

| SAFETICA ONE COMPLETE DOCUMENTATION

SAFETICA ONE COMPLETE DOCUMENTATION

product Safetica ONE (version 10.4)

Author: Safetica a.s.

Safetica ONE was developed by Safetica a.s.

All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.

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: 2023

CONTENT

Introduction

About Safetica ONE

1 Architecture	6
----------------------	---

Installation

1 Automatic installation	9
2 Manual installation	9
Before installation	9
Installing server	10
Microsoft SQL Server settings.....	12
Configuring an Existing SQL server	12
Microsoft SQL Server installation.....	13
Installing a new SQL Server Express	15
Configuring existing SQL Server Express	16
Installing console	17
Installing client	18
3 Initial configuration	19
Batch Installation of Downloader Agent using GPO	21
Manual installation of Downloader Agent	25

Management Console

1 Interface description	26
2 Setting mode	29
3 Records mode	32
4 Management and settings	36
Dashboard	36
Alerts	37
Reports	39
Maintenance	43
Endpoint overview	43
Update and deploy	44
Endpoints deactivation.....	47
Integration settings.....	49
Endpoint settings.....	53
Information collection.....	56
Database management.....	57
Tasks.....	58
Archives.....	60
Maintenance.....	62
Access management.....	63
License management.....	65
Categories.....	66
Computer utilization.....	67
Redirecting client to another server.....	68
Protection against unauthorized manipulation with Safetica client	70
Profile	71
Server settings.....	72
5 Discovery	75
Functions settings	75
Devices	77
Print	78

Network traffic	79
E-mails	80
Files	81
6 Protection	83
DLP logs	83
DLP policies	85
Data categories	85
Sensitive content.....	85
Existing classification.....	86
Context rules.....	86
File properties.....	88
Zones	88
Disk guard	93
Device control	95
BitLocker devices	98
BitLocker disks	99

Endpoint Client

1 Notification Dialogs	101
------------------------------	-----

1 Introduction

Dear user,

Thank you for choosing Safetica ONE to protect your company. In this document, you will find a detailed description of all Safetica ONE components and instructions for using individual features. It will guide you step-by-step through the whole installation and initial deployment, common usage, evaluation of output, and solving the most frequent problems. If you do not find the necessary information here, please contact technical support at <https://www.safetica.com/support/contact-support>.

Safetica ONE is the only mature data security solution designed for scalability and needs of SMBs and enterprises. Get your valuable data under control with great time to value. Go beyond data loss prevention with holistic behavior analysis to detect insider threats even earlier and respond even before they turn into incidents. Leverage insights into company workspace, digital assets, and operations to optimize costs.

If you want to install the software as quickly as possible, please read the *Safetica ONE Installation Manual*. To master basic practices and usage, use the *Safetica ONE Quick Guide*.

Thank you,

Your Safetica Team



2 About Safetica ONE

Safetica ONE is an all-in-one solution for **data loss prevention** and **insider threat protection** that helps you identify security risks, manage data flow, and protect sensitive data. It can also facilitate your compliance with legal regulations. You can be informed about security incidents with instant alerts and customizable reports. Safetica ONE is easy to deploy and affordable for businesses of all sizes.

A more detailed introduction to our new products and modules can be found on our [website](#) or in the [Safetica Knowledge Base](#).

Safetica ONE consists of three main products and two extra modules:

Safetica ONE products

Safetica ONE Discovery

Safetica ONE Discovery focuses on security audits of file operations and transfers. It will help you detect suspicious activities, better understand your security processes, and find out what is happening inside your organization.

Safetica ONE Protection

With Safetica ONE Protection, you can use flexible DLP policies to secure data and prevent leaks of important files across varied devices and platforms. You will also have BitLocker encryption and Safetica Zones at your disposal.

Safetica ONE Enterprise

Safetica ONE Enterprise adds features geared towards big organizations. It enhances your DLP solution with automated third-party integrations, multi-domain support for Active Directory, and workflow management. You will be also able to use your own logo in endpoint notifications.

Safetica modules

With our modules, you can expand your Safetica ONE solution to even more use cases:

Safetica UEBA

Our User and Entity Behavior Analytics module focuses on user activities and insider threats. You can learn more in the [Safetica Knowledge Base](#).

Safetica Mobile

Our Mobile Device Management (MDM) solution focuses on securing data on mobile devices. You can learn more in the [Safetica Knowledge Base](#).

Legacy products

Our new alternative for **Safetica Auditor** is now **Safetica Discovery + Safetica UEBA**.

Based on customer needs, the new alternative for **Safetica DLP** is now either **Safetica Protection + Safetica UEBA**, or **Safetica Enterprise + Safetica UEBA**.

We also offer alternatives for **Safetica Supervisor** features. You can learn more about **Application control** and **Web control** [here](#) and about **Print control** [here](#). If you are still using this legacy module, you can find information about it in the [Safetica Knowledge Base](#).

2.1 Architecture

Safetica is based on client-server architecture. The Safetica Client runs on endpoints and communicates with the server. Together with Safetica Client, the Downloader Agent runs on endpoints and is used to install, update and manage other client components. To manage, set up, and display obtained data, the Safetica Management Console or WebSafetica is used. Data obtained from indi-

vidual endpoints 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.

Safetica 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.

Recommended hardware and software requirements

- 2.4 GHz quad-core processor
- 8 GB RAM and more
- 100 GB of available disk space
- A shared or dedicated server, support of virtual machines and cloud hosting
- Requires connection to server with MS SQL 2012 and higher or Azure SQL
- MS Windows Server 2012 and higher (64-bit only)

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

Safetica Management Console

Safetica Management Console is used to set up and manage the Safetica service (server), the database, Safetica Clients, and Downloader Agents on endpoints. You can also use it to set up all Safetica features on endpoints. 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

Only 64-bit operating systems are supported. Other than that, requirements are the same as for Safetica Client.

WebSafetica

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

Only 64-bit operating systems are supported.

Learn more about its use and deployment in the [Safetica Knowledge Base](#).

Downloader Agent

Downloader Agent is used to manage the Safetica Client on endpoints. It allows remote installation, updating and other management tasks.

Recommended hardware and software requirements

Downloader Agent for Windows: Requirements are the same as for Safetica Client.

Downloader Agent for macOS: Requirements are the same as for Safetica Client.

Safetica Client

Safetica Client provides all the security and monitoring features of Safetica at endpoints. Client service is always launched at operating system startup and provides monitoring, enforces DLP policies and facilitates communication with the database and server.

Safetica Client installation will also install the Downloader Agent, unless it has been installed previously.

Safetica Client continues to work, even if the server is not available (e.g. server is down, or the Safetica Client is on a different network). It uses a local encrypted and protected database where it stores all settings and logs until it is reconnected to the server again.

Note: The minimum supported version of Safetica Client is 9.0.

Recommended hardware and software requirements

Safetica Client for Windows:

- 2.4 GHz dual-core processor
- 2 GB RAM and more
- 10 GB of available disk space
- MS Windows 7, 8.1, 10, 11 (32-bit [x86] or 64-bit [x64])
- MSI installation package
- .NET 4.7.2 and higher

Safetica Client for macOS:

- 2.4 GHz quad-core processor
- 2 GB RAM and more
- 10 GB of available disk space
- macOS 10.10 and higher. To use the full Protection module feature set, we recommend 10.15 and higher.

Database

The database contains endpoint activity and security logs.

Recommended hardware and software requirements

- MS SQL Server 2012 and higher, or MS SQL Express 2017 and higher, or Azure SQL.
MS SQL Express is part of the universal installer and recommended for up to 200 protected endpoints.
- 200 GB of available disk space (optimally 500 GB or more, depending on the range of collected data).
- A shared or dedicated server, support of virtual machines, and cloud hosting. The database can be hosted on one machine together with Safetica Server.

You can find more detailed information about hardware and software requirements in the [Safetica Knowledge Base](#).

3 Installation

Safetica is installed using a universal installer that includes all necessary components. Once you run it, you can choose 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

After launching the installer, you can choose from two options: *Automatic* or *Manual* installation. This guide will only describe the *Automatic installation* which installs the server component, administrative consoles including WebSafetica, IIS web server and Microsoft SQL Server Express database server on the current computer. 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 also WebSafetica. The recommended configuration is a quad-core processor, 8 GB RAM, 100 GB free disk space. This installation is intended exclusively for testing or for a smaller number of Safetica clients installed on end computers.

If you want to adjust the installation parameters or perform the installation for more clients, we recommend choosing the Manual installation. Its description is available in the full manual which you can open in the installer under *Manual installation -> Documentation -> Complete manual*.

After launching the Safetica installer, proceed as follows:

1. Click on *Automatic installation* and confirm the license agreement
2. The next step displays the hardware requirements. Read them and continue.
3. Enter a strong password for the default administrator account *safetica*. Confirm the license conditions of the SQL server and start the installation by clicking *Install*.

Note: WebSafetica uses the Microsoft IIS web server and is available on ports 80 and 443.

Make sure that there is no application running on the computer that would block ports 80 and 443 or configure different IIS ports after installation.

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 endpoints.
6. Use console [to install the client](#) on the endpoints (client installation via console is only possible on computers with 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:

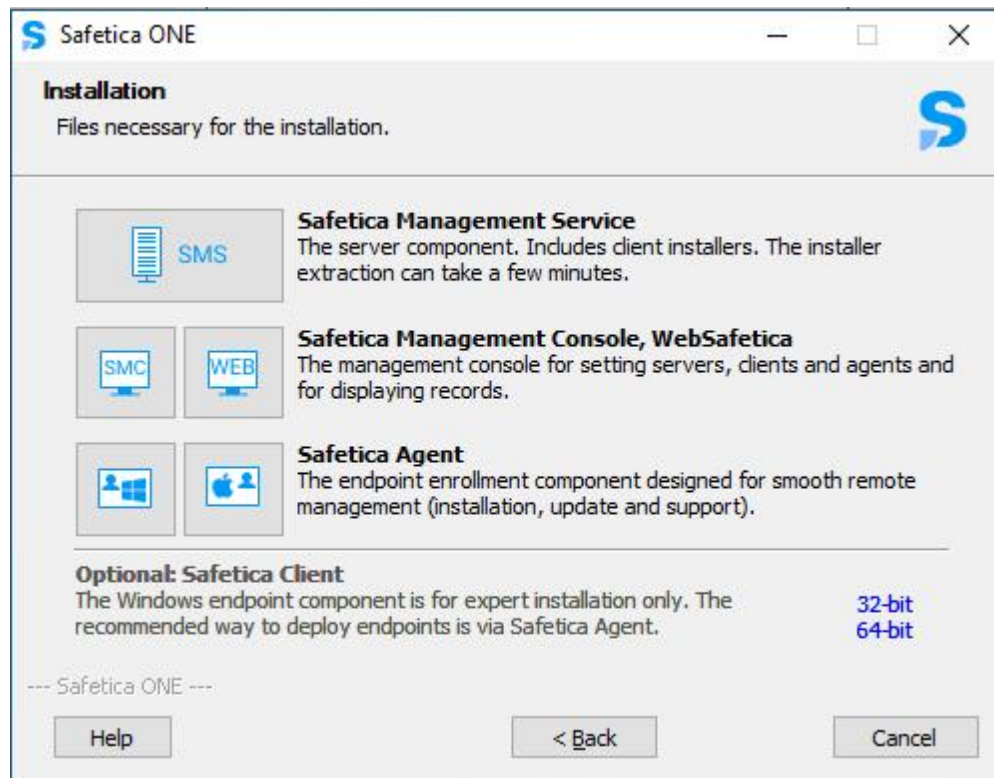
- Decide on what PCs you are going to install the server in your environment. When making the decision, take the following into account:
 - The PC with Safetica server must be able to connect to the SQL server on which the main databases will be stored.
 - Depending on the number of SECs connected and 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.
 - 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.
 - Decide on what PCs you are going to install Downloader Agent in your network.
 - The PC with Downloader Agent must be able to connect to some server in your environment.
 - 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.
 - 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.
- 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).
 - Add exceptions for the process STAConsole.exe on the PCs on which you will install the console.
 - 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.
 - 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.
- 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.



2. Here you several options:

- Run the installation directly from the universal installer by clicking on Run Installer.
- 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 2017 Express. If you are going to install Microsoft SQL Server 2017 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:

- *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*.
- *Send statistics automatically* – select this option to allow console to send anonymous statistical information to Safetica a.s. 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.

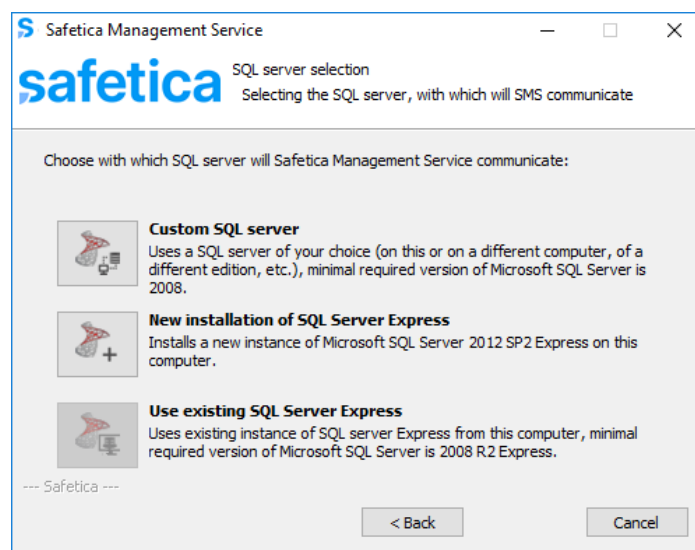
8. Once the installation has successfully completed, verify that the STAService.exe is running (Task Manager -> Services -> STAService – running)
9. Finally, verify that you have added exceptions to your firewall and antivirus for the STAService.exe process and that ports 4438, 4441 and 4442 are not 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 2017 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 2017 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](#).



3.2.2.1.1 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 username.
- *Database name prefix* – adds a prefix in front of the database name. For instance, when using the *db* prefix, the resulting database name will be *db_data*.

Safetica Management Service

safetica 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

Skip >>>

--- Safetica ---

< Back Next > Cancel

2. Click *Verify and save*.

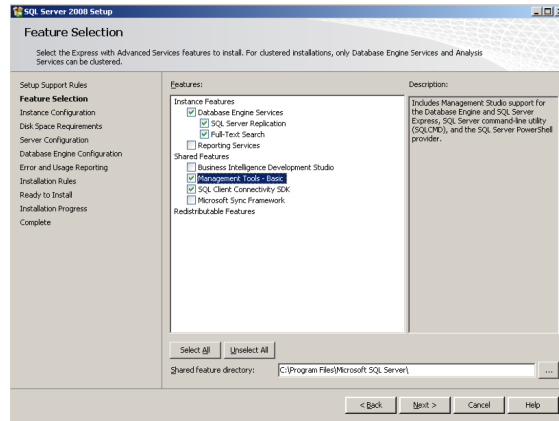
3. Click *Next* and finish server installation. After completing the server installation, a database named *safetica_data* will be created on the SQL server.

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

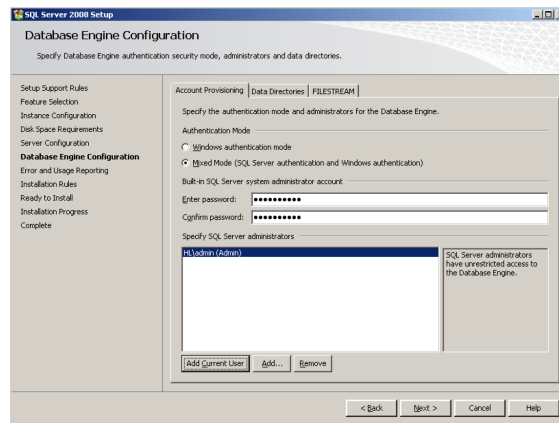
Microsoft SQL Server installation

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

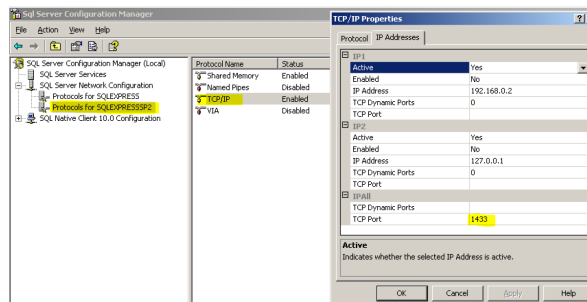
1. Install MS SQL on your server from the following components.



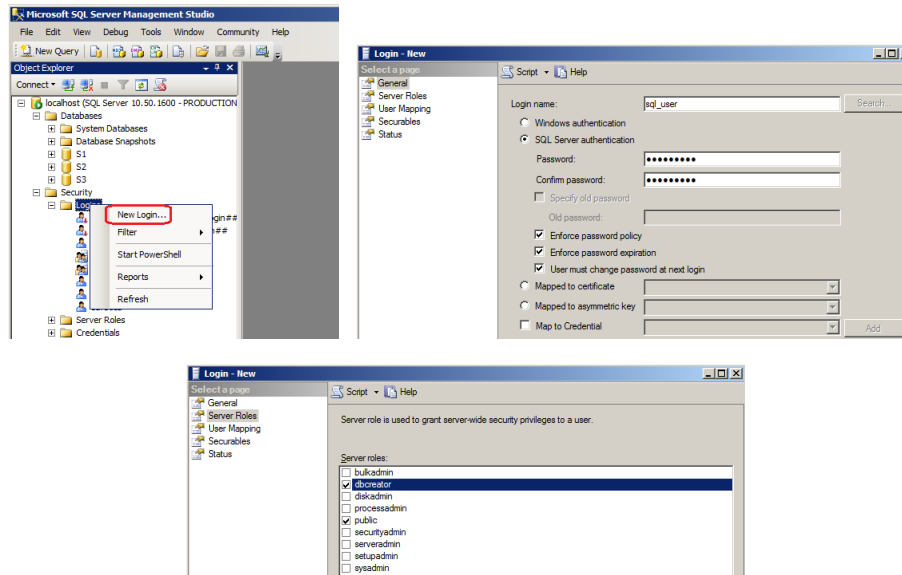
2. Set up Mixed mode authentication in the relevant installation step.



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



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



The connection of server to these databases is set via console in section [Server settings](#).

3.2.2.1.2 Installing a new SQL Server Express

If you do not own any SQL Server, you can install Microsoft SQL Server 2017 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 MS SQL Express server, the maximum number of seats is 250.

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 "S@fetic@2004". The "sa" user will be used for database access.

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.

After clicking the *Use default values* checkbox, 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 2017 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 username and password for the server that will be used for database access. The default user is *safetica* with password *S@fetic@2004*. For security reasons, we recommend changing the default user password *safetica*.

Safetica Management Service
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: *****

Skip >>>

< Back Next > Cancel

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
safetica 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

Skip >>>

< Back Next > Cancel

Continue and [finish server installation](#). After successful completion of the server installation, a database named *safetica_data* will be created on the SQL server.

Note: You can later change the connection to the server via the console in the [Server settings](#) section.

3.2.2.1.3 Configuring existing SQL Server Express

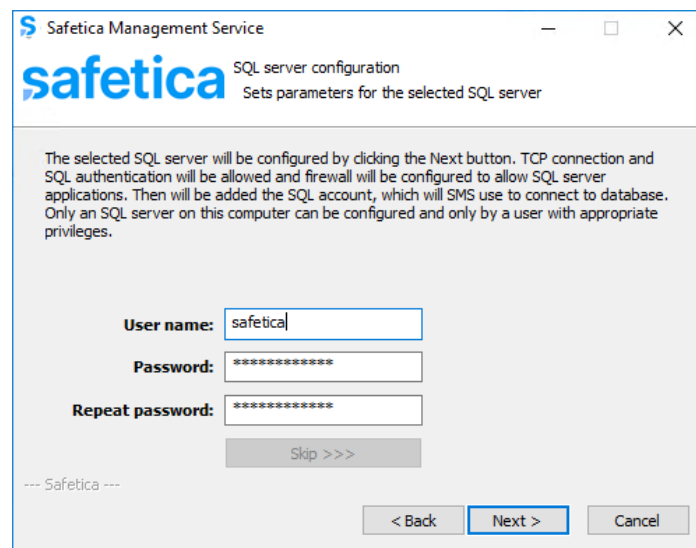
If you have Microsoft SQL Server 2017 Express already installed on the PC where you are installing the server, you can use it for creating the databases. The installer will automatically re-configure the existing SQL server installation on that PC. Server will automatically connect to this instance and 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 MS SQL Express server, the maximum number of seats is 250.

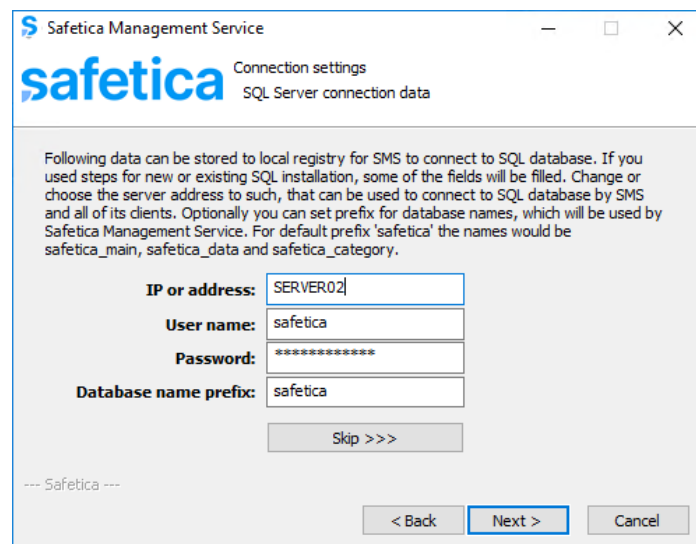
In the first dialog enter the SQL server username and password for the server that will be used for database access. The default user is *safetica* with password *S@fetic@2004*. For security reasons, we recommend changing the default user password *safetica*.



The screenshot shows the 'SQL server configuration' dialog box. It has a title bar 'Safetica Management Service' and a subtitle 'SQL server configuration'. Below the Safetica logo, it says 'Sets parameters for the selected SQL server'. A paragraph of text explains that clicking 'Next' will configure the SQL server, allowing TCP connection and SQL authentication, and adding the SQL account. The form contains three input fields: 'User name' with 'safetica', 'Password' with '*****', and 'Repeat password' with '*****'. A 'Skip >>>' button is below these fields. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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*.



The screenshot shows the 'Connection settings' dialog box. It has a title bar 'Safetica Management Service' and a subtitle 'Connection settings'. Below the Safetica logo, it says 'SQL Server connection data'. A paragraph of text explains that the following data can be stored to local registry for SMS to connect to SQL database. The form contains four input fields: 'IP or address' with 'SERVER02', 'User name' with 'safetica', 'Password' with '*****', and 'Database name prefix' with 'safetica'. A 'Skip >>>' button is below these fields. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

Continue and finish server installation. After successful completion of the server configuration, a database named *safetica_data* will be created on the SQL server.

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 lan-

guage and agreeing to the license terms, go to *Installation -> Safetica Management Console*.

2. Here you several options:

- Run the setup directly from the universal installer by clicking on the *Run installer* button.
- Extract only the 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 Client or Microsoft SQL Server 2017 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 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 DLP policies and ensures that all the features 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 Downloader Agent [on the endpoint](#).
2. Safetica client installation should be performed remotely over *Maintenance -> [Update and deploy](#)*.

Manual installation using the universal installer

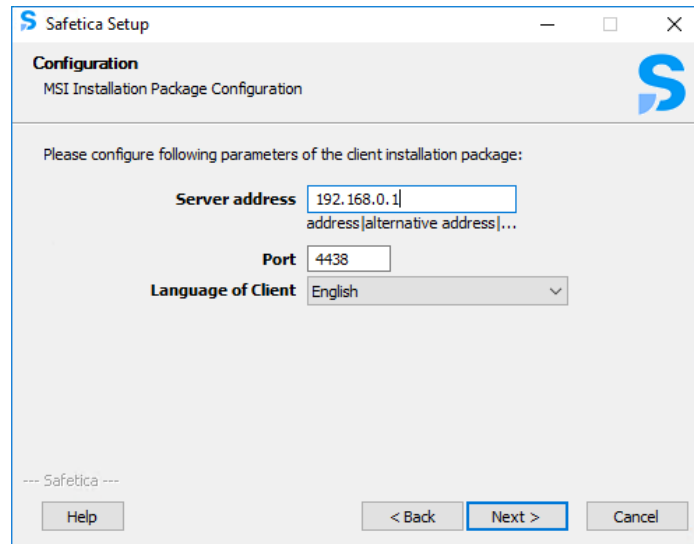
1. Launch the universal installer that you have previously downloaded. After selecting your language and agreeing to the license terms, go to *Installation > Safetica Management Client x86 or x64* – this depends on which operating system version is installed on the endpoint.
2. Here you several options:
 - 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 Client or Microsoft SQL Server 2017 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.



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. If you cannot find the endpoint in the console, verify that the STCService.exe service is running on the endpoint (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.

3.3 Initial configuration

After successfully installing Safetica Management Console and server, the whole system must be set up properly. Only then will you be able to start installing the Downloader Agent and Safetica Client on endpoints. All administration and settings are performed via Safetica Management Console.

Overview of main configuration steps:

1. Start Safetica Management Console. In the dialog 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. Use the default port 4441 for Safetica Management Console log on to the server. Finally, press OK to confirm.

2. After you start Safetica Management Console, the initial configuration wizard is opened. In the second step, you can add your own SMTP server so that Safetica can send you Alerts and Reports.
3. In the third step, you can change your *safetica* service account password for logging into the Safetica Management Console. Click *Continue*.

Note: The service account has full authorization for all Safetica features 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 Maintenance -> [Access management](#) -> User accounts -> Add account.

4. In the fourth step, you can import your company's Active Directory structure. This is only possible, however, when the Safetica server is located within the domain. If you do not use this option, newly connected clients will be placed into the *Unknown* group. You can perform import from Active Directory later in *Profile* -> *Connection* -> [Server settings](#) -> *Active Directory*.
5. The fifth step will help you install the Downloader Agents and Safetica Clients on endpoints. After clicking the *Get Downloader Agent* button, an installation file with Downloader Agent is generated and you can install it at endpoints. You can choose from two options to install the Downloader Agent:
 - [Remote \(batch\) installation](#)
 - [Manual installation](#)

After installing Downloader Agent, you can automatically install and activate Safetica Clients by clicking *Automatically enroll endpoints*. The Safetica Client installation task can be managed from *Maintenance* -> [Update and Deploy](#).

6. In the sixth step, insert the license key or customer ID. You may also enter them later in *Maintenance* -> [License management](#). Safetica features will not be available without the license key or customer ID.
7. In the seventh step, you can insert your company name and email address to which Safetica alerts will be sent.
8. In the eighth step, you can define your company's email zone and specify content rules to

describe sensitive data. You can choose from ID numbers, credit card numbers, IBAN numbers and many others. In this step, you may also enable blocking of dangerous web and application categories (malware, keyloggers, miners etc.).

By default, monitoring of applications, webs, network traffic, devices and printing is enabled.

9. Congratulations! Your Safetica is configured and you can start protecting your data.

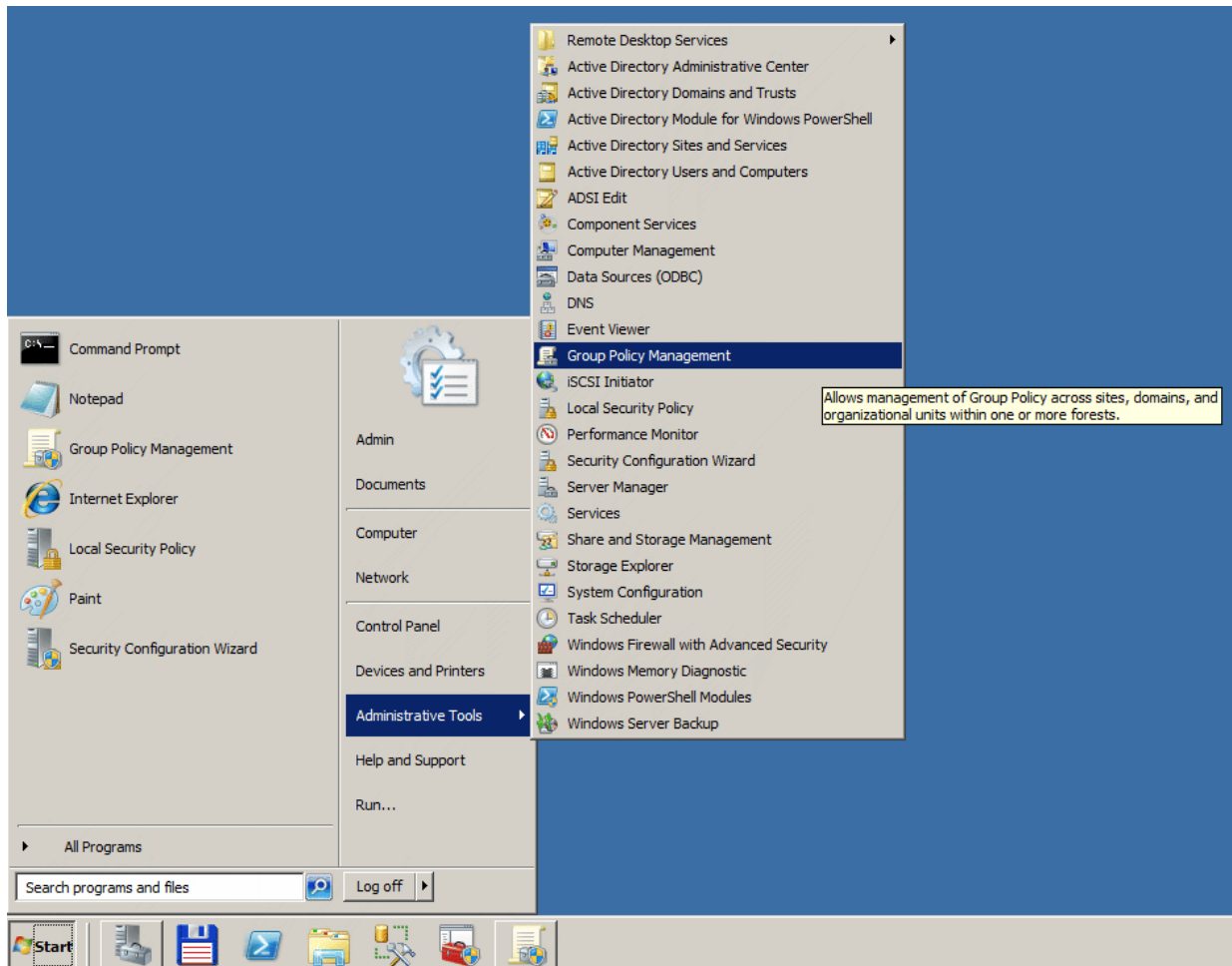
All settings can be changed or viewed in Safetica Management Console after you finish the initial configuration wizard.

3.3.1 Batch Installation of Downloader Agent using GPO

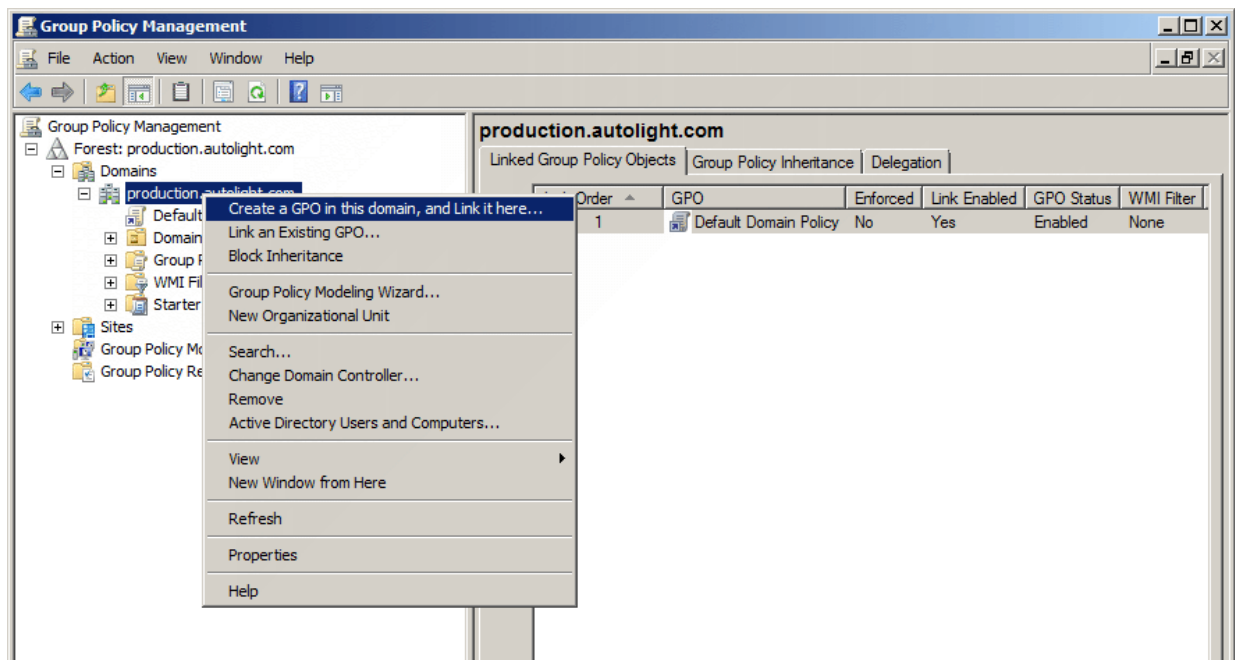
If you are using Active Directory, you can bulk install the Downloader Agent using a Group Policy. To use the bulk installation, it is necessary to extract the relevant MSI package of the Downloader Agent from the universal package.

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.

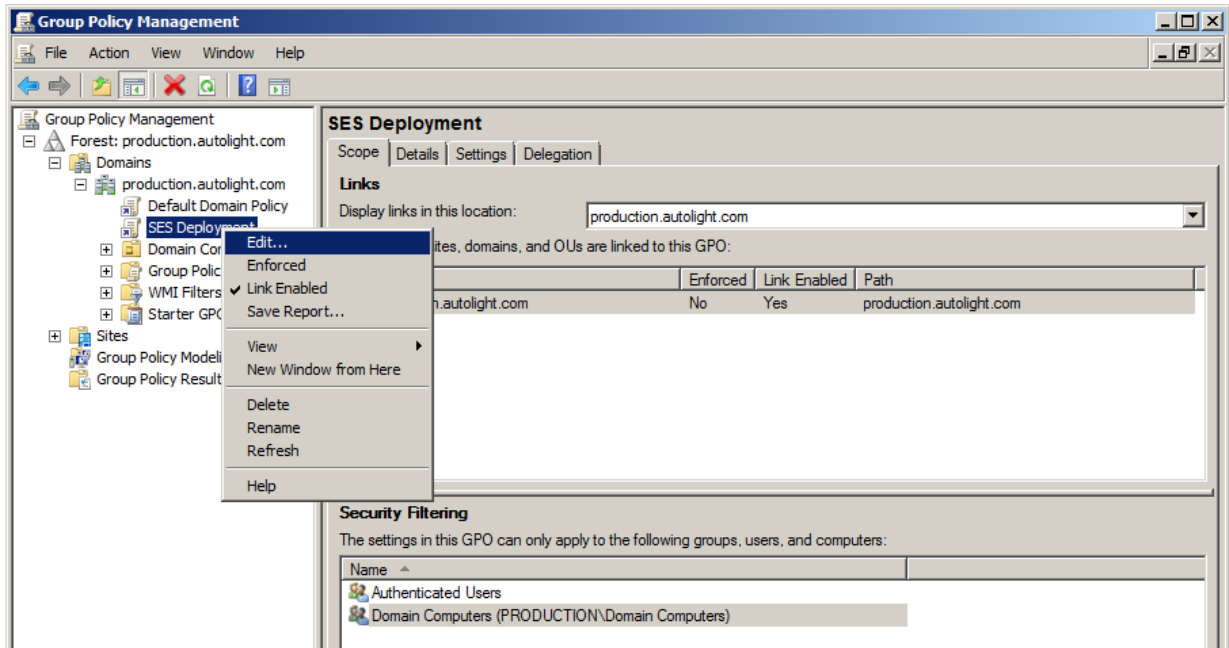
1. Start the Safetica universal installer.
2. Go to *Installation -> Downloader Agent -> Extract installer*. In the installer configuration, enter the server address and port to which the Downloader Agent will connect. Save the installation package on a shared disk or shared directory in the corporate 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*.



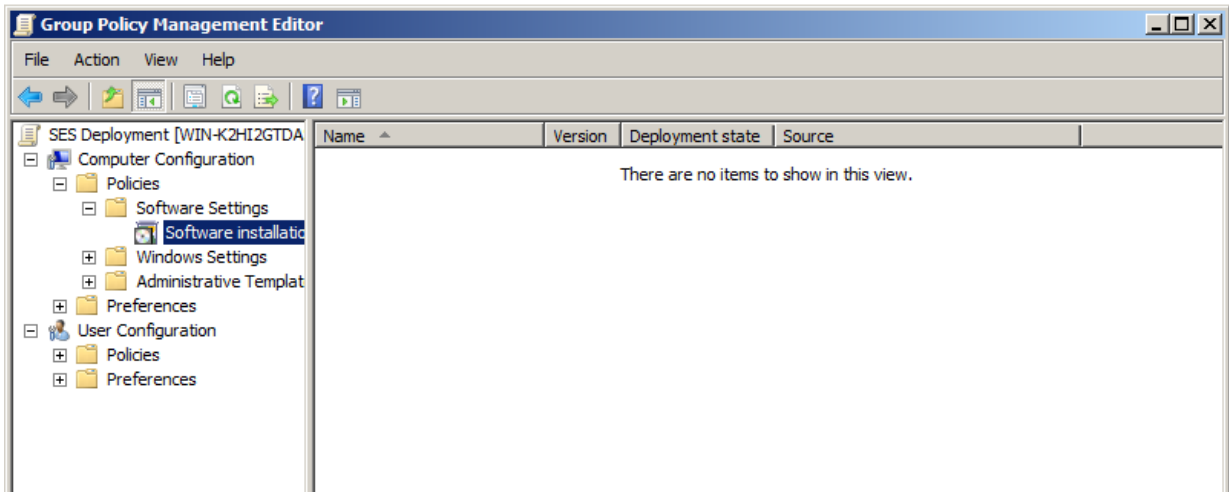
4. Right-click the organizational unit to which you want to deploy the Downloader Agent and select *Create a GPO in this domain and link it here ...*



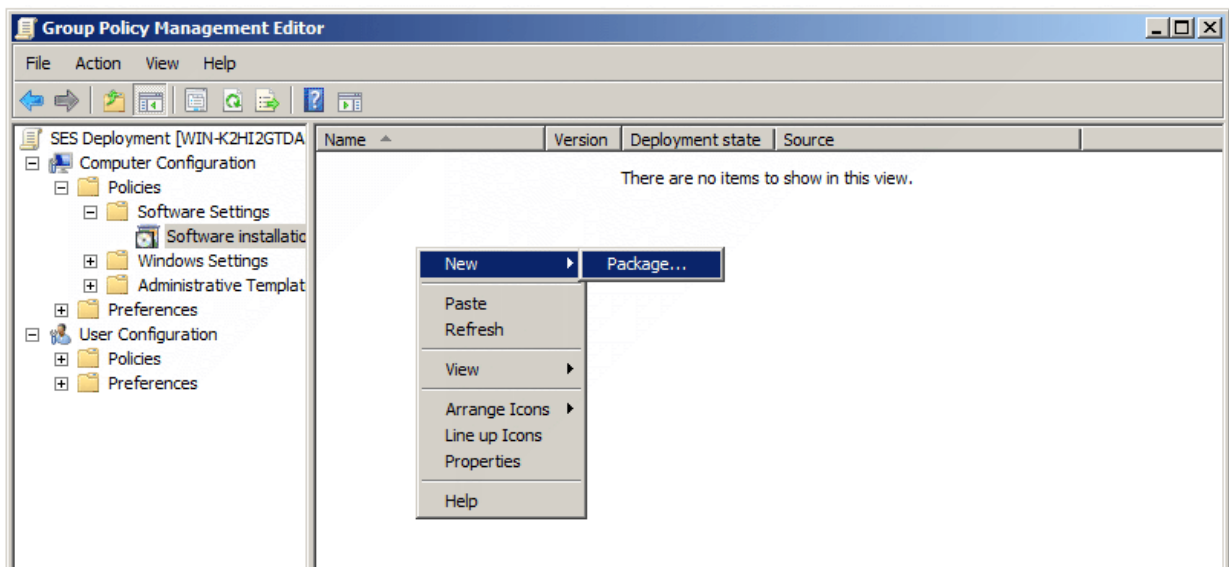
5. Give an arbitrary name to the new object (for example, Safetica Deployment).
6. Select your newly created group policy and right-click to select *Edit*.



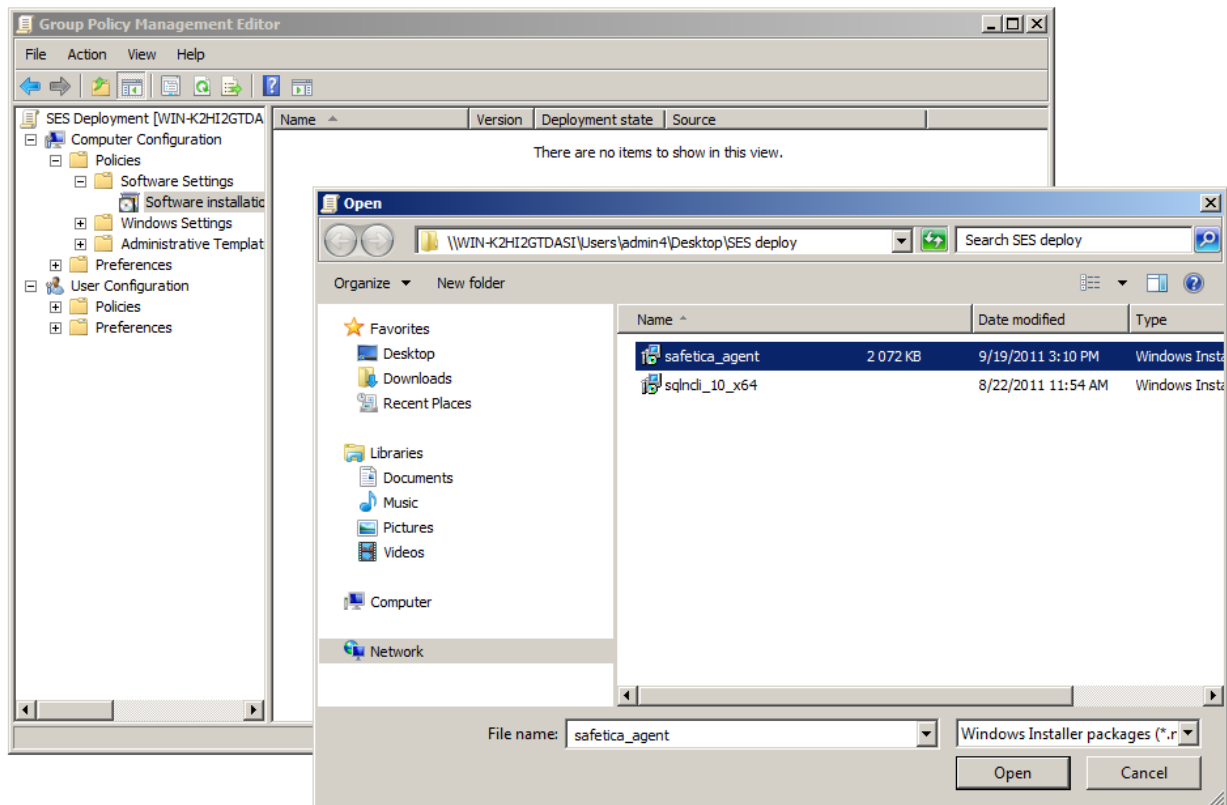
7. In the window that opens, navigate to *Computer Configuration -> Policies -> Software Settings* and click on *Software installation*.



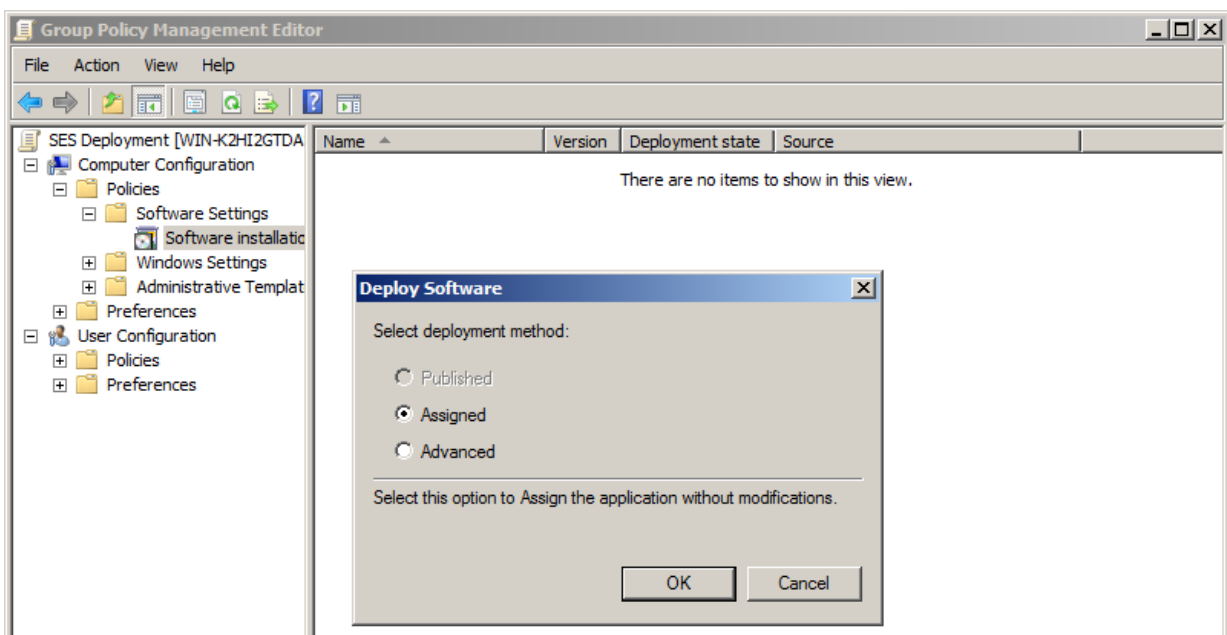
8. Right-click on the window with a list of software and select *New Item -> Package ...*



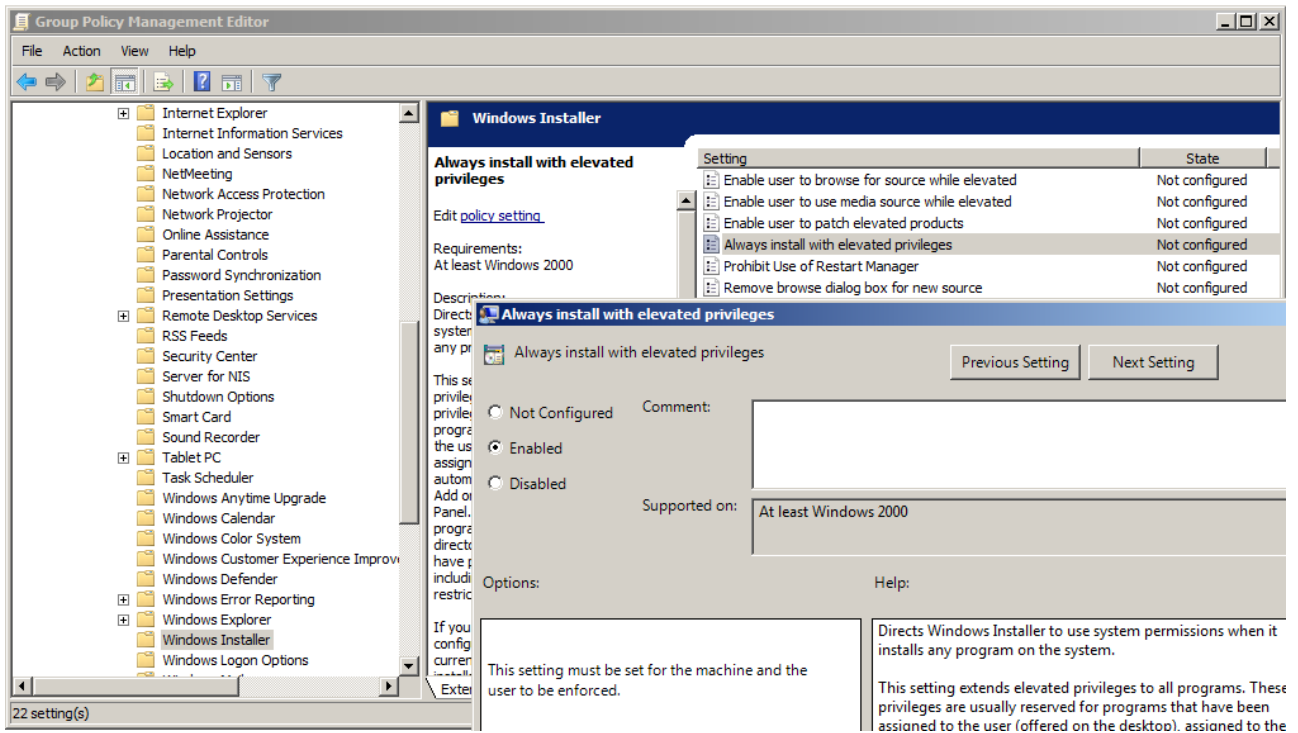
9. In the MSI package selection dialog box, navigate to the shared network folder where you copied the MSI package with Downloader Agent, and select it.



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



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 Downloader Agent will be installed on endpoints properly and without problems.



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

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

3.3.2 Manual installation of Downloader Agent

Downloader Agent is used to install, update and manage the Safetica client at the endpoints. For manual installation of Downloader Agent at the endpoint, proceed as follows:

1. Open the universal installer and select your language. Confirm the license conditions and go to *Installation > Downloader Agent*.
2. Here you have several options:
 - Launch the installation directly from the universal installer by using the *Run installer button*.
 - 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:


- *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 in 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.

- *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 *Next*, Downloader Agent will install on the endpoints and then connect to the server.

Successful Downloader Agent installation can be verified from console, where the user tree will show the  icon with the endpoint name. Client can be remotely installed on endpoints with installed Downloader Agent.

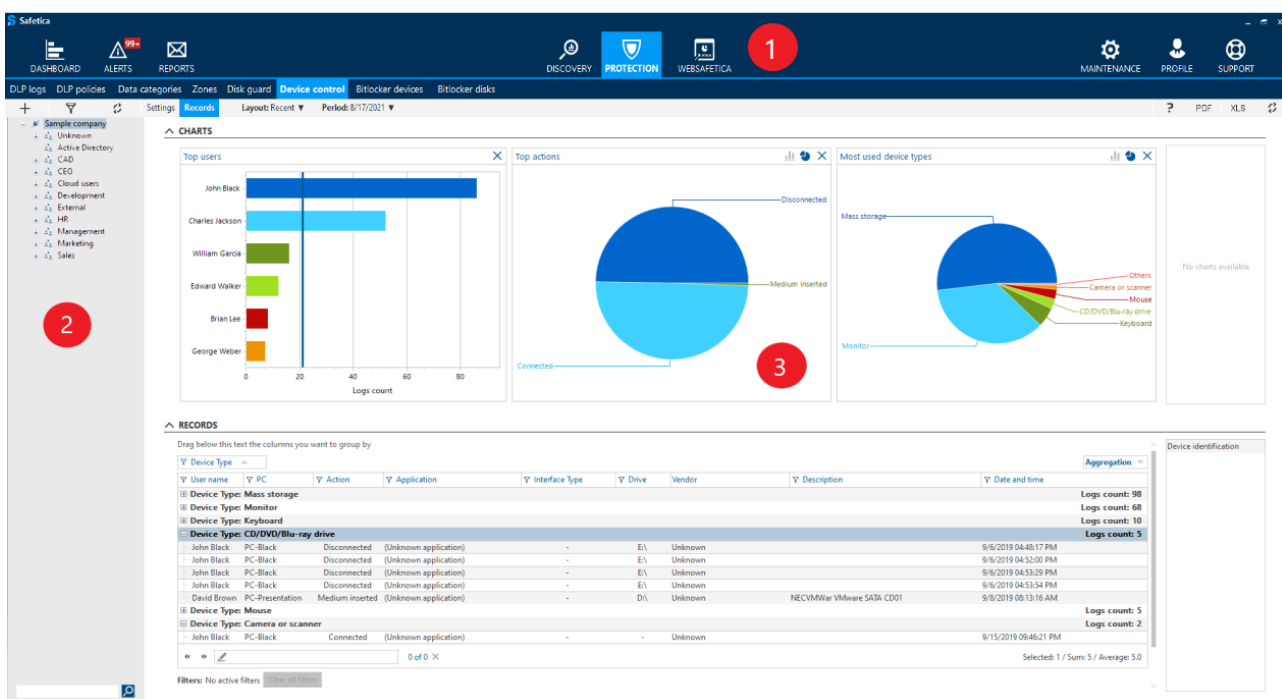
Note: The Downloader Agent component will be automatically installed along with the client.

4 Management Console

All features 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 features 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 Management Console, you will see the following interface:



1. Main menu

In the main menu, you can switch between Safetica features and components. In the gray upper banner, there is a switch used in some features of *Protection* and *Maintenance* to switch between the *Settings* and the *Records* modes. The *Discovery* section only uses the *Records* mode:

- *Settings mode* – settings can be configured for groups, users, or computers highlighted in the user tree. The changes in settings are applied only when saved using  button in the top right corner of the view. The changes may also be canceled by the  button.
- *Records mode* – in this mode, you can see the recorded data, summary reports, charts, and statistics for Safetica features. Data on groups, users and computers highlighted in the user

tree are displayed for a specified time period.

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 features.
- [Alerts](#) - automatic alert setting.
- [Reports](#) - settings for sending regular summary reports.

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

- [Discovery](#)
- [Protection](#)
- [WebSafetica](#)

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

- [Maintenance](#) – management and setup of all Safetica components.
- [Profile](#) – basic settings of your account, such as connection to the server, and custom settings of Safetica Management Console.
- [Support](#) – access to the Safetica Knowledge Base.



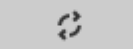



Below the upper toolbar with console controls, there is a list of features. The list changes depending on the currently used module - *Discovery*, *Protection*, or *Maintenance*.

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 connected to server with unknown certificate – connection is allowed.
-  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 [feature settings](#) and [records 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 grayed out: .
-  – computer on which the client is installed and is on-line. If the computer is off-line, its icon is grayed 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. MAC endpoint has the icon .
-  – 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](#).
 -  – redirection has been set.
 -  – 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:
 -  - active management has been set, but client has not yet updated the settings.
 -  - 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. Selected filters are confirmed with the OK button.
- The  button updates the user tree.

3. Display area (view)

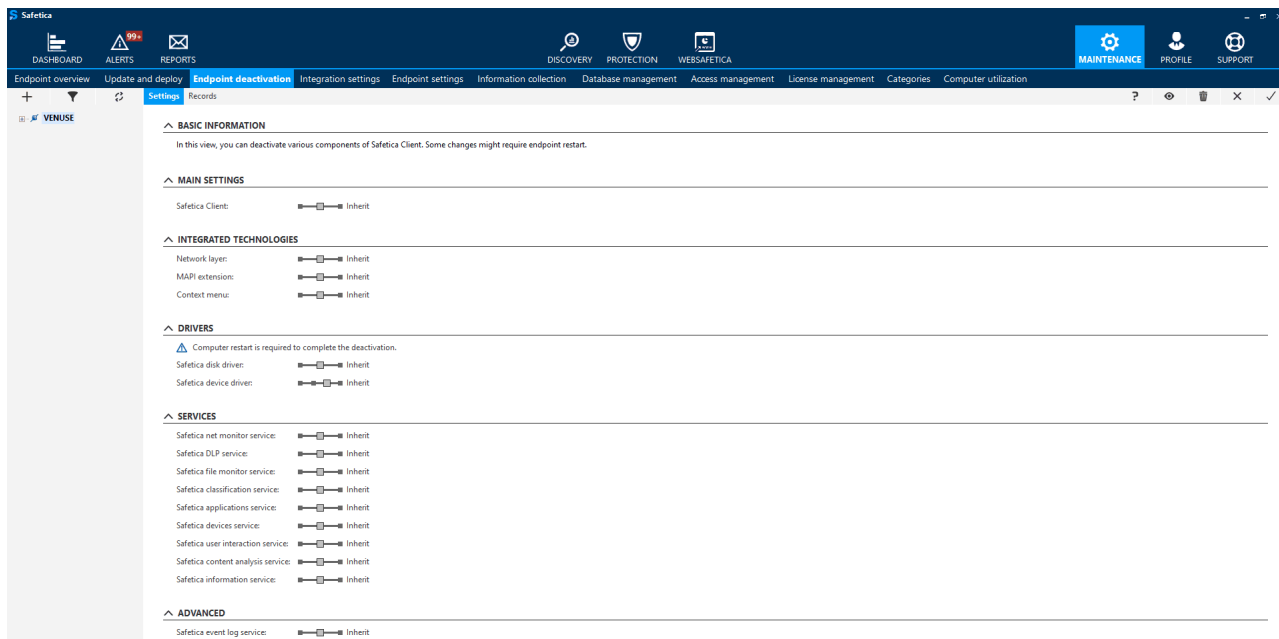
The display area, also called the view area, is used for data visualization and settings of individual features. The contents of the view area change based on which feature you are currently browsing and in which mode (*Settings*, *Records*).

You can switch between individual features by clicking one of the modules in the main menu and then the desired feature.

4.2 Setting mode

In the *Settings* mode, you can configure Safetica features for users, groups, or computers. As the first step, always select the relevant users, groups, or computers in the user tree.

You can enter the *Settings* mode by clicking the *Settings* button in the upper gray banner.





Use the  button to view help for the current feature.

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

Setting mode

You set the following modes for almost every feature:

- *Disable* – the feature is not activated.
- *Inherit* – the feature is not set. Setting is inherited from parent group.
- *Enable* – the feature is activated.

The chosen setting is applied only to users, groups or computers highlighted in the user tree. To apply the settings, you must save the changes by clicking . You can cancel the changes by clicking  in the upper right corner.

Items in the user tree for which the feature is set (*Enable*, *Disable*) are highlighted in blue in the user tree.


Setting inheritance

- You can create settings for users, groups (including branches) and computers via the user tree in Safetica Management 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 computer it contains.
- A setting on the lower level of the user tree is considered stricter, 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.


We have 2 types of settings:

- *Explicit* – a setting made manually for specific users, groups, computers or whole servers.

You can delete an *explicit* setting by clicking .

- *Effective* () – a setting made automatically by joining individual object settings. It is calculated by passing the user tree from the lowest items (high priority) to the root (or server, lower priority) and by joining the individual settings.

Calculation of an effective setting

Safetica Management Console always displays the *explicit setting*. Using the  button, you can display *effective setting* of the current feature and highlighted items in the user tree.

As described above, the setting saved for a user has a higher priority than the settings for the group the user belongs to. The joining of settings 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 apply. 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 applying the "stricter" one. For example:
 - Setting of *Enable* vs. *Disable* is joined to *Enable* (example: enabling the device audit).
 - Interval values are always joined into the stricter interval.
 - For some features, a list of rules is created and you can specify their mode: either Allow list (whitelisting), or Deny list (blacklisting). If this setting differs, the Allow list is applied, since it is stricter (only items listed in it are allowed).
 - If the lists contain rules of the same mode (*Allow list* or *Deny list*), the lists are joined into one.

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* of the user and the given computer.
2. The result of joining the settings for the computer and 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 nor computer. Default settings are described in individual features.
 - Anything that is set for both is applied based on the priority that can be set in [Endpoint settings](#). By default, the computer has higher priority (computer settings are prioritized over user settings).
 - Rule lists are joined if their modes are the same. Otherwise, the list is again selected based on priority.

General rules for using settings

Safetica provides a wide range of possible settings to help you configure your branches to the most minute details. However, a bad approach to settings can result in chaos in the whole system. That is why we recommend more complex settings only to advanced users.

To keep your settings clear and simple, we recommend following these rules:

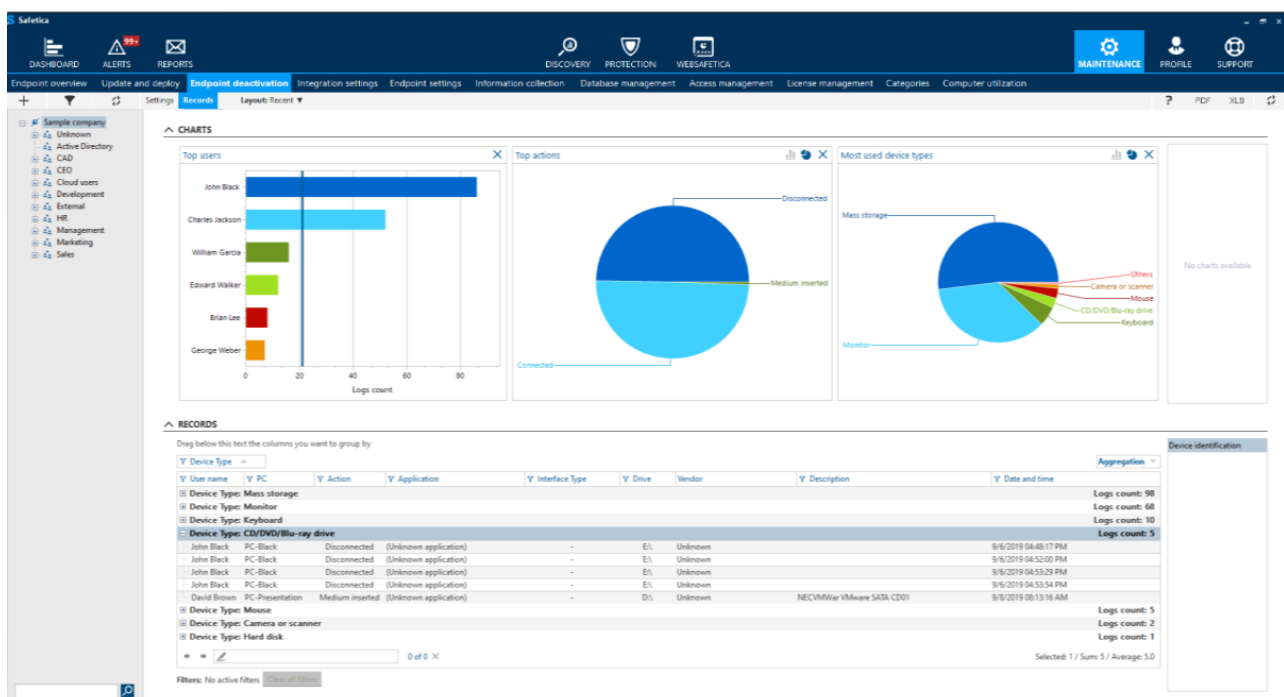
- Apply the settings only to groups. Then assign users or computers to these groups according to what settings you want to apply to them.

Example: There are three departments in your company: Marketing, Development and Support. You want to run different modules and features for the employees in these departments. Do not assign settings to employees by simply selecting them in the tree. Rather, create a group for each department and assign the employees into these groups. Then, create settings for each group. This way, the settings will be applied to the employees as well.

- If it is necessary to set something directly for a user, it means the user is special and does not belong to that group. It is better to create a new group or subgroup for such user, rather 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 assign the respective user to the given group.
- Assigning users to groups helps prevent confusion when moving them to other groups. You might expect a user to inherit the settings from a group you are moving him/her to, however, a higher-priority setting may exist for the user.
- Settings applied to groups take less space in the database than individual settings for each user.


4.3 Records mode

You can enter the *Records* mode by clicking the *Records* button in the upper gray banner. The charts and data displayed for the items selected in the user tree differ based on the selected feature. Some features do not include the *Records* mode.



Records and charts are shown for users, computers or groups highlighted in the user tree. You can display the data acquired during a given time period. To do this, click *Period* on the upper left side of your view. You have several options to choose from:






- *Today* – records are displayed for the current day.
- *Yesterday* – records are displayed for the previous day.
- *Last week* – records are displayed for the last seven days including the current day.
- *Last month* – records are displayed for the last 31 days including the current day.
- *One day* – you can view records for one selected day. You can select whole day or time interval. Confirm selection by the *Confirm date* button.
- *Range* – you can view records for a specific time period. You can select a time interval made of days. You can also specify time within one day. Confirm selection by the *Confirm date* button.

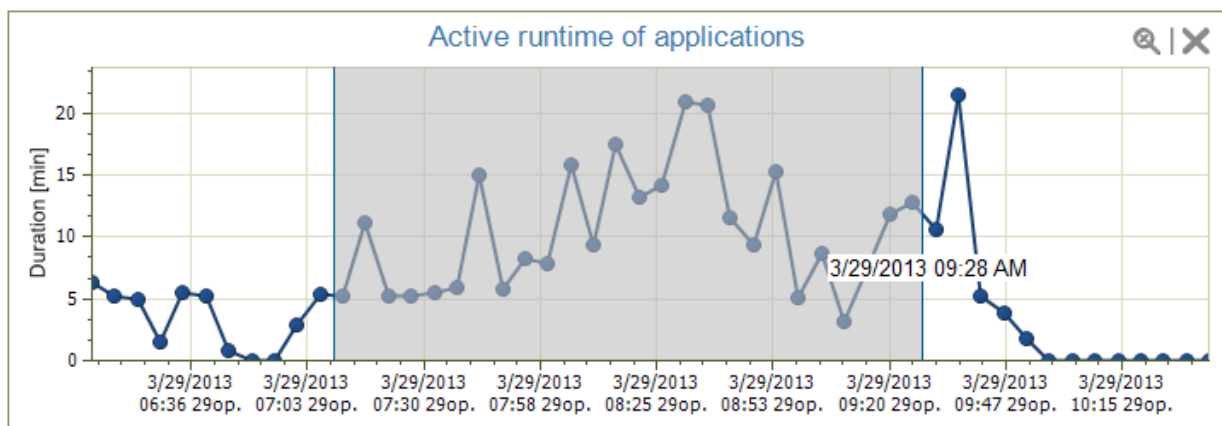
You can refresh records and charts by clicking the  button in the upper right corner.

Use the  button to view help for the current feature.

Charts

The top part of the *Records* mode features an area for showing charts. You can find their list at the right.



- To display the chart, drag and drop it on the right into the viewing area. You can display 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 on the right.
- By clicking the ,  or  buttons, you can change the type of the chart (pie chart, bar chart or line chart).
- Clicking the pie or bar will set a corresponding filter for the records below. If you click multiple pies or bars, multiple filters will be set. To remove the filter simply click the pie or bar again.
- You can select time range in some line charts by mouse. To cancel the selection, click the  button.





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

Records

The bottom part of the *Records* mode contains a table with detailed records. You can find a list of columns that you can add to it on the right side of the view.

- To display the column in the table, drag the column into the table area.
- Clicking the  button will display a filter for that column. Fill in and confirm the filter by clicking the *OK* button.
- Under the table, you will find a search field. Entering text will highlight the expression in the table. Click  to remove the highlighting.
- Drag a column header above the table to group the table data according to that column. You can drag multiple columns above the table.

Filters

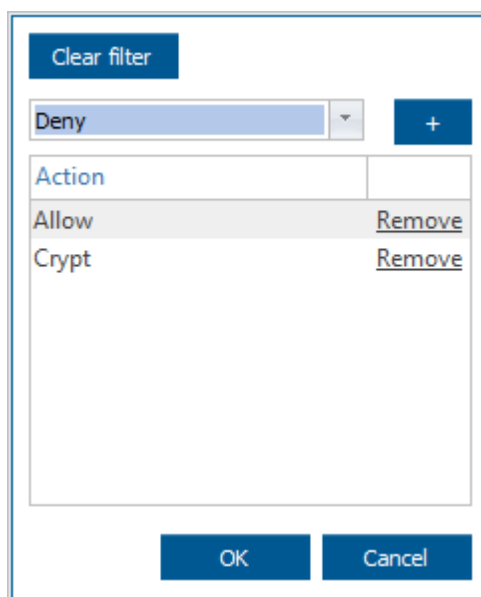
You can filter records as well. You can open the filter for any column by clicking the  button in the header of the respective column. Enter text or choose an item from the list, and select the condition based on which you wish to filter the column. Clicking the  button will add the item into the list 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 for the column. Header is be also highlighted.

You can set a filter by clicking the pie or bar inside a chart.

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



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.

[Clear filter](#)

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.

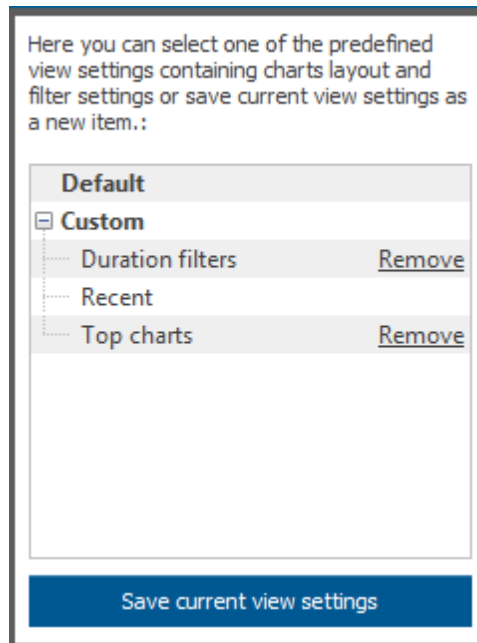
[Clear filter](#)

Title	
(No items)	

☒ Empty items

Layouts

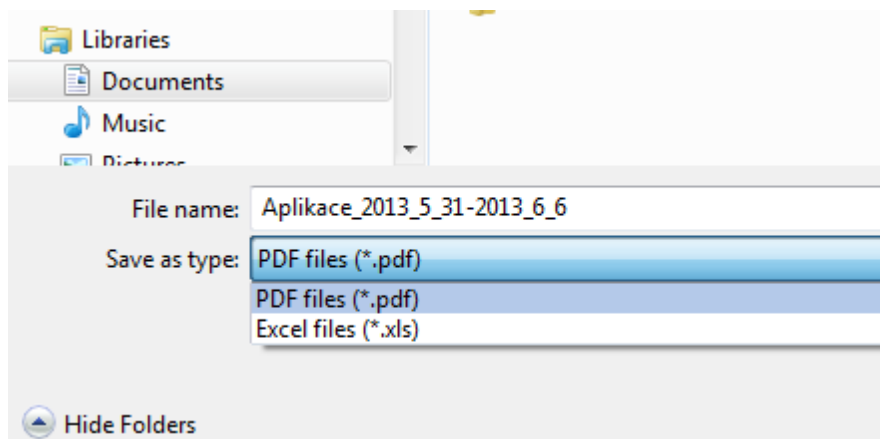
You can create your own layouts of charts, columns and filters in each feature. This is done using the layout manager. You can open the layout manager by clicking *Layout* button in the top left corner.



- Each Safetica user can have their own layouts for each feature.
- You can set the default layout by clicking *Default* in the layout manager.
- You can set the recently used layout by clicking the *Recent* option.
- You can save the current layout by clicking *Save current view settings*.

Export to PDF and XLS

You can export displayed charts and records to PDF or Excel using the [PDF](#) or [XLS](#) buttons in the top right corner.



Note: All data corresponding to selected users, time period, and filter settings will be exported to Excel. Record aggregation is also reflected in the Excel file.

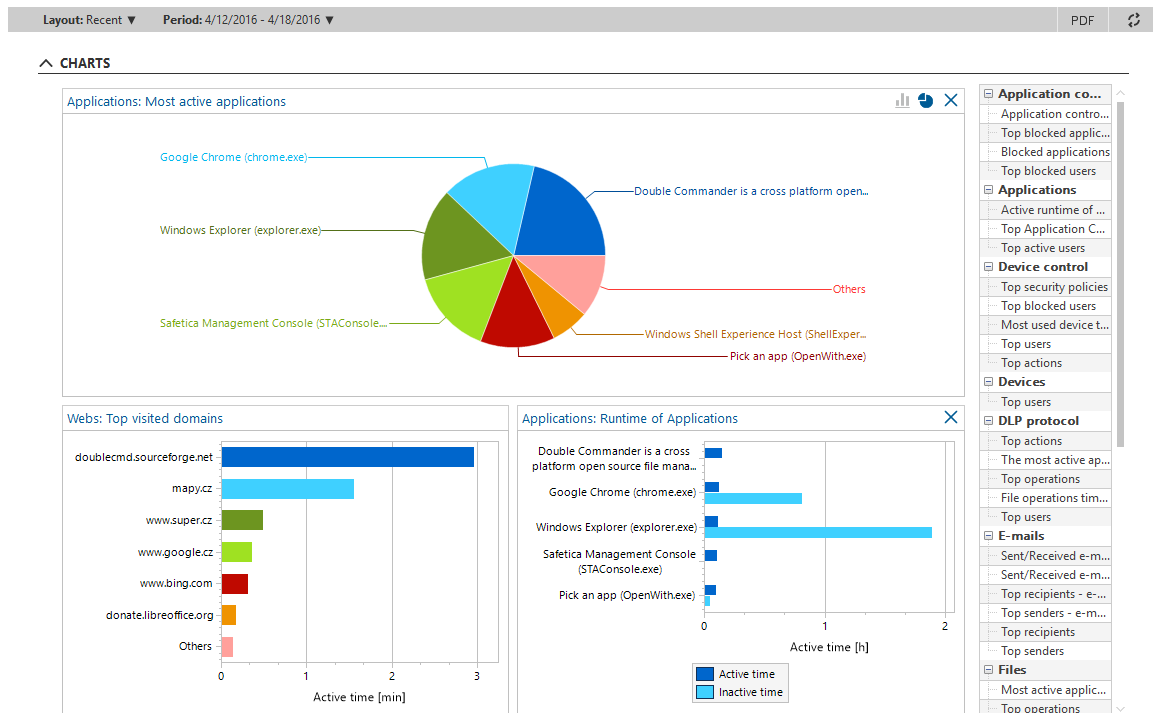
4.4 Management and settings

4.4.1 Dashboard

With the Dashboard view, you can display charts from all modules and features in a single place. This brings together the most important summaries, such as audit results or security incidents, to give you a quick overview of the status of your organization.

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

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



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 features are divided by features 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 [Records mode](#).

You can export displayed charts to PDF using the button .

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 Management 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 alert 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 four main categories:

- **Security alerts** – 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 *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 alerts** – used to notify the administrator on service incidents.
- **Smart alerts** – These alerts are shown only in WebSafetica. They are not displayed in Safetica Management Console nor sent via email.

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 endpoint with client under the account of the user who caused the incident. These settings apply to the entire server.

ACTION TRIGGERS					
Add trigger					
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:

Deny_copy.bat

Arguments:

-d

Working directory:

C:\data\scripts\deny

OK

Cancel

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 sec-

tion.

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 endpoint immediately after the incident.

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*.
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*. 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.

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.

Records

All alerts get recorded and you can view them later in the Records 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 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. To change the settings for reporting, click *Reports* in the main menu.

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.

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 part of the screen.
3. This section contains a list of available reports. The list is based on view reports (see [Records mode -> Layouts](#)), with which you can create custom layout for charts, columns and filters in the Records mode of each Safetica feature.
 - *Default layouts* – here are the default reports of charts, columns and their filters for each feature in the individual Safetica modules.
 - *Custom layouts* – here are the reports created by Safetica users in different features.
 - *Special layouts* – special sets reports are provided here:
 - *Active time* – reports contain active time spent in selected categories of applications. Categories can be selected when the *Active time* box is checked.
 - *Overview* – the basic overview of Safetica features 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 > Create new item

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

✓ 1. Report name: dlsdf
⊙ 2. Choose chart types and tables

^ DEFAULT LAYOUTS

Layout

- ☐ Discovery
 - ☐ Network traffic
 - ☐ Files
 - ☐ Print
 - ☐ Devices
- ☐ Protection
 - ☐ DLP logs
 - ☐ Disk guard
 - ☐ Device control
- ☐ Supervisor
 - ☐ Application control
 - ☐ Web control
- ☐ Maintenance
 - ☐ Computer utilization
 - ☐ Alerts
 - ☐ Endpoint settings
 - ☐ Endpoint management
 - ☐ Endpoints deactivation
 - ☐ Information collection

^ CUSTOM LAYOUTS

Layout

(No items)

- 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 *Next*.

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	
<div> <div>Service: 192.168.29.99</div> <div> Development Remove </div> </div>	
<div> <div>Sales</div> <div> Remove </div> </div>	

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 *Add email* to add email 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 file on the hard drive. 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*.

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
 ⚙ 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:

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 Maintenance

4.4.4.1 Endpoint overview

In this section, you will find an overview of endpoints, for example the total number of endpoints, the number of endpoints with installed Safetica Client or the number of endpoints with installed Downloader Agent.

Below the summary, there is a table with details about endpoints, Safetica Client and Downloader Agent.

Each record contains the following information:

- *PC* – name of the endpoint where Safetica Client is installed.
- *Client version* – version number of the installed Safetica Client.
- *Agent version* – version number of Downloader Agent.
- *Last settings update* – time of last Safetica Client settings synchronization.
- *Operating system* – version of operating system on endpoint.
- *Network layer* – type of the Safetica network layer used (see [Integration settings](#)).
- *Unsent records* – the number of records Safetica Client has not yet sent to the server and the time for which the record is valid.
- *Last logs sent* – date and time when Safetica Client sent the latest records into the database.
- *IP Address* – address of the endpoint with Safetica Client installed.
- *Certificate refused* – whether Safetica Client rejected the certificate of the new server.
- *System edition* – identification of the operating system edition.
- *Service pack* – identification of the service pack for the operating system.

- *System type* – whether the operating system uses 32-bit or 64-bit architecture.
- *System details* – detailed information on the operating system.
- *Download all logs* – click on this link to force sending all records from the respective Safetica Client to the central database. This option is available only if there are over 100 unsent records on Safetica Client.
- *Installation state (attempts)* – displays the status of Safetica Client installation or upgrade.
- *Conflicting SW* – list of applications installed on the endpoint which can be conflicting with Safetica.
- *.NET* – whether Microsoft .NET Framework is installed at the endpoint.
- *Repeat installation* – use this button to restart the installation/update at the endpoint if not performed successfully before.
- *Service installed* – whether the Safetica Client Service, which is a part of Safetica Client, is installed on the endpoints.
- *Service running* – whether the Safetica Client is running on the endpoint.
- *Database connection* – the status of Safetica Client connection to the database after its installation.
- *Webdetector version* – current version number of the webdetector.
- *Computer type* – whether endpoint is desktop or notebook.
- *Build number* – operating system build number.
- *Missing SW* – missing required software or components that are necessary for correct functioning of Safetica Client or any of its parts.
- *Active in domain* – whether the endpoint is active in Active Directory.

Learn more about the Records mode in chapter [Records mode](#).

4.4.4.2 Update and deploy

In this section, you can install and manage Safetica Client on endpoints. You can also find out what server and endpoint updates are available and install them.

Server update

This section is used for updates of the Safetica server. Update to the current version is performed by clicking the *Download and update to version* button. The update is performed for the server selected in the user tree.

Endpoint enrollment



Here you can install, update and manage Safetica Clients on all connected endpoints.

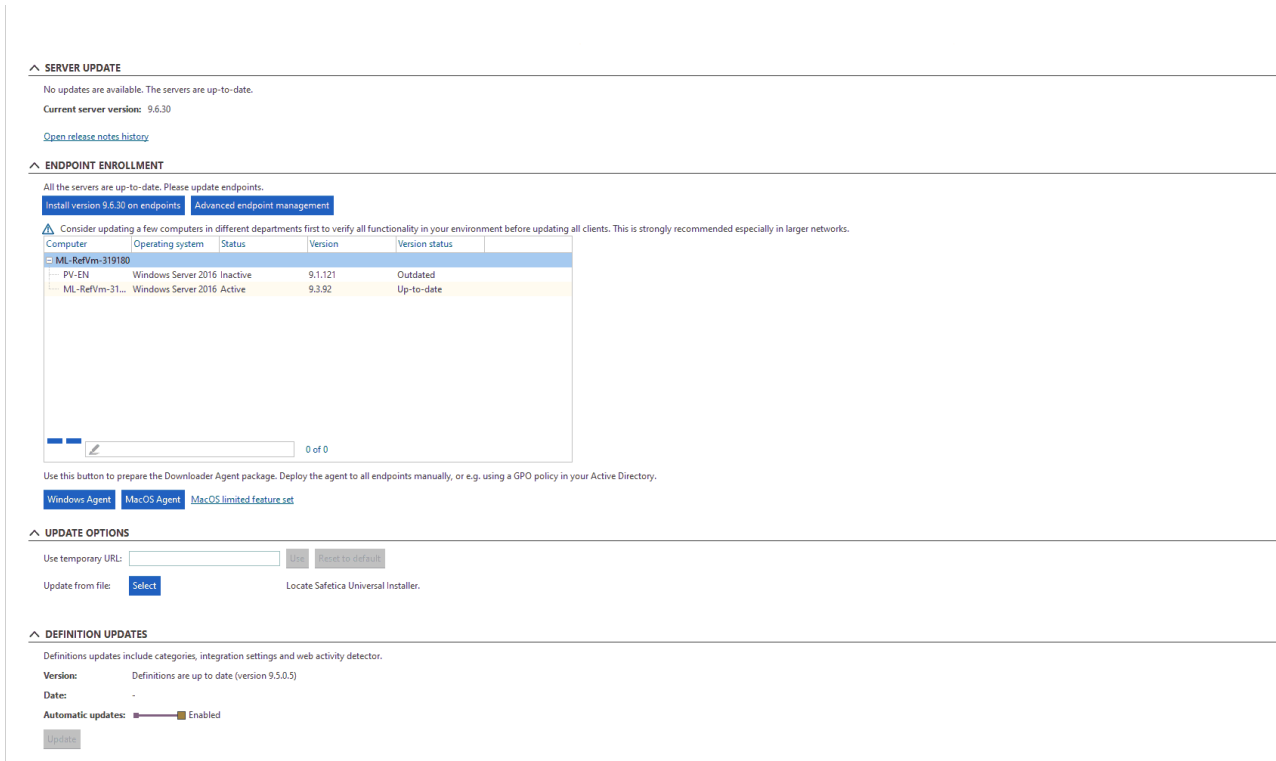
If you want to install Safetica Client on a new computer, first click the *Windows Agent* or *macOS Agent* button (depending on which system the endpoint is using). The installation package of Downloader Agent will be downloaded, so you can install it on the new computer. After connecting to the server, install Safetica Client using the *Install version on endpoints* button. Clicking this button also performs updates of Safetica Client.

You can perform remote advanced installation, update and uninstall of Safetica Clients on connec-

ted endpoints after clicking the *Advanced endpoint management* button.

Note: Safetica Client can only be managed on those endpoints that have Downloader Agent installed.

Endpoint management is set up for the server selected in the user tree. To apply the settings, you need to save the changes using the  button. You can cancel the changes using the  button in the upper right corner.



The screenshot displays the Safetica management interface. The top section, 'SERVER UPDATE', indicates that no updates are available for the current server version (9.6.30). Below this, the 'ENDPOINT ENROLLMENT' section shows a table of endpoints. A warning message advises updating a few computers first to verify functionality. The table lists endpoints with columns for Computer, Operating system, Status, Version, and Version status. Below the table, there are buttons for 'Windows Agent', 'MacOS Agent', and 'MacOS limited feature set'. The 'UPDATE OPTIONS' section includes a 'Use temporary URL' field and a 'Select' button for 'Update from file'. The 'DEFINITION UPDATES' section shows that definitions are up to date (version 9.5.0.5) and that automatic updates are enabled.

Computer	Operating system	Status	Version	Version status
ML-RefVm-319180				
PV-EN	Windows Server 2016	Inactive	9.1.121	Outdated
ML-RefVm-31...	Windows Server 2016	Active	9.3.92	Up-to-date

Advanced endpoint management

After clicking this button, you can *Install/Update* or *Uninstall* Safetica Client or Downloader Agent on endpoints.

In the table, there is a list of created management tasks. The properties of individual tasks can be edited based on their type:

- For the *Install/Update* type, you can:
 - *Install / update Safetica Client and update Downloader Agent* - installs or updates Safetica Client. When updating Safetica Client, Downloader Agent is updated as well.

Note: Remote Safetica Client installation or update is only possible, when the Downloader Agent is installed on the endpoint. Installing Downloader Agent at the endpoint is only possible locally or using a bulk installation tool (for example a Group Policy in Active Directory).
 - *Update Downloader Agent* - updates Downloader Agent.
- For the *Uninstall* type, you can use the slider to specify whether to uninstall only Safetica Client or both Safetica Client and Downloader Agent.

After performing any type of task, you can use the slider to force endpoint restart.

Basic statistics are given about the status of each task:

- On how many computers the task was executed.

- On how many computers the task was executed successfully.
- On how many computers the task failed.
- On how many computers reboot is pending.
- On how many computers the task execution is pending.

To remove a task, use the *Remove* button. All completed tasks remain in the table until you remove them manually.

Installation or update

To start Safetica Client or Downloader Agent installation or update, click the *Install/Update* button.

1. In the first step, use the drop-down to select the version number you want to install or update to.

Afterwards, choose the type of task:

- Install / update Safetica Client and update Downloader Agent - installs or updates Safetica Client and Downloader Agent.
- Update Downloader Agent - updates Downloader Agent.

At the end of the first step, select whether to reboot the endpoint after the task is completed.

Endpoint management > Add action

1. Action settings 2. Computers and groups


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:

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 *Finish* and then save the task using the  button.

Note: Computers with assigned task are bold.

Endpoint management > Add action

1. Action settings **2. Computers and groups**

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

Select computers and groups

Computer / group	
Development	Remove
Support	Remove


Uninstalling

To start Safetica Client or Downloader Agent uninstallation, click *Uninstall*.

1. The first step is to select which components you want to uninstall:
 - Uninstall Safetica Client - uninstalls only Safetica Client.

- Uninstall Safetica Client and Downloader Agent - uninstalls both Safetica Client and Downloader Agent.

Caution: Uninstalling Downloader Agent disables remote Safetica Client installation and management at endpoints.

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

Update options

In this section, you can specify how updates are performed.

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

To perform the update using *Safetica Universal Installer* from a local path, use the *Select* button in the *Update from file* section.

Definition updates

Here you can turn on automatic definition updates. Updates include only changes in categories, integration settings and webdetector.

Click the *Update* button for manual update.

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

Records

In the Records mode, you can view records of successful and unsuccessful updates. If any error occurs during an update, you can view its detailed description by clicking the *More Information* link. You can copy the text into the clipboard by clicking the *Copy* button. You can then send the details to the Safetica Tech Support, which will help you discover and possibly fix the problem.

4.4.4.3 Endpoints deactivation



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

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

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

Settings

The deactivation feature 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 endpoint.

Main Settings

- *Safetica Client* – use the slider to deactivate all client features (drivers, integrated technologies and services). If you want to completely switch off the client (including the drivers), you

must reboot the endpoint. Client will continue running, but only for the purpose of re-activation. To see which Safetica Client components are deactivated, check the *Records* mode > *Records* table > *Deactivated parts* column.

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 endpoint.

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 these drivers for their activities.

- *Safetica disk driver* - driver used by some Safetica features that work with the file system. The following Safetica features will be affected by the deactivation:
 - Client installation folders will not be protected, see [Protection against unauthorized manipulation with Safetica client](#).
 - [Device control](#)
 - [DLP policies](#)
 - [Disk guard](#)
- *Safetica device driver* – driver used by some Safetica features, for example by *Device control*. This driver can be either *Deactivated* or completely *Removed*.

The *Remove* option completely uninstalls Safetica driver. *Deactivate*, on the other hand, just switches the driver to passive mode, but it remains installed.

When you want to be 100% sure that a device issue is not caused by Safetica, you can try to *Remove* the driver. In other cases, it is enough to *Deactivate* it.

A reboot is required to remove the driver.

Services

In this section, you can turn off (disable) services which ensure the functioning of various Safetica features.

- *Safetica net monitor service* – provides some Safetica features for networking.
- *Safetica DLP service* – provides Safetica DLP features.
- *Safetica file monitor service* – provides Safetica file tracking features ([Files](#), [DLP logs](#)).
- *Safetica classification service* – provides Safetica features for file analysis and tagging.
- *Safetica applications service* – provides Safetica features for application blocking.
- *Safetica devices service* – provides Safetica features for [device monitoring and blocking](#).
- *Safetica user interaction service* – monitors all user activities in application windows and displays popups.
- *Safetica content analysis service* – scans the content of files and analyzes, whether they are sensitive.
- *Safetica information service* – telemetry services for analyzing information from endpoints.

Advanced

Safetica event log service – collects events for debugging from Safetica components.

Records

The Records mode provides an overview of activated and deactivated client parts at the endpoints.

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

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

4.4.4.4 Integration settings

Integration settings define the behavior of Safetica on endpoints.

You can find *Integration settings* in *Safetica Management Console > Maintenance*.


Application integration

Application integration defines which applications Safetica Client audits on endpoints.

To protect an application with Safetica or to audit file operations, the application needs to be integrated. Otherwise, you will just see that the application was running in *Discovery > Applications*, but you won't see any operations inside the application and DLP protection won't be possible.

Integration of Safetica into unknown applications may sometimes cause them to slow down, freeze for short periods of time, or interfere with their network communication. This makes the *Application integration* section a very useful place for troubleshooting - if you suspect an application is negatively affected by Safetica, this is the right place to fine-tune its integration to achieve the required level of protection without negative effects.

You can enable or disable Safetica integration into individual applications manually. Application in-

Integration is set up for the server highlighted in the user tree. To apply the settings, you need to save the changes with the  button.

Supported applications are integrated and network communication is monitored by default.

There are two lists of applications in this section:































- **All non-system applications** detected on endpoints.
- System applications integration - important **applications of the operating system**.

System applications have defined integration settings; it is not advisable to change these settings. The change in behavior may affect the functionality of the working environment.

We recommend consulting any change in application integration with Safetica Support.

APPLICATION INTEGRATION

Integration settings define, which applications Safetica Client monitors on endpoints. You can manually enable or disable Safetica ONE integration into individual applications. Before you use this functionality, please read the help information.































Application	Integration state	Date and time	Integration into application's operations	Integration into network communication	Min. client version	
(Adobe.CC.XD.exe)	 Active	1/29/2020 01:44:39 PM	 Active	 Inactive		Details Reset
(Adobe.CC.XD.exe)	 Inactive	8/31/2020 04:17:58 PM	 Active	 Inactive		Details
(adplus.exe)	 Inactive	2/14/2020 10:27:04 AM	 Active	 Inactive		Details
(adplusmanager.exe)	 Inactive	2/14/2020 10:27:04 AM	 Active	 Inactive		Details
(apivalidator.exe)	 Inactive	2/20/2020 12:04:10 PM	 Active	 Inactive		Details
(BackupToUrl.exe)	 Active	1/29/2020 01:43:39 PM	 Active	 Inactive		Details
(bulkmetadatapackagingwizard.exe)	 Inactive	1/31/2020 10:14:34 AM	 Active	 Inactive		Details
(CheckProgramRunning.exe)	 Inactive	1/29/2020 11:48:49 AM	 Active	 Inactive		Details
(chklogd2.exe)	 Inactive	6/9/2020 08:36:13 AM	 Active	 Inactive		Details
(chklogo.exe)	 Inactive	4/9/2020 03:57:24 PM	 Active	 Inactive		Details

[Reset to default settings](#)

Applications in Custom mode count: 18

SYSTEM APPLICATIONS INTEGRATION

System applications have defined settings which are not recommended to change. Changing the settings may affect system functionality.

Application	Integration state	Date and time	Integration into application's operations	Integration into network communication	Min. client version	
.NET Runtime Optimization Servi...	 Inactive	1/29/2020 11:48:49 AM	 Active	 Inactive		Details
A tool to aid in developing servic...	 Active	12/17/2020 11:25:47 AM	 Active	 Inactive		Details
Accessibility On-Screen Keyboar...	 Active	2/26/2020 01:34:27 PM	 Active	 Inactive		Details
Accessibility shortcut keys (sethc...	 Active	1/29/2020 12:08:25 PM	 Active	 Inactive		Details
Accounts Control Host (account...	 Inactive	1/29/2020 11:48:49 AM	 Inactive	 Inactive		Details
Add Hardware Wizard (hdwwiz.e...	 Inactive	9/24/2020 10:03:56 AM	 Active	 Inactive		Details
AddinUtil.exe (AddinUtil.exe)	 Inactive	1/29/2020 11:48:49 AM	 Inactive	 Inactive		Details
Advanced System Settings (Syste...	 Inactive	1/29/2020 12:08:25 PM	 Inactive	 Inactive		Details
Advanced User Accounts Contro...	 Inactive	2/3/2020 11:55:48 AM	 Active	 Inactive		Details
Antimalware Service Executable (...)	 Inactive	1/29/2020 11:48:49 AM	 Inactive	 Inactive		Details

Both application lists contain the following information:

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

- *Date and time* – date and time of application detection.

In the following options, you can enable or disable integration into individual functional 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.
- *Integration into network communication* – if integration is active, Safetica will be able to monitor all network communication of the application (including encrypted SSL/TLS network communication) and/or enter into such communication with the aim of applying security.

Click *Reset* to restore individual application integration settings to their default values. Click *Restore to default settings* under the list to change all the applications in the list to their default settings.

Trusted servers

To this table, you can add web addresses for which Safetica will not affect their secured SSL/TLS communication. New addresses are added to the list by using the *Add address* button.

Ignored devices

Learn more in the [Safetica Knowledge Base](#).

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.

System paths

In *Maintenance > Integration settings > System paths*, you can specify paths that Safetica will treat like default system paths (these are in particular folders with OS files, installed applications, or temporary files of running applications).

Examples of default system folders and sub-folders:

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

File operations are not logged for these folders. To add your own path to these default ones, click the *Add path* button and enter the path to the folder. All subfolders will be considered system

folders too.

You can also use system paths for file tagging. Go to the application rules of a **context** data category (*Protection > Data categories > Configure data category > Application rules > Add > Advanced > Include system*) where you can choose to enable the tagging of system files. This option is disabled by default.

Office 365 integration

Safetica 9.5 or higher automates the configuration of auditing and DLP protection features for emails and files stored in the cloud. DLP protection is available in Safetica ONE Protection and Safetica ONE Enterprise. Safetica ONE Discovery contains auditing features. Learn more in the [Safetica Knowledge Base](#).

FortiGate integration

Integration with FortiGate network security solution is only available in Safetica ONE Enterprise. Learn more in the [Safetica Knowledge Base](#).


Network certificates

Safetica performs SSL inspection at endpoints to protect data in encrypted network communication. Network certificate validation is performed as well. You can decide how strictly certificates are validated:


- *Full* – all errors of untrusted certificates are shown on endpoints.
- *Moderate* – default mode. Some errors of untrusted certificates are ignored.
- *Full - custom* – enables you to synchronize SSL inspection on endpoints with network inspection. Here you can import certificates used by your network security solution. After import, certificates are distributed to all endpoints running Safetica. After connecting to the corporate network (and to the Safetica server), Safetica will decrypt only those SSL connections that are also decrypted by your network solution.

Note: The purpose of decryption is solely to inspect communication for DLP protection. Communication is re-encrypted after inspection.

Safetica performs SSL inspection on endpoints to provide network DLP features. Network certificate validation is performed as well. By default, strict validation is performed, and all certificate errors are shown on endpoints.

Certificate validation mode:  Full

Custom certificate validation mode allows Safetica to synchronize SSL inspection on endpoints with network inspection.





Certificate name
(No items)

Imported certificates will be distributed to all endpoints running Safetica. When in company network (with connection to Safetica Management Service), Safetica will inspect only those SSL connections which are inspected also by your network appliance.

4.4.4.5 Endpoint 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 STCSer-service.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:
 - *Hide all* – all dialogs on client are hidden.
 - *Show only interactive dialogs* – dialogs are hidden except for dialogs that require user interaction.
 - *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 *Web sites* and *Applications* features of the Safetica UEBA module.
- *Safe mode* – by selecting *Block*, you prevent non-admin users from logging into the system in Safe mode.

Debug logs

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


Notifications

This feature is only available in Safetica ONE Protection and Safetica ONE Enterprise. You can partially adjust the appearance of notification dialogs displayed to users:

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

Settings:

^ NOTIFICATIONS

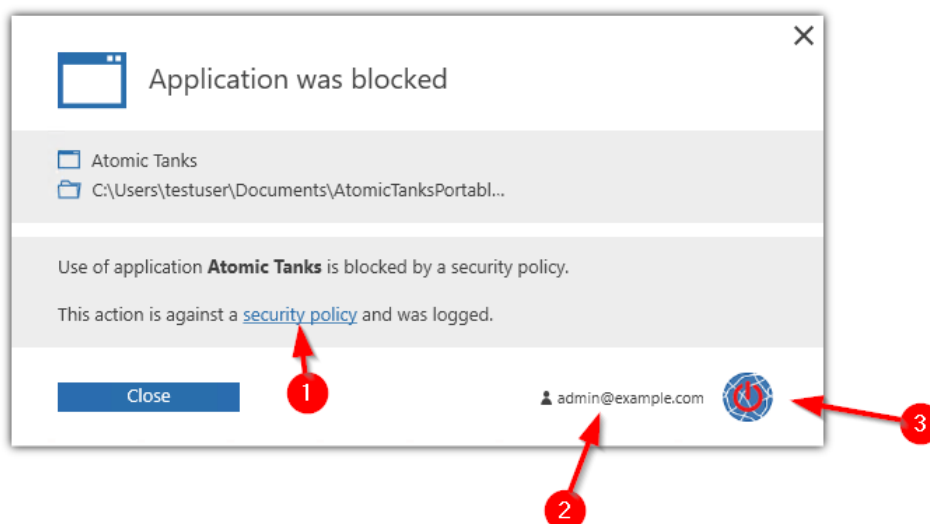
Notification logo: [Load logo](#) 

Size: max 92x62 px
[Delete logo](#)

Contact e-mail:

Security policy:

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



For more information, read the [Notification Dialogs](#) section in help.

User-based data classification

This feature is only available in Safetica ONE Protection and Safetica ONE Enterprise. You can learn more in the [Safetica Knowledge Base](#).

Non-working hours

This feature is available in the Safetica ONE Protection and Safetica ONE Enterprise products and also in the Safetica UEBA module. It enables you to specify how Safetica behaves outside working hours. The settings 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.

Records

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 Records mode in chapter [Records mode](#).

4.4.4.6 Information collection

In this section, you can create a task to collect debugging information from Safetica Client.

Collection of debugging information can be found in Safetica Management Console under *Maintenance -> Information collection*.

Collection of debugging information is set up for the server selected in the user tree. To apply the settings, you need to save the changes using the  button. You can also cancel the changes using the  button in the upper right corner.

Collecting settings


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

To create a new task, click 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. You can choose from the following options:
 - *Custom* – you can choose the information to be collected from Safetica Client manually from the list below the slider.
 - *Advanced* – the collection will include more information from Safetica Client. The contents of the collection is shown below the slider.
 - *Basic* – the collection will include only basic information from Safetica Client. The contents of the collection is shown below the slider.
 - *From SMS* – information is collected from the Safetica Management Service, not from

endpoint. You can use this option to troubleshoot issues with the server where Safetica is running.

After selecting, click *Next*.

2. In the second step, select groups or computers from which you want to obtain debugging information. Then click *Finish* and 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 endpoint or group the collection was performed, which files were included in the collection and the status of downloads on server.

Click *Remove* to cancel the respective task.

After clicking *Download*, a dialog box opens. Here you can select a local location, into which to download all the collected debugging information from server.

After clicking *Details*, a window with details on the collection of debugging information opens. Here you can download individual files from the collection.

Downloads

In this section, you can see which debugging information was downloaded from server to the local console. If an error occurs during download, you can repeat it by clicking *Download again*.

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

Records

In the Records mode, you will find a table with records on the size of files with debugging information on endpoints.



Each record contains the following information:

- *PC* – endpoint name.
- *Change* – date of last update of sizes for files with debugging information.
- There are also sizes of each individual file with debugging information.

Learn more about the Records mode in chapter [Records mode](#).

4.4.4.7 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

You can use Database management for database maintenance, data archiving or settings backups. It also allows you to connect and view data archives. When archiving and storing archived data, keep in mind any regulatory requirements for data retention, access, data privacy and protection against unauthorized access which may apply to the data.

Tasks Archives Maintenance

ARCHIVATION TASKS

Task name	Archive name	Archive directory	Schedule execution at	Type of task	From / Older than	To	Repeat task	Selected objects	
DB backup	DB	C:\Users\Safetica\Desktop\Test	3/10/2020 02:35:00 PM	Backup	3/1/2020	3/9/2020	No	Presentation	Remove

^ NEW ARCHIVATION TASK

Task name:

Type of task: Repeat task: ☒ Every week

Archive name:

Archive directory:

Logs to be processed:

Schedule execution at: Automatic rescheduling: ☒ Enabled

Selected objects: 1 objects selected [Change selection](#)

[Update task](#) [Add as new](#)

^ ADVANCED SETTINGS OF MAINTENANCE

Automatic database maintenance: ☒ Disabled Maximal database size: 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: ☒ No

4.4.4.7.1 Tasks

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

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

- *Task name* – name of the task.
- *Type of task* – you can choose from the following options: *Backup*, *Backup and delete*, *Delete*. More information about each task can be found below.
- *Repeat task* – how often will be the task repeated:
 - *Every week*
 - *Every 14 days*
 - *Every month*
 - *Every three months*
- *Archive name* – the backup file name. It must not contain illegal characters like spaces (<http://go.safetica.com/help/1hwuax>)
- *Archive directory* – the path to the folder where the backup database file will be saved. It is the path on the computer that is running the SQL server. The selected path must already exist, because the SQL server is unable to create the path.
- *Logs to be processed*:
 - From-To – it is possible to choose a time period for backup of monitored data
 - Log older than – processed are logs older than specified date. Available for delete tasks or repeated backup tasks.
- *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 feature 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 selected users, computers, or groups. The backup will contain records about file operations and user activities. Product and features settings are not included in the backup. Two files are created: one (*.mdf) contains all the data from the database and the second (*.ldf) is the log of operations performed with this data. 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 re-indexation, 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.

Advanced maintenance settings

In this section you can specify the maintenance options for the records 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.

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.

Records



The Records mode 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*.
- *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 Records modes in chapters [Settings mode](#) and [Records mode](#).

4.4.4.7.2 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 archive-viewing mode, all setup operations in the console are inactive.

BASIC INFORMATION

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.

Tasks **Archives** Maintenance

ARCHIVES

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

ARCHIVE IMPORT

Archive path: ...

Target service:

[Import archive](#)

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.

Records



The Records mode 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 Record modes in chapters [Settings mode](#) and [Record mode](#).

4.4.4.7.3 Maintenance

In the *Maintenance* section, you will find detailed information on the usage of log database for the various servers you administer via Safetica Management 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 a.s. Statistics will be sent once per week and contain the following information:

- License 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 a.s. 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 a.s. 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.

4.4.4.8 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 Management 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 features 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 features and settings.
 - Login: safetica
 - Default password: S@fetic@2004
 - After first log on to Safetica using this account, the user is prompted to change the password.
 - This account cannot be deleted, disabled or renamed.
 - 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 features.
 - Login: starter
 - 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 features and settings the user will have access to:

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

Access settings

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

Note: Some features 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 features
- *View records* – the right to display charts for a selected employee
- *Full access* – the right to display and change settings of individual modules and features

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

Modules:

- *Discovery*
- *Protection*

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.

SIEM / Syslog

Here you can add the address of your SIEM or syslog server, to which to send records of actions performed by users in the Safetica Management Console (e.g. which section they accessed, what settings they changed, etc.). This feature is only available in Safetica ONE Enterprise.

Records

In 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 (feature) 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 Records mode in chapter [Records mode](#).

4.4.4.9 License management

License management is used for entering and checking licenses. Only the Safetica Client is licensed, and licenses are assigned to endpoints, where the clients run. Without an assigned license, Safetica features are not active on endpoints.

License management can be found in Safetica Management Console under *Maintenance -> License management*.

Licenses are assigned for the server selected in the user tree. To apply the settings, you need to save the changes using the  button. You can also cancel the changes using the  button in the upper right corner.

General settings

Enter the license key or customer ID into the text box. Activation of endpoints with Safetica Client will be automatic. After connecting to the server, Safetica Client downloads a license and activates its features.

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 endpoints with Safetica Client may be activated and also the validity of the license.

Click *Synchronize with license server* in order to synchronize and update your entered license data with the Safetica license server.

To this list, you can add groups from the user tree, for which you wish to change the license assignment rules. For these specified groups and each license type, you may enable or disable automatic license assignment to computers in the group.

The *Edit license assignments* button helps you assign licenses to groups of users. You can prioritize some user groups or block license assignment to others. If you have less licenses than endpoints running Safetica Client, you can ensure that priority users are always assigned a license.

Groups are selected from a tree displayed after clicking the *Add* button. Selected groups can then be seen in a list, where you can enable or disable the assignment of individual license types for them. Licensing rules are applied based on their position in the list.

In the bottom section, there is an overview of activated licenses on endpoints. An activated license on a computer with Safetica Client is indicated by . Number at the root item, which represents the server, indicates the total number of activated licenses.

License expiration

When a license expires, Safetica features on the endpoint will be deactivated. To restore the features, it is necessary to enter a new license.

Exceeding the limit of available licenses

When the number of endpoints with installed Safetica Client exceeds the number licenses, a warning is displayed in the view. In this case, you must purchase a license which increases the number of endpoints with activated Safetica Client.

4.4.4.10 Categories

Safetica includes ready categories of websites, applications and extensions. The categories are used in various Safetica features for better orientation in the recorded data and setting of different DLP 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 categorized applications and websites on all endpoints with the client. This speeds up updates of application or website categorization if changes are made in the console. We recommend using this option only in exceptional and really urgent cases.

Note: Deletion of the categorization 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.

[Application Categories](#) [Web categories](#) [File type categories](#)

[Browse database](#)

^ 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](#)

4.4.4.11 Computer utilization

In this section, you will find records on the activity on endpoints where the Safetica is installed.

Computer utilization can be displayed in Safetica Management Console under *Maintenance -> Computer utilization*.

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

Note: Records of activity on the endpoint 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 *Records* mode 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 feature 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, you will find a table with records of user actions on the endpoint. 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)

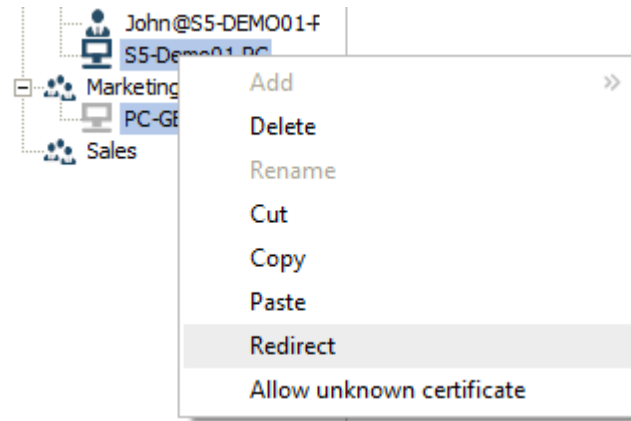
4.4.4.12 Redirecting client to another server

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 ad-

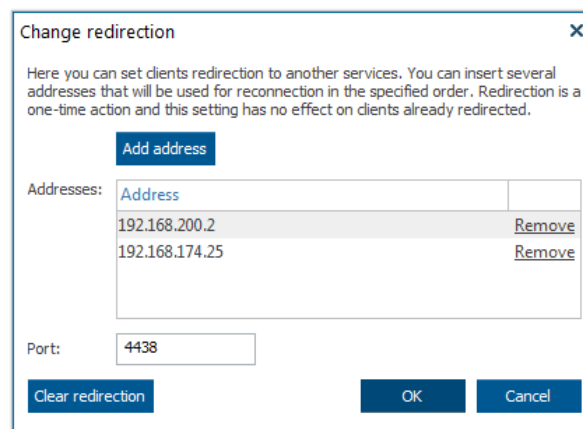
dress.

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 server addresses into the list. Safetica Client will always connect to the first Safetica server available. Connection attempts will be performed based on the address order from the first address to the last. Under the address list, enter the port which Safetica Client uses for server connections. If you have not changed the port, leave the default one. This port is the same for all servers in the list. If you would like to connect to a specific server using another port, add it directly behind the address of the server in question and separate it with a colon (e.g. 192.168.200.12:4000). Confirm the dialog with OK.



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.

4.4.4.13 Protection against unauthorized manipulation with Safetica client

Because Safetica client is responsible for the enforcement of your company's policy on endpoints, 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 endpoint, 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 endpoints, 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 endpoints.

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

Permission for these tasks can also be granted directly from the endpoint 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: `S@fetic@2004`

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):

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 username 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 format types:

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

Connection

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

Connection 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.

Caution: You can only be logged on to multiple servers simultaneously if all the connected servers have the same username and password.

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 Safetica Management Console version number.

You can use the slider to specify whether Safetica Management Console should be launched after system start.

Use the *Use proxy settings* slider to specify whether Safetica Management Console should use a proxy server during update. Proxy server settings are copied from the Windows settings of the user under which Safetica Management Console is run.

Confirm the changes with .

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 features

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*](#).
- 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*.

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 Safetica database prefix. For example, if the *st* prefix is entered, the database name will be *st_data*. 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*](#)

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

In this section, you can configure access to your Active Directory, from which you can import nodes, security groups, or departments. This way, you can work with your existing organizational structure.

Enter your Active Directory username and password into the respective text fields.

To import parts of your Active Directory into the configured server, click the *Add* button. You have three import options:

- *AD node* – import selected nodes from your Active Directory into the configured server. After confirming the dialog, all the domain users and computers from these nodes will be loaded into Safetica [user tree](#). Both users and computers are placed into an Active Directory synchronization group, from which you can copy them into other groups.
- *Security group* – if you have security groups defined in your Active Directory, you can choose which to import into the Safetica user tree.
- *Department* – if you have departments defined in your Active Directory, you can choose which to import into the Safetica user tree.

Use the *Synchronize now* button to force an update of users and computers from your Active Directory into the Safetica user tree. Active Directory is normally synchronized once per day or after the settings are changed.

Root certificate

Safetica integrates with network communication in order to detect or restrict user activity in the network. By default, Safetica uses its own SSL certificates that provide a basic level of security using 256-bit AES encryption. You can use your own SSL certificates that you trust to increase security even further.

Here you can import your own SSL root certificate. If an SSL certificate is already in use, first click on *Remove* and then import a new certificate.

Learn more about creating your own root certificate in the [Safetica Knowledge Base](#).

Detailed description of how Safetica uses certificates can be found in the [Safetica Knowledge Base](#).

Under [Alerts](#), you can configure the certificate expiration warning.

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.

Proxy settings

Use the slider to set whether Safetica Management Service, or Safetica Management Service + en-

dpoints should communicate via a proxy server specified below.

Use the *Copy system proxy* button to copy the proxy server settings from the Windows settings of the user under which Safetica Management Console is run.

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

Data analytics

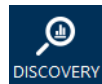
Integration with data analytics tools is only available in Safetica ONE Enterprise. Learn more in the [Safetica Knowledge Base](#).

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 Discovery

The Discovery section brings you an overview of potential security issues and enables you to better understand your security processes. With Discovery, you will be able to audit sensitive files which may pose a security risk. Information obtained from Discovery may also help you facilitate the implementation of DLP policies. Thanks to hardware audit, you can see to what devices your files are transferred. You can also see how your printers are utilized and what files are uploaded and downloaded via your company network.



You can switch to Discovery by clicking the  icon in the console [main menu](#). After clicking one of the features, you will see its [Settings](#) or [Records modes](#) (depending on the mode you are currently using).



4.5.1 Functions settings

In this view you can configure individual Discovery features.

Type of settings

You can use the slide bar to specify the behavior of individual features:

- *Disable* – the feature is not active.
- *Inherit* – the feature is not set. Settings are inherited from the parent group.
- *Enable* – the feature 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 in the upper right corner. You can also cancel the changes you have made using the  button.

You can set the following features:

- [Devices](#) – logs the connection and disconnection of USB storage devices (flash drives, external drives etc.) on endpoints.
- [Print](#) – print monitoring on endpoints.
- [Network traffic](#) – logs the volume of data sent or received on endpoints.
- [E-mails](#) – audit of emails with attachments sent from endpoints.
- [Files](#) – file handling monitoring on endpoints.

After enabling the features and clicking on the *Show advanced settings* button, additional settings will be displayed for the *Print* and *Files* features.

Advanced print settings

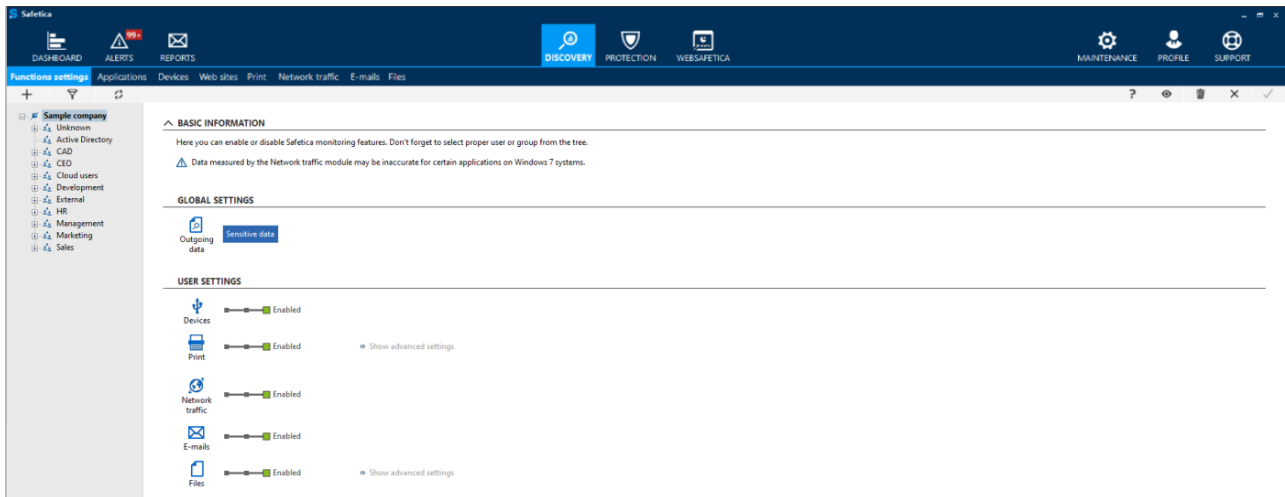
If you enable this option, printing will be logged for all applications (including unknown ones that are not [integrated](#)). These records will be listed under *Unknown application* in the audit logs. You can choose which applications are integrated (and, therefore, monitored by Safetica) in *Maintenance -> Integration settings -> Integration mode*. By default, Safetica integrates only into known and well-tested applications to avoid performance and compatibility issues.

Advanced file settings

The *Files* feature monitors events which may lead to files leaving the computer and the secure company network (e.g. web uploads, file operations on external devices or local paths, FTP transfers etc.). In the advanced settings, after clicking the *Add extension* button, you can enable logging of operations for specific file extensions. You can choose a whole category of extensions after clicking the three dots icon. This might, however, have an impact on log database size and the usability/readability of audit logs. You can monitor database size in *Maintenance -> Database management -> Maintenance*.

Sensitive data in Safetica ONE Discovery

If you have purchased Safetica ONE Discovery, you will see a special version of *Functions settings* that substitutes functionality available in higher editions. If you have Safetica ONE Protection or Safetica ONE Enterprise, you can find information about sensitive data in [Sensitive content](#) and [DLP policies](#).



To create a sensitive data category:

1. Go to *Discovery > Functions settings* and click the *Sensitive data* button. It allows you to specify which data your company considers sensitive and detect files that contain it. You can detect specific keywords, specify built-in dictionaries, pre-defined algorithms, and regular expressions within your company files.
2. Click *New data category* and enter the category name and description.
3. Click *New detection rule*, and choose from pre-defined algorithms and dictionaries, add custom regular expressions or custom dictionaries. To learn more about these features, go to chapter [Sensitive content](#) (the *Set up and run discovery task* option is only available in the Safetica ONE Protection and Safetica ONE Enterprise products).
4. After you are done, click *OK* and then click *Finish* in the bottom right corner of the screen.

4.5.2 Devices

The *Devices* feature provides information about external devices like USB flash drives, mobile phones, printers etc. You will be able to see details like device ID, application used, interface type or vendor.

Settings

In the tab *Discovery* -> [Functions settings](#) you can turn this feature off or on.

Records

The following charts are available in the Records mode:

- *Top users* – this chart shows users who work with external devices the most (up to 7 most active users are shown).
- *Most used devices types* – this chart shows the most used types of external devices.
- *Top actions* – this chart shows the ratio of tasks performed.

Each record contains the following information:

- *Date and time* – date and time of record logging.
- *PC* – name of the computer for which the record was logged.

- *User name* – name of the user for whom the record was logged.
- *Description* – detailed device description.
- *Action* – shows whether the device was *Connected* or *Disconnected*.
- *Drive* – to what drive (letter) the device is mapped.
- *Device identification* – numbers identifying the device <vendor's ID>-<product series ID>-<serial number>
- *Vendor* – vendor's ID.
- *Device type*
- *Interface type* – type of interface concerned: USB, Bluetooth, FireWire, IrDA, LPT, COM.
- *Application* – in which application the task was performed.

Learn more about the Records mode in chapter [Records mode](#).

4.5.3 Print

The *Print* feature provides detailed overview of company printers and printed documents. You will see all printed documents, number of pages, printer names or types of print (color or black/white).

Settings

In the tab *Discovery* -> [Functions settings](#) you can turn this feature off or on.

Records

The following charts are available in the Records mode:

- *Top printing users* – this chart shows users who print the most, based on the number of printed documents (up to 7 users are shown).
- *Most used printers* – this chart shows the most-used printers (up to 7 printers are shown).
- *Top printing applications* – this chart shows applications most often used for printing (up to 7 applications are shown).
- *Printer types* – this chart shows the number of prints based on the type of printer. Several printer types are available: *Unknown printer type*, *Local printers*, *Virtual printers* (like PDF Creator, XPS Writer, etc.), *Network printers* and *Redirected printers*.
- *Print monitor timeline* – this chart shows the total number of prints over time.

Each record contains the following information:

- *Date and time* – date and time of record logging.
- *PC* – name of the computer for which the record was logged.
- *User name* – name of the user for whom the record was logged.
- *Application* – name of the application from which printing was done.
- *Device name* – name of the printer which was used for printing.
- *Printer type* – several printer types are available: *Unknown printer type*, *Local printers*, *Virtual printers* (like PDF Creator, XPS Writer, etc.) and *Network printers* and *Redirected printers*.
- *Document name* – name of the printed document.

- *Paper size* – size of the paper used for printing.
- *Print color*
- *Duplex print*
- *Total number of pages* – number of pages printed from a document.

Learn more about the Records mode in chapter [Records mode](#).

4.5.4 Network traffic

The *Network traffic* feature provides information about downloads and uploads on endpoints and offers statistics of network usage. Information is grouped by applications and application categories.

Note: Data measured by the Network traffic feature may be inaccurate for certain applications on Windows 7 systems.

Settings

In the tab *Discovery* -> [Functions settings](#) you can turn this feature off or on.

Records

The following charts are available in the Records mode:

- *Top downloads by users* – this chart shows users with the highest amount of received data (up to 7 users).
- *Top uploads by users* – this chart shows users with the highest amount of sent data (up to 7 users).
- *Top downloads by applications* – this chart shows applications with the highest amount of received data.
- *Top uploads by applications* – this chart shows applications with the highest amount of sent data.
- *Top downloads by application categories* – this chart shows application categories with the highest amount of received data.
- *Top uploads by application categories* – this chart shows application categories with the highest amount of sent data.
- *Network traffic timeline* – this chart summarizes sent and received data.

Each record contains the following information:

- *PC* – name of the computer for which the record was logged.
- *User name* – name of the user for whom the record was logged.
- *From* – record start time.
- *To* – record end time.
- *Received / Sent* – whether data was received or sent.
- *Application* – application which sent or received data.
- *Application category*
- *Data amount* – amount of data received or sent during the record period.

Learn more about the Records mode in chapter [Records mode](#).

4.5.5 E-mails

The *E-mails* feature provides information about outgoing e-mails with attachments sent through e-mail clients and Exchange Online. It does not, however, audit webmails. You will be able to see the attached documents, subjects, recipient's domain, sender's domain and other details. It might be useful to know, whether company documents are sent to private addresses or to competition.

For e-mail auditing, see [Discovery](#) -> *E-mails*.

Settings

In the tab *Discovery* -> [Functions settings](#) you can turn this feature off or on.

Records

The following charts are available in the Records mode:

- *Sent e-mails with attachments* – number of sent and received e-mails with attachment over time.
- *Top recipients – e-mail addresses* – this chart shows the proportion of e-mail addresses receiving the highest number of e-mails.
- *Top recipients – domains* – this chart shows the proportion of e-mail domains receiving the highest number of e-mails.

Each record contains the following information:

- *Date and time* – date and time of record logging.
- *PC* – name of the computer for which the record was logged.
- *From* – e-mail address of the sender. In case the e-mail address is not detected, this field is left blank.
- *Recipient* – e-mail address of the recipient. In case the e-mail address is not detected, this field is left blank.
- *Subject* – subject of the logged e-mail.
- *Files* – names of any e-mail attachments.
- *Sender – domain* – e-mail domain of the sender.
- *Recipient – domain* – e-mail domain of the recipient.
- *Application* – e-mail client name.
- *Size* – message size.

Learn more about the Records mode in chapter [Records mode](#).

4.5.6 Files

The *Files* feature enables you to see file operations like web uploads, web downloads, copy/move/rename/create/delete/open, FTP transfers, or instant messaging. In the details, you will find file-name, source and destination types, date and time, user or file size. It might be useful to see what files are copied to USB flash drives or uploaded to file sharing sites or webmails.

You can also enable logging of operations for specific file extensions.

Note: Auditing files downloaded from the web is supported only for Mozilla Firefox, Internet Explorer and Google Chrome. Files downloaded via other browsers will be classified as newly created files.

You can find this feature in [Discovery](#) -> *Files*.

Settings

In the tab *Discovery* -> [Functions settings](#) you can turn this feature off or on.

Records

The following charts are available in the Records mode:

- *Most active users* – this chart shows users who work with files the most.
- *Most active applications* – this chart shows applications that are most frequently used for working with files.
- *File operations timeline* – this chart shows the most popular file operations.
- *Top operations* – this chart shows the number of operations executed over time.

Each record contains the following information:

- *From* – start of operation (for operations that take a long time).
- *To* – end of operation (for operations that take a long time).
- *PC* – name of the computer for which the record was logged.
- *User name* – name of the user for whom the record was logged.
- *Application* – name of the application that performed the file operation.
- *Source* – name and path of the file used in the file operation.
- *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 from Microsoft or TeamViewer.
 - Cloud drive – local cloud drive folder. Supported cloud drives are: *Google Drive*, *OneDrive*, *Dropbox*, *Box sync*.

- Web
- E-mail
- Webmail
- Instant messaging
- File share – file sharing websites.
- Mobile
- *Destination type* – type of destination path:
 - Local path
 - USB
 - Network path
 - FTP
 - Other external
 - Remote transfer – file transfer using Remote Desktop from Microsoft or TeamViewer.
 - Cloud drive – local cloud drive folder. Supported cloud drives are: *Google Drive, OneDrive, Dropbox, Box sync.*
 - Web
 - E-mail
 - Webmail
 - Instant messaging
 - File share – file sharing websites.
 - Mobile
- *Operation* – type of file operation performed: *Open, Copy, Delete, Move, Create, Web download, FTP transfer, Rename, Web upload, IM - Send file, E-mail.*
- *Source device* – device name and SID. After clicking the name, detailed information about the device will be displayed. Here you can specify what [zones](#) the device belongs to. You can do this by clicking *Edit zone* and checking the respective zones.
- *Destination device* – device name and SID. After clicking the name, detailed information about the device will be displayed. Here you can specify what zones the device belongs to. You can do this by clicking *Edit zone* and checking the respective zones.
- *File* – name of the file. If you group, order or filter files using this column, the file name from the *Source* column will be used. If the source is empty, the file name will be taken from the *Destination* column.
- *File size*
- *Extension* – file extension. If you group, order or filter extension using this column, the file extension from the *Source* column will be used. If the source is empty, the file extension will be taken from the *Destination* column.
- *Sensitive content* – shows whether the file contains sensitive data.
- *Risk* – informs you whether the operation might potentially present a security threat. Learn more about risk in [Safetica Knowledge Base](#).

- Action
- Data category – data categories with which the file is tagged
- Details

Learn more about the Records mode in chapter [Records mode](#).

4.6 Protection

The Protection section is only available in Safetica ONE Protection and Safetica ONE Enterprise products. Here you can protect your organization's sensitive data against misuse, and thus prevent financial losses and damage to your reputation. Together with [Discovery](#), it informs you about and protects you from the dangerous activities that could lead to data loss.

There are several ways of how to set up DLP protection in the Protection section:

- *Based on content (Sensitive content)* – the main, easiest and also the recommended DLP protection method which utilizes a deep analysis of content. Sensitive data is identified based on their content using dictionaries, algorithms, keywords or regular expressions. The data is not tagged in any way.
- *Based on data tagging by third-party applications (Existing classification)* – another DLP protection option is based on existing metadata tagging performed for example by another classification application. This approach can be used to protect data that has already been assigned some classification or security level (e.g. internal, sensitive etc.).
- *Based on context (Context rules)* – the final option is DLP protection based on context. This means that data is protected based on who works with it, where it is stored, where it is transferred, who works with it, in which applications etc. Sensitive data is protected with the Safetica tag. This method can be used to protect data that cannot be classified based on content. It's more difficult to implement and maintain than the other options. The method requires more advanced knowledge of Safetica as well as a detailed analysis and compliance with corporate processes for working with data.
- *Based on file properties (File properties)* – File property data categories allow you to protect files based on their properties, such as file extensions, regardless of their content or classification. For example, you can protect all outgoing .pdf or .cad files. These categories can also expand existing DLP policies to protect files which cannot be scanned for classification or sensitive data (such as encrypted files).

4.6.1 DLP logs

In DLP logs you will find records of operations with data or applications, which are subject to [DLP policies](#).

DLP logs can be found in *Protection -> DLP logs*.

The following charts are available:

- *Top users* – this chart shows users who work with files most actively.
- *Top actions*
- *Top operations* – this chart shows the most frequent file operations.
- *The most active applications* – this chart shows applications used most frequently for working with files.

- *File operations timeline* – this chart shows the timeline of file operations.
- Overrides per user

Each record contains the following information:

- *From* – start of operation.
- *To* – end of operation.
- *PC* – name of the computer for which the record was logged.
- *User name* – name of the user who executed the file operation.
- *Application* – name of the application that executed the file operation.
- *Source* – name and path to the file involved in the operation.
- *Destination* – the destination path in copying and 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 about the device will be displayed. Here you can specify what [zones](#) the device will 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 about the device will be displayed. Here you can specify what zones the device will belong to. You can do this by clicking the *Edit zone* button and checking the respective zones.
- *File* – name of the file. If you group, order or filter the records 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, Copy, Move, Print, Virtual print, E-mail, Web upload, IM - Send file*.
- *Action* – whether the operation was allowed or blocked by Safetica.
- *Action context*
- [Data category](#) – data categories with which the file is tagged.
- *Modules* – name of the Safetica feature used to create the record: *DLP logs, [Disk guard](#) or [Device control](#)*
- *Details*
- *File size*
- *Sensitive content* – whether the operation was performed with sensitive data.
- *Safe zone*
- *Policy*
- *Risk* - informs you whether the operation might potentially present a security threat. Learn more about risk in [Safetica Knowledge Base](#).
- *Shadow copy* - informs you whether a [shadow copy](#) of the file was created. If so, you can collect it by clicking the Yes (*collect*) link.

Learn more about the Records mode in chapter [Records mode](#).

4.6.2 DLP policies

Safetica uses DLP policies for data protection on endpoints and for controlling application behavior.

Learn more about **DLP policies in general** in the [Safetica Knowledge Base](#).

Learn how to **create a new DLP policy** in the [Safetica Knowledge Base](#).

Learn more about the **Shadow Copy** feature in the [Safetica Knowledge Base](#).

Learn more about the **Override** feature, which is available for the **Log and block** mode, in the [Safetica Knowledge Base](#).

4.6.3 Data categories

In the **Data categories** section, you can create an unlimited number of data categories. Data categories are used for classifying files into different groups depending on who, where and how can work with them. Subsequently, you can create various [DLP policies](#) for each data category, and thus secure classified data.

In this section, you can also configure the languages for **Optical character recognition**. Learn more in the [Safetica Knowledge Base](#).

Learn more about **data categories in general** in [Safetica Knowledge Base](#).

Learn to **create and configure** a new:

- [sensitive content category](#)
- [data category based on existing classification](#)
- [context data category](#)
- [file properties data category](#)

You can also integrate Safetica with the **Netwrix Data Classification** solution to extend sensitive data discovery and classification. Learn more in [Safetica Knowledge Base](#).

4.6.3.1 Sensitive content

Find out what sensitive data is hiding inside your company files. By scanning file content, you can classify files that contain sensitive data. You can choose from many pre-set algorithms or define your own search patterns using keywords, dictionaries, or regular expressions.

Learn how to **create and configure a sensitive data category** in the [Safetica Knowledge Base](#).

After you create a sensitive content category, you can use it in DLP policies or to **set up and run a**

discovery task. Learn more about data discovery tasks in the [Safetica Knowledge Base](#).

Learn more about **detection rules** in the [Safetica Knowledge Base](#).

You can also use **Optical character recognition** to find sensitive data in image-based files. Learn more in the [Safetica Knowledge Base](#).

4.6.3.2 Existing classification

If you use third-party tools to classify sensitive data, you can configure them in this section.

Learn how to **create and configure a data category based on existing classification** in the [Safetica Knowledge Base](#).

After you create a data category based on existing classification, you can use it in DLP policies or to **set up and run a discovery task**. Learn more in the [Safetica Knowledge Base](#).

4.6.3.3 Context rules

Based on the rules, the files corresponding to them will be classified with the selected data category.

Each file can be classified with only one context data category.

Learn how to **create and configure a context data category** in the [Safetica Knowledge Base](#).

Learn more about **classification using persistent meta-data** in the [Safetica Knowledge Base](#).

If you have persistent meta-data enabled, you can use the category in [user-based classification](#).

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 dialog (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 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.

Task repetition

You can repeat the file tagging task at regular intervals. 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. This may be necessary for example because of access privileges.

Advanced

- Tagging operations:
 - *Merge tags by priority* – the file will be tagged by the data category that has a higher priority. If a file is already tagged, the priorities of the current and new data categories are compared and the file is tagged with the higher priority category.
 - *Replace tag* – replaces an existing tag with the selected data category. The priority of the data category is ignored.

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 enter at least one part. If a part is not entered, it will apply to all cases.

Click on *Finish* to confirm rule generation.

Context tag removal

Context tag removal in **Protection > Data categories** is 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 *Context tag removal* button.

Generating a tagging removal rule is analogous to generating [a Paths rule in the Context rules](#). 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.

Settings

Records

?

×

✓

^

BASIC INFORMATION

Data categories identify data and categorize them based on your configuration. These categories can later be used in DLP policies for granular data management. Some types of categories also allow you to run tasks to discover data stored in your organization. To find out more about data categories, visit the [Safetika knowledge base](#).

New data category

Manage Netwrix data categories

Category	
GDPR	Remove
GLBA	Remove
GDPR Restricted	Remove
PCI DSS	Remove
HIPAA	Remove
Financial Records	Remove
PII	Remove
Credentials	Remove
CMMC	Remove
PHI	Remove
FTFileProp	Edit Remove
CCPA	Remove
JV_new_content_test	Edit Remove
MK_test	Edit Remove
mk_nasb	Edit Remove
PeBr - test	Edit Remove
Sensitive data	Edit Remove
Context data category	Edit Remove
Sensitive data 2	Edit Remove
Obsah	Edit Remove
Kontext	Edit Remove
Default_Sensitive_Data_ca...	Edit Remove
Default_ExistingClass_Dat...	Edit Remove
Default_Context_Data_Cat...	Edit Remove
Default_SafetikaMetadata...	Edit Remove

DATA CATEGORY DETAILS

Name: GDPR

Data categorized by: Netwrix

Identifier: 3c7a922a-9b46-432f-a166-82ec1dff5d2c

Description: -

DATA DISCOVERY

Last discovery: 11/13/2021 12:00 AM

Set up and run discovery task

^

CONTEXT TAG REMOVAL

Context tag removal allows you to discard specific Safetika tags which are used by data categories defined by expert context rules.

Context tag removal

4.6.3.4 File properties

Using the **File properties** category, you can protect files that are not compatible with Safetika content scanning technology, third-party classifications, or you can choose to protect all files with a specified extension.

Learn how to **create and configure a file properties data category** in the [Safetika Knowledge Base](#).

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 [DLP policies](#).

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 description and specify if it is a safe zone.

Click *Add zone* to open the new zone dialog, enter a name and description for it.

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 endpoints with client. These devices and printers have not been assigned to any zone yet.
 - By moving them to the middle list or clicking *Add*, you can assign them to the zone marked on the left.
 - Click *Remove* to return the device or printer to the Unassigned group.
 - 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.
 - 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.

BASIC INFORMATION

Zone content Unassigned items (0)

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

Add zone

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

ZONE INFORMATION

Zone name: Office 01
Description: -

Add item

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](#)

« » 0 z 0 X

Creating a new zone and adding items

Click *Add zone* to open the new zone dialog, enter a name and description for it.

To edit the zone content, proceed as follows:

1. In the zone list on the left, mark the zone whose content you wish to edit. The zone's current content will be displayed in the left bottom. Click the *Remove* link with the respective zone item and the item will be removed. To add a new item to the zone, click *Add item*.

2. The wizard lets you choose from among the following items which the zone can contain:
 - *External devices*
 - *IP addresses*
 - *Network paths*
 - *E-mails*
 - *Printers*
 - *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:

- *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.
- *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: ☐ Manually ☒ 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

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 ☐ 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

Add

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.

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

Add IP address

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:

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:

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 and 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 network printers to zone

PRINTER

Printer type: ☐ Raw ☒ Shared

Printer name:

Network path:

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. 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. 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`. 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`. 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. Item choice **2. Domain**

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

WEB ADDRESS

Web address:	<input type="text" value="www.safetica.com"/>	Web address	
Level:	<input type="text" value="*.safetica.com/*"/>	<input type="text" value="www.safetica.com"/>	Remove
<input type="button" value="Add"/>			

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 [Protection](#) -> *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 the Records 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.

Add local path
Add network path

Path	Access	
Local paths		
C:\backup	<input checked="" type="checkbox"/> Read only	Remove
D:\data\01	<input checked="" type="checkbox"/> Allow	Remove
Network paths		
\\backup-server	<input checked="" type="checkbox"/> Allow	Remove
Drives		
A	<input checked="" type="checkbox"/> Deny	
B	<input checked="" type="checkbox"/> Deny	
C	<input checked="" type="checkbox"/> Read only	
D	<input checked="" type="checkbox"/> Read only	
E	<input checked="" type="checkbox"/> Deny	
F	<input checked="" type="checkbox"/> Deny	

Path rules

You can specify access rights for three types of paths:

- *Local paths* – path to folders on an endpoint (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 *OneDrive Personal*, *OneDrive Business*, *SharePoint*, *Google Drive*, *Dropbox* 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* – feature is not set. Settings are inherited from the higher-level group.
- *Block* – 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.

Records

There are following charts in the Records 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:

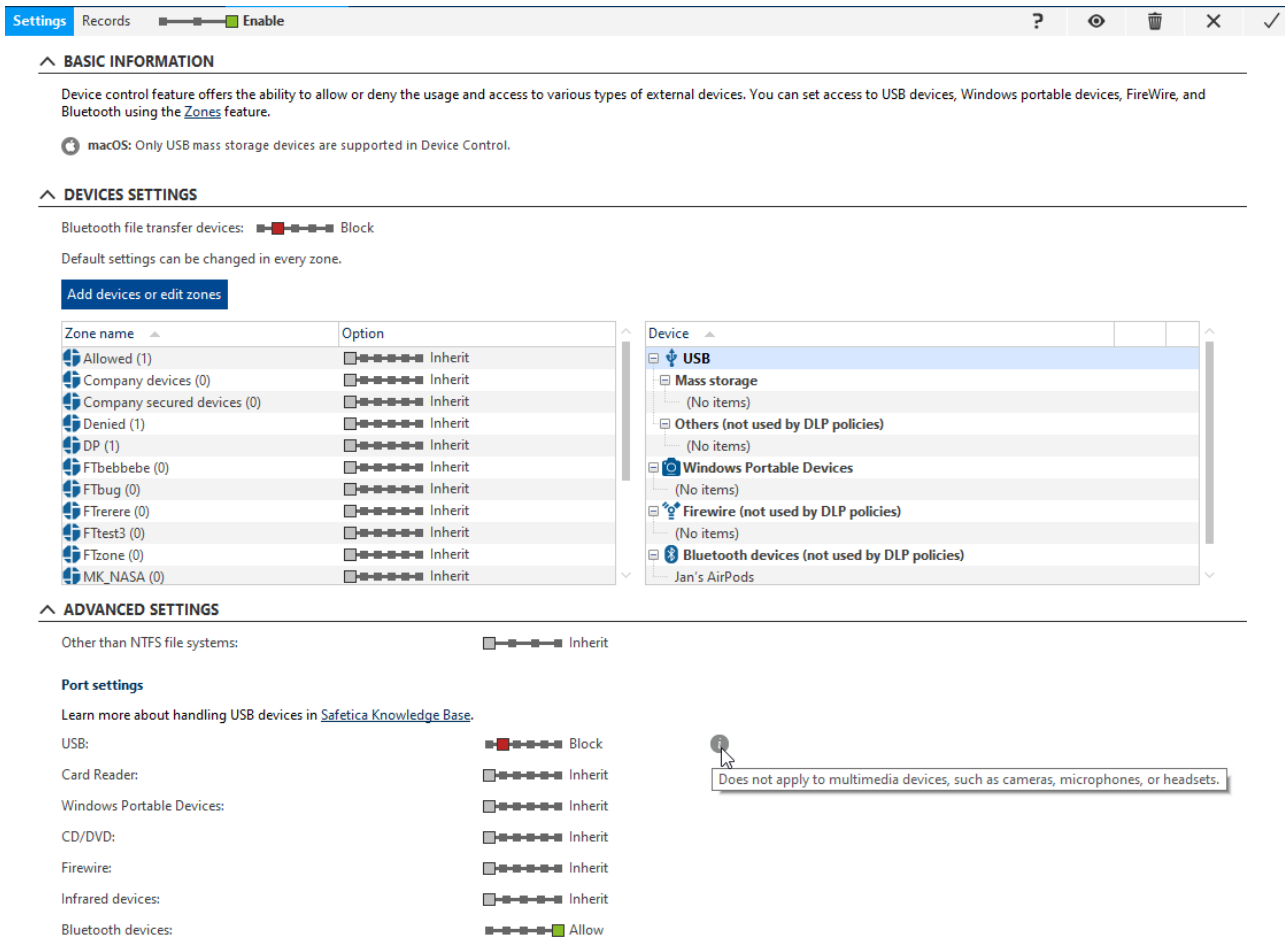
- *Date and Time* – date and time when the record was logged.
- *PC* – name of the PC where the record was taken.
- *User Name* – the name of the user under whom the record was made.
- *Application* – name of the application which used the access path or disk.
- *Source* – the name and path of the file 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.
- *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 Records mode in chapter [Records 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](#).

In the [console setting](#) mode, you can switch off or switch on this feature by using the slide bar in the view header.



Devices settings

In this section, you can specify in more detail the basic properties of Device control.

With the **Bluetooth file transfer devices** slider, you can apply DLP restrictions only to Bluetooth devices that can transfer files (e.g. notebooks or smartphones). This is different from the **Bluetooth devices** slider in **Advanced settings** which applies restrictions to **all** Bluetooth devices.

Example: You can select **Block** with the **Bluetooth file transfer devices** slider, and **Allow** with the **Bluetooth devices** slider in **Advanced settings**. This way, devices with a storage will be blocked, but devices without storage (such as headphones or cameras) will be allowed.

You can override both settings by adding devices to zones and adjusting these to your liking.

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:

- *Inherit* – settings are inherited from the parent group.
- *Block* – reading and writing on the external devices is disabled.
- *Read only* – the external device can only be read from, but not written to.
- *Notify* – when using an external device, the user will see a notification in the dialog box and a corresponding record will be created.
- *Test mode* – similar behavior 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 behavior of

the setting.

- *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 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.

You can also specify, how you will handle different types of external devices.

Types of devices (ports):

- USB - learn more about how Safetica handles USB devices in [Safetica Knowledge Base](#).
- Card reader
- Windows portable devices
- CD / DVD
- FireWire
- Infrared devices
- Bluetooth devices
- 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.

Records

There are records about access to devices defined in settings mode. There are following charts in the Records 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 DLP 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*
- *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* – which DLP policy was applied.
- *Application* – in what application was action recorded.
- *Restriction reason* – what restriction setting was used when access to an external device was denied: *Port, Device, File system, Unlocking by Bitlocker has failed*.
- *Interface type* – the type of external device: *USB, Bluetooth, FireWire, IrDA, LPT, COM*.

You can learn more about the Records mode in chapter [Records mode](#).

4.6.7 BitLocker devices

This feature 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 feature (Windows 7 Ultimate, Enterprise, Windows 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 *Protection* -> *Bitlocker 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 *Protection* -> *Bitlocker 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.

4.6.8 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 <http://go.safetica.com/help/t8s38q>.

Note: Bitlocker Drive Encryption can only be used at endpoints with Windows 7 Ultimate, Enterprise, Windows 8.1 Pro and higher, Windows 10 Pro and higher, Windows Server 2008 R2 and higher. 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	<input type="checkbox"/> 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:
 - *Password* – when starting the PC, the user is prompted to enter the password set by the user when applying the policy.
 - *TPM* – the system disk is unlocked automatically in the start. The password is stored in a TPM security chip (<http://go.safetica.com/help/dhh7rl>).
 - *TPM+Pin* – 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 8.1 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 <http://go.safetica.com/help/57fgi4>.

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.

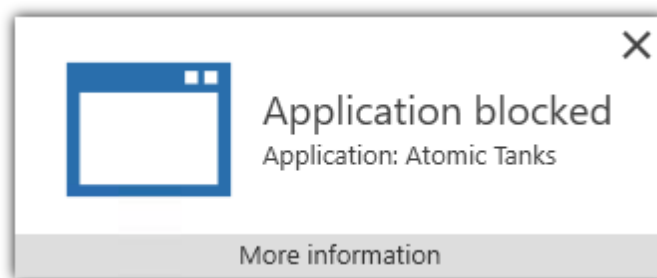
5 Endpoint Client

5.1 Notification Dialogs

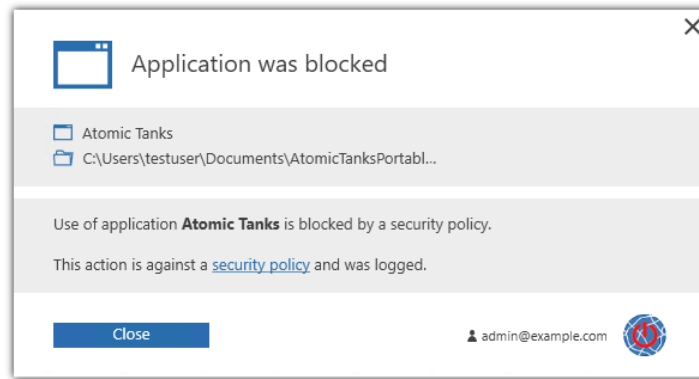
Safetica ONE Protection and Safetica ONE Enterprise display various notifications and messages to users, informing them about prohibited or permitted activities using notification dialogs.

The dialogs display in the lower right corner of the desktop. There are several types of notification dialogs. Each dialog requires different interaction with the user (confirmation, rejection, selection from options or paths).

Example of a notification dialog:

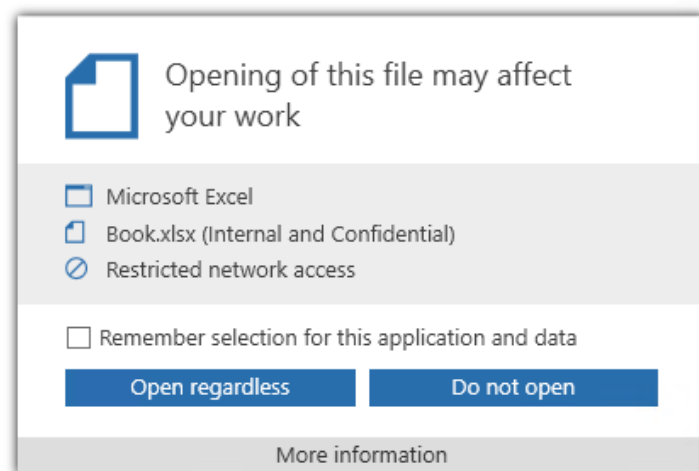


More details will be displayed after clicking on *More information*:

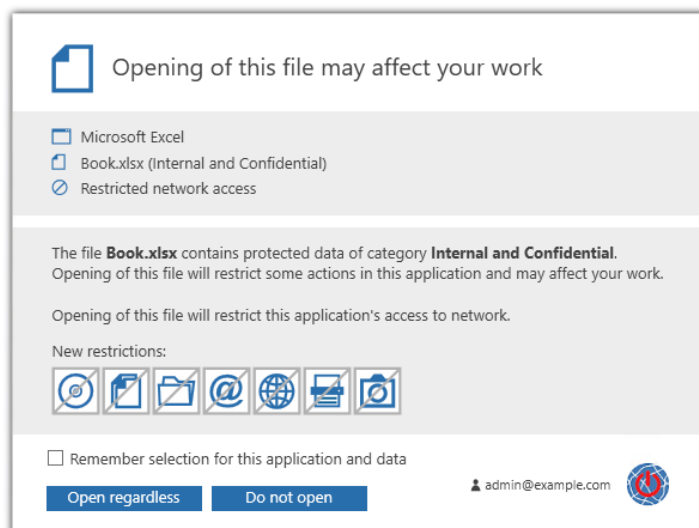


Notification when working with protected data

When the user opens data protected by the DLP policy, the information dialog will appear:



Clicking on the *More information* displays more details about restrictions applied on the application:



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

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.

