SAFETICA
COMPLETE DOCUMENTATION

safetica®

SAFETICA
COMPLETE DOCUMENTATION

product Safetica version 5.2.0

Author: Safetica Technologies s.r.o.

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

For more information visit www.safetica.com.

Published: 2013

CONTENT

WELCOME!

ABOUT SAFETICA

DEPLOYMENT OF SAFETICA

MANAGEMENT OF SAFETICA

MODULES OF SAFETICA

SAFETICA ENDPOINT CLIENT

1 WELCOME!

Dear user,

Thank you for your confidence in choosing Safetica. We are certain that you will be fully satisfied. In this document you will find a detailed description of all components of the product and manual help for using the individual features. This documentation will guide you in detail from installation and initial deployment on the company network to common usage, evaluation of output and solving the most frequent problems.

If you do not succeed in solving a problem even after consulting this information, please contact technical support at http://www.safetica.com/support.

Safetica offers a completely new approach to internal security. It is the first security solution combining real prevention with actual protection against internal threats. By monitoring 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 by employees. No other software application can protect a company against all major internal threats in such an all-encompassing manner.

If you want to install the software as quickly as possible, please read this *Safetica installation manual*. To quickly master basic practices and usage, use the *Safetica quick wizard*. Answers to frequently asked questions about using the software can be found in *Frequently asked technical questions of Safetica users*.

Thank you,

Safetica Technologies team, vendor of Safetica

2 ABOUT SAFETICA

Every day your company can be damaged by its own employees. They may only pretend to be working, misuse company resources or steal and lose sensitive data. Safetica security software is the only application in the world that protects your company against all the major failures of your staff: sensitive data leaks, financial losses and damage to your company's reputation. At the same time, it alerts you to potentially dangerous behavior among your staff long before their conduct threatens your company.

Major Benefits

- Protect your company against the consequences of the failings of your own employees.
- Detect employee behavior that may damage your company in good time.
- Obtain an overview on the working activity and productivity of your staff.
- Ensure that sensitive company data remains where it should be – inside the company.

- Protect your company's interests with regard to your employees' privacy.
- Ensure that staff access sensitive information only in the authorized way.
- Work with security software that does not disrupt your company’s current processes.
- Reach compliance with industrial standards, regulations and laws easily.

Safetica Modules

Auditor

Detect potentially dangerous employee behavior right from the time it starts. Monitor employee working activity and detect who is trying to damage your company.

DLP

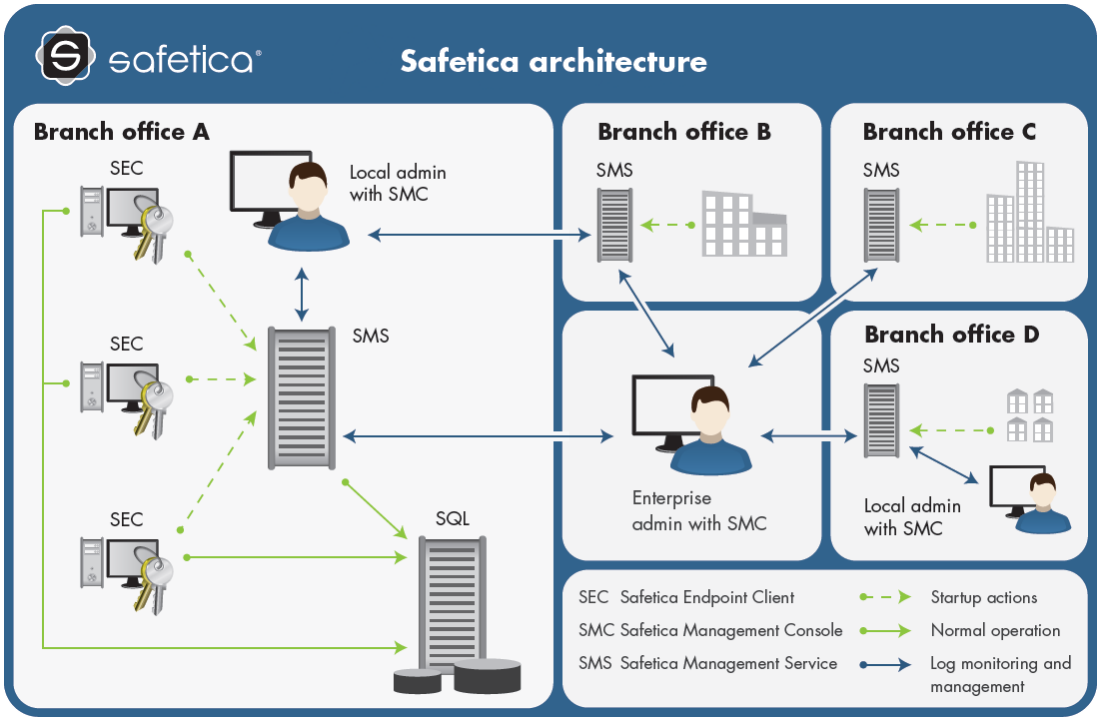
Prevent your employees from misusing data they are granted access to and protect sensitive company information against unauthorized persons.

Supervisor

Obtain control over employees’ working activity. Eliminate undesirable behavior and thus increase employee productivity.

2.1 Architecture

Safetica product is based on a client – server architecture. The client application Safetica Endpoint Client (SEC) runs on end workstations. This application communicates with the Safetica Management Service (SMS) server component. Security managers or administrators can use Safetica Management Console (SMC) for a remote connection. Data obtained by monitoring individual end stations is stored on a database server. The software is optimized for operating extensive networks including branch support, even multinational ones.



Safetica is therefore a decentralized solution. It allows employing multiple servers and centrally managing them from a single console (independent management is of course also possible). Each of the servers can service a part of the company environment, so it is possible to divide the load further. This architecture makes it possible to support multiple branches and in fact an unlimited number of users and computers.

Each of the following components may be installed on a separate computer.

SMS represents the server part. It runs as a service on a server. Multiple services may run in one domain thanks by means of tofor the load distribution. using division of the Active Directory tree. An alternative for small networks is the option of installing the service on a network without a domain, so that it can run on a standard computer.

On each Safetica Management Service it is possible to assign different rights to individual administrators (or managers) using Safetica Management Console, so the company security control can be divided into different roles (e.g. local admin, enterprise admin, security manager, etc.).

SMC is a management center that serves to set and control client stations (Safetica Endpoint Client), server services (Safetica Management Service) and databases. It also displays the output of monitoring, statistics and graphs. It can run anywhere you have a connection to the server service. The number of console installations and number of users are not limited by the license.

SEC represents a client component which runs on the end stations of each of your employees. It comprises two main parts:

- Safetica Client Service – launches at each start of the operating system as a service and performs monitoring, enacting the security policy and carrying out communication with the database and Safetica Management Service. The client service manages the functioning of the Auditor, DLP and Safetica Endpoint modules on the end stations.
- Endpoint Security Tools – user interface with security tools and a contextual menu. This part is available only with a valid DLP module license. It can work in three modes depending on settings:

1. Normal mode – user interface with security tools and contextual menu available by right-clicking on in the notification area (available only with a valid DLP license).
2. Tray mode with basic user actions available only from the contextual menu without a user interface (available only with a valid DLP license).

3. Invisible mode without Endpoint Security Tools and the contextual menu. Only the Safetica Client Service runs on the client station. This mode does not hide processes of the SEC component on its own. Hiding processes can be carried out in the Endpoint Security Tools settings.

SQL Database

The SQL database is the last component, used for storing data obtained through monitoring and settings. It also includes the categorization database with such categories as applications, websites and appendices.

- SEC uses the SQLite database for temporary storage of records, settings and categories.
- Every SMS uses databases on the SQL server for storing settings, records and categories. Every SMS needs three designated databases on the SQL server for storing records, settings and applications, websites and appendices categories. To store a database, you can use your own Microsoft SQL Server or Microsoft SQL Server 2008 R2 Express which comes with the installer.

Data calculator

The data calculator can help you to estimate the capacity that an SQLite or MS SQL database requires to run the Safetica software. By selecting the number of users, level of user activity, screenshot quality and desired modules, you can easily obtain sharable estimates of database capacity requirements.

You can find the data calculator at the website http://calc.safetica.com/.

Note

All of the components described above can be installed on one computer. Depending on the security policy settings, SMS and SMC performance may be negatively affected if this is done. For example, if you disable network communication on the computer, other SECs will not have a connection to the SMS.

2.2 Requirements

As described in the Architecture section, Safetica is made up of several components, each developed for a specific function. Each of these components also has its own operating system, hardware and software requirements.

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

2.2.1 Safetica Management Service

Minimum hardware requirements:

- Processor:

  1.8 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single-core processor

- RAM:

  1 GB

- Hard disk space requirements:

  4 GB reserved space

Recommended hardware requirements:

- Processor:

2,4 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) dual-core processor

- RAM:

  2 GB

- Hard disk space requirements:

  10 GB reserved space

Supported operating systems:

- *Microsoft Windows XP SP3 32-bit and 64-bit*
- *Microsoft Windows Vista 32-bit and 64-bit*
- *Microsoft Windows 7 32-bit and 64-bit.*
- *Microsoft Windows 8 32-bit and 64-bit*
- *Microsoft Windows Server 2003 SP1 32-bit and 64-bit*
- *Microsoft Windows Server 2003 R2 32-bit and 64-bit*
- *Microsoft Windows Server 2008 32-bit and 64-bit*
- *Microsoft Windows Server 2008 R2*
- *Microsoft Windows Server 2012*

Note: There could be only one instance of Safetica Management Service installed on one PC.

2.2.2 Safetica Management Console

Minimum hardware requirements:

- Processor:

  1.5 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single-core processor

- RAM:

  512 GB

- Hard disk space requirements:

  2 GB reserved space

Recommended hardware requirements:

- Processor:

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

- RAM:

  1 GB

- Hard disk space requirements:

  2 GB reserved space

Supported operating systems:

- *Microsoft Windows XP SP3 32-bit and 64-bit*
- *Microsoft Windows Vista 32-bit and 64-bit*

- *Microsoft Windows 7 32-bit and 64-bit.*
- *Microsoft Windows 8 32-bit and 64-bit*
- *Microsoft Windows Server 2003 SP1 32-bit and 64-bit*
- *Microsoft Windows Server 2003 R2 32-bit and 64-bit*
- *Microsoft Windows Server 2008 32-bit and 64-bit*
- *Microsoft Windows Server 2008 R2*
- *Microsoft Windows Server 2012*

Note: Safetica Management Console could be used by multiple users on one PC.

2.2.3 Safetica Endpoint Client

Minimum hardware requirements:

- Processor:

  1.5 gigahertz (GHz) 32-bit (x86) or 64-bit (x64) single-core processor
- RAM:

  512 GB
- Hard disk space requirements:

  2 GB reserved space

Recommended hardware requirements:

- Processor:

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

  1 GB
- Hard disk space requirements:

  2 GB reserved space

Supported operating systems:

- *Microsoft Windows XP SP3 32-bit and 64-bit*
- *Microsoft Windows Vista 32-bit and 64-bit*
- *Microsoft Windows 7 32-bit and 64-bit.*

2.2.4 Microsoft SQL Database

Every Safetica Management service uses three own reserved SQL databases for record, settings and category storage.

Supported SQL Servers

- *Microsoft SQL Server 2008 32-bit and 64-bit*
- *Microsoft SQL Server 2008 Express 32-bit and 64-bit*
- *Microsoft SQL Server 2008 R2 32-bit and 64-bit*

- *Microsoft SQL Server 2008 R2 Express 32-bit and 64-bit (je soucástí instalátoru)*
- *Microsoft SQL Server 2012 32-bit and 64-bit*
- *Microsoft SQL Server 2012 Express 32-bit and 64-bit*

Note: You will find hardware and software requirements of listed SQL servers on the Microsoft web page (www.microsoft.com).

3 DEPLOYMENT OF SAFETICA

When installing, proceed as follows:

1. Before commencing the installation, check to make sure that your network meets the specified service requirements.
2. Install Safetica Management Service on selected PC(s). During installation, choose which Microsoft SQL Server shall be used by SMS for storing data.
3. Install Safetica Management Console on the computer from which you would like to manage Safetica.
4. Using Safetica Management Console, connect to Safetica Management Service and configure the server.
5. Install Safetica Endpoint Client on each client.
6. Perform the initial setup and verify that all components have been correctly installed and properly communicate with each other.

After installing all the components and checking to make sure that everything has been installed correctly, you may begin using Safetica.

In the following sections, each step of the deployment will be described in detail.

3.1 Before installation

Take the following steps before installation:

1. Check whether the hardware and software requirements of all three Safetica components are met.
2. Analyze your corporate network:
   - o Decide on what PCs you are going to install the Safetica Management Service (SMS) in your environment. When making the decision, take the following into account:
     - The PC with SMS must be able to connect to the SQL server on which the main databases will be stored.
     - Depending on the number of SECs connected and the database server type, set how many SMS you wish to install in your environment. The number of SECs that can connect to one SMS is limited by the SQL database which the SMS uses for storing data – see below.
   - o Decide on what PCs you are going to install the Safetica Management Console (SMC) in your network. The PC with SMC must be able to connect to all SMS you wish to administer by using the administration console.
   - o Decide on what PCs you are going to install the Safetica Endpoint Client (SEC) in your network. When making the decision, take the following into account:
     - For every SEC, decide what SMS it will be connected to. Not every PC will be connected to all PCs with SMS.

- The PC with SEC must be able to connect to some SMS in your environment.
- The PC with SEC must be able to connect also to the SQL server which has the SMS databases. SEC exchanges settings and records from SMS via these databases.

o Select and designate SQL servers on which the central databases of the individual SMS will be stored. When making the decision, take the following into account:

- Every SMS needs three designated databases on the SQL server: one for settings, one for records and one for the category database.
- The databases of multiple SMS may be stored on a single SQL server, but this can affect the number of SECs which the SQL server can serve.
  - When using the Microsoft SQL Server of the Express edition, the ideal number of connected SECs is 50, with a maximum of 70. These counts apply to the installation of the entire SQL Server.
  - When using the Microsoft SQL Server of the standard edition (Standard, Enterprise, etc.), the ideal number of connected SECs is 200, with a maximum of 300. These counts apply to the installation of the entire SQL Server.

3. Before installing the various Safetica components (SMS, SMC, SEC), ensure they will not be blocked by a firewall or antivirus software.

o Add exceptions for incoming connections to the process STAService.exe and the following ports on the PCs on which the Safetica Management Service will be installed:

- 4438 (communication SEC -> SMS, database).
- 4441 (communication SMC -> SMS).

o Add exceptions for the process STAConsole.exe on the PCs on which you will install the Safetica Management Console.

o Set exceptions for the following processes on the PCs on which you will install the Safetica Endpoint Client: STCService.exe, STMonitor.exe, STUserApp.exe, Safetica.exe, STPCLock.exe, outgoing and incoming connections.

o Set exceptions for port 1433 (default port for database connection) on the PCs on which you will install the databases.

4. Download the universal installer with the latest Safetica release (http://downloads.safetica.com/safetica_5_setup.exe).

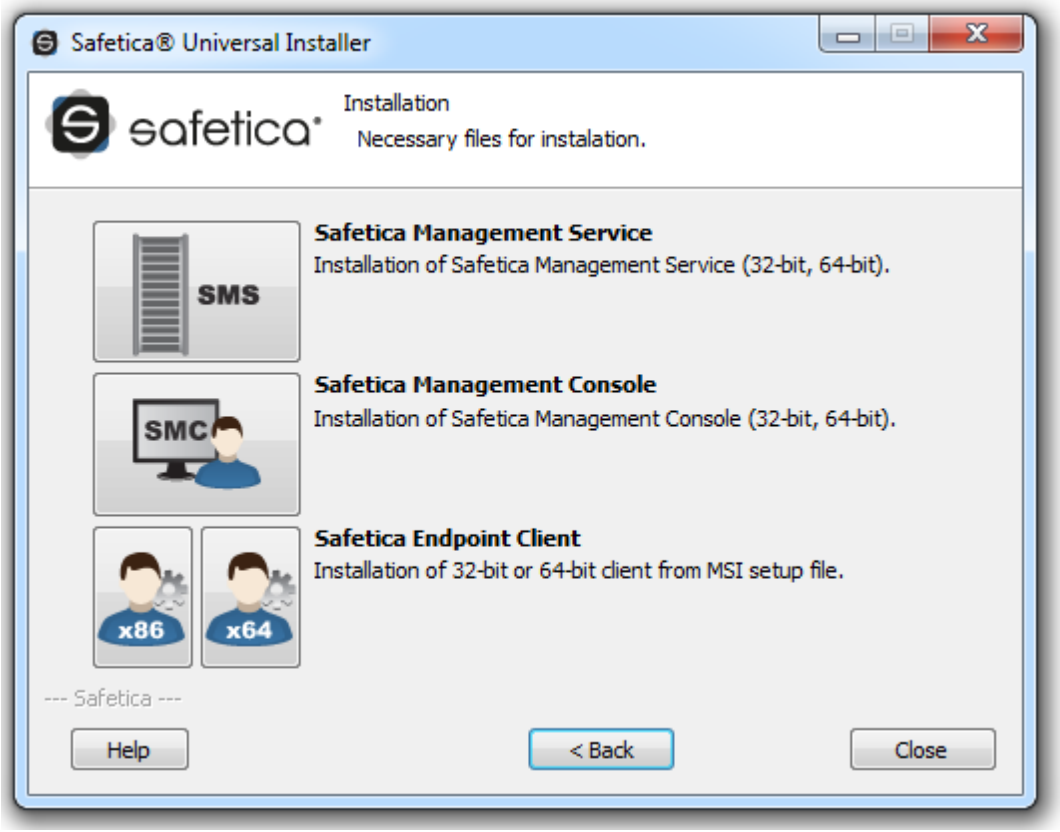
o The universal installer contains all components necessary for installation.

3.2 Installation of Safetica Management Service

Safetica Management Service is a central server component of Safetica. It ensures that all Safetica clients (SEC), the console (SMC) and the databases are interconnected.

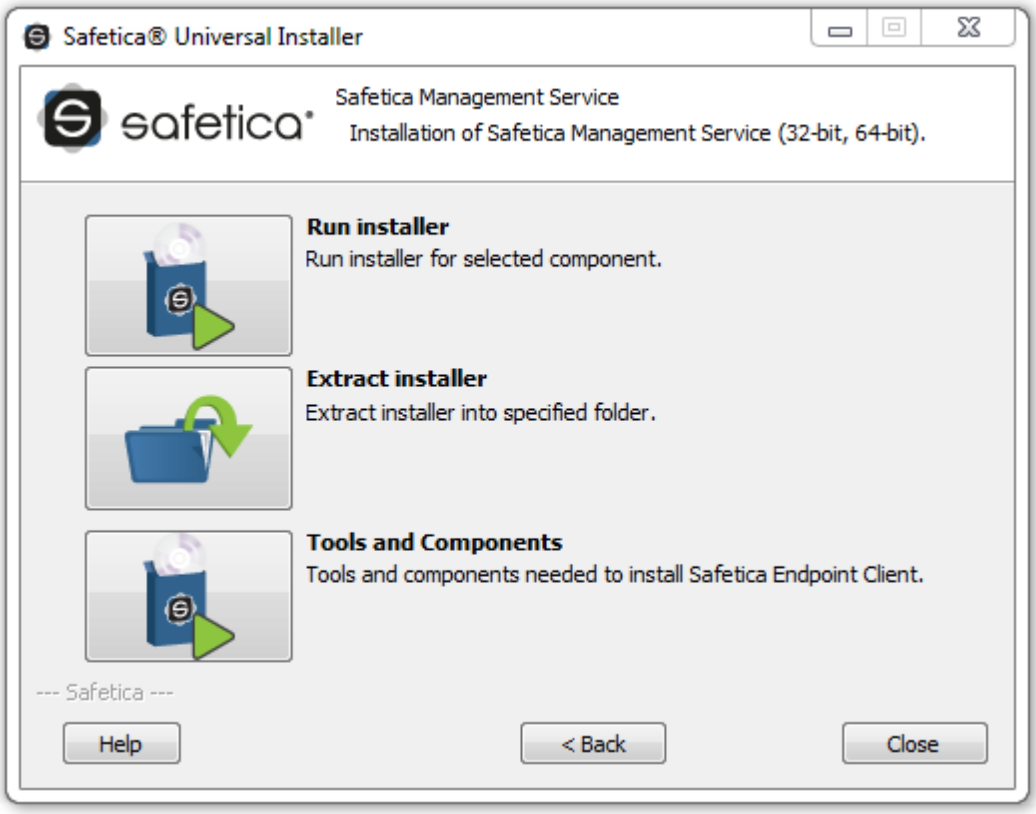
To perform the installation, proceed as follows:

1. Launch the universal installer that you have downloaded. After selecting your language, and agreeing to the license terms, go to Installation > Safetica Management Service.

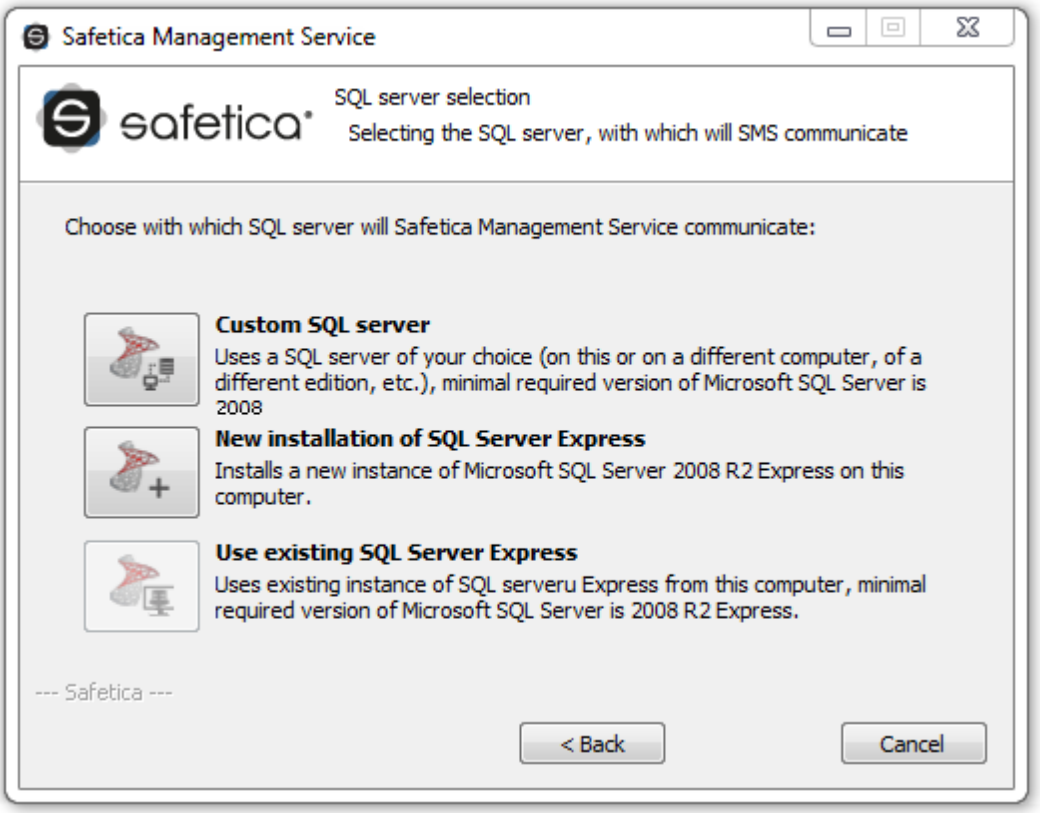


2. Here you several options:
   - Run the installation directly from the universal installer by clicking on Run Installer.
   - Extract only the Safetica Management Service installer, which you can then use separately for later installation.

     Note: In the third part Tools and Components you will find components essential for correct installation of the Safetica Endpoint Client or Microsoft SQL Server 2008 R2 Express. If you are going to install Microsoft SQL Server 2008 R2 Express from this installer, make sure you have installed the Microsoft Installer 4.5 component. If this component is not installed, install it now.



3. After running the installer (either from the universal installer or from the extracted one), select your language once again and accept the license terms. Select the installation folder.
4. Select the Installation Folder.
5. Next, you must choose the SQL Server on which the SMS installed will store the databases. You can choose from the following options:
   a. If choosing this option, you can use your existing Microsoft SQL Server installation to create the database. Supported Microsoft SQL Servers are listed in the requirements. For a description of the configuration, continue to Configuring an Existing SQL Server.
   b. If choosing this option, you will install Microsoft SQL Server 2008 R2 Express on your existing PC. The new server will be used for creating the SMS databases. For a description of the installation, continue to Installation of New SQL Server Express.
   c. If you have an existing instance of Microsoft SQL Server 2008 R2 Express on the PC where you are going to install SMS, you can choose this last option. The existing SQL Server will be used for storing SMS databases. For a description of the configuration, continue to Configuring an Existing SQL Server.



6. Before starting installation, you can still disable Integration settings. Integration is enabled in the default mode (recommended).
7. Complete the installation. Safetica Management Service will install and then launch automatically.
8. Once the installation has successfully completed, verify that the STAService.exe is running (Task Manager -> Services -> STAService – running)
9. Finally, verify that you have added exceptions to your firewall and antivirus for the STAService.exe process and that ports 4438 and 4441 are not blocked.

Note: By default, Safetica Management Console normally uses port 4441 for connecting to Safetica Management Service and port 4438 for connecting to Safetica Endpoint Client . You can change the settings to use different ports here as well.

3.2.1 Configuring an Existing SQL server

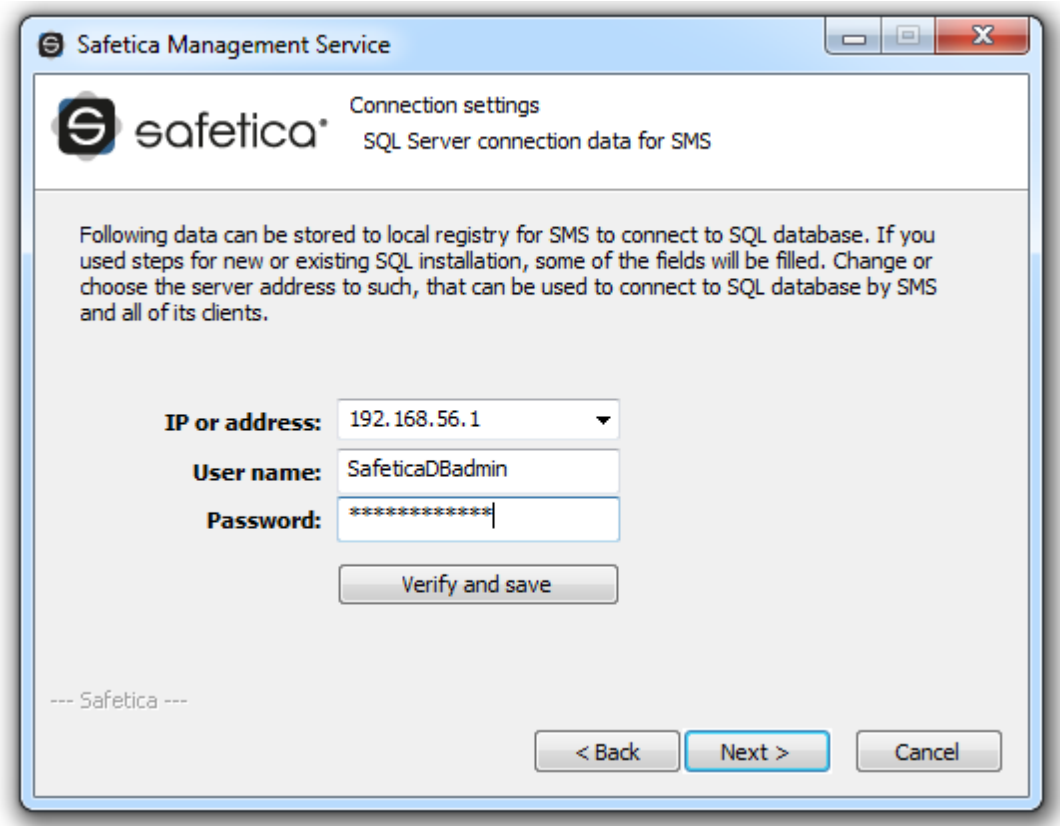
If you choose your own SQL server during Safetica Management Service (SMS) installation, you need to check first if this server is correctly set for storing SMS databases.

- Check whether SQL Server authentication is set to mixed mode – SQL Server authentication and Windows authentication (Microsoft SQL Server Management Studio -> Server settings -> Security -> SQL Server and Windows Authentication mode).
- The SQL server must be available in the network via the TCP/IP protocol (SQL Server Configuration Manager -> SQL Server Network Configuration -> TCP/IP Enabled).
- A user with sufficient rights to create a database (dbcreator) must be created in the SQL server. Apply this user when entering the data.

If you have no SQL server installed, follow the instructions and go to Installation of User's Own SQL Server.

If you have the SQL Server installed and it meets all criteria set the opening section, you can begin the configuration:

1. First complete the following:
   - *IP or address* – enter the IP address or SQL Server name here. The SQL server must be available via this address or name both for newly installed SMS and for clients (Safetica Endpoint Client – SEC) that will connect via this SMS. When filling this in, you can specify the SQL Server instance (e.g. 192.168.100.1\InstanceName). If entering a plain IP address or name, the default SQL server instance will be applied.
   - *User name* – enter the name of the user for the SQL server. The user must have at minimum rights to create databases (dbcreator). The user will be applied for creating and connecting to all three databases that will be automatically created on the SQL server after SMS installation.
   - *Password* – SQL server user name.



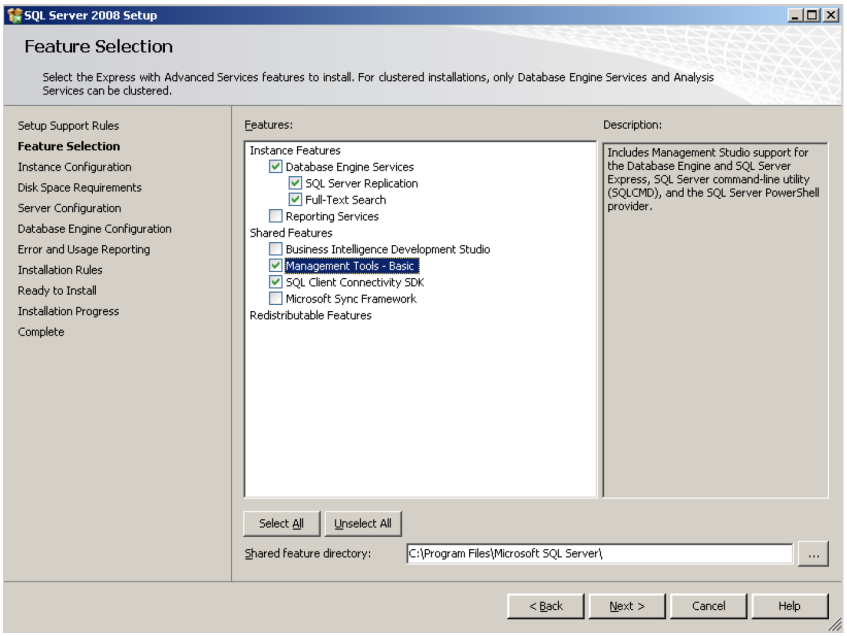
2. Click *Verify and save*.
3. Click *Next*, continue and finish Safetica Management Service installation. After completing the SMS installation, three databases will be created on the SQL server:
   - safetica_main – used for storing and sharing settings between SMS and SEC.
   - safetica_data – used for storing data recorded from clients (SEC).
   - safetica_category – used for storing applications, websites and appendices categories.

Note: You can later change the connection to the Safetica Management Service via the Safetica Management Console in the Server settings section. The configuration of this connection is described in the section Safetica Management Service Configuration.

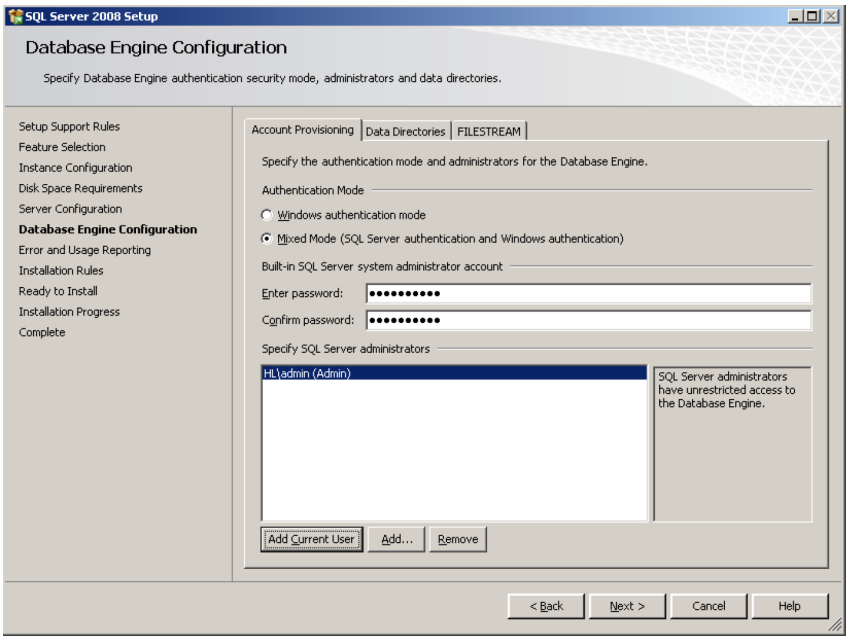
3.2.1.1 Microsoft SQL Server installation

If you don't have SQL Server installed proceed as follows when installing new SQL Server:

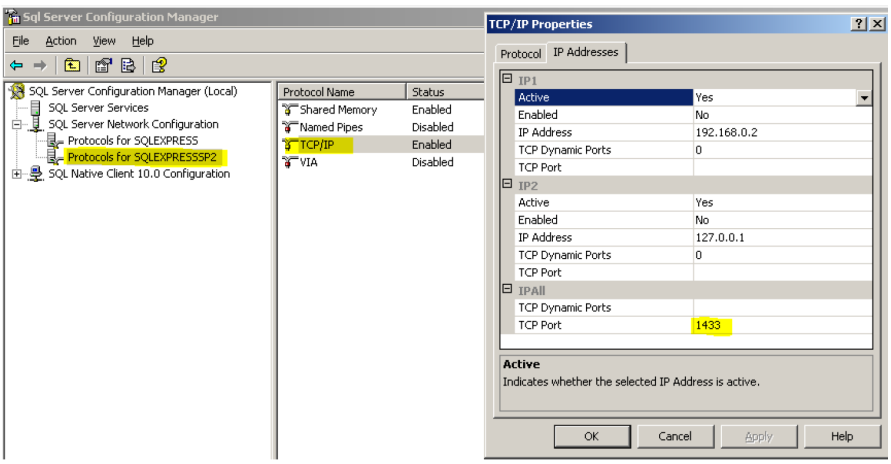
1. Install MS SQL on your server from the following components.



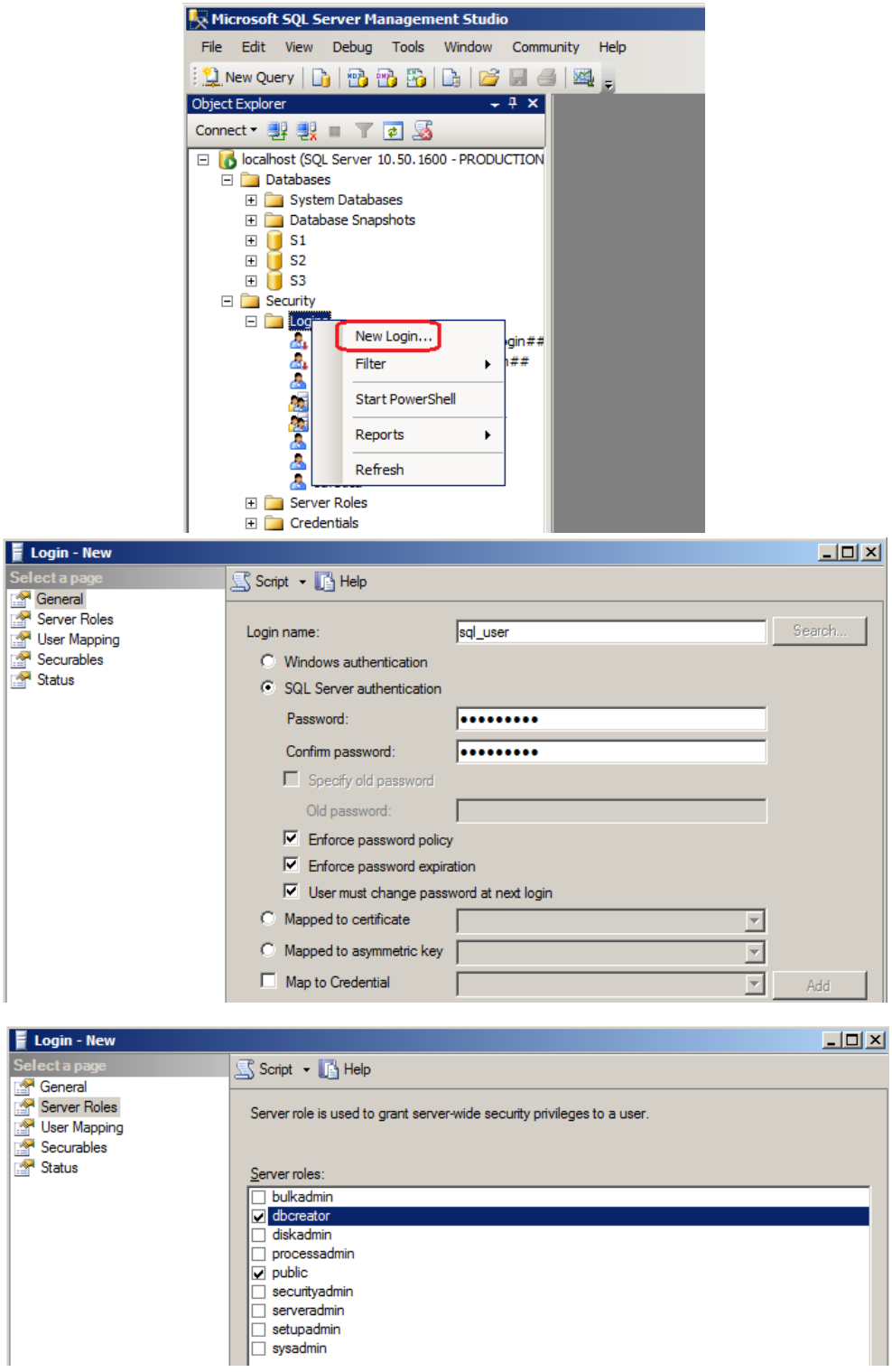
2. Set up Mixed mode authentication in the relevant installation step



3. Make sure that you have the MS SQL server set to listen, for example, on port 1433. You can do this using the Sql Server Configuration Manager tool



4. Create a new MS SQL user with sufficient rights to create databases using the Sql Server Management Studio tool. Select the authentication type in the setup as SQL Server authentication and enter a new password.



The connection of Safetica Management Service to these databases is set via Safetica Management Console in section Server settings. For a description of how to configure this connection, see the section Configuration of Safetica Management Service

3.2.2 Installing a new SQL Server Express

If you do not own any SQL Server, you can install Microsoft SQL Server 2008 R2 Express from this installer.

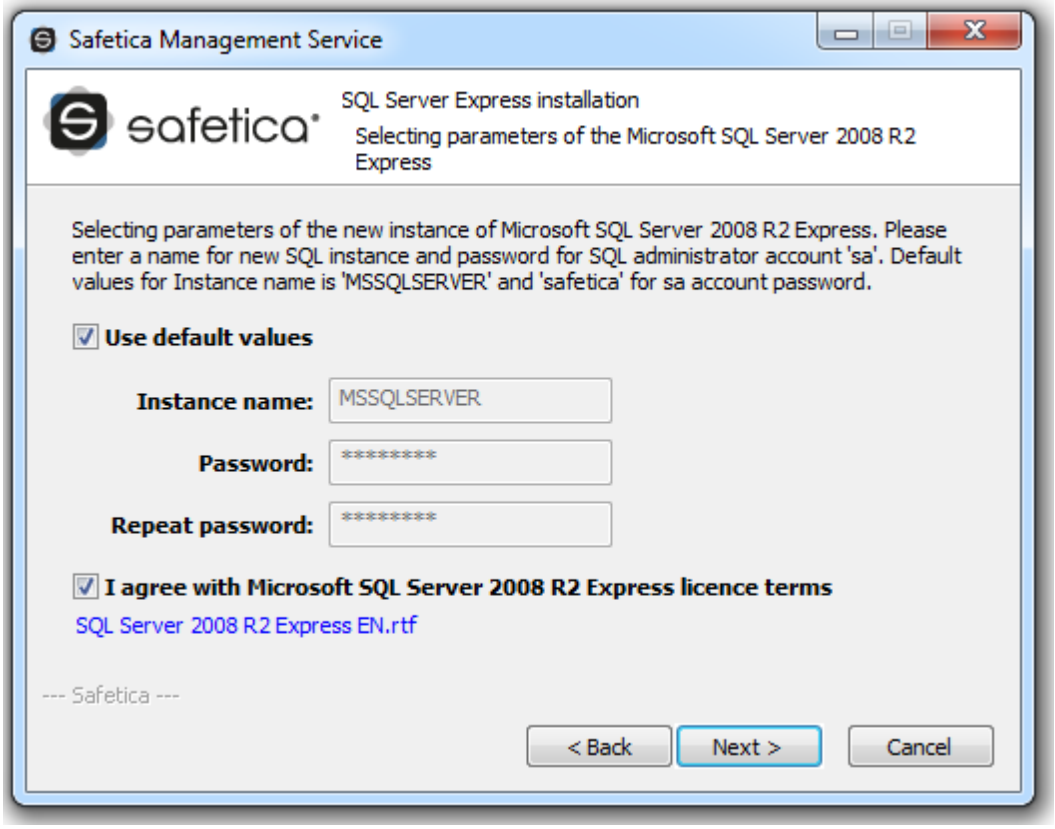
Note: The Express edition comes with the following restrictions:

- It uses only one processor.
- It uses maximum 1 GB of RAM.
- The maximum database size is 10 GB.

Due to these restrictions to the Express edition of the SQL Server, the ideal number of SECs connected to SMS with this SQL server is 50, with a maximum of 70.

In the configuration of the new SQL Server the following settings are entered by default:

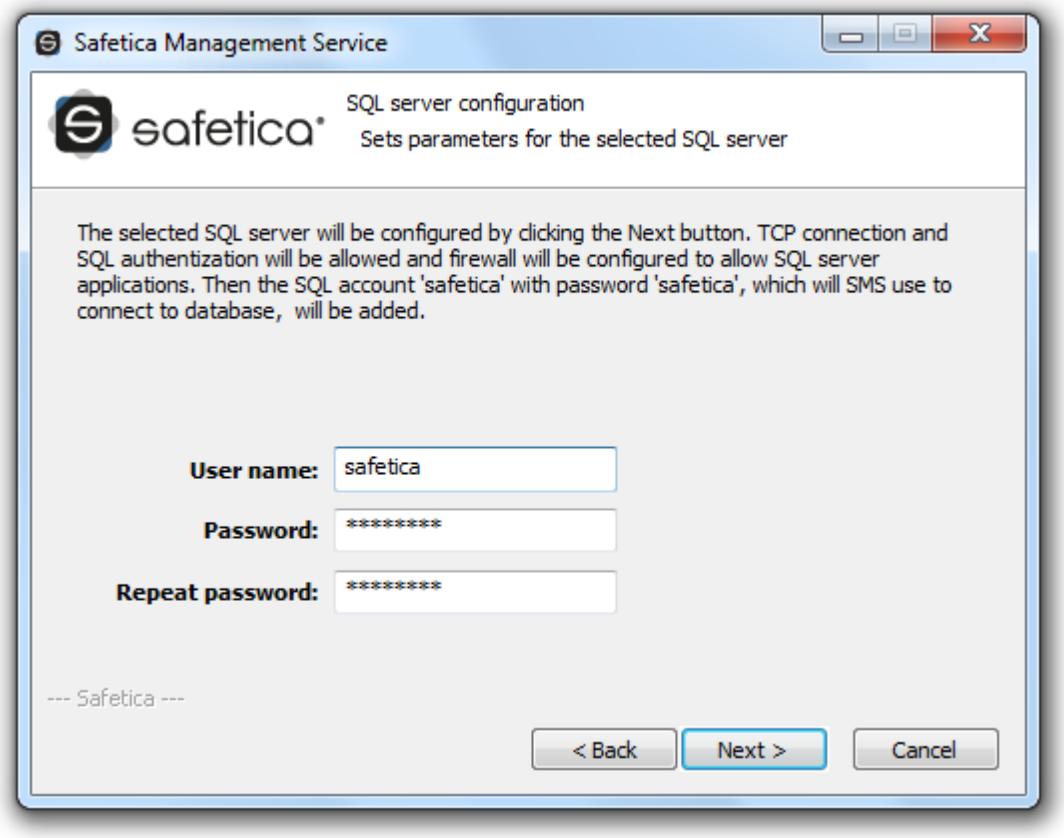
- The SQL server instance name is MSSQLSERVER.
- The default password for the user "*sa*" is set to "*safetica*". The "sa" user will be applied for access to all three databases.



After clicking the *Use default values* button, you can change the data shown above. For security reasons, we recommend using a different name for the user "*sa*".

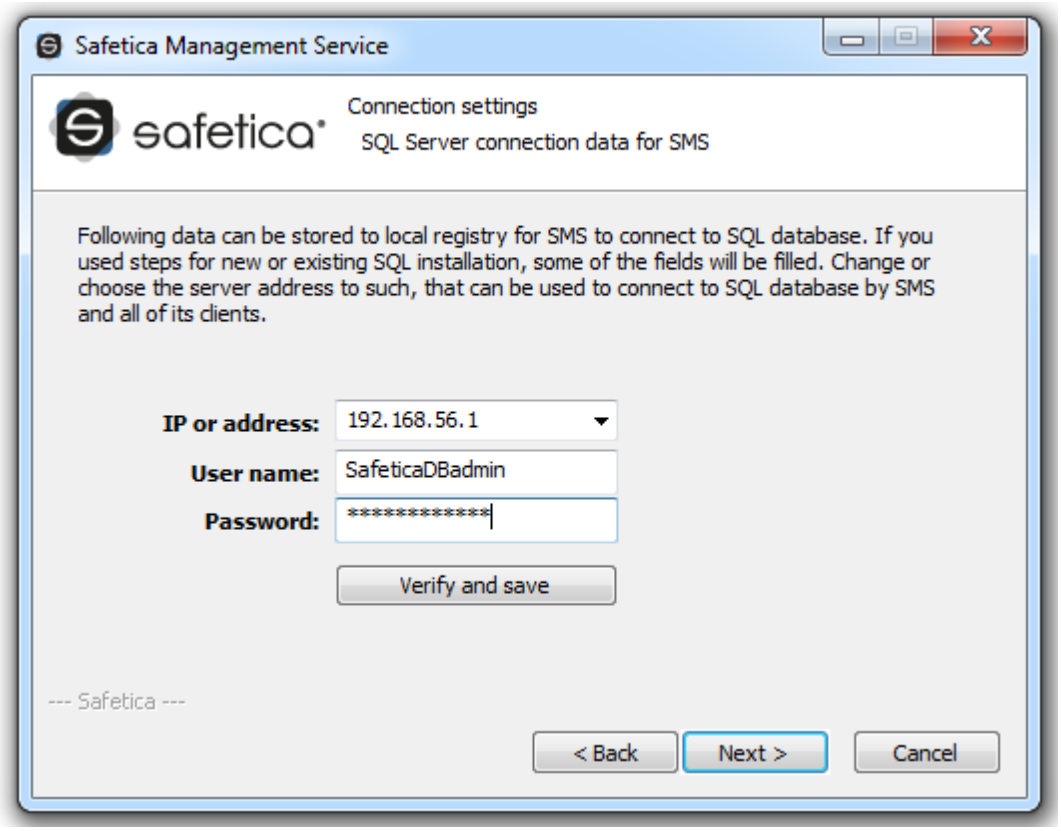
After accepting the License Terms of Microsoft SQL Server 2008 R2 Express, you can click *Next* to launch the SQL server installation.

After completion of SQL Server Express installation, click Next and enter the SQL server user name and password for the server that will be used for database access. The default user is *safetica* with password *safetica*. For security reasons, we recommend changing the default user password *safetica*.



Click Next.

When SQL server configuration has been completed, click Next and confirm the settings for SQL server connection in the following dialog by clicking *Verify and save*. Click *Next*.



Continue and finish Safetica Management Service installation. After successful completion of the SMS installation, three databases will be created on the SQL server:

- safetica_main – used for storing and sharing settings between SMS and SEC.

- safetica_data – used for storing data recorded from clients (SEC).
- safetica_category – used for storing applications, websites and appendices categories.

Note: You can later change the connection to the Safetica Management Service via the Safetica Management Console in the Server settings section. The configuration of this connection is described in the section Safetica Management Service Configuration.

3.2.3 Configuring existing SQL Server Express

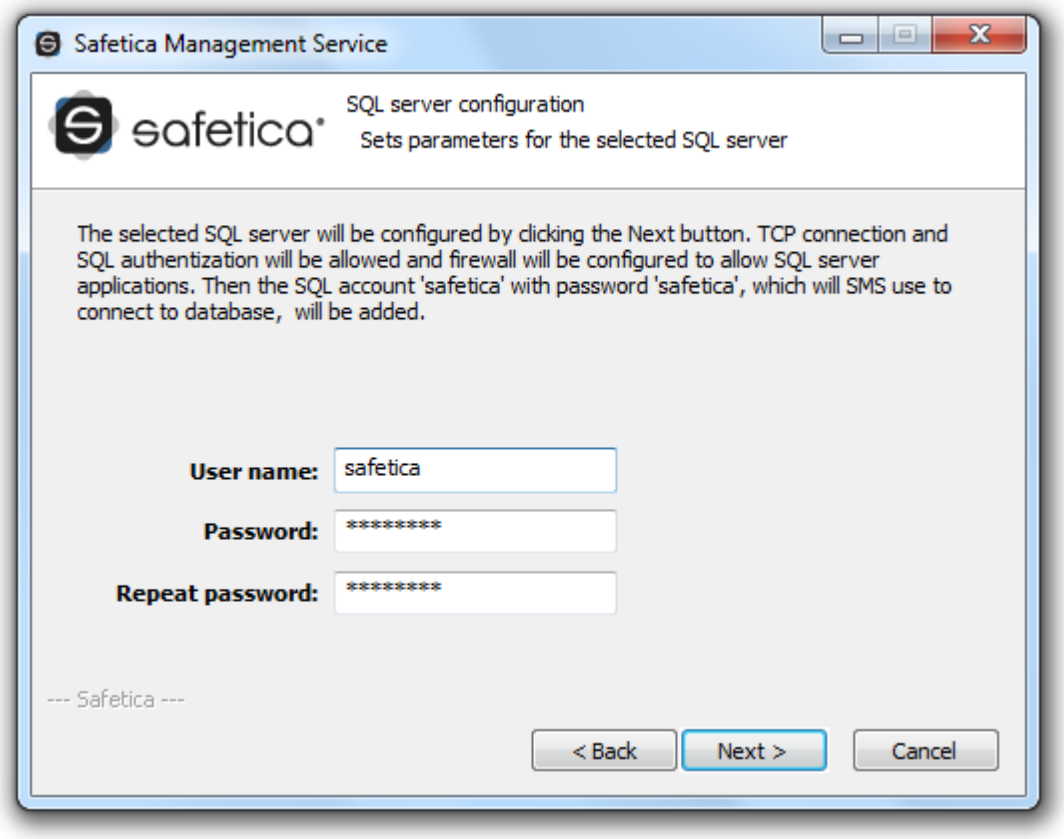
If you have Microsoft SQL Server 2008 R2 Express already installed on the PC where you are installing the Safetica Management Service, you can use it for creating the databases. The installer will automatically re-configure the existing SQL server installation on that PC. SMS will automatically connect to this instance and create the respective databases after installation.

Note: The Express edition comes with the following restrictions:

- It uses only one processor.
- It uses maximum 1 GB of RAM.
- The maximum database size is 10 GB.

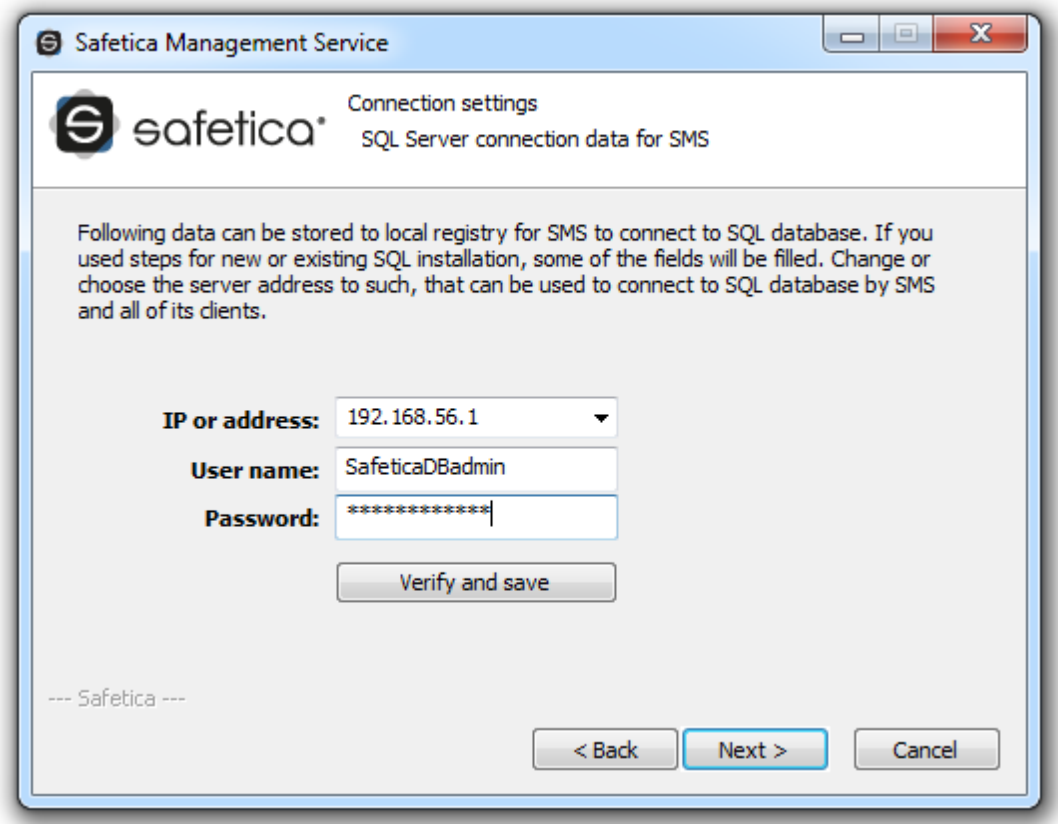
Due to these restrictions to the Express edition of the SQL Server, the ideal number of SECs connected to SMS with this SQL server is 50, with a maximum of 70.

In the first dialog enter the SQL server user name and password for the server that will be used for database access. The default user is *safetica* with password *safetica*. For security reasons, we recommend changing the default user password *safetica*.



Click *Next*.

When SQL server configuration has been completed, click Next and confirm the settings for SQL server connection in the following dialog by clicking *Verify and save*. Click *Next*.



Continue and finish Safetica Management Service installation. After successful completion of the SMS configuration, three databases will be created on the SQL server:

- safetica_main – used for storing and sharing settings between SMS and SEC.
- safetica_data – used for storing data recorded from clients (SEC).
- safetica_category – used for storing applications, websites and appendices categories.

Note: You can later change the connection to the Safetica Management Service via the Safetica Management Console in the Server settings section. The configuration of this connection is described in the section Safetica Management Service Configuration.

3.3 Installation of Safetica Management Console

The console is the central point for managing the software. It is used for setting up and managing both Safetica Endpoint Clients (SEC) and Safetica Management Services (SMS) as well as for database management, and of course for the management of Safetica modules. The console also shows statistics, charts, and monitoring outputs. By using the Safetica Management Console (SMC), you can manage multiple instances of SMS. All you need is a SMC running on any computer that can access the managed SMS. Neither the number of console installations nor the number of its users is limited by the license.

Proceed with the installations as follows:

1. Launch the universal installer that you have previously downloaded. After selecting your language and agreeing to the license terms, go to Installation -> Safetica Management Console.
2. Here you several options:
   - Run the setup directly from the universal installer by clicking on the *Run installer* button.
   - Extract only the SMC installer, which you can then use separately for later installation.

     Note: In the third part Tools and Components are components that are necessary for

proper function of Safetica Enpoind Client or Microsoft SQL Server 2008 R2 Express. If you will be installing Microsoft SQL Server 2008 R2 Express from the installer, make sure you have installed the component Microsoft Installer 5.4. If not, install it from here.

3. After running the installer (either from the universal installer or from the extracted one), select your language once again and accept the license terms. Select the installation folder and complete the installation.
4. Finally, verify that you have added exceptions to your firewall and antivirus for the STConsole.exe process.

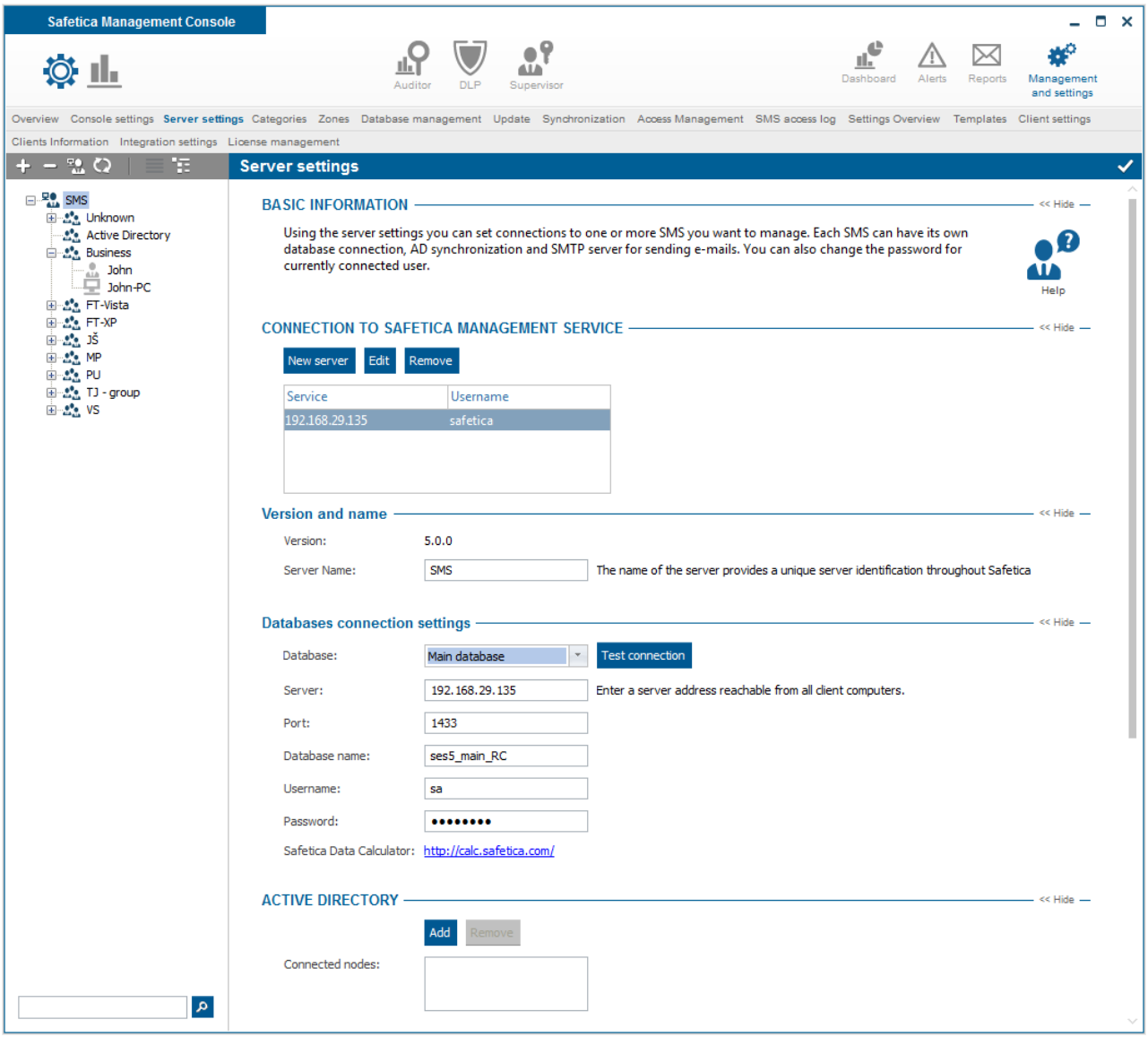
3.4 Configuration of Safetica Management Service

After successfully installing the Safetica Management Console (SMC) and Safetica Management Service (SMS), the entire system must be properly configured before you can begin installing Safetica Endpoint Client on the endpoint computers. All administration and settings are carried out via SMC.

The main configuration steps are as follows:

1. Launch SMC and enter a new access password for the console.
2. Connect SMC using Management and settings -> *Server settings* to the relevant server component of SMS by providing the default credentials, login name safetica and password safetica.
3. Use SMC to update the database of categories. To do this, go to Management and settings -> *Categories*.
4. Change the default password for the default SMS account (safetica). To do this, go to *Management and settings -> Server Settings -> Change connected SMS user password*. Select the appropriate server and change your password (you must be logged into the server with your safetica account to be able to do this).
5. 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.

   This part of the setup is not essential, but the category functions will not be available without it.
6. If you have a license number, enter it into *Management and settings -> License management*. 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 have installed and connected the client to the server, again in the same view.



Additional recommended steps

- When you are using Active Directory services 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 Active Directory group in the user tree.
- If you have installed several SMS on your company network, we recommend repeating the above-mentioned steps on all of these SMS. Display the Server settings again to connect to another SMS; this can be displayed by entering Management and settings -> Console settings in the main SMC menu. Click on the New server button and enter the connection information. Use the console to connect to every SMS. First, change the password in the default administrator account. Then go to Management and settings -> Access management and create the appropriate access accounts for each SMS with various access rights based on your company security policies. Each SMS has its own separate access accounts. Examples of possible accounts and their access rights:
  - Security administrator – can access module settings DLP and Supervisor. Cannot view any data obtained through employee monitoring.
  - Manager – can display data obtained through employee monitoring in all modules, cannot change any settings.
  - Auditor – can change the settings of the Auditor module and view data obtained through employee monitoring.

Of course, you may arbitrarily change the access rights for individual users to any SMS. For more information about setting up accounts and access rights for individual modules and functions, see Access management.

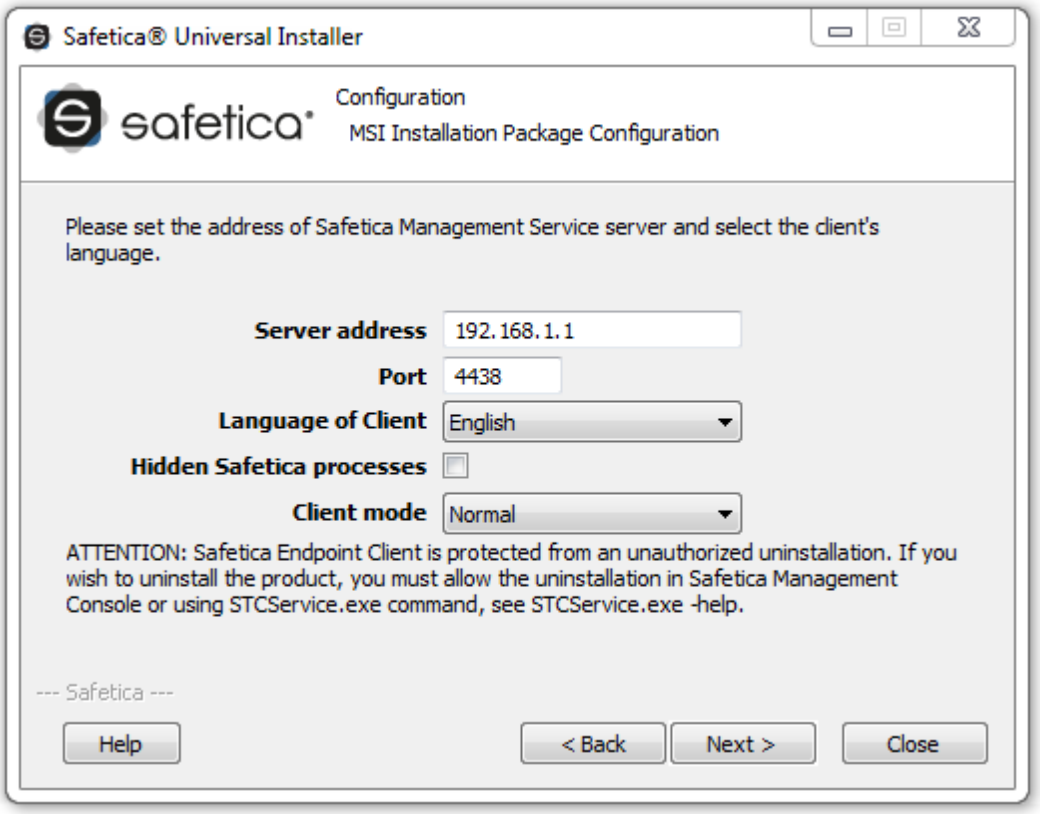
3.5 Installation of Safetica Endpoint Client

Safetica Endpoint Client (SEC) is the last component of the Safetica product that you need to install. It is an essential component. On the client computers, it ensures the enforcement of security policies and ensures that all the functions configured in Safetica Management Console (SMC) run properly. For end users, it can also provide a set of security tools for their own use.

Proceed with the installations as follows:

1. Launch the universal installer that you have previously downloaded. After selecting your language and agreeing to the license terms, go to *Installation* > *Safetica Management Client x86* or *x64* – this depends on which operating system version is installed on the endpoint.
2. Here you several options:
   - Run the setup directly from the universal installer by clicking on the *Run installer* button.
   - Extract only the SEC installer, which you can then use separately for later installation.

     Note: In the third part Tools and Components are components that are necessary for proper function of Safetica Enpoind Client or Microsoft SQL Server 2008 R2 Express. If you will be installing Microsoft SQL Server 2008 R2 Express from the installer, make sure you have installed the component Microsoft Installer 5.4. If not, install it from here.
3. You will be asked to enter the following information before extraction or running the installer:
   - *Server address* – address of SMS for SEC to connect to.
   - *Port* – port on which the SMS listens. The default is 4438.
   - *Language of client* – language of SEC.
   - *Hidden safetica processes* – all SEC processes are hidden immediately after installation when this is checked (*STCService.exe, STPCLock.exe, STMonitor.exe, STUserApp.exe,* and *Safetica.exe*). This can always be changed by going to Management and settings -> *Client settings* -> Hide safetica processes.
   - *Client mode* – graphical interface mode of Endpoint Security Tools. This can always be changed by going to *DLP* -> *Endpoint Security Tools settings* -> *Client GUI mode*.



4. After running the installer (either from the universal installer or from the extracted one), select your language once again and accept the license terms.
5. Select the installation folder.
6. After successfully completing the installation, verify that the STCService.exe service is running (Windows Task Manager > Services > STCService – running).
7. Finally, make sure that in your firewall and antivirus you have established exceptions for the following processes: STCService.exe, STPCLock.exe, STMonitor.exe, STUserApp.exe, and Safetica.exe.

To configure SEC as well as the whole Safetica product, proceed by reading the After Installation chapter and by carrying out the configuration.

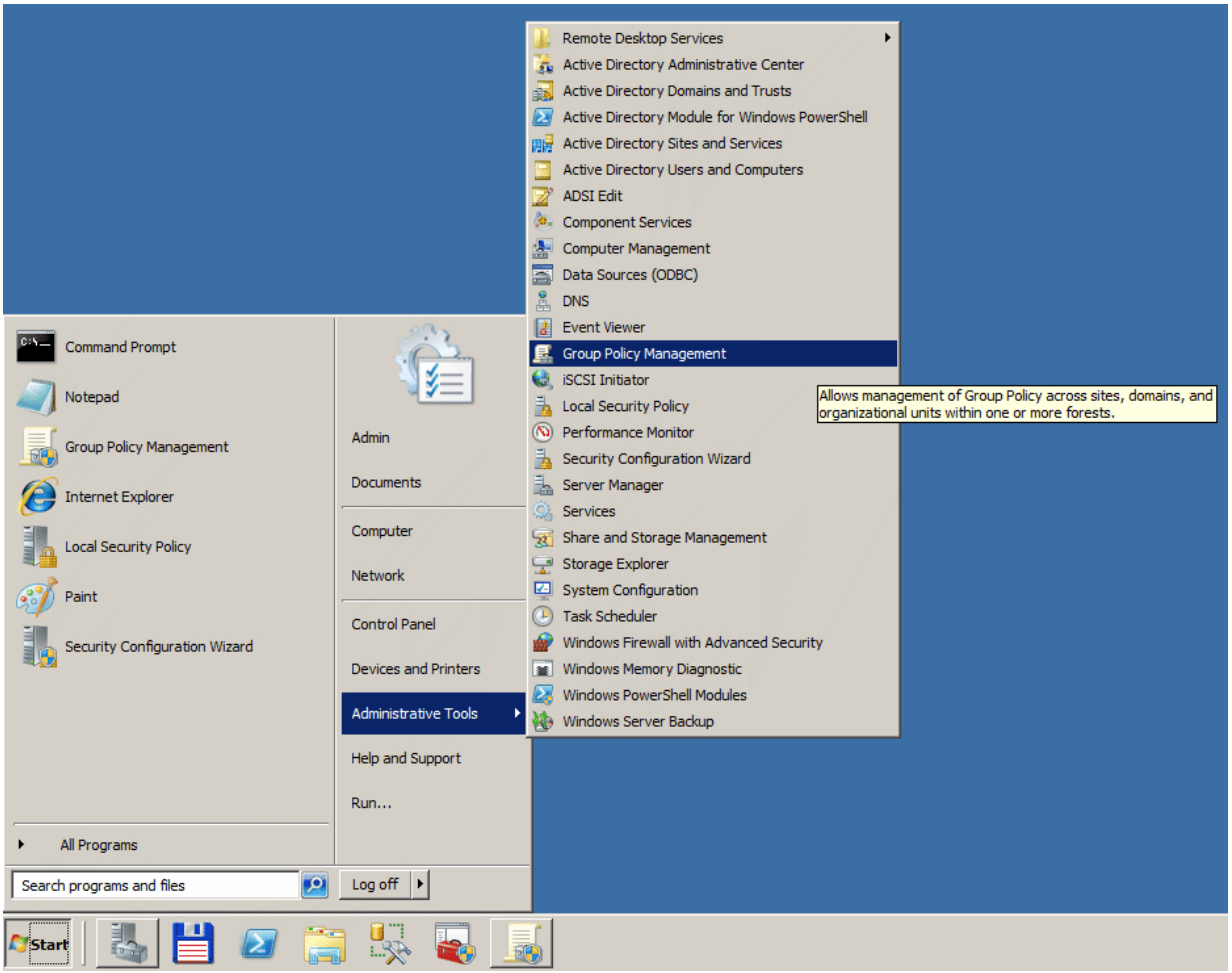
3.5.1 Installation using GPO

It is possible to perform a bulk installation of Safetica Endpoint Client using Group Policy Management. Before you can do this, it is necessary to extract the MSI package of Safetica Endpoint Client from the Safetica universal installer.

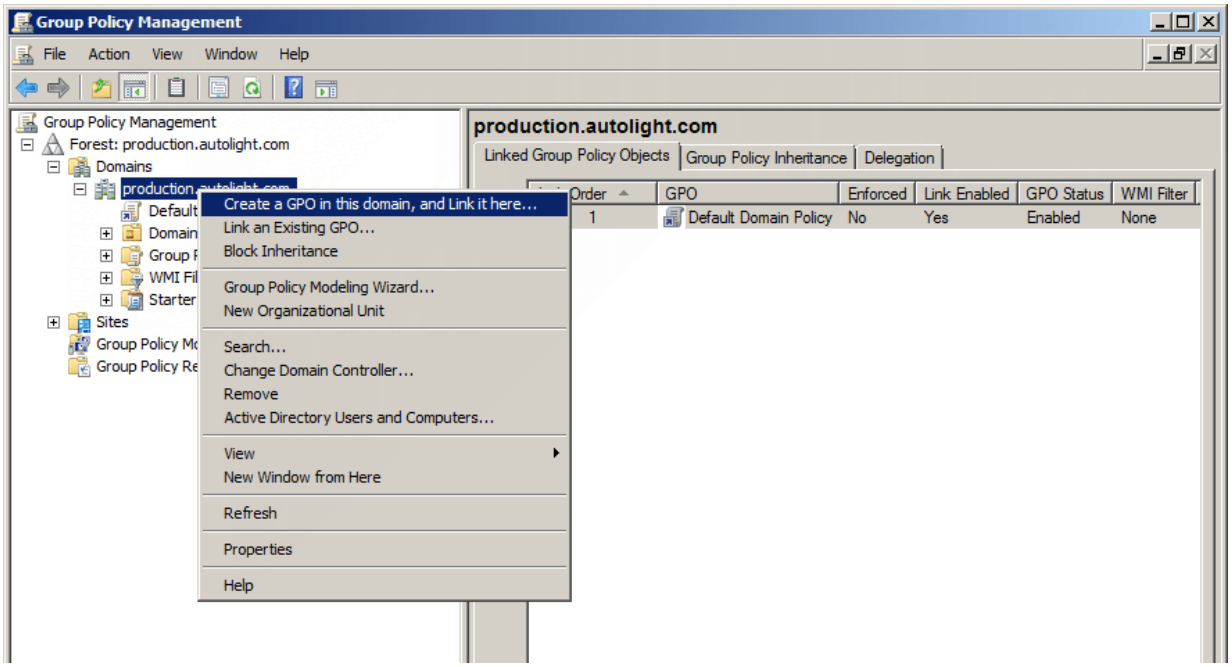
We will further describe only the first kind of installation – assign (the description herein may not always correspond to reality; depending on the version of your server system, the labels may vary). The following describes bulk installation by means of GPO on Windows Server 2008 R2:

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

tools -> Management of group policies.

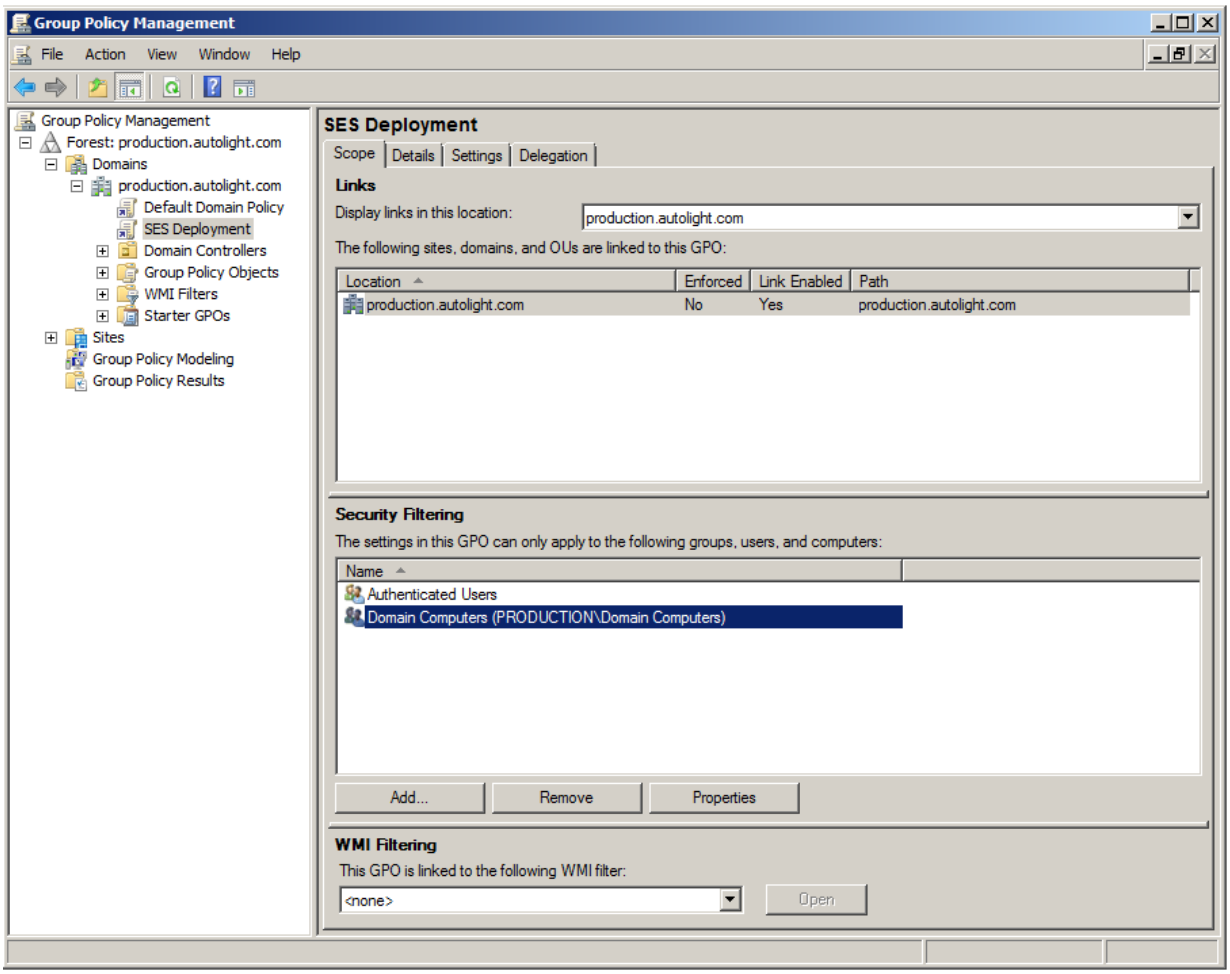


5. Right-click on the organizational unit for which you wish to deploy SES and select Create new group policies object in this domain and interconnect it...

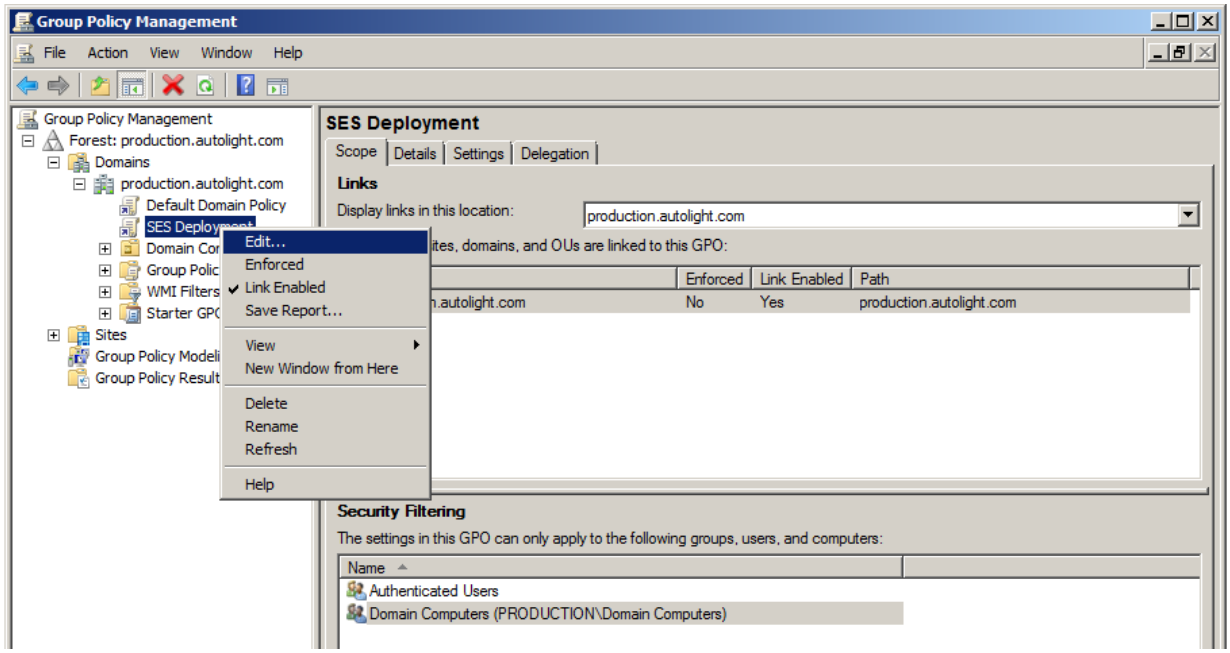


6. Give a name to the new project (e.g. SES Deployment).

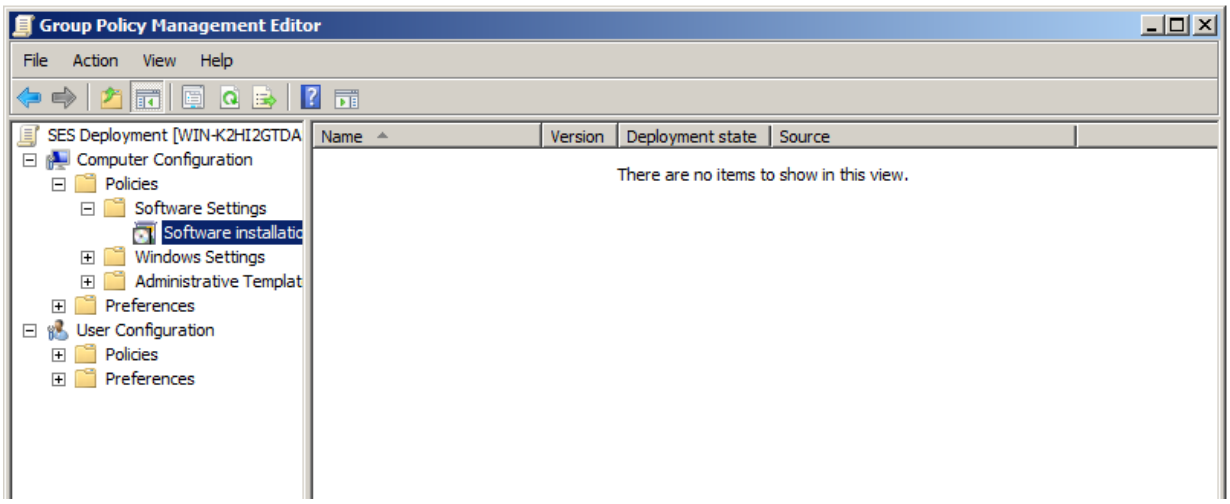
7. Select the new object on the right side of the window (the tab Scope) and add the group Domain Computers to the already existing group Authenticated Users.



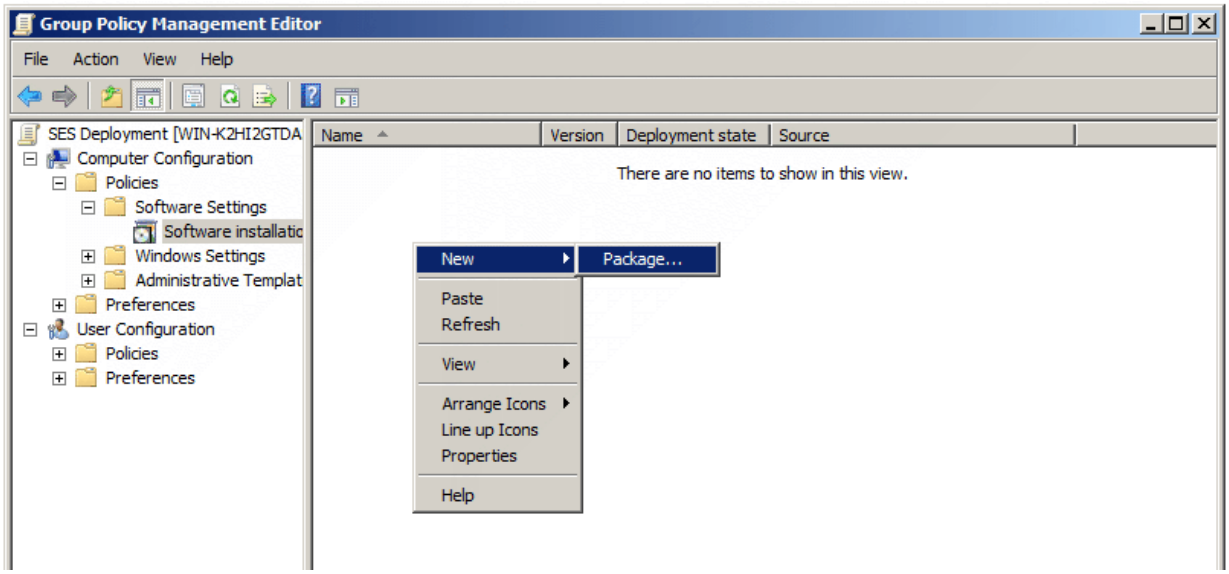
8. Select your newly created group policy and right-click on *Edit*.



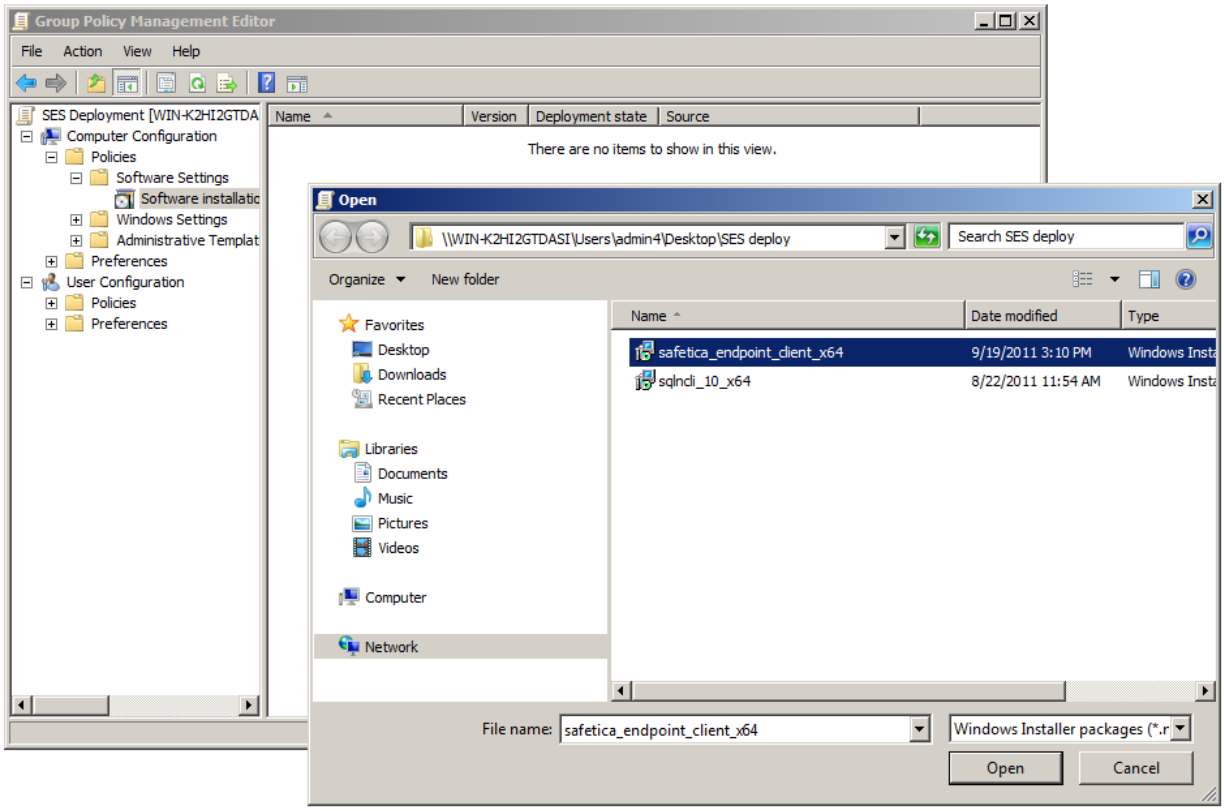
9. In the pop-up window choose *Computer setup -> Policies -> Software settings and click on Software installation*.



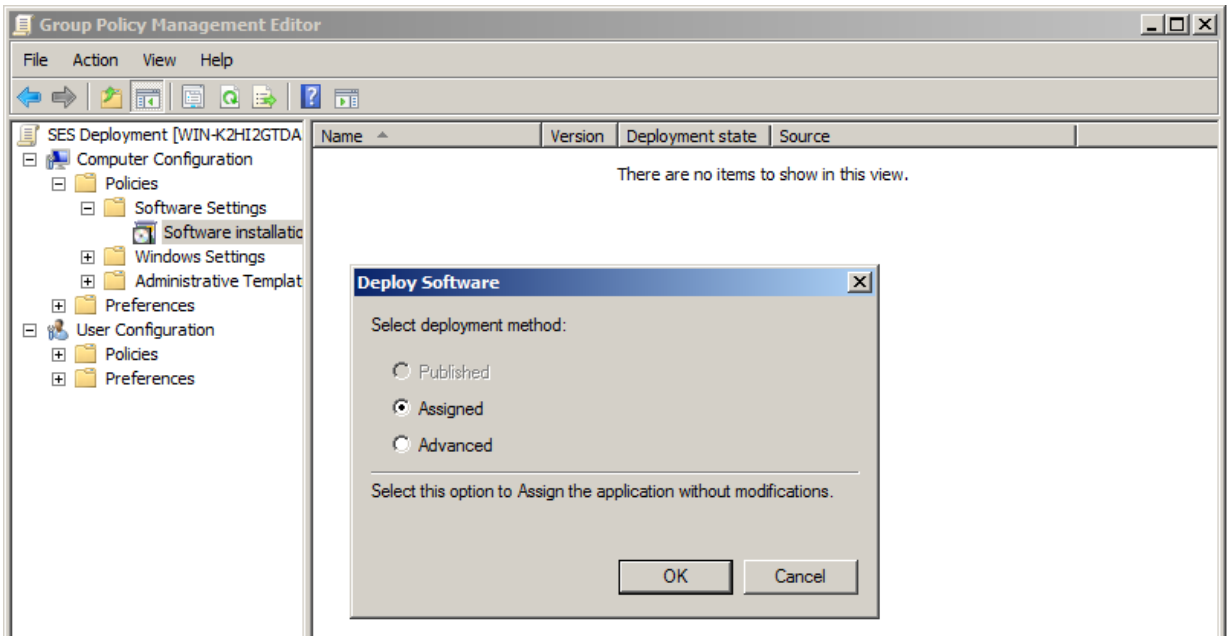
10. Right-click on the window in which software is listed and select New item -> Package...



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

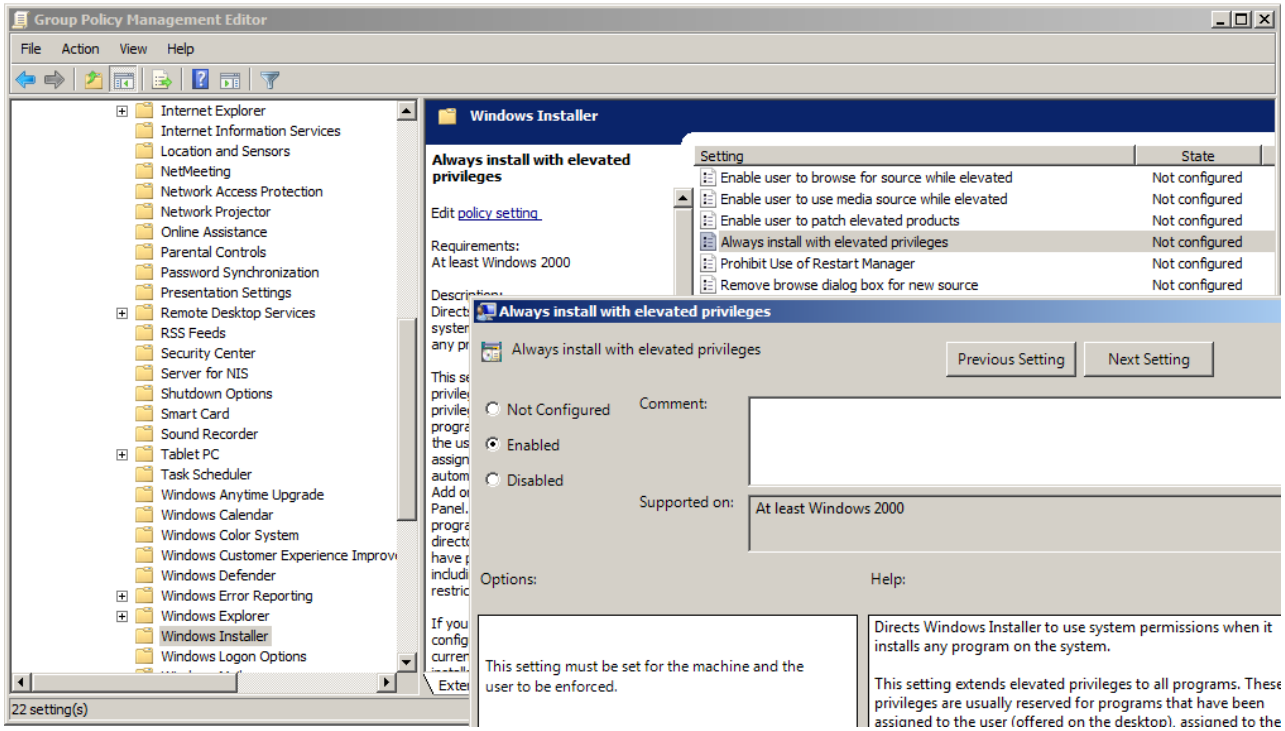


12. In the next dialog window, select Assigned and confirm.

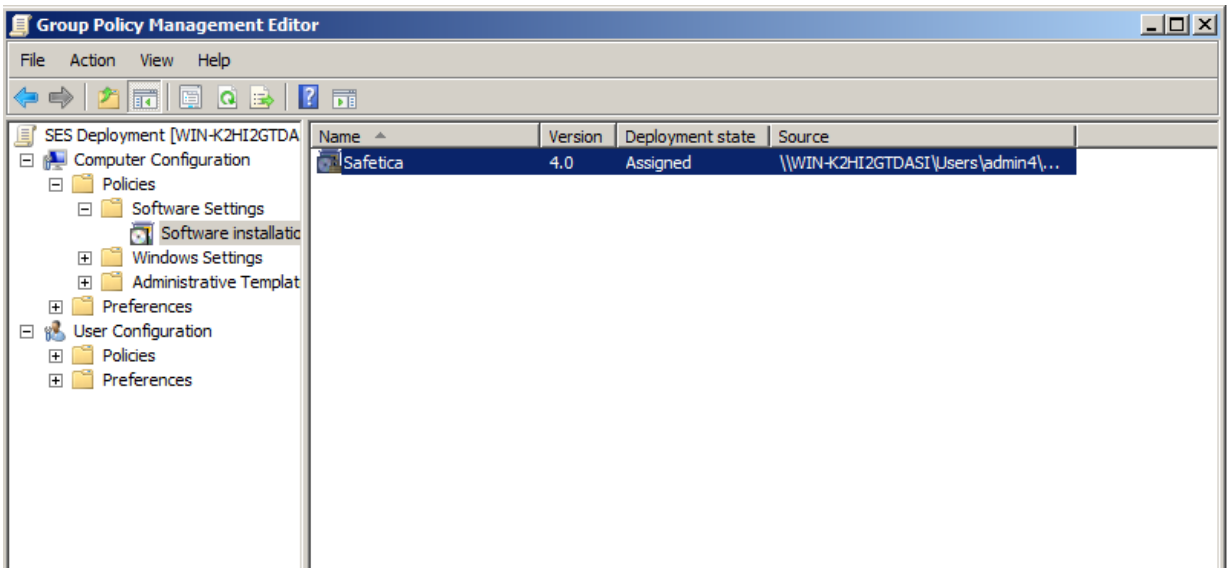


Warning! When installing from the 32-bit MSI package, it is necessary to disable installation onto 64-bit systems. You can do this by selecting the deployment method in Advanced -> *Deployment -> Extended -> Specify ->* and uncheck *Make this 32bit version of X86 application available for computers with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

13. 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 onto end stations successfully and smoothly.



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



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

For configuration and settings of the whole Safetica proceed to After installation.

3.6 After installation

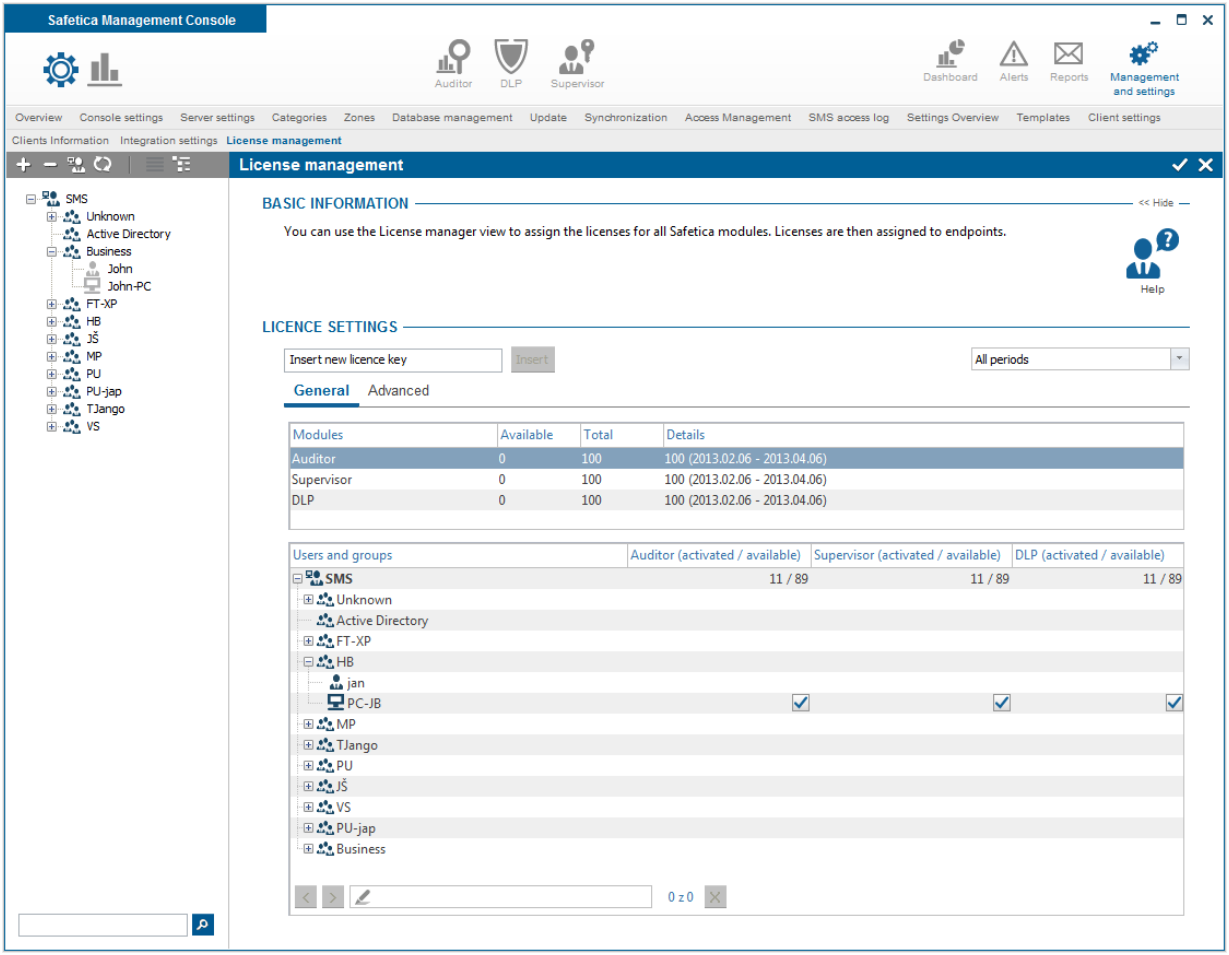
Once you have installed all Safetica components, you are left with just a few final steps to take before you can start using Safetica.

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.

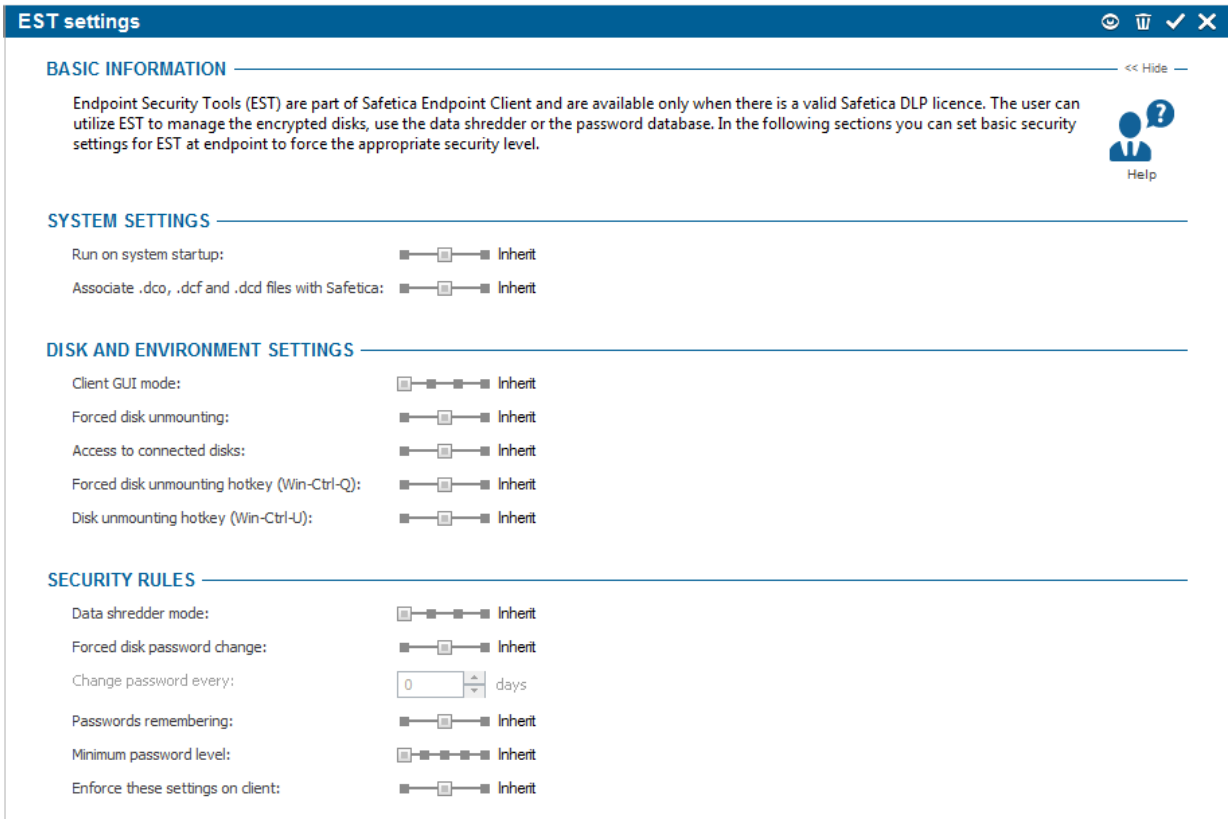
   - John-PC / John — SEC is online and connected to SMS.

- 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.



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:
   - *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.



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

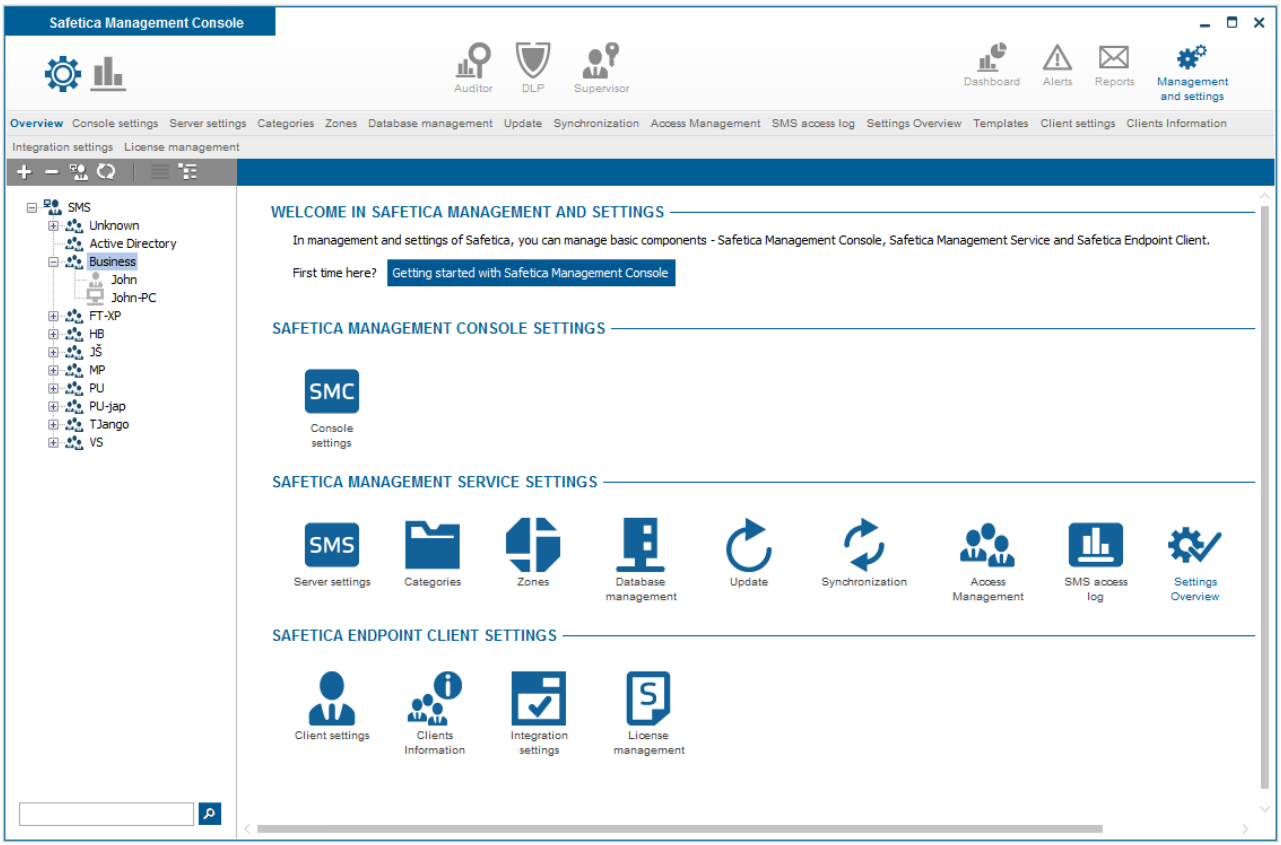
At this point, Safetica is now ready to use.

4 MANAGEMENT OF SAFETICA

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. Displaying and settinging 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.

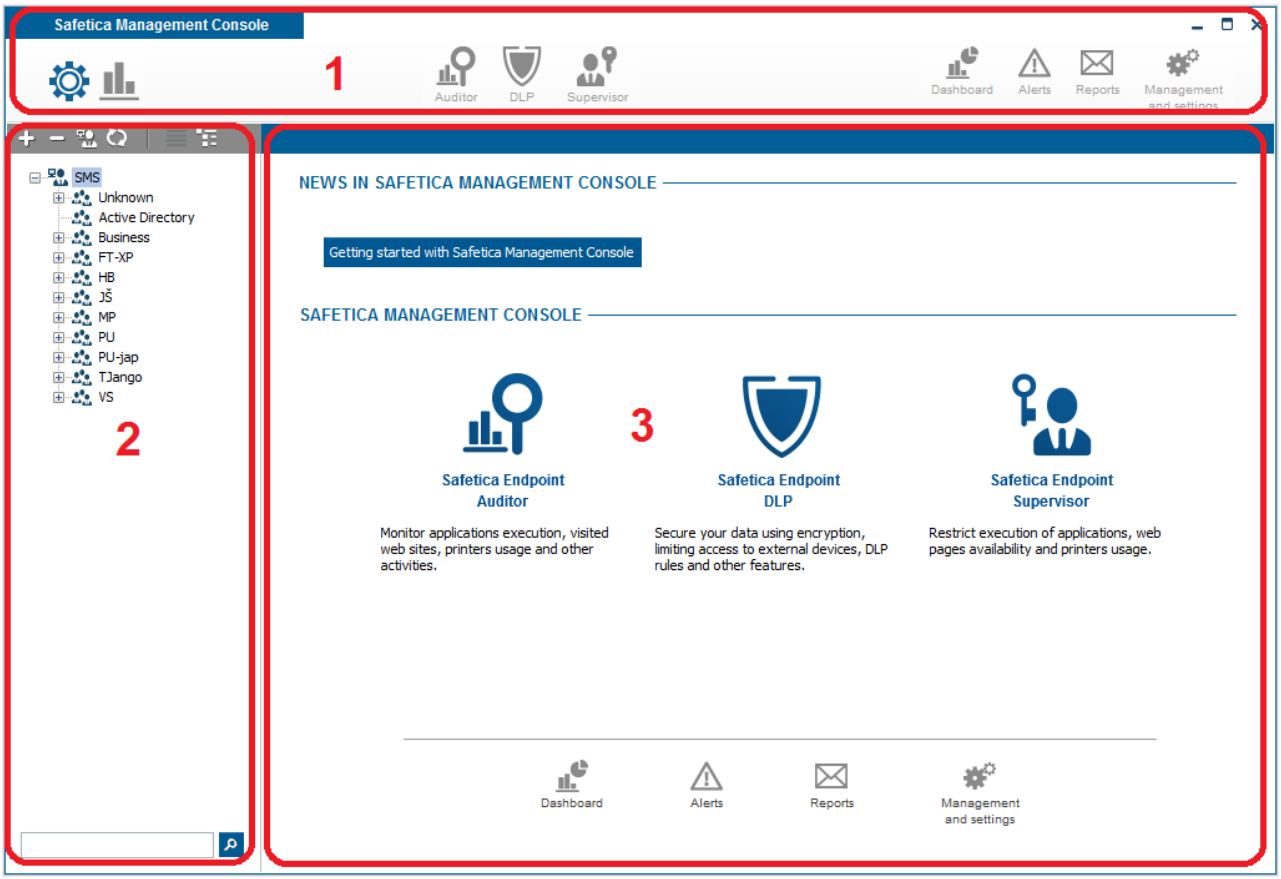
The Safetica Management Console can run anywhere you have a connection to server services. The number of console installations and number of users are not limited by the license.


Safetica Management Console
Auditor
DLP
Supervisor
Dashboard
Alerts
Reports
Management and settings
Overview
Console settings
Server settings
Categories
Zones
Database management
Update
Synchronization
Access Management
SMS access log
Settings Overview
Templates
Client settings
Clients Information
Integration settings
License management
SMS
Unknown
Active Directory
Business
John
John-PC
FT-XP
HB
JŠ
MP
PU
PU-jap
TJango
VS
WELCOME IN SAFETICA MANAGEMENT AND SETTINGS
In management and settings of Safetica, you can manage basic components - Safetica Management Console, Safetica Management Service and Safetica Endpoint Client.
First time here?
Getting started with Safetica Management Console
SAFETICA MANAGEMENT CONSOLE SETTINGS
Console settings
SAFETICA MANAGEMENT SERVICE SETTINGS
Server settings
Categories
Zones
Database management
Update
Synchronization
Access Management
SMS access log
Settings Overview
SAFETICA ENDPOINT CLIENT SETTINGS
Client settings
Clients Information
Integration settings
License management

4.1 Safetica Management Console

4.1.1 Interface Description

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



1. Main menu

On the left you will 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 have an overview of data obtained through monitoring, summaries, graphs, logs of blocked entries, logs of your employees' activities and other logs depending on which part of the console you are currently browsing. The data is displayed for the selected group, user, computer or branch and for the selected time period.
- *Setting mode* – this mode allows you to configure the behavior of individual functions and modules. This does not include settings of the console itself. The mode allows you to specify the behavior of each function in every module (allow, block or specify other details of its behavior). All changes of settings made in the settings mode will only take effect only after saving. To save, press the  button in the top right corner of the view. The changes can also be cancelled by pressing the  button at the same location.

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, re-

ports, 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 how regular reports and summaries are sent.
- *Management and settings* – management and settings of the SEC, SMC a SMS

Switchers for individual module functions can be found under the upper toolbar. These switchers change based on which module you are currently in. (Auditor, 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" refers to the Safetica Management Service together with a database and a connected client station (Safetica Endpoint Client). The drop-down list above the tree contains the branches which the console is currently connected to. You can set a new connection to the branch in the Server settings. This list allows you to either select a single branch, the items of which will be displayed in the tree, or all branches at once. In this case the root items of the tree will represent individual branches. For more information about Safetica Management Service and division into individual branches, see Architecture.

By selecting an item in the user tree you can select the users, computers, groups or branches whose settings you want to change or whose records you wish to view. The same goes for the visualization mode. You can also select multiple items at the same time by holding down Ctrl or Shift and selecting them with the mouse.

More information about using the user tree for visualization and settings can be found in the section Working with visualization and settings modes.

You will also find the search field and other control panels of the list above the user tree itself:

- The button  will expand all nodes in the user tree.
- The button  will collapse all nodes in the user tree.
- The button  switches between displaying computers, users or both together. Division into groups remains the same.
- The button  updates the user tree.

Other operations over the user tree, such as adding computers and users, deleting or renaming them, copying, etc., are found in the context menu opened by right-clicking on the user tree or individual items.

Built-in groups

Safetica Management Console contains built-in groups in the user tree based on the type of installation. There are two built-in groups:

- *unknown* – cannot be deleted. Default group for newly connected computers or users.
- *Active Directory* – cannot be deleted. This is used for Active Directory synchronization.

New users and computers are placed into *unknown* group after a new client station (Safetica Endpoint Client) is connected. You can then move or copy these users and computers from the unknown group into your custom groups. If you delete a user or computer from your own group, they will be moved back into the unknown group. You can completely delete users or computers by deleting them in the unknown group.

An Active Directory group is present, which is used to synchronize with Active Directory. You can select the Active Directory tree in the settings and, after confirmation, users and computers will be copied into the AD group. This group is read-only, so you cannot create new users and computers here nor delete existing ones, but you can copy them into your custom groups. The AD group is only used as a connection between the Active Directory tree and the user tree in Safetica Management Console.

Other properties of the user tree

- Groups can be nested, so one group may have several subgroups. However, each group can only have a single parent group.
- Groups may contain users and computers.
- Users and computers may be copied into several groups (the same user or computer may be present in several separate groups or branches simultaneously).
- If a user or computer is grayed out, it means that they are currently offline. All settings that you set concerning those users or computers will only be evident when the user or computer is on-line again.
  - o  computer is online.
  - o  user is online.
  - o  computer is offline.
  - o  user is offline.

3. Display area (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.). When describing individual functions we will refer to this area as the view area.

To switch between individual module functions, select a 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.

4.1.2 Console settings

In this setting you can change the SMC language or access password. Note that by changing the password here, you only change the password for launching your console. It will not change the password of your account used for the connection to SMS!

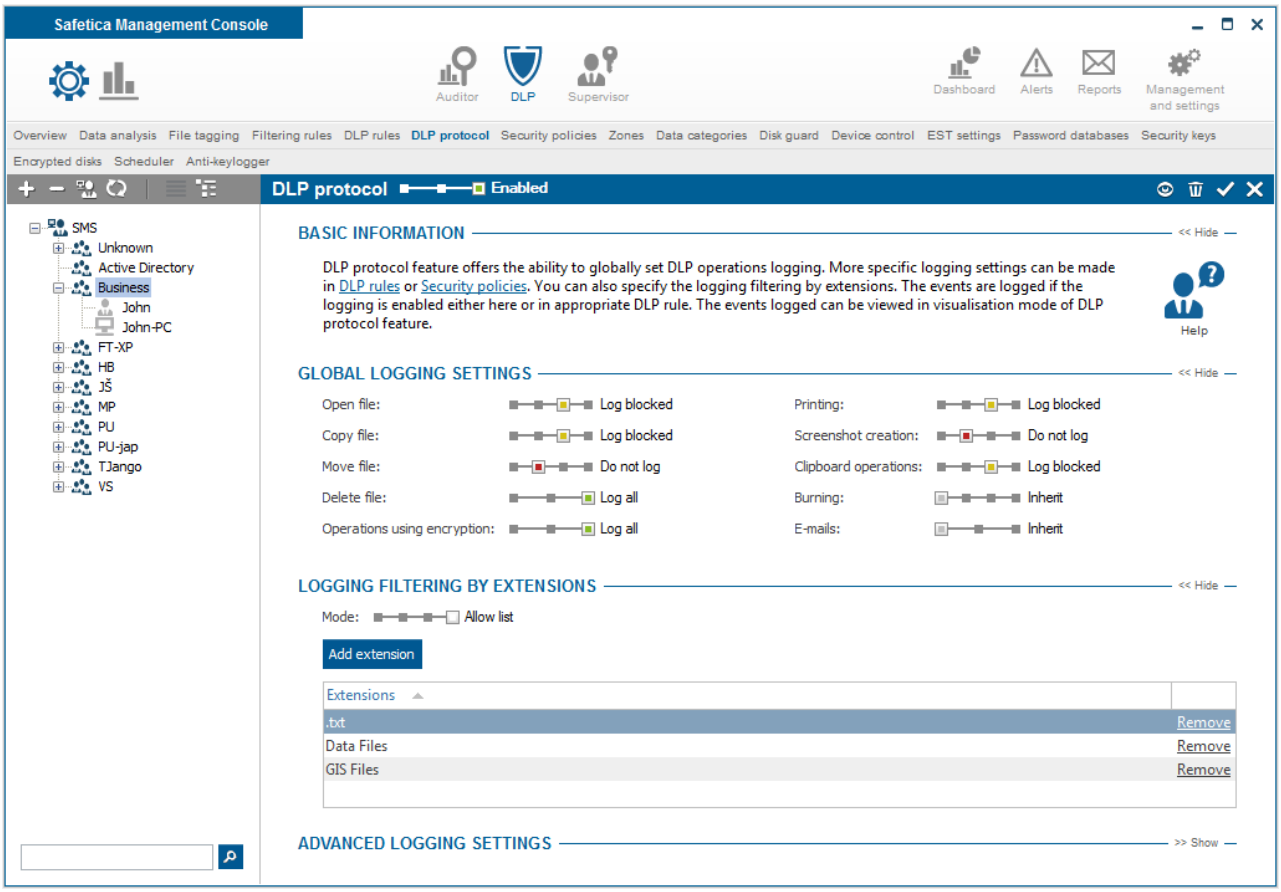
Confirm changes by pressing the  button.

4.1.3 Working with setting and visualization mode

4.1.3.1 Setting mode

The user tree contains a list of branches, groups, users and computers (entries). The root entries are always individual branches that Safetica Management Console is connected to. The behavior of a branch in the user tree is the same as that of a group. The only difference is that a branch cannot be copied, moved, deleted or inserted into other groups or branches.

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



Settings that are made using the user tree have the following properties:

Setting mode

You set the 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.

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 must save the changes by clicking on  . You can cancel the changes you have made by clicking on  in the upper right corner.

Setting inheritance

- You can create settings for users, groups (including branches) and computers by means of the user tree in the console.
- A setting is inherited from a group to its subgroups, users or computers. A setting made for a group is also set for all subgroups, users and computers in this group.
- A setting on the lower level of the user tree is considered more strict, and therefore of higher priority. For example, if you create settings for a group and then for users or computers within this group, the decisive setting is the one made for users or computers. Such a setting is called an explicit setting. Settings for a group and its subgroups, users or computers have to be calculated (joined) based on a pass through the user tree from the lowest object (of a high priority) to the root or branch (of lower priority). Calculated settings are called effective settings.

- You can delete an explicit setting in the function by pressing the button  . Every setting is set to a default value.

In short:

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

Calculation of an effective setting

The Safetica Management Console always displays the *explicit setting*. Using the  button, it is possible to have the effective setting displayed for the current feature and highlighted items in the user tree. However, these settings always have to be calculated, which may take more time.

As described above, the calculation is made from leaves (e.g. a user or a computer) in the user tree to the tree root. The setting saved for a user has a higher priority than the settings made for the group that the user belongs to. The join is made in the following way: Where there is nothing set for the user, the setting of his group is used. If some settings are available for the group as well as for the user, those of the user will be effective. This applies to nested computers and groups as well.

Computer or user in several groups

You can copy computers and users to several groups. If a user or a computer is contained in several groups, the following steps will be performed in order to calculate their effective settings:

1. Effective settings are calculated for each path, in which the user or computer is located, so the result is two (or more) effective settings. 2. These settings are joined into one by taking the "stricter" one. For example:
   - Setting of *Enable* vs. *Disable* is joined to *Enable*. Example: enabling the application monitoring.
   - Interval values are always joined into the stricter interval. For example, if the screenshot interval is *one minute* in one group and *two minutes* in another one, the final setting is *one minute*.
   - For some features, such as Application control or Web control, a list of rules is created and it is possible to specify the type of rules: either Allow list, or Deny list. If this setting differs, the Allow list is applied.
   - If the types of lists (*Allow list* or *Deny list*) are the same, the lists are joined into one. Lists are joined if their mode (*Deny list*, *Allow list*) is the same.

Settings for a user and a computer

The user tree allows creating settings for users and for computers. Settings for a computer are applied to each user logged from the given computer in the following way:

1. The resulting settings for the user at the given computer are calculated by joining the *effective settings* for the given user and the given computer.
2. The result of joining the settings for the computer and for the user is the final setting that is joined automatically in the following way.
   - Anything that is not set for the user will be taken from the computer settings.
   - The default setting will be used, if nothing is set neither for user or computer. Default settings are described with individual features.

- Anything that is set for both is applied based on the priority that can be set for each module in Client settings. By default (when nothing is set), the computer has higher priority (computer settings are preferred to user settings).
- Rule lists are joined if their modes are the same. Otherwise, the selection of the list is also performed based on priority.

Data size in databases

The size of data that accumulates as monitoring proceeds mainly depends on the number of users for which you are setting up the system and on the activated functions in each module of Safetica. You can get an approximate size estimation based on these criteria by using our data calculator, which is available on the web at http://calc.safetica.com/.

General policy for using the settings

Safetica provides a wide range of possible settings in order to set the security in your branches to every detail. However, bad attitudes towards the settings can result in worse orientation through the whole system. That is why we recommend making the more complex settings only for advanced users.

If you want to keep the settings synoptical and simple, we recommend the following general policies:

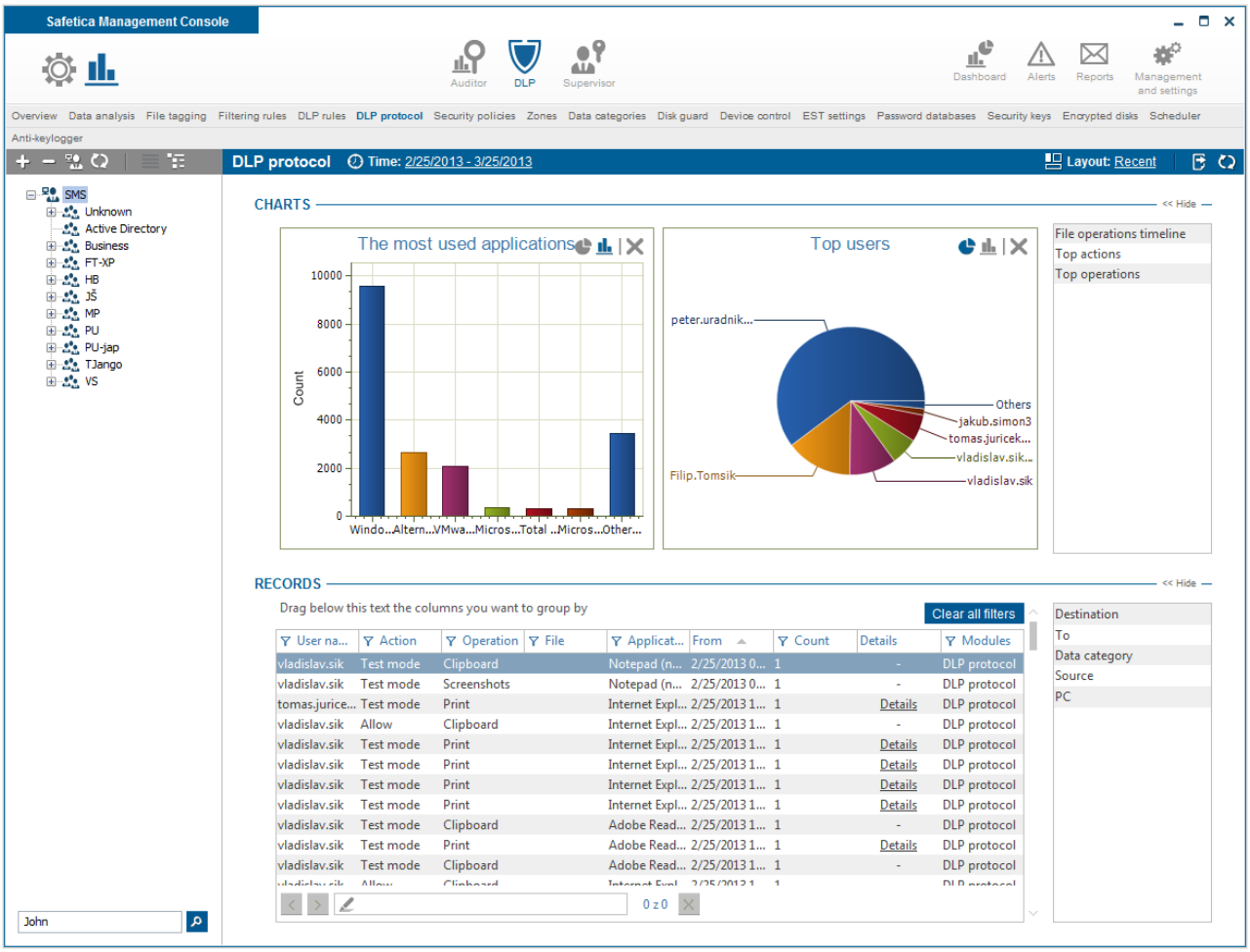
- Make the settings only for groups, not for users or computers. Then, assign the users or computers to groups according to what settings you want to apply to them.

  Example: Let us suppose that there are three departments in your company: Marketing, Development and Support. You want to run different modules and features for employees in these departments. Do not assign the settings to employees in these departments by simple selection of users in the tree. Rather, create a group for each department and assign the employees to groups. Then, make settings for each group; this way, the settings will be assigned to employees in these groups.
- If it is necessary to set something directly for a user, it means that the user is special and does not belong to that group. It is better to create a new group or subgroup for such user and assign that user to it than to change the settings specifically for that user. The reason is that you might want to make the same settings for another user in the future. In that case, you can simply reassign the respective user to the given group.
- Assigning to groups helps prevent confusion when moving to other groups. You might expect a user to inherit the settings from the group that you are moving him/her to, but in fact a setting for the user may exist which has higher priority.
- Moreover, settings directly for groups take less space in the database than separate settings for each user.

4.1.3.2 Records and visualization mode

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 the visualization mode by clicking on  button in the upper left corner of SMC.



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:
  - *Today* – records are displayed for the current day.
  - *Yesterday* – records are displayed for the yesterday.
  - *Last week* – records are displayed for the last seven days including current day.
  - *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.

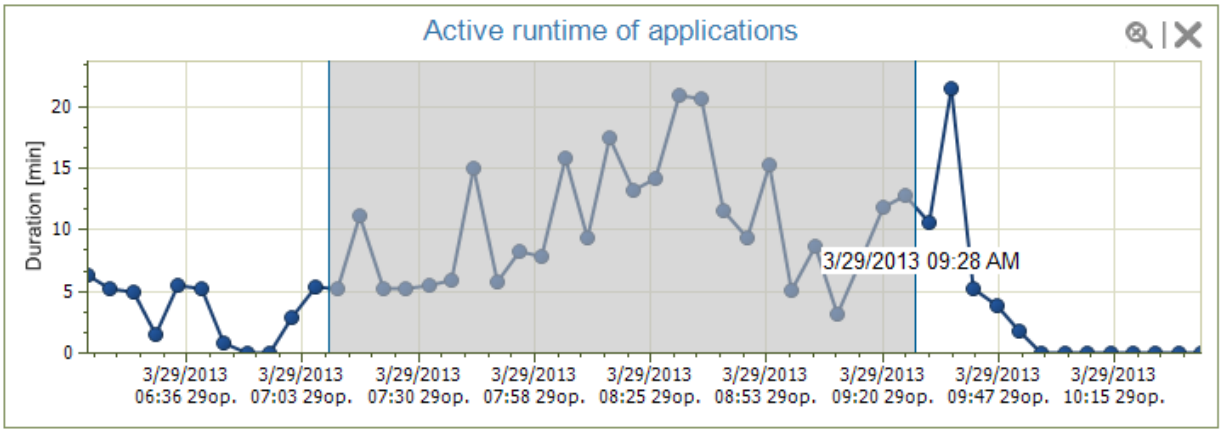
You can reload records and charts by clicking on the button in the upper right corner.

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 the 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 the pie or bar will set a filter on corresponding column and records below will be accordingly filtered. This can be done on multiple pies or bars inside the display area – multiple filters will be set. To remove the filter simply click on the pie or bar again.
- You can select time range in some of line charts by mouse selection. To cancel selection click on button.



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. Entering text will highlight the expression searched for in the table. Click on 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.

Filters

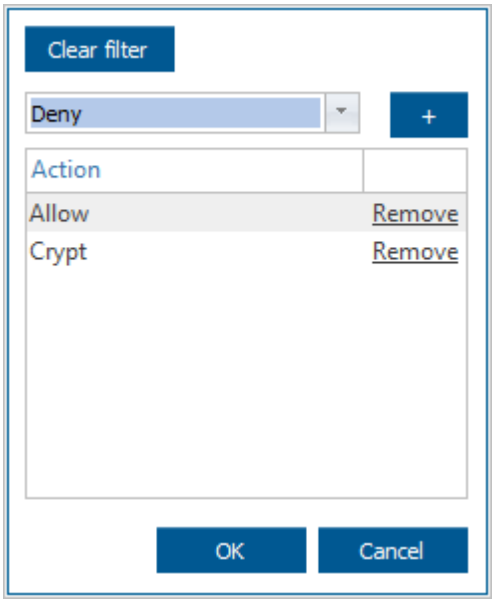
You can filter the records as well. For a column of your choice, click on the at the head of the column to open up its filter dialog. Enter text into the dialog or choose an item from the presented list in order to specify the item by which you want to sort the column. Click on the + button to add the selected item to the filter list. This list may be 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.

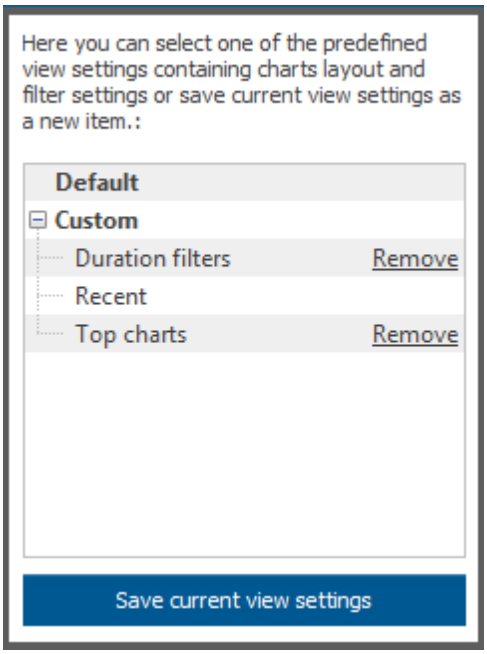
You can set a filter by clicking on the pie or bar inside the graph as was described above in Charts.

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



Layouts

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

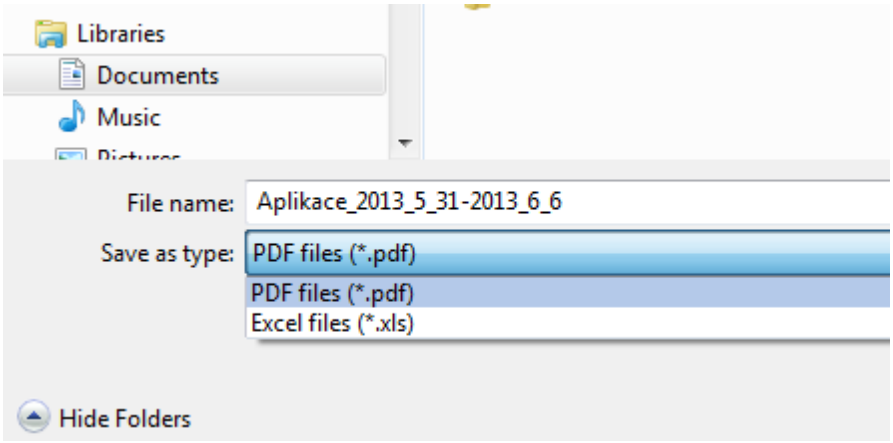


- Each SMS user can have their own visualization layouts for each function.
- You can set a default visualization layout by clicking on Default item in the layout manager.
- You can set the recently used layout by clicking on the Recent item.
- You can save the current layout of charts, columns and filter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

Export to PDF

You can export current displayed charts to PDF or Excel using the button in the top right

corner.



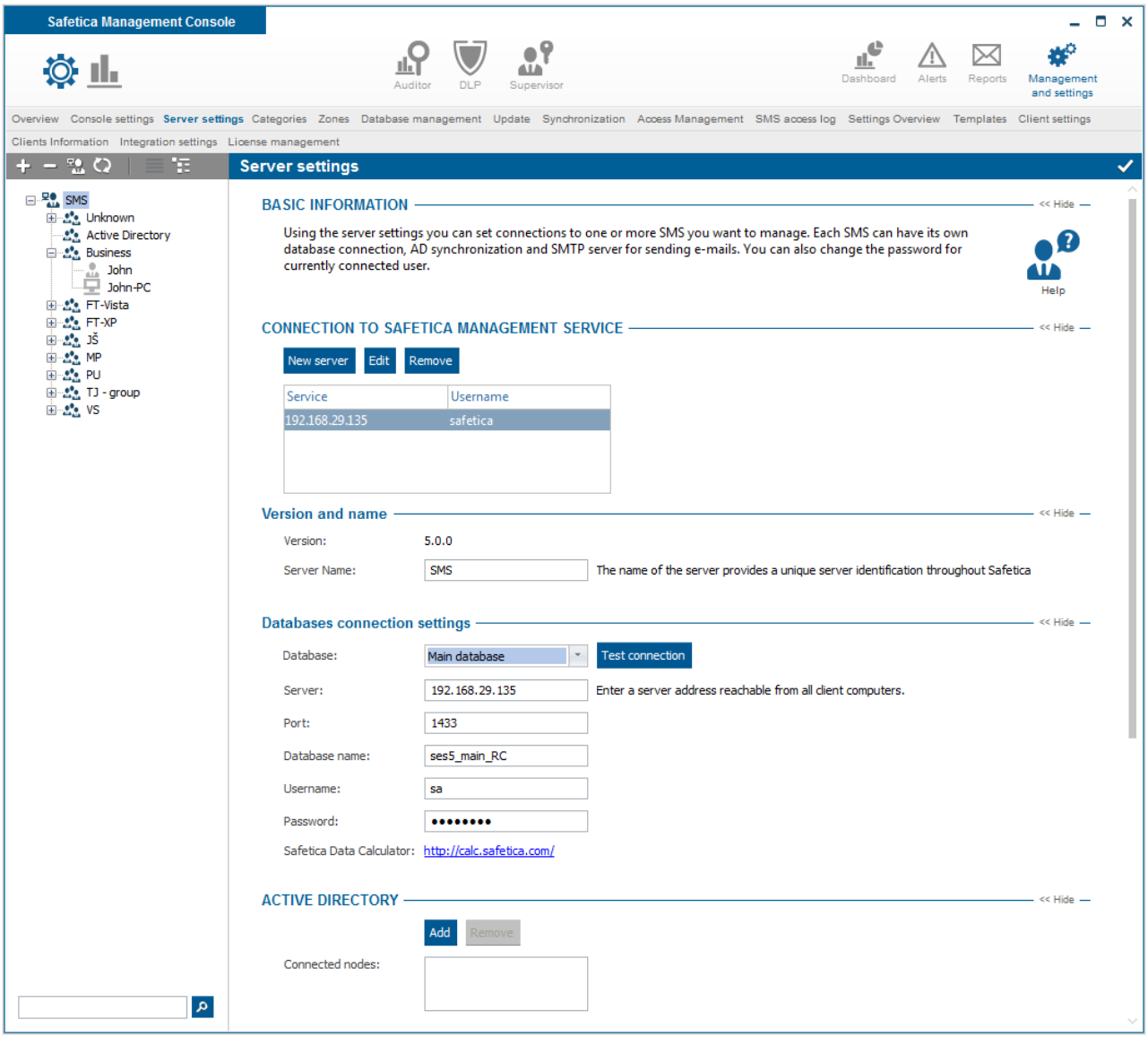
Note: All data corresponding to selected users, the time period in visualization and filter settings will be exported to Excel. Groups of records are also exported to Excel. The export limit is 60,000 records (Excel table limit). If the number of records exceeds this limit, the first 60,000 records will be exported.

4.2 Safetica Management Service

4.2.1 Server settings

Server settings in Safetica Management Console (SMC) are used for configuration of parameters necessary for proper functioning of the whole Safetica system. The principle of the setting is based on the distributed architecture of Safetica, i.e. the possibility of multiple servers – multiple instances of Safetica Management Service (SMS) connected to SMC. Each SMS has its own settings.

You can display the settings by clicking on *Main menu -> Management and settings -> Server settings*.



Description of the view

A list of SMS which are connected to SMC can be found in the top part of the view. Selecting a connected SMS in the list will show, in the space below, its detailed properties such as SMS name, database settings, Active Directory synchronization, etc.

You can connect to a new SMS by clicking on the *New server* button.

You can edit current connection information by selecting the SMS in the list and clicking on the *Edit* button.

You can disconnect from SMS by selecting the SMS in the list and clicking on the *Remove* button.

All setting changes must be confirmed by  button to take affect.

Connect SMC to a new SMS

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

1. Enter the following information:
   - *Server* – IP address or name of the computer where the SMS you wish to connect to is running.
   - *Port* – enter the port number of the SMS for SMC connection. The default port number is *4441.*

- *Username* and *Password* – enter login credentials of the SMS user. SMS user accounts are created in Access management. The default service account is *safetica* with password *safetica*.

2. Confirm by clicking on the OK button in the dialog. During the connection attempt you will also be asked to confirm the server footprint. Select Yes if you want to connect. The new SMS will be added to the list.

SMS properties

Version and name

Here you can view the SMS version number or set name.

Database connection settings

The MS SQL database connection settings can be found in the middle part. Select a database in the drop-down list and enter the appropriate information for each:

- *Server – the address in domain form (server.com) or the IP address of the server running the MS SQL instance. If you have already named the instance, enter the address in the following form: "server address\MS SQL instance name".*
- *Port* – the number of the port the MS SQL instance is running on.
- *Database name* – name of the appropriate database you want to create. Database is created automatically.
- *Username* – username of a MS SQL database user with access to the administration of the above-mentioned database and with MS SQL privileges to create database.
- *Password* – the password of the database user.

By clicking on the Test connection button you can test connection from Safetica Management Service to SQL databases.

Active Directory

There is the an *Add* button to import the Active Directory roots into SMS administration. After a dialog prompts you to confirmconfirming a dialog, all domain users and all computers will be added from these roots into the user tree (they will be added to the SMS you are currently setting up). These users and computers will be placed into the group designated for synchronization with the Active Directory (*AD*), from which you can later copy them into their appropriate groups. For more information, see Working with visualization and settings modes.

SMTP server (outgoing mail server)

Here one can set the outgoing mail server (SMTP server), which is used for sending e-mail messages (reports) and notifications (alerts).

You can verify that the entered data is correct and the connection with the SMTP server is functioning properly by pressing the Test connection button.

Change connected SMS user password

There you can change the password of SMS user account under which you are currently connected to SMS. Only there you can change password for default service account .

4.2.2 Access management

User accounts allow setting of user accounts for accessing individual Safetica Management Service (SMS) modules and their rights. The user accounts can be created, edited and removed. Each account contains a username and a password. By default an account is created that you can use for initial login in Safetica Management Service. This account has exclusive rights to all ac-

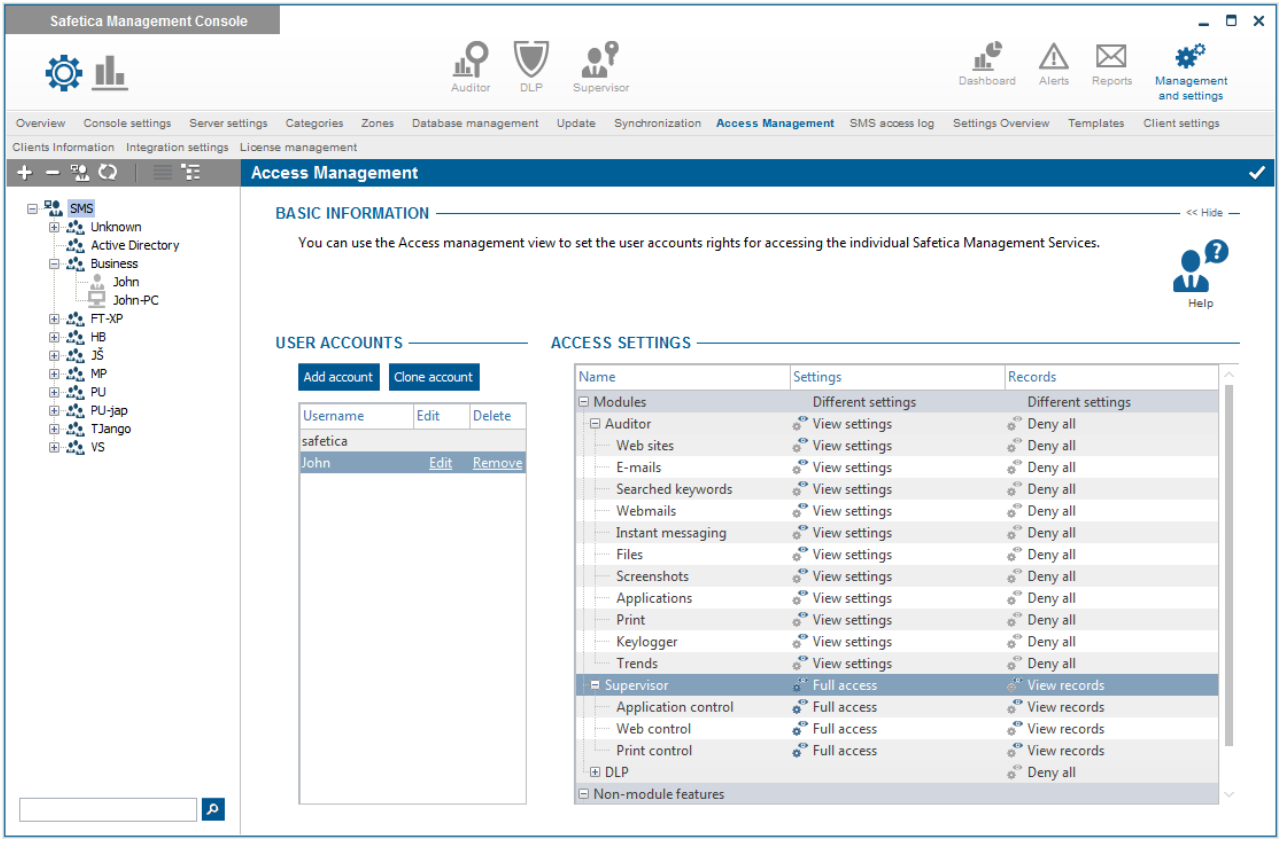
tions.

Access details of the default service account:

login: *safetica*

password: *safetica*

It is strongly recommended to change the password of the default service account immediately after installation. This can be done from Management and settings -> *Server settings*.



Description of the view

There is a list of SMS accounts on the left. On the right you can find access settings for each part of Safetica.

You can add a new account by clicking on the *Add account* button.

You can create an account with the same settings by selecting the original account and clicking on *Clone account*.

You can edit the name and password of the selected account connection information by selecting the SMS in the list and clicking the *Edit* button.

You can disconnect from an SMS by selecting the SMS in the list and clicking on the *Remove* button.

SMS account management

Administration is accessible from the main menu of Safetica Management Console (SMC). You can create a new account by pressing Add account. In the dialog that appears, you can enter the new username and password and confirm the entry.

After it is created, an account can be edited by highlighting it in the list of accounts and pressing Edit account. In case you want to remove an account, follow the same steps and after highlighting the account, press Remove account. The last option is Clone account. You can use this option in case you have rights preset for the user account and you do not want to set it again. You can simply select the user with the prepared preset, press Clone account, enter the username and

password and confirm the option for creation of a new account.

User accounts are displayed only for the selected Safetica Management Service in the user tree.

User rights

For each user account you can assign one of the following rights to individual modules, functions or settings:

- *Not set* – all settings are inherited from the parent level
- *Deny all* – viewing records and settings or setting and updating policies is restricted
- *View settings* – the right to display current settings of individual modules and functions
- *View records* – the right to display visualization graphs for a selected employee
- *Full access* – the right to display and change settings of individual modules and functions

Each setting can be applied on the selected account and individual modules and functions divided according to the main menu:

Modules:

- *Auditor*
- *Supervisor*
- *DLP*

Non-module features

- *Management and settings*
- *Other settings*

After making any changes in the setting of the user account, the settings must be saved. The recommended procedure for creating user accounts is making an initial connection to Safetica Management Service and then creating all required user accounts for Safetica Management Service. On any other Safetica Management Console you will connect to Safetica Management Service using the created user account.

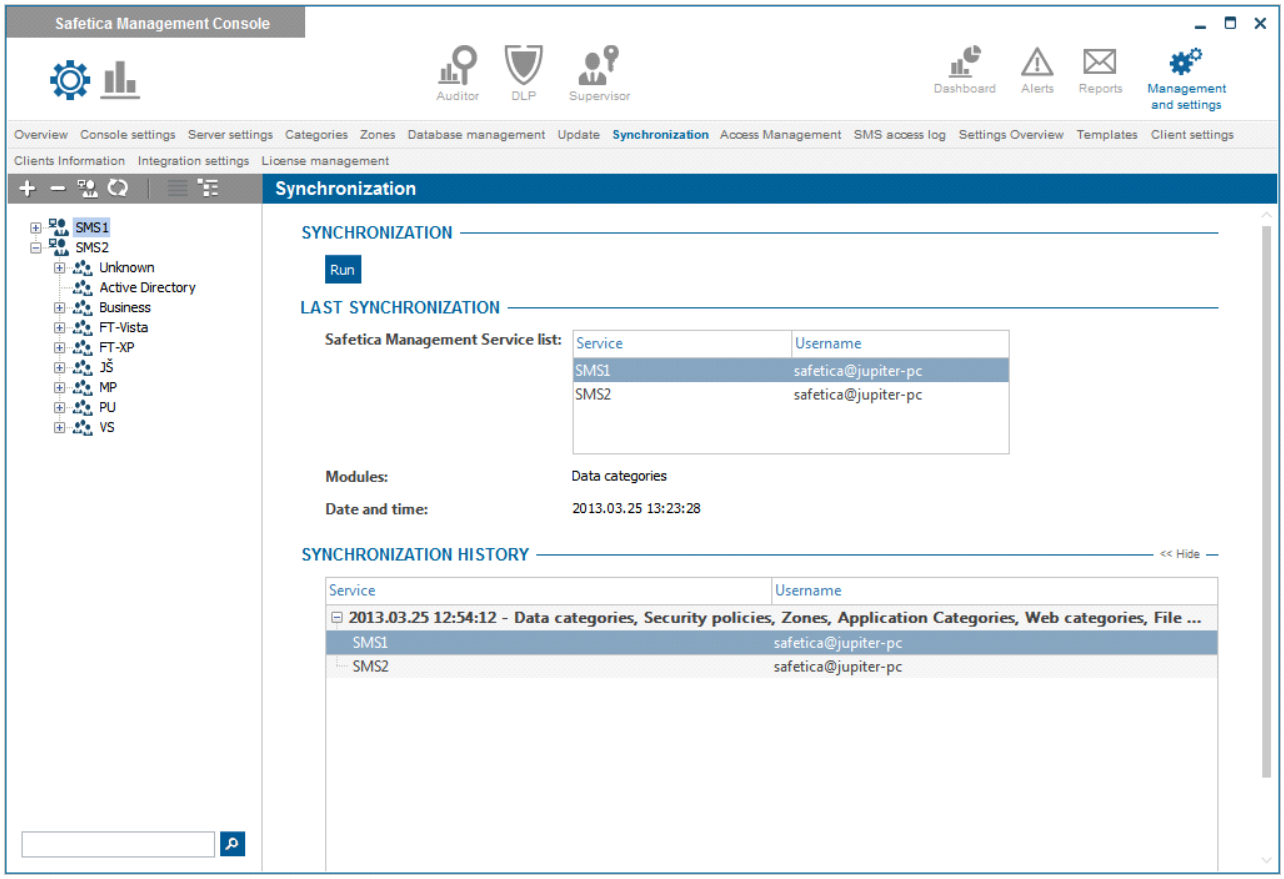
4.2.3 Synchronization

With Synchronizazion you can synchronize important settings between two or more Safetica Management Services. This is a set of settings called synchronization items, they are independent of user tree and they are common to an entire Safetica Management Service. They are:

- Data category
- Classification rules
- Security policy
- Zones
- Web categories
- Application categories
- File categories

Description of the view

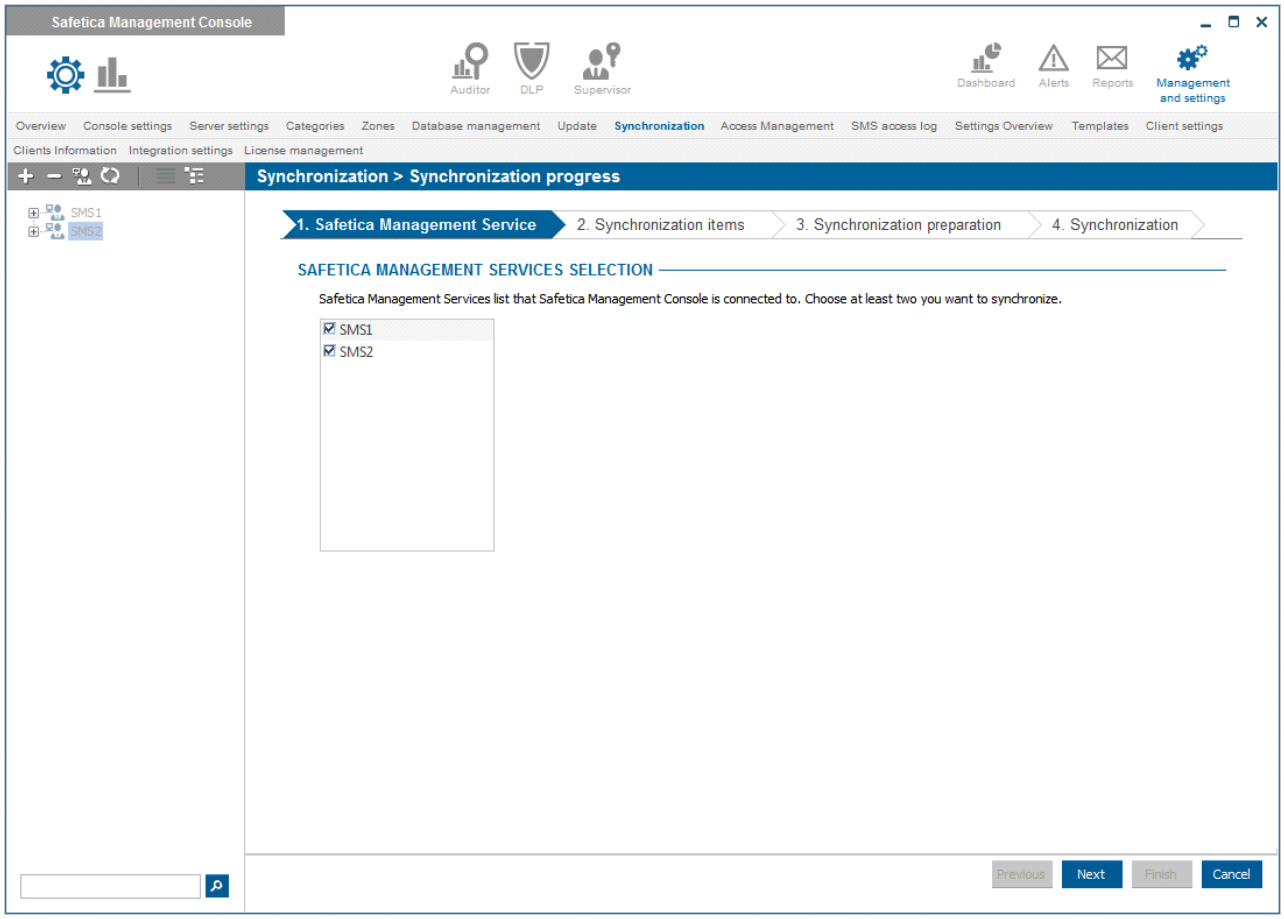
At the top of the view is detailed overview of a last executed synchronization. The lower part is an overview of all executed synchronization tasks.



Setting Up and Running sychronization

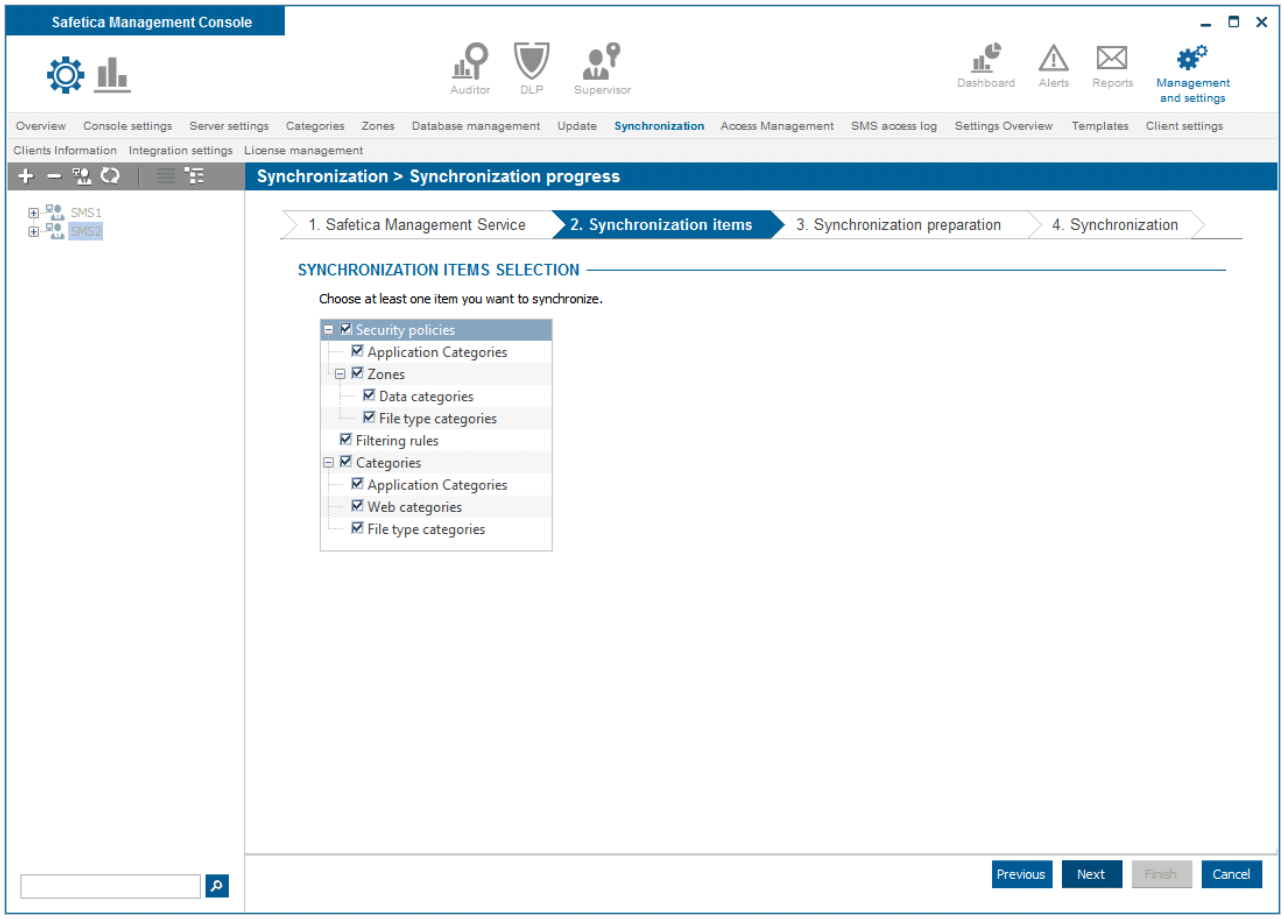
1. To set a new synchronization, click *Run*.
2. First, in the list of Safetica Managemen Services select those services you want to synchronize. The list includes only those Safetica Management Services (SMS), to which you are connected from your Safetica Management Console (SMC). After completing your selections, click *Next*.

   Note: The synchronization is performed simultaneously at all SMS. Each setting on one SMS will be on all other SMS when synchronization finishes. During synchronization, conflicts can arise that need to be resolved - see Conflict Resolution.



3. In the next step, select the synchronization items that you want to synchronize. Then click *Next*.

   Note: It is always recommended to synchronize all items due to possible dependencies, which are shown in the tree.



4. In this step are synchronization items prepared to be sent between SMS. At this point conflicts may occur.
5. *Conflict resolution* – if some value has been changed on two or more SMS, then there is a conflict, which you have to solve manually, ie. select value from one SMS, that will be used on all other SMS.

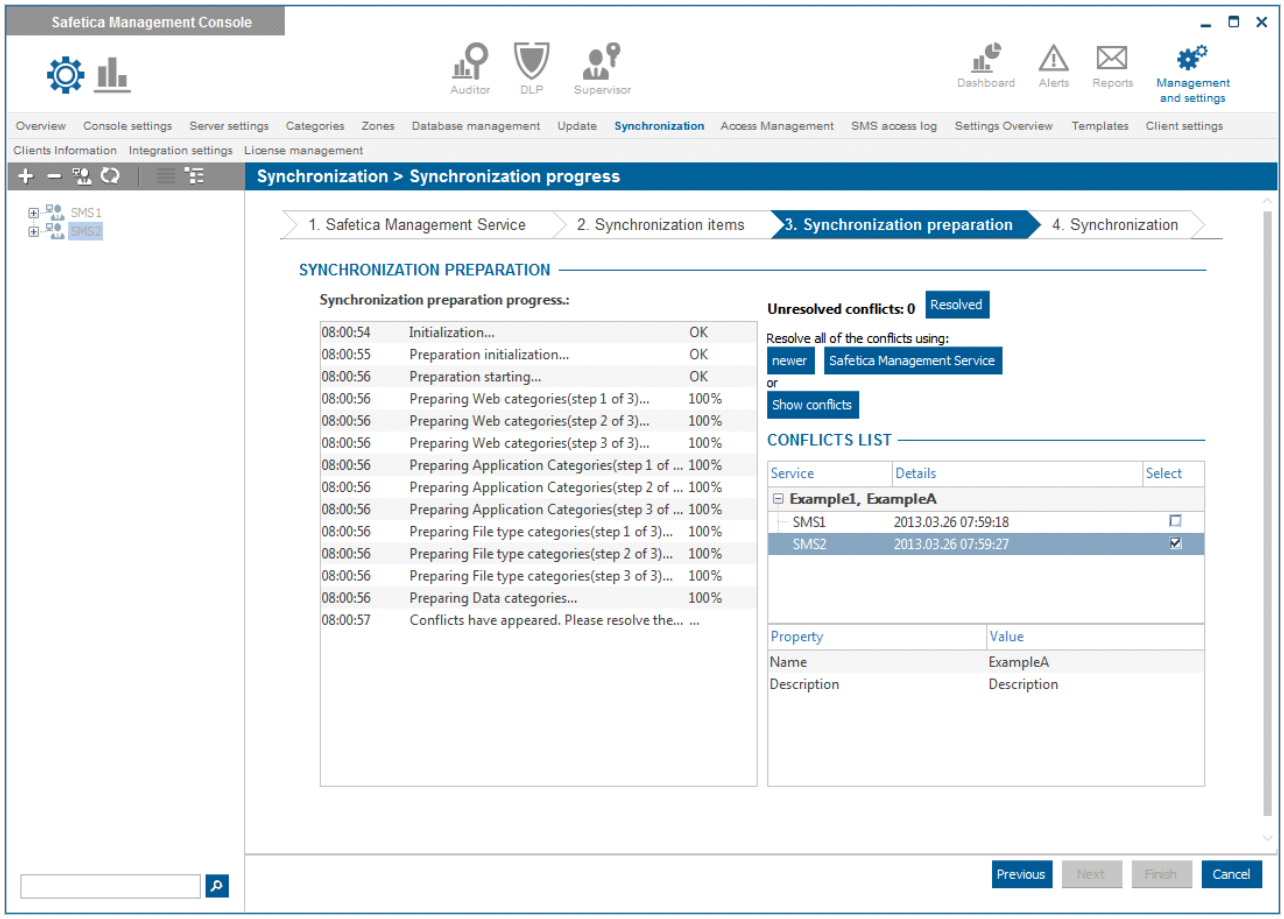
   (An example might be a data category named Example, which was – by a previous synchronization – stored on SMS1 and SMS2. On SMS1 was renamed to Example1 and on SMS2 was the same data category later renamed to ExampleA.)

   Conflict resolution options are:

   a) use a newer value – uses the latest conflicting value for all conflicts (here will be used ExampleA). Click on *newer* button.

   b) use a value from selected SMS – uses value from selected SMS for all conflicts (select SMS2, which means using ExampleA),

   c) manual selection – using the button *Show conflicts* you can display window with conflicts, from which you can select the most suitable value (for example: you would select ExampleA from the list).
6. After resolving all conflicts press *Resolved*.



7. After a successful preparation of all synchronization items, you can continue using the *Next* button.
8. In the last step, data are exchanged between all SMS. Any error will end the synchronization process. A detailed error description can be found in a log file on the failing SMS (default path is C:\ProgramData\Safetica Management Service\Logs\Service_lastrun.txt). At the end, you can click the *Finish* button.

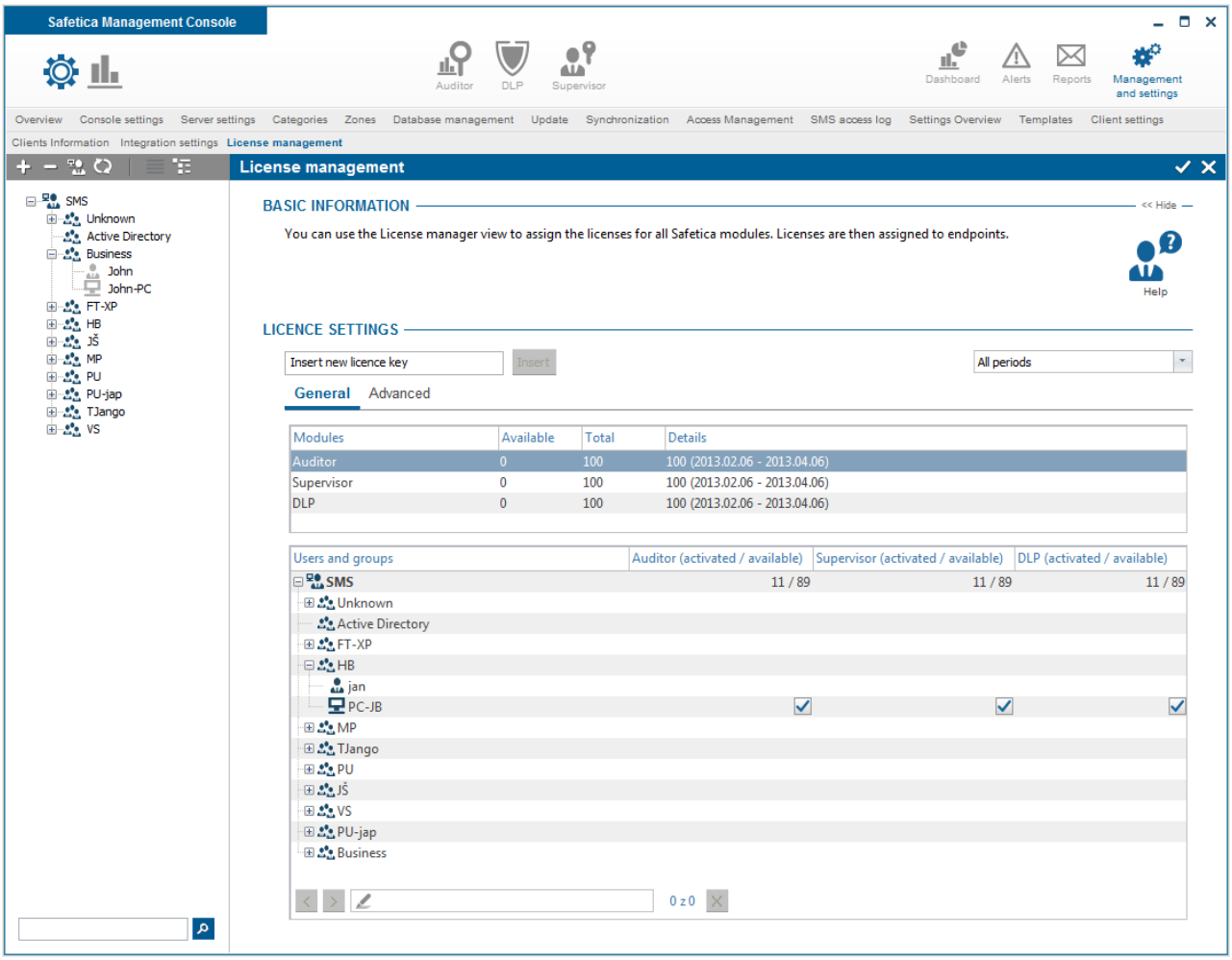
   Note: Synchronization may fail if some of the SMS has updated categories database and other not. First update the categories database on all SMS.

4.2.4 License management

License management is used for management of Safetica Endpoint Client licenses. Licenses are assigned per computer. Licensed are individual modules of Safetica – Safetica Auditor, Safetica DLP and Safetica Supervisor. Module functions will not be available without assigned licenses.Safetica nformation on licensed modules, the number of licenses for the clients and the validity period are contained in the license number that you receive from your distributor. You can enter the licenses for all modules at once, for one or various combinations of these three modules using one license number.

You get 100 trial licenses for each module after installing Safetica. These licenses are used to try out Safetica. These licenses will be valid for one month and after that functionality will be limited.

Trial licenses are assigned automatically to all new clients connected to the limit of 100 per module, so you do not have to assign trial licenses manually. When you insert a purchased license number, the trial licenses will be canceled and you must then assign licenses to computers so that Safetica will function properly.



Insert a new license key

To insert a new license number, enter the number into the text field in the upper left part of the License manager and then press the Insert button.

On the right is a drop-down list with the period of validity of the inserted license numbers. Here you can choose the period of licenses that will be displayed below.

Assign module license to SEC

Before functions of specific modules on SEC can be used, you need to assign a module license to SEC. To assign licenses for specific groups, users or directly for computers (SEC), enter the number of the licenses into the appropriate column and cell you want to activate on SEC.

An activated module on SEC is marked by ☑.

Note: If you assign a license to a user, the license will activate the module on the computer with SEC on which the user logins for the first time. If you assign licenses to group, the license will activate the module on the computer with SEC inside the group. More about license assigning can be found in Differences between license assigning.

4.2.4.1 General

This tab is used to allocate the available licenses for individual modules between computers, users and groups.

The upper part displays the number of available / unassigned licenses, total number of licenses, and details such as the period of validity of licenses for each module of Safetica.

At the bottom of the table that you can assign module licenses for individual computers, groups and users. This is done by inserting the number of licenses in the proper cell in the table. Changes

must be confirmed by pressing the  button.

You can see the following information in the table:

 The user or computer has activated a license for the module. This means that the license has been downloaded to the client and all functions of the module are active.

2/3 The group containing this information has a total of 5 licenses assigned. There are two licenses activated (licenses are assigned to a computer with the client inside the group) and three licenses are still available (licenses are not assigned to a computer with a client).

 Some computers, groups or users inside the group labeled with this icon have licenses assigned. When you move the mouse pointer over the icon, the number of available and activated licenses within the marked group will be displayed.

2/3 The group containing this information has a total of 5 licenses assigned. There are two licenses assigned and three licenses still available for assignment and activation. At the same time certain computers, groups or users within the marked groups also have assigned licenses. Move the mouse pointer over the icon to view detailed information about activated and available licenses inside the marked group.

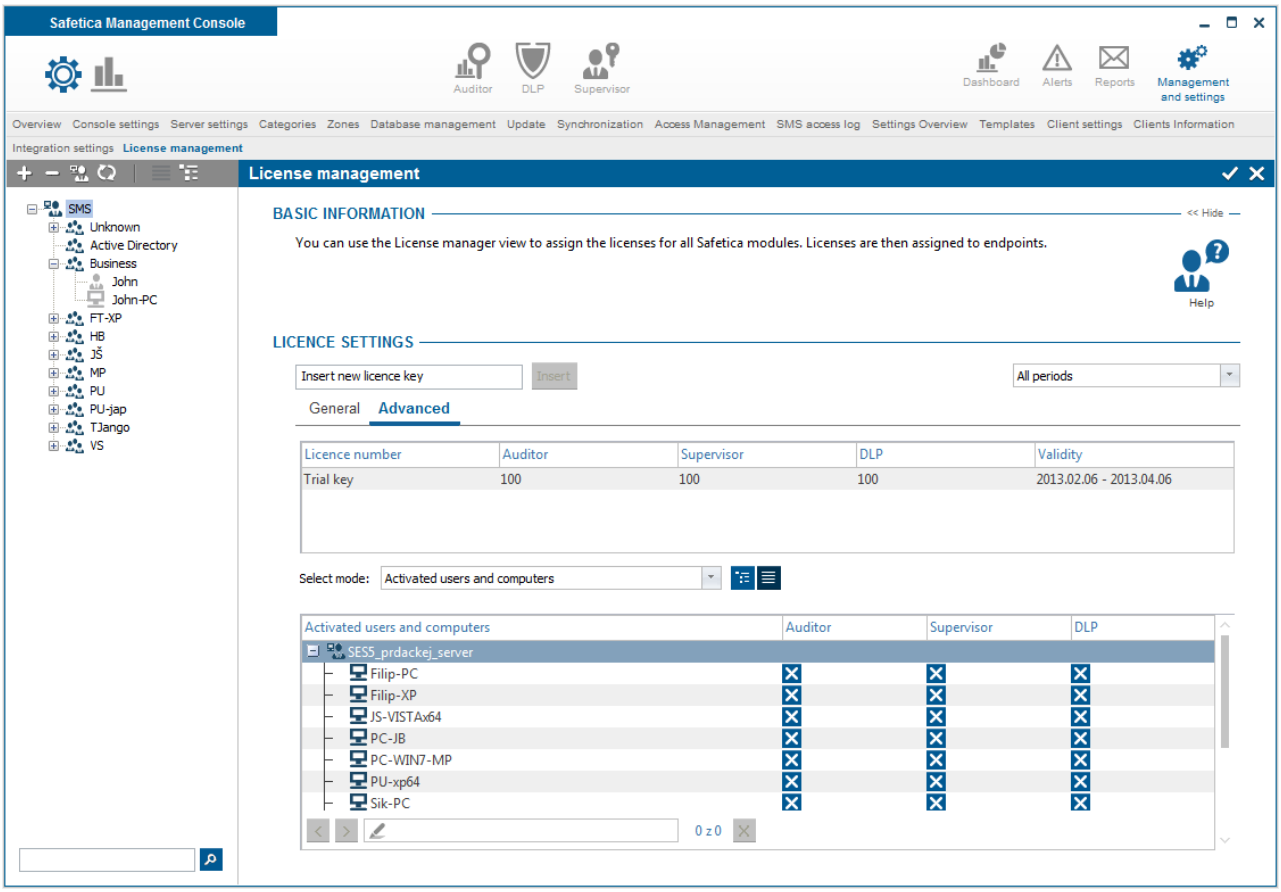
If there are certain groups, computers or users that have a grayed-out field in the table, they were excluded from the assignment of licenses. See Advanced -> Excluded users and computers.

4.2.4.2 Advanced

This tab is used for detailed license management. There is nothing to configure or change during basic configuration.

The upper part shows a list of entered license numbers along with the number of licenses for individual modules and their period of validity. For unambiguous identification of license numbers, the first five license characters are displayed. Other characters are hidden for security and marked out by x instead.

At the bottom, depending on the mode, one can find a detailed table of license management.



Activated users and computers

The table shows the users and computers that have an activated license. At With each activated module is is shown also the period of its validity.

By clicking on the icon you can remove the relevant module license from the computer or user.

Non-activated computers

The table shows the computers that do not have a license activated.

By clicking on the icon you can assign the license. After clicking on the icon, a pop-up menu will appear. Select an item from the context menu to choose where the license will be assigned from: either from all licenses not yet assigned, or directly from a specific group if the computer is inside a group which has licenses available. The name of the group is shown in the context menu along with an indication of activated and available licenses (21/29 – 21 activated, 29 still available for assignment).

By clicking on the icon you can add a module of that computer to the excluded computers list.

Excluded users and computers

If you click on the icon of the appropriate module of the SMS server, a dialog will appear where you can exclude the specific group, computer or user from the license assignment. These modules are grayed out for these groups, computers or users in the General tab and a module license cannot be assigned to them.

By clicking on the icon you remove the module from the list of excluded.

4.2.4.3 Differences between license assigning

Assigning a license to a group

Licenses assigned to a group are automatically assigned to computer with the client and without license. Computer must be located inside this group.

License is also assigned to a computer (with a client without a license), which is not in this group, but user who is located in this group has log on to this computer.

License is also assigned to a user who logs on to the terminal server.

Licenses are not assigned to a computer or users who are listed in the excluded users and computers list. See *Advanced -> Excluded users and computers.*

Assigning a license to a computer

When the client connects to the server for the first time the client download a license and activate appropriate module.

Assigning a license to a user

When a user logs on the computer with no assigned licenses, the license will download to a computer and activates the appropriate module.

When a user logs on with a client computer with assigned licenses, the license remains assigned to the user until he logs on to a computer without a license.

A user who connects to the terminal server must have license assigned.

4.2.5 Integration settings

Safetica uses a mechanism that allows you to control users' activity with the application, the application itself and its access to system resources. This mechanism is used for most of the functionalities in DLP, Auditor and Supervisor. Most DLP products are limited to only supporting a specific set of applications, but Safetica allows you to guard any application or even all running processes. Due to the high degree of complexity, difficulties and susceptibility to conflicts with third-party applications, most manufacturers of DLP systems have adopted this dangerous compromise. They can only ensure data protection in the most common applications for which they have created a specific implementation. The simplicity and speed of this option to create DLP software led to this approach spreading among most manufacturers. Very rarely, however, customers become aware of the fact that they can just use any application that this kind of DLP software does not support and thus evade any security policy.

Consequently, investment in such software just does not make sense for many of today's security managers. Safetica has a different philosophy. We've created an advanced mechanism that allows you to protect against leakage of data from any application that the user is working with.

There are two basic modes and an ability to determine which applications will or will not be included in the selected mode. By default, the Compatibility mode is used, where officially supported applications are guarded and others can be added manually. Advanced mode automatically activates the control mechanism over all applications in the system and allows you to exclude some applications from guarding.

You can disable integration entirely by using the slider at the top of the screen.

View description

At the top of the view you can select the integration mode.

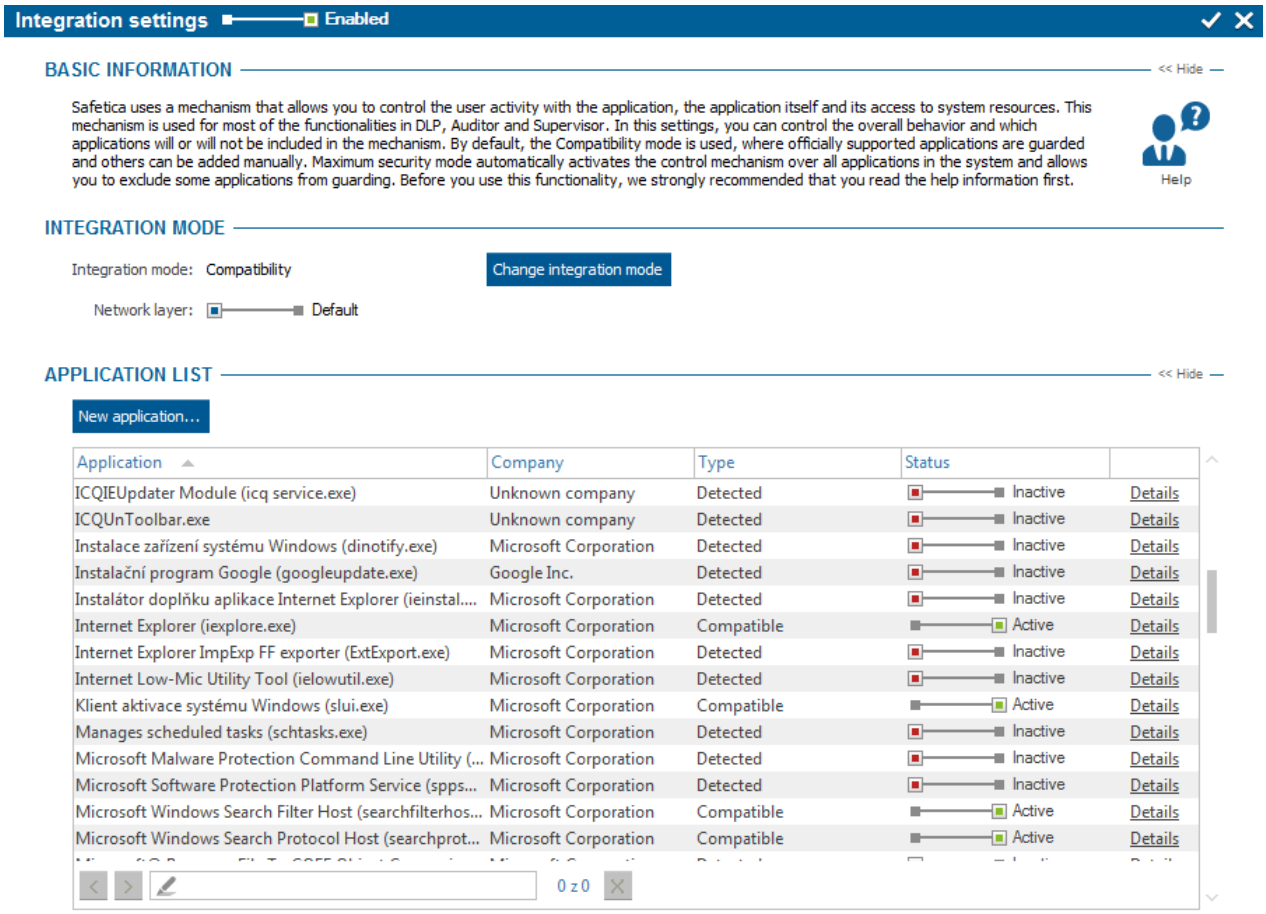
At the bottom, there is a table containing all the applications found on workstations with SEC installed. The table includes basic information such as the application name and developer. It also contains information on whether the application is compatible (officially supported) or detected (an application that has not yet undergone the certification process).

For each of the applications in the table you can manually activate or deactivate guarding, regardless of the selected mode.

By clicking the New Application button, you can add any application that you want guarded and is not yet in the list.

Click on the *Details* button in every application and a dialog with detailed integration settings will appear for the respective application. You can find more in the Integration mode detailed settings.

At the bottom you will find a table where you can enter the websites for which you want Safetica to enter secured communication.



Integration mode settings

Click on the Change button to select the integration mode. You have two choices:

- *Compatible* – in compatible mode only officially supported applications are guarded. Others can be added manually. This mode is set by default.
- *Maximum security* – maximum security mode automatically activates guarding of all applications. Some applications can be excluded from this mode if required.

Setting Safetica network layer

The Safetica network layer is needed for correct functionality of some Safetica features that monitor or otherwise affect network traffic. The network layer switch is used for handling exceptional issues with the default network layer on Windows Vista SP1 systems and higher. These issues should be first handled through other settings in this view (integration mode global settings, integration settings for different applications, SSL integration settings). Should this not solve the issue, you can switch the default network layer over to a layer compatible with Windows 8.

These settings will not affect the layer applied to systems with Windows XP and Windows 8 where the compatible layer is chosen automatically and cannot be changed.

- *Default* – in the default mode a network layer compatible with Windows XP is used on PCs with the Safetica Endpoint Client (SEC). In exceptional scenarios this layer can cause problems with some applications on systems with Windows Vista and Windows 7.

- *Prefer Win 8 layer* – if you apply this layer, you can solve possible issues caused by the use of the default layer on systems with Windows Vista SP1 and higher. After switching over to this layer, the compatibility of the entire system and applications will be tested on systems with Windows Vista SP1 and higher. If no compatibility-related issue has been detected, the Windows 8 layer will be used.

Warning: The Windows 8 layer can have problems if running in parallel with some security products such as Kaspersky, Avast, Nod32 and ZoneAlarm antivirus software. Before using this layer with such security products, we recommend a consultation with your Safetica vendor and trying this layer on a selected reference PC.

In the Clients Information view you will find out the layer used on different PCs with SEC. We recommend restarting the PC before switching the layer.

Note: You can change the network layer also locally on the PC with SEC via the STCService -installlayer command. Find more details on commands for local security administration in the Components Administration section via the command line Managing components using the command line.

Changing the settings for a specific application

Regardless of the selected mode, by using the sliders in the table, you can set set up if a particular application will be guarded – (the rule is Active) or unguarded – (the rule is Inactive).

Integration mode detailed settings

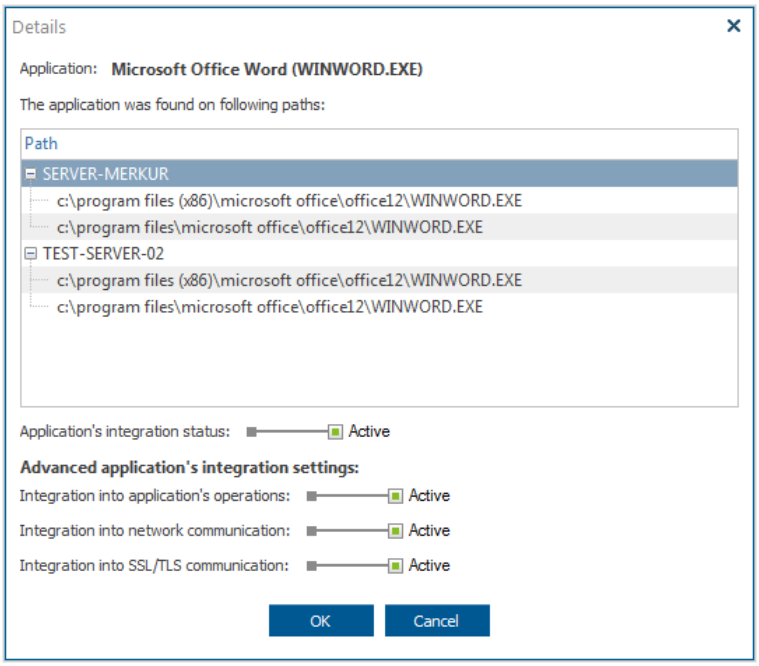
Click on the Details button in every application and a dialog with detailed Safetica integration settings will appear for the respective application.

At the top you will find a list of paths on which the application was found on clients. At the bottom you can specify different integration parts:

- *Integration into application operations* – Safetica will be integrated into all operations inside the application. If integration is active, Safetica will be able to monitor internal application operations and/or enter into such operations with the aim of applying security. This can happen for example in an enforced security policy.

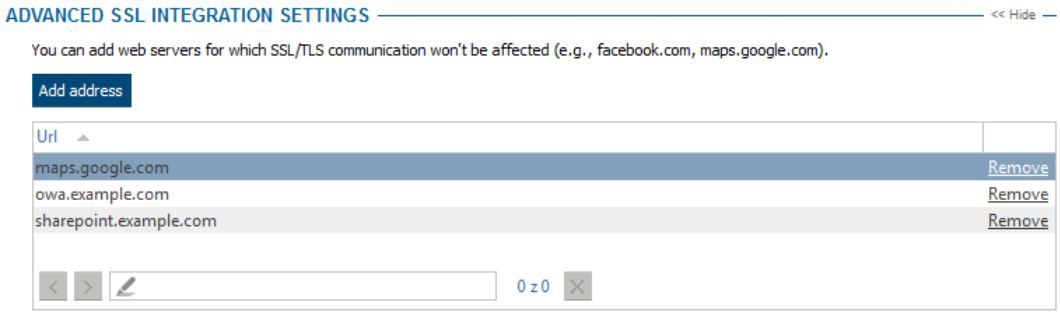
- *Integration into network communication* – Safetica will be integrated into all network communication. If integration is active, Safetica will be able to monitor all network communication of the application and/or enter into such communication with the aim of applying security. This can happen for example in an enforced security policy.

- *Integration into SSL/TLS communication* – Safetica will be integrated into all secured network communication. If integration is active, Safetica will be able to monitor all secured SSL/TLS network communication of the application and/or enter into such communication with the aim of applying security. This can happen for example in an enforced security policy.



Advanced settings of SSL integration

You can use the table in SSL integration advanced settings to add new websites where you wish Safetica to enter secured SSL/TLS communication. New websites are added to the list by using the Add website button.



Adding new applications

Every application installed on the workstations is synchronized with the list on the SMS. If you want to predefine settings for an application that was not detected on the workstations, use this function.

After clicking on the New Application button, select the binary file of the application you want to add. The application binary file should therefore be accessible from the station where you are currently running SMC.

Important Information

These settings are common to all users, computers and groups from the selected SMS.

If you decide to activate *Maximum security* mode or activate guarding of officially unsupported applications, always follow these recommendations:

- Before activating the monitoring of unknown applications or using Advanced mode, always try out such a change first on a non-production system (e.g. a virtual machine).
- Guard only applications where it makes sense, that is, applications that can be used to manipulate data (generally read on input and process on output). The more guarded applications there are, the greater the demand on system resources.
- If you want to use the Advanced mode, you must first carry out performance tests and, if ne-

cessary, increase the hardware capabilities of the end stations.

- If end users have the right to install new applications or use their own, then it is recommended to use Advanced mode. If you use this mode by default, it is necessary to check that the applications currently used on end stations function correctly. We have therefore assumed that unsupported applications cannot always be guaranteed to work correctly. In such a case, contact Safetica Technologies technical support with a request to add this application to the list of supported applications. This list is updated each time we release a new version of the product. The process usually takes around five weeks and may require access to the application for our developers.

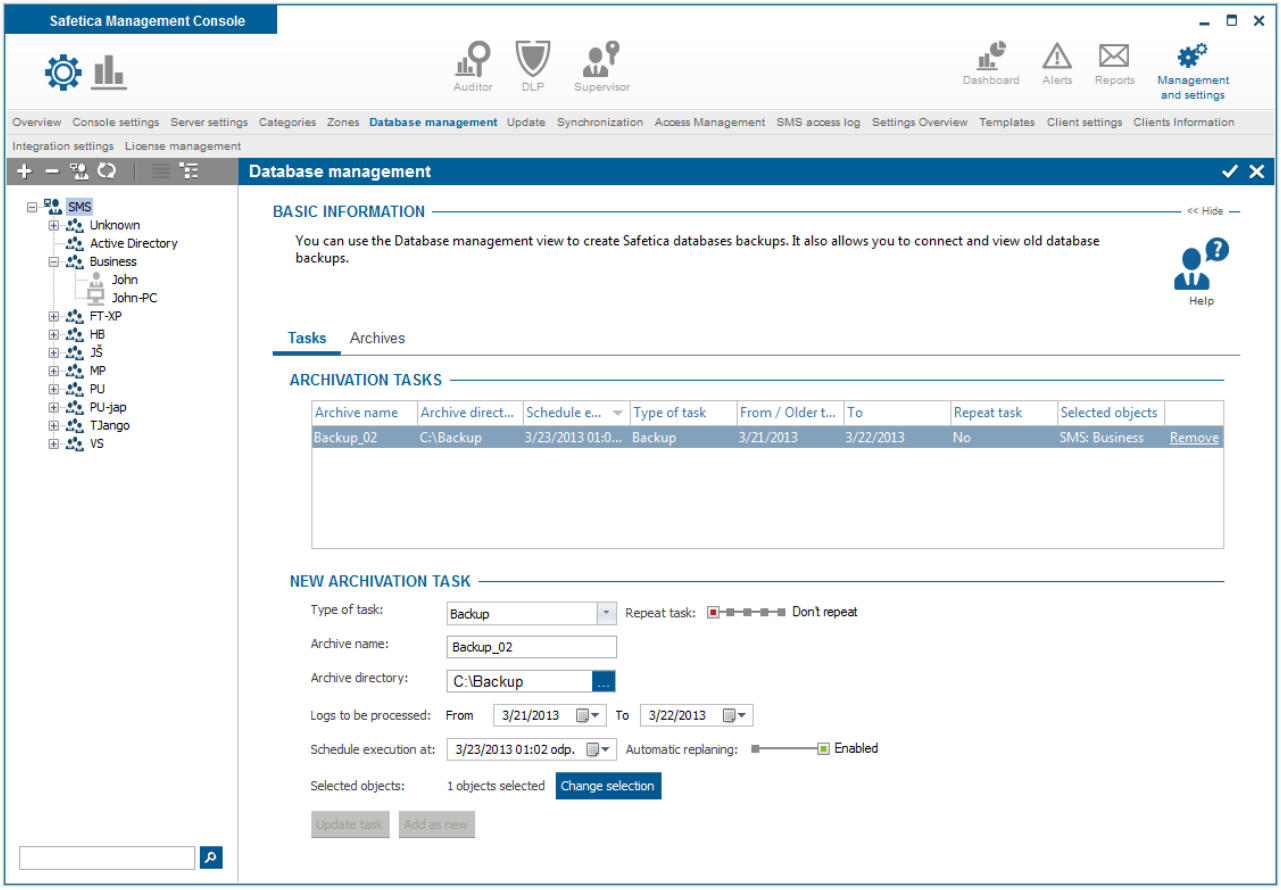
We assume, therefore, that the unsupported applications can not always be guaranteed to work correctly. In such case, contact the support of Safetica Technologies with a request to add this application to the list of supported applications. This list is updated everytime we release a new version of the product. The process usually takes around five weeks and may require acces to the application for our developers.

4.2.6 Database management

The database manager is used to back up monitored data, settings and for deleting monitored data.

The database manager has two main parts:

- Tasks – here you can create a task to back up the database (create archives) and delete data produced during monitoring.
- Archives – using this tab it is possible to connect previously created archives to a selected Safetica Management Service (SMS) to review the data.



4.2.6.1 Tasks

Tasks are used to work with data stored in the database. Data can be backed up from the operational SES database (archive) or they can be directly deleted.

All tasks are created using New archiving task menu – new task has several parameters:

- Type of task – you can choose from the following options: backup, backup and delete, delete, delete screenshots, settings backup. More information about each task can be found below.
- Archive name – the backup file name. It must not contain illegal characters like spaces (http://msdn.microsoft.com/en-us/library/aa365247%28V=VS.85%29.aspx)
- Archive directory – the path to the folder where the backup database file will be saved. It is the path on the computer that is running the SQL server. The selected path must already exist, because the SQL server is unable to create the path.
- Logs to be processed:
  - From-To – it is possible to choose a time period for backup of monitored data
  - Log older than – processed are logs older than specified date. Available only when delete task is created.• Schedule execution at – exact time when the task will be executed. This time must be set outside the time period of logs to be processed
- Automatic replanning – when enabled, this function ensures that if a task is run at a time when another job is running or the task start time has already passed, then the task start time will be automatically moved to the next free time. Only one task can run at a time on one SMS or SQL instance, so this feature is applied only when an error with time occurs. In every other conflict (lack of disk space, insufficient rights to write, etc.) no rescheduling will occur.
- Selected objects – it is necessary to select for which users, computers or groups the backup or delete task will be performed.

Backup

A backup will be created at the specified time for the selected users, computers or groups. The backup will contain records obtained from the monitoring of users. Module and functions settings are not included in the backup. Two files are created on output: one (*.mdf) is a record from the DB and the second (*.ldf) is the log of operations over this DB. Each SMS has its own database, so if we want to archive data from a database, we need to run the backup task over each SMS and these tasks will be independent of each other.

There is a considerable load on the SQL server when a backup is being created, so there is a possibility that client stations will be temporary unable to communicate with a database, and therefore new tasks should be scheduled at a time when the load on the database is at a minimum (at night, for example). The process may take several hours depending on the amount of backup data and the size of the original database. During backup it is not recommended to perform database operations, such as reindexation, because backup operation could fail.

Delete

The Delete task performs deletion of user settings, logs and screenshots. The deletion will be done from the beginning to the specified time. After erasing the data, it is recommended to manually run the SHRINK command on the Safetica SQL databases. This command will physically shrink the database file.

Delete screenshots

The parameters are identical with those of the Delete task, but only screenshots are deleted from the Auditor functions Screenshots, Instant Messaging and *Webmail*.

Settings backup

This performs a copy of the database along with the settings. A .bak file will be created. This backup file can be restored to the database using the SQL server command RESTORE.

Advanced maintenance settings

In this section you can specify the maintenance options for the records database:

- *On the fly logs validity* – use the slider to specify how long records from on the fly data tagging functionality will be stored in the database. Records older than the value specified will be deleted from the database.
- *Automatic database maintenance* – here you can specify the largest possible size for a records database. If exceeded, some records in the database will be automatically deleted, so that the database can reach 70% of its maximum size as set. The size is checked on a daily basis. If you enter for instance 100GB as the largest database size, then the size will be reduced to approximately 70GB.

  Warning: When records are deleted as part of database maintenance, they will be irretrievably lost. It is always the oldest records that are deleted.

  Note: When using Microsoft SQL Server 2008 Express, the biggest size is determined by this edition. It is therefore 10GB. If a bigger limit is entered, then the limit used for this edition will be automatically reduced to 10GB.

4.2.6.2 Archives

In the Archives section, we can view the previously created archives. It is first necessary to connect the archive to the SMS. After connecting, the archive acts as a common database of records. In this mode all setup operations in the SMC are inactive (e.g., DLP cannot set rules, deny running of applications, etc.)

Import archive

An archive which was not created on the SMS can be manually imported. This is done by specifying the path to the archive and the target SMS to which the archive will be connected. Then, use the *Import archive* button to import it to the list.

Close archive – disconnect from SMS

Disconnecting an archive is possible with the user tree or Database management view. Either right-click on the name or address of the SMS and select Close archive, or open Database management -> Archives and click on the *Close archive* link for a particular archive.

Archive operations log

All operations that are done using database manager are recorded, and all records can be displayed in the visualization mode. The view is divided into operations with *Tasks* and *Archives*. Records can have the following states: *Created, Running, Completed, Updated, Error.*

4.2.7 Categories

Does it sometimes happen you do not know exactly what operations a program performs and whether it leads to employee efficiency? Are you unsure whether a website's content is suitable for your employees? Safetica offers a categories-matching system providing you with an extensive database of records filed into appropriate categories. Not only you will understand program names or website addresses, but you will also know what categories of use they belong to.

Category setting is accessible from *Management and settings -> Categories.*

Description of the view

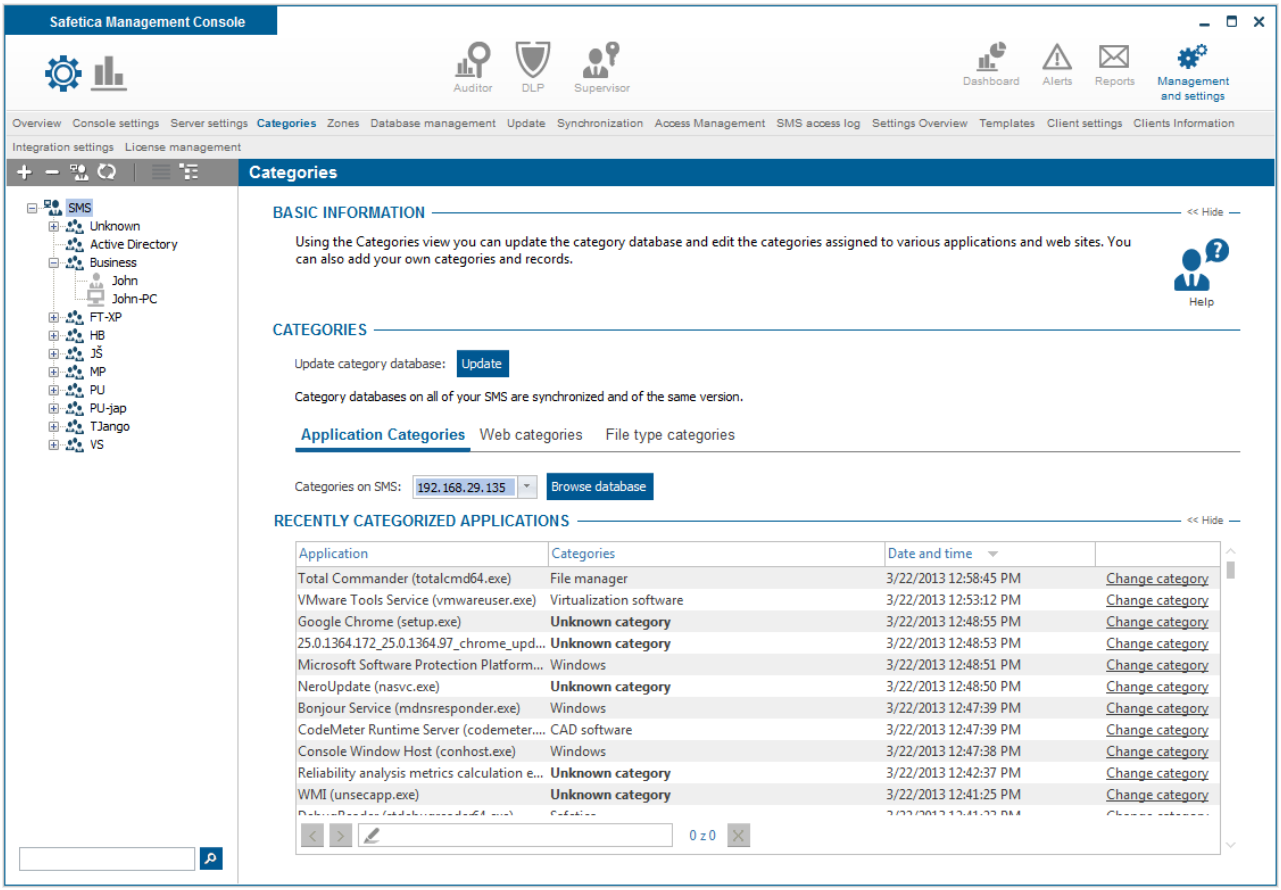
On the top of the view is button to update database of categories.

There are three tabs in the middle of the view:

- *Web Categories* – access to web categories management.
- *Application categories* – access to application categories management.
- *File type categories* – access to extension categories management.

You can access category management by selecting the SMS on which you want to manage categories, and then clicking on the Browse categories button.

On the bottom is a table with a list of the last categorized websites or applications according to the tab selected. You can manually change the category there by clicking on Change category next to each record.



4.2.7.1 Category update

The category database is not provided with the default installation of Safetica, because we always want to provide you with the latest version of our database. You can update the database in one of the following ways:

- Update from internet (on service) – the database update is carried out by the Safetica Management Service server. A dialog will appear to show the progress of the update.

Note: Safetica Management Service must have a connection to the internet.

- Update from a folder (on service) – the database will be updated from a folder located on the computer hard drive. This method is suitable if you have downloaded an update but are not currently connected to the internet. The path you need to enter is the path to the update file on the computer where Safetica Management Service is installed. It is not a path on the com-

puter where you are currently running Safetica Management Console.

- Download updates (on console) – the update file will be downloaded from the web server to the computer hard drive. You can upload the file to the server service manually or by using the above-mentioned update from folder. A dialog will appear to show the progress of the update.

Safetica will not fully function without the category database, because the records are required to run specific functions. After product installation, download and update the category database. You can modify or extend the database any way you like. If you already have the newest database version, you will be notified by a message informing you that no new updates are available.

4.2.7.2 Web categories

Websites categories is a sub-module of Safetica and is free of charge. It enables setting and editing the database of website and websites addresses categories. Not only does it enable you to add more records to the database but you can also edit individual categories arbitrarily. If you encounter a case when an employee directs his or her web browser to an address that has not been added to the system yet, the most secure action on your part would be to add this address to the database. On any future attempts to navigate to the same address on clients' stations, this site will be identified and classified into a selected category.

Web categories are set up from the main panel of Safetica Management Console. The program includes a window for editing categories and a window for editing web addresses. After launching it, you can view web categories that are organized into a tree structure. For the currently selected category, all web addresses from the database are displayed in the bottom window. If you want to create your own category, click on the Add category button and fill in the category name. Each time you want to add a category under an existing one, you must select the parent category before adding a child category. Otherwise, if you want to make the created category a top-level one, make sure that no category is selected before adding it.

Before adding a new web address, make sure that it has not been entered into the system yet. Otherwise it will not be possible to designate the category that the web address belongs to! To add a new web address, first select the category under which you want to include this address. Then, click the Add web button and enter the web address into the form. Finish adding the address by selecting Confirm. If you have inserted the record into the wrong category, you can remove it by clicking *Remove*.

Categories Database

The categories database contains thousands of records. Searching for the right category is made easier with the Browser function that is located at the top part of the screen. You can search for the category by entering the required category or web address. After you enter the name of a web category, you will be sent to the place where this category is located within the tree structure. Within the database the categories are classified as:

- *World (in English)* – under these categories are websites that are used by people worldwide.
- *National (in a national language)* – these websites are organized by the country suffix of the web address (.cz, .sk, .ua, etc.) and they are mostly visited by residents of the respective country. You can find these websites in the categories under the bookmark World - "required country".

Websites Database

The web addresses database contains records on websites that are recognized by Safetica Endpoint Client. These are always linked to a selected category. Therefore, before selecting or adding a new web address, ensure that you have correctly selected the web address category.

Adding a web address in the domain format is a must. Do not write the protocol (e.g. HTTP or HTTPS) in front of the web address but instead write the web address without arguments or slashes. In order that the address can be recognized, the format in which you write the web address into the database must be the same as the user puts into the browser.

Example 1: Examples of incorrectly entered web addresses

- http://www.google.com – the connection protocol was specified
- www.google.com/ – there is a slash at the end of the URL (this is not part of the web address)
- www.google.com/#sclient=psy&hl=cs&q=a&aq=f&aqi=g3g – the URL includes arguments (they are required to view the website but are not part of the web address)

Example 2: Examples of correctly entered web addresses

- www.google.com – search engine specification
- www.google.com/maps – using map services

4.2.7.3 Application categories

Like website categories, this module forms part of the Safetica It enables adding and editing settings of categories and assigned applications. Every application is classified into a specific category that best describes this application. After installing the application into the system, it will be recognized also in other modules. Identification of applications is a key sub-module of Safetica, and the software offers a basic database of applications and their categories. To ensure the most effective protection and monitoring of applications, it is necessary to modify settings of applications and categories to correspond with your clients' environment.

Application categories are set up from the Safetica Management Console (SMC) taskbar, which includes a window for editing categories and a window for editing the actual applications. To facilitate searching for categories, use the function of search engines. You may search for a category or an application that belongs to this category. Categories are displayed in a well-ordered list. After selecting the category, a list of applications in the database is displayed in the bottom window. You can search for applications using Application Name, Vendor or Process Name. Add new applications to the database by clicking on Add Application. When adding applications, make sure that a particular application has not already been added to the system.

You can edit the existing record by double-clicking on the application and editing the information in the dialog that will appear. To change a category of the existing application, select a new category from the list of categories and confirm your selection by pressing Confirm.

The application database collects all available information about applications that is later used for their identification:

- *Name* – Application name
  - *Process* – Name of an executable file (including the .exe extension)
- *Full Path* – Full path to the application’s executable file. You can search for the name of an executable process in Applications Administration under Process Name.
- *Vendor* – An application developer or distributor
- *Description* – description of the respective application

A software application may contain several executable files. In this case, it is necessary to add an application for every executable file.

Example 1: Adding the Notepad application distributed with Windows into the application database.

- Select Category Text Editor
- Name – Notepad
- Process – notepad.exe
- Full Path – C:\Windows\System32\notepad.exe
- Vendor – Microsoft Corporation
- Description – A notepad

4.2.7.4 Extension categories

Extension categories are used for classification of files within the DLP module. These are a handy aid for specifying classification rules. You can limit the classification rule only to certain data types and thus make the result of the classification faster and more specific. Extensions can be edited, added or deleted any time. All extensions are arranged into categories. Categories correspond to file types according to the way the files are processed later on.

Administration of extension categories

Administration is accessible from the main menu of Safetica Management Console. In the upper part of the dialog box, there is a window which displays extension categories. The bottom part is designated for the extension database. You can look up extensions saved in the database by searching (Search). Extensions are to be entered without a dot; write only the abbreviation of the extension searched for.

To add a new extension, select the category and click on Add extension. A dialog will appear, enter the name of the extension to be added to the database . If you wish to change the category of the existing extension, double-click on it and select a new category. If you cannot find an appropriate category, create your own by clicking on *Add category*.

Extension database

The extension database contains information on all available extensions that have been categorized according to their application type. You do not have to enter all graphics or text extensions, because Safetica provides a complete list which is downloaded whenever you update the category database. When using this list, at any time you can edit and add categories and adjust the database to correspond to your needs.

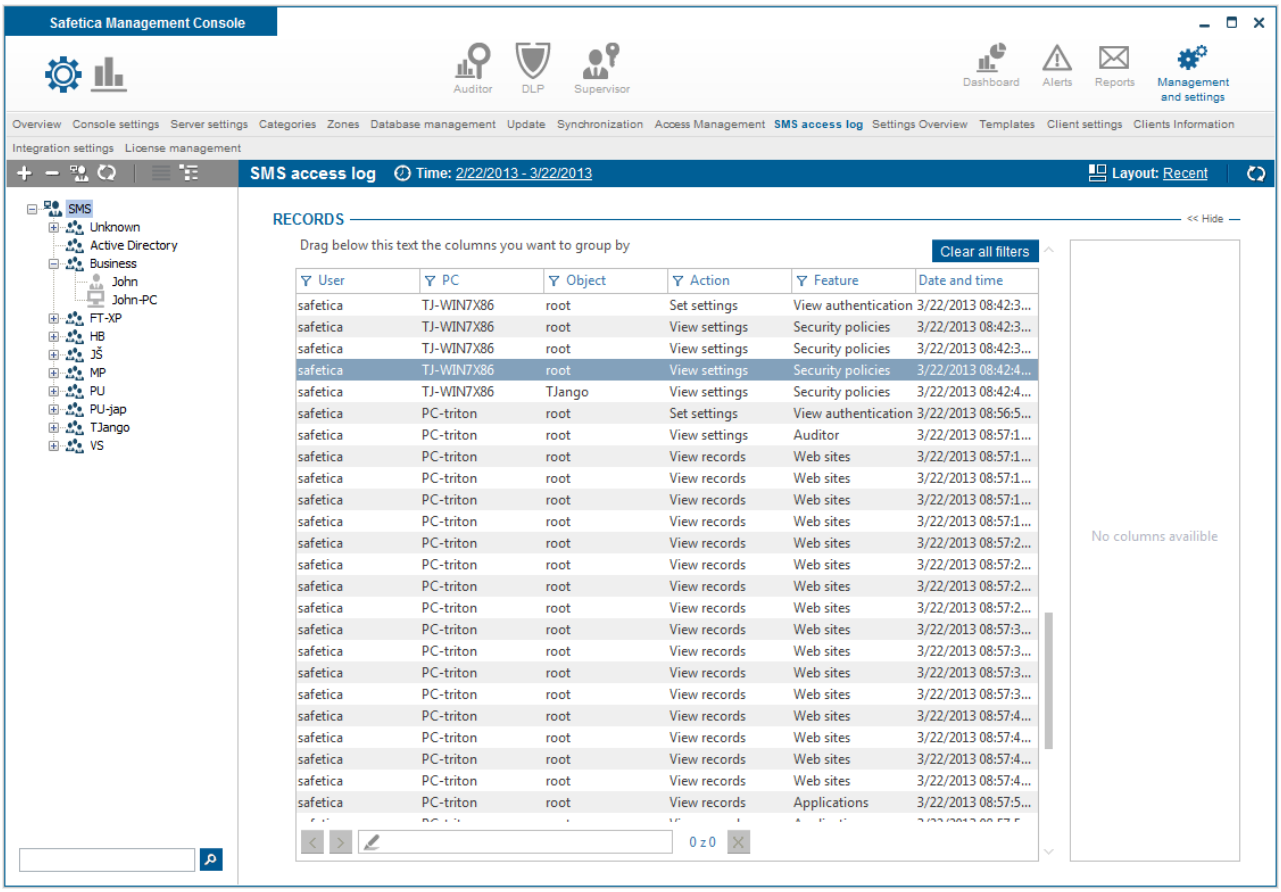
4.2.8 SMS access log

In the SMS access log you can find records of which administrator (SMS user) carried out an action and when or which user in the user tree the action was related to.

View description

Here you will find a table with records of SMS user actions. A record consists of the following information:

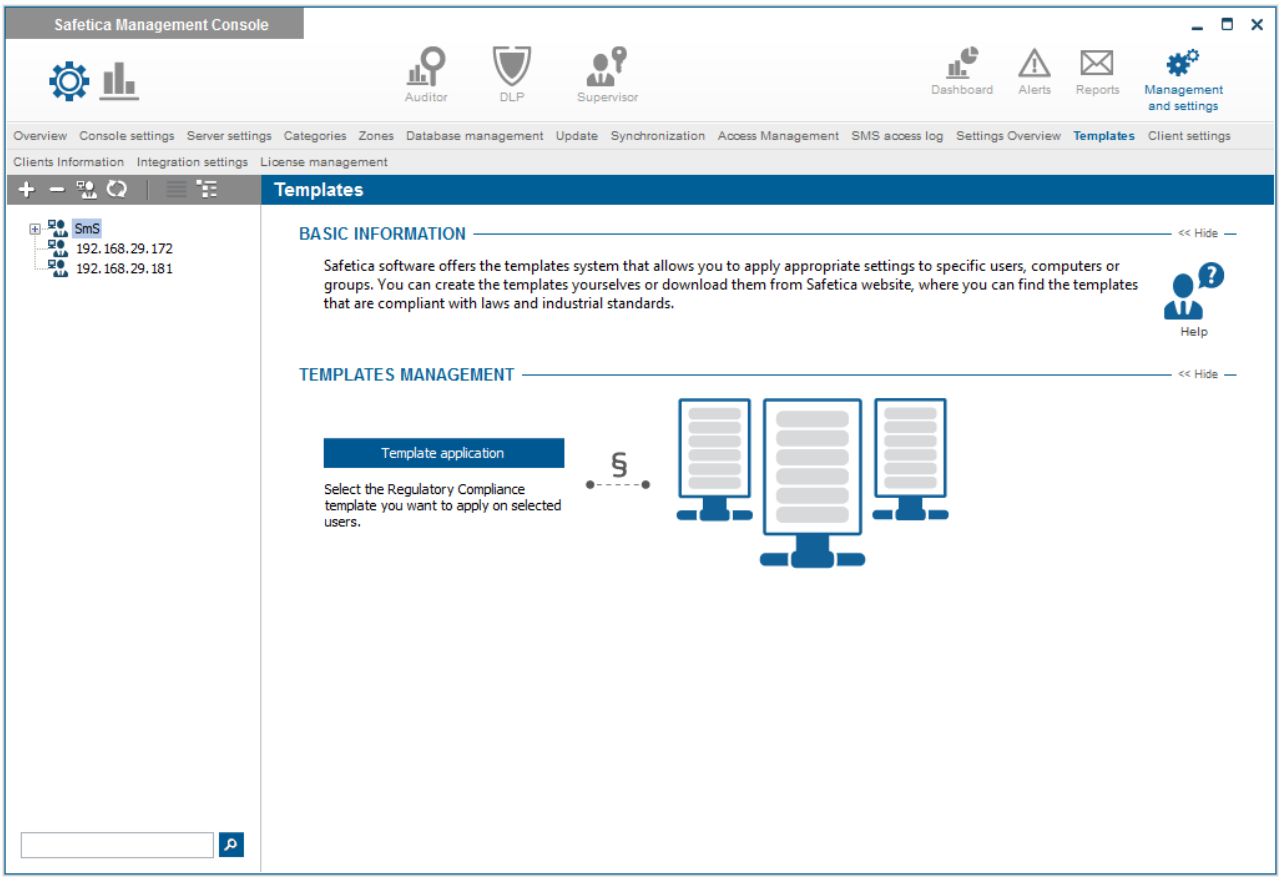
- *Date and time* – the date and time when the record was made.
- *PC* – name of the PC from which the SMS user was connected to SMS.
- *User name* – the name of the SMS user who performed the action.
- *Action* – identification of the action performed by the SMS user.
- *Feature* – name of the view (function) where the action was performed.
- *Object* – name of the user, group or computer from the user tree to which the action performed was related to.



4.2.9 Templates

Safetica software offers templates system that allows you to apply appropriate setting to specific users, computers or groups.

You can download templates from Safetica website (www.safetica.com), where you can find the templates that are compliant with laws and industrial standrds.



How to apply setting templates

Click the Template application button and follow the import wizard.

1. The first step is to locate on the hard drive the template to be exported and applied.
2. Select users, PCs or groups which you want to apply the settings template to.
3. Finish template application.

How to export setting templates

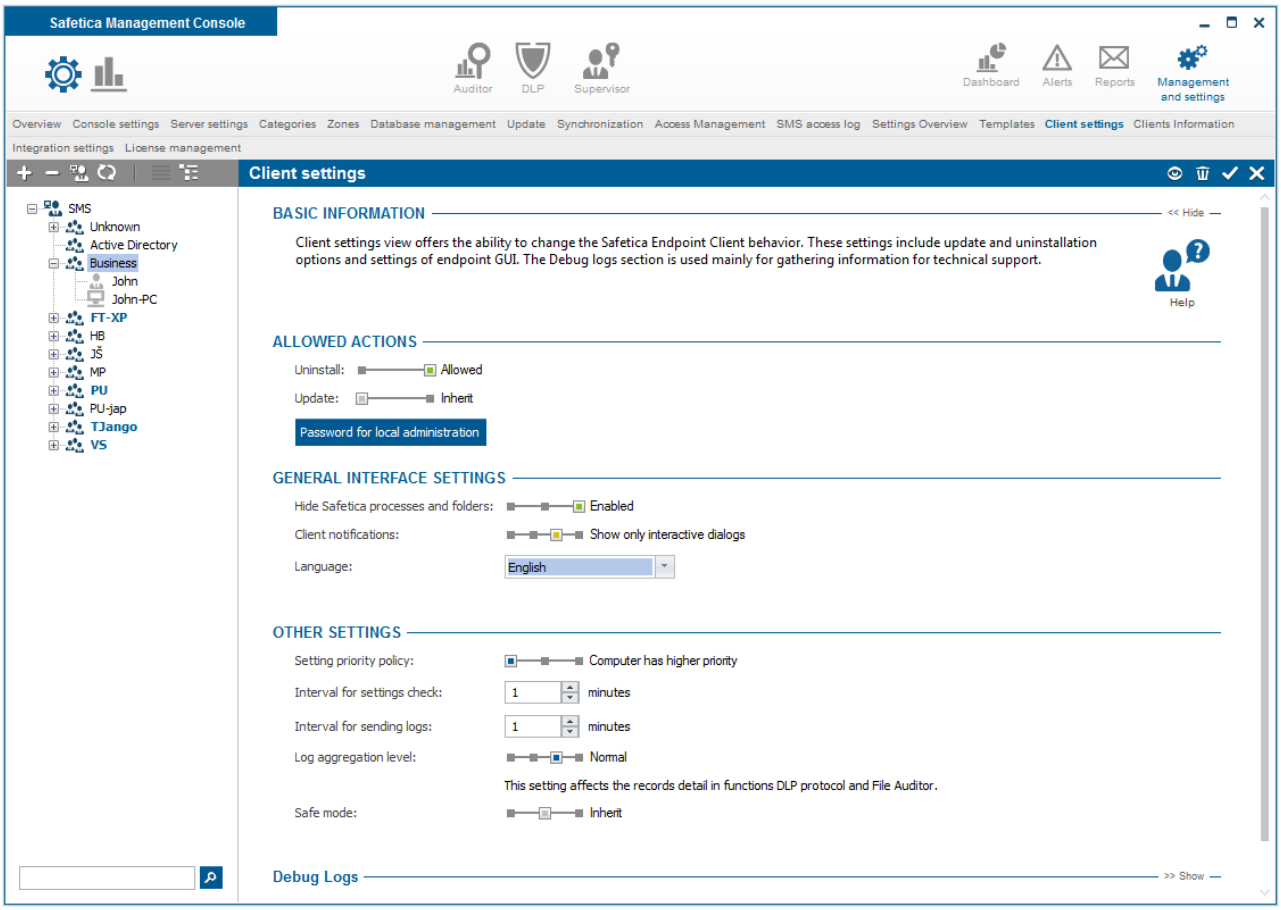
Click on the Template export button and follow the export wizard.

1. The first step is to enter the name and description of the settings template to be exported.
2. Select the user, PC or group from which you want to export the settings and specify whether you want to export effective or explicit settings.
3. Select the functions from which you want to export the settings.
4. Enter the location of the template exported and finish export.

4.3 Safetica Endpoint Client

4.3.1 Client settings

Client settings include general settings of the Safetica Endpoint Client station (SEC), which are shared by all Safetica modules.



Client deactivation

You can use the slider to disable all SEC functions. The client continues running, but only for the purpose of re-activation. If deactivation is set for any of the users logged in, then SEC is disabled for the entire end station.

Client uninstallation

You can use the slider to completely uninstall SEC from computer. This option does not require Allow uninstall option in Allowed actions.

Warning: If you do not change the setting back to the inherited, client will be uninstalled again immediately after the re-installation.

Allowed actions

By enabling Uninstall or Update, you permit uninstalling or updating the Safetica Endpoint Client. Without permitting this, it is impossible for security reasons to uninstall, update, or otherwise disrupt the running of Safetica Endpoint Client, even with administrator rights. You can use the password button to set up a new password for permitting those tasks directly from the client station, using the command line. For more about Safetica Endpoint Client protection, see Protection against unauthorized manipulation of Safetica Endpoint Client.

You can deny all locally allowed actions by clicking on *Disable local management actions*.

General interface settings

- *Hide Safetica processes and folders* – if you enable this setting, the processes STCService.exe, STMonitor.exe, STUserApp.exe and STPCLock.exe that ensure that Safetica Client Service is running will be hidden on the client station and will not be displayed in the Windows Task Manager or in any similar program that shows running processes. SEC installation and configuration folders will be hidden also (in Windows 7: *C:\Program Files\Safetica*, *C:\ProgramData\Safetica* and *C:\ProgramData\Safetica Client Service*). By doing this, you can prevent users from finding out that Safetica is running on their computers. This setting does not disable SES notification dialogs.
- *Client notifications* – using this setting you can enable or disable displaying of announcement dialogs to users working on client computers. The announcement dialogs inform users of various security events or notify them of illegal activity. You have several options for how to set notifications:
  - *Hide all* – all dialogs on SEC are hidden.
  - *Show only interactive dialogs* – dialogs are hidden except for dialogs that require user interaction.
  - *Show all* – all dialogs are enabled.
- *Language* – SEC language setting.

Other settings

- Setting priority policy – by setting the option User settings has a higher priority than computer settings, you can ensure that the settings you've assigned to the user override the settings of the computer that the user is logged on to. Under the default settings, the computer's settings have priority. You can set these priorities only for users.
- Interval for sending logs – with this setting you can determine how often the data recorded on the client stations will be sent in batches and stored in a database.
- Interval for settings check – with this setting you can determine how often Safetica Endpoint Client will query Safetica Management Service for new settings. By doing this you can affect the time required for transferring the settings made using SMC to SEC.
- Log aggregation level – here you can set how records from DLP protocol and Files function are grouped.
  - Detailed – all identical records obtained within one minute are grouped together.
  - Normal – all identical records obtained within ten minutes are grouped together.
  - Rough – all identical records obtained within one hour are grouped together.
- *Safe mode* – by selecting *Disable* you can prevent users to star Windows in safe mode.

Debug logs

Here it is possible to set the level of client debug logging from only the most Critical logs to Verbose logs. It is intended for the use of system administrators or Safetica technical support.

Network traffic monitor

Network traffic monitor records amount of sent and received data on endpoint station. Records are available in the visualization view.

Note

You can only assign client settings to users, groups or computers, that you have checked in the

user tree. To apply the settings you must save the changes by pressing the  button or you can cancel the changes by pressing the  button located on the upper right side.

4.3.2 Clients information

This view provides a list of users and computers that are connected to individual Safetica Management Services. It also contains several information about the Safetica Endpoint Client instance.

View description

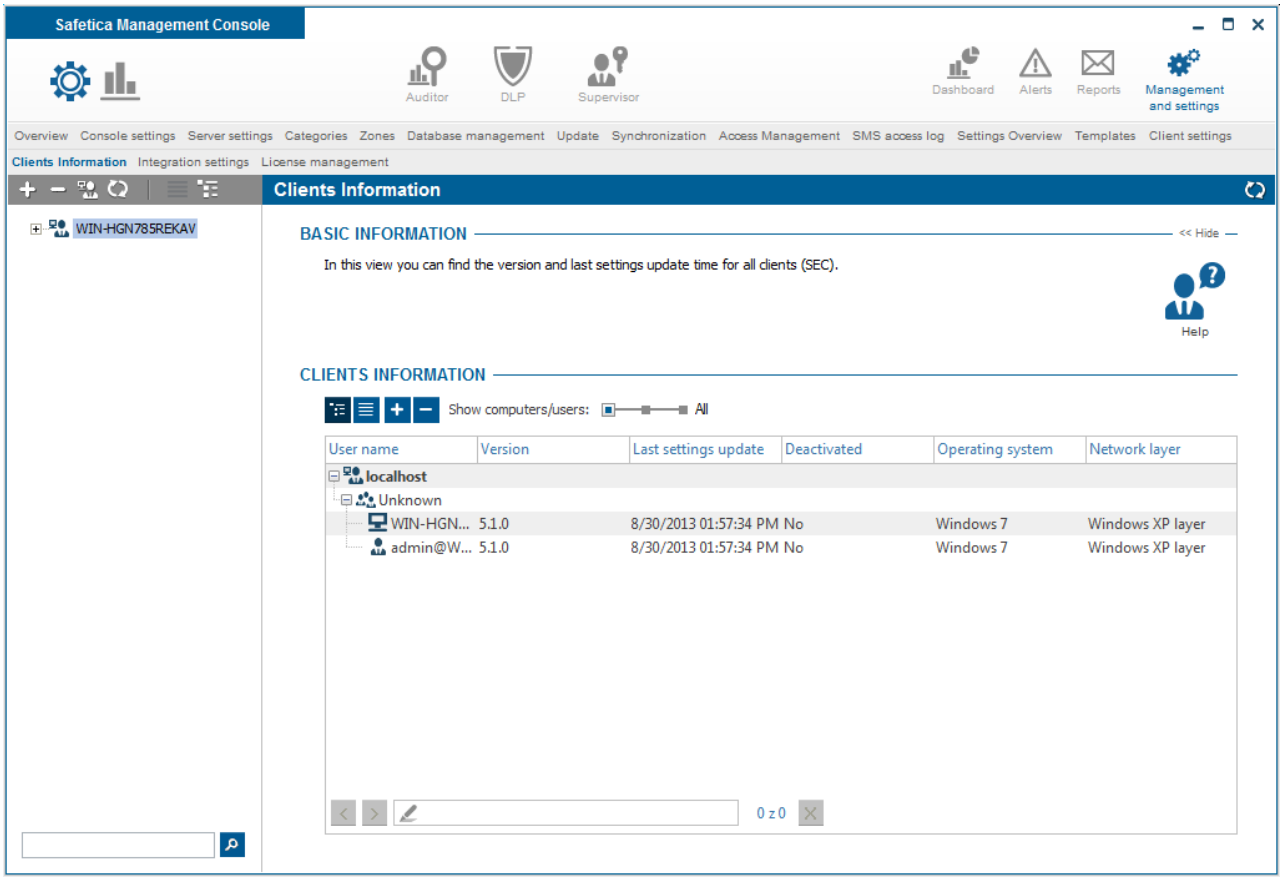
There are control buttons above the tree of users and clients. The first button displays a list of users, groups and clients in a form identical to the user tree on the left.

The second button displays all computers and users for each SMS in one list, while groups are hidden from the list.

Other controls can be used to collapse and/or expand the tree, and for filtering purposes.

The table contains the following information:

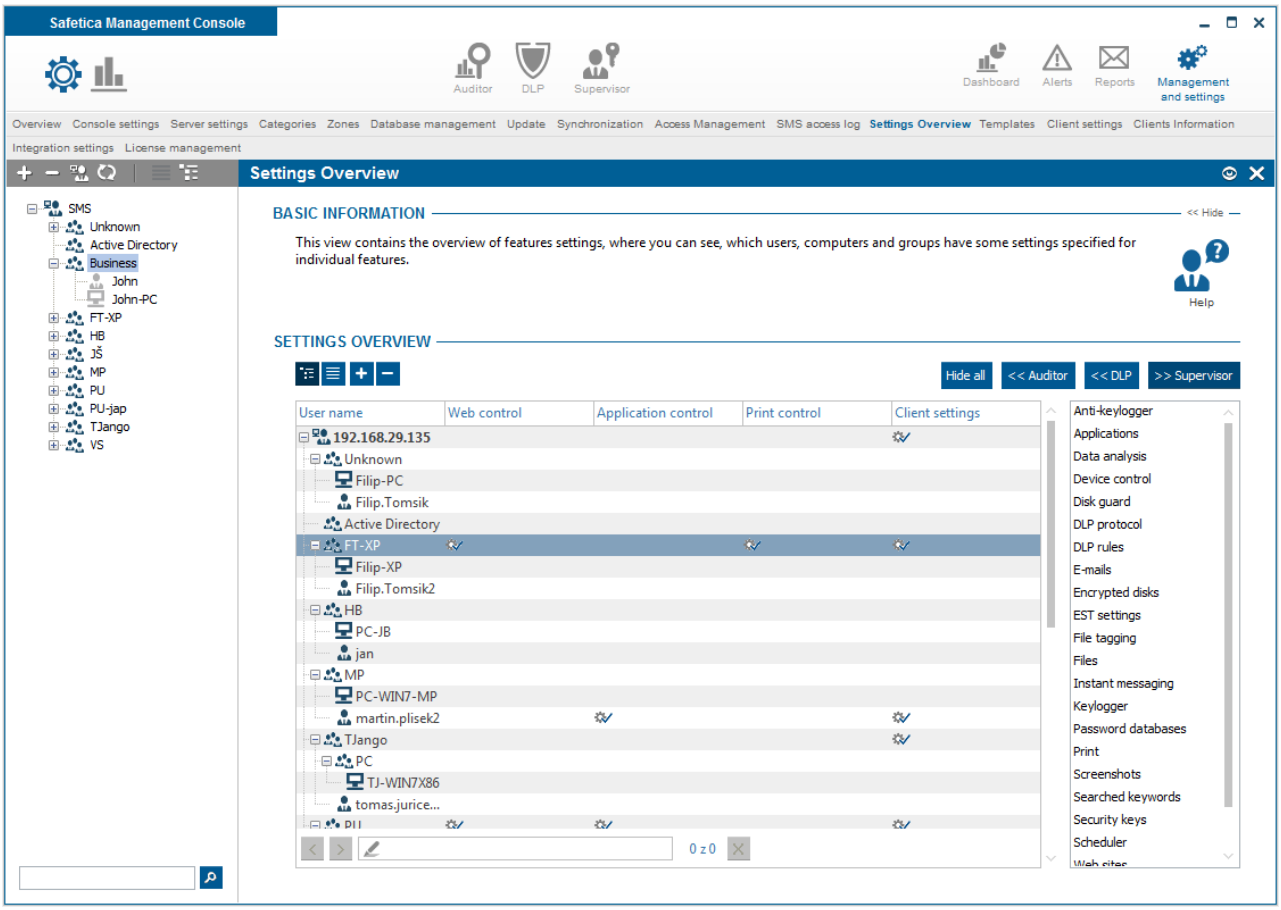
- User name – name of user, PC or group.
- Version – release number of the Safetica Endpoint Client (SEC) instance installed.
- *Last settings update* – time of last SEC settings synchronization.
- *Deactivated client* – shows if SEC is enabled on the workstation.
- *Operating system* – version of the operating system installed on the workstation
- *Network layer* – type of Safetica network layer (see Integration settings)
- *Unsent records* – contains the number of records SEC has not yet sent to the server and the time as of which the record is valid.



4.3.3 Settings overview

This view contains a table with an overview of function settings, where you can see what users, computers and groups have what settings specified for individual functions.

If a user, computer or group have settings set in any function, an image is shown in the appropriate table cell. A row represents the user, computer or group. Columns represent appropriate functions. The list of available columns can again be found on the right side of the table. Dragging a column from the list and dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. To remove a column from the table, drag it back to the list of columns on the right.



There are several buttons above the table which allow you to manage the table contents:

- On the left are buttons for management of the user tree in the table ().
- *Hide all* – hide all columns in the table
- *Auditor* – display or hide columns (functions) of Auditor.
- *DLP* – display or hide columns (functions) of DLP.
- *Supervisor* – display or hide columns (functions) of Supervisor.

4.3.4 Protection against unauthorized manipulation of Safetica Endpoint Client

Because Safetica Endpoint Client is responsible for the enforcement of your company's policy on end stations, it must be protected from unauthorized intervention by users who seek, for example, to circumvent blocking or monitoring by turning Safetica Endpoint Client off. Safetica Endpoint Client is also protected against intervention by a user with administrator rights.

The uninstallation, updating, or turning off of SCS can be set from SMC or it can be done directly from an end- station, with commands and a password generated by SMC.

What is being protected?

- *Registries* – it is not possible to display or change records in registries concerning the Safetica Endpoint Client, including the SMS IP address.
- *Processes* – all Safetica Endpoint Client processes are protected. They are protected against being stopped and it is also possible to turn on the hiding of them in Client settings , so that the list of processes cannot be seen.

- *Service (STCService)* – it is not possible to turn off the STCService service even with administrator rights. •
- *Installation file* – it is not possible to move or rename files and folders in the Safetica Endpoint Client installation folder
- *Database files* – these cannot be moved, renamed, or deleted. The contents of databases are encrypted.
- *Uninstallation* – SEC is protected from uninstallation.
- *Tags* – file symbols (tags) are protected against rewriting or changes.

Uninstall and update permission from SMC

In Client settings of each module, permission can be granted by checking Uninstall, or Update in the user tree for selected users, groups, or end stations, or by changing the password for local administration (see below). By checking these and saving, you will permit these tasks to be executed with respect to the Safetica Endpoint Client component on end stations.

Permitting the uninstalling, updating, and turning off of SCS from SEC

Permission for these tasks can also be granted directly from the end station on which the Safetica Endpoint Client is installed. You must first generate a password for selected users in the SMC (*Client settings -> Allowed actions)*.

The following password is set as the default for all users: *safetica*

You can assign a password in Client settings by clicking *Password.* You will be asked to enter your new password.

The following commands are required:

1. Launch the command line as an administrator
2. Go to the Safetica Endpoint Client installation folder. The standard path is: C:\Program Files \Safetica\
3. Then enter the following commands into the command line, based on what you need. After you have entered these commands, you will be asked for the password you generated in the Safetica Management Console

   To permit the turning off of the service (STCService), execute the following command:

   STCService -allow stop

   This command will make it possible to stop the STCService by subsequently launching the file StopClientService.bat or restarting the service with the file RestartClientService.bat. This is not possible without permissions!

   To permit the uninstallation of the Safetica Endpoint Client:

   STCService -allow uninstall

   To permit updating the Safetica Endpoint Client:

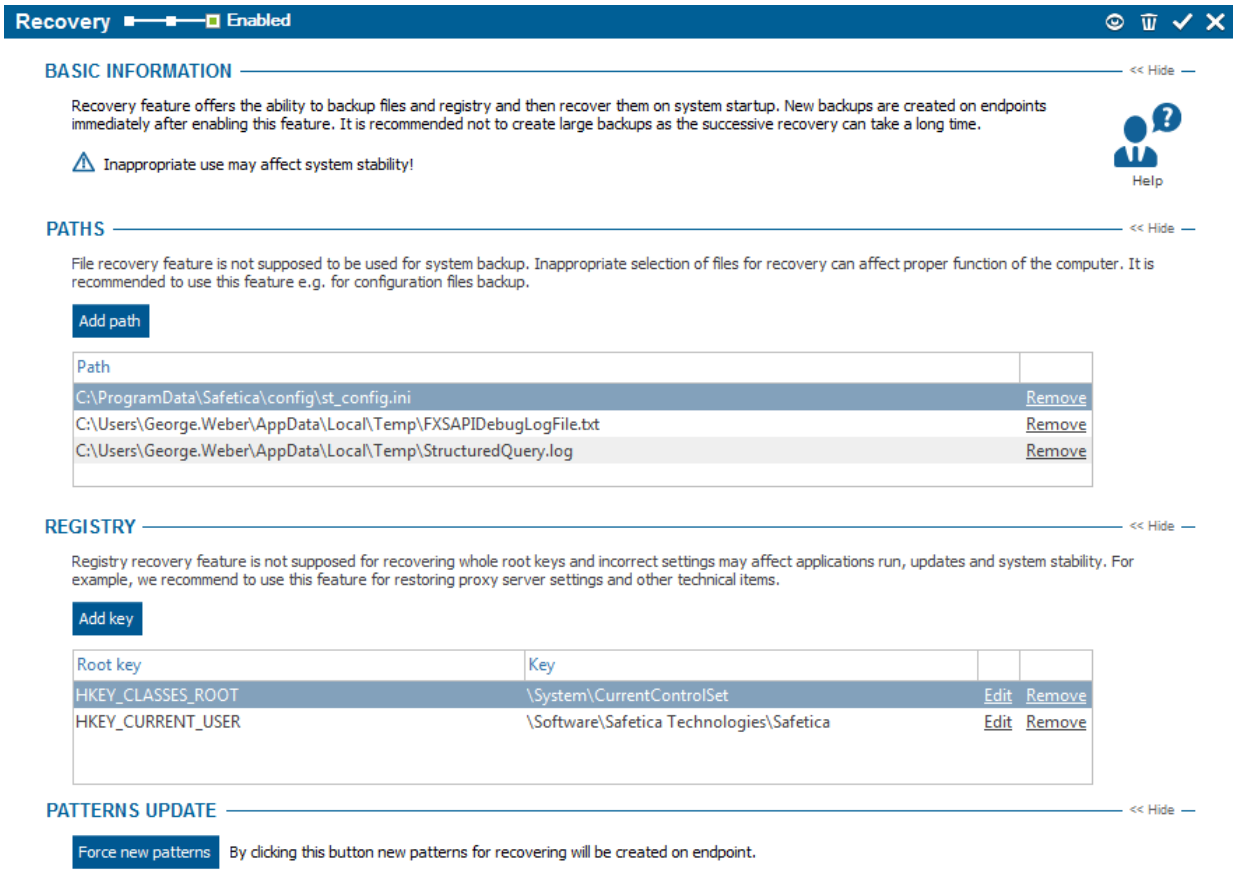
   STCService -allow reinstall

   ATTENTION: These commands do not execute the relevant tasks, they only grant permission for them.
4. After launching the commands mentioned above, permissions will be applied until you launch the command STCService - deny. This command will cancel all permissions that you granted with the previously mentioned commands. This operation does not require a password.

4.3.5 Recovery

With this function you can choose system paths and records in Windows registers where a backup will be made. After restarting your operating system, the registers and selected paths will be restored from this backup. Required backups will be made on the PC with Safetica Endpoint Client immediately after the function has been set.

Warning: This function must NOT BE USED for creating backups of large files. It is intended only for small configuration files or records in the register. Any inappropriate use can affect the operation and stability of the operating system.



Settings

In the console setting mode you can disable or enable this function by using the slider on the screen top.

- *Disabled* – restoration is disabled.
- *Inherit* – function is not set. The settings are inherited from the higher-level group.
- *Enabled* – this option will enable the restoration function.

The restoration function is set only for users, groups or PCs marked in the user tree. To apply the settings, you need to save the changes with the button or you can cancel the changes with at the top right.

Paths

In this section you can add a path to the file you wish to back up. Add the path with the button Add path.

Registry

In this section you can enter the key to the record in the register you wish to back up. Enter the key

with the button Enter key.

In the dialog which appears, select the root key type and in the field below enter the path to the key in the register.

Example:

HKEY_CURRENT_USER

\Software\Safetica Technologies\Safetica

Patterns update

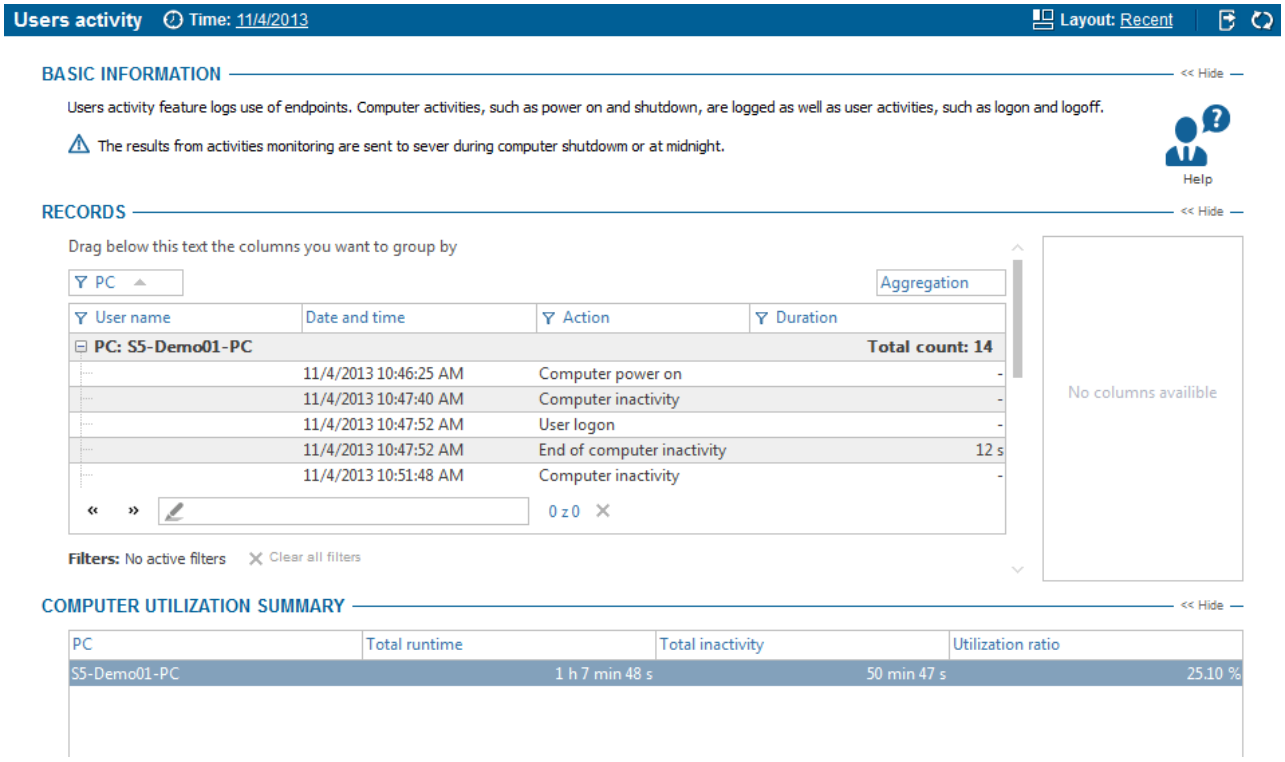
You can enforce the update of backed-up paths and registers with *Force new patterns* button. The old backup will be overwritten with current configuration files or register records.

4.3.6 Users activity

In this section you will find records on the activity on workstations where the Safetica Endpoint Client is installed.

You can display user activity in the main section of *Management and settings -> User activity*.

Note: Workstation activity records are sent to the server upon shutting down the PC or at midnight. They are therefore not immediately available after the record has been made.



View description

At the top of the visualization you will find a table with records of user actions on the end station. The records give the following information:

- *Date and time* – date and time of record creation
- *PC* – name of PC where the record was made
- *User name* – name of user under which the record was made
- *Action* – type of action recorded:
  - *Computer power on* – PC start

- *Computer power off* – PC shutdown
- *User logon* – user login
- *User logoff* – user logout
- *Lock* – PC locking
- *Unlock* – PC unlocking
- *Computer inactivity* – the user was not working with the PC
- *End of computer inactivity* – time when the user started working with the PC again
- *Sleep*
- *Wakeup*

- *Duration* – shows time from action start to action end (e.g. from Start to Shutdown, from Login to Logout, from Inactivity start to Inactivity end, from Locking to Unlocking)

At the bottom you will find a summary of how the PCs were used. The table contains records with information showing how the PCs where SEC is installed were used.

- *PC* – name of PC where the record was made
- *Total runtime* – total PC run time
- *Total inactivity* – time over which the PC was not used
- *Utilization ratio* – use of a PC for an activity, in percent (user was working on the PC)

4.4 Managing components using the command line

You can both locally control Safetica Endpoint Service and Safetica Client Service, and manage their advanced settings through the command prompt.

4.4.1 Safetica Management Service

Safetica Management Service runs on the server as a service. To start working with SMS, launch the command prompt as an administrator (cmd). Open the installation file of SMS (the default is C:\Program Files\Safetica Management Service) and then you may enter the following commands:

STAService.exe -install

Installs SMS onto the system.

STAService.exe -remove

Removes SMS from the system.

STAService.exe -start

Starts SMS.

STAService.exe -stop

Stops SMS.

STAService.exe -adminport <new port number>

Creates a new number for the port on which SMC and SMS communicate. The default port number is 4441. This takes effect after you restart SMS.

STAService.exe -clientport <new port number>

Creates a new number for the port on which SEC and SMS communicate. The default port number is 4438. This takes effect after you restart SMS.

STAService.exe -console

Run Safetica Management Service in command line, for debugging only.

In the SMS installation folder you can also find startup files for easier starting, closing and restarting of SMS:

- *stop.bat*

  STAService.exe -stop

  STAService.exe -remove

- *restart.bat*

  STAService.exe -stop

  STAService.exe -remove

  STAService.exe -install

  STAService.exe -start

Changing the connection port for Safetica Endpoint Client

If you want Safetica Management Service to listen for client connections on a port other than 4438, perform the following steps:

1. On the computer with SMS start the command line with administrative privileges
2. Go to the installation folder of Safetica Management Service. C: \Program Files\Safetica Management Service by default.
3. Run command *STAService.exe -stop*
4. Run command *STAService.exe -clientport <new port number>* (for example *STAService.exe -clientport 1234*)
5. Run command *STAService.exe -start*

Changing the connection port for Safetica Management Console

If you want Safetica Management Service to listen for client connections on a port other than 4441, perform the following steps:

1. On the computer with SMS start the command line with administrator privileges
2. Go to the installation folder of Safetica Management Service, the default is C: \Program Files\Safetica Management Service.
3. Run command *STAService.exe -stop*
4. Run command *STAService.exe -adminport <new port number>* (e.g. *STAService.exe -adminport 1234*)
5. Run command *STAService.exe -start*

4.4.2 Safetica Endpoint Client

Safetica Client Service is a component of Safetica Endpoint Client (SEC) and it runs on the client stations as a service. Launch the command prompt as an administrator to start working with Safetica Client Service. Open the installation folder of SEC (the default is C:\Program Files\Safetica) and then you may enter the following commands:

STCService.exe -help

Displays a list of usable switches together with their descriptions in the command prompt.

STCService.exe -install

Installs Safetica Client Service onto the system.

STCService.exe -remove

Removes Safetica Client Service from the system. It is necessary to first enable this action by entering the command STCService.exe -allow <stop|uninstall|reinstall>

STCService.exe -start

Starts Safetica Client Service.

STCService.exe -stop

Stops Safetica Client Service. It is necessary to first enable this action by entering the command STCService.exe -allow stop

STCService.exe -server <SMS IP address>[:port]

Sets the address of Safetica Management Service (i.e. the address of the server to which SEC or SCS will connect). It is necessary to first enable this action by entering the command STCService.exe -allow connection. This takes effect after you restart STCService.exe (SCS).

STCService.exe -unknown <yes|no>

Enables or disables receiving unknown server certificates. It is necessary to first enable this action by entering the command STCService.exe -allow connection. This takes effect after you restart STCService.exe (SCS). By default, receiving of unknown server certificates is enabled.

STCService.exe -network <yes|no>

Enables or disables network mode, i.e. connecting the client (SEC) to the server (SMS/SQL). When the network mode is disabled, it is only possible to use Endpoint Security Tools on the client. It is necessary to first enable this action by entering the command STCService.exe -allow connection. This takes effect after you restart STCService.exe (SCS). Network mode is enabled by default.

STCService.exe -allow <stop|uninstall|reinstall|connection|layer|debug>

Enables one of the given actions, each of which requires entering the main password (by default this password is safetica). The password can be changed locally by entering the command STCService.exe -password, or remotely in SMC.

STCService.exe -deny

Disables enabled actions by entering the command STCService.exe -allow <...>

STCService.exe -list

Displays the list of enabled actions.

STCService.exe -password

Sets a new main password for enabling actions. You must know the old password as well.

STCService.exe -debug <0|1>

Enables or disables extended logging for debugging.

STCService.exe -installlayer

Install recommended Safetica network layer.

STCService.exe -installlayer [default|win8]

Install LSP (default) or WFP (win8) Safetica network layer, which is used for monitoring and blocking web sites.

STCService.exe -removelayer

Remove Safetica network layer.

STCService.exe -checklayer

List of currently installed network layers.

STCService.exe -console

Run Safetica Client Service in command line, for debugging only

STCService.exe -clear <*log*|*settings*|*settingswrite*|*settingscommon*>

Clear all data from selected table in local Safetica database.

In the SEC installation folder you can also find startup files for easier closing and restarting of SCS:

- *StopClientService.bat*

  STCService.exe -stop

- *RemoveClientService.bat*

  STCService.exe -stop

  STCService.exe -remove

- *RestartClientService.bat*

  STCService.exe -stop

  STCService.exe -start

How to manually stop STCSevice

To manually stop STCService perform the following steps:

1. On the computer with SEC start the command line with administrative privileges.
2. Go to the installation folder of Safetica Endpoint Client, by default this is C:\Program Files \Safetica
3. Run command *STAService.exe -allow -stop*
4. Enter the administrative password when prompted, by default this is safetica
5. Run command *STAService.exe -stop*
6. Run command *STAService.exe -remove*
7. For security reasons, run command *STCService.exe -deny* command (this disallows all actions for which permissions had been granted)

How to change the IP address of Safetica Management Service (SMS) on Safetica Endpoint Client (SEC)

If you incorrectly set the IP address of SMS during installation, or if the IP address of the computer with SMS has changed, you must manually change the connection IP address on the SEC side. To change the IP address of the SMS on SEC, perform the following steps:

1. On the computer with SEC start the command line with administrator privileges.
2. Go to the installation folder of Safetica Endpoint Client, by default this is *C:\Program Files \Safetica Insight*
3. Run command *STCService -allow stop*

4. Enter the administrative password when prompted, by default this is *safetica*
5. Run command *STCService -stop*
6. Run command *STCService -allowconnection*
7. Enter the administrative password when prompted, by default this is *safetica*
8. Run command *STCService.exe -server <IP address SMS>* (e.g. *STCService.exe -server 192.168.1.1* if the server IP address is 192.168.1.1).
9. Run command *STCService -start*
10. For security reasons, run command *STCService.exe -deny* command (this disallows all actions for which permissions had been granted).

How to remove the Layered Service Provider (LSP) layer

Safetica uses its own LSP layer to monitor network traffic. Sometimes it is necessary to remove this layer from the system. To do this, perform the following steps:

1. On the computer with SEC start the command line with administrator privileges
2. Go to the installation folder of Safetica Endpoint Client, by default this is C:\Program Files \Safetica
3. Run command *STCService -allowstop*
4. Enter the administrative password when prompted, by default this is safetica
5. Run command *STCService -stop*
6. Run command *STCService -allowlsp*
7. Enter the administrative password when prompted, by default this is safetica
8. Run command *STCService.exe -removelsp*
9. Run command *STCService -start*
10. For security reasons, run command *STCService.exe -deny* command (this disallows all actions for which permissions had been granted)
11. Restart the PC

4.5 Dashboard

With the Dashboard view you can display charts from all modules and functions in a single place. This brings together the most important summaries to give you a quick overview of the status of your organisation. These may be monitoring results, security incidents, or logs of blocked web pages or applications.

The overview is available from the main menu of the *Safetica Management Console -> Dashboard*.

Data in the Dashboard is only shown for the users, computers, or groups that you have selected in the user tree. Available charts can be found in the list on the right. Charts of individual functions are divided by functions and modules. Clicking on them and dragging them to the chart viewing area will show them. To remove a group of charts from the list, click on the button in the top right corner of each group of charts. You will find more about using graphs in Logs and visualization mode.

You can export displayed charts to PDF using the button .

4.6 Reports

By means of automated reporting included in Safetica, you can keep abreast of the current situation inside your company. You can have activity reports sent to you, either for individual employees or for whole offices. To change the settings for reporting, go to *Reports* under the main menu.

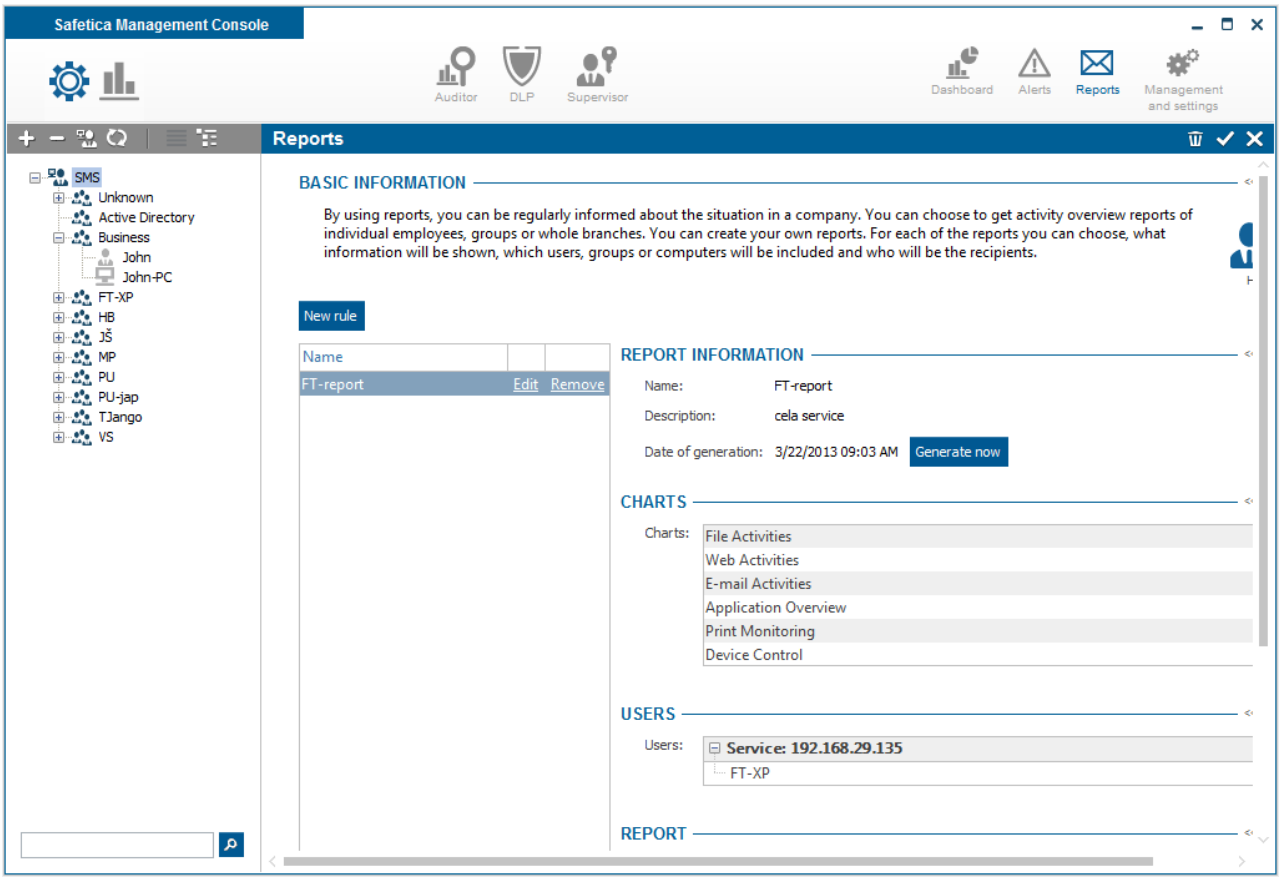
You can create your own layout for the reports. In each report, you can choose what it will contain, which users, groups, or computers it will concern, and who should be sent the report. Each report can only be created for the user account from which you are presently connected to the server. In short, each list will not show reports that have been created under a different account.

View description

The left part of the view contains a list of the reports that have been created. Selecting a report in the list on the left will show, on the right, its properties such as its name, the date on which it was last generated, a list of included reports, a list of users included in the report, and a list of e-mail addresses to which the report will be sent and in what format.

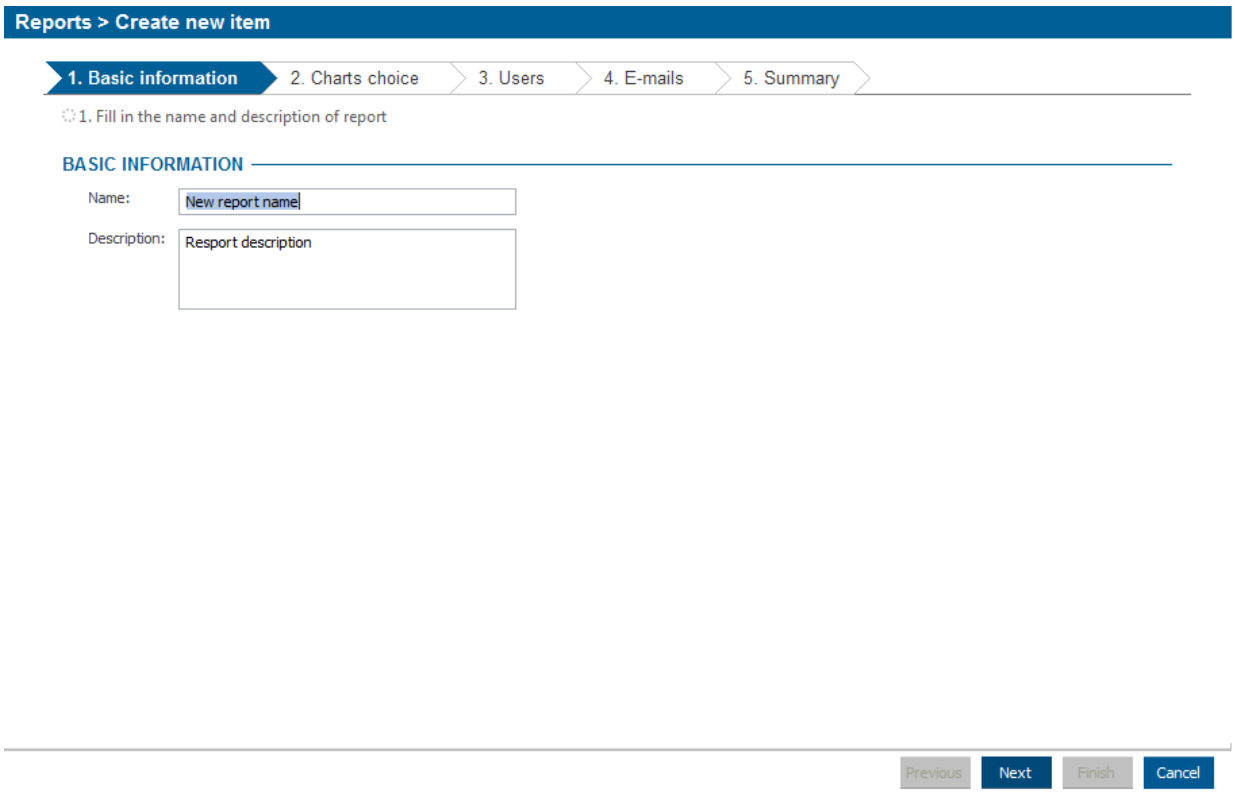
You can start generating a report right away by clicking on the Generate Now button.

You can bring an item up to date by clicking on the Edit button next to it.



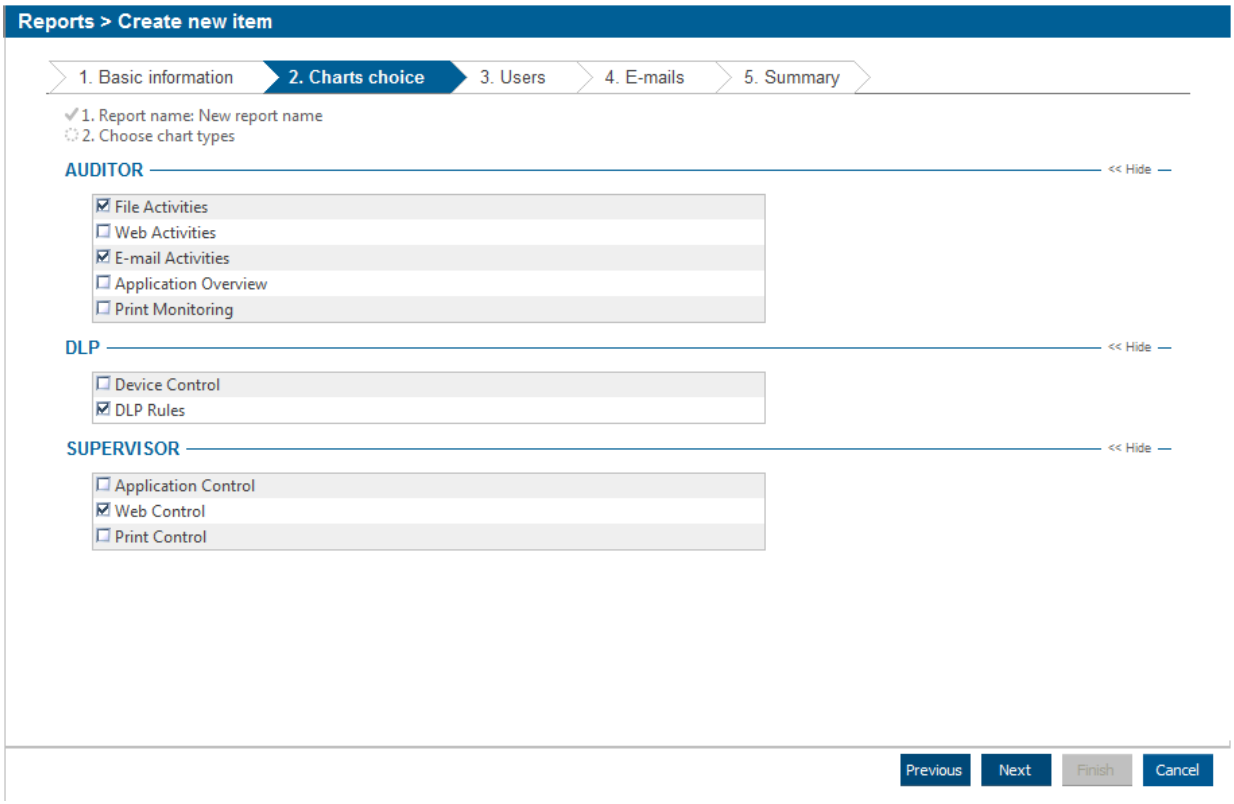
Creating a new report

1. To create a new report, click on the *Add report* button.
2. Enter a name and a description for the new report and click on *Next* in the right bottom corner.

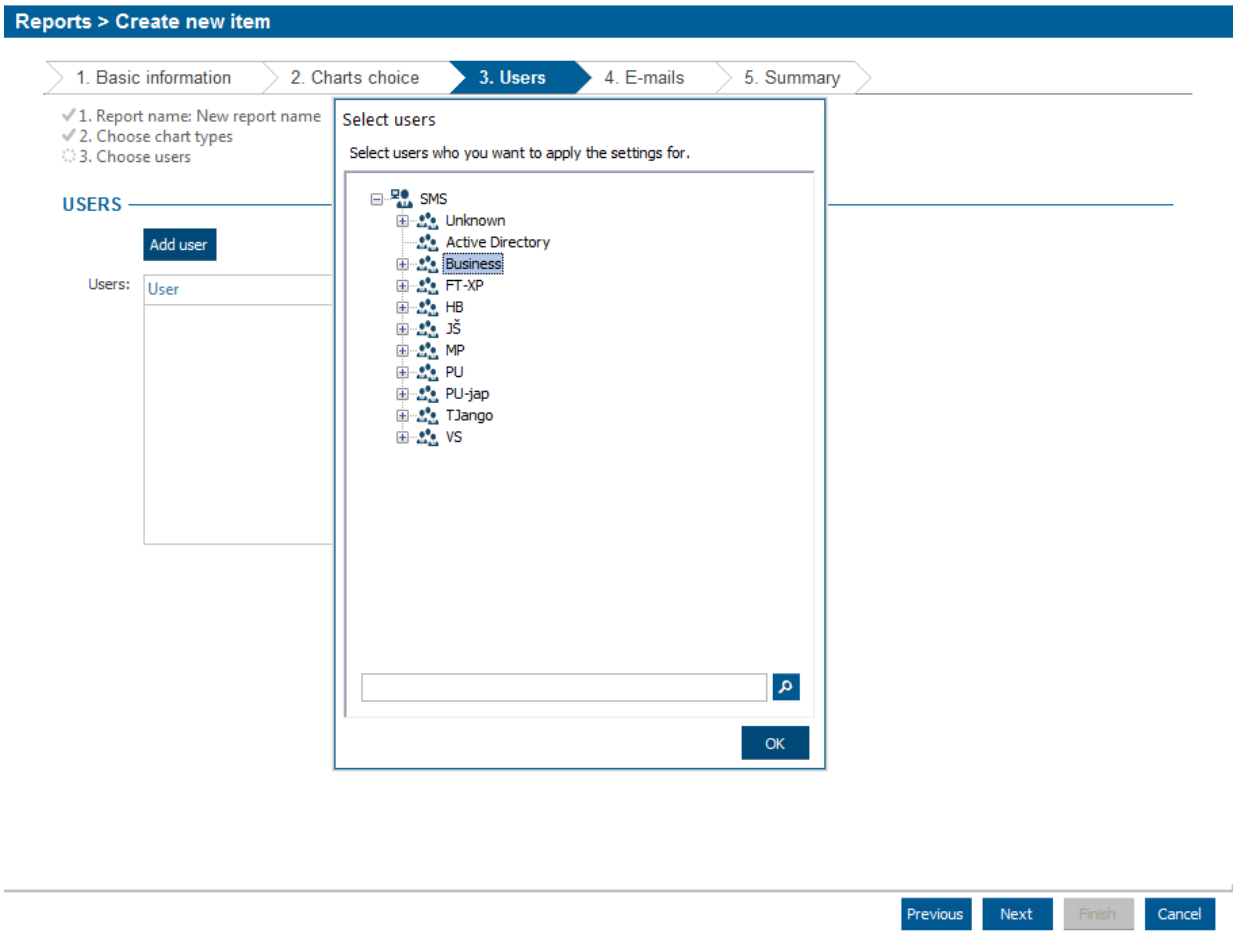


3. In the next step you will see lists of records divided into reports with charts and reports created into an Excel table (.xls). You can therefore choose required reports from the list. You

can include several types of records from all modules and tables at once. For reports exported from the table you can also specify for what application categories Excel records shall be created. You can display the Add category dialog by clicking the Add category button.



4. In the next step, click on the *Add users* button. You will be presented with a dialog for choosing individual users, computers, or groups. Reports generated according to the specification provided in the previous step will then be sent exclusively about the selected users, computers, and groups. Click on the *Next* button.



5. For the next step, specify in greater detail the frequency, type of generation, and the recipients of the generated reports.

   a. Click on the *Add e-mail address* button to add e-mail addresses of recipients.

   b. Use the scrollbar to choose in what format the generated report will be sent (PDF or HTML). If you opt for PDFs, the reports will be sent as e-mail attachments.

   c. Next, choose whether you want to save the generated report to a disk file. If so, supply the path to where to the report will be saved tosave the report. The reports are saved to the computer where Safetica Management Service (SMS) is running. The entered path must exist on the computer. If reports are to be created in multiple instances of Safetica Management Service (SMS), the path must exist on each of the SMS hosts on which the report is to be created.

   d. Finally, specify if the report is to be scheduled to be sent out automatically in intervals or not. You can choose from the following options:

      i. *Do not mail automatically* – reports will not be sent on a regular basis. Manual report generation only.

      ii. *Daily* – reports will be mailed each day after midnight.

      iii. *Weekly* – reports will be mailed on Mondays after midnight.

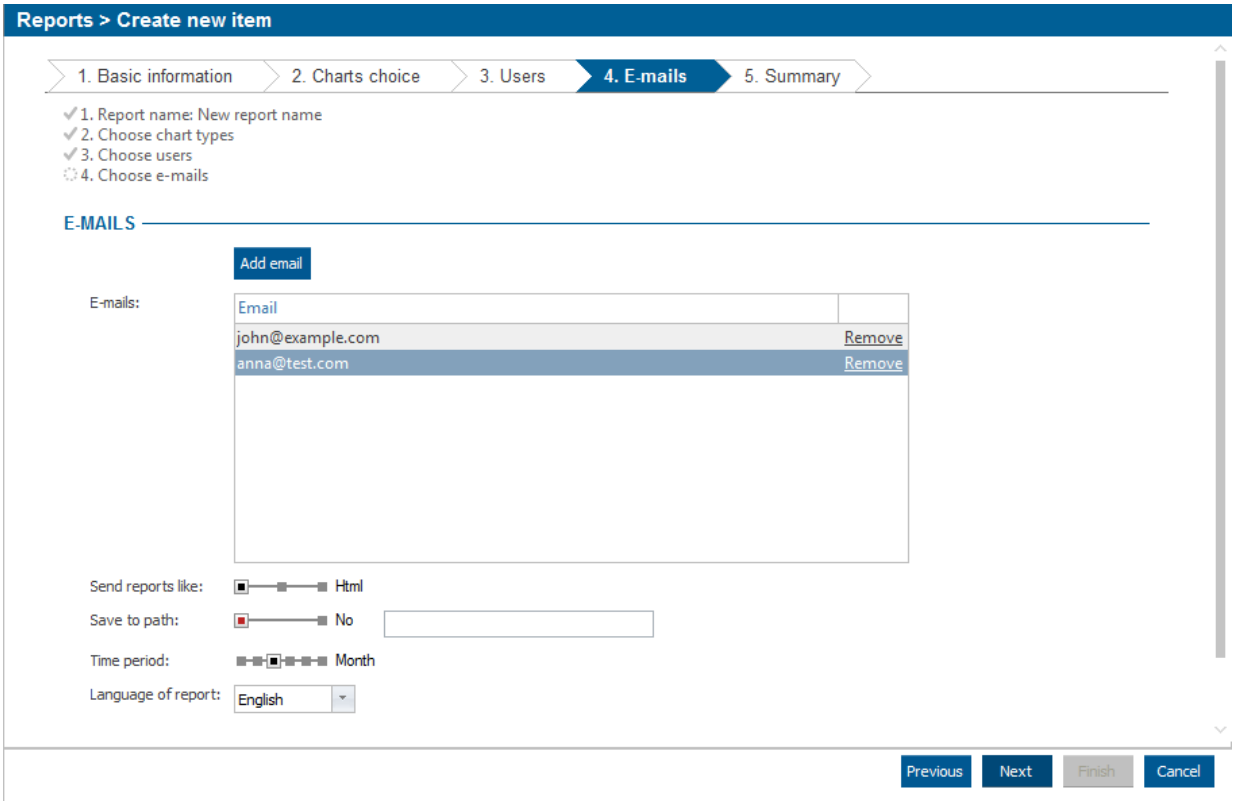
      iv. *Monthly* – reports will be sent on the first day of each month, after midnight.

      v. *Quarterly* – reports will be sent on the first day of January, April, July, or October, respectively, after midnight.

      vi. *Semiannually* – reports will be sent on the first of January and the first of July after midnight.

      vii. *Annually* – reports will be sent on January 1 after midnight.

Click on *Next* when finished.



6. The last step of the wizard will show an overview of your report generation settings. Click on the *Done* button to add the report to the list. To save the changes, click on the button.

Examples of using a new report

Assume your company has several departments, each with a couple of employees. As a manager, you want be kept up to date about the applications used and the websites visited in each department. On the other hand, you do not have the time to browse through the records and charts in the Console. This is when you create an automated monthly report. Start by choosing a suitable name and description. Then, choose the Application and Websites option from the list of available report types under the Auditor module. In the following step, select employees from the targeted department. Continue by filling in the e-mail address the report will be sent to and the format it should be sent in. Finish by specifying automated reporting on a monthly basis. Once you have saved the settings, you will start receiving a monthly overview of the applications used and the websites visited by your employees.

4.7 Alerts

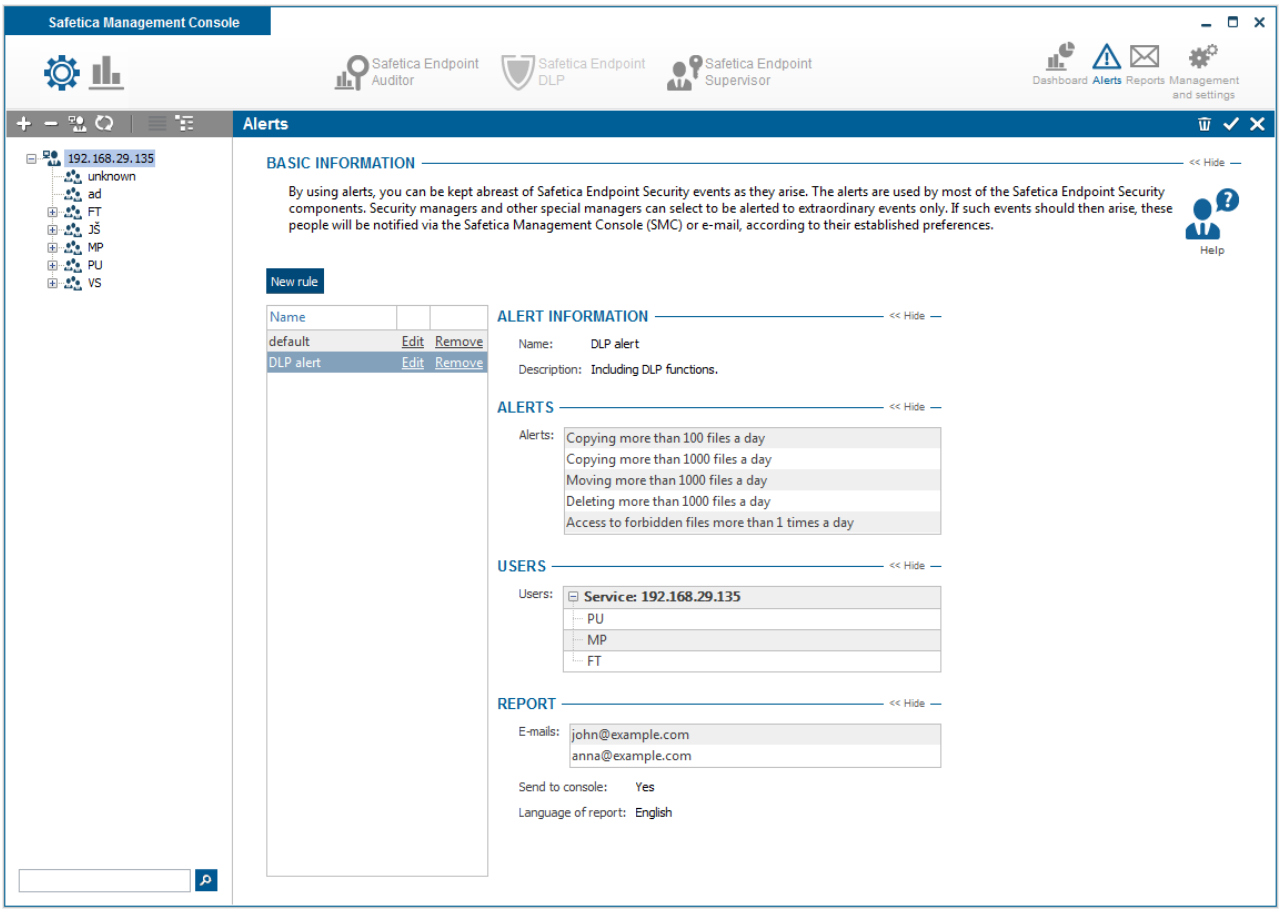
By using alerts, you can be kept abreast of Safetica events as they arise. The alerts are used by most of the Safetica components. Security managers and other special managers can select to be alerted to extraordinary events only. If such events should then arise, these people will be notified via the Safetica Management Console (SMC) or e-mail, according to their established preferences.

You can set up and view alerts in the Alerts section of the main menu (top right corner in the console).

View description

In the left part of the view you'll find a list of created alerts sets. After selecting an alert set in the list on the left, alert details, such as the name, list of notifications, the user list that the alert pertains to and the mailing list for the alert will appear on the right.

By clicking on the *Edit* button, you can update an item.

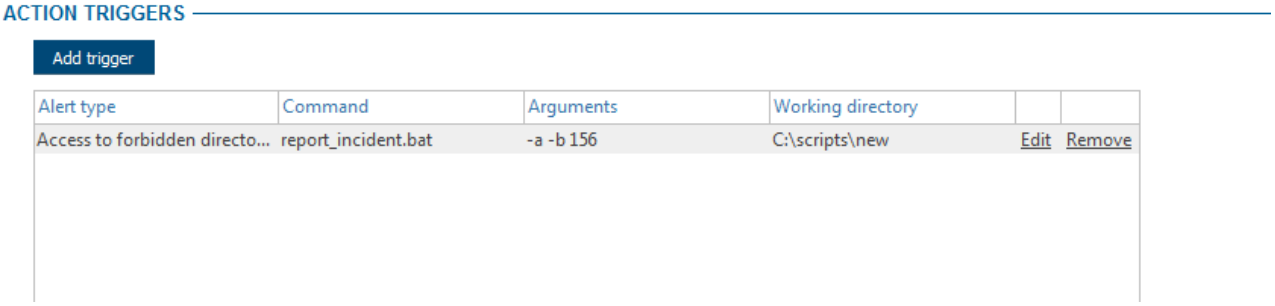


Settings

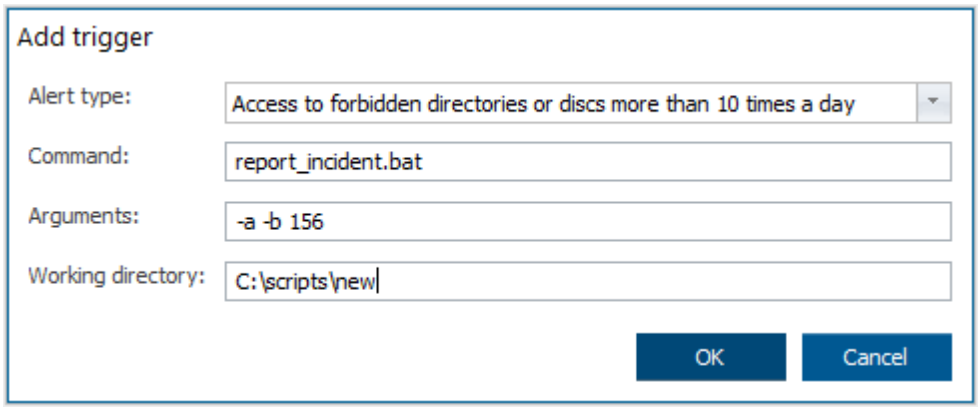
In Settings, you can choose your own alerts sets. For each alerts set, you can select the type of the alert, the target users, groups, or computers, and the destination of the alert, i.e. either the console, e-mail, or both. Each alerts set is only created for the user account via which you are connected to the server at the time of its creation. This effectively means that connecting under a different account from the list will make alerts sets created under a different account inaccessible.

Action triggers

In the Action triggers section you can set, based on activity records, the command or script start with particular arguments and in a selected folder. The command will be run on the client station with SEC under the account of the user who caused the incident. These settings apply to the entire SMS.

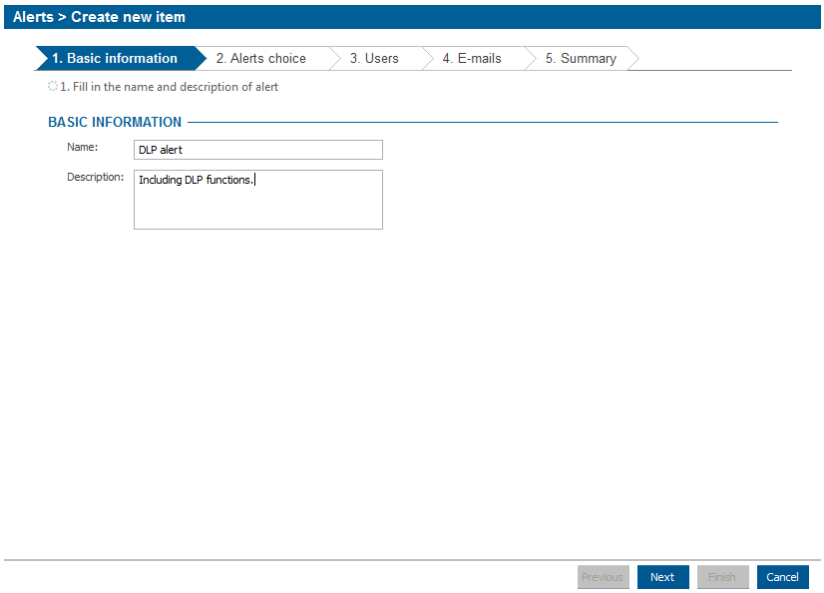


You can display dialog for adding the new trigger by clicking on *Add trigger* button.

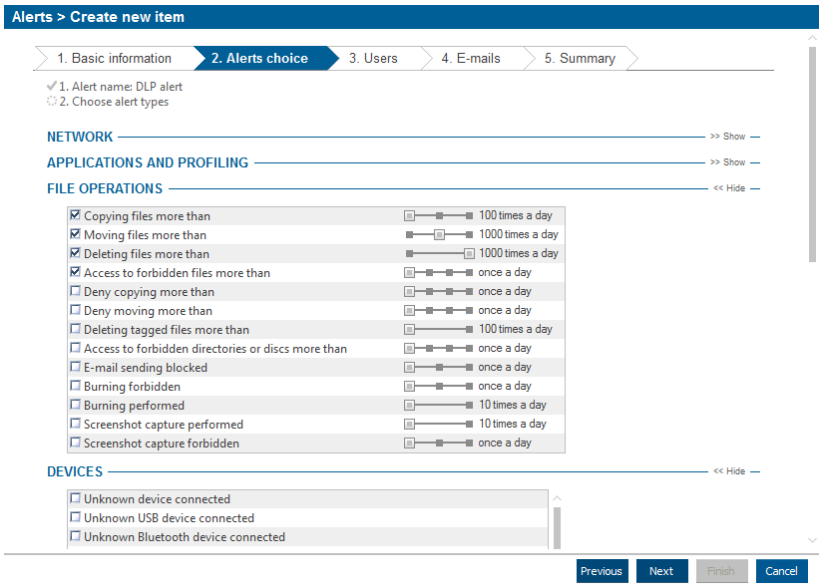


Setting up a new alert

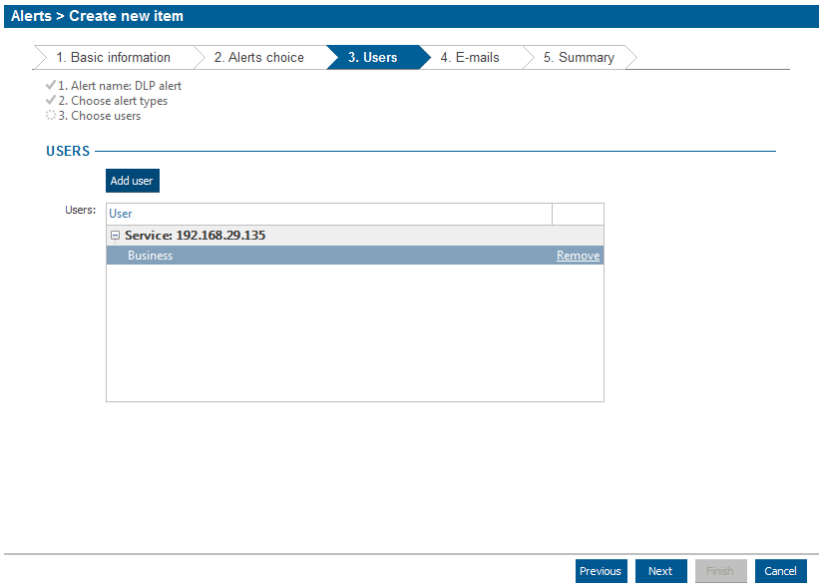
1. To create a new alerts set, click on the *New rule* button.
2. Enter a name and description for the new alerts set and click on the *Next* button in the bottom right corner.



3. Next you will see lists of various types of alerts sorted by categories. Choose the type of alert from the list. You can select multiple types of alerts from multiple categories. When finished with your selection, click on the *Next* button.

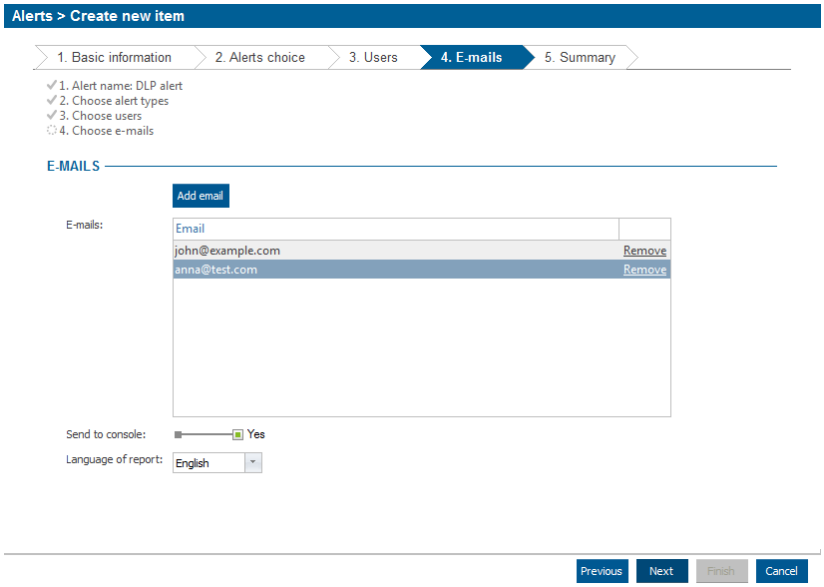


4. In the next step, click on the *Add user* button. A dialog will appear in which you can select computers, groups, or individual users. The alert you selected in the previous step will then only be sent to the users, computers, or groups you select in this step. Click on the Next button.



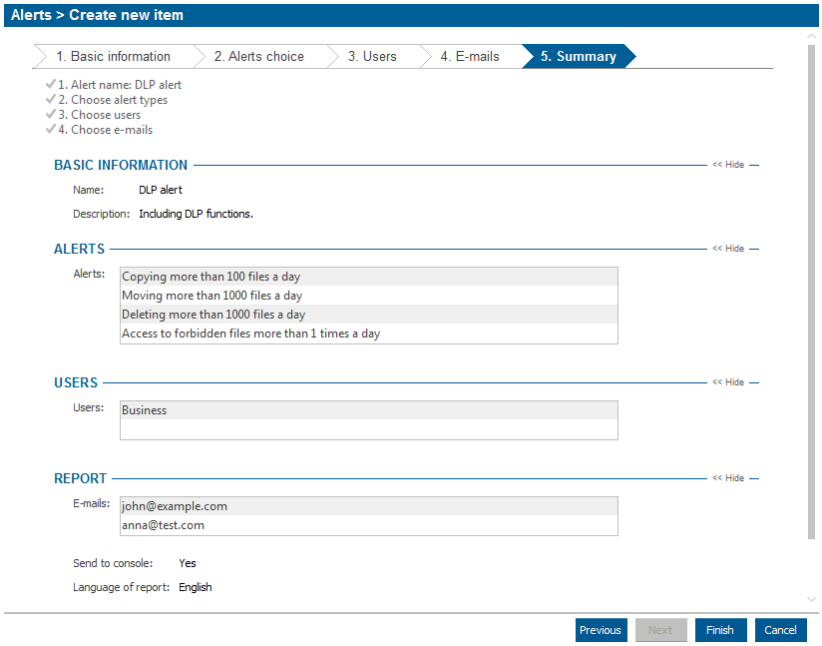
5. In this step, you will be selecting the e-mail addresses to which the alert notification will be sent. To accomplish this, click on the *Add email* button. You can also have alert notifications sent directly to the console. You can do this with the slider named *Send alert notifications to Safetica Management Console*. By using the SIEM / Syslog slider, you can activate logging to servers supporting syslogs. Just fill out the server address and port. The server must be available from the respective SMS. Click on the *Next* button.

   Note: A new warning that has arrived over the console is shown by a number above the Alert icon in the top right corner of the console. The number represents the number of the alerts that are set to be mailed to the console and have not yet been read.



6. The last step shows an overview of the settings you have made while setting up the alert.

   Clicking on the *Done* button will add the alert to the list. Finish by clicking on the  button in the top right corner to save your changes.



An example of using an alert

Suppose you have an office with several employees who are, via the Web Control function of the Supervisor module, forbidden from accessing social networks. You want to stay informed about any attempts at printing that your employees make. What you want to do in a situation like this is set up a new alert. Start by choosing a suitable name and description. Next choose the *Access to forbidden website* option from the list of available alerts under the *Network* section. In the next step, choose an employee from the given office. As the last step, set up an e-mail address to which the alert will be sent and also specify that alerts should be sent to the console. After saving your changes, you will be instantly notified, by e-mail or the console, of any attempt your employees make at accessing social networks.

Visualization

All alerts get recorded and you can view them later in the visualization mode. In the top part, you will find statistics and charts. In the bottom part of your view, is a list of generated alerts. Clicking on the relevant statistics in the bottom part of the screen will view the alerts relevant to those statistics. New, unviewed alerts are highlighted. Alerts that are set to be sent to the console are included in the figure that shows the number of new alerts that have been sent to the console. This figure is shown above the Alerts icon in the top right corner of the console.

4.8 Update

Via the Update Manager, you can discover available Safetica updates, download them, and install them. In this manner, you can centrally update to a new version of the Safetica Endpoint Client (SEC) component as well as a new version of the Safetica Management Service (SMS) component.

You can find the update management tools in Safetica Management Console (SMC) under *Management and Settings -> Update Management*.

Note: You can only manage those SMS that are connected to your SMC.

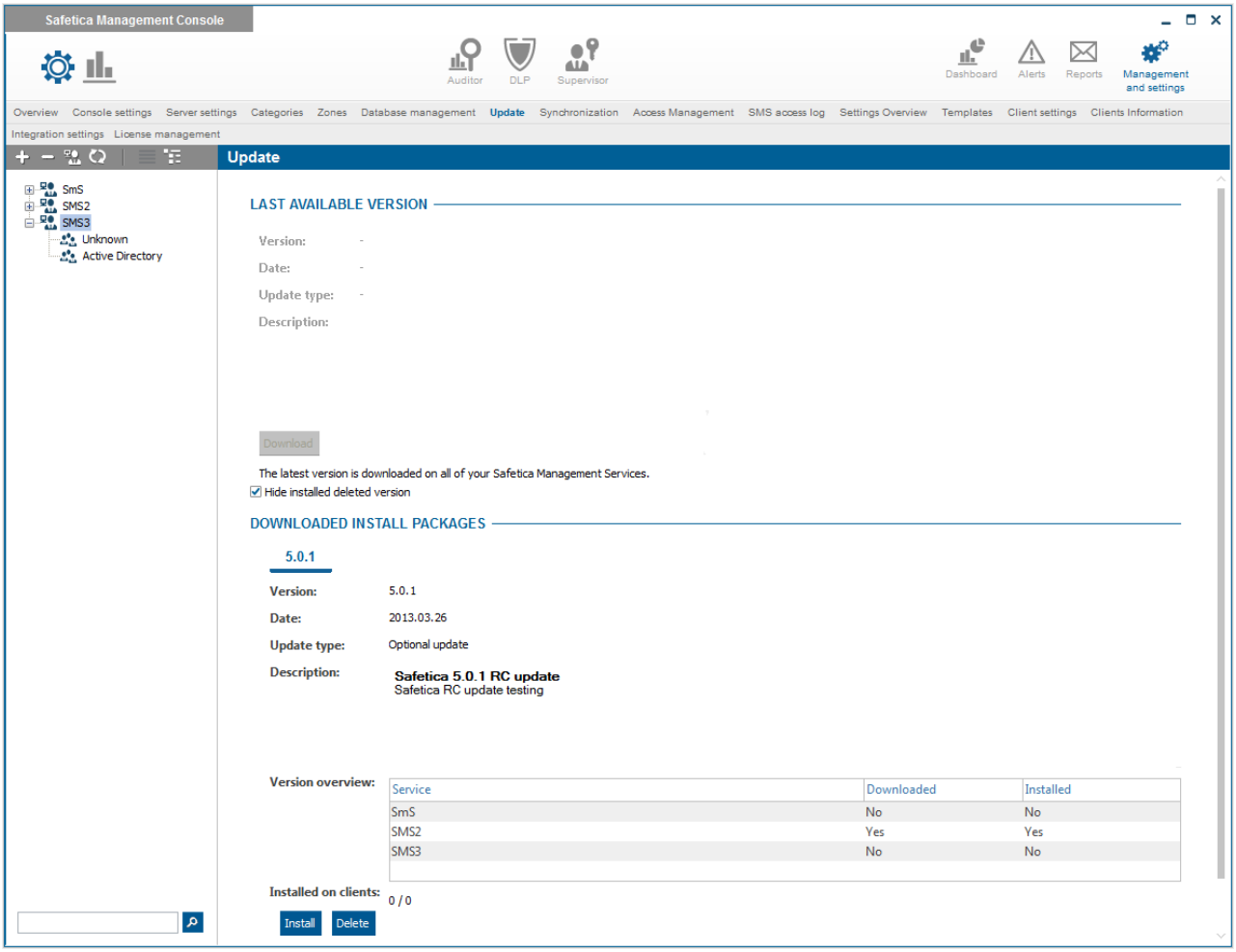
View description

In the top part of the view are up-to-date data on the last available version. The information presented contains the number of the version, its release date, update priority, and a description of changes. There is also a button for downloading the new version to the connected SMS. The update package is then downloaded to each SMS separately.

The bottom part has an overview of downloaded versions. General version information is presented there for each downloaded version, and you will find there an overview of the SMS that this version has been has been downloaded to as well as the number of SEC where this version has already been installed. Under the informative part, there are two buttons.

The *Install* button installs new versions to the connected SMS and SEC.

The *Delete* button deletes downloaded installation packages from a SMS.



Downloading updates to SMS

1. To download an up-to-date version to an SMS, click on the Download button that you can find in the part with new version information.
2. In the window, select those connected SMS to which you want to download the up-to-date version. You have two download options:
   - *Directly from the Internet* – the fastest method. Will download updates directly to the computers where SMSs are installed. This is only possible if each SMS is connected to the Internet.
   - *Via the console* – can be used if a computer with an SMS is not connected to the Internet. The installation package will first be downloaded to SMC and then be automatically sent to the each SMS.

   After finishing your selection, click on the *OK* button to have the new version download automatically to each SMS.

Note: In the top right part, information will show up about the progress of the download. By clicking on the Modify button, you can change downloading on those SMS where the up-to-date version has not been downloaded yet. You can change whether the installation package should be actually downloaded to that particular SMS or you can change the method of downloading (Directly from the

Internet, Via the Console).

As soon as the new version has been downloaded to at least one SMS, a tab will appear at the bottom part of the screen, showing the version number of the package that has been downloaded. After the download has completed, you can run an installation of a new version of the SMS and SEC any time.

Installing updates for each SMS and SEC

After downloading a new version to your SMS, you can continue by installing it. You can run the installation only on those SMS where the given version has been downloaded and on those SEC which are connected to these SMS.

1. After opening the installation, click on the *Update* button next to the relevant version at the bottom part of the view.
2. From the list of SMSs and connected SECs, choose the SMS, user, computers or groups for which you want to run the update. Once finished with your selection, click on the *OK* button.

Notes:

- Choosing a user, computer or group will also select its superior SMS, since an SMS and the SEC connected to it must be of the same version.
- When selecting a user, all SEC on all computers that do not have an up-to-date version will become updated when the users logs in.
- The SMS will be updated automatically without the need to restart the computer.
- The new version of SEC will be only installed after the computer has been restarted.

3. You can watch over the progress of the update directly in the downloaded-version overview. See Installed on SMS and Installed on SEC.

Removing the update package from SMS

You can delete the downloaded installation package after the update has been run. To do that, do the following:

1. In the overview of downloaded versions, click on the version for which you want to remove all installation files.
2. Click on the *Remove Installation Package* button.
3. In the list select those SMSs for which you want to delete the installation package and click on the *OK* button.

Visualization

In the visualization view, you can view a record of successful and unsuccessful updates.

In the bottom part of the view is a table with the individual update records. Clicking on the relevant statistic in the top part will show, in the bottom part, the records that correspond to that statistic. If any error occurred during an update, you can view a detailed description of the error next to the relevant record by clicking on the More Information link. After opening this record, you can copy the text into the clipboard by clicking on the Copy button. You can then send the detailed record to the Safetica Technologies Tech Support, which will help your discover and possibly fix the arisen problem.

4.9 Uninstall

In the following sections, instructions for uninstallation of Safetica components will be given.

Safetica Management Service

1. Open the Windows control panel *Add or remove program* (Uninstall a program in Windows 7)
2. Select Safetica Management Service from the list and select uninstall.
3. Restart the computer.

Safetica Management Console

1. Open the Windows control panel *Add or remove program* (Uninstall a program in Windows 7)
2. Select Safetica Management Console from the list and select uninstall. You do not have to restart the computer.

Safetica Endpoint Client

Locally on the computer with SEC:

Warning: A client installed using GPO should not be uninstalled locally.

1. You have to enable this action first. You can do this in two ways. You can do this locally on the station on which SEC is installed by entering the command STCService.exe -allow uninstall You will be asked to enter a password (the default password is *safetica*). You can also enable this action remotely via SMC *Management and Settings -> Client settings -> Allowed actions* by checking the item Uninstallation and saving the changes. Read more in Protection of Safetica Endpoint Client and Management of SEC through the command prompt.
2. Open the Windows start menu *Add or remove program* (Uninstall a program in Windows 7)
3. Select Safetica Endpoint Client from the list and select uninstall.
4. Restart the computer.

Remotely by means of Group Policy Object (GPO):

1. Access the server where you have remotely installed SEC through GPO. Go to *Management tools -> Management of group policies*.
2. Select the group policy which you have used for distributing SEC, and right-click on Edit.
3. In the pop-up window, choose *Computer setup -> Policies -> Software* settings and click on Software installation.
4. A new item should appear in the list: Safetica. Right-click on this item and select All tasks -> Remove.
5. In the dialog that appears, select Uninstall immediately...
6. Safetica will be gradually uninstalled from all client stations after they are restarted.

4.10 Technical support

If necessary, you can contact our technical support by e-mail at support@safetica.com.

In the event of issues with the software, we need as much information as possible to successfully solve it.

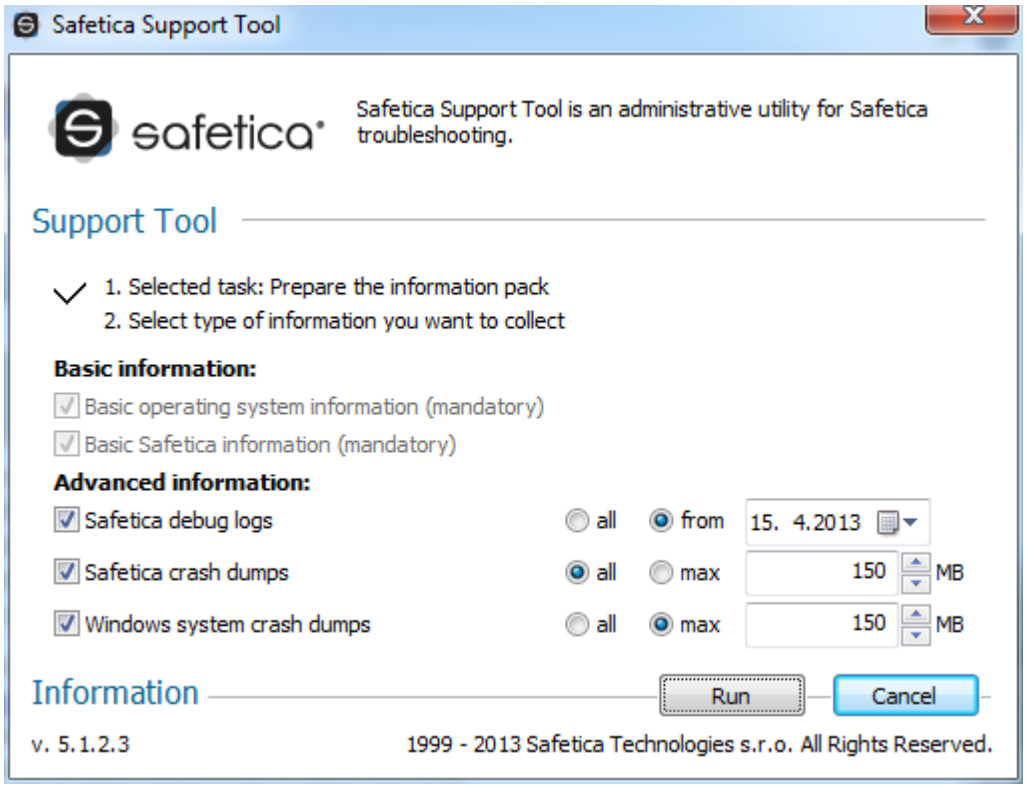
Obtain information using Safetica Support Tool

Safetica Support Tool was created to automatically obtain the most important information about Safetica Endpoint Client. Information obtained by this tool can greatly help us with solving potential issues.

You can find Safetica Support Tool inside the installation folder of Safetica Endpoint Client (the default location is C:\Program Files\Safetica\Tools\STSupportTool.exe).

How to obtain debug information using Safetica Support Tool:

1. Run *STSupportTool.exe* as administrator.
2. Click on the *Prepare the information pack* button.
3. Now you can specify Advanced settings. You can specify the time from which you want to export debug logs and the maximum size of Safetica and Windows crash dumps. Basic settings are mandatory and cannot be changed.
4. The report is now generated. After it is finished, click on the Save button and save the report to a disk. The report will be saved in .dcf format (Safetica encrypted archive).
5. Finally, sent the generated archive to support@safetica.com.



Obtain debug information manually

You can provide us with information manually by sending the following folders and files from the individual components of Safetica:

Safetica Management Console

Windows 7 x86/x64 and Windows Server 2008:

C:\Users\<user>\AppData\Local\Safetica Technologies\Safetica Management Console\Dump\

C:\Users\<user>\AppData\Local\Safetica Technologies\Safetica Management Console\Logs\

Windows XP:

C:\Documents and Settings\<user>\Application Data\Safetica Technologies\Safetica Management Console\Dump\

C:\Documents and Settings\<user>\Application Data\Safetica Technologies\Safetica Management Console\Logs\

Safetica Management Service

Windows 7 x86/x64 and Windows Server 2008:

C:\ProgramData\Safetica Management Service\Dump\

C:\ProgramData\Safetica Management Service\Logs\

C:\ProgramData\Safetica Management Service\debugLog.txt

Windows XP:

C:\Documents and Settings\All Users\Application Data\Safetica Management Service\Dump\

C:\Documents and Settings\All Users\Application Data\Safetica Management Service\Logs\

C:\Documents and Settings\All Users\Application Data\Safetica Management Service\debugLog.txt

Safetica Endpoint Client

Windows 7 x86/x64 and Windows Server 2008:

C:\ProgramData\Safetica Client Service\Dump\

C:\ProgramData\Safetica Client Service\Logs\

C:\ProgramData\Safetica Client Service\debugLog.txt

C:\ProgramData\Safetica Client Service\Debug.db

Windows XP:

C:\Documents and Settings\All Users\Application Data\Safetica Client Service\Dump\

C:\Documents and Settings\All Users\Application Data\Safetica Client Service\Logs\

C:\Documents and Settings\All Users\Application Data\Safetica Client Service\debugLog.txt

C:\Documents and Settings\All Users\Application Data\Safetica Client Service\Debug.db

Basic information we need to solve the issue

- The exact version number of Safetica.
- The hardware and software configuration of the end computer.
- Operating system version.
- A list of antivirus, anti-malware, anti-spyware and firewall software installed on end computers.
- Which functions of Safetica have you enabled?
- Is the issue occurring repeatedly or at random?
- Do you have a module license (Auditor, DLP, Supervisor) assigned?

How to turn on debug logs

To obtain more information for us, you can turn on debug logs and then repeat the problematic action again. The debugging data thus obtained will be written into a Debug.db file on the Safetica Endpoint Client station (the default path is Windows XP and Server 2003: C:\Documents and Settings\All Users\Application Data\Safetica Client Service\Debug.db, Windows 7 and Server 2008:

C:\ProgramData\Safetica Client Service\Debug.db). This data can help us identify and solve the issue more quickly.

You can turn on debug logs in *Management and Settings -> Client settings -> Debug logs*. The level Verbose logs the greatest amount of information into the Debug.db file and the level Critical logs the least amount of information.

Turning on debug logs may negatively affect end station performance.

How to manually obtain debug logs about occurred issue

If a client station shows any problem, we need as much information as possible for successfully resolving it. One of the main sources are debug logs. To obtain debug logs perform the following steps:

1. Turn on the client station with the issue and set the level of debug logs for this station to Verbose (in Safetica Management Console *Management and Settings -> Client settings -> Debug logs*).
2. Check if the debug log settings were successfully transferred onto the client station (*Management and Settings -> Clients Information*).
3. Repeat the action that leads to the issue.
4. Finally, send us a copy of the Debug.db file from the client station (Windows XP and Server 2003: C:\Documents and Settings\All Users\Application Data\Safetica Client Service\Debug.db, Windows 7 and Server 2008: C:\ProgramData\Safetica Client Service\Debug.db).

5 MODULES OF SAFETICA

The Safetica product comprises three modules.

- Auditor
- DLP
- Supervisor

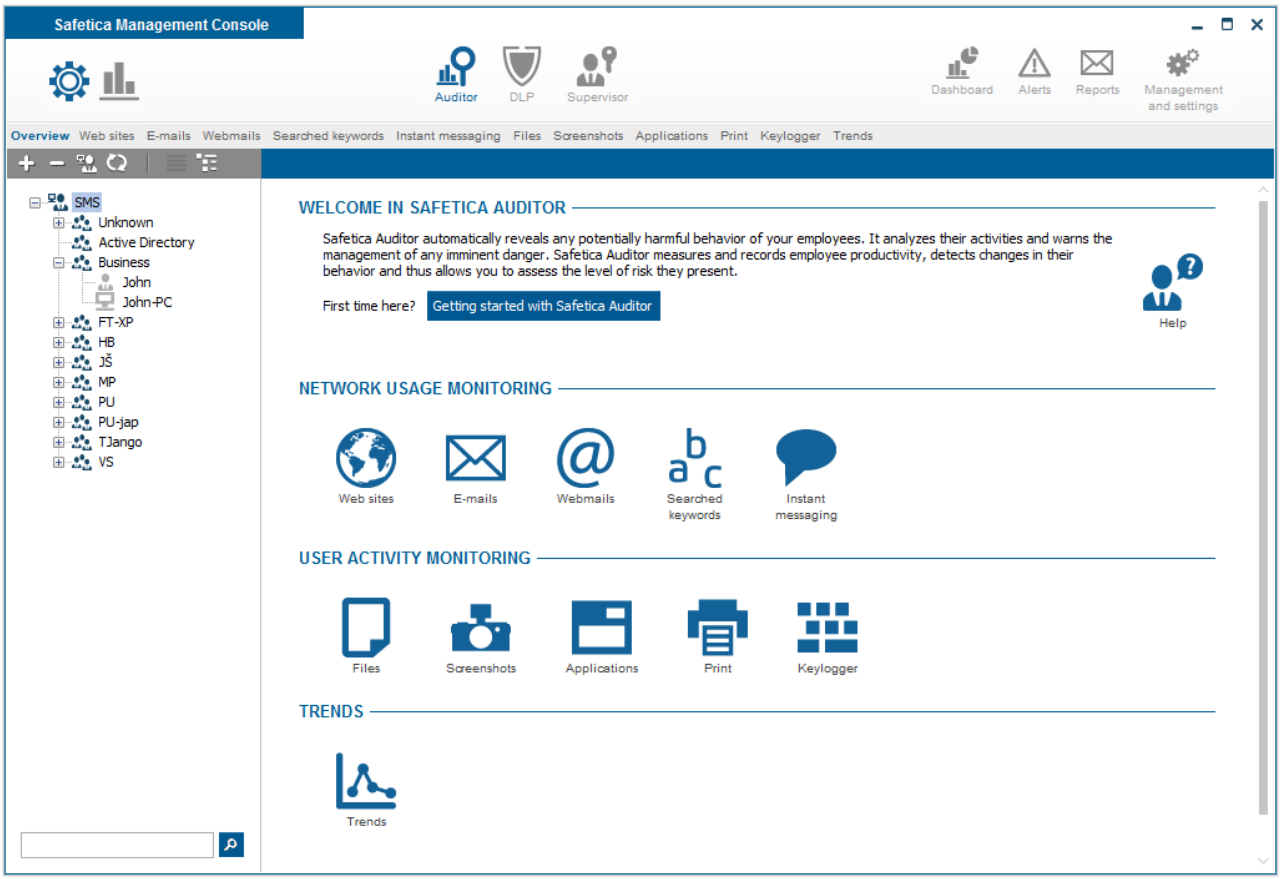
The following articles will explain their individual functions in detail.

5.1 Auditor

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

Main Benefits

- Obtain a detailed overview of your employees' work.
- Stay informed of the bad intentions of your employees before they become an issue and prevent them from damaging your company.
- Detect employees who are not working effectively or are only pretending to work.
- Obtain an overview on the use of the company printers by individual employees.
- Protect your company's interests with regard to your employees' privacy.
- Avoid changes to company processes and the costs they might incur.
- Reach compliance with industrial standards, regulations and laws easily.
- Increase your employees' productivity by blocking unsuitable websites and applications.
- Protect your company computers against harmful software activated by employees.
- Reduce printing costs through restrictions on problem employees' printing.



5.1.1 Network usage monitoring

5.1.1.1 Web sites

Expose which websites your employees visit during working hours. Safetica delivers clearly organized statistics of the most frequently visited websites and the amount of time spent browsing them to company managers. The websites are sorted according to category, number of visits and productivity rate. It does not matter which browser employees use – Auditor can process data from them all.

Web activity is in the section Auditor -> *Web sites*

Setting

You can enable or disable this function using the slider in the header of this view

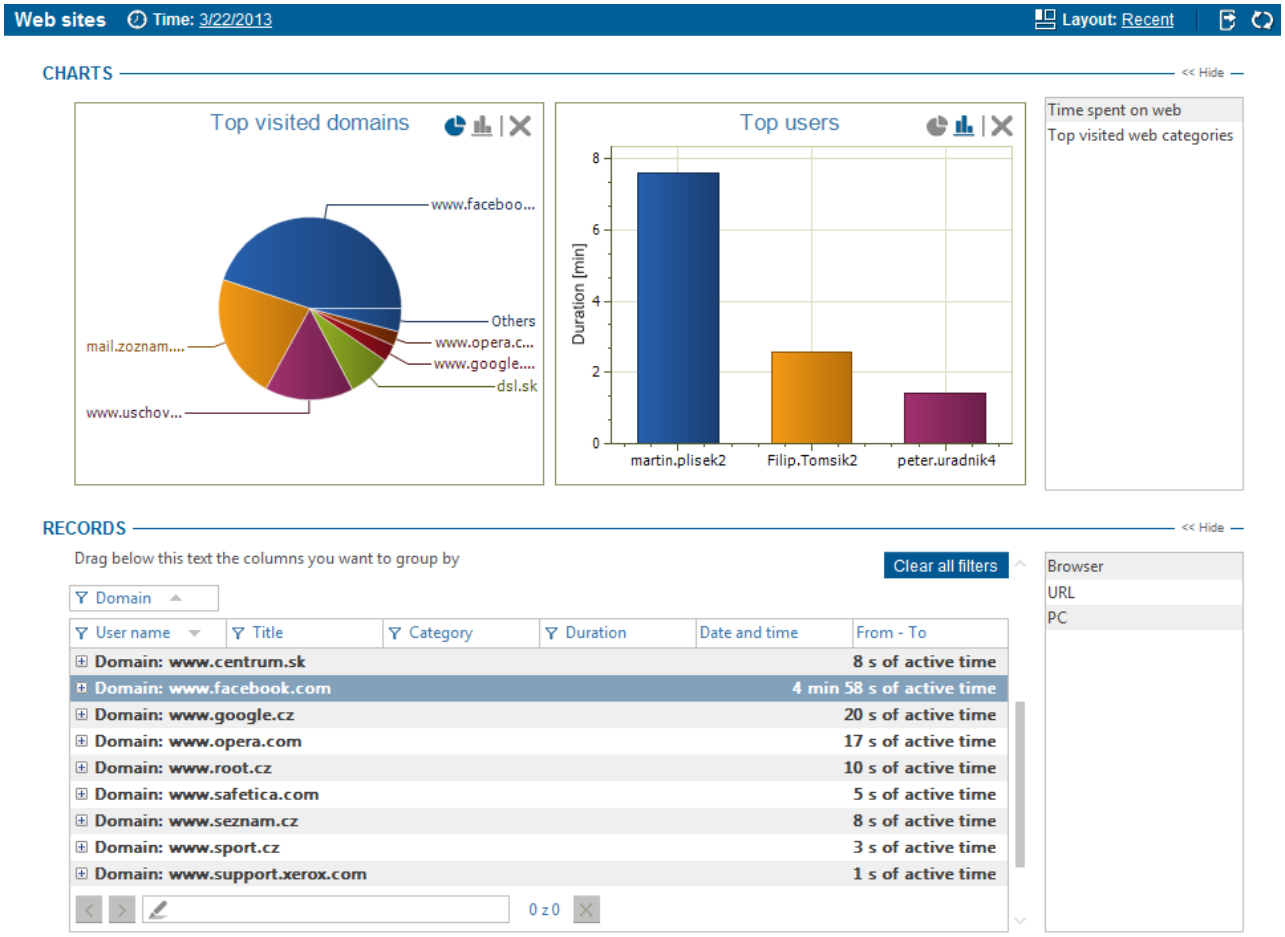
- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Web activity is only set for users, computers, groups or branches you have highlighted in the user tree. To apply the settings, you have to save the changes using the button or you can cancel the changes you have made using the button in the upper right corner.

Visualization

Data that you can see in the visualization mode is only shown for the users, computers, or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each

chart.



Available charts:

- *Top visited domains* – a chart containing the most frequently visited domains (up to 7 domains are shown).
- *Most active users* – a chart containing users who have spent the most time on the web
- *Top visited web categories* – a chart containing the most frequently visited web categories (up to 7 categories are shown).
- *Time spent on web* – a chart containing total time spent on the web.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it on the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.
- *User name* – the name of the user under whom the record was made.
- *Browser* – name of the browser.
- *Duration* – active time spent browsing the web site.

- *From - To* – time of activity on the web.
- *Domain* – domain name (part of URL).
- *URL* – website URL.
- *Title* – website title.
- *Category* – name of the web category (how it was categorized).

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.1.2 E-mails

Do your employees communicate actively with competitors or do they forward dozens of chain e-mails with funny pictures? Expose what kind of e-mails they send during working hours. If suspicions ariseus,, responsible managers can obtain detailed information about employees'' communication, including enclosures attachments that might contain sensitive information.

You will can find e-mail monitoring in the section *Auditor -> E-mails.*

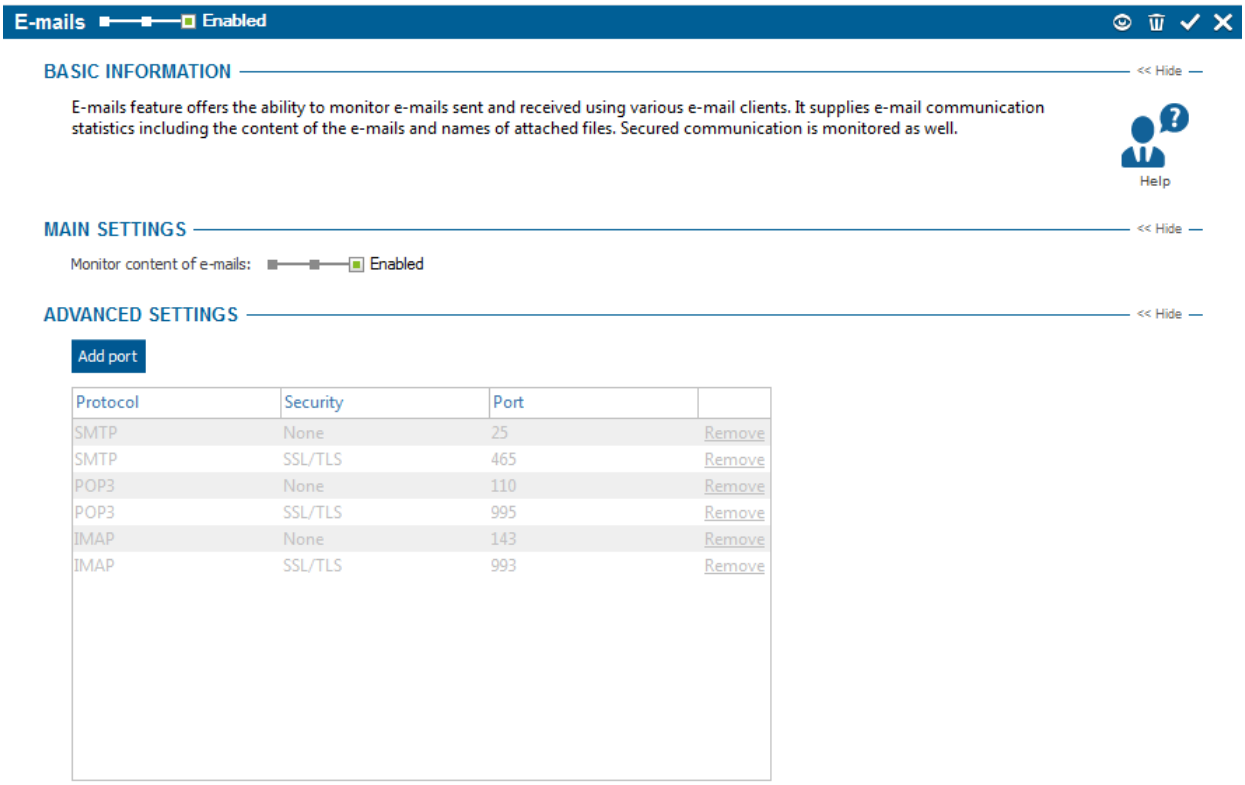
Setting

You can enable or disable this function using the slider in the header of this view.

- Disabled – function is not activated.
- Inherit – function mode is not set. Settings are inherited from the parent group.
- Enabled – function is activated.

You can also specify the following using the slider:

- *Monitor content of e-mails* – the contents of outgoing and incoming e-mails will be monitored when set to Enabled.



Advanced settings

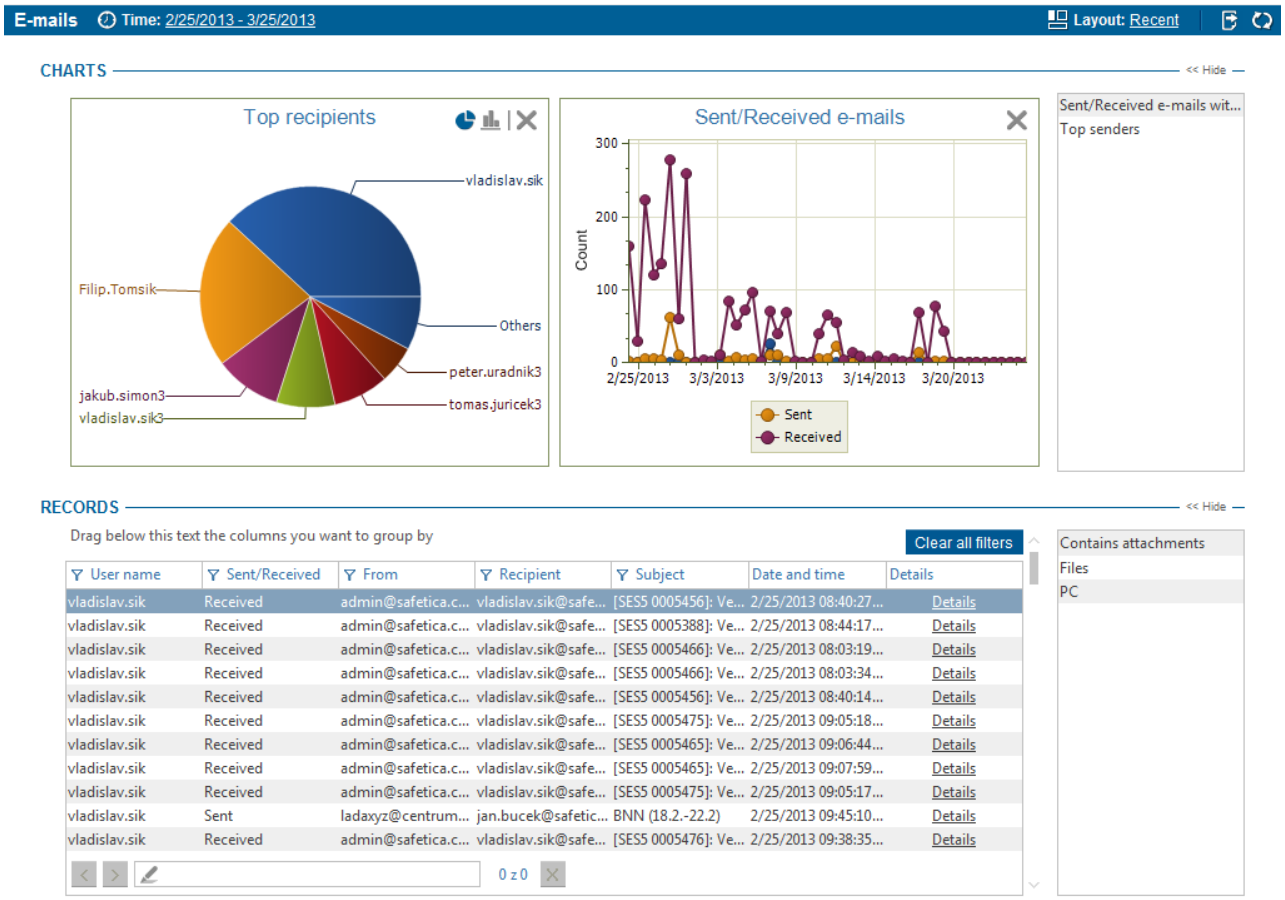
In the advanced settings you have the option to specify the type of security (none, STARTTLS, SSL/TLS) and ports for supported protocols (SMTP, POP3, IMAP). E-mail communication will be monitored only on protocols and ports listed here. By default, this list includes the most frequently used combinations of protocols, ports and security types as shown above.

You can add another protocol by clicking on the Add button. Then, specify the type of the protocol, security and port number.

Email monitoring is enabled only for users, groups, computers or branches you have selected in the user tree. To apply the settings, you have to save the changes using the button or you can cancel the changes you have made using in the upper right corner.

Visualization

The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them on the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each chart.



Available charts:

- *Sent/Received e-mails* – a chart containing the number of sent and received e-mails.
- *Sent/Received e-mails with attachments* – a chart containing the number of sent and received e-mails with attachments.
- *Top Recipients* – a chart containing users with the highest number of received e-mails.
- *Top Senders* – a chart containing users with the highest number of sent e-mails.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at on the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the e-mail was sent.
- *From* – e-mail sender.
- *Recipient* – e-mail recipients.
- *Subject* – subject of e-mail.
- *Sent/Received* – if the e-mail was sent or received.

- *Attachment* – if the e-mail has an attachment or not.
- *Files* – file names of attachments.
- *Details* – you can open dialog with content of the mail by clicking on *Details* link.

You can open a dialog with the contents of the e-mail by double-clicking on the record in the table. There you can switch between the message display mode (HTML, Plain text, Other) by ticking the appropriate option.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the *OK* button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.1.3 Webmails

Some employees use the web interface for undetectable e-mail communication. However, Auditor also uncovers this form of communication. When visiting company or personal webmail, it records the content of sent e-mails. The responsible manager is then informed of the communication that the employee is trying to hide. Auditor can also deal with a secure connection using the HTTPS protocol.

Webmail setting is accessible from *Auditor -> Webmail.*

Setting

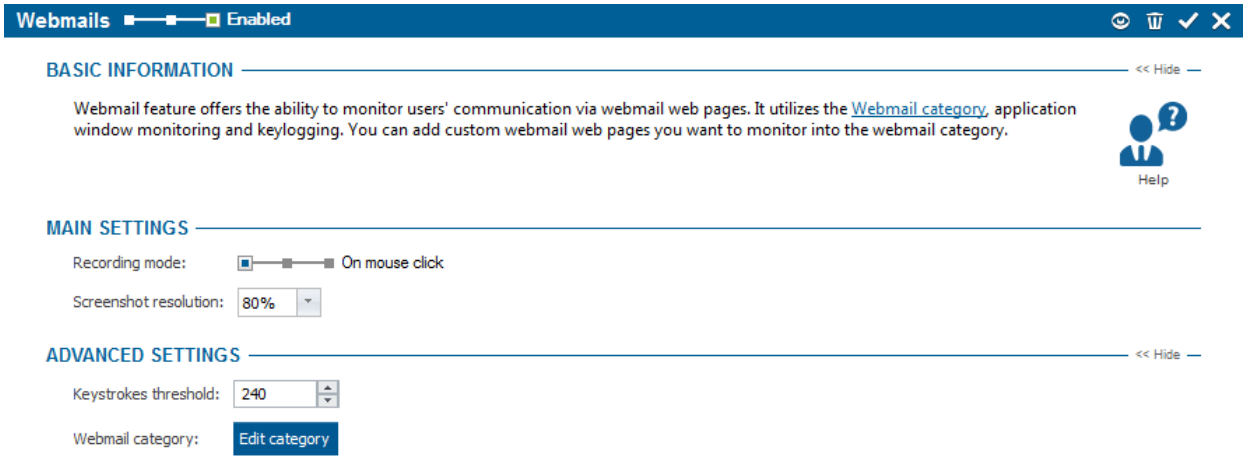
You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from parent group.
- *Enabled* – function is activated.

You can further specify this option using *Create record* slider:

- *Inherit* – function mode is not set. Settings are inherited from parent group, if one exists.
- *On mouse click* – a record (screenshot, text) will be taken at the moment that the user clicks the mouse button.
- *On mouse click or when the keystrokes threshold is reached* – a record (screenshot, text) will be taken when the user clicks the mouse button or when the keystrokes threshold is reached. You can set the threshold in the Advanced settings.

The last option is Screenshot resolution – each recording creates a screenshot of the given webmail window. With this option you can define the screenshot resolution of this screenshot with respect to the resolution set on the client station. You can set the quality in the range of 30–100%.



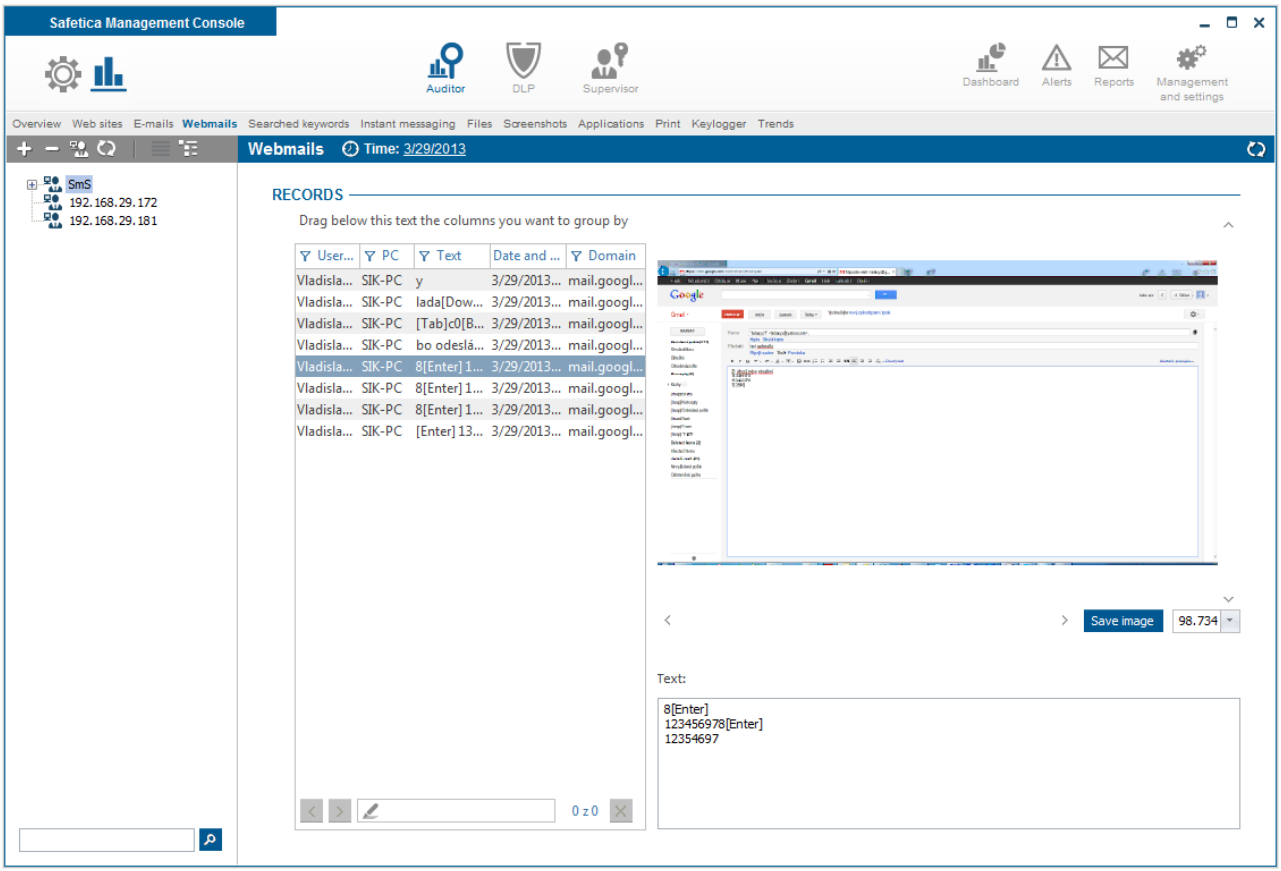
Advanced settings

By using the Edit category button in the Advanced settings you can open the web category database containing webmail sites. You can also add your own webmail sites to this category. Webmail monitoring will be done for those webmail sites that are listed in this category or for those which are identified by our heuristic algorithm.

You can also set the keystrokes threshold here.

Visualization

In the following figure you can see a view of the visualization mode of the Webmails function.



In the left section you will find a text list of records of the webmail communication. Each item contains information on the time of recording and the application in which webmail was opened.

In the bottom right section you will find a text box displaying the text of the message captured for the given record in webmail.

The upper right section of the visualization mode includes a preview of an application window in which you worked with webmail. If you click on this preview, a window with a screenshot of the application window will be displayed. You can change the size of this screenshot by means of a drop-down menu below. There is a *Save image* button, which you can use for exporting the screenshot to the PNG format.

5.1.1.4 Searched keywords

One of the most frequent activities of employees is web browsing. However, it is not always a required activity. They might be looking for a new job, searching for sensitive files or they might be interested in subjects that they do not need for work. Safetica offers you a detailed overview of what employees are browsing within the system and on the Internet.

The feature supports recording of searches on a local computer (option Start -> Search in Windows XP and searching through the explorer in Windows 7 systems – Windows Vista is not supported) as well as searches in web browsers. Recording will include all searched strings e.g. from Google, Yahoo, AOL, MSN, Bing, Seznam.cz and many others. Obviously, support is provided for logging when searches are done using search plugins in web browsers.

The searched keywords feature is accessible from the menu *Auditor* -> *Searched keywords*.

Setting

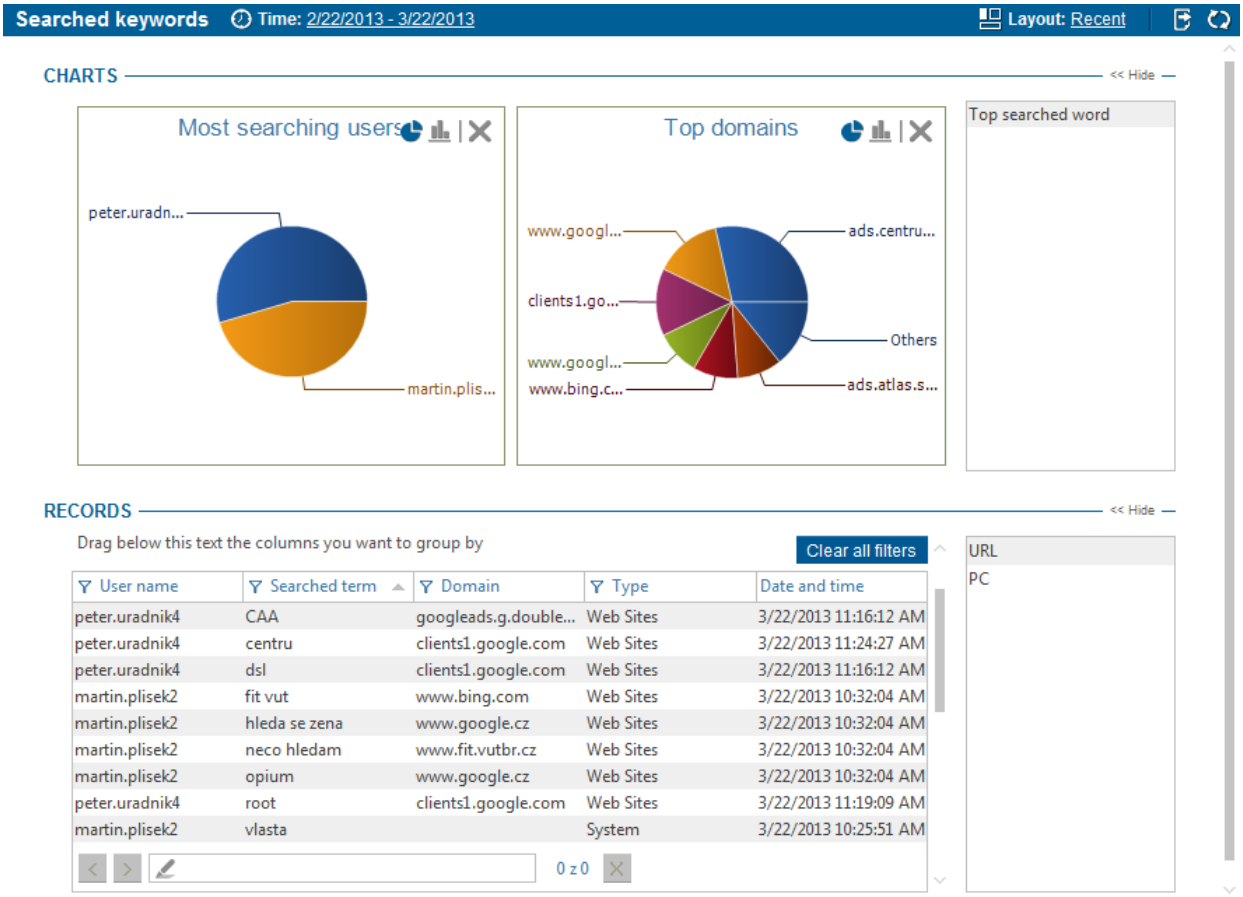
You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

The searched keywords function is only set for users, computers, groups or branches you have highlighted in the user tree. To apply the settings, you have to save the changes using the  button or you can cancel the changes you have made using the  button in the upper right corner.

Visualization

Data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them on the chart viewing area will make them visible. To remove a chart from the list, click on the  button in the top right corner of each chart.



Available charts:

- *Most searching users* – a chart containing the most searching users. (up to 7 users are shown).
- *Top searched words* – a chart containing the most searched words/ (terms). (Up to 7 words are shown).
- *Top domains* – a chart containing the most used search domains. (up to 7 domains are shown.)

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at on the table will make the column visible in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of column list of columns on the right.

Available columns:

- *Date and time* – date and time when record was logged.
- *PC* – name of the PC where the record was taken.
- *User name* – the name of the user under whom the search e-mail was sent was done.
- *Searched terms* – searched terms or words.
- *Type* – where the text string was searched::
  - o *System* – using the search function in windows Window search (Windows Vista is excluded).

- Web Sites – using search engines on the web.

- *URL* – URL address of the search engine where the search was done.
- *Domain* – domain used to search.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Type in text into the ensuing dialog or choose an item from the list to filter the column by that item. Clicking on the + button will add the item into the filter listthe item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.1.5 Instant Messaging

The instant Messaging feature offers the ability to monitor users' communication via instant messaging (IM) applications. Monitoring of these applications is based on the Instant messaging Application category. IM applications listed in the Instant messaging category are monitored.

Settings are available from the main menu *Auditor* -> *Instant Messaging*.

Setting

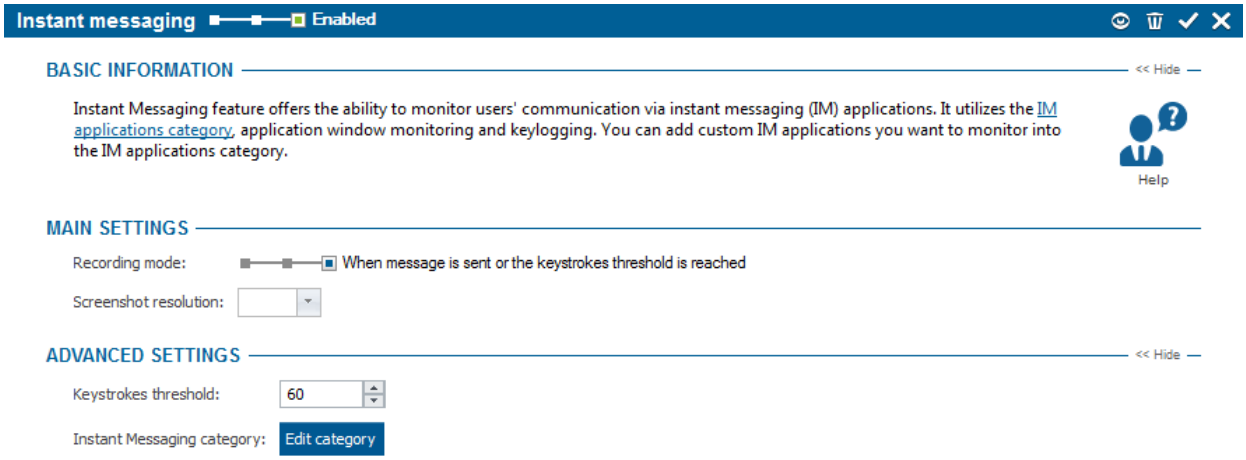
You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

You can further specify the following settings:

- *Inherit* – function mode is not set. Settings are inherited from parent group, if one exists.
- *On mouse click* – a record (screenshot, text) will be taken at the moment that the user clicks the mouse button.
- *On mouse click or when the keystrokes threshold is reached* – a record (screenshot, text) will be taken when the user clicks the mouse button or when the keystrokes threshold is reached. You can set the threshold in the Advanced settings.

The last option is Screenshot resolution – each recording creates a screenshot of the given application window. With this option you can define the screenshot resolution of this screenshot with respect to the resolution set on the client station. You can set the quality in the range of 30–100%.



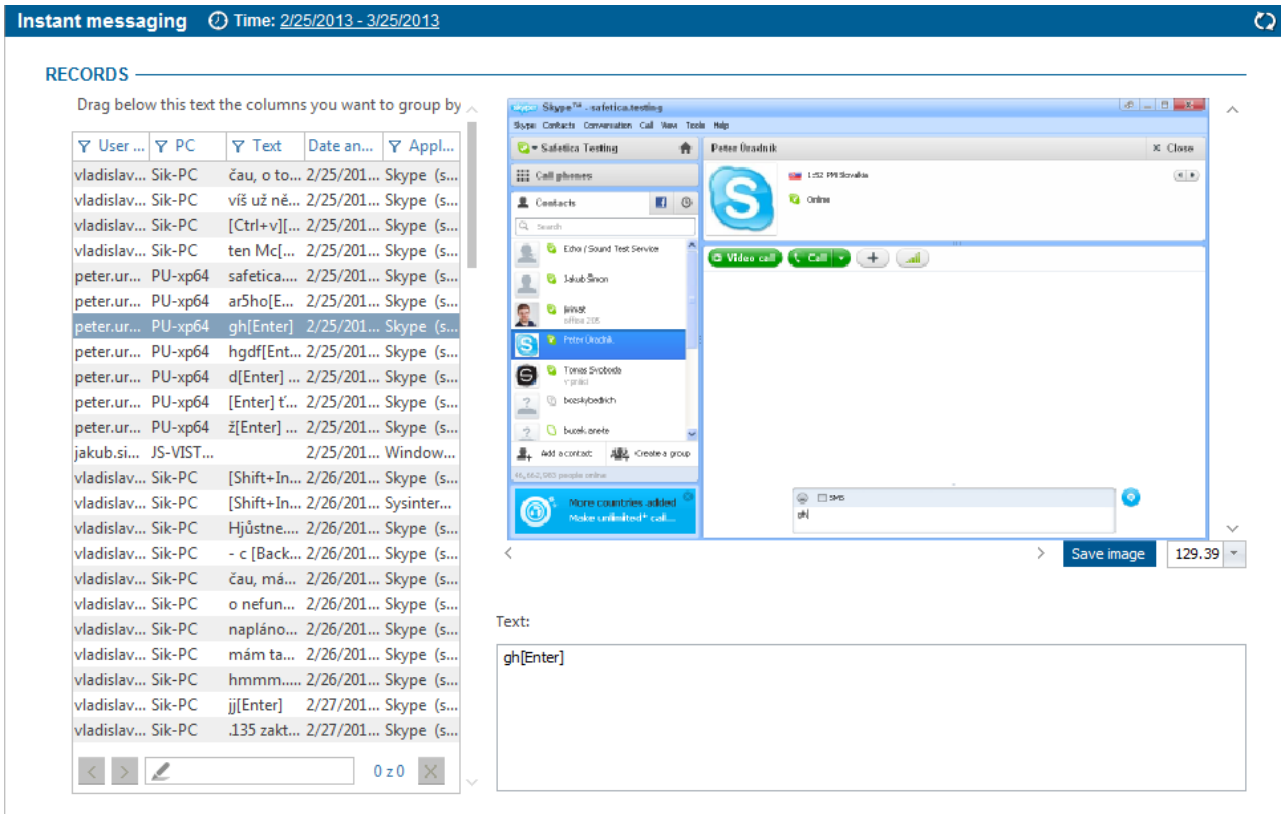
Advanced settings

By using the *Edit category* button in the advanced settings you can open the application category database containing instant messaging applications. You can add your own instant messaging applications to this category. IM monitoring will be done only for those instant messaging applications that are listed in this category.

You can also set the keystrokes threshold here.

Visualization

The following picture shows the visualization mode of the IM Monitoring feature.



In the upper right section you can set the period you want to check.

In the upper left section you will find a text list of records of IM communication. Every item includes information on the IM client, the time of the record and the vendor of the IM client. You can apply various filters on these items in the list.

Below the list you will find a text box which displays the text of the message captured for the given record.

The right section of the visualization mode includes a preview of the application window where the message was created. If you click on this preview, a window with a screenshot of the application window in a preset resolution will be displayed. You can change the size of this screenshot by means of a drop-down menu below. In the bottom part of this window there are two buttons. The first is Save, which you can use for exporting the screenshot to the PNG format.

There are Previous and Next buttons for browsing through records.

5.1.2 User activity monitoring

5.1.2.1 Files

An employee accessing any sensitive data is a potential danger for the company. Even if they are authorized to access the data, they might misuse it. You will have a detailed overview for every employee of what files they used the most, what they did with them and what applications they used to

access them.

File monitoring is available in *Auditor* -> *Files*.

The file monitoring feature monitors the basic actions that can be performed with files. These actions include opening, copying, moving and deleting files.

Main settings

You can enable or disable this function using the slider in the header of this view.

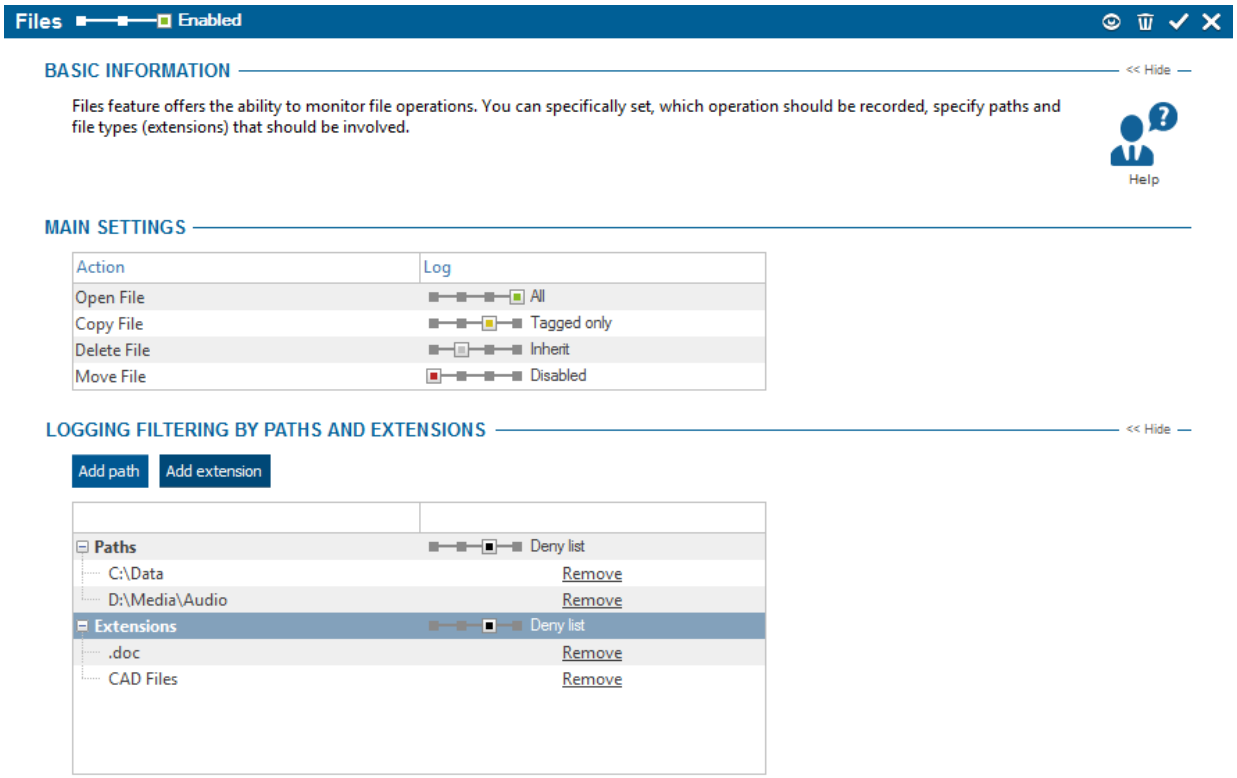
- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

You can monitor and log following file operations: *Open File, Copy File, Delete File, Move File, Create file, Web Download, FTP transfer (file download and upload).*

Note: Surveillance of files downloaded from the web is supported only in the browsers Mozilla Firefox, Internet Explorer and Google Chrome. In other browsers the files downloaded will be classified as newly created files.

You can set following log options for each of file operations:

- *Do not log* – file operation is not logged.
- *Log tagged only* – only file operations are logged that involve files tagged by some data category (*Data categories*). Will work only with Safetica DLP license.
- *Inherit* – nothing is set. Settings are inherited from the File auditor setting of the parent group, if one exists. Otherwise, operations are not logged.
- *Log all* – file operation with every file is logged.



Logging filtering by paths and extensions

In the section Logging filtering by paths and extensions you can determine which file operations will be logged, using the *Allow list* or *Deny list* of extensions or paths.

- *Disabled* – filtering is disabled
- *Inherit* – nothing is set. Settings are inherited from the Files setting of the parent group, if one exists. Otherwise, it is the same as the Disabled option
- *Deny list* – only file operations with files in the paths that are not in the list or with file extensions that are not in the list will be logged
- *Allow list* – only file operations with files in the paths that are in the list or with file extensions that are in the list will be logged

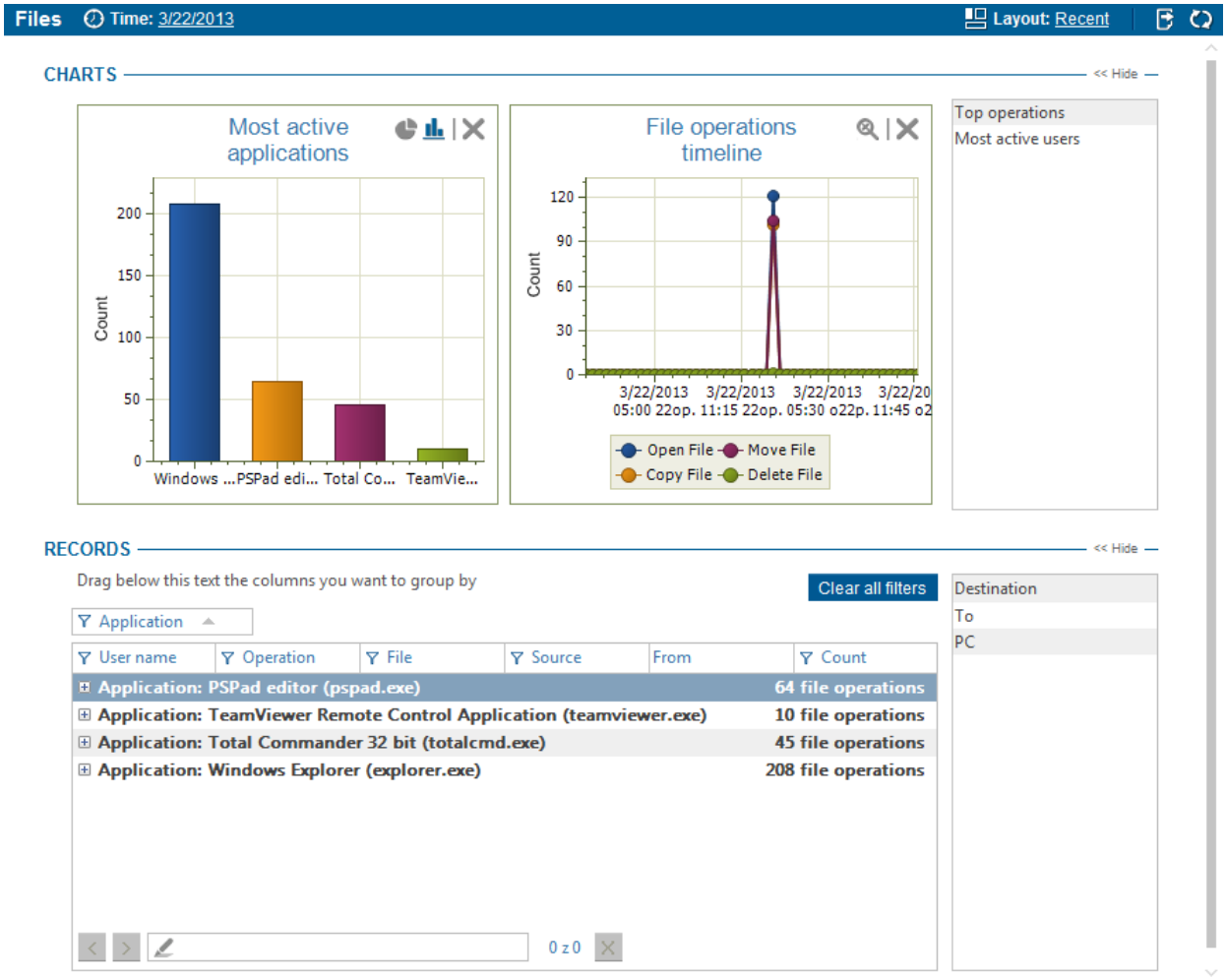
You can add paths to the list by clicking on the Add path button and then entering the path. You can choose this path using the dialog that appears when you click on the button with three dots.

You can add extensions to the list by clicking on the Add extension button and then entering the extension or choosing the extension category. To add extension category click on button with three dots.

The file auditor is set only for users, computers, groups or SMS you have highlighted in the user tree. In order to apply settings, you have to save the changes using the  button or you can cancel the changes you have made using the  button in the upper right corner.

Visualization

The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them on the chart viewing area will show them. To remove a chart from the list, click on the  button in the top right corner of each chart.



Available charts:

- *Most active users* – a chart containing the users who work with files the most (up to 7 users are shown).
- *Most active applications* – a chart with the applications that are most frequently used in working with files.
- *File operations* – a chart with the most frequent file operations.
- *Top operations* – a chart containing a count and ratio of executed operations.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it on the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- From – start date when the first record was created. This depends on Management and Settings -> *Client settings* -> *Log aggregation level* settings.
- *To* – end date when the last record was created. It depends on *Management and Settings -> Client settings -> Log aggregation level* settings.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the file operation was done.

- *Application* – the name of the application that performed the file operation.
- *Source* – the name and path of the file that the file operation concerned.
- *Destination* – this will show the target path for copying and moving operations.
- *Source type* – whether the source path to the file is local, external or network-based
- *Target type* – whether the target path is local, external or network-based
- *Operation* – the type of the file operation that was performed: *Open File, Copy File, Delete File, Move File, Create file, Web Download, FTP transfer.*
- *Source device* – device name and SID.
- *Target device* – device name and SID.
- *Count* – number of identical records in one record. This grouping can be changed in *Management and Settings -> Client settings -> Log aggregation level*
- *File* – name of the file.
- *File size*

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.2.2 Screenshots

Avoid uncertainty about whether employees are really working. Show them a record of their actions on their screen and expose what they really do during their working hours. If you suspect that an employee is doing something undesirable, the results of Intelligent Screen Record serve as precise proof of what really happened on the screen.

View snapshots of users' desktops in the sub-module *Auditor -> Screenshots*

Setting

You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

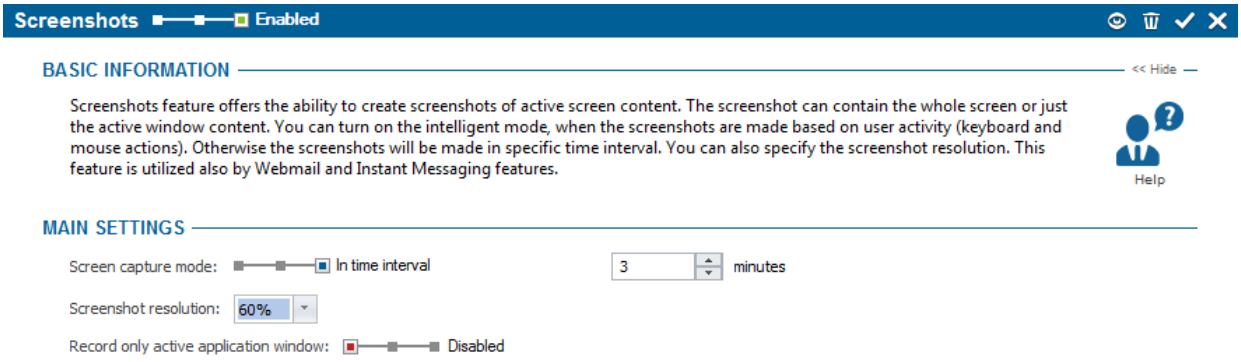
Additionally, you can use the slider to select the screenshot mode:

- *Intelligent Recording* – capture screens on user activity (keyboard, mouse, change application window focus). If the user is not active in this mode, no screens are captured. This way, space needed for storing logs on the disk is saved. If the user activity is high (switching between windows frequently, clicking frequently), a large number of records will be created. Therefore, it is recommended to use this mode mainly in cases when you suspect that an employee is being unproductive or behaving illegally.
- *Inherit* – no additional mode is set. Settings are inherited from the parent group.
- *In time interval* – you must specify the interval (in minutes) in which the screens will be cap-

tured.

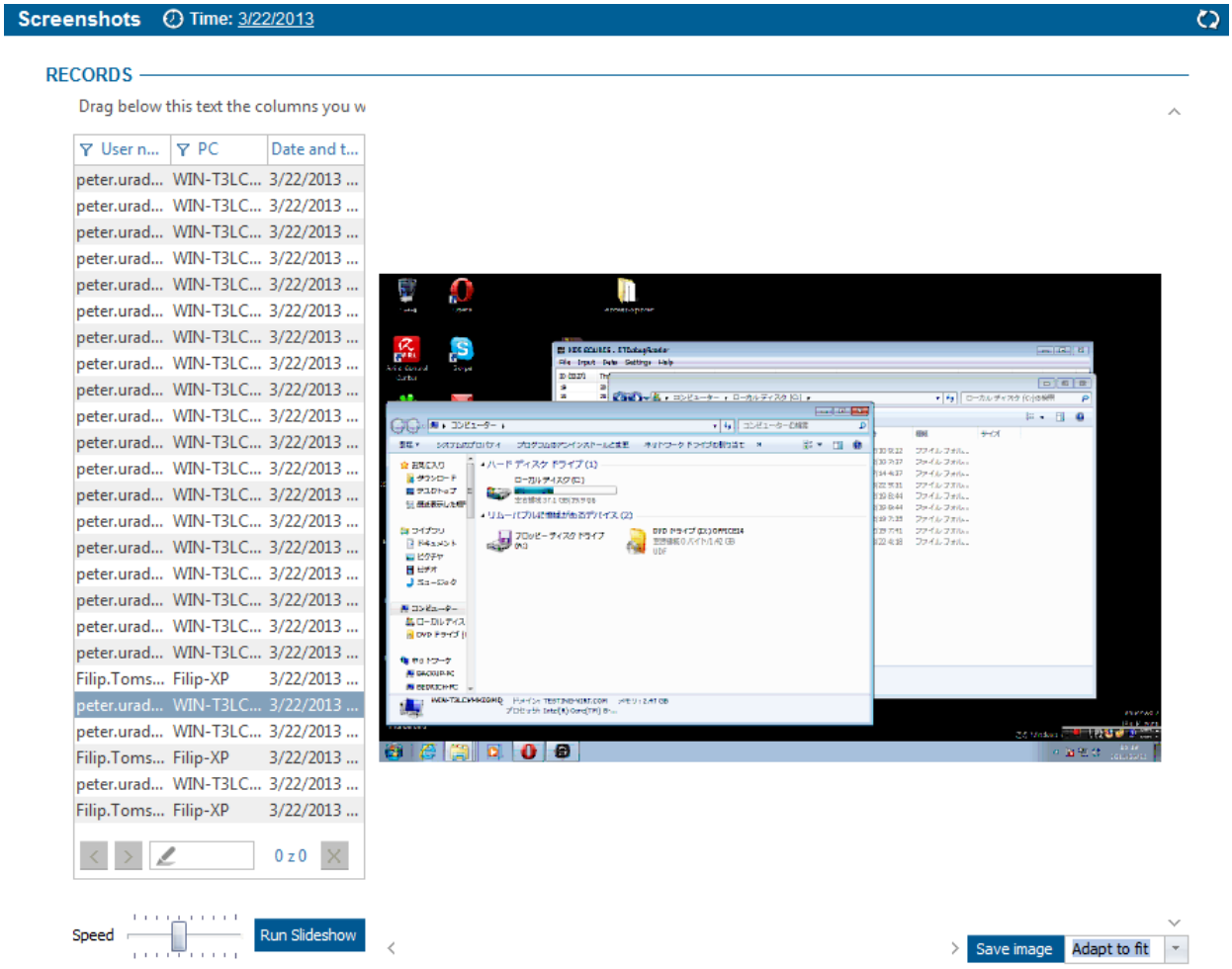
Screenshot resolution can be set in the range of 30-100% of the original size.

The last setting option is the Record only active application window. This setting activates capturing only the window currently displayed for the user in the foreground. This also saves disk space.



Screenshot viewing

The following figure shows a view of the visualization mode of the screen capture function.



A text list of screenshots with time and date of capturing is shown in this mode. When you click a record, the respective screenshot is displayed.

If there is a screenshot displayed and you want to export it from the console, you can click the Save button to save it on the hard disk. Screenshots are saved in the PNG format.

Screenshots can also be viewed in the so-called movie mode. The main control in this mode is the scrollbar that can be used for setting the rate of displaying the screenshots.

Next to the scrollbar, the Run slideshow button is displayed. When you click it, the screenshots start to display. When the last record is reached, the viewing starts from the first one again. You can also modify the speed of slideshow using the slider at the bottom of the view.

The last setting option in this mode allows changing the size of the given screenshot. It can be set using the drop-down menu in the bottom right area. Some common values are predefined here. It is also possible to edit the field and enter a custom size in percent.

5.1.2.3 Applications

The application monitor function records what applications are launched by users and how long they keep them in the foreground or background. Applications monitoring also divides the applications used into categories so you get the fastest possible overview of what type of applications your employees use the most.

You can find Application control in the section *Auditor* -> *Applications*

Setting

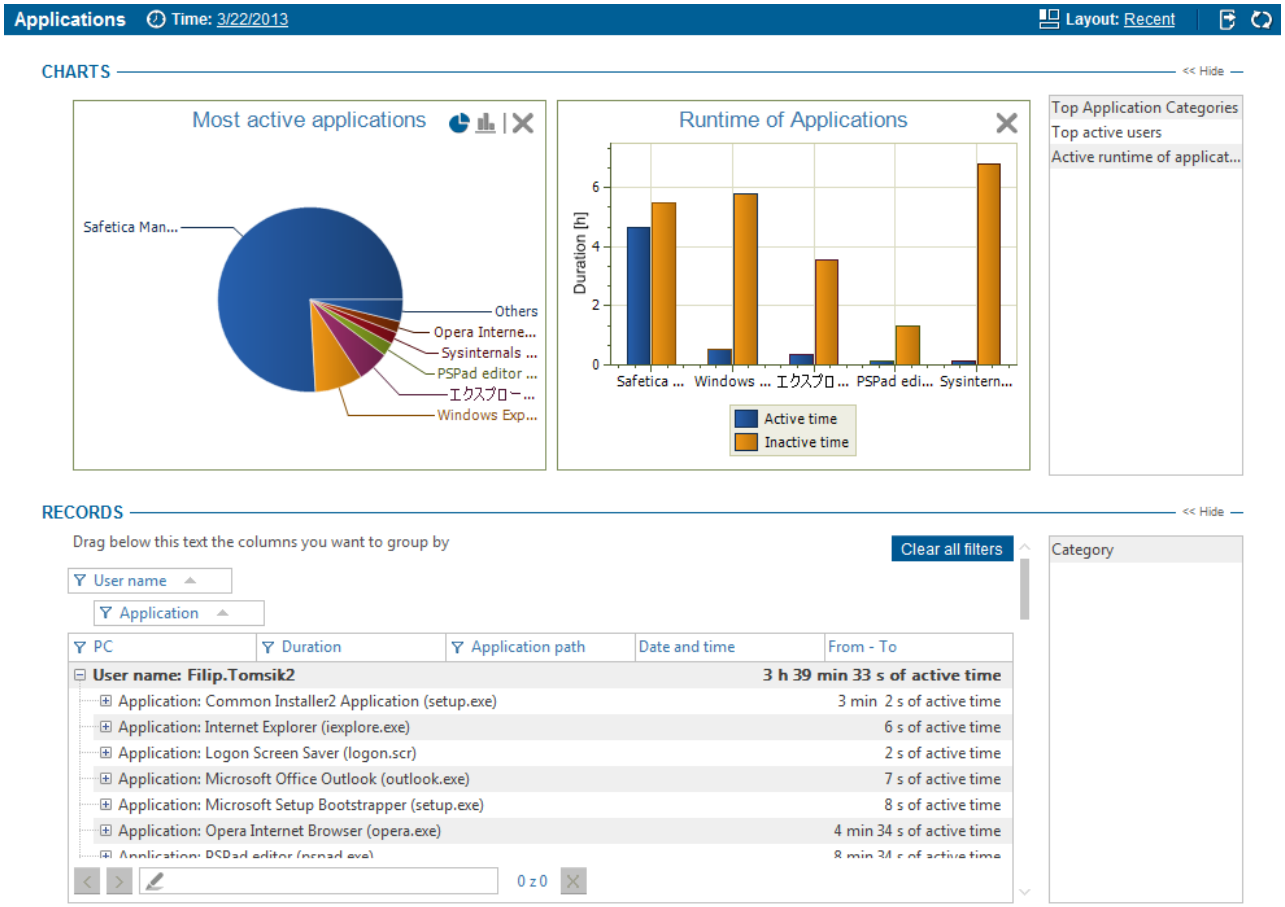
You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Application monitoring is only set for users, computers, groups or branches you have highlighted in the user tree. To apply the settings, you have to save the changes using the  button or you can cancel the changes you have made using the  button in the upper right corner.

Visualization

The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them on the chart viewing area will show them. To remove a chart from the list, click on the  button in the top right corner of each chart.



Available charts:

- *Runtime of applications* – a chart containing the most used applications and their active and inactive times.
  - o *Active time* – the time when the application is in the foreground and the user actively uses the application application (mouse, keyboard).
  - o *Inactive time* – the time when application is in the background (not in the foreground) and the user doesn't isn't actively using use the application application (mouse, keyboard).
- *Active runtime of applications* – a chart containing the total active time of all applications in time.
- *Top application categories* – a chart containing the top used categories of applications. (uUp to 7 categories are shown).
- *Top active users* – a chart containing the top application users. (uUp to 7 users are shown).
- *Most active applications* – a chart containing the longest running applications in active time (u. Up to 7 applications are shown).

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at the table dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of column list of columns on the right.

Available columns:

- *Date and Time* – date and time when record was logged.

- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was donemade.
- *Application* – name of the application.
- *Duration* – active time of running.
- *From - To* – time range when application was running.
- *Application path* – path to application executable.
- *Category* – name of the application category.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.2.4 Print

Obtain a detailed overview on the use of company printers. Find out how many documents were printed by employees and who prints most of them. Obtain evidence against employees who misuse company printers for personal purposes or who try to print sensitive documents protected by DLP.

Setting

You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Print monitoring is set only for users, groups, computers or branches that you have highlighted in the user tree. To apply the settings you have to save the changes using the button or you can cancel the changes you have made using the in the upper right corner.

Visualization

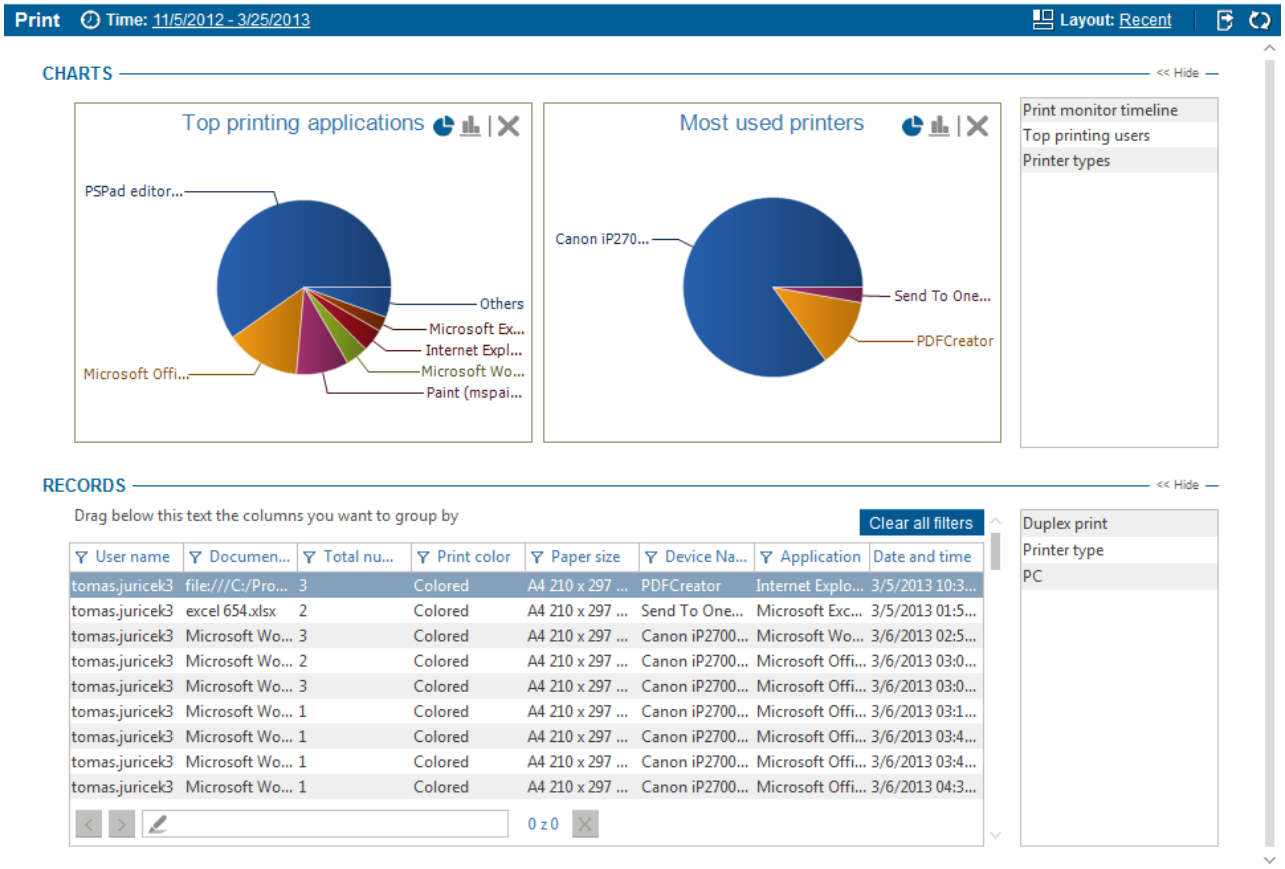
The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each chart.

Available charts:

- *Top printing users* – this chart contains the users with most printswho have printed the most . Up to 7 users.(up to 7 users are shown)
- *Top printing devices* – this chart contains the most- used printing devices . Up to 7 devices. (up to 7 devices are shown)

- *Top printing applications* – this chart contains applications most often used to print . Up to 7 applications.(up to 7 applications are shown)
- *Printer type* – this chart contains the number of prints divided by the type of printer. There are three types of printers: Physical printer, Virtual printer (like PDF Creator, XPS Writer, etc.) and Network printer.
- *Print monitor timeline* – this chart contains the number of prints in over time.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at the table dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of column list of columns on the right.



Available columns:

- *Date and Time* – date and time when record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was made.
- *Application* – name of the application from which printing was done.
- *Device name* – name of the printer.
- *Printer type* – there can be three types of printers: Local printer, Virtual printer (like PDF Creator, XPS Writer, etc.) and Network printer.
- *Document name*
- *Paper size*

- *Color*
- *Duplex print* – printing on both sides of the paper at once.
- *Total number of pages*

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.1.2.5 Keylogger

Keylogger is a foolproof tool that offers you an overview of what a user types on the keyboard. The tool works in the background and its presence will not be noticed by the employee in any way. Keylogger is used by other tools of Auditor.

Keylogger can be found in the section Auditor -> *Keylogger*

Setting

You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Keyboard logging is set only for users, groups or computers you have highlighted in the user tree.

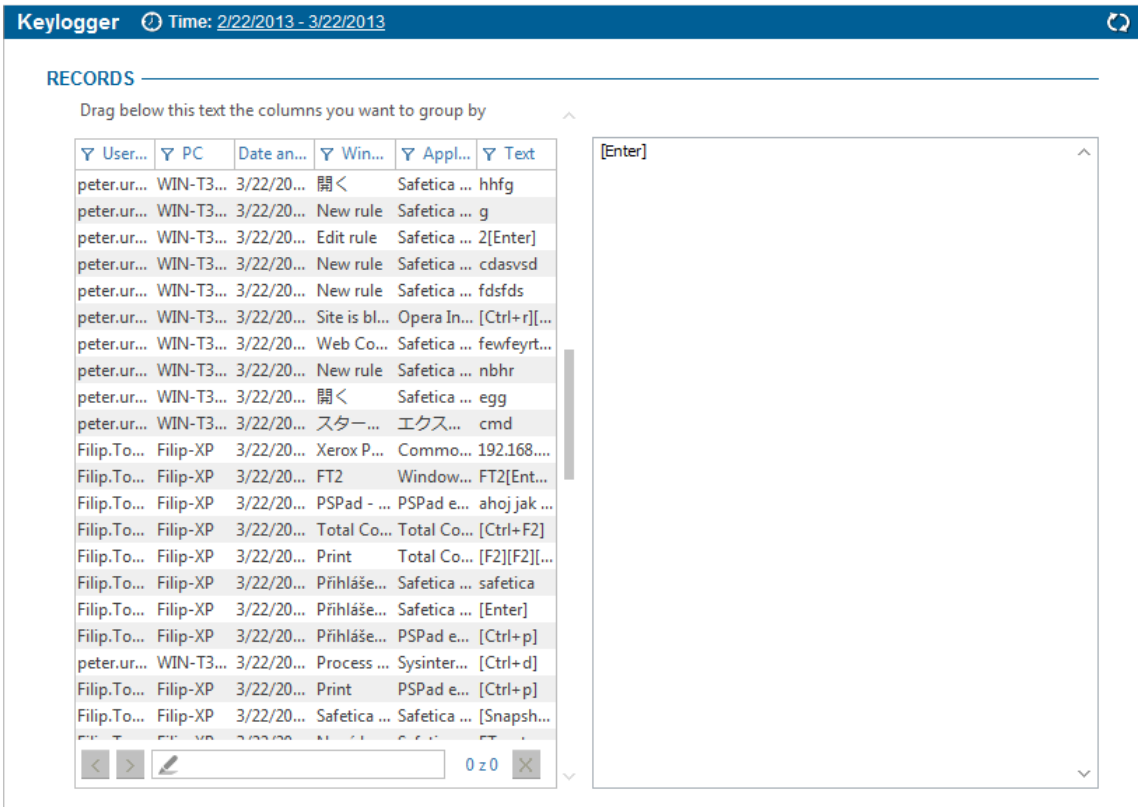
To apply the settings, you have to save the changes using the button or you can cancel the changes you have made using the button in the upper right corner.

Visualization

Visualization mode allows logging the captured keystrokes using a clear list. Each list entry contains information about the user, time of capturing, application where the activity was performed and the location of that application. When you select an entry in the list, information about the keys that were pressed will be displayed on the right-hand side of the working area.

The given list can be filtered according to various specified criteria. You can select the period of data you are interested in in the upper right corner.

The data that you see in the visualization is only displayed for users or groups that you have selected in the user tree.



5.1.2.6 Network traffic

Network traffic function offers the ability to monitor sent and receiveddata on endpoints. It offers statistics of network usage and network utilization. It does not distinguish between individual applications or protocols.

You can find Network traffic control in the section *Auditor -> Network traffic*

Setting

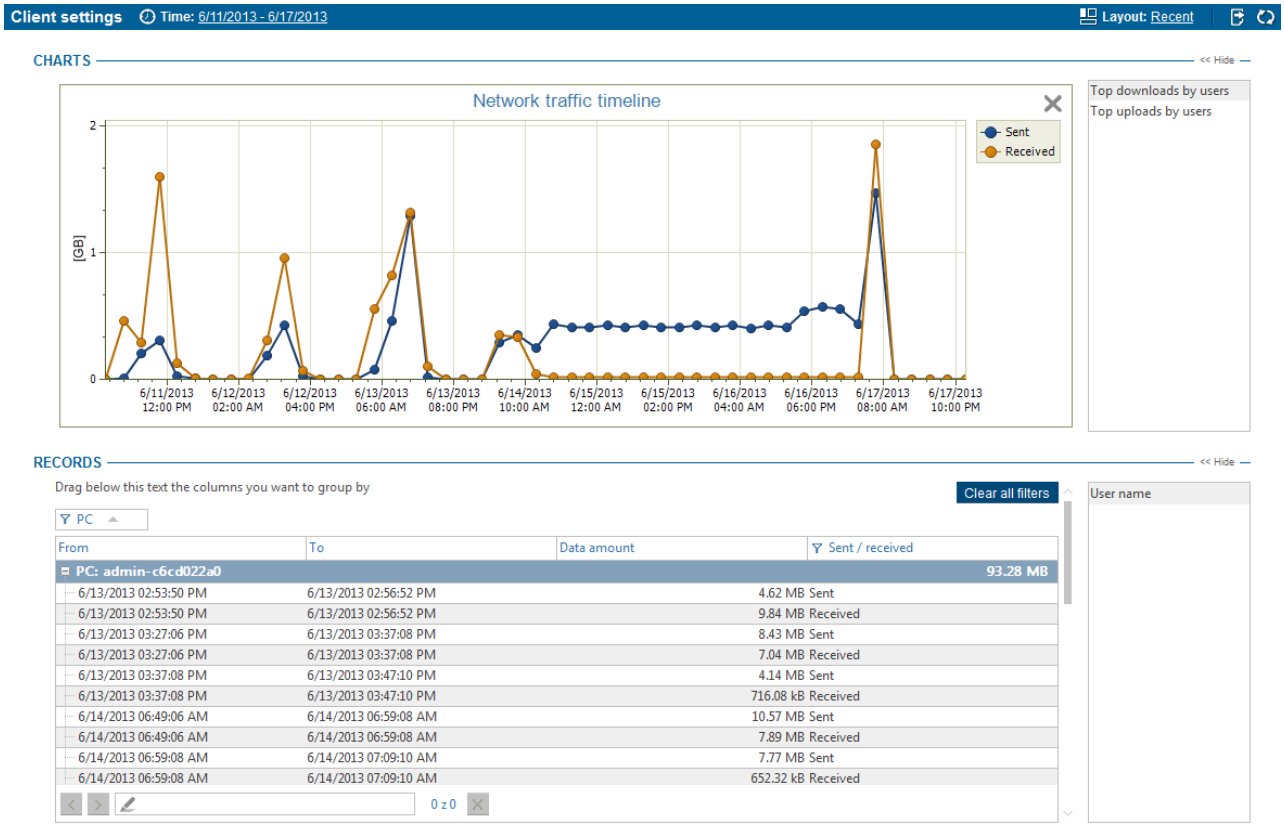
You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Network traffic monitoring is only set for users, computers, groups or branches you have highlighted in the user tree. To apply the settings, you have to save the changes using the button or you can cancel the changes you have made using the button in the upper right corner.

Visualization

Visualization shows records on volumes of data received from and sent to the end station. Data is recorded from all network interfaces.



In the upper visualization section you will find the following charts summarizing network activity:

- *Most received data per user* – this chart includes users with the highest amount of received data (up to seven users).
- *Most sent data per user* – this chart includes users with the highest amount of sent data (up to seven users).
- *Network traffic history* – this chart summarizes sent and received data.

In the bottom section you will find a table with detailed network activity records. Records are created on a regular basis, every ten minutes. Each record contains the following information:

- *PC* – name of PC where the record was made
- *User name* – name of user under which the record was made
- *From* – record start time
- *To* – record end time
- *Received/Sent* – if data was received or sent
- *Data volume* – volume of received or sent data during the record period

At the bottom you will find a summary of how the PCs were used. The table contains records with information showing how the PCs where SEC is installed were used.

5.1.3 Trends

Trends function allows users behavior monitoring and profiling. It offers clearly organized outputs, which can be used to get the overview of possible personal and security problems in advance. Profiling and behavior monitoring takes place automatically when the Trends function is enabled.

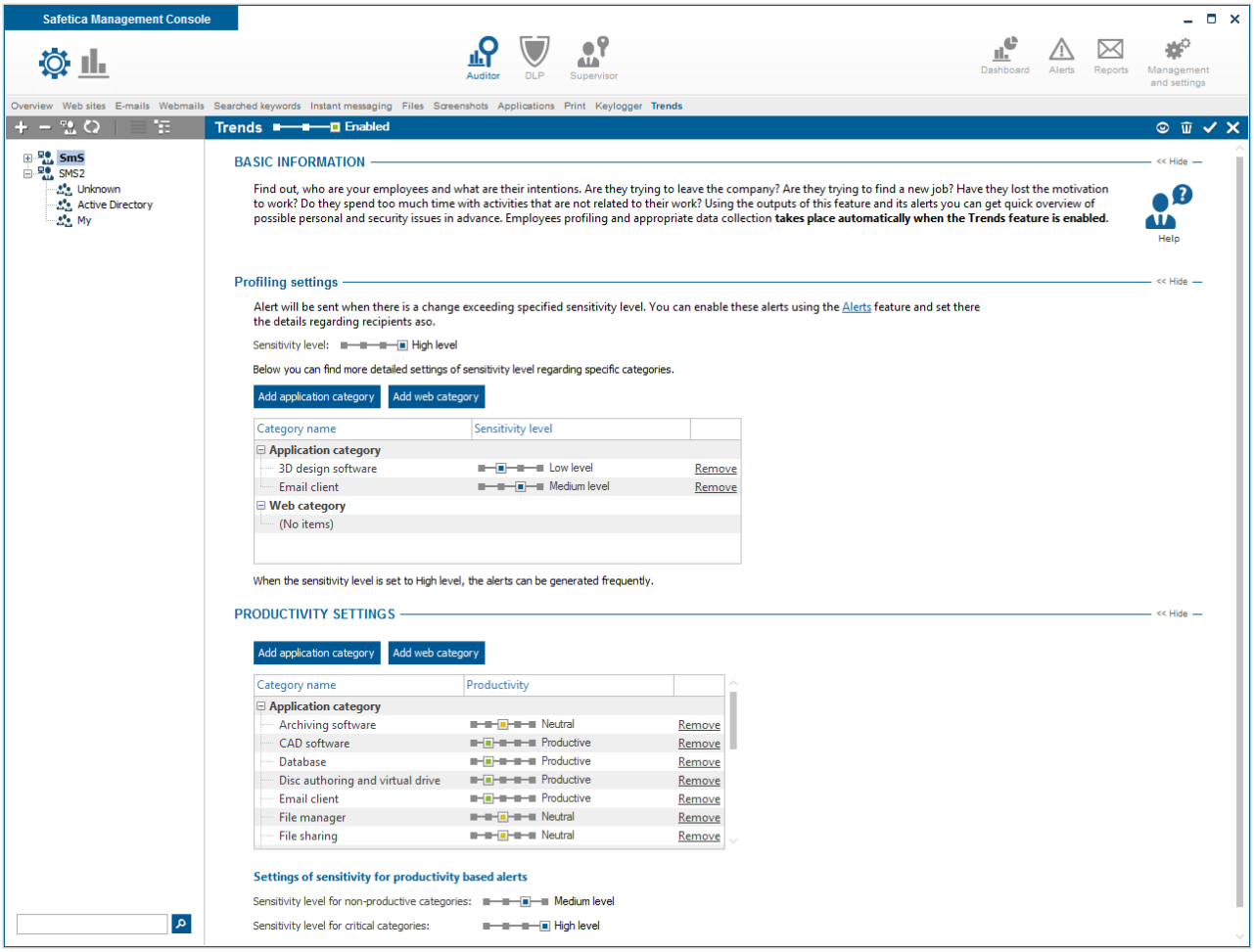
Trends function is in the section Auditor -> *Trends.*

Settings

You can enable or disable this function using the slider in the header of this view.

- *Disabled* – function is not activated. Data needed for trends visualization are not collected.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated. Data needed for trends visualization are logged henceforth.

Trends are only set for users, computers, groups or branches you have highlighted in the user tree. To apply the settings, you have to save the changes using the button or you can cancel the changes you have made using the button in the upper right corner.



Profiling settings

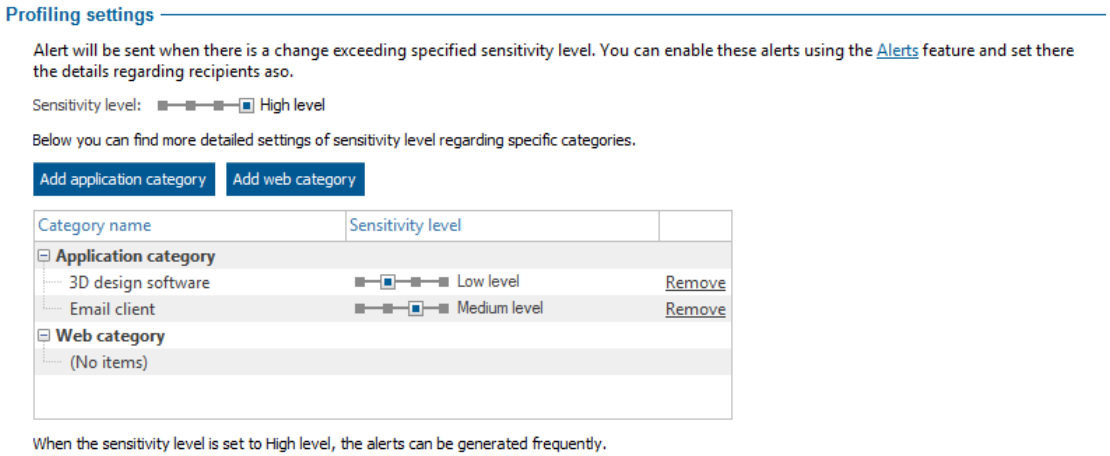
Using the detailed profiling settings you can set general level of sensitivity, which will be used for alerting of user's supsicious behavior. In case you want to be informed about increased activity in particular category, e.g. Games, you can adjust the sensitivity level for this category in the table.

You can set the sensitivity level to 4 different values:

- *Inherit* – not set, settings are inherited from the parent.
- *Low level* – low level of behavior changes sensitivity.
- *Medium level* – set this option, if you are not sure about the appropriate level
- *High level* – use this option, if you want to be informed even about slight changes of behavior. Set the High level for critical categories, where you want to be alerted even of slight changes. Low level should be used for common categories, where you want to be alerted

only of bigger changes in behavior.

Example: If you want to deny social networks, you can set High level to this category, therefore even the slight changes will be alerted.



Productivity settings

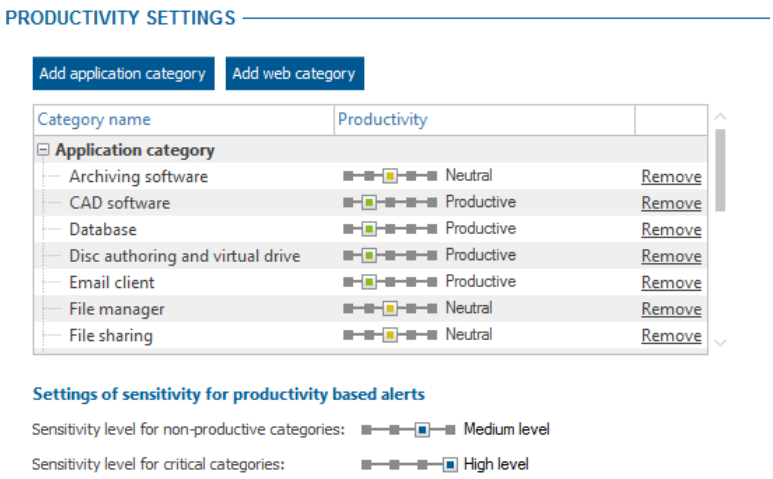
Using the productivity settings, you can set the level of productivity for individual application and web categories.

In the detailed productivity settings you can use the toggles to set the productivity for particular categories. You can also set the default productivity level, which will be used for categories, that don't have the productivity explicitly set.

At the bottom of this section you can set the sensitivity level, that will be used for alerting the productivity changes.

Productivity settings:

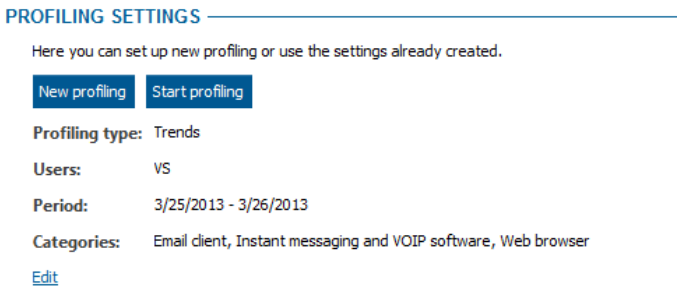
- *Inherit* – not set, settings will be inherited from the parent.
- *Productive* – set this option for categories that the employees should use.
- *Neutral* – set this option for categories you are not sure about. Categories should be set as Neutral if they can be useful and unuseful at the same time.
- *Nonproductive* – should be set for categories that are not essential for employee to fulfill his tasks.



Visualization

In the visualization, you can create new profiling or execute existing profiling. Profiling is taken on the data monitored during the period when the Trends function was enabled.

You can save the profiling settings using the Layout button in the upper right corner. Saved settings can be executed later, if you need to.



New profiling

The wizard will guide you through individual steps of setting the profiling options.

1. Type – this step is used to select the profiling type. You can select from the following options:

   o *Trends* – using this profiling type you can view the trend of individual categories usage.

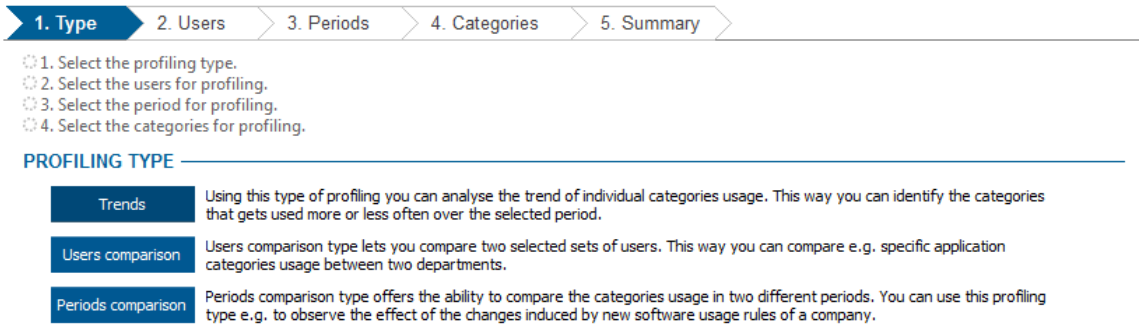
   Example: Employees want to use some new software claiming it will make them more efficient. The employer decides to install the trial version and after the trial period he can easily find out, whether the employees are really using the new software and choose to buy it or not.

   o *Users comparison* – enables you to compare two different sets of users in terms of categories usage.

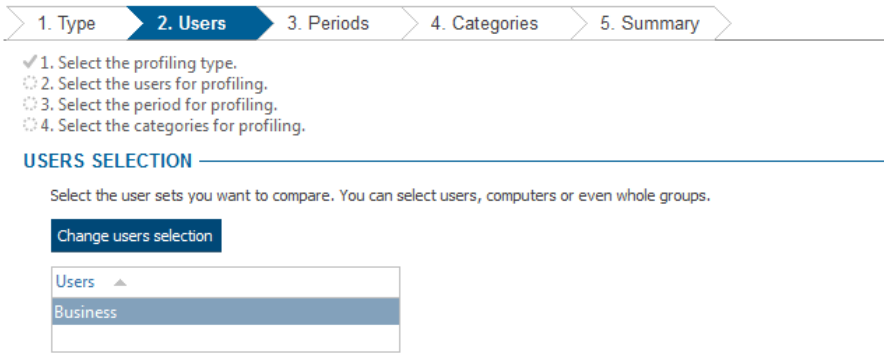
   Example: The employer wants to compare two affiliates, where the new software has been installed, to see, which affiliate uses the new software more and has therefore incorporated this software better to the production process.

   o *Periods comparison* – you can use this type to compare the categories usage in two different periods. Using this type you can see the changes induced by new company policies.

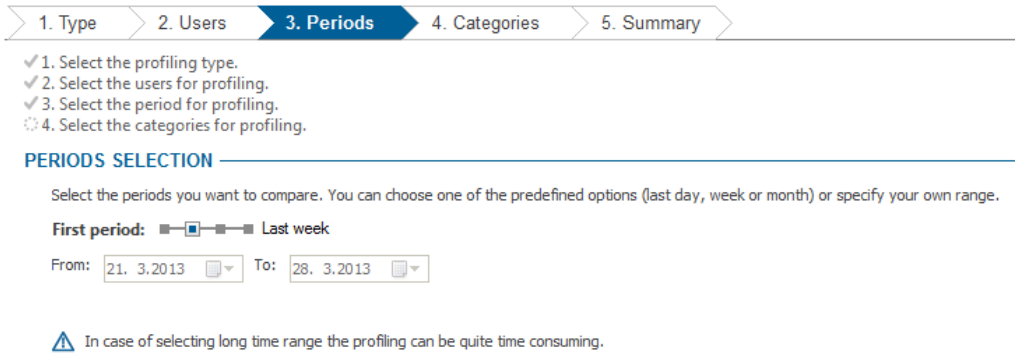
   Example: The employer can use this type to compare the same set of users accross two different periods and see, whether the employees are working more or less at some time (e.g. during holidays).



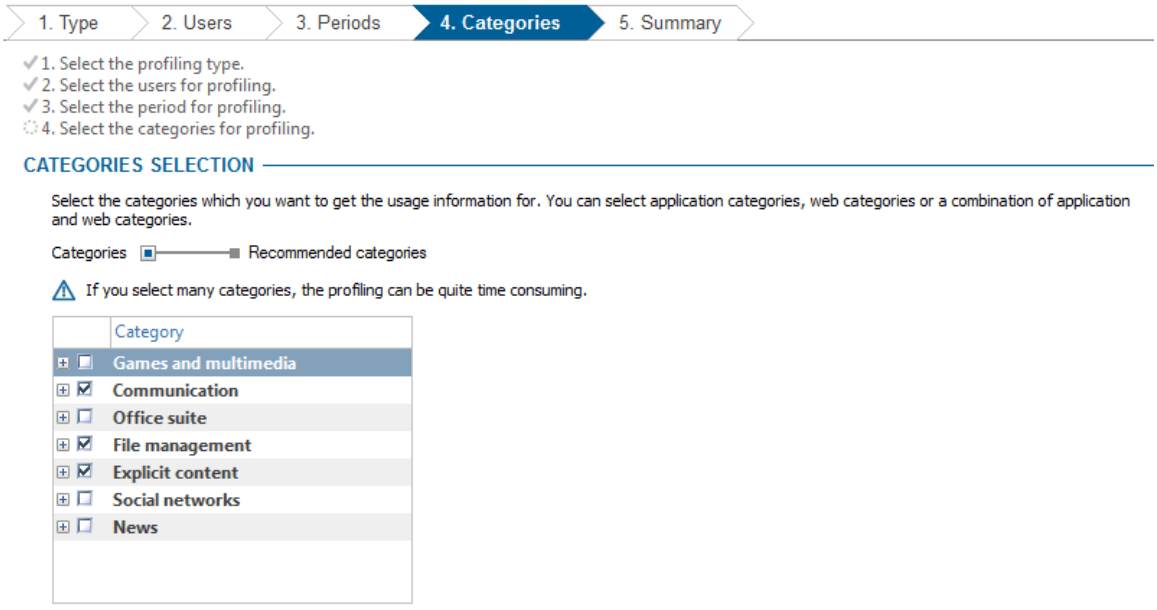
2. Users – in this step you can select the users, computers or groups you want to include in profiling. If you selected the Users comparison type, you have to select two different sets of users, computers and groups.



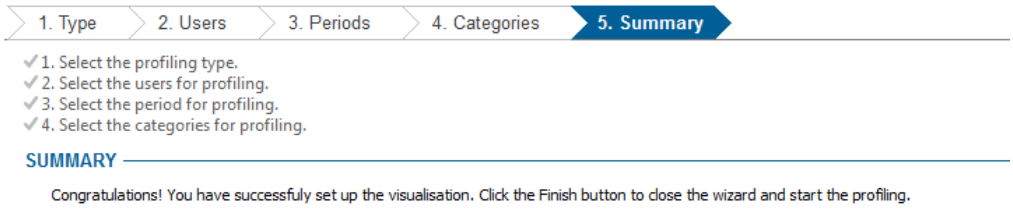
3. Periods – in this step, you can select the period, that you want to execute profiling on. You can select one of the predefined values or set custom time range. When you select the Periods comparison type, you have to select two different periods.



4. Categories – in this step you can select the categories you want to include in profiling. You can use the predefined sets of categories or make your own selection.

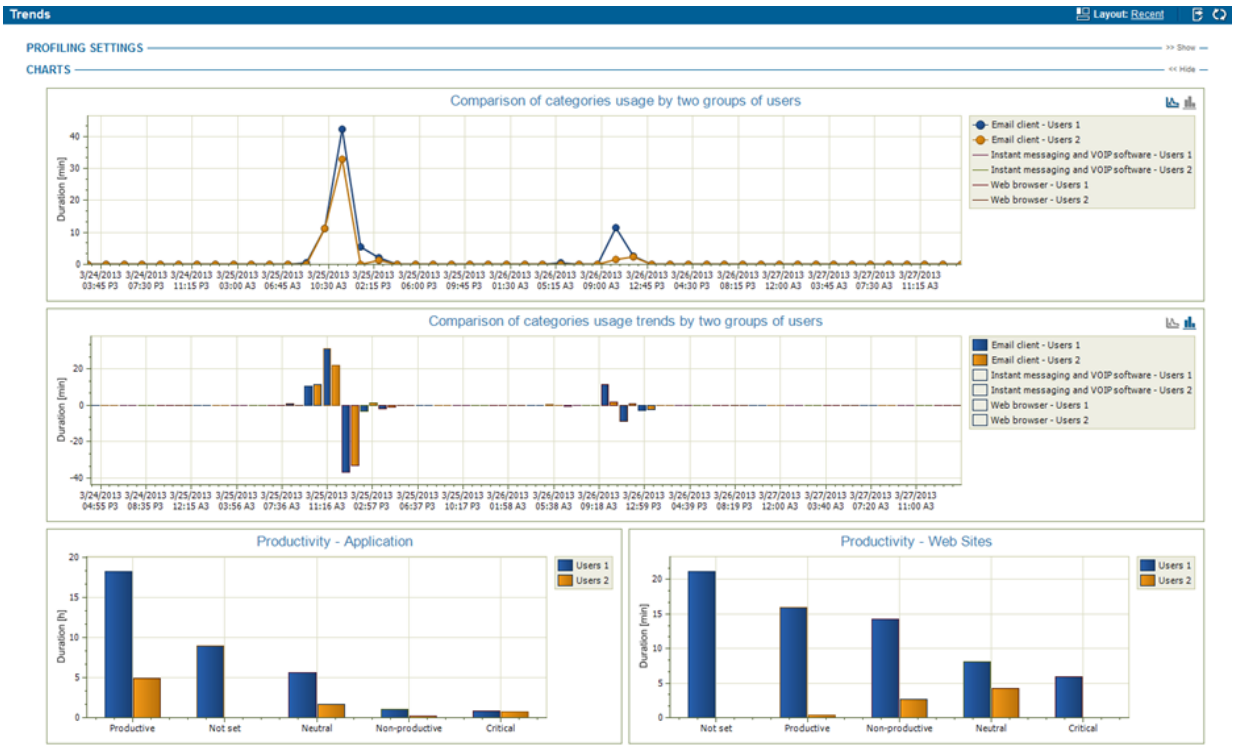


5. Summary – when you reach this step, you can click the Finish button to set the profiling settings and start its execution.



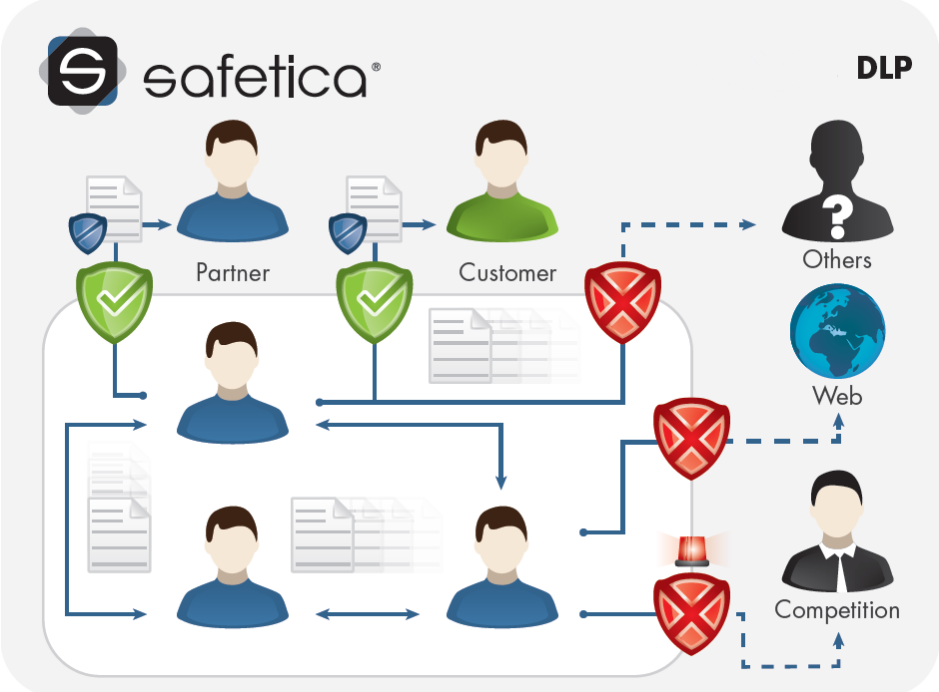
In the following picture you can see an example of profiling output:

- The first chart contains the active time (time actively spent) of individual application and web categories.
- The second chart contains the differences of application and web categories usage during the time.
  - o Positive values – the user has spent more time in this category then in previous period.
  - o Zero values – the user keeps spending the same amount of time in the category as usually.
  - o Negative values – the user has spent more time in the selected category than before.
- Last two charts show the ratio of active time spent in productive, neutral, nonproductive and critical applications and webs.



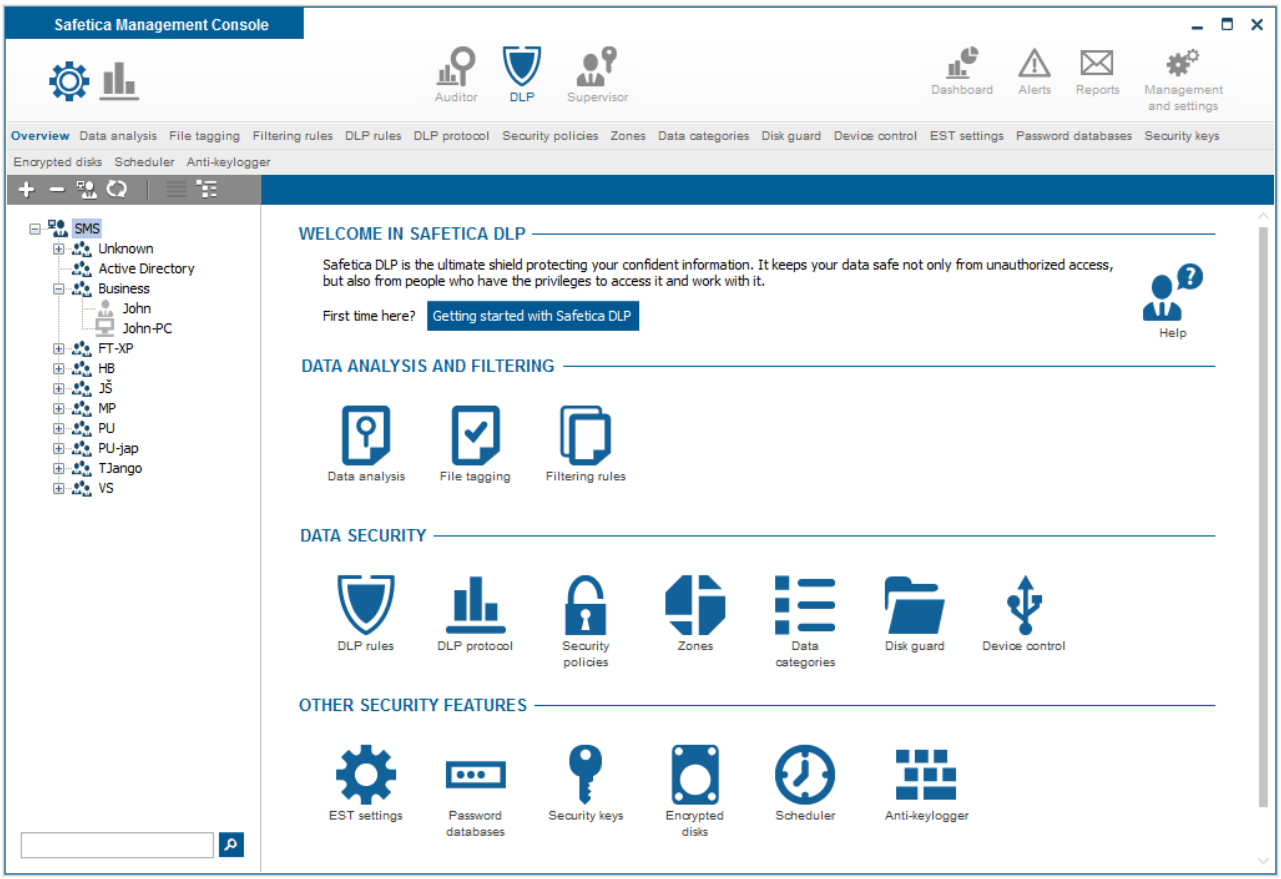
5.2 DLP

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's reputation. In cooperation with the Auditor, the DLP will protect you from the undesirable activities of your employees long before a problem even appears.



Main Benefits

- Protect your company against damage to its reputation and financial losses caused by leaks of sensitive information.
- Ensure that your employees use data only in the way which you require.
- Prevent unauthorized persons from accessing sensitive company data.
- Protect sensitive data during physical and network transfer.
- Obtain control over portable devices used by your employees to potentially save sensitive data.
- Avoid changes to company processes and the costs related to them.
- Reach compliance with industrial standards, regulations and laws easily.



5.2.1 Data analysis and filtering

5.2.1.1 Data analysis

With the data nalysis function you can search through files on end users' PCs. You can perform the search based on a filtering rule or directly based on a path to folders with files. In path-based search, all files located in the folders and their subfolders will be searched automatically. Files found through data analysis can be further tagged by using such functions as File tagging and DLP rules and/or security policies can be defined for them.

Data analysis is available via *Safetica Management Console -> DLP -> Data analysis*.

View description

The left side of the view shows the analysis list. The current status of each analysis (running, finished) and number of files found in the respective analysis are displayed. There is also progress bar which show analysis status:

- *Green* – finnished tasks.
- *Orange* – running tasks.
- *Blue* – tasks waiting to run.
- *Red* – stopped tasks.

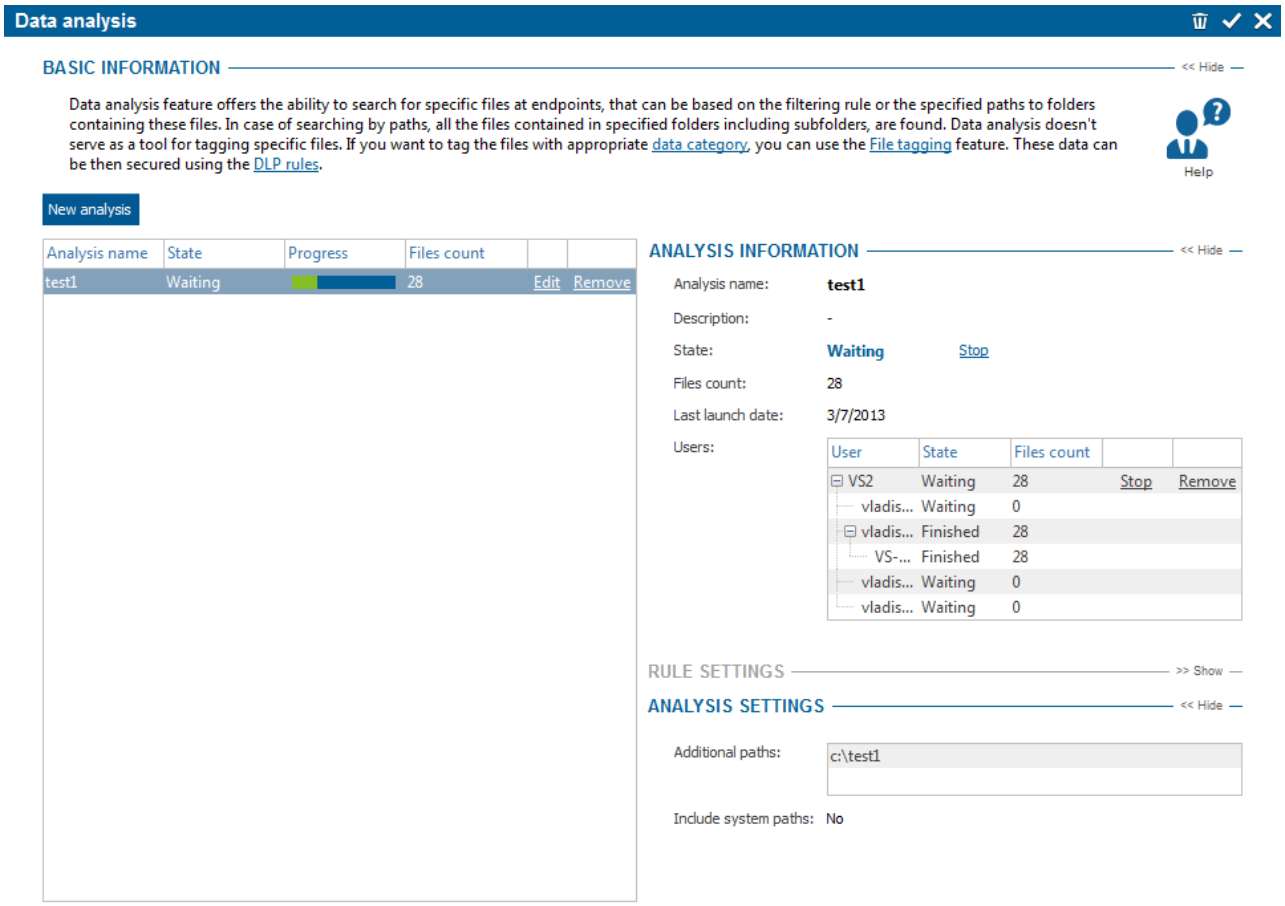
After selecting the desired analysis in the list, detailed information on this analysis will be displayed in the top right section of the view.

In the Basic Information section you can see the general analysis status, start date and status of analyses for different users or PCs. You can also stop or remove an analysis from the list here.

You can stop the analysis by clicking Stop.

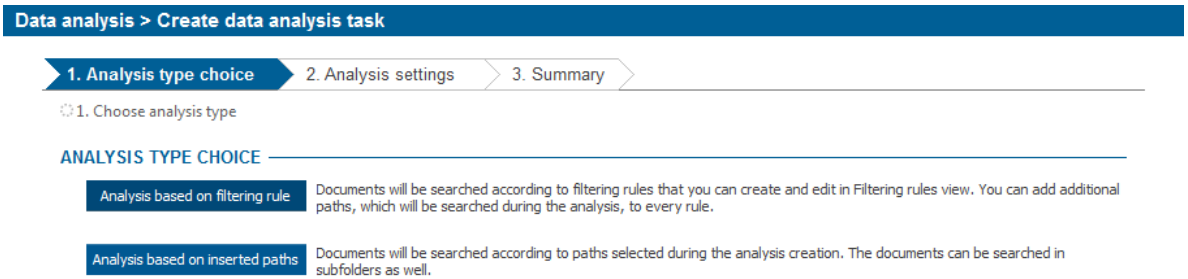
Data analysis is set only for users, groups or PCs selected in the user tree. To apply the settings,

you need to save the changes with the button or you can cancel the changes with in the top right part.



Performing an analysis

1. Click the New analysis button to start the new analysis wizard.
2. First you need to choose the rule based on which the analysis shall be performed. You can choose from two options:
   a. *Data search based on filtering rule* – the file search will be performed based on filtering rules you create in the Filtering rules view.
   b. *Data search based on your own paths* – the file search will be performed in folders you enter. The respective subfolders will also be searched.



Rule-based search settings

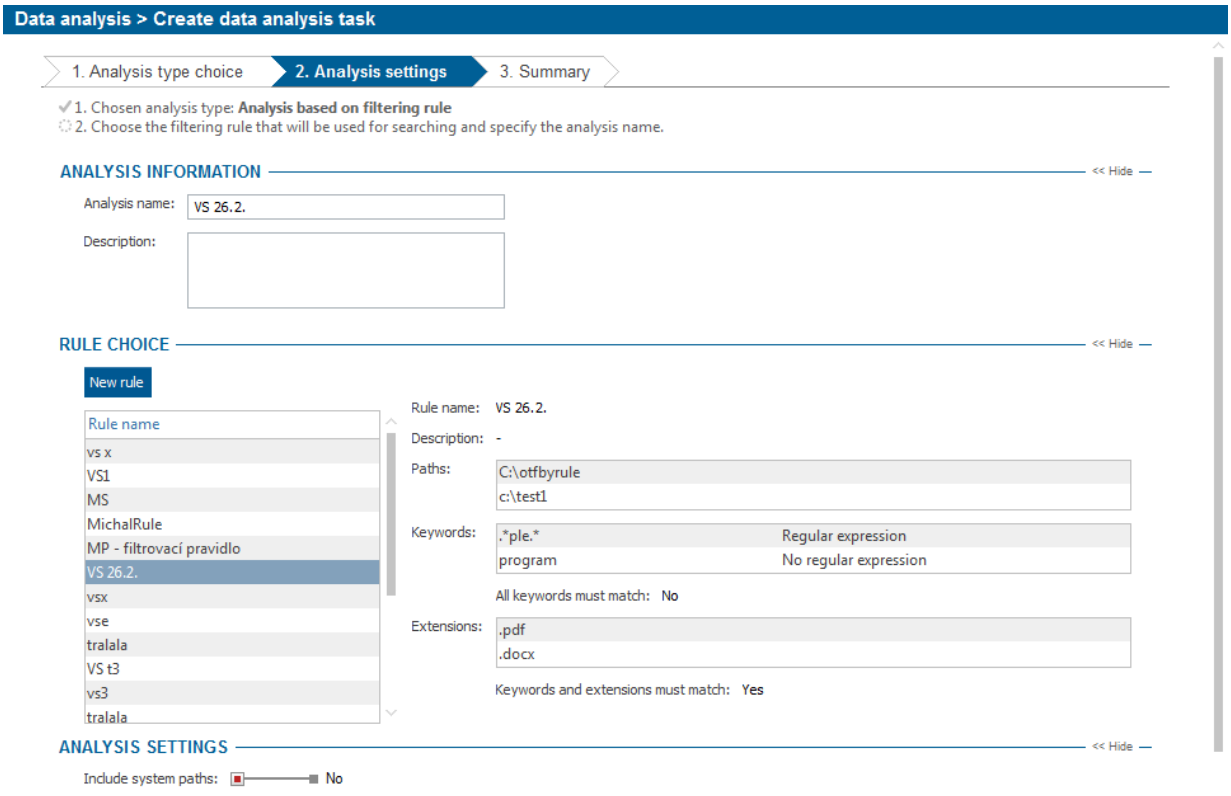
1. In the left part of the view select a rule to be used for the search. After selecting the rule in the list, detailed information on this rule will be shown in the right part. If no filtering rules have been created, click the *New filtering* rule button. This will take you to the Filtering rule view where you can create the new rule. Finally, use the slider Include system paths to spe-

cify whether the search shall include also system folders. To confirm your choice, click *Next*.

Note: System folders can be searched only if such paths appear in the filtering rule and if the slider Include system folders is set to Yes. As system folders are considered these:

- C:\System Volume Information
- C:\Users\<User name>\AppData
- C:\Program Files
- C:\Program Files (x86)
- C:\Windows

2. In the last step of the new analysis wizard you will see a summary of all analysis settings. To edit an item, click Previous. To finish the process, click Finish.
3. After clicking the Finish button, a dialog box will appear asking you if the analysis shall be started now. You can start the analysis from the view listing the analyses you have created.



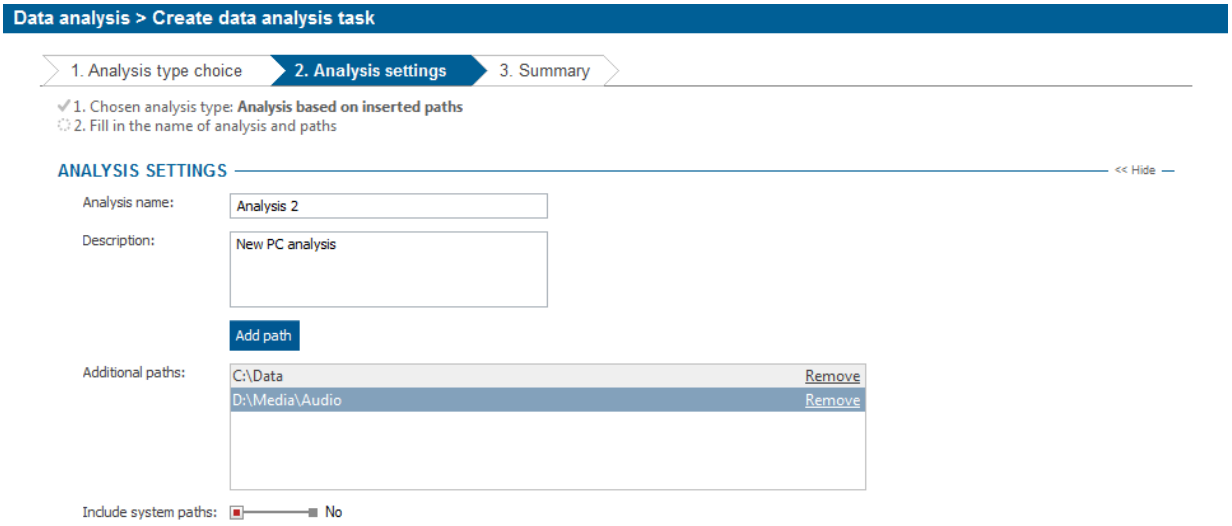
Search settings based on the user's own paths

1. Enter the analysis name and description. Click *Add path* to open the dialog where the path to the folder can be entered. You can even input several paths this way. In the path-based analysis, all files located in the folders you have entered and in their subfolders will be searched automatically. Finally, use the slider Include system folders to specify whether the search shall take place also in system folders (e.g. C:\Windows). To finish your choice, click *Next*.

   Note: System folders can be searched only if such folders or subfolders are in the rule and if the slider Include system folders is set to Yes.

2. In the last step of the new analysis wizard you will see a summary of all analysis settings. To edit an item, click Previous. To finish the process, click *Finish*.
3. After clicking the Finish button, a dialog window will appear asking you if the analysis shall

be started now. You can start the analysis from the view where the analyses you have created are listed.



Starting an analysis

You can start the data analysis either when creating a new analysis or at a later time, from the view where the analyses you have created are listed. Just select the desired analysis in this view in the right part with detailed analysis information and click Start.

You can see results of the analysis in the visualization mode, after the analysis task has finished.

Stopping an analysis

You can stop an analysis from the view where the analyses you have created are listed. Just select the desired analysis in this view in the right part with detailed analysis information and click Stop.

Visualization

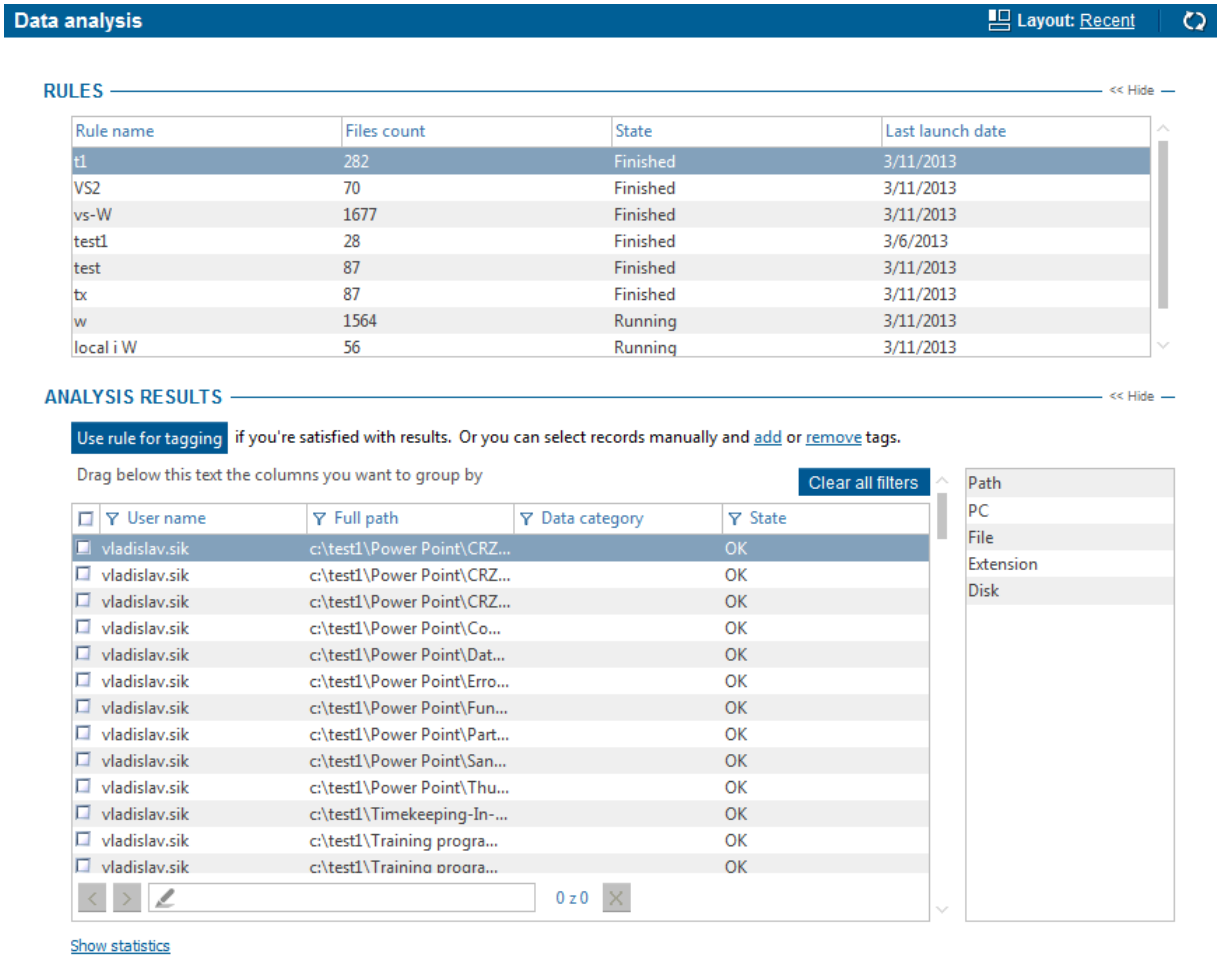
The data you can see in the visualization will be displayed only for users, PCs and groups you have selected in the user tree. The visualization mode is split up into three sections.

In the top section on the left you will find summary statistics on the analyses you have performed. In the top right part there is a list of tagging jobs with detailed information.

The bottom visualization section offers a table with records on the files you have tagged. Every record contains several types of information presented in columns. The list of available columns is again shown to the right of the table. The column will appear in the table after clicking and dragging the column from the list onto the table. Click and drag the column header to change the column order in the table. In the same way, you can drag column headers onto the section above the table. Records in the table will then be pooled above the table based on the column type. You can remove a column from the table by dragging it back onto the column list on the right side.

By clicking any of the statistics or tagging job in the top section, the respective records on the files matching the statistics or tagging job will appear in the table.

By clicking *Use rule for tagging* button you can use performed analysis to tag found files by data catecory. Tagging is done using File tagging function.



Columns available:

- *PC* – name of PC where the record was made.
- *User name* – name of the user under which the record was made.
- *Disk* – disk letter on which the file was found.
- *Path* – path to the file found.
- *File* – name of the file found including file extension.
- *Extension* – file type extension
- *Full path* – full path to the file.
- *Data category* – data categories by which the file is tagged.
- *State* – state of analysis: Ok or Failed.

You can filter the records as well. Open the filter for any column by clicking at the header of the respective column. Enter text in the dialog or choose an item from the list based on which you wish to filter the column. Click + to add an item to the filter list. The length of this list is unlimited. After confirming the filter with OK, the table will feature only such records which correspond at least to one filter listed.

Find more on settings and visualization in the section Working with Setting and Visualization Mode.

5.2.1.2 File tagging

In the File tagging Management you can search and tag files with the corresponding data category on PCs equipped with the Safetica Endpoint Client. You can secure files tagged this way by applying DLP rules.

File tagging remains fixed with the file regardless of any operations you perform (moving, copying, change of file). The tagging will not noticeably change the file either.

Files can be tagged in two ways:

- *On the fly tagging* – a tagging task set to continuous tagging continues running. This means that where new files appear that either match the filtering rule or are located in the folder entered when creating tagging tasks, such files are automatically tagged with the respective data category. When tagging, security rules determined by the Security Policy for the data category used in the tagging are immediately applied to the files.
- *On demand tagging* – a tagging task set to one-time tagging will be executed only once. This means that files matching the filtering rule at the moment the task is executed or are just located in the folder entered when creating tagging tasks are automatically tagged with the respective data category. When tagging, security rules are immediately applied to such files, as given by the DLP rule used for the data category. New files, matching the filtering rule or located in the respective folder, will not be tagged.

File tagging is available via Safetica Management Console -> DLP -> File tagging.

View description

The left section of the view shows the tagging tasks list. The current status of each task (running, finished) and tagging type (on the fly, one-time) are displayed. There is also progress bar which show tagging status:

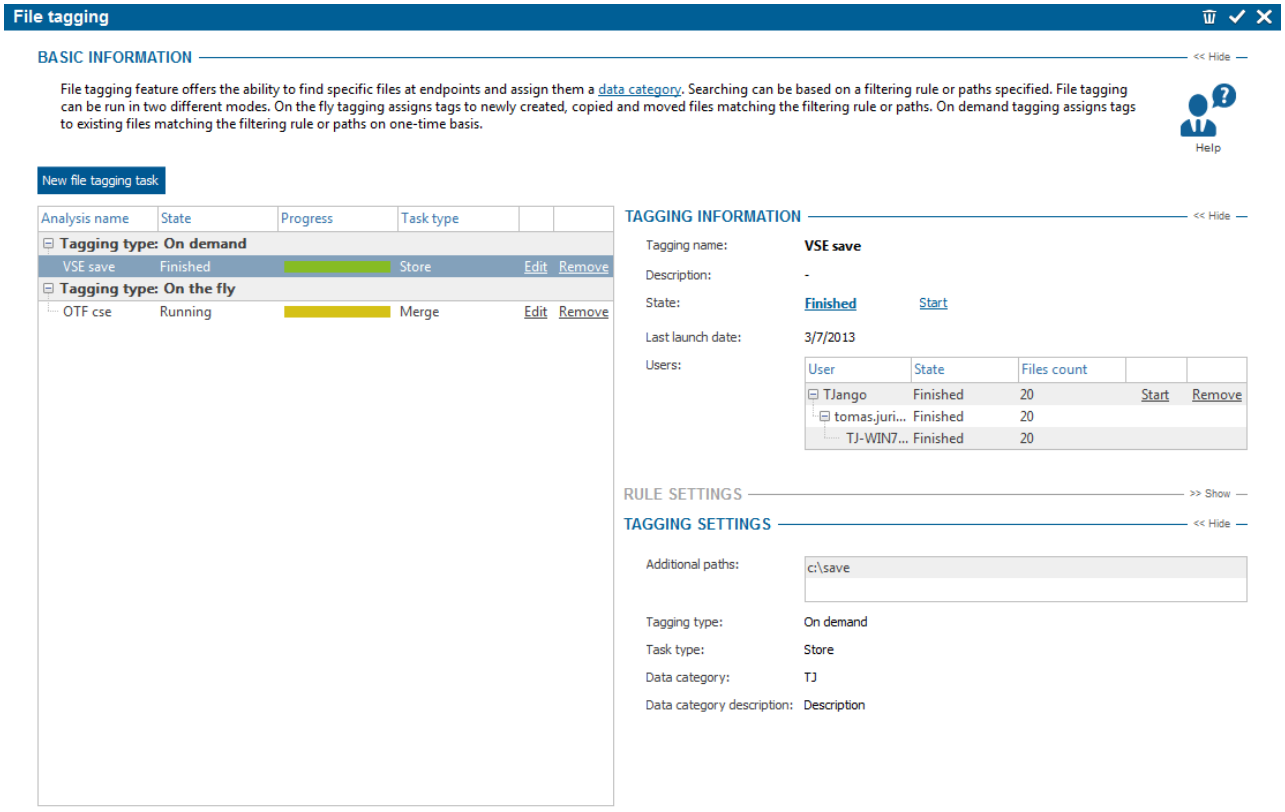
- *Green* – finnished tasks.
- *Orange* – running tasks.
- *Blue* – waiting for run.
- *Red* – stopped tasks.

After tagging the desired task in the list, detailed information on this task will be displayed in the top right section of the view.

In the Basic Information section you'll find the general tagging task status, start date and status for different users or PCs. You can also stop or completely remove a tagging task from the list here.

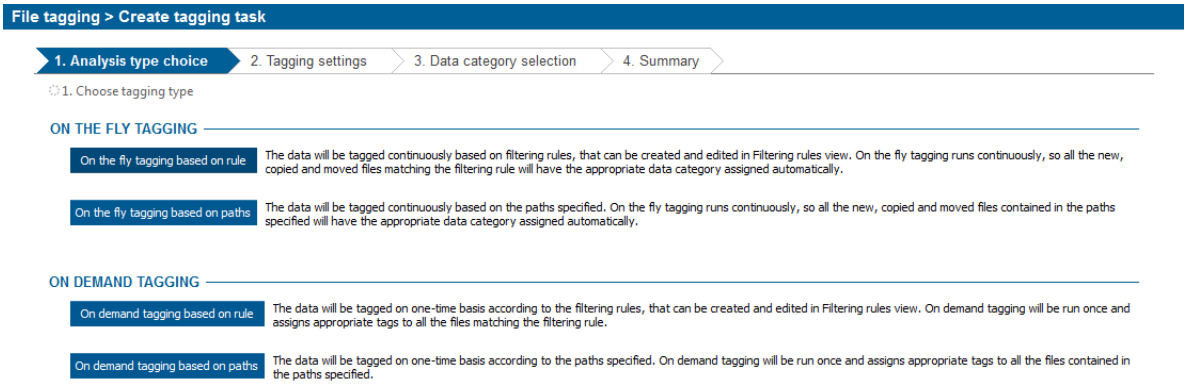
You can stop the tagging task by clicking Stop.

You set tagging tasks only for users, groups or PCs tagged in the user tree. To apply the settings, you need to save the changes with the  button or you can cancel the changes with  in the top right part.



Creating tagging tasks

1. Click the New file tagging task button to start the new tagging task wizard.
2. First, you need to choose based on what rule the tagging task shall be executed and what tagging type this shall be – one-time or continuous. You can choose from several options:
   a. *On the fly tagging based on filtering rule* – continuous data tagging based on a filtering rule created in the Filtering rules view. On the fly tagging continues running, so every new, copied or moved file matching the filtering rule is automatically tagged with the respective data category.
   b. *On the fly tagging based on your own paths* – the file tagging will be performed in folders you enter. Also the respective subfolders will be searched. On the fly tagging continues running, so every new, copied or moved file that appears in any of the paths you have entered is automatically tagged with the respective data category.
   c. *On demand tagging based on filtering rule* – one-time data tagging based on a filtering rule created in the Filtering rules view. On demand tagging will be performed once. All files currently matching the filtering rule will be tagged with the respective data category.
   d. *On demand tagging based on paths* – the file tagging will be performed in folders you enter. The respective subfolders will also be searched. On demand tagging will be performed once. All files currently located in the paths you have entered will be tagged with the respective data category.

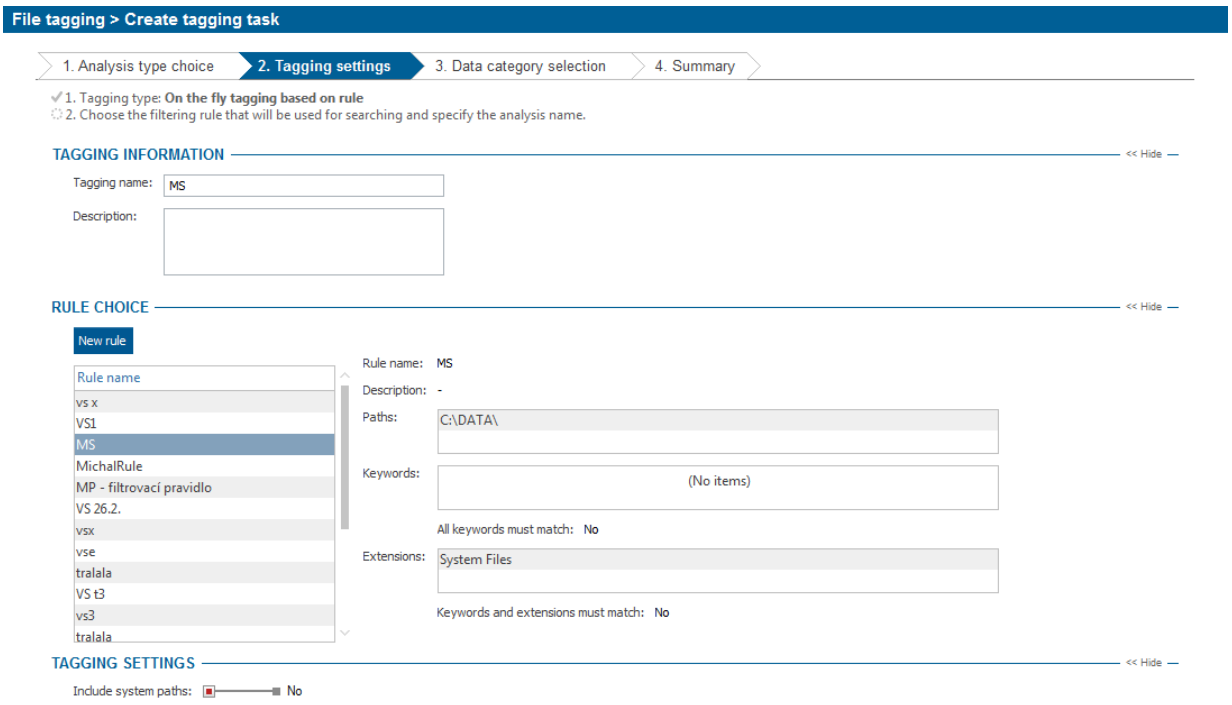


On the fly and On demand data tagging based on a filtering rule

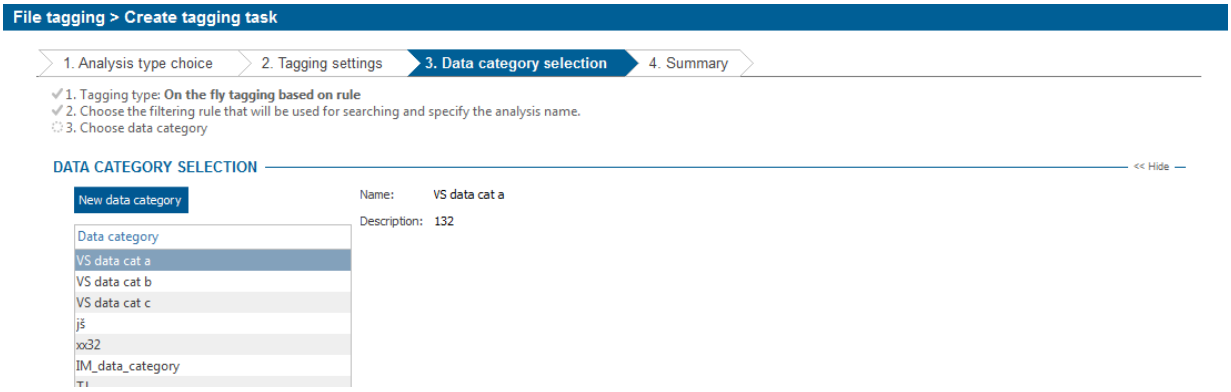
1. In the left part of the view choose the filtering rule to be applied for the search and tagging. Choose a name for the tagging task as well. After clicking the rule in the list, detailed information on this rule will be shown in the right part. If no filtering rules have been created, click the *New filtering* rule button. This will take you to the Filtering rule view where you create the new rule. Finally, use the slider *Include system paths* to specify whether the search shall include also system folders. To confirm your choice, click *Next*.

   Note: System folders can be searched only if such paths appear in the filtering rule and if the slider Include system folders is set to Yes. As system folders are considered these:

   - C:\System Volume Information
   - C:\Users\<User name>\AppData
   - C:\Program Files
   - C:\Program Files (x86)
   - C:\Windows



2. In the next step choose a data category from the list. If you wish to create a new data category, click *New data category*. Enter a name and description for it in the dialog and click *OK*. The new data category will appear in the list. To finish the choice of the data category, click *Next*.

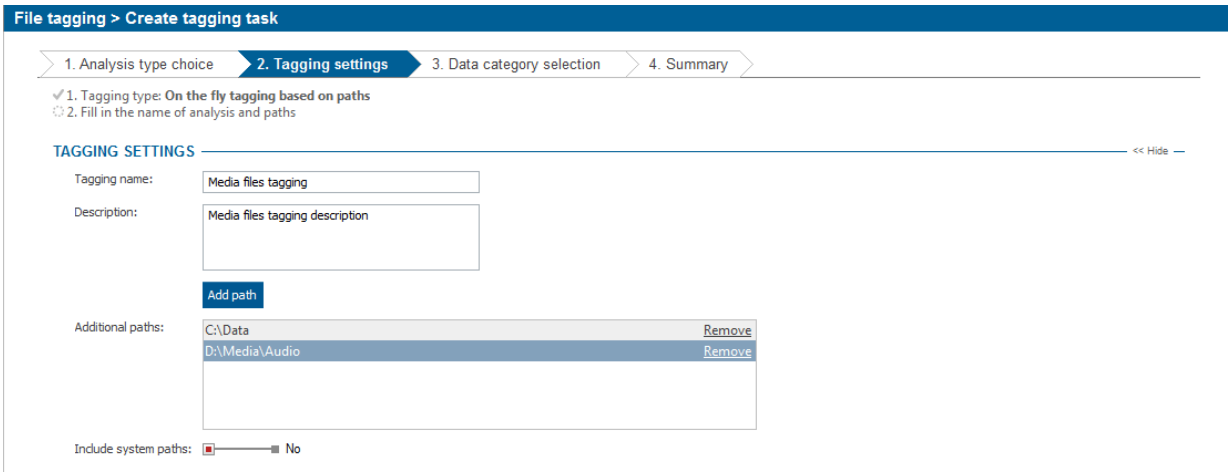


3. In the last step of the new tagging task wizard you will see a summary of the settings. To edit an item, click Previous. To finish the process, click *Finish*.
4. After clicking the Finish button, a dialog box will appear asking you if the tagging task shall be started now. You can start the tagging task from the view where the tasks you have created are listed.

On the fly and On demand data tagging based on the user's own paths

1. Enter the tagging task name and description. Use the *Add path* button in the bottom section of the view to add paths to folders in which all files shall be tagged. Files will be tagged also in the subfolders of the paths entered. Finally, use the slider *Include system paths* to specify whether the search shall include also system folders. To confirm your choice, click *Next*.

   Note: System folders can be searched only if such paths appear in the filtering rule and if the slider Include system folders is set to Yes.



2. In the next step choose a data category from the list where the files will be tagged. If you wish to create a new data category, click *New data category*. Enter a name and description for it in the dialog and click *OK*. The new data category will appear in the list. To confirm the choice of the data category, click *Next*.
3. In the last step of the new tagging task wizard you will see a summary of the settings. To edit an item, click Previous. To finish the process, click Finish.
4. After clicking the Finish button, a dialog window will appear asking you if the tagging task shall be started now. You can start the tagging task from the view where the tasks you have created are listed.

Starting a tagging task

You can start the tagging task either when creating a new tagging task or at a later time, from the view where the tagging tasks you have created are listed. Just select the desired tagging task in this view in the right part with detailed tagging task information and click Start.

You can see results of the tagging in the visualization mode, after the tagging task is done.

Stopping a tagging task

You can stop a tagging task from the view where the tagging tasks you have created are listed. Just select the desired tagging task in this view in the right part with detailed tagging task information and click Stop.

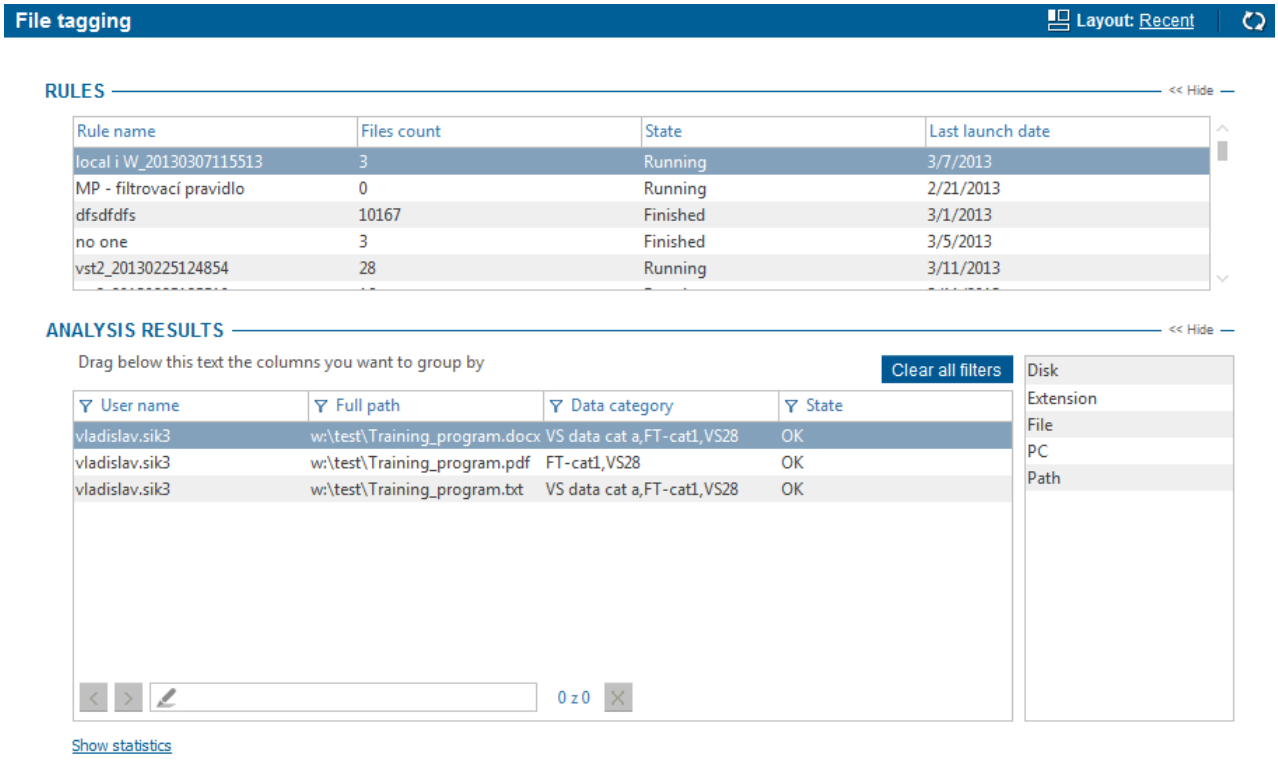
Visualization

You can only see results of on demand tagging tasks in the visualization mode. Records contain information about tagged files. The data you can see in the visualization will be displayed only for users, PCs and groups you have tagged in the user tree. The visualization mode is divided into three sections.

In the top section on the left you will find summary statistics on the tagging tasks you have performed. At the top right you will see a list of tagging tasks with detailed information.

The bottom visualization section offers a table with records on the files you have tagged. Every record contains several types of information presented in columns. The list of available columns is again shown to the right of the table. The column will appear in the table after clicking and dragging the column from the list onto the table. Click and drag the column header to change the column order in the table. In the same way, you can drag column headers onto the section above the table. Records in the table will then be pooled above the table based on the column type. You can remove a column from the table by dragging it back to the column list on the right side.

By clicking any of the statistics or tagging task in the top section, the respective records on the files matching the statistics or tagging task will appear in the table.



Columns available:

- *PC* – name of PC where the tag of a file was made.
- *User name* – name of user under which the tag of a file was made.
- *Disk* – letter of the disk on which the tag of a file was made.
- *Path* – path to the tagged file.

- *File* – name of the tagged file.
- *Extension* – extension of the tagged file.
- *Data category* – list of data categories under which the file is tagged.
- State – state of file tagging: *OK* or *Failed*.

You can filter the records as well. Open the filter for any column by clicking at the header of the respective column. Enter text in the dialog or choose an item from the list based on which you wish to filter the column. Click + to add an item to the filter list. The length of this list is unlimited. After confirming the filter with OK, the table will feature only records corresponding to at least one filter listed.

Find more information on settings and visualization in the section Working with setting and visualization mode.

5.2.1.3 Filtering rules

The Filtering rules function is integrated with other functions of Safetica, allowing the user to ensure effective data protection against unauthorized use or misuse on end workstations.

Rules for filtering are intended for creating rules based on which data (files) are searched on end workstations. Data found in this way and tagged using File tagging function can then be protected by DLP rules function.

Filtering rules are available via *Safetica Management Console -> DLP -> Filtering rules*.

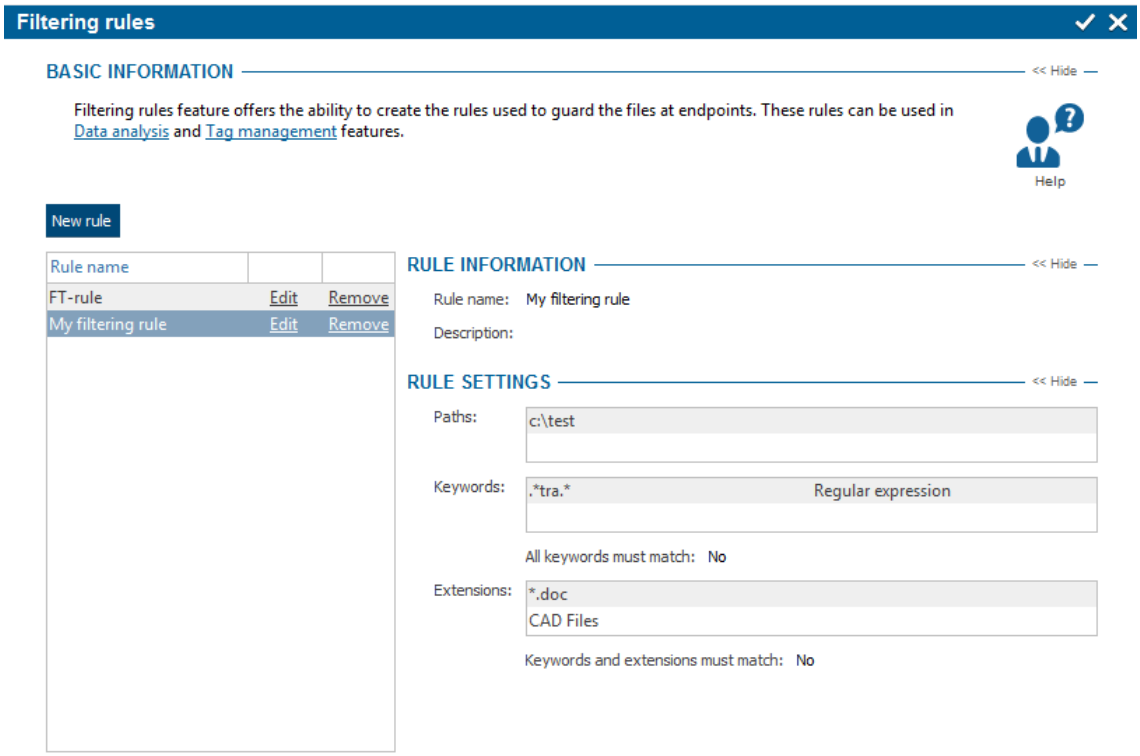
View description

In the left part of the view you will find a list of filtering rules you have created – rules based on which files on end workstations will be searched.

After selecting the desired rule in the list, detailed information on this rule will be displayed in the top right section of the view.

Click Edit on the respective rule section to edit this rule section.

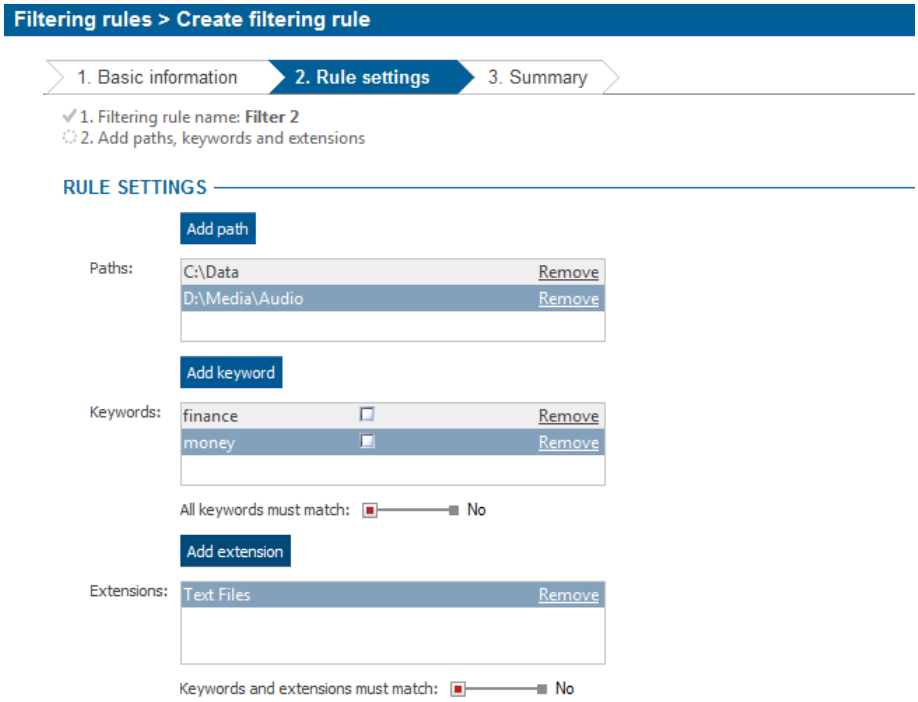
Click New filtering rule to launch the new rule wizard. When created, the rule will be added to the rules list.



Creating rules for filtering

1. To create a new filtering rule, click *New filtering rule*.
2. In the next step enter the rule name and description. Then click Next at the bottom right.
3. In this step set the file search rule in detail. You can search based on the path to files, key words in the file name or the file extension. You can also create a rule corresponding to all three conditions.
   a. *Add path* – after clicking on this button, a dialog will open for entering the path to be used for file search. You can add multiple paths.
   b. *Add keyword* – after clicking on this button, a dialog will open for entering key words to be used for file search. You can add multiple key words. The key word you have entered will be used for searching in file names and whenever it is found, the file will correspond to this filtering rule. You can use regular expressions as well (https://en.wikipedia.org/wiki/Regular_expression).
   c. *Add extension* – click on this button and a dialog for entering the file extension to be used for file search will open. Extensions can be entered manually or selected from a file extension database included in Safetica.
   d. *All keywords must match* – you can use the slider to specify whether all files containing all key words shall be searched, or only files containing at least one key word.
   e. *Keywords and extensions must match* – you can use the slider to specify whether all files matching the key words and extensions shall be searched or if only files that match the keywords or extensions shall be searched.

   After creating rules for filtering, click Next.



4. In the last step you can view the details of the rule you have created. By using Previous or Edit, you can return to any desired step and modify a rule section. After clicking Finish, the rule will be added to the filtering rules list. To save the rule, click  in the top right corner of the view.

5.2.2 Data security

5.2.2.1 DLP rules

The DLP rules function (DLP – Data Loss Prevention) is intended for creating security rules for files and applications. Files are identified based on their tagging with data categories. Applications are identified based on their application category classification. When creating these rules, security policies are used. It allows centralized management of settings in more extensive environments.

You can deploy DLP rules on files to specify the operations that may be performed on them and the places that files may be moved to. For applications, the rules can determine what operations are Allow, what files the application may access and how all files saved from the application can be secured. Any DLP rule created must be coupled with a security policy. Exceptions can, however, be set to assigned security policies.

DLP rules are available via Safetica Management Console -> DLP -> DLP rules.

View description

On the left of the screen you will find the list of DLP rules created. The rules are divided according to their type:

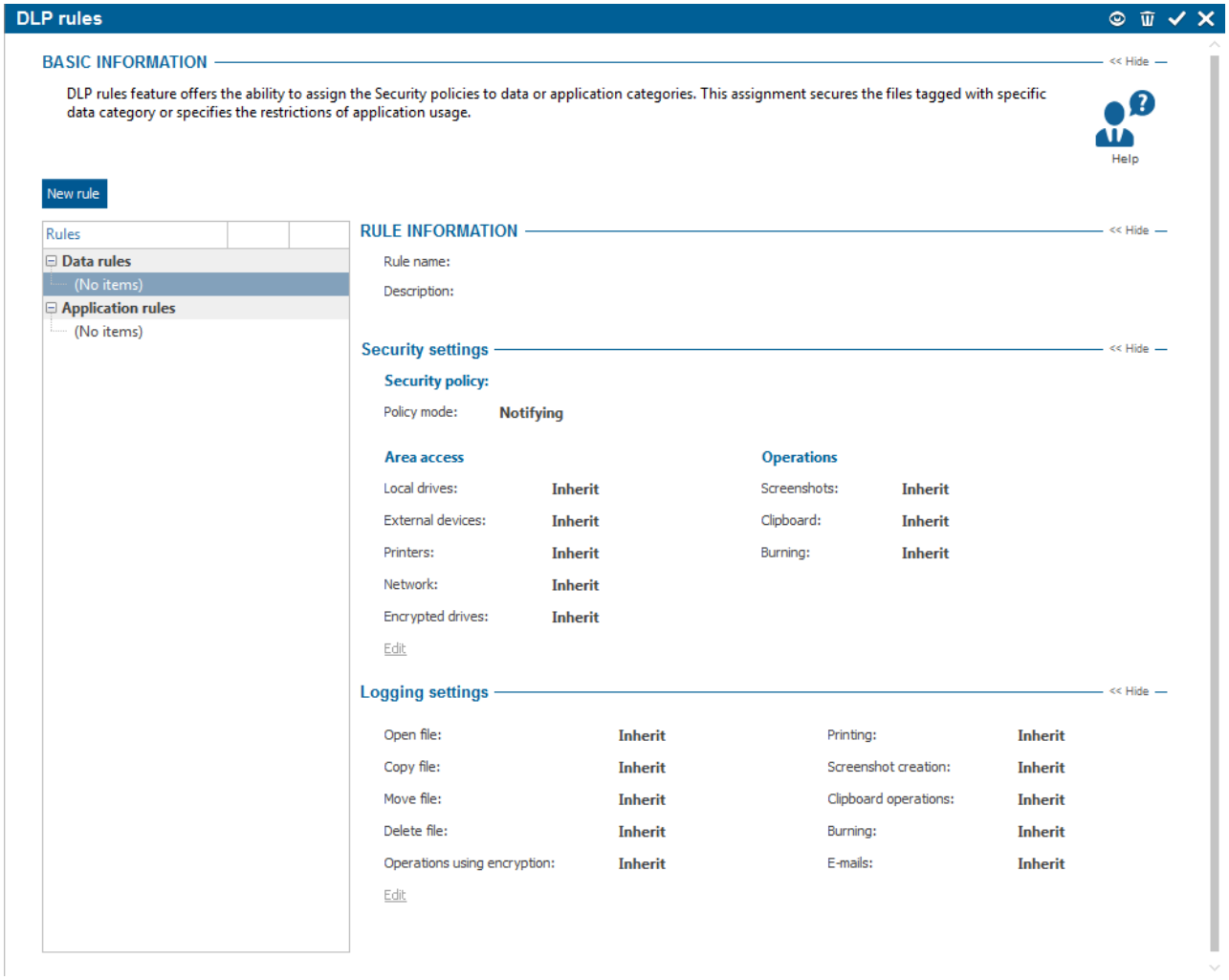
- DLP rules for Data categories – these are DLP rules assigned to the respective data category. The files tagged with the data category are then protected in accordance with the DLP rule assigned for the data category.
- DLP rules for Application categories – these are DLP rules assigned to the respective application category. Applications in the application category will behave according to the DLP rule that has been assigned to them.

Click New DLP rule to launch the new rule wizard. When created, the rule will be added to the rules list.

After marking the desired rule in the list, detailed information on this rule will be displayed in the top right section of the view.

Click Edit on the respective DLP rule section to edit this rule section.

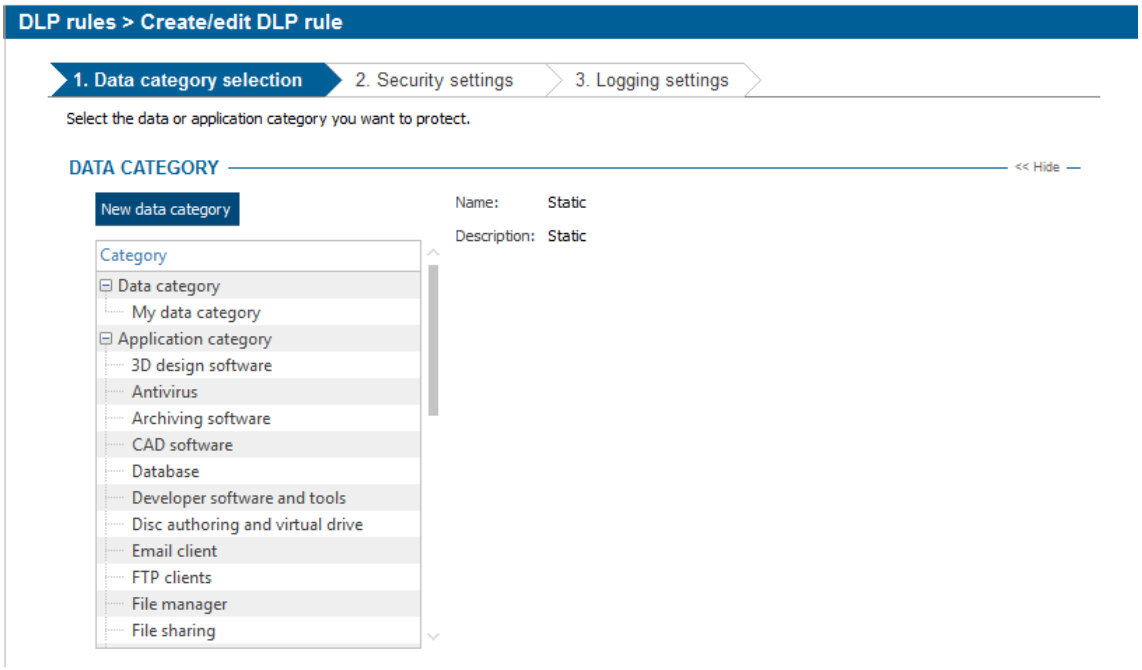
To save the changes and rules you have just created, you need to confirm the changes with the button or you can cancel your changes with the button on top right.



Creating a new DLP rule

To create a new DLP rule, click the New rule button.

1. In the first step select from the list on the left a data or application category for which you will create the DLP rule. If no data category has been created, you must create one first – click New data category. To confirm the choice of the category, click Next.



2. In the second step, you must first choose the security policy. Then, specify the policy mode, i.e. how the security policy shall be applied, and finally decide if you wish to create exceptions in the security policy. Three security policies modes are available:

   a. *Restrictive* – the security policy will be applied exactly according to its settings. The user will be able to access only allowed areas and any other deny operations will be blocked as well. This mode is recommended only after testing the security policy in the testing mode.

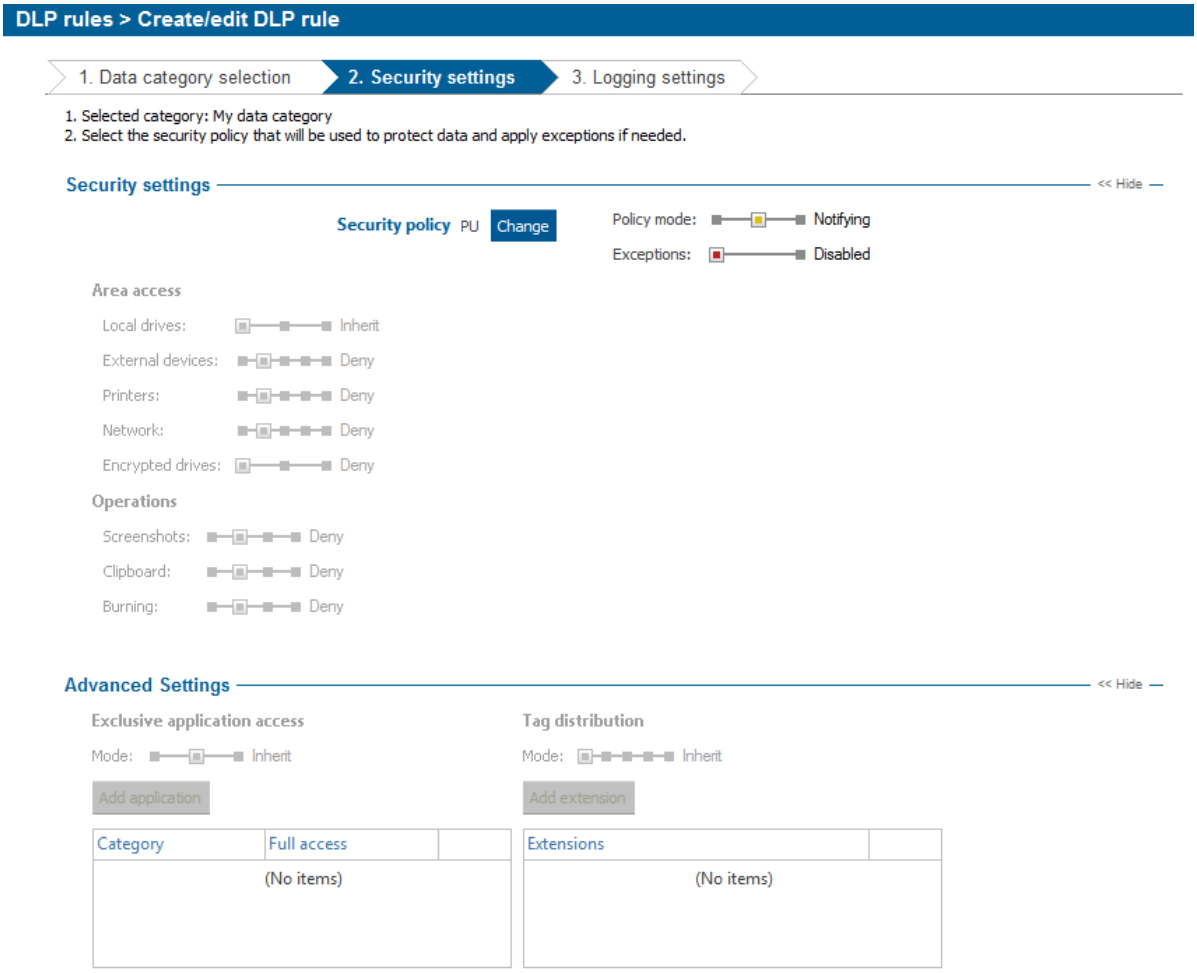
   b. *Notifying mode* – the security policy will not be strictly applied. This means that for operations and security policy areas set to Deny, operations or access to an area will still be allowed, but the user will be notified and a record will be made in the DLP protocol. This mode is intended for testing the security policy under real conditions. To ensure a seamless deployment without any disruption to work on user PCs, we recommend applying the security policy in this mode at first. If, after some time, the security policy settings prove to be the desired ones, you can switch to Restrictive mode and security will then be applied.

   c. *Testing* – almost same as Notifying policy with exception that user is not notified about DLP actions on endpoint PC. Only record will be made in the DLP protocol. This policy is designed for testing DLP rules setting.

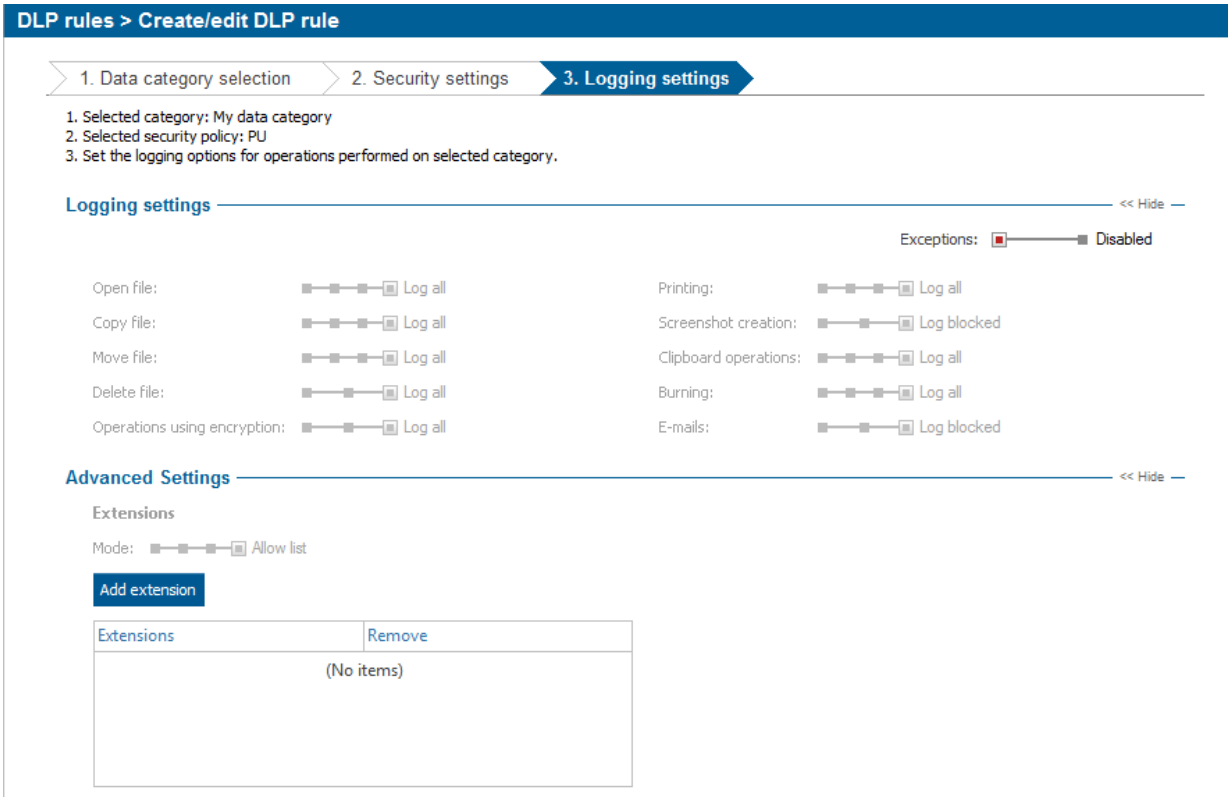
   The security policy in the DLP rule is set to *Notifying mode* by default.

   (Voluntary) After choosing a security policy and the mode, you can set exceptions in the security policy. Use the *Exceptions* slider for this. Exceptions are disabled in the security policy by default. Exceptions are applied only in the DLP rule created and will not change the security policy you have chosen and on which you will set exceptions. You can set exceptions for all security policy areas. For more on the various parts of security policies and their settings, see the section *Security policies*.

   To finish, click the *Next* button.



3. In the last step you will see the settings for how operations and actions are recorded in the security policy. If you want to change this setting you need to allow exceptions by using the slider on the right side of the view. Exceptions will only apply to the DLP rule you are creating and they will not apply to the security policy on which the DLP rule is based. Finally, click Finish and the DLP rule will be added to the list. To save and apply the DLP rule to selected groups, users or PCs, click  .



5.2.2.2 DLP protocol

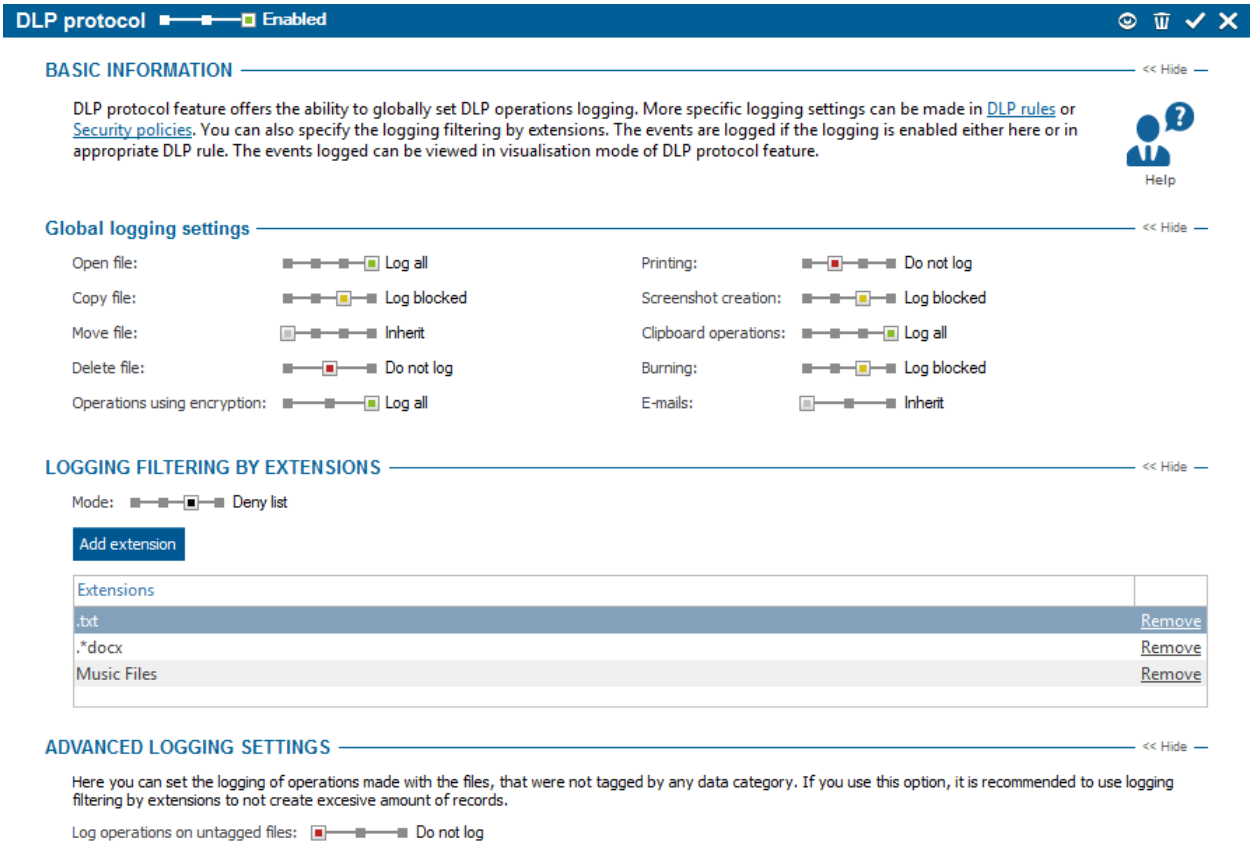
The DLP protocol function is intended for creating global settings of user activity monitoring. You can set in detail which operations shall be recorded and specify which file type shall be recorded based on extensions. The settings will be applied in DLP rules where they are not designated by Security policies.

DLP protocol can be found in the section *Safetica Management Console -> DLP -> DLP monitoring*.

View description

In the top part of the view you will find the main settings. Here you can specify how files shall be recorded for different operations involving files. Using the list of extensions, you can also filter only specific file types for which operations shall be recorded.

Advanced settings can be found in the bottom section. You can use them to allow or disallow the recording of non-tagged files – see Data categories and Data tagging administration.



Main settings

In the console setting mode you can switch this function on or off by using the slider bar in the view header.

- Disabled – the application of DLP protocol global settings is off.
- Inherit – nothing is set. Settings are inherited from the higher-level group.
- Enabled – this option will allow the DLP protocol global settings to be applied.

In the next part of the main settings you can specify which operations shall be recorded.

- Open file – a record is made when a file is opened.
- Copy file – a record is made when a file is copied.
- Move file – a record is made when a file is moved.
- Delete file – a record is made when a file is deleted on the client workstation.
- Encrypted file operations – a record is made when a file is encrypted by Safetica.
- Printing – a record is made when a file is printed.
- Screenshot creation– a record is made when a screenshot is taken.
- Clipboard operations – a record is made on every operation involving the clipboard.
- Burning – a record is made when a file is burnt on a CD or DVD.

Every operation has several recording modes:

- Do not log – the respective operation is not recorded.
- Log blocked – only respective blocked operations are recorded.
- Inherit – settings are inherited from the higher-level group. The behavior is the same as for

the Do not record mode unless set otherwise.

- Log all – all files are monitored.

You can set DLP monitoring only for users, groups or PCs tagged in the user tree. To apply the settings, you need to save the changes with the  button or you can cancel the changes with  in the top right part.

In the bottom part of the main settings you can use the Deny list or Allow list to specify which files shall be monitored. This is done by adding extensions to the list. For the Deny list, operations will be monitored on all files in the system except for those whose extensions are on the list. For the Allow list, only operations on files with extensions on the list will be monitored.

Advanced settings

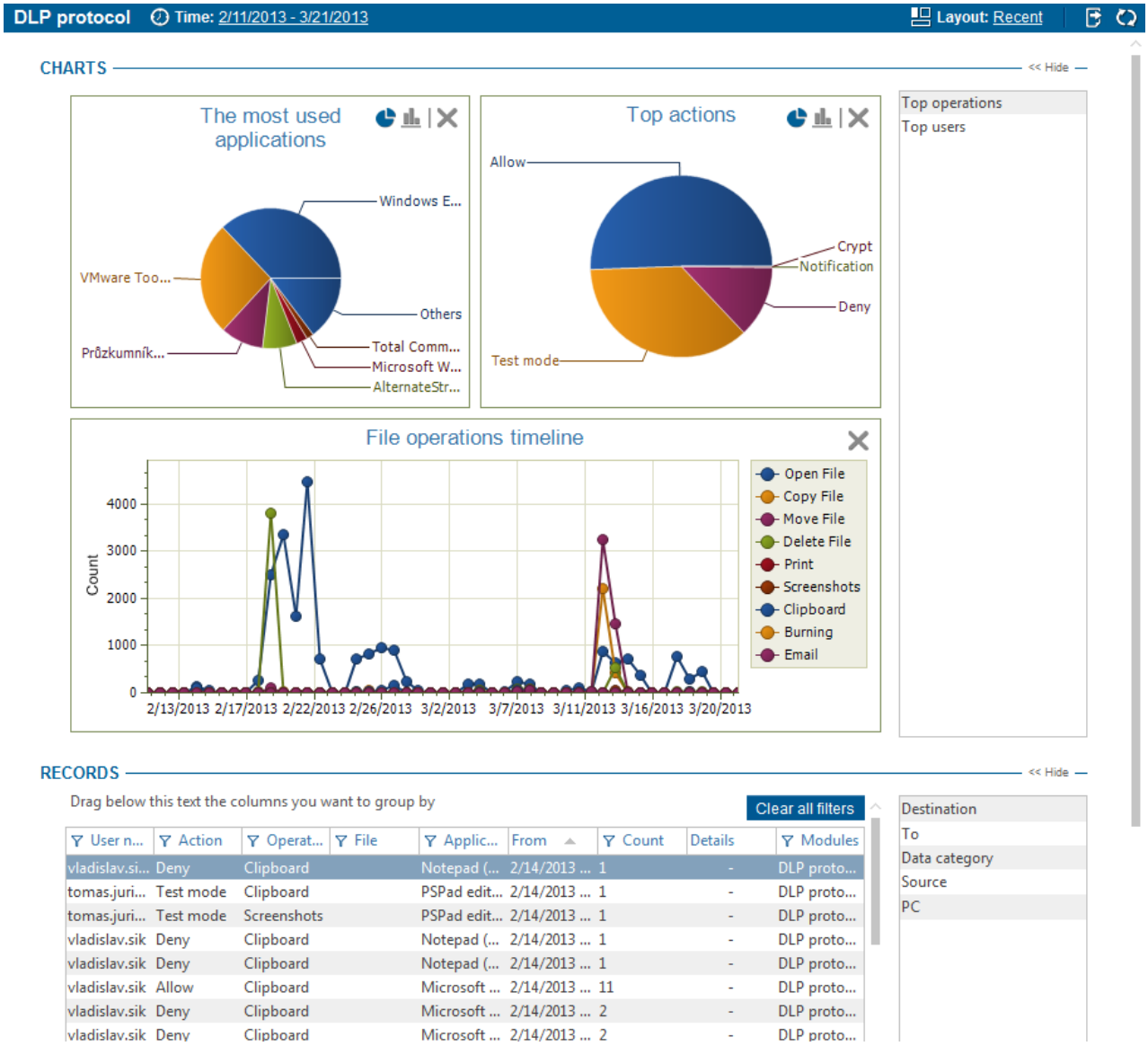
With the DLP monitoring function, file operations are recorded by default only for non-tagged files. You can use the slider bar in advanced settings to amend this and allow the monitoring of non-tagged files as well.

- Tagged files – these files have been tagged by any of the data categories through the Data marking administration function.
- Non-tagged files – any files that have not been tagged.

Visualization

The data you can see in the visualization will be displayed only for users, PCs and groups you have marked in the user tree. The visualization mode is divided into two sections.

The top section of the view offers space where charts are shown. You can find the charts available for the current function on the list in the right section. To display them, click and drag them over the chart. Charts are taken back to the list by clicking the button in the top right corner of each chart.



Charts available:

- *Top users* – this chart shows the users who work with files most of all.
- *Most used applications* – this chart shows the applications used most frequently for working with files.
- *Top operations* – this chart shows the most frequent operations involving files.
- *Top actions* – this chart shows the most frequent actions performed on file operations.
- *File operations* – this chart shows the number of file operations by type of operation.

In the bottom section you will find a table with detailed records. Every record contains several types of information presented in columns. The list of available columns is again shown to the right of the table. The column will appear in the table after clicking and dragging the column from the list onto the table. Click and drag the column header to change the column order in the table. In the same way, you can drag column headers onto the section above the table. Records in the table will then be pooled above the table based on the column type. You can remove a column from the table by dragging it back onto the column list on the right side.

Columns available:

- *From* – time when the record started.
- *To* – time when record ended.

- *PC* – name of the PC where the record was made.
- *User name* – name of the user under which a file operation was executed.
- *Application* – name of the application that executed the file operation.
- *Source* – name and path to the file involved in the operation.
- *Destination* – the path to the destination in copying or moving operations.
- *Source type* – whether the source path to the file is local, external or network-based.
- *Target type* – whether the target path is local, external or network-based.
- *Source device* – device name and SID.
- *Target device* – device name and SID.
- *File* – name of the file.
- *Operation* – type of file operation executed: *Open file, Copy file, Move file, Delete file, Print, Screenshots, Clipboard, Burning, E-mail, Write, Read, Create file.*
- *Action* – if the operation was allowed or blocked by Safetica.
- *Count* – count of identical operations that occur in the time interval specified by set time range. The number of these operations is based on the record aggregation level setting in *Safetica Management Console -> Management and settings -> Client settings*.
- *Data category* – data categories by which the file is tagged.
- *Modules* – name of the Safetica function that was used to take record: *DLP protocol, Disk guard* or *Device control*
- *Details*

You can filter the records as well. You can open the filter for any column by clicking at the header of the respective column. Enter text in the dialog or choose an item from the list based on which you wish to filter the column. Click + to add an item to the filter list. The length of this list is unlimited. After confirming the filter with OK, the table will feature only records corresponding to at least one filter listed.

Find more on the settings and visualization in the section Working with Setting and Visualization Modes.

5.2.2.3 Security policies

Security policies are intended to create named rules of DLP sets for working with data and applications on user PCs. You can apply the policies you have created in the DLP rules function where you can assign them to Data or Application categories and thus apply required restrictions. Security policies seek to allow centralized DLP setting administration over different categories for different groups, users and PCs.

Security policies are available via Safetica Management Console -> DLP -> Security policies.

View description

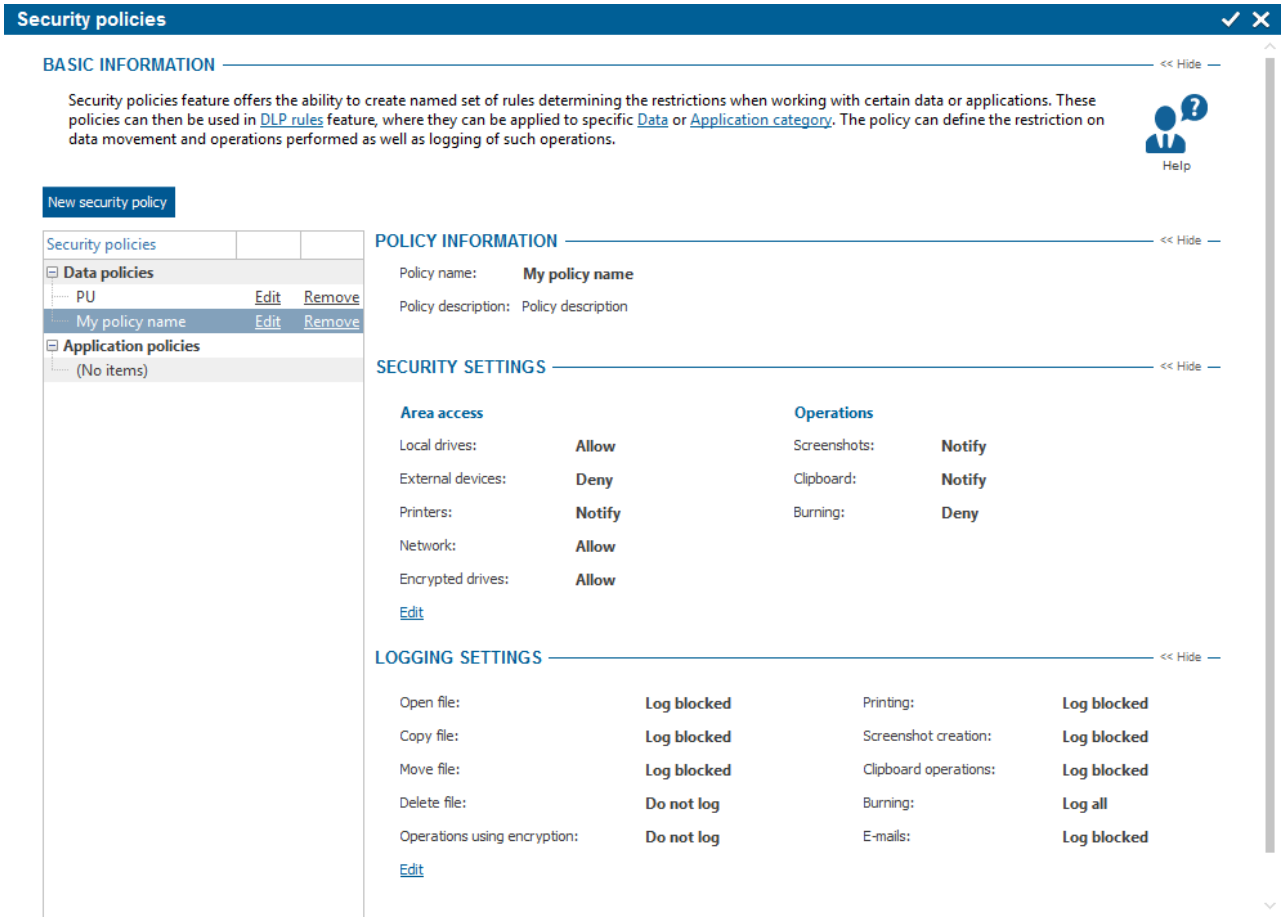
The left section of the view shows the list of security policies that have been created. You can choose from two types of security policies:

- Data policy
- Application policy

Click New security policy to launch the new security policy wizard. When created, it will be added to the list in the section on the left. To save a new security policy that you have created, click the button or cancel the changes with the button on the top right.

After tagging the desired policy in the list, detailed information on this policy will be displayed in the top right section of the view.

Click Edit in the respective section of a selected policy to modify the settings.



Security Policy

Security policies are rules by which data is protected. Two types of security policies are available. You can apply a policy either for data or an application involving working with data.

- *Data policy* – you can use data policies to prepare a set of restrictions for working with files, e.g. you can determine what storage sites are allowed where files can be moved and sent. You can then decide which applications will be able to access these files. A data policy can be assigned to any data category. Data tagged with such a category will be protected in accordance with the regulation of this policy.
- *Application policy* – you can use application policies to determine where applications may store their outputs, how they can work with data and what operations they are allowed to perform. Unlike data policies that can be assigned to data groups, application policies can be assigned to any application category. Working with files in applications subject to this application category is then secured based on the settings in the application policy assigned to it.

You can assign data and application policies to the respective data or application category with the DLP rule function.

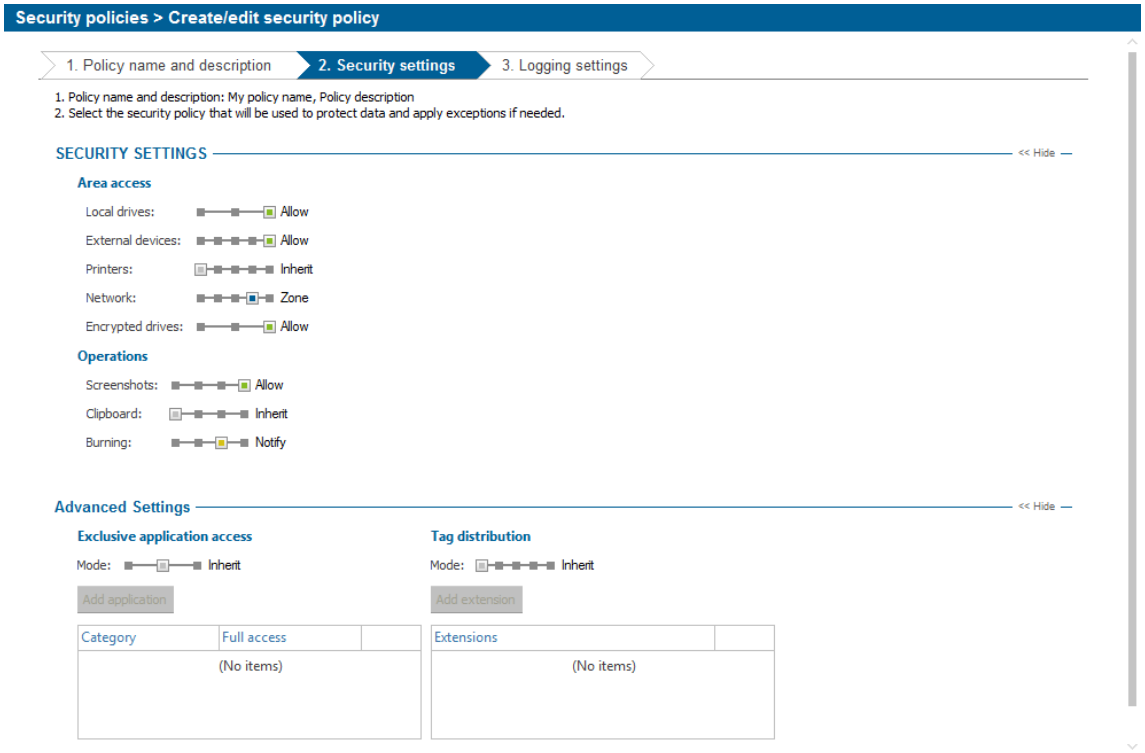
Every single security policy – data and application policies alike – comprises two parts:

1. Security settings

2. Logging settings

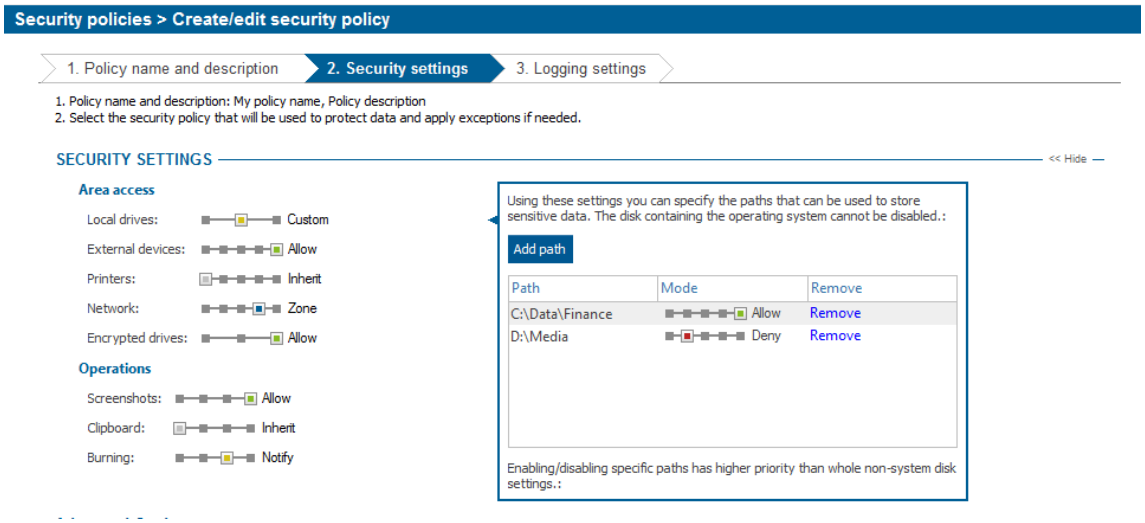
Security settings – data policy

In security settings for data policies you can set where files may be stored and where they can be moved.

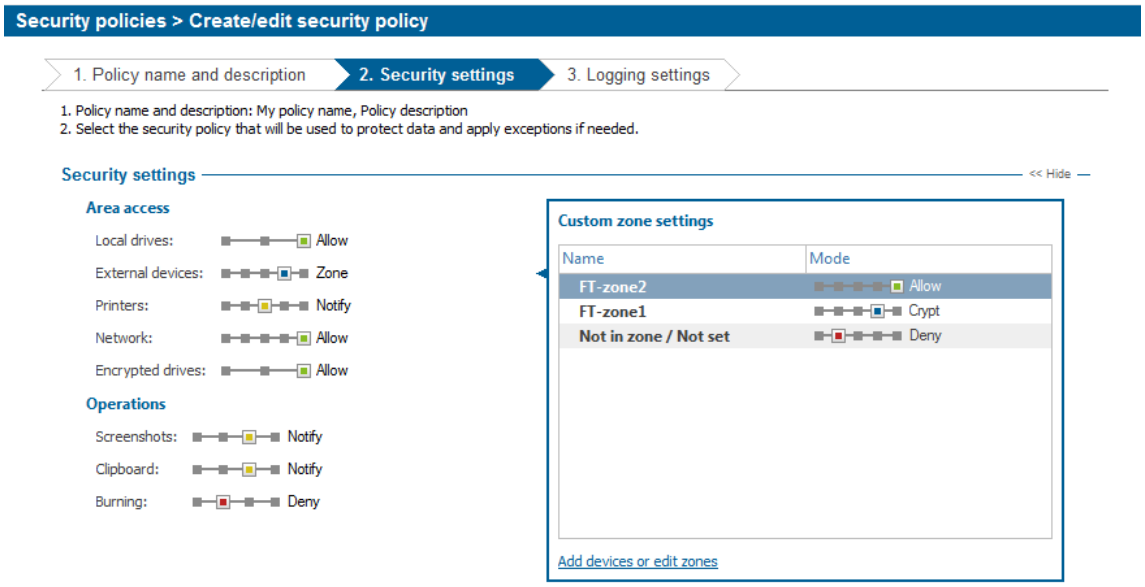


Setting an area access

- *Local drives* – here you set where files may be saved and copied in the file system on the user PC. In these settings, please note that certain applications, in order to run correctly, need to store temporary files and related files on the local disk. By applying too stringent settings, they may stop working. You can choose from the following options:
  - o *Allow* – files may be stored everywhere on the user PC.
  - o *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
  - o *Custom* – after choosing your own settings, you can specify the restrictions for disks and folders where files may be moved. Use the *Add path* button to add path to the list. You can use the scroll bar and specify the following for every independent path or disk:
    - *Deny* – files may not be saved or copied to the path.
    - *Crypt* – the file will be encrypted when copied or moved to this path. The user will be asked to enter a password. Then the files will be saved as an encrypted archive (.dcf). To unpack the archive, the user will need to enter the same password as used for creating the archive. For more on working with archives, see the section Archives.
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
    - *Notify* – when saving or copying a file to this path or disk, the user will see a notification in the dialog and a corresponding record will be made in the DLP protocol.
    - *Allow* – copying or saving to a path will be allowed.



- *External devices* – here you can set what external device files may be saved on or copied to. You can choose from the following options:
  - *Deny* – files may not be saved or copied to any external device.
  - *Notify* – when saving or copying a file to an external device, the user will see a notification in the dialog and a corresponding record will be made in the DLP protocol.
  - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
  - *Zone* – this options allows you to specify for every zone whether files may be saved or copied to an external device in the respective zone.
    - Deny – files may not be saved or copied to an external device being part of the zone.
    - *Encrypt* – when saving or copying files to an external device being part of the zone, the user will need to enter a password. After entering the password, the files will be saved on the external device as an encrypted archive (.dcf). To unpack the archive, the user will need to enter the same password as used for creating the archive. For more on working with archives, see the section Archives.
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
    - Notify – when saving or copying a file to an external device being part of the zone, the user will see a notification in the dialog and a corresponding record will be made in the DLP protocol.
    - *Allow* – copying or saving on external device being part of the zone is allowed.



o *Allow* – copying or saving on any external device will be allowed.

- *Printers* – the settings of the security policy for printers are analogous to those for external devices.
- *Network* – the settings of the security policy for network access are analogous to those for external devices.
- *Encrypted drives* – here you can allow or Deny access to disks encrypted by Safetica. You can also specify access to different types of encrypted disks: Local encrypted disks, Network encrypted disks and External encrypted disks. For more on encrypted disks, see the section Virtual and Physical disks.

Setting an operation

- *Screenshots* – here you can allow or deny the print screen function or similar screenshot functions for files.
- *Clipboard* – here you can allow or deny the use of the clipboard for files (Ctrl+C, Ctrl+V, Ctrl +X, etc.). If denied, the clipboard cannot be used on file contents. If denied, the Ctrl+C action can be used on the file in the file system but operation Ctrl+V operation will be denied if the file will be copied to restricted area or application.
- *Burning* – here you can allow or deny the writing of files on a medium.

Advanced settings

Exclusive application access

Through the Allow list or Deny list, you can specify for the application category what applications shall have access to the files to which the security policy applies. For the Allow list only applications in the application categories found on the list will have access to the files. For the Deny list only applications in the application categories not found on the list will have access to the files.

Click Add application category and a dialog will appear where you can choose the application category. After choosing a category, click OK and the application category will be added to the list, so you can set access to the data category in it.

Tag distribution

When you open a file tagged with a data category to which this security policy shall apply in any application, then any file saved from this application will be tagged with the same data category as the file opened in the application. You can set the extension of the tagging as follows:

- Deny – tag distribution is denied. The files saved from the application will not be tagged with any data category.
- Inherit – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
- Allow list – output files with an extension present on the list will be tagged with the data category of the file that is open. If you leave the list blank, no output file will be tagged.
- Deny list – output files with an extension not present on the list will be tagged with the data category of the file that is open. If you leave the list blank, all output files will be tagged.
- All files – all files to be saved from the application in the application category will be tagged with the data category.

Example: A data category Financial files has been created and several files are tagged. The data category has a security policy assigned in which tagging extension to the Allow list is set. The list shows only the .docx extension. When the user opens a file tagged with the “Financial data” data category in any application and saves a new file with the .docx extension from that application, then this new file will be tagged with the data category Financial data.

Logging settings – data policy

You can set in the data policy which file operations shall be recorded in the DLP protocol. You can record the following operations:

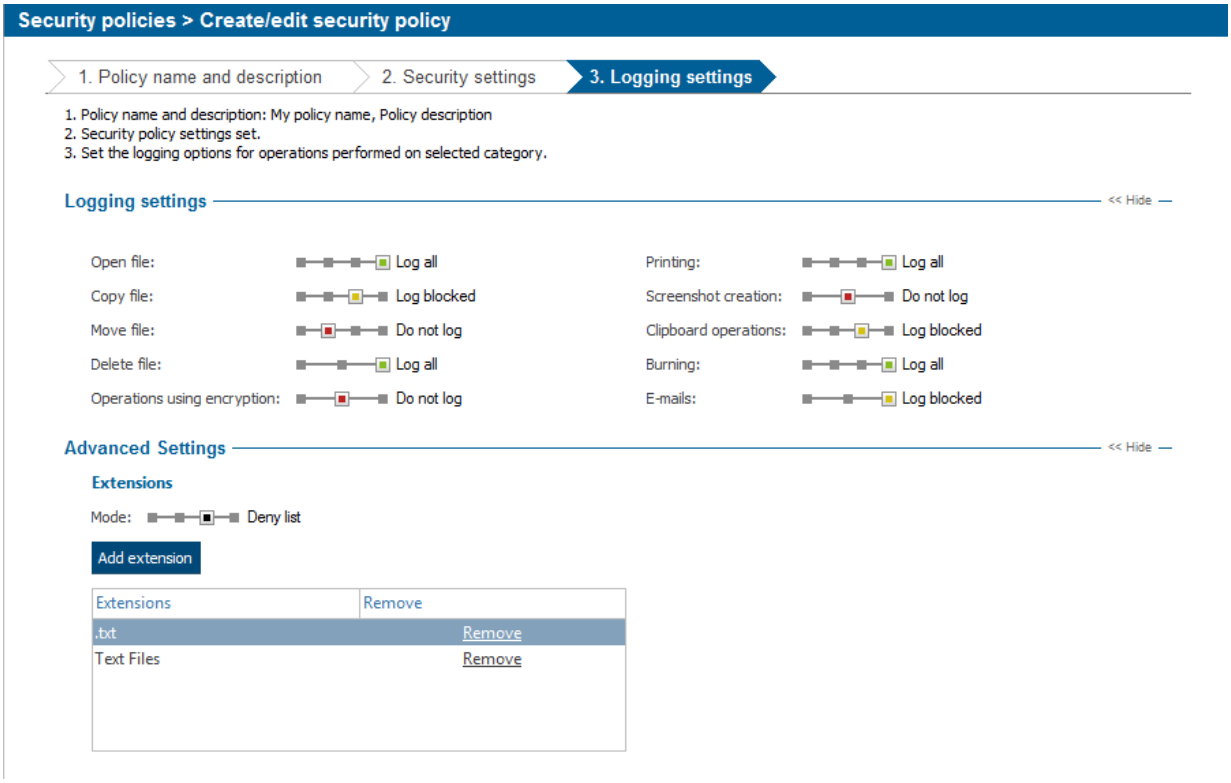
- *Open file* – a record is made when a file tagged with the data category is opened.
- *Copy file* – a record is made after a file tagged with the data category is copied.
- *Operations using encryption* – a record is made of operations in which a file is encrypted by Safetica.
- *Delete file* – a record is made when a file tagged with the data category is deleted on the client workstation.
- *Printing* – a record is made when a file tagged with the data category is printed.
- *Screenshot creation* – a record is created whenever a screenshot is made.
- *Clipboard operations* – a record is created whenever user uses clipboard for file operation.
- *Burning* – a record is made when a file tagged with the data category is written on a medium.

Operations have several recording modes:

- *Do not log* – the respective operation is not recorded.
- *Log blocked* – only blocked file operations are recorded.
- *Inherit* – settings are inherited from the higher-level group.
- *Log all* – allowed and blocked operations alike are recorded.

Note: The recording settings can be influenced by Global settings with the DLP protocol function where the recording of operations can be activated globally. In this case, operations are recorded if at least one of these settings allows recording. A simple rule is applied here: “recording” prevails over “not recording”. For example, when recording the Opening of a file:

- *Local* (in data policy) – Do no record.
- *Global* (in DLP protocol) – Record all.
- Resulting settings –> Record all.



Advanced settings

In Advanced settings you can use the Deny list or Allow list to determine which file types shall be recorded. You do this by adding extensions or their categories to the list. For the Deny list, operations will be recorded on all files in the system except for those whose extensions are on the list. For the Allow list, only operations on files with extensions on the list will be recorded.

Security settings – application policy

Security settings for the application policy are intended for deciding how users can work with applications. You can specify applications' access to paths and disks in the system and decide which operations shall be allowed or denied in these applications. The settings are analogous to the data policy settings.

Setting an area access

- *Local drives* – here you can set what parts of the file system applications will have access to on the user PC.
- *External devices* – here you can set what external devices applications will have access to.
- *Printers* – the settings of the security policy for printers are analogous to those for external devices.
- *Network* – the settings of the security policy for network access are analogous to those for external devices.
- *Encrypted drives* – here you can allow or deny access of applications to disks encrypted by Safetica. You can also specify access to different types of encrypted disks: Local encrypted disks, Network encrypted disks, External encrypted disks. For more on encrypted disks, see the section Virtual and Physical disks.

Setting an operation

- *Screenshots* – here you can allow or deny the use of the print screen function for applications.

- *Clipboard* – here you can allow or deny the use of the clipboard for applications (Ctrl+C, Ctrl +V, Ctrl+X, etc.).
- *Burning* – here you can allow or deny the writing of applications on a medium.

Advanced settings

Data access

Through the Allow list or Deny list, you can specify for the data categories to what data categories (files marked with a data category) the application category shall have access. For the Allow list the application category will have access only to the data categories found on the list. For the Deny list the application category will have access only to the data categories not found on the list.

You can use this option to specify what files, tagged with the data category, the applications to which this security policy applies can access.

Click Add data category and a dialog will appear where you can choose the data category. After choosing a category, click OK and the data category will be added to the list, so you can set what access applications from the application category will have to it – allow or deny.

Tag distribution

When you open a file, tagged with a data category, from the application category to which this security policy applies and create a new file in this application, then this file will be tagged with the same data category as the one used for tagging the file that is open. You can specify to what files the tagging shall be extended on application output in the following ways:

- *Deny* – tag distribution is denied. The files saved from the application will not be tagged with any data category.
- *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the higher-level group (if such a security policy exists).
- *Allow list* – new files with an extension present on the list will be tagged with the data category of the file that is open. If you leave the list blank, no output file will be tagged.
- *Deny list* – new files with an extension not present on the list will be tagged with the data category of the file that is open. If you leave the list blank, all output files will be tagged.
- *All files* – all files to be saved from the application in the application category will be tagged with the data category.

Example: There is a security policy in which tagging extension is set to the Deny list assigned to the Picture eImage editors application category. The list shows only one .jpeg extension. When you open a file tagged with any data category in a picture eImage ditor and subsequently save a new file from it with any extension but .jpeg, then this new file will be tagged with the data category Financial data.

Default tags

Default tags

In this section you can specify what data category the files saved from applications in the application category subject to the security policy shall be marked with. Files saved from the application will be automatically marked with data categories found on the list.

Extensions

You can use the affixes in the *Allow* list or Deny list to specify what files shall be marked with the data category on the output. For the Allow list only files with their affix found on the list will be marked. For the Deny list only files with their affix not found on the list will be marked.

Recording settings – application policy

In the application policy you can set which application operations shall be recorded in the DLP protocol. You can record the following operations:

- *Open file* – a record is made when an application file is opened.
- *Copy file* – a record is made when a file is copied.
- *Operations using encryption* – a record is made of operations in which a file is encrypted on application output by Safetica.
- *Delete file* – a record is made when an application from the application category deletes a file on the client workstation.
- *Printing* – a record is made when a file from the application in the application category is printed.
- *Screenshot creation* – a record is made whenever a screenshot is made and the application from the application category is in the foreground
- *Clipboard operations* – a record is made for a clipboard operation in the application.
- *Burning* – a record is made when an application file from the application category is written on a medium.

Every operation has several recording modes:

- *Do not log* – the respective operation is not recorded.
- *Log blocked* – only blocked file operations are recorded.
- *Inherit* – settings are inherited from the higher-level group.
- *Log all* – only files are recorded.

Note: If nothing is set in this section, recording will proceed based on global settings in the DLP protocol. If there is a difference between local and global settings in the DLP protocol, the settings with the allowed recording option is applied. For example, when setting the recording of the Opening of a file:

- Local (in data policy) – Do no record.
- Global (in DLP protocol) – Record all.
- Resulting settings –> Record all.

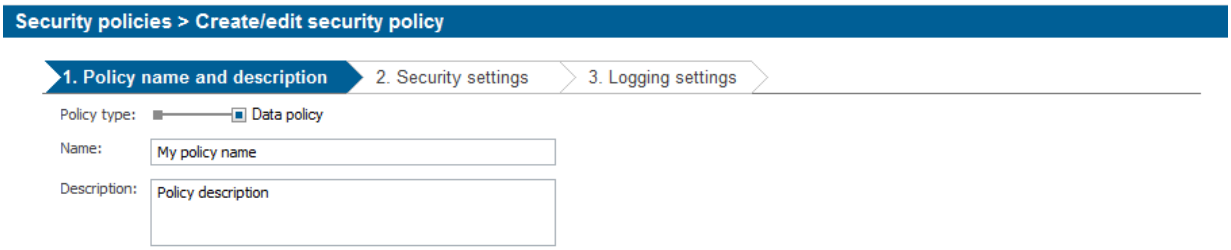
Advanced settings

In Advanced settings you can use the Deny list or Allow list to determine which file types shall be recorded. You can do this by adding extensions or their categories to the list. For the Deny list, operations will be recorded on all files in the system except for those whose extensions are on the list. For the Allow list, only operations on files with extensions on the list will be recorded.

Creating a security policy

If you wish to create a new security policy, click New security policy.

1. In the first step specify the name, description and type of the new security policy using the slider:
    - Data policy
    - Application policy



When finished, click *Next*.

2. In the second step use the slider and list of basic and/or advanced security settings for the security policy you are creating. When finished, click Next.
3. In the second step use the slider and list of basic and/or advanced security settings for the recording of files subject to the security policy. Finally, click Finish. The security policy will be added to the respective list of policies. To save the policy, click  .

5.2.2.4 Zones

Zones can be used for creating named sets of external devices, printers, IP addresses, network paths and e-mails which we can link to as separate entities. You can then use them in security policies, DLP rules and Device control. Zones can be arranged in a tree structure.

Zones are available via Safetica Management Console -> DLP/Administration and settings -> Zones.

View description

The upper left section of the view shows the list of zones that have been created. After marking a zone in the list on the left, detailed information on the zone will be displayed on the left: zone name, and description.

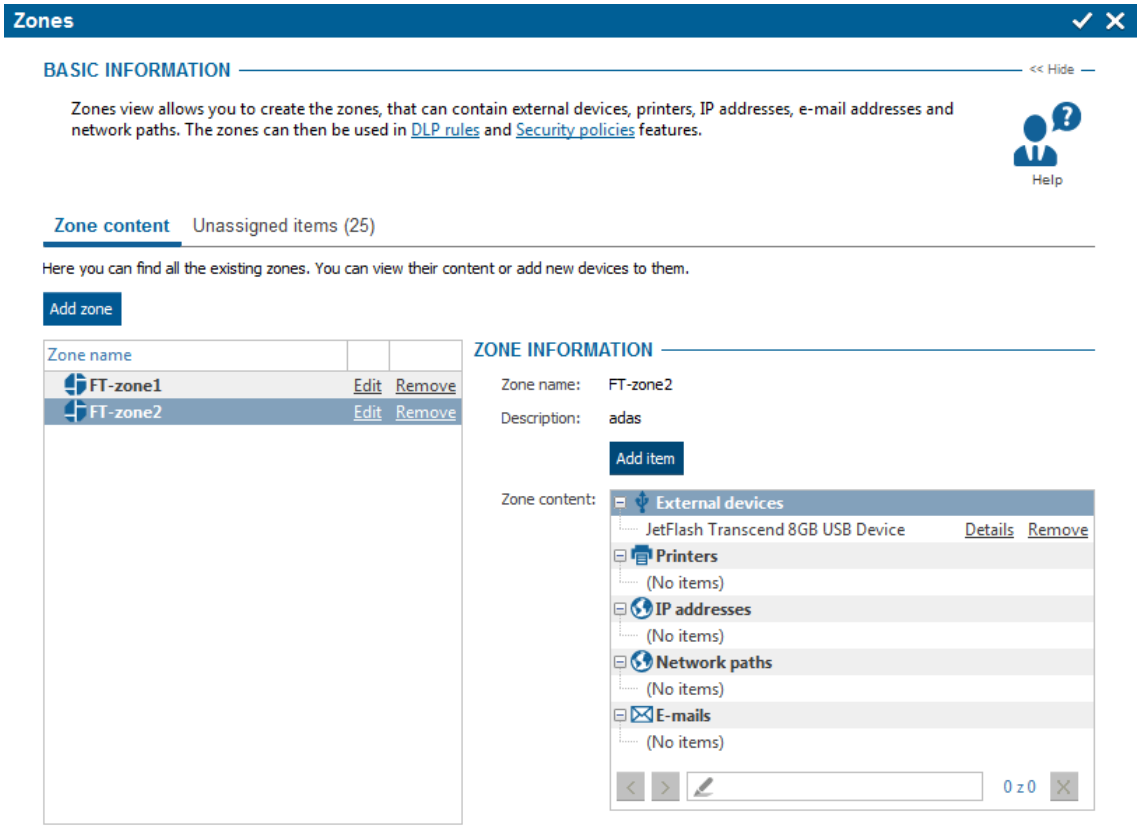
The content of the zone can be found in the bottom left of the view.

Click *Add zone* to open the new zone dialog, enter a name and description for it and specify whether it shall have a parent zone or not. A parent zone is one which had been marked in the list on the left when creating a new zone.

Click *Add item* in zone content and the new item wizard will open to add a new item to a zone.

By clicking *Edit* with the respective zone in the list on the left, you can change its name and description.

The Unassigned items section on the right contains a list of available external devices and printers found on workstations with SEC. These devices and printers have not yet been assigned to any zone. By moving them to the zone content list on the left, you can assign them to the zone marked on the left.



Creating a new zone and adding items

To create a new zone, you first need to decide whether the new zone shall be on the top level or whether it shall have a parent zone. Parent zones cover all zones below them.

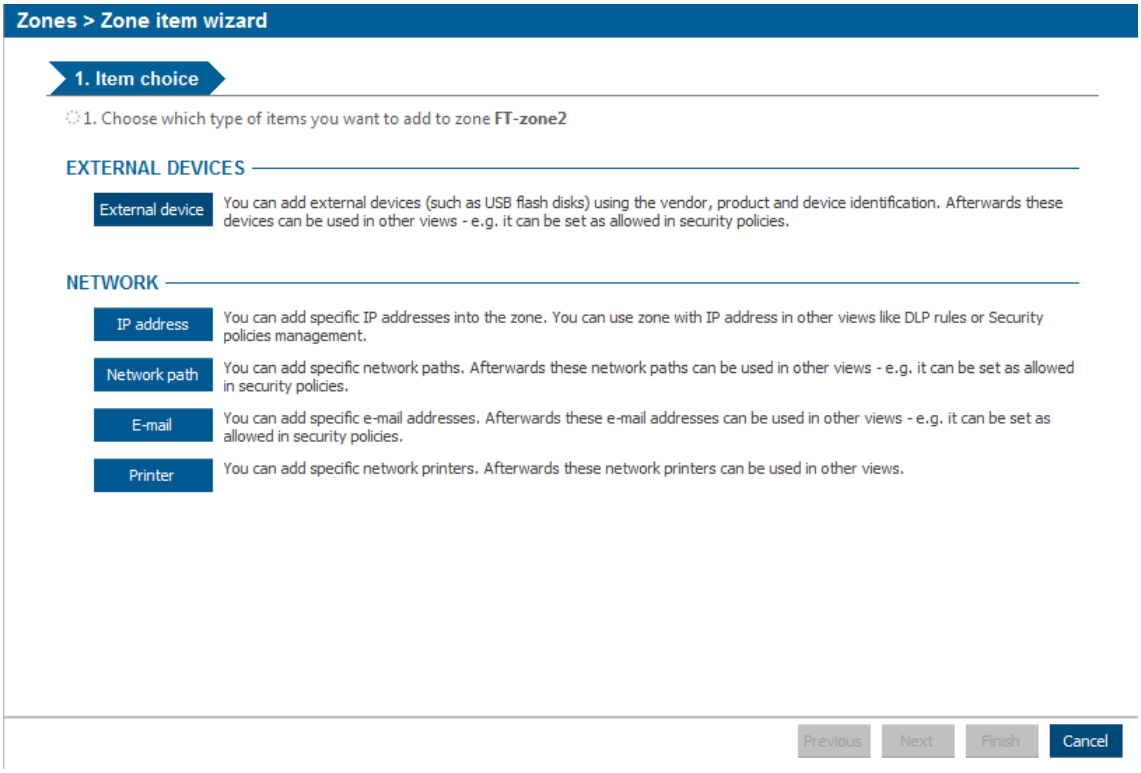
- Top level zone – click Add zone. In the dialog enter the name and description, and set the parent zone slider to None. Confirm what you have input with OK and the zone will be added to the list.
- Zone with parent zone – go to the zone list and mark the zone that you wish to act as the parent zone for the zone being created. Click Add zone. In the dialog enter a name and description for it, and set the Parent zone slider to the name of the parent zone. Confirm what you have input with OK and the zone will be added to the list.

  Note: You can move zones within the tree structure by dragging them using the mouse.

To edit the zone content, proceed as follows:

1. In the zone list on the left, mark the zone whose content you wish to edit. The zone's current content will be displayed in the left bottom. Click the Remove link with the respective zone item and the item will be removed. To add a new item to the zone, click Add item.
2. The wizard lets you choose from among the following items which the zone can contain:
   - *External devices*
   - *Printers*
   - *IP addresses*
   - *Network paths*
   - *E-mails*

Click the item you wish to add. The corresponding view for adding the item will open.

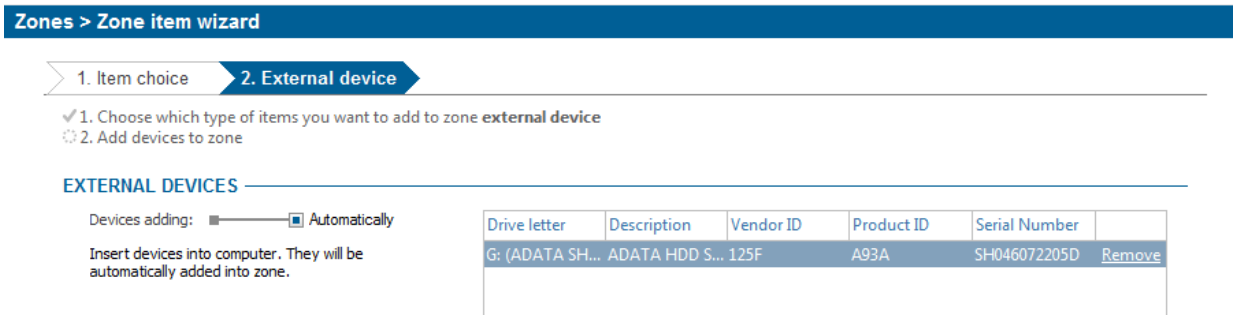


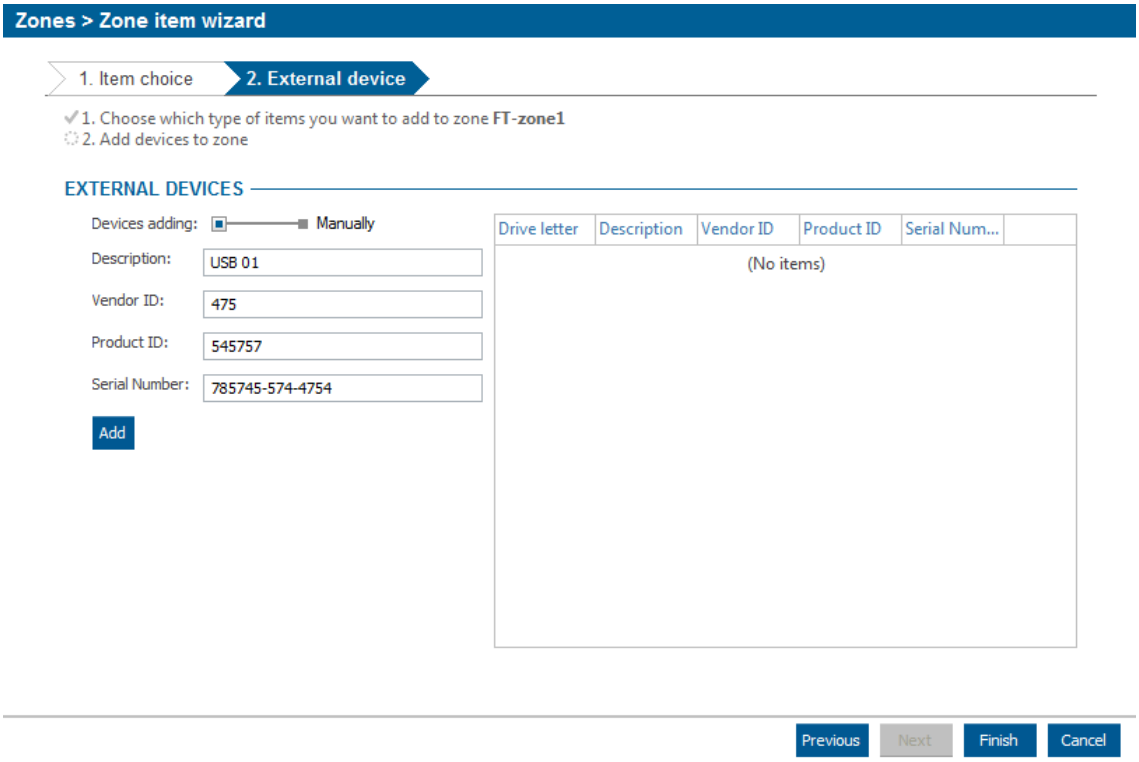
Adding an external device

There are two options for adding an external device to the zone. Choose one of the following options with the slider:

- *Automatically* – in automatic mode it is enough to connect the external storage device to the PC where SMC is running. When connected, the device will be added to the list.
- *Manually* – in this mode you must enter the data on the device in the text fields first, so that the device can be clearly identified. This includes the Vendor ID, Product ID and serial number. You can obtain this information from the device packaging or from the manufacturer. Click Add and the device will be added to the list.

You can add several external devices to the list.



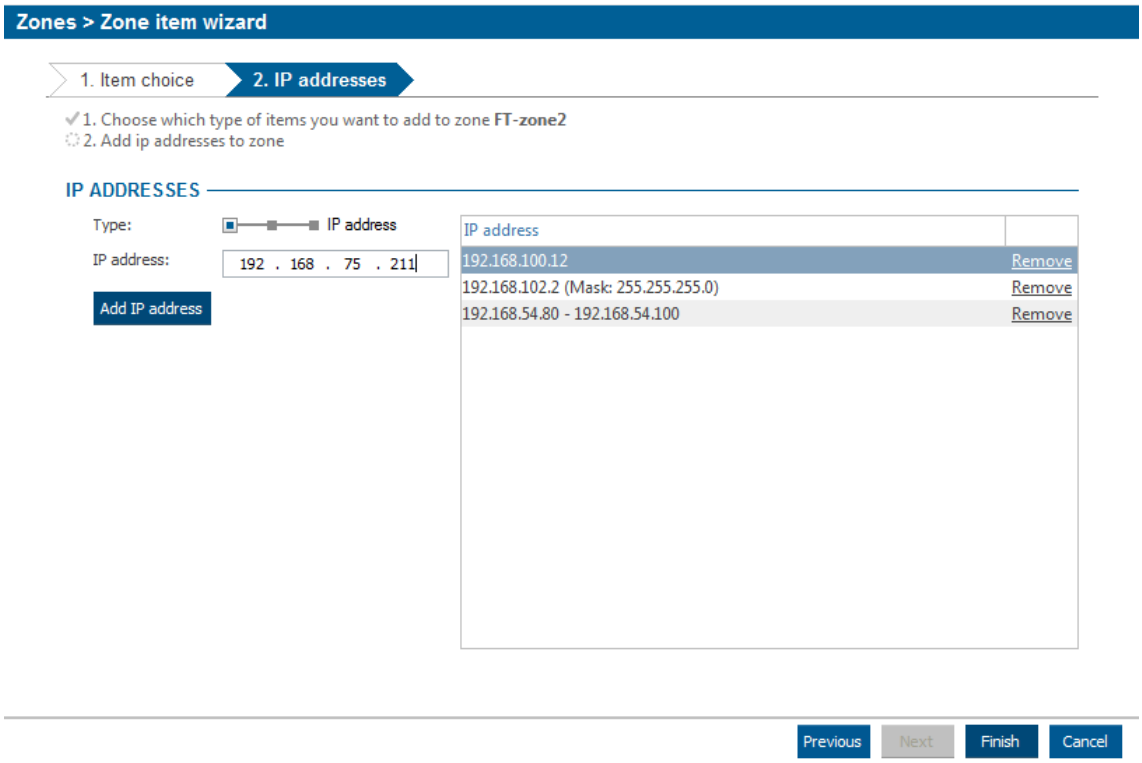


Adding an IP address

You can add an IP address to the zone in three ways. Choose one of the following options with the slider:

- *IP address* – enter the IP address in the respective field and click Add to add the IP address to the list on the right.
- *IP address with mask* – enter the IP address in the respective field with the network mask and click Add to add the IP address to the list on the right.
- *IP range* – enter the start and end address of the range in the respective box and click Add to add the range to the list on the right. All addresses within this range, including the start and end addresses you have entered, will now belong to the zone.

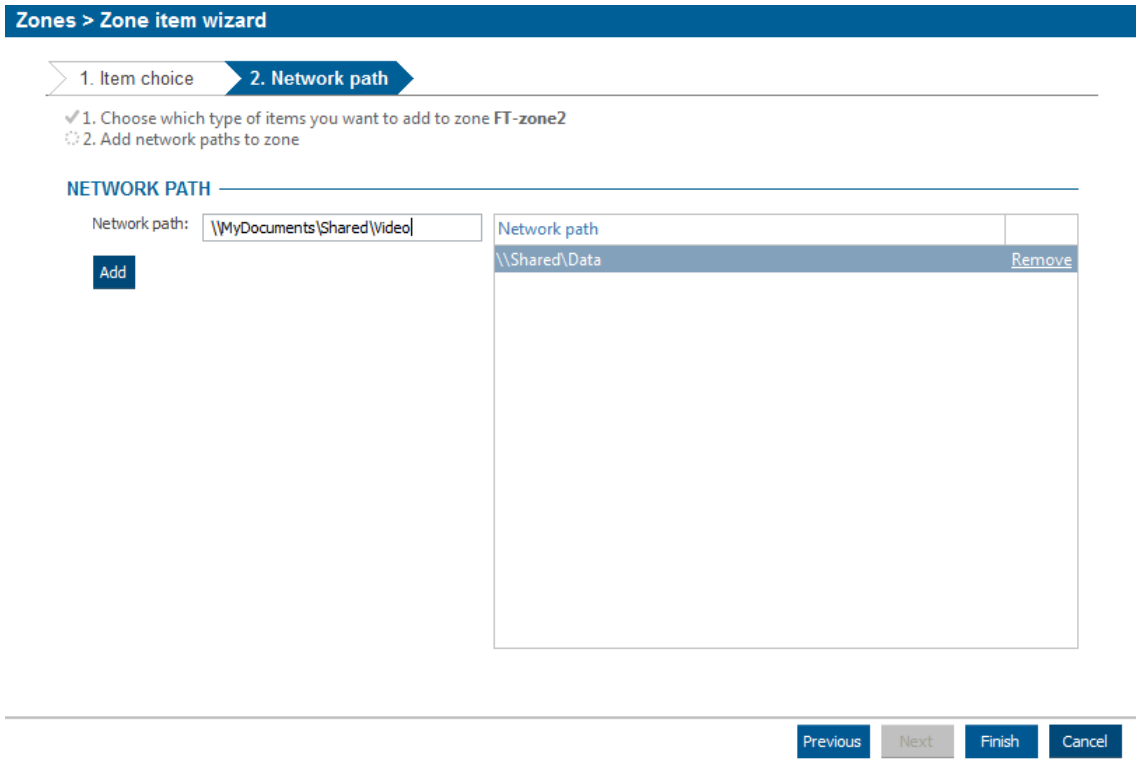
You can add several addresses to the list.



Adding a network path

Enter the path in the network format (e.g. \\Data\Finance) in the text field and click Add to add the path to the list on the right.

You can add several network paths to the list.

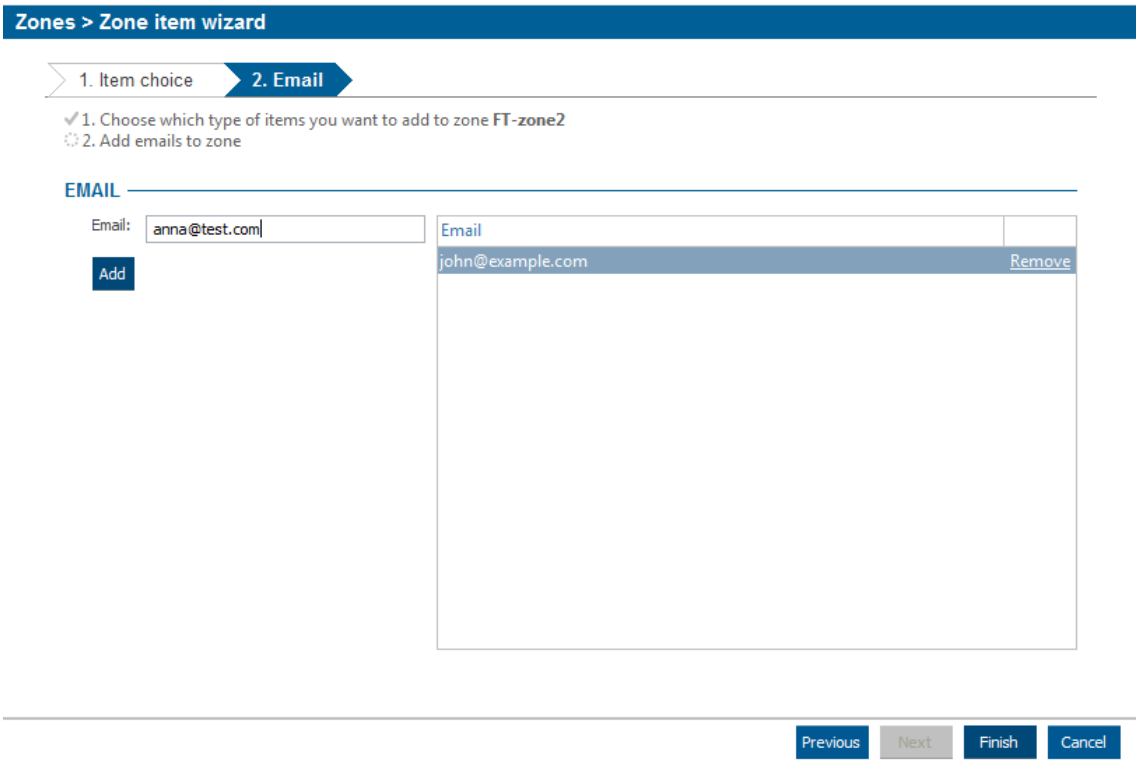


Adding an e-mail

Enter the e-mail address in the text field and click Add to add the address to the list on the right. You can add addresses in two ways: the conventional way (e.g. name@domain.com) or by domains (e.g. @domain.com applies to the e-mail addresses anna@domain.com, thomas@domain.com, etc.) where all e-mail addresses in the e-mail domain entered will be added to the

zone.

You can add multiple e-mail addresses to the list.

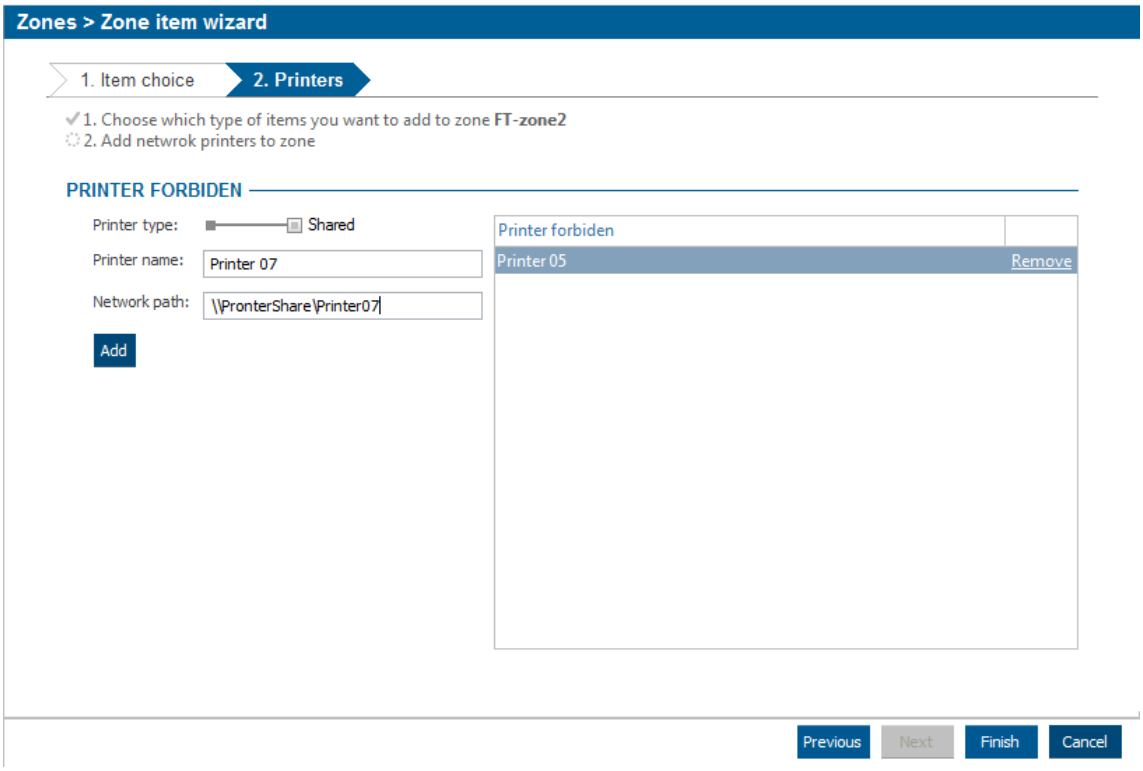


Adding a printer

You can add two printer types to the zone. Use the slider to choose the printer type you wish to add.

- *TCP/IP (network printer)* – this printer is connected directly to the network. Enter the printer name and printer IP address in the respective fields. Then, use the slider to select the type of the printer protocol (Raw, LPR) and – depending on the protocol type – enter the port number andof queue name. By clicking Add, the printer will be added to the list on the right.
- *Shared printer* – this printer is shared across the network. Enter the printer name and path to the printer in the respective fields (e.g. \\Server\SharingName). By clicking Add, the printer will be added to the list on the right.

You can add several printers to the list.



3. Finally, click Finish and the respective item will be added to the zone. To confirm the changes, click the  button on the top right.

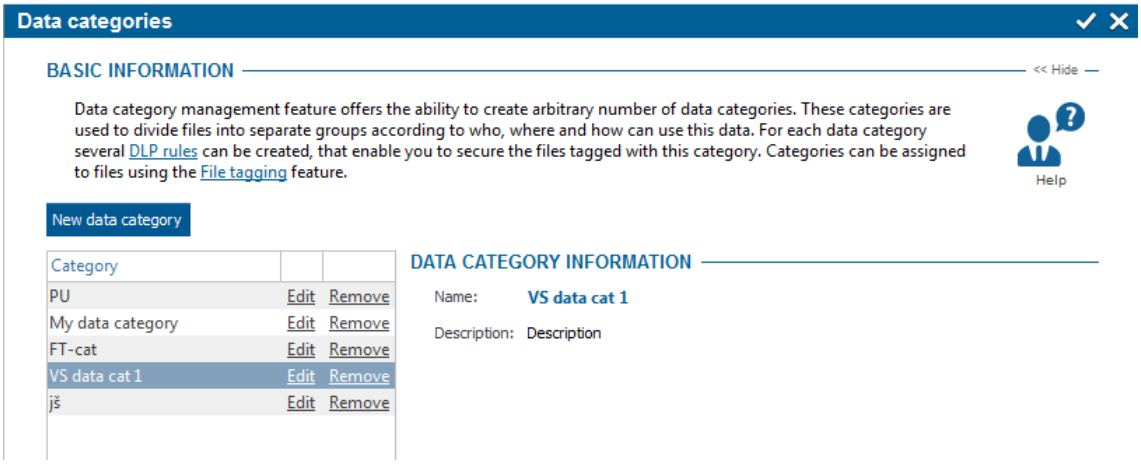
5.2.2.5 Data categories

In the Data categories view you can create an unlimited number of data categories. Data categories are used for splitting files into different groups depending on who can work with the files. Subsequently, different DLP rules – intended for securing the data category of tagged files – can be applied for every data category. In File tagging you can then assign these categories to different files. This is what we call “data tagging”.

Data categories are available via *Safetica Management Console -> DLP -> Data categories*.

View description

The left section of the view shows the list of data categories. After selecting the categories on the list, the name and description of the data category will be displayed on the right.



Creating a new data category

If you wish to create a new data category, click New data category. Enter a name and description and by clicking OK the category will be added to the list shown on the left. To save a new category,

click or cancel the changes you have made with on the top right.

Editing a data category

You can edit the name and description of an existing data category by clicking the Edit button on the list with each data category.

5.2.2.6 Disk guard

Disk guard allows you to set access rights for the users, computers or groups to access a system and network paths or system disks through a simple set of rules. For example, you can choose drives the users can access or only use for reading, or select specific paths or folders.

Disk guard is under *DLP -> Disk guard*

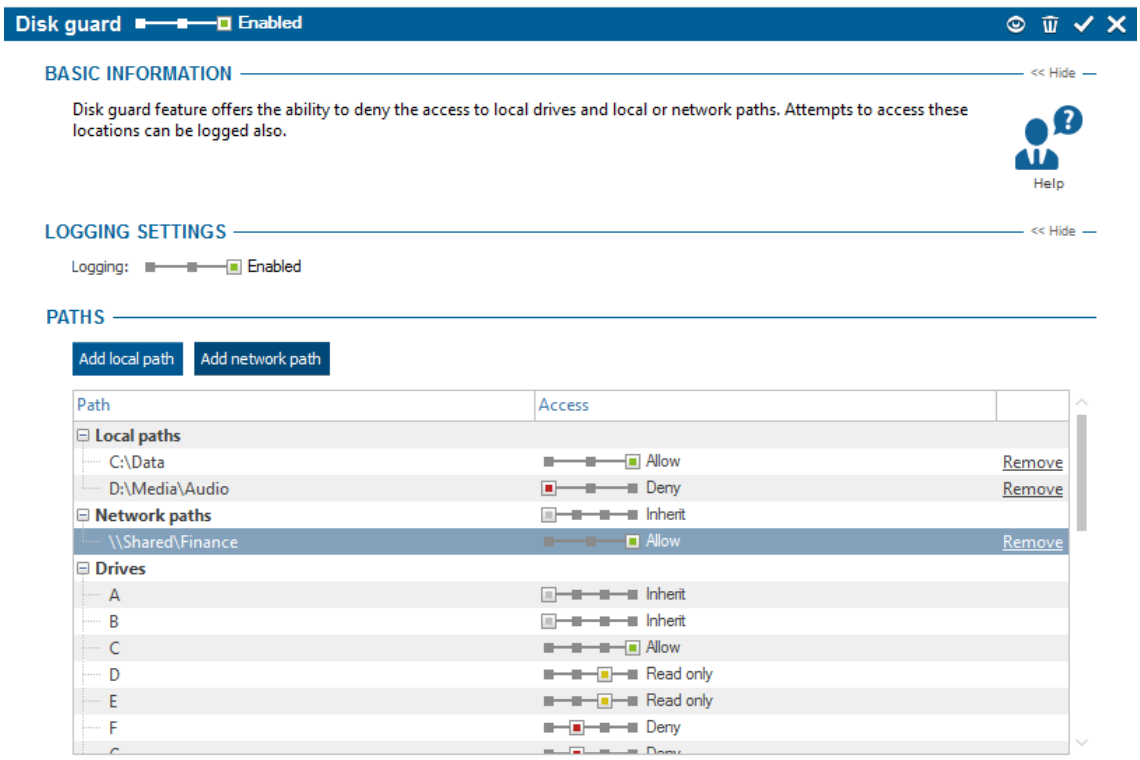
Main settings

In the SMC settings mode this feature can be enabled or disabled using the slider in the header of this view.

- Disabled – function is not activated.
- Inherit – function mode is not set. Settings are inherited from the parent group.
- Enabled – function is activated.

Using the *Logging* slider you can enable logging of access actions. You can view a record about these actions in visualization mode.

Disk guard is set only for users, computers, groups or SMS you have highlighted in the user tree. In order to apply settings, you have to save the changes using the button or you can cancel the changes you have made using the button in the upper right corner.



Path rules

You can specify access rights for three types of paths:

- *Local paths* – path to folders on an end station (e.g. D:\Folder\name).
- *Network paths* – path to folders shared over the network. You must enter the path in the network format (e.g. //Shared/Folder)
- *Drives* – there is a list of letters which identifies drives. You can set access rights for each drive there.

The following types of access settings are available:

- *Inherit* – function is not set. Settings are inherited from the higher-level group.
- *Deny* – users have no access to disks or paths.
- *Read only* – a user can only view or read content on this disk or path. This means they cannot save anything to these path or disk.
- *Allow* – this disk or path can be accessed by a user in any way.

You can add a local path by clicking on the *Add local path* button.

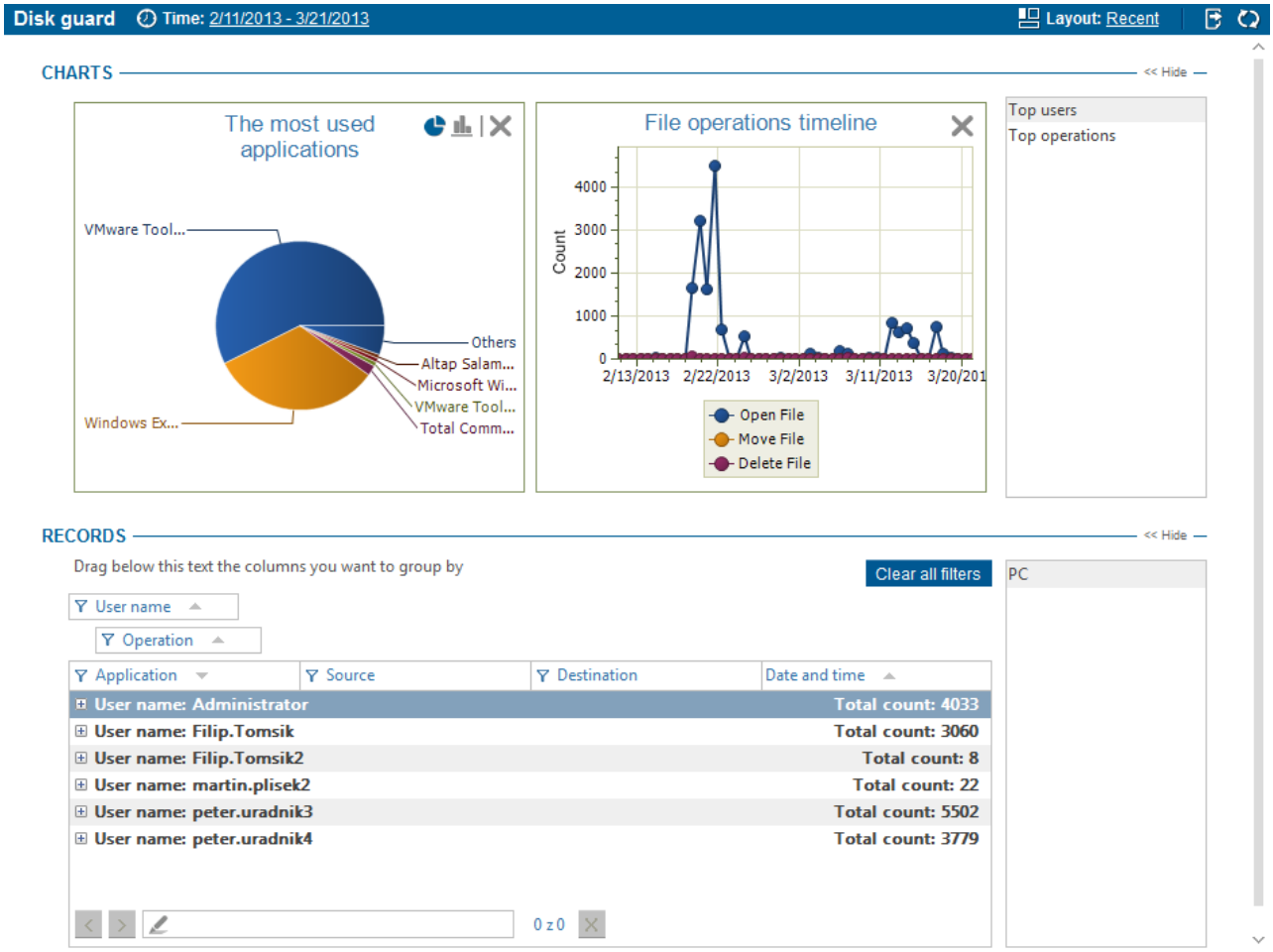
You can add a network path by clicking on the *Add network path* button.

You can set access rights to specific drives identified by letters after expanding the Drives section.

Note: If you enter the system disk letter as a parameter, operating system features on a client station might be blocked.

Visualization

There are records about access to paths and drives defined in settings mode. The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the  button in the top right corner of each chart.



Available charts:

- *Top users* – a chart containing the users who have the most records (up to 7 users are shown).
- *The most used applications* – a chart with the applications that the users most frequently use to work with files (up to 7 applications are shown).
- *Top operations* – a chart with the most frequent file operations.
- *File operations timeline* – a chart containing a count of file operations in time.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was made.
- *Application* – name of the application which used the access path or disk.
- *Source* – the name and path of the file operated on.
- *Destination* – the target path in copying and moving operations.

- *Operation* – the type of the access operation that was performed: *Open File, Delete File, Move File, Write, Read*.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.2.2.7 Device control

Safetica controls the access that peripheral devices connected to the PC have to the system, and disables them if appropriate. This helps to protect against users installing unwanted applications and viruses on company computers as well as preventing them from taking sensitive company information on unauthorized media. For example, you can disable all USB devices and progressively allow particular devices for particular employees.

Device control for USB devices is based on *Zones*. Before you start setting access to USB devices, you must create a zone and insert USB devices there.

For devices connected via USB and Bluetooth interfaces, DLP provides the ability to set more detailed access rights using several parameters.

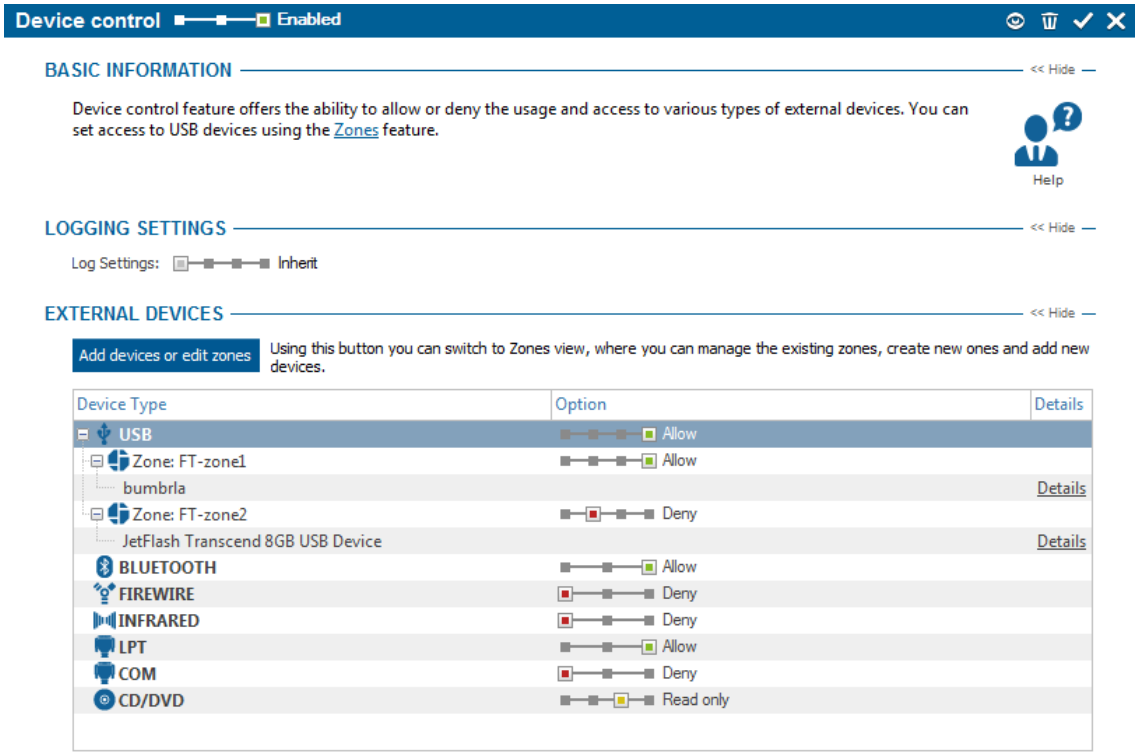
Main setting

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

You can edit zones by clicking on the *Edit zones* button.

Device control is only set for users, groups, computers or branches you have highlighted in the user tree. To apply the settings you have to save the changes using or you can cancel the changes you have made by in the upper right corner.



Logging settings

Additional settings provide tools for monitoring and alerts.

- *Log settings* – Serves as a parameter for creating information for the detailed overview.
  - *Inherit* – settings are inherited from the parent group.
  - *Do not log* – No information about connected devices at the client station is logged in the detailed overview.
  - *Log blocked* – Information about devices that are blocked due to set rules is logged in the detailed overview.
  - *Log all* – Information about blocked and enabled peripheral devices connected to the client station is logged in the detailed overview.
- *Advanced monitoring* – when choosing this option, also other types of devices of types other than "USB Mass Storage" will be recorded.

Overview of devices and configuration options

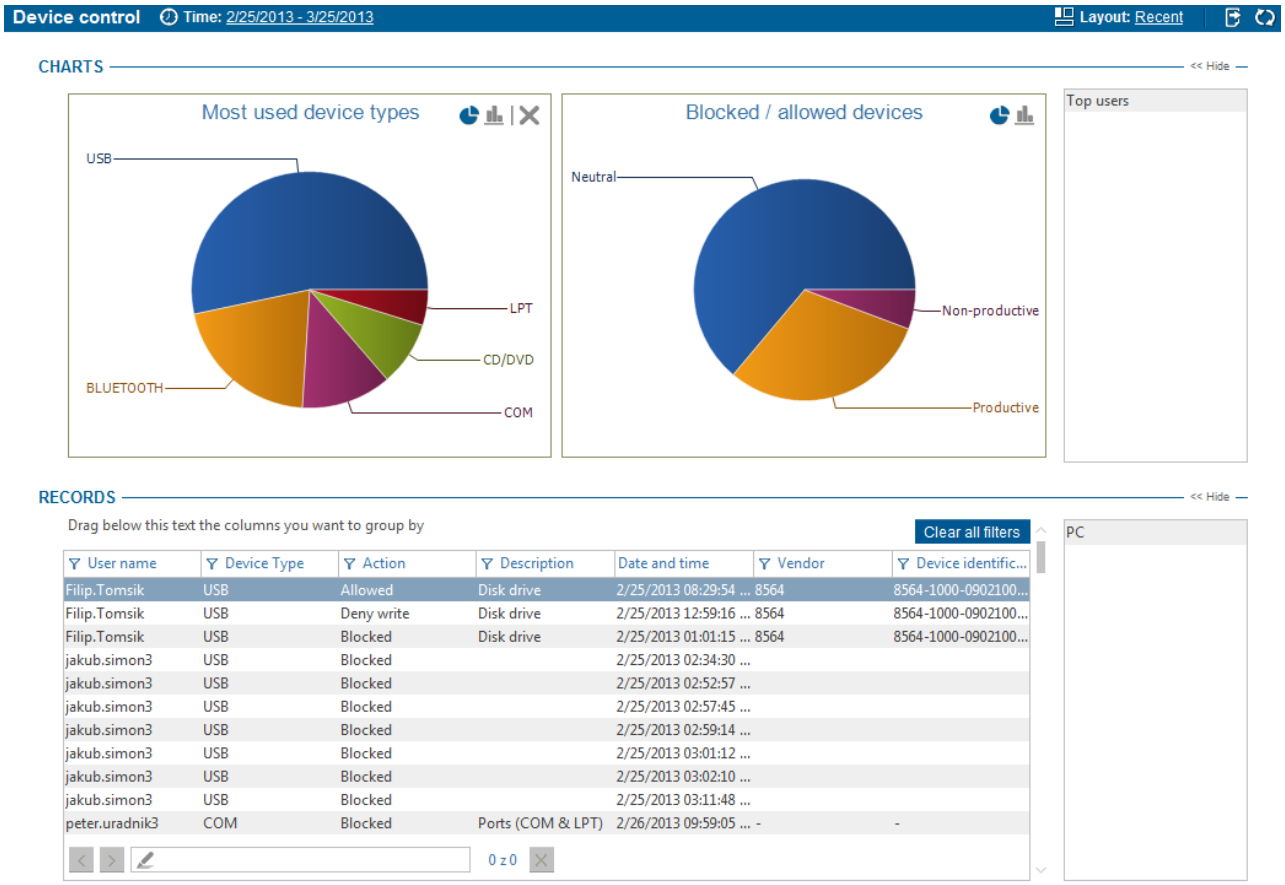
You can specify access to several types of devices:

- *USB* – you can specify user access to USB devices using Zones, so you must create a zone first and insert USB devices into the zone. To add new USB devices to a zone or create a new zone, click on Add devices or edit zones button. You can set the following options for each zone or USB device:
  - *Inherit* – option is not set. Settings are inherited from the parent group
  - *Deny* – access to the USB device is denied.
  - *Read only* – USB device is connected in read-only mode. A user cannot write to the USB device.
  - *Allow* – access to the USB device is allowed without restriction.
- *Bluetooth, FireWire, Infrared , COM, LPT, CD/DVD, Generic* – for these devices you can set

the same options as for USB.

Visualization

There are records about access to devices defined in settings mode. The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each chart.



Available charts:

- *Blocked/Allow devices* – a chart containing blocked and allowed devices.
- *Type of devices* – a chart containing the number of records divided by device type.
- *Top users* – a chart containing the users who have the most records (up to 7 users are shown).

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.

- *User Name* – the name of the user under whom the record was made.
- *Device type*
- *Description* – detailed description of device.
- *Action* – if the device was Allowed, Blocked, set as Read-only, Disconnected.
- *Drive* – to what unit (drive letter) the device is mapped.
- *Device identification* – ID numbers which identify the device: <Vendor ID>-<Product ID>-<Serial number>.
- *Vendor* – name of the device vendor including vendor ID.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.2.3 Endpoint Security Tools

What good are top security systems when employees use easy passwords or even note them down on a piece of paper? Teach them to observe correct security habits. Make work easier for your IT support staff in fixing forgotten passwords every day.

Provide for your employees to safely and irrevocably delete any unnecessary data and lock their computers when leaving for lunch. This way you will prevent casual bystanders from using company computers and accessing sensitive company data.

Even your employees will be able to use the Endpoint Security Tools features. Endpoint Security Tools can run in the following modes depending on the setting:

1. *User interface* with security tools and a context menu available by right-clicking on the icon (available only with a valid DLP license)
2. *Hidden mode* with basic user actions available only from the contextual menu without a user interface (available only with a valid DLP license).
3. *Invisible mode* without Endpoint Security Tools and a contextual menu. Only Safetica Client Service runs on the client station and the functions of Endpoint Security Tools will not be available.

If you allow your employees to use Endpoint Security Tools in any of the modes mentioned above, it will empower them to cooperate in maintaining the highest level of security in your company. It is the interest of employees to keep the company healthy and protect it from leaks of sensitive data.

Endpoint Security Tools form a part of the DLP module.

Main benefits

- Eliminate the use of passwords endangering your company security
- Reduce the stress on your IT support staff who have had to deal with endless tickets for forgotten passwords.
- Deleted data will remain unreadable forever.
- Guard information from spyware.

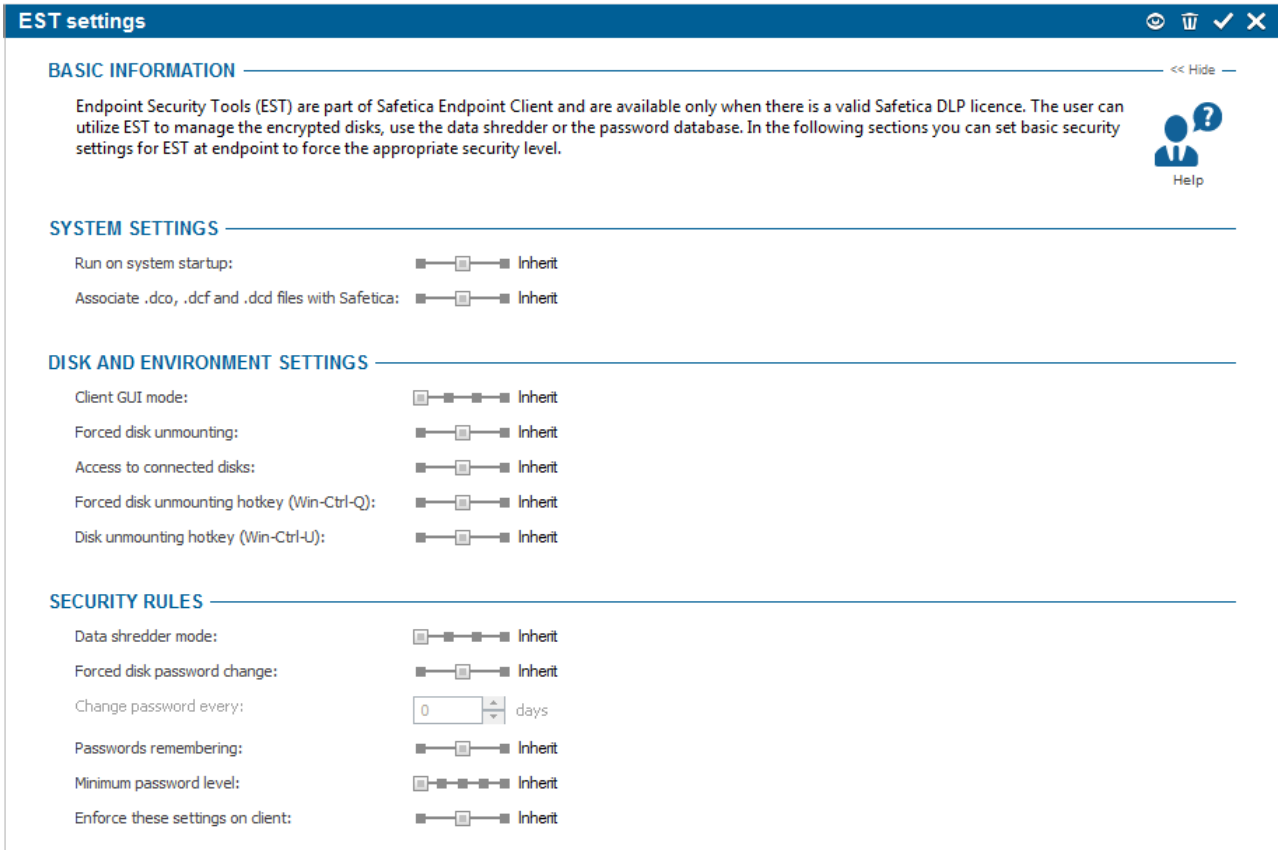
- Users forgetting passwords will not cost you any important data.
- Protect workstations when employees are absent from their desks.

5.2.3.1 Endpoint Security Tools settings

Here you can customize a large part of Endpoint Security Tools in the main settings.

You can find the Endpoint Security Tools main settings in *DLP -> EST settings.*

The settings will apply only to users, computers or whole groups you have highlighted in the user tree.



System settings

- *Run on system startup* – if you enable this option, Endpoint Security Tools GUI is automatically started when the operating system starts up. This option does not affect the client service startup, as this is always started.
- *Associate .dco, .dcf and .dcd files with Safetica* – files with Safetica software extensions can be opened outside the Windows Explorer if this option is enabled.

Disk and environment settings

- *Client GUI mode* – Endpoint Security Tools can work in three modes defining which features of Endpoint Security Tools will be available to users.
  - *Invisible* – there is no Endpoint Security Tools graphic interface on the client. Only a service connecting to the administrator console and enforcing modules' (Auditor, DLP, Supervisor) security settings is running. Endpoint Security Tools are therefore not available to the user.
  - *Tray only* – in the notification area (tray) you can find the icon, which enable managing (connecting, disconnecting, creating) disks over the contextual menu. The main Endpoint Security Tools user interface is not available to the user. They can only use

features for managing encrypted data.

  - *Normal* – in this mode, the entire graphic interface is visible including the contextual menu and icon in the main panel. It allows users to fully use Endpoint Security Tools options and features. Users can therefore create encrypted disks and files using the archive manager or create and manage password databases, etc.

- *Forced disk unmounting* – this option allows users to "force" disconnection of a disk, which means disconnecting a disk even if the system is working with it. We strongly recommend against this option, as it can cause damage or loss of data in encrypted disks.
- *Access to connected disks* – there are two modes how the encrypted disk could be accessed.
  - *For user only* – only the user who connected an encrypted disk will have access to it.
  - *For whole computer* – an encrypted disk connected by any user will be accessible to all users who can connect to the computer. This option is important for computers where multiple users can be logged on.
- *Forced disk unmounting hotkey (Win-Ctrl-Q)* – if you enable this option, you will allow users will be allowed to use the hotkey Win-Ctrl-Q to "force" disconnect all encrypted disks.
- *Disk unmounting hotkey (Win-Ctrl-U)* – if you enable this option, users will be allowed to disconnect all disks in a standard way by pressing the key combination *Win-Ctrl-U*.

Security rules

- *Number of rewrites used by data shredder* – within this setting you define how many cycles discarded data will be overwritten in. Multiple overwrites is better for security, but shredding takes much longer. Sufficient security is ensured with 7 overwriting cycles.
- *Force disk password change* – if you enable this option, you can set an interval after which changing the password of encrypted disks will be enforced. When the number of days you enter have passed, the user will be prompted to change the password when connecting the disk.
- *Password remembering* – by enabling this option, you will allow Endpoint Security Tools to remember entered passwords. Users will be able to tick the "Remember password" option, allowing them to connect further disks without entering a password. However, this option is not recommended for security reasons.
- *Minimum password level* – using this option you can choose a security level for the passwords in use. You can select from Weak, Middle, Good and Strong. These options define the minimum length of password and the kind of characters the password must contain. We recommend setting the minimum security level to Good.
- *Enforce these settings on client* – if you enable this option, all settings in this view will be enforced. This means it will not be possible for users to change these settings locally from Endpoint Security Tools settings on the client station. If it is disabled, users can change the settings locally from Endpoint Security Tools on the client station.

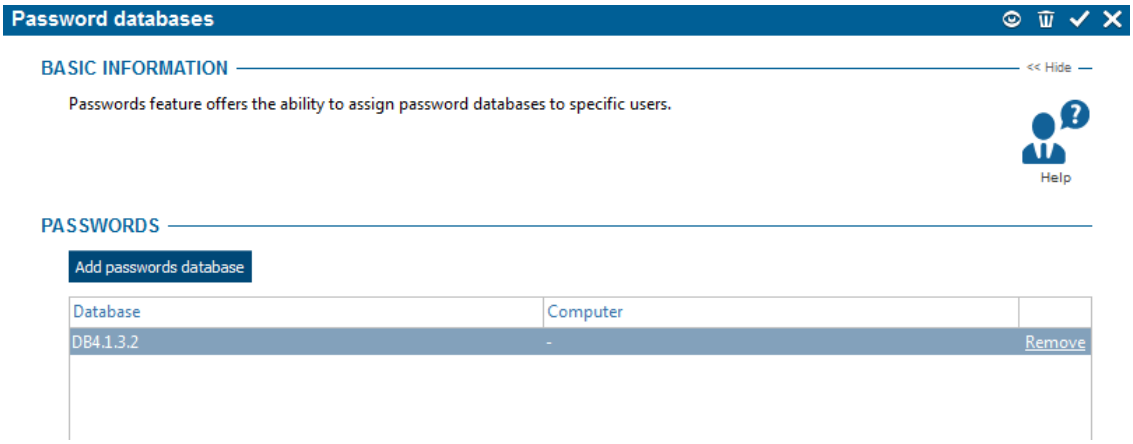
5.2.3.2 Password databases

Do your employees use many passwords daily? And do they remember all of them or do they simplify them and write them on pieces of paper and attach them to the monitor? Such behavior endangers a company's internal security. An unauthorized employee or a thief can enter highly protected systems and sensitive company data thanks to the information they find.

The Safetica Tools package offers your employees a safe file for safekeeping of passwords, logon data and other confidential information. A single password or security key suffices for access to all of them, but the whole database remains unreadable without this password or key.

You can create a password database using Endpoint Security Tools.

In the section *DLP* -> *Password databases* these databases can be monitored, assigned or removed. Above is a list of password databases assigned to users, computers or groups marked in the user tree, bellowbelow is a button for adding a database.



Assigning a password database

1. To add a new password database to the list on the server click on the Add button under the list of the password database on the server.
2. In the file open dialog, choose a password database that has been created (password database files have the extension .dcd). Highlight the selected database and after confirming the selection, the new database will be added to the list of databases.

You assign password databases only to users, groups, computers or branches 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.

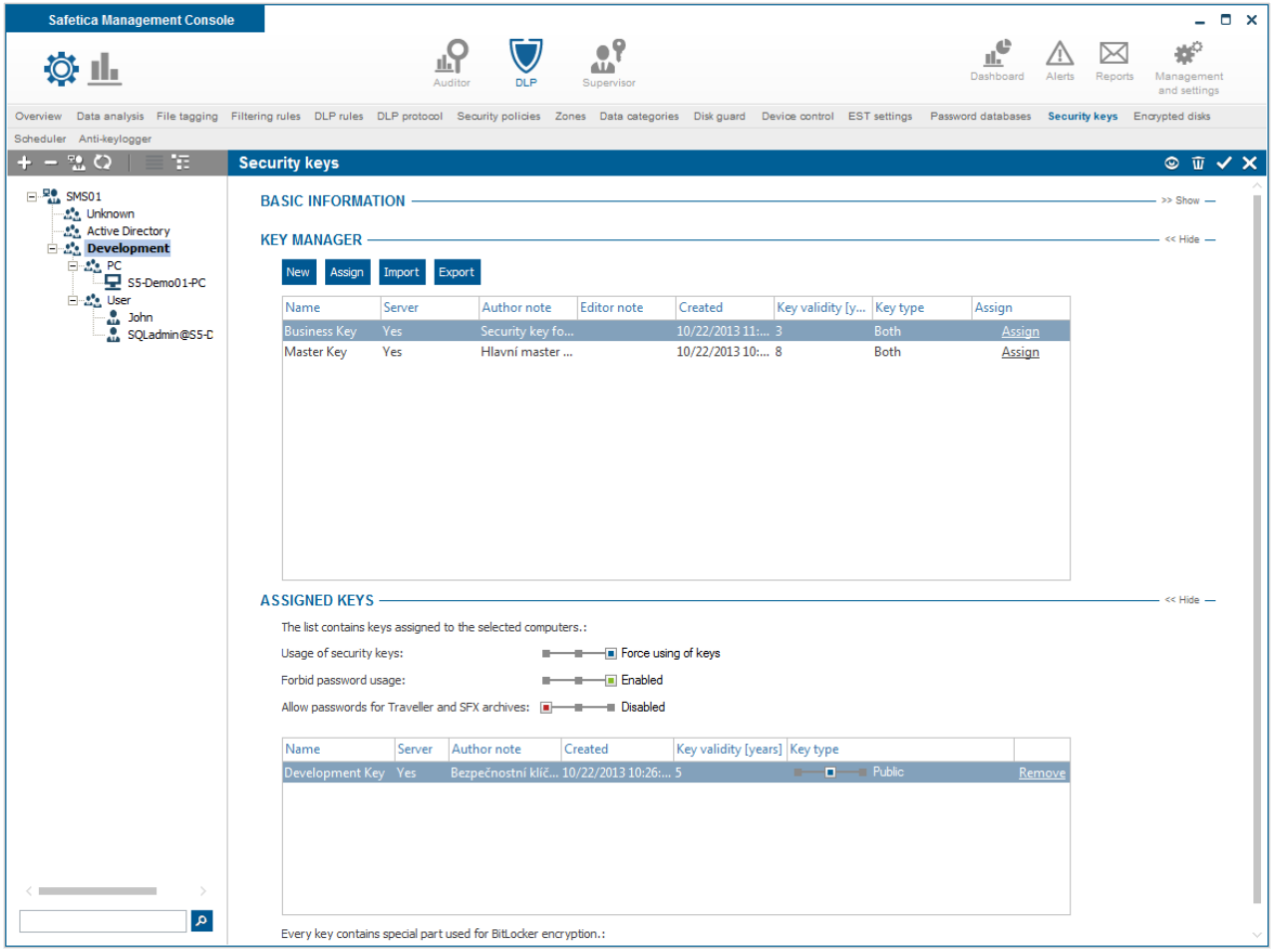
Removing a database

To remove a password database from a client, click on the button next to the appropriate database in the list.

5.2.3.3 Security keys

Besides an access password, access to an encrypted drive is protected also by a so-called security key. The security key is something like a master key to all rooms in a hotel, the only difference being that the security key is merely a data file. It can unlock encrypted drives for which this functionality is active. Security keys can be used primarily when you have forgotten the password. As with any important key, this security key must be stored in a safe place, such as burned to a CD and stored in a safe.

Remember that the security key is the only option for accessing your data if you have forgotten the password to your drives!



Every Safetica security key consists of two sub-keys and a special section for *Bitlocker*:

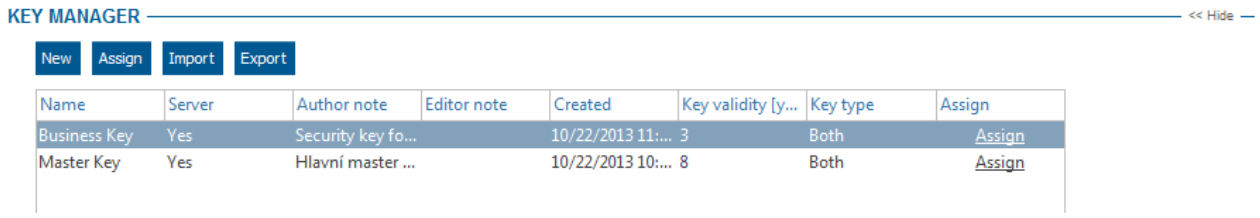
- *Public key (.pubkey)* – used only for data encryption. To access encrypted data, a corresponding Private key must be used. The key must not be used for unlocking encrypted data. It can be freely distributed to other users.
- *Private key (.privkey)* – used only to unlock encrypted data (drives, files, folders, etc.) encrypted by a corresponding public key. It cannot be used for data encryption. The key must be stored in a safe place.

  Example: A public key – something like a lock – is used for data encryption (e.g. on the drive). To unencrypt (unlock) a drive encrypted this way, you can only use the corresponding key which unlocks the drive's lock, the private key. There is only one public key corresponding to every private key and vice versa.
- *Bitlocker key section* – this is a special section of the key used for encryption and unlocking of drives encrypted by Bitlocker. Find out more on using this key in the Bitlocker encryption section.

Security keys are assigned only to users, groups, PCs and subsidiaries that you have marked in the user tree. To apply the settings, you need to save the changes with the button or you can cancel the changes with at the top right.

Key management

The table lists available security keys you can assign to users, PCs or groups.



Use the buttons above the table to perform the following operations:

- *New* – opens a new security key creation wizard to guide you through the entire process step by step. In the first step the wizard will ask you to do something unconventional. A blank rectangle will be displayed in the middle of the dialog in which you must randomly move the mouse cursor. The wizard will obtain random data in this way, so that it can generate a high-quality key. As soon as a sufficient amount of random data has been collected, the wizard will immediately begin generating a key. This operation can take several minutes depending on the speed of your PC. When the key has been generated, the wizard will ask you to enter detailed information on the key. You need to enter a name for the key, target folder, validity period and general description.
- *Assign* – the selected security key will be assigned to a user, PC or group chosen. Assigned keys are displayed in the table *Assigned keys* at the bottom.
- *Import* – opens the security key import dialog. It will gradually select the public key (.pubkey) and corresponding private key *(*.privkey*)* you wish to import.
- *Export* – opens the save file dialog. Select the location where you wish to export the public and corresponding private key to.

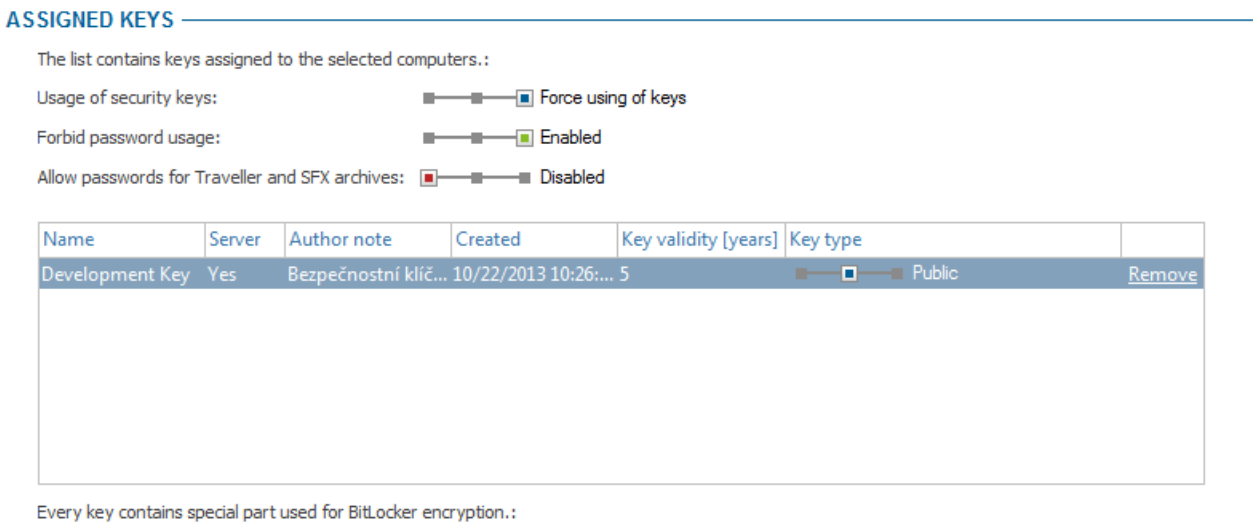
  Attention: When keys are exported, only the public and private keys are exported without the corresponding sections for drives encrypted by Bitlocker. This section can be exported separately for every drive in Encrypted disks in the Bitlocker section (*Encrypted drives -> Bitlocker -> Information -> Export*).

The security key record contains the following data:

- *Name*
- *Server* – whether the security key was created on the server (Safetica Management Service) or the client (Safetica Endpoint Client).
- *Author's note*
- *Editor's note*
- *Created* – date when the security key was created.
- *Validity* – how long the security key is valid for.
- *Key type* – which part of the key is stored in the database (public, private or both).
- *Assign* – click this button to assign a selected security key to a user, PC or group.

Assigned keys

This table lists keys assigned to users, PCs or groups marked in the user tree.



For the keys assigned you can specify the following settings:

- *Use of security keys* – you can enforce the use of security keys here.
  - o *Inherit* – settings are inherited from the higher-level group.
  - o *Do not enforce* – the security key does not need to be used for encryption on the client station. A password is sufficient.
  - o *Force using of keys* – use of security keys is enforced on the client station.
- *Disallow passwords* – if you disallow the use of passwords, only the security key can be used for encryption.
- *Allow passwords for the Traveller and SFX archives* functions – you can allow the use of passwords for the Traveller and SFX archives functions.

With every key assigned, you can specify the key type available to the user:

- *Public* – the user will only be able to encrypt data with the security key.
- *Private* – the user will only be able to use the security key for unlocking (unencrypting) data encrypted with the corresponding public key.
- *Both* – the user will be able to encrypt and unencrypt data with the security key.

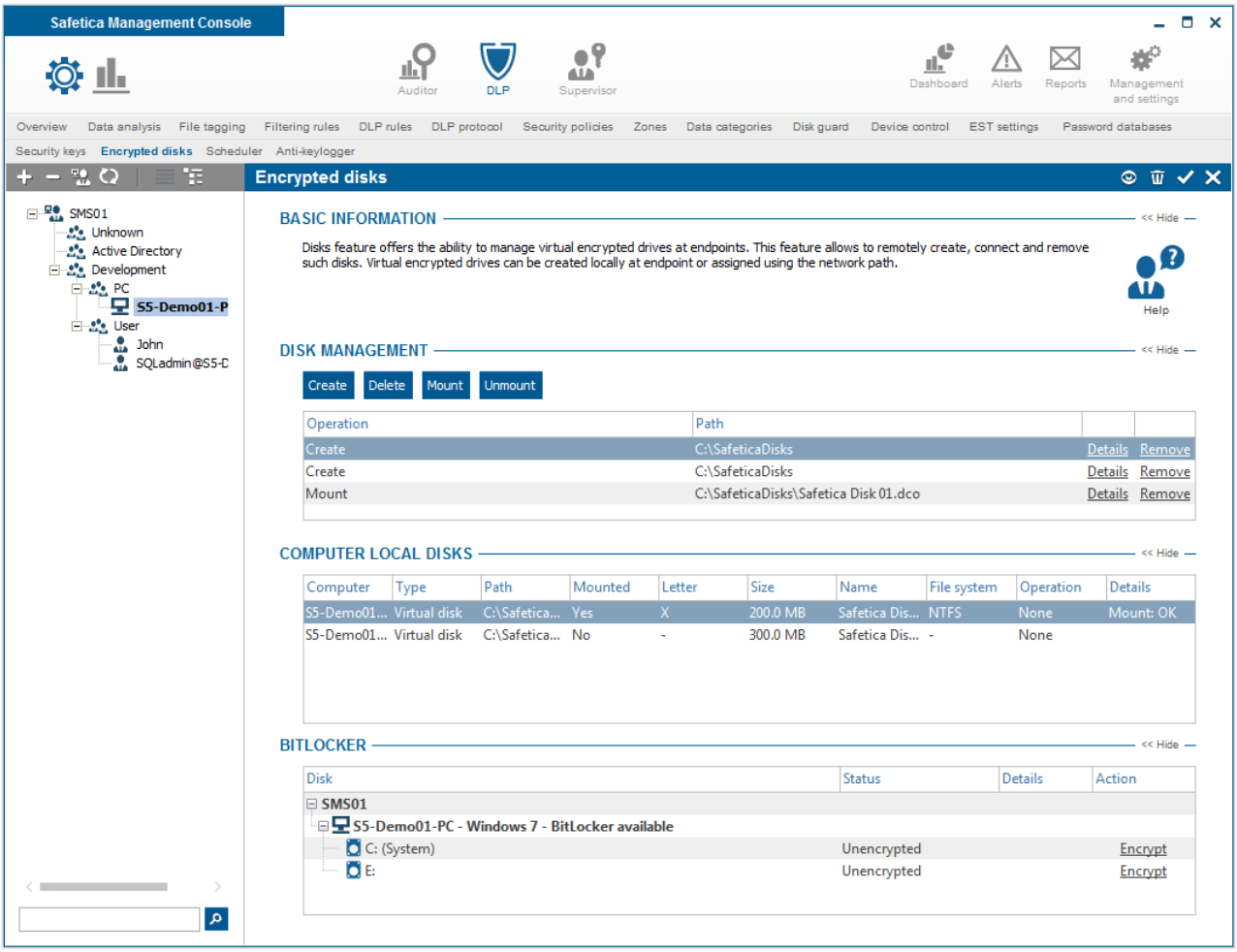
5.2.3.4 Encrypted disks

In the section *DLP* ->*Disk Encryption* you have access to administration, creation, allocating or removing encrypted client disks. Here you can remotely create virtual disks or allocate virtual disks from a network location to users, computers or groups in the user tree.

A virtual disk is a Safetica encrypted file that, after connecting to it, behaves like an ordinary physical hard disk. This means that on this disk you can create, modify and copy files or work with your data in other ways. You can also perform low-level operations on the disk, such as formatting, defragmentation, etc. There is only one difference: the contents of the disk will be encrypted with military-grade security.

In the upper part, labeled Disk Management, a list of operations performed on disks is displayed. You can Create, Remove, Connect or Disconnect disks. If you want to remove a disk operation from the list, click on the minus button on the right.

After performing disk operations, don't forget to save the changes. All changes will take effect after they are saved. You can save them by clicking on  button in the top right corner of the view.

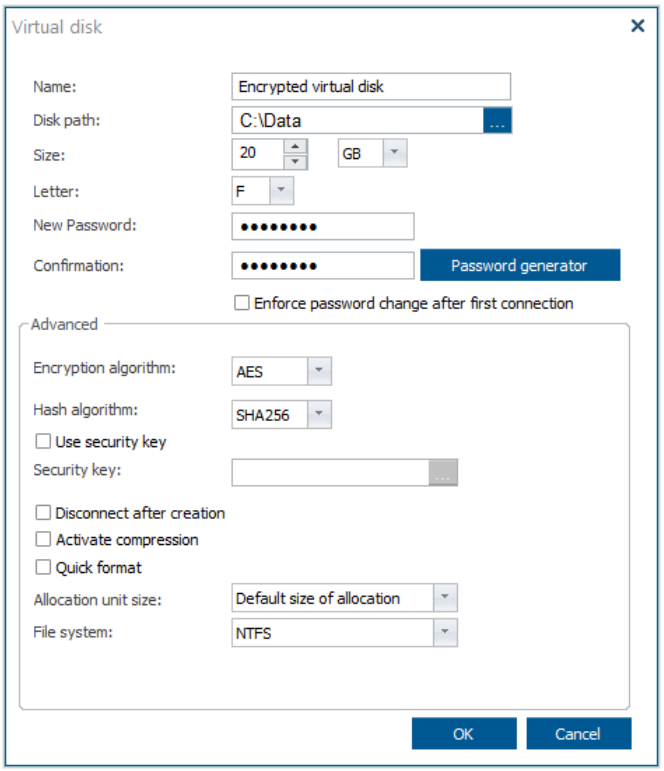


Disk managements

In the upper part, labeled Disk Management, a list of operations performed on disks is displayed. You can Create, Remove, Connect or Disconnect disks. If you want to remove a disk operation from the list, click on the minus button on the right.

Creating a virtual disk

After clicking on the *Create* button and subsequently selecting Virtual from the list, a dialog for virtual disk creation will be shown. Enter the name for the disk, its location, size, the letter under which it will be mounted within the filesystem and a password that can be created by using a generator. You can also choose a safety key which is to be used while creating the disk, as well as other advanced settings such as *Unmount after creating*, *Activate compression* and *Fast formatting*. By ticking *Force password change*, you will force the user to change the password on the first login. After confirming the data you've entered, the process of disk creation starts.



Creation of a network drive

After clicking on the Create button and subsequently selecting Network from the list, a dialog will appear where you can chose a previously created virtual disk which must be located in the network (in a folder shared over the network).

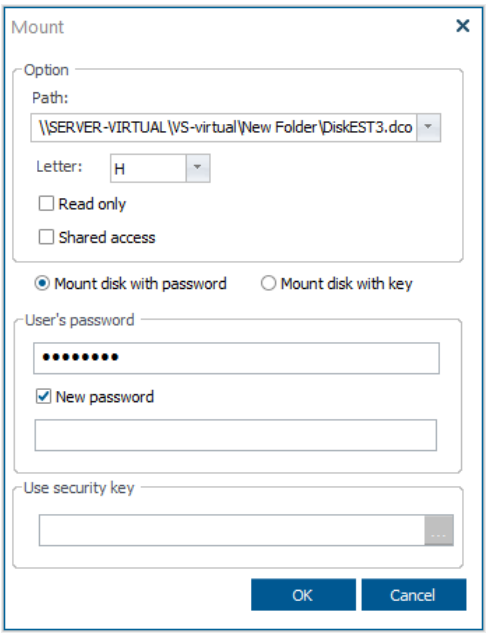
Removing a disk

You can remove a disk by clicking on Remove and selecting the disk you want to safely remove from the list. You can perform the disk removal with greater security by choosing how many times the disk will be overwritten. To make disk removal secure, we recommend overwriting it at least 7 times. A disk removed in this way cannot be restored.

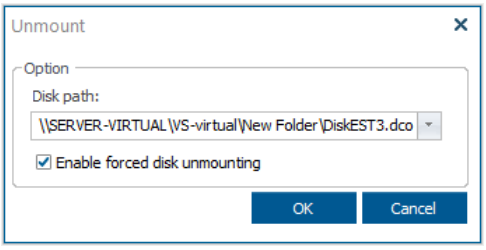
Mount and unmount disk

You can connect a disk by clicking on Connect. In the dialog, chose from the list a disk you want to connect for selected users. You can also specify what letter the disk should be connected under, whether it should be connected read-only or if you want to connect the disk using a password or a security key. Enter a key or password and to perform an operation, confirm by OK If you have selected connection with a key, you also need to enter the path to the respective security key (extension .privkey).

Using this dialog you can also change the disk password.



You can disconnect the disk by clicking on *Disconnect* and choosing the disk from list of disks. If you select hard disconnection, the disk will be disconnected even if a user is working with it. In such a case, data loss may occur!



You assign disk operations only to users, groups, computers or branches you have highlighted in the user tree.

Computer local disks

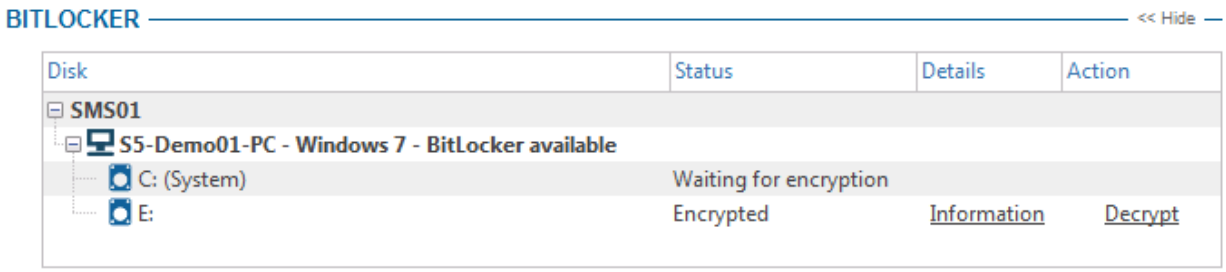
In the lower part, labeled *Computer* local discs, you can view Safetica encrypted virtual disks of a particular computer. You can also see the basic information about the disks.

Bitlocker Drive Encryotion

In the section you will find the control panel for Bitlocker Drive Encryption. Bitlocker is used for physical encryption of system and non-system drives. Find more information on Bitlocker at http://windows.microsoft.com/en-us/windows7/products/features/bitlocker.

Note: Bitlocker Drive Encryption can only be used on client stations with operating systems *Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro* and *Windows 8 Enterprise*.

In the Bitlocker control panel you will find the Safetica Management Service (SMS) list with PCs connected to the different SMS. With every PC you will see whether the Bitlocker functionality is available and the list of physical system and non-system drives you can encrypt.



Bitlocker section of the security key and key export

To encrypt and subsequently connect a drive encrypted by Bitlocker, you need to use a special part of the Safetica security key. If you use for encryption a security key that you have created, a special part will be saved with that key to be used for the connection of a drive encrypted by Bitlocker. A unique record is stored with the security key with every drive encrypted by the Bitlocker.

Example: You have two physical drives C and D on the client station. They are both encrypted by Bitlocker with the security Development Key. Two records are stored in a special part of the Development Key: one for drive C connection and one for drive D connection.

With every drive encrypted by Bitlocker, you can export the record for its connection without Safetica 5 installed. Export the record by clicking Information -> Export with the respective drive and choosing the target folder.

We strongly recommend exporting the driver's Bitlocker key as a file with the .bek extension for every Bitlocker encrypted drive. This file is essential if you want to connect (unencrypt) a drive on a PC where Safetica 5 is not installed.

Non-system drive encryption

No operating system is stored on the non-system drive. To encrypt a non-system drive, proceed as follows:

1. In the Safetica Management Console click Encrypt with the respective non-system drive and select in the dialog the security key to be used for encryption. Save the settings by clicking the  button in the top right corner of the view.

   Note: In the security keys list you will only find keys assigned to the PC where encryption will be performed. Find more about how to assign keys in the section Security keys.

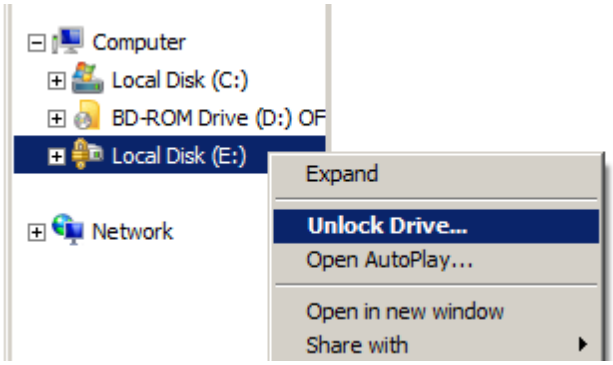
2. The drive on the client station will subsequently be encrypted. This operation is performed in the background and in the meantime you can continue working with the PC without restrictions – it may only slow down your work.

   Note: The PC can be shut down, set to hibernate or restarted while encryption is running. The encryption operation will be restored the next time the PC starts.

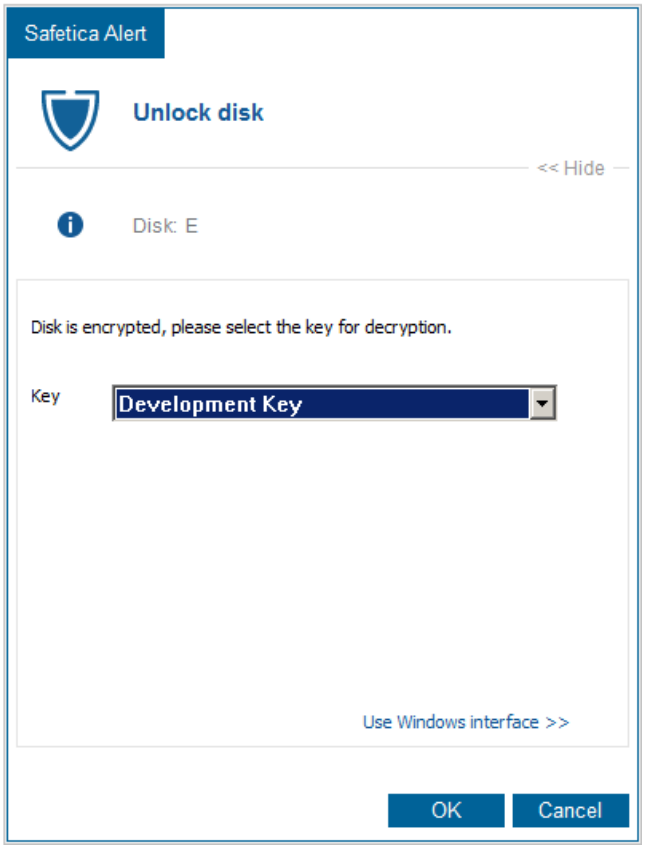
Non-system drive connection

1. To connect a non-system drive, the user must open Windows Explorer, right-click on the

respective drive, open the menu and choose Unlock unit.



2. The Safetica dialog for unlocking a drive encrypted by Bitlocker will appear. Here, the user needs to select the corresponding security key used for drive encryption. After confirming the dialog, the drive will unlock and connect to the system.



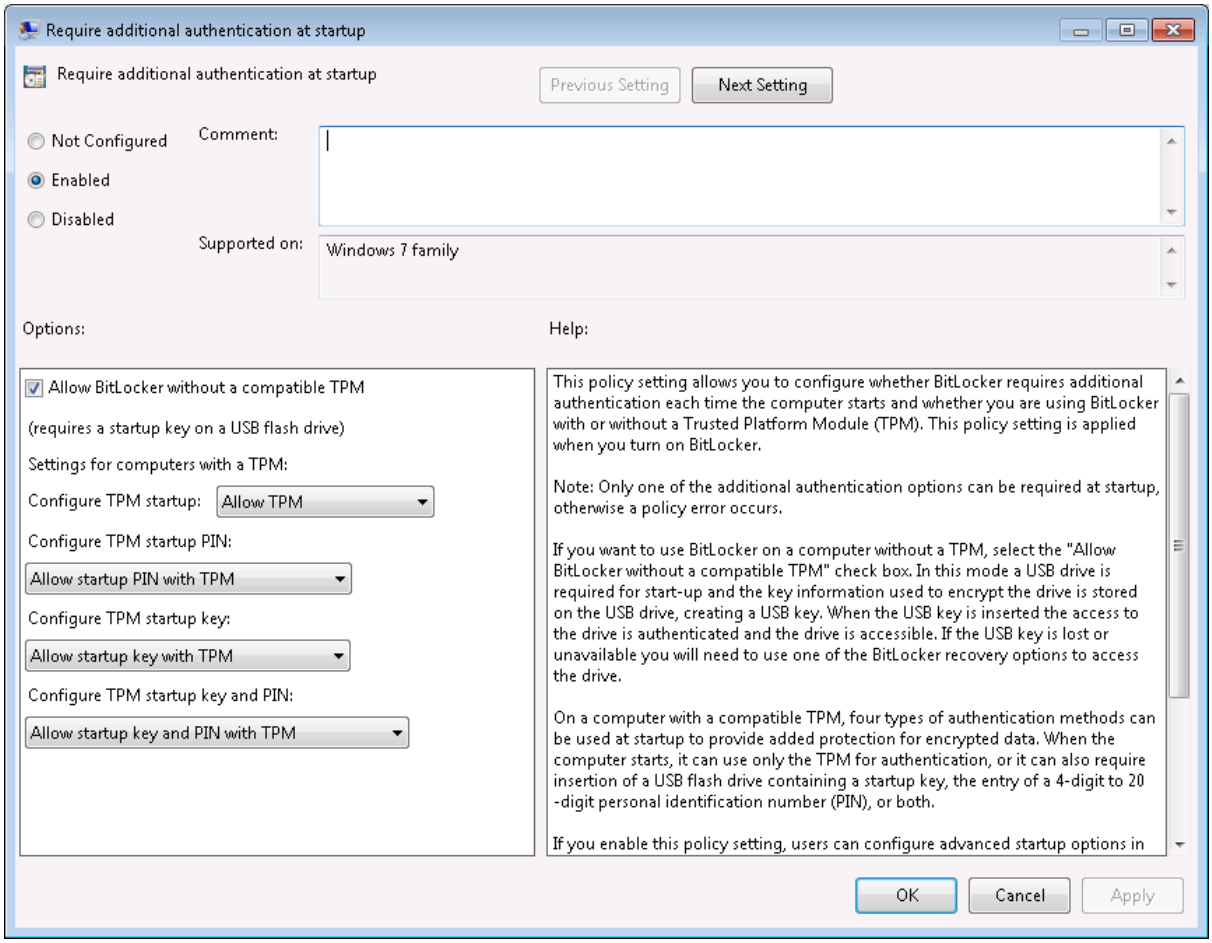
System drive encryption

The operating system is stored on the system drive. Among the drives (mostly drive C) listed, this usually has the tag System. To encrypt the system drive, proceed as follows:

1. The end user must have a designated USB storage disk ready to store the Bitlocker key. The user will use this storage disk with the Bitlocker key for system disk connection when the PC boots.

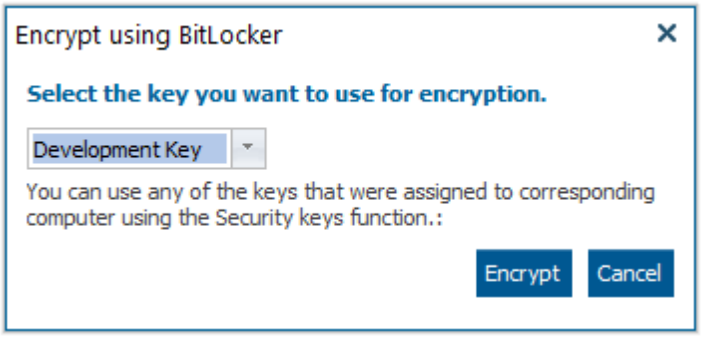
   Note: The BIOS of the PC must be able to read from the USB storage disk prior to system start.

2. Make sure that the use of Bitlocker without a TPM chip is allowed in local or domain group principles on the client station where you are going to encrypt the system drive. You will find these settings in the section *Computer Configuration -> Administrative Templates -> Windows Components -> Bit Locker Drive Encryption -> Operating System Drives -> Require additional authentication at startup*. Allow these settings and check the option Allow the Bitlocker tool without compatible TPM chip.

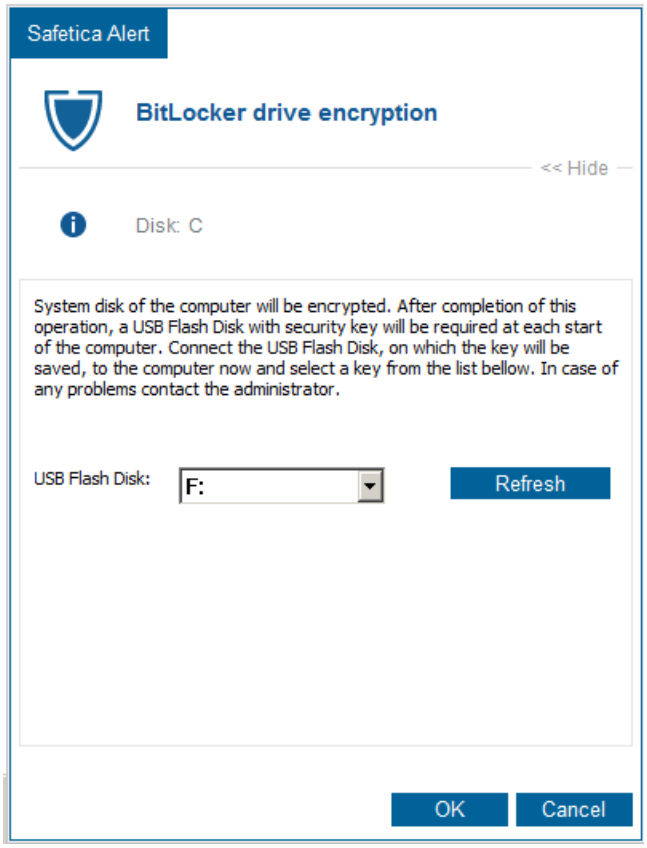


3. In the Safetica Management Console click Encrypt with the respective system drive and select in the dialog the security key to be used for encryption. Save the settings by clicking the  button in the top right corner of the view.

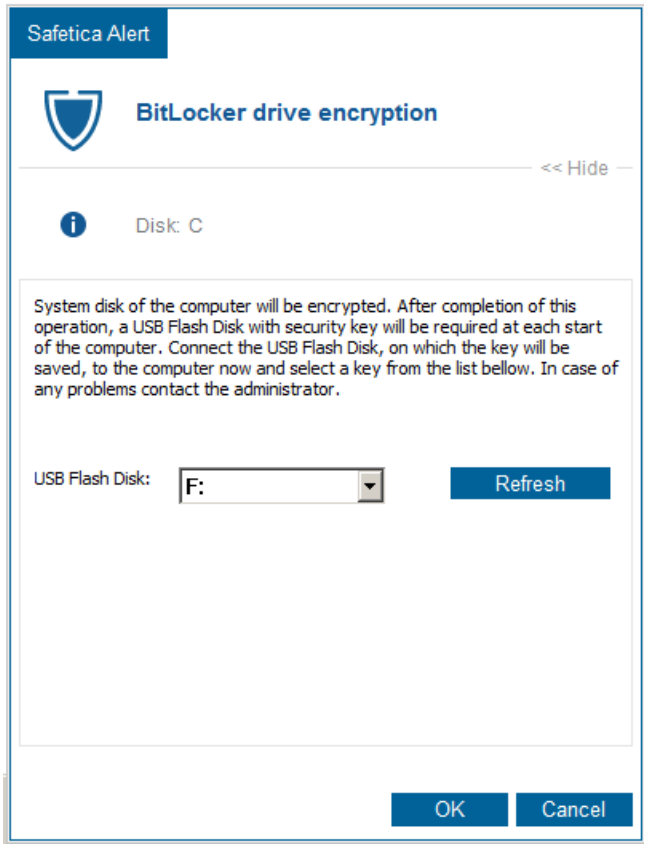
   Note: In the security keys list you will only find keys assigned to the PC where the drive shall be encrypted. Find more about how to assign keys in the section Security keys.



4. The client station will be prepared for encryption and the user will be asked to restart the PC.



5. After restarting, at login the user will be asked to connect the USB storage drive on which the Bitlocker key for system drive connection is stored. Using the dialog shown below, the user must select and confirm the USB storage drive unit.



6. When confirmed, the PC will be restarted again and the system disk connection process verified. While this operation is running, the USB storage drive with the Bitlocker key must be connected to the PC.

7. After successful verification, the PC will be started in the usual way and the system drive encryption will be launched. This operation is performed in the background and in the meantime you can work with the PC without restrictions – it may only slow down your work.

   Note: The PC can be shut down, set to hibernate or restarted while encryption is running. The encryption operation will be restored the next time the PC starts.

System drive connection

To connect the system drive, the user needs to connect the USB storage drive with the Bitlocker key used for encryption every time the PC is started. When verified, the drive will be connected and the operating system started.

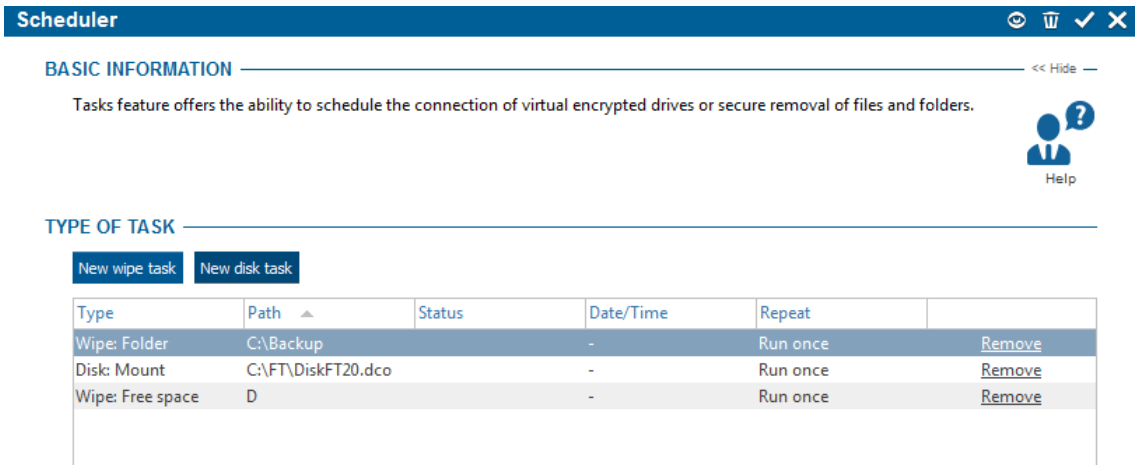
Decrypting drives

To decrypt a drive, click the *Decrypt* button on the respective system or non-system drive. Save the settings by clicking the  button in the top right corner of the view. The respective drive will be automatically decrypted after the settings are downloaded to the client station.

5.2.3.5 Scheduler

Did you know that by deleting files alone, you cannot ensure they have been removed securely? Even data from formatted disks can be easily restored. With data shredding, however, data cannot be recovered (even under laboratory conditions).

The console sub-module *DLP*-> *Scheduler* offers a fast and simple approach to creating shredding, connecting or disconnecting tasks.

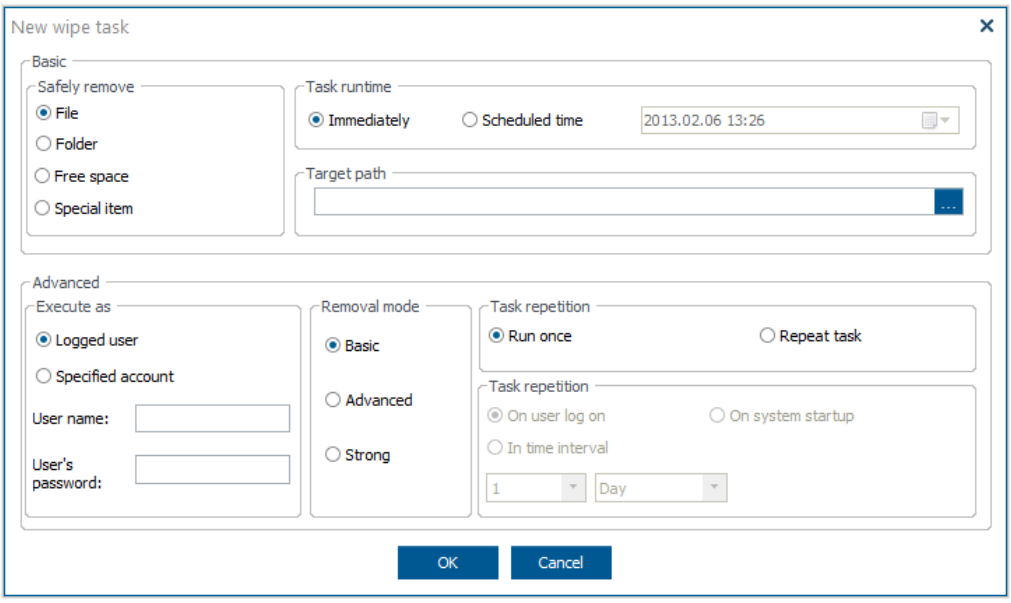


In the view you can see a list of created tasks. Each task shows the type in the left section, that is, whether it is a disk or shredding task. The central section contains other task information, such as what file or disk the particular operation relates to. It also shows task execution times or whether it is a one-off task or a repeated task. On the right there is a button for removing the task.

To create a new task you only need to click on the respective buttons *New wipe task* or *New disk task.* Then the respective window for task creation will be shown.

Wipe task

In the first step select exactly what you want to shred safely – files, whole folders, disks, special folders (contents of the recycle bin, browser history, etc.). Provide the path to the respective file, folder or disk. You can then specify the task execution time, whether it is repeating and, if required, also change the account under which the task is run. You can use this option e.g. in cases when the selected user's account does not have sufficient rights to delete certain sensitive components. Therefore, when creating the task you must enter the username and password for the account under which the task being executed will have sufficient privileges.



Finally, you can change the Mode of removal:

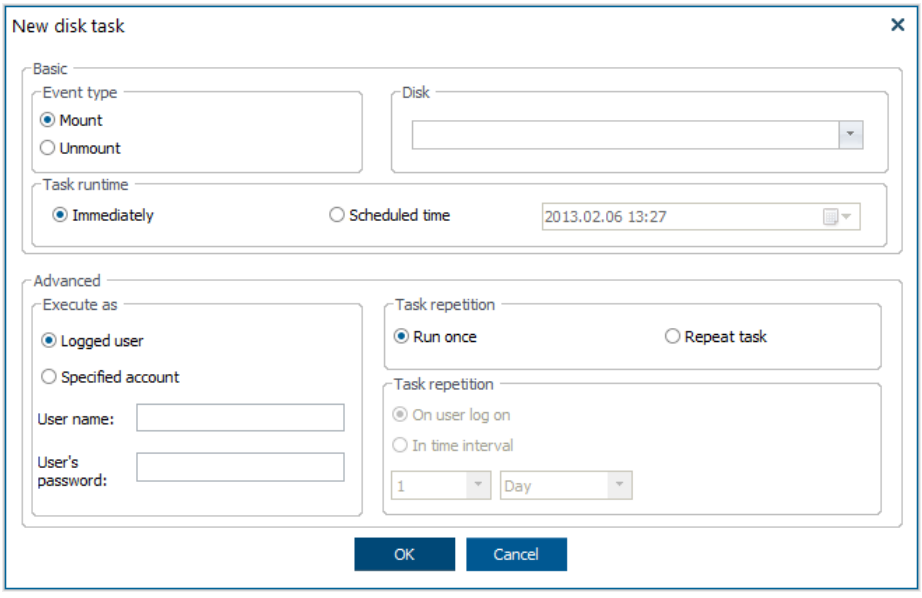
- Basic – shredded files are overwritten 3 times
- Advanced – files are overwritten 7 times
- Extra powerful – files are overwritten 35 times

The stronger the mode you select, the more effective shredding of the selected files will be, but the process will take longer as well. If you are not deleting highly sensitive data, leave the mode set to Basic.

Finally, confirm everything by clicking on OK. The task will be added in the task list and upon saving it will be assigned to the selected users. If the task is scheduled to be executed immediately, it will be executed when its settings reach the client station.

Disk task

In this dialog chose an encrypted disk from the list which you want to disconnect or connect (the password is not saved upon connection – it is entered on the client side where a window for password entry will appear). After that you can specify the task execution time, whether it is repeating and, if necessary, you can also change the account under which the task runs.



In the end confirm everything again by clicking *OK*. The task will be added in the task list and upon saving it will be assigned to the selected users. If the task is scheduled to be executed immediately it will be executed when its settings reach the client station.

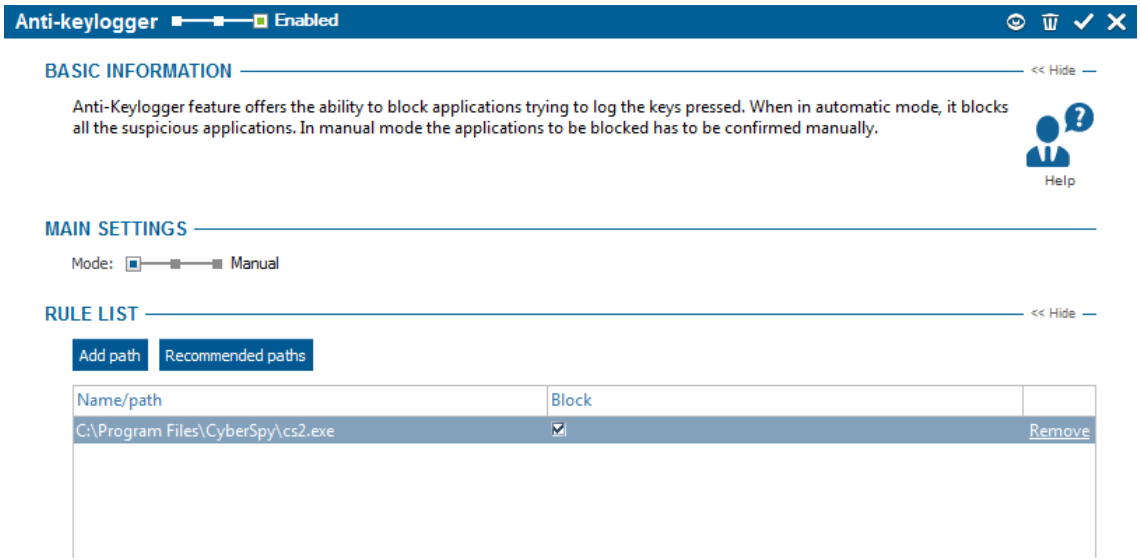
Note

You assign tasks only to users, groups, computers or branches you have highlighted in the user tree. To apply the settings you have to save the changes using  or you can cancel the changes you have made by  in the upper right corner.

5.2.3.6 Anti-keylogger

Spy programs – keyloggers – can bug your computer to pick up passwords and other sensitive data input by keyboard. Anti-keylogger is a tool that intelligently and automatically executes a check of launched applications. If it detects an application that shows the behavior of a keylogger, it terminates it and informs the appropriate security manager. If you use a specific application that behaves like a keylogger, it can be unlisted from the Anti-keylogger settings and authorized.

You can set Anti-keylogger and display records of its activity in *DLP -> Anti-keylogger.* If you display records of Anti-keylogger or if you wish to set it up, it depends on the general console mode (Setting, Visualization).



Setting

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

- *Disabled* – Anti-keylogger is not activated
- *Inherit* – function mode is not set. Settings are inherited from the parent group
- *Enabled* – Anti-keylogger is activated

Anti-keylogger can operate in two modes:

- *Automatic* – if Anti-keylogger in this mode captures a new harmful program; it will automatically block it from launching.
- *Manual* – if Anti-keylogger in this mode captures a new harmful program, it will send a notice of this unauthorized attempt to the administratorbut it will not block the program. The decision whether the program should be blocked or allowed must be made by the administrator based on his own judgment. The program may then be blocked or allowed in the monitoring section.

Rule list

This section provides a list of blocked or allowed programs. You can manually change the setting of particular programs for blocking (allow, block). If you use manual mode new records will not have the blockings set. With these records you must specify the settings (permit, block) Here you can also manually add or remove the blocked programs using the keys *Add*, *Remove*.

Here you can also manually add blocked programs using the *Add* button, or display *Recommended paths*. After clicking *Recommended paths*, a dialog will be displayed with a list of paths to potentially harmful programs that have been previously detected among the users of Safetica Management Service. By choosing the paths for blocking, you will block the application for the currently selected users.

Visualization

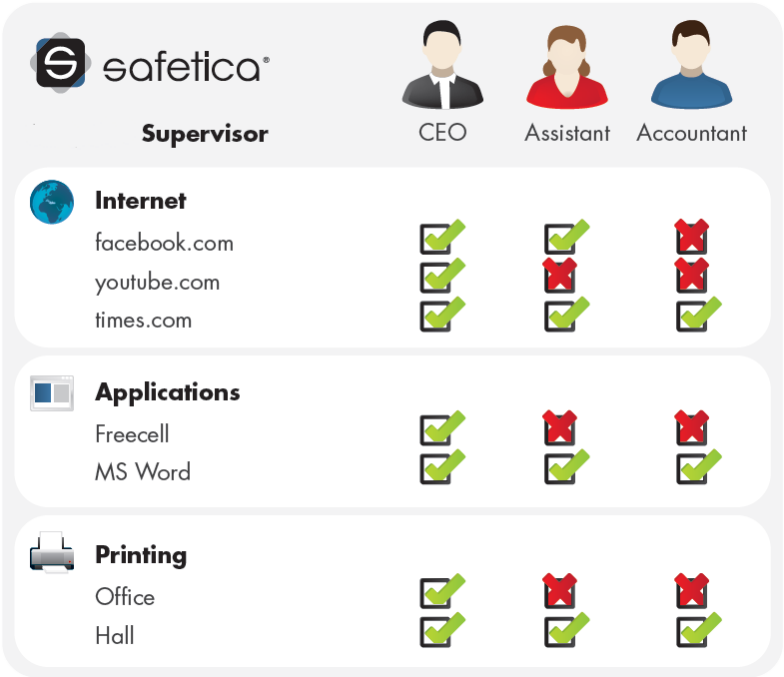
The visualization mode includes records of blocked applications. If you right-click on the records, a menu will be displayed with the items Deny list and Allow list. If you choose the List of Prohibited, you will see a tree of users, from which you can choose those users, groups, and computers to whom or to which you want to prohibit the program detected. Those users will then have a blocking rule added to their list in the Anti-Keylogger. If you choose the List of Permitted, you can hose the users that you want to allow to run the program.

Note

Anti-keylogger is only set for users, groups, computers or branches you have highlighted in the user tree. To apply the settings you have to save the changes using  or you can cancel the changes you have made by  in the upper right corner.

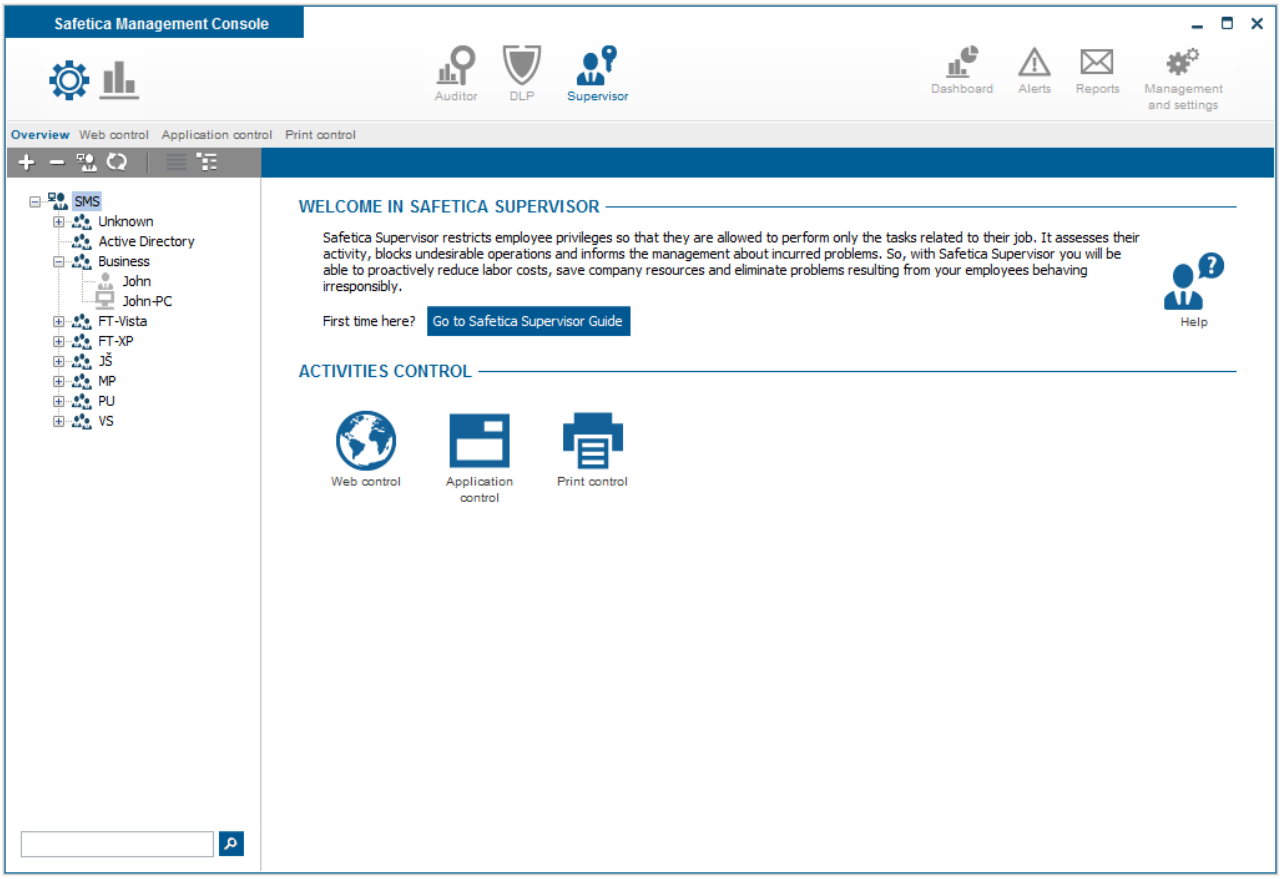
5.3 Supervisor

Supervisor thoroughly keeps watch over your employees to ensure they are doing their job. It evaluates their activity, blocks undesirable activities and informs management about problems incurred. With Supervisor, you can reduce labor costs, save company finances and eliminate problems resulting from your employees' undesirable activities.



Main Benefits

- Increase your employees' productivity by blocking unsuitable websites and applications.
- Obtain detailed control over your employees' work.
- Protect company computers against harmful software run by employees.
- Save money by limiting problem employees' printing.
- Avoid changes to company processes and costs related to them.
- Reach compliance with industrial standards, regulations and laws easily.



5.3.1 Web control

Stop employees from browsing websites for their amusement and block attempts to visit illegal and harmful websites. Thanks to Supervisor, you can easily determinate which websites employees are allowed to visit (Allow list) and which are off-limits to them (Deny list). You can stop employees from wasting working time or breaking the law by participating in illegal activities. Auditor also reliably blocks websites which are accessed by means of protected HTTPS port.

In the section *Supervisor* -> *Web control* you can access control of web sites which users can visit.

Main Settings

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

- *Disabled* – function is not activated.
- *Inherit* – function mode is not set. Settings are inherited from the parent group.
- *Enabled* – function is activated.

Web control has two modes:

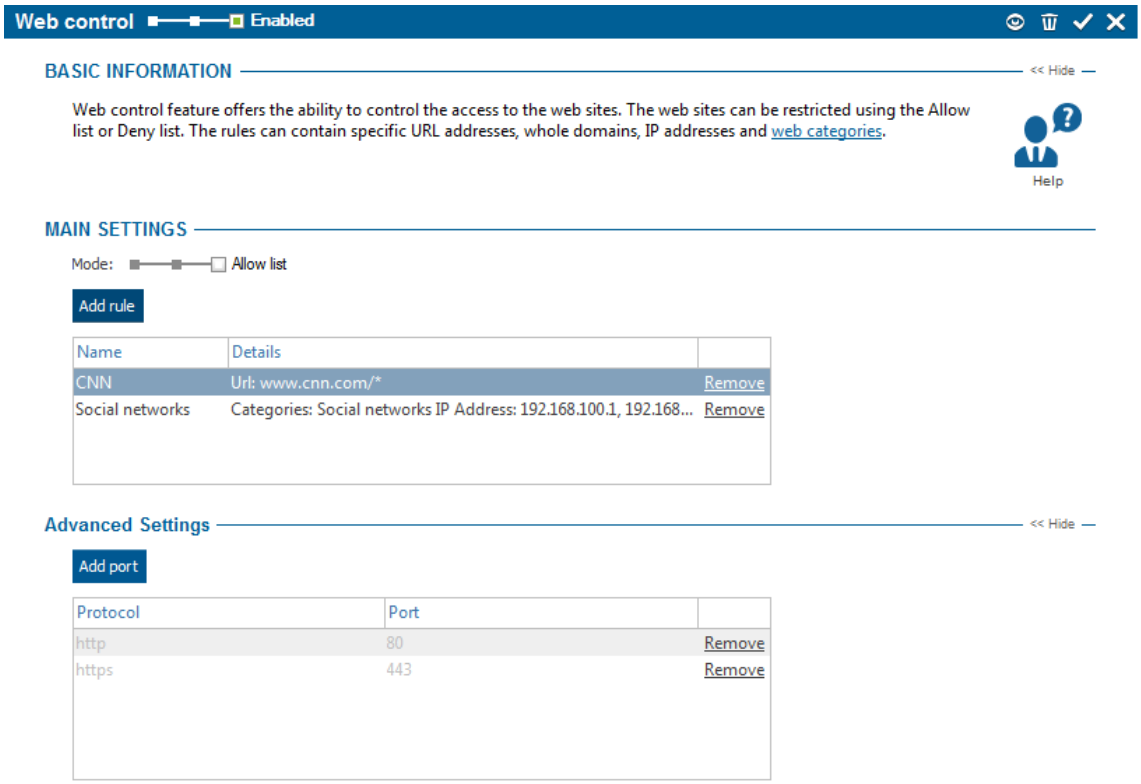
- *Allow list* – in this mode all internet access is disabled by default and you can add rules that allow access for specific cases.
- *Deny list* – in this mode all internet access is enabled by default and you can add rules that deny access in specific cases.

Under the mode slider you can find a list of rules.

Using the *Remove* button you can remove selected rule.

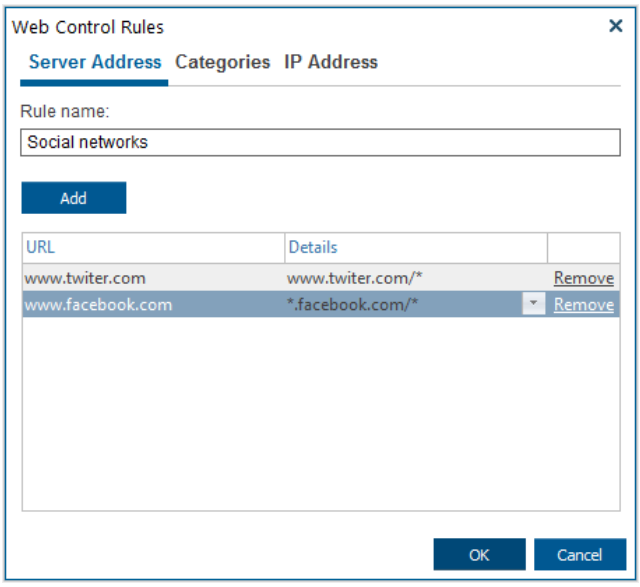
You can edit the selected rule by double-clicking on it.

Web control rules are only set for users, groups, computers or branches you have highlighted in the user tree. To apply the settings you must save the changes using  or you can cancel the changes you have made by  in the upper right corner.

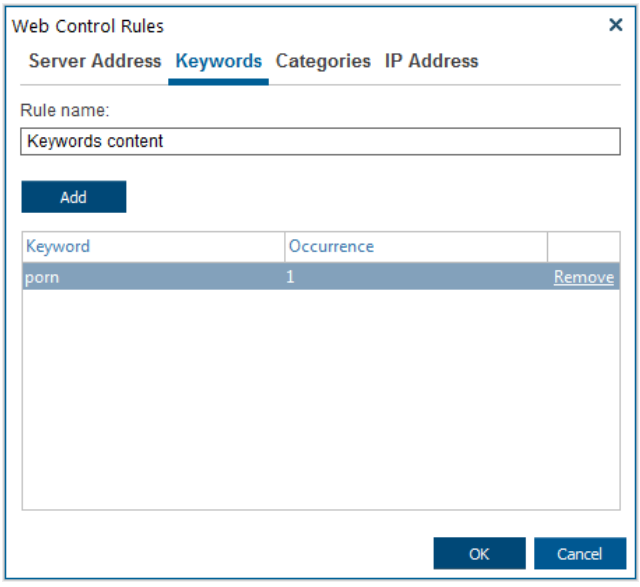


Creating a new rule

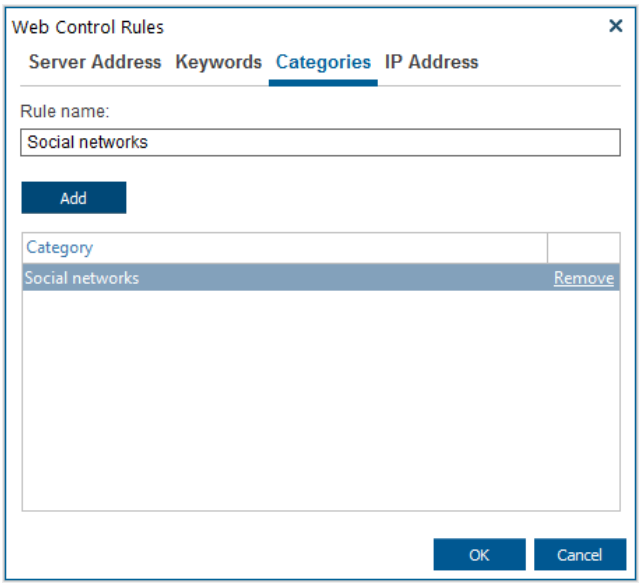
1. Click on Add rule button and new rule definition wizard will open.
2. Enter a name and description for the rule.
3. Enter the URL and specify on what level of domain the rule will be applied using Click the Add button to add the address to the list. You can add multiple addresses to the list. Click the Next button when you are finished.



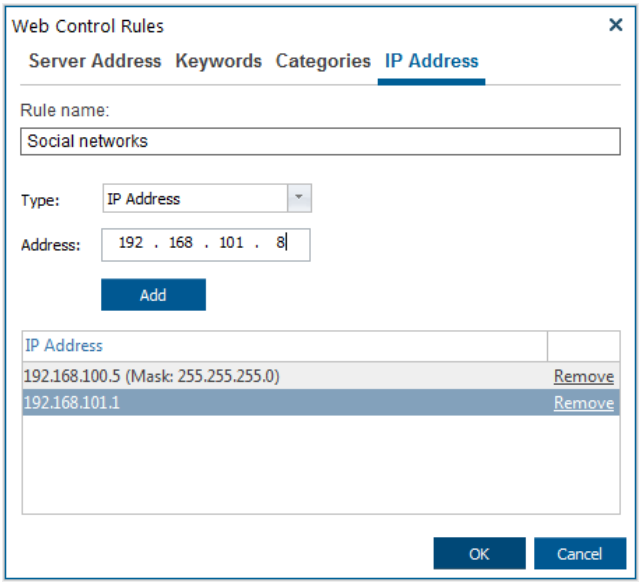
4. (Deny list only) Enter a word or text string into the Keyword field. The rule will be applied when the text is found in the content or URL of a website. Then, enter the number of times the text must occur before the rule is applied. Click *Add keyword* to add it to the list. You can add multiple keywords into the list. Click the *Next* button when you are finished.



5. Click on the Add category button and choose a specific web category from the dialog. Click on Select to add the web category to the list. You can add multiple categories to the list. Click the Next button when you are finished.



6. You can add three types of IP addresses into the rule. First, select the type using the slider.
   - *IP address* – enter a single IP address into the IP address field and then click on the Add button to add it to the list.
   - *IP with mask* – enter a single IP address with the subnet mask and then click on the Add button to add it to the list.
   - *IP range* – enter a range of addresses by entering From and To addresses. The rule will be applied to each IP address inside the range, inclusive of the IP addresses entered for specifying the range. Click on the Add button to add it to the list.



7. Confirm what you have input in the rule definition wizard by clicking on the Finish button

Note: Points 2, 3, 4 and 5 are optional. The rule is applied if at least one of the rule components (URL, web categories or IP address) corresponds to user behavior on the internet.

Edit rule

Click on the Edit button or double-click on the rule in the list to edit the rule.

Server address

A Web web address or URL (Uniform Resource Locator) is an address that identifies the source on the Internet. For each address inserted added toin the list, you can specify on which level the rule will be applied. For example, if you enter www.facebook.com, , you can use specify the follow-

ing options in Details:

- www.facebook.com/* – the rule will be applied on www.facebook.com and on all other addresses starting with this sequence, e.g.. For example www.facebook.com/AAA/ , www.facebook.com/AAA/BBB, etc.
- *.www.facebook.com/* – the rule will be applied on www.facebook.com and on all other addresses, which containing this sequence. , e.g.For example www.facebook.com/AAA/ or ccc.www.facebook.com/AAA/BBB, etc.
- *.facebook.com/* – the rule will be applied on all addresses , which containing .facebook.com, e.g.. For example www.facebook.com/AAA/ or ccc.facebook.com/AAA/BBB, etc.
- *.com/* – the rule will be applied on all addresses , which containsing the sequence: .com. This will block all the sites ending in .com. , e.g. For example www.facebook.com/AAA/ or www.cnn.com.

By default, the first option is used, i.e. www.facebook.com/ *.

Keywords

Key words are searched for in page contents and headingheaders. For each keyword the number of its occurrences is stated on the website when the rule is used. If Safetica Endpoint Security finds a keyword in the header content, the rule is applied regardless of the required number of occurrences. There is no limit to the number of keywords specified in the rule is not limited.

You can also specify whether the key chain shall be searched inside the text or as a whole word.

Categories

After selecting the specific category, all web addresses that fall into that category are included in the rule. To modify websites, use the category category accessible from the main menu.

IP address

In the IP address section you can choose for which IP address the rule will be applied to. There are three options for creating a new IP address rule:

- *IP address* – The address of the website specified by four numbers in the 0-–255 range, separated by dots. If you do not know the server address, contact the administrator and ask him to convert the URL addressURLes into IP addresses.
- *IP range* – The rule will be applied to each IP address inside the range, including inclusive of the IP addresses entered for specifying the range.
- *IP with mask* – The rule will be applied to the an entered IP address entered with its subnet mask.

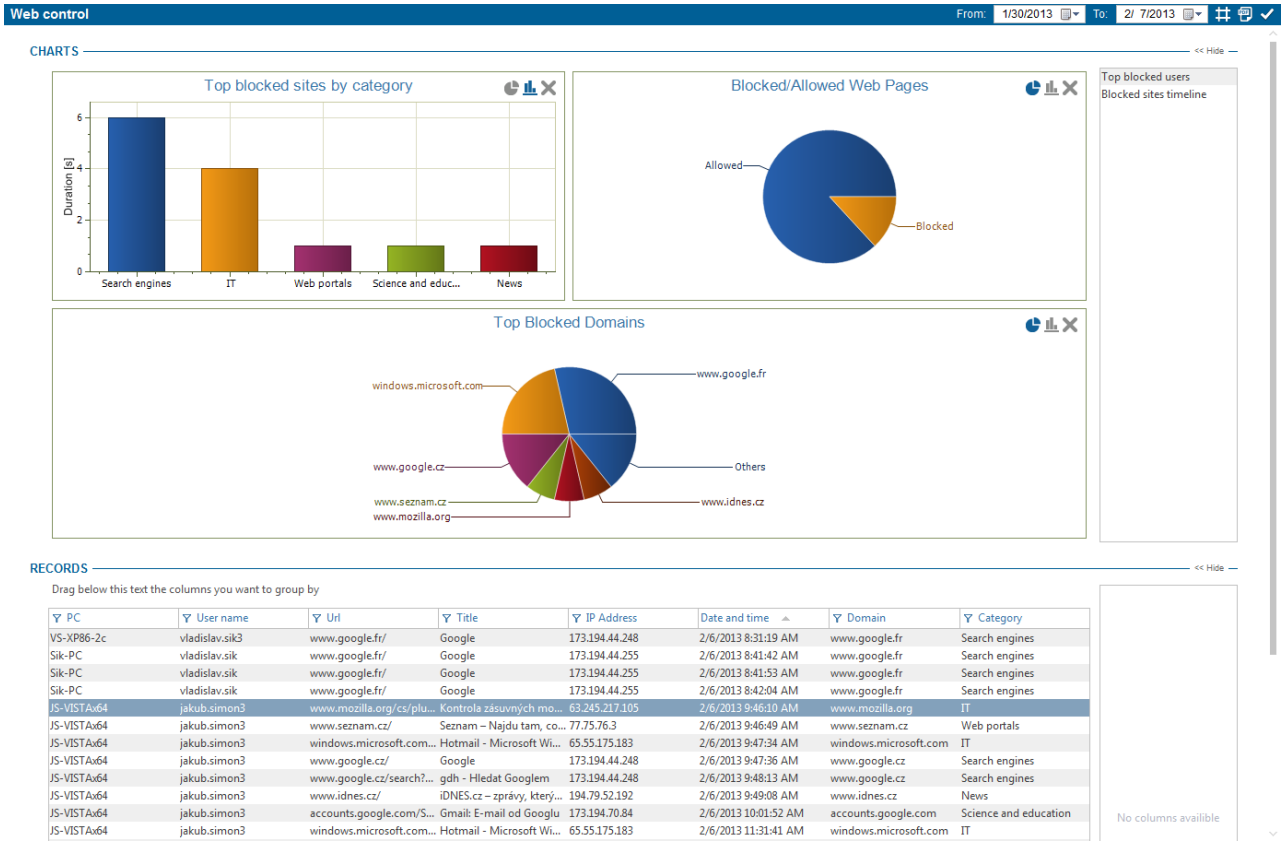
Advanced settings

In the advanced settings you have the option to specify the ports on which the http HTTP and https HTTPS protocols are running. Web control will be applied only to the protocols and ports entered in the list. By default, the list includes the most frequently used combinations of protocols and ports, see picture the figure above.

Visualization

Data that you can see in the visualization mode are only shown for the usersThe data that you can see in the visualization mode is only shown for the , computers, or groups users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the  button in the top right

corner of each chart.



Available charts:

- *Blocked/Allow web pages* – the chart contains the number of blocked and allowed web pages.
- *Top blocked domains* – the chart contains the most blocked domains along with the number of their blocking (up to seven domains are shown).
- *Top blocked users* – the chart contains users with the highest number of blocked web sites (up to seven users are shown)
- *Blocked sites timeline* – chart contains number of blocked web sites over time.
- *Top blocked sites by category* – chart contains the number of blocked web sites by category.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of columns on the right.

Available columns:

- *Date and time* – date and time when record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was made.
- *URL* – URL of blocked website.
- *Title* – title of blocked website.

- *IP address* – IP address of blocked website.
- *Domain* – domain address.
- *Category* – website category.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.3.2 Application control

Application control provides prevention and protection against your employees launching unauthorized applications and ensures the integrity of controlled applications. You can easily define rules for blocking applications across the entire company.

Applying rules on client stations will enable or disable a particular application/application category on client stations.

In the section *Supervisor* -> *Application control* you can access control of the applications your employees run.

Main settings

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

- *Disabled* – function is not activated
- *Inherit* – function mode is not set. Settings are inherited from the parent group
- *Enabled* – function is activated

Application control has two modes:

- *Allow list* – in this mode all applications are disabled by default and you can add to the rules only those applications/application categories you want a user to be able to launch.

  Attention: If you set this mode and there are no rules enabling applications, all applications which a user launches will be blocked! In this mode you have complete control over applications which a user launches!

- *Deny list* – in this mode launching applications is allowed by default and by using rules, you can deny particular applications/categories.

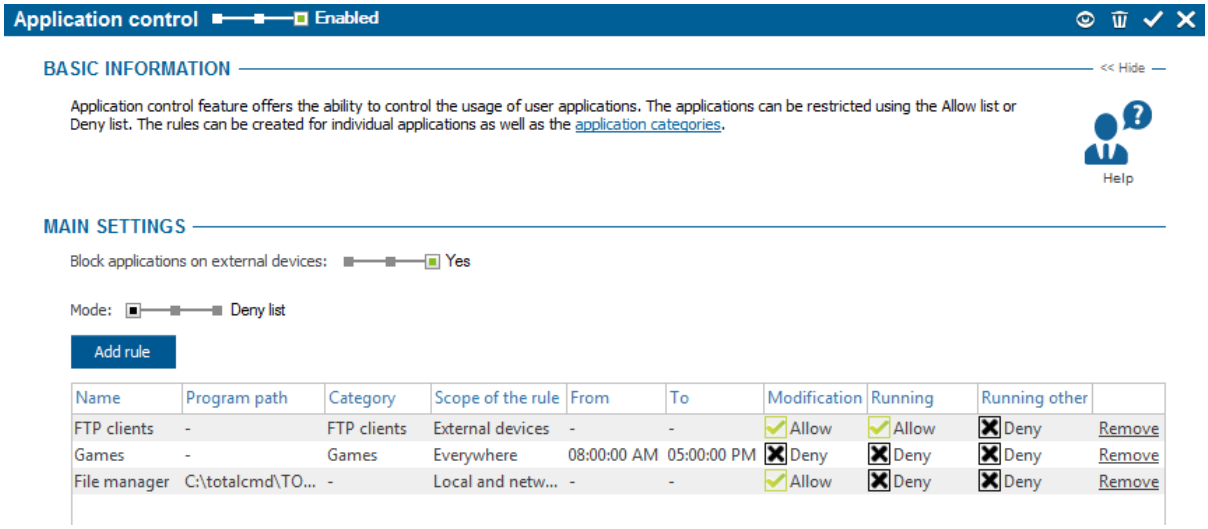
Under the mode slider you can find a list of rules.

Using the *Remove* button you can remove the selected rule.

You can edit the selected rule by double-clicking on it.

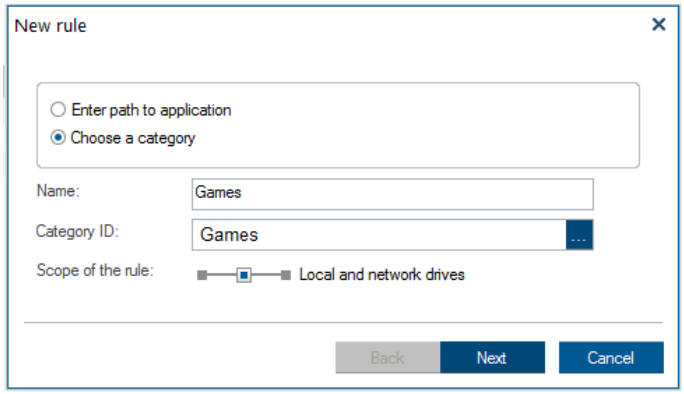
Application control is set only for users, groups or computers you have highlighted in the user tree.

To apply settings you have to save the changes using the in the upper right corner.



Creating a new rule

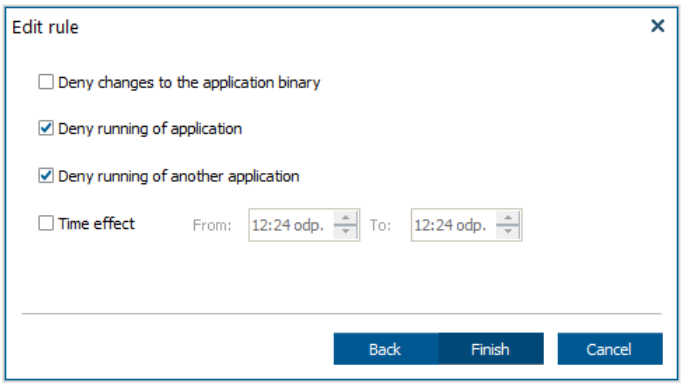
1. Click on Add rule button and the new rule definition wizard will open.
2. Now you have two options for choosing an application:
   - Enter path to application – by entering the name, you can select one application the rule will apply to.
   - Choose category – enter a name and select one of the application category. The rule will apply to all application listed in this category.



   - *Scope of rule* – with this scroll bar you can specify the scope of validity of the rule created:
     - *Only external devices* – the rule will be valid only for applications run from external devices.
     - *Local and network paths* – the rule will be valid only for applications run from local or network paths.
     - *Everywhere* – the rule will be valid for all applications the user runs.

   Click on the *Next* button.
3. Edit rule properties in this step:
   - *Deny changes to the application binary* – denies modification of the program executable. Modification of a program could occur, for example, during updates.
   - *Deny running of application* – running of the application will be blocked.
   - *Deny running of another application* – prevents applications that are allowed to launch from launching other applications (e.g. Total Commander could not launch anything else etc.).

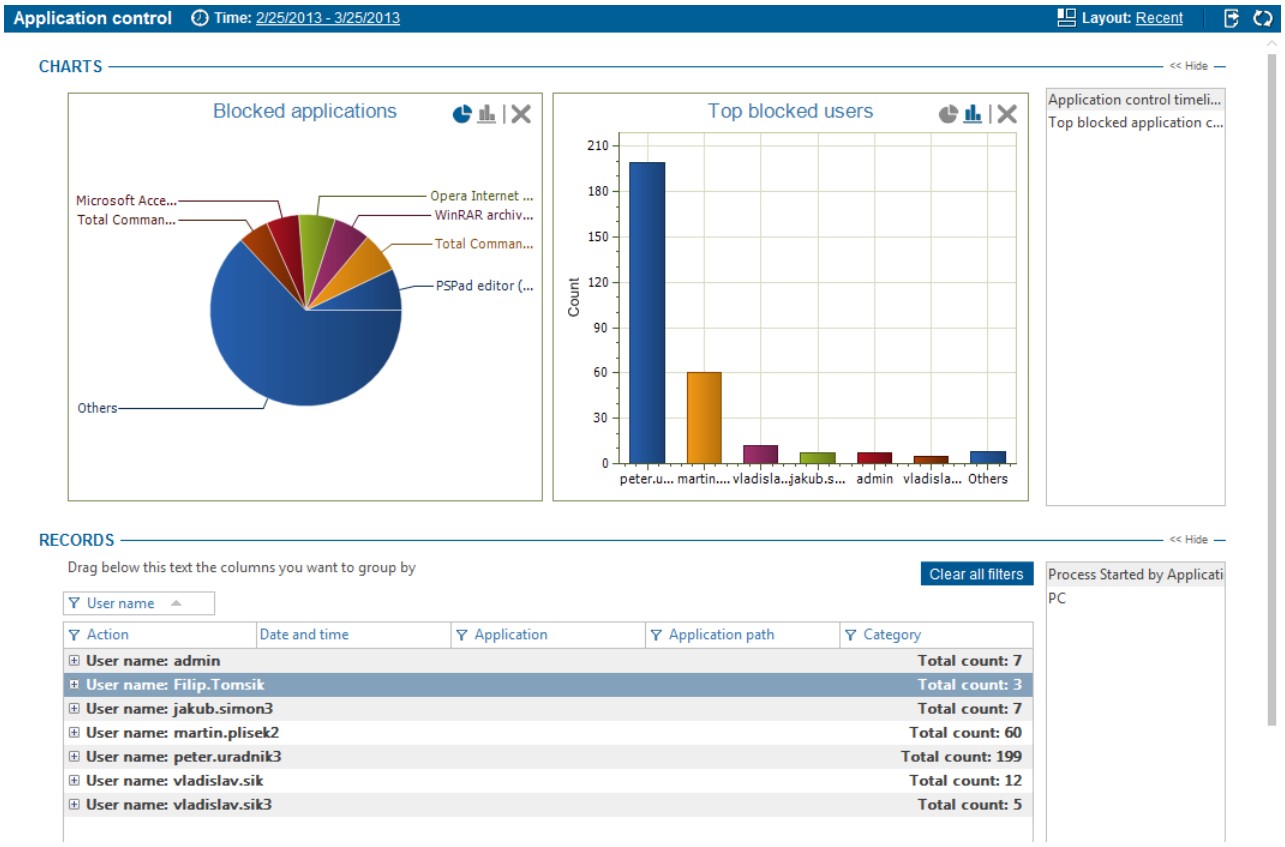
- *Time effect* – you can set a rule to be valid only for a certain period of time.



4. Confirm what you have entered in the rule definition wizard by clicking the Finish button.

Visualization

The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each chart.



Available charts:

- *Application control timeline* – the number of specific application control actions in over time.
- *Blocked applications* – the chart contains blocked applications along with number of their blocking. (Up up to seven 7 applications are shown).
- *Top blocked users* – the chart contains users with the most highest number of blocked applications. (up to seven users are shown).

- Top blocked application categories – the chart contains blocked application categories (up to seven categories are shown).

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at the table dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of column list of columns on the right.

Available columns:

- *Date and Time* – date and time when record was logged.
- *PC* – name of the PC where the record was taken.
- *User name* – the name of the user under whom the record was done under whom the record was made.
- *Application* – name of the application.
- *Action* – if running of the application was allowed or blocked.
- *Process started by application* – name of the process that was launched by this application.
- Application path – path to application executable file.
- Category – name of the application category.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

5.3.3 Print control

Printing management provides you with a means of overall printing administration in your company. Based on the list of printers, you can determine which users can print where. You can choose applications that are allowed to print, or you can set user quotas for printing.

You can find the printing management tools in the module *Supervisor -> Print control*.

Settings overview

In the console mode, you can turn this function on and off via the slider in the view's header.

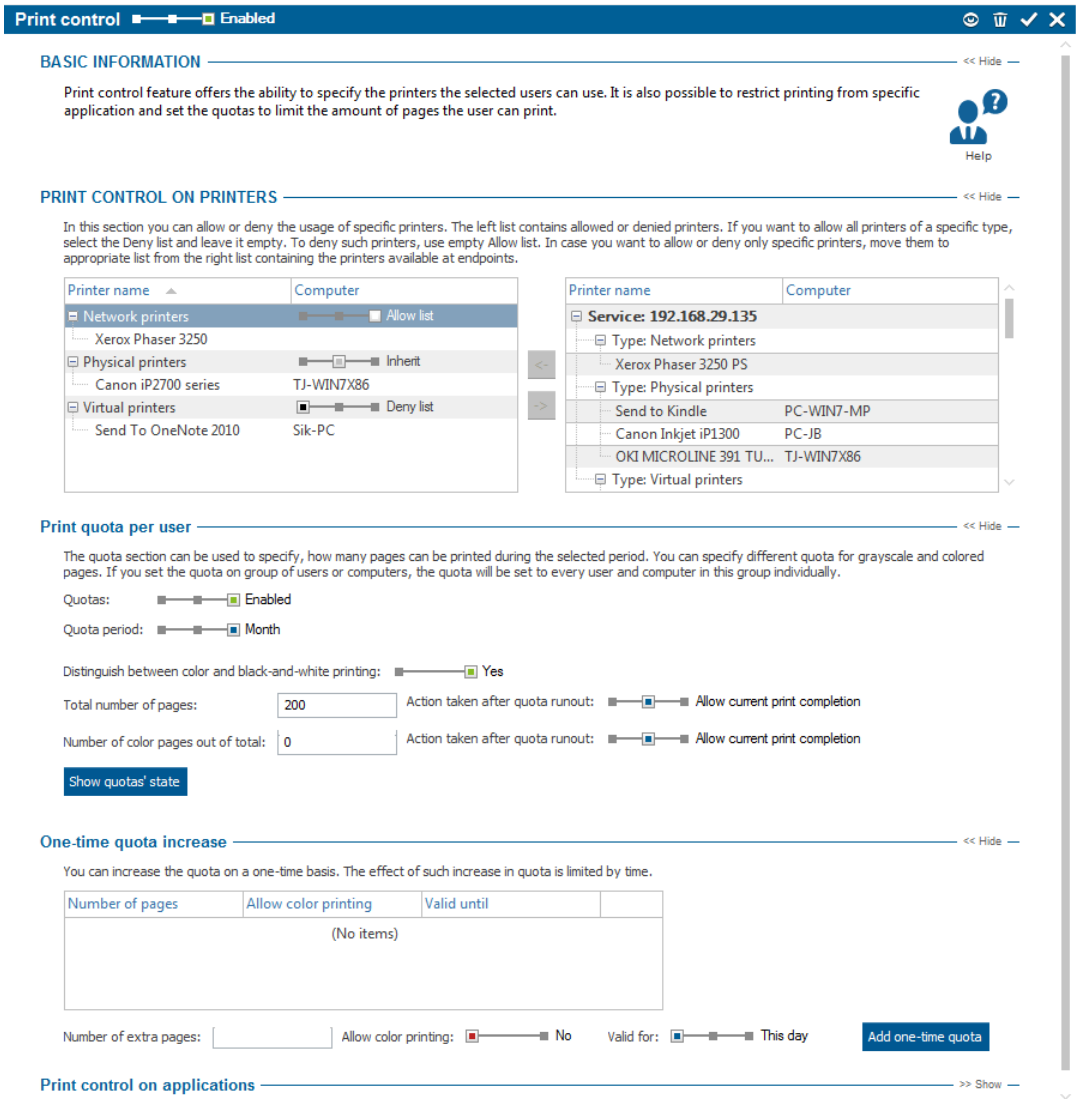
- *Enabled* – printing management is turned off.
- *Inherit* – the function is not set. The settings are inherited from the parent group.
- *Disabled* – this option will allow the printing management function.

The rest of the Overview introductory tab contains information on the type of printing management that is currently set. Clicking on the Modify button in the relevant part of Printing Management will allow you to modify that part.

Printing Management contains three parts. Each part can be turned on or off separately.

- *Print control on printers* – create lists of allowed or forbidden printers.
- *Print quota per user* – sets printing limits. The quota set for a group is applied per individual user or computer in this group.
- *Print control on applications* – allows or denies printing from given applications.

Printing management is only set for the users, groups, or computers that you have selected in the user tree. To apply the settings you have to save the changes by clicking on the button. Alternatively, you can cancel your changes by clicking on the button in the top right corner.



Print control on printers

In the printer tab there are two tables. In each is a list of printers, which is divided into three categories according to the type of the printer – physical, virtual, or network printers. In the table on the right is a list of available printers, which are connected to a computer with a Safetica Endpoint Client (SEC).

In the table on the left are printers for which you want to set up a rule. You can either allow the printer or deny it. This depends on whether the given category is set in the Allow List or in the Forbidden Deny lList. You can decide this by means of the slider next to that category.

Moving printers between the two tables can be done by means of the arrow buttons located between the tables.

With each table you can use the search field below. Found text will be highlighted in the table. Click-

ing on the X next to the search field will cancel the highlighting.

Print quota per user

In this section you can set up detailed printing quotas along with the actions that should be taken if the quota is exceeded. In the bottom part, you can set up one-time quotas, which can be used, for example, to temporarily increase current quotas. This is useful when quotas have been exceeded and you do not want to change all settings.

A quota set for a group is applied per individual user or computer in the group. User on endpoint PC is notified about quota status when 50, 75 and 90% of quota is exceeded.

Attention: The quota does not apply to print from virtual printer. Quotas are applied only to the physical and network printers.

With quotas, you can choose from the following options:

- *Quota period* – what the duration of the quota will be.
- *Distinguish between color and black and white printing* – switching to Yes will allow you to set up separate quotas for color printing and other printing.
- *Total number of pages* – the total number of pages that are allowed to be printed within the period of time specified above.
  - *Action taken after quota runout* – here you can choose the action that will be carried out once the quota has been exceeded. You can choose from the following actions: Block printing immediately; Allow the last printing job to finish; Issue a notification.
- *Number of color pages out of total* – if you have selected differentiating between color printing and black and white printing, then here you can specify how many pages out of the total number of pages can be printed in color.
  - *Action taken after quota runout* – here you can choose the action that will be carried out once the quota has been exceeded. You can choose from the following actions: Block printing immediately; Allow the last printing job to finish; Issue a notification.

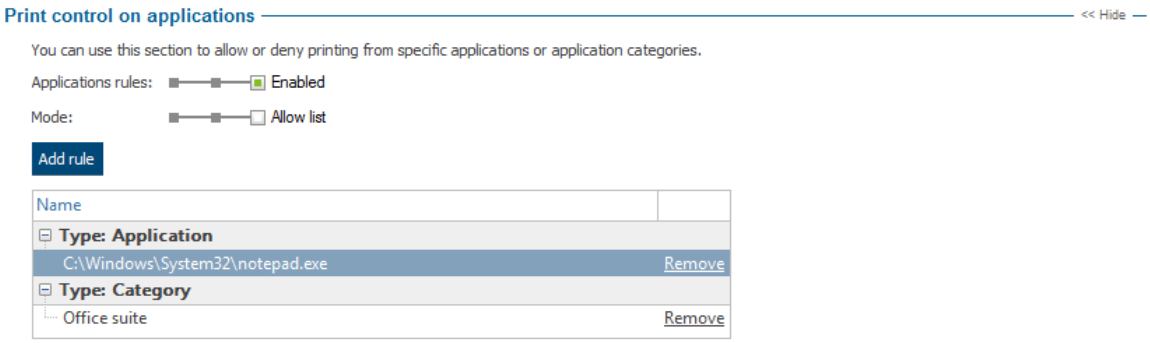
In the bottom part of the tab is a section labeled One-time quota increase. If you want to temporarily increase the quota, follow these steps:

1. Enter the number of pages by which the quota will increase.
2. Using the slider, determine if you want to allow or deny color printing.
3. Finally, set the validity time. You have three options:
   a. Today – temporary quota will apply until end of current day.
   b. This week – temporary quota will apply until end of current week.
   c. This month – temporary quota will apply
4. Click *Add* button to add the temporary quota to the list. Save and apply changes using 

Print control on applications

In this part of the application you can add the actual application or application category and further specify whether or not users will be allowed to print from them. You can do this by changing the type of the list. The list is either the list of applications that denied printing or the list of applications that are allowed to print.

Clicking the *Add* button will open up a dialog for entering the path to the application or whole application category.



Visualization

The data that you can see in the visualization mode is only shown for the users, computers or groups that you have selected in the user tree. The visualization mode is then divided into two sections. In the top part of the view is an area for rendering charts. Available charts for the current function can be found in the list on the right. Clicking on them and dragging them to the chart viewing area will show them. To remove a chart from the list, click on the button in the top right corner of each chart.

Available charts:

- *Top blocked printers* – the chart contains printers with the most blocked prints (up to seven printers are shown).
- *Top blocked users* – the chart contains users with the most blocked prints (up to seven users are shown).
- *Printer type* – the chart contains the number of prints divided by the type of printer. There are three types of printers: Physical printer, Virtual printer (like PDF Creator, XPS Writer, etc.) and Network printer.
- *Print blocking reason* – the chart contains the number of blocked prints divided by the reasons of for blocking. There are three types of reasons for print blocking: Application (printing is blocked for the specified application), Printer (printing is blocked for the specified printer), Quota exceeded (the print quota has been exceeded).
- *Blocked applications* – the chart contains the number of blocked prints form from applications.
- *Print control timeline* – the chart contains the number of blocked prints in over time.

In the bottom part is a table with detailed records. Each record contains several types of information represented by columns. The list of available columns can again be found at the right side of the table. Dragging a column from the list and dropping it at the table dropping it onto the table will view that column in the table. By clicking on the header of the column and dragging it, you can change the ordering of the columns in the table. Use the same method to drag column headers to the part above the table. The records in the table will then be grouped according to the type of the column above the table. To remove a column from the table, drag it back to the list of column list of columns on the right.

Available columns:

- *Date and time* – date and time when record was logged.
- *PC* – name of the PC where the record was taken.
- *User name* – the name of the user under whom the record was doneunder whom the record was made.
- *Application* – name of the application from which the printing was done.

- *Device name* – Name name of the printer.
- *Printer type* – there could be three types of printers: Local printer, Virtual printer (like e.g. PDF Creator, XPS Writer, etc.) and Network printer.
- *Document name*
- *Print blocking reason* – there are three types of reasons for print blocking: Application (printing is blocked for the specified application), Printer (printing is blocked for the specified printer), Quota exceeded (print quota exceeded).
- *Paper size*
- *Print color*
- *Duplex print* – printing from on both sides of the paper page at once.

You can also filter the records. To open a filter for a column of your choice, click on the button next to the header of that column. Enter text in the dialog that appears or choose an item from the list to filter the column by that item. Clicking on the + button will add the item to the filter list. This list can be of any length. After confirming the filter by pressing the OK button, the table will only show those records that corresponded to at least one filter in the list.

You can learn more about the settings and visualization interface in the chapter Logs and visualization.

6 SAFETICA ENDPOINT CLIENT

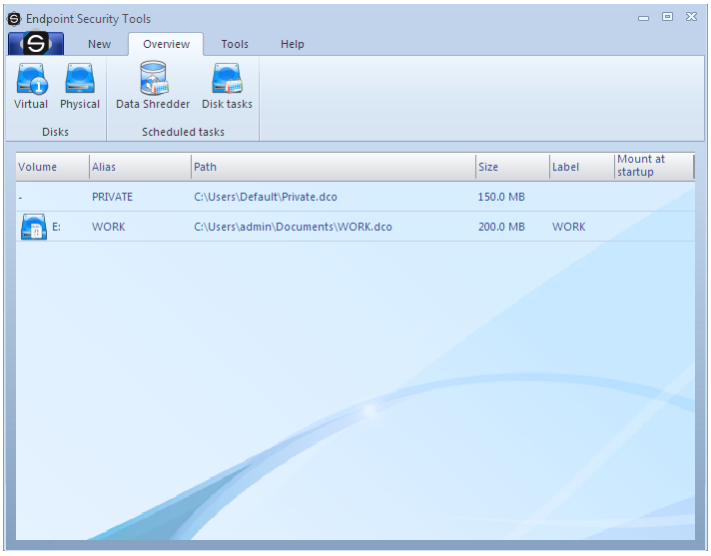
Safetica Endpoint Client is a part of Safetica. The module runs on client stations and allows the use of security tools and functions of Endpoint Security Tools on these stations.

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:

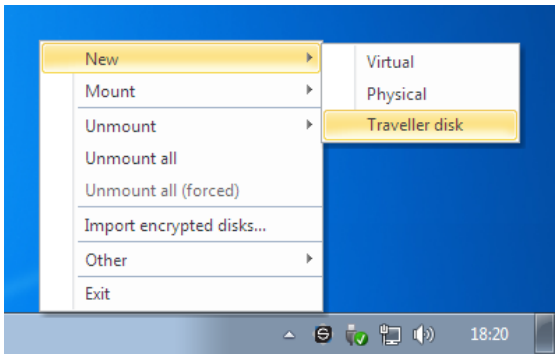
1. The Endpoint Security Tools user interface with all security tools and a contextual menu available by right click on in the tray.
2. Context menu mode (Quick menu) with no user interface and basic security functions.



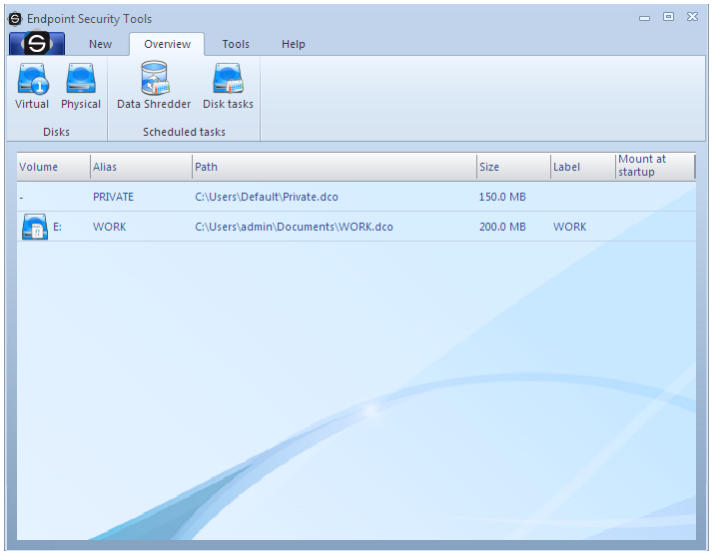
6.1 Endpoint Security Tools Description

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.



6.1.1 Overview

Tab Overview provides you menu with different overviews based on the description. There is a tab Overview on the image above.

1. Virtual disks

   This option shows a view of virtual disks only.

2. Physical disks

   This option shows a view of physical disks only.

3. Wipe Tasks

   Views wipe tasks.

4. Disk tasks

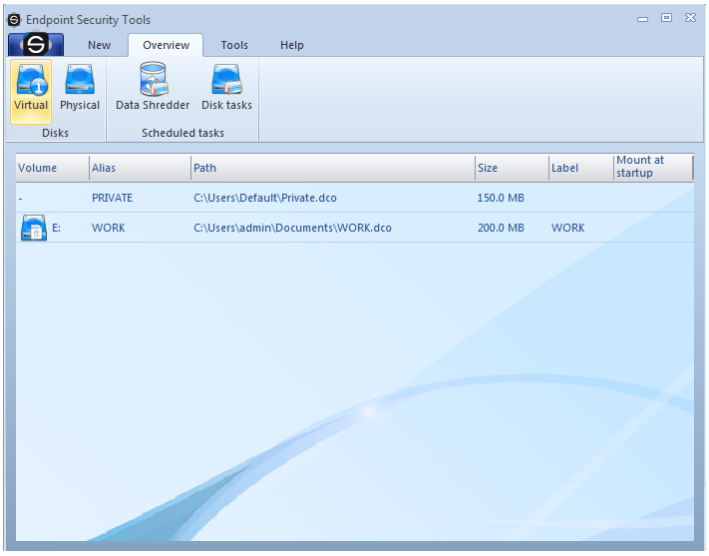
   Views disk tasks

Navigation buttons make for simplifying the orientation in the program, switching between individual views of disk types and setting up Safetica® properties. For more information on other navigation features click on individual options of a help.

6.1.1.1 Virtual disks

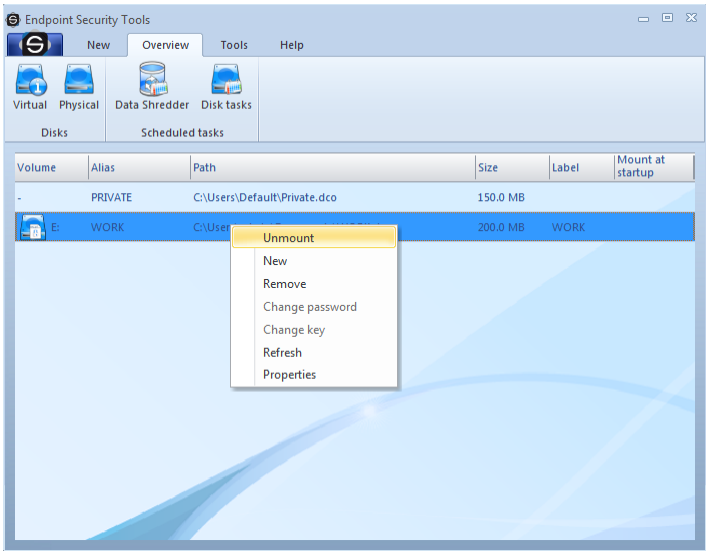
Virtual disk is a file encrypted by the Endpoint Security Tools software that behaves as a classical hard disk after connection. It means that you can create, modify, and copy files or otherwise work with your data on this disk. Furthermore, you can do low level operations with this disk such as formatting,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

Virtual disks make a favorite way of data encryption. You do not have to use the whole disk for encryption as you have to in the case of physical disks. You just need enough free space on the disk. A guide through adding a virtual disk creates a file, the content of which is interpreted by the operating system as a physical disk.



The view of Virtual disks shows an overview of the virtual disks available. After adding a file of a virtual disk click on a Quick Menu - search virtual disks. Afterwards, select a path to the directory, where the file with a virtual disk is located and confirm your selection.

It is possible to manipulate with disks via a subnavigation the same way as with the physical disks. A subnavigation consists of the following items:



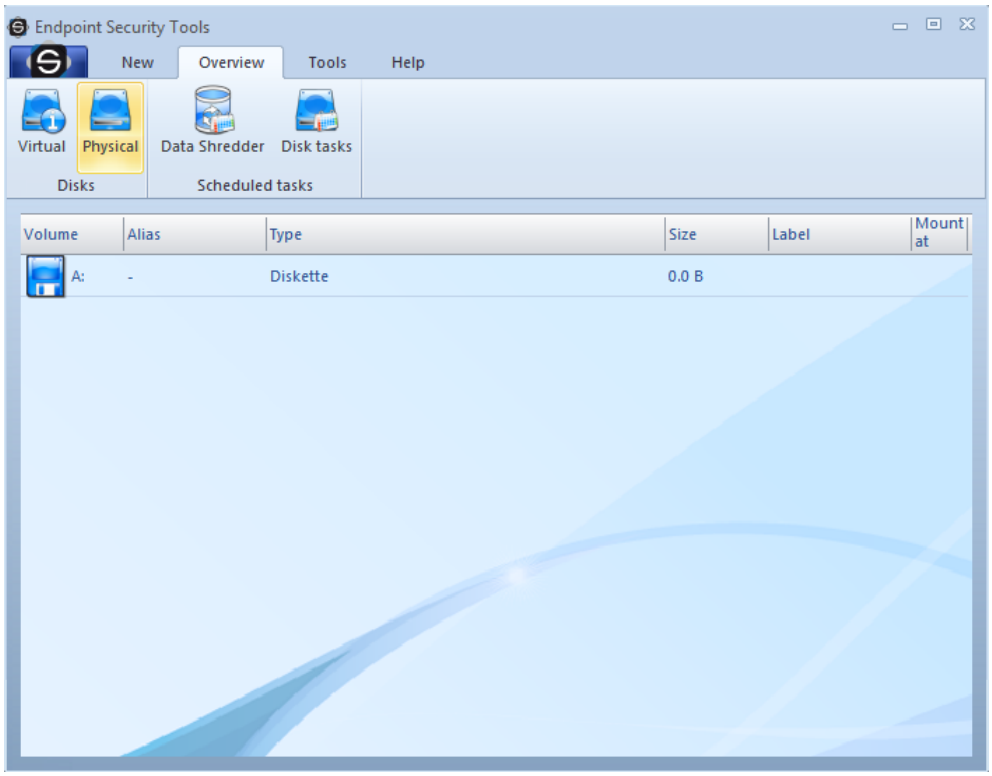
1. **Mount / Unmount** - The selected disk gets connected by clicking on this button provided that it is not connected yet. Otherwise, the disk gets disconnected.
2. **New** - Launches a guide that encrypts the disk selected.
3. **Remove** - Removes the encrypted format from the disk selected.
4. **Refresh** - Renews the information about selected disks.
5. **Properties** - Displays advanced information about a particular disk. Enables to change some disk properties.

6.1.1.2 Physical disks

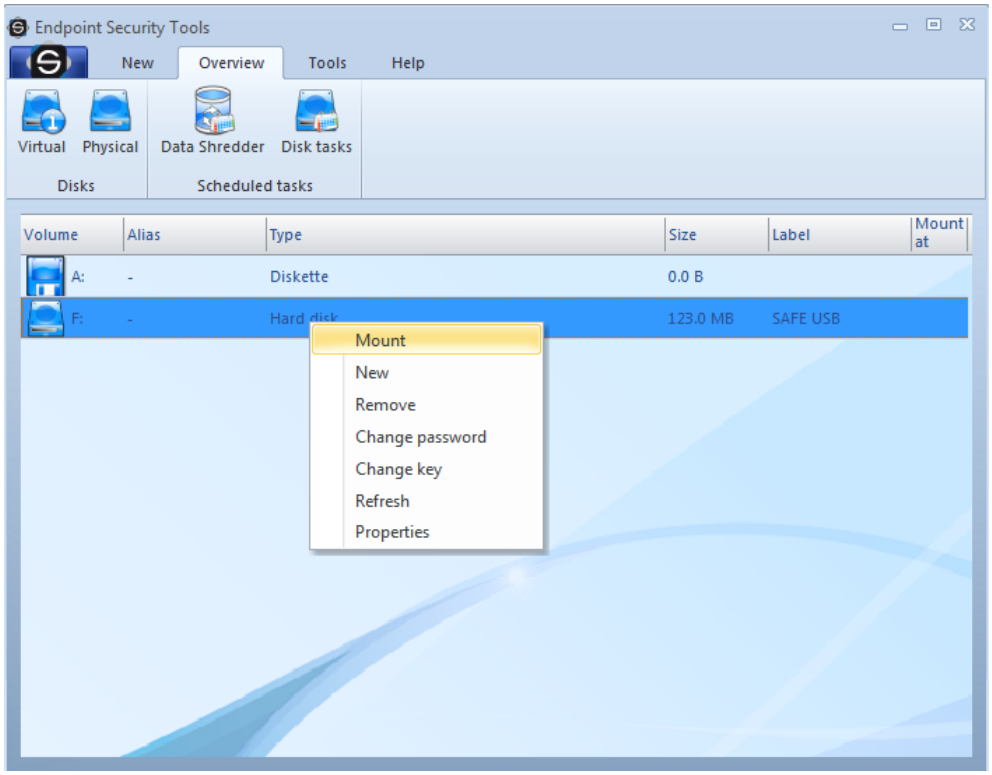
Physical disk is a medium capable of a random access. Namely, hard disks, disk partitions, exchangeable disks, flash disks, floppy disks 3,5", Zip drives etc. If you have a memory card reader, you can also encrypt any memory card. For example, Secure Digital, Compact Flash, xD-extreme Digital etc. But this is definitely not the end of the list of physical media. New and new types of stor-

age devices emerge on the market every day. The encryption system Endpoint Security Tools is able to secure these devices as well.

The view of physical disks on the desktop shows an overview of the existing hard as well as exchangeable disks, Flash memories and floppy disks of all types. Every disk is represented by one line with detailed information.



Before manipulating with disks a selection of a particular disk on the desktop is required. You can manipulate with disks via subnavigation that consists of the following items:



1. **Mount / Unmount** - If you click on this button, the selected disk gets connected provided

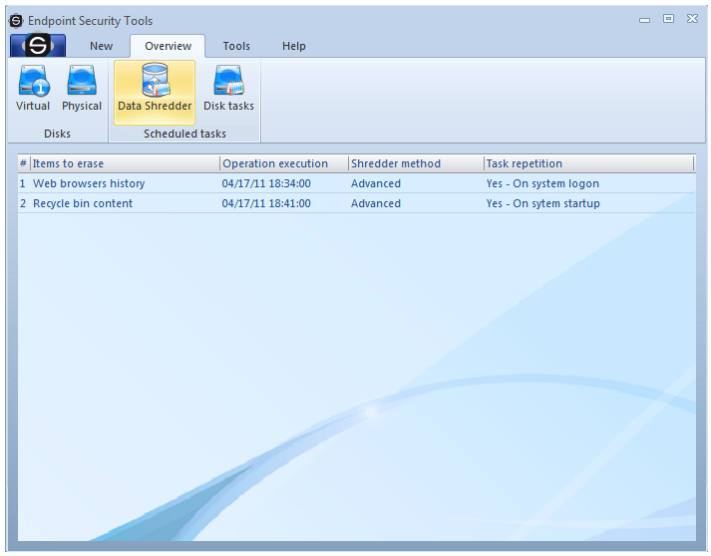
that it was not connected before. Otherwise, the disk gets disconnected.

2. **New** - Launches a guide to the encryption the selected disk.
3. **Remove** - Removes the encryption format from the selected disk.
4. **Refresh** - Renews information about the selected disks.
5. **Properties** - Displays advanced and useful information about the disk selected.

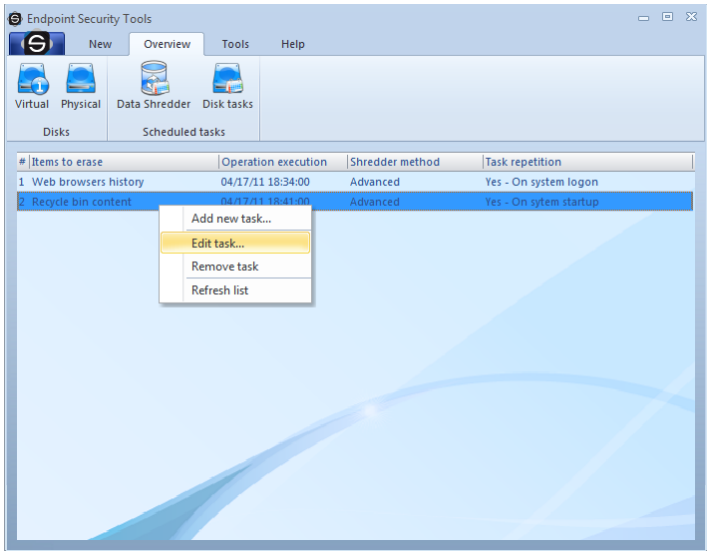
Note. Although the usage of the expression physical disk is not entirely accurate, it is used further in the text for simplicity.

6.1.1.3 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.

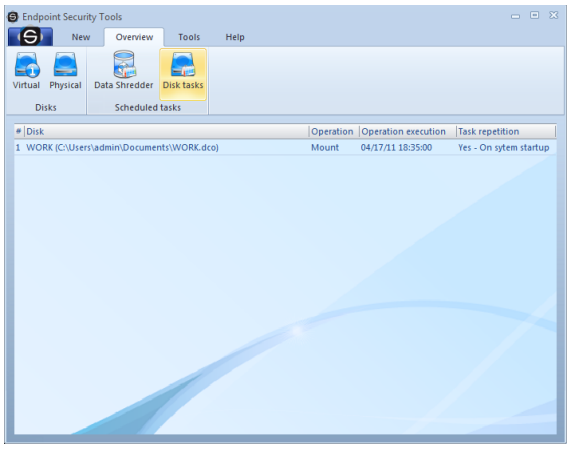


You can simply add or remove scheduled tasks.

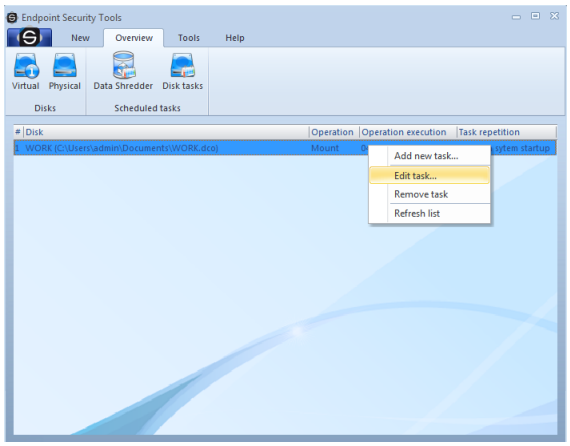


6.1.1.4 Disk tasks

With Endpoint Security Tools you can also create disk tasks. Disk tasks allows you to plan connection or disconnection of disks (to specific time, after logon). To view disk tasks, click the *Overview* tab and *Disk task* card.

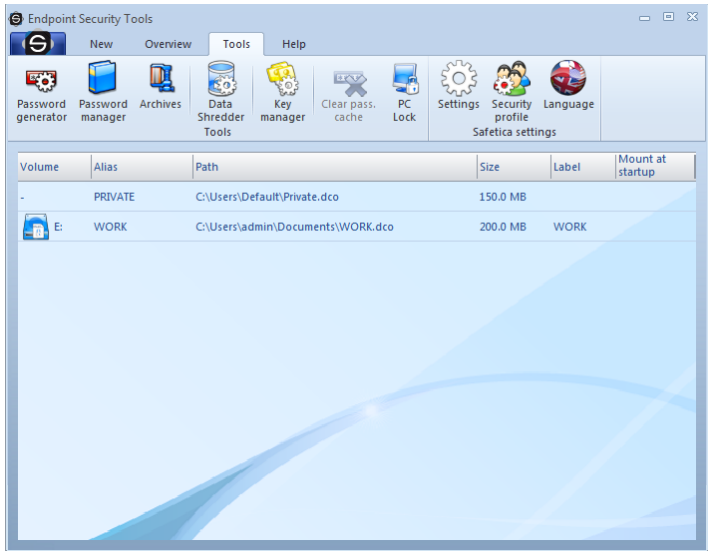


You can simply add, remove or edit disk by right-clicking on task in list.



6.1.2 Tools

The Tools tab mainly includes the access to Program Setting and to functions like Password manager, Archives, Key Manager or PC Lock.

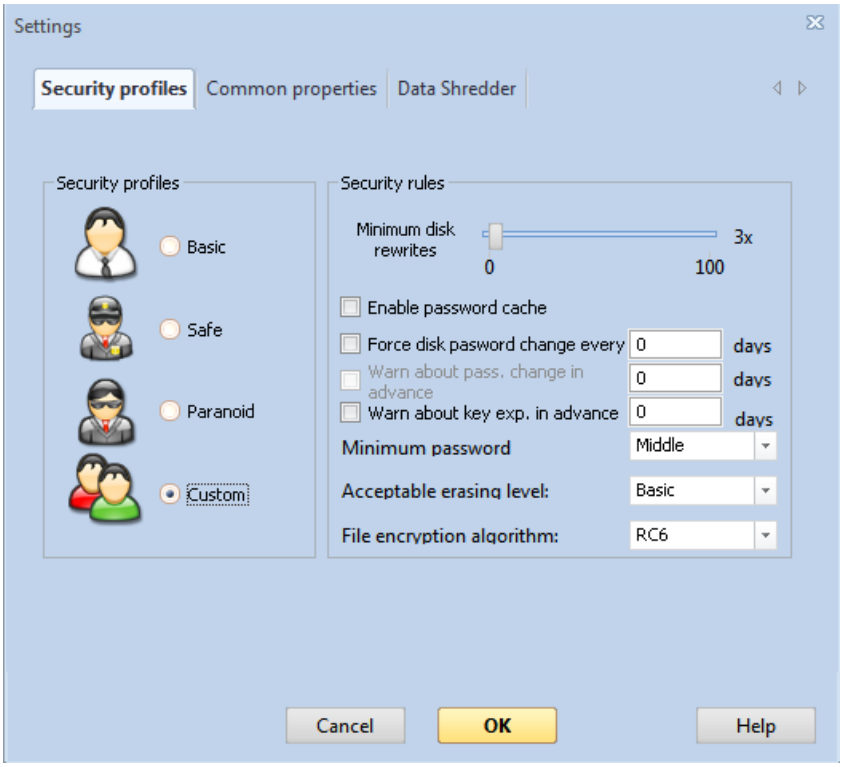


6.1.2.1 Settings

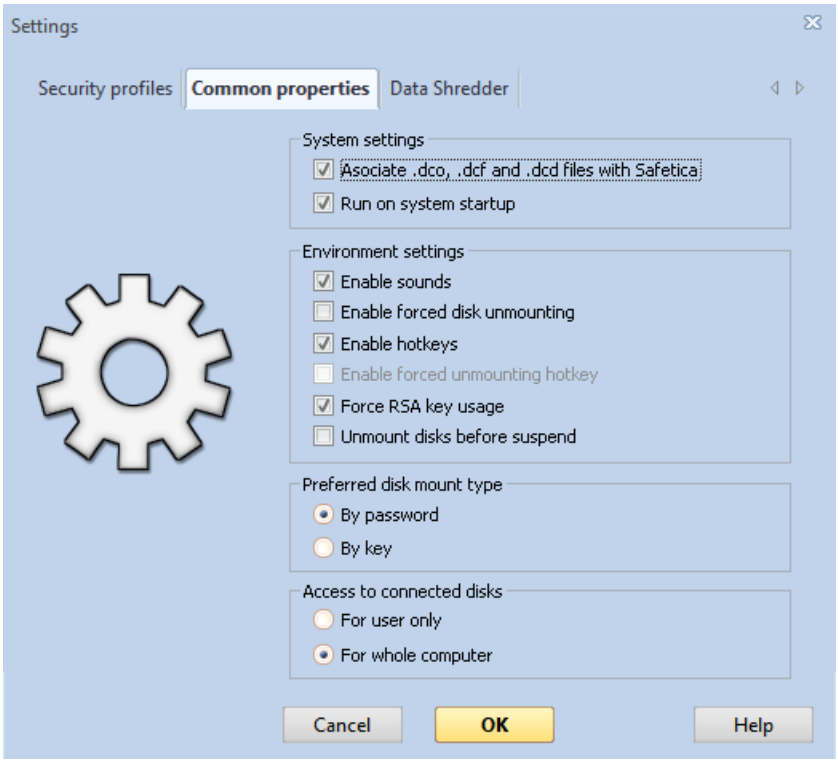
In the program setting you can switch on, off or change some useful options the Endpoint Security Tools offers. Thus it enables you to tune the program behavior according to your needs. You will be able to manage general and specific features as well as particular security functions.

Security profiles

Setting of security profiles is an option specifically for advanced users. In this setting you can change profiles from standard to User one by means of which you have set advanced security features on your own.



General features



From the system setting you can set general features related to your operation system.

- **Associate .dco, .dcf and .dcd files with Safetica**

  By clicking on a .dco type file in the Windows Explorer which is standard file of virtual encrypted disk of the system.

- **Run on system startup**

  Enables or restricts automatic launch of the Endpoint Security Tools jointly with operation system start.

  The Program setting enables you to better use the Endpoint Security Tools optional features according to your needs.

- **Enable sounds**

  Sets use of sound effects at various program activities.

- **Enable forced disk unmounting**

  Only advanced users are recommended to tick this option. This option enables hard disconnection of disks which means disconnection of disks even when the system works with them. This option is strongly not recommended because it may cause data damage on encrypted disks.

- **Enable hotkeys**

  Comfortable option for all users. By pressing the Win-Ctrl-U key combination you ensure disconnection of all disks in standard manner.

- **Enable forced unmounting hotkey**

  By the Win-Ctrl-Q hot key you ensure disconnection of all encrypted disks in hard mode.

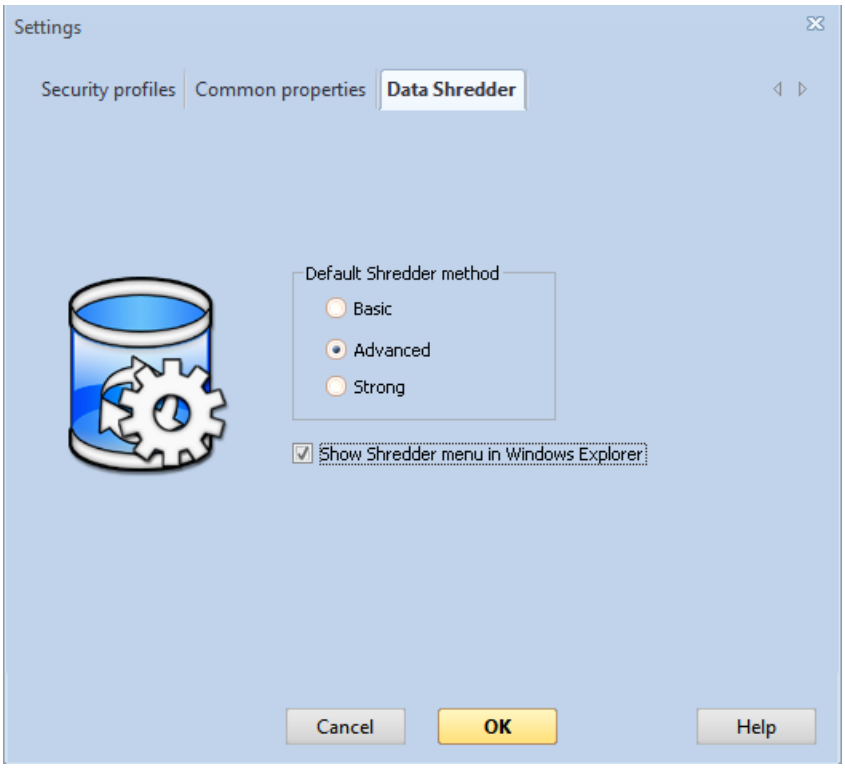
- **Force RSA key usage**

  By this option you will set the Endpoint Security Tools behavior so that the system will require use of security key at each disk creation from the user. This setting is suitable as prevention and possible rescue in case of password loss however it requires great caution. More in the

chapter Security keys.

Data shredder

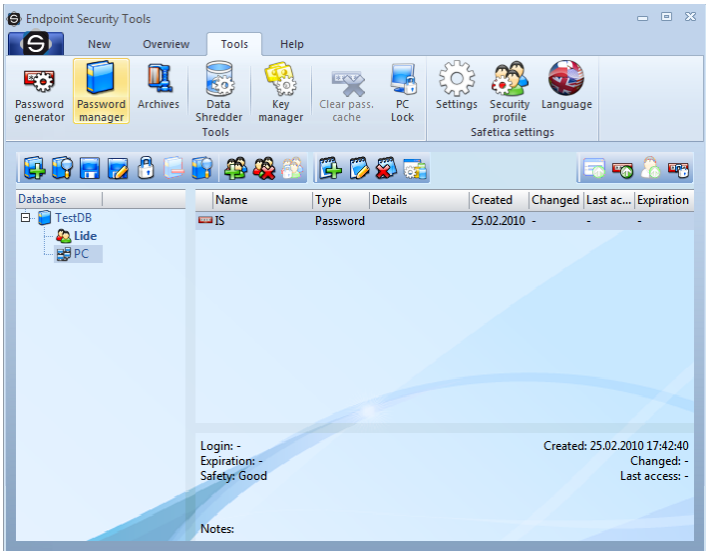
Setting of data shredder automatically sets the level according to the selected security profile. If you have your own security profile then you define the security of shredding algorithms on your own.



6.1.2.2 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.



There is the Tree of your databases and groups on the left, on the right in the main part the records and details of selected database, group or record are shown. This view is dynamically changed upon concrete selected item. There is a toll bar in the upper part, divided in groups according to functions for databases, groups and records. Rightmost on this bar there are functions for copying of record in the box or showing of passwords in detail.

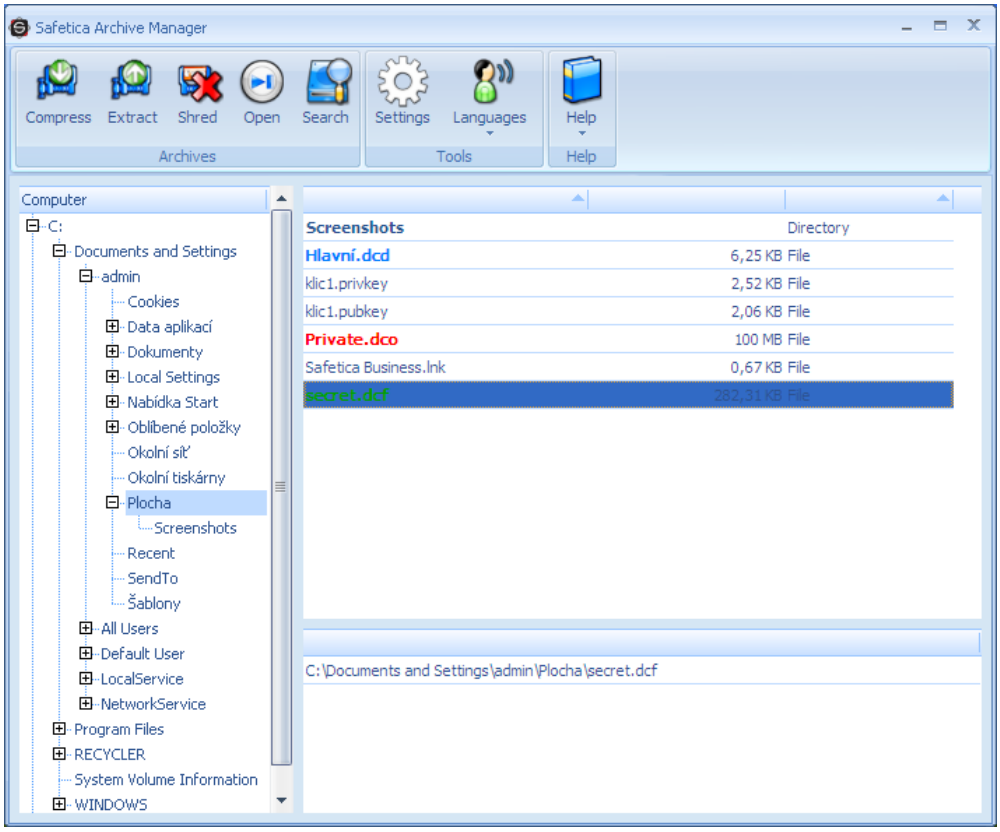
More detailed information on how to use the Password manager you will find in this chapter.

6.1.2.3 Archives

You certainly use the ZIP, RAR or eventually other archives. There are many expensive products supporting only archives and that do not offer any other options. In addition to the privacy security itself the Endpoint Security Tools also provides user with support of compression archives. The Endpoint Security Tools manages with all common archive files of ZIP, RAR, ARJ type and many others. Therefore you do not need to buy a separate and expensive compression software for nothing.

Endpoint Security Tools also supports the practical self-extracting archives. The data are simply packed into an executable file, transferred to another PC and unpacked by mere click and entering a password in. By use of self-extracting archives there is absolutely no need to use the Endpoint Security Tools software in target computers.

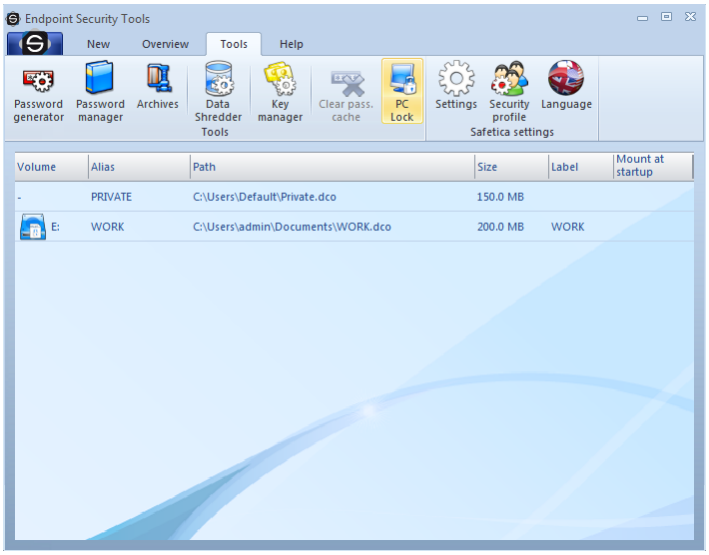
Beside the safe DCF format you can easily archive data in favorite type like: ZIP, GZIP, TAR, BZIP2. With Safetica Archive Manager you easily unpack common formats like: RAR, ZIP, CAB, ISO, ARJ, LZH, CHM, Z, CPIO, RPM, DEB and DCF.



6.1.2.4 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.



You can make your unique key for access to your PC from any common flash disk. Compared to common locking of PC by the Windows system the locking within the Endpoint Security Tools is quicker and far more secure. You do not have to be afraid of key copying onto other disk, the Endpoint Security Tools will recognize any attempts for key duplication.

Use

1. In the Tools tab select the PC Lock option.
2. Select from menu your flash disk which you plan to use as a key (if you still have not inserted it you can do it just now, the program will recognize a newly connected disk).
3. Press the Lock station button.
4. Take the flash disk you have selected as your key out of your PC. As soon as you make it the PC will lock itself and maximized window in Safetica colors will be displayed.
5. For repeated unlocking insert the flash disk you have used as your key.

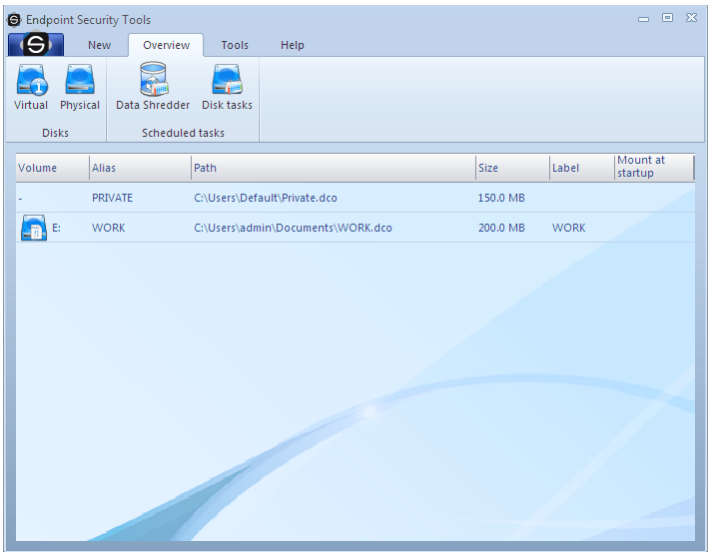
Advanced - opens advanced options settings

- Generate token - it will generate token and save it onto selected Flash disk. The token serves to correct Flash disk identification at unlocking of the PC.
- Verify the token - it will verify if correct token is saved in the Flash disk.
- Delete token - it will delete the token from the Flash disk.

Important: if the Task manager is on, you have to switch it off. If not it will not be possible to lock the PC.

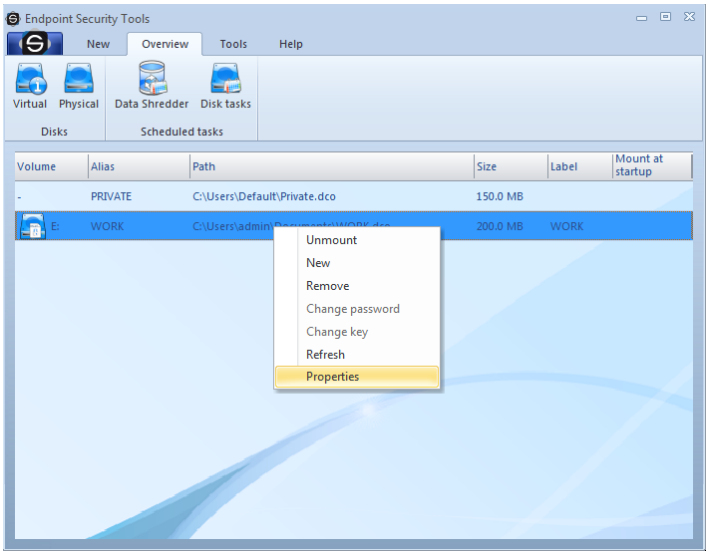
6.1.3 Desktop

The desktop includes the list of all encryptable disks. It also includes a detailed description of disk properties such as drives, labels, sizes, disk types, cipher types, and connection modes.



All important information about a particular view of an encrypted disk is collected on the desktop.

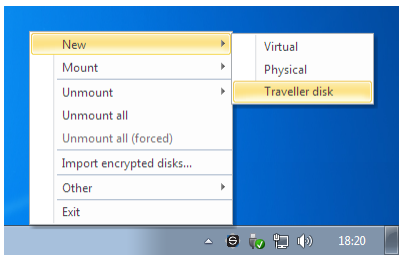
Each line corresponds to one item.



Right-clicking on the desired disk brings up a menu for working with this disk. This menu is variable according to the view.

6.1.4 Quick Menu

The quick menu can be opened by right-click on the following icon in the tray. It allows you to perform the following operations over encoded drives (virtual, physical):



- ***New*** - you can create a new *Virtual, Physical* or *Traveler disk.*
- ***Mount*** - drive connection menu.
- ***Unmount*** - drive disconnection menu.
- ***Unmount all (force)*** - everything is disconnected, even if the drives are currently working. Data loss may occur.
- ***Import encrypted disks...*** - Opens the dialog for a virtual drive import.
- ***Other*** - allows other operations over drives:

  Remove - selects the drive to be removed from a list.

  Properties- *displays* the properties of the connected drive.

  Change password - select the drive for password change.

  Change key - select the drive where the security key should be changed.
- ***Exit*** - Closes the Safetica Endpoint Client graphical interface (the client service keeps running).

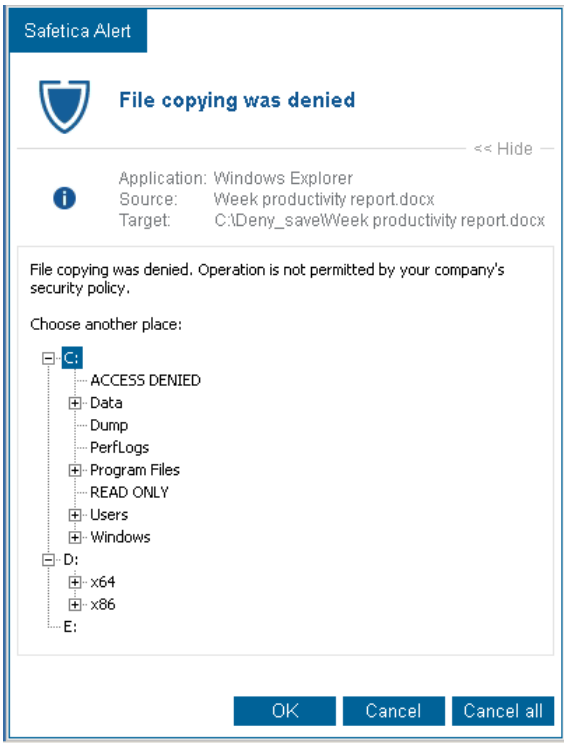
6.1.5 User Dialogues

Using the announcement dialogs, Safetica Endpoint Client displays for the end users messages about forbidden or allowed activities or displays queries and notifies of important events.

The dialogs display in the lower right corner of your desktop. There are several types of announcement dialogs. Individual types of dialogs require different interaction with the user (confirmation, rejection, selection from options or paths).

Description of announcement dialog

The announcement dialog has its name included in the header. In the center is the name of the announcement with the announcement itself. Below the announcement are buttons for confirmation, cancellation and other buttons depending on the announcement dialog type. In the lower left section you can switch between the announcements if there are more unread ones.

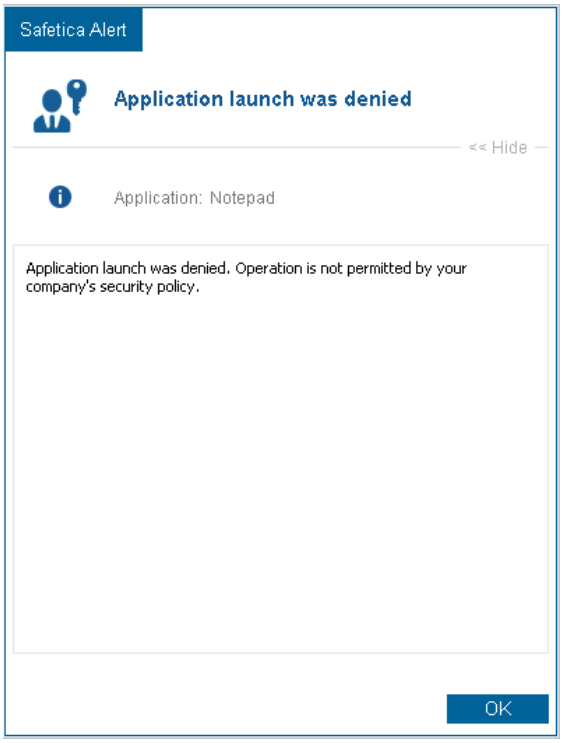


Types of announcement dialogs

Notification dialogs

Information dialogs only inform you about the situation that occurs. Such as blocking of a forbidden application or a USB disk.

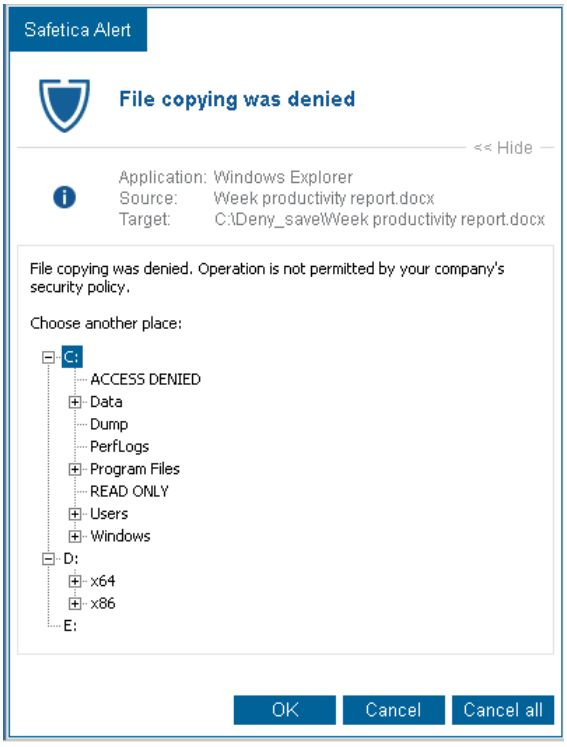
Following is an example of dialog:

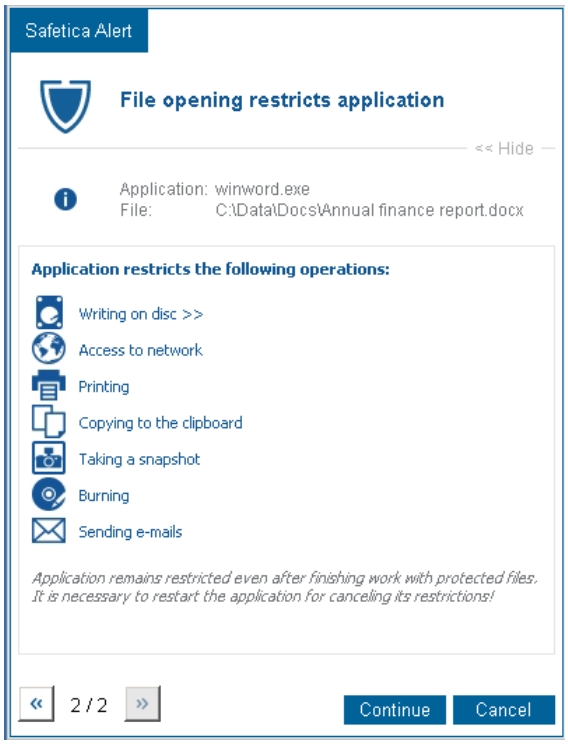


Query dialogs requiring larger intervention of the user

This type of a dialog is displayed only by the DLP module. In addition to the read confirmation as in the previous type these dialogs require a more extensive action. For example, when copying a secured file to an unsecured location you are notified of this fact and you can select a secured target location etc. The options you will have at disposal depend on a type of the particular action.

Following is an example of dialog:

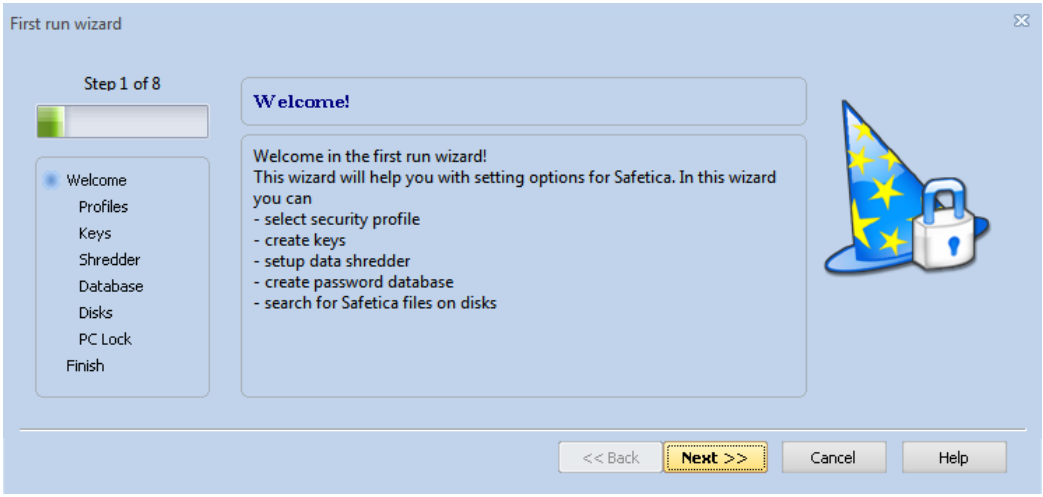


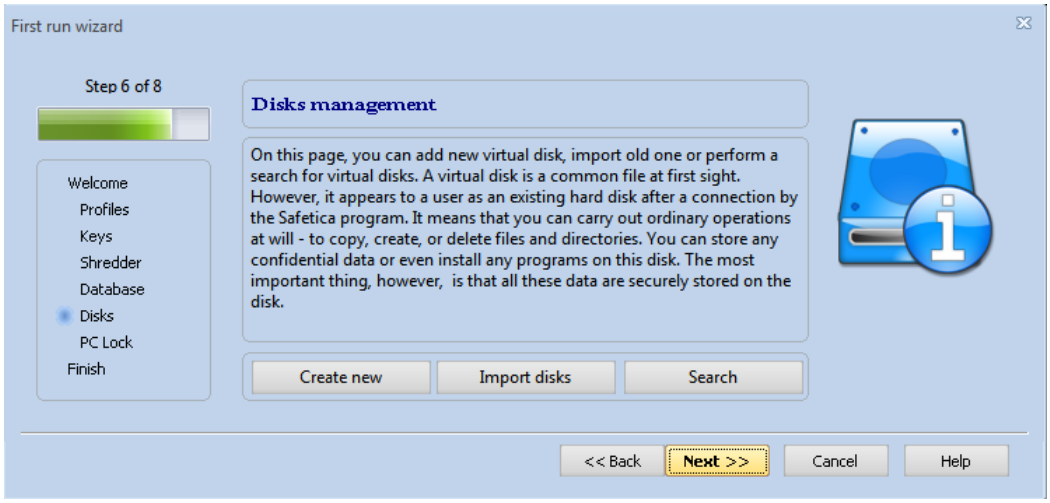


6.2 Using Endpoint Security Tools

6.2.1 First launch

For acceleration and improvement of work with the Endpoint Security Tools the program will guide you by first run wizard. It will reliably guide you through the Endpoint Security Tools so that even a less experienced user can use it. From selection of security profile through formation of access data database to creation of virtual disk or import of old settings.





Having finished the wizard the Endpoint Security Tools welcomes you by its main window. After first run we recommend to study the Help first in order you are able to control the Endpoint Security Tools even more easily. Therefore select in the Help tab the item Help topics.

You will also find the contact button here which will direct you to our pages with contacts to technical support. You can also display Tips of the day which are shown after the start. If you want to pass again through the program setting, create new disks, databases or keys in one step, use again the First start wizard.

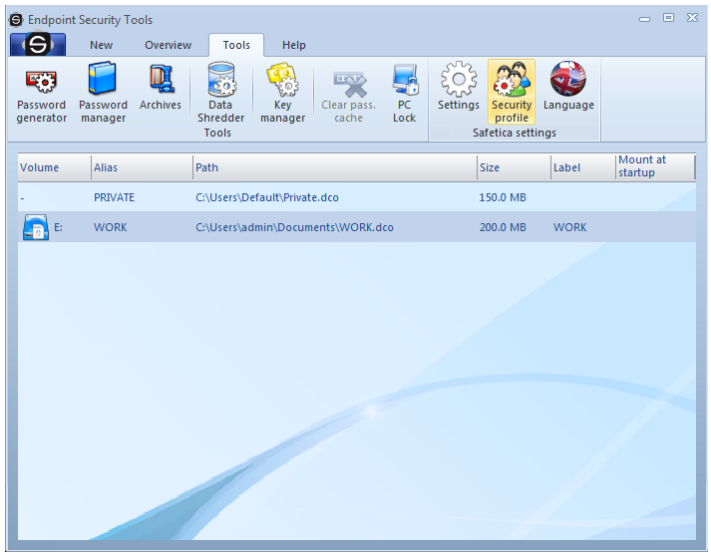
If you wish to secure your disks, continue by clicking the chapters about disk creation: How to create a physical disk, New virtual disk creation.

6.2.2 Security profiles

Security always begins with the choice of a good and a high quality password. Another choices - such choosing of cipher algorithms and levels of shredding-are recommended much more for advanced users. Common user does not have to bother with these particular settings and can let

Endpoint Security Tools to set it for them. Endpoint Security Tools will offer you a choice from prepared security profiles - from the basic up to the most safe one.

For advanced users there is a Custom profile, where you can set every part of security feature yourself, after choosing this profile, the settings will be available in Settings section. In the tab Tools select Security profiles.



The wizard helps you to select the right profile for you.

Security profiles:

- **Basic** – Allow medium level of passwords, automatic choice of quick and safe cipher and data shredder with 3 cycles.
- **Safe** – forced use of high level passwords, the AES cipher will be used (winner of the new encryption standard), data shredder with 7 cycles, permitted password remembering.
- **Paranoid** – password remembering is not allowed, data shredding in 35 cycles (according to Gutmann standard of department of defense of USA), used the most safe block cipher Serpent and forced frequent password changing.

For common use it is just enough the Basic profile, but we recommend the Safe profile.

6.2.3 Security keys

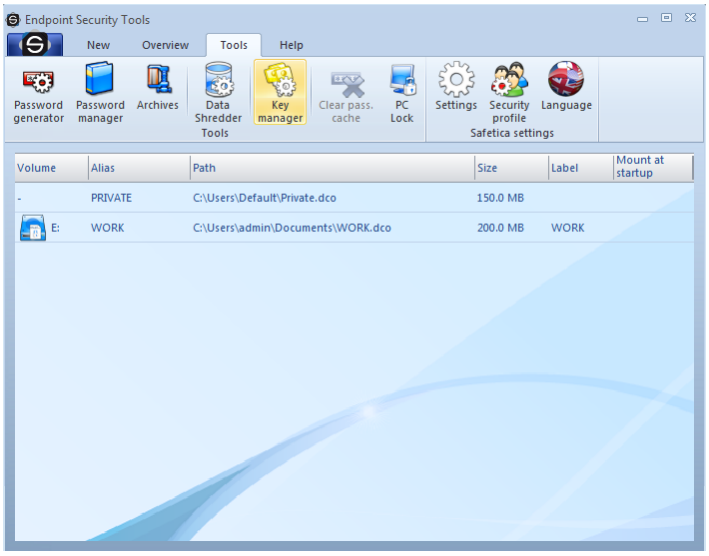
An important feature of the Endpoint Security Tools is the possibility of restoring the user data from the virtual disks, as well as the physical ones. The security key is in case of forgetting the password the only possibility, how to make an access to your data.

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.

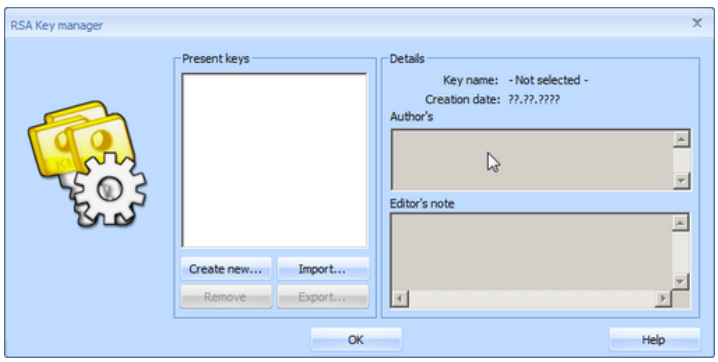
Every security key pair is mutual. If you create more security keys (pairs - the private key and the public one), only the corresponding pairs will cooperate. With the concrete public key you interlock only one concrete private key. You can use the private key to lock only these disks, which are locked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

6.2.3.1 Creating of the Security key

When you first run the main Endpoint Security Tools, there will be a question about the possibility of creating your security key. In the Key Manager dialogue you can create the security key manually - in the menu click on the *Tools -> Key Manager.*

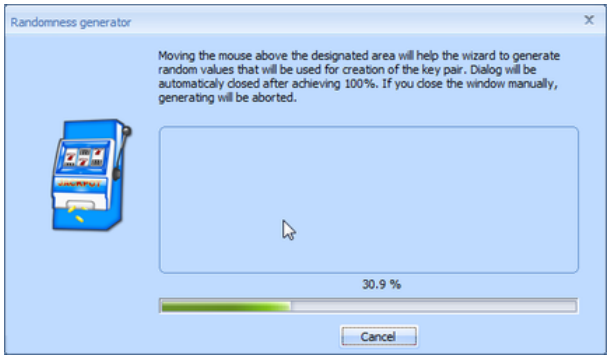


If you haven't created a security key yet, click on the Create new button.

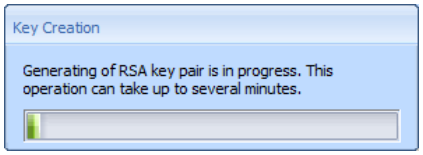


The creating of the security key wizard will guide you through the process step by step. In the first step the wizard asks you to do an unusual thing. In the middle of the dialogue an empty rectangle will show up. You will move the mouse cursor randomly as to how the image shows you. The wizard gains amounts of random data, so that he can ensure a generating of a high-quality key to your

disks.



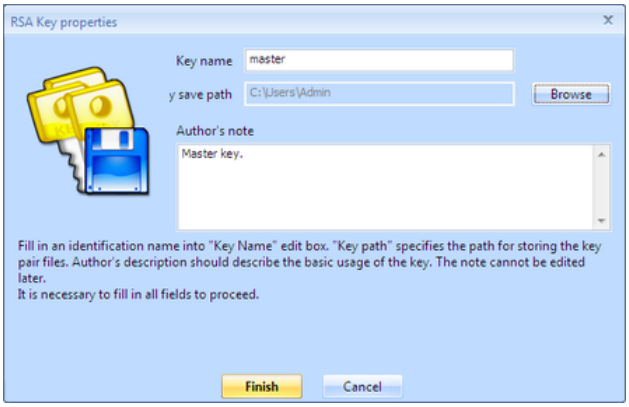
Once the sufficient amount of random data is gathered, the wizard immediately starts the generating of the security key. This operation may take several minutes depending on the speed of your computer.



The key is now created. The wizard asks you for entering the name of the key as well as its description, which you can use, when you want to recognize it. Now click on the Browse button and choose a secured place, where you save the file with its private key.

WARNING!

It is necessary to save the private security key to maximum secured and reliable place within the range of possible attacker. Using the private security key it is possible to unlock the data on your disks, which are created using the security key. Devote to choosing of the place maximum precaution.

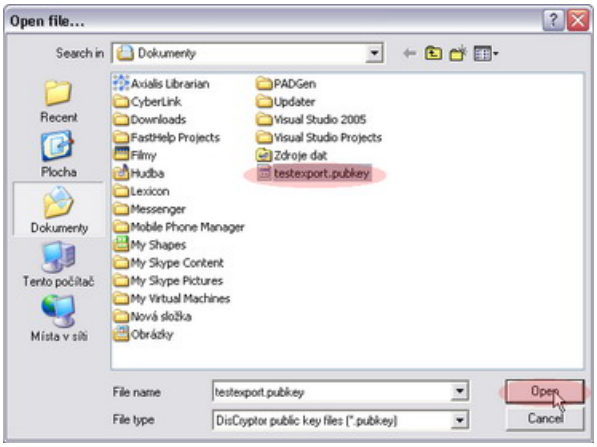


As soon as the choosing of the place is complete, click on the Save button and finish the wizard by the Finish button. If everything went well, the dialogue about the successful saving of the private key will show up. Now click on the OK button. Now your security key has been placed to the Endpoint Security Tools, you can abandon the Key Manager.

6.2.3.2 Key administration

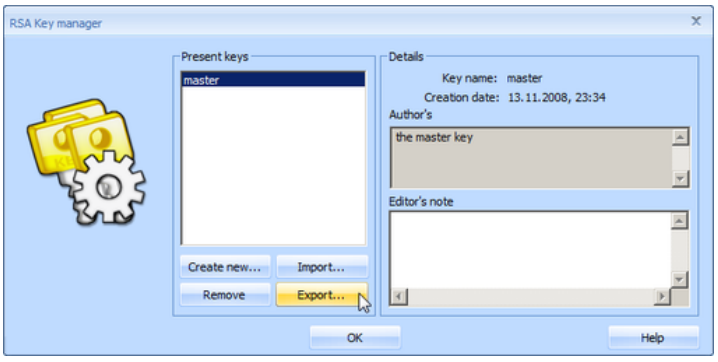
The main administration of the security keys you can perform in the Key Manager - in the menu click on the *Tools -> Key Manager*. If you are the server administrator, you can force the user to use the key.

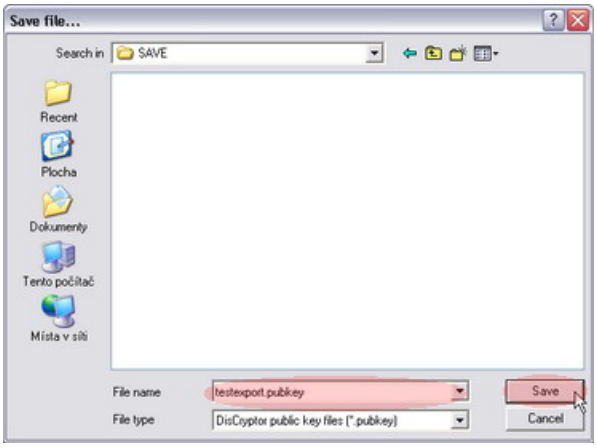
After the addition of the created public security key click in the Key Manager on the Import button. Choose appropriate security key and confirm this by clicking on the Open button.



Exporting of the created key

For the distribution of the public key it is necessary to export this key to the file at first. Choose the key in the table and click on the ***Export*** button. In the dialogue choose a file, which will be used for saving the key and click on the ***Save*** button. Keys exported this way you can distribute e.g. on another computers in your whole network.

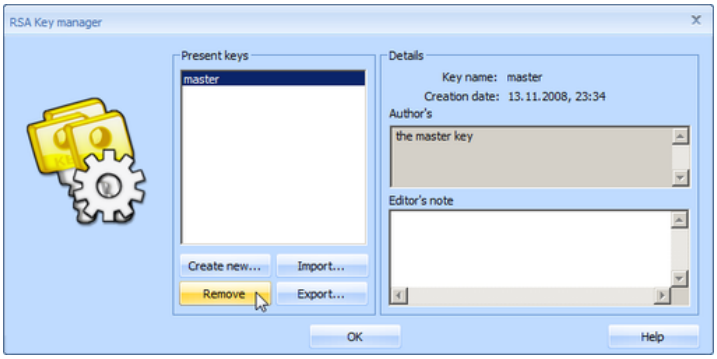




Deleting of the security key

The existing keys you can also erase. Choosing the key and clicking on the Remove button you erase the public security key from the list. The Key manager allows you only erasing of your public security keys. The private keys keep untouched. You can therefore restore data from the disks by the private key.

But by erasing of the present keys list you will no longer be able to create alike disks for the restoration by the same private key! Thus we don't recommend removing the keys!



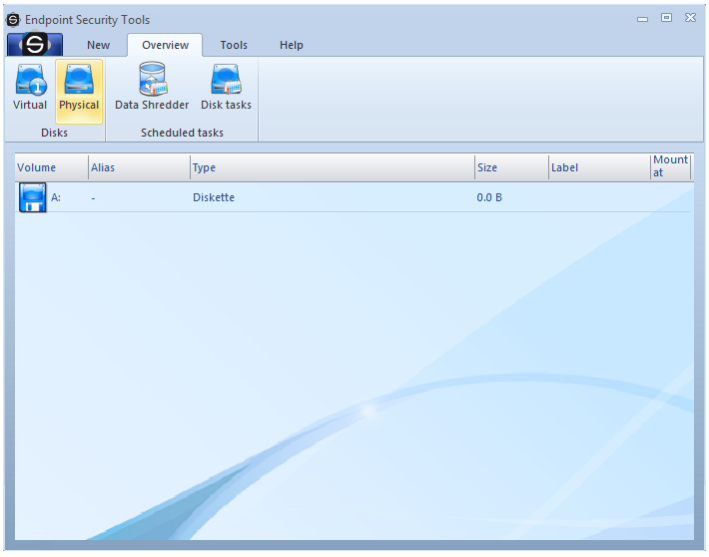
6.2.4 How to create a disk?

6.2.4.1 Encryption of an existing physical disk

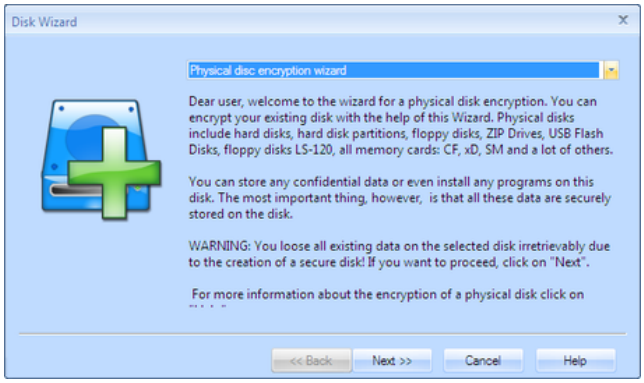
Physical disk is an existing disk of the following type: hard disk, USB disk, flash disk, floppy disk 3.5", ZIP Drive, memory cards, and a lot of other types of exchangeable disks. Physical disk is also a hard disk partition. Endpoint Security Tools is able to encrypt all of these devices very easily.

WARNING: You lose all original data by encryption. Do a backup of all data prior to the encryption! After the encryption process is finished, you can copy your data back to the encrypted disk.

In order to encrypt a physical disk, click on the navigation button Physical disks, select the disk you want to encrypt on the desktop and click on the subnavigation button New. Then a guide opens that guides you step by step through the encryption.

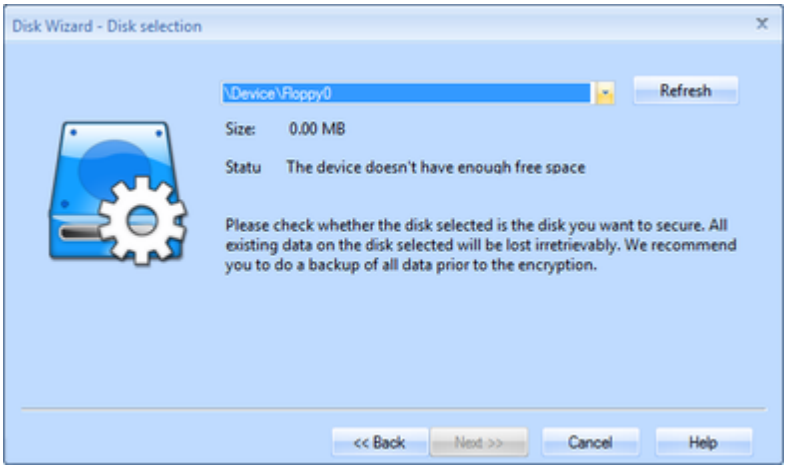


After you read the information on the first page of the guide, click on *Next*.

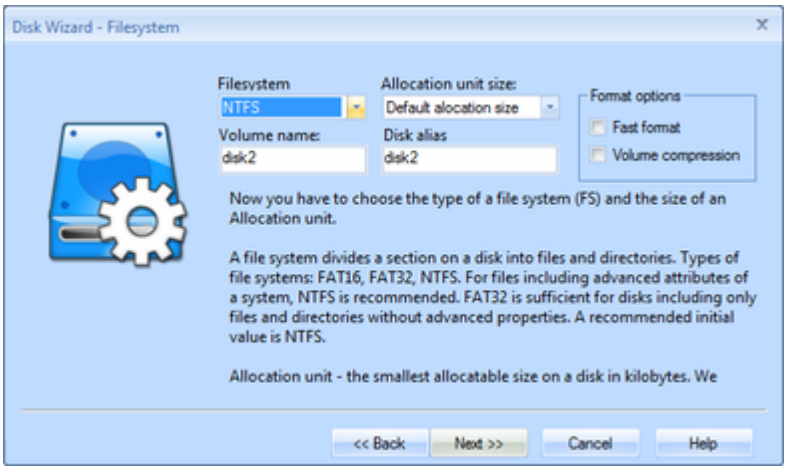


In contrast to a virtual disk, the size of which you can choose at will, a physical disk always has a fixed value.

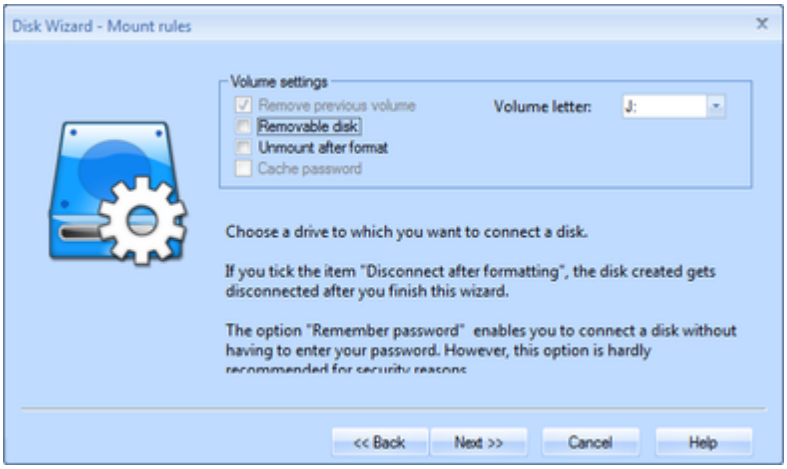
Check whether the disk you selected is the disk you want to encrypt. Then click on ***Next***.



Now you have to choose a file system, an allocation unit and a disk label. If you want to encrypt a physical disk or its partitions, the NTFS file system is highly recommended. We also advise you to set the size of an allocation unit to the *initial size of allocation*. For exchangeable disks, in particular for those of smaller size, FAT32 is enough. After you perform these actions, click on *Next*.



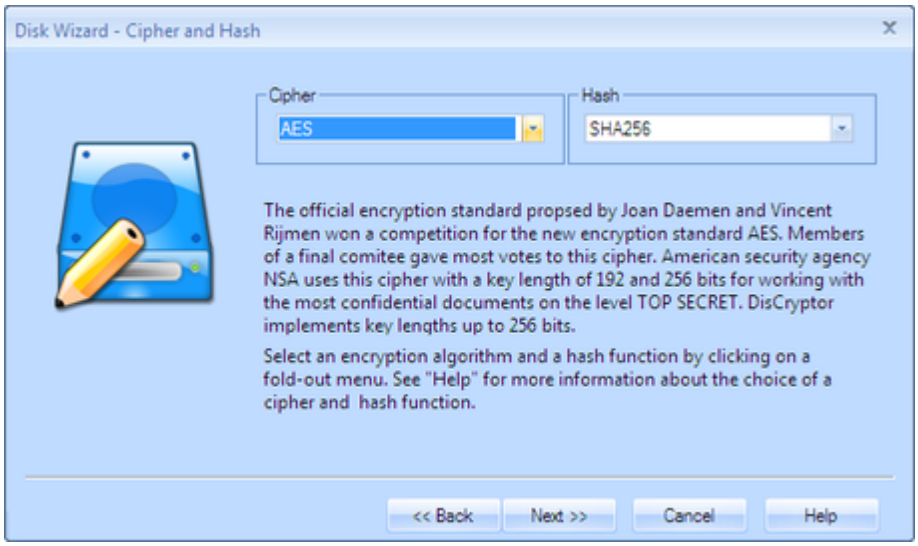
In the next window you can choose a drive you want to connect a disk to or you can just keep previous settings. After you finish your selection, click on **Next**.



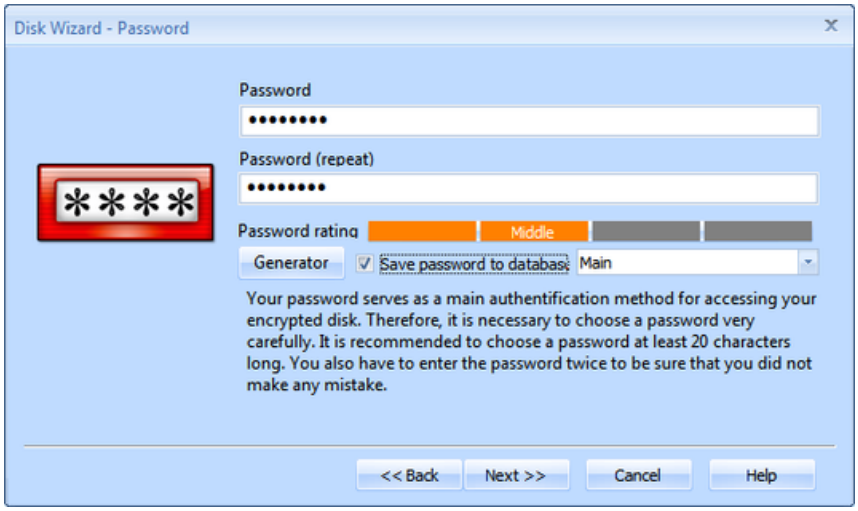
The next step is the choice of ciphers. You cannot make a mistake whichever cipher you choose. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed.

In case you save very risky stuff or programs, we recommend you to use the following ciphers: Serpent, Twofish, Rijndael(AES) or Blowfish. On the contrary, for less inhospitable conditions, and for frequent and bulky file transfers the RC5, RC6, or Twofish are recommended. These ciphers excel not only in security but also in the speed.

Generally, we have to point out, however, that the choice of a cipher itself is a secondary matter. Above all, we recommend you to choose your access password very carefully. You can learn more about the security of ciphers in the chapter Frequently asked questions. To confirm your selection click on Next.



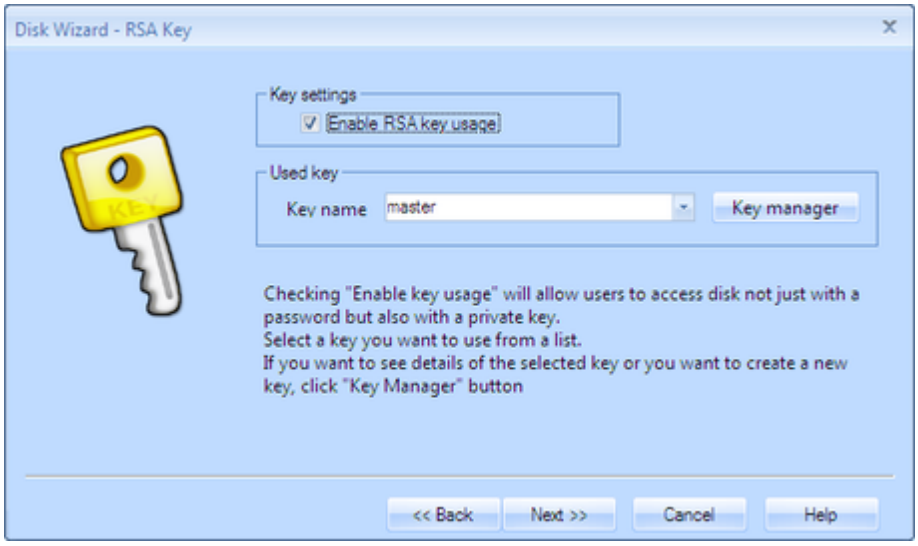
A key decision in the whole guide is the choice of a suitable password. There is a special chapter on this topic. To generate a safe password can you use the Password generator, which is integrated in the dialog. Your password can be immediately stored in any database or group in the Password manager. Before you choose a password, we recommend you to study materials given here. Generally, it is recommended to choose a password with al least twenty characters. After you enter your password and re-enter it for verification, click on Next.



The wizard has automatically generated the disk key, which will be used for the encryption of the disk.

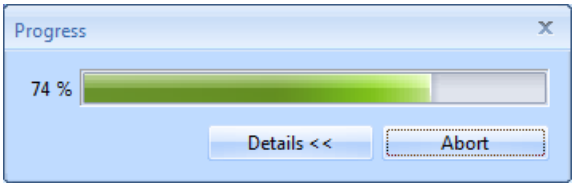
According to the program settings you can or must choose the using of the rescue security key for the creating disk. This security key is used for the access to the creating encrypted disk in the case of forgetting its access password. It is therefore a rescue fail-safe, but it is necessary to treat with it very carefully. If the security key comes at unwanted, the attacker can easily abuse the disk, on whose the security key is used. In the case in the Endpoint Security Tools exists no security key, the wizard will be automatically engaged. You can create or import a key in this wizard. You can allow using of the security key by ticking the Allow using of the security key and choosing the key from the highlighted menu. When the choosing is finished, click on the *Next* button.

You can learn more about the security key problems in the Security keys chapter.

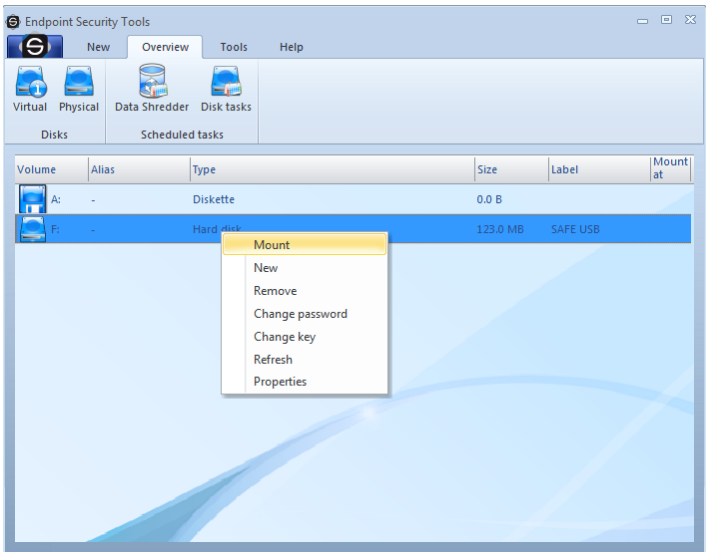


Check the entered data for the last time and click on the *Finish* button.

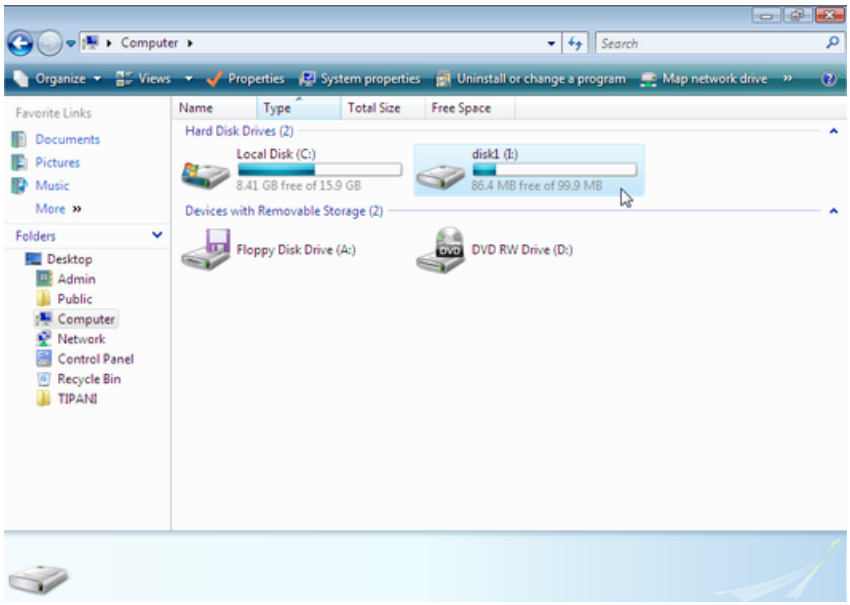
It is also necessary to format a disk before you use it. The guide is just doing it for you.



Congratulations! Your physical disk has just been encrypted and connected automatically. The highlighted line displays the newly encrypted disk. You can open this disk by a double-click in Windows Explorer. If you want to connect this disk later, simply click on the view of Physical disks in the navigation, right-click on the line with this disk and select Connect.



This disk will show up in the system as a drive you selected in the guide, in our case drive I: From now on you can use this disk as any other disk. If you click on "My computer" in your Windows system, your encrypted disk will be displayed together with other disks.



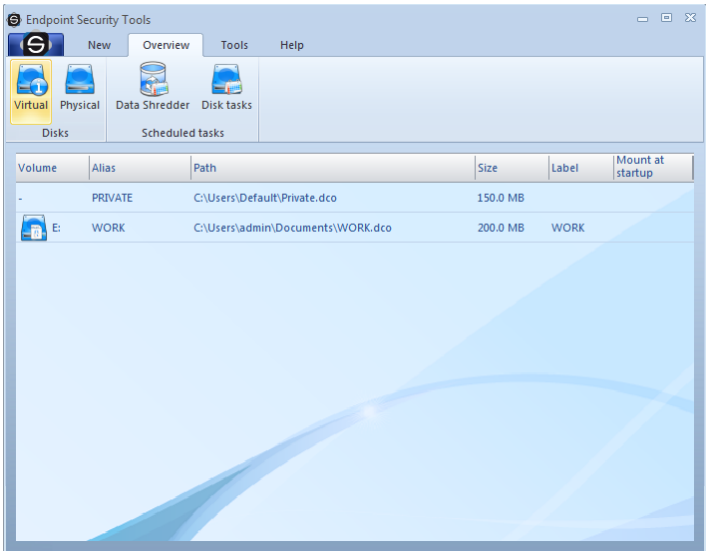
6.2.4.2 Creating a new virtual disk

Virtual disk is a file encrypted by the Endpoint Security Tools, which behaves same as an existing physical hard disk after connection. It means that you can create, modify, and copy files or otherwise work with your data on this disk. 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.

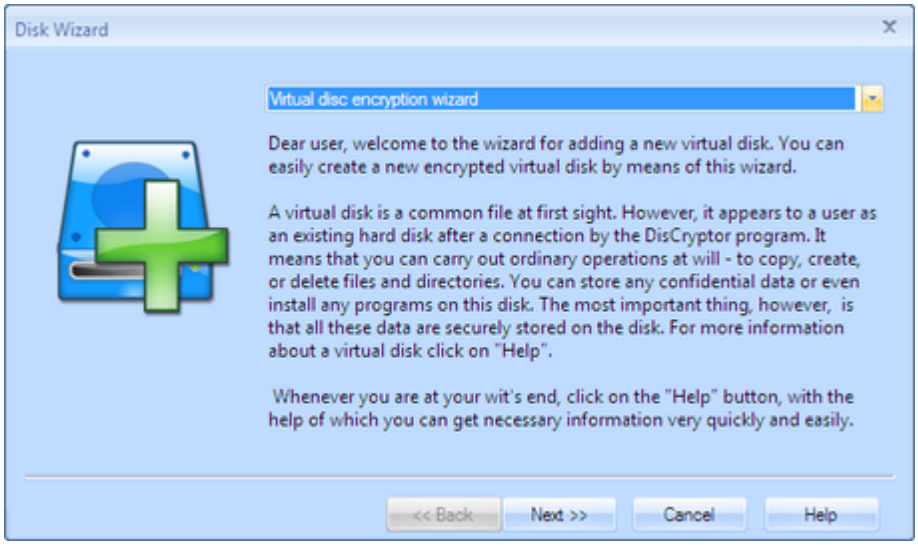
If you want to make your data accessible even on computers where the Endpoint Security Tools is not installed, choose the guide to a Travel disk. This utility of Endpoint Security Tools prepares a directory with a file of a virtual disk. Later on you can burn it on a CD/DVD or save it on another memory medium. If you insert this medium into a computer, you are automatically requested to enter your access password. After you do so, Endpoint Security Tools enables you to access your

virtual disk.

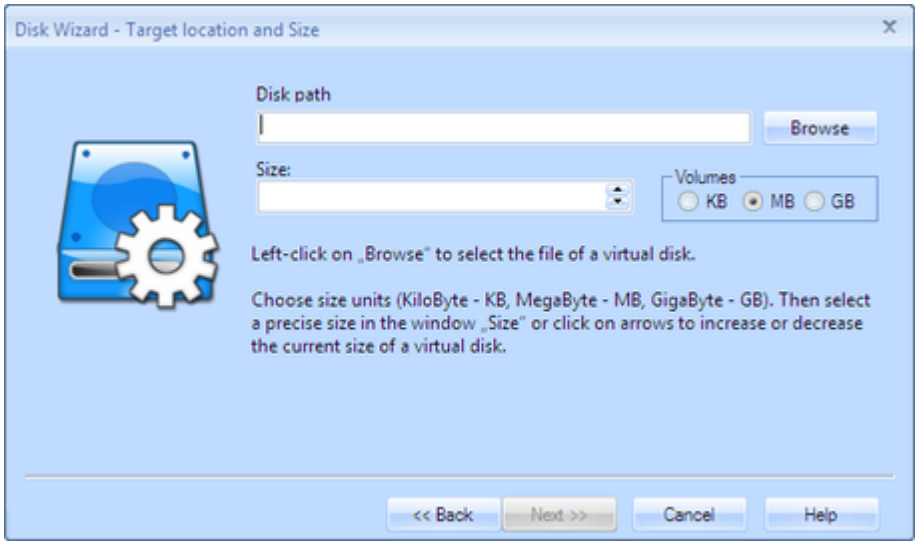
In order to create a new virtual disk, click on the navigation button Virtual disks and the subnavigation button New. A guide to adding a virtual disk opens. This guide is an ideal aid, with the help of which you can quickly and easily create your secure virtual disk. The guide prepares, creates and formats the disk on its own. It also helps you with key choices you have to make throughout this procedure.



In the first step the guide welcomes you and gives you a brief information about a physical disk itself and about its creation. Click on ***Next***.

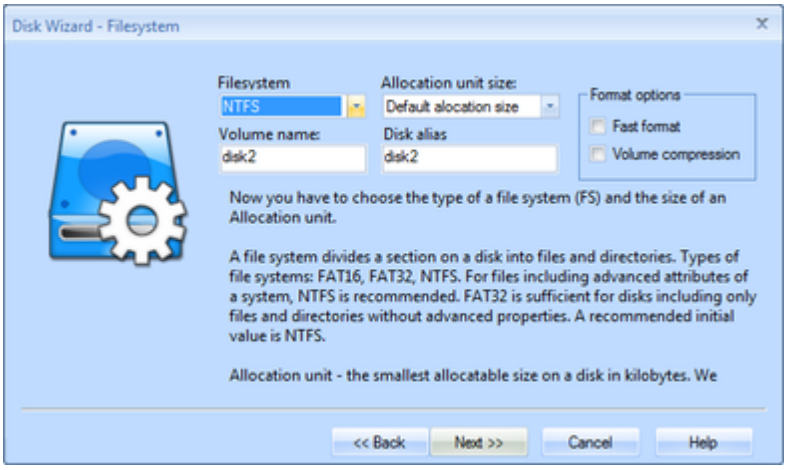


By clicking on *Browse* pick up the file that will represent your new virtual disk and choose its size. This file will then take a corresponding amount of space on the host computer. Next you can enter a disk label. After that click on *Next*.

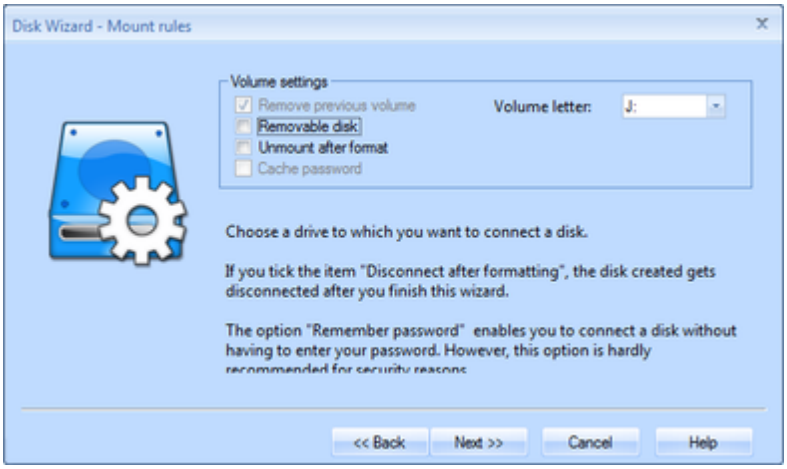


The size and location have been chosen already. Now you have to select a file system and an allocation unit. Manual selection of an allocation unit size is recommended only for experienced users. Generally, however, we recommend you to set the size of an allocation unit on the initial value of an allocation.

The choice of a file system is a dilemma. While the FAT32 file system is rather simple, the NTFS file system offers a lot of other options, in particular file and directory permissions as well as a possibility of compression. With regard to the character of new Windows operating systems we recommend to use NTFS. If you are ready with this selection, click on *Next* again.



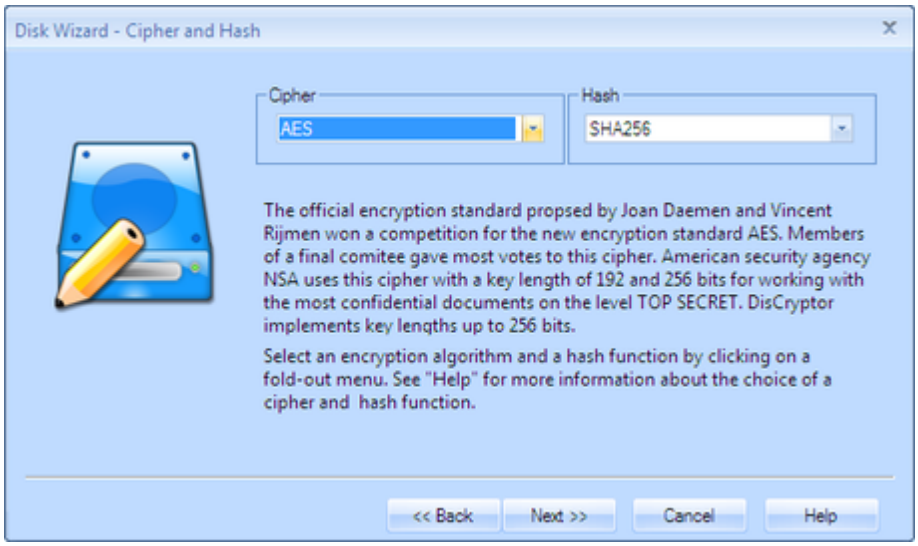
Choose a drive to which you will connect your virtual disk. After you are ready with this selection, click on *Next*.



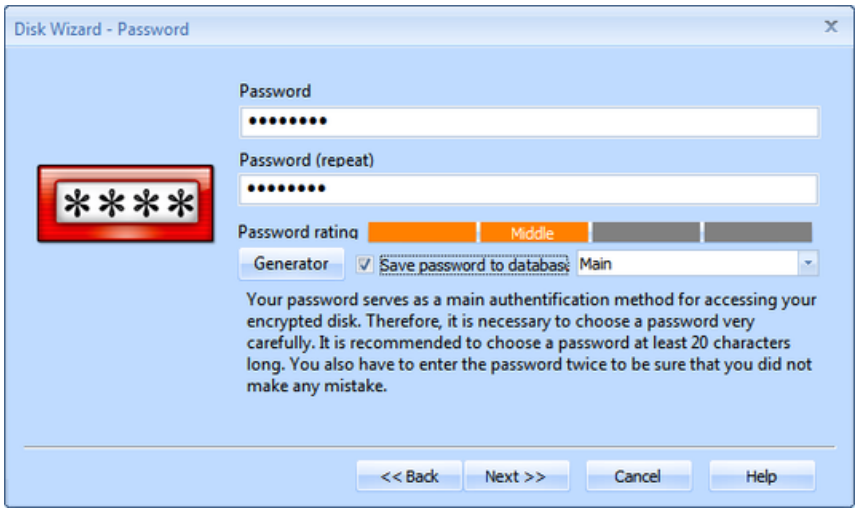
The next step is the choice of ciphers. You cannot make a mistake whichever cipher you choose. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed.

In case you save very risky stuff or programs, we recommend you to use the following ciphers: Serpent, Twofish, Rijndael(AES) or Blowfish. On the contrary, for less inhospitable conditions, and for frequent and bulky file transfers the RC5, RC6, or Twofish are recommended. These ciphers excel not only in security but also in the speed.

Generally, we have to point out, however, that the choice of a cipher itself is a secondary matter. Above all, we recommend you to choose your access password very carefully. You can learn more about the security of ciphers in the chapter Frequently asked questions. To confirm your selection click on *Next*.



A key decision in the whole guide is the choice of a suitable password. There is a special chapter on this topic. To generate a safe password can you use the Password generator, which is integrated in the dialog. Your password can be immediately stored in any database or group in the Password manager. Before you choose a password, we recommend you to study materials given here. Generally, it is recommended to choose a password with al least twenty characters. After you enter your password and re-enter it for verification, click on Next.

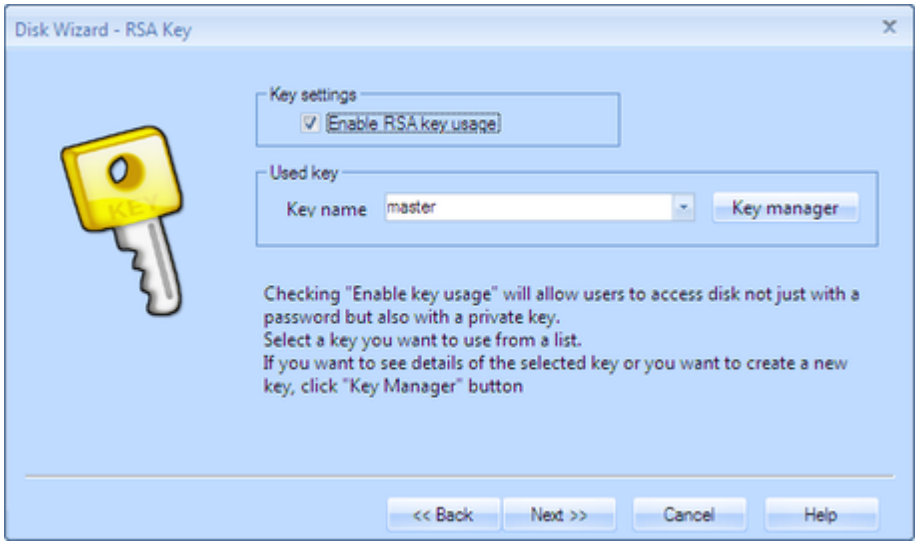


The wizard has automatically generated the disk key, which will be used for the encryption of the disk.

According to the program settings you can or must choose the using of the rescue security key for

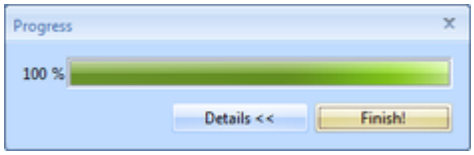
the creating disk. This security key is used for the access to the creating encrypted disk in the case of forgetting its access password. It is therefore a rescue fail-safe, but it is necessary to treat with it very carefully. If the security key comes at unwanted, the attacker can easily abuse the disk, on whose the security key is used. In the case in the Endpoint Security Tools exists no security key, the wizard will be automatically engaged. You can create or import a key in this wizard. You can allow using of the security key by ticking the Allow using of the security key and choosing the key from the highlighted menu. When the choosing is finished, click on the Next button.

You can learn more about the security key problems in the Security keys chapter.

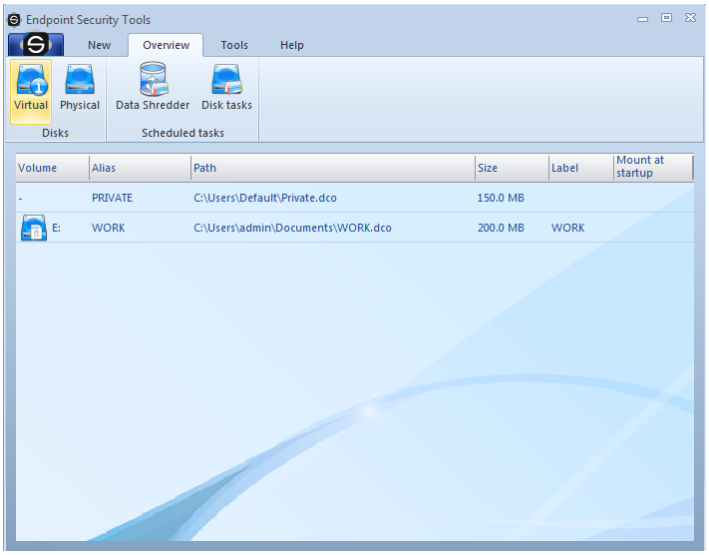


Check the entered data for the last time and click on the *Finish* button.

It is also necessary to format a disk before you use it. The guide is just doing it for you.

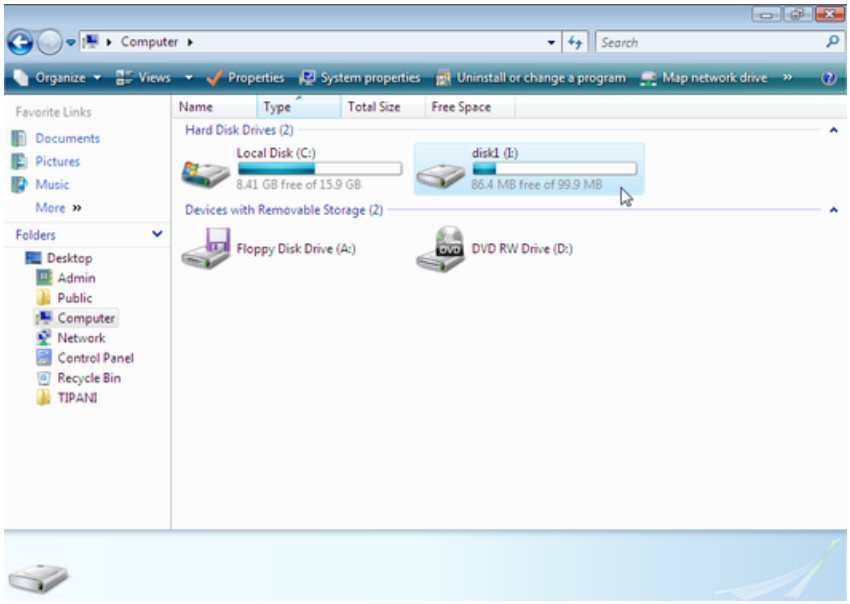


Congratulations! Your new virtual disk has just been successfully created. This disk will show up in the system as a drive you selected in the guide, in our case drive E:



From now on you can use this disk as any other disk. If you click on "My computer" in your Win-

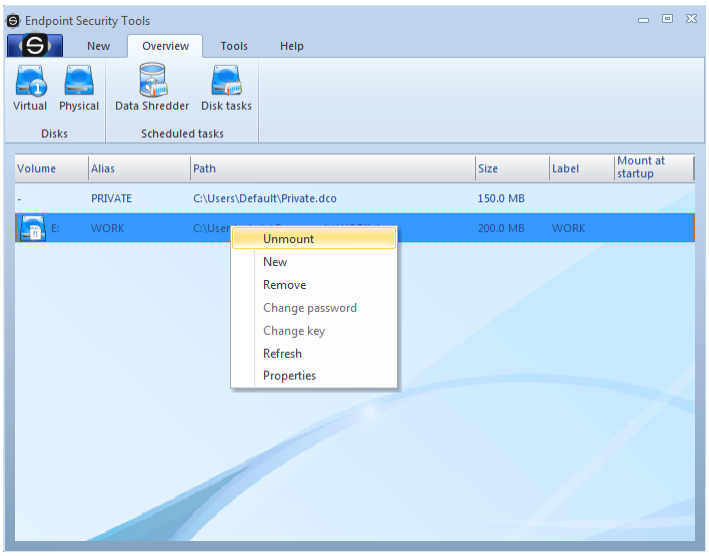
dows system, your encrypted disk will be displayed together with other disks.



6.2.4.3 Overwriting an existing disk

If you want to replace an existing encrypted disk by a new encrypted disk, you have to do the procedure the same way like when you create a new disk. However, a guide to removing a current disk will be launched in this case at first. You can overwrite any type of a disk (either physical or virtual).

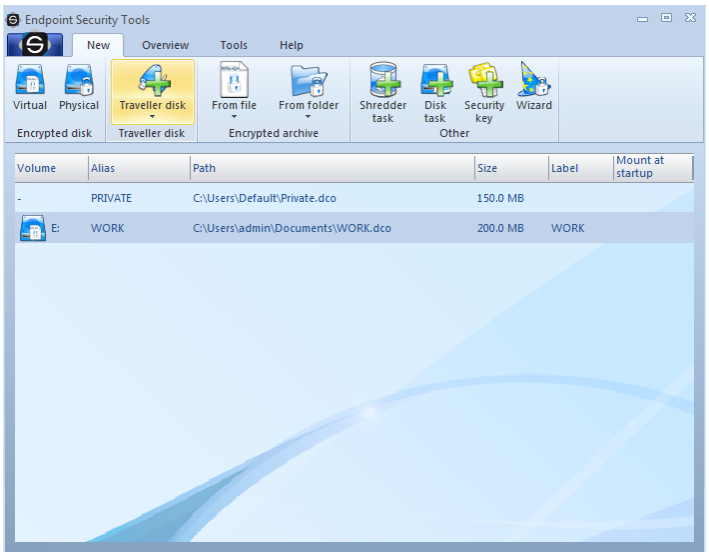
Click on the corresponding encrypted disk on the desktop that you intend to overwrite a choose *New* in the subnavigation.



Immediately after clicking you are welcome by a new guide - it is either a guide to a disk encryption or a guide to adding a virtual disk. After you go through this guide a new disk is created.

6.2.4.4 Traveller disk

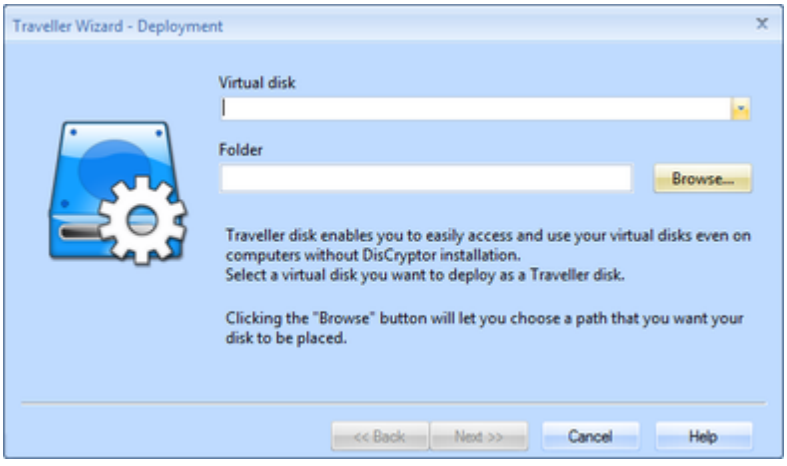
One of the main benefits of Endpoint Security Tools is the feature Traveller Disk.



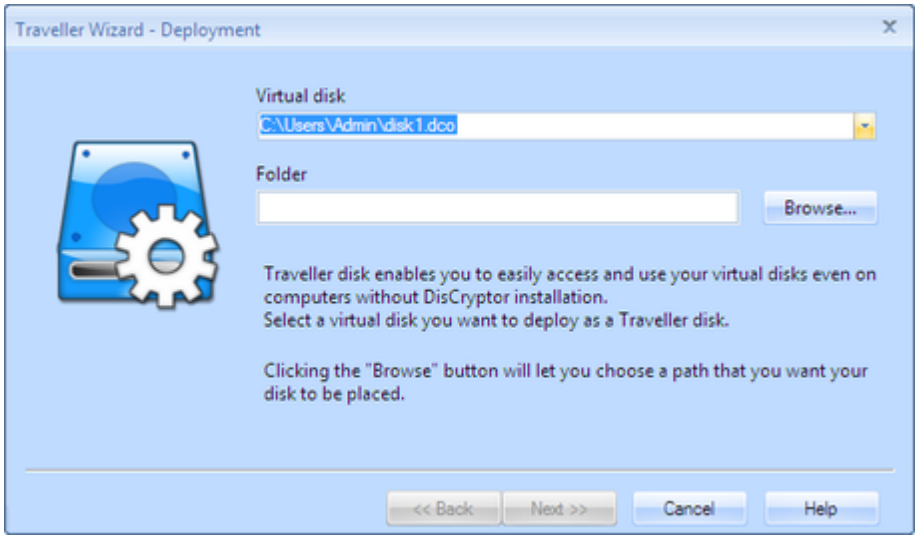
Traveller disk allows you to simply access virtual disk even on computers, which do not have the Endpoint Security Tools installed. Travel disk has equal security level like another types of disks encrypted with Endpoint Security Tools. It means - if you lost your traveller disk, the data will be absolutely unreadable for thieves.

To create a new travel disk select the tab New and then select the option Travel disk. If you want to use an existing virtual disk to export to a travel disk choose desired disk from desktop and select the option *From virtual disk...*. Otherwise just choose *New disk...*. The wizard is very similar to Creating a new virtual disk - you can follow the link.

Next description is for option *From virtual disk...*.



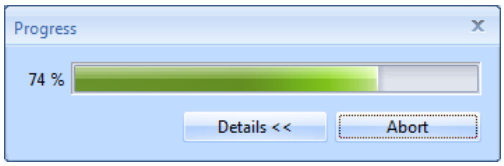
Endpoint Security Tools welcomes you with Traveller disk wizard. If you correctly selected the disk from desktop it will automatically find its path. You can still change this by clicking on the arrow on the right of the first line - there will be list of existing disks.



In the next step choose the path where your future traveller disk will take a place. If you are going to place it on CD or DVD just place it to some temporary folder and then burn it with your favorite burning software on the disk. In case of using flash disk, just choose a place on that disk.

Now click *Finish*.

And that is all. There will show up progress dialog and the rest is on Endpoint Security Tools. At the end just click *Ok*.

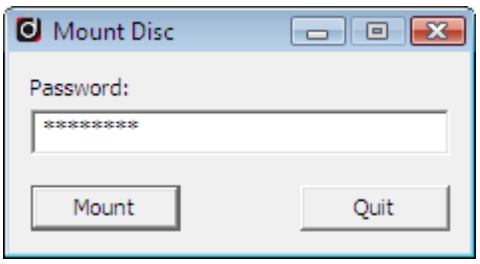


Congratulations. Your new secured traveller disk has been created.

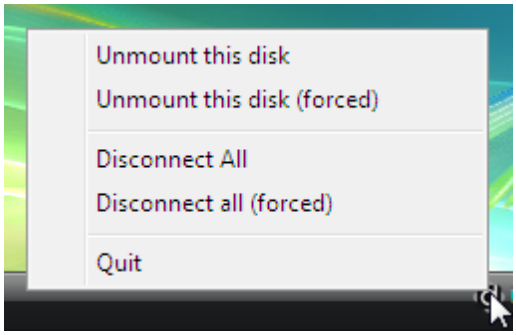
How to access the traveller disk?

Due to the automatic start of inserted disk with this option turned on in Windows (autorun), you can choose *Connect encrypted disk* and Endpoint Security Tools automatically asks you to enter password and connects the disk.

Enter now your password, which you have entered in the Travel disk wizard and confirm by clicking *Ok*.



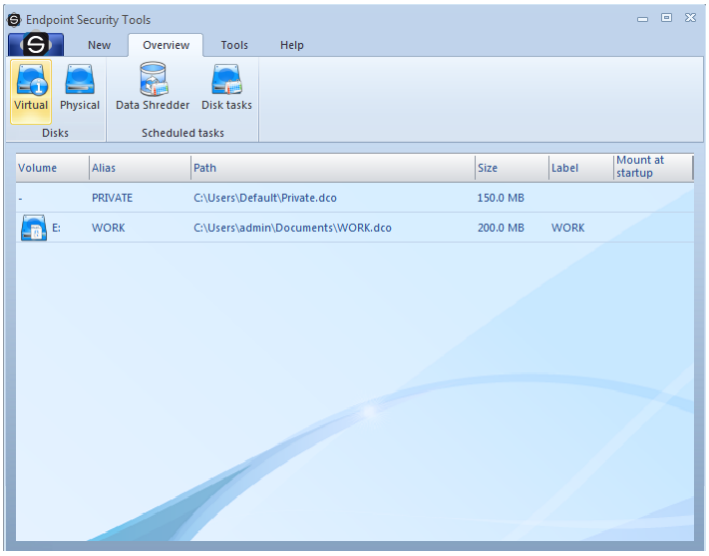
If you wish to disconnect the disk, just right-click on the tray icon , choose your travel disk to *Unmount this disk*.



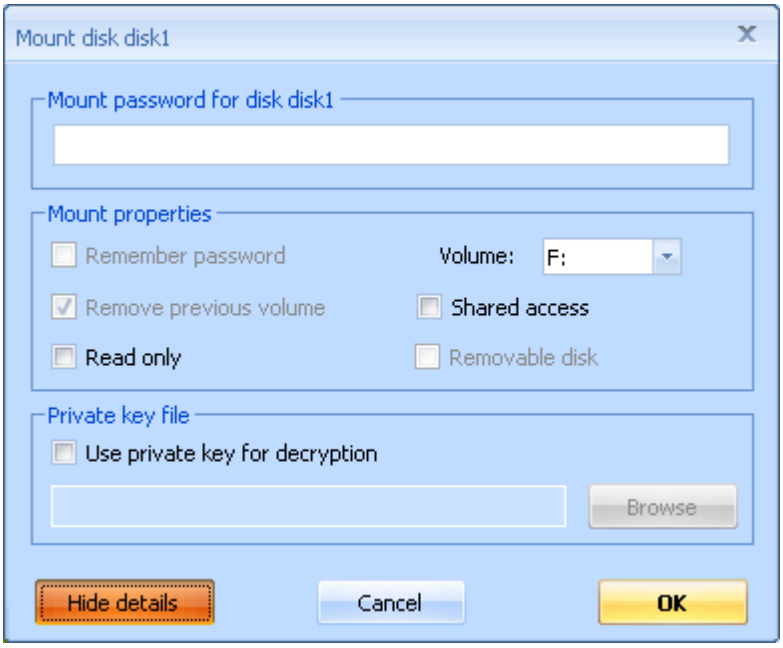
6.2.5 Disks administration

6.2.5.1 How to connect a disk?

The easiest way how to connect a disk is to choose an overview of all disks by clicking on the navigation button *Overview*. Then choose a disk you want to connect - right-click on the desired disk on the desktop and select "Mount".



To access your disk enter your password and confirm by Enter. You can also do some additional settings in the window of a disk connection.



Connecting options:

1. **Remember password** - If you want to use that option, you have to allow it first in Settings. From security reasons we do not recommend using this option! Password is remembered through all the computer activity until shutdown. If you wish to delete the remembered password just choose the tab Tools -> Delete remembered passwords.
2. **Remove previous volume** - (only for physical disks) Endpoint Security Tools removes the original drive while the disk is connected.
3. **Read only** - By turning on this option it will be not possible to write on the disk.
4. **Shared access** - shares access to disk
5. **Removable disk** - (only for physical disks) Choose in the case that the device you are connecting is containing removable disks like card reader, ZIP Drive, etc.
6. **Use private key for decryption** - if you enable this option you will be able to connect a disk by your private key.

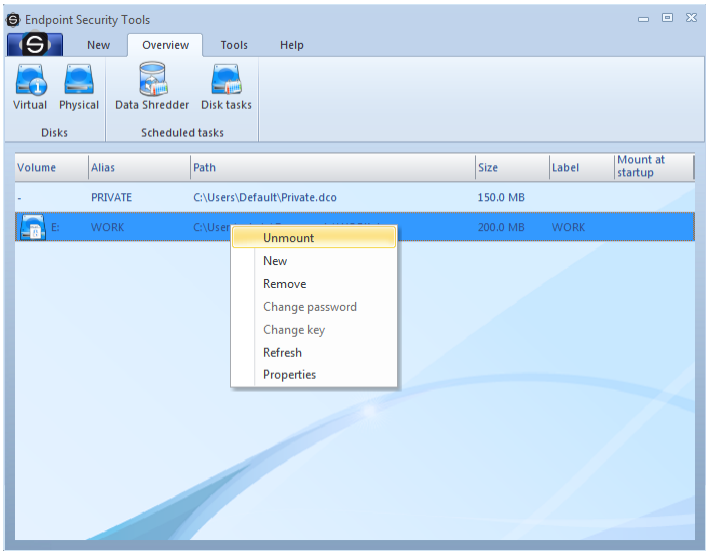
If you want to connect a virtual disk that is not known in the list of virtual disks, click on the view of virtual disks in the navigation, and then on "Search" in the subnavigation. Choose a path where your file with a virtual disk is located and confirm by clicking on "Open". After the disk is found proceed in connection as described in the second paragraph of this section.

6.2.5.2 How to disconnect a disk?

There are two ways how to disconnect an encrypted disk.

1. **Forced** (hard) - disconnects all disks even if they are being used. Therefore, we recommend you to use this way of disconnection only in case of security emergency - when your data are in danger (by default using WIN-Ctrl-Q keyboard combination). However, this function has to be enabled in settings.
2. **Unforced** - a standard way of disconnection. A disconnection cannot be carried out in this way if a disk is being used. If you want to disconnect a disk and the disconnection does not work, terminate all applications that utilize a disk and try to disconnect it again. You can perform the disconnection of all disks by a keyboard combination WIN-Ctrl-U.

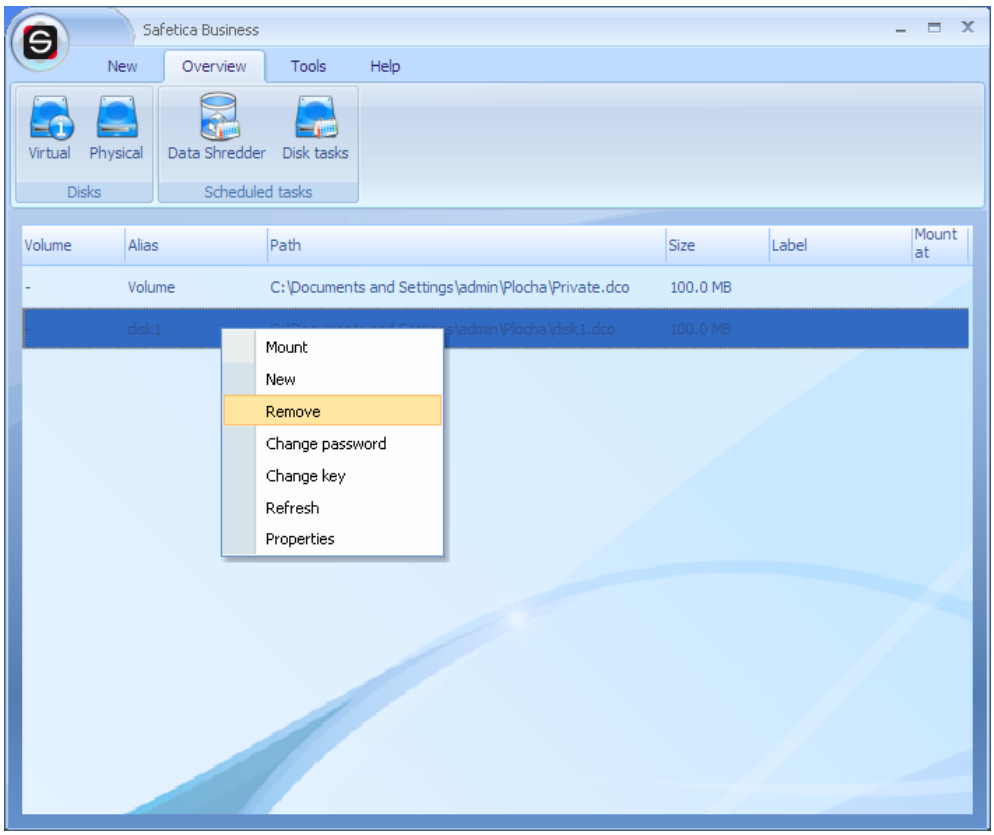
You can carry out a disconnection of particular disks by their selection on the desktop and by right-clicking on the particular disk and by selecting "*Unmount*".



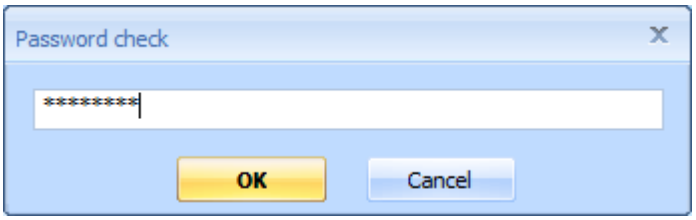
If you are right now working in Windows and you do not want to open the main window of Endpoint Security Tools, just click on the icon in tray and choose Disconnect and the disk you want to be disconnected.

6.2.5.3 How to remove a disk?

If you want to remove a disk, select the disk to be removed on the desktop and right-clicking on the particular disk and by selecting "*Remove*". If you really want to remove the disk, click on *Yes*.



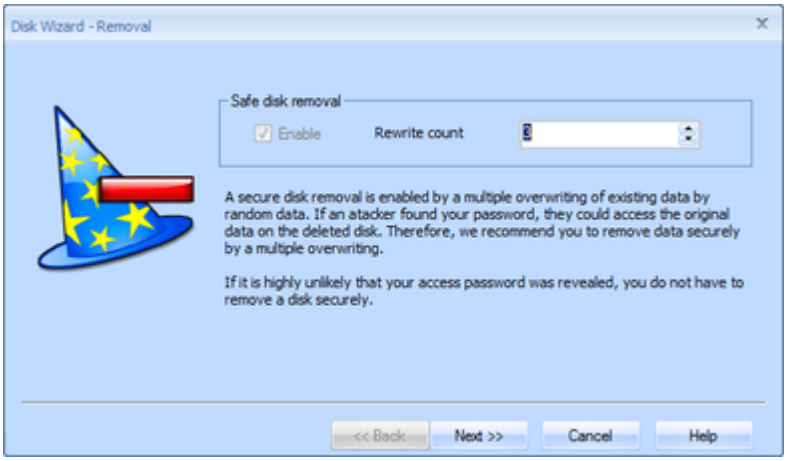
Before the removal itself, you have to enter your access password.



After you enter the password, you have to choose the type of removal.

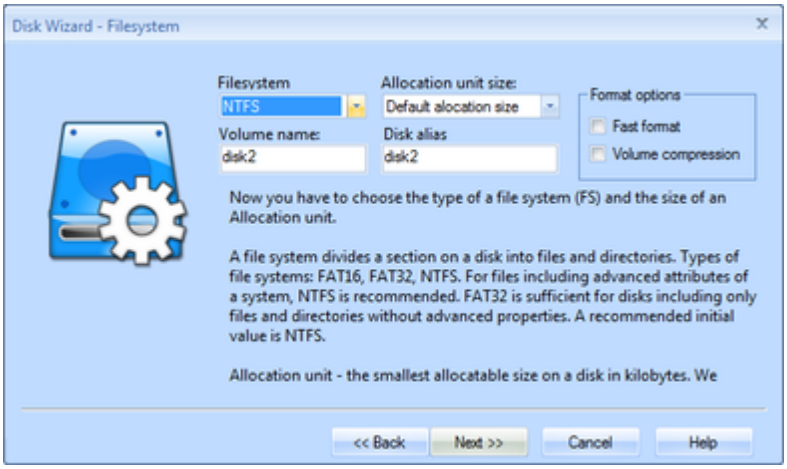
There are two types of disk removals.

1. **Deleting** - Deleting is the most common way of a disk removal. In case of a virtual disk it is just a deletion of a file with a virtual disk that is carried out. In case of a physical disk the disk is only formatted.
2. **Secure removal** - a markedly more secure way of removal. In case you need to remove your data from the disk on suspicion of a password leak, select *Enable*. A disk is overwritten several times by random data. Users themselves set the number of overwritings in Program settings. Five overwritings are sufficient for the most common needs. A very secure way of removal is the choice of *at least 15 overwritings*. The probability of reading original data is negligible, indeed, with such a high number. Thirty overwritings are recommended for military purposes. The process of a secure removal may take a long time depending on the number of overwritings.



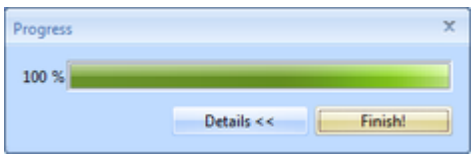
Choose the way of removal and proceed by clicking on *Next*. Confirm the removal.

In case you remove a virtual disk, the removal of the disk is carried out already in this step. At the end just terminate the guide by clicking on *Close*. If you remove a physical disk, you also have to format the disk so that it can be prepared for its next usage. Select a drive under which you want to use the disk subsequently and click on *Next*.



Select a file system you want to use on the disk and you can optionally enter a stream label. Then click on *Next*.

The process of disk formatting:



This procedure can take a long time depending on the number of overwritings and depending on the speed of the disk used. After the disk formatting the disk is prepared for a common usage under the drive chosen before.

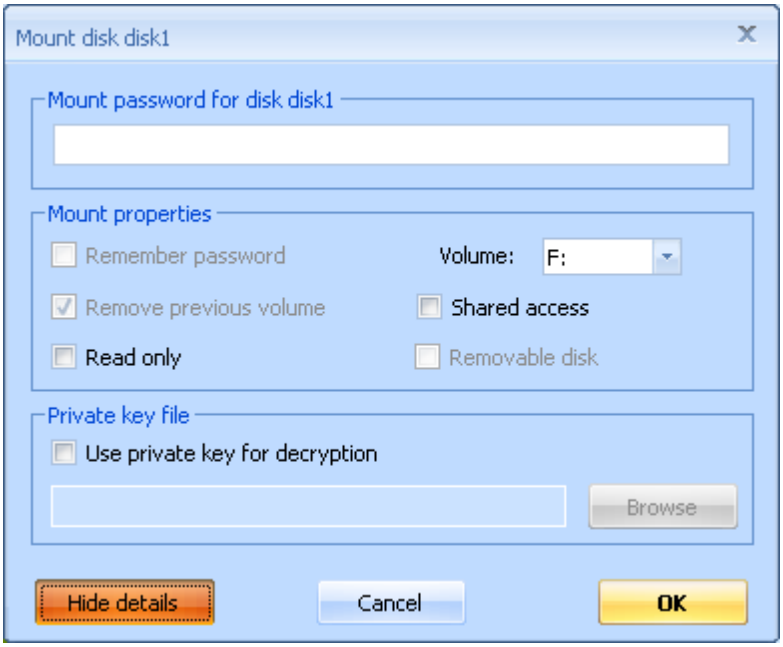
6.2.5.4 Forgotten password?

The private security key is used for unlocking the disk. For a successful unlocking the disk is needed. If the disk hasn't been created by the security key, the disk isn't in no manner possible to unlock in the case of forgetting the password. The picture shows you the system of the unlocking.

Choose the path to the private security key file, which has been used for creating the unlocking

disk.

You can connect the disk similarly like in the Connect disk dialogue. But you do not enter the password, but the path to the private security key. In the connection dialogue, which appears soon, click on the *Show details*, then enable Use private key for decryption, click on the *Browse* button, choose the private key file and confirm the choice by clicking on the Open button. You can start up the opening by clicking on the *OK* button.

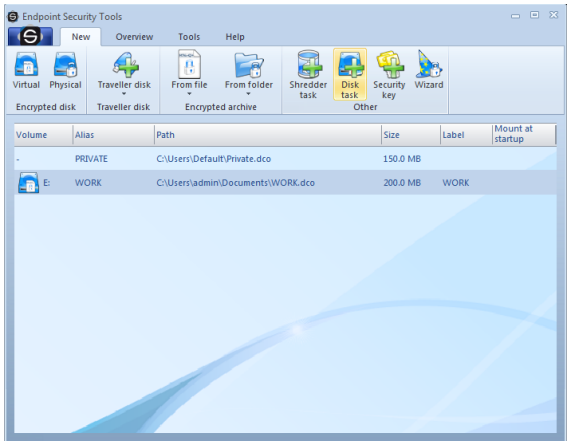


The disk is now connected and if you have forgotten the password and wish to change it, click on the desktop by the right mouse button on the appropriate disk and in the menu choose *Change password*. In the dialogue enter the path of the private security key file, two times enter your new password and confirm by clicking on the *Change* button.

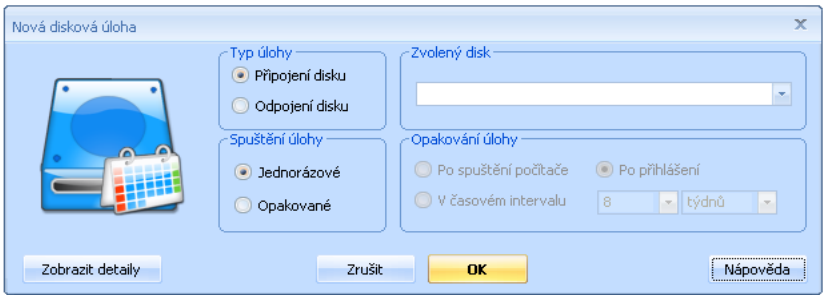
6.2.5.5 How to create disk task?

Disk task allows you to connect or disconnect the selected virtual or physical disk in a given time.

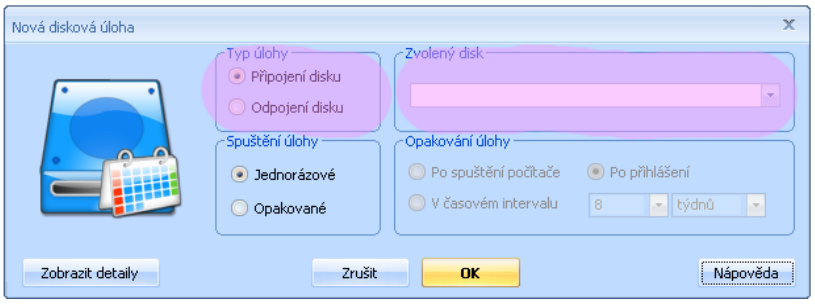
You can create a new disk task by clicking the *Disk task* icon in the *New* tab.



The following transparent dialogue will appear.

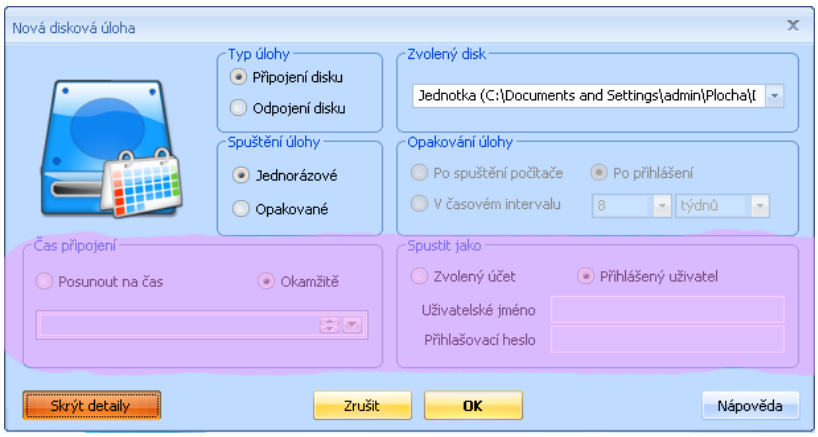


In the first step, choose the drive from. Next choose if you intend to connect or disconnect the drive. Additionally, you can choose whether to join the disc once or repeatedly. If you choose repeatedly, you can specify when (when you start your computer, after logging), and in what interval.

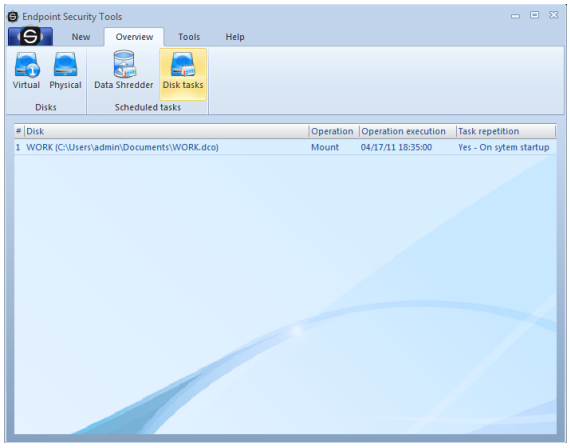


Disk task can be also set in detail. When you click *Show Details* button in the lower left corner, the dialog with detailed disk tasks setting will appear. You can set the exact date and time of connection, or under what user account will have access to.

You can hide detailed setting by clicking *Hide Details* button. If you have done the disk task setting, click ***OK*** to add it to the Windows Task Manager.



You can view created disk tasks by clicking the *Overview* tab and *Disk tasks* icon.

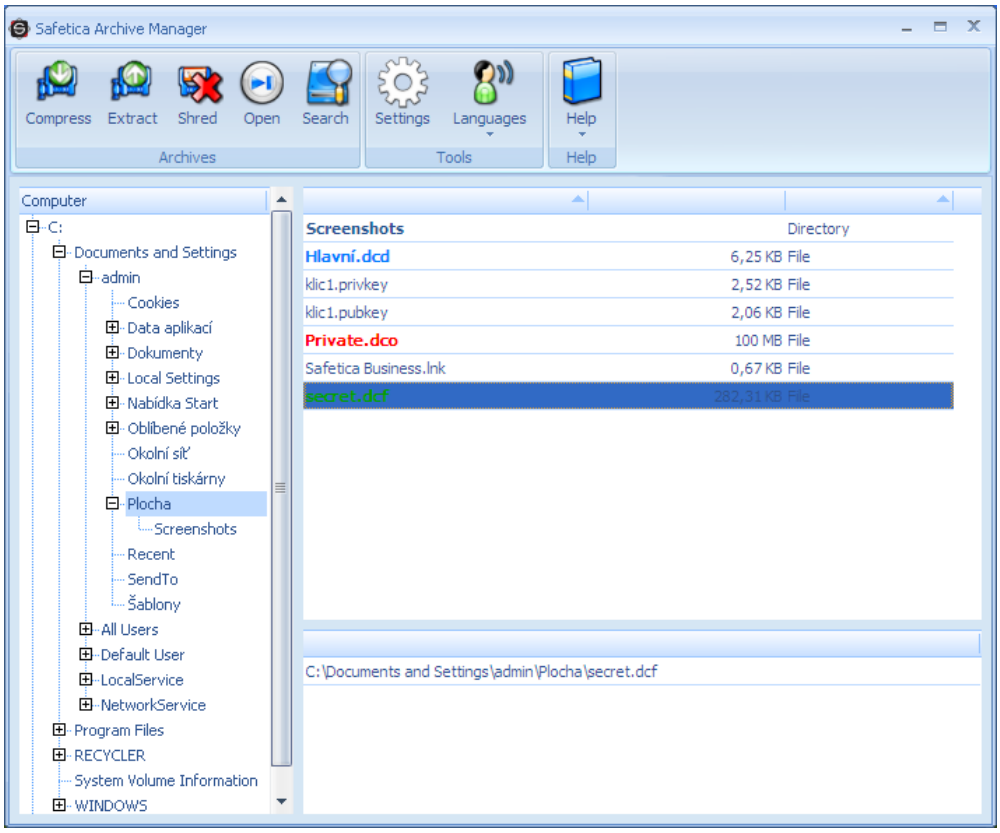


6.2.6 Archives

6.2.6.1 Overview

The Safetica Archive Manager is part of the Endpoint Security Tools. It includes file and folder encryptions in DCF archives (note: formerly encryption on file level, context offer - Encrypt..., Encrypt and Send...), which were separate in the previous editions.

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.



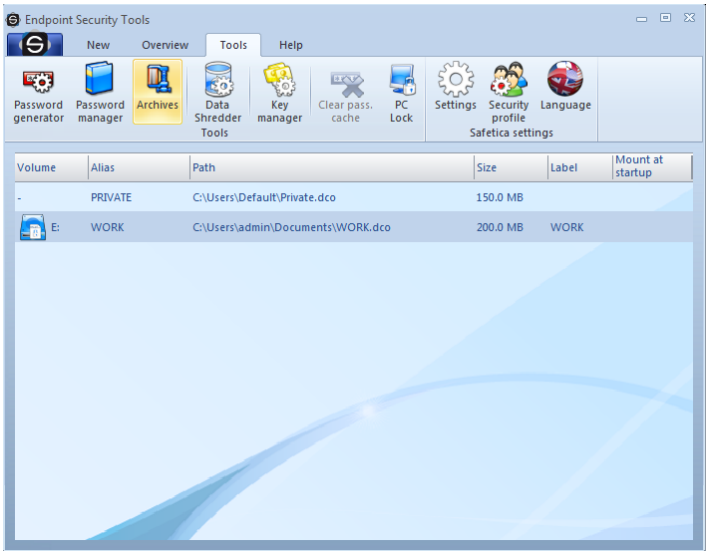
The Safetica Archive Manager is launched separately from the tab *Tools -> Archives*. Main window contains likewise the Windows Explorer two parts - directory structure tree on the left and currently opened folder or disk on the right (it also shows the content of archives). In the bottom window only archives from the given folder are displayed for better overview. All relevant items are highlighted at the same time.

There is a function with following options in the upper part of the window.

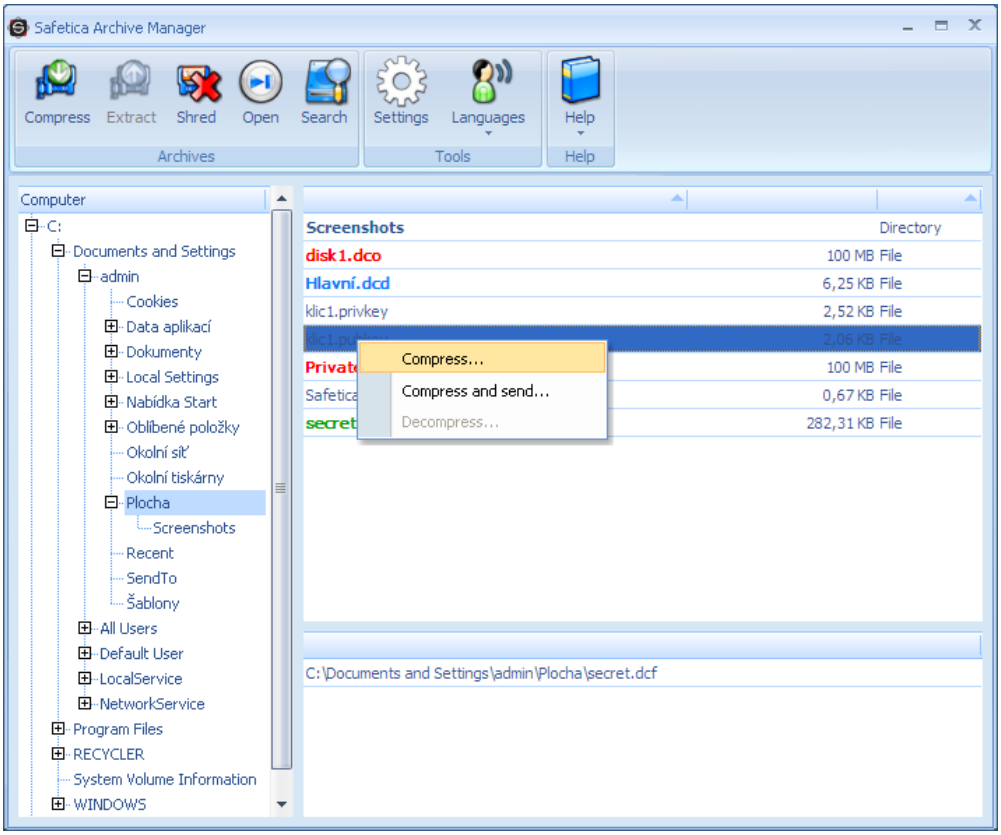
- **Compress** - selected files or folders will be packed in the required format.
- **Extract** - extracts selected archives to required path.
- **Shred** - by means of Data Shredder it deletes selected items from the disk.
- **Open** - opens or launches selected items.
- **Search** - opens searching dialogue.
- **Settings** - opens Setting dialogue.

6.2.6.2 Compression files and folders

For security or compression of a file and folder open the Safetica Archive Manager in the Tools tab as illustrated in the picture. The compression also includes the encryption of selected items if the DCF format is used.



Further select the required file or folder and then select from the function bar the option Compress or click with the right button and from context menu select Compress. If you wish to send the encrypted files safely by e-mail click on the chapter bellow.

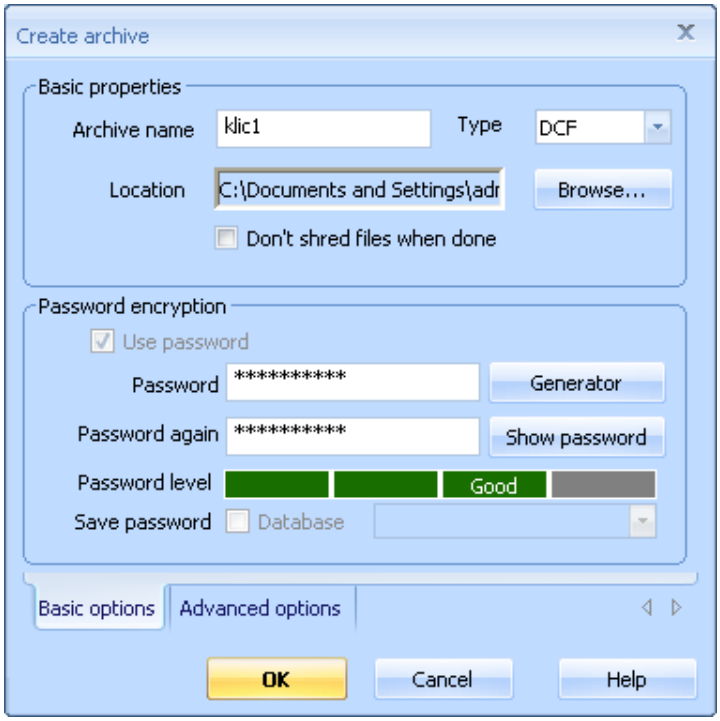


If you prefer the Windows Explorer just click with the right button on the file or folder and select the particular option.

The dialogue with request for entering the access password appears immediately. Select the format you want to use for compression, name of output archive and location. If you wish the original files to be removed tick the option Shred files after archiving.

Warning: Shredding is a time-consuming operation and subject to selected data size it may take even several hours (shredding of 4 GB data may take more than ten hours). It is not recommended to encrypt big folders or system folders (like Documents and Settings, Users etc.). Your key decision comes – selection of correct password. For secure password generating you can use the Password generator integrated directly within the dialogue. The given password can be immediately added to any database or group in the Password manager. This important questions are described in separate chapter. The password to the given archive you can save directly to your con-

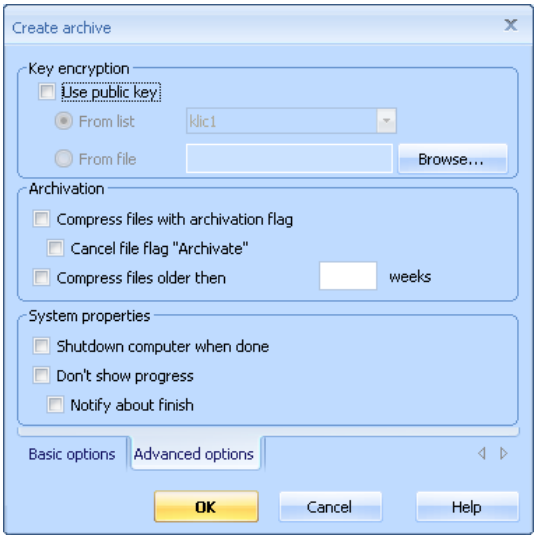
nected database. Before selecting the password we recommend to study materials about correct password selection. Enter your password once more for control and click the OK button.



Now the dialogue with indicator of compression course will be displayed and new archive will immediately appear in the same directory and as a new item of archive list. Just confirm by clicking OK. Any encrypted file by the Endpoint Security Tools is easily recognized according to .DCF extension and Safetica logo icon.

If you transfer the encrypted files to other computer, it will be necessary to decrypt them again! How to decrypt files and folders quickly is described in the following chapter.

Option to use the password is obligatory only with DCF archives (this one is only one secure with password use because it is encrypted!), with others this possibility is optional if available.

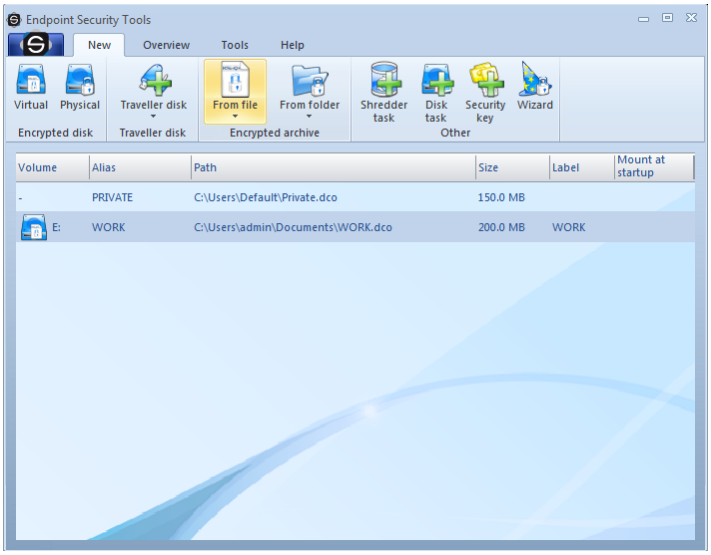


Advanced setting

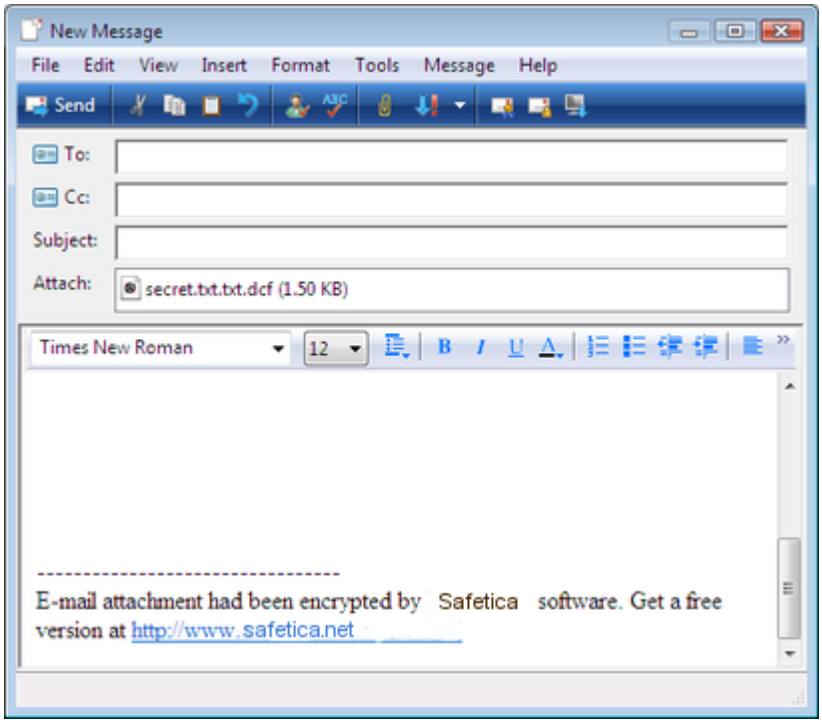
In this tab details of archive formation can be set. The use of public key for file encryption is the most important in case you would have forgotten the password.

6.2.6.3 Compression and sending in an email

Click the tab New and then either From file or From folder icons as shown in the picture. Then click the option Encrypt the file/folder and send by e-mail..., and select the required file which you want to securely send. The same dialogue as described in the previous chapter will be opened.



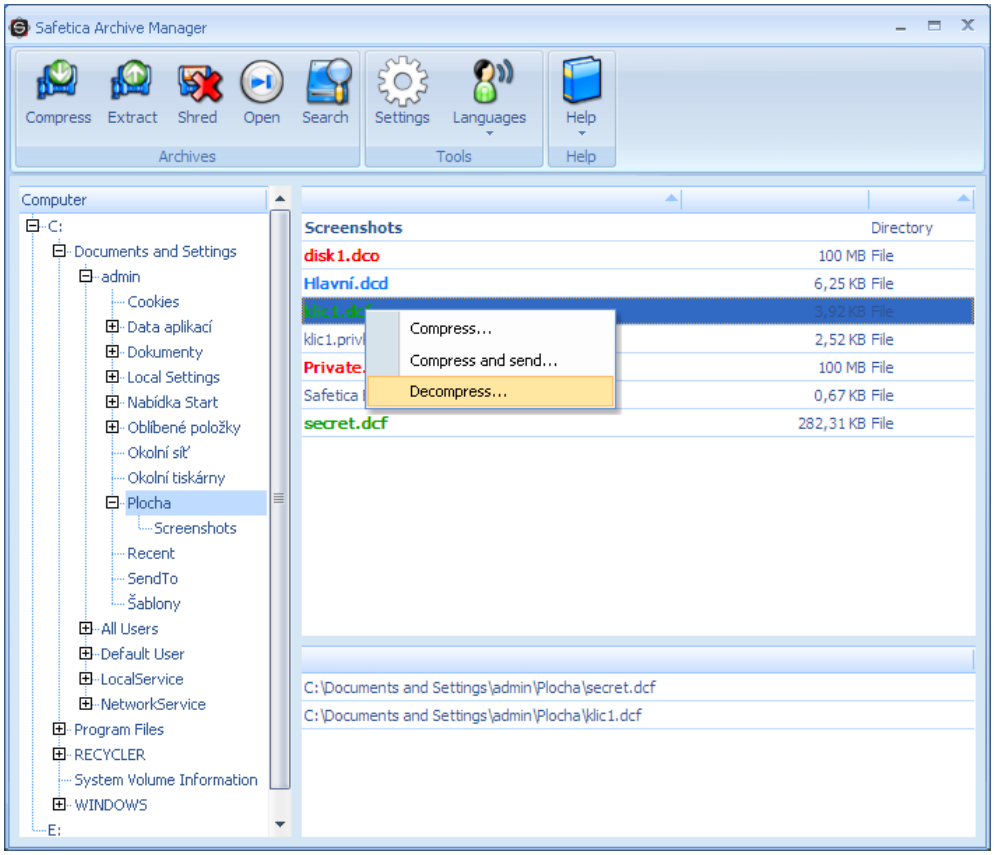
If you prefer the system Explorer just click with the right button on file or folder and select the option Compress and send. The same possibility you can also find in the context menu of the Safetica Archive Manager.



In the last step your favorite email client will be launched and the encrypted file will be automatically connected as attachment. It is enough to fill in the e-mail address of the recipient and send the e-mail. The recipient will receive automatically enclosed instructions how to encrypt the attached file easily. If you use the self-extracting EXE archive the recipient does not need to install any software. The recipient has to obtain from you the password and then he is able to decrypt the file easily. **However we do not recommend to send passwords by e-mail!**

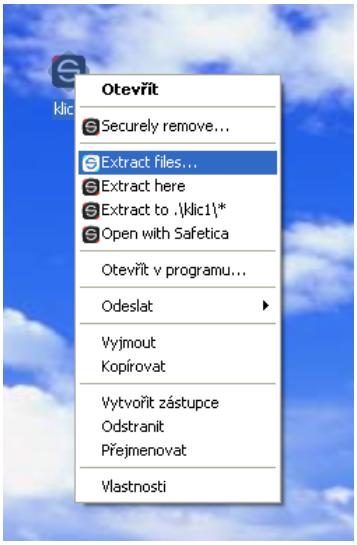
6.2.6.4 Decompression archives

The decompression of archives is very easy. In the Safetica Archive Manager select by right button the required archive and select the Extract option.

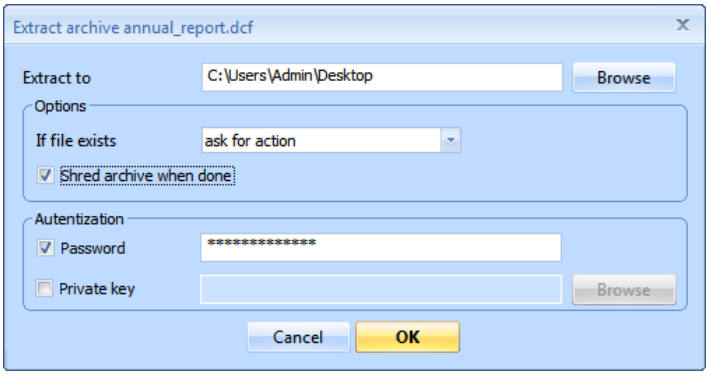


Compressed files and directories are very well recognizable thanks to Safetica icon by which all encrypted files are presented within the system.

In the Windows Explorer double click the compressed file icon or click just once with the right button and select the Extract option as illustrated in the picture bellow.

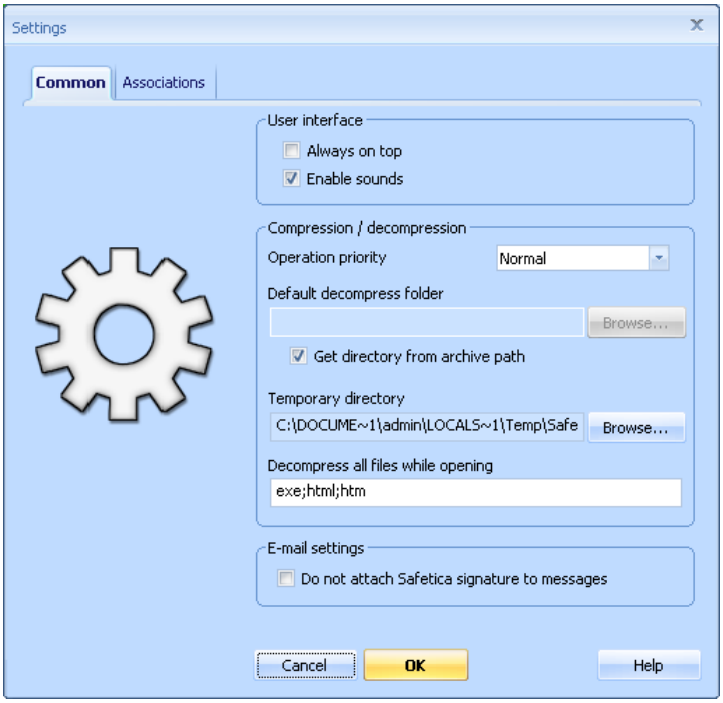


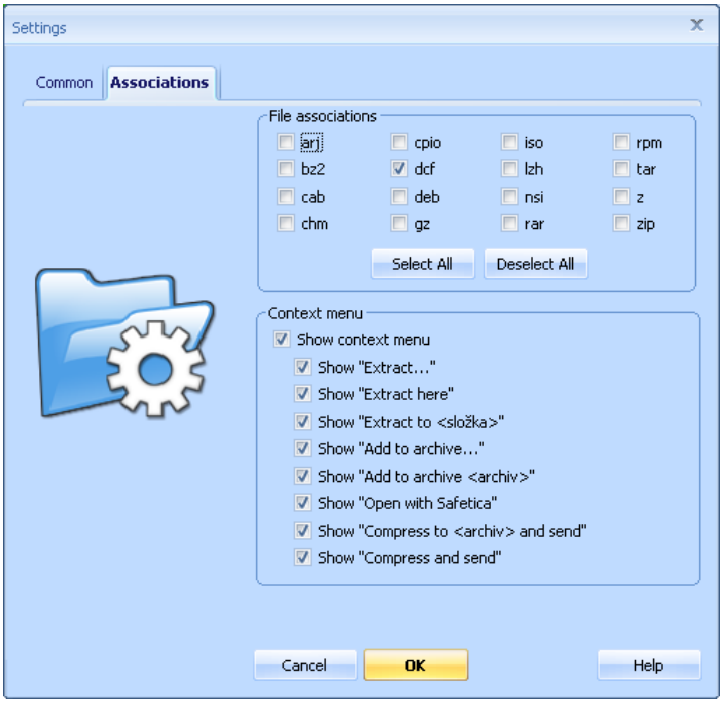
Enter the original password in for decompression or decryption if the DCF archive or some other with use of a password was used. If it is the DCF archive and the public key were used for encryption, for decryption you can use the private key.



6.2.6.5 Setting

Setting of the Safetica Archive Manager includes some useful options. Thus it enables you to tune the program behavior according to your needs.

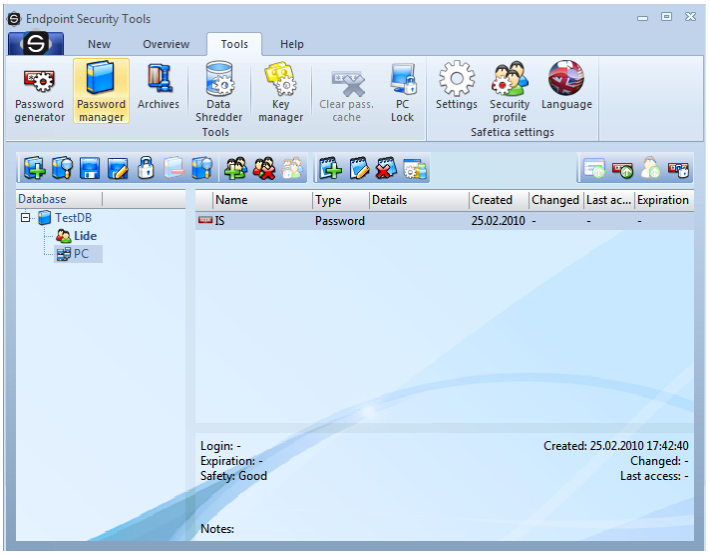




6.2.7 Password manager

6.2.7.1 Database

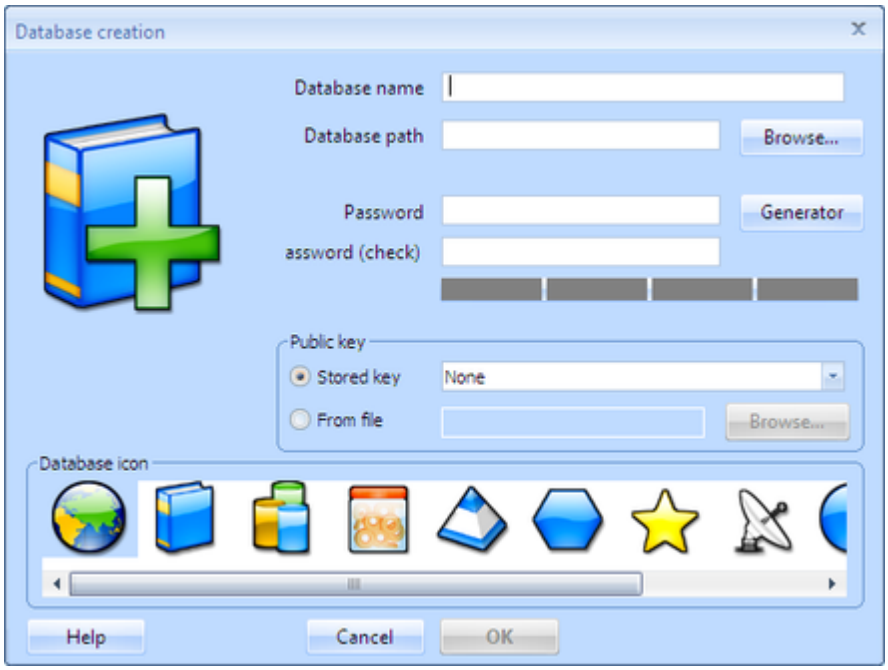
Database is a default structure to store records. They are stored and encrypted locally on your computer and their count is limitless. Working with database is similar to working with a word document. All changes must be saved and the data are in that process encrypted. Database can contain groups, subgroups and mostly the records. Password for database is mandatory unlike for the groups. Level of this password is set according to the chosen security profile and it is recommended to use the strongest password as possible. You can also use the security key.



To manage databases there are first six icons from the left on the toolbar. All of these actions can be reached also in the context menu. You can unlock or lock database with double-click in itself.

1. **New database** - opens a dialog to create a new database
2. **Import database** - imports an existing database into the list
3. **Save database** - saves all changes
4. **Save database as...** - saves database at the selected path as a new file

5. **Unlock/Lock database** - unlocks or locks the database - icon and tooltip changes dynamically
6. **Remove database** - removes the database from the list and asks if you want to remove the database also from the disk



When creating a database, it is important to fill in name, path and password. Icon and security key is optional.

6.2.7.2 Groups

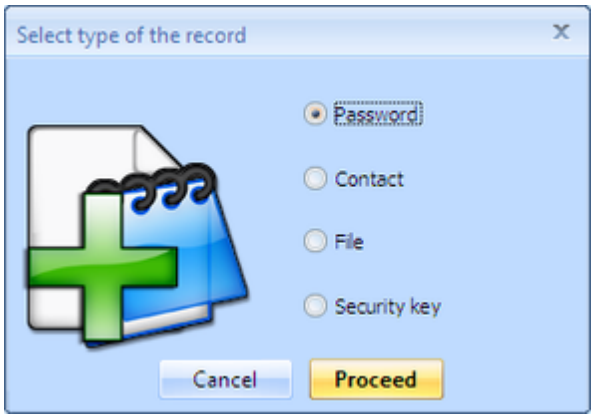
With groups you can separate records into logical structures. The structure of groups depends only on your needs and groups can have subgroups. You can set for every group a different icon, password and security key (which is by groups optional).

1. **Create group** - opens dialog for creating of a new group
2. **Remove group** - removes selected group with all its subgroups and records
3. **Unlock/Lock group** - unlocks or locks the group - icon and tooltip changes dynamically

Mandatory field is only name of the group, everything else is optional.

6.2.7.3 Creating records

Elementary item in the database is a record. Record can be placed in the root of the database or into groups or subgroups. To create a record just click on desired database or group, which you want to place it in and select the icon "Create record" from the toolbar, or use right-click and select the option from context menu. After that will appear the dialog, where you can select type of the record. Mandatory field in all records is only the name.

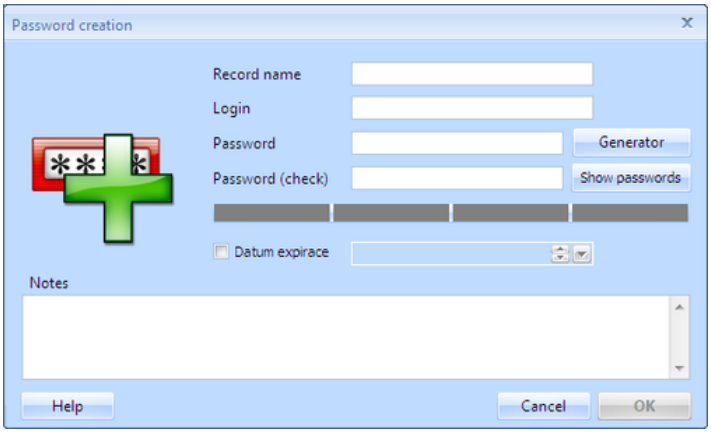


Record are divided into four types

- **Password** – this record stores user names and passwords.
- **Contact** – it allows to store all information typical for a contact record.
- **File** – stores the file directly into the database (e.g. an e-certificate).
- **Security key** – secures in database a private and a public key.

Password

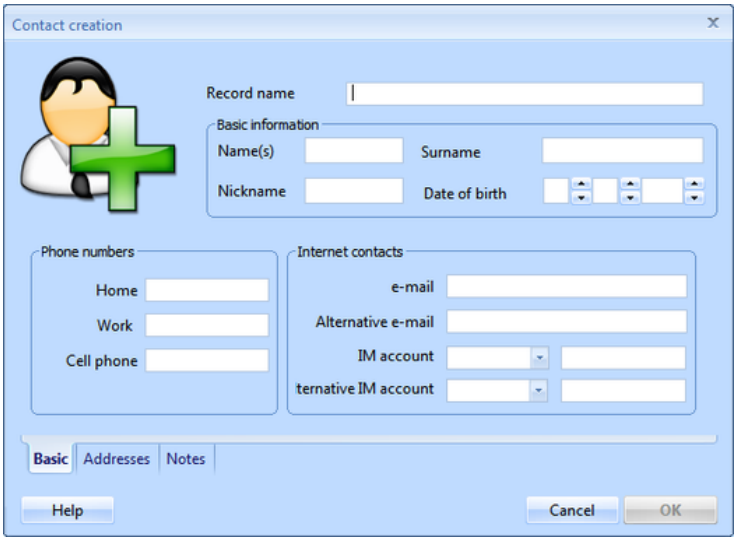
Password record represents for example authentication information such as login and password. You can write a note or set a date expiration as well. If you are right now creating a password, you can use directly the Password generator.



You can copy into clipboard the login or the password from an existing password record. Using the toolbar icon or through the context menu.

Contact

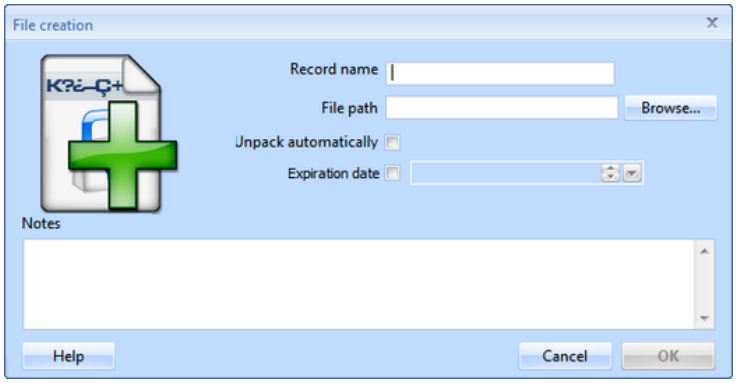
The contact record can store all contact information for a person or a company. From name, address, to IM contact or internet address. You can use with this record the Safetica as an electronic diary as well.



In the lower section of the dialog, there are tabs which switch into different views for different kinds of information.

File

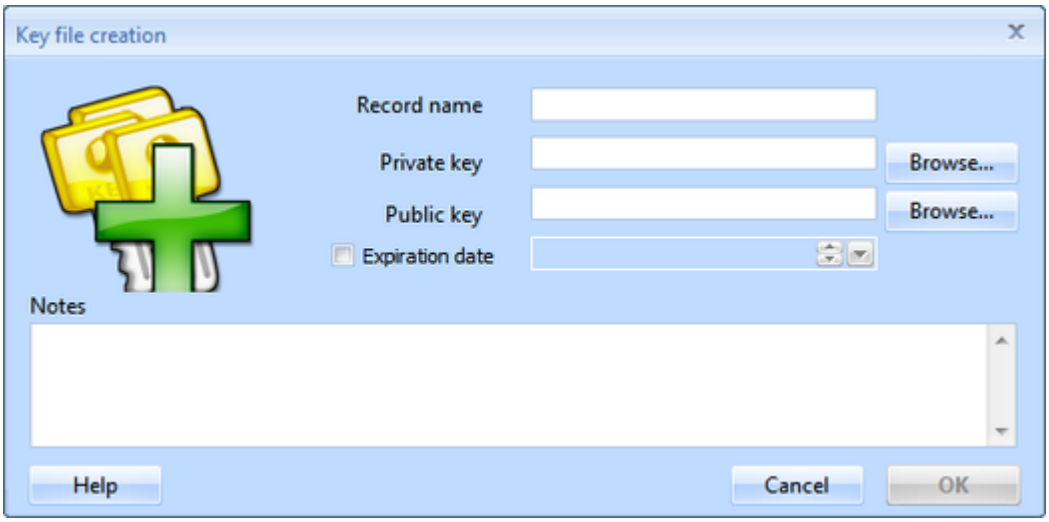
In the database can be stored files as well - it is useful for files like electronic certificates, etc. Of course you can store any kind of file. It is recommended to store smaller files.



The option Default extraction causes after every unlock of the database export of the file to the path from which it was selected, otherwise it can be exported through context menu. You can write a note or set date of expiration as well.

Security keys

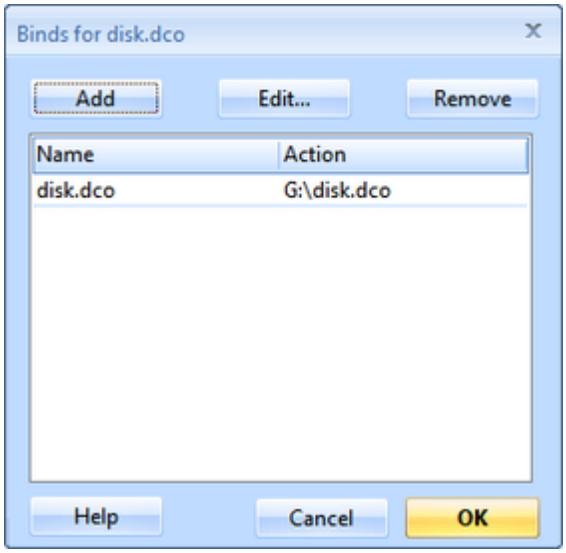
The last type of record is Security keys from Safetica.



Like in every other record the date of expiration and a text note can be set. Keys can be exported from the database through the context menu.

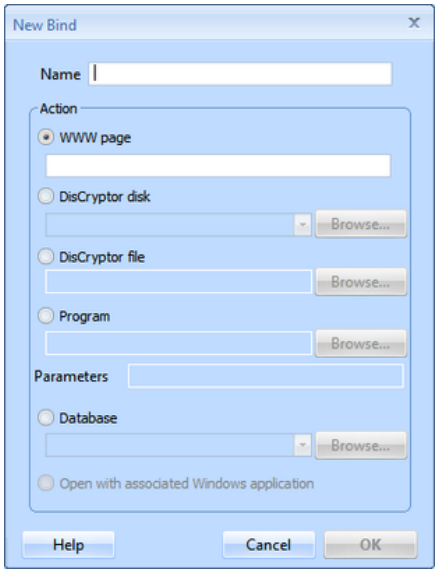
6.2.7.4 Bindings

For every record a different kind of action can be set, which appears then in the context menu. To create user defined actions select "Set actions" from the context menu. There can be limitless number of actions and they can be edited.



Actions which can be set:

- **WWW page** - opens a web page
- **Safetica disk** - from the record password or security key connects a disk
- **Safetica file** - from the record password or security key decrypts a file
- **Application** - runs an application - parameters can be set as well
- **Database** - from the record password or security key connects a database
- **Open with an associated application** - runs an application according to the settings of the system

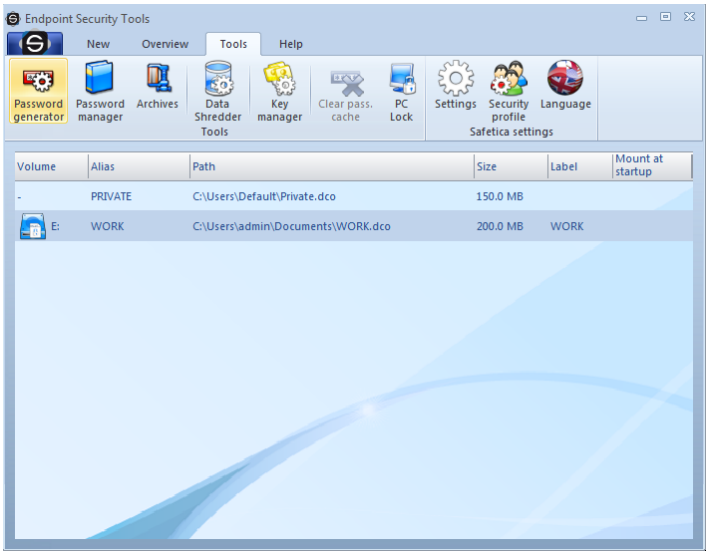


6.2.8 Password generator

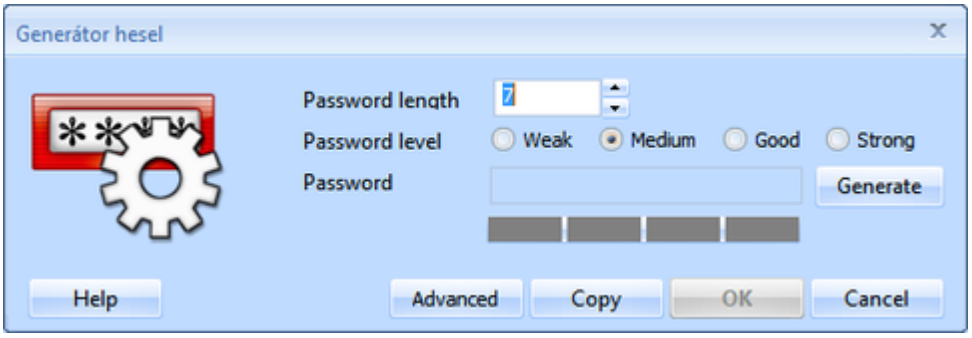
We have often to choose different passwords and not every time passwords like „alice“ are safe enough. Logical tendency is to use known words, names, birth dates or similar phrases. Unfortunately these options are the first ones the attackers try with techniques like dictionary attack or brute force 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.

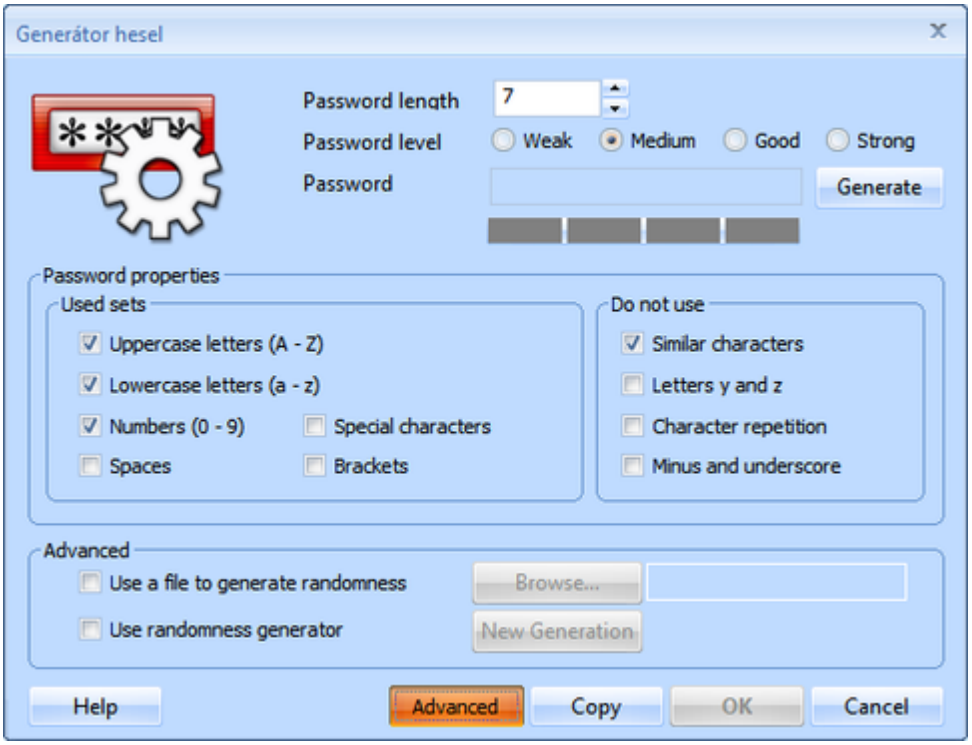
Password generator is integrated into all required sections of Endpoint Security Tools - you can directly from the dialogs for choosing a password open this generator and generate a password. And not only that, you can store immediately the password into database as well.



This tool is accessible from the tab Tools and from all passwords dialog as well.



In the basic view of the generator, you can choose simply what level of password and its length you need and after selecting the button Generate, the desired password will appear. Password can be immediately copied into clipboard and used in a web service registration for example.



The advanced view allows to set detailed options and to select what characters the password will contain or not.

To generate random passwords we use standardized randomness generators. To generate totally random sample you can use a picture file for example or use a widget, where you, by moving the cursor in a window, generate random sample, as well.

6.2.9 Choosing a password

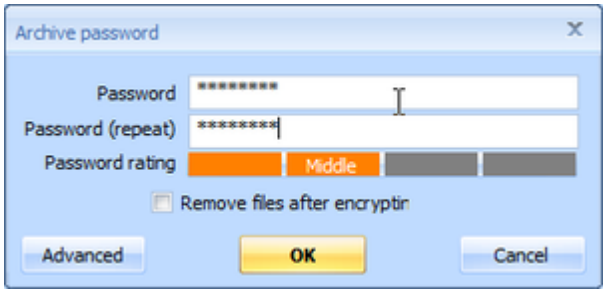
It is not the choice of an encryption algorithm that plays a key role in data security but a correct choice of an access password. Main keys are derived from the password by means of complicated algorithms. These keys are indirectly used for the encryption process itself.

If an attacker was able to solve one DES cipher within one second, they would solve one AES cipher in 149 trillion years provided that the key size is 128 bits. If the access password was "aaa" under the same conditions one could hardly speak about a real security of the data saved. An attacker would have a trivial access to your data by using an attack of dictionary type. A recommended length of a password is at least 20 characters. The password should contain small as well as big letters, numbers, and special characters (~!@#$%^&*():"<>?{}|\][;'/.,`).

A password should not contain:

- Name or surname of the user, their relatives or parts of their names
- Dates of birth of a user and their relatives or other memorable days.
- Names and relationships related to the user
- Well-known names or words, or words that exist in the Czech or English language.

You do not have to be afraid from choosing safe password - the dialog of Endpoint Security Tools will immediately analyze your password and graphically shows you level of password. If the bar is green you can be sure you entered a safe password.



How to remember a long password?

Do not get scared because of the length of the password. You can use mnemonics, for example a rhyme, to remember your password. A password can be then composed of letters at the beginnings of words in the rhyme.

Example:

Abbtsbpobichtwm.Ithftbhdntma!

"A big broken tooth should be pulled out because it could hurt the whole mouth.

I told him five times but he did not take my advice!"

How to store password?

The absolute recommendation of storing password is by remembering it. At no cost do not give anybody your password and do not write it down nowhere and do not store it in any other way! Endpoint Security Tools never stores password (unless you choose it from advanced options, but this is not recommended) neither the encryption key and if this key is stored in computer memory, it prohibits to the Operation System to store it on the hard drive (see paging). From this view the weakest part of Endpoint Security Tools is the Human Factor - so we strongly do not recommend to underestimate the choice of good password! If you will learn, how to enter safe passwords, you do not have to be afraid of loosing your data.

I forgot the password, what now?

If you are using security keys, you do not have to be worried. The procedure how to recover data is here.

6.2.10 Recommendations for increasing security

Security is not a permanent state but a long-time process...

1. **Important!** Switch off hibernation in Windows. If you switch your computer to a hibernation mode, the whole content of internal memory will be stored on a disk. After leaving the hibernation mode this content will be reloaded and the system will be at the same place as before hibernation. In case the hibernation mode was used it could happen (highly likely) that the a part of memory with the encryption key would be saved on the disk in the non-encrypted form. This risk is extremely huge and the program cannot fight back.

   You can disable Hibernate in this way

   Click on:

   Start -> Control Panel -> Power Options -> Hibernate

   Then untick: Enable hibernate mode If your computer supports other modes of hibernation it is not recommended to use them and we advise you to disable them. Otherwise, you take a risk of a key leakage in case of theft.

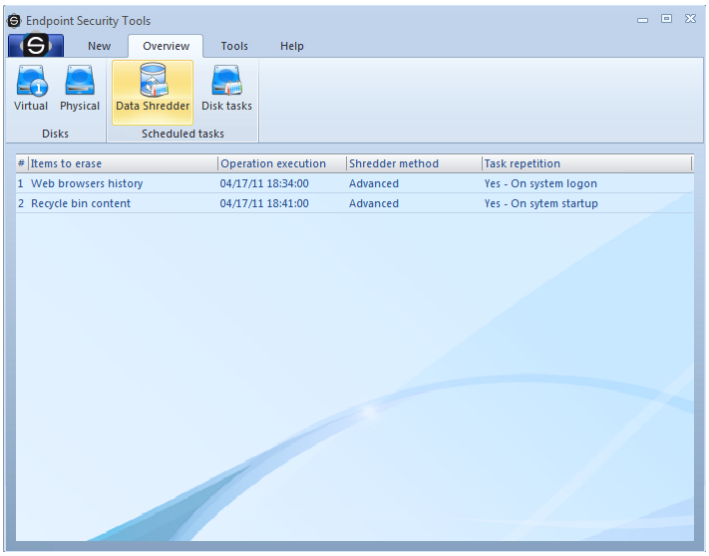
2. **Important!** Never tell your password to anybody else, do not keep your password in any form. Password is the most important thing you need to be able to access your data. We

recommend you to study the following topic about choosing a suitable password.

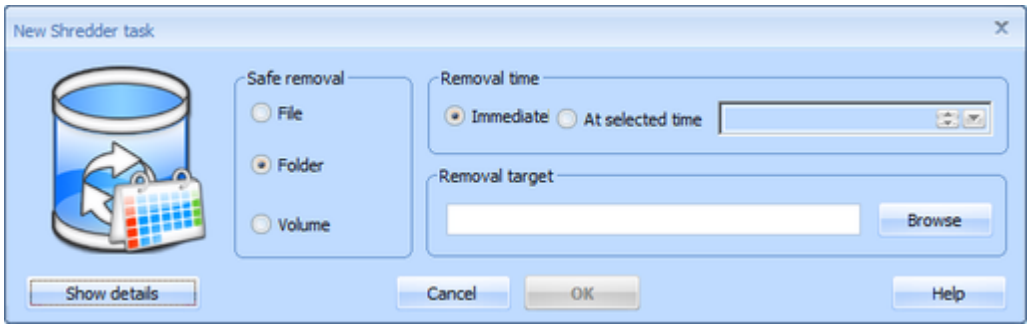
6.2.11 Data shredder

Did you know, that by deleting the files, you cannot ensure their safe removal? Even data from formatted disks can be easily recovered. Shredded data can never be renewed (not even in an IT lab).

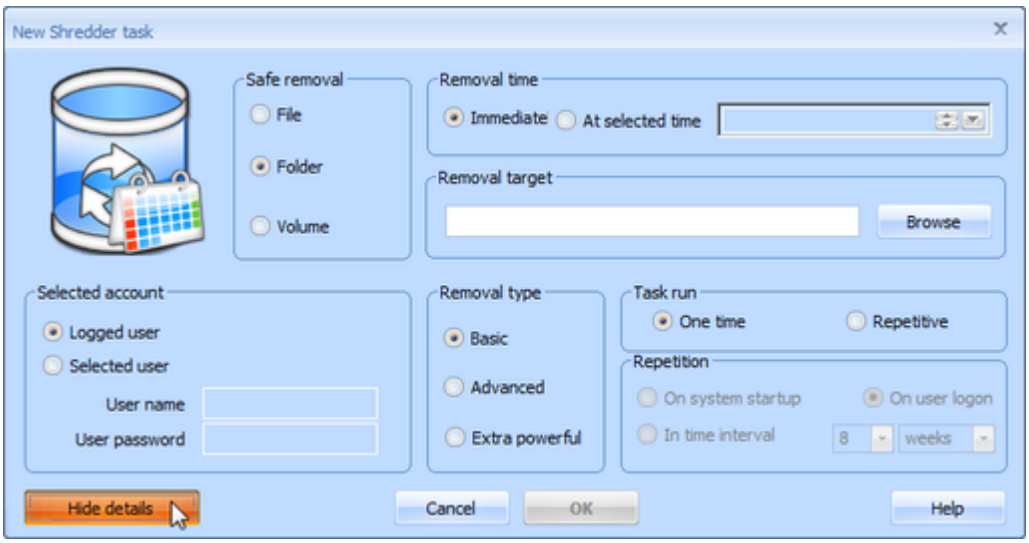
You can start the shredding by choosing from the tab *New -> Data shredder*.



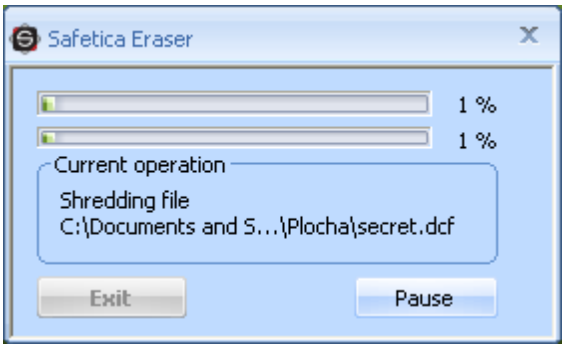
There will appear a simple dialog.



In the first step choose which data you want to shred - files or whole folders or even empty place on the drive.



At the end choose method and time of shredding and confirm it by clicking Ok. If time of the task is selected "Now" it will immediately start after selecting Ok. Otherwise at the time you selected (and it can be periodically if you wish).



For those, who prefer removing data straight from Windows Explorer or from favorite file manager, they can do it from context menu, which is reachable by right-clicking on the file/folder.

6.3 Advanced security

Security is at this time the most actual topic in IT. Today, there are practically no problems with the speed of executing the data, data saving, or in the slow access to such data or lack of storage holds. The most information problems of today and tomorrow are in securing such data

Endpoint Security Tools ensures a full protection of all your data against theft, and also against dangerous or curious colleagues. Our cutting-edge security Endpoint Security Tools will in case of a theft, give the attacker just worthless and unreadable data. With the help of advanced security methods, you will be able to protect your software and valuable data, which are necessary for your work.

The encryption mode of the Endpoint Security Tools is build on the PKCS #5 v2.0 encryption standard with the support of the safest hashing functions.

The ciphers were carefully chosen and there is not missing the AES cipher, certified by the American organization - National Institute of Standards and Technology (NIST) for use in the most strict conditions for TOP SECRET materials and used by the government of the USA. Endpoint Security Tools contains really only the most modern encryption standards.

6.3.1 The choice of cipher

You cannot make a mistake whichever cipher you choose in Endpoint Security Tools. We did our best to choose optimal ciphers and sizes of their keys with emphasis on their security and speed for a demanding business use.

In case you save very risky materials or programs we recommend you to use ciphers Serpent, Twofish, Rijndael or Blowfish. On the contrary, for the needs of frequent and huge data transfers RC5, RC6 or Twofish are recommended.

Generally, however, we point out that the choice of cipher is a secondary matter from the security point of view. We recommend you to focus on a careful choice of an access password.

6.3.2 Selection of hash functions

Hash function is a secret function that is needed especially when deriving a password. For all common operations the SHA-256 function is sufficient. It is not necessary to address this topic.

For an interested person we give an explanation and description of these functions:

The choice of a hash function is uniquely motivated by its simplexity and the absence of collisions. These attributes have been recently broken through in case of a lot of world wide recognized and frequently used functions (RIPEMD, MD5, SHA-0). These functions are naturally not implemented in Endpoint Security Tools. We have employed only the best quality algorithms consisting of Tiger algorithms and the SHA-2 family. We recommend you to use the initial SHA-256 function. Hash functions SHA-384 or SHA-512 are made-to-measure for truly intransigent advocates of security and military bodies.

- **TIGER** – A new method of generating prints have been invented by researches Ross Anderson and Eli Biham in 1995. This method is ready to fully exploit the potential of the forthcoming 64-bite architecture of a new computer generation. It generates a 20- or 24-byte print fully meeting the needs of an advanced disk encryption.
- **SHA-2** - The latest hash class SHA (Secure Hash Algorithm). The specification of this class includes definitions of new variants (sometimes collectively denoted as SHA-2) that include SHA-256, SHA-384 a SHA-512. It generates 32,48 or 64-byte prints.

6.3.3 Ciphers used

- **Blowfish** – One of the most secure ciphers proposed by a specialist in cryptology Bruce Schneider. Although it has been designed already in 1993, it is still one of the best and most often used ciphers. Blowfish is used as a standard cipher in the OpenBSD operating system, that is still considered by specialists as one of the most secure operating systems in the world. We offer this cipher with a key length of *448 bits*.
- **CAST5** - Created in 1996 and used by the Canadian government and its spy services Communications Security Establishment for a long time. Authors are Carlisle Adams a Stafford Tavares. It enables encryption by a *key 40-128 bits* long. Endpoint Security Tools supports a key length of 128 bits.
- **CAST6** -derived from CAST5, created by the same authors in 1998 and often used until now. This cipher has also been proposed as a AES standard. Its main advantage over CAST5 is a longer key - *256 bits* for a double size of an encrypted block compared to the predecessor.
- **MARS** – Another cipher from the AES top-five, designed in cooperation with the IBM corporation. Its author, Don Coppersmith, worked as a coauthor on the creation of the DES encryption standard in 1975. MARS has a quality design, works with a key *448 bits* long and is intended for inhospitable environments.
- **RC5** – RC is an abbreviation for Rivest Cipher according to the name of its author Ronald Rivest. This cipher was designed in 1994, it is fast and has a variable key lengths. We have implemented RC5 with a key length of *512 bits*. It is recommended to use this cipher on disks where big amount of data are often processed.
- **RC6** – a successor of RC5, that was also a runner-up in the AES final group. Overtakes a quality design, which is manifested not only in the security but also in the speed of an algorithm. Complements the RC5 cipher with an increased security and a key length of *512 bits*. Because of its speed we recommend you to use this cipher in case a big amount of data is often saved.
- **Rijndael (AES)**: an official advanced encryption standard proposed by Joan Daemen a Vincent Rijmen, it is a winner of the contest for a new AES encryption standard. Members of a final committee gave most votes to this cipher. The National Security Agency (NSA) classified this cipher with key lengths of 192 and 256 bits for the application on materials with the level of secrecy *TOP SECRET*. The key length for the Rijndael-AES cipher in Endpoint Security Tools is *256 bits*.
- **Serpent** – considered by cryptologists as one of the most *secure block ciphers*. Its excellent security parameters classify it among the leading ciphers in a secure storage of confid-

ential materials. In case of using the new 64-bit computer architecture it's implementation in Endpoint Security Tools is not only very secure but also very efficient. The key length is *256 bits*.

- **Twofish** - Another high quality encryption method. As a Blowfish-successor it fully meets the requirements on a high security and speed of encryption. It is also an AES runner-up and has very good security results. The implemented Twofish cipher is *256 bits*.

6.3.4 Deniability

One of other benefits that the Endpoint Security Tools provides is the deniability of data. Data are protected by strong ciphers that are impossible to decipher within real time. Encrypted data protected by Endpoint Security Tools look on the original disk as common random data and they appear for other potential attackers as if there were no data. Therefore, you can deny the existence of the data whenever you want.

All materials protected in this way for any needs are not detectable.

6.4 List of definitions

- **Allocation unit** - The smallest part of a disk space that we can use for saving a file. An example: Let's choose the size of an allocation unit to be 32kB. If a small file of 1kB size is written on a disk the whole 32kb cluster is occupied. On the one hand, increasing the size of an allocation unit leads to a speed up of access for disk operations, but on the other hand it is wasting of disk space in case of small files. It is recommended in the Endpoint Security Tools to keep the initial value.
- **Bit** - A basic unit of information. It takes the value 0 or 1.
- **Byte** - A unit of information quantity, a sequence of 8 bits.
- **Cluster** - see Allocation unit.
- **DES** - A standard encryption algorithm from the middle 1970's. It is very obsolete nowadays and today's modern computers can break this cipher within a couple of hours.
- **File system** - see File system.
- **Hash function** - It is a formula for the calculation of a check sum (print) for a message or a bigger amount of data. It can serve for controlling data integrity, fast comparing of a pair of messages, indexing, searching etc. It is an important constituent of cryptographic systems for digital signatures.
- **Simplexity** - It is a property of a hash function which indicates that it is computationally impossible to obtain an original pattern from a hash value already computed.
- **Disk label** - A text string representing the name of a particular disk partition.
- **Collision of a hash function** - An undesirable phenomenon upon which a couple of input texts are found within real time such that a hash function creates the same print for them.
- **Compilation** – The process of making up a program from source files, written by programmers, into an executable form (e.g. the well-known “.exe“ extension).
- **Operating system** (OS) – Basic software of a computer. Program equipment enabling elementary work with computer hardware and a communication with additional devices. Among the best-known operating systems are e.g. systems of Microsoft® Windows® family.
- **Dictionary attack** – Trial and error method for determining a password by trying possibilities derived from a list of words in a dictionary.

- **File system** - A designation for the way of organizing information (files) stored on memory devices (hard disks, tapes, CDs, DVDs). A file system divides a section on a disk into files and directories. Examples: FAT16, FAT32, NTFS.
- **Paging** - It is a process during which a less-used part of internal memory is temporarily stored by an operating system on a disk so that space can be made for new and more-used data. The reason for that is a more optimal usage of memory space, the disadvantage is a slower operation of an operating system at a frequent disk activity.
- **Encryption key** - It is a block of data used as a key for encryption. Its length is usually given in bits. This block of data has to be kept in confidence. Otherwise it looses its sense.
- **Internal memory** - Memory for the work of a computer processor. It is fast, much faster than external memory - hard disks etc.

7 List of definitions

Term	Synonym	Abbreviation	Description
Safetica	product		Product name.
Auditor	Auditor		One of the main Safetica modules.
DLP	DLP		One of the main Safetica modules.
Supervisor	Supervisor		One of the main Safetica modules.
Safetica Management Service	server service	SMS	A service representing one branch.
Safetica Management Console	console	SMC	A management console for Safetica.
Safetica Endpoint Client	client station	SEC	A client on the employees' end stations. It is responsible for enforcement of the security policy and alternatively it enables the employees to use the security instruments.
Safetica Client Service	client service	SCS	A service on the client station that handles connection with the server service and database.
Endpoint Security Tools		EST	Security instruments on the client station. Available only with a valid DLP license.
Module			General identification of Auditor, DLP or Supervisor module.
Function			General description of the parts of the individual modules such as Disks, Anti-keylogger , Applications....
Main menu			The upper bar in the Safetica Management Console interface containing the controls.
User tree			Identification of the main user tree in the left part of Safetica Management Console containing users, computers, groups and branches (SMS servers).
View			General identification of the part of the graphic interface in Safetica Management Console that serves for displaying the settings and visualization of the selected functions.
Branch			General identification of one SMS together with the users, computers and groups that are connected to it and the corresponding database.
Visualization mode			Name of the console mode used for viewing data and graphs obtained from monitoring.
Setting mode			Name of the console mode used for setting modules and functions.
Log			List of records with detailed information
Web categories			Identification of the database of webs for categorization
Application cat-			Identification of the database of applications for categoriza-

egories			tion
Extension categories			Identification of the database of suffixes for categorization
Alerts			Automatic notifications sent when a certain event occurs.
Tag			The mark of the product Safetica that is saved together with the file or folder and places it in a certain group of secured data unambiguously.
DLP			Data Loss Prevention/Protection

INDEX

- V -

www.safetica.com