000-1-100000-0-54400	Default Department						ZQEWX
	Mobile Device Management		againes i		10000000 I		175-43803-75481 (assocration)	Default Department Default Department	104-029-022	-sime management		1980:		◩९≡∞⊗ ◪९≡∞⊗
	Offline Temporary Password	9 resu	llts [ 50 💌	per page]										
-														
	Reports and Analysis	Ð	Create	Ģ	Ð	port	🛞 Delet	•	8	ack				
	Reports and Analysis Alerts	Ð	Create	ģ	Ð	cport	Delet	•	B	ack				
-		<b>⊕</b>	Create	Q	Ð	rport	8 Delet	•	_ 8	ack				
-	Alerts	Ð	Create	Ó	Ð	rport	😣 Delet	•	<u> </u>	ack				
	Alerts Directory Services		Create		Ð	cport	😣 Delet	•	_ B	ack				
	Alerts Directory Services Appliance	Ð	Create	•	d B	cport	🛛 🛞 Detet		_ B	ack				
	Alerts Directory Services Appliance System Maintenance	Ð	Create	ē	j Đ	sport	8 Delet	•	_ 8	ack				
	Alerts Directory Services Appliance System Maintenance System Configuration		Create	Ø	Ð	port	Contraction Contraction		_ 8	ack				
	Alerts Directory Services Appliance System Maintenance System Configuration System Parameters	•	Create	٥	j D	port	S Delet		_ 8	ack				

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.

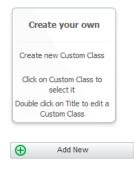
The users can be arranged in groups for easier management at a later point. Users can also be imported into Endpoint Protector from Active Directory through the Active Directory Plug-in.

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 add	ing devices to the Custom Class.
Name:	
Description:	
Rights:	Deny Access 🗸
Save Save	

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

• Add new device – will open a pop-ul, 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					$\times$
USB Storage Device	Vendor ID	Product ID	Serial Number	Description	Ð
Save Save	S Cancel				

 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.

I Device Types Vame				ndor ID	Product ID	Serial Number	C
All	Name	Vendor ID	Product ID	Serial Num	ber	Last Location	
]	HID Keyboard Device	2101	20f	HID-VID_210	1&PID_020F&REV_0	CRISTIB	
]	HID Keyboard Device	0	0	HID-MLIT_HI	D&Col01/HID_DEVIC	CRISTIB	
]	Communications Port (COM1)	0	0	COM_ACPI_F	NP0501_1_1VR32D!	CRISTIB	
]	HL-DT-ST DVDRAM GH24NSB0	0	0	CDROM&VEN	_HL-	CRISTIB	
]	STORAGE_MEDIA	54c	9c2	5C071058DF	9B156A86	CRISTIB	
]	HID Keyboard Device	2101	20f	HID-VID_210	18PID_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.

Add new devices ba	ase on Serial Number	Range			(	×
USB Storage Device	Vendor ID	Product ID	first Serial Number in the range	last Serial Number in the range	Description	
Save Save	S Cancel					

#### 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.

Bulk add devices	×
Choose device type:	USB Storage Device 🗸
Choose bulk enrollment option:	Paste device list      Import device list
Paste device list	
Maximum 500 devices at once. For futher information please of	heck the .xls sample.
Example: 5ac, 5b9, BB4001110130000001, STORAGE_MEDIA' 125f; db19; 13118154214600BB; USB_FLASH_DRIVE'	
Save Save Cancel	

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

	ENDPOINT PROTECTOR	Repo	rting and Admini	stratior	n Tool								English	Welcome   Logout
	Dashboard	Edit Custor	n Class											Show all departments
	Endpoint Management	Custom Cl	ass Description											
	Dashboard	Note: Ple	ase provide and save the	Name and	Description before ad	ding devices to the	Custom Class.							
	Devices Computers	Name:				Custom Class								
	Users Groups	Description	12			Example								
	Custom Classes	Rights:				Allow Access			~					
00	Endpoint Rights	0	Save											
X	Endpoint Settings	Add devic	es to Custom Class											
	Content Aware Protection (CAP)	Ð	Add new device	*	Add existing device	• 🕀 A	idd Serial Number range	1	Bulk add devices					
8	EasyLock Enforced Encryption													
	Mobile Device Management	Device Filt	ers											<u> </u>
	Offline Temporary Password	Device Typ Vendor ID					~							
	Reports and Analysis	Product ID												
		Serial Num												
	Alerts	Serial Num												
Ø	Directory Services	Serial Num Description												
	Appliance	0	Reset	Q	Apply filter									
*	System Maintenance	Device Lis												
	System Configuration		t Device Type		Vendor ID	Product ID	Serial Number			umber Start	Serial Number End			Actions
	System Parameters								Senal	umber start	Serial Number End	Description		
_			Additional Keyboard USB Storage Device		0 1251	0 cb19	HID-MLIT_HID&Co 13118154214600					HID Keyboard Device/(Standard keyboards) USB_FLASH_DRIVE'		8
$\bigcirc$	Support		USB Storage Device		5ec	569	BB400111013000					STORAGE_MEDIA'		8
			[ 50 - per page]											
		8	Delete											
		0	Delete											
Endp	oint Protector 4 Copyright 2004 - 2016 Col	SoSys Ltd. Al	rights reserved.											Ready Version 4.5.0.1

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.

m Classes						Show all departm
om Classes						Switch to list v
Test Class #1	Test Class #2	Test Class #3	Test Class #4	Create your own		
Test.	This is a test.	This is also a t	Yet again.	Create new Custom Class		
Allow Access Device Type/D	Allow Access Device Type	Allow Access if Device Class	Block WiFi if wi Device Type	Click on Custom Class to select it		
On	On	On	On	Double click on Title to edit a Custom Class		
				Custom Class		
Add New	Edit	Delete				
Add New	Edit	🛞 Delete				
	Edit	Delete		Custom Class		
ustom Classes	Edit	S Delete				
Add New ustom Classes	Edit	© Delete			Right	Action
ustom Classes	Edit				Right Alow Access	22
ustom Classes	Edit	Description				

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 vill be displayed for ease of identification, as seen below:

	Dashboard	List of 0	Computors														
	Endpoint Management	Filter															
8	Endpoint Rights	Result	•														
6	Endpoint Settings		Computer Name	IP	Department	Workgroup	Domain	Mac Address	Users	Last Time Online +	Version	License	Modified at	Modified by	Groups	Terminal Server	Actions
)	Content Aware Protection (CAP)	0	Contraction of the local division of the loc	192.168.0.89	Default Department			00-0c-29-75-33-ft	-	08-May-2015 14:12	4.4.2.4 - (PC)	Licensed					2930
	Scanning Data At Rest		-	192.165.0.149	Defout Department			00-25-90-45-50-32		08-May-2015 14:12	4.4.2.4 - (PC)	Lkensed	27-Apr-2015 17:12:56	root		~	<u> 240</u>
1	Mobile Device Management								more (6)								
		8	CONTRACTOR .	192.168.0.109	Default Department		NAME AND ADDRESS OF TAXABLE PARTY.	00-01-29-00-27-00	Resident.	08-May-2015 14:12	4.4.2.4 - (PC)	Lkensed.					3930
	Offline Temporary Password		CONTRACTOR OF STREET,	192.168.0.112	Default Department	WORKGROUP		40-6c-8f-56-89-87	1000	08-Mey-2015 10:20	1.4.3.4 - (Macintosh)	Offline	24-Apr-2015 15:19:58	root			3930
ï		0	Contraction of the local division of the loc	192.168.56.1	Default Department			08-00-27-00-1c-ac		07-May-2015 18:34	4.4.2.8 - (PC)	Offine	29-Apr-2015 18:22:14				3930
L	Reports and Analysis			169.254.157.11	Default Department	WORKGROUP		02-20-6c-f2-09-01	and the second s	07-May-2015 16:18	4.4.2.6 - (PC)	Offine	24-Apr-2015 15:19:58	root			2930
1	Alerts		COLUMN TO .	192.168.0.195	Default Department	WORKGROUP		00-1a-4d-43-ec-d8		06-May-2015 11:09	4.4.2.9 - (PC)	Offine	D4-May-2015 17:03:14	root			349
	Directory Services	8	and the second	192.168.0.33	Default Department		Records Con-	00-e0-4c-11-3b-10	noUser RD\$1	05-May-2015 19:05	4.4.2.9 - (PC)	Office	05-May-2015 17:55:35	root		~	<u> 8</u> 440 <u>0</u> 00
2			19980	192.168.230.1	Default Department	WORKGROUP		00-50-56-¢0-00-01	Concession in which the Party number of the Pa	04-May-2015 10:07	4.4.2.6 - (PC)	Office	30-Apr-2015 12:18:18	root			2940
P	Appliance	8	Carlos Contractor	192.168.0.147	Default Department	WORKGROUP		08-60-6e-75-02-9f	PROFESSION NO.	30-Apr-2015 18:30	4.4.2.8 - (PC)	Offine	30-Apr-2015 18:27:01	root			2930
ŝ		10	Const Constant of the	192.168.0.127	Default Department		And in case of the local division of the	00-0c-29-ac-68-b2	ALC: NO.	29-Apr-2015 18:55	4.4.0.6 - (PC)	Offline					39333
l	System Maintenance		CONTRACTOR OF STREET,	192,168.0.69	Default Department	WORKGROUP		00-0c-29-72-70-8b	10000	27-Apr-2015 17:39	4.4.2.6 - (PC)	Offline					2930
ï	2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 / 2 /	8	Street, Square, 750.	192.168.0.63	Default Department	WORKGROUP		b8-e8-56-3a-b3-ft	PROFESSION.	27-Apr-2015 14:19	1.4.3.0 - (Macintosh)	Offine	24-Apr-2015 15:19:58	root			2930000
J	System Configuration		Contraction of the local division of the loc	192.168.0.63	Default Department	WORKGROUP		58-55-ca-et-46-a1	840	17-Apr-2015 14:16	1.4.3.2 - (Mecintosh)	Office	24-Apr-2015 15:19:59	root			2940.
	Client Software		The second s	192.168.0.63	Default Department	WORKGROUP		c8-28-14-0f-8b-92	100 C	16-Apr-2015 15:55	1.4.3.2 - (Macintosh)	Offine	24-Apr-2015 15:19:58	foot			2940
	Client Software Upgrade		Contraction in the	192,168.0.140	Default Department	WORKGROUP		6c-40-05-89-65-ca	2980	16-Apr-2015 15:04	1.4.3.2 - (Macintosh)	Offine	24-Apr-2015 15:19:58	root			2930
	Client Uninstall	0	and the second sec	192.168.0.205	Default Department		and the second s	bc-ae-c5-69-d2-2d	and the second s	15-Apr-2015 18:01	4.3.1.4 - (PC)	Offine	24-Apr-2015 15:19:58	root		~	2930000
	Download EasyLock Software		CONTRACTOR OF STREET, STRE	192.168.0.63	Default Department	WORKGROUP		6c-40-08-8f-b1-4a	and the second s	11-Apr-2015 20:13	1.4.2.2 - (Mecintosh)	Offline	24-Apr-2015 15:19:58	root			2940000
	System Administrators	8	Contract Name	169.254.78.203	Default Department	WORKGROUP		02-20-6c-12-09-02	And and a second	08-Apr-2015 15:26		Unicensed	24-Apr-2015 15:19:59	root		~	2930
	System Departments System Security	8	California Company	10.0.2.15	Default Department	WORKGROUP		08-00-27-6e-5b-95	and the second division of	06-Apr-2015 16:14	4.3.1.4 - (PC)	Offine	24-Apr-2015 15:19:58	root	Test Group		2930000
	System Policies System Settings	41 re	sults [ 20 🔹 per pa	9e]													H 4 123 >
	System Licensing	æ	Create	GW	Export	8	Delete	Back									
a'	System Parameters				actival i			0011									

#### 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

An Allow Access right set to the RDP Storage device type will enable all users that connect to the Terminal Server by RDP to transfer files to and from their local disk volume or shared storage devices such as USBs.

By contrast, a Deny Access right set to the RDP Storage will not allow any user that connects to the Terminal Server by RDP to transfer files to and from their local disk volume or shared storage devices such as USBs.

#### Note!

The option to Use User Rights must be checked in the settings bar from System Configuration > System Settings > Endpoint Rights Functionality for the rights policy to apply on user logins with user priority.

Secondly, the menu from Endpoint Rights > User Rights will present an additional device type for all the Users in Endpoint Protector, namely Thin Client Storage (RDP Storage).

ENDPO PROTE		Reporting and Administration Tool			English
Dashboard	ń	Edit User Rights			
Endpoint Managen	ment	User Name:	noUser		
Endpoint Rights		First Name:	No user No User		
Device Rights User Rights		Device Types (To view all supported devices and rig	hts, go to Device Types in System Param	eters)	
Computer Rights Group Rights		Unknown Device	Preserve global setting 💌	WiFi	Preserve global setting 💌
Global Rights		USB Storage Device	Preserve global setting	Bluetooth	Preserve global setting 💌
Effective Rights File Whitelist		Internal CD or DVD RW	Preserve global setting 💌	FireWire Bus	Preserve global setting 👻
Endpoint Settings		Internal Card Reader	Preserve global setting 💌	Serial Port	Preserve global setting 👻
Endpoint Settings		Internal Floppy Drive	Preserve global setting 💌	PCMCIA Device	Preserve global setting 💌
Content Aware Pro	otection =	Local Printers	Preserve global setting 💌	Card Reader Device (MTD)	Preserve global setting 💌
		Windows Portable Device (Media Transfer Protocol)	Preserve global setting 💌	Card Reader Device (SCSI)	Preserve global setting
Mobile Device Mar	nagement	Digital Camera	Preserve global setting 💌	ZIP Drive	Preserve global setting
		BlackBerry	Preserve global setting	Teensy Board	Preserve global setting
Offline Temporary	Password	Mobile Phones (Sony Ericsson, etc.)	Preserve global setting	Thunderbolt	Preserve global setting 💌
Reports and Analy	/sis	SmartPhone (USB Sync)	Preserve global setting	Network Share	Preserve global setting 💌
Alerts		SmartPhone (Windows CE)	Preserve global setting	Infrared Dongle	Preserve global setting 💌
Alerts		SmartPhone (Symbian)	Preserve global setting	Parallel Port (LPT)	Preserve global setting 💌
Directory Services	;	Webcam	Preserve global setting	Thin Client Storage (RDP Storage)	Allow Access 💌
Appliance		iPhone	Preserve global setting 💌	Additional Keyboard	Preserve global setting 💌
		iPad	Preserve global setting 💌	USB Modem	Preserve global setting 💌
System Maintenan	nce	iPod	Preserve global setting 💌	Android Smartphone (Media Transfer Protocol)	Preserve global setting 💌
System Configurat	tion	Serial ATA Controller	Preserve global setting		

Multiple users can be recognized as active users on any given Terminal Server, and so, this rights setting can be used as a powerful tool to create access policies to specific users, as detailed in the use case below.

	192.168.0.149	Default Department		Administrator	14-May-2015 18:21	4.4.2.9 - (PC)	Licensed 13-May-2015 17:43:06 roc	t ThinGroup 🗸	◪९⋞◙◾◼■∞⊗
100000-022	192.168.0.19	Default Department		08-00-27-00-94-36		4424-(PC)	Offline		7 4 4 🗉 🖬 🖉 🐼
10001-94221	111.33.33.12	Default Department	WORKGROUP	00-19-66-dd-6d-0f	Users for this Terminal T3-May-2015 16:48	4.4.2.9 - (PC)	Unlicensed 13-May-2015 16:49:26 roc	11 🗸	🔁 🔍 💐 🗊 📰 🗏 🛯 😣

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

Offline Device Authorization	?	x
Offline Device Authorization - TSVR2012		
Select Device		
<ul> <li>(Standard keyboards) / HID Keyboard Devic</li> <li>(Standard port types) / Communications Port</li> <li>(Standard port types) / Communicatintypes</li> <li>(Standard port types) / Communicatintypes&lt;</li></ul>	t (COM t (COM t (COM (F)	2)
Code for Administrator: C000		
Password:		
Enter		
To authorize a device contact your admir Contact info:	nistrat	or.
Last server connection at:	112	65
Endpoint Protector Version		

# 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.

E	Dashboard	Management of Rights p	er Devices			Show	/ all department
]	Endpoint Management	Filter					
P	Endpoint Rights	Device Name:					
	Device Rights	Device Type:	USB Storage Device				
	User Rights	VID:					
	Computer Rights Group Rights	PID:					
	Global Rights Effective Rights	Serial Number:					
2	File Whitelist Endpoint Settings	<b>O</b> Reset	Q Apply filter				
	Enupoint Settings						
	Offline Temporary Password	Results					
	Reports and Analysis	Device Name +	Device Description	Device Type	VID PID	Serial Number	Actions
		USB_SD_READER	USB_SD_READER / GENERIC	USB Storage Device	-		Ľ
2	System Alerts	USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device	1000		Ľ
	Directory Services	USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device	1000		Z
		USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device	-	Contraction of the local diversion of the local diversion of the local diversion of the local diversion of the	Z
	System Maintenance	USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device	1001		2
		USB_FLASH_DRIVE	USB_FLASH_DRIVE / ADATA	USB Storage Device	1000		Z
	System Configuration	Port_#0004.Hub_#0004	Port_#0004.Hub_#0004 / Ironkey Inc.	USB Storage Device	1000	Contraction of the	B
ar I		FREEAGENT	FREEAGENT / SEAGATE	USB Storage Device	1000	Contraction of the local diversion of the local diversion of the local diversion of the local diversion of the	e
	System Parameters	DISK	DISK / EASY	USB Storage Device	1000 10000		Z
		9 results [ 50 🖵 per p	agel				

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

0

"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.

						Welcome Su	per Administrator   Logout
1	PROTECTOR	Reporting and Admir	nistration Tool			English 💌	Q Advanced Search
_		54					<u></u>
	Dashboard	Edit Device Rights				s	how all departments
Í	Endpoint Management						
00	Endpoint Rights	△ Currently the system is u	ising both computer and	user rights, comput	er rights have priority		
	Device Rights User Rights	Device					
	Computer Rights Group Rights	Device Name:	the states of				
	Global Rights	Device Description:					
	Effective Rights File Whitelist	Last User:					
X	Endpoint Settings	Groups					
	Offline Temporary Password	•					
	Reports and Analysis	Computers					
	System Alerts	NAME OF TAXABLE PARTY.		- Allow Access	- Standard	*8	
0	Directory Services	Ð					
	System Maintenance	Users					
0	System Configuration			- Allow Access	- Standard	*8	
Ħ	System Parameters	⊕ Save ▲Back					
0	Support						
Endpo	pint Protector Copyright 2004 - 2011 Co	SoSys Ltd. All rights reserved.					Ready Version 4.0.0.8

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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool			English	Welcome   Logou
	Dashboard	Edit User Rights				
	Endpoint Management	${\color{black} \Delta}$ Currently the system is using both computer and user	r rights, computer rights l	nave priority.		
Cho	Endpoint Rights					
	Device Rights	User				
	User Rights Computer Rights	User Name:				
	Group Rights	First Name:				
	Global Rights	Last Name:				
	Effective Rights File Whitelist	Device Types (To view all supported devices and rights, go to Device	Types in System Parameters	)		
X	Endpoint Settings	Unknown Device	Preserve global setting 💌	Serial ATA Controller		Preserve global setting 💌
0	Content Aware Protection (CAP)	USB Storage Device	Allow Access	WiFi		Preserve global setting 💌
	Mobile Device Management	Internal CD or DVD RW	Preserve global setting 💌	Bluetooth		Preserve global setting 💌
	mobile bevice management	Internal Card Reader	Preserve global setting 💌	FireWire Bus		Preserve global setting 💌
	Offline Temporary Password	Internal Floppy Drive	Preserve global setting 💌	Serial Port		Preserve global setting 👻
M	Reports and Analysis	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
Δ	Alerts	Digital Camera	Preserve global setting	Card Reader Device (SCSI)		Preserve global setting 💌
0	Directory Services	BlackBerry	Preserve global setting 💌	ZIP Drive		Preserve global setting 💌
	Appliance	Mobile Phones (Sony Ericsson, etc.)	Preserve global setting	Teensy Board		Preserve global setting 💌
		SmartPhone (USB Sync)	Preserve global setting	Thunderbolt		Preserve global setting 💌
X	System Maintenance	SmartPhone (Windows CE)	Preserve global setting	Network Share		Preserve global setting 💌
Ø	System Configuration	SmartPhone (Symbian)	Preserve global setting 💌	Infrared Dongle		Preserve global setting 💌
		Webcam	Preserve global setting	Parallel Port (LPT)		Preserve global setting 💌
	System Parameters	iPhone	Preserve global setting	Additional Keyboard		Preserve global setting 💌
	Support	iPad	Preserve global setting 💌	USB Modem		Preserve global setting 💌
		iPod	Preserve global setting			
		Already Existing Devices				
		<b>⊕</b>				
			★ Back			
		Save Save	▲ Back			
Endpo	pint Protector 4 Copyright 2004 - 2014 Cos	SoSys Ltd. All rights reserved.				Ready Version 4.4.0.

## 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 • Q Advanced Search
	Dashboard	Edit Computer Rights		
	Endpoint Management	$\triangle$ Currently the system is using both computer and us	or rights, computer rights have priority	
200	Endpoint Rights	Currently the system is using both comparer and as	er rights, compater rights have providy.	
9	Device Rights	Computer		
	User Rights	Computer Name:		
	Computer Rights Group Rights	Location:		
	Global Rights Effective Rights	Device Types (To view all supported devices and rights, go to Devi	e Types in System Parameters)	
50	File Whitelist	Unknown Device	Preserve global setting   Serial ATA Controller	Preserve global setting
×	Endpoint Settings	USB Storage Device	Allow Access ViFi	Preserve global setting 💌
	Content Aware Protection (CAP)	Internal CD or DVD RW	Preserve global setting  Bluetooth	Preserve global setting
	Mobile Device Management	Internal Card Reader	Preserve global setting V FireWire Bus	Preserve global setting
	Hobie Device Management	Internal Floppy Drive	Preserve global setting  Serial Port	Preserve global setting
88	Offline Temporary Password	Local Printers	Preserve global setting  PCMCIA Device	Preserve global setting
	Reports and Analysis	Windows Portable Device (Media Transfer Protocol)	Preserve global setting Card Reader Device (MTD)	Preserve global setting 💌
	Alaska	Digital Camera	Preserve global setting  Card Reader Device (SCSI)	Preserve global setting 💌
	Alerts	BlackBerry	Preserve global setting 💌 ZIP Drive	Preserve global setting 💌
0	Directory Services	Mobile Phones (Sony Ericsson, etc.)	Preserve global setting 💌 Teensy Board	Preserve global setting 💌
	Appliance	SmartPhone (USB Sync)	Preserve global setting 💌 Thunderbolt	Preserve global setting 💌
		SmartPhone (Windows CE)	Preserve global setting  Network Share	Preserve global setting 💌
×	System Maintenance	SmartPhone (Symbian)	Preserve global setting 💌 Infrared Dongle	Preserve global setting
Ø	System Configuration	Webcam	Preserve global setting  Parallel Port (LPT)	Preserve global setting 💌
	Custom Demonstration	Phone	Preserve global setting 💌 Additional Keyboard	Preserve global setting
	System Parameters	iPad	Preserve global setting 💌 USB Modern	Preserve global setting
$\bigcirc$	Support	iPod	Preserve global setting 💌	
		Already Existing Devices		
		•		
		Save Save	1_ Back	
Endpo	int Protector 4 Copyright 2004 - 2014 Cos	SoSys 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.

Dashboard	Management of Rights per Groups		Show all departme
Endpoint Management	Filter		
Endpoint Rights	Results		
Device Rights User Rights	Name 🔺	Description	Actions
Computer Rights Group Rights			Z
Global Rights	1.12.00 September	Contraction of the second s	2
Effective Rights		Contraction of Contraction of Contraction of Contraction	B
File Whitelist			2
Endpoint Settings	Training and the second s	The second second second second second second second	Z
	Contract Advantage	Contraction and provide the second second second	R
Offline Temporary Password	100000000000000	Construction and the second part of the	ľ
	Contract Contractor	- All the of the second second second	2
Reports and Analysis	Trans Courses	- 1100 to 10 control	Z
System Alerts	100mmm10104mmm	- A Statement of Control of Contr	2
System Alerts		The support of the strength of the support	Z
Directory Services	States - Content - Content	Contraction of the second s	Z
	The other committees	Contraction of the Contraction o	2
System Maintenance		Contraction Contraction of the Second State	Z
			Ľ
System Configuration			Z
System Parameters	Contraction of Contraction		Z
System Furdineters	Contraction (Contraction)	The second we are as a first second second	2
Support			Z
	and the second	Contraction of the second s	2
	22 results [ 20 💌 per page]		H 4 12 F H

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.

	Dashboard	Management of Global Rights					
	Endpoint Management	$\triangle$ Currently the system is using both computer a	user rights, computer	r righte	have priority		
6	Endpoint Rights	een en	io osci rigito, compute				
a	Device Rights	Groups					
	User Rights	Name:	Global				
	Computer Rights Group Rights	hand	Global Group including all the ma	chines			
	Global Rights	Device Types (To view all supported devices and rights, go to	Device Types in System Pa	rameters	5)		
	File Whitelist						
R	Endpoint Settings	Unknown Device	Deny Access	-	Serial ATA Controller	Deny Access	•
	Content Aware Protection (CAP)	USB Storage Device	Allow Access	•	WiFi	Allow Access	•
9	Content Aware Protection (CAP)	Internal CD or DVD RW	Deny Access	-	Bluetooth	Allow Access	•
	Mobile Device Management	Internal Card Reader	Deny Access	•	FireWire Bus	Deny Access	-
	Offline Temporary Password	Internal Floppy Drive	Deny Access	-	Serial Port	Deny Access	-
5	onine remporary resortere	Local Printers	Deny Access	-	PCMCIA Device	Deny Access	-
٦	Reports and Analysis	Windows Portable Device (Media Transfer Protocol)	Deny Access	•	Card Reader Device (MTD)	Deny Access	•
	Alerts	Digital Camera	Deny Access	-	Card Reader Device (SCSI)	Deny Access	•
		BlackBerry	Deny Access	-	ZIP Drive	Deny Access	
•	Directory Services	Mobile Phones (Sony Ericsson, etc.)	Deny Access	•	Teensy Board	Deny Access	-
	Appliance	SmartPhone (USB Sync)	Deny Access	-	Thunderbolt	Deny Access	-
		SmartPhone (Windows CE)	Deny Access	-	Network Share	Allow Access	
5	System Maintenance	SmartPhone (Symbian)	Deny Access	•	Infrared Dongle	Deny Access	•
X	System Configuration	Webcam	Deny Access	-	Parallel Port (LPT)	Deny Access	-
	System Parameters	Phone	Deny Access		Additional Keyboard	Deny Access	•
5	System Parameters	iPad	Deny Access	•	USB Modem	Deny Access	V
	Support	Pod	Deny Access	-			
		Already Existing Devices					
		Ð					
		Save 🔁 Back					

## 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.

•	ENDPOINT PROTECTOR 4	Reporting and Administration Tool							English 🗸	Welcome   I
	lashboard	Effective Rights								
9	indpoint Management	$\triangle$ Currently the system is using both co	mputer and user rights, c	omputer rights h	ave priority.					
	indpoint Rights	Effective Rigths Filter								
	Nevice Rights Iser Rights	Effective Rights for:	Device Control	~						
	Computer Rights Group Rights	Select right:	N/A	~						
ł	llobal Rights ffective Rights	Select a computer:	CRISTIB	~						
	ile Whitelist	Select a user:	N/A	~						
	indpoint Settings	Select a device type:	N/A	*						
0	Content Aware Protection (CAP)	Select a device:	N/A	*						
E	asyLock Enforced Encryption	👌 Reset Q Appl	/ filter							
1	Nobile Device Management									
(	Offline Temporary Password	Results								
F	leports and Analysis	A The rights are displayed from lower to high	hest priority and they are in	a raw form.						
	leports and Analysis	A The rights are displayed from lower to hig	hest priority and they are in	a raw form.	Device	Right	Using File Whitelist	Observation	Defined 0	n
,			hest priority and they are in	a raw form.	Device		-	Observation Inherited from Global Policies	Defined O Global	n
,	Jerts hirectory Services	Device Type Unknown Device	hest priority and they are in	a raw form.	Device	Deny Access	Using File Whitelist No			n
,	Jerts	Device Type Unknown Device USB Storage Device	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No No	Inherited from Global Policies Inherited from Global Policies	Global Global	n
/ (	Jerts Nirectory Services	Device Type Uninown Device USB Storage Device Diglat Camera	hest priority and they are in	a raw form.	Device	Deny Access Deny Access Deny Access	No No No	Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies	Global Global Global	8
/	Jerts hirectory Services	Device Type Unknown Device USB Storage Device Digital Camera SmatPhone USB Sync)	hest priority and they are in	a raw form.	Device	Deny Access Deny Access Deny Access Deny Access Deny Access	No No No No	Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies	Global Global Global Global	n
	Jerts irrectory Services ppliance lystem Maintenance	Device Type Uninown Device UBS Storage Device Digital Camera Smart/Phone (USB Sync) Smart/Phone (VidB sync)	hest priority and they are in	a raw form.	Device	Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access	No No No	Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies	Global Global Global	n
	Jerts Nirectory Services	Device Type Unisown Device Utili Storage Device Digital Camera Simethone (VidDews CE) Simethone (VidDews CE) Benefhone (VidDews CE)	hest priority and they are in	a raw form.	Device	Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access	No No No No No No	Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies Inherited from Global Policies	Giobal Giobal Giobal Giobal Giobal Giobal	n
/ c / s	Jerts Jirectory Services ppliance lystem Maintenance lystem Configuration	Device Type Unitation Device Utilit Storage Device Digital Camere Smerthhere (Utilit Styre) Smerthhere (Utilities) ES Smerthhere (Utilities) ES Smerthhere (Utilities) ES Smerthhere (Syntas) Mermal Carel Steader	hest priority and they are in .	a raw form.	Device	Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access	No No No No No No No	Inherted from Global Policies Inherted from Global Policies	Giobai Giobai Giobai Giobai Giobai Giobai	8
/ c / s	Jerts irrectory Services ppliance lystem Maintenance	Device Type USB Strange Device USB Strange Device Digital Careira Smarthrous (OSB Struct) Smarthrous (Struct) Smarthrous (Struct) Smarthrous (Struct) Smarthrous (Struct) Interal (Care Stadar) Fotos (Care Stadar)	hest priority and they are in .	a raw form.	Device	Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access Deny Access	No No No No No No No No	Inherted from Global Polices Inherted from Global Polices	Global Global Global Global Global Global Global	0
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type Dence Type USB Strange Dence Diptic Canno Smarthhee (USB Stric) Smarthhee (USB Stric) Smarthhee (USB Stric) Smarthhee (USB Stric) Franket Cannot Stranger PCICICA Dence PCICICA Dence	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No	Interfed from Global Policies Interfed from Global Policies	Giobal Giobal Giobal Giobal Giobal Giobal Giobal Giobal	n
	Jerts Jirectory Services ppliance lystem Maintenance lystem Configuration	Dense Type Utilitativa Dense Utilitä Tanapas Dense Digilar Canad Samerhona (1988 Samo) Disarthona (1996 Samo) Disarthona (1996 Samo) Heland Carl Rakat Heland Carl Rakat Pravilita Bus Zarlona	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No No No No No No No No	Interfact from Global Policies Interfact from Global Policies	Cicked Cicked Cicked Cicked Cicked Cicked Cicked Cicked Cicked Cicked Cicked Cicked	n
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type USB Dences Type USB Dences Office Dearthore (USB Strict) Standthore (USB Strict) Standthore (USB Strict) Standthore (USB Strict) Standthore (USB Strict) Facility Covers Facility Covers Facility Covers Textilet Bas ZP Drive Internet Car Dev Drive	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	Ne Ne No No No No No No No No	Interted from Cickal Pilotes Interted from Cickal Pilotes	Global Global Global Global Global Global Global Global Global Global	2
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dense Type Utilitations Dence Utilit Storage Dence Digital Carent Searthow (SISB Sync) Searthow (SISB Sync) Searth	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No No No No No No No No No No No No	Inherited from Oblad Photos Inherited from Oblad Photos	Global Global Global Global Global Global Global Global Global Global Global	9
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type Utilitizens Dence Utilitizens Dence Utilitizens Dence Utilitizens Denerfhene (Utilitizen Denerfhene Denerfitizen Den	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	-           No	Interfet from Diala Pholos Interfet from Diala Pholos	Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies Cilcies	8
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type Utilitations Device Utilitätions Device Digidi Carrier Snarthoue (Utilitätion) Snarthoue (Utilitätion) S	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No No No No No No No No No No No No No	whetler from Oakal Nuices Inhetler from Oakal Nuices	Global Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal Oliceal	n 
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type USB Dence Type USB Dence Type USB Dence Type	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	Image: Control of the second secon	Interfet from Diala Plaices Interfet from Diala Plaices	Classi Cl	n
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type Util Statework Device Util Statework Device Diglia Charma Smarthnea (Util Struc) Smarthnea (Util Struc) Smarthnea (Util Struc) Smarthnea (Util Struc) Smarthnea (Util Struc) Denteman (Hargo Toto I Prinrikh Pan Herman (Grup Oto Ref Leaf Reader Device (Util Struc) Carl Reader Device (Util Struc) Carl Reader Device (Util Struc) Wolkewa Refabb Christen (Util Struc)	hest priority and they are in	a raw form.	Device	Deny Access Deny Access	No No No No No No No No No No No No No N	whetlet from Diale Noices Inhetlet from Calcel Noices Inhetlet from Calcel Noices Inhetlet from Calcel Noices Inhetlet from Diale Noices	Global Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal Otlobal	n
	lerts irrectory Services ppliance ystem Maintenance ystem Configuration ystem Parameters	Dence Type USB Dence Type USB Dence Type USB Dence Type	hest priority and they are in	a row form.	Device	Deny Access Deny Access	Image: Control of the second secon	Interfet from Diala Pholos Interfet from Diala Pholos	Classi Cl	n

# 4.7. File Whitelist

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

							Advanced Searc
Dashboard	File Whi	nitelist				Show	v all departments
Endpoint Manag	ement Folder o	containing Whitelist files					
Endpoint Rights	Folder	ei	c:/TempWeb		- T		
Device Rights User Rights Computer Rights Group Rights Global Rights	Only file:		ll be saved in the Whitelist. d Files				
Effective Rights File Whitelist	Status	s Filename	File Path		File Extension	Last Modified	Size
Endpoint Setting	s 🔽	Report 10 Studenter		Construction and a second	doc	1 June 2011 16:13:25 EEST	38.5 kB
Offline Tempora	F Pacquord	1-10-10-10-10-10-10-10-10-10-10-10-10-10	C. T. Reconstruction of the	State Transfer	log	2 June 2011 16:12:16 EEST	12.02 MB
Online rempora		Contraction of the local division of the loc			log	1 June 2011 10:52:25 EEST	0 B
Reports and Ana					test	1 June 2011 09:30:14 EEST	8 B
System Alerts		s found [Check All Unch	eck All ]				
Directory Service	Sav	ave					
System Mainten	ance						
System Configur	ation						
System Paramet	ers						
Support							

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.

File Whitelist		Show all departments
Folder containing W	hitelist files	
Folder	c:/TempWeb	
Only files selected fo	r hashing will be saved in the Whitelist.	
Stresh Refresh	Upload Files	

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

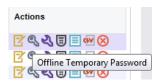
Depending on the options selected from the drop-down menus, the Offline Temporary Password (or OTP) can be generated for the exact device or computer needed.

	ENDPOINT PROTECTOR	Reporting and Administration Tool						English	C	Welcome   Log C
	Dashboard	Offline Temporary Password								
	Endpoint Management	Offline Temporary Password								
8	Endpoint Rights	Offline Temporary Password for:	Device	*						
6	Endpoint Settings	Duration:	30 min	~						
	Content Aware Protection (CAP)	Choose computer:	N/A	*						
	EasyLock Enforced Encryption	Enter device code(case sensitive) or search for device:		* \$						
1	Mobile Device Management	Justification:	Mention the reason why you	are creating the OTP						
	Offline Temporary Password									
_	Offline Temporary Password Reports and Analysis	Generate OTP code								
	Alerts									
	Directory Services									
	Appliance									
:	System Maintenance									
:	System Configuration									
] :	System Parameters									
) :	Support									
dpoir	t Protector 4 Copyright 2004 - 2016 Co	SoSys Ltd. All rights reserved.								Ready Version 4

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  $\stackrel{\times}{\sim}$ .

For additional verification, the administrator can check the authenticity of a given device code by using the "Refresh Device Codes" option  $\clubsuit$ . 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).

Offline Device Authorization	×								
ENDPOINT PROTECTOR									
Offline Device Authorization - Cr Select Device	istiB								
<ul> <li>Standard keyboards) / HID Keyboard Device</li> <li>Standard keyboards) / HID Keyboard Device</li> <li>Standard port types) / Communications Port (COM1)</li> <li>SONY / STORAGE_MEDIA</li> <li>(Standard CD-ROM drives) / HL-DT-ST DVDRAM GH24NSB0 SCSI Cd</li> </ul>									
•	•								
Code for Administrator: C695									
Password:									
En	ter								
To authorize a device contact yo Contact info:	ur administrator. +123123 aaa@bbb.ccc								
Last server connection at:	12-Aug-2016 13:50:48								
Endpoint Protector Client Versior	1: 4.5.8.0								

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.

Phone:	+(40)0740000001	
E-mail:	Administrator@example.com	
*Note: This contact info	formation is referring to Offline Temporary Password only! For Alerts, you must setup	o the e-mail address from System Administrators > Edit info

# 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.

Sestore Group/Global Settings

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.

Bestboard Edit Settings for Computer	
Endpoint Management Computer	
Logic Endpoint Rights Default User: -	
knowit Settings Pr Mc. Adverse	
Computer Settloga Computer Name: ARREIP-VIN10	
Grady Settings Loator: Geb/ Settings	
Caten Cent Itelfactors Hode	
Context Avere Protection (CAP) Refer hitraria (ac): 0	
EaryLack Enforced Encryption Mode: Normal 🗸	
Mobile Device Management Retracting and Shadowing	
Offine Temporary Password Piet Textrac	
Reports and Analysis Pile Stadowing: Z Al Z Removable Devices and Officer ① Z Content Aware Protection Z Evail Body ①	
After         Database for Stadowij ()         Aday           Adder Statewise for Stadowij ()         Aday         Aday	
O prectory Services	
Applica Chart Setting	
System Maintenance         Logithmid (mit):         30         Localing Size (MI):         30           System Maintenance         System Maintenance         System Maintenance         System Maintenance         Status	
System Configuration Men His Ease for Studioung (92); 0 Max-Ris Ease for Studioung (92); 512	
System Parameters         Remember Devices Recomp Fielder Nationaum Size (ME)         2000         Recomp Fielder Releases (Med)         3         0           Institute Language         Papale         Papale         O         Accomp Fielder Releases (Med)         3         0	
Institut Longage:	
Loging	
Created at: 25-34-4306 506739 Created by: AMD Created by: AMD	
Modified by: rest	
🔗 Save 🕐 Instance Conceptibilited Safetysa	
	adv 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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool							English Welcome   Logost
	Dashboard	Management of Global Settings							
-	Endpoint Management	Group							
20	Endpoint Rights	Name:	Global						
×	Endpoint Settings	Description:	Gooal Group in	nduding all the machines					
	Computer Settings	Mode							
	Group Settings Global Settings	Refresh Interval (sec):	0						
	Custom Client Notifications	Mode:	Normal	~					
۲	Content Aware Protection (CAP)	File Tracing and Shadowing							
	EasyLock Enforced Encryption	File Tracing:	🗹 Al	Removable Devices	esata HDD	Network Share			
	Mobile Device Management	File Shadowing:		Removable Devices and Other	Content Aware Protection	E-mail Body			
	Offline Temporary Password	Exclude Extensions from Shadowing: 🕜	.fsdgh;						
88	Omine Temporary Password	Exclude Extensions from CAP Scanning: 🕐	.gdsfg;						
<u>~</u>	Reports and Analysis								
	Alerts	Default Client Settings							
6	Directory Services	Log Interval (min):	30		Local Log Size (MB):		10		
-	A sublement	Shadow Interval (min):	60		Shadow Size (MB):		512		
_	Appliance	Min File Size for Shadowing (KB):	0		Max File Size for Shadowir		512		
*	System Maintenance	Removable Devices Recovery Folder Maximum Size (MB):	5000	0	Recovery Folder Retentio		3	0	
٢	System Configuration	Notifier Language: Enable Advanced Printer and MTP Scanning	English		Use Custom Client Notifica	tions for this Language:			
	System Parameters	-							
$\overline{\mathbf{O}}$	Support	Logging							
•	Subbour	Created at:	30-34-2007 20	0:07:02					
		Created by: Modified at:	root 12-Aug-2016 0	38-54-08					
		Modified by:	root						
		Save 👌 Restore default Se	tings 🛍	Back					
Endp	aint Protector 4 Copyright 2004 - 2016 Col	SoSys Ltd. All rights reserved.							Ready Version 4.4.1.0

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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool								English 🗸	Welcome   Logout
	Dashboard	Management of Global Settings									
	Endpoint Management	Group									
20	Endpoint Rights	Name:	Global								
×	Endpoint Settings	Description:	Gooal Group	including all the machines							
	Computer Settings	Mode									
	Group Settings Global Settings	Refresh Interval (sec):	0								
	Custom Client Notifications	Mode:	Normal	>							
0	Content Aware Protection (CAP)	File Tracing and Shadowing									
	EasyLock Enforced Encryption	File Tracing:	🗹 Al	Removable Devices		esata HDD	Network Share				
	Mobile Device Management	File Shadowing:	🗹 Al	Removable Devices and Other	0	Content Aware Protection	E-mail Body 🕜				
	Offline Temporary Password	Exclude Extensions from Shadowing: ⑦ Exclude Extensions from CAP Scanning: ⑦	.fsdgh; .qdsfq;								
	Reports and Analysis	Exclude Extensions from CAP Scanning:	.gdsfg;								
	Alerts	Default Client Settings									
_		Log Interval (min):	30			Local Log Size (MB):		10			
Ø	Directory Services	Shadow Interval (min):	60			Shadow Size (MB):		512			
	Appliance	Min File Size for Shadowing (KB):	0			Max File Size for Shadowin	g (43):	512			
*	System Maintenance	Removable Devices Recovery Folder Maximum Size (MB):	5000	0		Recovery Folder Retention	n Period (days):	3	0		
	System Configuration	Notifier Language:	English	~ 🕐		Use Custom Client Notifica	tions for this Language:				
		Enable Advanced Printer and MTP Scanning									
-	System Parameters	Logging									
	Support	Created at:	30-Jul-2007	20:07:02							
		Created by:	root								
		Modified at:	12-Aug-201	5 OB: 56:OB							
		Modified by:	root								
		Save 👌 Restore default Se	tings	Back							
Endpo	int Protector 4 Copyright 2004 - 2016 Co	SoSys Ltd. All rights reserved.									Ready Version 4.4.1.0

## 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.

8	ENDPOINT 4 PROTECTOR	Reporting and Administration Tool						English		
										Advance
1	Dashboard	Custom Client Software Notifications Languag	0							
6	Endpoint Management	Device Types (To view all supported devices and	ights, go to Device Types in Syster	n Parameters)						
6	Endpoint Rights	All								
	Endpoint Settings	Bluetooth Radio				Pod				
	Computer Settings	Unknown Device				Serial ATA Controller				
	Group Settings	USB Storage Device				WE				
	Global Settings	Bluetooth Smartphone				Bluetooth				
9	Custom Client Notifications	Bluetooth Tablet				FireWire Bus				
) (	Content Aware Protection (CAP)	Internal CD or DVD RW				Serial Port				
		Bluetooth Keyboard				PCMCIA Device				
E	EasyLock Enforced Encryption	Internal Card Reader				Card Reader Device (MTD)				
1,	Mobile Device Management	Bluetooth Mouse				Card Reader Device (SCSI)				
	House Perice Humpgement	Internal Floppy Drive				ZIP Drive				
(	Offline Temporary Password	Local Printers				Teensy Board				
		Windows Portable Device (Media Transfer Protocol)				Thunderbolt				
۰ ۱	Reports and Analysis	Digital Camera				Network Share				
	Alerts	BlackBerry				Infrared Dongle				
		Mobile Phones (Sony Ericsson, etc.)				Parallel Port (LPT)				
1	Directory Services	SmartPhone (USB Sync)				Thin Client Storage (RDP Storage)				
		SmartPhone (Windows CE)				Additional Keyboard				
• 1	Appliance	SmartPhone (Symbian)				US8 Modem				
1	System Maintenance	Webcam				Android Smartphone (Media Transfe	r Protocol)			
9		Phone				Chip Card Device				
1	System Configuration	Pad								
	System Parameters	Results								
•	Support	Name	Code	Customized Token	•		Enabled Tokens	Actio	ns	
		English	en	9			9			
		French	fr	0.5			0			
		German	de	0			0			
		Romanian	ro	0			0			
		Polish	pl	0			0			
		Japanese	ja	0			0			
		Hungarian	hu	0			0			
		Korean	ko	0			0			

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!"

All	Original	Customized
	- · · goun-	
	Security Warning	Message from Endpoint Protector
<ul> <li>(Body)</li> </ul>	An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.	This device is not allowed!
(Title)	Panic Mode	
Body	) 961 entered the panic mode. Your devices have been blocked.	
(Title)	Security Warning	
Body	) The print screen functionality is disabled.	
(Title)	Restart needed	
(Body	%1 detected that you need to restart your system for the latest device rights to be applied.	
(Title)	Security Warning	
(Hole)		
(Title)	Endpoint Protector - TrustedDevice enabled Endpoint Protector - TrustedDevice enabled	
	- Liupoir Proeta - Huseberre eleber	
(Title)	Trial Information	
(Body	961 is expired	
(Title)	Trial Information	
Body	) You are currently using a 30 day trial version. It will expire in %1 %2	
(Title)	Content Threat Detected	
Body	File transfer %1. You attempted to copy sensitive information. Contact the PCs administrator for more information. Text: '%2' was matched in file '%3' as '%4'	
(Body	File transfer %1. You attempted to copy sensitive information. Contact the PCs administrator for more information. Text: %2" was matched in file %62" as %94"	

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 and Shadowing					
File Tracing:		Removable Devices		esata HDD	Network Share
File Shadowing:		Removable Devices and Other	0	Content Aware Protection	🗹 E-mail Body 🕜
Exclude Extensions from Shadowing: ⑦	.fsdgh;				
Exclude Extensions from CAP Scanning: 🕜	.gdsfg;				

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:		Removable Devices		esata HDD	Network Share
File Shadowing:		Removable Devices and Other	0	Content Aware Protection	🗹 E-mail Body 🕜
Exclude Extensions from Shadowing: ⑦	.fsdgh;				
Exclude Extensions from CAP Scanning: 🕜	.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):	30	Local Log Size (MB):	10	
Shadow Interval (min):	60	Shadow Size (MB):	512	
Min File Size for Shadowing (KB):	0	Max File Size for Shadowing (KB):	512	
Removable Devices Recovery Folder Maximum Size (MB):	5000 ⑦	Recovery Folder Retention Period (days):	3	0
Notifier Language:	English 🔻 🕜	Use Custom Client Notifications for this Language:		
Enable Advanced Printer and MTP Scanning				

#### 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:

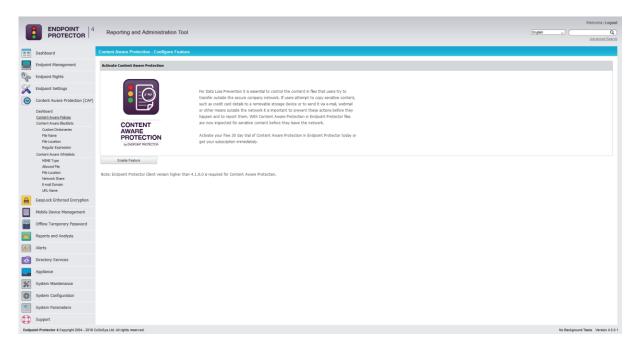
- Personally Identifiable Information (PII): social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.
- Financial and credit card information: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Dinners 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 requires a simple activation by pressing the *Enable Feature* button and providing contact details for the Main Administrator.



#### 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, Email, 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.

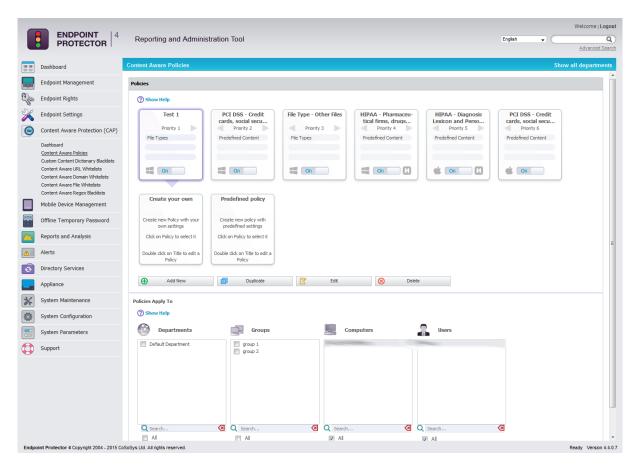
#### Note!

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.



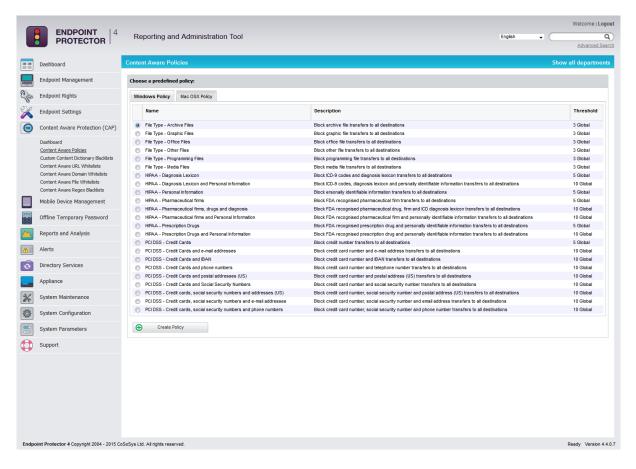
The available actions are: **Add New**, **Duplicate**, **Edit** and **Delete**. A new policy can be created also by clicking on the **Create your own** policy icon. An existing policy can be edited also by double-clicking the upper part of the policy icon.

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".



### 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	REPORTED	Information will be reported.
IGNORED	REPORTED	REPORTED	Information will be reported.
REPORTED	REPORTED	REPORTED	Information will be reported.
IGNORED	IGNORED	BLOCKED	Information will be blocked.
IGNORED	BLOCKED	BLOCKED	Information will be blocked.
BLOCKED	BLOCKED	BLOCKED	Information will be blocked.
IGNORED	REPORTED	BLOCKED	Information will be reported.
IGNORED	BLOCKED	REPORTED	Information will be blocked.

REPORTED	IGNORED	BLOCKED	Information will be reported.
BLOCKED	IGNORED	REPORTED	Information will be blocked.
REPORTED	BLOCKED	IGNORED	Information will be reported.
BLOCKED	REPORTED	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.

ENDPOINT PROTECTOR	4 Reporting and Administration Tool						English Jadvanc
Dashboard	Add a new Policy						Show all depart
Endpoint Management	Policy OS Type						
Endpoint Rights	OS Type:	Windows	🗰 Омесоях 💧 Ош	ux			
Endpoint Settings	Policy Information						
Content Aware Protection	Policy Name						
Dashboard	Policy Description:						
Content Aware Policies	Policy Action:	Report only	Block & Report				
Content Aware Bladdists		-	-				
Custom Dictionaries	Policy Status:		Disabled (OFF)				
File Name	Client Notifications:	Show notifications (	Hide notifications				
File Location	Threshold Value:	1		0			
Regular Expression	Threshold Type:	Regular	⊖ Global	0			
Content Aware Whitelists MDME Type	File Size Threshold:			0			
Allowed File File Location	Control Transfers To						
Network Share	Applications 🕐 🔽 Storage Devices 🕐 🔽 Net						
		work share 🔍 💆 Thin Clier	its 🔍 🛛 Cipboard 🔍 🖸				
E-mail Domain							
E-mail Domain URL Name	Web Browser @ E-mail C	0	Instant Messaging 🕐	Cloud Services / File	Sharing 🕐 Social Media / Othe	rs 🕐	
	Web Browser ② E-mail ③	ok (Attachments 🔺	Instant Messaging ⑦	_	EasyLock     Windows DVD Maker	^	
URL Name	Web Browser  E-mail  E-mail  Control Internet Explorer Modia Prefox Modia Prefox Modia Prefox Modia Prefox Modia	ak (Attachments  A ak (Body) Thunderbird Thunderbird	<ul> <li>✓ ICQ</li> <li>✓ AIM</li> <li>✓ Skype</li> <li>✓ Windows Live Messeng</li> </ul>	Cloud Services / File	EasyLook     Windows DVD Maker     ALFTP     PHeZila	^	
URL Name EasyLock Enforced Encryptio	Web Browser         E-mail           In         Chimret Explorer         A         Colds           IV         Chimret Explorer         A         Colds           IV         Chimret Explorer         A         Colds           IV         Modia Frefox         Modia         Modia           IV         Safari         C         BHL         BHL           IV         ALA Desktop 9.6         III BHL         IIII         IIII	ak (Attachments A ak (Body) 9 Thunderbird 9 Thunderbir	ICQ AIM Skype Windows Live Messeng Yahoo! Messenger Gem	Cloud Services / File Google Drive Clent Cloud Drive Clent Cloud Drive Uforrent Difformet Dawn Cloud Xitt Otleh uCloud	EasyLock     Windows DVD Maker     ALFTP     FileZila     GoToMeeting     HTC Sync for Androi	<b>A</b>	
URL Name EasyLock Enforced Encryptio Mobile Device Management	Web Browser         E mail 0           Different Explorer         O Onto           Of Transe         O Onto           Different Explorer         Model           Different Explorer         Word           Different         Word           Different         Word           Different         Word           Different         Word           Different         Word	sk (Body) Thunderbird Thunder	ICQ     ICQ     AIM     Skype     Windows Live Messeng     Yshool Messenger     Gaim     HanbiroTalk     Pilgin     Trillium	Cloud Services / File	EasyLock     Windows DVD Maker     ALFTP     FileZill     GoToMeeting     HirtCSync for Androi     Infrailecorder CD - D     Tures     Loctebla Bin	d	
URL Name EasyLock Enforced Encryptio Mobile Device Management Offline Temporary Password	Web Browser         E-mail           If zerrer Explorer         A         Oxfor           If Zerrer Explorer         A         Oxfor           If Zerrer Explorer         A         Oxfor           If Zerrer Explorer         Mosfor         Mosfor           If Zerrer Explorer         Mosfor         Mosfor           If Zerrer Explorer         Mosfor         Mosfor           If Zerrer Explorer         If Mosfor         Mosfor           If Zerrer Explorer         If Mosfor         If Mosfor	sk (Body) Thunderbird Thunder	<ul> <li>✓ ICQ</li> <li>✓ AM</li> <li>✓ Skype</li> <li>✓ Windows Live Messeng</li> <li>✓ Yahool Messenger</li> <li>✓ Gaim</li> <li>✓ HanbiroTalk</li> <li>✓ Pidgin</li> </ul>	Cloud Services / File Google Drive Clent Cloud Drive Cloud Drive Daum Cloud Daum Cloud Noret Drive Never N Drive Never N Drive	EasyLock     Windows DVD Maker     ALFTP     FileZila     GoToMeeting     HTC Sinc for Androi     InfraRecorder CD - D     Tures     Trunes	<b>A</b>	
URI Name EasyLock Enforced Encryptio Mobile Device Management Offline Temporary Password Reports and Analysis	Web Browser O         E mail O           Diment Explorer         A           Diment Explorer         B           Diment Explorer         A           Diment Explorer         B           Diment Explorer         C           Diment Explorer         <	sk (Body) Thunderbird Thunder	ICQ     ICQ     Skype     Skype     Vindows Live Messeng     Vinhol Messenger     Gaim     HenbiroTalk     P Highin     C. Triflien     Q Search	Cloud Services / File Cloud Services / File Cloud Drive Cloud Drive	EasyLook     Windows DVD Naker     Wind	d	
URL Name EasyLock Enforced Encryptio Mobile Device Management Offline Temporary Password Reports and Analysis Alerts	Web Browner O         E mail O           Dement Explorer         A           Policy Context         A	A (Attachments A & (Body) Thundeford thundeford thun Pieter (Att thun Pieter (Att	ICQ     ADM	Coud Services / He Coud Dee Dee Clerk Coud Dree Urrent Dear Coet Dear Coet Dear Coet Dear Coet	Eleptod     Eleptod     AUT     Eleptod     AUT     Elevtod     AUT     Elevtod     AUT     Elevtod     Elevt	d	
UR: Name EasyLock Enforced Encryptio Mobile Device Management Offline Temporary Password Reports and Analysis Alerts Directory Services	Web Browser O         E mail O           Diment Explorer         A           Diment Explorer         B           Diment Explorer         A           Diment Explorer         B           Diment Explorer         C           Diment Explorer         <	A (Attachments A & (Body) Thundeford thundeford thun Pieter (Att thun Pieter (Att	ICQ     ADM	Cloud Services / File Cloud Services / File Cloud Drive Cloud Drive	EasyLook     Windows DVD Naker     Wind	d	
UR: Name EasyLock Enforced Encryptio Mobile Device Management Offline Temporary Password Reports and Analysis Alerts Directory Services Appliance	Web Browser         E mail ①           Starret Explorer         C offset           O transmer         D offset           O core         O offset           O offset         D offset           O offset         D offset           O offset         D offset           O offset         D offset	A (AttaCherneth A k (Gody) Thrundebrid thrundebrid than Nater (Att than Nater (Att than Nater (Att the Nater (Att .	You Conception of the second sec	Coud Services / File Coud Cher Coud Cher Cher Coud Cher Coud Cher Coud Cher	A Use and a set of the set o	4	
UR: Iteme Eanytock Enforced Encryptio Mobile Device Management Offline Temporary Password Alerts Directory Services System Maintenance System Configuration	Web Browser         E and C           Description         C and C	A (Statubents A global) 15 Durchorted 15 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 17 Durchorted 17 Durchorted 17 Durchorted 18 Durchorted 18 Durchorted 18 Durchorted 19	CO	Could Service / File Could Service / File Could Device / Could Device / Device / Cells / Cells / Could Could / Could /	Constant Constan	4 G	
URL Iteme EasyLock Inforced Encryptio Mobile Device Management Offline Temporary Password Reports and Analysis Alerts Directory Services Appliance System Maintenance	Web Browser     E-mail ()       Brinnet Explorer     A       Corea     Brinnet Explorer       Corea     A       PaceInset Explorer     A       Corea     Brinnet Explorer       Dif	A (AttaCherneth A k (Gody) Thrundebrid thrundebrid than Nater (Att than Nater (Att than Nater (Att the Nater (Att .	You Conception of the second sec	Could Service / File Could Service / File Could Device / Could Device / Device / Cells / October Could Could Could Could Could	A Use and a set of the set o	4¥	
UR: Inne Eanytock Enforced Encryptio Mobile Device Management Offline Temporary Password Alerts Directory Services Appliance System Maintenance System Configuration	Web Browser         E and C           Description         C and C	A (Statubents A global) 15 Durchorted 15 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 16 Durchorted 17 Durchorted 17 Durchorted 17 Durchorted 18 Durchorted 18 Durchorted 18 Durchorted 19	LAY	Coud Services / File Coud Services / File Coud one Coud one Co	Constant Constan	4 G	

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.

Applications 🕐 🔲 Storag	je Devices	O Network Share	Thin (	Clients 🕐 📄 Clipboard 🕐	Pri	int Screen 🕐 📄 Printers 🕐	
Web Browser ⑦		E-mail 🕜		Instant Messaging ⑦		Cloud Services / File Sharing ⑦	Social Media / Others ⑦
Internet Explorer		Outlook (Attachments		ICQ		Google Drive Client	EasyLock
Chrome		Outlook (Body)		MIA 🔲		iCloud Drive	Windows DVD Maker
Mozilla Firefox		Mozilla Thunderbird		Skype		uTorrent	ALFTP
Opera		Mozilla Thunderbird		Windows Live Messeng		BitComet	FileZilla
Safari		IBM Lotus Notes (Att		Yahoo! Messenger		Daum Cloud	GoToMeeting
AOL Desktop 9.6		IBM Lotus Notes (Bod		Gaim		KT Olleh uCloud	HTC Sync for Android
Aurora Firefox		Windows Live Mail		HanbiroTalk		Naver N Drive	InfraRecorder CD - D
K-Meleon		GroupWise Client		Pidgin		Azureus	iTunes
Maxthon	*	Outlook Express	-	Trillian	-	OneDrive (Skydrive)	LogMeIn Pro
Q Search	(X)	O Search	X	Q Search	<ul> <li>X</li> </ul>	Q Search	O Search

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

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

Туре	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, Twhirl, 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 NDrive, 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
Natal	

#### 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 polices, 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 o filters.

Policy Content							
File Type Filter Predefined Content Filter	Custom Content Filter	URL Whitelists	Domain Whitelists	File Whitelists	Regular Expressions	HIPAA	

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 a	oply to selected File Types							
Graphic Files:		JPEG	PNG	GIF	ICO	BMP	TIFF	More File Types
Office Files:	All	Word	Excel	PowerPoint	PDF	<ul> <li>Infopath</li> </ul>	Outlook	More File Types
Archive Files:	All	ZIP	ZIP/password	7z	RAR	ACE	TAR.	More File Types
Programming Files	: 🔽 All	🔽 c, cpp, java	РУ	🔽 sh, csh	🔽 bat, cmd	🔽 pas	🔽 xml, dtd	More File Types
Other Files:	IIA N	AutoCAD files	Text files	DRM Files	🔽 exe, sys, dl	✓ so	Unidentified	More File Types
Media Files:		₩ mov	₩ mp3	₩ m4a	wav	wma	v avi	More File Types

#### 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.

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 va	rious 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
✓ 55N:	🗹 Austria 🗹 Canada 🗹 France 🕼 Germany 🕼 Japan 🕼 Korea 🕼 Netherlands 🖉 Poland 🕼 Romania 🕼 Spain 🕼 Switzerland
JD:	🖉 Germany 🖉 Poland 🖉 Singapore 🕼 South Africa 🕼 Turkey China (🖓 Mainland 🖓 Macau 🕼 Hong Kong )
Passport:	🗹 Japan 🗹 Korea China (🖓 Mainland 🖓 Macau 🖓 Hong Kong )
Phone Number:	🗹 International 🗹 Japan 🗹 Korea 🖓 Turkey China (🖓 Mainland 🖓 Macau 🖓 Hong Kong )
Tax ID:	🗹 International 🖉 Italy 🗹 Poland 🔽 United States
Driving License:	🖌 Korea
Health Insurance Number:	🗹 Australia 🗹 Korea 🗹 United Kingdom
✓ Internet Protocol Addresses:	☑ Internet Protocol Version 4 (IPv4) ☑ Internet Protocol Version 6 (IPv6)

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.



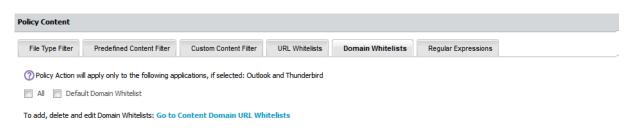
By checking the Case Sensitive option, the agent can differentiate the uppercase and lowercase letters when inspecting the content.

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).

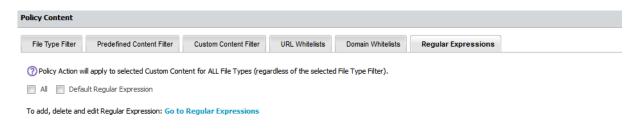
The "URL Whitelist" displays a list of URL whitelists. By selecting one or more whitelists, the Content Aware Protection agent will not scan uploads or attachments to the web addresses present in the whitelists. Whitelisting works for Internet Explorer.



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.



The "Regular Expressions" shows the list of the created regular expressions and the administrator can select up to five (5) 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:	1		0
Threshold Type:	Regular	⊖ Global	0

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 O 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	0
----------------------	----	---

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:

#### 64 | Endpoint Protector | User Manual

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	2 🗉 😣
Add New							
Dictionary Information							
Dictionary Name:		Confidential Dictionary					
Dictionary Description:		List of Confidential Terms					
Dictionary Content (separated by semicolon):		Agak Rahasia Armee intern od. dienstlich/Interne Begrenset Beperkte Verspreiding Bizalmas Classified information Clearance Confidencial Confidential Confidential Confidentiel défense Diffusion restreinte	au service	•			
Save Save	Import Dictionary	Export As	$\otimes$	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.  $\mathbb{Z}$ 

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.

ist of Filename Blacklists								
Dictionary Name +	Dictionary Description		Created at	Created by	Modified at	Modified by	Words/Items	Actions
858	858		15 October 2015 17:18	root	17 November 2015 11:14	root	3	200
Cristi	For Test		17 November 2015 10:08	root	17 November 2015 11:06	root	10	200
marius	do not delete me		6 November 2015 12:31	root	17 November 2015 11:15	root	3	200
test	test		15 October 2015 12:07	root	15 October 2015 17:27	ovidiu	3	200
Test1	Test1 Description		15 October 2015 10:41	root	15 October 2015 17:17	ovidiu	7	200
test123			18 November 2015 13:41	root	18 November 2015 13:41	root	0	200
test2	test2		16 October 2015 10:39	root	16 October 2015 10:39	root	1	200
test3	test3		16 October 2015 10:46	root	16 October 2015 10:46	root	1	200
test4	test4		16 October 2015 10:51	root	16 October 2015 10:51	root	15	200
ilename Blacklist Information Filename Blacklist Name:		leName Blacklist 1						
Filename Blacklist Descriptio	on: Te	est						
	e) .e	ample.pdf pp						

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.\*.

Content Aware URL Whitelists	5					Shov	w all departmen
URL Whitelists							
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	0	2 🗉 😣
Add New	]						
Edit Dictionary Information							
URL Whitelist Name:	Defaul	t URL Whitelist					
URL Whitelist Description:	Defaul	t URL Whitelist					
URL Whitelist Content (separa semicolon):	ated by new line, comma or						
Save Save	Import Whitelist	E E	kport As	🛞 Dele	te		

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

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.

	ENDPOINT PROTECTOR 4	Report	ling and Adminis	tration Tool							1	English	• (		Welcome   Advances	٩
	Dashboard	Content Aw	vare File Whitelists											Show	all departn	nents
	Endpoint Management	File Whiteli	ists													
Com	Endpoint Rights	File White	list Name 🔺	File Whitelist Description		Created at		Created by	/	Modified at		Modified by		Files	Actions	
X	Endpoint Settings	Default File	Whitelist	Default File Whitelist				root				root		0	$\mathbb{Z} \otimes$	
		Test		2		20 February 2015 14:	35	root		20 February 2015 14:35		root		0	$\mathbb{Z} \otimes$	
0	Content Aware Protection (CAP)	Test 1		1		20 February 2015 14:	35	root		20 February 2015 14:35		root		3	28	
	Dashboard Content Aware Policies Custom Content Dictionary Bladdists	🕀 Ad	ld New Whitelist													
	Content Aware URL Whitelists	File Whiteli	ist - Information													
	Content Aware Domain Whitelists Content Aware File Whitelists	File Whitels	et Nama-	Def	ault File W	/hitelist										
	Content Aware Regex Blacklists		st Description:		ault File W											
	Mobile Device Management	<b>S</b> :	Save Whitelist													
5712 000	Offline Temporary Password	_														
<u>~</u>	Reports and Analysis	File Whiteli	ist - Manage Files													
	Alerts	Results														
ø	Directory Services		File Name 🔺	Hash			File Extension	on	File Size	Modified by	Last	Modified			Actions	
	Appliance		Confidential.docx	c44f91a2ba2d2be91114ea629			docx		11 kB	root		bruary 2015 14:			8	
	, ppilonee		image001.png photo.PNG	ded946a8a51672d5452a07541 4a7a785272085096215b89ec6			png PNG		15 kB 107 kB	root		bruary 2015 14: bruary 2015 14:			8 8	
×	System Maintenance			48/8/052/2005090215009800	0/859000		PNG		IU/ KD	1001	20 Fe	oruary 2015 14.	55		0	
	System Configuration		ts [ 10 💌 per page]													
	System Parameters	<b>S</b> A	dd Files To Whitelist	Upload Files	8	Remove From White	ist (	Delete S	Selected							
$\overline{\mathbf{O}}$	Support															
Endpo	pint Protector 4 Copyright 2004 - 2015 Co	SoSys Ltd. All ri	ights reserved.											F	eady Versio	on 4.4.0.7

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** 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.

olicy Content							
File Type Filter Blacklist	Predefined Content Filter Blacklist	Custom Content Filter Blacklist	URL Whitelist	Domain Whitelist	File Whitelists	Regular Expression Blacklist	
🔲 All 📄 Default File W	'hitelist 📝 Test1 📝 Test2 📝 Tes	ting					

## 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.

Content Aware Domain Whitelist	ts						Show	all departments
Domain Whitelists								
Domain Whitelist Name 🔺	Domain Whitelist Description	on	Created at	Created by	Modified at	Modified by	Words/Items	Actions
Default Domain Whitelist	Default Domain Whitelist			root		root	2	2 🗉 🛇
Add New								
Edit Domain Whitelist Content								
⑦ Content Aware Domain Whitelists w	orks only for Outlook and Thund	erbird on Win	dows.					
Domain Whitelist Name:		Default Doma						
Domain Whitelist Description:		Default Doma	in Whitelist					
Domain Whitelist Content:		endpointprot						
Save Save	Import Whitelist		Export /	As	Delete			

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.

twork Share Whitelists									Show all depa
Results									
Network Share Whitelist Name *	Whitelist D	escription	Created at	Create	ed by Mod	lified at	Modified by	Items	Actions
Default Network Share Whitelist	Default Netw	vork Share Whitelist						Default Network Share Whitelist	ZØ
Test	Share		24 November 2015 1	3:01 root	24 N	ovember 2015 15:28	root	192.168.0.1\public\users\test;fileserver	28
test2	share		24 November 2015 1	3:06 root	24 N	ovember 2015 13:06	root		$\mathbb{Z} \otimes$
3 results [ 10 🔻 per page]									
Add New									
etwork Share Information									
Network Share Whitelist Name:	Te	est							
Network Share Whitelist Description:	sh	nare							
Network Share Whitelist Content (separa comma or semicolon):	ted by new line, 19 fil	92.168.0.1\public\users\test leserver\documents\examples							
Network Share Whitelist Computers:		CRISTIB							
	0	Test's i Mac							
		Search	X						

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.

egular 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		root		root	Z⊗
lit Regular Expression In	formation						
		Default Regular Expression					
<b>dit Regular Expression In</b> Regular Expression Name Regular Expression Descu		Default Regular Expression Expression To Verify An E-mail Address					

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:	[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+\.[ <u>a-zA-Z]</u> {2,4}	
Add Content For Testing Regular Expression:	test@test.com	
Matched Regular Expression:	test@test.com	
Save Save Delete	Back Test	

## 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.

Dashboard		Whitelist - List of File Types				Show all departr
Endpoint Management	Filter					
Endpoint Rights	Results					
Endpoint Settings	E All	Whitelisted	File Type Group	File Type +	MIME Types	
Content Aware Protection (CAP)			Archive Files	X8/	application/x-com.apple.xar-archive	
content Aware Protection (CAP)			Archive Files	7z	application/x-7z-compressed	
Dashboard	8		Archive Files	ACE	application/x-ace	
Content Aware Policies			Archive Files	ACE/password	application/encrypted-x-ace	
Custom Content Dictionary Blacklists	B		Media Files	af	audio/x-aiff	
Content Aware URL Whitelists		✓	Programming Files	asm	textix-asm	
Content Aware Domain Whitelists	B	-	Other Files	AutoCAD files	application/x-autocad	
Content Aware File Whitelists			Media Files	avi	video/x-msvideo, video/x-msvideo	
Content Aware Regex Blacklists			Programming Files	bat, cmd	text/x-msdos-batch	
Content Aware Type Whitelist		~	Graphic Files	BMP	image/x-ms-bmp	
Mobile Device Management			Archive Files	bz2	application/x-bzip2	
			Programming Files	c, cpp, java	text/x-java, text/x-c++, text/x-c	
Offline Temporary Password			Other Files	CATIA	application/catia-file	
			Graphic Files	CGM	image/cgm	
Reports and Analysis	E		Graphic Files	Corel Photo-Paint	application/x-cpt	
		~	Graphic Files	CoreDraw	application/x-cdr	
Alerts	E		Graphic Files	DJV	image/vnd.djvu	
			Other Files	DBM Files	application/x-scdsa	
Directory Services			Graphic Files	EPS	application/postscript	
			Office Files	Excel	application/vnd.ms-excel, application/vn	
Appliance	68 results [ 20 - pr	er page]				H < 1234 >
System Maintenance	Whitelist Selecter	d On-Whitelist Selected				
System Configuration						
System Parameters						
System Parameters						

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 *whitelist Selected* button.

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

To remove the file type, simply select it and click on the <sup>O Un-Whitelist Selected</sup> 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.

#### 71 | Endpoint Protector | User Manual

indust Indust   indust <t< th=""><th>ENDPOINT PROTECTOR</th><th>Reporting and Administration Tool</th><th></th><th>Welcome   Logost English • Q Advanced Search</th></t<>	ENDPOINT PROTECTOR	Reporting and Administration Tool		Welcome   Logost English • Q Advanced Search
Image: start right right   Image: start right right   Image: start right right   Image: start right rig	Dashboard	File Location Whitelists		
Windowski       For Landowski	Endpoint Management	No Results		
Index end roution (content have r	Endpoint Rights	Add New		
Deskert     in the method into its       Control Aware Binders     Control Market Binders       Control Market Binders     File Location Windeled Execution:       Pile Inter     File Location:       Pile Pile Pile Pile Pile Pile Pile Pile	Endpoint Settings	File Location Information		
Absolution   Outstate Aware Failed   Control Aware Failed   Control Aware Failed   Control Aware Failed   Control Aware Failed   Pic Location Mitclebi Econtent   Pic Location<	Content Aware Protection (CAP)	1. Fill in the informations	2. Apply to entities	
System Maintenance         System Configuration         System Parameters         Sport	Control Awar Palocs     Control Awar Vibilities     Pel Ionion     System Mantenance     Pel Ionion     System Canfguration	File Location Whitelet Name         Default Name           File Location Whitelet Description:         Default Description           File Location Whitelet Content (separated by new Res, comma or semicolar):         C/DestagCefault_File_Isochon	Computers adduth adduth ansis ansis Dravy Mastook	-
	Endpoint Protector 4 Copyright 2004 - 2016	CoSoSys Ltd. All rights reserved.		Ready Version 4.4.0.9

#### 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.

ENDPOINT 4	Reporting and Administration Tool					English	•	Welcome   Logos Q Advanced Searc
Dashboard	File Location Blacklists							
Endpoint Management	File Location Blacklists							
Endpoint Rights	File Location Blacklist Name A	Blacklist Description	Created at	Created by	Modified at	Modified by	Items	Actions
K Endpoint Settings	Test	Testing	2 February 2016 13:32	root	11 March 2016 17:02	root		28
Content Aware Protection (CAP)	1 result [ 10 v per page]							
Dashboard Content Aware Policies	Add New							
Content Aware Bladdists	File Location Information							
Custom Dictionaries File Name File Location Regular Expression	1. Fill in the informations		2. Apply to entities					
Catter K-ware Striktets Medical Strikt Allowed File Allowed File Allowed File Allowed File Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Allowed File Strikt Strikt Allowed File Strikt S	File Location Blackhol Hame: File Location Blackhol Conception: File Location Blackhol Content (separated by new line, comma or semicoluo):	Default Name Default Description C:/Desktap/Default/Vie_Jocotion	ACCOMP AC	N10 E				
Orrectory Services           Applance           System Mointenance           System Configuration           System Parameters           System Support	Sant							
Endpoint Protector 4 Copyright 2004 - 2016 Co	SoSys Ltd. All rights reserved.							Ready Version 4.4.0

# 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 Downloaded Content
	Webmail Attachments	Blog Posts
	File Attachments	E-MAIL Content for other E-
	Microsoft Outlook E-MAIL Content	MAIL Services
	Microsoft Outlook Forwarded and Saved Attachments	Forwarded Attachments
E-MAIL Clients	Microsoft Outlook E-mailed directly from Windows Explorer	Saved Attachments
	Microsoft Outlook Copied Attachments from one E-MAIL to another	Attachments e-mailed directly from Windows Explorer
	Mozilla Thunderbird E-MAIL Content	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.

Type Filter Blacklist Predefined Content Filter Blacklist Custom	Content Filter Blacklist	URL Whitelist	Domain Whitelist	File Whitelists	Regular Expression Blacklist	HIPAA
te: A HIPAA Policy should include PIIs like addresses, phone and fax numb	ers, emails and custom dictio	naries. Please m	ake sure you include the	em from the previou	s tabs.	
FDA recognised pharmaceutical firms	8.00 KB	Ŧ				
FDA recognised pharmaceutical prescription drugs (branded)	12.00 KB	<u>*</u>				
FDA recognised pharmaceutical prescription drugs (generic)	74.00 KB	<u>*</u>				
ICD-10 codes and diagnosis lexicon	429.50 KE	÷ 🕹				
ICD-9 codes and diagnosis lexicon	1.01 MB	.+.				

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 Conte	ent Filter Blacklist	Custom Content Filter Black	ist URL Whitelist	Domain Whitelist	File Whitelists	Regular Expression Blacklist	HIPAA		
Policy Action will apply t	io selected Predefined C	Content for ALL File Type	es (regardless of the selected	ile Type Filter).						
The below filters help en	sure compliance with va	rious regulations like PC	I DSS and HIPAA.							
Credit Cards:		Amex D	Diners Discover Discover	B Mastercard	Visa					
Personal Identifiabl	e Information:	IBAN Da	🗌 IBAN 🗌 Date 🔲 E-mail 🔲 Address 🕜							
Country Specif	ic:	SSN ID	Passport Phone	umber 🗌 Tax ID [	Driving License	Health Insurance N	umber			
Internet Protocol A	ddresses:	Internet Proto	ocol Version 4 (IPv4) 🔲 Int	rnet Protocol Version 6	(IPv6)					
Save Save	1	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

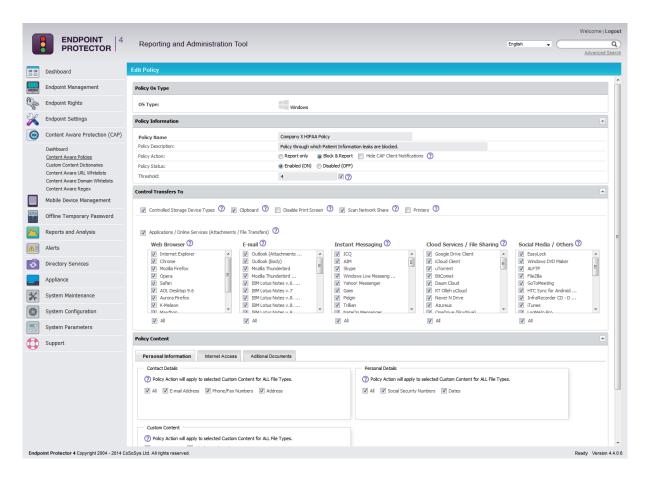
HIPAA policies can be created and used on their own or in combination with regular policies, for a better control of the data inside the network. These policies are available for Windows, Mac OS X or Linux computers. They are marked in the bottom right corner of the policy tab with a distinctive H.

Windows CAP Policy	Windows HIPAA Policy	MAC HIPAA Policy
Priority 1	Priority 2	Priority 3
File Types	Predefined Content	Predefined Content
Off		é On 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:



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 PIIs 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:

#### 76 | Endpoint Protector | User Manual

Policy Information	
Policy Name	Policy Y
Policy Description:	Polcy that blocks 10 or more PIIs
Policy Action:	💿 Report only 🛛 💿 Block & Report 🔲 Hide CAP Client Notifications 🕜
Policy Status:	Enabled (ON)     Disabled (OFF)
Threshold:	10 🖉 🕜

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:	Polcy that reports 3 or more of the same PIIs
Policy Action:	Report only Object & Report Hide CAP Client Notifications
Policy Status:	Enabled (ON)      Disabled (OFF)
Threshold:	3 🖸 🕜

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.

	Dashboard	Logs Report											
	Endpoint Management	Filter											
	Endpoint Rights	Results											
2	Endpoint Settings	Event	Client Computer	IP Address	Domain Name	Client User	Device Type	Device	Files	Date/Time(Server)	Date/Time(Client)	OS Type	Action
5	Content Aware Protection (CAP)	Blocked		192.168.0.198	Harrie	0301	Internal CD or DVD RW	MATSHITA DVD-RAM UJ8C2 S ATA Device	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55		
<u>'</u>	content Aware Protection (CAP)	Blocked	SALES THE PERSON NAMES	192.168.0.198		Transies:-	Webcam	USB2.0 HD UVC WebCam	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55	Windows	
	Mobile Device Management	Unblocked	HALL STREET, STREET, ST.	192.168.0.198		TORE:	WFi	Atheros AR9485WB-EG Wireless Network Ada	0	10-Sep-2014 10:57:26	10-Sep-2014 12:00:55	Windows	
		Unblocked	NAMES OF TAXABLE PARTY.	192.168.0.198		TORE:	WIFi	Atheros AR9485WB-EG Wireless Network Ada	0	10-Sep-2014 10:57:25	10-Sep-2014 12:00:54	Windows	
	Offline Temporary Password	Blocked	SALES AND DESCRIPTION OF	192.168.0.198		MARKET:	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	SALES FRANK PROPERTY.	192.168.0.198		NUMBER:	Webcam	USB2.0 HD UVC WebCam	0	10-Sep-2014 10:57:23	10-Sep-2014 12:00:52	Windows	
	Reports and Analysis	Connected	144405-14400-14600-14			Table :		MATSHITA DVD-RAM UJ8C2 S ATA Device	0		10-Sep-2014 12:00:52		_
	Logs Report	Connected	14427-142210-1000	192,168.0.198		Table -	WFi	Atheros AR9485WB-EG Wireless Network Ada.	0		10-Sep-2014 12:00:51		
	File Tracing	Connected	14421794217555800V			Transformation of the Institution of the Institutio	Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0		10-Sep-2014 12:00:51		
	File Shadowing	Blocked	AND TRACTORISM			Transie:		MATSHITA DVD-RAM UJ8C2 S ATA Device	0	04-Sep-2014 09:27:30			
	Content Aware Report	Blocked	HALF-MARKEN V.			Table -	Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:30			
	Content Aware File Shadowing	Blocked				Transie	Webcam	USB2.0 HD UVC WebCam	0	04-Sep-2014 09:27:30			=
	Admin Actions	Unblocked	LALE PROPERTY.			Transie:	WiFi	Atheros AR9485WB-EG Wireless Network Ada	-	04-Sep-2014 09:27:30			_
	Online Computers	Connected	BALL TRACTORES			TRANSCO ::	Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:30			_
		Connected	In the second			Table -	Webcam	USB2.0 HD UVC WebCam	0	04-Sep-2014 09:27:24 04-Sep-2014 09:27:21			_
	Alerts					Transie			0				=
h	Directory Services	Connected				Table -		MATSHITA DVD-RAM UJ8C2 S ATA Device		04-Sep-2014 09:27:21			
	birectory services	Connected		102.100.0.100			WiFi	Atheros AR9485WB-EG Wireless Network Ada		04-Sep-2014 09:27:21			_
	Appliance	Connected 18 results	[ 50 v per page]	192.168.0.198		DOM:C:	Serial ATA Controller	Standard AHCI 1.0 Serial ATA Controller	0	04-Sep-2014 09:27:21	04-Sep-2014 10:30:50	Windows	
	System Maintenance	GV	Export		Back								
	System Configuration	GY	Export	1	Dack								
1	System Parameters												
2	Support												
-													

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.

Logs Report
Filter
Results
Event name
Show/Hide Columns

#### 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.

ilter			
Event:		$\sim$	
Computer:			
IP Address:			
Domain Name:			
User:			
Device Type:		~	
Device:			
Date/Time(Server):		<b>H</b>	<b>=</b>
Date/Time(Client):			<b>.</b>
OS Type:	All	~	

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.

Protected Area	ĺ
Additional Password Protection:	
Unloc	ck 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.

Additional Security Password for S	ensitive Data Protection
Current Password:	
New Password:	
New Password (confirm):	
Save	

## 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.

<ul> <li>Indexide a second and analysis</li> <li>File Copy</li> <li>File Copy<!--</th--><th>Percent       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Content Aware Protection (CAP)       Mobile Device Management       File Address       Device 10 User       Network Starsge Device       File Mann       File Mann         Offline Temporary Password       Reports and Analysis       Te Device 102 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         Offline Temporary Password       File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device        File Deate</th><th>A</th><th>Advanced S</th></li></ul>	Percent       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Content Aware Protection (CAP)       Mobile Device Management       File Address       Device 10 User       Network Starsge Device       File Mann       File Mann         Offline Temporary Password       Reports and Analysis       Te Device 102 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         Offline Temporary Password       File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device        File Deate	A	Advanced S
Individual Management   Endpoint Rights   Endpoint Rights   Endpoint Rights   Endpoint Rights   Content Aware Protection (CAP)   Mobile Device Management   Offline Temporary Password   Reports and Analysis   Defend Taxard Line 200   Defend Taxard Line 200   Pie Device Tipe Taxard Nutrities 200   Defend Taxard Line 200   Defend Taxard Line 200   Defend Taxard Line 200   Defend Taxard Line 200   Diffline Temporary Password   Reports and Analysis   Fie Device Tipe 12:180.1188 DATARVILER.200   Using Storage Device   Fie Device Tipe 12:180.1188 DATARVILER.200   Diffline Temporary Password   Fie Device Tipe 12:180.1188 DATARVILER.200   Diffline Cony   Fie Device Tipe 12:180.1188 DATARVILER.200   Diffline Cony   Fie Device Tipe 12:180.1188 DATARVILER.200   Diffline Cony   Fie Device Tipe 12:180.1188 DATARVILER.200   Diffline Cony  <	Percent       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Endpoint Rights       Filter         Content Aware Protection (CAP)       Mobile Device Management       File Address       Device 10 User       Network Starsge Device       File Mann       File Mann         Offline Temporary Password       Reports and Analysis       Te Device 102 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         Offline Temporary Password       File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device       attrass 100 Strange Device         File Deate       192 (180 118) DATRAVELER 2.0       USB Strange Device       attrass 100 Strange Device       attrass 100 Strange Device        File Deate	how all d	iepartme
Endpoint Rights   Endpoint Settings   Content Aware Protection (CAP)   Mobile Device Management   Mobile Computers   Mobile Computers   Mobile Computers   Mobile Computers   Mobile Computers   Mobile Computer	Bit       Results         Endpoint Rights       Results         Endpoint Settings       Event Computer IP Address Device User Device Type File Hame       File Hamh         Content Avvare Protection (CAP)       Mobile Device Management       File Read       192 188.0 180 DATRAVELER_2.0       USB Strange Device       3d74e356e797br/dca11121f7e456ea         Offline Temporary Prossword       File Copy       192 188.0 180 DATRAVELER_2.0       USB Strange Device       3d74e356e797br/dca11121f7e456ea         File Device Management       Offline Temporary Prossword       File Copy       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         Icog Report       File Device       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         File Device       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         File Device       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         File Dovice       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         File Dovice       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c423de00733911303         File Dovice       192 188.0 180 DATRAVELER_2.0       USB Strange Device       at1339a 10d55c4245d0658134 MTD	_	
Endpoint Settings   Content Auvare Protection (CAP)   Mobile Device Management   Offline Temporary Password   Reports and Analysis   Logis Report   He Casy   Logis Report   He Casy   He Casy   Logis Report   He Casy   He Casy   Logis Report   He Casy   He Casy   Directory Services   Alerts   System Maintenance   System Maintenance   System Maintenance   System Maintenance   System Parameters	Endpoint Settings       Event       Computer       IP Address       Device       User       Device Type       File Name       File Name         Content Aware Protection (CAP)       Mobile Device Management       192 168.0.108       NT LAN Manager       Network Share       Ge006eacd34d3380bad77101s1ebee         Offline Temporary Password       File Read       192 168.0.108       NT LAN Manager       Network Share       Ge006eacd34d3380bad77101s1ebee         Reports and Analysis       File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff4339610c55c223d6069733911303         Icigs Report       File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff4339610c55c223d609733911303         File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff4339610c55c223d609733911303         File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff4339610c55c223d60973911303         File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff4339610c55c223d60973911303         File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff433960c57875aff5ed05807347105ea8         File Copy       192 168.0.108       DATATAVLER, 2.0       USB Strange Device       aff433960c57875aff5ed05		
Content Aware Protection (CAP)       Nobile Device Management       De006eac0343338bad77101a1ebced8         Offline Temporary Password       File Bade       192 168 0.168 DATARAVELER_20       USB Storage Device       3774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       3774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       3774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       3774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       4774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       4774e356e6737b7dca111217f2456eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       426cac7b75a115e6c069134tf075eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       426cac7b75a115e6c069134tf075eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       426cac7b75a115e6c069134tf075eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       426cac7b75a115e6c069134tf075eab         People       192 168 0.168 DATARAVELER_20       USB Storage Device       426cac7b75a115e6c069134tf075eab	Content Aware Protection (CAP)       Nel Read       192.168.0100 NT CAH Manager       Network Store       Qu005exd3343380bad77101a1ebee         Mobile Device Management       Offline Temporary Password       Fie Copy       192.168.0180 DATATRAVELER_2.0       USB Strange Device       3d74e350ef7877.dca11121/f645ee         Reports and Analysis       Fie Copy       192.168.0180 DATATRAVELER_2.0       USB Strange Device       af1e33a610e55c22ae60973911303         Logis Report       Fie Device       192.168.0180 DATATRAVELER_2.0       USB Strange Device       af1e33a610e55c22ae60973911303         Fie Dovice       192.168.0180 DATATRAVELER_2.0       USB Strange Device       af1e33a610e55c32ae60973911305         Fie Dovice       192.168.0180 DATATRAVELER_2.0       USB Strange Device       af1e33a610e55c42ae60973911305         Fie Dovice       192.168.0180 DATATRAVELER_2.0       USB Strange Device       af1e4530a610e55c4775415e6005813410715ee<		
Content Aware Processing Core       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       3d7435066737b7dca111217f456eab         Mobile Device Management       File Cory       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       3d7435066737b7dca111217f456eab         Offline Temporary Password       File Cory       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       3d7435066737b7dca111217f456eab         Reports and Analysis       File Cory       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d50a10605ca2346067339f13039b         File Debete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d50a10605ca2346067339f13039b         File Debete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d50a10605ca234606737b7dca111217f456eab         File Debete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d50a10605ca234f075eaa         File Debete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d50ac7b75d1156cc096134f075eaa         File Debete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d74350e677b7dca111217f456eab         File Dobete       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d74350e677b7dca111217f456eab         File Cory       192 168 0.198 DATATRAVEER_2.0       USB Storage Device       4d74350e677b7dca111217f6456eab         File Cor	Content Aware Production (Corv)         File Device         192:168.0198         DATATRAVELER_2.0         USB Strange Device         3d74e356e678777dcs11121776456ea           Mobile Device Management         Offline Temporary Password         File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af1e33ea floed5eb23ee678777dcs11121776456ea           Reports and Analysis         File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af1e33ea floed5eb23ee678777dcs11121776456ea           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af1e33ea floed5eb23ee678777dcs11121776456ea           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af1e33ea floed5eb73547f5e006973341705eaa           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af2ecac7b75415e006973341705eaa           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af7ec30ea77b7dcs111217645ea           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af7ec30ea77b7dcs111217645ea           File Copy         192:168.0198         DATATRAVELER_2.0         USB Strange Device         af7ec30ea77b7dcs111217645ea           File Copy         192:168.0198         DATA	File Size	File Type
Mobile Device Management       3/743554e737b7dcatf12176456eab         Offline Temporary Password       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       3/743554e737b7dcatf12176456eab         Reports and Analysis       Importary Password       Fie Debete       192160.198       DATATAVELER_2.0       USB Starage Device       at1839a10c65cb23da6097339113939         Mobile Device Management       Importary Password       Fie Debete       192160.198       DATATAVELER_2.0       USB Starage Device       at1839a10c65cb23da6097339113939         Mobile Device Management       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       at1839a10c65cb23da6097339113939         Mobile Device Management       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       at1839a10c65cb23da6097339113939         Mobile Computers       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       at1839a10c65cb23da6097391107caa1112176456eab         Mohine Computers       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       at1639a10c6cb775d15e6c059134tf0fLeae         Mohine Computers       Fie Copy       192160.198       DATATAVELER_2.0       USB Starage Device       at1639a10c6cb775d15e6c059134tf0fLeae         Mohine Computers       Fie Copy       192160.198	Mobile Device Management         File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         3074e350e67797b7dea111217f8458ea           Offline Temporary Password         File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         af13310055c223e609739713931393           Reports and Analysis         File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         af13310055c223e609739713931393           Logs Report         File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         af14550e5737726a11121776458ea           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac7b75a115e8c089734f1058aa           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac7b75a115e8c089734f1058aa           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac7b75a115e8c089534f1058aa           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac7b75a115e8c089534f1058aa           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac7b75a115e8c089534f1056aa           File Copy         192188.0199         DATATAVELER, 2.0         USB Strange Device         e26cac	8 532.2 KE	
Offline Temporary Password       Fie Deete       192 163.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de00733913939b         Reports and Analysis       Fie Covy       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de00733913939b         His maxing       Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de00733913939b         Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de00733913939b         Fie Shadowing       Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de007339113939b         Content Amare Report       Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de007339113939b         Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de007339113939b         Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de007339113939b         Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de007339113939b         Admarks       Fie Deete       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23de00734112176456e8b         Fie Device       Fie Copy       192 168.0 180 DATARAVELER_2.0       USS Strage Device       at183810056cb23	Offline Temporary Password       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af1633a10.656.6223a6067334173353         Reports and Analysis       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af1633a10.656.6223a6067334170353         Log Report       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af1633a10.656.6223a6067334170353         He Tracon       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af1633a10.656.62334670341703534         He Tracon       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af1633a10.656.623736713471041121716456ee         Fie Stadowing       Content Aware Report       Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af164306737770411721716456ee         Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af164306737770411721716456ee       3f164306677775411560.009573417076ea         Fie Ooelee       192180.0190       DATATAVELER_2.0       USB Strange Device       af16430677776417641121716456ee       3f1643066777764117647121716456ee       3f16430677776417641121716456ee       3f16430677776417641121716456ee       3f16430677776417641121716456ee       3f16430677776417641121716456ee       3f164306777776417641121716456ee       3f164306	0.10.10	.java file
Offline Temporary Password       Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       af183a10c55cb23de0097339113939b         Reports and Analysis       If a Debeta       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f5aa         Logs Report       Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f5aa         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Debeta       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac2cac7b75d15e5cc08d134f0f7aas         Fib Copy       192 168.0 198 DATARAVELER_2.0       USB Storage Device       ac7cac9b1e4c57f5d15e5cc08d14af704         Fib Copy       192 168.0 188 DATARAVELER_2.0<	Offline Temporary Password         File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         af1339a10c55c522da609733911333           Reports and Analysis         File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c0891341075eas           Logi Report         File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c0891341075eas           File Stadowing Content Aware File Stadowing Content Aware File Stadowing Other Computers         ATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c0891341075eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c0891341075eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c0891341075eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c08913417015eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c08913417015eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage Device         c26cac7b75a115e6c08913417015eas           File Copy         192 168.0.198         DATATRAVELER, 2.0         USB Strage De	3.43 KB	.java file Python Fi
Reports and Analysis   Logs Report   His Trading   File Baddwing   Content Aware Report   Fie Copy   Fie Copy   Fie Copy   Statem Maintenance   System Configuration   System Configuration   System Configuration   System Configuration   System Configuration	Reports and Analysis       File Debte       192 168.0190       DATATRAVELER_2.0       USB Strange Device         Logs Report       File Debte       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c0897334f075eas         He Transmitter       File Debte       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c0897334f075eas         File Transmitter       File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c0897334f075eas         Content Aware File Shadowing       Content Aware File Shadowing       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c0897334f075eas         File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c087334f075eas         File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c087334f075eas         File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c08734f016eas         File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c08734f10Feas         File Copy       192 168.0190       DATATRAVELER_2.0       USB Strange Device       e26cac7b75af15e0c08734f10Feas         Orine Computers       File Copy       1	19 R	Python Fi
Reports and Analysis       File Deelee       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as         Logs Report       File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as         File Shadowing       Content Aware Report       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as         File Shadowing       Content Aware Report       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as         Content Aware Report       File Shadowing       Content Aware Report       e26ca72r5af166c009134f076as       e26ca72r5af166c009134f076as         Admin Actions       Online Computers       File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as         File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as       e26ca72r5af166c009134f076as         File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e26ca72r5af166c009134f076as       e26ca72r5af166c009134f076as         File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e76c6014/1376436c686413760       e76c614/1376436c686413670         File Copy       192 168.0 188 DATARAVELER_2.0       USB Storage Device       e76c614/1376436c6864136204667434	Reports and Analysis         Fie Dealer         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           His Datadom         Fie Copy         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Stadowing         Content Aware Report         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Stadowing         Content Aware Report         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Admin Actions         Fie Doaler         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Doaler         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Doaler         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Aim Actions         Fie Doaler         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Copy         192180.0190         DATATRAVELER_2.0         USB Strange Device         #26cac7b75a115e0c089134f0078ass           Fie Copy         192180.0190         DATATRAV	10.0	Python Fi
Logs Report       File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       3d74a350e6797b7dca1112176456eab         File Shadowing       File Debete       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       3d74a350e6797b7dca1112176456eab         File Debete       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       620ea/7b75415ebc0691341f02feas         File Debete       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       620ea/7b75415ebc0691341f07feas         Content Aware Report       File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457ff634b1c4e51a670         Content Aware Report       File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457ff634b1c4e51a670         File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457ff634b1c4e51a670         File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457ff634b1c4e51a670         File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457ff734b1c4e51a6700         File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       60f572ee491e457f734b1c4e51a6700         File Copy       192 168.0 198 DATATRAVELER_2.0       USB Storage Device       75f0125bd451db824e6245c0fc584         S	Log Report       File Copy       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       3d74e350ed737b7dea111217f6456ea         File Shadowing       File Debice       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       2d74e350ed737b7dea111217f6456ea         File Shadowing       File Debice       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       2d74e350ed737b7dea111217f6456ea         Content Aware Report       Content Aware File Shadowing       Adm Actions       00182 Computers       00172ee491e457ff34b11e461a870         Orline Computers       File Opy       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       001572ee491e457ff44b1e461a870         Orline Computers       File Opy       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       001572ee491e457ff44b1e461a870         Orline Computers       File Opy       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       001572ee491e457ff44b1e4641a870         Directory Services       File Opy       192 168.0 198       DATATRAVELER 2.0       USB Strange Device       005572ee491e457ff44b1e4645fa870         Appliance       File Opy       192 168.0 198       DATATAVELER 2.0       USB Strange Device       75f8125bd431de68a4e89449c0fc88         System Maintenance       174 results       100 per page)       17		.java file
File Tradends     Solvers Overset     Solvers Overset       File Shadowing     File Debete     192 168 0.158 0.4TATAVELER_2.0     USB Storage Device       File Debete     192 168 0.158 0.4TATAVELER_2.0     USB Storage Device     Content Aware Report       Content Aware Report     Content Aware Report     Content Aware Report     Content Aware Report       Content Aware Report     Content Aware Report     Content Aware Report     Content Aware Report       Content Aware Report     Content Aware Report     Content Aware Report     Content Aware Report       Content Aware Report     Content Aware Report     Content Aware Report     Content Aware Report       Content Aware Report     Content Aware Report     Content Aware Report     Content Aware Report       Content Aware Report     File Corp     192 168 0.158 0.ATATAVELER_2.0     USB Storage Device     Content Aware Report       Content Aware Report     File Corp     192 168 0.158 0.ATATAVELER_2.0     USB Storage Device     Storage Device       File Corp     192 168 0.158 0.ATATAVELER_2.0     USB Storage Device     Storage Device     Storage Device       File Corp     192 168 0.158 0.ATATAVELER_2.0     USB Storage Device     Storage Device     Storage Device       File Corp     192 168 0.158 0.ATATAVELER_2.0     USB Storage Device     Storage Device     Storage Device       File Corp <td>He Trading         He Outy         He Class (He Clas) (He Clas) (He Class (He Class (He Clas) (He Class (He Clas) (</td> <td>7.47 KB</td> <td>Python Fi</td>	He Trading         He Outy         He Class (He Clas) (He Clas) (He Class (He Class (He Clas) (He Class (He Clas) (	7.47 KB	Python Fi
He Shadowing Content Avare Report Content Avare Report     Fie Deete     192 168 0.198 DATARAVELER_20     USB Storage Device       Fie Deete     192 168 0.198 DATARAVELER_20     USB Storage Device     e26car/b75415e6c069134f0fFeas       Content Avare Report Content Avare Report     e26car/b75415e6c069134f0fFeas     e0572ee491e457ffc94b1c4e81n870       Content Avare Report Content Avare Report     e26car/b75415e6c069134f0fFeas     e0572ee491e457ffc94b1c4e81n870       Content Avare Report     e26car/b75415e6c069134f0fFeas     e0572ee491e457ffc94b1c4e81n870       Content Avare Report     e26car/b75415e6c09134f0fFeas     e0572ee491e457ffc94b1c4e81n870       Fie Copy     192168.0188 DATARAVELER_2.0     USB Storage Device     e07ee60f41792e95c6863424f0e703f       Fie Copy     192168.0188 DATARAVELER_2.0     USB Storage Device     75fc1250d481de8a4e89460dc8f4       Fie Deete     192168.0188 DATARAVELER_2.0     USB Storage Device     75fc1250d481de8a4e89460dc8f4       Fie Deete     192168.0188 DATARAVELER_2.0     USB Storage Device     75fc1250d481de8a4e89460dc8f4       System Maintenance     fie Deete     192168.0188 DATARAVELER_2.0	Pie Shadowing Content Aware Report         In C Debete         112:180.1196         DATATRAVELER_2.0         USB Strange Device         e26cac7b75415e0c88734/f07Eaa           Content Aware Report         File Debete         112:180.1196         DATATRAVELER_2.0         USB Strange Device         e26cac7b75415e0c88734/f07Eaa           Content Aware Report         File Debete         112:180.1196         DATATRAVELER_2.0         USB Strange Device         e26cac7b75415e0c88734/f07Eaa           Ohne Computers         File Debete         112:180.1196         DATATRAVELER_2.0         USB Strange Device         60f72ee491457ffc34b1c4e5fa870           Ohne Computers         File Debete         112:180.1196         DATATRAVELER_2.0         USB Strange Device         60f72ee491457ffc34b1c4e5fa870           Ohne Computers         File Device         1012:180.1196         DATATRAVELER_2.0         USB Strange Device         60f572ee491457ffc34b1c4e5fa870           Directory Services         File Device         1012:180.1196         DATATRAVELER_2.0         USB Strange Device         60f572ee491457ffc34b1c4e5fa870           Appliance         File Device         112:180.1196         DATATRAVELER_2.0         USB Strange Device         75f9125b431de468a469449c0fc387           System Maintenance         Tif Debete         192:180.198         DATATAVELER_2.0         USB Strange Device         75f9125b431d	3.43 KB	.java file
Content Aware Report     The Debte     192 188 0.198 DATARAVELER_2.0     USB Storage Device       Content Aware Fie Shadowing Adm Actions     Fie Copy     192 188 0.198 DATARAVELER_2.0     USB Storage Device       Allerts     Fie Copy     192 188 0.198 DATARAVELER_2.0     USB Storage Device     60/572ee/31e/s070/54b1/ce81nf870       Directory Services     Fie Copy     192 188 0.198 DATARAVELER_2.0     USB Storage Device     60/572ee/31e/s070/54b1/ce81nf870       Directory Services     Fie Copy     192 188 0.198 DATARAVELER_2.0     USB Storage Device     60/572ee/31e/s070/64b1/64b1/s070/64b1/64b1/s070       Appliance     Fie Copy     192 188 0.198 DATARAVELER_2.0     USB Storage Device     07/56/81/1792/452/66/853/44b1/64b1/s070/6556       System Configuration     System Configuration     50/572ee/31e/s0.198 DATARAVELER_2.0     USB Storage Device     75/612/50/481/46/84/69/4/07/6/84       System Parameters     System Parameters     Storage Device     75/612/50/481/46/84/69/4/07/6/84     75/612/50/481/46/84/69/4/0//6/84	Content Aware Report         File Codet         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         e26cac7b75415860698733417015eas           Content Aware File Shadowing Admin Actions         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         80/1572ee491e4571fc34b1c4e518570           Online Computers         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         80/1572ee491e4571fc34b1c4e518570           Alerts         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         60/1572ee491e4571fc34b1c4e518570           Directory Services         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         60/1572ee491e4571fc34b1c4e518570           Directory Services         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         60/1572ee491e4571fc34b1c4e518570           Appliance         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         75/11250431db634e8449c0fc80           System Maintenance         File Cody         192:183.0190 DATATAV/LER_2.0         UUS Strange Device         75/11250431db634e48449c0fc80           System Configuration         System Configuration         File Codet         192:183.0190 DATATAV/LER_2.0         UUS Strange Device		.ace file
Content Aware File Stadowing Adm Actions Online Computers         File Copy         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         801572e491e457ff034b1c485fa670           Alents         File Copy         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         801572e491e457ff034b1c485fa670           Alents         File Copy         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         801572e491e457ff034b1c485fa670           Directory Services         File Copy         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         07606f041792485068d541c447201           Directory Services         File Copy         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         07606f041792485068d541c447201           Appliance         File Debet         192 168.0.198 DATATRAVELER_2.0         USB Storage Device         7510125bd481db884e89449c0fc8/84           System Maintenance         Tif results [20] per page]         IIII         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Content Aware File Shadowing Adm Actions         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         801572ee491e457ffc94b1c4651a570           Adm Actions         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         801572ee491e457ffc94b1c4651a570           Alerts         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         801572ee491e457ffc94b1c4651a570           Directory Services         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         801572ee491e457ffc94b1c4651a570           Directory Services         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         805572ee491e457ffc94b1c4651a570           Appliance         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         75f1125o4481dx684e489449c01c806           System Configuration         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         75f1125o4481dx684e489449c01c806           System Configuration         File Copy         192 168.0 190         DATATRAVELER, 2.0         USB Strage Device         75f1125o4481dx684e489449c01c806           System Configuration         File Copy         Strage Device         75f1125o4481dx684e489449c01c806         File Copy         <		Python F
Alerts     File Delete     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     80/572e491 e45/17/094b1 c4e81af870       Alerts     File Copy     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     80/572e491 e45/17/094b1 c4e81af870       Directory Services     File Copy     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     80/572e491 e45/17/094b1 c4e81af870       Directory Services     File Copy     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     07606/01/17/2245638a9 164772031       Directory Services     File Copy     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     0555385e4173520942546024314e       Appliance     File Delete     192 168 0.198 DATATRAVELER_2.0     USB Storage Device     751122bd431de684e83449cdr6814       System Maintenance     174 results     20 - per pagel     11     11/4 results     20 - per pagel       System Configuration     Export     Back     Back     11/4 results     11/4 results     11/4 results	Alamin Accoms         File Dekte         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         00/15/26e491e457ffc94b1c4e51a577           Alerts         File Copy         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         00/15/26e491e457ffc94b1c4e51a577           Alerts         File Copy         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         00/15/26e491e457ffc94b1c4e51a577           Directory Services         File Copy         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         076601417922485c83a9a16477203           Appliance         File Copy         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         7511256c4816b06a4e89449c01c686           System Maintenance         File Deate         192 168 0.198 DATATRAVELER_2.0         USB Strange Device         174 results [20] per page]           V         m         Export         Back         10         10	7.47 KB	Python F
Directory Services         File Copy         192 168.0.198         DATATRAVELER_2.0         USB Storage Device         07626/01/1792451625382316072307           Pirectory Services         File Copy         192 168.0.198         DATATRAVELER_2.0         USB Storage Device         07626/01/179245362383816072307           Pirectory Services         File Copy         192 168.0.198         DATATRAVELER_2.0         USB Storage Device         07626/01/179245362383816072307           Appliance         File Copy         192 168.0.198         DATATRAVELER_2.0         USB Storage Device         75612504451de68469449:016/844           System Maintenance         File Device         192 168.0.198         DATATRAVELER_2.0         USB Storage Device         114 results [         102 · per page]           System Configuration         System Configuration         Image: Storage Device         Ima	Directory Services         File Copy         192 188.0 190         DATATAVELER_2.0         USB Strage Device         60/57/2ee491e457ff:94b1c4e51a570           Alerts         File Copy         192 188.0 190         DATATAVELER_2.0         USB Strage Device         07/2eb104/179248c6983a1dc47203           Directory Services         File Copy         192 188.0 190         DATATAVELER_2.0         USB Strage Device         055320e491e457ff:94b1c4e5ta570           Appliance         File Copy         192 188.0 190         DATATAVELER_2.0         USB Strage Device         75/61125ba481db68a4e69449c01c050           System Maintenance         File Device         192 188.0 190         DATATAVELER_2.0         USB Strage Device         174 results         180 chartaveler 2.0         198 Strage Device         174 results	224 B	.ace file
Alerts     File Copy     192 168.0.198     DATATRAVELER_2.0     USB Storage Device     07e06/01417912485:2889841d:47203f       Directory Services     File Copy     192 168.0.198     DATATRAVELER_2.0     USB Storage Device     65533089641735240962546862434e       Appliance     File Delete     192 168.0.198     DATATRAVELER_2.0     USB Storage Device     7561125bd451db684e69449.0fr.6844       System Maintenance     If the Delete     192 168.0.198     DATATRAVELER_2.0     USB Storage Device     174 results [     20 - per page]       System Configuration     Export     Eack     Image: Configuration     Image: Configuration     Export     Eack	Alerts         File Copy         192 168 0.198         DATATRAVELER_2.0         USB Strage Device         07e0610/417912485c98a9a1047203           Directory Services         File Copy         192 168 0.198         DATATRAVELER_2.0         USB Strage Device         65553086e41735209b225e60223F           Appliance         File Copy         192 168 0.198         DATATRAVELER_2.0         USB Strage Device         75fs12564810668ae894450f0586           System Maintenance         r         r         r         r         r           System Configuration         Export         Back         Back         File Copy         Export	_	.ace file
File Copy     192 168 0.188     DATATRAVELER_2.0     USB Storage Device     65553869e417352d9925466b2434e       Directory Services     File Copy     192 168 0.198     DATATRAVELER_2.0     USB Storage Device     75612504481de6844894480dr6.8644       Appliance     File Delete     192 168 0.198     DATATRAVELER_2.0     USB Storage Device     75612504481de6844894480dr6.8644       System Maintenance     174 results     20 - per pagel     III     IIII       System Configuration     600     Export     Back	File Copy         192 168 0.190         DATATRAVELER_2.0         USB Storage Device         655536964173524994256682436           Directory Services         File Copy         192 168 0.190         DATATRAVELER_2.0         USB Storage Device         751012564451046884469449c01c88           Appliance         File Deteite         192 168 0.190         DATATRAVELER_2.0         USB Storage Device         751012564451046884469449c01c88           System Maintenance         File Deteite         192 168 0.190         DATATRAVELER_2.0         USB Storage Device           System Configuration         Export         Back         Mill         Mill         Mill		.ace file
Directory Services     File Copy     192 168.0 198 DATATRAVELER_2.0     USB Sorrage Device     7519125bd481db684e68449c0fc884       Appliance     File Debite     192 168.0 198 DATATRAVELER_2.0     USB Sorrage Device     7519125bd481db684e68449c0fc884       System Maintenance     T/4 results [ 20 w per page]     Image: Comparison of the Compariso	Directory Services         File Copy         192 183 0198 DATATRAVELER 2.0         USB Storage Device         75/51125048180684489449c01c88           Appliance         File Detete         192 183 0198 DATATRAVELER 2.0         USB Storage Device         75/51125048180684489449c01c88           System Maintenance         File Detete         192 183 0198 DATATRAVELER 2.0         USB Storage Device         174 results         20 mm           System Configuration         Export         Back         114         Back         115		.ace file
Appliance     File Deete     192 168.0 198 DATATRAVELER_2.0     USB Storage Device       System Maintenance     File Deete     192 168.0 198 DATATRAVELER_2.0     USB Storage Device       System Configuration     Image: Configuration     Image: Configuration     Image: Configuration       System Parameters     System Parameters     Image: Configuration     Image: Configuration	Appliance     File Delete     192 168.0.198 DATATRAVELER_2.0     USB Storage Device       System Maintenance     174 results     20 per page)       System Configuration     Image: Configuration     Image: Configuration       System Parameters     Export     Back		.ace file .ace file
Appliance     File Debte     192 168.0 198 DATATRAVELER_2 0 USB Storage Device       System Maintenance     174 results [ 20 * per page]       System Configuration     * m       System Parameters     * Back	Appliance     File Delete     192 168 0.198 DATATRAVELER_2.0     USB Storage Device       System Maintenance     174 results [ 20 ] per page]     IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	7.20 KD	Python Fi
System Maintenance System Configuration System Parameters	System Configuration Export Esot		Python Fi
System Parameters     Image: Configuration	System Configuration Export Back		
System Parameters	System Parameters		
Support	Support		

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.

	ENDPOINT 4 PROTECTOR			Reporting and Administration Tool						Eng	lish 🔹 🤇	ł	Advanced
1	Dashboard	Fil	le Sha	adowing							S	how all o	lepartm
]	Endpoint Management		Filter										
	For design Dights	-	inter										Ľ
•	Endpoint Rights	R	Results	5									
	Endpoint Settings		E Fi	ile Name	File Size	File Type	Users	Computer	IP Address	Date/Time(Client)	Date/Time(Server)	OS Type	Actions
	Content Aware Protection (CAP)				73.32 KB	PNG Image	100000000000000000000000000000000000000	- Borrow College	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	
	Mahila Davies Management				121.16 KB	PNG Image	Contrast of the	Balance and Control	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	
	Mobile Device Management				94.95 KB	PNG Image	Contrast Excit	507700 C-040	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30	Windows	
	Offline Temporary Password				108.33 KB	PNG Image			192.168.0.96		2014-03-12 09:06:30	Windows	
				The same support of the same sector of the same	67.26 KB	PNG Image	Contrast Co. (1)	CONTRACTOR OF CARD	192.168.0.96	2014-03-12 10:06:21	2014-03-12 09:06:30		
	Reports and Analysis			the state sufficient of the state state of the state of the	14.24 KB	PNG Image	Concerns of the	Contraction of the	192.168.0.96		2014-03-12 09:06:30	Windows	
				the state of the s	67.26 KB	PNG Image	Concerns of the	Contraction of Contract	192.168.0.96	2014-03-11 17:29:30	2014-03-11 16:29:35	Windows	
	Logs Report File Tracing				94.95 KB	PNG Image	The second second	Contraction of the second	192.168.0.96	2014-03-11 17:29:22		Windows	
	File Shadowing			the light sufficiency of the second	121.16 KB	PNG Image	0.0000000000000000000000000000000000000	Contraction of the second	192.168.0.96	2014-03-11 17:29:20	2014-03-11 16:29:26	Windows	
	Content Aware Report			And a second processing of the second s		PNG Image	The second second	Contraction of the second			2014-03-11 16:29:25	Windows	
	Admin Actions				108.33 KB	PNG Image	Contrast Co. 17	Contraction of the second	192.168.0.96	2014-03-11 17:29:17	2014-03-11 16:29:23	Windows	
	Online Computers			And the second		PNG Image	The second second	Contraction of the	192.168.0.96		2014-03-11 16:29:17	Windows	
	Online Users				106.85 KB	PNG Image		1000	192.168.0.21	2014-03-11 14:59:40	2014-03-11 13:59:44		
	Alerts				226.28 KB	PNG Image		1000	192.168.0.21		2014-03-11 13:58:34	Windows	
	Alerts			Constanting of Consta	36 B				192.168.0.20	2014-03-11 12:06:27		Macintosh	
	Directory Services			CONTRACTOR CONTRACTOR CONTRACTOR	36 B		10000				2014-03-11 11:03:14		
				Constant Constant Constant Constant	36 B					2014-03-11 12:02:03		Macintosh	
	Appliance			Characteristic Constant Constant Constant Constant	36 B					2014-03-11 12:00:19		Macintosh	
				Charles Charles International Contraction	36 B						2014-03-11 10:58:30	Macintosh	
	System Maintenance				36 B				192.168.0.20	2014-03-11 11:40:35		Macintosh	
	Sustam Configuration			2790/00 (Constant of the Constant of the Const	205 B			100000000000000000000000000000000000000			2014-03-11 10:39:19		
	System Configuration				36 B						2014-03-11 10:37:30	Macintosh	
	System Parameters				46.63 KB	.icns file		1000	192.168.0.21		2014-03-11 10:35:20		
	-,				9 B						2014-03-11 10:35:19		
	Support				i 784 B				192.168.0.21		2014-03-11 10:35:13		
					613 B	autornine ritereneiteee			192.168.0.21		2014-03-11 10:35:13	Windows	
					28 B			1000			2014-03-11 10:35:13		
					36 B						2014-03-10 16:33:50		
				Contraction of the Contraction o		ping					2014-03-10 15:23:40		
				The second	205 B	data		CONTRACTOR OF THE OWNER.	192.168.0.115	2014-03-10 15:24:15	2014-03-10 14:24:15	Macintosh	

#### 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.

1	PROTECTOR	Reporting and Adminis	tration tool			English	•	Advanced
	Dashboard	Content Aware Report						Show all departm
	Endpoint Management	Filter						
R	Endpoint Rights	Results						
K	Endpoint Settings	Content Policy	Destination Type	Destination	File Name	File Hash	File Size	Matched Item
2	Content Aware Protection (CAP)	Undefined Policy	screen-capture		screen-capture-image			
9	content i future i fotocolori (criti)	Undefined Policy	screen-capture		screen-capture-image			
	Mobile Device Management	RO	Web Browser	Mozilla Firefox	11006600000117541_11008444555	80f48c1f435fe040d33665030f719132	7.77 MB	application/x-dosexec
		RO	Web Browser	Mozilla Firefox	The second states and	f3e7a015c1d541528085d3f9581ab41f	220 KB	application/x-dosexec
	Offline Temporary Password	RO	Web Browser	Mozilla Firefox	Construction and Construction of the	46860396033a0d3b326cbc8a8719577a	245.5 KB	application/x-dosexec
		RO	file-type	explorer	NOT THE COMPLEX COMPLEX OF	f3e7a015c1d541528085d3f9581ab41f	220 KB	application/x-dosexec
m	Reports and Analysis	RO	file-type	explorer	No. 750. Consideration Considerations	f3e7a015c1d541528085d3f9581ab41f		application/x-dosexec
		RO	file-type	explorer		f3e7a015c1d541528085d3f9581ab41f	220 KB	application/x-dosexec
	Logs Report	RO	file-type	explorer		732a2aad77ea6d56e7a534086881e230		application/x-dosexec
	File Tracing	RO	file-type	explorer	Street, Charles Charles and Street, St	83af340778e7c353b9a2d2a788c3a13a		application/x-dosexec
	File Shadowing	RO	file-type	explorer	Contract Constant Contract Contract Contract Contract Contract	6368baa2c6d3ae01ce29106c48847def		application/x-dosexec
	Content Aware Report	RO	file-type	explorer	School Charles Construction Construction Construction	6368baa2c6d3ae01ce29106c48847def		application/x-dosexec
	Content Aware File Shadowing	RO	file-type	explorer	STORE Training and the second second	414b5bb94da8e1250ad043cfd7ac5053		application/x-dosexec
	Admin Actions	RO	file-type	explorer	School Constant Constant Constant Constant Constant	732a2aad77ea6d56e7a534086881e230		application/x-dosexec
	Online Computers	RO	file-type	explorer	School Constant Constant	83af340778e7c353b9a2d2a788c3a13a		application/x-dosexec
_	Alerts	RO	file-type	explorer				application/x-dosexec
	Alerts	RO	file-type	explorer	Michael Consideration Colona, States	be258009e663442f8d0512bffcc050a7		application/x-dosexec
5	Directory Services	RO	file-type	explorer			9.07 MB	application/x-dosexec
£*	Directory Services	RO	file-type	explorer	No. of the second se	6368baa2c6d3ae01ce29106c48847def		application/x-dosexec
	Appliance			-				
-	Appliance	test for exceptions from sys policies		Mozila Thunderbird	and the second second billion of the second s	79fb3436099fe00487bc874fd0313d13	19.33 KB	image/x-icon
$\mathbf{v}$	System Maintenance	test for exceptions from sys policies	-	-				text/x-c++
r	System municenance	test for exceptions from sys policies		Mozilla Firefox		0b4c5b394dfb23ee1a92a8ce9e0530bf		text/x-tex
ð.	System Configuration	test for exceptions from sys policies		Mozilla Firefox		69d6ba69f6ce6f14d10f40dedcf8abfd	10.72 KB	text/x-shellscript
W	_,	test for exceptions from sys policies		Mozilla Firefox	No. Constraint Anna Constraint Ann	7e861912881c4ee677a7865f5648bff2	3.98 KB	text/x-tex
	System Parameters	test for exceptions from sys policies		Mozilla Firefox	The support of the second s		3.08 KB	text/x-tex
1.1.1		test for exceptions from sys policies		Mozilla Firefox		3d74e350e6797b7dca1f121f76456eab		text/x-c++
	Support	test for exceptions from sys policies		Mozilla Firefox	Constanting - sale - State	cbd5c5895db6336e15312eb126d27d21		application/x-ace
9		test for exceptions from sys policies		Mozilla Firefox	TrankGR	ca2dbdece86e29101bf9f7bc06693b39	1013 KB	image/gif
		test for exceptions from sys policies		Mozilla Firefox	Trans	0de7cc7a79396fbd6d08cc27c6f09895	140.65 KB	
		test for exceptions from sys policies		Mozilla Firefox	THE CARE THE C	730ddd0fe402efc1d41f33e574f6c08d	3.08 KB	text/x-tex
		test for exceptions from sys policies		Mozilla Firefox	The constant of the constant o	69d6ba69f6ce6f14d10f40dedcf8abfd	10.72 KB	text/x-shellscript
		test for exceptions from sys policies	-	_				text/x-python
		test for exceptions from sys policies	-					text/x-python
		test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	The conversion			text/x-c++
		test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0				text/x-python
		test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0				application/encrypted-x-a
		test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	Construction of the second second			application/encrypted-x-ac
		test for exceptions from sys policies	USB Storage Device	DATATRAVELER_2.0	Capability and the same of the	65853869e8417352d09d25a66b243f4e	571 B	application/encrypted-x-ac
			HOD Charges Devices					

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.

#### 82 | Endpoint Protector | User Manual

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):	
S Reset Q Apply filter	

#### 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.

		PROTECTOR	Rept	orting and Administration Tool						English	•	Advanced S
Endpoint Rights       Results         Endpoint Rights       I is lame       Fis Size       User       Computer       IP Address       Date/Time(Clent)		Dashboard	Content	Aware File Shadowing								
Endpoint Settings       I All File Hame       File Size       User       Computer       IP Address       Date/Time(Client)       Date/Time(Server) +       O S Type       Actembra         Mobile Device Management       1299 KB       1299 KB       192186 5.1       201499-01183152       201499-061523       Mindows IP Computer       IP		Endpoint Management	Filter									
Endpoint Settings       I All File Hame       File Size       User       Computer       IP Address       Date/Time(Client)       Date/Time(Server) +       O S Type       Actembra         Mobile Device Management       1299 KB       1299 KB       192186 5.1       201499-01183152       201499-061523       Mindows IP Computer       IP		Endpoint Rights	Results									
Mobile Device Management       220 kB       192.468.5k1       2014.09.10 10.12.22       2014.09.60 66.15.20       Windows	2	Endpoint Settings	IIA 🗐	File Name	File Size	User	Computer	IP Address	Date/Time(Client)	Date/Time(Server) -	OS Type	Actions
Mobile Device Management       22 KB       12 2 KB       12 2 KB       2014 0-9 10 10:22       2014 0-96 06 15:20       Windows       S         Offine Temporary Password       220 KB       12 2 KB       12 2 KB       2014 0-90 10 10:22       2014 0-96 06 15:20       Windows       S         Logs Report       12 2 KB       12 2 KB       12 2 KB       2014 0-90 10 10:22       2014 0-96 06 15:20       Windows       S       S         Logs Report       12 2 KB       12 2 KB       12 2 KB       2014 0-90 18 01:19       2014 0-90 51 20:53       Windows       S       <	,	Content Aware Protection (CAP)			12.69 KB	milit:	Rinnetto	192.168.0.20	2014-09-10 16:31:52	2014-09-06 12:38:23	Macintosh	
Offline Temporary Password       22 k 8       1 22 k 8       1 22 k 8 5       2014 0-00 10 25 23       2014 0-00 60 55 53       Windows       1 20         Lops Reports and Analysis       1 22 k 8       1		· · · ·		Construction Construction Construction	220 KB	<b>BRACE</b>	And and a second second second	192.168.56.1	2014-09-10 10:12:22	2014-09-06 06:15:20	Windows	
Offline Temporary Password       22 kB       12 2 kB       12 kB <td></td> <td>Mobile Device Management</td> <td></td> <td>The second se</td> <td>245.5 KB</td> <td>ENGLIST.</td> <td>And and a second second</td> <td>192.168.56.1</td> <td>2014-09-10 10:12:22</td> <td>2014-09-06 06:15:20</td> <td>Windows</td> <td></td>		Mobile Device Management		The second se	245.5 KB	ENGLIST.	And and a second second	192.168.56.1	2014-09-10 10:12:22	2014-09-06 06:15:20	Windows	
Reports and Analysis       120 kg       120 kg       120 kg       2014 09-09 17.63.31       2014 09-09 13.05.81       Windows       ISO         Logs Report       132 kg       132 kg       132 kg       132 kg       2014 09-09 16.05.82       2014 09-09 12.05.83       Windows       ISO         Logs Report       132 kg       132 kg       132 kg       132 kg       132 kg       2014 09-09 16.05.83       2014 09-05 12.05.83       Windows       ISO					220 KB	<b>BREAD</b>	and and the second second	192.168.56.1	2014-09-10 09:52:33	2014-09-06 05:55:31	Windows	
tops Reports and Analysis       132 kB       192 kB8 of 192 kB8 of 120 kB9 of 120 k		Offline Temporary Password			220 KB	<b>BRACE</b>	Sector State	192.168.56.1	2014-09-09 18:01:19	2014-09-05 14:04:18	Windows	
Ligg Report       122 KB       122 KB       122 KB       122 KB       122 KB       122 KB       124 KB </td <td>1</td> <td>Poporte and Analysis</td> <td></td> <td></td> <td>220 KB</td> <td><b>Distant</b></td> <td>100 C 100 C</td> <td>192.168.56.1</td> <td>2014-09-09 17:53:31</td> <td>2014-09-05 13:56:31</td> <td>Windows</td> <td></td>	1	Poporte and Analysis			220 KB	<b>Distant</b>	100 C 100 C	192.168.56.1	2014-09-09 17:53:31	2014-09-05 13:56:31	Windows	
File Trading       1933KB       192168561       2014.09.091422.46       2014.09.051022.46       Windows       S         File Shadowing       2234 KB       192.168.561       2014.09.09131.641       2014.09.050021.42       Windows       S         Content Aware Report       1072 KB       192.168.561       2014.09.09131.641       2014.09.050021.42       Windows       S         Admin Actions       380 KB       192.168.561       2014.09.09131.641       2014.09.050021.42       Windows       S         Onitent Aware File Shadowing       380 KB       192.168.561       2014.09.09131.641       2014.09.050021.42       Windows       S         Onitent Aware File Shadowing       380 KB       192.168.561       2014.09.09131.641       2014.09.050021.42       Windows       S         Alerts       3.08 KB       192.168.561       2014.09.09131.643       2014.09.05091.92       Windows       S       S         Directory Services       3.08 KB       192.168.561       2014.09.09131.615       2014.09.05091.92       Windows       S       S         System Maintenance       3.04 KB       192.168.561       2014.09.0912.1614       2014.09.05082.73       Windows       S       S         System Configuration       3.04 KB       192.168.561       2014.09.091		Reporta dilu Andiyala			132 KB	<b>BREAT</b>		192.168.0.198	2014-09-09 16:05:58	2014-09-05 12:08:58	Windows	
File Shadowing Content Aurane Report Content Aurane Repor		Logs Report		The Part Change Courses and the Street	132 KB	ENGINE .	And and a second second	192.168.56.1	2014-09-09 16:05:58	2014-09-05 12:08:58	Windows	🗎 😣
22348       19218551       201409-09 131841 </td <td></td> <td>File Tracing</td> <td></td> <td>President Collection and President</td> <td>19.33 KB</td> <td>ERECTOR .</td> <td>1000 Con 1000</td> <td>192.168.56.1</td> <td>2014-09-09 14:22:46</td> <td>2014-09-05 10:25:46</td> <td>Windows</td> <td>8</td>		File Tracing		President Collection and President	19.33 KB	ERECTOR .	1000 Con 1000	192.168.56.1	2014-09-09 14:22:46	2014-09-05 10:25:46	Windows	8
Content Aware File Shadowing Admin Actions       1001100       1001000       10100000       10100000       10100000       10100000       101000000       101000000       1010000000000000000000000000000000000		File Shadowing		and the second second second	22.34 KB	ENGLIST.	And and a second second	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	
Adam Actions       3.98 KB       192/168.56.1       2014/09/09/13/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/12/18.41       2014/09/09/					10.72 KB	ENGINE .	And and a second second	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	8
Online Computers       3.08 K8       192.188.56.1       2014.09-09 13:16.31       2014.09-09 09:12:82       Windows       Image: Computers         Alerts       3.43 K8       192.188.56.1       2014.09-09 13:16.31       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:13:63       2014.09-09 09:12:63       Image: Computers       Image: Co					3.98 KB	ENGLIST.		192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	
Alerts       3.43 kB       122.168.56.1       2014.09.09 13.16.33       2014.09.09 13.16.33       2014.09.09 13.16.33       2014.09.09 13.16.33       2014.09.09 13.16.31       2014.09.09 13.16.				The second s	3.08 KB	ENGINE .	And and a second second	192.168.56.1	2014-09-09 13:18:41	2014-09-05 09:21:42	Windows	
Directory Services       3.06 KB       192.168.56.1       2014.09.05 00.19.24       Windows       S         Appliance       10.72 KB       102.188.56.1       2014.09.05 00.19.24       Windows       S         System Maintenance       10.72 KB       192.185.56.1       2014.09.05 00.19.24       Windows       S         System Configuration       30.46 KB       192.185.56.1       2014.09.05 00.21.24       2014.09.05 00.21.24       Windows       S         System Configuration       30.46 KB       192.185.56.1       2014.09.05 00.21.24       Windows       S       S         System Parameters       30.46 KB       192.185.61.1       2014.09.49 12.18.14       2014.09.45 00.22.13       Windows       S       S					3.43 KB	ENGINE .	and an and a second second	192.168.56.1	2014-09-09 13:16:53	2014-09-05 09:19:53	Windows	8
Directory Services       10.72 KB       192.168.56.1       2014-09-09 13.16.15       2014-09-05 09.19.16       Windows       So         Appliance       192.168.56.1       2014-09-09 13.16.15       2014-09-05 09.19.16       Windows       So         System Maintenance       30.46 KB       192.168.56.1       2014-09-09 12.16.14       2014-09-05 08.21.14       Windows       So         System Configuration       System Parameters       Delete       Windows       So       Delete       Windows       So		Alerts		Transferration of the second	140.65 KB	and the second	Sector Control Man	192.168.56.1	2014-09-09 13:16:31	2014-09-05 09:19:32	Windows	
Appliance       192.168.56.1       2014.09-09 12.54.32       2014.09-05 08.57.32       Windows       Image: Configuration         System Configuration       30.46 K8       192.168.56.1       2014.09-09 12.18.14       2014.09-09 12.18.14       2014.09-05 08.27.32       Windows       Image: Configuration         System Parameters       Image: Configuration       Image: Configuration <t< td=""><td></td><td></td><td></td><td>THE CONTRACT CONT</td><td>3.08 KB</td><td>ETRACIO T</td><td>1000 Con 1000</td><td>192.168.56.1</td><td>2014-09-09 13:16:23</td><td>2014-09-05 09:19:24</td><td>Windows</td><td>🗎 😣</td></t<>				THE CONTRACT CONT	3.08 KB	ETRACIO T	1000 Con 1000	192.168.56.1	2014-09-09 13:16:23	2014-09-05 09:19:24	Windows	🗎 😣
Appliance       10.72 KB       192.168.56.1       2014.09-09 12.18.35       2014.09-09 08.21.36       Windows       Solution         System Maintenance       30.46 KB       192.168.56.1       2014.09-09 12.18.14       2014.09-09 08.21.36       Windows       Solution         System Configuration       System Parameters       Delete       Image: Configuration       Image: Config	J	Directory Services		The constant of the second sec	10.72 KB	STREET,		192.168.56.1	2014-09-09 13:16:15	2014-09-05 09:19:16	Windows	8
System Maintenance     10/2/X8     12/2/X8     12/2/X8     12/2/X8     2014/09-09 12/18.35     2014/09-09 12/18.35     2014/09-09 12/18.35     2014/09-09 12/18.14 <td< td=""><td></td><td>Appliance</td><td></td><td>Trappaget Transition</td><td></td><td>ENGINE T</td><td>And and a second second second</td><td>192.168.56.1</td><td>2014-09-09 12:54:32</td><td>2014-09-05 08:57:32</td><td>Windows</td><td>🗎 😣</td></td<>		Appliance		Trappaget Transition		ENGINE T	And and a second second second	192.168.56.1	2014-09-09 12:54:32	2014-09-05 08:57:32	Windows	🗎 😣
System Parameters System		Appliance		THE CONCERNMENT OF CONCERNMENT OF	10.72 KB	ETRACIO -		192.168.56.1	2014-09-09 12:18:35	2014-09-05 08:21:36	Windows	8
System Configuration     #4 results [ 20 • per page]       System Parameters     Belete	1	System Maintenance		The same provide the second	30.46 KB	ENGINE .	And and the second second	192.168.56.1	2014-09-09 12:18:14	2014-09-05 08:21:14	Windows	🖹 😣
System Parameters Delete	J		44 resi	ults [ 20 💌 per page]							N 4 12	3 🕨
System Parameters	J	System Configuration	8	Delete								
Support		System Parameters	Ø	2000								
Subbuc		Support										
	1	Support										

## 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.

	PROTECTOR	Repo	rting and Administrati	ion lool		English 🗸	Advanced
] (	Dashboard	Admin Actions				Showing departments	s: Default Departn
] [	Endpoint Management	Filter					•
E	Endpoint Rights	Results					
ł	Endpoint Settings	Administrator	Section	Action Type	Before	After	Created at +
(	Content Aware Protection (CAP)	root	Computer Settings	EDIT	P	IP	07-Mar-2014 15:35:1
	. ,	root	Computer Rights	EDIT	Computer Name	Computer Name	07-Mar-2014 15:34:5
1	Mobile Device Management	root	Content Aware Policies	POLICY APPLIED TO	Policy Name	Policy Name	07-Mar-2014 15:31:4
	off) T 0	root	Content Aware Protection (CAP)	CREATE			07-Mar-2014 15:30:4
(	Offline Temporary Password	root	User Authentification	SIGN OUT		User Sign Out	07-Mar-2014 15:27:5
	Reports and Analysis	root	Administrators	CREATE		Username	07-Mar-2014 15:27:4
	toporto ana / maryolo	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
1	Logs Report	root	Device Rights	EDIT	Device Name	Device Name	07-Mar-2014 15:10:5
	File Tracing	root	Device Rights	EDIT	Device Name	Device Name	07-Mar-2014 15:10:4
	File Shadowing	root	Device Rights	EDIT	Device Name	Device Name	07-Mar-2014 15:10:3
	Content Aware Report Admin Actions	root	Content Aware Regex	CREATE		Regular Expression Name	07-Mar-2014 15:00:4
	Online Computers	root	Client Software	DOWNLOAD		Downloaded Endpoint Protector Client Sof	07-Mar-2014 14:59:2
	Online Users	root	User Authentification	SIGN IN		User Logging	07-Mar-2014 14:58:5
	* * *	root	User Authentification	SIGN IN		User Logging	07-Mar-2014 14:35:1
1	Alerts	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
l	Directory Services	root	Client Software	DOWNLOAD		Downloaded Endpoint Protector Client Sof	07-Mar-2014 14:16:0
	Appliance	root	User Authentification	SIGN IN		User Logging	07-Mar-2014 14:14:3
	opininee	root	Content Aware Regex	EDIT	Regular Expression Name	Regular Expression Name	07-Mar-2014 14:08:2
5	System Maintenance	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
5	System Configuration	root	Content Aware Protection (CAP)	EDIT			07-Mar-2014 14:02:2
	Denter Deneration	root	Configuration	signedEnvelope		Certificate Signing Request (CSR)	07-Mar-2014 14:01:2
-	System Parameters	root	User Authentification	SIGN IN		User Logging	07-Mar-2014 13:55:5
	Support	root	User Authentification	SIGN IN		User Logging	07-Mar-2014 13:50:2
		root	User Authentification	SIGN IN		User Logging	07-Mar-2014 13:40:3
		root	User Authentification	SIGN IN		User Logging	07-Mar-2014 13:37:0
		root	Administrators	EDIT	First Name	Email	07-Mar-2014 06:20:5
		root	User Authentification	SIGN IN		User Logging	07-Mar-2014 06:20:2
		root	User Authentification	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

	Dashboard	Online Computers							Show all	departme
]	Endpoint Management	Results								
3	Endpoint Rights	Name▲	User Logged	Domain	Workgroup	IP	MAC Address	Location	Status	Actions
	Endpoint Settings	10000-+++4108501					1020-0020-0048-1		Online	E
1	Offline Temporary Password	-				1000001000			Online	
	onine remporary rassifiera	2 computers onli	ine [ 20 💌 per page]							
	File Tracing File Shadowing <u>Online Computers</u> Online Users Online Devices									
2	File Shadowing Online Computers Online Users Online Devices Statistics Graphics System Alerts									
5	File Shadowing <u>Online Computers</u> Online Users Online Devices Statistics Graphics									
5	File Shadowing Online Computers Online Users Online Devices Statistics Graphics System Alerts									
) ) )	File Shadowing Online Computers Online Users Online Devices Statistics Graphics System Alerts Directory Services									
P	File Shadowing Online Computers Online Devices Statistics Graphics System Alerts Directory Services System Maintenance									

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.

#### 85 | Endpoint Protector | User Manual

	Dashboard	Online Users					Show all departmen
Ţ	Endpoint Management	Results					
the set	Endpoint Rights	Username	Name	Computer Name	IP	Connecte	d Device
X	Endpoint Settings					none	
		THE OWNER OF THE OWNER OWNER OF THE OWNER OWNER OWNER OWNER OWNER OWNER OWNE OWNE OWNE OWNE OWNE OWNE OWNE OWNE				none	
	Offline Temporary Password	2 users online [	[ 20 💌 per page]				
	Reports and Analysis						
	File Tracing File Shadowing Online Computers <u>Online Users</u>						
	File Shadowing Online Computers						
	File Shadowing Online Computers <u>Online Users</u> Online Devices Statistics Graphics						
	File Shadowing Online Computers Online Users Online Devices Statistics Graphics System Alerts						
	File Shadowing Online Computers <u>Online Users</u> Online Devices Statistics Graphics System Alerts Directory Services						
	File Shadowing Online Computers Online Devices Statistics Graphics System Alerts Directory Services System Maintenance						

## 8.9. Online Devices

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

		Rej	porting an	d Administ	ration Tool				English 💌 🤇	Ac	Ivanced Se
	Dashboard	Connected De	evices							Show all de	epartmer
p	Endpoint Management	Results									
	Endpoint Rights	Computer Name *	User Logged	IP	Device Type	Device Name	VID	PID	Serial No		Actions
	Endpoint Settings	HARLING CO.	-		Card Reader Device (SCSI)	NVIDIA nForce Serial ATA Controller	1000	-	CONTRACTOR OF THE OWNER		ES
	off: T 5 1	Hallower .		Concession, Prant	Internal Floppy Drive	(Standard floppy disk drives)					ES
6	Offline Temporary Password	THE OWNER OF T			Serial Port	Communications Port (COM3)			10 million - 44 million - 55 million		
1	Reports and Analysis	100000000000000000000000000000000000000	-		Serial Port	Communications Port (COM1)			10 M 2 P 2000		
		HARDON C	-	100000000000	USB Storage Device	TS1GJFV30	1000	-			
	Logs Report	THE OWNER OF THE OWNER OWNER OF THE OWNER OWNE OWNER OWNE	-	Concerning 1 States	USB Storage Device	USB_SD_READER	-	-			
	File Tracing File Shadowing			Constraint for	Internal CD or DVD RW	ASUS DRW-1814BL			The second s	10000	EQ
	Online Computers			10000	USB Storage Device	USB_FLASH_DRIVE	10000	-	A TEMPERATING		EQ
	Online Users	THE OWNER OF THE OWNER OWNER OF THE OWNER OWNE			USB Storage Device	Port_#0004.Hub_#0004	100000-0	1000	Sand, Tanke ordered.		
	Online Devices Statistics Graphics	9 devices co	nnected [ 2	o 💽 perpag	ge]						
5	System Alerts										
]	Directory Services										
	System Maintenance										
ķ	System Configuration										
-	System Parameters										
)	Support										

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.

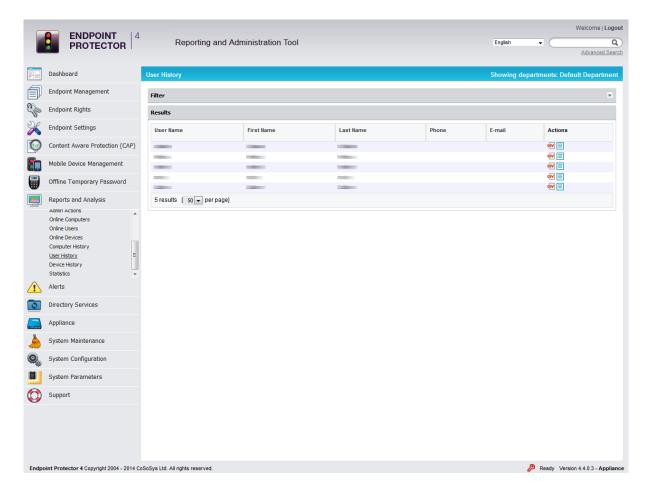
#### 8.10. Computer History

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.

Dashboard	Computers History					Showing departments	: Default Depart
Endpoint Management	Filter						
Endpoint Rights	Results						
Endpoint Settings	Computer Name	Domain 1	WorkGroup	IP	Computer Location	Last Time Online 👻	Actions
Content Aware Protection (CAP)		v	WORKGROUP	192.168.0.21		07-Mar-2014 17:17	<u>مە</u>
,,			WORKGROUP	192.168.0.20		07-Mar-2014 17:05	<u>هب</u>
Mobile Device Management	Contraction of Street Streets		WORKGROUP	192.168.0.89		07-Mar-2014 16:52	65V 📃
060-			WORKGROUP	192.168.0.20		07-Mar-2014 05:32	6V 📃
Offline Temporary Password	COMPANY OF THE OWNER.	V	WORKGROUP	192.168.0.20		07-Mar-2014 05:32	(SV 📄
Online Users Online Devices <u>Computer History</u> User History Device History Statistics Alerts							
Online Devices Computer History User History Device History Statistics Alerts Directory Services							
Online Devices <u>Computer History</u> User History Device History Statistics Alerts							
Online Devices Computer History User History Device History Statistics Alerts Directory Services							
Online Devices Computer History User History Device History Statistics Alerts Directory Services Appliance							
Online Devices Comouter History User History Statistics Alerts Directory Services Appliance System Maintenance							
Online Devices Computer History User History Device History Statetics Alerts Directory Services Appliance System Maintenance System Configuration							

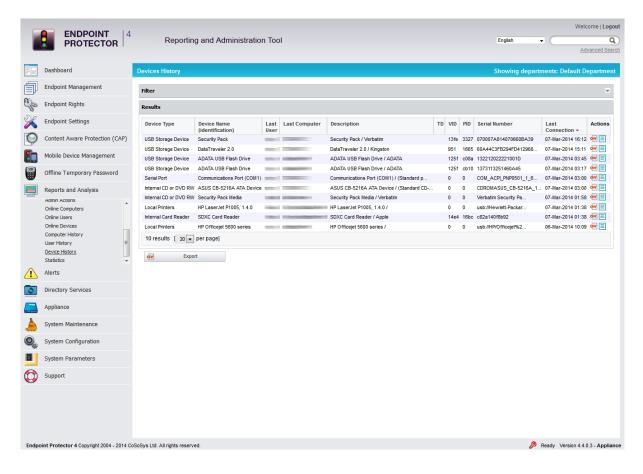
#### 8.11. User History

This module shows all users 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 User log" will show the Logs Report page filtered for the respective User.



#### 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.



#### 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.

						Welcome	Super Administrator   Logout	
		Reporting and	Administration Tool			English 💌	٩)	
-							Advanced Search	
	Dashboard	Statistics					Show all departments	
Í	Endpoint Management	Search Criteria						
20	Endpoint Rights	Report:	Most Active (Device Connection					
X	Endpoint Settings	Period:						
	Offline Temporary Password	On: Q Apply filter	Computers 💌					
	Reports and Analysis	Results						
	Logs Report File Tracing File Shadowing	Computer Name	Default User	Group	IP	Total Connections		
	Online Computers Online Users				COLUMN AND DESIGN	13		
	Online Devices	Contraction of the second s			2000 C	3		
	Statistics Graphics	2 results						
	System Alerts							
0	Directory Services							
	System Maintenance							
0	System Configuration							
	System Parameters							
0	Support							
Endp	oint Protector Copyright 2004 - 2011 Co	SoSys Ltd. All rights reserved.				S	ystem 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		
*Note: The test e-mail will be sent	to	
Hostname:	smtp.gmail.com	Example: smtp.cososys.com
SMTP Port:	465	Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication:		
Username:		Example: Your full email address (including @cososys.com).
Password:	•••••	Your SMTP password.
Encryption Type:	SSL 💌 Example: None, SS	L or TLS/STARTTLS.
Send test e-mail to my account:		
Proxy Server Settings		
IP:		
Username:		

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".

PROTECTOR	4 Reporting and	Administration Tool		English  Advanced Se
Dashboard	List of Administrators			Show all departmen
Endpoint Management	Filter			
Endpoint Rights	Results			
Endpoint Settings	User Name	Created at	Last Login	Actions
Offline Temporary Password	1000		01-Jul-2011 11:11	
	Concept of Concepts	8 June 2011 12:53	08-Jun-2011 12:55	
Reports and Analysis	-	8 June 2011 12:59	08-Jun-2011 13:02	☑ 💷 😣
	-	8 June 2011 16:25		
System Alerts		23 June 2011 15:28	23-Jun-2011 15:34	[] ≡ ⊗
Directory Services	5 results [ 50 💌 per pag	je]		
System Maintenance	Gereate			
System Configuration				
System Configuration Client Software System Administrators System Departments System Policies				
Client Software System Administrators System Departments System Policies System Verses System Lierses				
Client Software <u>System Administrators</u> System Departments System Security System Policies System Settings				
Client Software <u>System Administrators</u> System Departments System Security System Policies System Licenses EasyLock Software				

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

#### ℤ == ⊗

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

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool		English	Welcome	Logout Q ed Search
	Dashboard	List of System Alerts				
	Endpoint Management	Results				
Cla	Endpoint Rights	Name	Event		Actions	
X	Endpoint Settings	Client Uninstall cc device control 100 test	Client Uninstall Device Control – Logs Amount		28 28	
0	Content Aware Protection (CAP)	APNS expire	APNS certificate		Ľ⊗	
	Mobile Device Management	3 results [ so v per page]				
88	Offline Temporary Password	Create				
	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					
0	Directory Services					
	Appliance					
×	System Maintenance					
	System Configuration					
	System Parameters					
	Support					
Endpo	pint Protector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.			Ready Vers	ion 4.4.0.4

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

There are several types of alerts available as shown below:

Create System Alert								
APNS certificate								
APNS certificate								
Updates and Support Endpoint Licenses								
Client Uninstall Server Disk Space Device Control – Logs Amount Content Aware – Logs Amount								

**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)

Endpoint Management       Exeluits         Endpoint Rights       Center       Computer       Group       Device Type       Device       Memory       Actions         Any       My testing Computer 1       Any       Any       Any       Contends       If is a strain 1       If is a strain 2       If is a strain 2 <th>C</th> <th>Dashboard</th> <th>List of Alerts</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>Show all dep</th>	C	Dashboard	List of Alerts						Show all dep
Image: Setting in the setting in the set is set in the set in the set is set in the set in the set in the set in the set is set in the set in the set in the set is set in the set is set in the set	E	Endpoint Management							
Any My My Any Any Any Bocked   Poble Device Management   Offline Temporary Password   Offline Temporary Password   Offline Temporary Password   Peports and Analysis   Alerts   Define Attriss   System Maintenance   System Configuration   System Configuration	E	Endpoint Rights	Client	Computer	Group	Device Type	Device	Event	Actions
Any       Any       Any       Any       Any       Any       Bocked         Mobile Device Management       Create	E	Endpoint Settings	Any	My testing Computer 1	Any	Anv	Any	Connected	<b>R</b> Ø
Wobile Device Management   Offline Temporary Password   Reports and Analysis   Alerts   Define Ontert Annere Alerts Astrony   Define Content Annere Alerts Hatory   Directory Services   Applance   System Maintenance   System Configuration   System Parameters								Blocked	
Offline Temporary Possword       Reports and Analysis       Aterts       Define Adrits       before Order Aware Adrits betopy       Context Aware Adrits betopy       Context Aware Adrits betopy       Directory Services       Applance       System Maintenance       System Configuration       System Porameters	0	Content Aware Protection (CAP)	2 results [ 20	n 💽 per page]					
Offline Temporary Password       Reports and Analysis       Alerts       Define Content Annee Alerts Define Content Annee Alerts Define Content Annee Alerts Alert Hatory       Doffine Vortes       Appliance       System Maintenance       System Configuration       System Parameters	h	Mobile Device Management							
Reports and Analysis       Alerts       Bodhe Adratis       Bodhe Content Anare Alerts Istory       Director Services       Orther Maintenance       System Maintenance       System Configuration       System Parameters			e ur	reate					
Alerts       Define AttAs       Define Context Aware Alerts       Define MOX Alerts       Are Is Natory       Context Aware Alerts Hatory       DO rectory Services       Jopinance       System Maintenance       System Configuration       System Parameters	0	Omine Temporary Password							
Zefine Adrts       Define Contern Xavere Aderts       Define MOM Aderts       Alerts History       Contern Xavere Alerts History       DD rectory Services       Appliance       System Maintenance       System Configuration       System Parameters	1								
Adres Alerts       Define KOMARY Alerts       Define KOMARY Alerts       Adres History       Content Anare Alerts History       Directory Services       Appliance       System Maintenance       System Configuration       System Parameters	F	Reports and Analysis							
Define Content Avarea Alerts       Define WOM Avarea Alerts Hatory       DOr ectory Services       Appliance       y System Maintenance       y System Configuration       System Paremeters	5								
MA Mets Hstory Directory Services Appliance System Maintenance System Configuration	P								
Appliance       System Maintenance       System Configuration       System Farameters		Alerts Define Alerts Define Content Aware Alerts Define MDM Alerts Alerts History							
System Maintenance System Configuration System Parameters		Alerts Define Alerts Define Content Aware Alerts Define MDM Alerts Alerts History Content Aware Alerts History							
System Configuration System Parameters		Alerts Define Alerts Define Content Aware Alerts Define MDM Alerts Alerts History Content Aware Alerts History MDM Alerts History							
System Parameters		Alerts Define Alerts Define Content Avwere Alerts Define MM Alerts Alerts Hattory MOW Alerts Hattory MOW Alerts Hattory Directory Services							
		Alerts Define Alerts Define Content Aware Alerts Define NDM Alerts Alerts History Content Aware Alerts History NDM Alerts History Directory Services Appliance							
Support		Alerts Define Alerts Define Content Aware Alerts Define DDM Alerts Alerts History Content Aware Alerts History MDM Alerts History Directory Services Appliance System Maintenance							
		Alerts <u>Define Alerts</u> Define Content Aware Alerts Define Content Aware Alerts Alerts History Content Aware Alerts History MDM Alerts History Directory Services Appliance System Maintenance System Configuration							

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

+ Create	]	
Create Alert		Show all department
Alert Name		
Alert Name:	Alert Test	
Alert Entities		
Groups 🕀	Computers 🕀 Any	
Users 🕀		
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.

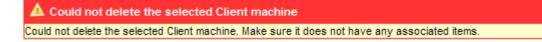
You can also select one or more administrators to receive the same notification(s). This is useful in case there is more than one administrator for Endpoint Protector.

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".

(+) Create			
Create Alert			Show all departments
Content Aware Alert Name			
Content Aware Alert Name:	Alert Test #2		
Content Aware Alert Entities			
Groups 🕀	Comput Any	iters 🕀	
Users 🕀 Any			
Content Aware Alerts fields			
Department:	Default Department		
Content Policy:	PDF Test		
Event:	Content Threat Detected	•	
Alert administrators			
	(root)		

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.

	ENDPOINT 4 PROTECTOR	Reporting and Administ	ration Tool			English	Welcome   Logout
	Dashboard	Create Mobile Device Management A	Vert				Show all departments
Í	Endpoint Management	Alert fields					
0	Endpoint Rights	Type:		Any 💌			
X	Endpoint Settings	Device Name:		Any			
0	Content Aware Protection (CAP)	Event:		Uninstall App 💌			
8	Mobile Device Management	Alert administrators					
	Offline Temporary Password	Administrators:		☐ (root) ☐ (Marketing-admin) ☐ (Financial-admin)			
	Reports and Analysis						
	Alerts						
	Define Alerts Define Content Aware Alerts <u>Define MDM Alerts</u> Alerts History Content Aware Alerts History MDM Alerts History	*Note: In order to have a complete list, plea	se make sure administrato	ors have their e-mail addresses set up from Syst	em Configuration > System Administrators > Edit Info.		
0	Directory Services	Save Save	Save Add	▲ Back			
	Appliance						
٨	System Maintenance						
0	System Configuration						
	System Parameters						
0	Support						
	oint Protector 4 Copyright 2004 - 2013 C	SoSys Ltd. All rights reserved					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.

	ENDPOINT 4					Welcome   Logout
	PROTECTOR 4	Reporting and Administration 1	Fool		English 🗸 🤇	٩
-						Advanced Search
	Dashboard	System Alerts History				
	Endpoint Management	Filter				
20	Endpoint Rights	Results				
X	Endpoint Settings	System Alert Name	System Event	System Event Option	Created at 🕶	
6	Content Aware Protection (CAP)	Client Uninstall cc	Client Uninstall	-	6 September 2014 12:00	
		device control 100 test	Device Control – Logs Amount	100 rows	5 September 2014 0:00	
	Mobile Device Management	Client Uninstall cc	Client Uninstall	-	4 September 2014 12:00	
12712		Client Uninstall cc	Client Uninstall	-	2 September 2014 0:00	
88	Offline Temporary Password	4 results [ 50 - per page]				
	Reports and Analysis	O Delete History				
	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					
0	Directory Services					
_,	Appliance					
×	System Maintenance					
Ø	System Configuration					
	System Parameters					
$\bigcirc$	Support					
Endpo	pint Protector 4 Copyright 2004 - 2014 Co	oSoSys Ltd. All rights reserved.				Ready Version 4.4.0.4

#### 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.

Endpoint Management       Feter         Endpoint Rights       Results         Endpoint Stattings       User Computer Device Type Device       Event Created at +         Content Aware Protection (CAP)       USB Strage Device       Mass Strage Device       Connected 10 September 2014 16.20         Mobile Device Management       USB Strage Device       Mass Strage Device       Connected 10 September 2014 16.30         Offline Temporary Password       Reports and Analysis       Bustooth       Bustooth       Bustooth       Device 10 September 2014 16.30         Alerts       Pad       Pad       Pad       Pad       Pad       Pad       Pad       Connected 10 September 2014 16.32         Define System Alerts       Pad	ashboard	Alerts Hist	tory				
Endpoint Settings       User       Computer       Device Type       Device       Event       Created at +         Content Aware Protection (CAP)       USB Storage Device       Mass Storage Device       Connected       10 September 2014 15:50         Mobile Device Management       Sarial XTA Controler       Hat(R) 7 Series/C216 Chipset Famly SA       Connected       10 September 2014 15:50         Offline Temporary Password       Buetooth       Buetooth       Buetooth       Buetooth       Buetooth         Aftrs       WFi       Wreass Network Adapter (802:11 ab/gh       Connected       10 September 2014 15:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define System Alerts Hotory       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define System Alerts Hotory       Pad       Pad       Pad       Connected       10 September 2014 11:40 <th>ndpoint Management</th> <th>Filter</th> <th></th> <th></th> <th></th> <th></th> <th></th>	ndpoint Management	Filter					
Content Aware Protection (CAP)       USB Storage Device       Ass Storage Device       Connected       10 September 2014 15:50         Mobile Device Management       WFi       Wetesk Network Adapter (60:11 abig/m       Connected       10 September 2014 15:50         Offline Temporary Password       Buetooth       Buetooth       Device       Connected       10 September 2014 15:50         Aferts       WFi       Wreess Network Adapter (60:11 abig/m       Connected       10 September 2014 15:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:42         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:42         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:42         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:42         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:41         Define Kints       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define Kints	ndpoint Rights	Results					
Content Aware Protection (CAP)       Serial ATA Controlser       Intel(R) 7 Series/C216 Chipset Famly SA       Connected       10 September 2014 15:50         Mobile Device Management       WFi       Wreas Network Adapter (802:11 abr)m       Connected       10 September 2014 15:50         Offline Temporary Password       Bluetooth       Bluetooth       Bluetooth Device       Connected       10 September 2014 15:24         Alerts       WFi       Wreass Network Adapter (802:11 abr)m       Connected       10 September 2014 15:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:24         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define System Alerts Hotory       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define Content Aware Alerts Hotory       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define Content Aware Alerts Hotory       Pad       Pad       Pad       Connected       10 September 2014 11:40         Define Content Aware Alerts Hotory       Pad       Pad       Pad       Connected </th <th>ndpoint Settings</th> <th>User</th> <th>Computer</th> <th>Device Type</th> <th>Device</th> <th>Event</th> <th>Created at -</th>	ndpoint Settings	User	Computer	Device Type	Device	Event	Created at -
Mobile Device Management       Serial ATA Controler       HetR) 7 Series/C216 Chyset Famly SA       Connected       10 September 2014 155.0         Offline Temporary Password       Buetooth Device       Connected       10 September 2014 155.0         Reports and Analysis       Buetooth Device       Connected       10 September 2014 155.0         Alerts       WFi       Wriess Network Adapter (602.11 abig/m)       Connected       10 September 2014 152.4         Alerts       Pad       Pad       Pad       10 September 2014 115.2         Define System Alerts       Pad       Pad       10 September 2014 115.2         System Alerts       Pad       Pad       10 September 2014 115.2         Define System Alerts       Pad       Pad       10 September 2014 115.2         Define Kerts       Pad       Pad       Pad       10 September 2014 11.4         Define Kerts       Pad       Pad       Pad       10 September 2014 11.4         Define Kerts       Pad       Pad       Pad       10 September 2014 11.4         Define Kerts       Pad       Pad       Pad       10 September 2014 11.4         Define Kerts Nare Alerts       Pad       Pad       10 September 2014 11.4       10 September 2014 11.4         Define Kerts Nare Alerts Hotory       P	ontant Awara Protection (CAP)	refere:	Talinero:	USB Storage Device	Mass Storage Device	Connected	10 September 2014 16:29
Mobile Device Management       Serial ATA Controller       Het(R) 7 Series/C216 Chapset Famy SA       Connected       10 September 2014 15:50         Offline Temporary Password       WFi       Wriess Metwork Adapter (002.11 a brig/m       Connected       10 September 2014 15:50         Reports and Analysis       Buetooth       Buetooth Device       Connected       10 September 2014 15:24         Alerts       WFi       Wriess Metwork Adapter (002.11 a brig/m       Connected       10 September 2014 15:24         Define System Alerts       Pad       Pad       Connected       10 September 2014 11:42         System Alerts       Pad       Pad       Connected       10 September 2014 11:42         Define System Alerts       Pad       Pad       Connected       10 September 2014 11:42         Define Alerts       Pad       Pad       Connected       10 September 2014 11:40         Define Alerts       Pad       Pad       Connected       10 September 2014 11:40         Define Alerts       Pad       Pad       Connected       10 September 2014 11:40         Define Alerts       Pad       Pad       Connected       10 September 2014 11:40         Define Marke Natry       Pad       Pad       Connected       10 September 2014 11:40         Define Marke Natry	ontent Aware Protection (CAP)	ADDRESS:	Contract Contracts				
Offline Temporary Password     WFi     Wrekes Network Adapter (802 11 ablgh     Connected     10 September 2014 15.37       Reports and Analysis     Buetooth     Buetooth     Buetooth     Detwork (500 series)     Connected     10 September 2014 15.37       Alerts     Buetooth     Buetooth     Buetooth     Buetooth     Detwork (500 series)     Connected     10 September 2014 15.24       Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define Krist Netory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Content Aware Alerts Netory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Krist Netory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Krist Netory     Pad     Pad     Pad     Connected     10 September 2014 11.40 </td <td>Iohile Device Management</td> <td>Interior:</td> <td>COMPANY STATISTICS</td> <td>Serial ATA Controller</td> <td></td> <td></td> <td></td>	Iohile Device Management	Interior:	COMPANY STATISTICS	Serial ATA Controller			
Reports and Analysis       Local Printers       HP Offcagle 5600 series       Connected       10 September 2014 1524         Alerts       Buetooth       WiFi       Wieses Network Adapter (802.11 abig/m       Connected       10 September 2014 1524         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 1124         Define System Alerts       Pad       Pad       Connected       10 September 2014 1114         Define System Alerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Pad       10 September 2014 1114         Directory Services       Pad       Pad       Pad       10 September 201	iobile betree Hanagement	MARKET.	Contractory of the second	WiFi		Connected	10 September 2014 15:37
Reports and Analysis       Local Printers       HP Offcagle 5600 series       Connected       10 September 2014 1524         Alerts       Buetooth       WiFi       Wieses Network Adapter (802.11 abig/m       Connected       10 September 2014 1524         Define System Alerts       Pad       Pad       Pad       Connected       10 September 2014 1124         Define System Alerts       Pad       Pad       Connected       10 September 2014 1114         Define System Alerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Connected       10 September 2014 1114         Define Nerts       Pad       Pad       Pad       10 September 2014 1114         Directory Services       Pad       Pad       Pad       10 September 201	ffline Temporary Password	MARKET.	linguisterers:	Bluetooth	Bluetooth Device	Connected	10 September 2014 15:37
Reports and Analysis     Buetooth     Buetooth     Buetooth     Buetooth     Connected     10 September 2014 15.24       Alerts     WFI     Wretess Network Adapter (802.11 abligh     Connected     10 September 2014 15.24       Define System Alerts System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.24       Define System Alerts System Alerts Network     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts System Alerts Network     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Name Alerts Content Aware Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Note Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40 </td <td>,</td> <td>inter-</td> <td>Concession (Proc.)</td> <td>Local Printers</td> <td>HP Officeiet 5600 series</td> <td>Connected</td> <td></td>	,	inter-	Concession (Proc.)	Local Printers	HP Officeiet 5600 series	Connected	
Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.42       System Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Content Aware Alerts     Pad     Pad     Connected     10 September 2014 11.40       Define Content Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Content Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define MOM Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       System Maintenance     System Configuration     Pad     Pad     Pad     208 results ( Dire per page)	eports and Analysis	inter-	Concentration of the second				
Alerts     Pad     Pad     Connected     10 September 2014 11.42       Define System Alerts     Pad     Pad     Connected     10 September 2014 11.42       System Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.42       Define Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Content Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Mont Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Mont Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Mont Aware Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Define Mont Aver Alerts Hotory     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Connected     10 September 2014 11.40       System Maintenance     Pad     Pad     Pad     Connected     10 September 2014 11.40       208 results ( Tort) – per page)     System Configuration     Delete History     Ext 4 1		inter-	Concerning of the second	WIFI	Wireless Network Adapter (802.11 a/b/g/n	Connected	10 September 2014 15:24
Define System Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts     Alerts History     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Context Aware Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Marker Alerts     Pad     Pad     Pad     Connected     10 September 2014 11.40       Define Marker Alerts     Pad     Pad     Connected     10 September 2014 11.40       Define Marker Alerts     Pad     Pad     Connected     10 September 2014 11.40       Define Marker Alerts     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       System Maintenance     System Configuration     Pad     Pad     Pad     208 results [ 20 r per page]	lerts	MARKET.	TRADITION OF THE OWNER	iPad			
System Acts Hatory     Pad     Pad     Connected     10 September 2014 1140       Define Adrets Hatory     Pad     Pad     Pad     Connected     10 September 2014 1140       Acts Hatory     Pad     Pad     Pad     Connected     10 September 2014 1140       Define Content Aware Acts Hatory     Pad     Pad     Pad     Connected     10 September 2014 1140       Define Content Aware Acts Hatory     Pad     Pad     Pad     Connected     10 September 2014 1140       Define MM Acts Hatory     Pad     Pad     Pad     Connected     10 September 2014 1140       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 1140       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 1140       System Maintenance     System Configuration     Pad     Pad     Pad     Pad		MARKS:	lighterer.	iPad	iPad	Connected	10 September 2014 11:40
System Address     Pad     Pad     Pad     00       Define Adress     Adress Hetory     Pad     Pad     00       Define Adress     Pad     Pad     00     00       Define Adress     Pad     Pad     00     00       Define Adress     Pad     Pad     00     00       Define Adress Hetory     Pad     Pad     00     00       Directory Services     Pad     Pad     Pad     00       Appliance     Pad     Pad     Pad     00     00       System Maintenance     System Maintenance     Pack     00     00		princ:	TRADITION OF THE OWNER	iPad	iPad	Connected	10 September 2014 11:40
Define RMrts     Pad     Pad     Pad     10 September 2014 11.40       Define Content Aware Alerts Hotory     Pad     Pad     Pad     10 September 2014 11.40       Define CM Marts     Pad     Pad     Pad     10 September 2014 11.40       Define KM Marts     Pad     Pad     Pad     10 September 2014 11.40       Define KM Marts     Pad     Pad     Pad     10 September 2014 11.40       Directory Services     Pad     Pad     Connected     10 September 2014 11.40       Appliance     Pad     Pad     Pad     Connected     10 September 2014 11.40       208 results [ 20 w per page]     V     V     1 2 3 4 5		TRACE.	Taliforer:	iPad	Pad	Connected	
Define Control Aware Alerts Control Aware Alerts Control Aware Alerts Control Aware Alerts History     Pad     Pad     Connected     10 September 2014 11:40       Define Control Aware Alerts History     Pad     Pad     Connected     10 September 2014 11:40       Define Control Aware Alerts History     Pad     Pad     Connected     10 September 2014 11:40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11:40       Appliance     Pad     Pad     Pad     Connected     10 September 2014 11:40       System Maintenance     System Configuration     Pad     Pad     Pad     Connected     10 September 2014 11:40		princ:	TRADITION OF THE OWNER				
Context Aware Aler's Hotory     Pad     Pad     Connected     10 September 2014 1140       Define MDM Aler's     Pad     Pad     Pad     00 September 2014 1140       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 1140       Appliance     Pad     Pad     Pad     Connected     10 September 2014 1140       System Maintenance     System Configuration     Pad     Pad     Pad     Connected     10 September 2014 1140		MARKET:	TRACTORES	iPad	iPad	Connected	
Define MOM Alerts MOM Alerts Notry MOM Alerts Notry Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Appliance     Pad     Pad     Pad     Connected     10 September 2014 11.40       System Maintenance     System Configuration     Connected     10 September 2014 11.40     Connected     10 September 2014 11.40		MARKET.	Maintener:	iPad	iPad	Connected	10 September 2014 11:40
Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Directory Services     Pad     Pad     Connected     10 September 2014 11.40       Appliance     Pad     Pad     Connected     10 September 2014 11.40       System Maintenance     System Configuration     Deleter History     Back		1990	Contractory of the second		iPad	Connected	10 September 2014 11:40
Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11.40       Appliance     Pad     Pad     Pad     Connected     10 September 2014 11.40       System Mointenance     208 results [20] per page]     Image: Connected     10 September 2014 11.40       System Configuration     Dekete History     Eack		princ:	TRADITION OF THE OWNER	iPad	iPad	Connected	10 September 2014 11:40
Directory Services     Pad     Pad     Pad     Connected     10 September 2014 11:40       Appliance     Pad     Pad     Pad     Connected     10 September 2014 11:40       System Maintenance     208 results ( 20 - per page)     Image: Connected     12 24 5       System Configuration     Delete History     Back		MARKS:	TRESPONDENCE:	iPad	Pad	Connected	
Appliance     Pad     Pad     Connected     10 September 2014 11:40       208 results [ @] per page]     It is a september 2014 11:40     It is a september 2014 11:40       System Maintenance     It is a september 2014 II:40     It is a september 2014 11:40       System Configuration     It is a september 2014 II:40     It is a september 2014 II:40	irectory Services	MARKET.	TRADITION OF THE OWNER	Pad	Pad		
System Maintenance     200 results [ 200 per page]       System Configuration     Delete History		MARKET:	TRACTORES	iPad	iPad	Connected	
System Configuration	ppliance	208 resi	ults [ 20 💌 per page]				₩
System Configuration	ystem Maintenance		Dalata Wistow	Part			
System Parameters	ystem Configuration	$\otimes$	Delete History	E Back			
	ystem Parameters						
Support	upport						
Support							

#### 9.7. Content Aware Alerts History

A history of the content aware alerts is kept in this tab for later auditing. Each event that triggers a content aware 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.

	<b>ENDPOINT</b> <b>PROTECTOR</b> 4	Reporting and A	Administration	1001				English 🗸 🤇	Advanc	ed
	Dashboard	Content Aware Alerts	History							
	Endpoint Management	Filter								Ŧ
P	Endpoint Rights	Results								
K	Endpoint Settings	Event Name	Client Computer	Client User	Destination Type	Destination	File Name	Content Policy	Item Type	N
2	Content Aware Protection (CAP)	Content Threat Detected	Richards 1	Transis.	date	Storage Device	Non-security of the second	Tony 1	Undefined Content	Ji
2		Content Threat Blocked		Transie II.	screen-capture			Undefined Policy	Predefined Content	
٦.	Mobile Device Management	Content Threat Blocked		Transien :-	screen-capture			Undefined Policy	Predefined Content	
		Content Threat Blocked	AND STREET, STREET, ST.	Transie In	Web Browser	Mozilla Firefox	The second s	RO	File Type	a
	Offline Temporary Password	Content Threat Blocked		Training:	Web Browser	Mozilla Firefox	The second state of the second state state of the second state of	RO	File Type	a
		Content Threat Blocked		Training	Web Browser	Mozilla Firefox	These states and the second second second	RO	File Type	a
m.	Reports and Analysis	Content Threat Blocked		TRACT.	file-type	explorer	E. S. Canada manage Construction	RO	File Type	a
		Content Threat Blocked	AND THE COMPANY	TRACT I	file-type	explorer	Street Charles Contract Constraints	RO	File Type	a
	Alerts	Content Threat Blocked	AND STREET, STREET, ST.	Transie	file-type	explorer	Barris Canada Canada Canada Sana	RO	File Type	a
_		Content Threat Blocked		Series -	file-type	explorer	State of the second	RO	File Type	a
	Define System Alerts System Alerts History	Content Threat Blocked		Training:	file-type	explorer	Contraction of the second s	RO	File Type	a
	Define Alerts	Content Threat Blocked		Table 1	file-type	explorer	Contraction of the second s	RO	File Type	a
	Alerts History	Content Threat Blocked		Constant of	file-type	explorer	Contract Contractor Contractor Contractor	RO	File Type	a
	Define Content Aware Alerts	Content Threat Blocked		TRACT -	file-type	explorer	States and the second	RO	File Type	a
	Content Aware Alerts History	Content Threat Blocked		Training	file-type	explorer	State of the second	RO	File Type	a
	Define MDM Alerts	Content Threat Blocked		COMPANY.	file-type	explorer	Constant Constant Constant Constant	RO	File Type	a
	MDM Alerts History	Content Threat Blocked		TRANSIC:	file-type	explorer	State of the second	RO	File Type	a
_		Content Threat Blocked		TRACT.	file-type	explorer	Rental Constant Constant Constant	RO	File Type	a
9	Directory Services	Content Threat Blocked	and the second second	TRANSPORT OF	file-type	explorer	BUTTER, TRANSFORMER, TAXABLE PARTY	RO	File Type	а
		Content Threat Blocked	AND CONTRACTOR OF	TRACT.	file-type	explorer		RO	File Type	a
	Appliance	Content Threat Blocked	ALL STRUCTURE OF	Training:	E-mail	Mozilla Thunderbird	ALTERNAL COLLEGE MARK	test for exceptions from sys policies	File Type	in
1	Contrast Martinesson	Content Threat Blocked	AND DESCRIPTION OF	CONTRACT.	USB Storage Device	DATATRAVELER_2.0	Concernation .	test for exceptions from sys policies	File Type	te
Kr.	System Maintenance	Content Threat Blocked	A CONTRACTOR OF THE OWNER OF	Training .	Web Browser	Mozilla Firefox	The support of the second second	test for exceptions from sys policies	File Type	te
*	System Configuration	Content Threat Blocked	AND TRACTOR	Table 1	Web Browser	Mozilla Firefox	The companying of the second second	test for exceptions from sys policies	File Type	te
¥.	System comgutation	Content Threat Blocked	ALL CONTRACTOR	Transien :	Web Browser	Mozilla Firefox	The construction of the construction	test for exceptions from sys policies		te
	System Parameters	Content Threat Blocked		TRACT.	Web Browser	Mozilla Firefox	Contraction of the second s	test for exceptions from sys policies	File Type	te
1.1.1	e joten i urumetero	Content Threat Blocked		Training	Web Browser	Mozilla Firefox		test for exceptions from sys policies		te
	Support	Content Threat Blocked		Table	Web Browser	Mozilla Firefox	TABLE REAL PROPERTY AND INCOME.	test for exceptions from sys policies		a
9		Content Threat Blocked		Training:	Web Browser	Mozilla Firefox	Transa Statis	test for exceptions from sys policies		in
		Content Threat Blocked		Transie	Web Browser	Mozilla Firefox	Transfer Line 7 (2010)	test for exceptions from sys policies		in
		Content Threat Blocked	AND TRACTORY OF	Transien :	Web Browser	Mozilla Firefox	THE CONTRACT OF THE CONTRACT.	test for exceptions from sys policies	File Type	te
		Content Threat Blocked	AND STREET, STREET, ST.	Transie	Web Browser	Mozilla Firefox	THE CONCERNENCE OF A	test for exceptions from sys policies	File Type	te
		Content Threat Blocked		Training:	USB Storage Device	DATATRAVELER_2.0	EGG/MMADD/	test for exceptions from sys policies		te
		Content Threat Blocked	VLADUT-NOTEBOOK	Vladut	-	DATATRAVELER_2.0		test for exceptions from sys policies		te
			VLADUT-NOTEBOOK			DATATRAVELER_2.0		test for exceptions from sys policies		te
			VLADUT-NOTEBOOK		-	DATATRAVELER_2.0		test for exceptions from sys policies		te
					-		E:/application_encrypted-x-ace.ace	test for exceptions from sys policies		a

# 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.

Indpoint Management   Image: Andpoint Sights   Image: Andpoint		ENDPOINT 4 PROTECTOR	R	eporting and Ac	dministrati	on Tool			English	Welcome   Logout
Notice Registing   Image: Setting and Analysis   Image: Content Analysis   Image: Conten		Dashboard	Mobile Devi	ce Management A	lerts History					Show all departments
Image: Weight Settings       Type 05       Device Name       Created at -         Image: Weight Advance Protection (CAP)       Minde Device Name, and the Sole 13:02       Minde Device Name, and the Sole 13:02         Image: Weight Advance Protection (CAP)       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance Protection (CAP)       Offline Temporary Password       Image: Weight Advance       Arry       Arry       12 March 2014 13:02         Image: Weight Advance Protection (CAP)       Offline Advance       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance       Arry       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance       Image: Weight Advance       Arry       Arry       Arry       Arry         Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image:	P	Endpoint Management	Filter							
Image: Weight Settings       Type 05       Device Name       Created at -         Image: Weight Advance Protection (CAP)       Minde Device Name, and the Sole 13:02       Minde Device Name, and the Sole 13:02         Image: Weight Advance Protection (CAP)       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance Protection (CAP)       Offline Temporary Password       Image: Weight Advance       Arry       Arry       12 March 2014 13:02         Image: Weight Advance Protection (CAP)       Offline Advance       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance       Arry       Arry       Arry       Arry       12 March 2014 13:02         Image: Weight Advance       Image: Weight Advance       Arry       Arry       Arry       Arry         Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance       Image: Weight Advance         Image: Weight Advance       Support       Image: Weight Advance       Image:	200	Endpoint Rights	Results							
Image: Mobile Device Management       Unituitad Apo       Any       Any       12 March 2014 9.05         Image: Mobile Device Management       Image: March 2014 9.05       Any       Any       March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05         Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.05       Image: March 2014 9.0		Endpoint Settings	Event Name	e		Туре О\$	Device Name	Created at -		
Image Mobile Device Management   Image Any   Any 11 March 2014 16:35   Image Any   Image	$\bigcirc$	Content Aware Protection (CAP)								
With Temporary Password       3 results [ 20 ] per page]         Image: Seports and Analysis       Image: Seports and Analysis         Image: Seports and Analysis       Image: Seports and Analysis         Image: Seports and Analysis       Image: Seports and Analysis         Image: Seports and Analysis       Image: Seports analysis         Image: Seports and Analysis       Image: Seports analysis         Image: Seports and Analysis       Image: Seports analysis         Image: Seports analysis       Image: Seports analysis         Image: Seports analysis       Image: Seports analysis         Image: Seports analysis       Image: Seport analysis         Image: Seport analysis       Image: Seport anal	-	Mobilo Dovico Managomont								
Winne reinporaly rassourd   Image: Reports and Analysis   Image: Reports and Analysis   Image: Reports and Analysis   Image: Define Addrs   Define Addrs   Define Addrs   Define Addrs   Image: Reports Hatory   Image: Reports Analysis		mobile bevice management				Any	Any	11 March 2014 16:3	5	
Reports and Analysis   Image: Altris   Define Altris   Define Altris   Define Altris   Define Altris   Content Aware Altris Hatory   System Maintenance   System Configuration   System Parameters   Support		Offline Temporary Password	3 results	[ 20 💌 per page]						
<ul> <li>Define Alerts</li> <li>Define Content Aware Alerts</li> <li>Define Kharts</li> <li>Alerts History</li> <li>Content Aware Alerts History</li> <li>Content Aware Alerts</li> <li>Content Aware Al</li></ul>		Reports and Analysis	$\otimes$	Delete History	1	Back				
<ul> <li>Define Content Aware Alers' Define VMI Alers' Alers History Content Aware Alers' History WMI Alers History WMI Alers History</li> <li>Optimication</li> <li>Optimicatio</li></ul>		Alerts								
Appliance       System Maintenance       System Configuration       System Parameters       Support		Define Content Aware Alerts Define MDM Alerts Alerts History Content Aware Alerts History MDM Alerts History								
<ul> <li>System Maintenance</li> <li>System Configuration</li> <li>System Parameters</li> <li>Support</li> </ul>	Q	Directory Services								
<ul> <li>System Configuration</li> <li>System Parameters</li> <li>Support</li> </ul>		Appliance								
System Parameters Support Support	٨	System Maintenance								
Support	0	System Configuration								
		System Parameters								
	0	Support								
Endpoint Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.3 - Ap	Endo	int Protector 4 Copyright 2004 - 2014 Cc	oSoSys Ltd. All rio	ints 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).

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool	English	• ⊂	Welcome   Logout Q Advanced Search
	Dashboard	Active Directory Import			
	Endpoint Management	Active Directory Import Wizard			
3	Endpoint Rights	This option will allow you to import Computers, Groups and Users from Active Directory.			
X	Endpoint Settings	Requirements: - Credentials to Domain Controller			
	Content Aware Protection (CAP)				
	Mobile Device Management				
	Offline Temporary Password				
<u>~</u>	Reports and Analysis				
	Alerts				
ð	Directory Services	Next			
	Active Directory Import Active Directory Sync				
	Appliance				
*	System Maintenance				
	System Configuration				
	System Parameters				
$\bigcirc$	Support				
Endpo	int Protector 4 Copyright 2004 - 2015 Co	SoSys Ltd. All rights reserved.		No Backgro	und Tasks

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

	ENDPOINT PROTECTOR 4	Reporting and Administration	i Tool		English
	Dashboard	Active Directory Import			
	Endpoint Management	S Connection is valid. Standard	Connection.		
Ch	Endpoint Rights				
X	Endpoint Settings		Active Di	ectory Import. Step 1: Define Connection	
	Content Aware Protection (CAP)	Domain Controller Server Name:	SUSE0.225	Example: w2003server	
		Domain Controller Port:	389	Default: 389 (Global Catalog: 3268)	
	Mobile Device Management	Domain/Search In:	ad4cososys rauk0	Example: example.cososys.com (?) Example: admin@example.cososys.com	
	Offline Temporary Password	Password:		example: auminigexample.cososys.com	
	Reports and Analysis				
	Alerts				
Ð	Directory Services				
	Active Directory Import				
	Active Directory Sync	Back	Next Te	t Connection	
	Appliance				
×	System Maintenance				
	System Configuration				
	System Parameters				
$\bigcirc$	Support				
Endp	pint Protector 4 Copyright 2004 - 2015 Co	SoSys Ltd. All rights reserved.			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".

		Welcome Super Administrator   Logout
PROTECTOR 4 Report	ing and Administration Tool	English 💌 Q
Dashboard       Active Directory In         Image: Indpoint Management       Image: Imag	nport  Connection is valid.  Active Directory Import. Step 2: Content  Computers  Comput	Advanced Search  Show all departments
Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reser	and a second sec	Ready Version 4.0.0.8
Enapoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reser	/ed.	Ready Version 4.0.0.8

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

C	ENDPOINT 4	Welcome Sup	oer Administrator   Logout
	PROTECTOR 4	Reporting and Administration Tool English	Q Advanced Search
	Dashboard	Active Directory Import SI	now all departments
Ì	Endpoint Management	Import completed	
Sp	Endpoint Rights		
×	Endpoint Settings	Active Directory Import. Step 2: Content	
	Offline Temporary Password		
	Reports and Analysis	Constant of the second se	
	System Alerts	erender in the second	
0	Directory Services	B      Controllers     E      Foreign SecurityPrincipals	
	Active Directory Import Active Directory Sync Active Directory Deployment	9 7 Program Data 9 5 System 9 1 Test	
	System Maintenance	9 🔁 Users	
0	System Configuration		
8	System Parameters		
0	Support		
		Back	
Endpo	bint Protector Copyright 2004 - 2011 CoS	ioSys Ltd. All rights reserved.	Ready Version 4.0.0.8

# 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).

	ENDPOINT PROTECTOR 4	Reporting and Administ	ration Tool			English	Welcome   Logout
	Dashboard	Active Directory Synchronizatio	n				
	Endpoint Management		A	ctive Directory Synchronization.	Step 1: Define Connection		
00	Endpoint Rights	Domain Controller Server Name:		Example: w2003server			
×	Endpoint Settings	Domain Controller Port:		Default: 389 (Global Catalog	: 3268)		
$\sim$	Enupoint Settings	Domain:		Example: example.cososys.			
	Content Aware Protection (CAP)	User:		Example: admin@example.c	ososys.com		
	Mobile Device Management	Password:					
	Offline Temporary Password						
	Reports and Analysis						
	Alerts						
Ð	Directory Services	Back	Next	Test Connection	]		View Sync List
	Active Directory Import Active Directory Sync						
	Appliance						
*	System Maintenance						
Ø	System Configuration						
	System Parameters						
0	Support						
Endp	Endpoint Protector 4 Cepyright 2004 - 2015 CoSoSys Ltd. All rights reserved. No Background Tasks. Version 4.4.0.7						

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.

	<b>ENDPOINT</b> PROTECTOR	4 Reporting and Adn	ninistration Tool		English		Q <u>Advanced Sear</u>
	Dashboard	Active Directory Synchronization	on			SI	now all departments
]	Endpoint Management			Active Directory Sync. Step 1: Define Connection			
B	Endpoint Rights	Domain Controller Server Name:		Example: w2003server			
R	Endpoint Settings	Domain:		Example: example.cososys.com			
	Offline Temporary Password	User:		Example: admin@example.cososys.com			
	Reports and Analysis	Password:	•••••				
2	System Alerts						
2	Directory Services						
	Active Directory Import Active Directory Sync Active Directory Deployment						
	System Maintenance	Back	ext Test Connection				
6	System Configuration						
	System Parameters						
	Support						

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.

	ENDPOINT 4				Welcome S	Super Administrator   Logout
	PROTECTOR 4	Reporting and Admi	inistration Tool		English 💌 (	٩)
-						Advanced Search
	Dashboard	Active Directory Synchronization	1			Show all departments
Í	Endpoint Management					
200	Endpoint Rights	S Connection is valid.				
×	Endpoint Settings			Active Directory Sync. Step 1: Define Connection		
	Offline Temporary Password	Domain Controller Server Name:		Example: w2003server		
	Reports and Analysis	Domain:		Example: example.cososys.com		
-	Reports and Analysis	User:	The second s	Example: admin@example.cososys.com		
	System Alerts	Password:	•••••			
0	Directory Services					
	Active Directory Import Active Directory Sync Active Directory Deployment					
	System Maintenance					
0	System Configuration	1		1		
	System Parameters	Back Nex	t Test Connection	J.		
0	Support					
Endpo	bint Protector Copyright 2004 - 2011 CoS	oSys Ltd. All rights reserved.				Ready Version 4.0.0.8

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".

		Welcome Super Administrator   Logout
PROTECTOR Reportin	ng and Administration Tool	English  Advanced Search
Dashboard Active Directory Sy	nchronization	Show all departments
Endpoint Management Son Endpoint Rights Control Endpoint Settings	Connection is valid.	
Offline Temporary Password Reports and Analysis	Computers Compu	
System Alerts Directory Services	<ul> <li>Domain Controllers</li> <li>Foreign SecurityPrincipals</li> <li>Program Data</li> <li>System</li> </ul>	
Active Directory Import Active Directory Sync Active Directory Deployment	Test	
System Maintenance System Configuration		
System Parameters		
Support		
	Sync Interval (in minutes):	
	Back Sync	
Endpoint Protector Copyright 2004 - 2011 CoSoSys Ltd. All rights reserve	ed.	Ready Version 4.0.0.8

You will see the message "Sync object added".

	ENDPOINT 4		Super Administrator   Logout
	PROTECTOR	Reporting and Administration Tool	Advanced Search
	Dashboard	Active Directory Synchronization	Show all departments
Í	Endpoint Management		
20	Endpoint Rights	Sync objects added	
20	Endpoint Settings	Active Directory Sync. Step 2: Content	
	Offline Temporary Password	a 😋 🔽 Active Directory	
	Reports and Analysis	E3  ☐ Builtin E3  ☐ Computers	
	System Alerts		
0	Directory Services	🖶 🔽 Frogram Data	
	Active Directory Import Active Directory Sync Active Directory Deployment	S Test S Tuses Cusers	
	System Maintenance		
0	System Configuration		
	System Parameters		
0	Support		
		Sync Interval (in minutes): 5	
		Back View Sync List	
Endpoi	nt Protector Copyright 2004 - 2011 Co	ioSys Ltd. All rights reserved.	Ready Version 4.0.0.8

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

		и			Welcom	e Super Administrator   Logout
	PROTECTOR	+ Reporting	and Administration Tool		English 💌	Advanced Search
						Advanced Search
	Dashboard	Active Directory Syncl	nronization			Show all departments
Í	Endpoint Management	Sync objects				
Co	Endpoint Rights	Sync objects	auteu			
X	Endpoint Settings			Active Synchronizations	;	
	Offline Temporary Password	Sync Interval 5 minutes	Domain Controller	User	Last Sync 2011-06-07 11:08:00	Actions
	Reports and Analysis					0
	System Alerts					
0	Directory Services					
	Active Directory Import Active Directory Sync Active Directory Deployment					
	System Maintenance					
0	System Configuration					
	System Parameters	Back				Refresh
0	Support					
Endp	oint Protector Copyright 2004 - 2011 C	boobys 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.

	ENDPOINT PROTECTOR     4     Reporting and Administration Tool     Engleh     C       Advanced Sear					
	Dashboard	Endpoint Protector Appliance - Syst	em Information			
	Endpoint Management	System Fail/Over Status				
Ch	Endpoint Rights	System Fail/Over Status:	Disabled - N/A			
X	Endpoint Settings	Disk Space		Info Disk Space		
	Content Aware Protection (CAP) Mobile Device Management Offline Temporary Password Reports and Analysis Alerts Directory Services Appliance Server Information Server Information Server Maintenance System Configuration	Disk Space System: Disk Space EPP Server: Logs on Disk: Shadows on Disk: Database Disk Space occupied Database Disk Space occupied: Number of Case I no Database: Number of Files Traced: Number of Files Shadowed: System Uptime:	2.06 - 12% from 19G 708H - 3% from 28G 3.0K stored in /var/eppfles/plas 4.0K stored in /var/eppfles/shadows 20M stored in /var/lb/mysd/eppdatabase 16 0 0 13:20:02 up 26 min, 0 users, load average: 0.00, 0.00, 0.00 - 1, 5 and	Please consider taking one of the following actions in System Maintenance tab if you have used up 95% of the storage recourse available on the applicance: 1. Back-up 8. Save old or unneeded log by going to File Maintenance and selecting the suitable option. 2. Remove did unmeeded log by yong to File Maintenance and selecting the suitable option. Alternatively, go to System Configuration > System Policies active 3. Daskels or Change the granularity of your policies. Activating File Tracing / Shadowing Inder Global Settings will greatly affect you Server performance. It is recommended to activate Tie Tracing / File Shadowing for specific Computers. 4. Shade the Automatic Log Cleanup feature and Set the HCD Disk Space percentage at which the process will begin		
	System Parameters	Linux Distribution :	Ubuntu 10.04.4 LTS			
	Support	System Information Update:	20144kov-28 13:20:02			
Endp	oint Protector 4 Copyright 2004 - 2014 Co	SoSys 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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool		Welcome   Logout English V Advanced Search				
	Dashboard	Endpoint Protector Appliance - Server Maintenance						
	Endpoint Management	Time Zone						
Sp	Endpoint Rights	Please select your timezone	Europe v / Bucharest v					
X	Endpoint Settings	NTP Server How often to syncronize	pool.ntp.org Once a week					
6	Content Aware Protection (CAP)	Current server time	2014-11-28 13:26:28					
	Mobile Device Management	Save Syncronize Time	Update current Time					
1111 88	Offline Temporary Password	IP Configuration						
	Reports and Analysis	IP Address:	192.168.7.159					
	Alerts	Gateway: Netmask:	192.168.7.1 255.255.255.0					
Ð	Directory Services	*Note: Modifying Network Configuration could stop communication	between EPP Clients and Server.					
	Appliance	DNS Configuration						
	Server Information	DNS 1: DNS 2:	192.168.0.1					
*	Server Maintenance System Maintenance		Appliance requires a functional DNS for sending e-mail alerts and for live update mechanism.					
Ø	System Configuration	Save						
	System Parameters	Appliance Operations						
	Support	Reboot the Hardware Appliance :	Reboot					
		Shutdown the Hardware Appliance :	Shutdown					
		Reset to Factory Defaults:	Factory Default					
		SSH Server						
		Enable:	۲					
		Disable:	0					
		Save						
Endpo	pint Protector 4 Copyright 2004 - 2014 Co	int Protector 4 Copyright 2004 - 2014 CoSoSys Ltd. All rights reserved. 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 Save button will save all the changes, but it will not trigger the synchronization process!

Pressing the Syncronize Time 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	Update current Time	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.

## 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.

	DPOINT 4	Reporting and Admin	istration Tool					English	Welcome   Logot
Dashboard	1	SIEM Integration							Show all departments
Endpoint Man	nagement	SIEM Servers							
Endpoint Righ	hts	() Show Help							
K Endpoint Sett	tings	SIEM	Syslog Server	Syslog Server 2	Add your own				
	are Protection (CAP)	Server Information:	Server Information:	Server Information:	Add new Siem Server with your own settings				
Mobile Device	e Management	IP: 192.168.7.226 Port: 514	19: 192.168.7.125 Port: 514	IP: 192.168.7.115 Port: 514	Click on SIEM Server to				
Offline Temps	porary Password	On On	On On	On On	select it Double click on Title to edit				
Reports and A	Analysis				a SIEM Server				
Alerts		Add New	Edit Edit	🚫 Delete					
Directory Sen	rvices								
Appliance									
Server Informat Server Mainten SIEM Integratio System Maint	nance ion								
System Confi	liguration								
System Paran	meters								
Support									
Endpoint Protector 4	Copyright 2004 - 2015 CoS	5oSys Ltd. All rights reserved.							Ready Version 4.4.0

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.

ENDPOINT PROTECTOR     A Reporting and Administration Tool		English • Q Advanced Search
Dashboard SIEM Integration - Add New Server		Show all departments
Endpoint Management SIEM Status		
Endpoint Rights SIEM Status: @ Enable O Disable		
Endpoint Settings Server Settings		
Content Aware Protection (CAP) Server Name: Syslog Server Server Description: Test		
Mobile Device Management Server IP: 192.168.7.115		
Security Dect		
Offline Temporary Password Disable MySQL Logging V (2)		
Reports and Analysis Log Types		
Alerts		
Device Control     Content Aware Protection		Other SIEM Logs
Directory Services     Directory Service	Change carrier Change SM card Jaibroken Uninetal App	AD Inport     Ad Inport     Adventersation     Adventersation     Adventersation     Adventersation     Adventersation     Adventersation     Adventersation     Adventersation     Control United     Control United
SPEEL Interaction  Speeler Maintenance  Proble IF Due of 1  Proble IF Due of 1  Proble IF Due of 2  Proble IF Due of 2  Proble IF Due of 3  Speeler Proble of 5		Device Control - Loga Amount
System Parameters Enabled		
Support Process Process Processes Procese		
S Seve		1. Back
Endpoint Protector 4 Copyright 2004 - 2015 CoSoSys Ltd. All rights reserved.		Ready Version 4.4.0.8

### 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.

	ENDPOINT PROTECTOR	Reporting and Administration Tool	English		Welcome   Logout Q Advanced Search
	Dashboard	File Maintenance		S	how all departments
Í	Endpoint Management	File Maintenance			
0	Endpoint Rights	Endpoint Protector Server stores several files for its functionality. Use this feature to retrieve/progenize and clean-up these files.			
X	Endpoint Settings	Temporary Logs Files			
$\bigcirc$	Content Aware Protection (CAP)	Shadow Files Delete File Whitelist			
	Mobile Device Management	Log Backup Files			
	Offline Temporary Password				
	Reports and Analysis				
	Alerts				
0	Directory Services				
	Appliance				
٨	System Maintenance				
	<u>File Maintenance</u> System Snapshots Log Backup Content Aware Log Backup				
0	System Configuration				
	System Parameters				
$\bigcirc$	Support				
Ende	oint Protector 4 Copyright 2004 - 2013 Cc				Version 4.4.0.1 - Appliance

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".

	<b>ENDPOINT</b> <b>PROTECTOR</b> 4	Reporting and Administration Tool		English		Velcome   Logout Q Advanced Search
	Dashboard	Save Current State			Show all	departments
Í	Endpoint Management	Snapshot Details				
Co	Endpoint Rights	Name:	MySnapshot			
X	Endpoint Settings	Description:	This is a snapshot.			
$\bigcirc$	Content Aware Protection (CAP)					
	Mobile Device Management					
	Offline Temporary Password					
	Reports and Analysis	Details:	Number of machines in the system: 6. Number of groups in the system: 3. Number of rights defined for existing devices: 3.			
	Alerts	Snapshot:	Currently the system is using both computer and user rights, computer rights have priority.  O Only rights O Only settings O Both			
Ø	Directory Services	Save 🔁 Back				
	Appliance	0				
٨	System Maintenance					
	File Maintenance <u>System Snapshots</u> Log Backup Content Aware Log Backup					
0	System Configuration					
	System Parameters					
0	Support					
Endpo	pint Protector 4 Copyright 2004 - 2013 Co	SoSys Ltd. All rights reserved.			Ready Version -	4.4.0.1 - Appliance

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".

	Dashboard	List of Available Snapsh	iots			Show all departm
ľ	Endpoint Management	C The current cur	tem state has been saved			
P	Endpoint Rights	• me current sys	tem state has been saved			
K	Endpoint Settings	Filter				
	Content Aware Protection (CAP)	Results				
	Mobile Device Management	Name	Description	Created at -	Created by	Actions
-		MySnapshot3	And a third one.	27 September 2013 10:57	root	<u>ڻ</u> 8
	Offline Temporary Password	MySnapshot2	This is another snapshot.	27 September 2013 10:57	root	<u> </u>
	Reports and Analysis	MySnapshot	This is a snapshot.	27 September 2013 10:56	root	©⊗
\	Alerts	3 results [ 20 💌 per	pagej			
	Directory Services	Hake Snapshot				
	Appliance					
	System Maintenance					
s.						
-	File Maintenance					
	System Snapshots					
	System Snapshots Log Backup					
	<u>System Snapshots</u> Log Backup Content Aware Log Backup					
2	<u>System Snapshots</u> Log Backup Content Aware Log Backup System Configuration					

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.

	ENDPOINT PROTECTOR	Reporting and Administration Tool	English	•	Welcome   Logout		
	Dashboard	Restore Snapshot			Show all departments		
Í	Endpoint Management	▲ By restoring a snapshot, all currently defined <u>rights and settings</u> will be overwritten.					
00	Endpoint Rights						
X	Endpoint Settings	Snapshot Details					
Ø	Content Aware Protection (CAP)	Name: MySnaphot Description: This is a manifest					
	Mobile Device Management	Description: This is a snapphot.  Details: Settings for 7 machines and 2 groups. There are 3 rights defined for existing devices. System uses both user and computer rights, prio Details:	site for some tor sights				
	Offline Temporary Password	Details: Settings for / meanines and 2 groups. There are 3 rights demes for existing devices. System uses donit user and computer rights, pro Options	ity for computer rights.				
	Reports and Analysis	Restore: C Only rights C Only settings C Both					
	Alerts	S Restore Back					
0	Directory Services						
	Appliance						
٨	System Maintenance						
	File Maintenance <u>System Snapshots</u> Log Backup Content Aware Log Backup						
0	System Configuration						
	System Parameters						
$\bigcirc$	Support						
Endo	aint Protector 4 Copyright 2004 - 2013 C			Read	y Version 4.4.0.1 - Appliance		
Engrann Freedor - Solo Gooday Las, Angina Calor Co.							

# 12.3. Log Backup

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

	ENDPOINT PROTECTOR	Reporting and Administration Tool	English		Welcome   Logout	
	Dashboard	Log Backup			Show all departments	
Í	Endpoint Management	Log Backup				
00	Endpoint Rights	This option allows you to delete old logs from the database and save them in an .CSV (Comma Separated Values) file. Please choose from the list below which logs you would like to backup:				
×	Endpoint Settings	C Al <sup>®</sup> (388 records) C Older than 30 days (0 records) C Older than none year (0 records)				
$\bigcirc$	Content Aware Protection (CAP)					
	Mobile Device Management	Note: A maximum number of 225000 log records can be deleted at once.  * Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.				
	Offline Temporary Password					
	Reports and Analysis					
	Alerts					
0	Directory Services	Maire Backup	Backup List	В	ackup Scheduler	
	Appliance					
۵	System Maintenance					
	File Maintenance System Snapshots <u>Log Backup</u> Content Aware Log Backup					
0	System Configuration					
	System Parameters					
$\bigcirc$	Support					
Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved. Ready Version 4.4.1						

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

	ENDPOINT 4 PROTECTOR	Reporting and Administration Tool	• <u>•</u>		elcome   Logout Q Advanced Search
	Dashboard	Log Backup		Show all	departments
Í	Endpoint Management	S Backup completed			
Ch	Endpoint Rights	Backup completed			
X	Endpoint Settings	Log Backup			
Ø	Content Aware Protection (CAP)	All logs have been deleted. Number of deleted logs: 588 Click here to manage the log backup files.			
8	Mobile Device Management				
	Offline Temporary Password				
	Reports and Analysis				
	Alerts				
٥	Directory Services				
	Appliance				
٨	System Maintenance	Back			
	File Maintenance System Snapshots Log Backup Content Aware Log Backup				
0	System Configuration				
Ħ	System Parameters				
$\bigcirc$	Support				
Endpo	int Protector 4 Copyright 2004 - 2013 Ci	SoSys Ltd. All rights reserved.		Ready Version 4	.4.0.1 - Appliance

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.

	<b>ENDPOINT</b> PROTECTOR	Reporting and Administration Tool	English	•	Welcome   Logout			
	Dashboard	Log Backup		5	Show all departments			
Í	Endpoint Management	Backup Scheduler						
20	Endpoint Rights	This option allows you to schedule an automatic backup routine, in order to delete old logs (to maintain performance) from the database. The logs will be saved in .CSV (Comma Separated Values) files.						
X	Endpoint Settings	Badup Trigger conditions: Badup time interval: every 2 weeks + Badup size limit: 500000 rows +						
O	Content Aware Protection (CAP)	Badup values:						
<b>E</b>	Mobile Device Management	C All * (0 records) ○ Older than 6 months (0 records)						
	Offline Temporary Password	C Older than 3 months (0 records) C Older than 2 months (0 records) C Older than 1 month (0 records)						
	Reports and Analysis	C Older than 2 weeks (0 records) C Older than 1 week (0 records)						
	Alerts	C Older than 2 days (0 records) C Older than 1 day (0 records)						
0	Directory Services	Note: A maximum number of 525000 log records can be backed up at once. Last Automatic Log Backup: 2012-04-19(13.26.01)						
	Appliance	* Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.						
٨	System Maintenance							
	File Maintenance System Snapshots Log Backup	Save			Back			
0	Content Aware Log Backup System Configuration							
	System Parameters							
0	Support							
Endp	int Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved. Ready Version 4.4.0.1 - Appliance							

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.

	ENDPOINT PROTECTOR	Reporting and Administration Tool	<b>.</b> (	Welcome   Logou Q Advanced Search
	Dashboard	Log Backup		Show all departments
í	Endpoint Management	Log Backup List		
20	Endpoint Rights	logsStats_2013_09_27-11_01_40.cv		
X	Endpoint Settings			
	Content Aware Protection (CAP)			
	Mobile Device Management			
	Offline Temporary Password			
	Reports and Analysis			
	Alerts			
0	Directory Services			Back
	Appliance			
٨	System Maintenance			
	File Maintenance System Snapshots Log Badup Content Aware Log Badkup			
0	System Configuration			
	System Parameters			
0	Support			
Endpo	pint Protector 4 Copyright 2004 - 2013 C	SSSSys Ltd. All rights reserved.	Read	y Version 4.4.0.1 - Appliance

## 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.

	<b>ENDPOINT</b> <b>PROTECTOR</b> 4	Reporting and Administration Tool	English	<b>.</b>	Welcome   Logout
	Dashboard	Content Aware Log Backup			Show all departments
Í	Endpoint Management	Content Aware Log Backup			
Ch	Endpoint Rights	This option allows you to delete old Content Aware logs from the database and save them in an .CSV (Comma Separated Values) file. Please choose from the list below which logs you would like to back	up:		
×	Endpoint Settings	C All * (28 records) C Dider than 30 days (0 records) G Dider than swonths (0 records)			
O	Content Aware Protection (CAP)	C Older than one year (0 records)			
	Mobile Device Management	Note: A maximum number of 225000 log records can be deleted at once.			
	Offline Temporary Password				
	Reports and Analysis				
	Alerts				
0	Directory Services	Make Backup	Backup List		Backup Scheduler
	Appliance				
۵	System Maintenance				
	File Maintenance System Snapshots Log Backup <u>Content Aware Log Backup</u>				
0	System Configuration				
	System Parameters				
$\bigcirc$	Support				
Endp	pint Protector 4 Copyright 2004 - 2013 Co	SoSys Ltd. All rights reserved.		Read	dy Version 4.4.0.1 - Appliance

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

	<b>ENDPOINT</b> <b>PROTECTOR</b> 4	Reporting and Administration Tool	English		Velcome   Logout Q Advanced Search
	Dashboard	Content Aware Log Backup		Show al	departments
Þ	Endpoint Management	6-1 - 1 - 1 - 1			
0	Endpoint Rights	S Backup completed			
X	Endpoint Settings	Content Aware Log Backup			
0	Content Aware Protection (CAP)	Al logs have been deleted. Number of deleted logs: 28 Click here to manage the log backup files.			
6	Mobile Device Management				
	Offline Temporary Password				
	Reports and Analysis				
	Alerts				
Φ	Directory Services				
	Appliance				
٨	System Maintenance	Back			
	File Maintenance System Snapshots Log Backup <u>Content Aware Log Backup</u>				
0	System Configuration				
Ħ	System Parameters				
0	Support				
	sint Protector 4 Convrint 2004 - 2013 C				440.1 - Appliance

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.

	ENDPOINT PROTECTOR	Reporting and Administration Tool		Welcome   Logout
	Dashboard	Content Aware Log Backup		Show all departments
Í	Endpoint Management	Content Aware Backup Scheduler		
0	Endpoint Rights	This option allows you to schedule an automatic backup routine, in order to delete Content Aware old logs (to maintain performance) from the database. The logs will be saved in .CSV (Comma Separated Values) files.		
X	Endpoint Settings	Badup Trigger conditions: Badup time interval: every month 👻 Badup size limit: 35000 Rows 👻		
Ø	Content Aware Protection (CAP)	Badup values:		
	Mobile Device Management	C All * (0 records) C Older than 6 months (0 records)		
	Offline Temporary Password	C Older than 3 months (0 records) C Older than 2 months (0 records) C Older than 1 month (0 records)		
<u></u>	Reports and Analysis	C Older than 2 weeks (0 records) C Older than 1 week (0 records)		
	Alerts	C Older than 2 days (0 records) C Older than 1 day (0 records)		
Ø	Directory Services	Note: A maximum number of 525000 log records can be backed up at once. Last Automatic Log Backup: never		
	Appliance	* Deleting all logs might temporarily affect the correct display of online computers, online devices and graphics reports.		
۵	System Maintenance			
	File Maintenance System Snapshots	Save		Back
	Log Backup Content Aware Log Backup			
0	System Configuration			
	System Parameters			
0	Support			
Endp	oint Protector 4 Copyright 2004 - 2013 C	oSoSys Ltd. All rights reserved.	Reg	adv Version 4.4.0.1 - Appliance

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.

	<b>ENDPOINT</b> 4 PROTECTOR	Reporting and Administration Tool	• (	Advanced Search
	Dashboard	Content Aware Log Backup		Show all departments
Í	Endpoint Management	Content Aware Log Backup List		
Co	Endpoint Rights	logsStatuCap_2013_09_27-11_25_08.csv		
X	Endpoint Settings			
0	Content Aware Protection (CAP)			
<b>E</b>	Mobile Device Management			
	Offline Temporary Password			
	Reports and Analysis			
⚠	Alerts			
0	Directory Services			Back
	Appliance			
۵	System Maintenance			
	File Maintenance System Snapshots Log Backup <u>Content Aware Log Backup</u>			
0	System Configuration			
	System Parameters			
$\bigcirc$	Support			
Endpo	sint Protector 4 Copyright 2004 - 2013 Co	SoSys Ltd. All rights reserved.	Read	y Version 4.4.0.1 - Appliance

# 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.

#### **122** | Endpoint Protector | User Manual

	ENDPOINT PROTECTOR	Reporting and Administration Tool	English	Welcome   Logout				
	Dashboard	Log and Content Aware Log Backup						
	Endpoint Management	A No modification can be made because there is a backup running!						
	Endpoint Rights	Log and Content Aware Log Backup						
×	Endpoint Settings	Note: This section allows management of old logs. Choose which logs you want to backup and export or delete from database						
0	Content Aware Protection (CAP)	Choose what type of backup to create						
	EasyLock Enforced Encryption	Audit Log Badup 🗹						
	Mobile Device Management	Keep or delete logs from server when creating the backup						
	Offline Temporary Password	Keep badeel up logs						
	Reports and Analysis	Keep backed up shadows 🗹						
	Alerts	Longe file shadows will affect the export procedure and the server performance. This should be managed separatly prior to export.						
0	Directory Services	Closes what logs to backup						
	Appliance	<ul> <li>Al</li> <li>Older than 1 year</li> </ul>						
*	System Maintenance	Older than 6 months     Older than 1 month						
	File Maintenance System Snapshots Log Backup	Oder fran Lveek     Goder fran Léver     Oder fran Léver     Oder fran Léver						
	Content Aware Log Backup Audit Log Backup	Average number of logs in one pack						
ø	External Storage System Backup System Configuration	<ul> <li>IN2.000</li> <li>IN2.000</li> <li>IN2.000</li> </ul>						
	System Parameters	© 500,000 @ 1.000,000						
Support     Cooce what He Shadows to include								
		Do not trailed file shadoos     do do not trailed file shadoos sandor that         file shadoos stange that         file shadoos sandor that         file						
		Make Bactup	Backup List	Backup Scheduler				
Endo	oint Protector 4 Copyright 2004 - 2016 Co	Sofus Ltd. All rights reserved.		Ready Version 4.4.0.8				

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 created reports for executives.

gs Filetrace Sha	dows								
ollection Shadow 2016-	01-28 17:22:13 - 2016-01-28 1	7:23:07 •							
iow 25 - entries								Search:	
Username	A Machine Name	machine Ip	Filename	Filehash	FileSize(Kb)	Filetype	Event Time	6 Log	Actio
tedate Pag	ANDREIP-WIN10	192.168.15.34	1 - Сору (10) - Сору - Сору - Сору - Сору - Сору - Сору.txt	15530/b1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:13	3701560558433075842	
and the first	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075843	
testes has	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075844	8
and the first state	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075846	
Index Proj	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075847	
teritori fina	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075850	
Index Pag	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075851	
nation that	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075852	
name top	ANDREIP-WIN10	192.168.15.34	1 - Сору (100) - Сору - Сору - Сору - Сору - Сору - Сору - Сору.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075849	
tentra lina	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075853	
Index Page	ANDREIP-WIN10	192.168.15.34	1 - Copy (10).txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075848	
nation that	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy.txt	15530/b1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075845	
termine the	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075854	8
hadred Page	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075855	8
index Page	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy - Copy.bt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075856	
Index Page	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075857	
1000	ANDREIP-WIN10	192-168-15-34	1 - Copy (1000) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075858	
nation in the	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075860	
nana ing	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075861	
1000	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075864	
testes top	ANDREIP-WIN10	192-168-15-34	1 - Copy (1002) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075865	
inter ing	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075863	
testes fra	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075866	
nation from	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075862	
	ANDREIP-WIN10	192.168.15.34	1 - Сору (1001) - Сору - Сору - Сору - Сору - Сору.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075859	
Search Username	Search Machine Name	Search machine to	Search Filename	Search Filehash	Search FileSize(Kb)	Search Filetype	Search Event Time	Search Log	1

## 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.).

	ENDPOINT PROTECTOR	Reporting and Administration Tool	English • (Logout English • Q) Advanced Elearch						
	Dashboard	og and Content Aware Log Backup							
	Coloring Management	Schedule Audit Log Backup	*						
	Endpoint Management	Schedule Audit Content Aware Log Backup							
00	Endpoint Rights	Choose the frequency for the backup							
×	Endpoint Settings	@ Every year							
	Content Aware Protection (CAP)	Every 6 months     Every nonth							
	EasyLock Enforced Encryption	© Every week © Every day							
	Mobile Device Management	p or delete logs from server when creating the backup							
	Offline Temporary Password	Keep baded up logs							
	Reports and Analysis	Keep bodied up shadows 📰 🔲 Leaving the above options undexided will delete add logs from the server and improve performance.							
	Alerts	Large file shadows will affect the export procedure and the server performance. This should be managed separatly prior to export.							
6	Directory Services	Choose what logs to backup							
	Appliance	⊛ Al ⊜ Clér than 1 year							
*	System Maintenance	Other than 6 months     Other than 1 month							
	File Maintenance	O differ than 1 week							
	System Snapshots	Older than 2 days							
	Log Backup	Older than 1 day							
	Content Aware Log Backup Audit Log Backup	Average number of logs in one pack							
	External Storage	@ 100,000							
_	System Backup	200,000							
٩	System Configuration	© 100,000 © 500,000							
	System Parameters	© 1.000,000 © 1.500,000							
	Support	Choose what File Shadows to include							
		Do not include file shadows							
		w u or not include me snakovis ○ Include all Reshadovis regardless of size							
		C Include fits shadows smaller than 100 MB							
		Save Cancel schedule	Back						
Endp	oint Protector 4 Copyright 2004 - 2016 CoSe	tSys Ltd. Al rights reserved.	Ready Version 4.4.0.8						

# 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:

ndpoint Protector Server - External S	torage Settings
External Storage Settings	
External Storage Type:	FTP Server
Enable FTP Storage:	
Keep copy on EPP Server:	V.
Server Address:	192.168.0.3
Remote Directory:	/DLP/logbadoup/ ⑦
Server Port:	21 ⑦
Passive Connection:	V.
Anonymous Login:	V.
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 Shado	ow Files and Log Backup Files to a network share or FTP server.

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 <u>saved</u> 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.

퉬 logbackup	3/2/2015 7:27 PM	File folder
퉬 shadows	3/2/2015 7:27 PM	File folder
퉬 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:

ternal Storage Settings	
External Storage Type:	Samba / Network Share 💌
Enable Network Share Storage:	
Keep copy on EPP Server:	V
Network Share Path:	//192.168.0.52/epp ⑦
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!

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.

	ENDPOINT PROTECTOR 4	Reporting and Adminis	stration Tool					English 🔹	Welcome   Logout
	Dashboard	List of Available Backups							
	Endpoint Management	Filter							
Co	Endpoint Rights	Results							
X	Endpoint Settings	Name	Version	Content		Description		Created at	Actions
	Content Aware Protection (CAP) Mobile Device Management Offline Temporary Password Reports and Analysis Alerts Directory Services Appliance System Maintenance System Maintenance System Snapahots Log Backup System Configuration System Configuration System Parameters Support	Backup for crash recovery Test Backup 17014 11014 4 Judie obsp auto_backup_100ct2014 4 results [20] per page]	4405 4404 4404	Database Content,	Application Sources Application Sources Upload	Just a test. For safety reasons. www Scheduled System Backup on 10-Oct Backup Scheduler	-2014	17-Oct-2014 11:24:02 17-Oct-2014 11:18:02 14-Oct-2014 11:48:01 10-Oct-2014 13:39:18 ck	
Endp	oint Profector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.							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 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:	Badkup 12122014
Description:	Just your regular backup.
Database Content:	The entire database content will be saved
Application Sources:	The entire application sources will be saved
Save L Back	

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.

System Backup Status								
System	Backup Status							
Creating system backup 30% done								
\$	Refresh	1	Back					

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:

ι	lpload System Backup				
					Upload System Backup
	Choose System Backup File:			Browse No file selecte	d.
	* Note: Please use a valid .eppb file.				
	S Upload	1	Back		
	• opload		Duon		

#### 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**.

List of Availal	ble Backups
S Backu	ip scheduled successfully
System Backu	ıp Scheduler
This option allow	is you to schedule an automatic system backup routine.
Backup Trigger o	conditions:
System Backup	p time interval: every 2 weeks
Last Automat	ic System Backup: 10-Oct-2014 (13:39:02)
8	Save Back

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.

Endpoint Protector Appliance - www.EndpointProtector.com							
CoSoSys Ltd Endpoint Protector Appliance							
Your current appliance IP is 192.168.7.151							
Please access your appliance through this address https:\\192.168.7.151 from your web-browser After accessing the appliance interface through your web-browser you will see a certificate error. Please ignore it.							
Your current setup IP is 111.33.33.111							
Please select option [1 - 4] or press <exit> to exit</exit>							
System Backup 3 Reboot 4 Shutdown							
5 Exit to Shell							
<pre></pre>							

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
- 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:

Host	:	192.168.0.3	
User	:		
Password	:		
Path	:	/Backups/test.eppb	

# 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.

	ENDPOINT 4	Reporting and Administration Tool			Englan • Ogoat Advanced Search
	Dashboard	Audit Backup List			
	Endpoint Management	Endpoint Protector Client Installation			
00	Endpoint Rights	The Endpoint Protector Client can be installed on:			
X	Endpoint Settings	Windows	Mac Mac	💩 Linux	
	Content Aware Protection (CAP)	Windows	Mac	<u>C3</u> Linux	
	EasyLock Enforced Encryption	Windows 10 Windows 8 Windows 7	Mac OS X 10.6 (Snow Leopard) Mac OS X 10.7 (Lion) Mac OS X 10.8 (Mountain Lion)	Ubuntu OpenSUSE CentOS	
	Mobile Device Management	Windows Vista Windows XP	Mac OS X 10.0 (Mountain Con) Mac OS X 10.9 (Mavericks) Mac OS X 10.10 (Yosemite)	RedHat	
	Offline Temporary Password	Windows Server 2003/2008/2012	Mac OS X 10.11 (El Capitan)		
<u>~</u>	Reports and Analysis	<ul> <li>Windows (32bit version) - Version: 4.4.5.3</li> <li>Windows (64bit version) - Version: 4.4.5.3</li> </ul>	Mac OS X - Version: 1.4.5.5	Clents for Linux distributions are only available on request! Submit Request for Endpoint Protector Client for Linux.	
	Alerts	C manufacture and a second			
ð	Directory Services		the Endpoint Protector Server IP, Port and Department C	iode.	
_	Appliance	Endpoint Protector Server IP: 192.16 Endpoint Protector Server Port: 443	1.0.230		
*	System Maintenance	Department Code: defdep			
٩	System Configuration	Pres	erve Server Settings on all download pages		
	<u>Client Software</u> Client Software Upgrade Client Uninstall	🛓 Download			
	System Administrators System Departments System Security System Policies	Endpoint Protector Client for Windows can be deployed on For more information, please refer to Endpoint Protect			
	System Fordes System Settings System Licensing				
_	System Parameters				
$\overline{\mathbf{O}}$	Support				
	nt Protector 4 Copyright 2004 - 2016 C				Reary Venion 4.4.3

### 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.

	Software Update			Show al	l departme
Endpoint Management			Step 1: Select the update you want to apply		
Endpoint Rights	Updates available for the Endpoint Protector Only Windows Client Software higher than 4 Only Macintosh 10.5+ Client Software higher	0.1.4 can be u			
Endpoint Settings					
Content Aware Protection (CAP)	OS Type O Windows	Default Yes	ersion Release Notes	Applicable on versions 4.0.1.5	Actions
content Aware Protection (CAP)	Mac OS X 10.5+ (Snow Leopard)	Yes	.4.0.6	1.0.9.5	*
Mobile Device Management	Mac OS X 10.4 (Tiger)	Yes	.090	none	*
	<ul> <li>Ubuntu 14.4 LTS</li> </ul>	Yes	0.5-1	none	*
Offline Temporary Password	Ubuntu 12.4 LTS	Yes	.0.3-1	none	*
Deports and Analysis	Ubuntu 10.4 LTS	Yes	.0.0-1	none	*
Reports and Analysis	OpenSUSE 11.4	Yes	0.0-1	none	*
Alerts	Windows	No	2.8.1	4.0.1.5	*
	Windows	No	266	4.0.1.5	*
Directory Services	Windows	No	25.7	4.0.1.5	*
	Windows	No	.2.3.0	4.0.1.5	*
Appliance	Windows	No	.1.7.0	4.0.1.5	*
System Maintenance	Windows	No	.1.4.4	4.0.1.5	*
	Windows	No	.1.3.7	4.0.1.5	*
System Configuration	Windows	No	1.2.3	4.0.1.5	*
Client Software	Windows	No	1.1.4	4.0.1.5	*
Client Software Upgrade	Windows	No	.1.0.7	4.0.1.5	*
Client Uninstall	Windows	No	.0.6.0	4.0.1.5	*
Download EasyLock Software	Mac OS X 10.5+ (Snow Leopard)	No	3.0.4	1.0.9.5	*
System Administrators	Mac OS X 10.5+ (Snow Leopard)	No	.2.3.1	1.0.9.5	*
System Departments	Mac OS X 10.5+ (Snow Leopard)	No	226	1.0.9.5	*
System Security System Policies	Mac OS X 10.5+ (Snow Leopard)	No	.2.1.6	1.0.9.5	*
System Policies System Settings	Mac OS X 10.5+ (Snow Leopard)	No	.1.1.0	1.0.9.5	*
System Licensing	Mac OS X 10.5+ (Snow Leopard)	No	.1.0.4	1.0.9.5	*
System Parameters	Mac OS X 10.5+ (Snow Leopard)	No	.1.0.0	1.0.9.5	*
System Functors	Mac OS X 10.5+ (Snow Leopard)	No	.0.9.1	none	*
Support	Next				

The  $\stackrel{\star}{\sim}$  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.

	Dashboard	Client	Uninstall - List	of Computer	S								Show all	lepartme
]	Endpoint Management	Filter												
B	Endpoint Rights	Resul	ts											
K	Endpoint Settings		Computer Name	IP	Department	Workgroup	Domain	Default User	Location	Last Time Online 💌	Version	License	Modified at	Modi
	Content Aware Protection (CAP)	740	Marrie	192.168.0.21	Default Department	WORKGROUP				26-Feb-2014 11:49	4.2.7.6 - (PC)	Offline	14-Mar-2014 15:3	
2				192.168.0.60	Default Department	WORKGROUP				17-Jan-2014 09:45			14-Mar-2014 15:3	2:02 root
	Mobile Device Management				Default Department					10-Dec-2013 13:00			14-Mar-2014 15:3	
				192.168.0.20	Default Department					25-Nov-2013 09:42			14-Mar-2014 15:3	
	Offline Temporary Password			192.168.0.106	Default Department	WORKGROUP				19-Nov-2013 12:59	4.2.6.6 - (PC)	Offline	14-Mar-2014 15:3	2:02 root
	Reports and Analysis			192.168.0.96	Default Department			Concession of the		17-Mar-2014 08:59			14-Mar-2014 16:5	
-	Reports and Analysis				Default Department			CONVERTMENT.		14-Mar-2014 17:01				
<u>\</u>	Alerts	7 res	sults [ 20 💌 p	er page]										
2	Directory Services	•												
۵ -	Directory Services Appliance	×	Client Unintall	Ĺ	_ Back									
			Client Unintall	1	_ Back									
	Appliance		Client Unintall	Ĺ	_ Back									
	Appliance System Maintenance		Client Unintali	Ĺ	_ Back									
	Appliance System Maintenance System Configuration Client Software Client Software Upgrade <u>Client Vinistall</u> Download EasyLock Software System Administrators		Client Unintall	1 1	_ Back									
	Appliance System Maintenance System Configuration Clent Software Upgrade Clent Vinistal Download EasyLock Software System Administrators System Departments System Departments System Security		Client Unintall	1	_ Back									
	Appliance System Maintenance System Configuration Client Software Client Software Upgrade Client Voltware System Administrators System Departments System Security System Security System Socies		Client Unintall		Back									
	Appliance System Maintenance System Configuration Client Software Client Software Upgrade Client Uninstal Download EasyLock Software System Administrators System Departments System Security System Policies System Settings		Client Unintali	1	Back									
	Appliance System Maintenance System Configuration Client Software Client Software Upgrade Client Uninstall Download EasyLock Software System Actinistators System Departments System Departments System Policies System Security System Polices System Security System Clienting		Client Unintali	1	Back									
	Appliance System Maintenance System Configuration Client Software Client Software Upgrade Client Uninstal Download EasyLock Software System Administrators System Departments System Security System Policies System Settings		Client Unintali	1	Back									

### 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.

	ENDPOINT PROTECTOR 4	Reporting and Admini	stration Tool			English 🗸 (	Welcome   Logout Q Advanced Search
	Dashboard	List of Administrators					Show all departments
	Endpoint Management	Filter					
Sp	Endpoint Rights	Results					
X	Endpoint Settings	User Name	Created at	Last Login	Super Admin	Acti	ions
	Content Aware Protection (CAP)	root vladut - root	4 September 2014 13:03	11-Sep-2014 09:16	~		
	Mobile Device Management	2 results [ 50 - per page]	4 September 2014 13:03		~	1	
88	Offline Temporary Password	Create					
	Reports and Analysis						
	Alerts						
0	Directory Services						
	Appliance						
*	System Maintenance						
	System Configuration						
	Client Software Client Software Upgrade Client Uninstall Download Easystock Software System Administrators System Security System Policies System Sectings System Leanang						
	System Parameters						
0	Support						
Endpo	oint Protector 4 Copyright 2004 - 2014 Co	SoSys 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.

#### 134 | Endpoint Protector | User Manual

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool	En	Welcome test test   Logout
	Dashboard	Administrator User		Show all departments
	Endpoint Management	Administrator Details		
	Endpoint Rights	User Name: Password:	root	
×	Endpoint Settings	Password Confirmation:		
	Content Aware Protection (CAP)	First Name:		
	EasyLock Enforced Encryption	Last Name: E-mail:		
-	Mobile Device Management	Phone:		
88	Offline Temporary Password	Administrator Settings		
<u>~</u>	Reports and Analysis	Super Administrator:		
	Alerts	Receive E-mail Alerts: Account is active:		
		Account is active: Enforce login IP restrictions:		
0	Directory Services	Managed Departments:	V Default Department	
	Appliance		test dep nume foarte lung de deapatament	
*	System Maintenance		internet volar de vog Gete Andergeneration in st_guard_group(name)	
	System Configuration			
	Client Software Client Software Upgrade Client Uninstall System Administrators			
	System Departments	Default UI Language:	English •	
	System Security System Policies	Last Login:	22-Mar-2016 11:19	
	System Settings	Current password set on:		
	System Licensing	Save Save Add	1 Beck	
	System Parameters	O Delete		
	Support			
Endpo	eint Protector 4 Copyright 2004 - 2016 Col	SoSys Ltd. All rights reserved.		Ready Version 4.4.0.8

# 13.5. System Departments

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

## $\mathbb{Z} \otimes$

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.

	ENDPOINT PROTECTOR 4	Reporting and Administration To	ol	English	Welcome   Logout
	Dashboard	List of Departments		S	how all departments
	Endpoint Management	Results			
Sp	Endpoint Rights	Department Name	Description	Department Code	Actions
X	Endpoint Settings	Default Department Secret Department	New entities will belong to this departm Secret		28
0	Content Aware Protection (CAP)	Public Department	public		₿⊗
	Mobile Device Management	3 results [ 50 v per page]			
88	Offline Temporary Password	Create			
	Reports and Analysis				
	Alerts				
ø	Directory Services				
	Appliance				
*	System Maintenance				
Ø	System Configuration				
	Client Software Client Software Upgrade Client Uninstal Download EasyLock Software System Administrators System Polare International System Polices System Polices System Licenaing System Parameters Support				
Endp	oint Protector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.			Ready Version 4.4.0.4

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

ld a New Department		Show all departmen
Details		
Department Name:	Testing	
Description:	This is the Testing Department.	
Unique Code:	335efr	

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".

	ENDPOINT 4	Reporting and Administration Tool		English 🗣		come   Logout Q dvanced Search
	Dashboard	System Security			Show all de	epartments
	Endpoint Management	🛆 You do not have an uninstall password defined.				
Sp	Endpoint Rights					
X	Endpoint Settings	ightarrow You do not have a security password for sensitive	e data defined.			
6	Content Aware Protection (CAP)	Security Password for Uninstall Protection				
	Mobile Device Management	Password:	•••••			
	Offline Temporary Password	Save				
<u>~</u>	Reports and Analysis	Data Security Privileges				
	Alerts	Restrict Sensitive Data Access only to super administrators:				
0	Directory Services	Save				
_	Appliance	Additional Security Password for Sensitive Data Protection				
×	System Maintenance					
	System Configuration	New Password:	•••••			
	Client Software Client Software Upgrade Client Univatil Download EasyLock Software System Administrators System Departments System Policies System Policies System Policies System Uciening System Varameters Support	New Password (confirm):				
Endpo	int Protector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.			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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool		English	•	Welcome   Logout
	Dashboard	System Security			Show a	all departments
	Endpoint Management	$\Delta$ You do not have an uninstall password defin	ed.			
Cho	Endpoint Rights	· ·				
X	Endpoint Settings	⚠️ You do not have a security password for sen	sitive data defined.			
	Content Aware Protection (CAP)	Security Password for Uninstall Protection				
	Mobile Device Management	Password:	•••••			
1988 1988	Offline Temporary Password	Save				
	Reports and Analysis	Data Security Privileges				
	Alerts	Restrict Sensitive Data Access only to super administrators:				
•	Directory Services	Save				
	Appliance	Additional Security Password for Sensitive Data Protection				
×	System Maintenance	Current Password:	•••••			
	System Configuration	New Password:	•••••			
	Clent Software Clent Software Upgrade Clent Unistall Download EasyLock Software System Administrators System Departments System Policies System Settings System Folicies System Lenning System Parameters Support	New Password (confirm): Save				
Endpo	oint Protector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.			R	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.

	ENDPOINT PROTECTOR	4	Reporting and Administration Tool				English 🗸	Welcome   Logout
<b>@</b>	Content Aware Protection	^	Default System Settings					Show all departments
(CAP)			Endpoint Protector Rights Functionality					^
	Scanning Data At Rest		Use computer rights					
	Mobile Device Management		O Use user rights					
	Offline Temporary Password		O Use both Priority: User rights Computer rights					
	Reports and Analysis		Custom Settings					
	Alerts							
	Alerts		Show MAC Address For Offline Temporary Password:					
Ð	Directory Services		Show User Domain:					E
	Appliance		EasyLock 2 - Settings					
×	System Maintenance		File Trading:					
			Offline File Tracing:					
	System Configuration	=	Active Directory Authentication					
	Client Software Client Software Upgrade		Enable Active Directory Authentication:					
	Client Uninstall		Domain Controller Server Name (or IP):	192.168.0.203				
	Download EasyLock Software		Domain Controller Port:	389				
	System Administrators System Departments		Domain Name:	DC=ad4cososys,DC=com		0		
	System Security		Account Suffix:	@ad4cososys.com		0		
	System Policies		User:	raulad		V		
	System Settings		Password:					
	System Licensing		Active Directory Administrators Group:	EPP Administrators		0		
	System Parameters		Active Directory Operations:	Sync AD Administrators	т	est Connection		
	Support	Ļ		oyno no Administratora				
Endpo	pint Protector 4 Copyright 2004 - 20	15 CoS	oSys Ltd. All rights reserved.					

#### 13.8.2. Proxy Settings

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

Proxy Server Settings		
IP:		
Username:		
Password:		
*Note: This information refers to netw	orks with configured Proxy server to allow ac	cess 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 <u>liveupdate.endpointprotector.com</u>. 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.

End	ENDPOINT 4 PROTECTOR	Reporting and Ad	ministration	Tool						Eng	jish .		Icome   Logout
End	shboard	Endpoint Protector Licer	ising System									Show all d	lepartments
K End	dpoint Management	System Status (Updates a	and Support)										
K End	dpoint Rights	() Show Help											
💿 Con	dpoint Settings	Number of total licenses pres	ent in the system:	55									
	ntent Aware Protection (CAP)	System		Status			End Dat	e					
Mot	bile Device Management	Updates		Yes									
Offi	fline Temporary Password	Support			ntrol ware Protection (C vice Management	AP)	02 Oct 2	)14 10:54:01 )14 10:54:01 )14 10:54:01					
Rep	ports and Analysis	F Buy Now											
Aler	erts	Feature Status											
Dire	rectory Services	(?) Show Help											
App	pliance	Feature				Status	End Date	Total	Used	Online			
🗙 Sys	stem Maintenance	Device Control				Trial Mode	02 Oct 2014 10:54:		7	2			
Sys	stem Configuration	Device Control and Content A Device Control and Content A Mobile Device Management				Trial Mode Trial Mode Trial Mode	02 Oct 2014 10:549 02 Oct 2014 10:549 02 Oct 2014 10:549	1 50	7 7 2	2 2 2			
	ent Software ent Software Upgrade					That mode	02 001 2014 10.04.		-	2			
Clier	ent Uninstall	General License Informat	ion										
Syst	wnload EasyLock Software stem Administrators	(?) Show Help											
	stem Departments stem Security	Mode	Period I	indpoints	Mobile Endpoint	ts Device Cont	rol Content Awa	ire Protectio	n (CAP)	Mobile Device Management	Updates	Support	
	stem Policies	Trial	30 Days	50	5	Yes	Win & Mac			Yes	Yes	Yes	
	stem Settings stem Licensing	Appetizer (Limited)	1 Year	5	5	Yes	Win only - Lim	ted		Yes - Limited	Yes	No	
Sys	stem Parameters	Buy Licenses		mport License	s	Paste Licenses		List License	s				
🚺 Sup	pport	n											
	Protector 4 Copyright 2004 - 2014 CoS												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.

F Buy Licenses

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 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.

Start Appetizer

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.

Start Free Trial

#### 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.

Import Licenses		
Paste Licenses		
Licenses List:		
Save	Back	

#### **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.

X	test [Compatibili	ty Mode] - Micros	oft Excel		_		٢
File Home Insert Page Layout Formulas	Data Review	View			۵ (	) — F	
$ \begin{array}{c c} & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ & & & \\ \end{array} $		.00 .0	B Conditional Formatting ▼ B Format as Table ▼ Cell Styles ▼	∎•= Insert × ■ Delete × ■ Format ×	✓ Filter	Find & Select *	
	ignment	🗟 Number 🗔	Styles	Cells	Editir	ıg	_
D26 • <i>f</i> *		1					×
A	C _	0.0	D				
1 Endpoint Protector Client License Keys for Import	License Type				_		
2 XXXX-XXXX-XXXX		Endpoint Protect					-
3 XXXX-XXXX-XXXX		Endpoint Protect					-
4 XXXX-XXXX-XXXX		Endpoint Protect					-
5 XXXX-XXXX-XXXX		Endpoint Protect					
6 XXXX-XXXX-XXXX-XXXX		Endpoint Protect					
7 2222-2222-2222-2222		Mobile Endpoint					-
8 2222-2222-2222-2222		Mobile Endpoint					
9 ZZZZ-ZZZZ-ZZZZ-ZZZZ	Mobile	Mobile Endpoint	License				
10 ZZZZ-ZZZZ-ZZZZ-ZZZZ		Mobile Endpoint					
11 2222-2222-2222-2222		Mobile Endpoint					
12 ZZZZ-ZZZZ-ZZZZ-ZZZZ		Mobile Endpoint					
13 YYYY-YYYY-YYYY 14 YYYY-YYYY-YYYY			ort for Mobile Device Manage ort for Device Control & Conte		ontion		
14 TTT-TTT-TTT-TTT 15 YYYY-YYYY-YYYY			ort for Device Control & Conte ort for Device Control	ent Aware Prote	ection		
16		oparios a Suppr					
17							
18							
19							
20 H 4 + H Endpoint Protector Client Keys						▶ [	T I
Ready				□ □ 100% (	Э		

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.

#### Paste Licenses

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

List Licenses

#### 145 | Endpoint Protector | User Manual

	<b>ENDPOINT</b> 4 <b>PROTECTOR</b> 4	Repo	orting and Adn	ninistration Tool					English 🗸	Advanced
Da	ashboard	List of Av	aliable Licenses						Shov	v all departm
Er	idpoint Management	Filter								¥
s Er	idpoint Rights	List of Li	censes							
	idpoint Settings	🔳 All	Order Number	License Validity	License Key	Valid until	License Type 👻	Assigned Computer	Assigned Mobile Device	Actions
	ontent Aware Protection (CAP)		1		TRIA-L000-0794-0118	02 Oct 2014 10:54:01	Updates & Support (Trial)			$\otimes$
			2		TRIA-LMDM-0367-0393	Active	Mobile Endpoint License		Her:	$\otimes$
M	obile Device Management		3		TRIA-LMDM-0878-0730	Active	Mobile Endpoint License		THE CONTRACT	8
			4		TRIA-LMDM-0128-0543	Active	Mobile Endpoint License			8
Of	fline Temporary Password		5		TRIA-LMDM-0991-0650	Active	Mobile Endpoint License			Ø
			6	•	TRIA-LMDM-0446-0446	Active	Mobile Endpoint License			8
Re	eports and Analysis		7		TRIA-LCAP-0024-0958	Active	Endpoint License			8
1	erts		8		TRIA-LCAP-0565-0321	Active	Endpoint License	Manufacture of the second s		$\otimes$
	eros		9		TRIA-LCAP-0510-0789	Active	Endpoint License	100000000		8
Di	rectory Services		10		TRIA-LCAP-0397-0112	Active	Endpoint License	approximation of the second		×
	,		11		TRIA-LCAP-0763-0973	Active	Endpoint License			×.
Ap	pliance		12		TRIA-LCAP-0742-0830	Active	Endpoint License	The second second second		×
			13		TRIA-LCAP-0748-0572	Active	Endpoint License	Initropole:		× ×
S)	stem Maintenance		14		TRIA-LCAP-0251-0995	Active	Endpoint License			×.
í –			15		TRIA-LCAP-0297-0836	Active	Endpoint License			×
5)	stem Configuration		16		TRIA-LCAP-0532-0668	Active	Endpoint License			×.
Cl	ent Software		17		TRIA-LCAP-0453-0689	Active	Endpoint License			×.
	ent Software Upgrade		18	<u> </u>	TRIA-LCAP-0463-0532	Active	Endpoint License			×.
Cl	ent Uninstall		19		TRIA-LCAP-0321-0379	Active	Endpoint License			ŏ
Do	ownload EasyLock Software		20	<u> </u>	TRIA-LCAP-0418-0040	Active	Endpoint License			×
	stem Administrators		21		TRIA-LCAP-0776-0000	Active	Endpoint License			8
	stem Departments		22	<u> </u>	TRIA-LCAP-0585-0801	Active	Endpoint License			×
	stem Security		22		TRIA-LCAP-0959-0150	Active	Endpoint License			8
	rstem Policies rstem Settings		23		TRIA-LCAP-0122-0469	Active	Endpoint License			8
	istem Licensing		24		TRIA-LCAP-0940-0520	Active	Endpoint License			8
			25							8
S)	stem Parameters		26	-	TRIA-LCAP-0582-0703 TRIA-LCAP-0494-0324	Active	Endpoint License Endpoint License			8
\ c.	innort		27							8
51	ipport				TRIA-LCAP-0534-0242	Active	Endpoint License			8
			29		TRIA-LCAP-0897-0786	Active	Endpoint License			
			30	•	TRIA-LCAP-0237-0194	Active	Endpoint License			8
			31		TRIA-LCAP-0623-0769	Active	Endpoint License			8
			32		TRIA-LCAP-0863-0076	Active	Endpoint License			8
			33		TRIA-LCAP-0459-0326	Active	Endpoint License			8
			34		TRIA-LCAP-0609-0780	Active	Endpoint License			8
			35		TRIA-LCAP-0706-0027	Active	Endpoint License			8

# 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.

	Dashboard	Device Types					
	Endpoint Management	Device Control	Content Aware Protection (CAP)				
3	Endpoint Rights	Name		Description	Windows	Mac	Linux
	Endpoint Settings	Unknown Device		Unknown Device	~	~	~
	Endpoint Settings	USB Storage Device		USB Storage Device (USB Flash Drives, U3 Drives, ExpressCard, Biometric USB Storage Devices, etc.)	~	~	~
	Content Aware Protection (CAP)	Internal CD or DVD R	w	Internal CD or DVD RW	~	~	~
		Internal Card Reader		Internal Card Reader (SD Cards, Memory Cards, Compact Flash, etc.)	~	~	~
	Mobile Device Management	Internal Floppy Drive		Internal Floppy Drive	~		~
		Local Printers		Local Printers connected to Computer	~	~	$\checkmark$
	Offline Temporary Password	Windows Portable De	evice (Media Transfer Protocol)	Windows Portable Device (Media Transfer Protocol)	~		
		Digital Camera		Digital Camera	~		~
	Reports and Analysis	BlackBerry		BlackBerry hand held Device	~		
		Mobile Phones (Sony	/ Ericsson, etc.)	Mobile Phones (Sony Ericsson, etc.)	~		
	Alerts	SmartPhone (USB Sy	/nc)	SmartPhone connected through USB	~		~
		SmartPhone (Window	vs CE)	Windows CE Device	~		
	Directory Services	SmartPhone (Symbian	n)	Nokia N Series	~		$\checkmark$
		Webcam		Web Camera	~	~	
	Appliance	iPhone		iPhone	~	~	
1	Curtary Maintenance	iPad		(Pad	~	~	
J	System Maintenance	iPod		iPod	~	~	
1	System Configuration	Serial ATA Controller		Serial ATA Controller	~		
J	System Comgaration	WiFi		Wireless Network	~	~	
1	System Parameters	Bluetooth		Bluetooth Devices	~	~	
J	-,	FireWire Bus		FireWire Bus	~	~	
	Device Types	Serial Port		Serial Port	~		
	Rights	PCMCIA Device		PCMCIA Device	~		
	Events	Card Reader Device	(MTD)	Card Reader Device based on Memory Technology Driver	~		
	File Types	Card Reader Device (	(SCSI)	Card Reader Device based on SCSI Adapter	~		
	Support	ZIP Drive		ZIP Drive	~		
		Teensy Board		USB-based Microcontroller Development System	~		
		Thunderbolt		Thunderbolt	$\checkmark$	$\checkmark$	
		Network Share		Network Share	~		
		Infrared Dongle		Infrared Dongle	~		
		Parallel Port (LPT)		Parallel Port (LPT)	~		
		Additional Keyboard		Additional Keyboard	~		
		USB Modem		USB Modem	~		

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.

	Endpoint Management	Device Control Content Aware Protection (CAP)			
8	Endpoint Rights	Name	Description	Windows	Mac
	Endpoint Settings	Unknown Device	Unknown Device		
	Endpoint Settings	USB Storage Device	USB Storage Device (USB Flash Drives, U3 Drives, ExpressCard, Biometric USB Storage Devices, etc.)	~	~
	Content Aware Protection (CAP)	Internal CD or DVD RW	Internal CD or DVD RW		
		Internal Card Reader	Internal Card Reader (SD Cards, Memory Cards, Compact Flash, etc.)	$\checkmark$	~
	Mobile Device Management	Internal Floppy Drive	Internal Floppy Drive		
		Local Printers	Local Printers connected to Computer	~	
	Offline Temporary Password	Windows Portable Device (Media Transfer Protocol)	Windows Portable Device (Media Transfer Protocol)		
		Digital Camera	Digital Camera		
	Reports and Analysis	BlackBerry	BlackBerry hand held Device		
		Mobile Phones (Sony Ericsson, etc.)	Mobile Phones (Sony Ericsson, etc.)		
	Alerts	SmartPhone (USB Sync)	SmartPhone connected through USB		
		SmartPhone (Windows CE)	Windows CE Device		
	Directory Services	SmartPhone (Symbian)	Nokia N Series		
		Webcam	Web Camera		
	Appliance	iPhone	iPhone		
		iPad	iPad		
	System Maintenance	iPod	iPod		
1		Serial ATA Controller	Serial ATA Controller	~	
	System Configuration	WIFi	Wireless Network		
1	System Parameters	Bluetooth	Bluetooth Devices		
J	System Parameters	FireWire Bus	FireWire Bus	~	~
	Device Types	Serial Port	Serial Port		
	Rights	PCMCIA Device	PCMCIA Device		
	Events	Card Reader Device (MTD)	Card Reader Device based on Memory Technology Driver	~	
	File Types	Card Reader Device (SCSI)	Card Reader Device based on SCSI Adapter	~	
	Current	ZIP Drive	ZIP Drive	~	
	Support	Teensy Board	USB-based Microcontroller Development System	*	
		Thunderbolt	Thunderbot	~	~
		Network Share	Network Share	, in the second se	•
		Infrared Dongle	Infrared Donole	•	
		Parallel Port (LPT)	Parallel Port (LPT)		
		Additional Keyboard	Additional Keyboard		
		USB Modem	USB Modem		

# 14.2. Rights

This list contains the access rights which can be assigned on the system for devices at any time.

	<b>ENDPOINT</b> 4 <b>PROTECTOR</b> 4	Reporting and Administration Tool	English 🗸	Advanced
	Dashboard	List of Possible Rights	Shov	v all departm
	Endpoint Management	Results		
<i>m</i>	Endpoint Rights	Name	Description	
~	Endpoint Settings	Deny Access	Deny Access	
		Allow Access	Allow Access	
)	Content Aware Protection (CAP)	Read Only Access Allow Access if TD Level 1	Read Only Access Allow Access if device is Trusted Device Level 1	
	Mobile Device Management	Allow Access if TD Level 2	Allow Access if device is Trusted Device Level 1	
		Allow Access if TD Level 3	Allow Access if device is Trusted Device Level 3	
	Offline Temporary Password	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	
	Reports and Analysis	8 results [ 50 💌 per page]		
	Alerts			
	Directory Services			
	Appliance			
]	System Maintenance			
ł	System Configuration			
	System Parameters			
	Device Types			
	Rights			
	Events			
	File Types			
	Support			
·				

## 14.3. Events

This list contains the events which will be logged for further reference.

tanagement lights ettings ware Protection (CAP) vice Management nporary Password id Analysis Services	Results Event Name Connected Disconceted Enabled Disabled File Read File Virte File Read-Virte File Read-Virte File Read-Virte File Deste Device TD Device not TD Delete	Description           Device Connected         Device Disconnected           Device Disconnected         Device Disconnected           Device Disbled         Device Disbled           File vorden to device         File vorden to device           File vorden to device         File road and write from device           File from device renamed         File deleted from device           File deleted from device         Device is trusted           Device is not trusted         Device is not trusted	Logging 	Quick Logging	Actions C C C C C C C C C C C C C C C C C C C
ettings ware Protection (CAP) vice Management mporary Password ud Analysis	Connected Disconnected Enabled Disabled File Read File Read-Write File Read-Write File Read-Write File Delete Device TD Device not TD Delete	Device Connected Device Disconnected Device Disconnected Device Disabled Pile vote Disabled File road from device File road and write from device File road and write from device File form device ensamed File deleted from device Device is not trusted	****	* * * * * * * * *	2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3
ware Protection (CAP) vice Management mporary Password ud Analysis	Disconnected Enabled Disabled File Read File Read-Write File Read-Write File Delete Device TO Device not TD Delete	Device Disconnected Device Disbed Device Disbled File road from device File road and write from device File road and write from device File form device renamed File deleted from device Device is not trusted	*****	· · · · · · · · · · · · · · · · · · ·	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
rice Management mporary Password Id Analysis	Enabled Disabled File Road File Write File Road-Write File Roame File Delete Device TD Device not TD Delete	Device Enabled Device Deabled File read from device File written to device File road and write from device File from device renamed File deleted from device Device is trusted	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	67 67 67 67 67 67 67 67
rice Management mporary Password Id Analysis	Disabled File Road File Write File Road-Write File Roame File Dokte Device TD Device not TD Device	Device Disabled File read from device File written to device File rand and write from device File from device renamed File deleted from device Device is funsted Device is not trusted	· · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	2 2 2 2 2
nporary Password	File Read File Write File Read-Write File Reame File Device Device TO Device not TO Device	File read from device File writen to device File read and write from device File from device renamed File deleted from device Device is trusted Device is not trusted	> > > > > > > > > > > > > > > > > > >	> > > > > >	2 2 2 2
nporary Password	File Write File Read-Write File Reame File Delete Device TD Device not TD Delete	File written to device File road and write from device File from device renamed File deleted from device Device is trusted Device is not trusted	· · · · · · · · · · · · · · · · · · ·		2 2 2
id Analysis	File Read-Write File Rename File Delete Device TD Device not TD Delete	File read and write from device File from device renamed File deleted from device Device is trusted Device is not trusted	* * * *	× × ×	2
id Analysis	File Rename File Delete Device TD Device not TD Delete	File from device renamed File dekted from device Device is trusted Device is not trusted	· · · · · · · · · · · · · · · · · · ·	~	Z
	File Delete Device TD Device not TD Delete	File deleted from device Device is trusted Device is not trusted	× 	~	
Services	Device TD Device not TD Delete	Device is trusted Device is not trusted	<u></u>		2
Services	Device not TD Delete	Device is not trusted			
Services	Delete		,	~	Z
Services			~	$\checkmark$	Z
		Delete an item	$\checkmark$	$\checkmark$	Z
	Enable Read-Only	Device Read-Only Enabled	$\checkmark$	$\checkmark$	Z
	Enable if TD Level 1	Device Enabled if TD Level 1	$\checkmark$	$\checkmark$	Z
intenance	Enable if TD Level 2	Device Enabled if TD Level 2	$\checkmark$	$\checkmark$	Z
	Enable if TD Level 3	Device Enabled if TD Level 3	$\checkmark$	$\checkmark$	Z
nfiguration	Enable if TD Level 4	Device Enabled if TD Level 4	$\checkmark$	$\checkmark$	Z
	AD Import	AD Import	$\checkmark$	$\checkmark$	Z
rameters	AD Synchronization	AD Synchronization	$\checkmark$	$\checkmark$	Z
s	Blocked	Blocked on the client side	$\checkmark$	$\checkmark$	Z
	Unblocked	Allowed on the client side	$\checkmark$	$\checkmark$	Z
	Offline Temporary Password used	Offline Temporary Password used	$\checkmark$	$\checkmark$	2
	User Login	User Login	$\checkmark$	$\checkmark$	Z
	File Encrypt	File Encrypt using EasyLock v2	$\checkmark$	$\checkmark$	2
	File Decrypt	File Decrypt using EasyLock v2	$\checkmark$	$\checkmark$	Z
	File Encrypt (offline)	File Encrypt (offline) using Easy Lock v	$\checkmark$	$\checkmark$	2
	File Decrypt (offine)	File Decrypt (offline) using Easy Lock v	$\checkmark$	$\checkmark$	Z
	Content Threat Detected	Content Aware Protection - Threat Detect	$\checkmark$	$\checkmark$	Z
	Content Threat Blocked	Content Aware Protection - Threat Blocke	$\checkmark$	$\checkmark$	Z
	File Copy	A file was copied to or from a removable	~	$\checkmark$	2
	Scanning Data at Rest	Found Object from Scanning Data at Rest	$\checkmark$	$\checkmark$	Z
	User Logout	User Logout	~	$\checkmark$	2
	32 results [ 50 - per page]				
	ameters	AD Synchronization Biocked Ubbocked Uffine Temporary Pasaword used User Login File Decrypt File Decrypt File Decrypt File Decrypt (offine) Content Threat Discked File Copy Saming Data at Rest User Logout	ameters         AD Synchronization         AD Synchronization           Blocked         Blocked         Blocked         Blocked           Unblocked         AD koved on the client side         Unblocked         Offine Temporary Password used           User Login         User Login         User Login         File Encrypt using EasyLock v2           File Encrypt         File Encrypt using EasyLock v2         File Encrypt using EasyLock v2           File Encrypt (offfine)         File Encrypt (offfine) using EasyLock v           File Encrypt (offfine)         File Encrypt (offfine) using EasyLock v           Content Threat Detection - Threat Detect         Content Aware Protection - Threat Detect           Content Threat Detection - Threat Detect         Content Threat Detection - Threat Detect           Scanning Data at Rest         User Logout         User Logout	ameters     AD Synchronization <ul> <li>AD Synchronization</li> <li>AD Synchronization</li> <li>Blocked</li> <li>Blocked</li> <li>Blocked</li> <li>Blocked</li> <li>AD Synchronization</li> <li>AD Synchronization</li> </ul> <ul> <li>AD Synchronization</li> <li>AD Synchronization</li></ul>	AD Synchronization     AD Synchronization     Image: Control Addition of the client side       Blocked     Blocked on the client side     Image: Control Addition of the client side       Offline Temporary Password used     Offline Temporary Password used     Image: Control Addition of the client side       Offline Temporary Password used     Offline Temporary Password used     Image: Control Addition of the Client side       User Login     User Login     Image: Control Addition of the Client side       File Encrypt     File Encrypt using EasyLock v/2     Image: Control Addition of the Client side       File Encrypt (offline)     File Encrypt (offline) using EasyLock v/2     Image: Control Addition of the Client Addition of the

#### 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.

Endpoint Management Endpoint Rights Endpoint Rights Content Aware Protect Mobile Device Manage Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance System Maintenance	tion (CAP) PNG image OpenOccument Text Setup Information Setup Information Setup Information Identifier Rie	Mime Type	Description           Microsoft Word Document           PKG Image           OpenDocument Text           Setup Information           Application           Jdentifier file           .data file	Actions 2' & 2'
Endpoint Settings Content Aware Protec Mobile Device Manage Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance	doc tion (CAP) PVG image GenoDocument Text Sebup Information ssword Application Application Addin file Hy3946 file Configuration Setups Microsoft Word-Document	Mime Type	Microsoft Word Document PNG Image OpenDocument Text Setup Information Application Jdentifier file	2 0 2 0 2 0 2 0 2 0 2 0
Content Aware Protec Mobile Device Manage Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance	tion (CAP) PNG mage ement OpenDocument Text Setup Information Application Application Addatine file Applied file Applied file Configuration Settops Microsoft Word-Dokument		PNG Image OpenDocument Text Setup Information Application Jdentifier file	2 8 2 8 2 8 2 8 2 8 2 8
Mobile Device Manage Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance	ement OpenDocument Text Setup Information Application deatifier file data file 1xp346 file Configuration Settings Microsoft Word-Dotument		OpenDocument Text Setup Information Application .Identifier file	E & E & E &
Mobile Device Manage Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance	ement OpenDocument Text Setup Information Application deatifier file data file 1xp346 file Configuration Settings Microsoft Word-Dotument		OpenDocument Text Setup Information Application .Identifier file	I & I & I &
Offline Temporary Pa Reports and Analysis Alerts Directory Services Appliance	ement Setup Information Seword Application dentifier file data file information Application data file information page 4 Configuration Settings Microsoft Word-Dokument		Setup Information Application .Identifier file	Z 8
<ul> <li>Offline Temporary Pa</li> <li>Reports and Analysis</li> <li>Alerts</li> <li>Directory Services</li> <li>Appliance</li> </ul>	sevor minadom sevoral Jednátkar file data file Hp3948 file Configuration Settings Microsoft Word-Dokument		Application .Identifier file	28
<ul> <li>Reports and Analysis</li> <li>Alerts</li> <li>Directory Services</li> <li>Appliance</li> </ul>	Jdentifier file .data file .Hp3948 file Configuration Settings Microsoft Word-Dokument		.ldentifier file	
<ul> <li>Reports and Analysis</li> <li>Alerts</li> <li>Directory Services</li> <li>Appliance</li> </ul>	Jedniffer file .data file .Hp3946 file Configuration Settings Microsoft Word-Dokument			$\mathbb{Z} \otimes$
Alerts Directory Services Appliance	.Hp3948 file Configuration Settings Microsoft Word-Dokument		.data file	
Directory Services	Configuration Settings Microsoft Word-Dokument			E 😣
Directory Services	Microsoft Word-Dokument		.Hp3948 file	
Appliance			Configuration Settings	E 😣
Appliance			Microsoft Word-Dokument	₫⊗
	.tmp file		.tmp file	₫⊗
	.ace file		.ace file	₫⊗
System Maintenance	.oft file		.oft file	IZ ⊗
10 Y	.p file		.p file	₫⊗
	.pas file		.pas file	IZ ⊗
System Configuration	.tex file		.tex file	[2]⊗
	GIF Image		GIF Image	E 😣
System Parameters	Python File		Python File	$\mathbb{Z} \otimes$
Device Types	.rar file		.rar file	[2]⊗
Rights	.sh file		.sh file	[2]⊗
Events	.java file		.java file	28
File Types	VLC media file (.bin)		VLC media file (.bin)	28
Support	docx		docx	28
Support	24 results [ 50 💌 per page]			
	Create			

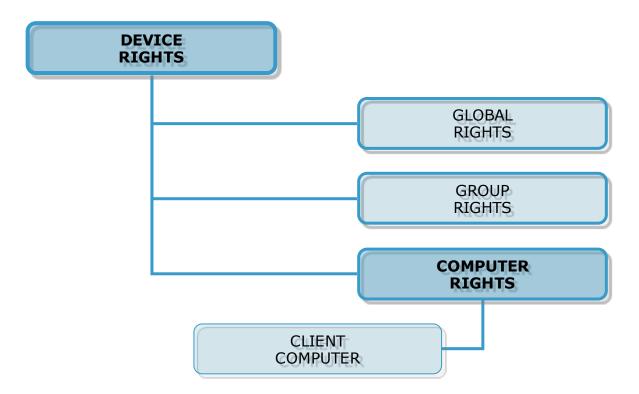
# 15. Setting up Policies

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.

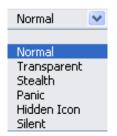


For example: in Global Rights, assign Allow for device X. If in Computer Rights, the same device does not have permission to be used; the device will not be usable. Same applies vice-versa: if the device lacks permission to be used in Global Rights, and has permission under Computer Rights, the device 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.

ENDPOINT PROTECTOR	Reporting a	and Administration Tool		Welcome   Logout English • Q Advanced Search
Dashboard	List of Administrators			
Endpoint Management	Filter			
Endpoint Rights	Results			
Endpoint Settings	User Name	Created at	Last Login	Actions
Offline Temporary Password	root		13-Sep-2011 10:52	[] ■ ⊗
Reports and Analysis	1 result [ 50 - per pa	age]		
System Alerts	Create			
Directory Services				
System Maintenance				
System Configuration				
Client Software Client Software Upgrade Download EasyLock Software <u>System Administrators</u> System Departments System Departments System Policies System Security System Policies System Licensing System Licensing System Parameters Support				
Endpoint Protector 4 Copyright 2004 - 2011 C				Ready Version 4.0.2.5 - Appliance

To add another Administrator or Super Administrator, click the "Create" button.

User Information		
User Name:	My Admin	
Password:	•••••	
Password Confirmation:	•••••	
Permissions and Department	5	
Is active:		
Is super admin:	Γ	
Departments:	Default Department	
Information		

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:	
Is super admin:	Г

**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.

Groups			
Name:	Global		
Description:	Global Group including all t	he entities	
Device Types			
USB Storage Device		Allow Access	iPhone
Internal CD or DVD RW		Preserve global setting Deny Access	iPad
Internal Card Reader		Allow Access Read Only Access	iPod
Internal Floppy Drive		Allow Access if TD Level 1 Allow Access if TD Level 2	Serial ATA Controller
Local Printers		Allow Access if TD Level 3 Allow Access if TD Level 4	WiFi
Windows Portable Device		Deny Access	Bluetooth
Digital Camera		Deny Access	FireWire Bus
BlackBerry		Deny Access	Serial Port
Mobile Phones (Sony Ericsso	n, etc.)	Deny Access	PCMCIA Device
SmartPhone (USB Sync)		Deny Access	Card Reader Device (MTD
SmartPhone (Windows CE)		Deny Access	Card Reader Device (SCS
SmartPhone (Symbian)		Deny Access	ZIP Drive
Webcam		Deny Access	

# 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.

	4 Reporting and Administration Tool	English	• ⊂	Welcome (Logout
Dashboard	EaryLock Enforced Encryption			
Endpoint Management	A When the Master Password feature is disabled, EasyLock Enforced Encryption actions will not be accessible. Please set up a Master Password.			
Endpoint Rights Endpoint Settings	Concernal torio     Exercised is detained by protect data saved on portable storage devices such as USB stoka, with military strength, 256bt AES encryston.     Information the hotions' information, a provides create-platform enforced encryston,     Information and the hotions' information.			
EasyLock Enforced Encrypt				
Selfing Clenic Letic/Listicid Clenic Letic/Listicid Clenic	Copy & Deschad or Copy the Early Calls guadage dends is the most of the UBB storage dence.     Copy & Deschad and at a guaranted.     Copy & Deschad and a guaranted.     Copy & Deschad and an except red protect them through Early Calls.     Copy & Deschad      Automatically Degley Early Calls.     To automatically Degley Early Calls.     To automatically Degley Early Calls.     To automatically Degley Early Calls.			
System Parameters	When USI Starge Devices will be plaqued in to computers where Endpoint Protector Clenis are displayed, Executed will be automatically publicly on the devices. The granularity of the Device Currich Rights also applies to the Executed deployment, as everyption can be entranced globally, per grady, computery, carry, device or custom classes.			
	Update EasyLock Automatically			
	Automatically update Earystod. Software when a new version is a walable		t.	Back
Endpoint Protector 4 Copyright 2004	2016 CoSoSys Ltd. Al rights reserved.			Ready Version 4.4.0.5

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.

	ENDPOINT PROTECTOR 4	Reporting and Administration Tool		English	•	Welcome   Logout
	Dashboard	EasyLock Enforced Encryption - Settings			Sho	w all departments
	Endpoint Management	EasyLock Master Password				
Co	Endpoint Rights	Old Master Password:				
×	Endpoint Settings	New Master Password:				
	Content Aware Protection (CAP)	Confirm New Master Password:				
	Mobile Device Management	EasyLock Security Details				
88	Offline Temporary Password	User Maximum Password Retries: User Minimum Password Length:	10 6			
<u>~</u>	Reports and Analysis	Device Status becomes "Inactive" after:	30 days			
	Alerts	EasyLock Installation and Execution				
Ð	Directory Services					
	Appliance	Allow EasyLock to be installed and run only on computers where the Endpoint Protector Client is present.				
*	System Maintenance	Save Settings				
	System Configuration	EasyLock File Tracing				
	System Parameters	File Tracing:				
	EasyLock Enforced Encryption	Offline File Tracing:	▼			
		Save File Tracing				
	<u>Settings</u> Clients	EasyLock License				
	Deploy EasyLock	EasyLock Site License:	8			
$\bigcirc$	Support				1	Back
					- <u>-</u>	Dack
Endpo	oint Protector 4 Copyright 2004 - 2016 C	oSoSys Ltd. All rights reserved.				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.

•	ENDPOINT PROTECTOR 4												Advanced
D	Dashboard	EasyLock Enforced Encryption - Manage Client											
E	Endpoint Management	Client Details											
E	Endpoint Rights	Name:	test			Use	ername:						
		Device Name (Identification):				Cor	mputer Name:		1000				
E	Endpoint Settings	Description:				Ver	ndor ID:						
) (	Content Aware Protection (CAP)	Status:	Active			Pro	duct ID:						
	content ( con )	Last Location IP:	192, 168.0, 153			Ser	ial Number:		-				
N	Mobile Device Management	Last Seen:	03-Feb-2016 15:39:1	2		Mo	dified at:						
		Created at:	03-Feb-2016 15:39:1	2		Mor	dified by:						
	Offline Temporary Password	Created by:	user										
R	Reports and Analysis												
		Save Details Send Meso	di Cha	nge User's Password	Reset Devic	Desco	d Master Password						
<b>A</b>	Alerts		wi cua	iye vael a rasamulu	Meser Den.	Ce Generativ	a master Password						
0	Directory Services	Actions History											
	Appliance	Туре		Status	Details	Created at		Modified at		Created by	Modified by	A	ctions
s	System Maintenance	Re-deploy Client		Completed		3 February 2016 15:3	9	3 February 2016 15:39		auto	auto		
1	system municendrice	Reset Device		Canceled		2 February 2016 17:4	2	2 February 2016 17:42		root	root		
s	System Configuration	Reset Device		Failed		2 February 2016 17:4	2	2 February 2016 17:42		root	root		
		Change Master Password				2 February 2016 17:4	1	2 February 2016 17:41		root	root		
s	System Parameters	Change User Password				2 February 2016 17:3	9	2 February 2016 17:39		root	root		
F	EasyLock Enforced Encryption	Send Message				2 February 2016 17:38	9	2 February 2016 17:39		root	root		
	caspearer entered entrypoon	Send Message				2 February 2016 17:3	8	2 February 2016 17:38		root	root		
	Settings	Send Message				2 February 2016 16:3	2	2 February 2016 16:32		root	root		
	Clients	Change Settings - Installation and Execution				2 February 2016 16:3	0	2 February 2016 16:30		root	root		
	Deploy EasyLock	Change Master Password				2 February 2016 15:4		2 February 2016 15:47		root	root		
) s	Support	Send Message				2 February 2016 15:2		2 February 2016 15:22		root	root		
		Send Message				2 February 2016 15:2		2 February 2016 15:22		root	root		
		Send Message				2 February 2016 15:2		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 12:4	4	1 February 2016 12:44		auto	auto		
		15 results [ 50 💌 per page]											
		w Export State	h List									t_ Be	ack

#### 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.

EasyLock File Tracing	
File Tracing:	
Offline File Tracing:	ø
Save File Tracing	

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!

Do you	want to run or save this file?
17	Name: EPPClientSetup_x86_32.msi Type: Windows Installer Package, 4.24MB From:
	While files from the Internet can be useful, this file type can botentially harm your computer. If you do not trust the source, do no

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.

	ENDPOINT PROTECTOR 4	Reporting and Administration	n Tool		English	• ⊂	Welcome   Logout
	Dashboard	Endpoint Protector Server - Download	d Client Software			Sho	ow all departments
	Endpoint Management	Endpoint Protector Client Installation					
00	Endpoint Rights	Note: Endpoint Protector Client version h		ed for Content Aware Protection.			
X	Endpoint Settings	The Endpoint Protector Client can be installed o - Windows 8 (32bit and 64bit)	n:				
0	Content Aware Protection (CAP)	Windows 7 (32bit and 64bit)     Windows Vista (32bit and 64bit)     Windows Vista (32bit and 64bit)					
	Mobile Device Management	<ul> <li>Windows XP (32bit and 64bit)</li> <li>Windows Server 2003/2008 (32bit and 64bit)</li> <li>Mac OS X 10.5+ (Snow Leopard)</li> </ul>					
	Offline Temporary Password	- Mac OS X 10.4 (Tiger) - Linux (Ubuntu, OpenSUSE)					
	Reports and Analysis	To install the Endpoint Protector Client on your	client computers, please downk	ad it from the following location:			
	Alerts	To install the client software, please provide the		nd Port.			
ø	Directory Services	Endpoint Protector Server IP: Endpoint Protector Server Port:	192.168.7.70 443				
_	Appliance	To install the client software under a certain de Department Code:	epartment, please provide the D defdep	epartment Code.			
*	System Maintenance	Windows (32bit version) - Version: 4	.2.9.2				
	System Configuration	Windows (64bit version) - Version: 4 Install Outlook Add-on: Yes O No					
	Client Software Client Software Download EasyLock Software System Administrators System Departments System Policies System Policies System Notices System Licenang System Parameters Support	Mac 05 X 10.5 + (Leopard) - Version: Mac 05 X 10.4 (Tiger) - Version: 1.0 Uniux - Ubuntu 10.4 TS - Version: 1.1 Uniux - Ubuntu 14.4 TS - Version: 1.1 Uniux - Ubuntu 14.4 TS - Version: 1.1 Uniux - OpenSUSE 11.4 - Version: 1.0 <u>Uniux - OpenSUSE 11.4 - Version: 1.0</u> Endpoint Protector Client for Windows can be d For more information, please refer to Endpoin	9.0 0.0-1 0.3-1 0.5-1 .0-1 leployed over Active Directory.				
Endpo	pint Protector 4 Copyright 2004 - 2014 Co	SoSys Ltd. All rights reserved.					Ready Version 4.4.0.4

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:

	About Endpoint Protector	
	End User License Agreement	
	Update Policies Now	
	Offline Temporary Password	
2	8/26/2014	

# 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 <u>https://192.168.0.201</u>).

If there is no certificate in your browser, you will be prompted with Certificate Error page like the screenshot below.

Certificate	Error: Navigation Blocked - Windows Internet Explorer		
0.		👻 🍕 🗙 📴 Bing	• ٩
🔶 Favorite	Certificate Error: Navigation Blocked	🟠 🔹 🔝 👻 🖶 🖶 Page 👻 Safety	▼ Tools ▼  ♥ *
8	There is a problem with this website's security certificate.		*
	The security certificate presented by this website was not issued by a trusted certificate authority. The security certificate presented by this website was issued for a different website's address.		
	Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.		
	We recommend that you close this webpage and do not continue to this website.		
	Ø Click here to close this webpage.		
	Continue to this website (not recommended).		
			+
Done		Internet   Protected Mode: Off	🕶 🔍 100% 💌

Continue your navigation by clicking <sup>Solution</sup> "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.

General	Security Priv	acy Content	Connections	Programs	Advan
Parenta	l Controls				
	Control the be viewed.	Internet conte	nt that can	Parental Co	ontrols
Conten	t Advisor				
0		p you control th this computer.	e Internet con	tent that car	n be
		Er	nable	🚱 Setti	ings
Certifica	the state				
9	Use certific	ates for encryp	ted connection	s and identif	ication.
		$\neg$			
	Clear <u>S</u> SL state	e <u>C</u> erti	ificates	Publishe	ers
		e <u>C</u> ert	ificates	Pu <u>b</u> lishe	ers
AutoCor	AutoComple on webpage	ete stores previ es and suggests	ous entries [	Pu <u>b</u> lish Settin	
AutoCor	AutoComple on webpag for you.	ete stores previ	ous entries [		
AutoCor	AutoComplete AutoComple on webpag for you. nd Web Slices	ete stores previ	ous entries [		gs
AutoCor	nplete AutoComple on webpag for you. nd Web Slices Feeds and content fro	ete stores previ es and suggests	ous entries s matches ide updated ( t can be	Settin	gs
AutoCor	nplete AutoComplete on webpag for you. nd Web Slices Feeds and content fro read in Inte	ete stores previ es and suggests Web Slices prov m websites that	ous entries s matches ide updated ( t can be	Settin	gs

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

rusted Root Certification Au	thorities Trusted Publishe	ers Untruste	d Publishers
Issued To	Issued By	Expiratio	Friendly Name
AddTrust External Certum CA Class 3 Public Prima Class 3 Public Prima Class 3 Public Prima Copyright (c) 1997 DigiCert High Assur Entrust.net Secure Equifax Secure Cer GlobalSign Root CA	Certum CA Class 3 Public Primary Class 3 Public Primary Copyright (c) 1997 Mi DigiCert High Assuran Entrust.net Secure Se	12/31/1999 11/10/2031 5/25/2019	VeriSign Class 3 VeriSign Microsoft Timest DigiCert Entrust
Import Export	<u>R</u> emove		<u>A</u> dvan

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.

File to Import						
Specify the file you want	to import.					
<u>F</u> ile name:						
	Browse					
Note: More than one cer	rtificate can be stored in a single file in the following formats:					
Personal Information	Exchange- PKCS #12 (.PFX,.P12)					
Cryptographic Messag	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)					
Microsoft Serialized Co	ertificate Store (.SST)					
losen mara shaut cartificata (	Sla Farmata'					
Learn more about <u>certificate f</u>	ne tormats					

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

Certificate Import Wizard						
Certificate Store Certificate stores are system areas where certificates are kept.						
Windows can automatically select a certificate store, or you can specify a location for the certificate.						
$\bigcirc$ Automatically select the certificate store based on the type of certificate						
Place all certificates in the following store						
Certificate store:						
Trusted Root Certification Authorities Browse						
Learn more about <u>certificate stores</u>						
< <u>B</u> ack Next > Cancel						

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

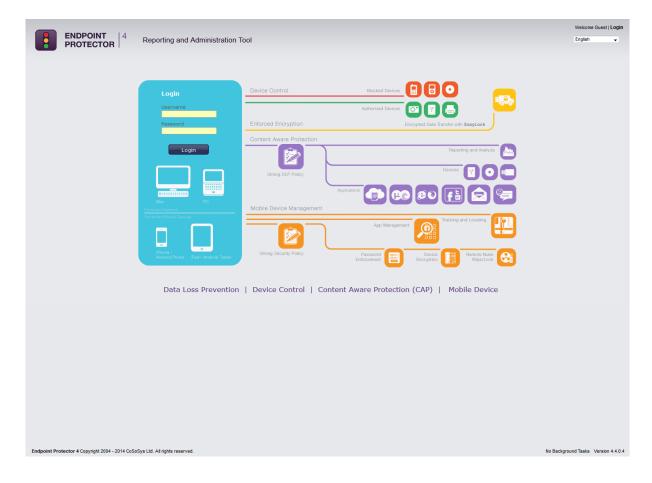
Certificate Import Wizard		×		
Completing the Certificate Import Wizard The certificate will be imported after you click Finish.				
	You have specified the following Certificate Store Selected by U Content File Name			
	< <u> </u>	4		
	< <u>B</u> ack	Finish Cancel		

A Security Warning window pops up. Just click "Yes".

ecurity W	/arning
Â	You are about to install a certificate from a certification authority (CA) claiming to represent:
	CoSoSys LTD - Endpoint Protector CA
	Windows cannot validate that the certificate is actually from "CoSoSys LTD - Endpoint Protector CA". You should confirm its origin by contacting "CoSoSys LTD - Endpoint Protector CA". The following number will assist you in this process:
	Thumbprint (sha1): ECF18C78 B5FEF644 0FAFB85C D1991CBA 12DD6D05
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
	Do you want to install this certificate?
	<u>Y</u> es <u>N</u> o

You have now successfully installed the Certificate.

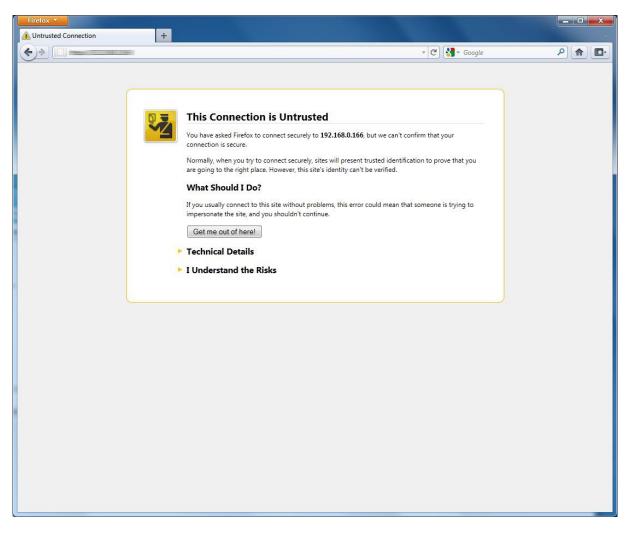
Close the Internet Explorer browser and try accessing the Endpoint Protector Administration and Reporting Tool IP address again.



### 19.2. For Mozilla Firefox

Open the Browser.

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



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.

Server	condice burnes, a		ther public sites wi	, not usk jou	to do tins.
Location:				<u>G</u> et (	Certificate
Certificate S	tatus				
This site att	empts to identify	itself with in	valid information.		View
Wrong Site					
Certificate b	elongs to a diffe	rent site, whi	ch could indicate an	identity theft.	
Unknown I	dentity				
Certificate is	not trusted, bec	ause it hasn'	t been verified by a i	ecognized aut	hority.

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 <u>http://www.cososys.com/help.html</u>.

You can also write an E-MAIL to our Support Department under the Contact Us tab from the Support module.

	<b>ENDPOINT</b> A Reporting and Administration Tool				English	•	Welcome   Logout Q Advanced Search
	Dashboard	Contact Support					
	Endpoint Management	Support Form					
Sp	Endpoint Rights	Sender E-mail *					
X	Endpoint Settings	Company Name	CSS				
0	Content Aware Protection (CAP)	Subject Content	Please describe here your problem or your suggestions!				
	Mobile Device Management						
	Offline Temporary Password						
<u>~</u>	Reports and Analysis						
	Alerts						
ø	Directory Services	Send					
	Appliance						
×	System Maintenance						
	System Configuration						
	System Parameters						
	Support						
	Ueer Manual MON User Manual AD Deployment Guide Contact Support						
Endor	pint Protector 4 Copyright 2004 - 2014 Co	SoSvs Ltd. All rights reserved.				No Background 1	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.

© 2004 – 2016 CoSoSys Ltd.; Endpoint Protector Basic, Endpoint Protector and My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.