EGOSECURE DATA PROTECTION

Installation guide

Version 23.0.3

Updated: January 2024

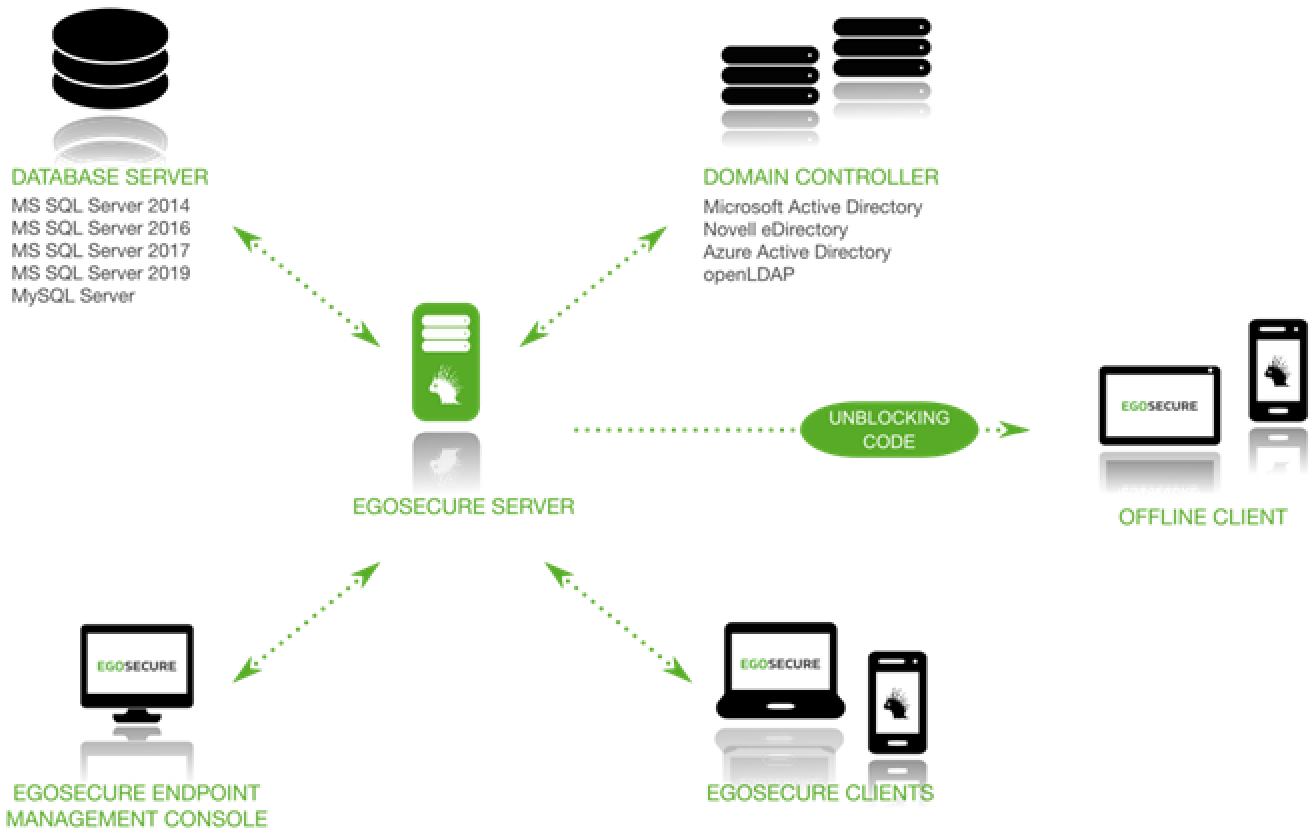
Matrix42 GmbH
Elbinger Street 7
60487 Frankfurt am Main

Telephone: +49 69 667738 222
E-Mail: helpdesk@matrix42.com
Self Service Portal: support.matrix42.com
Internet: https://matrix42.com

CONTENTS

1. About EgoSecure Data Protection

1.1. System architecture



EgoSecure Server:

- Installed on any computer in your network.
- Handles the central management of your EgoSecure clients.
- Synchronizes with your existing Microsoft Active Directory, Novell eDirectory, LDAP (Lightweight Directory Access Protocol) or Azure Active Directory, and stores it in its own database.

ATTENTION	**Active Directory schema** The Active Directory schema synchronizes as is, no changes are made. EgoSecure Data Protection creates a copy of the structure which is updated afterwards. A user with read-only rights is required for synchronization.

- Manages all data in an SQL database.
- Transmits any changes to the clients immediately, and saves them in the database.

ATTENTION	**Applying changes** All changes in **User management** and **Computer management** section take effect immediately.

EgoSecure Agent (Client):

- Uses a push/pull process to get any changes from the server.
- Transmits all communication between the console, server, kernel driver, and user.
- Offline management: rights changes for a system or a use outside a corporate are applied via the unblocking code.

ATTENTION	**Connection between systems and users** For network load efficiency, the connection between systems and users occurs on rights changing. If polling is enabled, the connection occurs according to a defined time interval.

Kernel filter driver:

- Installed on the Windows system with EgoSecure client component.
- Controls access rights to external devices and applications.
- Applies the assigned permissions.
- Enforces permissions set for offline clients.
- Provides a high degree of security.

1.2. Tools

EgoSecure Console:

- Controls the functionality of **EgoSecure Data Protection**.
- Functions irrespective of the location, i.e. can be installed and launched on any workstation.

EgoSecure Admin Tool:

- Used to adjust EgoSecure Server settings.
- For details about Admin Tool, see chapter 6.

2. System Requirements

2.1. Hardware requirements

To use EgoSecure products, your system must meet the following minimum hardware requirements:

EgoSecure Server

Components	Minimum	Recommended
RAM	2 GB	4 GB
Free hard disk space	20 GB	50 GB
Processor	Dual core	Quad core

EgoSecure Agent (Client computer)

Components	Minimum	Recommended
RAM	2 GB	4 GB
Free hard disk space	5 GB	15 GB
Processor	Dual core	Quad core

Database

To use **EgoSecure Data Protection**, an SQL database is required. The required hard disk space varies greatly depending on the product usage.
We recommend to not change the default auto growth and maximum size parameters of the database.
The **Secure Audit** module can generate large amounts of data, especially in combination with other modules.

2.2. Software requirements

To use the EgoSecure products the system must meet the requirements below. Starting from **EgoSecure Data Protection** 13.1, the **EgoSecure Server** can be installed only on 64-bit systems, but the **EgoSecure Console** is available both in 32- and 64-bit versions under **Program Files/EgoSecure/EgoSecure Server**.

Server

Operating system
Windows Server 2016, 2019 or 2022 (to 22H2)
Windows 10 (to 22H2) or 11 (to 23H2)

You can use an existing SQL Server or install a separate SQL Server.

SQL Server
Microsoft SQL Server: 2014, 2016, 2017, 2019, or 2022 Express edition of the enumerated above Microsoft SQL Server versions is also supported.
MySQL Community Server 5 and higher ! Support for MySQL will be withdrawn in 24.0.0

Client

Operating system
Windows 10 (to 22H2) or 11 (to 23H2)
Windows Server 2016, 2019 or 2022 (to 22H2) ! The EgoSecure Antivirus ATC module is not supported on Windows Server.

Support of
Remote Desktop Services
Citrix XenApp & XenDesktop 7.15 LTSR
Citrix Virtual Apps and Desktops 7 1912 LTSR

Service Bus Adapter

Operating system
Windows Server 2016, 2019 or 2022 (to 22H2)
Windows 10 (to 22H2) or 11 (to 23H2)

3. SQL Server Installation

3.1. Installing Microsoft SQL Server

Please, pay attention to the following points before installing the SQL Server:

Using Microsoft SQL Express Server

- Use Express versions of Microsoft SQL Server only for demonstration purposes and for very small organizations.
- SQL Express Server size is limited to 10 GB. This limit may be reached quickly, especially when using **Secure Audit**. In this case errors will occur when executing **EgoSecure Data Protection**.

Connecting to the Microsoft SQL Server

When using the named instances on the Microsoft SQL Server, meet the following conditions so that the EgoSecure Server can connect to the SQL Server during the installation and can create the database for EgoSecure:

- **Firewall**: Open ports *1434/udp* and *1434/tcp* and set the *SQL Browser* service to *Start Automatically*.
- **Firewall**: Allow the application for incoming connections. The SQL server executable file can usually be found at `%ProgramFiles%\Microsoft SQL Server\`*`<name of instance>`*`\MSSQL\Binn\sqlservr.exe`.
- Assign the *dbcreator* server role for the SQL user used for the EgoSecure installation. After the installation, the *dbowner* server role can be assigned instead.

INFO

Microsoft SQL Express

Microsoft SQL Express always uses a named instance.

Logging in to the database

- **Database authentication via a mixed mode**:
  To select the mixed mode as the authentication method during the database installation, perform a custom installation depending on the version number, or customize the authentication method in the SQL Installation Center later.
- **Database authentication via Windows user account**:
  To login to the database using a Windows user account, specify an authorized Windows user during the EgoSecure Server installation. For details, see Windows authentication.

4. EgoSecure Server Installation

4.1. Before installation

Make sure that the following requirements are met:

- EgoSecure Data Protection installation file (available in the EgoSecure download area);
- License key (.lic & .txt) (not required for trial installation);
- Minimum hardware requirements;
- User with read access to Microsoft Active Directory/Novell eDirectory/LDAP;
- SQL user with a permission to create databases.

4.2. Preparing the installation

Please check that the following preparations are done:

- **SQL-server installed**. If an SQL-server is installed, start the installation immediately. Otherwise, install an SQL-server first.
  For details about free installation of SQL Server Express, see chapter SQL Server Installation.
- **Case-insensitive collation selected**. Select a case-insensitive collation in the database server settings so that the EgoSecure Server can identify the computers and users by name correctly.
  Case-insensitive collation example: `SQL_Latin1_General_CP1_CI_AS`.

4.3. Installation

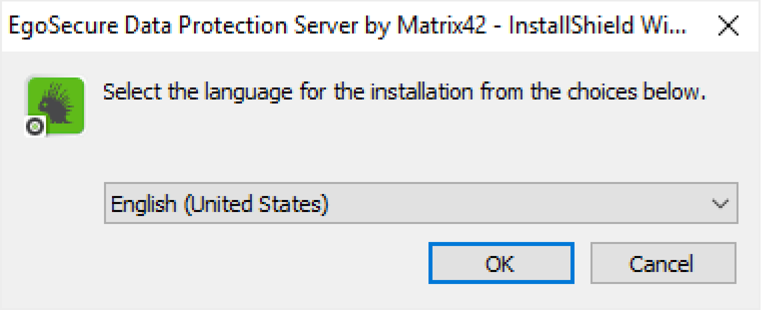
To work with **EgoSecure Data Protection**, install the Server components on your server. The following components of **EgoSecure Data Protection** are installed:

- EgoSecure Data Protection Console
- EgoSecure Server (Service)
- EgoSecure AdminTool

Installing server components

1. Open the setup file (EgoSecureSetup_x64.exe).

   → The installation routine in InstallShield opens.

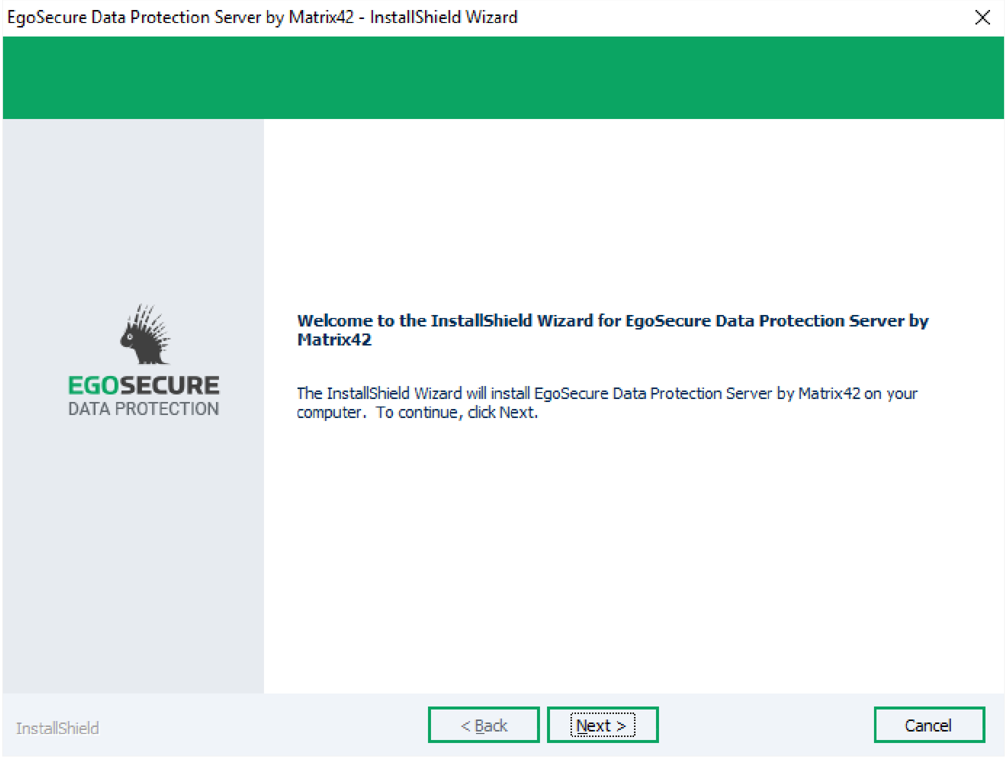


EgoSecure Data Protection Server by Matrix42 - InstallShield Wi...

Select the language for the installation from the choices below.

English (United States)

2. Select the language of the setup process and click **OK**. The welcome dialog opens.
3. In the **Welcome** dialog, click **Next** to continue.

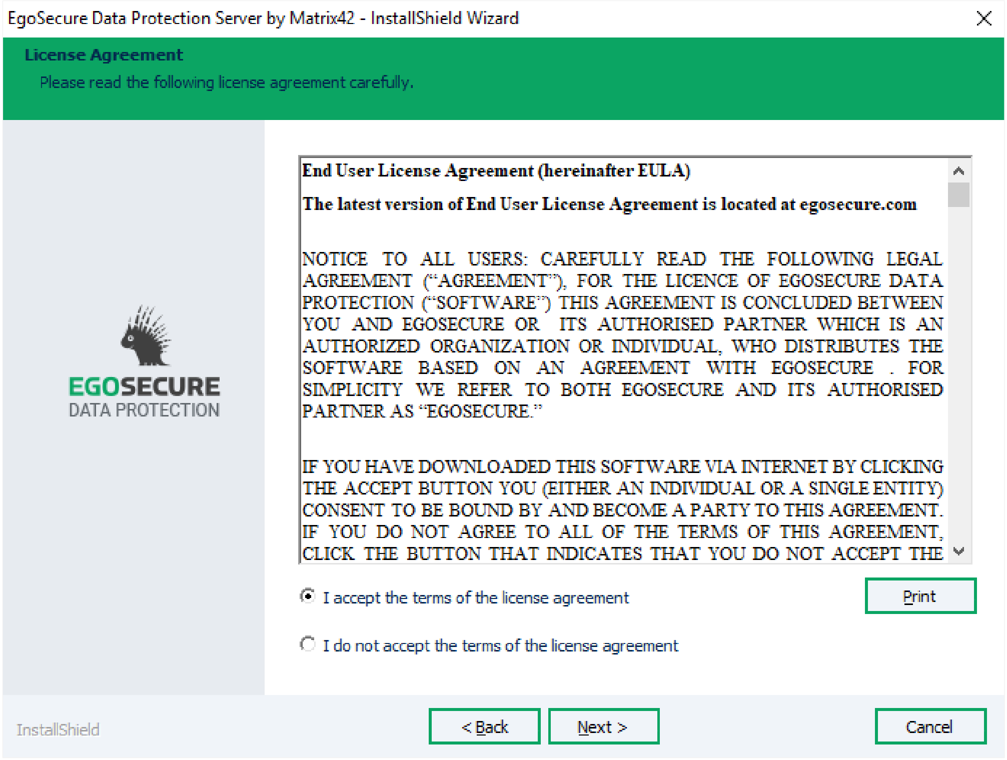


EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Welcome to the InstallShield Wizard for EgoSecure Data Protection Server by Matrix42

The InstallShield Wizard will install EgoSecure Data Protection Server by Matrix42 on your computer. To continue, click Next.

4. Select **I accept the terms of the license agreement** and click **Next**.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

End User License Agreement (hereinafter EULA)

The latest version of End User License Agreement is located at egosecure.com

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF EGOSECURE DATA PROTECTION ("SOFTWARE") THIS AGREEMENT IS CONCLUDED BETWEEN YOU AND EGOSECURE OR ITS AUTHORISED PARTNER WHICH IS AN AUTHORIZED ORGANIZATION OR INDIVIDUAL, WHO DISTRIBUTES THE SOFTWARE BASED ON AN AGREEMENT WITH EGOSECURE . FOR SIMPLICITY WE REFER TO BOTH EGOSECURE AND ITS AUTHORISED PARTNER AS "EGOSECURE."

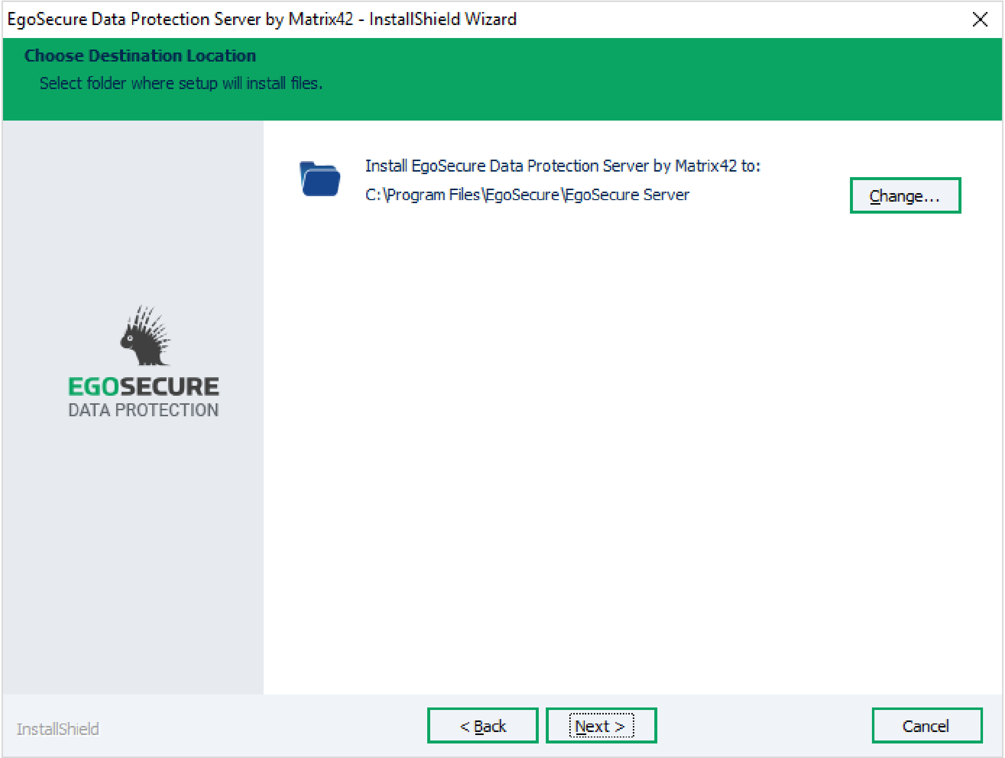
IF YOU HAVE DOWNLOADED THIS SOFTWARE VIA INTERNET BY CLICKING THE ACCEPT BUTTON YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

Figure 1. License agreement

5. Click **Next** to install **EgoSecure Data Protection** in the default folder. Click **Change...** to specify another installation path.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

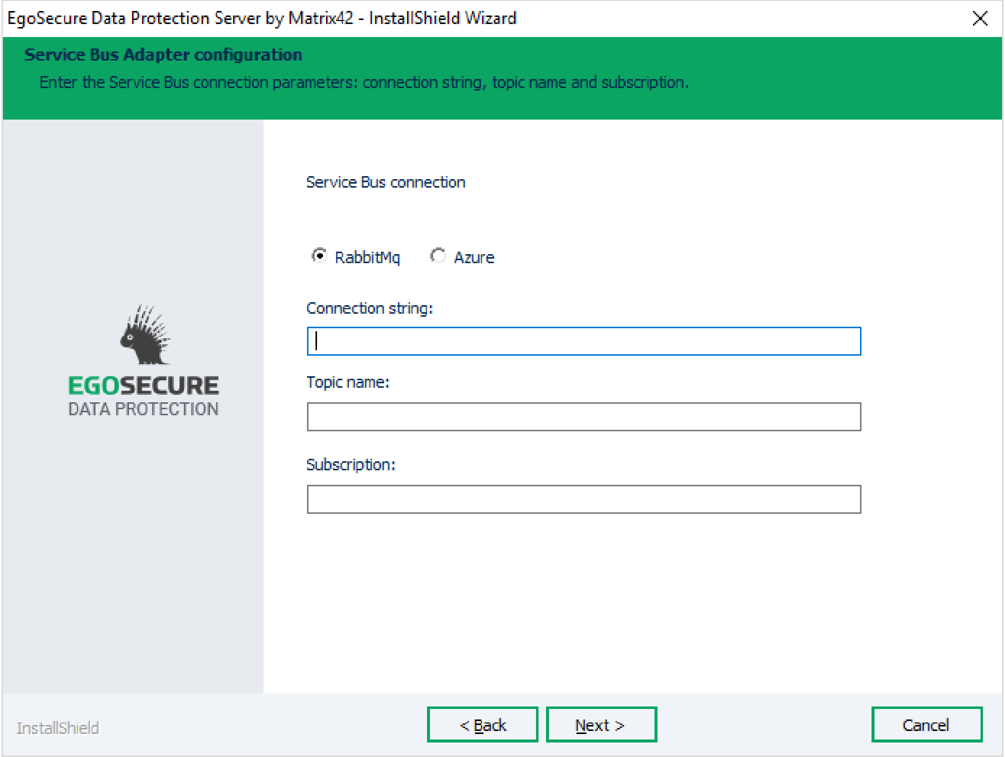
Install EgoSecure Data Protection Server by Matrix42 to:
C:\Program Files\EgoSecure\EgoSecure Server

Figure 2. Installation path

→ The dialog for selecting additional components for installation appears.

6. Enable EgoSecure Service Bus Adapter if you want to install it and click **Next**. For details about EgoSecure Service Bus Adapter, see the article.

   → If you selected to install EgoSecure Service Bus Adapter, the dialog for configuring parameters appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Service Bus Adapter configuration

Enter the Service Bus connection parameters: connection string, topic name and subscription.

Service Bus connection

● RabbitMq ○ Azure

Connection string:

Topic name:

Subscription:

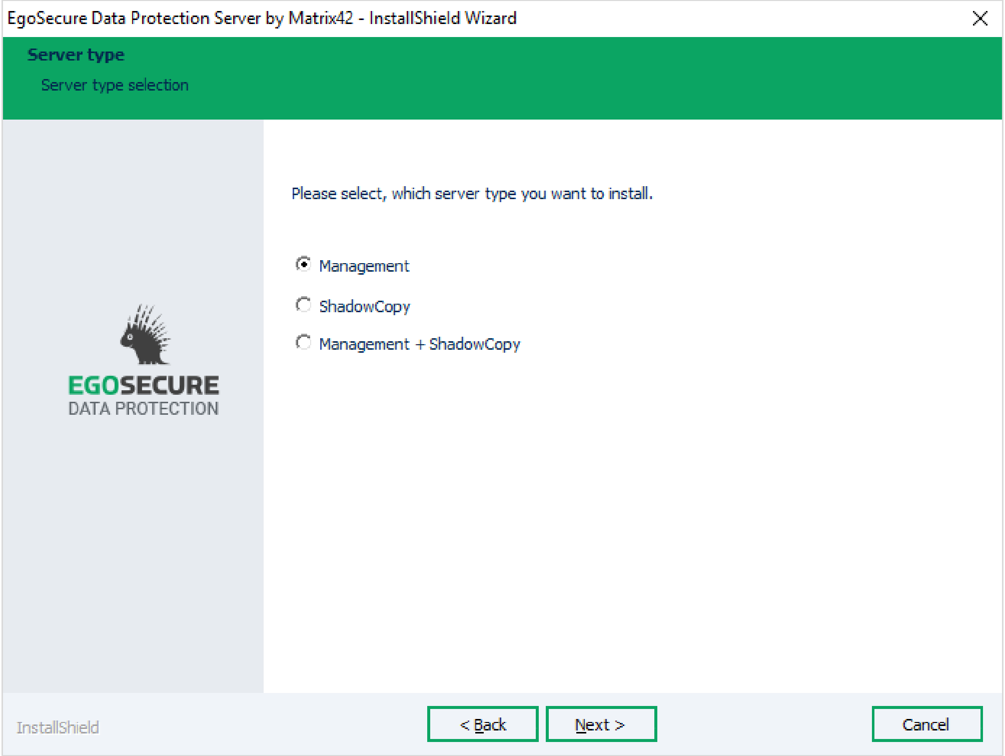
7. Define configuration parameters for EgoSecure Service Bus Adapter:
   a. Select which Service Bus system you use: **RibbitMq** or **Azure**.
   b. Fill in the **Connection string**, **Topic name** and **Pipeline name** fields, with the data from the Service Bus system you already have.

   The configuration parameters can later be changed in the Admin Tool.
8. Click **Next**.

   → The dialog for selecting the EgoSecure Server type appears.

9. Select the server type and click **Next** to continue.

   The server type can later be changed in the Admin Tool.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Server type

Server type selection

Please select, which server type you want to install.

● Management

○ ShadowCopy

○ Management + ShadowCopy

Figure 3. Server type

→ The dialog for specifying ports appears.

10.Define the following ports:

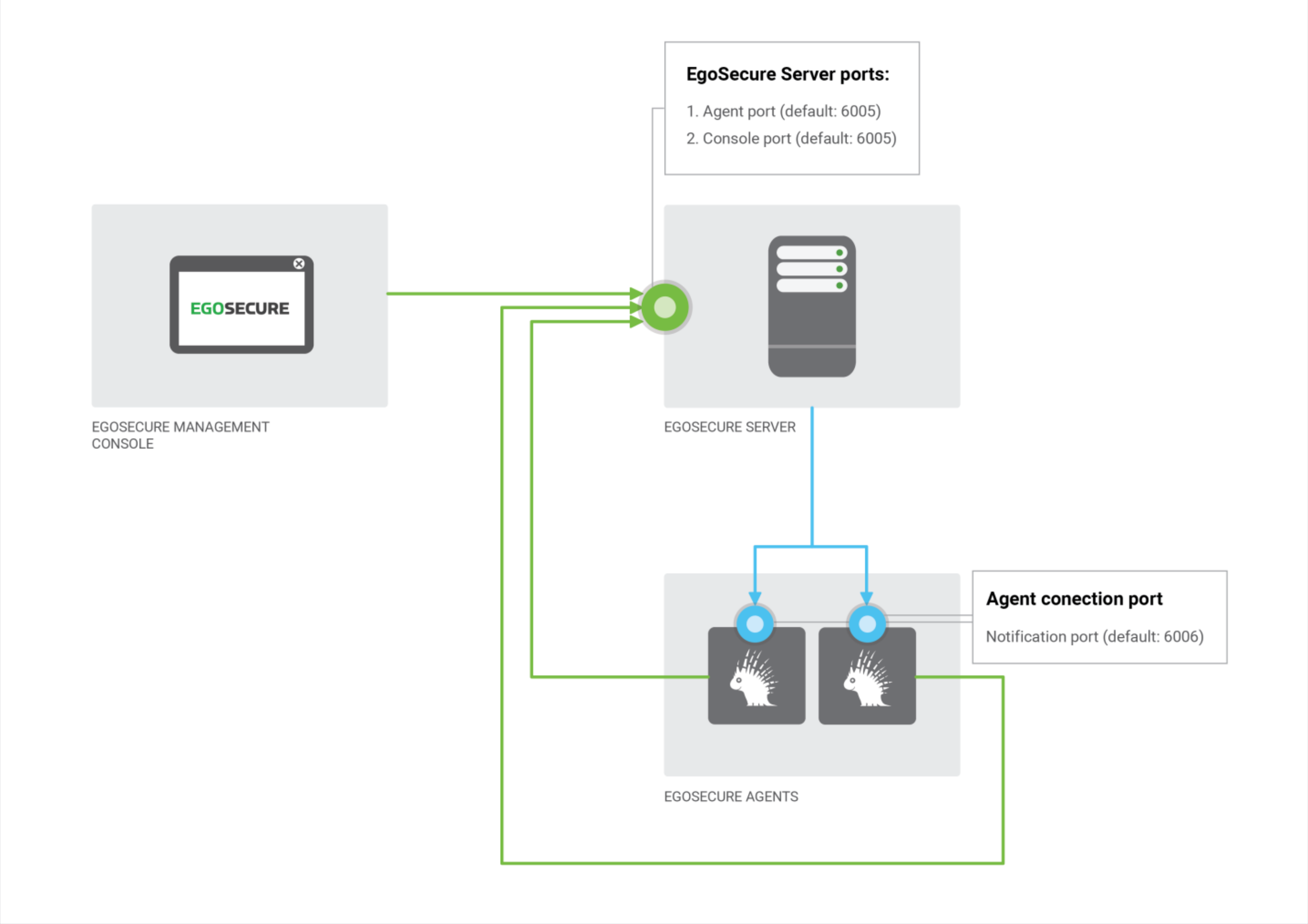
- *Server Connection Port* (default value: 6005) is a port on the Server for incoming data traffic used by the Agents and the Console to connect to the Server. In the Admin Tool, server connection ports are represented with the **Agent** port and the **Console** port.

ATTENTION

Port overloading problem

If you have a huge number of Agents, the port 6005 may be overloaded by Agents and Console has to wait for the connection.
Solution: prioritize the Console connection by specifying another port for Console in the Admin Tool once the installation is finished.

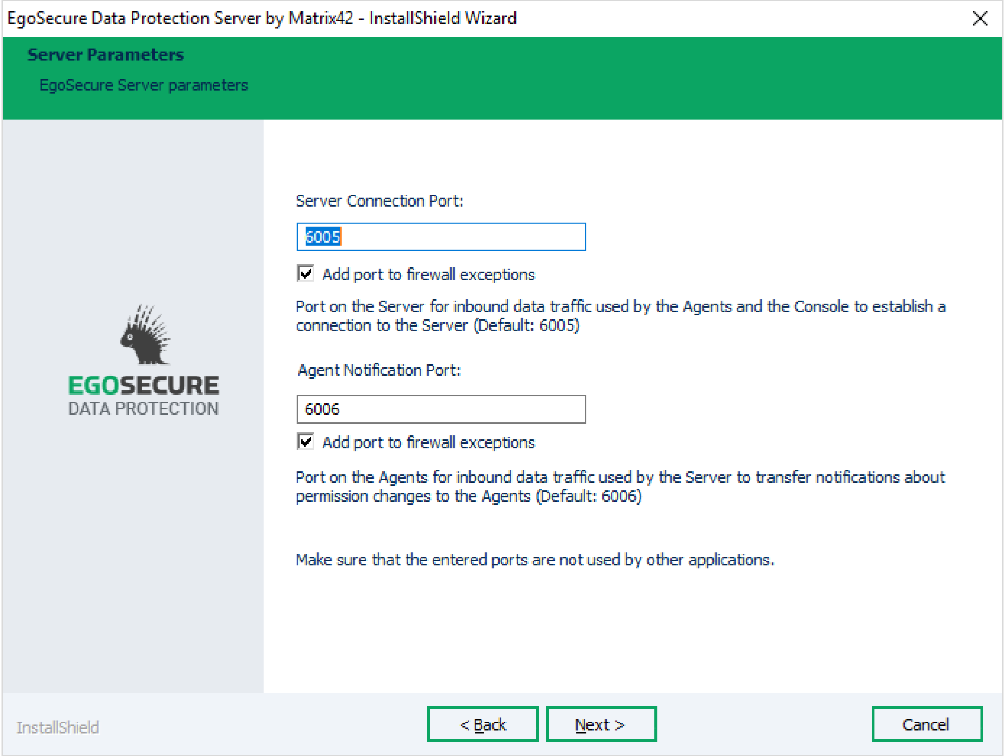
- *Agent Notification Port* (default value: 6006) is port on the Agents for incoming data traffic used by the Server to send notifications about permission changes to the Agents. **If the polling mode is enabled**, the Agent notification port is not used by the Server, because in case of polling the Server doesn't send notifications directly to the Agent. Notifications are stored in the database till the moment the Agent checks for them during one of its polling intervals.



EgoSecure Server ports:
1. Agent port (default: 6005)
2. Console port (default: 6005)
EGOSECURE
EGOSECURE MANAGEMENT CONSOLE
EGOSECURE SERVER
Agent conection port
Notification port (default: 6006)
EGOSECURE AGENTS

11. To add the specified port as a firewall inbound rule for EgoSecure automatically, enable **Add port to firewall exceptions**. To add exception ports on server and client computers manually, create an inbound rule on the Server (TCP 6005, Allow the connection) and on the Agent (TCP 6006, Allow the connection) in the **Advanced settings** of the Windows Firewall.

ATTENTION	**Adding ports** Adding ports as exceptions is highly recommended, because it ensures the communication between Agent and Server.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Server Parameters

EgoSecure Server parameters

Server Connection Port:

6005

☑ Add port to firewall exceptions

Port on the Server for inbound data traffic used by the Agents and the Console to establish a connection to the Server (Default: 6005)

Agent Notification Port:

6006

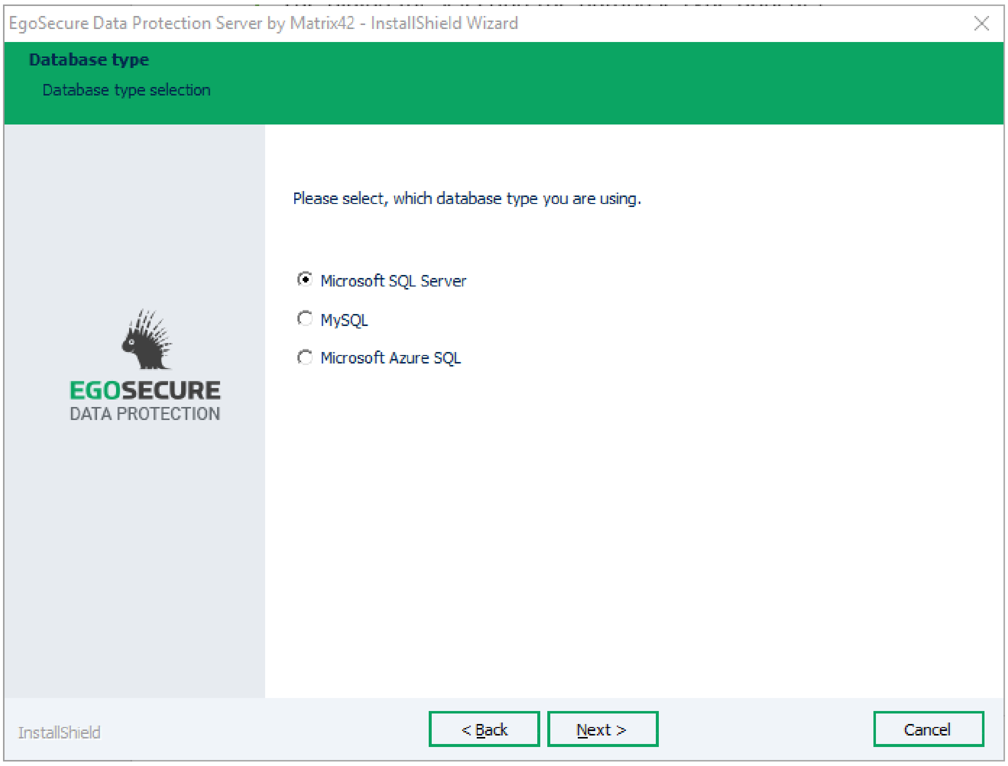
☑ Add port to firewall exceptions

Port on the Agents for inbound data traffic used by the Server to transfer notifications about permission changes to the Agents (Default: 6006)

Make sure that the entered ports are not used by other applications.

Figure 4. Server parameters

→ The dialog for selecting the database type appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Database type

Database type selection

Please select, which database type you are using.

● Microsoft SQL Server

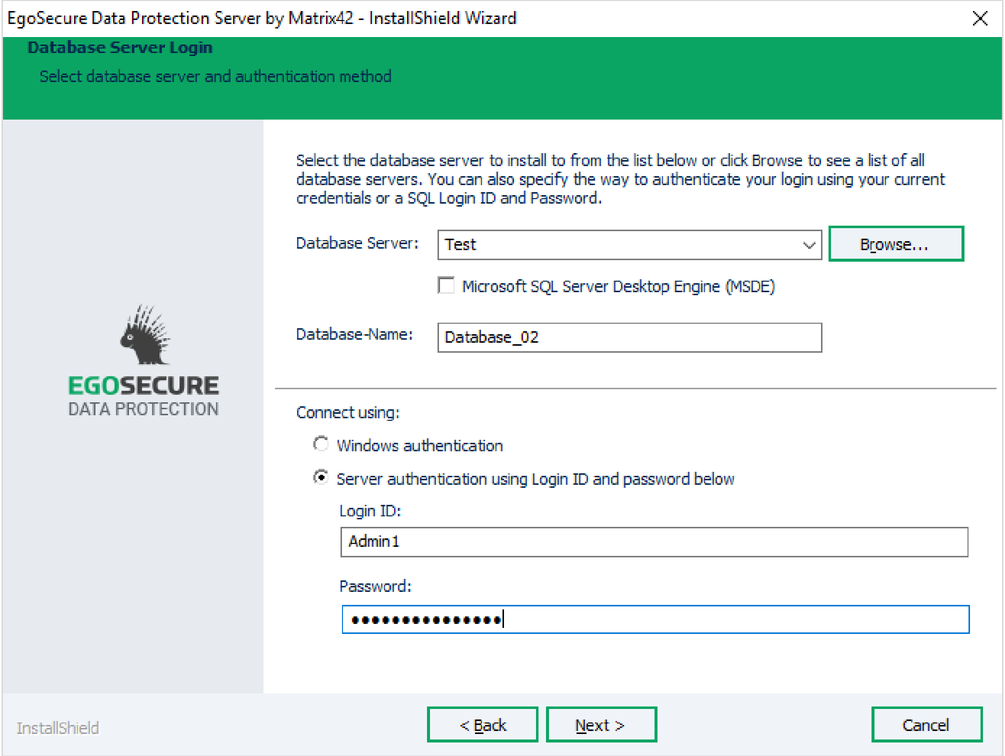
○ MySQL

○ Microsoft Azure SQL

Figure 5. Selecting the database type

12.Select the database type and click **Next**.

→ The dialog for configuring the database server login appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Database Server Login

Select database server and authentication method

Select the database server to install to from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current credentials or a SQL Login ID and Password.

Database Server: Test

□ Microsoft SQL Server Desktop Engine (MSDE)

Database-Name: Database_02

Connect using:

○ Windows authentication

● Server authentication using Login ID and password below

Login ID: Admin1

Password: •••••••••••••••

Figure 6. Database server login

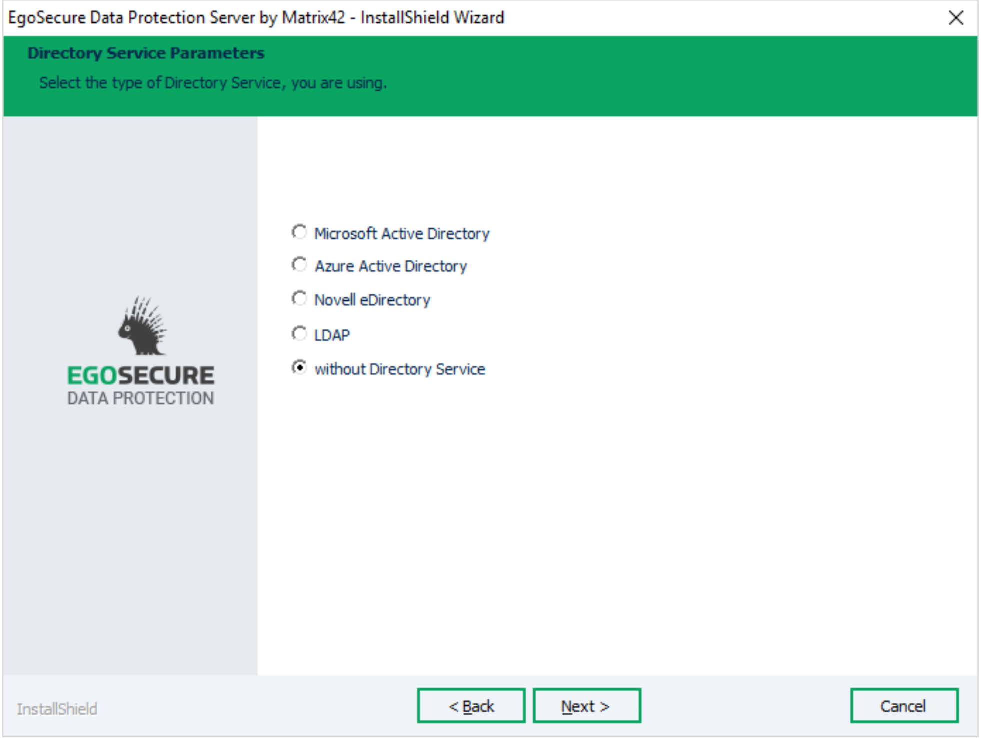
13.Configure the database server: enter the name of the SQL-server. Click **Browse** to select the available database server.

14.Set the **Microsoft SQL Server Desktop Engine** check box if MSDE is used.

15.In the **Database Name** field, enter the database name.
By default, **EgoSecure** is displayed.

INFO	**Database name not specified OR specified name does not exist** If you do not specify the database name OR the specified database name doesn’t exist on the database server: ◆ **For Microsoft SQL Server and MySQL**: a new database with the name “EgoSecure” is generated automatically. ◆ **For Microsoft Azure SQL**: a new database is NOT generated automatically and a warning appears. Please, use an existing database name.

→ The dialog for selecting a directory service type appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Directory Service Parameters

Select the type of Directory Service, you are using.

○ Microsoft Active Directory
○ Azure Active Directory
○ Novell eDirectory
○ LDAP
● without Directory Service

16. Select the type of the directory service and click **Next**.
    Permitted directory services are Active Directory, Novell eDirectory (4.91 SP2 or higher), directory services which support LDAP protocol, Azure AD and the EgoSecure internal directory. If **without Directory Service** is selected, skip the next step in the instruction.
17. Enter the credentials for adding a domain controller of the selected directory service. More domain controllers of other directory service types can be added later in the EgoSecure Data Protection Console interface.

Microsoft Active Directory credentials

- Enter the name of your ***Domain Controller***.
- Enter the Active Directory administrator as ***User***, and enter the ***Password***.

Novell eDirectory credentials

- Enter the name of the NDS server under **NDS Server**.
- Enter the context of your Novell environment under **Context**.
- Enter the Novell supervisor as ***User*** and the respective **Password**.

LDAP credentials

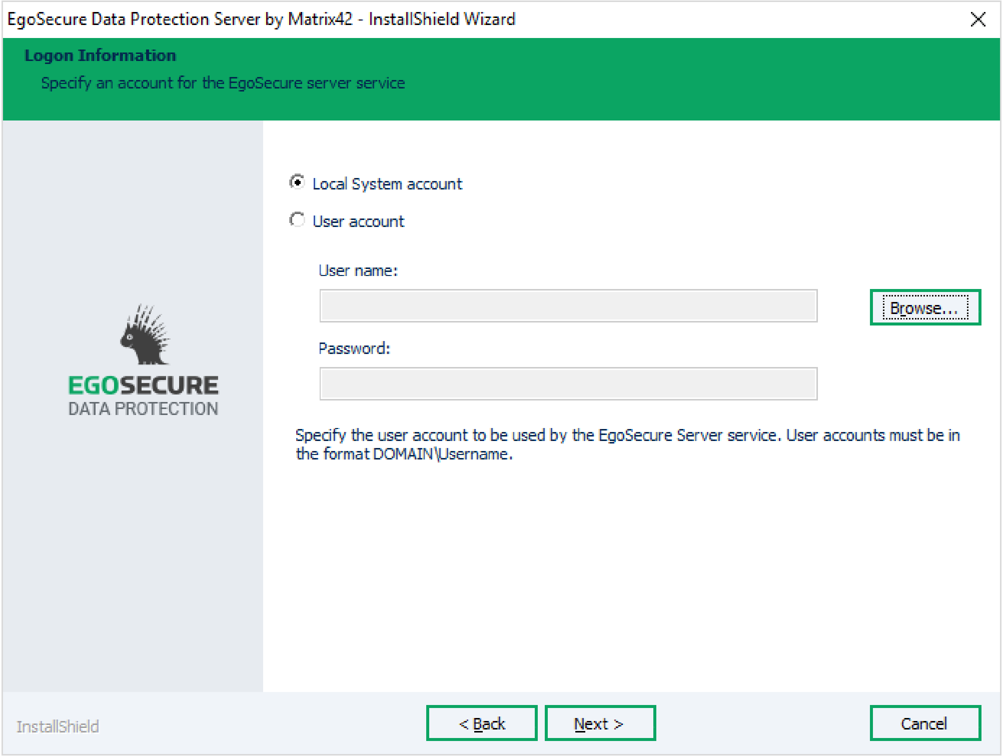
- In the **LDAP Server** field, enter the name of the LDAP server.
- In the **Context** filed, enter the context of you LDAP environment.
- Enter the LDAP supervisor in the **User** field and the necessary **Password**.

Azure Active Directory credentials

- In the **Directory (tenant ID)** field, enter the identification number of the Azure Active Directory.
- In the **Application (client) ID** field, enter the unique ID of the application registered in the Azure portal.
- In the **Application password (client secret)** field, paste the newly generated application client secret.

18.Click **Next**.

→ The dialog for specifying logon information for the EgoSecure Server service appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Logon Information

Specify an account for the EgoSecure server service

● Local System account

○ User account

User name:

Password:

Specify the user account to be used by the EgoSecure Server service. User accounts must be in the format DOMAIN\Username.

19.Select one of the following connection options:

- **Windows authentication**: Logging in to the database is performed via a Windows user account. In the next step, select the **user account** radio button and define user login data. This user account needs the rights:
  - to create a database on the SQL Server.
  - to write to the registry of the EgoSecure server machine.

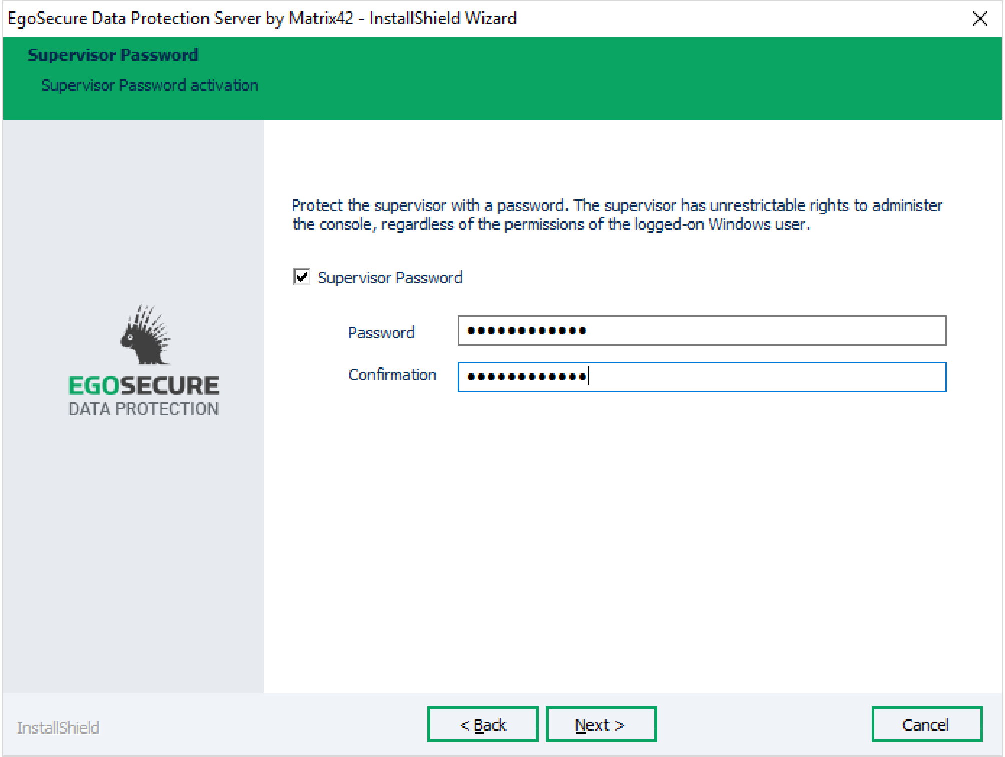
- **Server authentication using Login ID and password below**: enter the database user login data. In the next step, select **Local system account** radio button.

20.Select one of the radio buttons depending on the selection in the previous step.

ATTENTION	**SQL Windows Authentication compatibility** SQL Windows Authentication is not compatible with System account used to run the server. That is why, select **user account** for **Windows authentication**.

21. Click **Next**.

→ The **Supervisor Password** dialog appears. This dialog doesn't appear if the specified database already contains the EgoSecure Supervisor password.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Supervisor Password

Supervisor Password activation

Protect the supervisor with a password. The supervisor has unrestrictable rights to administer the console, regardless of the permissions of the logged-on Windows user.

☑ Supervisor Password

Password: ••••••••••••

Confirmation: ••••••••••••

Figure 7. Supervisor password

22. Enable the **Supervisor Password** check box and define the password. The supervisor can fully manage the **EgoSecure Data Protection Console** and create super administrators and administrators.
   You can also set the supervisor password when logging in to the **Console** for the first time, or in the **Administration** main menu of the **Console**.

ATTENTION	**Supervisor password not specified** If a supervisor password is not specified, any system administrator of the company can manage the server.

WARNING

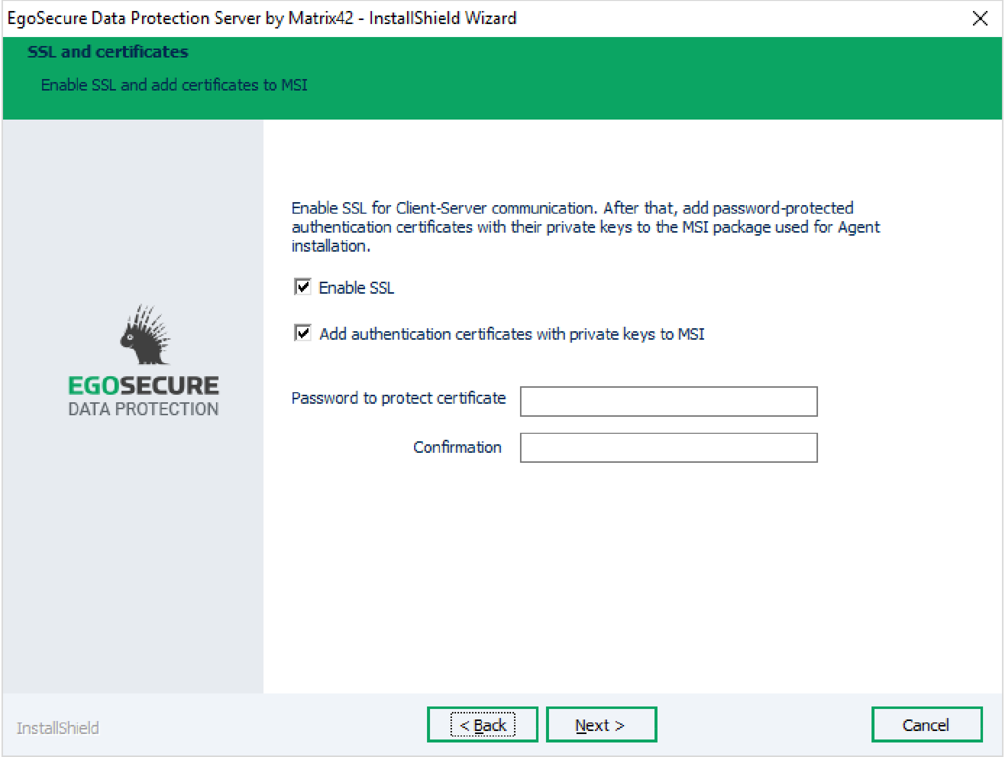
Not possible to restore supervisor password

EgoSecure does not store the supervisor password on its side, therefore the supervisor password can not be restored. Store the password in a safe location.

- You can change the password via the **/sp** admin tool command (involving the EgoSecure support). For details, see the EgoSecure AdminTool – commands guide.

23.Click **Next**.

→ The **SSL and certificates** dialog appears.
If the defined database already contains the EgoSecure password for protecting Agent authentication certificates and its private keys, the dialog is not shown.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

SSL and certificates

Enable SSL and add certificates to MSI

Enable SSL for Client-Server communication. After that, add password-protected authentication certificates with their private keys to the MSI package used for Agent installation.

☑ Enable SSL

☑ Add authentication certificates with private keys to MSI

Password to protect certificate

Confirmation

24.Set the **Enable SSL** box.

→ Once the EgoSecure Server starts, SSL EgoSecure certificates are generated automatically.

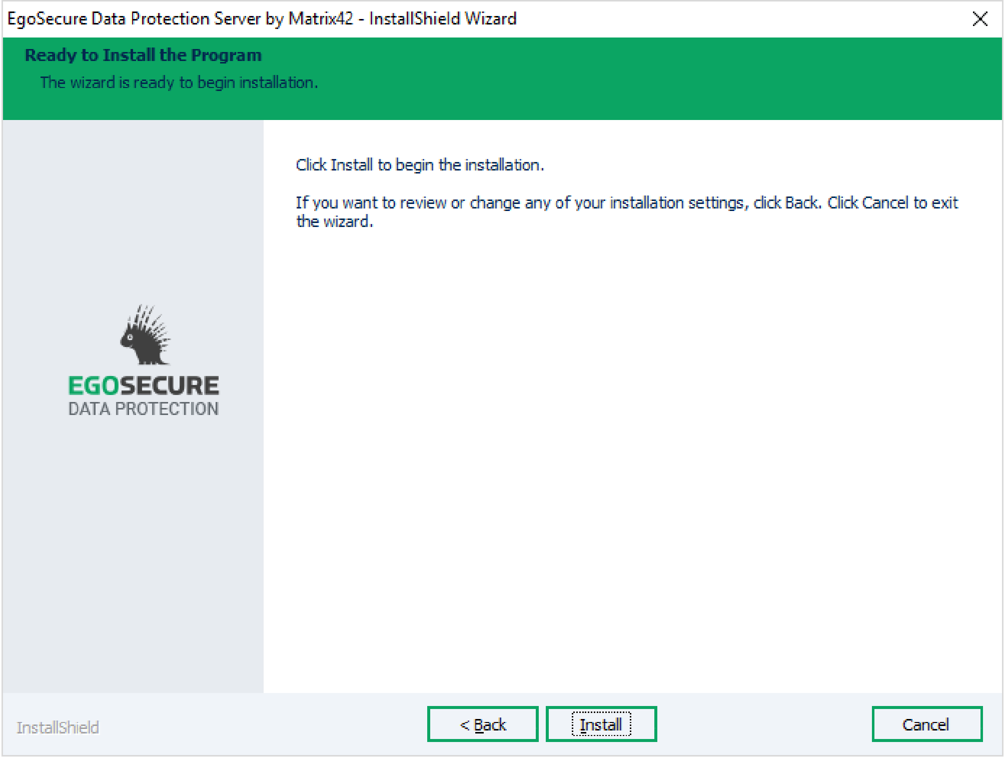
25.Check the **Add authentication certificates with private keys to MSI** box and define a password to include Agent authentication certificates to the MSI package (use only printable characters from the ASCII table for the password).
This option is used only if you are going to distribute certificates via the MSI package. If you do not set the check box on this step, make sure to distribute certificates to Agents using another way. For details about distributing certificates (both EgoSecure

and not EgoSecure ones), see the *Configuring SSL* chapter of the EgoSecure Console Manual.

26. Click **Next**.

    → The **Ready to install the Program** dialog appears.

27. Click **Install** to start the installation.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

28. Once the server installation is complete, click **Finish** to exit the wizard.

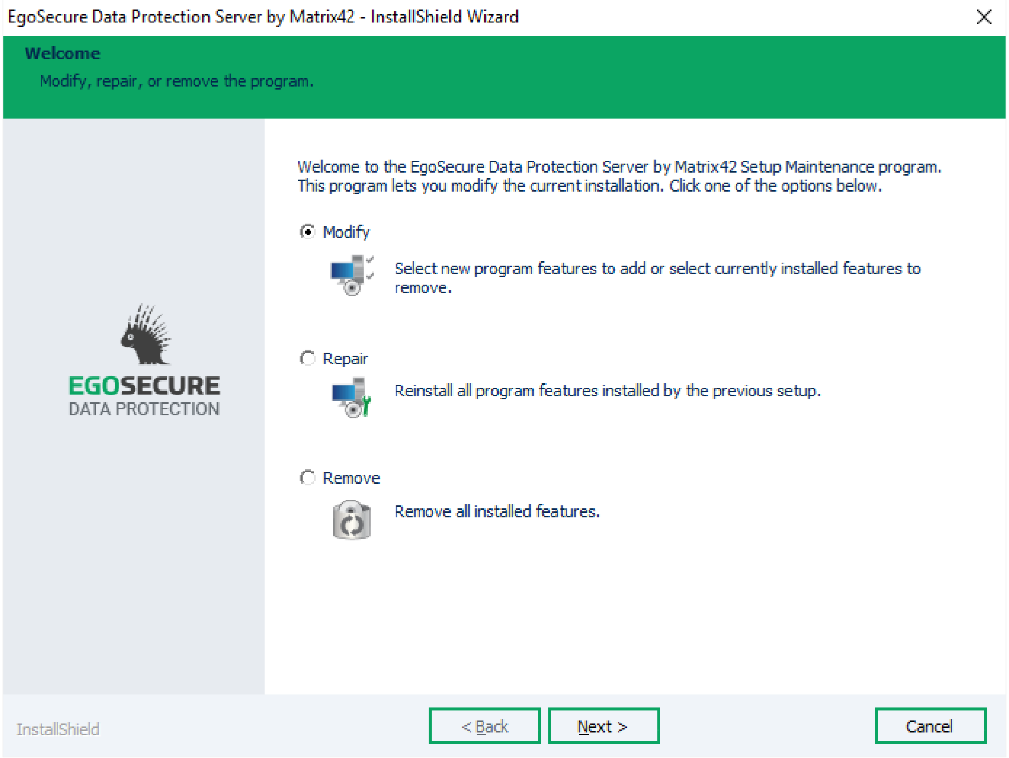
The EgoSecure Server is now installed. The EgoSecure Console icon appears on the desktop.

4.4. Modifying the installation

Modify the EgoSecure Server to install or uninstall the additional components.

1. Start the **EgoSecureSetup_x64.exe** file of the same EgoSecure Server version that is currently installed or click **Modify** in the Windows section for adding or removing programs.

   → The Welcome dialog appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Welcome

Modify, repair, or remove the program.

Welcome to the EgoSecure Data Protection Server by Matrix42 Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

● Modify

Select new program features to add or select currently installed features to remove.

○ Repair

Reinstall all program features installed by the previous setup.

○ Remove

Remove all installed features.

2. Click **Modify** and then click **Next**.
3. Enable the component to install it, disable the component to uninstall it
4. Click **Next**.

   → The installation modification starts.

5. Once the installation is complete, click **Finish**.

4.5. Silent installation

To perform a silent server installation, install the server on one computer and then install on other computers via the silent installation command.

1. Run **cmd.exe** as an administrator.
2. Copy `EgoSecureSetup_x64.exe` to a specific location. E.g. to disk `C:\`.
3. Enter the following command:

   ```
   C:\EgoSecureSetup_x64.exe -a -r -
   f1"%USERPROFILE%\Desktop\EgoSecureSetup.iss"
   ```

   → The Server InstallShield opens.

4. Install the server with your parameters.

   → All the installation parameters are automatically written to the `EgoSecureSetup.iss` file.

5. Once the server is installed, copy the `EgoSecureSetup.iss` and the `EgoSecureSetup_x64.exe` files to another computer.
6. On another computer, run cmd.exe as an administrator and then execute the following command: `C:\EgoSecureSetup_x64.exe -a -s -f1"%USERPROFILE%\Desktop\EgoSecureSetup.iss"`

   → Once the server is installed successfully, **ResultCode=0** is written to the **setup.log** file created automatically on the desktop. If the installation was not successful, then **ResultCode=-3** is written.

5. EgoSecure Server Update

5.1. Before update

Depending on the version, configuration and environment, the problems during an update may occur. This limits the software functionality on servers and endpoints. During an update, the EgoSecure Server, the database and the EgoSecure Data Protection Console are updated. What is more, the MSI package becomes available to install the EgoSecure Agent client component and can be deployed immediately.

To avoid problems during an update, we recommend to perform the following before starting the update:

1. **Check and save the database**:

- Create a database backup before the update.
- If the **Secure Audit** product (or such products with an audit functionality as Application Control or Insight) is enabled in the company, make sure the transaction log of the SQL Server is set up to avoid a *Full Transaction Log* error. For details, see the Microsoft article Troubleshoot a Full Transaction Log (SQL Server Error 9002).

2. **Disable automatic updates**:

- In the EgoSecure Data Protection Console, under **Installation | EgoSecure agents | Installation settings**, enable **automatically** under **Download parameters** and **at once** under **Update parameters**.
  As a result, the update of all EgoSecure Agents is started once the Server is updated.

ATTENTION

Using several servers

When several servers are in use, please update the main server first and perform the first console login. Only after that you can proceed with the update of other servers.

5.2. Updating from older versions

Before updating to the latest version, check the compatibility with your installed Server and Agent version.

ATTENTION

Agent version vs. Server version

Agent version must never be higher than the Server version.

Server compatibility

Installed Server version	Highest compatible Server version
22.0.0	22.0.1
21.0.3	22.0.1
21.0.2	22.0.1
21.0.1	22.0.1
21.0.0	22.0.1
15.4	22.0.1
15.3	22.0.1
15.2	22.0.0
15.1	21.0.3
14.4	21.0.2
14.3	21.0.1
14.2	21.0.0
14.1	15.4
13.3	15.3
13.2	15.2
13.1	15.1
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

Agent compatibility

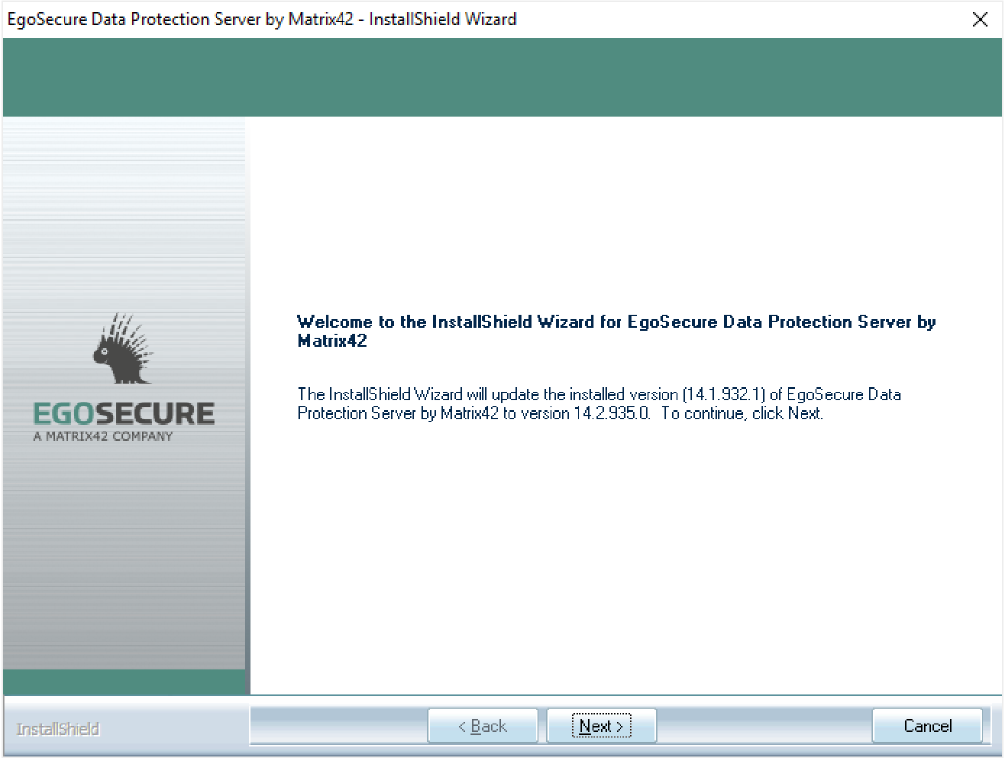
Installed Agent version	Highest compatible Agent version
22.0.0	22.0.1
21.0.3	22.0.1
21.0.2	22.0.1
21.0.1	22.0.1
21.0.0	22.0.1
15.4	22.0.1
15.3	22.0.1
15.2	22.0.1
15.1	22.0.0
14.4	21.0.2
14.3	21.0.1
14.2	21.0.0
14.1	15.4
13.3	15.3
13.2	15.2
13.1	15.1
12.3	14.3
12.2	14.2
12.1	14.1
11.3	13.3
11.2	13.2
11.1	13.1
10.3	12.3
10.2	12.2
10.1	12.1

5.3. Update process

ATTENTION	**Downgrade** Downgrade is not possible. To downgrade, uninstall a new version and perform a clean installation of an older version.

1. Start the EgoSecureSetup_x64.exe file.

→ The **Welcome** dialog appears.

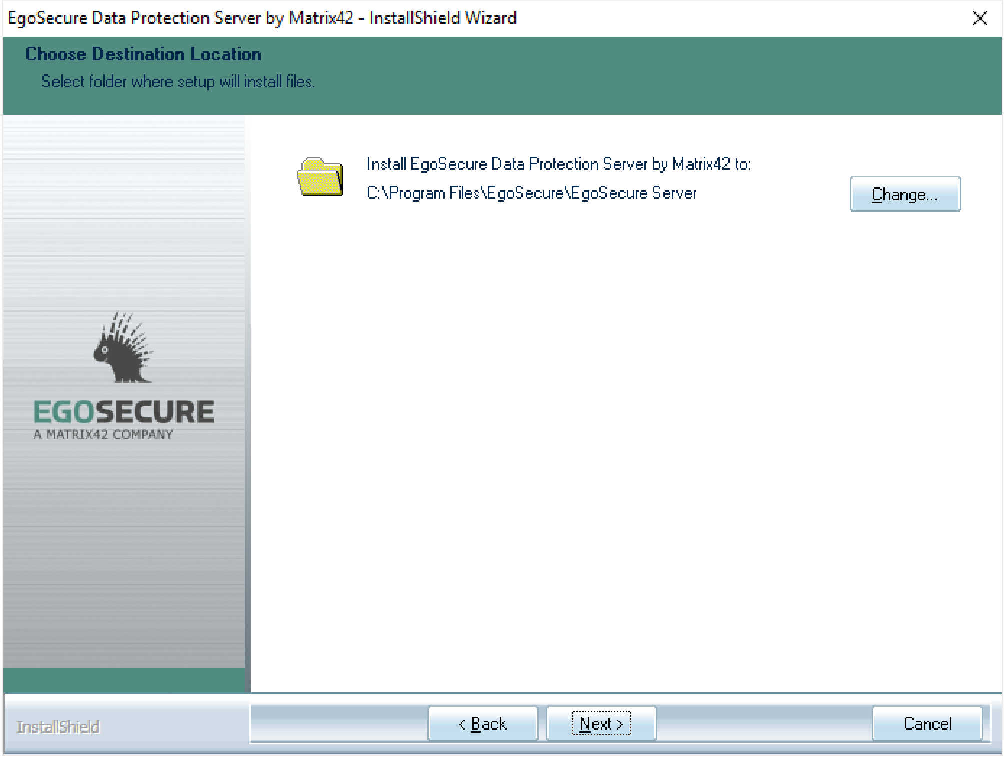

EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Welcome to the InstallShield Wizard for EgoSecure Data Protection Server by Matrix42

The InstallShield Wizard will update the installed version (14.1.932.1) of EgoSecure Data Protection Server by Matrix42 to version 14.2.935.0. To continue, click Next.

2. Click **Next**.

→ If you are updating from versions where 32-bit EgoSecure Data Protection Server version was supported (12.3 and lower), the **Choose destination folder** step appears.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

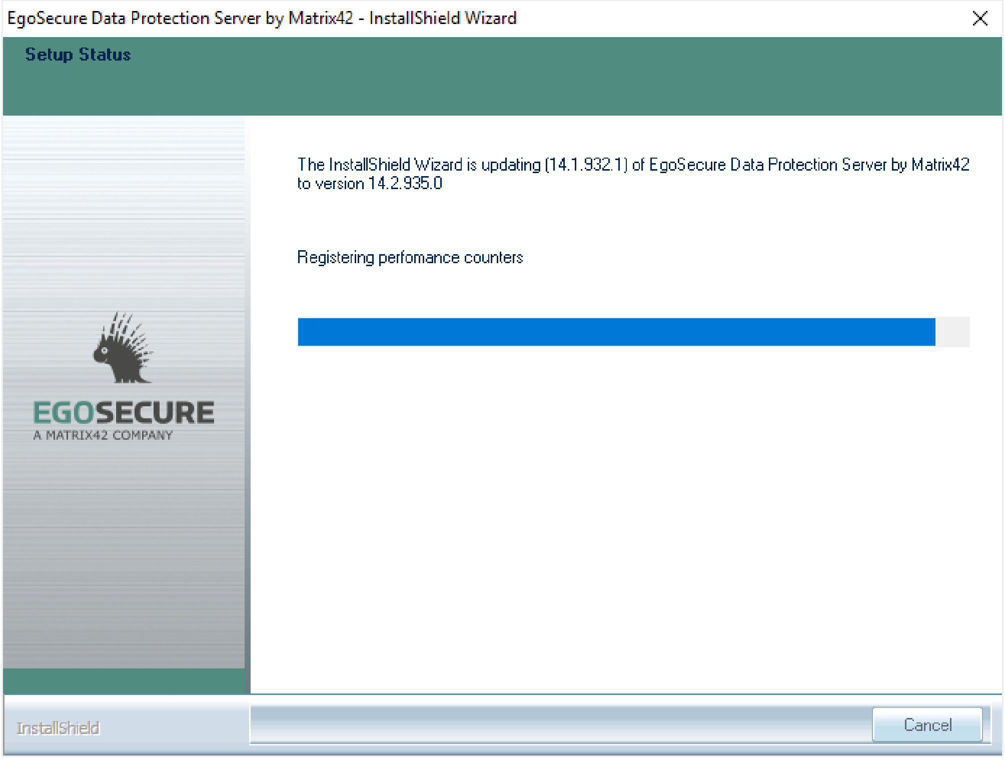
Choose Destination Location

Select folder where setup will install files.

Install EgoSecure Data Protection Server by Matrix42 to:
C:\Program Files\EgoSecure\EgoSecure Server

3. Change the folder where to install the Server, if necessary and click **Next**.

→ The update process starts.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Setup Status

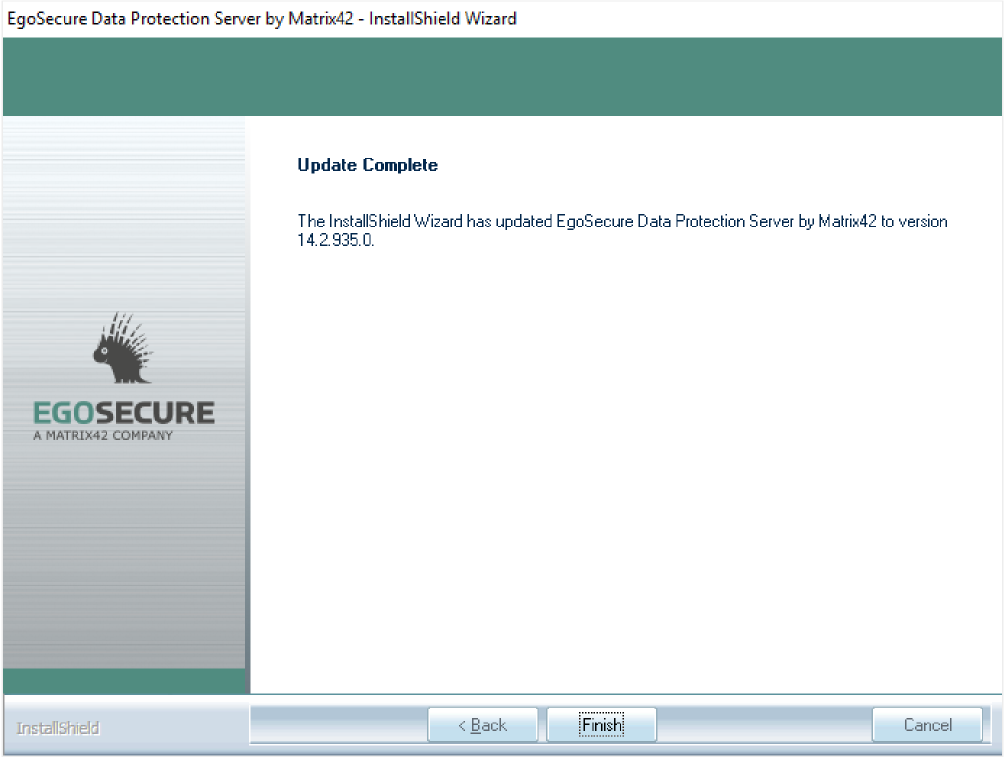
The InstallShield Wizard is updating (14.1.932.1) of EgoSecure Data Protection Server by Matrix42 to version 14.2.935.0

Registering perfomance counters

Figure 8. EgoSecure Server update process

→ Once finished, the **Update Complete** dialog appears.

4. Click **Finish**.
5. To check the functionality of endpoints, install the newly generated MSI package locally on a single computer and test the basic features you are using.
6. Once the new Agent version is successfully tested, start the installation on the clients.



EgoSecure Data Protection Server by Matrix42 - InstallShield Wizard

Update Complete

The InstallShield Wizard has updated EgoSecure Data Protection Server by Matrix42 to version 14.2.935.0.

7. Restart the computer (recommended).

6. Admin Tool

- Allows for changing parameters set on installation.
- Located in Start -> EgoSecure product group.

6.1. Database settings

ATTENTION	**Permissions of the database user** The specified user account must at least have the role *dbcreator* to create a database (can be reset to *dbowner* after creating it). Check the permissions of the database user in SQL Server Management Studio under **Server | Security | Logins**.

Specifying a database

1. Select a database type.
2. Enter the name of the database server.
3. Specify the user data of an authorized database user. To log on to the database with a valid Windows user account, leave the **User** and **Password** fields empty and enable the **Windows authentication** check box.
4. If you use Microsoft SQL Server and Always On availability groups are set up, you can enable MultiSubnetFailover option. For details about MultiSubnetFailover, see the Microsoft article.

Creating a new database

1. Select a database type (MySQL or SQL Server).
2. Enter the name of the database server.
3. Enter the name for a new database.
4. Specify the user data of an authorized database user.
5. Click **Test**.

   → If no database with such a name exists on the server, the new dialog that prompts to create a database appears.

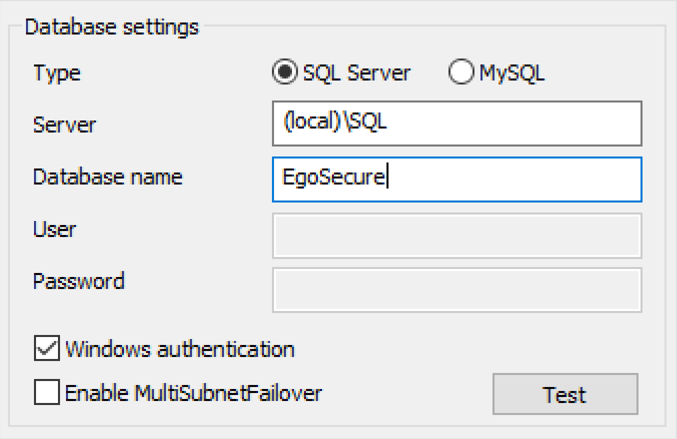
6. Click **Yes**.

New database is created.

Enabling Windows authentication

ATTENTION	**Windows authentication** To use Windows Authentication, EgoSecure Server and SQL Server must be in the same domain.

1. Log in to the EgoSecure Server computer as a domain user.
2. Enable the **Windows Authentication** checkbox in the **Database Settings** section. If you have already specified a local account to log in to the EgoSecure Server service, a warning message appears, because you must specify a user account for Windows Authentication. In this case, enter a user account (step 3).



Database settings

Type ● SQL Server ○ MySQL

Server (local)\SQL

Database name EgoSecure

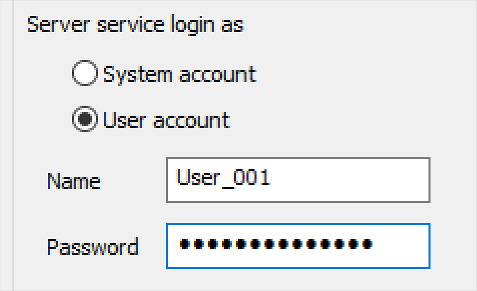
User

Password

☑ Windows authentication

□ Enable MultiSubnetFailover

3. Specify the domain **user account** in the **Server service login as** field in Admin Tool.



Server service login as

○ System account

● User account

Name User_001

Password ••••••••••••••

4. Click **Save**. Click **Yes** to restart the server.

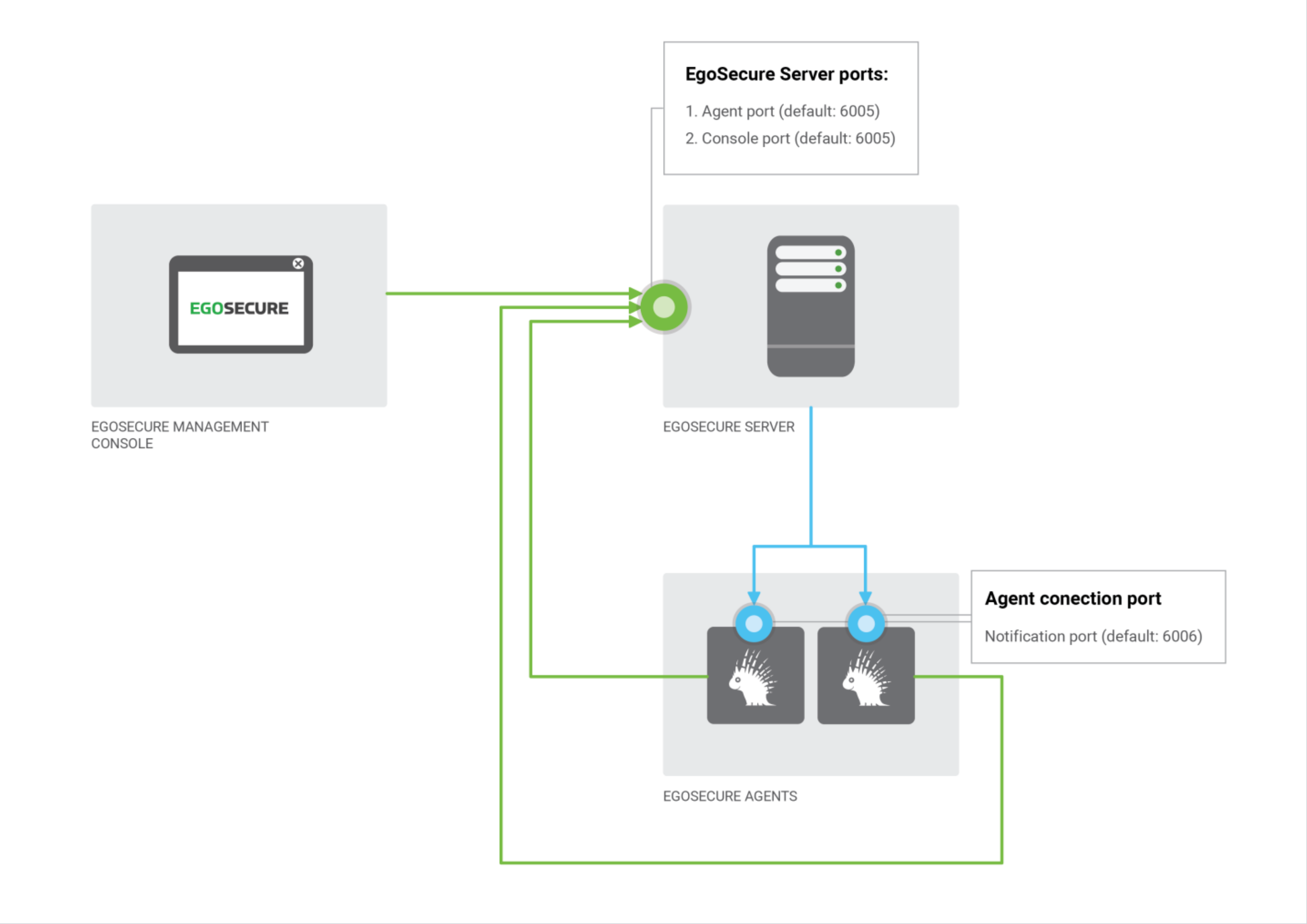
→ AdminTool closes.

6.2. Log level

Option	Description
Normal	Only error events are stored in the log file.
Administration	Detailed log file.
Debug	Very detailed log file. When the mode is enabled, log files take a lot of space. But this mode is used to analyze errors by the EgoSecure support.

6.3. Server settings

For the communication between the EgoSecure Server and the EgoSecure Agents various ports are used.


EgoSecure Server ports:
1. Agent port (default: 6005)
2. Console port (default: 6005)
EGOSECURE
EGOSECURE MANAGEMENT CONSOLE
EGOSECURE SERVER
Agent conection port
Notification port (default: 6006)
EGOSECURE AGENTS

Port	Usage
Agent port	Port on the Server for incoming connections used by Agents.
Console port	Port on the Server for incoming connections used by the Console. By default, the same port for transferring changes to the Server is used by the Agents. To increase the performance of Console-to-Server transfers, specify a different port here.
HTTPS port	Port for incoming connections on the Server via HTTPS.
Agent notification port	Port on the Agents for incoming connections. In the **Normal** mode, this port is used by the Server to send notifications about permission changes to the Agents. In the **Polling** mode, this port is NOT used, because notifications about permission changes are saved to the database and the Agents take them from the database during one of their intervals.

If the default ports are already used by another application, change the values of the **Agent Port** and **Agent Notification Port** to make communication between Agent and Server possible.

- **Use FQDN for client connections**. This option is disabled by default. In the **FQDN** mode, no IPs are used for communicating, only the full Agent computer name (e.g.: username.domain.local). Enable this option only if the default way of connection (IP + short domain name) is not possible.
- **Enable IPV6 support**. By default, IPV4 protocol is used for the communication between Agent and Server. To use IPV6, enable the check box.

6.4. Receiving data from Agents – options

- **Accept audit data**. This option is enabled by default. If disabled, the EgoSecure Server doesn’t receive audit data from Agents.
- **Accept shadowcopy data**. This option is enabled by default. If disabled, EgoSecure Server doesn’t receive shadowcopy data from Agents and, therefore, it is not available to download a shadow copy of a file from Console.
- **Accept data for devices DB**. This option is enabled by default. If disabled, the information about devices is not saved to the devices database, which can be used in Console under **Permitted devices | Individual device permissions**, **Permitted device models**, **Bluetooth devices**, **Devices list for encryption**.

6.5. Service Bus configuration

Service Bus is used to transfer changes from the EgoSecure database (used for the desktop version of Console - the EgoSecure Data Protection Console) to the UUX platform database (used for the browser version of the Console – the EgoSecure Data Protection UUX Console).

Enabling and configuring Service Bus

1. Set the **Enable Service Bus** check box.
2. Near **Service Bus system**, select which system you use.
3. Fill in the **Connection string**, **Topic name** and **Pipeline name** fields, with the data from the Service Bus system you already have.
4. Click **Save**.

   → If you have already setup other components, the synchronization starts. If not, use the **Resynchronize** button when all elements are set up.

For details, about using Service Bus, see Service Bus Integration.

7. EgoSecure Agent Installation: Windows computers

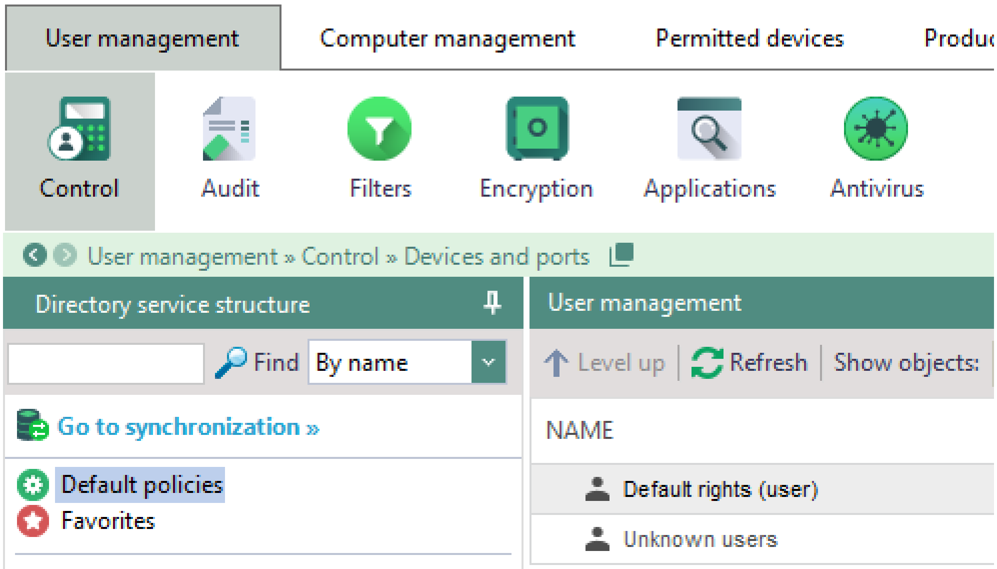
7.1. Configuring basic protection

Permissions are assigned during the installation of EgoSecure Agents. So, even offline clients are provided with a basic protection.

In the following basic protection configuration, you first block all device classes for online and offline users. Every new user in the Console first gets inherited default user rights. Inheritance can then be disabled for individual users or groups to grant them individual user rights or group rights.

Configuring basic protection

1. Open the EgoSecure Data Protection Console.
2. Go to **User management | Control | Directory service structure | Default policies**.



3. In the **User management** work area, click **Default rights (user)**.

4. In the **Devices and ports** tab, right-click a device class, and select **no access**. Repeat the procedure for all device classes, and click **Save**.
5. In the **Profile** drop-down, select offline and repeat step 4.
6. Select **Unknown users** in the **User management** work area and repeat steps 4 and 5.

➥ Basic protection for new users is set. The basic protection takes effect once an EgoSecure Agent is activated.

7.2. Synchronizing directory services

The Active Directory/NDS/LDAP/Azure AD synchronization allows for:

- Transferring users and groups from the existing directory service into the EgoSecure database.
- The Active Directory schema synchronizes as is, no changes are made.

INFO	**Before the first synchronization** Before the first synchronization, define default rights for users in **User management | Default policies**.

For details about synchronization settings, see the EgoSecure Console Manual, chapter “Synchronizing directory service”.

7.3. Creating MSI package (only Windows)

Once the Server is installed for the first time, the MSI package is generated automatically with default settings. If settings change is required, configure and then generate an MSI package manually. MSI package is always stored on the Server computer and is regenerated automatically after the Server update.

- Generating an MSI package on the Server computer
- Generating an MSI package for local installation/update or for update from network folder
- Settings included in the MSI package

Generating an MSI package on the Server computer

1. Navigate to **Installation | EgoSecure agents | Create MSI package**.
2. If you are a supervisor, select how to generate MSI packages on the Server:
   a. **Generate tenant-specific MSI packages**. A package with its specific settings is generated for each tenant individually. When updating the Server, all existing tenant-specific MSI packages are updated as a result.

b. **Generate a single MSI package for all tenants**. One single package with the settings of a default tenant is generated and used by all tenants.
Note: If administrators or super administrators generate an MSI package with different settings, the single MSI package is modified as a result. To forbid them to make changes to MSI settings, disable the displaying of the **Create MSI package** section in the layout for all admins and super admins under **Administration | Superadmin | Consoles layout**.

> INFO
>
> **Restrictions on using MSI generation options**
>
> The way of generating MSI packages is a global setting that affects all existing tenants and their administrators. Only the supervisor can make changes to this setting. For super administrators and administrators, these radio buttons are greyed out.

3. In the **Settings of MSI package** area, check the settings, which must be included.
4. If you are going to use SSL in the company, you can include an SSL certificate for the Agent to the MSI package via enabling the **Add SSL certificate and its private key** option and defining a password for certificate protection.

   → The certificate for the Agent with its private key is added to the MSI package if the certificate with its private key is provided under **Administration | Administrator | SSL configuration**. There are also other ways of distributing SSL certificate to Agents (for details, see the *Configuring SSL* chapter of the EgoSecure Console Manual).
5. In the **Path to the MSI package** area, select the **Server** radio button.
6. Click **Browse** to specify the location where the MSI package is stored on the server computer.

   ! Do not use the path `C:\ProgramData\EgoSecure\EgoSecureServer\MSI` because there the MSI templates are located.
7. Specify another name of a file in the **File name** field, if necessary.
8. Click **Generate**.

The MSI package is generated on the Server. Once the Sever is updated, the MSI package is regenerated automatically.

Generating an MSI package for local installation/update or for update from network folder

1. Navigate to **Installation | EgoSecure agents | Create MSI package**.
2. In the **Settings of MSI package** area, check the settings, which must be included.

3. If you are going to use SSL in the company, you can include an SSL certificate for the Agent to the MSI package via enabling the **Add SSL certificate and its private key** option and defining a password for certificate protection (use only printable characters from the ASCII table for the password).

   → The certificate for the Agent with its private key is added to the MSI package if the certificate with its private key is provided under **Administration | Administrator | SSL configuration**. There are also other ways of distributing SSL certificate to Agents (for details, see the *Configuring SSL* chapter of the EgoSecure Console Manual).

4. In the **Path to the MSI package** area, select the **Other destination** radio button.
5. Click **Browse** to specify the location on the computer where the Console is launched or in the network folder where the MSI package must be stored.
6. Specify another name of a file in the **File name** field, if necessary.
7. Click **Generate**.
8. To update from a network folder, copy the path to the **Directory** filed under **Installation | EgoSecure agents | Installation settings**.

The MSI package is generated in the specified location. Once the Sever is updated, the MSI package is NOT regenerated automatically in the specified location.
Once the package is generated and the Console content is refreshed (e.g. by changing the console menu), an automatic switch to the default option – Server - occurs. The path set for the **Other destination** option is saved.

Settings included in the MSI package

The following settings are included in the MSI package and are applied on endpoints not waiting for the connection to the Server:

- Default policies for unknown users (**User management | Default policies | Unknown users**).

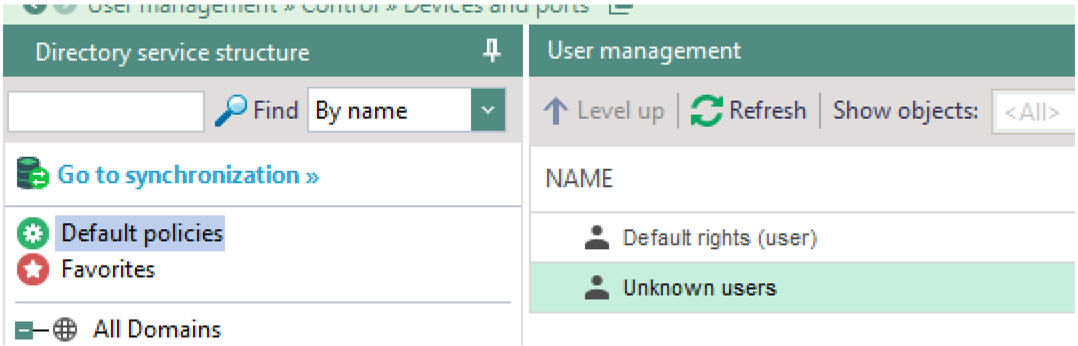


Figure 9. Default policies

- Client settings under **Administration | Clients | Client settings**.

- MSI package settings under **Installation | EgoSecure agents | Create MSI package**. For details about the MSI package settings, see the EgoSecure Console Manual.
- List of permitted EgoSecure servers under **Administration | Servers | EgoSecure servers**. Shortly after the Agent installation, only the servers selected with check marks are permitted to Agents. If the list of server changes (new servers are marked), this list is sent to Agents.

7.4. EgoSecure Agent installation: Windows devices

- Installing via EgoSecure Data Protection Console remotely;
- Installing MSI package locally;
- Installing via 3rd party Software Distribution;
- Install via Microsoft Group Policy.

WARNING

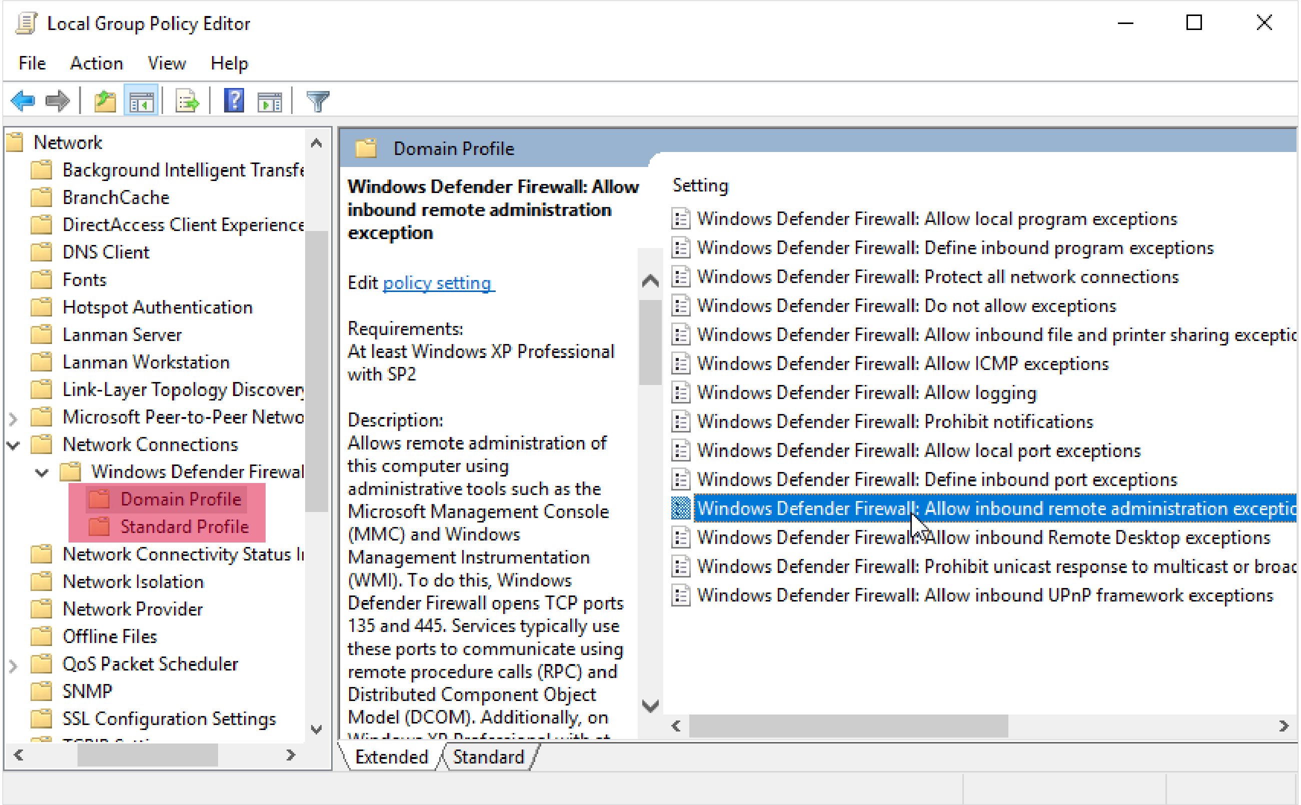
Avoiding system conflicts

Make sure that Agent version is NOT higher than Server version. If Agent version is higher, the connection between them cannot be established.

Customizing Windows Firewall settings

When installing the Agents via the Console, enable the remote administration exceptions in the Windows Firewall. It can be customized via GPO or, as described below, locally for each Agent:

1. Open the Group Policy Editor via the Windows Settings or by running the gpedit.msc file.
2. On the computer with the **EgoSecure Agent**, under **Computer configuration**, navigate to **Administrative Templates | Network | Network Connections | Firewall**.
3. Enable the **Allow inbound remote administration exception** option for the **Domain profile** and the **Standard profile**.



Windows Defender Firewall: Allow inbound remote administration exception

Edit policy setting

Requirements:
At least Windows XP Professional with SP2

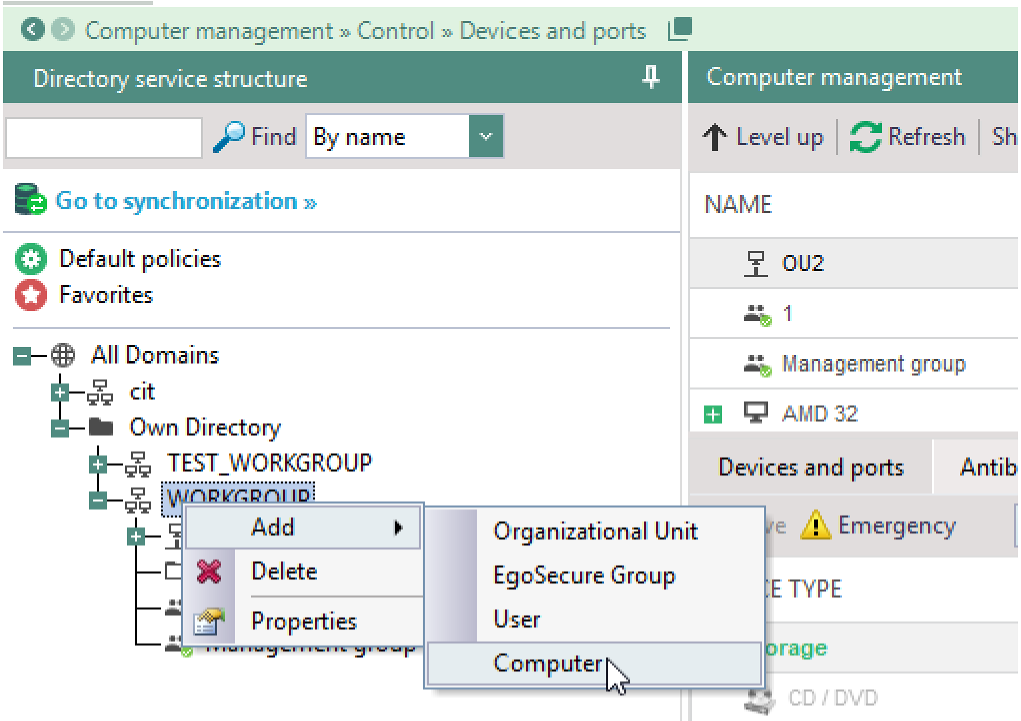
Description:
Allows remote administration of this computer using administrative tools such as the Microsoft Management Console (MMC) and Windows Management Instrumentation (WMI). To do this, Windows Defender Firewall opens TCP ports 135 and 445. Services typically use these ports to communicate using remote procedure calls (RPC) and Distributed Component Object Model (DCOM). Additionally, on

Setting
- Windows Defender Firewall: Allow local program exceptions
- Windows Defender Firewall: Define inbound program exceptions
- Windows Defender Firewall: Protect all network connections
- Windows Defender Firewall: Do not allow exceptions
- Windows Defender Firewall: Allow inbound file and printer sharing exceptic
- Windows Defender Firewall: Allow ICMP exceptions
- Windows Defender Firewall: Allow logging
- Windows Defender Firewall: Prohibit notifications
- Windows Defender Firewall: Allow local port exceptions
- Windows Defender Firewall: Define inbound port exceptions
- Windows Defender Firewall: Allow inbound remote administration exceptic
- Windows Defender Firewall: Allow inbound Remote Desktop exceptions
- Windows Defender Firewall: Prohibit unicast response to multicast or broac
- Windows Defender Firewall: Allow inbound UPnP framework exceptions

Installing via EgoSecure Console

Preparing the installation

1. Set up the inbound remote exception. For details, see Customizing Windows Firewall settings.
2. Open the EgoSecure Data Protection Console.
3. For computers, which are NOT in a directory service:
   a. Go to **Computer management** and right-click a domain under the **Own Directory** folder.
   b. Select **Add | Computer** from the context menu.



c. Enter a name of a computer where to install the Agent.
d. Set up WMI on the computer where Agent will be installed to provide an access to administrative shares for the administrator specified in step 5.

4. Go to **Installation | EgoSecure agents | Installation settings**.
5. In the **Remote installation settings** work area, specify the login data of the administrator who has enough rights for installing the EgoSecure Agent on the devices.
6. Click **Save**.
7. Configure the settings of the MSI package and generate it under **Installation | EgoSecure agents | Create MSI package**.

By default, the Agents are installed in the following directory: **C:\Program Files\EgoSecure\EgoSecure Agent**

You can change the path, if necessary. For details, see Set different installation path.

Starting installation

1. In the EgoSecure Data Protection Console, go to **Installation | EgoSecure agents | Install/Update**.
2. Select **Only computers without agents** from the drop-down menu.
3. Select the clients for installation.
4. Click Install/Update.

Installing MSI package locally

Agent can be installed manually from MSI packages. In addition to this, 3rd party software distribution, Microsoft Group Policy can be used to automatically distribute EgoSecure Agents to client computers or users.

- Start the **ESAgentSetup.exe** file.

Once the Agent is installed and connects to the Server, its user and computer appears in the Console under **Computer management**/**User management | Directory service structure | Own directory | Unsorted** folder.
Make sure the **"Own directory" mode support** is enabled in Console under **Administration | Synchronization | Directory service settings**.

Installing MSI package via msiexec

In the **EgoSecure Server** installation directory under **EgoSecure Server\MSI**, you can find the .BAT files: **install.bat** and **uninstall.bat**, which contain the recommended installation parameters.

ATTENTION	**Paths and permissions** To perform the installation via the BAT file, run the file as administrator and specify in the file the full path for the MSI package and for the log file.

When installing via msiexec you can use the following options:

Option	Description
/i <MSI package>	Install MSI package Example: /i ESAgentSetup_x64.msi
/x <MSI package>	Uninstall MSI package Example: /x ESAgentSetup_x64.msi
INSTALLDIR="<installation path>"	Install Agent to the path other than the default one INSTALLDIR="D:\Programs\EgoSecure\Agent"
/l* <path>	Path and options of the logfile Example: /l* D:\AgentInstall.log
<Property>	Any properties Example: REINSTALLMODE="vamus" For details, see: Microsoft Docs - Property Reference
ADMINPWD="<password>"	Password for uninstallation/update defined in the MSI package settings. The password is defined in Console under **Installation | EgoSecure agents | Create MSI package** before generating the package. **Note**: Make sure that you setup the necessary encoding for the .bat file so that the characters contained in the password can be correctly identified.
PKCS12_PASS="<password>"	Password for protecting the SSL certificate and its private key. The password is defined in Console under **Installation | EgoSecure agents | Create MSI package** before generating the MSI package or in the InstallShield Wizard during the Server installation (**SSL and certificates** step). **Note:** Make sure that you setup the necessary encoding for the .bat file so that the characters contained in the password can be correctly identified.
SERVER_NAME="<name>"	The EgoSecure Server name for connecting Agent manually to it.
SERVER_IP="<IP address>"	The EgoSecure Server IP address for connecting Agent manually to it.
SERVER_PORT="<port>"	The EgoSecure Server port for connecting Agent manually.

For details, see Microsoft Docs - Command line options.

Set different installation path

By default, Agents installed remotely via the EgoSecure Data Protection Console, are located in C:\Program Files\EgoSecure\EgoSecure Agent. But in some cases, administrators want to change the Agent installation path, for example, to install Agents via a 3rd party software distribution system. In such cases, the default Agent installation path is changed manually as described below.

1. Open **install.bat** or **install_x64.bat** file with notepad.
2. Enter INSTALLDIR="*installation path*" after ESAgentSetup_x64.msi.
3. Save the changes and close the text file.

4. Start the file.

Example of the installation path in the 64-bit version	start /B msiexec /i ESAgentSetup_x64.msi INSTALLDIR="C:\Program files\EgoSecure\Agent" /l* AgentInstall.log REINSTALL="ALL" REINSTALLMODE="vamus" ADMINPWD=""

Example of the installation path in the 32-bit version	start /B msiexec /i ESAgentSetup.msi INSTALLDIR="C:\Program files\EgoSecure\Agent" /l* AgentInstall.log REINSTALL="ALL" REINSTALLMODE="vamus" ADMINPWD=""

Transferring SSL certificate password to Agents

In case of script-based Agent installation/update, the password for protecting the SSL certificate and its private key is defined manually. The password is transferred to Agents in an unencrypted form.

1. Open **install.bat** or **install_x64.bat** file with notepad.
2. Enter `PKCS12_PASS=""`.
   E.g.: `msiexec /fvamus ESAgentSetup_x64.msi PKCS12_PASS="1uU22iI33nN*!h"`
3. Save the changes and close the text file.
4. Start the file.

Connecting Agent to another Server manually

❗ **WARNING**	**Avoiding system conflicts** Make sure that Agent version is the same or lower than that of the Server version. If Agent version is higher than Server version, the connection between them cannot be established.

Assign a different Server - on first Agent installation

1. Go to C:\Program Files (x86)\EgoSecure\EgoSecure Server\MSI.
2. Right-click the install.bat (or install_x64.bat) file and select Edit from the context menu.

   → The file is opened in the editor.

3. Add the following parameters:

`SERVER_NAME="PC_NAME" SERVER_IP="111.111.0.1" SERVER_PORT=port_number` (default value: `6005`; if the default value is used, `SERVER_PORT` parameter can be omitted)

4. Save the changes and close the editor.
5. Launch the install.bat file. Installation starts.

-or-

1. Run *cmd*.
2. Enter the following parameters:

```
Msiexec /i ESAgentSetup.msi SERVER_NAME="PC_NAME"
SERVER_IP="111.111.0.1" SERVER_PORT=6005
```

3. Press **Enter**.

Assign a different Server - on Agent update

1. Go to C:\Program Files (x86)\EgoSecure\EgoSecure Server\MSI.
2. Right-click the install.bat (or install_x64.bat, depends on the system bit version) file and select Edit from the context menu.
   → The file opens in the editor.
3. Add the following parameters:

`SERVER_NAME="PC_NAME" SERVER_IP="111.111.1.1" SERVER_PORT =port_number` (default value: `6005`; if the default value is used, `SERVER_PORT` parameter can be omitted) `REINSTALL="ALL" REINSTALLMODE="vamus"`

4. Save the changes and close the editor.
5. Launch the install.bat file. Update starts.

-or-

1. Run *cmd*.
2. Enter the following parameters:

```
Msiexec /i ESAgentSetup.msi SERVER_NAME="PC_NAME"
SERVER_IP="111.111.0.1" SERVER_PORT=6005 REINSTALL="ALL"
REINSTALLMODE="vamus"
```

3. Press **Enter**.

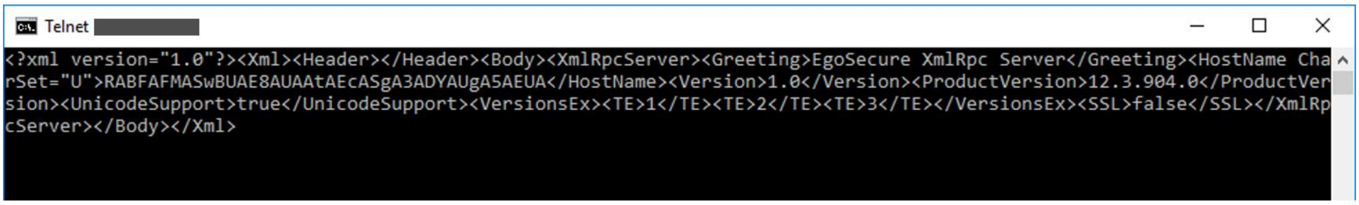
Testing connection

INFO	**Enabling Windows Telnet** To enable Telnet, type **OptionalFeatures** in the Windows search box and then check the **Telnet Client** box in the **Windows Features** dialog.

Test the connection between Server and Client via Telnet.

1. Open the Windows command prompt and enter the following:
   a. To test the connection from Server to Client:
      `telnet [Client IP address] 6006`
   a. To test the connection from Client to Server:
      `telnet [Server IP address] 6005`

   → For a functioning communication, the result looks like this:



Telnet [redacted]

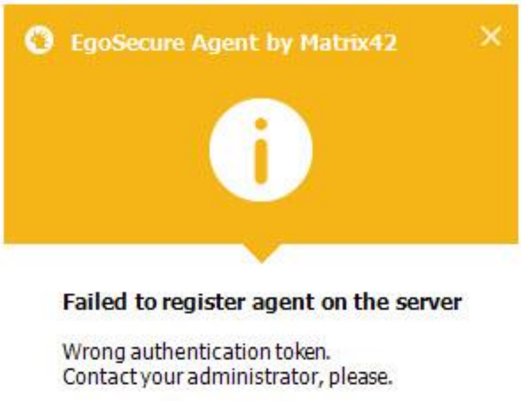
```
<?xml version="1.0"?><Xml><Header></Header><Body><XmlRpcServer><Greeting>EgoSecure XmlRpc Server</Greeting><HostName Cha
rSet="U">RABFAFMASwBUAE8AUAAtAEcASgA3ADYAUgA5AEUA</HostName><Version>1.0</Version><ProductVersion>12.3.904.0</ProductVer
sion><UnicodeSupport>true</UnicodeSupport><VersionsEx><TE>1</TE><TE>2</TE><TE>3</TE></VersionsEx><SSL>false</SSL></XmlRp
cServer></Body></Xml>
```

2. If the command fails:
   Check whether another component of your network environment is blocking the communication.

Troubleshooting wrong authentication code on the Agent

Problem

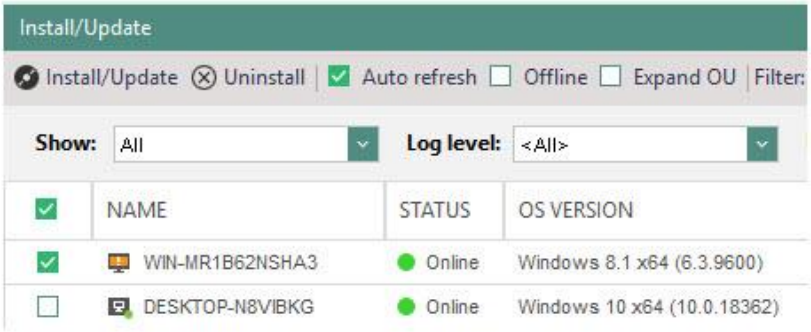
Shortly after an Agent local reinstallation or Windows reinstallation, the **Failed to register agent on the server** dialog may appear on the Agent side and a warning icon 🖥 appears in the Console under **Installation | EgoSecure agents | Install/Update**.



EgoSecure Agent by Matrix42

Failed to register agent on the server

Wrong authentication token.
Contact your administrator, please.



Install/Update

Show: All Log level: <All>

☑	NAME	STATUS	OS VERSION
☑	WIN-MR1B62NSHA3	● Online	Windows 8.1 x64 (6.3.9600)
□	DESKTOP-N8VIBKG	● Online	Windows 10 x64 (10.0.18362)

As a result, functionality on the Agent side is partly restricted. Such a case happens when a newly installed Agent with a new authentication token tries to connect to the Server, but the Server already has a previous token. This token appeared on the Server during a previous Agent registration.

The communication problem is caused by security improvements implemented in EgoSecure Data Protection 13.3.927.1 and higher.

Reason

During an Agent installation, for each Agent an individual authentication token is generated and assigned. This token is saved both on the Agent and on the Server side and the token validation is performed each time when the Agent connects to the Server. Such an additional security measure is performed to protect the Agent from being replaced with another Agent, when encryption keys or user access rights or any other important data might be spoofed.

Below are the most common cases when the Server recognizes the authentication token as an invalid one:

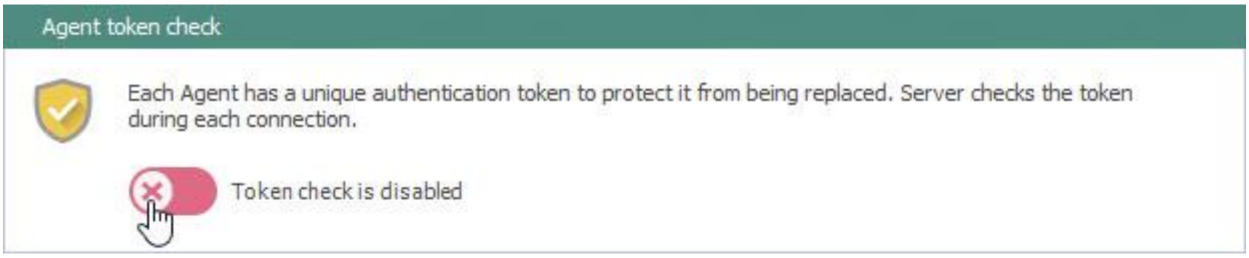
- Windows was reinstalled and Agent was installed back locally or via software distribution tools.
- Agent, which is known to the Server was reinstalled in such a way that Server was unaware about (locally or via software distribution tools).

Solutions

Solution 1: Temporarily disable authentication token check

This solution is mostly suitable if the problem is with a huge number of Agents. Remember that the check for an authentication token is a security measure and it is not recommended to disable it for a long time, especially if SSL is disabled.

1. Go to **Installation | EgoSecure agents | Installation settings**.
2. In the **Agent token check** area, disable the **Token check** option.



Agent token check

Each Agent has a unique authentication token to protect it from being replaced. Server checks the token during each connection.

Token check is disabled

3. Click **Save**.
4. Refresh rights on the Agent.
5. Enable the **Token check** back once the warning icon disappears for the Agent in the Console under **Installation | EgoSecure agents | Install/Update**.

Solution 2: Manually delete the Agent with the wrong authentication token

This solution is mostly suitable if the problem is with a small number of Agents.

1. In the Console, go to **Installation | EgoSecure agents | Install/Update**.
2. Right-click the Agent with the warning icon ⚠ and select **Delete** from the context menu to delete the Agent data and its previous authentication token.
3. On the Agent, click the **Refresh rights** button or restart the Agent.

↳ The old authentication code is deleted on the Server side and the new one is sent and registered on the Server.

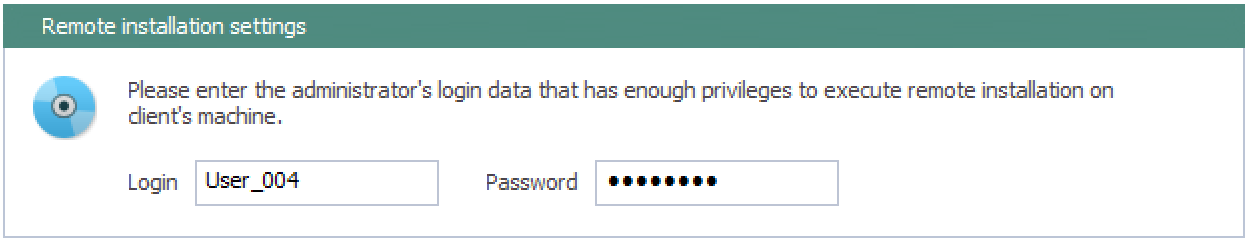
7.5. EgoSecure Agent installation: IoT devices

EgoSecure Agent is installed on IoT devices remotely via the EgoSecure Data Protection Console. Such EgoSecure Agents have the following limitations:

- Have no graphic user interface.
- Only the **Access Control** (AC) product can be activated. Via AC only the **External storage** device class is controlled.
- Works only in the **Polling** mode. It means that EgoSecure Agent checks the server for new settings in a certain time period (polling interval). The polling interval for Agents on IoT devices is one minute and it cannot be changed.

Installing Agent when IoT device is in the directory service

1. On an IoT device, set up WMI to enable the remote access to the device. For details, see the Microsoft article Allow WMI/PowerShell Remote Access on a Device.
2. In the EgoSecure Data Protection Console, navigate to **Installation | EgoSecure agents | Installation settings**.
3. In the **Remote installation settings** area, enter the login data of the administrator who has enough rights for installing the EgoSecure Agent on this device.

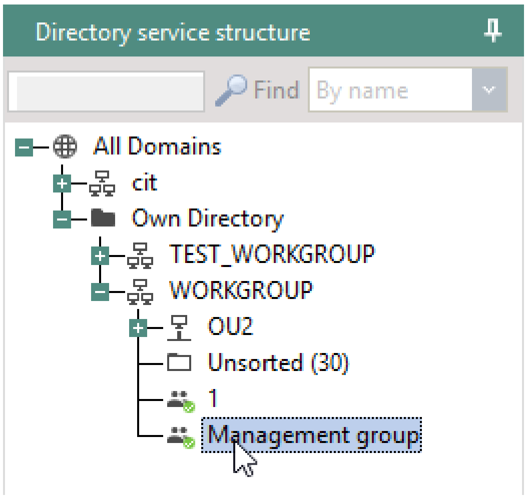


Remote installation settings

Please enter the administrator's login data that has enough privileges to execute remote installation on client's machine.

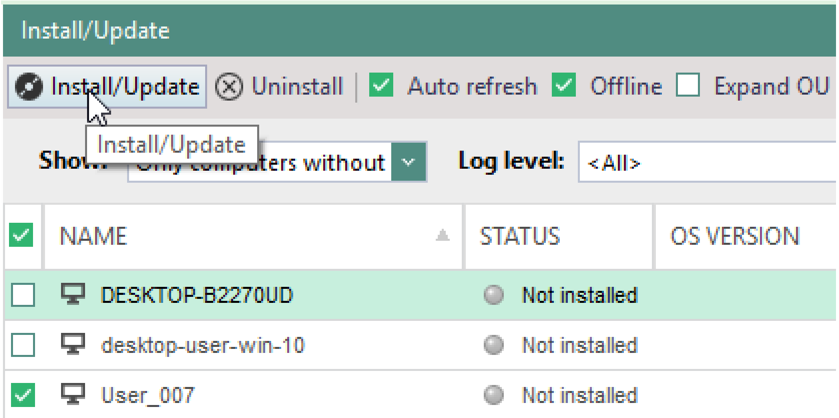
Login: User_004 Password: ●●●●●●●●●

4. Go to **Installation | EgoSecure agents | Install/Update**.
5. In the **Directory service structure** area, select a directory object from the directory structure, to which the IoT device belongs.



→ The computers of the directory object (e.g. group) are displayed on the right in the **Install/Update** main area.

6. In the **Show** drop-down list, select **Only computers without agents**.
7. Check devices where **EgoSecure Agent** will be installed.
8. Click **Install/Update**.



☑	NAME	STATUS	OS VERSION
□	DESKTOP-B2270UD	Not installed	
□	desktop-user-win-10	Not installed	
☑	User_007	Not installed	

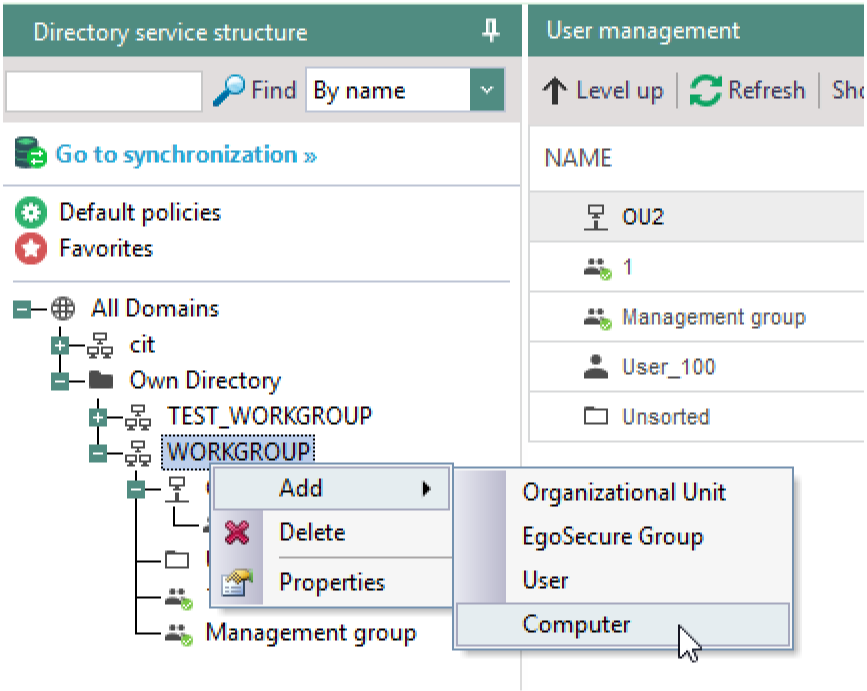
EgoSecure Agent installation starts. Once finished, the icon of the device changes to the following: ⚙.

Installing Agent when IoT device is NOT in the directory service

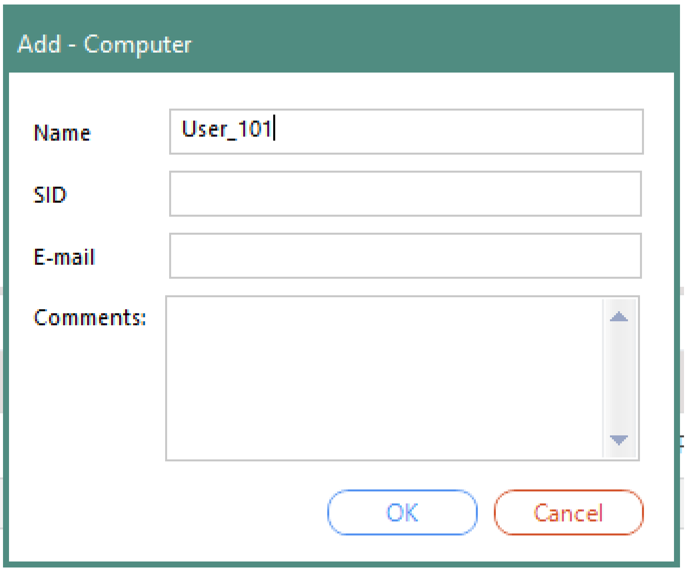
When IoT device is not the directory service structure, create a device with the same name in the Own directory so that EgoSecure Server finds it in the network. Make sure the **"Own directory" mode support** is enabled under **Administration | Synchronization | Directory service settings**.

1. Add a computer to the Own directory:
   a. Go to **User management/Computer management**.
   b. In the **Directory service structure** area, right-click an OU or domain of the **Own Directory**.

c. Select **Add | Computer** from the context menu.



→ The **Add – Computer** dialog appears.



Name: User_101

SID:

E-mail:

Comments:

d. In the **Name** field enter the name of the IoT device as is. This name was defined during the installation of Windows on it.

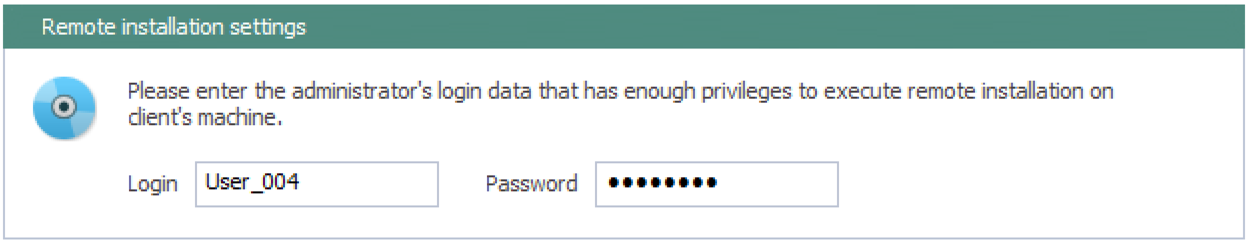
e. (Optional) In the **SID** field, enter the device SID.

f. (Optional) In the **E-Mail** field, enter the contact e-mail address of a device owner.

g. Click **OK**.

→ The computer entry appears in the **Workgroup** OU.

2. On an IoT device, set up WMI to enable the remote access to the device. For details, see the Microsoft article Allow WMI/PowerShell Remote Access on a Device.
3. In the EgoSecure Data Protection Console, navigate to **Installation | EgoSecure agents | Installation settings**.
4. In the **Remote installation settings** area, enter the login data of the administrator who has enough rights for installing the EgoSecure Agent on this device.



Remote installation settings

Please enter the administrator's login data that has enough privileges to execute remote installation on client's machine.

Login: User_004 Password: ••••••••

5. Go to **Installation | EgoSecure agents | Install/Update**.
6. In the **Directory service structure** area, select a domain where the IoT device was added in step 1.
7. In the **Show** drop-down list, select **Only computers without agents**.
8. Check device where **EgoSecure Agent** will be installed.
9. Click **Install/Update**.

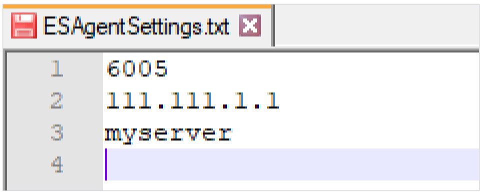
   → EgoSecure Agent installation starts. Once finished, the icon of the device changes to the following:

Installing Agent on IoT device locally

1. On an IoT device, set up WMI to enable the remote access to the device. For details, see the Microsoft article Allow WMI/PowerShell Remote Access on a Device.
2. Install Windows 10 IoT Core Dashboard.
3. Using *IoT Dashboard*, copy the appropriate installation file (according to the processor and bit value of the IoT device) from the computer with installed EgoSecure Server (C:\Program Files\EgoSecure\EgoSecure Server\IoT\).
4. In the directory where the installation file was copied, create a file with settings:

   a. Name the file as **ESAgentSettings**,
   b. Open the **ESAgentSettings** file and enter the following values in the following order:

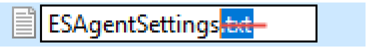
- Server port
- Server IP address
- Server host name
- Empty string



ESAgentSettings.txt

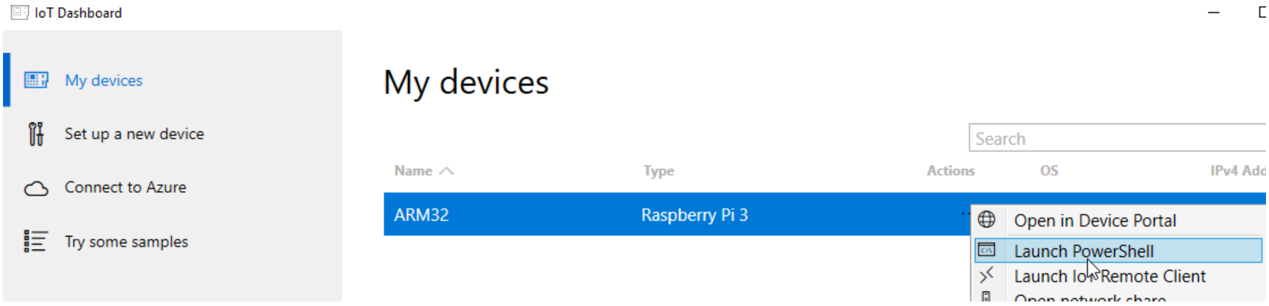
```
6005
111.111.1.1
myserver
```

c. Save the changes.

d. Remove the file extension:  ESAgentSettings~~.txt~~.

5. In the **IoT Dashboard**, install the Agent:

a. launch PowerShell:



b. In the new dialog, enter login and password.

c. Select the directory where the Agent executable file is stored.
`cd [path to the .exe file]`

d. Launch the installation via the following command:
`.\ESAgent_ARM32.exe -i`

The installed Agent appears in the EgoSecure Data Protection Console under **Installation | EgoSecure agents | Install/Update**.

8. EgoSecure Agent update and uninstallation

8.1. Update

In this part you can find information about the Agent update process. There are two ways:

- Updating via EgoSecure Data Protection Console
- Updating via install.bat or ESAgentSetup.exe file

Defining automatic update settings

1. Go to **Installation | EgoSecure Agents | Installation settings**.
2. In the **Automatic update of EgoSecure agents – client parameters** area, select a source from where MSI package is downloaded:

- **EgoSecure Server** to update from the folder on the Server computer. The MSI package in this location is regenerated automatically along with the server update.
- **Network directory** to update from the folder on the network. Once the **Server** is updated, the MSI package in this location must be regenerated manually.

> **!** The msi package stored on the network must have the name *ESAgentSetup.msi*. If a package is tenant-specific (has additions to the name, e.g., ESAgentSetupTenant1.msi) please, rename it.

3. If network directory was selected in the previous step, define the path to the MSI package and user login data to access the specified directory.
4. In the **Directory** field, select the directory from where the MSI package will be downloaded.
5. Under **download parameters**, select:

- **Manually** to download MSI package manually (Installation **|** EgoSecure agents **|** Install/Update).
- **Automatically** to download an updated MSI package each time when the EgoSecure Server is updating.
- **Schedule** to download an updated MSI package at the specified date and time.

6. Under **update parameters**, select:

- **At once** to start an update process shortly after finishing an automatic, scheduled or manual package downloading.
- **Schedule** to start an update process at the specified date and time.

7. In the **Automatic update of EgoSecure agents – server parameters** area, set how many clients can be updated simultaneously.

8. Specify a maximum network load of a computer where the Server is installed. If this value is exceeded, other clients are waiting for an update.
9. Click **Save**.

Update via EgoSecure Data Protection Console manually

1. In the EgoSecure Data Protection Console, go to **Installation | EgoSecure agents | Install/Update**.
2. Check the Agents for update.
3. Click **Install/Update**.

Update via install.bat file locally

WARNING	**Avoiding system conflicts** Make sure that Agent version is NOT higher than Server version. If Agent version is higher, the connection between them cannot be established.

1. Go to **Installation | Create MSI package**.
2. Define the settings, path and name for the package, and then press **Generate**. To see the setting description, select the setting and read the description in the bottom of the dialog.
3. Copy the following files to endpoints depending on the bitness of the system:
   a. **64-bit**: *ESAgentSetup_x64.msi* and *install_x64.bat*
   b. **32-bit**: *ESAgentSetup.msi* and *install.bat*
4. Open the .bat file with notepad and define the path to *ESAgentSetup.msi* (or *ESAgentSetup_x64.msi*) and to the *AgentInstall.log* file.
   If the password for update has been defined, add it via the ADMINPWD="" command.
   Example:

```
start /B msiexec /i C:\EgoSecure\MSI\ESAgentSetup_x64.msi
/l* C:\EgoSecure\MSI\AgentInstall.log REINSTALL="ALL"
REINSTALLMODE="vamus" ADMINPWD="" PKCS12_PASS=""
```

5. Save the changes.
6. Run *install.bat* (or *install _x64.bat*) as administrator.

Update via ESAgentSetup.exe file locally

WARNING	**Avoiding system conflicts** Make sure that Agent version is NOT higher than Server version. If Agent version is higher, the connection between them cannot be established.

1. Go to **Installation | Create MSI package**.

2. Define the settings, path and name for the package, and then press **Generate**. To see the setting description, select the setting and read the description in the bottom of the dialog.
3. Copy the following files to endpoints depending on the bitness of the system:
   a. **64-bit**: *ESAgentSetup.exe* and *ESAgentSetup_x64.msi*
   b. **32-bit**: *ESAgentSetup.exe* and *ESAgentSetup.msi*
4. Start *ESAgentSetup.exe*.
5. Enter the update password if it was defined in the MSI package settings.

8.2. Uninstallation

- Uninstallation via EgoSecure Data Protection Console
- Uninstallation via bat-file
- Uninstallation via Windows control panel

INFO

Password request for uninstallation

On configuring the MSI package, password request for uninstallation can be activated. With the following uninstallation variants, the password is required:

- Uninstallation via bat-file
- Uninstallation via Windows control panel.

Uninstallation via EgoSecure Data Protection Console

1. In the EgoSecure Data Protection Console, go to **Installation | Install/Update** under **EgoSecure agents**.
2. Select **All agents** from the drop-down menu.
3. Select the clients for uninstallation.
4. Click **Uninstall**.

Uninstallation via .bat file

1. Open C:\Program Files\EgoSecure\EgoSecure Server\MSI.
2. Copy uninstallation files according to a client bit version:

64-bit

- ESAgentSetup_x64.msi
- uninstall_x64.bat

32-bit

- ESAgentSetup.msi
- uninstall.bat

3. If an uninstallation password is set up, add the password to the **uninstall.bat** file. (Open the **uninstall.bat file** with notepad > enter the command ADMINPWD=" " > enter the password).
4. Start the uninstall.bat or uninstall_x64.bat file.

Uninstallation via Windows Control Panel

⊞ **| Control panel | Add or remove programs (programs and features) |** click **Delete**. Uninstallation password can be required, if it was set on creating the MSI package.