

| SAFETICA ONE INSTALLATION MANUAL

safetica

SAFETICA ONE INSTALLATION MANUAL

for 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	5
----------------------	---

Installation

1 Automatic installation	7
2 Manual installation	8
Before installation	8
Installing server	9
Microsoft SQL Server settings.....	11
Configuring an Existing SQL server	11
Microsoft SQL Server installation.....	12
Installing a new SQL Server Express	14
Configuring existing SQL Server Express	15
Installing console	16
Installing client	16
3 Initial configuration	18
Batch Installation of Downloader Agent using GPO	19
Manual installation of Downloader Agent	23

1 Introduction

Dear user,

Thank you for choosing Safetica ONE to protect your company. In this manual, you will find a step-by-step guide taking you through the whole installation process for all supported network environments. Should you encounter a problem during installation, first consult *Safetica ONE Complete Documentation*. If you do not find a solution there, 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.

After successful installation of the product, we recommend reading *Safetica ONE Complete Documentation*. Here you can find detailed information about initial deployment, examples of usage, evaluation of output, or how to solve the most frequent problems.

To quickly 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 individual 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 in-

stallation. 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:
 - o Decide on what PCs you are going to install the server in your environment. When making the decision, take the following into account:
 - The PC with Safetica server must be able to connect to the SQL server on which the main databases will be stored.
 - Depending on the number of SECs connected and the database server type, set how many servers you wish to install in your environment. The number of SECs that can connect to one server is limited by the SQL database which the server uses for storing

data – see below.

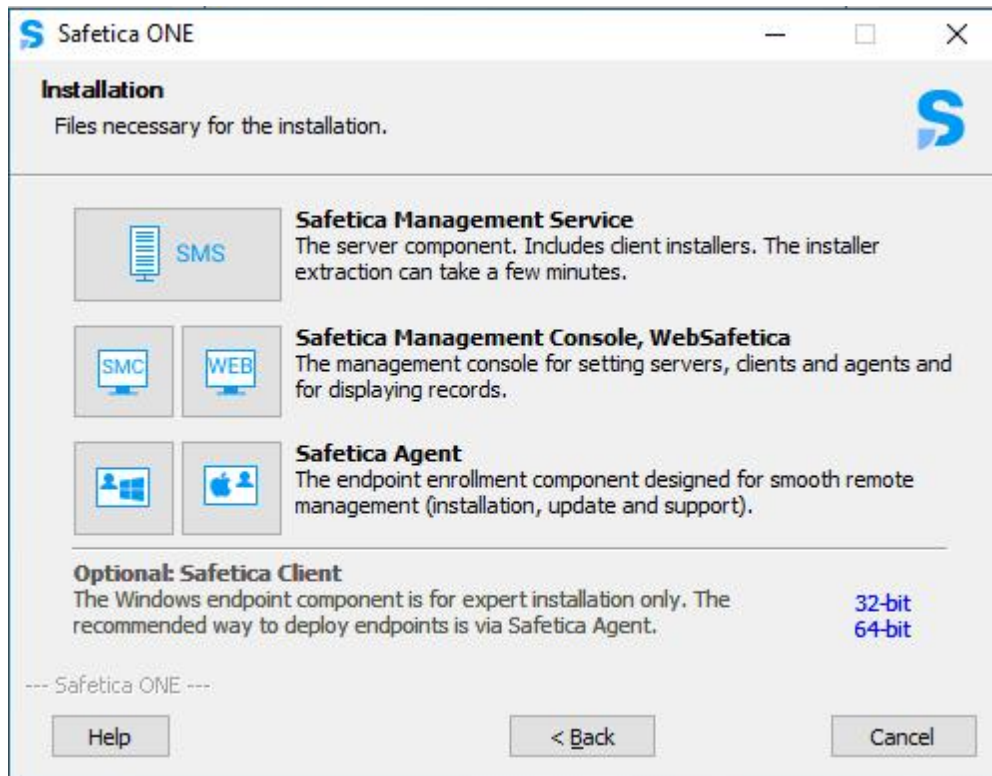
- Decide on what PCs you are going to install the console in your network. The PC with console must be able to connect to all servers you wish to administer by using the administration console.
 - Decide on what PCs you are going to install Downloader Agent in your network.
 - The PC with Downloader 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)

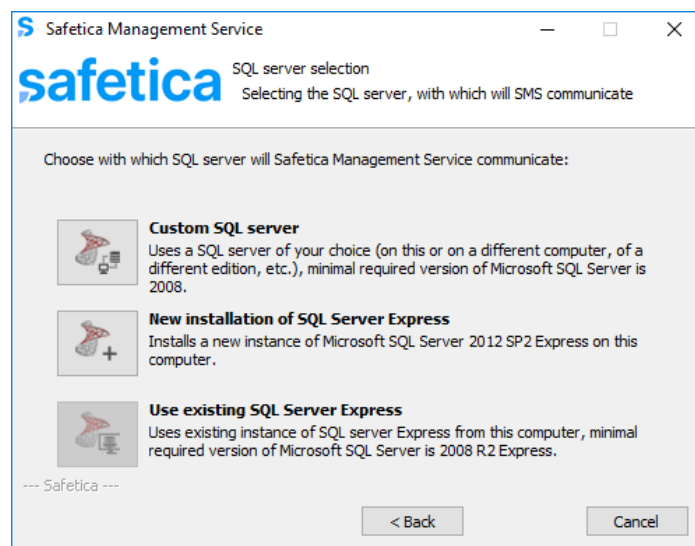
9. Finally, verify that you have added exceptions to your firewall and antivirus for the STASer-vice.exe process and that ports 4438, 4441 and 4442 are not blocked.

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](#).



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

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

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.

SQL Server 2008 Setup

Feature Selection

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

Setup Support Rules

Feature Selection

Instance Configuration

Disk Space Requirements

Server Configuration

Database Engine Configuration

Error and Usage Reporting

Installation Rules

Ready to Install

Installation Progress

Complete

Features:

Instance Features

☒ Database Engine Services

☒ SQL Server Replication

☒ Full-Text Search

☐ Reporting Services

Shared Features

☐ Business Intelligence Development Studio

☒ Management Tools - Basic

☒ SQL Client Connectivity SDK

☐ Microsoft Sync Framework

Redistributable Features

Description:

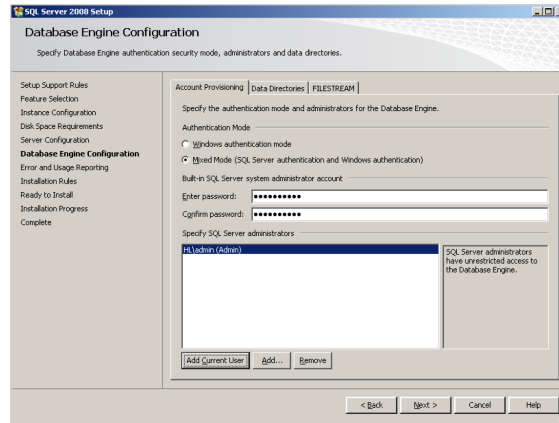
Includes Management Studio support for the Database Engine and SQL Server Express, SQL Server command-line utility (SQLCMD), and the SQL Server PowerShell provider.

Select All Unselect All

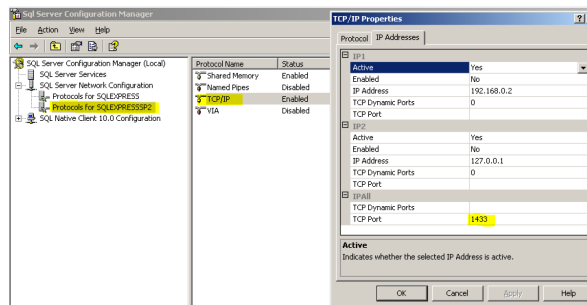
Shared feature directory: C:\Program Files\Microsoft SQL Server\

< Back Next > Cancel Help

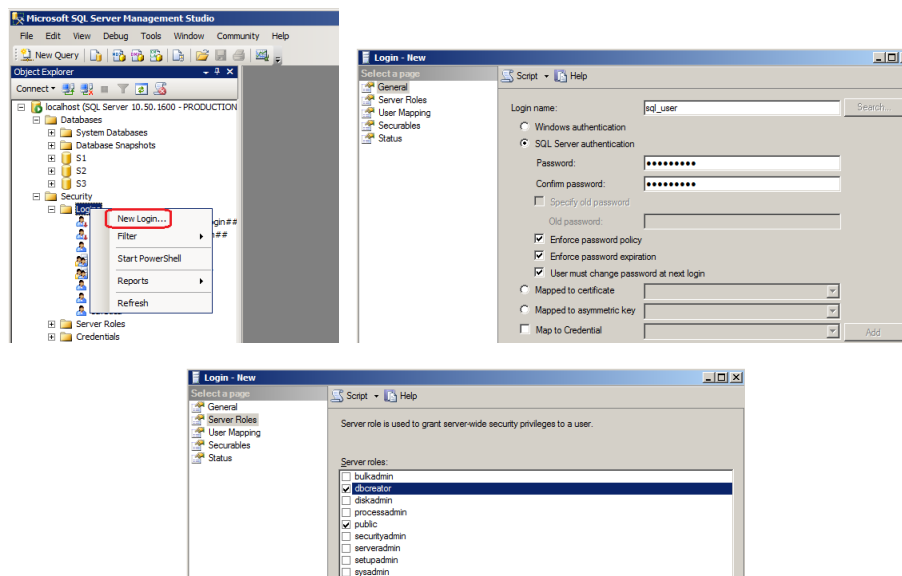
2. Set up Mixed mode authentication in the relevant installation step.



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.

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:

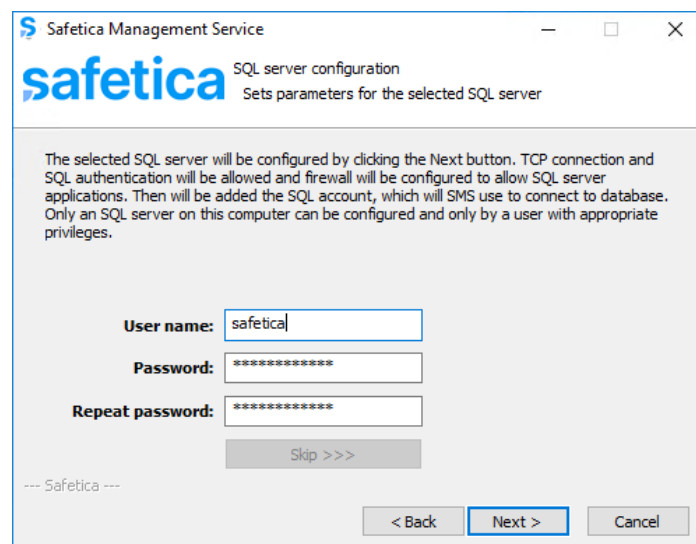
- The SQL server instance name is MSSQLSERVER.
- The default password for the user "sa" is set to "S@fetic@2004". The "sa" user will be used for database access.

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*.



The screenshot shows a window titled "Safetica Management Service" with a subtitle "SQL server configuration". Below the title bar, it says "Sets parameters for the selected SQL server". The main content area contains a paragraph of text: "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." Below this text are three input fields: "User name:" with the text "safetica" entered, "Password:" with asterisks, and "Repeat password:" with asterisks. There is a "Skip >>>" button below the password fields. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a blue border.

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 >>>

--- Safetica ---

< 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.

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*.

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 >>>

--- Safetica ---

< 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*.

The screenshot shows a window titled "Safetica Management Service" with a subtitle "Connection settings" and "SQL Server connection data". The Safetica logo is in the top left. A paragraph of text explains that data can be stored in the local registry for SMS to connect to a SQL database, and that some fields may be pre-filled. Below this, there are four input fields: "IP or address:" with the value "SERVER02", "User name:" with the value "safetica", "Password:" with masked characters "*****", and "Database name prefix:" with the value "safetica". A "Skip >>>" button is below the fields. At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel". The text "--- Safetica ---" is visible in the bottom left corner of the dialog area.

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 language and agreeing to the license terms, go to *Installation -> Safetica Management Console*.
2. Here you have 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

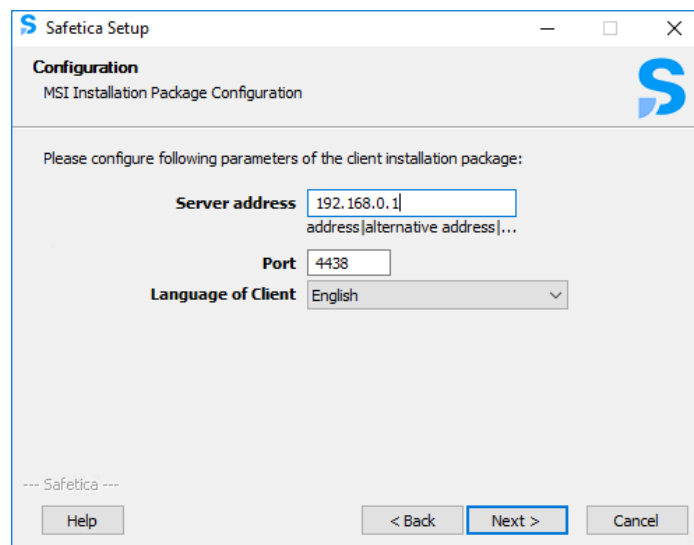
1. Launch the universal installer that you have previously downloaded. After selecting your language and agreeing to the license terms, go to *Installation > Safetica Management Client x86 or x64* – this depends on which operating system version is installed on the endpoint.
2. Here you several options: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

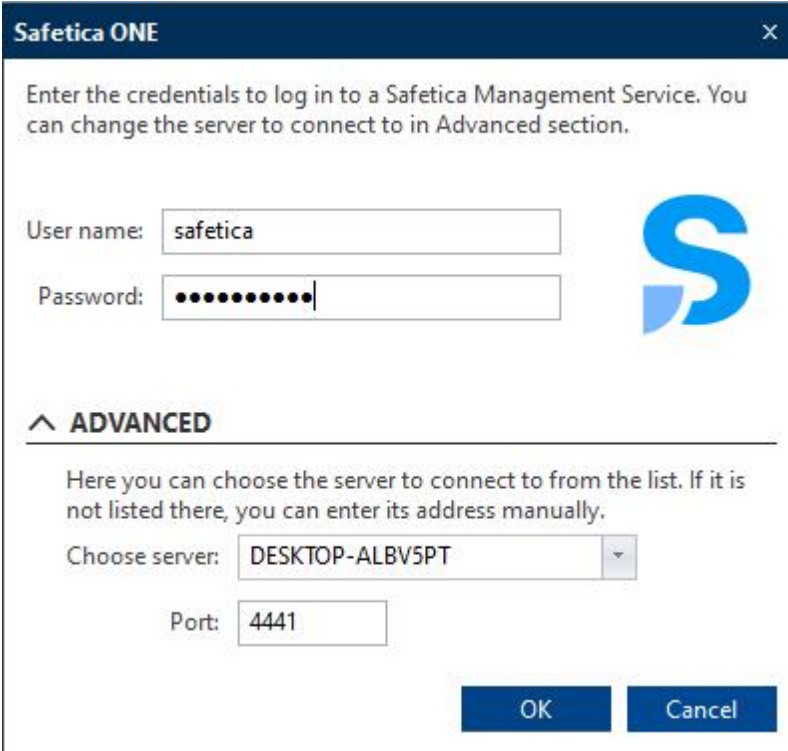
vices > STCSservice – running) and make sure that in your firewall and antivirus you have established exceptions for the following processes: STCSservice.exe, STPCLock.exe, STMonitor.exe, STUserApp.exe, and Safetica.exe.

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.

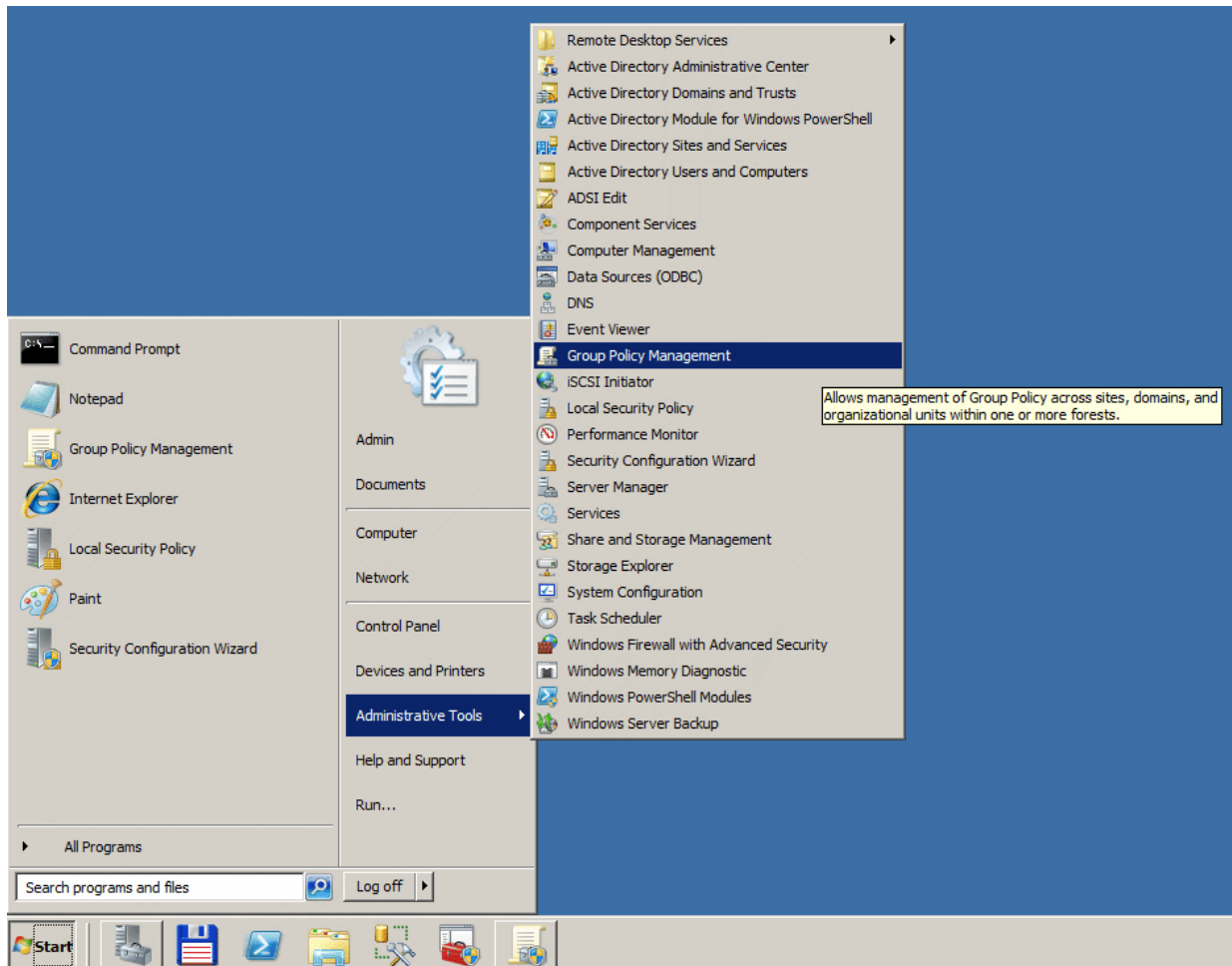
All settings can be changed or viewed in Safetica Management Console after you finish the initial configuration wizard.

3.3.1 Batch Installation of Downloader Agent using GPO

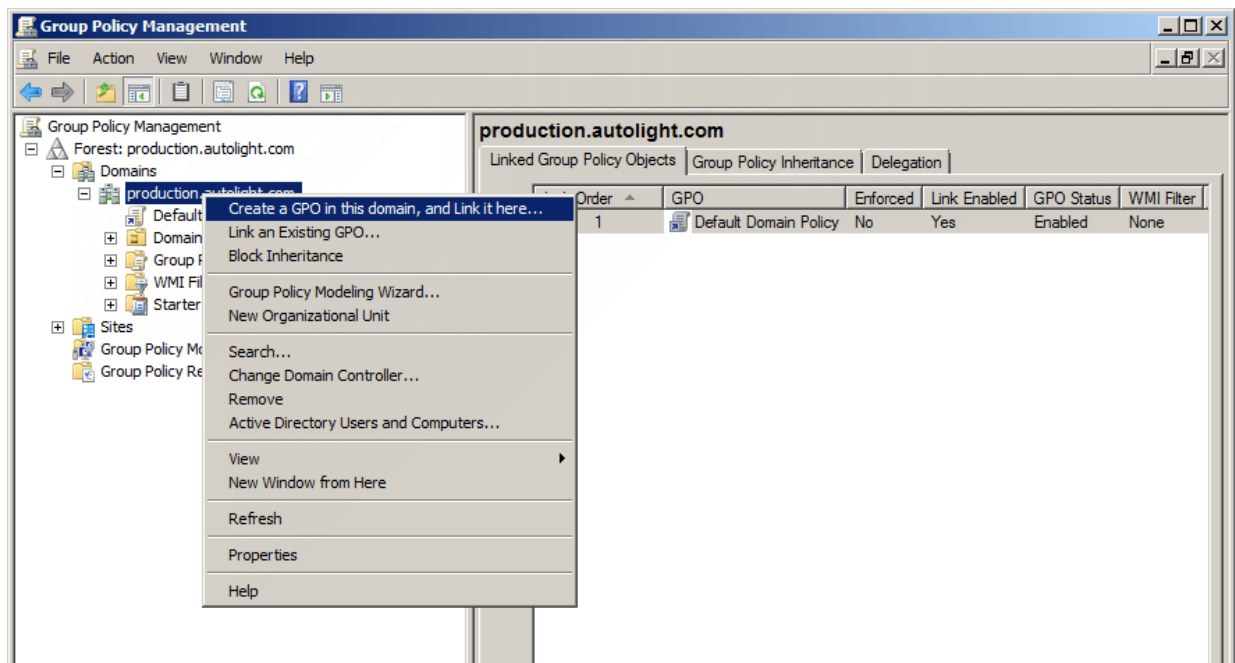
If you are using Active Directory, you can bulk install the Downloader Agent using a Group Policy. To use the bulk installation, it is necessary to extract the relevant MSI package of the Downloader Agent from the universal package.

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.

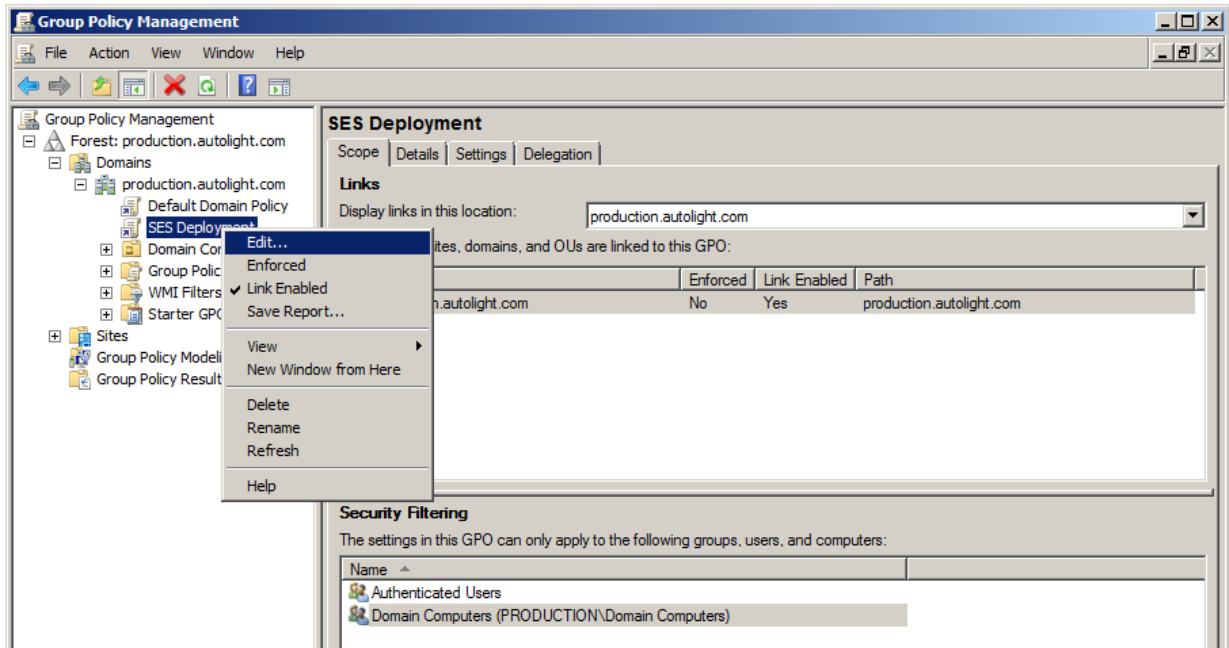
1. Start the Safetica universal installer.
2. Go to *Installation -> Downloader Agent -> Extract installer*. In the installer configuration, enter the server address and port to which the Downloader Agent will connect. Save the installation package on a shared disk or shared directory in the corporate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



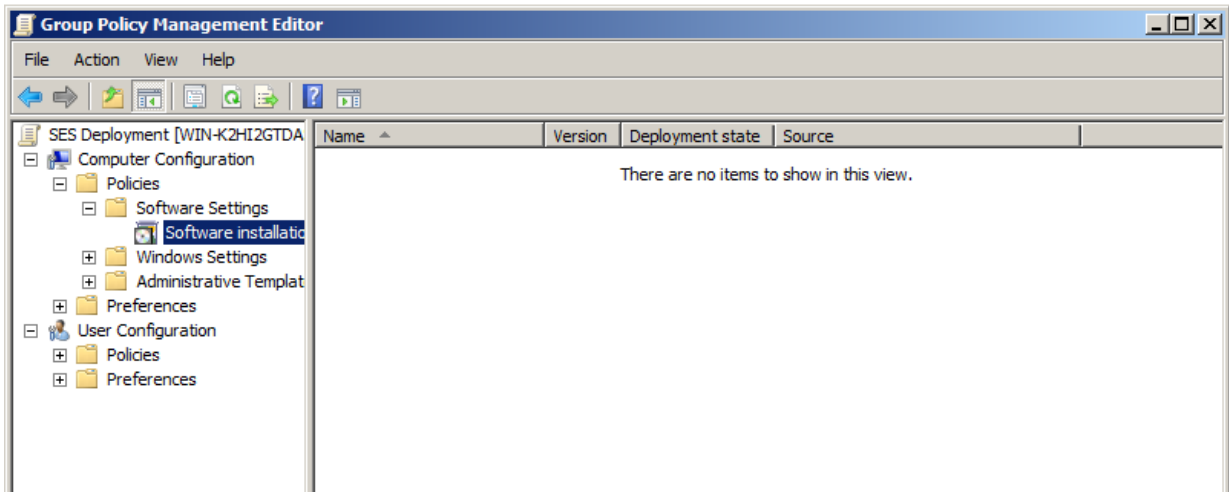
4. Right-click the organizational unit to which you want to deploy the Downloader Agent and select *Create a GPO in this domain and link it here ...*



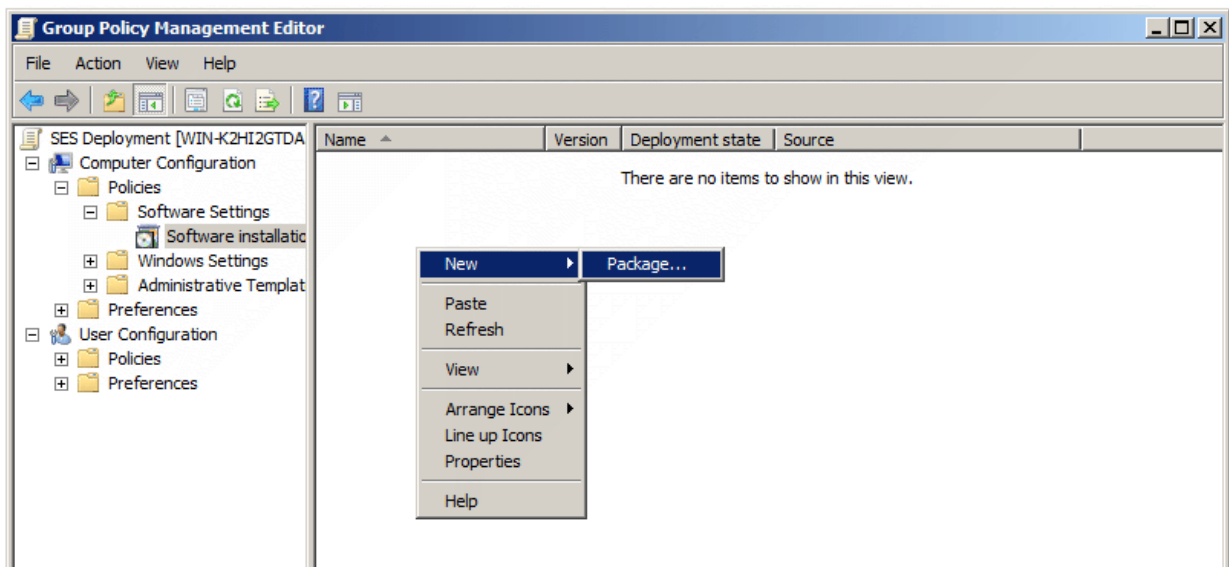
5. Give an arbitrary name to the new object (for example, Safetica Deployment).
6. Select your newly created group policy and right-click to select *Edit*.



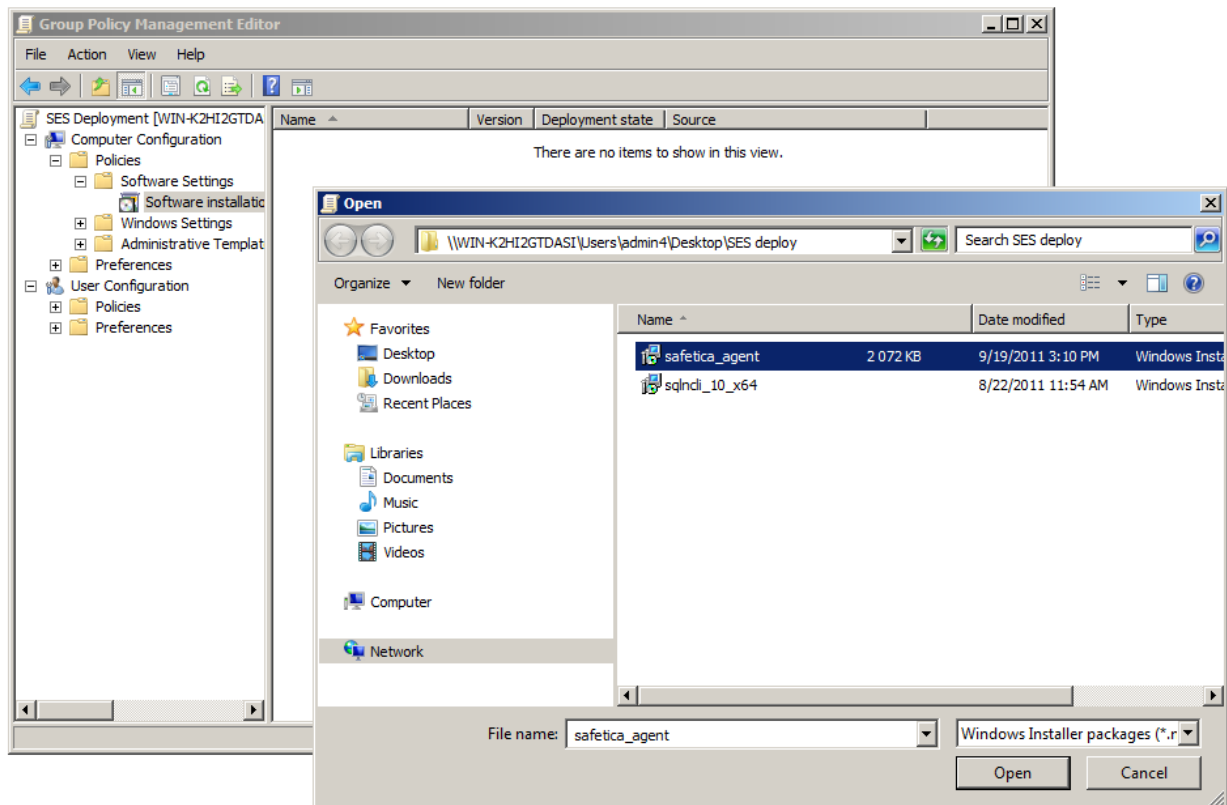
7. In the window that opens, navigate to *Computer Configuration -> Policies -> Software Settings* and click on *Software installation*.



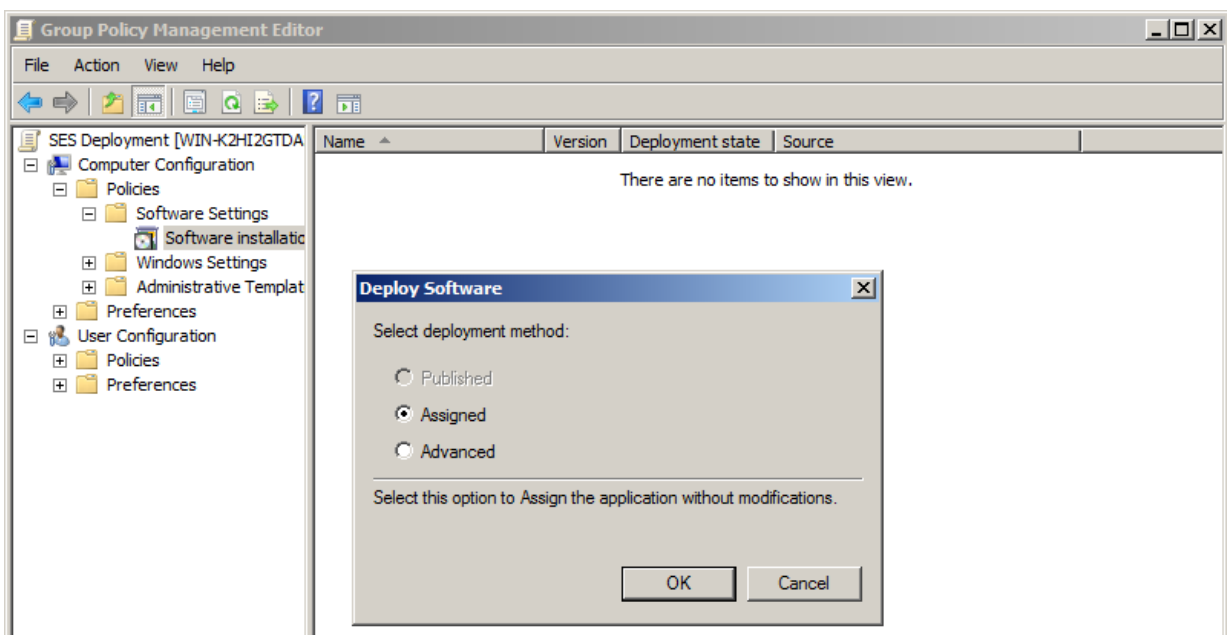
8. Right-click on the window with a list of software and select *New Item -> Package ...*



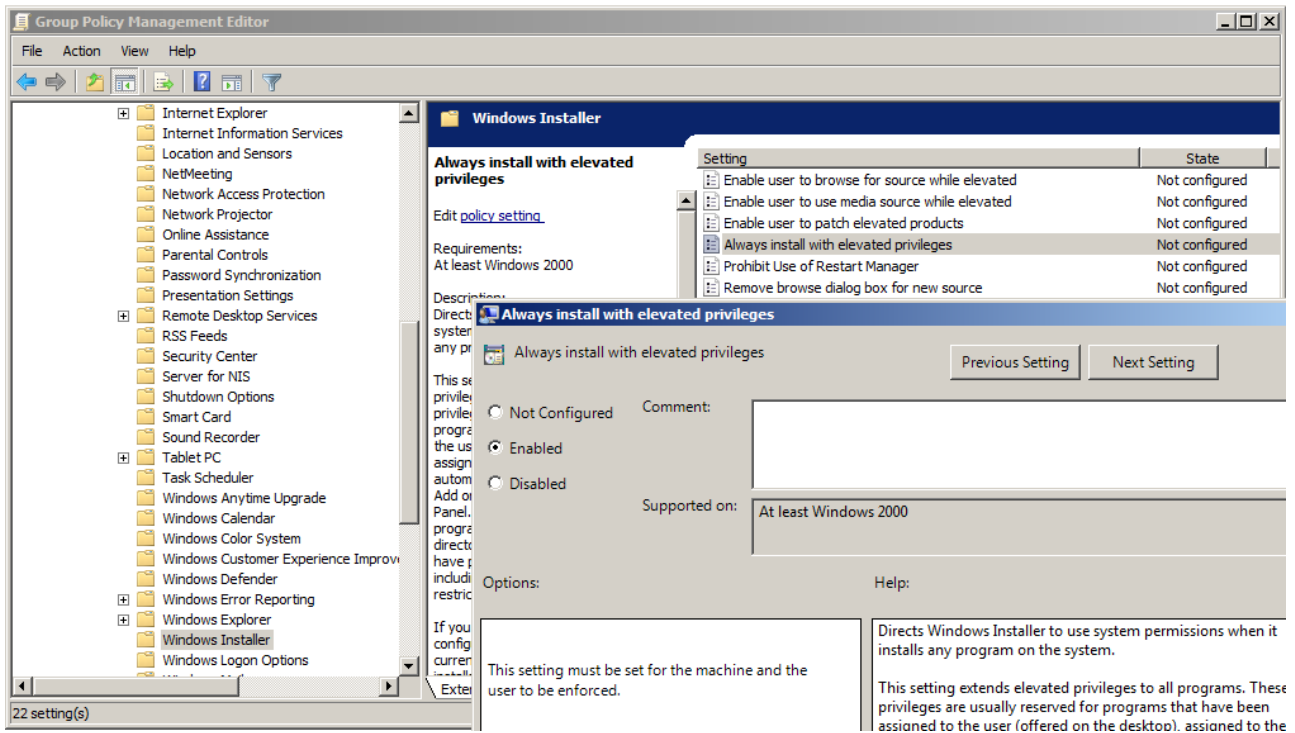
9. In the MSI package selection dialog box, navigate to the shared network folder where you copied the MSI package with Downloader Agent, and select it.



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.

