SAFETICA QUICK GUIDE

www.safetica.com

SAFETICA QUICK GUIDE

for Safetica version 5.0.4

Author: Safetica Technologies s.r.o.

Safetica was developed by Safetica Technologies s.r.o.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

For more information visit www.safetica.com.

Published: 2013

CONTENT

Introduction

Main modules of Safetica

Architecture

Installation

Safetica Management Console

Safetica Endpoint Client

1 Introduction

Dear user,

We are very pleased by your confidence in selection of Safetica and we believe that you will be fully satisfied. In this document you can find brief description of all components of the product and instructions for acquiring all required components. Safetica quick wizard will guide you through the installation, the initial run in the company network and illustrative examples of use.

Safetica brings completely new insight in the internal security. It is the first security solution, which combines real prevention with actual protection against internal threats. By monitoring of users it reveals their risk behavior and by blocking unsolicited actions and protection against data leakage (DLP) it protects the company from the consequences of undesirable activities of its employees. No other software can protect a company against all major internal threats in such a complex manner.

Should you encounter a problem when using the software, consultthe complete documentation of Safetica at first or Frequently asked technical questions of Safetica users and if you still cannot solve it, kindly contact the technical support at http://www.safetica.com/support.

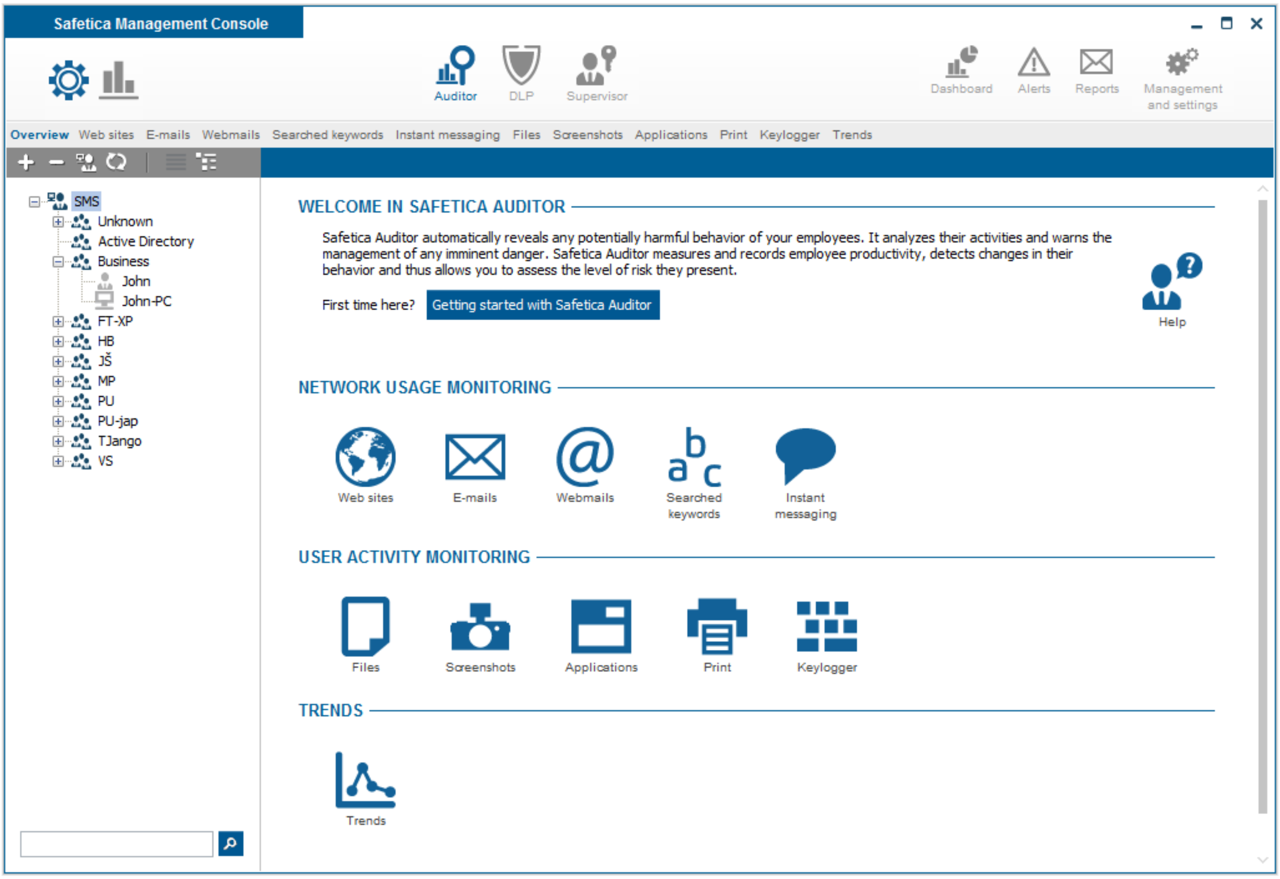
Thank you,

Safetica Technologies team, producer of Safetica

2 Main modules of Safetica

2.1 Auditor

Auditor automatically reveals any potentially dangerous behavior of your employees. It analyzes their activities and warns the management of any imminent danger. It provides synoptical information on your employees' real productivity and reveals changes in their behavior caused for example by the loss of motivation or a better offer from the competition. In case of doubt it provides detailed information on every single activity of your employees: Which applications they launched, websites they visited, whom they wrote to and what files they worked with.

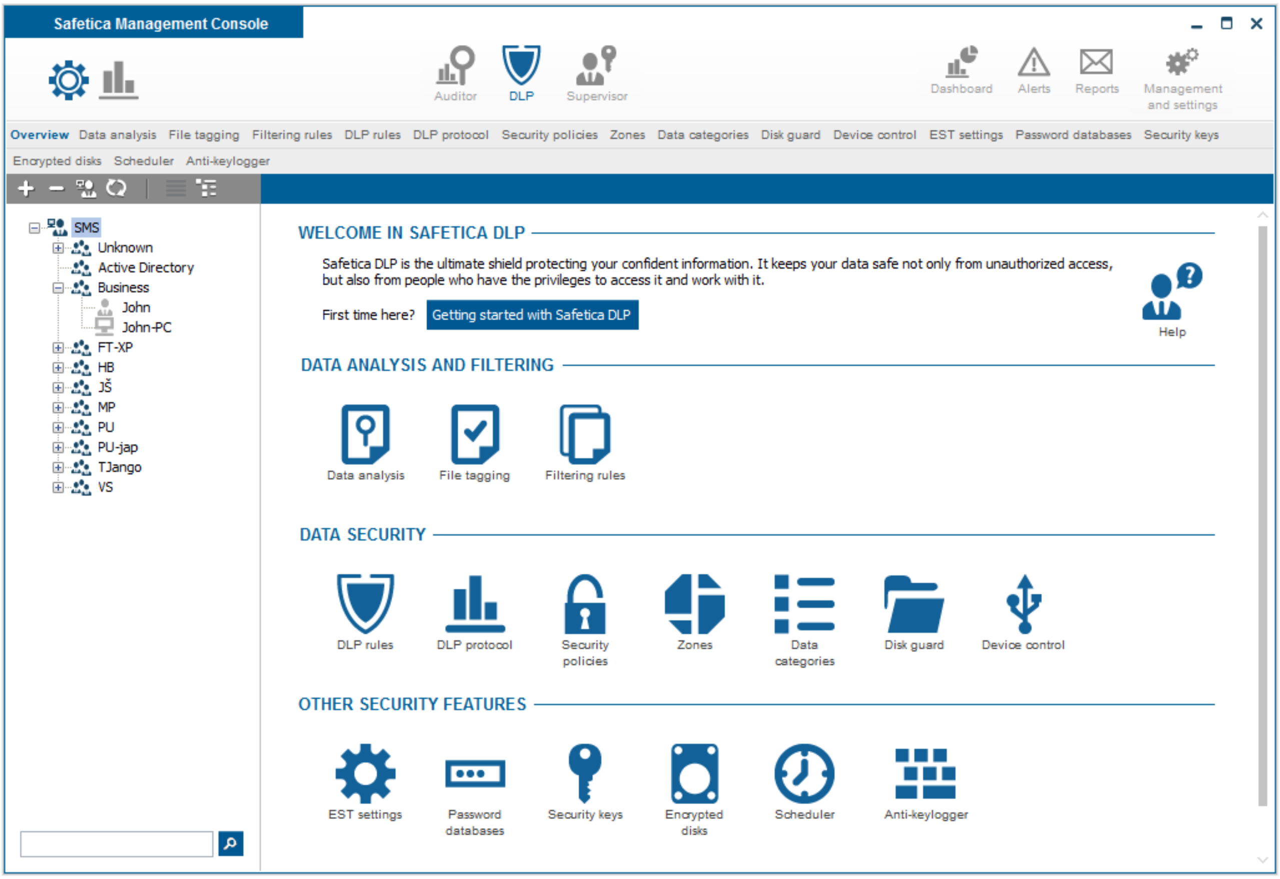


Safetica Auditor automatically reveals any potentially harmful behavior of your employees. It analyzes their activities and warns the management of any imminent danger. Safetica Auditor measures and records employee productivity, detects changes in their behavior and thus allows you to assess the level of risk they present.

First time here? Getting started with Safetica Auditor

2.2 DLP

DLP will protect your company’s sensitive information against misuse by authorized persons and even against third party access. It thus prevents financial losses and damage to your company goodwill. In cooperation with the Auditor, the DLP will protect you from the undesirable activities of your employees long before even any problem appears.



WELCOME IN SAFETICA DLP

Safetica DLP is the ultimate shield protecting your confident information. It keeps your data safe not only from unauthorized access, but also from people who have the privileges to access it and work with it.

First time here? Getting started with Safetica DLP

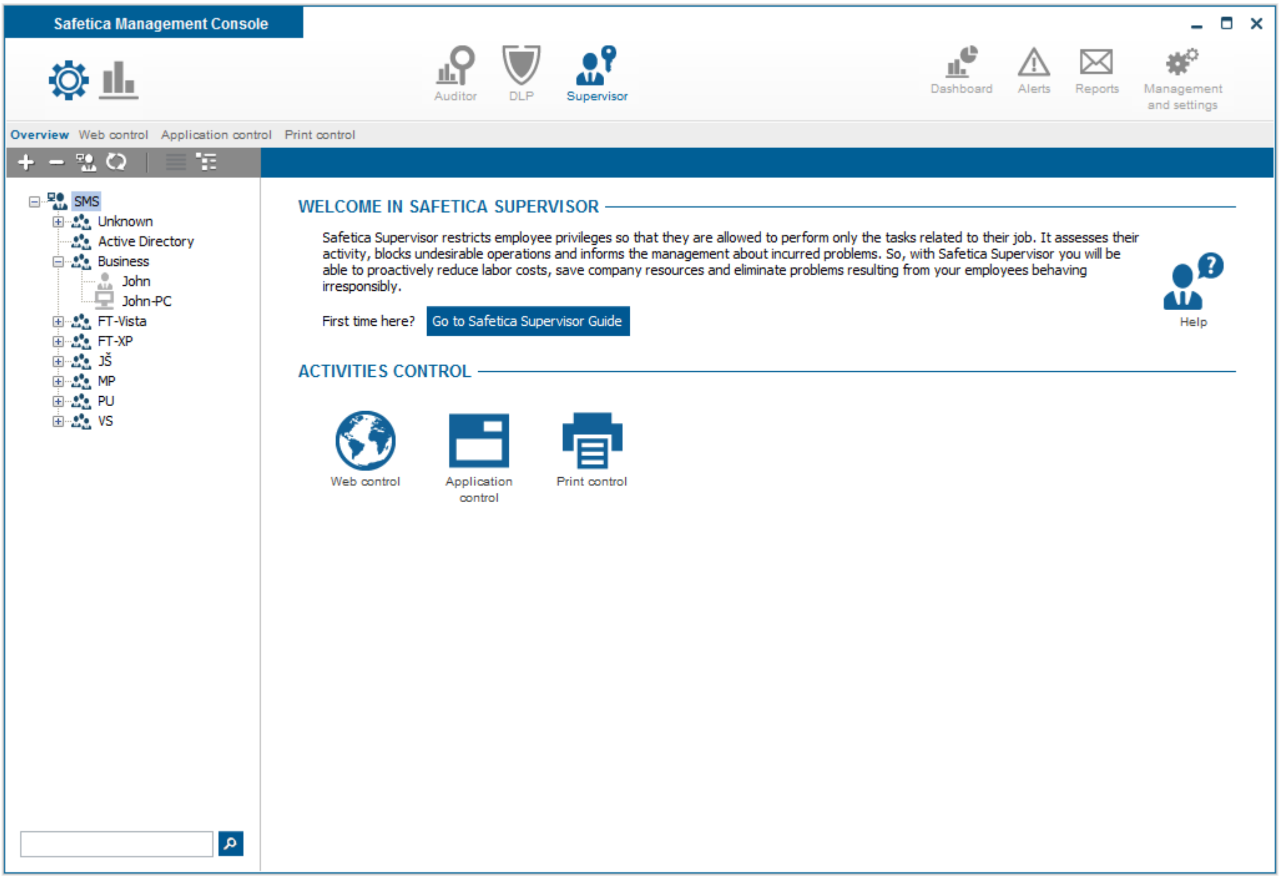
DATA ANALYSIS AND FILTERING

DATA SECURITY

OTHER SECURITY FEATURES

2.3 Supervisor

Supervisor thoroughly controls your employees so that they perform only their job. It evaluates their activity, blocks undesirable activities and informs management on incurred problems. So, with Supervisor you will be able to reduce labor costs, save company finances and eliminate problems resulting from your employees' undesirable activities.



WELCOME IN SAFETICA SUPERVISOR

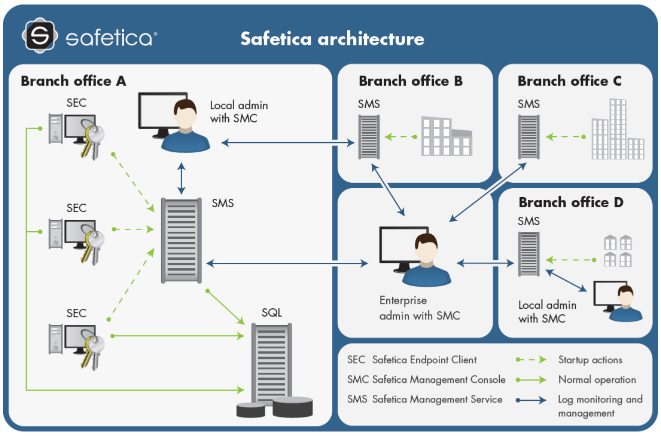
Safetica Supervisor restricts employee privileges so that they are allowed to perform only the tasks related to their job. It assesses their activity, blocks undesirable operations and informs the management about incurred problems. So, with Safetica Supervisor you will be able to proactively reduce labor costs, save company resources and eliminate problems resulting from your employees behaving irresponsibly.

First time here? Go to Safetica Supervisor Guide

ACTIVITIES CONTROL

3 Architecture

Safetica product is based on the client-server architecture. Client application Safetica Endpoint Client (SEC) is running on end stations. This application communicates with Safetica Management Service (SMS) server component. Security managers or administrators use Safetica Management Console (SMC) for remote connection. Data obtained by monitoring individual end stations are stored on the database server.



Each of following parts may be installed on a separate computer.

SMS represents the server part. It runs as a service on the server. More of them may run in one domain thanks to the load distribution using division of the Active Directory tree.

SMC is a management center for setting and controlling client stations (Safetica Endpoint Client), server services (Safetica Management Service) and databases. It also displays outputs of monitoring, statistics and graphs.

SEC represents client part which runs on end stations of all your employees. It is composed of two main parts:

- Safetica Client Service - launches at each start of the operating system as a service and performs monitoring, forcing security policy and communication with database and Safetica Management Service.
- Endpoint Security Tools (only with a valid DLP module license) - user interface with security tools and contextual menu. It can operate in three modes:
  1. Endpoint Security Tools - a mode with user interface
  2. Hidden mode - basic user actions available only from the contextual menu.
  3. Invisible mode - without Endpoint Security Tools

SQL database is the last part and serves for storage of monitoring data and settings. Its part is also a category database with applications, websites and extensions categories. There are differences between Standard and Small installation in usage of database engines.

- *Standard installation:*
  - SEC uses *SQLite* database to temporarily store logs, settings and categories.
  - SMS uses *Microsoft SQL Server platform* for main databases (Settings, Logs, Categories). Microsoft SQL Server must be installed and configured before SMS installation and three databases must be created too.
- Small installation:
  - SEC uses *SQLite* database to temporarily store logs, settings and categories.
  - SMS uses *SQLite* for main databases (Settings, Logs, Categories). Databases are auto-

matically created and configured upon SMS installation and they are on the same computer as SMS.

Data calculator

Data calculator can help you with estimation of capacity demand of SQLite and MS SQL database needed to run Safetica software. By selecting number of users, level of users' activity, screenshot quality and desired modules, you can obtain easily sharable estimates of database capacity requirement.

You can find data calculator on the web page http://calc.safetica.com/.

3.1 Type of installation

Standard installation

Installation for the companies using Microsoft Active Directory. Used usually for networks with 20 or more computers. MS SQL is used for a database. Active Directory is supported.

Small installation

Installation for small networks with less than 20 computers. Does not require Microsoft Active Directory or a server. The database uses SQLite, which is installed and configured automatically during installation. Active Directory is not supported.

4 Installation

4.1 Installation requirements

The following section describes the requirements for individual components of Safetica.

Safetica Management Service

Recommended hardware requirements

- 2.4 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) dual-core processor
- 2GB RAM
- 10GB hard drive space

Software requirements

Large network (Standard installation):

- Operating systems: Windows Server 2003 SP1, 2003 R2, 2008, 2008 R2, 2012 32-bit or 64-bit, with a domain and Active Directory
- Database MS SQL 2008, 2008 R2, 2012 including Express edition and 32-bit or 64-bit

Small network (Small installation):

- MS Windows XP SP2, Vista, 7, 32-bit or 64-bit without a domain and of course server operating systems as for large installation.

Safetica Management Console

Recommended hardware requirements

- 2.4/1.6 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single/dual-core processor

- 1 GB RAM
- 2 GB hard drive space

Minimum hardware requirements

- 1.5 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single-core processor
- 512 MB RAM
- 2 GB of space free on hard drive

Software requirements

Safetica Management Console can be installed anywhere. It supports the following operating systems: MS Windows XP SP3, Vista, 7, 32-bit or 64-bit (installation is also possible on the server operating systems listed in the requirements for the Safetica Management Service).

Safetica Endpoint Client

Recommended hardware requirements

- 2,4/1.6 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single/dual-core processor
- 1GB RAM
- 2GB hard drive space

Software requirements

- Operating systems: MS Windows XP SP3, Vista, 7, 32-bit or 64-bit, MS installer package

Safetica Management Console

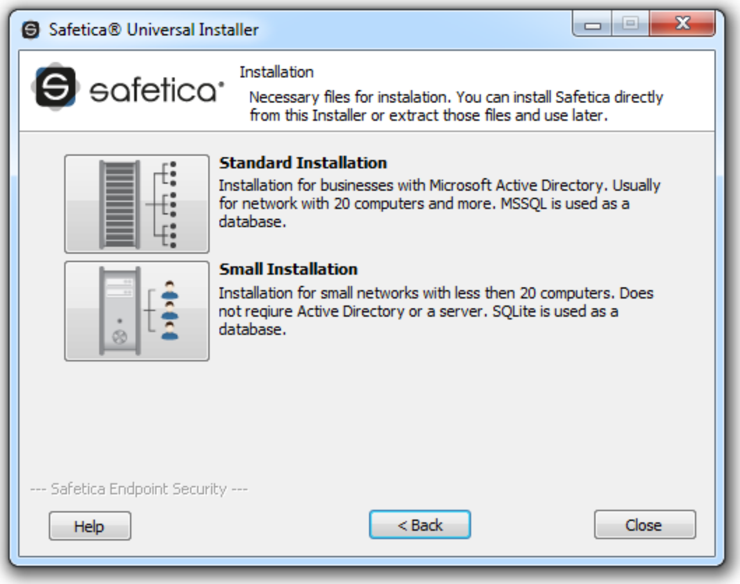
The requirements are the same as for Safetica Endpoint Client, but it could be also installed on server OS: Windows Server 2003 SP1, 2003 R2, 2008, 2008 R2, 2012 32-bit or 64-bit.

4.2 Installation step by step

Installation of Safetica is very easy and uses standard tools. All components necessary for installation are included in the universal installer, which can be free downloaded from www.safetica.com.

Universal installer

The universal installer of Safetica includes all components necessary for successful installation. Safetica Management Console, Safetica Management Service, and Safetica Endpoint Client.


Safetica® Universal Installer

Installation

Necessary files for instalation. You can install Safetica directly from this Installer or extract those files and use later.

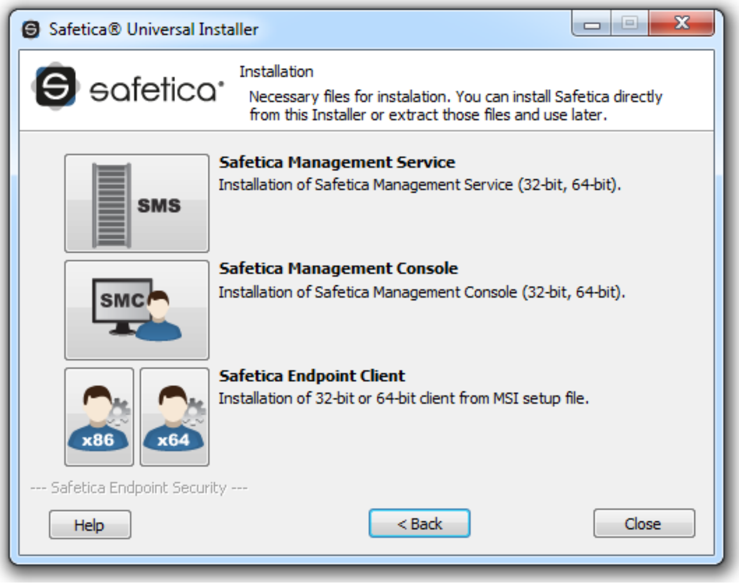
Standard Installation

Installation for businesses with Microsoft Active Directory. Usually for network with 20 computers and more. MSSQL is used as a database.

Small Installation

Installation for small networks with less then 20 computers. Does not reqiure Active Directory or a server. SQLite is used as a database.

--- Safetica Endpoint Security ---


Safetica® Universal Installer

Installation

Necessary files for instalation. You can install Safetica directly from this Installer or extract those files and use later.

Safetica Management Service

Installation of Safetica Management Service (32-bit, 64-bit).

Safetica Management Console

Installation of Safetica Management Console (32-bit, 64-bit).

Safetica Endpoint Client

Installation of 32-bit or 64-bit client from MSI setup file.

--- Safetica Endpoint Security ---

First steps of installation

1. Language selection
2. Confirmation of License terms
3. Start dialog of universal installer - start point of the Safetica installation. Here you can view the complete documentation or proceed in installation.
4. Selection of installation type - this is a very important step in installation Select which installation you want to perform based on size and architecture of your network.

   Standard installation

   Small installation

Further steps vary based on the choice of installation. Proceed to steps in the relevant chapter describing the type of installation, which you want to perform.

4.2.1 Standard installation

After selecting the standard installation you can choose from the installations of the individual Safetica components.

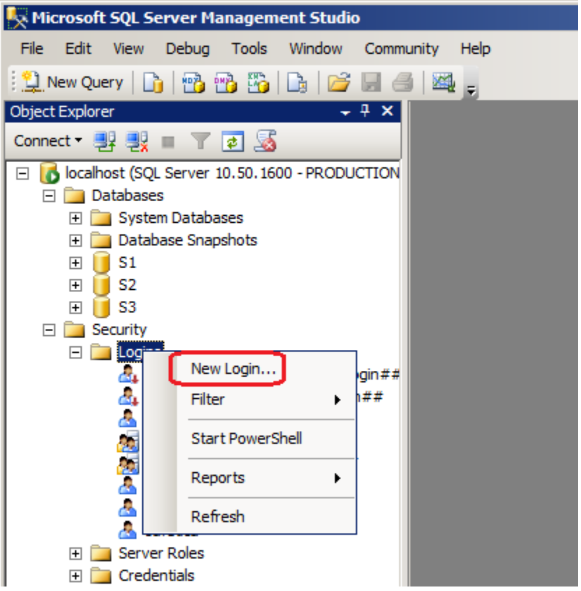
- Installation of Safetica Management Service

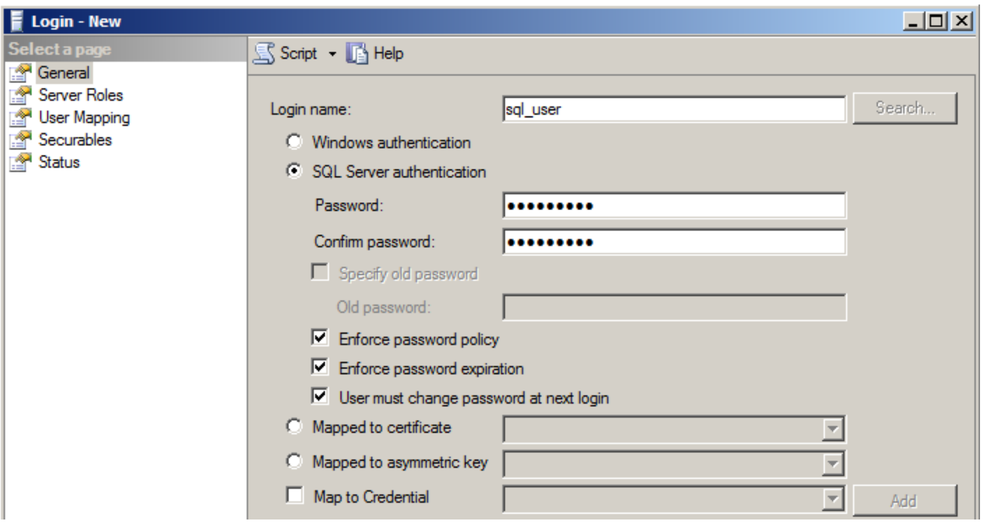
- Installation of Safetica Management Console
- Installation of Safetica Endpoint Client (here you have to select the installer for the right type of the end client station architecture - 64-bit or 32-bit)

The individual components can be installed directly by means of a universal installer or installers of the individual Safetica components extracted from the universal one.

1. Creating SQL server user login in MS SQL

In Microsoft SQL Server create a new user in SQL Server authentication mode with sufficient rights to create databases. Supported Microsoft SQL Servers can be found in the Requirements.





Login name: sql_user

○ Windows authentication

● SQL Server authentication

Password: •••••••••

Confirm password: •••••••••

□ Specify old password

Old password:

☑ Enforce password policy

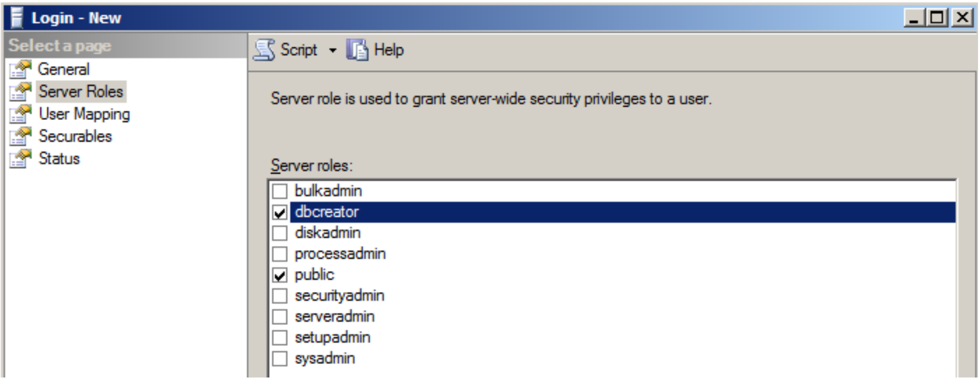
☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential



Server role is used to grant server-wide security privileges to a user.

Server roles:

□ bulkadmin
☑ dbcreator
□ diskadmin
□ processadmin
☑ public
□ securityadmin
□ serveradmin
□ setupadmin
□ sysadmin

2. Installation of Safetica Management Service on server

The first part of the whole integration is installation of Safetica Management Service (SMS) which within one branch provides for interconnection of all parts of Safetica.

The installation is to be performed on the server operation system with the Active Directory domain service.

You do not have to pay much attention to the component installation wizard. The service starts automatically immediately upon installation. To run the check please type "services.msc" in the Run box, the service's name is "Safetica Management Service", and check if it is present and running (and verify the startup type - "Automatically"). The installation of the Safetica Management Service component is now completed.

Install SMS on the servers that will serve one branch.

3. Installation of Safetica Management Console on administration station

The installation is performed through an installation wizard that does not need much attention. It depends on you to whom and on which station you want to install the console. The console can be run on a server as well as on client stations.

4. Distribution of Safetica Endpoint Client on end stations

Safetica Endpoint Client must be installed on the end stations of all employees. The deployment can be performed in several ways.

When installing Safetica Endpoint Client on the end stations you have two options.

Installation from an extracted installer or directly from the universal installer

Manual installation using the universal installer directly or the appropriate MSI package extracted from the universal installer is easily configurable. Perform the installation separately on each client station on which you want Safetica Endpoint Client to run. The installation itself has a form of a classic installation wizard where you do not have to make any important settings. You do not have to pay much attention to the details of this installation.

Before extracting or launching the installer, you will be asked for the initial setting with which the Safetica Endpoint Client will be installed:

- the IP address of the SMS server to which SEC will connect
- Port, on which the SMS runs
- the SEC language
- the setup of SEC process hiding
- the Client mode (see Architecture)

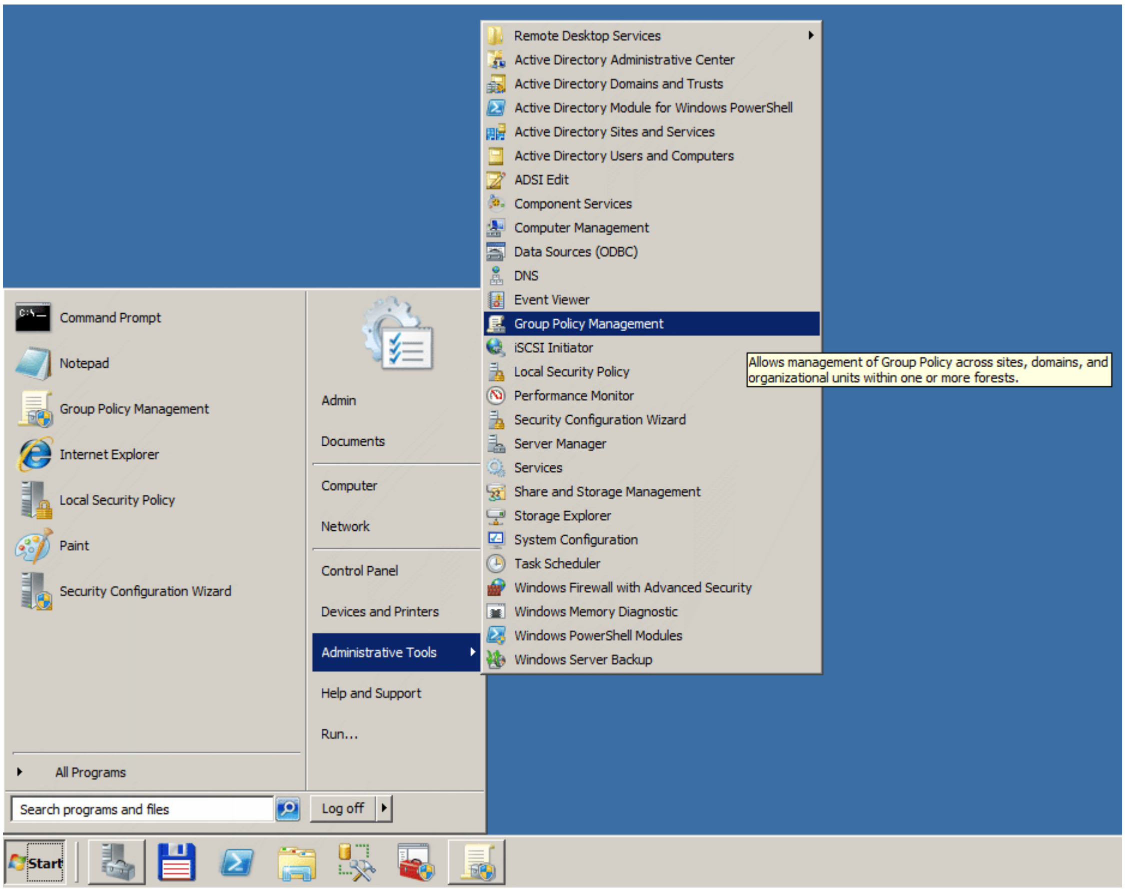
Bulk installation via the Group Policy Object service

The option of bulk installation via the MSI packet and using GPO (Group Policy Object) is a more difficult one. When using this bulk installation you need to extract from the universal package the appropriate MSI package of Safetica Endpoint Client. When performing bulk installation you have two options.

- Assign - following installation the Safetica Endpoint Client component will be automatically installed for selected domain clients without the need of interaction on the part of users.
- Publish - this distribution requires interaction of the user. The required domain clients/groups will be granted free access to installation from the menu *Add/remove programs -> Add new programs*.

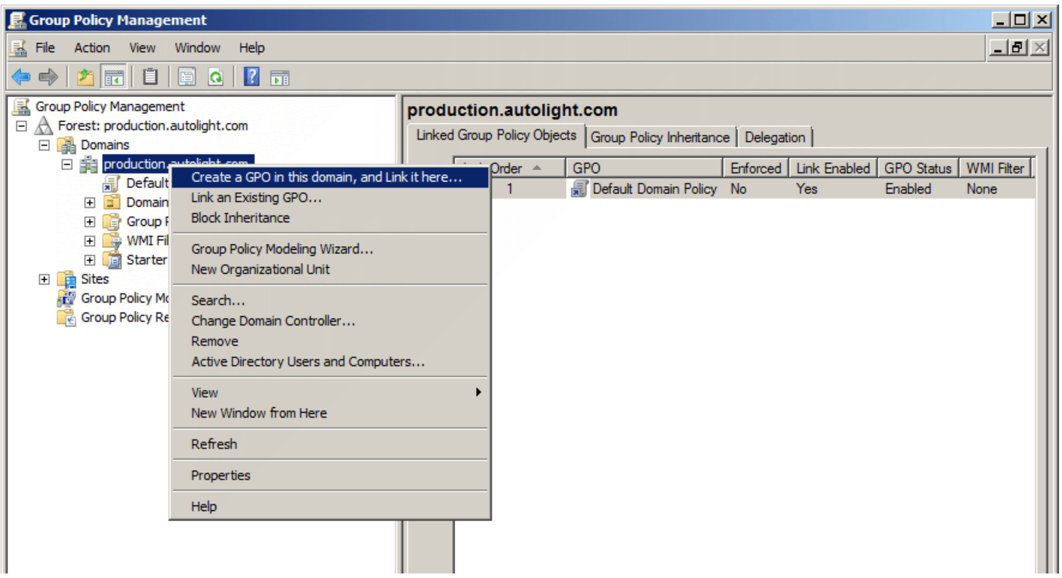
We will further describe only the first kind of installation - assign (The description herein may not always correspond to reality, depending on the version of your server system, the labels may vary.) .Description of bulk installation by means of GPO on Windows Server 2008 R2:

1. Start the universal installer of Safetica.
2. Select *Standard installation.*
3. Select the respective client according to the architecture (x86 or x64).
4. Export the MSI package onto a shared disk or into a shared folder in the company network and set the access rights (it is enough to set reading and launching rights) to this folder. These rights will be binding for the desired group of users (by default, it is the group of Domain Users and Domain Computers).
5. Access the server where you have installed SEC remotely through GPO. Go to *Management tools -> Management of group policies.*



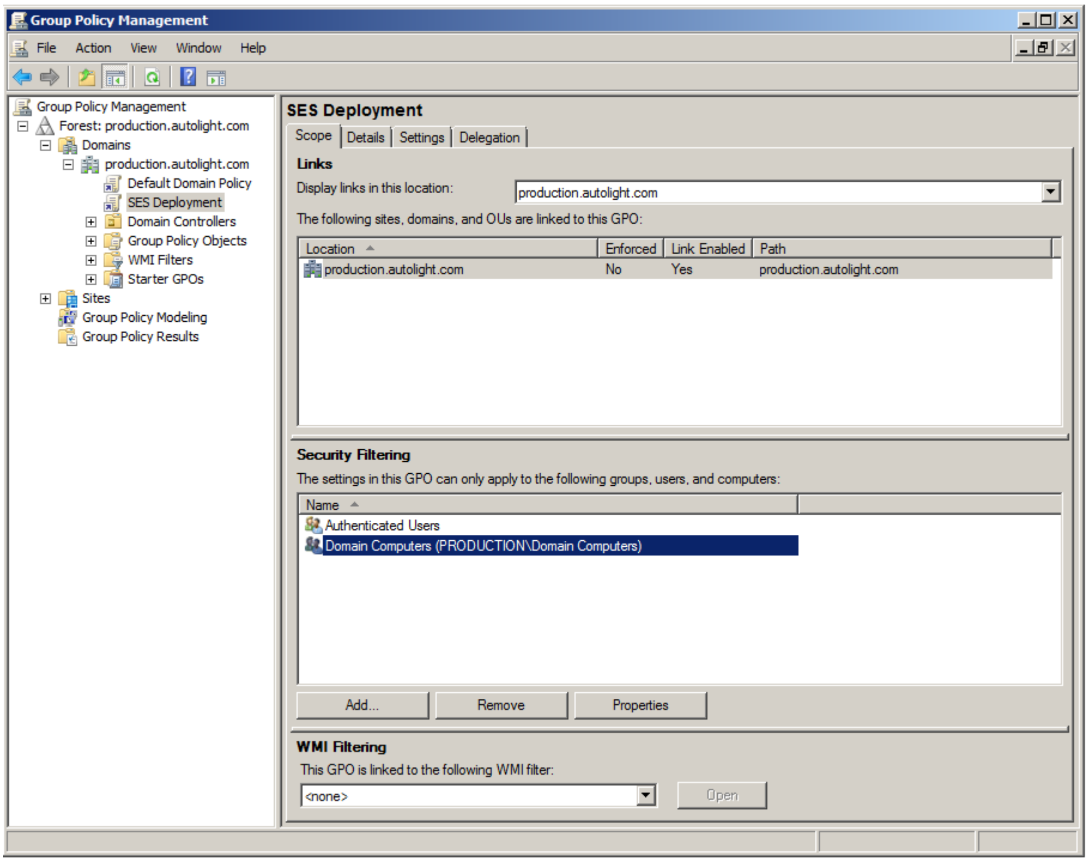
Allows management of Group Policy across sites, domains, and organizational units within one or more forests.

6. Click with the right mouse button on the organizational unit, on which you wish to deploy SES and select *Create new group policies object in this domain and interconnect it...*



Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Default Domain Policy	No	Yes	Enabled	None

7. Give a name to the new project (e.g. SES Deployment).
8. Select the new object on the right side of the window (Tab *Scope*) add the group *Domain Computers* to the already existing group *Authenticated Users*



SES Deployment

Links

Display links in this location: production.autolight.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
production.autolight.com	No	Yes	production.autolight.com

Security Filtering

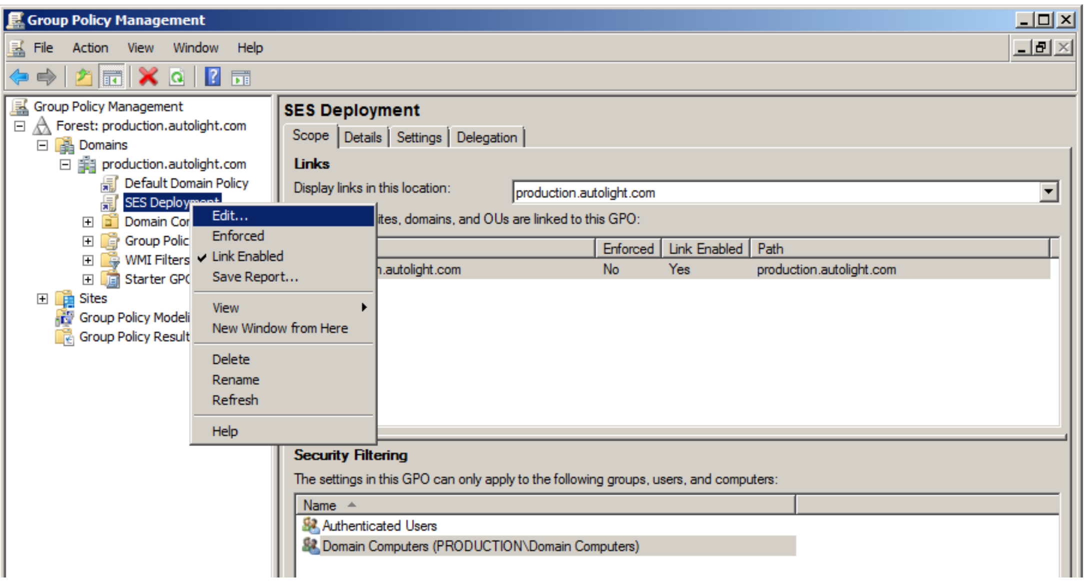
The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users
Domain Computers (PRODUCTION\Domain Computers)

WMI Filtering

This GPO is linked to the following WMI filter: <none>

9. Select your newly created group policy and with the right mouse button select *Edit.*



SES Deployment

Links

Display links in this location: production.autolight.com

ites, domains, and OUs are linked to this GPO:

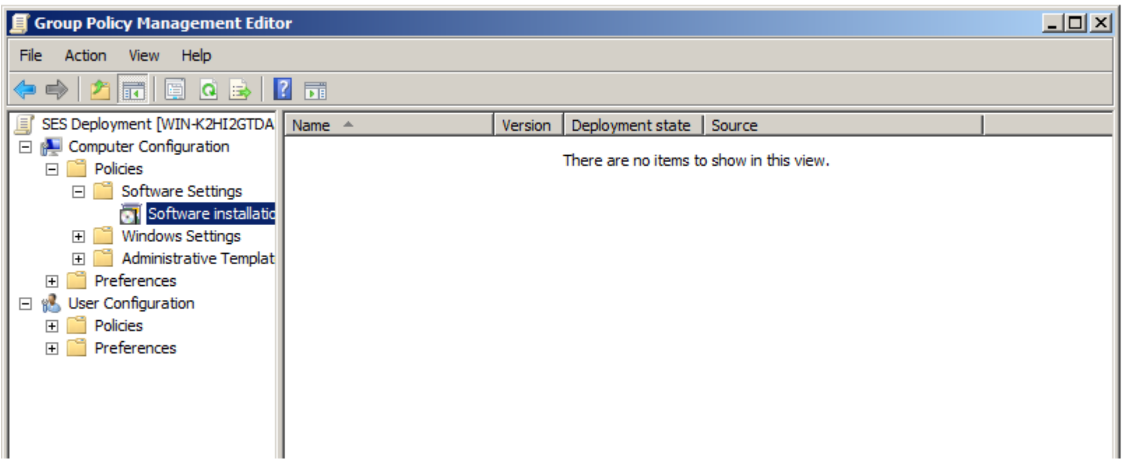
	Enforced	Link Enabled	Path
ı.autolight.com	No	Yes	production.autolight.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

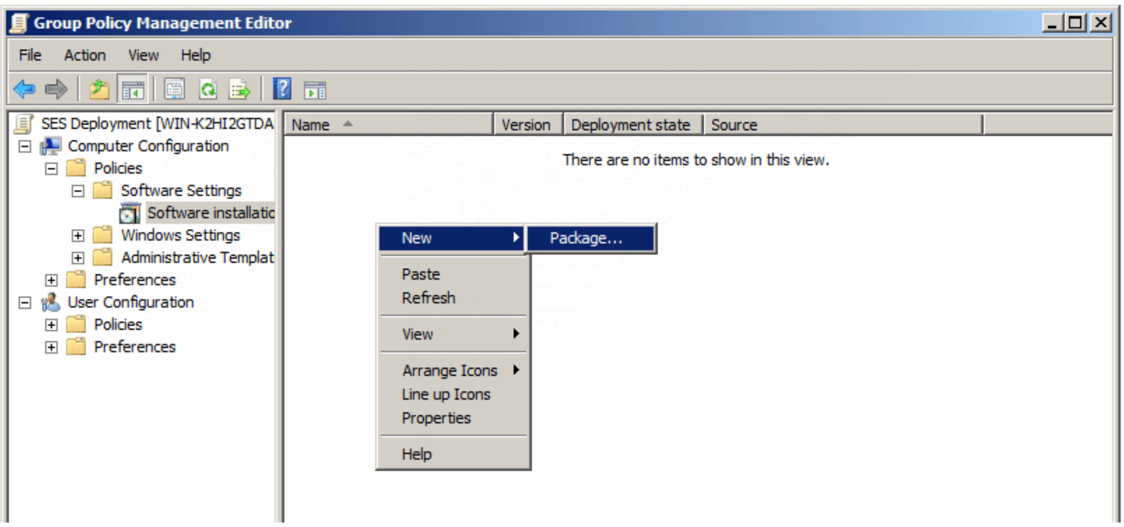
Name
Authenticated Users
Domain Computers (PRODUCTION\Domain Computers)

10. In the pop-up window choose *Computer setup -> Policies -> Software settings* and click on *Software installation.*



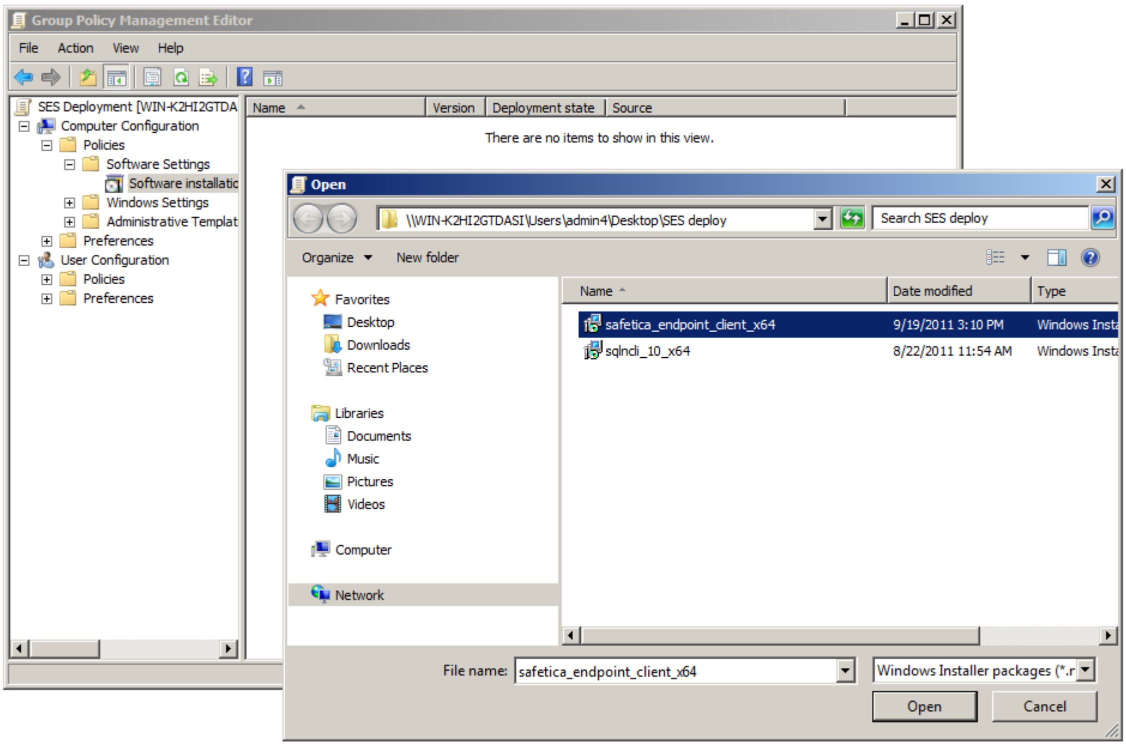
There are no items to show in this view.

11. With the right mouse button, click on the window in which software is listed and select *New item -> Package..*



There are no items to show in this view.

12. In the dialogue box of the msi package choose the shared network files into which you have copied the MSI package and SEC, and select the package.



There are no items to show in this view.

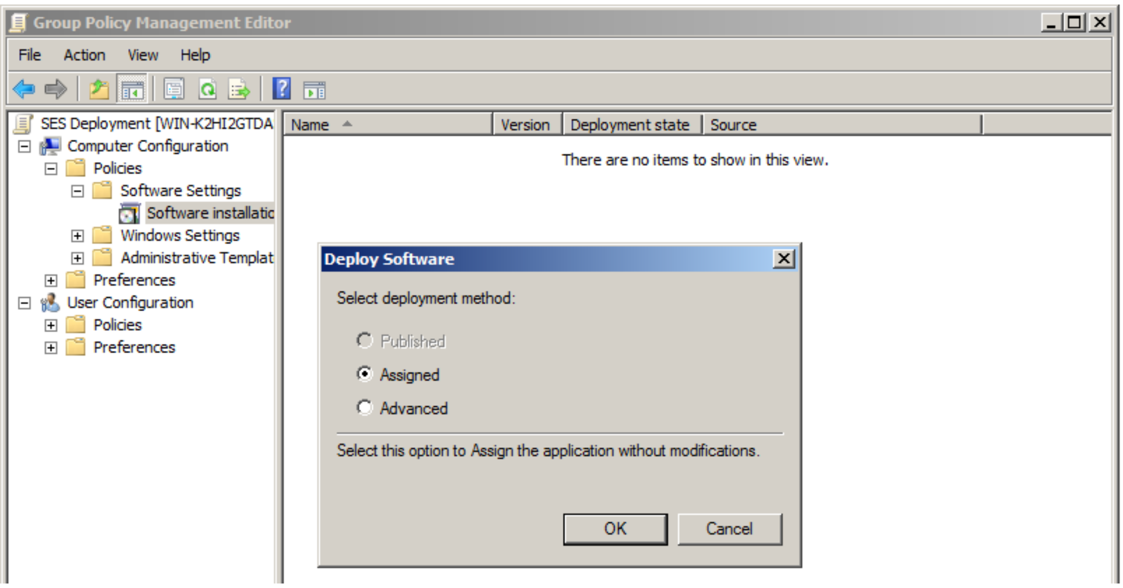
\\WIN-K2HI2GTDASI\Users\admin4\Desktop\SES deploy

Name	Date modified	Type
safetica_endpoint_client_x64	9/19/2011 3:10 PM	Windows Insta
sqlncli_10_x64	8/22/2011 11:54 AM	Windows Insta

File name: safetica_endpoint_client_x64

Windows Installer packages (*.r

13. In the next dialogue window, select *Assigned* and confirm.



There are no items to show in this view.

Deploy Software

Select deployment method:

○ Published

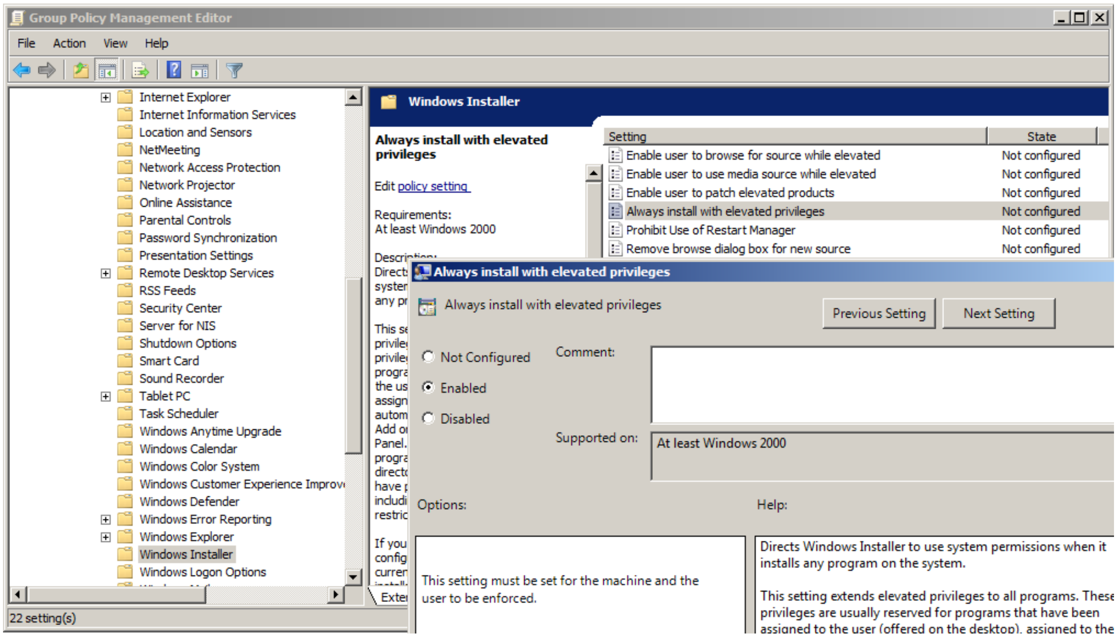
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

Warning! When installing from the 32-bit MSI package, it is necessary to disable installation onto 64-bit systems. You can do this by selecting the deployment method in *Advanced -> Deployment -> Extended -> Specify ->* and uncheck *Make this 32bit version of X86 application available for computers with the Win64 architecture* .

14. Next, open *Computer setup -> Management templates -> Windows components -> Windows Installer.* There you should find the item: *Always install with elevated privileges*. Choose Enabled. By doing this you will ensure that Safetica Endpoint Client will be installed to end stations successfully and smoothly.



Always install with elevated privileges

Requirements:
At least Windows 2000

Setting	State
Enable user to browse for source while elevated	Not configured
Enable user to use media source while elevated	Not configured
Enable user to patch elevated products	Not configured
Always install with elevated privileges	Not configured
Prohibit Use of Restart Manager	Not configured
Remove browse dialog box for new source	Not configured

Always install with elevated privileges

Always install with elevated privileges

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

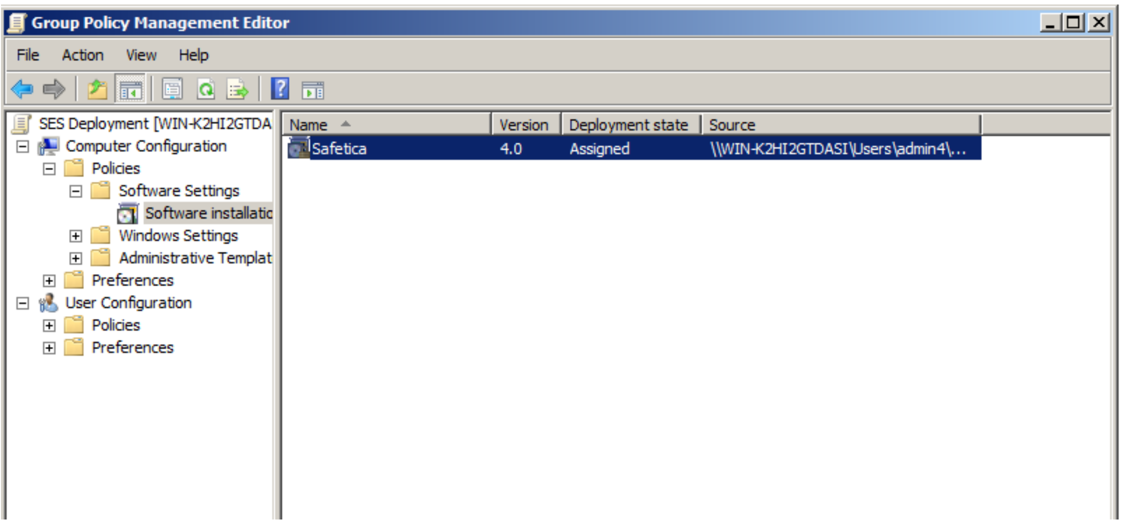
This setting must be set for the machine and the user to be enforced.

Help:

Directs Windows Installer to use system permissions when it installs any program on the system.

This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the

15. After the client stations for which the chosen policy was designed have been restarted, SEC will automatically start to install onto them.



SES Deployment [WIN-K2HI2GTDA
- Computer Configuration
  - Policies
    - Software Settings
      - Software installatio
    - Windows Settings
    - Administrative Templat
  - Preferences
- User Configuration
  - Policies
  - Preferences

Name	Version	Deployment state	Source
Safetica	4.0	Assigned	\\WIN-K2HI2GTDASI\Users\admin4\...

16. The policy configuration is now complete and client distribution is ready. Safetica Endpoint Client will be installed immediately after the client computer starts.

Note

Safetica supports deployment also in a computer network without a domain server. Therefore, it is necessary to analyze the network in your company first and schedule on which computers you will install the individual components of Safetica, with respect to the requirements of the administrator of your network and the corporate network policies .

It is also necessary to provide for exceptions in your corporate Firewall, or Anti Virus for the following component processes and their ports:

- Safetica Endpoint Client - STCService.exe, STMonitor.exe, STUserApp.exe, Safetica.exe, STPCLock.exe
- Safetica Management Service - STAService.exe
- Safetica Management Console - STAConsole.exe

SES components communicate by default on following ports:

SEC communicates with SMS on port 4438. You can change this port number by using the command STAService.exe -clientport <new port number>on a computer with SMS.

SMC communicates with SMS on port 4441. You can change this port number by using the command STAService.exe -adminport <new port number>on a computer with SMS.

SMS, SEC and SMC communicate with the SQL database on port 1433. You can change this port number in the SQL database.

4.2.2 Small installation

After selecting the small installation you can choose from installations of the individual Safetica components.

- Installation of Safetica Management Service
- Installation of Safetica Management Console
- Installation of Safetica Endpoint Client (here you have to select the installer for the right type of the end client station architecture - **64-bit** or **32-bit**)

The individual components can be installed directly by means of a universal installer, or installers of the individual Safetica components extracted from the universal one.

1. Installation of Safetica Management Service on server

The first part of the whole integration is installation of Safetica Management Service (SMS), which within one branch provides for interconnection of all parts of Safetica.

The installation is to be performed on the server operation system with the Active Directory domain service.

You do not have to pay much attention to the Component installation wizard. The service starts automatically immediately upon installation. To run the check please type "services.msc" in the Run box, the service's name is "Safetica Management Service", and check if it is present and running (and verify the startup type - "Automatically"). The installation of the Safetica Management Service component is now completed.

Install SMS on the servers that will serve one branch.

2. Installation of Safetica Management Console on administration station

The installation is performed through an installation wizard that does not need much attention. It depends on you to whom and on which station you want to install the console. The console can be run on server as well as on client stations.

3. Installation of Safetica Endpoint Client on end stations

You can perform the installation using an universal installer or the appropriate MSI package extracted from the universal installer. Perform the installation separately on each client station on which you want the Safetica Endpoint Client to run. The installation itself has a form of a classic installation wizard where you do not have to make any important settings.

The installation itself is in the form of a traditional installation guide, where the most important parts are network mode activation, IP address setup of a computer with the SMS and port number on which the SMS runs. Here you can also turn off the network mode, which will install only the Endpoint Security Tools itself without the possibility of monitoring or other security policy enforcement.

Note

In order to secure trouble-free running of Safetica it is also necessary to provide for exceptions in your corporate Firewall, or Anti Virus for the following component processes and their ports:

- Safetica Endpoint Client - STCService.exe, STMonitor.exe, STUserApp.exe, Safetica.exe, STPCLock.exe
- Safetica Management Service - STAService.exe
- Safetica Management Console - STAConsole.exe

SES components communicate by default on following ports:

SEC communicates with SMS on port 4438. You can change this port number by using the command STAService.exe -clientport <new port number>on a computer with SMS.

SMC communicates with SMS on port 4441. You can change this port number by using the command STAService.exe -adminport <new port number>on a computer with SMS.

SMS, SEC and SMC communicate with the SQL database on port 1433. You can change this port number in the SQL database.

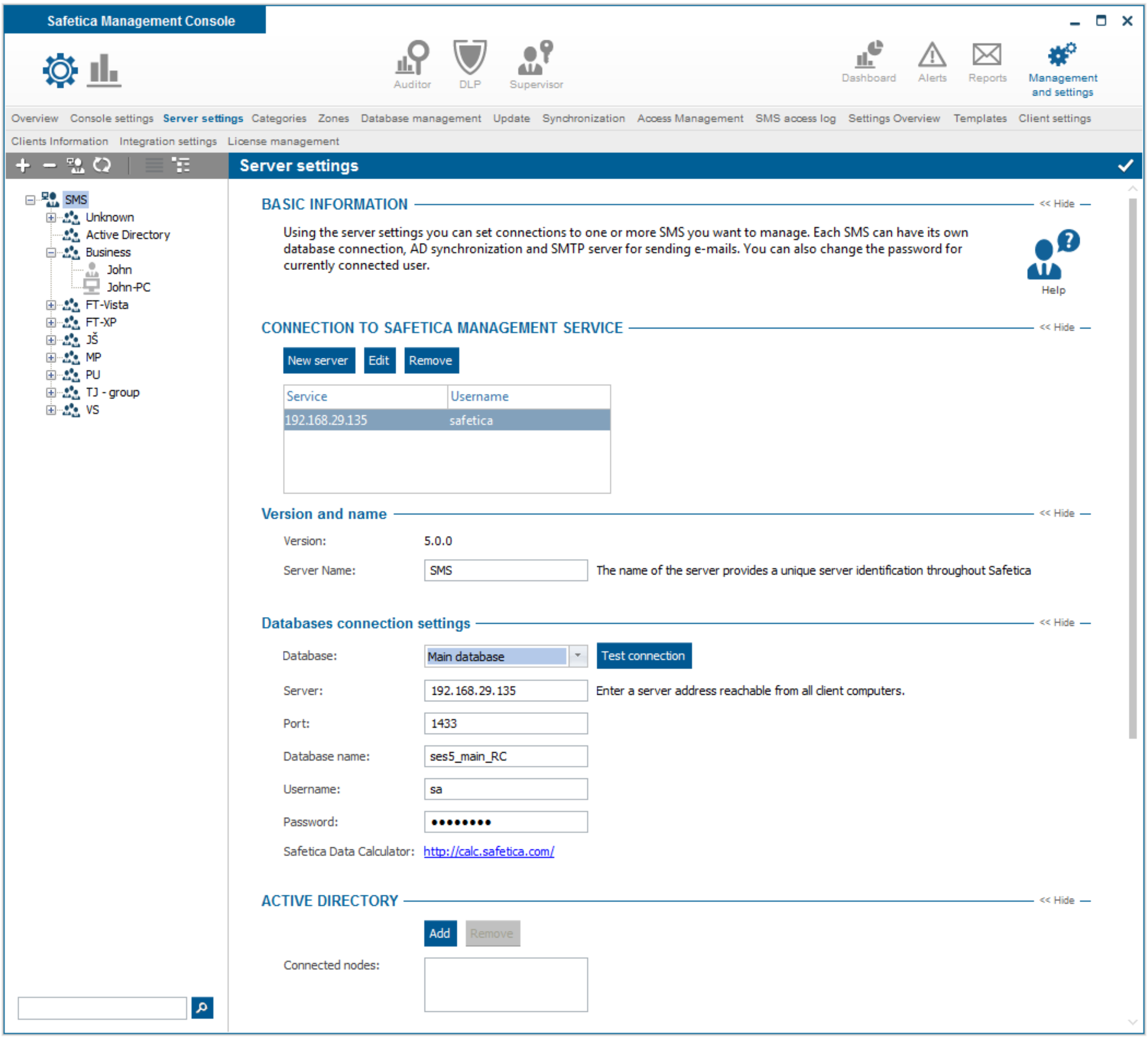
4.3 First launch and setup

After the successful installation of all components of Safetica, it is necessary to setup the whole system properly. All administration and configuration is performed via the Safetica Management Console.

Please launch the Safetica Management Console (SMC).

4.3.1 Configuration of SMS

1. Start up SMC and enter a new access password for the console.
2. Connect SMC *Management and settings -> Server settings* to the relevant server component of SMS by providing the default credentials – login name: *safetica*; password: *safetica*.



Server settings

BASIC INFORMATION

Using the server settings you can set connections to one or more SMS you want to manage. Each SMS can have its own database connection, AD synchronization and SMTP server for sending e-mails. You can also change the password for currently connected user.

CONNECTION TO SAFETICA MANAGEMENT SERVICE

New server | Edit | Remove

Service	Username
192.168.29.135	safetica

Version and name

Version: 5.0.0

Server Name: SMS — The name of the server provides a unique server identification throughout Safetica

Databases connection settings

Database: Main database — Test connection

Server: 192.168.29.135 — Enter a server address reachable from all client computers.

Port: 1433

Database name: ses5_main_RC

Username: sa

Password: ••••••••

Safetica Data Calculator: http://calc.safetica.com/

ACTIVE DIRECTORY

Add | Remove

Connected nodes:

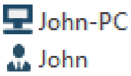
3. Configure the login information for the three Microsoft SQL Server databases (use SQL Authentication login with rights to create databases). Creation and initialization of these databases will be done automatically after confirming the settings dialog.
4. Optionally, run synchronization with Active Directory. This can be done by selecting the appropriate organizational unit in *Management and settings -> Server Settings -> Active Directory*. Users and computers from this organizational unit will be loaded into the *ad* group in the user tree.
5. Use SMC to update the database of categories. To do this, go to *Management and settings -> Categories*.
6. Change the default password for the default SMS account (*safetica*). To do this, go to *Management and settings -> Server Settings -> Password settings*. Select the appropriate server, and change your password (you must be logged on to the server with your *safetica* account to be able to do this).
7. Change your password for the local administration of Safetica Endpoint Client (SEC) – see Protection against unauthorized manipulation with Safetica Endpoint Client. As before, the default password is *safetica*.

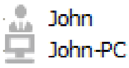
8. If you have a license number, type it into *Management and settings -> License Manager*. The license is only applied to Safetica Endpoint Clients. Safetica functions will be activated after you have assigned the appropriate module license to the client. This can be done after you install and connect the client to the server, again in the same view.

4.3.2 After installation

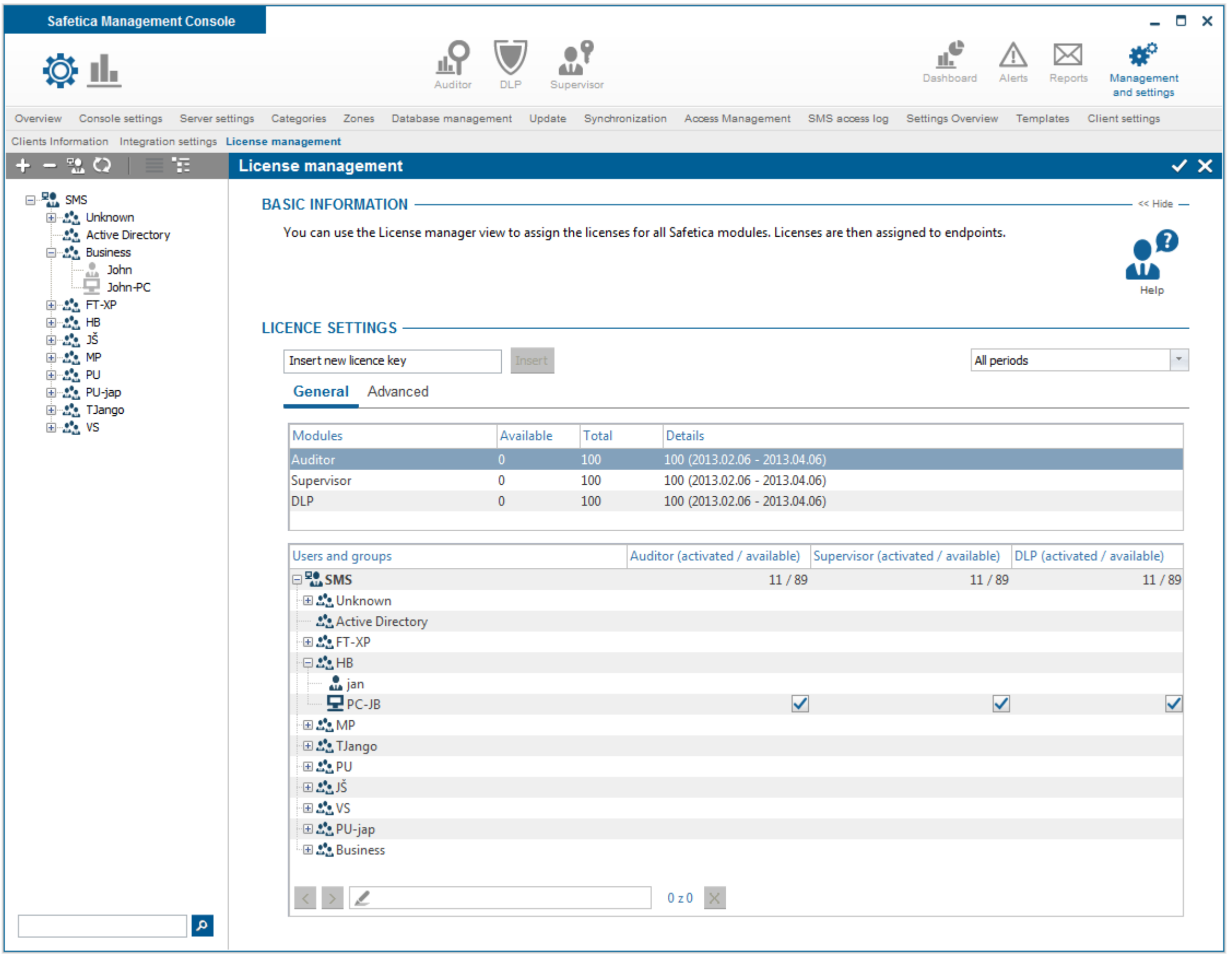
Once you have installed all Safetica components, you are left with just a few final steps to take before you can start using Safetica.

1. First, verify that all Safetica Endpoint Clients (SEC) are connected to the server Safetica Management Server (SMS). In the user tree, both users and computers will be shown in color.

   o 
   John-PC
   John
   SEC is online and connected to SMS

   o 
   John
   John-PC
   SEC is offline and not connected to SMS

2. Use the License Manager to assign licenses for relevant modules to clients. Each computer and module will show a check mark if their license has been successfully assigned. Without assigned licenses, module functions will not be active.



License management

BASIC INFORMATION

You can use the License manager view to assign the licenses for all Safetica modules. Licenses are then assigned to endpoints.

LICENCE SETTINGS

Insert new licence key | Insert | All periods

General | Advanced

Modules	Available	Total	Details
Auditor	0	100	100 (2013.02.06 - 2013.04.06)
Supervisor	0	100	100 (2013.02.06 - 2013.04.06)
DLP	0	100	100 (2013.02.06 - 2013.04.06)

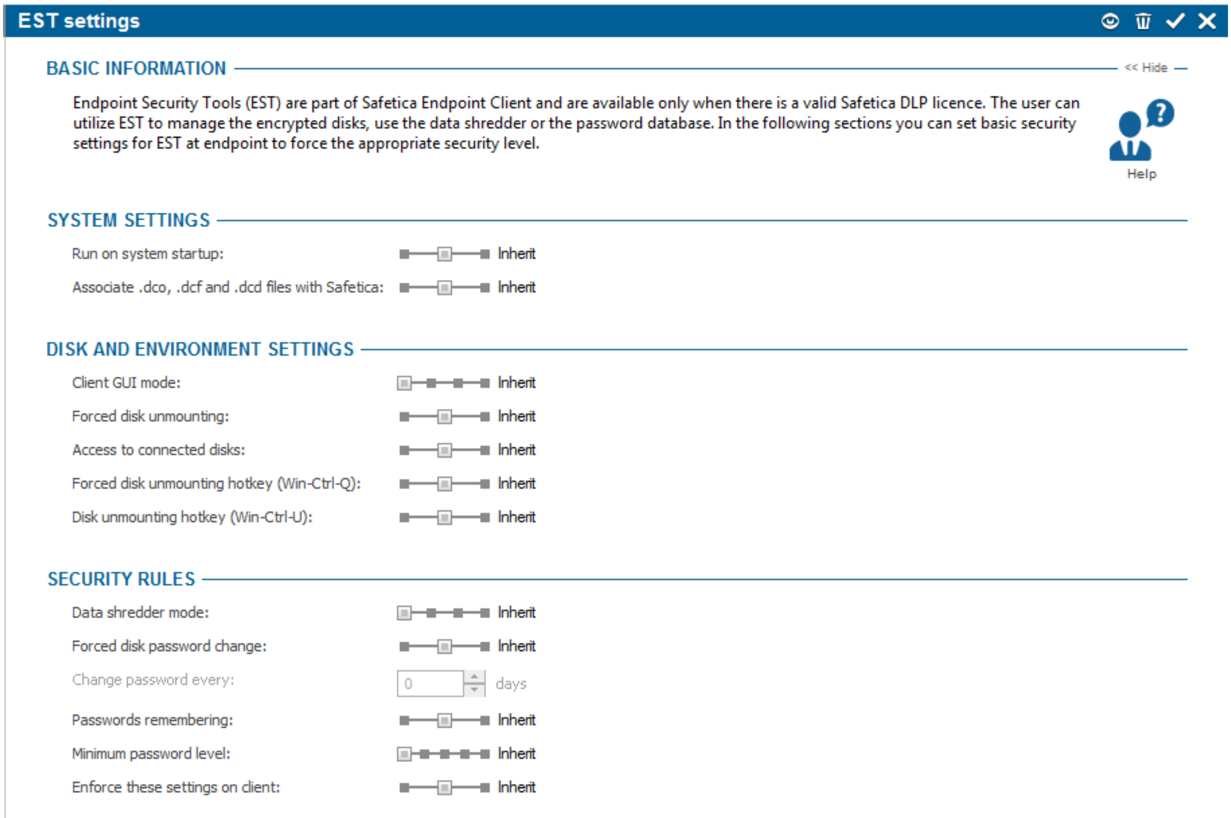
Users and groups	Auditor (activated / available)	Supervisor (activated / available)	DLP (activated / available)
SMS	11 / 89	11 / 89	11 / 89
Unknown			
Active Directory			
FT-XP			
HB			
jan			
PC-JB	☑	☑	☑
MP			
TJango			
PU			
JŠ			
VS			
PU-jap			
Business			

0 z 0

3. If you have assigned a license to the DLP module, select Client GUI mode. By default, your employees can access functions of the Endpoint Security Tools (Normal mode). You can choose from three modes (DLP -> Endpoint Security Tools settings -> Client GUI mode:

   o *Normal* – an Endpoint Security Tools user interface with security tools and a context menu.

- *Tray only* – users can only access basic functions available from the context menu. No user interface.
- *Invisible* – users can access neither context menu functions nor Endpoint Security Tools functions.



EST settings

BASIC INFORMATION

Endpoint Security Tools (EST) are part of Safetica Endpoint Client and are available only when there is a valid Safetica DLP licence. The user can utilize EST to manage the encrypted disks, use the data shredder or the password database. In the following sections you can set basic security settings for EST at endpoint to force the appropriate security level.

SYSTEM SETTINGS

Run on system startup:	Inherit
Associate .dco, .dcf and .dcd files with Safetica:	Inherit

DISK AND ENVIRONMENT SETTINGS

Client GUI mode:	Inherit
Forced disk unmounting:	Inherit
Access to connected disks:	Inherit
Forced disk unmounting hotkey (Win-Ctrl-Q):	Inherit
Disk unmounting hotkey (Win-Ctrl-U):	Inherit

SECURITY RULES

Data shredder mode:	Inherit
Forced disk password change:	Inherit
Change password every:	0 days
Passwords remembering:	Inherit
Minimum password level:	Inherit
Enforce these settings on client:	Inherit

Try activating some of the functions (e.g., *Application monitoring*) to see if they work properly and are collecting data.

At this point, your Safetica is now ready to use.

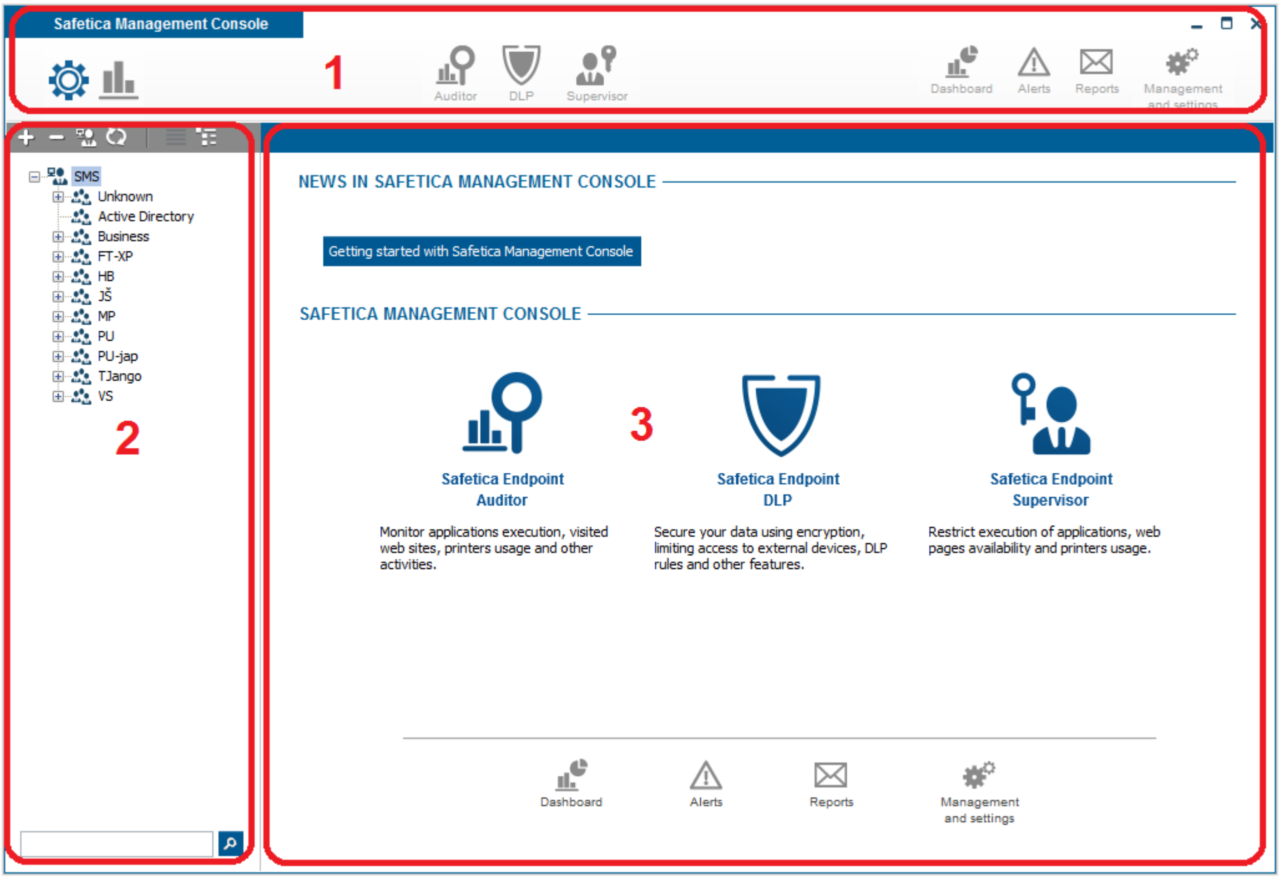
5 Safetica Management Console

Safetica Management Console is a management center serving for setting and controlling client stations (Safetica Endpoint Client), server services (Safetica Management Service) and databases.
It also displays outputs of monitoring, statistics and graphs. Display and setting options in individual modules and functions of Safetica depend on which user account is used to connect to individual Safetica Management Services from the console. User account administration for connecting to the server service can be found in *Access management*.

The Safetica Management Console can run anywhere you have a connection to server services. The number of console installations and number of its users are not limited by the license.

5.1 User interface

After launching Safetica Management Console (SMC) you will see the following interface.



NEWS IN SAFETICA MANAGEMENT CONSOLE

SAFETICA MANAGEMENT CONSOLE

Safetica Endpoint Auditor

Monitor applications execution, visited web sites, printers usage and other activities.

Safetica Endpoint DLP

Secure your data using encryption, limiting access to external devices, DLP rules and other features.

Safetica Endpoint Supervisor

Restrict execution of applications, web pages availability and printers usage.

1. Main menu

On the left you see the console mode switcher. The switcher allows you to change the modes available for the console.

- Visualization mode - This mode allows you to display and overview data obtained through monitoring, summaries, graphs, logs of blocked entries and logs of your employees' activities for the individual functions of Safetica.
- Settings mode - This mode allows you to configure the behavior of individual functions and modules. This does not include configuration of the console itself.

The middle area contains icons used to switch between the three main modules Safetica

- Auditor
- DLP
- Supervisor

The right side contains icons which may be used to view summaries, license settings, alerts, reports, accesses, templates and the settings of the console itself:

- Dashboard – a graphical view of the data obtained via monitoring for all enabled module functions.
- Alerts – automatic alert settings
- Reports – settings for sending regular reports and summaries
- Management and settings – management and settings of SEC, SMC a SMS

Switchers for individual module functions can be found under the upper toolbar with the console controls. These switchers change based on which module you are currently in. (Auditor, Safetica Endpoint DLP, Supervisor).

2. User tree

The user tree is located on the left side of the console under the right bar. It contains a list of all users, computers and their groups divided into the individual branches they belong to. Here branch means the Safetica Management Service together with a database and a connected client station (Safetica Endpoint Client). You can set a new connection to the branch in the *Main menu -> Management and settings -> Server settings*.

You will also find the search field and other controls of the list above the user tree itself.

If a user or computer are grey, it means that they are currently off-line. All settings that you set concerning those users or computers will only be evident when the user or computer are on-line again.

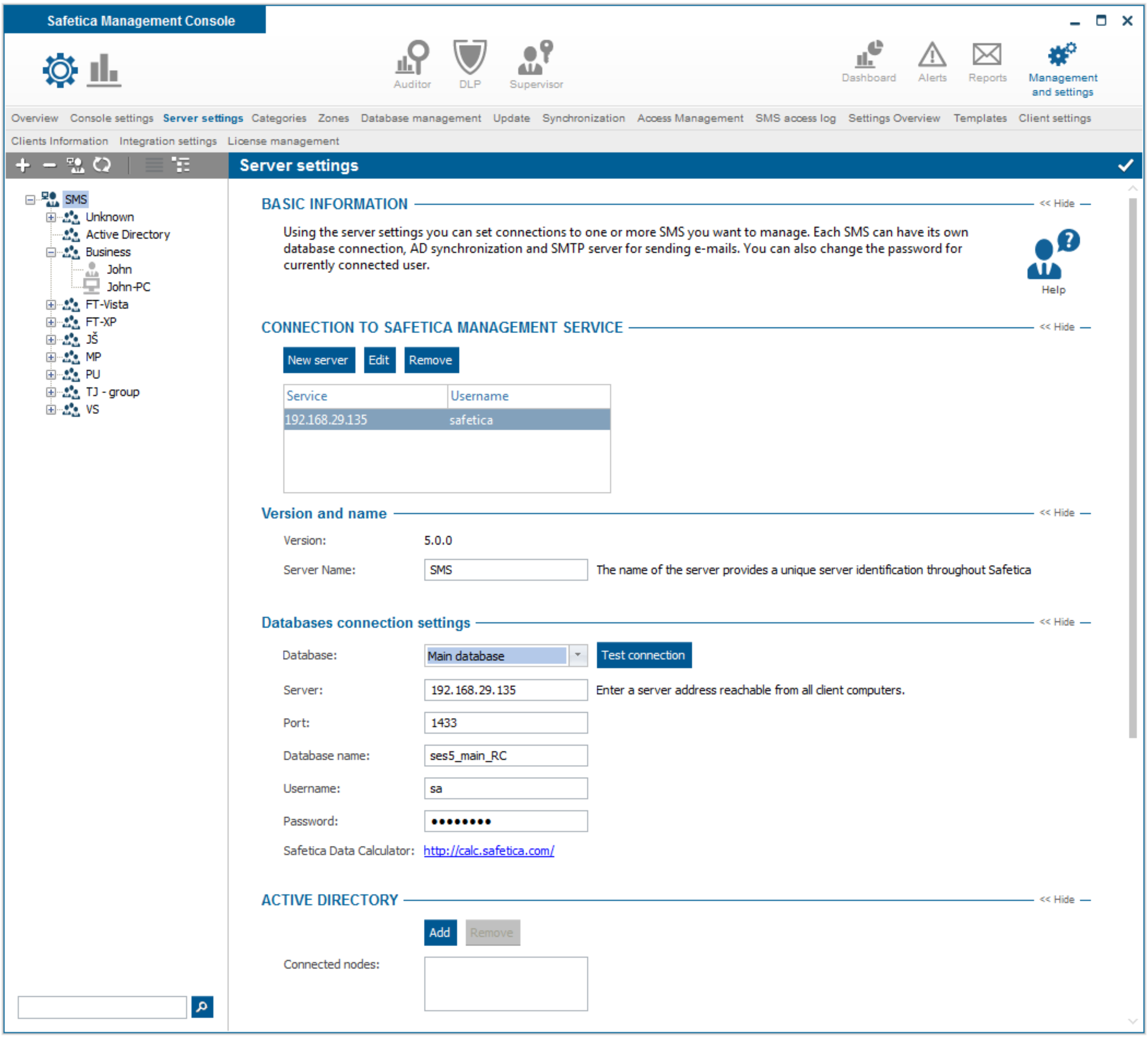
3. View

The display area, also called the view area, is used for data visualization and changing the settings for individual functions. The contents of the view area change based on which function you are currently browsing and your current mode (settings, visualization etc.).

You can switch over individual module functions, select some module in the main menu to display its list of functions, and then move a function to the view area by clicking on its name.

5.2 Connection of SMC to SMS

To connect SMC to new SMS go to *Management and settings -> Server settings*.



Server settings

BASIC INFORMATION

Using the server settings you can set connections to one or more SMS you want to manage. Each SMS can have its own database connection, AD synchronization and SMTP server for sending e-mails. You can also change the password for currently connected user.

CONNECTION TO SAFETICA MANAGEMENT SERVICE

Service	Username
192.168.29.135	safetica

Version and name

Version: 5.0.0

Server Name: SMS The name of the server provides a unique server identification throughout Safetica

Databases connection settings

Database: Main database

Server: 192.168.29.135 Enter a server address reachable from all client computers.

Port: 1433

Database name: ses5_main_RC

Username: sa

Password: ••••••••

Safetica Data Calculator: http://calc.safetica.com/

ACTIVE DIRECTORY

Connected nodes:

Connect SMC to new SMS

To connect SMC to new SMS click on *New server* button.

1. Enter the following information:
   - *Server* – IP address or name of the computer where the SMS you want to connect to is running.
   - *Port* – enter port number of SMS for SMC connection. Default port number is *4441.*
   - *Username* and *Password* – enter login credentials of the SMS user. SMS user accounts are created in Access management. Default service account is *safetica* with password *safetica*.
2. Confirm dialog by *OK* button. During the connection attempt you will also be asked to confirm the server footprint. Press *Yes* button if you want to connect. New SMS will be added into the list.

5.3 Module and functions setting

In order to set the functions of the individual modules you have to switch the console to the setting mode first. You can enter to the settings mode by clicking on ⚙ button in the upper left corner of SMC.

Then click on the required module (Auditor, DLP, Supervisor) to the rightbeside the switch and the list of its functions displays in the main menu.

By clicking on a function you can display the options of its settings in the view.

The setting that you choose in the view of the function is assigned only to users, groups or computers that you have highlighted in the user tree. To apply the settings you have to save the changes using the ✓ or you can cancel the changes you have made by ✖ in the upper right corner.

Setting mode

You set following modes for almost every function:

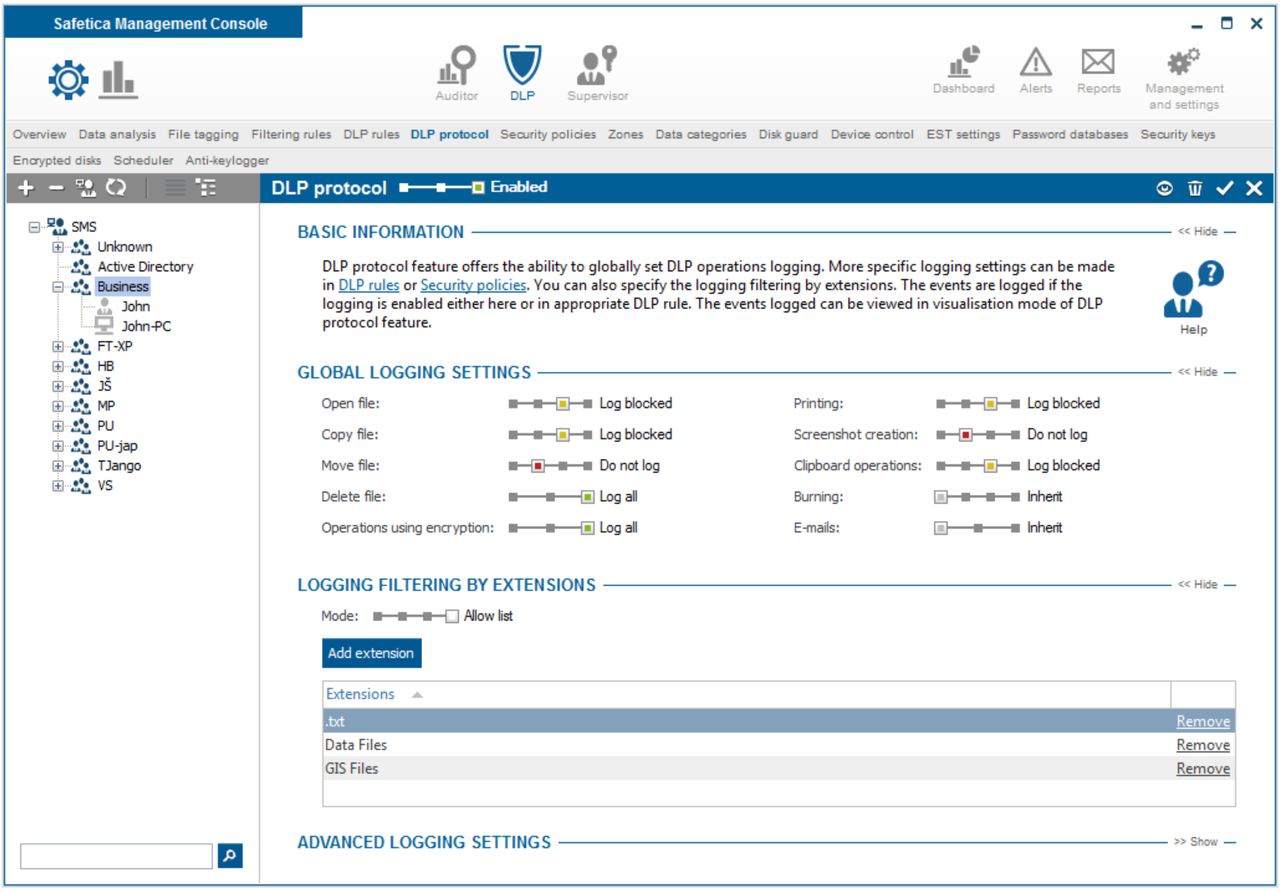
- *Disabled* – appropriate function is not activated.
- *Inherit* – appropriate function mode is inherited. Setting is inherited from parent group, if such setting is set on one or more parent groups.
- *Enabled* – appropriate function is activated.

There are two types of settings:

- *Explicit settings* – is a setting made manually for users, computers or groups.
- *Effective settings* – this setting is made automatically by joining the individual settings of groups, subgroups, users and computers. It is calculated based on a pass through the user tree from the lowest tree object (of a high priority) to the root or branch (of a lower priority) and by joining the individual settings.

By clicking on 🗑 you can delete the complete setting of the function.

By clicking on 👁 you can display the effective settings and by clicking again you display the explicit settings.



DLP protocol Enabled

BASIC INFORMATION

DLP protocol feature offers the ability to globally set DLP operations logging. More specific logging settings can be made in DLP rules or Security policies. You can also specify the logging filtering by extensions. The events are logged if the logging is enabled either here or in appropriate DLP rule. The events logged can be viewed in visualisation mode of DLP protocol feature.

GLOBAL LOGGING SETTINGS

Open file: Log blocked
Copy file: Log blocked
Move file: Do not log
Delete file: Log all
Operations using encryption: Log all
Printing: Log blocked
Screenshot creation: Do not log
Clipboard operations: Log blocked
Burning: Inherit
E-mails: Inherit

LOGGING FILTERING BY EXTENSIONS

Mode: Allow list

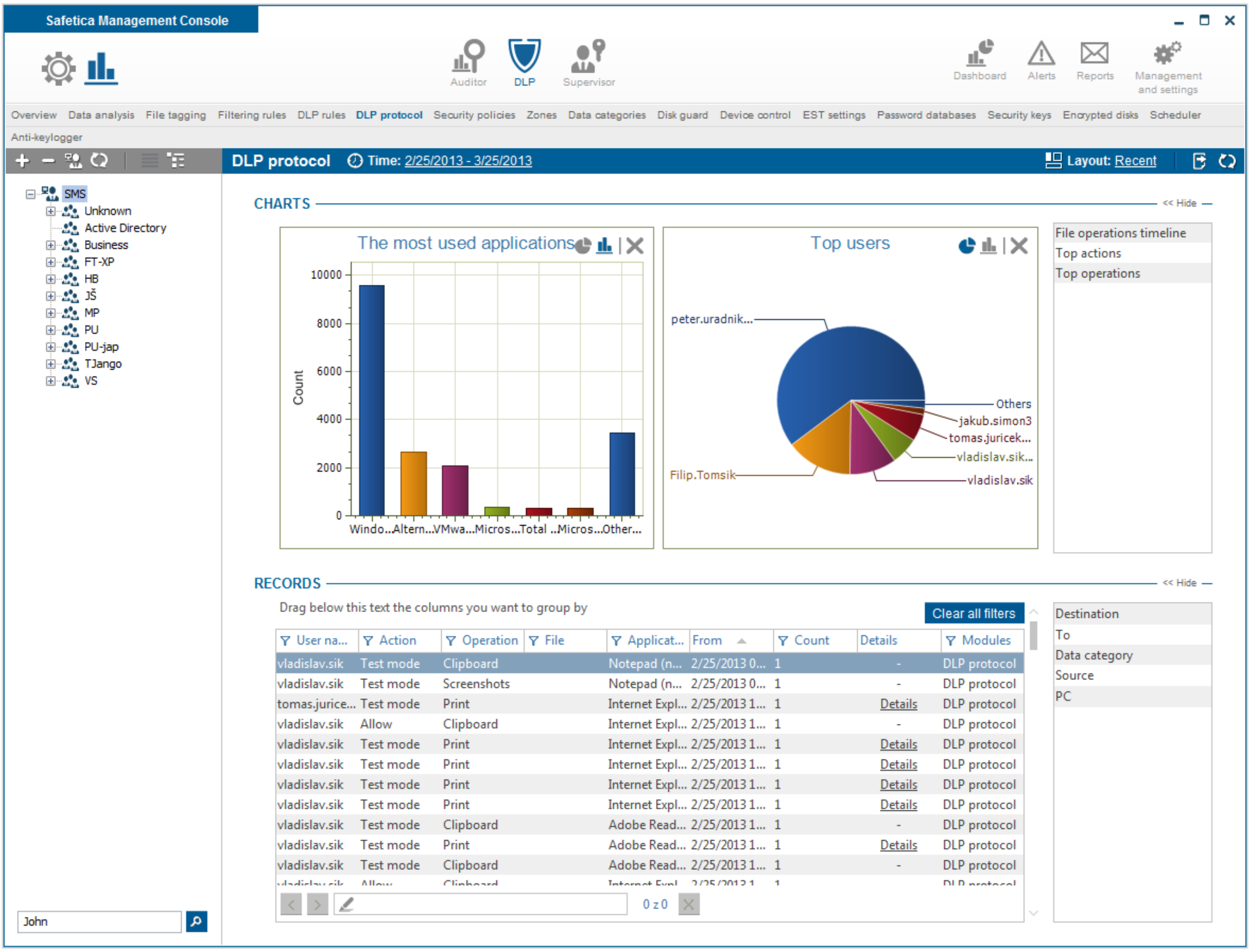
Extensions	
.txt	Remove
Data Files	Remove
GIS Files	Remove

ADVANCED LOGGING SETTINGS

5.4 Data visualization

In the visualization mode of Safetica, you can view the data that has been recorded about your employees. You can enter this mode via one of the mode setters that you will find on the left hand side of the main menu. Depending on the module and function you find yourself in at that point, you will then be presented with the recorded data and charts related to the subjects selected in the user tree. Due their nature, some functions do not include the visualization part. The functions of Endpoint Security Tools may serve as an example.

You can enter to the visualization mode by clicking on 📊 button in the upper left corner of SMC.



User na...	Action	Operation	File	Applicat...	From	Count	Details	Modules
vladislav.sik	Test mode	Clipboard		Notepad (n...	2/25/2013 0...	1	-	DLP protocol
vladislav.sik	Test mode	Screenshots		Notepad (n...	2/25/2013 0...	1	-	DLP protocol
tomas.jurice...	Test mode	Print		Internet Expl...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Allow	Clipboard		Internet Expl...	2/25/2013 1...	1	-	DLP protocol
vladislav.sik	Test mode	Print		Internet Expl...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Test mode	Print		Internet Expl...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Test mode	Print		Internet Expl...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Test mode	Print		Internet Expl...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Test mode	Clipboard		Adobe Read...	2/25/2013 1...	1	-	DLP protocol
vladislav.sik	Test mode	Print		Adobe Read...	2/25/2013 1...	1	Details	DLP protocol
vladislav.sik	Test mode	Clipboard		Adobe Read...	2/25/2013 1...	1	-	DLP protocol
vladislav.sik	Allow	Clipboard		Internet Expl...	2/25/2013 1...	1		DLP protocol

Records and charts are shown for users, computers or groups highlighted in the user tree, you can choose to show the data acquired by monitoring over only a given period of time. To do this, click on the date next to the Time: at the upper left side of your view. You have several option how to specify date:

- *Predefined* – you can choose from predefined time ranges:
    - o *Today* – records are displayed for the current day.
    - o *Yesterday* – records are displayed for the yesterday.
    - o *Last week* – records are displayed for the last seven days including current day.
    - o *Last month* – records are displayed for the last 31 days including current day.
- *One day* – you can view records for one selected day. You can select whole day or time interval. Confirm selection by *Confirm date* button.
- *Range* – you can view records for specific period of time. You can select from and to day. You can also specify time. Confirm selection by *Confirm date* button.

You can reload records and charts by clicking on the ⟳ button in the upper right corner.

Charts

The top part of the visualization view features an area for showing charts. You can find a list of the charts that are available in your current view at the right edge of the view.

- To show the chart, all you have to do is drag it from panel on the right to the notification area where there can be multiple charts at once.

- To remove the chart from the viewing area, press the ✕ button. Doing so will move the chart back to the list at the right.

- By clicking on the 📊, ◔ or 📈 buttons, you can change the type of the chart (pie chart, bar chart or line chart).

- Clicking on pie or bar will set filter on corresponding column and records below will be accordingly filtered. It can be done on multiple pies or bars inside display area – more filters will be set. To remove filter just click on pie or bar again.

Records

The bottom part of the visualization mode contains a table of detailed records. You can find a list of the columns that are available in your current view at the right edge of the view.

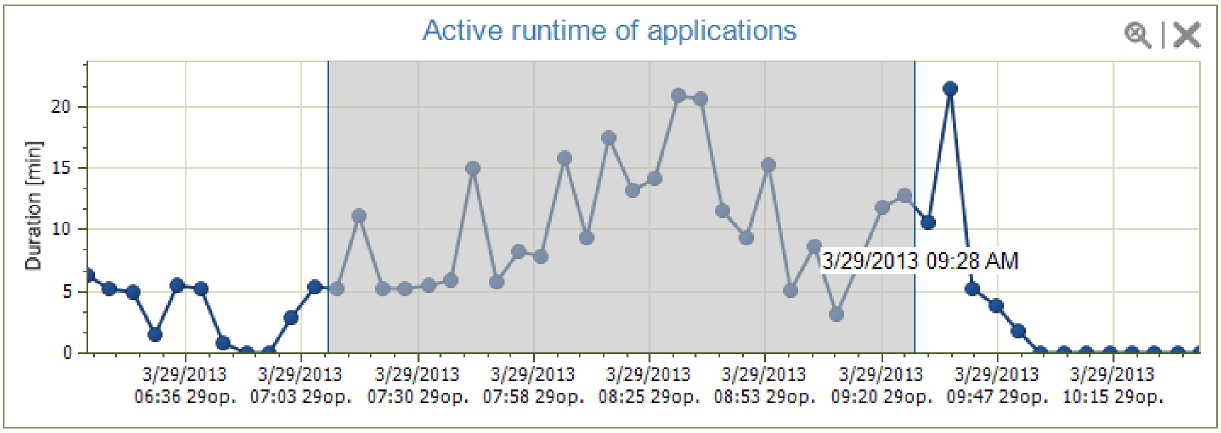
- To show the column in a table, all you have to do is drag the column to the table area.

- Clicking on the ▽ button at the head of the column will show a filter for that column. Fill out and confirm the filter by clicking the *OK* button in order to apply the filter to that column.

- Under the table you will find a search field. Filling it out will highlight the searched for expression in the table. Click on the ☒ to remove the highlighting.

- Drag a column head above the table to group the table data by that column. You can drag multiple columns above the table and you can sort these columns hierarchically, so records in the table will be grouped according to order.

- You can select time range in some of line charts by mouse selection. To cancel selection click on 🔍 button.



Filters

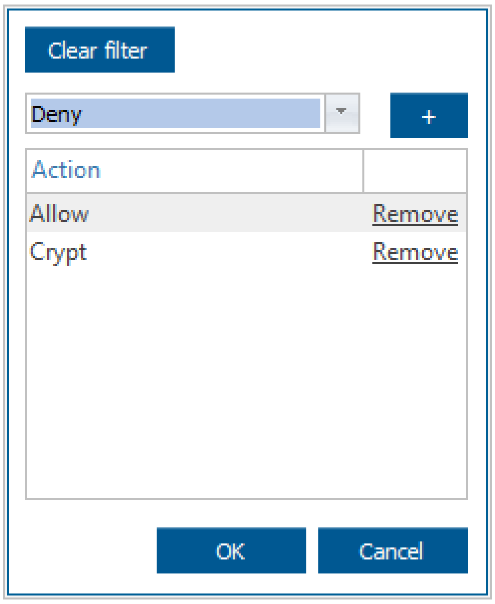
You can filter the records as well. For a column of your choice, click on the ▽ at the head of the column to open up its filter dialog. Fill text into the dialog or choose an item from the presented list in order to specify the item by which you want to sort the column. Click on the + button to add the selected item into the filter list. This list may of any length. Press the *OK* button to confirm and the table will only show the records that match at least one of the filters in the list.

▽ filter for column is not set.

▼ there is some filter set on the column.

You can set filter by clicking on pie or bar inside graph as was described above in Charts part.

You can remove all set filters by clicking on *Clear all filters* button.

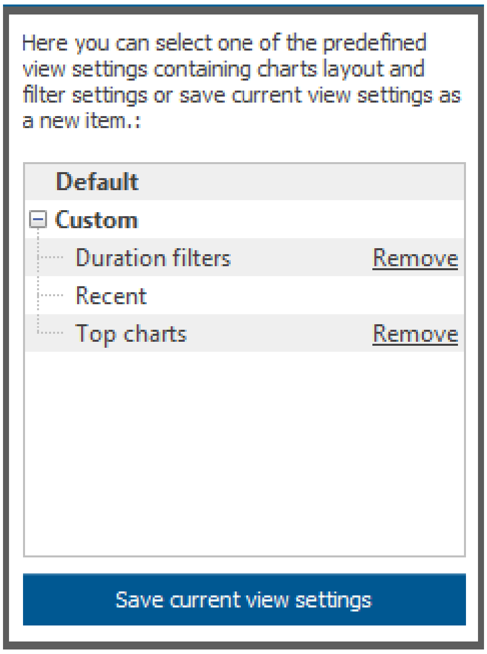


Deny

Action	
Allow	Remove
Crypt	Remove

Layouts

You can create your own layout of charts, columns and filters in each function. It is done using layout manager. You can open layout manager by clicking on Layout: button in top right corner.



Here you can select one of the predefined view settings containing charts layout and filter settings or save current view settings as a new item.:

- Default
- ⊟ Custom
  - Duration filters Remove
  - Recent
  - Top charts Remove

- Each SMS user could have own visualization layouts for each function.
- You can set default visualization layout by clicking on *Default* item in the layout manager.
- You can set recently used layout by clicking on *Recent* item.
- You can save current layout of charts, columns and filter by clicking on *Save current view settings.*

Export to PDF

You can export current displayed charts to PDF using button in top right corner.

6 Safetica Endpoint Client

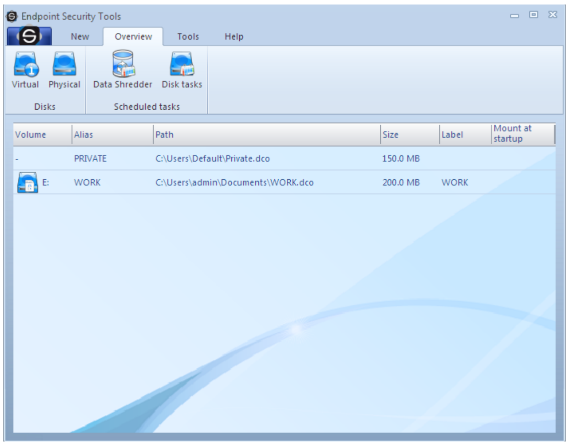
Safetica Endpoint Client is a part of Safetica. The module runs on client stations and allows the use of security tools and functions of Endpoint Security Tools on these stations.

You can use Endpoint Security Tools to quickly encrypt all storage devices - hard drives, USB drives, flash drives, floppy disks, ZIP drives, memory cards and many others. The data shredder can be used to safely and irretrievably delete sensitive information. You can also create an encrypted virtual drive which will behave as a classic full-fledged hard drive and work with it in the same way. Endpoint Security Tools also contain an advanced security manager for the organization of passwords and other information. All of this with a selection of the world's best ciphers. Using these and other functions of Endpoint Security Tools can ensure that your company data is safe and prevent a leak of sensitive information. This allows you to significantly contribute to the security of your company.

Safetica Endpoint Client is composed of two main parts:

- *Safetica Client Service* – launches on operating system startup as a service which communicates with the database and Safetica Management Service. The client service ensures that the security and monitoring modules of Safetica have access to the client stations.
- *Endpoint Security Tools* – the user interface with security tools and contextual menu. Can work in the following modes, based on the administrator's settings in Safetica Management Console:

1. The Endpoint Security Tools user interface with all security tools and a contextual menu available by right click on in the tray.
2. Context menu mode (Quick menu) with no user interface and basic security functions.

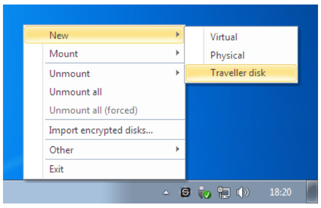


Volume	Alias	Path	Size	Label	Mount at startup
-	PRIVATE	C:\Users\Default\Private.dco	150.0 MB		
E:	WORK	C:\Users\admin\Documents\WORK.dco	200.0 MB	WORK	

6.1 Endpoint Security Tools User interface

Endpoint Security Tools user interface is composed of following parts:

1. *Quick menu* – basic user menu marked by an icon . It provides first of all quick choices - disks disconnection, safety profiles set up, looking up existing archives or closing a program.



2. *Bookmarks* – selecting a bookmark you select your goal. If you want to secure a disk or archive, view a overview of current options, use a tool or view the help, simply select the

appropriate bookmark and an icon with target action in appropriate tab.

3. *Tabs* – tabs will display a detailed selection of options corresponding with individual bookmarks.
4. *Desktop* - displays all processing information about your safe disks, encrypted documents, planned tasks or others. User's complete activity with disks and archives is routed to the desktop.
5. *Contextual menu* – allows creating encrypted archives or safely data removing by means of the contextual menu of the browser.

6.2 Overview of functions

The list of security functions offered by Endpoint Security Tools to its users follows.

6.2.1 Encrypted disks

Virtual disks

Virtual disk is a file encrypted by the Endpoint Security Tools software that behaves as a classical hard disk after connection. It means that you can create, modify, and copy files or otherwise work with your data on this disk. Furthermore, you can do low level operations with this disk such as formatting, defragmentation etc. There is one exception, however - the entire content will be encrypted with a security on an army level.

To launch the Creating new virtual disk wizard click on *New -> Virtual.*

To view an overview of created virtual disks click on *Overview -> Virtual.*

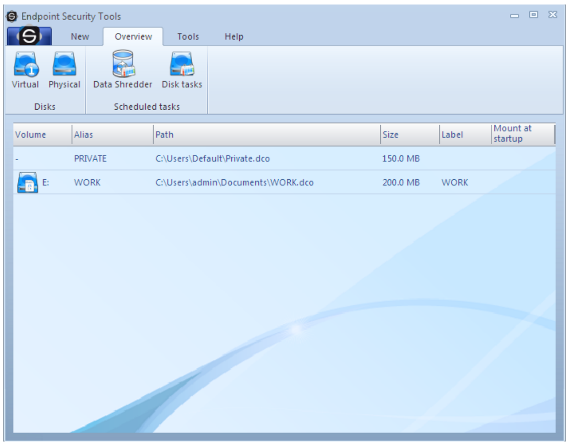
Physical disks

A physical disk is an existing physical disk of the following type: hard disk, USB disk, flash disk, 3.5" floppy drive, ZIP Drive, memory cards and many more types of exchangeable disks. An exchangeable disk is also a hard disk partition. The Endpoint Security Tool system can encrypt all such devices without problems.

NOTE: Encryption will cause loss of all original data. Back up all data before encrypting! When the encryption is completed, you can copy the data back on the encrypted disk.

To launch the Creating new physical disk wizard click on *New -> Physical.*

To view an overview of created physical disks go to *Overview -> Physical.*



Volume	Alias	Path	Size	Label	Mount at startup
-	PRIVATE	C:\Users\Default\Private.dco	150.0 MB		
E:	WORK	C:\Users\admin\Documents\WORK.dco	200.0 MB	WORK	

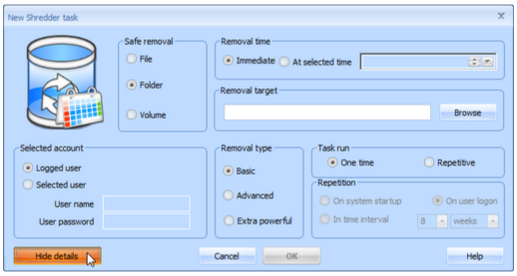
6.2.2 Traveller disks

Traveller disks allow you to make virtual disks easily accessible even on computers not equipped with Endpoint Security Tools software. Traveller disk has an equivalent security features as other disk types encrypted by Endpoint Security Tools software. It means, if the media with this disk are stolen, your data will be completely intelligible to the thief.

You can launch the Creating new traveller disk wizard by clicking on *New -> Traveller disk.*

6.2.3 Data shredder

Shredding tasks is another feature of the Endpoint Security Tools. The activity of the shredder can be planned. It is possible to periodically safe-remove unnecessary data, for example temporary files created by surfing on the web. Just click on the tab Overview and Scheduled tasks.



New Shredder task

Safe removal: ○ File ● Folder ○ Volume

Removal time: ● Immediate ○ At selected time

Removal target

Selected account: ● Logged user ○ Selected user

User name

User password

Removal type: ● Basic ○ Advanced ○ Extra powerful

Task run: ● One time ○ Repetitive

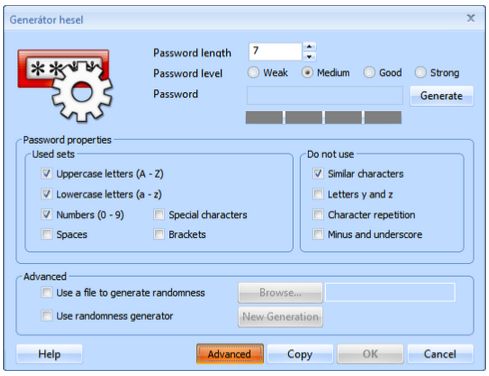
Repetition: ○ On system startup ● On user logon ○ In time interval 8 weeks

You can start shredding by clicking on *New -> Shredding task*.

6.2.4 Password Generator

We have often to choose different passwords and not every time passwords like „alice“ are safe enough. Logical tendency is to use known words, names, birth dates or similar phrases. Unfortunately these options are the first ones the attackers try with techniques like dictionary attack or brute force attack. Requirement for a safe password are combinations of small and capital letters, numbers, special characters, minimal length, etc. When this combination is strong enough, it is impossible to break such password not even in hundred years.

It is complicated to create such password. With the help of the Password generator integrated in Endpoint Security Tools this task is matter of seconds. Simply choose the level of password you want or length, combination of characters and the rest does Endpoint Security Tools for you.



Generátor hesel

Password length 7

Password level ○ Weak ● Medium ○ Good ○ Strong

Password

Password properties

Used sets

☑ Uppercase letters (A - Z)

☑ Lowercase letters (a - z)

☑ Numbers (0 - 9)

☐ Special characters

☐ Spaces

☐ Brackets

Do not use

☑ Similar characters

☐ Letters y and z

☐ Character repetition

☐ Minus and underscore

Advanced

☐ Use a file to generate randomness

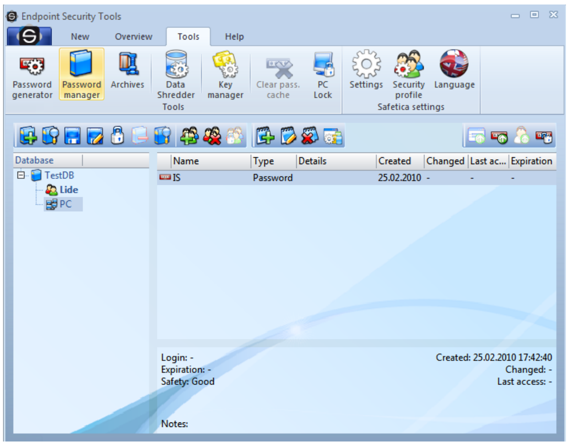
☐ Use randomness generator

You can launch the password generator by clicking on *Tools -> Password Generator.*

6.2.5 Password manager

The **Password manager** within the Endpoint Security Tools product provides secure control and overview of the most sensitive information we have. User names, passwords, access codes, PINs, payment card numbers, security keys, certificates and whatever other short text data and files can be organized and secured on the highest level by the Endpoint Security Tools through main strong password on army level.

All these information are saved in encrypted local structured databases. Various types of information can be divided in groups and subgroups, in types as for example password, contact, file or security key. Every other level can be secured by further password or security key according to information importance.



Name	Type	Details	Created	Changed	Last ac...	Expiration
IS	Password		25.02.2010	-	-	-

Login: -
Expiration: -
Safety: Good

Created: 25.02.2010 17:42:40
Changed: -
Last access: -

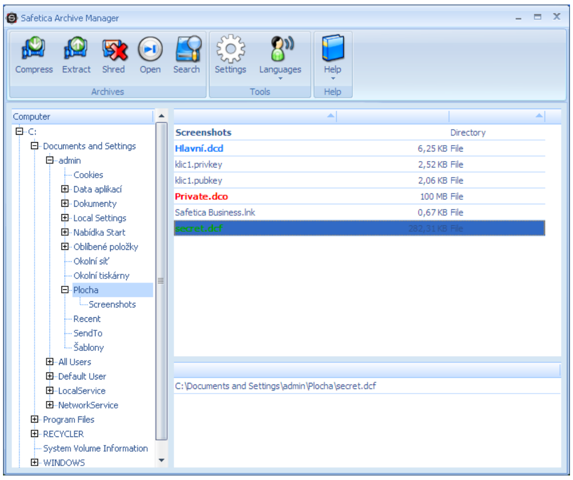
Notes:

You can display the Password Manager by clicking on *Tools -> Password Manager.*

6.2.6 Archive manager

The Safetica Archive Manager is part of the Endpoint Security Tools. It includes file and folder encryptions in DCF archives.

In addition to file and folder encryption in own DCF format this component serves for complete work with archives and data compression. Beside standard formats compression methods the program enables to simultaneously encrypt and compress files or folders in the self-extracting EXE archive.



Screenshots		Directory
Hlavní.dcd	6,25 KB	File
klic1.privkey	2,52 KB	File
klic1.pubkey	2,06 KB	File
Private.dco	100 MB	File
Safetica Business.lnk	0,67 KB	File
secret.dcf	282,31 KB	File

C:\Documents and Settings\admin\Plocha\secret.dcf

You can launch the Archive Manager by clicking on *Tools -> Archives.*

6.2.7 Security keys

An important feature of the Endpoint Security Tools is the possibility of restoring the user data from the virtual disks, as well as the physical ones. The security key is in case of forgetting the password the only possibility, how to make an access to your data.

Every security key consists of two subkeys - the private security key and the public security key. The private key serves for unlocking of the encrypted disk in case of losing the password; on the contrary, the public key creates in the Creating disks wizard a lock for the private key, which will open this lock. The private key is saved as a file on the secured and reliable place (like a CD disk and saved in the safe), while the private key is possible to move among computers and use it for mutual creating of the security locks to your data. For the distribution of the public keys the import and export commands serve, which will be inscribed below. You can find more about this also in the chapter about the exporting and importing.

Every security key pair is mutual. If you create more security keys (pairs - the private key and the public one), only the corresponding pairs will cooperate. With the concrete public key you interlock only one concrete private key. You can use the private key to lock only these disks, which are locked by the same private key.

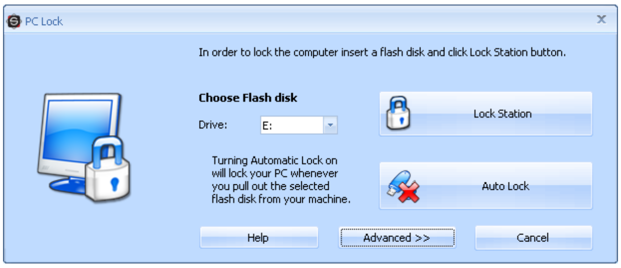
You can launch Security Key Manager by clicking on *Tools -> Key Manager*.

A wizard for creating a new pair of security keys can be launched by clicking on *New -> Security key*.

6.2.8 PC Lock

Various circumstances force you to leave from your computer. Thus an occasion for attackers occurs. While you are at some other place an attacker may take a chance and seriously damage the computer. In better case you can expect some joke from your colleagues in a worse one foreign attackers can delete or steal some important documents.

If you use the common locking of computer by means of password you have to enter the password in for a long time and an attacker may guess your password. The PC Lock function will release you from similar threats. By means of PC Lock you will lock your PC by mere flash disk disconnection and open it by its connection. Your flash disk will ensure all what is necessary.



In order to lock the computer insert a flash disk and click Lock Station button.

Choose Flash disk

Drive: E:

Turning Automatic Lock on will lock your PC whenever you pull out the selected flash disk from your machine.

The dialog used for setting the PC lock can be opened by clic on *Tools -> PC lock*.

safetica®