



ENDPOINT PROTECTOR 2009

User Manual Version 3.0.5.2

User Manual



Table of Contents

1.Introduction	1
1.1. What is Endpoint Protector?	2
1.2. Main Features.....	4
1.2.1. Centralized web based Device Management / Dashboard	4
1.2.2. Control your data flow: File Tracing / File Shadowing	4
1.2.3. Audit Trail – Device Activity Logging	5
1.2.4. Audit Trail – Reporting and Analysis Tools	5
1.2.5. File Whitelist.....	5
1.2.6. Easy Enforcement of Your Security Policies.....	5
1.2.7. Network "Offline" Mode to Support Your Field Employees	5
1.2.8. Enforced Encryption - protecting sensitive data in transit / TrustedDevice	6
1.2.9. Client Uninstall Protection	6
1.2.10. Client Stop Protection / Tamper Protection	6
1.2.11. Backup Scheduler	6
1.3. Controlled Device Types / Ports	7
1.4. Conclusions.....	9
2.Server Functionality / Server Components	10
2.1. Endpoint Protector – Web Service	11
2.2. Administration and Reporting Tool	11
2.3. Accessing the Administration and Reporting Tool	14
2.4. Login Credentials (Username and Password)	15
3.Management	16
3.1. Devices.....	16
3.2. Device Functionality	17
3.2.1. Give / Deny Access to Devices	18
3.2.2. Enable Device Read-Only Access.....	20
3.2.3. TrustedDevice Level 1 to Level 4.....	20
3.2.4. WiFi - Block if wired network is present.....	20
3.3. Computers	21
3.4. Groups	23
3.5. Users	24

4. Rights	26
4.1. Device Rights	27
4.2. User Rights	28
4.3. Computer Rights	29
4.4. Group Rights	30
4.5. Global Rights	31
4.6. File Whitelist	32
5. Offline Temporary Password	34
5.1. Generating the Offline Temporary Password	34
5.2. Offline Device Authorization	37
5.3. Setting the Administrator Contact Information	38
6. Settings	39
6.1. Computer Settings	42
6.2. Group Settings	43
6.3. Global Settings	44
6.4. File Tracing	45
6.5. File Shadowing	46
7. Reports and Analysis	49
7.1. Logs Report	50
7.2. File Tracing	51
7.3. File Shadowing	52
7.4. Online Computers	53
7.5. Online Users	54
7.6. Connected Devices	55
7.7. Computer History	56
7.8. User History	57
7.9. Device History	58
7.10. Statistics	59
7.11. Graphics	60
8. System Alerts	62

9. System Parameters	67
9.1. Device Types	68
9.2. Rights	69
9.3. Events	70
9.4. File Types	71
9.5. System Licenses	72
9.5.1. Import Licenses	73
9.6. System Security / Client Uninstall Protection	74
10. System Configuration	76
10.1. Active Directory Functionalities	76
10.1.1. Active Directory Import	77
10.1.2. Active Directory Sync	80
10.1.3. Active Directory Client Deployment	84
10.2. System Administrators	90
10.3. System Policies	91
10.4. System Settings	92
10.5. System Snapshots	97
10.6. Log Backup	99
10.6.1. Backup Scheduler (Automatic Log Backup)	100
11. Setting up Policies	102
12. Modes for Users, Computers and Groups	104
12.1. Transparent Mode	105
12.2. Stealth Mode	105
12.3. Panic Mode	105
12.4. Adding new administrator(s)	106
12.5. Working with logs and reports	108
12.6. Finding users, devices, computers and groups	109
12.7. Search	109
13. Enforced Encryption with Trusted Devices	110
13.1. How a Level 1 Trusted Device Works	111

13.2. EasyLock Software for Trusted Devices Level 1	112
14. Endpoint Protector Client	114
14.1. Endpoint Protector Client Security	114
14.2. Client Notifications (Notifier)	114
14.3. Offline Functionality for Endpoint Protector Client	115
14.4. DHCP / Manual IP address	115
14.5. Client Removal	115
14.5.1. Client Removal on Windows OS	115
14.5.2. Client removal on MAC OS X	116
15. Installing Root Certificate to your Internet Browser	117
15.1. For Microsoft Internet Explorer	117
15.2. For Mozilla Firefox	123
16. Terms and Definitions	125
16.1. Server Related	125
16.2. Client Related	126
17. Support	128
18. Important Notice / Disclaimer	129

1. Introduction

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

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

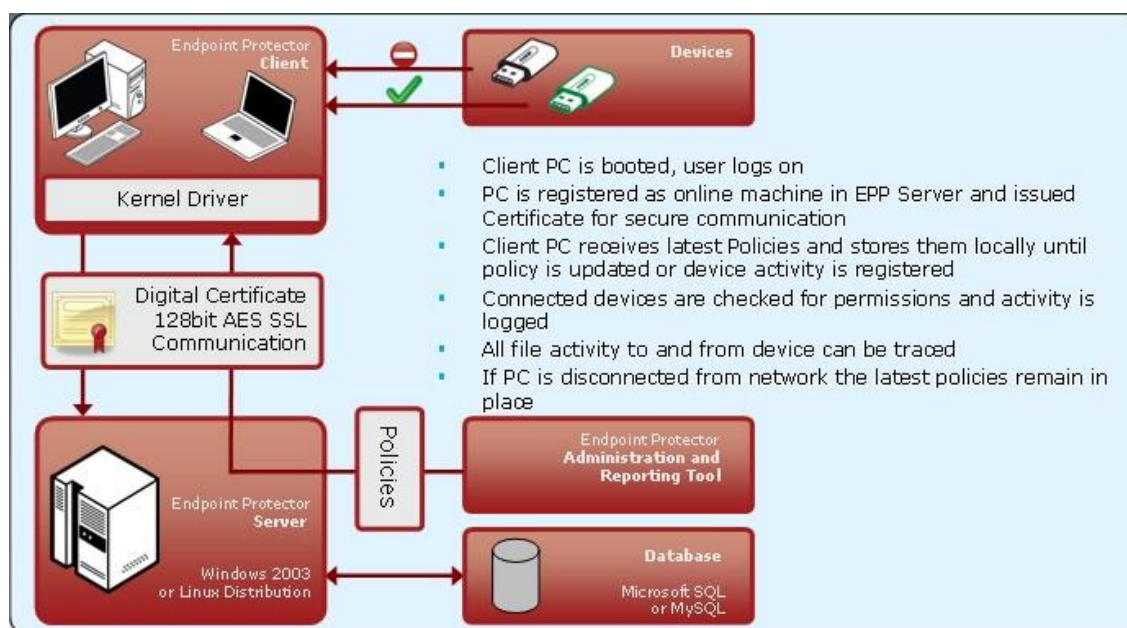
Data theft or data loss or infecting companies' computers or network through a simple connection is easy and doesn't take more than a minute. Network administrators had little chance to prevent this from happening or to catch the responsible user(s). This was the hard reality. Now Endpoint Protector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

1.1. What is Endpoint Protector?

Endpoint Protector will help you secure your PCs endpoints within your network. You will be able to restrict the use of both internal and external devices which can be used for data storage and transfer and to manage PC and MAC ports.

Endpoint Protector gives network administrators the control needed to keep network endpoints safe.

- Control use of all USB and other storage devices
- Tracking of what data is saved to storage devices
- Tracking of what data is copied from and to storage devices
- Authorize the use of USB storage devices
- Securing data on USB storage devices
- Powerful reporting tool and audit



The modular and intuitive Web-based administration interface has been designed to offer fast access to controlling computer, devices and user behavior in a large network. It also offers several ways to track any kind of portable device related activity registered on the system. A detailed report including timestamps, file names, action(s) taken, logged user, etc. allows for pin-pointing malicious behavior and users.

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

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

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

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

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

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

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

<http://www.EndpointProtector.com>

1.2. Main Features

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

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

Endpoint Protectors full feature set is available for Windows. A reduced feature set is available for Macintosh (OS X).

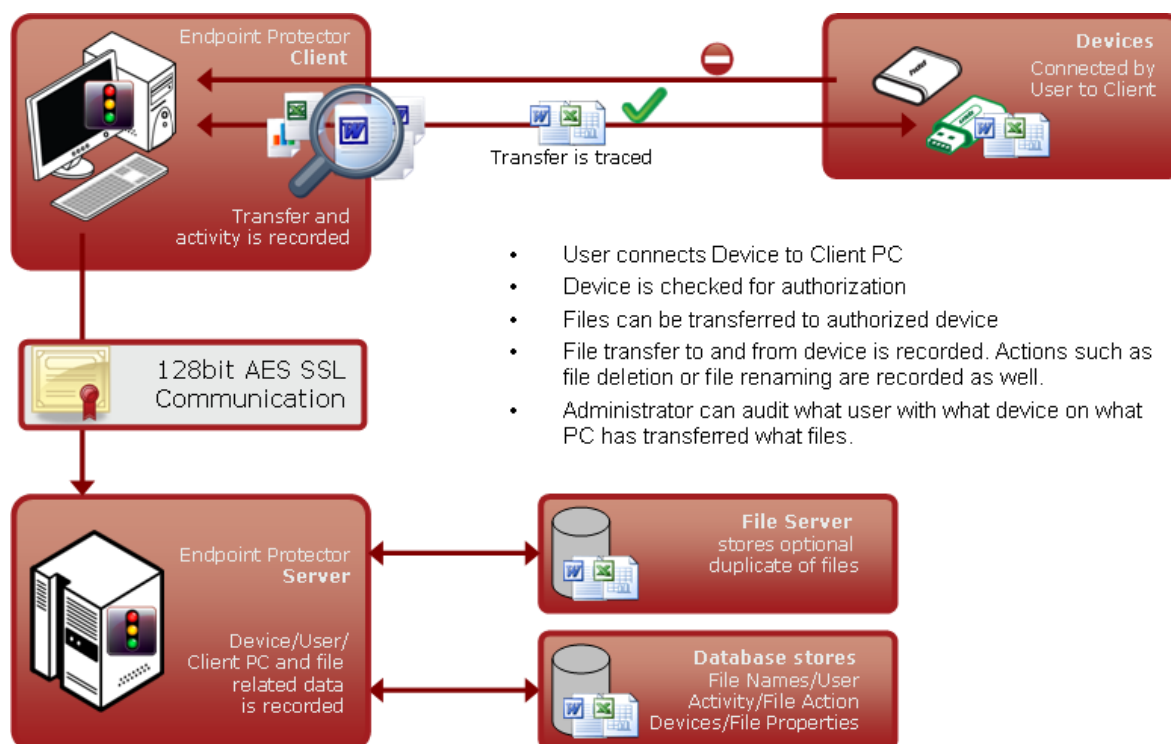
Protects PCs from threats posed by removable portable storage and endpoint devices like USB Flash Drives, MP3 Players, iPods, digital cameras and other devices that could be intentionally or accidentally used to leak, steal, lose, virus or malware infect your data. Even self-executing devices like a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

1.2.1. Centralized web based Device Management / Dashboard

Network administrators have the ability to centrally manage and authorize the use of devices. The Endpoint Protector 2009 Dashboard is designed to meet the needs of both management and security staff and offer access to real-time information, charts and reports about organization wide controlled device and data transfer activity. All in an integrated single view and web based Administration and Reporting Tool.

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

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



1.2.3. Audit Trail – Device Activity Logging

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

1.2.4. Audit Trail – Reporting and Analysis Tools

Endpoint Protector 2009 is equipped with powerful reporting and analysis tools to make the data audit process easy and straightforward.

1.2.5. File Whitelist

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

1.2.6. Easy Enforcement of Your Security Policies

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

1.2.7. Network "Offline" Mode to Support Your Field Employees

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

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

1.2.8. Enforced Encryption - protecting sensitive data in transit / TrustedDevice

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

1.2.9. Client Uninstall Protection

Endpoint Protector 2009 offers a password-based solution that prevents the users from uninstalling the Endpoint Protector Clients, thus ensuring continuous data protection.

1.2.10. Client Stop Protection / Tamper Protection

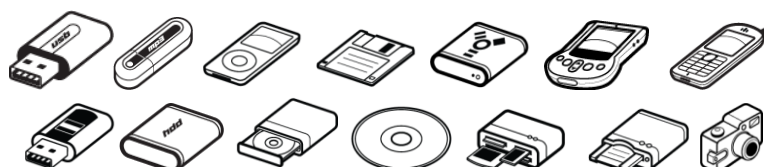
Endpoint Protector 2009 is preventing the users from stopping the Endpoint Protector Clients at any time.

1.2.11. Backup Scheduler

Endpoint Protector 2009 is providing an automatic log backup solution in order to prevent the server from overloading.

1.3. Controlled Device Types / Ports

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



- Removable Storage Devices
 - Normal USB Flash Drives, U3 and Autorun Drives, Disk on Key, etc.
 - USB 1.1, USB 2.0, USB 3.0
 - Wireless USB
 - LPT/Parallel ports

By controlling the Parallel ports of a PC using Endpoint Protector, the network administrator can deny or allow users access to storage devices connected to these ports.

* APPLIES ONLY TO STORAGE DEVICES
 - Floppy disk drives

Access to floppy disk drives can be managed through Endpoint Protector and can be turned on/off completely.
 - Memory Cards - SD Cards, MMC Cards, and Compact Flash Cards, etc.

These devices can be enabled / disabled via Endpoint Protector.
 - Card Readers - internal and external

These devices can be enabled / disabled via Endpoint Protector.
 - CD/DVD-Player/Burner - internal and external

These devices can be enabled / disabled via Endpoint Protector.
 - Digital Cameras

These devices can be enabled / disabled via Endpoint Protector.

- Smartphones / Handhelds / PDAs
This category includes Nokia N-Series, Blackberry, and Windows CE compatible devices, Windows Mobile devices, etc.
- iPods / iPhones / iPads
These devices can be enabled / disabled via Endpoint Protector.
- MP3 Player / Media Player Devices
These devices can be enabled / disabled via Endpoint Protector.
- External HDDs / portable hard disks
These devices can be enabled / disabled via Endpoint Protector.
- FireWire Devices
These devices can be enabled / disabled via Endpoint Protector.
- PCMCIA Devices
These devices can be enabled / disabled via Endpoint Protector.
- Biometric Devices
These devices can be enabled / disabled via Endpoint Protector.
- Bluetooth
These devices can be enabled / disabled via Endpoint Protector.
- Printers
Applies to serial, USB and LTP connection methods. These devices can be enabled / disabled via Endpoint Protector.
- ExpressCard (SSD)
These devices can be enabled / disabled via Endpoint Protector.

1.4. Conclusions

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

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

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

2. Server Functionality / Server Components

The functionality is designed to be around several physical entities:

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

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

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

2.1. Endpoint Protector – Web Service

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

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

2.2. Administration and Reporting Tool

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

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

Dashboard – Lets you view statistics of the server such as the number of clients and devices currently corrected, total number of computers, log and shadow size, last logged action, newest added client, etc. and also provides shortcuts to the essential management tools.– Lets you view statistics of the server such as the number of clients and devices currently corrected, total number of computers, log and shadow size, last logged action, newest added client, etc. and also provides shortcuts to the essential management tools.

The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The top bar includes the logo, title, and user information. The sidebar on the left lists navigation options. The main content area is titled 'System Overview' and contains several panels:

- System Information:** Displays statistics such as 'Number of computers online: 1', 'Total number of computers: 1', 'Number of devices connected: 1', 'Total number of devices: 1', and 'Total number of users: 3'.
- Recently Added:** Lists recently added computers, devices, and users. For example, under 'Computers', it shows 'MacBook Pro [raul]'. Under 'Devices', it shows 'USB2.0 FlashDisk [raul [MacBook Pro]]'. Under 'Users', it shows 'raul raul [MacBook Pro]', 'No user No User [N/A]', and 'AutoRun User AutoRun User [N/A]'.
- Shortcuts:** A grid of links to various management functions like Management, Computers, Users, Devices, Settings, Rights, Reporting, etc.
- Latest System Alerts:** A table showing alerts with columns for Computer, Device, User, and Event. It lists three entries for MacBook Pro with USB2.0 FlashDisk connected by user 'raul'.
- Statistics:** A section showing 'Most active computers' (MacBook Pro), 'Most active devices' (USB2.0 FlashDisk), and 'Most active users' (raul).

The footer of the dashboard displays 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

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



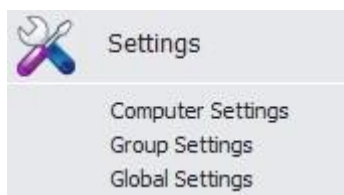
In this module, the administrator can edit, manage rights and settings for or even delete devices, computers or groups. He can also create groups and add or remove client users.

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



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

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



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

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



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

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



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



2.3. Accessing the Administration and Reporting Tool

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

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

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

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

If you use Internet Explorer, we recommend that you add this page to Internet Explorer's trusted sites. To do this, follow the steps in paragraph 15 "Installing Root Certificate to your Internet Browser".

2.4. Login Credentials (Username and Password)

The default username and password for Endpoint Protector 2009 Administration and Reporting Tool are:

USERNAME: root

PASSWORD: epp2009

To change the user name and password and to create additional administrators please see paragraph 10.2 "System Administrators".

3. Management

3.1. Devices

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

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

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, title, and user information (Welcome Super Administrator | Logout). A sidebar on the left contains a menu with options: Dashboard, Management (selected), Devices, Computers, Users, Groups, Custom Classes, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'List of Devices' and features a 'Filter' dropdown and a 'Results' table. The table lists one device with the following details:

Status	ID	Device Type	Device Name (Identification)	Description	Last Location	Last User	Last Connection	VID	PID	Serial Number	Actions
		USB Storage Device	USB2.0 FlashDisk	USB2.0 FlashDisk / Kingmax	MacBook Pro	raul	17-Jul-2010 11:34	1687	6211	777090211FFFFFF000000...	

Below the table, it indicates '1 result' and '20 per page'. A 'Create' button is located at the bottom left of the results area. The footer contains copyright information for CoSoSys Ltd. and the version number 3.0.5.0.

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



Edit, Manage Rights, Delete

Manage Rights is actually a shortcut to the Devices Rights module, and will be explained in one of the following chapters.

The status column indicates the current rights for the devices.



Red means that the device is blocked in the system.



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



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

3.2. Device Functionality

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



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

- Preserve Global settings
- Deny access to devices
- Allow access to devices
- Enable read-only access
- TrustedDevice Level 1 to Level 4



3.2.1. Give / Deny Access to Devices

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

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

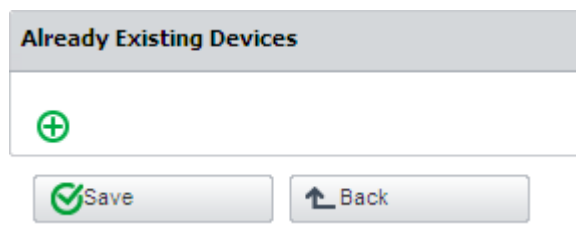
The File Whitelisting feature allows the super administrator to control the transfer of only authorized files to previously authorized portable storage devices.

To configure File Whitelisting, please see paragraph 4.6 "File Whitelist".

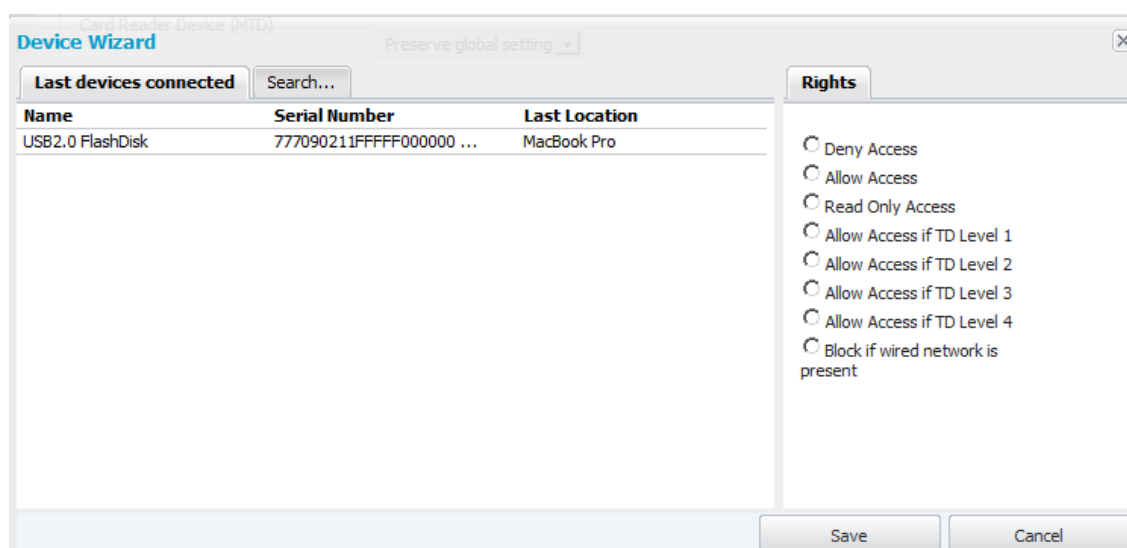
Once configured, you can enable this feature for devices, users, computers and groups. To do this, simply access the Rights module and select device, computer, user or group rights, depending on the rights priority configuration of your server.



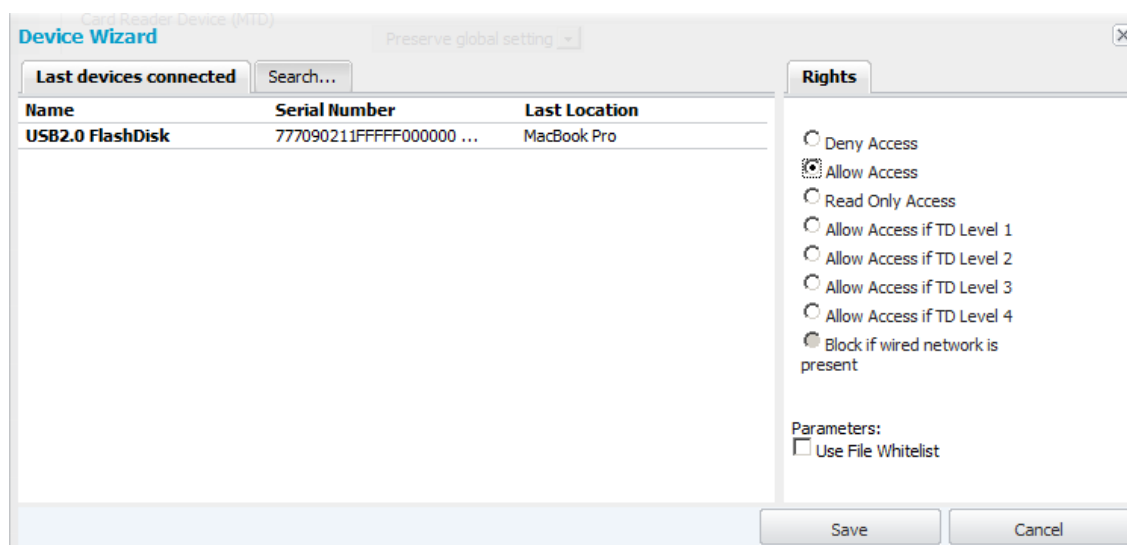
Select the device, user, computer or group you wish to manage rights for and click the + (plus) button at the bottom of the page, under “Already Existing Devices”



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



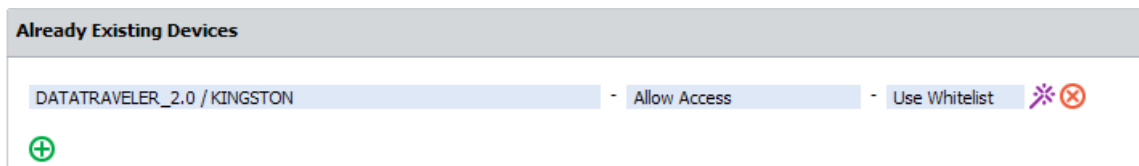
Selecting a device will allow you to select one of the rights for that device.



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

Click “Save” to store your changes.

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



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

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



3.2.2. Enable Device Read-Only Access

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

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

3.2.3. TrustedDevice Level 1 to Level 4

This option has four levels. Selecting either one of these implies that you already have knowledge and understanding of how TrustedDevices™ and EasyLock™ work.

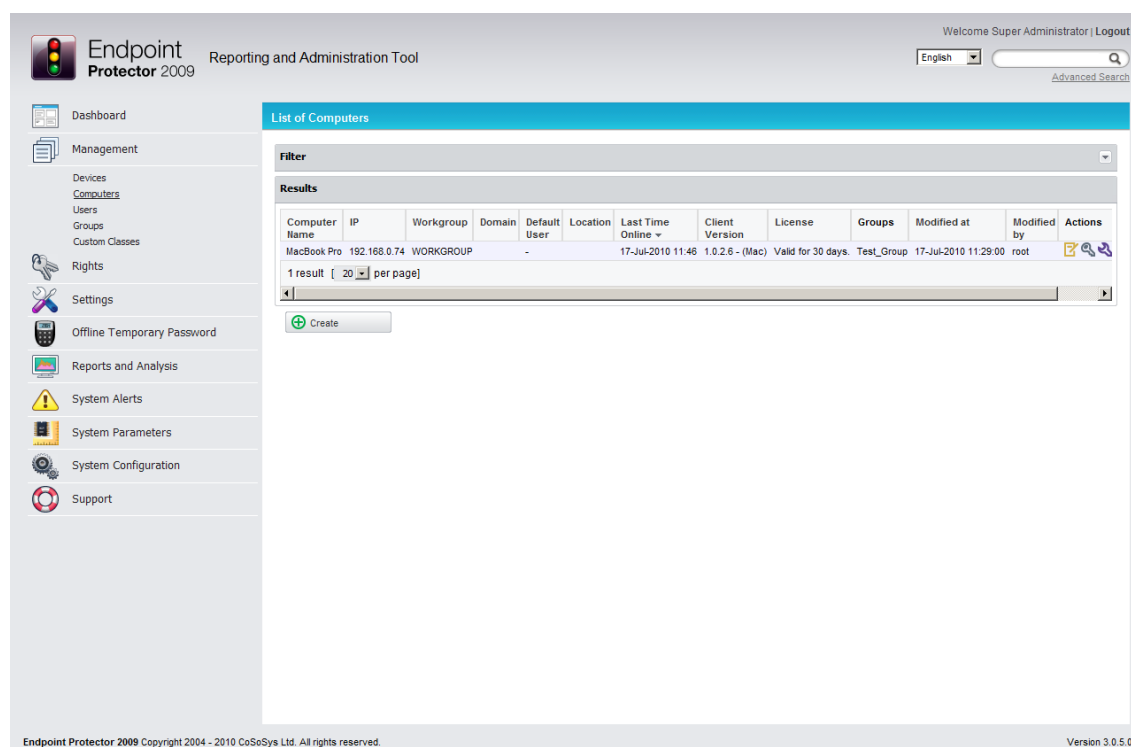
For more information please refer to section “How a Level 1 TrustedDevice Works” in this user manual.

3.2.4. WiFi - Block if wired network is present

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

3.3. Computers

This is the module responsible for managing the client computers.



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

NOTE!

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

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

For details, please consult the paragraph 10.1.1 "Active Directory Import".

The available actions here are:



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

For a better organization and manageability, a computer can be assigned as belonging to a Group (several computers within the same office, a group of computers which will have same access rights or settings).

3.4. Groups

This module is responsible for editing groups. Edit it is the only command available from this sections.

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The top navigation bar includes the product logo, a 'Welcome Super Administrator | Logout' message, a language dropdown set to 'English', and a search bar with an 'Advanced Search' link. A left-hand sidebar contains a menu with icons and labels for: Dashboard, Management (with sub-items: Devices, Computers, Users, **Groups**, Custom Classes), Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'List of Groups' and features a 'Filter' section with a dropdown arrow. Below this is a 'Results' table with the following data:

Name ^	Description	Modified at	Modified by	Actions
Test_Group	test	17-Jul-2010 11:41:00	root	[Edit] [Add] [Delete]

Below the table, it indicates '1 result [20 per page]' and includes a 'Create' button with a plus icon. The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' on the left and 'Version 3.0.5.0' on the right.

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

3.5. Users

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

The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, title, and user information. The left sidebar contains a menu with options like Dashboard, Management, Devices, Computers, Users, Groups, Custom Classes, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area displays the 'List of Users' page, which includes a filter section and a table of results. The table lists three users: noUser, autorunUser, and raul. Each user entry has a set of action icons (edit, delete, etc.) in the 'Actions' column. Below the table, there is a 'Create' button and a footer with copyright information.

Username	First Name	Last Name	Phone	E-mail	Modified at	Modified by	Actions
noUser	No user	No User					[Edit] [Delete] [Add]
autorunUser	AutoRun User	AutoRun User					[Edit] [Delete] [Add]
raul	raul	raul					[Edit] [Delete] [Add]

3 results [20 per page]

Create

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

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



Actions available in this group are: **Edit** and **Delete**.

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

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

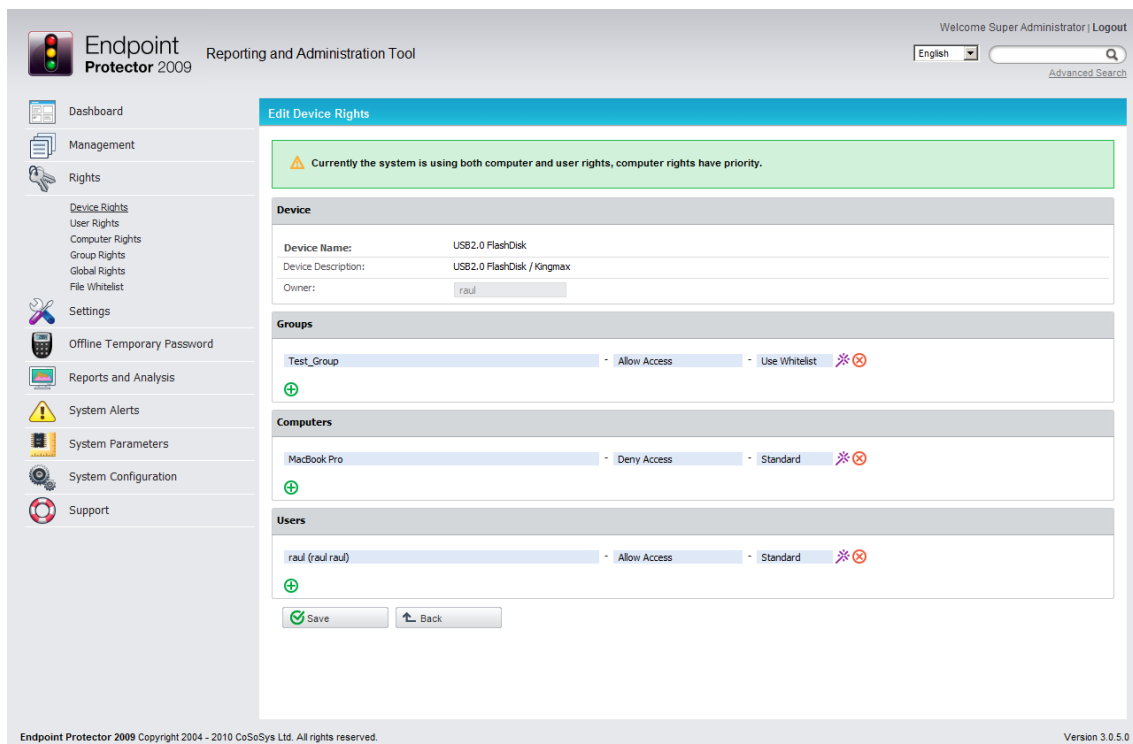
autorunUser – indicates that an installer has been launched by Windows from the specific device. It is the user attached to all events generated by the programs launched from the specific device when Autoplay is enabled in the Operating System.

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

For details, please consult the paragraph 10.1.1 Active Directory Import”.

4. Rights

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

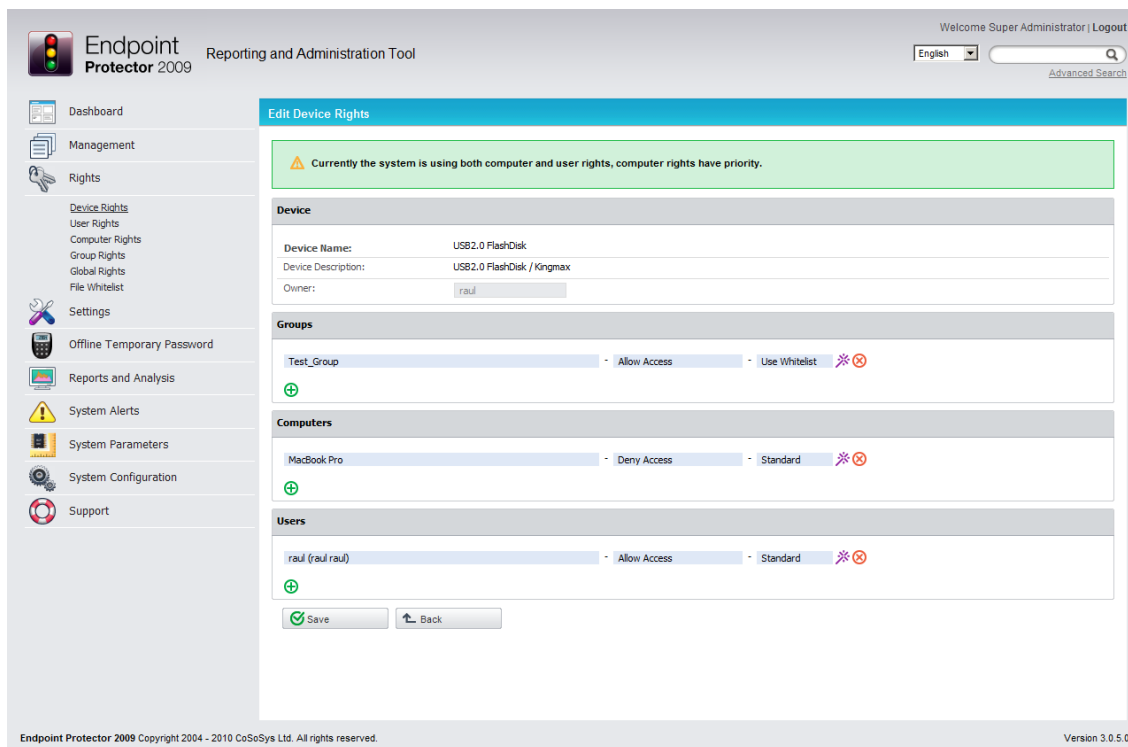


The rule of inheritance is as follows (from most important to least important): Computer Rights -> Group Rights -> Global Rights. The rights are overwritten in this order.

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

4.1. Device Rights

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



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

4.2. User Rights

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

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The top navigation bar includes the product logo, the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with a magnifying glass icon and the text 'Advanced Search'. The left sidebar contains a tree view with the following items: Dashboard, Management, Rights (selected), Device Rights, User Rights (sub-item under Rights), Computer Rights, Group Rights, Global Rights, File Whitelist, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support.

The main content area is titled 'Edit User Rights' and contains the following sections:

User Information:

- User Name: raul
- First Name: raul
- Last Name: raul

Device Types:

Unknown Device	Preserve global setting ▼
USB Storage Device	Preserve global setting ▼
Digital Camera	Preserve global setting ▼
SmartPhone (USB Sync)	Preserve global setting ▼
SmartPhone (Windows CE)	Preserve global setting ▼
SmartPhone (Symbian)	Preserve global setting ▼
Internal Card Reader	Preserve global setting ▼
PCMCIA Device	Preserve global setting ▼
FireWire Bus	Preserve global setting ▼
ZIP Drive	Preserve global setting ▼
Internal CD or DVD RW	Preserve global setting ▼
Internal Floppy Drive	Preserve global setting ▼
Card Reader Device (MTD)	Preserve global setting ▼
Card Reader Device (SCSI)	Preserve global setting ▼
Windows Portable Device	Preserve global setting ▼
Mobile Phones (Sony Ericsson, etc.)	Preserve global setting ▼
Local Printers	Preserve global setting ▼
Bluetooth	Preserve global setting ▼
WiFi	Preserve global setting ▼
BlackBerry	Preserve global setting ▼
Webcam	Preserve global setting ▼
Serial Port	Preserve global setting ▼

The footer of the application window shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' on the left and 'Version 3.0.5.0' on the right.

4.3. Computer Rights

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

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The top navigation bar includes the logo, 'Welcome Super Administrator | Logout', and a language dropdown set to 'English'. A left sidebar contains a tree view with categories: Dashboard, Management, Rights (selected), Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. Under 'Rights', sub-items include Device Rights, User Rights, **Computer Rights** (highlighted), Group Rights, Global Rights, and File Whitelist.

The main content area is titled 'Edit Computer Rights' and features a green warning banner: 'Currently the system is using both computer and user rights, computer rights have priority.' Below this, the 'Computer' section shows 'Computer Name: MacBook Pro' and an empty 'Location' field. The 'Device Types' section contains a table with 20 rows, each listing a device type and a corresponding dropdown menu set to 'Preserve global setting'.

Device Types	Setting
Unknown Device	Preserve global setting
USB Storage Device	Allow Access
Digital Camera	Preserve global setting
SmartPhone (USB Sync)	Preserve global setting
SmartPhone (Windows CE)	Preserve global setting
SmartPhone (Symbian)	Preserve global setting
Internal Card Reader	Preserve global setting
PCMCIA Device	Preserve global setting
FireWire Bus	Preserve global setting
ZIP Drive	Preserve global setting
Internal CD or DVD RW	Preserve global setting
Internal Floppy Drive	Preserve global setting
Card Reader Device (MTD)	Preserve global setting
Card Reader Device (SCSI)	Preserve global setting
Windows Portable Device	Preserve global setting
Mobile Phones (Sony Ericsson, etc.)	Preserve global setting
Local Printers	Preserve global setting
Bluetooth	Preserve global setting
WiFi	Preserve global setting

The footer of the application window shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' on the left and 'Version 3.0.5.0' on the right.

4.4. Group Rights

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

The screenshot displays the 'Edit Group Rights' window within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights (selected), Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The 'Rights' section is further divided into Device Rights, User Rights, Computer Rights, Group Rights (selected), Global Rights, and File Whitelist.

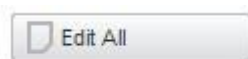
The main content area is titled 'Edit Group Rights' and contains a table of device types and their associated rights. The table has two columns: 'Device Types' and a dropdown menu for selecting the right. The 'Already existing devices' section is currently empty.

Device Types	Right
Unknown Device	Preserve global setting
USB Storage Device	Allow Access
Digital Camera	Preserve global setting
SmartPhone (USB Sync)	Preserve global setting
SmartPhone (Windows CE)	Allow Access
SmartPhone (Symbian)	Deny Access
Internal Card Reader	Preserve global setting
POMCIA Device	Preserve global setting
FireWire Bus	Allow Access
ZIP Drive	Preserve global setting
Internal CD or DVD RW	Read Only Access
Internal Floppy Drive	Preserve global setting
Card Reader Device (MTD)	Preserve global setting
Card Reader Device (SCSI)	Preserve global setting
Windows Portable Device	Preserve global setting
Mobile Phones (Sony Ericsson, etc.)	Preserve global setting
Local Printers	Preserve global setting
Bluetooth	Preserve global setting
WiFi	Preserve global setting
BlackBerry	Preserve global setting
Webcam	Preserve global setting
Serial Port	Preserve global setting

Below the table, there is a section titled 'Already existing devices' with a green plus icon and a dropdown arrow.

At the bottom of the window, the footer text reads: 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

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



4.5. Global Rights

This module applies rights to computers in the entire system.

The screenshot displays the 'Management of Global Rights' interface within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights (with sub-options: Device Rights, User Rights, Computer Rights, Group Rights, Global Rights, File Whitelist), Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area shows the 'Management of Global Rights' section with a 'Groups' table and a 'Device Types' table.

Groups

Name:	Global
Description:	Global Group including all the entities

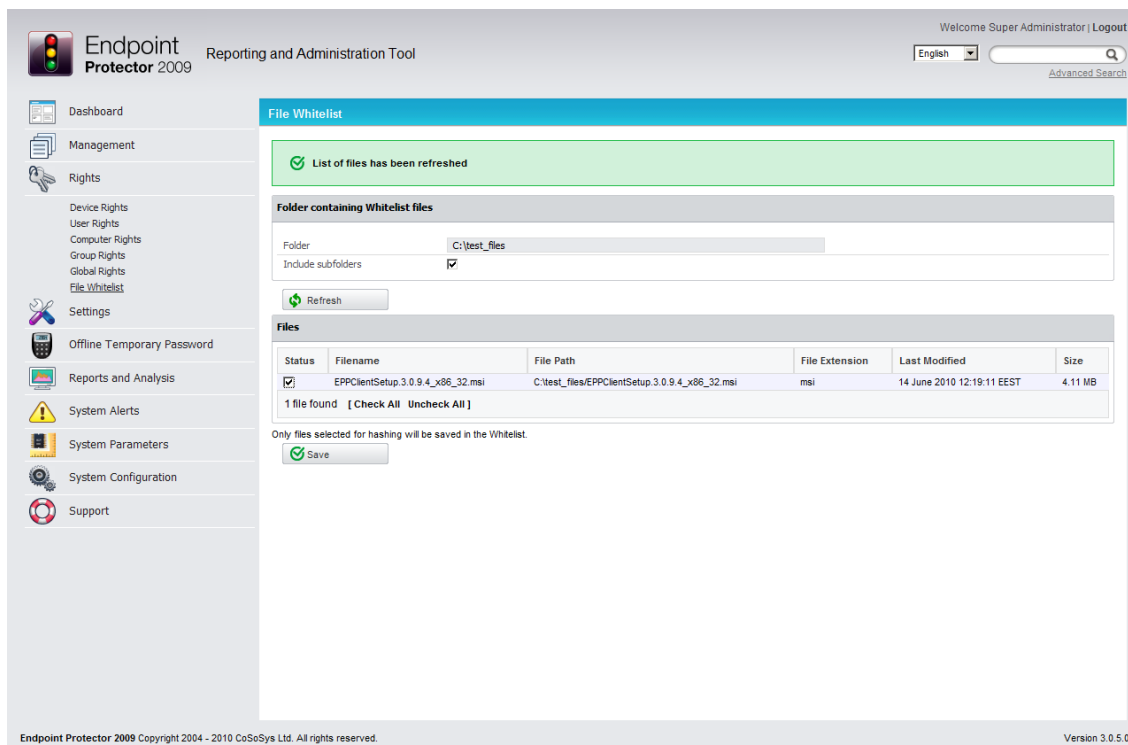
Device Types

Unknown Device	Deny Access	▼
USB Storage Device	Deny Access	▼
Digital Camera	Deny Access	▼
SmartPhone (USB Sync)	Deny Access	▼
SmartPhone (Windows CE)	Deny Access	▼
SmartPhone (Symbian)	Deny Access	▼
Internal Card Reader	Deny Access	▼
PCMCIA Device	Deny Access	▼
FireWire Bus	Deny Access	▼
ZIP Drive	Deny Access	▼
Internal CD or DVD R/W	Deny Access	▼
Internal Floppy Drive	Deny Access	▼
Card Reader Device (MTD)	Deny Access	▼
Card Reader Device (SCSI)	Deny Access	▼
Windows Portable Device	Deny Access	▼
Mobile Phones (Sony Ericsson, etc.)	Deny Access	▼
Local Printers	Deny Access	▼
Bluetooth	Deny Access	▼
WiFi	Allow Access	▼
BlackBerry	Deny Access	▼

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

4.6. File Whitelist

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



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



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

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

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

Note!

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

5. Offline Temporary Password

5.1. Generating the Offline Temporary Password

This module allows the super administrator to generate a temporary password for a specific device on a client user computer. It can be used when there is no network connection between the client computer and the Server.

Note!

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

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

The password will give permission to the device for the specified amount of time.

The time intervals which can be selected are: 30 minutes, 1 hour, 2 hours, 4 hours, 8 hours, 1 day, 2 days, 5 days, 14 days and 30 days.

The screenshot shows the 'Generate Offline Temporary Password' wizard in the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Offline Temporary Password (selected), Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Generate Offline Temporary Password' and contains the following sections:

- Computer Details:**
 - Computer Name: MacBook Pro
 - IP: 192.168.0.74
 - MAC Address: c4-2c-03-01-b9-6d
 - Domain:
 - Workgroup: WORKGROUP
- Devices:**
 - Search for device: USB2.0 FlashDisk
 - or
 - Enter device code (case sensitive): F953
- Other Options:**
 - Duration: 30 min
 - ☒ Generate Code
- Generated Password:**
 - Password: 6niifqtd0

The footer of the application displays 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

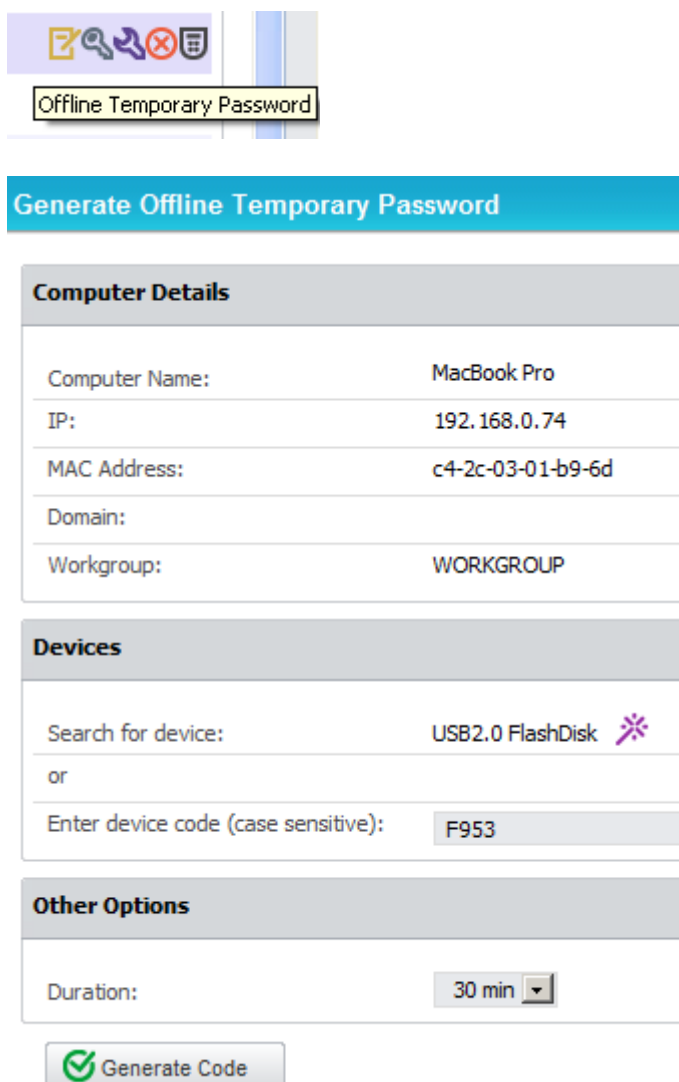
The administrator can either search for an existing device using the search

wizard

or, in case the device is not already in the database, he can introduce the device code communicated by the client user (explained in below paragraph).

After selecting the duration, the password will be generated by clicking "Generate Code" button.

Another way to generate a password is by selecting a client computer from Management Computers list, with the action "Offline Temporary Password".




The image shows a software interface for generating an offline temporary password. At the top, a menu bar contains several icons, with 'Offline Temporary Password' highlighted. Below this is a dialog box titled 'Generate Offline Temporary Password'.


Computer Details


Computer Name:	MacBook Pro
IP:	192.168.0.74
MAC Address:	c4-2c-03-01-b9-6d
Domain:	
Workgroup:	WORKGROUP

Devices

Search for device:	USB2.0 FlashDisk 
or	
Enter device code (case sensitive):	F953

Other Options

Duration:	30 min 
-----------	--

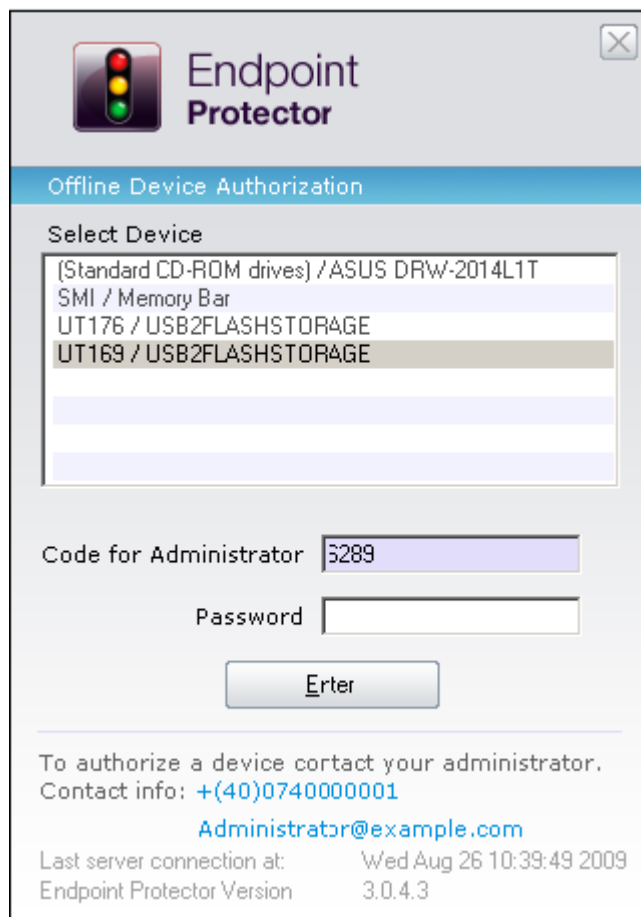
 Generate Code

The obtained password will be communicated to the user for temporarily allowing his specific device as explained bellow.

5.2. Offline Device Authorization

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

The user will select the device from the list and contact the administrator at the displayed contact information.



The screenshot shows a window titled "Endpoint Protector" with a traffic light icon. The main heading is "Offline Device Authorization". Below this is a "Select Device" section with a list box containing the following items: "(Standard CD-ROM drives) / ASUS DRW-2014L1T", "SMI / Memory Bar", "UT176 / USB2FLASHSTORAGE", and "UT169 / USB2FLASHSTORAGE". The last item is selected. Below the list box are two input fields: "Code for Administrator" with the value "3289" and "Password" which is empty. An "Enter" button is positioned below the password field. At the bottom, there is a message: "To authorize a device contact your administrator. Contact info: +(40)0740000001" followed by "Administrator@example.com" in blue. Below this, it shows "Last server connection at: Wed Aug 26 10:39:49 2009" and "Endpoint Protector Version 3.0.4.3".

The user will tell the administrator the code for the device and the administrator will tell the user the password, after generating it on the Server (see above paragraph for password generation).

The password will be inserted in the correspondent field and applied by clicking "Enter".

5.3. Setting the Administrator Contact Information

The Administrator contact information can be edited under “System Configuration” module, “System Settings” panel, edit “Main Administrator Contact Details”, then click “Save”.

Main Administrator Contact Details

Phone:	<input type="text" value="+ (40) 0740000001"/>
E-mail:	<input type="text" value="Administrator@example.com"/>

Save

6. Settings

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

Computer Settings (settings applied to one exact computer).

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Computer Settings (selected), Group Settings, Global Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Edit Settings for Computer' and is divided into several sections:

- Computer**: Fields for Default User (empty), IP (192.168.0.74), MAC Address (c4-2c-03-01-b9-6d), Computer Name (MacBook Pro), and Location (empty).
- Mode**: Fields for Refresh Interval (sec) (10) and Mode (Normal).
- File Tracing and Shadowing**: Checkboxes for File Tracing (checked) and File Shadowing (checked).
- Settings**: Fields for Log Interval (min) (1), Local Log Size (MB) (10), Shadow Interval (min) (1), Shadow Size (MB) (99999), Min File Size for Shadowing (KB) (0), Max File Size for Shadowing (KB) (99999), and Notifier Language (English).
- Logging**: A section with a dropdown arrow.

The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' on the left and 'Version 3.0.5.0' on the right.

Group Settings (settings applied on a group).

The screenshot shows the 'Edit Group Settings' page in the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Computer Settings, Group Settings, Global Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Edit Group Settings' and contains the following sections:

- Group:**
 - Name: Test_Group
 - Description: test
- Mode:**
 - Refresh Interval (sec): 10
 - Mode: Normal
- File Tracing and Shadowing:**
 - File Tracing: ☒
 - File Shadowing: ☐
- Settings:**
 - Log Interval (min): 30
 - Local Log Size (MB): 10
 - Shadow Interval (min): 60
 - Shadow Size (MB): 512
 - Min File Size for Shadowing (KB): 0
 - Max File Size for Shadowing (KB): 512
 - Notifier Language: English
- Logging:**
 - Created at: 17-Jul-2010 11:41:00
 - Created by: root
 - Modified at: 17-Jul-2010 11:41:00

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

Global Settings (settings applied for all the computers).

The screenshot shows the 'Management of Global Settings' page in the Endpoint Protector 2009 Reporting and Administration Tool. The interface is similar to the previous one, with the same sidebar and main content area. The main content area is titled 'Management of Global Settings' and contains the following sections:

- Group:**
 - Name: Global
 - Description: Global Group including all the entities
- Mode:**
 - Refresh Interval (sec): 10
 - Mode: Normal
- File Tracing and Shadowing:**
 - File Tracing: ☒
 - File Shadowing: ☐
- Settings:**
 - Log Interval (min): 30
 - Local Log Size (MB): 10
 - Shadow Interval (min): 60
 - Shadow Size (MB): 512
 - Min File Size for Shadowing (KB): 0
 - Max File Size for Shadowing (KB): 512
 - Notifier Language: English
- Logging:**
 - Created at:
 - Created by: root
 - Modified at: 15-Jul-2010 12:53:00

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

The settings and the rights for computers are sent to the client computer at an exact interval of time, set in this section.

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

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

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

This mechanism is optimal when a client computer has a lot of activity, because it will send the information very quickly to the server, so the administrator can be informed almost instantly about the activities on that computer.

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

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

Minimum File Size for Shadowing (in kilobytes) – represents the minimum file size that should be shadowed. If a value is set here than files smaller in size than that value will not be shadowed. If "0" –null is the value set for this field, then it will be ignored and only the maximum file size will be taken into consideration.

Maximum File Size for Shadowing (in kilobytes) – represents the maximum file size that should be shadowed. If a value is set here, then files larger in size than that value will not be shadowed. If "0" –null is the value set for this field, then it will be ignored and only the minimum file size will be taken into consideration.

6.1. Computer Settings

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

The screenshot displays the 'Edit Settings for Computer' window within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Computer Settings (selected), Group Settings, Global Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Edit Settings for Computer' and contains several sections:

- Computer**: Fields for Default User (set to '-'), IP (192.168.0.74), MAC Address (c4-2c-03-01-b9-6d), Computer Name (MacBook Pro), and Location.
- Mode**: Fields for Refresh Interval (sec) (set to 10) and Mode (set to Normal).
- File Tracing and Shadowing**: Checkboxes for File Tracing and File Shadowing, both of which are checked.
- Settings**: Fields for Log Interval (min) (1), Local Log Size (MB) (10), Shadow Interval (min) (1), Shadow Size (MB) (99999), Min File Size for Shadowing (KB) (0), Max File Size for Shadowing (KB) (99999), and Notifier Language (English).
- Logging**: A section at the bottom, currently empty.

The footer of the application shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

Defining custom settings for all computers is not necessary, since a computer is perfectly capable of functioning correctly without any manual settings defined. It will do this by either inheriting the settings of a group it's in or, if not possible, the global settings, which are mandatory and exist in the system with default values from installation.

6.2. Group Settings

This module will allow the administrator to edit group settings.

The screenshot displays the 'Edit Group Settings' window within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Computer Settings, Group Settings (selected), Global Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Edit Group Settings' and contains several sections:

- Group**: Fields for Name (Test_Group) and Description (test).
- Mode**: Fields for Refresh Interval (sec) (10) and Mode (Normal).
- File Tracing and Shadowing**: Checkboxes for File Tracing (checked) and File Shadowing (unchecked).
- Settings**: Fields for Log Interval (min) (30), Local Log Size (KB) (10), Shadow Interval (min) (60), Shadow Size (KB) (512), Min File Size for Shadowing (KB) (0), Max File Size for Shadowing (KB) (512), and Notifier Language (English).
- Logging**: Fields for Created at (17-Jul-2010 11:41:00), Created by (root), and Modified at (17-Jul-2010 11:41:00).

The footer of the application shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

We mentioned earlier that computers can be grouped so that editing of settings should be easier and more logical.

6.3. Global Settings

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

The screenshot displays the 'Management of Global Settings' page in the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings (with sub-items: Computer Settings, Group Settings, Global Settings), Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Management of Global Settings' and contains the following sections:

- Group:**
 - Name: Global
 - Description: Global Group including all the entities
- Mode:**
 - Refresh Interval (sec): 10
 - Mode: Normal
- File Tracing and Shadowing:**
 - File Tracing: ☒
 - File Shadowing: ☐
- Settings:**
 - Log Interval (min): 30
 - Local Log Size (MB): 10
 - Shadow Interval (min): 60
 - Shadow Size (MB): 512
 - Min File Size for Shadowing (KB): 0
 - Max File Size for Shadowing (KB): 512
 - Notifier Language: English
- Logging:**
 - Created at:
 - Created by: root
 - Modified at: 15-Jul-2010 12:53:00

The footer of the application shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' on the left and 'Version 3.0.5.0' on the right.

6.4. File Tracing

Endpoint Protector's file tracing feature allows monitoring of data traffic between protected clients and portable devices. It shows what files were copied, to which location, at what time and by which user. It also shows other actions that took place, such as file renamed, deleted, accessed, accessed and modified, etc.

It is an essential feature for administrators since they can keep track of all data that's being transferred to and from devices. All traffic is recorded and logged for later auditing.

Administrators have the ability to enable or disable the file tracing feature. This can be done from within the Endpoint Protector Administration and Reporting Tool.

Access the "System Configuration" module and select "System Policies".

Default System Policies	
Mode	
Refresh Interval (sec):	15
Mode:	Normal 
File Tracing and Shadowing	
File Tracing:	<input checked="" type="checkbox"/>
File Shadowing:	<input checked="" type="checkbox"/>

If you wish to disable the file tracing feature, simply uncheck the box next to it and click "Save".

6.5. File Shadowing

Endpoint Protector's File Shadowing feature works simultaneously together with File Tracing, creating exact copies of files accessed by users. The creation of shadow copies can be triggered by the following events: file read, file write, and file read/write. Events such as file deleted, file renamed, etc. do not trigger the function.

Same as File Tracing, Shadowing of files can be turned on or off, from the "System Configuration -> System Policies" module of the Endpoint Protector Reporting and Administration Tool. Please note, however, that this feature cannot be used without the File Tracing feature enabled.

Default System Policies	
Mode	
Refresh Interval (sec):	15
Mode:	Normal 
File Tracing and Shadowing	
File Tracing:	<input checked="" type="checkbox"/>
File Shadowing:	<input type="checkbox"/>

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

Default Client Settings	
Log Upload Interval (min):	30
Local Log Size (KB):	10
Shadow Upload Interval (min):	60
Local Shadow Size (MB):	512
Minimum File Size for Shadowing (KB):	0
Maximum File Size for Shadowing (KB):	512

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

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

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

This mechanism is optimal when a client computer has a lot of activity, because it will send the information very quickly to the server, so the administrator can be informed almost instantly about the activities on that computer.

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

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

Minimum File Size for Shadowing (in KB) – Represents the minimum file size that should be shadowed. If a value is set here than files smaller in size than that value will not be shadowed. If "0" –null is the value set for this field, then it will be ignored and only the maximum file size will be taken into consideration.

Maximum File Size for Shadowing (in KB) – Represents the maximum file size that should be shadowed. If a value is set here, then files larger in size than that value will not be shadowed. If "0" –null is the value set for this field, then it will be ignored and only the minimum file size will be taken into consideration.

The shadow directory can be selected from the “System Configuration” module under the “System Settings” tab.



Default System Settings	
Storage Folders	
Log Dir:	<input type="text"/>
Shadow Dir:	<input type="text"/>

Since shadow size can reach large amounts, we strongly recommend that a separate, large capacity Hard Disk is used for shadow storage.

Note!

Shadowing Files 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.

7. Reports and Analysis

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

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, Log Report, File Tracing, File Shadowing, Online Computers, Online Users, Connected Devices, System Alerts, System Parameters, System Configuration, and Support. The 'Reports and Analysis' section is expanded, showing 'Log Report' as the selected option. The main content area displays a 'Log Report' table with columns: Event, Client Computer, Client User, Device Type, Device, Files, Date/Time(Server), Date/Time(Client), and Actions. The table lists various file operations (File Read, File Write, File Read-Write) on USB Storage Devices. At the bottom, it shows '97 results (20 per page)' and a 'Export' button. The footer indicates 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSecure Ltd. All rights reserved.' and 'Version 3.0.5.0'.

Event	Client Computer	Client User	Device Type	Device	Files	Date/Time(Server)	Date/Time(Client)	Actions
File Read-Write			USB Storage Device		1	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read			USB Storage Device		1	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read-Write			USB Storage Device		1	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read			USB Storage Device		11	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read-Write			USB Storage Device		1	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read			USB Storage Device		3	17-Jun-2010 09:05:00	17-Jun-2010 16:05:00	[Icon]
File Read-Write			USB Storage Device		1	17-Jun-2010 09:04:00	17-Jun-2010 16:03:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:04:00	17-Jun-2010 16:03:00	[Icon]
File Read			USB Storage Device		7	17-Jun-2010 09:04:00	17-Jun-2010 16:03:00	[Icon]
File Read			USB Storage Device		4	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Read-Write			USB Storage Device		1	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Read			USB Storage Device		1	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Read			USB Storage Device		3	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Read			USB Storage Device		2	17-Jun-2010 09:03:00	17-Jun-2010 16:02:00	[Icon]
File Write			USB Storage Device		1	17-Jun-2010 09:01:00	17-Jun-2010 16:01:00	[Icon]
File Read			USB Storage Device		1	17-Jun-2010 09:01:00	17-Jun-2010 16:01:00	[Icon]

7.1. Logs Report

The most powerful and detailed representation of activity recordings can be achieved using this module. It allows the administrator to see exactly what actions took place at what time. This information also contains the computer name, user and device used and also the action taken and the files accessed. The granular filter included in this module is designed to make finding information quick and easy.



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

- Client Computer: [Text input field]
- Client User: [Dropdown menu]
- Device Types: [Text input field]
- Device: [Text input field]
- Event: [Dropdown menu]
- Date/Time(Server): [Text input field] [Clear icon]
- Date/Time(Client): [Text input field] [Clear icon]

At the bottom of the filter section, there are two buttons: 'Reset' and 'Apply filter'.

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

7.2. File Tracing

Displays the list of file properties traced of files that have been transferred from a protected computer to a portable device.

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The 'Reports and Analysis' section is expanded, showing 'Logs Report' and 'File Tracing' (which is selected). The main area shows a 'Log Report' with a 'Filter' dropdown and a 'Results' table. The table has columns: Event, File Name, File Size, File Type, Date/Time(Client), Shadow, and User. The table lists 212 results, with the first few rows showing file transfer events. At the bottom, it indicates '212 results (20 per page)' and a page number '12345'.

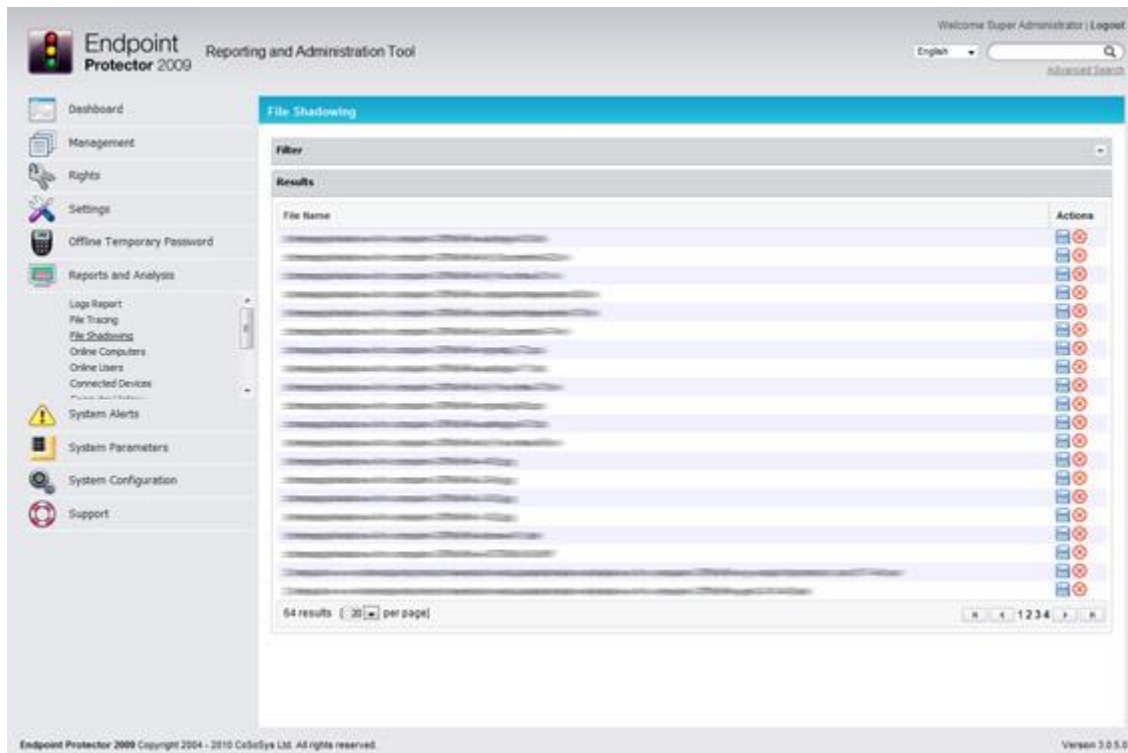
Event	File Name	File Size	File Type	Date/Time(Client)	Shadow	User
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	113 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	113 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	126 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	113 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	147 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	113 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	9 KB	Database File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	147 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	113 B	Initialization File	17-Jun-2010 16:25:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	147 B	Initialization File	17-Jun-2010 16:19:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:19:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	23 B	Initialization File	17-Jun-2010 16:19:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	9 KB	Database File	17-Jun-2010 16:19:00	N/A	
File Transfer	C:\Program Files\Endpoint Protector\Endpoint Protector.exe	126 B	Initialization File	17-Jun-2010 16:19:00	N/A	

212 results (20 per page) 12345

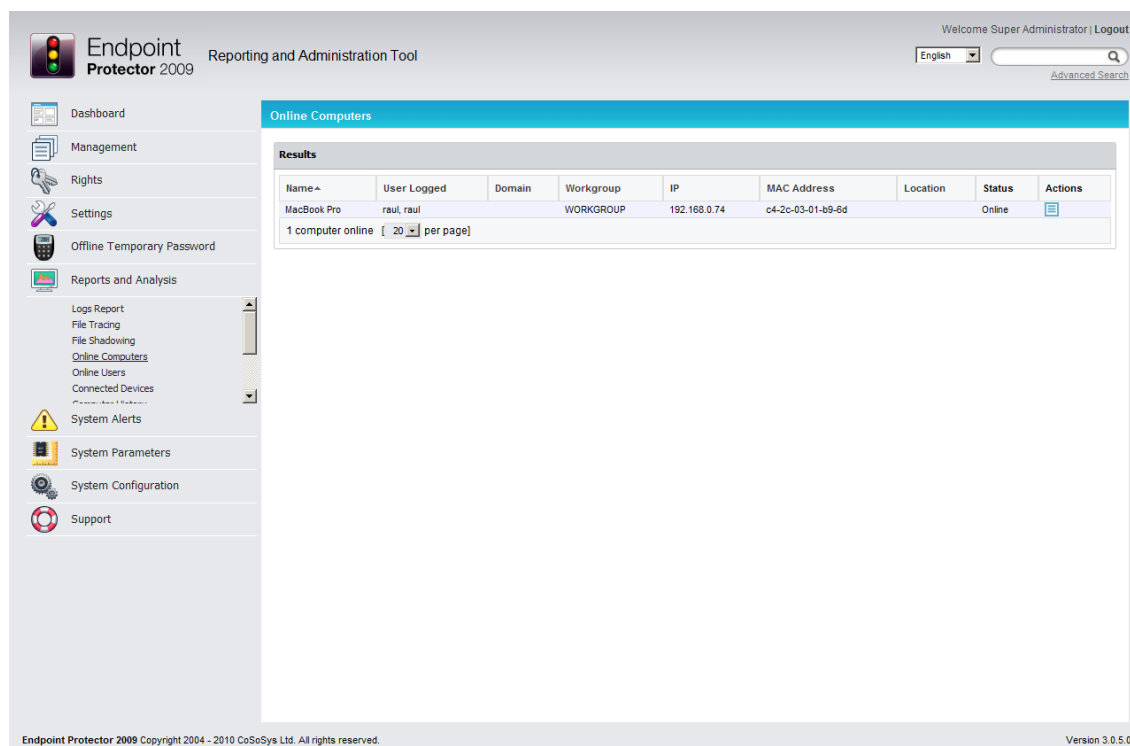
Endpoint Protector 2009 Copyright 2004 - 2010 CoSecure Ltd. All rights reserved. Version 3.0.5.6

7.3. File Shadowing

Displays the list of file shadows, of files, that have been transferred from a protected computer to a portable device.



7.4. Online Computers



The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis (with sub-links: Logs Report, File Tracing, File Shadowing, Online Computers, Online Users, Connected Devices), System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'Online Computers' and displays a table of results. The table has columns: Name, User Logged, Domain, Workgroup, IP, MAC Address, Location, Status, and Actions. One computer is listed: MacBook Pro, with user raul, raul, domain WORKGROUP, IP 192.168.0.74, MAC Address c4-2c-03-01-b9-6d, and Status Online. The Actions column contains a list icon. Below the table, it says '1 computer online' and '[20 per page]'. The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

Name	User Logged	Domain	Workgroup	IP	MAC Address	Location	Status	Actions
MacBook Pro	raul, raul	WORKGROUP		192.168.0.74	c4-2c-03-01-b9-6d		Online	

1 computer online [20 per page]

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

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

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



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

7.5. Online Users

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

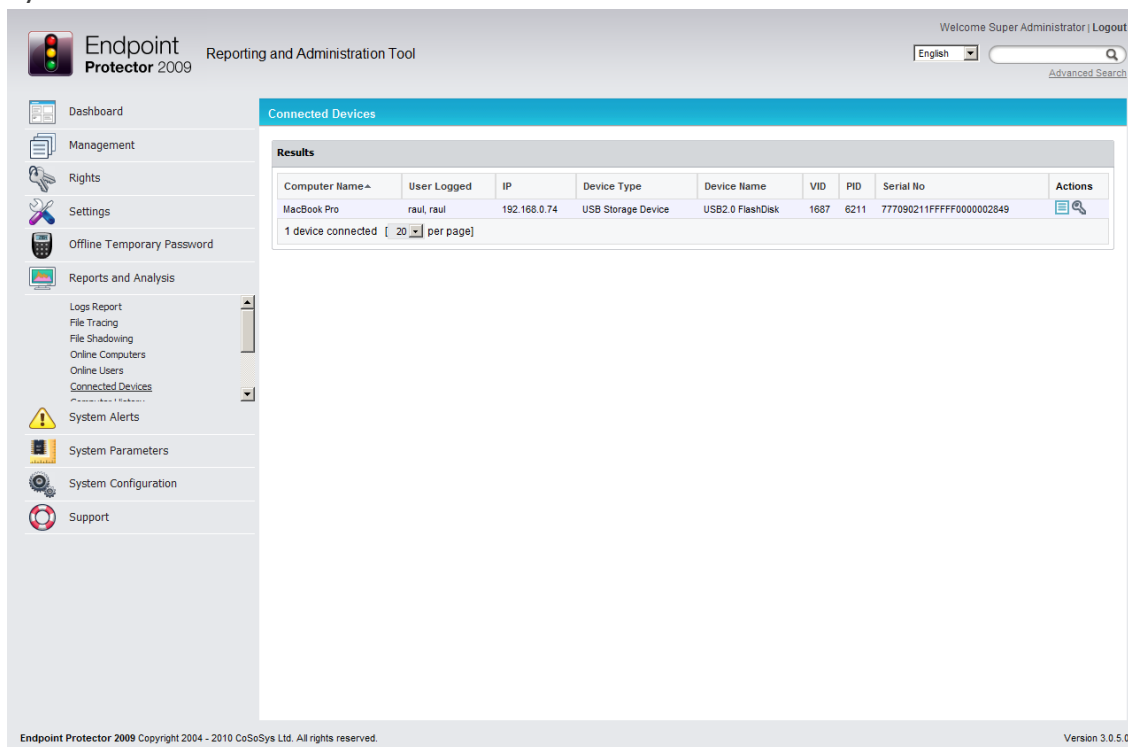
The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, the title "Endpoint Protector 2009 Reporting and Administration Tool", a language dropdown set to "English", a search bar, and a "Welcome Super Administrator | Logout" link. The left sidebar contains a menu with the following items: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis (with a sub-menu showing Logs Report, File Tracing, File Shadowing, Online Computers, Online Users, and Connected Devices), System Alerts, System Parameters, System Configuration, and Support. The main content area is titled "Online Users" and shows a "Results" table with the following data:

Username	Name ^	Computer Name	IP	Connected Device
raul	raul raul	MacBook Pro	192.168.0.74	USB2.0 FlashDisk



Below the table, it indicates "1 user online" and a pagination control showing "20 per page". The footer of the interface contains the copyright notice "Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved." and the version number "Version 3.0.5.0".

7.6. Connected Devices

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



The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with the following items: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis (with sub-items: Logs Report, File Tracing, File Shadowing, Online Computers, Online Users, **Connected Devices**, and System Alerts), System Parameters, System Configuration, and Support. The main content area is titled 'Connected Devices' and shows a table of results. The table has columns for Computer Name, User Logged, IP, Device Type, Device Name, VID, PID, Serial No, and Actions. One device is listed: MacBook Pro, accessed by user raul, with IP 192.168.0.74, identified as a USB Storage Device (USB2.0 FlashDisk) with VID 1687, PID 6211, and Serial No 777090211FFFFF0000002849. Below the table, it indicates '1 device connected' and a pagination control set to '20 per page'. The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

Computer Name	User Logged	IP	Device Type	Device Name	VID	PID	Serial No	Actions
MacBook Pro	raul, raul	192.168.0.74	USB Storage Device	USB2.0 FlashDisk	1687	6211	777090211FFFFF0000002849	 

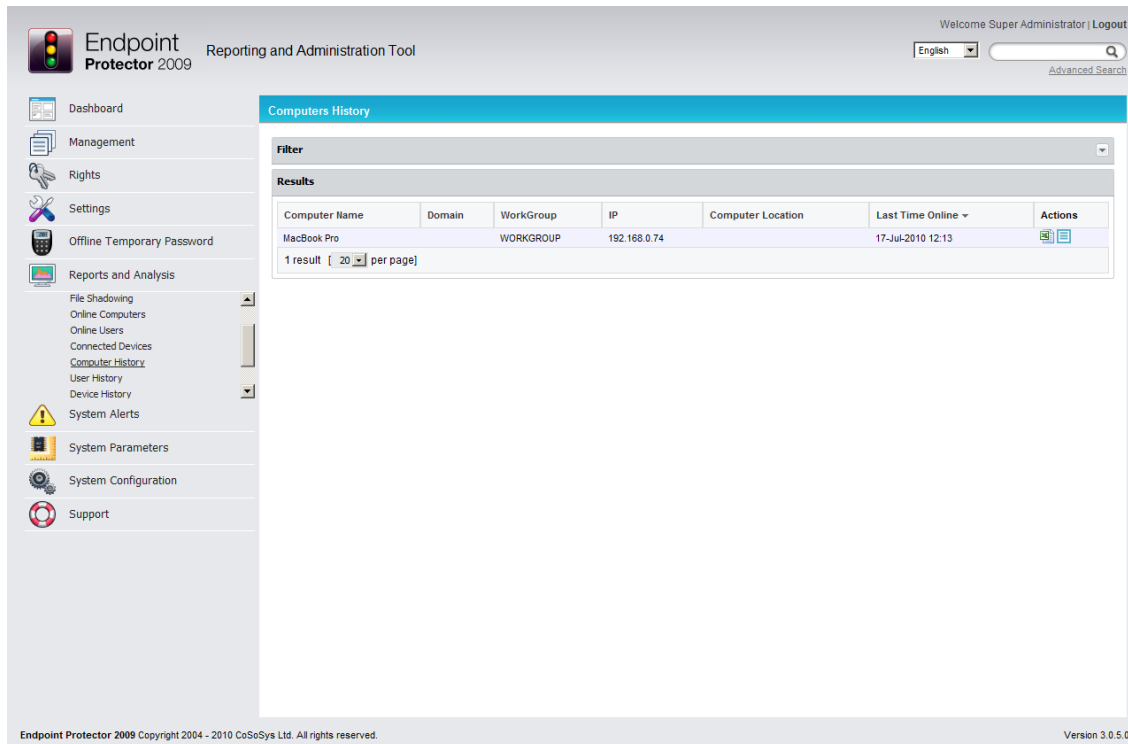
1 device connected [20 per page]

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



7.7. Computer History

This module displays a list of all computers that were once connected to the system.



The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, the title "Endpoint Protector 2009 Reporting and Administration Tool", a language dropdown set to "English", a search bar, and a "Logout" link. The left sidebar contains a menu with the following items: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis (with a sub-menu showing File Shadowing, Online Computers, Online Users, Connected Devices, **Computer History**, User History, and Device History), System Alerts, System Parameters, System Configuration, and Support. The main content area is titled "Computers History" and features a "Filter" section and a "Results" table. The table has columns for Computer Name, Domain, WorkGroup, IP, Computer Location, Last Time Online, and Actions. A single result is displayed for "MacBook Pro" in the "WORKGROUP" domain with IP "192.168.0.74" and "Last Time Online" of "17-Jul-2010 12:13". Below the table, it indicates "1 result" and "20 per page". The footer contains the copyright notice "Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved." and the version number "Version 3.0.5.0".

Computer Name	Domain	WorkGroup	IP	Computer Location	Last Time Online	Actions
MacBook Pro		WORKGROUP	192.168.0.74		17-Jul-2010 12:13	







The administrator has the possibility of either exporting the log for a computer as an Excel document or simply view it in the Logs Report module. Both reports will contain all activities performed by the computer in question.



7.8. User History

This module displays a list of all client users that were once connected to the system.

The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, the title "Endpoint Protector 2009 Reporting and Administration Tool", a language dropdown set to "English", a search bar, and a "Welcome Super Administrator | Logout" link. The left sidebar contains a menu with categories: Dashboard, Management, Rights, Settings, Offline Temporary Password, and Reports and Analysis. Under "Reports and Analysis", the "User History" option is selected and highlighted. The main content area displays the "Users History" module. It features a "Filter" section with a dropdown arrow, followed by a "Results" table. The table has columns for "User Name", "First Name", "Last Name", "Phone", "E-mail", and "Actions". It lists three users: "noUser", "autorunUser", and "raul". Each user entry has corresponding first and last names and a set of action icons. Below the table, it indicates "3 results" and "20 per page". The footer contains the copyright notice "Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved." and the version number "Version 3.0.5.0".

User Name	First Name	Last Name	Phone	E-mail	Actions
noUser	No user	No User			 
autorunUser	AutoRun User	AutoRun User			 
raul	raul	raul			 

Just like in the Computer History module, the administrator has the possibility of either exporting the log for a computer as an Excel document or simply view it in the Logs Report module.

7.9. Device History

Same as the previous two modules, this module generates a list of all devices that were connected to the system. This report can be generated for each device.

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis (with sub-links: File Shadowing, Online Computers, Online Users, Connected Devices, Computer History, User History, Device History, System Alerts), System Parameters, System Configuration, and Support. The main content area is titled 'Devices History' and features a 'Filter' section and a 'Results' table. The table lists one device: a USB Storage Device named 'USB2.0 FlashDisk' owned by 'raul', described as 'USB2.0 FlashDisk / Kingmax', with VID 1687, PID 6211, and Serial Number 777090211FFFFFF000000... It shows a last connection on 17-Jul-2010 at 11:34. The bottom of the interface includes the copyright notice 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and the version 'Version 3.0.5.0'.

Device Type	Device Name (identification)	Owner	Description	TD	VID	PID	Serial Number	Last Connection	Actions
USB Storage Device	USB2.0 FlashDisk	raul	USB2.0 FlashDisk / Kingmax		1687	6211	777090211FFFFFF000000...	17-Jul-2010 11:34	[Icons]

1 result [20 per page]

If viewed as such, the Excel report will, again, offer the complete information regarding the device: VID, PID, Serial Number, where it was used, what action did it suffer, who changed the rights for it, etc.

7.10. 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.

Statistics

Search Criteria

Report:

Please Select

Period:

Please Select

On:

Please Select

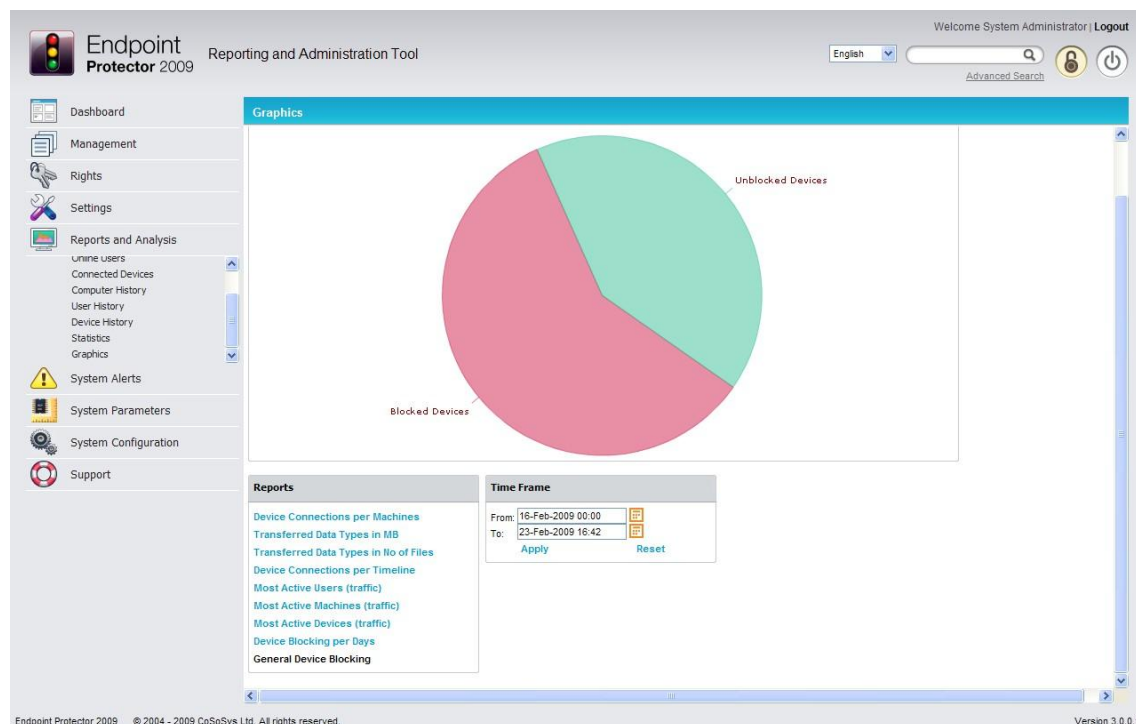
Apply filter

Results

no results

7.11. Graphics

Endpoint Protector let's you visualize the traffic in your environment making audit trails easier and more efficient.



The Graphical Reports offered by Endpoint Protector includes:

- Device blocking per Days
- General Device Blocking
- Device connections per Computer
- Device connections per Timeline
- Most active Computers (PCs)
- Most active Users
- Most active Devices
- Number of Device Connections
- Transferred data in MB
- Transferred data by extensions

The Graphics module of Endpoint Protector can be accessed from the "Reports & Analysis" module, by clicking the "Graphics" tab.

Selecting the timeline for the graphs is done by selecting the "From" and "To" date of the desired date range. After selecting the date range click the "Change" button to update the graph.

Besides the categorized view of data traffic, Endpoint Protector can also generate a Top 10, 20 and 30 for the category you are currently viewing.



8. System Alerts

Endpoint Protector allows you to set notifications (Alerts) for Devices, Computers, Groups and Users making monitoring them easier. An Alert will trigger an e-mail that will be sent to the selected administrator(s) that are intended to receive the alerts. You can set up alerts in the System Alerts-> Define System Alerts module in Endpoint Protector.

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, title, and user information. The left sidebar contains a menu with options like Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, and Support. The main content area is titled 'List of Alerts' and shows a table with one alert entry. The table has columns for Client, Computer, Group, Device Type, Device, Event, and Actions. The entry shows 'Any' for Client, 'MacBook Pro' for Computer, 'Any' for Group, 'Any' for Device Type, 'Any' for Device, and 'Connected' for Event. The Actions column contains icons for a checkmark and a cross. Below the table, there is a 'Create' button. The footer contains copyright information and the version number.

Endpoint Protector 2009 Reporting and Administration Tool

Welcome Super Administrator | Logout

English

Advanced Search

Dashboard

Management

Rights

Settings

Offline Temporary Password

Reports and Analysis

System Alerts

Define System Alerts

Alerts History



System Parameters

System Configuration

Support

List of Alerts

Results

Client	Computer	Group	Device Type	Device	Event	Actions
Any	MacBook Pro	Any	Any	Any	Connected	 

1 result [20 per page]

Create

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.

Version 3.0.5.0

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

Welcome Super Administrator | Logout

English [Search]

Endpoint Protector 2009 Reporting and Administration Tool

Default System Settings

Storage Folders

Log Directory: c:\TempEPP
Shadow Directory: c:\TempEPP

Endpoint Protector Rights Functionality

☐ Use computer rights
☐ Use user rights
☒ Use both
Priority: ☐ User rights ☒ Computer rights

E-mail Server Settings

Hostname: smtp.lund1.com
Username: test
Password: ****
Send test e-mail to my account: ☐

Main Administrator Contact Details

Phone: 049-766221
E-mail: test@cososys.com

***Note:** This contact information is referring to Offline Temporary Password only! For Alerts, you must setup the e-mail address from System Administrators > Edit info.

Save

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

You can also verify if your settings are correct by checking the box next to “Send test e-mail to my account”.

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

Welcome Super Administrator | Logout

English [Search]

Endpoint Protector 2009 Reporting and Administration Tool

List of Administrators

Filter

Results

User Name	Created at	Last Login	Actions
root	17 July 2010 11:30	17-Jul-2010 11:48	[Edit] [Delete] [Add]
Restricted			[Edit] [Delete] [Add]

2 results [20 per page]

Create

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

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



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

The screenshot shows the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Import, Active Directory Sync, Active Directory Deployment, System Administrator, System Policies, System Settings, and Support. The main content area is titled "Administrator User" and contains two sections: "Details" and "Interface".

Details

Username:	root
First Name:	Super
Last Name:	Administrator
E-mail:	administrator@cososys.com
E-mail Alert:	<input checked="" type="checkbox"/>
Phone:	049-544322

Interface

Language:	English
-----------	---------

At the bottom of the form are two buttons: "Save" and "Back".

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

Now you are set up to receive e-mail alerts.

Go back to "Define System Alerts" and click "Create" to start creating the first alert.



Create Alert

Alert fields	
Group:	All Groups ▾
Client:	Any ▾
Computer:	MacBook Pro ▾
Device type:	Any ▾
Device:	USB2.0 FlashDisk ▾
Event:	Connected ▾

Alert administrators	
Administrators:	<input checked="" type="checkbox"/> Super Administrator (root)

☒ Save
 ☒ Save Add

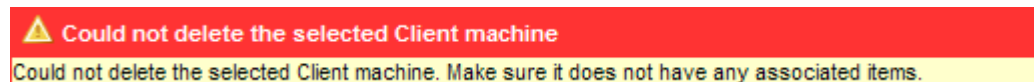
Then select the Group, Client, Computer, Device type or Device, - depending if you mean a single device or all devices of a certain type-, and the event that will trigger the notification.

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

Example: if you want to be notified when a certain device is connected to a certain computer you must set up an alert choosing the specific device and computer that you wish to be notified of and selecting the "Connected" event from the events list.

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

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



9. System Parameters

This module of Endpoint Protector is designed for super administrators. The advanced settings available here determine the functionality of the entire system.

Note!

Many of these parameters should be untouched and left as they are by installation default. Introducing wrong values can limit the functionality and performance of the entire system.

9.1. Device Types

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

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the logo, the title 'Endpoint Protector 2009 Reporting and Administration Tool', a language dropdown set to 'English', and a search bar. A sidebar on the left contains icons and links for Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, Device Types (highlighted), Rights, Events, File Types, System Licenses, System Security, System Configuration, and Support.

The main content area is titled 'List of Device Types' and displays a table of results. The table has two columns: 'Name' and 'Description'. It lists 22 device types, including Unknown Device, USB Storage Device, Digital Camera, SmartPhone (USB Sync), SmartPhone (Windows CE), SmartPhone (Symbian), Internal Card Reader, PCMCIA Device, FireWire Bus, ZIP Drive, Internal CD or DVD RW, Internal Floppy Drive, Card Reader Device (MTD), Card Reader Device (SCSI), Windows Portable Device, Mobile Phones (Sony Ericsson, etc.), Local Printers, Bluetooth, WiFi, and BlackBerry. Each device type is paired with a brief description.

At the bottom of the table, it indicates '22 results' and '20 per page'. Navigation buttons for the table are visible at the bottom right of the results area.

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

9.2. Rights

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

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. The top navigation bar includes the product logo, the title 'Reporting and Administration Tool', a language dropdown set to 'English', and a search bar with a 'Q' icon and a link to 'Advanced Search'. The left sidebar contains a menu with icons and labels for: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, Device Types, Rights, Events, File Types, System Licenses, System Security, System Configuration, and Support. The main content area is titled 'List of Possible Rights' and features a table with two columns: 'Name' and 'Description'. The table lists eight rights, including 'Deny Access', 'Allow Access', 'Read Only Access', and various 'Allow Access if TD Level' entries. At the bottom of the table, it indicates '8 results' and a pagination control set to '20 per page'. The footer of the interface shows the copyright notice 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and the version number 'Version 3.0.5.0'.

Name	Description
Deny Access	Deny Access
Allow Access	Allow Access
Read Only Access	Read Only Access
Allow Access if TD Level 1	Allow Access if device is Trusted Device...
Allow Access if TD Level 2	Allow Access if device is Trusted Device...
Allow Access if TD Level 3	Allow Access if device is Trusted Device...
Allow Access if TD Level 4	Allow Access if device is Trusted Device...
Block if wired network is present	Block Wireless network device is wired n...

8 results [20 per page]

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

9.3. Events

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

The screenshot displays the 'List of Events' window in the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Management, Rights, Settings, and Reports and Analysis. The main area shows a table of events with columns for Event Name, Description, Logging, Quick Logging, and Actions. The table lists various system events such as 'Connected', 'Disconnected', 'Enabled', 'Disabled', 'File Read', 'File Write', 'File Read-Write', 'File Rename', 'File Delete', 'Device TD', 'Device not TD', 'Delete', 'Enable Read-Only', 'Enable if TD Level 1', 'Enable if TD Level 2', 'Enable if TD Level 3', 'Enable if TD Level 4', 'AD Import', 'AD Synchronization', and 'Blocked'. Each event has a corresponding description and status indicators for logging and quick logging. The bottom of the table shows '22 results' and a 'per page' dropdown set to '20'.

Event Name	Description	Logging	Quick Logging	Actions
Connected	Device was connected to computer	✓	✓	✗
Disconnected	Device was disconnected from computer	✓	✓	✗
Enabled	Device was enabled by Administrator	✓	✓	✗
Disabled	Device is disabled by default or by Admin...	✓	✓	✗
File Read	File was read from device	✓	✓	✗
File Write	File was written to device	✓	✓	✗
File Read-Write	File read and write from and to device	✓	✓	✗
File Rename	File from device was renamed	✓	✓	✗
File Delete	File was deleted from device	✓	✓	✗
Device TD	Device is a TrustedDevice	✓		✗
Device not TD	Device is not a TrustedDevice	✓		✗
Delete	An item was deleted	✓	✓	✗
Enable Read-Only	Device Read-Only modus was enabled	✓	✓	✗
Enable if TD Level 1	Device was enabled if it is a Level 1 Tr...	✓	✓	✗
Enable if TD Level 2	Device was enabled if it is a Level 2 Tr...	✓	✓	✗
Enable if TD Level 3	Device was enabled if it is a Level 3 T...	✓	✓	✗
Enable if TD Level 4	Device was enabled if it is a Level 4 T...	✓	✓	✗
AD Import	AD Import	✓	✓	✗
AD Synchronization	AD Synchronization	✓	✓	✗
Blocked	Blocked on the client side	✓	✓	✗

22 results [20 per page]

Note!

Changing this list without CoSoSys' acknowledgement can limit system functionality and performance; however, such customizations/implementations can be performed by request by one of our specialists as part of our Professional Services offered to customers.

9.4. File Types

This list contains common file type extensions and a description for each of them making them easier to recognize when creating audits.

The screenshot displays the 'List of File Types' section within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, Device Types, Rights, Events, File Types (selected), System Licenses, System Security, System Configuration, and Support. The main content area shows a table of file types with columns for Extension, Mime Type, Description, and Actions. The table lists 17 common file types, each with a corresponding extension, mime type, and description. The Actions column contains icons for adding, deleting, and editing each entry. At the bottom of the table, it indicates '127 results' and '20 per page'. A 'Create' button is located below the table.

Extension	Mime Type	Description	Actions
.doc		Microsoft Word Document	
.log		Log File	
.msg		Mail Message	
.rtf		Rich Text Format	
.txt		Text File	
.wpd		WordPerfect Document	
.wps		Microsoft Works Word Processor Document	
.123		Lotus 1-2-3 Spreadsheet	
.3dm		Rhino 3D Model	
.3dmf		QuickDraw 3D Metafile	
.3gp		3GPP Multimedia File	
.8bi		Photoshop Plug-in	
.aac		Advanced Audio Coding File	
.ai		Adobe Illustrator File	
.aif		Audio Interchange File Format	
.app		Mac OS X Application	
.asf		Advanced Systems Format File	
.asp		Active Server Page	
.asx		Microsoft ASF Redirector File	
.avi		Audio Video Interleave File	

127 results [20 per page] 1 2 3 4 5

Create

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

9.5. System Licenses

In this module the administrator can import Endpoint Protector Client licenses. These licenses are in the form of an Excel file which contains special formatting.

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains navigation links: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters (Device Types, Rights, Events, File Types, System Licenses, System Security), System Configuration, and Support. The main content area is titled 'List of Computers with Licenses' and shows the following summary:

- Total number of licenses: 1
 - PC licenses: 0
 - MAC licenses: 0
- Number of valid unassigned licenses: 0
 - PC licenses: 0
 - MAC licenses: 0

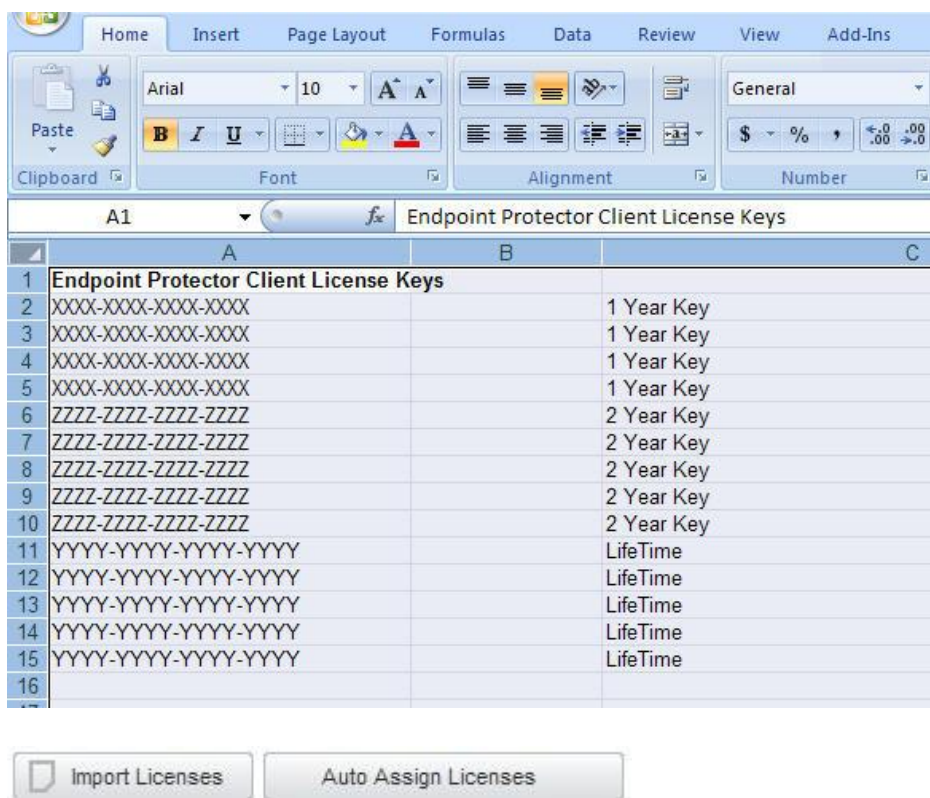
Below the summary is a table with the following data:

License Validity	Name	IP	Workgroup	Domain	Last Seen	Serial	Validity	Actions
	MacBook Pro	192.168.0.74	WORKGROUP		17 July 2010 12:18	TRIA-LCOD-E000-0001	Valid for 30 days.	

At the bottom of the table, it indicates '1 result' and '20 per page'. Below the table is an 'Import Licenses' button. The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

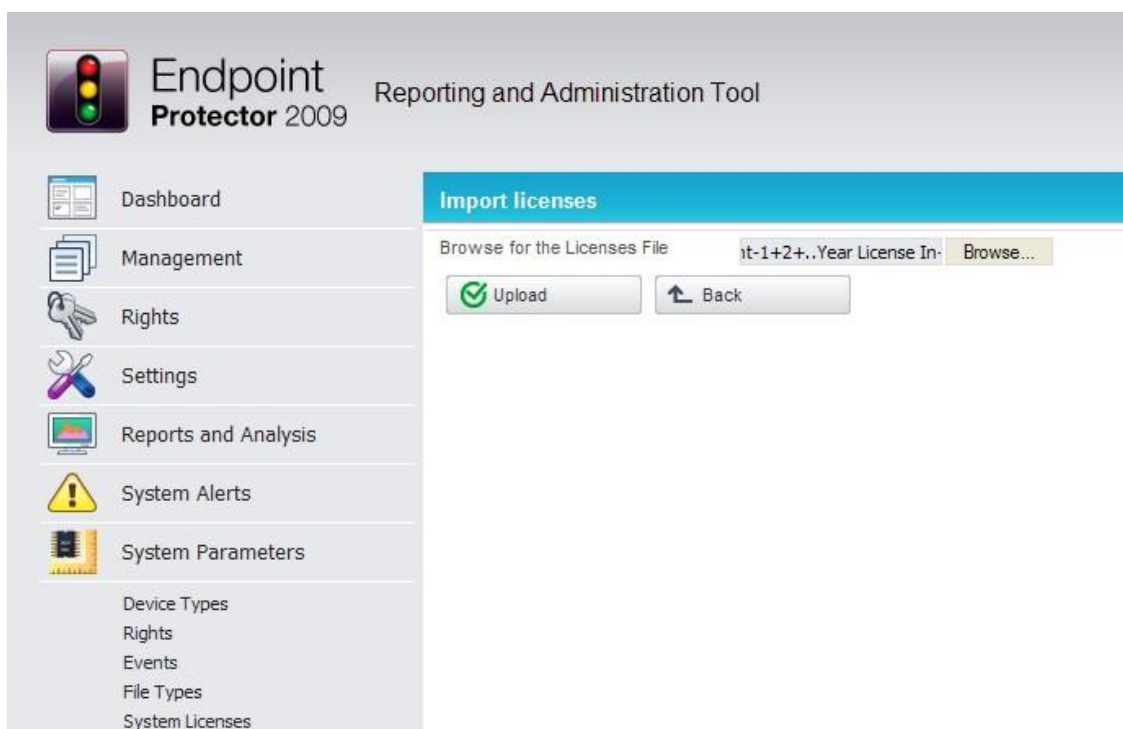
Attention!

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.



9.5.1. Import Licenses

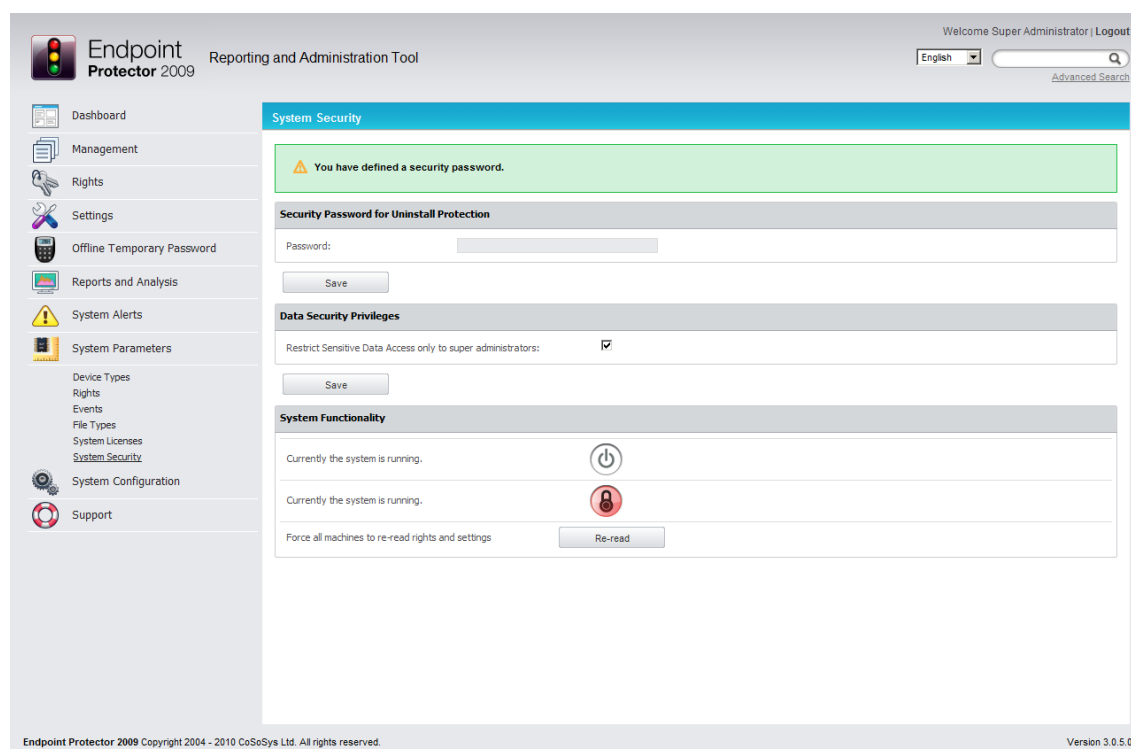
This gives you the possibility to browse for an Excel file that contains licenses. After you have selected the file, click Upload.



9.6. System Security / Client Uninstall Protection

The Client Uninstall Protection feature protects the Endpoint Protector Client from being uninstalled by using a password-based mechanism. The Administrator of the system defines this password from within the Reporting and Administration Tool of Endpoint Protector 2009. When somebody tries to uninstall the Endpoint Protector Client, they will be prompted for the password. If they do not know the password, the Client removal cannot continue.

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



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

The “**Re-read**” command will force all computers to re-read rights instantly. This is useful in case you modified the global system settings and computers need a longer time to get their rights from the Server.

You can also access the "System Lockdown" and "ON/OFF" buttons from this module as well as the "Re-read" command.



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

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

10. System Configuration

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

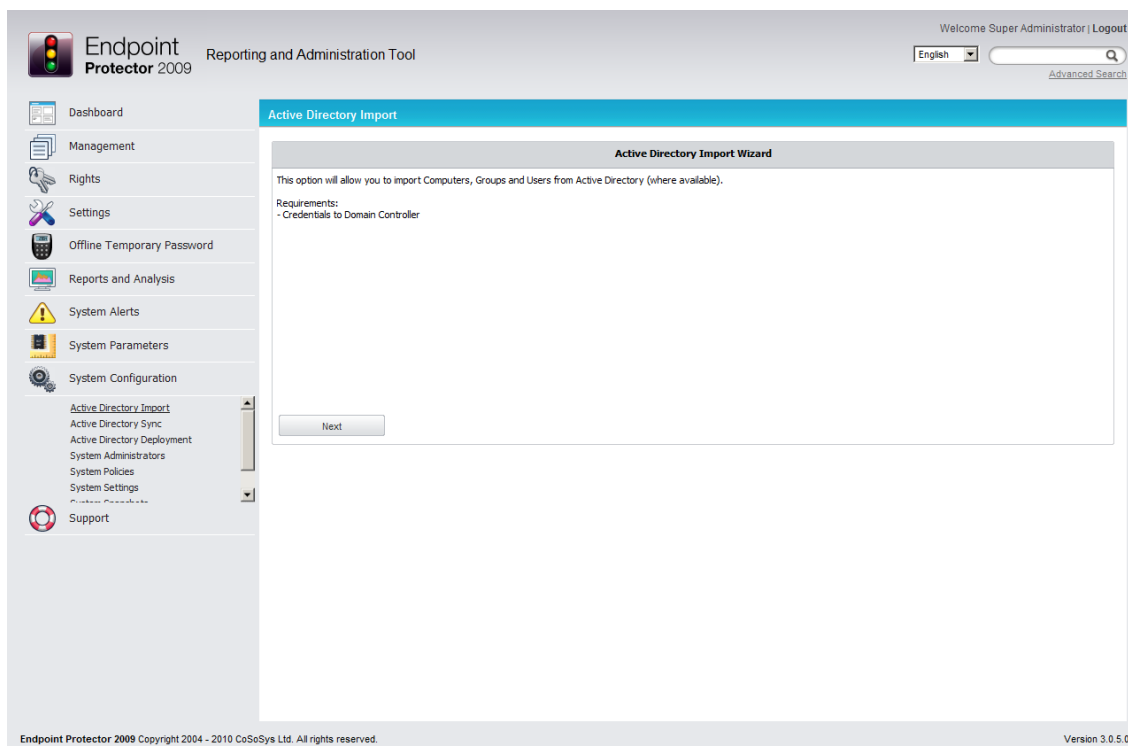
10.1. Active Directory Functionalities

Attention!

The previous versions of the AD Plug In (ADPlugIn.msi) can interfere with the new functionality of Active Directory on Endpoint Protector Server version 3.0.3.1 or higher. Please make sure you uninstall this add-on in case of an update of the server to this version.

10.1.1. Active Directory Import

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



If you have the requirements, simply click “Next”.

Endpoint Protector 2009 Reporting and Administration Tool

Welcome Super Administrator | Logout

English

Advanced Search

Active Directory Import

Active Directory Import. Step 1: Define Connection

Domain Controller Server Name:	192.168.0.193	Example: w2003server
Domain:	ad-cososys.com	Example: example.cososys.com
User:	Administrator@ad-cososys.com	Example: admin@example.cososys.com
Password:	*****	

Back Next Test Connection

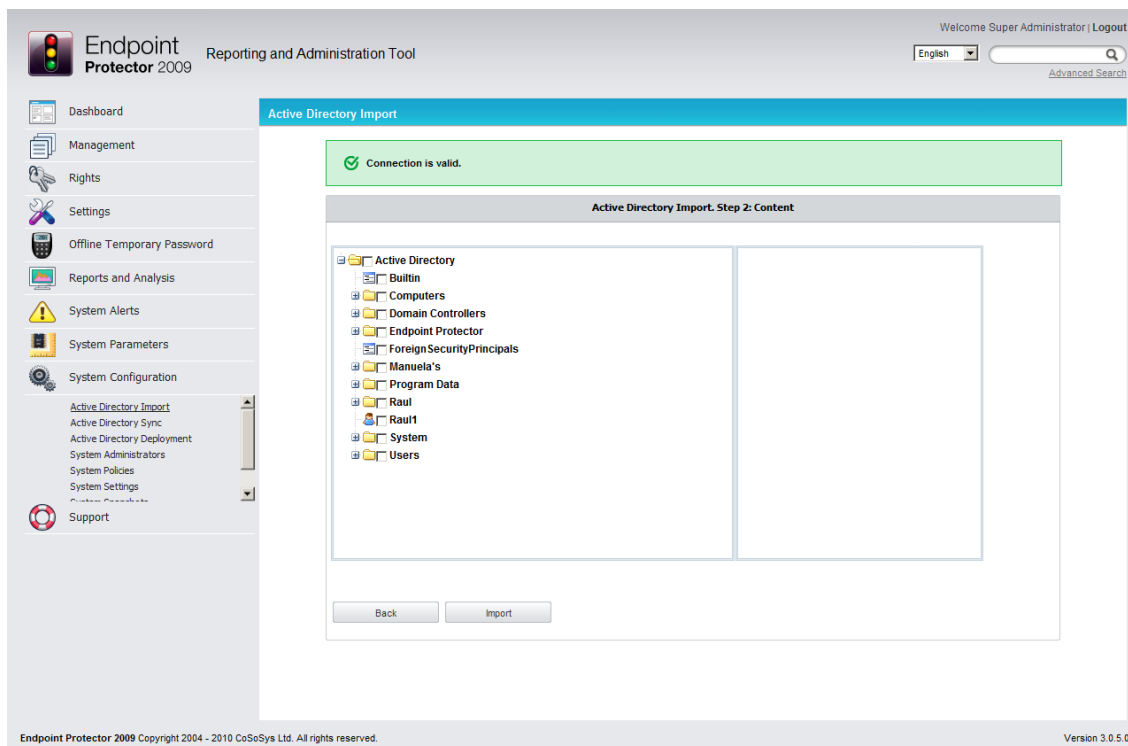
Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

Enter the Active Directory domain controller server name, the domain name and a username and password in the format as in the examples presented in the form. First, you can push the “Test Connection” button to test if the connection is established successfully. If the connection is valid, push the “Next” button.

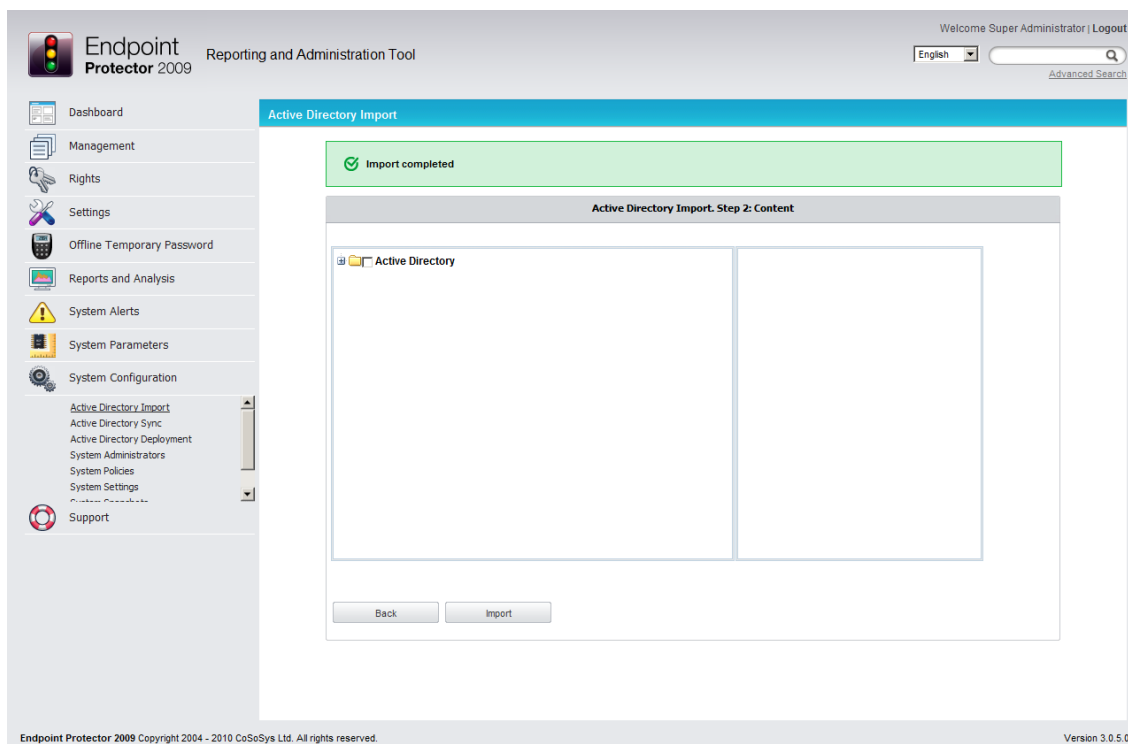
Note!

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

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



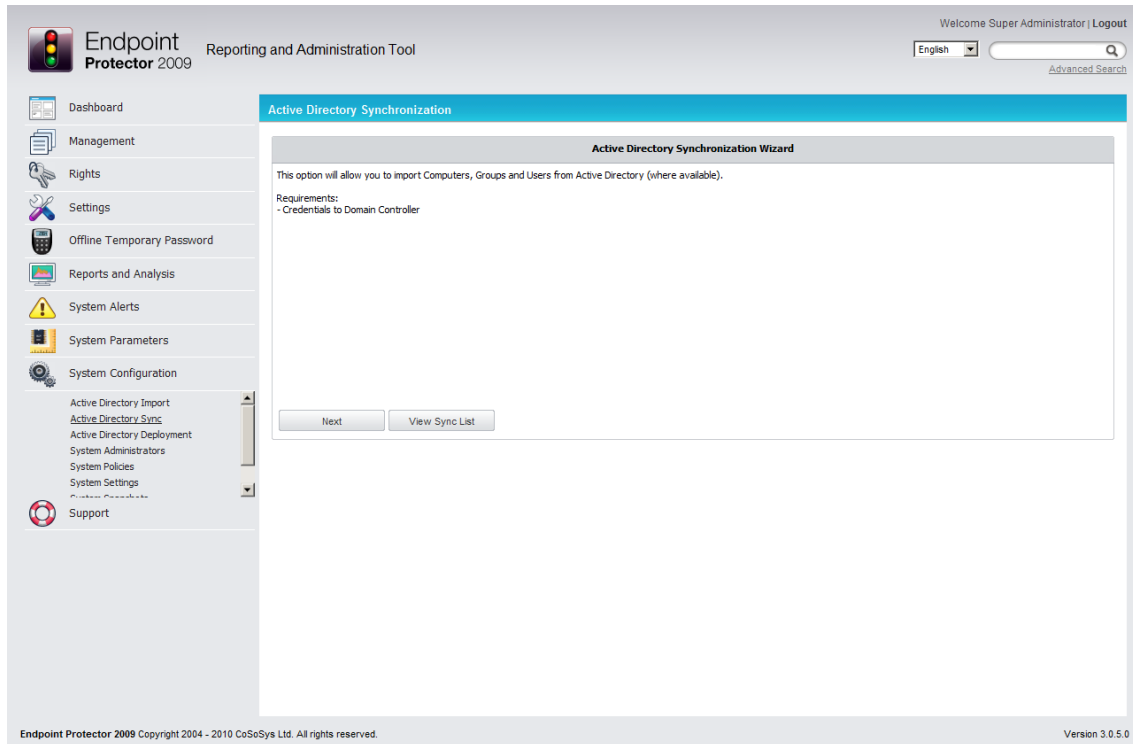
If the import procedure was successful, you will see the message “Import completed”.



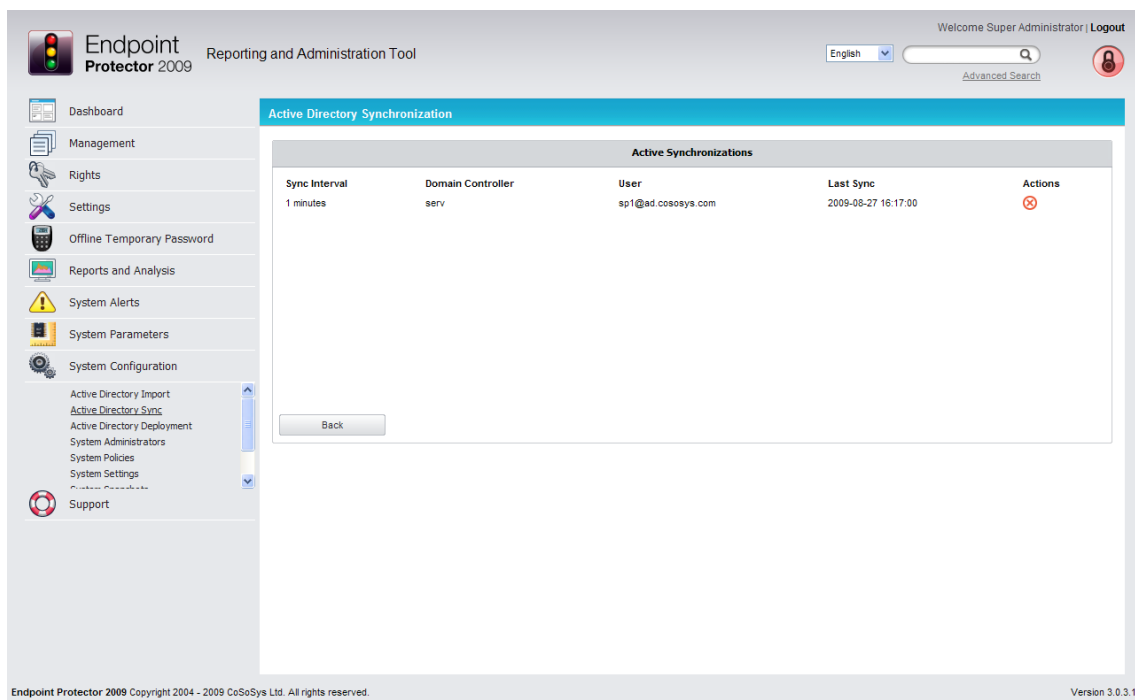
10.1.2. Active Directory Sync

Special requirements: Endpoint Protector Timer, or the Windows Scheduler setup to call the synchronization PHP script.

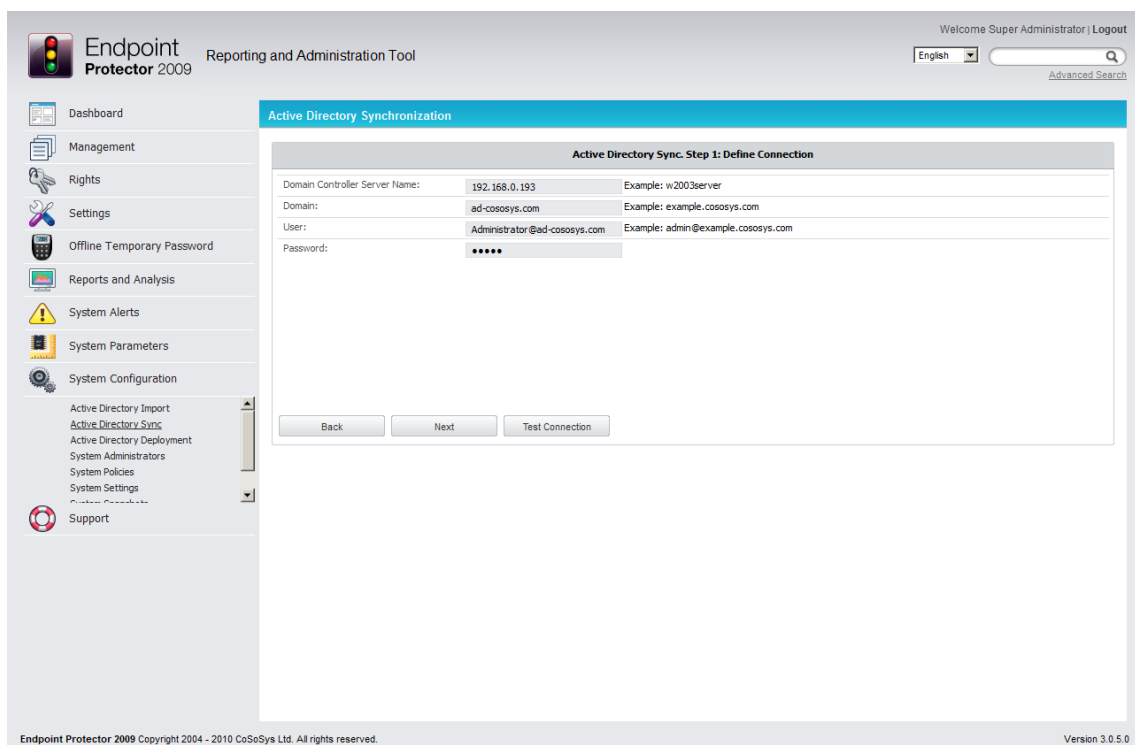
This module allows you to synchronize the entities in Endpoint Protector with the entities in Active Directory (Computers, Users, and Groups).



You can either examine existing synchronizations by clicking the “View Sync List” button,

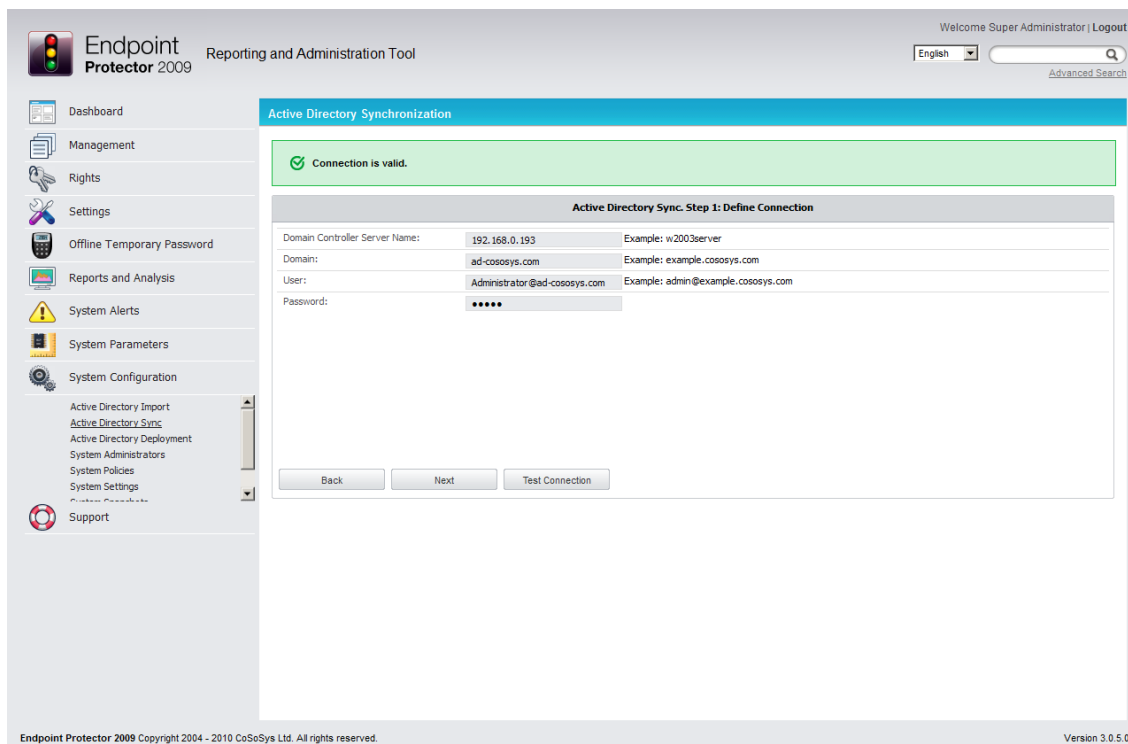


or, if you have the requirements, simply click “Next” to set up your synchronization settings.



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

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



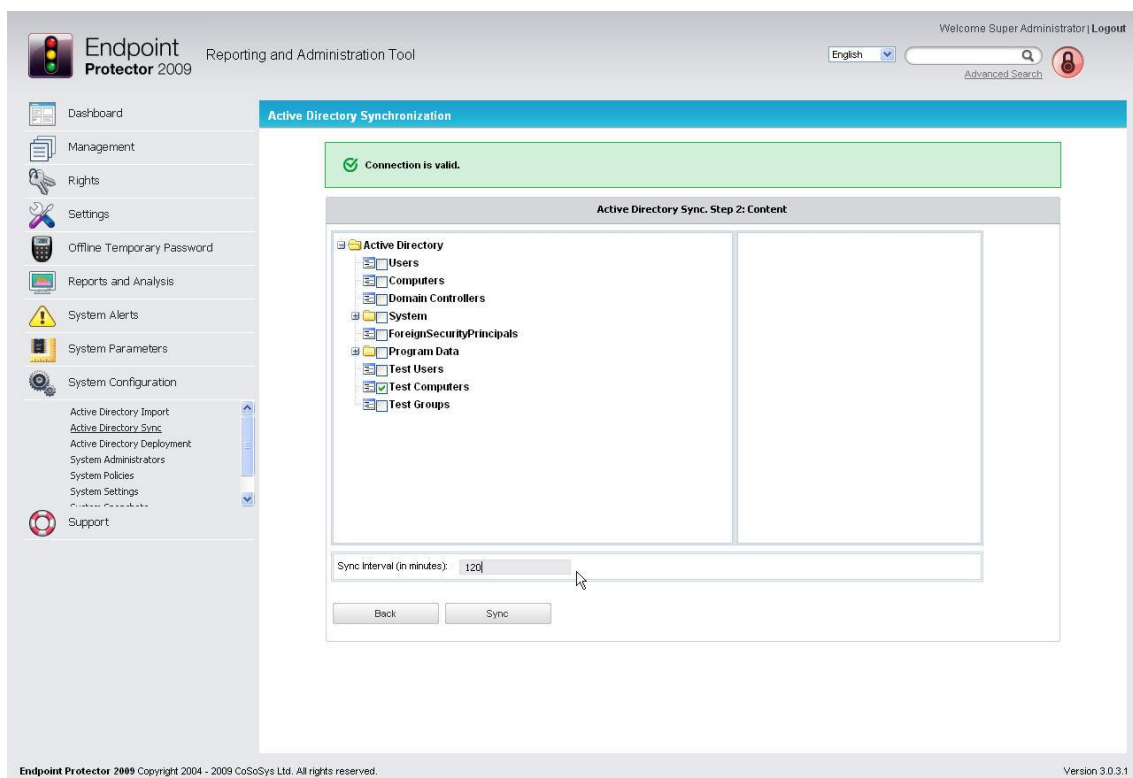
You should see a message “Connection is valid” on the top of the page.

Click “Next” to continue.

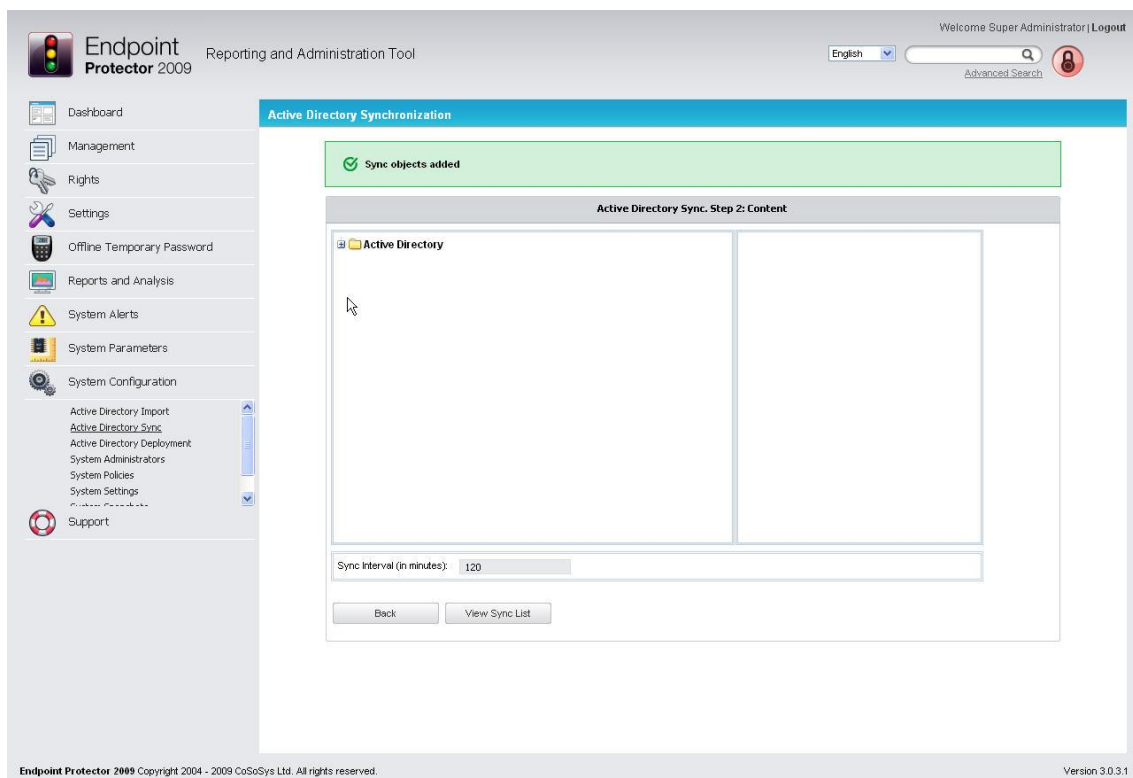
Note!

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

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



You will see the message "Sync object added".



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

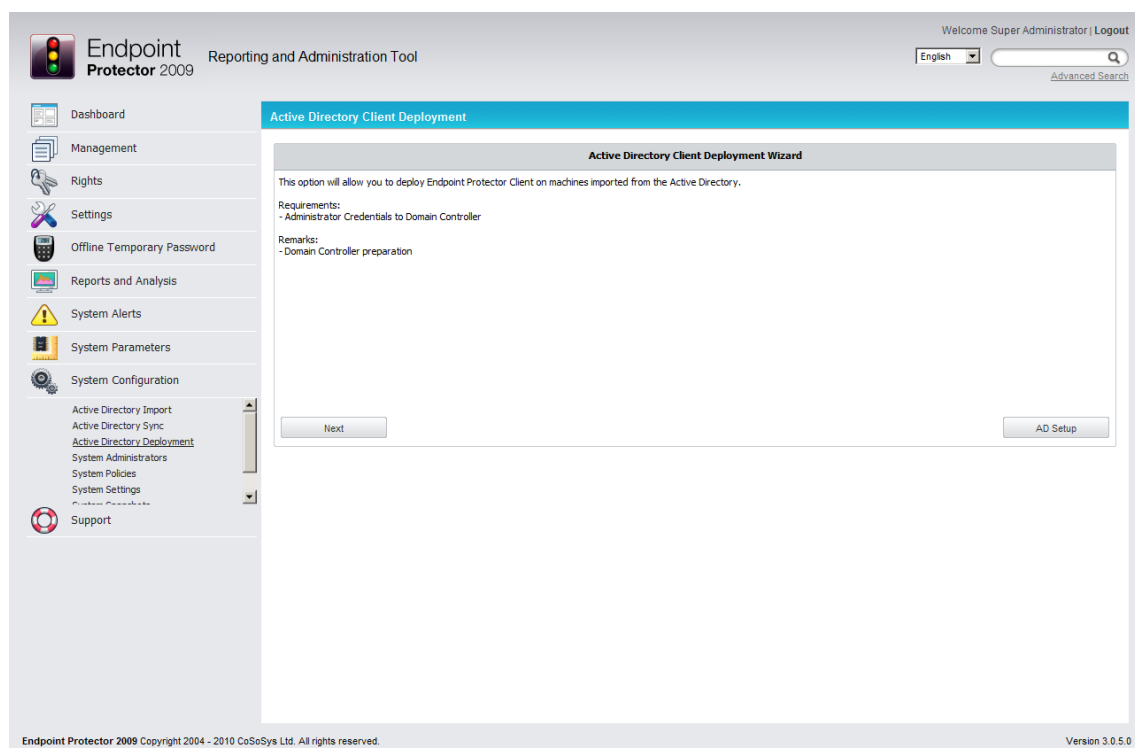
The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Import, Active Directory Sync, Active Directory Deployment, System Administrators, System Policies, System Settings, and Support. The main content area is titled "Active Directory Synchronization" and features a table of "Active Synchronizations".

Sync Interval	Domain Controller	User	Last Sync	Actions
1 minutes	serv	sp1@ad.cososys.com	2009-08-28 09:17:00	
23 minutes	w2003se-loan	administrator@loan-ad.cososys.com	2009-08-28 09:17:00	
120 minutes	newDC	administrator@new-ad.cososys.com	-	

Below the table is a "Back" button. The footer of the interface shows "Endpoint Protector 2009 Copyright 2004 - 2009 CoSoSys Ltd. All rights reserved." and "Version 3.0.3.1".

10.1.3. Active Directory Client Deployment

With the new “Active Directory Deployment” feature of Endpoint Protector you have the possibility to deploy Endpoint Protector Clients on computers imported from Active Directory. This implies that you first have to import the computers you wish to install Endpoint Protector Client on, from Active Directory to the Endpoint Protector Server using the Active Directory Import Wizard.



Requirements for this feature:

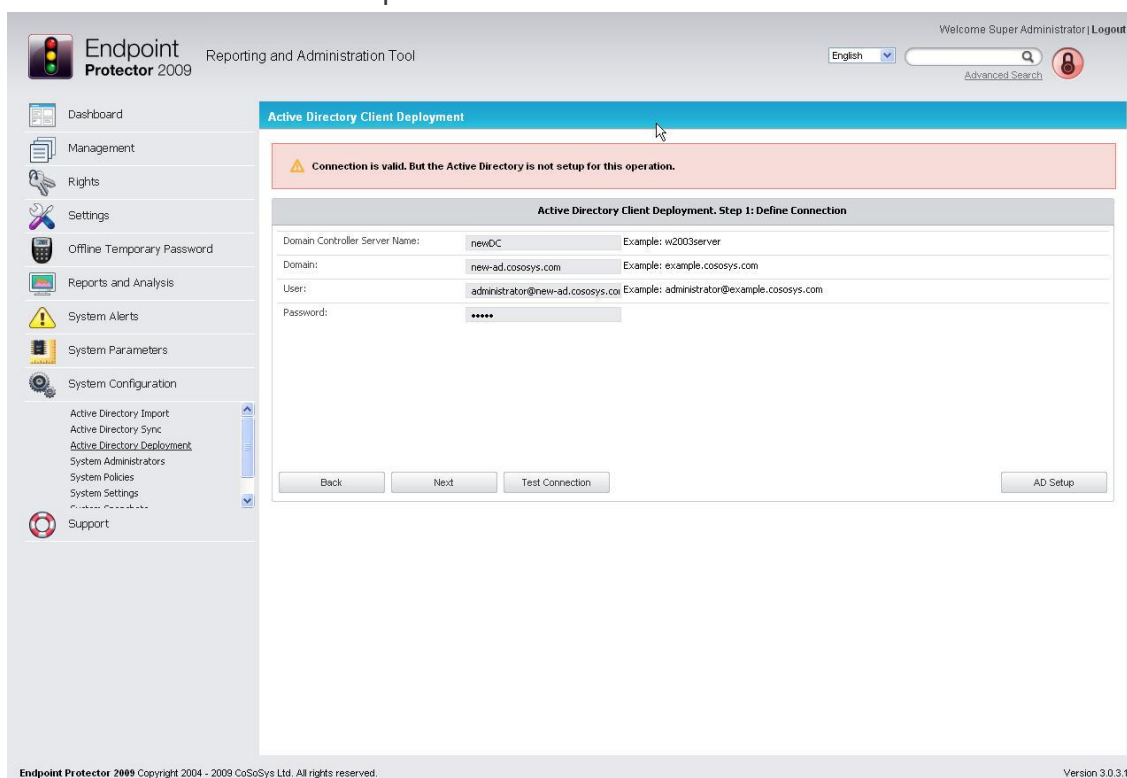
- Administrator credentials to the Active Directory Domain Controller
- Active Directory Domain Controller Microsoft Group Policy Management Console (GPMC). You can download it from the Microsoft's website:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=0A6D4C24-8CBD-4B35-9272-DD3CBFC81887&displaylang=en>

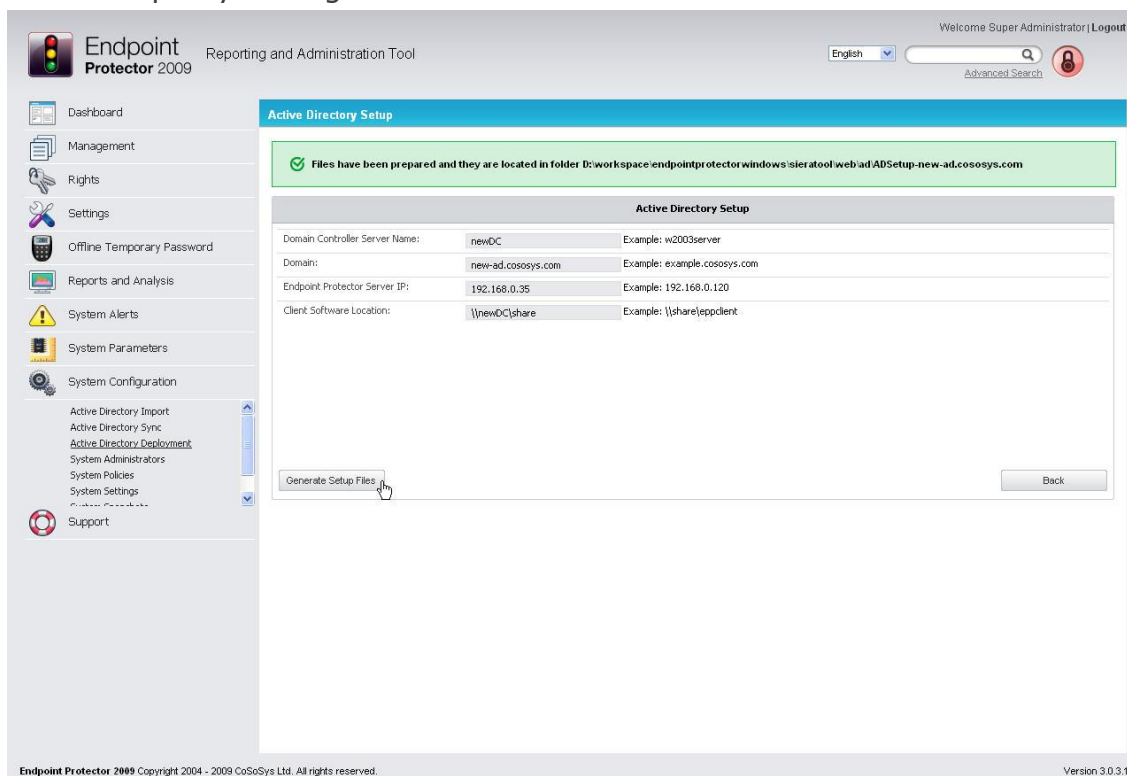
Preparations:

1. Create a shared network folder and be sure to set the sharing and security permissions for the folder to "Everyone" – Read Only. Copy to this location the files 'EPPClientSetup_x86_32.msi' and 'EPPClientSetup_x86_64.msi'.

- From the Endpoint Protector web interface, after selecting “Next”, enter the required information in the correct format and push the “Test Connection” button. Before continuing with the deployment process you will need to run “AD Setup”.

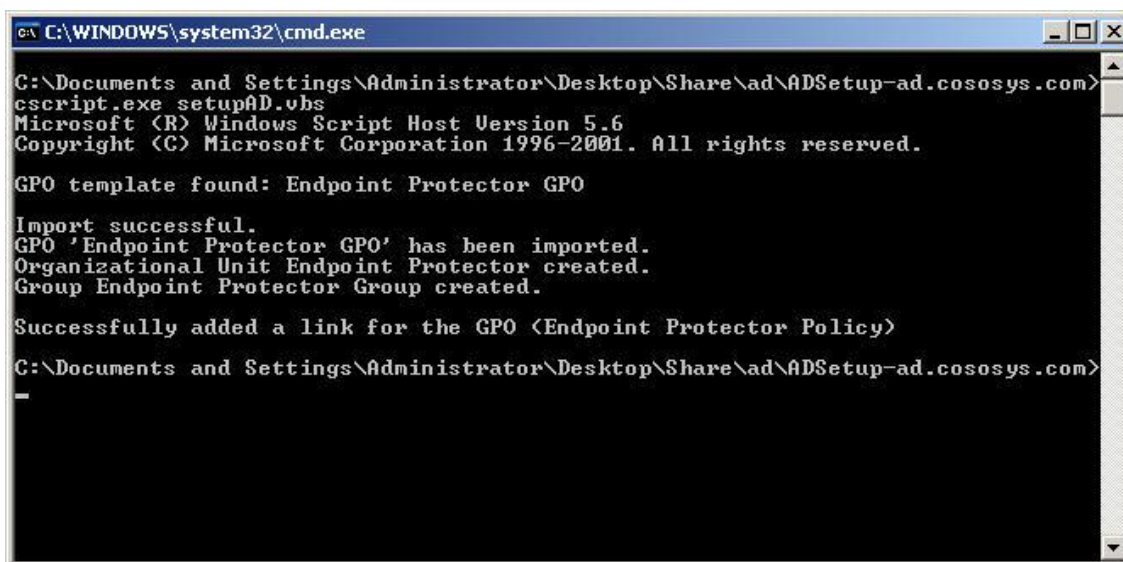


- Run AD Setup from Endpoint Protector Web interface for each domain you have setup in your organization.



As a result of this step you will get a new folder located on the Endpoint Protector Server, under: InstallPath\endpointprotector\sieratool\web\ad\ with the following name: ADSetup-"DOMAINNAME"

1. Copy the file 'Install_EPP_Client.vbs' located in above directory to the shared network folder created at Step 1
2. Copy the rest of the files and folders to a new created folder located on the Domain Controller
3. On the Domain Controller computer run the command:
cscript.exe setupAD.vbs
within Command Prompt



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator\Desktop\Share\ad\ADSetup-ad.cososys.com>
cscript.exe setupAD.vbs
Microsoft (R) Windows Script Host Version 5.6
Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.

GPO template found: Endpoint Protector GPO

Import successful.
GPO 'Endpoint Protector GPO' has been imported.
Organizational Unit Endpoint Protector created.
Group Endpoint Protector Group created.

Successfully added a link for the GPO (Endpoint Protector Policy)
C:\Documents and Settings\Administrator\Desktop\Share\ad\ADSetup-ad.cososys.com>
```

The mechanism of deployment is the following:

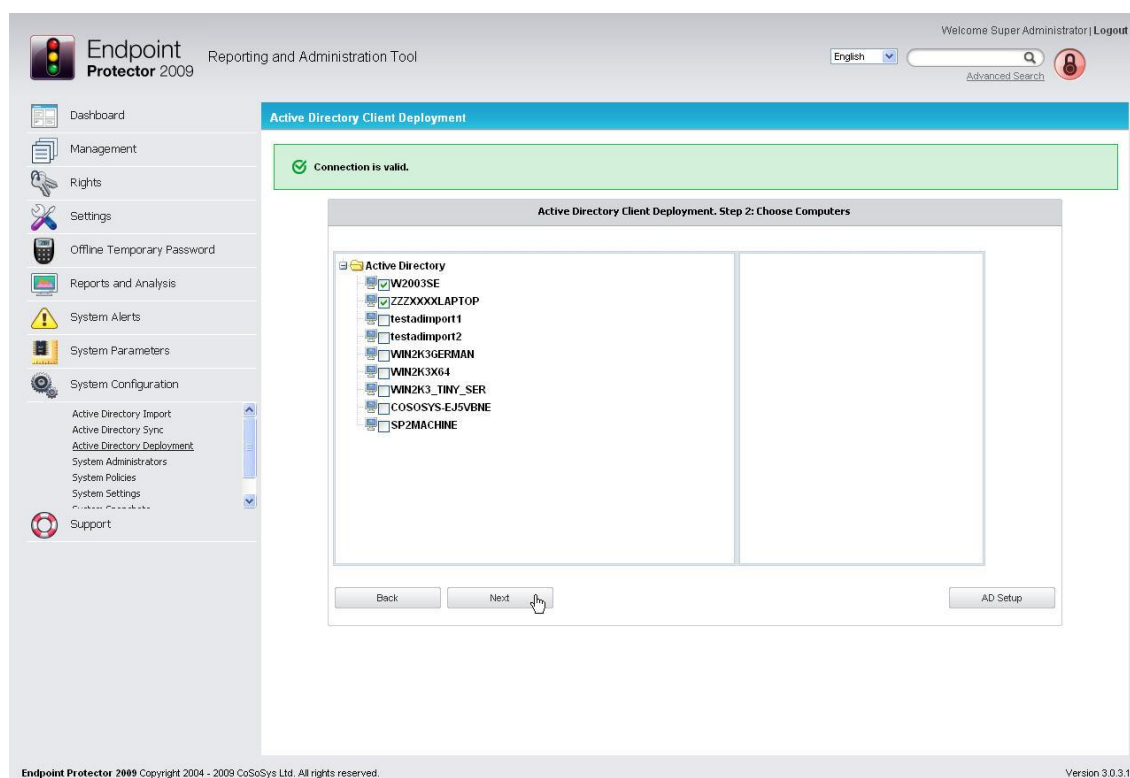
1. Through the Endpoint Protector interface you have to provide the information regarding the Active Directory: domain controller server name, the domain name and a username and password in the format as in the examples presented in the form

The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Import, Active Directory Sync, Active Directory Deployment (highlighted), System Administrators, System Policies, System Settings, and Support. The main content area is titled 'Active Directory Client Deployment' and shows 'Step 1: Define Connection'. The form includes the following fields and examples:

Field	Value	Example
Domain Controller Server Name:	serv	w2003server
Domain:	ad.cososys.com	example.cososys.com
User:	sp1	administrator@example.cososys.com
Password:	***	

At the bottom of the form are buttons for 'Back', 'Next', 'Test Connection', and 'AD Setup'. The footer of the interface shows 'Endpoint Protector 2009 Copyright 2004 - 2009 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.3.1'.

2. In the next step a tree is being built with the computers that exist in the Endpoint Protector's database and were imported from Active Directory. Here you have to select the computers to which you want to deploy the Endpoint Protector Client.



Next time the computers from the Endpoint Protector Group reboot, the Startup script will run and it will install Endpoint Protector Client on each of them.

Technical information regarding the setupAd.vbs script

This script has to be run on all Active Directory on which you want to deploy Endpoint Protector Client.

What it does:

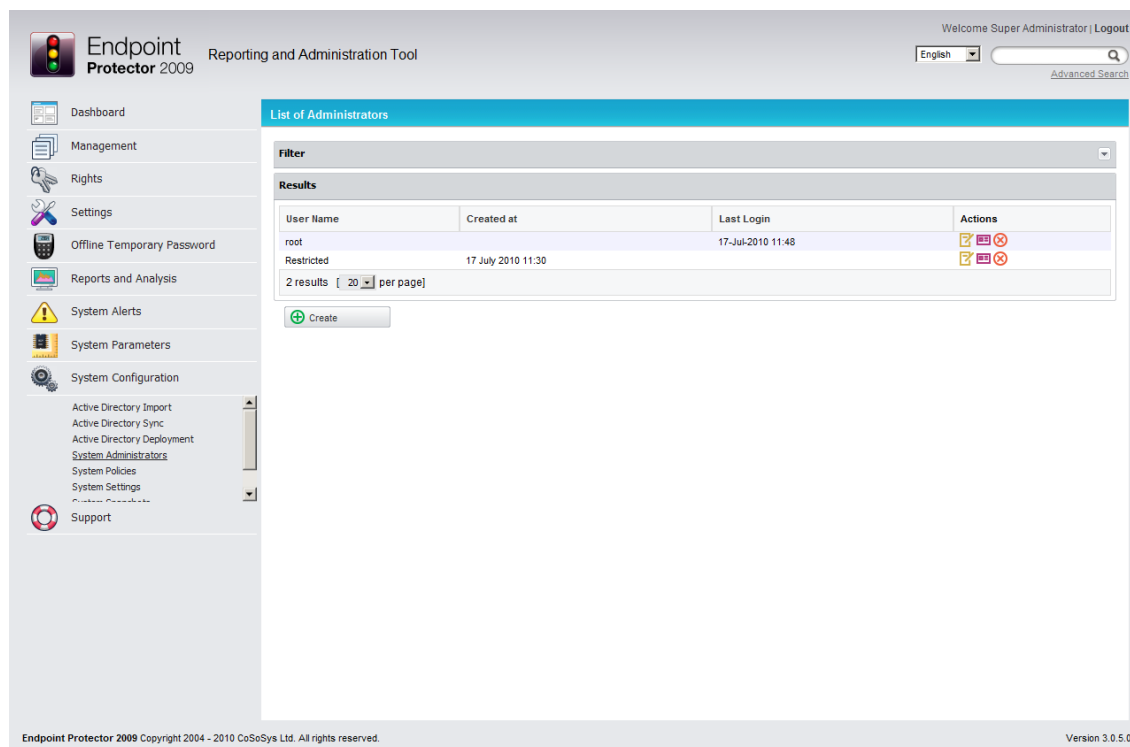
1. It creates a new GPO called Endpoint Protector Policy
Import into the GPO above the settings for installing Endpoint Protector Client, generated from web interface
2. Create an Organization unit called Endpoint Protector
Create a new Group Endpoint Protector Group
3. Link Endpoint Protector Policy to domain
Restrict the applying of this GPO to Endpoint Protector Group only

Technical information regarding the web deployment interface

Each computer you select for deployment will be added as a member of the group Endpoint Protector Group, and so applying the policies/settings defined in this GPO.

10.2. System Administrators

This list contains all the administrators who have access to the Administration and Reporting Tool. As described earlier in this document the administrators can be of two types: regular administrators, which have some limitations and super administrators which have full access to the system, including advanced features.



The screenshot displays the 'List of Administrators' page within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Import, Active Directory Sync, Active Directory Deployment, System Administrators (highlighted), System Policies, System Settings, and Support. The main content area shows a table of administrators with columns for User Name, Created at, Last Login, and Actions. Two administrators are listed: 'root' and 'Restricted'. The 'root' user was created on 17 July 2010 at 11:30 and last logged in on 17-Jul-2010 at 11:48. The 'Restricted' user was created on 17 July 2010 at 11:30. The table shows 2 results with a pagination control set to 20 per page. A 'Create' button is located below the table. The footer indicates 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

User Name	Created at	Last Login	Actions
root		17-Jul-2010 11:48	[Edit] [Delete] [Add]
Restricted	17 July 2010 11:30		[Edit] [Delete] [Add]

2 results [20 per page]

Create

For more information on administrators, please consult the paragraph 10.2 “Adding new administrator(s)”.

10.3. System Policies

This module provides a useful shortcut to default server and device rights settings. By accessing this module you can quickly and easily configure the Endpoint Protector 2009 Server settings such as Log Upload Interval (in minutes), Local Shadow Size (in MB), Local Log Size (in KB), etc. and default device group behavior, for each device type, separately.

The screenshot displays the 'Default System Policies' configuration page within the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options and a main content area with several sections for configuration.

Endpoint Protector 2009 Reporting and Administration Tool

Welcome Super Administrator | Logout

English [Search]

Default System Policies

Mode

Refresh Interval (sec): 10

Mode: Normal

File Tracing and Shadowing

File Tracing: ☒

File Shadowing: ☐

Default Client Settings

Log Upload Interval (min): 30

Local Log Size (KB): 10

Shadow Interval (min): 60

Shadow Size (MB): 512

Minimum File Size for Shadowing (KB): 0

Maximum File Size for Shadowing (KB): 512

Notifier Language: English

Default Rights

Unknown Device	Deny Access
USB Storage Device	Deny Access
Digital Camera	Deny Access
SmartPhone (USB Sync)	Deny Access
SmartPhone (Windows CE)	Deny Access
SmartPhone (Symbian)	Deny Access
Internal Card Reader	Deny Access

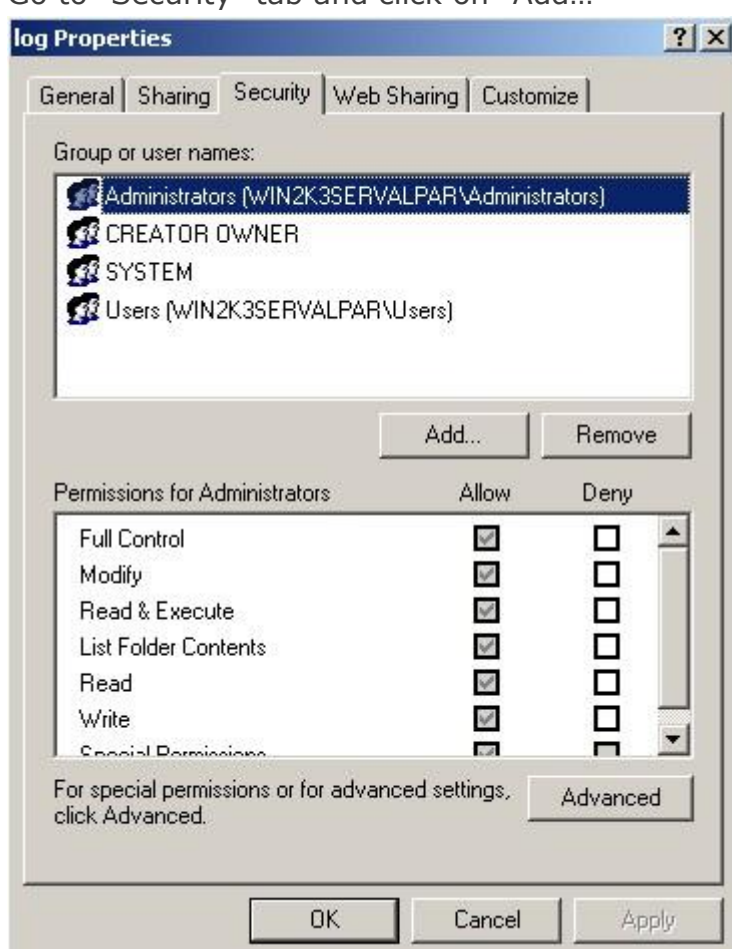
Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

To store your setup, simply click "Save".

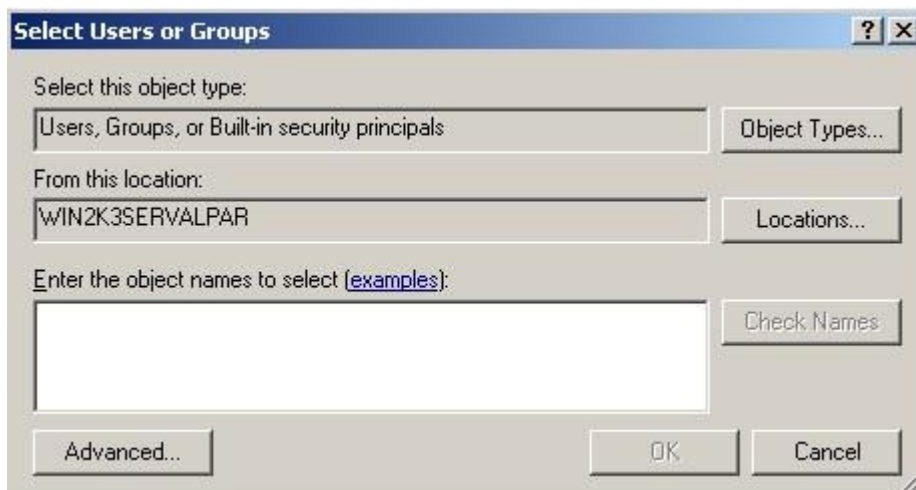
10.4. System Settings

In the System Settings module, you can modify Endpoint Protector 2009 Server Rights functionalities by giving priority to either User Rights or Computer Rights default Log and Shadow directory's and you can specify where the log and shadow files should be saved. Please note that these folders need Internet Guest Account rights (IUSR_MACHINE_NAME). To do this:

1. Create the folder(s) where you wish to store the data
2. Right-click it and select "Properties"
3. Go to "Security" tab and click on "Add..."



4. Click on “Advanced...”



Select Users or Groups

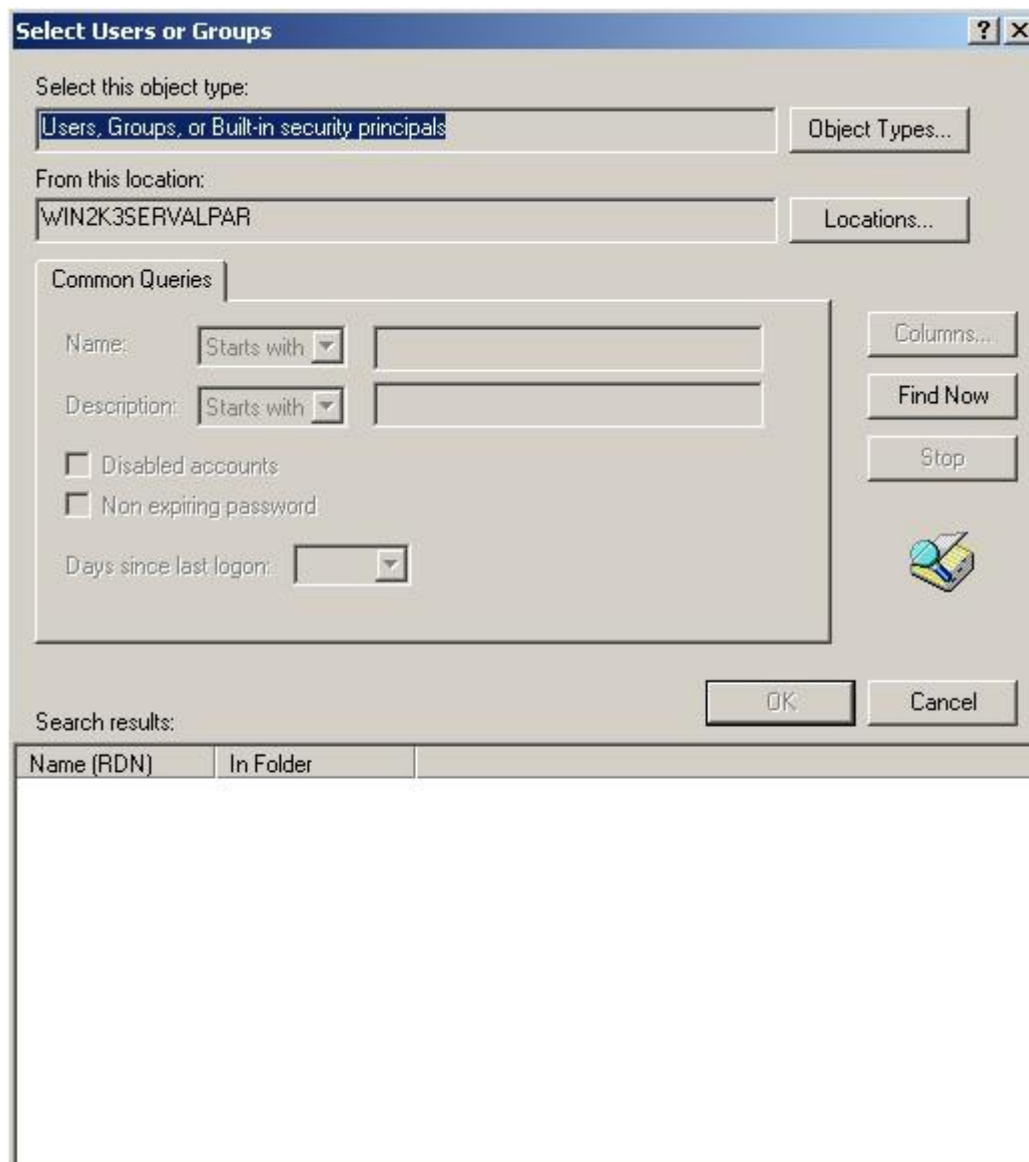
Select this object type:
 Users, Groups, or Built-in security principals Object Types...

From this location:
 WIN2K3SERVALPAR Locations...

Enter the object names to select (examples):
 Check Names

Advanced... OK Cancel

5. Click “Find Now”



Select Users or Groups

Select this object type:
 Users, Groups, or Built-in security principals Object Types...

From this location:
 WIN2K3SERVALPAR Locations...

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts


☐ Non expiring password

Days since last logon:

Columns...

Find Now

Stop

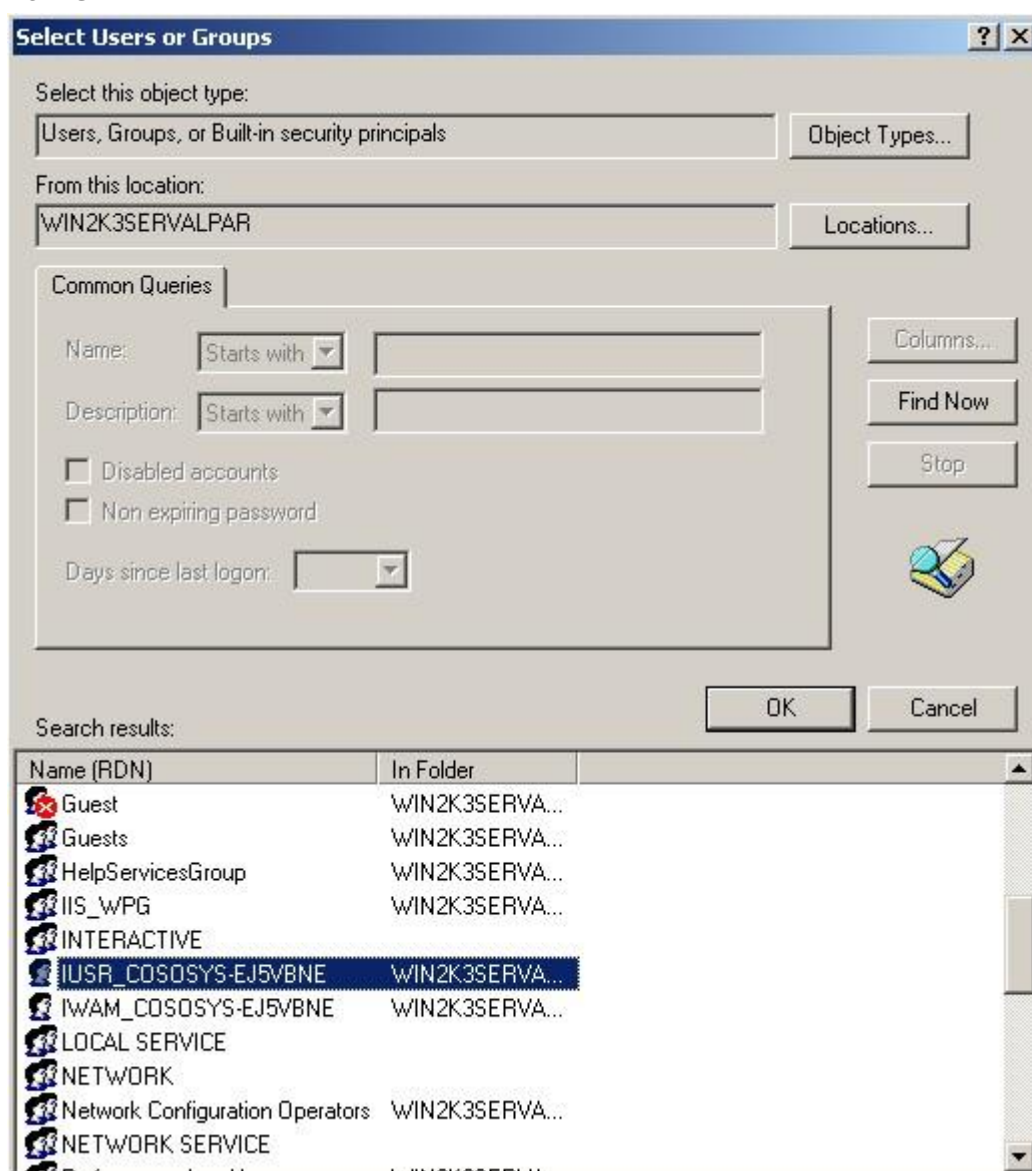


OK Cancel

Search results:

Name (RDN)	In Folder

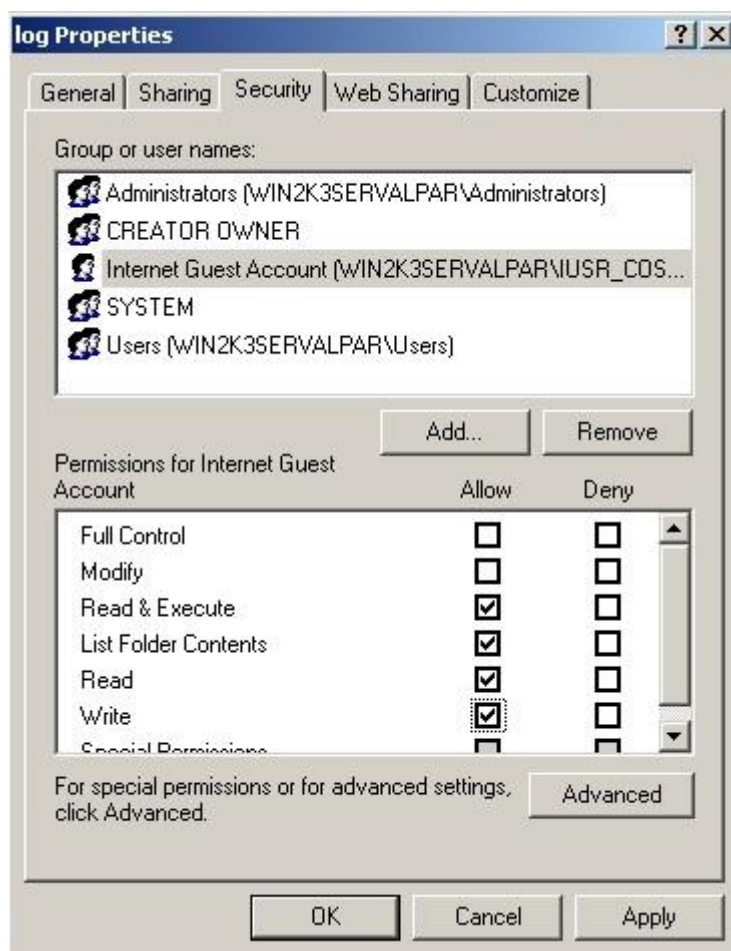
6. Select your machine from the list. The format will be "IUSR_your machine name".



7. Click "OK"



8. Check the box next to "Write" for your newly added Internet Guest Account user.



9. Click "OK".

If you created two separate folders, one for log files, the other for shadowed files, repeat the aforementioned steps for the remaining folder.

Please consult the “Setting up policies” chapter of this document for more information on this area.

Endpoint Protector 2009 Reporting and Administration Tool

Welcome Super Administrator | Logout

English

Advanced Search

Dashboard

Management

Rights

Settings

Offline Temporary Password

Reports and Analysis

System Alerts

System Parameters

System Configuration

Active Directory Import

Active Directory Sync

Active Directory Deployment

System Administrators

System Policies

System Settings

Support

Default System Settings

Storage Folders

Log Directory: c:\TempEPP

Shadow Directory: c:\TempEPP

Endpoint Protector Rights Functionality

☐ Use computer rights

☐ Use user rights

☒ Use both

Priority: ☐ User rights ☒ Computer rights

E-mail Server Settings

Hostname: smtp.1und1.com

Username: test

Password: ****

Send test e-mail to my account: ☐

Main Administrator Contact Details

Phone: 049-766221

E-mail: test@cososys.com

***Note:** This contact information is referring to Offline Temporary Password only! For Alerts, you must setup the e-mail address from System Administrators > Edit info.

Save

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.5.0

10.5. System Snapshots

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

After installing the Endpoint Protector 2009 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".

The screenshot displays the 'Endpoint Protector 2009 Reporting and Administration Tool' interface. On the left is a navigation menu with options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Sync, Active Directory Deployment, System Administrators, System Policies, System Settings, System Snapshots (highlighted), Log Backup, and Support. The main content area is titled 'Save Current State' and contains a 'Snapshot Details' form. The form has the following fields and options:



- Name:** testSnapshot
- Description:** test
- Details:** Number of machines in the system: 2. Number of groups in the system: 2. Number of rights defined for existing devices: 0. System uses both user and computer rights, computer rights have priority.
- Snapshot:** Radio buttons for 'Only Rights', 'Only Settings', and 'Both' (selected).
- Buttons:** 'Save' (with a green checkmark icon) and 'Back' (with a left arrow icon).

At the bottom of the window, the footer text reads: 'Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved.' and 'Version 3.0.5.0'.

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 screenshot shows the 'List of Available Snapshots' window in the Endpoint Protector 2009 Reporting and Administration Tool. The interface includes a sidebar with navigation options like Dashboard, Management, Rights, Settings, and System Alerts. The main content area displays a table of snapshots.

Name	Description	Created at	Created by	Actions
testSnapshot	snapshot	17 July 2010 11:31	root	 

Below the table, it indicates '1 result [20 per page]' and provides a 'Make Snapshot' button.

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.



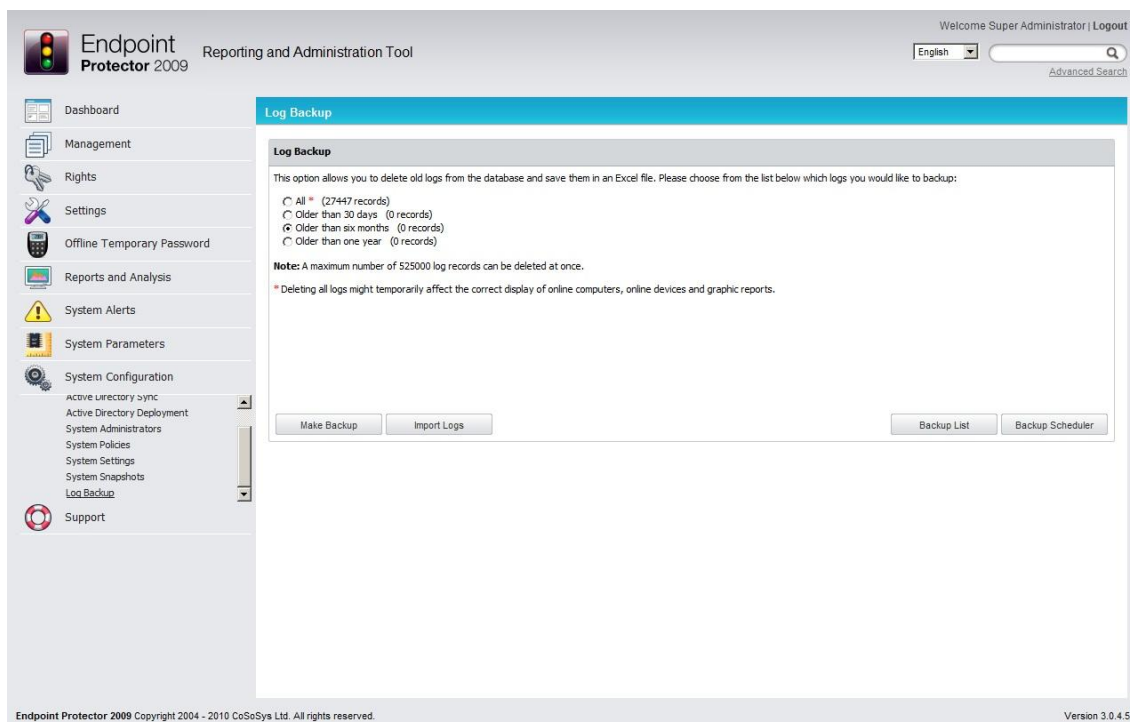
- Restore

Confirm restoration by clicking the “Restore” button again in the next window.

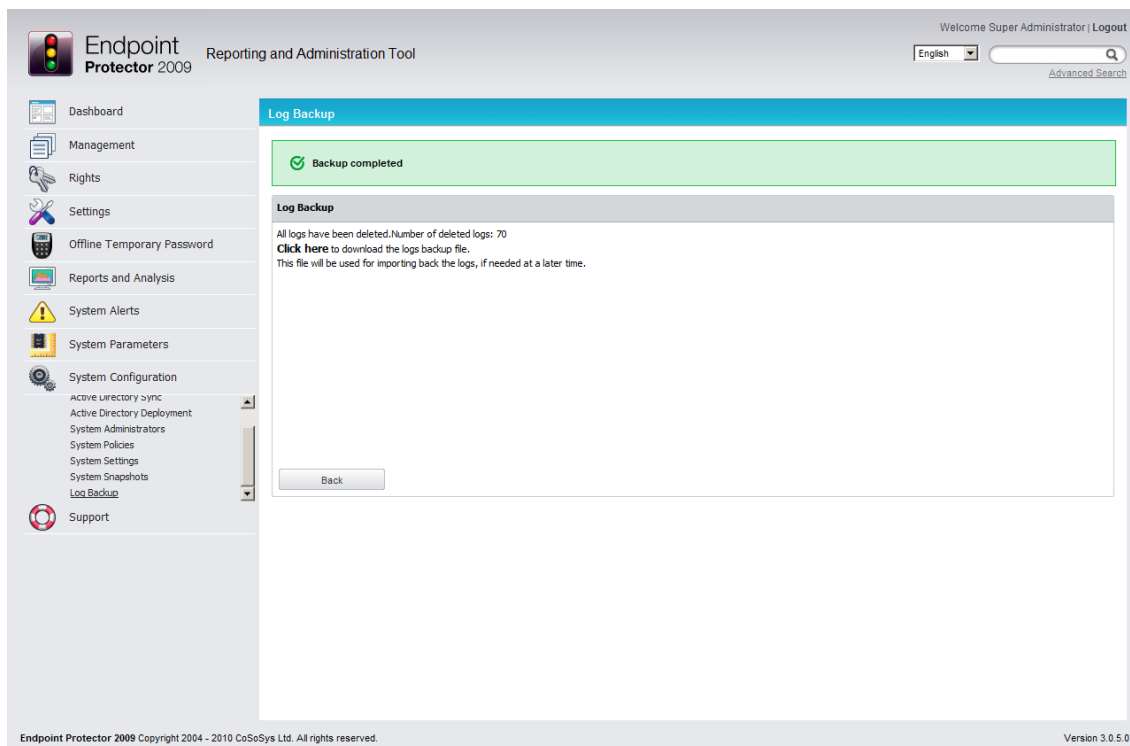
The screenshot shows the 'Restore Snapshot' window. It features a warning message: 'By restoring a snapshot, all currently defined rights and settings will be overwritten.' Below this, the 'Snapshot Details' section shows the selected snapshot 'testSnapshot' with description 'snapshot'. The 'Options' section allows choosing what to restore: 'Only rights', 'Only settings', or 'Both' (selected). At the bottom, there are 'Restore' and 'Back' buttons.

10.6. Log Backup

This module allows you to delete old logs from the database and save them in an Excel document. It also allows you to import logs that you previously created.



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



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

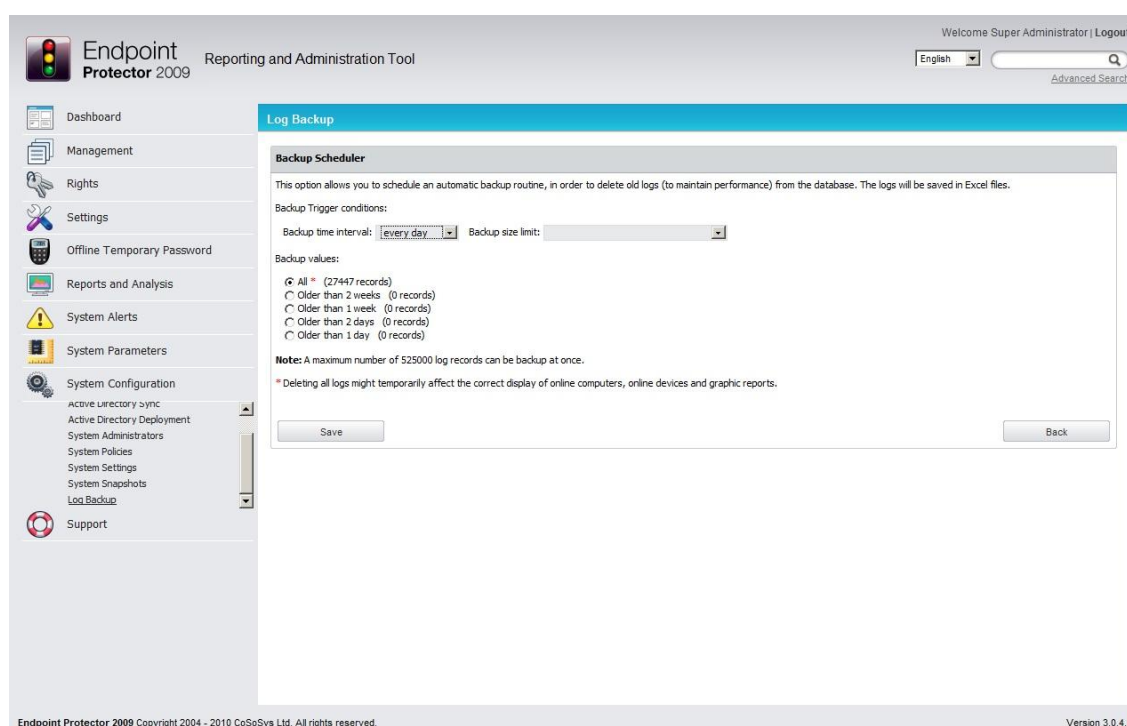
You can download and view the logs by selecting the “click here” link.

To import a log file, click the “Import Logs” button then search for the log file, via the “Browse” button.



10.6.1. Backup Scheduler (Automatic Log Backup)

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



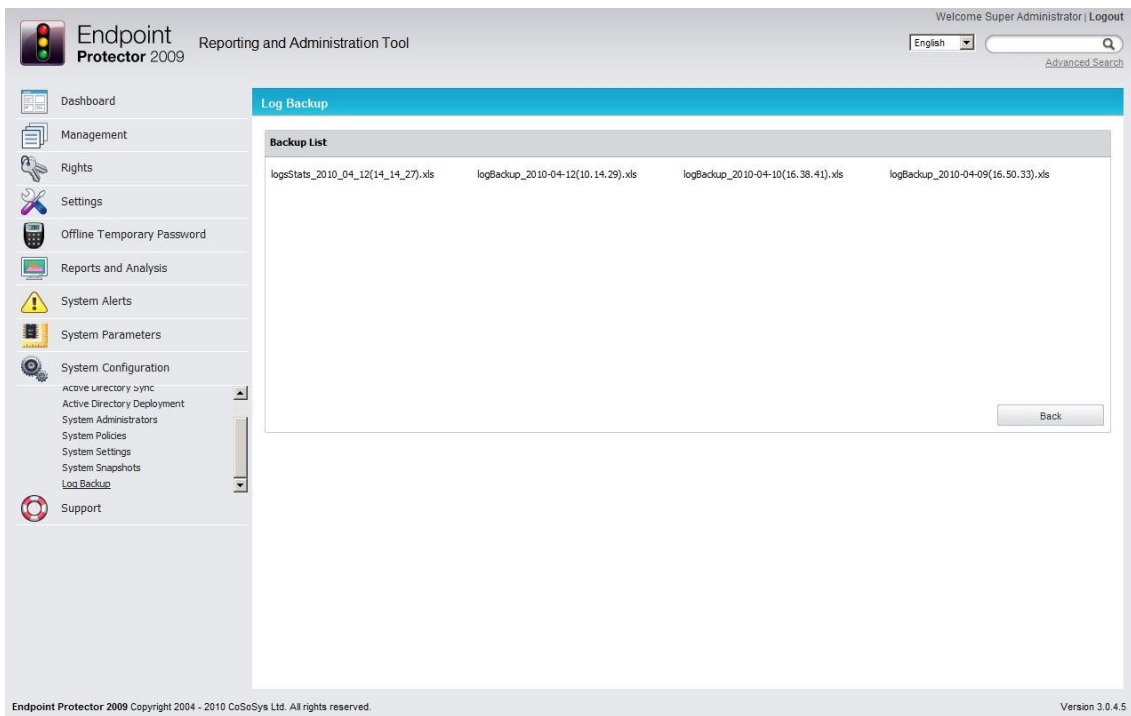
Here you can schedule an automatic backup routine by setting two trigger conditions:

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

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

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

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



The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The top navigation bar includes the product logo, name, and version, along with a language dropdown set to 'English' and a search bar. A left-hand sidebar contains a menu with options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration (with a sub-menu including Active Directory >sync, Active Directory Deployment, System Administrators, System Policies, System Settings, System Snapshots, and Log Backup), and Support. The main content area is titled 'Log Backup' and features a 'Backup List' table. The table contains four entries, each representing a backup file with its name and timestamp. A 'Back' button is located at the bottom right of the table area. The footer of the interface shows the copyright information and the version number.

Backup List			
logsStats_2010_04_12(14_14_27).xls	logBackup_2010-04-12(10.14.29).xls	logBackup_2010-04-10(16.38.41).xls	logBackup_2010-04-09(16.50.33).xls

Back

Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved. Version 3.0.4.5

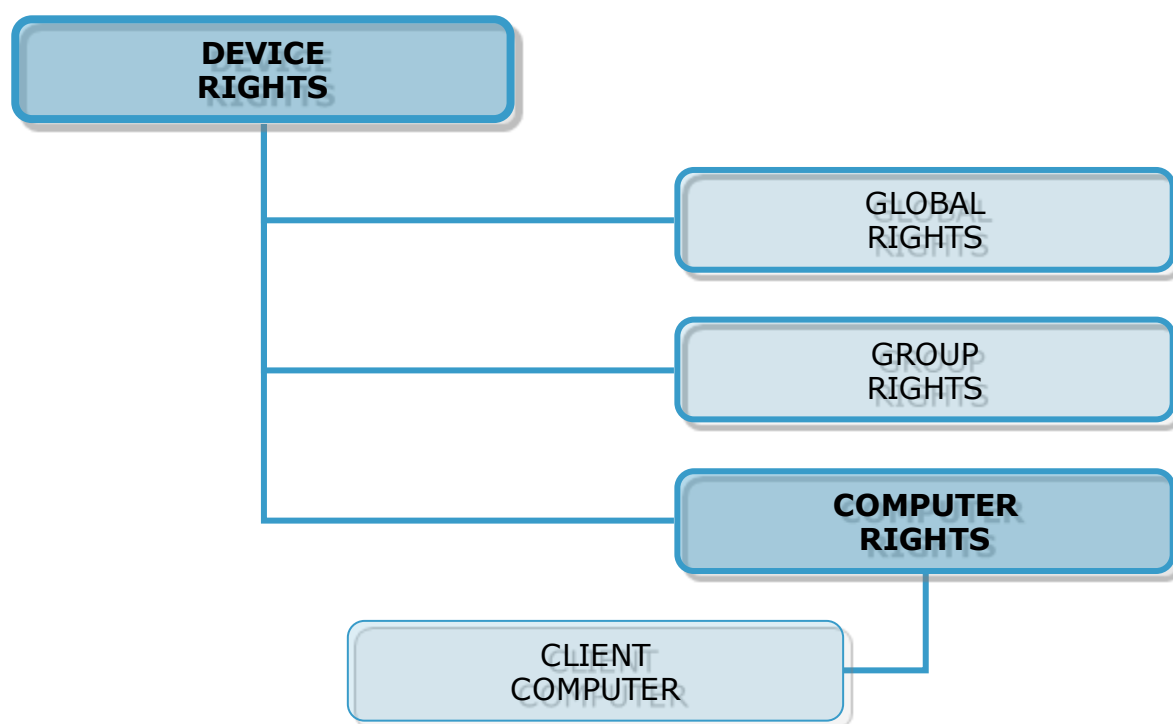
11. Setting up Policies

Most companies like to limit their employee's access to data, especially if it is confidential. Through Endpoint Protector you can enforce your security policies and keep confidential data away from the hands of curious employees. You can start setting your policies in the Rights section of Endpoint Protector. There are four sections here that need to be mentioned.

Device Rights, Computer Rights, Group Rights and Global Rights. You can find descriptions of these items in the previous paragraphs. Before configuring computers and devices, there are certain aspects of Endpoint Protector you should be aware of.

Computer Rights, Group Rights and Global Rights form a single unit and they inherit each-others settings, meaning that changes to any one of these modules affect the other ones. There are three levels of hierarchy: Global Rights, Group Rights and Computer Rights, the later being the deciding factor in rights management.

The Device Rights module surpasses all settings from Computer Rights, Group Rights and Global Rights. If you give permission to a device to be available to clients, it will be usable under any circumstances.

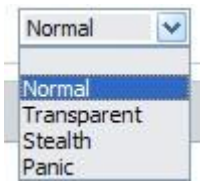


For example: in Global Rights, assign Allow for device X. If in Computer Rights, the same device does not have permission to be used; the device will not be usable. Same applies vice-versa: if the device lacks permission to be used in Global Rights, and has permission under Computer Rights, the device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

	DEVICE 1	DEVICE 2	DEVICE 3	DEVICE 4	DEVICE 5	DEVICE 6
GLOBAL RIGHTS	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED
GROUP RIGHTS	NOT ALLOWED	NOT ALLOWED	ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED
COMPUTER RIGHTS	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED
CLIENT COMPUTER	ALLOWED	NOT ALLOWED	NOT ALLOWED	ALLOWED	ALLOWED	NOT ALLOWED

12. Modes for Users, Computers and Groups

Endpoint Protector features several functionality modes for users, computers and groups. These modes are accessible for each item (users, computers, groups) from the Settings module of Endpoint Protector using the "Edit" button.



You can change these at any given time.

There are four modes from which you can choose from:

- Stealth Mode
- Transparent Mode
- Panic Mode
- Normal Mode (as it currently is running in current specification applying the last know policy)

12.1. Transparent Mode

This mode is used if you want to block all devices but you don't want the user to see and know anything about EPP activity.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is blocked regardless if authorized or not
- Administrator receives alerts (dashboard also shows alerts) for all activities

12.2. Stealth Mode

Similar to Transparent mode, Stealth mode allows the administrator to monitor all of the users and computers activities and actions with all devices allowed.

- no system tray icon is displayed
- no system tray notifications are shown
- everything is allowed (nothing is blocked regardless of what activity)
- file shadowing and file tracing are enabled to see and monitor all user activity
- Administrator receives alerts (dashboard shows also alerts) for all activities

12.3. Panic Mode

If Stealth Mode and Transparent Mode are set manually, Panic Mode will be set automatically by the system, when it considers it necessary.

- system tray icon is displayed
- notifications are displayed
- everything is blocked regardless if authorized or not
- Administrator receives alert (dashboard also shows alerts) when PCs are going in and out of Panic mode

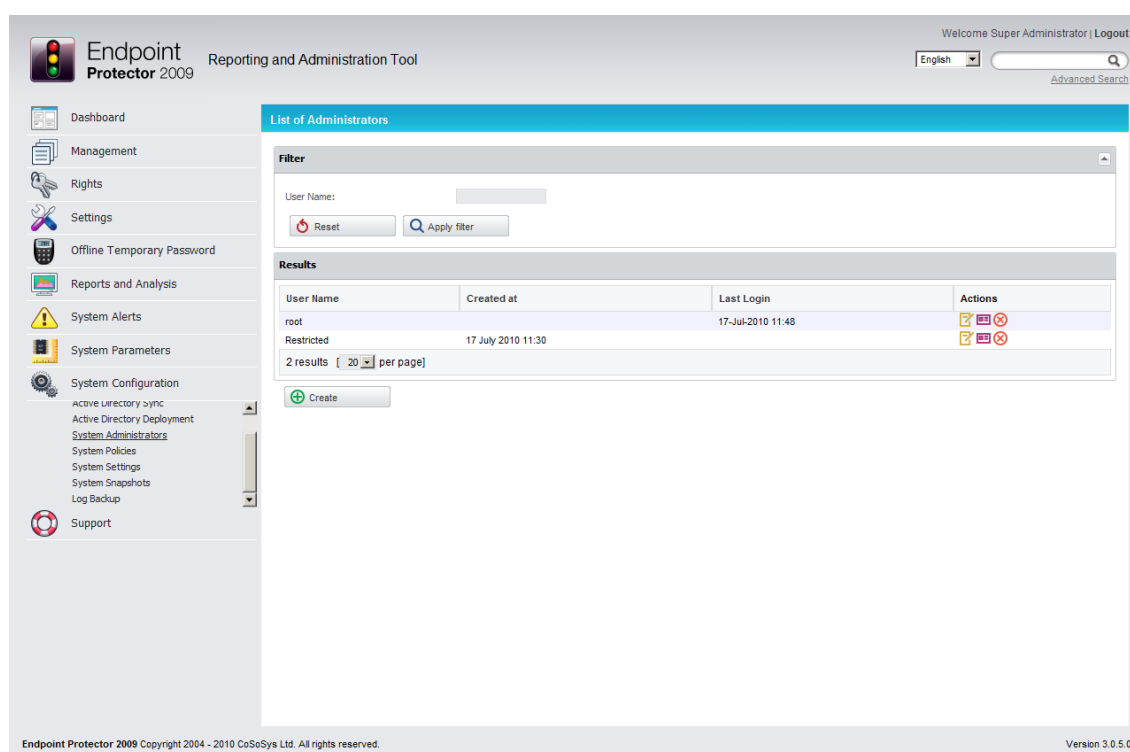
12.4. Adding new administrator(s)

You can add an unlimited number of system administrators, depending on the size and manageability of your network.

While fewer administrators are recommended for easier data loss prevention, it is easier to manage a large network with more.

To add an administrator or Super Administrator in Endpoint Protector, you must login as a super administrator and access the "System Configuration" module then the "Administrators" panel.

Here you can see a list of current Administrator and Super Administrators.



The screenshot displays the Endpoint Protector 2009 Reporting and Administration Tool interface. The left sidebar contains a navigation menu with options: Dashboard, Management, Rights, Settings, Offline Temporary Password, Reports and Analysis, System Alerts, System Parameters, System Configuration, Active Directory Sync, Active Directory Deployment, System Administrators, System Policies, System Settings, System Snapshots, Log Backup, and Support. The main content area is titled "List of Administrators" and includes a "Filter" section with a "User Name" input field, "Reset", and "Apply filter" buttons. Below the filter is a "Results" table with columns: User Name, Created at, Last Login, and Actions. The table lists two administrators: "root" and "Restricted". The "root" user was created on 17 July 2010 at 11:30 and last logged in on 17-Jul-2010 at 11:48. The "Restricted" user was created on 17 July 2010 at 11:30. The table shows 2 results with a pagination of 20 per page. A "Create" button is located below the table. The footer of the interface includes the copyright notice "Endpoint Protector 2009 Copyright 2004 - 2010 CoSoSys Ltd. All rights reserved." and the version number "Version 3.0.5.0".

User Name	Created at	Last Login	Actions
root	17 July 2010 11:30	17-Jul-2010 11:48	[Edit] [Delete] [Reset]
Restricted	17 July 2010 11:30		[Edit] [Delete] [Reset]

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

Administrator User	
User Informations	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Password Confirmation:	<input type="password"/>
Permissions and groups	
Is active:	<input checked="" type="checkbox"/>
Is super admin:	<input type="checkbox"/>
Information	
Last Login:	
<input type="button" value="Save"/> <input type="button" value="Save and Add"/> <input type="button" value="Back"/>	

Enter the desired user name and password for the new account, then set if the account is active or not or whether is a super admin or not.

Permissions and groups	
Is active:	<input checked="" type="checkbox"/>
Is super admin:	<input type="checkbox"/>

Is active – if this option is not enabled the selected user cannot log in to the Endpoint Protector console. Use this option in case you want to create temporary admin or super admin privileges to a certain user and then remove them or if you want to disable an administrator but do not want to delete his credentials from the server.

Is Super Admin – Super Administrators have more rights than administrators. Super Administrator can create, delete and modify administrator and super administrator settings, while standard administrators do not have this right. The most important difference is that only super administrators are able to view the "Reports and Analysis" section if the option "Data Security Privileges" is selected (please see paragraph 9.6 "System Security / Client Uninstall Protection").

12.5. Working with logs and reports

Endpoint Protector creates a device activity log in which it records actions from all clients and devices connected along with all administrative actions such as device authorizations, giving a history for devices, PCs and users for future audits and detailed analysis.

Logs Report - The most powerful and detailed representation of activity recording can be achieved using this module. This allows the administrator to see exactly which device, computer a user used on a specific time interval, and whether the shadowing for that user/device is enabled or not. There is a special filter designed to make it easier to find this information.

Online Users - Online users are end users who have logged on to a client computer.

Online Computers - Online Computers are client computers which have been set up to communicate with the Endpoint Protector server by installing the Endpoint Protector Client. Here you can see a list of computers which are currently powered on and you can view the actions they have taken.

Connected Devices - Connected Devices are devices which are currently plugged-in to one of the (online) client computers. Here again you have the possibility to view an activity log, this time, of the device.

User History - This module records all of the users (clients) that have been registered via the Endpoint Protector Client in the Endpoint Protector Server. You can also find more information on the client users, such as first name, last name, phone number, e-mail(s) and the actions they have taken.

Device History - Here you will find a history of recorded devices and actions. These are sorted by device type, device name, owner, description, TD (TrustedDevices), vendor and product ID (VID, PID), serial number and last known time of connection. You can export the history for each device separately in an Excel format.

Computer History - contains a list with all registered computers (clients). These are sorted by computer name, domain, workgroup, IP, computer group, computer location and last known time of connectivity (last time online). You can export the history for each computer separately in an Excel format.

Statistics - The statistics module can generate reports on registered computers, devices and users based on traffic, connections or overall activity. You can set a period for this report (last week, month or year).

12.6. Finding users, devices, computers and groups

12.7. Search

Endpoint Protector's search feature lets you easily find what you are looking for, whether is a newly added device, user or a previously created computer or group.

To use the advanced search feature of Endpoint Protector, log in and access the "Dashboard" module, then the "Search" module.

Now you can choose to search for computers, devices, users or groups. Endpoint Protector also lets you choose the number of results you see on each page.

Search Criteria























































Term:

Search In: ☒ Machines ☒ Devices ☒ Users ☒ Groups **[Check All Uncheck All]**

Match: ☒ Partial ☐ Exact

Results per page:

If you are not sure what you are looking for, you may browse through all computers, devices, users and groups just below the "Search" button, in the same window.

Results					
Type	Name	Description	Modified at	Modified by	Actions
Device	/				  
User	Administrator		2009-02-19 16:12:01	root1	  
User	SUPPORT_388945a0		2009-02-19 16:12:01	root1	  
User	krbtgt		2009-02-19 16:12:01	root1	  
User	Guest		2009-02-19 16:12:01	root1	  
Device	(Standard floppy disk drives)	(Standard floppy disk drives) / (Standard floppy disk drives)			  
Device	(Standard floppy disk drives)	(Standard floppy disk drives) / (Standard floppy disk drives)			  
Device	(Standard floppy disk drives)	(Standard floppy disk drives) / (Standard floppy disk drives)			  
Computer	aamachine		2009-02-20 10:01:17	root	  
User	UUUUUU	abcdefg	2009-02-19 15:59:01	root1	  
Group	Account Operators	Members can administer domain user and group accounts	2009-02-19 16:12:00	root1	  
Group	Administrators	Administrators have complete and unrestricted access to the computer/domain	2009-02-19 16:12:00	root1	  
User	Alpar	Alpar Alpar			  
User	alpar26 - test user	alpar26 - test user alpar26 - test user			  
Device	arcade	arcade / cliente			  
Device	ASUS CB-5216A ATA Device	ASUS CB-5216A ATA Device / (Standard CD-ROM drives)			  
Device	ASUS DRW-1814BL	ASUS DRW-1814BL / (Standard CD-ROM drives)			  
Device	ASUS DRW-2014L1T	ASUS DRW-2014L1T / (Standard CD-ROM drives)			  

For easier navigation, these items can be sorted by Type (device, user, computer and group), name, description, and actions.

13. Enforced Encryption with TrustedDevices

Damage control

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. If a TrustedDevice fails to get authorization from the Endpoint Protector 2009 Server, it will not be usable.

How does it work?

Enforcing Encryption can be done by utilizing TrustedDevices. TrustedDevices must receive authorization from the Endpoint Protector 2009 Server, otherwise they will be unusable.

There are four levels of security for TrustedDevices:

- **Level 1** - Minimum security for office and personal use with a focus on software based encryption for data security. Offers companies already regulatory compliance.
Any USB Flash Drive and most other portable storage devices can be turned into a TrustedDevice Level 1 with EasyLock Software from CoSoSys.
No hardware upgrade is required.
<http://www.endpointprotector.com/en/index.php/products/easylock>
- **Level 2** - Medium security level with biometric data protection or advanced software based data encryption.
Requires special hardware that includes security software and that has been tested for TrustedDevice Level 2.
Hardware is widely available in retail stores.

- **Level 3** - High security level with strong hardware based encryption that is mandatory for sensitive enterprise data protection for regulatory compliance such as SOX, HIPAA, GBLA, PIPED, Basel II, DPA, or PCI 95/46/EC.
Requires special hardware that includes advanced security software and hardware based encryption and that has been tested for TrustedDevice Level 3.
- **Level 4** - Maximum security for military, government and even secret agent use. Level 4 TrustedDevices 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.
Requires special hardware that is available primarily through security focused resellers.

13.1. How a Level 1 TrustedDevice Works

User connects Device to Endpoint Protector protected Client PC. Device is blocked by Endpoint Protector (default action).

Device is checked for authorization.

If device is an authorized TrustedDevice Level 1, the EasyLock software on Device will automatically open.

User can transfer files via Drag & Drop in EasyLock from the PC to the TrustedDevice.

Data transferred to devices is encrypted via 256bit AES.

User cannot access the device using Windows Explorer or similar applications (e.g. Total Commander).

User does not have the possibility to copy data in unencrypted state to the TrustedDevice.

“TrustedDevice” implies that the devices offer a safe, risk-free environment to transfer sensitive data and tracking or shadowing files and file transfers is not needed for these devices.

Administrator can audit what user, with what device, on what PC, has transferred what files.

13.2. EasyLock Software for TrustedDevices Level 1

EasyLock allows portable devices to be identified as TrustedDevices and protects data on the device with government-approved 256bit AES CBC-mode encryption. With the intuitive Drag & Drop interface, files can be quickly copied to and from the device.

To install EasyLock on an USB Flash drive one has to copy the file "EasyLock.exe" to the root folder of a partition associated with that device.

Managing TrustedDevices from EPP server console

Access to TrustedDevices can be configured from the Global Rights module of Endpoint Protector 2009, under Rights tab.

Access the drop-down box next to USB Storage Device and select the desired level of TrustedDevices you wish to grant access to.

More information about EasyLock:

<http://www.endpointprotector.com/en/index.php/products/easylock>

Edit Global Rights



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

Groups

Name:	Global
Description:	Global Group including all the entities

Device Types

Unknown Device	Deny Access
USB Storage Device	Deny Access
Digital Camera	<div> Preserve global setting Deny Access Allow Access Read Only Access Allow Access if TD Level 1 Allow Access if TD Level 2 Allow Access if TD Level 3 Allow Access if TD Level 4 </div>
SmartPhone (USB Sync)	
SmartPhone (Windows CE)	
SmartPhone (Symbian)	
Internal Card Reader	Deny Access
PCMCIA Device	Deny Access
FireWire Bus	Deny Access
ZIP Drive	Deny Access
Internal CD or DVD RW	Deny Access
Internal Floppy Drive	Deny Access
Card Reader Device (MTD)	Deny Access
Card Reader Device (SCSI)	Deny Access
Windows Portable Device	Deny Access
Mobile Phones (Sony Ericsson, etc.)	Deny Access

14. Endpoint Protector Client

The Endpoint Protector Client is the application which once installed on the client Computers (PC's), communicates with the Endpoint Protector Server and blocks or allows devices to function, as well as sends out notifications in case of unauthorized access.

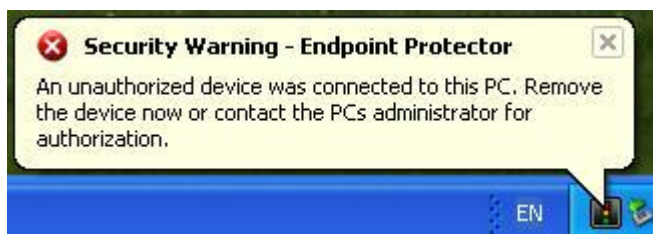
14.1. Endpoint Protector Client Security

The Endpoint Protector Client has a built in security system which makes stopping the service nearly impossible.

This mechanism has been implemented to prevent the circumvention of security measures enforced by then network administrator.

14.2. Client Notifications (Notifier)

The Endpoint Protector Client, depending in the mode it is currently running on, will display a notification from the taskbar icon when an unauthorized device is connected to the system. Not only does it log any attempts to forcefully access to system, it can also trigger the system's Panic mode.



14.3. Offline Functionality for Endpoint Protector Client

Depending on the global settings the Endpoint Protector Client will store a local file tracing history and a local file shadow history that will be submitted and synchronized with the Endpoint Protector Server upon next connection to the network.

14.4. DHCP / Manual IP address

Endpoint Protector Client automatically recognizes changes in the network's configuration and updates settings accordingly, meaning that you can keep your laptop protected at the office (DHCP) and at home (Manual IP address) too without having to reinstall the client or modify any changes.

14.5. Client Removal

14.5.1. Client Removal on Windows OS

The Endpoint Protector Client cannot be uninstalled without specifying the password set by the administrator(s) in the Reporting and Administration Tool.

To use this password-protect feature, please consult the paragraph 9.6 "System Security / Client Uninstall Protection".

The password sent by the Endpoint Protector Server is hashed and stored in the registry. If it is deleted, the uninstall process will instantly stop. Tampering with the registry value of the hash will lead to an irremovable client.



14.5.2. Client removal on MAC OS X

To remove the Endpoint Protector Client you need to run (double click in Finder) the "remove-epp.command" file that was attached to the "Endpoint Protector" client package that you downloaded.

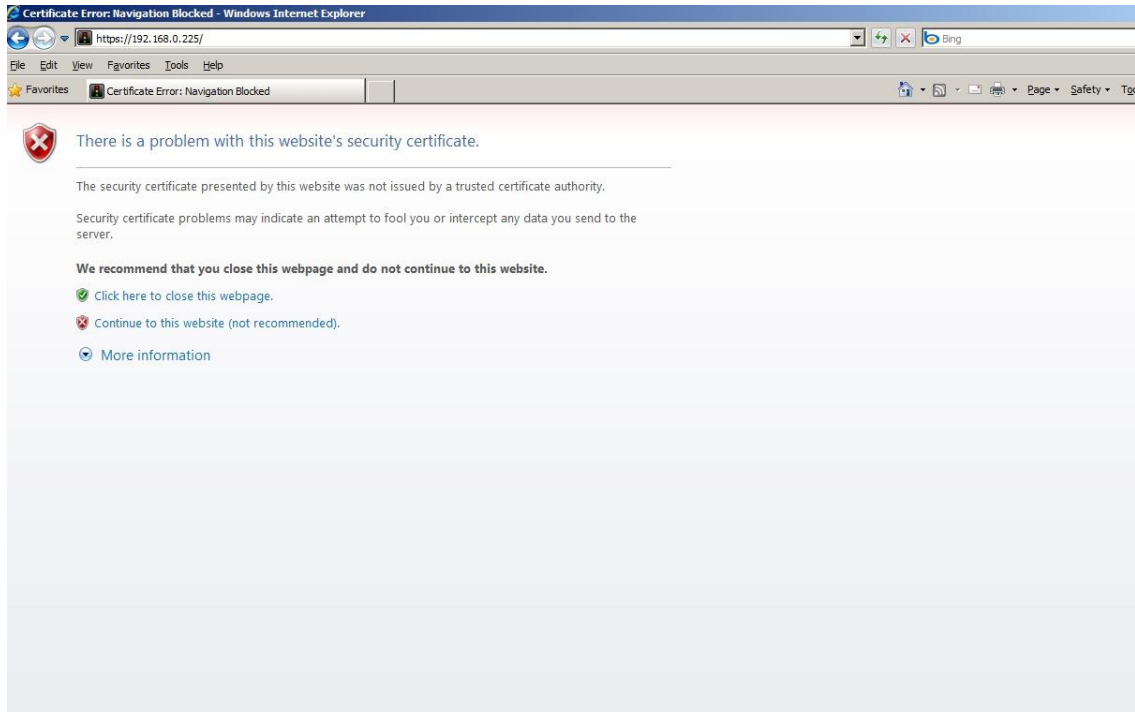
You will be prompted to enter the root password to perform administrative tasks.


15. Installing Root Certificate to your Internet Browser

15.1. For Microsoft Internet Explorer

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

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



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

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

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

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

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

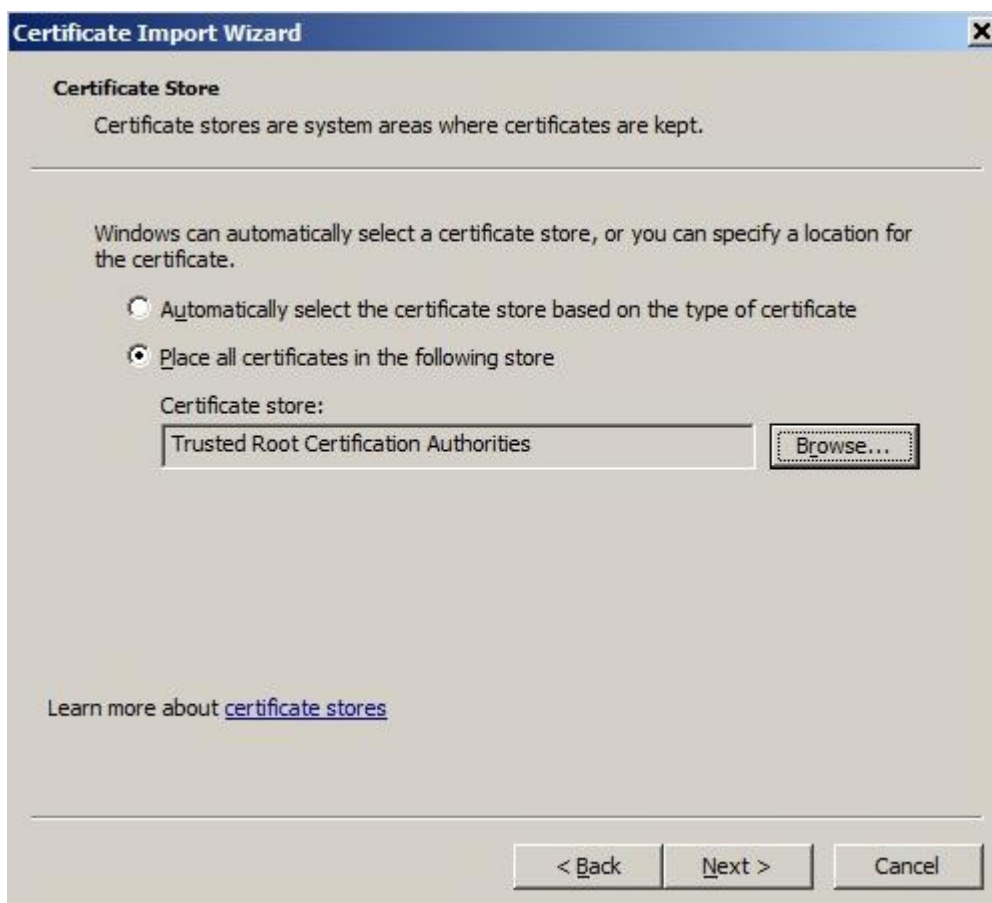


Select the "General" tab and then click "Install Certificate..." button as shown above.

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



In Certificate Import Wizard window, select “Place all certificates in the following store” radio button.



Click “Browse” button.

From the browser list, select “Trusted Root Certification Authorities”.

Then click the “Next” button.



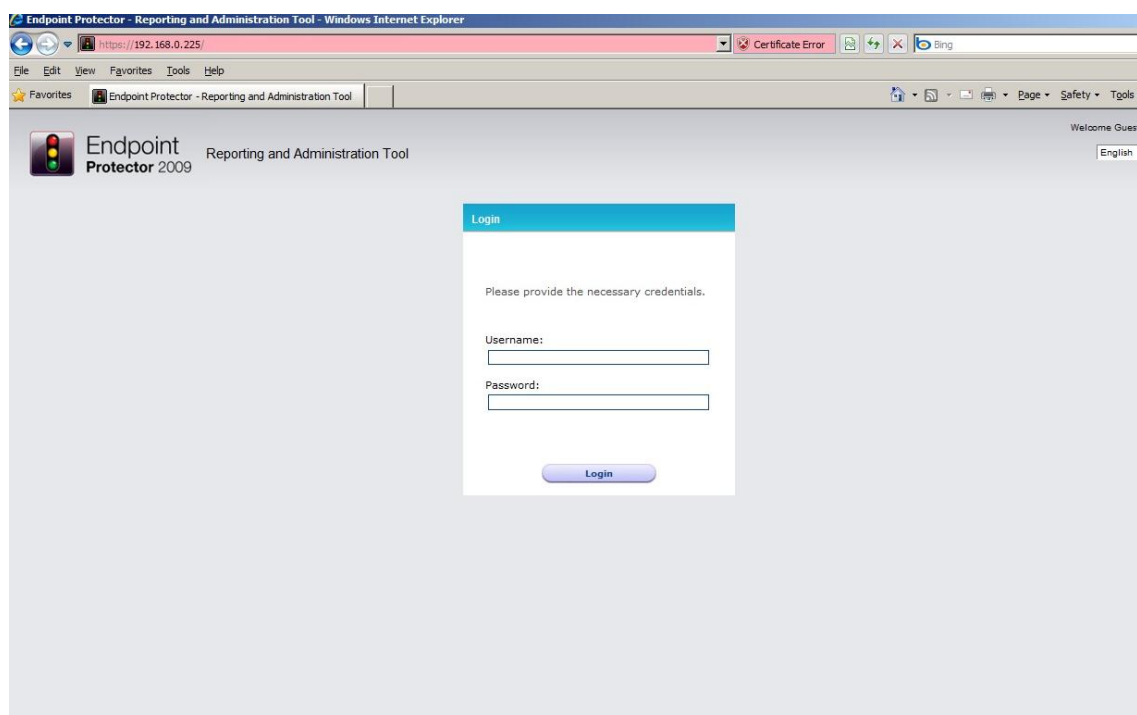
Another "Completing the Certificate Import Wizard" pops up. Just click the "Finish" button.

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



You have now successfully installed the Certificate.

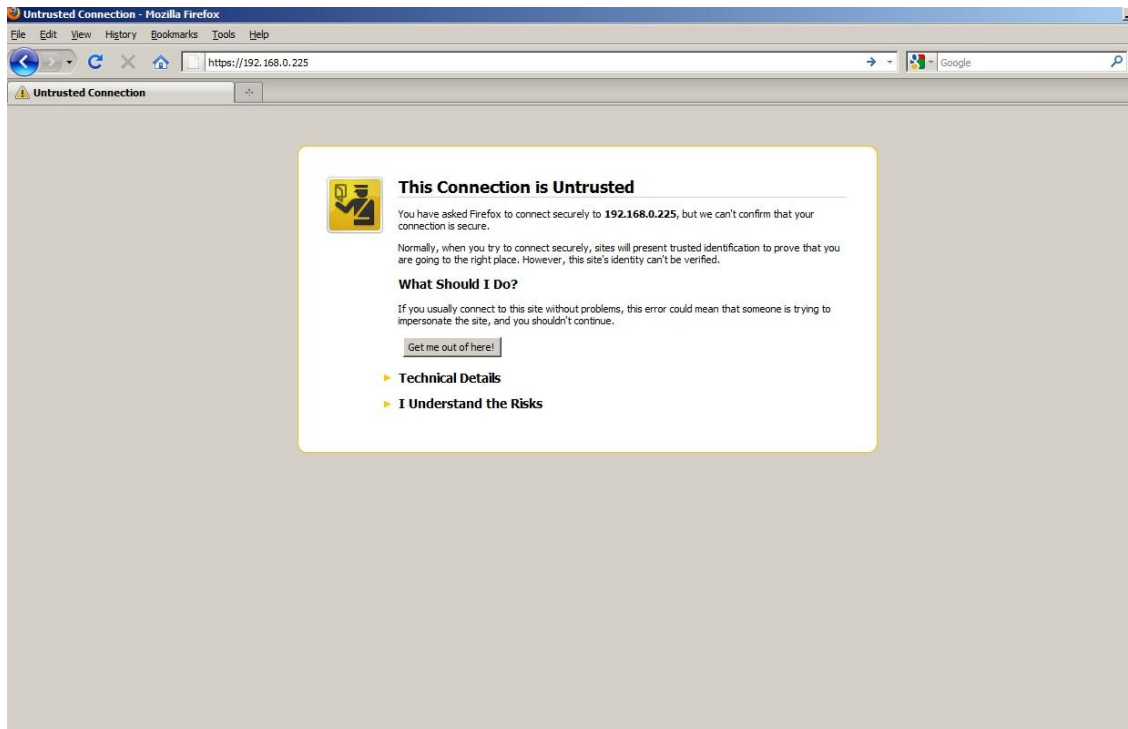
Close the Internet Explorer browser and try to access the Endpoint Protector Administration and Reporting Tool IP address again.



15.2. For Mozilla Firefox

Open the Browser.

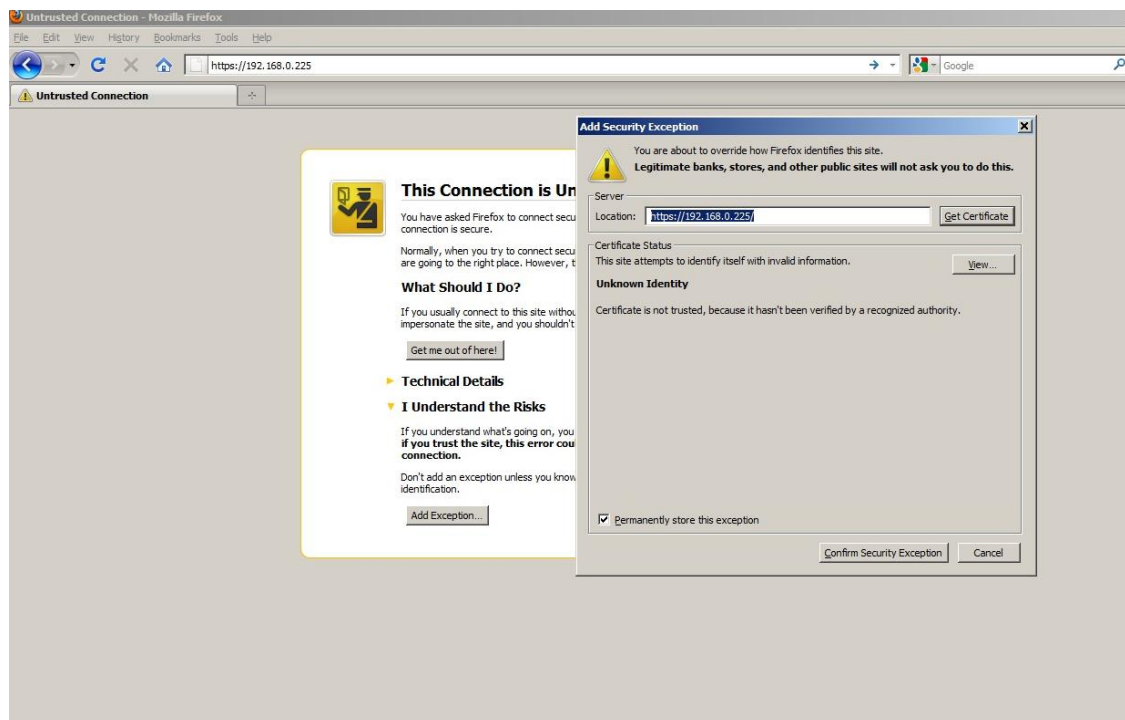
Open Endpoint Protector Administration and Reporting Tool IP address. (Your Appliance static IP Address, example <https://192.168.0.201>).



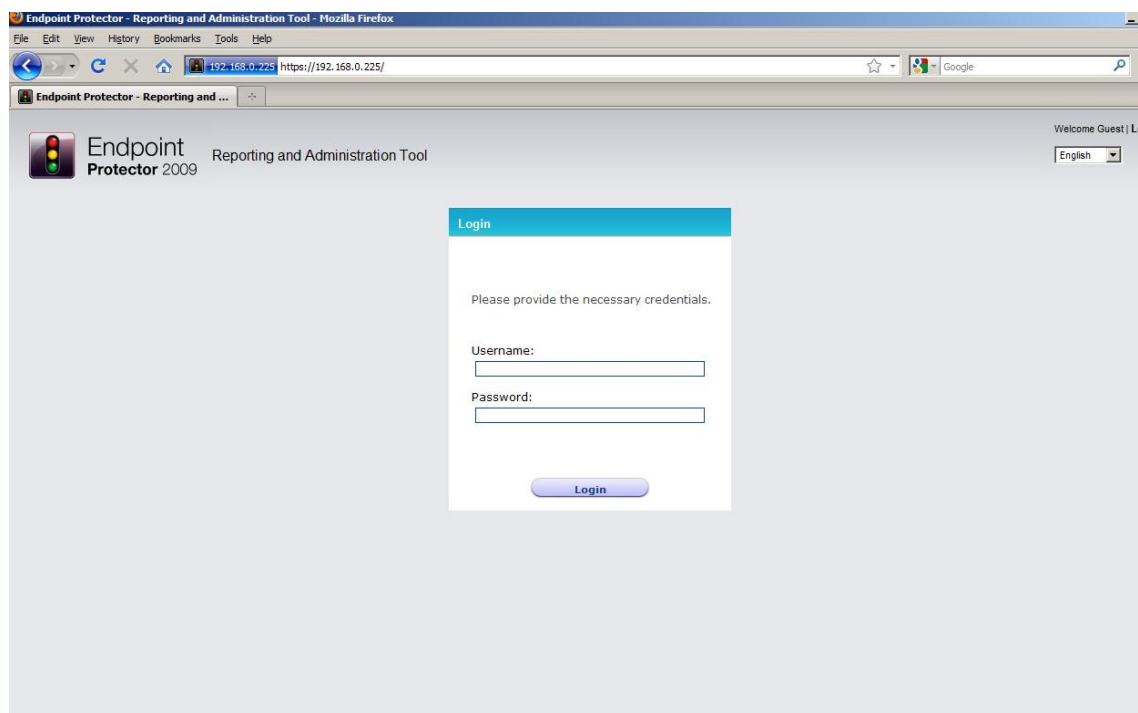
From the above screenshot This Connection is Untrusted, choose I Understand the Risks. Click Add Exception.

Security Warning window pops up.

Just click Get Certificate button and then the Confirm Security Exception button.



Close the browser and start it again.



16. Terms and Definitions

Here you can find a list of terms and definitions that are encountered throughout the user manual.

16.1. Server Related

Appliance – Appliance refers to the Endpoint Protector Appliance which is running the Endpoint Protector Server, Operating System, Databases, etc.

Computers – refers to PC's, workstations, thin clients, notebooks which have Endpoint Protector Client installed.

File Tracing - this feature will track all data that was copied to and from prior authorized portable storage devices.

File Shadowing – this feature saves a copy of all, even deleted files that were used in connection with controlled devices on a network storage server.

Devices – refers to a list of known portable storage devices, ranging from USB storage devices to digital cameras, LTP storage devices and biometric devices.

Groups – can be groups of devices, users or computers. Grouping any of these items will significantly help the server administrators to easily manage rights and settings for them.

16.2. Client Related

Endpoint – can be a Personal Computer, a Workstation you use at the office or a Notebook. An endpoint can call and be called. It generates and terminates the information stream.

TrustedDevices – portable storage devices that carry a seal of approval from the Endpoint Protector Server and can be utilized according to their level (1-4). For more information please see “Enforced Encryption with TrustedDevices” section.

Client - refers to the client user who is logged in on a computer and who facilitates the transaction of data.

Rights – applies to computers, devices, groups, users and global rights; it stands for privileges that any of these items may or may not possess.

Online computers – refers to PC's, Workstations and/or Notebooks which have Endpoint Protector Client installed and are currently running and are connected to the Endpoint Protector server.

Connected devices – are devices which are connected to online computers.

Events – are a list of actions that hold major significance in Endpoint Protector. There are currently 17 events that are monitored by Endpoint Protector:

- Connected – the action of connecting a device to a computer running Endpoint Protector Client.
- Disconnected – the action of (safely) removing a device from a computer running Endpoint Protector Client.
- Enabled – refers to devices; the action of allowing a device access on the specified computer(s), group(s) or under the specified user(s).
- Disabled – refers to devices; the action of removing all rights from the device, making it inaccessible and therefore unusable.
- File read - a file located on a portable device was opened by a user or the file was automatically opened if the portable device was autorun by the operating system.
- File write – a file was copied onto a portable device.
- File read-write – a file located on a portable device was opened and edited; changes were saved to the file.
- File renamed – a file located on a portable device has been renamed.

- File delete – a file located on a portable device has been deleted.
- Device TD – means that a device is registered as a TrustedDevice and has access to files accordingly
- Device not TD – means that a device is not trusted and does not have automatic access to files
- Delete – refers to computers, users, groups, alerts and devices; the action of removing any of these items from the list
- Enable read-only – refers to devices; the action of allowing access to devices but disabling the ability to write on them. User(s) can copy files from device(s) but cannot write anything onto the device.
- Enable if TD Level 1-4 – refers to TrustedDevices; grants the device access if the device is a level one, two, three or four TrustedDevice.
- Offline Temporary Password used – refers to computers, the action of temporarily allowing access to a specific device on a certain client computer.

17. Support

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

One of our team members will contact you in the shortest time possible.

Even if you do not have a problem but miss some feature or just want to leave us general comment we would love to hear from you. Your input is much appreciated and we welcome any input to make computing with portable devices safe and convenient.

18. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2010 CoSoSys Ltd.; Endpoint Protector Basic, EPPBasic, Endpoint Protector, My Endpoint Protector are trademarks of CoSoSys Ltd. All rights reserved. Windows is registered trademark of Microsoft Corporation. Macintosh, Mac OS X are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.