SAFETICA
COMPLETE DOCUMENTATION

safetica®

SAFETICA
COMPLETE DOCUMENTATION

product Safetica version 7.5.x

Author: Safetica Technologies s.r.o.

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

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

For more information visit www.safetica.com.

Published: 2017

CONTENT

Introduction

About safetica

Installation

Console

Client

INDEX

1 Introduction

Dear user,

Thank you for choosing Safetica. We are certain that you will be fully satisfied. In this document you will find a detailed description of all the components of the product and manual 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 of 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 master basic practices and usage quickly, use the *Safetica quick* guide.

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 reputation. At the same time, it alerts you to potentially dangerous behavior among your staff long before their conduct threatens your company.

Safetica modules

Auditor

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

DLP

Prevent your employees from misusing the 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

The Safetica product is based on a client – server architecture. On end workstations, the Safetica client runs communicating with the server. Together with the client, the downloader agent runs on workstations, which is designed to install, update and manage other client components. To manage, set up, and display the obtained data, the console or WebSafetica is used. Data obtained from individual end workstations are stored on a database server. The database also stores the settings for all Safetica components.

Each of the following parts can be installed on a separate computer.

Server

The Safetica server runs as a service on a dedicated server, provides connection between the database and other Safetica components and enables their remote management.

On each server, a console can be used to set up different rights for individual administrators (or managers), making it possible to create different roles for security management (e.g. local admin, enterprise admin, security manager and more).

Recommended hardware and software requirements

Quad-core processor 2.4 GHz, 2 GB RAM, 3 GB disk space. Supported operating systems are Microsoft Windows Server 2008 R2 or later.

Note: Only a single server instance can be installed on one computer.

Console

The console is used to set up and manage clients and downloader agents on end computers and for server services (of the server) and databases; it's also used to set up all Safetica functions on endpoint stations. It also displays the output of acquired data, statistics and graphs. It can run anywhere provided there is a connection to the managed server.

Recommended hardware and software requirements

Dual-core processor, 2 GB RAM, 2 GB of disk space. Supported operating systems are Microsoft Windows 7 32-bit and 64-bit and newer versions of the Windows operating system.

WebSafetica

WebSafetica is a web console for managing Safetica and displaying records obtained from endpoint stations.

Help for its use and deployment is available online at https://support.safetica.com/English.

Downloader Agent

The Downloader client is a Safetica component used to manage the Safetica client on end computers. It allows remote installation, updating and other management tasks.

Recommended hardware and software requirements

The same as the requirements of the console.

Client

The client provides all the security and monitoring functions of Safetica at endpoint stations. It consists of the following main parts:

- *Client service* – is always launched at system startup and provides monitoring, enforces the security policy and facilitates communication with the database and server. The client service manages the operation of the Auditor, DLP and Supervisor modules on the endpoint stations.

During the installation of the client, the *Downloader Agent* component will be installed automatically unless it has been installed previously.

Note: The minimum supported version of the Safetica client is 6.8.

Recommended hardware and software requirements

The same as the requirements of the console.

Database

The database is used to save the settings and records received from all Safetica components. Each server needs three dedicated databases to store logs, settings and categories of applications, sites and extensions. To save the databases, Microsoft SQL Server 2008 32-bit and 64-bit and higher versions, including Express editions (www.microsoft.com) can be used. WebSafetica is available only for MS SQL 2012 and higher, including Express editions

Note: For hardware and software requirements of the database servers mentioned above, please visit the website of the manufacturer.

3 Installation

Safetica is installed using a universal installer that includes all necessary components. Once you run it, you can chose one of the two installation methods:

- Automatic installation (Safetica installation) – automatically installs all components on a computer.
- Manual installation (Expert installation and extraction of components) – manual installation of individual Safetica components.

Choose one of them and continue in the installation.Enter topic text here.

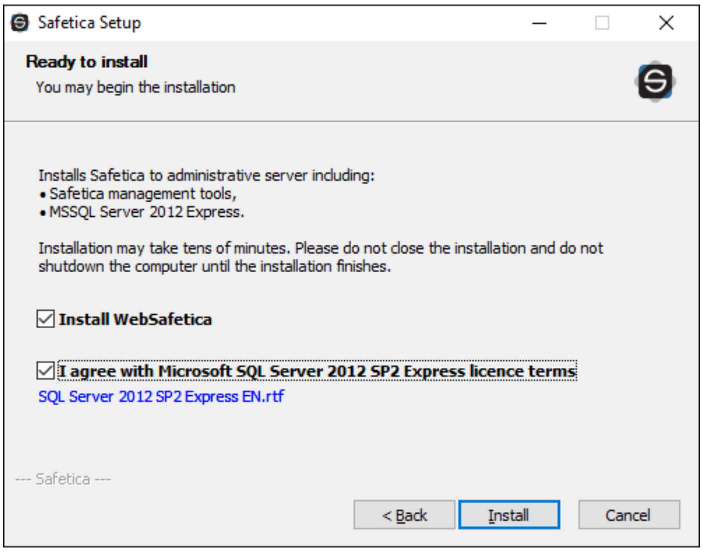
3.1 Automatic installation

In automatic installation, the following Safetica components are installed on the computer: Safetica server, Microsoft SQL Server Express database, WebSafetica (optional installation).

Clients are installed during the first launch of Safetica after installation. Make sure the computer has enough computing power to handle operation of the database, server and optionally also WebSafetica. The recommended configuration is a quad-core processor, 8 GB RAM, 100 GB free disk space.

After launching the Safetica installer, proceed as follows:

1. Click on Automatic installation and confirm the licence agreement
2. The next step displays the hardware requirements. Read them and continue.
3. Before you start the installation, you can choose whether you also want to install WebSafetica (this option may extend the total installation time). Confirm the licence conditions of the SQL server and start the installation by clicking Install.



Safetica Setup

Ready to install

You may begin the installation

Installs Safetica to administrative server including:
- Safetica management tools,
- MSSQL Server 2012 Express.

Installation may take tens of minutes. Please do not close the installation and do not shutdown the computer until the installation finishes.

☑ **Install WebSafetica**

☑ **I agree with Microsoft SQL Server 2012 SP2 Express licence terms**

SQL Server 2012 SP2 Express EN.rtf

4. After the installation, the management console will launch automatically, opening a wizard that will help you complete the initial setup of Safetica.

Note: The integration mode in automatic installation is set to Stealth. For more information about Safetica integration please see Integration Settings.

3.2 Manual installation

Please follow this procedure for Safetica deployment:

1. Before installation please check whether your network fulfils the deployment conditions.
2. Install the server on selected computers. During installation, choose which database will be used by server for storing data.
3. Install the console or WebSafetica on the PC from which you want to manage Safetica.
4. Using console, connect to the server and perform initial Safetica configuration.
5. Install downloader agent on the end workstations.
6. Use console to install the client on the end workstations (client installation via console is only possible on computers with the downloader agent installed).

After deploying all components and checking if everything has been correctly installed, you can start working with Safetica.

In the chapters below you can find a more detailed description of each deployment step.

3.2.1 Before installation

Take the following steps before installation:

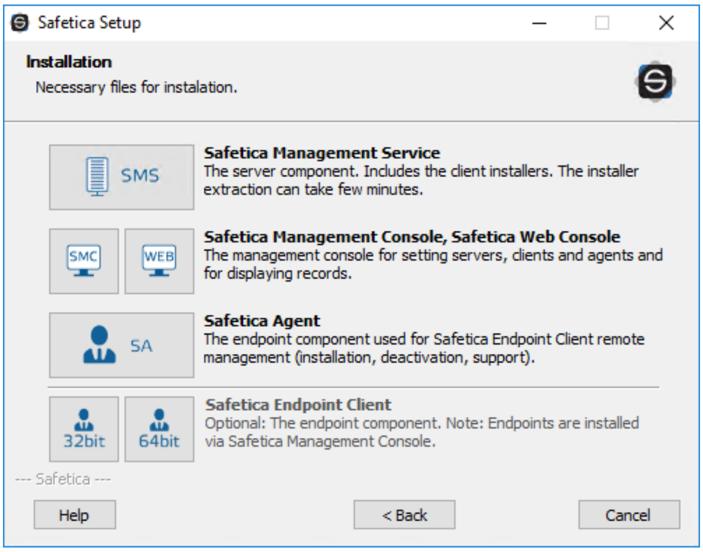
1. Check whether the hardware and software requirements of all three Safetica components are met.
2. Analyze your corporate network:
   - o Decide on what PCs you are going to install the server in your environment. When making the decision, take the following into account:
     - The PC with Safetica server 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 servers you wish to install in your environment. The number of SECs that can connect to one server is limited by the SQL database which the server uses for storing data – see below.
   - o Decide on what PCs you are going to install the console in your network. The PC with console must be able to connect to all servers you wish to administer by using the administration console.
   - o Decide on what PCs you are going to install the downloader agent in your network.
     - The PC with downloader agent must be able to connect to some server in your environment.
   - o Decide on what PCs you are going to install the Safetica client in your network. When making the decision, take the following into account:
     - For every Safetica client, decide what server it will be connected to. Not every PC will be connected to all PCs with server.
     - The PC with client must be able to connect to some server in your environment.
   - o Select and designate SQL servers on which the central databases of the individual server will be stored. When making the decision, take the following into account:
     - Every server needs three designated databases on the SQL server: one for settings, one for records and one for the category database.
3. Before installing the various Safetica components (server, console, client), 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 server will be installed:
     - 4438 (communication client -> server, database).
     - 4441, 4442 (communication console -> server).
   - o Add exceptions for the process STAConsole.exe on the PCs on which you will install the console.
   - o Set exceptions for the following processes on the PCs on which you will install the client: STCService.exe, STUserApp.exe, Safetica.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.
     - 1443 (communication client, server -> database).
4. Download the universal installer with the latest Safetica release.
   - o The universal installer contains all components necessary for installation.

3.2.2 Installing server

Safetica server ensures that all Safetica clients, the console 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.



Installation

Necessary files for instalation.

Safetica Management Service
The server component. Includes the client installers. The installer extraction can take few minutes.

Safetica Management Console, Safetica Web Console
The management console for setting servers, clients and agents and for displaying records.

Safetica Agent
The endpoint component used for Safetica Endpoint Client remote management (installation, deactivation, support).

Safetica Endpoint Client
Optional: The endpoint component. Note: Endpoints are installed via Safetica Management Console.

2. Here you several options:

   o Run the installation directly from the universal installer by clicking on Run Installer.

   o Extract only the server 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 client or Microsoft SQL Server 2012 SP2 Express. If you are going to install Microsoft SQL Server 2012 SP2 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. This is followed by an important step of configuring Microsoft SQL Server where the installed server will store its databases.

6. Furthermore, please specify:

   o *Enable automatic definition update* – by selecting this option you allow console to automatically install the updates of definitions (if Internet and database connections are available). The updating process may increase the workload of the SQL Server. This setting can be changed any time you like in *Console -> Maintenance ->* *Update* *-> Definition updates.*

   o *Send statistics automatically* – select this option to allow console to send anonymous statistical information to Safetica Technologies which in turn allows us to actively solve any problems and to improve the product. No sensitive information or security-related information is sent. You can change this setting any time you like in *Console -> Maintenance -> Database management ->* *Maintenance* *-> Statistics sending*.

   It is advisable to keep both the options enabled.

7. Complete the installation. Server 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, 4441 and 4442 are not blocked.

Note: By default, console uses ports 4441, *4442 for connecting to server and client uses port 4438. You can change the settings to use different ports as well.*

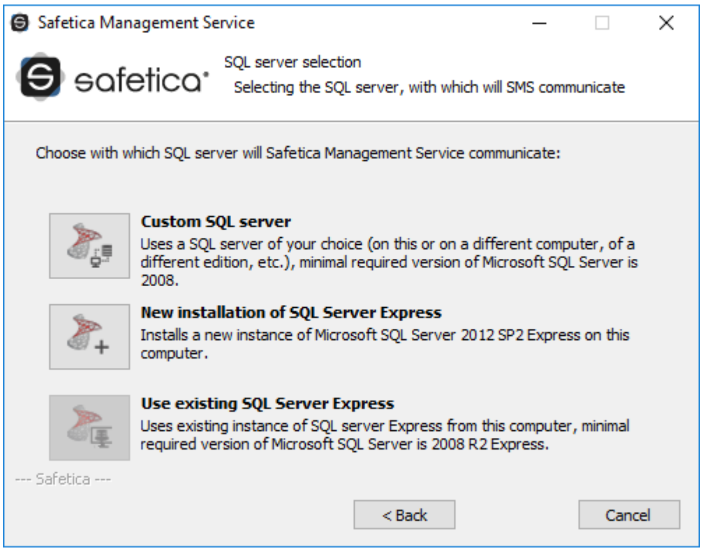
3.2.2.1 Microsoft SQL Server settings

Next, you must choose the SQL Server on which the server will store the databases. You can choose from the following options:

a. *Custom SQL Server* – 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. *New installation of SQL Server Express* – If choosing this option, you will install Microsoft SQL Server 2012 SP2 Express on your existing PC. The new server will be used for creating the server databases. For a description of the installation, continue to Installation of New SQL Server Express.

c. *Use existing SQL Server Express* – If you have an existing instance of Microsoft SQL Server 2012 SP2 Express on the PC where you are going to install server, you can choose this last option. The existing SQL Server will be used for storing server databases. For a description of the configuration, continue to Configuring an Existing SQL Server.



Safetica Management Service

SQL server selection

Selecting the SQL server, with which will SMS communicate

Choose with which SQL server will Safetica Management Service communicate:

Custom SQL server
Uses a SQL server of your choice (on this or on a different computer, of a different edition, etc.), minimal required version of Microsoft SQL Server is 2008.

New installation of SQL Server Express
Installs a new instance of Microsoft SQL Server 2012 SP2 Express on this computer.

Use existing SQL Server Express
Uses existing instance of SQL server Express from this computer, minimal required version of Microsoft SQL Server is 2008 R2 Express.

Configuring an Existing SQL server

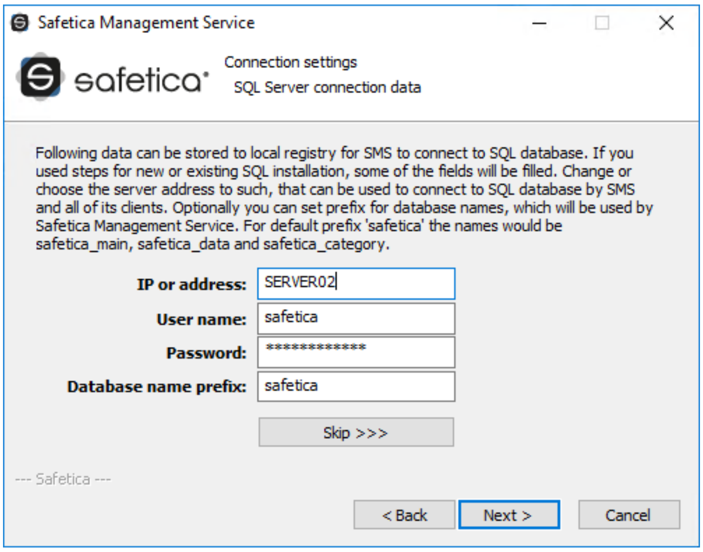
If you choose your own SQL server during Safetica server installation, you need to check first if this server is correctly set for storing databases.

- 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 administration rights (*sysadmin*) 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 server and for Safetica clients that will connect via this server. 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 administration rights (*sysadmin*). The user will be applied for creating and connecting to all three databases that will be automatically created on the SQL server after server installation.
   - *Password* – SQL server user name.
   - *Database name prefix* – adds a prefix in front of the database name. For instance, when using the *db* prefix, the resulting database names will be *db_main*, *db_log* and *db_category*.



Following data can be stored to local registry for SMS to connect to SQL database. If you used steps for new or existing SQL installation, some of the fields will be filled. Change or choose the server address to such, that can be used to connect to SQL database by SMS and all of its clients. Optionally you can set prefix for database names, which will be used by Safetica Management Service. For default prefix 'safetica' the names would be safetica_main, safetica_data and safetica_category.

IP or address: SERVER02
User name: safetica
Password: *************
Database name prefix: safetica

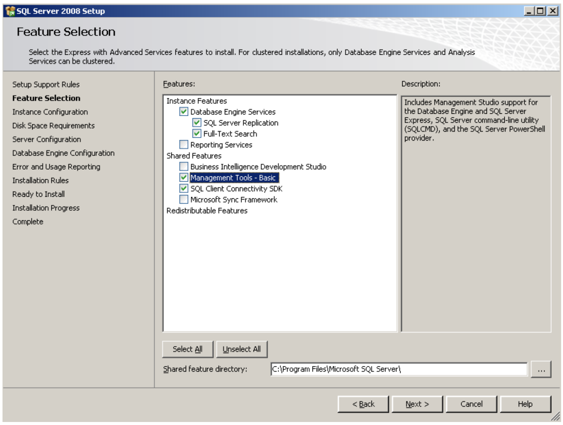
2. Click *Verify and save*.
3. Click *Next*, continue and finish server installation. After completing the server installation, three databases will be created on the SQL server:
   - *safetica_main* – used for storing and sharing settings between server and client.
   - *safetica_data* – used for storing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

Note: You can later change the connection to the server via the console in the Server settings section. The configuration of this connection is described in the section server settings.

3.2.2.1.1.1 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.



SQL Server 2008 Setup

Feature Selection

Select the Express with Advanced Services features to install. For clustered installations, only Database Engine Services and Analysis Services can be clustered.

Features:

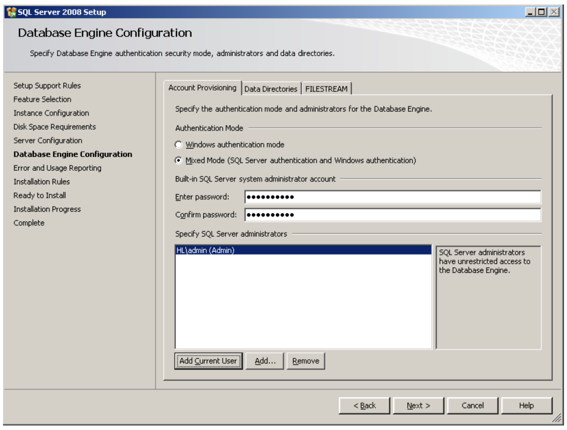
- Instance Features
  - ☑ Database Engine Services
    - ☑ SQL Server Replication
    - ☑ Full-Text Search
  - □ Reporting Services
- Shared Features
  - □ Business Intelligence Development Studio
  - ☑ Management Tools - Basic
  - ☑ SQL Client Connectivity SDK
  - □ Microsoft Sync Framework
- Redistributable Features

Description:

Includes Management Studio support for the Database Engine and SQL Server Express, SQL Server command-line utility (SQLCMD), and the SQL Server PowerShell provider.

Shared feature directory: C:\Program Files\Microsoft SQL Server\

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



SQL Server 2008 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators and data directories.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Built-in SQL Server system administrator account

Enter password: ••••••••••

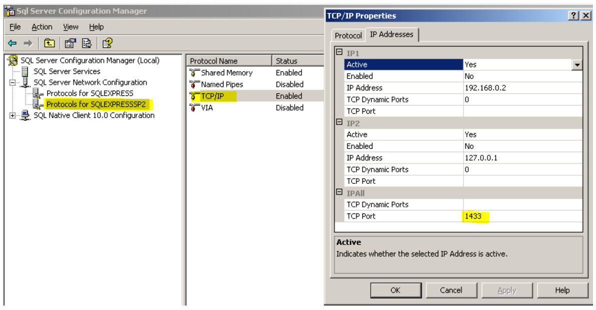
Confirm password: ••••••••••

Specify SQL Server administrators

HL\admin (Admin)

SQL Server administrators have unrestricted access to the Database Engine.

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



Sql Server Configuration Manager

- SQL Server Configuration Manager (Local)
  - SQL Server Services
  - SQL Server Network Configuration
    - Protocols for SQLEXPRESS
    - Protocols for SQLEXPRESSSP2
  - SQL Native Client 10.0 Configuration

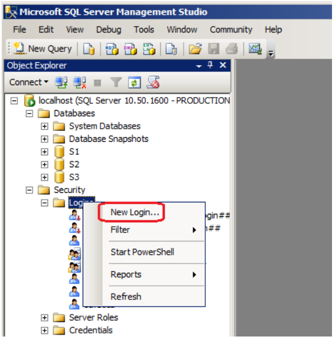
Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Disabled
TCP/IP	Enabled
VIA	Disabled

TCP/IP Properties

IP1	
Active	Yes
Enabled	No
IP Address	192.168.0.2
TCP Dynamic Ports	0
TCP Port	
IP2	
Active	Yes
Enabled	No
IP Address	127.0.0.1
TCP Dynamic Ports	0
TCP Port	
IPAll	
TCP Dynamic Ports	
TCP Port	1433

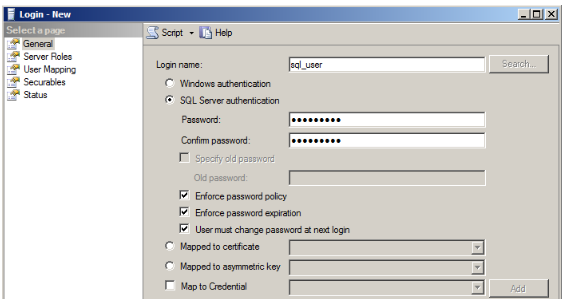
Active
Indicates whether the selected IP Address is active.

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.



Microsoft SQL Server Management Studio

- localhost (SQL Server 10.50.1600 - PRODUCTION
  - Databases
    - System Databases
    - Database Snapshots
    - S1
    - S2
    - S3
  - Security
    - Logins
    - Server Roles
    - Credentials



Login - New

Login name: sql_user

○ Windows authentication

● SQL Server authentication

Password: •••••••••

Confirm password: •••••••••

□ Specify old password

Old password:

☑ Enforce password policy

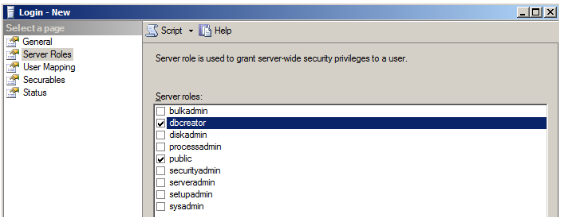
☑ Enforce password expiration

☑ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

□ Map to Credential



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

Server roles:

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

The connection of server to these databases is set via console in section Server settings.

Installing a new SQL Server Express

If you do not own any SQL Server, you can install Microsoft SQL Server 2012 SP2 Express from this installer.

Note: The Express edition comes with the following restrictions:

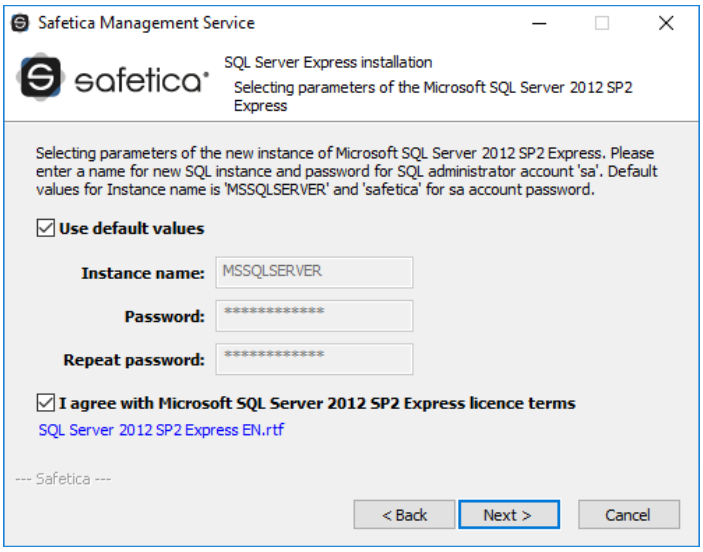
- It uses only one processor.
- It uses maximum 1 GB of RAM.
- The maximum database size is 10 GB.

Due to these restrictions to the Express edition of the SQL Server, the ideal number of SECs connected to server 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.

Note: If the group policy (local or domain policy) defines a certain password complexity, then a password must be entered for SQL installation that corresponds to the policy set.



SQL Server Express installation

Selecting parameters of the Microsoft SQL Server 2012 SP2 Express

Selecting parameters of the new instance of Microsoft SQL Server 2012 SP2 Express. Please enter a name for new SQL instance and password for SQL administrator account 'sa'. Default values for Instance name is 'MSSQLSERVER' and 'safetica' for sa account password.

☑ **Use default values**

Instance name: MSSQLSERVER

Password: *************

Repeat password: *************

☑ **I agree with Microsoft SQL Server 2012 SP2 Express licence terms**

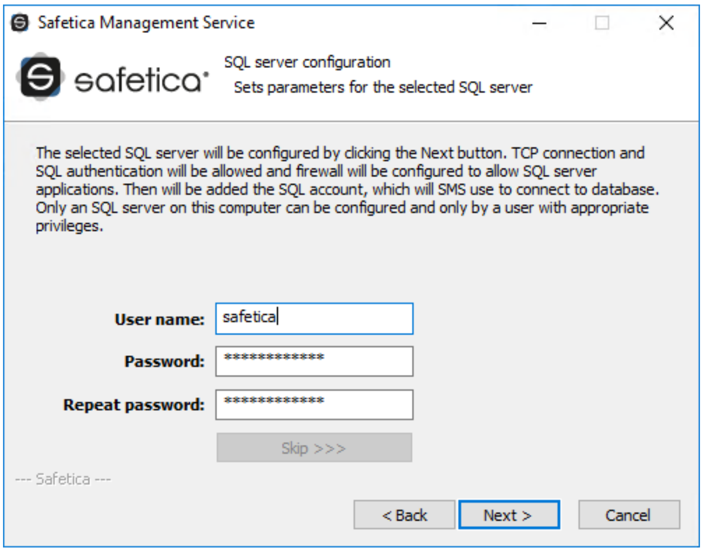
SQL Server 2012 SP2 Express EN.rtf

--- Safetica ---

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 2012 SP2 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*.


Safetica Management Service

SQL server configuration

Sets parameters for the selected SQL server

The selected SQL server will be configured by clicking the Next button. TCP connection and SQL authentication will be allowed and firewall will be configured to allow SQL server applications. Then will be added the SQL account, which will SMS use to connect to database. Only an SQL server on this computer can be configured and only by a user with appropriate privileges.

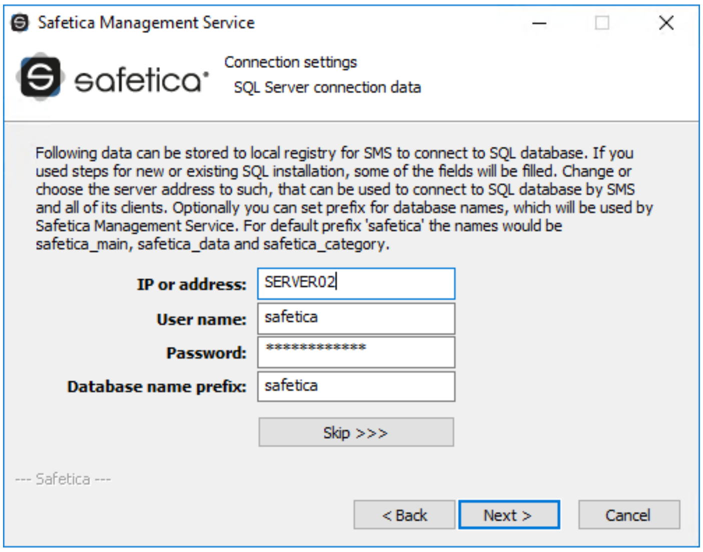
User name: safetica

Password: *************

Repeat password: *************

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*.


Safetica Management Service

Connection settings

SQL Server connection data

Following data can be stored to local registry for SMS to connect to SQL database. If you used steps for new or existing SQL installation, some of the fields will be filled. Change or choose the server address to such, that can be used to connect to SQL database by SMS and all of its clients. Optionally you can set prefix for database names, which will be used by Safetica Management Service. For default prefix 'safetica' the names would be safetica_main, safetica_data and safetica_category.

IP or address: SERVER02

User name: safetica

Password: *************

Database name prefix: safetica

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

- safetica_main – used for storing and sharing settings between server and client.
- safetica_data – used for storing data recorded from clients.
- safetica_category – used for storing applications, websites and appendices categories.

Note: You can later change the connection to the server via the console in the Server settings section.

Configuring existing SQL Server Express

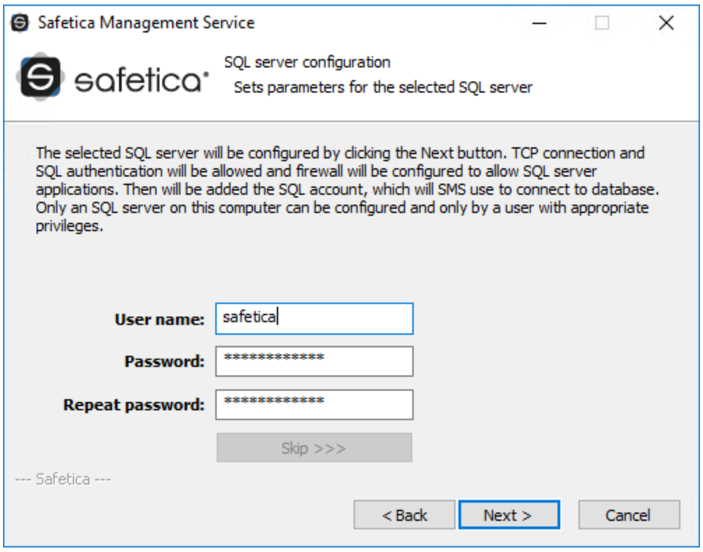
If you have Microsoft SQL Server 2012 SP2 Express already installed on the PC where you are installing the server, you can use it for creating the databases. The installer will automatically re-configure the existing SQL server installation on that PC. Server will automatically connect to this instance 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 clients connected to server 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*.



SQL server configuration

Sets parameters for the selected SQL server

The selected SQL server will be configured by clicking the Next button. TCP connection and SQL authentication will be allowed and firewall will be configured to allow SQL server applications. Then will be added the SQL account, which will SMS use to connect to database. Only an SQL server on this computer can be configured and only by a user with appropriate privileges.

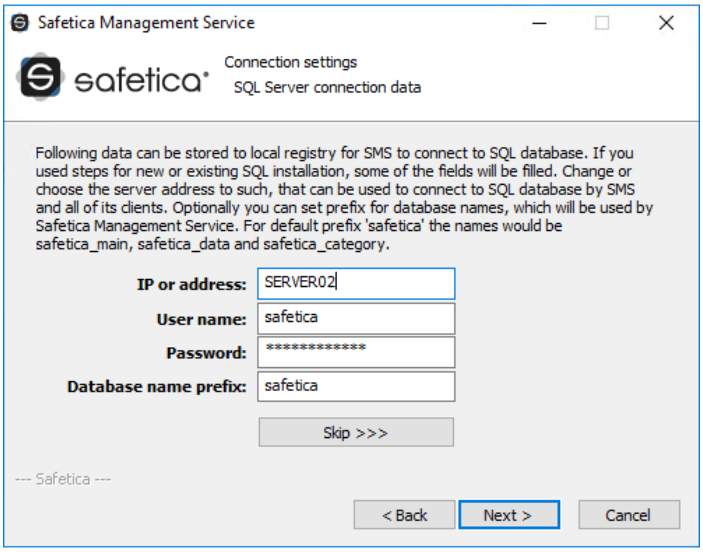
User name: safetica

Password: *************

Repeat password: *************

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*.



Connection settings

SQL Server connection data

Following data can be stored to local registry for SMS to connect to SQL database. If you used steps for new or existing SQL installation, some of the fields will be filled. Change or choose the server address to such, that can be used to connect to SQL database by SMS and all of its clients. Optionally you can set prefix for database names, which will be used by Safetica Management Service. For default prefix 'safetica' the names would be safetica_main, safetica_data and safetica_category.

IP or address: SERVER02

User name: safetica

Password: *************

Database name prefix: safetica

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

- safetica_main – used for storing and sharing settings between server and client.
- safetica_data – used for storing data recorded from clients.
- safetica_category – used for storing applications, websites and appendices categories.

Note: You can later change the connection to the server via the console in the Server settings section.

3.2.3 Installing console

The console is the central point for managing the software. It is used for setting up and managing both clients and servers 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 console, you can manage multiple instances of Safetica servers. All you need is a console running on any computer that can access the managed server. 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 Manahement Console*.
2. Here you several options:
   - o Run the setup directly from the universal installer by clicking on the *Run installer* button.
   - o Extract only the console installer, which you can then use separately for later installation.

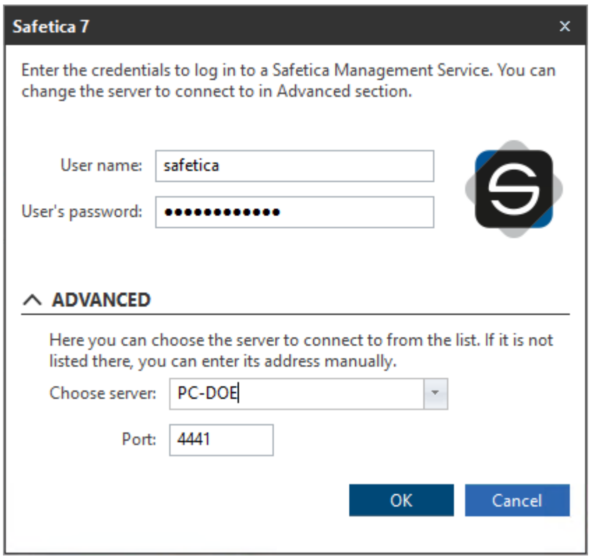
     Note: In the third part Tools and Components are components that are necessary for proper function of Safetica Enpoind Client or Microsoft SQL Server 2012 SP2 Express. If you will be installing Microsoft SQL Server 2012 SP2 Express.
3. After running the installer (either from the universal installer 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 *STAConsole.exe* process.

3.2.4 Initial configuration

After successfully installing the console and server, the whole system must be set up properly, before starting installing the downloader agent and client on end computers. All administration and settings are carried out via the console.

Overview of main configuration steps:

1. Start the console. In the dialogue box, enter the service account credentials to log on to the server. The service account username is *safetica* and the default password is *S@fetic@2004*. In the advanced settings, enter the address or name of the server with the installed server. Use the default port 4441 for the console logon to the server Finally, press OK to confirm.



Enter the credentials to log in to a Safetica Management Service. You can change the server to connect to in Advanced section.

User name: safetica

User's password: ●●●●●●●●●●●●

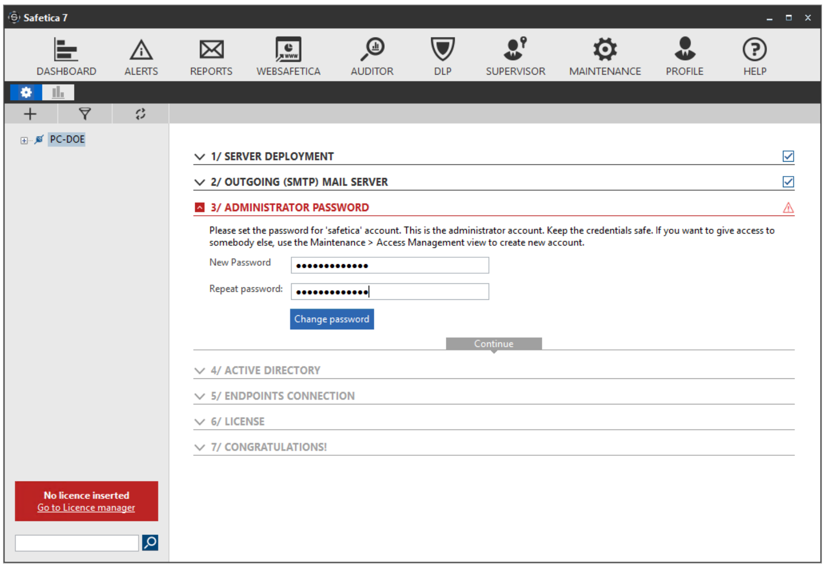
Here you can choose the server to connect to from the list. If it is not listed there, you can enter its address manually.

Choose server: PC-DOE

Port: 4441

2. Then the wizard for initial configuration is opened in Safetica. The setting of the Safetica server and SMTP server for sending e-mails is done during installation. If all goes well, the wizard opens in item three. Set the new Safetica service account password for logging into the Safetica console. Click on Continue.

   Note: The service account has full authorisation for all Safetica functions and settings. Keep the login credentials for this account in a safe place. If you want to provide others with the access to Safetica, create a new account for them in the tab Maintenance -> Access management -> Add account.



1/ SERVER DEPLOYMENT ☑

2/ OUTGOING (SMTP) MAIL SERVER ☑

3/ ADMINISTRATOR PASSWORD

Please set the password for 'safetica' account. This is the administrator account. Keep the credentials safe. If you want to give access to somebody else, use the Maintenance > Access Management view to create new account.

New Password: ••••••••••••••

Repeat password: ••••••••••••••

Change password

Continue

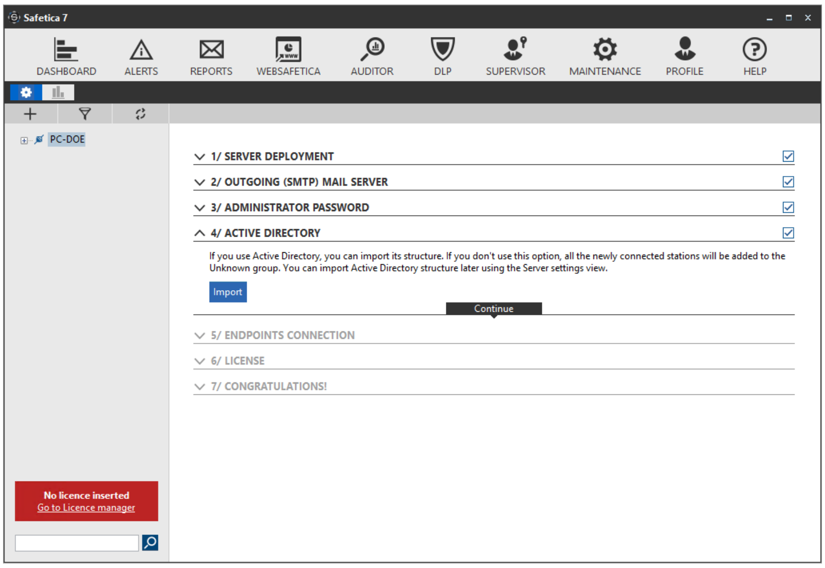
4/ ACTIVE DIRECTORY

5/ ENDPOINTS CONNECTION

6/ LICENSE

7/ CONGRATULATIONS!

3. You can import your corporate structure to Safetica from your corporate Active Directory. This is only possible if the computer with Safetica server is in the domain. If you do not make of use of this option, the new connected clients will be put in Unknown group. You can perform import from Active Directory later in *Profile->* *Server settings* in *Database connection setting* section.



1/ SERVER DEPLOYMENT ☑

2/ OUTGOING (SMTP) MAIL SERVER ☑

3/ ADMINISTRATOR PASSWORD ☑

4/ ACTIVE DIRECTORY ☑

If you use Active Directory, you can import its structure. If you don't use this option, all the newly connected stations will be added to the Unknown group. You can import Active Directory structure later using the Server settings view.

Import

Continue

5/ ENDPOINTS CONNECTION

6/ LICENSE

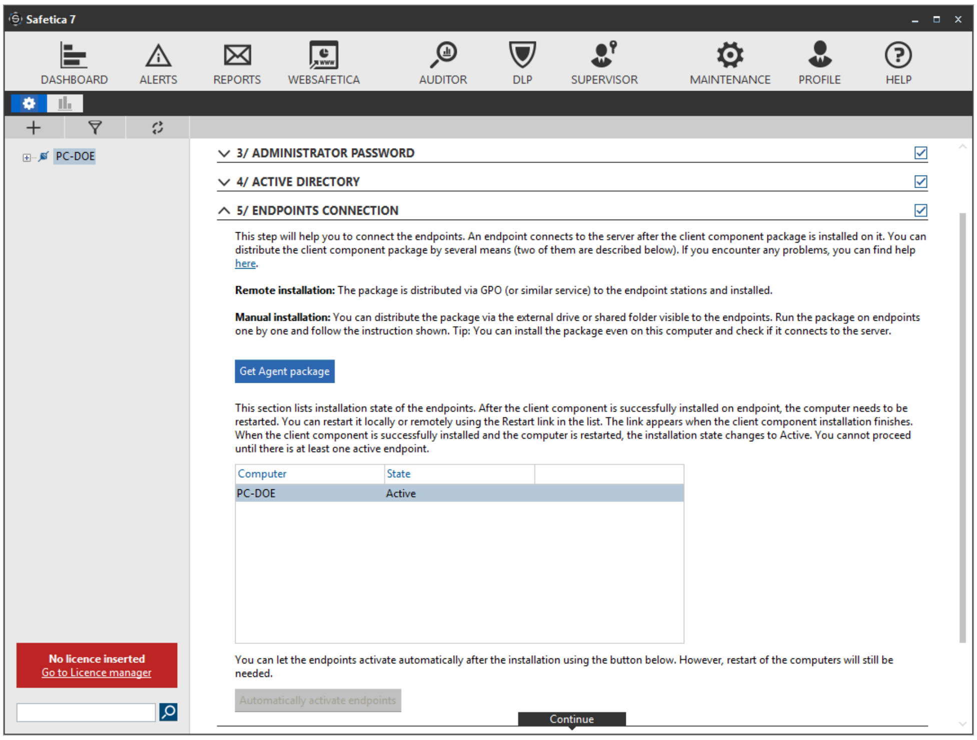
7/ CONGRATULATIONS!

4. This step will help you install a downloader agent on endpoints, so that they can be connected to Safetica. After clicking on *Get Agent package*, an installation file of the downloader agent is generated that you can install at workstations. The agent installation can be done in two ways:

   o Remote (batch) installation

   o Manual installation

   After installation of downloader agents you can automatically install and activate Safetica clients by clicking *Automatically activate endpoints*. The task of the client installation can be managed from *Console -> Maintenance -> Endpoint management*.



3/ ADMINISTRATOR PASSWORD ☑

4/ ACTIVE DIRECTORY ☑

5/ ENDPOINTS CONNECTION ☑

This step will help you to connect the endpoints. An endpoint connects to the server after the client component package is installed on it. You can distribute the client component package by several means (two of them are described below). If you encounter any problems, you can find help here.

Remote installation: The package is distributed via GPO (or similar service) to the endpoint stations and installed.

Manual installation: You can distribute the package via the external drive or shared folder visible to the endpoints. Run the package on endpoints one by one and follow the instruction shown. Tip: You can install the package even on this computer and check if it connects to the server.

Get Agent package

This section lists installation state of the endpoints. After the client component is successfully installed on endpoint, the computer needs to be restarted. You can restart it locally or remotely using the Restart link in the list. The link appears when the client component installation finishes. When the client component is successfully installed and the computer is restarted, the installation state changes to Active. You cannot proceed until there is at least one active endpoint.

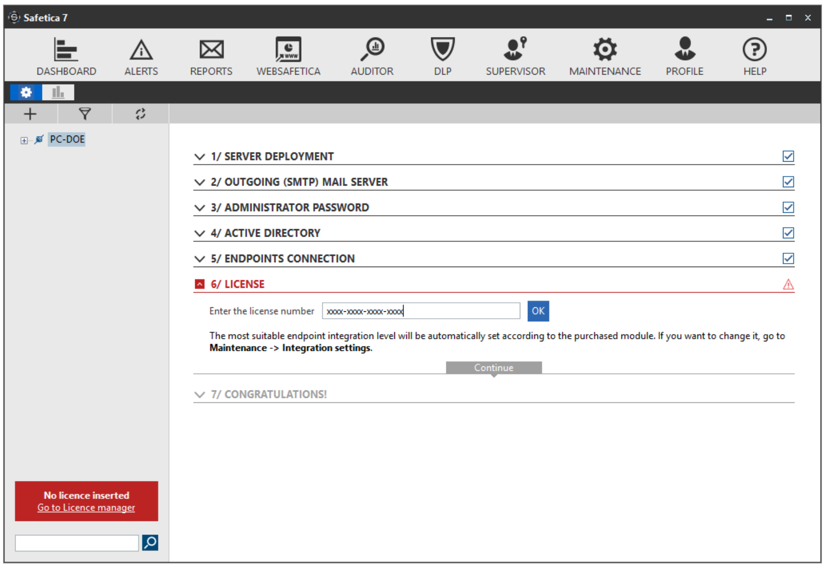
Computer	State
PC-DOE	Active

You can let the endpoints activate automatically after the installation using the button below. However, restart of the computers will still be needed.

Automatically activate endpoints

Continue

5. In this step, enter the license key in Safetica. The license key may be entered later in *Maintenance -> License management*. The functions of Safetica will not be available without the license key.



1/ SERVER DEPLOYMENT ☑

2/ OUTGOING (SMTP) MAIL SERVER ☑

3/ ADMINISTRATOR PASSWORD ☑

4/ ACTIVE DIRECTORY ☑

5/ ENDPOINTS CONNECTION ☑

6/ LICENSE ⚠

Enter the license number xxxx-xxxx-xxxx-xxxx OK

The most suitable endpoint integration level will be automatically set according to the purchased module. If you want to change it, go to **Maintenance -> Integration settings.**

Continue

7/ CONGRATULATIONS!

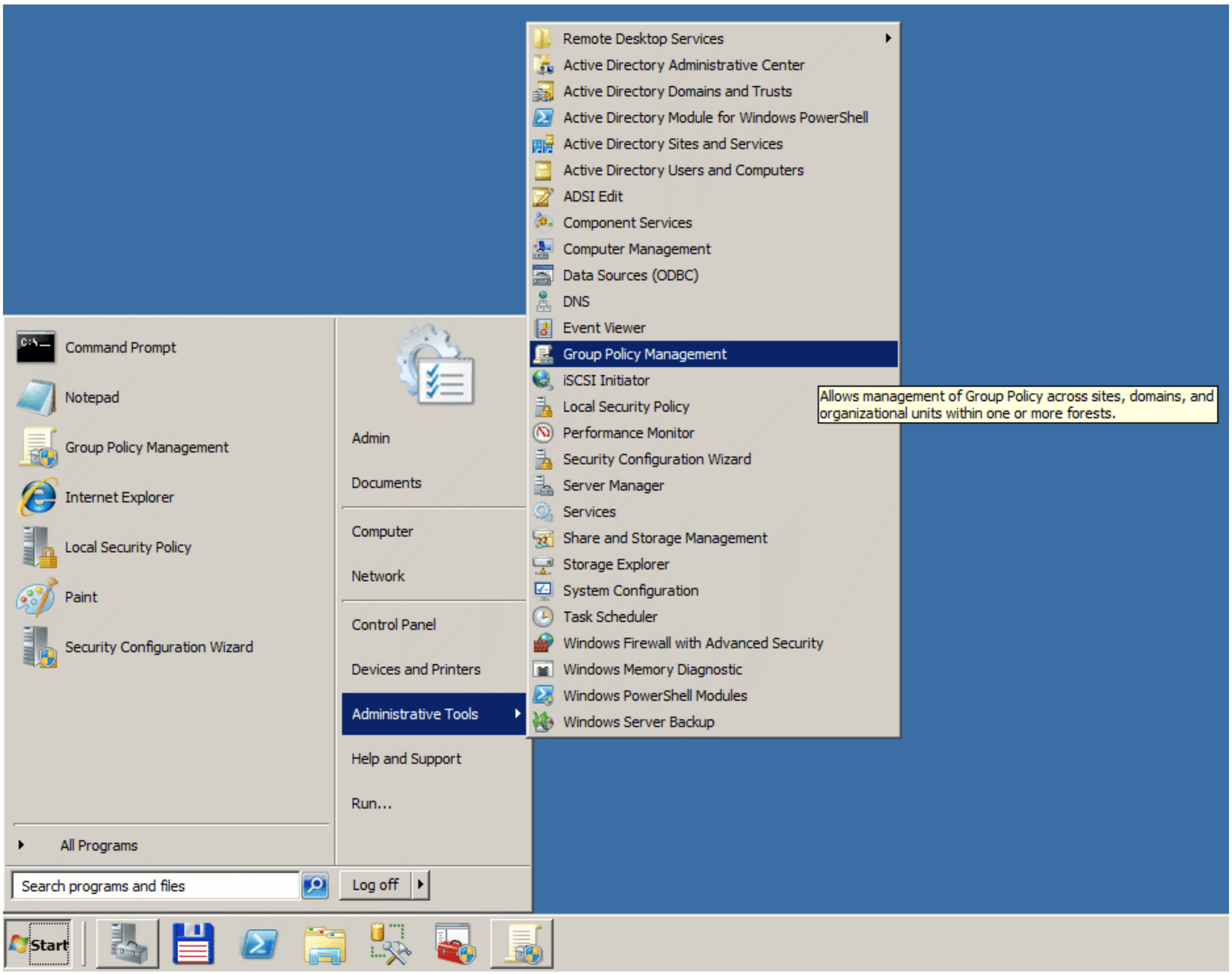
6. In the last step of the wizard you can either choose the preset functions of Safetica or adjust them manually in each function.
7. Exit the wizard by clicking on *Start protection!*

3.2.4.1 Batch Installation of downloader agent using GPO

If you are using Active Directory, you can bulk install the downloader agent using a Group Policy. To use the bulk installation, it is necessary to extract the relevant MSI package of the downloader agent component from the universal package.

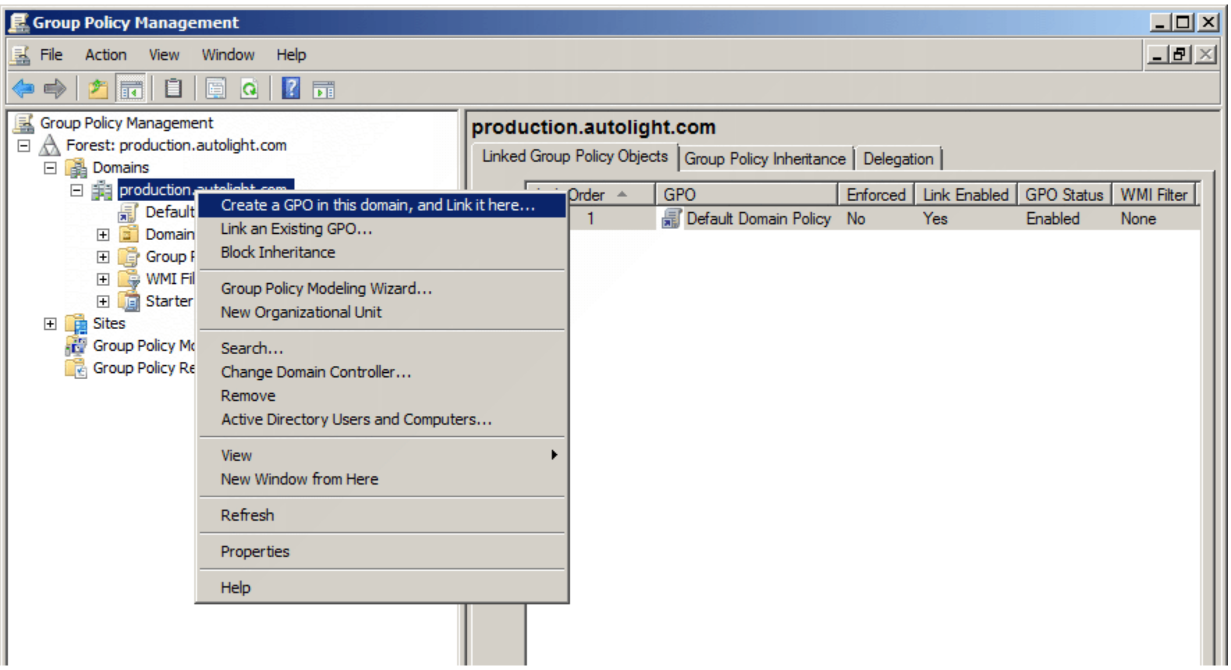
The installation will be described on an example of installation using the Group Policy in Windows Server 2008 R2. Described names and some steps may vary slightly depending on the version of the server system.

1. Start the Safetica universal installer.
2. Go to *Installation -> Safetica Agent -> Extract installer*. In the installer configuration, enter the server address and port to which the downloader agent will connect. Save the installation package on a shared disk or shared directory in the corporate network and set access rights (read and run will be sufficient) to this folder for the desired group (probably default - *Domain Users* and *Domain Computers*).
3. Go to *Administrative Tools -> Group Policy Management.*



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

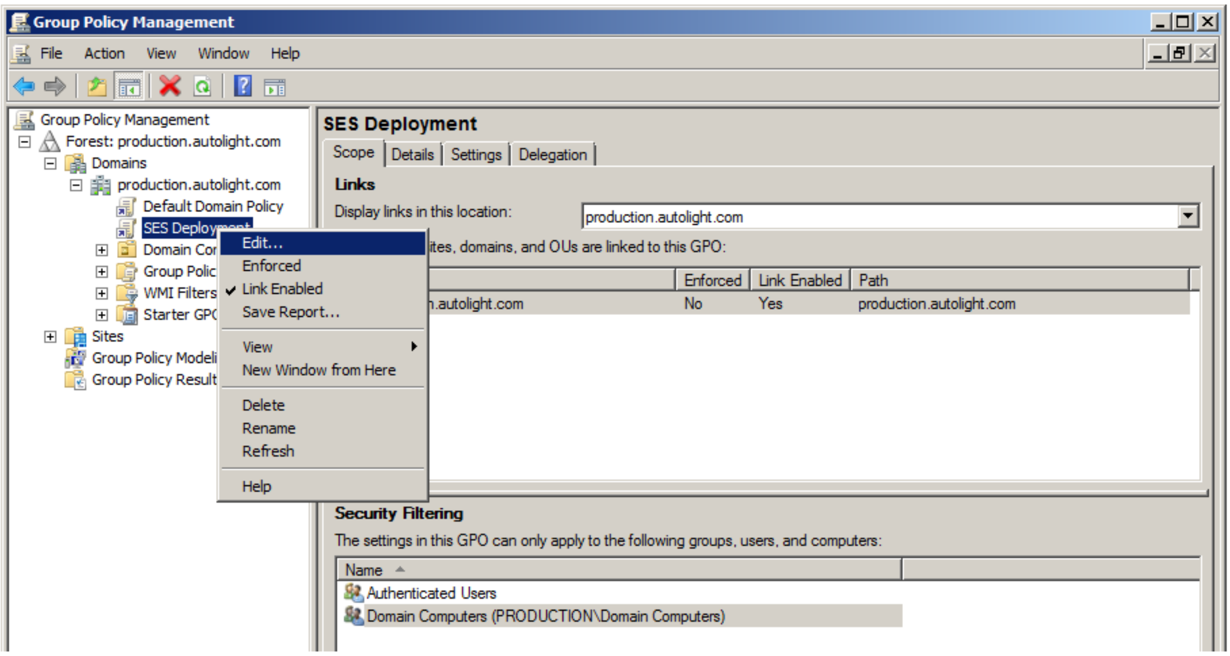
4. Right-click the organizational unit to which you want to deploy the downloader agent and select *Create a GPO in this domain and link it here ...*



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

5. Give an arbitrary name to the new object (for example, Safetica Deployment).

6. Select your newly created group policy and right-click to select *Edit.*



Display links in this location: production.autolight.com

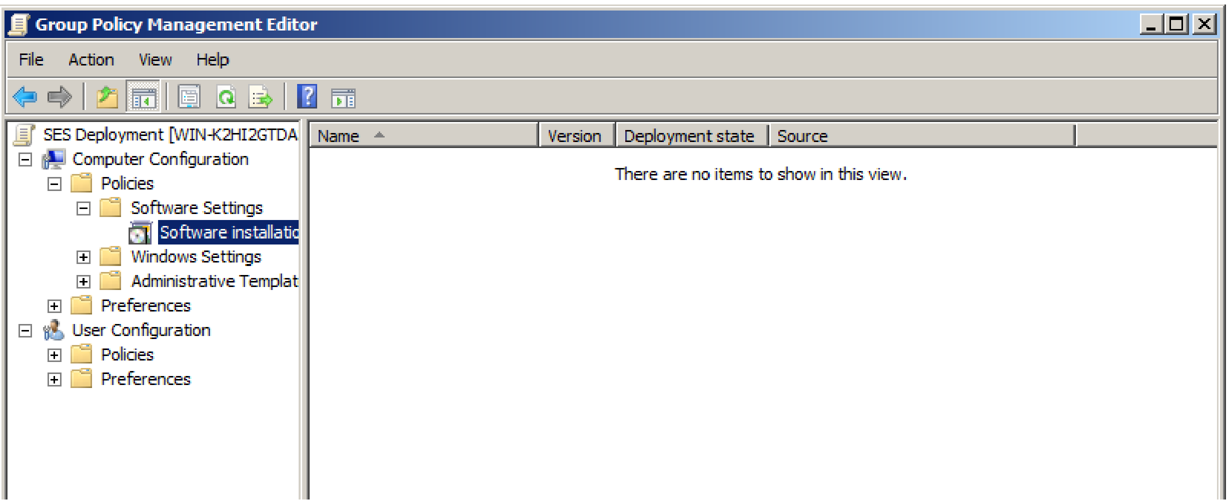
…ites, domains, and OUs are linked to this GPO:

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

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

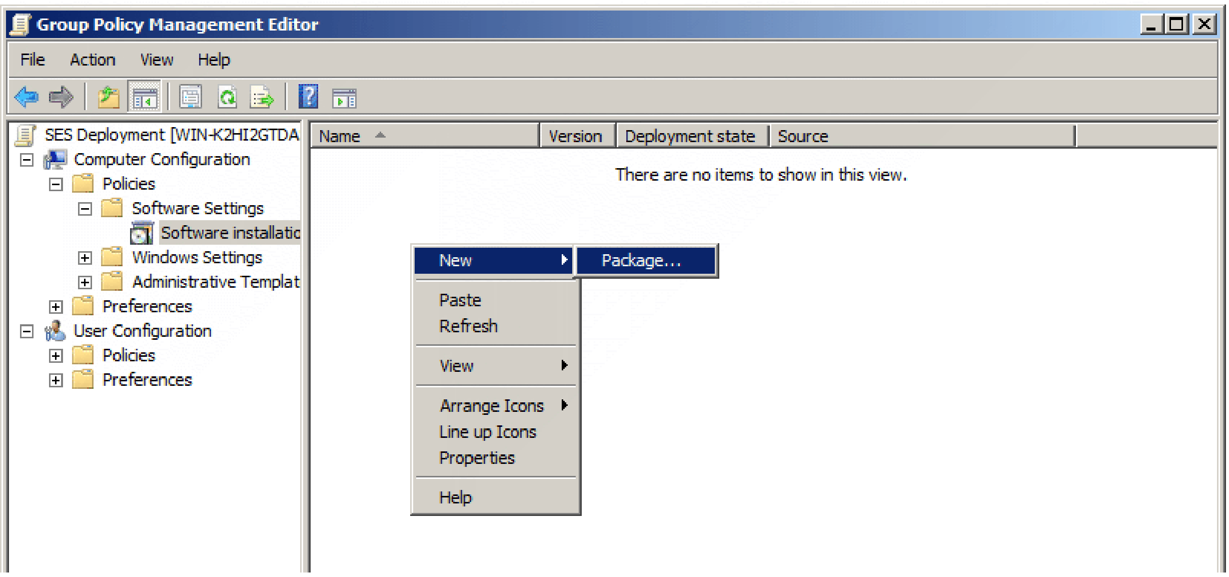
Name
Authenticated Users
Domain Computers (PRODUCTION\Domain Computers)

7. In the window that opens, navigate to *Computer Configuration -> Policies -> Software Settings* and click on *Software installation.*



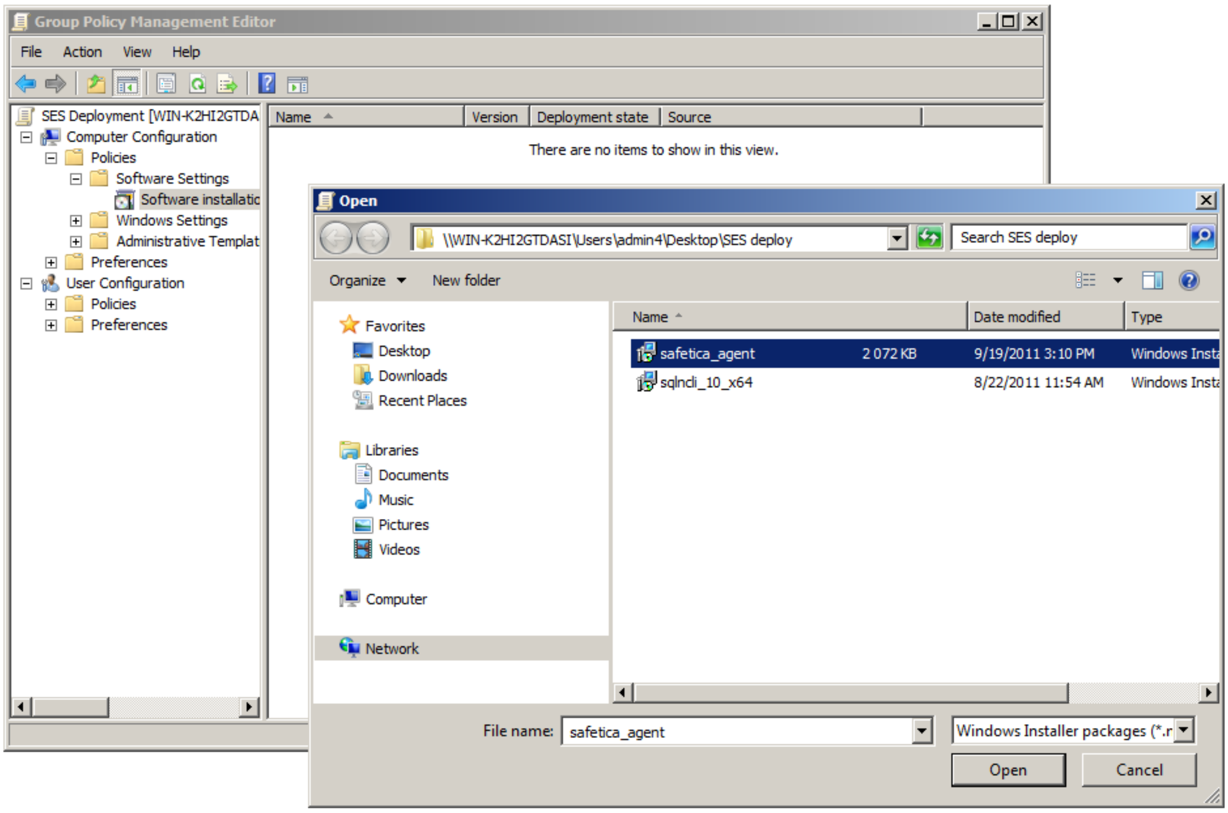
There are no items to show in this view.

8. Right-click on the window with a list of software and select *New Item -> Package ...*



There are no items to show in this view.

9. In the MSI package selection dialog box, navigate to the shared network folder where you copied the MSI package with the downloader agent, and select it.



There are no items to show in this view.

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

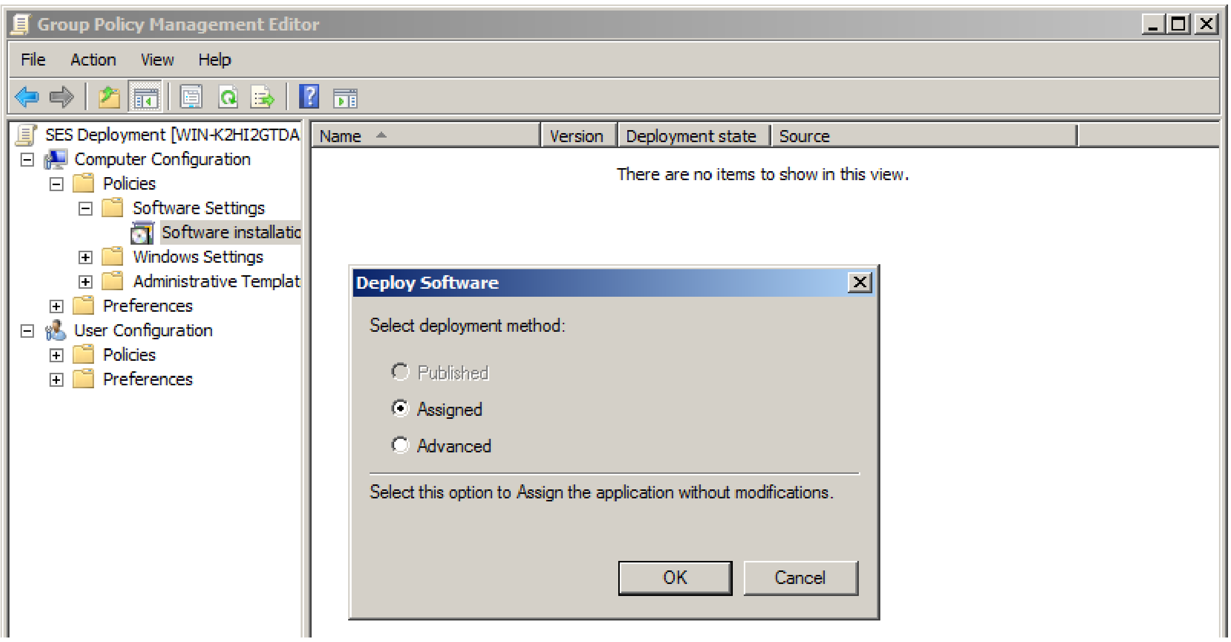
Search SES deploy

Name		Date modified	Type
safetica_agent	2 072 KB	9/19/2011 3:10 PM	Windows Insta
sqlncli_10_x64		8/22/2011 11:54 AM	Windows Insta

File name: safetica_agent

Windows Installer packages (*.r

10. In the next dialog window, select *Assigned* and confirm.



There are no items to show in this view.

Select deployment method:

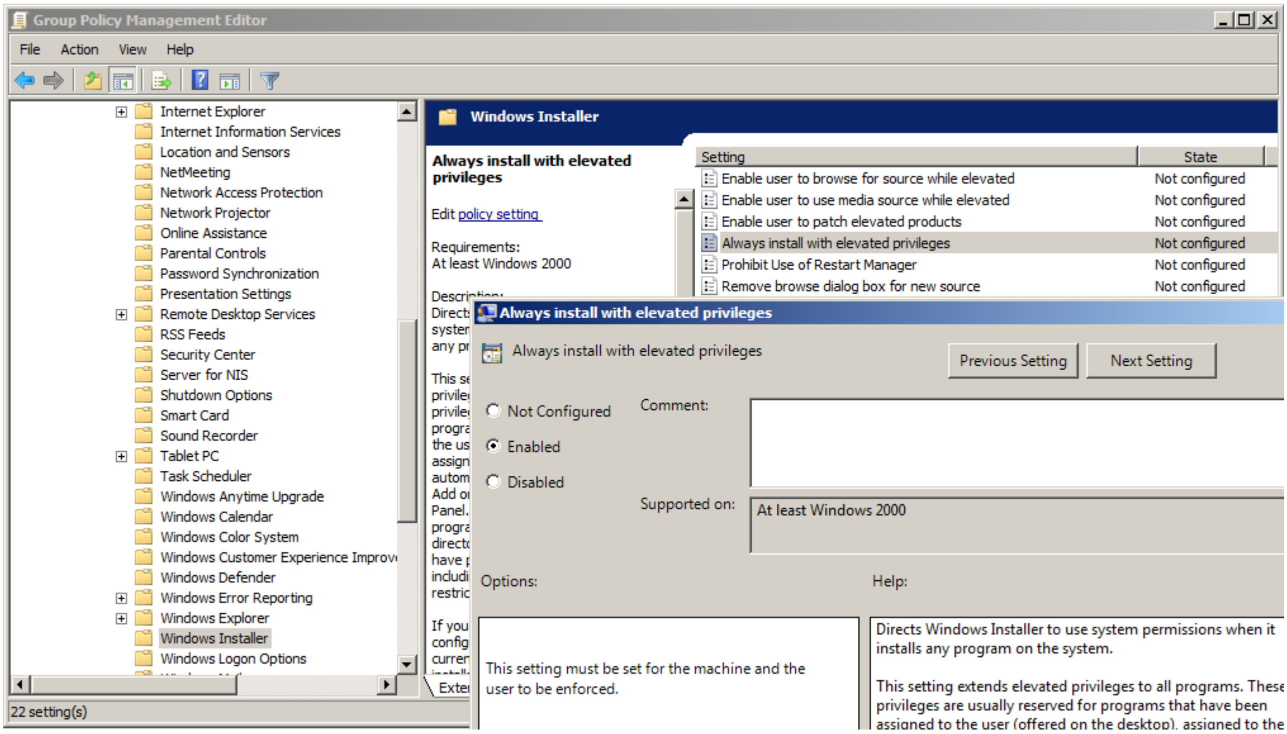
○ Published

● Assigned

○ Advanced

Select this option to Assign the application without modifications.

11. Next, open *Computer Setup -> Management Templates -> Windows Components -> Windows Installer.* There, you should find the item *Always install with elevated privileges* and set it to *Enabled*. This ensures that the downloader agent will be installed on end workstations properly and without problems.



- Internet Explorer
- Internet Information Services
- Location and Sensors
- NetMeeting
- Network Access Protection
- Network Projector
- Online Assistance
- Parental Controls
- Password Synchronization
- Presentation Settings
- Remote Desktop Services
- RSS Feeds
- Security Center
- Server for NIS
- Shutdown Options
- Smart Card
- Sound Recorder
- Tablet PC
- Task Scheduler
- Windows Anytime Upgrade
- Windows Calendar
- Windows Color System
- Windows Customer Experience Improv
- Windows Defender
- Windows Error Reporting
- Windows Explorer
- Windows Installer
- Windows Logon Options

22 setting(s)

Windows Installer

Always install with elevated privileges

Edit policy setting

Requirements:
At least Windows 2000

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

Always install with elevated privileges

Always install with elevated privileges

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

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

Help:

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

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

12. After rebooting client computers for which the policy was created, the downloader agent will automatically install. To enforce policy updates, enter the *gpupdate /force command on a client workstation.*

13. Policy configuration is completed and the distribution of the downloader agent is ready now. When the client computers are started, the downloader agent installs.

3.2.4.2 Manual installation of downloader agent

The downloader agent is used to install, update and manage the Safetica client at the end workstations. For manual installation of the downloader agent at the end workstation, proceed as follows:

1. Open the universal installer and select your language. Confirm the license conditions and go to *Installation > Safetica Agent.*

2. Here you have several options:

   o Launch the installation directly from the universal installer by using the *Run installer button.*

   o Extract only the downloader agent installer that you can use separately for later installations.

   Note: *In the third part - Tools and Components you will find components essential for correct client or Microsoft SQL Server installation.*

3. In the next step, fill in the following information for proper downloader agent connection to server:

   o *Server address* – server address to which the downloader agent will connect.

   Note: You can also enter multiple addresses that can be used by the downloader agent *to connect to one server. This is useful is scenarios where the downloader agent is installed on a laptop being used also outside the company premises where it will have a different address for server connection. If you enter more addresses, separate them with the* | *symbol. Example: 192.168.100.2|158.142.12.10|145.65.87.22.*

   o *Port* – the port where server will be listening. The default port is 4438.

Click on *Next.*

4. After the configuration is saved, the downloader agent installer will launch. After clicking on *Next*, the downloader agent will install on the end workstation and then connect to the server.

Successful downloader agent installation can be verified from console, where the user tree will show the SA icon with the end workstation name. Client can be remotely installed on the end workstation with the downloader agent installed.

Note: The downloader agent component will be automatically installed along with the client.

3.2.5 Installing client

Safetica client 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 console run properly. For end users, it can also provide a set of security tools for their own use.

Recommended installation procedure

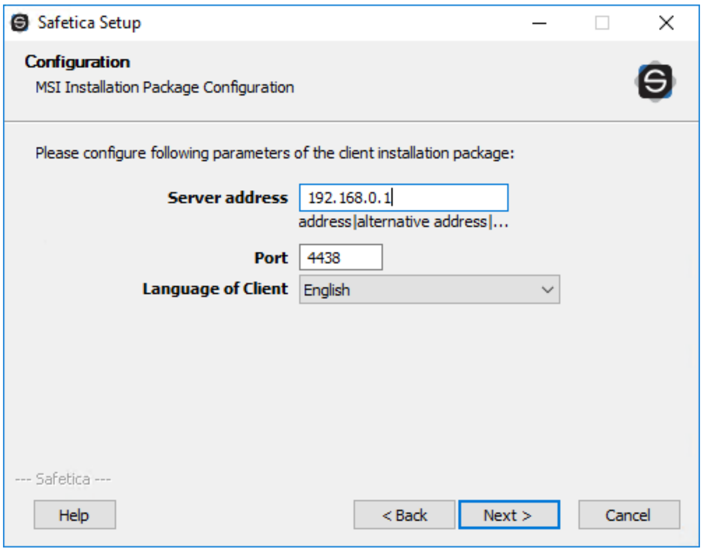
1. Install the downloader agent on the endpoint station.
2. Safetica client installation should be performed remotely over *Console -> Maintenance -> Endpoint Management*. Follow the instructions in the *Endpoint management section.*

Manual installation using the universal installer

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 client 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 2012 SP2 Express.
3. You will be asked to enter the following information before extraction or running the installer:
   - *Server address* – address of server for client to connect to.

     Note: You can enter multiple addresses that client can use for connecting to a single server. This is useful in scenarios where client is installed on a laptop that is used also outside company premises, where it will have a different address for server connection. If you enter multiple addresses, separate them with the | symbol. Example: 192.168.100.2|158.142.12.10|145.65.87.22.
   - *Port* – port on which the server listens. The default is 4438.
   - *Language of client* – language of the client.



Safetica Setup

Configuration

MSI Installation Package Configuration

Please configure following parameters of the client installation package:

Server address: 192.168.0.1

address|alternative address|...

Port: 4438

Language of Client: English

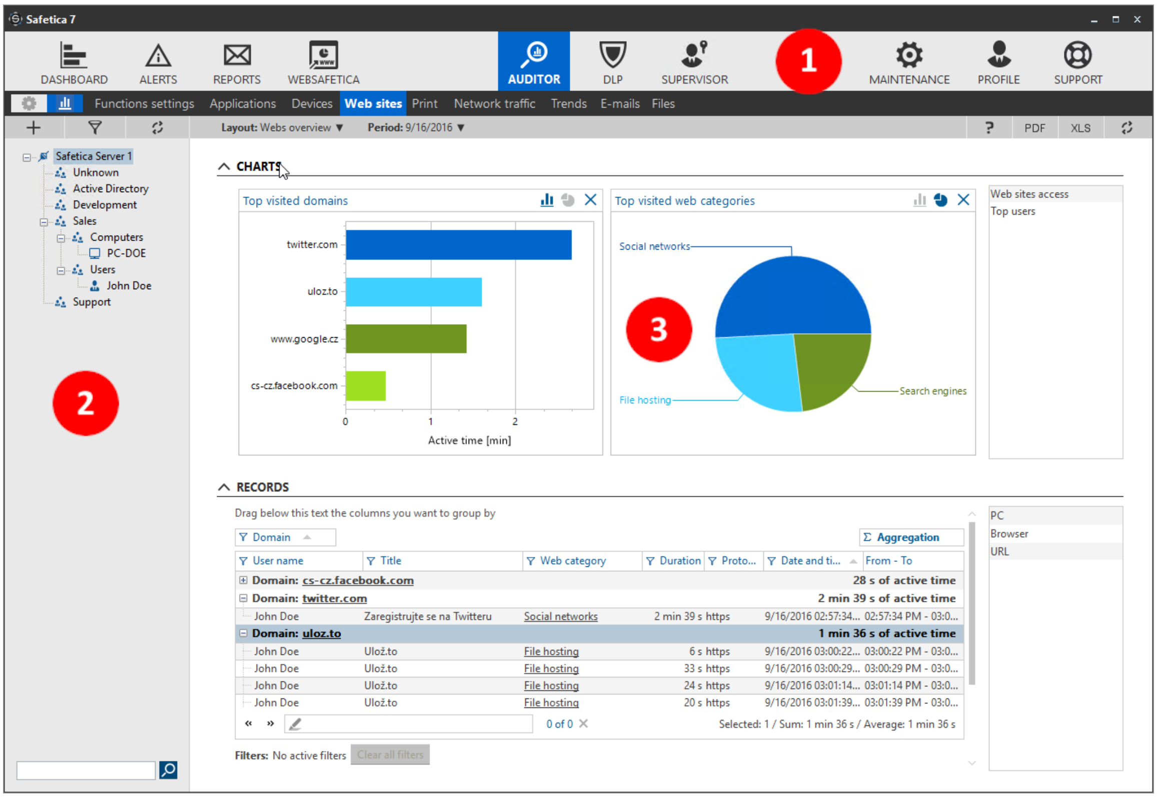
4. Select the installation folder.
5. You can verify successful installation from the console where you will find icon 🖥 in the user tree with the name of the endpoint station. If you cannot find the endpoint station in the console, verify that the STCService.exe service is running on the endpoint station (Windows Task Manager > Services > STCService – running) and 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.

4 Console

All functions and components of Safetica (clients, servers, databases) are managed via web or desktop console. It also allows to display outputs of monitored data, statistics and charts. After starting it, you must log in through the user account. The items you can view or set in individual functions of Safetica depend on the rights of the user logged in Safetica. You can manage users and their rights in Access management.

4.1 Interface description

After launching Safetica console you will see the following interface.



Drag below this text the columns you want to group by

Domain | Σ Aggregation

User name	Title	Web category	Duration	Proto...	Date and ti...	From - To
Domain: cs-cz.facebook.com						**28 s of active time**
Domain: twitter.com						**2 min 39 s of active time**
John Doe	Zaregistrujte se na Twitteru	Social networks	2 min 39 s	https	9/16/2016 02:57:34...	02:57:34 PM - 03:0...
Domain: uloz.to						**1 min 36 s of active time**
John Doe	Ulož.to	File hosting	6 s	https	9/16/2016 03:00:22...	03:00:22 PM - 03:0...
John Doe	Ulož.to	File hosting	33 s	https	9/16/2016 03:00:29...	03:00:29 PM - 03:0...
John Doe	Ulož.to	File hosting	24 s	https	9/16/2016 03:01:14...	03:01:14 PM - 03:0...
John Doe	Ulož.to	File hosting	20 s	https	9/16/2016 03:01:39...	03:01:39 PM - 03:0...

« » 0 of 0 ✕ Selected: 1 / Sum: 1 min 36 s / Average: 1 min 36 s

Filters: No active filters Clear all filters

1. Main menu

The console mode switch is situated in the bottom left of the main menu.

- *Setting mode (* ⚙ *)* – the setting of each Safetica function is displayed in this mode (except Auditor functions). The setting of all Auditor module functions can be found in *Auditor -> Functions settings*. This mode does not relate to the console or server settings. These are managed through separate settings in Maintenance. The functions are set for groups, users or computers identified in the user tree. The changes in the setting are effective only when saved using ✓ button in the top right corner of the function setting. The changes may also be cancelled by the ✕ button.
- *Visualization mode (* 📊 *)* – in this mode, the recorded data, summary reports, charts and statistics are shown in the functions of Safetica. Data on groups, users and computers identified in the user tree are shown for a specified period of time.

On the left, there are icons that you can use to get to different overviews with summary information:

- Dashboard – overview of data collected from all active functions.
- Alerts - automatic alert setting.
- Reports - regular summary report delivery settings.

In the center, there are icons used to switch between the three main Safetica modules.

- Auditor
- DLP
- Supervisor

On the right, there are icons used to access the administration of all Safetica components and help.

- *Maintenance* – management and setup of connected servers and clients, together with the downloader agent.
- *Profile* – basic settings of your account such as connection to the server, and custom settings of the console.
- *Help* – access to the Safetica Help.

Below the upper toolbar with console controls, a list of module functions is located. The list updates depending on the currently used module - Auditor, DLP, Supervisor.

2. User tree

The user tree is located on the left side of the console under the upper toolbar. All the Safetica servers to which you are connected are shown in the tree. A new connection to the server can be set up in the *Profile* section. Each server in the tree contains groups, *users and computers* that are connected to it. For selected items in the tree, either the settings or data obtained using the corresponding functionality are shown in the display area or view (section 3 on the figure). Multiple items can be selected by holding down *Ctrl* or *Shift* and checking the items one by one. For additional details about the server, please read the Architecture section.

Items of the tree

Root items of the tree are the servers to which you are connected via the console. The following icons in the user tree specify connection status of each server:

- ⊞ SMS 01 – you are connected with the console to the server with the name SMS 01.
- ⊞ SMS 01* - where the server name is followed by an asterisk, the tree has changed and it needs to be updated. For example, using the ⟳ *button.*
- SMS 01 – your console is not connected to server because the server is not available or not running.
- SMS 01 – in some views the setting is common for the entire server. In this case only such servers are displayed in the user tree to which you are connected with the console (the tree cannot be unpacked).

For additional details about the use of the user tree, please see the Help section on functionality settings and visualization of data collected.

The main tree items are as follows:

- – the user who is logged onto the computer with the client or downloader agent and is on-line. If the user is off-line, its icon is greyed out: .
- – computer on which the client is installed and is on-line. If the computer is off-line, its icon is greyed out: . If the downloader agent is installed on the computer, you can restart the *Safetica Client Service (Restart Service)* or the entire computer (*Restart Computer*) from the contextual menu.
- SA – computer on which only the downloader agent is installed and is on-line. Via a contextual menu, you can restart the *Safetica Client Service* on the computer or restart the entire computer.
- – a group that contains users, computers, or other groups.

Further operations on the user tree, such as adding groups, deleting, renaming users and computers are performed using a contextual menu that is invoked by right-clicking the tree item. Items in the tree can be moved using the mouse (drag and drop). The contextual menu for computers is extended with the following options:

- *Redirect* - redirects client to another server. See Redirecting client to another server.
  - o 🖥 – redirection has been set.
  - o 🖥 – redirection completed.
- *Allow unknown certificate* - authorizes client to connect to another server (will also receive a certificate from another server).
- *Enable Active management* - with this setting, the transfer of settings to the client and the transfer of records to the DB will take the shortest possible time. Client management will be almost instantaneous for the specified period. Active management has a higher priority than the interval of setting and record transfer set in the *Client settings* and can only be enabled for a limited period of time (1, 2, 4 and 24 hours). If your computer has active management enabled, its icon in the tree changes to the following:
  - o 🖥 - active management has been set, but client has not yet updated the settings.
  - o 🖥 - active management has been set and is active.

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 are marked by 👥 icon.
- 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).

Built-in groups

There are two built-in groups in the user tree:

- *Unknown* - this group cannot be deleted. Once a new client is connected, the newly connected users and computers are allocated into the group. You can copy and paste/move these users and computers from the *Unknown* group to the groups you have created by yourself. If you delete the user or computer from your own groups, they will move back to the *Unknown* group. The same applies to the users and computers from a group which has been deleted in the user tree. Delete the users or computers from the *Unknown* group to erase them completely.
- *Active Directory* – cannot be deleted. This is used for Active Directory synchronization to server. You can select the Active Directory tree in the Server 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 console.

Tree controls

Above the user tree, there are several controls:

- The + button will expand all nodes in the user tree.
- The − button will collapse all nodes in the user tree.

- The ▽ button displays a quick filter for the tree. The filter can be used to specify which items will be displayed in the tree. Click on the appropriate filter to set it. Click again to remove it. You can set multiple filters at a time. In this case, the tree only displays items that match all your filters. You can choose from the following filters:
    - *Users* - the tree displays only users.
    - *Computers* - the tree displays only computers.
    - *Active* - the tree displays users who are logged into the system or computers that are turned on and on which client or downloader agent is running.
    - *Inactive* - the tree displays users who are not logged into the system or computers that are turned off or computers on which client or downloader agent is not running.
    - *With Client* - the tree displays users/computers with client installed.
    - *No Client* - the tree displays users/computers without client installed.
    - *Deactivated client* - the tree displays users or computers that have client installed, but disabled. See *Disabling end workstations*.
    - *With Agent* - the tree displays users/computers with downloader agent installed.
    - *No Agent* - the tree displays users/computers without downloader agent installed.
    - *With license* - the tree displays users/computers with a Safetica license assigned. See *License Manager*
    - *With license* - the tree displays users/computers with a Safetica license assigned.
    - *Redirected* - the tree displays only redirected computers. See *Redirecting client to another server*.
    - *Not Redirected* - the tree displays only computers that are not redirected.
    - *Removed from AD* - the tree displays users/computers that have been removed from the Active Directory that is synchronized with server.
  - *Active management* - the tree displays only computers that have active management enabled.

  Selected filters are confirmed with the OK button.

- The ⟳ button updates the user tree.

3. Display area (view)

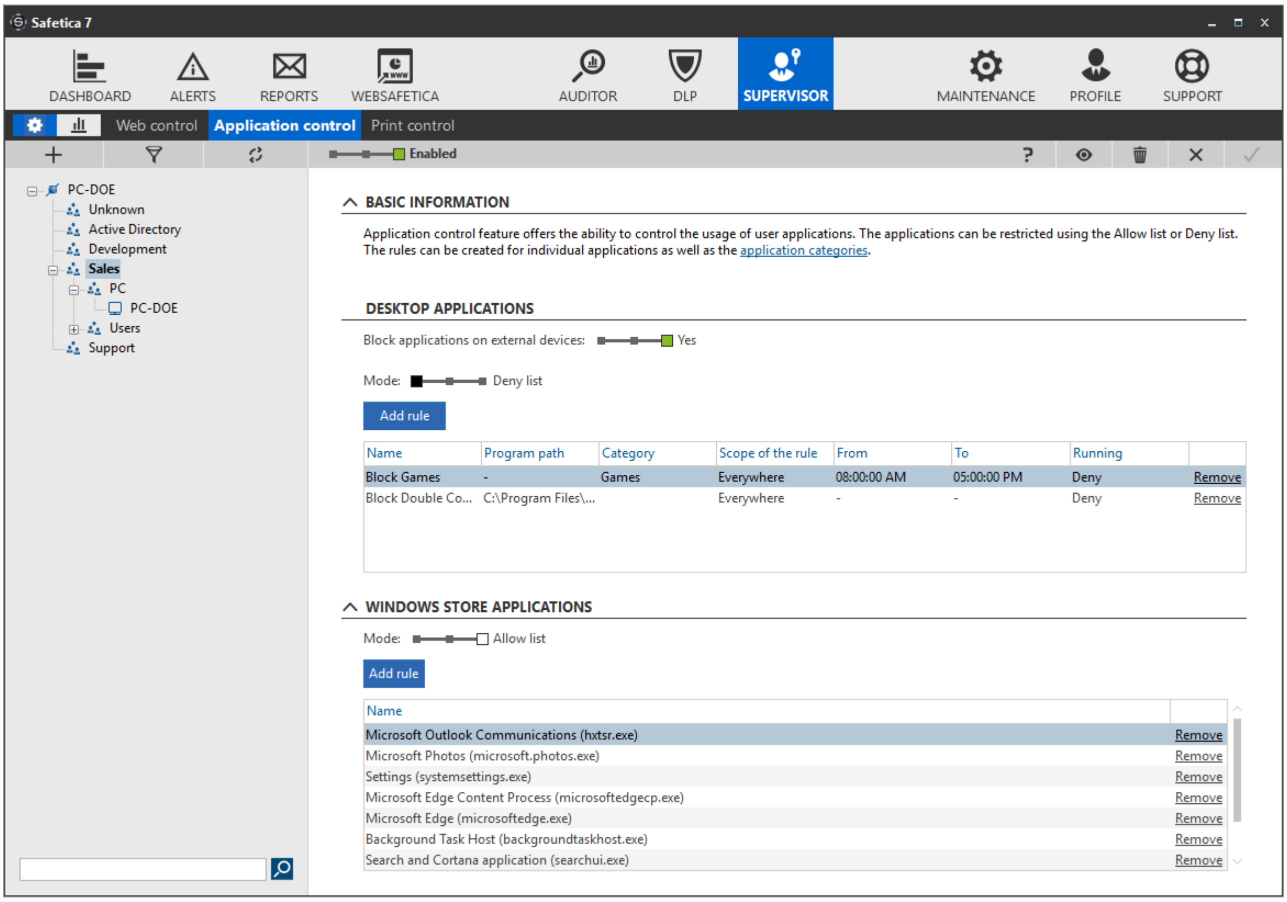
The display area, also called the view area, is used for data visualization and changing the settings for individual functions. The contents of the view area change based on which function you are currently browsing and your current mode (settings, visualization, etc.). When describing individual functions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

4.2 Setting mode

The user tree contains a list of branches, groups, users and computers (entries). The root entries are always individual branches that Safetica 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 console.



BASIC INFORMATION

Application control feature offers the ability to control the usage of user applications. The applications can be restricted using the Allow list or Deny list. The rules can be created for individual applications as well as the application categories.

DESKTOP APPLICATIONS

Block applications on external devices: Yes

Mode: Deny list

Add rule

Name	Program path	Category	Scope of the rule	From	To	Running	
Block Games	-	Games	Everywhere	08:00:00 AM	05:00:00 PM	Deny	Remove
Block Double Co...	C:\Program Files\...		Everywhere	-	-	Deny	Remove

WINDOWS STORE APPLICATIONS

Mode: Allow list

Add rule

Name	
Microsoft Outlook Communications (hxtsr.exe)	Remove
Microsoft Photos (microsoft.photos.exe)	Remove
Settings (systemsettings.exe)	Remove
Microsoft Edge Content Process (microsoftedgecp.exe)	Remove
Microsoft Edge (microsoftedge.exe)	Remove
Background Task Host (backgroundtaskhost.exe)	Remove
Search and Cortana application (searchui.exe)	Remove

Use the ? button to view help for the relevant function.

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.

Items in the user tree of for which the function is set (*Enabled, Disabled*) are highlighted in blue in the user tree.

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 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.

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.

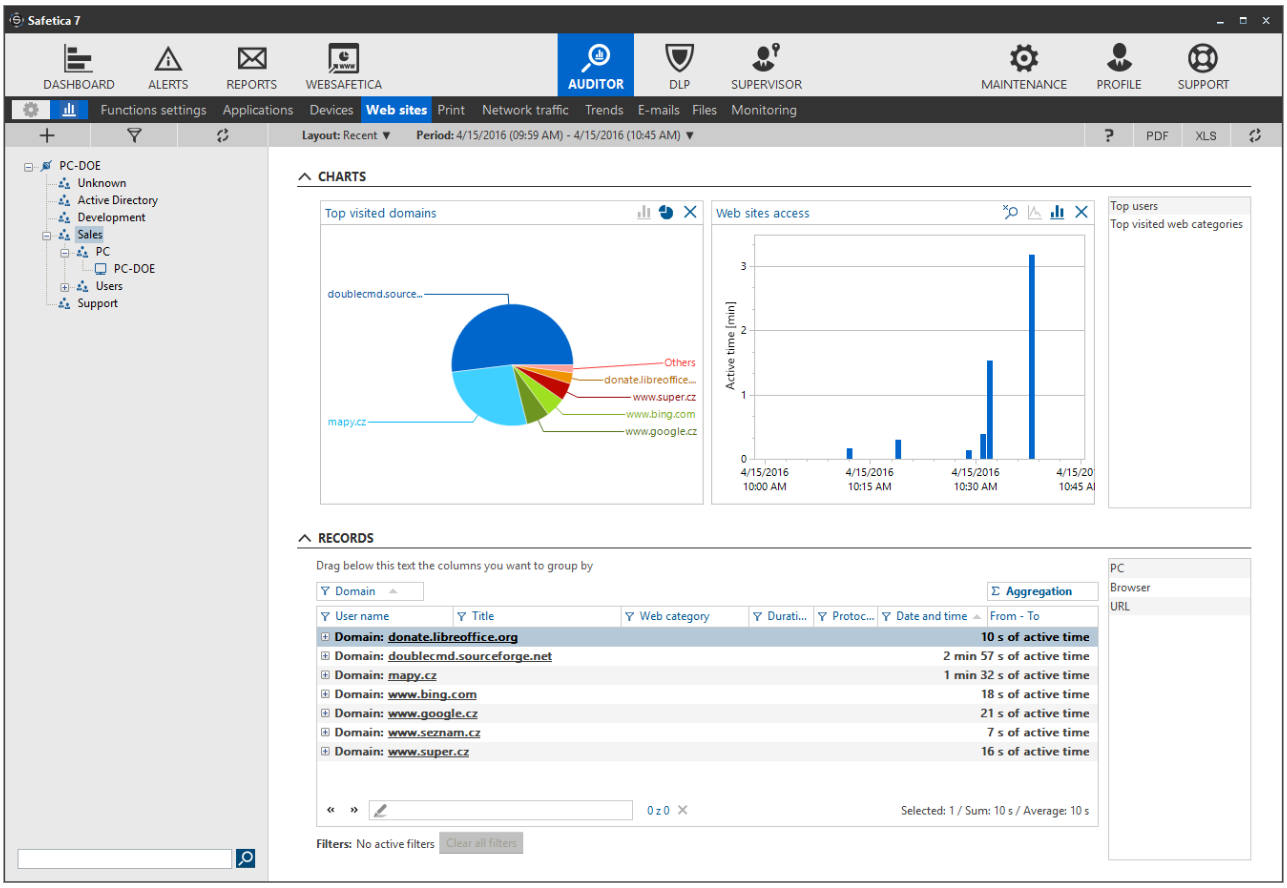
- Assigning to groups helps prevent confusion when moving to other groups. You might expect a user to inherit the settings from the group that you are moving him/her to, but in fact a setting for the user may exist which has higher priority.

- Moreover, settings directly for groups take less space in the database than separate settings for each user.

4.3 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.

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



User name	Title	Web category	Durati...	Protoc...	Date and time	From - To
⊞ **Domain: donate.libreoffice.org**						**10 s of active time**
⊞ **Domain: doublecmd.sourceforge.net**						**2 min 57 s of active time**
⊞ **Domain: mapy.cz**						**1 min 32 s of active time**
⊞ **Domain: www.bing.com**						**18 s of active time**
⊞ **Domain: www.google.cz**						**21 s of active time**
⊞ **Domain: www.seznam.cz**						**7 s of active time**
⊞ **Domain: www.super.cz**						**16 s of active time**

« » 0 z 0 ✕ Selected: 1 / Sum: 10 s / Average: 10 s

Filters: No active filters Clear all filters

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 *Period* at the upper left side of your view*.* You have several option how to specify date:

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

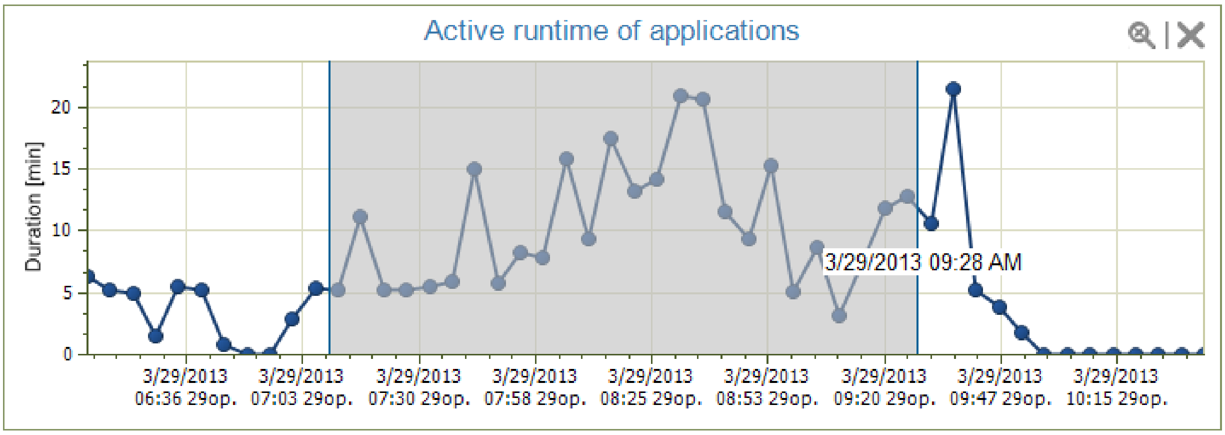
You can reload records and charts by clicking on the ⟳ button in the upper right corner.

Use the ? button to view help for the relevant function.

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.



- Some charts display a blue vertical line which shows the average value of data in the chart.

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.

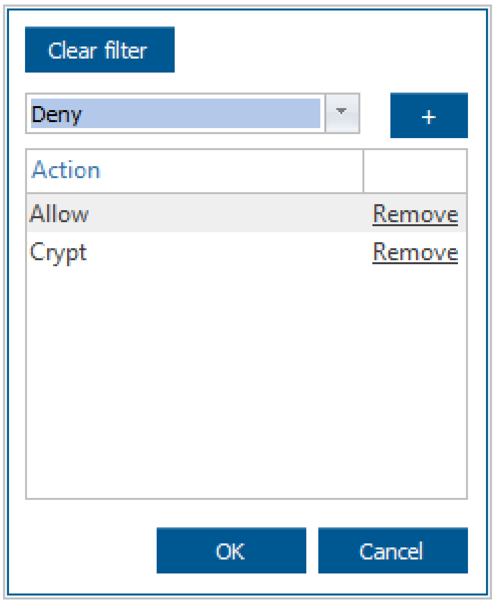
Filters

You can filter the records as well. You can open the filter for any column by clicking the ⛛ button at the header of the respective column. At the top of the dialogue box, enter text or choose an item from the list, selecting the condition for which you wish to filter the column. Clicking the + button will add the item to the list of filter conditions (you can also add items by confirming with *OK*). The list may include multiple conditions. After confirming the filter with *OK*, the table will only show records which meet all of the filter conditions.

- ▽ filter for column is not set.
- ▼ there is some filter set on the column. Header will be also bold.

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.

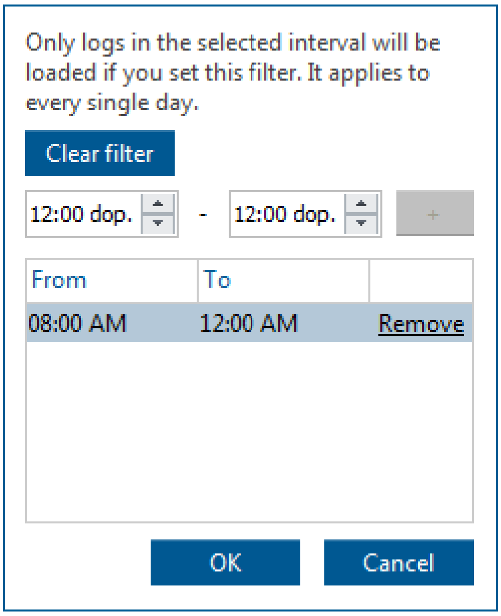


Deny

Action	
Allow	Remove
Crypt	Remove

You can use the filter for every *Date and time* column and enter a time interval to specify from which part of the day records shall be displayed.

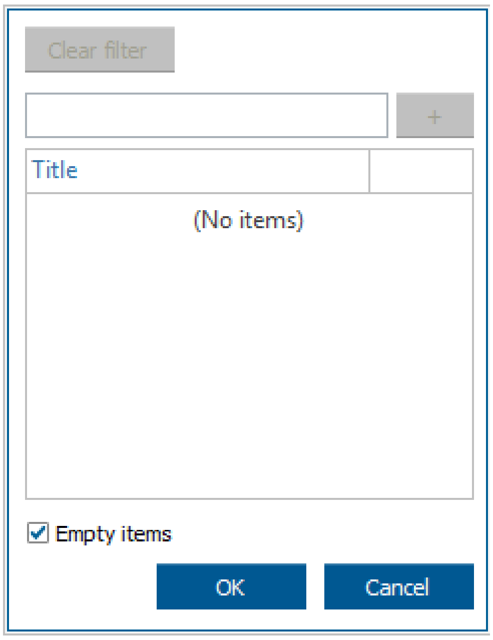
You can also enter multiple simultaneous intervals.


Only logs in the selected interval will be loaded if you set this filter. It applies to every single day.

12:00 dop. - 12:00 dop.

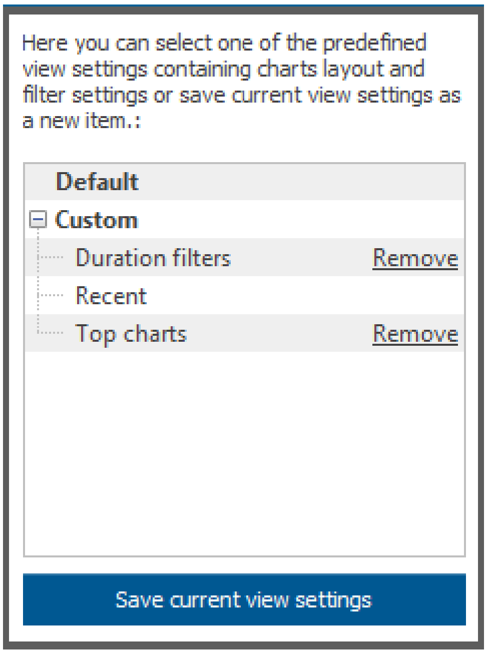
From	To	
08:00 AM	12:00 AM	Remove

In text filters you can search empty items as well. You can do so by checking the *Empty items* box in the respective filter.



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 left corner.

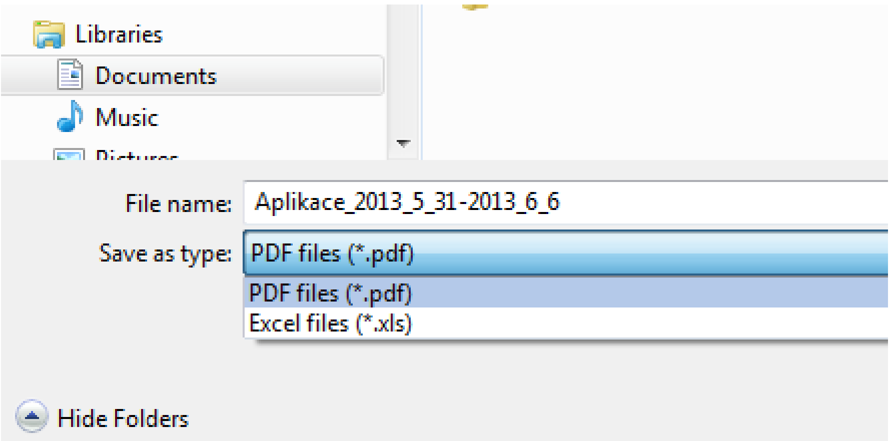


Here you can select one of the predefined view settings containing charts layout and filter settings or save current view settings as a new item.:

- Each Safetica 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 PDF button in the top right corner.



File name: Aplikace_2013_5_31-2013_6_6

Save as type: PDF files (*.pdf)

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.

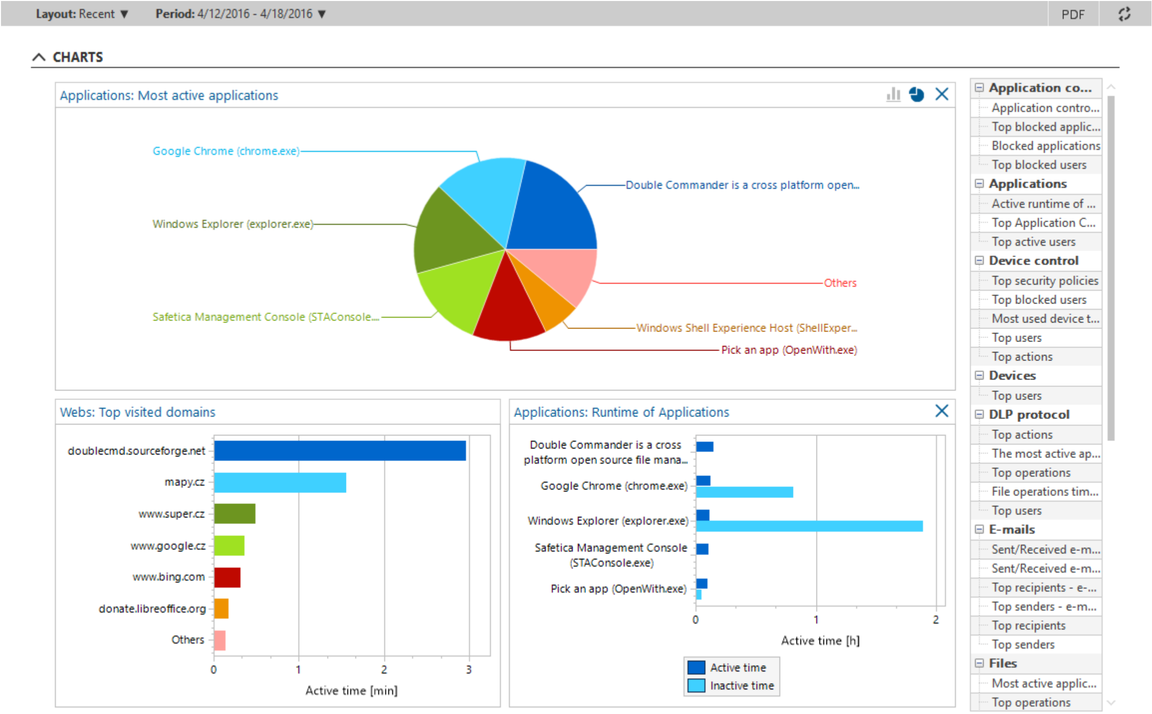
4.4 Management and settings

4.4.1 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.

Reports can be viewed by clicking on the *Dashboard* button in the top left corner of the Safetica console.

Reports will only be displayed for users, groups, computers or the server selected in the user tree.



Layout: Recent ▼ Period: 4/12/2016 - 4/18/2016 ▼

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 PDF.

4.4.2 Alerts

By using alerts, you can be notified about Safetica events as they arise. The alerts are used by most of the Safetica components. The security administrator or any other authorized administrator can set warnings of selected exceptional situations. If any such warning occurs, the administrator is notified (depending on the settings) by the Safetica console or in an e-mail message.

Alerts can be viewed by clicking on the *Alerts* button in the upper left corner of the console.

Settings

Alerts are set up for the server 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 the ✕ button in the upper right section.

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.

In the *Created by* column you will find the name of the account for connecting to the server under which the alert was created.

Click on *Edit* to update the appropriate item.

Click on *Remove* to remove an alert.

In settings, you can choose your own alert sets. For each alerts set, you can select various alerts and specify the target users, groups, or computers, and the destination of the alert, i.e. either the console, e-mail, or both.

Alerts are divided into three main categories:

- *Safety warning* – these alerts are sent immediately after the situation occurs. For some alerts, you can specify to which data categories or types of equipment the alert will apply. If no preference regarding the category or device is specified, the alert will apply to all of them. After clicking on *All data categories* or *All devices* a dialog opens where you can specify the data categories or devices to which the alert will apply.

- *Informative alerts* – these alerts are sent in daily and weekly intervals when exceeding a specified value for a day or a week. For some alerts, you can specify to which web and application category the entered values ?for the day and week apply. If no categories are specified, it will apply to all of them. Categories can be selected via a dialog box; to display it for the relevant alert, click the *Add categories link.* This way you can add multiple categories. For each individual category, you can set different daily and weekly values.

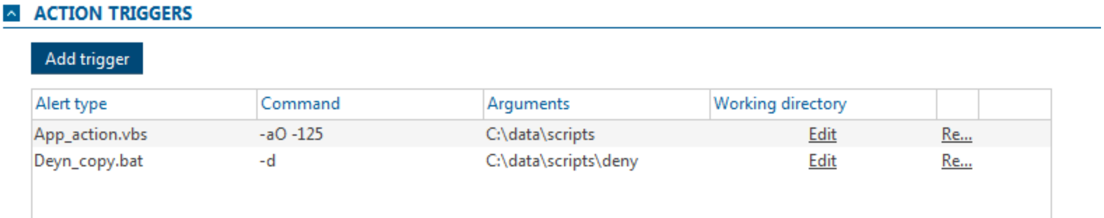
- *Service alert* – used to notify the administrator on service incidents.

- *Incidents* – These are alerts to security incidents that appear only in WebSafetica. They will not be displayed in the console and no notifications will be sent by E-mail.

After installation, a default alert (warning) is automatically created, which contains all of the alerts from the *Service alerts -> Service category.*

Action triggers

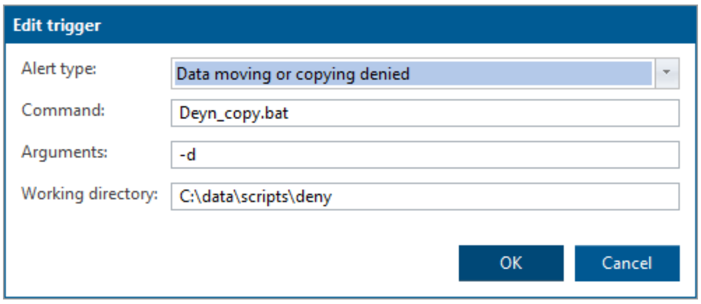
In the action triggers section you can set, based on activity records, the command or script start with particular arguments and in a selected folder. The command will be run on the client station with client under the account of the user who caused the incident. These settings apply to the entire server.



ACTION TRIGGERS

Alert type	Command	Arguments	Working directory		
App_action.vbs	-aO -125	C:\data\scripts	Edit	Re...	
Deyn_copy.bat	-d	C:\data\scripts\deny	Edit	Re...	

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



Edit trigger

Alert type: Data moving or copying denied

Command: Deyn_copy.bat

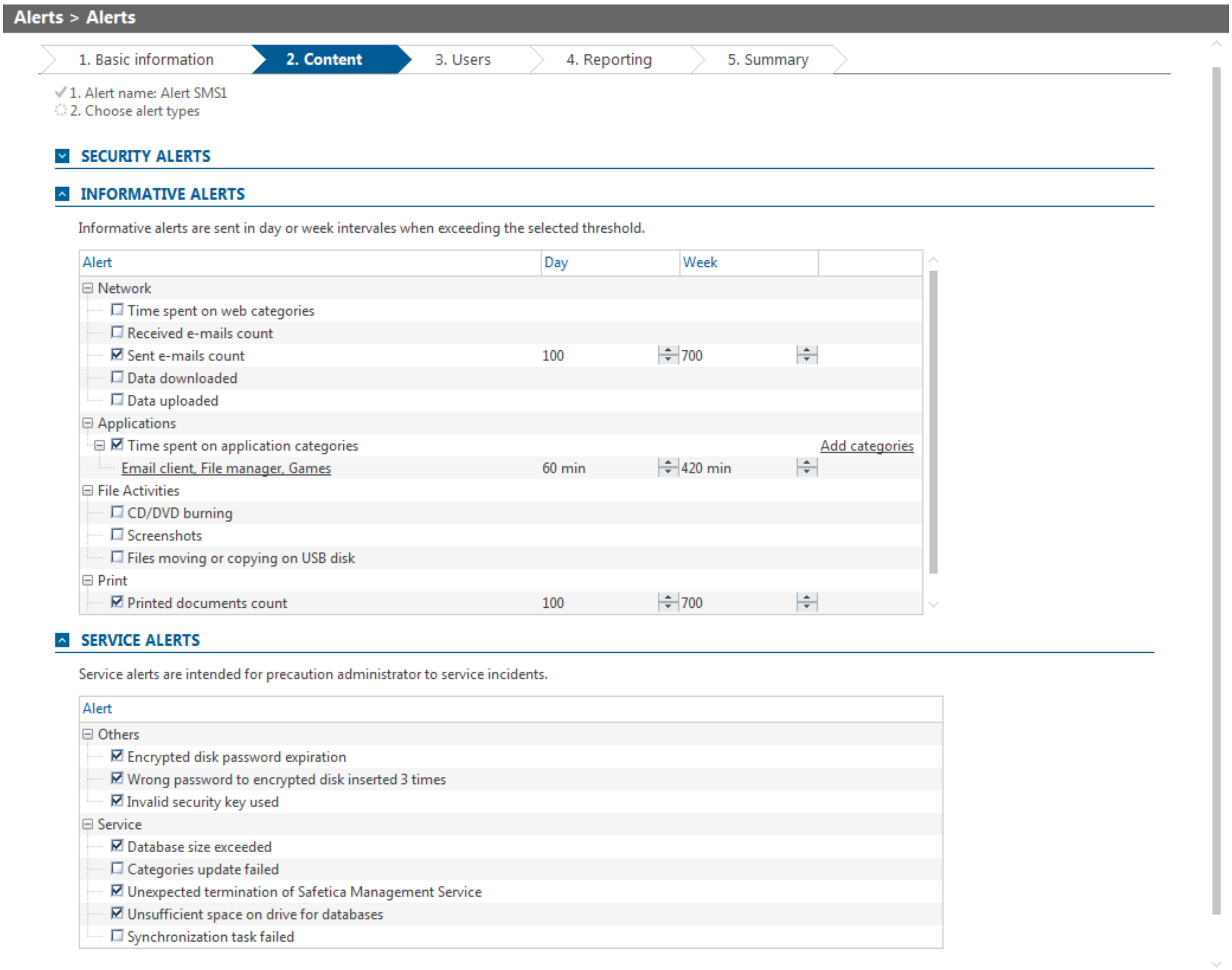
Arguments: -d

Working directory: C:\data\scripts\deny

Setting up a new alert

1. To create a new alert set, click on *New alert.*
2. Enter a name and description for the new alert set and click on *Next* in the bottom right section.
3. Next you will see lists of various types of alerts sorted by categories. Select the required alert from the list. You can select multiple types of alerts from multiple categories. After completing your selection, click *Next.*

   Notes: Informative alerts are sent only based on user behavior. To receive informative alerts, users must be included in the alert set. Security alerts are created in the context of users and computers. They are sent from the end workstation immediately after the incident.



Alerts > Alerts

1. Basic information | **2. Content** | 3. Users | 4. Reporting | 5. Summary

✓1. Alert name: Alert SMS1
2. Choose alert types

SECURITY ALERTS

INFORMATIVE ALERTS

Informative alerts are sent in day or week intervales when exceeding the selected threshold.

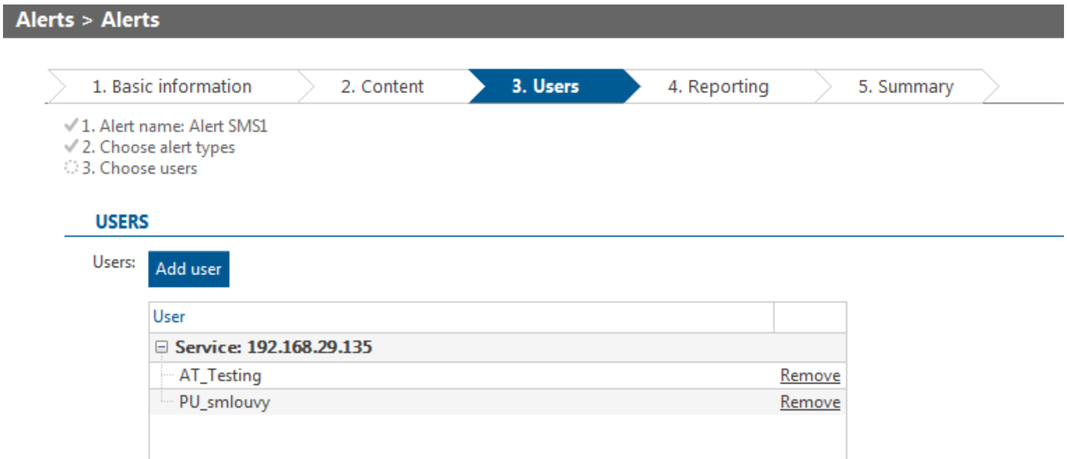
Alert	Day	Week	
⊟ Network			
□ Time spent on web categories			
□ Received e-mails count			
☑ Sent e-mails count	100	700	
□ Data downloaded			
□ Data uploaded			
⊟ Applications			
⊟ ☑ Time spent on application categories			Add categories
Email client, File manager, Games	60 min	420 min	
⊟ File Activities			
□ CD/DVD burning			
□ Screenshots			
□ Files moving or copying on USB disk			
⊟ Print			
☑ Printed documents count	100	700	

SERVICE ALERTS

Service alerts are intended for precaution administrator to service incidents.

Alert
⊟ Others
☑ Encrypted disk password expiration
☑ Wrong password to encrypted disk inserted 3 times
☑ Invalid security key used
⊟ Service
☑ Database size exceeded
□ Categories update failed
☑ Unexpected termination of Safetica Management Service
☑ Unsufficient space on drive for databases
□ Synchronization task failed

4. In the next step, click *Add User*. 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 *Next.*



Alerts > Alerts

1. Basic information | 2. Content | **3. Users** | 4. Reporting | 5. Summary

✓1. Alert name: Alert SMS1
✓2. Choose alert types
3. Choose users

USERS

Users:

User	
⊟ **Service: 192.168.29.135**	
AT_Testing	Remove
PU_smlouvy	Remove

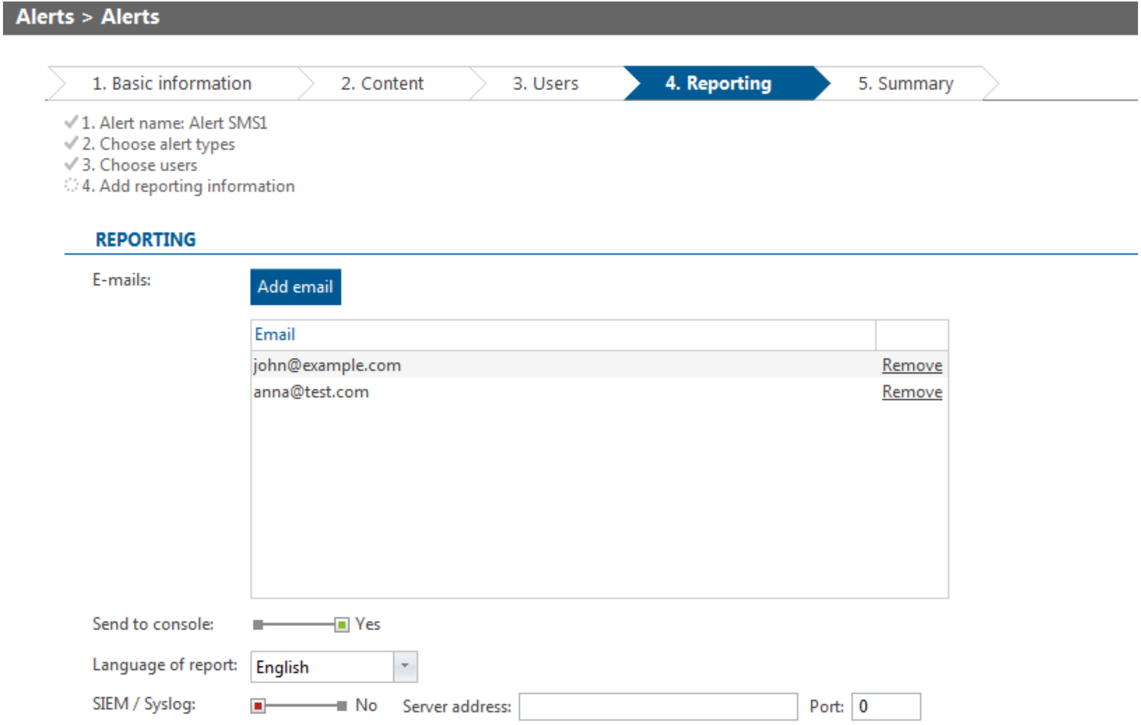
5. In this step, you will be selecting the e-mail addresses to which the alert notification will be sent. To do this, click *Add e-mail.* You can also have alert notifications sent directly to the console. To do this, use the *Send alert notifications to Safetica Management Console slider*. By using 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 server.

   Once finished, click *Next.*

   Note 1: SMTP server must be configured for sending mails. Its configuration is done in Profile -> Server settings -> SMTP server.

   Note 2: 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.



✓ 1. Alert name: Alert SMS1
✓ 2. Choose alert types
✓ 3. Choose users
4. Add reporting information

E-mails:

Email	
john@example.com	Remove
anna@test.com	Remove

Send to console: Yes

Language of report: English

SIEM / Syslog: No Server address: Port: 0

6. The last step shows an overview of the settings you have made while setting up the alert. Clicking on the *Finish* button will add the alert to the list. To save the changes, click the button ✓ on the right at the top.

Visualization

All alerts get recorded and you can view them later in the visualization mode. The Safetica user only has alerts created under his account shown here.

In the top part, you will find statistics and charts. In the bottom part of your view, there is a list of generated alerts. Clicking on the relevant statistics in the bottom part of the screen will display 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 left corner of the console.

4.4.3 Reports

By means of automated reporting included in Safetica, you can be regularly informed about the current situation inside your company. You can have activity reports sent to you, either for individual employees, groups or the whole server. To change the settings for reporting, go to the *Reports* 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 receive the report.

Reports can be viewed by clicking on the *Reports* button in the upper left corner of the Safetica console.

Settings

Reports are set up for the server 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 the ✕ top right button.

The left section of the view shows the list of records made. After selecting the report in the left list, its details are displayed on the right side, such as name, date of last creation, list of included reports, list of users whom the report concerns and a list of e-mails where it will be sent and in what format.

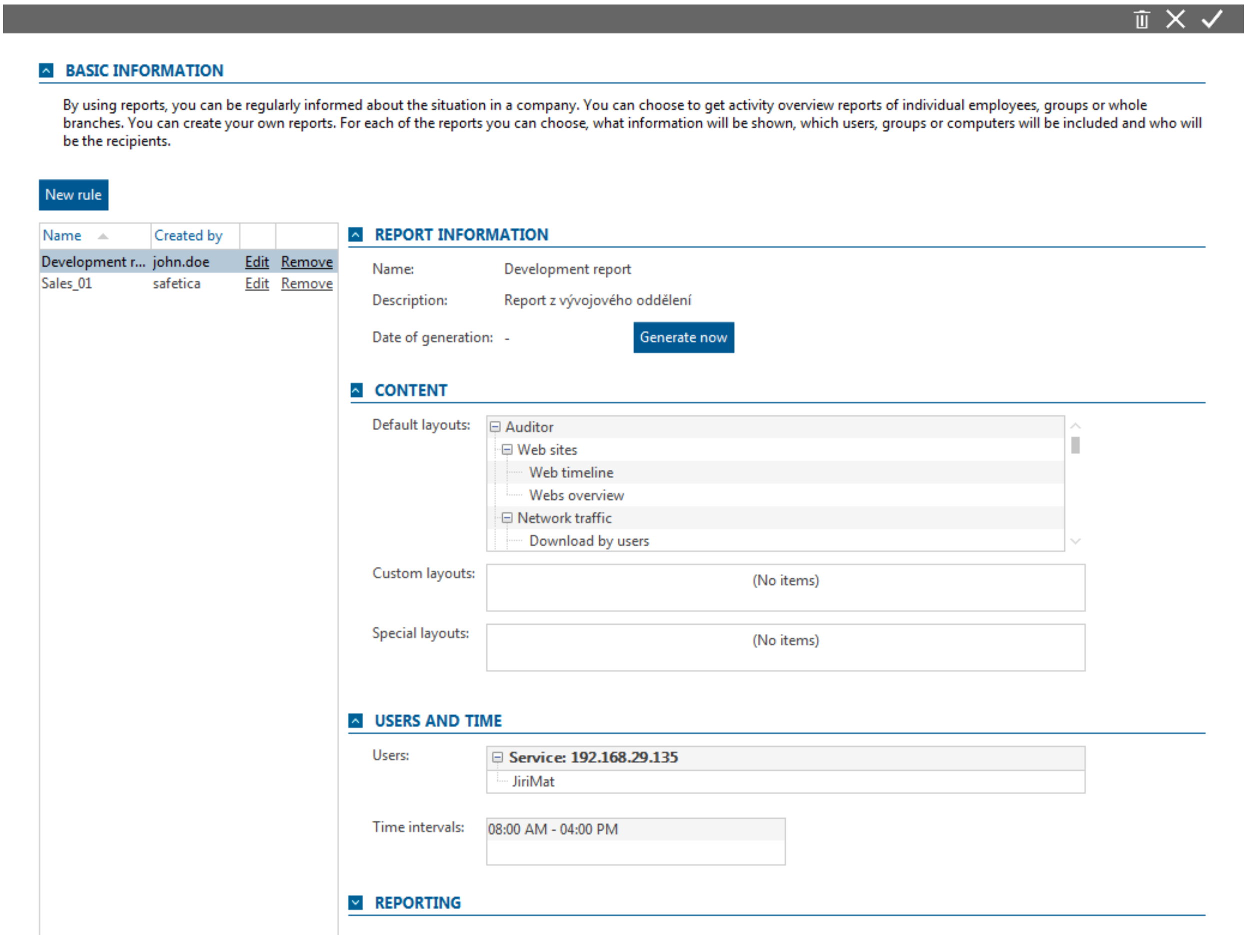
Click *Generate now* to immediately create the report.

In the *Created by* column you will find the name of the account for connecting to the server under which the report was created.

Click the *Edit* button next to the relevant item of the report to update the item.

Click on *Remove* to remove a report.

Note: You can also create reports in the WebSafetica.



BASIC INFORMATION

By using reports, you can be regularly informed about the situation in a company. You can choose to get activity overview reports of individual employees, groups or whole branches. You can create your own reports. For each of the reports you can choose, what information will be shown, which users, groups or computers will be included and who will be the recipients.

Name	Created by		
Development r...	john.doe	Edit	Remove
Sales_01	safetica	Edit	Remove

REPORT INFORMATION

Name: Development report

Description: Report z vývojového oddělení

Date of generation: -

CONTENT

Default layouts:
- Auditor
  - Web sites
    - Web timeline
    - Webs overview
  - Network traffic
    - Download by users

Custom layouts: (No items)

Special layouts: (No items)

USERS AND TIME

Users:
- **Service: 192.168.29.135**
  - JiriMat

Time intervals: 08:00 AM - 04:00 PM

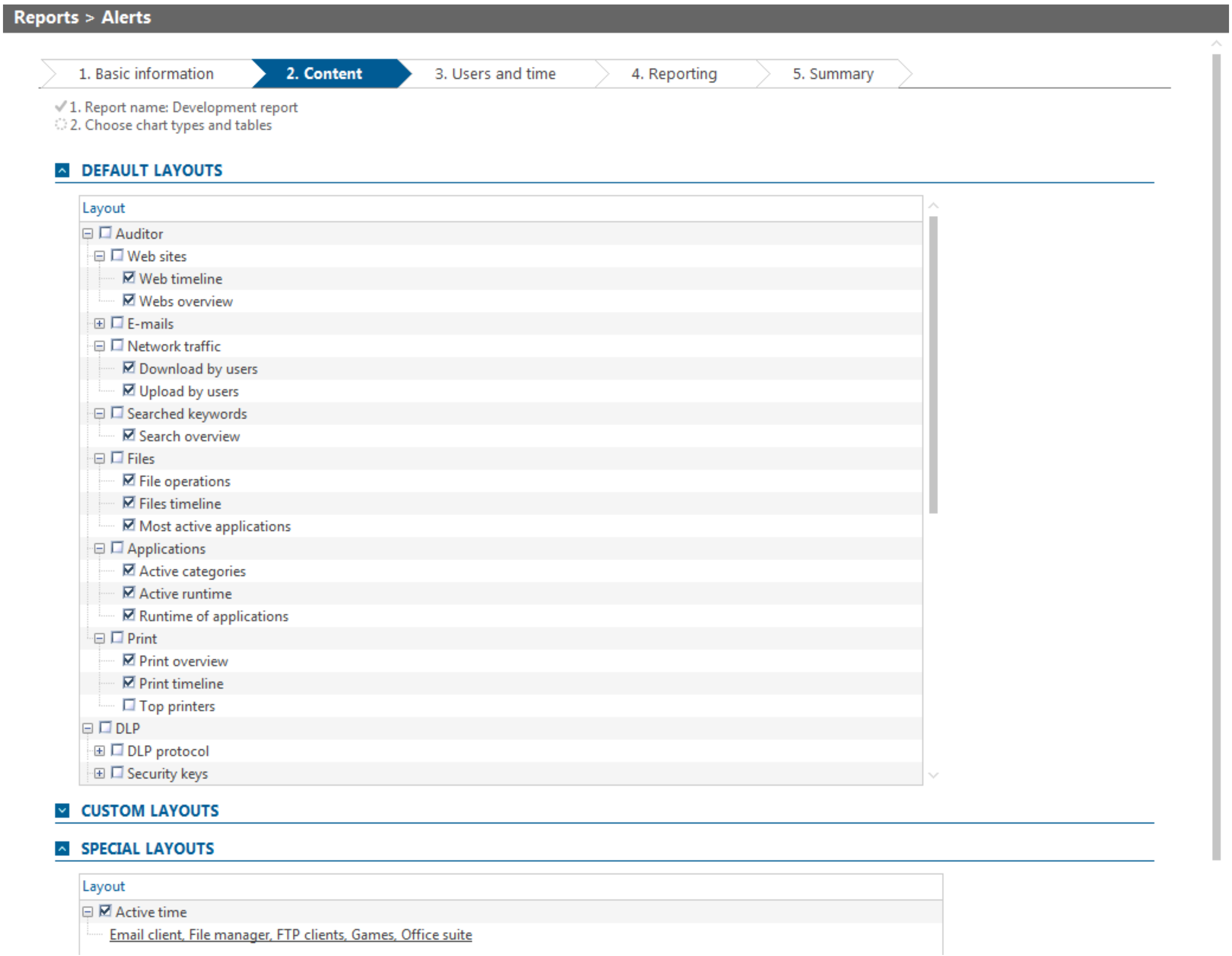
REPORTING

Creating a new report

1. To create a new report, click on *New rule.*
2. Enter a name and description for the new report and click on *Next* in the bottom right section.
3. This section contains a list of available reports. The list is based on view reports (see *Visualization Mode -> Layouts*), with which you can create custom layout for charts, columns and filters in the visualization modes of each Safetica function.
   - o *Default* – here are the default reports of charts, columns and their filters for each function in the individual Safetica modules.
   - o *Custom* – here are the reports created by Safetica users in different functions.

- *Special* – special sets reports are provided here:
  - *Active time* – reports contain active time in selected categories of applications. Categories can be selected when the *Active time* box is checked.
  - *Overview* – the basic overview of Safetica functions is included in the report.

In the list, select the reports you want to include in the overall report. When the selection is complete, click *Next.*



Reports > Alerts

1. Basic information | 2. Content | 3. Users and time | 4. Reporting | 5. Summary

✓ 1. Report name: Development report
2. Choose chart types and tables

DEFAULT LAYOUTS

Layout
- ⊟ □ Auditor
  - ⊟ □ Web sites
    - ☑ Web timeline
    - ☑ Webs overview
  - ⊞ □ E-mails
  - ⊟ □ Network traffic
    - ☑ Download by users
    - ☑ Upload by users
  - ⊟ □ Searched keywords
    - ☑ Search overview
  - ⊟ □ Files
    - ☑ File operations
    - ☑ Files timeline
    - ☑ Most active applications
  - ⊟ □ Applications
    - ☑ Active categories
    - ☑ Active runtime
    - ☑ Runtime of applications
  - ⊟ □ Print
    - ☑ Print overview
    - ☑ Print timeline
    - □ Top printers
- ⊟ □ DLP
  - ⊞ □ DLP protocol
  - ⊞ □ Security keys

CUSTOM LAYOUTS

SPECIAL LAYOUTS

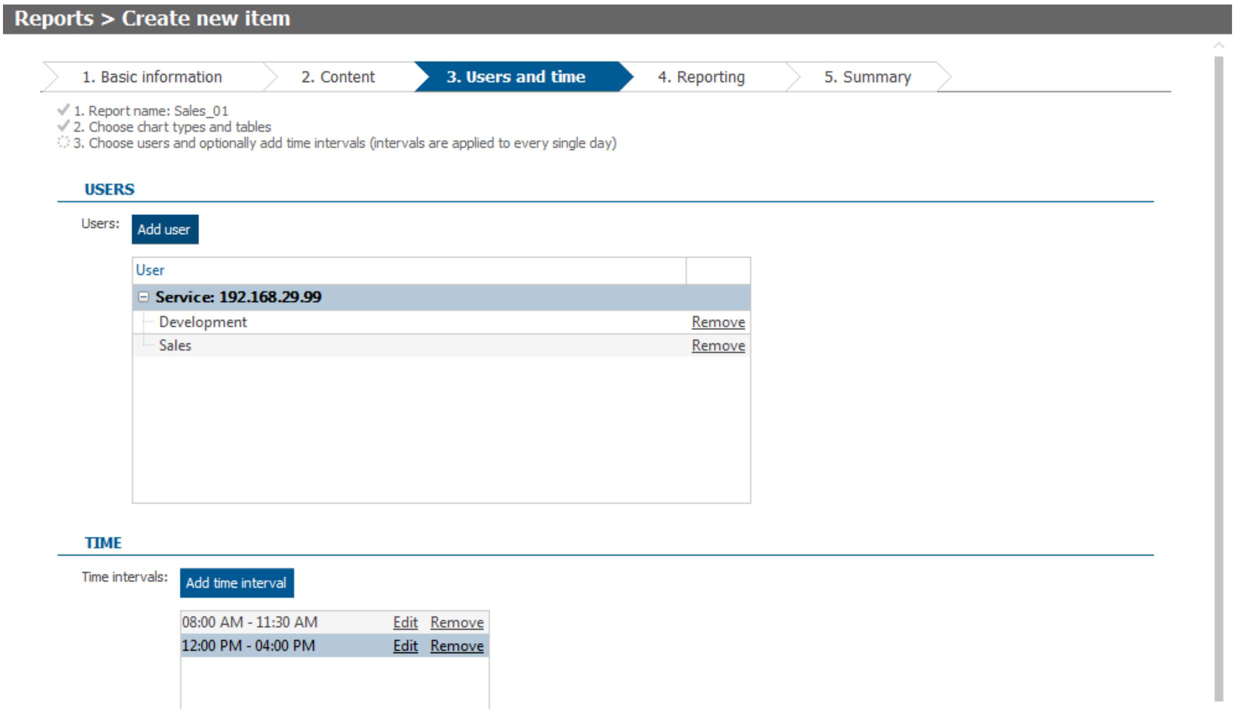
Layout
- ⊟ ☑ Active time
  - Email client, File manager, FTP clients, Games, Office suite

4. In the next step, click *Add User*. A dialog will appear in which you can select computers, groups, or individual users. Selected reports from the previous step will then only be sent to the users, computers, or groups you select in this step.

   Note: Only users, computers and groups from the selected server are displayed in the default Reports view.

   Under *Time*, you can specify what data are used in the report. Reports will be created only from records that were created in the specified time intervals of the day. If the list of intervals is empty, data from the whole day will be used.

   Click on *Next.*



Reports > Create new item

1. Basic information | 2. Content | 3. Users and time | 4. Reporting | 5. Summary

✓ 1. Report name: Sales_01
✓ 2. Choose chart types and tables
3. Choose users and optionally add time intervals (intervals are applied to every single day)

USERS

Users: Add user

User	
⊟ Service: 192.168.29.99	
Development	Remove
Sales	Remove

TIME

Time intervals: Add time interval

08:00 AM - 11:30 AM	Edit	Remove
12:00 PM - 04:00 PM	Edit	Remove

5. In the penultimate step specify to whom, how often and in which way the reports will be created.

a. Click on *Add e-mail* to add e-mail addresses to which the generated report will be sent.

b. Use the slider to choose what form the reports will have, the format in which the generated report will be sent.

i. *Charts (pdf)* – reports are only sent in the form of charts in pdf.

ii. *Logs (xls)* – reports are only sent in the form of records in an Excel table.

iii. *Charts (pdf) and logs (xls)* – reports are sent in the form of charts in pdf and records in an Excel table.

c. Next, select whether you want to save the created reports to a disk file. If yes, specify the path where to save the report. The report will be stored on a PC where the server is running. The specified path must exist on that machine. In the case of creating reports across multiple servers, the path must exist on all computers with server where the report will be generated.

d. As the penultimate step, specify whether the report should be sent at regular intervals or not. You can choose from these options:

i. *Day* – the report will be sent every day after midnight. The report contains data for the last day.

ii. *Week* – the report will be sent on Monday after midnight. The report contains data for the last week.

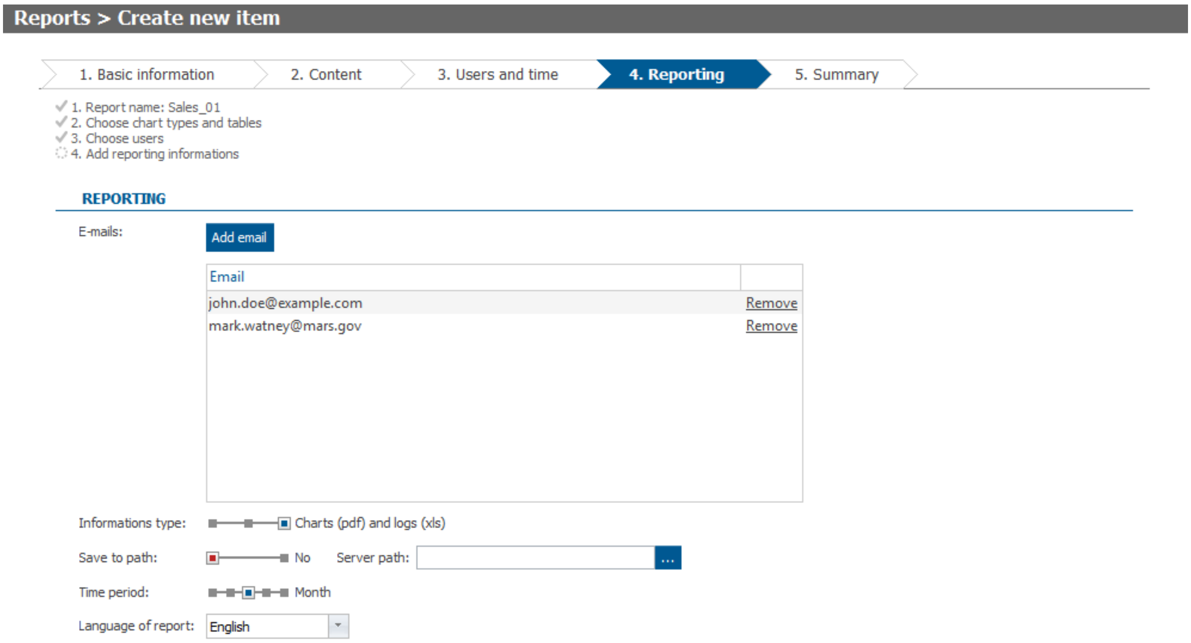
iii. *Month* – the report will be sent on the first day of the new month, after midnight. The report contains data for the last month.

iv. *Quarter* – the report will be sent on 1 Jan, 1 Apr, 1 Jul and 1 Oct, after midnight. The report contains data for the quarter.

v. *Half-year* – the report will be sent on 1 Jan and 1 Jul, after midnight. The report contains data for the last six months.

e. Finally, enter the language of the report.

Once finished, click *Next.*



Reports > Create new item

✓ 1. Report name: Sales_01
✓ 2. Choose chart types and tables
✓ 3. Choose users
4. Add reporting informations

REPORTING

E-mails: Add email

Email	
john.doe@example.com	Remove
mark.watney@mars.gov	Remove

Informations type: Charts (pdf) and logs (xls)

Save to path: No Server path: ...

Time period: Month

Language of report: English

6. The last step shows an overview of the settings you have made while setting up the report. Clicking on the *Finish* button will add the report to the list. To save the changes, click the button ✓ on the right at the top.

4.4.4 Maintanance

4.4.4.1 Categories

Safetica includes ready categories of websites, applications and extensions. The categories are used in various Safetica functions for better orientation in the recorded data and setting of different security policies.

In Categories tab, you can update the category database, edit categories and create custom categories of applications or websites.

Category setting is accessible from *Maintenance -> Categories.*

Description of the view

In the upper part of the view, there is a button labelled *Clear local cache*. Clicking this button will delete the local cache of categorised applications and websites on all endpoint stations with the client. This speeds up updates of application or website categorisation if changes are made in the console. We recommend using this option only in exceptional and really urgent cases.

Note: Deletion of the categorisation cache will only be performed on server-connected clients that are managed from the currently running console. This operation can take longer depending on when current settings are downloaded by the individual clients.

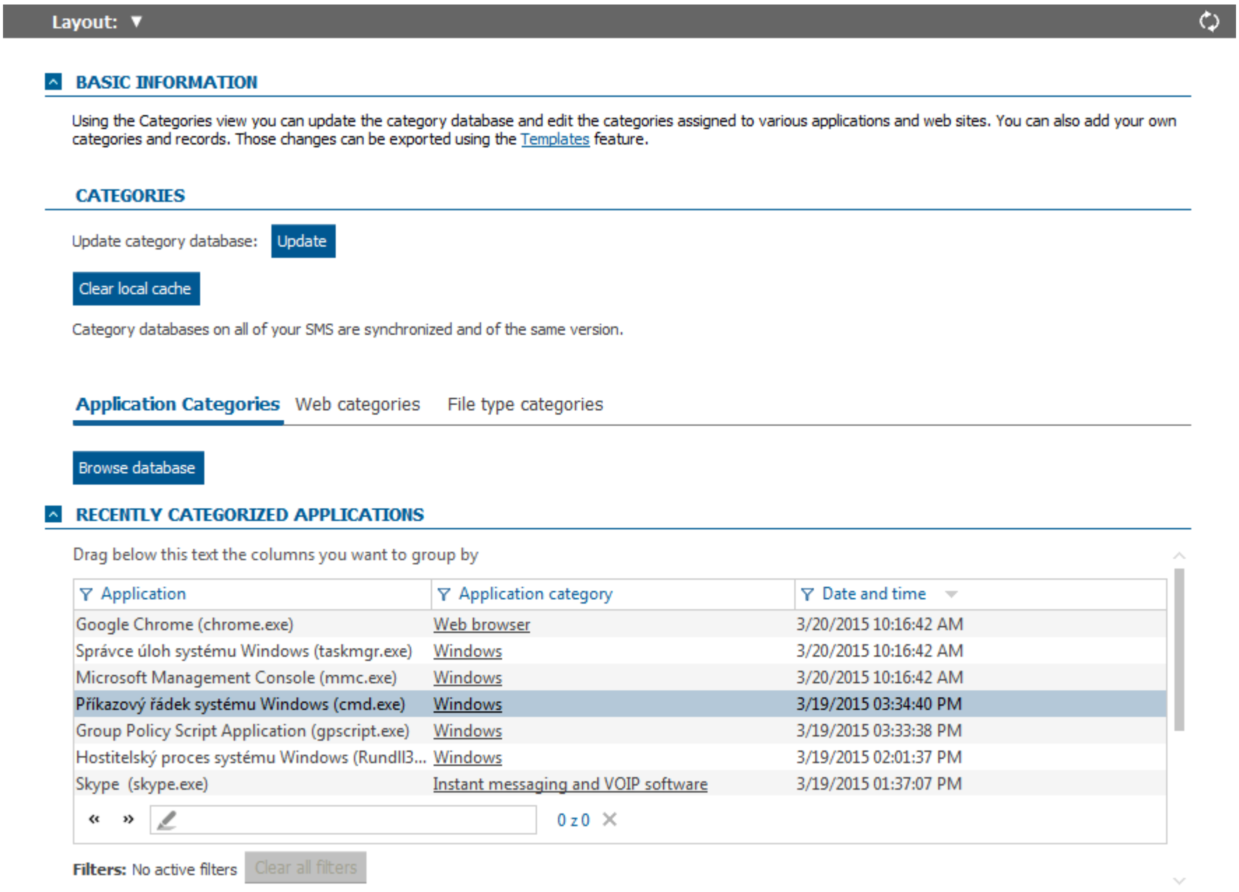
In the middle of the view, there are the following options for each category:

- *Web category* – access to web categories administration. You can add your own categories and websites here.
- *Applications category* – access to applications categories administration. You can add your own categories and applications here.
- *Extensions category* – access to extension categories administration. You can add your own categories and extensions here.

Select from the tree the server on which you wish to administer the categories. You can display categories by clicking the *Browse categories* button. If you mark several server instances in the tree, only categories which share the server selected will be displayed after clicking the 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.

Note: You can also use a categorization in the WebSafetica.



BASIC INFORMATION

Using the Categories view you can update the category database and edit the categories assigned to various applications and web sites. You can also add your own categories and records. Those changes can be exported using the Templates feature.

CATEGORIES

Update category database: Update

Clear local cache

Category databases on all of your SMS are synchronized and of the same version.

RECENTLY CATEGORIZED APPLICATIONS

Drag below this text the columns you want to group by

Application	Application category	Date and time
Google Chrome (chrome.exe)	Web browser	3/20/2015 10:16:42 AM
Správce úloh systému Windows (taskmgr.exe)	Windows	3/20/2015 10:16:42 AM
Microsoft Management Console (mmc.exe)	Windows	3/20/2015 10:16:42 AM
Příkazový řádek systému Windows (cmd.exe)	Windows	3/19/2015 03:34:40 PM
Group Policy Script Application (gpscript.exe)	Windows	3/19/2015 03:33:38 PM
Hostitelský proces systému Windows (Rundll3...	Windows	3/19/2015 02:01:37 PM
Skype (skype.exe)	Instant messaging and VOIP software	3/19/2015 01:37:07 PM

Filters: No active filters Clear all filters

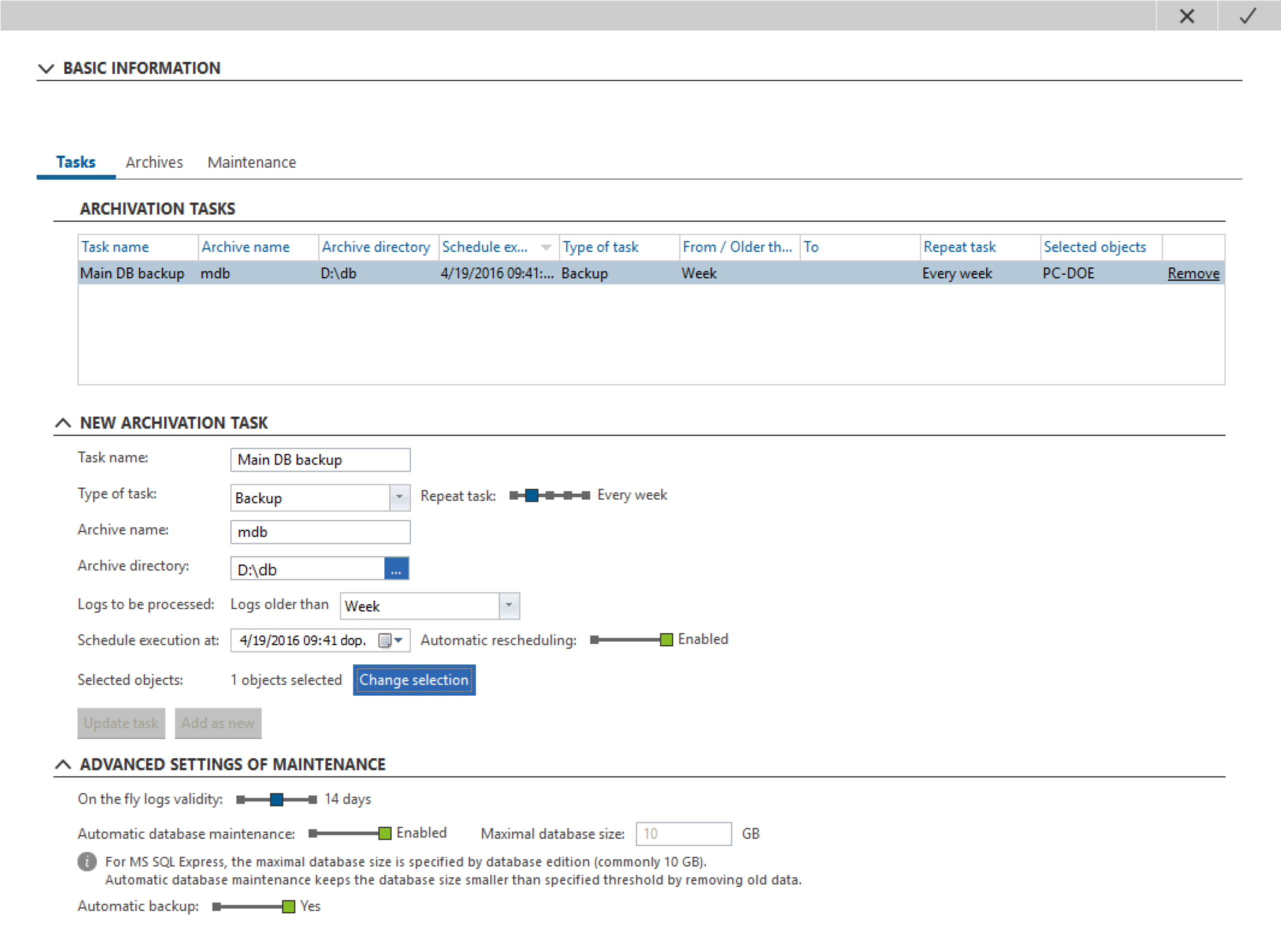
4.4.4.2 Database management

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

You manage databases of the server 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 the ✕ top right button.

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 server to review the data.
- *Maintenance* – shows information on the databases of all server instances that you are administering through the console. This information can be exported to XML format.



BASIC INFORMATION

Tasks | Archives | Maintenance

ARCHIVATION TASKS

Task name	Archive name	Archive directory	Schedule ex...	Type of task	From / Older th...	To	Repeat task	Selected objects	
Main DB backup	mdb	D:\db	4/19/2016 09:41:...	Backup	Week		Every week	PC-DOE	Remove

NEW ARCHIVATION TASK

Task name: Main DB backup

Type of task: Backup Repeat task: Every week

Archive name: mdb

Archive directory: D:\db

Logs to be processed: Logs older than Week

Schedule execution at: 4/19/2016 09:41 dop. Automatic rescheduling: Enabled

Selected objects: 1 objects selected Change selection

ADVANCED SETTINGS OF MAINTENANCE

On the fly logs validity: 14 days

Automatic database maintenance: Enabled Maximal database size: 10 GB

For MS SQL Express, the maximal database size is specified by database edition (commonly 10 GB).
Automatic database maintenance keeps the database size smaller than specified threshold by removing old data.

Automatic backup: Yes

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:

- *Task name* – name of the task.
- 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.
- *Repeat task* – how often will be the task repeated:
  - o *Every week*
  - o *Every 14 days*
  - o *Every month*
  - o *Every three months*
- *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*:
  - o From-To – it is possible to choose a time period for backup of monitored data
  - o 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

- *Schedule execution at* – the exact time when the task will run. Start time job must be processed outside the interval of processed records.
- *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 server 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 server has its own database, so if we want to archive data from a database, we need to run the backup task over each server 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.

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.

- *Automatic backup* – Safetica performs each day at about midnight automatic database backup to prevent the risk of possible damage to the database. The backup is kept for the period of one month. These backups do not replace the user database backups.

Visualization

The task visualization includes a table with detailed records on executed database administration tasks.

Every record contains several types of information presented in columns. The list of available columns is located 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 located on the right side.

Available columns with records of executed tasks:

- *Date and time* – date and time of record creation.
- *User name* – name of the Safetica user account (User accounts) that was used for administration. After the account name you can see the name of the PC from which the administration task was performed (<account name>@<PC name>).
- *Task name*
- *Archive name*
- *Archive directory* – folder in which the archive will be stored.

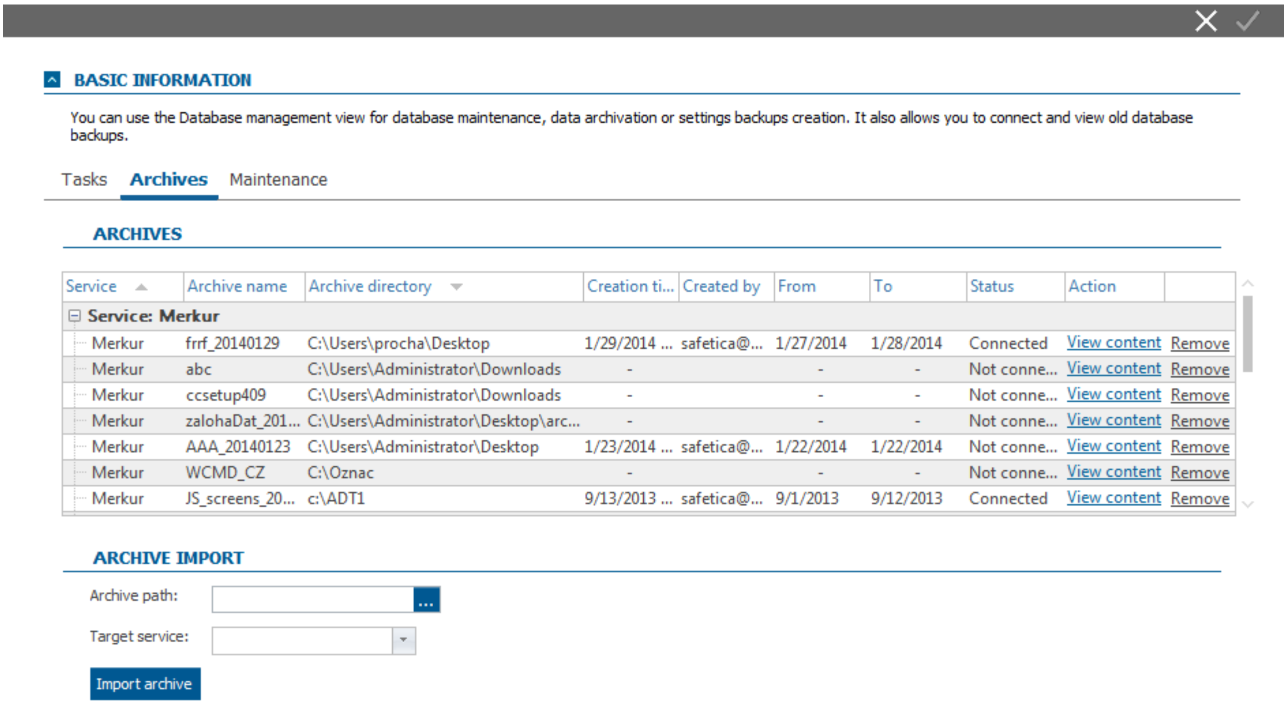
  Note: It is the folder on the PC with the Safetica database.
- *Type of task* – type of the task executed: Back-up, Back-up and remove, Remove, Remove screenshots, Back-up settings.
- *Details* – task details will be displayed after clicking the Details button.

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.

Archives

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



You can use the Database management view for database maintenance, data archivation or settings backups creation. It also allows you to connect and view old database backups.

Service	Archive name	Archive directory	Creation ti...	Created by	From	To	Status	Action	
Service: Merkur									
Merkur	frrf_20140129	C:\Users\procha\Desktop	1/29/2014 ...	safetica@...	1/27/2014	1/28/2014	Connected	View content	Remove
Merkur	abc	C:\Users\Administrator\Downloads	-		-	-	Not conne...	View content	Remove
Merkur	ccsetup409	C:\Users\Administrator\Downloads	-		-	-	Not conne...	View content	Remove
Merkur	zalohaDat_201...	C:\Users\Administrator\Desktop\arc...	-		-	-	Not conne...	View content	Remove
Merkur	AAA_20140123	C:\Users\Administrator\Desktop	1/23/2014 ...	safetica@...	1/22/2014	1/22/2014	Not conne...	View content	Remove
Merkur	WCMD_CZ	C:\Oznac	-		-	-	Not conne...	View content	Remove
Merkur	JS_screens_20...	c:\ADT1	9/13/2013 ...	safetica@...	9/1/2013	9/12/2013	Connected	View content	Remove

Import archive

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

Browsing the archives

You can connect the corresponding archive (backup) to console by clicking on *View content* link. It is possible to connect multiple archives at once. Each attached archive appears as a new root item in the user tree.

Close archive – disconnect from server

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

Visualization

The visualization contains a table with detailed records on how the database archives that were created were handled.

Every record contains several types of information presented in columns. The list of available columns is located 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 located on the right side.

Available information with archive handling records:

- *Date and time* – date and time of record creation.
- *User name* – name of Safetica user account (User accounts) that was used for administration. After the account name you can see the name of the PC from which the administration task was done (<account name>@<PC name>).

- *Archive path* – path to the archive as saved.

  Note: This is the folder on the PC with the Safetica database.
- *Server name* – name of the server instance to which the archive was connected.
- *Action* – operation performed with the archive: Browse database, Connect, Disconnect, Close archive.
- *Details* – after clicking the Details button, details on how the archive was handled will be displayed.

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.

Maintanance

In the Maintenance section you will find detailed information on the usage of main and record databases in the various servers instances that you administer with the console.

By clicking the *Export* button, you can save a summary of used database capacity to an Excel spreadsheet (.xls). Along with the table, also an XML file with the same name will be exported, containing detailed database information.

Statistics sending

Use the *Send statistics automatically* button to enable the sending of basic statistics on your Safetica installation to Safetica Technologies. Statistics will be sent once per week and contain the following information:

- Licence number information
- Version and amount of Safetica clients installed
- XML file containing detailed information on database saturation

Outgoing data is used to improve products and services of Safetica Technologies and do not contain any sensitive data.

Maintenance scripts

In this section, the user can run scripts used for database maintenance. For safety reasons, only scripts signed by Safetica Technologies are permitted.

To begin, first select the script to run. This is done through the file selection dialog, which can be opened using the ... button. Click on *Send* to run the specified script. After completing the script, you will be prompted to save a file with the output of the executed script.

4.4.4.3 Update

The update management allows you to find out what server updates are available, and to download and install them. You can update Safetica client in the Endpoint management view.

You can find the update management tools in Safetica console under *Maintanance -> Update*.

Note: You can only manage those Safetica servers that are connected to your console.

Server update

This section is used for updates of the Safetica server. Update to the current version is performed by clicking on *Download and update to version*. This will download and install the current Safetica server.

Endpoint enrollment

Here, you can update all connected clients after the installation of the current server. The update is made automatically by clicking on *Update clients to version.*

Note: The clients can be managed manually through the tab Endpoint management

If you want to install the client on a new computer, click on *Get Downloader Agent* to download the latest installation package of the downloader agent. Then install it on a new computer and after connecting it to the server install the client using the tab *Endpoint management.*

Update options

In this section you can specify how updates shall be performed.

The text box *Use temporary URL* is used for entering the address to alternative files for update. After clicking the *Use* button, installation files will be downloaded from the address you entered. By clicking *Reset to default*, you can cancel use of an alternative address.

You can use the *Select* button in the *Update from file* section to choose the *Safetica Universal Installer* from a local site to be used for the update.

Definition updates

Here, you can turn on the automatic definition updates. Updates include only changes in categories, integration settings and web activity detector.

Click the *Update* button for manual update.

Note: Automatic update may increase the workload of the SQL Server.

Visualization

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

There 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.

4.4.4.4 Access management

Here you can manage accounts for logging on to individual server modules and their access rights or settings. The account also provides access to the Safetica console. All accounts are authenticated with username and password.

User account management can be found in the console, under *Maintenance -> Access management.*

Settings

In the settings view, the left side shows a list of created accounts in the currently linked server. The right pane shows access rights to individual functions and settings for the selected account and item in the tree.

User accounts

This part shows a list of Safetica user accounts.

Default accounts:

- Service administrator account with exclusive access to all functions and settings.
  - o Login: safetica
  - o Default password: S@fetic@2004
  - o After first log on to Safetica using this account, the user is prompted to change the password.
  - o This account cannot be deleted, disabled or renamed.
  - o Its password can be changed only after logging on to Safetica with this account under Profile -> Change password
- Account with preset basic rights to Safetica functions.
  - o Login: starter
  - o The account cannot be deleted or renamed.

New accounts are added by clicking Add account and filling out a new username and password.

The Clone account button can be used to create a new account with the same settings as the source account.

By clicking the Edit button next to an account, you can change its name and password or disable the account. Disabled accounts cannot be used to access Safetica. Disabled accounts can be re-enabled. After enabling, the username and password will remain the same as before.

Accounts can be deleted by clicking on the Delete button next to the account.

Types of accounts:

The type of account specifies the functions and settings the user will have access to:

- *Administrator* – has full access to all functions and settings.
- *Manager* – can display records from all functions, but cannot make settings.
- *Custom* – you can specify the access to various functions and settings in Access Settings.

Access settings

You can set up the following access rights for each user account. These access rights to individual functions will only apply to users, groups or computers selected in the tree.

Note: Some functions cannot be set for individual items in the tree. Their settings apply to the entire Safetica.

- *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 server and then creating all required user accounts for server. On any other console you will connect to the server using the created user account.

Visualization

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

Each record contains several types of information represented by columns:

- *Date and time* – the date and time when the record was made.
- *PC* – name of the PC from which the Safetica user was connected to Safetica server.
- *User name* – the name of the Safetica user who performed the action.
- *Action* – identification of the action performed by the Safetica 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.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.4.4.5 Client settings

Client settings include general configuration of the Safetica client.

Settings

The client settings are set only for users, groups or PCs or the server 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 the ✕ top right button.

Allowed actions

By enabling Uninstall or Update, you permit uninstalling or updating the client. Without permitting this, it is impossible for security reasons to uninstall, update, or otherwise disrupt the running of 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 client protection, see Protection against unauthorized manipulation of 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 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. Client will not be visible in *Add or Remove programs* list. Client 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 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:

  o *Hide all* – all dialogs on client are hidden.

  o *Show only interactive dialogs* – dialogs are hidden except for dialogs that require user interaction.

  o *Show all* – all dialogs are enabled.

- *Language* – client 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.When a large amount of records have accumulated, the sending interval will be automatically shortened. The sending time interval will return to the original value after the amount of records collected has been reduced.

- *Interval for settings check* – with this setting you can determine how often client will query server for new settings. By doing this you can affect the time required for transferring the settings made using console to client.

- *Time spent by sending records* – here you can set a percentage of how much time it takes to send a client records into the database. Lower values prevent excessive network load.

  Note: The default value is 10%, which without good reason and knowledge do not change. If you want to change the setting anyway, consult it with Safetica technical support first.

- *Interval for the user's inactivity determination* – here you can specify the time after which the status of the user activity measured shall change from active to inactive time. In other words, if a user does not work with his/her PC (does not use the mouse or keyboard) for this period of time, the status of his/her measured activity will change to inactive. These settings affect the measurement of active time in the website functions Applications and Trends.

- *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.

Network Settings

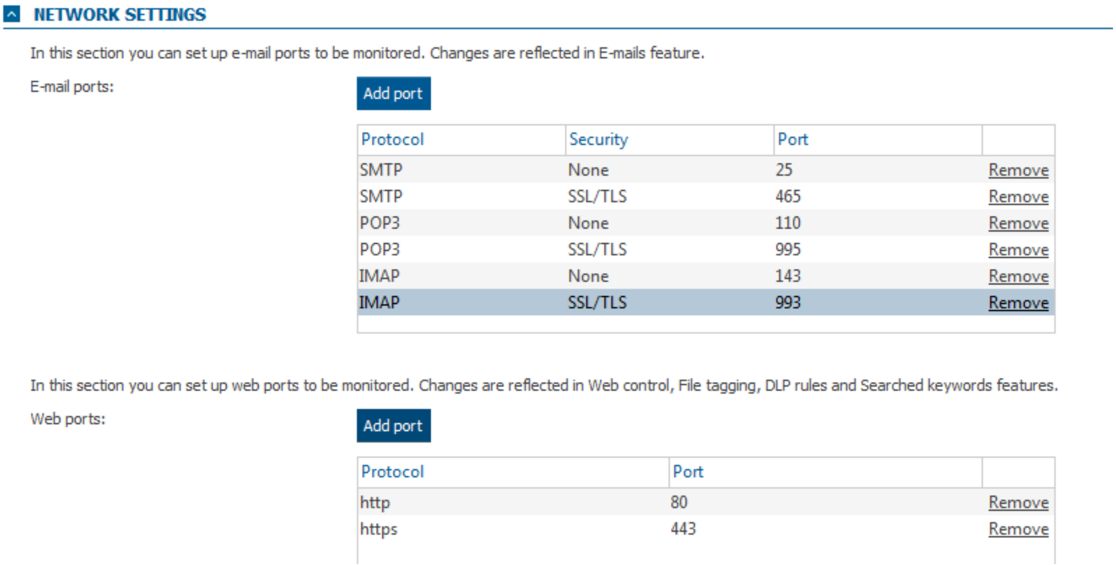
In this setting, you can change the port number used by some protocols to match your environment. These settings have an effect on some functionalities.

- *E-mail ports* - for the supported protocols (SMTP, POP3, IMAP) you can specify their security settings (none, STARTTLS, SSL/TLS) and ports where they are running. The changes will be reflected in the E-mail function. Monitoring of e-mail communication will take place on the protocols and ports listed. By default, the list contains the most common combinations of protocols, ports and security features as shown above.

  Note: For some non-standard e-mail clients, it is necessary to check integration into the SSL/TLS communication in the Integration settings and activate it manually if necessary. Without Safetica integration into the SSL/TLS communication, you will not be able to monitor secured e-mail communication.

  Integration into SSL/TLS communication in the default settings will be performed only for e-mail clients and webmail. For other applications, integration into SSL/TLS communication is disabled in default settings. For non-standard e-mail clients, these settings must be checked and integration activated manually if necessary.

- *Web Ports* - for supported protocols, i.e. *http* and *https* , you have an option here to specify on which ports they are available. Changes will take effect in the following functions: Web Control, Data Tagging, DLP Rules. By default, the list contains the most common combinations of protocols and ports.
- *Detecting proxy settings* - if this option is enabled, proxy settings on the client are checked and the relevant ports are added to the network settings.



NETWORK SETTINGS

In this section you can set up e-mail ports to be monitored. Changes are reflected in E-mails feature.

E-mail ports:

Protocol	Security	Port	
SMTP	None	25	Remove
SMTP	SSL/TLS	465	Remove
POP3	None	110	Remove
POP3	SSL/TLS	995	Remove
IMAP	None	143	Remove
IMAP	SSL/TLS	993	Remove

In this section you can set up web ports to be monitored. Changes are reflected in Web control, File tagging, DLP rules and Searched keywords features.

Web ports:

Protocol	Port	
http	80	Remove
https	443	Remove

Debug logs

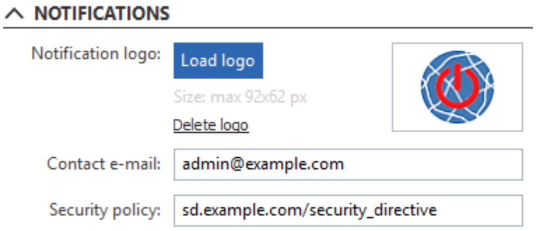
Here it is possible to set the level of client debug logging from only the most Critical logs to Verbose logs. It is intended for the use of system administrators or Safetica technical support. Verbose logs can negatively affect client performance.

Notifications

You can partially adjust the appearance of notification dialogues displayed to users:

1. *Notification logo* – replaces the default dialogue logo with your own. The selected logo must have a size of 96 x 62 pixels and be in .png, .jpg or .bmp format.
2. *Contact e-mail* – e-mail address that will be located at the bottom of the dialogue.
3. *Security policy* – URL address of your security policy.

Settings:



NOTIFICATIONS

Notification logo: Load logo

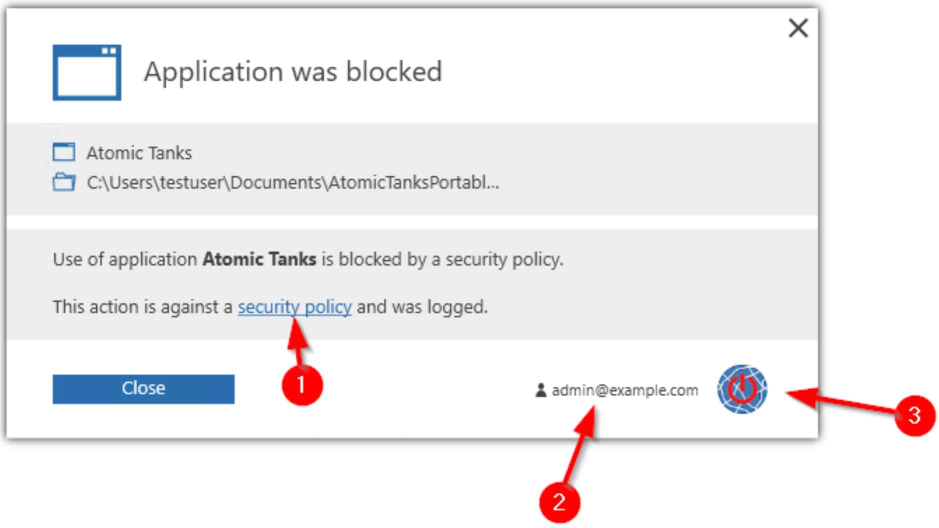
Size: max 92x62 px

Delete logo

Contact e-mail: admin@example.com

Security policy: sd.example.com/security_directive

The resulting notification dialogue with detailed information that will be displayed to users:



Application was blocked

Atomic Tanks

C:\Users\testuser\Documents\AtomicTanksPortabl...

Use of application **Atomic Tanks** is blocked by a security policy.

This action is against a security policy and was logged.

Close

admin@example.com

For more information, read the Notification Dialogues section in help.

Non-working hours

With these settings, you can specify how Safetica will behave outside working hours. These settings will affect the monitoring and blocking of applications and websites. Data protection will always be functional regardless of the local setting of working hours.

Using the switch, you can select one of the following options of how Safetica will behave during non-working hours:

- *Productivity-based monitoring and blocking* – during non-working hours, Safetica will behave in the same way as during working hours.

- *Do not block by productivity* – during non-working hours, applications and websites will be monitored but they will not be blocked.
- *No productivity-based monitoring and blocking* – during non-working hours, applications and websites will not be monitored or blocked.

Working hours

Detailed settings of working hours can be accessed by clicking the button with the same name. These settings apply to the entire server. You can specify which days are working days, and choose the beginning and end of working hours.

Non-working days

You can set non-working days here. You can add predefined holidays from the list of holidays for each country, add your own non-working days and holidays, or use a combination of both these approaches.

Visualization

Each record contains several types of information represented by columns:

- *Date and time* – date and time when a local administration operation was performed.
- *PC* – name of PC where the operation was performed.
- *User name* – name of the user under which the operation was performed.
- *Operation* – what local administration task was performed.
- *Details* – contains other possible information on the operation performed.

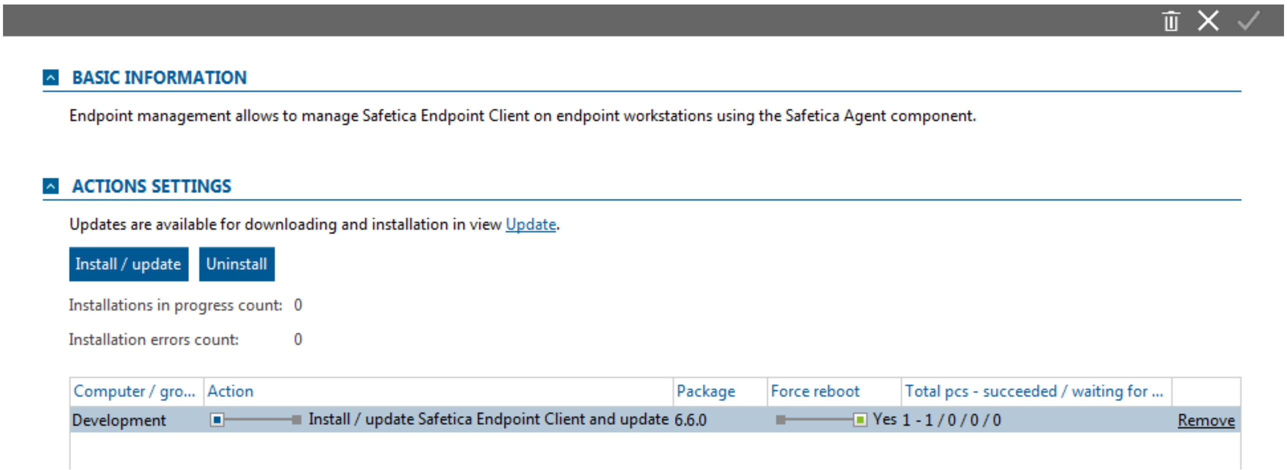
You can learn more about the visualization interface in the chapter *Visualization mode*.

4.4.4.6 Endpoint management

Endpoint Management lets you remotely manage the installation of the Safetica client on endpoint stations using downloader agent components.

Note: Client can be managed only on those workstations that have the downloader agent component installed.

Endpoint management can be found in the console under *Maintenance -> Endpoint management.*



BASIC INFORMATION

Endpoint management allows to manage Safetica Endpoint Client on endpoint workstations using the Safetica Agent component.

ACTIONS SETTINGS

Updates are available for downloading and installation in view Update.

Install / update | Uninstall

Installations in progress count: 0

Installation errors count: 0

Computer / gro...	Action	Package	Force reboot	Total pcs - succeeded / waiting for ...	
Development	Install / update Safetica Endpoint Client and update	6.6.0	Yes	1 - 1 / 0 / 0 / 0	Remove

Settings

Endpoint management is set up for the server 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 the ✕ button in the upper right section.

Action settings

In this section you can *Install/Update* or *Uninstall* client or the downloader agent on end workstations.

At the bottom, there is a table with a list of created administrative tasks. For each task in the table, depending on its type, you can edit some of its features:

- For the Install/Update type, you can:
    - *Install / Update ...* - with this option, client is installed or updated. When updating client, the downloader agent is also updated.

      Note: Remote client installation or upgrade is only possible if the downloader agent is installed on the end workstation. Installing the downloader agent at the end station is only possible locally or using a bulk installation tool. For example, using a Group Policy in Active Directory.
    - *Update downloader agent*
- For the *Uninstall* type, you can use the slider to specify whether to uninstall only client or client and the downloader agent simultaneously.

Then you have an opportunity for each type of task to use the slider to force the restart of the end workstation afterwards.

For each task, the basic statistics are given about its status:

- On how many computers the task will be executed
- On how many computers the task has been successfully executed
- On how many computers the task has failed
- On how many computers reset is being awaited
- On how many computers the task has not yet been executed.

To remove a task, use the button of the same name. For the sake of clarity, all the tasks remain in the table even after completion until manually removed.

Note: Client installation, update or uninstallation over this view does not have to be enabled in Client Settings.

Installation or Update

To start client or downloader agent installation or update, click *Install/Update.*

1. In the first step, use the drop-down list to select the item to install or upgrade. Client versions in the list are automatically downloaded to the computer with the server when it is updated through the Updates view.

   Installation files for the appropriate version can also be entered manually. Just select *New Package* from the drop-down list and enter the path to the each component in the dialog box:

    - MSI package with Safetica Endpoint Client 64-bit
    - MSI package with Safetica Endpoint Client 32-bit

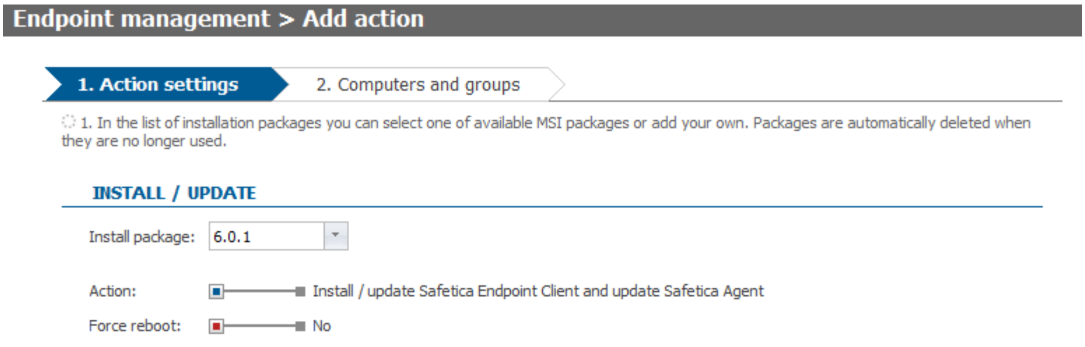
- MSI package with the downloader agent

Note: You do not have to enter the paths to all packages. You can specify paths to the client packages or just to packages with downloader agent or to all at once.

After selecting the version, choose the type of task:

- Installation or update of the Safetica client and update of the downloader agent
- Updating the downloader agent

At the end of the first step, select whether to restart the end workstation after the task is completed.



Endpoint management > Add action

1. In the list of installation packages you can select one of available MSI packages or add your own. Packages are automatically deleted when they are no longer used.

INSTALL / UPDATE

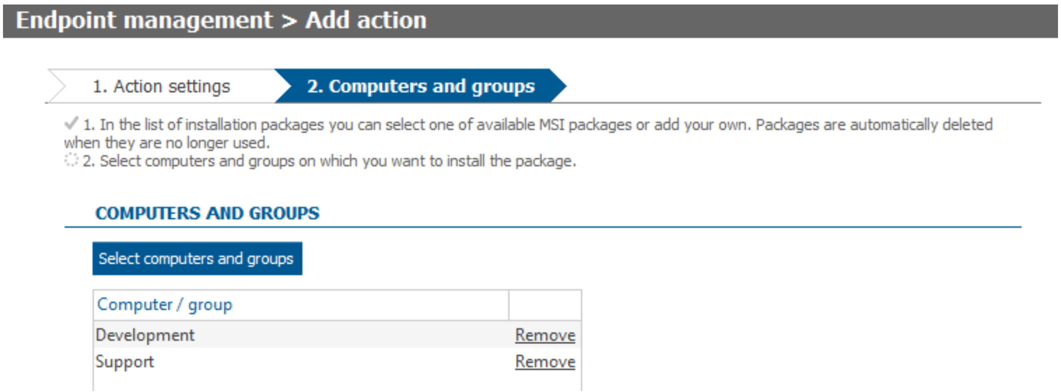
Install package: 6.0.1

Action: Install / update Safetica Endpoint Client and update Safetica Agent

Force reboot: No

2. In the second step, enter groups or computers on which to execute the task. Finally, click on *Finish* and then save the task using the ✓ button.

Note: Computers with assigned task are highlighted.



Endpoint management > Add action

✓ 1. In the list of installation packages you can select one of available MSI packages or add your own. Packages are automatically deleted when they are no longer used.
2. Select computers and groups on which you want to install the package.

COMPUTERS AND GROUPS

Computer / group	
Development	Remove
Support	Remove

Uninstalling

To start client or downloader agent uninstallation, click *Uninstall.*

1. The first step is to select which components you want to uninstall:
   - Safetica client
   - Safetica client and downloader agent

     Caution: Uninstalling the downloader agent disables the remote client installation and management at the end workstation.
2. In the second step, enter groups or computers on which to execute the uninstallation. Finally, click on *Finish* and then save the task using the ✓ button.

Visualization

At the top, there is a summary of the number of end workstations and the number of stations with client or downloader agent installed.

Below the summary, there is a table detailing the end workstations and client and downloader agent components.

Each record contains several types of information represented by columns:

- *PC* – name of the end station on which the client is installed.
- *Client version* – number of the installed client version.
- *Agent version* – displays the version number of the downloader agent.
- *Last settings update* – last time of client settings synchronization.
- *Operating system* – version of the operating system on the end workstation.
- *Network layer* – type of the Safetica network layer used (see Integration settings).
- *Unsent records* – contains the number of records client has not yet sent to the server and the time as of which the record is valid.
- *Last logs sent* – date and time when client sent the latest records into the database.
- *IP* – address of the PC with client installed.
- *Certificate refused* – shows whether client rejected the certificate of the new server.
- *System edition* – identification of the operating system edition.
- *Service pack* – identification of the service pack of the operating system.
- *System type* – identification of the operating system type.
- *System details* – detailed information on the operating system.
- *Download all logs* – click on this link to force sending all records to the central database for the respective client. This option is available only if there are over 100 unsent records on the client.
- *Installation state* – displays the status of client installation or upgrade.
- *Conflicting SW* – there is a list of applications installed on your computer which can be potentially conflicting with Safetica.
- *.NET* – whether Microsoft .NET Framework is installed at the end workstation.
- *Repeat installation* – use this button to restart the installation/update at the end workstation if not performed successfully before.
- *Service installed* – whether the Safetica client service, which is part of client, is installed on the end workstation.
- *Service running* – whether the Safetica Client Service is running on the end workstation.
- *Database connection* – displays the status of client connection to the database after its installation.
- *Webdetector version* – current version number of the webdetector.
- *Computer type* – desktop or notebook.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.4.4.7 Endpoints deactivation

In this view, you can disable individual functional components of the Safetica client.

Note: If you want to change the settings, consult it with Safetica technical support first.

End workstation deactivation can be found in the console under *Maintenance -> Endpoints deactivation.*

Settings

The deactivation function is set only for users, groups or PCs or the server 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 the ✕ top right button. If deactivation is set for any functional client part with respect to any of the users logged in, then the client is disabled for the entire end station.

Main Settings

- *Safetica Endpoint Client* – use the slider to turn off all client functions (drivers, integrated technologies and services). To switch off the client completely, the end workstation must be rebooted. client continues running, but only for the purpose of re-activation.
- *Full deactivation* – can be used when the client deactivation does not help. To apply the setting, the workstation must be rebooted.

Integrated technologies

You can turn off (disable) some parts of Safetica here.

- *Network layer* – network layer is used by some Safetica features for networking. Disabling the network layer will affect the functionality of some Safetica features.
- *MAPI extension* – use the slider to disable the Safetica extension for the Microsoft Outlook e-mail client. The extension is required for the proper function of monitoring communication through Outlook e-mail client. To apply the settings, you need to restart Outlook on the client station.

  Note: After deactivating the MAPI extension, only the monitoring of e-mails connected via Microsoft Exchange will cease to work. Monitoring of e-mails via other protocols will continue working.
- *Contextual menu* – you can disable the integration of some Safetica features into the contextual menu of Windows.

Drivers

In this section, you can remove (disable) drivers that Safetica installed in the system. Driver removal will affect the functionality of some Safetica features that need them for their activities.

- *Safetica disk driver* - driver used by some Safetica features that work with the filesystem. The following Safetica functions will be affected if switched off:
  - Client installation folders will not be protected, see *Protection against unauthorized handling with the client*.
  - *Device administration*
  - *DLP rules*
  - *Disk guard*
- *Safetica process monitor driver* – driver needed by Safetica to work with other processes in the system.

- *Safetica encryption driver* – driver used by some Safetica features for encryption.
- *Safetica device driver* – driver used by some Safetica device control features.

To disable the drivers, you need to restart the client station.

Services

In this section, you can turn off (disable) services ensuring that various Safetica functions can run.

- *Safetica networking service* – service providing some Safetica functions for networking.
- *Safetica DLP service* – service providing the Safetica DLP function.
- *Safetica file monitor service* – service providing Safetica file tracking function (Files, DLP protocol).
- *Safetica classification service* – service providing Safetica functions for file analysis and tagging.
- *Safetica applications service* – service providing Safetica functions for application blocking.
- *Safetica devices service* - service providing Safetica functions for device monitoring and blocking.

Visualization

The visualization view mode provides an overview of activated and deactivated client parts at the end workstations.

At the top, there is a summary with the numbers of completely and partially deactivated client.

At the bottom, there is a table detailing the activated and deactivated client parts at the end workstations.

4.4.4.8 Debugging informations collection

Using this view, you can create a task to collect debugging information from Safetica client.

Collection of debugging information can be found in the console under *Maintenance -> Debugging informations collection.*

Settings

Debugging information collecting is set up for the server 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 the ✕ button in the upper right section.

Collecting settings

In this section, you can create new tasks of collecting debugging information from the client. The collected information will be saved to a folder in the appropriate server, which is specified at the beginning of the settings. The path to the collected data location on the server can be changed.

To create a new task, click on the *Add collecting task* button. A task creation wizard will open:

1. In the first step, use the slider to select the information you want to obtain from client. You can choose from these options:
   - *Basic* – the collection will include only basic information about client. The contents of the collection is shown below the slider.

    - *Advanced* – the collection will include more information about client. The contents of the collection is shown below the slider.
    - *Custom* – with this option, you can choose the content of collected client information manually. From the list below the slider select the desired collection items.

   After selecting, click on *Next.*

2. In the second step, select groups or computers from which you want to obtain debugging information about the client. Then click on *Finish* and then save the task using the ✓ button.

At the bottom of the collection settings, there is a table with an overview of existing tasks. For each task, it is specified from which end workstation or group the collection was carried out, which files were included in the collection and the status of downloads on server.

Click on *Remove* to can cancel the respective task.

After clicking on *Download* a dialog box opens in which you can select a local location where you want to download all the collected debugging information from server.

After clicking on *Details* a window opens containing detailed information on the collection of debugging information. You can download individual files from the collection here.

Downloading

This section is an overview of downloading collected debugging information from server to a local console. If an error occurs while downloading, you can repeat it by clicking on *Download again.*

By clicking on *Clear completed downloads*, all the records of completed debugging information collection will be deleted.

Visualization

In the visualization mode, the table with records on the size of the file with debugging information is at the end workstations. Each record contains the following information (columns):

- *PC* – name of the end workstation.
- *Changed* – date of the last update of the size for the file with debugging information.
- It also contains information on the size of each file with debugging information.

4.4.4.9 Integration settings

Integration settings defines the behaviour of Safetica on the endpoint stations.

For integration settings, see console under *Maintenance -> Integration settings*.

You can choose from several integration modes, where every higher mode always includes the features and functions of the previous one(s) on a lower level. The lowest level mode is *No integration* whereas the highest level mode is *Maximum integration*. By switching over the integration modes you can en-/disable the desired applications excluding those that have been edited manually. Integration does not affect the Auditor functions and Application control in Supervisor.

You can choose from the following integration levels:

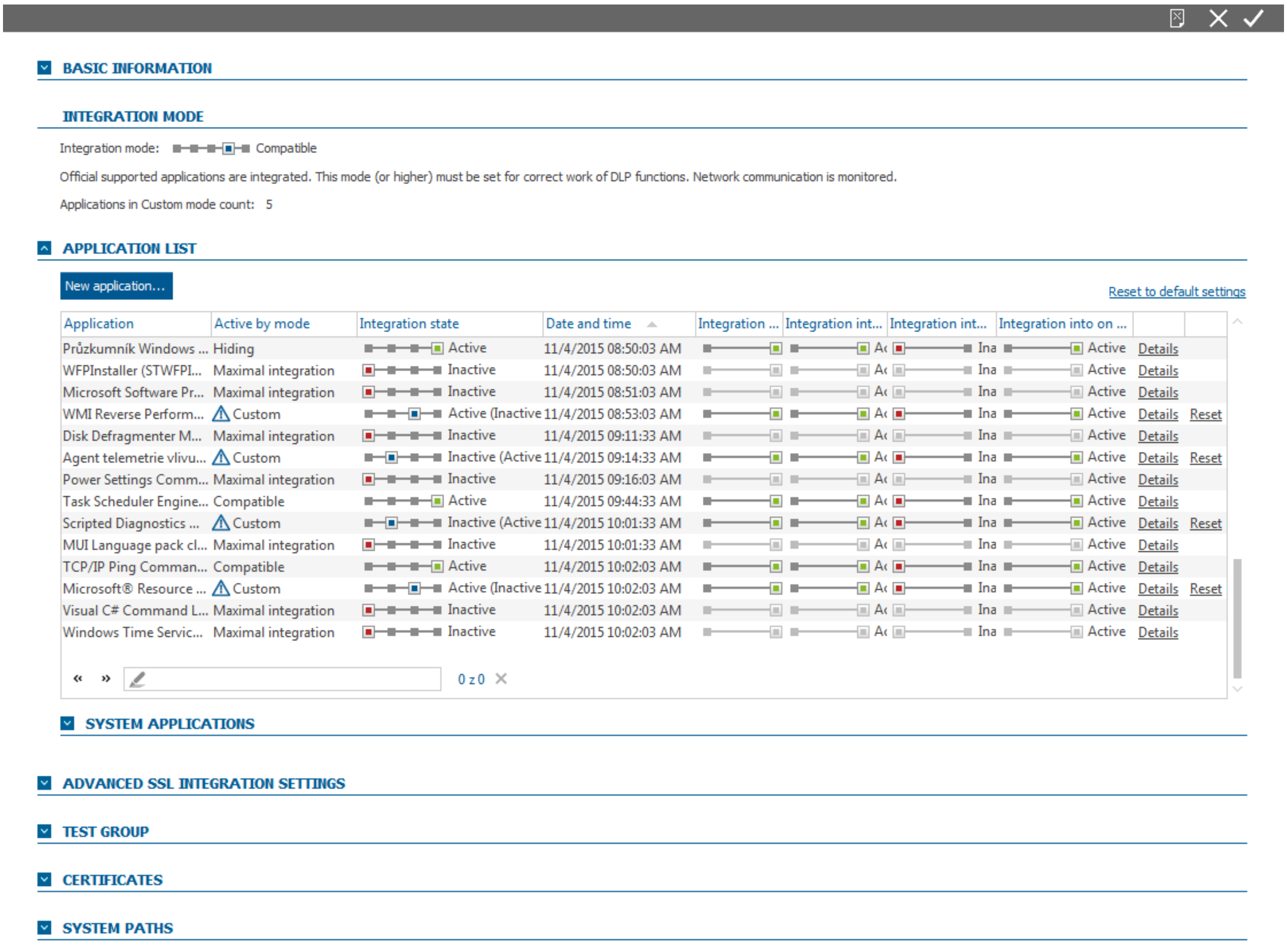
- *No integration* – applications are not integrated.
- *Hiding* – there are integrated applications that allow hiding Safetica on the endpoint station. Users will not be able to simply detect that there is Safetica running on the computer.
- *Advanced monitoring* – there are integrated applications that allow monitoring the file-related operations and obtaining better outputs for the Files function. Network communication is not

affected.

- *Compatible* – officially supported applications are integrated. This mode (or a higher one) is required for the proper functioning of DLP. Network communication is monitored.
- *Maximum integration* – all applications are integrated, with the exception of known incompatible ones, such as antivirus programs. This mode may essentially affect the functionality of the working environment. Network communication is monitored.

Integration management is set up for the server highlighted in the user tree. To apply the settings, you need to save the changes with the ✓ button or you can cancel the changes with the ✕ button in the upper right section.

It is recommended to consult every individual change in the integration settings with the Safetica Technologies technical support.



BASIC INFORMATION

INTEGRATION MODE

Integration mode: Compatible

Official supported applications are integrated. This mode (or higher) must be set for correct work of DLP functions. Network communication is monitored.

Applications in Custom mode count: 5

APPLICATION LIST

New application...

Reset to default settings

Application	Active by mode	Integration state	Date and time	Integration ...	Integration int...	Integration int...	Integration into on ...		
Průzkumník Windows ...	Hiding	Active	11/4/2015 08:50:03 AM		Ac	Ina	Active	Details	
WFPInstaller (STWFPI...	Maximal integration	Inactive	11/4/2015 08:50:03 AM		Ac	Ina	Active	Details	
Microsoft Software Pr...	Maximal integration	Inactive	11/4/2015 08:51:03 AM		Ac	Ina	Active	Details	
WMI Reverse Perform...	⚠ Custom	Active (Inactive	11/4/2015 08:53:03 AM		Ac	Ina	Active	Details	Reset
Disk Defragmenter M...	Maximal integration	Inactive	11/4/2015 09:11:33 AM		Ac	Ina	Active	Details	
Agent telemetrie vlivu...	⚠ Custom	Inactive (Active	11/4/2015 09:14:33 AM		Ac	Ina	Active	Details	Reset
Power Settings Comm...	Maximal integration	Inactive	11/4/2015 09:16:03 AM		Ac	Ina	Active	Details	
Task Scheduler Engine...	Compatible	Active	11/4/2015 09:44:33 AM		Ac	Ina	Active	Details	
Scripted Diagnostics ...	⚠ Custom	Inactive (Active	11/4/2015 10:01:33 AM		Ac	Ina	Active	Details	Reset
MUI Language pack cl...	Maximal integration	Inactive	11/4/2015 10:01:33 AM		Ac	Ina	Active	Details	
TCP/IP Ping Comman...	Compatible	Active	11/4/2015 10:02:03 AM		Ac	Ina	Active	Details	
Microsoft® Resource ...	⚠ Custom	Active (Inactive	11/4/2015 10:02:03 AM		Ac	Ina	Active	Details	Reset
Visual C# Command L...	Maximal integration	Inactive	11/4/2015 10:02:03 AM		Ac	Ina	Active	Details	
Windows Time Servic...	Maximal integration	Inactive	11/4/2015 10:02:03 AM		Ac	Ina	Active	Details	

« » 0 z 0 ✕

SYSTEM APPLICATIONS

ADVANCED SSL INTEGRATION SETTINGS

TEST GROUP

CERTIFICATES

SYSTEM PATHS

Application list

There are two lists of applications in this section. The first list contains all non-system applications detected on the endpoint stations. The applications are integrated on the basis of a particular integration mode. In the Stealth mode and higher modes, it is possible to manually en-/disable the integration of any application.

The list contains the following information:

- *Application* – application name
- *Date and time* – date and time of application detection.
- *Active by mode* – from what mode is the application integration active. If *Custom* is entered here, integration has been set manually.

- *Integration state* – here you can specify the mode of integration for individual applications
  - o *Inactive* – application is not integrated.
  - o *Inactive (Active in the test group)* – the application is integrated only in the computers mentioned in the test group, see *Test group* below.
  - o *Active (Inactive in the test group)* – the application is integrated everywhere, with the exception of the computers mentioned in the test group.
  - o *Active* – application is integrated in all the computers.

In the following options you can enable or disable the integration in individual functional parts of the application. You can enable or disable the integration in the parts of the application:

- *Integration into application's operations* – 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* – 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* – if integration is active, Safetica will be able to monitor the encrypted SSL/TLS network communication and/or enter into this communication with the aim of applying security. This can happen for example in an enforced security policy.
- *Application's outputs tagging* – if integration is active, Safetica will be able to monitor operations of the application and continuously tag their output data on the basis of the applicable security policies.

Click on *Reset* to restore the integration settings to their default values. Click on *Restore to default settings* over the list to change all the applications in the list to their default settings.

Adding a new application

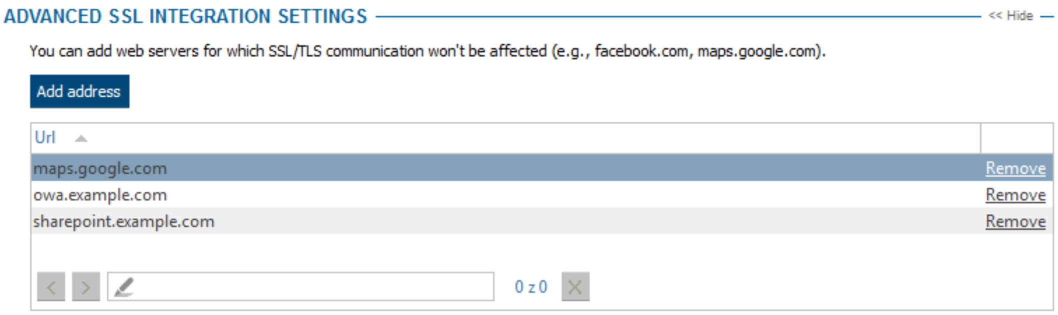
Every application installed on the endpoint stations is synchronised with the list on console. If you want to pre-create the settings for the application which has not yet been detected on the endpoint station, click on *New application ...* In the dialog box, select the .exe file for the application you want to add. The application process file should therefore be accessible from the station where console is currently running. Once confirmed, Safetica loads information that is necessary for proper identification of the application on all systems.

System applications

This table shows the important applications of the operating system. These applications have defined integration settings; it is not advisable to change these settings. The change in behaviour may affect the functionality of the working environment.

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.



ADVANCED SSL INTEGRATION SETTINGS

You can add web servers for which SSL/TLS communication won't be affected (e.g., facebook.com, maps.google.com).

Url	
maps.google.com	Remove
owa.example.com	Remove
sharepoint.example.com	Remove

Test group

The PC test group is intended for verifying correct functionality of the Safetica interface across various applications. Add only those PCs to the test group that perfectly match the hardware and software equipment of the majority of PCs in your environment. Also, do not add PCs that constitute an essential component of your infrastructure or contain sensitive data. The way Safetica integration behaves on the PCs listed and outside the PCs is described above in the section Integration settings for specific applications.

To the PC to the list, click Add PC and mark in the dialog the PCs that you wish to add to the test group. Confirm your choice with OK.

Certificates

In this section you can add certificates which Safetica will use for ensuring that end users have seamless access to certain secured websites.

If an incorrect certificate for accessing such websites was assigned, a warning about this incorrect certificate would be displayed on the PC with client during the attempt to access the website.

All clients connected to server on which you assigned the certificates will download the certificates.

You can add the certificate by clicking *Add certificate* and choosing the corresponding certificate. The certificate format must be in base64 (Base-64 encoded x.509) format in the non-encrypted form. The following certificate suffixes will be accepted: *.crt, .cer* a *.pem*.

System paths

A system path exception can be set in the functions Files, File tagging, DLP protocol. In the default settings this applies particularly to folders in which operating system files, installed applications and temporary files of running applications are stored. The following are the main folders and subfolders:

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

You can add your own folders to these default folders. You can add a new path by clicking the Add path button and entering the path to the folder. All subfolders of the path entered will be considered as system folders.

Export of settings

Integration settings can be exported to PDF (PDF) or Excel (XLS) using the appropriate buttons in the top right corner of the view.

4.4.4.10 License management

License Manager is used for entering and checking licenses. Only the Safetica client is licensed and licenses are assigned to the end workstation where client is running. Without an assigned license, Safetica functions are not active on client workstations.

The License Manager can be found in the console under *Maintenance -> License management.*

Settings

Licenses are assigned for the server 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 the ✕ top right button.

Types of licenses

- *Normal* – standard purchased license. May have limited or unlimited validity in time.
- *Trial* – license designed for testing the product. The trial license is valid for a limited period, during which all Safetica components are fully functional .

Each license number contains information on its validity and the number of client, which can be activated with the license.

General Settings

Here you can enter a *Normal* or *Trial* license. The license number can be entered into the text box and then click *Insert to confirm.* Activation of end workstations with client will be automatic. After connecting to the server, client downloads a license and activates its functions.

Advanced settings

This section provides an overview of entered license numbers. For each license number in the overview, only the first five characters are displayed for security reasons. Furthermore, for each license number, it is shown how many end workstations with client may be activated and the time scope of the license.

In the bottom section, there is an overview of activated licenses on end workstations. An activated license on a computer with client is indicated by ☑. Number at the root item representing the server indicates the total number of activated licenses.

License expiration

On the expiry of the license, Safetica functions on the end workstations will be deactivated. To restore the functions, it is necessary to enter a new license.

Exceeding the limit of available licenses for client

After the number of terminal stations with client which can be activated using the entered license is exceed, a warning about exceeding the limit of activated licenses is displayed in the view. In this case, you must purchase a license which increases the number of end workstations with client to be activated.

4.4.4.11 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.

Settings

Settings overview can be found in the console under *Maintenance -> Settings overview.*

Settings overview is displayed for the server selected in the user tree.

On the right side above the table you will find several buttons allowing you to quickly add or remove columns representing functions of each module from the table:

- On the left side, there are buttons for user tree management in the table (☷ ≡ + −).
- *Hide all* – all columns in a table will be hidden*.*
- *Auditor* – display or hide columns representing the Auditor functions.
- *DLP* – show or hide columns representing DLP capabilities.
- *Supervisor* – show or hide columns representing the functions of the Supervisor module.
- *Others* – functions that do not fall into any Safetica modules.

The settings overview can be exported to an Excel table (XLS) or a PDF file (PDF) using the buttons in the top right of the view. .

4.4.4.12 Users activity

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

User activity can be displayed in the console under *Maintenance -> Users activity.*

User activity will be displayed for users, groups, computers or the server selected in the user tree.

Note: Records of activity on the end workstation are sent to the server when the PC is shut down. They are therefore not available immediately after a record is made.

View description

The data you can see in the visualization will be displayed only for users, PCs and groups that you have marked in the user tree. The view is divided into several sections.

The top section of the view offers a space where charts are shown. You can find the charts available for the current function on the list in the section to the right. To display them, click and drag them onto the chart area. Charts can be taken back to the list by clicking the button in the top right corner of each chart.

Charts available:

- *Most inactive PCs* – this chart shows the PCs (up to six) that were least used. The PC order in the chart corresponds to the inactivity time.

- *Least used PCs* – this chart shows the PCs (up to six) that were least used. The PC order in the chart is based on inactivity expressed in percent.
- *Most used PCs* – this chart shows the PCs (up to six) that were most used. The PC order in the chart is based on activity expressed in percent.
- *Highest total uptime PCs* – this chart shows the PCs (up to six) that were running for the longest time including their uptime.
- Most active PCs – this chart shows the PCs (up to six) that were most active. The PC order in the chart corresponds to the activity time.
- Lowest total uptime PCs – this chart shows the PCs (up to six) that were running for the lowest time including their uptime.

Note: Active time means the time that the user was really working with the PC. This time is identified based on the frequency of typing on the keyboard and moving the mouse.

In the middle 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*
- *Remote client* – name of the PC that is connected to a terminal server.
- *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 client is installed were used.

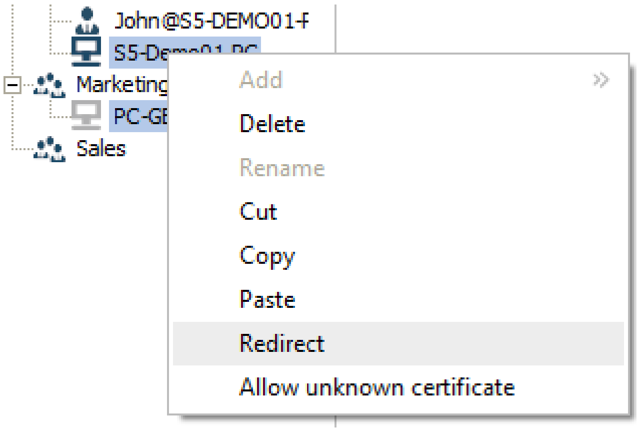
- *PC* – name of PC where the record was made
- *Total runtime* – total PC run time
- *Total inactivity* – time over which the PC was not used
- *Utilization ratio* – use of a PC for an activity, in percent (user was working on the PC)

4.4.4.13 Redirecting client to another server

Sometimes, for various reasons (server change, upgrade, change in network architecture), it can happen that the existing server will not be available for the Safetica client under the same address. Before making any such change, the existing client can be forwarded to another server and address.

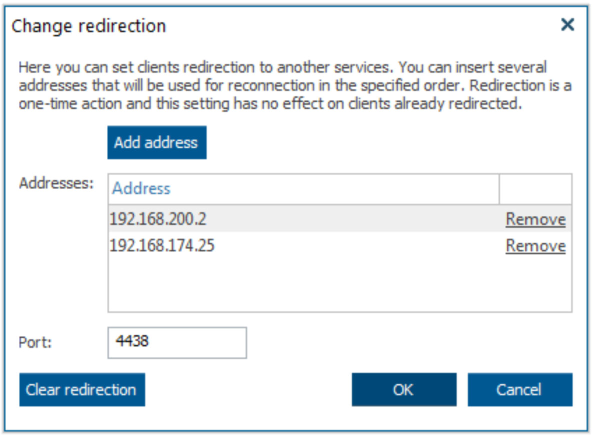
You can change the server address for the various clients as follows:

1. Mark the PCs in the user tree for which you want to enter a new server address.



2. Right-click on them and select *Redirect*. A redirection dialog will appear.

3. Use the *Add address* button to enter new addresses of the server in the list. You can enter more than one address. Client will then connect to the first server available. Connection attempts will be carried out based on the address order from the first address in the list to the last. Enter the port which client uses for server connection under the address list. If you have not changed the port, leave it as the default one. Confirm the dialog with OK.



Change redirection

Here you can set clients redirection to another services. You can insert several addresses that will be used for reconnection in the specified order. Redirection is a one-time action and this setting has no effect on clients already redirected.

Addresses:

Address	
192.168.200.2	Remove
192.168.174.25	Remove

Port: 4438

4. When confirmed, a red arrow will appear next to the PCs forwarded in console. After updating the settings, client will connect to a new server instance. When successfully redirected, the arrow next to the PCs turns green. When the new addresses have been downloaded, client will no longer be available via the original server. Administration of the SECs forwarded is done via the new server.

You can cancel the redirection before client downloads new addresses by clicking with the right button on *Cancel redirection*.

Client redirection is in the user tree represented as follows:

- 🖥 – redirection has been set.
- 🖥 – redirection completed.

4.4.4.14 Protection against unauthorized manipulation with Safetica client

Because Safetica 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 client off. Client is also protected against intervention by a user with administrator rights.

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

What is being protected?

- *Registries* – it is not possible change records in registries concerning the client, including the server IP address.
- *Processes* – all 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 client installation folder
- *Database files* – these cannot be moved, renamed, or deleted. The contents of databases are encrypted.
- *Uninstallation* – client is protected from uninstallation.
- *Tags* – file symbols (tags) are protected against rewriting or changes.

Uninstall and update permission from console

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 client component on end stations.

Permitting the uninstalling, updating, and turning off client service from endpoint

Permission for these tasks can also be granted directly from the end station on which the client is installed. You must first generate a password for selected users in the console (*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 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 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 client:

STCService -allow uninstall

To permit updating the 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.

4.4.5 Profile

This section gives a basic overview of setting up your account, with which you are connected to the server.

Access your profile using *Console -> Profile.*

Accounts for connection to server can be created and managed in the *Console -> Maintenance -> Access management* section*.*

User information

The user name under which you are connected to server is displayed here. You can change the password for this account or log off. After logout, a dialog for logging on to server opens.

The language of the console can also be changed here. Use the slider to change the format of time displayed in the different console views. You can choose from two time format types:

- *Based on selected console language*.
- *Based on the settings of the system on which console is running.*

Connection to server

This section contains the server to which you are logged in with the above account.

Connecting to server

To connect to a new server, click *Add server.* In the dialog box, enter the server address and port to connect the console (default is 4441) and confirm.

Adjusting server settings

For connected server, you can change the main settings by clicking on the appropriate button at the relevant server. You can specify the database connection, SMTP name, sync with AD, etc. For more details, see *Server settings*.

The server to which you are logged in can be removed by clicking on the appropriate link at the relevant server.

Local settings

In this section you will find basic information on console such as the manufacturer, its website and release number.

You can use the slider to specify whether console should be launched after system start.

Use the *Use proxy server* slider to specify whether console should use a proxy server during an update. Proxy server settings will be copied from the Windows settings of the user under which you are currently running console.

Confirm the changes with ✓.

Note: Since Safetica version 6, each user’s reports are stored on the server. They are available to the user after their login from any console.

4.4.5.1 Server settings

Here you can manage the basic settings of the appropriate Safetica server.

Connecting to the server can be managed in the *Profile section of the console.*

All changes must be saved using the ✓ button in the upper right corner of the view.

Version and name

Here you can view the server version number or set the server name that will appear in the user tree.

Setting up the database connection

Here you can configure the Safetica server and Safetica client connection to central databases.

Note: If you have direct access to the database set for Safetica clients in the Client settings, the server and the clients must have access to the database through at least one address provided in the list. If the connection is set via the server, the database must be accessible only from the server.

By clicking the *Add* button, you can add addresses of the MS SQL server to the *Server addresses list*. This includes addresses at which Safetica databases will be accessible from the workstation and the server. Client and server will try the addresses one by one until a connection to the database is successfully established. You can click *Remove* to remove an address from the list.

In the middle section you will find settings for connection to MS SQL databases.

- *Username* - user name used to access the database from server.

  Note: The Microsoft SQL server user must set the authentication mode to SQL login (SQL Server Authentication) *and/or* Mixed mode. *The Microsoft SQL Server instance must also have this authentication type permitted.*

- *Password* – user password used for access to the database from server.

- *User has highest privileges* – use the scrollbar to specify whether the above mentioned account shall have the highest rights for database access (*sysadmin*). Some Safetica functions cannot be used if an account lacks the highest rights:

  - The same account as that for server connection will be used for client connection to the central database without the highest rights set.

  - Also, archive connection in *Database management will not be available*.

- o If the database account does not have the highest-level privileges, then at least the *db-creator* role is necessary for Safetica to be able to create its databases. If the account does not have this role, empty databases will have to be made and set up on the SQL server. The names of these databases must correspond with the database name entered in the advanced settings (see *Database name prefix* below).

  When using the account with the highest right, an account with limited access to the central database will be automatically created for client for the sake of higher security.

You can check the correctness of the data entered and ensure that the server successfully connects to MS SQL by clicking *Connection test*.

Caution: In the Safetica 5.4.0 release changes were made to the way the user works with databases. After updating from a lower version, you will have to rename the databases in some cases, so that they correspond to the formátu prefix_main, prefix_data, prefix_category format. Now, all three Safetica databases must run within a single database instance. Contact the technical support if you need help with setting the changes.

Advanced

In advanced database connection settings you can specify these items:

- *Instance name* – name of MS SQL server instance. MSSQLSERVER will be used if not entered.
- *Port* – the number of the port on which the MS SQL instance is running. The default port is 1433. If not entered, the dynamic port will be used.
- *Database names prefix* – name of the prefix for all Safetica databases. For example, if the *st* prefix is entered, the database names will be as follows: *st_main, st_data, st_category*. If you leave the box blank, the prefix *safetica will be used.*
- *Client account password* – password to the account used by client for database access. If server uses a user account with the highest rights (*sysadmin*) for connection to the central database, an account with lower rights will be automatically created in the database. Client will use this account for connection to the central database. In this case you can reset the password to this account. To do the reset, click *Reset password.* When resetting the password , a new password will be automatically generated and sent to all SECs connected to server. SECs will use this new password for connection to the central Safetica database.

Caution: Some items in the settings database are synchronized with record databases. Specifically, this includes the following items:

- *User tree*
- *Safetica users*
- *List of external devices*
- *Data categories*
- *Security keys*

If you delete any of the items specified above from the settings database, related information will also be deleted from the records database.

Examples:

- *If you delete a user in the user tree, all records related to this user will be deleted from the records database.*
- *If you replace the entire settings database with a new (empty) database, all records will be deleted from the records database.*

We strongly recommend creating back-ups in Database management prior to every operation with *the database settings or database records.*

Active Directory

Right at the bottom, you can click *Add* to import Active Directory roots into the management of the configured server. After the confirmation of a dialogue, all domain users and all computers will be loaded into the user tree (they will be added to the tree for the server you are configuring) from the roots added this way. These users and computers will be placed into the group designated for synchronization with the Active Directory (*AD*), from which you can copy them into your groups. For more information, see *Working with setting modes and visualization*.

Use the *Synchronize now* button to force an update of users and computers from the Active Directory to the user tree.

SMTP server (outgoing mail server)

Here you can set the outgoing mail server (SMTP server), which is used for sending e-mail messages – reports or alerts.

You can verify that the entered data is correct and the connection with the SMTP server is functioning properly by pressing *Test connection.* A test message will be sent to the specified e-mail from server.

Setting a proxy

Here you can set the proxy server for the selected server. The server will use the proxy server to download updates from the web.

Use the slider to set whether a proxy server shall be used.

Use the *Copy system proxy button* to copy the proxy server settings from the Windows settings of the user under which you are currently running the console.

You can also enter the proxy server address and port manually.,

Other settings

In this section, it is possible to set the debugging logs – Errors, Debug and Verbose. Only for Safetica system administrators and technical support. Start can adversely affect the performance of the client station.

4.5 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.

4.5.1 Functions settings

In this view you can activate individual Auditor functions.

Type of settings

You can use the scroll bar to specify how the functions shall behave:

- *Enable* – the function is not active.
- *Inherit* – the function is not set. The settings are inherited from the parent group.
- *Disable* – the function is active.

The settings will be applied only to 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.

You can set these functions here:

- *Applications* – application monitoring on workstation.
- *Web sites* – web browsing monitoring on the workstation.
- *E-mails* – e-mail communication monitoring on the workstation.
- *Print* – print monitoring on the workstation.
- *Files* – file handling monitoring on the workstation.
- *Devices* – records the connection and disconnection of peripheral USB storage devices (flash disks, external drives, etc.) on the workstation.
- *Network traffic* - this function is used to record the volume of data sent or received on the workstation.
- *Trends* - uses data recorded by Websites and Applications functions. For proper functioning of Trends, these two functions must be ON (enabled).

After enabling the function and clicking on the Show advanced settings button, some additional settings which you can define will be displayed in the Files.

Files function advanced settings

This function records the creation, opening and deletion of files in local paths or external storage sites on the workstation. After clicking the Add extension button, you can add file extensions to the list. File operations will be recorded only for files that have an extension on the list.

Using other controls, you can further specify recording:

- *Log local file operations* – here you can allow or disallow the recording of file operations on local disks of the workstation.
- *Log only specified extensions only* – here you can set the recording of only the files with l?sted extensions. You can edit the list of extensions. The filter by file extensions is not applied for FTP transfers, downloading and uploading. Everything will be recorded for these types of operations.

  Note: System paths include the following:

  o *C:\ProgramData*

  o *C:\Windows*

  o *C:\Program Files*

  o *C:\Program Files (x86)*

  o *C:\Users\<User name>\AppData*

4.5.2 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*

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

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.
    - *Active time* – the time when the application is in the foreground and the user actively uses the application application (mouse, keyboard). Fast switching between other application windows (within three seconds) is not recorded as active time spent on the website. Also a screensaver running under the user is not recorded as active time.
    - *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).

  Note: In client settings you can change the time after which – if the user is inactive – active time changes into inactive time.
- *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.
- *Change category* – after clicking the link with this name, a dialog for changing the application category will open in this column. Select one or more new categories in the dialog and confirm your changes with Select.

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.

4.5.3 Devices

In this visualization you will find records of user access to external devices.

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

Visualization

There are following charts in the visualization mode:

- *Top users* – the chart shows users who work with external devices most of all users (the chart shows up to seven most active users).
- *Most used devices types* – the chart shows the most used types of external devices.
- *Top actions* – this chart shows a ratio of tasks performed.

Each record contains several types of information represented by columns:

- *Date and time* – date and time of record creation.
- *PC* – name of the computer where the record was made.
- *Username* – name of the user under which the record was made.
- *Description* – detailed device description.
- *Action* – shows if the device was Connected or Disconnected.
- *Unit* – to what unit (letter) the device is mapped.
- *Device identification* – numbers identifying the device <producer's ID>-<ID of product series>-<serial number>

- *Vendor* – vendor's ID.
- *Device type*
- *Interface type* – the type of interface concerned: USB, Bluetooth, FireWire, IrDA, LPT, COM.
- *Application* – which application the task was performed in.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.5.4 Web sites

Check the pages your employees are viewing during the working hours. Safetica provides the managers with clear statistics of the most visited pages and the time spent viewing them. The pages are classified according to category, number of openings and the level of productivity. No matter what browser the employees use – the auditor can process data from them all. It can even analyse encrypted HTTPS connection.

Website monitoring can be found in the module *Auditor -> Websites.*

Settings

In the tab *Auditor -> Functions settings* you can turn this feature off or on.

Visualization

There are following charts in the visualization mode:

- *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).
- *Web sites access* – a chart containing total time spent on the web.

Each record contains several types of information represented by 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 on a website (working in the browser). Fast switching between other application windows and the web browser (within three seconds) is not recorded as active time spent on the website.The screensaver running under the user is not recorded as active time.
- *Protocol* – type of internet protocol: *http, https.*
- *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).
- *Change category* – after clicking the link bearing the same name in this column, a dialog will open for changing the website category. Select one or two new categories in the dialog and confirm the change with *Select*.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.5.5 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.

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

Visualization

There are following charts in the visualization mode:

- *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.

Each record contains several types of information represented by 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 learn more about the visualization interface in the chapter *Visualization mode*.

4.5.6 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*

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

Visualization

There are following charts in the visualization mode:

- *Top downloads per user* – this chart includes users with the highest amount of received data (up to seven users).
- *Top uploads per user* – this chart includes users with the highest amount of sent data (up to seven users).
- *Top downloads per applications* – the chart shows applications with the highest volume of data received.
- *Top uploads per applications* – the chart shows applications with the highest volume of data sent.
- *Top downloads per application categories* – the chart shows application categories with the highest volume of data received.
- *Top uploads per application categories* – the chart shows application categories with the highest volume of data sent.
- *Network traffic history* – this chart summarizes sent and received data.

Each record contains several types of information represented by columns:

- *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 client is installed were used.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.5.7 Trends

Trends are used for profiling and tracking user productivity in applications and on websites. It offers clearly organized outputs and immediate alerts when limits are exceeded, which can be used to get the overview of possible personal and security issues in advance. User profiling and behavior monitoring takes place automatically when the Trends function is enabled.

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

Settings

For proper functioning of Trends, Web sites and Applications functions must be enabled in *Auditor -> Functions setting*.

Active time means the time that the user was really working with the PC. This time is identified based on the frequency of typing on the keyboard and moving the mouse.

Visualization

Charts show the summary of user activities and change in user activity in selected application and website categories. The charts show information for selected periods, users and groups.

Activity (active time) means the time of active work with the application or website that was on the foreground and the user was working or doing any activity with the application or website (typing on the keyboard, moving the mouse).

You will find two chart types in this view:

- *The most active users* - chart containing the values of active time spent by the users in a given category. Values are calculated from records obtained from all days containing any data in the selected time range. The blue colour in the chart shows the average category activity. This value is also indicated below the chart.

- *Top activity changes* – the average active time spent in the corresponding category during the basic period is benchmarked against the average active time spent in this category during the current period. The difference between these two values is shown in the chart as the percentage increase (positive values) or decrease (negative values). The order of the values in the chart corresponds to their absolute values – from the highest to the lowest. In front of the chart you can find average values for the corresponding category along with the number of days for a specific period.

  - *Base period* – period against which the current period is benchmarked. This involves the first two thirds of selected time range. Example: the basic period is the first eight days for the 12-day range selected (the figure can be sometimes rounded up or down, so the actual number of days can differ slightly).

    Caution: The basic period must contain at least three days on which the data was being collected for the respective category and user. Otherwise, the data will not be displayed due to possible inaccuracy.

  - *Current period* – this is the period benchmarked against the basic period. It covers the last third of the time range selected. Example: the current period is the last four days for the 12-day range selected (the figure can be sometimes rounded up or down, so the actual number of days can differ slightly).

    Caution: The current period must contain at least three days on which the data was being collected for the respective category and user. Otherwise, the data will not be displayed due to possible inaccuracy.

You can find the charts available for trends in the right section of the list. To display them, click and drag on the chart area. Charts are taken back to the list by clicking the ✕ button in the top right corner of each chart.

Note: When evaluating the information displayed, consider the period and average time of recorded activity in the corresponding category for that period. Example: the average hourly activity on one day has different significance than average activity of the same length recorded over one entire month.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.5.8 E-mails

Do your employees communicate actively with competitors or do they forward dozens of chain e-mails with funny pictures? Find out what kind of e-mails they keep sending during working hours. If suspicion arises, responsible managers can obtain detailed information about the e-mail communication of their employees. And that includes attachments that might contain sensitive information.

For e-mail monitoring, see *Auditor* -> *E-mails.*

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

Visualization

There are following charts in the visualization mode:

- *Sent/received e-mails* – number of sent and received e-mails over time.
- *Sent/received e-mails with attachments* – number of sent and received e-mails over time with an attachment.
- *Top recipients* – a chart showing users who received the highest number of e-mails.
- *Top senders* – a chart showing users who sent the highest number of e-mails.
- *Top recipients – e-mail addresses* – a chart showing the proportion of e-mail addresses receiving the highest number of e-mails.
- *Top senders – e-mail addresses*– a chart showing the proportion of e-mail addresses sending the highest number of e-mails.
- *Top recipients – domains* – a chart showing the proportion of e-mail domains receiving the highest number of e-mails.
- *Top senders – domains* – a chart showing the proportion of e-mail domains sending the highest number of e-mails.

Each record contains several types of information represented by columns:

- *Date and time* – date and time of record creation.
- *PC* – name of the computer where the record was made.
- *Username* –- name of the user under which the record was made.
- *From* – e-mail address of the sender. In the event that e-mail address is not detected, this field is left blank.
- *Recipient* – e-mail address of the addressee. In the event that e-mail address is not detected, this field is left blank.
- *Subject* – subject of the recorded e-mail.
- *Contains attachments*
- *Files* – names of any e-mail attachments.
- *Sent/Received* – information on whether the recorded e-mail was received or sent.
- *Sender – Domain* – e-mail domain of the sender.

- *Recipient – Domain* – e-mail domain of the recipient.
- *Size* – message size.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.5.9 Files

This function is used to record file operations on workstations. When activated, you will see what the user is doing with files on the workstation. The function tracks information on:

- Copying a file
- Moving (includes renaming a file)
- Creating a file
- Deleting a file
- Opening a file (optional)
- Web download

  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.

- Web upload
- FTP file transfer

Settings

In the tab *Auditor* -> *Functions settings* you can turn this feature off or on.

Main settings

File operations on external devices and in network locations are recorded automatically. In the main settings you can specify where file operations shall be recorded.

- *Log local file operations* – here you can allow or disallow the recording of file operations on local disks of the workstation.
- *Log open file operation* – here you can specify whether the file opening operation shall be recorded. This applies to all file locations (local, external disk or network storage).

Note: Logging operations on local disks and file opening operations can dramatically increase the amount of recorded data.

Filtering according to extensions

In this section you can specify through a suffix list which files shall be subject to file operation monitoring. You can specify file extension-based filtering with the help of the following settings:

- *Use extension filter on local paths only* – here you can set the suffix filter only for operations with files located on local drives.
- *Filtering according to extensions* – here you specify how the suffix list shall be used in the settings.

  o *Disabled* – filtering based on the suffix list will be deactivated.

  o *Inherit* – nothing is set; the settings are inherited from the higher-level group.

  o *Deny list* – only operations with files with their suffix not listed will be recorded.

- o *Allow list* – only operations with files with their suffix listed will be recorded.

You can add extensions to the list with the *Add extension* button. You can enter the extension directly or choose it with the help of the extension category. You can open the extension categories database by clicking the button with three dots (...).

Filtering according to paths

In this section you can specify through a path list which locations shall be subject to file operation monitoring. You can specify path-based filtering with the help of the following settings:

- *Include system paths in logging* – here you can set the suffix filter only for operations with files located on local drives.

Note: System path are for example::

- o *C:\ProgramData*
- o *C:\Windows*
- o *C:\Program Files*
- o *C:\Program Files (x86)*
- o *C:\Users\<UserName>\AppData*

- *Filtering according to paths* – here you specify how the path list shall be used in the settings.
  - o *Disabled* – filtering based on the path list will be deactivated.
  - o *Inherit* – nothing is set; the settings are inherited from the higher-level group.
  - o *Deny list* – only operations with files not in the listed folder will be recorded.
  - o *Allow list* – only operations with files in the listed folder will be recorded.

Note: Path-based filtering is superior to other types of filtering. Therefore, for example, the list of allowed paths defines locations in which all operations are monitored. Other locations will be monitored based on the settings of other filters. The list of disallowed paths defines locations not to be monitored at all.

You can add paths to the list by clicking the *Add path* button and entering the path to the folder.

Visualization

There are following charts in the visualization mode:

- *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.

Each record contains several types of information represented by 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* – type of source path:
  - Local path
  - USB
  - Network path
  - FTP
  - CD/DVD
  - Other external
  - Remote transfer – file transfer using Remote Desktop Services from Microsoft
  - Cloud drive – a local cloud drive folder. Supported cloud drives are: *Google Drive, OneDrive, Dropbox, Box sync.*
  - Web
- *Target type* – type of target path:
  - Local path
  - USB
  - Network path
  - FTP
  - CD/DVD
  - Other external
  - Remote transfer – file transfer using Remote Desktop Services from Microsoft
  - Cloud drive – a local cloud drive folder. Supported cloud drives are: *Google Drive, OneDrive, Dropbox, Box sync.*
  - Web
- *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. After clicking the name, detailed information on the device will be displayed. Here you can specify what zones the device shall belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- *Target device* – device name and SID. After clicking the name, detailed information on the device will be displayed. Here you can specify what zones the device shall belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- File – name of the file. If you make a group, create an order or filter by using this column, the file name will be taken from the *Source* column. If the source is empty, the file name will be taken from the *Destination* column.
- *File size*
- *Extension* – the file extension. If you make a group, create an order or filter by using this

column, the file extension will be taken from the *Source* column. If the source is empty, the file extension will be taken from the *Destination* column.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.6 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.

4.6.1 File tagging

With the file tagging feature, you can search and tag files with the corresponding data category on PCs with the Safetica client. You can secure files tagged this way by applying DLP rules.

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

The function is available in *Console -> DLP -> File tagging*.

Settings

The left section shows a list of data categories. After clicking on the Manage data categories button, you can create, modify or delete data categories

Rules for the selected data category are shown on the right. Based on the rules, the files corresponding to them will be tagged with the selected data category or the tagging changes. Every file can be tagged with several data categories at once.

There are several kinds of rules to be used for searching and tagging files:

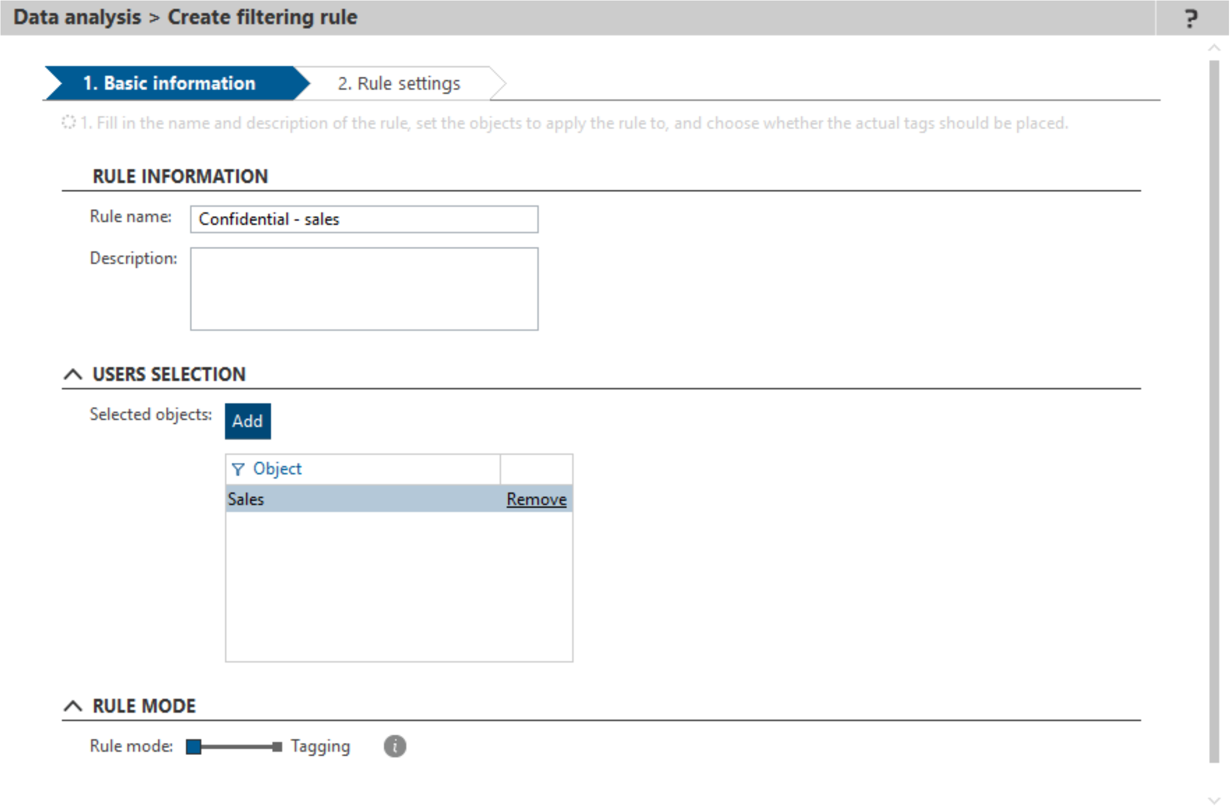
Application rules

Application rules are used to determine applications and application categories in which the output files are to be tagged with the selected data category.

For example, a setting can be made where all applications in the CAD software category tag files with the relevant data category so that the relevant limitations are subsequently applied to the files concerned.

Creating an application rule for a selected data category:

1. Select the relevant data category in the list of data categories and click on the *Add* button in the Application rules section. A wizard for adding an application rule will appear.
2. Enter the following in the first step:
    - Name and description of the rule.
    - Select users, computers or groups from the user tree to which the application rule for tagging output files will apply.
    - Rule mode:
        - *Testing* – files will not be tagged. Records will be generated only on files that correspond to the rule. In Visualization, you can check whether the right files would be tagged. You can later switch the rule to the Tagging mode.
        - *Tagging* – files that correspond to the rule will be tagged with the selected data category.



Data analysis > Create filtering rule

1. Basic information | 2. Rule settings

1. Fill in the name and description of the rule, set the objects to apply the rule to, and choose whether the actual tags should be placed.

RULE INFORMATION

Rule name: Confidential - sales

Description:

USERS SELECTION

Selected objects: Add

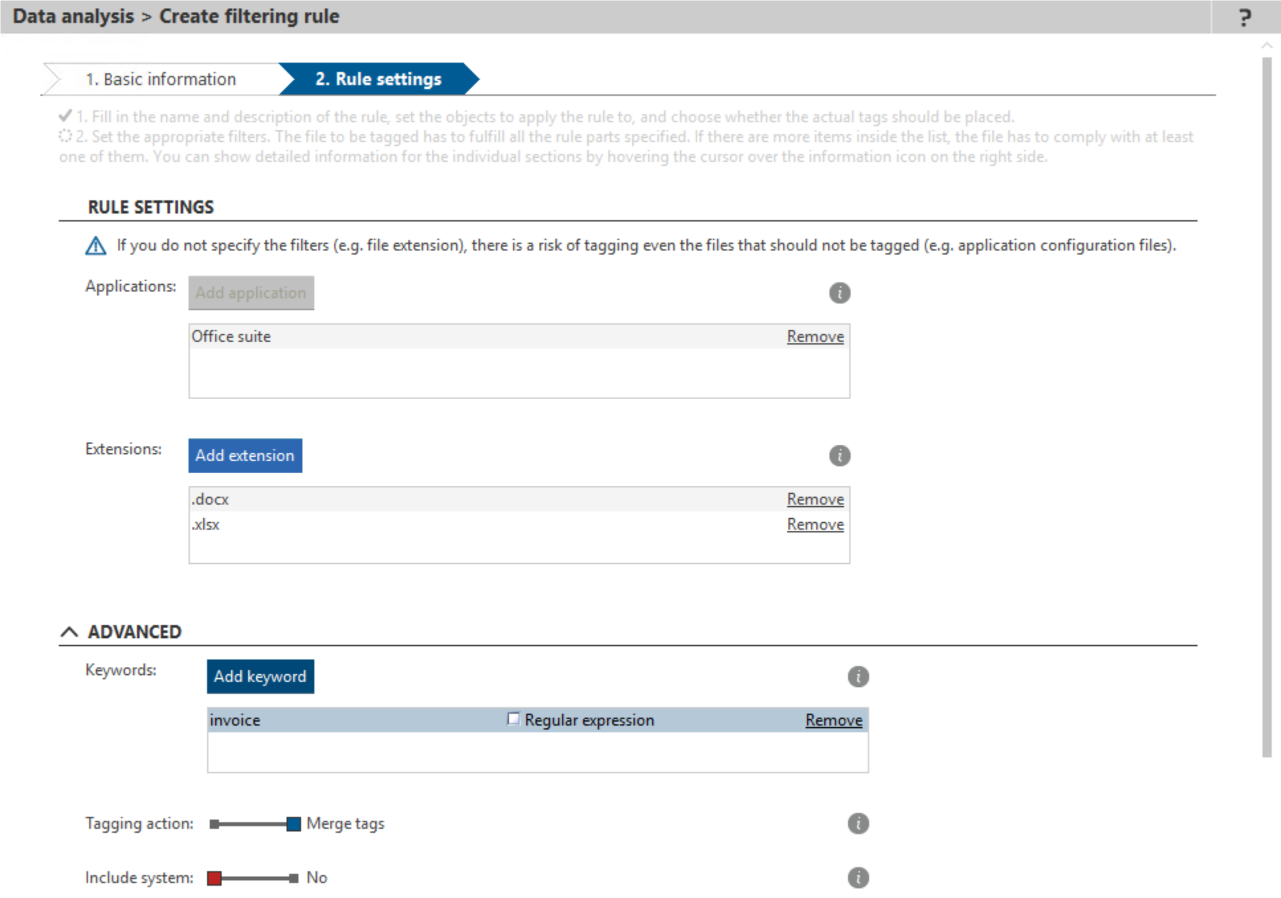
Object	
Sales	Remove

RULE MODE

Rule mode: Tagging

3. In the second step:
   - *Applications* – select application category. Output files from applications in the selected application categories will be tagged with the data category.
   - *Extensions* – enter extensions into the list or select extension category. Files with extensions indicated in the list or contained in the selected extension category will be tagged.
   - Advanced:
     - *Keywords* – enter keywords into the lists. Files that contain at least one of the defined keywords in the filename will be tagged. Even a regular expression can be used as a keyword (see http://www.cplusplus.com/reference/regex/ECMAScript)
     - *Tagging action*:
       - *Merge tags* – sets tagging with the selected data category for the file. If the file is already tagged, the new tagging is merged with the existing ones and the file is tagged with several data categories.
       - *Replace tags* – replaces all existing file tags with a new tagging. The file will be tagged only with the new data category. Use this option carefully.
     - Include system – with this option, you can activate tagging of system files. In Integration settings, custom paths can be added to system files. Use this option carefully and only in justified cases.

   Files to which all parts of the rule apply will be tagged. Not all parts of the rule need to be entered. It is sufficient to complete at least one part. If a part is not completed, it will apply to all parts.



Data analysis > Create filtering rule

1. Basic information 2. Rule settings

✓ 1. Fill in the name and description of the rule, set the objects to apply the rule to, and choose whether the actual tags should be placed.

2. Set the appropriate filters. The file to be tagged has to fulfill all the rule parts specified. If there are more items inside the list, the file has to comply with at least one of them. You can show detailed information for the individual sections by hovering the cursor over the information icon on the right side.

RULE SETTINGS

⚠ If you do not specify the filters (e.g. file extension), there is a risk of tagging even the files that should not be tagged (e.g. application configuration files).

Applications: Add application

Office suite	Remove

Extensions: Add extension

.docx	Remove
.xlsx	Remove

ADVANCED

Keywords: Add keyword

invoice	□ Regular expression	Remove

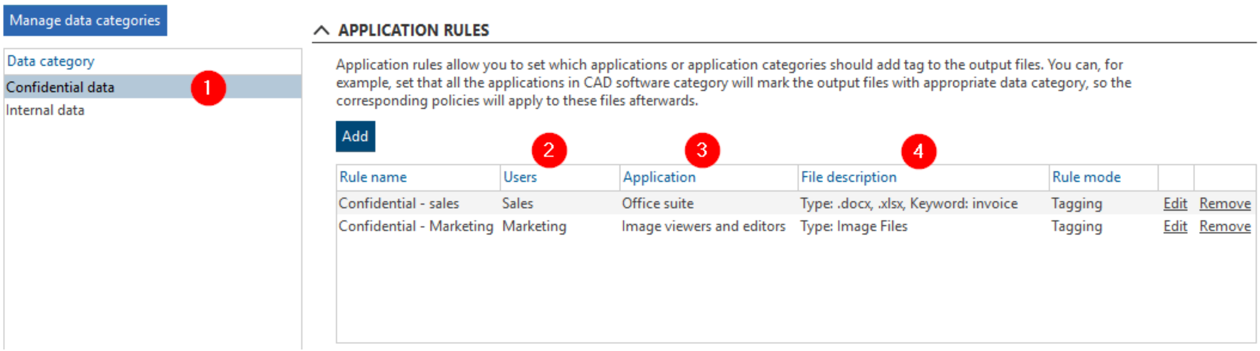
Tagging action: Merge tags

Include system: No

4. Click on *Finish* to confirm rule generation

Example of application rules for Confidential data:

- *If users from the Sales group (2) save into a location a file with the .xlsx or .docx extension (4) with the word “invoice” (4) in the filename from an application in the Office suite application category (3), the file will be tagged with the data category Confidential data (1).*
- *If users from the Marketing group (2) save into a location a file with an extension from the Image files category (4) from an application in the Image viewers and editors application category (3), the file will be tagged with the data category Confidential data (1).*



Manage data categories

Data category
Confidential data
Internal data

APPLICATION RULES

Application rules allow you to set which applications or application categories should add tag to the output files. You can, for example, set that all the applications in CAD software category will mark the output files with appropriate data category, so the corresponding policies will apply to these files afterwards.

Add

Rule name	Users	Application	File description	Rule mode		
Confidential - sales	Sales	Office suite	Type: .docx, .xlsx, Keyword: invoice	Tagging	Edit	Remove
Confidential - Marketing	Marketing	Image viewers and editors	Type: Image Files	Tagging	Edit	Remove

Web rules

Web rules can be used to set tagging of files downloaded from defined domains or domains included in a selected web category.

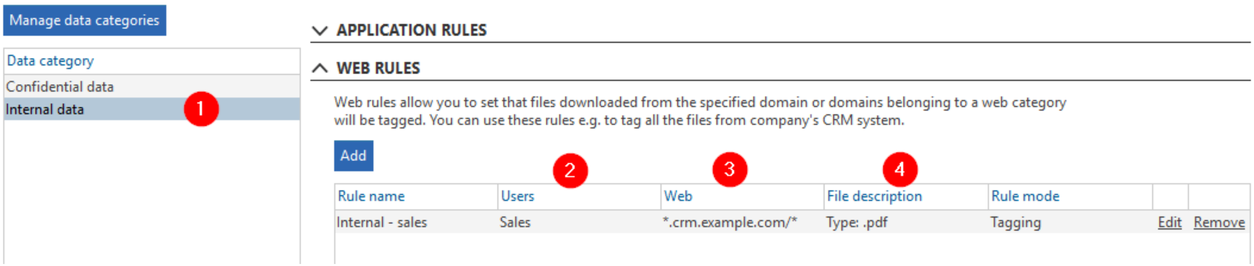
This type of rule can be used, for example, to tag all files downloaded from the corporate CRM system.

A wizard for adding a web rule will appear after clicking on the Add button.

Generating a web rule is analogous to generating an application rule. The only difference is the second step where there is a list of web addresses instead of the list of applications. Only files that were downloaded from such addresses and correspond to the other parts of the rule (extensions, keywords, etc.) will be tagged.

Example of a web rule for Internal data:

- *If users from the Sales group (2) save into a location a file with the .pdf extension (4) from the crm.example.com (3) website, the file will be tagged with the data category Internal data (1).*



Data category
Confidential data
Internal data

APPLICATION RULES

WEB RULES

Web rules allow you to set that files downloaded from the specified domain or domains belonging to a web category will be tagged. You can use these rules e.g. to tag all the files from company's CRM system.

Rule name	Users	Web	File description	Rule mode		
Internal - sales	Sales	*.crm.example.com/*	Type: .pdf	Tagging	Edit	Remove

Location rules

Location rules can be used to select folders whose content is to be tagged. All files placed in these files will be tagged automatically. In addition, it is possible to set a repetitive task that will tag data in selected folders in regular intervals, tagging also files placed in these folders from computers not protected by Safetica.

A wizard for adding a location rule will appear after clicking on the Add button.

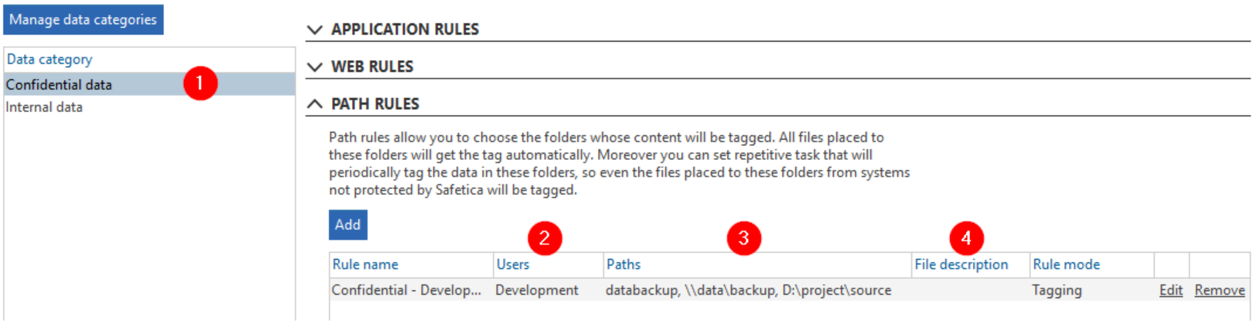
Generating a location rule is analogous to generating an application rule. The only difference is the second step where there is a list of paths to folders instead of a list of applications. Only files that are or will be located in these folders and all their sub-folders and correspond to the other parts of the rule (extensions, keywords, etc.) will be tagged.

In addition, it is possible to activate here the task for repeated tagging of files corresponding to the rules. This ensures that the files in the selected location are tagged even if they were placed in this location using a computer not protected by Safetica.

For a repeating task, you can specify the user for whom the tagging will be made (e.g. for the purposes of access privileges).

Example of a location rule for data category Confidential data:

- *If users from the Development group (2) place any files (4) in the folders (including subfolders) \\ data \ backup or D:\project\source (3), the file will be tagged with data category Confidential data (1).*



Data category
Confidential data
Internal data

APPLICATION RULES

WEB RULES

PATH RULES

Path rules allow you to choose the folders whose content will be tagged. All files placed to these folders will get the tag automatically. Moreover you can set repetitive task that will periodically tag the data in these folders, so even the files placed to these folders from systems not protected by Safetica will be tagged.

Rule name	Users	Paths	File description	Rule mode		
Confidential - Develop...	Development	databackup, \\data\backup, D:\project\source		Tagging	Edit	Remove

Tag distribution rules

Tag distribution rules can be used for a setting ensuring that when a file tagged with a selected category is open in an application, the tagging will be distributed also to the outputs from that application.

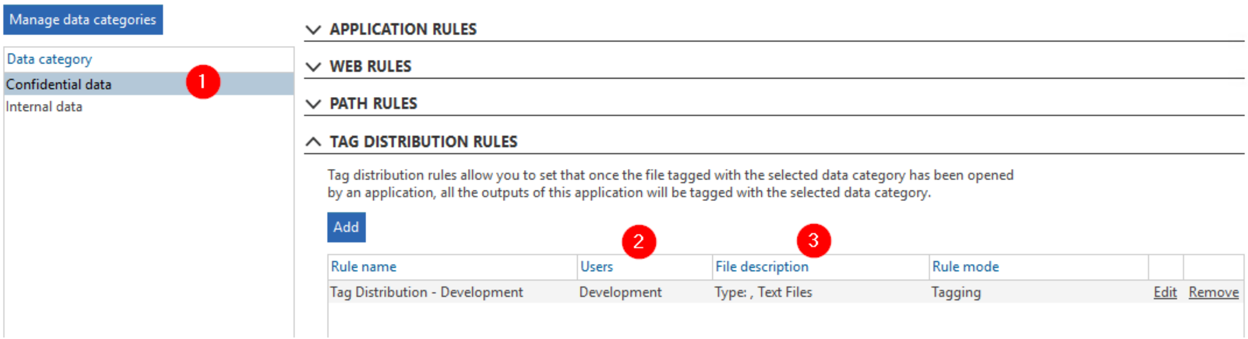
Note: Regardless of this rule, tagging is always distributed to files saved from an application via the *standard saving dialogue (Save as). A tag distribution rule covers other non-standard outputs from the application. For example, export to another format, etc.*

A wizard for adding a tag distribution rule will appear after clicking on the Add button.

Generating a tag distribution rule is analogous to generating an application rule. The only difference is in the second step where there is not a list of application. The rule applies to all applications where a file tagged with the selected data category is open. The tagging will be distributed only to those files whose extension is contained in the list and which correspond to the other parts of the rule such as keywords.

Example of a tag distribution rule for the data category Confidential data:

- *If users from the Development group (2) open a file tagged with the data category Confidential data (1) in an application, all output text files (3) from the application will be tagged with the same data category Confidential data (1).*



Tag distribution rules allow you to set that once the file tagged with the selected data category has been opened by an application, all the outputs of this application will be tagged with the selected data category.

Rule name	Users	File description	Rule mode		
Tag Distribution - Development	Development	Type: , Text Files	Tagging	Edit	Remove

Process rules

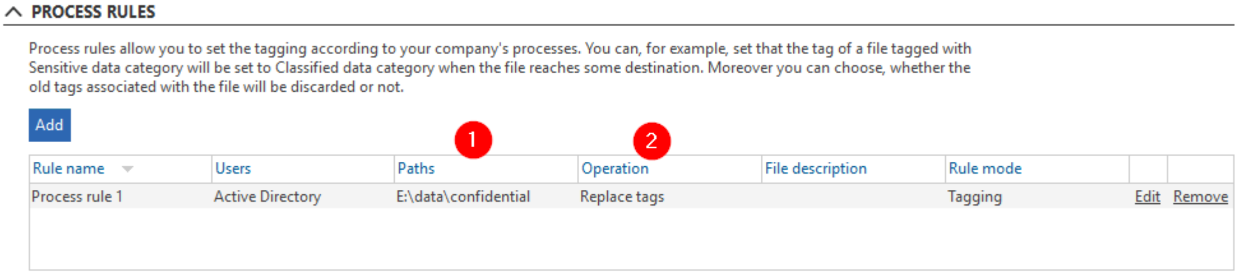
Process rules can be used to set the tagging of files in accordance with corporate processes. For example, you can use a setting in which files tagged with the Internal data category are set to the Confidential data category whenever they are moved to a location. In addition, it is possible to decide whether the tagging originally assigned to the file should be removed.

A wizard for adding a process rule will appear after clicking on the Add button.

Generating a process rule is analogous to generating a location rule. The only difference is in the second step. In section Original data category, select data category and specify for it, in section Tagging operations, what should be done with the selected data category:

- *Replace tags* – tag replacement is done for files that correspond to all parts of the rule. Simultaneously, at least one of the existing file tagging must be the data category selected by you in section Original data category. In replacement, all potential tagging (data categories) of the relevant files will be replaced by a data category selected in the following list.
- *Replace original tag and merge with others* – for files corresponding to the rule, the data category you selected in section Original data category will be replaced with the data category selected in the following list. Simultaneously, the new tagging will be merged with the other data categories by which the files can be tagged.
- *Remove tag* – the tagging selected by you in section Original data category will be removed for files corresponding to the relevant rule. Other tagging of the file will be preserved.

Example: A file is tagged with data categories Confidential and Internal. The file will be placed in folder E:\data\confidential (1), for which a process rule has been created. Data category Confidential is selected in section Original data category. The Replace tags (2) option is set as the tagging operation and the Confidential category is selected in the list. The file will be tagged with the only data category, Confidential, after being placed in folder E:\data\confidential.



PROCESS RULES

Process rules allow you to set the tagging according to your company's processes. You can, for example, set that the tag of a file tagged with Sensitive data category will be set to Classified data category when the file reaches some destination. Moreover you can choose, whether the old tags associated with the file will be discarded or not.

Add

Rule name	Users	Paths	Operation	File description	Rule mode		
Process rule 1	Active Directory	E:\data\confidential	Replace tags		Tagging	Edit	Remove

Tagging removal rules

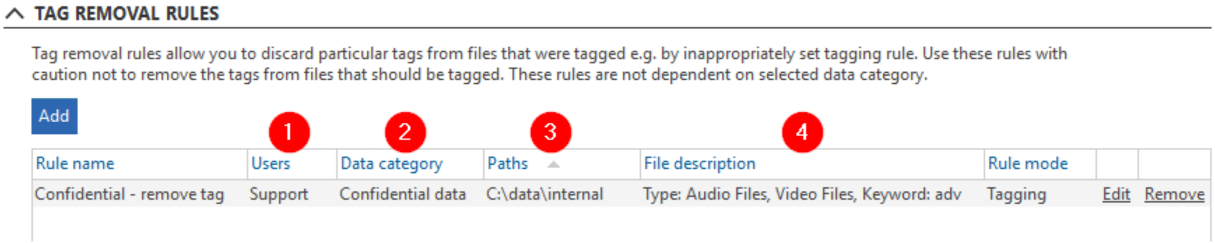
The tagging removal rules are used for removing tagging from files that were tagged by accident (e.g. due to a wrongly set rule). Use these rules carefully to avoid removing tags from files that should be tagged. These rules are not dependent on the category selected.

A wizard for removing tagging will appear after clicking on the Add button.

Generating a tagging removal rule is analogous to generating a location rule. The only difference is that the data category tagging is removed from files corresponding to the rules. You can also select in the second step whether you want to remove all tagging or select in the list a data category to be removed from the files.

Example of a rule for removing tagging:

- *If users from the Support group (1) save Audio and Video files with the “adv” string in the filename (4) into the C:\data\internal (3) folder, tagging with the data category Confidential data (2) will be removed from the files concerned.*



TAG REMOVAL RULES

Tag removal rules allow you to discard particular tags from files that were tagged e.g. by inappropriately set tagging rule. Use these rules with caution not to remove the tags from files that should be tagged. These rules are not dependent on selected data category.

Add

Rule name	Users	Data category	Paths	File description	Rule mode		
Confidential - remove tag	Support	Confidential data	C:\data\internal	Type: Audio Files, Video Files, Keyword: adv	Tagging	Edit	Remove

Note: The tagging of system files is always removed. You can also add your own paths to system files in Integration setting.

Visualization

If a file is tagged with a data category, a corresponding record is generated; you can view the record using visualization. A list of data categories and their rules is shown on the left in the charts section. After clicking on data categories or rules, the corresponding records with detailed information on file tagging are shown in the bottom list.

The following charts are available in the visualization:

- *Most active users* – users with the highest number of tagged files
- *Most active applications* – number of tagged files classified by applications from which the files were saved.
- *Extensions*
- *Most blocked servers*

Every record consists of the following items:

- *Date and time* – date and time when the record was generated.
- *PC* – name of the computer on which the record was generated.

- *Username* – name of the user under whom the record was generated.
- *Rules* – name of the rule based on which the file was tagged.
- *Application* – name of the application which worked with the file.
- *Data category* – name of the data category using which the file was tagged.
- *Domain* – name of the web domain from which the file was downloaded.
- *Extension* – file extension.
- *Source* – path to the folder in which the file was tagged.
- Type of operation:
  - *Merge* – tagging was merged.
  - *Store* – tagging was set.
  - *Remove* – tagging was removed.
- *Details*.

For more on the visualization interface, go to the Visualization mode section in help.

4.6.1.1 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 *Console -> DLP -> Data categories*.

Settings

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.

4.6.2 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 *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.

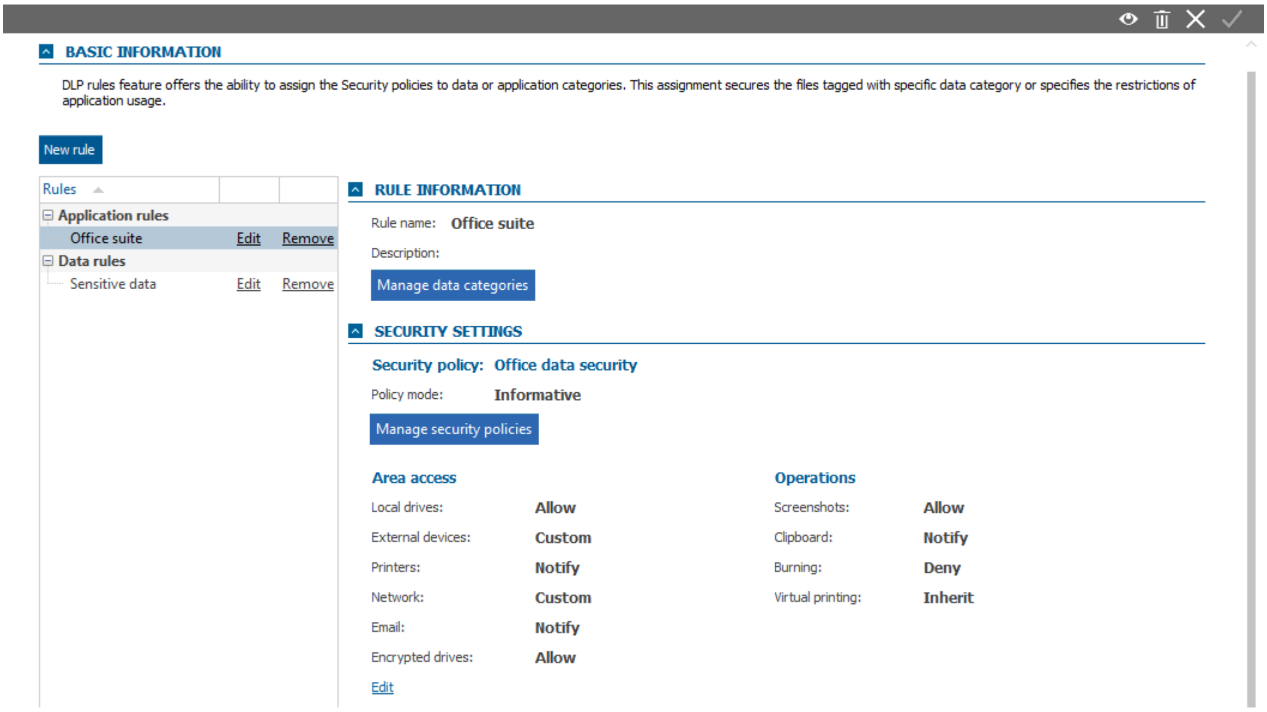
Click New DLP rule to launch the new rule wizard. When created, the rule will be added to the rules list.

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.

On the right you will find detail information about the selected rule.You can also manage Data categories and Security policies using buttons there.



BASIC INFORMATION

DLP rules feature offers the ability to assign the Security policies to data or application categories. This assignment secures the files tagged with specific data category or specifies the restrictions of application usage.

Rules		
⊟ Application rules		
Office suite	Edit	Remove
⊟ Data rules		
Sensitive data	Edit	Remove

RULE INFORMATION

Rule name: Office suite

Description:

SECURITY SETTINGS

Security policy: Office data security

Policy mode: Informative

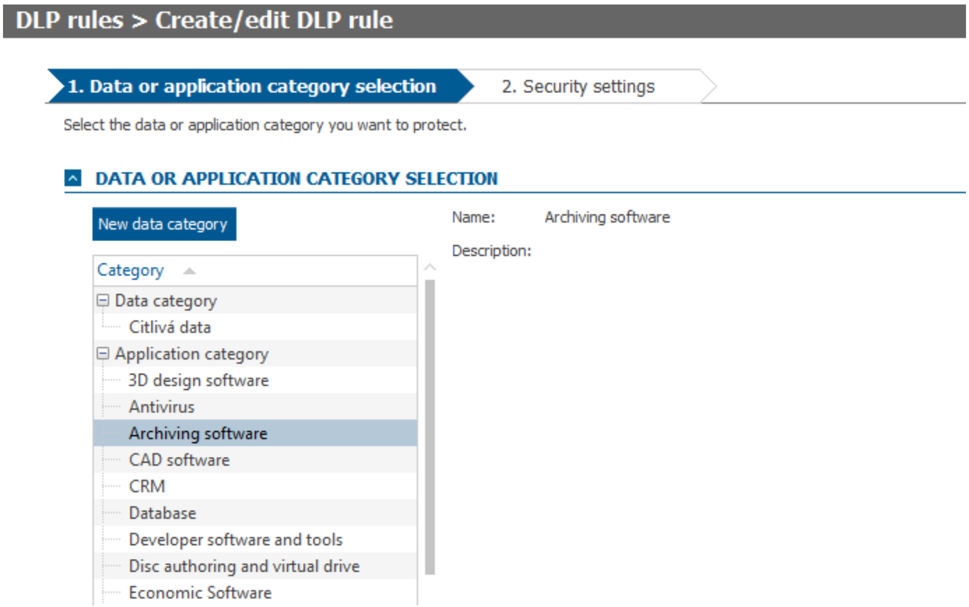
Area access		Operations	
Local drives:	Allow	Screenshots:	Allow
External devices:	Custom	Clipboard:	Notify
Printers:	Notify	Burning:	Deny
Network:	Custom	Virtual printing:	Inherit
Email:	Notify		
Encrypted drives:	Allow		

Edit

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.



DLP rules > Create/edit DLP rule

1. Data or application category selection

2. Security settings

Select the data or application category you want to protect.

DATA OR APPLICATION CATEGORY SELECTION

New data category

Name: Archiving software

Description:

Category

- Data category
  - Citlivá data
- Application category
  - 3D design software
  - Antivirus
  - Archiving software
  - CAD software
  - CRM
  - Database
  - Developer software and tools
  - Disc authoring and virtual drive
  - Economic Software

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. 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.

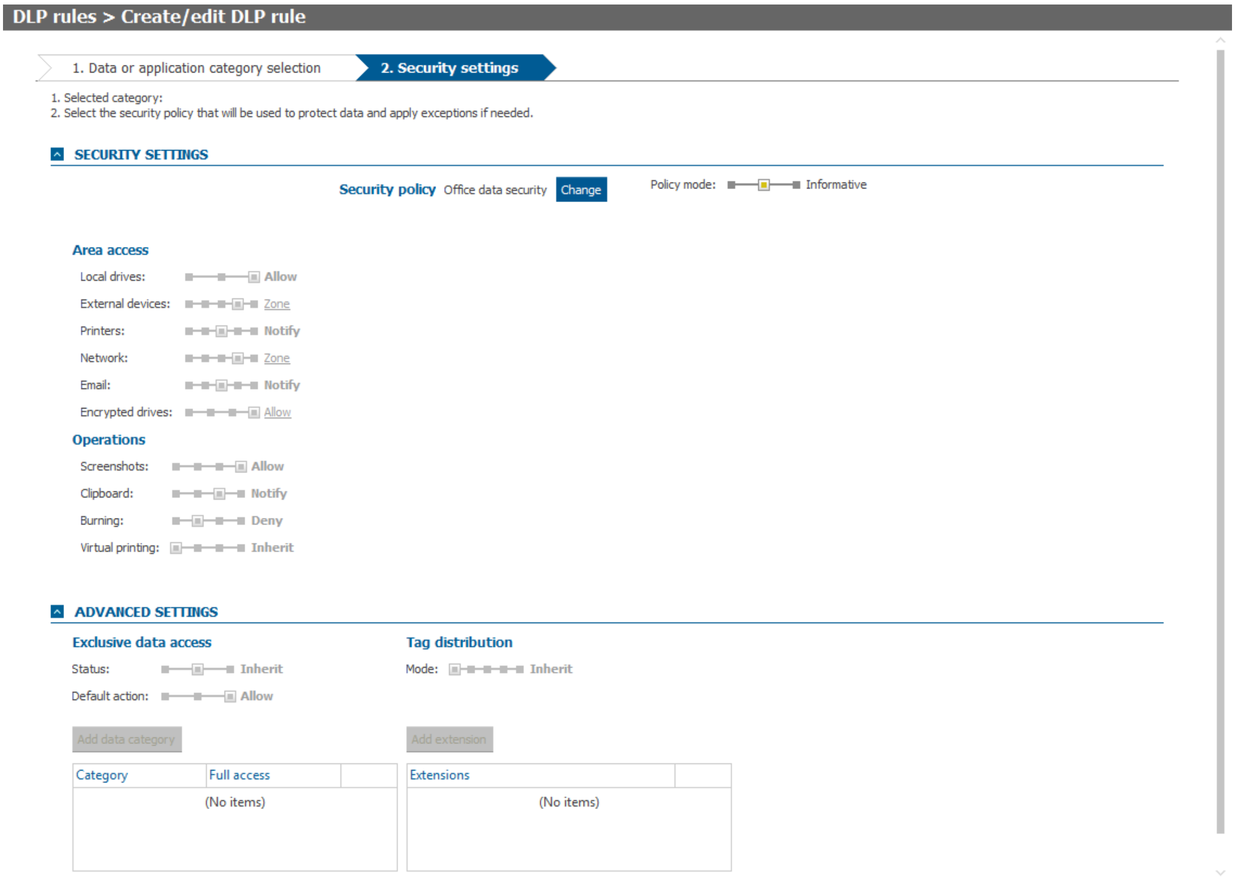
   b. *Informative* – the security policy will not be strictly applied. This means that for operations and security policy areas set to Deny, operations or access to an area will still be allowed, but the user will be notified and a record will be made in the DLP protocol. This mode is intended for testing 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.

   For more on the various parts of security policies and their settings, see the section *Security policies*.

   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 ✓.



DLP rules > Create/edit DLP rule

1. Data or application category selection
2. Security settings

1. Selected category:
2. Select the security policy that will be used to protect data and apply exceptions if needed.

SECURITY SETTINGS

Security policy: Office data security Change

Policy mode: Informative

Area access

Local drives: Allow
External devices: Zone
Printers: Notify
Network: Zone
Email: Notify
Encrypted drives: Allow

Operations

Screenshots: Allow
Clipboard: Notify
Burning: Deny
Virtual printing: Inherit

ADVANCED SETTINGS

Exclusive data access

Status: Inherit
Default action: Allow

Add data category

Category	Full access
(No items)	

Tag distribution

Mode: Inherit

Add extension

Extensions
(No items)

4.6.2.1 Security policies

This function is used to create security rules for data security and protection on end workstations or for work with applications. These policies will be used in the DLP rules function, where you can assign them to Data or Application categories.

Security policies are available via *Console -> DLP -> Security Policies*.

Settings

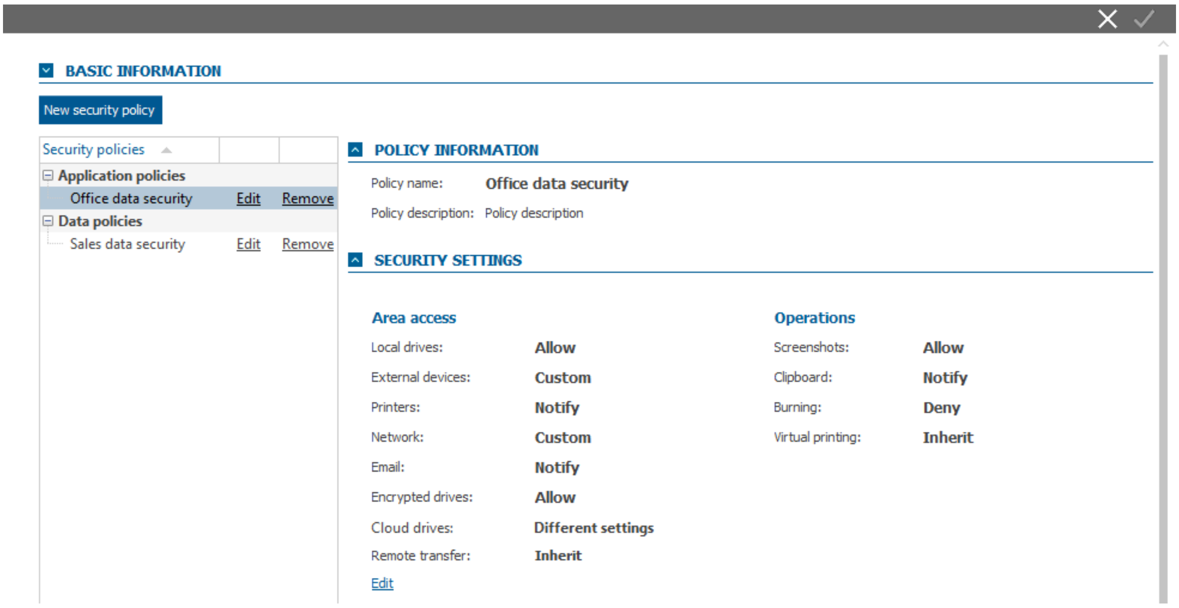
The left section of the view shows the list of security policies that have been created. There are two types of security policies:

- *Data Policy*
- *Application Policy*

When you select a policy in the list, detailed information about this security policy will be displayed on the right side of the view.

Click on *Adjust* at the relevant section of the security policy to change this section.

Click on *New security policy* to launch the new security policy wizard. When created, it will be added to the list in the left section. To save the newly created security policy, click the ✓ button or you can cancel the changes with the ✕ button in the upper right corner.



BASIC INFORMATION

Security policies

- Application policies
  - Office data security — Edit — Remove
- Data policies
  - Sales data security — Edit — Remove

POLICY INFORMATION

Policy name: Office data security

Policy description: Policy description

SECURITY SETTINGS

Area access	
Local drives:	Allow
External devices:	Custom
Printers:	Notify
Network:	Custom
Email:	Notify
Encrypted drives:	Allow
Cloud drives:	Different settings
Remote transfer:	Inherit

Operations	
Screenshots:	Allow
Clipboard:	Notify
Burning:	Deny
Virtual printing:	Inherit

Security policy

Security policies are rules through which data is protected. Two types of security policies are available. You can apply a policy either on data or on an application working with the data.

- *Data policy* – using data policy, you can determine what can be done with the data (files). Where the data can be stored, where they will be able to move and what applications will have access to the data. A data policy can be assigned to a data category, so any data tagged with a data category will be protected using a specific rule created in the data policy. Thus, the data policy applies to data files tagged with data categories. Data policies can be assigned to data categories using the DLP rules function.

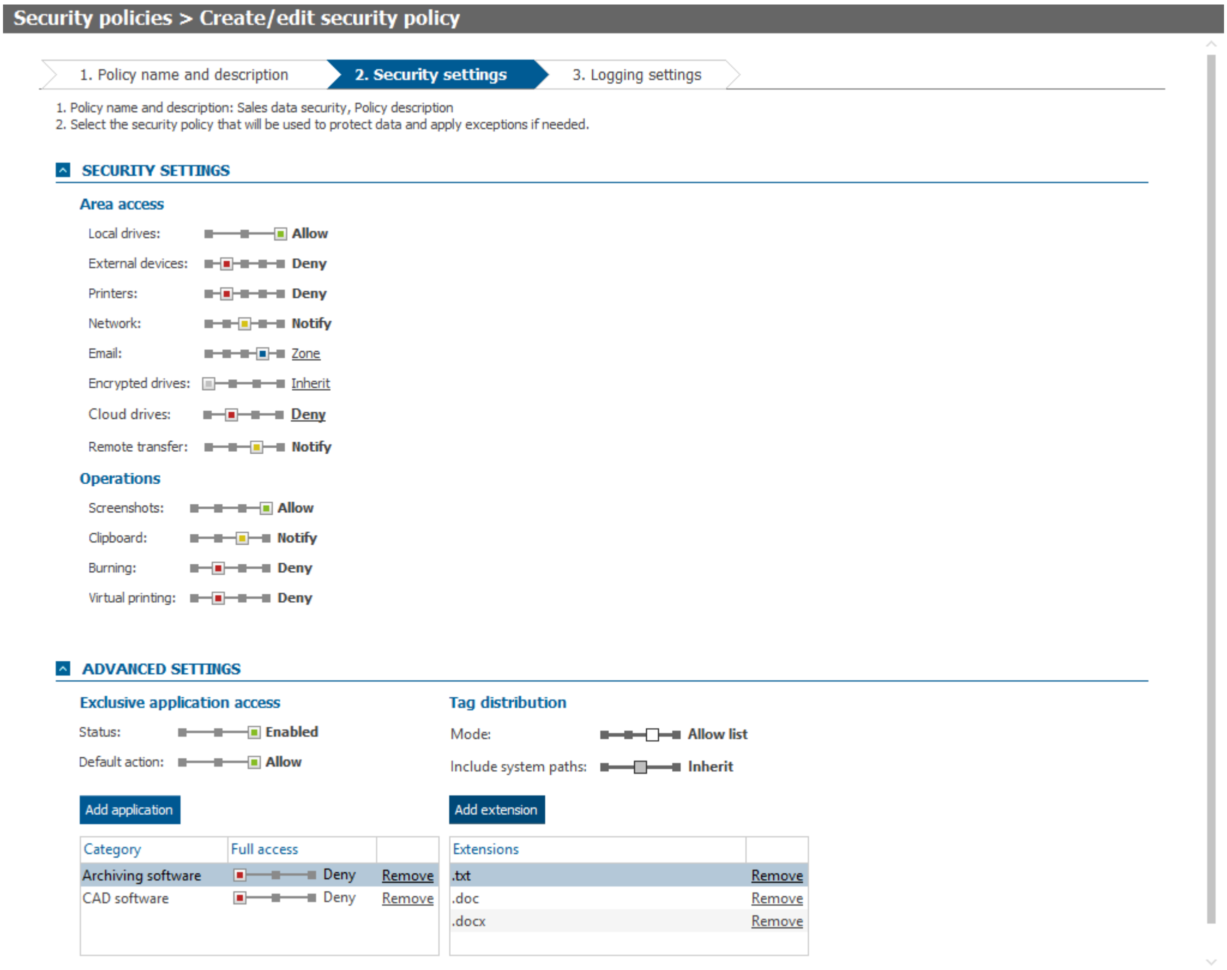
- *Application policy* – using the application policy, you can specify to which location applications will have access and how they can work with the data. Application policy can be assigned to any application category, so work with files in applications within the application category will be secured using the associated application policy. The application policy relates to work with files in applications from the application category to which the application policy applies. Application policies can be assigned to application categories using the DLP rules function.

Every single security policy – data and application policies alike – comprises two parts:

1. *Security settings*
2. *Recording settings*

Security Settings – Data Policy

Security settings for data policy are used to set where files can be stored and where they can move.



Security policies > Create/edit security policy

1. Policy name and description: Sales data security, Policy description
2. Select the security policy that will be used to protect data and apply exceptions if needed.

SECURITY SETTINGS

Area access

Local drives: Allow
External devices: Deny
Printers: Deny
Network: Notify
Email: Zone
Encrypted drives: Inherit
Cloud drives: Deny
Remote transfer: Notify

Operations

Screenshots: Allow
Clipboard: Notify
Burning: Deny
Virtual printing: Deny

ADVANCED SETTINGS

Exclusive application access

Status: Enabled
Default action: Allow

Category	Full access	
Archiving software	Deny	Remove
CAD software	Deny	Remove

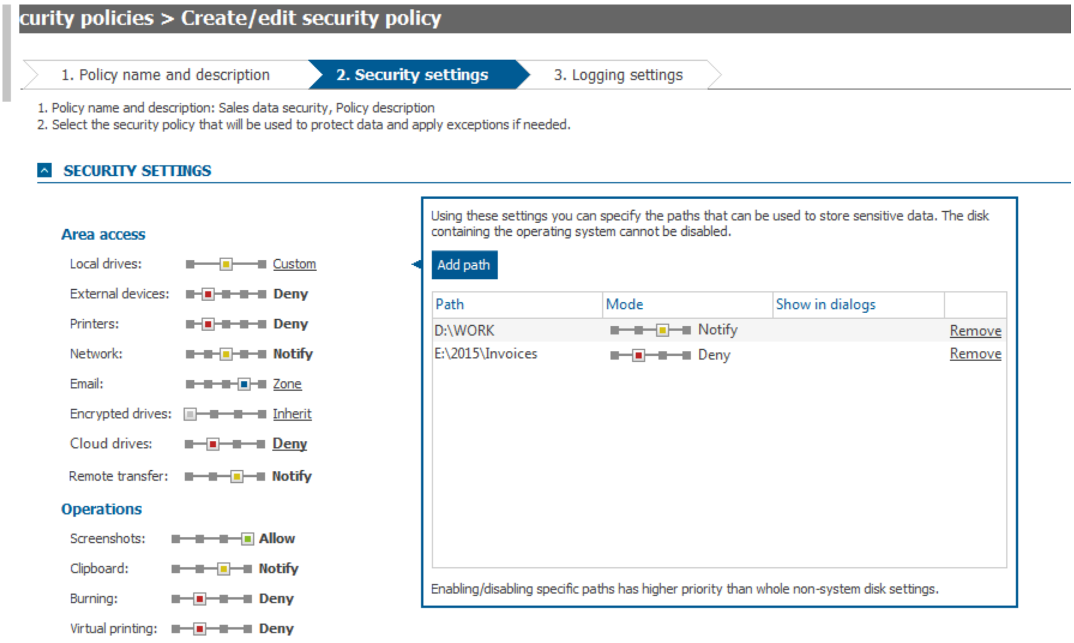
Tag distribution

Mode: Allow list
Include system paths: Inherit

Extensions	
.txt	Remove
.doc	Remove
.docx	Remove

Access to locations

- *Local disks* – here you set where files may be saved and copied in the file system on the user PC. You can choose from these options:
  - *Allowed* – files can be stored anywhere on the end workstation.
  - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such security policy exists).
  - *Custom* – after choosing your own settings, you can specify the restrictions for disks and folders where files may be moved. Use the *Add path* buttons to add the path to the folder. For each separate path, you can use the slider to specify the following:
    - *Disallowed* – files can not be saved or copied to the path.
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such 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 storing to the path will be permitted. In the *Show in dialogs* column, you can specify whether the enabled item will be displayed in Safetica notification dialogue boxes.



curity policies > Create/edit security policy

1. Policy name and description | 2. Security settings | 3. Logging settings

1. Policy name and description: Sales data security, Policy description
2. Select the security policy that will be used to protect data and apply exceptions if needed.

SECURITY SETTINGS

Area access

Local drives:	Custom
External devices:	Deny
Printers:	Deny
Network:	Notify
Email:	Zone
Encrypted drives:	Inherit
Cloud drives:	Deny
Remote transfer:	Notify

Operations

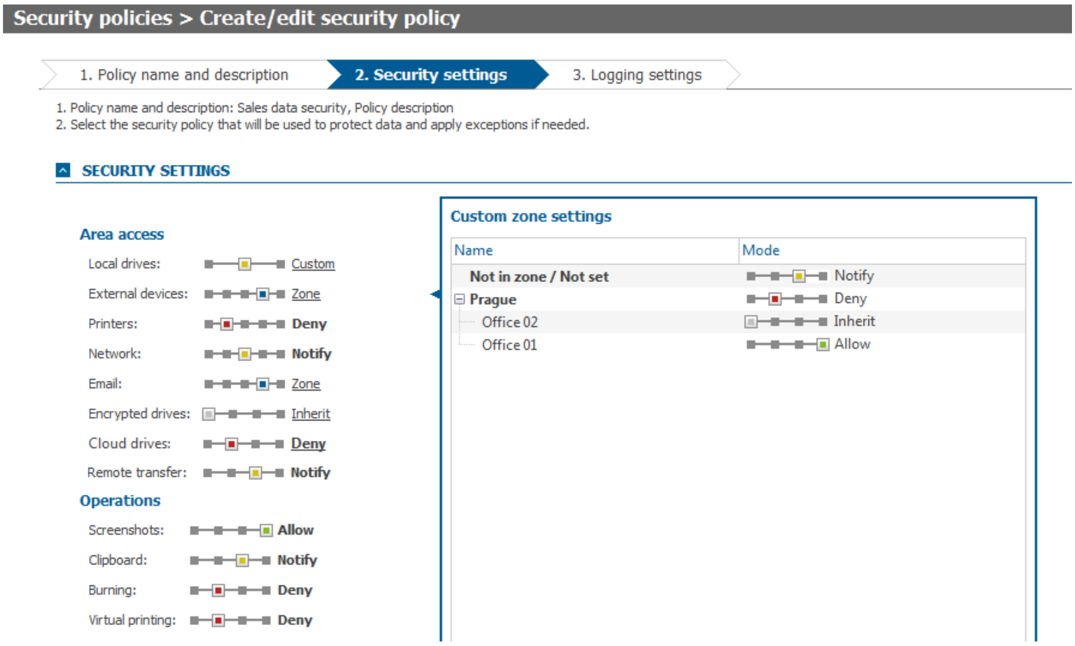
Screenshots:	Allow
Clipboard:	Notify
Burning:	Deny
Virtual printing:	Deny

Using these settings you can specify the paths that can be used to store sensitive data. The disk containing the operating system cannot be disabled.

Path	Mode	Show in dialogs	
D:\WORK	Notify		Remove
E:\2015\Invoices	Deny		Remove

Enabling/disabling specific paths has higher priority than whole non-system disk settings.

- *External Device* – here you can set an external device to which files may be stored or copied. You can choose from these options:
  - *Disallowed* – files can not be saved or copied to any external device.
  - *Notify* – when saving or copying a file to an external dervice, 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 parent group (if such 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.
    - *Disallow* – files may not be saved or copied to an external device being part of the zone.
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such security policy exists).
    - *Notify* – when saving or copying a file to an external device, which is included in the zone, the user will see a notification in the dialog and a corresponding record will be made in the DLP protocol.
    - *Allowed* - copying or saving to an external device which is included in the zone is permitted.
  - *Allowed* - copying or storing of any external devices will be allowed.



Security policies > Create/edit security policy

1. Policy name and description | 2. Security settings | 3. Logging settings

1. Policy name and description: Sales data security, Policy description
2. Select the security policy that will be used to protect data and apply exceptions if needed.

SECURITY SETTINGS

Area access

Local drives:	Custom
External devices:	Zone
Printers:	Deny
Network:	Notify
Email:	Zone
Encrypted drives:	Inherit
Cloud drives:	Deny
Remote transfer:	Notify

Operations

Screenshots:	Allow
Clipboard:	Notify
Burning:	Deny
Virtual printing:	Deny

Custom zone settings

Name	Mode
Not in zone / Not set	Notify
Prague	Deny
Office 02	Inherit
Office 01	Allow

- *Printers* – security policy settings for the printer are analogical to settings for external devices.
- *Network* – security policy settings for access to the network are analogical to settings for external devices.
- *E-mails* – security policy settings for sending e-mails are analogical to settings for external devices. This security policy will be applied only for E-mail clients listed in the respective application category (E-mail client).

  Note: These settings have a higher priority than the network security policy. If e-mails are enabled and the network disabled, then e-mails can be sent only from e-mail clients listed in the respective application category.

- *Encrypted disks* – here you can allow or disallow access to disks encrypted by Safetica. You can also specify access to different types of encrypted disks: *Local encrypted disks, External encrypted disks.*
- *Cloud drives* – here you can specify access settings for local folders that are used by certain cloud services. The supported cloud services are Google Drive, OneDrive, Dropbox and Box Sync. You can set up access rights for all of the supported cloud services or for each of them individually. You can choose from these options:
  - o *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such security policy exists).
  - o *Deny* – files cannot be saved or copied to a local cloud folder.
  - o *Notify* – when saving or copying a file to a local cloud folder, the user will be shown a notification dialogue box and a corresponding record will be made in the DLP log.
  - o *Allow* – copying or storing data to the local cloud folder will be permitted.
- *Remote transfer* – here, you can specify in more detail the settings for the file transfer via the Microsoft Remote Desktop Services:
  - o *Inherit* – the settings will be inherited from the security policy set in the DLP rules on the parent group (if such security policy exists).
  - o *Deny* – files cannot be copied via the remote desktop.
  - o Notify – when copying a file via the remote desktop, the user will see a notification in a dialog box and a corresponding record will be made in the DLP protocol. Copying will not be

blocked.

- o *Allow* – copying files via the remote desktop is enabled.

Operation

- *Screenshots* – here you can allow or disallow the print screen function or similar screenshot functions for files. Alternatively, you can only set an alert when a screenshot is taken.
- *Clipboard* – here you can allow or disallow the use of the clipboard for files (Ctrl+C, Ctrl+V, Ctrl+X, etc.). If disallowed, the clipboard cannot be used for file contents or directly for the file in the file system. Alternatively, you can only set an alert when the clipboard is used.
- *Burning* – here you can allow or disallow the writing of files to a medium. Alternatively, you can only set an alert when writing is used.
- *Virtual printing* - here you can allow or disallow the use of virtual printers. Alternatively, you can only set an alert when they are used.

Advanced settings

Exclusive access for applications

In this section, you can specify which applications will have exclusive access to files to which the security policy applies. The security policy will not be applied to the application categories enabled. You can choose with the *Default action* scroll bar what the default rule for application access to the data category should be.

After clicking *Add application* , a dialog opens with a selection of application categories. When chosen and after clicking*OK*, the application category will be added to the list, so you enable or disable exclusive access to the data category for it.

Tag distribution

When you open a file marked with a data category to which a security policy shall apply in any application, then the files you are going to save from this application will be marked with the same data category as the file you opened in the application.

Tags are automatically propagated to user outputs of the application. In the next setting, you can add more extensions to this mechanism by clicking on Add extension.

Propagation of tags to system paths is disabled.

Security settings – application policy

Security settings for the application policy are intended for deciding how users can work with applications. You can specify access of applications to paths and disks in the system and decide which operations shall be allowed or denied in these applications. The settings are analogical to the data policy settings.

Setting area access

- *Local disks* – here you set where files may be saved and copied in the file system on the user PC. You can choose from these options:
  - o *Allow - files can be stored anywhere on the end workstation.*
  - o *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such 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* buttons to add the path to the folder. For each separate path, you can use the slider to specify the following:

- *Disallowed* – files can not be saved or copied to the path.
- *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such 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 storing to the path will be permitted. In the *Show in dialogs* column, you can specify whether the enabled item will be displayed in Safetica notification dialogue boxes.

- *External Device* – here you can set an external device to which files may be stored or copied. You can choose from these options:
    - *Deny – files can not be saved or copied to any external device.*
    - *Notify* – when saving or copying a file to an external dervice, 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 parent group (if such 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.
        - *Disallow* – files may not be saved or copied to an external device being part of the zone.
        - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such security policy exists).
        - *Notify* – when saving or copying a file to an external device, which is included in the zone, the user will see a notification in the dialog and a corresponding record will be made in the DLP protocol.
        - *Allowed* – copying or saving to an external device which is included in the zone is permitted.
    - *Allowed* – copying or storing of any external devices will be allowed.
- *Printers* – security policy settings for the printer are analogical to settings for external devices.
- *Network* – security policy settings for access to the network are analogical to settings for external devices.
- *E-mails* – security policy settings for sending e-mails are analogical to settings for external devices.

    Note: These settings have a higher priority than the network security policy. If e-mails are allowed and the network denied, e-mails can be sent.
- *Encrypted disks* – here you can allow or disallow access to disks encrypted by Safetica. You can also specify access to different types of encrypted disks: *Local encrypted disks, External encrypted disks.*
- *Cloud drives* – here you can specify access settings for local folders that are used by certain cloud services. The supported cloud services are Google Drive, OneDrive, Dropbox and Box Sync. You can set up access rights for all of the supported cloud services or for each of them individually. You can choose from these options:
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rule on the parent group (if such security policy exists).
    - *Deny* – files cannot be saved or copied to a local cloud folder.

    - *Notify* – when saving or copying a file to a local cloud folder, the user will be shown a notification dialogue box and a corresponding record will be made in the DLP log.
    - *Allow* – copying or storing data to the local cloud folder will be permitted.
- *Remote transfer* – here, you can specify in more detail the settings for the file transfer via the Microsoft Remote Desktop Services:
    - *Inherit* – the settings will be inherited from the security policy set in the DLP rules on the parent group (if such security policy exists).
    - *Deny* – files cannot be copied via the remote desktop.
    - Notify – when copying a file via the remote desktop, the user will see a notification in a dialog box and a corresponding record will be made in the DLP protocol. Copying will not be blocked.
    - *Allow* – copying files via the remote desktop is enabled.

Setting an operation

- *Screenshots* – here you can allow or deny the use of the print screen function for applications. Alternatively, you can only set an alert when a screenshot is taken.
- *Clipboard* – here you can allow or disallow the use of the clipboard for applications (Ctrl+C, Ctrl+V, Ctrl+X, etc.). Alternatively, you can only set an alert when the clipboard is used.
- *Burning* – here you can allow or disallow the writing of applications to a medium. Alternatively, you can only set an alert when writing is used.
- *Virtual printing* – here you can allow or deny the use of virtual printers. Alternatively, you can only set an alert when they are used.

Advanced settings

Exclusive data access

In this section you can specify to which data categories (files tagged with a data category) the application category shall have exclusive access. The security policy will not be applied to the data categories enabled. You can choose with the *Default action* scroll bar what the default rule for application access to the data categories will be.

Click *Add data category* and a dialog will open where you can choose the data category. When chosen, click *OK* and the data category will be added to the list, so you can set access of applications from the application category for it – allow or deny.

Tag distribution

When you open a file tagged with a data category in an application 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 file that is open.

Tags are automatically propagated to user outputs of the application. In the next setting, you can add more extensions to this mechanism by clicking on Add extension.

Propagation of tags to system paths is disabled.

Creating a Security Policy

Click on *New security policy* to launch the new security policy wizard.

1. In the first step use the scroll bar to specify the name, description and type of the new security policy:
    - *Data Policy*

   - *Application Policy*

Once finished, *click*Next.

2. In the second step use the scroll bar and list of basic and/or advanced security settings for the security policy you are creating. Once finished, *click*Next.
3. In the second step use the scroll bar and list of basic and/or advanced security settings for the monitoring of files subject to the security policy. Once finished, click *Done*. The security policy will be added to the respective list of policies. To save the policy, click ✓.

4.6.3 DLP protocol

The DLP protocol is used to set the monitoring operations with data or applications, which are subject to the security policy. You can set in detail which operations shall be recorded and specify which file type shall be recorded based on extensions. The data recording is applied after setting in the DLP rules.

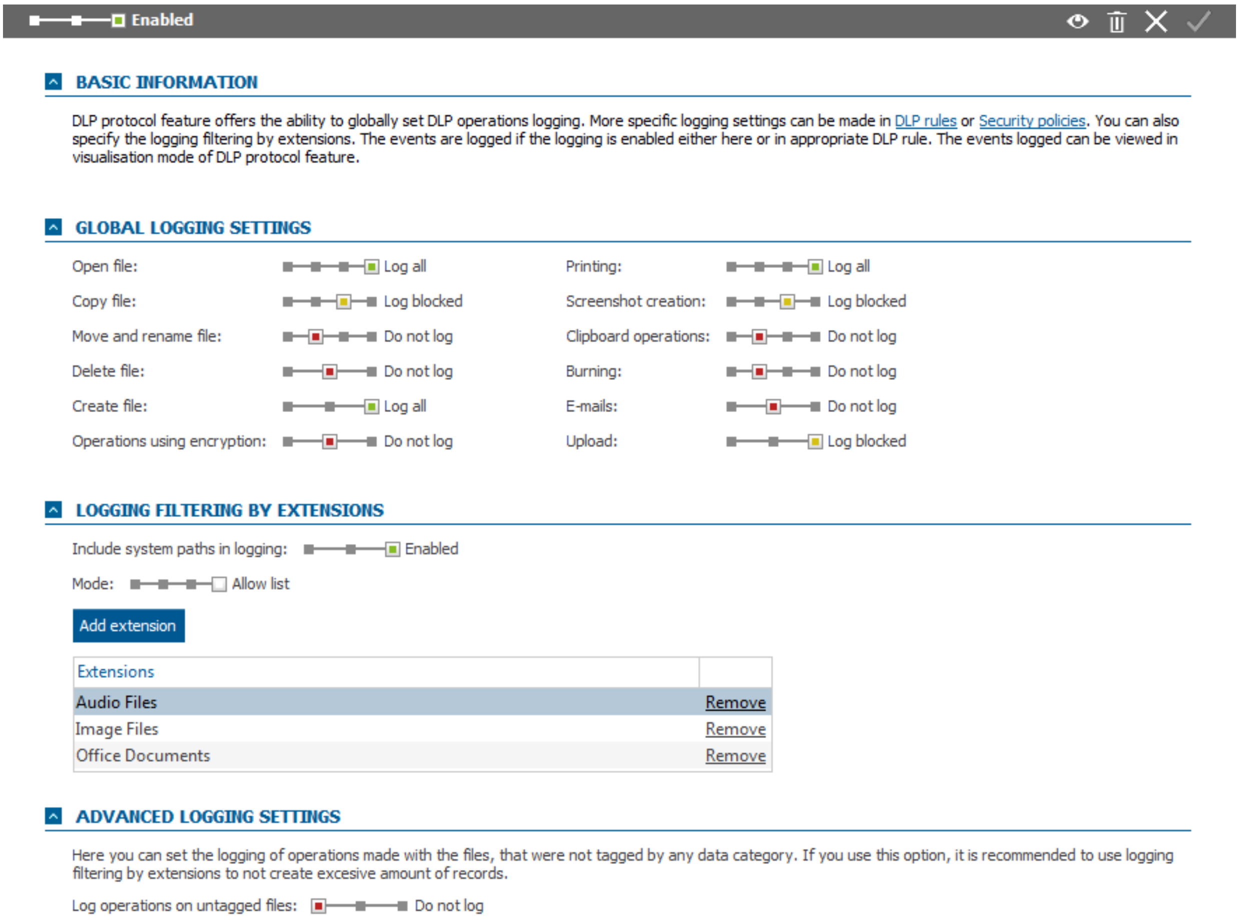
DLP protocol can be found in the section *Console -> DLP -> DLP protocol*.

Settings

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

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.



Enabled

BASIC INFORMATION

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

GLOBAL LOGGING SETTINGS

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

LOGGING FILTERING BY EXTENSIONS

Include system paths in logging: Enabled

Mode: □ Allow list

Add extension

Extensions	
Audio Files	Remove
Image Files	Remove
Office Documents	Remove

ADVANCED LOGGING SETTINGS

Here you can set the logging of operations made with the files, that were not tagged by any data category. If you use this option, it is recommended to use logging filtering by extensions to not create excesive amount of records.

Log operations on untagged files: Do not log

Global logging settings

In the next part of the main settings you can specify which operations should 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 and rename file* – a record is made when a file is moved.
- *Delete file* – a record is made when a file is deleted.
- *Create file* – a record is made when a file is createdregarding this activity.
- *Operations using encryption* – 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.
- *E-mails* – a record is made when an attempt to send a file by email is blocked.
- *Upload* – a record is made when an attempt to upload a file to the network or the Internet is blocked.

Every operation has several recording modes:

- *Inherit* – settings are inherited from the parent group.
- *Do not log* – the respective operation is not recorded.
- *Log blocked* – only respective Safetica-blocked operations are recorded.
- *Log all* – all files are monitored.

Logging filtering by extensions

In the upper section you can use the Add system paths to logging slider to specify whether also system paths should be included in recording. An example is C:\Windows. The filter can be enabled or disabled by using the slider.

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.

Visualization

There are following charts in the visualization mode:

- *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.

Each record contains several types of information represented by columns:

- *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.
- *Destination type* – whether the target path is local, external or network-based.
- *Source device* – device name and SID. After clicking the name, detailed information on the device will be displayed. Here you can specify what zones the device shall belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- *Destination device* – device name and SID. After clicking the name, detailed information on the device will be displayed. Here you can specify what zones the device shall belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- *File* – name of the file. If you make a group, create an order or filter by using this column, the file name will be taken from the *Source* column. If the source is empty, the file name will be taken from the *Destination* column.
- *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.
- *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*
- *File size*

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.6.4 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 *Console* -> DLP/Administration and settings -> Zones.

Settings

The 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.

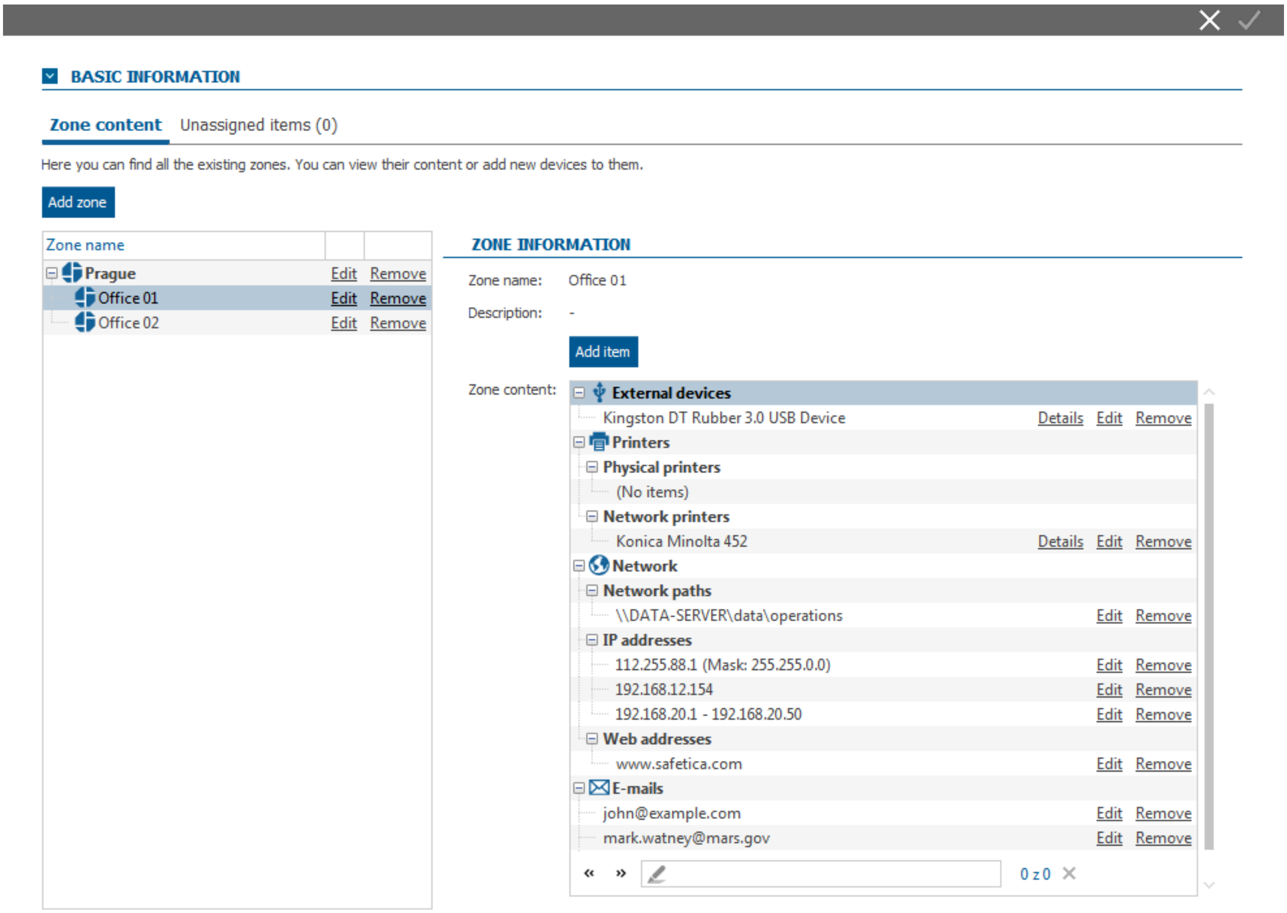
Click *Add zone* to open the new zone dialog, enter a name and description for it and specify whether it shall have a parent zone or not. You can select a parent zone using dropdown menu.

By clicking *Edit* with the respective zone in the list on the left, you can change its name and description.

There are two tabs above the list of zones: *Zone content* and *Unassigned items.* Content of the right section of the view depends on tab you have selected:

- *Zone content* – this section contains a list of items in the selected zone. Click *Add item* in zone content and the new item wizard will open to add a new item to a zone. You can edit item in the zone by clicking on *Edit*.
- *Unassigned items* – In the section to the right you will find a list of available external devices and printers found on workstations with client. These devices and printers have not been assigned to any zone yet.
  - o By moving them to the middle list or clicking *Add*, you can assign them to the zone marked on the left.
  - o Click *Remove* to return the device or printer to the Unassigned group.
  - o By clicking *Edit*, you can edit the description of the device displayed in the records on the console and in the notification windows on the PC with client.
  - o You can click *Details* to display detailed information on the item.

Note: You can use the mouse in the lists to select and move multiple items at once.



Here you can find all the existing zones. You can view their content or add new devices to them.

Zone name		
Prague	Edit	Remove
Office 01	Edit	Remove
Office 02	Edit	Remove

Zone name: Office 01

Description: -

Zone content:

- External devices
  - Kingston DT Rubber 3.0 USB Device — Details Edit Remove
- Printers
  - Physical printers
    - (No items)
  - Network printers
    - Konica Minolta 452 — Details Edit Remove
- Network
  - Network paths
    - \\DATA-SERVER\data\operations — Edit Remove
  - IP addresses
    - 112.255.88.1 (Mask: 255.255.0.0) — Edit Remove
    - 192.168.12.154 — Edit Remove
    - 192.168.20.1 - 192.168.20.50 — Edit Remove
  - Web addresses
    - www.safetica.com — Edit Remove
- E-mails
  - john@example.com — Edit Remove
  - mark.watney@mars.gov — Edit Remove

Creating a new zone and adding items

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. You can select a parent zone using dropdown menu.

Note: You can move zones within the tree structure by dragging them using the mouse.

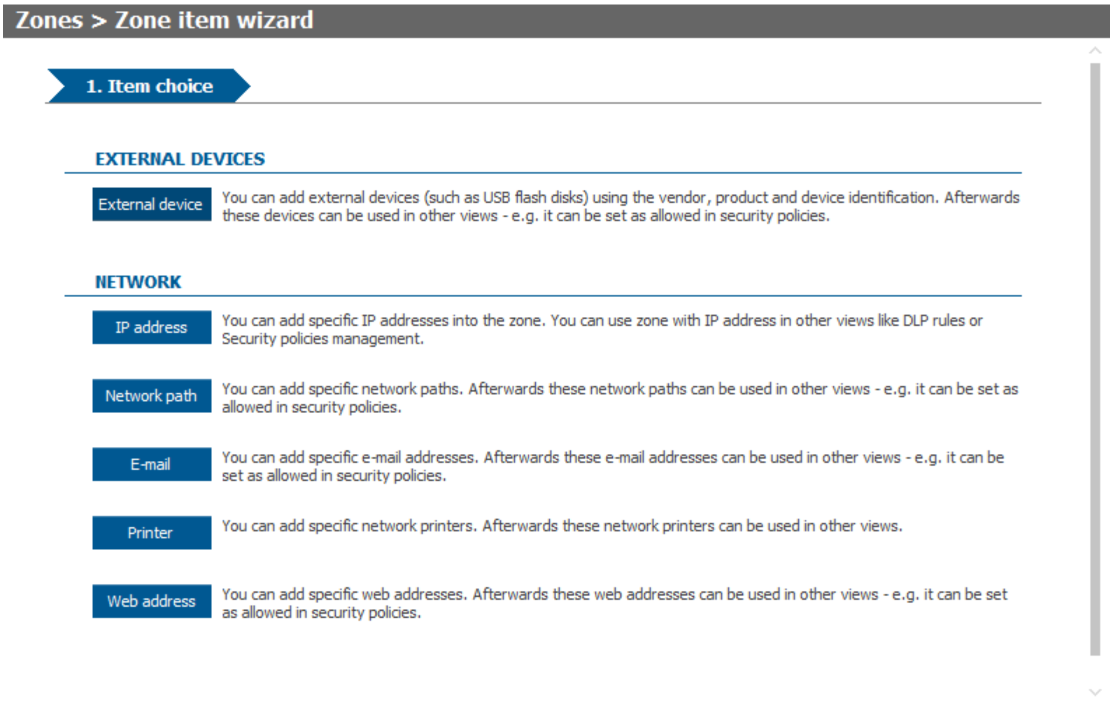
To edit the zone content, proceed as follows:

1. In the zone list on the left, mark the zone whose content you wish to edit. The zone's cur-

rent 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:
   - o *External devices*
   - o *IP addresses*
   - o *Network paths*
   - o *E-mails*
   - o *Printers*
   - o *Web addresses*

Click the item you wish to add. The corresponding view for adding the item will open.



Zones > Zone item wizard

1. Item choice

EXTERNAL DEVICES

External device — You can add external devices (such as USB flash disks) using the vendor, product and device identification. Afterwards these devices can be used in other views - e.g. it can be set as allowed in security policies.

NETWORK

IP address — You can add specific IP addresses into the zone. You can use zone with IP address in other views like DLP rules or Security policies management.

Network path — You can add specific network paths. Afterwards these network paths can be used in other views - e.g. it can be set as allowed in security policies.

E-mail — You can add specific e-mail addresses. Afterwards these e-mail addresses can be used in other views - e.g. it can be set as allowed in security policies.

Printer — You can add specific network printers. Afterwards these network printers can be used in other views.

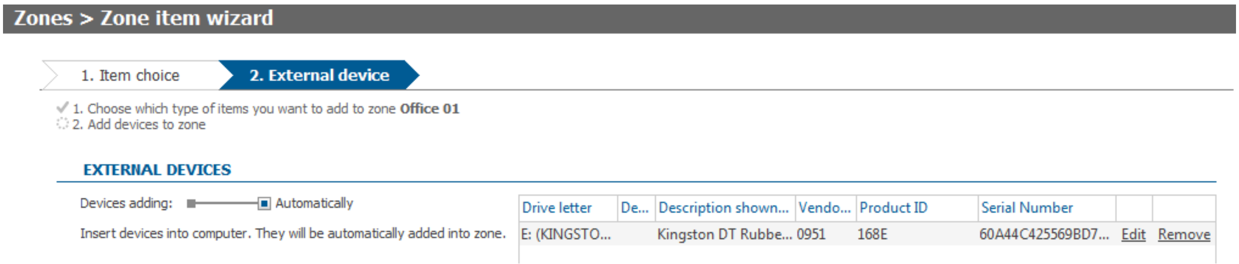
Web address — You can add specific web addresses. Afterwards these web addresses can be used in other views - e.g. it can be set as allowed in security policies.

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:

- o *Automatically* – in automatic mode it is enough to connect the external storage device to the PC where console is running. When connected, the device will be added to the list.
- o *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.



Zones > Zone item wizard

1. Item choice — 2. External device

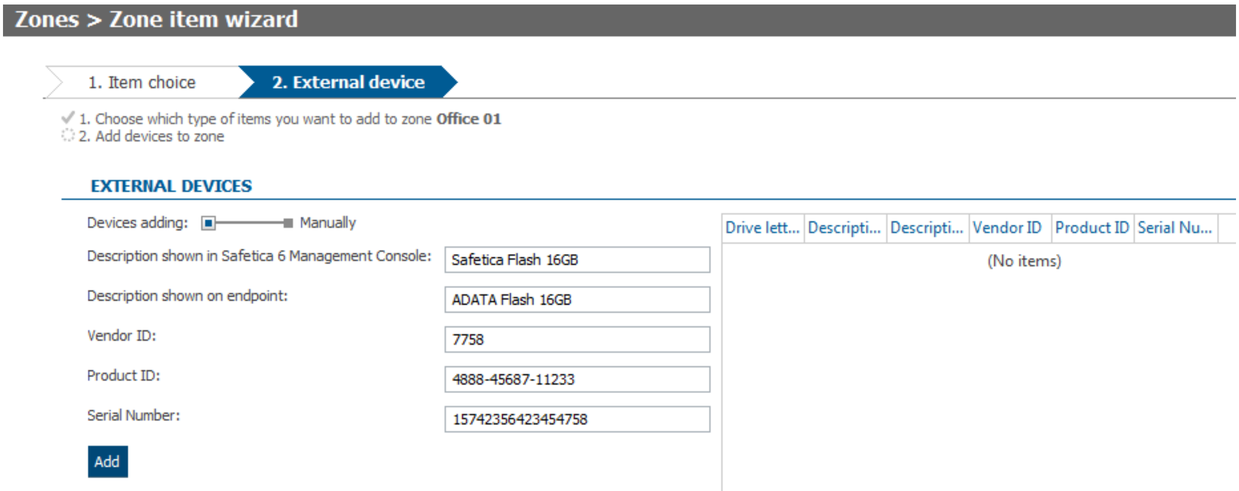
✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add devices to zone

EXTERNAL DEVICES

Devices adding: Automatically

Insert devices into computer. They will be automatically added into zone.

Drive letter	De...	Description shown...	Vendo...	Product ID	Serial Number		
E: (KINGSTO...		Kingston DT Rubbe...	0951	168E	60A44C425569BD7...	Edit	Remove



Zones > Zone item wizard

1. Item choice | 2. External device

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add devices to zone

EXTERNAL DEVICES

Devices adding: Manually

Description shown in Safetica 6 Management Console: Safetica Flash 16GB

Description shown on endpoint: ADATA Flash 16GB

Vendor ID: 7758

Product ID: 4888-45687-11233

Serial Number: 15742356423454758

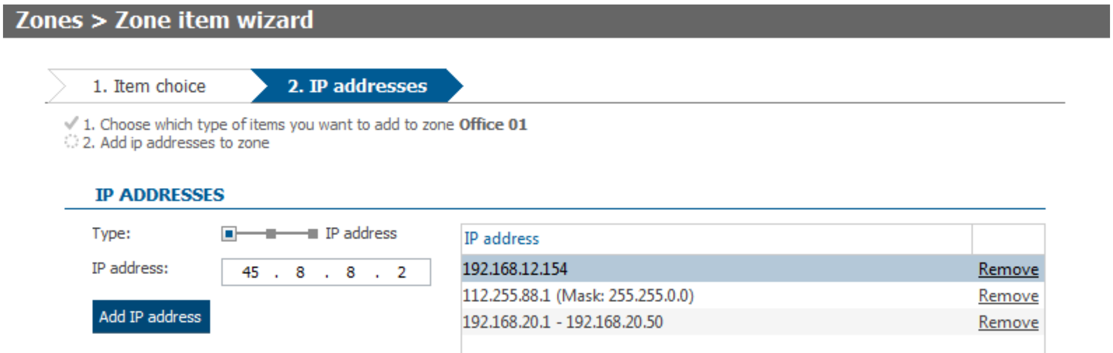
Drive lett...	Descripti...	Descripti...	Vendor ID	Product ID	Serial Nu...
(No items)					

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.



Zones > Zone item wizard

1. Item choice | 2. IP addresses

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add ip addresses to zone

IP ADDRESSES

Type: IP address

IP address: 45 . 8 . 8 . 2

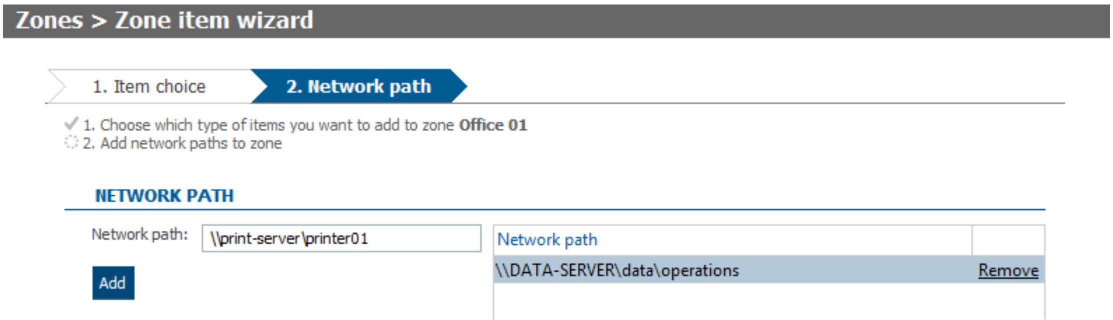
IP address	
192.168.12.154	Remove
112.255.88.1 (Mask: 255.255.0.0)	Remove
192.168.20.1 - 192.168.20.50	Remove

Adding a network path

Enter the path to a shared folder in the network format (e.g. \\Data\Finance) in the text box and click Add to add the path to the list on the right.

You can add several network paths to the list.

You can add your entire computer on which the shared folders are located to the zone. You can do this by entering the path in the root format. For example, \\DATA-SERVER\. In this case, the zone will include all folders shared from the specified computer.



Zones > Zone item wizard

1. Item choice | 2. Network path

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add network paths to zone

NETWORK PATH

Network path: \\print-server\printer01

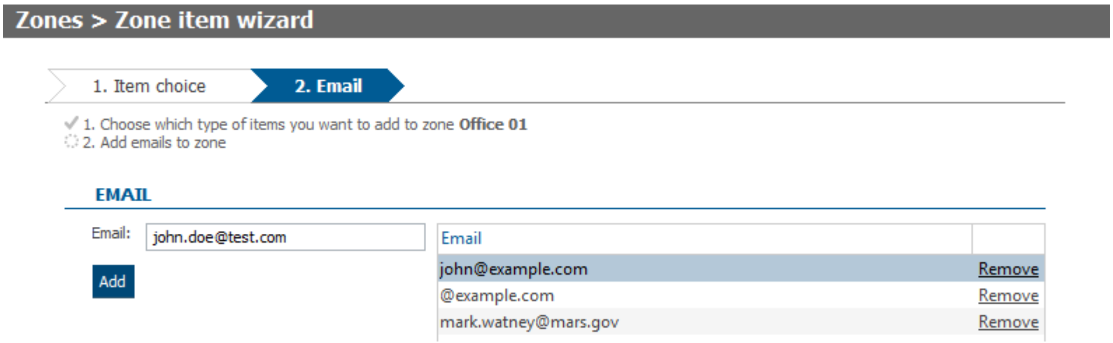
Add

Network path	
\\DATA-SERVER\data\operations	Remove

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.



Zones > Zone item wizard

1. Item choice | 2. Email

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add emails to zone

EMAIL

Email: john.doe@test.com

Add

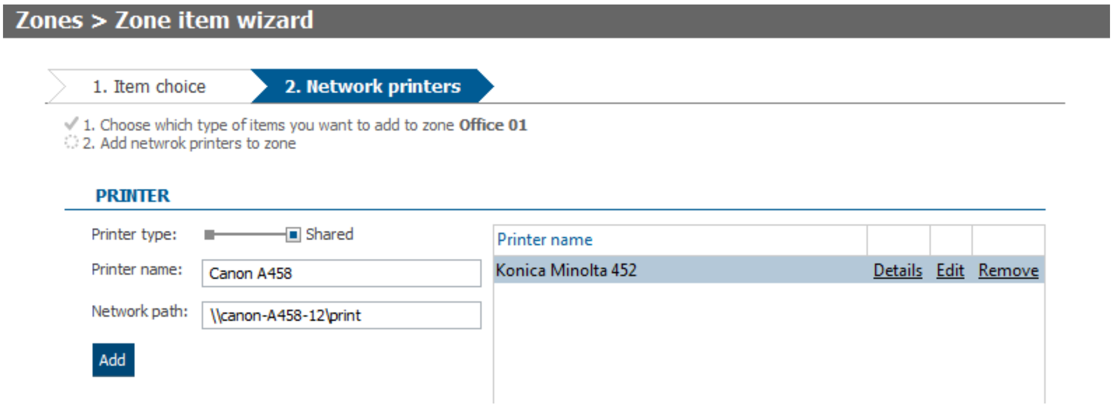
Email	
john@example.com	Remove
@example.com	Remove
mark.watney@mars.gov	Remove

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.



Zones > Zone item wizard

1. Item choice | 2. Network printers

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add netwrok printers to zone

PRINTER

Printer type: Shared

Printer name: Canon A458

Network path: \\canon-A458-12\print

Add

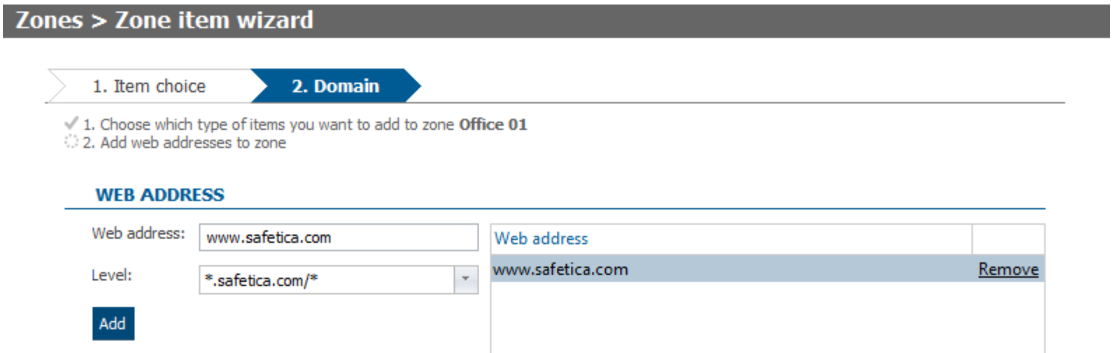
Printer name			
Konica Minolta 452	Details	Edit	Remove

Web address

There you can add web addresses to the zone. For each address inserted added to 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 following options in Level:

- www.facebook.com/* – to the zone will belong 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/* – to the zone will belong 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/* – to the zone will belong all addresses, which containing .facebook.com, e.g.. For example www.facebook.com/AAA/ or ccc.facebook.com/AAA/BBB, etc.
- *.com/* – to the zone will belong all addresses, which containing 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/ *.



Zones > Zone item wizard

✓ 1. Choose which type of items you want to add to zone **Office 01**
2. Add web addresses to zone

WEB ADDRESS

Web address: www.safetica.com

Level: *.safetica.com/*

Web address	
www.safetica.com	Remove

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.

4.6.5 Disk guard

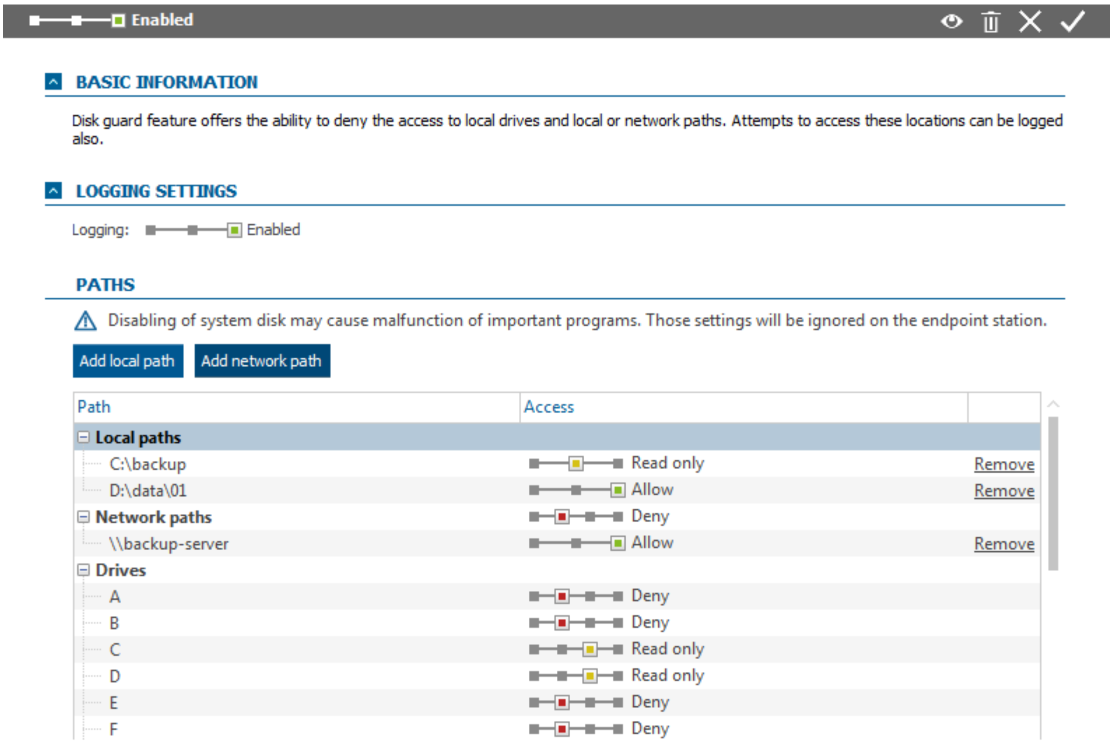
Disk guard allows you to set access rights for the users, computers or groups to access a system and network paths or system disks through a simple set of rules. For example, you can choose drives the users can access or only use for reading, or select specific paths or folders.

Disk guard is under *DLP* -> *Disk guard*

Settings

In the console settings mode this feature can be enabled or disabled using the slider in the header of this view.

Using the *Logging* slider you can enable logging of access actions. You can view a record about these actions in visualization mode.



Enabled

BASIC INFORMATION

Disk guard feature offers the ability to deny the access to local drives and local or network paths. Attempts to access these locations can be logged also.

LOGGING SETTINGS

Logging: Enabled

PATHS

⚠ Disabling of system disk may cause malfunction of important programs. Those settings will be ignored on the endpoint station.

Path	Access	
⊟ **Local paths**		
C:\backup	🟨 Read only	Remove
D:\data\01	🟩 Allow	Remove
⊟ **Network paths**	🟥 Deny	
\\backup-server	🟩 Allow	Remove
⊟ **Drives**		
A	🟥 Deny	
B	🟥 Deny	
C	🟨 Read only	
D	🟨 Read only	
E	🟥 Deny	
F	🟥 Deny	

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.
- *Cloud drives* – here you can specify access settings for local folders that are used by certain cloud services. The supported cloud services are Google Drive, Dropbox, OneDrive, and Box Sync. You can set up access rights for all of the supported cloud services or for each of them individually.

  Note: It is indicated in individual cloud services in the table how many computers selected in the tree of users have an appropriate cloud client installed.

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 following charts in the visualization mode:

- *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.

Each record contains several types of information represented by columns:

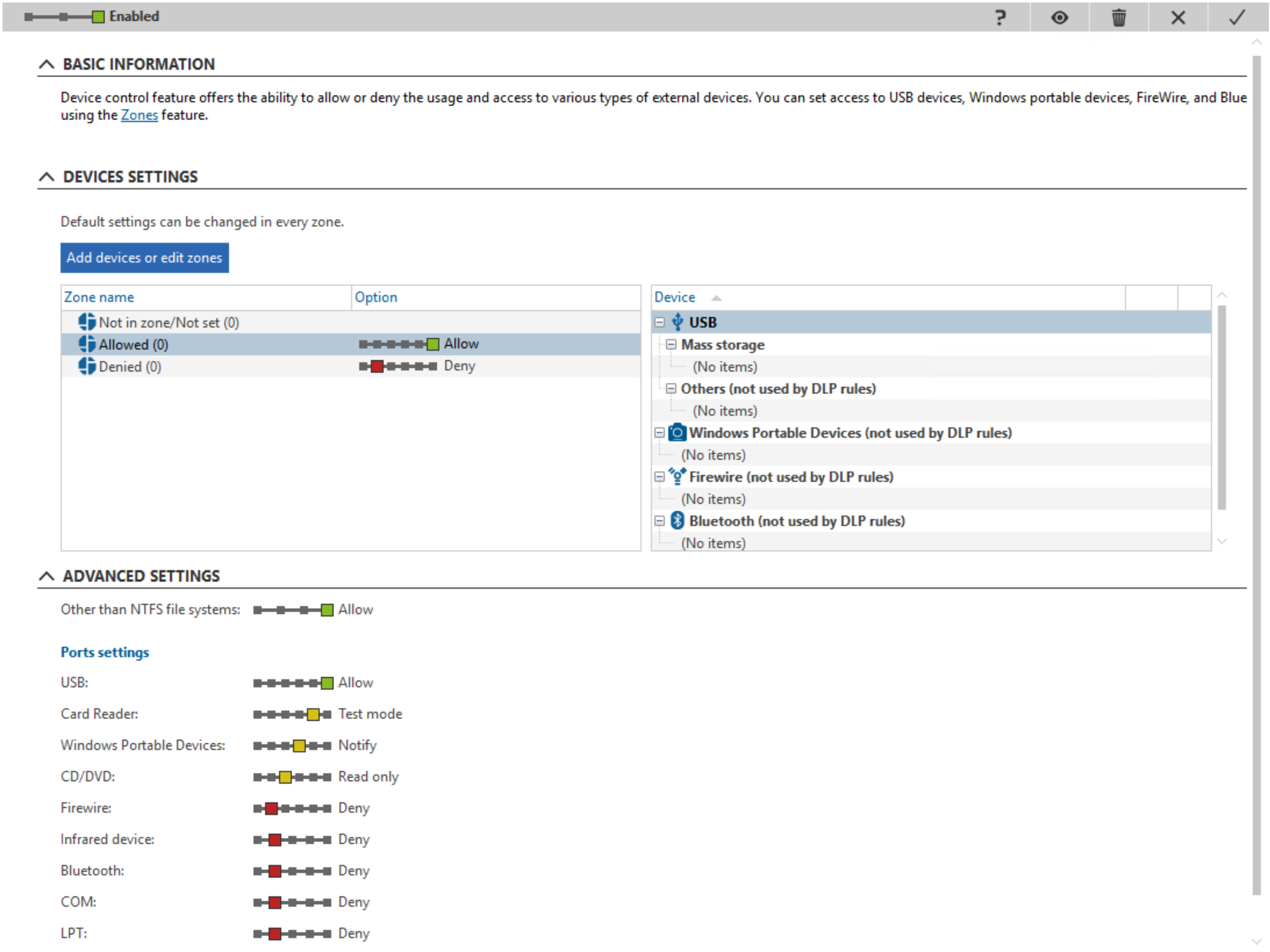
- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was made.
- *Application* – name of the application which used the access path or disk.
- *Source* – the name and path of the file 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*.
- *Action* – name of action performed: *Enable, Test mode, Notification, Disable, Encrypt.*
- *Source type* – whether the source path to the file is: *Local, Network-based, USB, FTP, CD/DVD, Other devices.*
- *Source device* – name of source device.
- *Destination type* – whether the destination path to the file is: *Local, Network-based, USB, FTP, CD/DVD, Other devices.*
- *Destination device* – name of target device.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.6.6 Device control

Using the Device control, you can enable or disable the use of and access to various types of external devices. Access to USB, Bluetooth, FireWire devices and portable Windows-system-based devices can be operated using Zones. Print control is used for managing the printers.

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



BASIC INFORMATION

Device control feature offers the ability to allow or deny the usage and access to various types of external devices. You can set access to USB devices, Windows portable devices, FireWire, and Blue using the Zones feature.

DEVICES SETTINGS

Default settings can be changed in every zone.

Zone name	Option
Not in zone/Not set (0)	
Allowed (0)	Allow
Denied (0)	Deny

Device
USB
Mass storage
(No items)
Others (not used by DLP rules)
(No items)
Windows Portable Devices (not used by DLP rules)
(No items)
Firewire (not used by DLP rules)
(No items)
Bluetooth (not used by DLP rules)
(No items)

ADVANCED SETTINGS

Other than NTFS file systems: Allow

Ports settings

USB:	Allow
Card Reader:	Test mode
Windows Portable Devices:	Notify
CD/DVD:	Read only
Firewire:	Deny
Infrared device:	Deny
Bluetooth:	Deny
COM:	Deny
LPT:	Deny

Devices settings

In this section, you can specify in more detail the basic properties of the Device control.

- Default devices settings – use this setting to choose how the Device control would initially access the external devices. The following are available options for default setting of the Device control:

  o *Inherit* – settings are inherited from the parent group.

  o *Deny* – reading and writing on the external devices is disabled.

  o *Read only* – the external device can only be read from, but not written to.

  o Notify – when using an external device, the user will see a notification in the dialog box and a corresponding record will be created.

  o *Test mode* – similar behaviour as the previous option *Notify*, but the end user is not informed in any way. A record is made only. This mode is intended for testing the behaviour of the setting.

  o *Allow* – reading and writing on the external devices is enabled.

Unless otherwise set later, these default settings will apply to all external devices.

Under the default setting, there is a list of the zones and devices in these zones. For each zone in the table you can set access right to the external devices in the zone. Options are the same as with the default setting.

Note: Zones can be nested. Setting for the zone at the lower level has a higher priority than the setting for a parent zone.

After clicking on the *Add device or edit zones* button the Zone view will be displayed. Here, you can easily create new zones and manage the content of the current ones. The zone may include the following types of external devices:

Advanced settings

In this section, you can globally specify in more detail the options for accessing individual types of devices or file systems other than NTFS. For example: FAT32, ext3, ext4, etc.

The following access options may be set for the other file systems:

- *Inherit* – settings are inherited from the parent group.
- *Disable* – access to devices with other than NTFS file system will be disabled.
- Read-only – access to devices with other than NTFS file system will be enabled for reading only.
- Enable – access to devices with other than NTFS file system will be enabled.

Note: This setting has the highest priority of all the settings in this view.

For each type of external device (port) you can set the same access options as those listed for the default device settings: *Inherit, Disable, Read only, Notify, Test mode.*

Types of devices (ports):

- USB
- Card reader
- Windows portable devices
- CD / DVD
- FireWire
- IrDA
- Bluetooth
- COM
- LPT

Note: Ports settings has a lower priority than the zone setting. For example, if USB ports are disabled in the port settings but enabled for a certain zone, the use of USB ports will be enabled in that particular zone.

Visualization

There are records about access to devices defined in settings mode. There are following charts in the visualization mode:

- *Top users* – a chart containing the users who have the most records.
- *Top actions* – a chart containing proportions of executed actions with external devices.
- *Most used device types* – a chart containing proportions of used device types.
- *Top security policies* – a chart containing the most applied security policies.
- *The most blocked users* – chart contains the users who have been blocked the most.

Each record contains several types of information represented by 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. After clicking the description, detailed information on the device will be displayed. Here you can specify what zones the device shall belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- *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.
- *Security policy* – jaká bezpecnostní politika byla prí akci aplikována.
- *Application* – in what application was v jaké aplikaci došlo k akci.
- *Restriction reason* – what restriction setting was used when access to an external device was denied: *Port, Zarízení, Souborový systém*.
- Interface type – the type of external device: *USB, Bluetooth, FireWire, IrDA, LPT, COM*.

You can learn more about the visualization interface in the chapter *Visualization mode*.

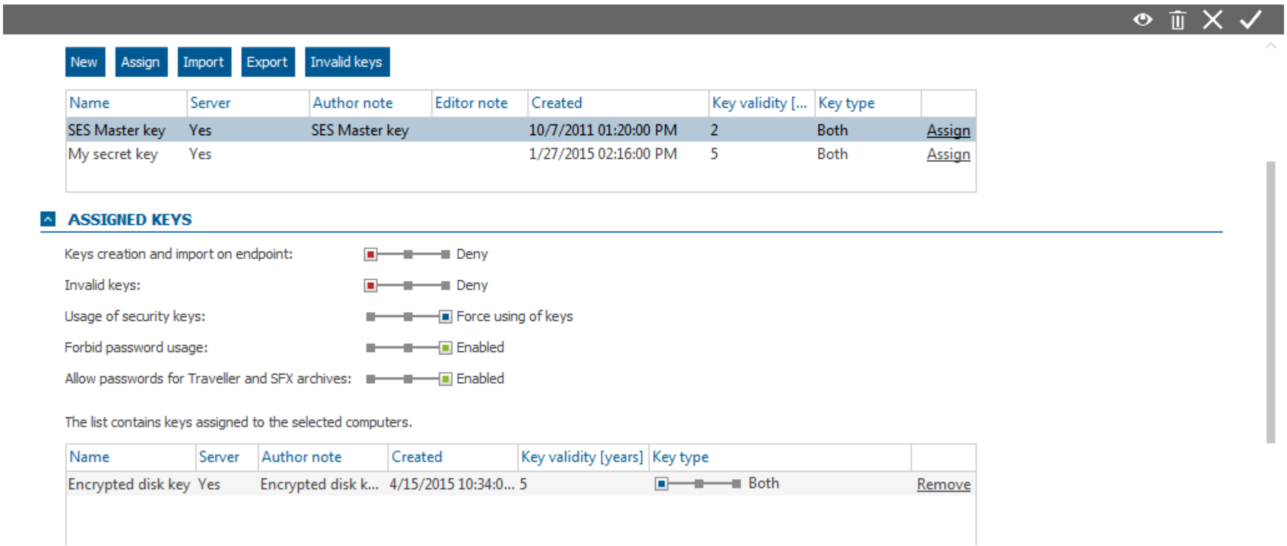
4.6.7 Encrypted disks

In the section *DLP ->Disk Encryption* you have access to administration, creation, allocating or removing encrypted client disks.

4.6.7.1 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!



Name	Server	Author note	Editor note	Created	Key validity [...	Key type	
SES Master key	Yes	SES Master key		10/7/2011 01:20:00 PM	2	Both	Assign
My secret key	Yes			1/27/2015 02:16:00 PM	5	Both	Assign

ASSIGNED KEYS

Keys creation and import on endpoint: Deny

Invalid keys: Deny

Usage of security keys: Force using of keys

Forbid password usage: Enabled

Allow passwords for Traveller and SFX archives: Enabled

The list contains keys assigned to the selected computers.

Name	Server	Author note	Created	Key validity [years]	Key type	
Encrypted disk key	Yes	Encrypted disk k...	4/15/2015 10:34:0...	5	Both	Remove

Every Safetica security key consists of two sub-keys and a special section for *Bitlocker*:

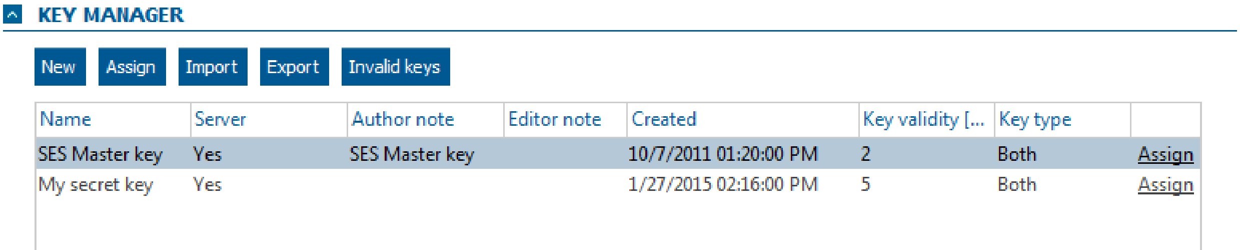
- *Public key (.pubkey)* – used only for data encryption. To access encrypted data, a corresponding Private key must be used. The key must not be used for unlocking encrypted data. It can be freely distributed to other users.
- *Private key (.privkey)* – used only to unlock encrypted data (drives, files, 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.



Name	Server	Author note	Editor note	Created	Key validity [...	Key type	
SES Master key	Yes	SES Master key		10/7/2011 01:20:00 PM	2	Both	Assign
My secret key	Yes			1/27/2015 02:16:00 PM	5	Both	Assign

Use the buttons above the table to perform the following operations:

- *New* - click on this button to start generating the security key. Once completed, enter the detailed information about the key – name, folder to save the key to (public and private part), validity, and general description.

  Note: The length of the generated security key is 4096 bits.
- *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.

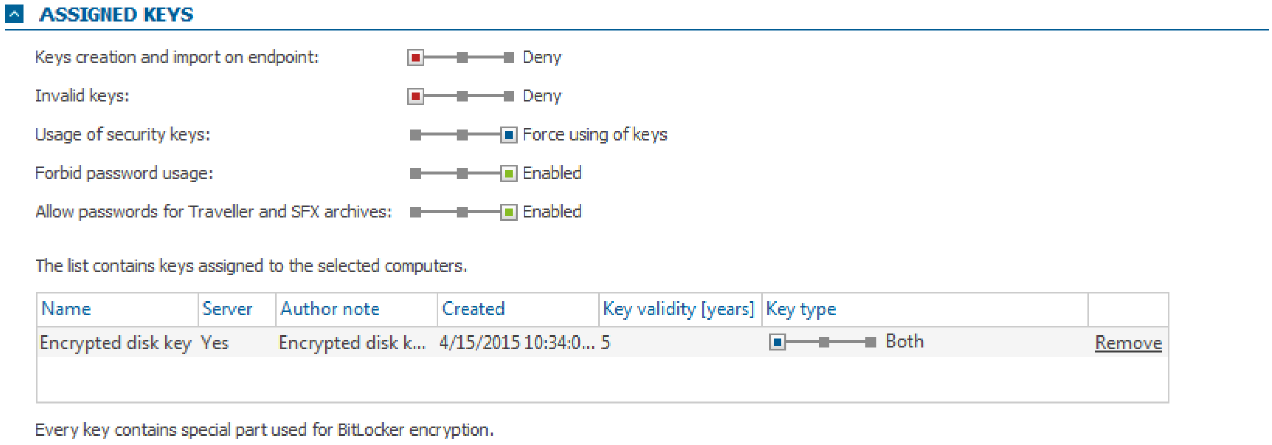
  Warning: When keys are exported, only the public and private keys are exported without the corresponding sections for drives encrypted by Bitlocker. This section can be exported separately for every drive in Encrypted disks in the Bitlocker section (*Encrypted drives -> Bitlocker -> Information -> Export*).
- *Invalid keys* – this opens a dialog with a list of keys whose validity has expired. If their validity is extended, these keys will appear again in the key administrator's list. You can extend the validity by double-clicking the box showing the validity and entering a new validity period (in years). The validity is still counted from the time that the key was created, so if you wish to restore validity, you need to enter a number of years which, when added to the number of years since key creation, will exceed the current date.

The security key record contains the following data:

- *Name*
- *Server* – whether the security key was created on the server or the 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.



ASSIGNED KEYS

Keys creation and import on endpoint: Deny

Invalid keys: Deny

Usage of security keys: Force using of keys

Forbid password usage: Enabled

Allow passwords for Traveller and SFX archives: Enabled

The list contains keys assigned to the selected computers.

Name	Server	Author note	Created	Key validity [years]	Key type	
Encrypted disk key	Yes	Encrypted disk k...	4/15/2015 10:34:0...	5	Both	Remove

Every key contains special part used for BitLocker encryption.

For the keys assigned you can specify the following settings:

- *Keys creation and import on endpoint* – here you can enable or disable the import and creation of security keys on the workstation. The user will be able to use only the security keys assigned to the server.
- *Invalid keys* – here you can specify what happens when a user attempts to use an expired security key.

  - o *Allow with warning* – usage of the security key (e.g. connection of an encrypted disk, creation of an encrypted archive, etc.) will be allowed, but a warning will be sent to the console. The sending must be set in the Warnings section, otherwise nothing will be sent.
  - o *Inherit* – settings are inherited from the higher-level group.
  - o *Disable* – usage of an invalid security key will be disallowed.
- *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.

Visualization

The visualisation mode shows a table with detailed information about operations performed with security keys.

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

4.6.8 BitLocker devices

This function allows encrypting USB flash drives using BitLocker. The access to encrypted devices can be assigned to individual users, computers or groups.

Device encryption

You can encrypt USB flash drives when they are connected to a computer where the console or the client is installed.

Note: The computer with the console where encrypting will be performed must support BitLocker function (Windows 7 Ultimate, Enterprise, Windows 8/8.1 Pro and higher, Windows 10 Pro and higher, Windows Server 2008 R2 and higher).

You can add an external device to the list with the BitLocker devices from the Zones using the *Add* button.

A device can be removed from the list using the *Remove* button.

Encryption on the endpoint with the client

1. Go to the tab *DLP -> Encrypted devices*.
2. Assign the flash drive to the user, computer or group.
3. Set *Encrypt* for the flash drive by the slider in *Action* column.
4. Flash drive will be encrypted upon connection to the computer to which was the flash drive assigned.

Encryption on the computer with the console

1. Launch the console with the administrative rights.
2. Plug the flash drive in the computer on which you are running the console.
3. Go to the tab *DLP -> Encrypted devices*.
5. Set *Encrypt* for the flash drive by the slider in *Action* column. Flash drive will be encrypted.

Assigning access

Perform assigning using the *Assign* slider in the table with the list of devices. The access to encrypted flash drives is only set for users, groups and computers marked in the tree of users.

Access to the encrypted flash drive

On computers with the storage device assigned the flash drive is unlocked (made accessible) automatically after its connection. On computers without the flash drive assigned or where no client is installed you will need to enter the password to access the flash drive.

Note: USB flash drive will be automatically unlocked even on the compute with installed console.

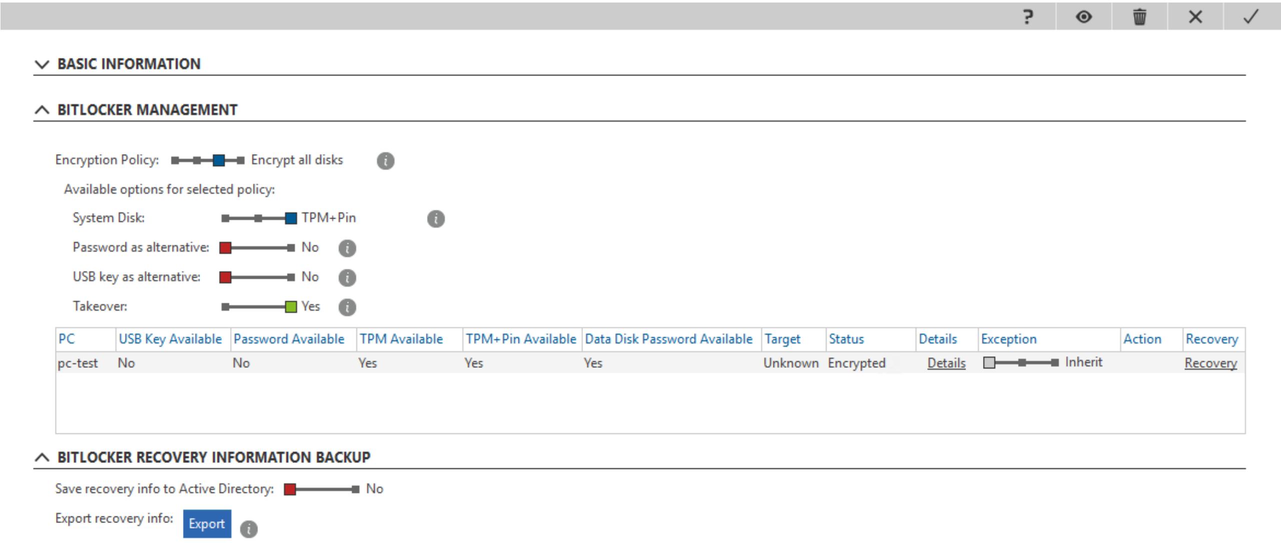
Export of passwords

The passwords for flash drives can be exported. Select in the list the respective flash drives that are encrypted, click on Export and save the CSV table with the passwords.

4.6.9 BitLocker disks

BitLocker Drive Encryption serves for physical encryption of system and non-system disks in computers. It is a Microsoft tool. More information on BitLocker is available at https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx.

Note: Bitlocker Drive Encryption can only be used at end workstations with Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro and Windows 8 Enterprise, Windows 10 Pro and newer Windows operating systems including server versions. Bitlocker is not compatible with dynamic disks.



BASIC INFORMATION

BITLOCKER MANAGEMENT

Encryption Policy: Encrypt all disks

Available options for selected policy:

System Disk: TPM+Pin

Password as alternative: No

USB key as alternative: No

Takeover: Yes

PC	USB Key Available	Password Available	TPM Available	TPM+Pin Available	Data Disk Password Available	Target	Status	Details	Exception	Action	Recovery
pc-test	No	No	Yes	Yes	Yes	Unknown	Encrypted	Details	Inherit		Recovery

BITLOCKER RECOVERY INFORMATION BACKUP

Save recovery info to Active Directory: No

Export recovery info: Export

BitLocker management

Encryption policy

Here you can set the BitLocker policy The selected policy will be applied and implemented in computers listed below if they support the selected policy. Alternatives can be chosen for those that do not support it. The following policies are available:

- *Decrypt* – decrypts the system disk and all data disks.
- *Encrypt all disks* – encrypts the system disk using the selected method (described below) and encrypts the data disk using randomly generated keys. Data disks will be unlocked automatically after unlocking the system disk.
- *Encrypt data disks* – only data disks are encrypted.

Edit one of the following options based on the selected policy:

- *System disk* – setting the manner of unlocking the system disk:
  - o *Password* – when starting the PC, the user is prompted to enter the password set by the user when applying the policy.
  - o *TPM* – the system disk is unlocked automatically in the start. The password is stored in a TPM security chip (https://en.wikipedia.org/wiki/Trusted_Platform_Module).
  - o *TPM+P*in – the password is stored in a PIN-protected TPM security chip. When starting the PC, the user is prompted to enter a PIN set by the user when applying the policy.
- *Password as an alternative* – a password will be set as an alternative method of unlocking the system disk. This can be set only when selecting the TPM and TPM+Pin unlock methods.

  Note: This option is available only on computers running Windows 8 and later versions of the system.
- *USB key as an alternative* – a key stored on a USB drive will be set as an alternative method of unlocking the system disk.

  Note: This option is available only on computers running Windows Vista and 7 and later versions of the system.
- *Takeover* – Safetica takes over management to disks previously encrypted directly by BitLocker without using Safetica. Old login and recovery keys will be deleted and replaced by new ones, compatible with the set policy. If this setting is inactive, some encryption attempts

may end with an error.

List of computers

The list includes all computers that have Safetica installed and contain groups tagged in the user tree. Detailed information on the current status of BitLocker in the relevant computer is indicated for every computer. For example, which particular BitLocker security options the computer supports and whether it is encrypted.

An exception can be set for every computer:

- *Ignore* – the encryption policy will not apply to the relevant computer.
- *Decrypt* – all disks in the relevant computer will be encrypted.

You can set an exception using the switch in the column of the same name.

BitLocker recovery information backup

In this section you can set the backup of recovery information in Active Directory or export the information directly into a selected folder. Backup into Active Directory must be enabled from https://technet.microsoft.com/en-us/library/dd875529(v=ws.10).aspx#BKMK_1.

Note: If the data required for recovery have been exported into the root folder of the connected USB disk, the disk can be used for restoring access to an encrypted disk.

4.7 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.

4.7.1 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.

Settings

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

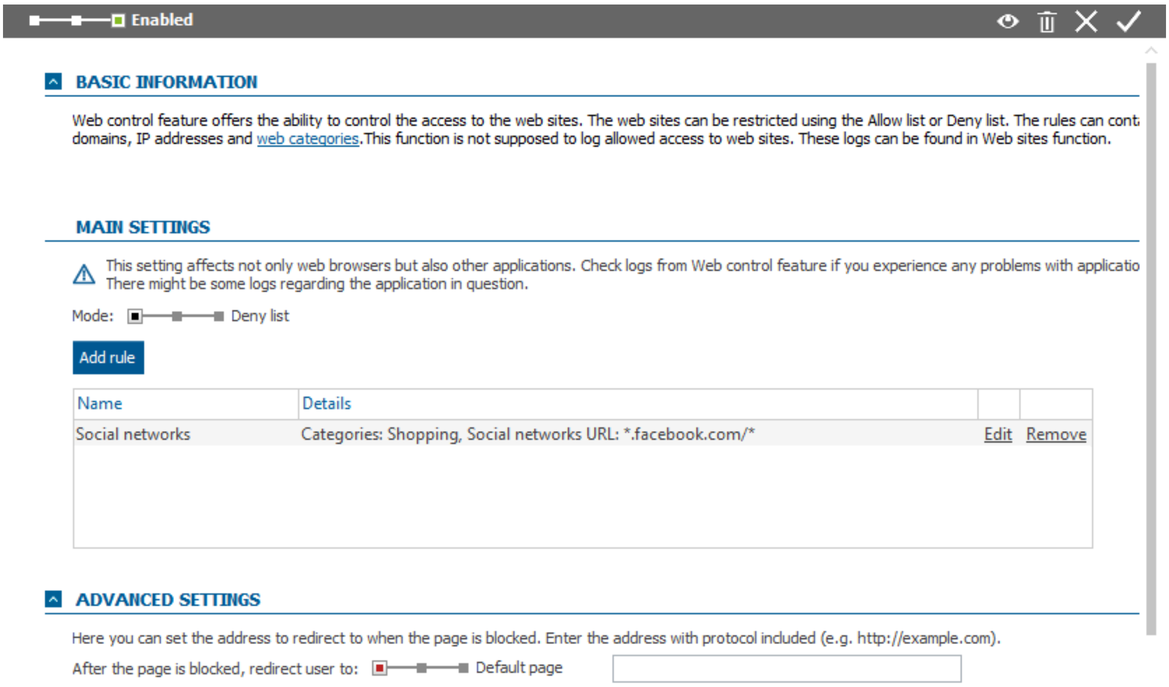
Web control has two modes:

- *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.



Enabled

BASIC INFORMATION

Web control feature offers the ability to control the access to the web sites. The web sites can be restricted using the Allow list or Deny list. The rules can cont domains, IP addresses and web categories.This function is not supposed to log allowed access to web sites. These logs can be found in Web sites function.

MAIN SETTINGS

This setting affects not only web browsers but also other applications. Check logs from Web control feature if you experience any problems with applicatio There might be some logs regarding the application in question.

Mode: Deny list

Add rule

Name	Details		
Social networks	Categories: Shopping, Social networks URL: *.facebook.com/*	Edit	Remove

ADVANCED SETTINGS

Here you can set the address to redirect to when the page is blocked. Enter the address with protocol included (e.g. http://example.com).

After the page is blocked, redirect user to: Default page

Warning: The settings apply not only to web browsers, but also to other applications that access the web. If you have trouble with updates or other network communication with any application, check the Website administration records to ensure that this function has not been blocked.

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. 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.
5. 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.
6. 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 address or *URL* (Uniform Resource Locator) is an address identifying an internet resource. For each address in the list, you can select on what level will the URL rules apply. For example, if you enter www.safetica.com, you can chose from the following options:

- *www.safetica.com* – the rule will only apply to *www.safetica.com*
- **.www.safetica.com/** – the rule will apply to *www.safetica.com* and all pages that include this address. Examples could be *www.safetica.com/AAA/* or *ccc.www.safetica.com/AAA/BBB*
- **.safetica.com/** – the rule will apply to all pages that include the address *.safetica.com*. Examples are *www.safetica.com/AAA/* or *ccc.safetica.com/AAA/BBB*
- **.com/** – the rule will apply to all pages that include the address *.com.* This blocks all web-sites ending with .com. Such as *www.safetica.com/AAA/* but also e.g. *www.cnn.com*
- **.www.safetica.** – works the same way as the previous rules.
- **.www.** – works the same way as the previous rules.

By default, the system is set to the first option, which in this example means www.safetica.com.

When entering addresses, you can use the wildcard * (asterisk). For example, if you enter **auto**, the rule will apply to all addresses that include the string *auto.*

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

At the top of the advanced settings, you can set the address to which the user will be redirected after visiting blocked websites.

- *Default page* – the Safetica web page with information about the blocking will be displayed.
- *Custom page* – if you choose a custom page, the end user will redirected to a website which you can enter into the text box next to the slider. Enter the address with its protocol (eg http://www.example.com).

Visualization

There are following charts in the visualization mode:

- *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.

Each record contains several types of information represented by 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.
- *Protocol* – type of internet protocol: *http, https.*
- *Application* – name of the application, which was used to access the blocked web site
- *Application path* – the entire path to the application.
- *Change category* – after clicking the link with this name, a dialog for changing the web site category will open in this column. Select one or more new categories in the dialog and confirm your changes with Select.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.7.2 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.

Settings

In the settings console mode this feature can be enabled or disabled using the slider in the header of this view.

Desktop applications

The process of managing the desktop applications can proceed to work in two modes:

- *Allow list* – in this mode, all applications are disabled by default, and you can specify in the rules which applications/categories of applications you want to allow the user to run.

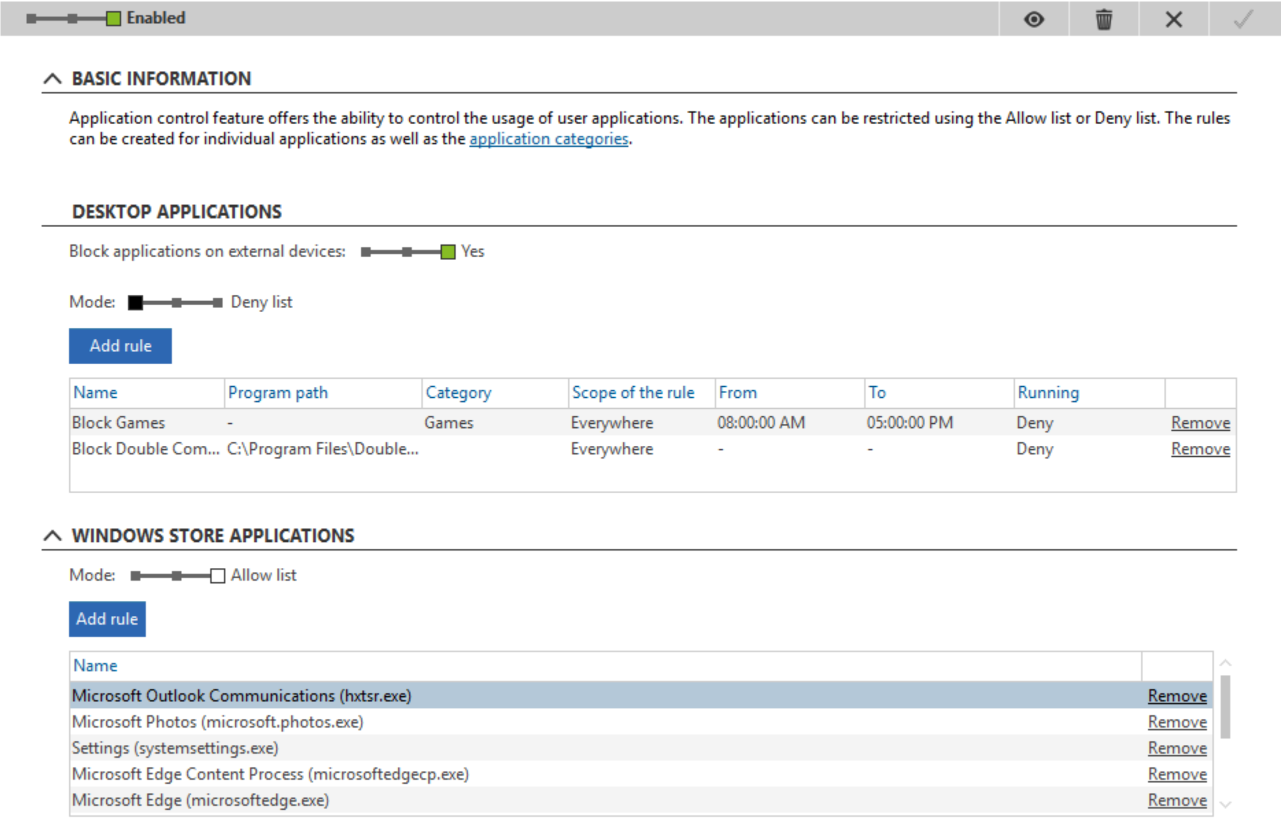
  Notice: If you have selected this mode but not created any rules for allowing certain applications, all the applications that the users launch will be blocked! In this mode, you have complete control over the applications run by the user.

- *Deny list* - In this mode, launching the applications is enabled by default. You can specify in the rules which applications/categories you want to disable or enable for individual cases.

Using the other slider you can enable or disable the blocking of all applications on the connected external devices. If you enable this option, launching all the applications that you have stored on external devices will be blocked. List of allowed applications has a higher priority, therefore the applications allowed by this list will always run according to the rule, regardless of their location on the external device.

Using the *Remove* button you can remove the selected rule.

You can edit the selected rule by double-clicking on it.



BASIC INFORMATION

Application control feature offers the ability to control the usage of user applications. The applications can be restricted using the Allow list or Deny list. The rules can be created for individual applications as well as the application categories.

DESKTOP APPLICATIONS

Block applications on external devices: Yes

Mode: Deny list

Name	Program path	Category	Scope of the rule	From	To	Running	
Block Games	-	Games	Everywhere	08:00:00 AM	05:00:00 PM	Deny	Remove
Block Double Com...	C:\Program Files\Double...		Everywhere	-	-	Deny	Remove

WINDOWS STORE APPLICATIONS

Mode: Allow list

Name	
Microsoft Outlook Communications (hxtsr.exe)	Remove
Microsoft Photos (microsoft.photos.exe)	Remove
Settings (systemsettings.exe)	Remove
Microsoft Edge Content Process (microsoftedgecp.exe)	Remove
Microsoft Edge (microsoftedge.exe)	Remove

Follow these steps to add new rule for desktop applications:

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 running of application* – running of the application will be blocked.
    - *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.

Windows Store Applications

With these settings you can allow or disallow the running of applications obtained from the Windows Store. The settings apply only to Windows Store Applications in supported Windows 8 and higher newer operating systems.

The list of Windows Store Applications can be set in two modes – list of allowed or disallowed applications (see description of desktop applications above).

A new rule for Windows Store Applications can be created in the following way:

1. Click *Add rule*. A dialog with a list of detected Windows Store Applications will open.

   Note: Listed are only applications that have been run at least once on workstations with the client.

2. Check your desired applications and add them to the list by confirming them with *OK*.

Visualization

There are following charts in the visualization mode:

- *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).

Each record contains several types of information represented by 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.
- *Application type* – type of application: *Desktop application, Windows Store application*.
- *Process Started by Application* – the application name (process name) that was launched from an application on which the specific rule is applied (see *Deny running of another application*).

- *Change category* – after clicking the link with this name, a dialog for changing the application category will open in this column. Select one or more new categories in the dialog and confirm your changes with Select.

You can learn more about the visualization interface in the chapter *Visualization mode*.

4.7.3 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

In the console mode, you can turn this function on and off via the slider in the view's header.

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 two 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 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 client .

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. Clicking on the X next to the search field will cancel the highlighting.

After right-clicking on the printer in the list, a menu will open in which you can rename the printer or change its type (physical, virtual).

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.

- *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.

Visualization

There are following charts in the visualization mode:

- *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.

Each record contains several types of information represented by 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 learn more about the visualization interface in the chapter *Visualization mode*.

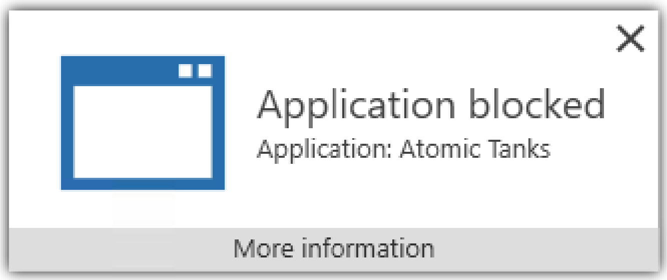
5 Client

5.1 Notification Dialogues

Safetica displays various notifications and messages to users, informing them about prohibited or permitted activities using notification dialogues.

The dialogues display in the lower right corner of the desktop. There are several types of notification dialogues. Each dialogue requires different interaction with the user (confirmation, rejection, selection from options or paths).

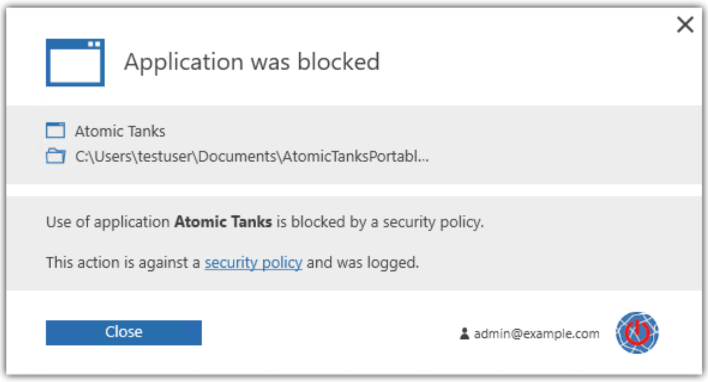
Example of a notification dialogue:



Application blocked

Application: Atomic Tanks

More details will be displayed after clicking on *More information*:



Application was blocked

Atomic Tanks

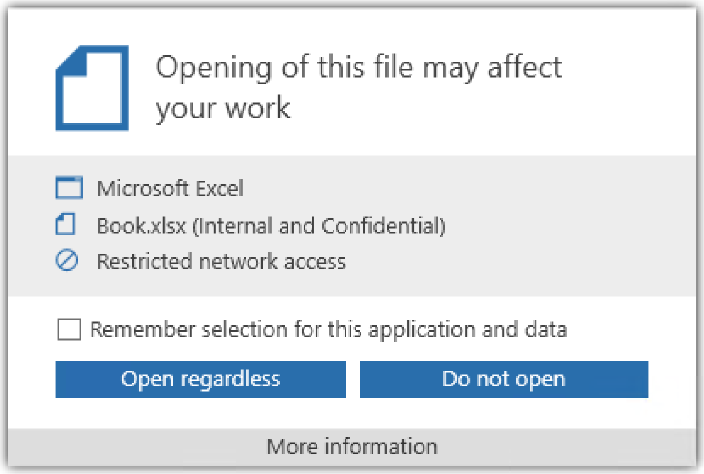
C:\Users\testuser\Documents\AtomicTanksPortabl...

Use of application **Atomic Tanks** is blocked by a security policy.

This action is against a security policy and was logged.

Notification when working with protected data

When the user opens data protected by the security policy, the information dialog will appear:

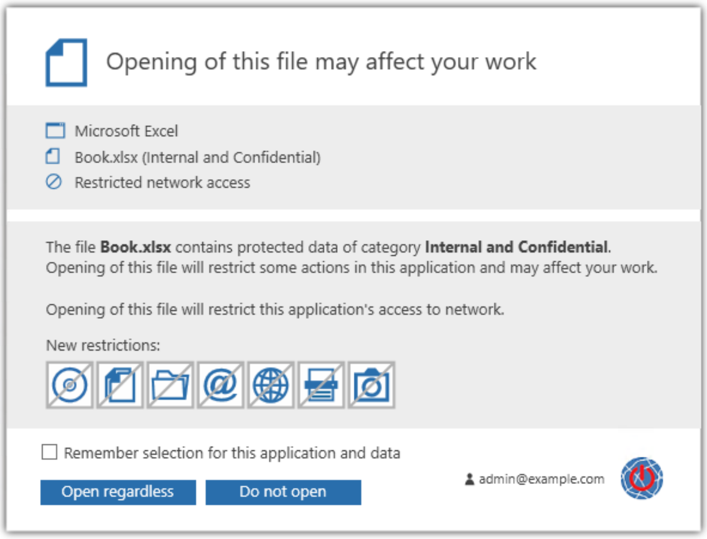


Opening of this file may affect your work

Microsoft Excel
Book.xlsx (Internal and Confidential)
Restricted network access

☐ Remember selection for this application and data

Clicking on the *More information* displays more details about restrictions applied on the application:



Opening of this file may affect your work

Microsoft Excel
Book.xlsx (Internal and Confidential)
Restricted network access

The file **Book.xlsx** contains protected data of category **Internal and Confidential**. Opening of this file will restrict some actions in this application and may affect your work.

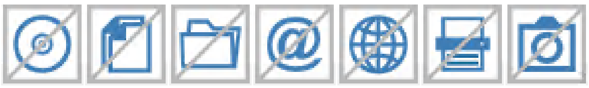
Opening of this file will restrict this application's access to network.

New restrictions:

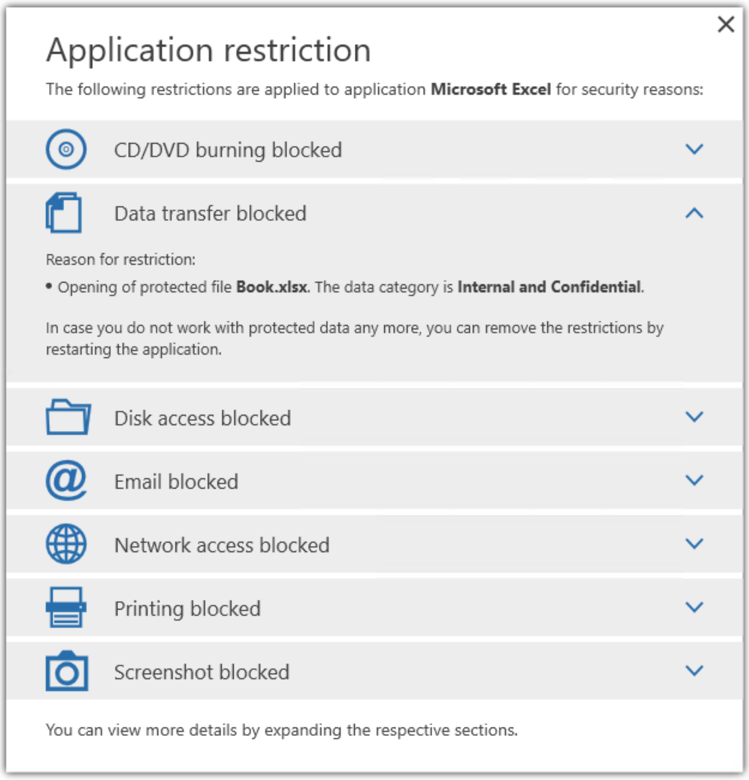
☐ Remember selection for this application and data

admin@example.com

The following icons representing prohibitions or restrictions in the application while working with protected data:



Clicking on the icons displays an explanation of the individual prohibitions or restrictions:



Application restriction

The following restrictions are applied to application **Microsoft Excel** for security reasons:

CD/DVD burning blocked

Data transfer blocked

Reason for restriction:

- Opening of protected file **Book.xlsx**. The data category is **Internal and Confidential**.

In case you do not work with protected data any more, you can remove the restrictions by restarting the application.

Disk access blocked

Email blocked

Network access blocked

Printing blocked

Screenshot blocked

You can view more details by expanding the respective sections.

www.safetica.com

safetica®