ENDPOINT PROTECTOR

User Manual for Version 5.2.0.6

User Manual

COSOSYS

Table of Contents

1. Introduction

Portable storage devices such as USB flash drives, external HDDs, digital cameras, MP3 players and iPods are virtually everywhere and are connected to a Windows, Mac or Linux computer within seconds. With virtually every computer having access to internet, online applications and collaboration tools, data theft or accidental data loss becomes a mere child's play.

Data loss and data theft through a simple internet connection or USB device is easy and does not take more than a few seconds. Network Administrators had little chance to prevent this from happening or to identify the responsible users. This was the hard reality until now.

Endpoint Protector, through its Device Control, Content Aware Protection, eDiscovery and Enforced Encryption modules, helps companies stop these threats. It not only controls all device activity at the endpoints, but monitors and scans all possible exit points for sensitive content detection. It ensures critical business data does not leave the internal network either by being copied on devices or sent via the Internet without authorization, reporting all sensitive data incidents. Moreover, data at rest residing on endpoints can be inspected for sensitive content and remediation actions can be taken. Additionally, enforcing encryption on the USB removable devices is also possible. Everything from a single web-based interface.

Information

Endpoint Protector is a complete Data Loss Prevention and Enterprise Mobility Management solution. While the DLP related features and functionality will be explained below, please reference the MDM User Manual for information related to smartphones and tablets. Additional information regarding deployment of the Endpoint Protector Server can be found in the Virtual and Hardware Appliance User Manual.

1.1. Main components

Endpoint Protector is designed around several physical entities:

- Computers
  Windows, Mac and Linux workstations that have the 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.

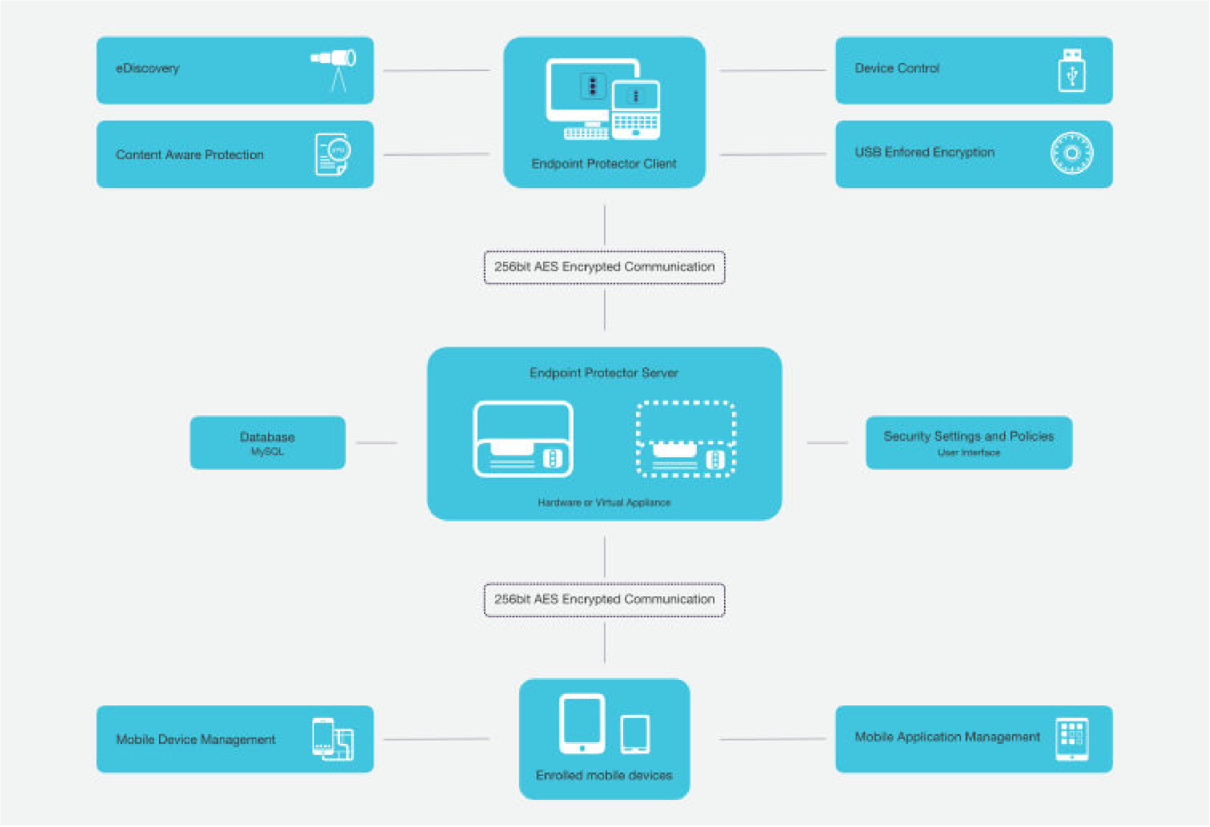
- Users
  The user who will be handling the devices and the computers.

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

- Endpoint Protector Hardware or Virtual Appliance – containing Operating System, Database, etc.

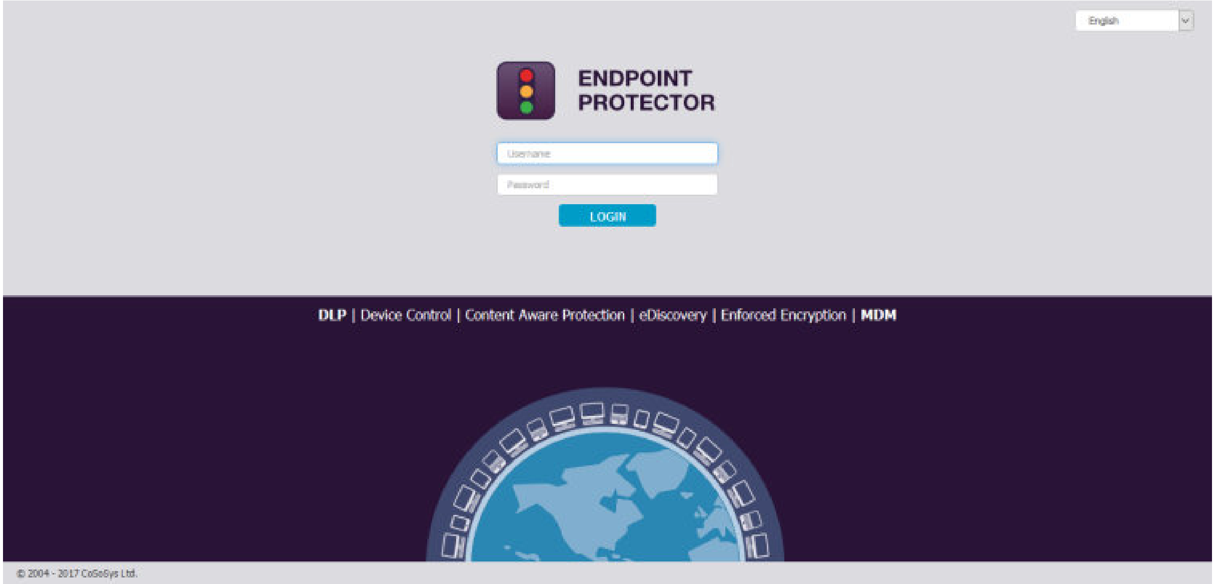
- Web Service – communicating with the Endpoint Protector Clients and storing the information received from them

- Endpoint Protector User Interface – managing the existing devices, computers, users, groups and their behavior in the entire system


eDiscovery
Content Aware Protection
Endpoint Protector Client
Device Control
USB Enfored Encryption
256bit AES Encrypted Communication
Endpoint Protector Server
Database
MySQL
Hardware or Virtual Appliance
Security Settings and Policies
User Interface
256bit AES Encrypted Communication
Mobile Device Management
Enrolled mobile devices
Mobile Application Management

2. Server Functionality

After the Endpoint Protector Hardware or Virtual Appliance setup, the User Interface can be accessed by simply entering the assigned IP address. The default Endpoint Protector Appliance IP address is https://192.168.0.201.


English
ENDPOINT PROTECTOR
Username
Password
LOGIN
DLP | Device Control | Content Aware Protection | eDiscovery | Enforced Encryption | MDM
© 2004 - 2017 CoSoSys Ltd.

Information

The default login credentials for Endpoint Protector are:

Username: root

Password: epp2011

To change these settings or to create additional administrators, please see chapter 15.4 System Administrators.

Note

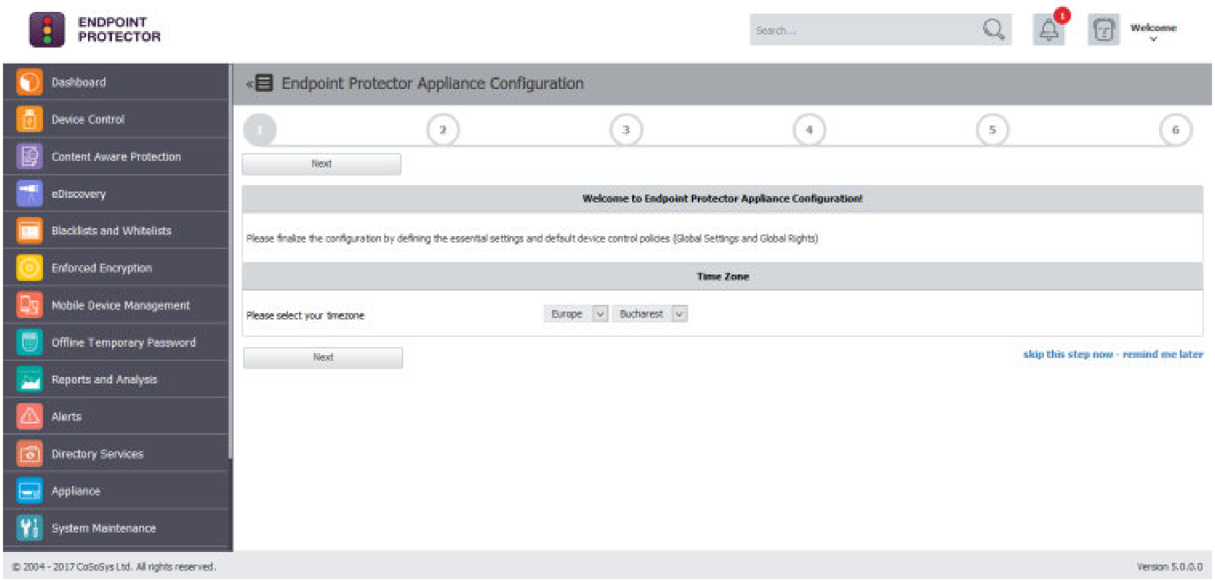
When entering the IP address, the HTTPS (Hypertext Transfer Protocol Secure) prefix must be used.

2.1. Endpoint Protector Configuration Wizard

The Configuration Wizard offers the Administrator some simple steps to define some basic settings. These include setting up the Server Time Zone, importing Licenses, Server Update or uploading Offline Patches, Global device rights, E-mail Server settings, Main Administrator details, etc. The settings can later be changed at any time.

Information

The Configuration Wizard only appears if the basic settings for Endpoint Protector have never been configured.



Endpoint Protector Appliance Configuration

Welcome to Endpoint Protector Appliance Configuration!

Please finalize the configuration by defining the essential settings and default device control policies (Global Settings and Global Rights)

Time Zone

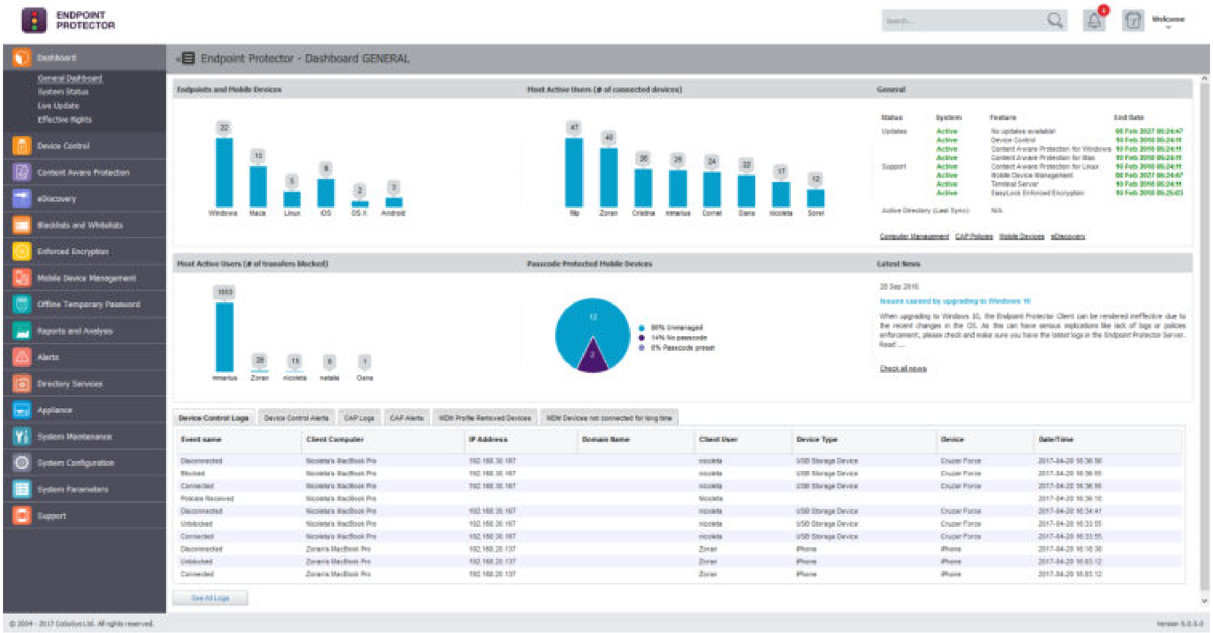
Please select your timezone: Europe, Bucharest

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

2.2. General Dashboard

This section offers a quick overview in the form of graphics and charts related to the most important activities logged by Endpoint Protector. General system information about licenses or latest news can also be found here. Additional information related to Device Control, Content Aware Protection and Mobile Device Management also displayed.



General

Status	System	Feature	End Date
Updates	Active	No updates available!	06 Feb 2027 05:24:47
	Active	Device Control	10 Feb 2018 05:24:11
	Active	Content Aware Protection for Windows	10 Feb 2018 05:24:11
	Active	Content Aware Protection for Mac	10 Feb 2018 05:24:11
Support	Active	Content Aware Protection for Linux	10 Feb 2018 05:24:11
	Active	Mobile Device Management	06 Feb 2027 05:24:47
	Active	Terminal Server	10 Feb 2018 05:24:11
	Active	EasyLock Enforced Encryption	10 Feb 2018 05:25:03

Active Directory (Last Sync): N/A

Computer Management CAP Policies Mobile Devices eDiscovery

Latest News

20 Sep 2016

Issues caused by upgrading to Windows 10

When upgrading to Windows 10, the Endpoint Protector Client can be rendered ineffective due to the recent changes in the OS. As this can have serious implications like lack of logs or policies enforcement, please check and make sure you have the latest logs in the Endpoint Protector Server. Read ...

Check all news

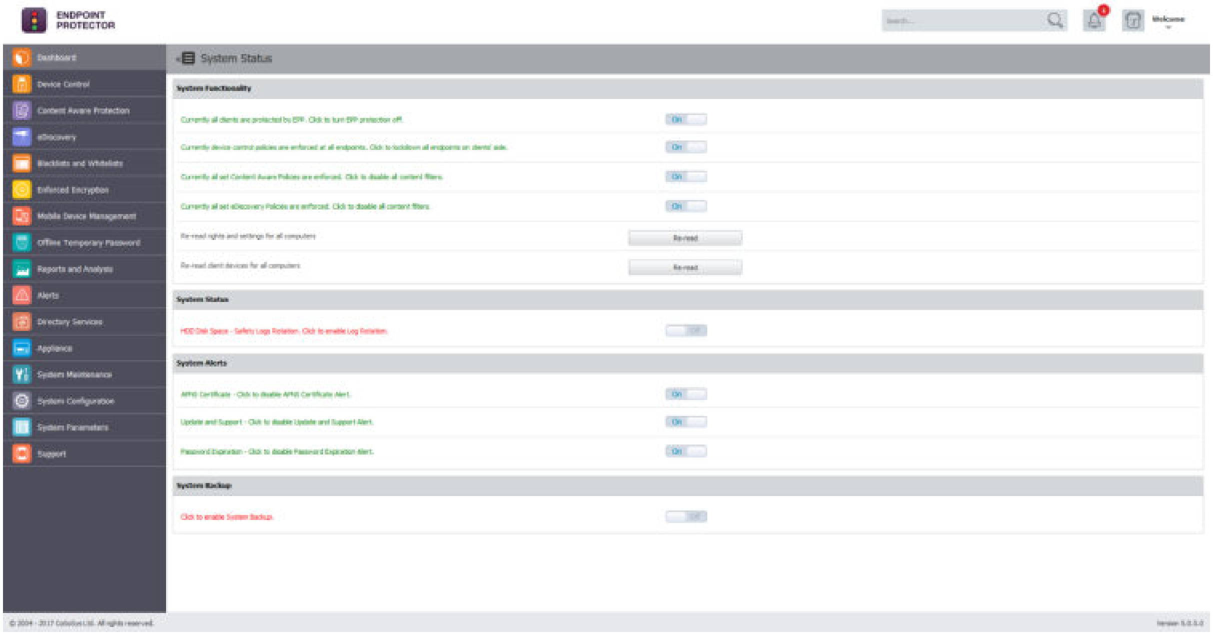
Event name	Client Computer	IP Address	Domain Name	Client User	Device Type	Device	Date/Time
Disconnected	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:36:56
Blocked	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:36:55
Connected	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:36:55
Policies Received	Nicoleta's MacBook Pro			Nicoleta			2017-04-20 16:36:10
Disconnected	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:34:41
Unblocked	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:33:55
Connected	Nicoleta's MacBook Pro	192.168.30.167		nicoleta	USB Storage Device	Cruzer Force	2017-04-20 16:33:55
Disconnected	Zoran's MacBook Pro	192.168.20.137		Zoran	iPhone	iPhone	2017-04-20 16:16:30
Unblocked	Zoran's MacBook Pro	192.168.20.137		Zoran	iPhone	iPhone	2017-04-20 16:03:12
Connected	Zoran's MacBook Pro	192.168.20.137		Zoran	iPhone	iPhone	2017-04-20 16:03:12

Information

More specific Dashboards are available at Device Control, Content Aware Protection and Mobile Device Management.

2.3. System Status

This section offers a quick overview on the system's functionality, alerts and backup status. There are several main functionalities that can be turned ON or OFF with just a click of a button.



System Functionality

Currently all clients are protected by EPP. Click to turn EPP protection off. On

Currently device control policies are enforced at all endpoints. Click to lockdown all endpoints on clients' side. On

Currently all set Content Aware Policies are enforced. Click to disable all content filters. On

Currently all set eDiscovery Policies are enforced. Click to disable all content filters. On

Re-read rights and settings for all computers Re-read

Re-read client devices for all computers Re-read

System Status

HDD Disk Space - Safety Logs Rotation. Click to enable Log Rotation. Off

System Alerts

APNS Certificate - Click to disable APNS Certificate Alert. On

Update and Support - Click to disable Update and Support Alert. On

Password Expiration - Click to disable Password Expiration Alert. On

System Backup

Click to enable System Backup. Off

From the System Functionality subsection, Endpoint Protector can be turned ON or OFF, as well as just specific modules (Device Control, Content Aware Protection or eDiscovery).

From the System Status subsection, the HDD Disk Space and Log Rotation can be turned ON or OFF.

Information

If this setting is ON, when the Server's disk space reaches a certain percentage, old logs will be automatically overwritten with the new ones coming in.

The percentage can be set starting with 50%, 60%, etc. up to 90%.

From the System Alerts subsection, important alerts notifying the expiration of the APNS Certificate, Updates and Support or Passwords can be turned ON or OFF.

From the System Backup subsection, the System Backup can be turned ON or OFF.

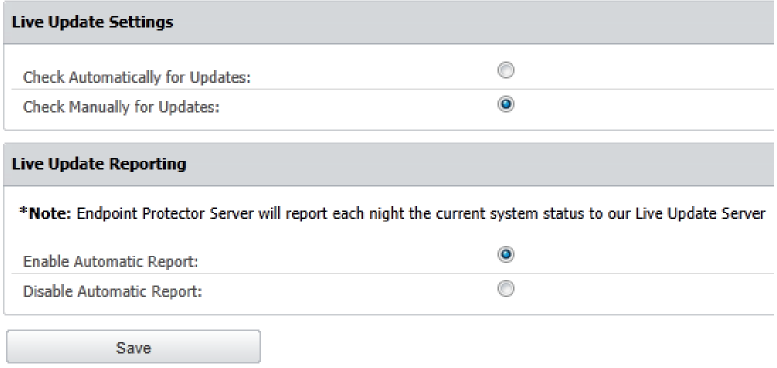
2.4. Live Update

This section allows checking and applying the latest Endpoint Protector Server updates.

Note

This feature communicates through port 80.

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



Live Update Settings

Check Automatically for Updates: ○

Check Manually for Updates: ●

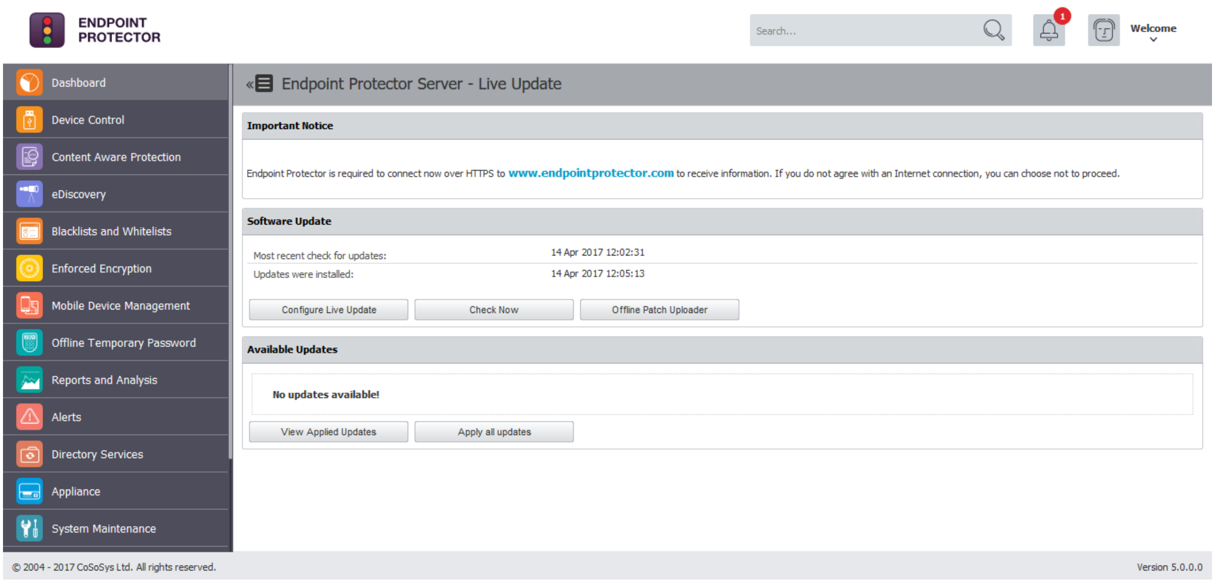
Live Update Reporting

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

Enable Automatic Report: ●

Disable Automatic Report: ○

By pressing the Check Now button, a search for the Endpoint Protector Server updates will begin.



Endpoint Protector Server - Live Update

Important Notice

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

Software Update

Most recent check for updates:	14 Apr 2017 12:02:31
Updates were installed:	14 Apr 2017 12:05:13

Available Updates

No updates available!

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

In case new updates are found, they are displayed under the Available Updates 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.

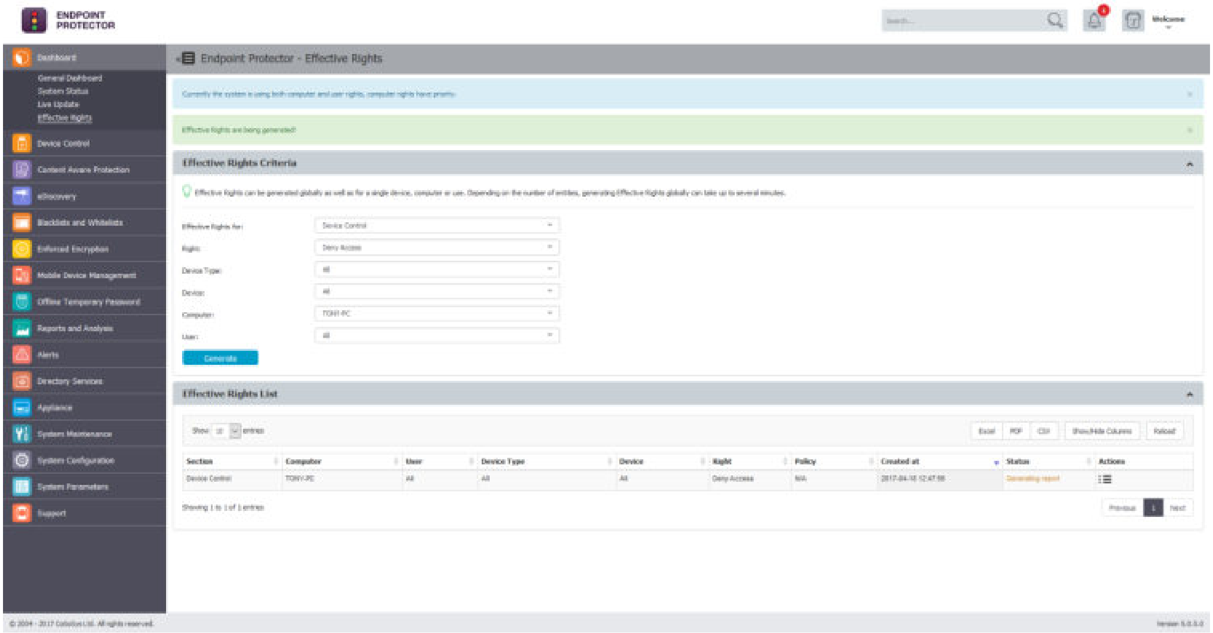
The Offline Patch Uploader offers the possibility to upload updates in situations where an internet connection is not available.

⚠ **Note**

Contact support@endpointprotector.com to request the Offline Patch.

2.5. 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 - Effective Rights

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

Effective Rights are being generated!

Effective Rights Criteria

Effective Rights can be generated globally as well as for a single device, computer or user. Depending on the number of entities, generating Effective Rights globally can take up to several minutes.

Effective Rights for: Device Control

Rights: Deny Access

Device Type: All

Device: All

Computer: TONY-PC

User: All

Generate

Effective Rights List

Show 10 entries

Excel | PDF | CSV | Show/Hide Columns | Reload

Section	Computer	User	Device Type	Device	Right	Policy	Created at	Status	Actions
Device Control	TONY-PC	All	All	All	Deny Access	N/A	2017-04-10 12:47:08	Generating report	☰

Showing 1 to 1 of 1 entries

Previous | 1 | Next

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.5.0

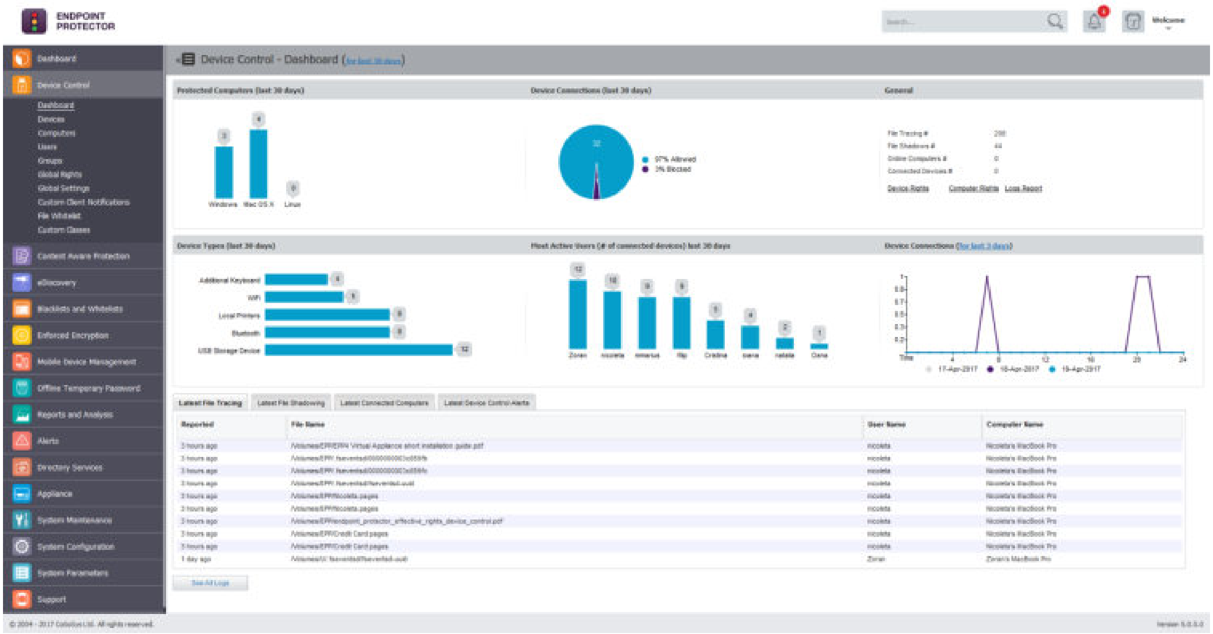
3. Device Control

From this section, the Administrator can manage all entities in the system, their subsequent rights and settings. The subsections are Dashboard, Devices, Computers, Users, Groups, Global (Rights and Settings), Custom Client Notifications, File Whitelists and Custom Classes.

While it includes some additional settings, this section can be considered the Device Control module. As the first layer of security within Endpoint Protector, it is activated by default in every configuration provided.

3.1. Dashboard

This section offers a quick overview in the form of graphics and charts related to the Endpoint Protector Entities. Additional information like the latest File Traces and File Shadows, latest Device Control Alerts, last connected Computers and most active Users are also displayed.



File Tracing # 200
File Shadows # 44
Online Computers # 0
Connected Devices # 0

Device Rights Computer Rights Logs Report

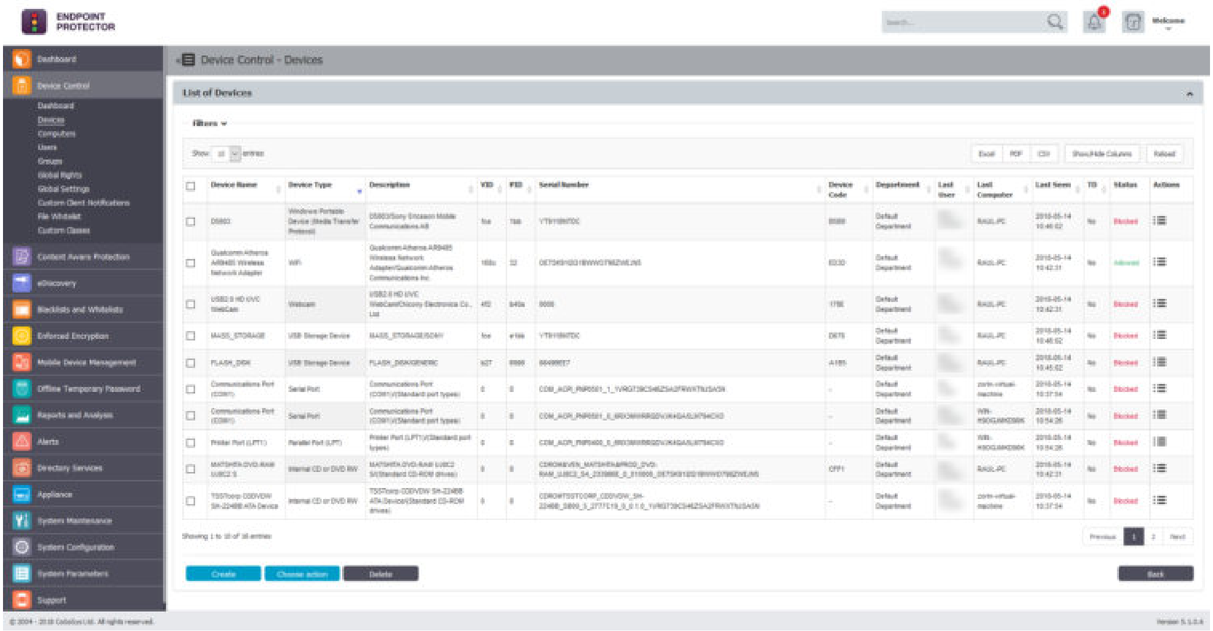
Latest File Tracing | Latest File Shadowing | Latest Connected Computers | Latest Device Control Alerts

Reported	File Name	User Name	Computer Name
3 hours ago	/Volumes/EPP/EPP Virtual Appliance short installation guide.pdf	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/.fseventsd/0000000003c059fe	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/.fseventsd/0000000003c059fe	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/.fseventsd/fseventsd-uuid	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/Nicoleta.pages	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/Nicoleta.pages	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/endpoint_protector_effective_rights_device_control.pdf	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/Credit Card.pages	nicoleta	Nicoleta's MacBook Pro
3 hours ago	/Volumes/EPP/Credit Card.pages	nicoleta	Nicoleta's MacBook Pro
1 day ago	/Volumes/U/.fseventsd/fseventsd-uuid	Zoran	Zoran's MacBook Pro

See All Logs

3.2. Devices

From this section, the Administrator can manage all devices in the system. Any new device connected to a protected computer is automatically added to the database, thus making it manageable.



□	Device Name	Device Type	Description	VID	PID	Serial Number	Device Code	Department	Last User	Last Computer	Last Seen	TD	Status	Actions
□	D5803	Windows Portable Device (Media Transfer Protocol)	D5803/Sony Ericsson Mobile Communications AB	fce	198	YT911BNTDC	8088	Default Department	[redacted]	RAUL-PC	2018-05-14 10:46:02	No	Blocked	☰
□	Qualcomm Atheros AR9485 Wireless Network Adapter	WiFi	Qualcomm Atheros AR9485 Wireless Network Adapter/Qualcomm Atheros Communications Inc	168c	32	0E7SK9102018WWO7M8ZWEJN5	E030	Default Department	[redacted]	RAUL-PC	2018-05-14 10:42:31	No	Allowed	☰
□	USB2.0 HD UVC WebCam	Webcam	USB2.0 HD UVC WebCam/Chicony Electronics Co., Ltd	4f2	b40a	0001	17BE	Default Department	[redacted]	RAUL-PC	2018-05-14 10:42:31	No	Blocked	☰
□	MASS_STORAGE	USB Storage Device	MASS_STORAGE/SONY	fce	e1bb	YT911BNTDC	D675	Default Department	[redacted]	RAUL-PC	2018-05-14 10:46:02	No	Blocked	☰
□	FLASH_DISK	USB Storage Device	FLASH_DISK/GENERIC	627	8999	86499EE7	A185	Default Department	[redacted]	RAUL-PC	2018-05-14 10:45:02	No	Blocked	☰
□	Communications Port (COM1)	Serial Port	Communications Port (COM1)/(Standard port types)	0	0	COM_ACPI_PNP0501_1_1VRGT39C346ZSA2FRWXT9USA5N	-	Default Department	[redacted]	zorin-virtual-machine	2018-05-14 10:37:54	No	Blocked	☰
□	Communications Port (COM1)	Serial Port	Communications Port (COM1)/(Standard port types)	0	0	COM_ACPI_PNP0501_0_8RX3WWRRQDVJK4GA5UXT94CXO	-	Default Department	[redacted]	WIN-HSOGJ4MKD98K	2018-05-14 10:54:26	No	Blocked	☰
□	Printer Port (LPT1)	Parallel Port (LPT)	Printer Port (LPT1)/(Standard port types)	0	0	COM_ACPI_PNP0400_0_8RX3WWRRQDVJK4GA5UXT94CXO	-	Default Department	[redacted]	WIN-HSOGJ4MKD98K	2018-05-14 10:54:26	No	Blocked	☰
□	MATSHITA DVD-RAM UJ8C2 S	Internal CD or DVD RW	MATSHITA DVD-RAM UJ8C2 S/(Standard CD-ROM drives)	0	0	CDROM&VEN_MATSHITA&PROD_DVD-RAM_UJ8C2_S4_2339BBB_0_010000_0E7SK9102018WWO7M8ZWEJN5	CFF1	Default Department	[redacted]	RAUL-PC	2018-05-14 10:42:31	No	Blocked	☰
□	TSSTcorp CDDVDW SH-224BB ATA Device	Internal CD or DVD RW	TSSTcorp CDDVDW SH-224BB ATA Device/(Standard CD-ROM drives)	0	0	CDROM TSSTCORP_CDDVDW_SH-224BB_SB00_3_2777C19_0_0.1.0_1VRGT39C346ZSA2FRWXT9USA5N	-	Default Department	[redacted]	zorin-virtual-machine	2018-05-14 10:37:54	No	Blocked	☰

Showing 1 to 10 of 18 entries

A device is identified by the device parameters (Vendor ID, Product ID, and Serial Number) but information like Name and Description of the device is also used. A device is assigned by default to the first user that handles the device. This, however, can later be changed.

The Administrator can manually create a new device at any time by providing the device parameters and information mentioned above. Devices can also be imported into Endpoint Protector from Active Directory.

Information

For more details about Active Directory, please see chapter 12 Directory Services.

The Actions column offers multiple option related to device management like Edit, Manage Rights, Device History and Delete.

The Status column indicates the current rights of the devices.

Information

There are several states a device can be in. As a general rule:

- red means the device is blocked in the system
- green means the device is allowed in computers or users
- yellow means the device is allowed on some users or computers with restrictions

If not otherwise configured, the device rights are inherited from the default Global Rights that are set per Device Types (USB Storage Device, Digital Camera, iPod, Thunderbolt, Chip Card Device, etc.).

Information

For more details about Device Type, please see paragraph 3.6.1.1 Device Types.

Note

If device rights will be configured granularly for all entities, the priority order, starting with the highest, will be:
Devices > Computers | Users > Groups > Global.

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.

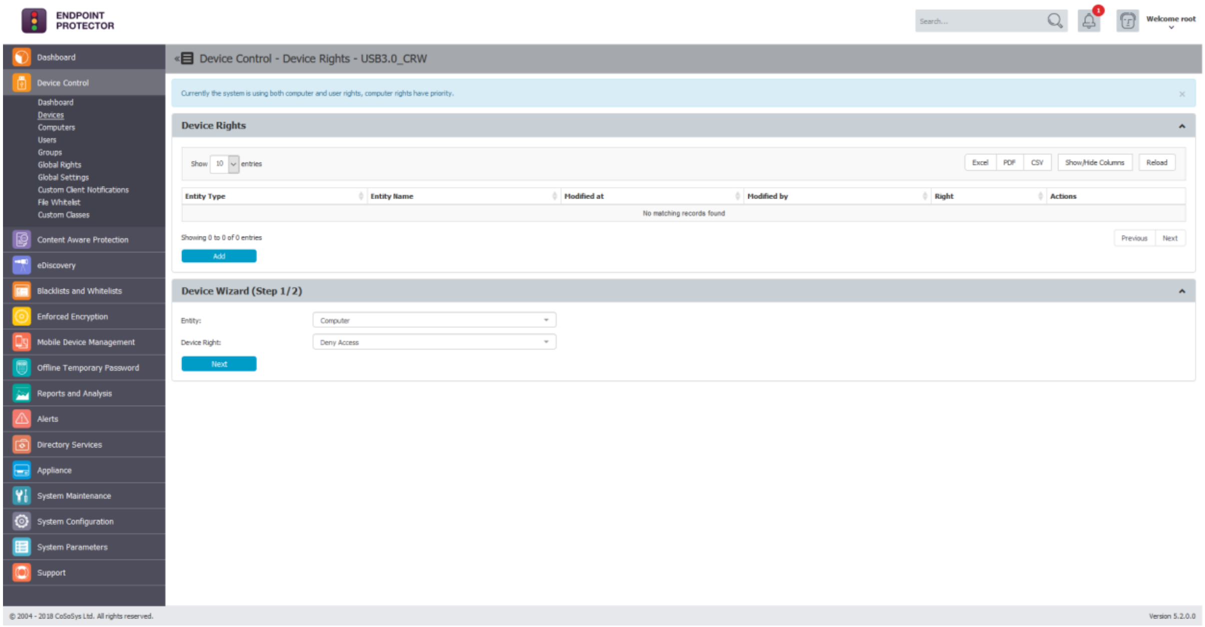
Information

The option to Export/Import Devices in JSON format is also available. This allows a list of devices to be exported from one Endpoint Protector Server and imported in a different Endpoint Protector Server.

This feature is intended to correlate the device rights and the Groups. Therefore, if the same Groups exist on both Servers, the imported devices will also maintain the access rights. If the Groups do not exist, the devices will still be imported but the access rights will be ignored.

3.2.1. Device Rights

The Device Rights can be accessed by going in the Actions column for the specific device and selecting Manage Rights. This section is built around the devices, allowing the Administrator to enable or disable them for specific computers, groups or users.



Device Control - Device Rights - USB3.0_CRW

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

Device Rights

Show 10 entries

Entity Type	Entity Name	Modified at	Modified by	Right	Actions
No matching records found					

Showing 0 to 0 of 0 entries

Device Wizard (Step 1/2)

Entity: Computer

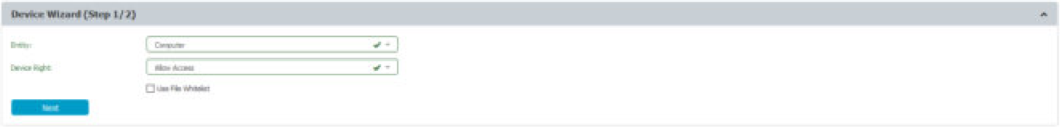
Device Right: Deny Access

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0

After selecting a device, assigning the specified rights to the desired users, computers or groups is straight forward, using the 2-step wizard:

- Select the Entity and the Device right



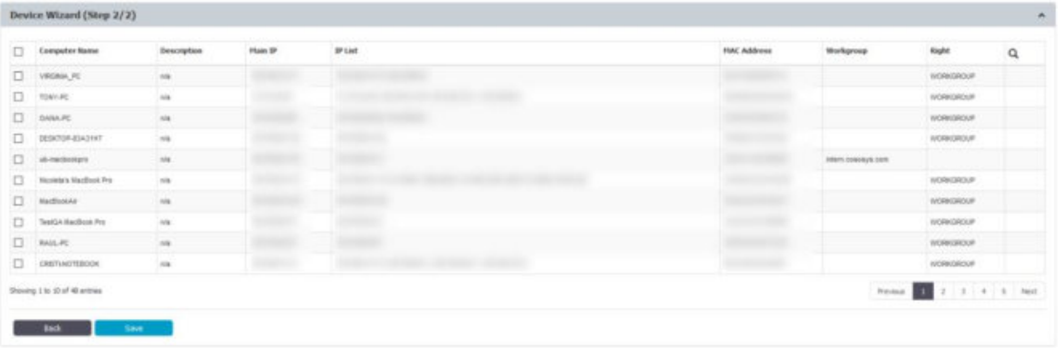
Device Wizard (Step 1/2)

Entity: Computer

Device Right: Allow Access

□ Use File Whitelist

- Select the Entities (Computers, Groups or Users)



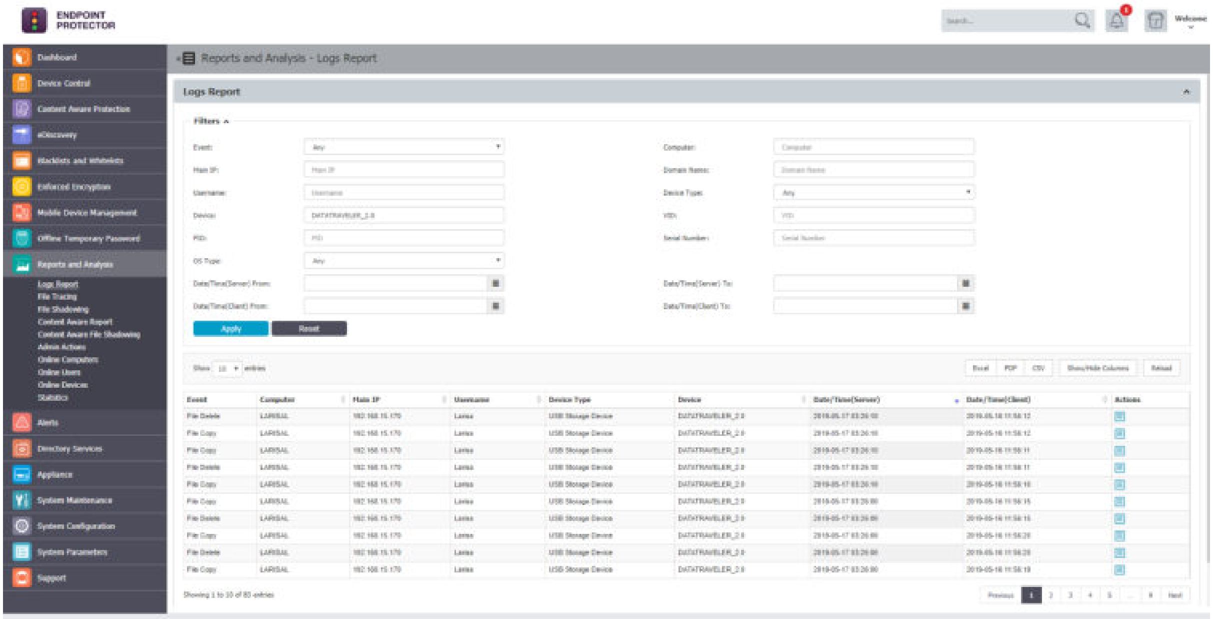
Device Wizard (Step 2/2)

□	Computer Name	Description	Main IP	IP List	MAC Address	Workgroup	Right
□	VIRGINIA_PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	TONY-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	DANA-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	DESKTOP-E3A31HT	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	ub-macbookpro	n/a	[redacted]	[redacted]	[redacted]	intern.cososys.com	
□	Nicoleta's MacBook Pro	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	MacBookAir	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	TestQA MacBook Pro	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	RAUL-PC	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP
□	CRISTI-NOTEBOOK	n/a	[redacted]	[redacted]	[redacted]		WORKGROUP

Showing 1 to 10 of 48 entries

3.2.2. Device History

From this section, the Administrator can view the device history by selecting the View Device History action. This will show the Logs Report page filtered for the respective device.



Logs Report

Event:	Any	Computer:	Computer
Main IP:	Main IP	Domain Name:	Domain Name
Username:	Username	Device Type:	Any
Device:	DATATRAVELER_2.0	VID:	VID
PID:	PID	Serial Number:	Serial Number
OS Type:	Any		
Date/Time(Server) From:		Date/Time(Server) To:	
Date/Time(Client) From:		Date/Time(Client) To:	

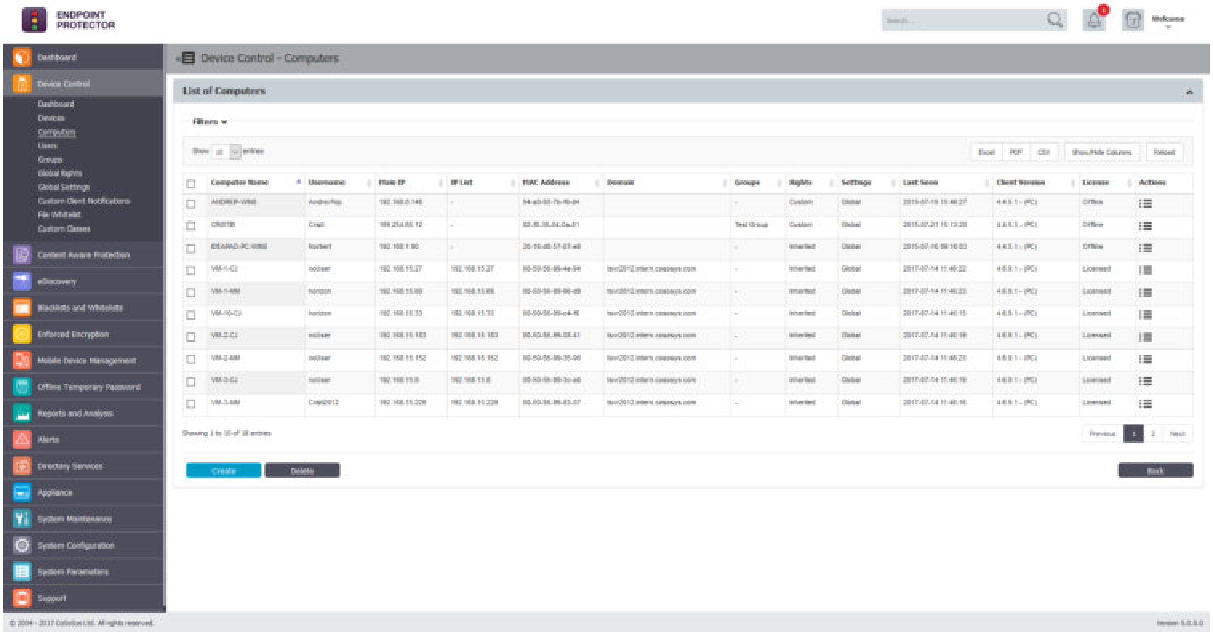
Show 10 entries

Event	Computer	Main IP	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:12	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:12	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:11	
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:11	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:16	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:00	2019-05-16 11:58:15	
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:00	2019-05-16 11:58:15	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:00	2019-05-16 11:58:20	
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:00	2019-05-16 11:58:20	
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:00	2019-05-16 11:58:19	

Showing 1 to 10 of 83 entries

3.3. Computers

From this section, the Administrator can manage all computers in the system. Any new computer that has the Endpoint Protector Client deployed will be automatically added to the database, thus making it manageable.



List of Computers

Show 10 entries

□	Computer Name	Username	Main IP	IP List	MAC Address	Domain	Groups	Rights	Settings	Last Seen	Client Version	License	Actions
□	ANDREIP-WIN8	Andrei Pop	192.168.0.148	-	54-a0-50-7b-f6-04		-	Custom	Global	2015-07-15 15:48:27	4.4.5.1 - (PC)	Offline	☰
□	CRISTIB	Cristi	169.254.85.12	-	02-f6-35-04-0a-01		Test Group	Custom	Global	2015-07-21 15:13:20	4.4.5.3 - (PC)	Offline	☰
□	IDEAPAD-PC-WIN8	Norbert	192.168.1.90	-	20-16-d8-57-07-e8		-	Inherited	Global	2015-07-16 09:16:03	4.4.5.1 - (PC)	Offline	☰
□	VM-1-CJ	[illegible]	192.168.15.27	192.168.15.27	00-50-56-89-4e-94	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:22	4.6.8.1 - (PC)	Licensed	☰
□	VM-1-AM	horizon	192.168.15.69	192.168.15.69	00-50-56-89-66-d9	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:23	4.6.8.1 - (PC)	Licensed	☰
□	VM-10-CJ	horizon	192.168.15.33	192.168.15.33	00-50-56-86-c4-f6	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:15	4.6.8.1 - (PC)	Licensed	☰
□	VM-2-CJ	[illegible]	192.168.15.183	192.168.15.183	00-50-56-89-08-41	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:19	4.6.8.1 - (PC)	Licensed	☰
□	VM-2-AM	[illegible]	192.168.15.152	192.168.15.152	00-50-56-89-35-00	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:23	4.6.8.1 - (PC)	Licensed	☰
□	VM-3-CJ	[illegible]	192.168.15.8	192.168.15.8	00-50-56-89-3c-a8	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:19	4.6.8.1 - (PC)	Licensed	☰
□	VM-3-AM	Cristi2012	192.168.15.228	192.168.15.228	00-50-56-89-83-07	tsvr2012.intern.cososys.com	-	Inherited	Global	2017-07-14 11:46:18	4.6.8.1 - (PC)	Licensed	☰

Showing 1 to 10 of 18 entries

The Endpoint Protector Client has a self-registration mechanism. This process is run once after the Client software is installed on a client computer. The Client will then communicate to the Server its existence in the system. The Server will store the information regarding the Computer in the database and it will assign a License.

⚠ **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.

Information

For more details about Licensing, please see chapter 15.9 System Licensing

A Computer is identified by the computer parameters (Main IP, IP List, MAC, Domain or Workgroup) but information like Name and Description is also essential. A computer is assigned by default to the first user that handles the computer. This, however, can later be changed and is updated automatically based on whoever logs into the computer.

The Administrator can manually create a new computer at any time by providing the computer parameters and information mentioned above. Computers can also be imported into Endpoint Protector from Active Directory.

Information

For more details about Active Directory, please see chapter 12 Directory Services.

Tips

For a better organization, computers can be assigned to:

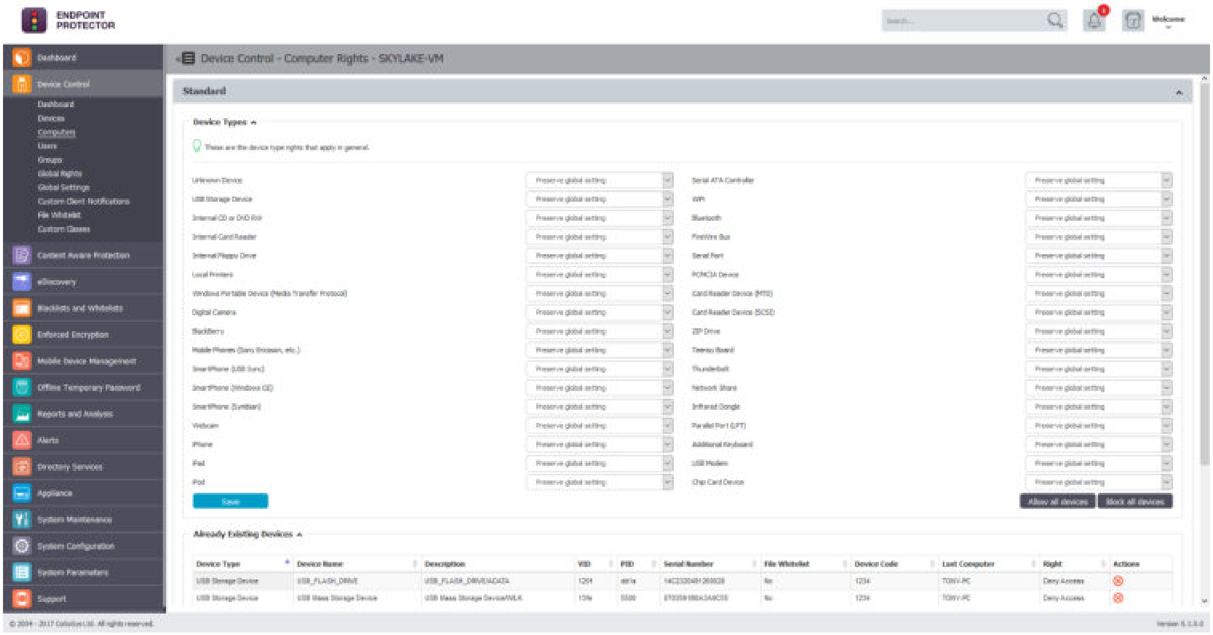
- Groups (e.g. several computers within the same office)

  For more details about Groups, please see chapter 3.5 Groups.
- Department (an alternative organization to Groups).

  For more details about Departments, please see chapter 15.6 System Departments.

3.3.1. Computer Rights

The Computer Rights can be accessed by going in the Actions column for the specific computer and selecting Manage Rights. This section is built around the computers, allowing the Administrator to specify which Device Types and also which Specific Devices can be accessible.



Device Control - Computer Rights - SKYLAKE-VM

Standard

Device Types

These are the device type rights that apply in general.

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

Already Existing Devices

Device Type	Device Name	Description	VID	PID	Serial Number	File Whitelist	Device Code	Last Computer	Right	Actions
USB Storage Device	USB_FLASH_DRIVE	USB_FLASH_DRIVE/ADATA	125f	db1a	14C2320481280028	No	1234	TONY-PC	Deny Access	⊗
USB Storage Device	USB Mass Storage Device	USB Mass Storage Device/WLK	13fe	5500	0703591BBEA3A9C58	No	1234	TONY-PC	Deny Access	⊗

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.1.3.0

Tips

The Standard device control rights includes the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, the administrator can create fallback policies for Outside Network and Outside Hours circumstances.

Information

For more details about Device Types and Specific Devices (Standard, Outside Network and Outside Hours), please see chapter 3.6.1 Global Rights.

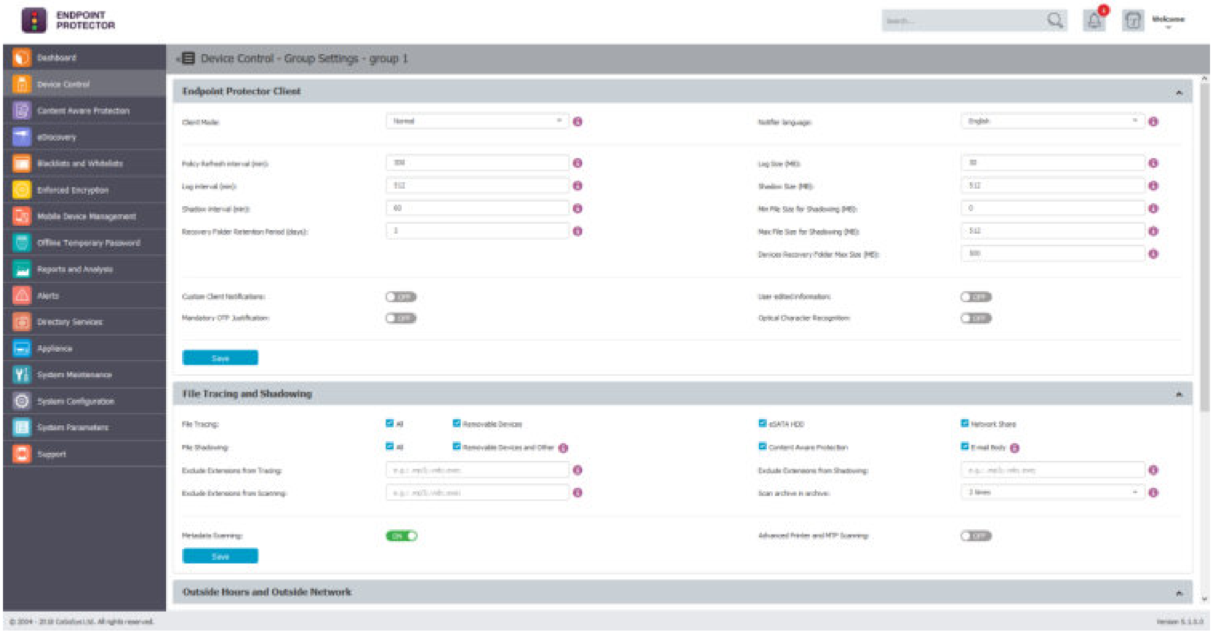
Note

The 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.

All Existing Devices that were added on that level will be deleted when the restore is used.

3.3.2. Computer Settings

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



Device Control - Group Settings - group 1

Endpoint Protector Client

Client Mode: Normal
Notifier language: English
Policy Refresh interval (sec): 300
Log interval (min): 512
Shadow interval (min): 60
Recovery Folder Retention Period (days): 1
Log Size (MB): 10
Shadow Size (MB): 512
Min File Size for Shadowing (MB): 0
Max File Size for Shadowing (MB): 512
Devices Recovery Folder Max Size (MB): 500
Custom Client Notifications: OFF
Mandatory OTP Justification: OFF
User edited information: OFF
Optical Character Recognition: OFF

File Tracing and Shadowing

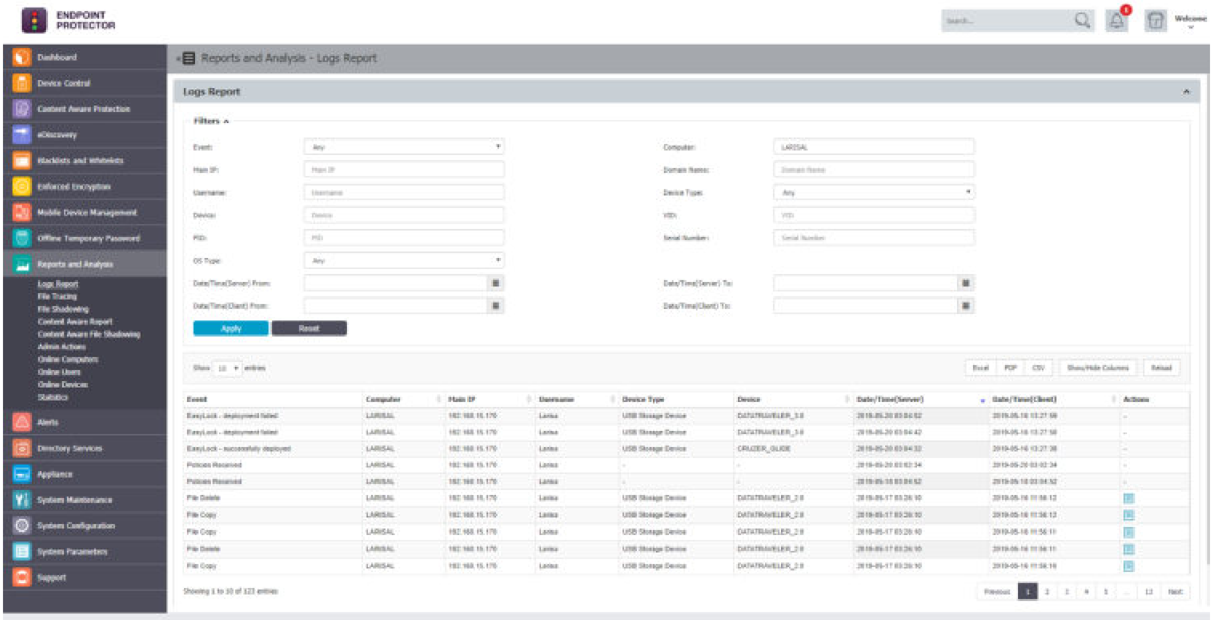
File Tracing: ☑ All ☑ Removable Devices ☑ eSATA HDD ☑ Network Share
File Shadowing: ☑ All ☑ Removable Devices and Other ☑ Content Aware Protection ☑ E-mail Body
Exclude Extensions from Tracing: e.g.: .mp3;.mkv;.mov
Exclude Extensions from Shadowing: e.g.: .mp3;.mkv;.mov
Exclude Extensions from Scanning: e.g.: .mp3;.mkv;.mov
Scan archive in archive: 2 times
Metadata Scanning: ON
Advanced Printer and MTP Scanning: OFF

Outside Hours and Outside Network

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 from the group it belongs to or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

3.3.3. Computer History

From this section, the Administrator can view the computer history by selecting the View Computer History action. This will show the Logs Report page filtered for the respective computer.



Reports and Analysis - Logs Report

Logs Report

Filters

Event: Any
Computer: LARISAL
Main IP: Main IP
Domain Name: Domain Name
Username: Username
Device Type: Any
Device: Device
VID: VID
PID: PID
Serial Number: Serial Number
OS Type: Any
Date/Time(Server) From:
Date/Time(Server) To:
Date/Time(Client) From:
Date/Time(Client) To:

Show 10 entries

Event	Computer	Main IP	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
EasyLock - deployment failed	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_3.0	2019-05-20 03:04:52	2019-05-16 13:27:58	-
EasyLock - deployment failed	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_3.0	2019-05-20 03:04:42	2019-05-16 13:27:58	-
EasyLock - successfully deployed	LARISAL	192.168.15.170	Larisa	USB Storage Device	CRUZER_GLIDE	2019-05-20 03:04:32	2019-05-16 13:27:38	-
Policies Received	LARISAL	192.168.15.170	Larisa	-	-	2019-05-20 03:02:34	2019-05-20 03:02:34	-
Policies Received	LARISAL	192.168.15.170	Larisa	-	-	2019-05-18 03:04:52	2019-05-18 03:04:52	-
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:12	▤
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:12	▤
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:11	▤
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:11	▤
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:10	▤

Showing 1 to 10 of 123 entries

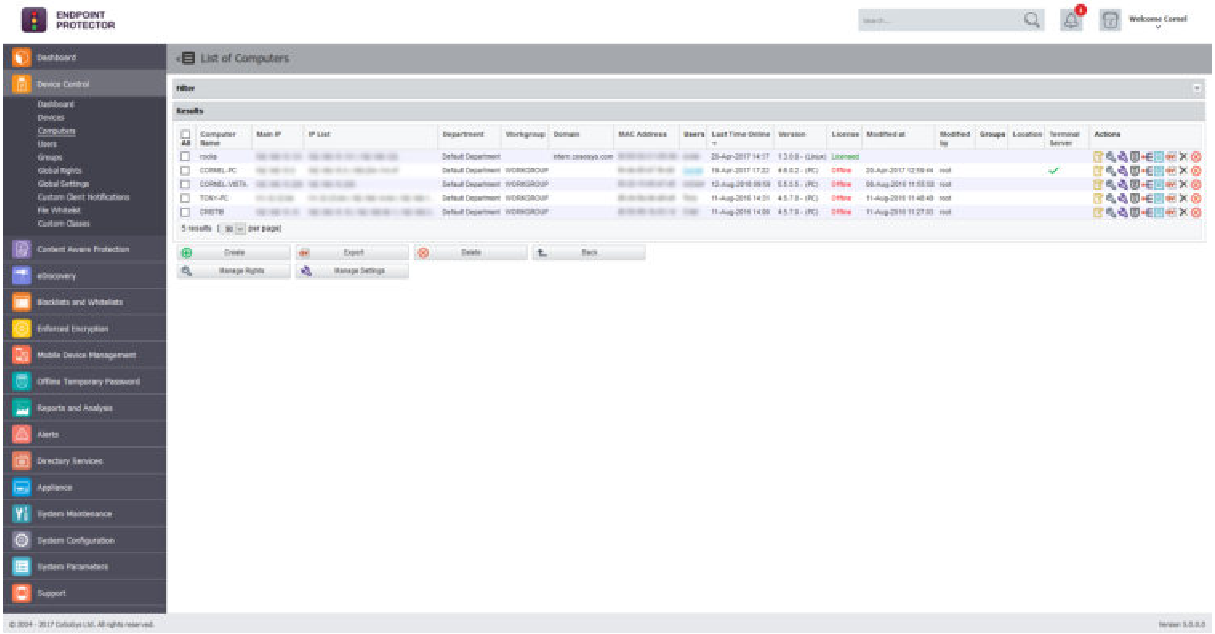
3.3.4. Terminal Servers and Thin Clients

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.

3.3.4.1. Initial Configuration

The process starts with the menu view from Device Control > Computers, namely the action to **Mark as Terminal Server** ·E|.

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



List of Computers

Filter

Results

□ All	Computer Name	Main IP	IP List	Department	Workgroup	Domain	MAC Address	Users	Last Time Online	Version	License	Modified at	Modified by	Groups	Location	Terminal Server	Actions
□	roots	[redacted]	[redacted]	Default Department		intern.cososys.com	[redacted]	[redacted]	20-Apr-2017 14:17	1.3.0.8 - (Linux)	Licensed						
□	CORNEL-PC	[redacted]	[redacted]	Default Department	WORKGROUP		[redacted]	[redacted]	19-Apr-2017 17:22	4.6.0.2 - (PC)	Offline	20-Apr-2017 12:59:44	root			✓	
□	CORNEL-VISTA	[redacted]	[redacted]	Default Department	WORKGROUP		[redacted]	[redacted]	12-Aug-2016 08:59	5.5.5.5 - (PC)	Offline	08-Aug-2016 11:55:50	root				
□	TONY-PC	[redacted]	[redacted]	Default Department	WORKGROUP		[redacted]	[redacted]	11-Aug-2016 14:31	4.5.7.0 - (PC)	Offline	11-Aug-2016 11:48:49	root				
□	CRISTB	[redacted]	[redacted]	Default Department	WORKGROUP		[redacted]	[redacted]	11-Aug-2016 14:00	4.5.7.0 - (PC)	Offline	11-Aug-2016 11:27:03	root				

5 results [50] per page]

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

Note

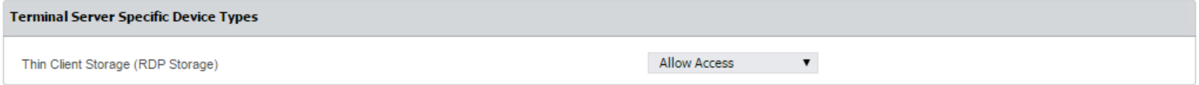
The computers that can be targeted by this action are strictly Windows Servers with Terminal Server roles properly configured

Information

Make sure that there is at least one 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 Device Control > Computers > 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

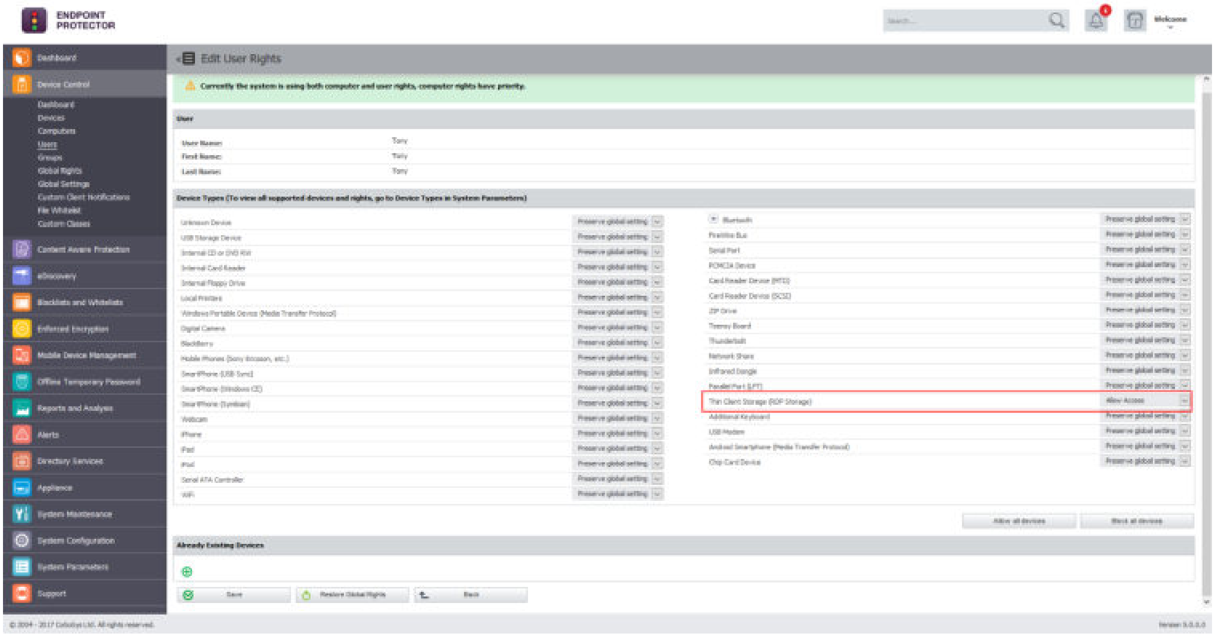
Thin Client Storage (RDP Storage)	Allow Access ▼

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 Device Control > Users > Rights will present an additional device type for all the users in Endpoint Protector, namely Thin Client Storage (RDP Storage).



Edit User Rights

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

User

User Name:	Tony
First Name:	Tony
Last Name:	Tony

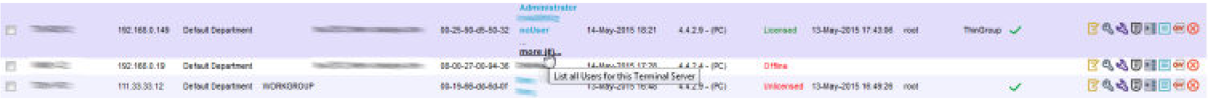
Device Types (To view all supported devices and rights, go to Device Types in System Parameters)

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

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

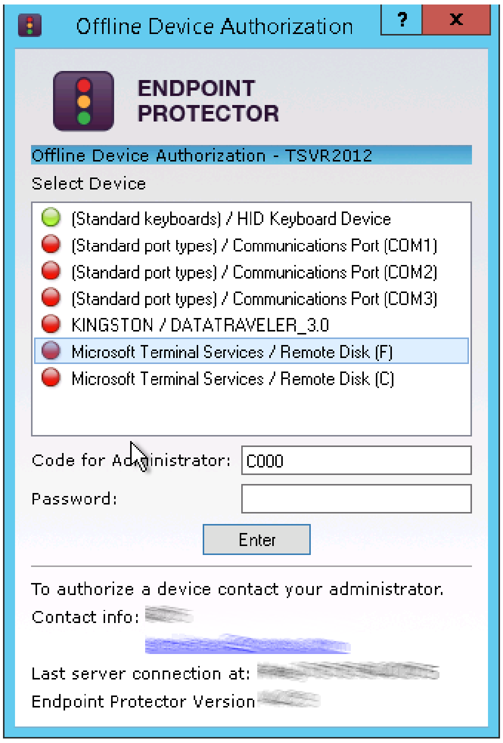
Multiple users can be recognized as active users on any given Terminal Server, and so, this rights setting can be used as a powerful tool to create access policies to specific users, as detailed in the use case below.



□	[redacted]	192.168.0.149	Default Department		[redacted]	08-25-90-d5-50-32	Administrator [redacted] rdUser ... more (4)...	14-May-2015 18:21	4.4.2.9 - (PC)	Licensed	13-May-2015 17:43:86	root	ThinGroup	✓
□	[redacted]	192.168.0.19	Default Department		[redacted]	08-00-27-00-94-36	[redacted]	14-May-2015 17:28	4.4.2.4 - (PC)	Offline				
□	[redacted]	111.33.33.12	Default Department	WORKGROUP		00-15-65-00-60-07	[redacted]	13-May-2015 16:48	4.4.2.9 - (PC)	Unlicensed	13-May-2015 16:49:26	root		✓

List all Users for this Terminal Server

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 - TSVR2012

Select Device

- ● (Standard keyboards) / HID Keyboard Device
- ● (Standard port types) / Communications Port (COM1)
- ● (Standard port types) / Communications Port (COM2)
- ● (Standard port types) / Communications Port (COM3)
- ● KINGSTON / DATATRAVELER_3.0
- ● Microsoft Terminal Services / Remote Disk (F)
- ● Microsoft Terminal Services / Remote Disk (C)

Code for Administrator: C000

Password:

To authorize a device contact your administrator.

Contact info: [redacted]

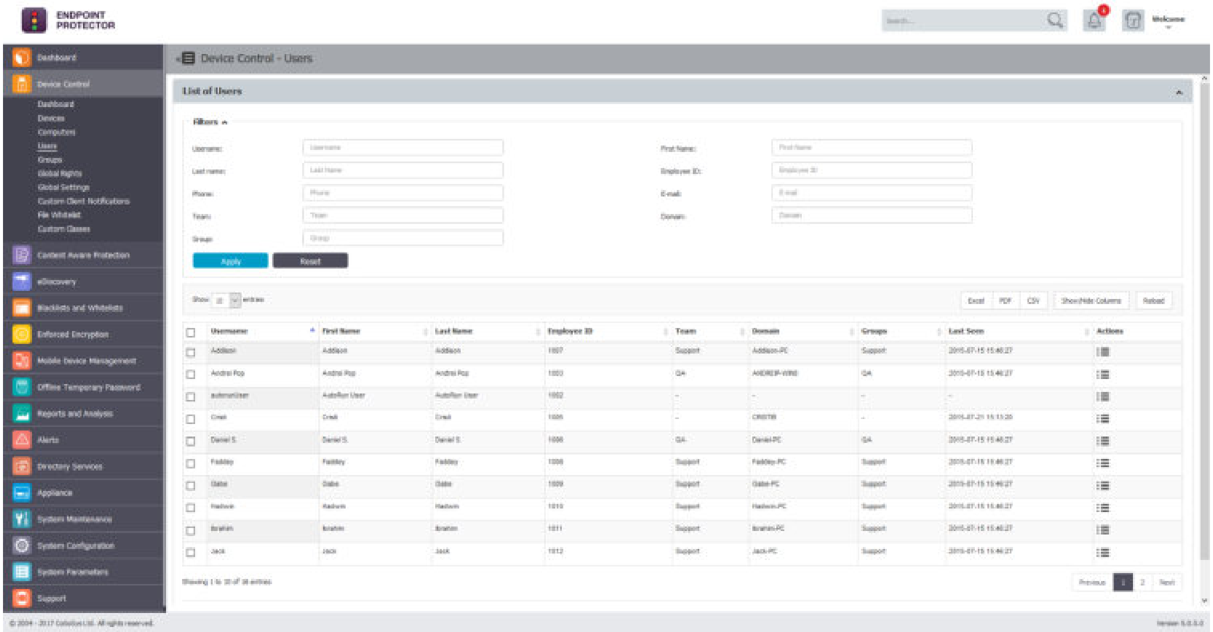
[redacted]

Last server connection at: [redacted]

Endpoint Protector Version [redacted]

3.4. Users

From this section, the Administrator can manage all the users in the system. Users are defined as the end users who are logged on a computer on which the Endpoint Protector Client software is installed. Any new user will be automatically added to the database, thus making them manageable.



□	Username	First Name	Last Name	Employee ID	Team	Domain	Groups	Last Seen	Actions
□	Addison	Addison	Addison	1007	Support	Addison-PC	Support	2015-07-15 15:40:27	☰
□	Andrei Pop	Andrei Pop	Andrei Pop	1003	QA	ANDREIP-WIN8	QA	2015-07-15 15:40:27	☰
□	autorunUser	AutoRun User	AutoRun User	1002	-	-	-	-	☰
□	Credi	Credi	Credi	1005	-	CREDTB	-	2015-07-21 15:13:20	☰
□	Daniel S.	Daniel S.	Daniel S.	1006	QA	Daniel-PC	QA	2015-07-15 15:40:27	☰
□	Faddey	Faddey	Faddey	1008	Support	Faddey-PC	Support	2015-07-15 15:40:27	☰
□	Gabe	Gabe	Gabe	1009	Support	Gabe-PC	Support	2015-07-15 15:40:27	☰
□	Hadwin	Hadwin	Hadwin	1010	Support	Hadwin-PC	Support	2015-07-15 15:40:27	☰
□	Ibrahim	Ibrahim	Ibrahim	1011	Support	Ibrahim-PC	Support	2015-07-15 15:40:27	☰
□	Jack	Jack	Jack	1012	Support	Jack-PC	Support	2015-07-15 15:40:27	☰

Showing 1 to 10 of 18 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.5.0

A user is identified by information like Name (Username, First Name, Last Name), Department, Contact Details (Phone, E-mail) and others and is also automatically assigned to a computer.

The Administrator can manually create a new user at any time by providing the user's parameters and information mentioned above. Users can also be imported into Endpoint Protector from Active Directory.

Information

For more details about Active Directory, please see chapter 12 Directory Services.

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 into 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.

Information

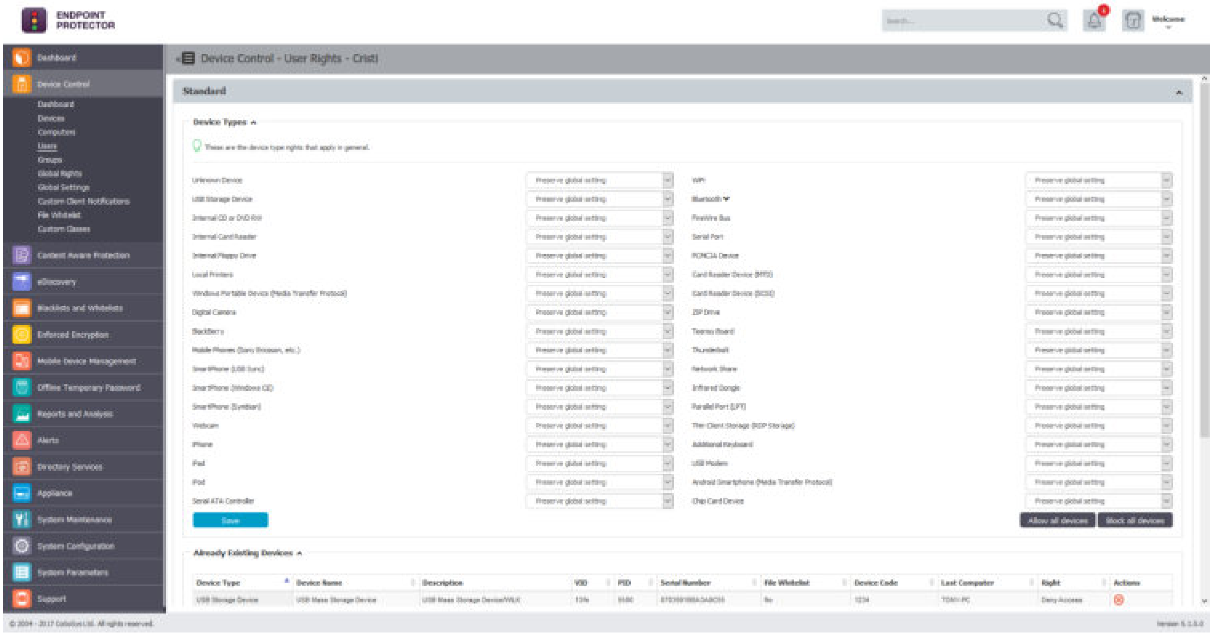
Depending on the OS, additional system users can appear:

- _mbsetupuser (for macOS, during updates)
- 65535, 62624, etc. (for Linux, during locked screens)

The Actions column offers multiple option related to user's management like Edit, Manage Rights, History and Delete.

3.4.1. User Rights

The User Rights can be accessed by going in the Actions column for the specific user and selecting Manage Rights. This section is built around the users, allowing the Administrator to specify what Device Types and also what Specific Devices can be accessible.



Device Control - User Rights - Cristi

Standard

Device Types

These are the device type rights that apply in general.

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

Already Existing Devices

Device Type	Device Name	Description	VID	PID	Serial Number	File Whitelist	Device Code	Last Computer	Right	Actions
USB Storage Device	USB Mass Storage Device	USB Mass Storage Device/WLX	13fe	5500	07D3091BBA3A8C55	No	1234	TONY-PC	Deny Access	⊗

Tips

The Standard device control rights includes the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, the administrator can create fallback policies for Outside Network and Outside Hours circumstances.

Information

For more details about Device Types and Specific Devices (Standard, Outside Network and Outside Hours), please see chapter 3.6.1 Global Rights.

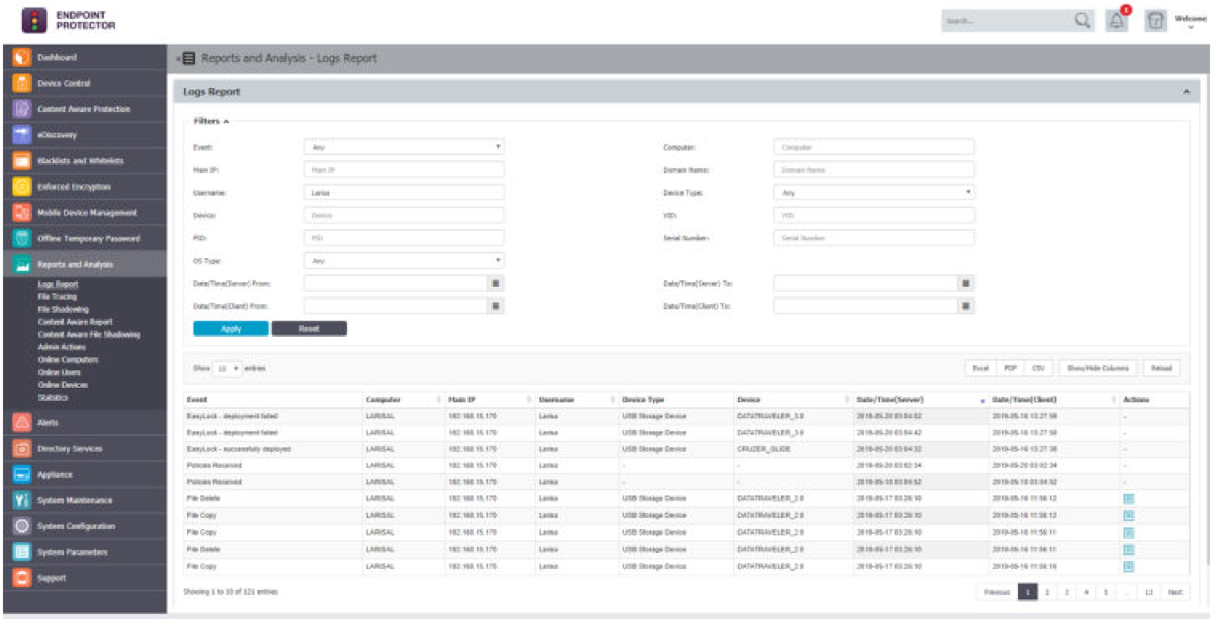
Note

The 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.

All Existing Devices that were added on that level will be deleted when the restore is used.

3.4.2. User History

From this section, the Administrator can view the user history by selecting the View User History action. This will show the Logs Report page filtered for the respective user.



Event: Any
Main IP: Main IP
Username: Larisa
Device: Device
PID: PID
OS Type: Any
Date/Time(Server) From:
Date/Time(Client) From:
Computer: Computer
Domain Name: Domain Name
Device Type: Any
VID: VID
Serial Number: Serial Number
Date/Time(Server) To:
Date/Time(Client) To:

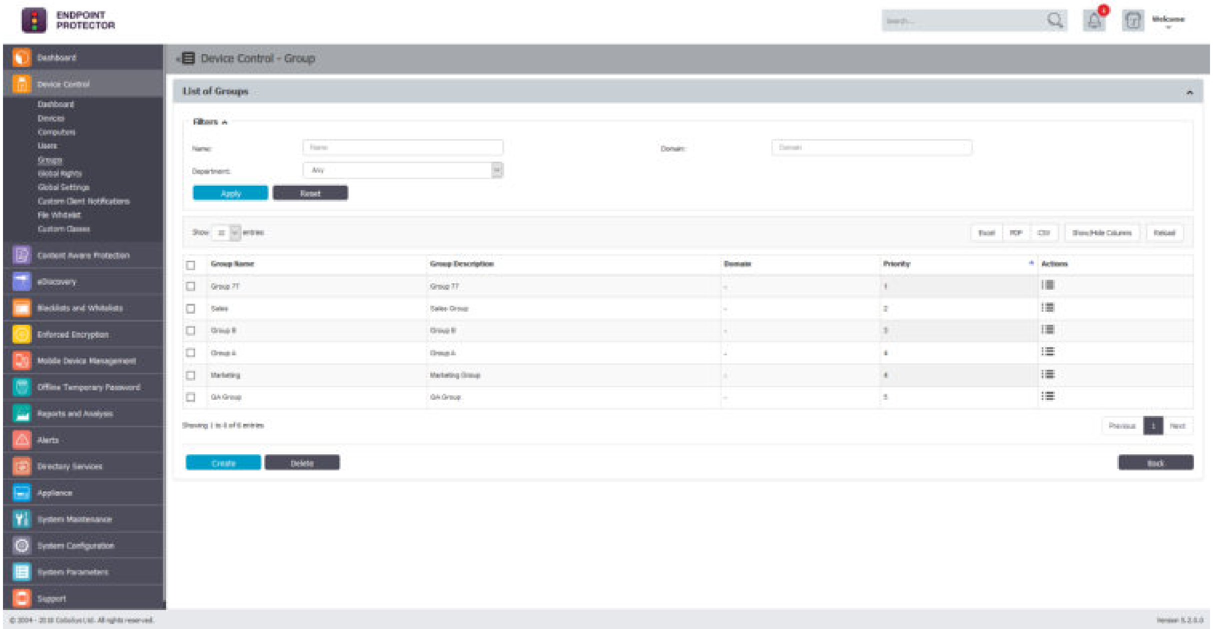
Show 10 entries

Event	Computer	Main IP	Username	Device Type	Device	Date/Time(Server)	Date/Time(Client)	Actions
EasyLock - deployment failed	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_3.0	2019-05-20 03:04:52	2019-05-16 13:27:59	-
EasyLock - deployment failed	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_3.0	2019-05-20 03:04:42	2019-05-16 13:27:58	-
EasyLock - successfully deployed	LARISAL	192.168.15.170	Larisa	USB Storage Device	CRUZER_GLIDE	2019-05-20 03:04:32	2019-05-16 13:27:38	-
Policies Received	LARISAL	192.168.15.170	Larisa	-	-	2019-05-20 03:02:34	2019-05-20 03:02:34	-
Policies Received	LARISAL	192.168.15.170	Larisa	-	-	2019-05-18 03:04:52	2019-05-18 03:04:52	-
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:12	▣
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:58:12	▣
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:11	▣
File Delete	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:11	▣
File Copy	LARISAL	192.168.15.170	Larisa	USB Storage Device	DATATRAVELER_2.0	2019-05-17 03:26:10	2019-05-16 11:56:16	▣

Showing 1 to 10 of 121 entries

3.5. Groups

From this section, the Administrator can manage all the groups in the system. Grouping computers and users will help the Administrator manage rights, or settings for these entities in a more efficient way.



Name: Name
Department: Any
Domain: Domain

Show 10 entries

☐	Group Name	Group Description	Domain	Priority	Actions
☐	Group 77	Group 77	-	1	☰
☐	Sales	Sales Group	-	2	☰
☐	Group B	Group B	-	3	☰
☐	Group A	Group A	-	4	☰
☐	Marketing	Marketing Group	-	6	☰
☐	QA Group	QA Group	-	5	☰

Showing 1 to 6 of 6 entries

A group is identified by information like Name and Description, as well as based on the entities (Computers and Users).

The Administrator can manually create a new group at any time by providing the group information mentioned above. Groups can also be imported into Endpoint Protector from Active Directory.

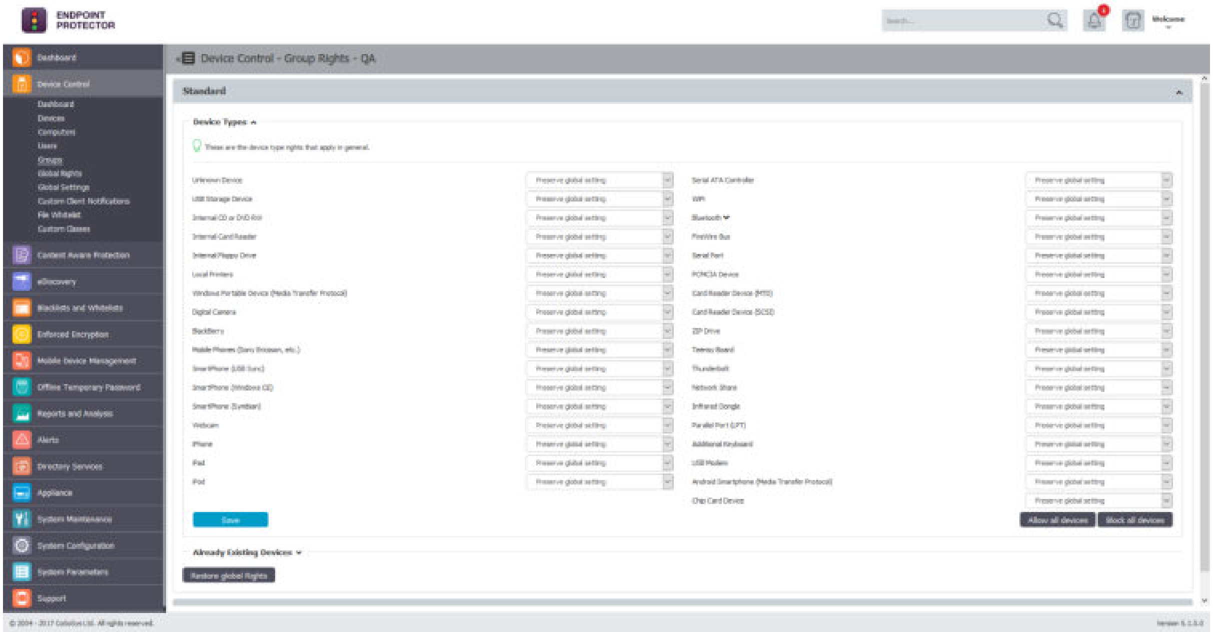
Information

For more details about Active Directory, please see chapter 12 Directory Services.

The Actions column offers multiple option related to group's management like Edit, Manage Rights, Manage Settings, History and Delete.

3.5.1. Group Rights

The Group Rights can be accessed by going in the Actions column for the specific group and selecting Manage Rights. This section is built around the group, allowing the Administrator to specify what Device Types and also what Existing Devices can be accessible.



Device Control - Group Rights - QA

Standard

Device Types

These are the device type rights that apply in general.

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

Already Existing Devices

This section is similar to the Computer Rights section, the difference being that it applies to all the computers that are part of the group simultaneously.

Tips

The Standard device control rights includes the Device Types and Already Existing Devices sections. These are generally the only device rights used.

In addition to the Standard device control rights, if enabled from the Global Settings, the administrator can create fallback policies for Outside Network and Outside Hours circumstances.

Information

For more details about Device Types and Specific Devices (Standard, Outside Network and Outside Hours), please see chapter 3.6.1 Global Rights.

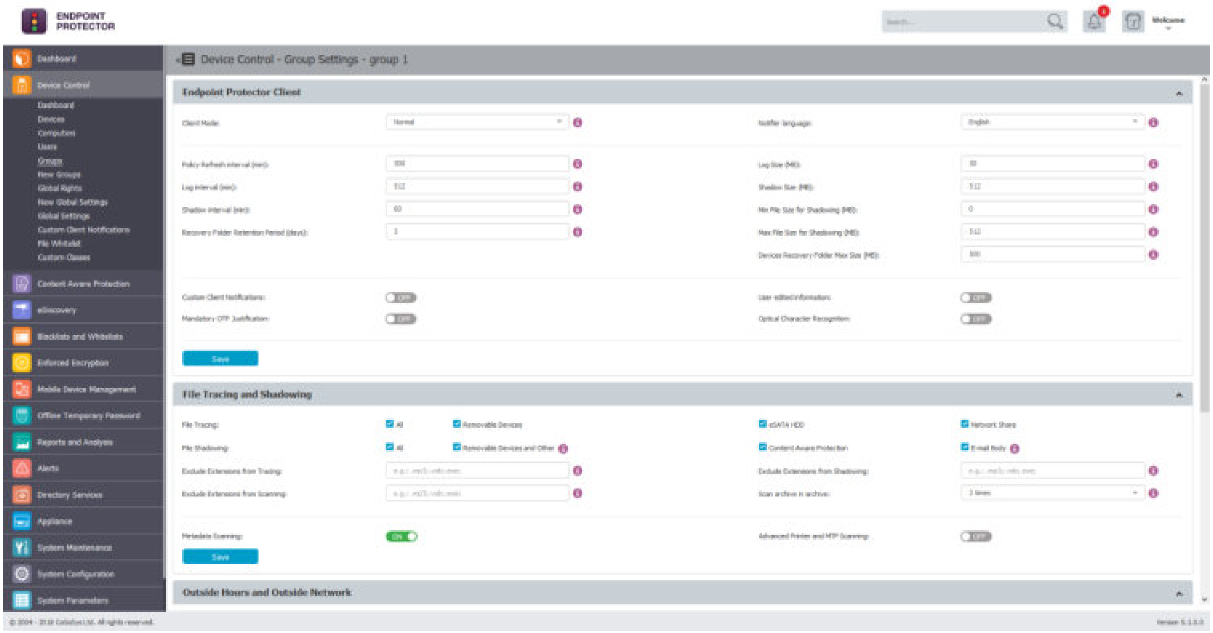
Note

The 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.

All Existing Devices that were added on that level will be deleted when the restore is used.

3.5.2. Group Settings

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



Device Control - Group Settings - group 1

Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Policy Refresh interval (min): 300

Log interval (min): 512

Shadow interval (min): 60

Recovery Folder Retention Period (days): 1

Log Size (MB): 30

Shadow Size (MB): 512

Min File Size for Shadowing (MB): 0

Max File Size for Shadowing (MB): 512

Devices Recovery Folder Max Size (MB): 500

Custom Client Notifications: OFF

Mandatory OTP Justification: OFF

User edited information: OFF

Optical Character Recognition: OFF

File Tracing and Shadowing

File Tracing: ☑ All ☑ Removable Devices ☑ eSATA HDD ☑ Network Share

File Shadowing: ☑ All ☑ Removable Devices and Other ☑ Content Aware Protection ☑ E-mail Body

Exclude Extensions from Tracing: e.g.: mp3, mkv, mov

Exclude Extensions from Shadowing: e.g.: mp3, mkv, mov

Exclude Extensions from Scanning: e.g.: mp3, mkv, mov

Scan archive in archive: 2 times

Metadata Scanning: ON

Advanced Printer and MTP Scanning: OFF

Outside Hours and Outside Network

We mentioned earlier that computers and users can be grouped in order to make editing the settings easier and more logical. Defining custom settings for all groups is not necessary, since a computer is perfectly capable of functioning correctly without any granular settings defined. It will do this by either inheriting the settings from the group it belongs to or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

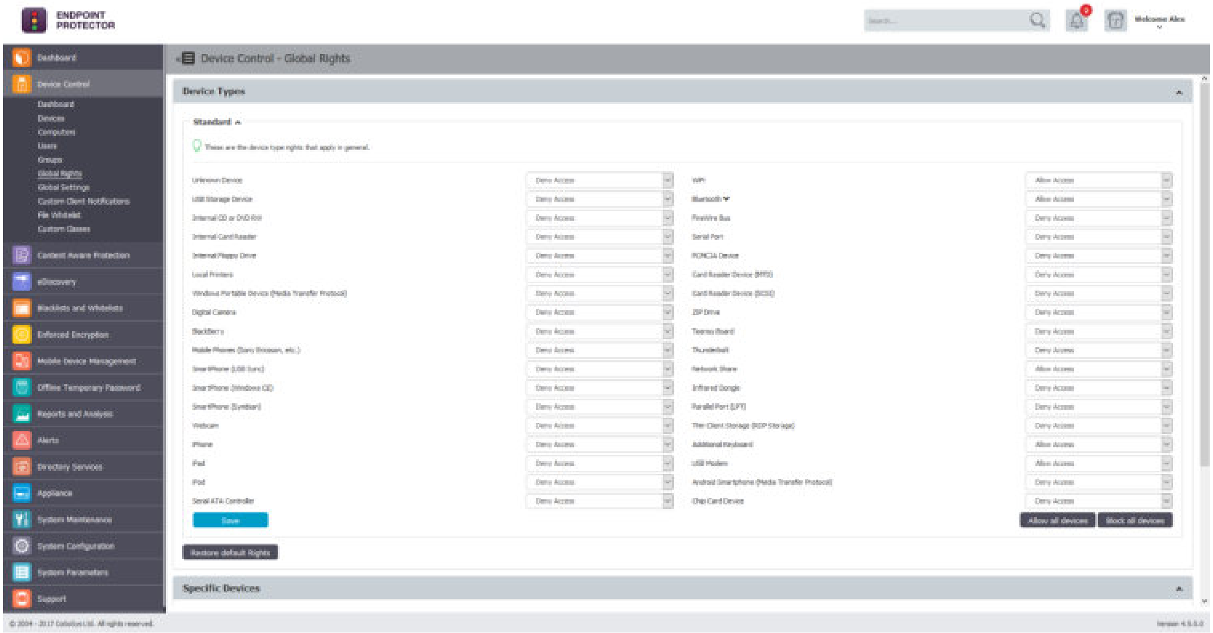
3.6. Global

From this section, the Administrator can manage the entire system. The Administrator can specify what rights and settings apply globally, to all Endpoint Protector entities.

> **Note**
>
> If device rights or other settings will be configured granularly for entities, the priority order, starting with the highest, will be:
> Devices > Computers | Users > Groups > Global.

3.6.1. Global Rights

This section relates to the entire system, allowing the Administrator to specify what Device Types and also what Specific Devices can be accessible.

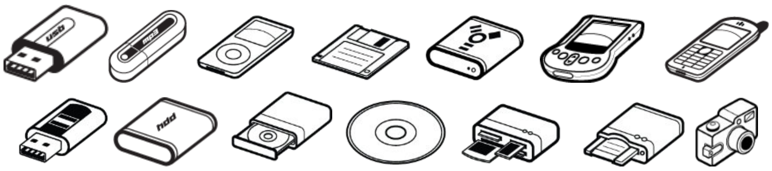


These are the device type rights that apply in general.

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

3.6.1.1. Device Types (Standard)

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
- Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.
- Card Readers - internal and external
- CD/DVD-Player/Burner - internal and external
- Digital Cameras
- Smartphones / Handhelds / PDAs (includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.)
- iPods / iPhones / iPads
- MP3 Player / Media Player Devices
- External HDDs / portable hard disks
- FireWire Devices
- PCMCIA Devices
- Biometric Devices
- Bluetooth
- Printers (applies to serial, USB and LTP connection methods)
- ExpressCard (SSD)
- Wireless USB
- LPT/Parallel ports *applies only to storage devices
- Floppy disk drives
- Serial ATA Controllers

Depending on the device type, besides the Allow and Deny Access rights, additional rights are also available. These include Read-Only Access or multiple combinations of Allow Access but with various limitations, such as Allow access but exclude from CAP scanning or Allow Access if TrustedDevice Level 1 to 4.

Information

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

For more information on TrustedDevices™ and EasyLock™, please see chapter 16.1.1 Trusted Devices.

Tips

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.

Note

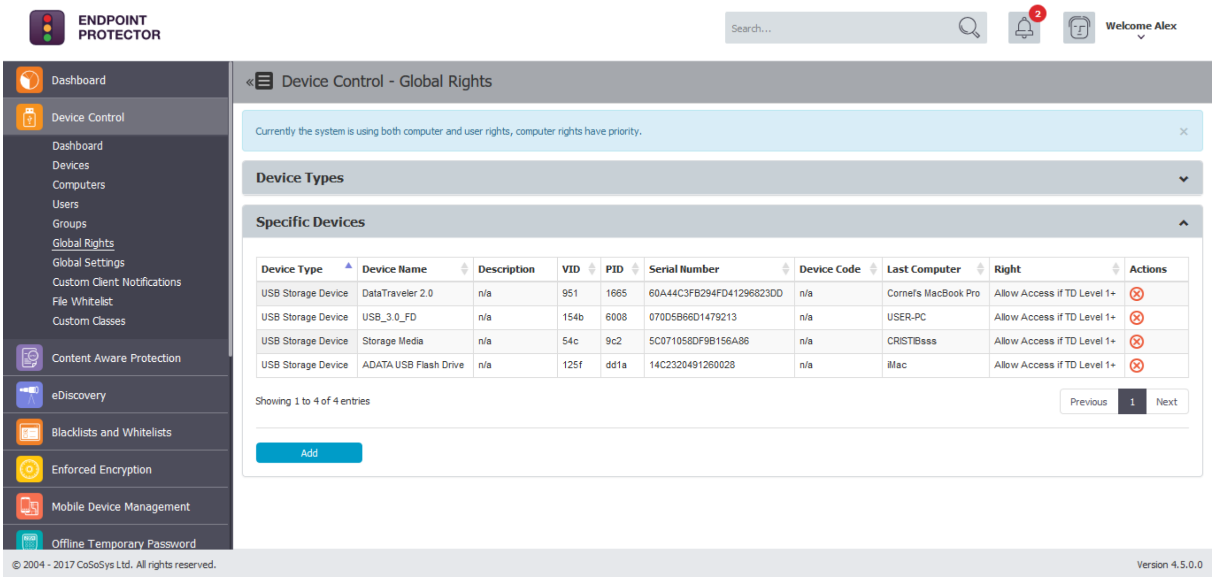
By default, the majority of device types are blocked. However, as a working internet connection or wireless keyboards are needed during the configuration process, several devices are set to Allow Access. These include WiFi, Bluetooth, Network Share, Additional Keyboard and USB Modem.

3.6.1.2. Already Existing Devices (Standard)

From this section, the administrator can manage access rights for a specific device.

Information

Device rights can be set either Globally or, per Group, User or Computer, by using the Manage Rights action from each section/entity.



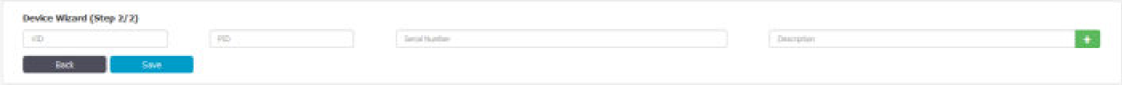
Currently the system is using both computer and user rights, computer rights have priority.

Device Type	Device Name	Description	VID	PID	Serial Number	Device Code	Last Computer	Right	Actions
USB Storage Device	DataTraveler 2.0	n/a	951	1665	60A44C3FB294FD41296823DD	n/a	Cornel's MacBook Pro	Allow Access if TD Level 1+	⊗
USB Storage Device	USB_3.0_FD	n/a	154b	6008	070D5B66D1479213	n/a	USER-PC	Allow Access if TD Level 1+	⊗
USB Storage Device	Storage Media	n/a	54c	9c2	5C071058DF9B156A86	n/a	CRISTIBsss	Allow Access if TD Level 1+	⊗
USB Storage Device	ADATA USB Flash Drive	n/a	125f	dd1a	14C2320491260028	n/a	iMac	Allow Access if TD Level 1+	⊗

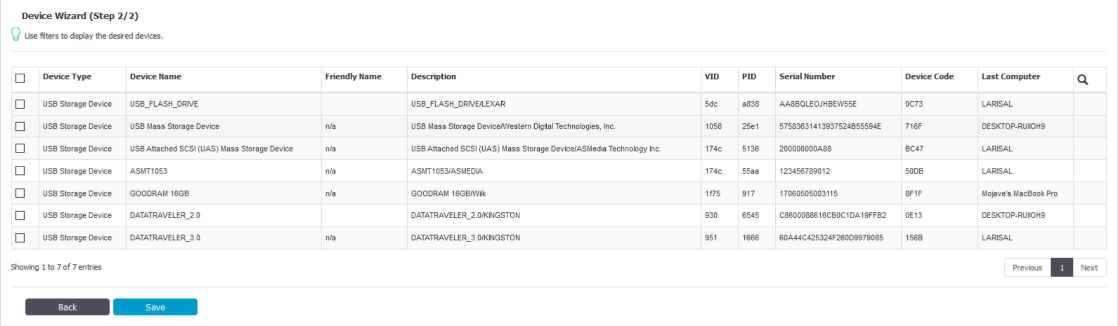
Showing 1 to 4 of 4 entries

Adding a new device in this section can be done by pressing the Add button and following the simple Device Wizard. There are multiple ways of adding devices:

- **New Device (VID, PID, Serial Number) –** will allow at Step 2 to add new devices based on Vendor ID, Product ID and Serial Number.



- **Existing Device (Wizard)** – will allow at Step 2 to add devices previously connected to protected computers and already in the Endpoint Protector database.



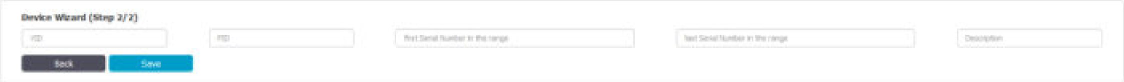
Device Wizard (Step 2/2)

Use filters to display the desired devices.

☐	Device Type	Device Name	Friendly Name	Description	VID	PID	Serial Number	Device Code	Last Computer
☐	USB Storage Device	USB_FLASH_DRIVE		USB_FLASH_DRIVE/LEXAR	5dc	a838	AA8BQLEOJHBEW55E	9C73	LARISAL
☐	USB Storage Device	USB Mass Storage Device	n/a	USB Mass Storage Device/Western Digital Technologies, Inc.	1058	25e1	57583631413937524B55594E	716F	DESKTOP-RUIIOH9
☐	USB Storage Device	USB Attached SCSI (UAS) Mass Storage Device	n/a	USB Attached SCSI (UAS) Mass Storage Device/ASMedia Technology Inc.	174c	5136	200000000A88	BC47	LARISAL
☐	USB Storage Device	ASMT1053	n/a	ASMT1053/ASMEDIA	174c	55aa	123456789012	50DB	LARISAL
☐	USB Storage Device	GOODRAM 16GB	n/a	GOODRAM 16GB/Wilk	1f75	917	17060505003115	8F1F	Mojave's MacBook Pro
☐	USB Storage Device	DATATRAVELER_2.0		DATATRAVELER_2.0/KINGSTON	930	6545	C8600088616CB0C1DA19FFB2	0E13	DESKTOP-RUIIOH9
☐	USB Storage Device	DATATRAVELER_3.0	n/a	DATATRAVELER_3.0/KINGSTON	951	1666	60A44C425324F260D9979085	156B	LARISAL

Showing 1 to 7 of 7 entries

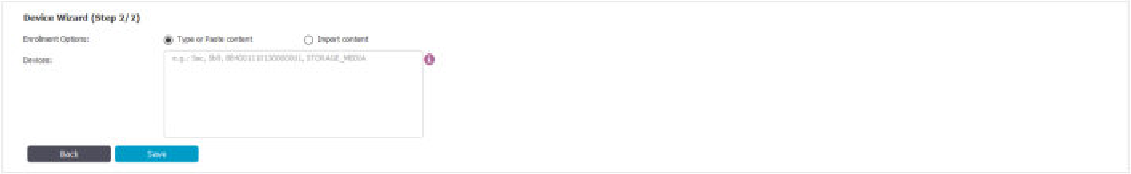
- **Device Serial Number Range** – will allow at Step 2 to add multiple devices at the same time, by specifying the first and last Serial Number in the range. The recommended use for this feature is for devices that have a consecutive range, with a clear, noticeable pattern.


Device Wizard (Step 2/2)
VID
PID
First Serial Number in the range
last Serial Number in the range
Description
Back
Save

Note

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

- **Bulk List of Devices –** will allow at Step 2 to add up to 500 devices at the same time. There are two methods to choose from, either importing a list or by simply pasting the information.



Device Wizard (Step 2/2)

Enrolment Options: ● Type or Paste content ○ Import content

Devices: e.g.: 5ac, 1b9, [illegible], STORAGE_MEDIA

Information

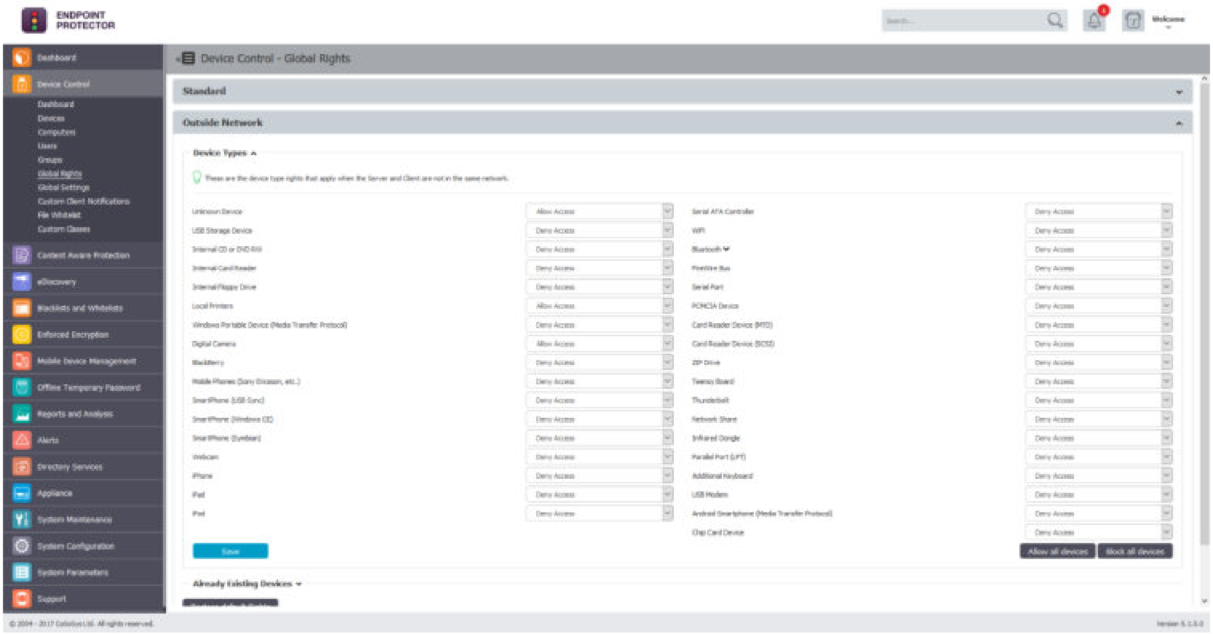
The File Whitelisting feature is also available for USB storage devices that have allows access. For more details about File Whitelisting, please see chapter 3.7 File Whitelists.

3.6.1.3. Outside Network

Note

In order for this to be available, the feature needs to be enabled in the Global Settings section.

From this section, the administrator can define fallback policies that will apply when outside the network. All of the functionalities are identical to the Standard section.



Device Control - Global Rights

Standard

Outside Network

Device Types

These are the device type rights that apply when the Server and Client are not in the same network.

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

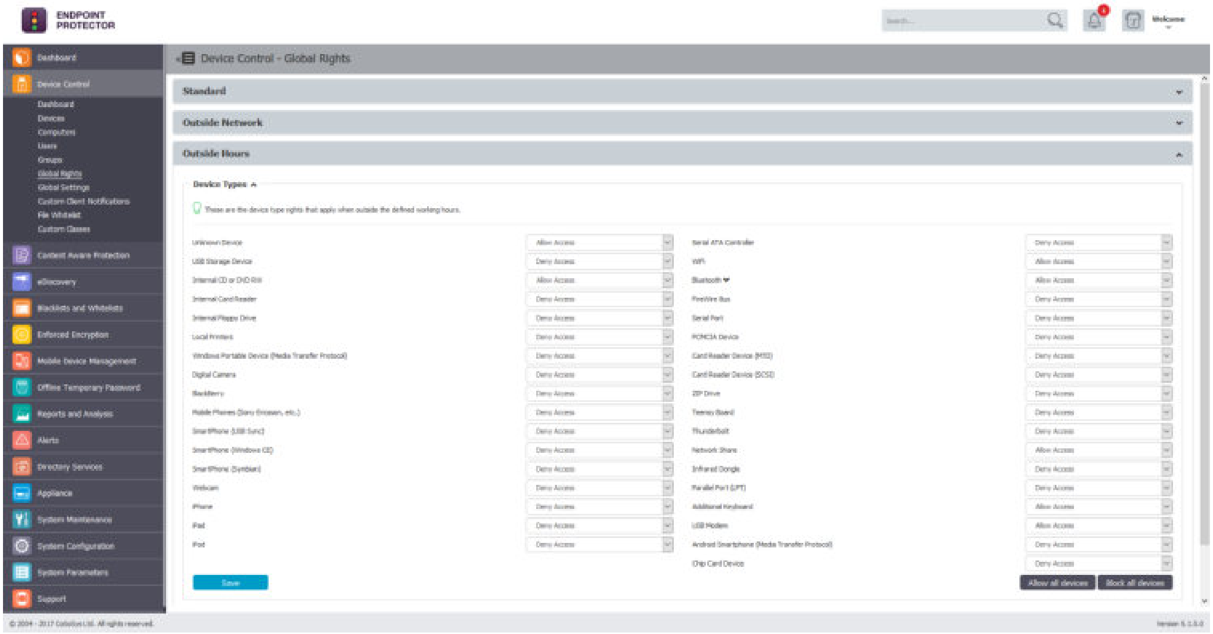
Already Existing Devices

3.6.1.4. Outside Hours

Note

In order for this to be available, the feature needs to be enabled in the Global Settings section.

From this section, the administrator can define fallback policies that will apply when outside working hours. All of the functionalities are identical to the Standard section.



Device Control - Global Rights

Standard

Outside Network

Outside Hours

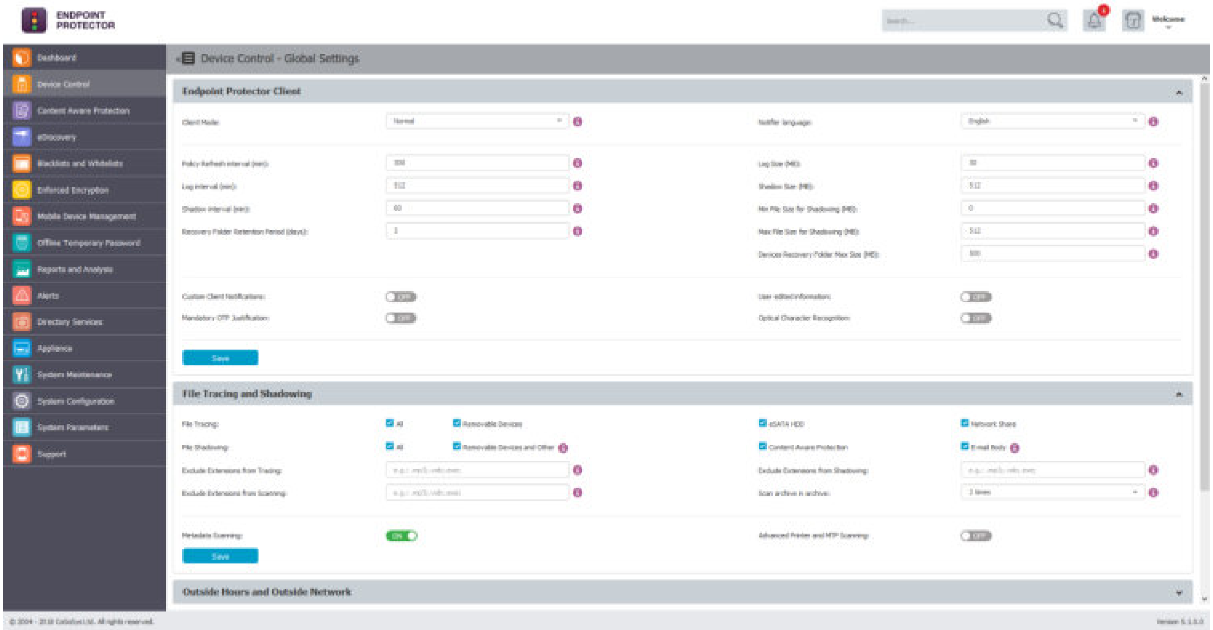
Device Types

These are the device type rights that apply when outside the defined working hours.

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

3.6.2. Global Settings

From this section, the Administrator can specify what settings apply globally, to all Endpoint Protector entities. If there are no settings defined granularly 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.



Device Control - Global Settings

Endpoint Protector Client

Client Mode: Normal
Notifier language: English
Policy Refresh interval (min): 300
Log Size (MB): 50
Log interval (min): 512
Shadow Size (MB): 512
Shadow interval (min): 60
Min File Size for Shadowing (MB): 0
Recovery Folder Retention Period (days): 1
Max File Size for Shadowing (MB): 512
Devices Recovery Folder Max Size (MB): 500
Custom Client Notifications: OFF
User edited information: OFF
Mandatory OTP Justification: OFF
Optical Character Recognition: OFF

File Tracing and Shadowing

File Tracing: ☑ All ☑ Removable Devices ☑ eSATA HDD ☑ Network Share
File Shadowing: ☑ All ☑ Removable Devices and Other ☑ Content Aware Protection ☑ E-mail Body
Exclude Extensions from Tracing: e.g.: mp3, mkv, exe
Exclude Extensions from Shadowing: e.g.: mp3, mkv, exe
Exclude Extensions from Scanning: e.g.: mp3, mkv, exe
Scan archive in archive: 2 times
Metadata Scanning: ON
Advanced Printer and MTP Scanning: OFF

Outside Hours and Outside Network

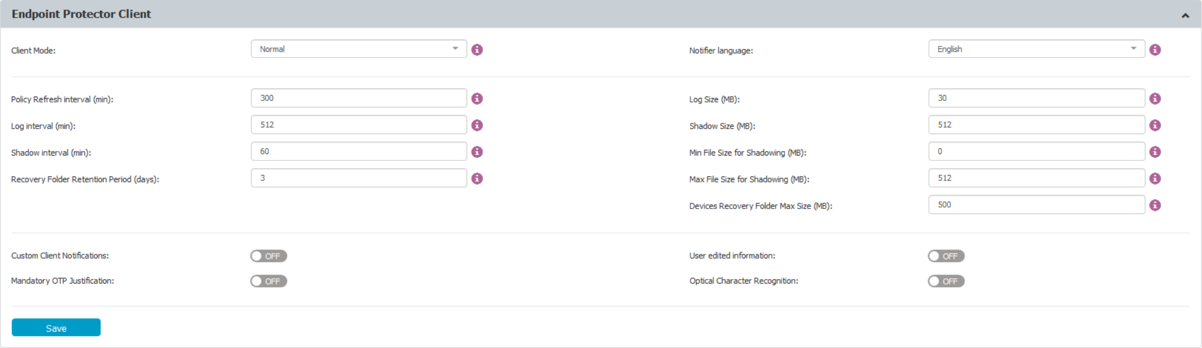
The Endpoint Protector Client, File Tracing and Shadowing, Outside Hours and Outside Network, as well as Transfer Limit settings can be set from set from this section. Due to their importance, they will be explained in their own subsections below.

⚠ **Note**

Some of the settings from this section relate also to other modules (e.g.: Content Aware Protection, eDiscovery, etc.) and not just the Device Control module.

3.6.2.1. Endpoint Protector Client Settings

There are several settings that relate directly to the Endpoint Protector Client. These relate to the Client's behavior for each specific entity (Global, Groups and Computers).



Endpoint Protector Client

Client Mode: Normal

Notifier language: English

Policy Refresh interval (min): 300

Log interval (min): 512

Shadow interval (min): 60

Recovery Folder Retention Period (days): 3

Log Size (MB): 30

Shadow Size (MB): 512

Min File Size for Shadowing (MB): 0

Max File Size for Shadowing (MB): 512

Devices Recovery Folder Max Size (MB): 500

Custom Client Notifications: OFF

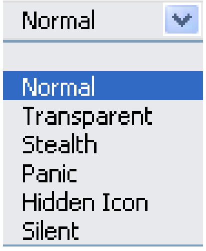
Mandatory OTP Justification: OFF

User edited information: OFF

Optical Character Recognition: OFF

Client Modes

The Endpoint Protector Client offers several modes that define its behavior.



There are six modes from which to choose from (and they can be changed at any given time):

- Normal Mode (default setting of Endpoint Protector)

> ⚠ **Note**
>
> We recommend not to change the Normal Mode without being fully aware of what the other modes imply.
>
> If the Normal Mode does not suit your needs, Hidden or Silent Mode are usually the best alternatives to consider.

- Transparent Mode

> **Information**
>
> This mode provides the following behavior:
>
> - no system tray icon is displayed
> - no system tray notifications are shown
> - everything is blocked, regardless if authorized or not
> - Administrator receives alerts for all activities

Tips

This mode is useful to block all devices but users remain unaware of any restrictions or presence of the Endpoint Protector Client and its activity.

- Stealth Mode

Information

This mode provides the following behavior:

- no system tray icon is displayed
- no system tray notifications are shown
- everything is allowed, regardless if authorized or not
- file shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts for all activities

Tips

This mode is useful to monitor all users and computers but users remain unaware of any restrictions or presence of the Endpoint Protector Client and its activity. As everything is on allow, there will be no disruptions in the day to day activities of the users.

- Panic Mode

Information

This mode provides the following behavior:

- system tray icon is displayed
- system tray notifications are shown
- everything is blocked, regardless if authorized or not
- file shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts when computers go in and out of Panic Mode

⚠ Note

This mode could be triggered automatically under extreme situations, when user’s malicious intent or activity is detected.

Under special circumstances, it can also be set manually by the Administrator in order to block all devices. However, using this mode in such a manner is not recommended!

- Hidden Icon Mode

Information

This mode provides the following behavior:

- no system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied as per their configuration

Tips

This mode is very similar to the Normal Mode. The difference is that Endpoint Protector Client is not visible to the user.

- Silent Mode

Information

This mode provides the following behavior:

- system tray icon is displayed
- no system tray notifications are shown
- all set rights and settings are applied as per their configuration

Tips

This mode is very similar to the Normal Mode. The difference is that the pop-up notifications are not visible to the user.

Notifier Language

The Endpoint Protector Client Notifier language.

Policy Refresh Interval (sec)

The time interval at which the Client checks with the Server and updates with the latest settings, rights and policies.

Log Size (MB)
The largest size of all logs stored on the Client. If the value is reached, new logs will overwrite the oldest ones. These circumstances occur only when the Client and Server do not communicate for a large period of time.

Log Interval (min)
The time interval at which the Client attempts to re-send the Logs to the Server.

Shadow Size (MB)
The largest size of all file shadow on the Client. If the value is reached, new shadows will overwrite the oldest ones. These circumstances occur only when the Client and Server do not communicate for a large period of time.

Shadow Interval (min)
The time interval at which the Client sends the Shadows to the Server.

Min File Size for Shadowing (KB)
The smallest size of a file at which a File Shadow is created.

Device Recovery Folder Retention Period (days)
Specific for Mac and Linux computers. It acts like a quarantine folder before a transferred file has been fully inspected for content, avoiding any potential file loss due to blocked transfers. After the specified time interval, the files are permanently deleted.

Max File Size for Shadowing (KB)
The largest size of a file at which a File Shadow is created.

Recovery Folder Max Size (MB)
Specific for Mac and Linux computers. Maximum size for quarantine folder. If the value is reached, new files will overwrite the oldest ones.

Custom Client Notifications
If enabled, the Client Notifications can be customized.

User edited information
If enabled, the User can edit the user and computer information from within the Endpoint Protector Client

Mandatory OTP Justification
If enabled, the Justification a User has to provide when requesting or using an Offline Temporary Password is mandatory.

Optical Character Recognition
If enabled, JPEG, PNG, GIF, BMP and TIFF file types can be inspected for content. This option will also change the global MIME Type Whitelists.

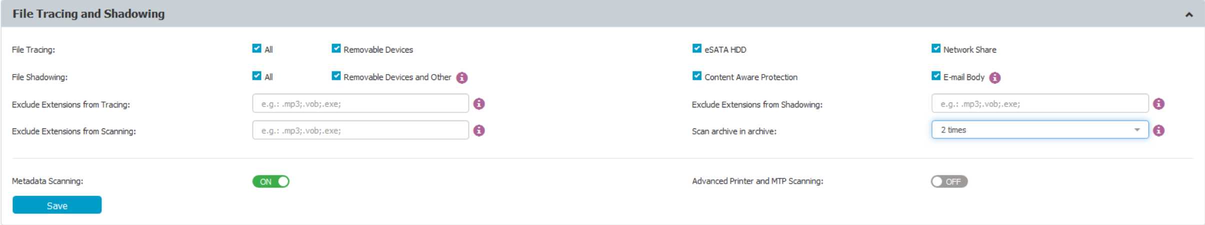
Deep Packet Inspection
If enabled, network traffic can be inspected for content. This option is required for both the Deep Packet Inspection Whitelists and URL and Domain Blacklist.

3.6.2.2. File Tracing and Shadowing

The **File Tracing** feature allows monitoring of data traffic between protected endpoints and removable devices, internal eSATA HDDs and Network Shares. It also shows other actions that took place, such as file renamed, deleted, accessed, modified, etc.

Information

It can be enabled from Device Control > Global Settings, or granularly for Groups or Computers.



File Tracing and Shadowing

File Tracing: ☑ All ☑ Removable Devices ☑ eSATA HDD ☑ Network Share

File Shadowing: ☑ All ☑ Removable Devices and Other ☑ Content Aware Protection ☑ E-mail Body

Exclude Extensions from Tracing: e.g.: .mp3;.vob;.exe;

Exclude Extensions from Shadowing: e.g.: .mp3;.vob;.exe;

Exclude Extensions from Scanning: e.g.: .mp3;.vob;.exe;

Scan archive in archive: 2 times

Metadata Scanning: ON

Advanced Printer and MTP Scanning: OFF

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

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.

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.

Information

File Shadowing cannot be used without File Tracing.

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

Note

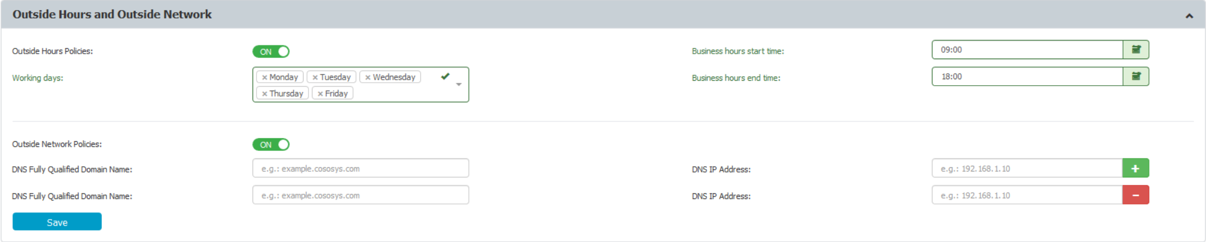
File Shadowing can be delayed due to network traffic and Endpoint Protector Settings for different computers or file sizes. Shadowed files are usually available after a few minutes.

Tips

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).

3.6.2.3. Outside Hours and Outside Network

This section allows the Administrator to enable or disable the Device Types – Outside Network polices and Device Types – Outside Hours policies.



Outside Hours and Outside Network

Outside Hours Policies: ON

Working days: × Monday × Tuesday × Wednesday × Thursday × Friday

Business hours start time: 09:00

Business hours end time: 18:00

Outside Network Policies: ON

DNS Fully Qualified Domain Name: e.g.: example.cososys.com

DNS IP Address: e.g.: 192.168.1.10

DNS Fully Qualified Domain Name: e.g.: example.cososys.com

DNS IP Address: e.g.: 192.168.1.10

For Device Types – Outside Hours policies, the Working days, Business hours start time and end time need to be set.

For Device Types – Outside Network polices, the DNS Fully Qualified Domain Name and DNS IP Address need to be set.

Once these settings are made, the fallback device type rights can be set Globally, per Groups, Users or Computers.

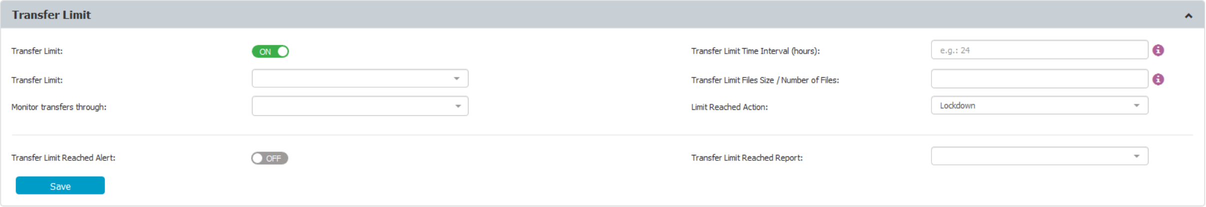
Note

When triggered, fallback policies supersede the standard device rights.

In regard to fallback policies, the Outside Network Policies supersede the Outside Hours Policies.

3.6.2.4. Transfer Limit

From this section, the Administrator can set Transfer Limit, within a specific time interval (hours). Once the limit is reached, file transfers to storage devices (Device Control) or to controlled applications (Content Aware Protection) will no longer be possible, until the time interval expires and the count is reset. Similarly, file transfers through Network Shares can also be included in the Transfer Limit.



Transfer Limit

Transfer Limit: ON

Transfer Limit:

Monitor transfers through:

Transfer Limit Time Interval (hours): e.g.: 24

Transfer Limit Files Size / Number of Files:

Limit Reached Action: Lockdown

Transfer Limit Reached Alert: OFF

Transfer Limit Reached Report:

Note

The mechanism that checks when the Transfer Limit is reached has been designed in such a way that it does not impact the performance of the computer.

Therefore, there might be a slight delay between the exact time the limit is reached and the enforcing of the transfer restrictions. In general, it's just a few seconds but also depending on the network, it could be up to a few minutes.

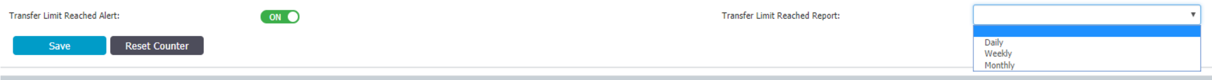
There are three actions to choose from when the Transfer Limit is reached:

- **Monitor Only** – simply reports when the limit is reached
- **Restrict** – blocks the devices and applications that have been defined in the Device Control policies
- **Lockdown** – blocks all devices, regardless if they have been defined within the Device Control policies; this includes the network interfaces and therefore, any type of transfer

Information

To re-establish the Server-Client communication before the Transfer Limit Time Interval expires, a Transfer Limit Reached Offline Temporary Password is available. For more information, please see chapter 9 Offline Temporary Password.

The option to enable a Transfer Limit Reached Alert is also possible. Additionally, a Transfer Limit Reached Report can be scheduled on a daily, weekly or monthly basis.

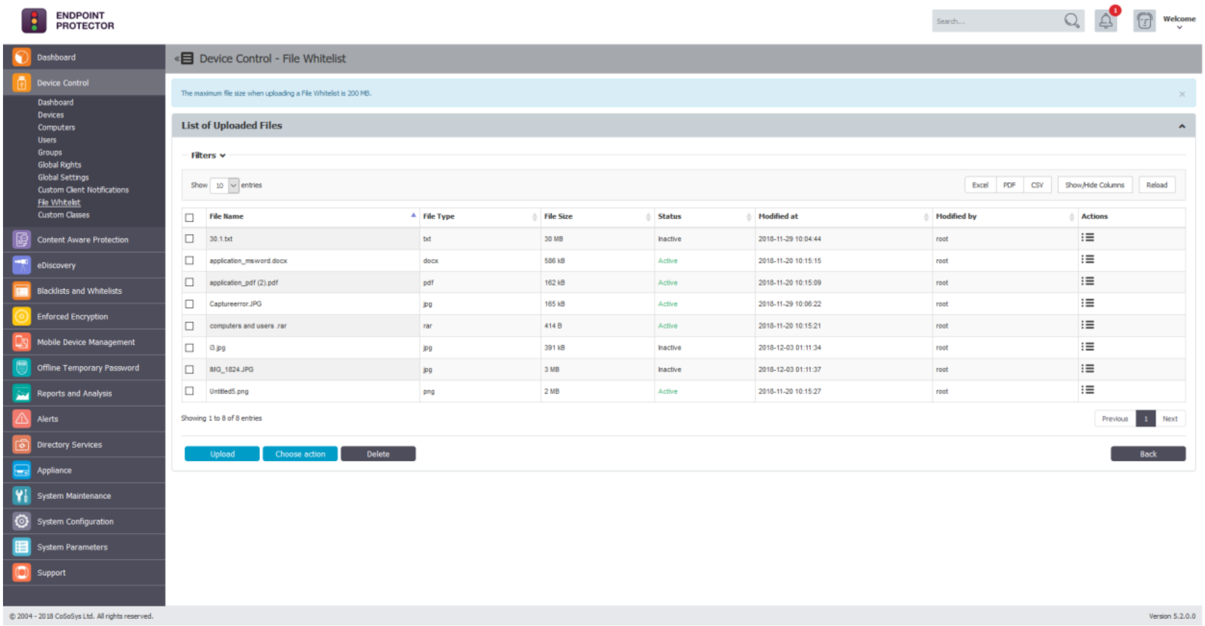


Transfer Limit Reached Alert: ON

Transfer Limit Reached Report:

3.7. File Whitelists

From this section, the Administrator can control the transfer of only authorized files to previously authorized portable storage devices.



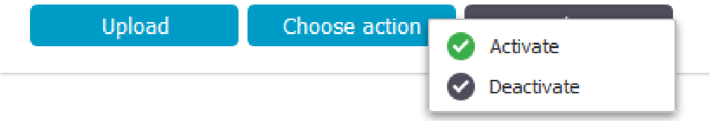
The maximum file size when uploading a File Whitelist is 200 MB.

List of Uploaded Files

□	File Name	File Type	File Size	Status	Modified at	Modified by	Actions
□	30.1.txt	txt	30 MB	Inactive	2018-11-29 10:04:44	root	☰
□	application_msword.docx	docx	586 kB	Active	2018-11-20 10:15:15	root	☰
□	application_pdf (2).pdf	pdf	162 kB	Active	2018-11-20 10:15:09	root	☰
□	Captureerror.JPG	jpg	165 kB	Active	2018-11-29 10:06:22	root	☰
□	computers and users .rar	rar	414 B	Active	2018-11-20 10:15:21	root	☰
□	i3.jpg	jpg	391 kB	Inactive	2018-12-03 01:11:34	root	☰
□	IMG_1824.JPG	jpg	3 MB	Inactive	2018-12-03 01:11:37	root	☰
□	Untitled5.png	png	2 MB	Active	2018-11-20 10:15:27	root	☰

Showing 1 to 8 of 8 entries

Management of which files can be copied to removable devices, and which cannot, is made by uploading the whitelisted files to the Endpoint Protector Server. Once the files are uploaded, an action for that particular file has to be taken: **Activate** or **Deactivate**.



Information

The maximum file size when uploading a File Whitelist is 190 MB.

Note

The File Whitelists will not apply to files copied from external sources onto computers. Moreover, if the Content Aware Protection module is activated and Policies set, they will have priority over the the Files Whitelisted in the Device Control module.

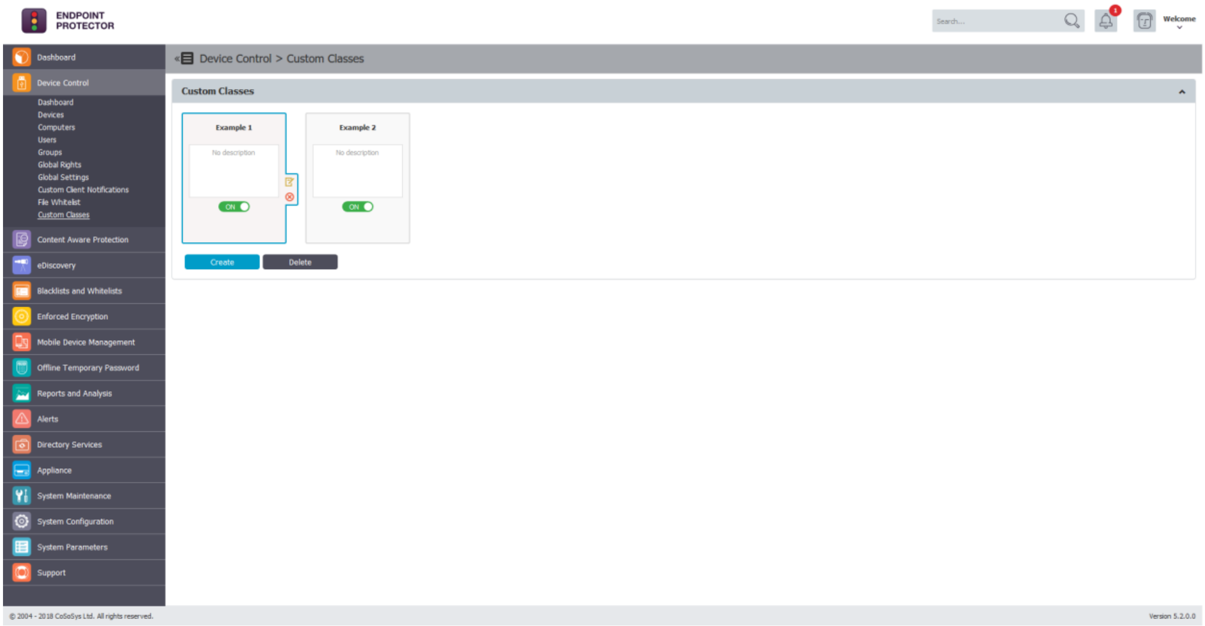
3.8. Custom Classes

This section provides the Administrator with 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 clicking on the Create. An existing policy can be edited by double-clicking on it.

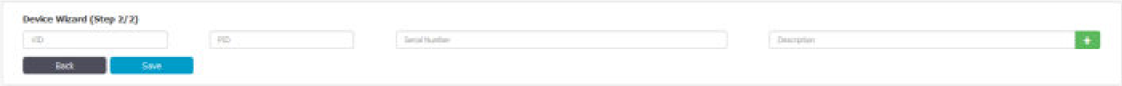
Information

The option to edit, duplicate or delete a policy is available after selecting the desired policy.

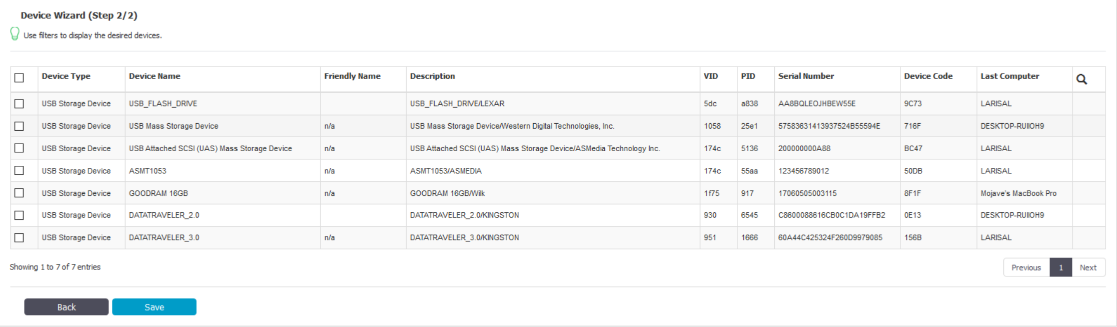


Before adding devices to a Custom Class, the Name, Description, Device Type (USB Storage Devices, Cameras, etc.), Device Right (Allow Access, Block Access, etc.) must be provided. Once this is done, there are multiple ways of adding devices to a Custom Class:

- **New Device (VID, PID, Serial Number) –** will allow at Step 2 to add new devices based on Vendor ID, Product ID and Serial Number.



- **Existing Device (Wizard)** – will allow at Step 2 to add devices previously connected to protected computers and already in the Endpoint Protector database.



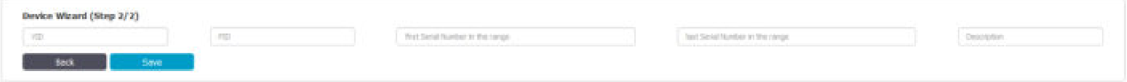
Device Wizard (Step 2/2)

Use filters to display the desired devices.

□	Device Type	Device Name	Friendly Name	Description	VID	PID	Serial Number	Device Code	Last Computer
□	USB Storage Device	USB_FLASH_DRIVE		USB_FLASH_DRIVE/LEXAR	5dc	a838	AA8BQLEOJHBEW55E	9C73	LARISAL
□	USB Storage Device	USB Mass Storage Device	n/a	USB Mass Storage Device/Western Digital Technologies, Inc.	1058	25e1	575836314139375 24B55594E	716F	DESKTOP-RUIIOH9
□	USB Storage Device	USB Attached SCSI (UAS) Mass Storage Device	n/a	USB Attached SCSI (UAS) Mass Storage Device/ASMedia Technology Inc.	174c	5136	200000000A88	BC47	LARISAL
□	USB Storage Device	ASMT1053	n/a	ASMT1053/ASMEDIA	174c	55aa	123456789012	50DB	LARISAL
□	USB Storage Device	GOODRAM 16GB	n/a	GOODRAM 16GB/Wilk	1f75	917	17060505003115	8F1F	Mojave's MacBook Pro
□	USB Storage Device	DATATRAVELER_2.0		DATATRAVELER_2.0/KINGSTON	930	6545	C8600088616CB0C1DA19FFB2	0E13	DESKTOP-RUIIOH9
□	USB Storage Device	DATATRAVELER_3.0	n/a	DATATRAVELER_3.0/KINGSTON	951	1666	60A44C425324F260D9979085	156B	LARISAL

Showing 1 to 7 of 7 entries

- **Device Serial Number Range** – will allow at Step 2 to add multiple devices 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.



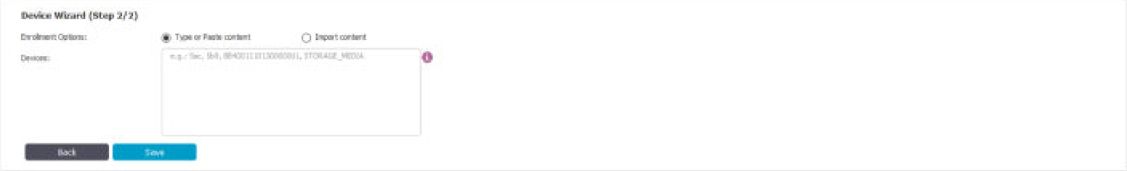
Device Wizard (Step 2/2)

VID
PID
First Serial Number in the range
last Serial Number in the range
Description
Back
Save

Note

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

- **Bulk List of Devices –** will allow at Step 2 to add up to 500 devices at the same time. There are two methods to choose from, either importing a list or by simply pasting the information.



Device Wizard (Step 2/2)

Enrollment Options: ● Type or Paste content ○ Import content

Devices:

- **Device Class (Device Type) –** will allow at Step 2 to add a specific right to a Device Type. This option is intended to be used in scenarios when a very fast way to change all device types in the system but specific device rights were granularly added to some users or computers.

Example

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.

3.9. Priorities for device rights

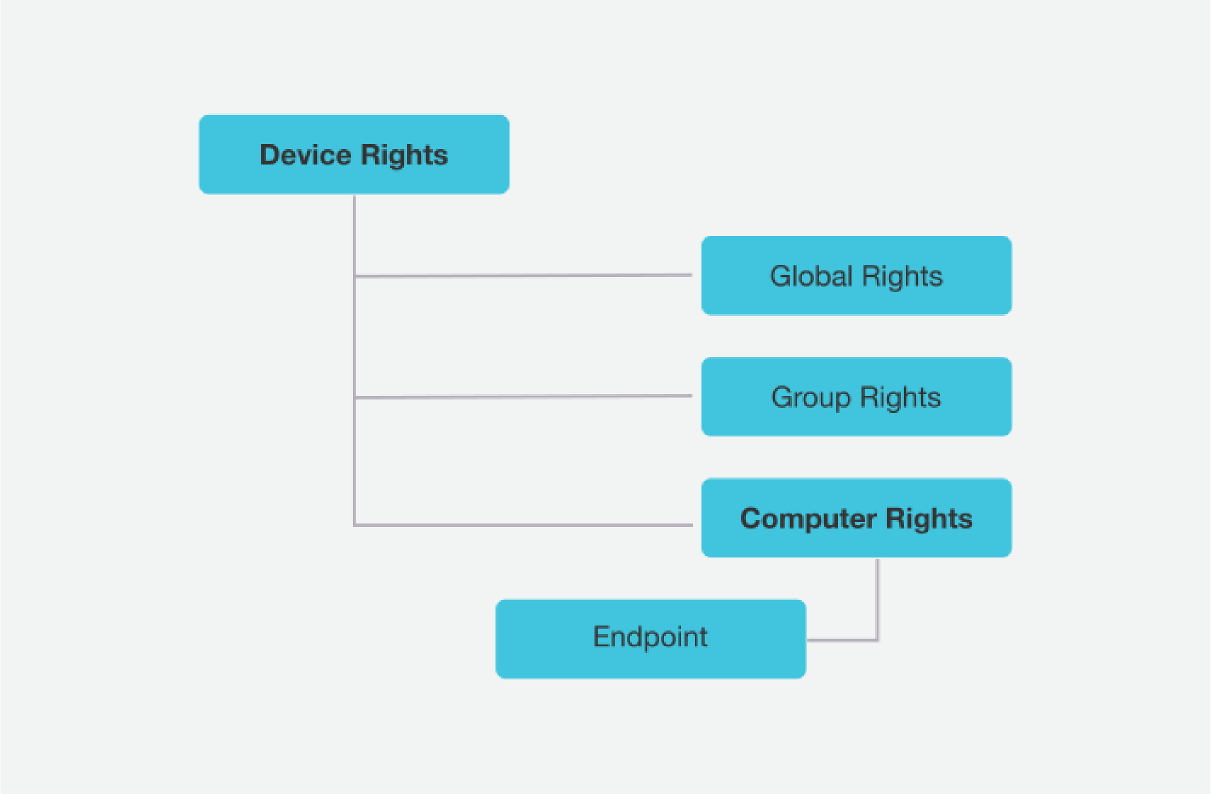
Computer Rights, Group Rights and Global Rights form a single unit and they inherit each-others settings. This means that changes to any one of these entities affect the other ones.

There are three levels of hierarchy: Global Rights, Group Rights and Computer Rights, the latter being the deciding factor in rights management.

Information

The device rights surpass all computer, group and global rights.

The user rights are on the same level with the computer rights. The priority can be set from the System Settings section. For more details about this setting, please see chapter 15.8.1 Endpoint Protector Rights Functionality.



Example

Device X is allowed from Global Rights. If in the Computer Rights section, the same device does not have permission to be used, the device will not be usable. Same applies vice-versa: if the device lacks access permission globally, and has permission set per computer, the device will be allowed. The same applies for Global Rights and Group Rights: if under globally the device does not have permission to be used, and group permission exists, the device will be allowed.

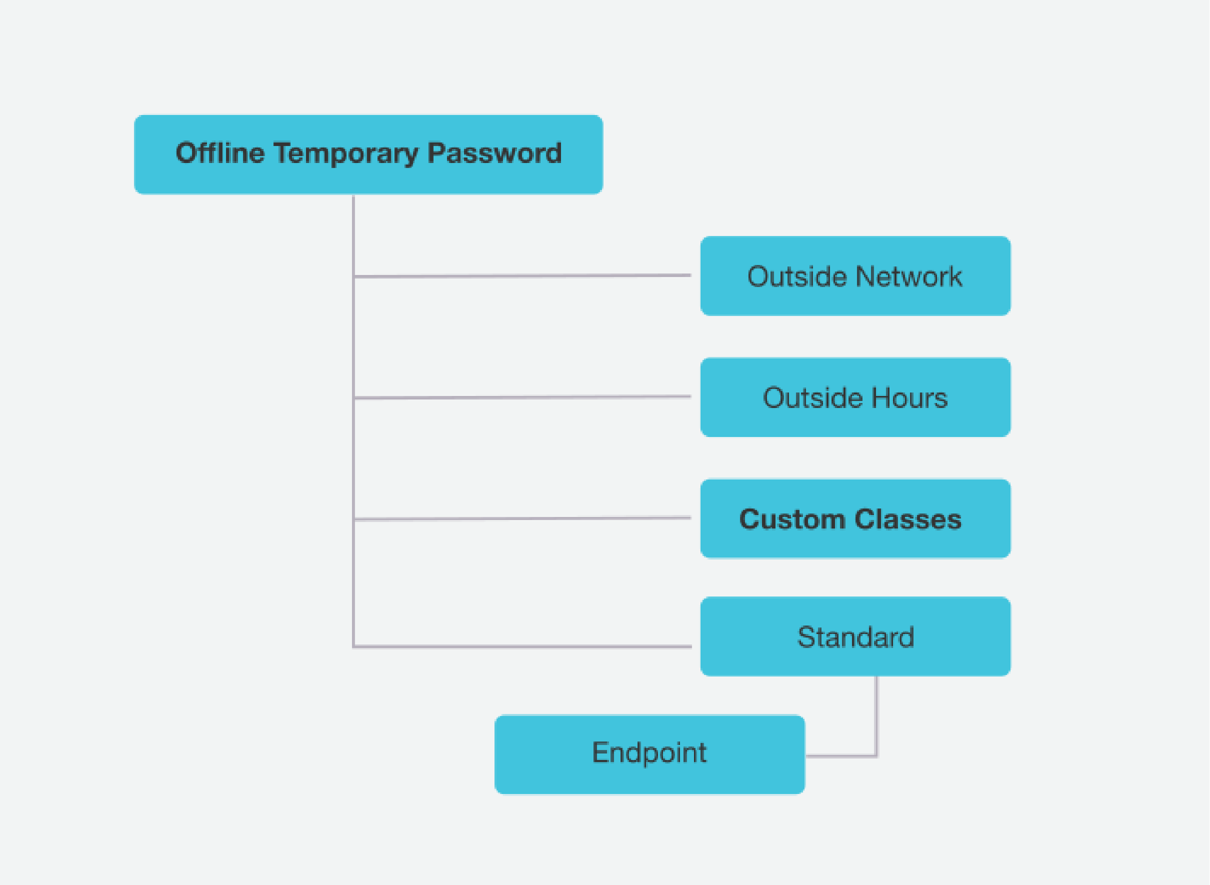
3.9.1. Priorities for Device Control Policies

By default, only the Standard Device Control Rights are available. They include the Device Types and the Already Existing Devices sections.

Custom Classes can be defined. They represent a group of devices that have a particular access right across the entire network. Custom Classes surpass the Standard rights.

If enabled, Outside Network and Outside Hours device rights can be configured. These surpass the Custom Classes rights.

The Offline Temporary Password rights allow the creation of exceptions form the rules. These rights surpass all other.



4. 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, etc.)
- Transfers to the cloud (iCloud, Google Drive, Dropbox, Microsoft SkyDrive, etc.)
- Transfers through Copy & Paste / Cut & Paste
- Print screens

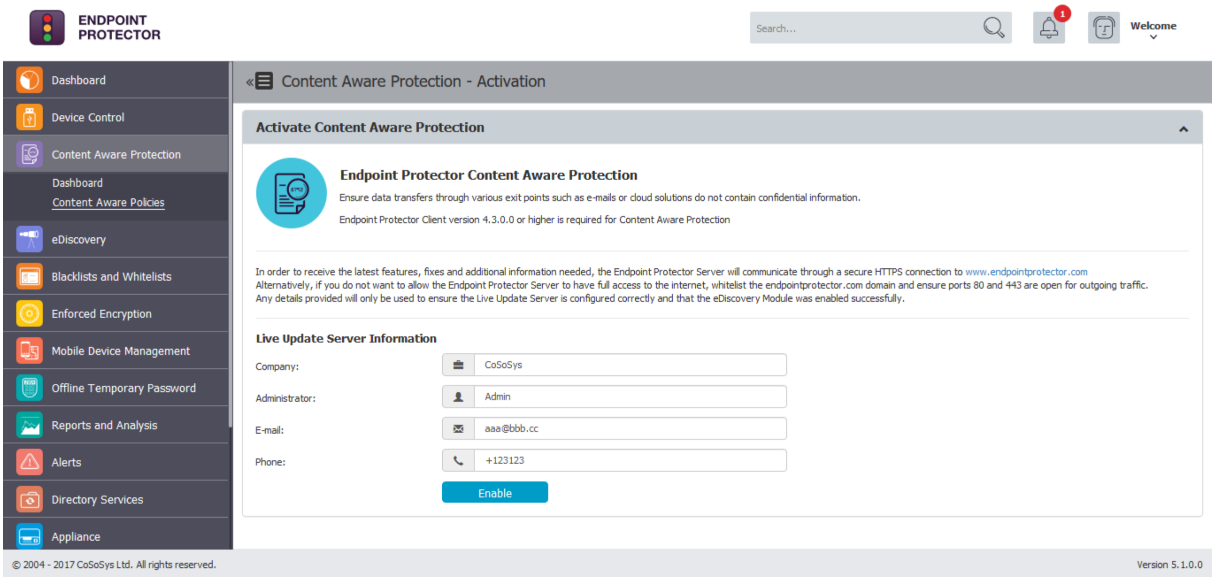
- Printers and others

4.1. Content Aware Protection Activation

Content Aware Protection comes as the second level of data protection available in Endpoint Protector. The module is displayed but requires a simple activation by pressing the Enable button. If not previously provided, the contact details of the Main Administrator will be required.

Information

Any details provided will only be used to ensure the Live Update Server is configured correctly and that the Content Aware Protection module was enabled successfully.



Endpoint Protector Content Aware Protection

Ensure data transfers through various exit points such as e-mails or cloud solutions do not contain confidential information.

Endpoint Protector Client version 4.3.0.0 or higher is required for Content Aware Protection

In order to receive the latest features, fixes and additional information needed, the Endpoint Protector Server will communicate through a secure HTTPS connection to www.endpointprotector.com
Alternatively, if you do not want to allow the Endpoint Protector Server to have full access to the internet, whitelist the endpointprotector.com domain and ensure ports 80 and 443 are open for outgoing traffic.
Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery Module was enabled successfully.

Live Update Server Information

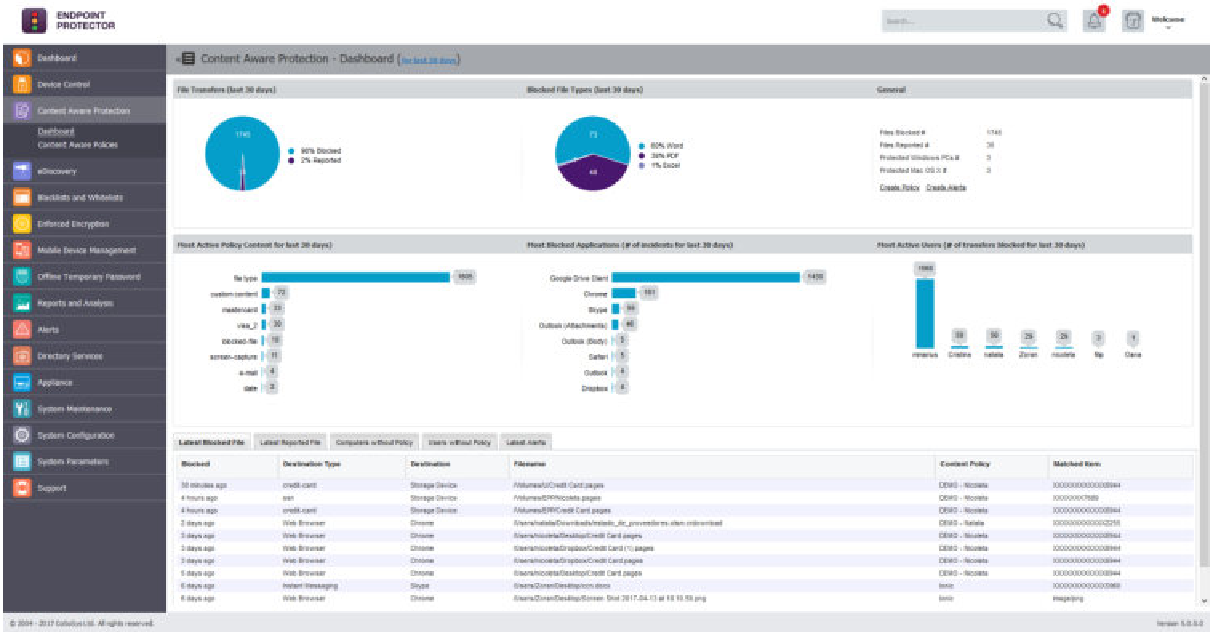
Company:	CoSoSys
Administrator:	Admin
E-mail:	aaa@bbb.cc
Phone:	+123123

Note

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

4.2. Dashboard

This section offers a quick overview in the form of graphics and charts related to the Content Aware Protection module. Information like the latest File Transfers, blocked File Types, Most Active Policy, Most Blocked Applications, Most Active Users, latest Content Aware Alerts and Computers and Users without Policies are also displayed.



Files Blocked #	1745
Files Reported #	38
Protected Windows PCs #	3
Protected Mac OS X #	3

Create Policy Create Alerts

Blocked	Destination Type	Destination	Filename	Content Policy	Matched Item
30 minutes ago	credit-card	Storage Device	/Volumes/U/Credit Card.pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
4 hours ago	ssn	Storage Device	/Volumes/EPP/Nicoleta.pages	DEMO - Nicoleta	XXXXXXX7589
4 hours ago	credit-card	Storage Device	/Volumes/EPP/Credit Card.pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
2 days ago	Web Browser	Chrome	/Users/natalia/Downloads/estado_de_proveedores.xlsm.crdownload	DEMO - Natalia	XXXXXXXXXXXX2255
3 days ago	Web Browser	Chrome	/Users/nicoleta/Desktop/Credit Card.pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
3 days ago	Web Browser	Chrome	/Users/nicoleta/Dropbox/Credit Card (1).pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
3 days ago	Web Browser	Chrome	/Users/nicoleta/Dropbox/Credit Card.pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
5 days ago	Web Browser	Chrome	/Users/nicoleta/Desktop/Credit Card.pages	DEMO - Nicoleta	XXXXXXXXXXXX8944
6 days ago	Instant Messaging	Skype	/Users/Zoran/Desktop/ccn.docx	ionic	XXXXXXXXXXXX5968
6 days ago	Web Browser	Chrome	/Users/Zoran/Desktop/Screen Shot 2017-04-13 at 10.10.58.png	ionic	image/png

4.3. 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
- **Exit Points:** establishes the transfer destinations to be monitored
- **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.

Example

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

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 (Device Control > 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.

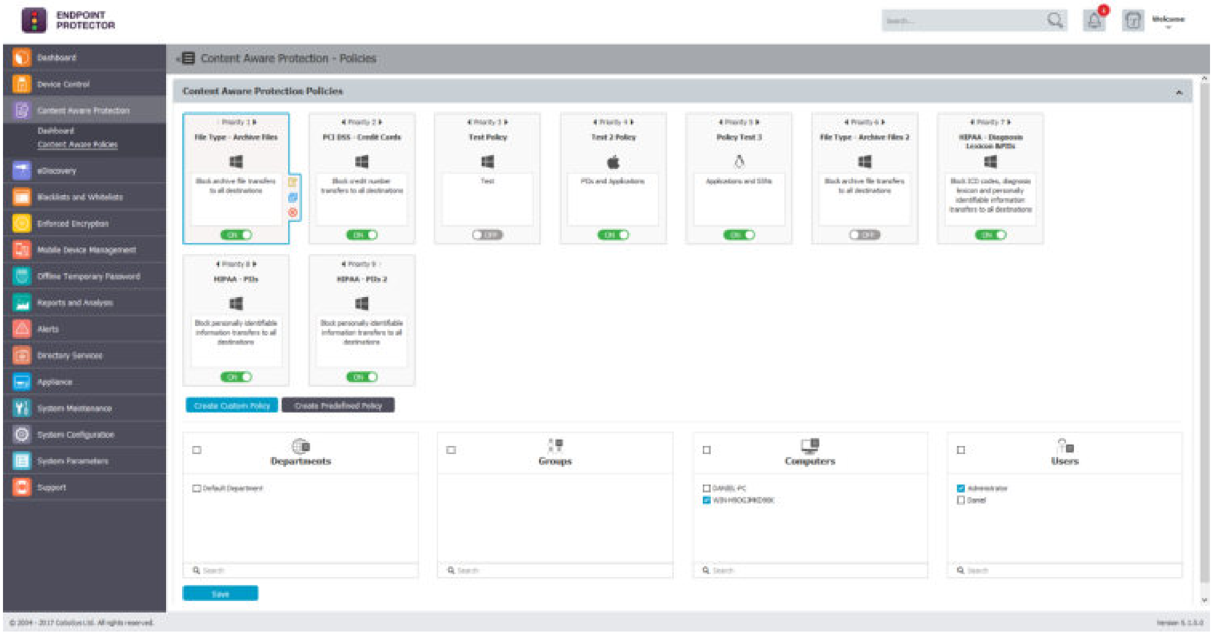
Information

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

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.

4.3.1. Creating a Content Aware Protection Policy

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



A new policy can be created by clicking on the Create Custom Policy button. An existing policy can be edited by double-clicking on it.

Information

The option to edit, duplicate or delete a policy is available after selecting the desired policy.

Tips

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.

When creating a new policy, the Policy Information (e.g. OS Type, Policy Name, and Policy Description), Policy Blacklists, Policy Whitelists and Policy Entities (Departments, Groups, and Computers) have to be selected.

The Policy Status can be set to Report only or to Block & Report all transfers of data that includes sensitive content.

Tips

Initially, we recommend using the Report only action in order 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 Thresholds that can be used are:

- Global Threshold (ON or OFF)
- If the Global Threshold is OFF, it can be considered a Regular Threshold.

Example

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 it will not block the transfers with 1, 2, 3 x SSN appearances.

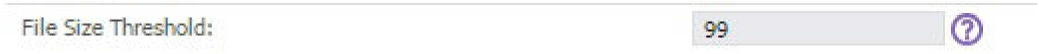
In contrast to the Regular Threshold which blocks 4 or more threats of the same type, the Global Threshold blocks 4 or more threats of different types combined. In another example, two (2) threats, one being a Social Security Number and the other being a Phone number, will not be blocked by a policy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

Tips

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.

- Threat Threshold value – Threshold Value

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



File Size Threshold: 99

To enable the File Size Threshold, a value bigger than 0 must be set. To disable the File Size Threshold, 0 or no value must be set.

Note

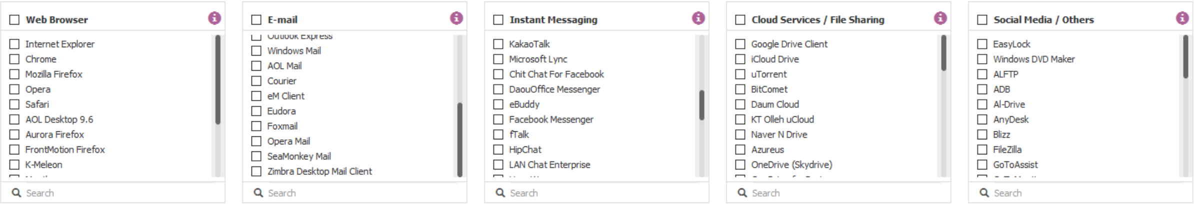
If a File Size Threshold is set, it will be applied to the whole policy, regardless of what file types or custom contents are checked inside the policy. The value used in the File Size Threshold must be a positive, whole number.

Information

Depending on the specific application and OS, some limitations may apply.

The exit points that can be monitored via the Controlled transfers to are:

- Applications



□ **Web Browser**
□ Internet Explorer
□ Chrome
□ Mozilla Firefox
□ Opera
□ Safari
□ AOL Desktop 9.6
□ Aurora Firefox
□ FrontMotion Firefox
□ K-Meleon
Search

□ **E-mail**
□ Outlook Express
□ Windows Mail
□ AOL Mail
□ Courier
□ eM Client
□ Eudora
□ Foxmail
□ Opera Mail
□ SeaMonkey Mail
□ Zimbra Desktop Mail Client
Search

□ **Instant Messaging**
□ KakaoTalk
□ Microsoft Lync
□ Chit Chat For Facebook
□ DaouOffice Messenger
□ eBuddy
□ Facebook Messenger
□ fTalk
□ HipChat
□ LAN Chat Enterprise
Search

□ **Cloud Services / File Sharing**
□ Google Drive Client
□ iCloud Drive
□ uTorrent
□ BitComet
□ Daum Cloud
□ KT Olleh uCloud
□ Naver N Drive
□ Azureus
□ OneDrive (Skydrive)
Search

□ **Social Media / Others**
□ EasyLock
□ Windows DVD Maker
□ ALFTP
□ ADB
□ Al-Drive
□ AnyDesk
□ Blizz
□ FileZilla
□ GoToAssist
Search

  - Web Browsers (e.g. Internet Explorer, Chrome, Firefox, Safari, etc.)
  - E-mail Clients (e.g. Outlook, Thunderbird, Lotus Notes, etc.)
  - Instant Messaging (e.g. Skype, Pidgin, Google Talk, etc.)
  - File Sharing (e.g. Google Drive Client, iCloud, Dropbox, DC++, etc.)
  - Other (e.g. iTunes, Total Commander, GoToMeeting, etc.)

Note

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

Information

The complete list of controlled Applications can be found directly in the Endpoint Protector User Interface.

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

Note

For Windows, file transfers will be monitored both to and from removable media.

> **Information**
> The option to monitor confidential data transfers only to Custom Classes and not all Storage Devices is also available.

- Network Share

> **Information**
> For Network Share for Macs, 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 are 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 Blacklists that can be used are:

- File Type

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

- Source Code

> **Tips**
> An N-gram based detection method is used to increase the accuracy of these file types. However, as various source code are closely linked together (e.g.: C, C++, etc.), these also be checked. To make things easier, Endpoint Protector automatically marks these correlations.

- Predefined Content

Tips

The majority of the Predefined Content items are country specific (e.g. Australia, Canada, Germany, Korea, United Kingdom, United States, .etc.). To avoid a large number of logs or potential false positives, only enable the Passports that apply to your region or sensitive data.

- Custom Content
- File Name
- File Location
- Regular Expressions
- HIPAA
- URL and Domain

The Whitelists that can be used are:

- MIME Type
- Allowed Files
- File Location
- Network Share
- E-mail Domain
- URL Name
- Deep Packet Inspection

Information

For more details about Blacklists and Whitelist, please see chapter 6 Blacklists and Whitelists.

Note

The Content Aware Protection Policies continue to report and/or block sensitive data transfers from protected computers even after they are disconnected from the company network. Logs will be saved within the Endpoint Protector Client and will be sent to the Server once connection has been reestablished.

The final step in creating a policy is selecting the entities that it will apply to. The entities that can be used are:

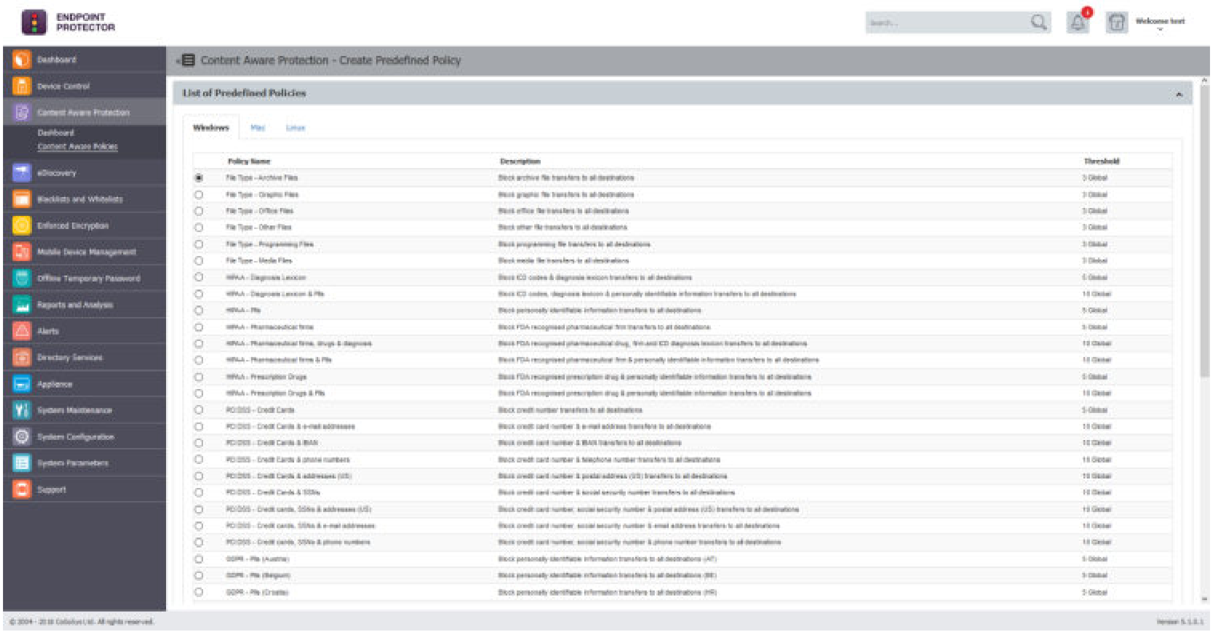
- Departments
- Groups
- Computers
- Users

Tips

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.

4.3.2. 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 Mac. 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.



Content Aware Protection - Create Predefined Policy

List of Predefined Policies

	Policy Name	Description	Threshold
●	File Type – Archive Files	Block archive file transfers to all destinations	3 Global
○	File Type – Graphic Files	Block graphic file transfers to all destinations	3 Global
○	File Type – Office Files	Block office file transfers to all destinations	3 Global
○	File Type – Other Files	Block other file transfers to all destinations	3 Global
○	File Type – Programming Files	Block programming file transfers to all destinations	3 Global
○	File Type – Media Files	Block media file transfers to all destinations	3 Global
○	HIPAA - Diagnosis Lexicon	Block ICD codes & diagnosis lexicon transfers to all destinations	5 Global
○	HIPAA - Diagnosis Lexicon & PIIs	Block ICD codes, diagnosis lexicon & personally identifiable information transfers to all destinations	10 Global
○	HIPAA - PIIs	Block personally identifiable information transfers to all destinations	5 Global
○	HIPAA - Pharmaceutical firms	Block FDA recognised pharmaceutical firm transfers to all destinations	3 Global
○	HIPAA - Pharmaceutical firms, drugs & diagnosis	Block FDA recognised pharmaceutical drug, firm and ICD diagnosis lexicon transfers to all destinations	10 Global
○	HIPAA - Pharmaceutical firms & PIIs	Block FDA recognised pharmaceutical firm & personally identifiable information transfers to all destinations	10 Global
○	HIPAA - Prescription Drugs	Block FDA recognised prescription drug & personally identifiable information transfers to all destinations	5 Global
○	HIPAA - Prescription Drugs & PIIs	Block FDA recognised prescription drug & personally identifiable information transfers to all destinations	10 Global
○	PCI DSS - Credit Cards	Block credit number transfers to all destinations	5 Global
○	PCI DSS - Credit Cards & e-mail addresses	Block credit card number & e-mail address transfers to all destinations	10 Global
○	PCI DSS - Credit Cards & IBAN	Block credit card number & IBAN transfers to all destinations	10 Global
○	PCI DSS - Credit Cards & phone numbers	Block credit card number & telephone number transfers to all destinations	10 Global
○	PCI DSS - Credit Cards & addresses (US)	Block credit card number & postal address (US) transfers to all destinations	10 Global
○	PCI DSS - Credit Cards & SSNs	Block credit card number & social security number transfers to all destinations	10 Global
○	PCI DSS - Credit cards, SSNs & addresses (US)	Block credit card number, social security number & postal address (US) transfers to all destinations	10 Global
○	PCI DSS - Credit cards, SSNs & e-mail addresses	Block credit card number, social security number & email address transfers to all destinations	10 Global
○	PCI DSS - Credit cards, SSNs & phone numbers	Block credit card number, social security number & phone number transfers to all destinations	10 Global
○	GDPR - PIIs (Austria)	Block personally identifiable information transfers to all destinations (AT)	5 Global
○	GDPR - PIIs (Belgium)	Block personally identifiable information transfers to all destinations (BE)	5 Global
○	GDPR - PIIs (Croatia)	Block personally identifiable information transfers to all destinations (HR)	5 Global

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.1.0.1

4.3.3. Applying multiple Content Aware Policies

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.

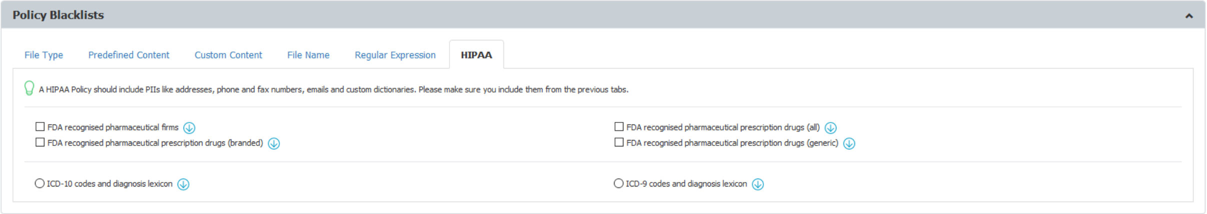
REPORTED	**BLOCKED**	IGNORED	Information will be reported.
BLOCKED	*REPORTED*	IGNORED	Information will be blocked.

⚠ **Note**

The information left unchecked when creating a policy will be considered as Ignored by Endpoint Protector and not as Allowed.

4.3.4. HIPAA compliance

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.

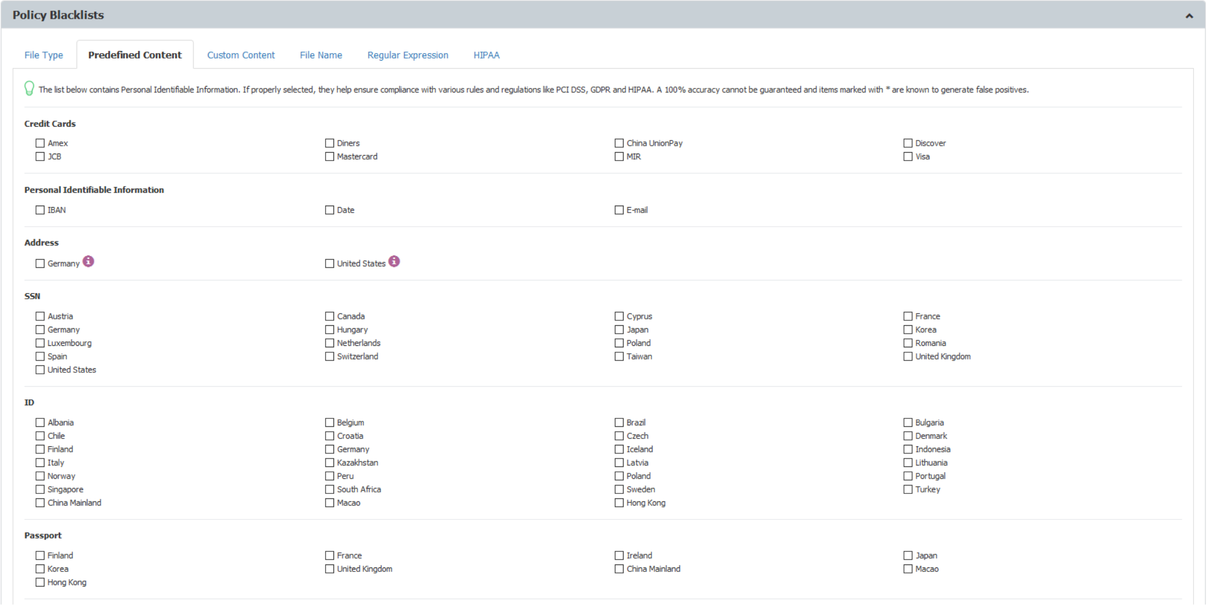


A HIPAA Policy should include PIIs like addresses, phone and fax numbers, emails and custom dictionaries. Please make sure you include them from the previous tabs.

□ FDA recognised pharmaceutical firms
□ FDA recognised pharmaceutical prescription drugs (all)
□ FDA recognised pharmaceutical prescription drugs (branded)
□ FDA recognised pharmaceutical prescription drugs (generic)

○ ICD-10 codes and diagnosis lexicon
○ ICD-9 codes and diagnosis lexicon

However, in order for a HIPAA policy to be effective, 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.



The list below contains Personal Identifiable Information. If properly selected, they help ensure compliance with various rules and regulations like PCI DSS, GDPR and HIPAA. A 100% accuracy cannot be guaranteed and items marked with * are known to generate false positives.

Credit Cards

□ Amex □ Diners □ China UnionPay □ Discover
□ JCB □ Mastercard □ MIR □ Visa

Personal Identifiable Information

□ IBAN □ Date □ E-mail

Address

□ Germany □ United States

SSN

□ Austria □ Canada □ Cyprus □ France
□ Germany □ Hungary □ Japan □ Korea
□ Luxembourg □ Netherlands □ Poland □ Romania
□ Spain □ Switzerland □ Taiwan □ United Kingdom
□ United States

ID

□ Albania □ Belgium □ Brazil □ Bulgaria
□ Chile □ Croatia □ Czech □ Denmark
□ Finland □ Germany □ Iceland □ Indonesia
□ Italy □ Kazakhstan □ Latvia □ Lithuania
□ Norway □ Peru □ Poland □ Portugal
□ Singapore □ South Africa □ Sweden □ Turkey
□ China Mainland □ Macao □ Hong Kong

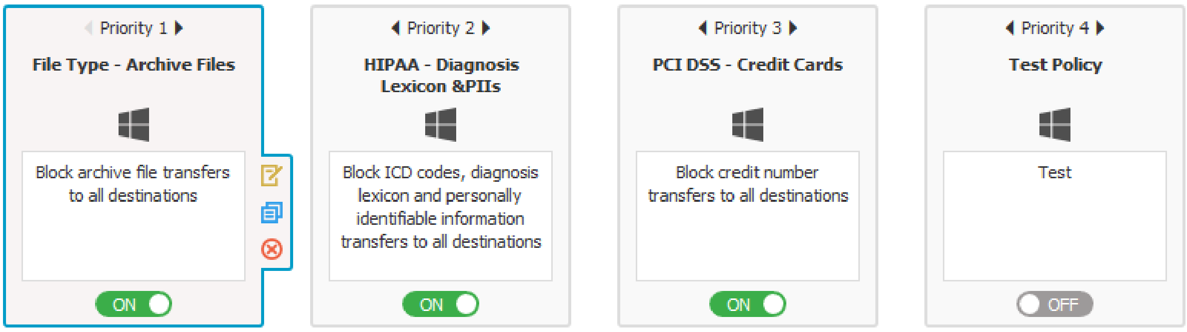
Passport

□ Finland □ France □ Ireland □ Japan
□ Korea □ United Kingdom □ China Mainland □ Macao
□ Hong Kong

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.



Priority 1
File Type - Archive Files
Block archive file transfers to all destinations
ON

Priority 2
HIPAA - Diagnosis Lexicon &PIIs
Block ICD codes, diagnosis lexicon and personally identifiable information transfers to all destinations
ON

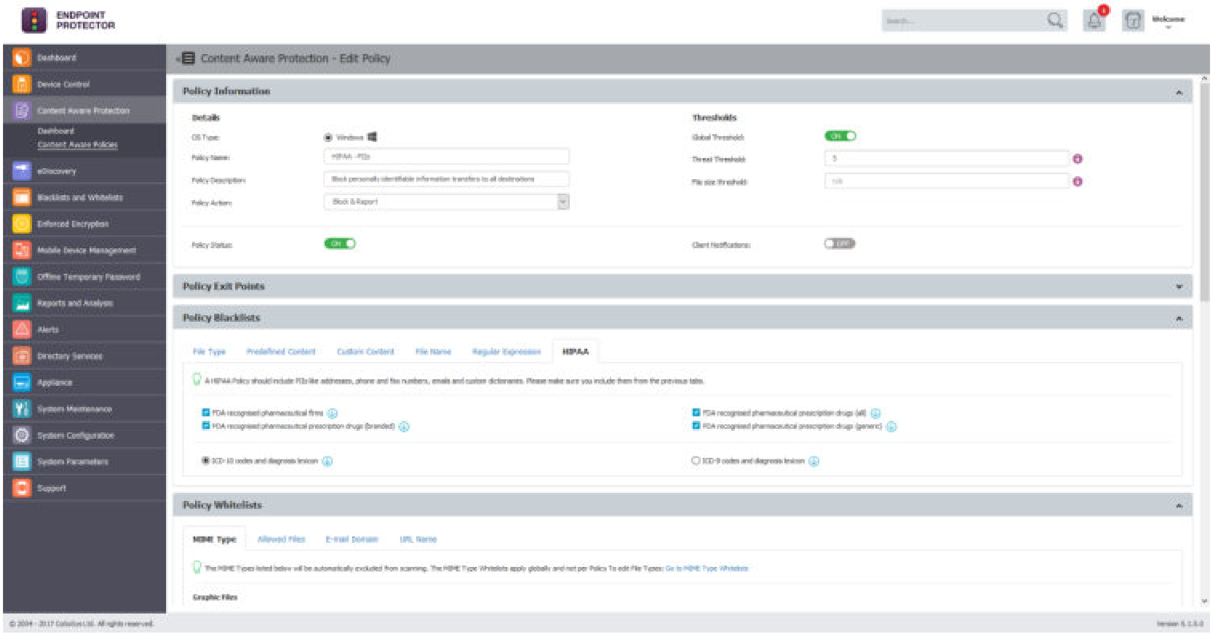
Priority 3
PCI DSS - Credit Cards
Block credit number transfers to all destinations
ON

Priority 4
Test Policy
Test
OFF

4.3.4.1. 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:



Content Aware Protection - Edit Policy

Policy Information

Details

OS Type: ● Windows

Policy Name: HIPAA - PIIs

Policy Description: Block personally identifiable information transfers to all destinations

Policy Action: Block & Report

Policy Status: ON

Thresholds

Global Threshold: ON

Threat Threshold: 5

File size threshold: n/a

Client Notifications: OFF

Policy Exit Points

Policy Blacklists

File Type | Predefined Content | Custom Content | File Name | Regular Expression | **HIPAA**

A HIPAA Policy should include PIIs like addresses, phone and fax numbers, emails and custom dictionaries. Please make sure you include them from the previous tabs.

☑ FDA recognized pharmaceutical firms

☑ FDA recognized pharmaceutical prescription drugs (branded)

☑ FDA recognized pharmaceutical prescription drugs (all)

☑ FDA recognized pharmaceutical prescription drugs (generic)

● ICD-10 codes and diagnosis lexicon

○ ICD-9 codes and diagnosis lexicon

Policy Whitelists

MIME Type | Allowed Files | E-mail Domain | URL Name

The MIME Types listed below will be automatically excluded from scanning. The MIME Type Whitelists apply globally and not per Policy. To edit File Types: Go to MIME Type Whitelists

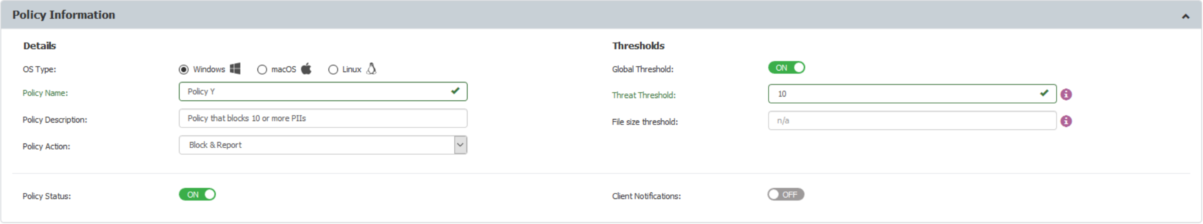
Graphic Files

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

4.3.4.2. 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:



Policy Information

Details

OS Type: ● Windows ○ macOS ○ Linux

Policy Name: Policy Y ✓

Policy Description: Policy that blocks 10 or more PIIs

Policy Action: Block & Report

Policy Status: ON

Thresholds

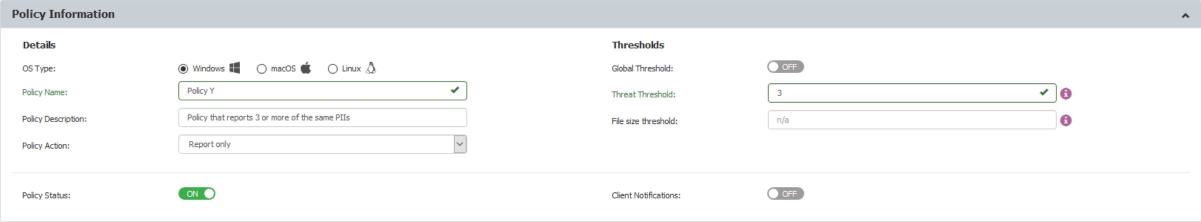
Global Threshold: ON

Threat Threshold: 10 ✓

File size threshold: n/a

Client Notifications: OFF

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

Details

OS Type: ● Windows ○ macOS ○ Linux

Policy Name: Policy Y ✓

Policy Description: Policy that reports 3 or more of the same PIIs

Policy Action: Report only

Policy Status: ON

Thresholds

Global Threshold: OFF

Threat Threshold: 3 ✓

File size threshold: n/a

Client Notifications: OFF

Information

As mentioned earlier, the Block & Report policy will have the 1st priority while the Report Only policy will be the 2nd.

5. eDiscovery

This module allows the Administrator to create policies that inspect data residing on protected Windows, Macs and Linux computers. The company's data protection strategy can be enforced and risks posed by accidental or intentional data leaks can be managed. The Administrator can mitigate problems posed by data at rest by discovering sensitive data, such as:

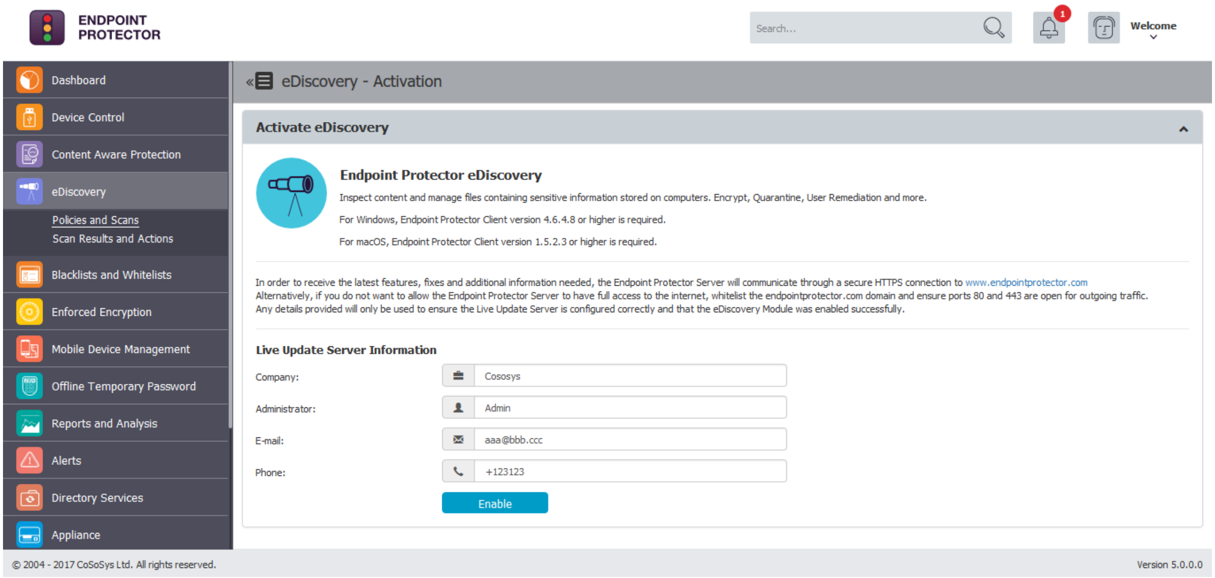
- Personally Identifiable Information (PII): social security numbers (SSN), driving license numbers, E-mail addresses, passport numbers, phone numbers, addresses, dates, etc.
- Financial and credit card information: credit card numbers for Visa, MasterCard, American Express, JCB, Discover Card, Dinners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

5.1. eDiscovery Activation

eDiscovery comes as the third level of data protection available in Endpoint Protector. The module is displayed but requires a simple activation by pressing the Enable button. If not previously provided, the contact details of the Main Administrator will be required.

Information

Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery module was enabled successfully.



eDiscovery - Activation

Activate eDiscovery

Endpoint Protector eDiscovery

Inspect content and manage files containing sensitive information stored on computers. Encrypt, Quarantine, User Remediation and more.

For Windows, Endpoint Protector Client version 4.6.4.8 or higher is required.

For macOS, Endpoint Protector Client version 1.5.2.3 or higher is required.

In order to receive the latest features, fixes and additional information needed, the Endpoint Protector Server will communicate through a secure HTTPS connection to www.endpointprotector.com
Alternatively, if you do not want to allow the Endpoint Protector Server to have full access to the internet, whitelist the endpointprotector.com domain and ensure ports 80 and 443 are open for outgoing traffic.
Any details provided will only be used to ensure the Live Update Server is configured correctly and that the eDiscovery Module was enabled successfully.

Live Update Server Information

Company:	Cososys
Administrator:	Admin
E-mail:	aaa@bbb.ccc
Phone:	+123123

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

Note

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

5.2. eDiscovery Policies and Scans

eDiscovery Policies are sets of rules for sensitive content detection for data stored on protected computers. An eDiscovery Policy is made up of five main elements:

- OS Type: the OS it applies to (Windows, Mac or Linux)
- Thresholds: the number of acceptable violations
- Policy Blacklists: the content to be detected
- Policy Whitelists: the content that can be ignored
- Entities: the departments, groups or computers it applies to

Information

Once the eDiscovery Policies is created, the desired type of eDiscovery Scan needs to be selected.

eDiscovery Scans are sets of rules for Policies, defining when to start the data discovery. There are several types of scans:

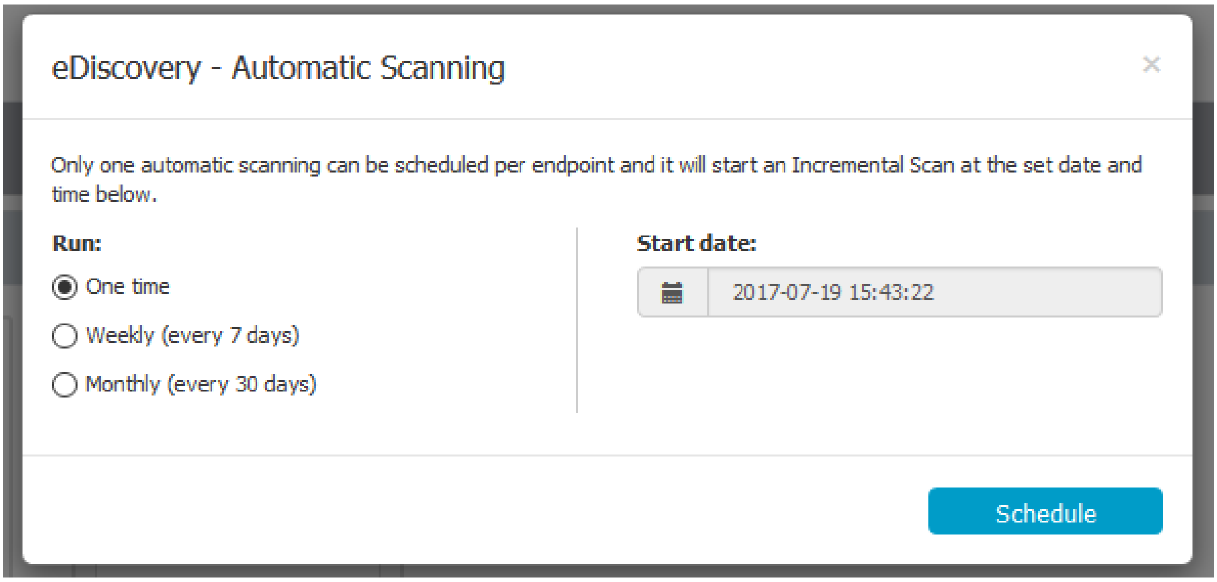
- Clean scan: stars a new discovery (from scratch)

- Incremental scan: continues the discovery (skipping the previously scanned files)

⚙ **Tips**

eDiscovery Automatic Scanning is also available, allowing the administrator to set an Incremental Scan

- One time – a scan will run once, at the specific date and time
- Weekly – a scan will run every 7 days, from the set date and time
- Monthly – a scan will run every 30 days, from the set date and time



eDiscovery - Automatic Scanning

Only one automatic scanning can be scheduled per endpoint and it will start an Incremental Scan at the set date and time below.

Run:

● One time

○ Weekly (every 7 days)

○ Monthly (every 30 days)

Start date: 2017-07-19 15:43:22

An eDiscovery Scan can be stopped at any time as results can also be automatically cleared. This can be done by using:

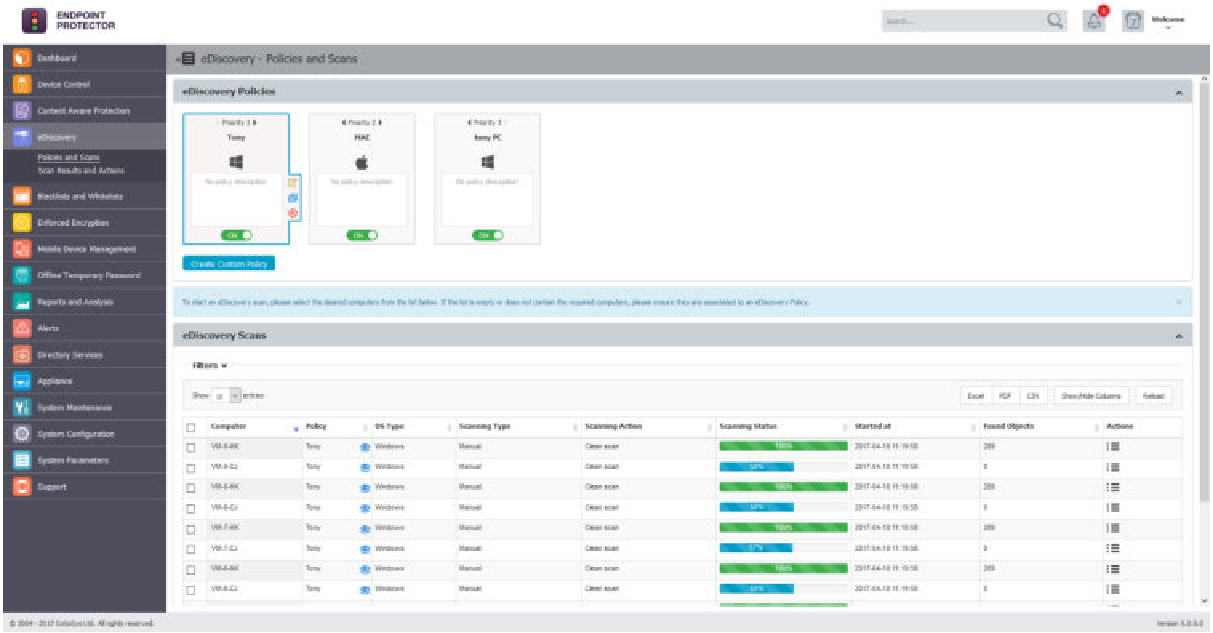
- Stop scan: stops the scan (but does not affect the logs)
- Stop scan and clear scan: stops the scan and clears the logs

⚠ **Note**

The Global Stop and Clear button can be used in situations where all the eDiscovery Scans need to be stopped and all the Logs cleared.

5.2.1. Creating an eDiscovery Policy and Scan

The Administrator can easily create and manage eDiscovery Policies and Scans from eDiscovery > Policies and Scans section.



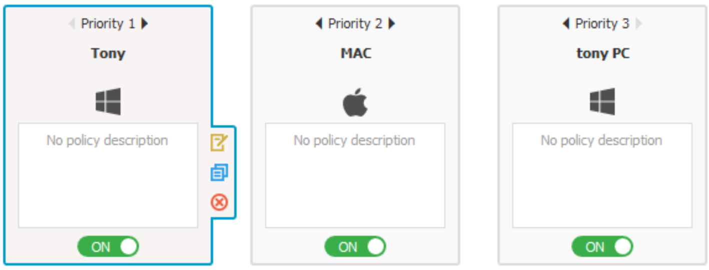
To start an eDiscovery scan, please select the desired computers from the list below. If the list is empty or does not contain the required computers, please ensure they are associated to an eDiscovery Policy.

□	Computer	Policy	OS Type	Scanning Type	Scanning Action	Scanning Status	Started at	Found Objects	Actions
□	VM-8-KK	Tony	Windows	Manual	Clean scan	100%	2017-04-18 11:19:58	289	
□	VM-8-CJ	Tony	Windows	Manual	Clean scan	58%	2017-04-18 11:19:58	3	
□	VM-8-KK	Tony	Windows	Manual	Clean scan	100%	2017-04-18 11:19:58	289	
□	VM-8-CJ	Tony	Windows	Manual	Clean scan	58%	2017-04-18 11:19:58	3	
□	VM-7-KK	Tony	Windows	Manual	Clean scan	100%	2017-04-18 11:19:58	289	
□	VM-7-CJ	Tony	Windows	Manual	Clean scan	57%	2017-04-18 11:19:58	3	
□	VM-6-KK	Tony	Windows	Manual	Clean scan	100%	2017-04-18 11:19:58	289	
□	VM-6-CJ	Tony	Windows	Manual	Clean scan	58%	2017-04-18 11:19:58	3	

A new policy can be created by clicking on the Create Custom Policy button. An existing policy can be edited by double-clicking on it.

Information

The option to edit, duplicate or delete a policy are available after selecting the desired policy.



When creating a new policy, the Policy Information (e.g. OS Type, Policy Name, and Policy Description), Policy Blacklists, Policy Whitelists and Policy Entities (Departments, Groups, and Computers) have to be selected.

The Thresholds that can be used are:

- Stop at Threat Threshold
- Threat Threshold value
- File Size Threshold

Information

More details about Thresholds can be found directly in the Endpoint Protector User Interface.

The Blacklists that can be used are:

- File Type

Tips

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

- Source Code

Tips

An N-gram based detection method is used to increase the accuracy of these file types. However, as various source code are closely linked together (e.g.: C, C++, etc.), these also be checked. To make things easier, Endpoint Protector automatically marks these correlations.

- Predefined Content

Tips

The majority of the Predefined Content items are country specific (e.g. Australia, Canada, Germany, Korea, United Kingdom, United States, .etc.). To avoid a large number of logs or potential false positives, only enable the Passports that apply to your region or sensitive data.

- Custom Content
- File Name
- Regular Expressions
- HIPAA

The Whitelists that can be used are:

- MIME Type

- Allowed Files

Information

For more details about Blacklists and Whitelist, please see chapter 6 Blacklists and Whitelists.

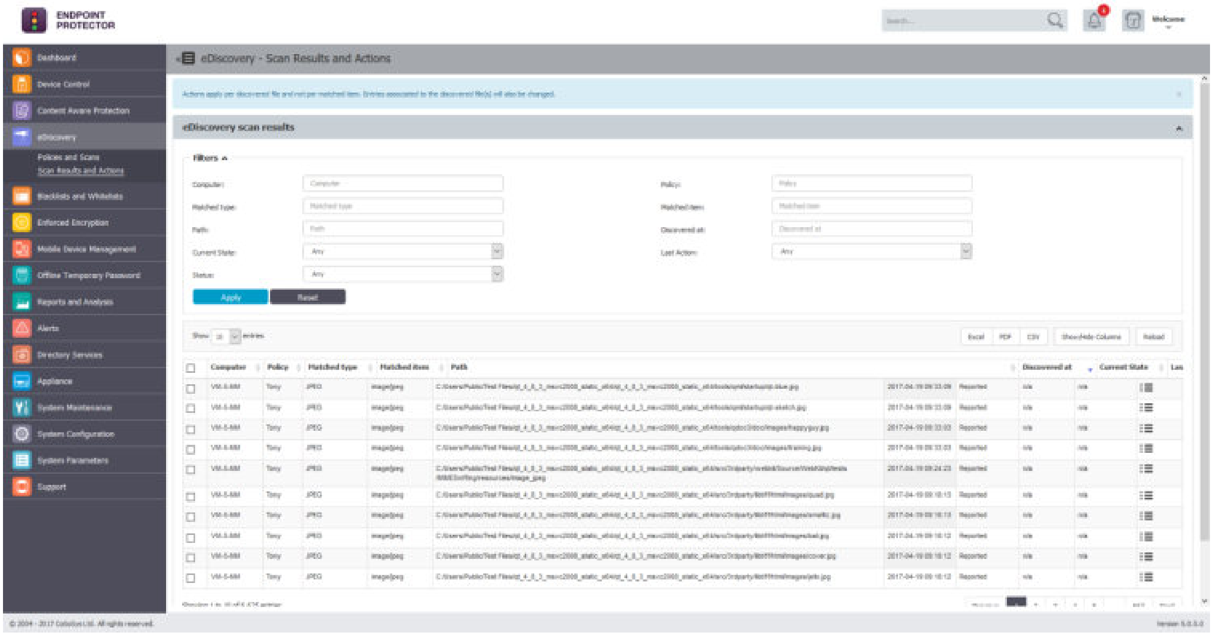
After the eDiscovery Policy has been created, Scanning Actions can be assigned. These include Start clean scan, Start incremental scan, Stop scan and Stop scan and clear logs.

Note

Exactly like Content Aware Protection Policies, the eDiscovery Policies and Scans continue to detect sensitive data stored on protected computers even after they are disconnected from the company network. Logs will be saved within the Endpoint Protector Client and will be sent to the Server once connection has been reestablished.

5.3. eDiscovery Scan Result and Actions

After an eDiscovery Scan stars, the found items can be inspected and remediation actions (e.g. delete on target, encrypt on target, decrypt on target, etc.). All results are displayed in eDiscovery > Scan Results and Actions section.



eDiscovery - Scan Results and Actions

Actions apply per discovered file and not per matched item. Entries associated to the discovered file(s) will also be changed.

eDiscovery scan results

Filters

Computer: Computer

Matched type: Matched type

Path: Path

Current State: Any

Status: Any

Policy: Policy

Matched item: Matched item

Discovered at: Discovered at

Last Action: Any

Show 10 entries

☐	Computer	Policy	Matched type	Matched item	Path			Discovered at	Current State	Las
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/tools/[illegible]blue.jpg	2017-04-19 09:33:09	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/tools/[illegible]sketch.jpg	2017-04-19 09:33:09	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/tools/[illegible]/images/happyguy.jpg	2017-04-19 09:33:03	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/tools/[illegible]/images/framing.jpg	2017-04-19 09:33:03	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/webkit/Source/WebKit/qt/tests/[illegible]/resources/image_jpeg	2017-04-19 09:24:23	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/[illegible]/images/quad.jpg	2017-04-19 09:18:13	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/[illegible]/images/[illegible].jpg	2017-04-19 09:18:13	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/[illegible]/images/ball.jpg	2017-04-19 09:18:12	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/[illegible]/images/cover.jpg	2017-04-19 09:18:12	Reported	n/a	n/a	☰
☐	VM-5-AM	Tony	JPEG	image/jpeg	C:/Users/Public/Test Files/qt_4_8_3_msvc2008_static_x64/qt_4_8_3_msvc2008_static_x64/src/3rdparty/[illegible]/images/[illegible].jpg	2017-04-19 09:18:12	Reported	n/a	n/a	☰

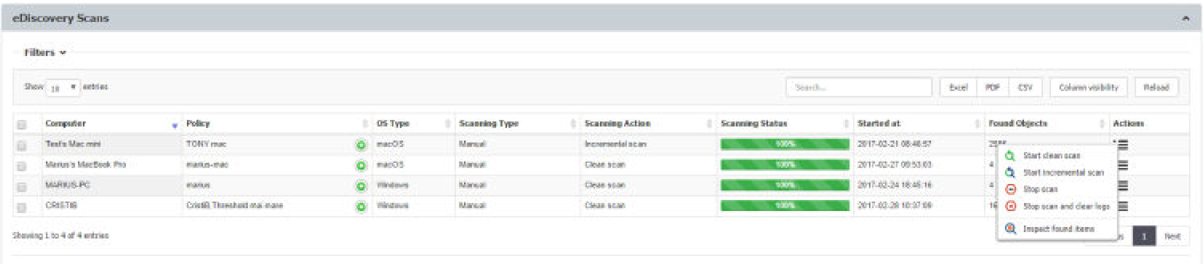
Showing 1 to 10 of [illegible] entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version [illegible]

Tips

The Scan Results and Actions section can also be accessed directly from eDiscovery > Policies and Scans by selecting a computer from the eDiscovery Scans list and choosing the Inspect found items action. This will automatically filter the Scan Results list and display the items only for that specific computer.



eDiscovery Scans

Filters

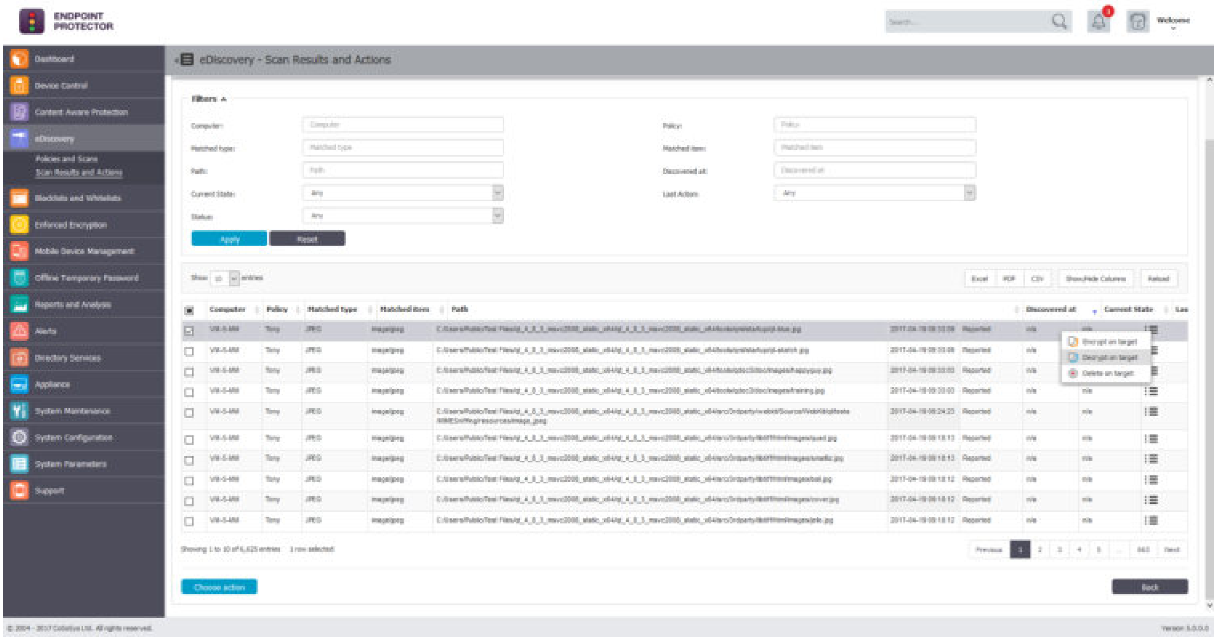
Show 10 entries

	Computer	Policy	OS Type	Scanning Type	Scanning Action	Scanning Status	Started at	Found Objects	Actions
□	Test's Mac mini	TONY mac	macOS	Manual	Incremental scan	100%	2017-02-21 08:48:57	25	
□	Marius's MacBook Pro	marius-mac	macOS	Manual	Clean scan	100%	2017-02-27 09:53:03	4	
□	MARIUS-PC	marius	Windows	Manual	Clean scan	100%	2017-02-24 18:46:16	4	
□	CRISTIB	CristiB Threshold mai mare	Windows	Manual	Clean scan	100%	2017-02-28 10:37:09	16	

Showing 1 to 4 of 4 entries

5.3.1. Viewing Scan Results and taking Actions

From this section, the Administrator can manage the scan results. A list with all the computers that were scanned can be viewed and actions such as deleting, encrypting or decrypting files can be taken.



eDiscovery - Scan Results and Actions

Filters

Computer: Computer
Policy: Policy
Matched type: Matched type
Matched item: Matched item
Path: Path
Discovered at: Discovered at
Current State: Any
Last Action: Any
Status: Any

Show 10 entries

☑	Computer	Policy	Matched type	Matched item	Path			Discovered at	Current State	Las
☑	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:33:08	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:33:08	Reported	n/a		
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:33:03	Reported	n/a		
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:33:03	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:24:23	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:18:13	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:18:13	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:18:12	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:18:12	Reported	n/a	n/a	
□	VM-5-MM	Tony	JPEG	image/jpeg	[illegible]	2017-04-19 09:18:12	Reported	n/a	n/a	

Showing 1 to 10 of 6,625 entries   1 row selected

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

The Administrator can apply the desired action to each item individually or, can select multiple items and apply the desired action simultaneously by using the Choose action button.

6. Blacklists and Whitelists

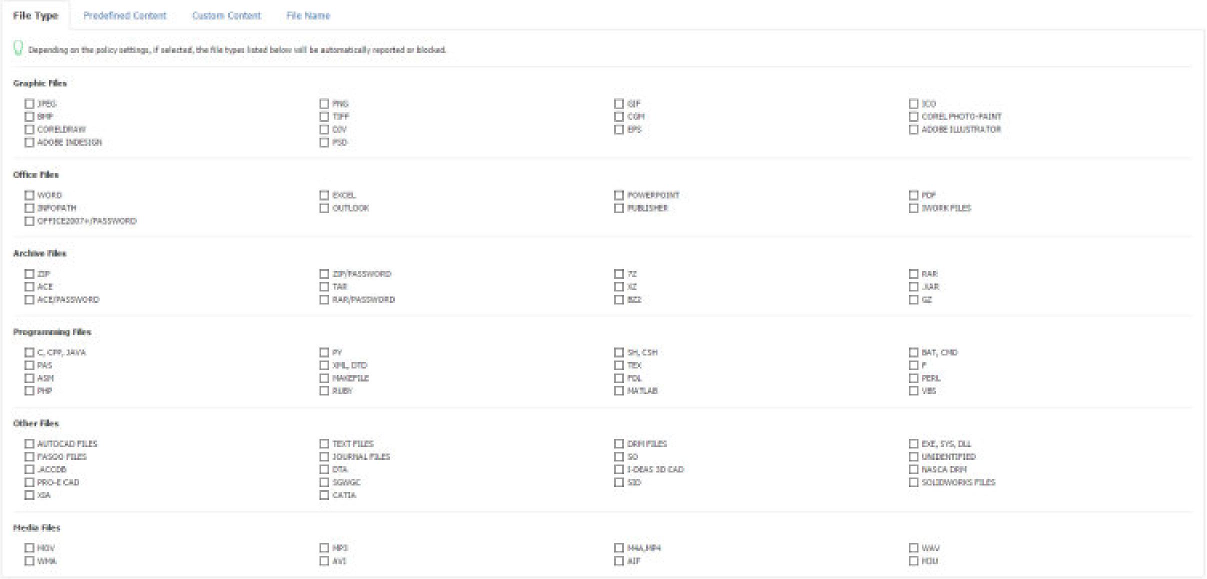
From this section, the Administrator can create Blacklists and Whitelists that can be used in both the Content Aware Protection and eDiscovery modules. Once defined, these blacklist and whitelist can be enabled in the desired Policy. The list of all Blacklists and Whitelists will be detailed below.

⚠ **Note**

Some Blacklist and Whitelists are OS related (e.g. E-mail Domain and URL Name are only available for Windows) or are not available for both modules.

6.1. File Type Blacklists

The content inspection functionally within Endpoint Protector can identify multiple file types. Additional file types are continually added, extending the available list with each Endpoint Protector Update. The Administrator can define what file types a Content Aware Protection or eDiscovery Policy scans for, but cannot directly extend the supported file type list. Since this is a predefined list, it only requires the Administrator to select the desired content from the File Type Content tab, within a Policy. This process has already been detailed in earlier paragraphs.



Depending on the policy settings, if selected, the file types listed below will be automatically reported or blocked.

Graphic Files

☐ JPEG
☐ BMP
☐ CORELDRAW
☐ ADOBE INDESIGN
☐ PNG
☐ TIFF
☐ DJV
☐ PSD
☐ GIF
☐ CGM
☐ EPS
☐ ICO
☐ COREL PHOTO-PAINT
☐ ADOBE ILLUSTRATOR

Office Files

☐ WORD
☐ INFOPATH
☐ OFFICE2007+/PASSWORD
☐ EXCEL
☐ OUTLOOK
☐ POWERPOINT
☐ PUBLISHER
☐ PDF
☐ IWORK FILES

Archive Files

☐ ZIP
☐ ACE
☐ ACE/PASSWORD
☐ ZIP/PASSWORD
☐ TAR
☐ RAR/PASSWORD
☐ 7Z
☐ XZ
☐ BZ2
☐ RAR
☐ JAR
☐ GZ

Programming Files

☐ C, CPP, JAVA
☐ PAS
☐ ASM
☐ PHP
☐ PY
☐ XML, DTD
☐ MAKEFILE
☐ RUBY
☐ SH, CSH
☐ TEX
☐ FDL
☐ MATLAB
☐ BAT, CMD
☐ F
☐ PERL
☐ VBS

Other Files

☐ AUTOCAD FILES
☐ FASOO FILES
☐ .ACCDB
☐ PRO-E CAD
☐ XSA
☐ TEXT FILES
☐ JOURNAL FILES
☐ DTA
☐ SGWGC
☐ CATIA
☐ DRM FILES
☐ SO
☐ I-DEAS 3D CAD
☐ SID
☐ EXE, SYS, DLL
☐ UNIDENTIFIED
☐ NASCA DRM
☐ SOLIDWORKS FILES

Media Files

☐ MOV
☐ WMA
☐ MP3
☐ AVI
☐ M4A,MP4
☐ AIF
☐ WAV
☐ M3U

Information

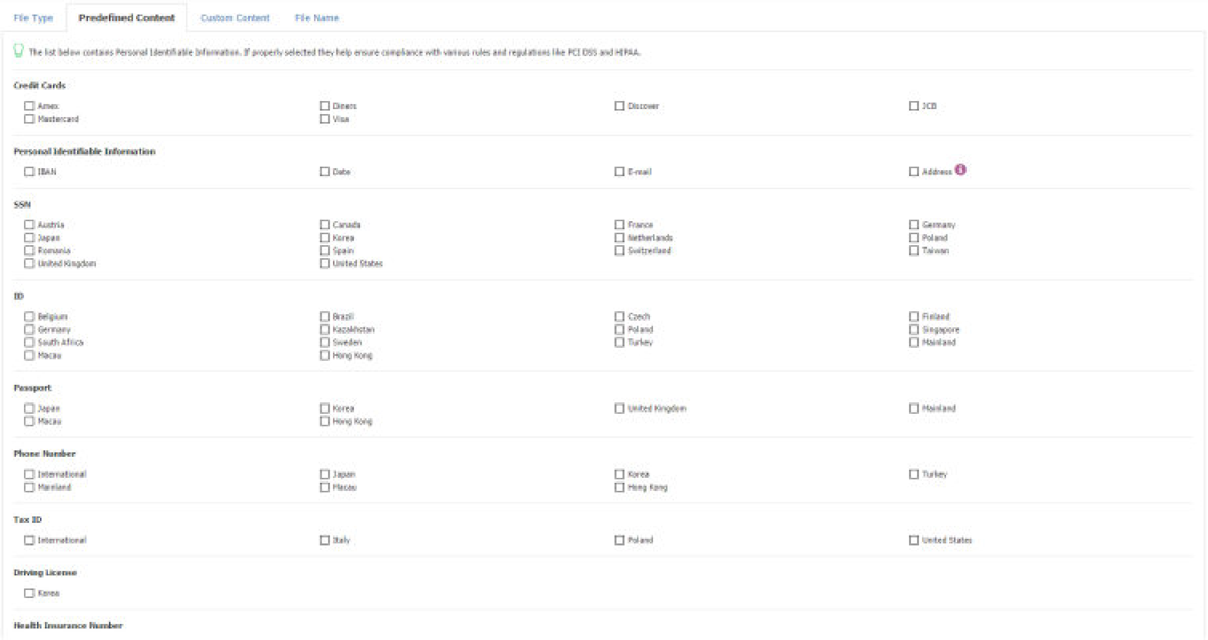
File Type Blacklists are available for both the Content Aware Protection and eDiscovery modules.

Note

File Type Blacklists refer to the true type of a file. If a user tries to circumvent the content inspection mechanism by manually changing the extension of the file, Endpoint Protector will still detect it.

6.2. Predefined Content Blacklists

Predefined Content Blacklists are predefined lists of terms and expressions to be detected as sensitive content by Endpoint Protector. Since this is a predefined list, it only requires the Administrator to select the desired content from within a Policy, from the Predefined Content tab.



The list below contains Personal Identifiable Information. If properly selected they help ensure compliance with various rules and regulations like PCI DSS and HIPAA.

Credit Cards

□ Amex □ Diners □ Discover □ JCB
□ Mastercard □ Visa

Personal Identifiable Information

□ IBAN □ Date □ E-mail □ Address

SSN

□ Austria □ Canada □ France □ Germany
□ Japan □ Korea □ Netherlands □ Poland
□ Romania □ Spain □ Switzerland □ Taiwan
□ United Kingdom □ United States

ID

□ Belgium □ Brazil □ Czech □ Finland
□ Germany □ Kazakhstan □ Poland □ Singapore
□ South Africa □ Sweden □ Turkey □ Mainland
□ Macau □ Hong Kong

Passport

□ Japan □ Korea □ United Kingdom □ Mainland
□ Macau □ Hong Kong

Phone Number

□ International □ Japan □ Korea □ Turkey
□ Mainland □ Macau □ Hong Kong

Tax ID

□ International □ Italy □ Poland □ United States

Driving License

□ Korea

Health Insurance Number

Information

Predefined Content Blacklists are available for both the Content Aware Protection and eDiscovery modules.

Predefined Content Blacklist include:

- Credit Cards

  Amex, Diners, China UnionPay, Discovery, JCB, MasterCard, MIR, Maestro, Visa

- Personal Identifiable Information

  IBAN, Date, E-mail, Address, etc.

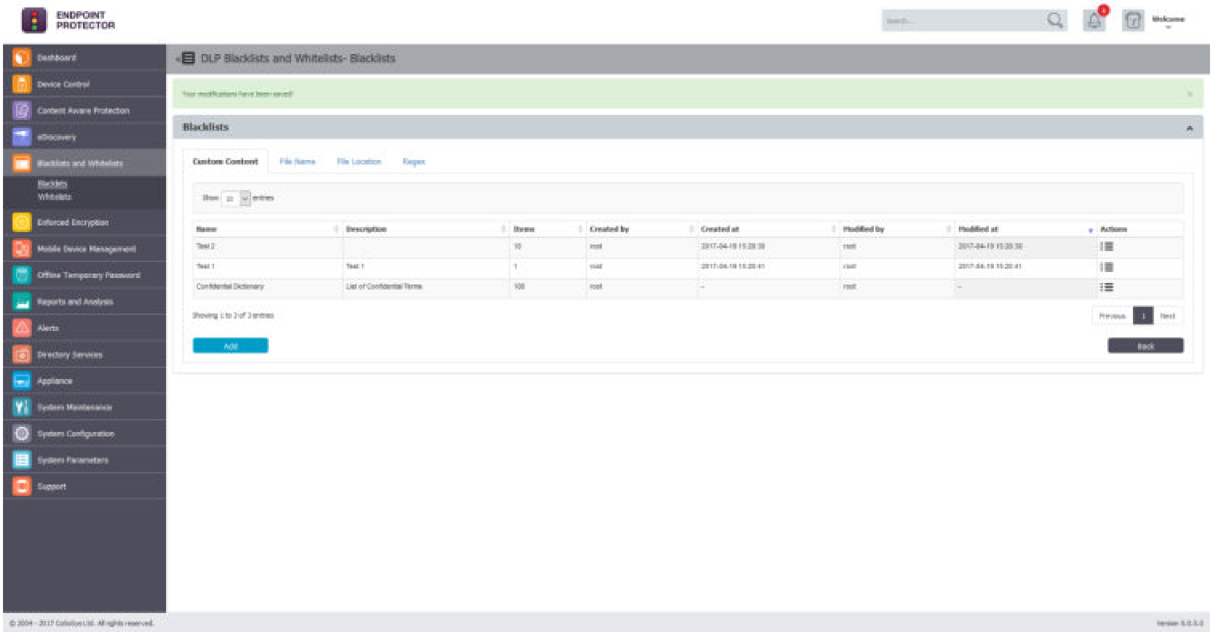
- Social Security Numbers (SSNs)
- Identifiers (IDs)
- Passports
- Tax IDs
- Driving Licenses
- Health Insurance Numbers

Tips

The majority of the Predefined Content items are country specific (e.g. Australia, Canada, Germany, Korea, United Kingdom, United States, .etc.). To avoid a large number of logs or potential false positives, only enable the Passports that apply to your region or sensitive data.

6.3. Custom Content Blacklists

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



Your modifications have been saved!

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Test 2		10	root	2017-04-19 15:28:38	root	2017-04-19 15:28:38	
Test 1	Test 1	1	root	2017-04-19 15:20:41	root	2017-04-19 15:20:41	
Confidential Dictionary	List of Confidential Terms	100	root	-	root	-	

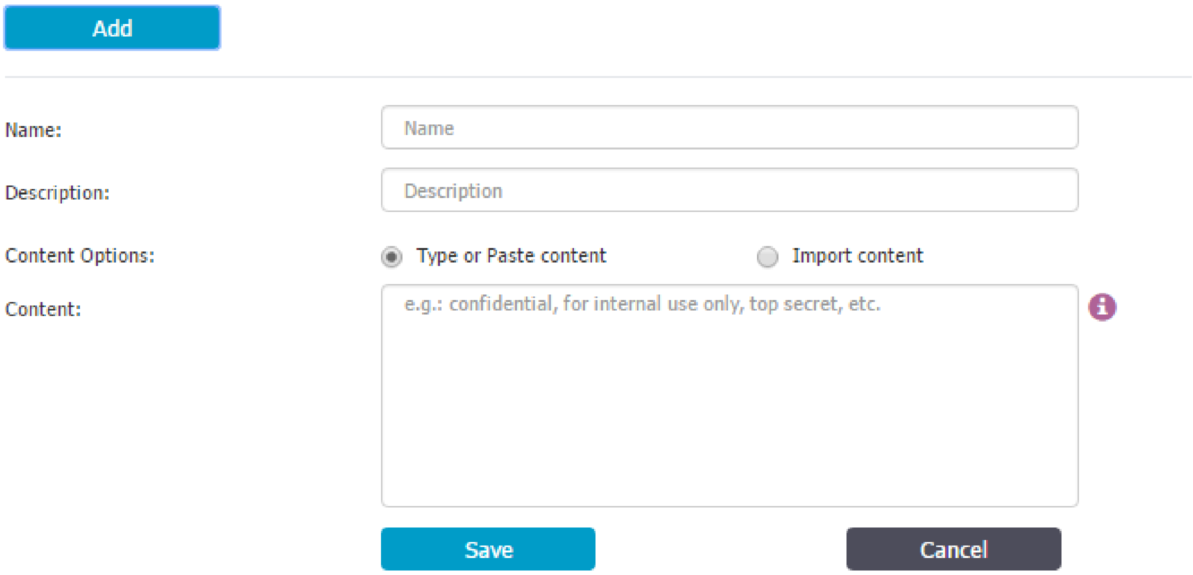
Showing 1 to 3 of 3 entries

Information

Custom Content Blacklists are available for both the Content Aware Protection and eDiscovery modules.

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

A new dictionary can be created by clicking on the Add button. To populate the content of a newly created dictionary, items of at least three characters can be entered either manually (typed or pasted) or imported.



Name: Name

Description: Description

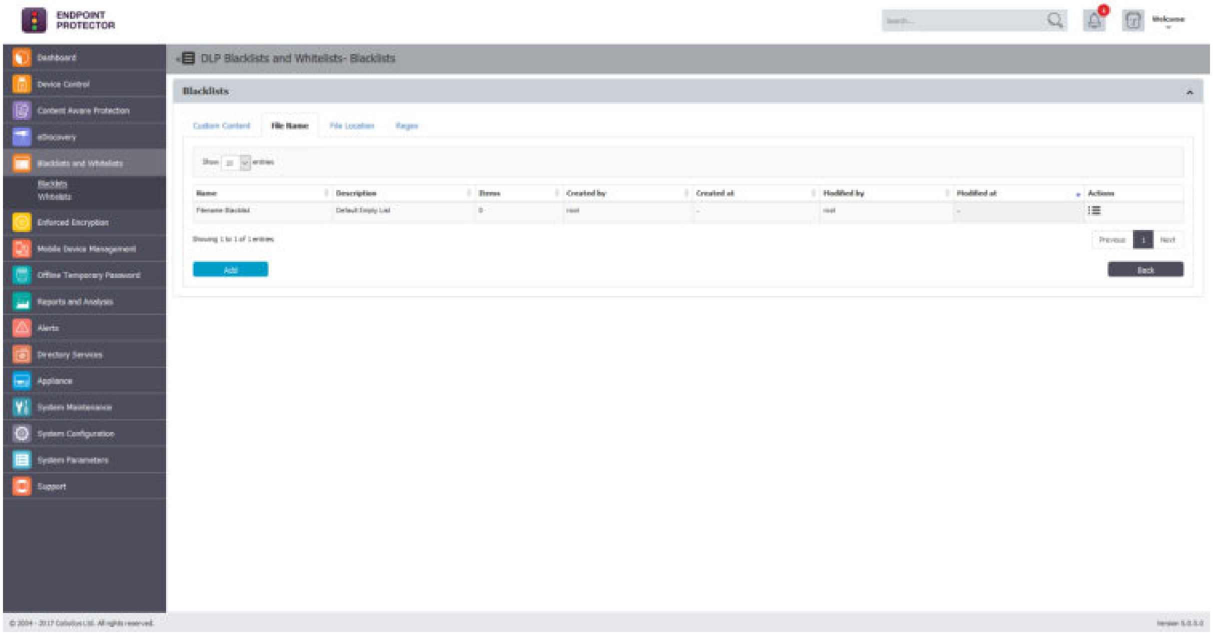
Content Options: ● Type or Paste content ○ Import content

Content: e.g.: confidential, for internal use only, top secret, etc.

Once a new dictionary is created, it will be automatically displayed inside the Custom Content tab. It will also be available when creating or editing a Content Aware Protection or eDiscovery Policy.

6.4. File Name Blacklists

File Name Blacklists are custom defined lists of file names detected by Endpoint Protector. The list of file names is available under DLP Blacklists and Whitelists > Blacklists > File Name tab.



Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Filename Blacklist	Default Empty List	0	root	-	root	-	☰

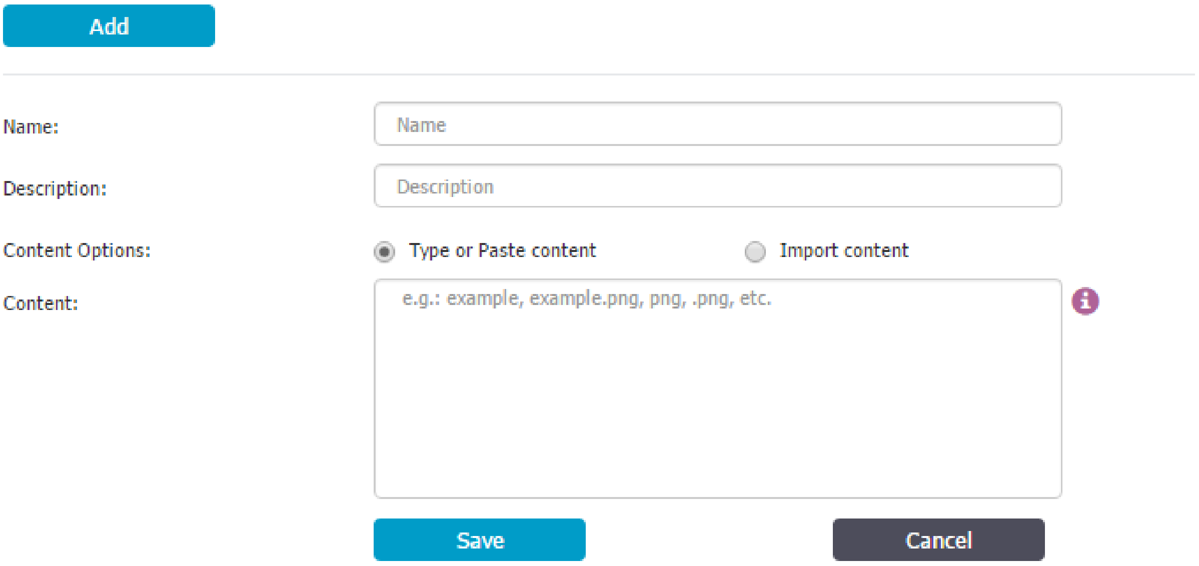
Showing 1 to 1 of 1 entries

Information

File Name Blacklists are available for both the Content Aware Protection and eDiscovery modules.

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

A new file name blacklist can be created by clicking the Add button. To populate the content of a newly created file name blacklist, items of at least two characters can be entered either manually (typed or pasted) or imported.



Name: Name

Description: Description

Content Options: ● Type or Paste content ○ Import content

Content: e.g.: example, example.png, png, .png, etc.

The content can be defined in multiple ways. It can be just the file name, file name and extension or just the extension.

Example

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

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

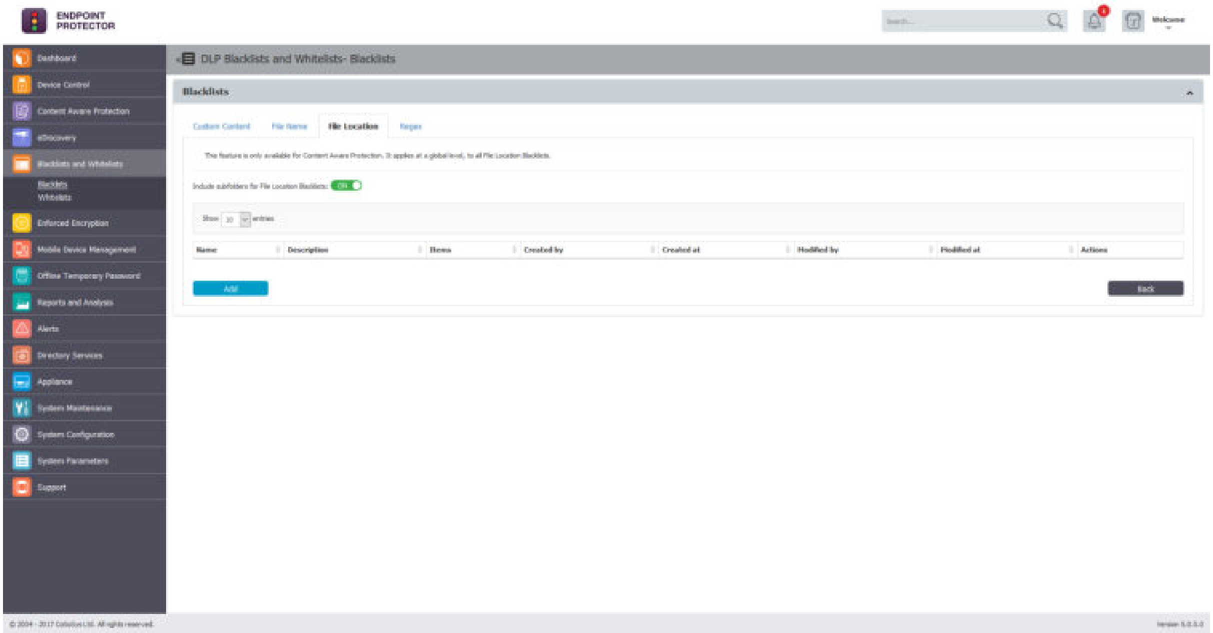
Once a new file name blacklist is created, it will automatically be displayed inside the File Name tab. It will also be available when creating or editing a Content Aware Protection or eDiscovery Policy.

Note

For Content Aware Protection, the File Name Blacklists work only for Block & Report type Policies. The Case Sensitive and Whole Words Only features do not apply.

6.5. File Location Blacklists

File Location Blacklists are custom defined lists of locations identified by Endpoint Protector. File transfers within this location are automatically blocked, regardless of the content inspection rules or permissions defined in various Policies. The list of locations is available under Blacklists and Whitelists > Blacklists > File Location tab.



This feature is only available for Content Aware Protection. It applies at a global level, to all File Location Blacklists.

Include subfolders for File Location Blacklists: ON

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions

⚠ Note

In addition to defining the File Location Blacklist, the browser or application used to transfer files also needs to be selected from within the Content Aware Protection Policy.

Tips

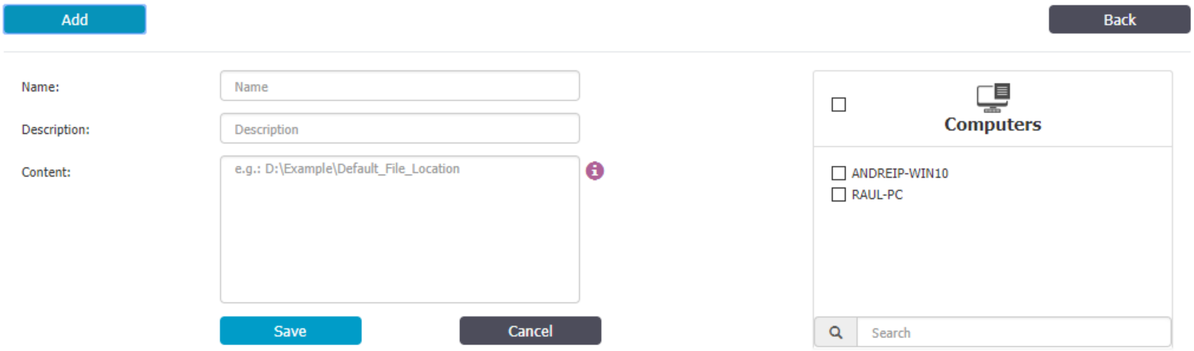
By default, the File Location Blacklists apply to all files located in the specific folder but also to any other files located in containing subfolders. While the “Include subfolders for File Location Blacklists” feature can be switched OFF, it will affect all other File Location Blacklists and Whitelists throughout the system.

Information

File Location Blacklists are available only for the Content Aware Protection module.

The available actions for each file name are: **Edit**, **Export** and **Delete**. ✎ ☒ ⊗

A new file location blacklist can be created by clicking the Add button. To populate the content of a newly created file location blacklist, items can be entered manually (typed or pasted). The computers to which it applies also need to be selected from the list on the right side.

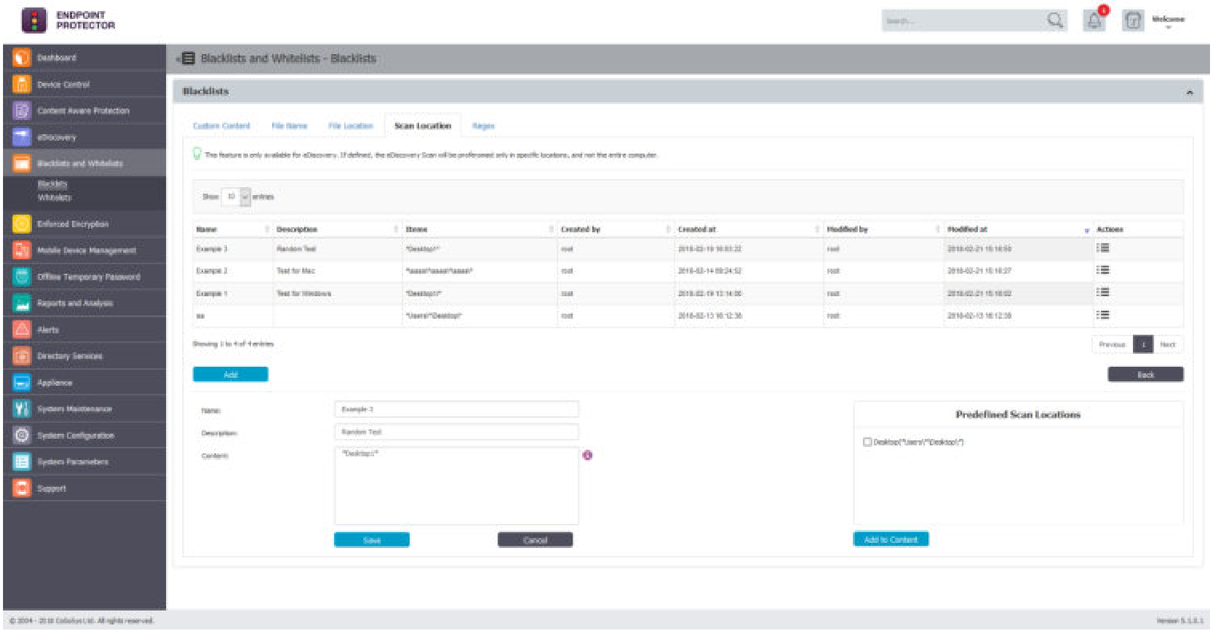


Name:	Name
Description:	Description
Content:	e.g.: D:\Example\Default_File_Location

□ Computers
□ ANDREIP-WIN10
□ RAUL-PC

6.6. Scan Location Blacklists

Scan Location Blacklists are custom defined lists of locations identified by the eDiscovery module. Data at rest within this location are automatically inspected for content, depending on the rules defined in various Policies. The list of locations is available under Blacklists and Whitelists > Blacklists > Scan Location tab.



This feature is only available for eDiscovery. If defined, the eDiscovery Scan will be preformed only in specific locations, and not the entire computer.

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Example 3	Random Text	*Desktop*	root	2018-02-19 16:03:22	root	2018-02-21 15:18:59	☰
Example 2	Test for Mac	*aaaa*aaaa*aaaa*	root	2018-02-14 09:24:52	root	2018-02-21 15:18:27	☰
Example 1	Test for Windows	*Desktop*	root	2018-02-19 13:14:00	root	2018-02-21 15:18:02	☰
aa		*Users*Desktop*	root	2018-02-13 16:12:38	root	2018-02-13 16:12:38	☰

Showing 1 to 4 of 4 entries

Name:	Example 3
Description:	Random Text
Content:	*Desktop*

Predefined Scan Locations
□ Desktop(*Users*Desktop*)

The available actions for each location are: **Edit** and **Delete**.

A new scan location blacklist can be created by clicking the Add button. To populate the content of a newly created scan location blacklist, items can be entered manually (typed or pasted).

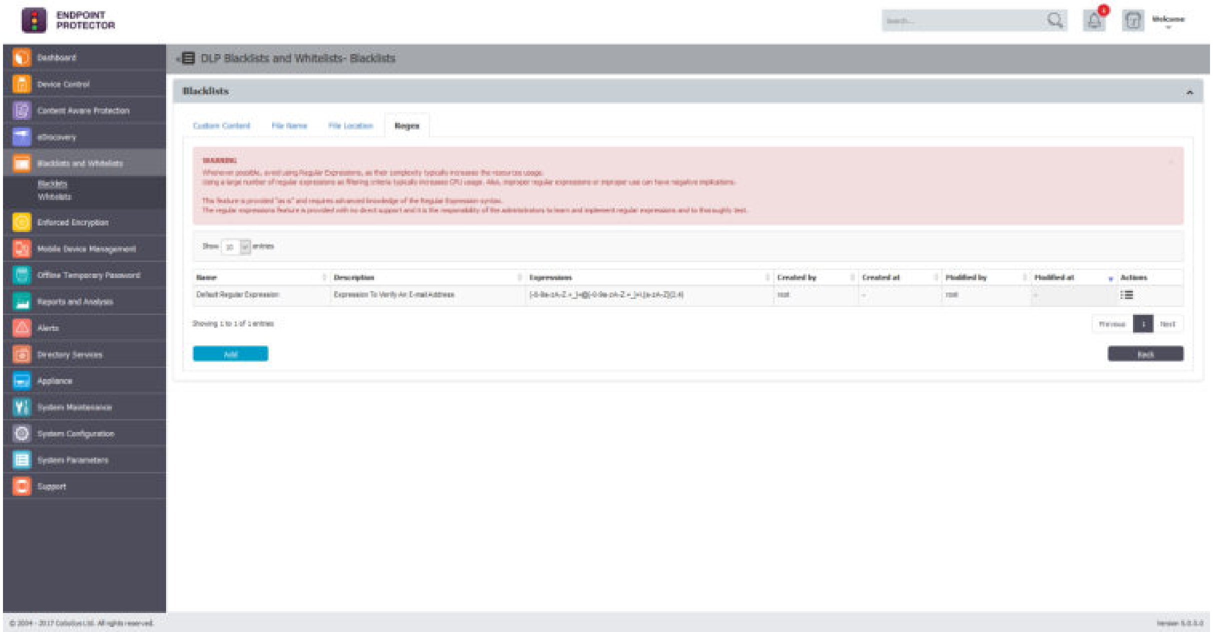
Information

A few predefined Scan Locations are available. They can also be adjusted to fit better to the desired results (e.g.: rather than scanning all Desktops, only some that follow a particular pattern can be defined).

When defining a Scan Location, some special characters can be used to tailor the path:
* - can be used to replace any word
? – can be used to replace any character

6.7. 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.



DLP Blacklists and Whitelists- Blacklists

Blacklists

WARNING:
Whenever 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 administrators to learn and implement regular expressions and to thoroughly test.

Show 10 entries

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

Showing 1 to 1 of 1 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

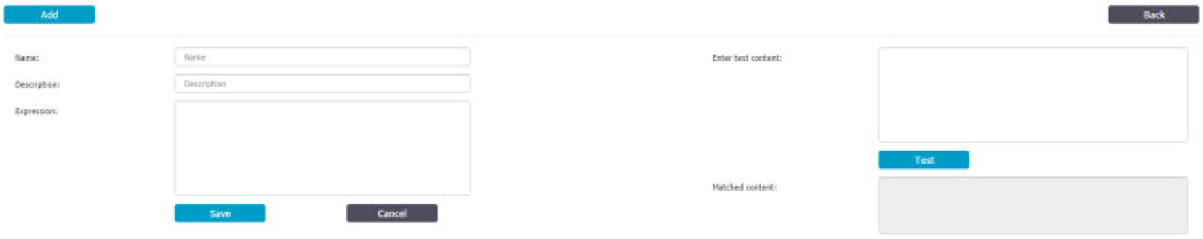
Version 5.0.0.0

Information

Regex Blacklists are available for both the Content Aware Protection and eDiscovery modules.

The available actions for each file name are: **Edit**, **Export** and **Delete**. 📝 ▣ ⊗

A new file regex blacklist can be created by clicking the Add button. Regular Expressions can be tested for accuracy. Insert into the Enter test content 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 content box, as shown below:



Example

To match an E-mail:

[-0-9a-zA-Z.+_]+@[-0-9a-zA-Z.+_]+\.[a-zA-Z]{2,4}

Example

To match 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}

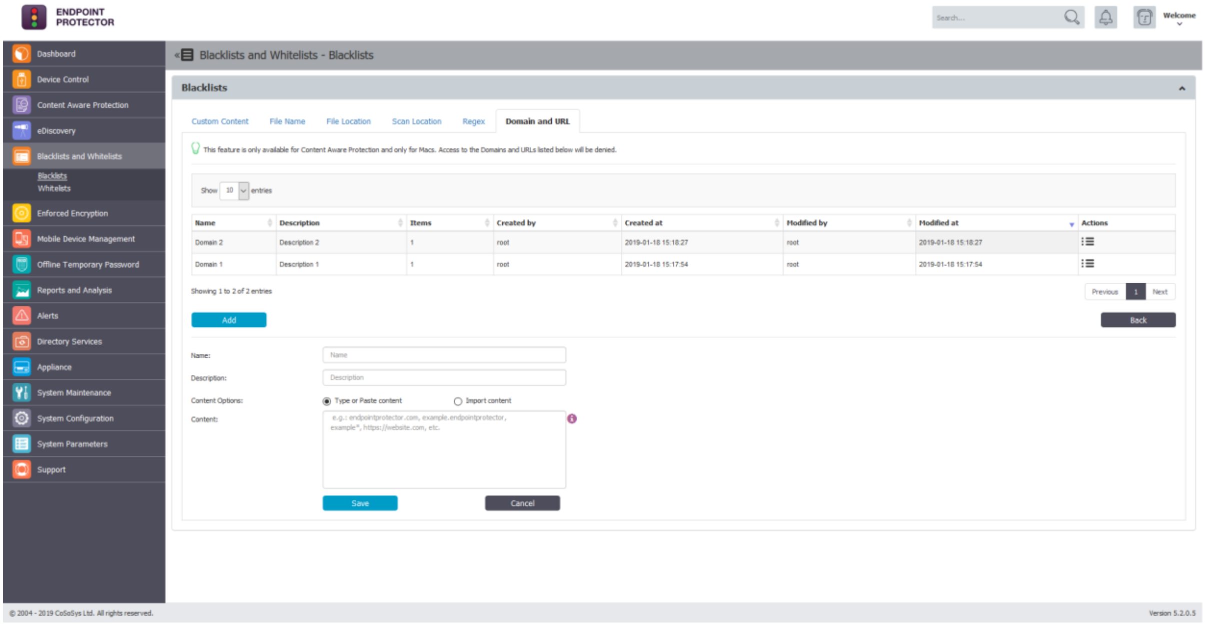
Note

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. No direct support is offered and it is the responsibility of the customers to learn and implement regular expressions and to thoroughly test.

6.8. Domain and URL Blacklists

Domain and URL Blacklists are custom defined lists of web addresses identified by Endpoint Protector. Access to domains and URLs from these lists will be denied. The list of domains and URLs is available under Blacklists and Whitelists > Blacklists > Domain and URL tab.



This feature is only available for Content Aware Protection and only for Macs. Access to the Domains and URLs listed below will be denied.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Domain 2	Description 2	1	root	2019-01-18 15:18:27	root	2019-01-18 15:18:27	☰
Domain 1	Description 1	1	root	2019-01-18 15:17:54	root	2019-01-18 15:17:54	☰

Showing 1 to 2 of 2 entries

Name: Name

Description: Description

Content Options: ● Type or Paste content ○ Import content

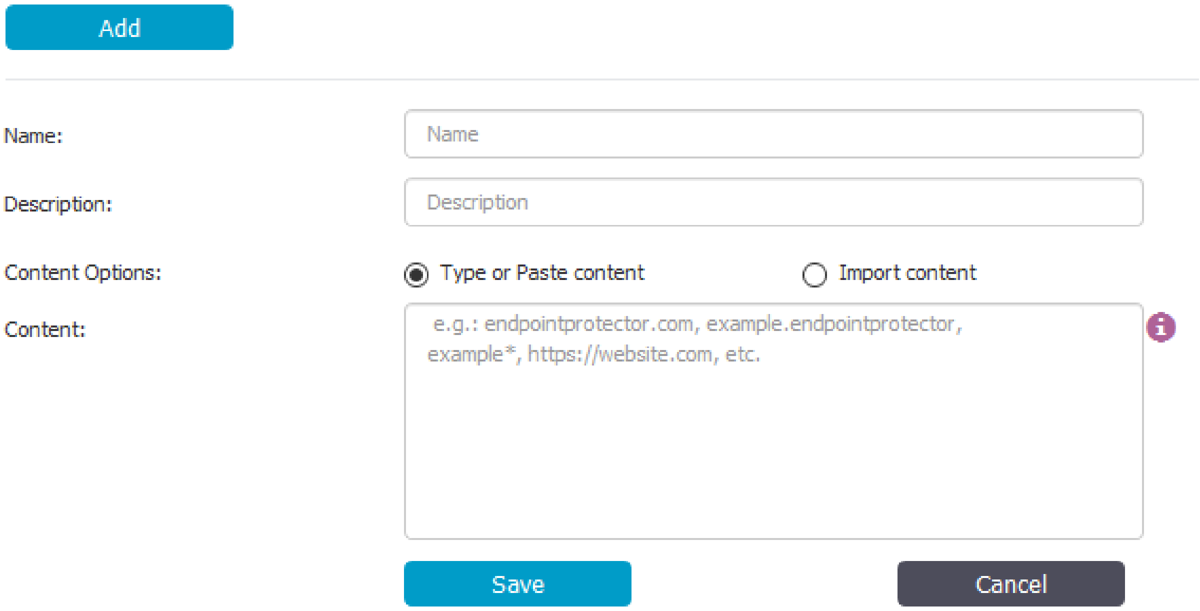
Content: e.g.: endpointprotector.com, example.endpointprotector, example*, https://website.com, etc.

Information

Domain and URL Blacklists are available only for the Content Aware Protection module and only for Macs.

The available actions for each file name are: **Edit**, **Export** and **Delete**. 📝 ☒ ⊗

A new domain and URL blacklist can be created by clicking the Add button. To populate the content of a newly created domain and URL blacklist, items can be entered either manually (typed or pasted) or imported.



Name: Name

Description: Description

Content Options: ● Type or Paste content ○ Import content

Content: e.g.: endpointprotector.com, example.endpointprotector, example*, https://website.com, etc.

The content can be defined in multiple ways. It can be just the file name, file name and extension or just the extension.

> **Example**
>
> pdf, test1example.pdf. example.endpointprotector.com, *example.com, *example*example, https://website.com

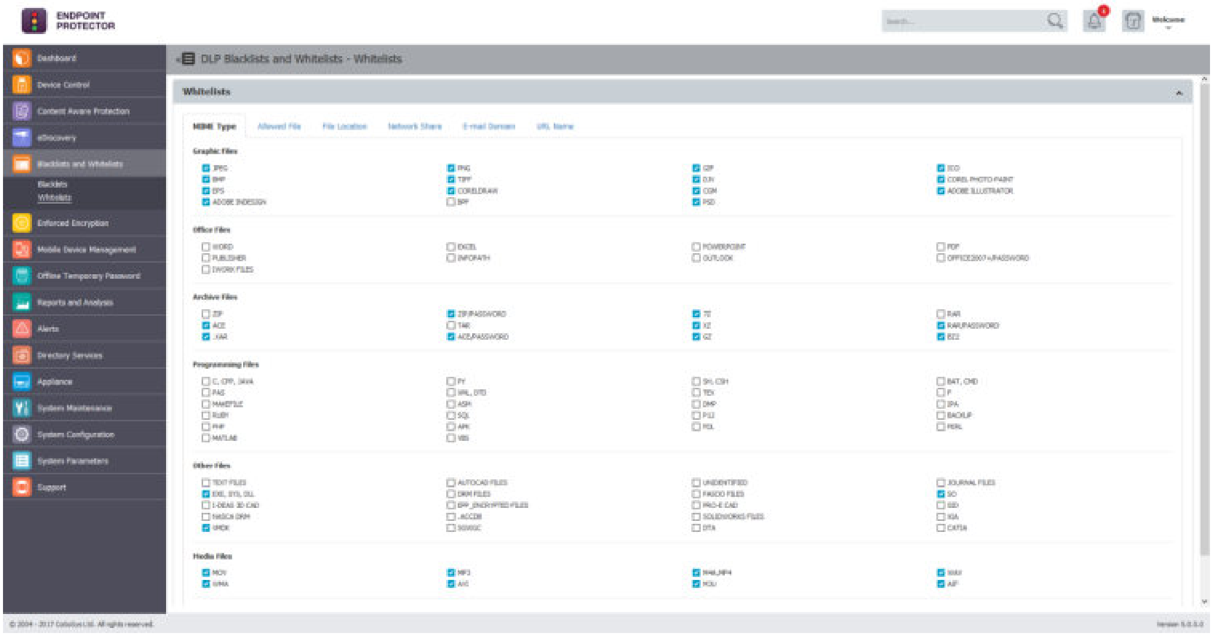
Once a new domain and URL blacklist is created, it will automatically be displayed inside the Domain and URL tab. It will also be available when creating or editing a Content Aware Protection Policy.

6.9. MIME Type Whitelists

The content inspection functionally within Endpoint Protector identifies multiple file types. While some files (e.g. Word, Excel, PDFs, etc.) can contain confidential information (e.g. PIIs, SSNs, Credit Cards, etc.), other files are highly unlikely to contain such data (e.g. .dll, .exe, .mp3, .avi, etc.).

The purpose of the MIME Type Whitelists is to eliminate the use of resources to inspect redundant and unnecessary files for content, as well as reducing false positives due to information detected in the metadata of files where the risk of data loss is extremely low.

> **Example**
>
> As songs or video files cannot contain lists of credit card numbers, there is no need to inspect them using content filters.



Graphic Files

☑ JPEG
☑ BMP
☑ EPS
☑ ADOBE INDESIGN
☑ PNG
☑ TIFF
☑ CORELDRAW
☐ BPF
☑ GIF
☑ DJN
☑ CGM
☑ PSD
☑ ICO
☑ COREL PHOTO PAINT
☑ ADOBE ILLUSTRATOR

Office Files

☐ WORD
☐ PUBLISHER
☐ IWORK FILES
☐ EXCEL
☐ INFOPATH
☐ POWERPOINT
☐ OUTLOOK
☐ PDF
☐ OFFICE2007+/PASSWORD

Archive Files

☐ ZIP
☑ ACE
☑ .XAR
☑ ZIP/PASSWORD
☐ TAR
☑ ACE/PASSWORD
☑ 7Z
☑ XZ
☑ GZ
☐ RAR
☑ RAR/PASSWORD
☑ BZ2

Programming Files

☐ C, CPP, JAVA
☐ PAS
☐ MAKEFILE
☐ RUBY
☐ PHP
☐ MATLAB
☐ PY
☐ XML, DTD
☐ ASM
☐ SQL
☐ APK
☐ VBS
☐ SH, CSH
☐ TEX
☐ DMP
☐ P12
☐ PDL
☐ BAT, CMD
☐ F
☐ IPA
☐ BACKUP
☐ PERL

Other Files

☐ TEXT FILES
☑ EXE, SYS, DLL
☐ I-DEAS 3D CAD
☐ NASCA DRM
☑ VMDK
☐ AUTOCAD FILES
☐ DRM FILES
☐ EPP_ENCRYPTED FILES
☐ .ACCDB
☐ SOSOGC
☐ UNIDENTIFIED
☐ FASOO FILES
☐ PRO-E CAD
☐ SOLIDWORKS FILES
☐ DTA
☐ JOURNAL FILES
☑ SO
☐ SID
☐ XIA
☐ CATIA

Media Files

☑ MOV
☑ WMA
☑ MP3
☑ AAC
☑ M4A_MP4
☑ M3U
☑ WAV
☑ AIF

Information

MIME Type Whitelists are available for both the Content Aware Protection and eDiscovery modules and apply to Custom Content, Predefined Content and Regular Expressions.

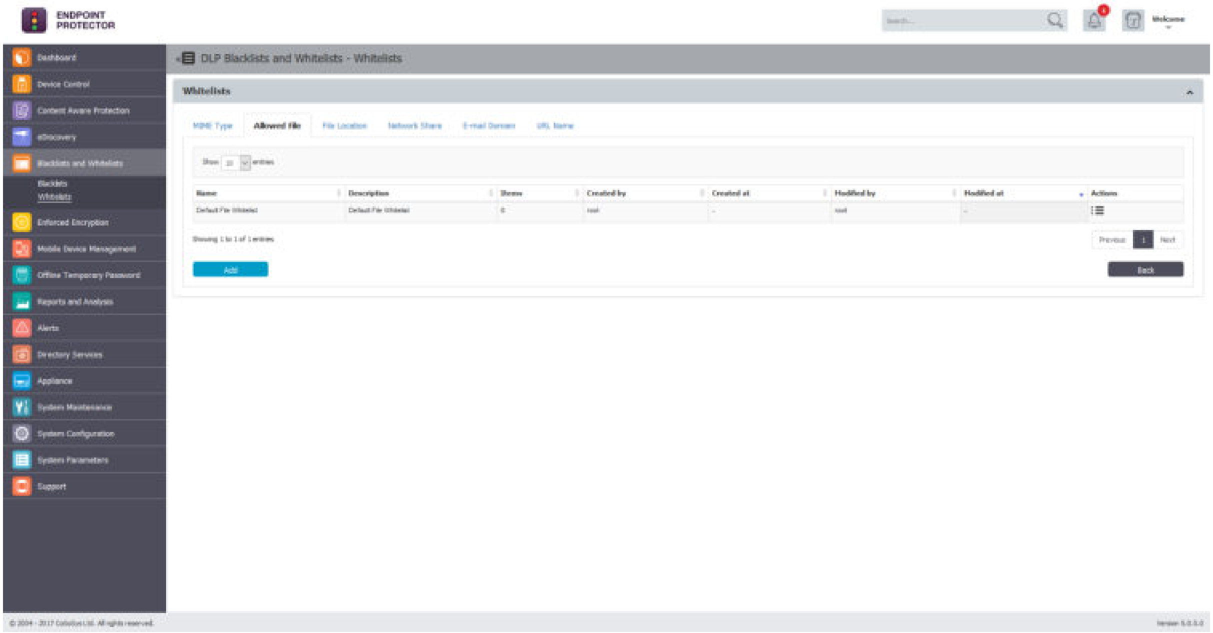
Tips

By default, graphic files, media files, some password protected achieve files and some system files are automatically defined within the MIME Type Whitelists. While this can easily be changed, we recommend only doing so after gaining a deeper understanding of the type of data transferred used or stored by the users in your system and, the subsequent logs increase in the Endpoint Protector Server.

The list of MIME types is available under DLP Blacklists and Whitelists > Whitelists > MIME Type tab.

6.10. Allowed Files Whitelists

Allowed Files Whitelists are custom groups of files which the administrator wishes to exclude from sensitive content detection by Endpoint Protector. The group of allowed files is available under DLP Blacklists and Whitelists > Whitelists > Allowed Files tab.



Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default File Whitelist	Default File Whitelist	0	root	-	root	-	☰

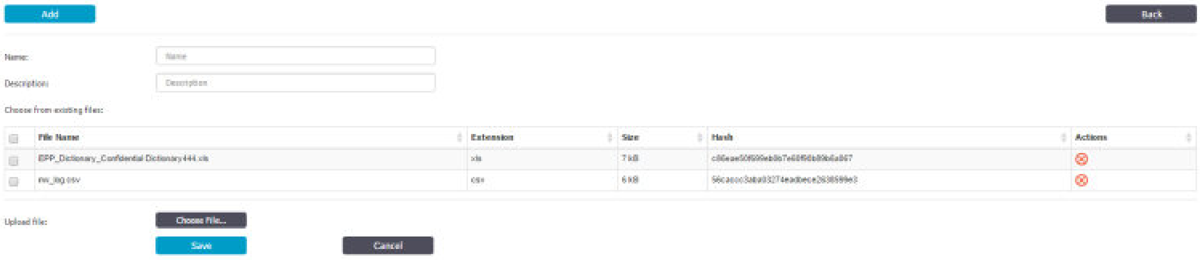
Showing 1 to 1 of 1 entries

Information

Allowed Files Whitelists are available for both the Content Aware Protection and eDiscovery modules.

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

A new allowed file whitelist can be created by clicking on the Add button. To populate the content of a newly created whitelist, allowed files need to be uploaded to the Endpoint Protector Server. Once files are uploaded, they can be used in multiple whitelists.



Name: Name

Description: Description

Choose from existing files:

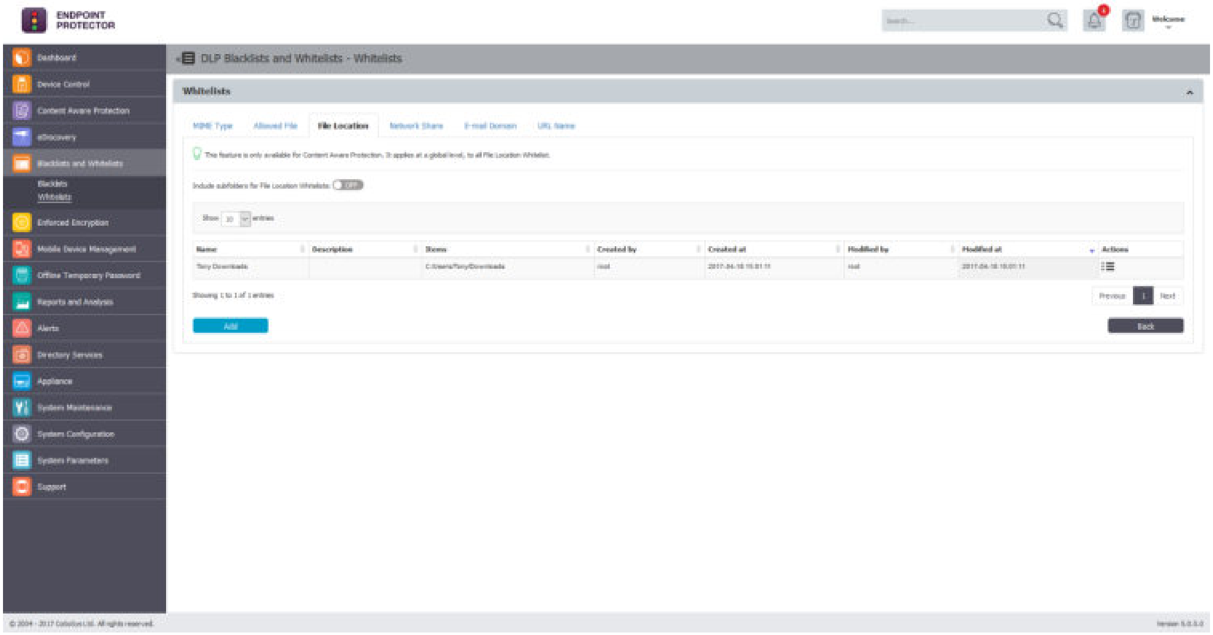
□	File Name	Extension	Size	Hash	Actions
□	EPP_Dictionary_Confidential Dictionary444.xls	xls	7 kB	c86eae50f699eb8b7e68f6bb89b6a867	⊗
□	nw_log.csv	csv	6 kB	56caccc3aba03274eadbece2638599e3	⊗

Upload file:

Once a new whitelist is created, it will be automatically displayed inside the Allowed File tab. It will also be available when creating or editing a Content Aware Protection or eDiscovery Policy.

6.11. File Location Whitelists

File Location Whitelists are custom defined lists of locations identified by Endpoint Protector. File transfers within this location are automatically allowed, regardless of the content inspection rules or permissions defined in various Policies. The list of locations is available under DLP Blacklists and Whitelists > Whitelists > File Location tab.



This feature is only available for Content Aware Protection. It applies at a global level, to all File Location Whitelist.

Include subfolders for File Location Whitelists: OFF

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Tony Downloads		C:\Users\Tony\Downloads	root	2017-04-18 15:01:11	root	2017-04-18 15:01:11	☰

Showing 1 to 1 of 1 entries

⚠ **Note**

In addition to defining the File Location Whitelist, the browser or application used to transfer files also needs to be selected from within the Content Aware Protection Policy.

⚙ **Tips**

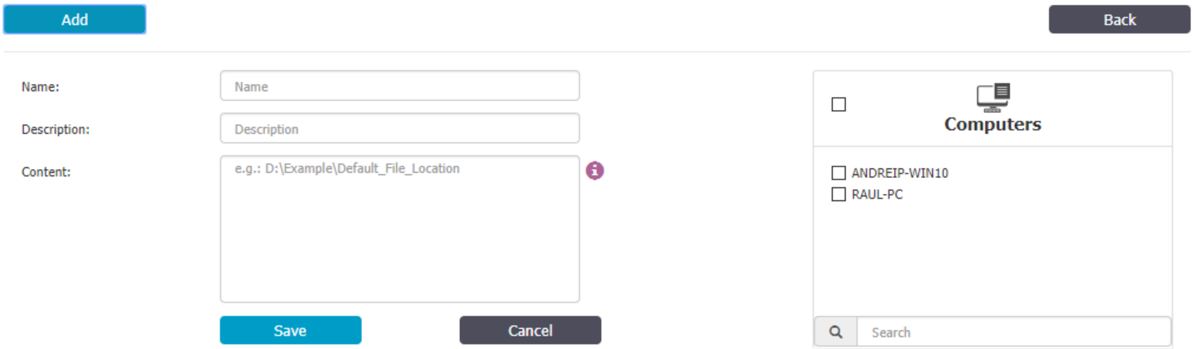
By default, the File Location Whitelists apply to all files located in the specific folder but also to any other files located in containing subfolders. While the "Include subfolders for File Location Whitelists" feature can be switched OFF, it will affect all other File Location Blacklists and Whitelists throughout the system.

Information

File Location Whitelists are available only for the Content Aware Protection module.

The available actions for each file name are: **Edit**, **Export** and **Delete**. 📝 ▦ ⊗

A new file location whitelist can be created by clicking the Add button. To populate the content of a newly created file location whitelist, items can be entered either manually (typed or pasted). The computers to which it applies also need to be selected from the list on the right side.



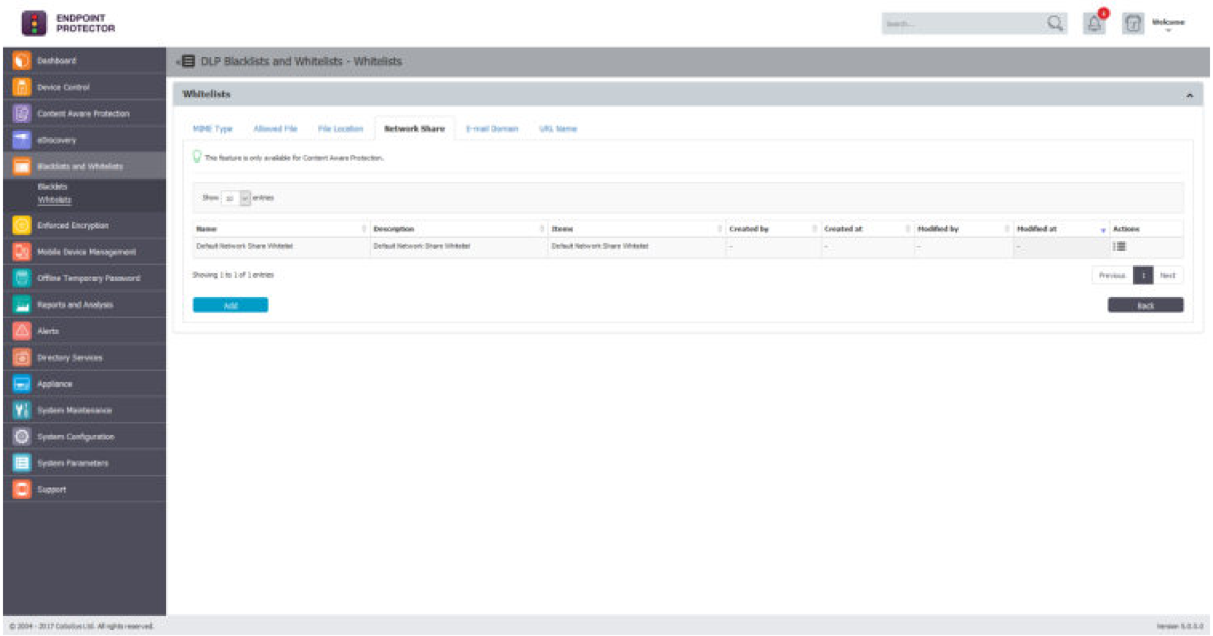
Name:	Name
Description:	Description
Content:	e.g.: D:\Example\Default_File_Location

□ Computers

□ ANDREIP-WIN10
□ RAUL-PC

6.12. Network Share Whitelists

Network Share Whitelists are custom defined lists of network share addresses where transfers of confidential information will be allowed by Endpoint Protector. The whitelisted network shares are available under DLP Blacklists and Whitelists > Whitelists > Network Share tab.



This feature is only available for Content Aware Protection.

Show 10 entries

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default Network Share Whitelist	Default Network Share Whitelist	Default Network Share Whitelist	-	-	-	-	☰

Showing 1 to 1 of 1 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

Information

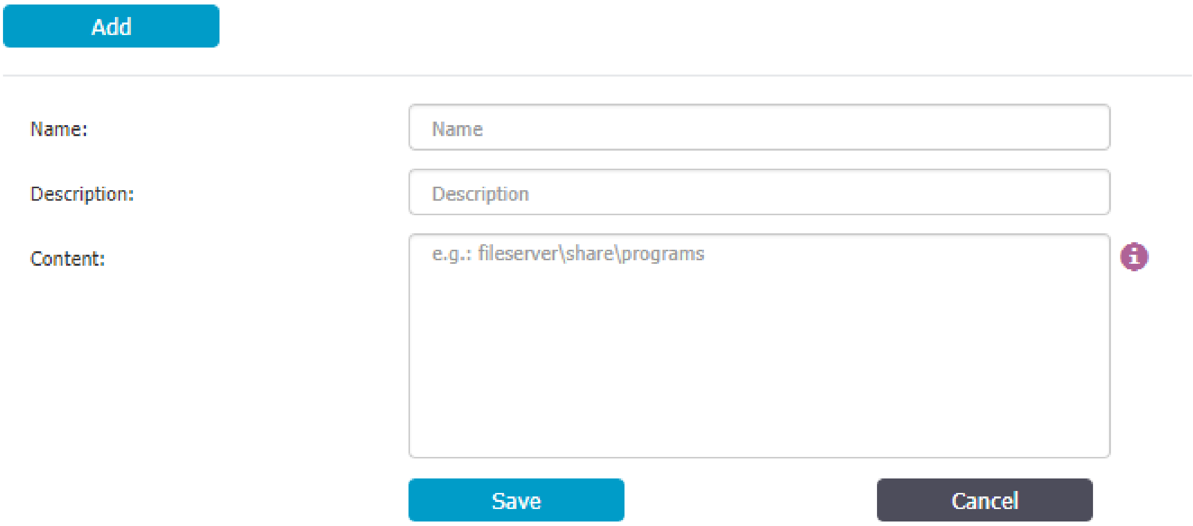
Network Share Whitelists are available only for the Content Aware Protection module.

Note

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 Protection Policy.

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

A new network share file whitelist can be created by clicking on the Add button. To populate the content of a newly created whitelist, the server name or IP address can be used to define a network share path.



⚠ **Note**

The network share path should not begin with backslashes (\\).

Example

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

Once a new whitelist is created, it will be automatically displayed inside the Network Share tab. It will also be available when creating or editing a Content Aware Protection Policy.

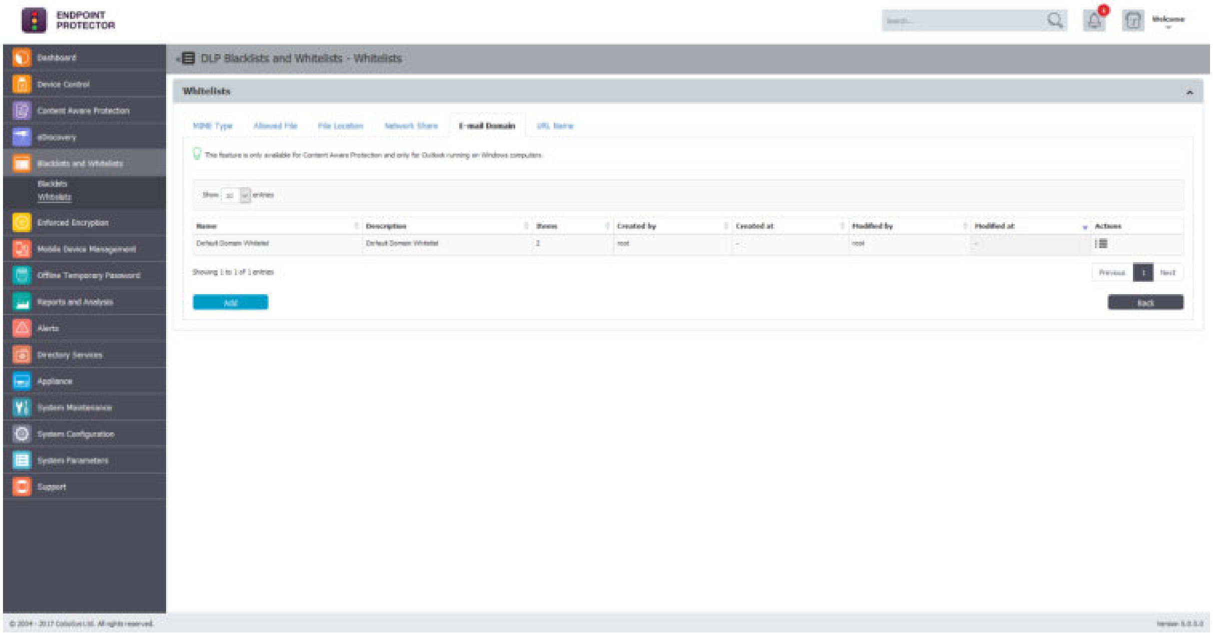
6.13. E-mail Domain Whitelists

⚠ **Note**

This feature is only available for Microsoft Outlook and IBM Lotus Notes for Windows computers. Outlook requires the related add-on to be deployed alongside the Endpoint Protector Client.

For more information, please read our FAQ.

E-mail Domain Whitelists are custom defined e-mail addresses to which sending of confidential information will be allowed by Endpoint Protector. The list of file URL names is available under DLP Blacklists and Whitelists > Whitelists > E-mail Domain tab.



DLP Blacklists and Whitelists - Whitelists

Whitelists

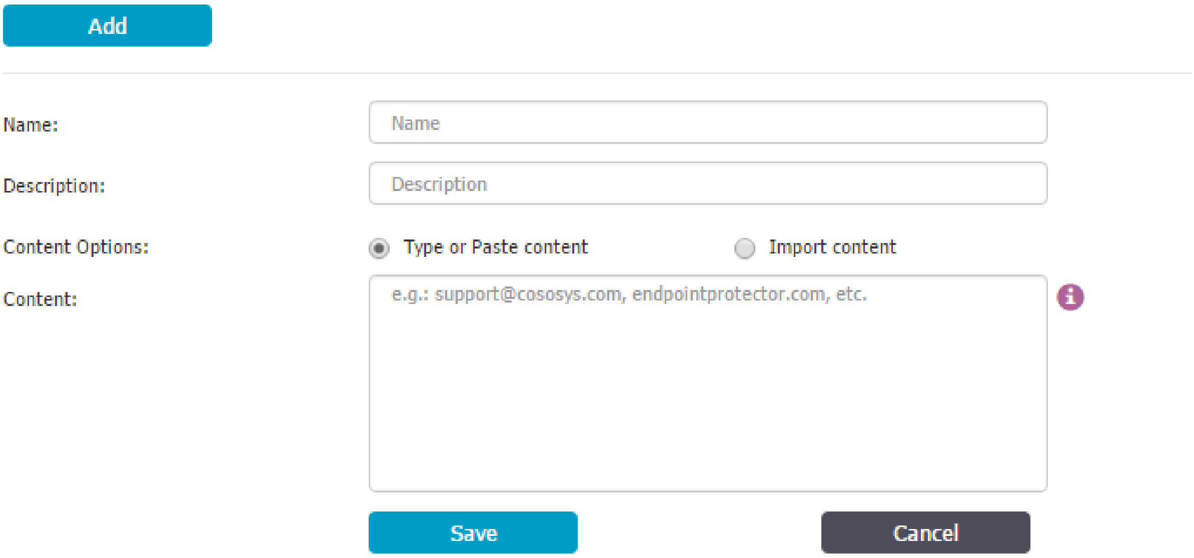
This feature is only available for Content Aware Protection and only for Outlook running on Windows computers.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default Domain Whitelist	Default Domain Whitelist	2	root	-	root	-	

Showing 1 to 1 of 1 entries

> **Information**
>
> E-mail Domain Whitelists are available only for the Content Aware Protection module.

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



Name:	Name
Description:	Description
Content Options:	● Type or Paste content ○ Import content
Content:	e.g.: support@cososys.com, endpointprotector.com, etc.

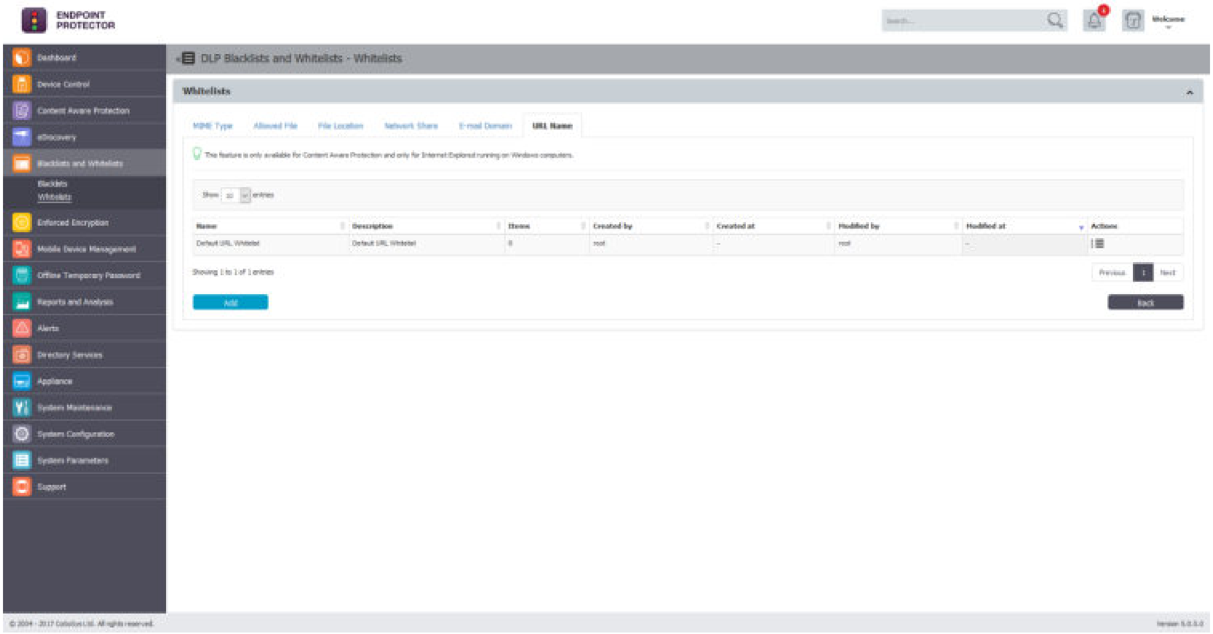
Once a new E-mail domain whitelist is added, it will be automatically displayed inside the E-mail Domain Whitelists tab. It will also be available when creating or editing a Content Aware Protection Policy.

6.14. URL Name Whitelists

Note

This feature is only available for Interned Explorer on Windows computers. It requires the related add-on to be deployed alongside the Endpoint Protector Client.

URL Name Whitelists are custom defined lists web addresses where uploading of confidential information will be allowed by Endpoint Protector. The list of file URL names is available under DLP Blacklists and Whitelists > Whitelists > URL Name tab.



This feature is only available for Content Aware Protection and only for Internet Explored running on Windows computers.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
Default URL Whitelist	Default URL Whitelist	8	root	-	root	-	

Showing 1 to 1 of 1 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

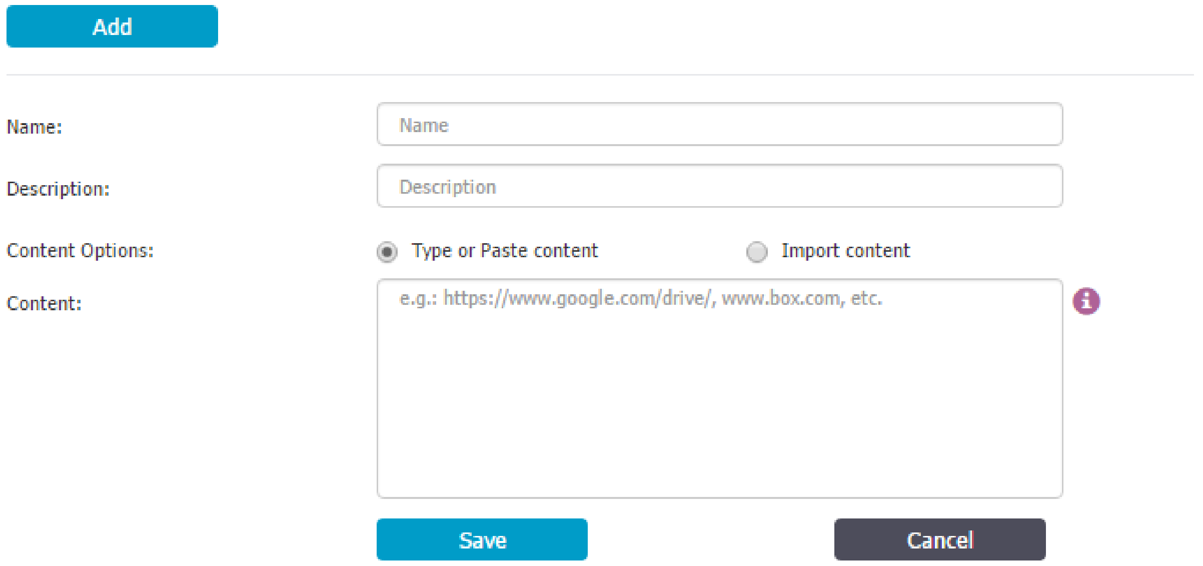
Version 5.0.5.0

Information

URL Name Whitelists are available only for the Content Aware Protection module.

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

A new URL name whitelist can be created by clicking the Add button. To populate the content of a newly created URL name whitelist, items of at least two characters can be entered either manually (typed or pasted) or imported.



Name: Name

Description: Description

Content Options: ● Type or Paste content ○ Import content

Content: e.g.: https://www.google.com/drive/, www.box.com, etc.

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

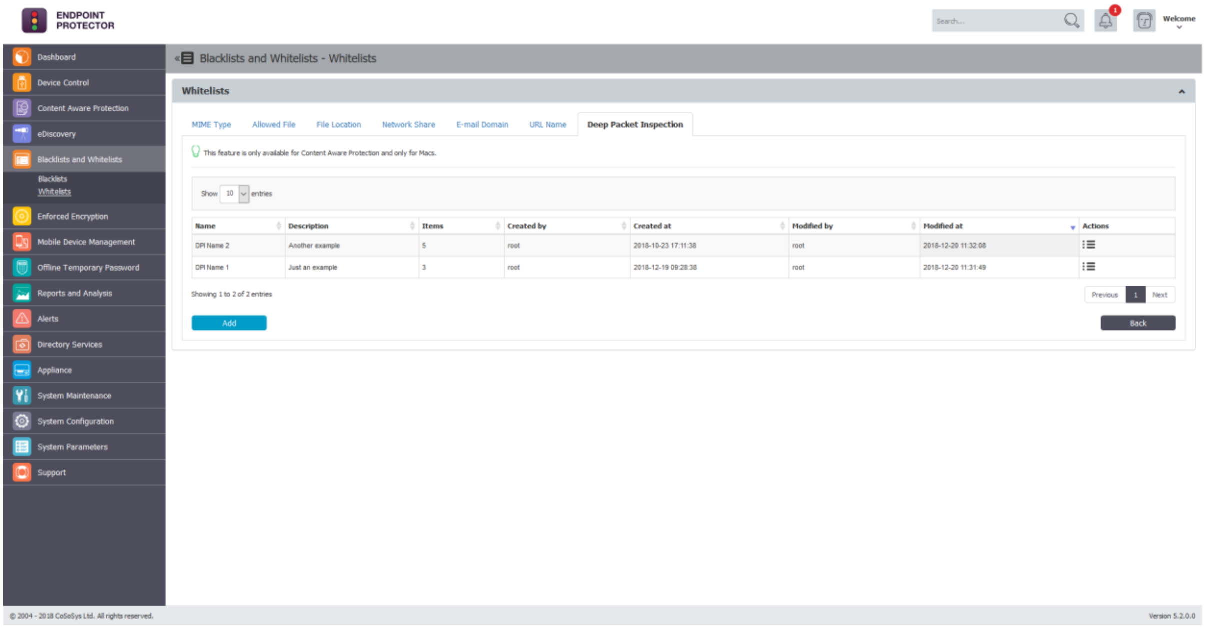
Example
endpointprotector.com (not www.endpointprotector.com)

Once a new URL name whitelist is added, it will be automatically displayed inside the URL Name Whitelists tab. It will also be available when creating or editing a Content Aware Protection Policy.

6.15. Deep Packet Inspection Whitelists

Note
This feature is only available for Macs.

Deep Packet Inspection Whitelists are custom defined lists web addresses where uploading of confidential information will be allowed by Endpoint Protector. The list of Deep Packet Inspection is available under DLP Blacklists and Whitelists > Whitelists > Deep Packet Inspection tab.



Blacklists and Whitelists - Whitelists

Whitelists

This feature is only available for Content Aware Protection and only for Macs.

Name	Description	Items	Created by	Created at	Modified by	Modified at	Actions
DPI Name 2	Another example	5	root	2018-10-23 17:11:38	root	2018-12-20 11:32:08	☰
DPI Name 1	Just an example	3	root	2018-12-19 09:28:38	root	2018-12-20 11:31:49	☰

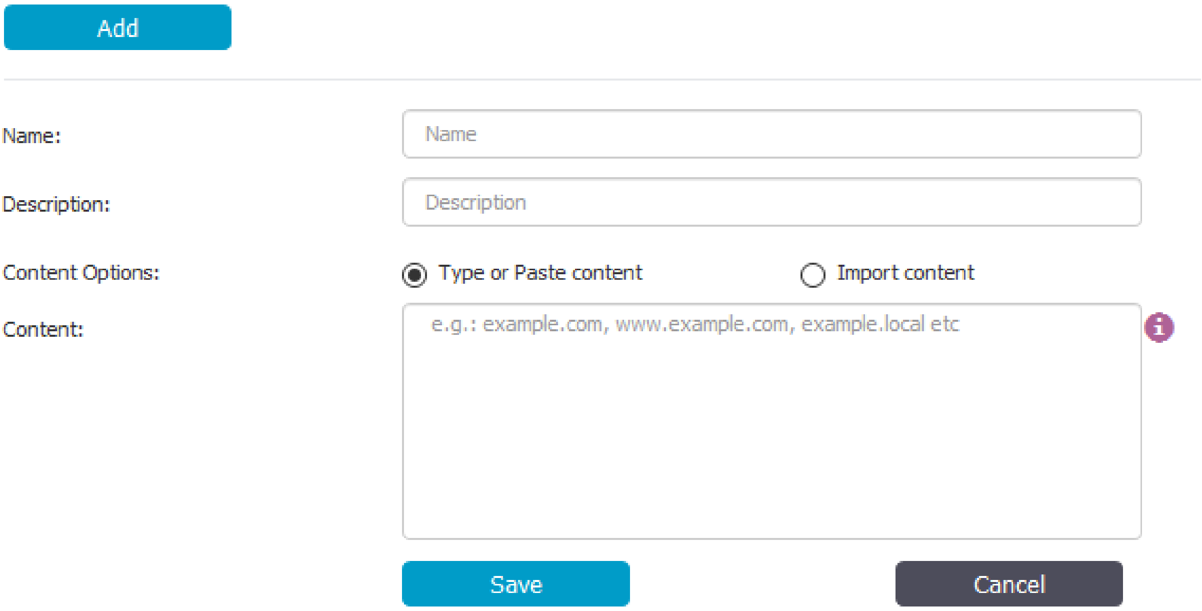
Showing 1 to 2 of 2 entries

Information

Deep Packet Inspection Whitelists are available only for the Content Aware Protection module.

The available actions for each deep packet inspection are: **Edit**, **Export** and **Delete**.

A new Deep Packet Inspection Whitelist can be created by clicking the Add button. To populate the content of a newly created Deep Packet Inspection whitelist, items of at least two characters can be entered either manually (typed or pasted) or imported.



Name:	Name
Description:	Description
Content Options:	● Type or Paste content ○ Import content
Content:	e.g.: example.com, www.example.com, example.local etc

⚙ **Example**

example.endpointprotector, *example.com, *example*, https://website.com, etc.

⚠ **Note**

“?” cannot be used to replace a character.

⚠ **Note**

Due to the way gmail works, depending on the desired outcome, the following needs to be considered:

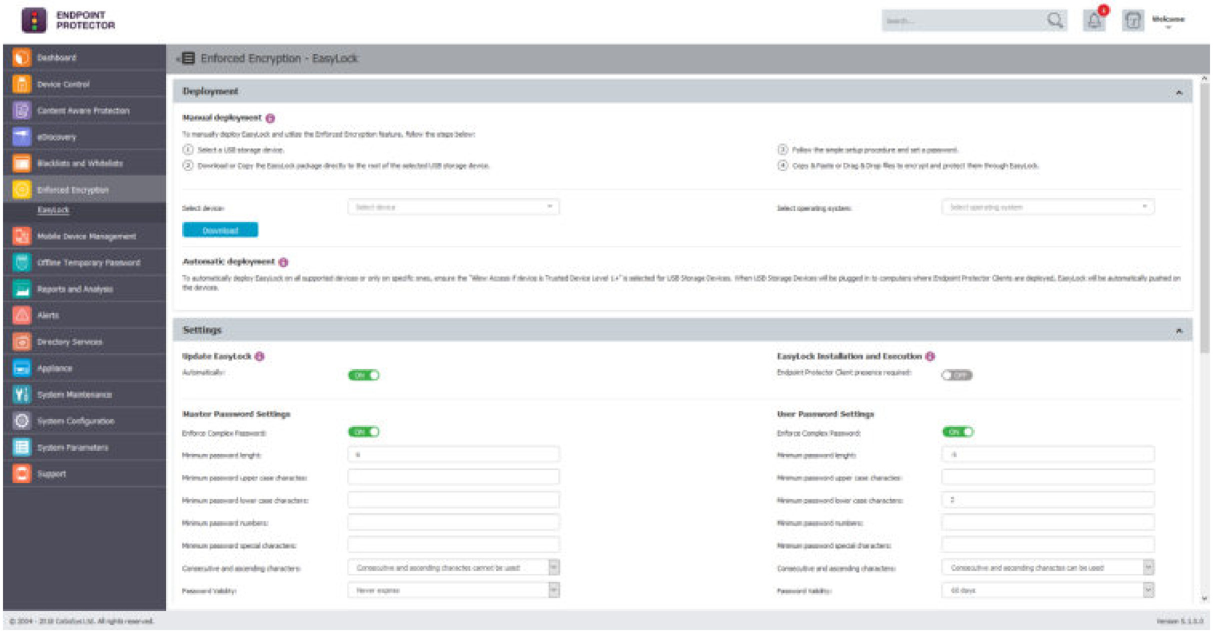
- Whitelisting mail.google.com will allow e-mail attachments or files that have been added using drag and drop
- Whitelisting doc.google.com will be needed when images are inserted in the body of the e-mail

Once a new Deep Packet Inspection whitelist is added, it will be automatically displayed inside the Deep Packet Inspection Whitelists tab. It will also be available when creating or editing a Content Aware Protection Policy.

7. Enforced Encryption

7.1. EasyLock

EasyLock is a cross-platform solution that protects data with government-approved 256bit AES CBC-mode encryption. For USB devices, it needs to be deployed on the root of the device. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device.



Deployment

Manual deployment

To manually deploy EasyLock and utilize the Enforced Encryption feature, follow the steps below:

1. Select a USB storage device.
2. Download or Copy the EasyLock package directly to the root of the selected USB storage device.
3. Follow the simple setup procedure and set a password.
4. Copy & Paste or Drag & Drop files to encrypt and protect them through EasyLock.

Select device: Select device

Select operating system: Select operating system

Automatic deployment

To automatically deploy EasyLock on all supported devices or only on specific ones, ensure the "Allow Access if device is Trusted Device Level 1+" is selected for USB Storage Devices. When USB Storage Devices will be plugged in to computers where Endpoint Protector Clients are deployed, EasyLock will be automatically pushed on the devices.

Settings

Update EasyLock

Automatically: ON

EasyLock Installation and Execution

Endpoint Protector Client presence required: OFF

Master Password Settings

Enforce Complex Password: ON
Minimum password lenght: 8
Minimum password upper case characters:
Minimum password lower case characters:
Minimum password numbers:
Minimum password special characters:
Consecutive and ascending characters: Consecutive and ascending characters cannot be used
Password Validity: Never expires

User Password Settings

Enforce Complex Password: ON
Minimum password lenght: 4
Minimum password upper case characters:
Minimum password lower case characters: 2
Minimum password numbers:
Minimum password special characters:
Consecutive and ascending characters: Consecutive and ascending characters can be used
Password Validity: 60 days

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.1.3.3

Information

For more details about using EasyLock itself, please reference the EasyLock User Manual.

Used in combination with Endpoint Protector, EasyLock allows USB storage devices to be identified as Trusted Devices Level 1. This can ensure that USB Enforced Encryption is used on protected computers. 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.

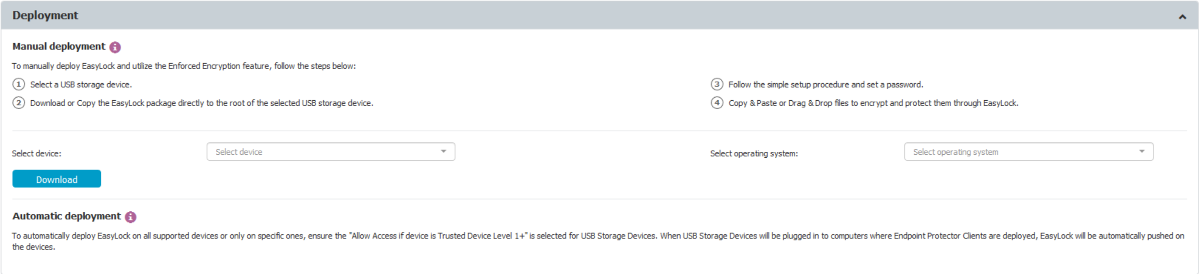
⚠ **Note**

While Endpoint Protector can detect any EasyLock USB encrypted device as a Trusted Device Level 1, to use the Enforced Encryption feature, a specific EasyLock version must be used. This is available for the Endpoint Protector User Interface.

7.1.1. EasyLock Deployment

Information

EasyLock Enforced Encryption is supported for both Mac and Windows computers.



Deployment

Manual deployment

To manually deploy EasyLock and utilize the Enforced Encryption feature, follow the steps below:

1. Select a USB storage device.
2. Download or Copy the EasyLock package directly to the root of the selected USB storage device.
3. Follow the simple setup procedure and set a password.
4. Copy & Paste or Drag & Drop files to encrypt and protect them through EasyLock.

Select device: Select device

Select operating system: Select operating system

Automatic deployment

To automatically deploy EasyLock on all supported devices or only on specific ones, ensure the "Allow Access if device is Trusted Device Level 1+" is selected for USB Storage Devices. When USB Storage Devices will be plugged in to computers where Endpoint Protector Clients are deployed, EasyLock will be automatically pushed on the devices.

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 Device Control > 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 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.

Tips

Starting with Endpoint Protector 5.2.0.0, manual deployment can also be made by the user if the device is set on **Allow Access**, by pressing the small USB icon- **Encrypt Device with EasyLock.**

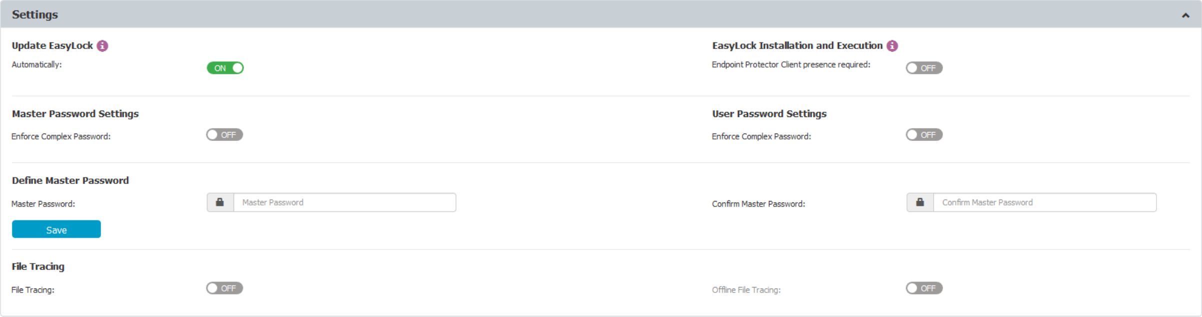
Both EasyLock deployments are straight forward and require the user only to configure a password.

Note

On Macs, USB storage devices with multiple partitions are not supported by EasyLock and Trusted Devices Level 1.

7.1.2. EasyLock Settings

This section allows the Administrator to remotely manage EasyLock encrypted devices. Before being able to take advantage of these features, the Administrator must configure a Master Password.



Settings

Update EasyLock

Automatically: ON

EasyLock Installation and Execution

Endpoint Protector Client presence required: OFF

Master Password Settings

Enforce Complex Password: OFF

User Password Settings

Enforce Complex Password: OFF

Define Master Password

Master Password: Master Password

Confirm Master Password: Confirm Master Password

Save

File Tracing

File Tracing: OFF

Offline File Tracing: OFF

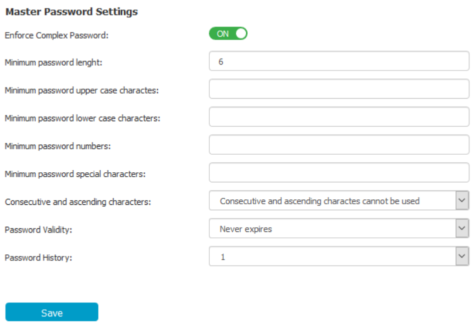
Information

EasyLock can be configured to be installed and run only in the presence of the Endpoint Protector Client, by enabling the Installation and Execution feature.

This functionality can be extended in order for EasyLock to work in relation to a list of trusted Endpoint Protector Servers by also enabling the EasyLock Multi Server feature.

In the Settings section, the Master Password can be configured, the EasyLock File Tracing enabled, as well as defining the installation and execution of EasyLock only on computers where the Endpoint Protector Client is present.

For both the Master Password and the User Password, complex rules can be enforced. If these are enabled, the password lengths, minimum characters, validity, history and other settings can be set.



Master Password Settings

Enforce Complex Password: ON

Minimum password lenght: 6

Minimum password upper case charactes:

Minimum password lower case characters:

Minimum password numbers:

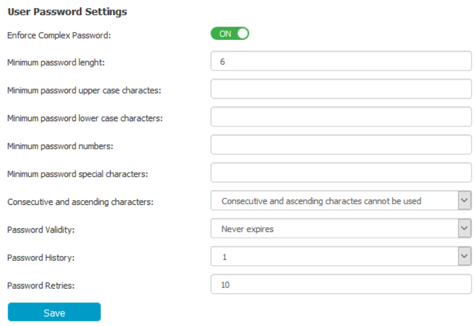
Minimum password special characters:

Consecutive and ascending characters: Consecutive and ascending charactes cannot be used

Password Validity: Never expires

Password History: 1

Save



User Password Settings

Enforce Complex Password: ON

Minimum password lenght: 6

Minimum password upper case charactes:

Minimum password lower case characters:

Minimum password numbers:

Minimum password special characters:

Consecutive and ascending characters: Consecutive and ascending charactes cannot be used

Password Validity: Never expires

Password History: 1

Password Retries: 10

Save

Endpoint Protector 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.

File Tracing

File Tracing: OFF

Offline File Tracing: OFF

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.

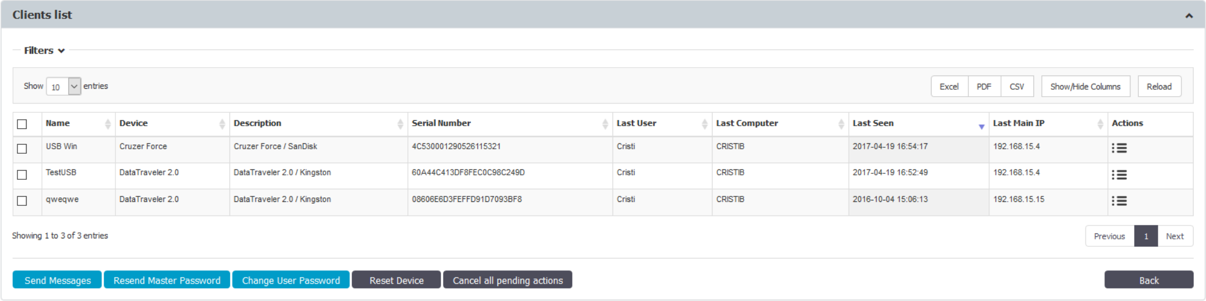
Additionally, Easy Lock performs File Shadowing for the files that are transferred, if Endpoint Protector Client is present and the File Shadowing option is enabled on the computer on which the events occur – through the Device Control module. This is a real-time event and no shadowing information is 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.

7.1.3. EasyLock Clients

In the Clients list 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.



□	Name	Device	Description	Serial Number	Last User	Last Computer	Last Seen	Last Main IP	Actions
□	USB Win	Cruzer Force	Cruzer Force / SanDisk	4C530001290526115321	Cristi	CRISTIB	2017-04-19 16:54:17	192.168.15.4	☰
□	TestUSB	DataTraveler 2.0	DataTraveler 2.0 / Kingston	60A44C413DF8FEC0C98C249D	Cristi	CRISTIB	2017-04-19 16:52:49	192.168.15.4	☰
□	qweqwe	DataTraveler 2.0	DataTraveler 2.0 / Kingston	08606E6D3FEFFD91D7093BF8	Cristi	CRISTIB	2016-10-04 15:06:13	192.168.15.15	☰

Showing 1 to 3 of 3 entries

8. Mobile Device Management

In the last past years, mobile devices have invaded business environments. Personally owned or company owned smartphones and tablets are used on a daily basis by employees to store and have access to their company e-mails, sales reports etc. everywhere they go.

The wide adoption of the BYOD (Bring-Your-Own-Device) model by companies worldwide led to the use of more personal mobile devices by employees for storing business information together with private data such as photos and music. This trend raised new issues for IT administrators, which are faced now with the challenge of protecting sensitive company data not only inside the secured company network, but also everywhere it is taken on mobile company endpoints. At the same time, a separation and close monitoring of company information from personal data must be imposed.

To face the security challenges by the increase mobility in business environments, Mobile Device Management by Endpoint Protector enables a complete control and detailed monitoring over the use of mobile devices both inside and outside corporate environments, allowing employees to have a secure access to both corporate and private data wherever they are and on whatever device they are using without business critical information getting compromised.

Information

Endpoint Protector is a complete Data Loss Prevention and Enterprise Mobility Management solution. While the DLP related features and functionality are explained in this user manual, please reference the MDM User Manual for information related to smartphones and tablets. Additional information regarding deployment of the Endpoint Protector Server can be found in the Virtual and Hardware Appliance User Manual.

9. Offline Temporary Password

This section allows the Administrator to generate Offline Temporary Passwords (or OTPs) and grant temporary access rights. In addition to situations when only temporary access is needed, it can also be used when there is no network connection between the protected computers and the Endpoint Protector Server. The Offline Temporary Password can be generated for the below entities:

- Device (a specific device)
- Computer and User (all devices)
- Computer and User (all file transfers)

A password is linked to a time period and is unique for a certain device and computer. This means the same password cannot be used for a different device or computer. It also cannot be used twice (except for Universal Offline Temporary Password). The time intervals available are: 15 minutes, 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days and 30 days or Custom.

Information

The Offline Temporary Password Duration offers a customized option, allowing the generation of time-based OTP Codes, with a Start Date/Time and an End Date/Time.

For large companies or multinational that have the Endpoint Protector Server and the protected endpoints on different time zones, taking into consideration how the Server Time and Client Time work is essential.

Example

The Endpoint Protector Server is located in Germany, making the Server Time UTC+01:00

The protected endpoints are located in Romania, making the Client Time UTC+02:00

When generating an OTP Code that should take affect tomorrow, from 16:00 on the endpoint time, it should actually be generated for tomorrow, from 15:00 (to adjust for the 1h difference in the time zone)

For the predefined durations, the above adjustment is not necessary. The OTP Code will be valid for that specific amount of time, starting with the moment it was redeemed. The only thing to consider is that the OTP Code needs to be redeemed the same day it was generated.

Note

The Universal Offline Temporary Password feature can also be turned on. If enabled, it can be used by any user, on any computer, for any device or file transfers – it eliminates security restrictions for one hour. It can be used multiple times, by any users that knows it.

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.

Information

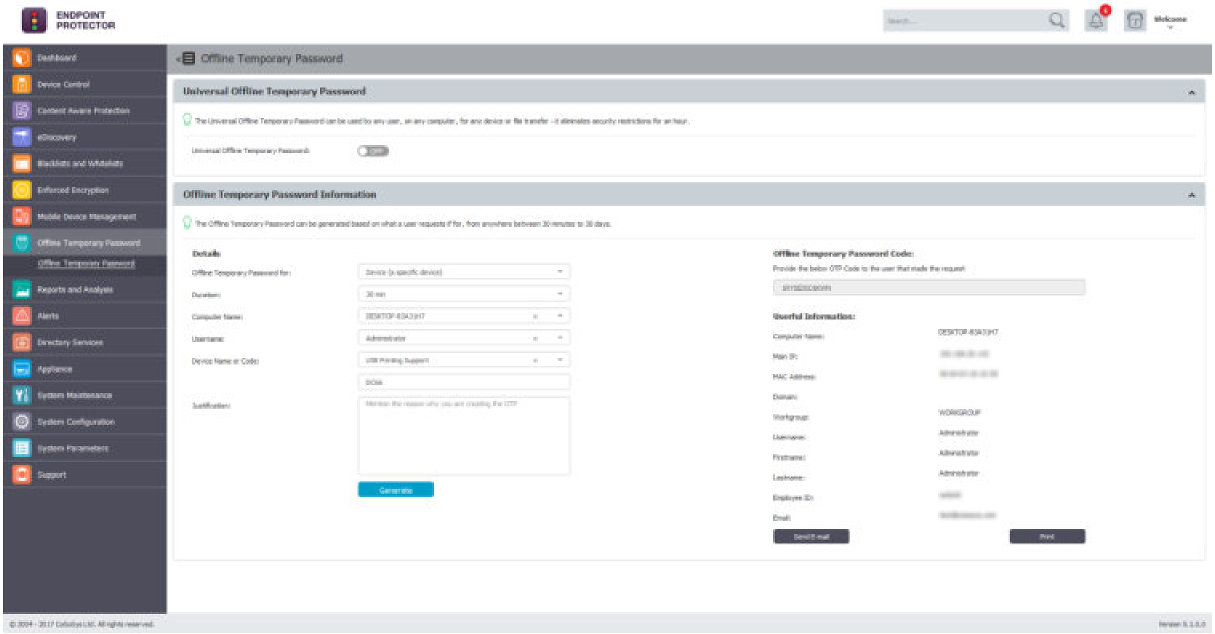
Once an Offline Temporary Password has been authorized, any other rights and settings saved afterwards on the Endpoint Protector Server will not take immediate effect. The Offline Temporary Password has to expire and the connection with the Server re-established.

Note

The Transfer Limit Reached Offline Temporary Password is only available if the Transfer Limit Reached feature is enabled and the actions are set to Lockdown. The main purpus of this type of Offline Temporary Password is to re-establish the Server-Client communication before the Transfer Limit Reached Time Interval has expired.

9.1. 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 an exact device, all devices or all file transfers.



Offline Temporary Password

Universal Offline Temporary Password

The Universal Offline Temporary Password can be used by any user, on any computer, for any device or file transfer - it eliminates security restrictions for an hour.

Universal Offline Temporary Password: OFF

Offline Temporary Password Information

The Offline Temporary Password can be generated based on what a user requests if for, from anywhere between 30 minutes to 30 days.

Details

Offline Temporary Password for:	Device (a specific device)
Duration:	30 min
Computer Name:	DESKTOP-83A3IH7
Username:	Administrator
Device Name or Code:	USB Printing Support
	DC66
Justification:	Mention the reason why you are creating the OTP

Offline Temporary Password Code:

Provide the below OTP Code to the user that made the request

Useful Information:

Computer Name:	DESKTOP-83A3IH7
Main IP:	
MAC Address:	
Domain:	
Workgroup:	WORKGROUP
Username:	Administrator
Firstname:	Administrator
Lastname:	Administrator
Employee ID:	
Email:	

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.1.0.0

When generating an Offline Temporary Password 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.

Tips

Another way to generate an Offline Temporary Password is directly from the Device Control > Computers section, and selecting the Offline Temporary Password option form the Actions column.

Information

When generating an OTP Code for a device, either the Device Code or the Device Name has to be entered (one of them will automatically fill in the other field).

The Computer Name and the Username fields do not need to be both filled in. The OTP Code is perfectly valid if only one of them is provided. However, if the OTP Code needs to be valid for an exact device, on an exact computer, for an exact user, all of the relevant fields need to be filled in.

Once the OTP Code has been generated, it will be displayed as per the right side of the image above.

As it needs to be provided to the person that made the request, Endpoint Protector offers two quick ways of doing this, either by sending a direct e-mail or by printing it out.

Information

For more details about how and Offline Temporary Password can be redeemed, please see chapter 17.4.1 Requesting and redeeming an Offline Temporary Password.

Note

The Administrator contact information that are displayed to a user can be edited under System Configuration > System Settings, as the Main Administrator Contact Details.

Information

Similar to generating an Offline Temporary Password for a specific device, when generating one for all devices or all file transfer, the Computer Name and the Username fields are not both mandatory. The OTP Code is perfectly valid if only one of them is provided. However, if the OTP Code needs to be valid for an exact computer and an exact user, all of the relevant fields need to be filled in.

10. Reports and Analysis

This section offers the administrator an overview of the System Logs, Device Control Logs and Shadows and Content Aware Logs and Shadows. In addition, Admin Actions, Statistics and other helpful information can be view from this section.

Details regarding eDiscovery Scans and EasyLock Enforced Encryption can be viewed in their own specific sections and not in the Reports and Analysis section.

Information

As an additional data security measure, this section may be protected by an additional password set by the Super Administrator. This can be set from System Configuration > System Security.

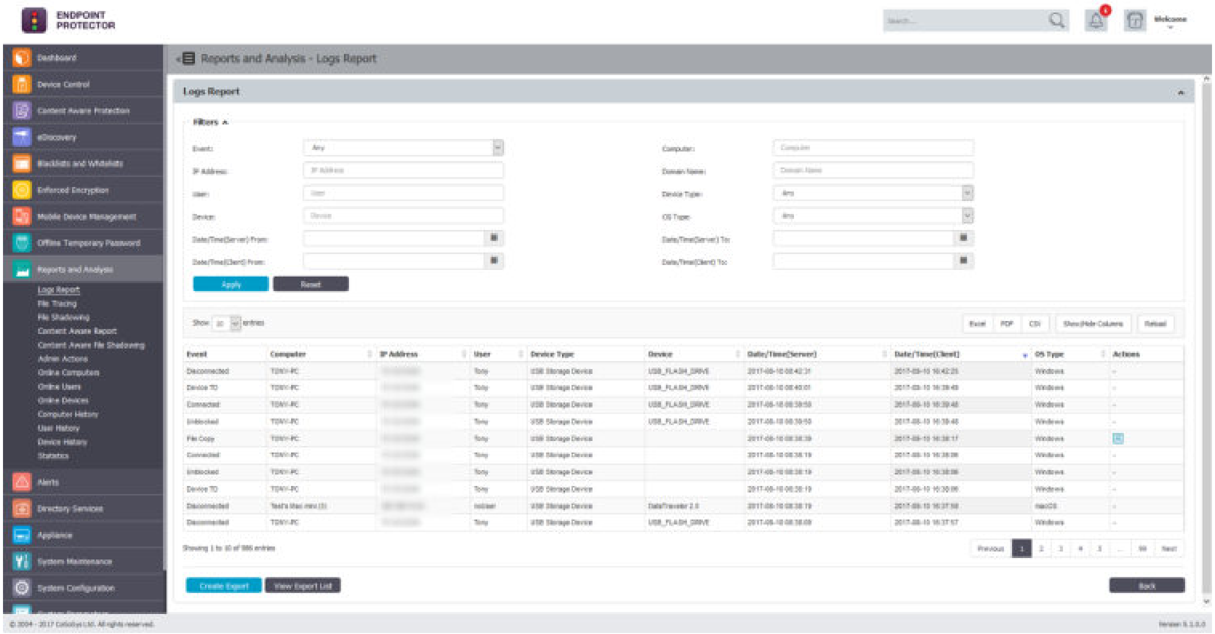
For more details about System Security, please see chapter 15.7 System Security.

10.1. Log Report

This section offers the administrator an overview of the main logs in the system. There are several event types such as User Login, User Logout, AD Import, AD Synchronization, Uninstall Attempt, etc., included in this section. Additionally, the main Device Control logs can be viewed from this section.

Tips

For a complete list of the log types included in this section, please use the Event drop-down available in the Filters part of this page.



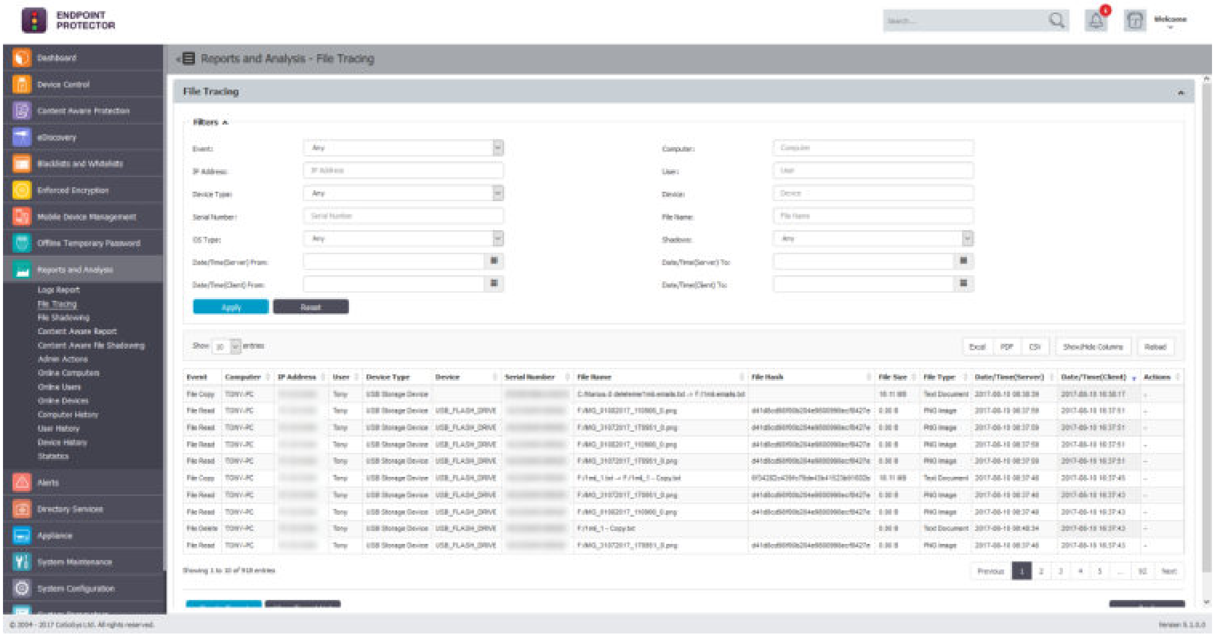
Event	Computer	IP Address	User	Device Type	Device	Date/Time(Server)	Date/Time(Client)	OS Type	Actions
Disconnected	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	2017-08-10 08:42:31	2017-08-10 16:42:25	Windows	-
Device TD	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	2017-08-10 08:40:01	2017-08-10 16:39:49	Windows	-
Connected	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	2017-08-10 08:39:50	2017-08-10 16:39:48	Windows	-
Unblocked	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	2017-08-10 08:39:50	2017-08-10 16:39:48	Windows	-
File Copy	TONY-PC	[redacted]	Tony	USB Storage Device		2017-08-10 08:38:39	2017-08-10 16:38:17	Windows	
Connected	TONY-PC	[redacted]	Tony	USB Storage Device		2017-08-10 08:38:19	2017-08-10 16:38:06	Windows	-
Unblocked	TONY-PC	[redacted]	Tony	USB Storage Device		2017-08-10 08:38:19	2017-08-10 16:38:06	Windows	-
Device TD	TONY-PC	[redacted]	Tony	USB Storage Device		2017-08-10 08:38:19	2017-08-10 16:38:06	Windows	-
Disconnected	Test's Mac mini (3)	[redacted]	noUser	USB Storage Device	DataTraveler 2.0	2017-08-10 08:38:19	2017-08-10 16:37:58	macOS	-
Disconnected	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	2017-08-10 08:38:09	2017-08-10 16:37:57	Windows	-

Showing 1 to 10 of 986 entries

The administrator has the possibility of exporting either the search results (as an Excel, PDF or CSV) or to Create and Export containing the entire log report as a .CSV file.

10.2. File Tracing

This section offers the administrator an overview on traced files that have been transferred from a protected computer to a portable device or to another computer on the network, and vice versa.



Event	Computer	IP Address	User	Device Type	Device	Serial Number	File Name	File Hash	File Size	File Type	Date/Time(Server)	Date/Time(Client)	Actions
File Copy	TONY-PC	[redacted]	Tony	USB Storage Device		[redacted]	C:\Marius.2.deleteme\1mb.emails.txt -> F:\1mb.emails.txt		10.11 MB	Text Document	2017-08-10 08:38:39	2017-08-10 16:38:17	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31082017_110900_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:59	2017-08-10 16:37:51	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31072017_175951_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:59	2017-08-10 16:37:51	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31082017_110900_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:59	2017-08-10 16:37:51	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31072017_175951_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:59	2017-08-10 16:37:51	-
File Copy	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\1mb_1.txt -> F:\1mb_1 - Copy.txt	6f04282ca4394c7fbde43b41623b91930e	10.11 MB	Text Document	2017-08-10 08:37:48	2017-08-10 16:37:45	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31072017_175951_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:48	2017-08-10 16:37:43	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31082017_110900_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:48	2017-08-10 16:37:43	-
File Delete	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\1mb_1 - Copy.txt		0.00 B	Text Document	2017-08-10 08:48:34	2017-08-10 16:37:43	-
File Read	TONY-PC	[redacted]	Tony	USB Storage Device	USB_FLASH_DRIVE	[redacted]	F:\IMG_31072017_175951_0.png	d41d8cd98f00b204e9800998ecf8427e	0.00 B	PNG image	2017-08-10 08:37:48	2017-08-10 16:37:43	-

Showing 1 to 10 of 918 entries

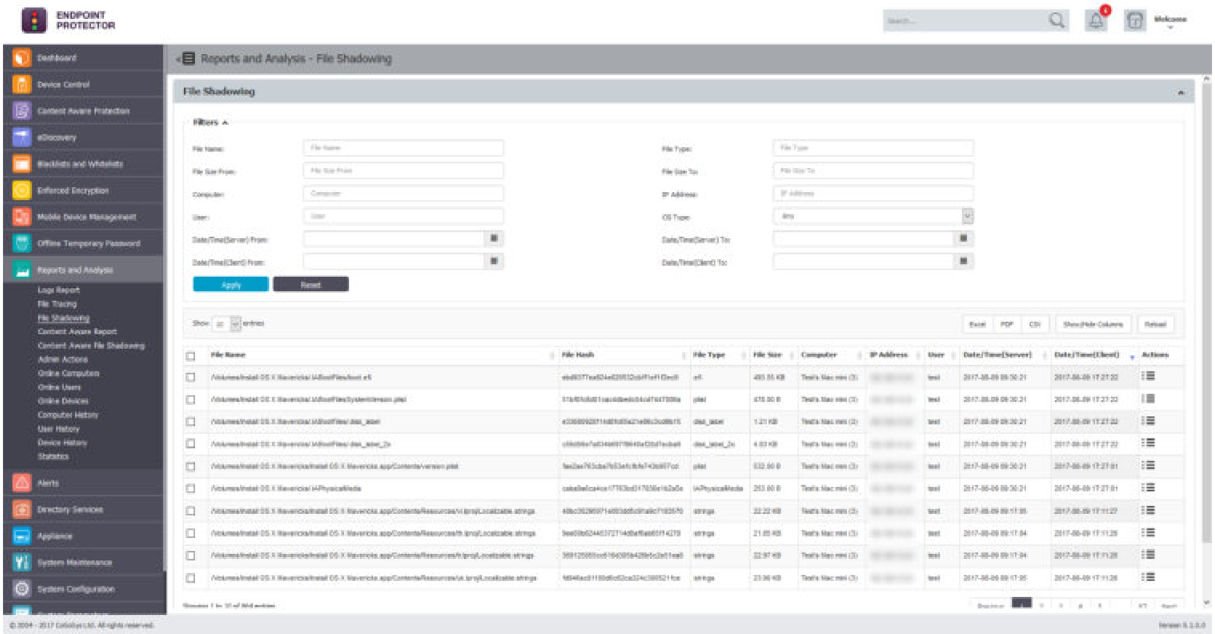
Information

A special mention is given here to the "File Hash" column. Endpoint Protector 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.

The administrator has the possibility of exporting either the search results (as an Excel, PDF or CSV) or to Create and Export containing the entire log report as a .CSV file.

10.3. File Shadowing

This section offers the administrator an overview on shadowed files that have been transferred from a protected computer to a portable device.



File Name:	File Name
File Type:	File Type
File Size From:	File Size From
File Size To:	File Size To
Computer:	Computer
IP Address:	IP Address
User:	User
OS Type:	Any
Date/Time(Server) From:	
Date/Time(Server) To:	
Date/Time(Client) From:	
Date/Time(Client) To:	

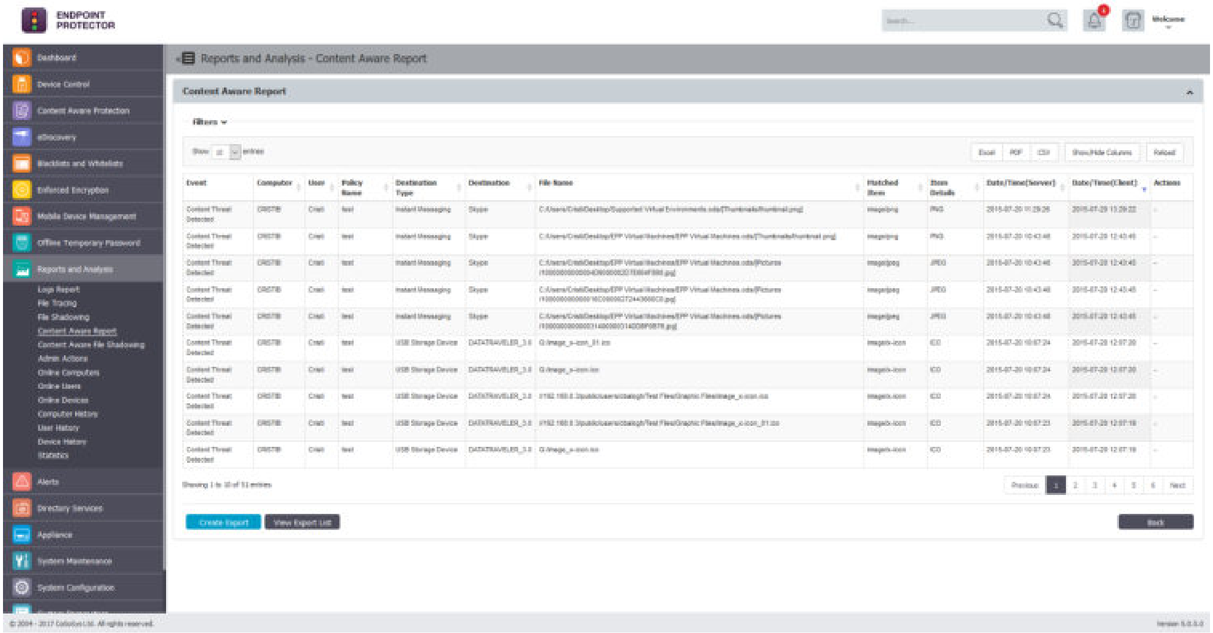
Show 10 entries

□	File Name	File Hash	File Type	File Size	Computer	IP Address	User	Date/Time(Server)	Date/Time(Client)	Actions
□	/Volumes/Install OS X Mavericks/.IABootFiles/boot.efi	[illegible]	efi	493.55 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:22	☰
□	/Volumes/Install OS X Mavericks/.IABootFiles/SystemVersion.plist	[illegible]	plist	478.00 B	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:22	☰
□	/Volumes/Install OS X Mavericks/.IABootFiles/.disk_label	[illegible]	disk_label	1.21 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:22	☰
□	/Volumes/Install OS X Mavericks/.IABootFiles/.disk_label_2x	[illegible]	disk_label_2x	4.83 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:22	☰
□	/Volumes/Install OS X Mavericks/Install OS X Mavericks.app/Contents/version.plist	[illegible]	plist	532.00 B	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:01	☰
□	/Volumes/Install OS X Mavericks/.IAPhysicalMedia	[illegible]	IAPhysicalMedia	253.00 B	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:30:21	2017-08-09 17:27:01	☰
□	/Volumes/Install OS X Mavericks/Install OS X Mavericks.app/Contents/Resources/vi.lproj/Localizable.strings	[illegible]	strings	22.22 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:17:35	2017-08-09 17:11:27	☰
□	/Volumes/Install OS X Mavericks/Install OS X Mavericks.app/Contents/Resources/th.lproj/Localizable.strings	[illegible]	strings	21.85 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:17:34	2017-08-09 17:11:28	☰
□	/Volumes/Install OS X Mavericks/Install OS X Mavericks.app/Contents/Resources/fr.lproj/Localizable.strings	[illegible]	strings	22.97 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:17:34	2017-08-09 17:11:28	☰
□	/Volumes/Install OS X Mavericks/Install OS X Mavericks.app/Contents/Resources/uk.lproj/Localizable.strings	[illegible]	strings	23.36 KB	Test's Mac mini (3)	[redacted]	test	2017-08-09 09:17:35	2017-08-09 17:11:28	☰

Showing 1 to 10 of [illegible] entries

10.4. Content Aware Report

This section offers the administrator an overview of the Content Aware Logs in the system. It allows the administrator to see exactly what data incidents were detected corresponding to the Content Aware Policies applied.



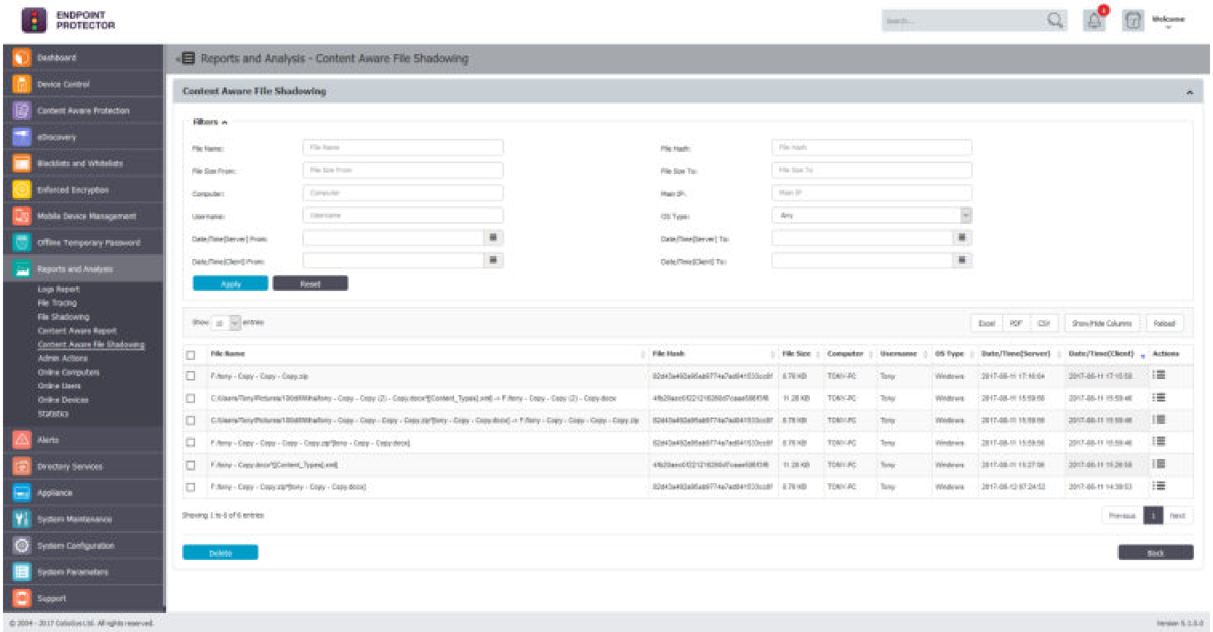
Event	Computer	User	Policy Name	Destination Type	Destination	File Name	Matched Item	Item Details	Date/Time(Server)	Date/Time(Client)	Actions
Content Threat Detected	CRISTIB	Cristi	test	Instant Messaging	Skype	C:/Users/Cristi/Desktop/Supported Virtual Environments.odt/[Thumbnails/thumbnail.png]	image/png	PNG	2015-07-20 11:29:26	2015-07-20 13:29:22	-
Content Threat Detected	CRISTIB	Cristi	test	Instant Messaging	Skype	C:/Users/Cristi/Desktop/EPP Virtual Machines/EPP Virtual Machines.odt/[Thumbnails/thumbnail.png]	image/png	PNG	2015-07-20 10:43:48	2015-07-20 12:43:45	-
Content Threat Detected	CRISTIB	Cristi	test	Instant Messaging	Skype	C:/Users/Cristi/Desktop/EPP Virtual Machines/EPP Virtual Machines.odt/[Pictures/10000000000004090000022715804F8B8.jpg]	image/jpeg	JPEG	2015-07-20 10:43:46	2015-07-20 12:43:45	-
Content Threat Detected	CRISTIB	Cristi	test	Instant Messaging	Skype	C:/Users/Cristi/Desktop/EPP Virtual Machines/EPP Virtual Machines.odt/[Pictures/10000000000001EC0000027244300C0.jpg]	image/jpeg	JPEG	2015-07-20 10:43:46	2015-07-20 12:43:45	-
Content Threat Detected	CRISTIB	Cristi	test	Instant Messaging	Skype	C:/Users/Cristi/Desktop/EPP Virtual Machines/EPP Virtual Machines.odt/[Pictures/10000000000003140000031400BF0878.jpg]	image/jpeg	JPEG	2015-07-20 10:43:48	2015-07-20 12:43:45	-
Content Threat Detected	CRISTIB	Cristi	test	USB Storage Device	DATATRAVELER_3.0	G:/image_x-icon_01.ico	image/x-icon	ICO	2015-07-20 10:07:24	2015-07-20 12:07:20	-
Content Threat Detected	CRISTIB	Cristi	test	USB Storage Device	DATATRAVELER_3.0	G:/image_x-icon.ico	image/x-icon	ICO	2015-07-20 10:07:24	2015-07-20 12:07:20	-
Content Threat Detected	CRISTIB	Cristi	test	USB Storage Device	DATATRAVELER_3.0	//192.168.0.3/public/users/cbalogh/Test Files/Graphic Files/image_x-icon.ico	image/x-icon	ICO	2015-07-20 10:07:24	2015-07-20 12:07:20	-
Content Threat Detected	CRISTIB	Cristi	test	USB Storage Device	DATATRAVELER_3.0	//192.168.0.3/public/users/cbalogh/Test Files/Graphic Files/image_x-icon_01.ico	image/x-icon	ICO	2015-07-20 10:07:23	2015-07-20 12:07:18	-
Content Threat Detected	CRISTIB	Cristi	test	USB Storage Device	DATATRAVELER_3.0	G:/image_x-icon.ico	image/x-icon	ICO	2015-07-20 10:07:23	2015-07-20 12:07:18	-

Showing 1 to 10 of 51 entries

The administrator has the possibility of exporting either the search results (as an Excel, PDF or CSV) or to Create and Export containing the entire log report as a .CSV file.

10.5. Content Aware File Shadowing

This section offers the administrator an overview on shadowed files that have been detected by a Content Aware Policy.



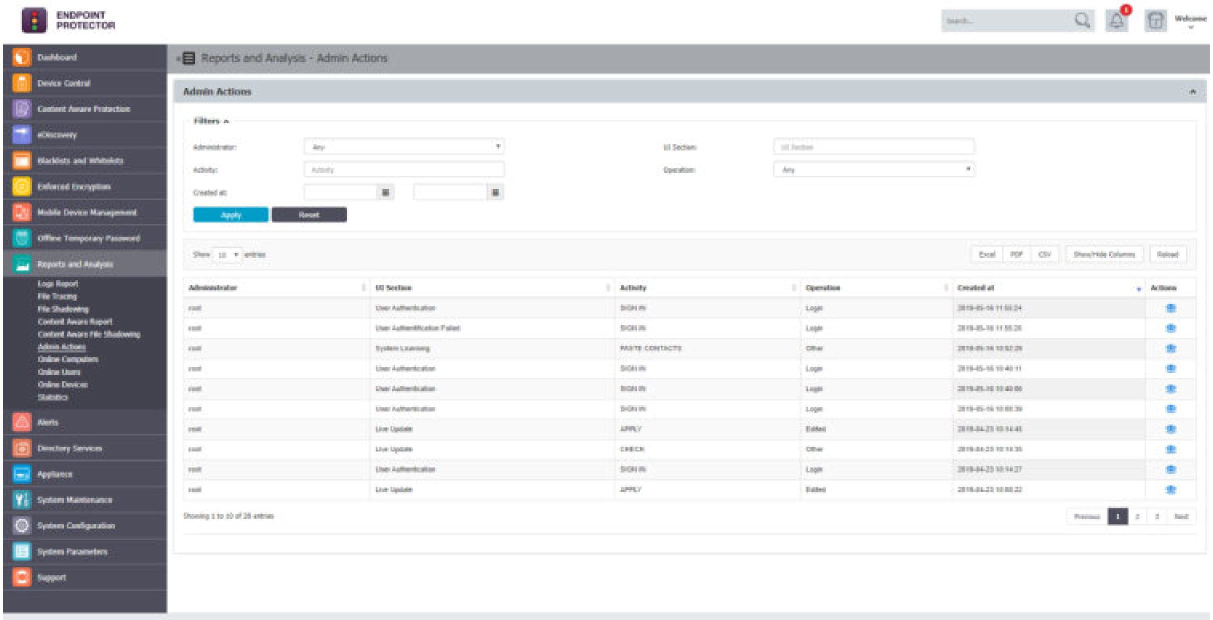
File Name:	File Name	File Hash:	File Hash
File Size From:	File Size From	File Size To:	File Size To
Computer:	Computer	Main IP:	Main IP
Username:	Username	OS Type:	Any
Date/Time(Server) From:		Date/Time(Server) To:	
Date/Time(Client) From:		Date/Time(Client) To:	

□	File Name	File Hash	File Size	Computer	Username	OS Type	Date/Time(Server)	Date/Time(Client)	Actions
□	F:/tony - Copy - Copy - Copy.zip	82d43a492a95ab9774a7ad841533cdbf	8.78 KB	TONY-PC	Tony	Windows	2017-08-11 17:16:04	2017-08-11 17:15:58	☰
□	C:/Users/Tony/Pictures/1308598/tony - Copy - Copy (2) - Copy.docx*[Content_Types].xml] -> F:/tony - Copy - Copy (2) - Copy.docx	4fb20aec0f2212182b0d7caae586f3f6	11.28 KB	TONY-PC	Tony	Windows	2017-08-11 15:59:58	2017-08-11 15:59:48	☰
□	C:/Users/Tony/Pictures/1308598/tony - Copy - Copy - Copy - Copy.zip*[tony - Copy - Copy.docx] -> F:/tony - Copy - Copy - Copy - Copy.zip	82d43a492a95ab9774a7ad841533cdbf	8.78 KB	TONY-PC	Tony	Windows	2017-08-11 15:59:58	2017-08-11 15:59:48	☰
□	F:/tony - Copy - Copy - Copy - Copy.zip*[tony - Copy - Copy.docx]	82d43a492a95ab9774a7ad841533cdbf	8.78 KB	TONY-PC	Tony	Windows	2017-08-11 15:59:58	2017-08-11 15:59:48	☰
□	F:/tony - Copy.docx*[Content_Types].xml]	4fb20aec0f2212182b0d7caae586f3f6	11.28 KB	TONY-PC	Tony	Windows	2017-08-11 15:27:08	2017-08-11 15:26:58	☰
□	F:/tony - Copy - Copy.zip*[tony - Copy - Copy.docx]	82d43a492a95ab9774a7ad841533cdbf	8.78 KB	TONY-PC	Tony	Windows	2017-08-12 07:24:52	2017-08-11 14:38:53	☰

Showing 1 to 6 of 6 entries

10.6. Admin Actions

This section offers the administrator an overview on every important action performed in the interface. The Action column offers the option to view additional information on each action.



Reports and Analysis - Admin Actions

Admin Actions

Filters

Administrator: Any

UI Section: UI Section

Activity: Activity

Operation: Any

Created at:

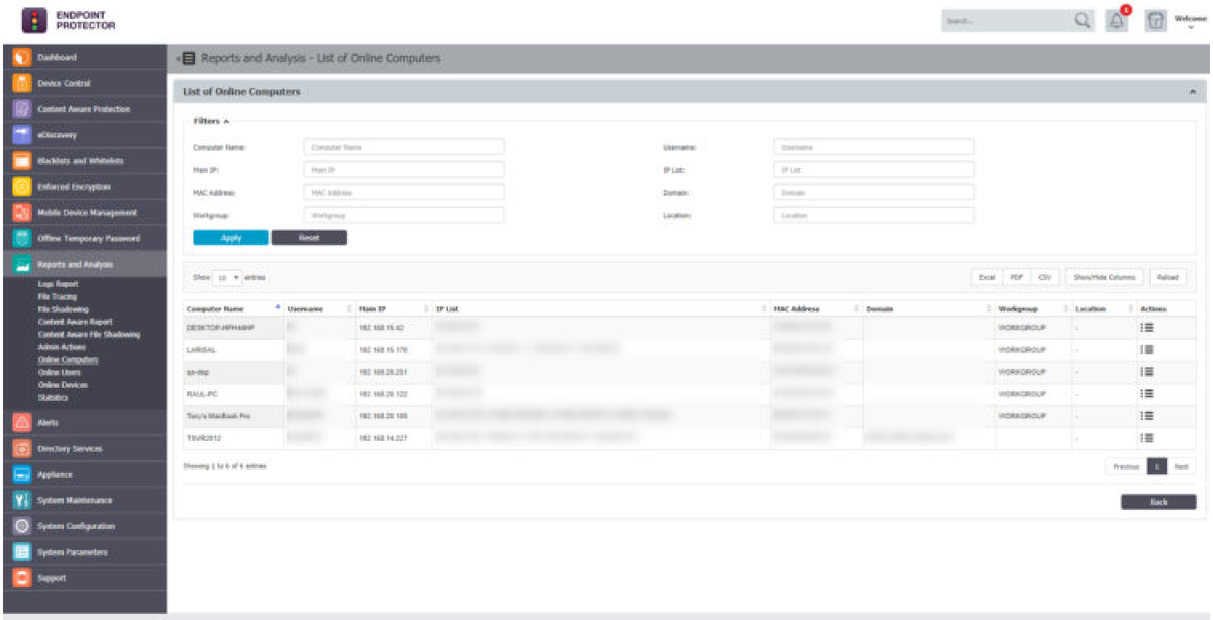
Show 10 entries

Administrator	UI Section	Activity	Operation	Created at	Actions
root	User Authentication	SIGN IN	Login	2019-05-16 11:50:24	
root	User Authentification Failed	SIGN IN	Login	2019-05-16 11:55:20	
root	System Learning	PASTE CONTACTS	Other	2019-05-16 10:52:28	
root	User Authentication	SIGN IN	Login	2019-05-16 10:40:11	
root	User Authentication	SIGN IN	Login	2019-05-16 10:40:00	
root	User Authentication	SIGN IN	Login	2019-05-16 10:00:39	
root	Live Update	APPLY	Edited	2019-04-23 10:14:45	
root	Live Update	CHECK	Other	2019-04-23 10:14:35	
root	User Authentication	SIGN IN	Login	2019-04-23 10:14:27	
root	Live Update	APPLY	Edited	2019-04-23 10:00:22	

Showing 1 to 10 of 28 entries

10.7. Online Computers

This section offers the administrator an overview on computers registered on the system which have an established connection with the server.



Reports and Analysis - List of Online Computers

List of Online Computers

Filters

Computer Name: Computer Name

Username: Username

Main IP: Main IP

IP List: IP List

MAC Address: MAC Address

Domain: Domain

Workgroup: Workgroup

Location: Location

Show 10 entries

Computer Name	Username	Main IP	IP List	MAC Address	Domain	Workgroup	Location	Actions
DESKTOP-HPH6IHP	[redacted]	192.168.15.42	[redacted]	[redacted]		WORKGROUP	-	
LARISAL	[redacted]	192.168.15.170	[redacted]	[redacted]		WORKGROUP	-	
sp-dsp	[redacted]	192.168.28.251	[redacted]	[redacted]		WORKGROUP	-	
RAUL-PC	[redacted]	192.168.28.122	[redacted]	[redacted]		WORKGROUP	-	
Tony's MacBook Pro	[redacted]	192.168.28.105	[redacted]	[redacted]		WORKGROUP	-	
TSVR2012	[redacted]	192.168.14.227	[redacted]	[redacted]	[redacted]		-	

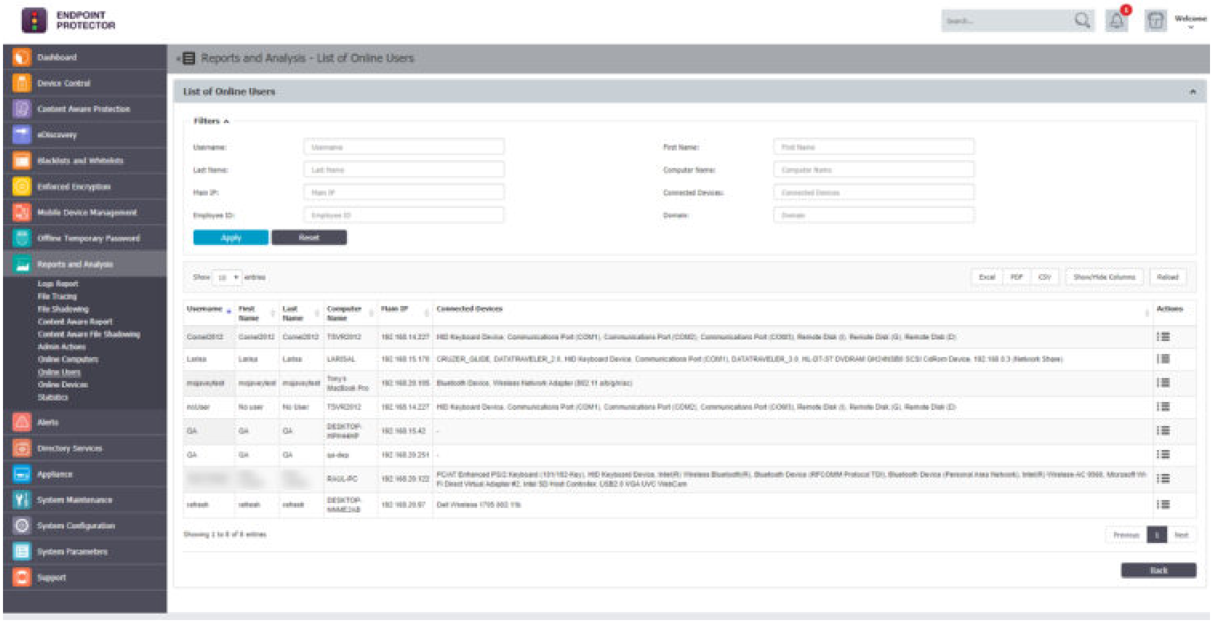
Showing 1 to 6 of 6 entries

Information

If the Refresh Interval for computer X is 1 minute, then the computer X was communicating with the server in the last 1 minute.

10.8. Online Users

This section offers the administrator an overview on users registered on the system which have an established connection with the server.

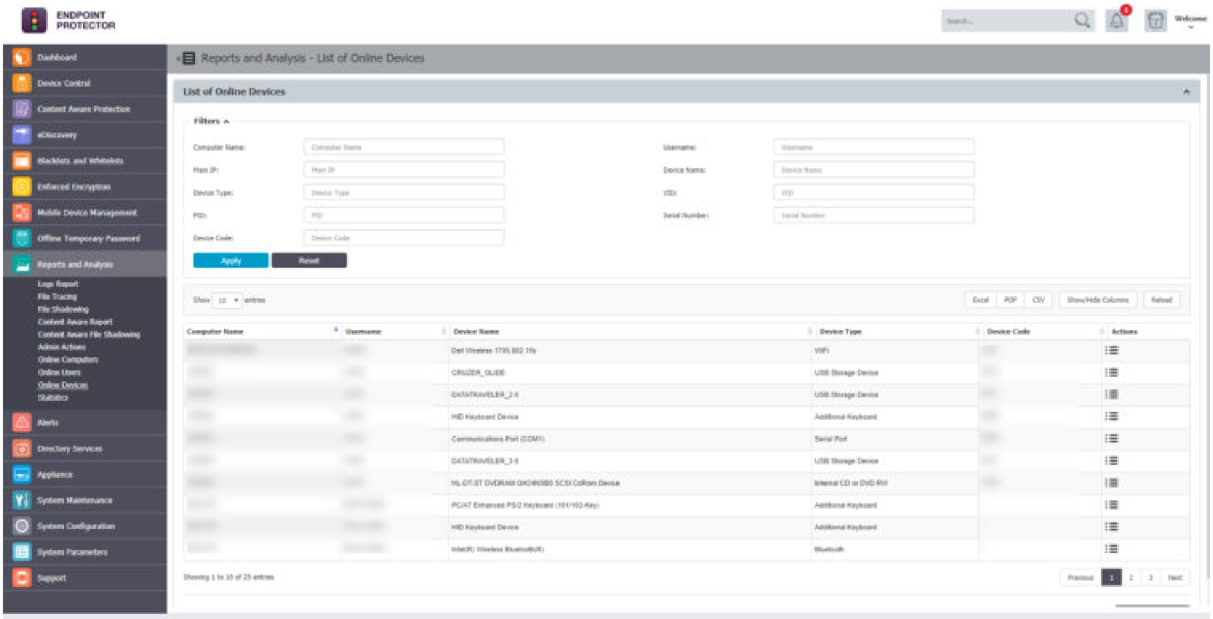


Username	First Name	Last Name	Computer Name	Main IP	Connected Devices	Actions
Corne2012	Corne2012	Corne2012	TSVR2012	192.168.14.227	HID Keyboard Device, Communications Port (COM1), Communications Port (COM2), Communications Port (COM3), Remote Disk (I), Remote Disk (G), Remote Disk (D)	
Larisa	Larisa	Larisa	LARISAL	192.168.15.178	CRUZER_GLIDE, DATATRAVELER_2.0, HID Keyboard Device, Communications Port (COM1), DATATRAVELER_3.0, HL-DT-ST DVDRAM GH24NSB0 SCSI CdRom Device, 192.168.0.3 (Network Share)	
mojaveytest	mojaveytest	mojaveytest	Tony's MacBook Pro	192.168.20.195	Bluetooth Device, Wireless Network Adapter (802.11 a/b/g/n/ac)	
noUser	No user	No User	TSVR2012	192.168.14.227	HID Keyboard Device, Communications Port (COM1), Communications Port (COM2), Communications Port (COM3), Remote Disk (I), Remote Disk (G), Remote Disk (D)	
QA	QA	QA	DESKTOP-[illegible]	192.168.15.42	-	
QA	QA	QA	qa-dep	192.168.20.251	-	
[redacted]	[redacted]	[redacted]	RAUL-PC	192.168.20.122	PC/AT Enhanced PS/2 Keyboard (101/102-Key), HID Keyboard Device, Intel(R) Wireless Bluetooth(R), Bluetooth Device (RFCOMM Protocol TDI), Bluetooth Device (Personal Area Network), Intel(R) Wireless-AC 9560, Microsoft Wi-Fi Direct Virtual Adapter #2, Intel SD Host Controller, USB2.0 VGA UVC WebCam	
refresh	refresh	refresh	DESKTOP-[illegible]	192.168.20.97	Dell Wireless 1705 802.11b	

Showing 1 to 8 of 8 entries

10.9. Online Devices

This section offers the administrator an overview on devices registered on the system which have an established connection with the server.



List of Online Devices

Filters

Computer Name: Computer Name

Main IP: Main IP

Device Type: Device Type

PID: PID

Device Code: Device Code

Username: Username

Device Name: Device Name

VID: VID

Serial Number: Serial Number

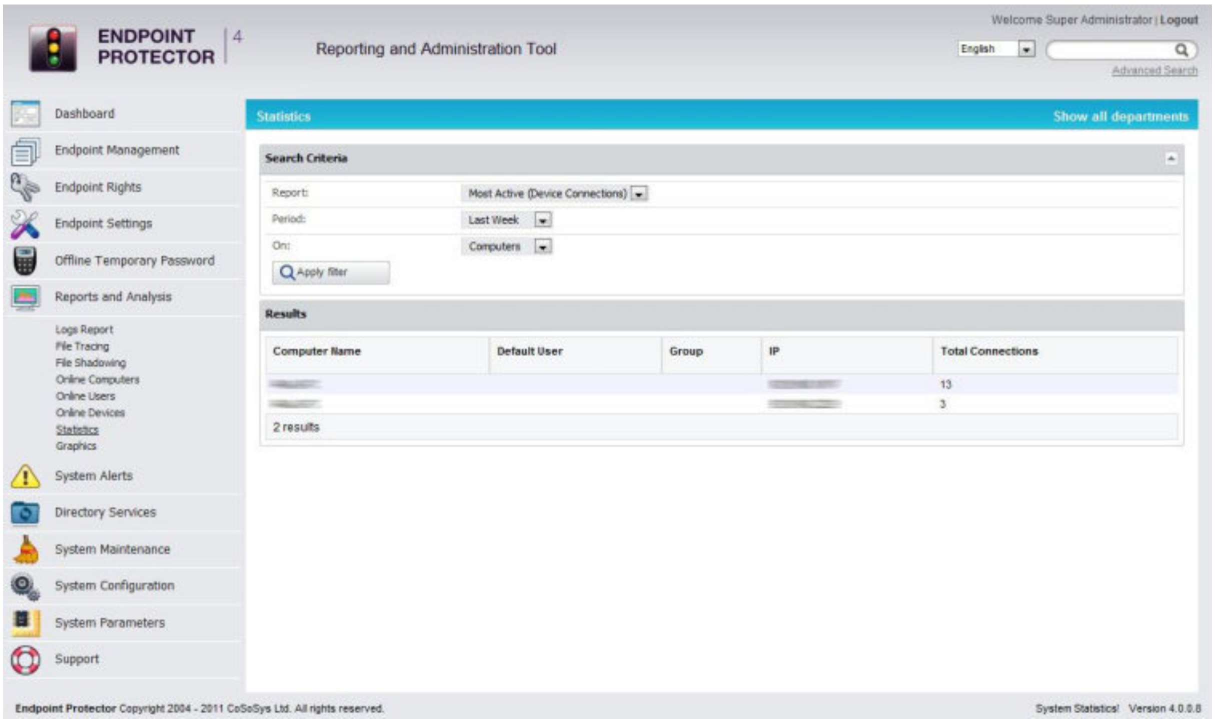
Show 10 entries

Computer Name	Username	Device Name	Device Type	Device Code	Actions
[redacted]	[redacted]	Dell Wireless 1705 802.11b	WiFi	[redacted]	☰
[redacted]	[redacted]	CRUZER_GLIDE	USB Storage Device	[redacted]	☰
[redacted]	[redacted]	DATATRAVELER_2.0	USB Storage Device	[redacted]	☰
[redacted]	[redacted]	HID Keyboard Device	Additional Keyboard	[redacted]	☰
[redacted]	[redacted]	Communications Port (COM1)	Serial Port	[redacted]	☰
[redacted]	[redacted]	DATATRAVELER_3.0	USB Storage Device	[redacted]	☰
[redacted]	[redacted]	HL-DT-ST DVDRAM GXD40SB0 SCSI CdRom Device	Internal CD or DVD RW	[redacted]	☰
[redacted]	[redacted]	PC/AT Enhanced PS/2 Keyboard (101/102-Key)	Additional Keyboard		☰
[redacted]	[redacted]	HID Keyboard Device	Additional Keyboard		☰
[redacted]	[redacted]	Intel(R) Wireless Bluetooth(R)	Bluetooth		☰

Showing 1 to 10 of 25 entries

10.10. 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.



Search Criteria

Report: Most Active (Device Connections)

Period: Last Week

On: Computers

Results

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

2 results

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

System Statistics! Version 4.0.0.8

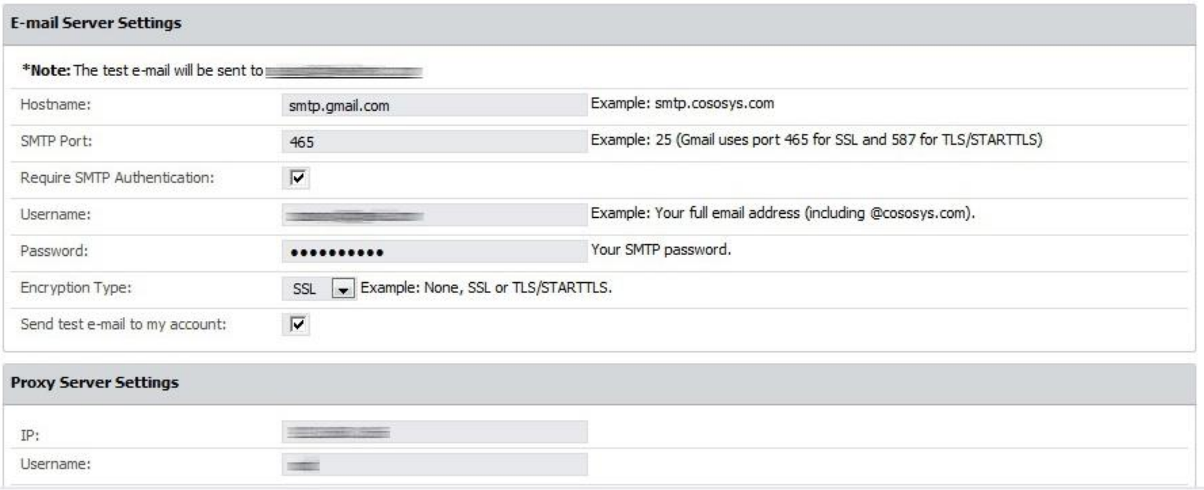
11. Alerts

From this section, the Administrator can define E-mail Alerts for the main events detected by Endpoint Protector: System Alerts, Device Control Alerts, Content Aware Alerts, EasyLock Alerts and Mobile Device Alerts.

Note

Before creating alerts, make sure the Endpoint Protector E-mail Server Settings have been configured from the System Configuration > System Settings section.

The option to verify these settings by sending a test E-mail is also available.



E-mail Server Settings

***Note:** The test e-mail will be sent to [redacted]

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:	[redacted]	Example: Your full email address (including @cososys.com).
Password:	●●●●●●●●●●●	Your SMTP password.
Encryption Type:	SSL	Example: None, SSL or TLS/STARTTLS.
Send test e-mail to my account:	☑	

Proxy Server Settings

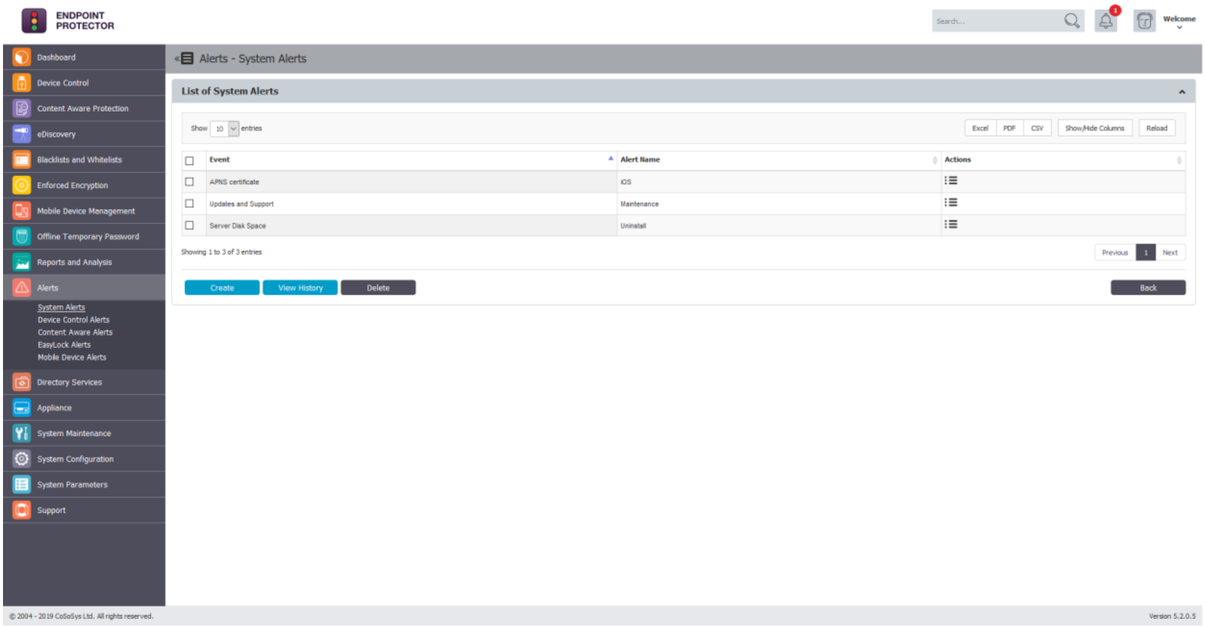
IP:	[redacted]
Username:	[redacted]

Information

In order for each Administrator to appear in the list of recipients for the Alerts, this has to be provided under the Administrator details from the System Configuration > System Administrators section.

11.1. System Alerts

From this section, the Administrator can create system alerts, including APNS certificate expiry, updates and support expiry, endpoint licenses used, etc.



Alerts - System Alerts

List of System Alerts

Show 10 entries

□	Event	Alert Name	Actions
□	APNS certificate	iOS	☰
□	Updates and Support	Maintenance	☰
□	Server Disk Space	Uninstall	☰

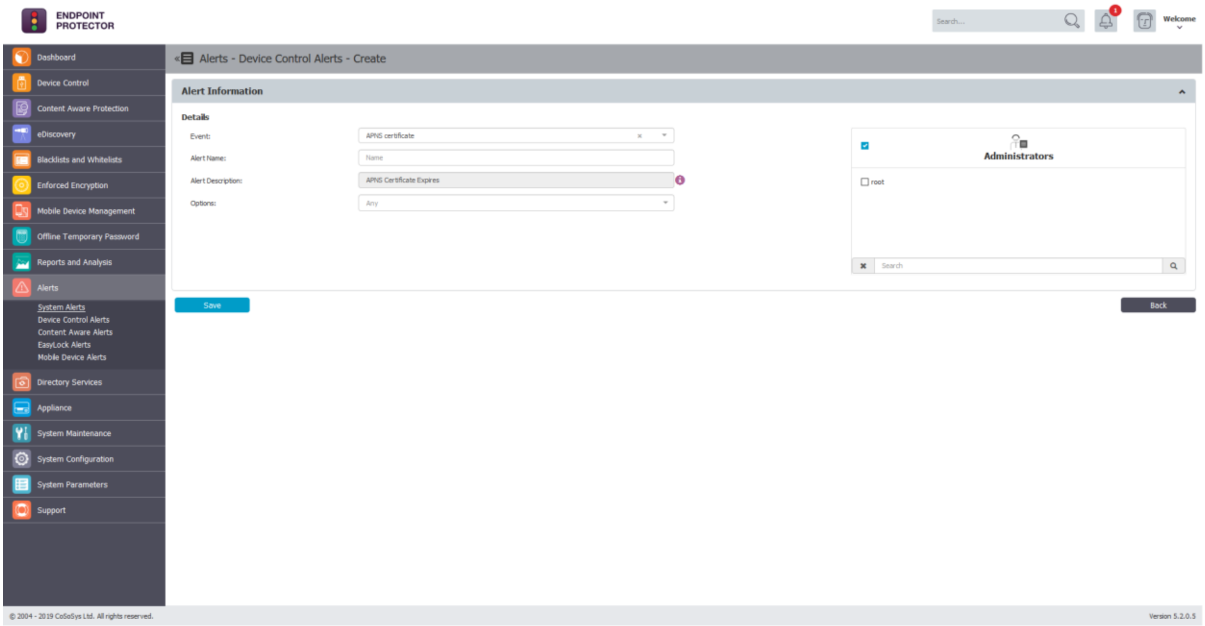
Showing 1 to 3 of 3 entries

A new Alert can be created by clicking on the Create button.

11.1.1. Creating a System Alert

When creating a new System Alert, the below information needs to be defined:

- **Event -** the event type that generates the alert (APNS certificate, Updates and Support, Client Uninstall, etc.)



Alerts - Device Control Alerts - Create

Alert Information

Details

Event: APNS certificate

Alert Name: Name

Alert Description: APNS Certificate Expires

Options: Any

☑ Administrators

□ root

APNS certificate – APNS certificates expire and have to be renewed on a regular basis. These alerts eliminate 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 rake advantage of everything Endpoint Protector has to offer, a reminder can be sent regarding each module maintenance status (Device Control, Content Aware Protection, eDiscovery 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.

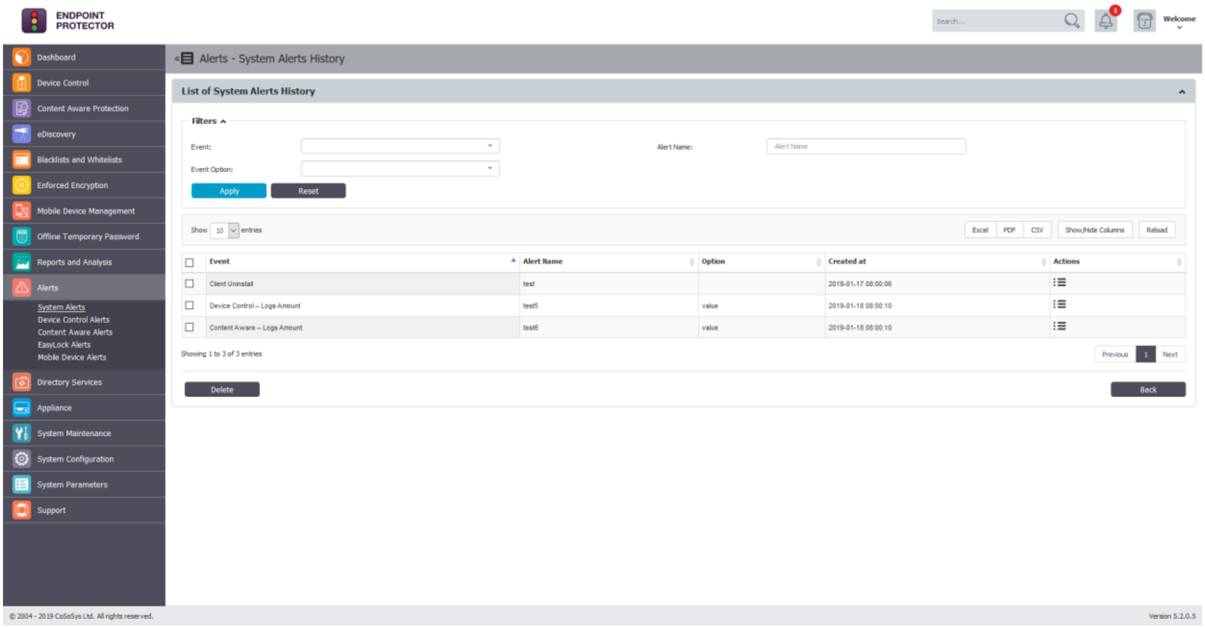
Not Seen Online – An alert can be sent each when a protected endpoint has not been seen online in the specific timeframe. This can also be used to identify computers where the Endpoint Protector Client might have been uninstalled.

⚠ **Note**

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

11.1.2. System Alerts History

From this section, the Administrator can view a history of the System Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.



Alerts - System Alerts History

List of System Alerts History

Filters

Event:

Event Option:

Alert Name: Alert Name

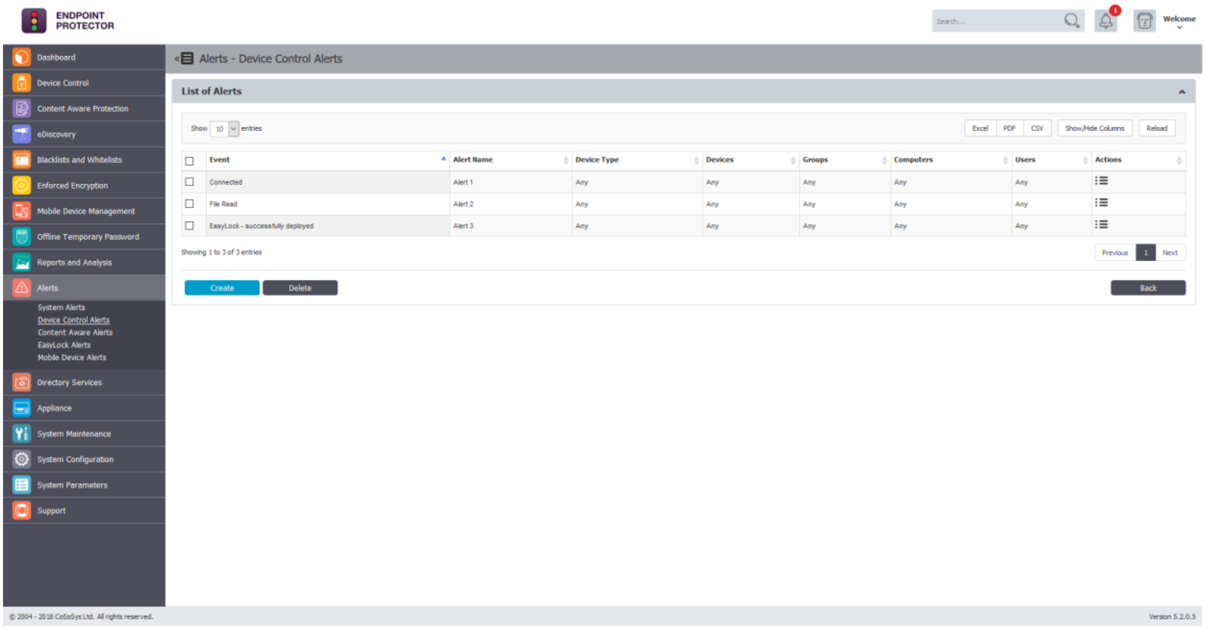
Show 10 entries

□	Event	Alert Name	Option	Created at	Actions
□	Client Uninstall	test		2019-01-17 08:00:06	☰
□	Device Control – Logs Amount	test5	value	2019-01-18 08:00:10	☰
□	Content Aware – Logs Amount	test6	value	2019-01-18 08:00:10	☰

Showing 1 to 3 of 3 entries

11.2. Device Control Alerts

From this section, the Administrator can create Device Control alerts, for events such as Connected, File Read, File Write, EasyLock – successfully deployed, etc.



Alerts - Device Control Alerts

List of Alerts

Show 10 entries

□	Event	Alert Name	Device Type	Devices	Groups	Computers	Users	Actions
□	Connected	Alert 1	Any	Any	Any	Any	Any	☰
□	File Read	Alert 2	Any	Any	Any	Any	Any	☰
□	EasyLock - successfully deployed	Alert 3	Any	Any	Any	Any	Any	☰

Showing 1 to 3 of 3 entries

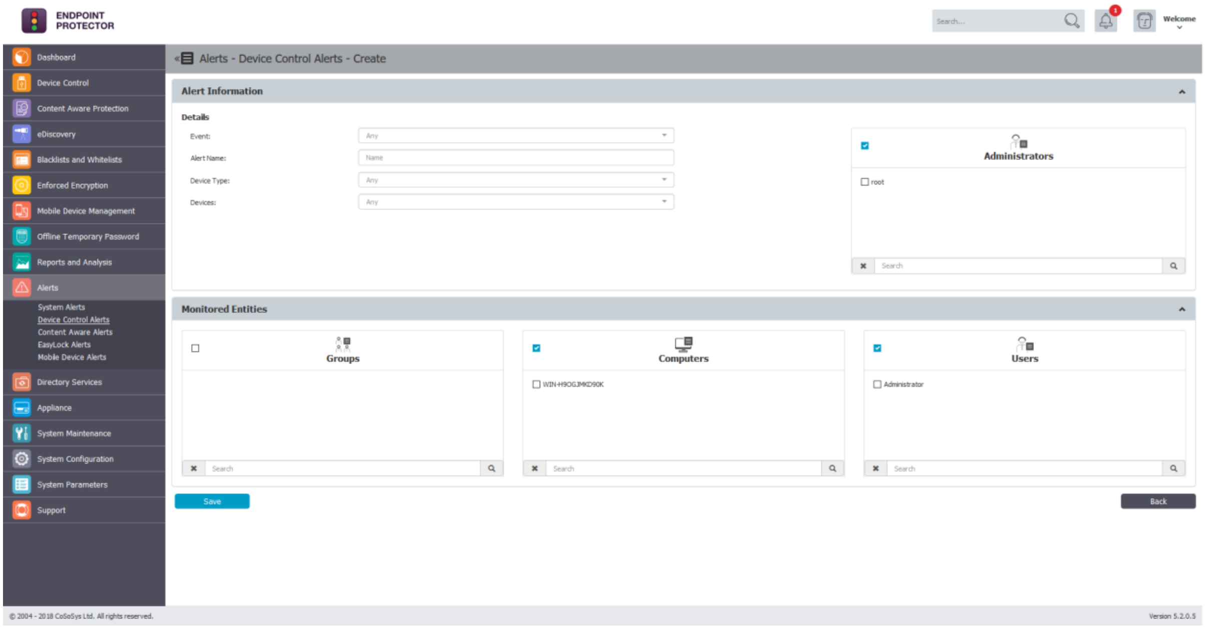
A new Alert can be created by clicking on the Create button.

11.2.1. Creating a Device Control Alert

When creating a new Device Control Alert, the below information needs to be defined:

- **Event -** the event type that generates the alert (Any, Connected, Disconnected, File Read, File Write, File Delete, etc.)

- **Alerts Name –** the name of the alert
- **Device Type** – the device type (Any, USB Storage Device, Bluetooth Smartphone, iPhone, ZIP drive, etc.)
- **Devices** – a specific device already available in the system
- **Monitored Entities** – the Groups, Computers or Users that generate the event
- **Recipients –** the Administrators that should receive the alert



Alerts - Device Control Alerts - Create

Alert Information

Details

Event: Any

Alert Name: Name

Device Type: Any

Devices: Any

☑ Administrators

□ root

Monitored Entities

□ Groups

☑ Computers

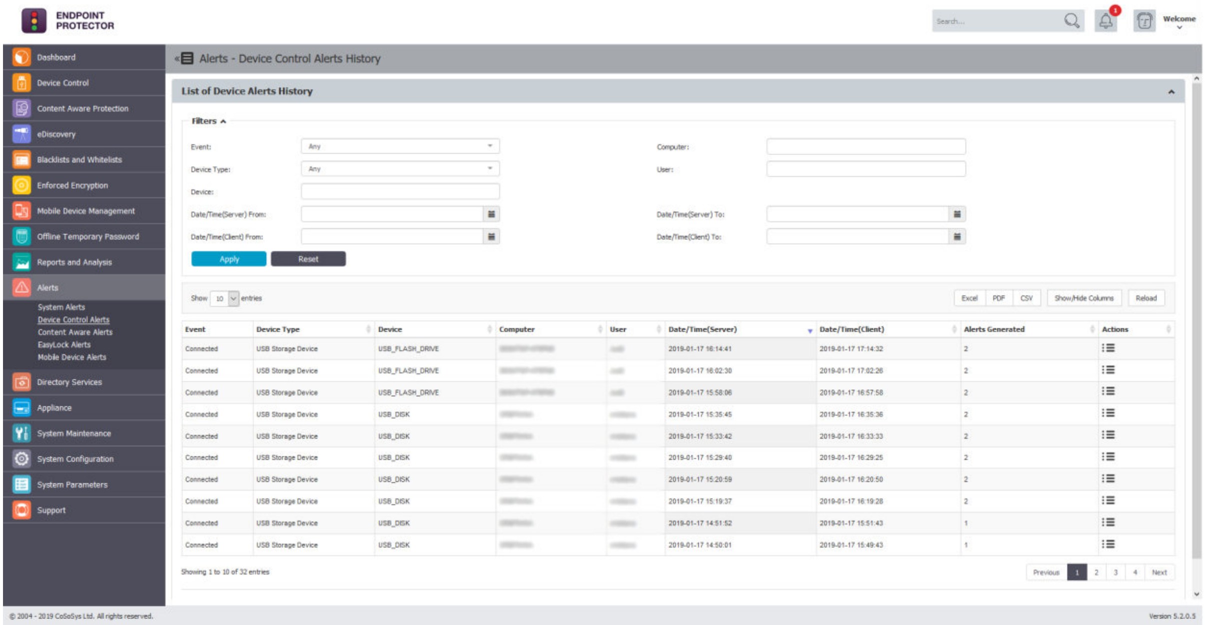
□ WIN-H9OGJMKD90K

☑ Users

□ Administrator

11.2.2. Device Control Alerts History

From this section, the Administrator can view a history of the Device Control Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.



Alerts - Device Control Alerts History

List of Device Alerts History

Filters

Event: Any

Device Type: Any

Device:

Date/Time(Server) From:

Date/Time(Client) From:

Computer:

User:

Date/Time(Server) To:

Date/Time(Client) To:

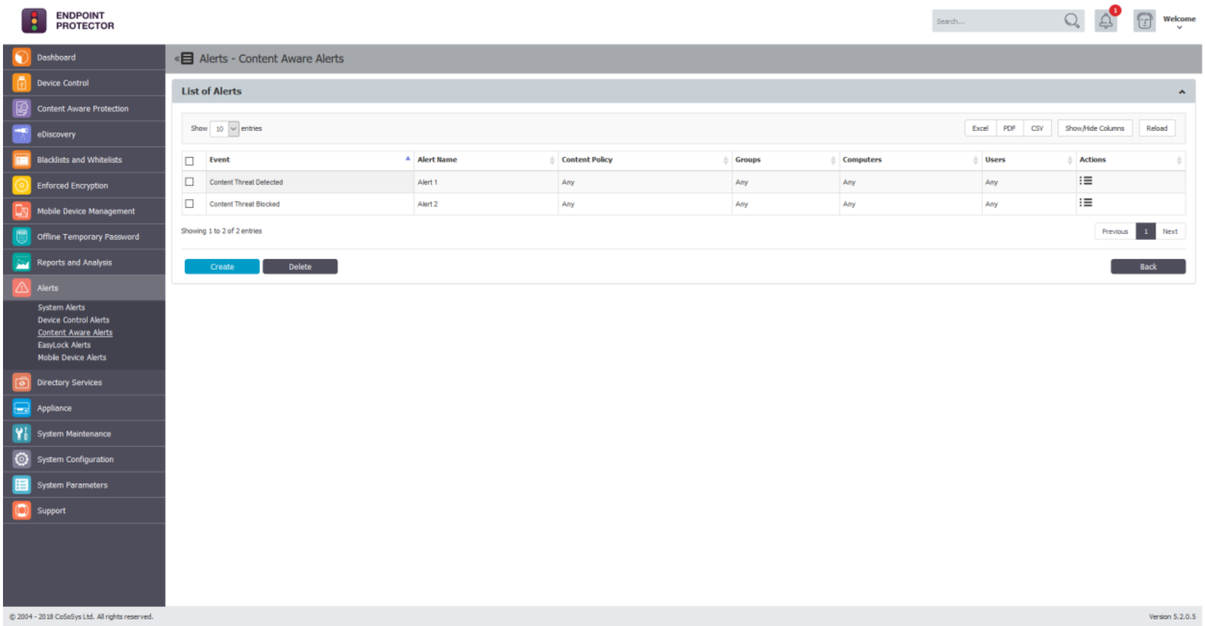
Show 10 entries

Event	Device Type	Device	Computer	User	Date/Time(Server)	Date/Time(Client)	Alerts Generated	Actions
Connected	USB Storage Device	USB_FLASH_DRIVE	[redacted]	[redacted]	2019-01-17 16:14:41	2019-01-17 17:14:32	2	☰
Connected	USB Storage Device	USB_FLASH_DRIVE	[redacted]	[redacted]	2019-01-17 16:02:30	2019-01-17 17:02:26	2	☰
Connected	USB Storage Device	USB_FLASH_DRIVE	[redacted]	[redacted]	2019-01-17 15:58:06	2019-01-17 16:57:58	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 15:35:45	2019-01-17 16:35:36	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 15:33:42	2019-01-17 16:33:33	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 15:29:40	2019-01-17 16:29:25	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 15:20:59	2019-01-17 16:20:50	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 15:19:37	2019-01-17 16:19:28	2	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 14:51:52	2019-01-17 15:51:43	1	☰
Connected	USB Storage Device	USB_DISK	[redacted]	[redacted]	2019-01-17 14:50:01	2019-01-17 15:49:43	1	☰

Showing 1 to 10 of 32 entries

11.3. Content Aware Alerts

From this section, the Administrator can create Content Aware alerts, for events such as Content Threat Detected or Content Threat Blocked.



Alerts - Content Aware Alerts

List of Alerts

Show 10 entries

□	Event	Alert Name	Content Policy	Groups	Computers	Users	Actions
□	Content Threat Detected	Alert 1	Any	Any	Any	Any	☰
□	Content Threat Blocked	Alert 2	Any	Any	Any	Any	☰

Showing 1 to 2 of 2 entries

A new Alert can be created by clicking on the Create button.

11.3.1. Creating a Content Aware Alert

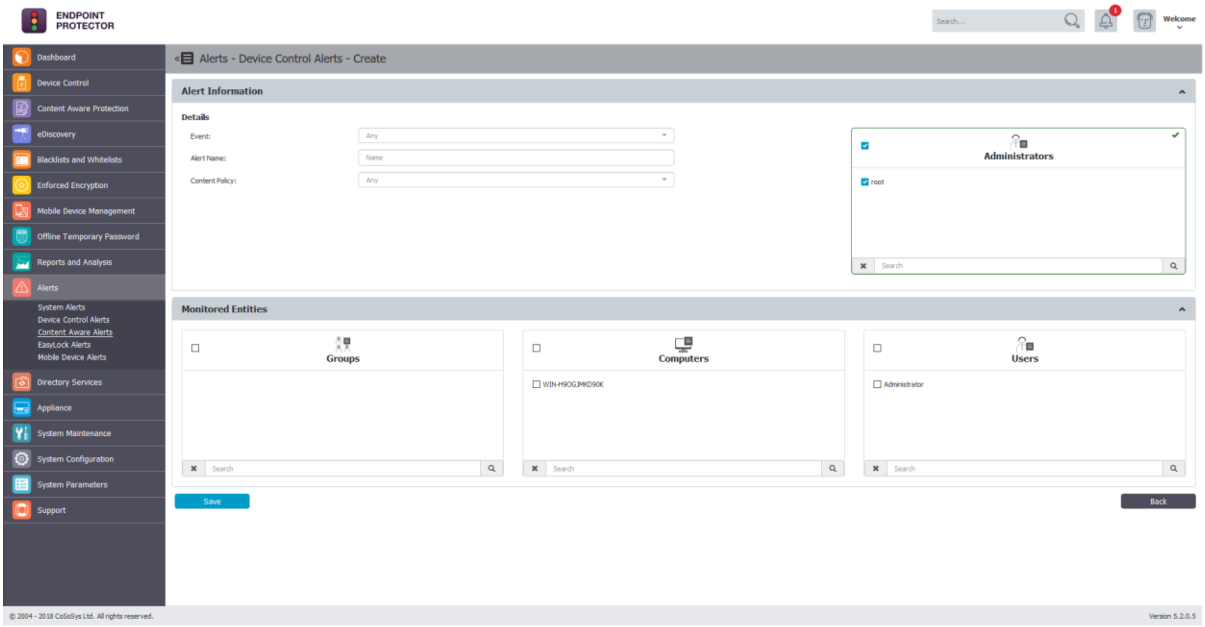
When creating a new Device Control Alert, the below information needs to be defined:

- **Event -** the event type that generates the alert (Content Threat Detected or Content Threat Blocked)

- **Alerts Name –** the name of the alert

- **Monitored Entities** – the Groups, Computers or Users that generate the event

- **Recipients –** the Administrators that should receive the alert



Alerts - Device Control Alerts - Create

Alert Information

Details

Event: Any

Alert Name: Name

Content Policy: Any

☑ Administrators

☑ root

Monitored Entities

□ Groups

□ Computers

□ WIN-H9OGJMKD90K

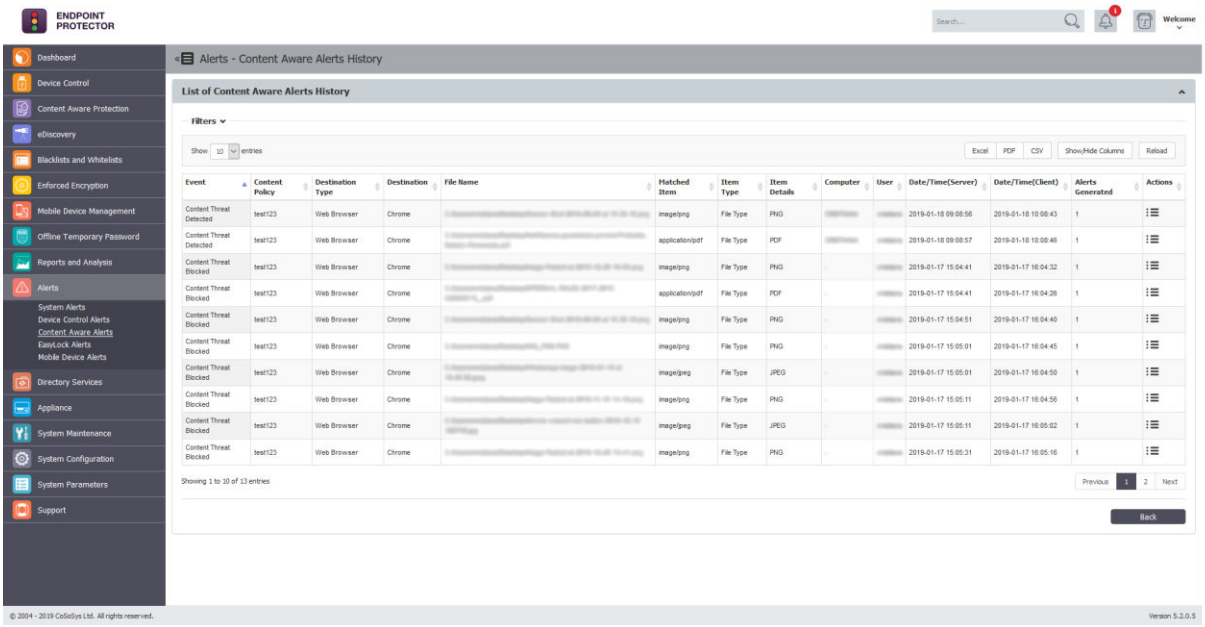
□ Users

□ Administrator

> **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.

11.3.2. Content Aware Alerts History

From this section, the Administrator can view a history of the Content Aware Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.



List of Content Aware Alerts History

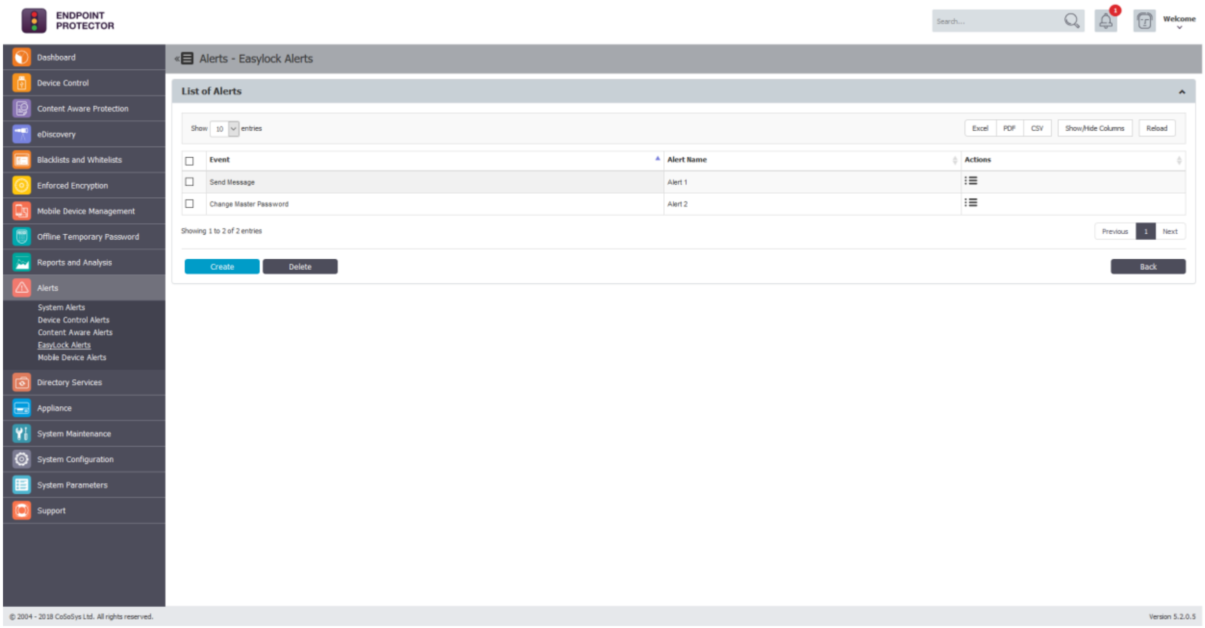
Show 10 entries

Event	Content Policy	Destination Type	Destination	File Name	Matched Item	Item Type	Item Details	Computer	User	Date/Time(Server)	Date/Time(Client)	Alerts Generated	Actions
Content Threat Detected	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	[redacted]	[redacted]	2019-01-18 09:08:56	2019-01-18 10:08:43	1	☰
Content Threat Detected	test123	Web Browser	Chrome	[redacted]	application/pdf	File Type	PDF	[redacted]	[redacted]	2019-01-18 09:08:57	2019-01-18 10:08:46	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	-	[redacted]	2019-01-17 15:04:41	2019-01-17 16:04:32	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	application/pdf	File Type	PDF	-	[redacted]	2019-01-17 15:04:41	2019-01-17 16:04:26	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	-	[redacted]	2019-01-17 15:04:51	2019-01-17 16:04:40	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	-	[redacted]	2019-01-17 15:05:01	2019-01-17 16:04:45	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/jpeg	File Type	JPEG	-	[redacted]	2019-01-17 15:05:01	2019-01-17 16:04:50	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	-	[redacted]	2019-01-17 15:05:11	2019-01-17 16:04:56	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/jpeg	File Type	JPEG	-	[redacted]	2019-01-17 15:05:11	2019-01-17 16:05:02	1	☰
Content Threat Blocked	test123	Web Browser	Chrome	[redacted]	image/png	File Type	PNG	-	[redacted]	2019-01-17 15:05:31	2019-01-17 16:05:16	1	☰

Showing 1 to 10 of 13 entries

11.4. EasyLock Alert

From this section, the Administrator can create EasyLock alerts, for events such password changes, messages sent, etc.



List of Alerts

Show 10 entries

□	Event	Alert Name	Actions
□	Send Message	Alert 1	☰
□	Change Master Password	Alert 2	☰

Showing 1 to 2 of 2 entries

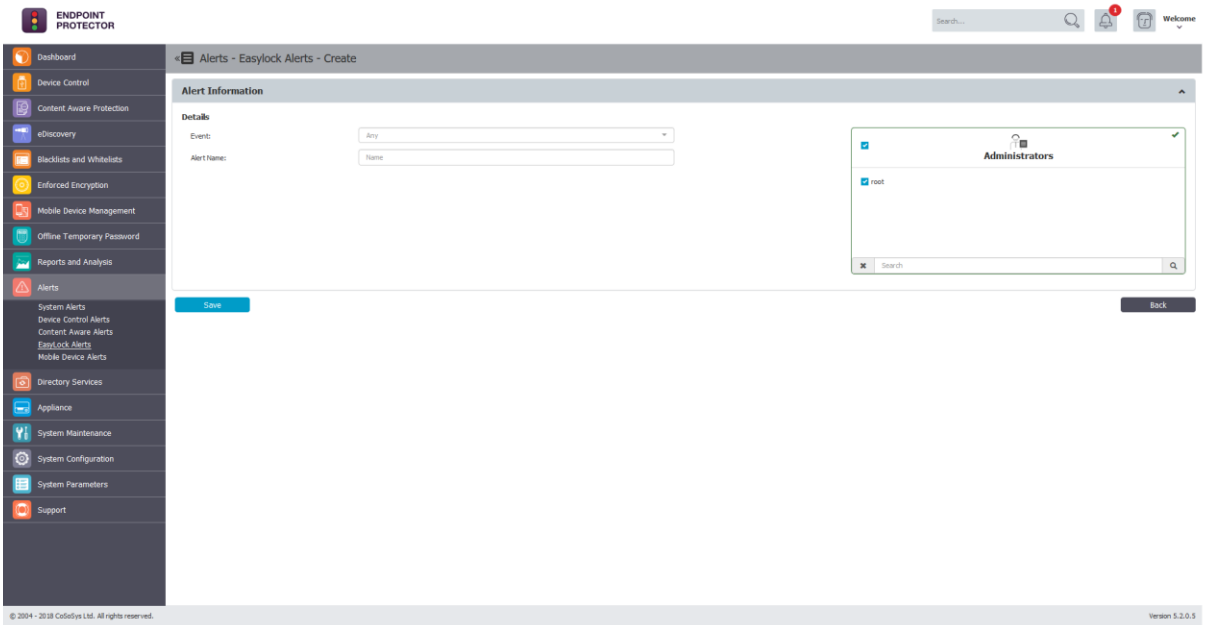
A new Alert can be created by clicking on the Create button.

11.4.1. Creating an EasyLock Alert

When creating a new EasyLock Alert, the below information needs to be defined:

- **Event -** the event type that generates the alert (Any, Send Message, Change User’s Password, Reset Device, Re-deploy Client, etc.)

- **Alerts Name –** the name of the alert
- **Recipients –** the Administrators that should receive the alert



Details

Event: Any

Alert Name: Name

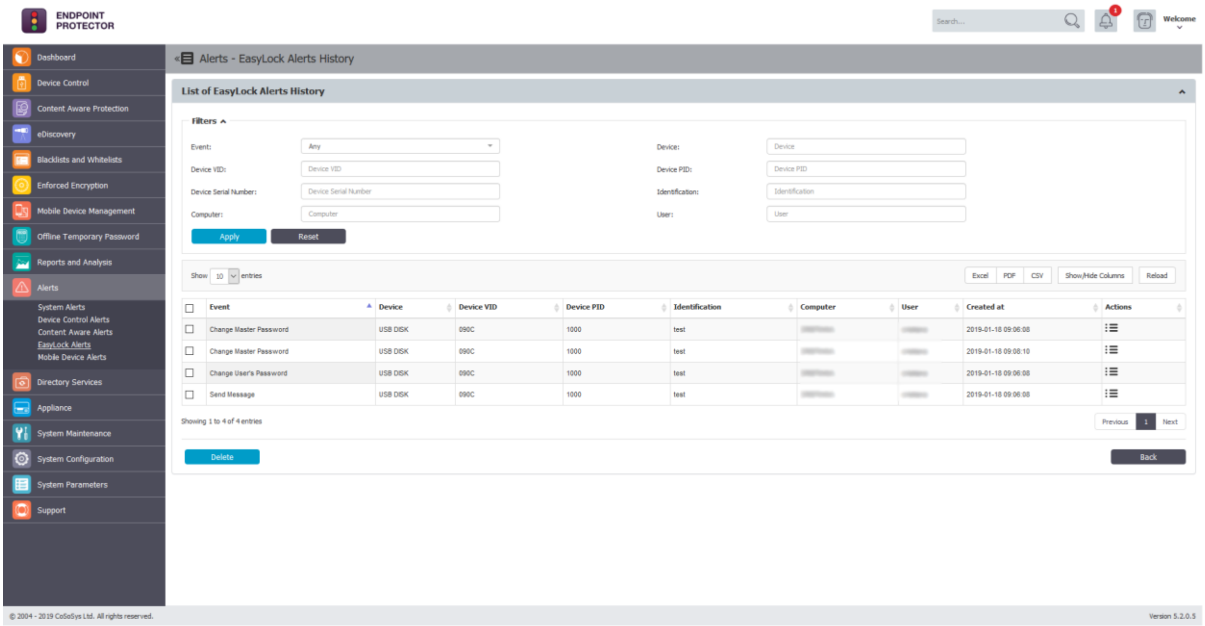
Administrators

☑ root

Search

11.4.2. EasyLock Alert History

From this section, the Administrator can view a history of the EasyLock Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.



Filters

Event: Any

Device: Device

Device VID: Device VID

Device PID: Device PID

Device Serial Number: Device Serial Number

Identification: Identification

Computer: Computer

User: User

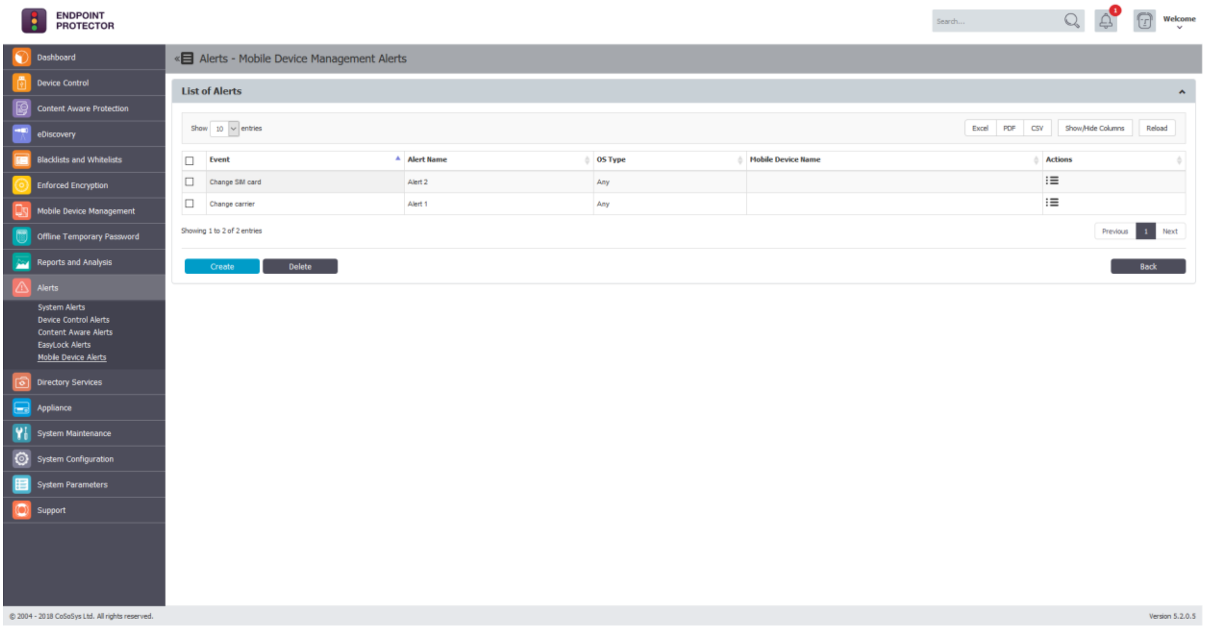
Show 10 entries

□	Event	Device	Device VID	Device PID	Identification	Computer	User	Created at	Actions
□	Change Master Password	USB DISK	090C	1000	test	[redacted]	[redacted]	2019-01-18 09:06:08	☰
□	Change Master Password	USB DISK	090C	1000	test	[redacted]	[redacted]	2019-01-18 09:08:10	☰
□	Change User's Password	USB DISK	090C	1000	test	[redacted]	[redacted]	2019-01-18 09:06:08	☰
□	Send Message	USB DISK	090C	1000	test	[redacted]	[redacted]	2019-01-18 09:06:08	☰

Showing 1 to 4 of 4 entries

11.5. Mobile Device Alerts

From this section, the Administrator can create Mobile Device alerts, for events such Carrier change, SIM change, etc.



List of Alerts

Show 10 entries

□	Event	Alert Name	OS Type	Mobile Device Name	Actions
□	Change SIM card	Alert 2	Any		☰
□	Change carrier	Alert 1	Any		☰

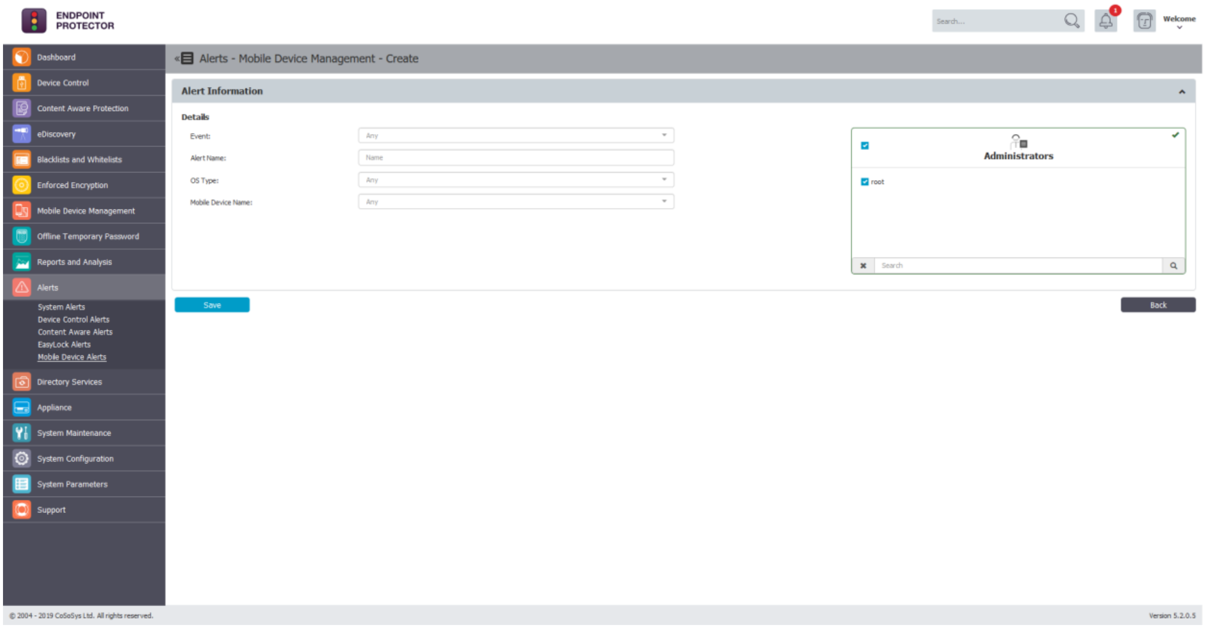
Showing 1 to 2 of 2 entries

A new Alert can be created by clicking on the Create button.

11.5.1. Creating a Mobile Device Alert

When creating a new Mobile Device Alert, the below information needs to be defined:

- **Event -** the event type that generates the alert
- **Alerts Name –** the name of the alert
- **Recipients –** the Administrators that should receive the alert



Alert Information

Details

Event: Any

Alert Name: Name

OS Type: Any

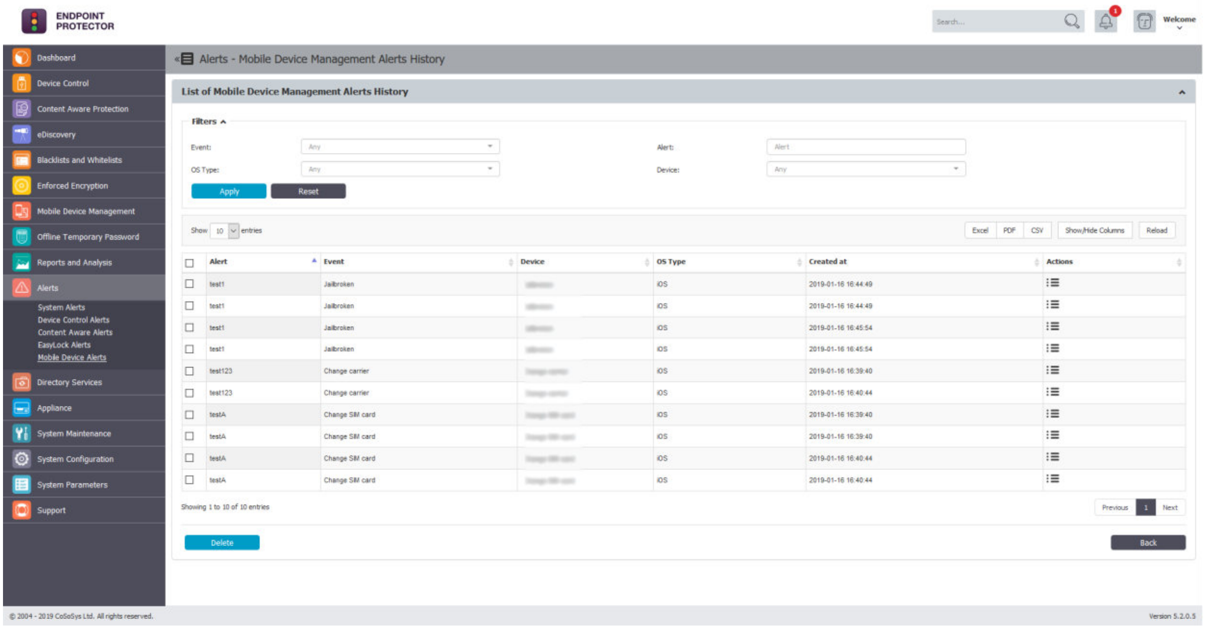
Mobile Device Name: Any

☑ Administrators

☑ root

11.5.2. Mobile Device Alert History

From this section, the Administrator can view a history of the Mobile Device Alerts. Alerts that are no longer needed for auditing purposes can later be deleted.



List of Mobile Device Management Alerts History

Filters

Event: Any

Alert: Alert

OS Type: Any

Device: Any

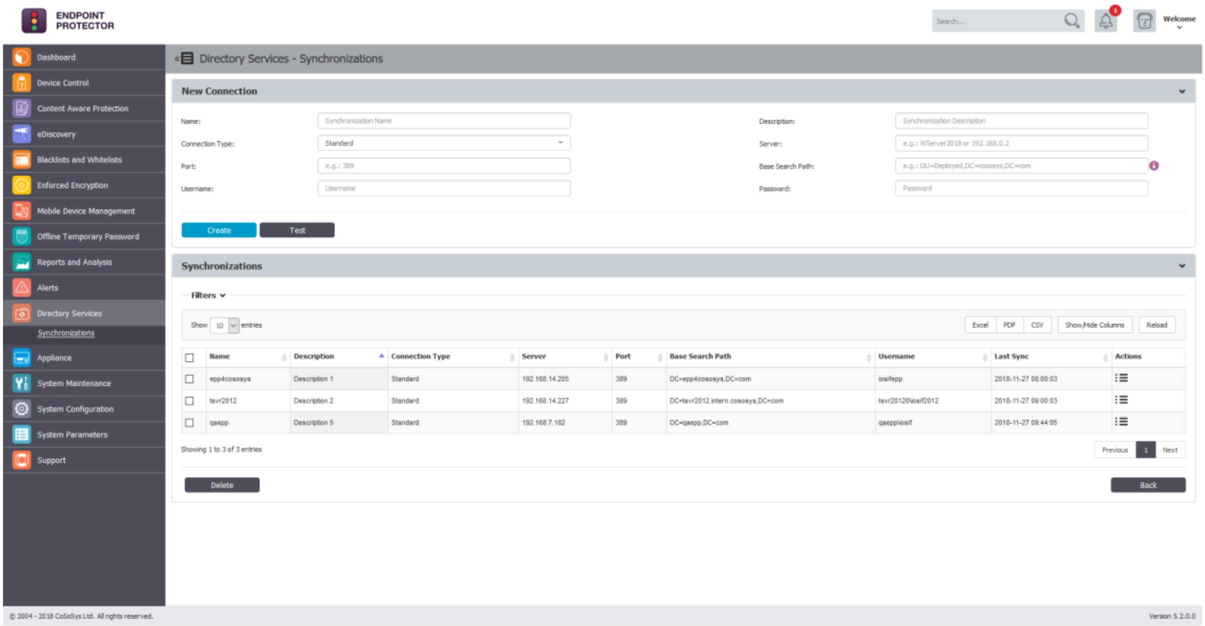
Show 10 entries

□	Alert	Event	Device	OS Type	Created at	Actions
□	test1	Jailbroken	[redacted]	iOS	2019-01-16 16:44:49	☰
□	test1	Jailbroken	[redacted]	iOS	2019-01-16 16:44:49	☰
□	test1	Jailbroken	[redacted]	iOS	2019-01-16 16:45:54	☰
□	test1	Jailbroken	[redacted]	iOS	2019-01-16 16:45:54	☰
□	test123	Change carrier	[redacted]	iOS	2019-01-16 16:39:40	☰
□	test123	Change carrier	[redacted]	iOS	2019-01-16 16:40:44	☰
□	testA	Change SIM card	[redacted]	iOS	2019-01-16 16:39:40	☰
□	testA	Change SIM card	[redacted]	iOS	2019-01-16 16:39:40	☰
□	testA	Change SIM card	[redacted]	iOS	2019-01-16 16:40:44	☰
□	testA	Change SIM card	[redacted]	iOS	2019-01-16 16:40:44	☰

Showing 1 to 10 of 10 entries

12. Directory Services

From this section, the Administrator can import and synchronize the entities (Users, Computers and Groups) from the company's Active Directory.



Directory Services - Synchronizations

New Connection

Name:	Synchronization Name	Description:	Synchronization Description
Connection Type:	Standard	Server:	e.g.: WServer2018 or 192.168.0.2
Port:	e.g.: 389	Base Search Path:	e.g.: OU=Deployed,DC=cososys,DC=com
Username:	Username	Password:	Password

Synchronizations

Show 10 entries

☐	Name	Description	Connection Type	Server	Port	Base Search Path	Username	Last Sync	Actions
☐	epp4cososys	Description 1	Standard	192.168.14.205	389	DC=epp4cososys,DC=com	iosifepp	2018-11-27 08:00:03	☰
☐	tsvr2012	Description 2	Standard	192.168.14.227	389	DC=tsvr2012.intern.cososys,DC=com	tsvr20120\iosif2012	2018-11-27 09:00:03	☰
☐	qaepp	Description 5	Standard	192.168.7.182	389	DC=qaepp,DC=com	qaepp\iosif	2018-11-27 09:44:05	☰

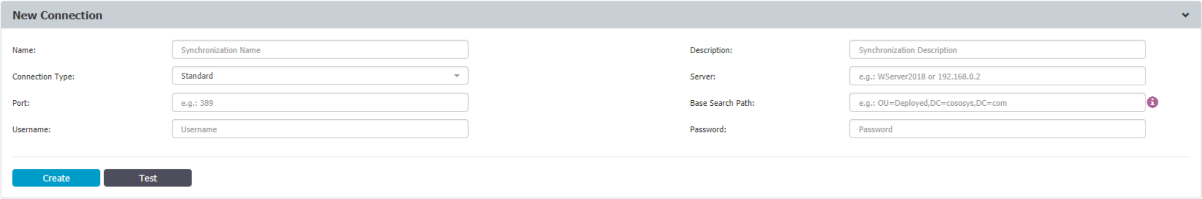
Showing 1 to 3 of 3 entries

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0

12.1. Creating a new Connection

The Administrator can create and manage connections from the Directory Services > Synchronizations section. The required information includes the Connection Type, Server, Port, Username and Password.



New Connection

Name:	Synchronization Name	Description:	Synchronization Description
Connection Type:	Standard	Server:	e.g.: WServer2018 or 192.168.0.2
Port:	e.g.: 389	Base Search Path:	e.g.: OU=Deployed,DC=cososys,DC=com
Username:	Username	Password:	Password

⚠ Note

When having to import a very large number of entities, we recommend using the Base Search Path in order to get only the relevant information displayed. 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.

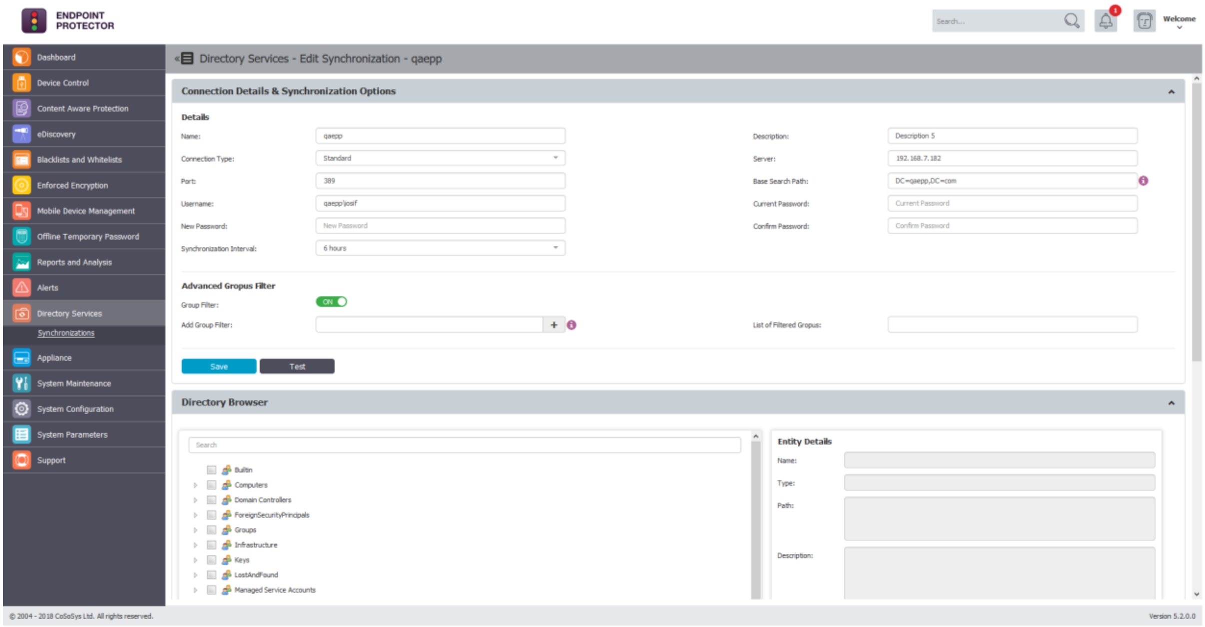
Tips

To ensure the provided information is correct, a new connection can be tested by pressing the Test button.

One a new connection has been created, it is available in the synchronization list and can be further edited, to include the required entities.

12.2. Connection Details & Synchronization Options

For the defined connectons, several syncronization options are available. From this section, the connection credentials and syncronization interval can also be changed.



Directory Services - Edit Synchronization - qaepp

Connection Details & Synchronization Options

Details

Name:	qaepp	Description:	Description 5
Connection Type:	Standard	Server:	192.168.7.182
Port:	389	Base Search Path:	DC=qaepp,DC=com
Username:	qaepp\iosif	Current Password:	Current Password
New Password:	New Password	Confirm Password:	Confirm Password
Synchronization Interval:	6 hours		

Advanced Gropus Filter

Group Filter: ON

Add Group Filter:

List of Filtered Gropus:

Directory Browser

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- Groups
- Infrastructure
- Keys
- LostAndFound
- Managed Service Accounts

Entity Details

Name:

Type:

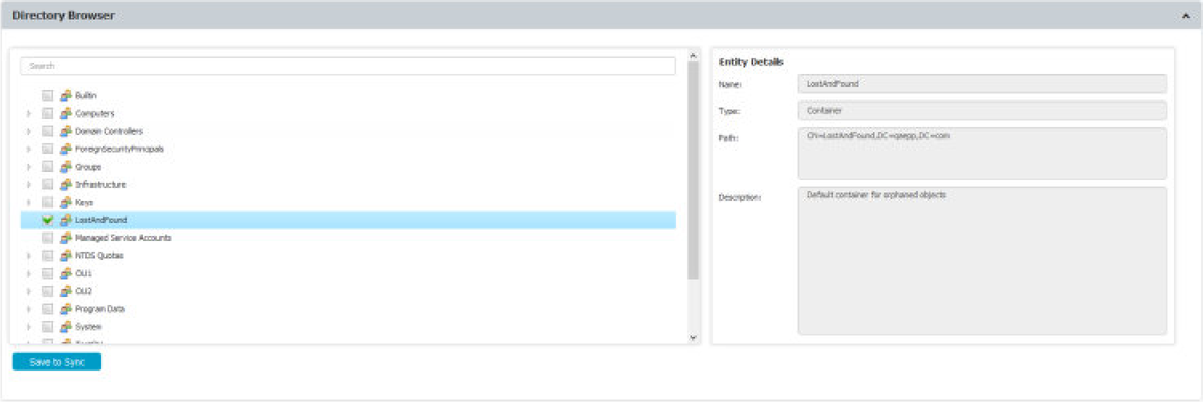
Path:

Description:

Tips

The Advanced Groups Filer can be used to import and synchronize only specific groups, ignoring all other entities.

From the The Directory Browser section, the Adminastrator can select the enteties that need to be synced.



Directory Browser

Search

- □ Builtin
- □ Computers
- □ Domain Controllers
- □ ForeignSecurityPrincipals
- □ Groups
- □ Infrastructure
- □ Keys
- ✓ LostAndFound
- □ Managed Service Accounts
- □ NTDS Quotas
- □ OU1
- □ OU2
- □ Program Data
- □ System

Entity Details

Name: LostAndFound

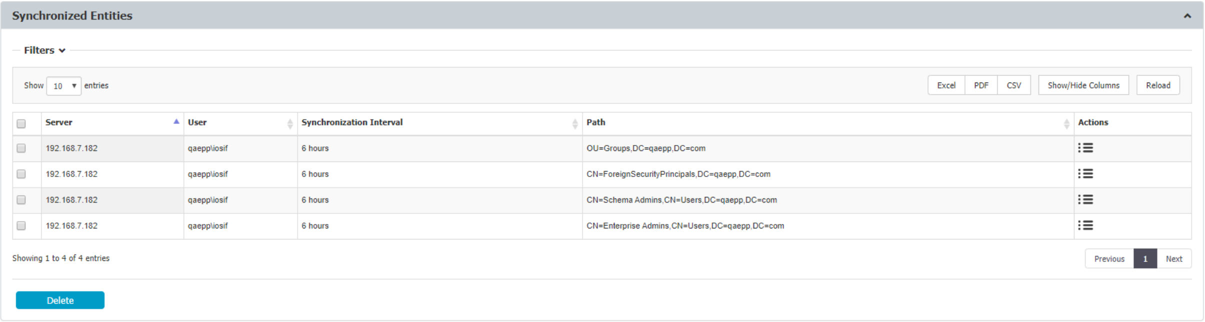
Type: Container

Path: CN=LostAndFound,DC=qaepp,DC=com

Description: Default container for orphaned objects

Save to Sync

Once the desired enteties have been chosen, they can be saved to sync.



Synchronized Entities

Filters

Show 10 entries

Excel PDF CSV Show/Hide Columns Reload

□	Server	User	Synchronization Interval	Path	Actions
□	192.168.7.182	qaepp\iosif	6 hours	OU=Groups,DC=qaepp,DC=com	☰
□	192.168.7.182	qaepp\iosif	6 hours	CN=ForeignSecurityPrincipals,DC=qaepp,DC=com	☰
□	192.168.7.182	qaepp\iosif	6 hours	CN=Schema Admins,CN=Users,DC=qaepp,DC=com	☰
□	192.168.7.182	qaepp\iosif	6 hours	CN=Enterprise Admins,CN=Users,DC=qaepp,DC=com	☰

Showing 1 to 4 of 4 entries

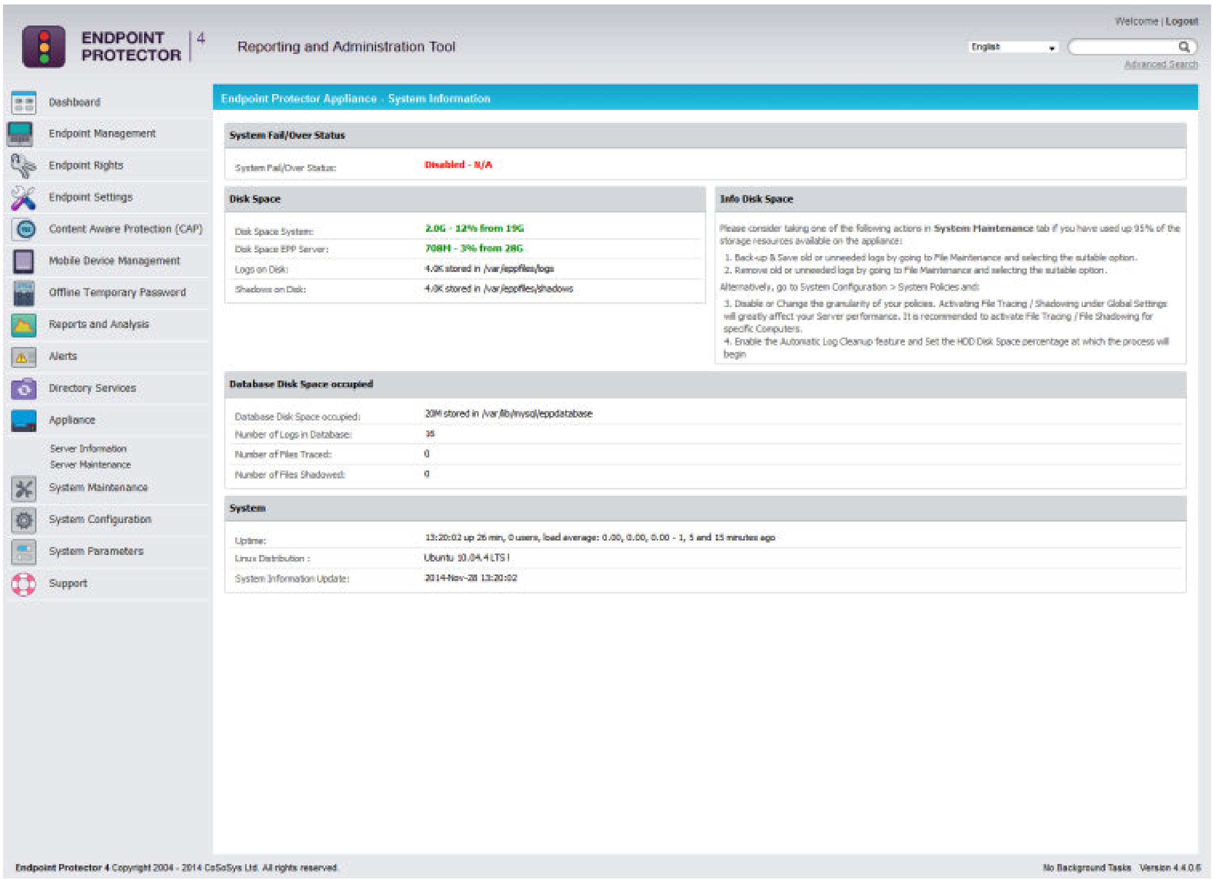
Previous 1 Next

Delete

13. Appliance

13.1. 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 Appliance - System Information

System Fail/Over Status

System Fail/Over Status:	Disabled - N/A

Disk Space

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

Info Disk Space

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

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

Alternatively, go to System Configuration > System Policies and:

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

Database Disk Space occupied

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

System

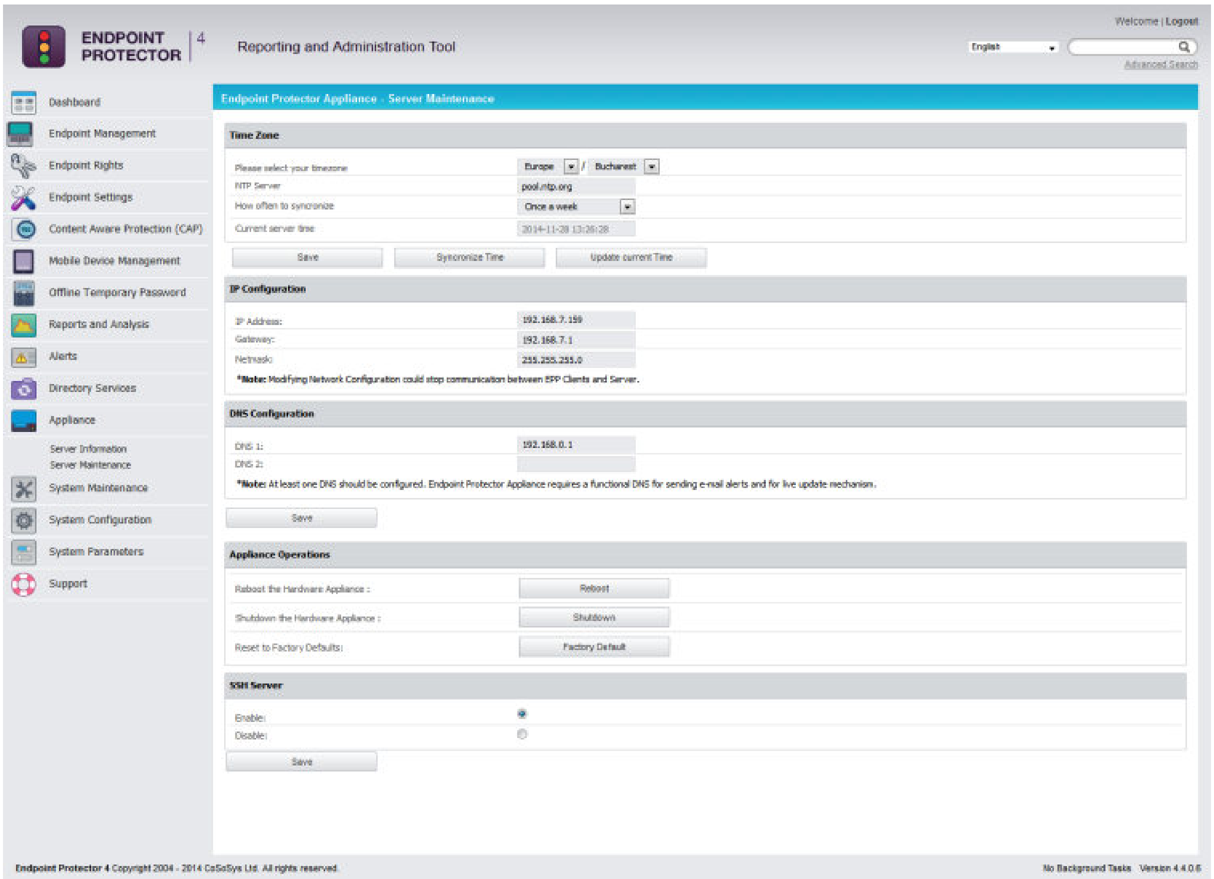
Uptime:	13:20:02 up 26 min, 0 users, load average: 0.00, 0.00, 0.00 - 1, 5 and 15 minutes ago
Linux Distribution :	Ubuntu 10.04.4 LTS l
System Information Update:	2014-Nov-28 13:20:02

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

No Background Tasks Version 4.4.0.6

13.2. 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 Appliance - Server Maintenance

Time Zone

Please select your timezone: Europe / Bucharest
NTP Server: pool.ntp.org
How often to syncronize: Once a week
Current server time: 2014-11-28 13:26:28

IP Configuration

IP Address: 192.168.7.159
Gateway: 192.168.7.1
Netmask: 255.255.255.0

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

DNS Configuration

DNS 1: 192.168.0.1
DNS 2:

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

Appliance Operations

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

SSH Server

Enable: ●
Disable: ○

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

13.2.1. 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

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.

13.2.2. 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!

13.2.3. 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.

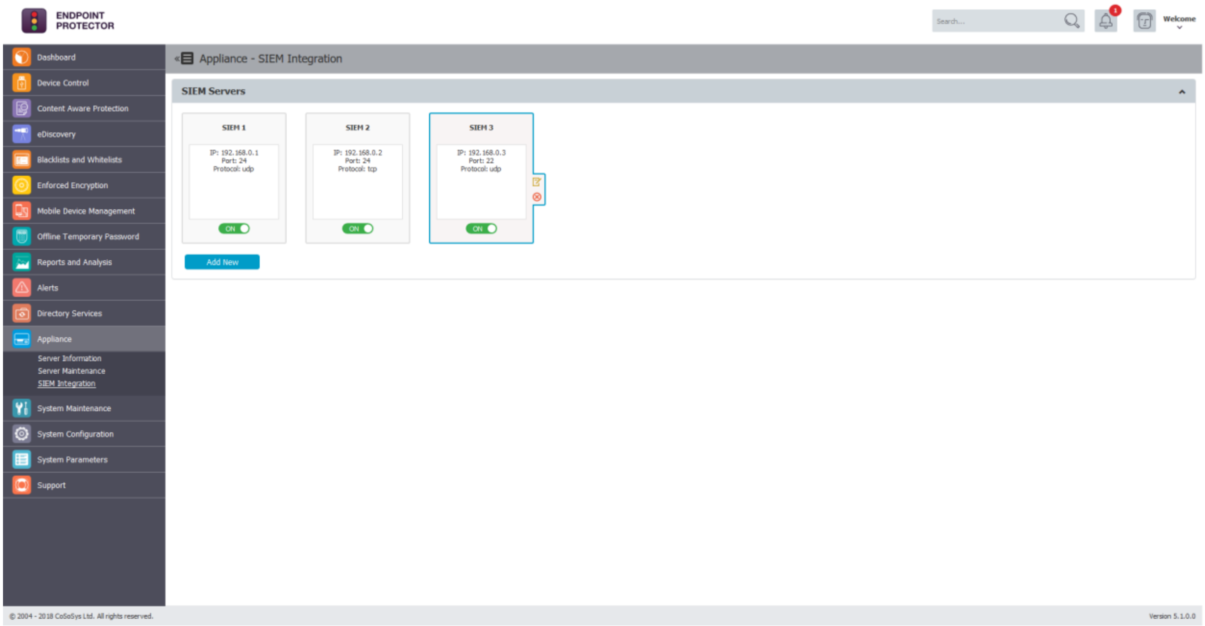
13.2.4. SSH Server

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.

13.3. 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 Appliance > SIEM Integration section.



SIEM 1
IP: 192.168.0.1
Port: 24
Protocol: udp

SIEM 2
IP: 192.168.0.2
Port: 24
Protocol: tcp

SIEM 3
IP: 192.168.0.3
Port: 22
Protocol: udp

A new SIEM Server can be added by clicking on the Add New button. An existing policy can be edited by double-clicking on it.

Information

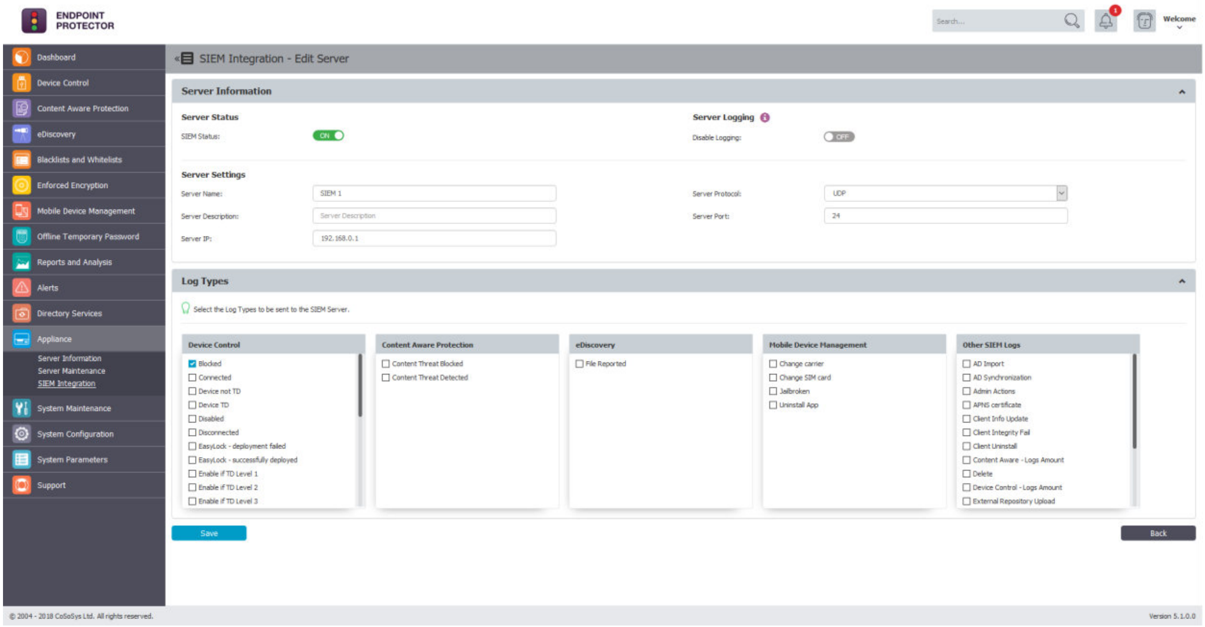
The option to edit or delete a SIEM Server is available after selecting the desired policy.

Setting up a SIEM Server requires the following information:

- **Server Name**
- **Server Description**
- **Server Protocol** – UDP or TCP
- **Server Port**
- **Server IP**
- **Log Types** – what logs to send to the SIEM Server

Note

The Disable Logging option allows the Administrator to also keep the logs on the Endpoint Protector Server or, only have them in the SIEM Server.



SIEM Integration - Edit Server

Server Information

Server Status

SIEM Status: ON

Server Logging

Disable Logging: OFF

Server Settings

Server Name: SIEM 1

Server Description: Server Description

Server IP: 192.168.0.1

Server Protocol: UDP

Server Port: 24

Log Types

Select the Log Types to be sent to the SIEM Server.

Device Control	Content Aware Protection	eDiscovery	Mobile Device Management	Other SIEM Logs
☑ Blocked	□ Content Threat Blocked	□ File Reported	□ Change carrier	□ AD Import
□ Connected	□ Content Threat Detected		□ Change SIM card	□ AD Synchronization
□ Device not TD			□ Jailbroken	□ Admin Actions
□ Device TD			□ Uninstall App	□ APNS certificate
□ Disabled				□ Client Info Update
□ Disconnected				□ Client Integrity Fail
□ EasyLock - deployment failed				□ Client Uninstall
□ EasyLock - successfully deployed				□ Content Aware - Logs Amount
□ Enable if TD Level 1				□ Delete
□ Enable if TD Level 2				□ Device Control - Logs Amount
□ Enable if TD Level 3				□ External Repository Upload

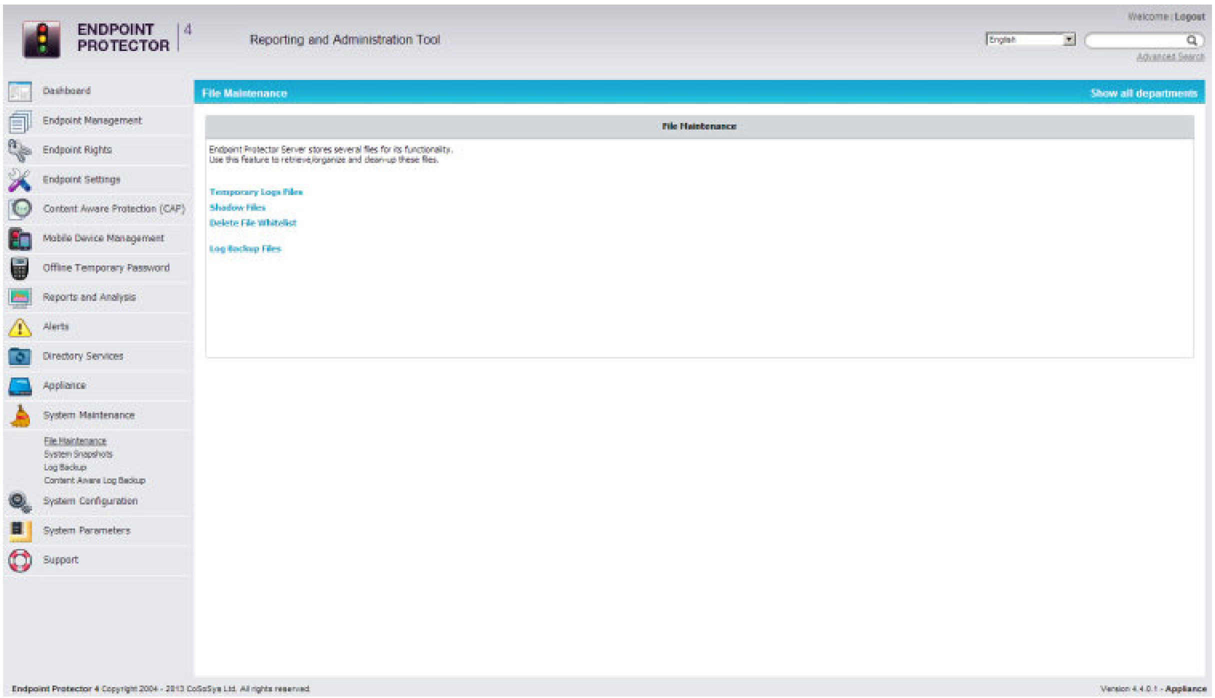
Information

The maximum number of SIEM hosts configured at any given time is four (4).

14. System Maintenance

14.1. File Maintenance

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



Endpoint Protector Server stores several files for its functionality.
Use this feature to retrieve/organize and clean-up these files.

Endpoint Protector 4 Copyright 2004 - 2013 CoSoSys Ltd. All rights reserved.

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

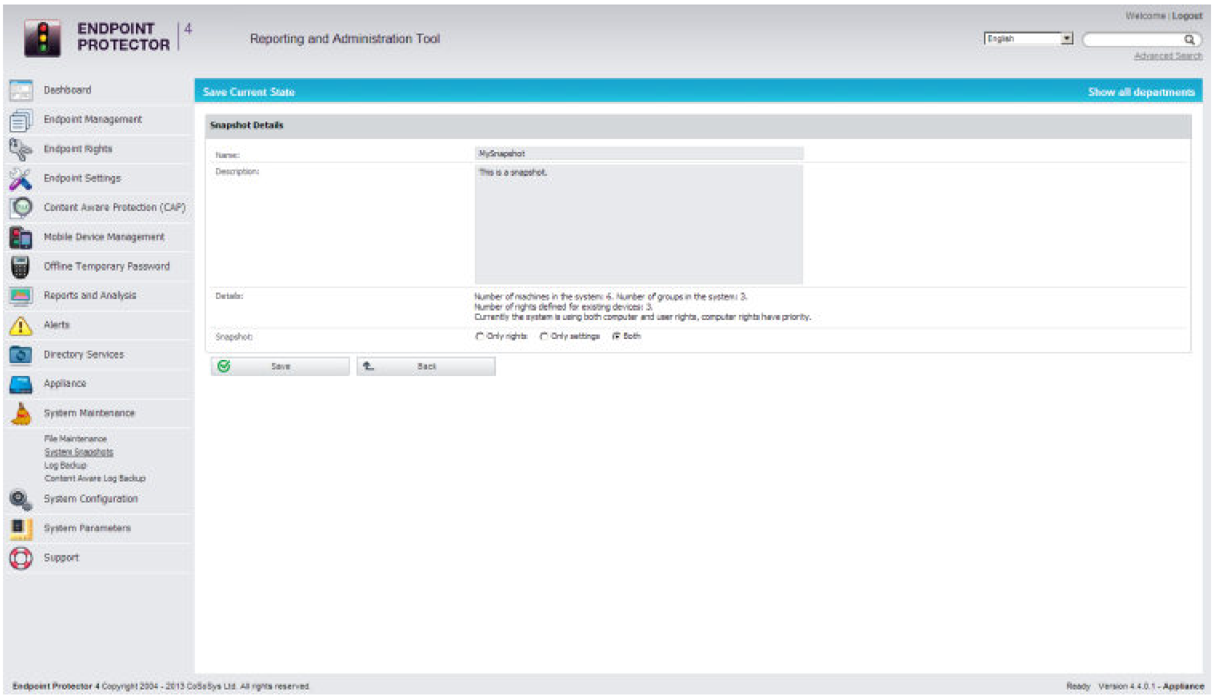
To archive a previously selected set of files, click the “Save as Zip” button, while to permanently remove a set of files from the Endpoint Protector Server use the “Delete” button.

14.2. 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 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”.



Save Current State

Snapshot Details

Name: MySnapshot

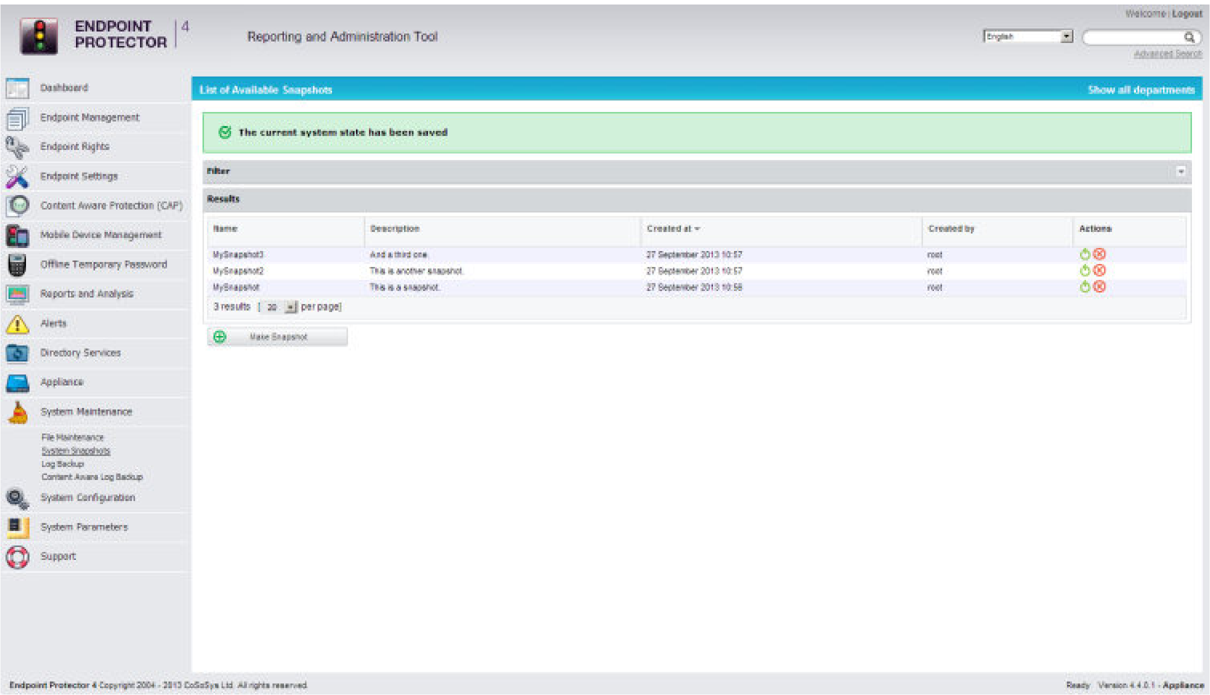
Description: This is a snapshot.

Details: Number of machines in the system: 6. Number of groups in the system: 3.
Number of rights defined for existing devices: 3.
Currently the system is using both computer and user rights, computer rights have priority.

Snapshot: ○ Only rights ○ Only settings ● Both

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”.



The current system state has been saved

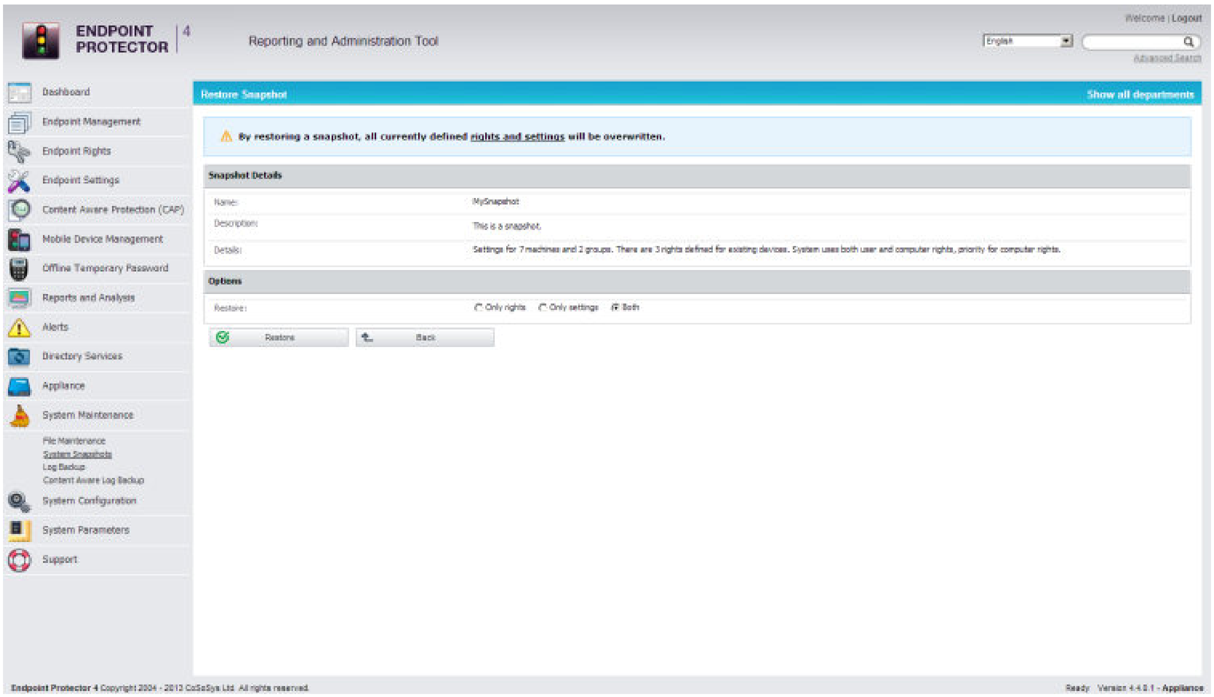
Name	Description	Created at ▾	Created by	Actions
MySnapshot3	And a third one.	27 September 2013 10:57	root	↻ ⊗
MySnapshot2	This is another snapshot.	27 September 2013 10:57	root	↻ ⊗
MySnapshot	This is a snapshot.	27 September 2013 10:56	root	↻ ⊗

3 results [20 ▾ per page]

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.



By restoring a snapshot, all currently defined rights and settings will be overwritten.

Snapshot Details

Name:	MySnapshot
Description:	This is a snapshot.
Details:	Settings for 7 machines and 2 groups. There are 3 rights defined for existing devices. System uses both user and computer rights, priority for computer rights.

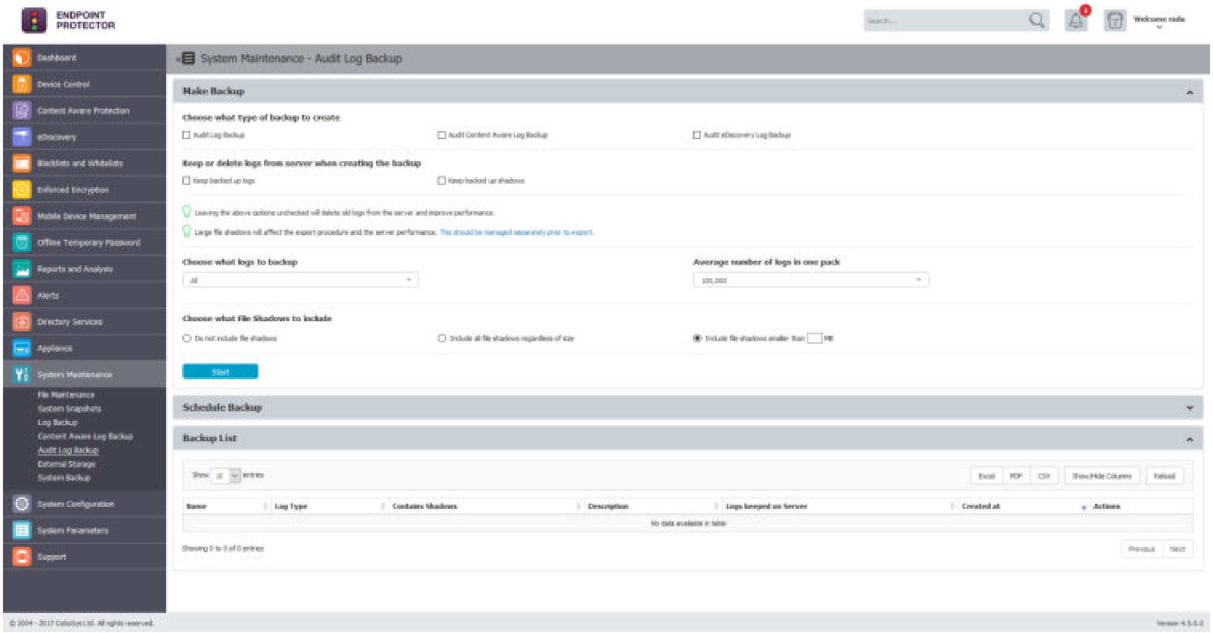
Options

Restore: ○ Only rights ○ Only settings ● Both

14.3. 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.



System Maintenance - Audit Log Backup

Make Backup

Choose what type of backup to create

□ Audit Log Backup □ Audit Content Aware Log Backup □ Audit eDiscovery Log Backup

Keep or delete logs from server when creating the backup

□ Keep backed up logs □ Keep backed up shadows

Leaving the above options unchecked will delete old logs from the server and improve performance.

Large file shadows will affect the export procedure and the server performance. This should be managed separately prior to export.

Choose what logs to backup: All

Average number of logs in one pack: 100,000

Choose what File Shadows to include

○ Do not include file shadows ○ Include all file shadows regardless of size ● Include file shadows smaller than ☐ MB

Start

Schedule Backup

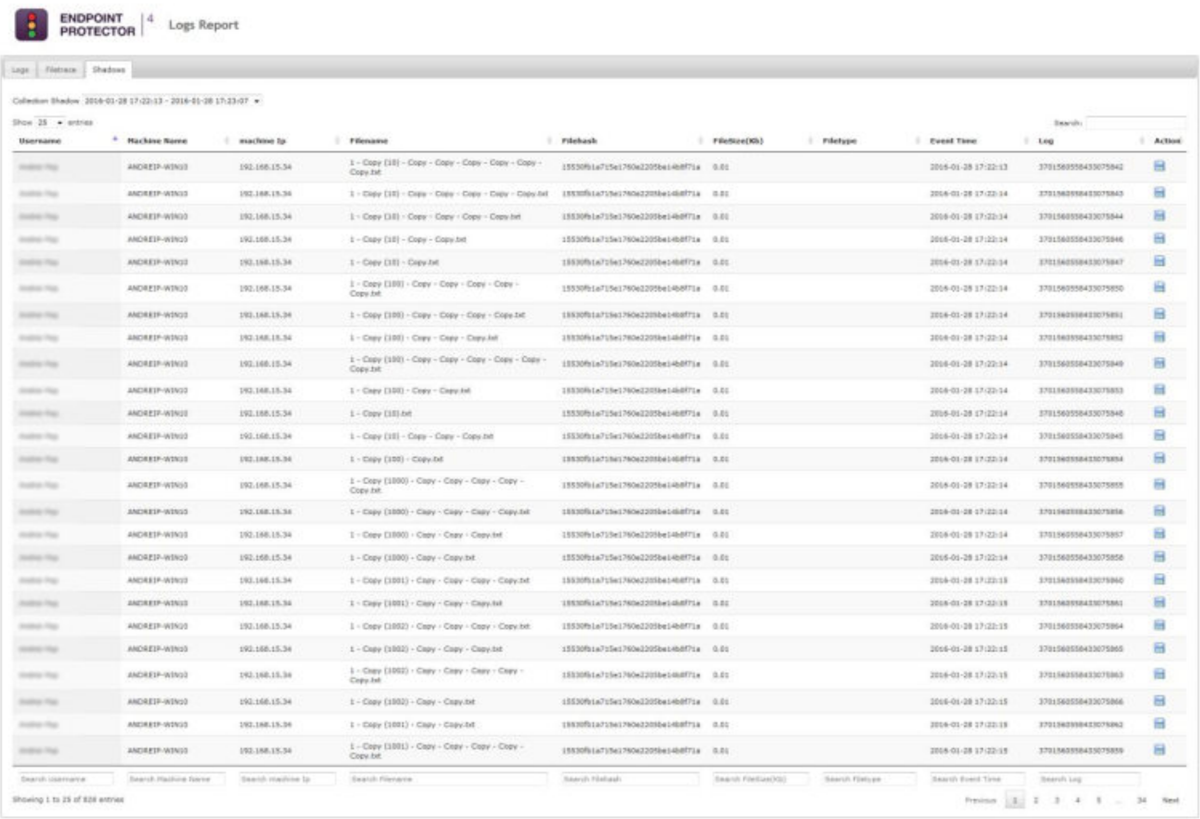
Backup List

Show 10 entries — Excel PDF CSV Show/Hide Columns Reload

Name	Log Type	Contains Shadows	Description	Logs keeped on Server	Created at	Actions
No data available in table						

Showing 0 to 0 of 0 entries — Previous Next

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.



Collection Shadow 2016-01-28 17:22:13 - 2016-01-28 17:23:07

Show 25 entries

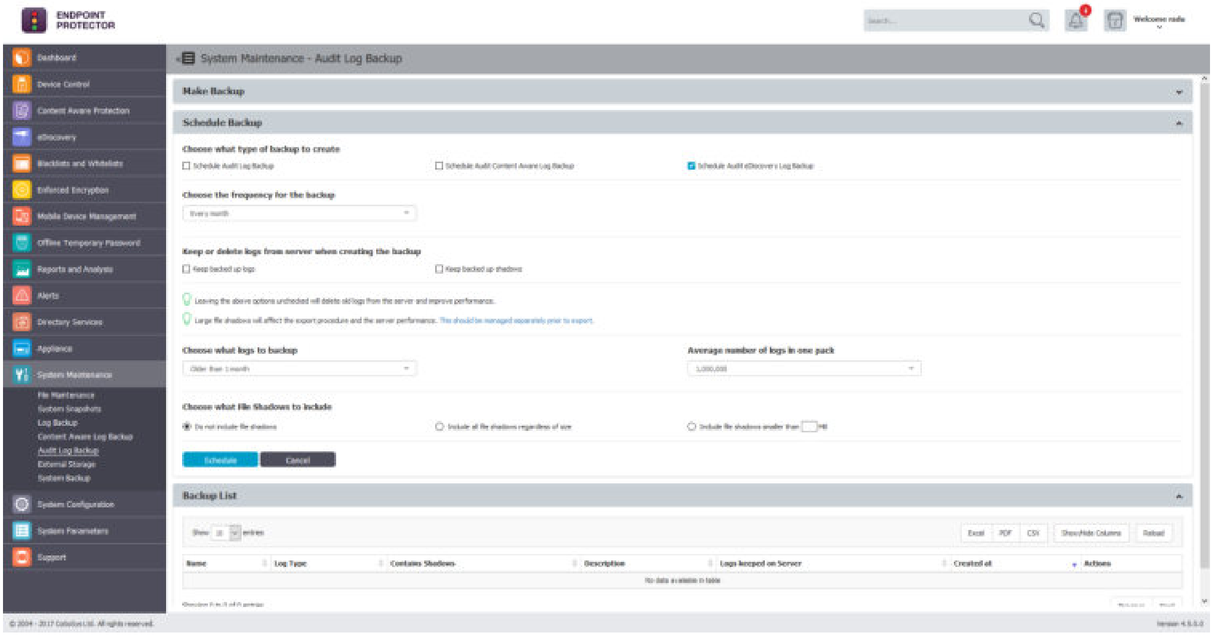
Search:

Username	Machine Name	machine Ip	Filename	Filehash	FileSize(Kb)	Filetype	Event Time	Log	Action
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:13	3701560558433075842	
[redacted]	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	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075844	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075846	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075847	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075850	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075851	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075852	
[redacted]	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	3701560558433075849	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075853	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10).txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075848	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (10) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075845	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (100) - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075854	
[redacted]	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	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075856	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075857	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1000) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:14	3701560558433075858	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075860	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075861	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075864	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075865	
[redacted]	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	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1002) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075866	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075862	
[redacted]	ANDREIP-WIN10	192.168.15.34	1 - Copy (1001) - Copy - Copy - Copy - Copy - Copy.txt	15530fb1a715e1760e2205be14b8f71a	0.01		2016-01-28 17:22:15	3701560558433075859	
Search Username	Search Machine Name	Search machine Ip	Search Filename	Search Filehash	Search FileSize(Kb)	Search Filetype	Search Event Time	Search Log	

Showing 1 to 25 of 828 entries

14.3.1. 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.).



System Maintenance - Audit Log Backup

Make Backup

Schedule Backup

Choose what type of backup to create

□ Schedule Audit Log Backup □ Schedule Audit Content Aware Log Backup ☑ Schedule Audit eDiscovery Log Backup

Choose the frequency for the backup: Every month

Keep or delete logs from server when creating the backup

□ Keep backed up logs □ Keep backed up shadows

Leaving the above options unchecked will delete old logs from the server and improve performance.

Large file shadows will affect the export procedure and the server performance. This should be managed separately prior to export.

Choose what logs to backup: Older than 1 month

Average number of logs in one pack: 1,000,000

Choose what File Shadows to include

● Do not include file shadows ○ Include all file shadows regardless of size ○ Include file shadows smaller than ☐ MB

Backup List

Show 10 entries

Name	Log Type	Contains Shadows	Description	Logs keeped on Server	Created at	Actions
No data available in table						

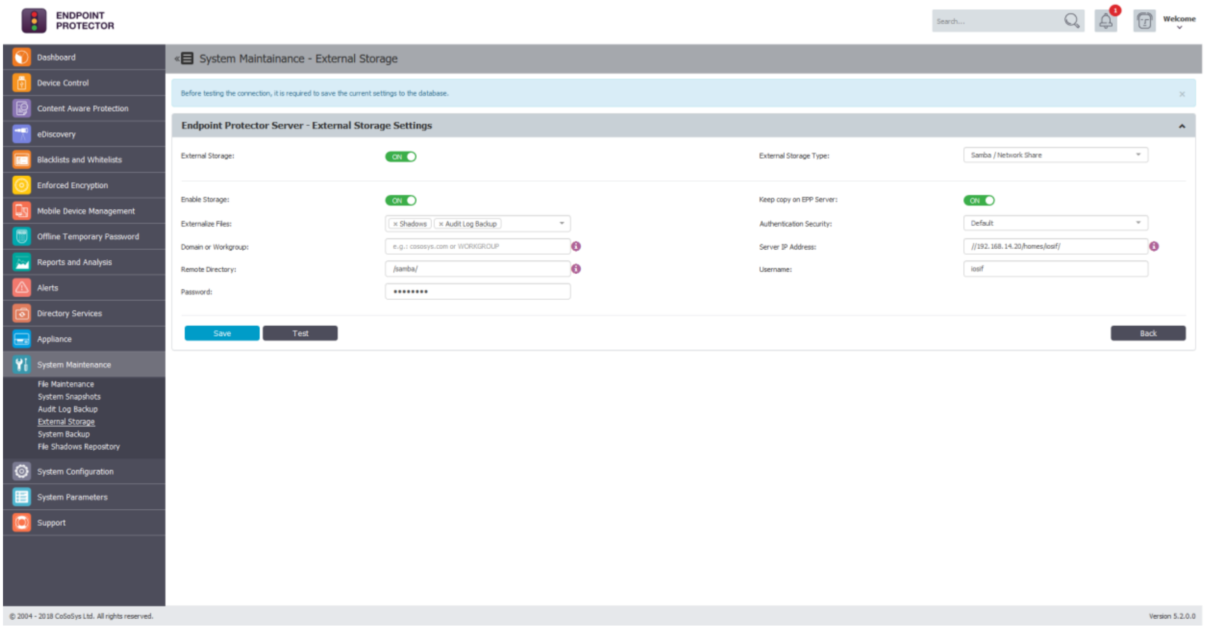
Showing 0 to 0 of 0 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 4.5.5.0

14.4. External Storage

From this section, the Administrator can externalize files generated by Endpoint Protector to a particular storage disk from the network. Files such as Shadows, Audit Log Backups and System Backups can be saved to an FTP, SFTP or Samba / Network Share server.



System Maintainance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage: ON

External Storage Type: Samba / Network Share

Enable Storage: ON

Keep copy on EPP Server: ON

Externalize Files: × Shadows × Audit Log Backup

Authentication Security: Default

Domain or Workgroup: e.g.: cososys.com or WORKGROUP

Server IP Address: //192.168.14.20/homes/iosif/

Remote Directory: /samba/

Username: iosif

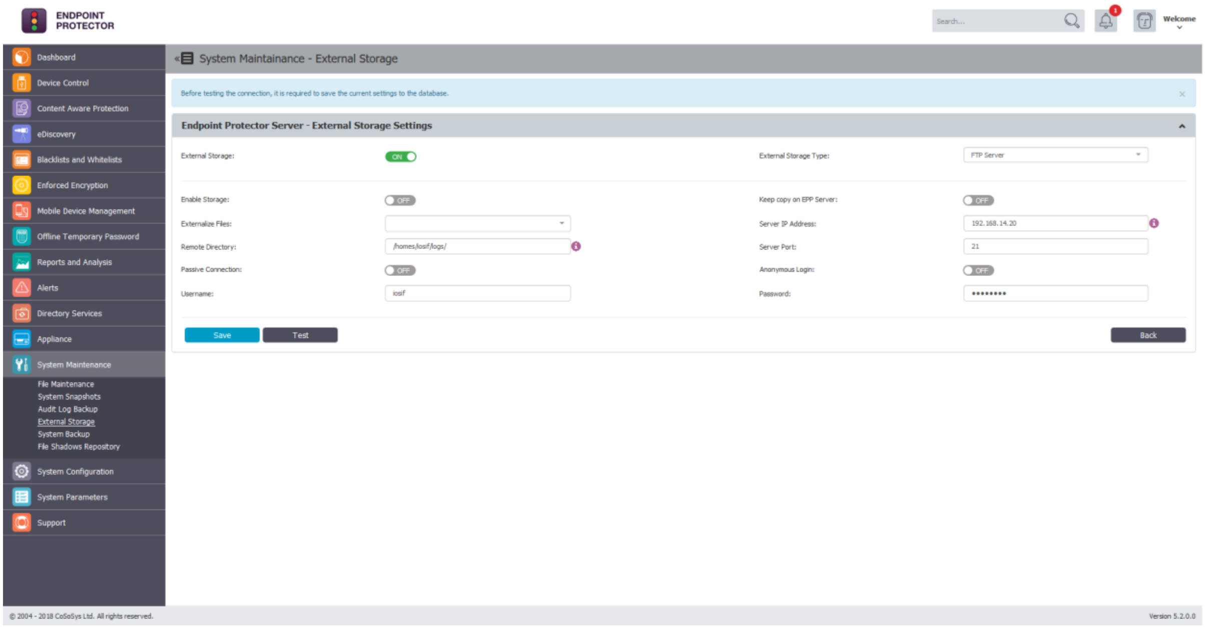
Password: •••••••••

> ⚠ **Note**
> The option to keep a copy of the files also on the Endpoint Protector Server can be turned ON or OFF for all External Storage Types.

14.4.1. FTP Server

To configure an FTP Server, the following parameters need to be provided:

- **Externalize Files –** the Endpoint Protector files: Shadows, Audit Log Backups or System Backups
- **Authentication Security** – the security protocols: Default, NTLM, NTLMv2, NTLMSSP
- **Domain or Workgroup –** only where applicable
- **Server IP Address** – the IP of the external server
- **Remote Directory** – a specific location on the external directory
- **Username –** the username of the external server
- **Password** – the associated password



System Maintainance - External Storage

Before testing the connection, it is required to save the current settings to the database.

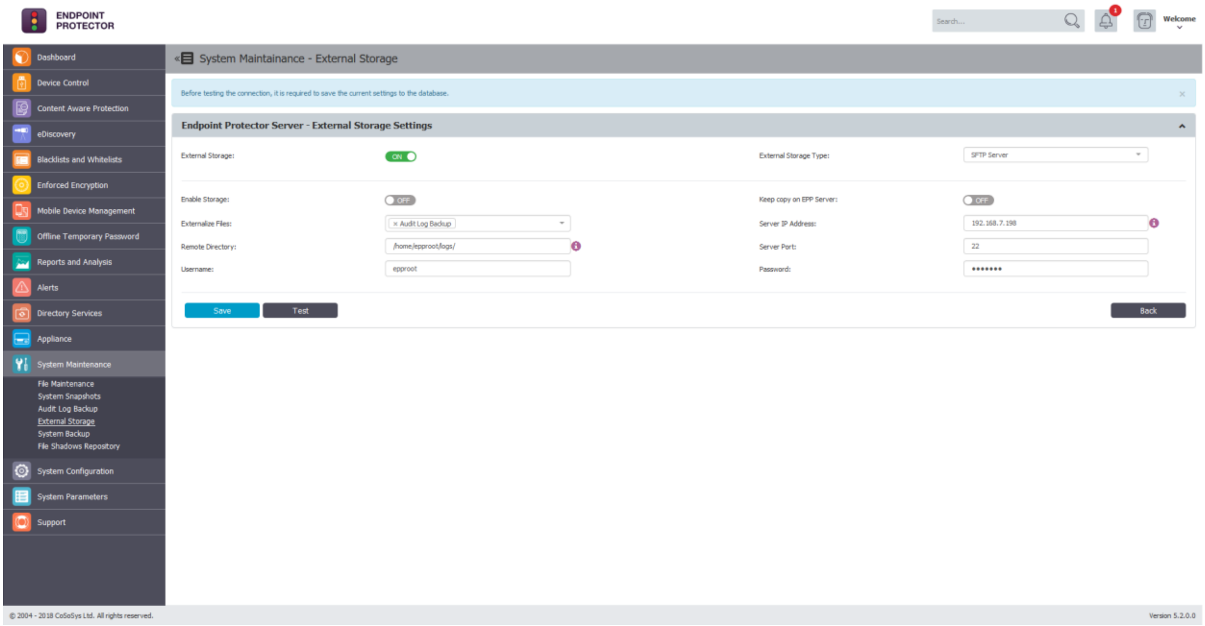
Endpoint Protector Server - External Storage Settings

External Storage: ON
External Storage Type: FTP Server
Enable Storage: OFF
Keep copy on EPP Server: OFF
Externalize Files:
Server IP Address: 192.168.14.20
Remote Directory: /homes/iosif/logs/
Server Port: 21
Passive Connection: OFF
Anonymous Login: OFF
Username: iosif
Password: ••••••••

14.4.2. SFTP Server

To configure an SFTP Server, the following parameters need to be provided:

- **Externalize Files –** the Endpoint Protector files: Shadows, Audit Log Backups or System Backups
- **Server IP Address** – the IP of the external server
- **Remote Directory** – a specific location on the external directory
- **Server Port** – the port of the external storage server
- **Username –** the username of the external server
- **Password** – the associated password



System Maintainance - External Storage

Before testing the connection, it is required to save the current settings to the database.

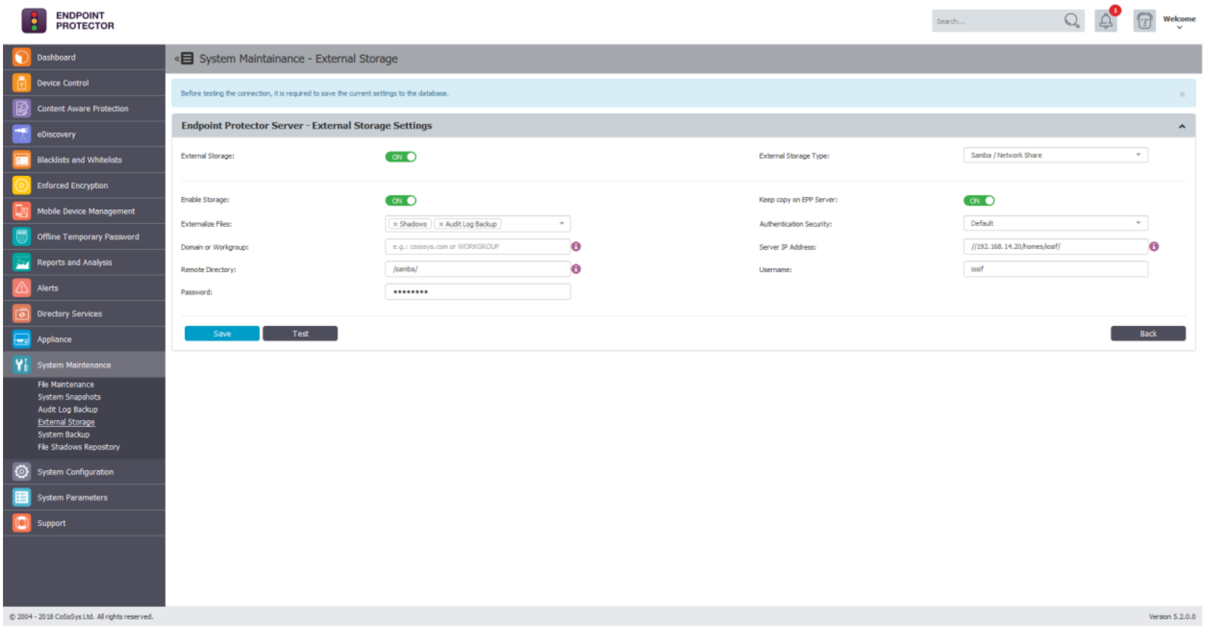
Endpoint Protector Server - External Storage Settings

External Storage: ON
External Storage Type: SFTP Server
Enable Storage: OFF
Keep copy on EPP Server: OFF
Externalize Files: × Audit Log Backup
Server IP Address: 192.168.7.198
Remote Directory: /home/epproot/logs/
Server Port: 22
Username: epproot
Password: •••••••

14.4.3. Samba / Network Share Server

To configure a Samba / Network Share Server, the following parameters need to be provided:

- **Externalize Files –** the Endpoint Protector files: Shadows, Audit Log Backups or System Backups
- **Authentication Security** – the security protocols: Default, NTLM, NTLMv2, NTLMSSP
- **Domain or Workgroup –** only where applicable
- **Server IP Address** – the IP of the external server
- **Remote Directory** – a specific location on the external directory
- **Username –** the username of the external server
- **Password** – the associated password



System Maintainance - External Storage

Before testing the connection, it is required to save the current settings to the database.

Endpoint Protector Server - External Storage Settings

External Storage:	ON	External Storage Type:	Samba / Network Share
Enable Storage:	ON	Keep copy on EPP Server:	ON
Externalize Files:	× Shadows × Audit Log Backup	Authentication Security:	Default
Domain or Workgroup:	e.g.: cososys.com or WORKGROUP	Server IP Address:	//192.168.14.20/homes/iosif/
Remote Directory:	/samba/	Username:	iosif
Password:	•••••••••		

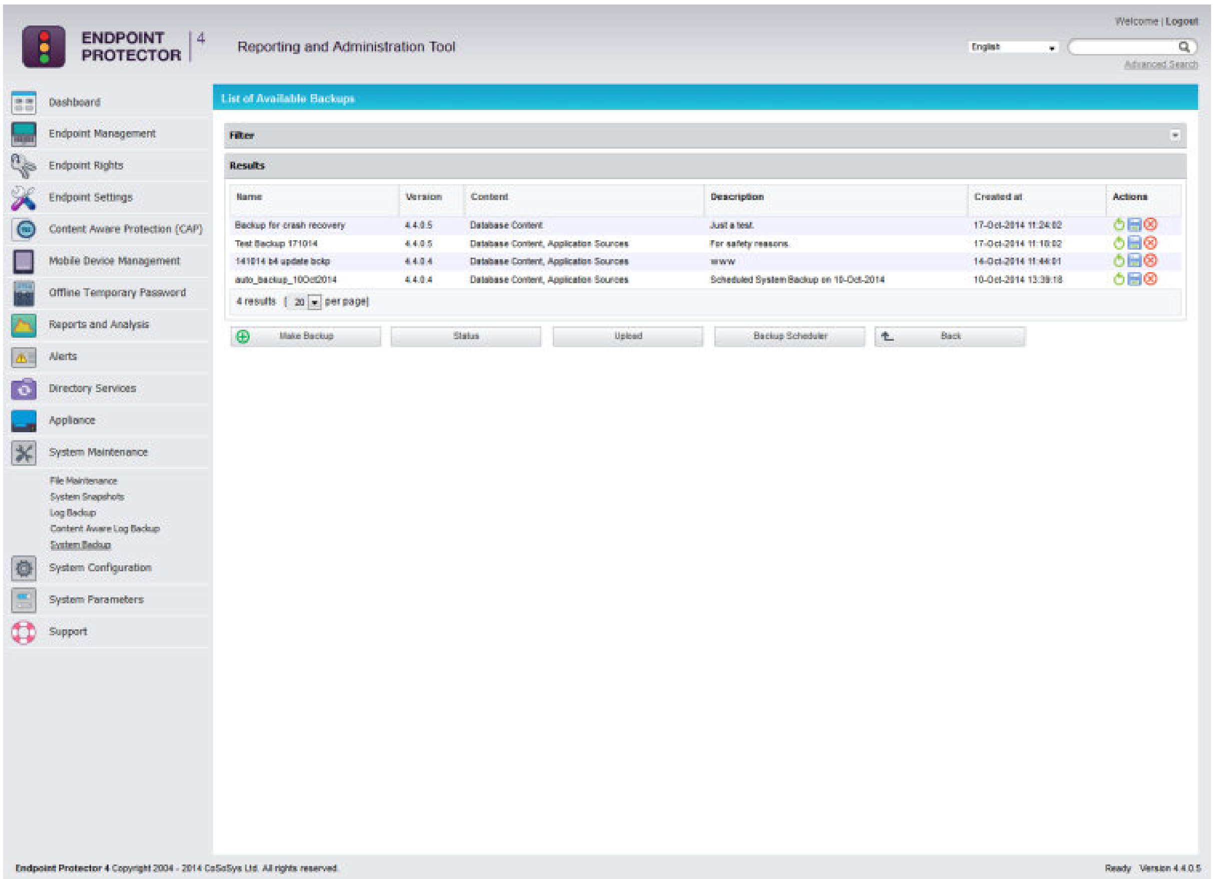
© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0

14.5. System Backup

14.5.1. From the Web Interface

This module allows the administrator to make complete system backups.



List of Available Backups

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

4 results [20 per page]

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!

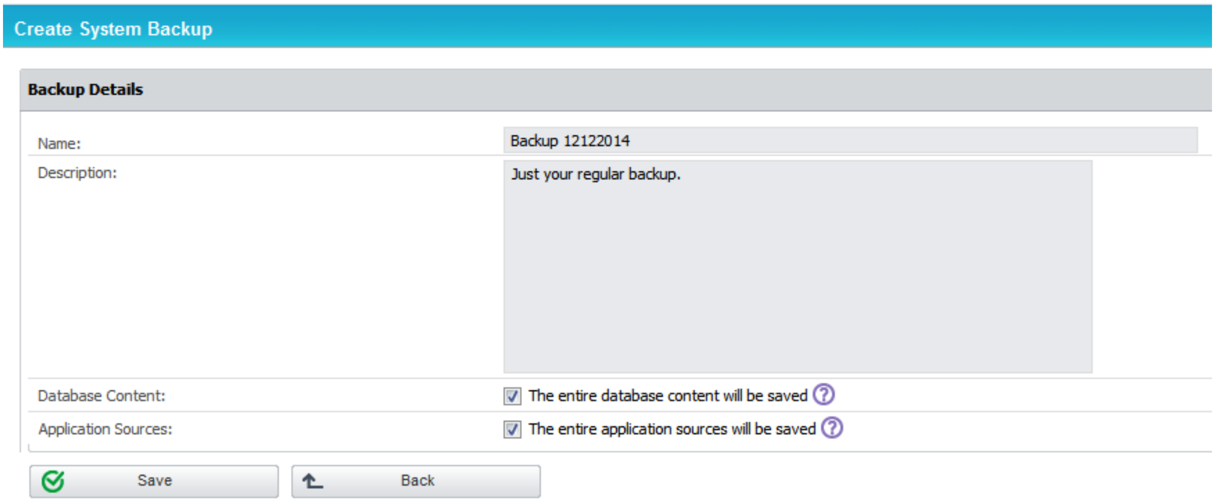
We recommend asking for Support assistance at support@endpointprotector.com when using the Restore Backup feature.

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: Backup 12122014

Description: Just your regular backup.

Database Content: ☑ The entire database content will be saved

Application Sources: ☑ The entire application sources will be saved

The administrator is presented here with two options:

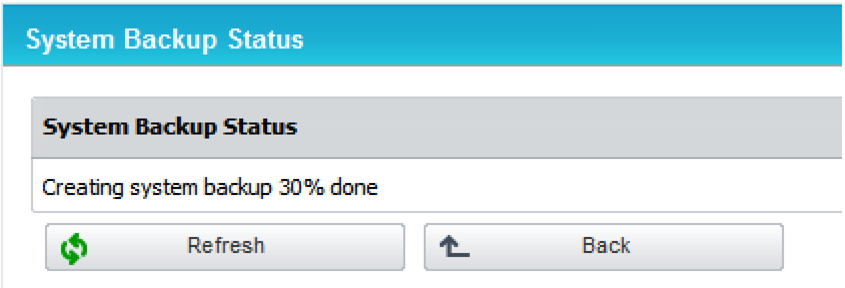
- To save the **Database content**. This option will make the backup file contain all the devices, rights, logs, settings and policies present on the EPP server at the making of the backup.

- To save the **Application sources**. This option will make the backup contain files such as the EPP clients and others related to the proper functioning of the server.

Note!

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

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



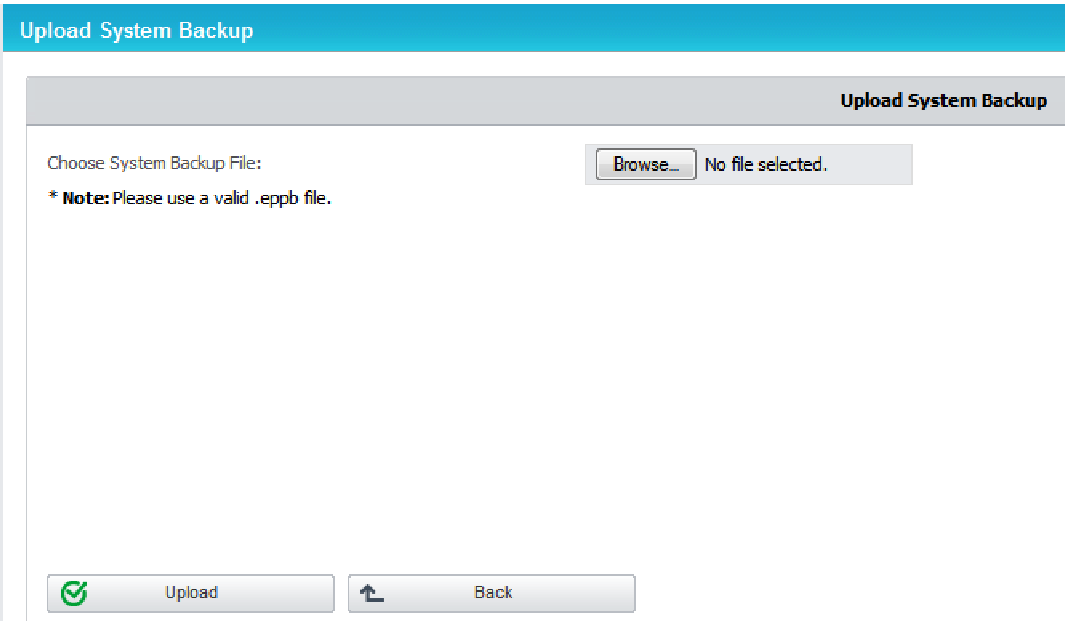
System Backup Status

System Backup Status

Creating system backup 30% done

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:



Upload System Backup

Upload System Backup

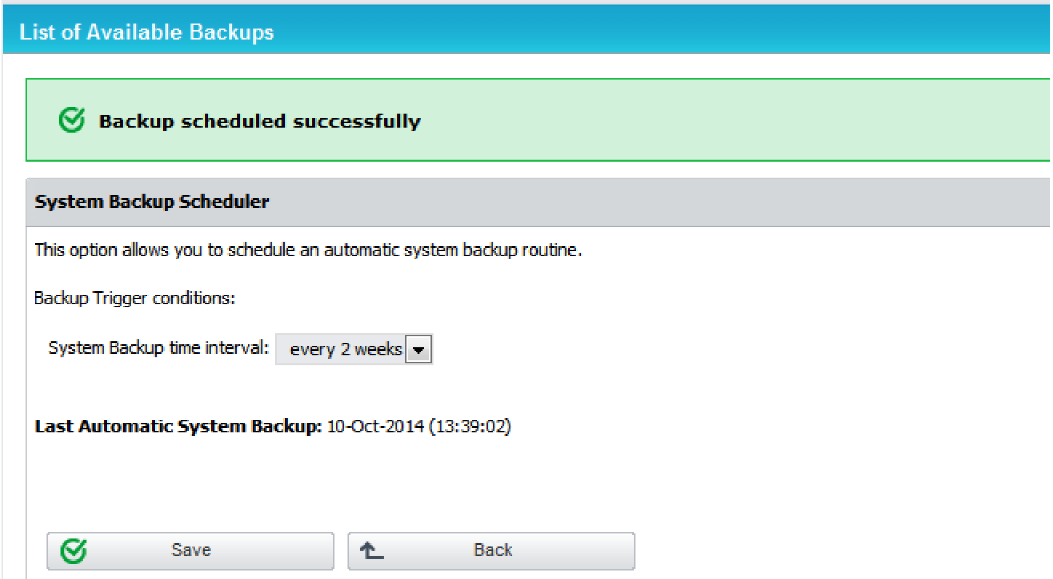
Choose System Backup File: No file selected.

* **Note:** Please use a valid .eppb file.

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 Available Backups

Backup scheduled successfully

System Backup Scheduler

This option allows you to schedule an automatic system backup routine.

Backup Trigger conditions:

System Backup time interval: every 2 weeks

Last Automatic System Backup: 10-Oct-2014 (13:39:02)

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.

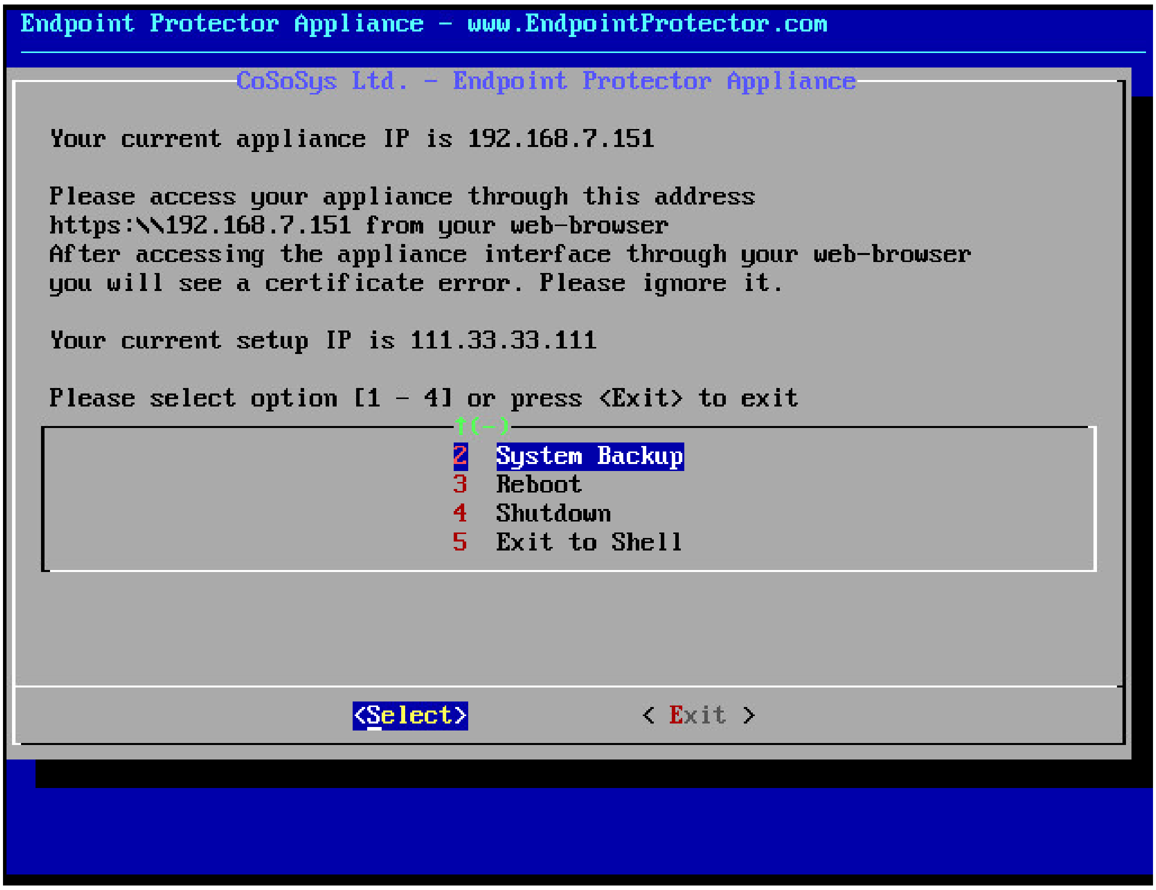
The Scheduler will also prompt the administrator with the **Last Automatic System Backup reminder**.

Note!

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

14.5.2. 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.



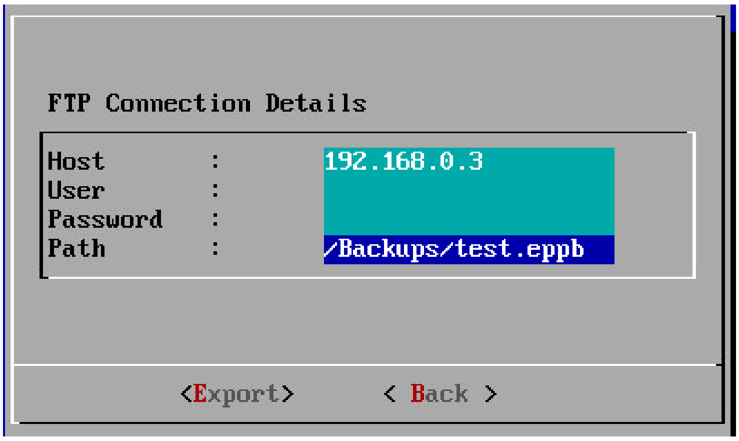
```
Endpoint Protector Appliance - www.EndpointProtector.com

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
```

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

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



FTP Connection Details

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

14.6. System Backup v2

From this section, the Administrator can migrate the database (entities, rights, settings, policies, configurations, etc.) from an older Endpoint Protector Server to a newer one.

⚠ **Note**

This feature is not intended as a replacement for the System Backup functionality but rather as a migration tool from older Endpoint Protector images to the ones starting with version 5.2.0.6.

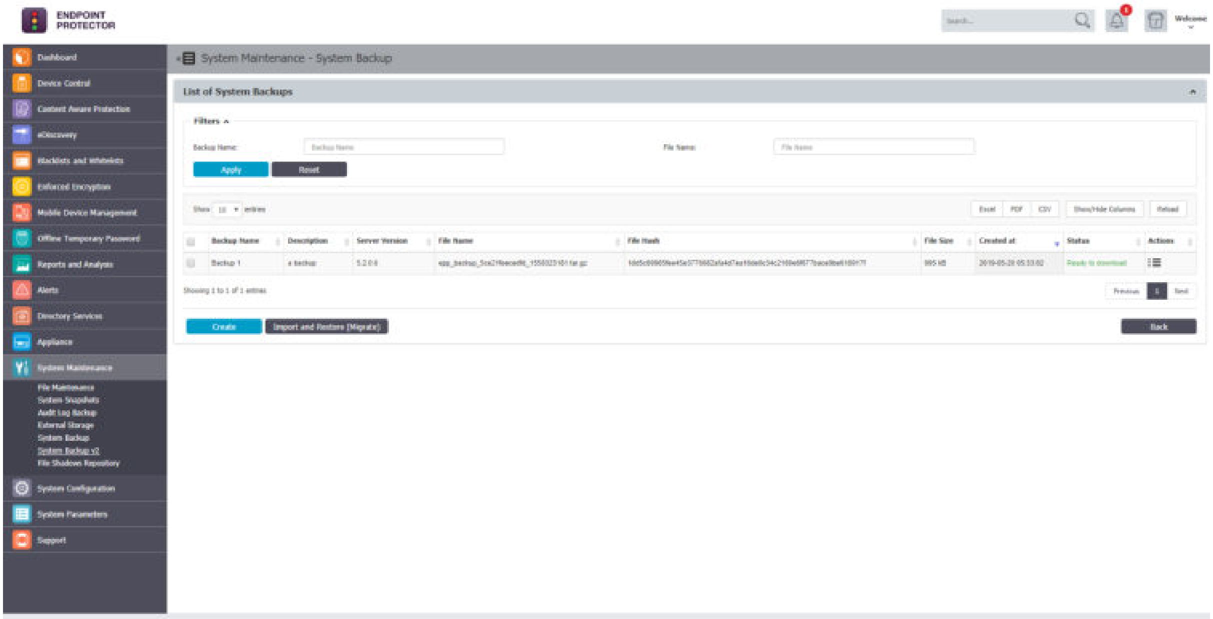
⚠ **Note**

It does not include logs, Audits or System Backups. If needed, these should be downloaded before proceeding.

⚙ **Example**

The initial Endpoint Protector deployed was version 4.4.0.7. Over time, updates were applied though the Live Update section, bringing the appliance to Endpoint Protector version 5.2.0.6. While these constantly included patches and security updates, they did not include a full rollout of a new core OS version (e.g.: the appliance is still running on Ubuntu 14.04 LTS).

As Ubuntu 14.04 no longer receives security patches since 2019, those that want to migrate to a Server running on the latest Ubuntu LTS version should take advantage of this functionality.



Backup Name: Backup Name

File Name: File Name

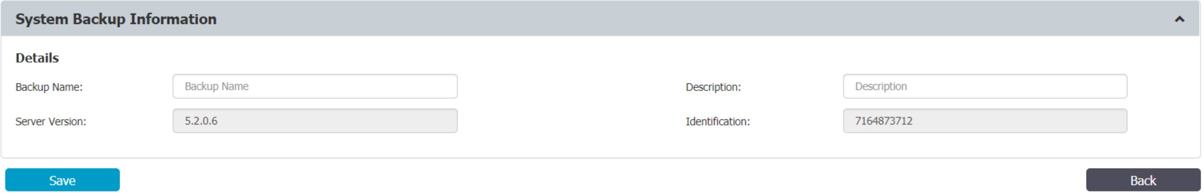
Show 10 entries

	Backup Name	Description	Server Version	File Name	File Hash	File Size	Created at	Status	Actions
□	Backup 1	a backup	5.2.0.6	epp_backup_5ca2f6eacedfd_1556023161.tar.gz	[illegible]	995 kB	2019-05-28 05:33:02	Ready to download	

Showing 1 to 1 of 1 entries

14.6.1. Creating a System Backup v2 (Migration)

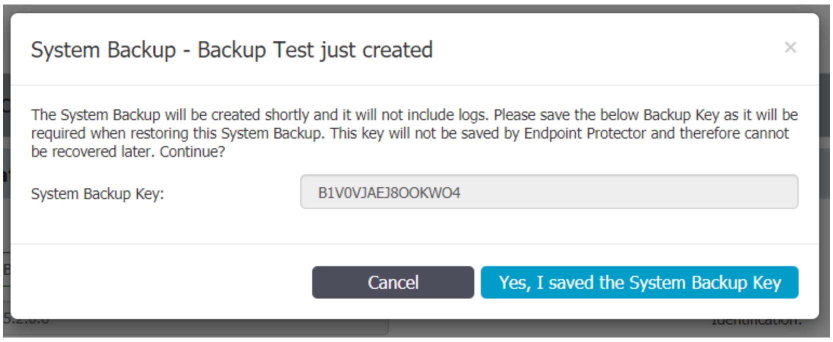
The Administrator can create a new migration backup from the System Maintenance > System Backup v2 section. This requires a Name and a Description.



Backup Name:	Backup Name	Description:	Description
Server Version:	5.2.0.6	Identification:	7164873712

Note

For security purposes, the System Backup Key will not be stored by Endpoint Protector. Before proceeding, make sure it is properly saved.


System Backup - Backup Test just created
×
Cancel
Yes, I saved the System Backup Key

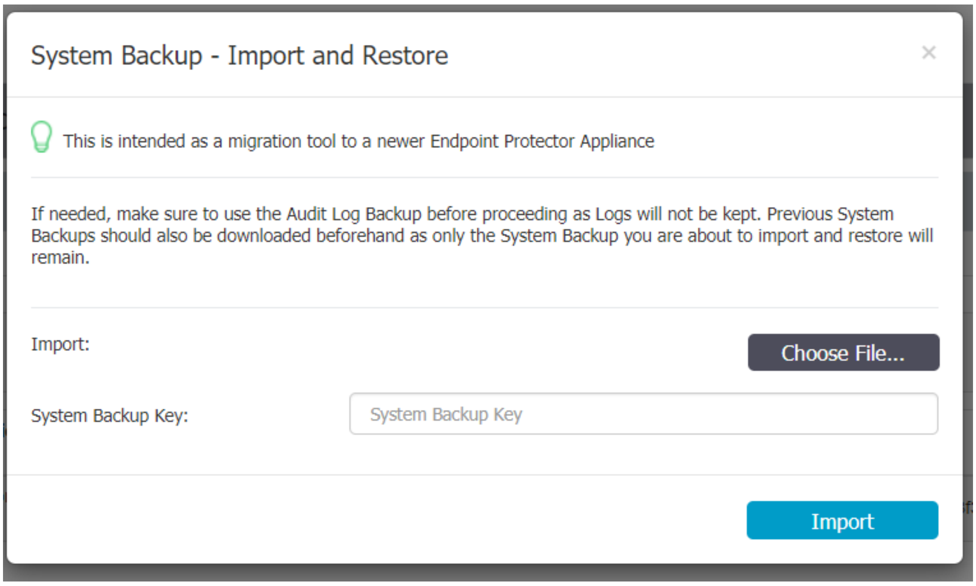
The System Backup will be created shortly and it will not include logs. Please save the below Backup Key as it will be required when restoring this System Backup. This key will not be saved by Endpoint Protector and therefore cannot be recovered later. Continue?

System Backup Key: B1V0VJAEJ8OOKWO4

14.6.2. Importing and Restore (Migrate)

A Backup can be restored on the same Endpoint Protector Server. However, the main use case would be to import and restore the backup on a newer Endpoint Protector Server (e.g.: version higher 5.2.0.6).

The migration process of a System Backup requires the backup file and System Backup Key.



System Backup - Import and Restore

This is intended as a migration tool to a newer Endpoint Protector Appliance

If needed, make sure to use the Audit Log Backup before proceeding as Logs will not be kept. Previous System Backups should also be downloaded beforehand as only the System Backup you are about to import and restore will remain.

Import:

System Backup Key:

Note

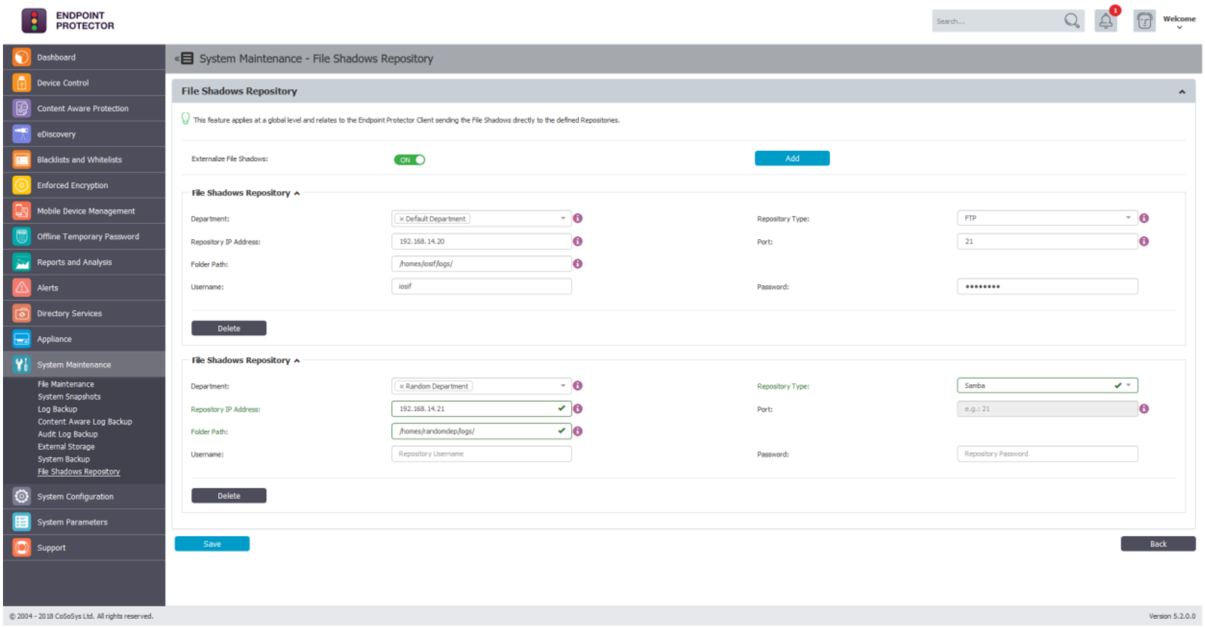
If needed, previous System Backups or Audit Log Backups should be downloaded prior to this step, as they will not be kept in process.

Information

After the Import and Restore (Migration) has been made to the new Appliance, the old Appliance should be turned off. It's IP would then have to be reassigned to the new Appliance in order for the deployed Endpoint Protector Clients to start communicating with the new Appliance.

14.7. File Shadow Repository

From this section, the Administrator can manage File Shadows Repositories. This feature allows the Endpoint Protector Client to send File Shadows directly to an externalized location.



System Maintenance - File Shadows Repository

File Shadows Repository

This feature applies at a global level and relates to the Endpoint Protector Client sending the File Shadows directly to the defined Repositories.

Externalize File Shadows: ON

File Shadows Repository

Department: × Default Department
Repository Type: FTP
Repository IP Address: 192.168.14.20
Port: 21
Folder Path: /homes/iosif/logs/
Username: iosif
Password: ••••••••

File Shadows Repository

Department: × Random Department
Repository Type: Samba
Repository IP Address: 192.168.14.21
Port: e.g.: 21
Folder Path: /homes/randomdep/logs/
Username: Repository Username
Password: Repository Password

Multiple File Shadow Repositories can be created and the option to specify how each endpoint manages the File Shadows is based on Department.

Information

In Endpoint Protector, the Department defines a collection of entities with the same attributes. It should not be confused with the department from an organizational chart.

In order to add a File Shadow Repository, the following things should be configured: Department, Repository Type, Repository IP Address, Port, Folder Path, Username and Password.

Information

Depending on the Repository Type – FTP or Samba – the Port may not be required and will be greyed out.

15. System Configuration

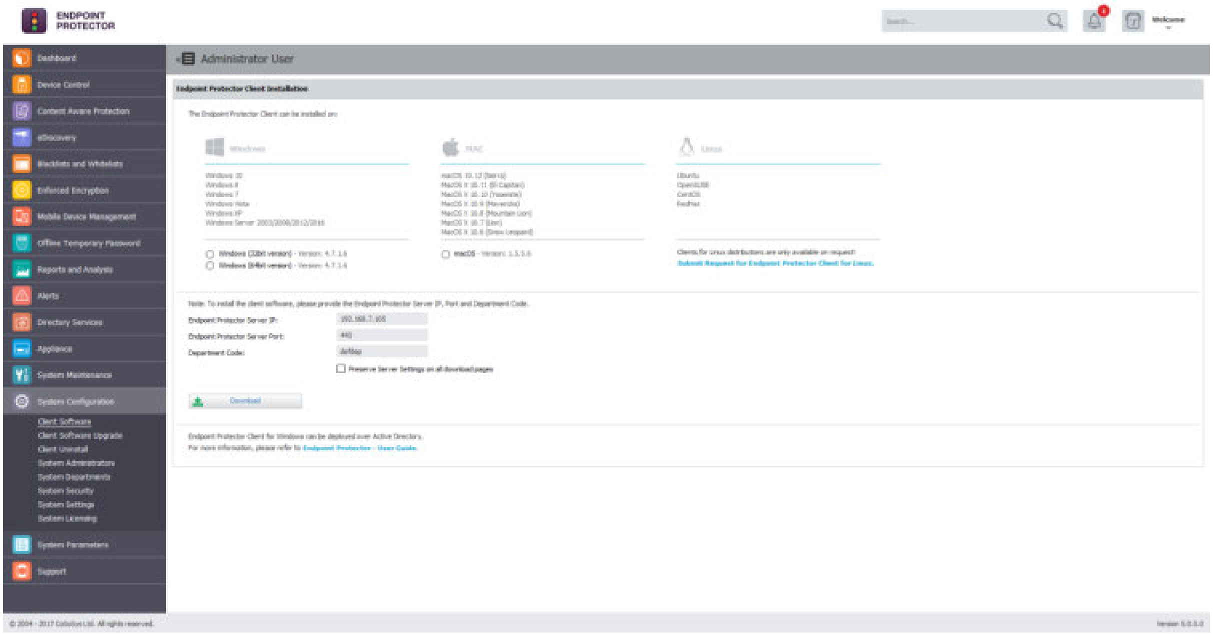
This section contains the Endpoint Protector Clients, System Licensing and other advanced settings, which influence the functionality and stability of the system.

15.1. Client Software

From this section, the administrator can download and install the Endpoint Protector Client corresponding to the used operating system.

Information

The Server and Client communicate through port 443.



Endpoint Protector Client Installation

The Endpoint Protector Client can be installed on:

Windows

Windows 10
Windows 8
Windows 7
Windows Vista
Windows XP
Windows Server 2003/2008/2012/2016

○ Windows (32bit version) - Version: 4.7.1.6
○ Windows (64bit version) - Version: 4.7.1.6

MAC

macOS 10.12 (Sierra)
MacOS X 10.11 (El Capitan)
MacOS X 10.10 (Yosemite)
MacOS X 10.9 (Mavericks)
MacOS X 10.8 (Mountain Lion)
MacOS X 10.7 (Lion)
MacOS X 10.6 (Snow Leopard)

○ macOS - Version: 1.5.5.6

Linux

Ubuntu
OpenSUSE
CentOS
RedHat

Clients for Linux distributions are only available on request!
Submit Request for Endpoint Protector Client for Linux.

Note: To install the client software, please provide the Endpoint Protector Server IP, Port and Department Code.

Endpoint Protector Server IP: 192.168.7.105
Endpoint Protector Server Port: 443
Department Code: defdep
□ Preserve Server Settings on all download pages

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

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 5.0.0.0

Tips

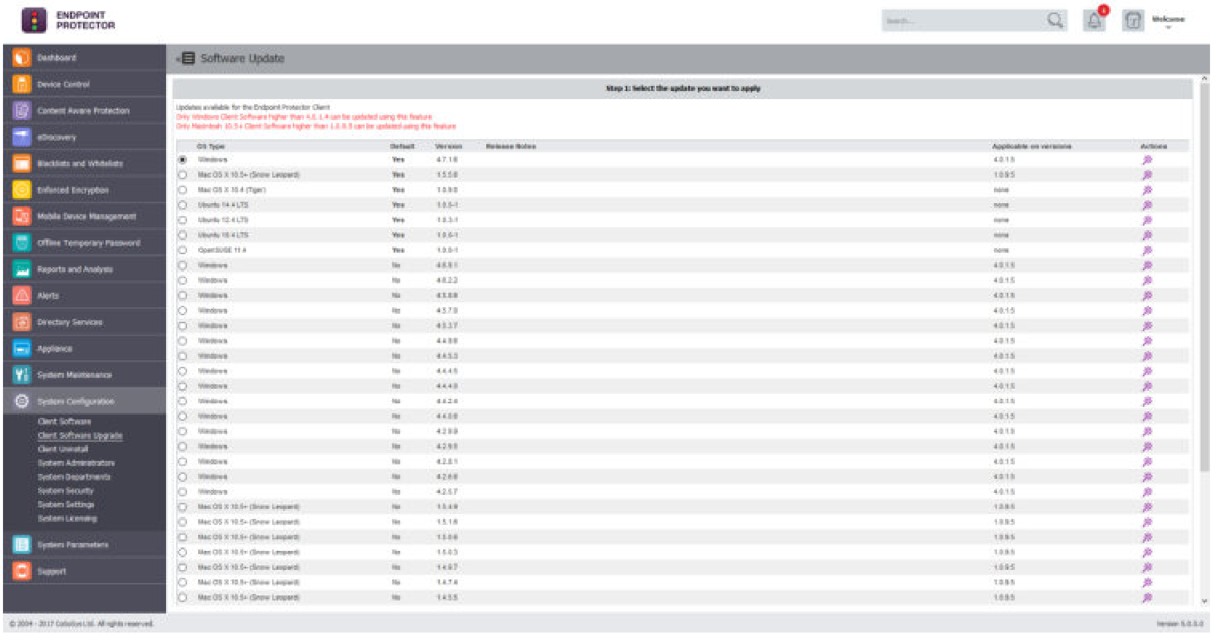
The Windows Client installers offer the option to download the package with or without add-ons. This option fixes any incompatibility that may arise between Endpoint Protector and the specific solutions.

15.2. Client Software Upgrade

From this section, the Administrator can perform automatic update of the installed Endpoint Protector Client.

Note

The feature is not available for Linux clients. Also, for really old versions (e.g. Windows Client version lower than 4.0.1.4), the update will not work.



Step 1: Select the update you want to apply

Updates available for the Endpoint Protector Client
Only Windows Client Software higher than 4.0.1.4 can be updated using this feature
Only Macintosh 10.5+ Client Software higher than 1.0.9.5 can be updated using this feature

	OS Type	Default	Version	Release Notes	Applicable on versions	Actions
●	Windows	Yes	4.7.1.6		4.0.1.5	
○	Mac OS X 10.5+ (Snow Leopard)	Yes	1.5.5.8		1.0.9.5	
○	Mac OS X 10.4 (Tiger)	Yes	1.0.9.0		none	
○	Ubuntu 14.4 LTS	Yes	1.0.5-1		none	
○	Ubuntu 12.4 LTS	Yes	1.0.3-1		none	
○	Ubuntu 16.4 LTS	Yes	1.0.6-1		none	
○	OpenSUSE 11.4	Yes	1.0.0-1		none	
○	Windows	No	4.6.9.1		4.0.1.5	
○	Windows	No	4.6.2.2		4.0.1.5	
○	Windows	No	4.5.8.8		4.0.1.5	
○	Windows	No	4.5.7.5		4.0.1.5	
○	Windows	No	4.5.3.7		4.0.1.5	
○	Windows	No	4.4.9.8		4.0.1.5	
○	Windows	No	4.4.5.3		4.0.1.5	
○	Windows	No	4.4.4.5		4.0.1.5	
○	Windows	No	4.4.4.0		4.0.1.5	
○	Windows	No	4.4.2.6		4.0.1.5	
○	Windows	No	4.4.0.8		4.0.1.5	
○	Windows	No	4.2.9.9		4.0.1.5	
○	Windows	No	4.2.9.5		4.0.1.5	
○	Windows	No	4.2.8.1		4.0.1.5	
○	Windows	No	4.2.6.8		4.0.1.5	
○	Windows	No	4.2.5.7		4.0.1.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.5.4.8		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.5.1.6		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.5.0.6		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.5.0.3		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.4.9.7		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.4.7.4		1.0.9.5	
○	Mac OS X 10.5+ (Snow Leopard)	No	1.4.5.5		1.0.9.5	

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

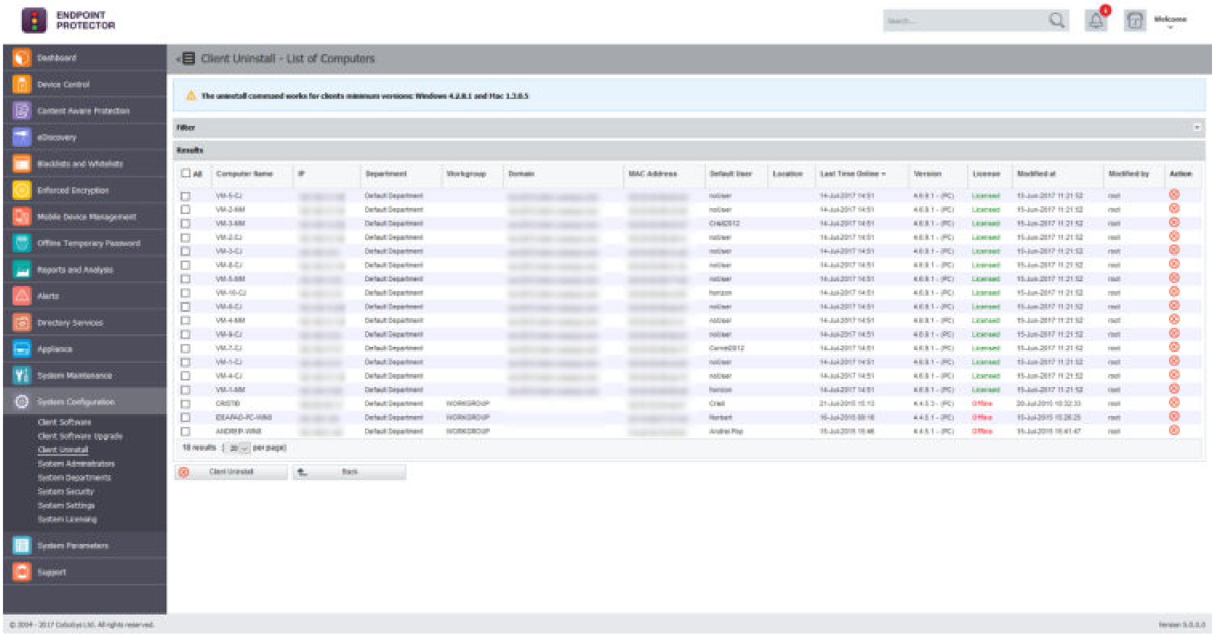
Version 5.0.0.0

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

15.3. Client Uninstall

From this section, the Administrator can perform a remote uninstall of the Endpoint Protector Client.

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



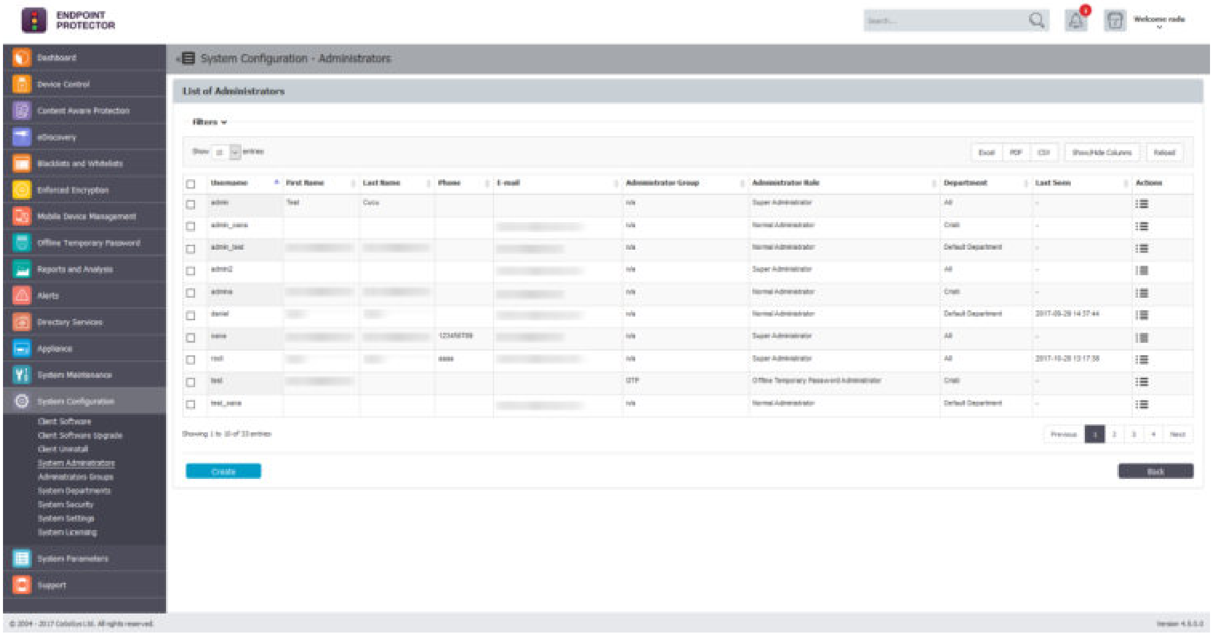
The uninstall command works for clients minimum versions: Windows 4.2.8.1 and Mac 1.3.0.5

□ All	Computer Name	IP	Department	Workgroup	Domain	MAC Address	Default User	Location	Last Time Online	Version	License	Modified at	Modified by	Action
□	VM-5-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-2-MM	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-3-MM	[redacted]	Default Department		[redacted]	[redacted]	Crist2012		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-2-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-3-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-8-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-5-MM	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-10-CJ	[redacted]	Default Department		[redacted]	[redacted]	horizon		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-6-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-4-MM	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-9-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-7-CJ	[redacted]	Default Department		[redacted]	[redacted]	Carme2012		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-1-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-4-CJ	[redacted]	Default Department		[redacted]	[redacted]	noUser		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	VM-1-MM	[redacted]	Default Department		[redacted]	[redacted]	horizon		14-Jul-2017 14:51	4.6.9.1 - (PC)	Licensed	15-Jun-2017 11:21:52	root	⊗
□	CRISTB	[redacted]	Default Department	WORKGROUP		[redacted]	Crist		21-Jul-2015 15:13	4.4.5.3 - (PC)	Offline	20-Jul-2015 10:32:33	root	⊗
□	IDEAPAD-PC-WIN8	[redacted]	Default Department	WORKGROUP		[redacted]	Herbert		16-Jul-2015 00:16	4.4.5.1 - (PC)	Offline	15-Jul-2015 15:28:25	root	⊗
□	ANDREIP-WIN8	[redacted]	Default Department	WORKGROUP		[redacted]	Andrei Pop		15-Jul-2015 15:46	4.4.5.1 - (PC)	Offline	15-Jul-2015 15:41:47	root	⊗

18 results (20 per page)

15.4. System Administrators

This section allows the creation of new Administrators. Once administrators are created, a list containing all the administrators will be displayed. Options to editing details and settings or delete unwanted administrators are also available.

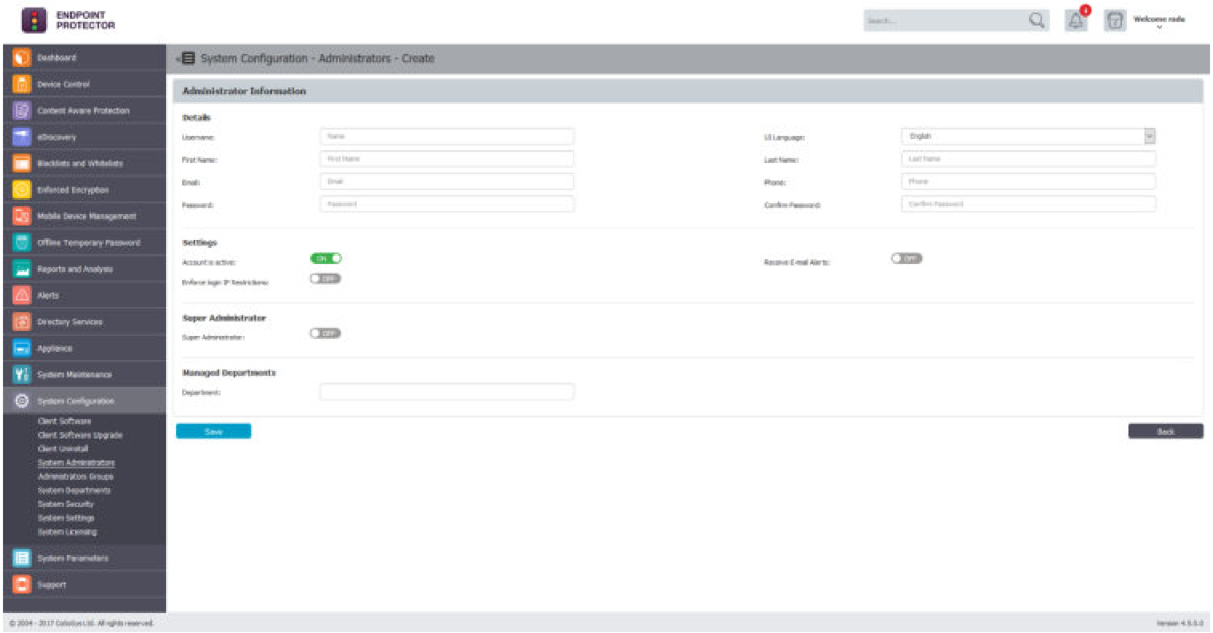


Show 10 entries

□	Username	First Name	Last Name	Phone	E-mail	Administrator Group	Administrator Role	Department	Last Seen	Actions
□	admin	Test	Cucu			n/a	Super Administrator	All	-	☰
□	admin_cucu				[redacted]	n/a	Normal Administrator	Craiti	-	☰
□	admin_test	[redacted]	[redacted]		[redacted]	n/a	Normal Administrator	Default Department	-	☰
□	admin2				[redacted]	n/a	Super Administrator	All	-	☰
□	admina	[redacted]	[redacted]		[redacted]	n/a	Normal Administrator	Craiti	-	☰
□	daniel	[redacted]	[redacted]		[redacted]	n/a	Normal Administrator	Default Department	2017-09-28 14:37:44	☰
□	ioana	[redacted]	[redacted]	123456789	[redacted]	n/a	Super Administrator	All	-	☰
□	root	[redacted]	[redacted]	4444	[redacted]	n/a	Super Administrator	All	2017-10-28 13:17:38	☰
□	test	[redacted]				OTP	Offline Temporary Password Administrator	Craiti	-	☰
□	test_ioana				[redacted]	n/a	Normal Administrator	Default Department	-	☰

Showing 1 to 10 of 33 entries

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.



System Configuration - Administrators - Create

Administrator Information

Details

Username:	Name	UI Language:	English
First Name:	First Name	Last Name:	Last Name
Email:	Email	Phone:	Phone
Password:	Password	Confirm Password:	Confirm Password

Settings

Account is active: ON

Receive E-mail Alerts: OFF

Enforce login IP Restrictions: OFF

Super Administrator

Super Administrator: OFF

Managed Departments

Department:

Information

If the Super Administrator option is enabled, the Administrator will have full privileges over the entire system.

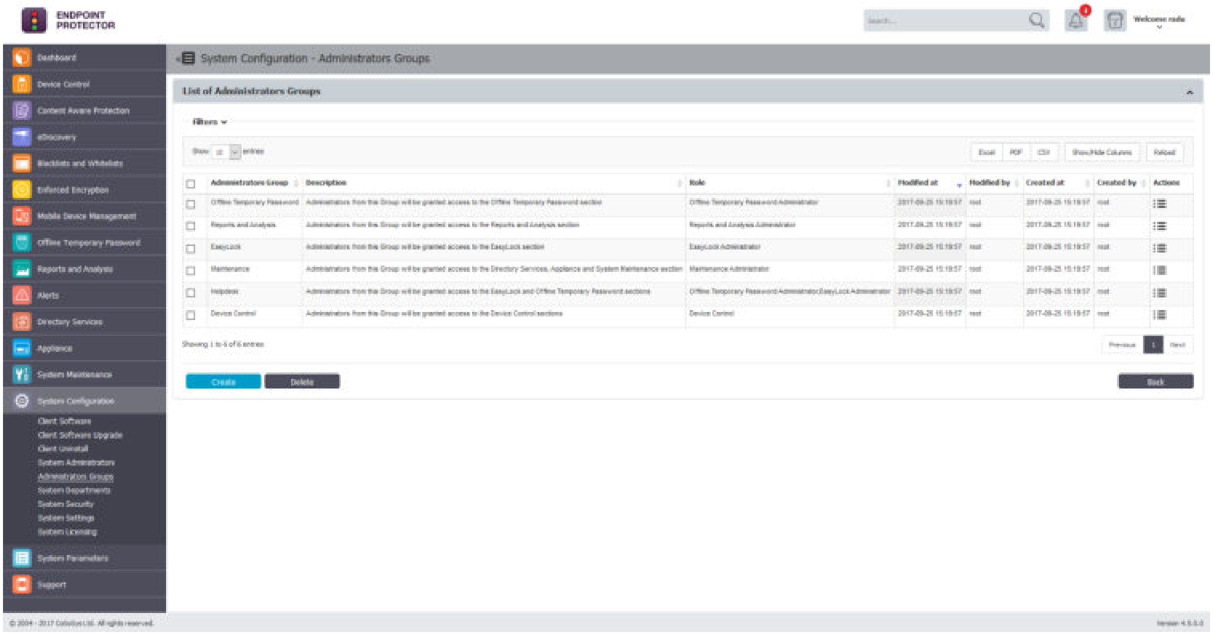
If the Super Administrator option is not enabled, the Administrator will have normal privileges and will be restricted from certain things in the system (e.g.: the administrator will only be able to manage the entities belonging to the system departments he is managing). These will be Normal Administrators.

Normal Administrators can be restricted even further by taking advantage of various roles. For a more restrictive access, the Normal Administrators would have to be included into Administrators Groups, each having a specific role attached to them (e.g.: Administrators can be added into a Helpdesk group, having the Offline Temporary Password and Enforced Encryption roles).

> ⚠ **Note**
>
> All administrators imported from an AD Admin Group will automatically be Super Administrators. These will have to be changed to different roles after the sync.
>
> For more information on how to allow AD Authentication for Administrators, please see paragraph 15.8.2 Active Directory Authentication.

15.5. Administrators Groups

This section allows the creation and management of Administrators Groups, providing Normal Administrators with various access roles (e.g.: Offline Temporary Password Administrators, EasyLock Administrators, Reports and Analysis Administrators, Maintenance Administrators, etc.).

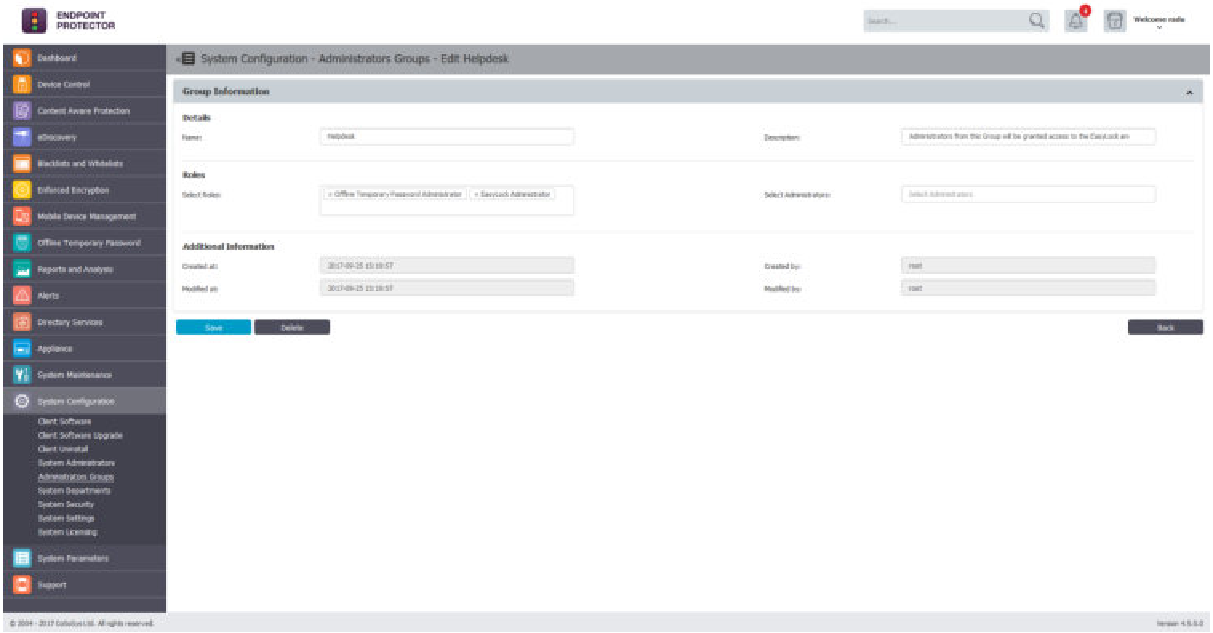


List of Administrators Groups

□	Administrators Group	Description	Role	Modified at	Modified by	Created at	Created by	Actions
□	Offline Temporary Password	Administrators from this Group will be granted access to the Offline Temporary Password section	Offline Temporary Password Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Reports and Analysis	Administrators from this Group will be granted access to the Reports and Analysis section	Reports and Analysis Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	EasyLock	Administrators from this Group will be granted access to the EasyLock section	EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Maintenance	Administrators from this Group will be granted access to the Directory Services, Appliance and System Maintenance section	Maintenance Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Helpdesk	Administrators from this Group will be granted access to the EasyLock and Offline Temporary Password sections	Offline Temporary Password Administrator,EasyLock Administrator	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰
□	Device Control	Administrators from this Group will be granted access to the Device Control sections	Device Control	2017-09-25 15:19:57	root	2017-09-25 15:19:57	root	☰

Showing 1 to 6 of 6 entries

The main information needed to create such a group is to give it a name, a description, select the roles and, select the Administrators that will be part of the group.



System Configuration - Administrators Groups - Edit Helpdesk

Group Information

Details

Name: Helpdesk

Description: Administrators from this Group will be granted access to the EasyLock an

Roles

Select Roles: × Offline Temporary Password Administrator × EasyLock Administrator

Select Administrators: Select Administrators

Additional Information

Created at: 2017-09-25 15:19:57

Created by: root

Modified at: 2017-09-25 15:19:57

Modified by: root

Tips

An Administrators Group can be created, having assigned a combination of roles. E.g.: The Helpdesk Group can have two roles assigned to it – Offline Temporary Password Administrators and EasyLock Administrators.

15.6. System Departments

This section allows the creation and management of System Departments.

Note

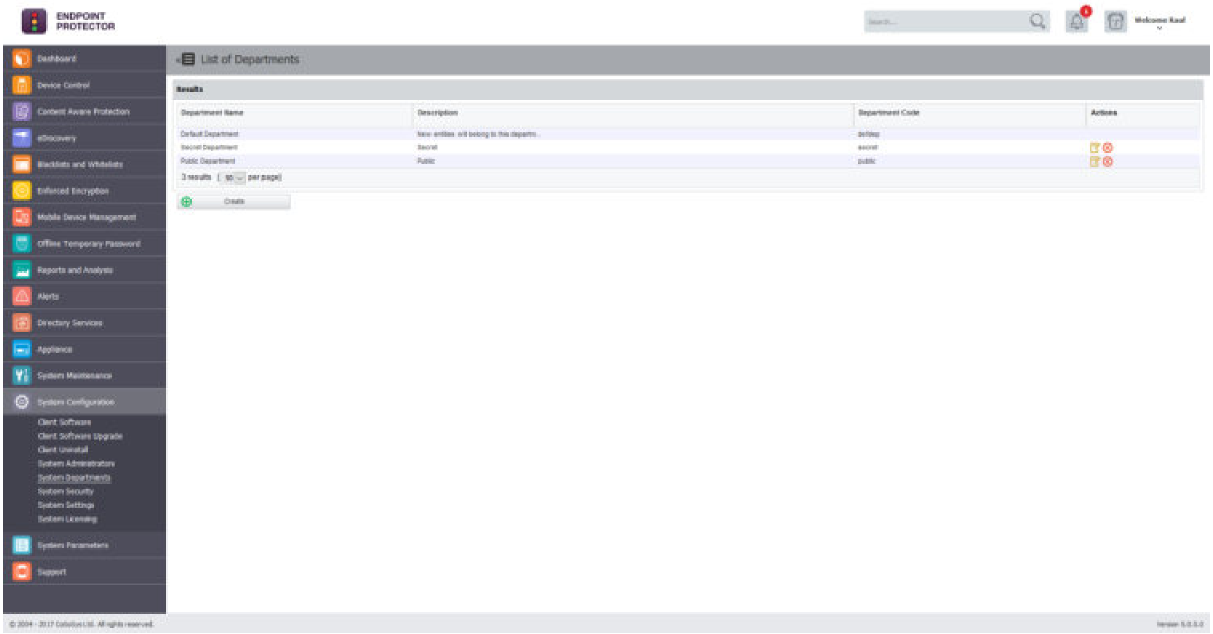
In case that, at registration, no department code is provided or a wrong department code is provided, the department code is considered invalid and that computer will be assigned to the default department (defdep).

Information

Using System Departments is optional. Endpoint Protector works perfectly well with just the Default Department (defdep). Moreover, most scenarios are best covered by simply using Devices, Computers, Users and Groups (the entities also available in AD).

The functionality becomes useful mainly in large installations, with a high number of Administrators and, where strict regulatory compliance rules are in place. Under these circumstances, departments can be created, allowing Normal Administrators to each only manage their own entities.

This functionality should not be confused with Groups of computers and user, nor with administrators' roles.



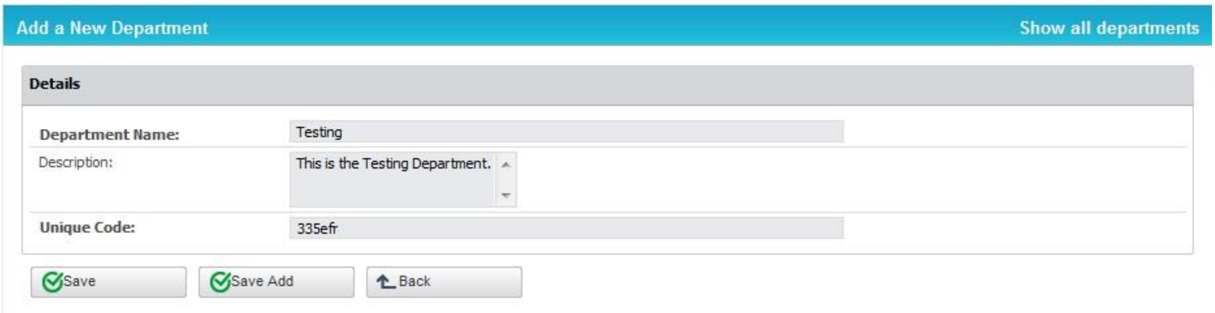
List of Departments

Results

Department Name	Description	Department Code	Actions
Default Department	New entities will belong to this departm...	defdep	
Secret Department	Secret	secret	
Public Department	Public	public	

3 results [50 per page]

Creating a new department is straightforward, and only requires a name, description and unique code.



Add a New Department

Details

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

In terms of terminology, a similarity between Endpoint Protector and Active Directory (or any other Director Service software) would make the Department equivalent to an 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 information about Organization Units, please see paragraph **Error! Reference source not found. Error! Reference source not found.**.

Each entity (e.g.: computer) must belong to a department. When deploying the Endpoint Protector Client, if a department having the given code is found, then the computer will register and it will belong to that department.

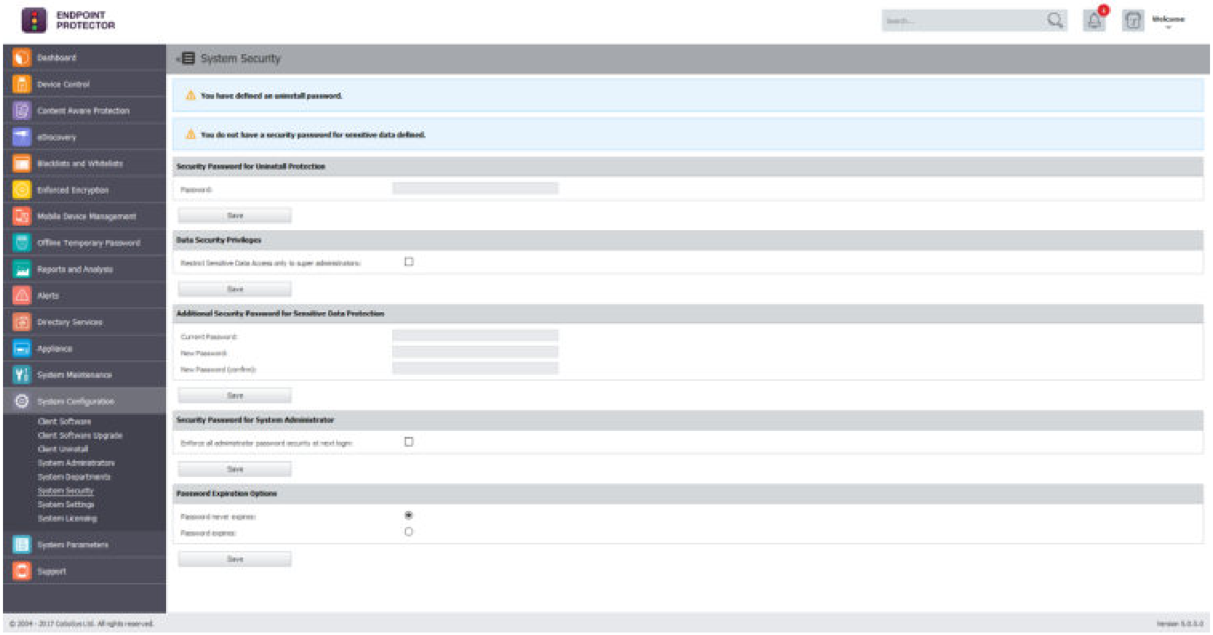
> ⚙ **Example**
>
> Computer Test-PC is registered to department “developers”. In this case, user Test logged on that computer will be assigned to the same department together with the devices connected on the computer Test-PC.

Super Administrators (e.g.: root) will have access to all the main entities regardless of their departments. They will also be able to create departments, as well as Normal Administrators or Administrators with other roles. Super Administrators will also be responsible for assigning administrators to manage departments.

A regular administrator can only manage the departments it was assigned to. It cannot see entities relating to other departments.

15.7. System Security

From this section, the Administrator can configure several security settings such as set a client uninstall password, restrict the access to sensitive information only to super administrators, set a password protection on that sensitive data, enforce all administrators’ password security at next login and password expiration options.



System Security

You have defined an uninstall password.

You do not have a security password for sensitive data defined.

Security Password for Uninstall Protection

Password:

Save

Data Security Privileges

Restrict Sensitive Data Access only to super administrators: ☐

Save

Additional Security Password for Sensitive Data Protection

Current Password:

New Password:

New Password (confirm):

Save

Security Password for System Administrator

Enforce all administrator password security at next login: ☐

Save

Password Expiration Options

Password never expires: ●

Password expires: ○

Save

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Note

Once the “Enforce all administrator password security at next login” is checked, this feature cannot be disabled.

If enabled, only complex passwords can be defined, complying with the below rules:

- the minimum length is 9 characters
- must contain small and capital letters, numbers and special characters
- consecutive characters and numbers in ascending order cannot be used

15.8. System Settings

From this section, the Administrator can configure some general settings that apply to the entire system. The majority of these settings might already be configured as they are included in the initial Endpoint Protector Configuration Wizard.

15.8.1. Endpoint Protector Rights Functionality

From this section, the Administrator can change the rights functionality by giving priority to either User Rights or Computer Rights (or both).

15.8.2. Active Directory Authentication

This section allows an AD group of administrators to be imported into Endpoint Protector as Super Administrators. If the Enable Active Directory Authentication is checked, these administrators can use their AD credentials to login to Endpoint Protector.

The process is straight forward and can be summarized in 4 simple steps:

- Input all credentials and requested information

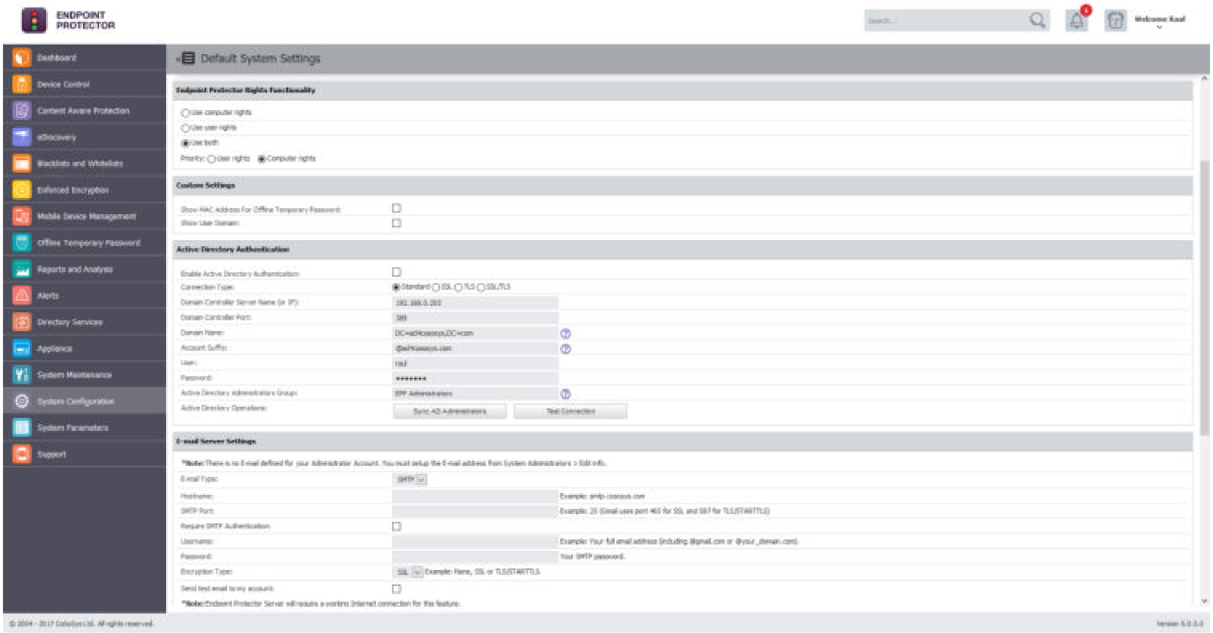
> **Information**
> The settings needed are the same as for the Directory Services section. For more details, please see chapter 12 Directory Services.

- Scroll to the bottom of the page and save the changes

> **Tips**
> The green confirmation messages that appears at the top of the page will confirm the save was successful.

- Return to the Active Directory Authentication section of the page and press the Test Connection button to verify everything is working as expected
- Press the Sync AD Administrators button

> **Note**
> Once the Active Directory Administrators Group has been defined, only users that are part of this AD group will be synced and imported as Super Administrators for Endpoint Protector. Any additional administrators (with different access control levels) can be created manually from the System Administrators section.



Default System Settings

Endpoint Protector Rights Functionality

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

Custom Settings

Show MAC Address For Offline Temporary Password: □
Show User Domain: □

Active Directory Authentication

Enable Active Directory Authentication: □
Connection Type: ● Standard ○ SSL ○ TLS ○ SSL/TLS
Domain Controller Server Name (or IP): 192.168.0.203
Domain Controller Port: 389
Domain Name: DC=ad4cososys,DC=com
Account Suffix: @ad4cososys.com
User: raul
Password: ********
Active Directory Administrators Group: EPP Administrators
Active Directory Operations:

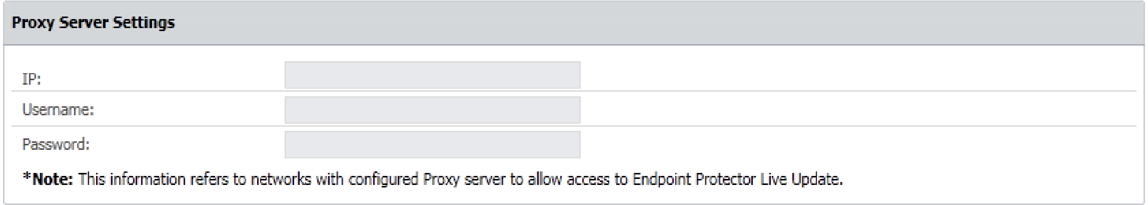
E-mail Server Settings

***Note:** There is no E-mail defined for your Administrator Account. You must setup the E-mail address from System Administrators > Edit info.
E-mail Type: SMTP
Hostname: Example: smtp.cososys.com
SMTP Port: Example: 25 (Gmail uses port 465 for SSL and 587 for TLS/STARTTLS)
Require SMTP Authentication: □
Username: Example: Your full email address (including @gmail.com or @your_domain.com).
Password: Your SMTP password.
Encryption Type: SSL Example: None, SSL or TLS/STARTTLS.
Send test email to my account: □
***Note:** Endpoint Protector Server will require a working Internet connection for this feature.

© 2004 - 2017 CoSoSys Ltd. All rights reserved.
Version 5.0.5.0

15.8.3. Proxy Settings

This section provides the option to configure a proxy, as seen below.



Proxy Server Settings

IP:
Username:
Password:

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

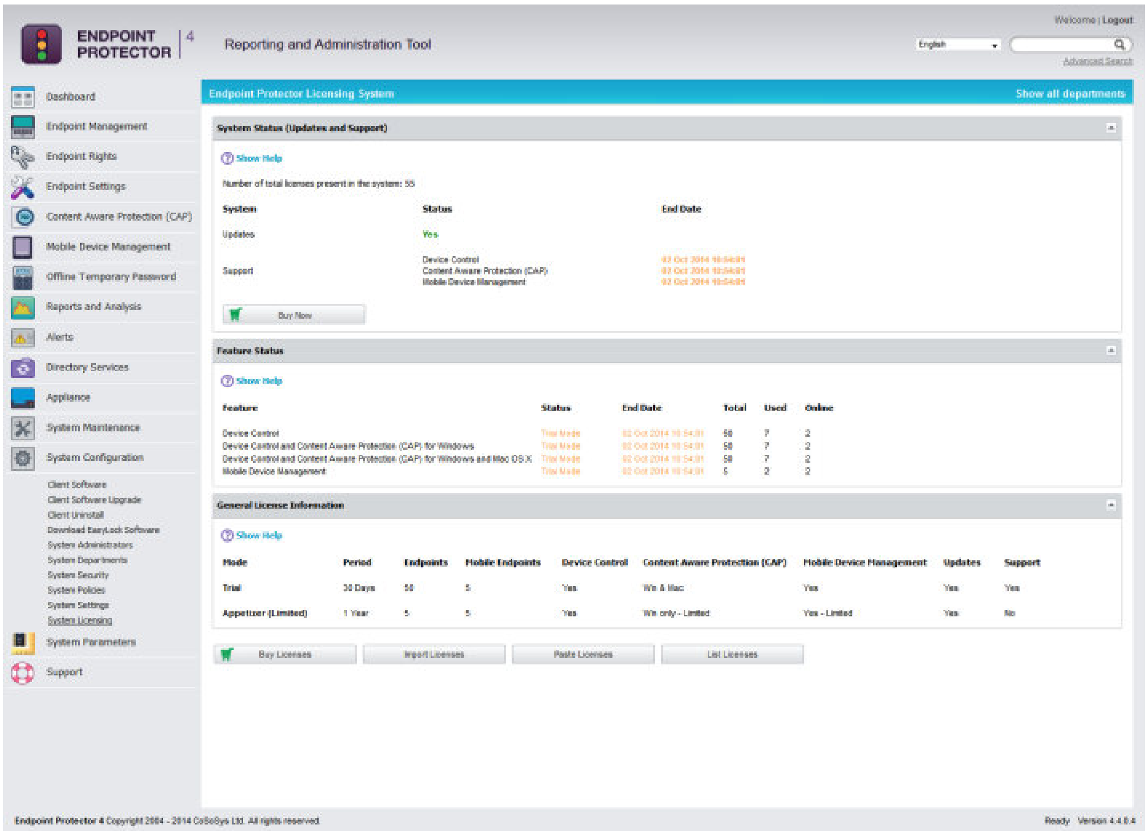
The required information is IP (Proxy Server IP) and optional, Username and Password (Proxy access credentials)

Note

If a Proxy Server is not configured, Endpoint Protector will connect directly to liveupdate.endpointprotector.com.

15.9. System Licensing

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



Endpoint Protector Licensing System

System Status (Updates and Support)

Number of total licenses present in the system: 55

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

Feature Status

Feature	Status	End Date	Total	Used	Online
Device Control	Trial Mode	02 Oct 2014 10:54:01	58	7	2
Device Control and Content Aware Protection (CAP) for Windows	Trial Mode	02 Oct 2014 10:54:01	58	7	2
Device Control and Content Aware Protection (CAP) for Windows and Mac OS X	Trial Mode	02 Oct 2014 10:54:01	58	7	2
Mobile Device Management	Trial Mode	02 Oct 2014 10:54:01	5	2	2

General License Information

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

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

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

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

Feature licenses are used for activating one of the three Endpoint Protector modules: Device Control, Content Aware Protection, respectively Mobile Device Management. Each of these modules can be used in Trial Mode for a period of up to 30 days. Then, a perpetual (permanent) license is required to be purchased and imported for the feature to remain active. Although the Device Control module appears by default as active in the Web Administration Interface, a license is required to enable the communication between Server and Client. The Content Aware Protection and Mobile Device Management features are displayed as blocked by default and require an additional Activation request to be performed by the administrator. The Features Status section offers an overview of the current features licensing status.

Updates & Support licenses are optional licenses that once purchased and imported into the system allow access to the latest Updates available for both

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

Note!

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

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

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

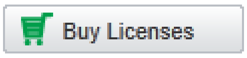
If you wish to manage also a fleet of 10 devices for 6 months, you will additionally require:

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

Note!

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

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



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

15.9.1. 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.

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)

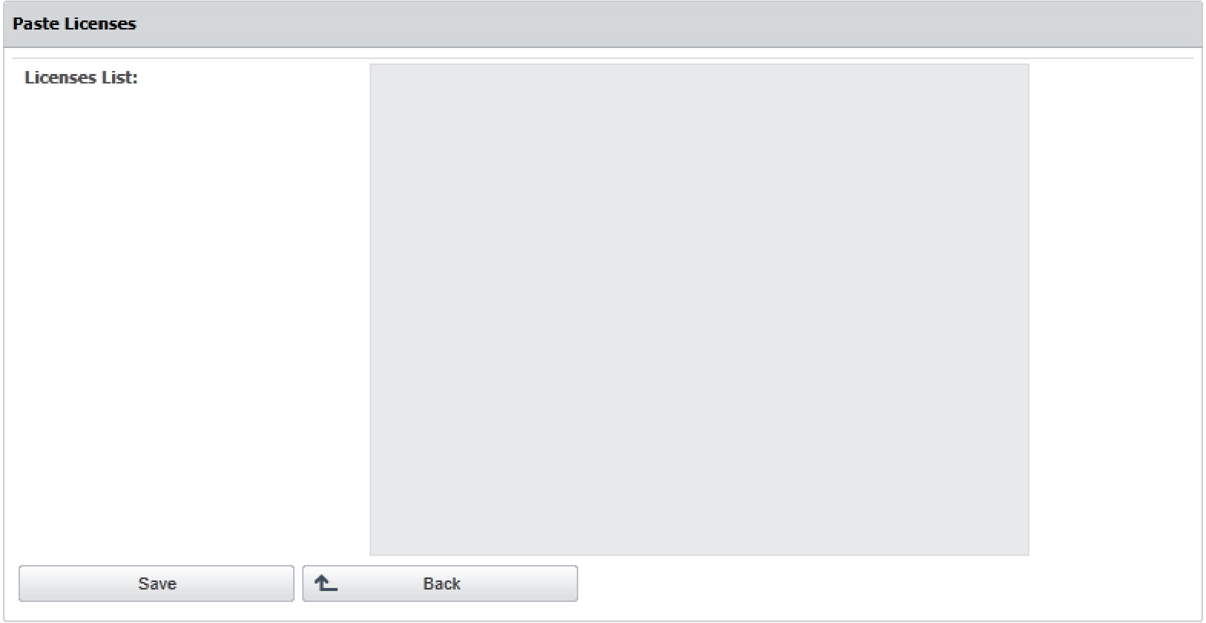
15.9.2. Trial Mode

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.

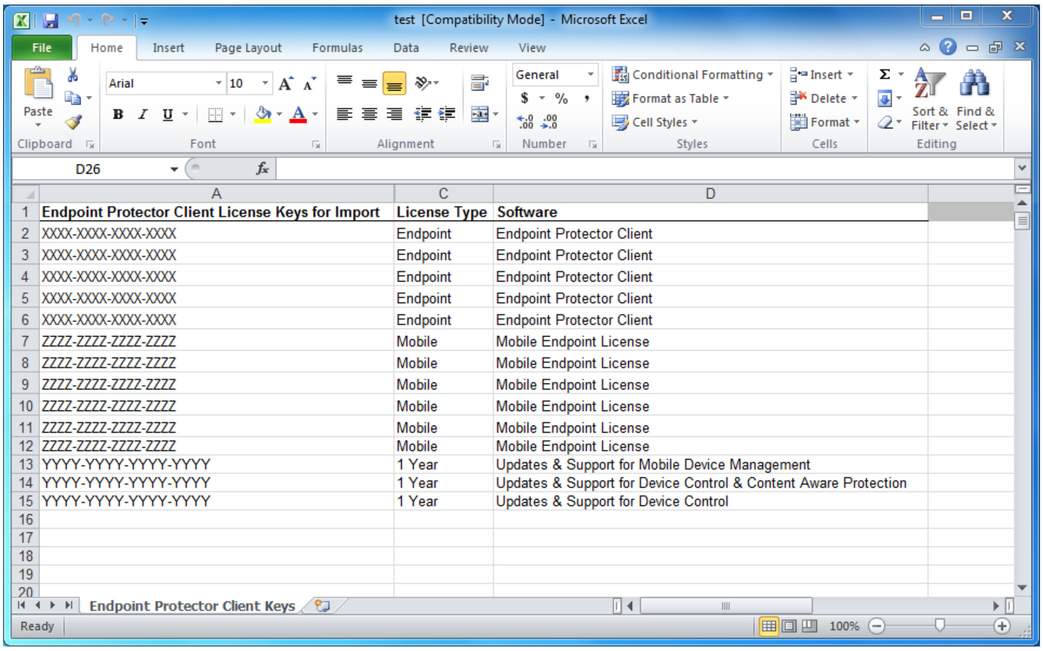
15.9.3. Import Licenses

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



Attention!

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



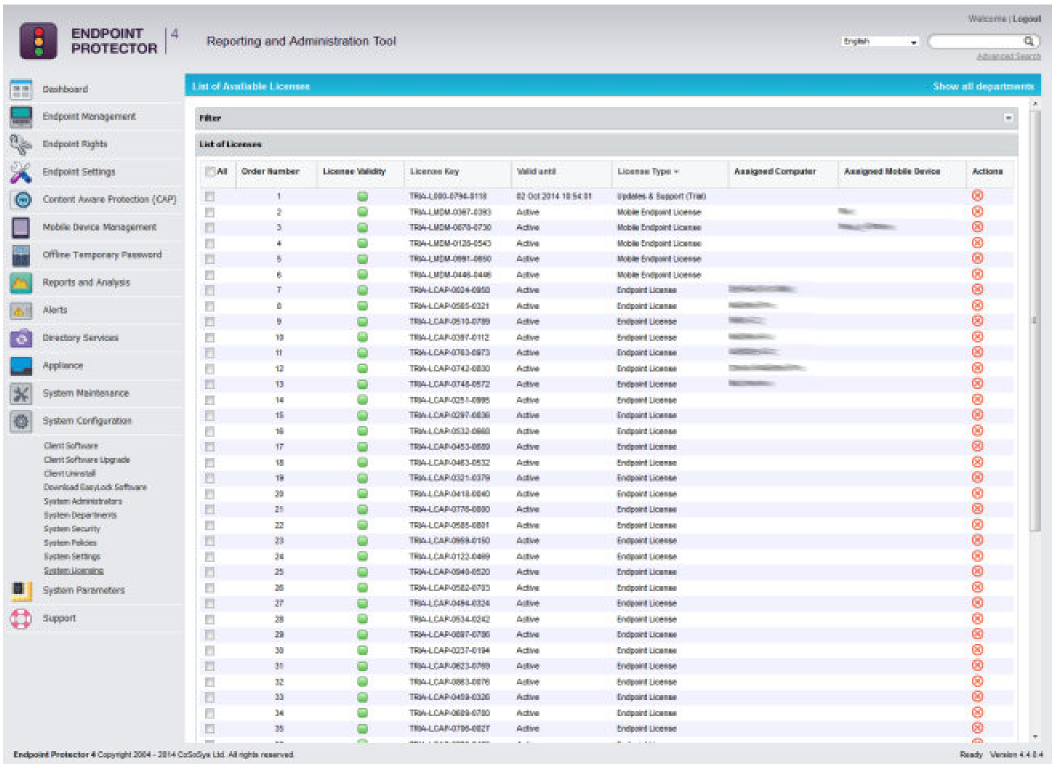
	A	C	D
1	Endpoint Protector Client License Keys for Import	License Type	Software
2	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
3	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
4	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector Client
5	XXXX-XXXX-XXXX-XXXX	Endpoint	Endpoint Protector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

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

Paste Licenses

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

List Licenses



List of Available Licenses

List of Licenses

□ All	Order Number	License Validity	License Key	Valid until	License Type	Assigned Computer	Assigned Mobile Device	Actions
□	1	●	TRIA-L000-0794-0118	02 Oct 2014 10:54:31	Updates & Support (Trial)			⊗
□	2	●	TRIA-LMDM-0367-0393	Active	Mobile Endpoint License		[redacted]	⊗
□	3	●	TRIA-LMDM-0679-0730	Active	Mobile Endpoint License		[redacted]	⊗
□	4	●	TRIA-LMDM-0120-0543	Active	Mobile Endpoint License			⊗
□	5	●	TRIA-LMDM-0991-0650	Active	Mobile Endpoint License			⊗
□	6	●	TRIA-LMDM-0446-0446	Active	Mobile Endpoint License			⊗
□	7	●	TRIA-LCAP-0024-0950	Active	Endpoint License	[redacted]		⊗
□	8	●	TRIA-LCAP-0585-0321	Active	Endpoint License	[redacted]		⊗
□	9	●	TRIA-LCAP-0513-0789	Active	Endpoint License	[redacted]		⊗
□	10	●	TRIA-LCAP-0387-0112	Active	Endpoint License	[redacted]		⊗
□	11	●	TRIA-LCAP-0763-0873	Active	Endpoint License	[redacted]		⊗
□	12	●	TRIA-LCAP-0742-0830	Active	Endpoint License	[redacted]		⊗
□	13	●	TRIA-LCAP-0748-0572	Active	Endpoint License	[redacted]		⊗
□	14	●	TRIA-LCAP-0251-0995	Active	Endpoint License			⊗
□	15	●	TRIA-LCAP-0297-0836	Active	Endpoint License			⊗
□	16	●	TRIA-LCAP-0532-0660	Active	Endpoint License			⊗
□	17	●	TRIA-LCAP-0453-0589	Active	Endpoint License			⊗
□	18	●	TRIA-LCAP-0463-0532	Active	Endpoint License			⊗
□	19	●	TRIA-LCAP-0321-0379	Active	Endpoint License			⊗
□	20	●	TRIA-LCAP-0418-0040	Active	Endpoint License			⊗
□	21	●	TRIA-LCAP-0776-0890	Active	Endpoint License			⊗
□	22	●	TRIA-LCAP-0585-0801	Active	Endpoint License			⊗
□	23	●	TRIA-LCAP-0959-0150	Active	Endpoint License			⊗
□	24	●	TRIA-LCAP-0122-0469	Active	Endpoint License			⊗
□	25	●	TRIA-LCAP-0940-0520	Active	Endpoint License			⊗
□	26	●	TRIA-LCAP-0582-0703	Active	Endpoint License			⊗
□	27	●	TRIA-LCAP-0494-0324	Active	Endpoint License			⊗
□	28	●	TRIA-LCAP-0534-0242	Active	Endpoint License			⊗
□	29	●	TRIA-LCAP-0597-0786	Active	Endpoint License			⊗
□	30	●	TRIA-LCAP-0237-0194	Active	Endpoint License			⊗
□	31	●	TRIA-LCAP-0623-0769	Active	Endpoint License			⊗
□	32	●	TRIA-LCAP-0863-0076	Active	Endpoint License			⊗
□	33	●	TRIA-LCAP-0459-0326	Active	Endpoint License			⊗
□	34	●	TRIA-LCAP-0609-0780	Active	Endpoint License			⊗
□	35	●	TRIA-LCAP-0796-0827	Active	Endpoint License			⊗

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

Ready Version 4.4.0.4

16. System Parameters

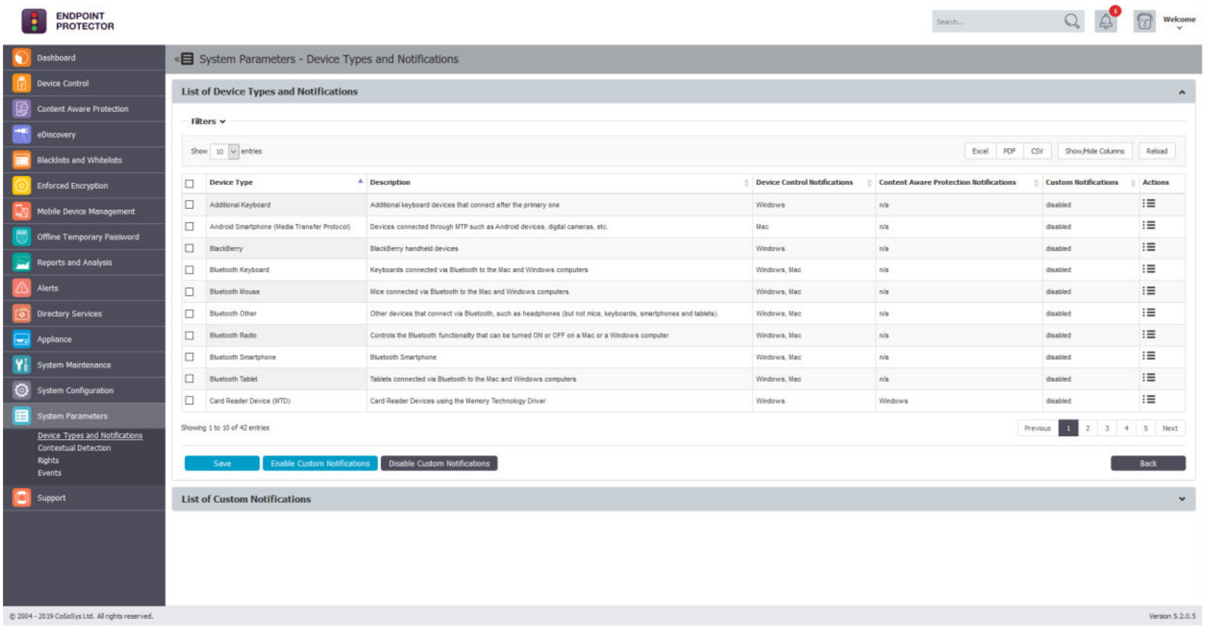
16.1. Device Types and Notifications

From this section, the Administrator can have an overview of the Device Types available in the system along with their availability for each operating system. Moreover, if those devices can or cannot be inspected by the Content Aware Protection module is displayed in the table.

Additionally, this section allows the Administrator to enable and edit the notification messages that appear on the Endpoint Protector Client.

Information

Custom Client Notifications can be globally enabled from Device Control > Global Settings. It can also be individually checked on computers or groups, from their specific Settings sections.



System Parameters - Device Types and Notifications

List of Device Types and Notifications

Show 10 entries

□	Device Type	Description	Device Control Notifications	Content Aware Protection Notifications	Custom Notifications	Actions
□	Additional Keyboard	Additional keyboard devices that connect after the primary one	Windows	n/a	disabled	☰
□	Android Smartphone (Media Transfer Protocol)	Devices connected through MTP such as Android devices, digital cameras, etc.	Mac	n/a	disabled	☰
□	BlackBerry	BlackBerry handheld devices	Windows	n/a	disabled	☰
□	Bluetooth Keyboard	Keyboards connected via Bluetooth to the Mac and Windows computers	Windows, Mac	n/a	disabled	☰
□	Bluetooth Mouse	Mice connected via Bluetooth to the Mac and Windows computers	Windows, Mac	n/a	disabled	☰
□	Bluetooth Other	Other devices that connect via Bluetooth, such as headphones (but not mice, keyboards, smartphones and tablets).	Windows, Mac	n/a	disabled	☰
□	Bluetooth Radio	Controls the Bluetooth functionality that can be turned ON or OFF on a Mac or a Windows computer	Windows, Mac	n/a	disabled	☰
□	Bluetooth Smartphone	Bluetooth Smartphone	Windows, Mac	n/a	disabled	☰
□	Bluetooth Tablet	Tablets connected via Bluetooth to the Mac and Windows computers	Windows, Mac	n/a	disabled	☰
□	Card Reader Device (MTD)	Card Reader Devices using the Memory Technology Driver	Windows	Windows	disabled	☰

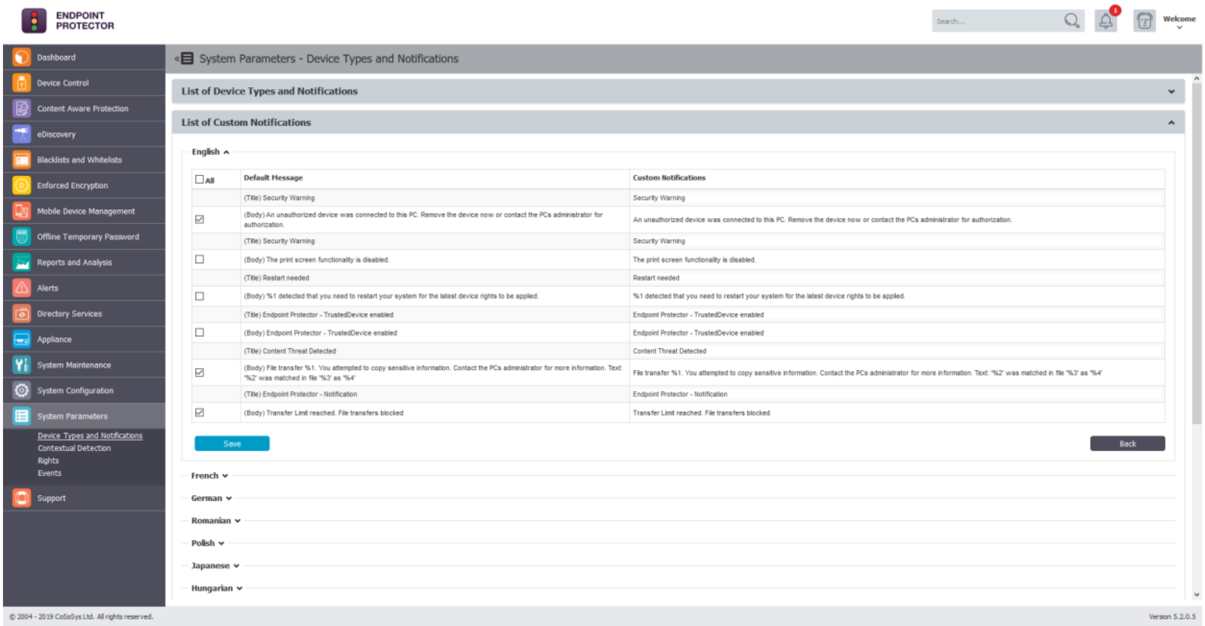
Showing 1 to 10 of 42 entries

List of Custom Notifications

© 2004 - 2019 CoSoSys Ltd. All rights reserved.

Version 5.2.0.5

By expending the List of Custom Notifications and selecting the desired language, the displayed message can be edited. Additionally, in case Administrators do not want to display some notifications, while showing others, these can be unchecked.



System Parameters - Device Types and Notifications

List of Device Types and Notifications

List of Custom Notifications

English

□ All	Default Message	Custom Notifications
	(Title) Security Warning	Security Warning
☑	(Body) An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.	An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.
	(Title) Security Warning	Security Warning
□	(Body) The print screen functionality is disabled.	The print screen functionality is disabled.
	(Title) Restart needed	Restart needed
□	(Body) %1 detected that you need to restart your system for the latest device rights to be applied.	%1 detected that you need to restart your system for the latest device rights to be applied.
	(Title) Endpoint Protector - TrustedDevice enabled	Endpoint Protector - TrustedDevice enabled
□	(Body) Endpoint Protector - TrustedDevice enabled	Endpoint Protector - TrustedDevice enabled
	(Title) Content Threat Detected	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'	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'
	(Title) Endpoint Protector - Notification	Endpoint Protector - Notification
☑	(Body) Transfer Limit reached. File transfers blocked	Transfer Limit reached. File transfers blocked

French

German

Romanian

Polish

Japanese

Hungarian

16.1.1. 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 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.

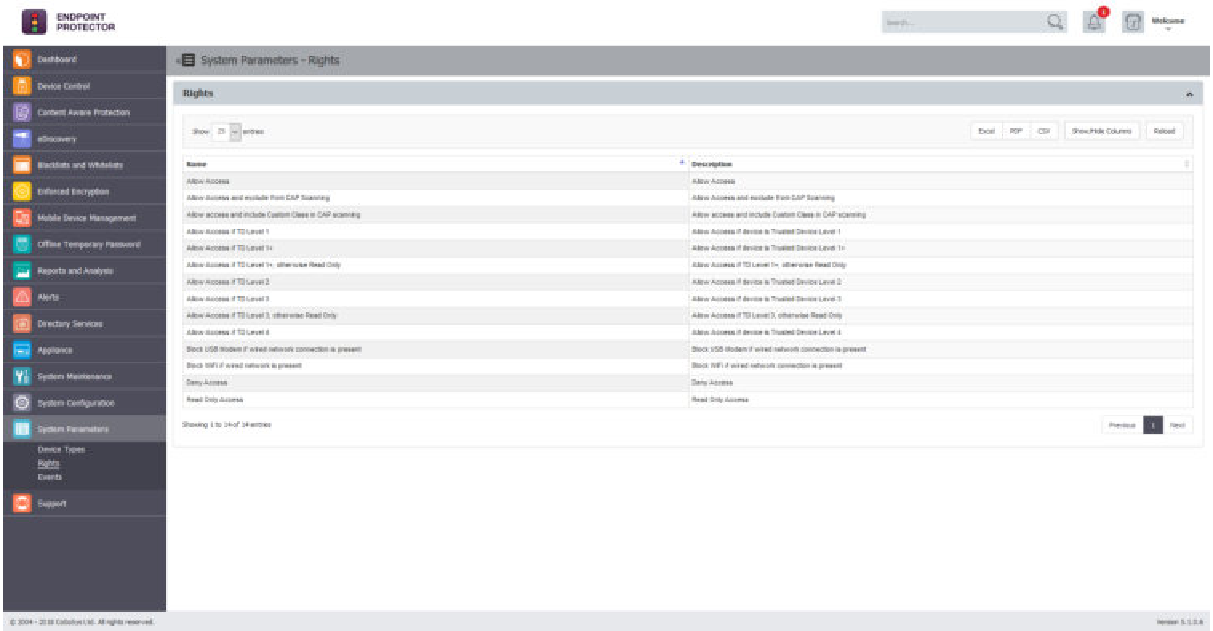
The table below provides a list of TrustedDevices:

Device Names	TrustedDevice Level
EasyLock Encrypted devices	1
AT1177	2
UT169	2
UT176	2
Trek ThumbDrive	2
BitLocker Encrypted devices	3
FileVault Encrypted devices	3
Buffalo Secure Lock	3
CTWO SafeXs	3
Integral Crypto	3
Integral Crypto Dual	3
Integral Courier Dual	3
IronKey Secure Drive	3
iStorage datAshur	3
Kanguru Bio Drive	3
Kanguru Defender	3

Kanguru Elite (30, 200 & 300)	3
Kanguru Defender Elite	3
Kingston DataTraveler Locker+	3
Lexar 1 (Locked I Device)	3
Lexar Gemalto	3
SaferZone Token	3
ScanDisk Enterprise	3
Verbatim Professional	3
Verbatim Secure Data	3
Verbatim V-Secure	3
iStorage datAshur Pro	4
Kanguru Defender (2000 & 3000)	4
SafeStick BE	4
Stealth MXP Bio	4

16.2. Device Rights

This subsection displays a list with all access rights which can be assigned to devices.



Name	Description
Allow Access	Allow Access
Allow Access and exclude from CAP Scanning	Allow Access and exclude from CAP Scanning
Allow access and include Custom Class in CAP scanning	Allow access and include Custom Class in CAP scanning
Allow Access if TD Level 1	Allow Access if device is Trusted Device Level 1
Allow Access if TD Level 1+	Allow Access if device is Trusted Device Level 1+
Allow Access if TD Level 1+, otherwise Read Only	Allow Access if TD Level 1+, otherwise Read Only
Allow Access if TD Level 2	Allow Access if device is Trusted Device Level 2
Allow Access if TD Level 3	Allow Access if device is Trusted Device Level 3
Allow Access if TD Level 3, otherwise Read Only	Allow Access if TD Level 3, otherwise Read Only
Allow Access if TD Level 4	Allow Access if device is Trusted Device Level 4
Block USB Modem if wired network connection is present	Block USB Modem if wired network connection is present
Block WiFi if wired network is present	Block WiFi if wired network connection is present
Deny Access	Deny Access
Read Only Access	Read Only Access

16.3. Contextual Detection

From this section, the Administrator can manage the contextual detection for the entire system. If enabled, the confidential information detected by Endpoint Protector will be inspected for both content and context. This means that in addition to the function that detects sensitive information (e.g.: Credit Cards, IDs, Passports, Driving Licenses, etc.), the context will also be taken into consideration (e.g.: proximity to other relevant keywords, other related functions, regular expressions, etc.).

⚙ **Tips**

In addition to providing context to the detected sensitive information, this functionality also helps decrease false positives.

⚠ **Note**

This feature applies at a global level, for both Content Aware Protection and eDiscovery Policies. If enabled, the context detection will supersede the content only detection through the system.

Please ensure the accuracy of the rules and the relevance for your scenarios before enabling this functionality.

Once the Contextual Detection feature is enabled, it will apply at a global level, based on the rules defined in the Contextual XML (but also linked to the configured Content Aware Protection and eDiscovery policies).

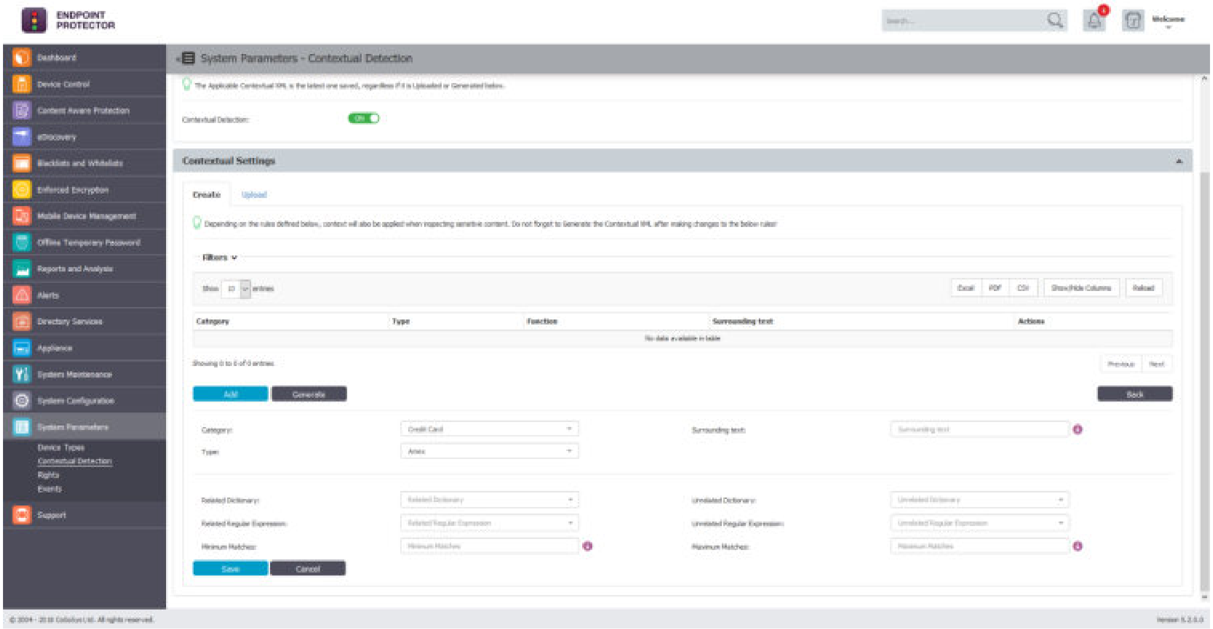
There are two options to create the Contextual rules:

- creating it directly from the Endpoint Protector Server.
- manually editing the Contextual XML and then uploading it to the Endpoint Protector Server,

16.3.1. Creating the XML

Information

This method is recommended for general use as it is the easiest method and it can cover most use cases.



System Parameters - Contextual Detection

The Applicable Contextual XML is the latest one saved, regardless if it is Uploaded or Generated below.

Contextual Detection: ON

Contextual Settings

Create | Upload

Depending on the rules defined below, context will also be applied when inspecting sensitive content. Do not forget to Generate the Contextual XML after making changes to the below rules!

Category	Type	Function	Surrounding text	Actions
No data available in table				

Showing 0 to 0 of 0 entries

Category: Credit Card

Type: Amex

Surrounding text: Surrounding text

Related Dictionary: Related Dictionary

Related Regular Expression: Related Regular Expression

Minimum Matches: Minimum Matches

Unrelated Dictionary: Unrelated Dictionary

Unrelated Regular Expression: Unrelated Regular Expression

Maximum Matches: Maximum Matches

© 2004 - 2018 CoSoSys Ltd. All rights reserved.

Version 5.2.0.0

For each category of Predefined Content (e.g.: Credit Cards, IDs, Passports, Driving Licenses, etc.), contextual detection can be configured by clicking on the **Add** button and selecting things like:

- **Category and Type** – the content aware detection function.
- **Surrounding text** – the number of characters of the search interval to determine the context.
- **Related Dictionary** – a set of keywords related to the PII.
- **Related Regular Expression** – an additional way of adding a related rule that is not among the content aware detection functions.
- **Related File Type** – the related file type.
- **Related File Size (MB)** – the related file size, in megabytes.
- **Minimum Matches** – the minimum number of items to match to validate the detection rule
- **Unrelated Dictionary**– a set of keywords not related to the PII.
- **Unrelated Regular Expression** – an additional way of adding a non-related rule that is not among the content aware detection functions.
- **Unelated File Type** – the unrelated file type.
- **Unrelated File Size (MB)** – the unrelated file size, in megabytes.
- **Maximum Matches** – the value above which the rule will not be validated (recommended value is 0).

⚠ **Note**

Do not forget to Generate the Contextual XML after creating or making changes to contextual rules!

16.3.2. Uploading the XML

Information

This method is recommended for advanced Administrators as it offers extended functionalities but it also requires a deeper understanding of the XML syntax.

Advance contextual functionalities are also available. For this method the Contextual XML file has to be edited manually by the Administrator and then uploaded to the Endpoint Protector Server.

Proximity, Dictionaries, Regex, etc. all have to be defined within the XML document. In addition to the functionalities described in the chapter above 16.3.1 Creating the XML, there are more complex options available like: **Confidence Level**, additional **Functions** to consider when determining the Main Function, etc.

Tips

The best way to understand the syntax needed in the Contextual XML is to look at the sample available within Endpoint Protector Server as it includes multiple examples. Additionally, the example below also provides a clear direction.

Example

```
 <Rules>
    <!-- SSN / Canada this is an example with multiple patterns -->
    <Entity id="ssn/canada" patternsProximity="300"
recommendedConfidence="75">
      <Pattern confidenceLevel="75">
        <Any minMatches="2">
         <Match idRef="keywords_Canada_SSN_1" />
         <Match idRef="keywords_Canada_SSN_2" />
         <Match idRef="validate_date_fct" />
         <Match idRef="regex_email_id" /> <!-- This is just an example -->
        </Any>
        <Any maxMatches="0">
         <Match idRef="keywords_exclude_Canada_SSN" />
        </Any>
      </Pattern>
    </Entity>

    <Function id="validate_date_fct" name="SEARCH_DATE_INTRL" />
<!-- name should be the same with the one on the client -->
       <Function id="func_dlp_is_valid_ssn" name="SEARCH_SSN_Canada"
/>  <!-- name should be the same with the one on the client -->
```

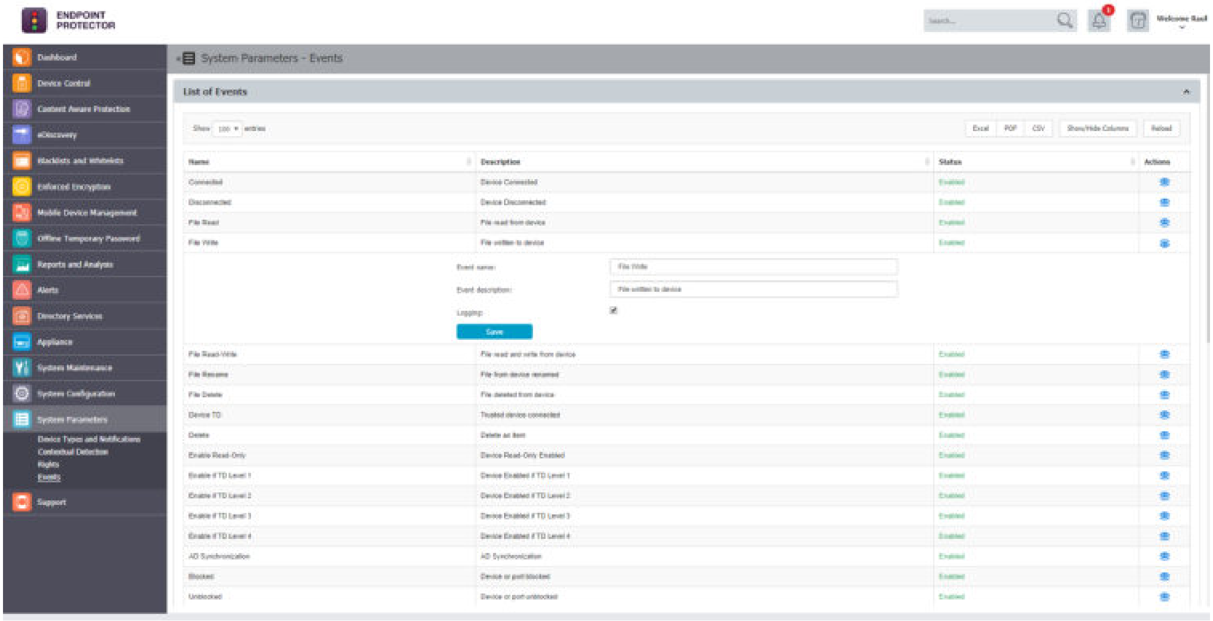
Example

```
 <Keyword id="keywords_Canada_SSN_1">
   <Group matchStyle="word">
        <Term>sin</Term>
        <Term>social insurance</Term>
        <Term>numero d'assurance sociale</Term>
        <Term>sins</Term>
        <Term>ssn</Term>
        <Term>ssns</Term>
        <Term>social security</Term>
        <Term>numero d'assurance sociala</Term>
        <Term>national identification number</Term>
        <Term>national id</Term>
        <Term>sin#</Term>
    </Group>
  </Keyword>

 <Keyword id="keywords_Canada_SSN_2">
    <Group matchStyle="word">
        <Term>driver's license</Term>
        <Term>drivers license</Term>
        <Term>driver's licence</Term>
        <Term>drivers licence</Term>
        <Term>DOB</Term>
        <Term>Birthdate</Term>
    </Group>
  </Keyword>

<Keyword id="keywords_exclude_Canada_SSN">
    <Group matchStyle="word">
        <Term>random word</Term>
    </Group>
  </Keyword>

  <Regex id="regex_email_id">[-0-9a-zA-Z.+_]+@[-0-9a-zA-
Z.+_]+\.[a-zA-Z]{2,4}</Regex>

 </Rules>
</RulePackage>
```

16.4. Events

This subsection displays a list events which are logged by Endpoint Protector. Additionally, the Actions column provides the option edit the event name and description or to disable logging for specific events.

From this section, the Administrator can manage the list of Events logged by Endpoint Protector. The option to edit the event name and description or to disable logging for specific events is also available.



Name	Description	Status	Actions
Connected	Device Connected	Enabled	⚙
Disconnected	Device Disconnected	Enabled	⚙
File Read	File read from device	Enabled	⚙
File Write	File written to device	Enabled	⚙

Event name: File Write

Event description: File written to device

Logging: ☑

Save

Name	Description	Status	Actions
File Read-Write	File read and write from device	Enabled	⚙
File Rename	File from device renamed	Enabled	⚙
File Delete	File deleted from device	Enabled	⚙
Device TD	Trusted device connected	Enabled	⚙
Delete	Delete an item	Enabled	⚙
Enable Read-Only	Device Read-Only Enabled	Enabled	⚙
Enable if TD Level 1	Device Enabled if TD Level 1	Enabled	⚙
Enable if TD Level 2	Device Enabled if TD Level 2	Enabled	⚙
Enable if TD Level 3	Device Enabled if TD Level 3	Enabled	⚙
Enable if TD Level 4	Device Enabled if TD Level 4	Enabled	⚙
AD Synchronization	AD Synchronization	Enabled	⚙
Blocked	Device or port blocked	Enabled	⚙
Unblocked	Device or port unblocked	Enabled	⚙

17. Endpoint Protector Client

The Endpoint Protector Client enforces the Rights and Settings received from the Endpoint Protector Server on the protected endpoints (Windows, Mac and Linux).

The Endpoint Protector Client can be downloaded directly from the Endpoint Protector UI.

Information

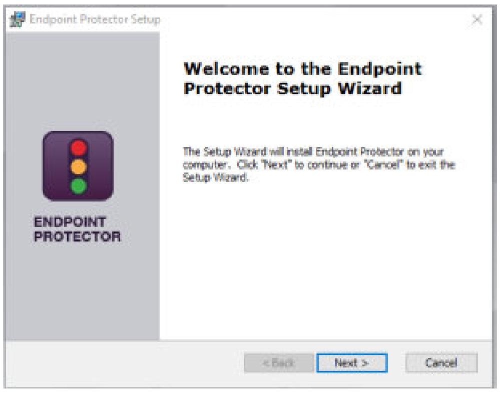
For more details about downloading the Endpoint Protector Client, please see chapter 15.1 Client Software.

Tips

Tools like Active Directory or Jamf can be used to deploy the Endpoint Protector Client in large networks.

17.1. Client Installation

The Endpoint Protector Client Installation is a straightforward one and can be followed by anyone. The Installation folder and Server information will have to be set, however, these are already preconfigured and just a simple “Next” is required.



Welcome to the Endpoint Protector Setup Wizard

The Setup Wizard will install Endpoint Protector on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Note

For Linux, please consult the readmeLinux.txt file available under the "Read this before installing" link for exact installation instructions corresponding to the distribution.

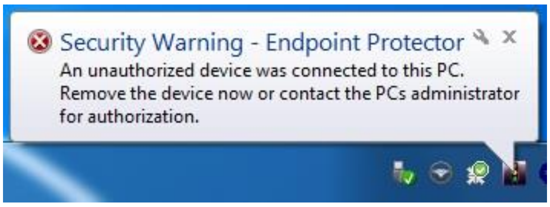
17.2. Client Security

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 the network administrator.

17.3. Client Notifications (Notifier)

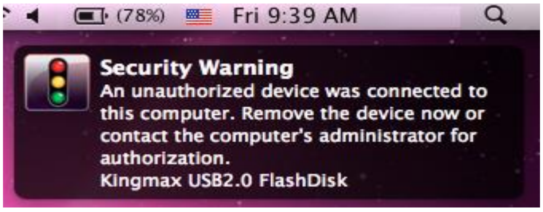
The Endpoint Protector Client will display a notification from the taskbar icon when an unauthorized device is connected to the computer. Notifications are also displayed when file transfer that do not comply with the internal policy are attempted.

Depending on the Operating System, the notifications look like the below:



Security Warning - Endpoint Protector

An unauthorized device was connected to this PC. Remove the device now or contact the PCs administrator for authorization.



Security Warning

An unauthorized device was connected to this computer. Remove the device now or contact the computer's administrator for authorization.

Kingmax USB2.0 FlashDisk

Information

The Endpoint Protector Client has several modes available. Depending on the chosen one, the notifications can be hidden to the user. Additionally, not only does it log any attempts to forcefully access the system, it can also trigger the Panic Mode.

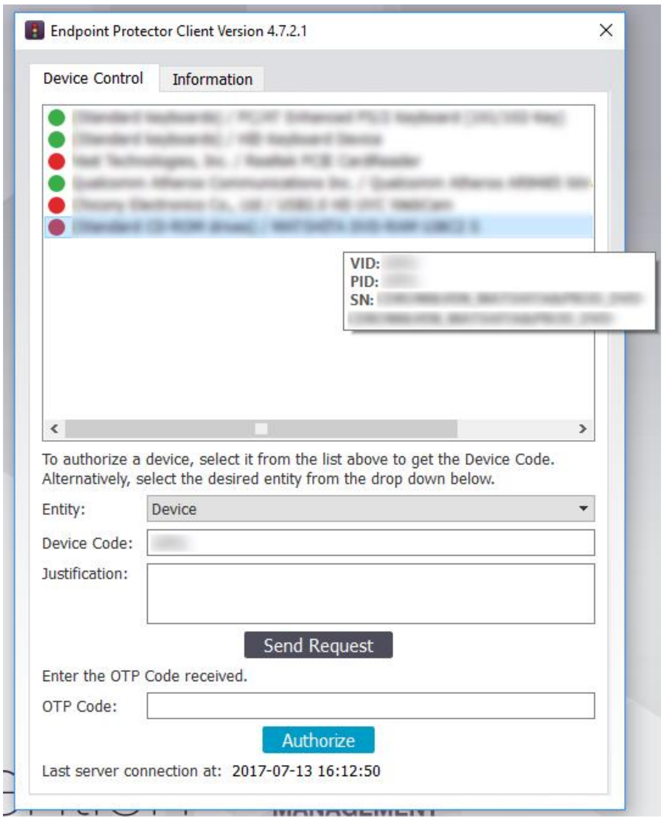
For more details, please see chapter 3.6.2.1 Endpoint Protector Client

17.4. Client Device Control tab

The Endpoint Protector Client's Device Control tab is designed to display information about all connected devices. It also shows the access right for each specific device.

Tips

Details such as VID, PID, and Serial Number are also displayed when hovering over a device from the list.



To authorize a device, select it from the list above to get the Device Code. Alternatively, select the desired entity from the drop down below.

Entity: Device

Device Code:

Justification:

Enter the OTP Code received.

OTP Code:

Last server connection at: 2017-07-13 16:12:50

17.4.1. Requesting and redeeming an Offline Temporary Password

When a user wants to request access for a device, there are some quick steps to follow.

- the device needs to be selected from the list and the Device Code will be filled automatically

Information

The Device Code is a unique way for Endpoint Protector to identify devices. Every device connected to a computer where the Endpoint Protector Client is present is assigned this identifier that is sent to the Server and can be seen in Device Control > Devices list.

- the Justification specifying why such action is needed has to filled in

Tips

The Justification can be a great help for auditing purposes.

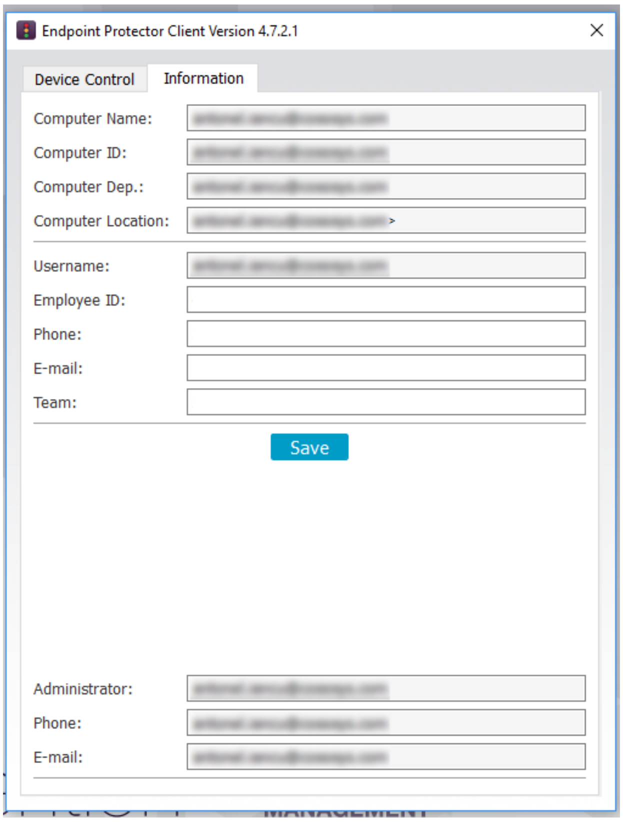
- pressing the "Send Request" button will automatically open the default e-mail client and generate all the information an Administrator needs to authorize a device

> **Information**
>
> Depending on what the OTP request has been made for, the e-mail will contain information such as Device, VID, PID, Serial Number, Computer Name, Username and Justification.

- the Administrator generates the OPT Code from the Endpoint Protector Server and provides it to the user.
- After the code received from the Administrator is entered in the OTP Code section, pressing the "Authorize" button will provide the necessary access privileges.

17.5. Client Information tab

The Endpoint Protector Client's Information tab is designed to display information about the computer, user, as well as contact information for the Endpoint Protector Administrator. Some of the information in this section is automatically filled in by the Endpoint Protector Client, some can be edited by the user, while some can be edited by the Administrator, from the Server.



Computer Name: [redacted]
Computer ID: [redacted]
Computer Dep.: [redacted]
Computer Location: [redacted]
Username: [redacted]
Employee ID:
Phone:
E-mail:
Team:
Administrator: [redacted]
Phone: [redacted]
E-mail: [redacted]

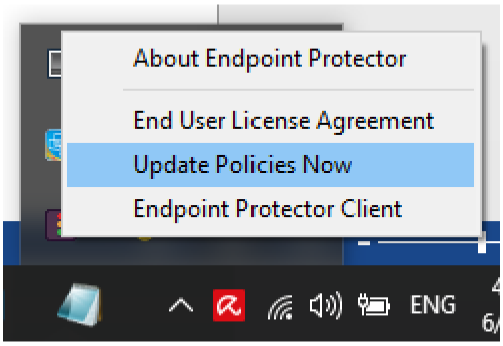
The Computer Name and Username are automatically filled in by the Endpoint Protector Server.

The Computer ID, Computer Dep., Computer Location, Administrator name, e-mail, and phone are received from the Endpoint Protector Server (if they have been filled in by the Administrator).

The Employee ID, Phone, E-mail and Team can be filled in by the User. Once the Save button is clicked, the information will be synced with the Server.

17.6. Client Policy Update

The Endpoint Protector Client has a built-in feature to ensure the latest policies are received. The Update Policies Now option is available by right clicking on the Endpoint Protector Client system tray icon, as shown below:



17.7. Client Offline Functionality

Depending on the Settings on the Server, 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.

17.8. Client DHCP and manual IP address

The Endpoint Protector Client automatically recognizes changes in the network's configuration and updates settings accordingly. This will protect the endpoint both in case of a DHCP (e.g. at the office) or a manual IP address (e.g. at home), without having to reinstall the Client or modify any changes.

17.9. Client Uninstall

17.9.1. Client Uninstall on Windows

To remove the Endpoint Protector Client, go to Programs and Features and select the application.

Additionally, if enabled by the Endpoint Protector Administrator, an uninstall password will also be required.

⚙ **Tips**

The option to remotely uninstall Clients form the Endpoint Protector Server is also available from the System Configuration > Client Uninstall section.

17.9.2. Client Uninstall on Mac

To remove the Endpoint Protector Client the "remove-epp.command" file that was included in the download package needs to be executed and enter the password needed to preformed administrative tasks.

Additionally, if enabled by the Endpoint Protector Administrator, an uninstall password will also be required.

⚙ **Tips**

The option to remotely uninstall Clients form the Endpoint Protector Server is also available from the System Configuration > Client Uninstall section.

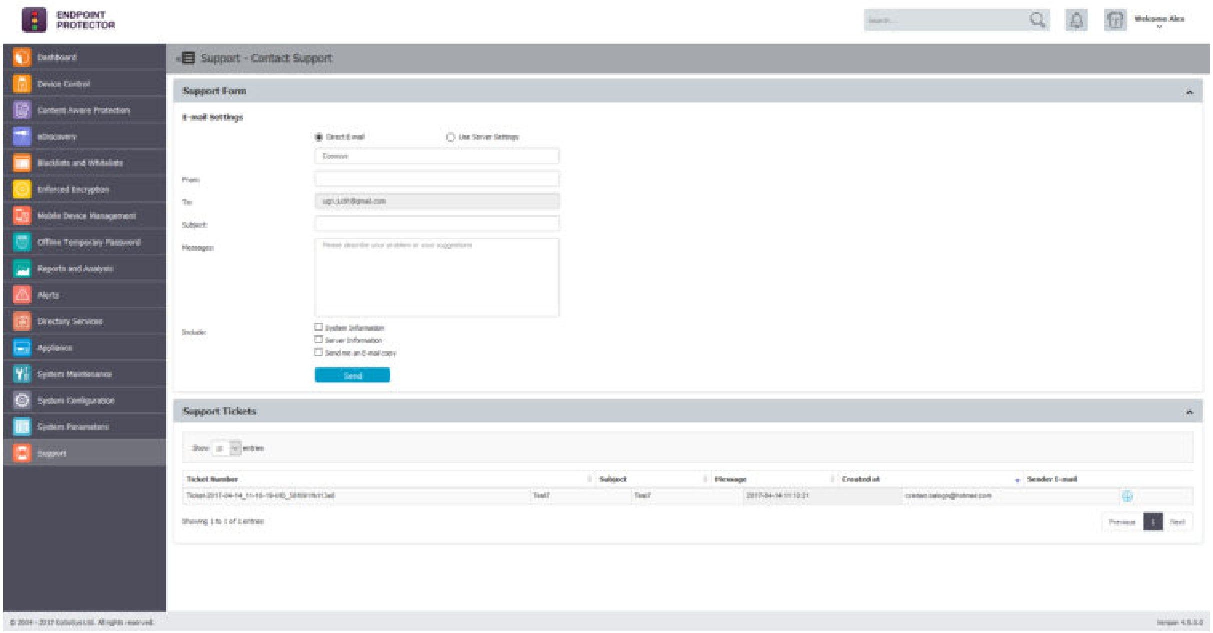
17.9.3. Client Uninstall on Linux

To remove the Endpoint Protector Client the "uninstall.sh" file that was included in the download package needs to be executed and enter the password needed to preformed administrative tasks.

18. Support

Additional support resources as available. Please visit our website for more manuals, FAQs, videos and tutorials, direct e-mail support and more at https://www.endpointprotector.com/resources

Our Support department can also be contacted directly from the Endpoint Protector User Interface from the Support > Contact Support section. One of our team members will contact you in the shortest time possible.



Support - Contact Support

Support Form

E-mail Settings

● Direct E-mail ○ Use Server Settings

Common

From:

To: upr_lucr@gmail.com

Subject:

Messages: Please describe your problem or your suggestions

Include: □ System Information □ Server Information □ Send me an E-mail copy

Support Tickets

Show 10 entries

Ticket Number	Subject	Message	Created at	Sender E-mail
Ticket-2017-04-14_11-15-19-UID_58f0919b113a6	Test7	Test7	2017-04-14 11:10:21	cristian.balogh@hotmail.com

Showing 1 to 1 of 1 entries

© 2004 - 2017 CoSoSys Ltd. All rights reserved.

Version 4.5.5.0

Even if you do not have a problem but miss some feature or just want to leave us a general comment, we would love to hear from you.

19. Disclaimer

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of your private information (if Automatic Live Update Reporting is DISABLED).

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.