EGOSECURE CONSOLE

User Manual

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

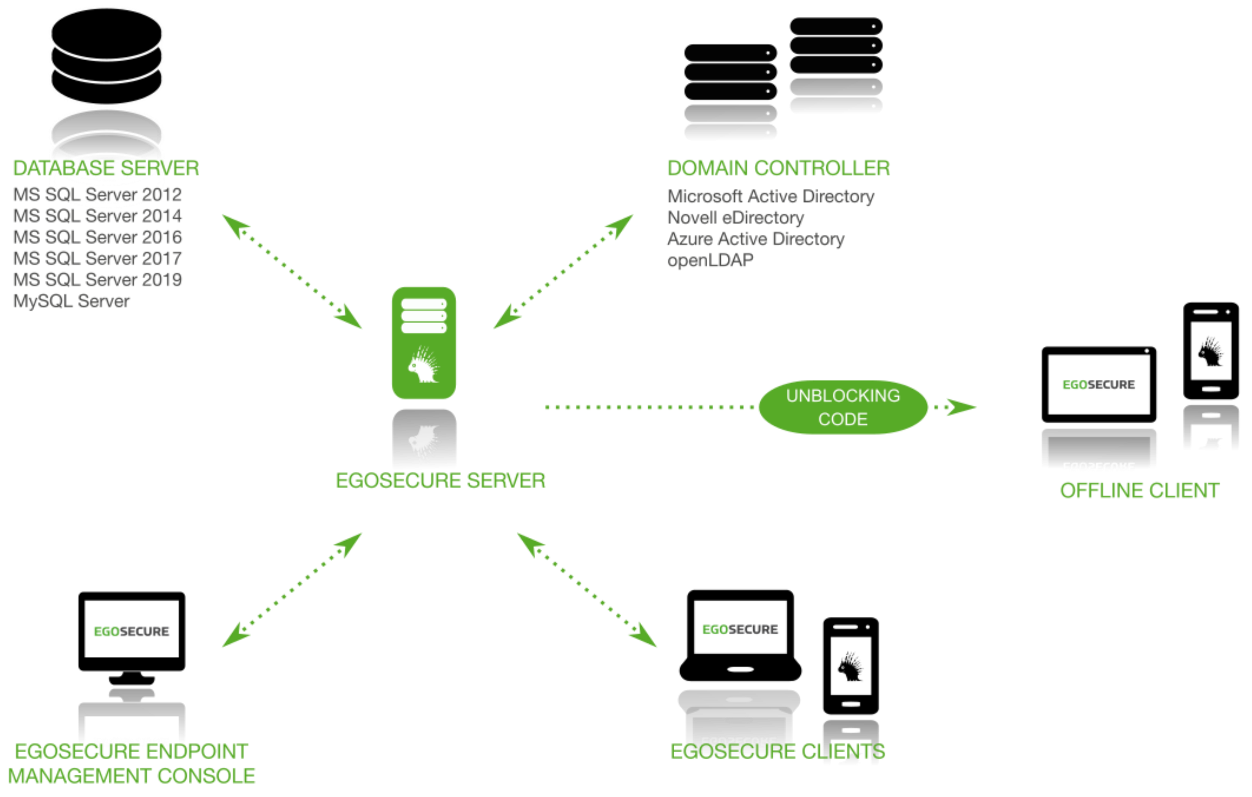
CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1. System architecture

The scheme shows the system architecture and links of the main components with each other.



Components

EgoSecure Server

- Installed on any computer of your network and has its own interface (EgoSecure Data Protection Console).
- Handles the central management of your EgoSecure clients.
- Synchronizes with your directory service (Microsoft Active Directory, Novell eDirectory, Azure Active Directory or LDAP).
- Stores administrative data in its own database.
- Transmits any changes to the clients immediately, and saves them to the database.

EgoSecure Agents (Clients):

- Communicates with the Server via push and pull process to get any changes when needed.

Kernel filter driver:

- Installed together with **EgoSecure Agent** on the client component.
- Controls access rights to external devices and applications.
- Enforces permissions set for online and offline clients.
- Provides a high degree of security.

EgoSecure Data Protection Console:

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

EgoSecure AdminTool:

- Application for adjusting the **EgoSecure Servers** settings.
  For details, see the Admin Tool chapter in the EgoSecure Installation Guide

Communication scheme

1. The administrator controls and manages the **EgoSecure Agents** via the **EgoSecure Data Protection Console**. The **Console** sends defined policies to the **Server**.
2. The **Agent** refreshes rights and settings if needed:

- If **Agent** is online (connection to Server is established), it receives a server notification that an update is required. Agent takes the settings and applies them immediately.
  In the Polling mode, the Server saves a notification to the database. The Agent checks on a regular basis whether changes are necessary and then takes and applies them.
- If **Agent** is offline (connection to Server can NOT be established), the notification is not saved to the database. Once the connection with the Sever is established, Agent takes all rights and settings and applies all of them.
  In the Polling mode, the Server saves the notification to the database. Agent makes a connection attempt automatically at regular intervals.

For details, see: Polling

1.2. After the installation

For the initial configuration of the **EgoSecure Data Protection Console** perform the following:

1. Start Console
2. Synchronize directory structure
3. Manage administrators
4. Create tenants (if needed)
5. Install EgoSecure Agents
6. Activate products
7. Configure default policies

For details, see: chapter Administration

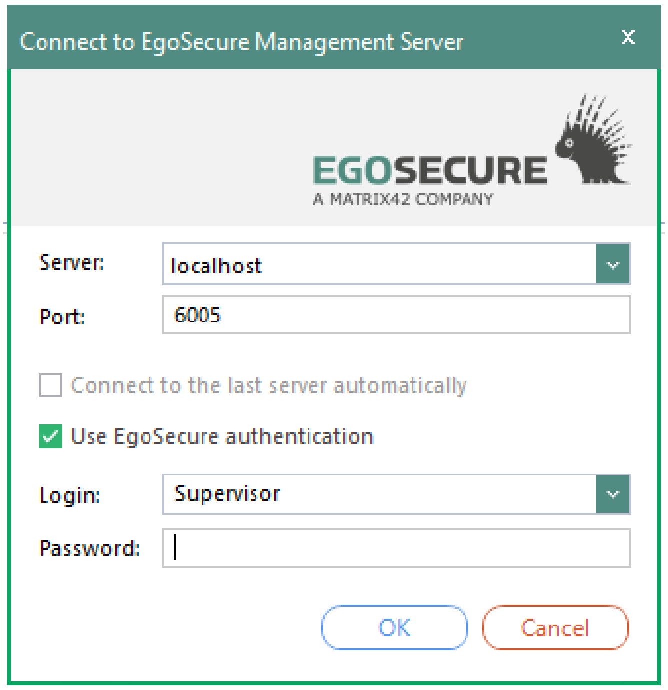
For a quick introduction to the configuration of the Console, the most important topics are covered in the following document: EgoSecure Console – Quick start guide

1.3. Starting Console

Login

1. Click the **EgoSecureConsole.exe** file or its shortcut to start the Console.

   → The **Connect to EgoSecure Server** dialog appears.



Connect to EgoSecure Management Server

Server: localhost

Port: 6005

□ Connect to the last server automatically

☑ Use EgoSecure authentication

Login: Supervisor

Password:

Figure 1. Console login dialog

2. In the **Server** field, enter the name or the IP of the server where you installed the **EgoSecure Server**. The default value is *localhost*.
3. In the **Port** field, enter the port for the server connection, which you specified during the installation. The default value is *6005*.
4. Login as the console administrator **Supervisor**. If you defined a supervisor password during the installation, enter it. If you haven't defined a supervisor password during the installation, you can define it in the next step or later under **Administration | Superadmin | Administrators & scopes**.
   For future logins to the Console you can also use a Windows user account instead of the EgoSecure login. For details, see: Granting administrative permissions to Windows user

   → The entered **Login** field data is remembered and will be offered for selection if the **Save entered user logins** check box is enabled in the Console under **Administration | Superadmin | Console policies**.

5. Click **OK** to confirm.

- The **EgoSecure Data Protection** Console opens.
- If the **EgoSecure Data Protection** Console has connected to the EgoSecure Server of a higher version, then it prompts to update the Console. To disable the prompt, go to **Administration | Superadmin | Console policies** and check the **Disable Console update prompt** box in the **Console update** area.

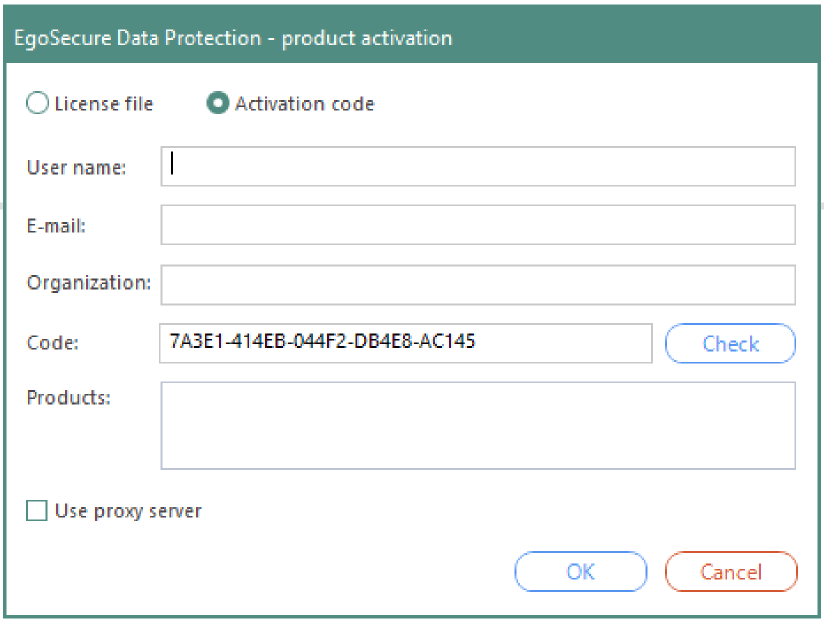
WARNING

If supervisor password is lost

The supervisor password can NOT be restored. Store the password in a safe location.
If the supervisor password is lost, access to the Console can be restored only after changing the supervisor password via the **/sp** AdminTool command (for details, see the guide EgoSecure AdminTool - Commands).

Importing a license

Once you have logged in to the Console, the dialog for product license activation appears. You can change the license information after the first activation under **Administration | Licenses | License management**.


EgoSecure Data Protection - product activation

○ License file ● Activation code

User name:

E-mail:

Organization:

Code: 7A3E1-414EB-044F2-DB4E8-AC145

Products:

□ Use proxy server

Figure 2: Activating license

1. If you received an activation code, enter it. Make sure you have an Internet connection.
   OR
2. Select the **License file** button.
3. In the **Name** field, enter the name of the licensee written in the **readme.txt** file.
4. To specify the license file path, click **Open**.

5. Enable the **Use proxy server** check box if you use proxy server to connect to the Internet. The Internet is required only when activating the license via an activation code.
6. Click **OK** to confirm.

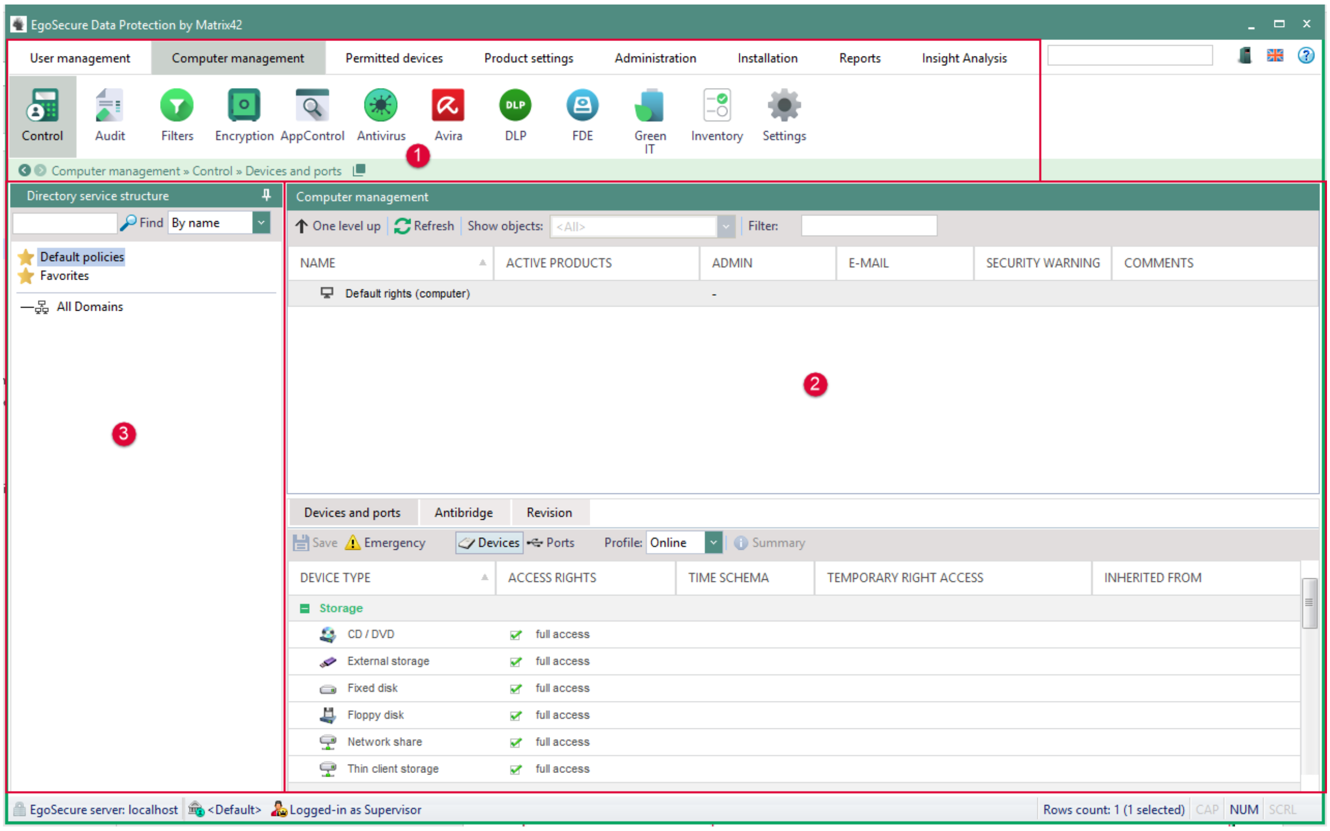
➥ You have activated the product licenses. Depending on the scope of the license, different products and functions are available to you.

You can change the license file or the activation code at any time and see the list of the licensed products. For details, see: Managing licenses
EgoSecure Data Protection offers a wide range of products including such products as **Access Control**, **Audit**, **Device Encryption** and others. Each product requires a license. A product license can be activated for either a user or a computer. If the license is activated for the computer, the defined permission settings apply to all users of this computer. When a product is activated for a user, its permission settings apply to the user regardless of the computer used. For details, see: Activating products

Console areas overview

Console is divided into three main areas:

1. Navigation pane
2. Work area
3. Directory service structure



NAME	ACTIVE PRODUCTS	ADMIN	E-MAIL	SECURITY WARNING	COMMENTS
Default rights (computer)		-			

DEVICE TYPE	ACCESS RIGHTS	TIME SCHEMA	TEMPORARY RIGHT ACCESS	INHERITED FROM
Storage				
CD / DVD	✓ full access			
External storage	✓ full access			
Fixed disk	✓ full access			
Floppy disk	✓ full access			
Network share	✓ full access			
Thin client storage	✓ full access			

EgoSecure server: localhost | <Default> | Logged-in as Supervisor | Rows count: 1 (1 selected)

Figure 3. Areas of EgoSecure Data Protection

On the navigation pane (1), select the main areas of the Console. The menu may be extended depending on the product licensing. Unlicensed products are greyed out.
When starting the Console, the **User management** menu item is active.
Under **User management**, configure the access rights for users, groups, OUs and rights for devices, files and applications.
Under **Computer management**, configure the access rights for computers, groups, OUs and rights for devices, files and applications.
Under **Permitted devices**, configure individually permitted devices for certain **Agents**.
Under **Product settings**, define the general settings for licensed products.
Under **Administration**, manage servers, clients and administrators.
Under **Installation**, configure the installation of the **EgoSecure Agents** and other licensed products such as **Antivirus** and **Full Disk Encryption**.
In **Reports**, you can find the tabular and graphical reports of the licensed products.

In the Directory service structure area (2), select directories, areas and objects, which you want to configure. The **Directory service structure** area in the navigation pane shows the available directory and its objects (OUs, users, groups, computers). If you use Active Directory or another directory service, you can synchronize it with the Console.
For details, see: AD Synchronization

In the work area (3), define settings for the objects of the directory service.

1.4. Rights concept

In **Default policies**, define default rights and settings for directory service known and unknown users, as well as directory service computers in online and offline mode.
For details, see: Configuring default policies
Offline mode means that the computer where **EgoSecure Agent** is running has no connection to **EgoSecure Server**.

The default policies are automatically transmitted to users and computers. You can disable the inheritance for certain users and computers and assign individual rights. Depending on the product activation, the predefined rights for computers or predefined rights for users are applied. For details, see: Activating products

EgoSecure verifies and prioritizes the permissions in the following order:

1. Computer rights (online/offline): Take effect if **Access Control** is activated for a computer. In this case, it doesn’t matter if **Access Control** is additionally activated for a user.
2. User rights (online/offline): Take effect if **Access Control** is activated only for a user. If **Access Control** is activated only for a user, it can be assigned to a computer to have special permissions there.

You can also define group-specific rights. The users and computers of a group get the rights of the group and no longer inherit the default policies. However, individual user/computer rights have priority over group rights.

The rights applied to a user depending on:

- Product activation (activated for a computer or a user)
- User registration in the EgoSecure database (known/unknown user)
- Connection between **EgoSecure Agent** and **EgoSecure Server** (offline/online)
- Group membership

Once a user signs in to a computer, the current permission profile is displayed on the **User rights** tab of the local **EgoSecure Agent**. The profile also indicates whether the user/computer is in online or offline mode.

1.5. Directory service structure objects

If you use a directory service (e.g., Active Directory), the objects like OUs, groups, users and computers contained there appear in the **Directory service structure** of User management and Computer management after the synchronization.

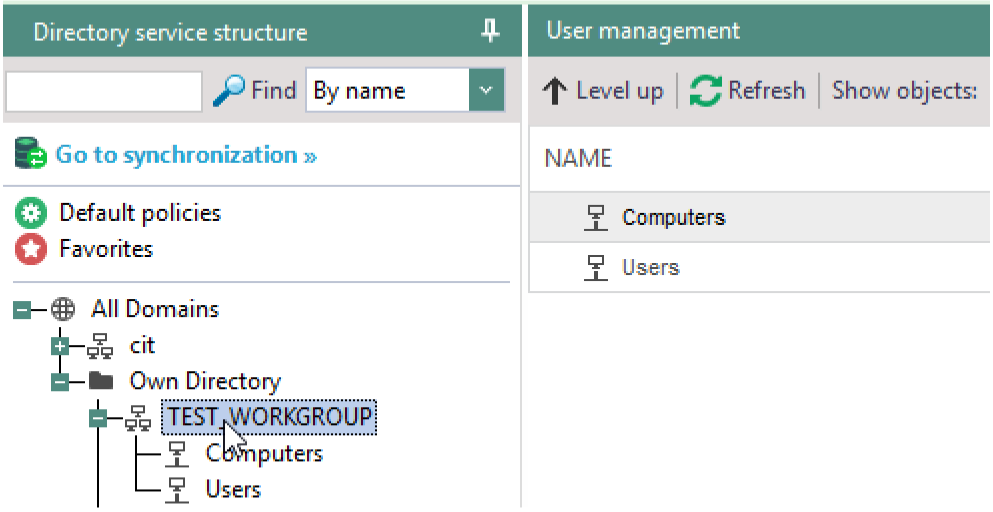


Figure 4. Directory service structure

Organizational units (OUs)

An organizational unit (OU) is a directory service object contained in domains. Once the directory service is synchronized, the OUs and objects contained there (OUs, users, and computers) appear in the directory service structure of the Console.

If you use no directory service, but use your **Own directory**, you can manually create OUs for structuring.

Assigning access rights to OU subobjects

1. In the **Directory service structure** area, select an object to which OU belongs.

2. In the **User management** or **Computer management** work area, select the OU whose objects you want to grant permissions.
3. Define access rights in the **Control** tab. For details, see: Controlling access

   → A warning message appears.

4. Click **OK** to confirm the message.

➥ The changes apply to all objects of the OU. These changes are not visible in the OU settings. The changes are visible only when selecting objects separately.
The rights are not inherited to newly added OU objects.

- To restore default rights, activate inheritance for individual objects.

Groups

A group is a directory service object consisting of users and/or computers. The group receives the default rights of users and computers for its members. These rights can be changed. For details, see: Controlling access

The group members can inherit different permissions of the group. However, individual permissions of users and computers have priority over the group rights. For details, see: Rights concept

If you activate a product for the group, it becomes activated for all group members. For details, see: Activating products

When performing a directory service synchronization, you can enable the options to automatically activate products for new users/computers of a group. For details, see: Synchronizing directory service

If you use no directory service, but use your **Own directory** you can manually create groups.

Viewing and adding group members

1. In the **Directory service structure** area of the **User management** or **Computer management** menu, right-click a group.
2. Select **Group members** from the context menu.

   → The **Group members** dialog appears. The group members are listed in the right pane of the dialog.

3. Select a user or a computer from the directory structure and click ›.

   → The new group member appears in the right pane.

4. Click **OK** to confirm.

➥ The group member inherits the permissions of the group.

If a user is a member of more than one group, permissions may differ. You can define, whether permissions or restrictions have a priority.

Rights priority for membership in several groups

1. Under **Product settings | Control | Inheritance settings**, define rights priorities:
    a. If you want permissions defined for the **Access Control** product to have priority, enable **Access permissions have priority**. Otherwise, enable **Access restrictions have priority**.
    b. If you want permissions defined for encryption products to have priority, enable **Access permissions have priority**. Otherwise, enable **Access restrictions have priority**.
2. Define, in which groups users inherit permissions:
    a. **EgoSecure groups**: only **EgoSecure** groups inherit permissions.
    b. **AD/Novell groups**: only directory service groups inherit permissions.
    c. **EgoSecure groups and AD/Novell groups**: all groups inherit permissions.
3. Click **Save**.

The inheritance settings are applied.

Regardless of the directory service, you can also create groups manually.

Creating EgoSecure groups

1. Under **User management/Computer management**, in the **Directory Service structure** area, right-click a directory object, under which you want to create a group.

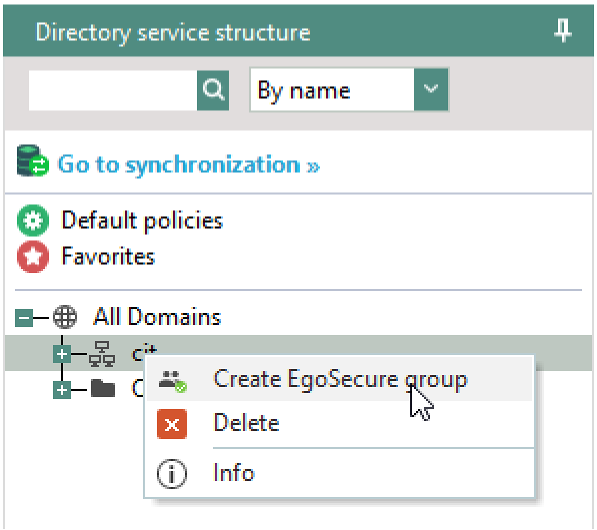


Figure 5. Adding EgoSecure group to the directory structure

2. Select **Create EgoSecure group** from the context menu.

    → The **Add - EgoSecure Group** dialog appears.

3. Define a group name and click **OK** to confirm.

    → The dialog closes and the new group appears in the directory structure.

4. Right-click a group and select **Group members** from the context menu.
   → The **Group members** dialog appears.
5. Select the directory objects to add them to the group.
6. Click **OK** to confirm.

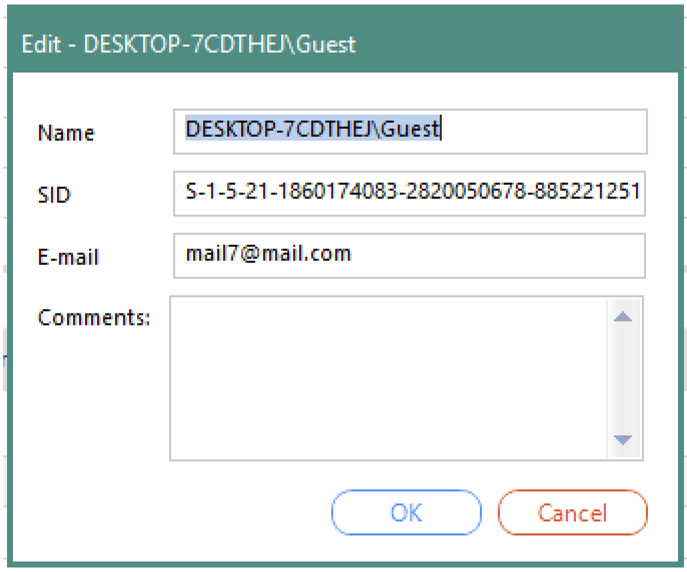
✓ You can now assign inheritable group rights and activate products.

User and computer

Users and computers are automatically subordinated to the corresponding directory service objects during synchronization. The following metadata is recorded (if available):

- Name
- SID
- E-mail

If you use no directory service, but the **Own Directory**, you can edit this data. For details, see: Own Directory



Edit - DESKTOP-7CDTHEJ\Guest

Name: DESKTOP-7CDTHEJ\Guest

SID: S-1-5-21-1860174083-2820050678-885221251

E-mail: mail7@mail.com

Comments:

Figure 6. Editing user/computer data

Deleting objects from directory service structure

If you use a directory service and the object still exists in the directory service, it will reappear in the directory service tree at the next synchronization. Delete the object first in the directory service and then in the **EgoSecure Console**.

- Right-click the object and select **Delete** from the context menu.

Own Directory

If you do not use a directory service, but selected **Own Directory** during the installation, a computer appears in the directory service tree only after installing **EgoSecure Agent** on the computer and a user appears only after logging in to an **EgoSecure Agent** computer. By default, they appear in the **Unsorted objects** folder.

Without an existing directory service, you can create OUs and EgoSecure groups to sort computers and users.

Editing user/computer name, SID or e-mail

1. In the **User management**/**Computer management** work area, double-click a user/computer.

   → The **Edit - <object name>** dialog appears.
2. Edit the data. Several mail addresses are added with a semicolon.
3. Click **OK**.

➥ New data is saved.

Adding objects to directory service tree

1. Right-click an element of the directory service tree to add an object there.
2. Select **Add | Organizational Unit** (**EgoSecure Group/User/Computer**) from the context menu.

   → The **Add - <Object type>** dialog appears.
3. Enter the valid meta data.
4. Click **OK** to confirm.

➥ The dialog closes and the new object appears in the directory service structure.

Moving objects

1. In the **Directory service structure**, select the element that contains the object you want to move.
2. In the **User management**/**Computer managemen**t area, right-click the object and select **Move into...** from the context menu.

   → The **Move** dialog appears.
3. Select an element of the directory service tree where you want to move the object.
4. Click **OK** to confirm.

➥ The dialog closes and the object is moved.

Transferring an Own Directory account to a directory service object

Transfer an Own Directory account to a directory service object for moving activated products with settings and permissions, encryption keys, audit and revision data, group membership. The own directory account is automatically deleted after a transfer.

1. Right-click an object under **User management**/**Computer management**.
2. Select **Transfer account to...** from the context menu.

   → The **Transfer account to...** dialog appears.

3. Select a directory service object to which to transfer the account.
4. Click **OK**.

➥ The Own directory account is transferred to the selected directory service object. The Own Directory account is deleted.

Device type icons in directory service structure

Agents can be installed on notebooks, desktop computers, server computers and virtual machines. Depending on a device group, different icons are displayed. For each device group, several chassis values belong (according to Microsoft Chassis Types).

Agent installation on Windows

Icon	Device group	Microsoft chassis value
🖥	Desktop computers	3, 4, 5, 6, 7, 15, 16
💻	Notebook	8, 9, 10, 11, 12, 14, 18, 21
🗄	Server	17, 23
🖥	All-in-one	13
📱	Tablet	30
▭	Mini PC	35
▬	Stick PC	36
🖥	Virtual machine	1
🖥	Unknown	2

Agent installation on IoT

Icon	Device type
●	IoT devices

Connection type icons

Icon	Description
🔒	Secure connection.
🔒	Secure connection, which demands attention. The client has a valid but not an up-to-date certificate, which must be replaced.
🔒	Connection is insecure. No certificate on the client side.
🔒	Connection is insecure. The client has a certificate, information about which is not in the database or the certificate has expired or the private key has been compromised.

2. ADMINISTRATION

2.1. Synchronizing directory service

To copy the objects and users of your directory service to the **Directory service structure** of the Console, synchronize the Console with the directory service domain controllers.
If only the structure of your directory service has changed, synchronize the structure. Only domains, OUs and folders are considered.
The first domain controller was added during the installation. After the installation, other domain controllers of different directory services are added in Console under **Administration | Synchronization | Directory service settings**.

Adding a domain controller

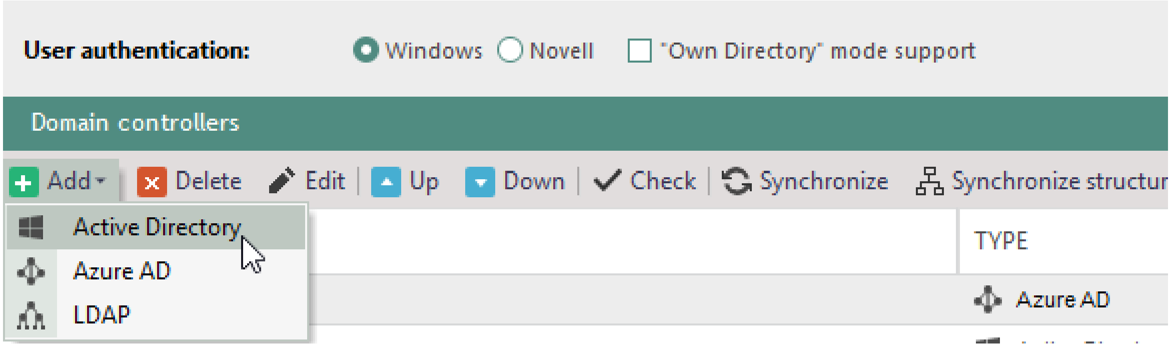
Synchronization requires the domain controller/server account information of the directory service. You can define or change these settings. If no user is specified, synchronization will be performed under the system account. The performing account must have at least read permission.

1. Go to **Administration | Synchronization | Directory service settings**.
2. Near **User authentication**, select how EgoSecure Agents identify users from your directory services: using *Windows Sid* or *Novell Guid*. The most common way is **Windows** authentication.

! **Novell** authentication must be used only when the Novell Client is installed on all computers with EgoSecure Agents.

3. In the **Domain controllers** area, click **Add** on the toolbar and select a directory service type from the drop-down menu:

- **Active Directory** (By default, AD doesn't use LDAP protocol. If you use LDAP protocol in your AD, select LDAP instead of AD.)
- **Azure AD**
- **LDAP** (Any directory service, which works via Lightweight Directory Access Protocol).
- **Novell eDirectory**.



User authentication: ● Windows ○ Novell □ "Own Directory" mode support

Figure 7. Adding a domain controller

→ The **Domain controller – [directory service]** dialog appears.

4. Define the name of the domain controller or of the NDS/LDAP Server. For details about filling in the fields for Azure AD, see Setting up Azure Active Directory and getting credentials.
5. Enter the account information of the directory service user.
6. Select where to start a directory service synchronization:
   a. For **Active Directory**, enter the organizational unit of in the **Start OU** field.
   b. For **NDS** / **LDAP** directory services, specify the server context in the **Context** field.
7. If required, activate the **Use SSL-based encryption** checkbox.

   → You should create an SSL certificate for use with your EDP and DC/LDAP servers.
8. Click **Check**.
9. Once the connection is tested successfully, click **OK** to confirm and close the dialog.
10. Click **Save** to save the changes.

    → If you selected LDAP in step 3, the **LDAP settings** tab appears under **Administration | Synchronization**. For details about LDAP settings, see Defining settings for LDAP synchronization.
11. Click **Synchronize** to perform the synchronization of the selected domain controller with the settings defined under **Administration | Synchronization | Synchronization**.

"Own directory" mode support

- Adding users in Console directly.
- No synchronization is needed.
- When a new user registers on the server, its entry appears under the own directory in the **Unsorted** folder.

Setting up Azure Active Directory and getting credentials

To get credentials from Azure AD necessary for EgoSecure, you need to register an application, define permissions for it and copy the application client secret (password).

1. Register a new application using the Azure portal. For details about registering an application, see Microsoft docs - Register an app (Preview).

   → Now you have credentials for **Application ID** and **Directory ID** fields in the InstallShield Wizard or under **Administration | Synchronization | Directory service settings**.
2. In the **Certificates & secrets** section, click **New client secret** and copy it. The client secret becomes not accessible once you leave the page. For details about adding a client secret, see Microsoft docs - Configure app to access web APIs (Preview).

→ Now you have credentials for the **Application password** field in the InstallShield Wizard or **Administration | Synchronization | Directory service settings**.

3. Add the following permissions for the application:

- User.Read.All
- Group.Read.All
- Directory.Read.All

For details about adding permissions, see Microsoft docs - Configure app to access web APIs (Preview).

Defining settings for LDAP synchronization

Under **Administration | Synchronization | LDAP settings**, define the rules for matching the EgoSecure classes and attributes with the LDAP classes and attributes so that during the synchronization the EgoSecure database can recognize objects from directories that work via the LDAP protocol. You have two ways: to activate the schema with predefined classes and attributes or add your own schema and define classes and attributes.

Enabling the predefined schema

1. Go to **Administration | Synchronization | LDAP settings**.
2. In the **LDAP schemas definition** area, right-click one of the predefined schemas and select **Activate**.
3. Below in the **LDAP Schema – [schema name]** area, under **Classes**, check whether EgoSecure classes match with LDAP classes.
4. Under **Attributes**, check whether EgoSecure attributes match with LDAP attributes.
5. Under **Alternative attributes**, define which EgoSecure classes and attributes correspond to which LDAP classes and attributes.
   E.g.: the **Name** attribute might have different values in LDAP depending whether it belongs to the **Group** or to the **Folder** class.
6. Click **Save** on the toolbar in the **LDAP schemas definition** area.

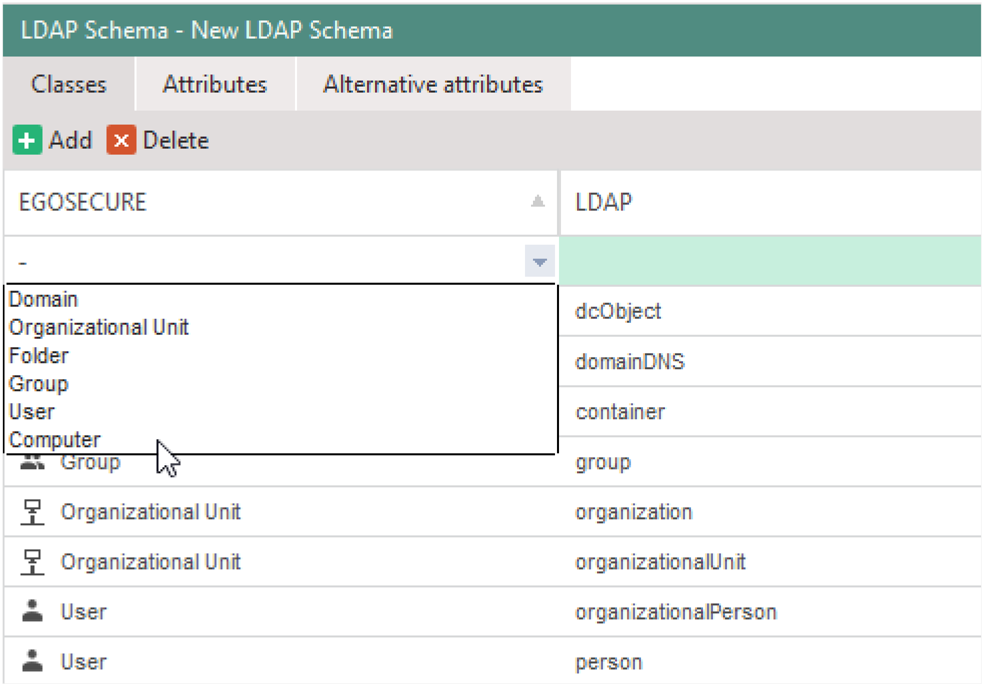
Creating and enabling you own schema

1. Go to **Administration | Synchronization | LDAP settings**.
2. In the **LDAP schemas definition** area, click **Add** on the toolbar.

   → The **New LDAP Schema** entry appears.

3. Define the schema name, if necessary.
4. Below in the **LDAP Schema – [schema name]** area, under **Classes**, define which EgoSecure classes correspond to which LDAP classes:
   a. Click **Add** on the toolbar.

b. In the **EgoSecure** column, select one of the EgoSecure classes from the drop-down.



EGOSECURE	LDAP
-	
	dcObject
	domainDNS
	container
Group	group
Organizational Unit	organization
Organizational Unit	organizationalUnit
User	organizationalPerson
User	person

Figure 8. Selecting an EgoSecure class for matching with LDAP class

c. In the **LDAP** column, enter the value that represents the selected class in LDAP.

d. Repeat step 4 for all classes you need.

5. Under **Attributes**, define which EgoSecure attributes correspond to which LDAP attributes:
   a. Click **Add** on the toolbar.
   b. In the **EgoSecure** column, select one of the EgoSecure attributes from the drop-down.
   c. In the **LDAP** column, enter the value that represents the selected attribute in LDAP.
   d. Repeat step 5 for all attributes you need.
6. Under **Alternative attributes**, define which EgoSecure classes and attributes correspond to which LDAP classes and attributes.
   a. Click **Add** on the toolbar.
   b. In the **EgoSecure class** column select one of the EgoSecure classes from the drop-down.
   c. In the **LDAP class** column, enter the value that represents the selected class in LDAP.
   d. In the **EgoSecure attribute** column, select one of the EgoSecure attributes from the drop-down for matching with the selected class.
   e. In the **LDAP attribute** column, enter the value that represents the selected attribute in LDAP.
   f. Repeat step 7 for all alternative attributes you need.

7. In the **LDAP schemas definition** area, right-click your created schema and select **Activate** from the context menu.
8. Click **Save** on the toolbar in the **LDAP schemas definition** area.

Setting up synchronization

You can select the scope of synchronization and define which products to automatically enable for new users, computers, or groups of the directory service, and how to deal with deleted users.
For details, see: Activating products

Synchronization settings

Option	Description
Synchronize directory structure only	Synchronizes only the directory service structure. For details, see Setting up synchronization of the structure
Synchronize only active users/computers	Synchronizes only active users and computers of the directory service. If **disable account** action has been performed for a user or a computer, such objects are not synchronized.
Synchronize only changes in AD for the last [x] days	Synchronizes the directory service changes of a specific time period. Enter the number of days. **!** This option does not take deleted directory service objects into account during synchronization. To detect objects deleted from AD/NDS, full synchronization is required.
Delete objects that were removed from the Directory after [x] days	Removes deleted directory service objects from the console after a defined period of time (Administration | AD Synchronization | Deleted objects). This option is available only if the option **Synchronize only changes in AD for the last [x] days** is disabled.
Detailed log file of the synchronization	Records all synchronization events into a separate synchronization log file. One log file is created for one day under C:\ProgramData\EgoSecure\EgoSecureServer\LOG.

Automatic product activation

Option	Description
Activate products for new users/computers ▪ **all selected products** ▪ **only group-matching products**	Automatically activates selected products for new users/computers. ▪ activates all selected products ▪ activates only the selected products, which are already activated for the group in which new user/computer is located.

	! A group must be synchronized with the server before adding new users/computers there. Otherwise, users/computers in this group are not considered as new ones.
Deactivate products for inactive users/computers	Deactivates products for inactive users/computers. *Inactive users/computers* are the objects of a directory service, for which the *disable account* operation has been performed. The option is available only if the option **Synchronize only active users/computers** is disabled in the Synchronization settings area.
Match product activation with the activated products of the group	Automatically activates only the products, which are already enabled for a group. Products are activated for both new and existing users/computers. **!** Products previously enabled for a user/computer become disabled if they are not enabled for a group. The option is available only if the options **Synchronize directory structure only** and **Activate products for new users/computers** are disabled. There are two types of groups: ■ Groups imported from the Active Directory ■ EgoSecure groups created in a domain under **User management**/**Computer management | Directory service structure**. EgoSecure groups created in the domain can contain only AD users/computers while EgoSecure groups created in the Own directory can contain only local users/computers.

INFO

Displaying members of synchronized directory service groups

Once directory service groups are synchronized, they appear in **Directory service structure** of the **User management**/**Computer management** menu. Directory service group members are not displayed.

- To display the members of a directory service group, right-click a group and select **Group members** from the context menu.

Setting up a full synchronization of the directory service

1. Go to **Administration | Synchronization | Synchronization**.
2. Specify the synchronization settings.
3. To exclude certain objects from the synchronization,
    a. Select the directory element in the **Directory service structure** area.

b. Click **Add**.

→ The excluded objects appear in the **Objects to exclude from synchronization** area.

> INFO
>
> **Massive exclusion of AD objects**
>
> It might be not convenient to define the objects, which must be excluded from the synchronization each time. Use the Active Directory attribute for the reasons of convenience.
>
> - To exclude certain directory objects during all synchronizations, add the **esSyncIgnore** attribute with the value **1** for directory objects directly in the Active Directory.

4. In the **Directory service structure** area, select a directory object in the tree, from which to start the synchronization. Select **All domains** to synchronize all domain controllers of a user authentication type specified under **Administration | Synchronization | Directory service settings**.
5. Click **Save**.

Setting up synchronization of directory structure (domains, OUs and folders)

1. Go to **Administration | Synchronization | Synchronization**.
2. Enable the **Synchronize directory structure only** check box.

   → Other check boxes become disabled and the **Include groups** check box appears.
3. To synchronize directory service groups, enable the **Include groups** check box.
4. Specify synchronization settings.
5. To exclude certain objects from the synchronization,
   a. Select the directory element in the **Directory service structure** area.
   b. Click **Add**.

   → The excluded objects appear in the **Objects to exclude from synchronization** area.
6. Click **Save**.

Initiating synchronization

You can perform synchronization manually or use a scheduler to perform synchronization automatically.

Performing synchronization manually

1. Go to **Administration | Synchronization | Synchronization**.
2. In the **Directory service structure** area, select a directory object from which to start the synchronization. Select **All domains** to synchronize all domain controllers of

a user authentication type specified under **Administration | Synchronization | Directory service settings**.

3. Edit the settings. For details see: Setting up synchronization
4. Click **Start**.

➥ The synchronization starts and the **Directory service structure** of the Console becomes updated.

Performing synchronization automatically at specific time

1. Go to **Administration | Synchronization | Schedule**.
2. In the **Directory service structure** area, select a directory object from which to start the synchronization. Select **All domains** to synchronize all domain controllers of a user authentication type specified under **Administration | Synchronization | Directory service settings**
3. In the **Server** drop-down, select an EgoSecure Server for performing a scheduled synchronization (applies for all tasks in the list).
4. Click Add in the work area.
5. Define the name and time or period for the synchronization.
6. Edit the settings. For details, see: Setting up synchronization
7. Click **Save**.

➥ The synchronization will be performed at the specified period of time.

Transferring an account to a directory service object

The objects deleted from Active Directory, Novell eDirectory, LDAP or Azure AD are displayed under **Deleted objects**. The objects appear in this list only after the synchronization.

Transfer an account of a deleted user to a directory service user for moving activated products with settings and permissions, encryption keys, audit and revision data, group membership.

1. Right-click a user under **Administration | Synchronization | Deleted objects**.
2. Select **Transfer account to...** from the context menu.

   → The **Transfer account to...** dialog appears.

3. Select a user whom to transfer the account.
4. Click **OK**.

➥ The account is transferred to the selected directory service user. The user is automatically deleted from the list and from the database.

2.2. Creating administrators and roles

There are three types of administrators in the Console:

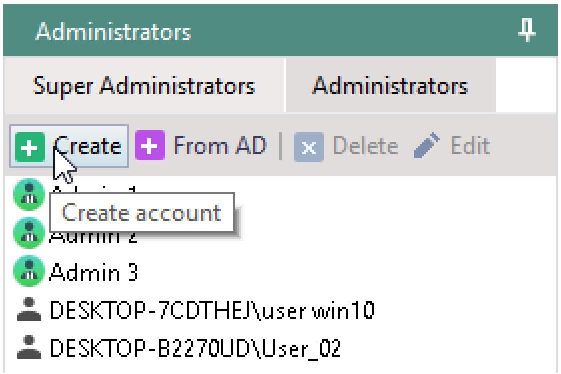
- **Supervisor**
  The supervisor is created during the installation of **EgoSecure Data Protection**. If not, supervisor is created during the first login to the Server. Receives all permissions, which cannot be restricted.
- **Super administrator**
  A super administrator is created by the supervisor. He owns all rights. The rights can be restricted by the supervisor by hiding console commands for the super administrator. Any number of super administrators can be created. A Windows user account can also act as a super administrator.
- **Administrator**
  An administrator is created by the supervisor or a super administrator. The rights of an administrator may be restricted by the supervisor or a super administrator through global or domain-specific roles. Any number of administrators can be created. A Windows user account can also act as an administrator.

Creating administrators in Console

You can create a new administrator in the Console or add a Windows user as an administrator. Once the Windows user is logged in to Windows, he can access the Console directly without further login (single sign-on).

Creating new administrator

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** area, click the **Super administrators** or **Administrators** tab.
3. Click **Create**.



Admin 3
DESKTOP-7CDTHEJ\user win10
DESKTOP-B2270UD\User_02

Figure 9. Creating an administrator

→ The **Create account** dialog appears.

4. Define login and password for the administrator account.

5. In the **E-mail** field, define an e-mail address of an administrator/super administrator. If later a super admin or a supervisor changes the e-mail of an administrator, the last changed e-mail is considered as a valid one.
6. Click **OK** to confirm.

↳ The new administrator appears in the **Administrators** tab.

Granting administrative permissions to Windows user

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** work area,
   a. click **From AD** in the **Super Administrators** tab to grant super administrative privileges
      or
   b. click **From AD** in the **Administrators** tab to grant administrative privileges.

   → The **Selection of users** dialog appears.

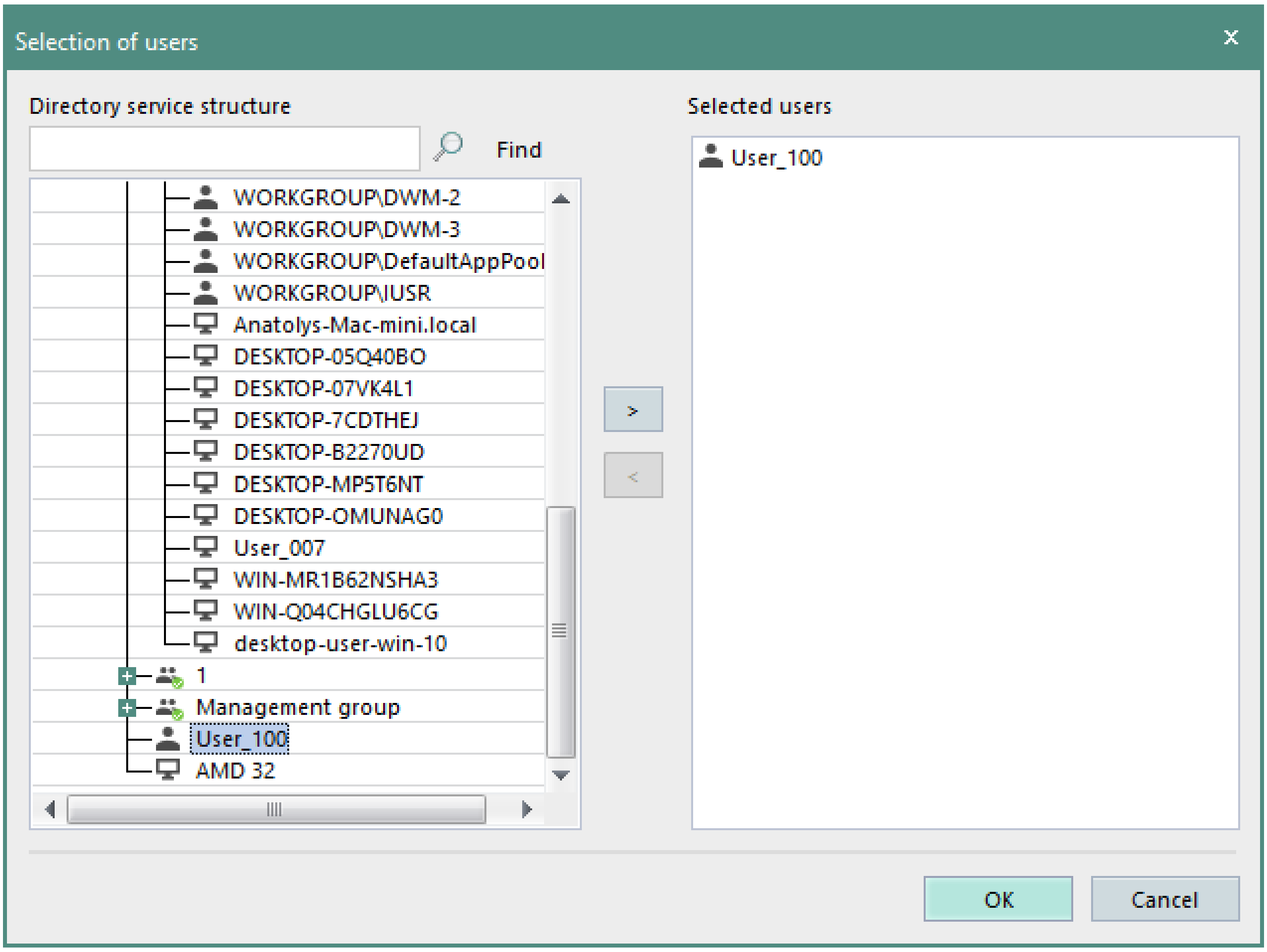
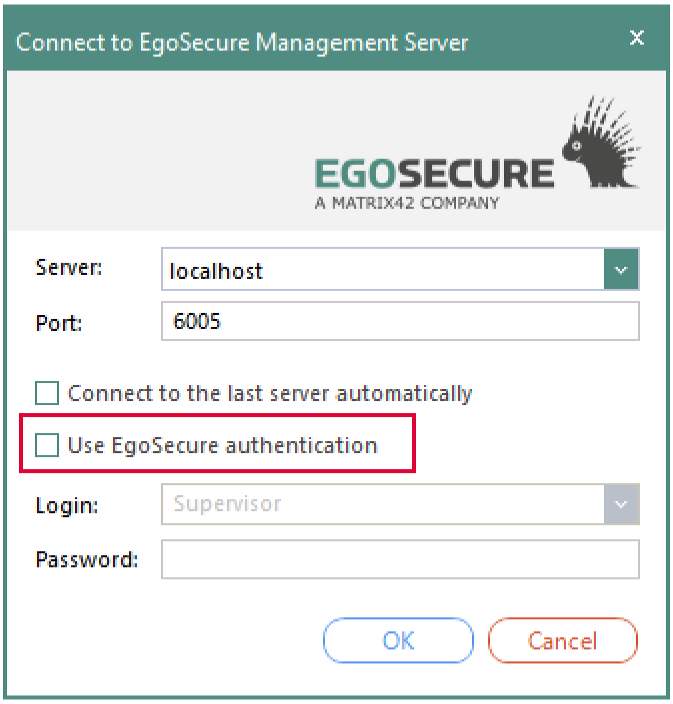


Figure 10. Granting administrative permissions to user

3. Select a user from a directory service structure. You can select several Windows user accounts as console administrators at once.
4. Click **OK**.

- The new administrator appears in the **Administrators** tab. The selected user can now log on to the Console with his current Windows account as an administrator without having to specify the login data again (single sign-on).


Connect to EgoSecure Management Server

Server: localhost

Port: 6005

□ Connect to the last server automatically

□ Use EgoSecure authentication

Login: Supervisor

Password:

Figure 11. Login with Windows user account

Restricting Console layout

Define which Console sections are visible to all available super administrators and administrators of a currently used tenant or only to administrators (depends on the selected Console policy). Administrators must additionally have the role for viewing or modifying the section that is permitted within the Console layout.

Defining visible and hidden Console layout elements

1. Go to **Administration | Superadmin | Console layout**.
2. Set the check boxes for layout elements which must be visible, clear the check boxes for layout elements which must be hidden.
3. Click **Save**.
4. Click **Export** to save the Console layout. Exported Console layout can later be imported to another server or another tenant.

Defining administrator types for applying the console layout

1. Go to **Administration | Superadmin | Console policies**.
2. In the **Console layout** area, select whether the Console layout applies to both super administrators and administrators or only to administrators.
3. Click **Save**.

Creating and assigning administrative roles

To restrict the rights of administrators (not super administrators), you can create roles and assign them to administrators. You determine, whether a role owner gets write or read access (or both) for certain options.
Global roles apply to all directory service structure objects.
Via **scope specific roles**, you determine for which areas of the directory service structure the roles apply.

Creating global role

1. Go to **Administration | Superadmin | Administrative roles**.
2. In the **Administrative roles** area, click the **Global roles** tab.
3. Click **Add**.

   → A new entry with the name **New role** appears in the list.

4. Double-click the name to edit it.
5. Press `Enter` to confirm the name change.
6. In the **Operations – [role name]**, edit the rights for certain options.
7. In the **Administrative roles** work area, click **Save** on the toolbar.

Assigning global role

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** area, select an administrator.
3. In the **Administrative roles – [admin name]** work area, click the Global roles tab.
4. Enable the check box with the role that you want to assign to the selected administrator.
5. In the **Administrative roles** work area, click **Save** on the toolbar.

Creating scope specific role

1. Go to **Administration | Superadmin | Administrative roles**.
2. In the **Administrative roles – [admin name]** area, click the **Scope specific roles** tab.
3. Click **Add**.

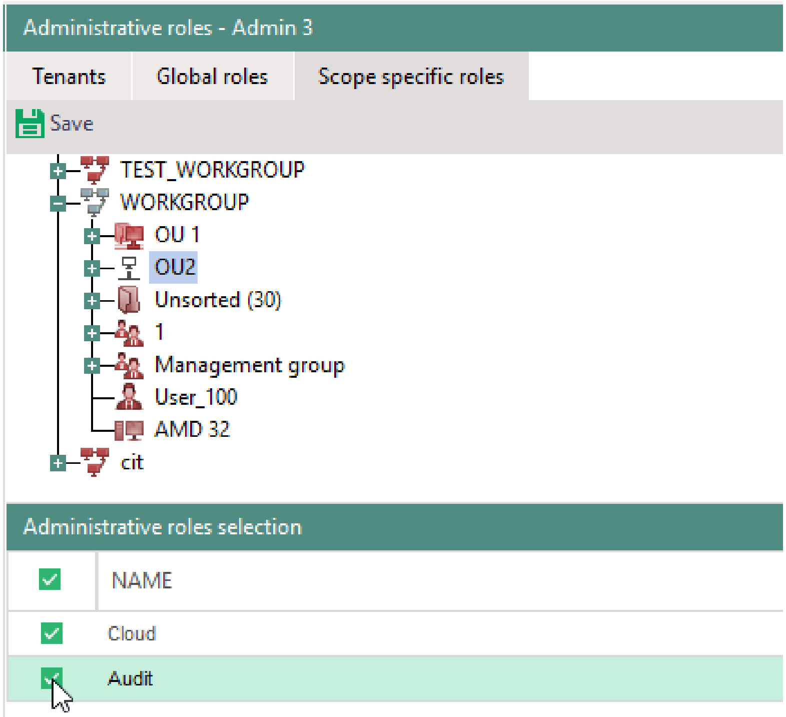
   → A new entry with the name **New role** appears in the list.

4. Double-click the name to edit it.
5. Press `Enter` to confirm the name.
6. In the **Operations – [role name]** area, edit the rights for certain options.
7. In the **Administrative roles** work area, click **Save**.

Assigning scope specific role

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** area, select an administrator.

3. In the **Administrative roles** work area, click the Scope specific roles tab.
4. Select an area in the directory service structure.
5. In the **Administrative roles selection** area, enable the checkbox of the role that you want to assign to the administrator of the selected area.
6. In the **Administrative roles – [admin name]** work area, click **Save**.



☑	NAME
☑	Cloud
☑	Audit

Figure 12. Administrative roles "Cloud" and "Audit" for OU 2

The administrator receives the rights of the role for the selected scope of the directory service structure. Other areas for which the role does not apply are marked in red. When clicking on one of the areas marked in red, the check box for the selected role disappears in the lower section.

2.3. Managing tenants

Tenants are used to separate areas of a directory service on one server. Each tenant can only access and view its own administration area. The settings of other tenants in the network are hidden.

By default, there is only one **<Default>** tenant in the Console which manages all objects of the existing directory service structure.

Global, tenant-independent data

Although the Console settings are tenant-separated and managed in isolation, the following areas are common for all tenants:

Product settings menu:

- Audit | Shadowcopy | Shadowcopy server settings work area
- Antivirus | Update settings | Server settings work area

Administration menu:

- Administrator | SSL configuration
- Superadmin | Import of settings from XML (global)
- Licenses | License management
- Servers | Log files
- Servers | EgoSecure servers
- Servers | Mail, proxy and others | Proxy server settings work area
- Synchronization (except Deleted objects)
- Servers | Integrity control
- All settings in **AdminTool**

Installation menu:

- EgoSecure agents | Installation settings | Automatic update of EgoSecure agents – server parameters work area

Tenant-specific database settings

You can set a maximum size of audit data per tenant. When the limit is reached, audit data is stored on the agent's computer until a capacity is available in the database. For details, see: Specifying size limit for Audit data

Creating and managing tenants

Creating new tenant

1. Go to **Administration | Superadmin | Tenants**.
2. Click **Add**.

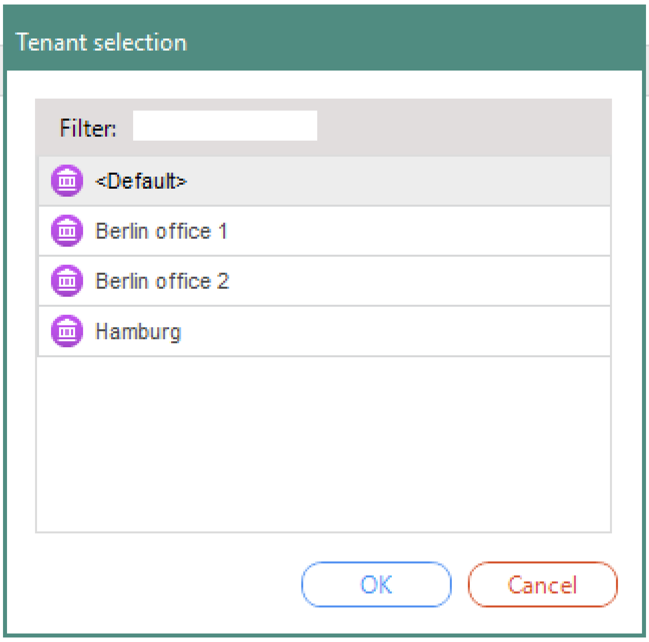
   → A new entry with the name **New Tenant** appears in the list.

3. Enter a name and press `Enter` to confirm.
4. Click on **No objects selected** entry in the OU column.

   → The **Selection of objects** dialog appears.

5. Select an **OU** in the directory service structure and click >.
6. Click **OK** in the dialog to confirm and then click **Save** on the toolbar.

The tenant is created, but can now only be managed by the supervisor. When logging in to the Server again, the tenant selection appears for the supervisor:



Tenant selection

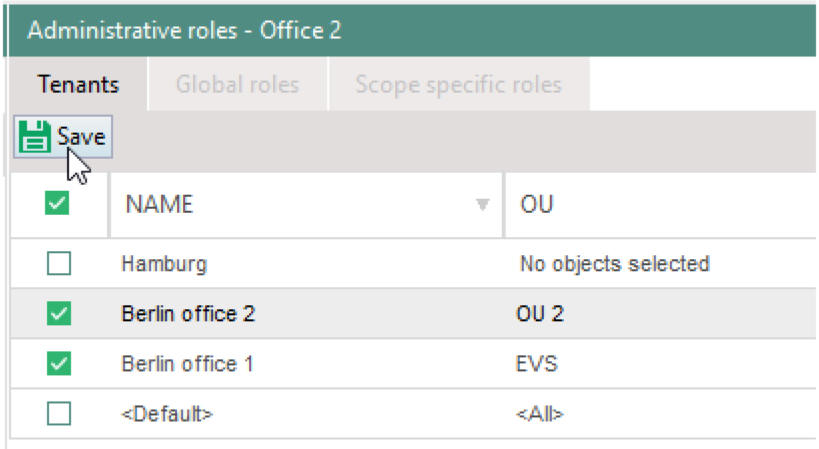
Filter:

- <Default>
- Berlin office 1
- Berlin office 2
- Hamburg

Figure 13. Tenant selection during login

Assigning tenant to administrator or super administrator

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** area, select the administrator to whom to assign a tenant.
3. In the **Administrative roles – [admin name]** area, enable the necessary tenants in the **Tenants** tab.



Administrative roles - Office 2

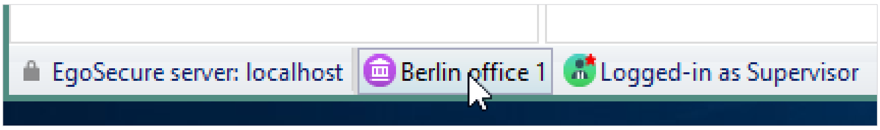
☑	NAME	OU
☐	Hamburg	No objects selected
☑	Berlin office 2	OU 2
☑	Berlin office 1	EVS
☐	<Default>	<All>

Figure 14. Assigning tenant

4. Click **Save**.

Switching between tenants

1. On the left bottom of the Console, click on [tenant name], to change the tenant.



EgoSecure server: localhost | Berlin office 1 | Logged-in as Supervisor

Figure 15. Changing tenant

→ The **Tenant selection** dialog appears.

2. Select a tenant and click **OK** to confirm.

➥ The Console opens with the settings defined for this tenant. The name of the tenant is displayed at the bottom left of the Console window.

2.4. Installing EgoSecure Agents

To install **EgoSecure Agents** on the clients, generate an MSI package via the **EgoSecure Console**.
In addition to the installation via software distribution, via the Microsoft Group Policy or via a local installation, you can install the **EgoSecure Agents** via the Console.

Details about the installation without Console you can find in the EgoSecure Installation Guide.

Before generating the MSI package, adjust the client settings and the settings for the MSI package, if necessary. For details, see Client settings
As soon as you initially install **EgoSecure Agent** on a client, the default permissions for users and computers will initially apply. If necessary, adjust these permissions before rolling out the MSI package. For details, see: Configuring default policies

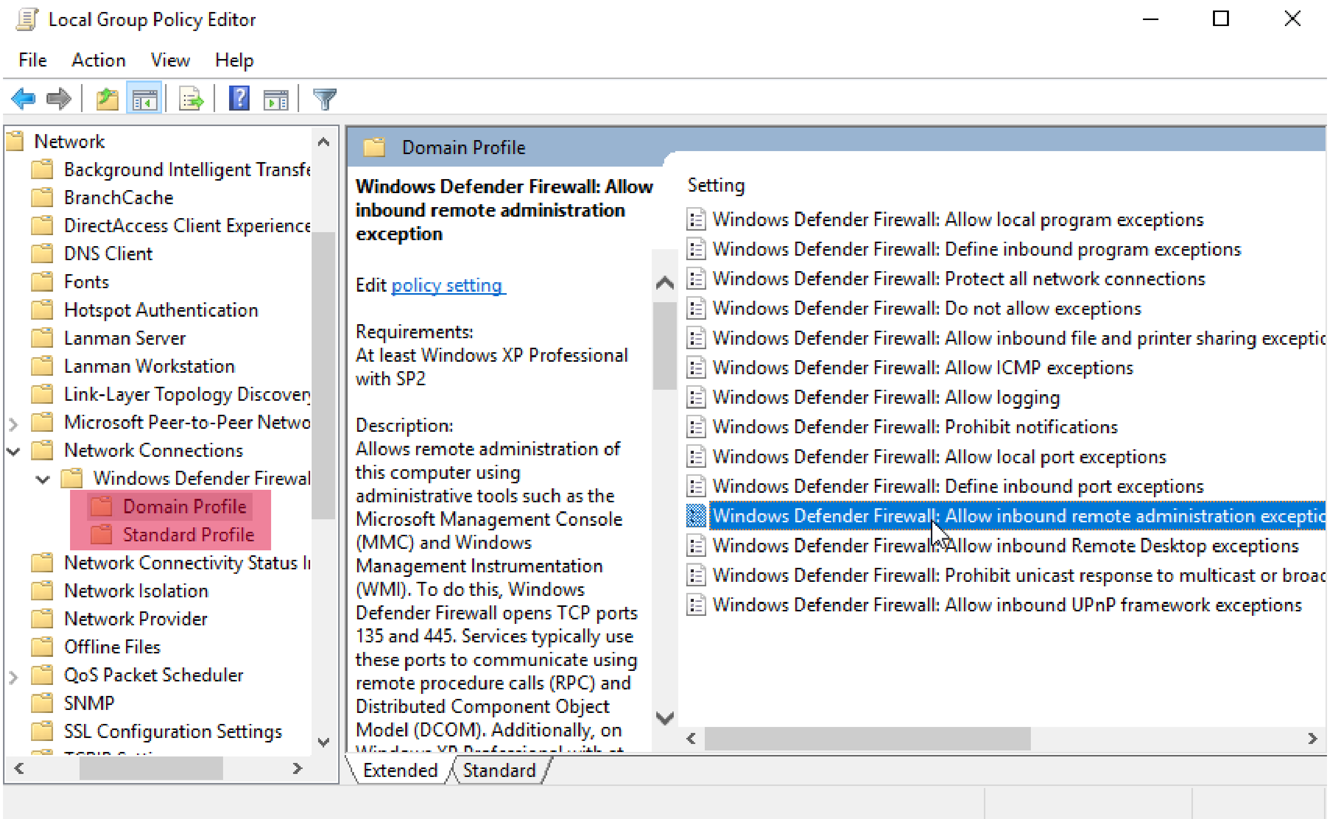
Adjusting Windows settings

For the **EgoSecure Agent** and **EgoSecure Server** to communicate with each other, enable the TCP ports on the Server and Client. If you did not enable **Add port to firewall exceptions** during the Server installation and you are using Windows Firewall, create the exception rules in Firewall **Advanced settings**.

If you install **EgoSecure Agents** via the Console, enable the **Allow inbound remote administration exception** option in addition. You can specify the setting locally via group policies or e.g. via GPO in AD.

Customizing group policy

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



- Network
  - Background Intelligent Transfe
  - BranchCache
  - DirectAccess Client Experience
  - DNS Client
  - Fonts
  - Hotspot Authentication
  - Lanman Server
  - Lanman Workstation
  - Link-Layer Topology Discover
  - Microsoft Peer-to-Peer Netwo
  - Network Connections
    - Windows Defender Firewal
      - Domain Profile
      - Standard Profile
  - Network Connectivity Status I
  - Network Isolation
  - Network Provider
  - Offline Files
  - QoS Packet Scheduler
  - SNMP
  - SSL Configuration Settings

Domain 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

Figure 16. Adjusting Windows settings

Adjusting client settings

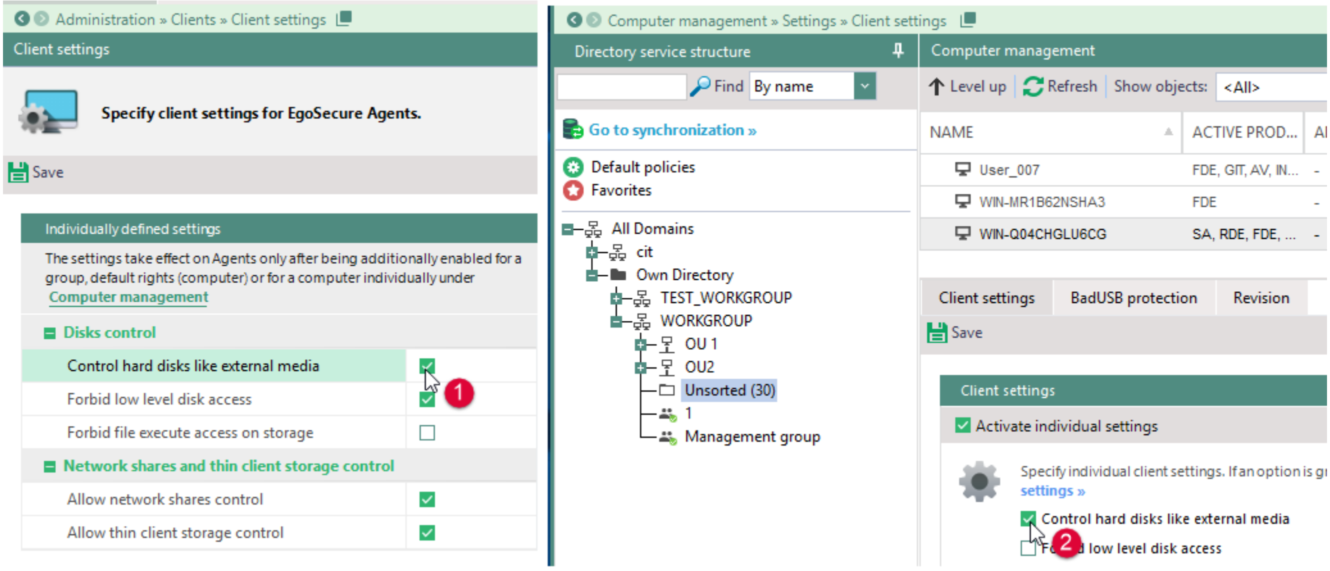
In the client settings, configure the extended settings of the **EgoSecure Agents**. These settings can also be changed after the Agent installation without reinstalling them.

Adjusting settings

1. Go to **Administration | Clients | Client settings**.
2. Edit the setting and click **Save**.

The client settings are divided into two groups:

- **Individually defined settings**. These settings are enabled under **Administration | Clients | Client settings**, but to take effect on Clients, these settings must be additionally enabled under **Computer management | <object selection> | Settings | Client settings** for a group, for default rights (computer) or for a computer.



Administration » Clients » Client settings

Client settings

Specify client settings for EgoSecure Agents.

Save

Individually defined settings

The settings take effect on Agents only after being additionally enabled for a group, default rights (computer) or for a computer individually under Computer management

Disks control

- Control hard disks like external media ☑
- Forbid low level disk access ☑
- Forbid file execute access on storage □

Network shares and thin client storage control

- Allow network shares control ☑
- Allow thin client storage control ☑

Computer management » Settings » Client settings

Directory service structure

Go to synchronization »

Default policies
Favorites
All Domains
cit
Own Directory
TEST_WORKGROUP
WORKGROUP
OU 1
OU2
Unsorted (30)
1
Management group

Computer management

Show objects: <All>

NAME	ACTIVE PROD...	AI
User_007	FDE, GIT, AV, IN...	-
WIN-MR1B62NSHA3	FDE	-
WIN-Q04CHGLU6CG	SA, RDE, FDE, ...	-

Client settings | BadUSB protection | Revision

Save

Client settings

☑ Activate individual settings

Specify individual client settings. If an option is g settings »

- ☑ Control hard disks like external media
- □ Fo d low level disk access

- **Globally defined settings**. The settings take effect on all Clients shortly after being enabled under **Administration | Clients | Client settings**. They must NOT be additionally enabled under **Computer management**.

Individually defined settings

Setting group	Setting	Description
Disks control	**Control hard disks like external media**	Treats additional hard disks like external media to apply encryption, filter, audit and DLP settings.
	Forbid low level disk access	Forbids the third-party applications a low-level access to external storage media and to hard disks (if they are controlled like external media).
	Forbid file execute access on external storage	Forbids to execute ***.exe** and ***.dll** files on CD/DVD disks, external storage devices (except mobile devices) and additional hard disks (if the **Control hard disks like external media** option is enabled). The option works independently of the **Access Control** product.
Network shares and thin client storage control	**Allow network shares control**	Allows EgoSecure to control network shares. If disabled, the EgoSecure products will not function on network shares: Access Control (including filters), Secure Audit, Network Share Encryption, Application Control, Data Loss Prevention, Insight Analysis and IntellAct Automation.
	Allow thin client storage control	Allow EgoSecure to control thin client storage. If disabled, the EgoSecure products will not function on thin client storage: Access Control (including filters), Secure Audit, Network

Setting group	Setting	Description
		Share Encryption, Application Control, Insight Analysis and IntellAct Automation.
Printers control	**Allow EgoSecure to control access to printers**	Controls access to local printers (physically connected) via EgoSecure instead of Windows.
Use account expiration date from the Active Directory	**Deny access for expired accounts**	As soon as an AD account expires, 🟩 access to all user devices and controlled clouds is denied (if the Access Control product is activated); 🟩 no applications can be started (if the Application Control product is activated), the exception is the applications from the Microsoft Windows vendor; 🟩 an access to encrypted files is no longer possible. Only the devices from an administrative white list of unique devices are permitted. The administrative white list of unique devices consists of devices assigned to <All users> under **Permitted devices | Removable devices | Individual device permissions**.
EgoSecure event log	**Write EgoSecure events into the Windows Event Viewer**	Writes the Agent activity into the Windows Event Viewer in addition to default log files.
	Write EgoSecure events into Syslog	Writes the Agent activity into the Syslog in addition to default log files.
Control input devices (BadUSB protection)	**Keyboard Control**	Allows the use of the primary keyboard. To allow other keyboards, add them to Individual device permissions. For details, see: Device permissions
	Automatic keyboard registration	Saves all connected keyboards to the user list of permitted devices. Disable the option once all available keyboards have been registered.
	Mouse Control	Allows the use of the primary mouse. To allow other mice, add them to Individual device permissions. For details, see: Device permissions
PRESENSE Connector (External storage analyzer)	**Enable PRESENSE Connector**	Enables the PRESENSE Connector. A certificate is required to use the connector.
	Certificate	Select a certificate. The certificate must correspond to the certificate of the PRESENSE configuration.

Globally defined settings

Setting group	Setting	Description
User permissions	**Allow requests for access rights**	Allows users to send requests for changing access rights. Requests are displayed under **Administration | Administrator | Access rights requests.**
	Allow log files remove	Allows users to delete log files of the EgoSecure Agent via the context menu of the tray.
Timeout on the client	**Timeout – common operations**	Defines how long the Agent or the Console waits for response from the Server while performing common operations. E.g.: timeout can be increased if the network is slow so that operations succeed successfully.
	Timeout – long operations	Defines how long the Agent or the Console waits for response from the Server while performing long operations such as Agent update, report generation, etc.
Disks control	**Drive letter assignment (first drive letter)**	Defines the first drive letter for external storage devices. This helps to avoid conflicts between network drives and external media.
Network shares and thin client storage control	**Protect 'fetrailer.metadata' file in the network**	Enable the option so that 'fetrailer.metadata' file cannot be deleted, moved or renamed. This file protects encrypted network folders from being deleted.
	Deactivate check for Windows offline file caching (not recommended)	Enable the option to ignore cache for offline files during network encryption. *Warning*: Enabling the option may lead to data damage! Once the option is disabled and offline files on the network contain cache, then the encryption of these files is not possible.
"Login as" timeout	**Auto reset "Login as" rights**	Define how long a user is permitted to use a login account with the rights of another user. Once the time is over, logout is performed automatically and the rights of the user currently logged on to the operating system are restored.
Polling	**Enable polling mode**	Enable Polling if the connection between the Server and the Agent cannot always be established due to network configuration (MSP, SaaS, etc.). With Polling, the Agent periodically connects to the Server and updates policies and settings if needed. In addition, define how often Agents
	Polling period (min.)	

Setting group	Setting	Description
		check for notifications on the Server. For details, see Setting up polling mode
Reduce traffic when metered connection is used	**Forbid Agent update**	Enable the option to forbid the update of EgoSecure Agents from the Server when metered connection is used. Updates of the Agents locally are still allowed. This option works only on Agents with Windows 10.
	Forbid audit data upload	Enable the option to forbid the audit data upload to the Server from EgoSecure Agents when metered connection is used. This option works only on Agents with Windows 10.
	Forbid shadowcopy data upload	Enable the option to forbid the shadowcopy data upload to the Server from EgoSecure Agents when metered connection is used. This option works only on Agents with Windows 10.
Privacy options (Windows 10 and later)	**Disable transmission of typing information**	Disable the built-in service that collects and sends typing information to Microsoft.
	Disable built-in Telemetry	Disable the automatic sending of information about your computer, installed programs and possible problems to Microsoft.
	Disable Windows Defender SpyNet	Disable the sending of data samples of possible threats and information about detected infections to Microsoft.
	Disable Users Steps Recorder	Disable the service that records all user steps and processes executed on computer.
	Disable Inventory Collector	Disable the collection of information from all computers in the network about installed applications, devices and system information.

Making polling mode available

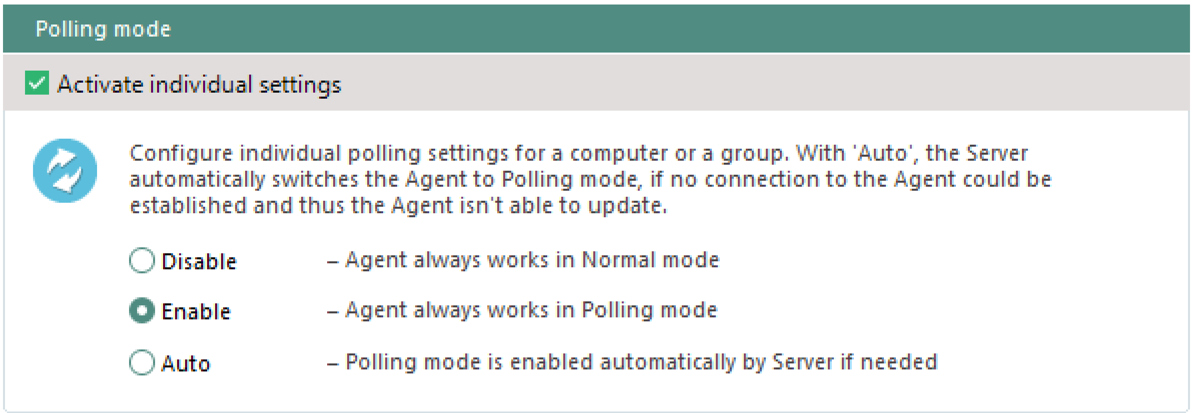
1. Under **Administration | Clients | Client settings**, check the **Enable polling mode** box.
2. Near **Polling period (min.)**, define at what intervals an Agent checks the Server for changes.
3. Click **Save**.

➥ Polling can now be enabled for all clients.

Enabling polling for default computer or for individual computer

1. Go to **Computer management**.

2. In the **Computer management** work area, select default rights (computer) or a directory service object (OU, computer, group).
   If you enable polling in default rights, the setting is inherited to all computers.
3. In the **Settings | Client settings** tab, select one of the following in the **Polling mode** area:
   a. **Disable**: the polling mode is disabled
   b. **Enable**: the polling mode is permanently enabled
   c. **Auto**: the polling mode is enabled automatically when needed
   To enable polling only for individual computers or the computers of a group, disable inheritance.



Polling mode

☑ Activate individual settings

Configure individual polling settings for a computer or a group. With 'Auto', the Server automatically switches the Agent to Polling mode, if no connection to the Agent could be established and thus the Agent isn't able to update.

○ Disable – Agent always works in Normal mode
● Enable – Agent always works in Polling mode
○ Auto – Polling mode is enabled automatically by Server if needed

Figure 17. Enabling polling for computer

4. Click **Save**.

Generating MSI package

When the Server is installed, the MSI package is automatically generated with the default settings and stored in the **EgoSecure Server** installation directory. Once the Server is updated, the MSI package is regenerated automatically and placed in the selected location on the **EgoSecure Server** computer.
If any setting change is required and/or you want to put the package on a different computer other than the Server computer, configure and generate the MSI package manually.

WARNING	**Possible data loss with immediate WLAN control installation** If for the setting **Install network driver for WLAN control** you select **Immediately**, the client network connection is temporarily interrupted after the Agent installation. This can lead to data loss. ◆ To install the WLAN control after the restart of the **EgoSecure Agent**, select **After restart**.

Configurable MSI package settings

Option	Description
EgoSecure Agent components installation	
Install network driver for WLAN control	Select if and when to install the kernel driver for WLAN control (esndislwf.sys). The following options are available: - **Do not install**: The WLAN control on the client remains disabled. - **Immediately** (not recommended): The driver is installed shortly after the MSI installation. Warning! The client network connection is temporary interrupted. - **After restart**: The driver is installed the first time the Client is restarted after the MSI installation.
Install kernel driver for CD/DVD control	Install the kernel driver (escdflt.sys) to encrypt on CD/DVD disks and control disk writing performed by third-party applications.
EgoSecure Agent service	
Protect EgoSecure Agent service and files	Protects the EgoSecure Agent service from being stopped and the EgoSecure Agent system files from being removed and renamed. Once a user tries to stop the EgoSecure Agent service, all device types listed under **Storage** group are blocked.
EgoSecure Agent UI	
Hide tray icon	Enable the option to make the EgoSecure Agent interface invisible. Users do not see any notifications, assigned permissions, etc. They can only use options available in the Windows Explorer context menu for encryption, Secure Erase, and Antivirus.
Tray UI language	Define the language of the EgoSecure Agent interface that is applied only during the first Agent installation. A user is permitted to change this language. The automatic language selection is performed in the following priority: 1. user-defined language (user key in the registry) 2. language specified when generating the MSI package 3. system language for the computer 4. English (if nothing above matches)

EgoSecure overlay icons priority	Define whether EgoSecure overlay icons have priority over other applications in Windows Explorer. Overlay icons identify an encryption type of files and folders. The following levels of adding EgoSecure Shell Icon Overlay Identifiers to the registry are available: - **Low** - adding z at the beginning of EgoSecure identifiers, no changes to the identifiers of other applications. - **Normal** - adding EgoSecure identifiers without spaces, no changes to the identifiers of other applications. - **High** - adding EgoSecure identifiers with spaces, no changes to the identifiers of other applications. - **Highest** - adding EgoSecure identifiers with spaces at the beginning, deleting spaces at the beginning of identifiers of other applications.
Uninstall/Update password	
Password	Optionally set a password required from users if they want to perform Agent uninstallation or update locally.
Check the password on	Select which operation with Agent is protected from unauthorized access: uninstallation or update
Rights for communication devices	
Apply after restart only	Define whether the rights for communication devices are applied shortly after the Agent installation or after a computer restart.
Write rights and settings into the MSI file (Offline Clients)	
Export access control rights	Export access rights defined in User management and Computer management under Control | Devices and ports tab.
Export permitted devices	Export a list of device permissions defined under Permitted devices | Permitted device models and under Permitted devices | Individual device permissions.
Export encryption settings	Export encryption types and encryption keys (including their private part) permitted for users or computers.
Export only public part of keys	Only having a public part of keys, a user is not permitted to decrypt, and therefore, open files encrypted on other Agents. Note: Files encrypted internally on this Agent can be decrypted.

Export EgoSecure Antivirus settings	Distribute AV signatures to selected computers via the MSI package not to overload the network; global antivirus exclusions are also applied. If proxy server settings are defined under **Administration | Servers | Mail, proxy and others** and the **Use proxy server** check box is set under **Product settings | EgoSecure Antivirus | Update settings**, proxy server settings are written. The proxy server settings will be used later for signature update on the Client side via the Internet (if update from the EgoSecure Server is not possible). For details, see Installing Antivirus via MSI
Selection of objects	Select the objects (user/computer) for which the rights and settings selected in this section are exported to the MSI file.
Write authentication certificate for SSL communication to MSI	
Add authentication certificate	Enable the option to add an Agent authentication certificate and its private key to the MSI package. The area with this option is greyed out if SSL is disabled. For details, see Configuring SSL.
Password	Enter a password to protect an Agent authentication certificate and its private key. This password is required from users during a local Agent installation/update or a remote Agent installation/update via script/software enrollment tools. Use only printable characters of the ASCII table.

INFO

Local installation on offline clients

To ensure that the permissions and settings defined under **User management** and **Computer management** are applied immediately after installation on Clients not waiting for a Server connection, write the permissions and settings of selected users/computers in the MSI file. For users/computers, which settings and permissions are NOT included in the package, the *Unknown user rights* are applied till the connection to the Server is established.

- In the **Write rights and settings into the MSI file** area, select which rights and permissions to write in the MSI file. Select the users/computers under **Selection of objects**.

Configuring and generating MSI package

1. Go 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.
   c. **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 for 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 **Path to the MSI package** area, define a folder where to save the MSI package.
   To save the MSI package to the location NOT on the computer with the **EgoSecure Server**, enable the **Other destination** option.
4. In the **Create MSI package** area, click **Generate**.
   → In the **Create MSI package** area on the right, the information about MSI package generation appears.
   → The defined selection for MSI settings is saved (except the **Other destination** option).
5. Click **Open folder** to open the location where the MSI package is stored.

➥ The MSI package can now be installed.

Installing EgoSecure Agents via Console

1. For computers of a directory service, which belong to **Own directory**:
   a. Go to **Computer management** and right-click a domain under the **Own Directory** folder.
   b. Select **Add | Computer** from the context menu.
   c. In the **Add – Computer** dialog, enter a name of a computer where to install the Agent.
   d. Click **OK** to confirm.

   e. Set up WMI on the computer where Agent will be installed to provide an access to administrative shares for the administrator.

2. Go to **Installation | EgoSecure agents | Installation settings**.
3. In the **Remote installation settings** area, specify the login data of the administrator who has enough rights for installing the EgoSecure Agent on the devices.
4. Click **Save** in the **Installation settings** area.
5. Go to **Installation | EgoSecure agents | Install/Update**.
6. Select **Only computers without agents** from the **Show** drop-down menu.
7. Select the clients for installation.
8. Click the **Install/Update** button.

➔ The Agents are now installed and activated on the clients.

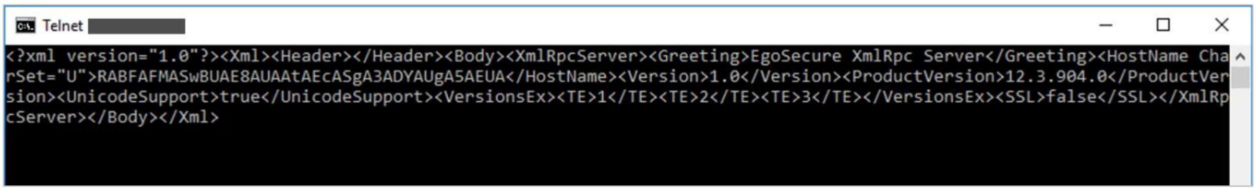
➔ You can use Windows Telnet to test the connection between the Server and Clients.

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.

1. Test the connection between Server and Client via Telnet. Open the Windows command prompt and enter the following:
   a. To test the connection from Server to Client:
   `telnet [Client IP address] 6006`
   b. 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>
```

Figure 18. Testing connection between Server and Client via Telnet

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

2.5. Activating products

For each Agent and computer, where a product will be used, you must activate the product in the Console. For each activated product you need a license. You can see the number of available and used licenses under **Administration | Licenses | License management**.

Activating products to objects

- To apply permissions to a computer and affect all its users, activate the product for the computer.

Regardless of the products and rights enabled for the user, the settings for the computer take effect.

- To allow a user to use the product on any (network) computer, enable the product for the user only.

The permissions set for the user are valid. These can be either the default rights of users, group rights or individual user rights.

You can additionally assign special permissions for a user on a certain computer. For details, see: Assigning user to computer

The following table gives an overview of products that can be activated to objects.

Activated only for computers	Activated only for users	Activated on users and on computers
BitLocker Management Green IT EgoSecure Antivirus Inventory Data Loss Prevention - Data at Rest	Cloud Storage Encryption Local Folder Encryption Network Share Encryption Password Manager Permanent Encryption Secure Erase Data Loss Prevention – Data in Use	Access Control Secure Audit Shadow Copy Application Control Removable Device Encryption Insight Analysis IntellAct Automation

Activating products

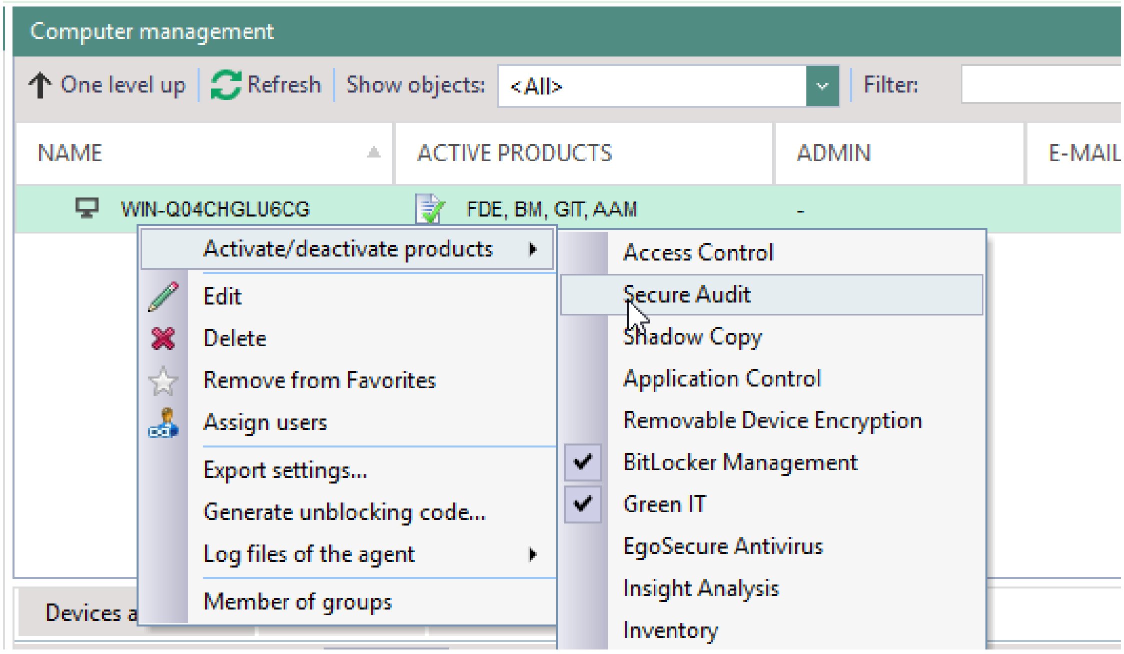
INFO

Activating Secure Audit and Encryption

- To activate **Secure Audit** for users, computers or groups, enable the secure audit functionality first under **Product settings | Audit | Secure Audit**.
- To activate encryption products for users, computers or groups, enable encryption under **Product settings | Encryption | Encryption options**.

1. Go to **User management/Computer management**.
2. In the **Directory service structure** area, select the OU/directory to which the user/computer or the group belongs.

   → The objects contained there appear in the **User management/Computer management** area.



NAME	ACTIVE PRODUCTS	ADMIN	E-MAIL
WIN-Q04CHGLU6CG	FDE, BM, GIT, AAM	-	

Figure 19. Activating product for computer

3. Right-click the object, for which you want to activate products.
4. In the context menu, select **Activate/deactivate products | [product name]**. If you select **Activate all**, all the available products are activated for the object.

In the **Active product** column, the shortcuts of products activated for the object are shown.

Activating products for all group members at once

- To automatically activate a product for all members or a group, activate the product for the group.

- For each group member a license is required. You can deactivate the product for individual group members.

Automatically activate products for new directory objects

If users and computers appear in the directory service structure via a synchronization, you can specify which products to automatically activate for new users and computers and whether product activation must depend on groups. For details, see: Setting up synchronization

2.6. Configuring default policies

In **Default policies**, define default rights and default settings for the known and unknown users of the directory service, as well as for computers. When a user or a computer is added to the directory service tree of the Console, it automatically inherits default rights and settings.

If a user is in the directory service tree and products are enabled for the user, he is considered a **known user**.
If a user is not in the directory service tree, or if no products are enabled for the user, he is considered an **unknown user**.

For each of the three default profiles, a distinction is also made between *online* and *offline* profiles for the **Access Control** product. *Offline* profile means that the client on which **EgoSecure Agent** was started has no connection to the **EgoSecure Server**.

INFO

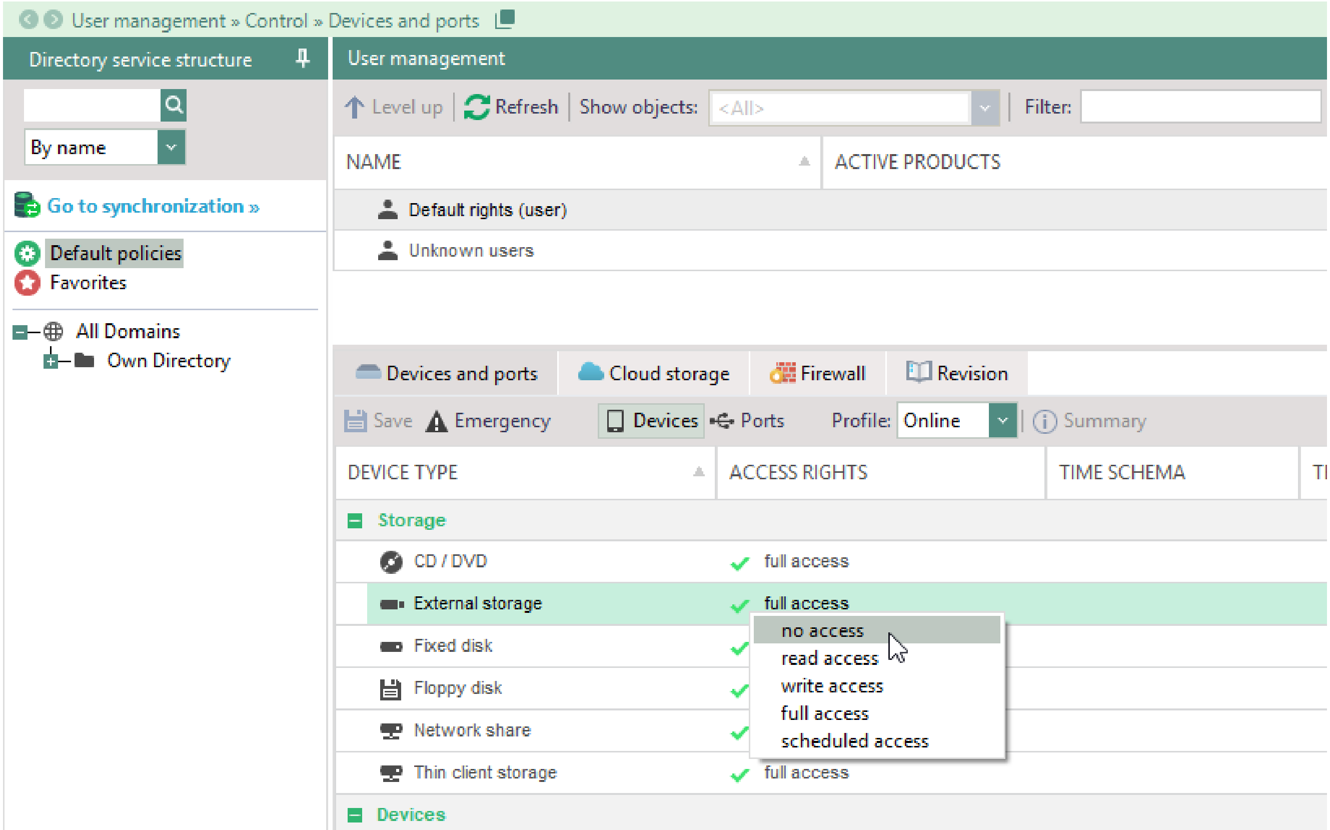
Activating Secure Audit and Encryption

- To activate **Secure Audit** for users, computers or groups, enable the secure audit functionality first under **Product settings | Audit | Secure Audit**.
- To activate encryption products for users, computers or groups, enable encryption under **Product settings | Encryption | Encryption options**.

Default rights and settings for user (known/unknown)

Customizing default rights for known users

1. Go to **User management | Directory service structure | Default policies**.
2. In the **User management** work area, select **Default rights (user)**.
3. Configure the rights of the default users for certain product areas. Depending on the available products, different tabs are available.



DEVICE TYPE	ACCESS RIGHTS	TIME SCHEMA	TI
Storage			
CD / DVD	full access		
External storage	full access		
Fixed disk			
Floppy disk			
Network share			
Thin client storage	full access		
Devices			

Figure 20. Configuring device access rights for default users in online mode

4. In the toolbar of the product area, click **Save**.

   → The settings are applied to default users in online mode.

5. When configuring **Access Control**:
   a. In the lower part of the work area, select **Offline** from the **Profile** drop-down.
   b. Define the settings for the offline profile of a default user.
      If the settings for the offline profile of a default user are not defined, the inheritance of access rights occurs from the online profile of a default user.
6. Click **Save** in the toolbar.

The defined rights apply to default users and are automatically inherited by all known users.

Customizing default rights for unknown users

1. Go to **User management | Directory service structure | Default policies | Unknown users**.
2. In the lower part of the work area, configure the rights of unknown users for certain device classes in online mode.
3. To define the rights of unknown users when they are offline, in the lower part of the work area, select **Offline** from the **Profile** drop-down.
4. Click **Save** in the toolbar.

- The defined default rights automatically apply to unknown users who login to the Server. Additionally, if global filters have been created under **Product settings | Filters | File type filters**, they are also applied to unknown users.

Customizing default settings for users

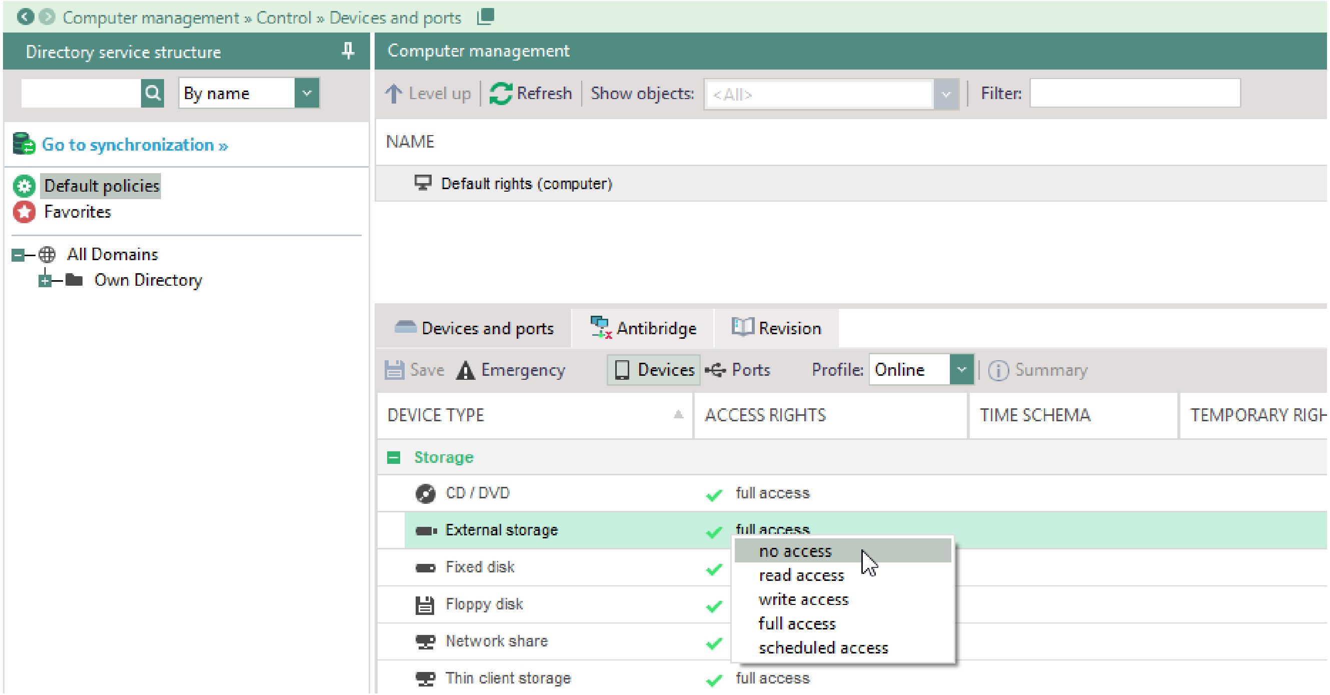
1. Go to **User management | Default policies** and select **Default rights (user**).
2. In the lower part of the work area, click the **Settings** tab.
3. To prohibit the downloading of files via the Internet Explorer, enable the check box in the **Internet** area.
4. To prohibit the usage of the clipboard, set the checkbox in the **Clipboard** area.
5. To scan the content of archives or MS Office for blocked file types, check the corresponding checkbox in the **File type filter** section. The checkboxes are only available if the options are enabled under **Product Settings | Filters | Settings**.
6. Click **Save**.

Default rights and settings for computer

Adjusting computer default rights

ⓘ INFO	**Rights priority for computer** If products are activated for both a user and a computer or only for a computer, the rights defined for computers always have priority. For details, see: Product activation

1. Navigate to **Computer management | Directory service structure | Default policies**.
2. Select **Default rights (computer)**.
3. In the lower part of the work area, configure the rights of default computers for certain products:



Computer management » Control » Devices and ports

Directory service structure

By name

Go to synchronization »

Default policies
Favorites

All Domains
Own Directory

Computer management

Level up | Refresh | Show objects: <All> | Filter:

NAME

Default rights (computer)

Devices and ports | Antibridge | Revision

Save | Emergency | Devices | Ports | Profile: Online | Summary

DEVICE TYPE	ACCESS RIGHTS	TIME SCHEMA	TEMPORARY RIGH
Storage			
CD / DVD	✓ full access		
External storage	✓ full access		
Fixed disk	✓		
Floppy disk	✓		
Network share	✓		
Thin client storage	✓ full access		

Figure 21. Configuring device access rights for default computers in online mode

4. When configuring **Access Control**:
   a. In the lower part of the work area, select **Offline** from the **Profile** drop-down.
   b. Define the settings for the offline profile of a default user.
      If the settings for the offline profile of a default user are not defined, the inheritance of access rights occurs from the online profile of a default user.
5. Click **Save** in the toolbar.

The defined rights apply to default computers and are automatically inherited by all computers of the directory service structure.

Configuring default settings for computers

The default settings for computers are only displayed in the **Settings** tab of the **Computer management** menu. Define the settings in the **Administration** menu under **Clients | Client settings**. For details, see: Adjusting client settings
These client settings are inherited by every computer and can be customized for individual computers. For details, see: Adjusting settings for computers

Adjusting settings for users

By default, users inherit the rights and settings of the default user. You can deactivate the inheritance and assign individual rights and settings. User rights only apply if the product is enabled for the user and not for the computer. For details, see: Activating products

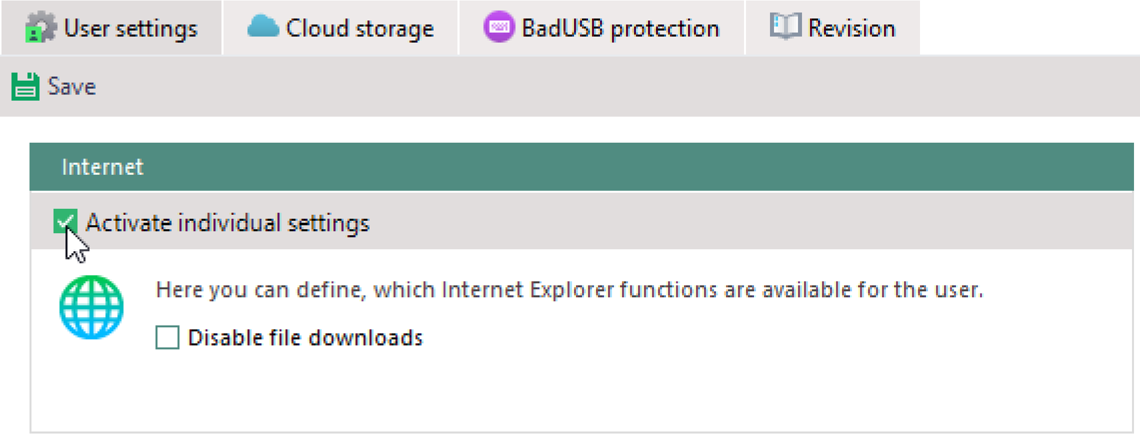
Adjusting settings for users

1. Go to **User management | Settings**.

→ See whether for the settings for **Internet, Clipboard** and **Communication** the inheritance is enabled and from where the user inherits the settings.

→ The settings in the **File type filter – embedded files** area are available only when options under **Product settings | Filters | Settings** are enabled.

2. Enable the **Activate individual settings** check box to deactivate inheritance and change the settings.



☑ Activate individual settings

Here you can define, which Internet Explorer functions are available for the user.

□ Disable file downloads

Figure 22. Deactivating inheritance and assigning individual user settings

3. Edit the settings and click **Save**.

➥ The selected user now receives the permissions that differ from the default user.

Customizing user rights for Secure Audit, Filters, Encryption and Application Control products

1. Select a user in **User management**.
2. In the navigation area, click the tab where you want to make changes.
3. Enable the **Activate individual settings** option.
4. Edit the settings and click **Save**.

Adjusting settings for computers

The settings defined for a computer in the **Settings** tab of the **Computer management** menu correspond to the client settings in the **Administration** menu. For details, see: Client settings

Adjusting settings for computers

1. Go to **Computer management | Settings**.
2. Select a computer in the **Computer management** area.
3. Enable the **Activate individual settings** check box to cancel the inheritance and to change the settings.
4. Disable the settings and click **Save**.

Customizing computer rights for Secure Audit, Filters, Encryption and Application Control products

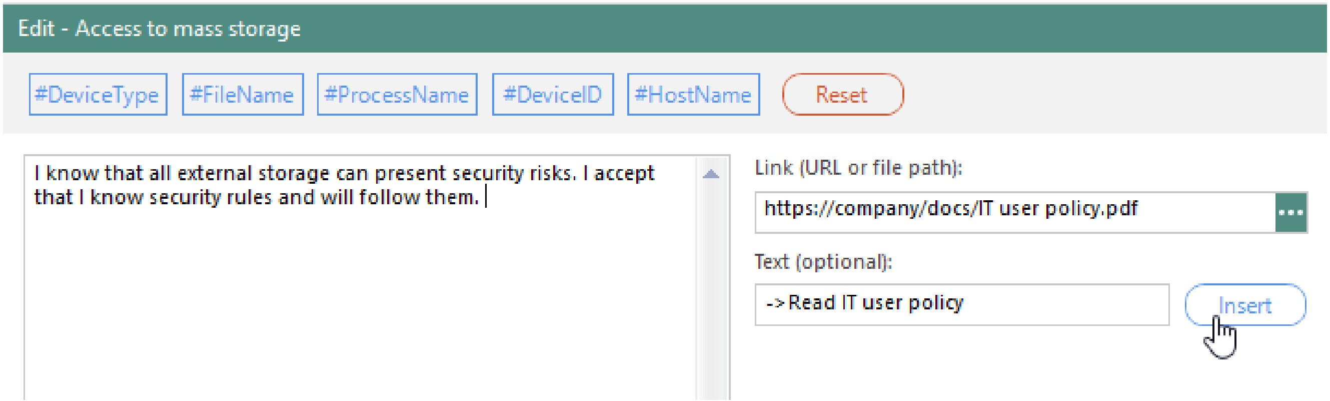
1. Go to **Computer management | Settings**.
2. Select a computer in the **Computer management** area.
3. Enable the **Activate individual settings** option.
4. Edit the settings and click **Save**.

2.7. Customizing user messages

You can customize the contents of module-specific user messages and security messages or completely disable messages.

Adjusting message

1. Go to **Administration | Clients | Custom messages**.
2. In the **Message** area, select a message type.
3. In the **Visible** column, enable or disable a message.
4. In the **Edit – [event name]** area, edit the message.
5. To insert a system variable into the message, click a variable on the toolbar.
6. To insert a link to the message,
   a. In the message text field, set the cursor to the place where you want to add the link.
   b. Add the link in the **Link** field.
   c. In the **Text (optional)** field, enter the text to be displayed.
   d. Click **Insert**.


Edit - Access to mass storage

I know that all external storage can present security risks. I accept that I know security rules and will follow them.

Link (URL or file path): https://company/docs/IT user policy.pdf

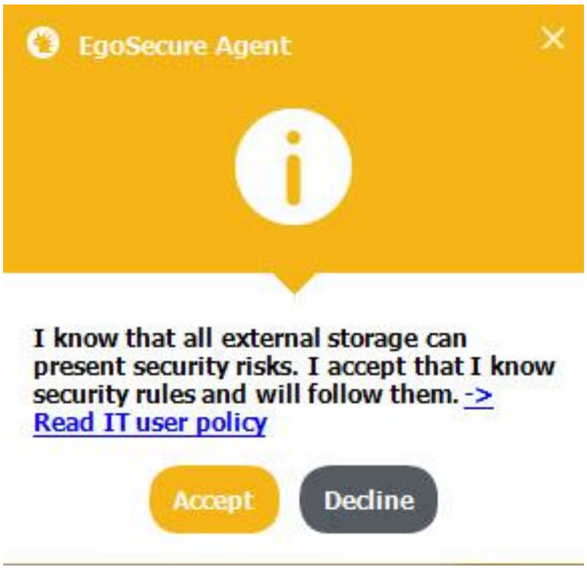
Text (optional): ->Read IT user policy

Figure 23. Editing message text

→ The link is added to the message text.

7. Click **Save**.

The changes apply.



I know that all external storage can present security risks. I accept that I know security rules and will follow them. -> Read IT user policy

Figure 24. Custom user message

2.8. Managing licenses

In the **Licenses** section, specify a license file or an activation code. You will also see the number of available and used licensed products.

Renewing or changing licenses

1. Go to **Administration | Licenses | License management**.
2. Click **Update license data**.

   → A dialog appears. You can activate products via a license file or via an activation code.

3. Product licensing via a license file:
   a. Select the **License file** radio button.
   b. In the **Name** field, enter the name of the licensee. You can find it in the attached **readme.txt**.
   c. Click **Browse ...** .
   d. Select a license file with ending **.lic** and click **Open**.
4. Product licensing via an activation code:
   a. Select the **Activation code** radio button.
   b. In the **Activation code** field, enter the activation code from the attached text file. Make sure you have an Internet connection.
   c. Fill in the **Organization** and the **E-mail** fields.
   d. Click **Check**.

   → The products contained in the license appear in the **Products** field.

   e. Click **OK** to confirm the dialog.
5. Click **Save**.

↳ The products included in the license (plus 5 trial licenses for non-purchased products) are now activated and can be assigned to users and computers. Once you

assign licenses to users or to computers, the number of used licenses appears in the **Active users** and **Active computers** columns.
See also: Activating products

2.9. Managing log files

Agent log files are used by the EgoSecure support to analyze a problem and help in finding a solution. Logs can be copied from Agent computers locally or via the Console. To copy logs from Agents via Console, Agents must be online (connected to the Server). By default, the Agent log files are stored under `C:\ProgramData\EgoSecure\EgoSecureAgent\LOG`. The path contains the log file of the tray (Agent) and the setup log (installation and update of drivers). The logs for installation and update are stored in the **Temp** folder (remote installation from Console) or in the MSI folder from where the Agent in installed (local installation).

In the **Log files** section, specify how detailed log files are, where and how long they are stored, and whether user names are hidden in them. You can also compress selected log files for EgoSecure support for error analysis.

Defining a custom log file path

1. Go to **Administration | Servers | Log files** or **Administration | Clients | Log files**.
2. In the **Log file directory** area, enable the **Custom** radio button.
3. Define your log file path.
4. Click **Save**.
5. Restart the Agent service or the Server service (depending where you define the log file path) to apply the changes.

Selecting log level

1. Go to **Administration | Servers | Log files** or **Administration | Clients | Log files**.
2. In the **Log level** area, select the level.

INFO

Debug and Extreme debug levels

The **Debug** and **Extreme debug** log levels gather detailed process information needed for the support to reproduce errors. However, very large log files are generated.

3. To allow logs of an extreme debug level:
   a. Go to **Installation | EgoSecure agents | Install/Update**.
   b. Select a computer. To multiselect, hold down `Ctrl` key and select.

   c. Right-click a computer and select **Log level | Extreme debug** from the context menu.
4. Click **Save**.
5. To apply the changes, restart the Agent service or the Server service (depending where you change the log level setting):
   a. if you change the log level from **Disabled** to **Normal**/**Administration**/**Debug**;
   b. if you change the log level from **Normal**/**Administration**/**Debug** to **Disabled**.

Saving log files

1. Under **Administration | Servers | Log files** or **Administration | Clients | Log files**, click **Compress...** on the toolbar.

   → The **Compress log files** dialog appears.
2. Select the components, Clients, and Servers, for which you want to group log files in a ZIP folder.
3. Change the destination folder, if necessary.
4. Click **Start**.

   → The selected log files are saved. A message about successful log file compression appears.
5. Click **OK** to confirm.
6. To open the target folder with the ZIP file in Windows Explorer, click **Open** in the **Compress log files** dialog.

Creating product-specific logs

1. Go to **Administration | Clients | Log files**.
2. In the **Log files settings by product** area, enable the log files:
   - **Write Full Disk Encryption log file** to create a separate log file for the **Full Disk Encryption** product
   - **Write EgoSecure Antivirus log file** to create separate log files for the **EgoSecure Antivirus** product
   - **Write log file for DLP DAR scans** to create a separate log file for **Data Loss Prevention – Data at Rest** scans
3. Click **Save**.

2.10. Managing Server

Under **Administration | Servers**, you can install additional servers, assign IP ranges and specify server priority. If you use multiple servers, you can define a favorite server for each Agent.
For details, see: Server connection - order and priorities

ATTENTION

Requirements for multi-server environments

- The installed EgoSecure version must be identical on all Servers used. It must be not lower than the version of the Agents that connect to the Server.
- The Servers must be in the same network so that they can communicate with each other.

Installing additional server

1. Install the same Server version as the already installed server.
   For details about the Server installation, see the EgoSecure Installation Guide.
2. During the installation, specify the same domain controller, SQL database, and database user as during the first installation.

➥ The new Server appears in Console under **Administration | Servers | EgoSecure servers**.

Server connection - order and priority

In a multi-server environment, an Agent attempts to connect to an available server in the following order:

1. **Favorite Server**: An attempt to establish a connection with the favorite Server.
2. **IP range**: If the favorite Server is not defined or not available, it searches for the Server with a defined IP range and verifies whether the Agent is in this range.
3. **Priority / Random**: If the Agent can not connect to either the favorite server or the primary IP range server, it tries to connect to the Server with the highest priority. If **Random selection** is selected in the **Server selection method** drop-down, the Server is selected randomly instead of the priority principle.

Assigning favorite Server

1. Go to **Installation | EgoSecure agents | Install/Update**.
2. Select an Agent from the list. To multi-select, hold down `Ctrl` and click.
3. Right-click an Agent and select **Favorite Management Server | [Server name]** from the context menu.

➥ The selected Server appears in the **Favorite server** column.

Assigning Server IP range

1. Go to **Administration | Servers | EgoSecure servers**.
2. Double-click a server entry in the **Primary IP-range** column.

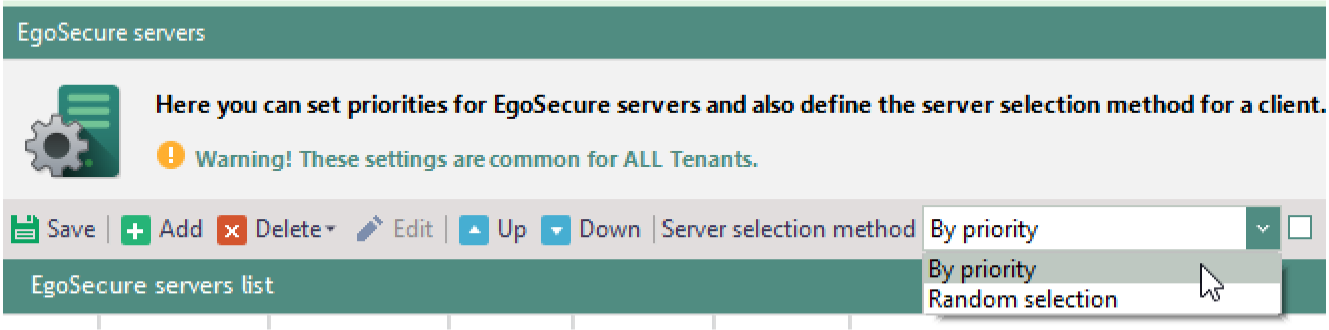
   → The column for this server is ready for editing.

3. Specify an IP range, to which Agents must belong to connect to the Server. Only IP addresses of the Ipv4 format are supported.
   You can use the asterisk symbol as a wildcard. Example: `192.168.1.*`, where `*` is any value from 0 to 255.
   It is also possible to set IP-range via en dash (e.g.: `192.168.10.10–192.168.10.200`) or via CIDR Notation (e.g.: `192.168.20.0/24`).
4. To add more than one IP address or range for the Server, divide them with the semicolon (`;`) without spaces.
5. Click **Save**.

All Agents that have IP addresses in the specified range can connect to the Server if the favorite Server is unreachable or undefined.

Enabling/disabling server priority

1. Go to **Administration | Servers | EgoSecure servers**.
2. In the **Server selection method** drop-down, select an option. This setting applies only if no favorite server is defined for the Agent and the Agent is not in the Server IP range:
   - **By priority**: Server selection occurs according to priority/order in the list
   - **Random selection**: Server selection occurs automatically (randomly)



EgoSecure servers

Here you can set priorities for EgoSecure servers and also define the server selection method for a client.

Warning! These settings are common for ALL Tenants.

Server selection method: By priority

Figure 25. Selecting Server according to priority/order

3. Click **Save**.

Setting a priority for a server

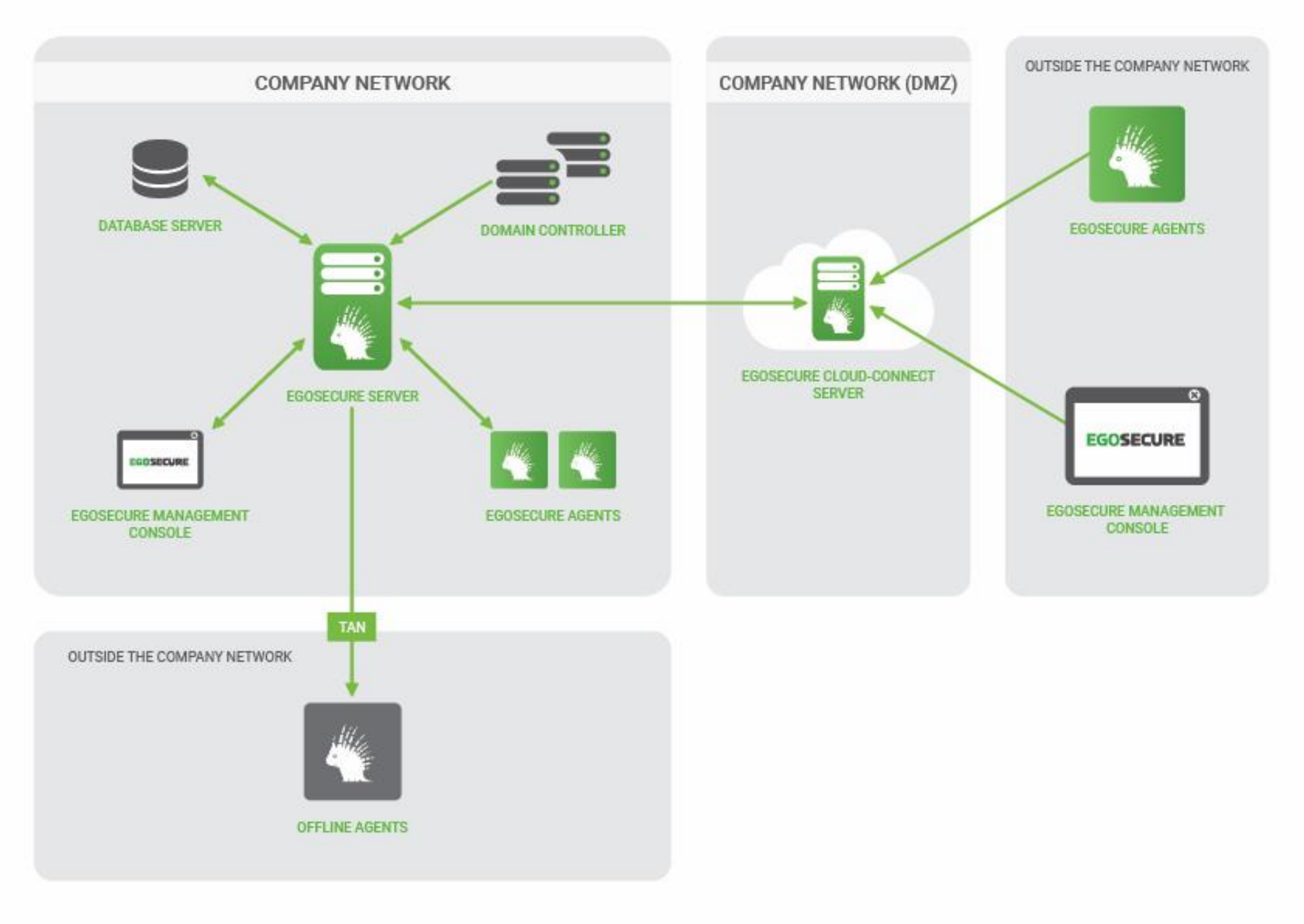
1. Go to **Administration | Servers | EgoSecure servers**.
2. In the **EgoSecure servers list** work area, right-click a server.
3. Select **Up** or **Down** from the context menu.

   → The Server moves in the list and the value of the **Priority** column changes.
4. Click **Save**.

The setting applies.

Configuring Cloud-Connect Server

EgoSecure Cloud-Connect Server (ES CCS) is an architecture element, which allows to manage computers/devices when they are outside a corporate network. The main idea is to install and deploy the main EgoSecure Server (ES Server) in the corporate LAN and connect the Agents to this main server. As soon as a part of the Agents is outside the corporate network, they connect to ES Server via ES CCS. ES CCS can be installed in the local network (e.g.: in the DMZ) or in the Internet.



Requirements for Cloud-Connect Server environment

- Enabled SSL. For details, see: Configuring SSL
- Enabled Polling mode (auto or permanently)
- Disabled HTTPS protocol. Communication via CCS is performed only using a default XML protocol.

Installing ES CCS

! There must be no **EgoSecure Agent** on the computer with **ES CCS**.

1. Launch the **ESCloudConnectSetup.exe** file.
2. Select the installation language and click **OK**.

   → The welcome dialog appears.

3. Click **Next**.

4. Change the location for the Cloud-Connect Server, if necessary, and click **Next**.
5. Specify the ports used on the Cloud-Connect Server:
   a. **Port for connecting servers**: a port for incoming connections from EgoSecure Servers (default: 8005).
   b. **Port for connecting clients**: a port for incoming connections from EgoSecure client applications (default: 8010).
6. Click **Next**.
7. Click **Install**.

Connecting EgoSecure Server and Agents to ES CCS

! Enable SSL to use **ES CCS**.

! Enable the specified ports on the computer with **ES CCS**.

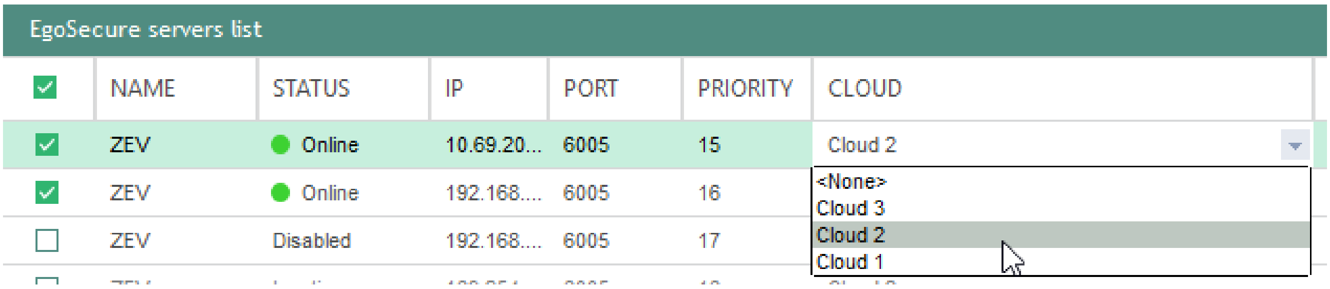
1. In the Console, go to **Administration | Servers | Cloud-Connect servers**.
2. Click **Add**.

   → The **Cloud-Connect server** dialog appears.

3. In the **Name** filed, define the name or IP address of **ES CCS**.
4. Specify the ports defined during the installation:
   a. **Port for serves**: a port for incoming connections from EgoSecure Servers (default: 8005).
   b. **Port for clients**: a port for incoming connections from EgoSecure client applications (default: 8010).
5. Click **OK** to confirm the changes and close the dialog.
6. Click **Save**.

   → The Console checks whether the added ES CCS is available via the defined ports and then shows the port status.

7. Define which Cloud-Connect server to use when connecting to the EgoSecure Server:
   a. Go to **Administration | Servers | EgoSecure servers**.
   b. In the **Cloud** column, select a Cloud-Connect server from the list.



EgoSecure servers list

☑	NAME	STATUS	IP	PORT	PRIORITY	CLOUD
☑	ZEV	● Online	10.69.20...	6005	15	Cloud 2
☑	ZEV	● Online	192.168....	6005	16	
☐	ZEV	Disabled	192.168....	6005	17	

Figure 26. Assigning Cloud-Connect Sever to EgoSecure Server

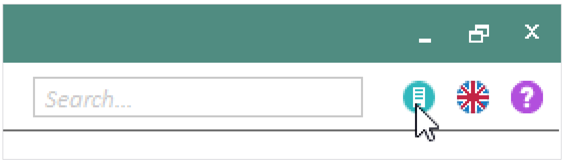
   c. Click **Save**.

↳ The communication between the EgoSecure Server and external Clients now occurs via **ES CCS.**

Connecting EgoSecure Console to ES CCS

1. Get the path for connecting to ES CCS, which consists of an ES CCS host, a port for clients and a server computer GUID:
   a. Go to **Administration | Servers | EgoSecure servers**.
   b. Right-click the EgoSecure Server entry and select **Copy Cloud-Connect path** from the context menu.
   → The path is copied to the clipboard.

2. In the main navigation, click 🖥 .



   → The **Connect to EgoSecure Management Server** dialog appears.

3. In the **Server** field, paste the path copied in step 1. The path has the mask `[host]:[port]/[server ID]`, where:
   a. `[host]` - host, where the ES CCS is deployed;
   b. `[port]` – port on the ES CCS for connecting the EgoSecure Console and Agents (by default: 8010);
   c. `[server ID]` – unique server identifier (GUID of the computer, where the EgoSecure Server is installed).

Example: 111.111.1.1:8010/1111a22b-2cc3-440d-5f5d-6e767ed888a9

   → The **Port** field is filled in automatically once the **Server** field is filled in. (Default: 8005).

4. Enter your login data and confirm with **OK**.

➥ The Console opens. **CCS** is now fully set up.

Deleting server

One server may work with several network adapters, that is why the procedure of deleting a server from the database is about deleting the whole server or deleting a network adapter.

Deleting network adapter

If a network adapter is currently inactive (e.g. network adapter is disabled in Windows settings), this entry is colored in light grey and such a network adapter can be deleted from the list. The active network adapters (colored in dark grey) can not be deleted from the list. To show only active network adapters, enable the **Hide inactive adapters** option.

1. Go to **Administration | Servers | EgoSecure servers**.
2. Select a network adapter. To multiselect, hold-down `Ctrl` and click.

3. Right-click one entry and select **Delete network adapter** from the context menu.
4. Click **Save**.

Information about selected network adapters is deleted from the database. Once network adapters are reconnected, they appear in the list.
In most cases, administrators delete the network adapters from the list, because they have been disconnected and administrators want to forbid Agents such a connection. But note that that the same can be achieved via removing the check box from this server so that it becomes unavailable.

Deleting a server completely

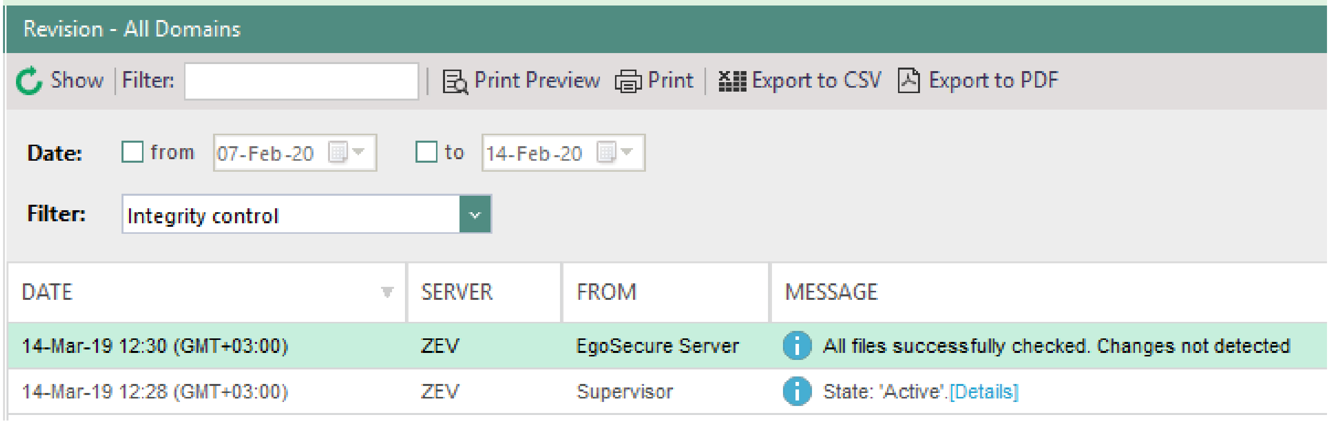
The server and all of its adapters — no matter whether they are available or not (colored in dark gray or in light grey, respectively) — can be deleted from the database via one option.

1. Go to **Administration | Servers | EgoSecure servers**.
2. Right-click a server and select **Delete server completely** from the context menu.
3. Click **OK** in the warning dialog to confirm.
4. Click **Save**.

Information about the server and all its network adapters is deleted from the database. Once network adapters of an installed server are reconnected, they appear in the list; if the server has been uninstalled, the reconnected network adapters do not reappear.

Protecting Console and Server files from damaging (Integrity control)

Use Integrity control to assure that **.exe** and **.dll** files under `C:\Program Files\EgoSecure\EgoSecure Server` (excluding **MSI** and **IoT** folders) are not damaged. If someone renames the files, or makes changes, our system displays it in **Reports | General | Revision**.



Date: □ from 07-Feb-20 □ to 14-Feb-20

Filter: Integrity control

DATE	SERVER	FROM	MESSAGE
14-Mar-19 12:30 (GMT+03:00)	ZEV	EgoSecure Server	All files successfully checked. Changes not detected
14-Mar-19 12:28 (GMT+03:00)	ZEV	Supervisor	State: 'Active'.[Details]

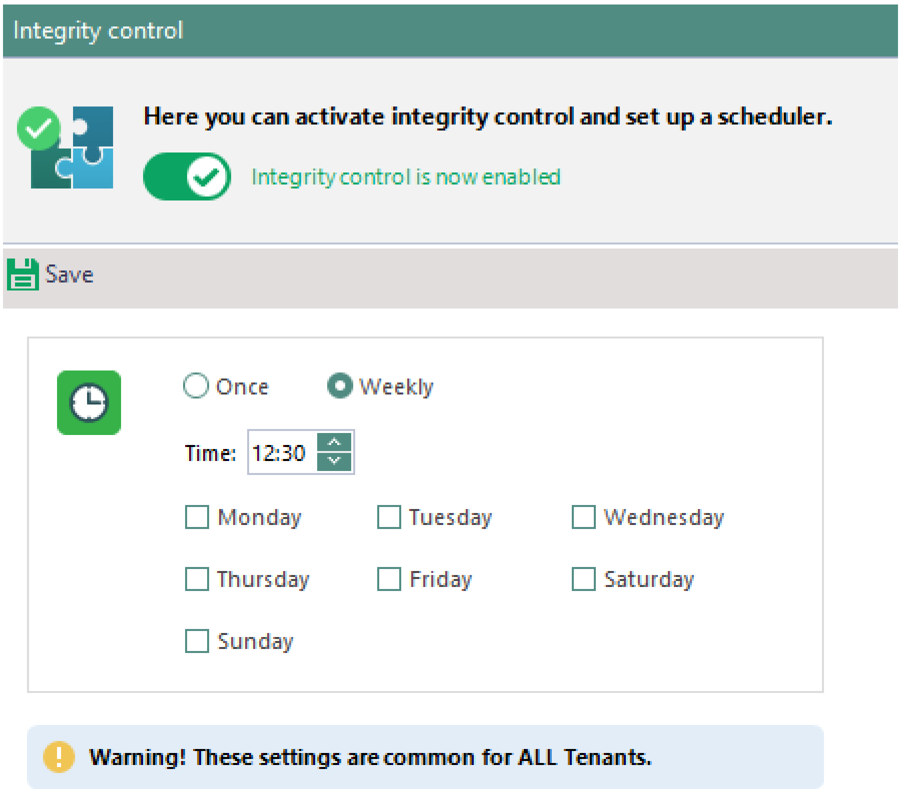
Figure 27. Integrity control result

With **IntellAct Automation**, you can create a rule to get notifications about integrity control actions via E-mail or SNMP. For details, see: IntellAct

Configuring Integrity control

1. Go to **Administration | Servers | Integrity control**.
2. Move the button to the right.

   → The status changes to **Integrity control is now enabled**.
3. Set frequency of control performing (once or weekly).



Integrity control

Here you can activate integrity control and set up a scheduler.

Integrity control is now enabled

Save

○ Once ● Weekly

Time: 12:30

□ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

□ Sunday

Warning! These settings are common for ALL Tenants.

Figure 28. Configuring Integrity control

4. Click **Save**.

➥ The Integrity control starts automatically at the specified time.

2.11. Setting up SMTP, proxy and other connections

Setting up SMTP server

SMTP server settings are specified to send, e.g., **IntellAct** notifications and automatically generated **Insight** reports by e-mail.

Defining SMTP server settings

1. Go to **Administration | Servers | Mail, proxy and others**.
2. In the **SMTP server settings** area, in the **Address "From"** field, enter e-mail to send notifications from this address.
3. Type an SMTP server name and port.

4. Check the **Use authentication** box to enable authentication on accessing SMTP server.
5. Define a user account.
6. Select an authentication method.
7. To check the entered information and test the connection, click **Check**.

   → If the connection has been tested successfully, a success message appears.
8. Click **Save**.

↳ An e-mail will be sent to the specified e-mail address for testing purposes. The e-mail address is ready to use.

Setting up proxy server

If you are using a proxy server, specify the connection information.

Setting up proxy server

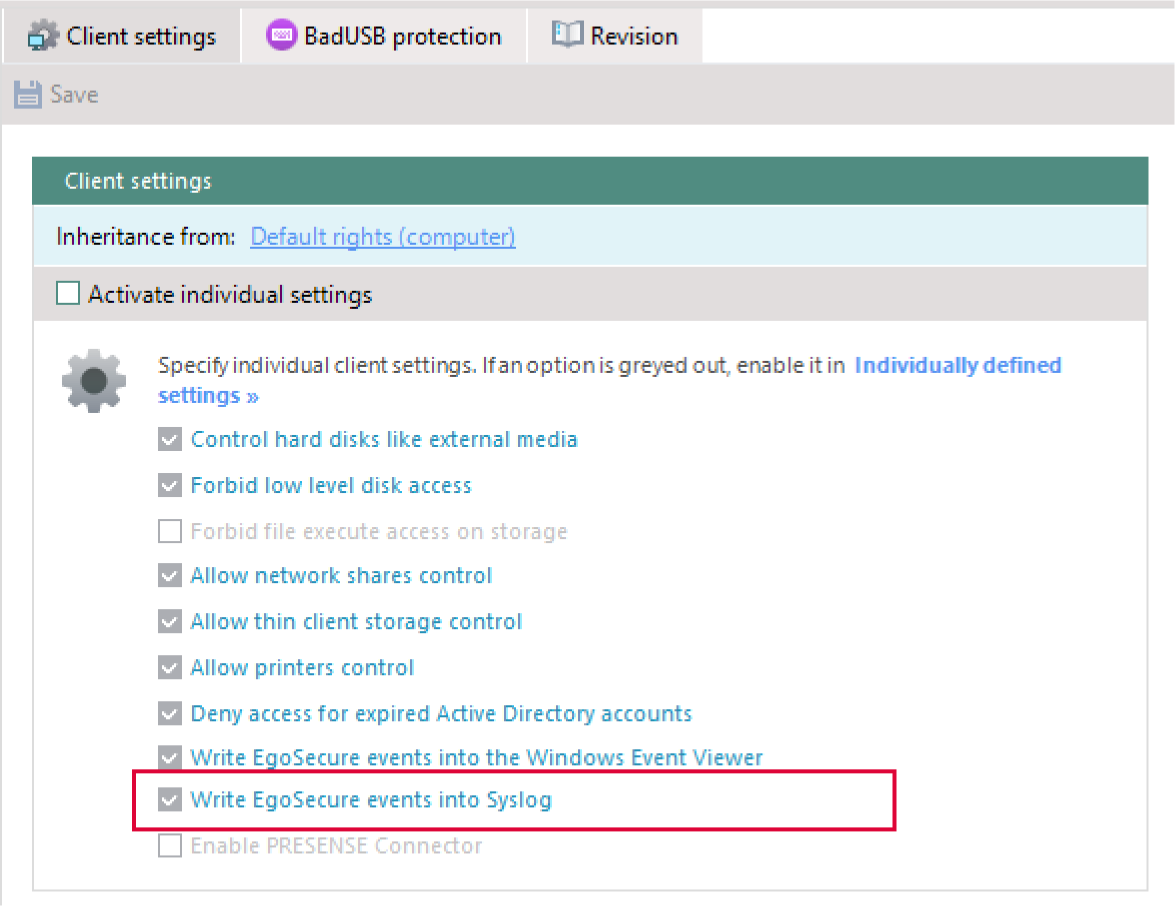
1. Go to **Administration | Servers | Mail, proxy and others**.
2. In the **Proxy server settings** area, enable **Connect through proxy server**.
3. Enter a proxy server name and port.
4. Enter a user name and password.
5. Click **Save**.

Setting up Syslog server

You can send notifications to a defined Syslog server after enabling Syslog and entering the server data of the Syslog server. All information types except the EgoSecure Server revision are sent directly from the EgoSecure Agent to Syslog server. The revision data is sent directly from the EgoSecure Server to Syslog.

Enabling Syslog

1. Open the **EgoSecure** application **AdminTool.exe**.
   a. Enable the **Write EgoSecure Server Syslog** check box.
   b. Click **Yes** to confirm the message about a server restart and close **AdminTool**.
2. In the Console, go to **Administration | Clients | Client settings**.
3. In the **EgoSecure event log** option group, enable the **Write EgoSecure events into Syslog** option and click **Save**.
4. Make sure that the option is not disabled for a computer under **Computer management | Settings | Client settings**.



Client settings

Inheritance from: Default rights (computer)

☐ Activate individual settings

Specify individual client settings. If an option is greyed out, enable it in Individually defined settings »

☑ Control hard disks like external media

☑ Forbid low level disk access

☐ Forbid file execute access on storage

☑ Allow network shares control

☑ Allow thin client storage control

☑ Allow printers control

☑ Deny access for expired Active Directory accounts

☑ Write EgoSecure events into the Windows Event Viewer

☑ Write EgoSecure events into Syslog

☐ Enable PRESENSE Connector

Figure 29. Inherited computer settings for syslog notifications

Setting up Syslog server

1. Go to **Administration | Servers | Mail, proxy and others**.
2. In the **Syslog server settings** area, define a server name (or its IP-address).
3. Enter a port (default: 514).
4. Select a protocol type.
5. Click **Save**.

Information sent to Syslog

Not all info is sent to Syslog. The available information types are listed below in the table.
The **Host** name column identifies the Server IP that sends information to syslog; in the **Date** and **Time** columns you can see the time of sending info to Syslog.
All information types except **Reports | General | Revision** are sent directly from the EgoSecure Agent to Syslog server. Revision data is sent directly from the EgoSecure Server to Syslog.

Info collected for Syslog	Info displayed in Syslog (Message column)
Reports | General | Revision Reports | Audit group Reports | EgoSecure Antivirus | Threat found	Information from all columns (including data that is displayed when clicking the **Details** link) of the Console report is gathered in the **Message** column.
Info about EgoSecure Server service start or stop	Server started/stopped.
Info about EgoSecure Agent connection to Server and about Agent service start and stop	When Agent connects, port and IP of the Server where Agent is connected are displayed.
Agent logon details	Logon Id Session Logon Type Logon Time Sid User Name Logon domain AuthPackage.

Setting up SNMP server

Specify an SNMP server to send notifications about **IntellAct** actions to the SNMP server. For details, see: IntellAct Automation

Setting up SNMP server

1. Go to **Administration | Servers | Mail, proxy and others**.
2. In the **SNMP server settings**, enter the name and port of the SNMP server.
3. Click **Save**.

Configuring Macmon NAC (Network Access Control)

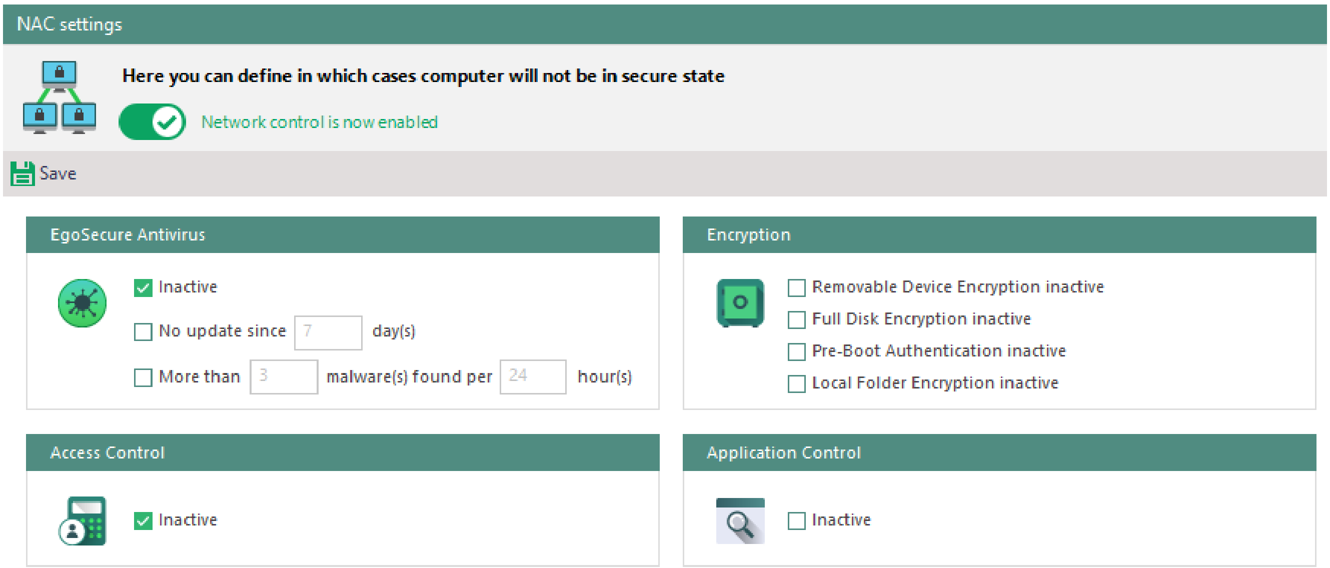
Network Access Control (NAC) verifies that the end devices in the network meet the specified security criteria.
If you use the NAC software **Macmon Network Access Control**, you can specify the connection information for the Macmon server and specify the circumstances on the Client to send a notification to Macmon.

Configuring NAC

1. Go to **Administration | NAC | NAC settings**.
2. Enable the network control.

   → NAC is now enabled.

3. Enable the options with **EgoSecure** products. If the defined options are not enabled on end devices, these devices are considered insecure and a message is sent to Macmon.



NAC settings

Here you can define in which cases computer will not be in secure state

Network control is now enabled

Save

EgoSecure Antivirus

☑ Inactive

□ No update since 7 day(s)

□ More than 3 malware(s) found per 24 hour(s)

Encryption

□ Removable Device Encryption inactive

□ Full Disk Encryption inactive

□ Pre-Boot Authentication inactive

□ Local Folder Encryption inactive

Access Control

☑ Inactive

Application Control

□ Inactive

Figure 30. Defining NAC settings

4. In the **Users to exclude from security state check** area, add users, who will not be checked for inactive **Removable Device Encryption**, **Local Folder Encryption**, **Access Control** and **Application Control** during NAC checks:
   a. Click **Add**.
   → The **Selection of users** dialog appears.
   b. Select the users.
   c. Click **OK** to close the dialog.
   → Selected users are added to the list.
5. Click **Save**.

Setting up Macmon server

1. Go to **Administration | NAC | Macmon settings**.
2. Check the **Activate Macmon** box.
3. Fill in the **Server** field (IP address, or host name of macmon server)
4. Enter user name and password.
5. Click **Save**.

Setting up Matrix42 Workspace Management Server

Matrix42 Workspace Management server is set up to receive information about IntellAct events via this server and undertake additional measures provided in the Matrix42 system. For details, see: Setting up IntellAct Automation to trigger Matrix42 Workspace Management workflows

2.12. Configuring SSL

To ensure secure data transmission between the EgoSecure components (Agent, Console and Server), a connection can be used via TLS, the next version of the SSL encryption protocol.

Version information

- TLS versions: 1.0/1.1/1.2/1.3
- OpenSSL version: 1.0.2n

Only exportable certificates are compatible.

Enabling SSL and distributing certificates

To use SSL in the company, the certificates must be generated either in the EgoSecure Console or in your own utility. In the EgoSecure database, three types of certificates can be stored and according to the selected type, the way of distribution changes:

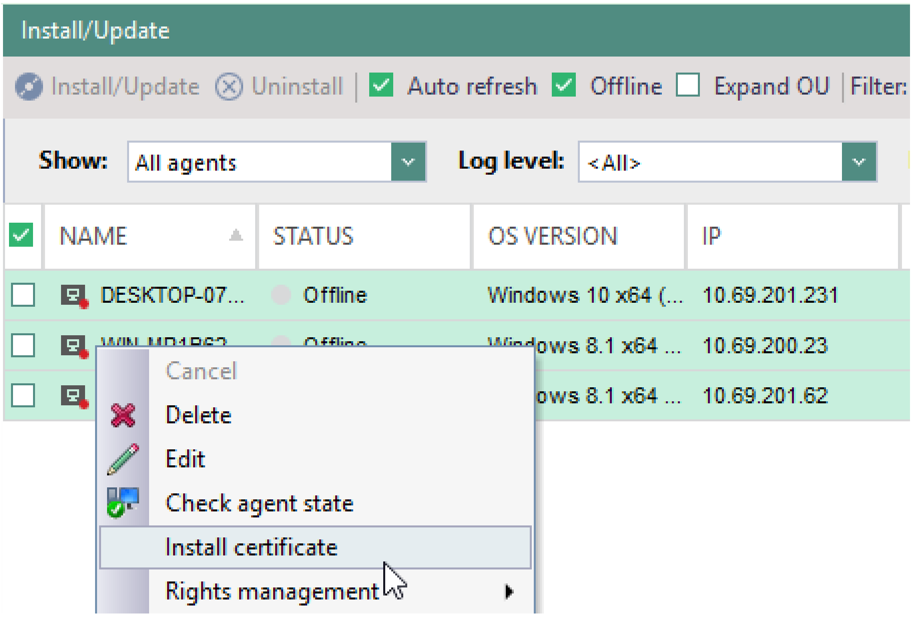
Certificate type	How to distribute?
EgoSecure certificates with their private keys	■ Way 1 ■ Way 2 ■ Way 3 ■ Way 4
NOT EgoSecure certificates with private keys	■ Way 1 ■ Way 2 ■ Way 3 ■ Way 4
NOT EgoSecure certificates without private keys	■ Way 3

Way 1: Update Agents to 13.3 (or higher) and install certificates via Console

1. Provide the certificates with their private keys to the Server database:
    a. *Using EgoSecure certificates*: Under **Administration | Administrator | SSL configuration**, click **Create** and then click **Generate all certificates**.
    To automatically renew the EgoSecure certificates, enable the Automatically renew certificates x days before expiration.
    b. *Using NOT EgoSecure certificates*: Under **Administration | Administrator | SSL configuration**, select a component and click **Import** to browse for a certificate with its private key. Repeat this step for all components (Agent, Server, Console).
2. Under **Administration | Administrator | SSL configuration**, enable the **Enable SSL and Allow communication without SSL** check boxes.
3. Click **Save**.

4. Go to **Installation | EgoSecure agents | Install/Update**.
5. Select the Agents via holding down `Ctrl` and clicking the rows. Do not use check boxes.
6. Right-click one entry and select **Install certificate** from the context menu.

! Make sure that Agents where certificates will be installed are updated to **13.3** version.



Install/Update

Install/Update | Uninstall | ☑ Auto refresh ☑ Offline □ Expand OU | Filter:

Show: All agents | Log level: <All>

☑	NAME	STATUS	OS VERSION	IP
□	DESKTOP-07...	Offline	Windows 10 x64 (...	10.69.201.231
□	WIN-MD1B62...	Offline	Windows 8.1 x64 ...	10.69.200.23
□			ows 8.1 x64 ...	10.69.201.62

→ Certificate distribution and installation starts.
To install certificates to offline Agents, use the polling mode, certificates will be installed once the connection with the Server occurs.

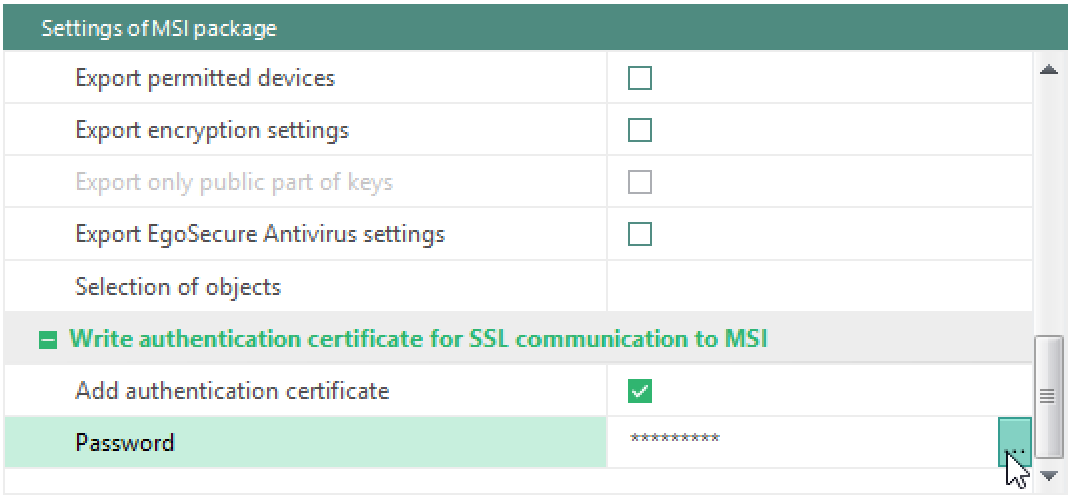
→ Once the installation finishes, in the **Info** column, check whether the certificate is installed successfully.

7. Once all certificates are distributed to Agents, disable the **Allow communication without SSL** option.

Way 2: Generate MSI with an authentication certificate and private key and reinstall or update Agents

1. Provide the certificates with their private keys to the Server database:
   a. *Using EgoSecure certificates*: Under **Administration | Administrator | SSL configuration**, click **Create** and then click **Generate all certificates**.
   To automatically renew the EgoSecure certificates, enable the **Automatically renew certificates x days before expiration** option.
   b. *Using NOT EgoSecure certificates*: Under **Administration | Administrator | SSL configuration**, select a component and click **Import** to browse for a certificate with its private key. Repeat this step for all components (Agent, Server, Console).
2. Under **Administration | Administrator | SSL configuration**, enable the **Enable SSL** check box.

3. Click **Save**.
4. Go to **Installation | EgoSecure agents | Create MSI package**.
5. Check the option **Add authentication certificate** and define a password to protect the Agent authentication certificate and its private key (use only printable characters from the ASCII table for the password).



Settings of MSI package	
Export permitted devices	□
Export encryption settings	□
Export only public part of keys	□
Export EgoSecure Antivirus settings	□
Selection of objects	
⊟ Write authentication certificate for SSL communication to MSI	
Add authentication certificate	☑
Password	*********

6. Click **Generate** to generate the MSI package.
7. If it is a first installation, install Agents. If Agents have already been installed, reinstall them via Console or perform update locally/via software distribution tools.

ATTENTION	**Update via Console** When updating Agents via Console, the certificate with it private key will not be installed. That is why, make sure to uninstall existing Agents and install new ones.

→ ***Local Agent installation/update***: The password defined in step 5 must be entered manually in the dialog that appears during installation.

→ ***Remote Agent installation via Console***: The password is transferred to the Agent in an encrypted form and is automatically applied. It is not needed to enter it manually on the Agent side.

→ ***Remote Agent installation/update via script/software enrollment tools***: Write a password directly in the script via the `PKCS12_PASS=""` command. The password is transferred to Agents in an unencrypted form.
E.g.: `msiexec /fvamus ESAgentSetup_x64.msi PKCS12_PASS ="mypassword"`

Way 3: Distribute certificates, update Agents to 13.3 (or higher) and provide certificates information to EgoSecure

1. Prepare certificates for distribution:

   a. *Using EgoSecure certificates*: generate certificates in Console and then export them under **Administration | Administrator | SSL configuration**.
   To automatically renew the EgoSecure certificates, enable the **Automatically renew certificates x days before expiration**.
   b. Using NOT EgoSecure certificates: omit this step.
2. Distribute certificates to Server, Agents and Console manually or via special tools for automatic certificate distribution.
3. Provide the data for EgoSecure to identify the certificates:
   a. Using EgoSecure certificates: omit this step.
   b. *Using NOT EgoSecure certificates*: provide the certificates without its private part via one of the following options:

- Option 1: import certificates for all components.
  Select the component from the list and click **Import**. In the **Import certificate** dialog, click **Browse** to select a certificate. Click **OK**.
- Option 2: select certificates from local storage for all components.
  On the computer where Console is launched, import the Agent and Server certificates to the local computer store (e.g., via mmc). In Console, select the component (Agent, Server or Console) and click **Select**. In the Windows Security dialog, click **More choices** to expand the list. Select the installed certificate.

4. Under **Administration | Administrator | SSL configuration**, enable the **Enable SSL** and **Allow communication without SSL** check boxes.
5. Click **Save**.
6. Update Agents to at least 13.3.
7. Once all Agents are updated and all certificates are distributed to all components, disable the **Allow communication without SSL** option.

Way 4: Generate certificates during Server installation, provide certificates information to EgoSecure and install Agents

1. On the **SSL and certificates** step of the Server InstallShield Wizard, check **Enable SSL**.
   The **SSL and certificates** step is not shown if the specified database already contains the EgoSecure password for protecting authentication certificates and its private keys.
2. Check the **Add authentication certificates with private keys to MSI** box and define a password to protect the Agent authentication certificates.
3. Click **Next** and finish the EgoSecure Server installation. For details about the EgoSecure Server installation, see the EgoSecure Installation Guide.
4. Provide the certificates with their private keys to the Server database:
   a. *Using EgoSecure certificates*: certificates are generated automatically shortly after the EgoSecure Server start.
   To automatically renew the EgoSecure certificates, enable the **Automatically renew certificates x days before expiration**.

   b. *Using NOT EgoSecure certificates*: In Console, under **Administration | Administrator | SSL configuration**, select a component and click **Import** to browse for a certificate with its private key. Repeat this step for all components (Agent, Server, Console).

5. Go to **Installation | EgoSecure agents | Create MSI package**.
6. Click **Generate** to generate the MSI package.
7. Install Agents.

   → **Local Agent installation**: The password defined in step 2 must be entered manually in the dialog that appears during installation.

   → **Remote Agent installation via Console**: The password is transferred to the Agent in an encrypted form and is automatically applied. It is not needed to enter it manually on the Agent side.

   →**Remote Agent installation via script/software enrollment tools**: Write a password directly in the script via the `PKCS12_PASS=""` command. The password is transferred to Agents in an unencrypted form.
   E.g.: `msiexec /fvamus ESAgentSetup_x64.msi PKCS12_PASS ="mypassword"`

Enabling HTTPS server and connecting components

Adding HTTPS server

1. Go to **Administration | Servers | EgoSecure servers**.
2. Click **Add**.

   → The **Server Alias** dialog appears.

3. In the **Alias** field, enter the server address according to the following template: *https://[Server name]* or *https://[Server IP]*. Example: *https://10.0.2.15*
4. (optional) In the **Primary IP-range** field, define IP addresses of Agents, which are permitted to connect to this Server. For details, see Assigning Server IP range.
5. In the **Port** field, type *7005*.
6. Click **OK**.

   → The dialog closes.

7. Click **Save**.

Connecting Console to HTTPS server

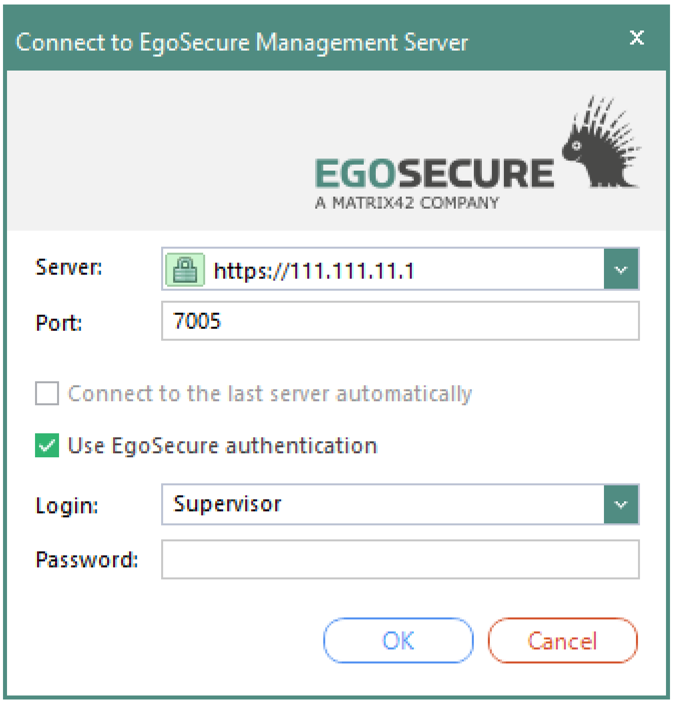
1. Start the Console.

   → The **Connect to EgoSecure Management Server** dialog appears.

2. In the **Server** field, enter:
   a. *https://[Server name]*. E.g.: *https://testserver123*
   OR
   b. *https://[Server IP]*. E.g.: *https://111.111.11.1*

→ A green lock icon appears in the **Server** field. If no certificate is selected, a gray lock appears. If an invalid certificate is selected, a red lock appears.

→ If necessary, click the icon to select a certificate.


Connect to EgoSecure Management Server

Server: https://111.111.11.1

Port: 7005

□ Connect to the last server automatically

☑ Use EgoSecure authentication

Login: Supervisor

Password:

Figure 31. Server login via https

3. In the **Port** field, enter *7005*.
   Make sure that port 7005 is not blocked by the Firewall or not used by another application. You can change the port in the AdminTool.
4. Enter login data and click **OK**.
   → The entered **Login** field data is remembered and will be offered for selection if the **Save entered user logins** check box is enabled in the Console under **Administration | Superadmin | Console policies**.

The Console opens.

Connecting Agents to HTTPS server

! The Agent version must be not higher that the Server version.

1. Go to **Installation | EgoSecure agents | Install/Update**.
2. Right-click an Agent. To select multiple Agents, hold down `Ctrl` and click.
3. From the context menu, select **Favorite Management Server** and select the HTTPS Server.

The Agent connects to the favorite Server first. If the favorite Server is not available, the Agent tries to connect to another Server in the following order:
1. The Server, for which the defined Agent IP range matches
2. The Server with the highest priority

Identifying client connections and updating certificates

Via the Console, you can verify that certificates are installed and valid on individual Clients. A distinction is made between archived (valid) certificates and expired (not valid) certificates:

- **Archived certificate**: A valid certificate, which was replaced with a new certificate. Such a certificate remains in the database. When the Agent with an archived certificate connects to the Server, the Server provides a new certificate to the Agent (if such a certificate with a private key exists on the Server database).
  If there is no certificate with a private key in a Server database, then update certificates on your own via software distribution tools and provide certificate information to EgoSecure as described here.
- **Expired certificate**: An invalid certificate, which cannot be used for communication more. When the Agent with an expired certificate tries to connect to the Server, the connection fails.
  Use any of the ways described under Enabling SSL to replace expired certificates.

Under **Installation | EgoSecure agents | Install/Update**, client connections are marked with the locks of different colors in the **Last connected** column:

Icon	Description
🔒	Secure connection.
🔒	Secure connection, which demands attention. The client has a valid but not an up-to-date certificate, which must be replaced.
🔒	Connection is insecure. No certificate on the client side.
🔒	Connection is insecure. The client has a certificate, information about which is not in the database or the certificate has expired or the private key has been compromised.

2.13. Managing Windows Firewall

Under **Administration | Clients | Firewall management**, define the Firewall settings on Clients relevant for Client-Server communication. The following options are available:

Option	Description
Activate Firewall Management with EgoSecure Data Protection	Enables Windows Firewall on all computers where Agents are installed. User can disable it manually. Once the option is enabled, the two options below become available for activation.
Firewall always active	Enables Windows Firewall on all computers where Agents are installed. If a user disables it manually, Firewall is automatically enabled back.

Open communication ports	Adds port 6006 (port on the Agents for incoming connections) to Firewall exclusions.

3. ACCESS CONTROL

3.1. Access Control - basics

With **Access Control**, you can manage access rights for users and computers in your directory. Activate **Access Control** for computers or for users accordingly.

- Configurable for users and computers.
- Applicable to device classes and port types (all external storage media, all scanners, etc.).
- Applicable to specific device and port models (based on model name, specific hardware ID, serial number, etc.).
- Offers different access rights for online and offline Agents.
- Makes it possible to differentiate between rights for online and offline Agents, and unknown or known users. Unknown users are either the users not registered on the Server or the own directory users for whom no products have been activated.

3.2. Controlling access to device and port types

Controlling access to drive and device types

INFO

Product activation required

For the access rights configuration to take effect, activate **Access Control** for the selected object (user/computer). For details, see: Activating products

ATTENTION

Not blocked devices

If a device (e.g. USB HID device) got no known functionality in Windows, it will not be detected in device classes. These devices got no security relevant functionalities and will not be blocked by EgoSecure Agent.

Allowing/blocking certain device types

1. In the **User management/Computer management | Control**, select a user or a computer in the **User management/Computer management** work area.
2. In the lower area, select the **Devices and ports** tab.
3. In the **Profile** drop-down, select whether permissions apply to online or offline mode. Offline mode means that there is no connection to **EgoSecure Server**.
4. Right-click a device.
5. Select an access type in the context menu. Depending on the device type, the following options are available:
   a. **Not controlled** (EgoSecure doesn’t control a selected device)

   b. **No access**
   c. **Read access** (only storage media)
   d. **Write access** (only storage media)
   e. **Print access** (only locally connected printers)
   f. **Full access**
   g. **Scheduled access**
      For details, see: Configuring scheduled access
   h. **Playback access** (only sound, video and game controllers)
   i. **Temporary access**
      For details, see: Configuring one-time access

6. Click **Save**.

➥ The new permissions apply on the Agents.

INFO	**Permissions in offline mode** Permissions specified for an online mode are automatically applied to an offline mode until making changes to the offline profile. ◆ To change permissions for the offline mode, repeat the steps from Allowing/blocking certain device types and select **Offline** profile in step 3.

Controlling access to port types

You can control access to ports. The following ports are controllable:

- FireWire
- PCMCIA
- Parallel
- Serial
- USB (except mice and keyboards)

Priority over device type settings

The settings for ports have priority over the settings for device types. So a full access to external storage media may be defined, but access will be blocked if the storage medium is connected via USB and an access to the USB port is not allowed. Individual device permissions, on the other hand, work independently of the access rights for ports.

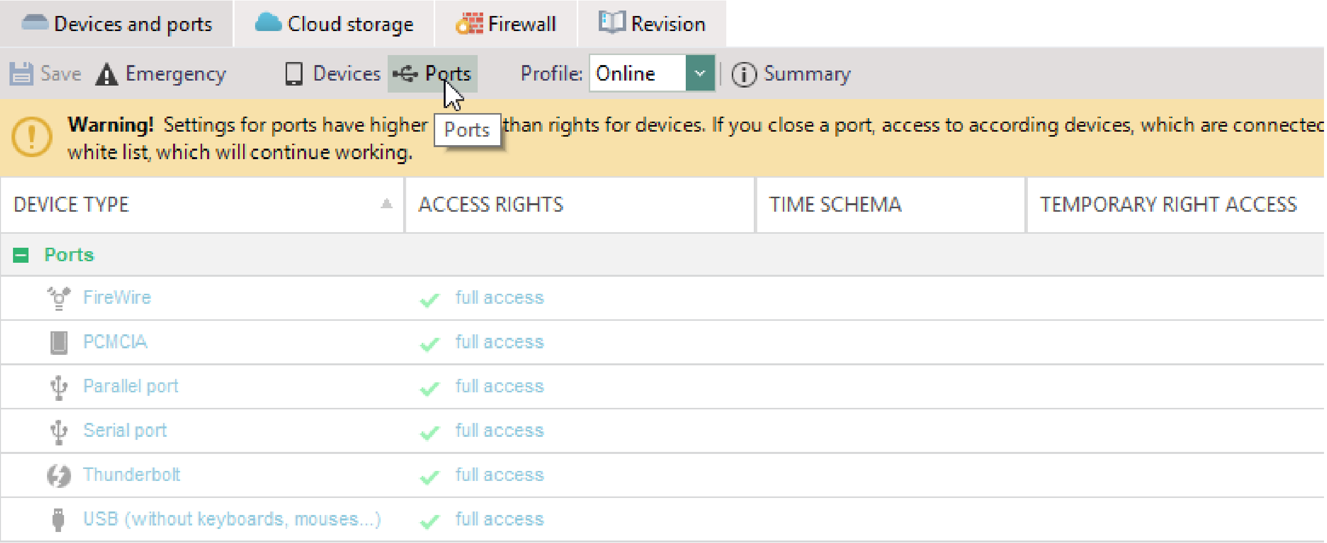
Online and offline mode

If you make the changes for an online profile, these changes are inherited to an offline profile. Once you make changes to the offline profile, different sets of rights are applied. If necessary, adjust access rights for the offline profile too.

Configuring access to ports

1. Go to **User management/Computer management | Control**.

2. Select a user or a computer in the **User management**/**Computer management** work area.
3. In the lower section, click the **Devices and ports** tab.
4. Click **Ports** on the toolbar.



Profile: Online

Warning! Settings for ports have higher Ports than rights for devices. If you close a port, access to according devices, which are connectec white list, which will continue working.

DEVICE TYPE	ACCESS RIGHTS	TIME SCHEMA	TEMPORARY RIGHT ACCESS
Ports			
FireWire	✓ full access		
PCMCIA	✓ full access		
Parallel port	✓ full access		
Serial port	✓ full access		
Thunderbolt	✓ full access		
USB (without keyboards, mouses...)	✓ full access		

Figure 32. Configuring access to ports

5. Right-click a port and select an access type.
6. Click **Save**.

The selected access type applies to all not individually permitted devices connected to the configured port.

Granting temporary or scheduled access

Configuring one-time access

1. On the navigation pane, go to **User management/Computer management | Control**.
2. Select a user or a computer in the **User management** or **Computer management** work area.
3. In the lower section, click the **Devices and ports** tab.
4. Right-click a device and a port and select **Temporary right access**.

   → The **Temporary right access** dialog appears.

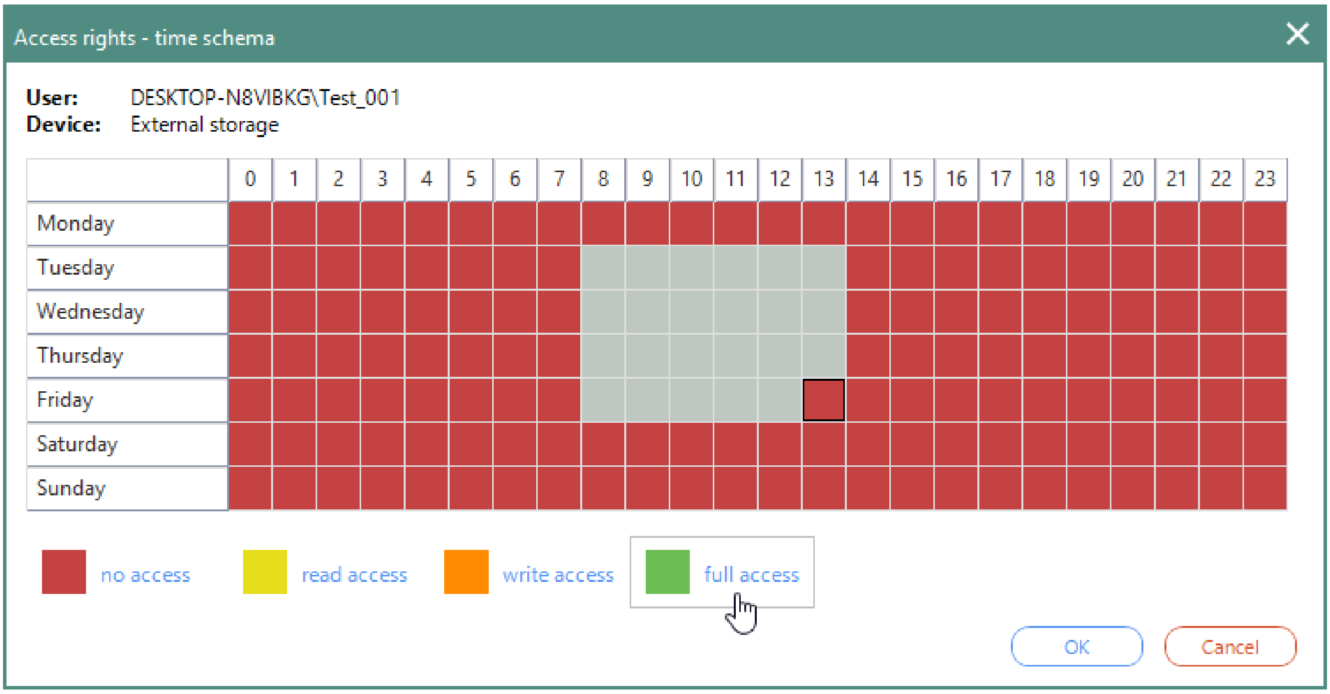
5. Select an access type and define a time period.
6. Click **OK** to confirm.
7. In the **Device and ports** tab, click **Save**.

Configuring scheduled access

1. Right-click a device or a port and select **Scheduled access**.

   → The **Access rights – time schema** dialog appears.

2. Click and drag to select a time period.
3. Select an access type.



Access rights - time schema

User: DESKTOP-N8VIBKG\Test_001
Device: External storage

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	⬜	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

🟥 no access 🟨 read access 🟧 write access 🟩 full access

Figure 33. Full access on external storage on Tuesday-Friday, 8.00 - 13.00

4. Click **OK** to confirm.
5. Click **Save** in the **Devices and ports** tab.

Blocking all devices (emergency)

You can block access to all devices and ports in case of emergency with one click.

Blocking all user/computer accesses

1. Go to **User management/Computer management | Control**, select a user or a computer in the **User management/Computer management** work area.
2. In the lower section, go to **Devices and ports** tab.
3. Click **Emergency** on the toolbar.
4. Click **OK** in the dialog.

➥ The user/computer permissions are now set to **No access** for all devices and ports. **No access** is not applied for network share, thin client storage and local printers device types if their control is disabled under **Computer management | Settings | Client settings**. For such device types enable the control and then apply **no access** manually.

3.3. Restricting or granting access to known devices

Via **User management** and **Computer management**, you can assign access rights for device classes and port types on the whole. This means that all device models of this device class (or all ports of this type) can be used. You can limit the usage of specific device models globally.
You can also assign individual rights for specific device models to certain users or computers.

Restricting access globally to device models

To globally limit the usage of specific device models, add them to permitted device models. Not listed device models are globally forbidden (exception: User-specific known devices).
Under **Permitted device models** you can add all devices ever connected to Clients.

Access rights for devices from permitted device models

Permitted device models have access rights assigned to a device class. E.g.: flash card **SMI USB DISK Device** has read access, because under **Computer management | Control | Devices and ports**, **read access** is assigned to the **external storage** device class.

Creating a list of permitted device models

1. Go to **Permitted devices | Removable devices | Permitted device models**.
2. To search on a computer for devices, which are currently connected or have been connected:
   a. Select a computer in the **List of EgoSecure Agents** work area. To multi-select computers, hold-down `Ctrl` and click.
   b. In the **Permitted device models** area, click **Scan computer**.

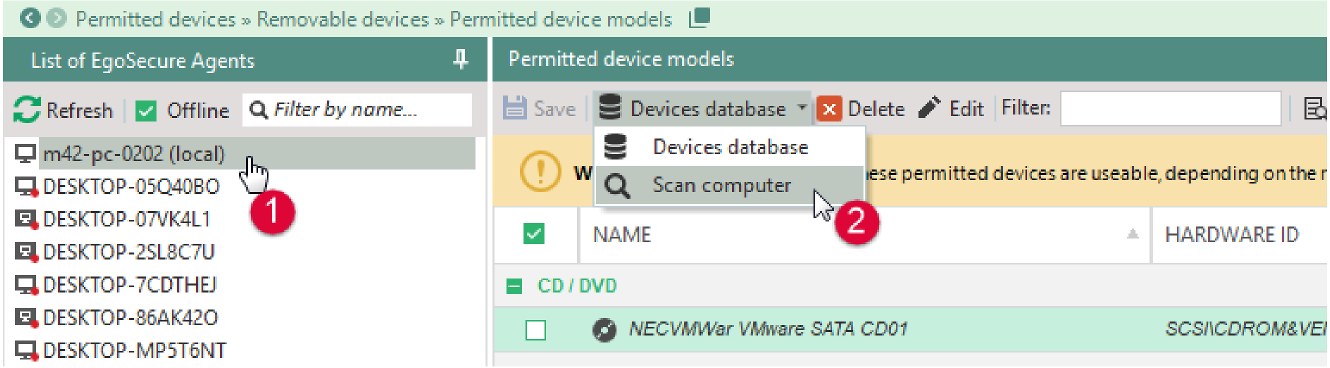
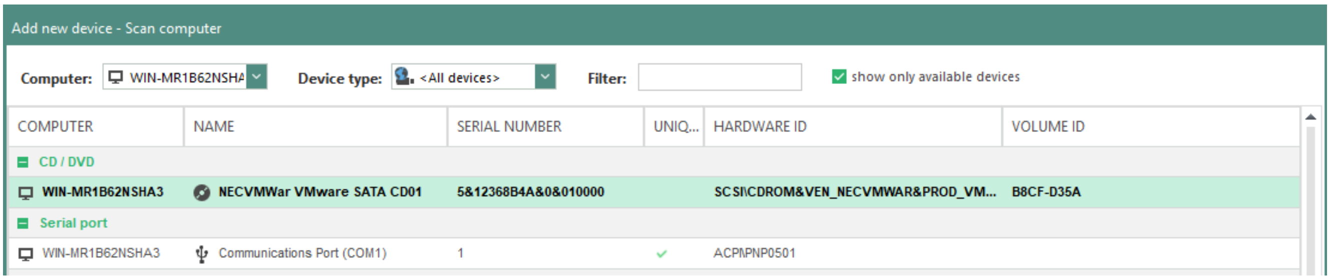


Figure 34. Scanning computer for device and port models (global list)

→ The **Add new device – Scan computer** dialog appears. Devices already added to the list of permitted ones are highlighted with bold, devices which were disconnected have a red icon.



Add new device - Scan computer

Computer: WIN-MR1B62NSHA Device type: <All devices> Filter: ☑ show only available devices

COMPUTER	NAME	SERIAL NUMBER	UNIQ...	HARDWARE ID	VOLUME ID
CD / DVD					
WIN-MR1B62NSHA3	NECVMWar VMware SATA CD01	5&12368B4A&0&010000		SCSI\CDROM&VEN_NECVMWAR&PROD_VM...	B8CF-D35A
Serial port					
WIN-MR1B62NSHA3	Communications Port (COM1)	1	✓	ACPI\PNP0501	

Figure 35. Adding device to permitted device models via computer scan

c. To hide unconnected devices, enable **Show only available devices**.
d. Select a device or a port from the list. To multi-select, hold-down `Ctrl` and click.
e. Click **Add**.

→ The dialog closes. The device is added to the list of permitted ones.

-or-

f. In the **Add new device – Scan computer** dialog, select the added device and click **Update** to close the dialog and update the device info.

3. To search the database for devices, which are currently connected or have been connected to network computers,
   a. In the **Permitted device models** area, select **Devices database**.

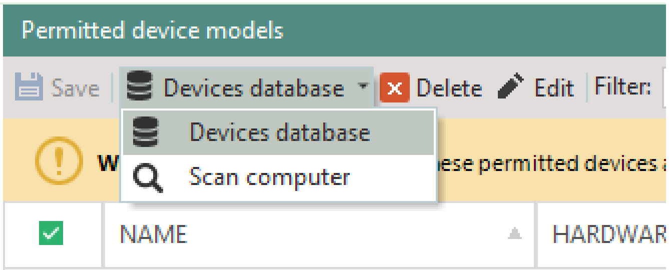


Figure 36. Searching database for previously connected devices

→ The **Add new device – Devices database** dialog appears.

INFO

Searching for devices in a database

You can search for devices on certain clients or in the database. To write data to a device database, enable the **Accept data for devices DB** option in the **AdminTool**.

b. In the **Computer** drop-down, select computers to see the list of devices on the selected computers.
Select **<All>** to see the list of devices on all computers of the directory.
c. Select a device. To multiselect, hold down `Ctrl` and click.
d. Click **Add**.

→ The dialog closes. The device is added to the list of permitted ones.

4. Click **Save**.

➥ The white list of device models is applied to all Agents of a company where **Access Control** is activated. Not listed device models are blocked.

Allowing user-specific or computer-specific known devices

In individual device permissions, you can specify the devices that a user/computer is allowed to use regardless of the list of permitted device models and the access rights for device types. Individual access rights also apply if access to the device type is not permitted for the user/computer (defined under **User management/Computer management | Control | Devices and ports**) or the device model is globally locked (defined under **Permitted devices | Permitted device models**).

What is more, you can allow certain devices to be used only on certain computers.

When allowing a device individually, select the criteria according to which the device is identified.

WARNING

Avoiding system conflicts

To avoid system conflicts, do not add one device with different criteria to the list.

You can use wildcards in the **Hardware ID**, **Serial number** and **Name** fields. These fields are case-sensitive.

Criteria

Criteria	Description
Hardware ID + serial number	Combination of Hardware ID and serial number (default). Serial number is not always the same. If a serial number is unique, the checkmark is displayed in the **Unique** column. You can use wildcards (e.g.: if you use devices with consecutive serial numbers): * replaces any number of characters ? replaces a single character
Hardware ID	Unique ID of a specific device model/port. Remains unchanged when connecting to different devices.
Volume ID	Windows unique ID created when formatting a drive.
Device + Volume ID	Combination of Hardware ID, serial number und volume ID. For Hardware ID and serial number, you can use wildcards: * replaces any number of characters ? replaces a single character

Name	Windows device name. To view the device name in Windows Explorer: right-click a device, click **Properties** button in the **Hardware** tab. Remains unchanged when connecting to different devices. You can use wildcards: * replaces any number of characters ? replaces a single character

Allowing device for user

1. Go to **Permitted devices | Removable devices | Individual device permissions**.
2. To search on a computer for devices, which are currently connected or have been connected:
   a. Select a computer in the **List of EgoSecure agents** work area. To multi-select, hold-down `Ctrl` and click.
   b. In the **Individual device permissions** area, click **Scan computer**.

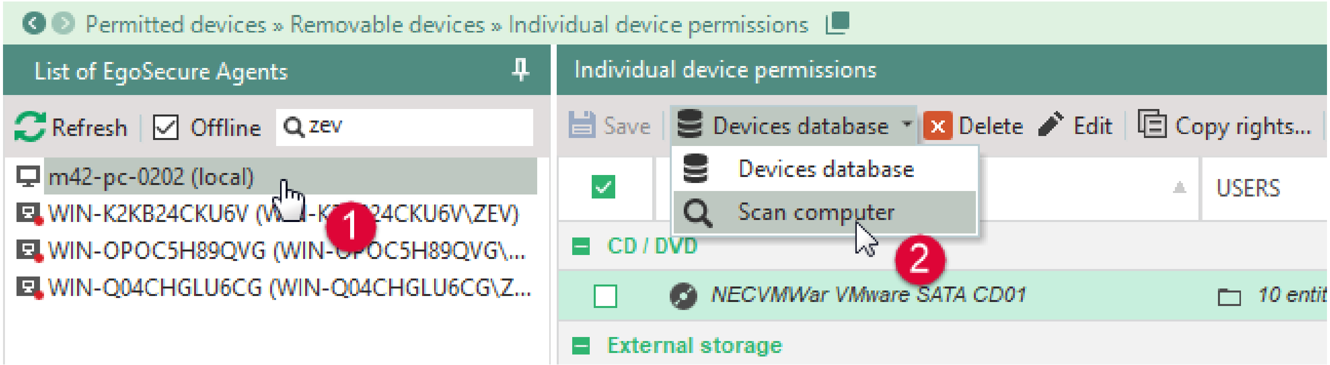

Permitted devices » Removable devices » Individual device permissions
List of EgoSecure Agents
Refresh
☑ Offline
zev
m42-pc-0202 (local)
WIN-K2KB24CKU6V (WIN-K2KB24CKU6V\ZEV)
WIN-OPOC5H89QVG (WIN-OPOC5H89QVG\...
WIN-Q04CHGLU6CG (WIN-Q04CHGLU6CG\Z...
1
Individual device permissions
Save
Devices database
Delete
Edit
Copy rights...
Devices database
Scan computer
2
USERS
CD / DVD
NECVMWar VMware SATA CD01
10 entit
External storage

Figure 37. Scanning computer for device and port models (individual list)

→ The **Add new device – Scan computer** dialog appears. Devices already added to the list of permitted ones are highlighted with bold, devices which were disconnected have a red icon.

   c. To hide unconnected devices, enable **Show only available devices**.
   d. Select a device or a port from the list. To multi-select, hold-down `Ctrl` and click.
   e. Under **Allow by criteria**, select according to which criteria the device is identified.
   f. Click **Add**.

→ The dialog closes. The device is added to the list of permitted ones.

-or-

   g. In the **Add new device – Scan computer** dialog, select the added device and click **Update** to close the dialog and update the device info.
3. To search the database for devices, which are currently connected or have been connected to network computers,
   a. In the **Individual device permissions** area, select **Devices database**.

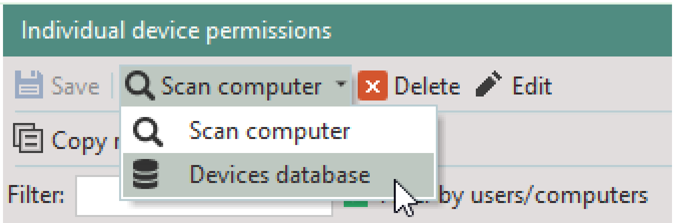


Figure 38. Searching database for previously connected devices

→ The **Add new device – Devices database** dialog appears.

INFO	**Searching for devices in a database** You can search for devices on certain clients or in the database. To write data to a device database, enable the **Accept data for devices DB** option in the **AdminTool.**

b. In the **Computer** drop-down, select computers to see the list of devices on selected computer.
Select **<All>** to see the list of devices on all computers of the directory.

c. Select a device. To multiselect, hold down `Ctrl` and click.
In the **Last used** column, the information about the last connection of a device to a computer is displayed.

d. Under **Allow by criteria**, select according to which criteria the device is identified.

e. Click **Add**.

→ The dialog closes. The device is added to the list of permitted ones.

4. Configure the individual rights for the device:
   - Allow a device to all users on a certain computer,
   - Allow a device for certain users on all computers or
   - Allow a device for certain users on certain computers.

Allowing a device to all users on a certain computer

1. Select the device in the list.
2. In the lower area, click **Add** in the **Computers** tab.

   → The **Selection of computers** dialog appears.

3. Select a computer and click **OK**.

   → The **Selection of computers** dialog closes. The computer appears in the **Computers** tab. In the **Users** tab, **<All users>** are listed (default).

4. If necessary, define other settings for using a device in the lower area.
5. Click **Save**.

All users are allowed to use this device on a selected computer. **Access Control** product activation is not required.

Allowing a device for certain users on all computers

1. Select the device in the list.
2. In the lower area, click **Add** in the **Users** tab.

   → The **Selection of users** dialog appears.
3. Select a user and click **OK**.

   → The **Selection of users** dialog closes. The user appears in the **Users** tab. In the **Computers** tab, **<All computers>** are listed (default).
4. If necessary, define other settings for using a device in the lower area.
5. Click **Save**.

The user is allowed to use this device on all computers. For the rights to apply, **Access Control** must be activated for a user and not activated for a computer.

Allowing a device for certain users on certain computers

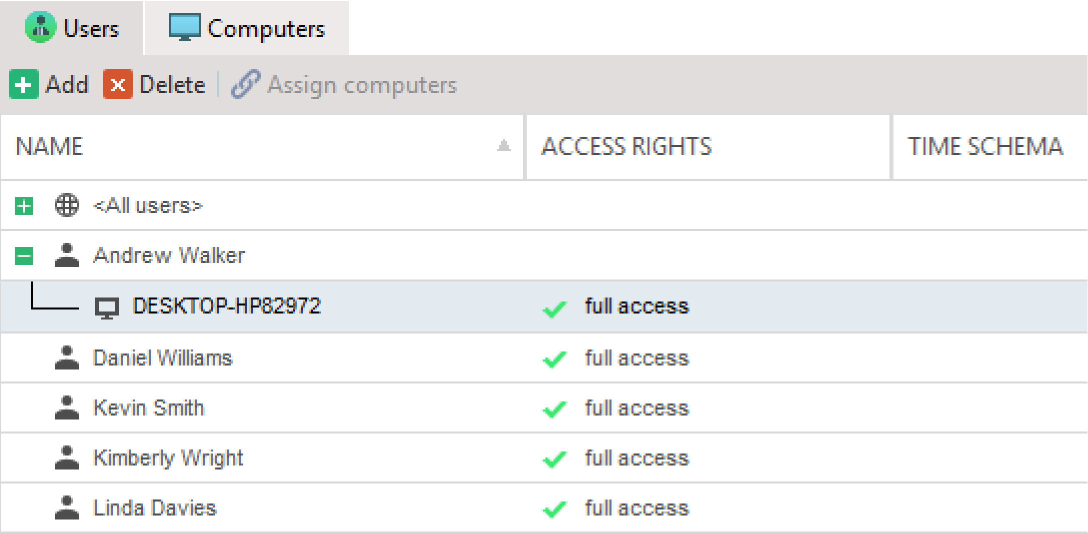
1. Select the device in the list.
2. In the lower area, click **Add** in the **Users** tab.

   → The **Selection of users** dialog appears.
3. Select a user and click **OK**.

   → The **Selection of users** dialog closes. The users appear in the **Users** tab.
4. Click **Assign computers** button.

   → The **Selection of computers** dialog appears.
5. Select a computer and click **OK**.

   → The dialog closes and a computer appears under a user.



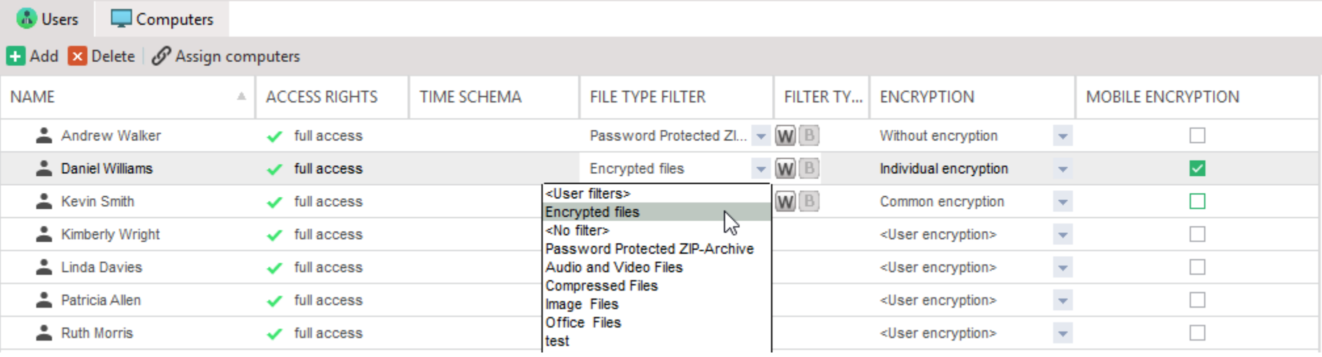
NAME	ACCESS RIGHTS	TIME SCHEMA
<All users>		
Andrew Walker		
DESKTOP-HP82972	✓ full access	
Daniel Williams	✓ full access	
Kevin Smith	✓ full access	
Kimberly Wright	✓ full access	
Linda Davies	✓ full access	

Figure 39. User-specific individual device permissions

6. If necessary, define other settings for using a device in the lower area.
7. Click **Save**.

The user is allowed to use this device only on the selected computer. For the rights to apply, **Access Control** must be activated for a user and not activated for a computer.

Defining other settings for using a device



NAME	ACCESS RIGHTS	TIME SCHEMA	FILE TYPE FILTER	FILTER TY...	ENCRYPTION	MOBILE ENCRYPTION
Andrew Walker	✓ full access		Password Protected ZI...	W B	Without encryption	□
Daniel Williams	✓ full access		Encrypted files	W B	Individual encryption	☑
Kevin Smith	✓ full access			W B	Common encryption	□
Kimberly Wright	✓ full access				<User encryption>	□
Linda Davies	✓ full access				<User encryption>	□
Patricia Allen	✓ full access				<User encryption>	□
Ruth Morris	✓ full access				<User encryption>	□

Figure 40. Applying other settings for using a device

1. **Access rights**: To change the access type for the devices (irrespective of the access rights specified under **User management** and **Computer management**), click the entry in the **Access rights** column. If you define a scheduled access right, the time scheme appears in the **Time schema** column.
   The individual access rights apply to a user only if **Access Control** is deactivated for a computer.
2. **File type filter**: Select which filters to apply when using this device. For details, see: Filters
   a. **<User filters>**: applies the filters assigned to user/computer in **User management/Computer management**.
   b. **<No filter>**: disables filters assigned to the user/computer (only for this device).
   c. **[Filter name]**: offers all available filters for selection.
3. **Filter type**: defines a mode for the selected filter:
   a. Click W for the **Whitelist** mode.
   b. Click B for the **Blacklist** mode.
4. **Encryption**: select an encryption type for a user (computer) exclusively on this device or allow to use this device without encryption:
   a. **<User encryption>**: applies the encryption types assigned to user/computer in **User management/Computer management**.
   b. **<Without encryption>**: allows a user/computer to use a device without encryption.
   c. **[Encryption type]**: offers all available encryption types for selection.
   Note: The selected encryption type must be assigned to the user/computer and an encryption product must be activated for the user/computer.

5. **Mobile encryption**: enable the check box to permit the adding of a mobile key for encryption.
   Note: The mobile encryption can not be activated if **<User encryption>** is selected in the previous step. Make sure to enable the mobile encryption for the user/computer; the user/computer must create a mobile key.

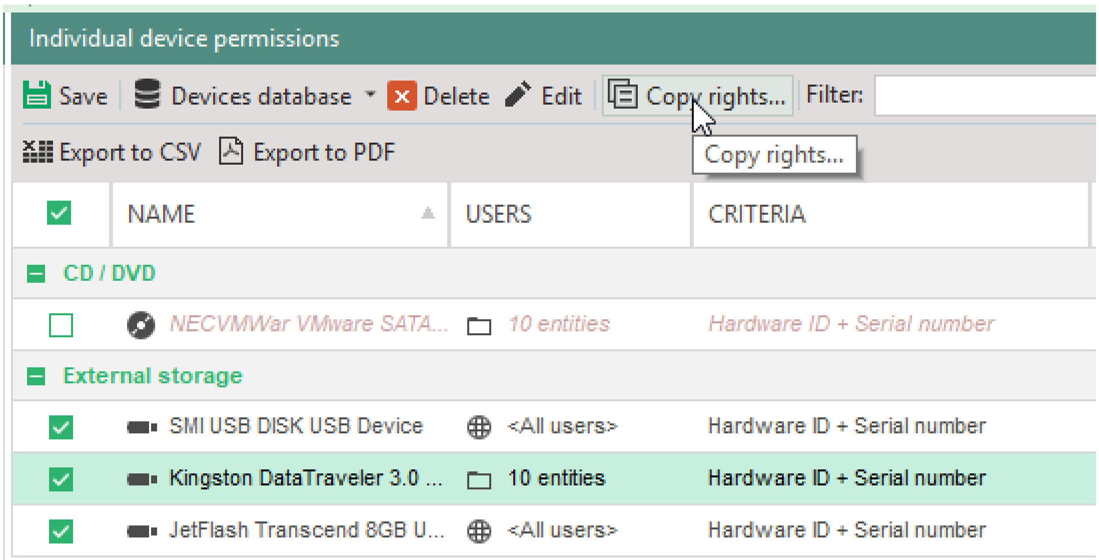
ATTENTION	**Process encryption type priority** Encryption type selected for a process has priority over encryption type selected for a device. *E.g.:* For the **notepad.exe** process the individual encryption is selected and for a device the group encryption type is selected. Once a text file is copied to the device, it is encrypted with the group encryption type. Once the text file is edited with the notepad, it is reencrypted with the individual type.

6. Click **Save**.

➜ Individual access permissions for one device are assigned. To assign the same access permissions to other devices, use the **Copy rights** button.

Copying usage settings

1. Select the device (where the rights are copied to) from the list.
2. Click the **Copy rights** button.



☑	NAME	USERS	CRITERIA
CD / DVD			
□	NECVMWar VMware SATA...	10 entities	Hardware ID + Serial number
External storage			
☑	SMI USB DISK USB Device	<All users>	Hardware ID + Serial number
☑	Kingston DataTraveler 3.0 ...	10 entities	Hardware ID + Serial number
☑	JetFlash Transcend 8GB U...	<All users>	Hardware ID + Serial number

Figure 41.Transferring the rights of another device for USB stick

→ The **Copy rights** dialog appears.

3. Select the device from where to copy the rights.
4. Select one of the options for copying rights:

- **Overwrite** to delete old rights and assign new ones.
- **Append** to add new rights in addition to the existing ones.

5. Click **OK** to confirm.

➥ The rights apply for the selected device.

3.4. Media permissions: allowing known optical storage media

Via media permissions, define CDs and DVDs, access to which is globally or user-specifically allowed. The access rights apply even if a user/computer is not permitted to access the CD/DVD device class (defined under **User management**/ **Computer management | Control | Devices and ports**).
Pay attention that **Media permissions** have priority over access rights for CD/DVD-ROMs (defined under **User management**/**Computer management | Devices and ports** and under **Permitted devices | Individual device permissions**).

ATTENTION	**Permission update required for changed data** EgoSecure calculates and stores a unique string (hash value) for each permitted media to identify it. The calculation is based on the media data. Once the data changes or new files are written to the media, the hash value changes and media permissions must be redefined.

Allowing CD or DVD

1. Go to **Permitted devices | Removable devices | Media permissions**.
2. In the **List of EgoSecure agents** work area, select a computer where a disk is currently connected. To multi-select computers, hold-down `Ctrl` and click.
3. Click **Scan computer**. The **Device database** option is not available, because disks can be added to the list only when they are connected at the moment of adding.

   → The **Add new device – Scan computer** dialog appears.

4. Select the CD/DVD and click **Add**.

   → The media appears in the list with the checked box.

5. Select the disk and define computer and user permissions for using this disk:
   a. In the lower area, click **Add**.
   b. In the **Selection of users**/**Selection of computers** dialog, select a user/computer.
   c. Click **OK** to confirm.

   → The user/computer appears in the lower area.

6. Click the entry in the **Access rights** column to specify access rights:
   a. **Full access**: Reading and writing allowed. Warning: Changing the data requires to redefine the permissions.

   b. **Write access**: Only writing allowed. Warning: Changing the data requires to redefine the permissions.
   c. **Read access**: Only reading allowed.
   d. **Scheduled access**: Opens the **Access rights – time schema** dialog, where you specify a time period for permissions.
7. Click **Save**.

To transfer the defined access rights to other optical storage media, use the **Copy rights** button. For details, see: Copying usage settings

3.5. Granting user requested access rights

Online Clients

Via the **Access request** tab, a user can request specific access rights for one or more device types.
The following access rights are available depending on a device type:

- Not controlled (**EgoSecure** doesn’t control a selected device)
- Read access (only storage media)
- Print access (only locally connected printers)
- Full access
- Playback access (only sound, video and game controllers)

Once the requested rights reach the Server, they appear under **Administration | Administrator | Access rights requests**.

Granting access to a device type

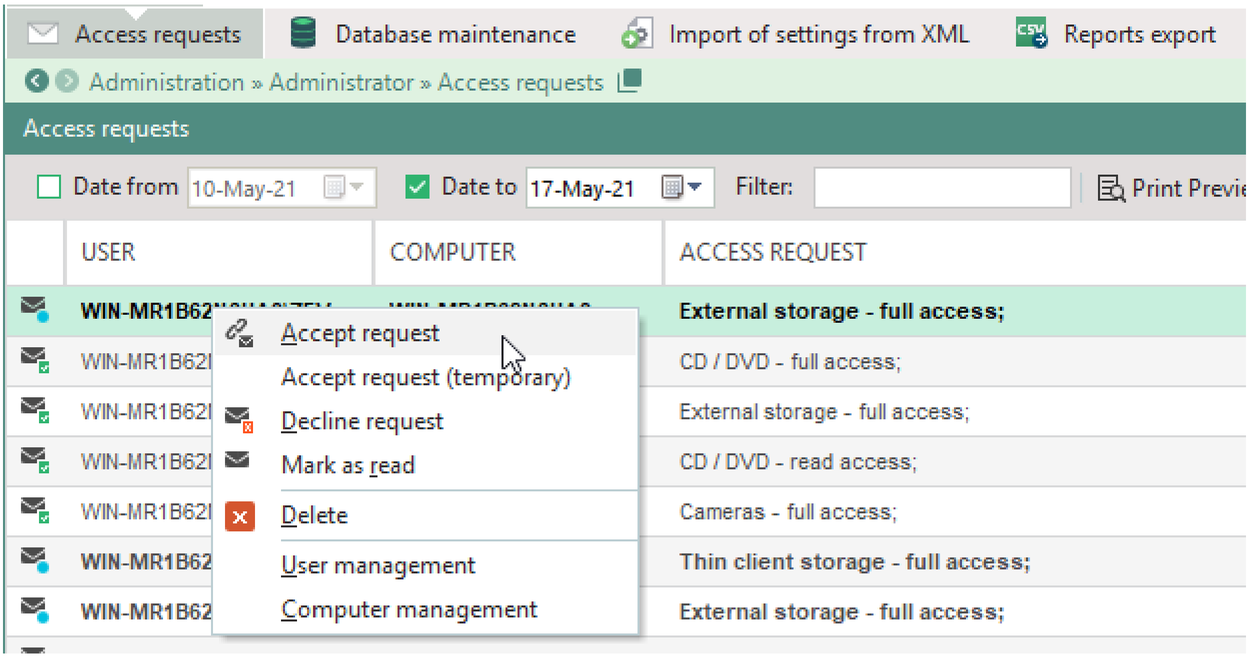
! To allow users to request access rights via EgoSecure Agent, enable the **Allow requests for access rights** option under **Administration | Clients | Client settings**.

1. In Console, go to **Administration | Administrator | Access rights requests**.

   → All received requests are displayed. Unprocessed requests are highlighted in bold.

2. Right-click an access rights request and select in the context menu:
   a. **Accept request**, to permit requested rights. The rights are changed automatically, the user receives a notification. Message text can be customized, for details, see: Customizing user messages.
   b. **Accept request (temporary)**, to grant the access right only for a certain time period. The user receives the same notification as for **Accept request**.
   c. **Decline request**, to decline requested access rights. The user receives notification, message text can be customized, for details, see: Customizing user messages.
   d. **Mark as read/unread**, to mark notifications for the reasons of convenience. No changes are made in user rights as a result.

e. **Delete**, to remove the notification from the list.
f. **User management**, to go to the user entry in **User management** and see the list of permissions and assign access rights manually, if necessary.
g. **Computer management**, to go to the computer entry in **Computer management** and see the list of permissions and assign access rights manually, if necessary.



□ Date from 10-May-21 ☑ Date to 17-May-21 Filter:

USER	COMPUTER	ACCESS REQUEST
WIN-MR1B62		**External storage - full access;**
WIN-MR1B62		CD / DVD - full access;
WIN-MR1B62		External storage - full access;
WIN-MR1B62		CD / DVD - read access;
WIN-MR1B62		Cameras - full access;
WIN-MR1B62		**Thin client storage - full access;**
WIN-MR1B62		**External storage - full access;**

Figure 42. Allowing requested rights

The access for the device remains except the case when you assign a temporary access right.

The access to certain device models on the Client can be changed via the Challenge-response procedure. For details, see: Allowing connected devices via unblocking code

Offline Clients

When the Agent is offline (no connection between Agent and Server), the settings defined for the offline profile apply. For details, see: Configuring offline profile
Changes to offline permissions take effect when Agent becomes online.

To apply the changes of rights and settings on offline Agents, use an unblocking code or import a file with settings.

- Exporting the whole user permission profile to a file
- Granting access to known devices via the Challenge-response procedure
- Granting access to a device type via an unblocking code

Exporting permission profile

You can export the following settings:

Setting	Definition in Console	Display on Agent
Access rights	**User management/Computer management | Control | Devices and ports** tab	**Access Control | User rights**
Permitted device models	**Permitted devices | Removable devices | Individual device permissions; Permitted device models; Media permissions**	**Access Control | Connected devices**
Encryption settings	Permitted encryption products and available encryption types are assigned under **User management/Computer management | Encryption**	**Encryption**
Export public keys only	Permitting only common encryption type and export the associated key	**Encryption | Encryption keys**

Exporting permission profile

1. Select a user in the **User management** work area.
2. Define access rights, permitted devices and encryption settings.
3. Right-click the user and select **Export settings** from the context menu.

   → A dialog for selecting the settings appears.

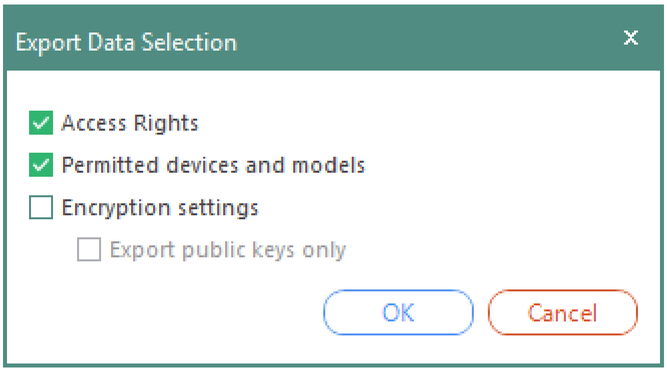


Figure 43. Selecting export settings

4. Select the settings for the export and click **OK** to confirm.

   → The **Save as** dialog appears.

5. Save the **.esd** file with the settings and send it to the user (e.g. by e-mail).

Via **EgoSecure Agent** the user can now import the file and receive the settings:

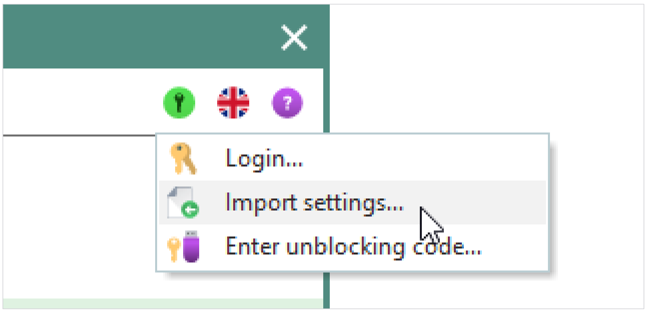
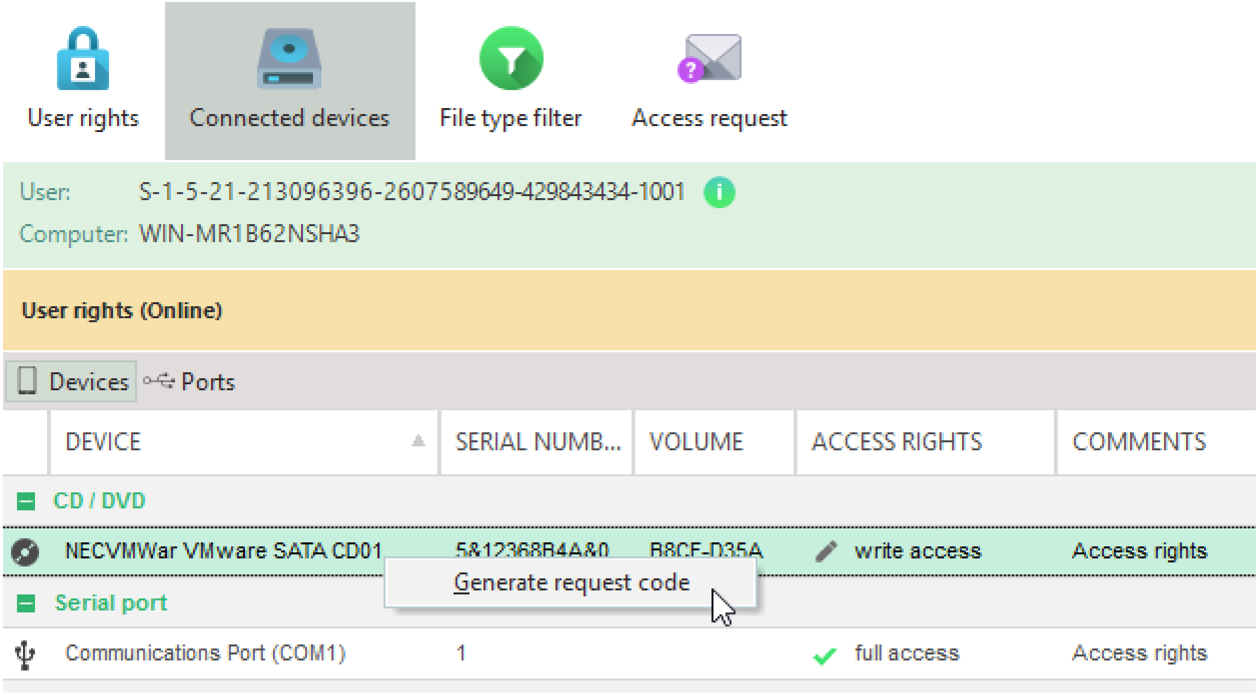


Figure 44. EgoSecure Agent: importing settings

Allowing connected devices via unblocking code

If a user wants to use a connected device for which he doesn't have access, he can request access rights only for the device. The user generates a request code and sends it to the administrator.



User: S-1-5-21-213096396-2607589649-429843434-1001

Computer: WIN-MR1B62NSHA3

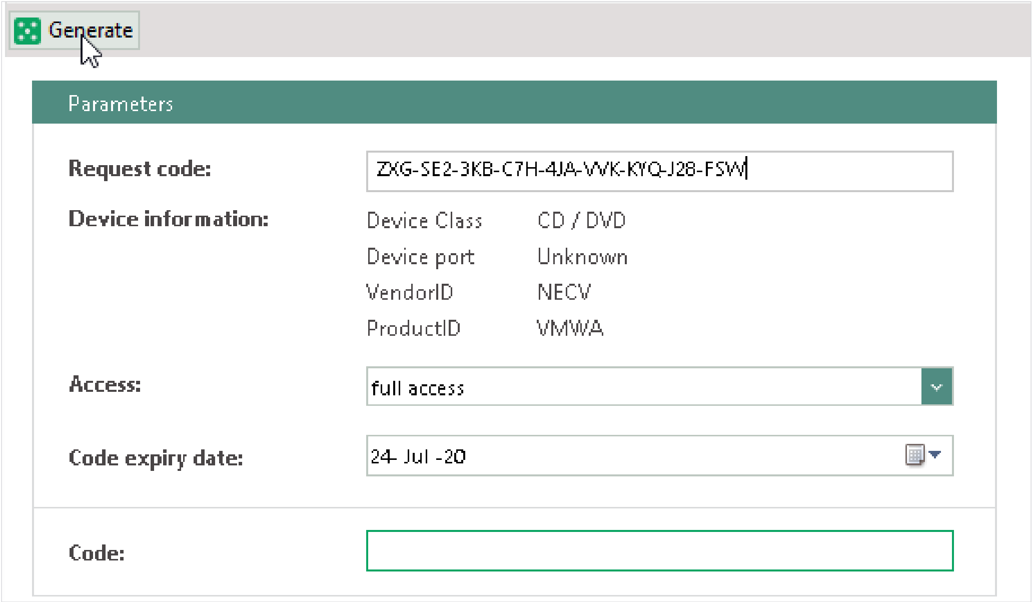
User rights (Online)

DEVICE	SERIAL NUMB...	VOLUME	ACCESS RIGHTS	COMMENTS
CD / DVD				
NECVMWar VMware SATA CD01	5&12368B4A&0	B8CF-D35A	write access	Access rights
Serial port				
Communications Port (COM1)	1		✓ full access	Access rights

Figure 45. EgoSecure Agent: generating request code

Generating a response code via Challenge-response

1. In Console, go to **Permitted devices | Challenge-response unblocking code**.
2. Enter the code that a user generated and provided.
3. If necessary, edit an access right in the **Access** drop-down.
4. In the **Code expiry date** field, select till what date the code is valid.
5. Click **Generate**.



Request code: ZXG-SE2-3KB-C7H-4JA-VVK-KYQ-J28-FSW

Device information:

Device Class	CD / DVD
Device port	Unknown
VendorID	NECV
ProductID	VMWA

Access: full access

Code expiry date: 24-Jul-20

Code:

Figure 46. Entering request code and generating response code

→ The generated code appears in the **Code** field. The code can be used several times till its expiration date.

6. Send the code to the user.

Via **EgoSecure Agent** the user can now enter the code and receive access rights:

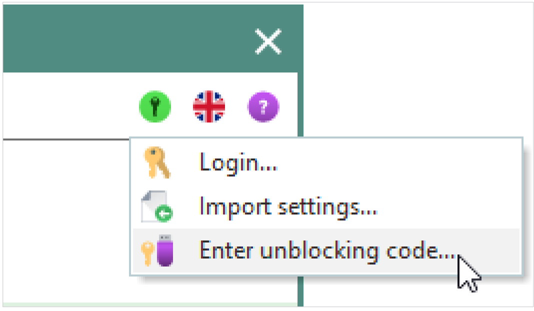


Figure 47. EgoSecure Agent: entering unblocking code

Once the connection between Agent and Server is established, an administrator is informed about the code activation under **Reports | Control | Unblocking codes review**.
New code doesn’t replace the previous one.

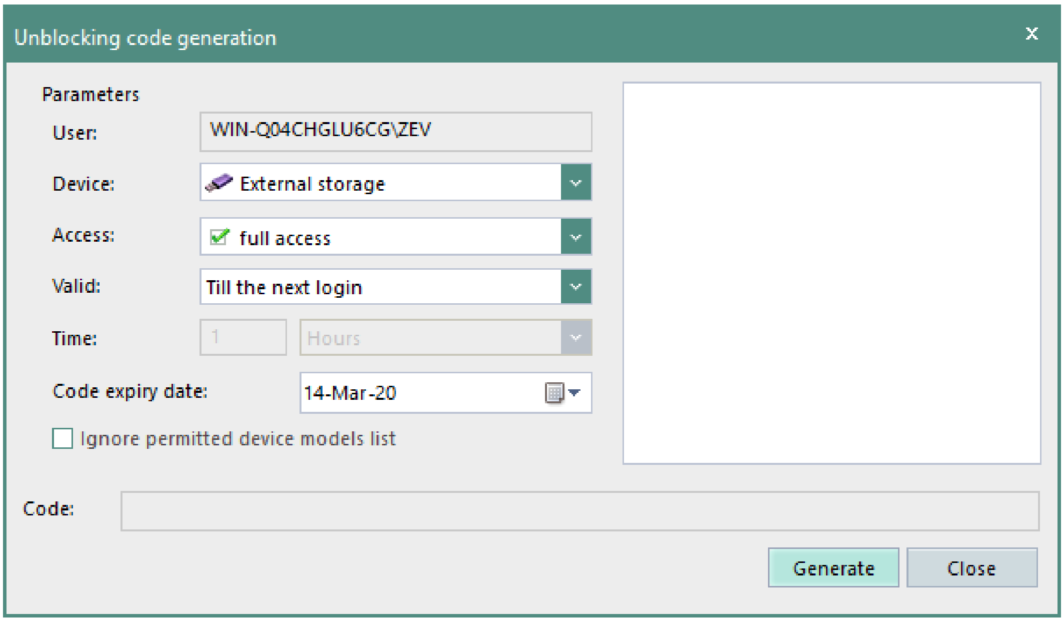
Granting access to a device type via unblocking code

You can grant access rights to certain device types via an unblocking code.

Generating unblocking code

1. Right-click a device class and select **Generate unblocking code...**.

→ The **Unblocking code generation** dialog appears.


Unblocking code generation

Parameters

User: WIN-Q04CHGLU6CG\ZEV

Device: External storage

Access: full access

Valid: Till the next login

Time: 1 Hours

Code expiry date: 14-Mar-20

☐ Ignore permitted device models list

Code:

Figure 48. Generating unblocking code

2. Select an access type and access period.
3. Change the code expiry date, if necessary.
4. Check the **Ignore permitted device models list** option, if a user needs a device not included in the list under **Permitted devices | Permitted device models**.
5. Click **Generate**.

   → The generated code appears in the **Code** field.

6. Copy the code and send it to the Client (e.g. by e-mail).

Via **EgoSecure Agent** the user can now enter the code and receive access rights:

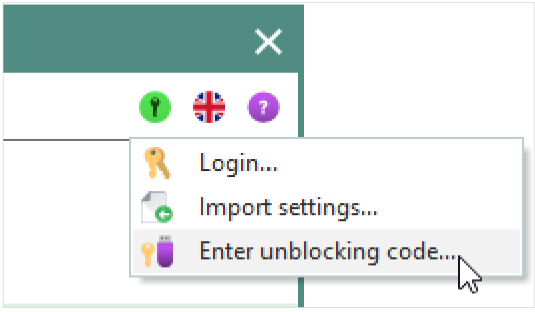


Figure 49. EgoSecure Agent: entering unblocking code

Once the connection between Agent and Server is established, an administrator is informed about code activation under **Reports | Control | Unblocking codes review**.
New code doesn’t replace the previous one.

3.6. Assigning different user rights for specific computers

! The product must be activated only for the user and not for the assigned computer. If a product is activated for the computer, computer rights take effect.

1. Right-click a user in the **User management** work area.
2. Select **Assign computers** from the context menu.

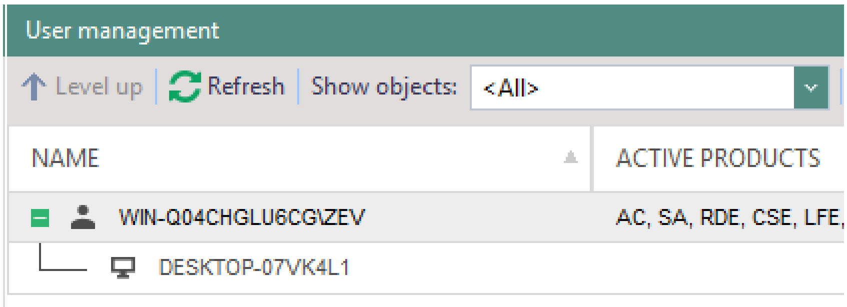
   → The **Selection of computers** dialog opens.

3. Select a computer from the directory service structure and click >.

   → The computer appears under **Selected computers**.

4. Click **OK** to confirm.

   → The computer appears under the user.



NAME	ACTIVE PRODUCTS
WIN-Q04CHGLU6CG\ZEV	AC, SA, RDE, CSE, LFE,
DESKTOP-07VK4L1	

Figure 50. User with assigned computer

5. Click on the computer and edit the user-specific permissions on this computer in the lower area. For details, see: Controlling access
6. Click **Save**.

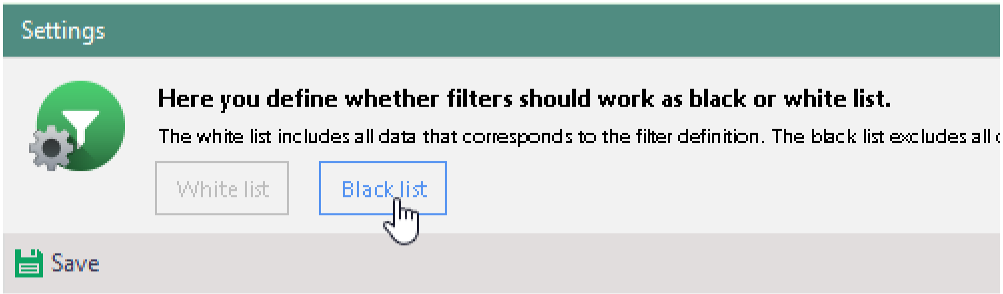
The user receives one set of access rights on the assigned computer and the other set of rights on other computers.

3.7. Filters: controlling access to the file formats

Via filters, define file formats that a user is allowed or not allowed to access on devices, network shares or in clouds. Specify either the access is allowed to all filtered file types (white list) or forbidden to all filtered file types (black list).

Specifying filter mode

1. Go to **Product settings | Filters | Settings**.
2. Click on
   a. **White list**, to allow only the file types that match the filter settings. All other file types are blocked.
   b. **Black list**, to forbid file types that match the filter settings. All other file types are allowed.



Here you define whether filters should work as black or white list.

The white list includes all data that corresponds to the filter definition. The black list excludes all

Figure 51. Applying setting for file type filter

3. To additionally scan archives and office files for allowed/blocked file types, enable the **In archives** or **In files of Microsoft Office** check boxes under **Scan embedded files**.

→ The options can now be activated for the default user under **User management | Default policies | Default rights (user)**. The inheritance of the options can be deactivated individually for a user.

4. Click **Save**.

✓ The specified filter mode applies to all filters assigned to users.

Creating filters

1. Go to **Product settings | Filters | File type filters**.

   → In the **File type filters** area, you can see the predefined filters for audio/video files, compressed files, image files and office files.

2. Click **Add**.

   → A new entry appears in the list.

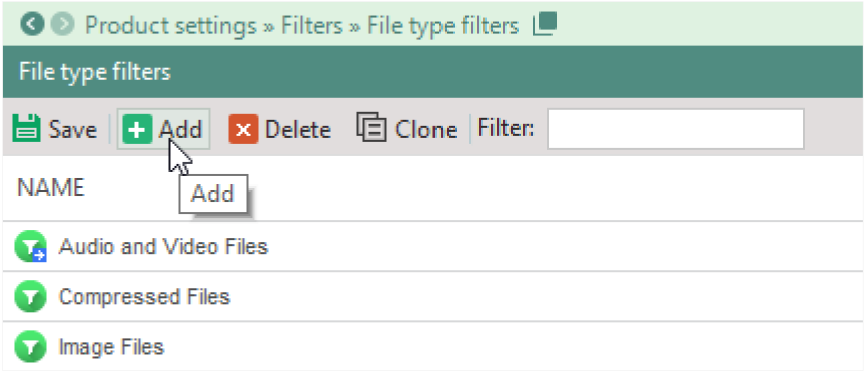


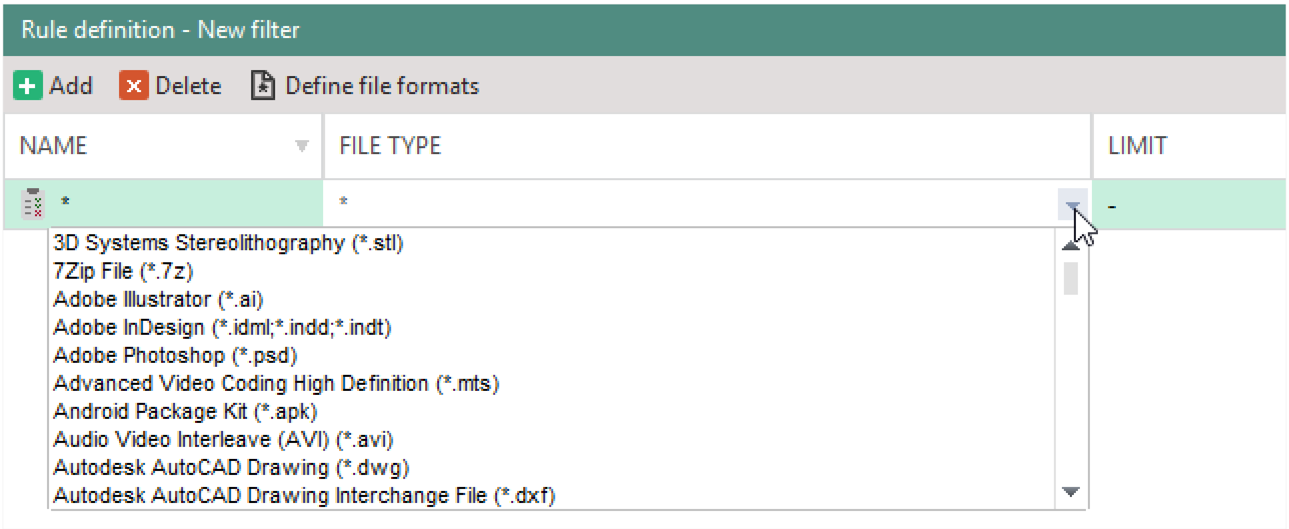
Figure 52. Adding new filter

3. Enter a filter name.
4. To assign the filter to all users where **Access Control** is activated, enable the **Global** check box. Global filters unlike inherited filters cannot be disabled individually.
5. In the **Rule definition** area, click **Add**.
6. Specify the rules. You can use wildcards (placeholders) for file names and formats:

   * replaces any number of characters

   ? replaces a single character

   a. Define a specific file name in the **Name** column.
   b. In the **File type** column, select a file format from the drop-down list
      or
      double-click on the field and enter a file extension. E.g.: *jpg* filters all jpg files, *jp** filters *jpeg* and *jpg*



NAME	FILE TYPE	LIMIT
*	*	-

3D Systems Stereolithography (*.stl)
7Zip File (*.7z)
Adobe Illustrator (*.ai)
Adobe InDesign (*.idml;*.indd;*.indt)
Adobe Photoshop (*.psd)
Advanced Video Coding High Definition (*.mts)
Android Package Kit (*.apk)
Audio Video Interleave (AVI) (*.avi)
Autodesk AutoCAD Drawing (*.dwg)
Autodesk AutoCAD Drawing Interchange File (*.dxf)

Figure 53. Defining filter rules

c. To specify a file size limit, double-click the entry in the **Limit** column. In the **File size** dialog, define the size of a file and click **OK**.
If you use a black list mode, all files whose size does not exceed the defined limit will be allowed.
If you use a white list mode, all files whose size exceeds the defined limit will be blocked.

7. Add other file formats, if necessary. For details about creating new file formats, see Defining file formats (advanced).
8. To copy a filter rule to another filter:
   a. Select a rule you want to copy. To select multiple rules, hold down `Ctrl` and click.
   b. Right-click a rule and select **Copy into...** from the context menu.
   → The **Select object** dialog appears.
   c. Select a filter where to copy the rule. To select multiple filters, hold down `Ctrl` and click.
   d. Click **Save** to confirm.
   → The rule is duplicated to another filter.
9. To move a filter rule to another filter:
   a. Select a rule you want to move. To select multiple rules, hold down `Ctrl` and click.
   b. Right-click a rule and select **Move into...** from the context menu.
   → The **Select object** dialog appears.
   c. Select a filter where to move the rule. To select multiple filters, hold down `Ctrl` and click.
   d. Click **Save** to confirm.
   → The rule is deleted from the current filter and assigned to the selected filter.

10.Click **Save**.

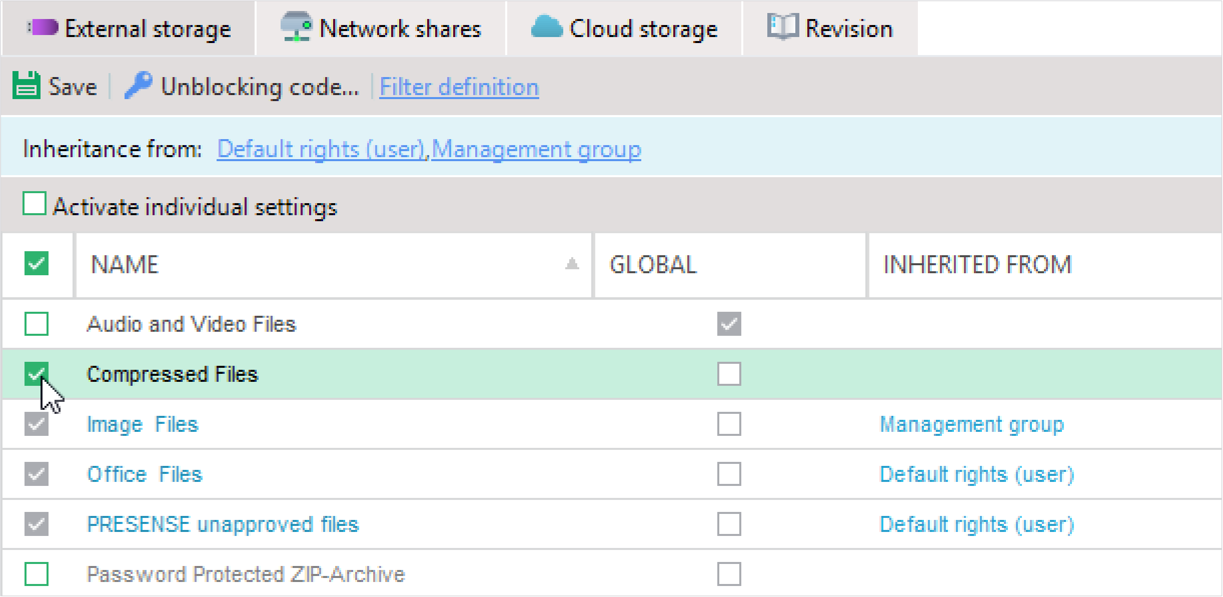
The new filter can now be assigned to users or groups.

Assigning filters

1. Go to **User management** and select a user.
2. Under **Filters**, select where a filter takes effect:
   - **External storage**
   - **Network shares** (including thin client storage if its control is enabled)
   - **Cloud storage**

ATTENTION	**File type filter in clouds: avoiding problems with OneDrive** - Disable the **Save space and download files as you use them** option.

3. Enable a filter.



Inheritance from: Default rights (user), Management group

□ Activate individual settings

☑	NAME	GLOBAL	INHERITED FROM
□	Audio and Video Files	☑	
☑	Compressed Files	□	
☑	Image Files	□	Management group
☑	Office Files	□	Default rights (user)
☑	PRESENSE unapproved files	□	Default rights (user)
□	Password Protected ZIP-Archive	□	

Figure 54. Assigning filter to user

→ Now all existing global filters, filters inherited from a group and/or default user and individually enabled filters are assigned to the user.

4. To disable inheritance, enable the **Activate individual settings** check box.

   → The previously inherited filters remain selected, uncheck them, if necessary. Global filters apply no matter whether they are enabled in the first column or not and whether inheritance is enabled or not.

5. Click **Save**.
6. If necessary, adjust the options for scanning archives and Microsoft Office files. For details, see: Specifying filter mode, step 3
7. Go to **User management | Settings | User settings**.

8. In the **File type filter – embedded files** area, enable the **Activate individual settings** check box and edit the settings.
9. Click **Save**.

All files corresponding to the filter are now either allowed (whitelisted) or blocked (blacklisted) for the user.

Temporary disabling filters

1. Select a user under **User management** and then select any tab under **Filters**. The tab selection plays no role, because the filters will be disabled for all storage types.
2. Click the **Unblocking code...** button.

   → The **Unblocking code generation – File type filter** dialog opens.
3. Specify a time period.
4. Click **Generate**.

   → The generated code appears in the **Code** field.
5. Copy the code and send it to the Client (e.g. by e-mail).

Via **EgoSecure Agent** the user can now enter the code and receive access rights:

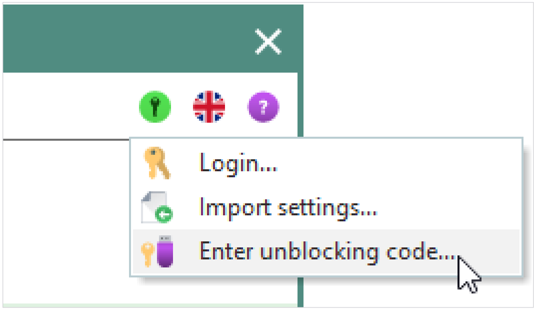


Figure 55. EgoSecure Agent: entering unblocking code

Defining file formats (advanced)

If the necessary file format is not in the list of predefined ones, it is possible to define own format if you have its *buffer* (file signature in a hexadecimal format) and *offset* (digit, which identifies a fixed place of a signature in a file) values. The buffer and offset values of the most popular file formats can be found on the Internet while unknown formats are requested from program developers.

1. Go to **Product settings | Filters | Content filter definition**.
2. In the **Rules definition** area, click **Define file formats**.

   → The **File format editor** dialog appears.
3. Click **Add**.

   → New entry appears.
4. In the **Format description** area, add information about a format:

a. In the **Name** field, define a format name.
b. In the **Extension(s)** field, enter file ending. E.g.: jpg, jpeg.
c. In the **Comment** field, add notes.
d. In the **Rule definition** area, define rules for a format:
e. In the **Buffer** field, enter a file signature in a hexadecimal format. E.g.: FF D8 FF
f. In the **Offset** field, enter a number which identifies the place of a signature in the file. E.g.: 0 (informs that file signature is at the beginning of the file).
g. Click **Save**.

→ The dialog doesn't close to all to add more formats.

5. Click **Close**.

→ The dialog closes.

➥ New format appears in the list of predefined formats in the drop-down of the File type column.

3.8. Controlling cloud access

INFO

No Box Drive support

Although Box Sync and Box Drive are the products of one company, **EgoSecure** supports only Box Sync.

Configuring access

Enabling control for clouds

1. Go to **User management | Settings**.
2. In the **User management** work area, select a default user, a group or an individual user.
3. In the **Cloud storage** tab, if you configure not the default user, enable the **Activate individual settings** check box.

   → The previously inherited clouds remain selected, uncheck them, if necessary.

4. Select clouds types to take them under control.
5. Click **Save**.

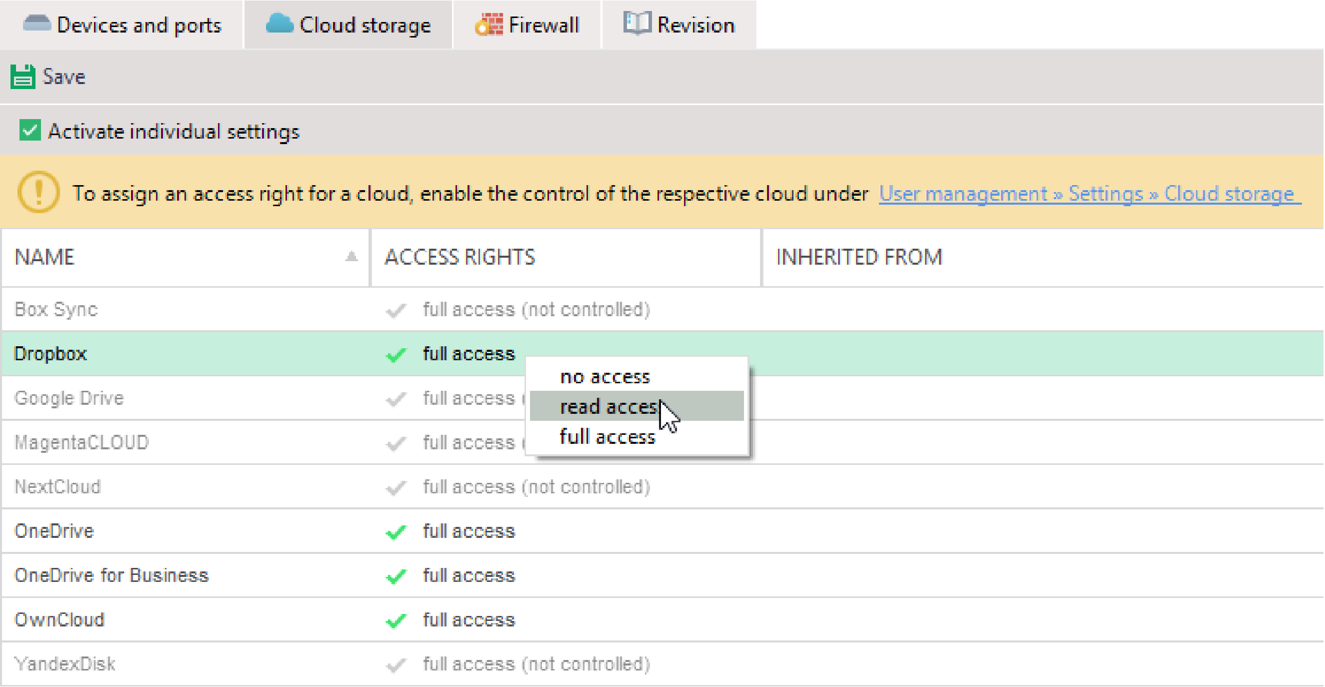
➥ Selected clouds are now under control. The cloud-related EgoSecure products will apply their actions only to the controlled clouds.

Assigning access rights for controlled clouds

1. Go to **User management | Control**.

2. In the **User management** work area, select a default user, a group or an individual user.
3. If you configure not the default user, enable the **Activate individual settings** check box in the **Cloud storage** tab.

   → Previously inherited rights for clouds selected, change them, if necessary.
4. Click in the **Access rights** column of a controlled cloud storage to change the rights.



☑ Activate individual settings

To assign an access right for a cloud, enable the control of the respective cloud under User management » Settings » Cloud storage

NAME	ACCESS RIGHTS	INHERITED FROM
Box Sync	✓ full access (not controlled)	
Dropbox	✓ full access	
Google Drive	✓ full access	
MagentaCLOUD	✓ full access	
NextCloud	✓ full access (not controlled)	
OneDrive	✓ full access	
OneDrive for Business	✓ full access	
OwnCloud	✓ full access	
YandexDisk	✓ full access (not controlled)	

Figure 56. Configuring cloud access

→ For the **OneDrive** cloud type, the **full access (without file fetching)** access type is available. For details, see: Use OneDrive to fetch files on a PC (external link).

→ Dropbox is controlled only in the **File Explorer** mode; Dropbox is not supported in the **Dropbox desktop app** mode.

5. Click **Save**.
6. To additionally block access to web addresses of controlled cloud storage types, go to **User management | Control | Firewall** and enable the **Block cloud web address** check box.
7. Click **Save**.

   → Web addresses of all controlled clouds are blocked for all applications except the cloud native applications, which are used for the automatic synchronization of the local cloud copy with a cloud itself.

INFO	**One Drive and One Drive for Business not controlled separately via Firewall** If either of the clouds – One Drive or One Drive for Business – is controlled, access to both their web addresses is blocked.

ATTENTION	**Using a proxy server** Cloud web address are not blocked if a computer connects to the Internet using a proxy server.

Restricting access to certain file formats

You can limit access to specific file formats in clouds: Creating file filters

1. Select a user under **User management**.
2. Enable a filter under **Filters | Cloud storage** tab.
3. Click **Save**.

➥ The filter takes effect on all cloud storage types where access rights are defined for a user under **User management | Control | Cloud storage**.

3.9. Controlling LAN/WLAN/LTE access

INFO	**Network driver required** To manage network access, install the network driver on the Clients. To install the network driver, enable the **Install network driver for WLAN control** option before generating the MSI package. ◆ If the option hasn’t been enabled during the first Agent installation, enable the option, generate the MSI package and update the Agents. For details, see: Installing EgoSecure Agents

Preventing simultaneous usage of different network connections (antibridging)

You can control network connections so that only one connection (LAN or WLAN) is always available on the clients at the same time.
To use this functionality, it is not necessary to activate the Access Control product for a computer, the Access Control license must be just available under **Administration | Licenses | License management**.

WARNING	**Local Agent reinstallation in case of wrong configuration** Selection of more than one antibridging options may lead to the situation when no network is available on the Client. As a result, connection between Agent and Server may be lost and no changes in the Antibridging settings can be transferred to the Agent. In this case, only Agent local reinstallation is a solution. ◆ Select the options to maintain the connection between Agent and Server.

1. Under **Computer management | Control**, select a computer from the directory service structure.
2. In the **Antibridging** tab, to disable the inheritance of settings from a group or from a default computer, enable the **Activate individual settings** check box.

   → Previously inherited options remain selected, uncheck them if needed.
3. Enable the options:
   a. **No WLAN when LAN is active**:
      Block all WLAN connections if LAN connection is available.
   b. **No WLAN when WLAN is active**:
      Block all WLAN connections except the one WLAN used for connection from Agent to Server at the moment of assigning this option. If no WLAN is used at the moment, any WLAN is randomly selected from the list of available WLANs.
   c. **No WLAN when LTE is active**:
      Block all WLAN connections if LTE connection is available.
   d. **No LAN when WLAN is active**:
      Block all LAN connections if WLAN connection is available.
   e. **No LAN when LAN is active**:
      Block all LAN connections except the one LAN used for connection from Agent to Server at the moment of assigning this option. If no LAN is used at the moment, any LAN is randomly selected from the list of available LANs.
   f. **No LAN when LTE is active**:
      Block all LAN connections if LTE connection is available.
   g. **No LTE when LAN is active**:
      Block all LTE connections if LAN connection is available.
   h. **No LTE when WLAN is active**:
      Block all LTE connections if WLAN connection is available.
   i. **No LTE when LTE is active**:
      Block all LTE connections except the one LTE used for connection from Agent to Server at the moment of assigning this option. If no LTE is used at the moment, any LTE is randomly selected from the list of available LTEs.
   j. **Ignore virtual devices**:
      Do not take network connections on virtual devices into account during antibridging.
4. Click **Save**.

INFO	**WLAN adapter is not disabled** EgoSecure does not disable WLAN adapters, but blocks the connection. A blocked adapter may continue to display as a **connected** one under Windows. However, data transfer does NOT occur. ◆ To check the antibridging functionality on the Client, open the WLAN connection status in the Control Panel (number of sent and received data is displayed as 0) or enter the command `ipconfig/all` in the Windows command prompt (connection must be displayed as disconnected).

Defining permitted WLANs

When defining permitted WLANs, only the assigned WLANs are permitted. Other WLANs not included in the list are blocked.

ATTENTION	**Blocked WLAN in case of enabled antibridging** ◆ Make sure that assigned WLAN is not blocked by Antibridging settings. For details, see: Antibridging

Defining permitted WLAN networks

1. Go to **Permitted devices | Removable devices | WLAN permissions**.
2. Click **Add** in the **WLAN permissions** area.
3. Define a name for a WLAN filter.
4. In the **Rule definition - <filter name>** area, click **Add** and then enter a **SSID** and/or **MAC address** of the WLAN access point.
5. Enable the **Password-protected** check box if the connection must be secure.
6. Define, for which computers the permission must take effect:
   a. To assign the WLAN filter for all computers of the directory service structure, enable the **Global** check box. This filter works independently of the **Access Control** product activation on Clients.
   b. To assign the WLAN filter only for an individual computer, leave the **Global** checkbox disabled and assign WLAN filters individually under **Computer management | Filters | WLAN permissions**.
7. Click **Save**.

↳ You can now assign the filter to a default computer (with inheritance to all existing computers where **Access Control** is activated) or to individual computers of a directory service.

Assigning WLAN filter

1. Select a computer under **Computer management | Filters**.
2. In the **WLAN permissions** tab, enable a filter.
3. To disable filters inherited from a group and/or from the default computer, enable the **Activate individual settings** check box.

   → The previously inherited filters remain selected, uncheck them, if needed.
4. Click **Save**.

➥ All WLAN connections that match the filter are now allowed on the computer. Other wireless connections are blocked.

3.10. Controlling access to input devices (BadUSB protection)

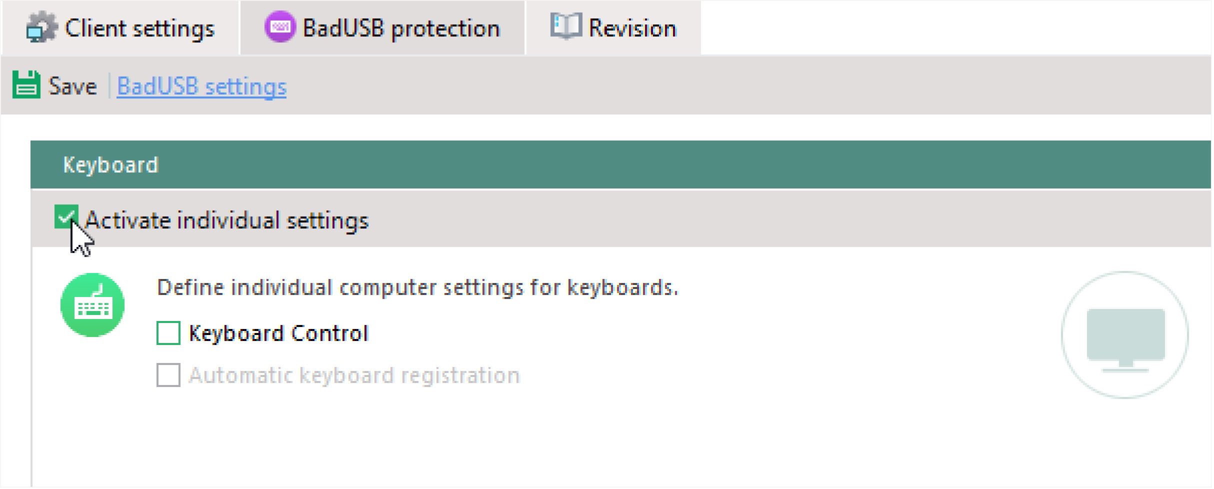
The firmware on USB devices is usually not protected and can be manipulated. A malicious USB stick registers in the operating system as a keyboard or a mouse to additionally distribute malware in the network.

Enabling keyboard control on computer

1. Go to **Administration | Clients | Client settings**.
2. In the **Control input devices** group, enable the Keyboard Control and **Automatic keyboard registration** options.

   → You can now enable the **Keyboard Control** for the default computer or only for an individual computer. If you enable the **Keyboard Control** for the default computer, this setting is inherited to all computers. The inheritance can be disabled for computers individually.
3. Click **Save**.
4. Go to **Computer management | Settings**.
5. Select the default computer under **Default policies** or a computer from the directory service structure.
6. In the **BadUSB protection** tab, enable the **Keyboard Control** check box.

   If you haven’t enabled the option for the default computer and want to enable it individually for a computer, first disable the inheritance by enabling the **Activate individual settings** check box:



☑ Activate individual settings

Define individual computer settings for keyboards.

□ Keyboard Control

□ Automatic keyboard registration

Figure 57. Deactivating inheritance from default rights

→ The keyboard that is currently connected becomes the primary one. This is the only keyboard permitted on this computer, all other keyboards are blocked.

7. Enable the **Automatic keyboard registration** option.

→ Newly connected keyboards are registered. While the option is enabled, all keyboards connected to the computer are automatically added to the individual list of permitted devices (**Permitted devices | Individual device permissions**) and assigned to the computer. Once the option is disabled, only registered keyboards and the primary keyboard are permitted.

8. Click **Save**.

The computer-based keyboard control is now enabled.

Allowing users to control keyboards

1. In **User management | Settings**, select a user from the directory service structure.
2. In the **BadUSB protection** tab, enable the **Grant keyboard control to user** option.

→ When connecting a keyboard that is not primary or not registered, a user now decides whether to include it to the individual list of permitted devices for this computer or not. When connecting the keyboard for the first time, a message appears.
The message text can be edited under **Administration | Clients | Custom messages**, section **Security warnings**. For details, see: Customizing user messages.

INFO

Message does not appear

If the keyboard is already in the list of **Individual device permissions**, but the administrator has removed the checkmark from it, the message does NOT appear and such a keyboard is locked.

3. Additionally, enable the **Ask user each time on keyboard connection** option to show the message each time on connecting a keyboard that is not primary or not registered. In this case, unlike the previous option, the permitted keyboard is not added to the list of individual device permissions for this computer.
4. Click **Save**.

➥ The user-based keyboard control is now enabled.

Enabling mouse control on computer

1. Go to **Administration | Clients | Client settings**.
2. In the **Control input devices** group, enable the **Mouse Control** option.

   → You can now enable the **Mouse Control** for a default computer or only for an individual computer. If you enable the **Mouse Control** for the default computer, this setting is inherited to all computers. The inheritance can be disabled for a computer individually.
3. Go to **Computer management**.
4. Select the default computer in **Default policies** or a computer in the directory service structure.
5. Under **Settings | BadUSB protection**, enable the **Mouse Control** option.
   If you haven't enabled the option for the default computer and want to enable it individually for a computer, first disable the inheritance by enabling the **Activate individual settings** check box.
6. Click **Save**.

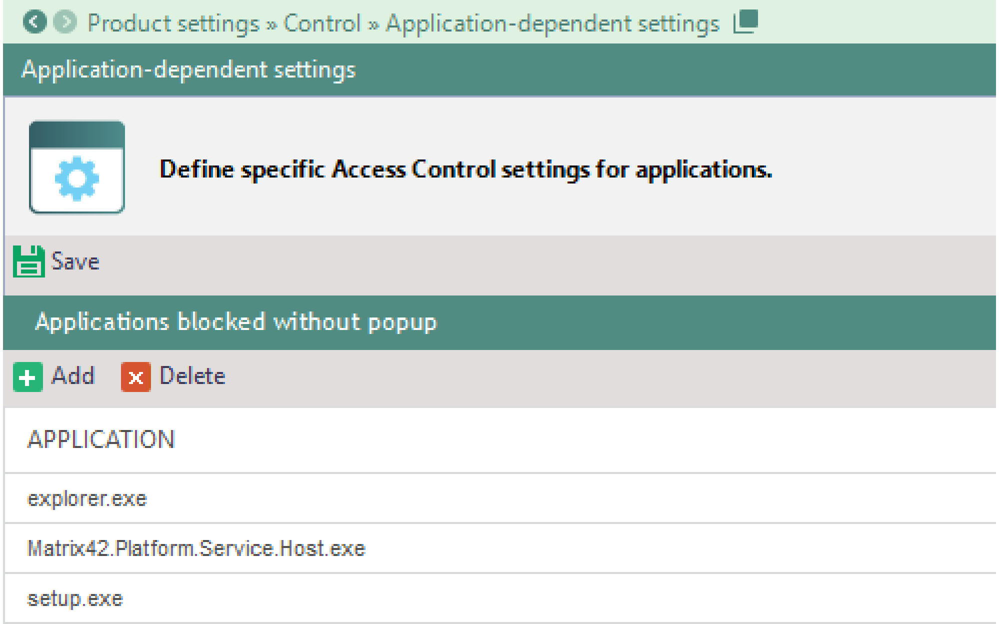
➥ The mouse that is currently connected becomes the primary one. This is the only mouse permitted on this computer, all other mice are blocked if they are not in the individual list of permitted devices.

3.11. Setting up application access to blocked devices

Very often some applications and processes try to access a blocked device on the background. In this case the EgoSecure popup appears. The solution is to enlist the processes for which no popup displays when it tries to access the forbidden device.

Creating a list of applications blocked without popups

1. Go to **Product settings | Control | Application-dependent settings**.
2. Under **Applications blocked without popup**, click **Add**.
3. Enter a process name.



Product settings » Control » Application-dependent settings

Application-dependent settings

Define specific Access Control settings for applications.

Save

Applications blocked without popup

Add Delete

APPLICATION
explorer.exe
Matrix42.Platform.Service.Host.exe
setup.exe

Figure 58. Making a list of applications for which access is blocked without popup

4. Click **Save**.

Once a listed application accesses a blocked device, the access for the application will be blocked, but no popup message appears.

3.12. Controlling access to Bluetooth devices

When managing Bluetooth devices, distinguish between the following types:

- Bluetooth port: access point on the Agent computer used for connection by Bluetooth devices (built-in or pluggable).
  Under **User management**/**Computer management | Control**, assign access rights for Bluetooth connections. For details, see: Controlling access rights for Bluetooth access point

- Bluetooth device categories: headsets, smartphones, keyboard etc. connected to the Agent computer via a Bluetooth port.
  Under **Permitted devices | Removable devices | Bluetooth devices**, restrict the usage of Bluetooth devices to specific device categories. For details, see: Allowing Bluetooth connections for specific device categories

- Bluetooth devices: known devices like keyboard, mouse, telephone etc., connected to the Agent computer via a Bluetooth port.
  Under **Permitted devices | Removable devices | Bluetooth devices**, permit to use specific Bluetooth devices. For details, see: Allowing Bluetooth connections for specific devices

Controlling access rights for Bluetooth access point

! The rights for a Bluetooth access point have a priority over Bluetooth whitelist. E.g: **Block virtual adapter** is set for Bluetooth access point and mobile devices are in whitelist. => File transfer on mobile devices is blocked.

1. Select a directory object under **User management**/**Computer management | Control**.
2. In the **Devices and ports** tab, right-click **Bluetooth**.
3. Select one of the following access rights:
   - **Full access** to allow Bluetooth connections on Agent computer.
   - **No access** to forbid Bluetooth connections on Agent computer.
   - **Block virtual adapters** to forbid only file sending, but to allow the connection from an Agent computer to devices via Bluetooth.
   - **Scheduled access** to apply access rights for a Bluetooth access point according to a scheduler.
4. Click **Save**.

Allowing Bluetooth connections for specific device categories

If the **full access** or the **block virtual adapters** access type is assigned to a Bluetooth access point, you can define Bluetooth devices permitted to connect to this access point. Specify Bluetooth device categories (Bluetooth whitelist) or specific Bluetooth devices that the user is allowed to use. Bluetooth device permissions have a priority over Bluetooth whitelist.

! Individual Bluetooth device permissions work only if at least one Bluetooth whitelist has been specified for the respective directory service object.

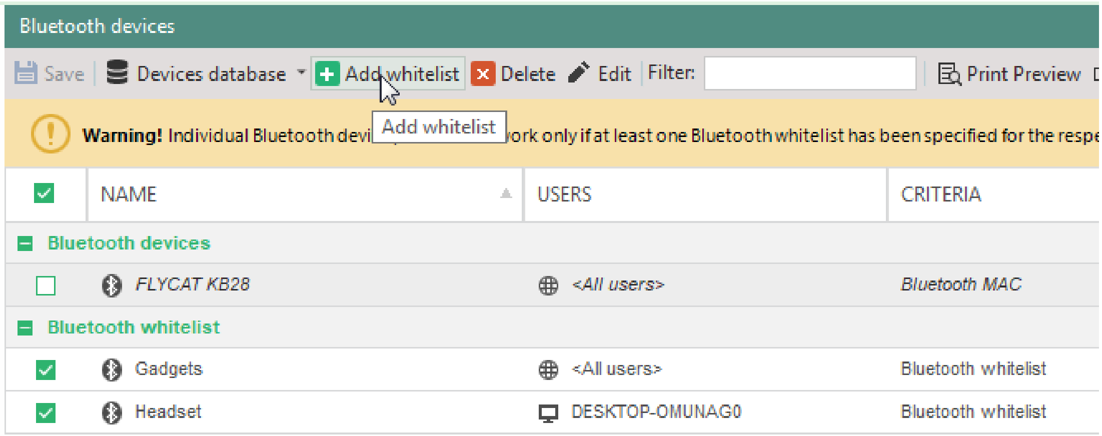
ATTENTION

Assigning several whitelists or an empty whitelist

- When assigning several whitelists where the same device categories have different permissions, the usage of these device categories is not allowed.
  E.g.: one whitelist allows keyboards while another list does not allow - in this case the usage of Bluetooth keyboards is forbidden.
- When assigning a whitelist with no selected categories (empty whitelist) to a directory object, all Bluetooth devices are forbidden to be connected to the end device. Exclusion: permitted known Bluetooth devices

Allowing Bluetooth device categories (Bluetooth whitelist)

1. Go to **Permitted devices | Removable devices | Bluetooth devices**.
2. Click **Add whitelist**.



Bluetooth devices

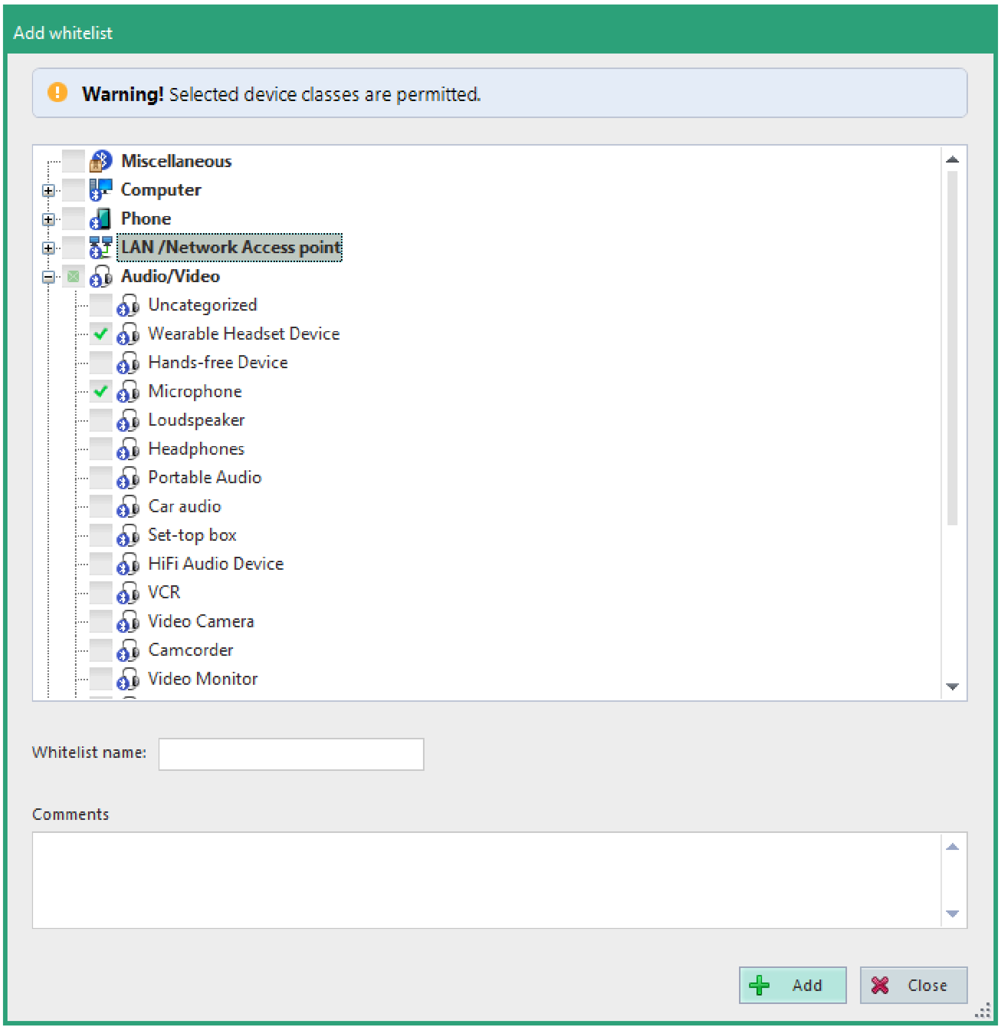
Warning! Individual Bluetooth devi… …ork only if at least one Bluetooth whitelist has been specified for the respe

☑	NAME	USERS	CRITERIA
⊟	Bluetooth devices		
□	*FLYCAT KB28*	*<All users>*	*Bluetooth MAC*
⊟	Bluetooth whitelist		
☑	Gadgets	<All users>	Bluetooth whitelist
☑	Headset	DESKTOP-OMUNAG0	Bluetooth whitelist

Figure 59. Creating Bluetooth whitelist

→ The **Add whitelist** dialog appears.

3. Select a category or a device class of Bluetooth devices allowed to connect to Agent computers.



Add whitelist

Warning! Selected device classes are permitted.

- □ Miscellaneous
- ⊞ □ Computer
- ⊞ □ Phone
- ⊞ □ LAN /Network Access point
- ⊟ ▨ Audio/Video
  - □ Uncategorized
  - ✓ Wearable Headset Device
  - □ Hands-free Device
  - ✓ Microphone
  - □ Loudspeaker
  - □ Headphones
  - □ Portable Audio
  - □ Car audio
  - □ Set-top box
  - □ HiFi Audio Device
  - □ VCR
  - □ Video Camera
  - □ Camcorder
  - □ Video Monitor

Whitelist name:

Comments

Figure 60. Selecting device class(es) for whitelist

4. In the **Whitelist name** field, define a name of a whitelist.

5. Click **Add**.

   → The dialog closes and the whitelist is added under **Bluetooth whitelist**.

6. Assign the whitelist to a directory object:
   a. In the lower area, select the **User** or **Computer** tab.
   b. Click **Add**.

   → The **Selection of users** or **Selection of computers** dialog appears.

   c. In the directory service structure, select a user or a computer where **Access Control** product is activated.
   d. Click **OK** to confirm.

   → The **Selection of users** or **Selection of computers** dialog closes.

7. In the **Bluetooth devices** area, click **Save**.

➥ Selected directory objects are allowed to use all Bluetooth devices of the whitelist categories. Devices of other categories are not allowed. The exclusion is known Bluetooth devices.

Allowing Bluetooth connections for known devices

If **full access** or **block virtual adapters** access type is assigned to a Bluetooth access point, you can define known Bluetooth devices permitted to connect to this access point. Define specific Bluetooth devices that the user is allowed to connect. Bluetooth device-specific permissions have a priority over Bluetooth whitelist.

1. Go to **Permitted devices | Bluetooth devices**.
2. To add a Bluetooth device, click **Scan computer** or **Devices database**. For details, see: Allowing device for user

   → The device appears in the list.

3. If there is no whitelist defined, add an empty whitelist to block all other Bluetooth devices except the ones listed:
   a. Click **Add whitelist**.
   b. Define a name and click **Add**.

   → Now only added Bluetooth devices are allowed.

4. Assign the device to a directory object:
   a. In the lower area, select the **User** or **Computer** tab.
   b. Click **Add**.

   → The **Selection of users** or **Selection of computers** dialog appears.

   c. In the directory service structure, select a user or a computer where **Access Control** product is activated.
   d. Click **OK** to confirm.

   → The **Selection of users** or **Selection of computers** dialog closes.

5. In the **Bluetooth devices** area, click **Save**.

➥ The added directory objects are allowed to use only listed Bluetooth devices.

3.13. Controlling data transfer via clipboard

Disabling clipboard

1. Under **User management | Settings**, select a user or edit the default rights of known users under **Default policies**.
2. In the lower area, navigate to the **User settings** tab.
3. To disable inheritance for a user and assign individual settings, enable the **Activate individual settings** check box in the **Clipboard** area.

   → The inheritance is now deactivated.

4. Enable the **Disable the use of the clipboard** option.
5. Click **Save**.

➥ The user is no longer allowed to use the clipboard.

3.14. Viewing directory object permissions and settings

In **User management** and **Computer management**, you can see a summary of permissions and settings for a certain user or a computer and export it, if needed.

Showing summary of settings

1. Under **User management/Computer management**, select a user/computer.
2. Under **Control | Devices and ports** tab, click **Summary** on the toolbar.

   → The **Summary – [user/computer name]** dialog opens. The overview of the rights and settings is displayed for the selected directory object.

3. To print the summary of rights and settings or export to CSV or PDF, click the respective button.
4. To close the dialog, click **Close**.

3.15. Using Access Control on IoT devices

EgoSecure Agent on IoT devices has no graphic user interface. Only the **Access Control** (AC) product can be activated. Via AC only the External storage device class is controlled.
Access rights are delivered to the IoT device once in one minute (because EgoSecure Agent works in the polling mode and checks the EgoSecure Server for new settings with an interval of one minute).

Available actions for IoT devices:

- Assigning an access right to the external storage device class

- Inheriting default rights
- Assigning temporary access right
- Assigning different rights for online and offline Agents

For details about installing **EgoSecure Agent** on IoT devices, see chapter 7 of the EgoSecure Installation Guide.

3.16. Configuring PRESENSE connector

PRESENSE Connector is used in companies where PRESENSE PROVAIA or PRESENSE JANUS are used. These devices analyze data on external storage, floppy disks and check the data for malware, suspicious files, etc. The result of such analysis is the creation of a report file (*.xml).

EgoSecure Agent denies access to external storage devices if Connector is enabled and one of the conditions is met:

- There is no report file on external storage.
- Report signature is not valid (not signed by the PRESENSE certificate).
- Report entries have status other than “clean” (if the PRESENSE approved/unapproved files filter is enabled, access to the whole device is permitted, only access to unapproved files is restricted). For details, see: Enabling and assigning PRESENSE filter

If new files have been created on the disk or existing files have been changed, access to these files will also be blocked after reconnecting the device. In this case, a re-analysis of the volume by PRESENSE is required.

INFO	**Files encrypted with Device Encryption** Files encrypted with **Removable Device Encryption** are recognized as changed during an encryption process. ◆ Decrypt the files so that no volume re-analysis is required.

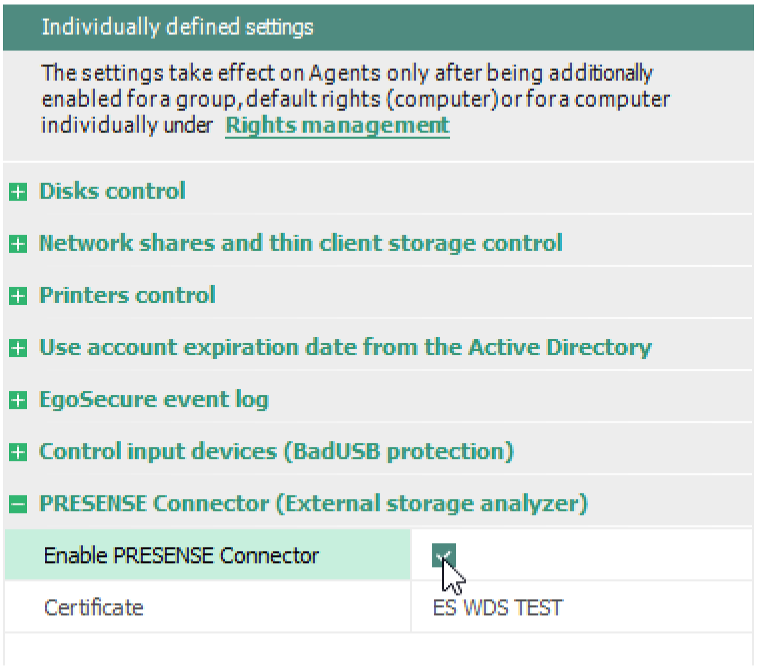
INFO	**Access to individually permitted devices** If the access to a device is denied by PRESENSE, the access is nevertheless permitted if the user has an individual device permission for the device.

Enabling PRESENSE control

! To use PRESENSE connector, the PRESENSE certificate is required.

1. Import the PRESENSE certificate for the **Current user**. For details, see in help center: Importing certificate
2. Go to **Administration | Clients | Client settings**.

3. Check the **Enable PRESENSE Connector** box.



Individually defined settings

The settings take effect on Agents only after being additionally enabled for a group, default rights (computer) or for a computer individually under Rights management

⊞ Disks control
⊞ Network shares and thin client storage control
⊞ Printers control
⊞ Use account expiration date from the Active Directory
⊞ EgoSecure event log
⊞ Control input devices (BadUSB protection)
⊟ PRESENSE Connector (External storage analyzer)

Enable PRESENSE Connector ☑

Certificate ES WDS TEST

Figure 61. Enabling PRESENSE

→ The **Windows Security** dialog appears.

4. Select the displayed certificate or click **More choices** to select a different certificate.
5. Click **OK** in the Windows Security dialog to confirm.

   → The **Windows Security** dialog closes.

6. Click **Save**.

PRESENSE connector is now enabled and configured. Storage devices where not clean files are detected, are blocked completely if no PRESENSE filter is enabled.

Enabling and assigning PRESENSE filter

If the PRESENSE report of a storage device contains files marked as 'not clean', **EgoSecure** denies access to the entire storage device.
If the PRESENSE filter is enabled for users, only access to unclean files is blocked. Access to other files is granted if they are not blocked by another file filter. For details, see: File type filters

Enabling filter

1. Select a user under **User management | Filters**.
2. In the **External storage** tab, enable the **PRESENSE approved files** (in case of the white list mode) or **PRESENSE unapproved files** (in case of the black list mode).
3. Click **Save**.

The PRESENSE filter is now assigned to the user.

3.17. Importing settings via XML file

You can apply permissions for a user or a computer via an XML file. Create an XML file with certain settings and specify file directory in the Console. **EgoSecure Server** processes the file and creates two subfolders in the directory: **Success** (for successful import) and **Fail** (for failed import).

The import can be performed tenant-specifically or globally for all tenants.

Importing settings via XML

1. Create the XML file with the settings. For details, see: XML import format
2. In the Console, go to **Administration | Administrator | Import of settings from XML** to import settings for a current tenant.
   To import settings for all tenants, go to **Administration | Superadmin | Import of settings from XML (global)**.

ATTENTION	**Avoiding issues with global import** If an xml file contains a tenant-specific command (e.g.: a command for applying individual device permissions to a group that exists only in one tenant), the import of non tenant-specific commands from this file fails. ◆ Import XML files with tenant-specific commands under **Administration | Administrator | Import of settings from XML**.

3. In the **Import folders** area, click **Browse** near **Folder for data import** and select the directory with the XML file.

   → The directory is also used to automatically create **Success** and **Fail** subfolders.

4. To import the settings, click **Save**.

- The import occurs. In the specified directory, the **Success** (for successful import) and **Fail** (for failed import) subfolders are created and the processed file is moved in one of the subfolders accordingly.
- Once a new file is uploaded to the specified directory, it is reprocessed.

3.18. Excluding user network login sessions from processing

Define a security identifier (SID) or name of a user to exclude network login sessions of this user from processing by EgoSecure Agent.
Usage example: if EgoSecure Agents are running on Citrix XenDesktop, it makes sense to add the server SID of XenDesktop controller to exclusions so that it is not processed by EgoSecure Agents and the processing therefore doesn’t cause high CPU.

Adding a network login session to exclusions

A network login session can be excluded based on a user name or a user SID.

ATTENTION	**Excluding by user name – not secure** We recommend to exclude network login sessions by SID. This ensures maximum security.

Adding a network login session to exclusions – by user SID

1. Go to **Product settings | Control | Network login exclusions**.
2. Click **Add SID** on the toolbar.

   → A new entry appears.
3. In the **Value** column, enter the SID of the user, whose network sessions you want to exclude from processing.
4. (optional) In the **Comments** column, add your description.
5. Click **Save**.

Adding a network login session to exclusions – by user name

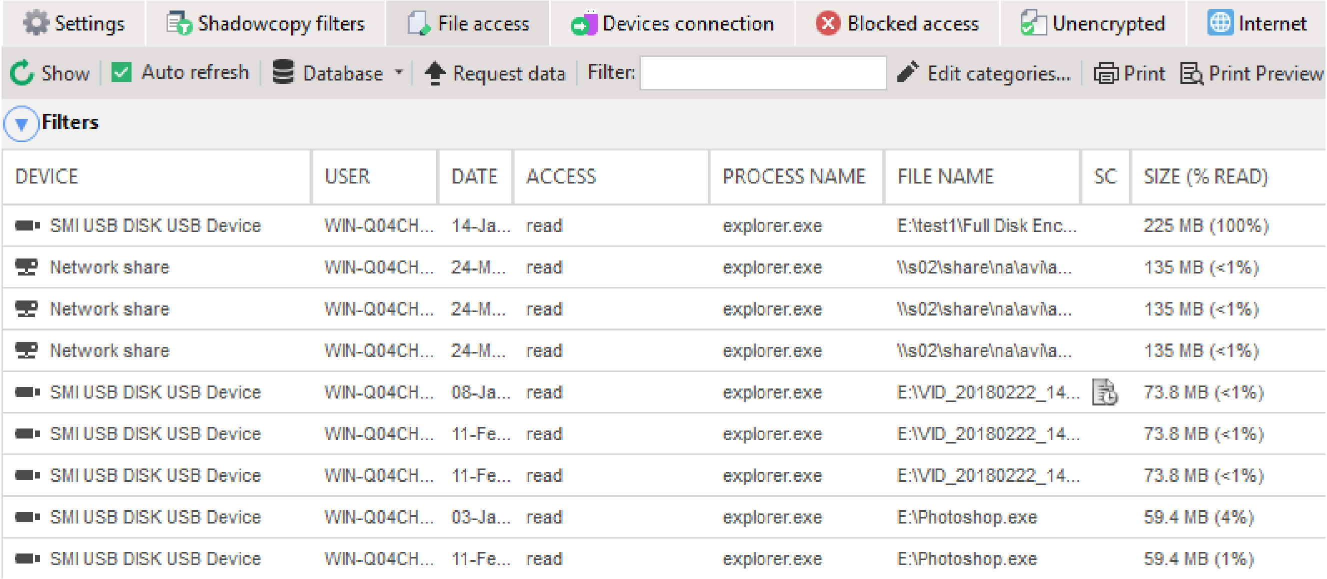
1. Go to **Product settings | Control | Network login exclusions**.
2. Click **Add name** on the toolbar.

   → A new entry appears.
3. In the **Value** column, enter the name of a user, whose network sessions you want to exclude from processing.
4. (optional) In the **Comments** column, add your description.
5. Click **Save**.

4. SECURE AUDIT

4.1. Secure Audit - overview

Secure Audit saves audited events to the database. Audit data is first saved on the Clients, then transferred from the Agent to the Server and finally deleted on the Clients. The Server saves the data in the database.
You can activate **Secure Audit** for a computer and for a user. The audit data about device connection and Wi-Fi is available only for the computer.



DEVICE	USER	DATE	ACCESS	PROCESS NAME	FILE NAME	SC	SIZE (% READ)
SMI USB DISK USB Device	WIN-Q04CH...	14-Ja...	read	explorer.exe	E:\test1\Full Disk Enc...		225 MB (100%)
Network share	WIN-Q04CH...	24-M...	read	explorer.exe	\\s02\share\na\avi\a...		135 MB (<1%)
Network share	WIN-Q04CH...	24-M...	read	explorer.exe	\\s02\share\na\avi\a...		135 MB (<1%)
Network share	WIN-Q04CH...	24-M...	read	explorer.exe	\\s02\share\na\avi\a...		135 MB (<1%)
SMI USB DISK USB Device	WIN-Q04CH...	08-Ja...	read	explorer.exe	E:\VID_20180222_14...	🗎	73.8 MB (<1%)
SMI USB DISK USB Device	WIN-Q04CH...	11-Fe...	read	explorer.exe	E:\VID_20180222_14...		73.8 MB (<1%)
SMI USB DISK USB Device	WIN-Q04CH...	11-Fe...	read	explorer.exe	E:\VID_20180222_14...		73.8 MB (<1%)
SMI USB DISK USB Device	WIN-Q04CH...	03-Ja...	read	explorer.exe	E:\Photoshop.exe		59.4 MB (4%)
SMI USB DISK USB Device	WIN-Q04CH...	11-Fe...	read	explorer.exe	E:\Photoshop.exe		59.4 MB (1%)

Figure 62. Secure Audit for file access

4.2. Activating Secure Audit

Before activating

To avoid performance problems, pay attention to the following before activating:

- **Audit data size**. Make sure to have enough space in the database. 1 million of **Secure Audit** entries takes space of about 500 MB. To avoid database overfilling, handle Secure Audit data properly by specifying the settings for archiving or removing of old audit data under **Administration | Administrator | Database maintenance**.
- **SQL Server transaction log**. Specify the transaction log settings to avoid a Full Transaction Log error. For details, see the Microsoft article Troubleshoot a Full Transaction Log (SQL Server Error 9002) (external link).
- **SQL Express**. Use SQL Express with enabled **Secure Audit** carefully. EgoSecure recommends SQL Express only for demonstration purposes and for very small organizations due to the fact that SQL Express raw size of the database is only 10 GB. It may lead to the database filling, which influences **Secure Audit** performance.

Enabling audit and selecting audit data

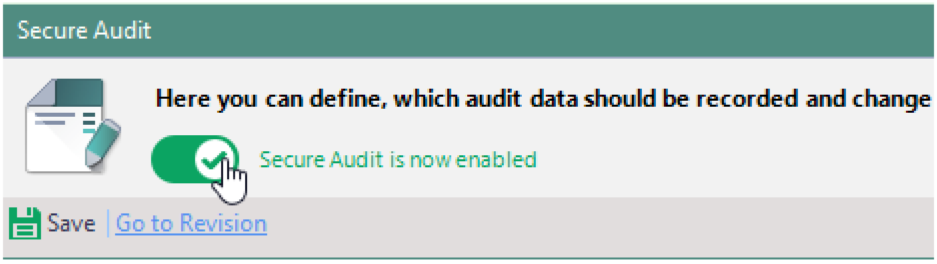
Activating **Secure Audit** for a user/computer occurs in several steps:

- Enabling Secure Audit in Console
- Setting up password protection (optional)
- Selecting audit data (used for default user/computer)
- Adjusting audit data for user/computer (optional)
- Activating Secure Audit for user/computer

Enabling Secure Audit

1. Under **Product settings**, go to **Audit | Secure Audit**.
2. Click on the button **Secure Audit is now disabled**.

➘ The audit is now enabled and can be configured.



Secure Audit

Here you can define, which audit data should be recorded and change

Secure Audit is now enabled

Figure 63. Enabled audit

To prevent unauthorized access, protect audit data with one password/two passwords:

Setting up password protection

1. Go to **Product settings | Audit | Secure Audit**.
2. In the **Access to the auditing database** area, enable **Protect all audit data with the same password set**.
3. Enable the button with the desired number of passwords for protection.

   → The corresponding number of password fields appears.

4. To change the password, click **Change**, near the password field.
5. In the dialog, enter the password and click **OK** to confirm.

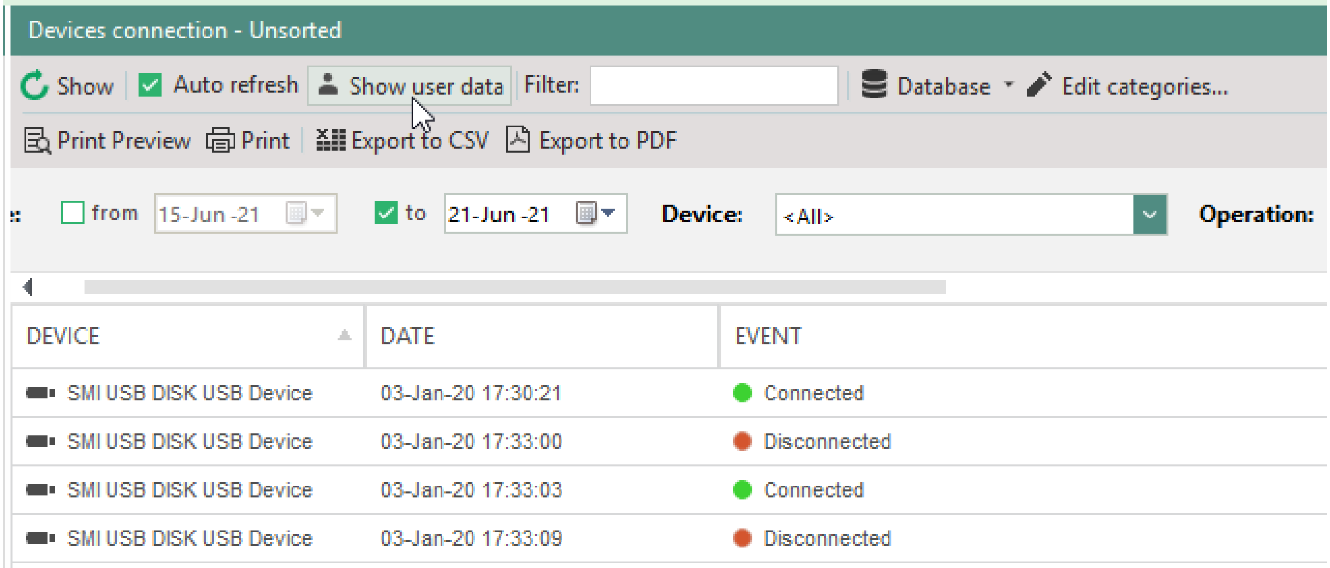
   → You have now set up a single scheme of protection for all audit data types. The password will be requested each time when accessing any audit data tab under **User management**/**Computer management | Audit** and under **Reports | Audit**.

6. To enable an individual scheme of protection for each audit data type, disable the **Protect all audit data with the same password set** check box.
7. Select the scheme of protection for each audit data type in the **Access to the audit data** column.

→ You have now set up an individual scheme of protection for each audit data type. The password will be requested each time when accessing a password-protected audit data tab under **User management/Computer management | Audit** and under **Reports | Audit**.

8. To allow access to password-protected audit data under **Reports | Audit**, but to hide user/computer names, enable the **Show auditing data without the user information unprotected**. For audit data tabs under **User management/Computer management | Audit** the password will continue to be requested.

   → When clicking **Show user data** button, a password is requested. Once the password is successfully entered, user/computer data appears.



☑ Auto refresh

□ from 15-Jun -21 ☑ to 21-Jun -21 **Device:** <All>

DEVICE	DATE	EVENT
SMI USB DISK USB Device	03-Jan-20 17:30:21	● Connected
SMI USB DISK USB Device	03-Jan-20 17:33:00	● Disconnected
SMI USB DISK USB Device	03-Jan-20 17:33:03	● Connected
SMI USB DISK USB Device	03-Jan-20 17:33:09	● Disconnected

Figure 64. Showing user data in menu Reports | Audit

9. Click **Save**.

Access to **Secure Audit** data is now password-protected. As a supervisor, you can change the password by entering a new one and then saving.
Being an administrator or a super administrator, you must first enter the old password to set a new password.

The following table gives an overview of data collected by **Secure Audit**:

Files	
External storage, Network share, Thin client storage, Cloud storage	Logs access to files and related processes, drives, network folders or thin client storage media. A distinction is made between read, write, delete and rename accesses. For details, see: Logged access types. ■ To audit on network shares and thin client storage, additionally enable the **Allow thin client storage control** and **Allow network shares control** options for a computer under **Computer management | Settings | Client settings**.

	■ To audit on clouds, additionally define the clouds to control under **User management | Settings | Cloud storage**. ■ To additionally define specific network shares for data collection, go to **Product settings | Audit | Network share** and add either the network shares from where the data is collected (in case of a white list) or only the network shares from where the data collection is blocked (in case of a black list).
Internet	
HTTP- and HTTPS connections	Logs the page visits via any Internet browser. The **HTTP protocol** option audits only unencrypted pages. The **HTTPS protocol** option audits only encrypted pages. Note: If you have set up a proxy server, page visits are not logged.
WLAN	Logs the connection data of the WLAN and indicates whether it is secure or not secure (open). For details, see: Defining permitted WLANs
Applications	
Applications launch	Logs running applications.
Use of applications	Logs the use of applications (duration of use, date of use).
DLL launch	Logs started program libraries (DLLs).
Java archives launch	Logs started Java archives (jar files).
General	
Devices connection	Logs the connection and removal of devices (can only be activated for computers).
System events	Logs events such as starting, shutting down, or locking a computer. For details, see List of logged system events
Unencrypted files transfer	Logs files that have been transferred unencrypted to devices (external storage media and CD/DVD) or to clouds. The option can only be activated if an encryption product is available and encryption is activated. Make sure that **Removable Device Encryption** or **Cloud Storage Encryption** are activated. If you have activated shadowcopy for the user, you can download unencrypted files from the **SC** column under **User management | Audit | Unencrypted**.
Blocked access	Logs attempts to access files that are blocked due to the lack of access rights, filter settings, etc.
Shadowcopy	
Shadow copies of read and/or written files	Saves a copy of all files that have been read, written or deleted by the user on external media, in clouds, network folders or on thin client storage media. For details, see: Enabling Shadowcopy. Here you can access shadow copies:

	User management/**Computer management | Audit**, **File access** and **Unencrypted** tabs, column **SC**. **Reports | Audit | File access** und **Unencrypted file transfer**, column **SC**.

INFO

Access types of the Access column

In some cases, read/write/delete access can take place simultaneously. In the **Access** column of an audit table, all types of access are shown. This does not necessarily have to be manual access performed by the user. For example, a process can simultaneously perform a read/write access or a write/delete access. Some programs such as Microsoft Office applications often create temporary files that are then deleted.

List of logged system events

Event type	Description
Unknown event	System event, which is not identified.
Computer start	Computer was turned on.
Computer shutdown	Computer was shut down.
Suspend	Computer was preparing for a sleep or hibernate. This is the stage when the screen blinks off but neither sleep, nor hibernation happened yet.
Sleep mode	Computer went to sleep.
Hibernation	Computer was hibernated.
Exit sleep mode	Computer was woken from sleep.
Exit hibernation	Computer was started after hibernation.
Computer lock	Lock screen for a user who is currently logged in to computer.
Computer unlock	Unlock computer for which the lock action was performed.
System login	Log in to a user account when starting a computer, switching users, exiting sleep mode etc.
System logout	Log out from a current account when a user, e.g., clicked the Sign out option.
Tray login	Login to the EgoSecure Tray application when a user, e.g., clicked the **Login…** option.
Tray logout	Logout from the EgoSecure Tray application when a user, e.g., clicked the **Logoff [current login]** option.

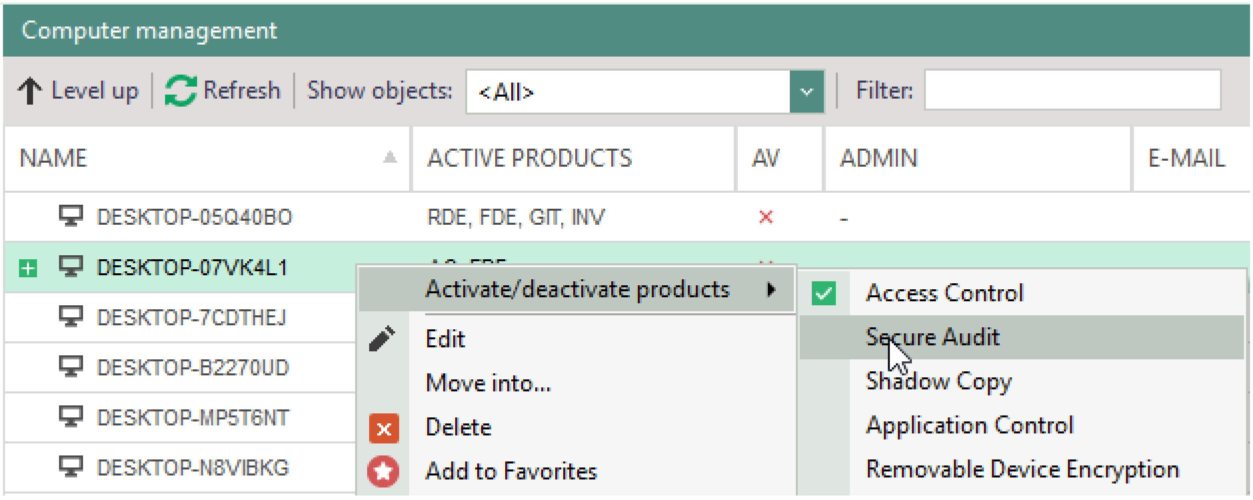
Selecting audit data

1. Go to **Product settings | Audit | Secure Audit**.
2. Enable the audit data that becomes available for activating on users and computers.
3. Click **Save**.

The selected logging data is applied to the default user and the default computer and then to the registered user/computer. You can disable some points for them individually. However, you cannot individually activate points that are not activated in the product settings.

Activating Secure Audit for user or computer

1. Go to **User management/Computer management | Audit**.
2. In the **User management/Computer management** work area, right-click the user/computer and select **Activate/deactivate products | Secure Audit**.

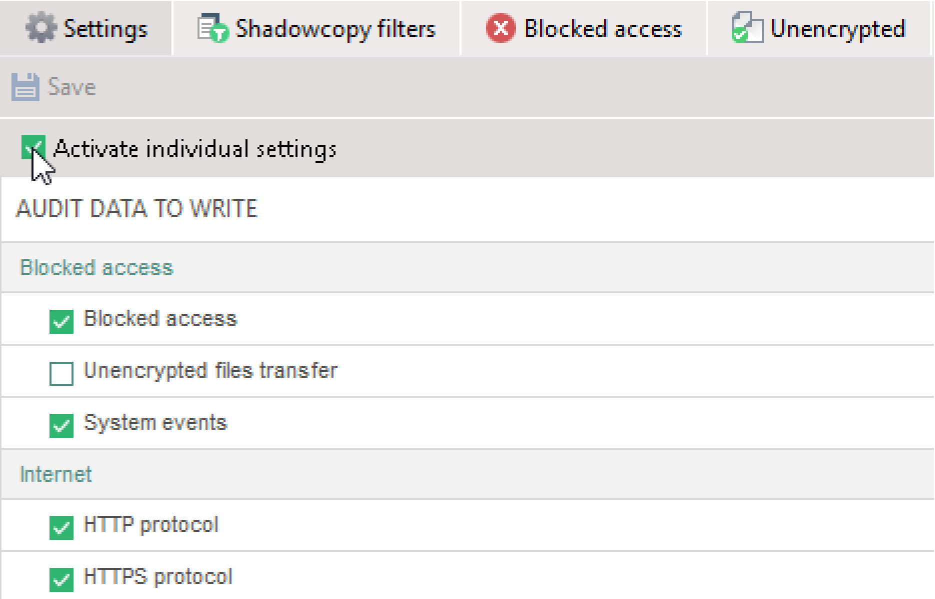


NAME	ACTIVE PRODUCTS	AV	ADMIN	E-MAIL
DESKTOP-05Q40BO	RDE, FDE, GIT, INV	×	-	
DESKTOP-07VK4L1				
DESKTOP-7CDTHEJ				
DESKTOP-B2270UD				
DESKTOP-MP5T6NT				
DESKTOP-N8VIBKG				

Figure 65. Activating Secure Audit for user

→ In the **Active products** column of the user/computer, there appears the short name **SA**. The settings of the default user/computer are applied to the object.

3. You can also adjust audit settings for an individual computer/user. To adjust,
   a. Enable the **Activate individual settings** check box under **Audit | Settings**.
      → The previously inherited options remain enabled. Uncheck them, if necessary.



☑ Activate individual settings

AUDIT DATA TO WRITE

Blocked access

☑ Blocked access
□ Unencrypted files transfer
☑ System events

Internet

☑ HTTP protocol
☑ HTTPS protocol

Figure 66. Configuring Secure Audit for user

b. Edit the settings.

c. Click **Save**.

Secure Audit is now enabled and configured. Audit data is saved to the database and will become reachable in the Console.

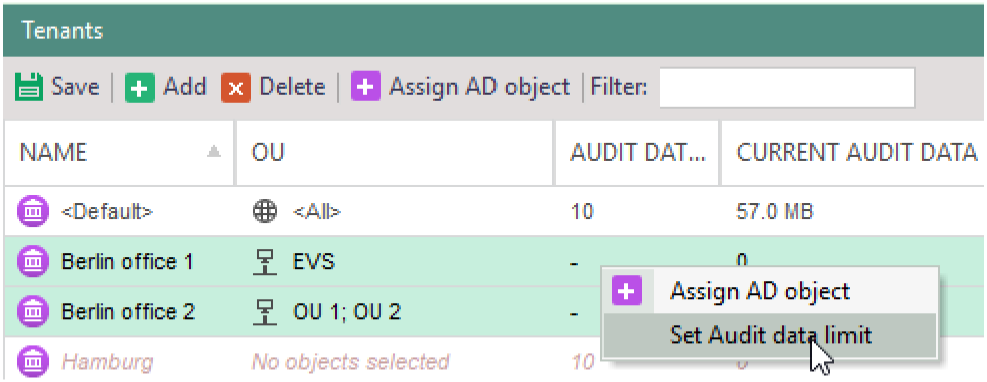
Specifying size limit for Audit data

You can set a maximum size of audit data per tenant. Once the limit is reached, audit data is stored on the Agent computer until a capacity is available in the database again (e.g. after Archiving or deleting old audit data).

Via **IntellAct Automation** you can create a rule that notifies administrators about clients who reached the limit. For details, see: Monitoring server activity with IntellAct

Specifying size limit for tenant

1. Go to **Administration | Superadmin | Tenants**.
2. Select a tenant. To select multiple tenants, hold down `Ctrl` and click.
3. Right-click the tenant and select **Set Audit data limit** from the context menu.



NAME	OU	AUDIT DAT...	CURRENT AUDIT DATA
<Default>	<All>	10	57.0 MB
Berlin office 1	EVS	-	0
Berlin office 2	OU 1; OU 2	-	
Hamburg	No objects selected	10	0

Figure 67. Specifying audit data limit for a tenant

→ The **File size** dialog appears.

4. Specify a limit and click **OK** to confirm.
5. Click **Save**.

4.3. Working with Secure Audit

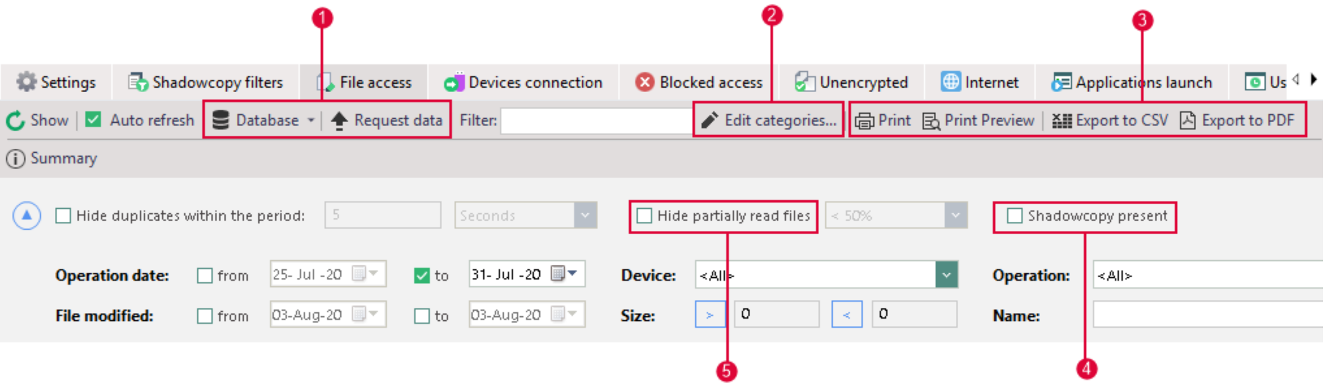
Showing audit data

Under **User management | Audit** and **Computer management | Audit** as well as under **Reports | Audit** you can see the audit data in a tabular form. You can configure the displaying and filter the records.

ATTENTION

Audit table display limitation

Each Secure Audit table can display only up to 100 thousand records. See also Archiving or deleting old audit data



☐ Hide duplicates within the period: 5 Seconds

☐ Hide partially read files < 50%

☐ Shadowcopy present

Operation date: ☐ from 25- Jul -20 ☑ to 31- Jul -20

Device: <All>

Operation: <All>

File modified: ☐ from 03-Aug-20 ☐ to 03-Aug-20

Size: > 0 < 0

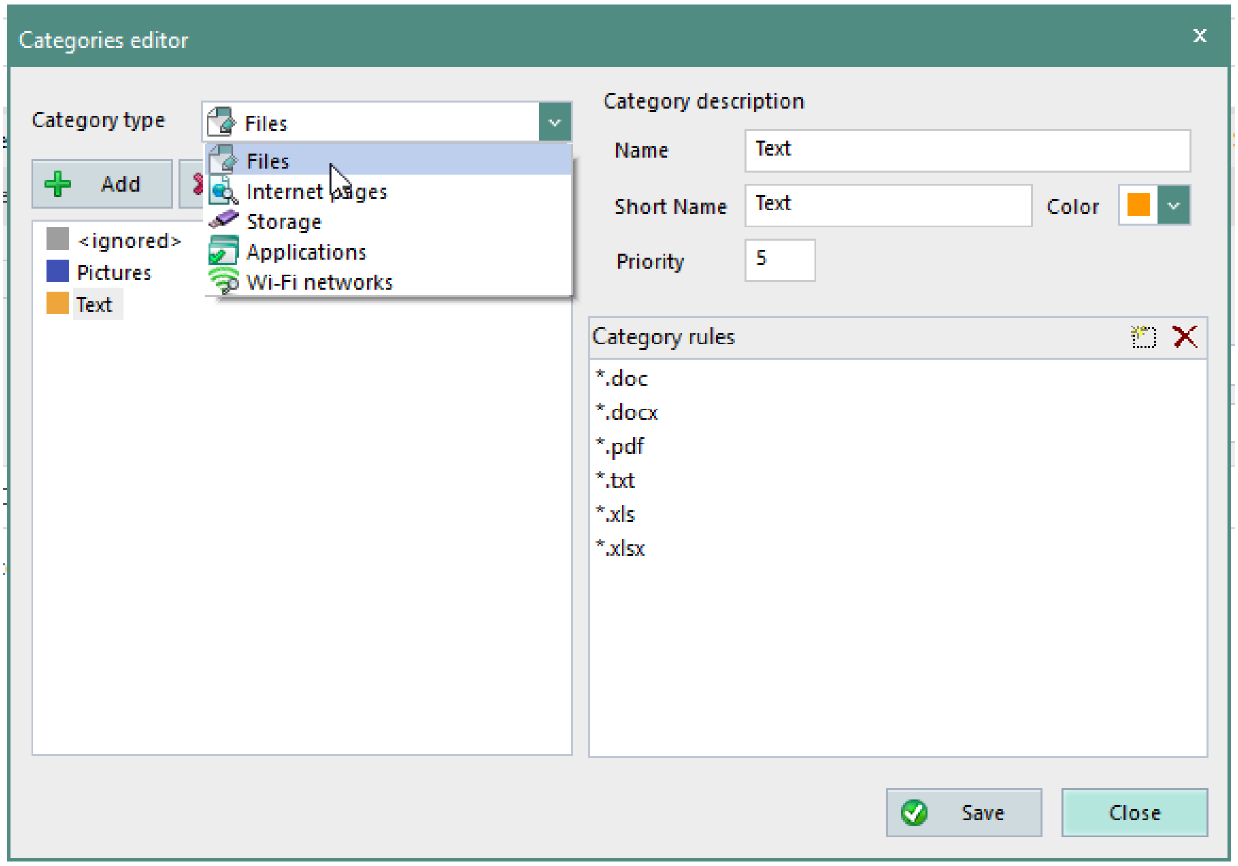
Name:

Figure 68. Displaying and filtering audit tables

1. **Database** (drop-down menu): display audit data from the database (default) or from an archive file. For details, see: Archiving or deleting old audit data
   Request data: get the current data in the database
2. Creating and editing categories to filter entries by categories. For details, see: Using categories
3. Print or export a current table
4. Show only data records where a shadowcopy exists
5. Hide entries for data that was read out only partially (applies only to files with **read** access, not **read/write**)

Using categories

Categories allow for distinguishing between different types of files, storage, Internet pages and applications. Assigning a color and rules to a category helps to find an item more quickly.
For example, for **Files** create **Text** and **Picture**, for **Applications** create **Text editing** and **Picture editing**.



Category type: Files

<ignored>
Pictures
Text

Category description

Name: Text

Short Name: Text

Color: 🟧

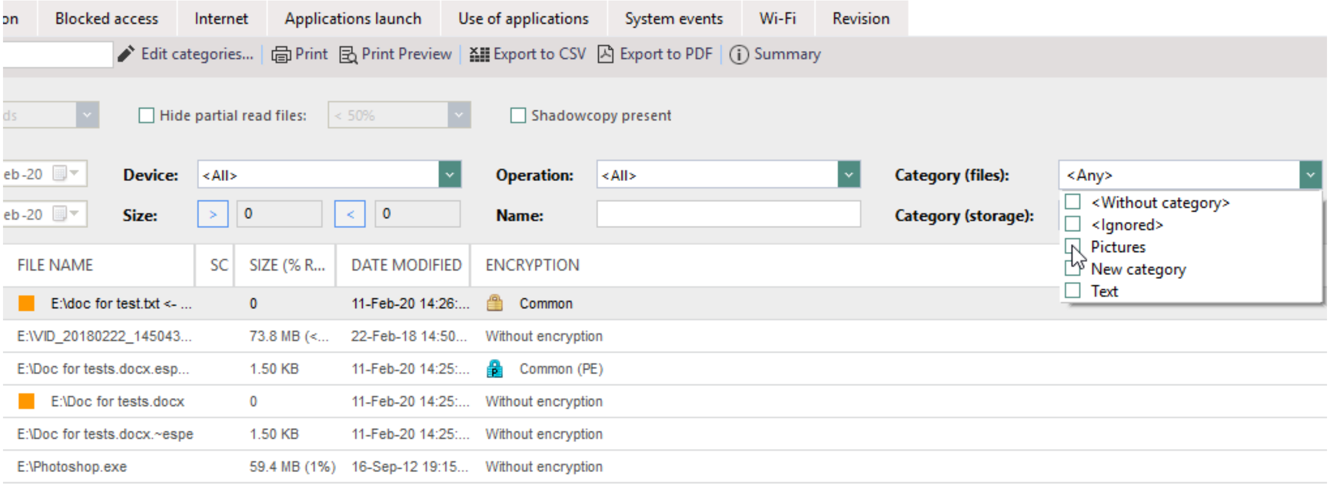
Priority: 5

Category rules

*.doc
*.docx
*.pdf
*.txt
*.xls
*.xlsx

Figure 69.Creating and editing categories

Entries that match the category are marked in color. You can also filter entries based on categories:



□ Hide partial read files: < 50% □ Shadowcopy present

Device: <All> Operation: <All> Category (files): <Any>

Size: > 0 < 0 Name: Category (storage):

FILE NAME	SC	SIZE (% R...	DATE MODIFIED	ENCRYPTION
🟧 E:\doc for test.txt <- ...		0	11-Feb-20 14:26:...	Common
E:\VID_20180222_145043...		73.8 MB (<...	22-Feb-18 14:50...	Without encryption
E:\Doc for tests.docx.esp...		1.50 KB	11-Feb-20 14:25:...	Common (PE)
🟧 E:\Doc for tests.docx		0	11-Feb-20 14:25:...	Without encryption
E:\Doc for tests.docx.~espe		1.50 KB	11-Feb-20 14:25:...	Without encryption
E:\Photoshop.exe		59.4 MB (1%)	16-Sep-12 19:15...	Without encryption

Figure 70. Categorized file types marked with orange

Creating categories

1. Click **Edit categories** above an Audit table (not available under **Shadowcopy filter** and under **System events**).

   → The **Categories editor** dialog window opens.

2. In the **Category type** drop-down, select a type.

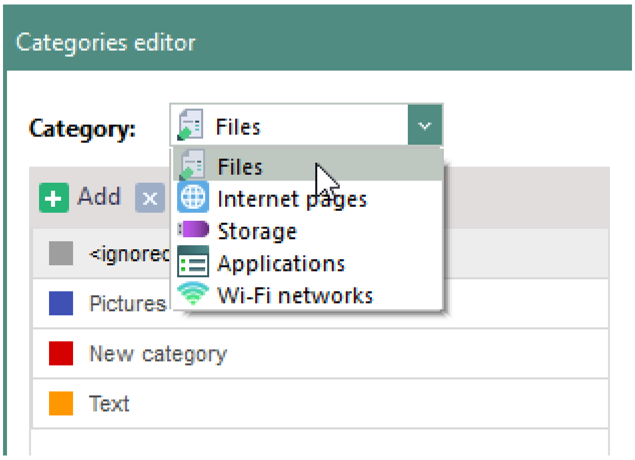
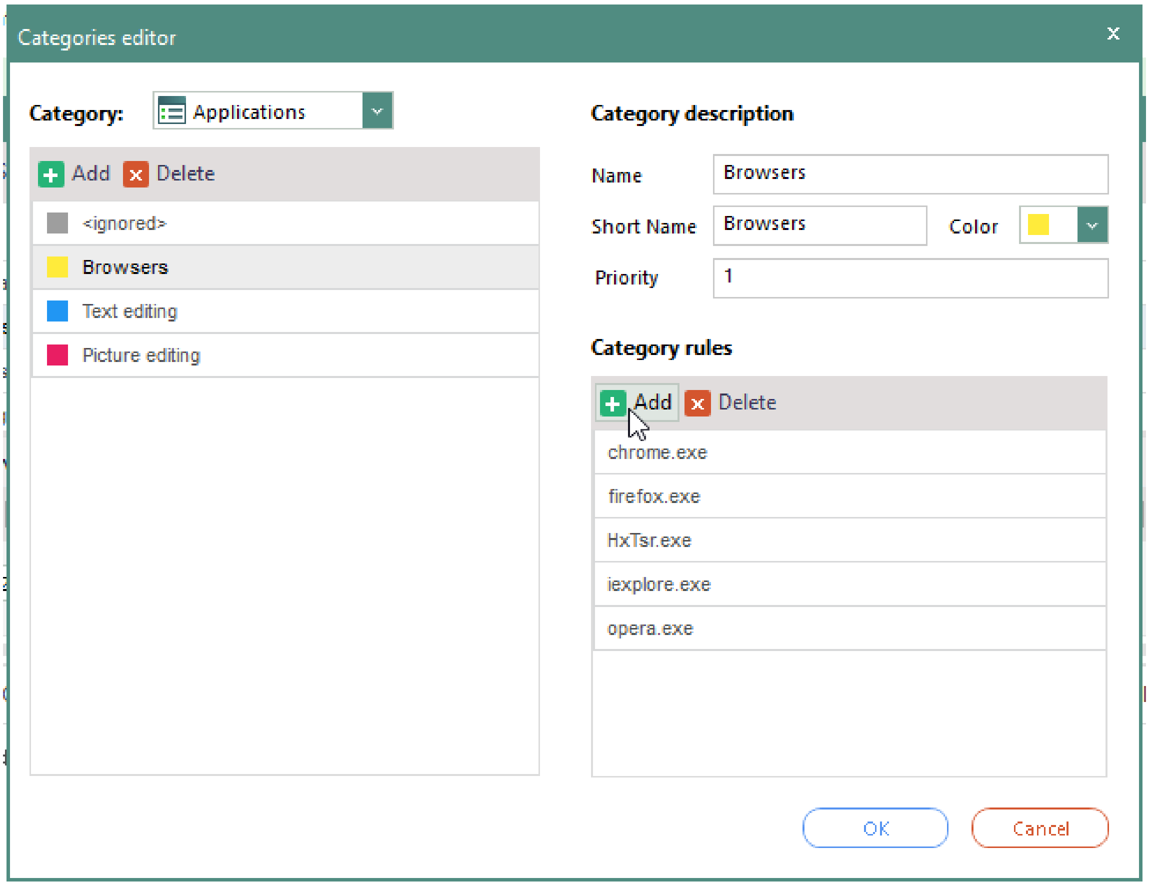


Figure 71. Selecting a category type

3. Click ➕ **Add**.

   → The **New category** entry appears on the left.

4. Specify the new category on the right:
   a. Enter a short name that will be displayed in the **Category** drop-down.
   b. Select a color to mark audit entries in the list.
   c. In the **Priority** field, define the position of a category in the list.
   d. Click **Add** to add a rule for a category. For details, see: Defining rules for categories



Name: Browsers

Short Name: Browsers

Color: 🟨

Priority: 1

chrome.exe

firefox.exe

HxTsr.exe

iexplore.exe

opera.exe

Figure 72. Creating a rule for the new category "Browsers"

5. Click **OK** to save the changes and close the **Categories editor** dialog.

➥ The new category is active. Entries that comply with the rules are highlighted in color and can be filtered.

Defining rules for categories

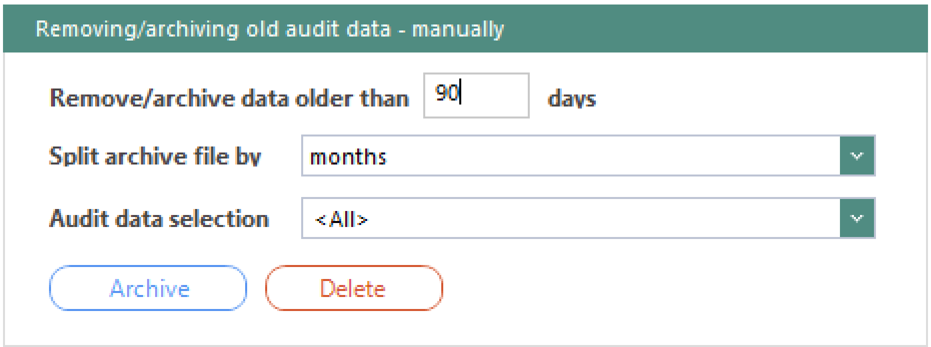
Category type	Rule definition
Files	File types of the format *.<ending> or specific files, e.g.: *.xml, egon.png
Applications	Application file name, e.g.: *chrome.exe*
Storage	Hardware ID + serial number, e.g.: *USB\VID_0951&PID_1666\60A44C3FAFE13090396D01E5&0*
Internet pages	Web addresses, e.g.: *www.google.com*, *EgoSecure.com*
WiFi networks	Wireless network name

Archiving or deleting old audit data

If database is overfilled, new audit data can NOT be stored there anymore. The solution is to archive or delete a part of audit data once manually or set up the archiving/deleting of old audit data so that it is performed regularly according to the scheduler.

Archiving/deleting Audit data manually

1. Go to **Administration | Administrator | Database maintenance**.
2. Configure the settings in the **Removing/archiving old audit data – manually** area:
   a. In the **Remove/archive data older than** field, specify how old the data must be to be archived/deleted.
   b. In the **Split archive file by** drop-down, select whether the archive data is split in separate files for each day/week/month/year.
   c. In the **Audit data selection** drop-down, select the types of audit data for archiving/deleting.
3. To permanently delete old data, click **Delete**.



Removing/archiving old audit data - manually

Remove/archive data older than 90 days

Split archive file by months

Audit data selection <All>

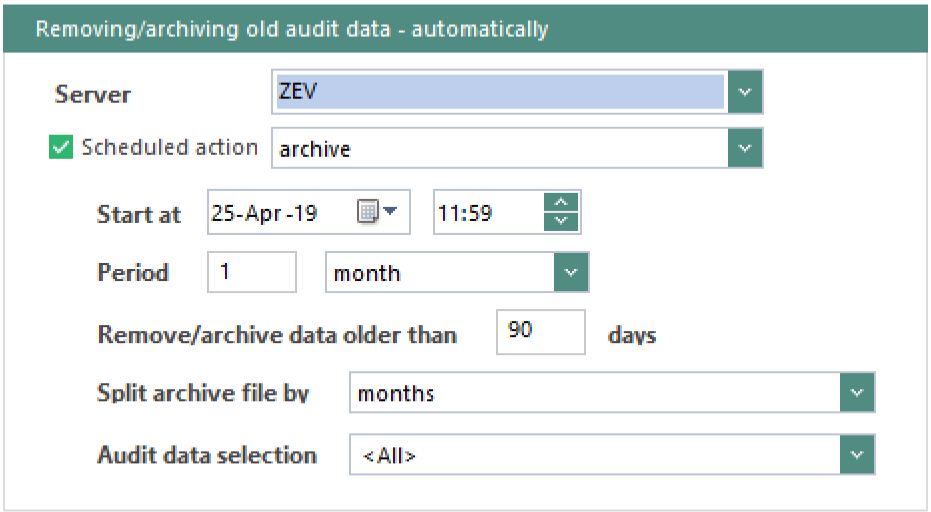
Figure 73. Manually archiving/deleting the Audit data

4. To archive old data, define an archive directory first and then click **Archive**.
5. Click **OK** in the warning dialog.

A message about data successfully archived/deleted appears under the **Database statistics** area.

Archiving/deleting Audit data automatically

1. Go to **Administration | Administrator | Database maintenance**.
2. In the **Removing/archiving old audit data – automatically** area, enable the **Scheduled action** check box and select the action from the drop-down menu (archive/delete).



Removing/archiving old audit data - automatically

Server: ZEV

☑ Scheduled action: archive

Start at: 25-Apr-19 11:59

Period: 1 month

Remove/archive data older than 90 days

Split archive file by: months

Audit data selection: <All>

Figure 74. Planned audit data archiving/deleting

3. Configure the action:
   a. In the **Start at** field, select the date and time when a synchronization process starts.
   b. In the **Period** field, define how often the synchronization is performed starting from the date defined in the previous step.
   c. In the **Remove/archive data older than … days** field, define how old the data must be to archive/remove it.
   d. In the **Split archive file by** drop-down, select whether the archive data is split in separate files for each day/week/month/year.
   e. In the **Audit data selection** drop-down, check the types of audit data for archiving/deleting.
   f. If you are using several EgoSecure Servers: In the **Server** drop-down, select the server that must perform the action.
4. Define an archive directory.
5. Save the settings.

The action is performed at the start time and is repeated according to the selected time interval.

Specifying directory for archive data

! The selected directory must be NOT a mapped network drive.

1. Go to **Administration | Administrator | Database maintenance**.
2. In the **Directory** field, select where archive files with audit data will be stored.
3. If a network directory was defined in the previous step, enter the respective user and password.
4. Save the settings.

Showing archive audit data

Archived .dat audit files can be opened in Console under:

- **User management/Computer management | Audit**
- **Reports | Audit**

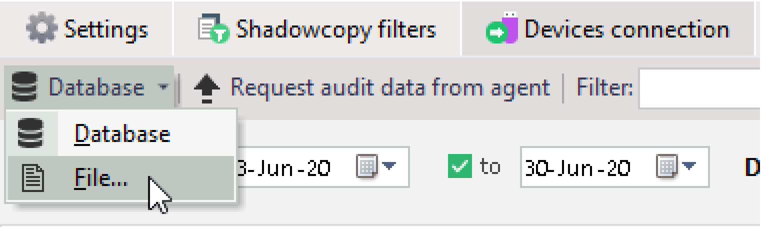


Figure 75. Showing archived audit data

4.4. Secure Audit - problems

Problem: Audit data is not displayed in real time.
Possible solutions:

- Check whether auditing functionality is enabled under **Product settings | Audit | Secure Audit**.
- Check the connection between Server and Agent. For details, see: Testing connection
- Check which audit data is enabled. For details, see: Selecting audit data, Activating Secure Audit for user or computer
- Check, whether the **Accept audit data** option is enabled in the **EgoSecure AdminTool**.

5. SHADOWCOPY

5.1. Shadowcopy – overview

Shadowcopy creates shadow copies of files used by users on external storage devices, thin client storage, network shares or cloud storage. The copies are first saved on the client computer and then transferred to the defined shadow copy server. The administrator can then access the shadow copies from the Console.
The usage of Shadowcopy is dependent from the Secure Audit module:

- To make it possible to activate **Shadowcopy** for a user/computer, enable auditing under **Product settings | Audit | Secure Audit**.
  For details, see: Activating Secure Audit
- As soon as you configure **Shadowcopy** for a storage, the audit of the file accesses to this storage location is also configured automatically.
  For details, see: Configuring Shadowcopy
- Once **Shadowcopy** is activated for a user/computer, the **Secure Audit** product is activated automatically, if it was not activated before.
  For details, see: Activating Shadowcopy for user/computer

Settings for shadow copies on special storage directories

Shadowcopy from…	Necessary settings
Network shares	Enable the option **Allow network shares control** under: ■ Administration | Clients | Client settings ■ Computer management | Settings | Client settings
Thin client storage	Enable the option **Allow thin client storage** control under: ■ Administration | Clients | Client settings ■ Computer management | Settings | Client settings
Cloud	Define controlled cloud storage types under **User management | Settings | Cloud storage**.

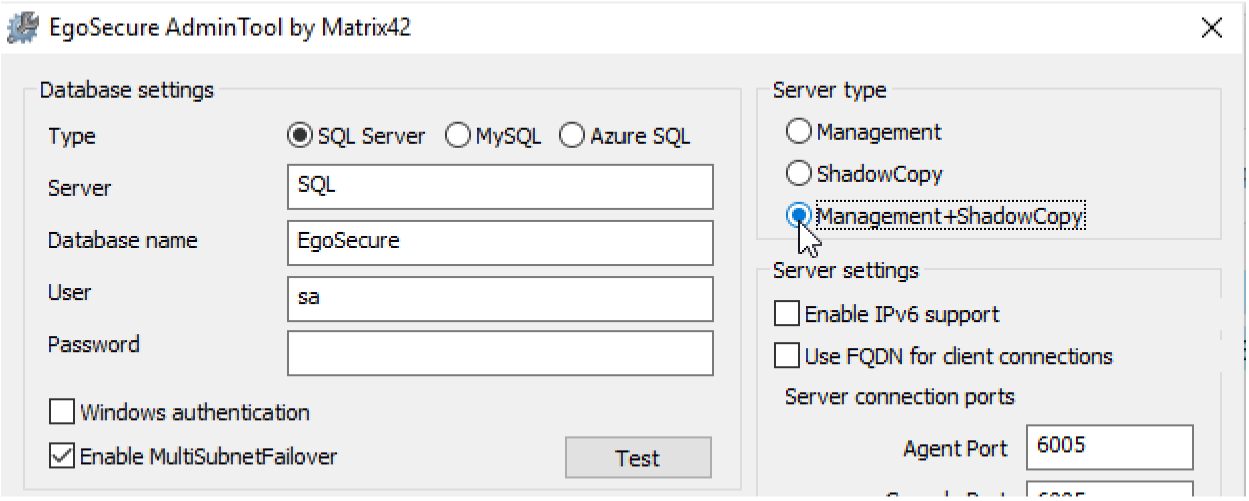
5.2. Configuring and activating Shadowcopy

Managing Shadowcopy server

You can use an existing EgoSecure Server as a shadow copy server or install/create a separate shadow copy server. During the installation specify which server type to use. You can change the setting later in the **AdminTool**.

Changing existing server type

1. Open the **AdminTool**. By default, the application is located in the **EgoSecure Server** folder in the EgoSecure installation directory.
2. Under **Server type**, enable the **Management+ShadowCopy** radio button.



EgoSecure AdminTool by Matrix42

Database settings

Type ● SQL Server ○ MySQL ○ Azure SQL

Server: SQL

Database name: EgoSecure

User: sa

Password:

□ Windows authentication

☑ Enable MultiSubnetFailover

Server type

○ Management

○ ShadowCopy

● Management+ShadowCopy

Server settings

□ Enable IPv6 support

□ Use FQDN for client connections

Server connection ports

Agent Port: 6005

Figure 76. AdminTool

3. In the lower area, enable the **Accept audit data** and **Accept shadowcopy data** checkboxes.
4. Click **Save** and close the **AdminTool**.

➥ You can now use the current EgoSecure Server installation as a shadowcopy server and configure Shadowcopy.

If you use multiple shadowcopy servers, you can set a preferred shadowcopy server for each client.

Setting up a preferred shadowcopy server

1. In Console, go to **Installation | EgoSecure agents | Install/Update**.
2. In the **Install/Update** area, select an Agent. To select multiple Agents, hold down `Ctrl` and click.
3. Select **Favorite ShadowCopy Server | [server name]** from the context menu.

➥ The selection appears in the **Favorite SC server** column.

Configuring Shadowcopy

To use Shadowcopy, decide the following:

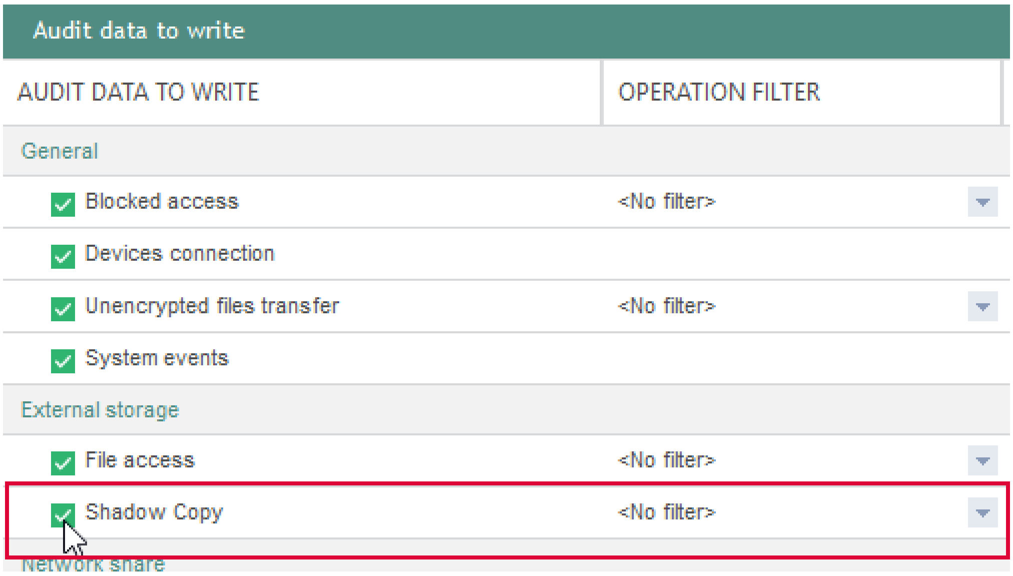
- from which storage types Shadow copies must be created
- of which types Shadow copies must be created
- where to store Shadow copies

Finally: enable Shadowcopy for user and computer.

Applying global settings for shadow copies

1. Open the Console and go to **Product settings | Audit | Secure Audit**.
2. Select the locations from where shadow copies must be made.

→ If you enable a shadow copy, the audit of file accesses of this device type enables automatically.



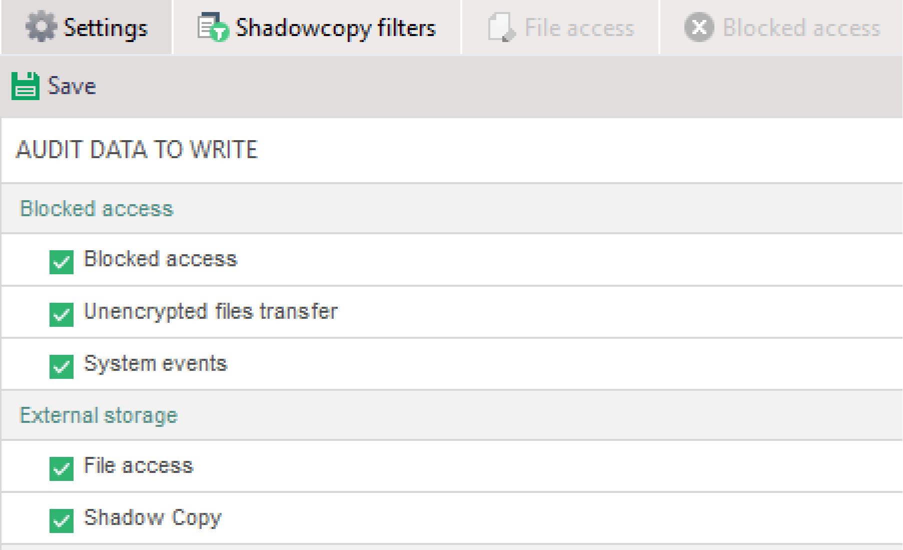
Audit data to write

AUDIT DATA TO WRITE	OPERATION FILTER
General	
☑ Blocked access	<No filter>
☑ Devices connection	
☑ Unencrypted files transfer	<No filter>
☑ System events	
External storage	
☑ File access	<No filter>
☑ Shadow Copy	<No filter>
Network share	

Figure 77. Selecting ShadowCopy

3. If needed, in the **Operation filter** column, select the operation for which no shadow copy must be created.
4. Click **Save**.

The selection is inherited to default users, default computers and all users/computers:



AUDIT DATA TO WRITE
Blocked access
☑ Blocked access
☑ Unencrypted files transfer
☑ System events
External storage
☑ File access
☑ Shadow Copy

Figure 78. Enabling ShadowCopy for a default user

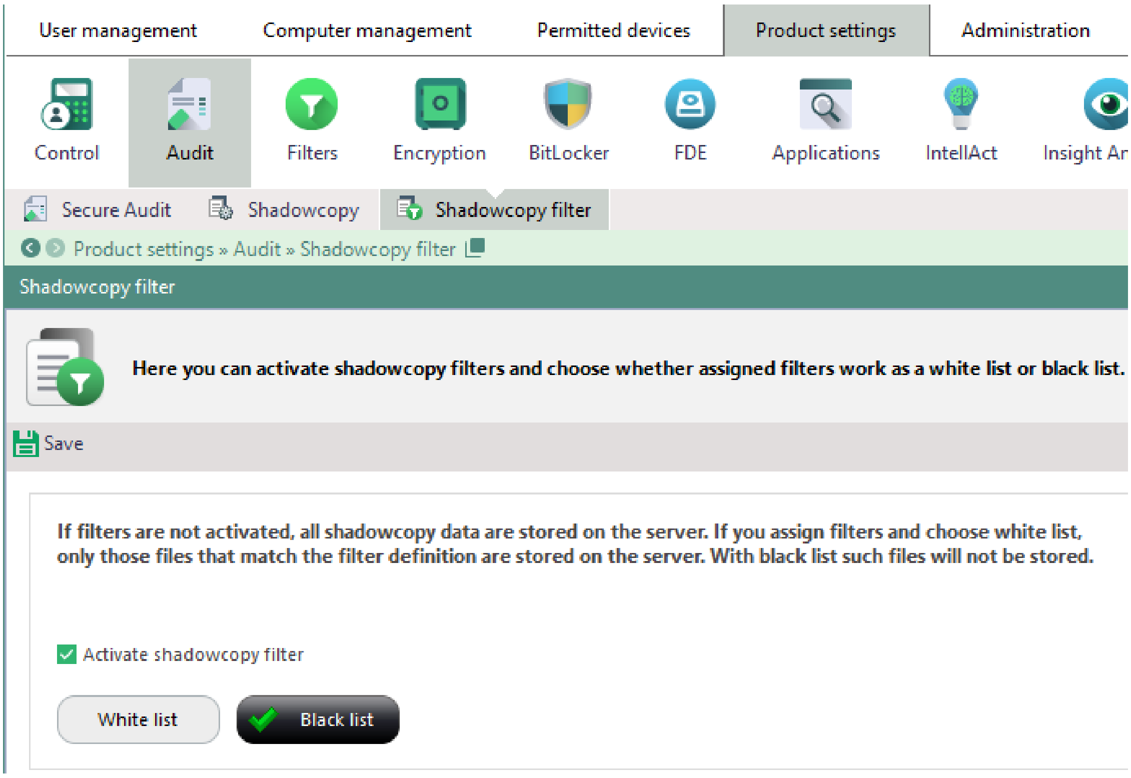
Shadowcopy filter

You can limit or exclude shadow copies of certain file types. To limit and exclude, specify how shadowcopy filters work (blacklist or whitelist) and assign the filters globally (using default policies) or individually (to user/computer). For details, see: Filters

Configuring file filter for shadow copies

1. Go to **Product settings | Audit | Shadowcopy filter**.
2. Enable the **Activate shadowcopy filter** check box.
3. Select how shadowcopy filters work:

- **White list**: Only files that match the filter definitions are copied to the server.
- **Black list**: Files that match the filter definitions are not copied to the server. All other files are copied.



Here you can activate shadowcopy filters and choose whether assigned filters work as a white list or black list.

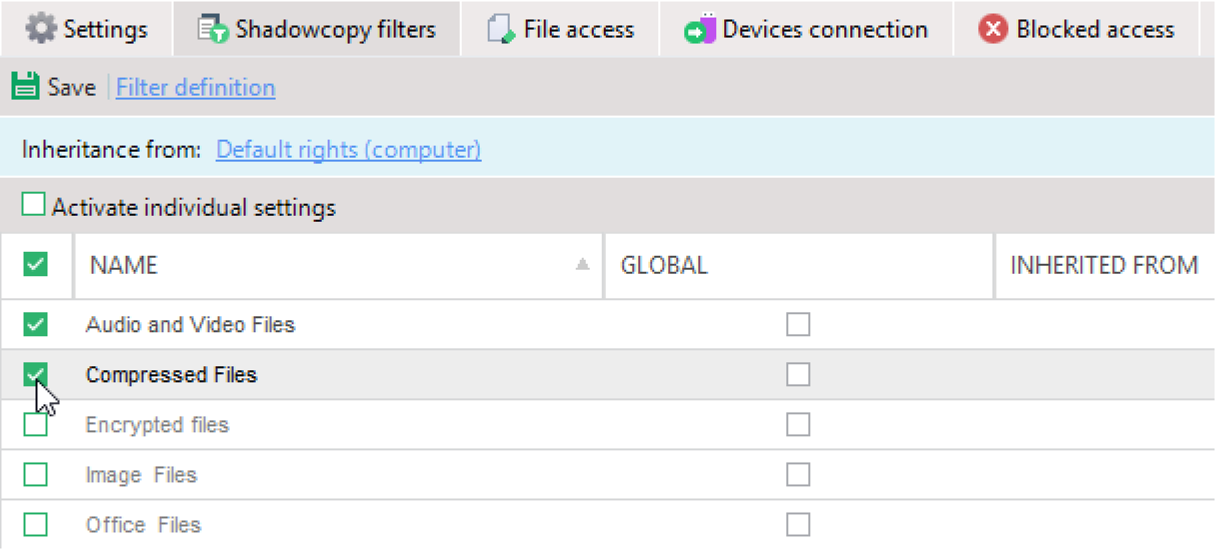
If filters are not activated, all shadowcopy data are stored on the server. If you assign filters and choose white list, only those files that match the filter definition are stored on the server. With black list such files will not be stored.

☑ Activate shadowcopy filter

Figure 79. Enabling and configuring filter for Shadowcopy

4. If necessary, create a new filter under **Product settings | Filters | File type filters**. Filters created there can be used for both **Access Control** and **ShadowCopy**.
5. Click **Save**.

You can now assign filters for shadow copy. For details, see: Activating shadowcopy for user/computer



Inheritance from: Default rights (computer)

□ Activate individual settings

☑	NAME	GLOBAL	INHERITED FROM
☑	Audio and Video Files	□	
☑	Compressed Files	□	
□	Encrypted files	□	
□	Image Files	□	
□	Office Files	□	

Figure 80. Assigning a filter for shadowcopy

Adjusting storage settings for shadow copies on the Server

1. Go to **Product settings | Audit | Shadowcopy**.
2. To change the location of shadow copies on the server,
   a. Click **Browse** in the **Shadowcopy server settings** area.
   b. In the **Simultaneous clients** field, define from how many Agents shadowcopy uploads can be performed simultaneously.
   c. In the **Maximum net load** field, specify the permitted maximum network load for shadowcopy uploads. E.g.: if network has a transmission rate of 100 Mbit/sec and we define the maximum network load as 30%, shadowcopy uploads can use only network transmission rate not higher than 30 Mbit/sec.
   d. To automatically delete shadow copies from the server after a certain time, enable the **Delete after...** checkbox and enter the number of days after which the deletion occurs.

   → As soon as a shadow copy is older than **x** days, it is automatically deleted from the server.

3. To change the location of shadow copies,
   a. Click **Browse** in the **Shadowcopy client settings** area.
   b. Under **How much disk space can be used for the Shadowcopy**, define how many % or GB of the hard disk space/partition can be used for shadow copies on the Client.
   c. Select when to copy files to the Server:
      - **Immediately**: The shadow copy is copied to the Server immediately after creation and can be opened/saved via the Console.
      - **After computer start**: The shadow copy is copied to the Server after the client restart and can be downloaded via the Console.
      - **Scheduled**: Shadow copies are copied to the Server once a day at the specified time and can be downloaded via the Console.

- **By request**: The shadow copy becomes available for downloading on the Server only if under **User management**/**Computer management | Audit | File access** tab an audit entry is right-clicked and **Increase upload priority** option is selected.

4. Specify an upload retry interval to repeat a sending of a file copy from Agent to Server one more time if a previous upload failed.
5. Click **Save**.

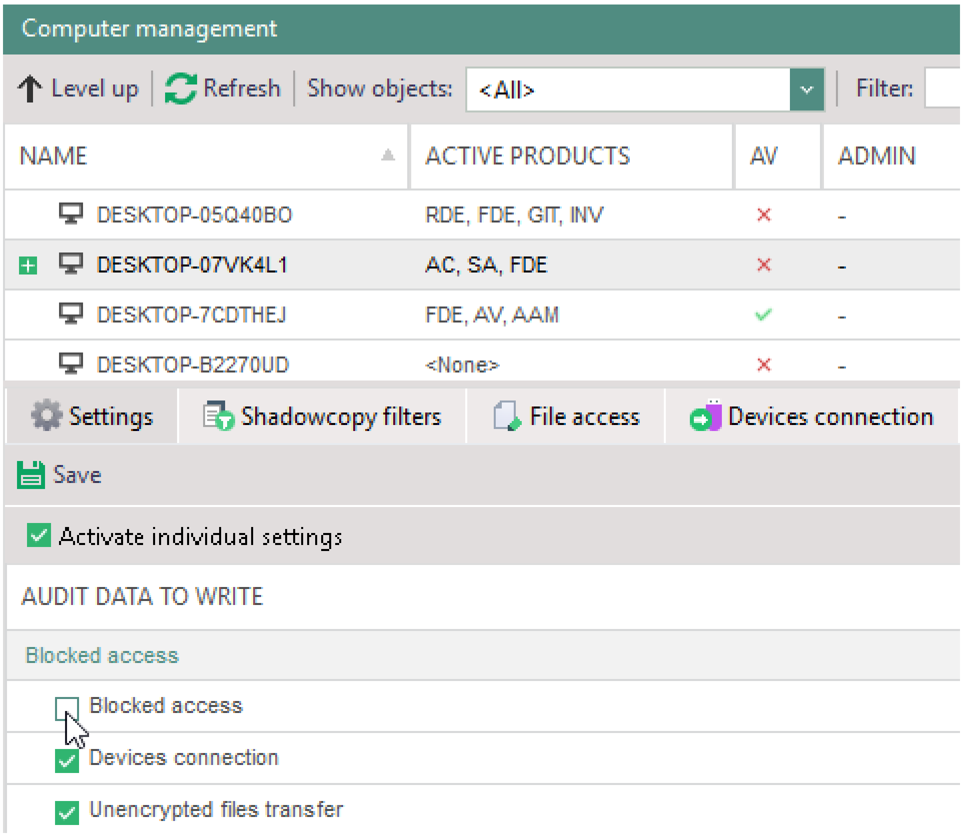
The settings are applied.

Activating shadowcopy for user/computer

1. Go to **User management/Computer management | Audit**.
2. Right-click a user/computer and select **Activate/deactivate products | Shadow Copy**.
3. Open the **Settings** tab in the lower area.

   → The user automatically inherits the Shadow Copy settings of a default user.

4. To define individual shadow copy settings for the user/computer and to deactivate shadow copy for certain storage locations, enable the **Activate individual settings** check box and disable the corresponding shadow copy check boxes.



NAME	ACTIVE PRODUCTS	AV	ADMIN
DESKTOP-05Q40BO	RDE, FDE, GIT, INV	✗	-
DESKTOP-07VK4L1	AC, SA, FDE	✗	-
DESKTOP-7CDTHEJ	FDE, AV, AAM	✓	-
DESKTOP-B2270UD	<None>	✗	-

☑ Activate individual settings

AUDIT DATA TO WRITE

Blocked access

□ Blocked access

☑ Devices connection

☑ Unencrypted files transfer

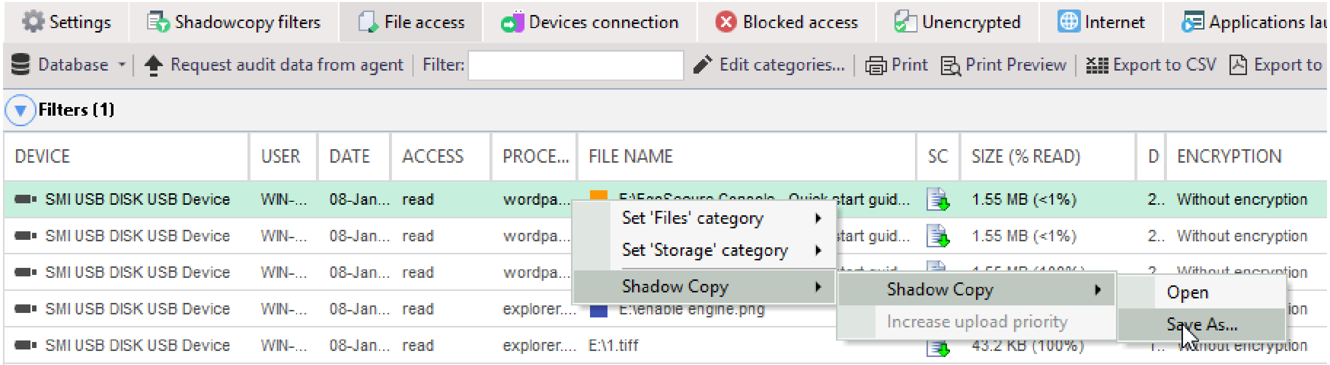
Figure 81. Individual ShadowCopy settings for directory service computers

5. To apply a file type filter to shadow copies, enable the filter in the **Shadowcopy filters** tab. For details, see: Shadowcopy filter
6. Click **Save**.

5.3. Opening and saving shadow copies

You can open or save shadow copies in the following areas:

- **User management/Computer management | Audit | File access** and **Unencrypted**
- **Reports | Audit | File access**



DEVICE	USER	DATE	ACCESS	PROCE...	FILE NAME	SC	SIZE (% READ)	D	ENCRYPTION
SMI USB DISK USB Device	WIN-...	08-Jan...	read	wordpa...	E:\EgoSecure Console - Quick start guid...		1.55 MB (<1%)	2..	Without encryption
SMI USB DISK USB Device	WIN-...	08-Jan...	read	wordpa...	start guid...		1.55 MB (<1%)	2..	Without encryption
SMI USB DISK USB Device	WIN-...	08-Jan...	read	wordpa...	start guid...		1.55 MB (100%)	2..	Without encryption
SMI USB DISK USB Device	WIN-...	08-Jan...	read	explorer....	E:\enable engine.png				ion
SMI USB DISK USB Device	WIN-...	08-Jan...	read	explorer....	E:\1.tiff		43.2 KB (100%)	1..	Without encryption

Figure 82. Downloading shadow copies

Opening or saving shadow copy

- In the **SC** column, click on and select **Open** or **Save as**.

If in the shadow copy settings the **By request** option is selected, the following symbol is displayed in the **SC** column:

- In the context menu, select **Shadowcopy | Increase upload priority**.

The appears the symbol and the copy can now be downloaded.

6. APPLICATION CONTROL

6.1. Application Control – overview

Application Control (APC) works in two modes: the **Application packages** mode and the **Trusted installer package** mode. The modes can be used either separately or can be combined. Each of the modes can be supplemented with additional functionality: trusted objects, additionally controlled file types, demo mode.

Criteria	Application packages mode	Trusted installer package mode
General description	Application packages are packages that contain any number of allowed (or blocked) applications.	Trusted installer package is a package of allowed applications which consists of two packages: an *initial package* and the so-called *monitored trusted installer package*.
Working with the modes		
Criteria for identifying applications in packages	🟩 Hash value	🟩 Vendor 🟩 Certificate 🟩 Original file name
Assigning packages to directory objects	You can assign application packages to any directory service object (users/computers/group). With the Global package you summarize applications that are allowed/blocked for all directory objects where the Application Control product is activated. **!** Using the **Application packages** mode if APC is activated for a user: the Application packages are assigned to a USER. E.g.: if a user logs in to comp1 and comp2, a single (user-specific) application package is applied on both comp1 and comp2.	You can assign the Trusted installer package to any directory service object (users/computers/group). **!** Using the **Trusted installer package** mode if APC is activated for a user: the Trusted installer package is assigned to a COMPUTER. E.g.: if a user logs in to comp1 and comp2, different (computer-specific) packages are applied on comp1 and on comp2. Make sure that the Trusted installer engine is enabled on computers where user logs in.
Applying package restrictions	Restrictions based on application packages take effect shortly after activating the **Application Control** product for a directory service object (user/computer/group).	Restrictions based on the Trusted installer package take effect shortly after activating the **Application Control** product for a directory service object (user/computer/ group) and enabling the Trusted installer engine.

Configuring settings	In the Settings, you determine whether only the applications from packages are allowed and all others are blocked (whitelist) or whether the applications from packages are blocked and all other applications are allowed (blacklist).	In the Trusted installer settings, you define the list of trusted installers. The Trusted installer mode allows the applications only if they are installed and updated only by the defined trusted installers.
Managing application updates	Once an application from a package is updated, the application package must be modified manually. No real-time monitoring is performed. ! Modify an application package manually once an application is updated. Otherwise, such an application is recognized as an unknown one and will be blocked.	Once an application from a package is updated, the trusted installer package is updated automatically due to the real-time monitoring. If application is from the initial package, update the initial package manually via rescanning under Computer management | Applications | Trusted installer. ! Make sure the Trusted installer engine is enabled to perform the monitoring in real time.
Supported additional Application Control settings		
Additionally controlled file types:		
Dynamic link libraries (DLL)	+	–
Java archives (JAR)	+	+
Demo mode	+	+
Trusted objects	+	+
Block applications with broken signature	+	+

Combining Application packages and Trusted installer package modes

Enabled modes and settings	Result
Application packages (whitelist) + Trusted Installer + Trusted objects	Applications that are allowed either via Application packages or via Trusted Installer or via Trusted objects are pemitted to be launched.

Application packages (blacklist) + Trusted Installer + Trusted objects	Applications allowed either via Trusted objects are pemitted to be launched. Trusted installer has a priority over blocking via the Trusted Installer and the Application packages. -or- Applications allowed via Trusted installer and not blocked via Application packages are pemitted to be launched.
Application packages (learning mode) + TI	Learning mode works as usually, Trusted Installer is ignored.

6.2. Setting up Application Control

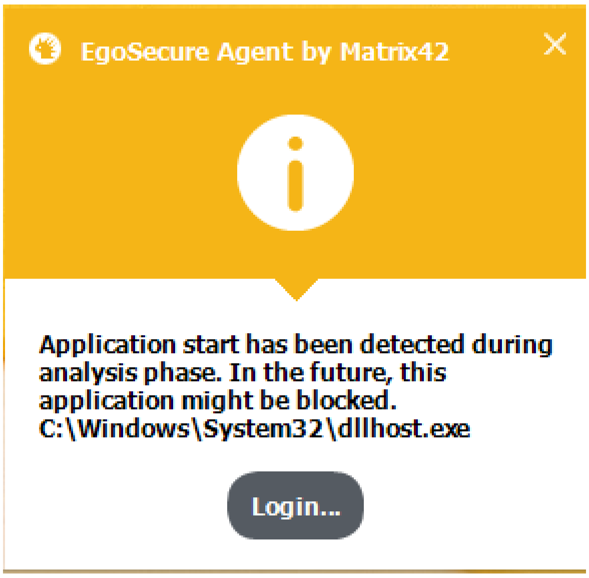
Enabling additional control of other file types

Define file types which will be controlled in addition to applications (executable files).
In the **Application packages** mode, you can control both DLL and JAR.
In the **Trusted installer package** mode, you can control only JAR.
Pay attention that the control of java archives can decrease the performance on the Agent side.

! ATTENTION	**Avoiding functional restrictions with enabled DLL control** Since DLLs of some applications are loaded dynamically (only when required), they are difficult to log in advance. This makes it difficult for you to allow them and can result in unlisted DLLs being blocked and the functionality of certain applications being restricted. ◆ If possible, use the list of trusted objects instead of DLL control. In this way you reduce the administrative effort and avoid functional restrictions. For details, see: Defining a list of trusted objects

Using demo mode for test purposes

Demo mode is enabled by administrators to test how Application Control works before enforcing it in the company. During the period when the demo mode is enabled, full functionality of the Application Control product is used, but with only one exception: forbidden applications are not blocked on a user side and a user sees a warning message.



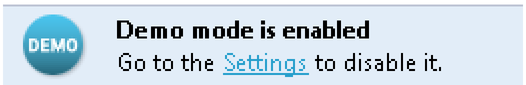
Application start has been detected during analysis phase. In the future, this application might be blocked.
C:\Windows\System32\dllhost.exe

Figure 83. User message when starting a not permitted application in demo mode

Enabling demo mode

1. Navigate to **Product settings | Applications | Settings**.
2. In the **Demo mode** area, enable the **Demo mode** check box.
3. Click **Save**.

   → The demo mode is now enabled. Under **Product settings | Applications** and under **User management/Computer management | Applications**, the following warning is shown:



Demo mode is enabled
Go to the Settings to disable it.

You can now create application packages, assign packages to objects and thus test the configuration.
See also: Customizing user messages

Defining a list of trusted objects

Trusted objects are defined to permit users the launch of applications even if they are blocked by application packages or by the Trusted installer package. Directories, manufacturers and file owners can be classified as trustworthy sources.

Adding trusted objects

1. Go to **Product settings | Applications | Trusted objects**.
   The list already contains predefined objects. If needed, enable them.
2. In the toolbar, click on one of the buttons:

Button	Description
Add directory	Specify a directory where permitted applications are located. Applications, DLLs and Java archives of this directory are allowed. - If the **Application Control** product is enabled for a user, the trusted directory %temp% is translated as `C:\Users\USERNAME\AppData\Local\Temp` - If the **Application Control** product is enabled for a computer, the trusted directory %temp% is translated as `C:\Windows\Temp` ! Trusted objects added via user environment variables (e.g.: %username%, %appdata%) do not apply in case of activating Application Control for a computer.
Add owner	Select a user from a directory structure who is permitted to access applications where he is an owner. To view an application owner, right-click an application in Windows Explorer (Properties | Security tab | Advanced). Applications, DLLs and Java archives of this owner are permitted.
Add vendor	Scan local computer, Agents and network computers for available vendors and add vendors as trusted ones. Selected datatypes (applications, DLLs, Java archives) of this developer are permitted.

3. Click **Save**.

ATTENTION	**Disabling Microsoft default vendors** Disabling the Microsoft default vendors might result in performance problems and problems with Windows update on Clients.

Blocking applications with broken signature

If the control of applications with broken signature is enabled, the applications, DLLs and java archives with a broken signature will be blocked.

1. Navigate to **Product settings | Applications | Settings**.
2. In the **Control applications with broken signature** area, check the **Block applications with broken signature** box.
3. Click **Save**.

➔ Now all applications where the signature is broken will be blocked.

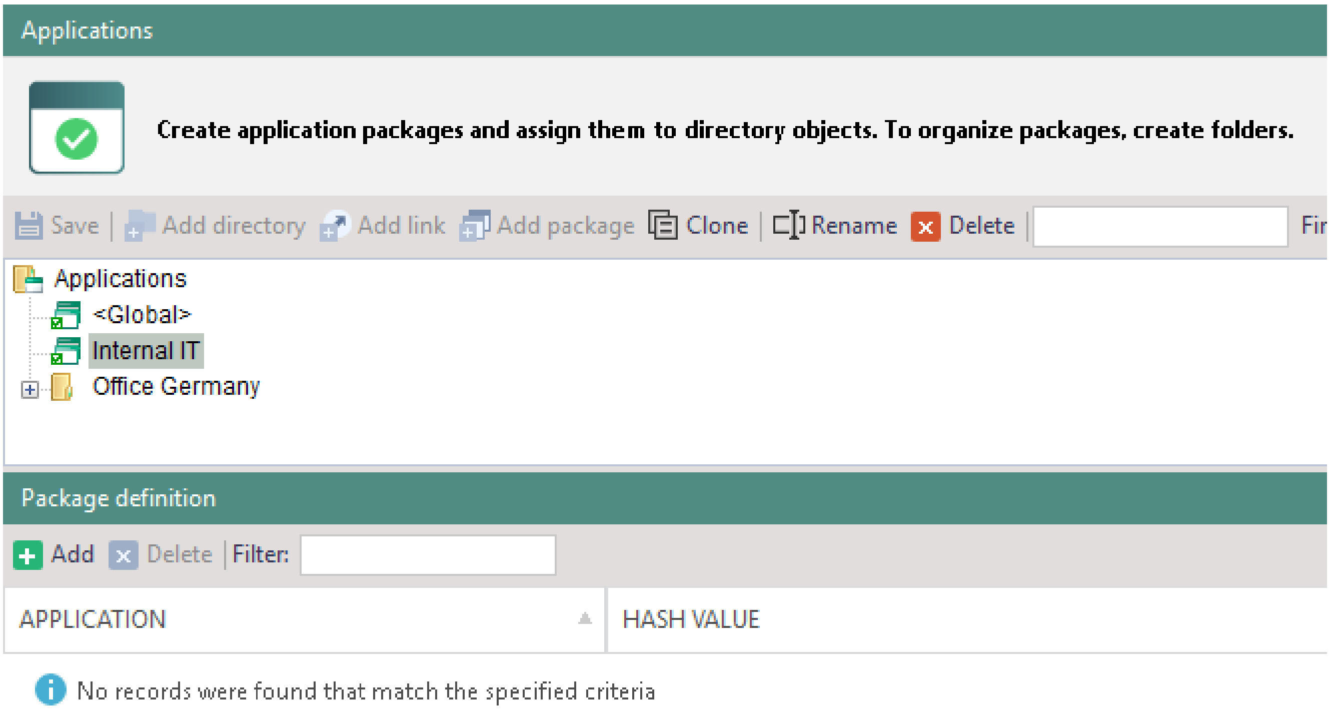
6.3. Working with Application Control: the Application packages mode

Creating an application package

Creating a new package

1. Under **Product settings | Applications | Settings**, in the **List type** area, select a mode according to which all application packages work:
   - **Whitelist** is a list of permitted applications. Access to non-listed applications is blocked.
   - **Blacklist** is a list of applications access to which is blocked. Access to non-listed applications is allowed.
2. Click **Save**.
3. Go to **Product settings | Applications | Application packages**.
   Existing packages are organized in a tree structure. The **<Global>** package is available by default and automatically assigned to all users/computers.
4. Click **Add package** on the toolbar.
   → The new package appears in the tree structure.
5. Enter a package name.

The package can now be filled. In the **Package definition** area, the contents of a selected package is listed:


Applications

Create application packages and assign them to directory objects. To organize packages, create folders.

APPLICATION	HASH VALUE

No records were found that match the specified criteria

Figure 84. New, empty application package

Filling an application package

You have several options to add applications/DLLs/Java archives to packages:

- Scanning Client computers
- Adding objects from launch history
- Learning mode (without **Secure Audit**)

ATTENTION	**Filling the Global package** If you fill in the existing **Global** package, the inserted package files apply to all users and computers, since the package is automatically assigned to all objects of the directory service structure and cannot be removed.

Scanning Client computers for applications/DLLs/Java archives

Search for applications ever launched on computers, dynamic link libraries (DLL) and java archives (JAR). Only online computers with Agents can be scanned.

1. Under **Product settings | Applications | Application packages**, select a package.
2. In the **Package definition** work area, click **Add**.

   → The **Search files** dialog appears.

3. In the **Source** column, select a computer with an online Agent where the search will be performed.
4. In the **Files type** drop-down box, select whether to search for *.exe, *.dll, *jar or all files.

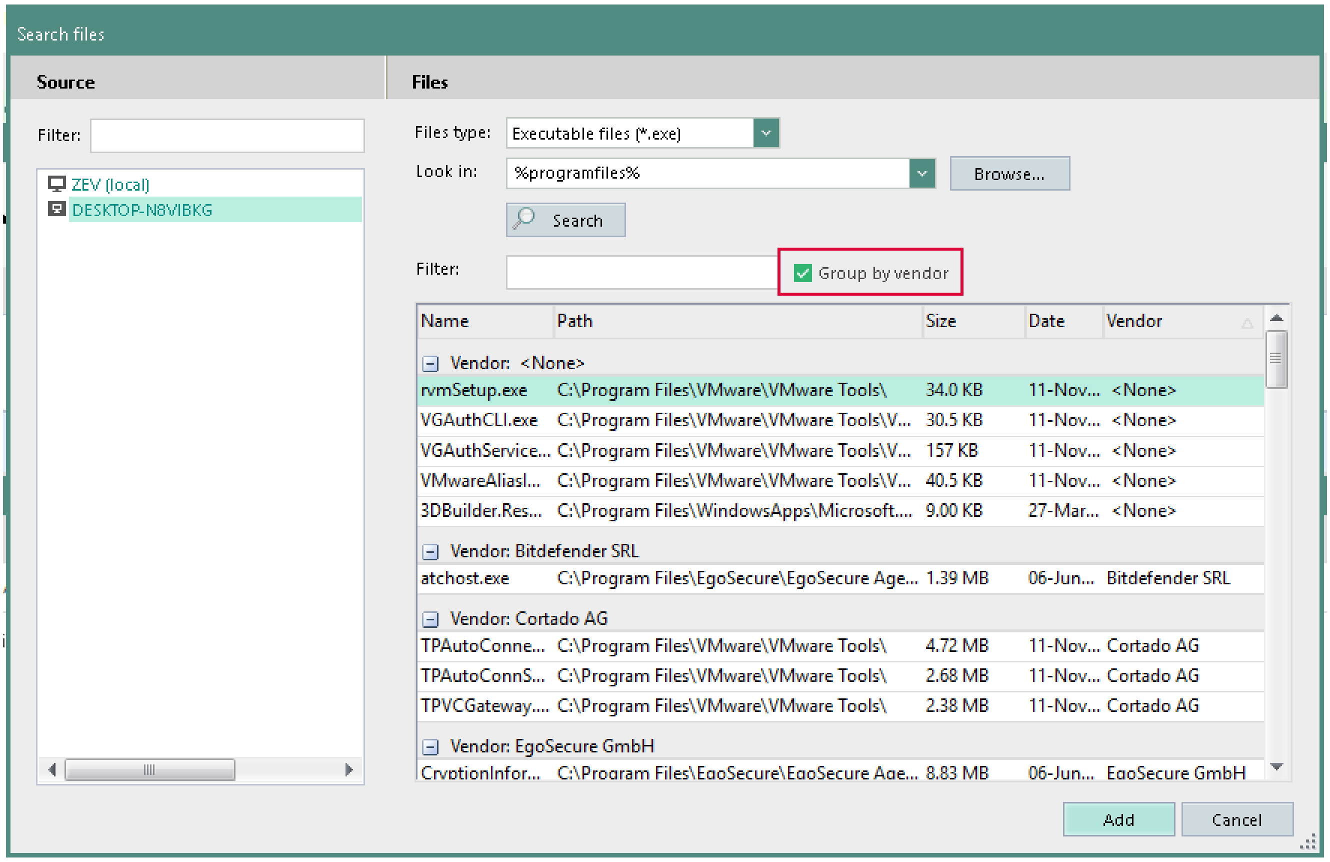
! The **All files** filter finds all file types, but only .exe, .jar and .dll (also other file types that refer to them) are supported.

5. Click **Search**.

   → The scan starts. Found files are listed. You can filter the search results by a term or group them by a manufacturer. Objects that are already in a package are highlighted in bold.

! The **Browse** button is active only when searching on local Agents.

! Encrypted files are not scanned as the scan runs from the system.



Search files

Source

Filter:

- ZEV (local)
- DESKTOP-N8VIBKG

Files

Files type: Executable files (*.exe)

Look in: %programfiles%

Filter:

☑ Group by vendor

Name	Path	Size	Date	Vendor
⊟ Vendor: <None>				
rvmSetup.exe	C:\Program Files\VMware\VMware Tools\	34.0 KB	11-Nov...	<None>
VGAuthCLI.exe	C:\Program Files\VMware\VMware Tools\V...	30.5 KB	11-Nov...	<None>
VGAuthService...	C:\Program Files\VMware\VMware Tools\V...	157 KB	11-Nov...	<None>
VMwareAliasI...	C:\Program Files\VMware\VMware Tools\V...	40.5 KB	11-Nov...	<None>
3DBuilder.Res...	C:\Program Files\WindowsApps\Microsoft....	9.00 KB	27-Mar...	<None>
⊟ Vendor: Bitdefender SRL				
atchost.exe	C:\Program Files\EgoSecure\EgoSecure Age...	1.39 MB	06-Jun...	Bitdefender SRL
⊟ Vendor: Cortado AG				
TPAutoConne...	C:\Program Files\VMware\VMware Tools\	4.72 MB	11-Nov...	Cortado AG
TPAutoConnS...	C:\Program Files\VMware\VMware Tools\	2.68 MB	11-Nov...	Cortado AG
TPVCGateway....	C:\Program Files\VMware\VMware Tools\	2.38 MB	11-Nov...	Cortado AG
⊟ Vendor: EgoSecure GmbH				
CryptionInfor...	C:\Program Files\EgoSecure\EgoSecure Age...	8.83 MB	06-Jun...	EgoSecure GmbH

Figure 85. Searching applications

6. Select an entry from the list and click **Add**. To select multiple elements, hold down `Ctrl` and click on objects.

   → The dialog closes. Selected entries appear in the **Package definition** area. The calculated hash value in the **Hash value** column uniquely identifies the application on all Clients.

7. Click **Save**.

➥ You can now assign the package to users, computers or groups.

Adding previously started objects from a launch history

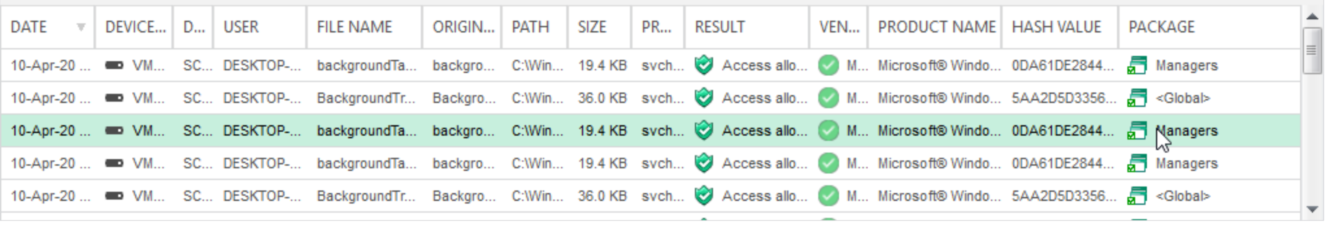
! If you do not have the **Secure Audit** product, you can view previously started objects and add them to packages only if you previously enabled the learning mode. For details, see Learning mode

1. Under **User management/Computer management | Applications**, select a user/computer from the directory service structure.
2. In the lower area, click on the **Applications launch** tab.
3. Filter the table if needed. For details, see: Showing audit data
4. Right-click an audit entry and select **Add to package** from the context menu.

   → The **Select object** dialog appears.

5. Select a package and click **OK** to confirm.

   In the **Package** column of the entry, the package name appears.



DATE	DEVICE...	D...	USER	FILE NAME	ORIGIN...	PATH	SIZE	PR...	RESULT	VEN...	PRODUCT NAME	HASH VALUE	PACKAGE
10-Apr-20 ...	VM...	SC...	DESKTOP-...	backgroundTa...	backgro...	C:\Win...	19.4 KB	svch...	Access allo...	M...	Microsoft® Windo...	0DA61DE2844...	Managers
10-Apr-20 ...	VM...	SC...	DESKTOP-...	BackgroundTr...	Backgro...	C:\Win...	36.0 KB	svch...	Access allo...	M...	Microsoft® Windo...	5AA2D5D3356...	<Global>
10-Apr-20 ...	VM...	SC...	DESKTOP-...	backgroundTa...	backgro...	C:\Win...	19.4 KB	svch...	Access allo...	M...	Microsoft® Windo...	0DA61DE2844...	Managers
10-Apr-20 ...	VM...	SC...	DESKTOP-...	backgroundTa...	backgro...	C:\Win...	19.4 KB	svch...	Access allo...	M...	Microsoft® Windo...	0DA61DE2844...	Managers
10-Apr-20 ...	VM...	SC...	DESKTOP-...	BackgroundTr...	Backgro...	C:\Win...	36.0 KB	svch...	Access allo...	M...	Microsoft® Windo...	5AA2D5D3356...	<Global>

Figure 86. Application packages of executed applications

Using the learning mode

If you are not using the **Secure Audit** product, you can use the learning mode to log a history of started applications.
All background and foreground applications started by the selected user/computer are logged. You can then add them to a package. For details, see: Adding objects from launch history.

Enabling the learning mode

1. Under **User management/Computer management | Applications**, select a user/computer.
2. Navigate to the **Applications** tab.
3. On the toolbar, click **Start learning mode**.

   → The **Learning mode setup** dialog opens.

4. Select **Automatically, by the specified time** to end the mode automatically in a certain period of time.
5. Select **Manually** to stop the mode by clicking the **Stop learning mode** button.
6. Click **OK** to confirm.

   The learning mode is now enabled. All applications started by the user/computer are now logged and listed in the **Applications launch** tab and can be added to a package there.

Assigning application packages

ATTENTION	**Check the package configuration** Before assigning application packages, make sure that applications necessary for the user are not blocked. See also: Using demo mode

Assigning application packages to directory objects

1. Under **User management/Computer management | Applications**, select a user/computer.
2. In the lower area, click on the **Applications** tab.

   → The **Global** package and other inherited packages are displayed. Users/computers can inherit packages from the default user/computer or from groups.

3. In the **Profile** drop-down, select whether this package is valid in online or in offline mode.

> INFO
>
> **Application Control on offline Agents**
>
> - By default, if no application package has been assigned to a directory object in offline profile, the same set of application packages is applied on the Agent both in online and offline mode.
>   Once at least one package is assigned to a directory object in the offline profile, from that moment different sets of application packages are applied on the Agent depending on whether it is online or offline.
> - The **Global** package is always applied in online and offline mode.

4. Click **Add**.

   → The **Select object** dialog appears.

5. Select a package and click **OK** to confirm.

   → The selected package appears in the **Applications** tab.

6. To disable the inheritance of packages from groups or default user/computer, enable the **Activate individual settings** check box.

   → The previously inherited packages remain in the list, delete them, if needed.

7. Click **Save**.

↳ The changes are applied to the directory service object.

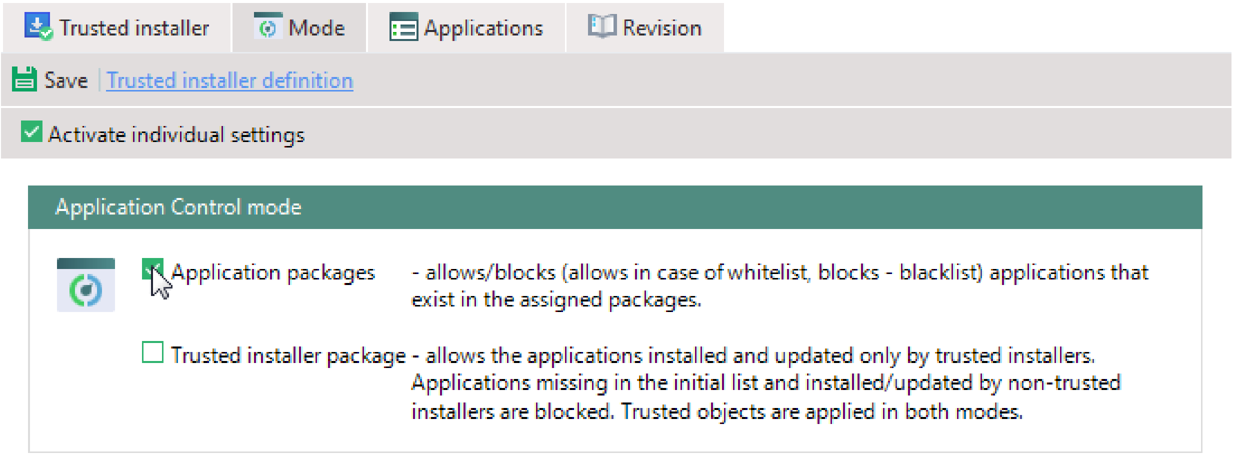
Enabling the Application packages mode

1. Under **User management/Computer management | Applications**, select a directory object.

   ! If a user/computer inherits different Application Control mode settings from several groups (e.g.: one group with Application packages mode, the other group with Trusted Installer package mode), the Trusted installer package mode has a priority.

2. Enable the **Activate individual settings** check box to disable inheritance from default rights or from groups to which a directory object belongs.

3. In the lower area, in the **Mode** tab, enable the **Application packages** check box.



☑ Application packages - allows/blocks (allows in case of whitelist, blocks - blacklist) applications that exist in the assigned packages.

□ Trusted installer package - allows the applications installed and updated only by trusted installers. Applications missing in the initial list and installed/updated by non-trusted installers are blocked. Trusted objects are applied in both modes.

Figure 87. Enabled Application packages mode

4. Click **Save**.
5. To additionally control applications on network shares and thin client storage, enable the **Allow network shares control** and **Allow thin client storage control** options for a computer under *Computer management* | *Settings* | *Client settings*.

Granting temporary access to blocked applications

Via the **Unblocking code**, temporary access to all blocked applications/DLLs/java archives can be granted to a user/computer if the Agent is offline (cannot connect to the EgoSecure Server) or if the **EgoSecure Agent** is online but just a temporary full access to all applications is needed.

Generating unblocking code for blocked applications

1. Under **User management/Computer management | Applications**, select a user or a computer.
2. In the lower area, in the **Applications** tab, click **Unblocking code**… on the toolbar.

   → The **Unblocking code generation – Application Control** dialog appears.

3. In the **Valid** drop-down, select how long you want to allow access to blocked applications.
4. Click **Generate**.

   → The code is generated and appears in the **Code** field.

5. Copy the code and send it to the user (E.g.: by mail).

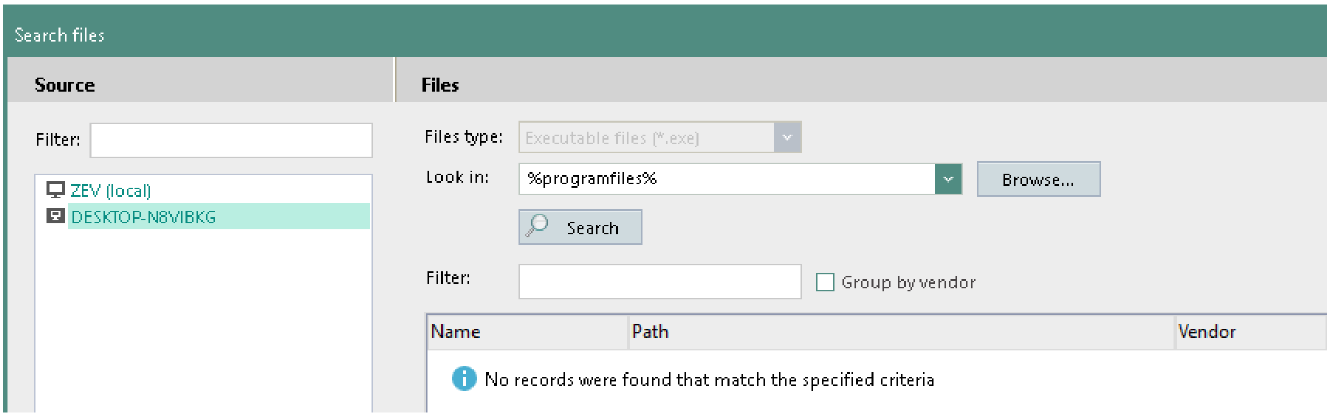
- Once a user activates the code, the user can access all blocked applications.
- Administrator can see the code activation details under **Reports | Control | Unblocking codes review**.
  New code doesn’t replace the previous one.

6.4. Working with Application Control: the Trusted installer package mode

Creating a list of trusted installers

1. Go to **Product settings | Applications | Trusted installer**.
2. On the toolbar, click **Add installer**.

   → The **Search files** dialog appears.



No records were found that match the specified criteria

Figure 88. Searching trusted installers

3. In the **Source** column, select a local computer or an online Agent computer to scan for executable files.
4. Define where to search for installers.
5. Click **Search**.

   → Scanning starts.

6. Once the scan finishes, select an installer.
   To multiselect, hold down `Ctrl` and click.
7. Click **Add**.

   → Installers are added to the list.

8. Click **Save**.

INFO

Missing attributes in the executable

Problem: An executable file must have at least one of the attributes: original filename, vendor or certificate. If all these attributes are missing, such a file will not be added to the list.
Solution: Add a trusted directory under Trusted objects.

Enabling the Trusted installer engine

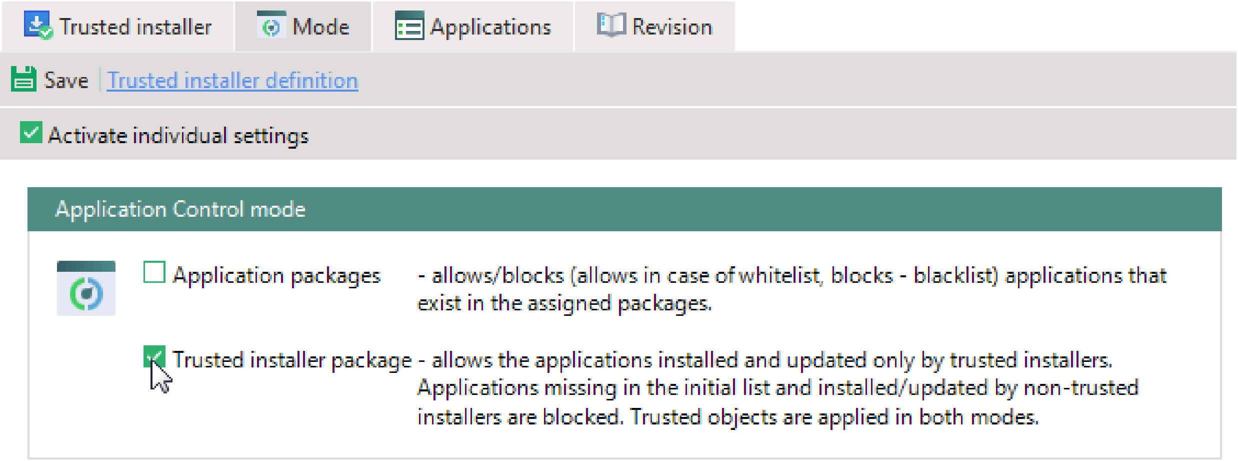
1. Go to **Computer management | Applications** and select a computer.

2. In the lower area, in the **Trusted installer** tab, check the **Enable trusted installer engine** box.
   To enable the **Trusted installer engine**, the **Application Control** license is not required.
3. Click **Save** on the toolbar.

Computer scanning for executable files on logical disks starts.
As a result, a list of currently installed applications (initial list) is created and the monitoring of applications installed by the Trusted installers starts. To apply restrictions, activate the **Application Control** product and enable the **Trusted installer package** mode for directory objects.

Enabling the Trusted installer package mode

1. Under **User management/Computer management | Applications**, select a directory object.
2. Enable the **Activate individual settings** check box to disable inheritance from default rights or from groups to which a directory object belongs.
3. In the lower area, in the **Mode** tab, enable the **Trusted installer package** check box.



☑ Activate individual settings

Application Control mode

□ Application packages - allows/blocks (allows in case of whitelist, blocks - blacklist) applications that exist in the assigned packages.

☑ Trusted installer package - allows the applications installed and updated only by trusted installers. Applications missing in the initial list and installed/updated by non-trusted installers are blocked. Trusted objects are applied in both modes.

Figure 89. Enabled Trusted installer package mode

4. Click **Save**.

From now on, only the applications installed by the specified Trusted installers and the applications from the *initial list* are allowed.
The initial list is not updated in real time, which means that if an application from the initial list is updated by a non-trusted installer, such an application will be blocked, because its hash value changes.

5. To additionally control applications on network shares and thin client storage, enable the **Allow network shares control** and **Allow thin client storage control** options for a computer under *Computer management* | *Settings* | *Client settings*.

7. FILE AND FOLDER ENCRYPTION

7.1. Encryption – overview

With the encryption products, files and folders can be encrypted both on the computer and in the network, as well as on external storage media and in cloud storage.

The following table provides an overview of encryption products and their encryption options:

Product	What?	Where?
Removable Device Encryption	Files (When encrypting a folder with **Removable Device Encryption**, the folder itself is not encrypted, only the contents of the folder (files). New files added to this folder are not encrypted automatically.	■ External storage ■ CD/DVD ■ Hard drives (if Control hard disks like external media option is enabled) ■ Floppy disk
Local Folder Encryption	Folder	■ Locally ■ In a local cloud storage if **Cloud Storage Encryption** is disabled ■ On additional hard drives
Cloud Storage Encryption	Files and folders	In a controlled local cloud storage
Network Share Encryption	Network shares of computers without **EgoSecure Agent**	■ Network share itself and subfolders ■ Thin client storage (encrypts only via the context menu)
Permanent Encryption	Files and folders	Everywhere

Encryption types

Depending on the type of encryption, data is encrypted with a specific key.
There are five types of encryption:

- **Common encryption**: Commonly encrypted data can be decrypted by all users who are registered on the same **EgoSecure Server** and who have the same common key.
- **Individual encryption**: Individually encrypted data can only be decrypted by the owner of the key.
- **Group encryption**: Data encrypted with group encryption can be decrypted by all members of an **EgoSecure** group or a directory service group that has the same group key. For details, see: Creating an encryption group

- **Mobile encryption**: Mobile encrypted data is usually password-protected and is used to transport data on external storage media or cloud storage. Except guest encryption, **Cloud Storage Encryption** and **Permanent Encryption**, mobile encryption is always used in addition to another encryption type.
- **Permanent encryption** only applies to files and adds the **.espe** file extension to them. In comparison to other types of encryption, permanent encryption remains when copying or moving files. For details, see Encrypting files permanently
  There is no separate key for permanent encryption, it uses the keys of the other encryption types.

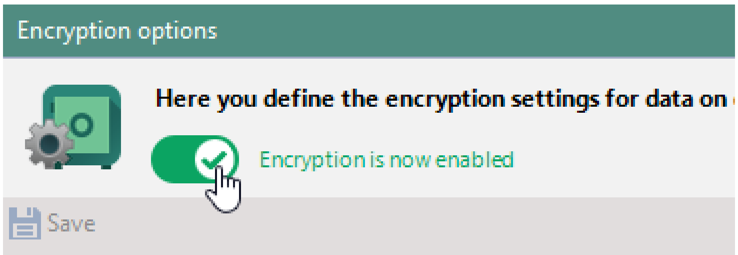
7.2. Applying general settings

Enabling encryption types

In the product settings, specify the encryption types, which become available for a user/computer once an encryption product is activated.

Selecting encryption types

1. Go to **Product settings | Encryption | Encryption options** and click on **Encryption is now disabled**.



Encryption options

Here you define the encryption settings for data on

Encryption is now enabled

Figure 90. Enabling encryption

→ The encryption is now enabled. The settings are not greyed out more.

2. In the **Available encryption types** area, enable the encryption types to make them available globally. Not activated encryption types can not be activated for directory objects.
3. Select a **Default encryption type** in the drop-down menu. This encryption type is used when the file is encrypted automatically.
4. Click **Save**.

The selected encryption types can now be activated for users, computers and groups.

Managing encryption keys

Keys for the encryption types are created automatically based on the key length and the encryption algorithm as soon as:

- an encryption product is activated (common key)

- a user/computer with a permission for individual encryption is logged on to the Server (individual key)
- an encryption group is created for group encryption (group key)

You can export and import keys to make them available to other Clients (common key) or to decrypt files using **EgoSecure Home Data Protection** (individual keys). For details, see: Exporting a key

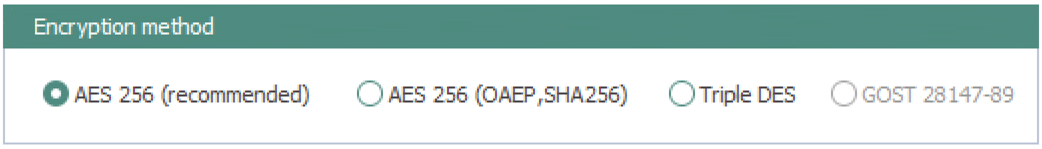
Master key for data recovery

To restore encrypted data that can no longer be decrypted by the user, create a master key. You save the master key as an encrypted file in a secure location or save it in the database with password protection. For details, see: Creating a master key

Defining key length and encryption algorithm

1. In the **Encryption key length** area, select length in bits. The key length applies to
   - the encryption key that is provided to the Agent
     and
   - the exchange key used to encrypt the encryption key. The exchange key is used to secure the key transfer between Server and Agent.
2. In the **Encryption method** area, select:

- **Triple DES**
- **AES 256** (recommended)
- **AES 256 (OAEP, SHA265)** (from Agent version 12.2.892.0)
- **GOST** (for details, see: GOST)


Encryption method

● AES 256 (recommended) ○ AES 256 (OAEP,SHA256) ○ Triple DES ○ GOST 28147-89

Figure 91. Selecting an encryption method

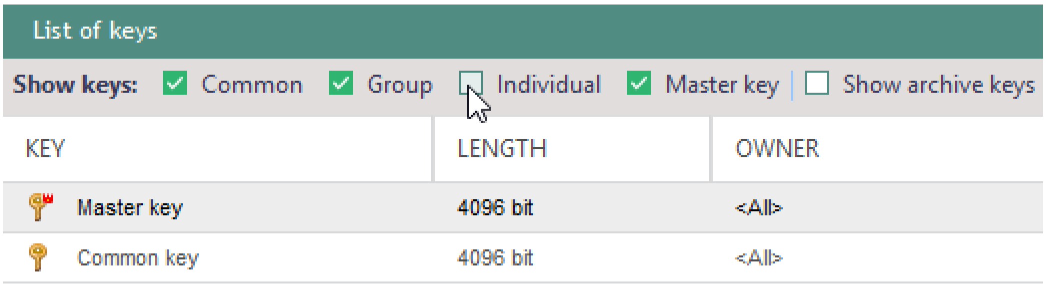
Using GOST encryption algorithm

! Make sure that no RSA key is available. Otherwise, the **GOST** method cannot be selected.

- To use the GOST method, install CryptoPro CSP (supported versions: 4.0 and higher) on computers with:
  a. **EgoSecure Agent**
  b. **EgoSecure Server**
  c. **EgoSecure Console**, to generate a master key (if Server and Console are NOT on one computer).
  d. Computers where **CryptionMobile.exe** is used.
- To switch between GOST 512 & GOST 1024 & RSA (AES, OAEP, 3DES) methods, regenerate all encryption keys in the **Key management** section.

Showing existing keys

1. Go to **Product settings | Encryption | Key management**.
2. In the **List of keys** area, select which keys to show.



Show keys: ☑ Common ☑ Group □ Individual ☑ Master key □ Show archive keys

KEY	LENGTH	OWNER
Master key	4096 bit	<All>
Common key	4096 bit	<All>

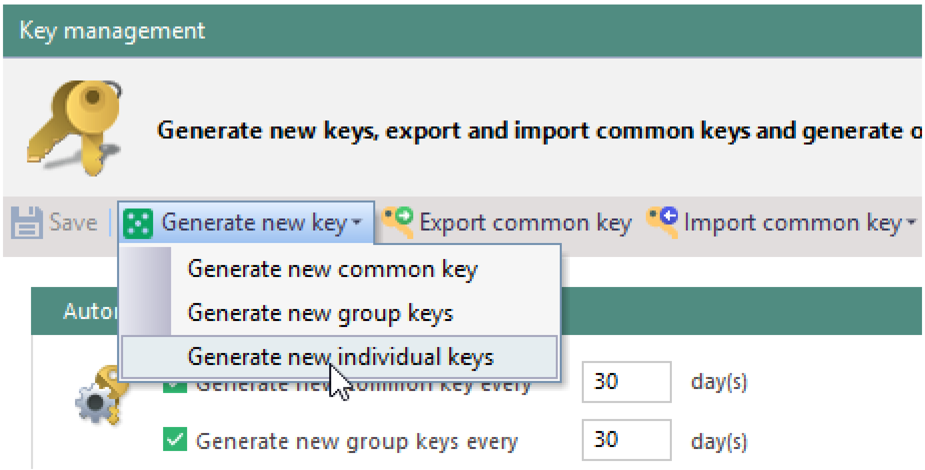
Figure 92. Showing and filtering available keys

- The **User** column shows the user/computer (individual key), the name of the encryption group (group key) and the entry **<All>** for all directory service objects.
- In the **Status** column, the entry **Valid** for active keys and **Archive keys** for archived keys are shown.

Generate new keys and archive old ones

1. To make old keys available only for a limited time (to decrypt data that has already been encrypted), enable the **Set expiration period for <key type>** checkbox and specify how many days archived keys can be used.
   If you do not set a validity period, archived keys will always remain valid.
2. To manually generate a new key, click **Generate new key** on the toolbar and select an entry.

   → A message informing you of the validity period of archived keys appears.
3. Click **Yes** to confirm the message.



Generate new keys, export and import common keys and generate o

☑ Generate new common key every 30 day(s)

☑ Generate new group keys every 30 day(s)

Figure 93. Generating new key manually

4. To automatically generate new keys, enable the checkbox of the key type under **Automatic key management** and specify in how many days to generate the keys.

→ The new keys are generated immediately/at the selected time and existing ones are archived.

➥ Encryption is performed with the new keys after generating the new ones. The new keys appear in the list.

Creating a master key

1. Under **Product settings | Encryption | Key management**, click **Create master key** on the toolbar.

   → The **Create master key** dialog appears.

2. Create the key:

   a. To store the key in an encrypted file, select **Generate a random key automatically**.

   b. To store the key password-protected in the database, select **Generate a key using a password** and enter a password.

   c. If you use **GOST** as the encryption method, provide both a location and password for the master key.

   d. To use a master certificate as a master key, click **Select a master certificate**:

   e. Click **Select**.

   → The **Windows Security** dialog appears.

   f. Select a certificate from the list.

      - The certificate must be previously imported to the local computer store of the computer where the EgoSecure Console is installed.
      - The certificate must be suitable for encryption: the **Key Usage** field of the certificate details must contain the **Key Encipherment** and/or **Data Encipherment** value.

   g. Click **OK**.

ATTENTION

Using master certificate with Agents lower than 15.3

To use a master key based on a master certificate, EgoSecure Agents must be of the version 15.3 and higher.

3. Confirm the dialog window with **OK**.
4. Click **OK** to confirm the dialog about the successful generation of the master key.

➥ Files encrypted now or later on the Client can be decrypted using the master key. For details, see: Decrypting files with a master key

Mobile encryption settings

If users have rights for mobile encryption on external or optical storage media or in clouds, they can access these files with password outside the EgoSecure network via the

mobile application **CryptionMobile.exe**. The **Cryption Mobile** application is automatically copied to the corresponding location.
Instead of a password, a PKI smart card can also be used for mobile encryption. For details, see: Using PKI smart card instead of password

Under **Product settings | Encryption | Mobile encryption**, define the settings for the mobile encryption:

Password security guidelines

- Specify guidelines to apply to the user when assigning a password for a mobile key. These guidelines are displayed on the Agent when user defines a password for a mobile key.

When closing Cryption Mobile

- **Search for unencrypted files and warn**
  a. **Files decrypted during current CM session**: The **Cryption Mobile** application warns a user that files decrypted during the session are not encrypted.
  b. **Current directory**: Searches for unencrypted files in the directory that is currently opened in **Cryption Mobile**.
  c. **All unencrypted files**: Search for unencrypted files in all device directories.
- **Remove temporary decrypted files and files that were decrypted onto hard disk**
  a. **With confirmation**: User confirms a removal.
  b. **Secure data delete**: No confirmation from a user for a removal is required.

Decryption options

- **Decrypt file directly**: Decrypts the file in its current location.
- **Decrypt file as a copy at the same media**: Decrypts the file as a copy in its current location.
- **Decrypt file as a copy to the other media**: Decrypts the file to another location.

Opening options

- Defining a location for saving files when opening them in Cryption Mobile.exe.

Other settings

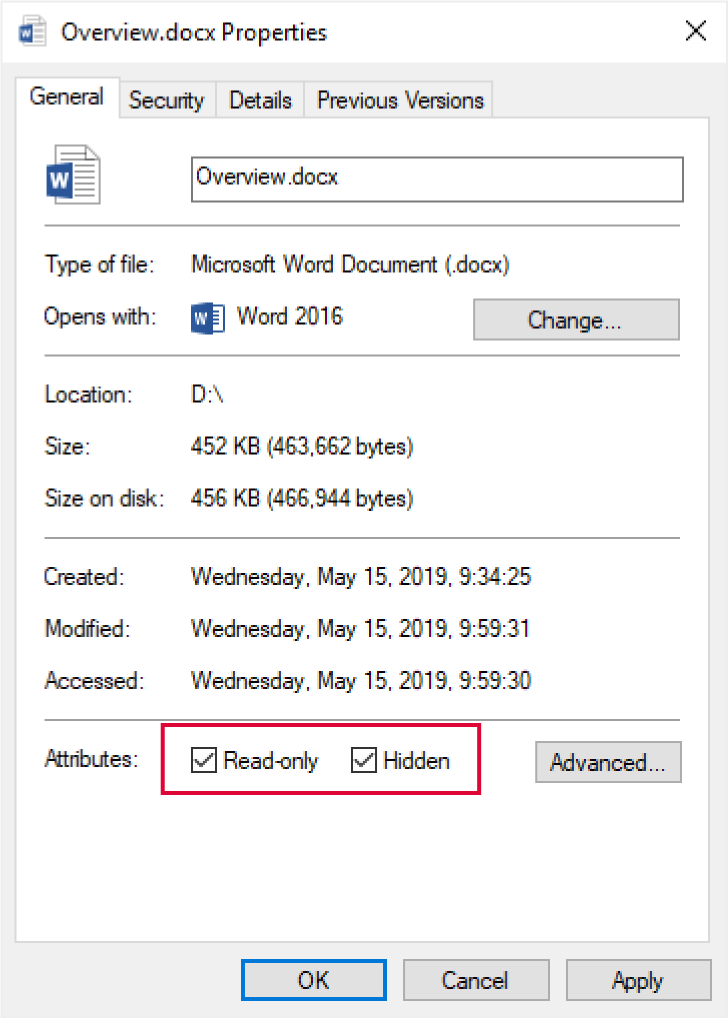
- **Copy CryptionMobile.exe to external media only after user writes or modifies data there**: If the option is enabled, **CryptionMobile.exe** is written to external storage* once the file copying or modifying finishes.
  If the option is disabled, the copying of **CryptionMobile.exe** to external storage* starts immediately.
  *External storage here is external devices like flash cards, hard drives (if Control

hard disks like external media option is enabled) and cloud storage in case of Cloud Storage Encryption.

- **Use timeouts to protect against password brute force attacks**: Prevents a password of a mobile key from being cracked by a brute force attack.
- **Show download button for Encryption Anywhere App:** In the **Encryption | External storage** and **Cloud storage**: On the **EgoSecure Agent**, displays a button with the download link for iOS and Android encryption applications.
- **Allow Permanent Encryption**: Permits or forbids the usage of permanent encryption in the **CryptionMobile.exe**. Once the option state changes, the current **CryptionMobile.exe** file is replaced with a new set of permissions.

Additional protection for encrypted data

You can additionally protect encrypted data on computers without activated encryption modules. The optional protection includes the activation of the **read-only** and **hidden** attributes for encrypted files. On computers with activated encryption products, the data remains visible and editable.



Overview.docx

Type of file: Microsoft Word Document (.docx)

Opens with: Word 2016

Location: D:\

Size: 452 KB (463,662 bytes)

Size on disk: 456 KB (466,944 bytes)

Created: Wednesday, May 15, 2019, 9:34:25

Modified: Wednesday, May 15, 2019, 9:59:31

Accessed: Wednesday, May 15, 2019, 9:59:30

Attributes: ☑ Read-only ☑ Hidden

Figure 94. File properties in Windows Explorer

Enabling additional protection

1. Navigate to **Product settings | Encryption | Encryption options**.
2. In the **Optional protection of encrypted files** area, enable the check box.
3. Click **Save**.

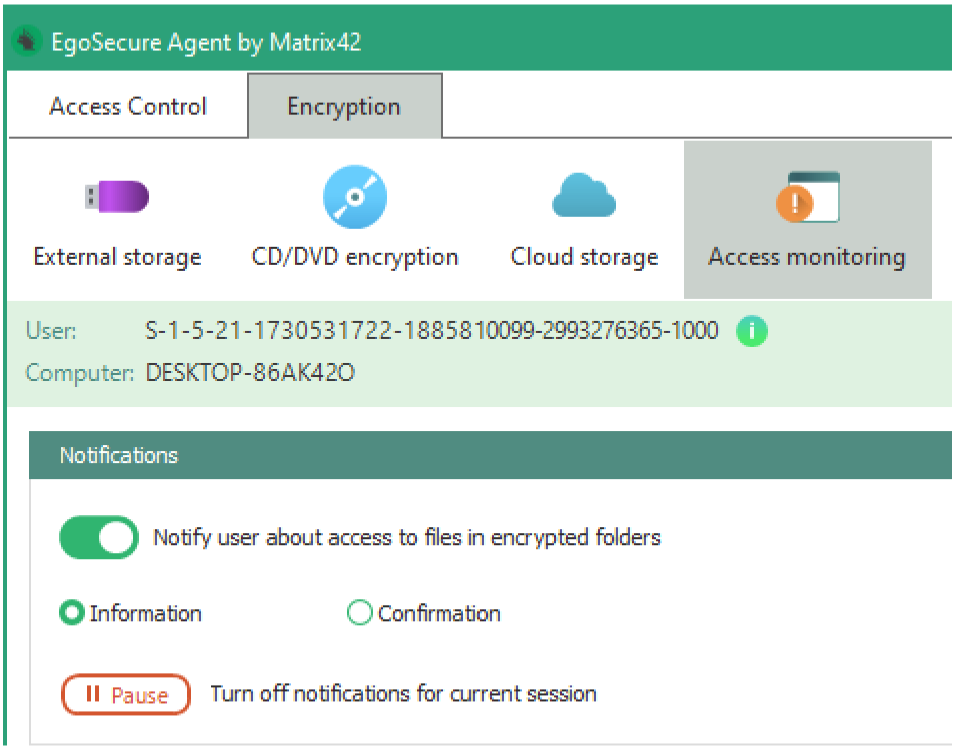
Monitoring and controlling access

You can allow the user to monitor and control access to encrypted folders. The control of the access applies to folders that have been encrypted with **Local Folder Encryption**, **Cloud Storage Encryption** or **Network Share Encryption**.

Enabling notifications for users about external access to encrypted folders (NSE, CSE, LFE)

1. Go to **Product settings | Encryption | Encryption options**.
2. In the **Access information** area, check the box.
3. Click **Save**.

From now on, users can receive notifications when encrypted folders are accessed. They can allow or deny access. For details about access monitoring on the user side, see the EgoSecure Agent – User guide.



User: S-1-5-21-1730531722-1885810099-2993276365-1000

Computer: DESKTOP-86AK42O

Notify user about access to files in encrypted folders

● Information ○ Confirmation

Turn off notifications for current session

Figure 95. Access monitoring settings on the Client side

7.3. Other encryption options

Creating an encryption group

Group encryption is used to make encrypted data accessible only to a certain group of people. Create groups and assign users and/or computers to them. A user can also be a member of several encryption groups.

Creating an encryption group

! To use group encryption, the **Group encryption** encryption type must be assigned to the user.

1. Go to **Product settings | Encryption | Groups management**.
2. Click **Add**.

   → The **Create group** dialog appears.
3. Specify a group name and click **OK** to confirm.

   → The new group appears under **Encryption groups**.
4. To arrange the groups hierarchically, move the group to another level using drag & drop.

   The users of a group can use the group encryption of all subordinate groups.

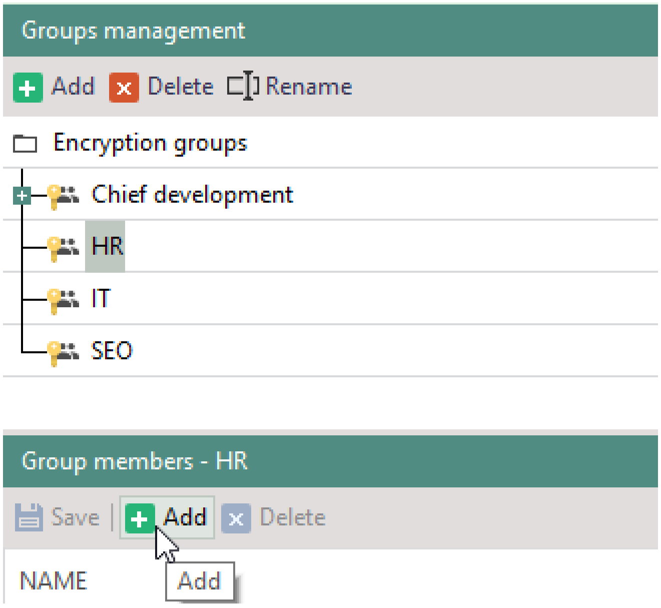


Figure 96. Adding user to encryption group

5. In the **Group members - <group name>** area, click **Add**.

   → The **Users/computers selection** dialog appears.
6. Double-click the user/computer in the directory service structure and click **OK** to confirm.

→ The dialog closes and the selected directory service objects appear under **Group members - <group name>** area.

7. Click **Save**.

Added users can use the key of the group (and subordinate groups) as long as the respective encryption product is activated for the user.
Added computers can use the key of the group (and subordinate groups) as long as the respective encryption product is activated for the computer.

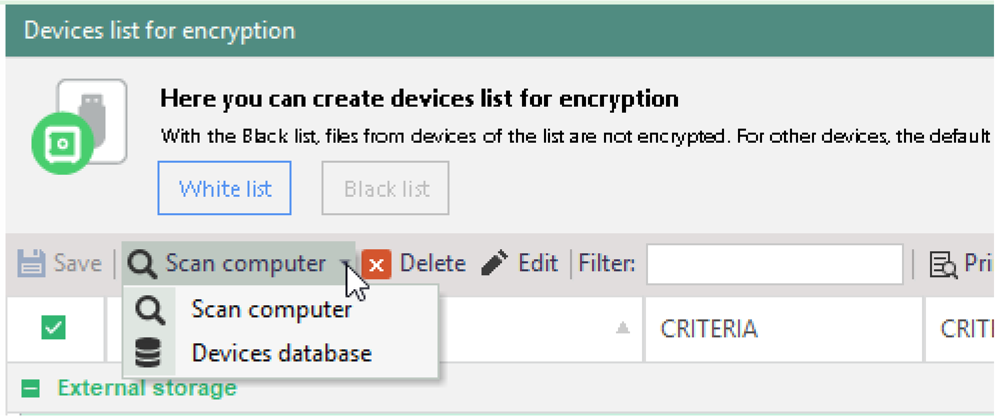
Allowing/blocking encryption device-specifically

By default, encryption is allowed on all devices. You can prevent encryption on certain devices. To prevent, scan **EgoSecure Agents** for devices or search for devices in the database.

ATTENTION	**Searching a database for devices** To see a device list of all Clients from the database, enable the **Accept data for devices DB** option in the **AdminTool**.

ATTENTION	**Permanent Encryption and Devices list for encryption** The device list for encryption doesn't apply for Permanent Encryption, because Permanent Encryption works independently of devices.

1. Go to **Permitted devices | Encryption | Devices list for encryption**.
2. Select a mode:
   - **Black list**: Encryption is not allowed on listed devices.
   - **White list**: Encryption is allowed only on listed devices.
3. To scan a Client for a device,
   a. In the **List of EgoSecure agents** area on the left, select the client computer. To multi-select, hold-down `Ctrl` and click.
   b. Click **Scan computer** on the toolbar of the **Devices list for encryption** area.


Devices list for encryption

Here you can create devices list for encryption

With the Black list, files from devices of the list are not encrypted. For other devices, the default

Figure 97. Drop-down menu of the Devices list for encryption area

→ The **Add new device – Scan computer** dialog appears. The currently connected devices are listed. Devices marked in bold are already in the device list.

c. To also display devices that were previously connected to the computer but are currently not available, disable the **Show only available devices** checkbox.

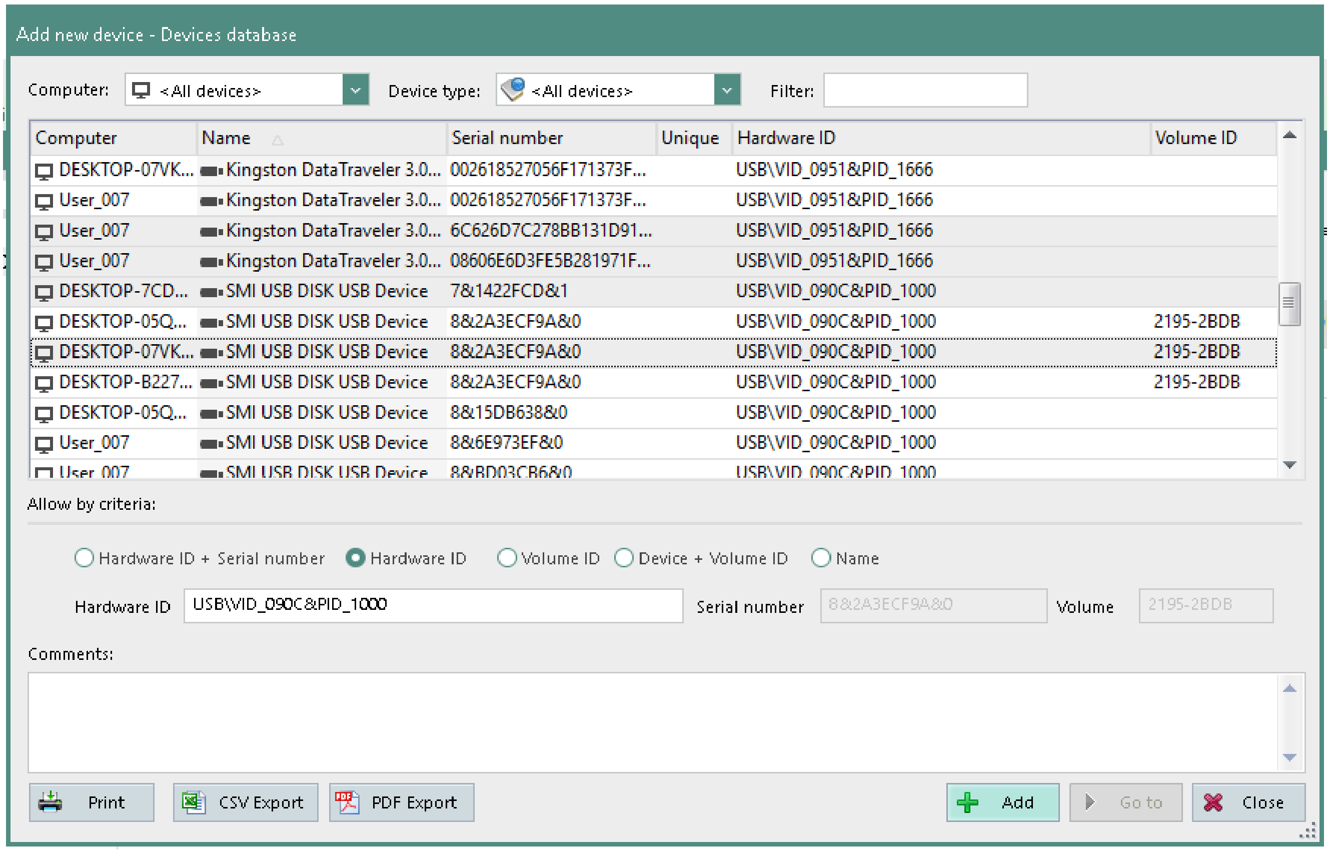
4. To search for a device list in the database,

a. Click **Scan computer** on the toolbar of the **Devices list for encryption** area.

→ The **Add new device – Devices database** dialog appears. The currently connected devices are listed. Devices marked in bold are already in the device list.

b. In the **Computer** drop-down, select computers or select **<All>** to see all devices of all computers of a directory service.

5. Select a device. To select multiple devices, hold down the `Ctrl` key and select.
6. Specify criteria for the device identification (default: **Hardware ID + Serial number**). For details, see: Criteria



Add new device - Devices database

Computer: <All devices> Device type: <All devices> Filter:

Computer	Name	Serial number	Unique	Hardware ID	Volume ID
DESKTOP-07VK...	Kingston DataTraveler 3.0...	002618527056F171373F...		USB\VID_0951&PID_1666	
User_007	Kingston DataTraveler 3.0...	002618527056F171373F...		USB\VID_0951&PID_1666	
User_007	Kingston DataTraveler 3.0...	6C626D7C278BB131D91...		USB\VID_0951&PID_1666	
User_007	Kingston DataTraveler 3.0...	08606E6D3FE5B281971F...		USB\VID_0951&PID_1666	
DESKTOP-7CD...	SMI USB DISK USB Device	7&1422FCD&1		USB\VID_090C&PID_1000	
DESKTOP-05Q...	SMI USB DISK USB Device	8&2A3ECF9A&0		USB\VID_090C&PID_1000	2195-2BDB
DESKTOP-07VK...	SMI USB DISK USB Device	8&2A3ECF9A&0		USB\VID_090C&PID_1000	2195-2BDB
DESKTOP-B227...	SMI USB DISK USB Device	8&2A3ECF9A&0		USB\VID_090C&PID_1000	2195-2BDB
DESKTOP-05Q...	SMI USB DISK USB Device	8&15DB638&0		USB\VID_090C&PID_1000	
User_007	SMI USB DISK USB Device	8&6E973EF&0		USB\VID_090C&PID_1000	
User_007	SMI USB DISK USB Device	8&BD03CB6&0		USB\VID_090C&PID_1000	

Allow by criteria:

○ Hardware ID + Serial number ● Hardware ID ○ Volume ID ○ Device + Volume ID ○ Name

Hardware ID: USB\VID_090C&PID_1000 Serial number: 8&2A3ECF9A&0 Volume: 2195-2BDB

Comments:

Figure 98. Searching a database for devices

7. Click **Add**.

   → The **Add new device** dialog closes. The device with an enabled check box appears in the list. Once you click **Save**, the settings apply to the devices with enabled check box.

8. Click **Save.**

The permissions or restrictions apply to activated devices.

Decrypting files with a master key

! To decrypt user files, the master key must exist at the time of encryption. This key must be available for decryption.
Decryption process depends on the encryption method you use (**AES/DES** or **GOST**).
For details, see: Creating a master key

Decrypting data with a master key (AES/DES)

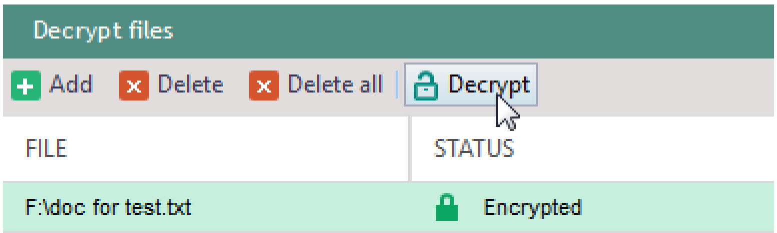
1. Navigate to **Product settings | Encryption | Files recovery**.
2. Select the master key that you created before encryption:
   a. If you saved the master key to a file, click **Browse** and select the corresponding file with the ending **.cpk**.

   b. If you saved the master key to the database, enter the password and select the key length of the master key (defined under **Product settings | Encryption | Encryption options | Encryption key length**).

3. In the **Decrypt files** area, drag a file into the blank area or click **Add** to select a file.

   → The file appears in the list. In the **Status** column the encryption status displays as **Encrypted**.

4. Click **Decrypt**.



FILE	STATUS
F:\doc for test.txt	Encrypted

Figure 99. Decrypting data with a master key

If the master key matches, the status changes to **Successfully decrypted** and the file is decrypted in the location where it is currently stored. When decrypting permanently encrypted files, both files (encrypted and decrypted) remain in the original location.

Decrypting data with a master key (GOST)

1. Click on **Browse** and select the appropriate master key for decryption.
2. In the **Decrypt files** section, drag a file into the blank area or click **Add** to select a file.
3. Click **Decrypt**.

   → The **Enter master key password** dialog appears.

4. Enter the password and click **OK**.

If the entered password matches, the status changes to **Successfully decrypted** and the file is decrypted in the location where it is currently stored.

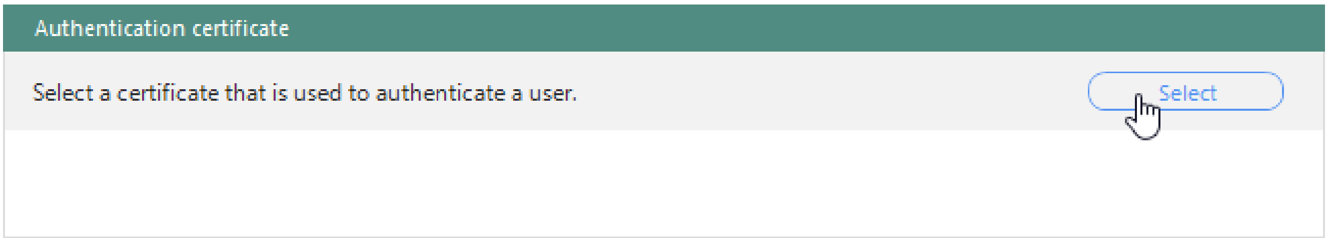
Protecting access via two-factor authentication

Two-factor authentication allows access to encrypted data of an encryption module once the user authenticates with a certificate (e.g. with a Windows certificate store or smart card).
Two-factor authentication is compatible with the following encryption modules: **Removable Device Encryption** (except the encryption of processes under **User management | Encryption | Processes**), **Cloud Storage Encryption**, **Local Folder Encryption**, **Network Share Encryption** and **Permanent Encryption**.

Authentication is required every time the user wants to access the certain location. It is valid until the current session on the Agent ends (e.g.: by logging out of Windows or by restarting). This also applies if the certificate is deleted beforehand or the smart card is ejected.

Enabling two-factor authentication

1. Install a certificate for two-factor authentication on the computer with the EgoSecure Server (start the certificate file and follow the instructions).
2. Provide the certificate to the user: via a smart card/chip card or via the installation on the client computer.
3. Under **User management | Encryption**, select a user.
4. In the **Settings** tab, click **Select** in the **Authentication certificate** area.



Authentication certificate

Select a certificate that is used to authenticate a user.

Figure 100. Selecting a certificate for two-factor authentication

5. Select the installed certificate and click **OK**.
6. Enable the two-factor authentication: Under **User management/Computer management | Encryption**, enable the **Use two-factor authentication** check box in the corresponding tab (External storage, CD/DVD, Cloud storage, Local Folder, Network Share or Permanent).
7. Click **Save**.

The two-factor authentication is configured. As soon as the user wants to access encrypted data, authentication starts and a user message appears.

Protecting mobile encrypted data via PKI smart card instead of password

You can restrict the authentication for mobile encryption. This means that authentication via a PKI smart card is required for all encryption modules and globally for all users when using mobile encryption. It is also no longer possible to enter a password to access mobile data.

1. Navigate to **Product settings | Encryption | Encryption options**.
2. Enable the **Use PKI smart cards for mobile encryption** check box in the **PKI authentication** area.

The PKI authentication is enabled. Users can not use passwords for the mobile encryption more. Only authentication via PKI smart card is permitted. Files previously encrypted with one of the mobile passwords can still be opened.

Allowing direct access to encrypted data to applications

If an application wants to access encrypted data via a user session, but no encryption module is activated for the user, **EgoSecure** blocks access to this data. You can define applications for which access to encrypted data is always permitted.

Allowing raw access to applications

1. Go to **Product settings | Encryption | Application-dependent settings**.
2. Click **Add**.

   → A new entry appears in the list.
3. Specify an application.
4. Click **Save**.

➥ The application now has access to encrypted data regardless of the active user session.

Exporting a key

Importing/exporting a common key

You can export a common key to

- make backup
- make the key available in other tenants

Exporting a common key

1. Navigate to **Product settings | Encryption | Key management**.
2. Click **Export common key** on the toolbar.

   → The **Save As** dialog appears.
3. Enter a file name and location.
4. Click **Save**.

➥ The key is saved in the protected **.cpk** format.

Importing a common key

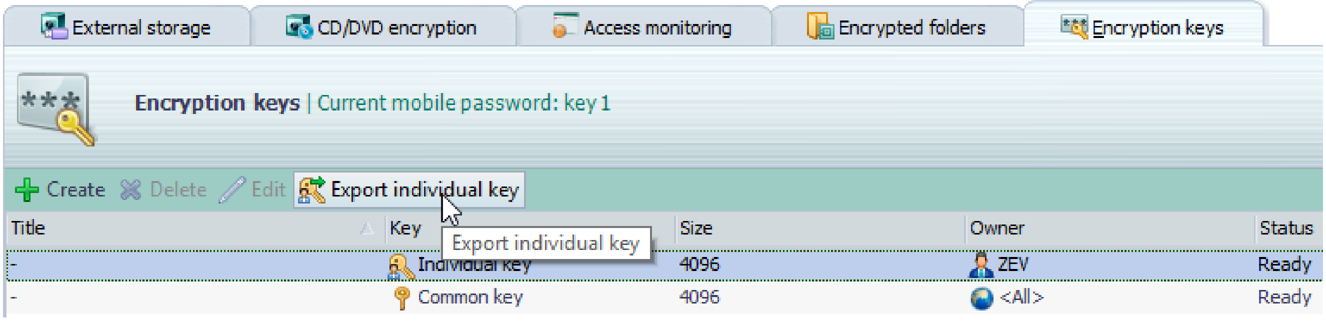
1. Navigate to **Product settings | Encryption | Key management** and click **Import common key** on the toolbar.
2. Select an option from the drop-down menu:
   a. **Replace common key**: Replaces the existing key with the imported key. The existing key is archived and is still valid unless you set a period of validity for common keys.
   b. **Import additional common key**: Imports and archives the new key. It is valid till you set a period of validity for common keys.

   → The **Open** dialog appears.
3. Select a previously exported common key and click **Open**.

- The key appears in the list of archived keys. Data encrypted with this key can now be decrypted by all directory service objects that use common encryption.

Exporting an individual key

Every user who has individual keys, can export it via **EgoSecure Agent**. For example, data can be decrypted and edited at home using **EgoSecure Home Data Protection**.



Title	Key	Size	Owner	Status
-	Individual key	4096	ZEV	Ready
-	Common key	4096	<All>	Ready

Figure 101. Key export via EgoSecure Agent

Guest encryption for external usage of EgoSecure products

It is not possible to run the **Cryption Mobile** mobile app on computers with the installed **EgoSecure Agent**. Visitors from other companies who also use **EgoSecure** encryption products will then not be able to access the encrypted data on their storage media or in clouds. With **Guest encryption**, you allow visitors to decrypt their encrypted data in Windows Explorer using the mobile password.

Enabling Guest encryption

1. Go to **Product settings | Encryption | Encryption options**.
2. Enable the check box in the **Guest encryption** area.
3. Click **Save**.

- The guest can now decrypt encrypted data with the password.

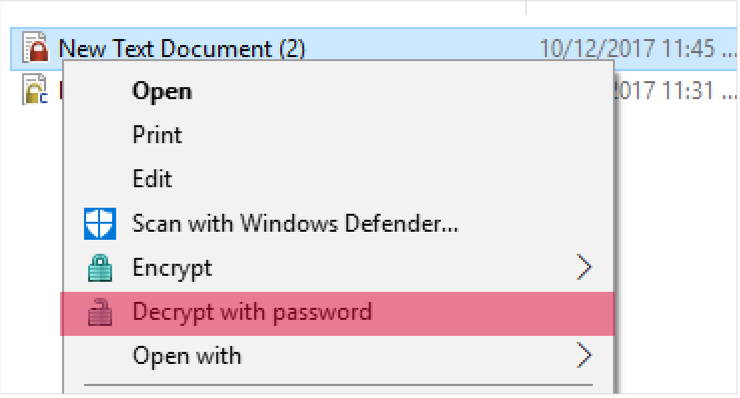


Figure 102. Decrypting with password

Defining shortcuts to switch between encryption types

A keyboard shortcut enables users to deactivate the encryption type for external storage media or switch from **Unencrypted** to the first available type next to None (the priority is the following: **Common encryption**, **Group encryption**, **Individual encryption**).

Defining shortcut for changing the encryption type

1. Go to **Administration | Clients | Fast access settings**.
2. Enable the **Use shortcuts to change encryption type** check box.
3. Select a key combination from the drop-down menus.
4. To emit a signal on the Client when changing, enable the **Use audio signal when encryption type changed** check box.
5. Click **Save**.

7.4. Removable Device Encryption (RDE)

Removable Device Encryption encrypts data on the following devices:

- External storage
- CDs/DVDs
- Hard disks if they are controlled like external media. For details, see: **Disks control** in the Client settings

RDE automatically encrypts files on the device as well as files that are copied to or created on the device.
If **EgoSecure Agent** has a valid key, the file is automatically decrypted on accessing it. If a valid key is not available, the access is blocked.

RDE can be activated for users and computers. When the product is activated for users and computers at the same time, computer settings have a priority.

If RDE is activated for the user, the files can be automatically encrypted if they are created, opened or edited with certain processes. For details, see: Process encryption

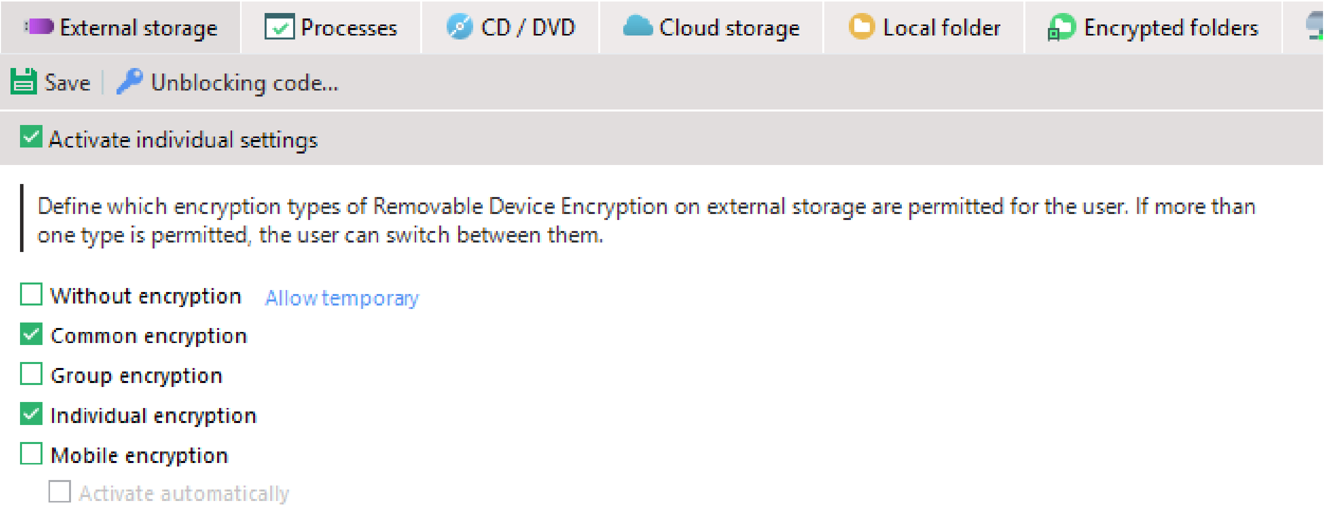
Enabling and customizing Removable Device Encryption for user/computer

1. Check whether all necessary settings for encryption have been made. For details, see: Applying general encryption settings
2. To encrypt on CD/DVD disks:
   a. Enable the **Allow CD/DVD encryption** check box under **Product settings | Encryption | Encryption options**.
   b. Make sure that **escdflt.sys** driver was installed on the Agent computer during the Agent installation (the **Install kernel driver for CD/DVD control** option). If no driver is installed, generate the MSI package with the enabled option "**Install kernel driver for CD/DVD control**" under **Installation | EgoSecure agents | Create MSI package** and update the Agent.

3. Under **User management/Computer management**, activate **Removable Device Encryption** for a directory object. For details, see: Activating products
4. Under **Encryption | External storage** and/or **CD/DVD**, enable the **Activate individual settings** option to deactivate inheritance and change the settings.

   → The previously inherited encryption types remain enabled. Uncheck them, if necessary.

5. Select encryption types to make them available for a directory object.
   If more than one encryption type is available, a user can select an encryption type for a storage medium with manual encryption and an encryption type for automatic encryption.



☑ Activate individual settings

Define which encryption types of Removable Device Encryption on external storage are permitted for the user. If more than one type is permitted, the user can switch between them.

☐ Without encryption
☑ Common encryption
☐ Group encryption
☑ Individual encryption
☐ Mobile encryption
☐ Activate automatically

Figure 103. Making encryption types available

6. If you enabled **Mobile encryption**, enable the following options, if necessary:
   a. **Activate automatically**, to automatically activate the mobile encryption on the Agent.
   b. **Always active**, to activate and deactivate the mobile encryption on the Agent automatically.
   c. **Remind to select password**, show a popup for a user so that he can select a current mobile key.
7. Click **Save**.

The user can now encrypt on external storage media according to the defined permissions and settings. A description of the procedure can be found in the EgoSecure Agent – User guide.

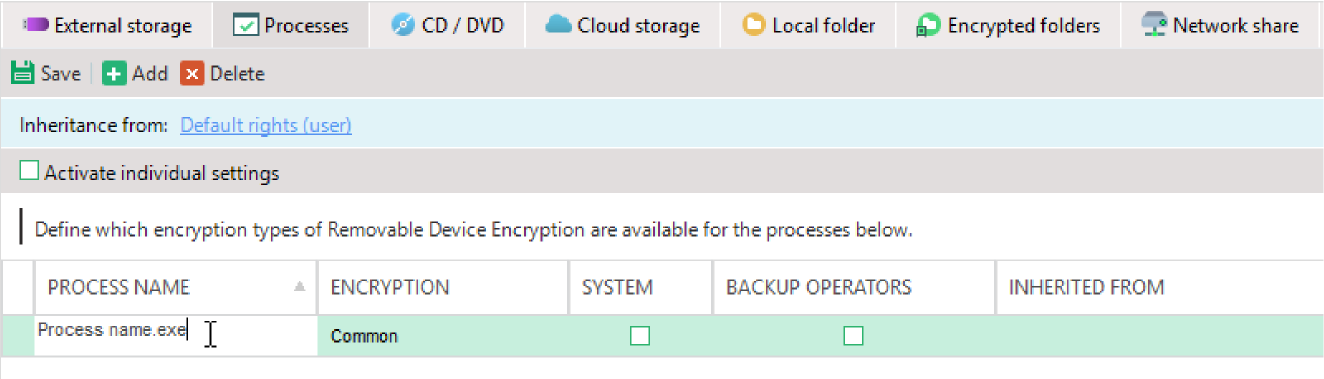
Encryption via processes

RDE activated on users can encrypt all files opened, edited and created with a certain process.

Adding processes

1. Under **Encryption | Processes**, click Add.

   → A new entry appears in the table.



Inheritance from: Default rights (user)

□ Activate individual settings

Define which encryption types of Removable Device Encryption are available for the processes below.

PROCESS NAME	ENCRYPTION	SYSTEM	BACKUP OPERATORS	INHERITED FROM
Process name.exe	Common	□	□	

Figure 104. Defining encryption options for a process

2. In the **Process name** column, enter the file name of the application.
3. Right-click the entry in the **Encryption** column and select an encryption type (if more than one is enabled in the **External storage** tab).
4. Enable the check box in the **System** column to enable encryption when the application is launched by a system.
5. To enable encryption when the application is launched from a user account of a Windows user group *Backup Operators*, enable the check box in the **Backup Operators** column.
6. Click **Save**.

Settings for unencrypted file transfer

You can allow the user to save data to external storage unencrypted (**Without encryption** encryption type). In the settings, define whether a user sees a security message about the related risk or whether the system automatically switches to a different encryption type after a certain period of time.

If the **Without encryption** encryption type is not allowed for a user/computer, you can temporary allow unencrypted file transfer.

INFO

Applicable only for Removable Device Encryption

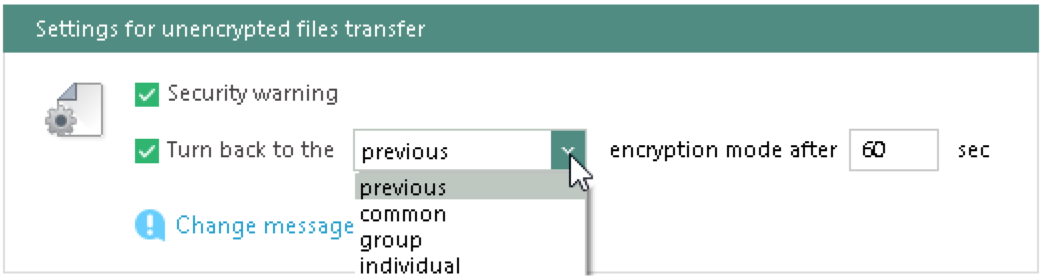
The setting only applies to **Removable Device Encryption**. For details, see: Removable Device Encryption

Showing message and returning encryption back

! The **Without encryption** encryption type must be enabled under **Product settings | Encryption | Encryption options | Available encryption types** and then under

User management/Computer management | Encryption for a certain user/computer.

1. Go to **Product settings | Encryption | Encryption options**.
2. To show a warning to the user when he selects the **Without encryption** type, enable the **Security warning** check box. You can edit the warning message text. For details, see: Customizing user messages



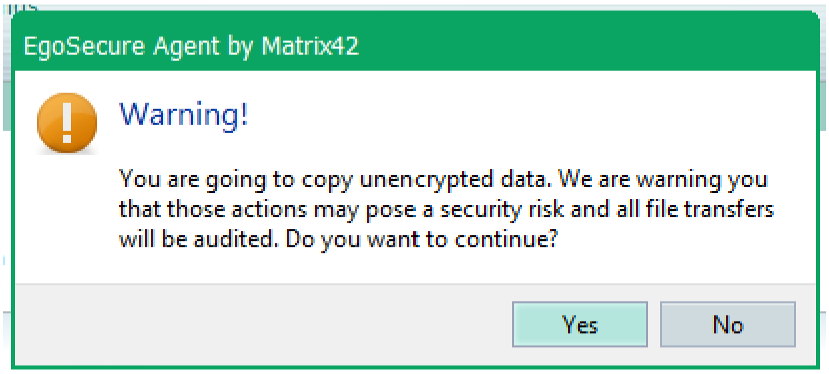
Settings for unencrypted files transfer

☑ Security warning

☑ Turn back to the previous encryption mode after 60 sec

Figure 105. Configuring encryption turn back

→ Once a user selects the **None** encryption type, the following message appears:



EgoSecure Agent by Matrix42

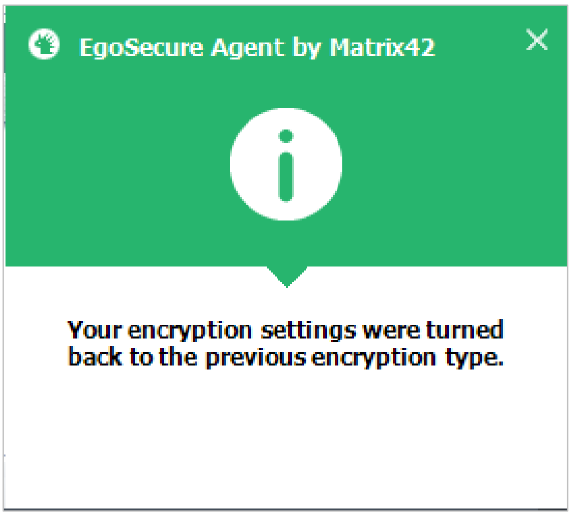
Warning!

You are going to copy unencrypted data. We are warning you that those actions may pose a security risk and all file transfers will be audited. Do you want to continue?

Figure 106. Warning message in case of unencrypted file transfer

3. To turn back to the default encryption type when the user selects the **None** encryption type, enable the **Turn back to the** checkbox and select an encryption type from the drop-down menu. Specify in how many seconds after finishing the file copying, the encryption type turns back.
   When relogging to the system, service restart or on computer restart, the turning back to the defined encryption type occurs.

   → The user gets a message when the encryption type turns back.



Your encryption settings were turned back to the previous encryption type.

Figure 107. User message after turning encryption back

4. Click **Save**.

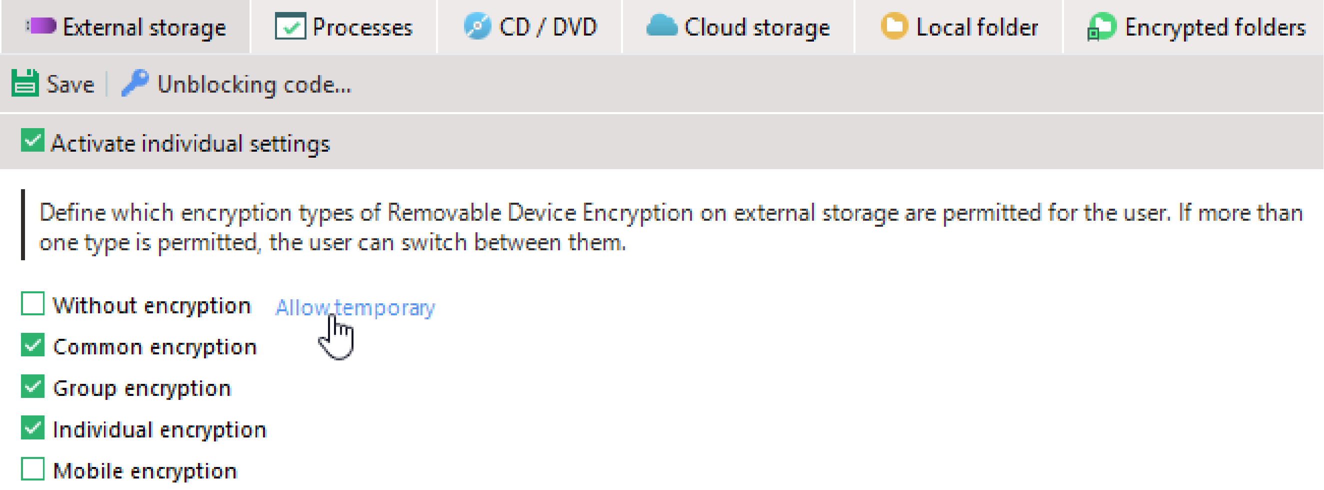
Temporary allowing unencrypted file transfer

! Enable the **Without encryption** encryption type under **Product settings | Encryption | Encryption options**.

1. Under **User management/Computer management | Encryption**, select a user/computer.
2. Navigate to **External storage** or **CD/DVD** tab in the lower area.

   → If the **Without encryption** encryption type is disabled for the default user/computer and no individual settings are available for the user/computer, the **Allow temporary...** button is available.
3. Enable the **Activate individual settings** option and disable the **Without encryption** check box.

   → The **Allow temporary...** button appears near the **Without encryption** encryption type.



☑ Activate individual settings

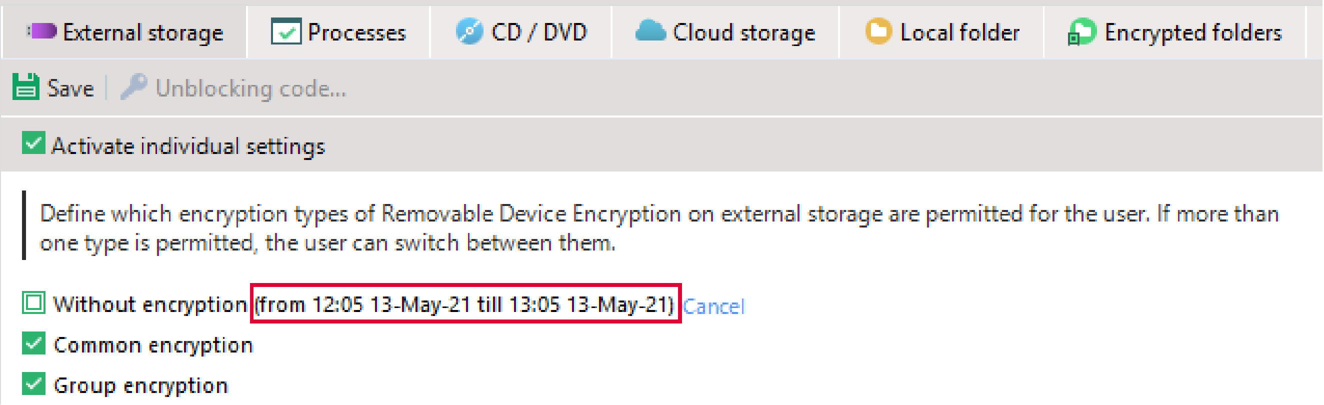
Define which encryption types of Removable Device Encryption on external storage are permitted for the user. If more than one type is permitted, the user can switch between them.

☐ Without encryption
☑ Common encryption
☑ Group encryption
☑ Individual encryption
☐ Mobile encryption

Figure 108. Permitted encryption types for file transfer to external storage

4. Click the **Allow temporary...** button and enter a time period in the dialog window.
5. Click **OK** to confirm.

The defined period of time and the **Cancel** button appear next to the **Without encryption** encryption type:



☑ Activate individual settings

Define which encryption types of Removable Device Encryption on external storage are permitted for the user. If more than one type is permitted, the user can switch between them.

□ Without encryption (from 12:05 13-May-21 till 13:05 13-May-21) Cancel
☑ Common encryption
☑ Group encryption

Figure 109. Temporary permitted unencrypted file transfer

7.5. Local Folder Encryption (LFE)

Local Folder Encryption automatically encrypts all files in a local folder as well as files copied to or created in the folder. To encrypt, the user activates encryption for a folder once.
If **EgoSecure Agent** has access to a valid key, an encrypted file is automatically decrypted when the user accesses it. If no valid key is available, all accesses to it are blocked.
Local Folder Encryption can be activated only for a user.
Pay attention to the list of folders excluded from encryption.

Enabling and customizing folder encryption for user

1. Check whether all necessary settings for encryption have been made. For details, see: Applying general encryption settings
2. Under **User management**, activate the **Local Folder Encryption** product for a user. For details, see Activating products
3. To deactivate inheritance and change the settings, enable the **Activate individual settings** check box under **Encryption | Local folder**.

   → The previously inherited encryption types remain enabled. Uncheck them, if necessary.
4. Select the encryption types to make them available for the user.
   If more than one type is available, the user can select between them.
5. Click **Save**.

The user can now use folder encryption. A description of the procedure can be found in the EgoSecure Agent – User guide.

Enforcing automatic encryption of user folders

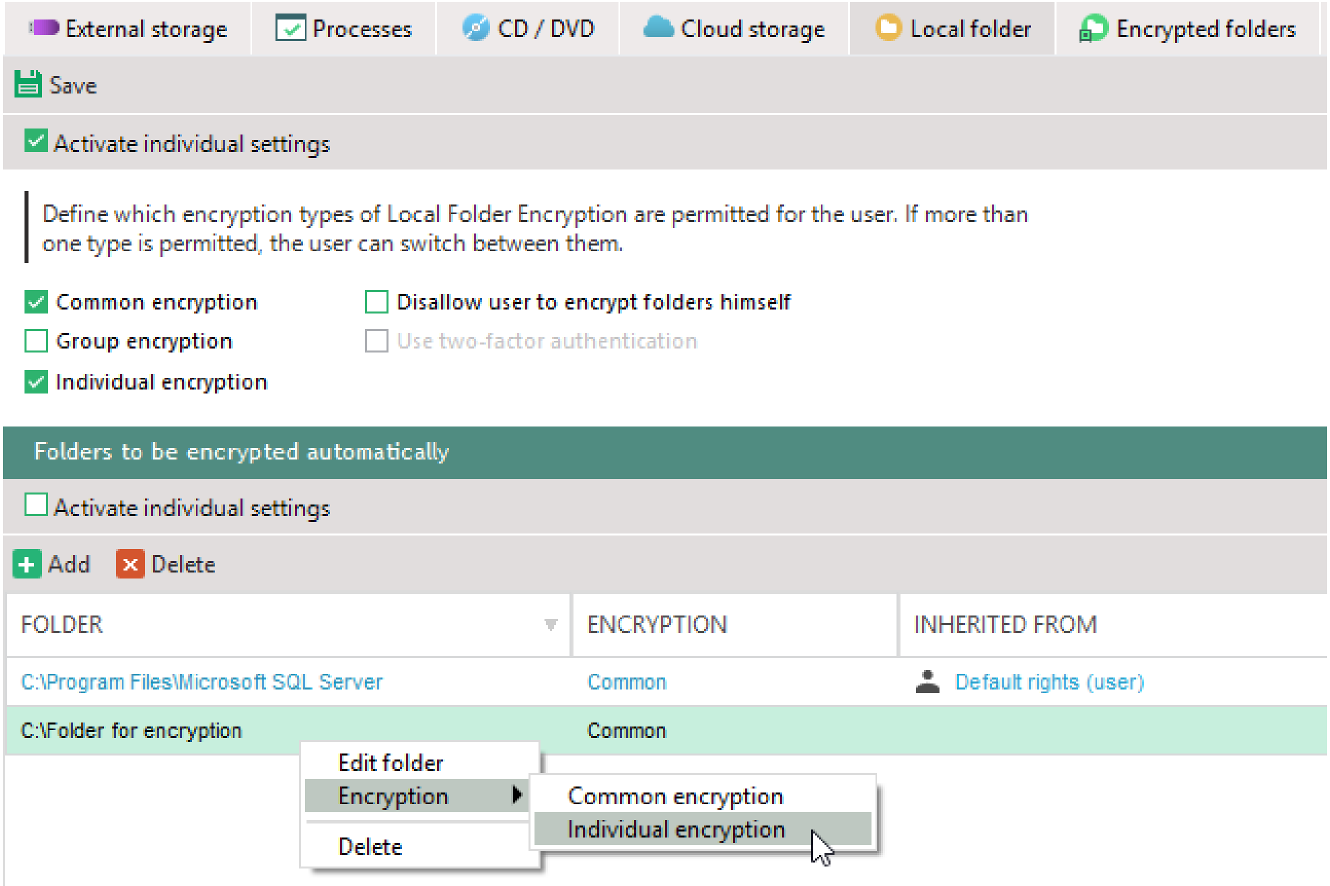
1. Select a user.
2. Click **Add** under **User management | Encryption | Local Folder**.

   → The dialog for selecting a directory appears.

3. Select a directory and click **OK** to confirm.

   → The dialog closes and the directory appears in the list.

4. Right-click the entry and select **Encryption | <encryption type>** from the context menu. In the **Folder encryption settings** area, you can select the permitted encryption types.



☑ Activate individual settings

Define which encryption types of Local Folder Encryption are permitted for the user. If more than one type is permitted, the user can switch between them.

☑ Common encryption
☐ Group encryption
☑ Individual encryption
☐ Disallow user to encrypt folders himself
☐ Use two-factor authentication

Folders to be encrypted automatically

☐ Activate individual settings

FOLDER	ENCRYPTION	INHERITED FROM
C:\Program Files\Microsoft SQL Server	Common	Default rights (user)
C:\Folder for encryption	Common	

Figure 110. Enforcing the encryption of local folders

5. Enable the **Activate individual settings** check box to disable the inheritance of folders from groups and default rights.

   → Only individually added folders remain in the list.

6. Click **Save**.

The folders from the list will be automatically encrypted on a computer (as soon as the corresponding **EgoSecure Agent** is online). The user can decrypt the folder if the **Disallow user to encrypt folder himself** option is disabled.

Viewing the list of encrypted folders

- To display a list of all encrypted user folders, click on **User management | Encryption | Encrypted folders**.

Local folders excluded from Local Folder Encryption

- Program Files with subfolders
- Program Files (x86) with subfolders
- Users (Documents and Settings)
- Program Data (Application Data) with subfolders
- Windows with subfolders
- AppData
- Folder with user profile
- Folders with the system attribute
- Folders that contain subfolders considered as exclusions.
  The **Users** folder can not be encrypted, because it contains system elements. But other subfolders with personal data (e.g.: Desktop, Favorites, My Documents, My Video) can be encrypted.

7.6. Cloud Storage Encryption (CSE)

Cloud Storage Encryption automatically encrypts files and folders in cloud storage once the encryption is enabled. If files are copied from other computers without EgoSecure Agent or directly from the browser into the cloud, the files have to be encrypted manually. If EgoSecure Agent has access to a valid key, the files are automatically decrypted when accessed. If no valid key is available, access to encrypted files is blocked.
Cloud Storage Encryption can be activated only for a user.

Enabling and customizing Cloud Storage Encryption

1. Check whether all necessary settings for encryption have been made. For details, see: Applying general encryption settings
2. Define the controlled cloud storage types under **User management | Settings | Cloud storage**.
3. Activate **Cloud Storage Encryption** for a user. For details, see: Activating products
4. To disable inheritance and change settings, enable the **Activate individual settings** check box under **Encryption | Cloud storage**.

   → The previously inherited encryption types remain enabled. Uncheck them, if necessary.
5. Select the encryption types to make them available for the user.
   If more than one type is available, the user can select between them.

6. Click **Save**.

↪ The user can now use cloud encryption. A description of the procedure can be found in the EgoSecure Agent – User guide

ATTENTION

Avoiding encryption problems with OneDrive

- During the initialization, the computer on which the initialization is performed must be restarted.
- Disable the **Save space and download files as you use them** option.

7.7. Network Share Encryption (NSE)

Network Share Encryption automatically encrypts all files existing in an encrypted network share as well as files copied, created and edited there. NSE is used on network computers that do not have EgoSecure Agent but have shared network folders. If an authorized user with a valid key copies an encrypted file from a network folder, the file is automatically decrypted.
Network Share Encryption can be activated only for a user.

ATTENTION

Avoiding decryption problems when NTFS compression is enabled

The NTFS file system has a built-in compression feature known as NTFS compression. The use of this compression will hinder the Agent to encrypt any compressed file or folder.
If NTFS compression is activated after encryption with EgoSecure, the affected files are no longer decryptable.

- Remove the NTFS compression to gain access to encrypted files.

Setting up Network Share Encryption

Network Share Encryption is set up for Agents with the activated Network Share Encryption and optionally for Agents where Network Share Encryption is NOT activated, but continues to check the encryption status of network share files.

Activating and setting up Network Share Encryption

1. Check whether all necessary settings for encryption have been enabled. For details, see: Applying general encryption settings
2. Under **Administration | Clients | Client settings**, enable the **Allow network shares control** option; enable the **Allow thin client storage control** option if you want to additionally allow users to encrypt on thin client storage via the context menu.
3. Click **Save**.

4. Under **User management**, activate the **Network Share Encryption** product for a user.

   → A warning message about the use of Windows offline files in connection with encrypted network folders appears.

WARNING	**Possible data loss when using Windows offline files at the same time** As offline files are stored in the local Windows cache, it is not possible to decrypt files that are available offline from encrypted network folders. If Windows offline files are still used in connection with **Network Share Encryption**, this can lead to data loss. ◆ Enable the **Disable Windows offline files** option under **User management | Encryption | Network share** or disable the usage of offline files directly on the Clients.

5. Click **OK** to confirm the dialog.
6. Under **Encryption | Network Share**, enable the **Activate individual settings** check box to disable the inheritance of settings from groups or the default user.

   → The previously inherited encryption types remain enabled. Uncheck them, if necessary.

7. Select the encryption types available for the user.
8. Enable the **Disallow user to encrypt network shares himself** check box to forbid a user to encrypt network share folders via the context menu.
9. Enable the **Hide encryption interface on Agent** check box to hide the encryption progress dialog on the Agent side when an encryption is enforced by the administrator.
10. Click **Save**.

Setting up Network Share Encryption (NSE) on Agents without activated NSE

Even if Network Share Encryption is deactivated, the Agent continues to check the encryption status of network share files and shows popups if access to encrypted files is denied. Not only the user, but also processes might want to access encrypted files, which results in many popups. In such a case you can disable the encryption state check on Agents with deactivated NSE. As a result, users can access encrypted files, but the file itself remains encrypted (when opening the file the so-called “garbage” is displayed).

1. Navigate to **Product settings | Encryption | Encryption options**.
2. In the **Access to network share files** area, enable the **Allow raw access to encrypted network share files** option.
3. Click **Save**.

Enforcing automatic encryption of network folders

Once **Network Share Encryption** is activated and set up, you can add network share folders for encryption. Network share folders can be:

- Added for a default user or individually for each user.
- Managed centrally with an automatic encryption of newly added unencrypted files (unencrypted files appear in an encrypted network share folder if they are copied there from a computer without Network Share Encryption).

WARNING	**No Agent on computer and granted write access** ◆ There must be no Agent on a computer with a network share. ◆ Write access to a folder where encryption will be performed must be granted to a user.

Enforcing automatic encryption of network folders – individually managed

1. Select a user.
2. Under **User management | Encryption | Network Share**, click **Add** on the toolbar.
3. Select a directory in the dialog window and click **OK** to confirm.

   ! Defining the path to mapped network shares and virtual drives is not recommended. It may lead to system conflicts when the same network share folder is added for encryption twice.

   → The path to a directory appears in the list.
4. In the **Encryption** column, click on an encryption type to select another one.
5. Enable the **Activate individual settings** check box to disable inheritance from groups and default rights.

   → Only individually added folders remain in the list.
6. Click **Save**.

- Once the changes are transferred to a user, the specified folders are encrypted. The specified encryption rule is also displayed under **Product settings | Encryption | Network share**, where all network share folders for encryption (within one tenant) are displayed.
- On the Agent side: Once the encryption starts, the **EgoSecure Encryption by Matrix42** progress dialog appears if the **Hide encryption interface on Agent** check box is disabled for a user under **User management | Encryption | Network share**.
- The network share folders encrypted by the administrator from Console can not be decrypted by a user.

> INFO
>
> **Folders already encrypted with an individual key**
>
> If admin wants to decrypt or reencrypt a folder that has been encrypted with an individual key, this occurs only after a user confirmation in the popup.

Enforcing automatic encryption of network folders – centrally managed

1. Go to **Product settings | Encryption | Network share**.
   In this location all the encryption rules defined for network share folders within the current tenant are displayed.
2. Click **Add** on the toolbar.

   → The **Specify a directory** dialog appears.
3. Specify a directory and click **OK** to confirm.

   ! Defining the path to mapped network shares and virtual drives is not recommended. It may lead to system conflicts when the same network share folder is added for encryption twice.

   → The path to a directory appears in the list.
4. In the **Encryption** column, click on an encryption type to select another one.
5. In the **User that encrypts** column, click the entry to select a user or a group for using their key for encryption.
   <Any user> value is displayed when no user or group has been selected for encryption or when an encryption entry has been created for a default user. The value means that any first available user with activated **Network Share Encryption** and disabled **Activate individual settings** check box (activated inheritance) is permitted to encrypt the folder.

   ! Make sure that for the selected user or group the selected encryption type is enabled under **User management | Encryption | Network share**.
6. In the **Agent that encrypts** column, click the entry to select a computer or a group that encrypts a folder.
   <Any computer> value means that any available computer will encrypt. The value is displayed when no computer or group has been selected for encryption or when an encryption entry was created for a default user.
7. In the **Rescan** column, set the check box for the entry to scan an encrypted folder for unencrypted files according to a scheduler and defined rules.
8. Click **Save**.

➥ The added network share folder is additionally displayed for each defined user (if **<Any user**> is defined: for all users with enabled inheritance) under **User**

management | Encryption | Network share.
Once the defined Agent (or first of the defined Agents) is online, the encryption starts and the encryption status changes in the **Status** column.

- On the Agent side: Once the encryption starts, the **EgoSecure Encryption by Matrix42** progress dialog appears if the **Hide encryption interface on Agent** check box is disabled for a user under **User management | Encryption | Network share**.
- The network share folders encrypted by the administrator from Console can not be decrypted by a user.

Setting up a scheduler for folder rescan

1. Under **Product settings | Encryption | Network share**, set the **Scan encrypted network folders for encrypted files** check box to enable a scheduler.
2. Select the week days when a scan starts.
3. Set the time when the scan starts on each selected week day.
4. Select a behavior type if new key is generated under **Product settings | Encryption | Key management**:

- **Encrypt unencrypted files with previous key**. If unencrypted files have been detected during a scheduled scan, the option automatically encrypts the unencrypted files with a previous (archived) key.
- **Reencrypt the whole folder with new key**. If during a scan a new key has been detected, the option automatically reencrypts all files (that are encrypted with a previous key) with a new key.

5. Click **Save**.

- The defined scheduler rules are valid only for the encryption entries with the enabled checkbox in the **Rescan** column.

Viewing the list of encrypted folders

- To display a list of all encrypted user folders, click on **User management | Encryption | Encrypted folders**.

7.8. Permanent Encryption (PE)

Permanently encrypted files remain encrypted when accessed or sent. Decryption can only be initiated manually and with existing key(s). Once a file/folder is encrypted, the file extension is extended with the **.espe** ending and the folder is transformed to a zipped **.espe** file. **Permanent Encryption** can also be performed on files that have already been encrypted with **Removable Device Encryption** or **Cloud Storage Encryption**. **Permanent Encryption** can be activated only for a user.

Enabling and configuring Permanent Encryption for a user

1. Check whether all necessary settings for encryption have been made. For details, see: Applying general encryption settings
2. Activate the **Permanent Encryption** product for a user. For details, see: Activating products
3. To disable inheritance and change settings, enable the **Activate individual settings** check box under **Encryption | Permanent**.

   → The previously inherited encryption types remain enabled. Uncheck them, if necessary.
4. Select the encryption types available for the user.
5. If more than one type is available, the user can select between them.
6. Select which options are available for the user in the context menu: only permanent encryption or only permanent decryption or both.
7. Click **Save**.

➥ Now the user can encrypt/decrypt files within the permitted encryption types. A description of the procedure can be found in the EgoSecure Agent – User guide

Setting up Permanent Encryption

1. Go to **User management | Encryption | Permanent**.
2. Select a directory object in the **User management** area.
3. Enable the **Delete source file after encryption** option to delete an original unencrypted file after encryption and leave only a new encrypted .espe file. If the option is disabled, both an original unencrypted file and an encrypted .espe file are left.
4. Enable the **Delete ESPE file after decryption** option to delete an encrypted .espe file and leave an original unencrypted file instead. If the option is disabled, both an original unencrypted file and an encrypted .espe file are left.
5. Click **Save**.
6. Go to **Product settings | Encryption | Encryption options**.
7. In the **Permanent Encryption** area, select a Secure Erase method for deleting files securely after encryption and/or decryption. Select **Non-secure method** to apply no Secure Erase method during file deletion.
   This option doesn’t depend on the Secure Erase license.
8. Click **Save**.

Enabling Permanent Encryption with a smart card/certificate

Permanent Encryption with a smart card/certificate encrypts files and folders with the help of an active directory certificate or any certificate suitable for encryption. Administrators on their own generate such certificates in the Active Directory and distribute them to the computers with the EgoSecure Agent. Certificates can be stored in

the Active Directory or in the Windows Store.
Each certificate has its own key length. That is why the length of the certificate key does NOT depend on the encryption key length defined under **Product settings | Encryption | Encryption options**.

INFO	**Not compatible with GOST** **Permanent Encryption** with a smart card/certificate is not compatible with the GOST encryption algorithm.

Certificate requirements:

- For **Certificate encryption**: The **Key Usage** field of the certificate details must contain the **Key Encipherment** and/or **Data Encipherment** value.
- For **Certificate signing**: The **Key Usage** field of the certificate details must contain the **Digital signature** value.
- For **Certificate encryption and signing**: The **Key Usage** field of the certificate details must contain the **Key Encipherment** and/or **Data Encipherment** value and the **Digital signature** value.

Permanent Encryption with a smart card/certificate is divided into three options:

- **Certificate encryption** (encrypts files with the help of a certificate)
- **Certificate signing** (protects file via signing their certificate; the digital signature protects the file from change and spoofing)
- **Certificate encryption and signing** (combines the two options above)

! To protect a file with both **Certificate encryption** and **Certificate signing**, use the **Certificate encryption and signing** option. If a user first selects the **Certificate encryption** option and after that selects **Certificate signing** (or vice versa), these protection options replace each other.

Enabling Permanent Encryption with a smart card/certificate

1. Go to **User management | Encryption | Permanent**.
2. Select a directory object in the **User management** area.
3. Enable the **Certificate encryption** option.

   → The **Certificate encryption** option becomes available on the Agent in the context menu.

4. Enable the **Digital signature using certificate** option.

   → The **Certificate signing** option becomes available on the Agent in the context menu.

→ The **Certificate encryption and signing** option becomes available on the Agent in the context menu if steps 3 and 4 are performed.

5. Click **Save**.

➥ Now on the user side, the certificate encryption and signing options become available in the context menu inside the **Encrypt permanently** group.
For details about Permanent Encryption with a smart card/certificate on the user side, see the EgoSecure Agent – User guide.

Enabling Post-Quantum Encryption in addition to Permanent Encryption

EgoSecure Post-Quantum Encryption encrypts files with password in such a way so that in the future quantum computers cannot override the security that exists nowadays. This high security level is provided due to the Kyber-1024 encryption method.
Once **Post-Quantum Encryption** is enabled, it becomes available on the Agent side if the Permanent Encryption product is already activated for a user.

Enabling Post-Quantum Encryption

1. Go to **Product settings | Encryption | Encryption options**.
2. Enable the **Allow Post-Quantum Encryption** box.
3. Click **Save**.

   → Now the option becomes available for activation in **User management**.

4. Go to **User management | Encryption | <user selection> | Permanent**.
5. Enable the **Allow Post-Quantum Encryption** check box.
6. Click **Save**.

➥ Now on the user side, **Post-Quantum Encryption** options become available in the context menu inside the **Encrypt permanently** group and depend on the state of the **Encrypt permanently** and **Decrypt permanently** check boxes.
For details about the Post-Quantum Encryption on the user side, see the EgoSecure Agent – User guide.

8. DATA LOSS PREVENTION

With **Data Loss Prevention** (**DLP**), you can search files for sensitive information and block them from being enclosed to the outside world.

To find text contents in files, create filters with search patterns (lexical expressions). The patterns can consist of strings or numbers, but also of complex regular expressions. The filters are assigned to users or computers.

DLP is divided into two modules, each module requires a license.

- **Data in Use** (**DIU**) for real-time scanning of external storage media (user-based)
- **Data at Rest** (**DAR**) for the scheduled scanning of hard drives and network folders (computer-based)

Module	Scanned devices	Scan start	Measures
DIU	Internal and external storage of computer, Network shares, Cloud storage, Hard disks (if they are controlled like external storage media),	When accessing a storage medium	■ Deny read or write access (or both read and write) to the file and audit. ■ Only audit. ■ Ask user for reason in the pop-up message and see the reason in audit. ■ Allow access to the file, but redact the sensitive info in the file (sensitive info will be hidden under ***) and audit. Audited events are displayed under User management/Computer management | DLP | Audit (DIU) tab.
DAR	Internal and external storage of computer, Network shares, Hard disks (if they are controlled like external storage media)	At the specified time according to the scheduler (once or weekly)	■ Move to quarantine and audit. ■ Delete and audit. ■ Only audit. ■ Audited events are displayed under Computer management | DLP | Audit (DAR) tab.

8.1. Preparing DLP: installation and settings

First of all, install the DLP Policy Server and specify common settings for it.

Installing or updating DLP

1. Go to **Product settings | DLP | Installation settings**.

2. Click ⋯ in the **Policy Server 32-bit/64-bit installation file** area depending on the operating system (32-/64-bit).
3. Select the location of the **DLPPolicyServer** (32-/64-bit) MSI file.
4. Go to **Computer management | DLP**.
5. In the **Computer management – DLP** area, select an online computer. To select multiple computers, hold down the `Ctrl` key.
6. Right-click a computer and select **Install/Update** from the context menu.

↳ The installation starts. In the **Product status** column, the current installation status displays.

DLP settings: error behavior, metadata analysis, scan timeout, quarantine

1. Go to **Product settings | DLP | Settings**.
2. In the **Error behavior** area, select whether an access to files must be allowed if the DLP server doesn't respond due to errors.
3. In the **Metadata analysis** area, check the **Enable metadata analysis** box to additionally scan the document properties of Microsoft Office files.
4. To avoid DLP getting stuck when scanning very large files, set a timeout for scanning one file in the **Scan timeout** area for the **DLP - Data in Use** and **DLP - Data at Rest** products.
5. To leave the bread crumb file instead of a quarantined file,
   a. enable the **Leave bread crumb file** check box in the **Quarantined files** area.
   b. In the text box, enter the user information to include it in a breadcrumb file.

   → Once a file, which matches the filter criteria is found and moved to quarantine, the original file name changes from, for example, "License codes.txt" to "License codes.txt.moved". Once a user opens the file, the message defined by an administrator is displayed.

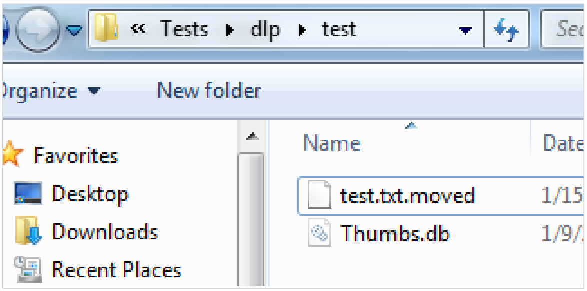


Figure 111. Bread crumb file in Windows Explorer

6. Click **Save**.

Writing log files for DAR scans

1. To write detailed log files for scheduled computer scans with DAR, go to **Administration | Clients | Log files**.

2. On the **Log file settings by product** tab, enable the **Write log file for DLP DAR scans** check box.

   ↳ Once the scan finishes on the client computer, its logfile is saved under **ProgramData\EgoSecure\EgoSecureAgent\Log**. It contains all search parameters and all search results of the scan.

Specifying controlled storage types for Data in Use

By default, the **DLP – Data in Use** product scans only external storage media. Additionally, it can scan the following storage types:

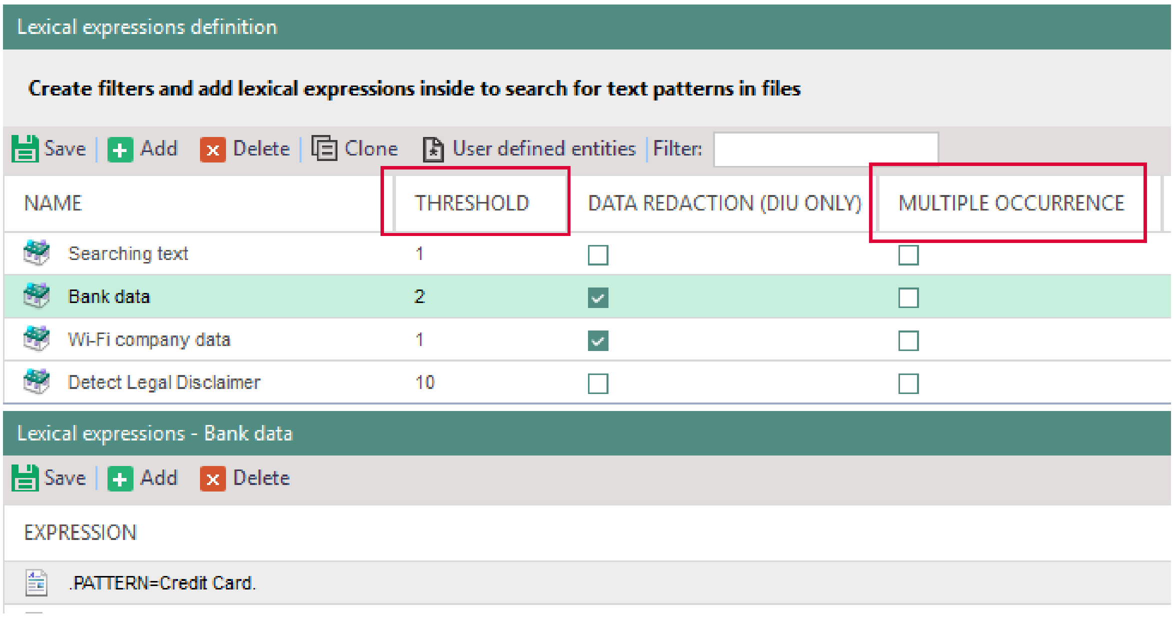
Storage type	Additional configuration required
Network shares	Enable **Allow network shares control** option under **Computer management | Settings | Client settings**.
Cloud storage	Define which cloud types to control under **User management | Settings | Cloud storage** tab.
Hard disks	Enable the **Control hard disks like external media** option under **Computer management | Settings | Client settings**.

8.2. Creating and assigning DLP filters

Create filters to assign them to users (DIU) or to use them for computer scans (DAR). You can add any number of lexical expressions to a filter. The conditions of a filter are met when the specified **Threshold** value of the filter is reached.

Threshold

The **Threshold** value is calculated from the weighting of individual expressions and the number of findings.



Lexical expressions definition

Create filters and add lexical expressions inside to search for text patterns in files

NAME	THRESHOLD	DATA REDACTION (DIU ONLY)	MULTIPLE OCCURRENCE
Searching text	1	□	□
Bank data	2	☑	□
Wi-Fi company data	1	☑	□
Detect Legal Disclaimer	10	□	□

Lexical expressions - Bank data

EXPRESSION
.PATTERN=Credit Card.

Figure 112. Setting up threshold for DLP filter

For every expression a value from 1 to 10 (weighting) can be defined. The values of found expressions are calculated throughout the whole scanned file.
When using the **Multiple occurrence** option, an expression can be counted several times if the expression is found more than once in the file.
You can also specify for expressions that the threshold is reached immediately for a single finding (without weighting).

Example: personal data

The filter is created to block files that contain a certain number of personal data. A threshold value is **20**; **multiple occurrence** is not enabled.

Expression	Weight	Findings	Value
Date of birth	**5**	1	5
Social security number	**5**	1	5
Plan number	**5**	0	0
Address	**5**	2	5

The scanned file contained the following expressions: *date of birth*, *social security number* and *address*. The last one was met two times; multiple occurrence is not enabled. The expression *plan number* was not found, resulting in a total of **15**.

- The threshold of **20** is not reached. **DLP** doesn't block the file.

Example: list of bank data

This filter is created to block files that contain lists of bank data such as, for example, IBAN or credit card numbers. Files that only contain individual IBAN or credit card numbers should not be blocked. As a result, multiple occurrence is enabled and threshold is set to 100.

Expression	Weight	Findings	Value
.PATTERN=Credit Card.	**5**	13	65
IBAN	**5**	9	45
Bank	**2**	3	6

The searched file contained the expression *.PATTERN = Credit Card*. **13** times. This expression is a (pre-defined) regular expression contained in **DLP**. This corresponds to one credit card number per occurrence.
In addition, the *IBAN* expression appeared **9** times in the file and the *Bank* expression appeared **3** times in the file.
Since the multiple occurrence is enabled, it counts the weighting of every found expression. It results in **116** total score, which meets the filter conditions.

- The threshold of **100** is reached. **DLP** blocks the file.

Example: sensitive information

The purpose of this filter is to check whether a file contains sensitive information. A threshold of **20** was set; **Multiple occurrence** is not enabled.

Expression	Weight	Findings	Value
Confidential information	**10**	1	10
Do not disclose	**5**	2	5
For employees only	**5**	0	0
Highly confidential	**detected**	1	detected

The searched file contained the expression *confidential information* one time and the expression *do not disclose* two times; the filter doesn't take multiple occurrences of an expression into account. Together, these expressions would have a threshold value of **15**, which would not meet the conditions of the filter. However, the file also contains the expression *highly confidential* that has the **detected** weighting and meets the condition of the filter due to a single occurrence.

➥ The threshold is reached because of the **detected** value. DLP blocks the file.

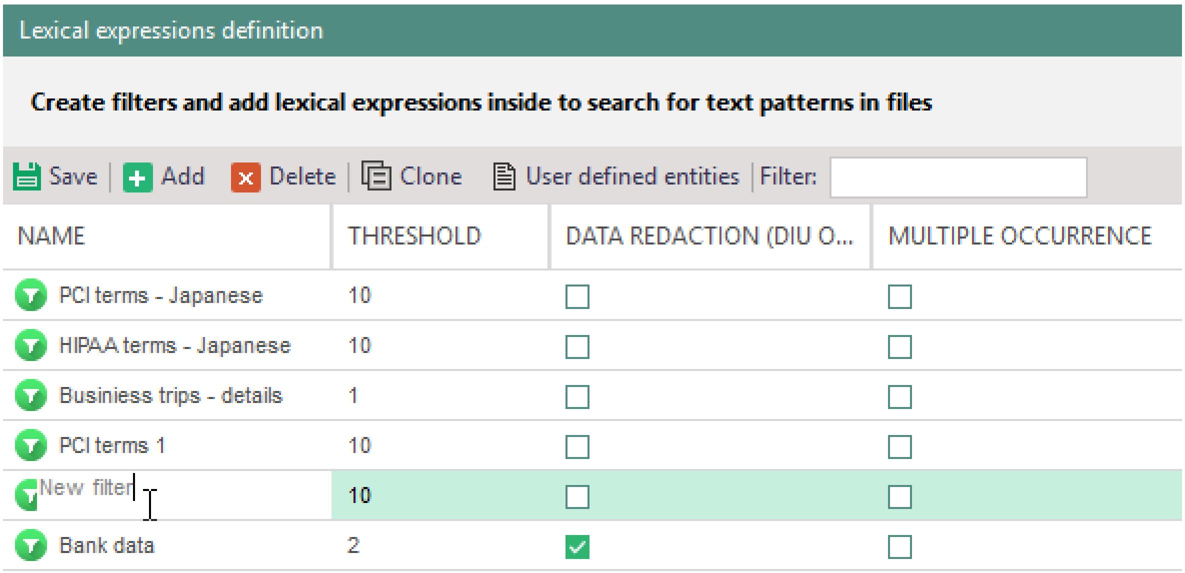
Creating filters with lexical expressions

1. Go to **Product settings | DLP | Lexical expressions definition**.

   → In the **Lexical expressions definition** area, the list of predefined expressions displays.

2. Click **Add** on the toolbar.

   → A new entry appears in the list.



Lexical expressions definition

Create filters and add lexical expressions inside to search for text patterns in files

NAME	THRESHOLD	DATA REDACTION (DIU O...	MULTIPLE OCCURRENCE
PCI terms - Japanese	10	□	□
HIPAA terms - Japanese	10	□	□
Business trips - details	1	□	□
PCI terms 1	10	□	□
New filter	10	□	□
Bank data	2	☑	□

Figure 113. Creating new DLP filter

3. Specify a filter name in the **Name** column.

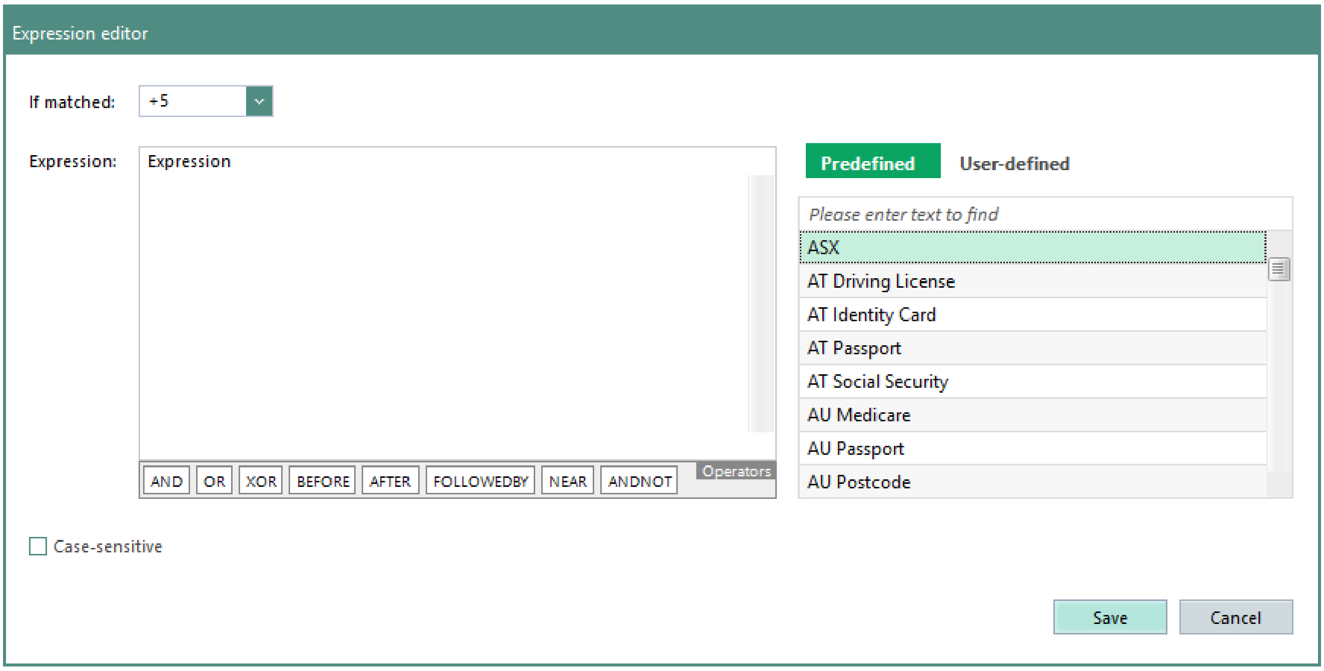
4. Double-click in the **Threshold** column to define the total score that must be reached so that a match occurs.
5. If the weighting of an expression found multiple times in one file should be counted as separate items, enable the **Multiple occurrence** check box.
6. In the **Lexical expressions – <filter name>** area, create a lexical expression for the filter to search for specific strings. For details, see: Creating a lexical expression
7. Click **Save**.

↳ The filter can now be assigned to user (DIU) or used for computer scanning (DAR).

Creating a lexical expression

1. Select a filter in the **Lexical expressions definition** area.
2. In the **Lexical expressions – <filter name>** area, click **Add**.

   → The **Expression editor** dialog appears.



Expression editor

If matched: +5

Expression: Expression

□ Case-sensitive

Figure 114. Defining lexical expression

3. In the **If matched** drop-down menu, select a weighing for the expression. To reach the threshold with the first finding, select **Instant**.
4. In the **Expression** field, enter a search pattern. You have the following options:
   - Selection of a predefined search pattern in the right column.
   - Selection of a user-defined search pattern in the right column. For details, see: User-defined entities
   - Manual input: simple or regular expressions.
     For details, see Appendix: DLP – lexical expression syntax
5. Enable the **Case-sensitive** box if the searched text is case sensitive.

6. Click **Save**.

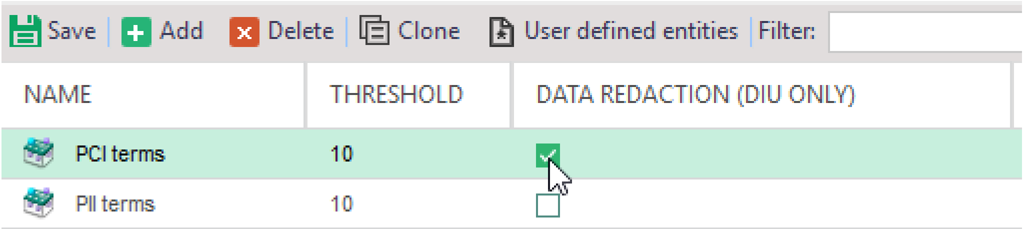
   → The **Expression editor** dialog closes and the expression is added.

7. In the **Lexical expressions definition** area, click **Save**.

The expression is added under the selected filter.

Assigning DLP filters to directory objects (DIU)

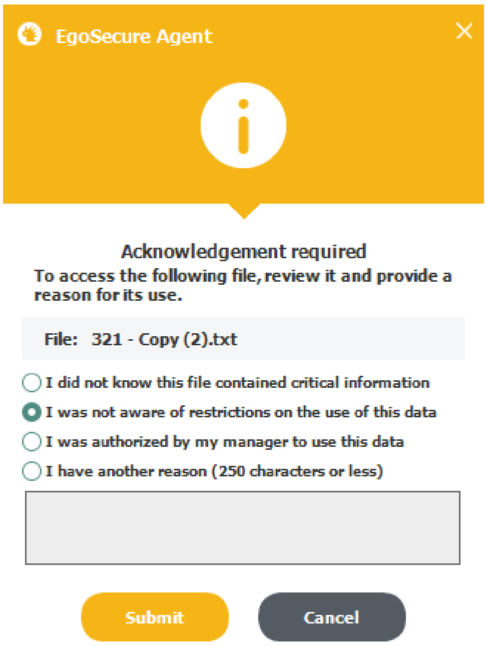
1. Under **User management | DLP**, select a user from the list.
2. In the lower area, select the tab with a storage type: **External storage**, **Network shares**, **Cloud storage**. Make sure to additionally configure controlled storage types.
3. Enable the **Activate individual settings** check box to assign only individual filters to the selected user. Clear the check box to assign individual filters in addition to the filters inherited from groups or from default rights.
4. Click in the **Access** column to select which access type is under control:
   a. **Read** (only read operations)
   b. **Write** (only write operations)
   c. **Read/write** (read and write operations)
5. In the **Action** column, select which action is performed with the selected access type:
   a. **No action (audit only)** to perform NO action if user accesses a file, which matches filter criteria and just inform about access in the **Audit (DIU)** tab.
   b. **Deny access** to deny access to a file, which matches filter criteria and inform about access in the **Audit (DIU)** tab.
   c. **Allow and redact** to hide sensitive info under *** in a file while access to the file is not restricted and inform about access in the **Audit (DIU)** tab. This action doesn’t not apply to files in RAR archives.
      This option is listed in the context menu only if the **Data redaction** parameter is enabled for a filter under **Product settings | DLP | Lexical expressions definition**:



NAME	THRESHOLD	DATA REDACTION (DIU ONLY)
PCI terms	10	☑
PII terms	10	□

Figure 115. Enabling data redaction for a filter

   d. **Allow and ask for reason** to show a pop-up on a user side once the user accesses a file, which matches filter criteria. User must select the reason from the list or write an explanation by his/her own. The access to the file is blocked till user explains the reason and clicks **Submit**. If user ignores the pop-up or clicks **Cancel**, the access remains to be denied. Such an action combined with the access reason is displayed in the **Audit (DIU)** tab; if user just tries to open the file, but clicks **Cancel** or ignores the popup, the administrator is not informed about it in audit, because NO file content is accessed.



Acknowledgement required

To access the following file, review it and provide a reason for its use.

File: 321 - Copy (2).txt

○ I did not know this file contained critical information
● I was not aware of restrictions on the use of this data
○ I was authorized by my manager to use this data
○ I have another reason (250 characters or less)

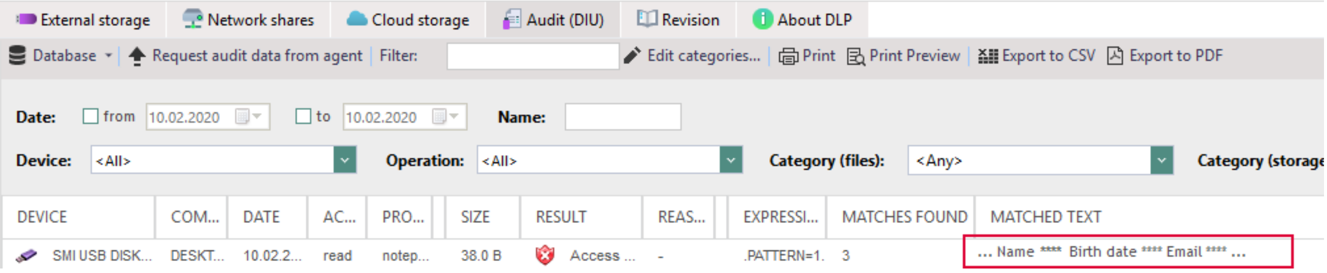
Figure 116. User message when accessing a file with DLP finding

6. Click **Save**.

The filter is enabled for a user.

User-defined entities

Custom entities are expressions that you save as a template. You can mark finds on such expressions as sensitive information. Sensitive information is not shown in plain text in the audit data, but hidden via ***.



Filter:

Date: □ from 10.02.2020 □ to 10.02.2020 Name:

Device: <All> Operation: <All> Category (files): <Any> Category (storage

DEVICE	COM...	DATE	AC...	PRO...	SIZE	RESULT	REAS...	EXPRESSI...	MATCHES FOUND	MATCHED TEXT
SMI USB DISK...	DESKT...	10.02.2...	read	notep...	38.0 B	Access ...	-	.PATTERN=1.	3	... Name **** Birth date **** Email **** ...

Figure 117. Sensitive info in audit data

Creating a used-defined entity

1. Go to **Product settings | DLP | Lexical expressions definition**.
2. Click the **User-defined entities** button.

   → The **User-defined entities** dialog appears.

3. Click **Add**.

→ A new entry appears in the list.

4. To edit the entity, select it from the list.
5. In the **Name** field, define a name for the entity.
6. In the **Expression** field, enter a search pattern.
7. Enable the **Case sensitive** box if the searched text is case sensitive.
8. To mark the expression as sensitive information and display it hidden in the audit data, enable the **Sensitive information** check box.
9. Click **Save**.
10. Add other entities if needed and click **Save**.

➥ The created user-defined entities appear in the **User-defined** tab of the expression editor. You can now use them in lexical expressions. For details, see: Creating a lexical expression

8.3. Scheduling scan tasks for computers

Setting up DAR for computers

1. Go to **Product settings | DLP | Scheduler**.
2. In the **Scheduler** area, click **Add**.

   → A new entry appears.

3. In the **Settings** area, enter a name for the action in the **Name** field.
4. In the **DLP filters** drop-down, select one or several filters. For details, see: Creating filters
5. In the **Scan mode** drop-down, select which scan to perform:
   - **Full scan**: Thorough scan of the entire device except network shares.
   - **My documents scan**: Scans the *My documents* folder. A user must be logged in to the system to perform this type of scan.
   - **Custom**: Scans selected files, folders or system folders locally on computers or network shares.
6. In the **Scan performance** drop-down, select how DLP scan influences the computer performance:
   - **Low**: the scan takes a lot of time, but requires less resources.
   - **Medium**: balanced use of time and resources during the scan.
   - **High**: the scan takes not so much time, but requires more resources.
7. If you are going to add network shares, files or folders to the list of scanned objects, define credentials of a user who has enough rights to access added network directories in the **Username** and **Password** fields.
8. In the **Objects to exclude from scan** area, add files, folders or file extensions, which must be excluded from scanning.

9. If the **Custom** scan mode has been selected, in the **Objects to scan** area, add files, folders or file extensions, which must be scanned locally on computers or on the network shares.
10. Define the date and time when to perform the scan.
11. Click **Save**.

➥ The planned scan can now be assigned to a computer.

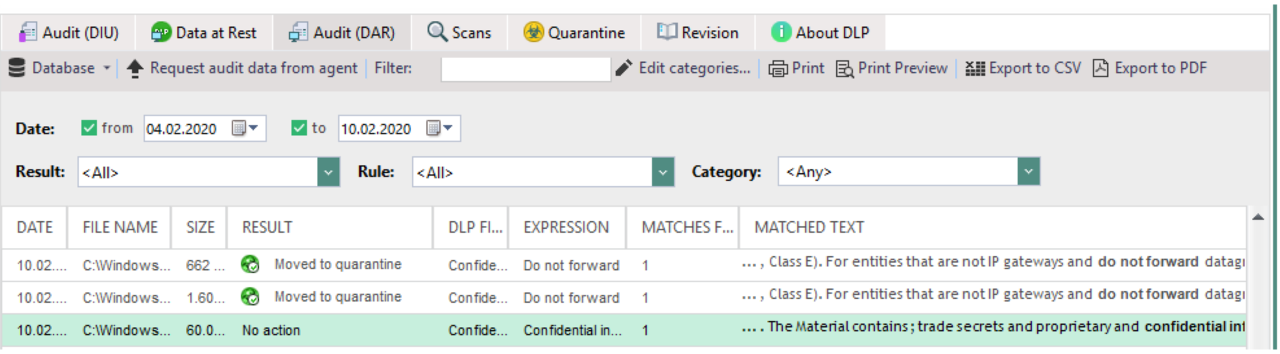
Enabling a planned scan for computer

1. Go to **Computer management | DLP** and select a computer.
   If you select **Default rights (computer)** under **Default policies**, the action is inherited to all computers with activated DLP and activated inheritance.
2. In the lower area, in the **Data at Rest** tab, select one or more actions.
3. To disable inherited actions, enable the **Activate individual settings** check box.
   Disable the **Activate individual settings** check box to assign other actions in addition to the inherited ones.
4. In the **Action** column, select what to do if a match occurs:
   - **No action (audit only)** to only write the fact of finding to the **Audit (DAR)** tab.
   - **Delete** to permanently delete files from their original location and write this event to the **Audit (DAR)** tab.
   - **Move to quarantine** to move to the **Quarantine** hidden folder locally and reformat these files so that user cannot open them.
5. Click **Save**.

➥ Once a scan starts, its progress appears in the **Scans** tab. The scan results appear in the **Audit (DAR)** tab.

8.4. Analyzing findings

Via the **Audit (DIU)** tab for **Data in Use** and the **Audit (DAR)** tab for **Data at Rest** you can see the audit data of the scans in the form of tables. Every finding is audited.
You can configure the displaying and filter the entries. The **Secure Audit** product is NOT required to view the logs of DLP events.



Date: ☑ from 04.02.2020 ☑ to 10.02.2020

Result: <All> Rule: <All> Category: <Any>

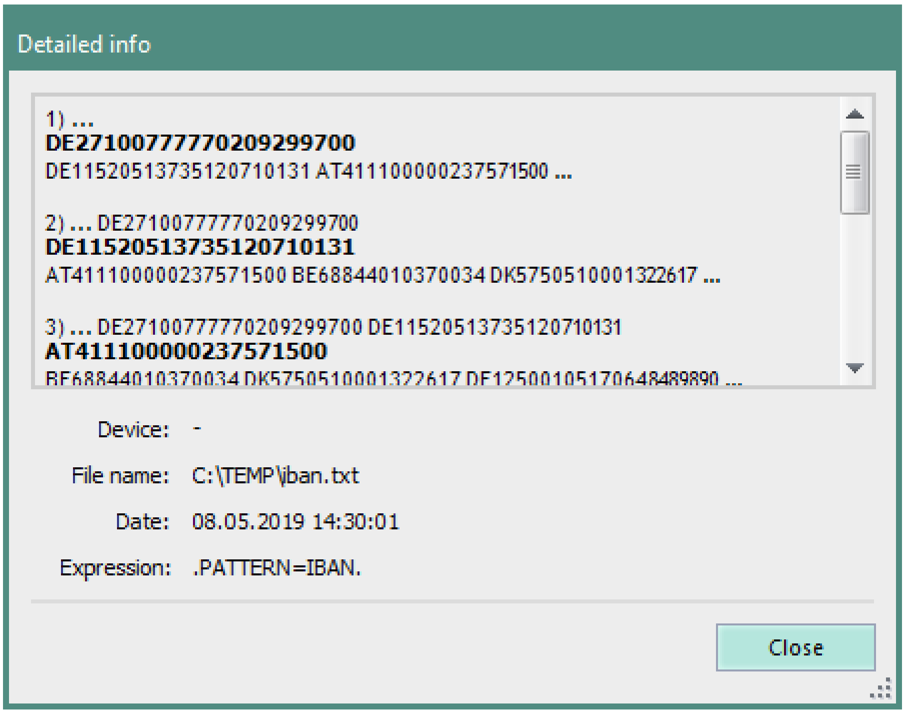
DATE	FILE NAME	SIZE	RESULT	DLP FI...	EXPRESSION	MATCHES F...	MATCHED TEXT
10.02....	C:\Windows...	662 ...	Moved to quarantine	Confide...	Do not forward	1	... , Class E). For entities that are not IP gateways and **do not forward** datagı
10.02....	C:\Windows...	1.60...	Moved to quarantine	Confide...	Do not forward	1	... , Class E). For entities that are not IP gateways and **do not forward** datagı
10.02....	C:\Windows...	60.0...	No action	Confide...	Confidential in...	1	... . The Material contains ; trade secrets and proprietary and **confidential** inf

Figure 118. Audit data of a scan with DAR

Showing findings

1. Go to **User management/Computer management | DLP | Audit (DIU)** and **Audit (DAR)**.
2. Configure data displaying and filter the data records, if needed.
3. Click in the **Matched text** column to show findings that do not fit the table column in a separate window.

   → A maximum of 4000 characters is displayed. You can see the complete list of findings in the DAR log file (enable the **Write log file for DLP DAR scans** option under **Administration | Clients | Log files**.



1) ...
DE27100777770209299700
DE11520513735120710131 AT411100000237571500 ...

2) ... DE27100777770209299700
DE11520513735120710131
AT411100000237571500 BE68844010370034 DK5750510001322617 ...

3) ... DE27100777770209299700 DE11520513735120710131
AT411100000237571500
BE68844010370034 DK5750510001322617 DE12500105170648489890 ...

Device: -

File name: C:\TEMP\iban.txt

Date: 08.05.2019 14:30:01

Expression: .PATTERN=IBAN.

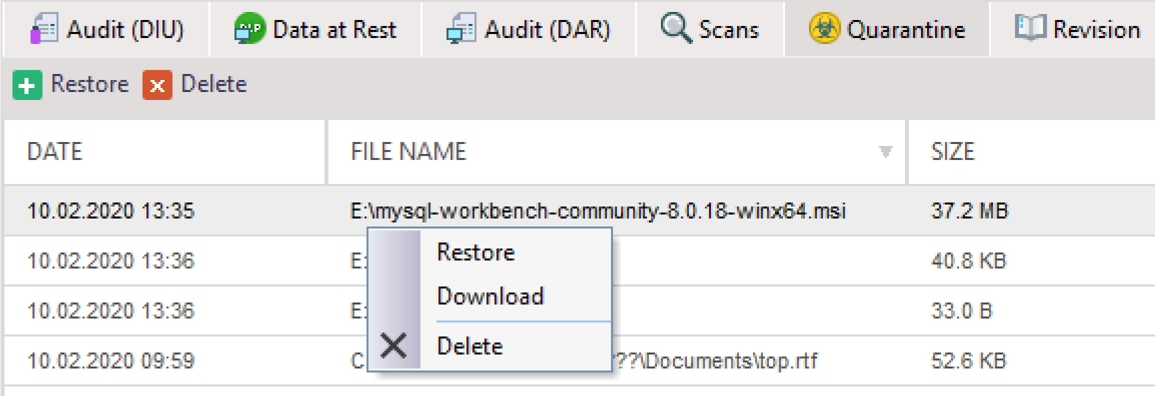
Figure 119. Detailed info on text findings

Processing quarantined files

1. Under **Computer management | DLP**, select a computer.
2. In the lower section, click on the **Quarantine** tab.

   → All files quarantined during a computer scan are listed.

3. Right-click an entry and select an action:
   - **Restore**: Restores a file to its original location and removes it from the quarantine.
   - **Download**: Saves a file in a defined location.
   - **Delete**: Deletes a file on the scanned computer and removes the entry from the quarantine.
     ! The file will be deleted permanently.



DATE	FILE NAME	SIZE
10.02.2020 13:35	E:\mysql-workbench-community-8.0.18-winx64.msi	37.2 MB
10.02.2020 13:36	E:	40.8 KB
10.02.2020 13:36	E:	33.0 B
10.02.2020 09:59	C ??\Documents\top.rtf	52.6 KB

Figure 120. Actions with quarantined files

9. EGOSECURE ANTIVIRUS

9.1. EgoSecure Antivirus - overview

EgoSecure Antivirus protects your computer from malware. Scannings are easily configured and planned.

You can view the status of the **EgoSecure Antivirus** installation on a computer using the **EgoSecure Console**. The status displays under **Computer management | EgoSecure Antivirus | Protection status**:

Status	Description
The computer is protected	**EgoSecure Antivirus** and two modules (ATC and Real-time protection) are activated.
The computer is threatened	At least one module is disabled.
The computer is not protected	**EgoSecure Antivirus** installation hasn't been finished yet.
Antivirus not installed	**EgoSecure Antivirus** product has been activated for a computer, but failed to be installed.

9.2. Installing and uninstalling EgoSecure Antivirus

EgoSecure Antivirus can be installed via the Console remotely or via the **EgoSecure Agent** installation using the MSI package.

WARNING

Possible conflict with existing third-party antivirus solution

Installation of two antivirus solutions from different vendors can result in serious conflicts, slowdowns, and system crashes.

- To avoid conflicts, make sure that 3rd party antivirus solution is not installed on a target computer.

Installing EgoSecure Antivirus on Agent remotely

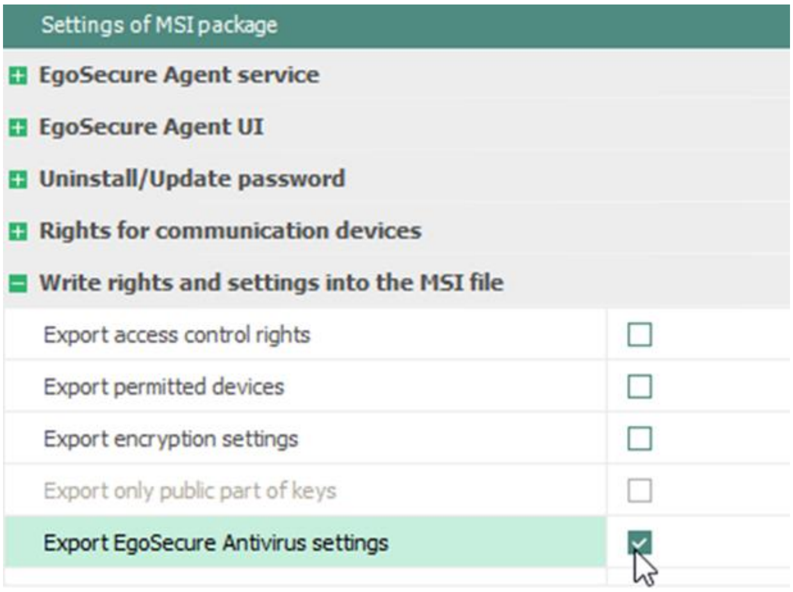
- Under **Computer management | Antivirus**, right-click a computer and select **Activate**.
  -OR-
- In **Computer management | Control**, right-click a directory object (computer or group) and select **Activate/deactivate products | EgoSecure Antivirus** from the context menu.

The license is activated. The installation on online computers starts. Installation on offline computers will be performed once they become online.

Installing EgoSecure Antivirus via MSI package

1. Activate the **EgoSecure Antivirus** product for a computer under **Computer management | EgoSecure Antivirus**. For details, see also: Activating products
2. Enable the **Export EgoSecure Antivirus settings** option under **Installation | EgoSecure agents | Create MSI package**.

   → If proxy server settings are defined and the Use proxy server option is enabled, the proxy server settings will be used for signature update on the Agent side via the Internet (if update from the EgoSecure Server is not possible).



Settings of MSI package

⊞ EgoSecure Agent service

⊞ EgoSecure Agent UI

⊞ Uninstall/Update password

⊞ Rights for communication devices

⊟ Write rights and settings into the MSI file

Export access control rights	☐
Export permitted devices	☐
Export encryption settings	☐
Export only public part of keys	☐
Export EgoSecure Antivirus settings	☑

Figure 121. Adding EgoSecure Antivirus settings to MSI package

3. Near **Selection of objects**, click ... to select the computers where the EgoSecure Antivirus product is already activated in step 1.

   → The **Users/computers selection** dialog appears.

4. Select the computers via a double-click and click **OK** to confirm.
5. Click **Generate**.

   → On the right, in the **Create MSI package** area, the information about the location and status of the MSI package generation displays.

6. Copy the **MSI** folder to removable storage or a network share.
7. On a network share/removable storage, create the following subfolders inside the MSI package:
   - ATC
   - AVDB_64 (or any name, which contains AVDB and 64)
   - AVDB_32 (or any name, which contains AVDB and 32)

8. Copy the following files to the **ATC** folder from the computer with the installed **EgoSecure Server**:
   - All files (except the **Plugins** folder) from the directory: **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - The files **versions.dat** and **versions.id** from the directory: **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\atc-sig-busi**
9. Copy the following files to the **AVDB_64** folder from the computer with the installed **EgoSecure Server**:
   - All files from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - The files **versions.dat** and **versions.id** from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\64**
10. Copy the following files to the **AVDB_32** folder from the computer with the installed **EgoSecure Server**:
    - All files from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
    - The files **versions.dat** and **versions.id** from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\32**
11. Run the **ESAgentSetup.exe** file on the computer where you want to install the **EgoSecure Antivirus**.

Uninstalling EgoSecure Antivirus

INFO	**Uninstallation only via the EgoSecure Console** **EgoSecure Antivirus** uninstallation is possible only via the **Console**. Local uninstallation from Agents is not possible.

1. Go to **Computer management | Antivirus**.
2. Right-click a computer and select **Deactivate** from the context menu.

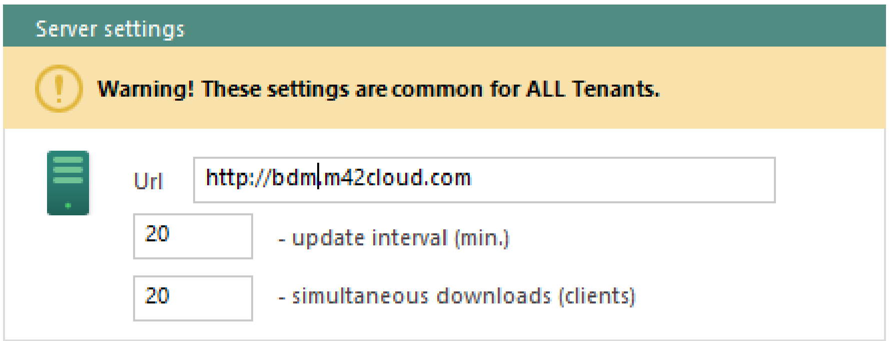
↳ The license is now deactivated and the uninstallation of **EgoSecure Antivirus** starts once the **Agent** is online.

9.3. Updating EgoSecure Antivirus

By default, the EgoSecure Server regularly checks for new virus signatures on the Internet. Once signatures are downloaded, automatic updates by the **EgoSecure Agent** become available at regular intervals. If required, **EgoSecure Antivirus** updates can also be triggered manually.

Configuring and performing updates

1. Go to **Product settings | Antivirus | Update settings**.
2. In the **Server settings** area, in the **URL** field, enter the URL from where the EgoSecure Server downloads signatures.
3. In the **Update interval** field, define how often the Server checks for new signatures on the Internet.
4. In the **Simultaneous downloads** field, define the number of Agents which can download signatures from the Server simultaneously.



Server settings

Warning! These settings are common for ALL Tenants.

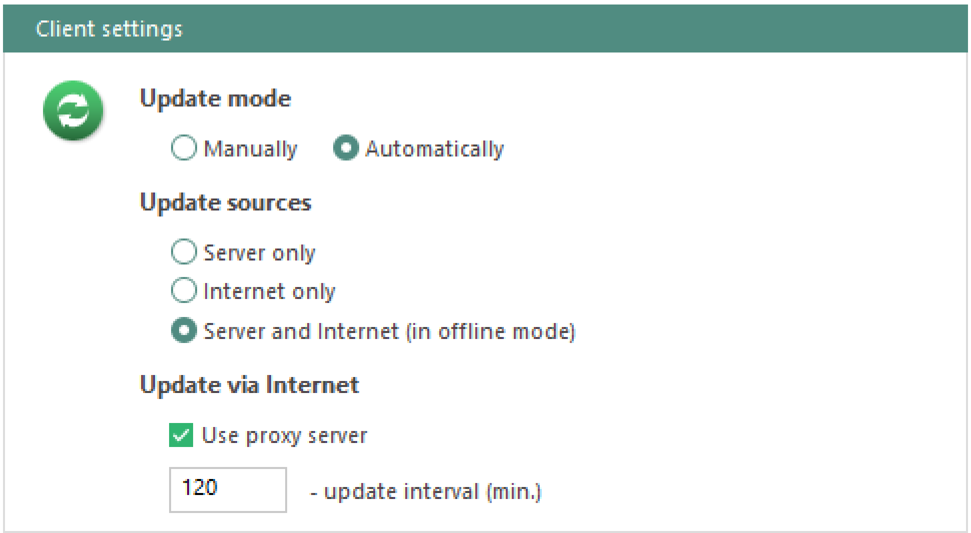
Url http://bdm.m42cloud.com

20 - update interval (min.)

20 - simultaneous downloads (clients)

Figure 122. Adjusting server settings for EgoSecure Antivirus

5. In the **Client settings** area under **Update mode**, select the option:
   - **Manually**, so that the **EgoSecure Antivirus** is not updated till the moment an administrator or a user initiates this process.
   - **Automatically** to update each time when new signatures appear on the Server.
6. Under **Update sources**, select the option:
   - **Server only** to allow the download of signatures only from the EgoSecure Server.
   - **Internet only** to allow the download of signatures only from the URL specified in the **Server settings** work area.
   - **Server and Internet (in offline mode)** to allow the download of signatures from the URL specified in the **Server settings** work area when **Agent** cannot update signatures from the EgoSecure Server.
7. For automatic updates: in the **Update interval** field, set the frequency of checking for signatures on the Internet when Agent becomes offline.
8. Enable **Use proxy server** check box to use proxy server when updating signatures from the Internet on the Agent side.
   Define proxy server settings under **Administration | Servers | Mail, proxy and others**.



Client settings

Update mode

○ Manually ● Automatically

Update sources

○ Server only
○ Internet only
● Server and Internet (in offline mode)

Update via Internet

☑ Use proxy server

120 - update interval (min.)

Figure 123. Adjusting client settings for EgoSecure Antivirus

9. Click **Save**.
10. To perform a manual update via the **Console**, do one of the following steps:
    a. Right-click a computer under **Computer management | Antivirus** and select **Update signatures DB** from the context menu.
    OR
    b. Under Computer management **| Antivirus**, in the Protection status tab, click the Update now button.

Performing updates on Agents offline

When Agent works in the offline mode, the Agent tries to perform automatic updates via the Internet. For details, see: Configuring and performing updates
If updates via the Internet are not allowed or there is no Internet connection, the update can be performed manually on the Client.

Performing manual updates on Agents in offline mode

1. Copy the MSI package that you generated during the installation of **EgoSecure Antivirus** to an external storage medium or network share, or generate a new MSI package, if necessary. For details, see: Installing EgoSecure Antivirus via MSI package (steps 1-4)
2. On a network share/removable storage, create the following subfolders inside the MSI package:
   - ATC
   - AVDB
3. Copy the following objects to the **ATC** folder from the computer with the installed **EgoSecure Server**:
   - All files (except the **Plugins folder**) from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\repository**

   - The files **versions.dat** and **versions.id** from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\atc-sig-busi**

4. Copy the following files to the **AVDB** folder from the computer with the installed **EgoSecure Server**:
   - All files from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\repository**
   - *By using 32-bit operating systems*: the files **versions.dat** and **versions.id** from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\32**
   - *By using 64-bit operating systems*: the files **versions.dat** and **versions.id** from the directory **C:\ProgramData\EgoSecure\EgoSecureServer\AVDIR\Db\64**
5. On the Agent, under C:\ProgramData\EgoSecure\EgoSecureAgent,
   a. Replace existing **AVBD** and **ATC** folders with the folders from a network share/removable storage (if AVDB and ATC folders WITHOUT a timestamp existed before in this location on the Agent).
   OR
   b. Copy **AVBD** and **ATC** folders from a network share/removable storage to this location (if there are no AVDB and ATC folders WITHOUT a timestamp in this location on the Agent).
6. Update virus signatures on Agents. For details, see the EgoSecure Agent – User guide.

9.4. Scheduling and performing virus scans

With **EgoSecure Antivirus**, you can save and manage the settings for virus scans in the so-called scan profiles. You can also use the **Scheduler** to plan regular scans in advance and perform them automatically. All the scans initiated by user or administrator are displayed in the **Scans** tab.

ATTENTION	**Scanning encrypted files** Encrypted files are not scanned (impacts only admin scans) as the scan runs from the system.

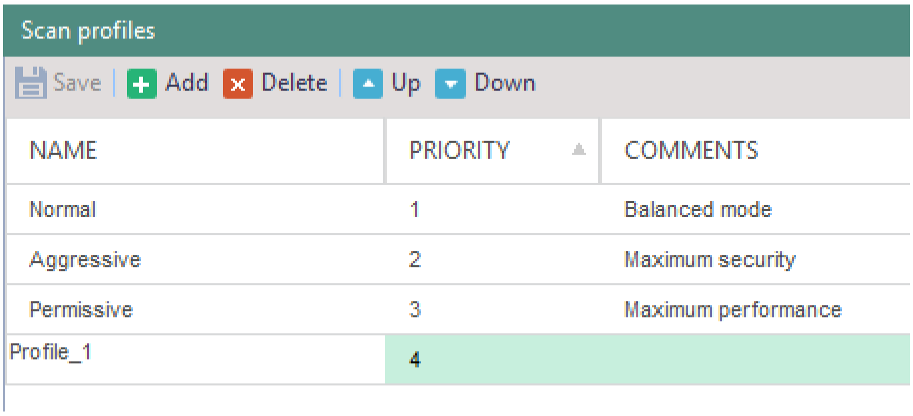
Creating and assigning scan profiles

Scan settings are defined in scan profiles. In addition to the three default scan profiles with presettings (Normal, Aggressive and Permissive), a profile with individual settings can be created and assigned to a computer.

Creating a scan profile

1. Go to **Product settings | Antivirus | Scan profiles**.
2. In the **Scan profiles** area, click **Add**.

   → A new entry appears in the list.
3. In the **Name** column, enter a scan profile name.



NAME	PRIORITY	COMMENTS
Normal	1	Balanced mode
Aggressive	2	Maximum security
Permissive	3	Maximum performance
Profile_1	4	

Figure 124. Overview of scan profiles for EgoSecure Antivirus

4. In the **Scan options** area, define the settings for the scan profile:
   - **On-access**: scans objects on access, e.g., when opening or copying (real-time protection).
   - **On-demand**: starts the scan manually either via the context menu of the object or by initiating a scan (quick, complete or user-defined).
   - **Actions**: Defines actions for infected or suspicious objects.
     - **Automatic** for infected objects means that Antivirus first tries to disinfect a file and then to move to quarantine. If it fails, the file is deleted.
     - **Try to disinfect else delete** for infected objects means that the Antivirus tries to disinfect the object. If the object cannot be disinfected, the file is deleted.

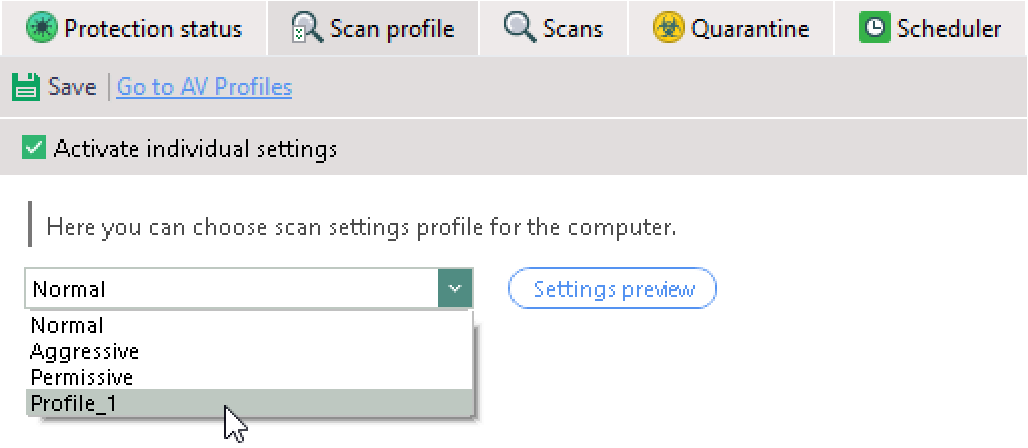
       ! The action result **successfully disinfected** informs that the file has been disinfected. This also means that the file was deleted, as some disinfection includes deletion.
   - **Active Threat Control**: Monitors all active processes and identifies potential threats.
5. Click **Save**.

Assigning a scan profile

1. Under **Computer management | Antivirus**, select a computer.
2. In the **Scan profile tab**, enable **Activate inheritance settings**.

   → The inheritance is now disabled for the selected computer and you can now assign individual scan profiles.

3. Select a scan profile from the drop-down menu.



☑ Activate individual settings

Here you can choose scan settings profile for the computer.

Normal

Figure 125. Assigning scan profile for selected computer

4. Click **Save**.

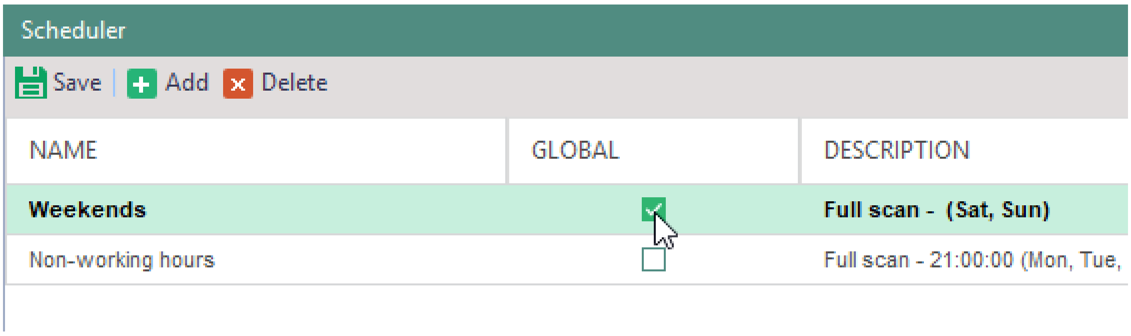
Scheduling and assigning automatic scans

Creating a task

1. Go to **Product settings | Antivirus | Scheduler**.
2. Click **Add**.

   → A new entry appears in the list.

3. In the **Name** column, enter a name for a task.
4. Enable the check box in the **Global** column to assign the task to all computers of the directory service.



NAME	GLOBAL	DESCRIPTION
Weekends	☑	**Full scan - (Sat, Sun)**
Non-working hours	□	Full scan - 21:00:00 (Mon, Tue,

Figure 126. Overview of created automatic scans

5. In the **Settings** area, select a scan mode and scan frequency (once or weekly). The following scan modes are available:
   - **Quick**: system directories and system memory are scanned.
   - **Full**: internal and external memory are scanned.
   - **Custom**: objects defined by administrator are scanned.
6. Add objects that must be scanned (in case of custom scanning).
7. Click **Save**.

Assigning a task to a directory object

1. Go to **Computer management** and select a computer.
2. Under **Antivirus | Scheduler**, enable the **Activate individual settings** check box to disable inheritance.

   → The previously inherited tasks remain enabled, uncheck them, if necessary.
3. Select a task from the list.
   Global tasks will always be additionally applied no matter whether they are enabled or disabled in the first column and whether inheritance is enabled or not.
4. Click **Save**.
5. To initiate the scanning now not waiting for a scan start:
   a. In the **Computer management – Antivirus** area, right-click a computer.
   To multi-select, hold down `Ctrl` and select the computers.
   b. Select **Scan now | [scan type]** from the context menu.

↳ Once the scan starts, its progress is shown on the **Scans** tab. To cancel a running scan, right-click it and select **Stop**.

9.5. EgoSecure Antivirus quarantine

EgoSecure Antivirus places objects in quarantine under the following circumstances:

- Infected objects when **Try to disinfect else move to quarantine** or **Move to quarantine actions** are applied.
- Suspicious objects when **Move to quarantine** action takes effect.
- Objects for which a user selected **Move to quarantine** (If **User's choice** action is selected in scan options).

Actions with quarantined objects

1. In **Computer management\Reports | Antivirus | Quarantine**, right-click a quarantined object.
2. Select one of the following options:
   - **Restore** to move the object from the quarantine list to the place where it was stored before.
   - **Restore and exclude from scanning** to remove the object from the quarantine list, place it to its original location and exclude from scanning on this computer.
   - **Restore and add to global exclusion list** to add the object to **Product settings | Antivirus | Exclusions**. This object will be excluded from scanning on all computers of a directory.
   - **Delete** to remove the object from the quarantine list and from a user computer.

9.6. Managing EgoSecure Antivirus exclusions

The following objects are excluded from scans:

- Static system files (for details, see: Default exclusions)
- Exclusions specified by a user on **EgoSecure Agent** (if the Change antivirus options check box is enabled under User management | Antivirus | Settings).
- Objects added to the global exclusion list in **Console** under **Product settings | Antivirus | Exclusions**.

Adding objects to exclusions

You can add objects to the list of exclusions in two different ways: either via the list of quarantined objects on a computer or by manually inserting a file or folder name.

Adding object to a quarantine list

1. Go to **Computer management\Reports | Antivirus | Quarantine**.
2. Right-click an object and select Restore and add to global exclusion list.

➥ The object is excluded from scans on all computers of the directory.

Adding object via file or folder name

1. Go to **Product settings | Antivirus | Exclusions**.
2. Click **Add file** or **Add directory** to select file/folder path.
3. Click **Save**.

➥ The selected object is excluded from scans on all computers of the directory.

Adding process-based exclusions

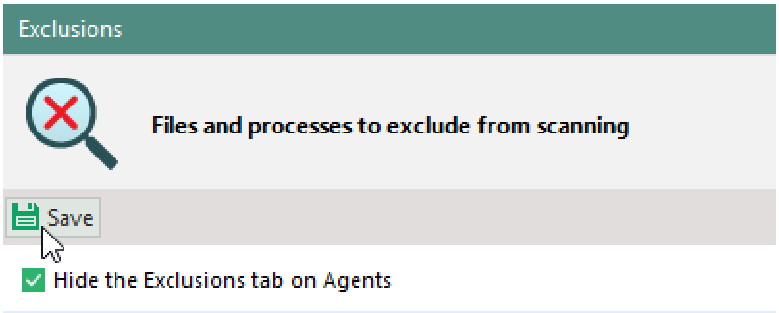
1. Go to **Product settings | Antivirus | Exclusions**.
2. Click **Add process** to select a process.
3. Clear the **Check for certificate** check box if the process doesn’t have a valid certificate.
4. Click **Save**.

➥ All the files accessed by selected process are excluded from scans on all computers of the directory.

Hiding the Exclusion tab on the Agent side

For the reasons of security, you can hide the list of defined exclusions on Agent so that nobody can see them.

1. Go to **Product settings | Antivirus | Exclusions**.
2. Enable the **Hide the Exclusions tab on Agents** option.
3. Click **Save**.


Exclusions

Files and processes to exclude from scanning

Save

☑ Hide the Exclusions tab on Agents

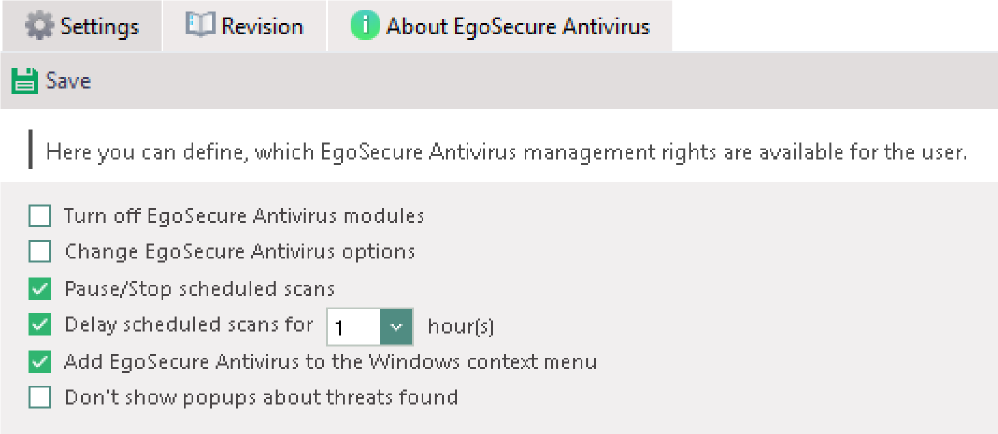
Figure 127. Hiding exclusions on Agents

9.7. Managing access rights to EgoSecure Antivirus

In the **User management** settings, you can assign individual user rights for managing **EgoSecure Antivirus**.

Specifying EgoSecure Antivirus rights for a user

1. Go to **User management** and select a user.
2. In the **Settings** tab, enable the options available for the user.



Here you can define, which EgoSecure Antivirus management rights are available for the user.

□ Turn off EgoSecure Antivirus modules
□ Change EgoSecure Antivirus options
☑ Pause/Stop scheduled scans
☑ Delay scheduled scans for 1 hour(s)
☑ Add EgoSecure Antivirus to the Windows context menu
□ Don't show popups about threats found

Figure 128. Assigning access rights for EgoSecure Antivirus

3. Enable **Pause/Stop scheduled scans** and **Delay scheduled scans** options to allow a user to pause/stop/delay scheduled scans assigned by administrator. User-owned scheduled tasks can be stopped independently of the options state.
4. Enable the **Change EgoSecure Antivirus options** option to grant the following permissions to the user:
   - Create and edit planned scans
   - Manage exclusions
   - Move objects from the quarantine to a location other than the original one

A user is not allowed to edit administrator exclusions and scheduled tasks 🌐 no matter whether the **Change Antivirus options** check box is enabled or disabled.

5. Click **Save**.

10. INSIGHT ANALYSIS

Insight Analysis is activated on a user and on a computer. The product logs events of the **Agent** and displays results in the form of diagrams and graphs. Allows for viewing the percentage of video files copied by users to flash cards, the number of social network sites visited, applications opened etc. Requires 10.1 EgoSecure Server version and higher.

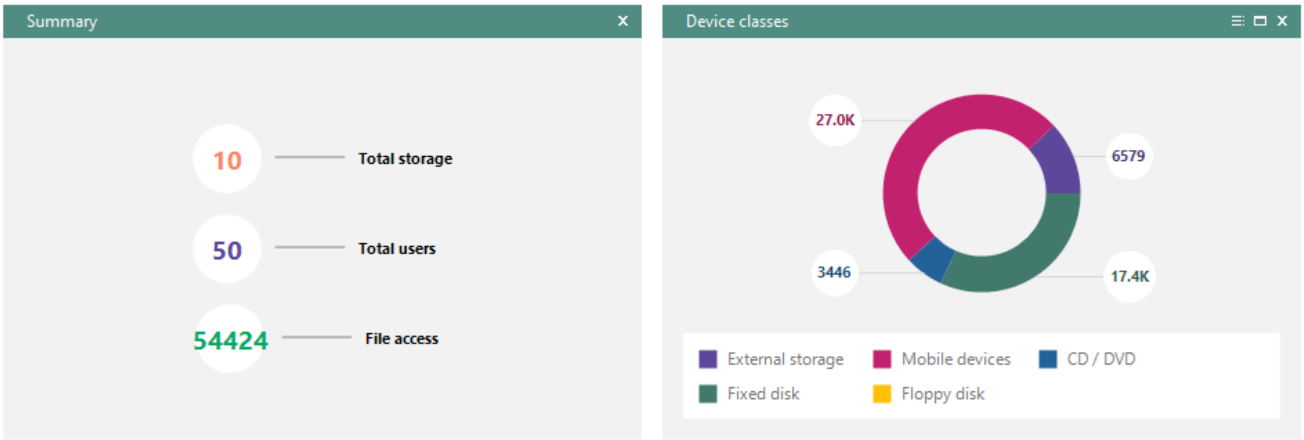


Figure 129. Graphical Insight report

INFO

Limited functionality in the trial version

- The **Details** work area with the reports in the tabular form is not available.
- **User names** are not shown.

10.1. Activating Insight Analysis

You can activate **Insight Analysis** for a user and a computer.

Activating Insight Analysis and applying basic settings

1. Under **User management**/**Computer management**, activate the product for a user, for a computer or for both.
2. Under **Product settings | Insight Analysis | Settings**, in the **Secure Audit** area, select events to be written for **Insight Analysis**.
3. To collect data from network shares and thin client storage, additionally enable the **Allow thin client storage control** and **Allow network shares control** options for a computer under **Computer management | Settings | Client settings**.
4. To additionally define specific network shares for data collection, go to **Product settings | Audit | Network share** and add either the network shares from where

the data is collected (in case of a white list) or only the network shares from where the data collection is blocked (in case of a black list).

5. To collect data from clouds, additionally define the clouds to control under **User management | Settings | Cloud storage**.
6. In the **Secure Audit reports calculations** area, define how statistics taken from all reports under **Reports | Audit** panel must be calculated to align with your company needs:
   - **User-based:** statistics are taken from a user, for whom the **Insight Analysis** product is activated. This user can sign in to different computers with one account.
   - **Computer-based**: statistics are taken from all users of a computer, for which the **Insight Analysis** product is activated. Several users with several accounts can sign in to one computer and statistics is calculated for the computer on the whole.
7. Click **Save**.

INFO

Audit-like functionality

- Insight Analysis enables the audit-like functionality for writing insight data to the database, which can lead to database filling if the database is not managed properly.

10.2. Defining favorite charts

You can create a custom view that shows your favorite charts.

Configuring My Insight

1. Go to **Insight Analysis | Favorites | My Insight**.
2. Click Select chart.

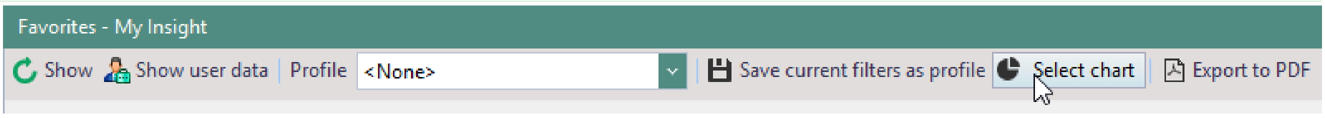


Figure 130. Creating a user-specific view

→ The **Select object** dialog appears.

3. Select the objects and click **Save**.

The favorite diagrams are now saved under **My Insight**.

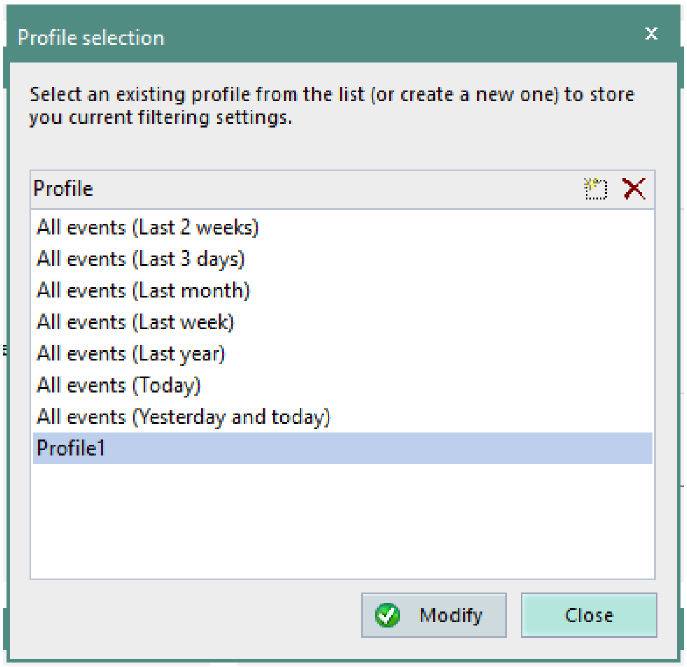
10.3. Using profiles

To quickly view only the necessary Insight information, create profiles. For example, administrator needs to see only the percentage of outbound traffic within last week.

Creating or editing a profile

1. Define settings to be included in a profile:
   a. Define a period of time and select whether to display ignored data or data without a category. For details, see: Using categories
   b. Filter data. For details, see: Using filters.
2. Click on **Save current filters as profile**.

   → The **Profile selection** dialog appears.
3. Click on ⬚ to add new profile or select a previously created profile from the list.



Profile selection

Select an existing profile from the list (or create a new one) to store you current filtering settings.

Profile

All events (Last 2 weeks)
All events (Last 3 days)
All events (Last month)
All events (Last week)
All events (Last year)
All events (Today)
All events (Yesterday and today)
Profile1

Figure 131. Creating a new profile

4. Enter a profile name and click `ENTER` to confirm.
5. Click **Modify** to save the changes.
6. Close the dialog window.

Loading a profile

- Select a profile from the **Profile** drop:

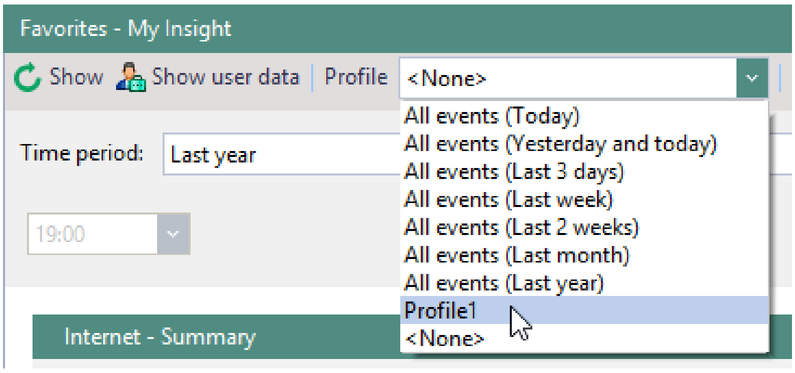


Figure 132. Loading a profile

The selected profile is now loaded.

10.4. Filtering reports

- Click a part of a graph or a property in the legend to filter all reports based on this property.

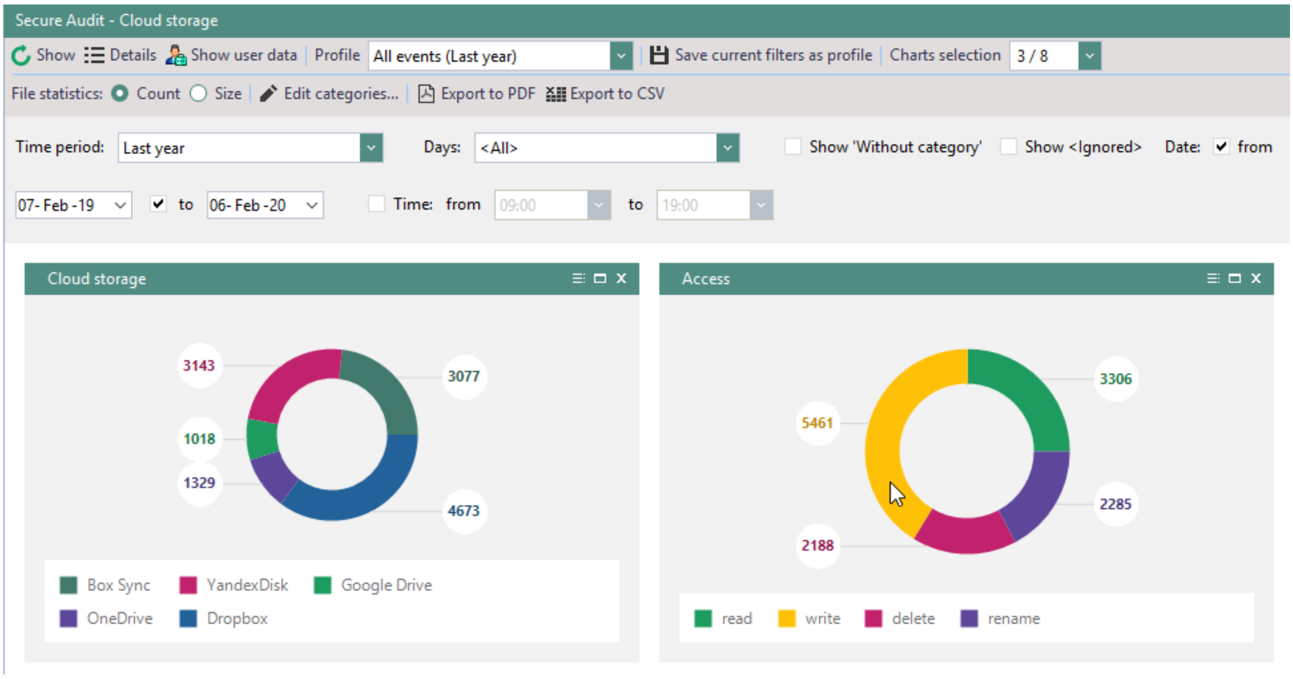
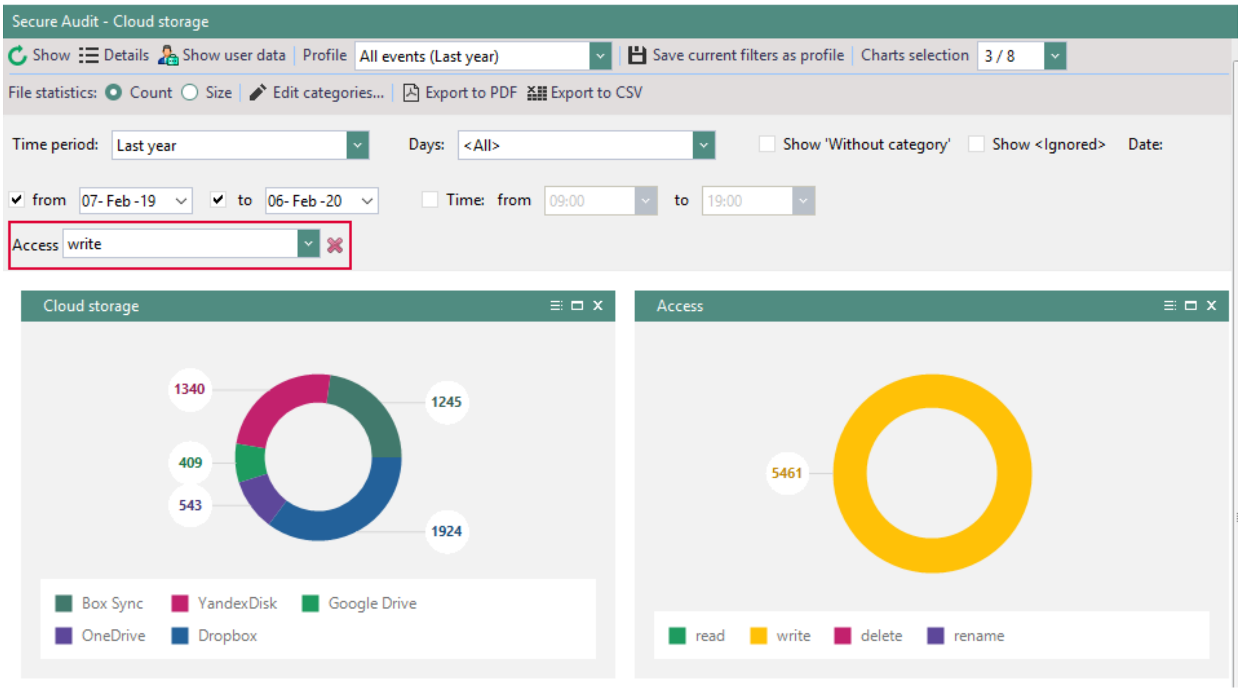


Figure 133. Clicking on write access

→ The settings now display the property according to which the data is filtered:



Secure Audit - Cloud storage

Show | Details | Show user data | Profile: All events (Last year) | Save current filters as profile | Charts selection: 3 / 8

File statistics: ● Count ○ Size | Edit categories... | Export to PDF | Export to CSV

Time period: Last year | Days: <All> | □ Show 'Without category' | □ Show <Ignored> | Date:

☑ from 07- Feb -19 | ☑ to 06- Feb -20 | □ Time: from 09:00 to 19:00

Access: write ✖

Figure 134. Filter results for writing access (including the related read access)

- To remove the filter, click on ✖.

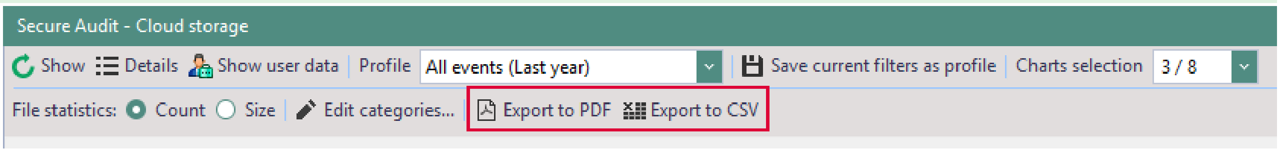
INFO

Filtering write access

If you filter data by write access, the read access made is also displayed. A user/computer who has write access automatically also has read access.

10.5. Exporting reports

You can export reports of a certain panel manually or of a specific time automatically. The export is performed in a PDF file. With a manual export, you can also write the data to a CSV file.



Secure Audit - Cloud storage

Show | Details | Show user data | Profile: All events (Last year) | Save current filters as profile | Charts selection: 3 / 8

File statistics: ● Count ○ Size | Edit categories... | Export to PDF | Export to CSV

Figure 135. Exporting report to file

INFO

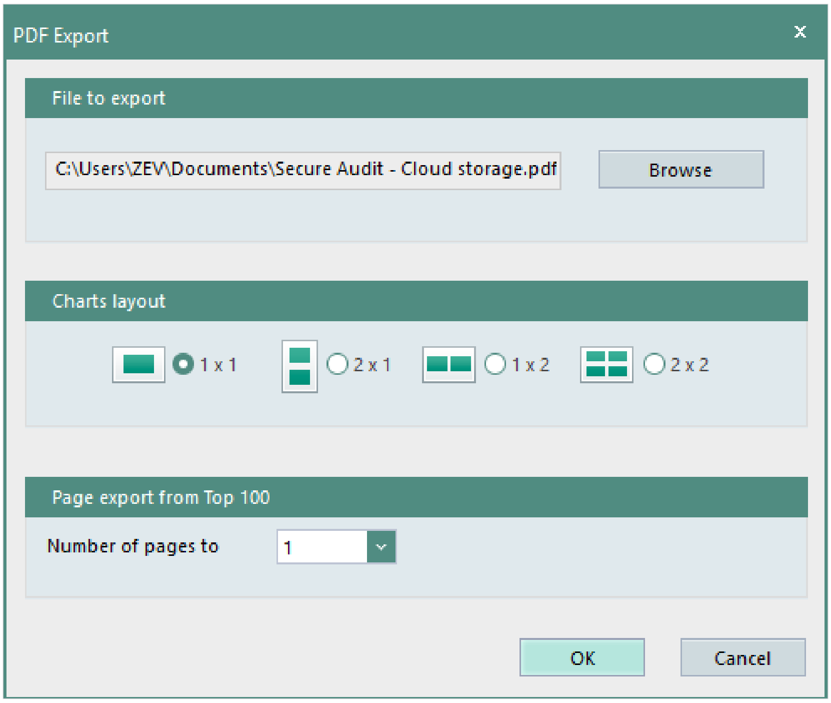
Data for first export

On first report export or for the reports that have’nt been exported for more than 30 days: only the data for the last 24 hours is exported.

Manual export

1. Under **Insight Analysis**, select an element of a panel (as shown in the example, **Insight Analysis | Audit | External storage**).
2. If necessary, filter the data or select a profile.
3. To export to PDF, click **Export to PDF** on the toolbar.

   → The **PDF Export** dialog appears.



PDF Export

File to export

C:\Users\ZEV\Documents\Secure Audit - Cloud storage.pdf

Charts layout

● 1 x 1 ○ 2 x 1 ○ 1 x 2 ○ 2 x 2

Page export from Top 100

Number of pages to: 1

Figure 136. Selecting PDF layout for exported data

4. Click **Browse** to specify report file location.
5. Select a location and layout for the displaying of the diagrams (portrait/landscape, number of diagrams per page).
6. Specify how many pages of a top 100 statistic should be exported (starting with top 1).
7. Click **OK**.

↳ The PDF is created.

Automatic export

1. Go to **Product settings | Insight Analysis | Report generation**.
2. In the **Server** drop-down menu, select a computer where **Server** is installed. Reports are saved to this computer in the folder defined in the next step.
3. In the **Directory** field, click **Browse** to specify a directory on the **Server** for storing report files.
4. Define time and date of the first sending of a report.
5. To send the export data also to e-mail:

   a. In the **Recipients** field, enter an e-mail address or a user name for sending reports there.
      If you specify a user name, an email must be specified for a user in **User management**.
   b. Under **Administration | Servers | Mail, proxy and others**, define the e-mail address settings. For details, see: Setting up SMTP server

6. In the **Report generation schedule** area, click **Add**.

   → A new entry appears.

7. Click on the columns to edit the settings.

Column	Description
Insight	Specifies the data type for which statistics are to be exported.
OU	Defines domains, organizational units or folders to which the export should be limited.
Time period	Specifies the time interval after which an automatic export should take place.
Profile	Defines a user-specific profile or a period for which a report is to be exported. If **<None>** is selected, the **Time period** column is taken into account (e.g.: select **Every week** in **Time period** column to include the data of the last week to a report).
Charts selection	Determines the diagrams of the respective data usage area that are exported. By default, all diagrams are selected.
Pages from top 100	Specifies how many pages of a top 100 statistic are exported (max. 10).
Charts layout	Determines the output layout: portrait or landscape, number of diagrams per page (number 1: number of rows, number 2: number of columns)
Last run	Displays the date and time of the most recent export.

8. Click **Save**.

10.6. Protecting user data displaying with a password

You can protect access to user data in reports with simple/double password protection. In the exported data and in the Console, a random sequence of letters is displayed instead of the user data. User data are only shown in the Console after entering the password(s). You need to enter the password each time you move to a different area of **Insight Analysis**.

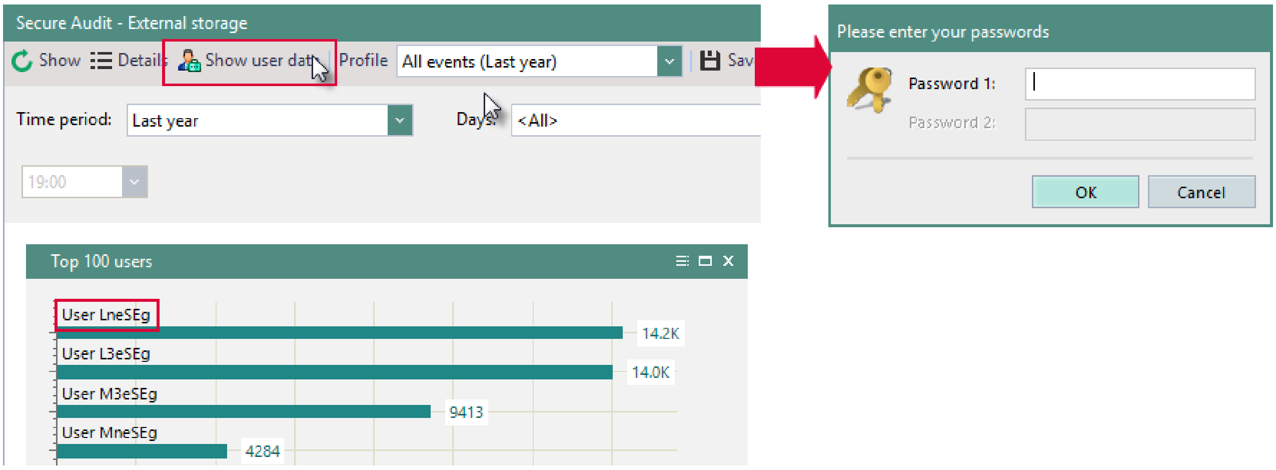


Figure 137. Showing user data in Insight Analysis

Enabling password protection

1. Go to **Product settings | Insight Analysis | Settings**.
2. Enable the **Protect user data with password** check box.
3. Select whether to protect with one or with two passwords.
4. Enter the password:
   a. Near the password, click **Change...** .
   → The dialog for entering password appears.
   b. Enter the password and confirm with **OK**.
5. Save the settings.

Changing password

1. Go to **Product settings | Insight Analysis | Settings**.
2. Click in the password field and then on **Change...** .
3. The dialog for entering passwords opens.
4. Enter the current password and define the new password.

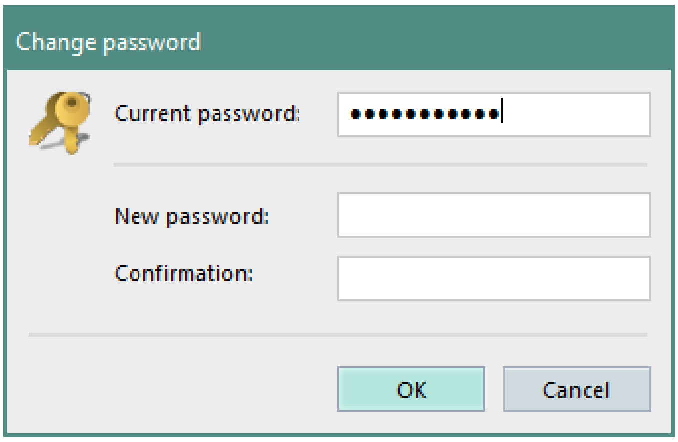


Figure 138. Changing password for displaying user data

5. Click **OK** to confirm.

11. INTELLACT AUTOMATION

IntellAct Automation (IAA) audits and analyzes the audited data to trigger protective measures for critical events. Use rules to define which actions must be executed in response to a critical event on the end device (Agent) or on the Server.

INFO

Limited IntellAct Automation functionality without IntellAct Automation license

If there is no license for **IntellAct Automation**, only the following functionality is available:

- All actions for all events under **Product settings | IntellAct | Rules - Server**.
- The **Mail notification** and **SNMP notification** actions under **Product settings | IntellAct | Rules - Client**.

You can configure predefined rules for servers and clients, as well as custom rules for specific operations. Depending on the rule type, certain actions can be triggered.

11.1. Actions for IntellAct events

When you define rules in IntellAct Automation, you can define certain actions that should be triggered when the corresponding process occurs or the rule is violated. Different actions are available depending on the type of the process.

Action	Description	Availability
Mail notification	Notification about the rule violation is send to the specified e-mail address. *Additional configuration*: set up the SMTP server settings. *Additional product activation*: required products to trigger mail and SNMP (only client rules). See also Grouping mail notifications (only for Rules - Custom and client rules).	All rules
SNMP notification	Notification about the rule violation is send to the specified e-mail address. *Additional configuration*: set up the SNMP server settings. *Additional product activation*: required products to trigger mail and SNMP (only client rules).	All rules

Inform tenant admins	Notification is sent via e-mail to the address specified under **Administration | Superadmin | Administrators & scopes**.	Server rules (only Audit data size control and Database size control)
Trigger workflow	A workflow is triggered in **Matrix42 Workspace Management**. For details, see: Triggering Matrix42 workspace management workflows via IntellAct Automation	Client rules
Deny access	**No access** status for all devices or for the selected ones is shown on Agent within the defined period of time. **<Used device>** blocks access only on the devices where the limit is violated. Activate **Access Control** for a user.	Client rules (except **Access rights requests**), Rules - Custom
Send status to Macmon	The defined status is sent to Macmon. Activate Macmon and define its parameters under **Administration | NAC | Macmon settings**. Activate NAC under **Administration | NAC | NAC settings**.	Client rules (except **Access rights requests**), Rules - Custom
Shut down computer	The computer of a user will be shut down.	Client rules, Rules - Custom
Show user message	A message is displayed to the user informing him of the rule violation.	Rules - Custom

Grouping mail notifications for events that occur on clients

Manage mail notifications about the violation of custom and client rules so that notifications about an event on one client are grouped and sent as a single message.

1. Go to **Product settings | IntellAct | Settings**.
2. Enable the **Group mail notifications within** option.
3. Select within which time period the mail notifications about one event are grouped in a single message.

   ! **Rules - Custom**: the event limit that is violated more than once a day (or till restart) is displayed in a message as one limit violation (first violation). For detailed info about all limit violations, go to **Product settings | IntellAct | Events | Incidents**.

4. Click **Save**.

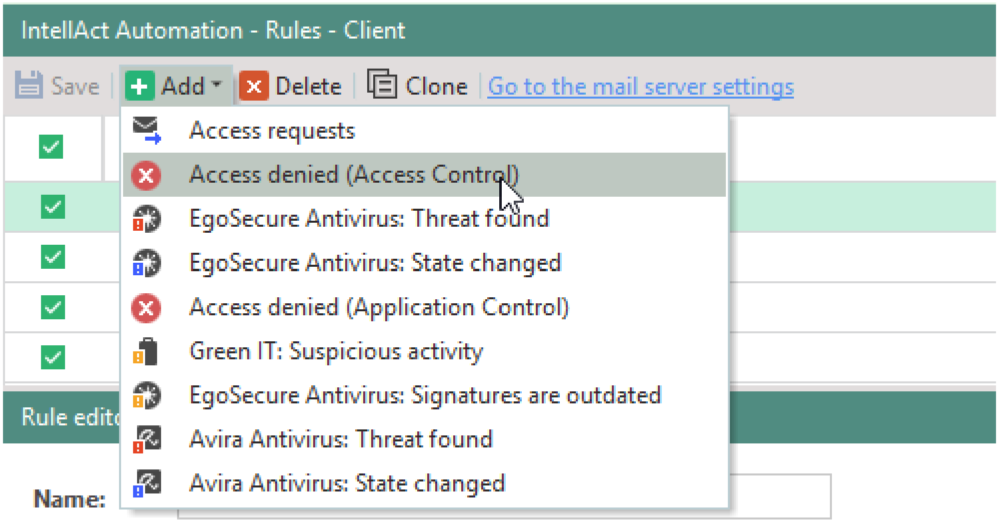
11.2. Configuring IntellAct Automation for Clients

With **IntellAct Automation**, you can define rules that monitor certain events on the client and undertake actions when they occur.

Defining rules for events on the clients

1. Go to **Product settings | IntellAct | Rules – Client**.
2. In the **IntellAct Automation – Rules – Client** area, click **Add** and select an event from the list.

   → A new entry appears in the list.



IntellAct Automation - Rules - Client

Save | Add | Delete | Clone | Go to the mail server settings

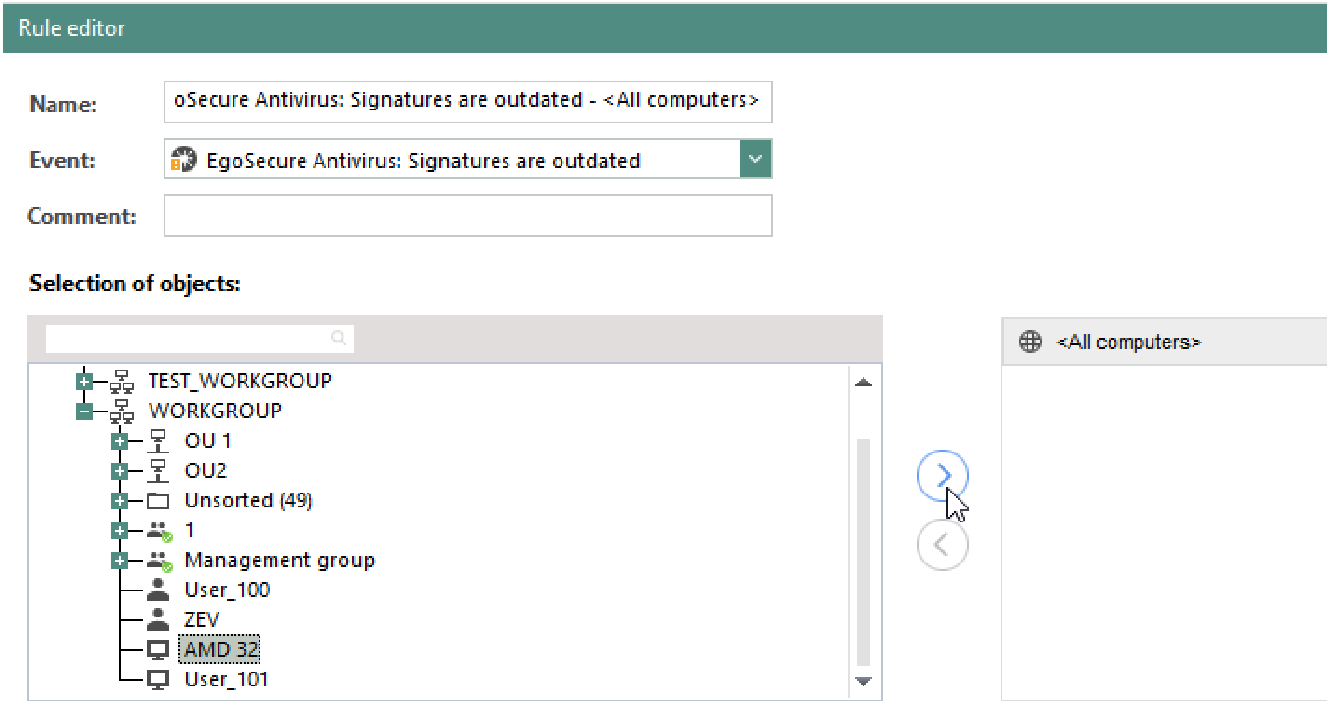
- Access requests
- Access denied (Access Control)
- EgoSecure Antivirus: Threat found
- EgoSecure Antivirus: State changed
- Access denied (Application Control)
- Green IT: Suspicious activity
- EgoSecure Antivirus: Signatures are outdated
- Avira Antivirus: Threat found
- Avira Antivirus: State changed

Rule edit

Name:

Figure 139. Adding IntellAct rule for operation on the client

3. To assign the rule to a certain user or computer, select a directory object under **Selection of objects**. If no object is selected, the rule is assigned to all users or all computers. For details, see: Assigning IntellAct rules



Rule editor

Name: oSecure Antivirus: Signatures are outdated - <All computers>

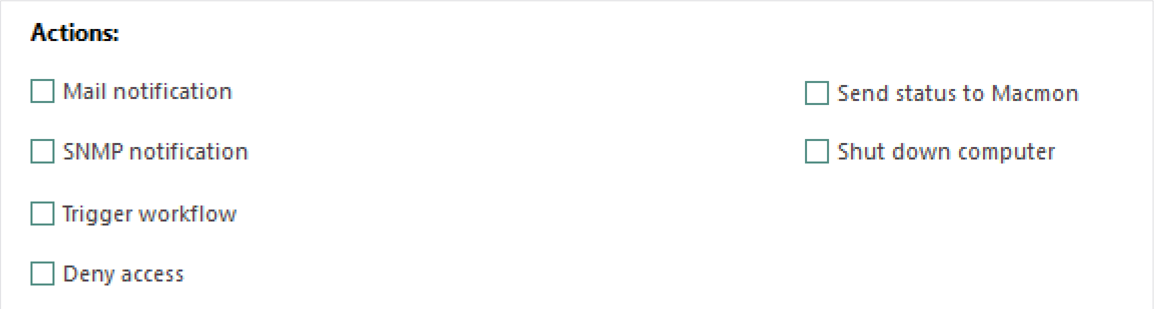
Event: EgoSecure Antivirus: Signatures are outdated

Comment:

Selection of objects:

Figure 140. Assigning a client event

4. For **Green IT: Suspicious activity** as well as for **EgoSecure Antivirus: signatures are outdated**, define the following settings under **Criteria**:
   - **Green IT: Suspicious activity**: define the regular working hours. Activities of the client outside of the specified time are considered a rule violation.
   - **EgoSecure Antivirus: signatures are outdated**: set the number of days since the last update after which signatures are considered outdated. The signatures are downloaded from the Internet to the Server and then updated on Agent. For details, see: Update settings for Antivirus
5. Under **Actions**, define what actions **IntellAct Automation** performs when an event occurs. For details, see: Actions for IntellAct rules



Actions:

☐ Mail notification

☐ SNMP notification

☐ Trigger workflow

☐ Deny access

☐ Send status to Macmon

☐ Shut down computer

Figure 141. Selection of possible IntellAct actions

6. Click **Save**.

Product activation for events to trigger Mail notifications and SNMP notifications

For users or computers from which the IntellAct information is collected, make sure to activate the following products to send mail or SNMP notifications:

Event	Additional product activation required
Access denied (Access Control)	🟩 Access Control (user or computer) 🟩 Secure Audit (user or computer)
Access denied (Application Control)	🟩 Application Control (user or computer) 🟩 Secure Audit (user or computer)
Access requests	🟩 Access Control (user or computer)
EgoSecure Antivirus: Signatures are outdated	🟩 EgoSecure Antivirus
EgoSecure Antivirus: Threat found	
EgoSecure Antivirus: State changed	

Green IT: Suspicious activity	🟩 Green IT

Blocked access due to IntellAct Automation

One possible action that can be triggered by IntellAct rules is to block user access to certain devices. A user, for example, has a limit of writing two files a day to external storage. Once the limit is exceeded, further access to external storage media can be blocked, for example, for an hour.

> INFO
>
> **Access rights due to IntellAct vs. Access Control**
>
> **IntellAct Automation** access rights have a priority over user/computer rights. Only permitted devices can overlap **IntellAct Automation** rights.

Restoring access denied by IntellAct

1. Select a user in **User management**.
2. Under **User management | Control | Devices and ports** tab, right-click a device.
3. Select **IntellAct Automation - unblocking code...** from the context menu.

   → The **Unblocking code generation – IntellAct Automation** dialog appears.
4. In the **Event** drop-down menu, select one of the following:
   a. A specific event to cancel access restriction due to this event and save access restriction (if any) because of another IntellAct event.
   b. **<All events>** to restore access to the device that happened due to several IntellAct events.
5. Click **Generate**.
6. Copy the code and send it to a user.

   → The client can now enter the code via the **EgoSecure Agent** and receive granted access rights:

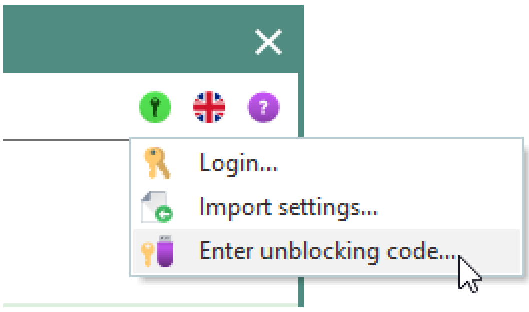


Figure 142. EgoSecure Agent: entering unblocking code

➥ The access block provided by **IntellAct Automation** is now cancelled and the previously defined access rights (full, read or write access) for the device are restored.
New code doesn’t replace the previous one.

11.3. Configuring IntellAct Automation for EgoSecure Server

With **IntellAct** you can create rules for certain events on the Server and define actions when an event occurs.

Defining rules for operations on the Server

1. Go to **Product settings | IntellAct Automation | Rules – Server**.
2. In the **IntellAct – Rules – Server** area, click **Add** and select a rule from the drop-down list.

   → A new entry appears in the list.
3. Under **Criteria**, define the settings for the rule. For details, see the table below.
4. Under **Actions**, select the way of notification. For details, see: IntellAct Automation events
5. Click **Save**.

Event	Criteria
Scheduled AD synchronization	Select the type of event you want to be notified of: ■ Errors only ■ Success only ■ Both results
Integrity control	Select the type of event you want to be notified of: ■ Errors only ■ Success only ■ Both results For details, see: Integrity control
SSL certificates control	Define the number of days before expiration when notification must appear.
EgoSecure Antivirus: signatured are outdated	Define the number of days since the last update after which signatures are considered outdated. The signatures are downloaded from the Internet to the Server and then updated on the Agent side.
License notifications	Define when to notify about expiring licenses and the limited percentage of unused licenses. Also set how often to remind about expired licenses and about reaching a maximum license quantity.
Database size control	Set when to notify about reaching database size and transaction log size limits.
Audit data size control	Determine when to inform you about the size of the audit data in the database. Specify what percentage of the maximum size can be reached. For details, see: Audit data size limit in the database

11.4. Configuring IntellAct Automation for users

In addition to the predefined rules for client and server, you can also create **IntellAct Automation** user rules. For this you create an event with certain parameters.

Before creating an event, define which values are used to calculate statistics.

Configuring statistics calculation parameters

1. Go to **Product settings | IntellAct Automation | Settings**.
2. Specify the time period (in days) to be used to calculate the average daily rate for custom operations.
3. Enter the minimum number of days that must be used to calculate the average daily rate.
4. Click **Save**.

INFO

Minimum number of days to calculate the average rate

If statistics are not available for enough days to reach the specified minimum number of days, events do not function, for which the option **Limit | Abnormality detection** is enabled in rule criteria. Corresponding rules do not apply.

- Ensure that there are enough statistics to calculate the average daily rate, or select the **Limit | Absolute value** option for the respective event.

The following custom events are available:

Event	Criteria	Controlled devices	Controlled access types	Additional configuration required
Storage: file access limit	A limit of reading and/or writing files	■ External storage (USB-sticks) ■ Mobile devices ■ CD/DVD disks ■ Floppy disk	■ Read ■ Write ■ Read/write	-
Network: file access limit	A limit of reading and/or writing files	■ Network shares ■ Thin client storage	■ Read ■ Write ■ Read/write	Enable the following options for a computer under *Computer management* | *Settings* | *Client settings*:

				■ Allow network shares control ■ Allow thin client storage control
Storage: unencrypted file transfer limit	A limit of transferring files without encryption	■ External storage (USB-sticks)	■ Write	■ Activate the **Removable Device Encryption** product for a user ■ Enable the Turn back to [encryption type from drop-down] encryption mode after x sec option
HTTP/HTTPS traffic limit	A limit of inbound and/or outbound traffic transferred via HTTP and HTTPS protocol	-	-	-
Cloud: file access limit	A limit of reading and/or writing files	■ Controlled cloud storage	■ -	■ Activate **Access Control** product for a user ■ Define controlled clouds under User management | Control | <user selection> | Cloud storage
Cloud: unencrypted file transfer limit	A limit of transferring files without encryption	■ Controlled cloud storage	■ Write	■ Activate **Access Control** product for a user ■ Define controlled clouds under User management | Control | <user

				selection> | Cloud storage ■ Activate **Cloud Storage Encryption** product for a user ■ Enable the Turn back to [encryption type from drop-down] encryption mode after x sec option
DLP DIU file access limit	A limit of the number of files, which match the criteria of DLP DIU filters assigned to a user	■ External storage (USB-sticks) ■ Network shares ■ Hard drives (if they are controlled like external storage)	■ Read ■ Write ■ Read/write	■ Activate **DLP – Data In Use** product for a user ■ Enable the **Allow network shares control** option for a computer (to control network shares) ■ Enable the **Control hard disks like external media** option to control hard disks if external storage is selected

Creating a custom event

1. Go to **Product settings | IntellAct | Events**.
2. In the **IntellAct Automation – Events** area, select an event from the drop-down list.

   → A new entry appears in the list.

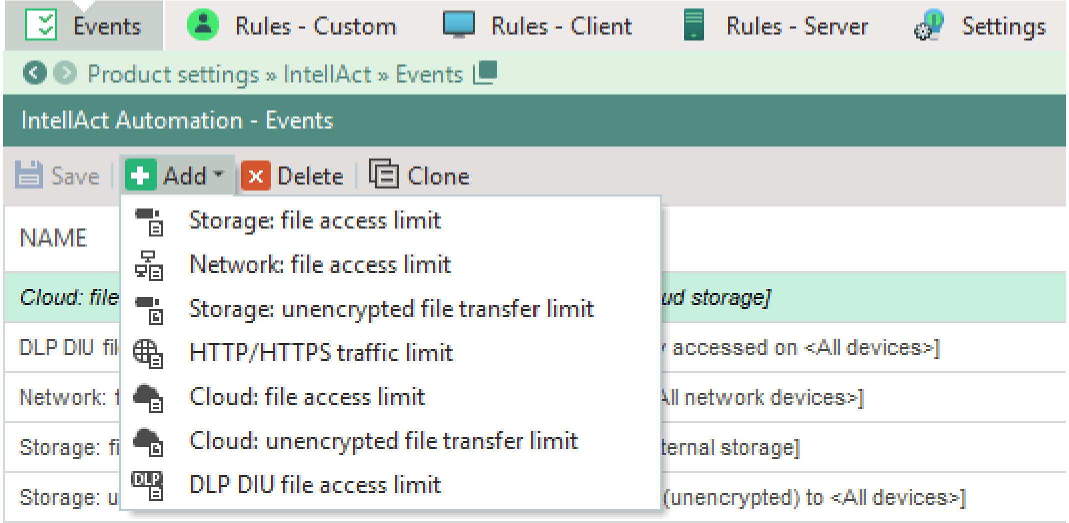
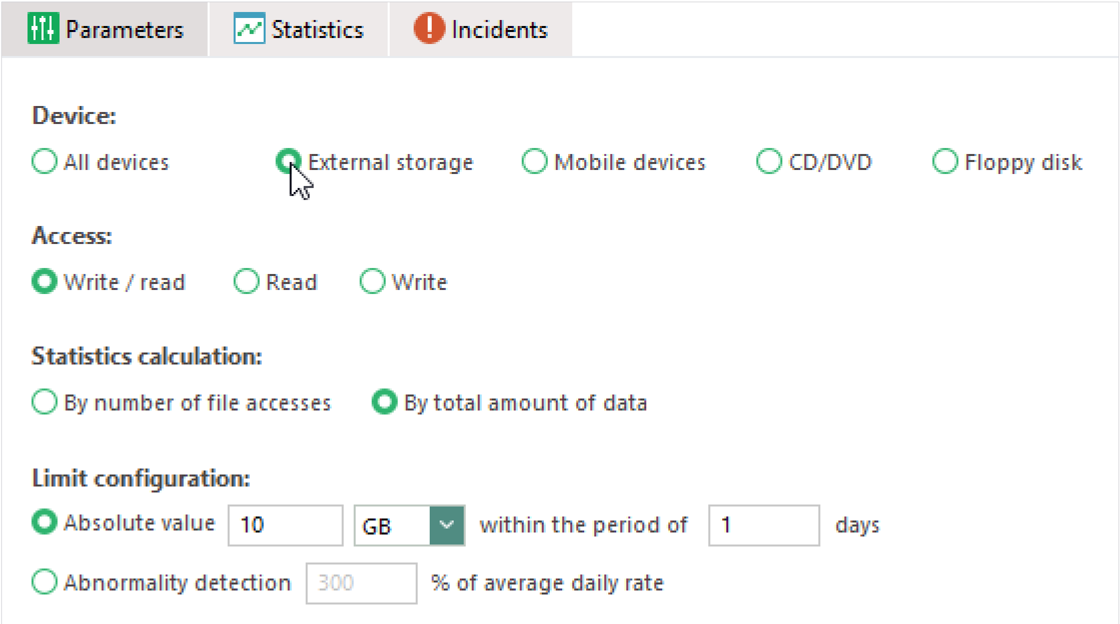

Events
Rules - Custom
Rules - Client
Rules - Server
Settings
Product settings » IntellAct » Events
IntellAct Automation - Events
Save
Add
Delete
Clone
NAME
Storage: file access limit
Network: file access limit
Storage: unencrypted file transfer limit
HTTP/HTTPS traffic limit
Cloud: file access limit
Cloud: unencrypted file transfer limit
DLP DIU file access limit
Cloud: file
ud storage]
DLP DIU fil
accessed on <All devices>]
Network: f
ll network devices>]
Storage: fi
ternal storage]
Storage: u
(unencrypted) to <All devices>]

Figure 143. Adding new IntellAct event

3. In the **Parameters** tab, select for which device class the event applies.



Device:
○ All devices ● External storage ○ Mobile devices ○ CD/DVD ○ Floppy disk

Access:
● Write / read ○ Read ○ Write

Statistics calculation:
○ By number of file accesses ● By total amount of data

Limit configuration:
● Absolute value 10 GB within the period of 1 days
○ Abnormality detection 300 % of average daily rate

Figure 144. Assigning device class to event

4. Under **Access**, select whether the event must only be used for read or write access or for both.
5. Under **Limit**, define the settings for the event. For details, see the table below:

Setting	Description
Statistics calculation	Define whether the number or the total size of the files that must be used for statistics calculation. This setting is not available for the HTTP/HTTPS traffic limit event.
Limit	Define the amount of data transfer to which the file transfer or HTTP traffic should be limited. To limit, specify an absolute value for a

	defined period of time or specify the percentage by which the daily amount of data may differ from the average daily rate.

6. Click **Save**.

Creating custom rules

1. Go to **Product settings | IntellAct | Rules - Custom**.
2. In the **IntellAct Automation – Rules – Custom** area, click **Add** and select an event to which to apply the rule.

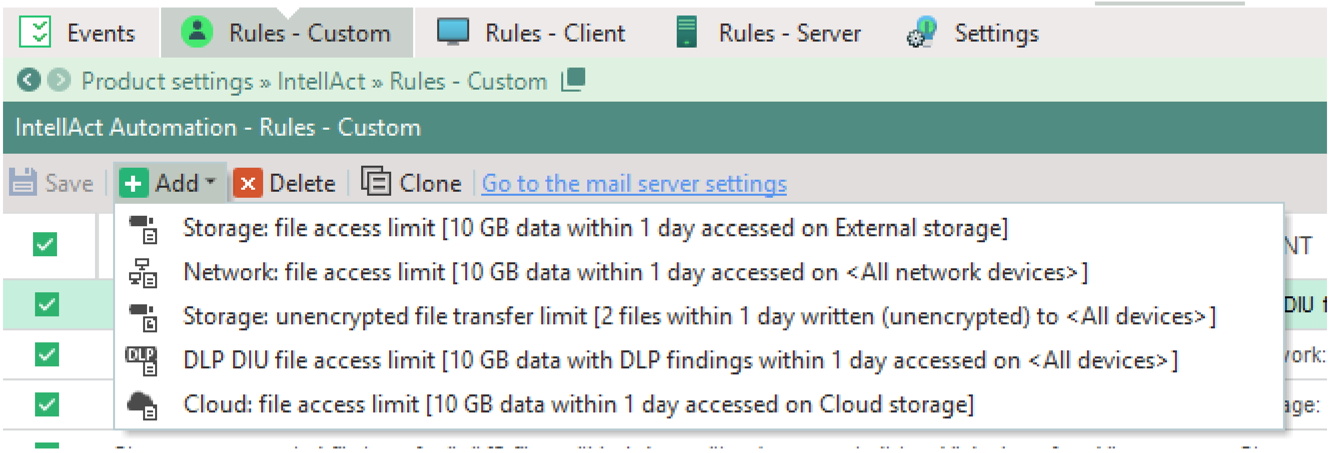
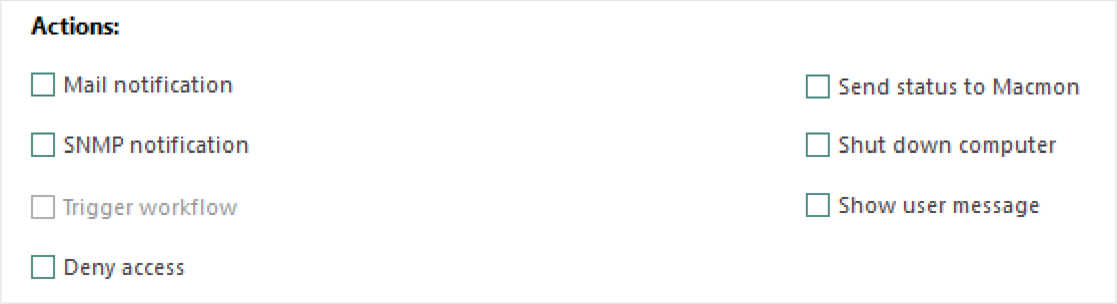

Events
Rules - Custom
Rules - Client
Rules - Server
Settings
Product settings » IntellAct » Rules - Custom
IntellAct Automation - Rules - Custom
Save
Add
Delete
Clone
Go to the mail server settings
Storage: file access limit [10 GB data within 1 day accessed on External storage]
Network: file access limit [10 GB data within 1 day accessed on <All network devices>]
Storage: unencrypted file transfer limit [2 files within 1 day written (unencrypted) to <All devices>]
DLP DIU file access limit [10 GB data with DLP findings within 1 day accessed on <All devices>]
Cloud: file access limit [10 GB data within 1 day accessed on Cloud storage]
NT
DIU
vork:
age:

Figure 145. Adding a custom IntellAct rule

→ A new entry appears in the list.

3. To assign the rule to specific users, choose the objects under **Selection of users**. If no object is selected, the rule applies to all users. For details, see: Assigning IntellAct rules
4. Under **Actions**, specify which actions to perform when an event occurs. For details, see: Actions for IntellAct events



Actions:

□ Mail notification
□ SNMP notification
□ Trigger workflow
□ Deny access
□ Send status to Macmon
□ Shut down computer
□ Show user message

Figure 146. IntellAct actions for user

5. Click **Save**.

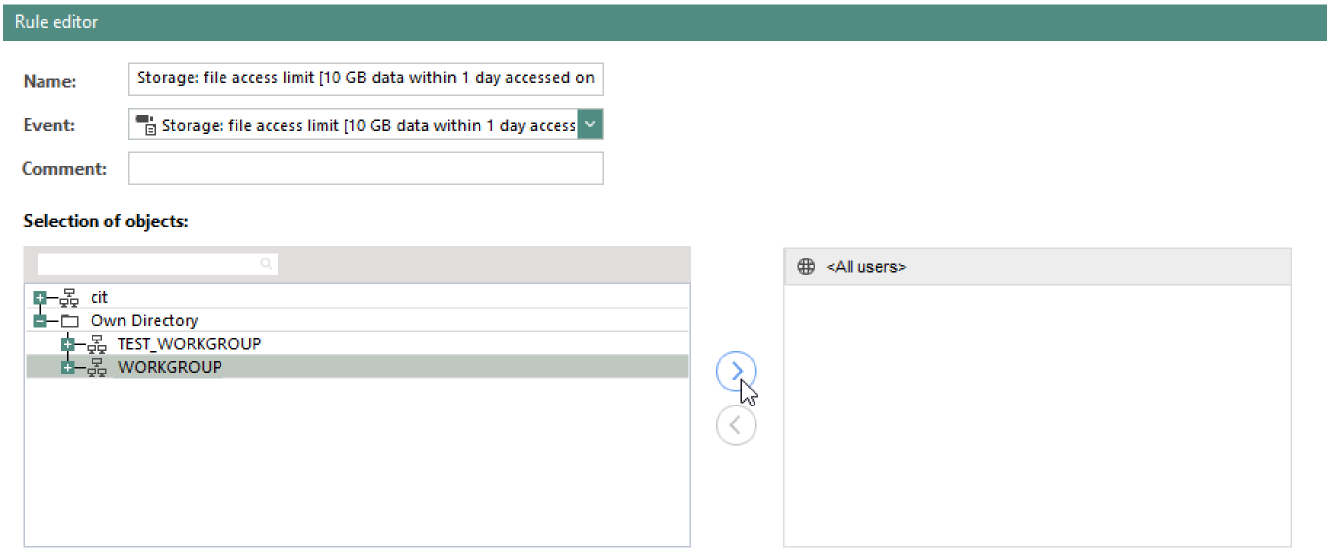
11.5. Assigning IntellAct rules

Depending on the event, client and custom rules can be assigned to certain users or computers. Once a rule is assigned to selected objects, it only applies to the events of

these users or on these computers of the directory. By default, no events are assigned; in this case, rules apply to all users or computers of the directory.
Custom rules as well as client rules for the events **Access denied (Access Control)**, **Access denied (Application Control)** and **Access rights requests** are assigned to users. Other client rules are assigned to computers.

Assigning IntellAct rule for user

1. Go to **Product settings | IntellAct | Rules – Custom** or **Rules – Client**.
2. Select the rule from the list.
3. Under **Selection of objects**, double-click the directory objects on the left or select the object and click the right arrow.



Rule editor

Name: Storage: file access limit [10 GB data within 1 day accessed on

Event: Storage: file access limit [10 GB data within 1 day access

Comment:

Selection of objects:

- cit
- Own Directory
  - TEST_WORKGROUP
  - WORKGROUP

<All users>

Figure 147. Selecting users to assign the IntellAct rule

→ The selected directory objects appear in the area on the right.

4. Click **Save** on the toolbar.

Assigning IntellAct rule to computer

1. Go to **Product settings | IntellAct | Rules – Client**.
2. Select the rule from the list.
3. In the **Rule editor** area, double-click the directory objects under **Selection of users**:

   → The selected objects appear in the area on the right.

4. Click **Save** on the toolbar.

11.6. Setting up IntellAct Automation to trigger Matrix42 Workspace Management workflows

The integration of two systems - the **Matrix42 Workspace Management** system and the **EgoSecure Server** - allows to extend the administration options in your company. Via the central management tool of the EgoSecure Server - the EgoSecure Data Protection Console - you can create IntellAct tasks and then select the Trigger workflow option as an action to trigger the previously defined workflow in the **Service Desk**, once the conditions of an IntellAct client rule are met.

INFO

Workflows are triggered only for client rules

In the current **EgoSecure Data Protection** version, the option for triggering workflows is available only for the predefined client rules. For future versions, the integration of this check box is planned for custom rules.

Connecting the EgoSecure Server and the Matrix42 Server

1. In the Matrix42 Workspace Management, navigate to **Administration | Integration | Web Services Tokens** and then click **Generate Api Token**.

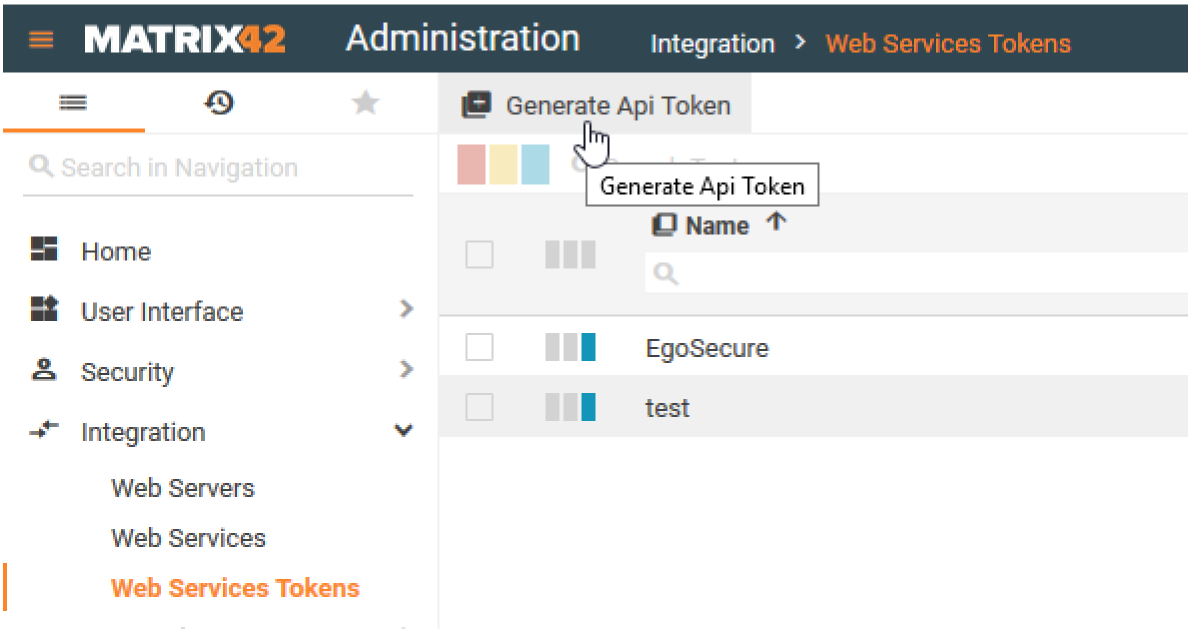
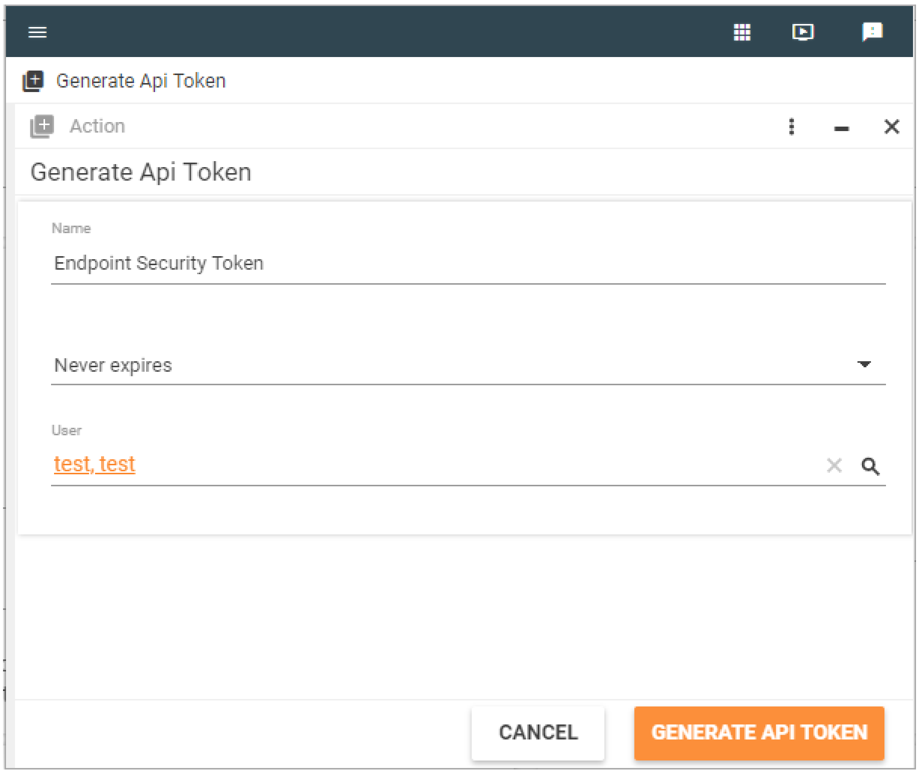


Figure 148. Creating token for connecting EgoSecure and Matrix42

2. In the **Name** field, define the token name.
3. In the **Expires on** drop-down menu, select **Never**.
4. In the **User** field, specify a user for whom this token is assigned. With the help of this key the specified user can perform only the actions permitted within his rights in the system.
5. Click **Generate API token**.



Generate Api Token

Name
Endpoint Security Token

Never expires

User
test, test

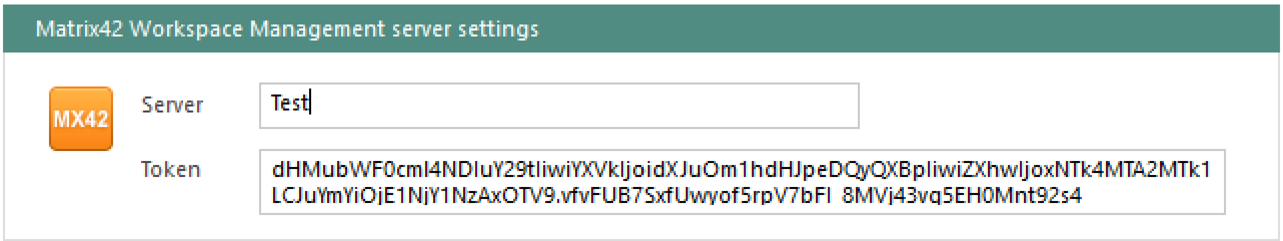
Figure 149. Editing parameters for the API token

6. Copy the **Api Token** value.

! Copy the Api Token value now, as it will not be available later.

Adding token to the Console

1. Open the EgoSecure Data Protection Console and navigate to **Administration | Servers | Mail, proxy and others**.
2. Scroll down to the Matrix42 Workspace Management server settings area.
3. In the **Server** field, define the web address of the **Matrix42 Workspace Management server**.
4. In the **Token** field, enter or paste the **Api Token** value, created in the steps before.



Matrix42 Workspace Management server settings

Server Test

Token dHMubWF0cml4NDIuY29tliwiYXVkljoidXJuOm1hdHJpeDQyQXBpliwiZXhwljoxNTk4MTA2MTk1LCJuYmYiOjE1NjY1NzAxOTV9.vfvFUB7SxfUwyof5rpV7bFI 8MVj43vq5EH0Mnt92s4

Figure 150. Connecting Matrix42 server with the EgoSecure Console

5. Click **Save**.

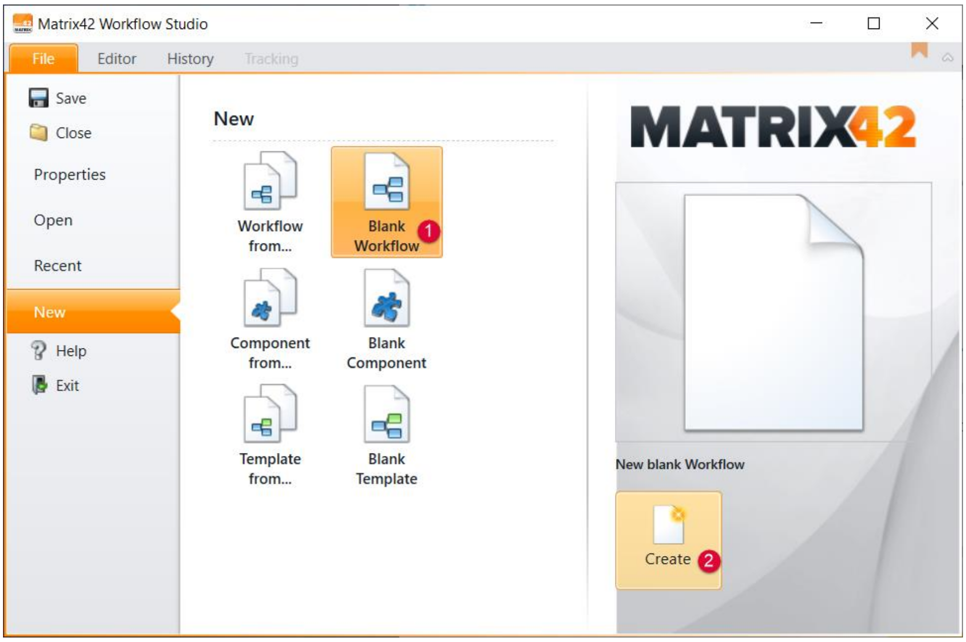
Creating and editing workflows for EgoSecure

In the current section you can find details about how to create a simple workflow that is used to get data from the **EgoSecure Server** and to create a task in the **Service**

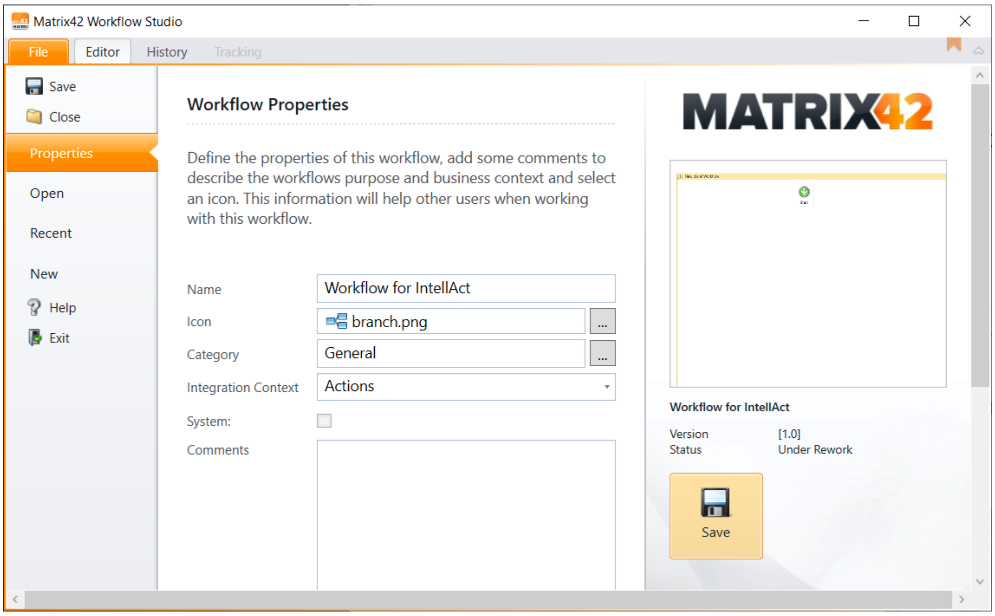
Management. You can create this simple workflow manually using the description below or you can skip this part and use the workflow with preconfigured arguments. To use the workflow with preconfigured arguments, all you need to do is to download the Service Management Security Connector from Matrix42 Marketplace (registration required) and install it on the computer with Matrix42 Workspace Management server.

For the advanced usage of workflows, see Matrix42 help files - workflows.

1. In the **Matrix42 Workflow Studio**, create a blank workflow. One workflow is created for one IntellAct event.



2. Define the workflow properties and click **Save**.



Define the properties of this workflow, add some comments to describe the workflows purpose and business context and select an icon. This information will help other users when working with this workflow.

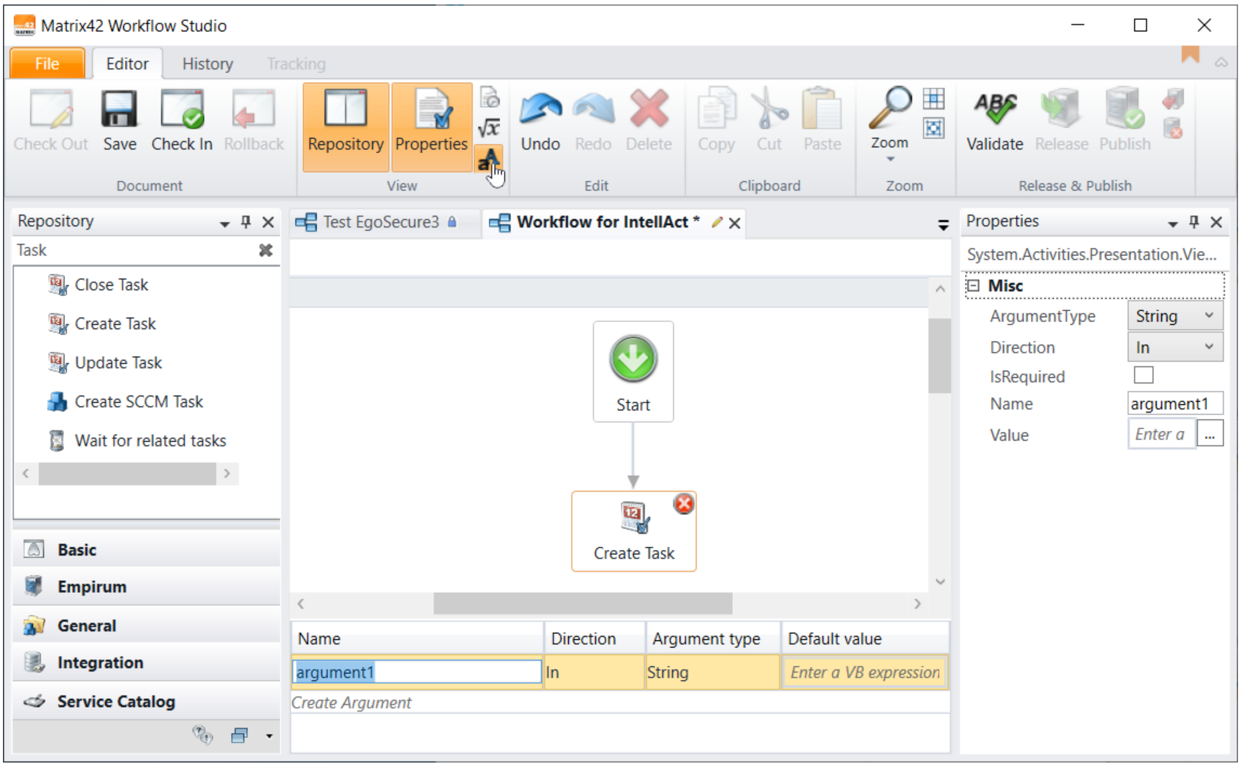
Name: Workflow for IntellAct
Icon: branch.png
Category: General
Integration Context: Actions
System: □
Comments:

Workflow for IntellAct
Version [1.0]
Status Under Rework

Figure 151. Creating workflow in Matrix42 Workflow Studio

3. Under **Repository**, search for **Create task** and drag it after **Start**
4. In the **View** menu, click aA.

   → The field for editing arguments appears on the bottom.



Name	Direction	Argument type	Default value
argument1	In	String	*Enter a VB expression*
Create Argument			

ArgumentType	String
Direction	In
IsRequired	□
Name	argument1
Value	*Enter a* ...

Figure 152. Adding arguments to Matrix42 workflow

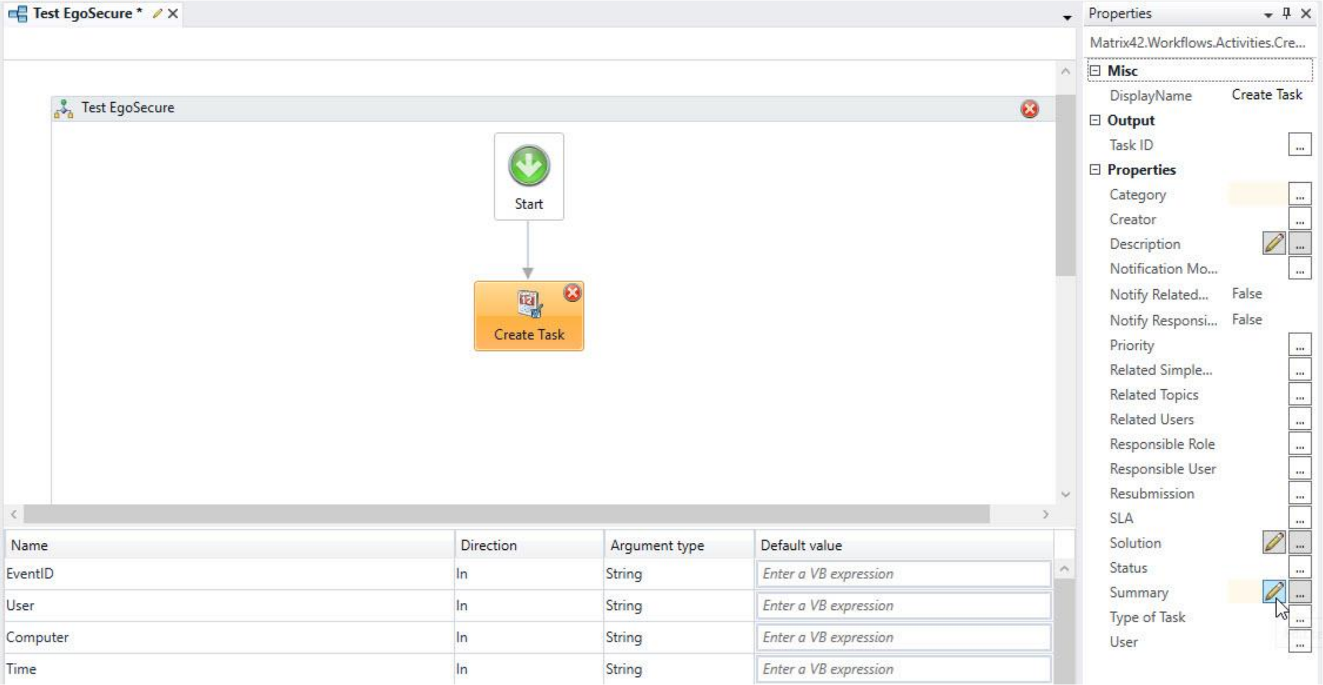
5. Add all arguments for an IntellAct event manually. One argument is per one string. For details, see the list of arguments for each event below in the table:

Event	Arguments	
Access rights requests	EventID User User SID Computer Computer GUID	EventDate Time RequestedRights Comments Server
Access denied (Access Control)	EventID DeviceClass DeviceName DeviceID User User SID Computer Computer GUID	EventDate Time Path Process Access Reason Server
EgoSecure Antivirus: Threat found	Computer Computer GUID EventDate	Reason Type Status

	Time EventID	Server
EgoSecure Antivirus: State changed	Computer Computer GUID EventDate Time	EventID Status Server
Access denied (Application Control)	EventID Application User User SID Computer	Computer GUID EventDate Time Reason Server
Green IT: Suspicious activity	EventID Computer Computer GUID EventDate	Time Event Server
EgoSecure Antivirus: Signatures are outdated	EventID Message Computer	Computer GUID Server

6. Add arguments to display them in a certain field of an incident, once an administrator receives it:

   a. Select the field and click on ✎.



DisplayName: Create Task

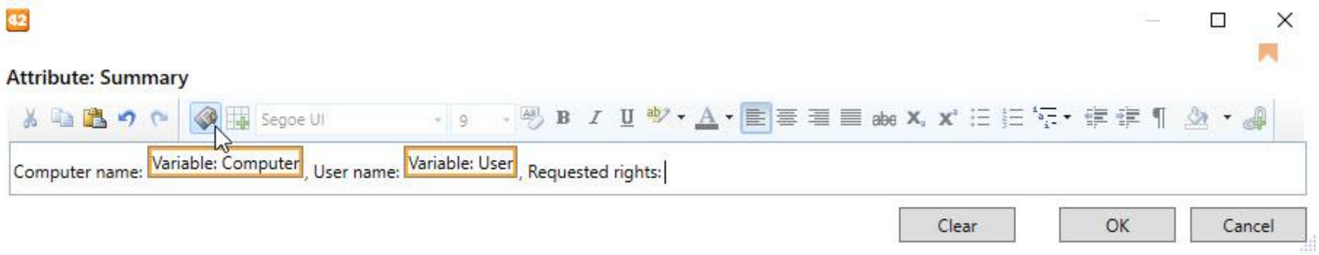
Notify Related...: False

Notify Responsi...: False

Name	Direction	Argument type	Default value
EventID	In	String	Enter a VB expression
User	In	String	Enter a VB expression
Computer	In	String	Enter a VB expression
Time	In	String	Enter a VB expression

→ The dialog for editing appears.

   b. Enter the text, which describes the argument and then click .



Attribute: Summary

Computer name: Variable: Computer, User name: Variable: User, Requested rights:

→ The **Select Variable** dialog appears.

c. Select the argument and click **OK** to close the dialog.

→ The argument appears after a user-defined text in an orange box.

d. Click **OK** to close the dialog and save the changes.

7. Publish the workflow:
   a. In the **Release & Publish** area, click **Validate**.
   b. In the **Document** area, click **Check In**.
   c. In the **Release & Publish** area, click **Release** and then **Publish**.

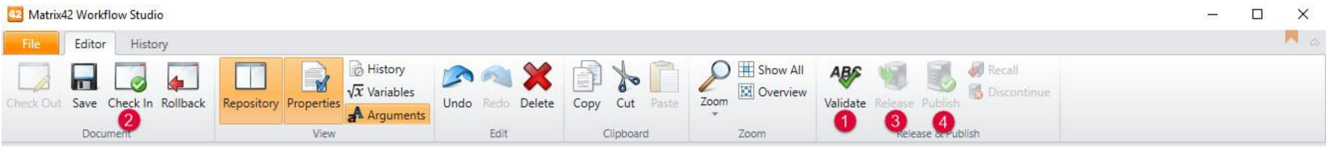
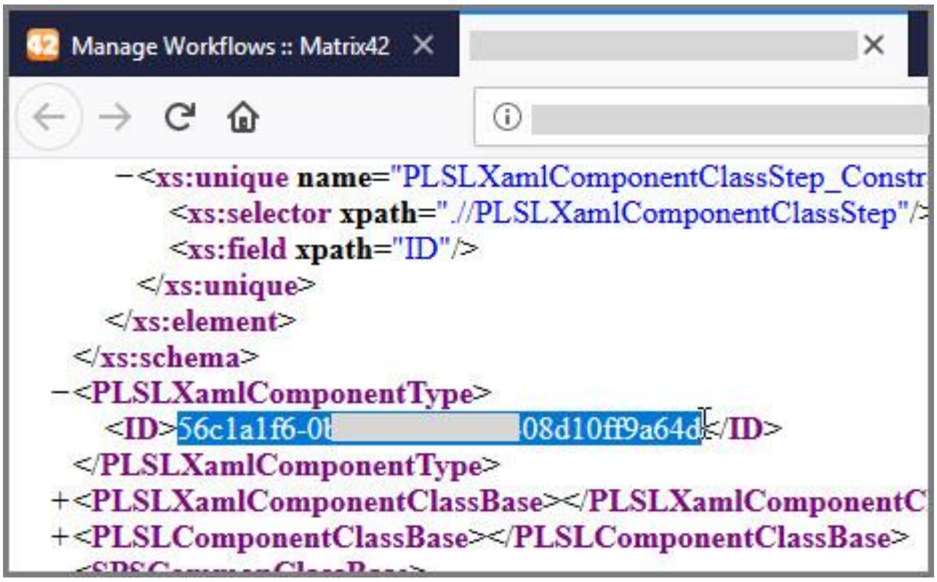


Figure 153. Publishing workflow

8. As soon as workflows for all IntellAct events are created, get the workflow ID:
   a. Navigate to **Administration | Services & Processes | Workflows | Manage Workflows**.
   b. Select a registered workflow from the list. For details about creating and managing workflows, see: Matrix42 Help - Workflows
   c. Click Export, select the **XML** radio button and then click **Export**.

   → The XML file opens in a new tab.

   d. To find the right place in the workflow XML, search for the tag `<PLSLXamlComponentType>` and copy the workflow ID below.

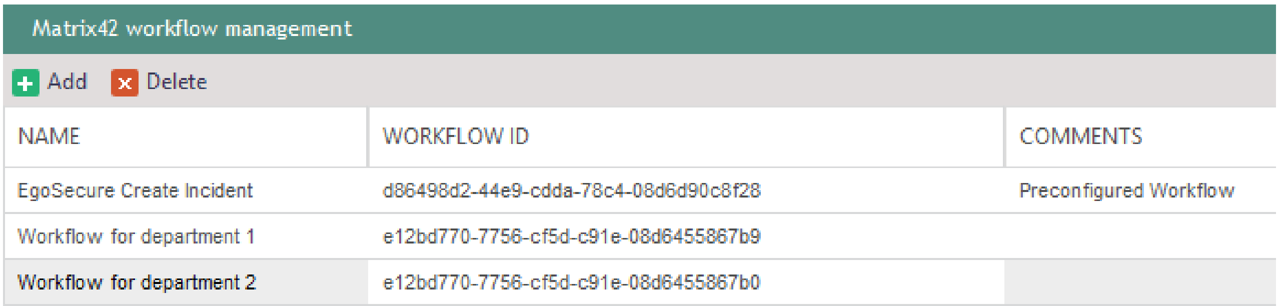


```
  −<xs:unique name="PLSLXamlComponentClassStep_Constr
     <xs:selector xpath=".//PLSLXamlComponentClassStep"/>
     <xs:field xpath="ID"/>
   </xs:unique>
  </xs:element>
</xs:schema>
−<PLSLXamlComponentType>
   <ID>56c1a1f6-0b[redacted]08d10ff9a64d</ID>
 </PLSLXamlComponentType>
+<PLSLXamlComponentClassBase></PLSLXamlComponentC
+<PLSLComponentClassBase></PLSLComponentClassBase>
```

Figure 154. Exported XML workflow

Setting up IntellAct rules for triggering workflows

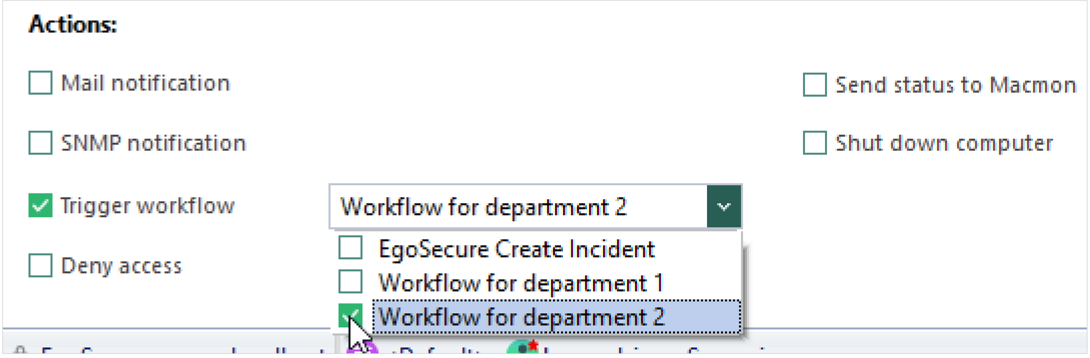
1. Skip this step and proceed with step 2 if you have installed the **Service Management Security Connector** instead of configuring a workflow manually.
   If you have configured a workflow manually, then in the EgoSecure Data Protection Console, create a workflow under **Product settings | IntellAct | Settings**:
   a. In the **Matrix42 workflow management** area, click **Add**.
   b. Define the workflow name in the **Name** column.
   c. Paste the ID you copied in the previous steps.
   d. Click **Save**.



NAME	WORKFLOW ID	COMMENTS
EgoSecure Create Incident	d86498d2-44e9-cdda-78c4-08d6d90c8f28	Preconfigured Workflow
Workflow for department 1	e12bd770-7756-cf5d-c91e-08d6455867b9	
Workflow for department 2	e12bd770-7756-cf5d-c91e-08d6455867b0	

Figure 155. Entering workflow ID in EgoSecure Console

2. Create an IntellAct rule under **Product settings | IntellAct | Rules - Client**. For details about creating IntellAct rules, see: Configuring IntellAct for computers
3. Under **Actions**, enable the **Trigger workflow** check box.
   The **Trigger workflow** check box is currently available only for **Rules – Client**. In next releases, we plan to integrate this check box for the **Rules - Custom** area.



Actions:

- □ Mail notification
- □ SNMP notification
- ☑ Trigger workflow: Workflow for department 2
  - □ EgoSecure Create Incident
  - □ Workflow for department 1
  - ☑ Workflow for department 2
- □ Deny access
- □ Send status to Macmon
- □ Shut down computer

4. Select the workflows from the list:
    a. Select any of the workflows if you configured them manually.
    b. **EgoSecure Create Incident** if instead of the manual workflow setup you installed the Service Management Security Connector.
5. Click **Save**.

Once the conditions are met, the **EgoSecure Server** sends all information to the **Matrix42 server** and the task is created in the **Service Desk**.

12. INVENTORY

Inventory gives an overview of the components of a computer such as computer physical memory, processors, disk drives, video cards, installed applications, files executed, *etc*.

Showing Inventory information

1. To get information about a certain component, go to **Reports | Inventory** and select the menu:
    - Logical disks
    - Disk drives
    - Physical memory
    - Processors
    - Video cards
    - Applications
    - Executable files (*.exe)
2. To show only devices or drives that are currently connected, enable the **Hide deleted checkbox** (not available for **Applications** and **Executable files** reports).
3. To group the list of the respective components according to certain attributes, select the attribute in the **Group by** selection menu.
4. To search for a specific term on the list, enter the search pattern in the **Filter** field.

13. GREENT IT

With **Green IT**, configure the energy options on end devices so that the energy is used only when it is really needed.
Green IT is activated only for computers.

Specifying settings to save costs

1. Go to **Product settings | Green IT | Settings**.
2. Enter the average power consumption for PCs and monitors and enter a price per kWh.
3. Click **OK** to confirm.

Defining Green IT access permissions for a user

1. Select a user in **User management**.
2. Go to **User management | Green IT | Settings** tab.
3. Specify whether a user is permitted to:

- **Turn off Green IT**.
- **Change Green IT parameters** (a user is permitted to change Green IT calculation settings and power profile settings, edit his own exclusions and scheduled tasks, enable and disable settings in the Settings tab of the Agent).
  A user is not allowed to edit administrator exclusions and scheduled tasks 🌐 no matter whether the Change Green IT parameters option is enabled or disabled.

4. Click **Save**.

13.1. Creating a power profile

Via power profiles, configure the advanced power settings for computers. **Green IT** actions (hibernation, standby or shutdown) are performed only if all the conditions defined in configuration profile settings are met. If no settings are defined, the default ones apply. For battery-operated devices, you can specify different settings for network operation (AC) and for battery operation (DC).

INFO

Power profile settings with predefined exceptions

If a program defined as an exception is started, energy profile settings do not apply. For details, see: Exceptions

Creating new energy profile

1. Under **Product settings | Green IT | Power profiles**, click **Add** on the toolbar.
   → A new entry appears.

2. In the **Name** column, enter the name of a profile.
3. In the **Power profile – <profile name>** area, specify the settings for device operation. For details about the settings, see the table below.
4. Click **Save**.

You can now assign the profile to computer.

Processor group

Option group	Option	Description
Idle settings	**Idle sensitivity**	Percentage of processor loading. If the current percentage is lower than the defined number, it is considered as idle.
	Mouse and Keyboard sensitive	If checked, mouse and keyboard clicks are taken into account. If unchecked, Green IT action is performed if all other conditions are met, despite the fact that keyboard or mouse are in use.
	Idle timeout	When time is over, “Idle action” performing is initiated.
	Idle action	Defining what must be performed when computer is idle.
Throttle settings	**Throttle policy**	Allows Windows to slow down processor speed to reduce power consumption. ■ **Adaptive** (lowers the performance of the processor to the lowest voltage available whenever there is insufficient demand to justify a higher voltage; engages processor clock throttling if the C3 state is not being utilized, and in response to thermal events). ■ **Constant** (does not allow the processor to use any high voltage performance states; will not engage processor clock throttling, except in response to thermal events). ■ **Degrade** (does not allow the processor to use any high voltage performance states; engages processor clock throttling when the battery is below a certain threshold, if the C3 state is not being utilized, or in response to thermal events). ■ **None** (no processor performance control is applied; the processor runs at its highest possible performance level; this policy will not engage processor clock throttling, except in response to thermal events).

	Forced throttle	Level of slowing the processor speed down (in percent).
Fan settings	**Fan throttle tolerance**	Low limit of processor speed when fan turn on.

Monitor group

Option	Description
Display timeout	Set how long computer is inactive before the display turns off.

Disk group

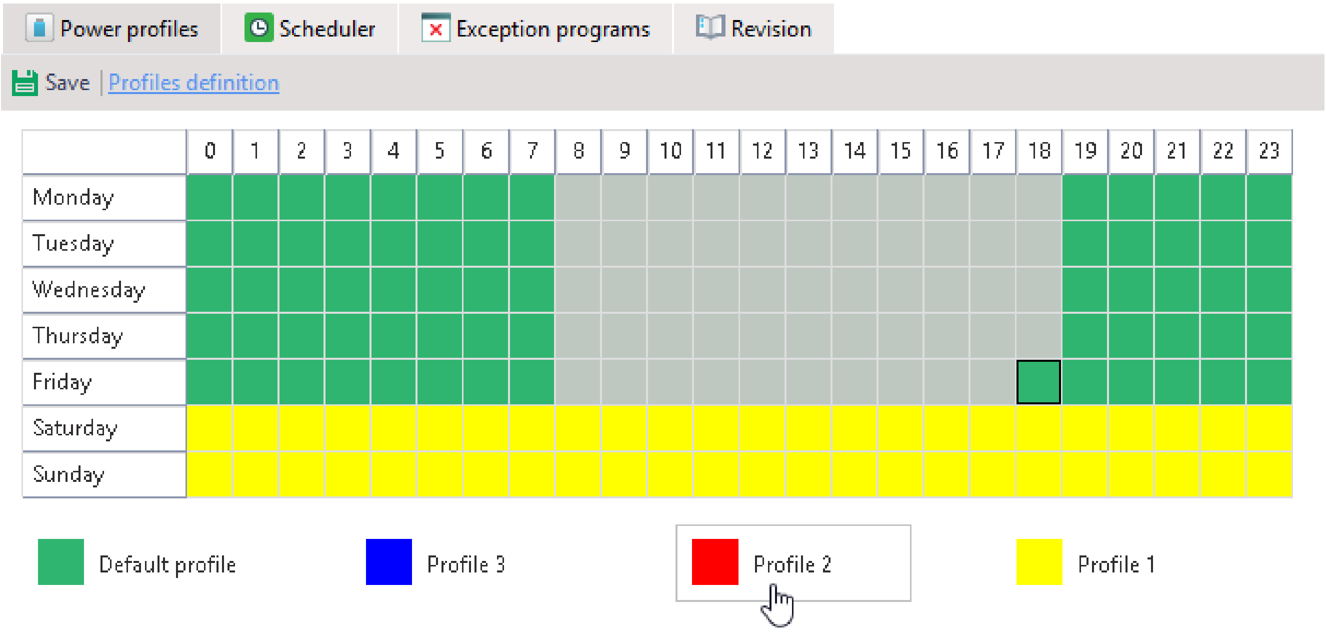
Option	Description
Spindown timeout	How long the hard drive is inactive before the disk turns off.

Devices group

Option group	Option	Description
Enable Autoplay	**- CD/DVD** **- USB**	Fast way to enable or disable autoplay dialog that appears on each device connection. Computer must be restarted for the setting to take effect.
Allow the computer to turn off devices	**Network adapters**	Check the box to allow the computer to turn off network adapters and USB Root Hub to save power consumption. It reduces the number of wakes, allowing computers to sleep for longer periods of time when idle.
	USB Root Hub	
Allow devices to bring the computer out of standby	**Network adapters**	If this setting is allowed, power consumption is higher.

Assigning a power profile

1. Select a computer in **Computer management**.
2. In the **Green IT | Power profiles** tab, drag with the mouse over the times of the day for which the profile works.



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Monday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩
Tuesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩
Thursday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩
Friday	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	⬜	🟩	🟩	🟩	🟩	🟩	🟩
Saturday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Sunday	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨

🟩 Default profile 🟦 Profile 3 🟥 Profile 2 🟨 Profile 1

Figure 156. Assigning power profile for specific days

3. Select a profile below the schedule.

   → The selected times of the day receive the color of the assigned profile.

Click **Save**.

13.2. Exceptions for power profile

Exception programs influence only the work of the power profiles. If one of the exception programs is running, computer doesn’t perform idle action. Exception programs do NOT prevent the performing of scheduled tasks.

Creating exceptions

1. Under **Product settings | Green IT | Exception programs**, click **Add**.

   → A new entry appears.

2. Edit the exception in the **Green IT settings** area:

   a. Select a launched application or a running process and then click on › or search for an application manually.

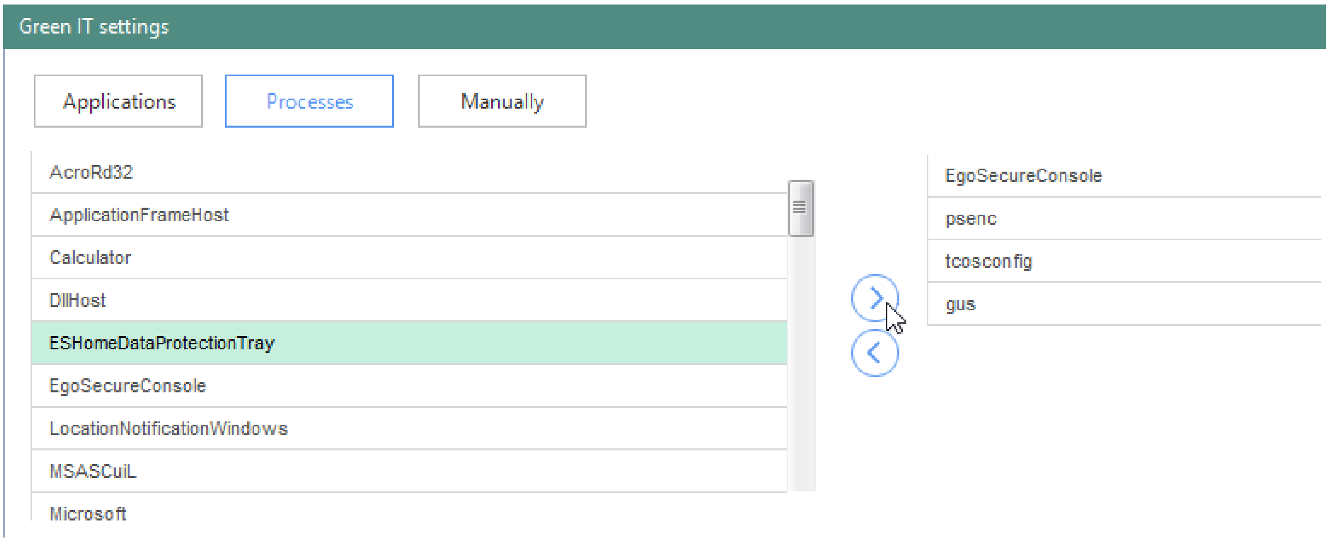


Figure 157. Creating Green IT exceptions

   b. Enable the **Network utilization** check box to take network activity into account.
   c. Specify how much % of **CPU** a program must use to be considered as an active one.
3. Click **Save**.

13.3. Scheduler

Via the **Scheduler** you can plan **Green IT** tasks and execute them automatically.

In the **Settings** tab, define which tasks must be performed before executing the scheduled task. For details, see: Green IT - Settings

Creating planned task for Green IT

1. Under Product settings **| Green IT | Scheduler**, click **Add**.

   → A new entry appears.

2. In the **Name** column, specify a name for the task.
3. Enable the check box in the **Global** column to assign the task to all users with an activated **Green IT** license.
4. In the **Green IT settings** area:
   a. In the **Action** drop-down, select an action, which must be performed.
   For details about the difference between hibernation and sleep, see: Microsoft help

! To assign the Wake-on-LAN action, make sure that the network card supports Wake-on-LAN and that the appropriate configuration is enabled in BIOS.

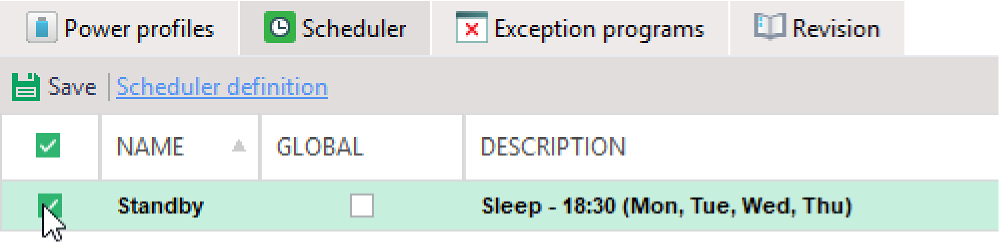
   b. Select when to perform the action (once or regularly).
5. Click **Save**.

6. To automatically save opened documents before executing a task and show a message to the user about the upcoming action, enable the respective option under **Product settings | Green IT | Settings**. For details, see: Setting up shutdown settings

You can now assign the scheduled tasks to computers.

Assigning task to computer

1. Select a computer under **Computer management**.
2. Enable a task in the **Green IT | Scheduler** tab.



☑	NAME	GLOBAL	DESCRIPTION
☑	Standby	□	Sleep - 18:30 (Mon, Tue, Wed, Thu)

Figure 158. Assigning Green IT task to computer

3. Click **Save**.

Green IT performs the action on the computer at the scheduled time.

13.4. Specifying shutdown settings

You can use the Green IT settings to define certain actions that must be carried out before a scheduled task is performed automatically. With the help of these options the user can save the work in time.

Adjusting settings for performing scheduled task

1. Go to **Product settings | Green IT | Settings**.
2. In the **Shutdown settings** area, enable the settings. For details, see the table:

Option	Description
Receive a message before performing a scheduled task	Enable the checkbox to display a message before the action is performed to postpone the action. In the **Timeout** field, enter in how many minutes before the task execution the message appears.
Automatic saving of documents	Documents opened in Microsoft Office (Excel, Word, Power Point, Access) are automatically saved before performing Green IT scheduled tasks. If the document hasn't been saved before, it is saved to the **My documents** folder of a user.

Use Windows Power Settings after Green IT is disabled	If the option is enabled: Green IT is disabled. Windows Power Management and its polices are permitted and take effect. If disabled: Green IT is enabled and Windows Power Management disabled.

13.5. Using Green IT in demo mode

Activate the Green IT demo mode to see the potential profit from using the **Green IT** product. In demo mode, statistic data are collected, but Green IT functionality does NOT work (shutdown and start, hibernate mode, sleeping mode etc.).

INFO	**Using Green IT demo mode** The functionality of the demo mode requires an active product license for **Insight Analysis.**

Using demo mode

1. Go to **Product settings | Green IT | Settings**.
2. In the **Demo mode** area, enable the check box.
3. Click **Save**.
4. To see the potential profit from using the licensed **Green IT** version, navigate to **Insight Analysis | Green IT | Your profit**.

14. SECURE ERASE

With **Secure Erase**, files, folders and partitions are deleted without recovery due to the methods of file overwriting.
Secure Erase is activated only for a user.

14.1. Securely delete files manually

With **Secure Erase** enabled for a user, you can add the **Secure Erase** option to the user's Windows context menu so that the user can erase files on demand with **Secure Erase.** You can also define which methods for file overwriting are available to the user.

Permitting a user to delete files securely via Windows context menu

1. Select a user in **User management**.
2. Under Secure Erase | Settings, enable Add Secure Erase to context menu.
3. Click **Save**.

Enabling Secure Erase methods for user

1. Select a user in **User management**.
2. Under **Secure Erase | Settings** tab, enable the check boxes with overwriting methods available for the user.
3. Click **Save**.

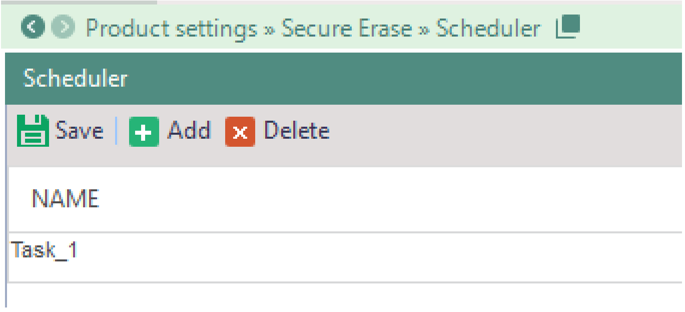
14.2. Planning scheduler tasks

Via the **Scheduler** you can plan and execute **Secure Erase** tasks. You can both delete predefined directories as well as the recycle bin or regularly empty the folder with temporary files. You can also safely erase empty sectors of the hard disk and free up unused hard disk space.

Planning a secure delete of files and folders

1. Go to **Product settings | Secure Erase | Scheduler**.
2. In the **Scheduler** area, click **Add**.

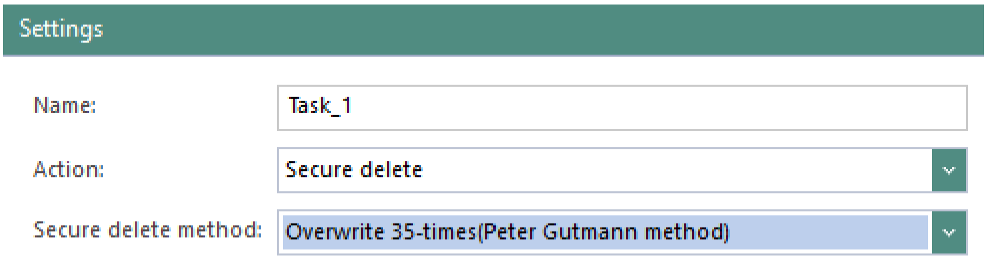
   → A new entry appears in the list.



NAME
Task_1

Figure 159. Creating new task in the scheduler

3. In the **Name** column, enter a task name.
4. Enable the check box in the **Global** column to assign the task to all users.
5. In the **Settings** area, select **Secure delete** from the **Action** drop-down.
6. In the **Secure delete method** drop-down, select a method of file overwriting.



Settings

Name: Task_1

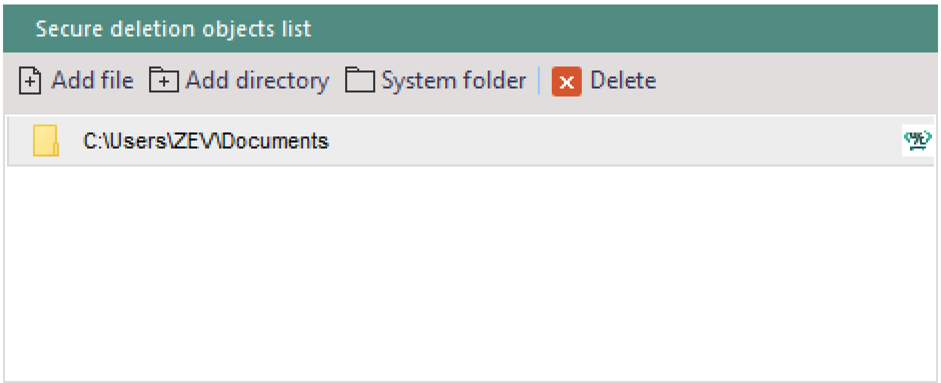
Action: Secure delete

Secure delete method: Overwrite 35-times(Peter Gutmann method)

Figure 160. Selecting a method for secure deletion

7. To select objects for deletion, click **Add file...**, **Add folder...** or **System folder...** button.

   → A dialog folder appears.

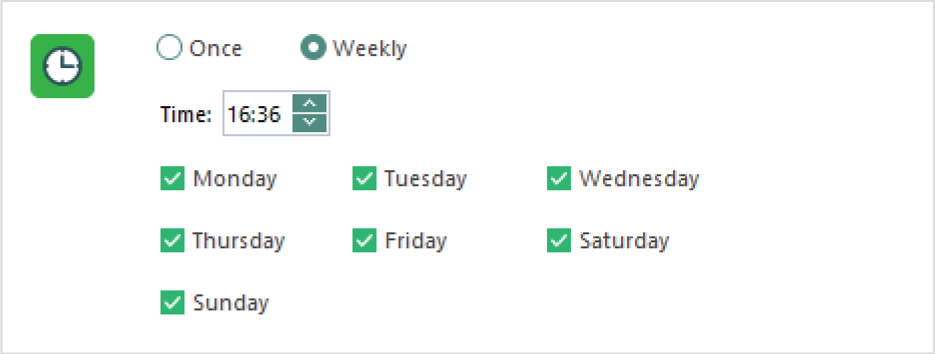


Secure deletion objects list

C:\Users\ZEV\Documents

Figure 161. Selecting objects for secure erase

8. Select objects and click **OK** or **Open** to confirm the selection.
9. Set the **Empty Recycle Bin securely** box to delete the contents of the Recycle Bin.
10. Select **Delete temporary directories securely** to clear the contents of the Windows temporary directories.
11. Select the task frequency (once or weekly).



○ Once ● Weekly

Time: 16:36

☑ Monday ☑ Tuesday ☑ Wednesday

☑ Thursday ☑ Friday ☑ Saturday

☑ Sunday

Figure 162. Planning frequency of scheduled task

12.Click **Save**.

Planning a secure delete of empty sectors

1. Go to **Product settings | Secure Erase | Scheduler**.
2. In the **Scheduler** area, click **Add**.

   → A new entry appears in the list.
3. In the **Name** column, define a task name.
4. In the **Settings** area, select **Empty sectors secure delete** from the **Action** drop-down.
5. Select the hard drives, where to delete empty areas. Only the free space is cleaned up.
6. Select the task frequency (once or weekly).
7. Click **Save**.

Assigning a planned task to a user

1. Under **User management**, select a user.
2. Under **Secure Erase | Scheduler**, enable the task.
3. Click **Save**.

15. REPORTS

The **Reports** menu gives you an overview of various statistics on computers and users in your directory as well as on the individual components of **EgoSecure Data Protection**. Depending on the menu item, various options are available.

15.1. Overview of reports

The following tables give you an overview of statistics available in the **Reports** menu and the information they contain.

Tenants

Report	Available information
Secure Audit data usage	Summary table with the database information for each tenant. Click the tenant row to see details about the size of certain Secure Audit types in the database for the selected tenant.
License usage	Summary table of all activated licenses per each tenant. Mouse over the column name to see the full name of a product license. In the **Show license** drop-down, select: ■ **Total** to see the total number of licenses activated for computers and users. ■ **Users** to see the number of licenses activated only for users. ■ **Computers** to see the number of licenses activated only for computers. ■ **Users + computers** to see the number of licenses activated for users and the numbers of licenses activated for computers.

See also: Managing tenants

General

Report	Available information
Management overview	Statistics to the following points: ■ Active users: the number of users with active products (green), and users with inactive products (grey). ■ Active computers: the number of computers with active products (blue), and computers with inactive products (grey).
Agents state	In the **Computers** area the number of computers where the EgoSecure Agent is installed and started, not started/not installed or offline (installed but cannot connect to the Server) is displayed. In the **Loaded agents** area, the state of Agent components is shown: status OK, driver not loaded or tray not started.
Synchronization log	Overview of successful and failed synchronization attempts. You will also receive information about the number of objects read or the reason for the synchronization failure (e.g. due to an error code).

Revision	Overview of **Console** operations, type of administrator who performed an operation, and an operation result.
Active/inactive products	Overview of users, computers or groups where selected products are activated or not activated. If at least one of the selected products is activated/not activated for the object, this object is shown.
New objects	The list of objects (users and computers) added to the directory structure within a defined period of time. *Active Directory-/LDAP-/Novell eDirectory-/Azure AD* objects appear in Reports after the synchronization *Own directory* objects are displayed immediately once added.
Windows Subsystem for Linux (WSL)	Overview of computers where the WSL feature is enabled (**WSL statuses** radio button) and Linux distributions are installed (**Linux distributions** radio button). To collect data from computers about WSL, enable WSL data collection.

Enabling WSL data collection

1. Go to **Computer management**.
2. In the **Computer management** work area, select default rights (computer) or a directory service object (OU, computer, group).

   If you enable WSL settings in default rights, the settings are inherited to all computers.
3. In the **Settings | Client settings** tab, enable the following check boxes in the **Windows Subsystem for Linux** area to collect WSL data:
   a. **Check WSL enabled** to collect information about the state of the WSL feature.
   b. **Detect installed Linux distributions** to collect information about installed Linux distributions.
4. Click **Save**.

➥ Data about WSL is now collected from selected directory objects.

Control

Report type	Available information
Not updated rights	Right changes which were defined in Console, but haven’t been applied to users or computers, for example, because a user didn’t log into the system
Analyzing of rights changes	Changes in the assigned access rights.
Rights analysis	Overview of the directory service objects that have selected access rights. For details, see: Showing rights analysis
Rights review – details	Overview of access rights for selected device classes. List of permissions per user, computer and/or group.

Rights review – summary	The percentage and the number of directory objects, to which certain access rights for the selected device class are assigned.
Difference with default rights	Directory objects, for which the assigned access rights for device classes differ from default access rights.
Broken inheritance	Directory objects, where the inheritance of access rights for device classes from a group has been deactivated
Temporary access rights	Directory objects, for which temporary access rights for a device classes are currently applied.
Unblocking codes review	Displaying unblocking codes generated for users and the time when users activated them.
Individual device permissions	All active and inactive individual device permissions assigned to directory objects.

See also: Access Control

Analyzing rights of a device type

1. Go to **Reports | Control | Rights analysis**.
2. Select a directory object type: users, computers and/or groups.
3. In the **Time schema** area, select the week day and time to see objects for which the selected access right is applied (scheduled access). This criterion also includes all objects for which one access right is applied constantly, in spite of a week day and time.

➥ The directory service objects with the corresponding rights appear in the list.

Audit

ATTENTION	**Audit table display limitation** Each Secure Audit report can display only up to 1 million records. See also Archiving or deleting old audit data

Report type	Available information
Management overview	🟩 Files transfer: the number of files transferred to the external storage, network, and cloud storage. 🟩 Unencrypted files transfer: the number of files transferred without encryption. 🟩 Blocked access: the number of files with restricted access.
File access	All operations with files which are audited by the Secure Audit product.
Blocked access	All user access attempts which have been violated.
Devices connection	Data about connecting external storage devices.

Unencrypted files transfer	Files transferred to controlled clouds and devices (external storage and CD/DVD) without encryption if **Removable Device Encryption** and **Cloud Storage Encryption** are activated. If **Encryption** is disabled under Product settings | Encryption options, the *Unencrypted files transfer* report is not displayed. If the shadow copy product is enabled for a user, open or save files directly from the **Console**.
Internet	The history of user browsers.
Wi-Fi	The facts of connection to the wireless networks and information whether the networks are secure or open (insecure).
Applications launch	Displaying the launch history of all applications, processes and dynamic link libraries.
Use of applications	Viewing the applications usage summary, including the usage date and duration.
System events	History of computer shut down, start, sleep, hibernation, etc.

For details, see: Secure Audit

Filters

Report type	Available information
Assigned filters	File type filters assigned to users. Group filters by filter names (Filter radio button) or by directory objects (Entities radio button).

For details, see: Filters: controlling access to the file formats

Encryption

Report type	Available information
Encrypted folders	Overview of local folders encrypted by an administrator and by users.
Encrypted network folders	Overview of network folders encrypted by an administrator and by users. Decrypted folders display with the *Not encrypted* status and are automatically deleted from the Console in 3 days after being decrypted.

BitLocker

Report type	Available information
Encryption status	Overview of all drives encrypted with BitLocker Management and the status of the encryption.

FDE

Report type	Available information
Management overview	- FDE status: status of the FDE component installation and initialization. - PBA status: status of the PBA component installation and initialization. - Product version: version of the installed Full Disk Encryption product on computers. - Encryption status: status of disk encryption on computers. The **Partially encrypted** status means that not all drives of the computer are encrypted. - ERI file: computers with the activated FDE product where ERI file is available or not.

Antivirus (EgoSecure Antivirus)

Report type	Available information
Management overview	- Status: the status of the EgoSecure Antivirus installation on computers. - Version of virus signatures DB: the status of updating the database with virus signatures. - Other antiviruses detected by EgoSecure Antivirus: statistics of other antivirus programs that prevented to install EgoSecure Antivirus. - Computer protection status: status of the EgoSecure Antivirus on computers.
Event log	Actions that an administrator performed with the Antivirus: installation, uninstallation, scans and their results, errors.
Threat found	Audits all infected and suspicious objects detected during a scan.
Quarantine	List of files that appear in Quarantine as a result of scan. For details, see: EgoSecure Antivirus quarantine

For details, see: EgoSecure Antivirus

DLP (Data Loss Prevention)

Report type	Available information
Data in Use	The history of access to text files, where matches are found.
Data at Rest	The history of finding text files, where matches are found and the actions performed with the found files.
Scans	The history of scans performed within the DLR – DAR product.
Quarantine	Files moved to quarantine as a result of the scan performed by DLP – DAR. You can restore, delete of download these files.

For details, see: Data Loss Prevention

Green IT

Report type	Available information
Your profit	A sum of money and power saved, and an amount of CO2 emissions reduced. The data allows for calculating a forecast for a year.
Suspicious activity	The duration of computers activity. The detailed filtering feature allows for filtering only the desired time period.

For details, see: Green IT

Inventory

Report type	Available information
Logical disks	Volume name, file system type, amount of filled space, volume size and data modified.
Disk drives	Disk model, its interface type, serial number, size, *etc*.
Physical memory	Physical memory, its manufacturer, serial number, capacity, and data modified.
Processors	Processor name, device and processor ID, family, manufacturer, architecture, speed, *etc*.
Video cards	Device ID, name, resolution, video memory, *etc*.
Applications	All applications installed on selected Agents with the following details: installation date, publisher, version, location.
Executable files (*.exe)	Files executed on Agents: date and time, size, hash value, vendor.

For details, see: Inventory

15.2. Exporting reports

With **EgoSecure**, you can select reports for export and save them locally, and also send them by e-mail.

INFO

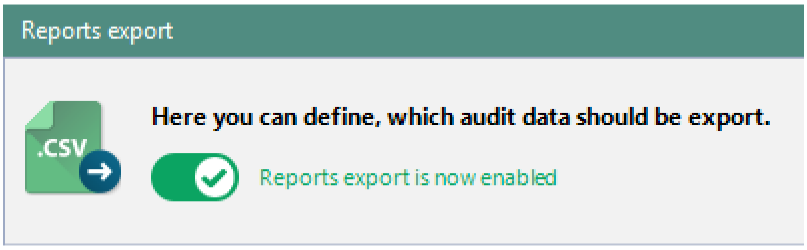
Sending reports via e-mail

To send report files by e-mail, specify an e-mail account from where to send reports.

- Define e-mail address settings under **Administration | Servers | Mail, proxy and others**. For details, see: Setting up SMTP

Setting up the export of reports

1. Go to **Administration | Administrator | Reports export**.
2. Enable the reports export.



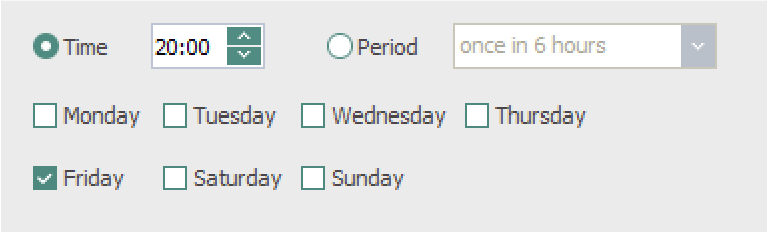
Reports export

Here you can define, which audit data should be export.

Reports export is now enabled

→ The reports export functionality is now enabled.

3. In the **Server** drop-down menu, select the **Server** where reports are exported and stored.
4. In the **Directory** field, specify the exact location where the reports are exported and stored on the **Server** computer.
5. In the **Recipients** field, enter e-mail address where reports are sent if the **Send copy to E-mail** check box is selected for a report entry. To send reports to multiple recipients, divide them with a semicolon (**;**). All generated reports are sent as a **.zip** archive.
6. Select a period or specific time and check the boxes with weekdays. On the example below, reports are sent every Friday at 20.00.



● Time 20:00 ○ Period once in 6 hours

□ Monday □ Tuesday □ Wednesday □ Thursday

☑ Friday □ Saturday □ Sunday

7. Enable **Hide user/computer data** to generate reports with unreal user names. Note: only in **Synchronization Log**, and **Assigned filters** real user names are written in any case.
8. In the **Language** drop-down menu, select in what language the reports are generated. **Default (system)** means that the language of the system, where the Server is installed, is used.
9. Under **Reports for export**, check the boxes with report types. If a report contains no information, this report type is generated, but has no data inside.

   → Selected reports are saved to the defined directory on the server computer.

10. Check the **Send copy to e-mail** box to send reports as zip archives to mail addresses defined in the **Recipients** field.

    Selected reports are additionally sent to defined e-mail addresses.
11. Click **Save**.

16. BITLOCKER MANAGEMENT

With **BitLocker Management** you can manage **Windows BitLocker** remotely from the **EgoSecure Console** on the client computers. BitLocker allows the encryption of entire drives and is integrated in the Windows operating system.

16.1. Setting up BitLocker Management

To encrypt disks via **Console** with BitLocker, activate **BitLocker Management** for a computer and set up the settings.

Activating and setting up BitLocker Management

1. Under **Computer management**, activate **BitLocker Management** for a computer. For details, see: Activating products.
2. Under **Product settings | BitLocker | BitLocker settings**, in the **Default method** drop-down, select an encryption method used by default for all computers. The method can also be selected for each computer before encryption via the **Encrypt with** option.
   For details, see: Available encryption methods
3. In the **Encryption key protection** work area, click **Change** and define a password. This password is used by default for locking and unlocking all encrypted volumes locally on computer and can be changed individually for each volume after the volume encryption.
4. Set the **Store recovery password for already encrypted drives in EgoSecure database** box to make the **Copy recovery password** option available in the context menu for all encrypted volumes.
5. Click **Save**.

Available encryption methods

BitLocker basically supports two different methods for disk encryption or two different key lengths:

- AES 128
- AES 256

Longer keys offer a higher level of security and are more difficult, for example, by cracking by brute force attacks. However, they can lead to noticeable losses in performance and slower encryption and decryption of data.
In addition to the key length, BitLocker supports the following options when selecting the encryption method:

- Diffuser algorithm
- XTS algorithm

It is recommended to enable **Automatic selection** as the default method. If this option is activated, the most suitable encryption method depending on the operating system is automatically selected.

16.2. Encrypting and decrypting disks

Encrypting a volume

1. Select a computer in **Computer management | BitLocker**.
2. In the lower area, in the **Drives** tab, right-click a volume.
3. To encrypt a volume:
    - Select **Encrypt** to encrypt with a default method defined in **Product settings | BitLocker | BitLocker settings**.
    - Select **Encrypt with** and select an encryption method from the context menu to encrypt with one of the available methods.

➥ The **Status** column value changes from **Not encrypted** to **Encryption in progress**. Once the encryption is finished, the **Fully encrypted** status is displayed. Now the volume is encrypted via **BitLocker** encryption.

To restrict access to encrypted disk with a password, lock a volume manually or restart a client computer once encryption is finished (the volume is locked automatically after the restart).

Locking a volume

1. Select a computer in **Computer management | BitLocker**.
2. Right-click a volume in the **Drives** tab.
3. Select **Lock** from the context menu.

➥ The status changes to **Volume is locked**. When client unlocks the volume on the computer (enters the password), the status **Volume is locked** remains. The unlocked volume is accessed without a password till the next computer restart.

Automatically unlocking an encrypted volume

1. Go to **Product settings | BitLocker | BitLocker settings**.
2. Enable the check box **Automatically unlock encrypted data volumes**.
3. Click **Save**.
4. Select a computer in **Computer management | BitLocker**.
5. Right-click an encrypted volume in the **Drives** tab.
6. Select **Enable auto-unlock** from the context menu.

Decrypting a volume

! Before decrypting, make sure the drive is unlocked. If necessary, unlock it by entering the password.

1. Select a computer in **Computer management | BitLocker**.
2. Right-click a volume in the **Drives** tab.
3. Select **Decrypt** from the context menu.

➥ The decryption starts. The status changes to **Decryption in progress**. Once the decryption finishes, the status changes to **Not encrypted**.

Viewing BitLocker encryption status

1. Go to **Reports | BitLocker | Encryption status**.
2. In the **Directory service structure** area, select the directory element, which contains computers.
3. Select the status from the drop-down list.
4. Click **Group by computer** to display volumes according to computers to which they belong.
5. Click **Show** to update information.

➥ The drives that match the selected directory service area and the selected encryption status are displayed.

16.3. Managing BitLocker passwords

By default, drives are locked with the password that was set in the product settings (see also: setting up BitLocker Management). However, you can customize the password for a drive individually.

Changing a volume password

! Before changing a password, make sure the volume is unlocked.

1. Go to **Computer management | BitLocker** and select a computer.
2. In the **Drives** tab, right-click an encrypted volume.
3. Select **Change password...** from the context menu.

   → The **Enter password** dialog appears.

4. Enter a new password and confirm it.

If you have lost the drive password, you will need a recovery password to access the encrypted drive.

Saving recovery password

! Recovery password is copied to restore user data in case of emergency. Recovery password is stored in the EgoSecure database and can be copied from there if **Store recovery password for already encrypted drives in EgoSecure database** box is enabled under **Product settings | BitLocker settings | Encryption key protection** work area. Recovery password can be copied from a locked or unlocked drive. See also: setting up BitLocker Management

1. Select a computer in **Computer management | BitLocker**.
2. Under the **Drives** tab, right-click an encrypted drive.
3. Select **Copy Recovery password** from the context menu.

   → The **Copy Recovery password** dialog appears.

4. Click **Copy**.

➥ The password is copied to the clipboard. Save the recovery password, e.g., to a text file.

17. FULL DISK ENCRYPTION

EgoSecure Full Disk Encryption is a product developed separately from **EgoSecure Data Protection Server**. **EgoSecure Full Disk Encryption** can be installed locally or via the **EgoSecure Data Protection Console** (remotely). Remote installation and management is performed if the **EgoSecure Agent** is installed on a computer.

The encryption settings and encryption keys under **Product settings | Encryption** are NOT connected to Full Disk Encryption.

Detailed information about **FDE** you can find in:
Installation and troubleshooting guide
Administration and usage guide

INFO	**Applying changes made locally** Changes made locally (except statuses about initialization/deinitialization and disk encryption) are not transferred to the **EgoSecure Server** and, therefore, not displayed in the **EgoSecure Data Protection Console**.

17.1. Installation

The installation of the Full Disk Encryption consists of three stages:

1. FDE installation
2. FDE initialization
3. PBA installation and initialization

FDE installation and update

Preparing the installation

1. Go to **Product settings | FDE | Installation settings**.
2. If the installation files will be located on the EgoSecure Server,
   a. Select the **EgoSecure Server** radio button.
   b. In the **FDE 32-bit installation file** and **FDE 64-bit installation file** areas, click **...** to upload the EgoSecure Full Disk Encryption by Matrix42 [version].msi and EgoSecure Full Disk Encryption by Matrix42 [version] x64.msi files respectively.
3. If the installation files are located in the network directory,
   a. Select the **Network directory** radio button.
   b. In the **Network folder** field, define a network folder where the Full Disk Encryption installation file is stored. Make sure the installation archive has been unzipped.

   c. In the **User** and **Password** fields, specify a login, with which the EgoSecure Server can access the share.
   d. Enter the file names of MSI files.
4. In the **Component selection** field, define which components to install on the clients. The FDE component is enabled automatically and cannot be disabled, because without it no other component can be installed.
   - **PBA**: PBA components
   - **Control Panel**: EgoSecure Full Disk Encryption Control Center Plugin for the Windows control panel
   - **Policy Builder**: Policy Builder components
   - **Report API**: Support for status information retrieval via third-party applications
   - **Recovery Tools**: Windows PE Emergency Recovery Disk (ERD), Secure Erase and Secure Wipe
5. Click **Save**.

Creating a configuration profile

1. Go to **Product settings | FDE | Configuration profiles**.
2. Click ✚ **Add**.

   → A new profile appears in the list.
3. Double-click the profile and enter a name.
4. In the lower area, specify the settings.
5. Click **Save**.

✓ You can now use the profile for the FDE installation. For details, see: Installing FDE.

Installing FDE

1. Go to **Computer management | FDE**.
2. Select the domain and folder in the **Directory service structure** work area.
3. In the **Computer management - FDE** work area, right-click an online computer and click **Activate**. To select multiple computers, hold down the `Ctrl` key and click.

   → The **Full Disk Encryption** license is activated for the selected computer.
4. To apply a user-defined profile or to specify settings manually, right-click on the client and select:
   a. **Configuration profiles | [profile name]**: install with a user-specific configuration profile. For details, see: Creating a configuration profile
   b. **Configuration profiles | <None>:** install without a profile.
   If this step is skipped, the **Default** profile is used.
5. Right-click the client and select **Install Full Disk Encryption** from the context menu.

→ The installation starts. In the **FDE status** column, the **Installation in progress** entry appears.

Updating FDE

1. Prepare the latest EgoSecure Full Disk Encryption installation files in the network directory or reupload them to the EgoSecure Server. For details, see Preparing the installation.
2. Go to **Computer management | FDE**.
3. Select a computer. To multiselect, hold down **Ctrl** and click.
4. Right-click a computer and select **Update Full Disk Encryption** from the context menu.

Fixing installation problems: solutions

- In **Product settings | FDE | Installation settings**, check whether the FDE installation package exists in the specified network share, check the credentials for accessing the network share.
- Check the access to the network share from the client computer using the same credentials specified in the **Console**.
- Check whether the **EgoSecure Agent** is installed on target computers.
- Check the communication and connectivity between the EgoSecure Server and the EgoSecure Agent:
  ```
  telnet computername 6006 –  to check connectivity from the Server to the Agent
  telnet servername 6005 –  to check connectivity from the Agent to the Server
  ```
- Windows Firewall or other 3rd party firewalls can block communication and exception rule is required for the communication ports used.

If nothing helps and installation fails, technical support and the EgoSecure engineering team needs the following information:

- Error message screenshot or behavior description.
- The time when the error occurred to locate the information in the log files (full screenshot with the time in the system tray is preferable).
- Server log file collected with maximum detail (Log level = Debug or Extreme debug).

FDE initialization

ATTENTION	**Client restart required** During the initialization, the computer on which the initialization is performed must be restarted.

Starting initialization

1. Under **Computer management | FDE**, right-click a computer. To select multiple ones, hold down `Ctrl` and click.
2. Select **Initialize FDE** from the context menu.
3. Click **OK** to confirm the message.
   → The initialization starts. In the **FDE status** column the **Executing script** entry appears.

➥ Once the FDE initialization is finished, the **not initialized** status in the **FDE** column changes to **initialized**.

PBA installation and initialization

PBA is installed together with **FDE** if the **PBA** check box is selected under **Product settings | FDE | Installation settings**. If PBA check box was not enabled before installation, right-click a computer and select **Install PBA** from the context menu.

! PBA can be initialized only after the FDE initialization.

1. Under **Computer management | FDE**, right-click a computer.
2. Select **Install PBA** from the context menu if PBA has not been installed along with FDE.
3. Select **Initialize PBA** from the context menu.

➥ PBA is installed and initialized, the script to transmit the changes is created.

Protecting installation with the administrator password

The administrator password is defined to forbid a user to make changes in Full Disk Encryption locally without a password.

Changing administrator password

1. Under **Computer management | FDE**, right-click a computer.
2. Select **Change administrator password** from the context menu.

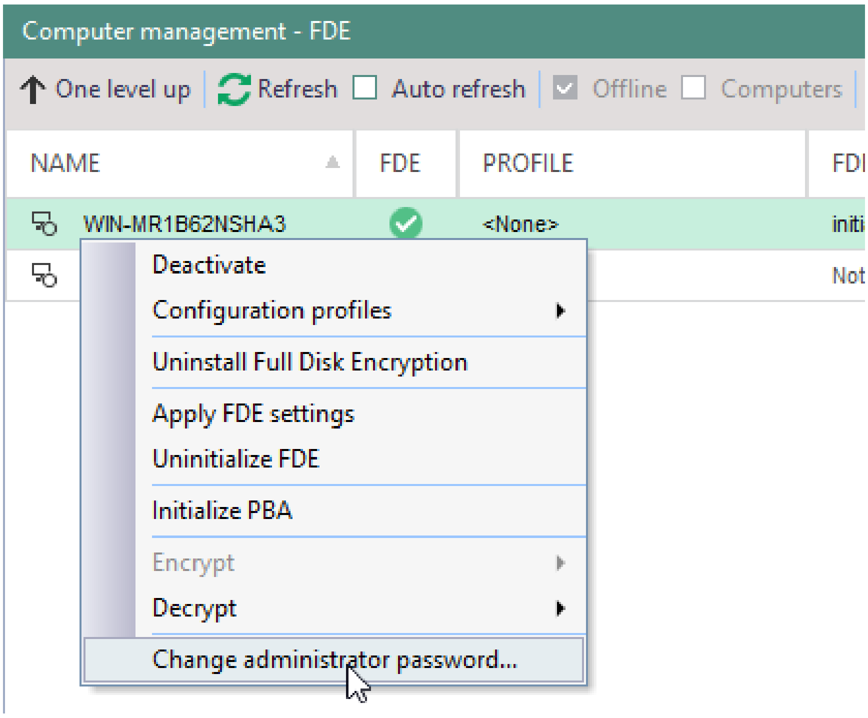


Figure 163. Changing administrator password

3. Enter a new password and confirm it.
4. Click **OK**.

! The administration password from the **Administrator** tab is used for computer authentication, but doesn’t change a password.

Entering password for authentication

! This password is used only to authenticate the client with FDE installed. This password must be the same as the administration password.

1. Select a computer under **Computer management | FDE**.
2. In the **Administrator** tab, **Administration password** area, click **Change**.

   → The **Enter password** dialog appears.

3. Enter the password and confirm it.
4. Click **OK**.

   → The dialog closes.

17.2. Configuring PBA

Configuring authentication via a smart card

Pre-boot authentication is performed via user credentials (domain, user and password) or via a smart card. To perform authentication via the smart card, a special certificate must be copied to it and the smart card must meet the requirements.

Requirements for smart cards

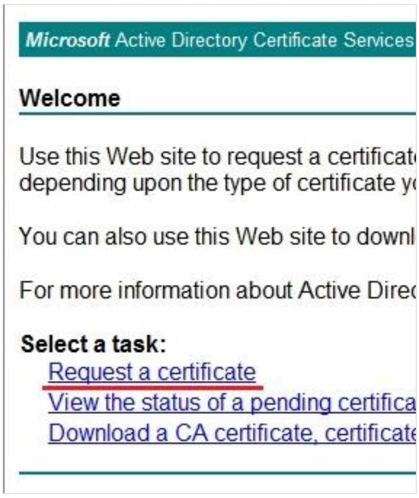
- Smart card model is supported by EgoSecure.
- Smart card supports buffer encryption (contains special key usage attributes).

WARNING	**Before using smart card in production environment** Before using smart cards in the production environment, check in the test environment whether the configured smart card works correctly.

Preparing a smart card

The steps below describe on how to get a certificate signed by Microsoft in the Active Directory Certificate Services. Smart cards with self-signed certificates may also work with PBA, but we cannot guarantee. That is why, better use the solution below.

1. Create a certificate signing request in the utility of your smart card or in the Microsoft Management Console.
2. Deploy the PKI. For details, see the Microsoft article which describes how to configure the internal certificate authority.
3. In **Internet Explorer**, open an enterprise Certification Authority page (generally, it looks like https://IP-adress_of_CA/certsrv or https://domain_name_of_certificate _authority/certsrv). When authorization is required, enter the credentials of the user, whom the certificate must be given to.
4. Click the Request a certificate link.



Microsoft Active Directory Certificate Services

Welcome

Use this Web site to request a certificat
depending upon the type of certificate y

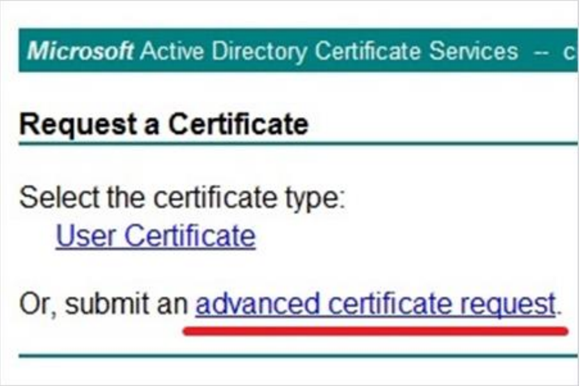
You can also use this Web site to downl

For more information about Active Direc

Select a task:
Request a certificate
View the status of a pending certifica
Download a CA certificate, certificate

Figure 164. Preparing smart card for PBA: certificate link

5. Click the advanced certificate request link.



Microsoft Active Directory Certificate Services -- c

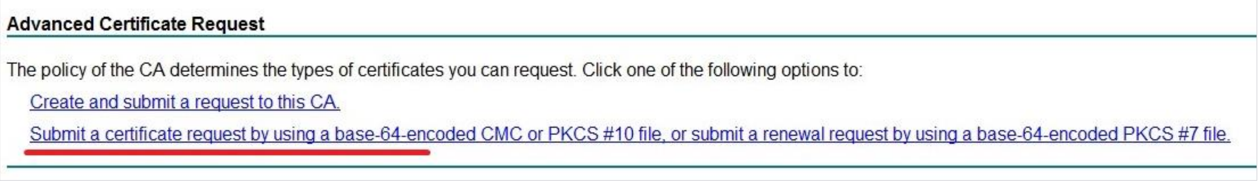
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Figure 165. Preparing smart card for PBA: certificate request

6. Click the link **Submit a certificate request by using a base 64-encoded CMC**…



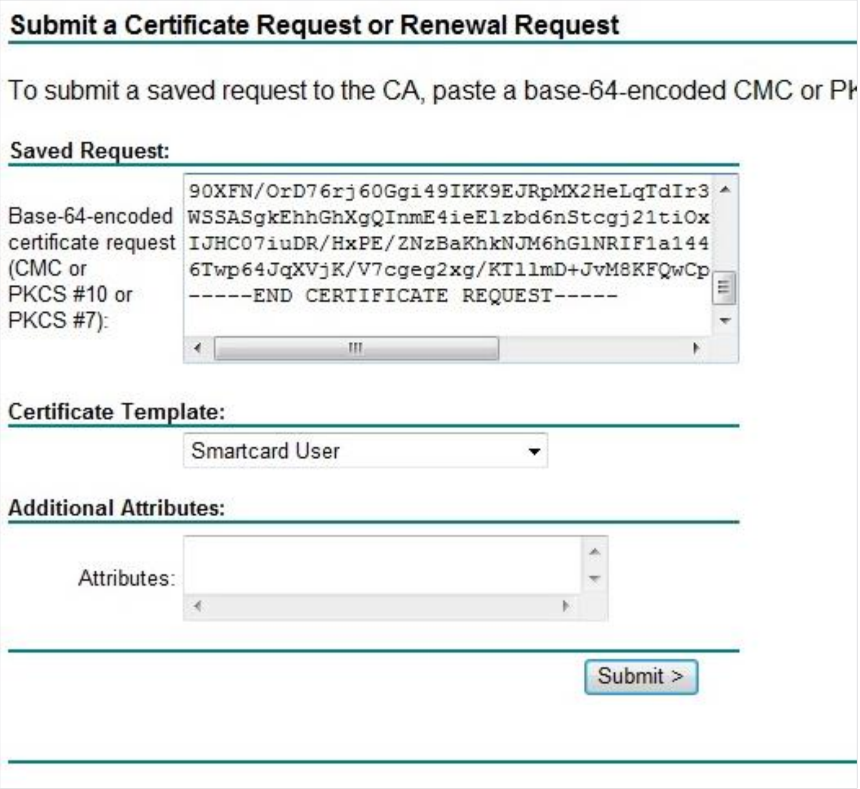
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

7. Open the certificate request file in any text editor (for example, Notepad), and copy its content to the clipboard.
8. Paste information from clipboard to the **Saved Request** field. In the **Certificate Template** section, select **Smartcard User** from the drop-down list, and press the **Submit** button.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or Pk

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
90XFN/OrD76rj60Ggi49IKK9EJRpMX2HeLqTdIr3
WSSASgkEhhGhXgQInmE4ieElzbd6nStcgj21tiOx
IJHC07iuDR/HxPE/ZNzBaKhkNJM6hGlNRIF1a144
6Twp64JqXVjK/V7cgeg2xg/KTllmD+JvM8KFQwCp
-----END CERTIFICATE REQUEST-----
```

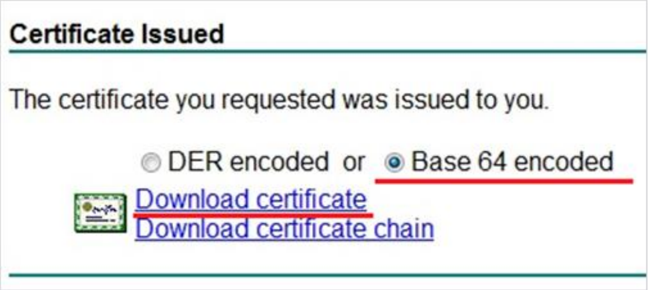
Certificate Template:

Smartcard User

Additional Attributes:

Attributes:

9. Select the **Base 64 encoded** radio button, and then click the **Download certificate** link to save the certificate in the **Base 64** format.



Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate

Download certificate chain

10.Save the certificate to the smart card.

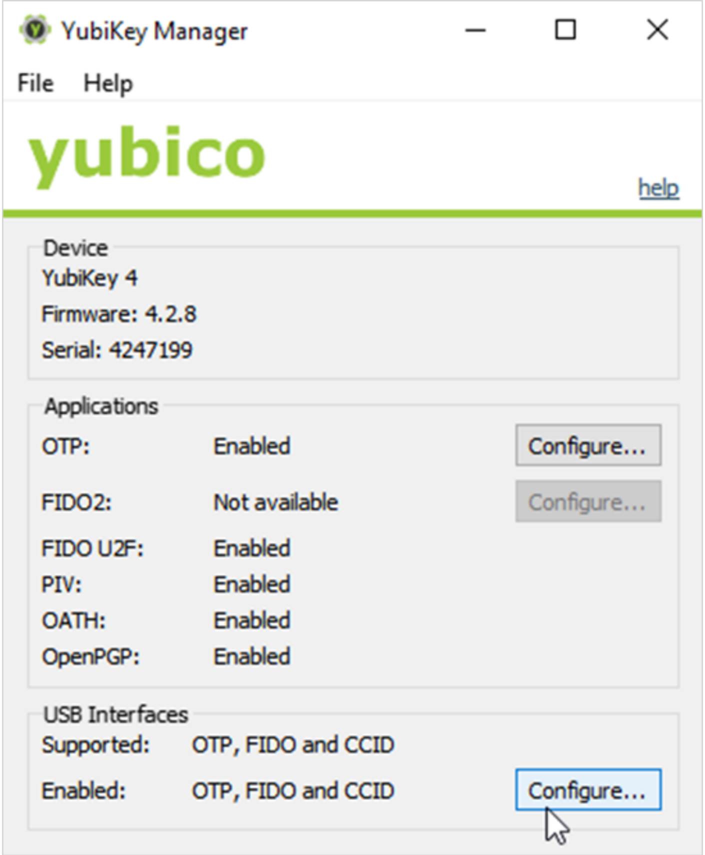
11.Unplug and re-attach the smart card.

Preparing YubiKey smart cards

1. Download and install the following utilities:

- YubiKey Manager
- YubiKey PIV Manager

2. Start the **YubiKey Manager** utility.
3. Click Configure.



Device
YubiKey 4
Firmware: 4.2.8
Serial: 4247199

Applications

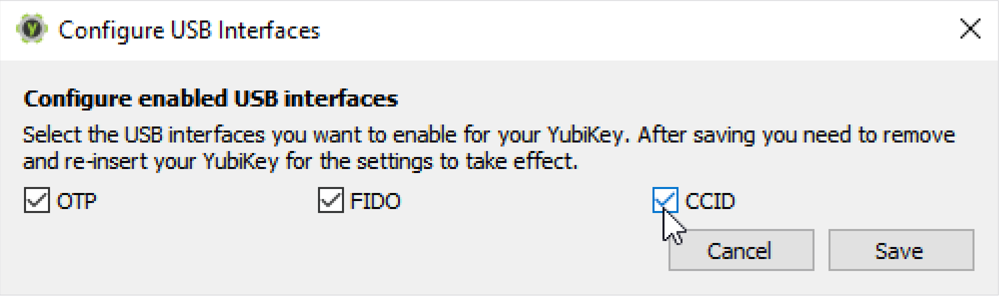
OTP:	Enabled	Configure...
FIDO2:	Not available	Configure...
FIDO U2F:	Enabled	
PIV:	Enabled	
OATH:	Enabled	
OpenPGP:	Enabled	

USB Interfaces

Supported:	OTP, FIDO and CCID	
Enabled:	OTP, FIDO and CCID	Configure...

→ The **Configure USB Interfaces** dialog appears.

4. Enable the **CCID** check box, and click **Save**.



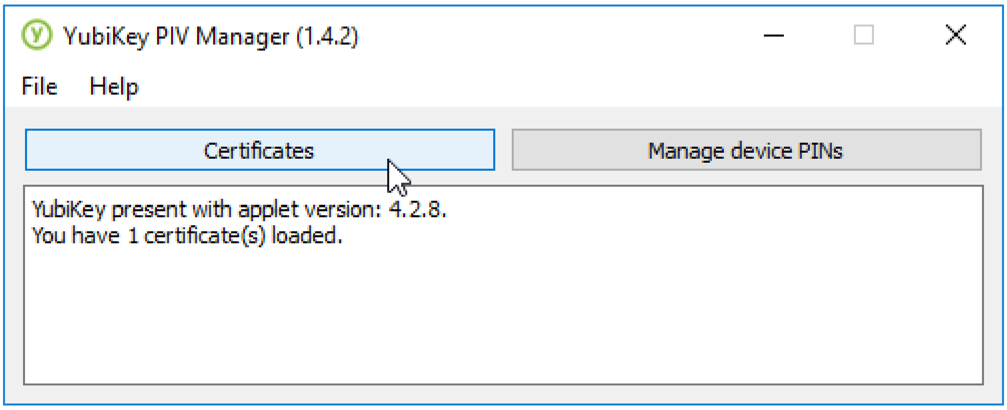
Configure USB Interfaces

Configure enabled USB interfaces

Select the USB interfaces you want to enable for your YubiKey. After saving you need to remove and re-insert your YubiKey for the settings to take effect.

☑ OTP ☑ FIDO ☑ CCID

5. Unplug and re-attach **YubiKey Neo** device, and close the **YubiKey Manager** utility.
6. Open the **YubiKey PIV Manager** utility, and click the **Certificates** button.



YubiKey present with applet version: 4.2.8.
You have 1 certificate(s) loaded.

7. In the **Authentication** tab, click **Generate new key**.
8. Select the **RSA (2048 bits)** encryption algorithm. In the **Output** panel, select the **Certificate Signing Request (CSR)** radio button.

! Only certificates signed by a domain with a Certificate Authority are supported.

9. Specify the path for the subject of the user in the Active Directory.
For example, for the user who is in the Organizational unit of the `cit.local` domain, the path looks like this:
`/CN=user/OU=OrganizationUnit/DC=cit/DC=local`

10.Click **OK**.

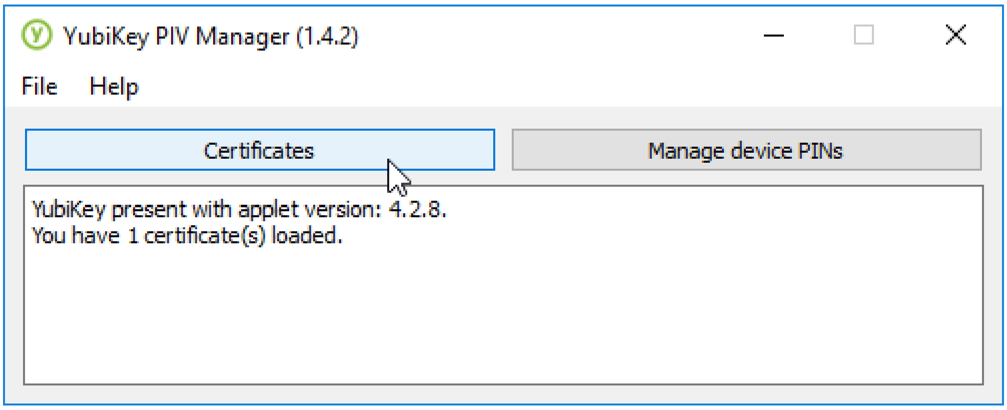
→ The **Save Certificate Signing Request as** dialog appears.

11. Enter a file name to save a certificate request, and select the folder where to store the file.

12.Enter PIN for device access.

→ The private key is generated and saved to the device. Perform steps 2-9 described in Preparing a smart card.

13. Open the **YubiKey PIV Manager** utility application, and then click the **Certificates** button.



YubiKey present with applet version: 4.2.8.
You have 1 certificate(s) loaded.

14. In the **Authentication** tab, press the **Import from file...** button to load the certificate created from file.
15. Unplug and re-attach the device to use the **YubiKey Neo** device with a new certificate.

Adding a smart card for PBA

Using the **EgoSecure Data Protection Console**, smart card can be added manually or automatically. It is better to use an automatic way of capturing credentials instead of a manual one till the moment the smart card is checked in a test environment. Once the logon with the smart card is performed successfully in the test environment, enable user capturing for all computers (automatically) or add smart card credentials for all computers manually.

- ***Adding a smart card automatically***:

1. Open the **EgoSecure Data Protection Console**. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, select the smart card logon method.
3. Check Enable user capturing.
4. Click **Save**.
5. Right-click the computer and select **Apply PBA settings**.

During next boot on the selected computer, smart card credentials are captured automatically and a user is added to the list. During all other boots performed after it, pre-boot authentication with the smart card occurs.

- ***Adding a smart card manually***

1. Open the EgoSecure Data Protection Console. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, select the smart card logon method.

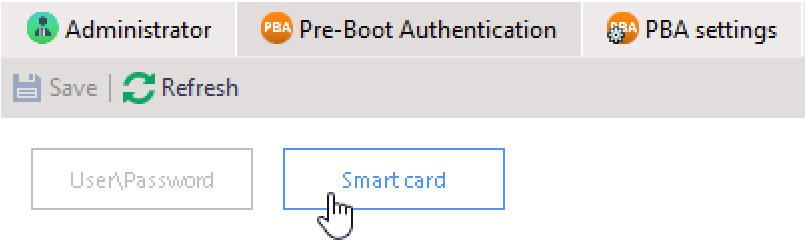
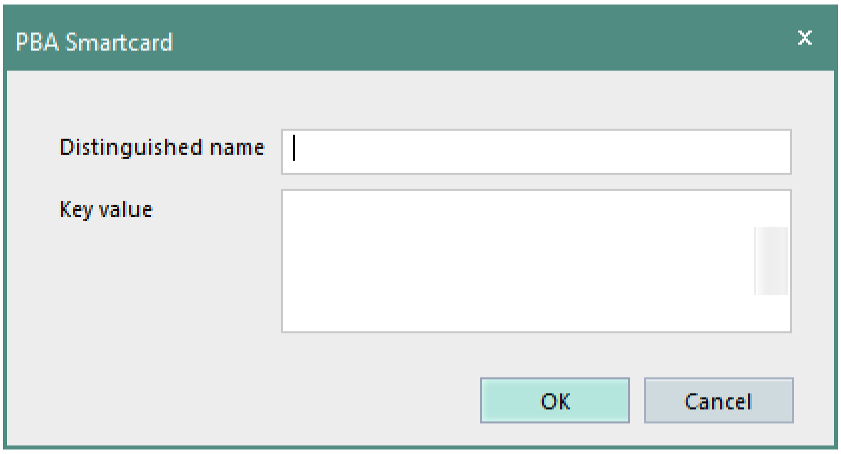


Figure 166. Configuring smart card logon method

3. Click **Add**.

   → The **PBA Smartcard** dialog appears.

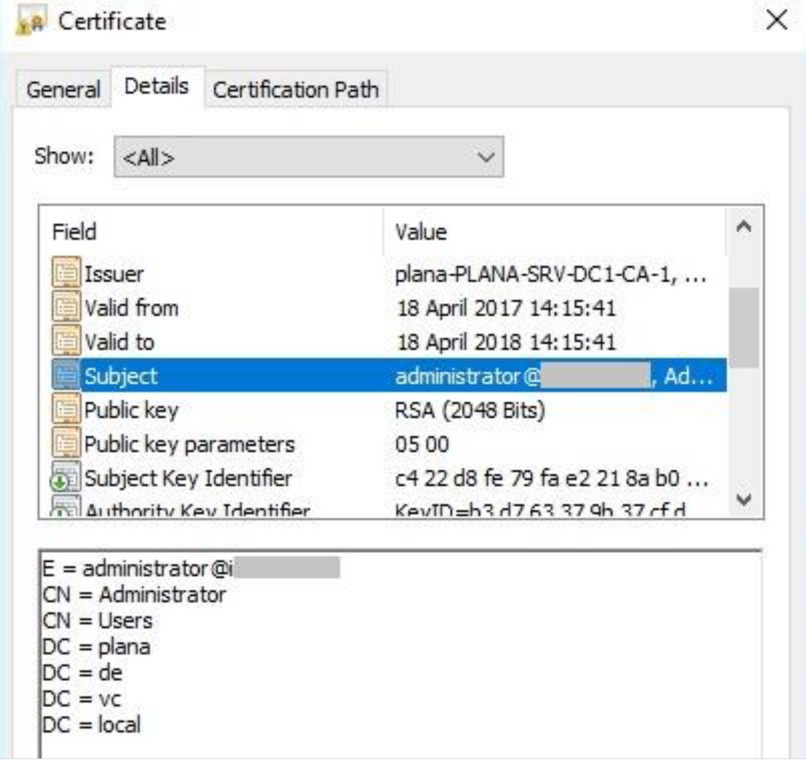


4. Double-click a smartcard certificate and select **Properties** from the context menu.

   → The **Certificate** dialog appears.

5. In the **Certificate** dialog, navigate to the **Details** tab.
6. Copy the data from the **Value** column of the **Subject** entry to the **Distinguished name** field of the **PBA smartcard** dialog. E.g.: local, vc, de, plana, Users, Administrator, administrator@....

ATTENTION	**Special characters and order** - In most cases, the values of the **Subject** field are pasted in the reverse order. Test if it works, if not - import a certificate locally (as described in the EgoSecure FDE – Installation and troubleshooting guide, "*Importing a certificate*") to see which order is the right one. The order depends on the smart card specification. - Special characters are not supported. Check if there are any special characters in the required fields.



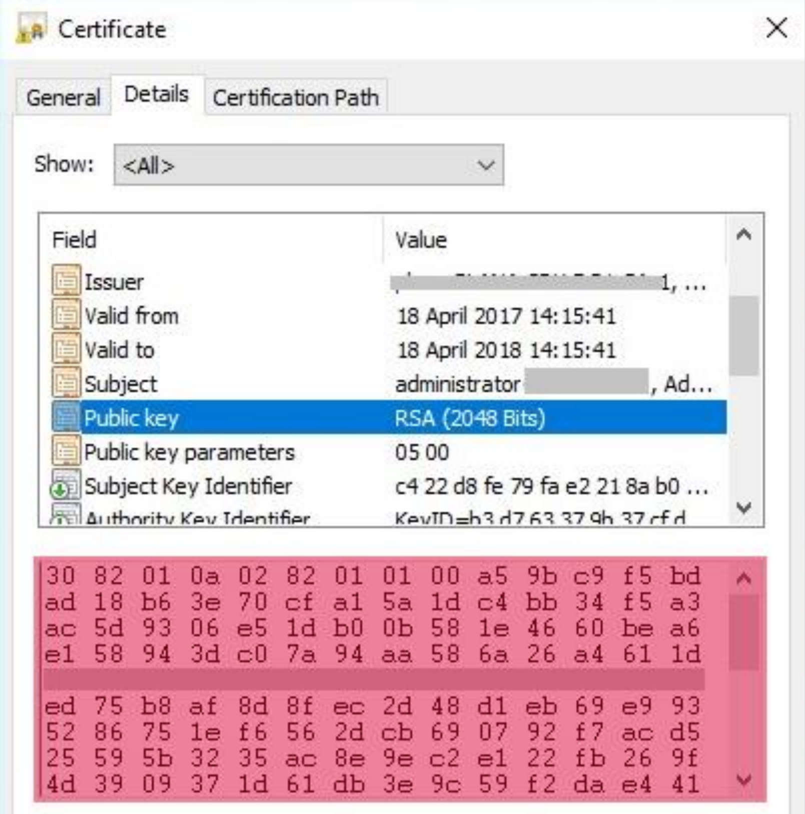
Certificate

Show: <All>

Field	Value
Issuer	plana-PLANA-SRV-DC1-CA-1, …
Valid from	18 April 2017 14:15:41
Valid to	18 April 2018 14:15:41
Subject	administrator@[redacted], Ad…
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	c4 22 d8 fe 79 fa e2 21 8a b0 …
Authority Key Identifier	KeyID=b3 d7 63 37 9b 37 cf d

```
E = administrator@i[redacted]
CN = Administrator
CN = Users
DC = plana
DC = de
DC = vc
DC = local
```

7. Copy the data of the **Public key** entry to the **Key value** field of the **PBA smartcard dialog**.



Certificate

Show: <All>

Field	Value
Issuer	[redacted]1, …
Valid from	18 April 2017 14:15:41
Valid to	18 April 2018 14:15:41
Subject	administrator[redacted], Ad…
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	c4 22 d8 fe 79 fa e2 21 8a b0 …
Authority Key Identifier	KeyID=b3 d7 63 37 9b 37 cf d

```
30 82 01 0a 02 82 01 01 00 a5 9b c9 f5 bd
ad 18 b6 3e 70 cf a1 5a 1d c4 bb 34 f5 a3
ac 5d 93 06 e5 1d b0 0b 58 1e 46 60 be a6
e1 58 94 3d c0 7a 94 aa 58 6a 26 a4 61 1d
[redacted]
ed 75 b8 af 8d 8f ec 2d 48 d1 eb 69 e9 93
52 86 75 1e f6 56 2d cb 69 07 92 f7 ac d5
25 59 5b 32 35 ac 8e 9e c2 e1 22 fb 26 9f
4d 39 09 37 1d 61 db 3e 9c 59 f2 da e4 41
```

8. Click **OK** in the **PBA Smartcard** dialog.
9. Right-click the computer and select **Apply PBA settings**.

Defining smart card reader and PKCS#11 provider

By default, the smart card reader and PKCS#11 provider are detected automatically, but it increases the amount of computer start time.

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Smart card** tab, in the smart card reader drop-down, select the card reader you want to use for PBA. Selecting *Automatically detect card reader* means that all the CCID-compliant readers contained in the generic CCID bundle delivered with *Linux* will be used – this will increase the startup time.
3. In the **PKCS#11 provider** drop-down, select the PKCS#11 provider mechanism on the smart card. Selecting *Automatically detect provider* means that all the providers will be checked upon startup - this setting does not work with several smart cards.

Defining criteria for selecting the certificate used for encryption (optional)

Define the criteria for selecting the certificate used for encryption. Certificates can be distinguished by labels or key usage.

! The certificate label and key label entries are case sensitive! Bear this in mind when defining the certificate labels or the key labels. If the labels are configured incorrectly, it will prevent the successful authentication of the user and, therefore, the system will not start.

If the **Key Usage** is set to the wrong values, i.e. no certificate on the smart card matches the usage set in the list, then authentication is also not possible and the system will not start.

Label

The term ‘Label’ refers to the filename of the certificate file on the smart card, for example User_Certificate.
Follow these steps to add a certificate based on a Label:

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Certificates** tab, select the **Label** radio button.
3. Enter the label into the **Label** field and click **Add**. If the smart card contains more than one certificate (multi-user access) then you should add the labels for those as well.
4. If you have mistakenly entered a false label, select it from the list and click the **Remove** button to remove it from the list.
5. To sort label preference, select a label in the list and click either **Up** or **Down** - the certificate that will be used for authentication is the first one in the list that matches the label criteria.

Key Usage

Key usage extensions define the purpose of the public key contained in a certificate. You can use them to restrict the public key to as few or as many operations as needed. For example, if you have a key used only for signing, select **Digital signature** and/or **Non-repudiation** extensions from the drop-down menu. Alternatively, if a key is used only for key management, select **Key encipherment**.

For further details about the key usages supported by **EgoSecure Full Disk Encryption** smart card authentication, see the EgoSecure FDE - Administration and Usage Guide, chapter 6.2.

Follow these steps to add a certificate based on Key Usage:

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Certificates** tab, select the **Key Usage** radio button.
3. Choose a standardized form of key usage from the **Key Usage** drop-down menu, for example, **Data Encipherment**.
4. Click **Add**.
5. To give preference to a specific key usage, select it from the list and click either **Up** or **Down**. Key usages at the top of the list have preference (the certificate that will be used for authentication is the first one whose key usage matches the criteria in the list).
6. Select one of the following matching policies:

- **Any**. The first certificate that contains any key usage from the list will be used.
- **All**. The certificate must fulfil all the key usages in the list.
- **None**. No certificate may contain any of the key usages from the list.

7. If you have mistakenly entered a false certificate label, select it from the list and click **Remove**.

Configuring authentication via user credentials

Using the **EgoSecure Data Protection Console**, user credentials be added manually or automatically. It is better to use an automatic way of capturing credentials instead of a manual one till the moment the smart card is checked in a test environment. Once the logon with the smart card is performed successfully in the test environment, enable user capturing for all computers (automatically) or add smart card credentials for all computers manually.

INFO	**PBA password length** The maximum password length for Pre-Boot Authentication is 32 symbols.

- Adding user credentials automatically

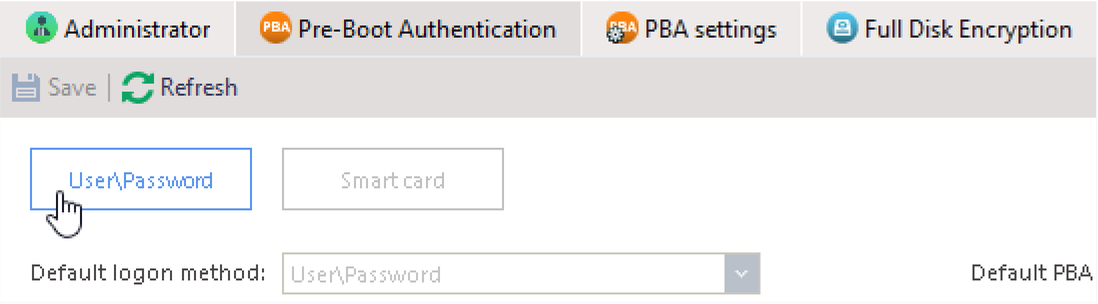
1. Open the EgoSecure Data Protection Console. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **PBA authentication** tab, select the user credentials logon method.

3. Check Enable user capturing.
4. Click **Save**.
5. Right-click the computer and select **Apply PBA settings**.

➥ During next boot on the selected computer, user credentials are captured automatically and a user is added to the list. During all other boots performed after it, pre-boot authentication with user credentials occurs.

- Adding user credentials manually

1. Open the EgoSecure Data Protection Console. In **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, select the **User/Password** logon method.

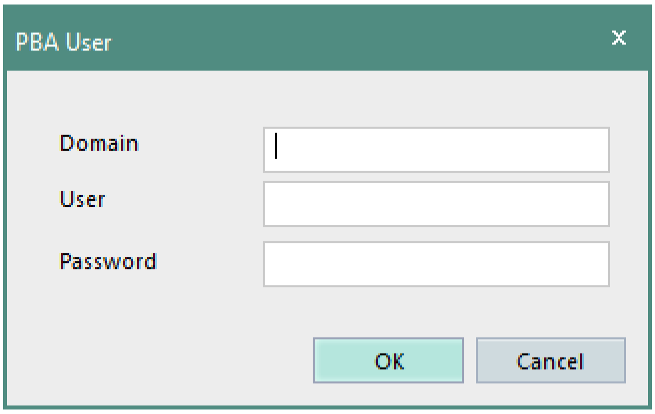


Default logon method: User\Password

Default PBA

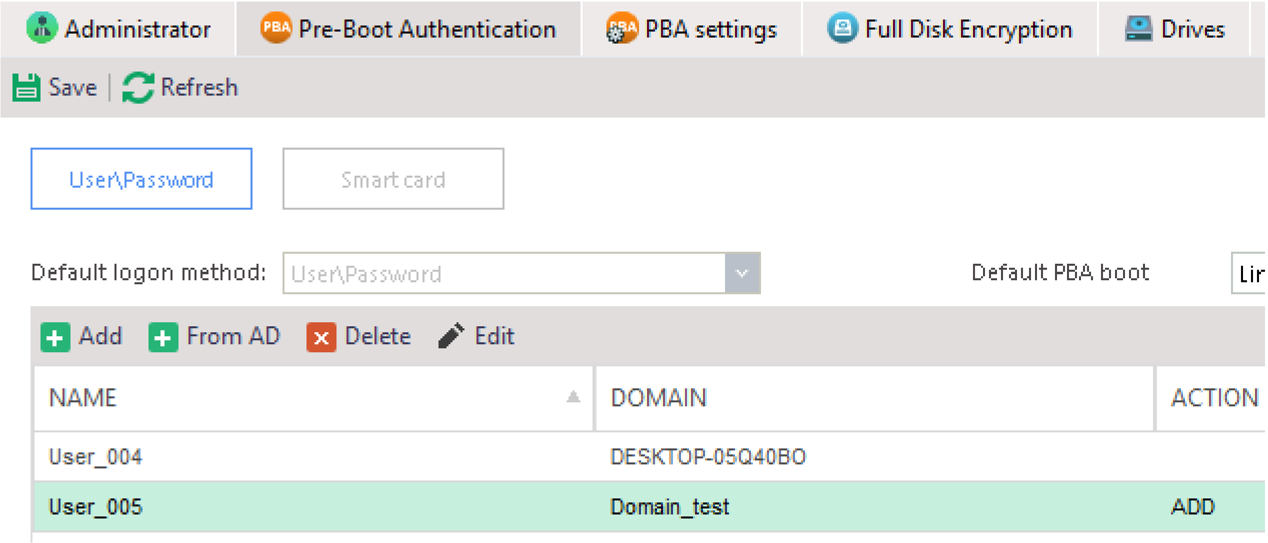
3. Click **Add**.

   → The **PBA User** dialog appears.



4. In the **Domain** field, enter a domain, to which a user belongs.
5. Enter a user name and password. The password must me no longer that 32 symbols.
6. Click **OK**.

   → The dialog closes and a new entry appears.



Default logon method: User\Password

Default PBA boot Lir

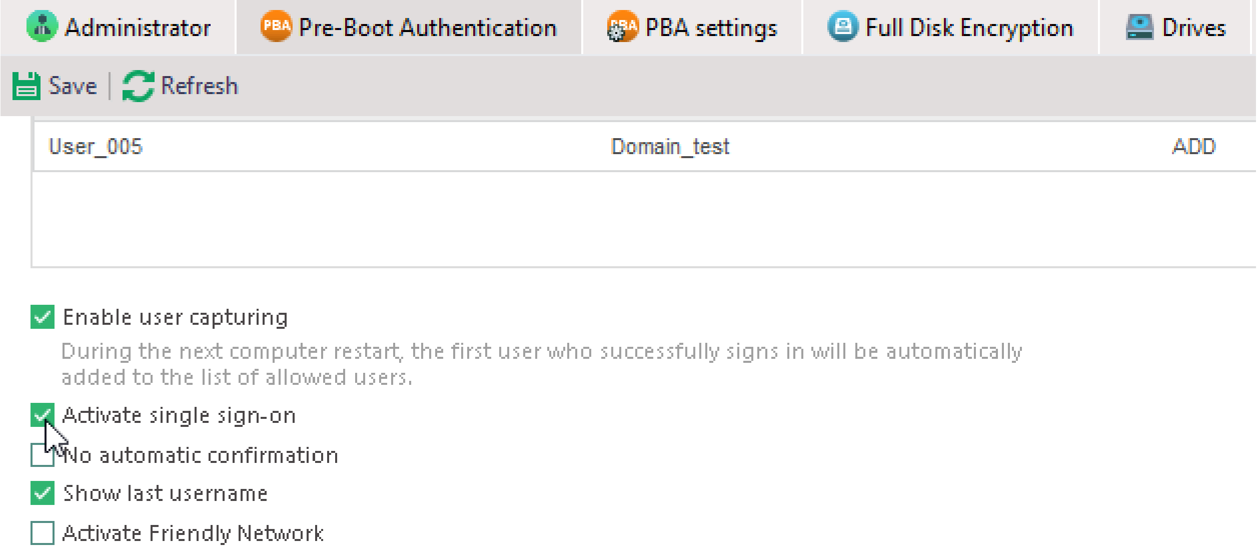
NAME	DOMAIN	ACTION
User_004	DESKTOP-05Q40BO	
User_005	Domain_test	ADD

7. Click **Save**.
8. Right-click the computer and select **Apply PBA settings**.

Permitting single sign-on (SSO) for a user

When SSO is enabled, a user only needs to enter smart card or user credentials in the EgoSecure PBA dialog once, because standard Windows logon dialog will be performed automatically. When SSO is disabled, a user needs to enter smart card or user credentials twice: in the **EgoSecure PBA** dialog and then in standard Windows logon dialog.

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, enable **Activate single sign-on**.



User_005	Domain_test	ADD

☑ Enable user capturing

During the next computer restart, the first user who successfully signs in will be automatically added to the list of allowed users.

☑ Activate single sign-on

□ No automatic confirmation

☑ Show last username

□ Activate Friendly Network

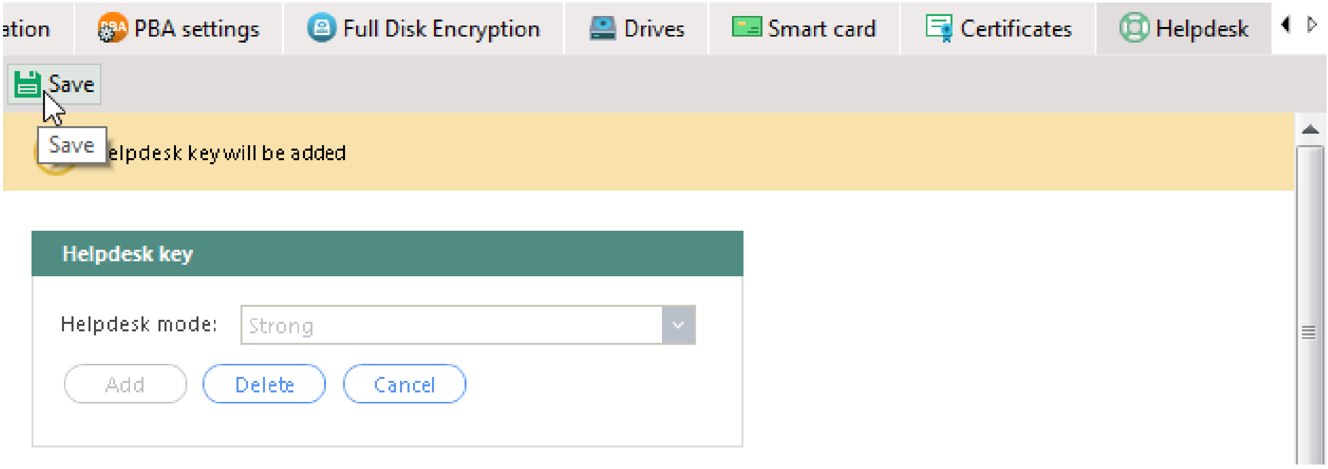
3. Enable the **No automatic confirmation** option so that user credentials will be pre-entered into the Windows logon dialog but user confirms them manually. If the option is not enabled, the Windows logon dialog doesn’t appear for a user at all.

4. Enable the **Show last username** option to always display the user name of the last known logged-on user in the **PBA logon** dialog.
5. Click **Save**.
6. Right-click the computer and select **Apply PBA settings**.

Enabling Helpdesk for a computer

Helpdesk assists users to boot their computers in case of emergency, for example, when a user has forgotten the password or lost the smart card. The Challenge-Response mechanism is used to securely unlock PBA.

1. Under **Computer management | FDE**, select a computer.
2. Go to the **Helpdesk** tab.
3. Select the mode (comfort or strong).
4. Click **Add**.
5. Click **Save**.



elpdesk key will be added

Helpdesk key

Helpdesk mode: Strong

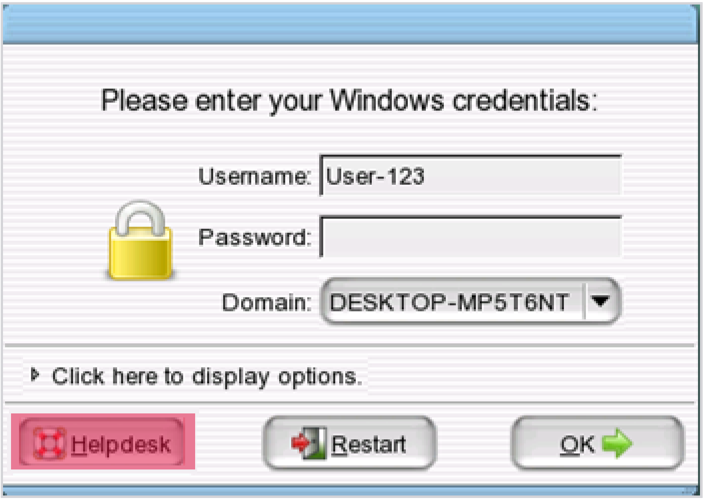
6. Right-click the computer in the **Computer management - FDE** work area.
7. Select **Apply PBA settings** from the context menu.

   → Once the script is executed, the **Helpdesk activated** message appears.

Using Helpdesk

Goal: to deactivate PBA for a user for 1 boot.
User:

1. Restarts a computer to boot Windows once PBA is installed and initialized.
2. Restarts a computer once again and cannot remember the password.
3. Clicks the **Helpdesk** button.



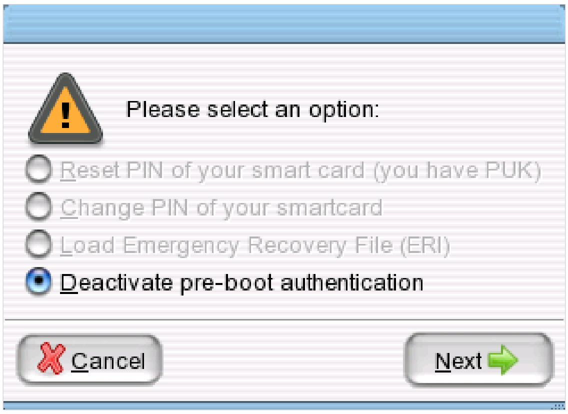
Please enter your Windows credentials:

Username: User-123

Password:

Domain: DESKTOP-MP5T6NT

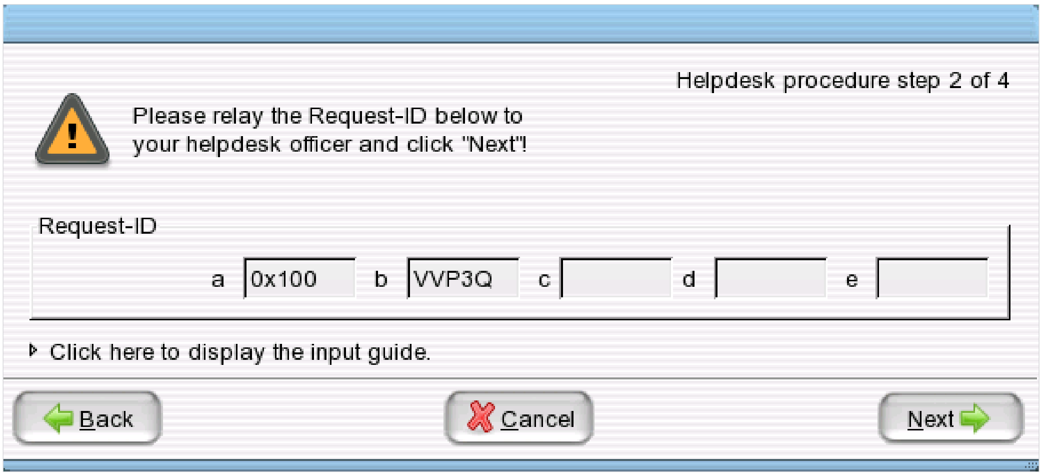
4. Selects the Deactivate pre-boot authentication option. Clicks Next.



Please select an option:

○ Reset PIN of your smart card (you have PUK)
○ Change PIN of your smartcard
○ Load Emergency Recovery File (ERI)
● Deactivate pre-boot authentication

5. Contacts an administrator and clicks **Next**.
6. Sends the displayed **Request ID** to the administrator. Clicks **Next**.



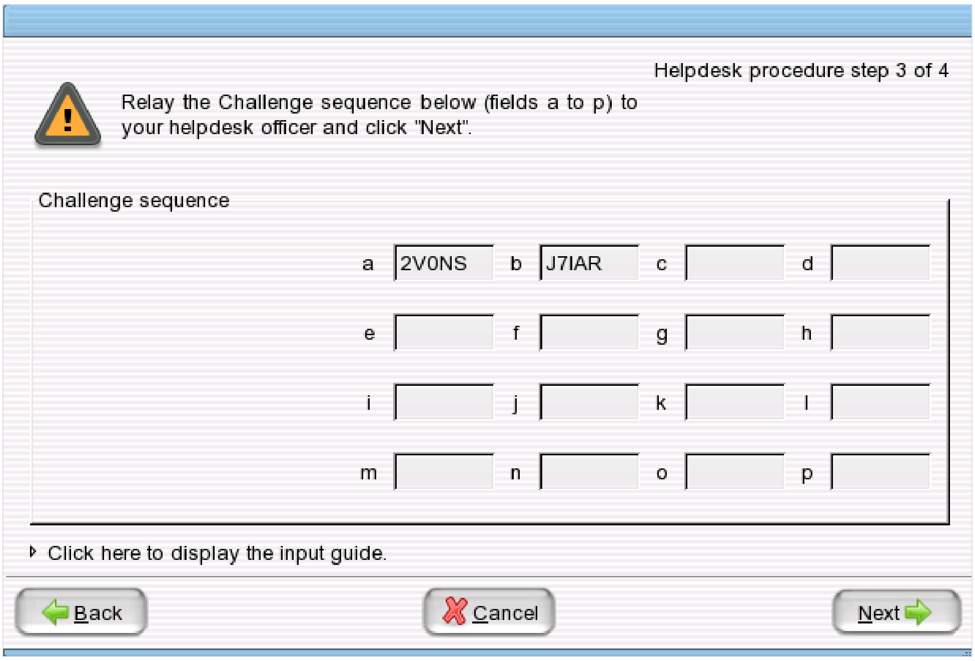
Helpdesk procedure step 2 of 4

Please relay the Request-ID below to your helpdesk officer and click "Next"!

Request-ID

a 0x100 b VVP3Q c d e

7. Sends the displayed **Challenge code** to the administrator. Clicks **Next**.



Helpdesk procedure step 3 of 4

Relay the Challenge sequence below (fields a to p) to your helpdesk officer and click "Next".

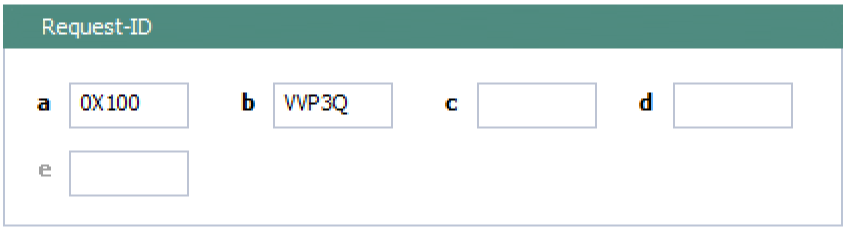
Challenge sequence

a	2V0NS	b	J7IAR	c		d	
e		f		g		h	
i		j		k		l	
m		n		o		p	

Click here to display the input guide.

Administrator:

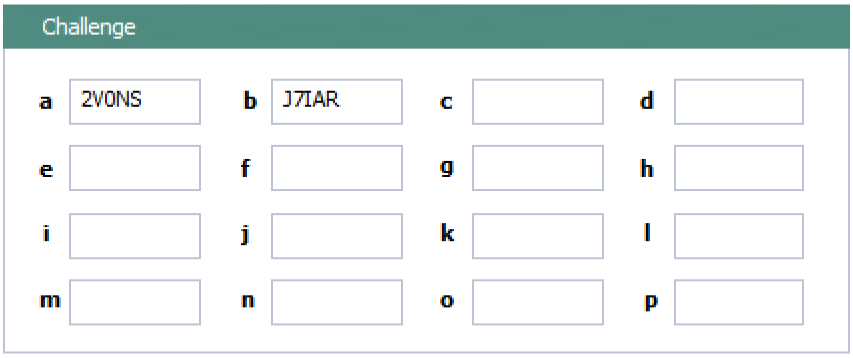
1. Enters the request ID code into the **Request ID** field.



Request-ID

a	0X100	b	VVP3Q	c		d	
e							

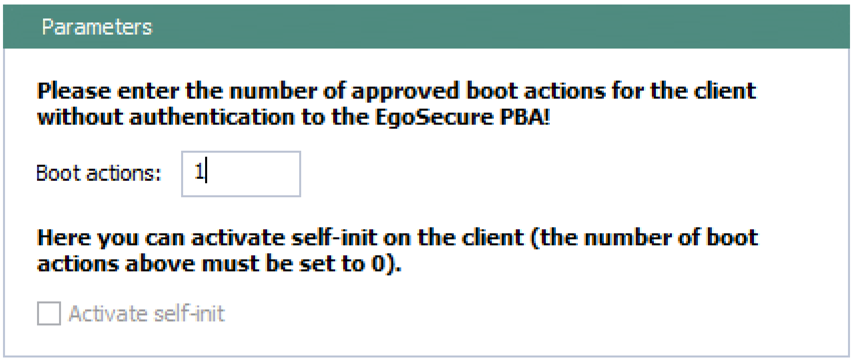
2. Enters the challenge code into the **Challenge** field.



Challenge

a	2V0NS	b	J7IAR	c		d	
e		f		g		h	
i		j		k		l	
m		n		o		p	

3. Sets the number of boot actions permitted without PBA authentication.



Parameters

Please enter the number of approved boot actions for the client without authentication to the EgoSecure PBA!

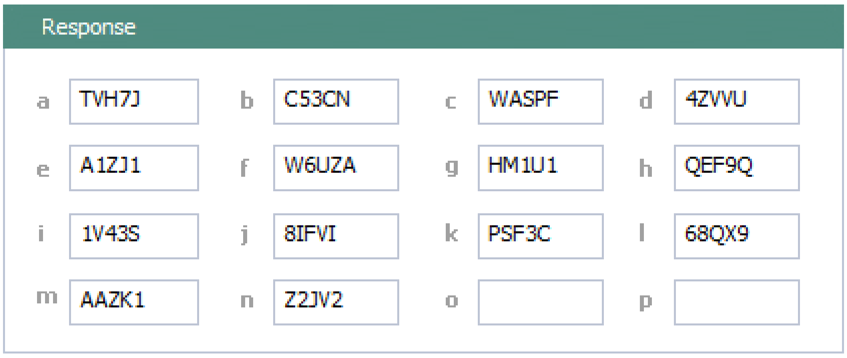
Boot actions: 1

Here you can activate self-init on the client (the number of boot actions above must be set to 0).

□ Activate self-init

4. Clicks **Generate**.

   → The response code is automatically generated in the **Response** field.



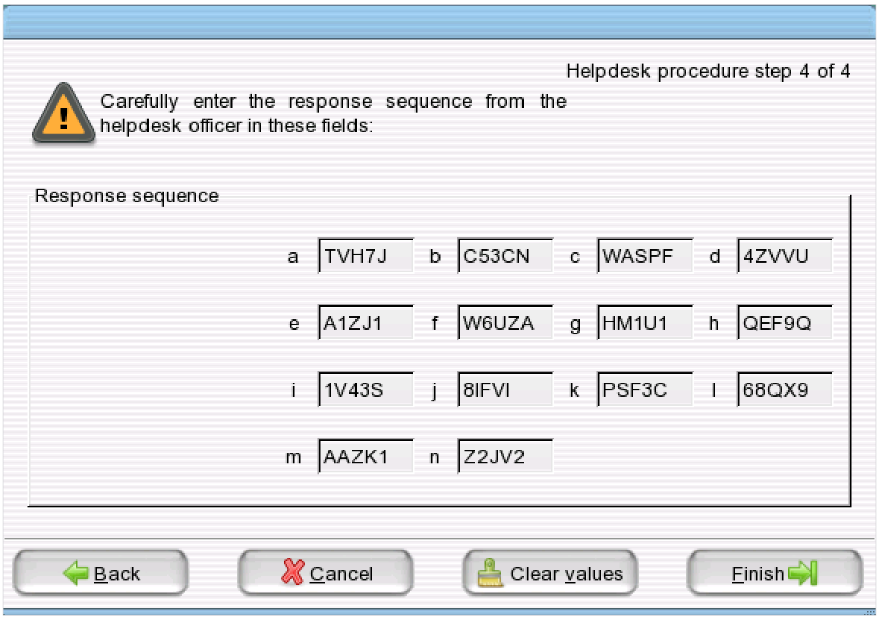
Response

a	TVH7J	b	C53CN	c	WASPF	d	4ZVVU
e	A1ZJ1	f	W6UZA	g	HM1U1	h	QEF9Q
i	1V43S	j	8IFVI	k	PSF3C	l	68QX9
m	AAZK1	n	Z2JV2	o		p	

5. Sends the code to the user.

User:

1. Enters the code.



Helpdesk procedure step 4 of 4

Carefully enter the response sequence from the helpdesk officer in these fields:

Response sequence

a	TVH7J	b	C53CN	c	WASPF	d	4ZVVU
e	A1ZJ1	f	W6UZA	g	HM1U1	h	QEF9Q
i	1V43S	j	8IFVI	k	PSF3C	l	68QX9
m	AAZK1	n	Z2JV2				

2. Clicks **Finish**.

Using Friendly network

Friendly network simplifies the process of booting if the network is known. If connection to the Server can be established during PBA, the authentication is skipped and boot into Windows occurs.
If computer is outside the known network, the PBA asks for authentication.

Functionality

PBA authentication phase is skipped with the help of Helpdesk. When PBA is booted, helpdesk request is generated and sent to the Server. An attempt to sign in to the system on the basis of a server response is made. If the attempt is successful, the computer is restarted followed by Windows boot. If the attempt is unsuccessful (incorrect network configuration, no connection to the Server etc.), PBA authentication is needed as usually.

Requirements

- Helpdesk is activated for the computer. For details, see helpdesk.
- Computer has at least one Ethernet adapter connected to the network that has access to the **EgoSecure Server**.
- The connected adapter is supported by EgoSecure. See the list of Supported Ethernet manufacturers for Friendly Network.
- The network supports DHCP protocol.
- The network uses IPv4.

Restrictions

- The ACPI boot mode is not supported.
- Not compatible with BIOS Simple PBA (text-based mode).
- Not compatible with Linux-based PBA if SSL is enabled.

INFO

Recommended on BIOS

Disable Quick Boot (Fast Boot) in BIOS settings as it skips the network drivers necessary for Friendly Network.

Enabling Friendly network

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, enable the **Activate Friendly Network** option.
3. Click **Save**.
4. Right-click the computer and select **Apply PBA settings**.

ATTENTION

Local changes do not display in Console

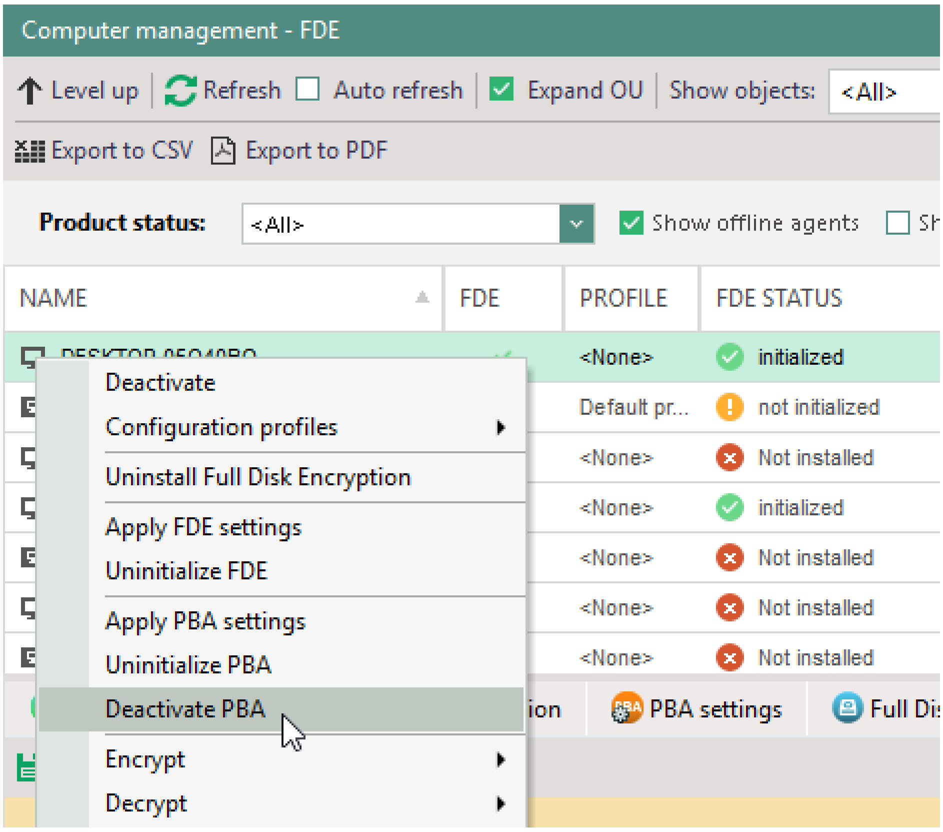
Friendly network is activated not only via the EgoSecure Data Protection Console, but also via the EgoSecure Full Disk Encryption Control Center. If the option state changes locally in the EgoSecure Full Disk Encryption

	Control Center, the option state in the EgoSecure Data Protection Console doesn’t change.

Temporary disabling PBA

Sometimes computer reboot without PBA is needed. To deactivate PBA and activate it automatically after reboot, the following steps are performed:

1. Go to Computer management | FDE.
2. Right-click a computer and select **Deactivate PBA** from the context menu.



NAME	FDE	PROFILE	FDE STATUS
DESKTOP-0E040BO	✓	<None>	initialized
		Default pr...	not initialized
		<None>	Not installed
		<None>	initialized
		<None>	Not installed
		<None>	Not installed
		<None>	Not installed

→ The **Deactivate PBA** dialog appears.

3. Enable the checkbox and define the number of reboots.
4. Click **OK**.

→ The dialog closes.

Once a defined number of reboots is performed, PBA is activated back automatically.

! Computer reboot can be initiated only when status in the PBA column is changed to **deactivated** and script is executed successfully.

Defining the number of failed PBA login attempts

The **locking** option enables the process of system locking when the user enters incorrect login data. Leaving the **Locking** option disabled allows users to enter their password incorrectly a limitless number of times without penalty.

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **PBA settings** tab, check the **Enable locking** option.
3. In the **Failed logins after which login is delayed** field, enter the number of times a user may enter an incorrect password before being penalized with a time penalty the next time they logon. This number should be less than that for *Maximum number of failed attempts*.
4. In the **Maximum number of failed logins** field, enter the number of times a user may attempt to enter the correct password. This number should be more than that for *Failed attempts after which login is delayed*. Entering the value 0 means that locking is deactivated!
5. Click **Save**.
6. Right-click the computer and select **Apply PBA settings**.

Configuring PBA login dialog

Selecting the background image and keyboard layout for PBA logon dialog

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **PBA settings** tab, under **Other settings**, select one of the **Background image** option for the PBA logon dialog:
   - **Default** to use a default PBA image.
   - **Sync desktop wallpaper** to use an individual desktop wallpaper of each computer where PBA is launched.
   - **Sync lock screen wallpaper** to use an individual lock screen wallpaper of each computer where PBA is launched.
   - **Custom** to select an optional background image. The image is automatically resized to the correct resolution and color depth for the PBA screen: 800x600 pixels, 24-bit.
3. If you selected **Custom** in the previous step, click ... in the **Custom image path** field to define a path for a background image.
4. In the **Keyboard layout** drop-down, select which keyboard layout is used for PBA.
5. Click **Save**.
6. Right-click the computer and select **Apply PBA settings**.

Showing the name of the last logged in user in the PBA logon dialog

1. Under **Computer management | FDE**, select a computer where PBA is initialized.
2. In the **Pre-Boot Authentication** tab, enable the **Show last username** option.

3. Click **Save**.
4. Right-click the computer and select **Apply PBA settings**.

If PBA loading with current motherboard failed

If PBA loading with current motherboard failed or your motherboard is considered as an old one, reinitialize FDE with the enabled **Use alternate loader** option.

1. Under **Computer management | FDE**, select a computer where FDE has been uninitialized.
2. In the **Full Disk Encryption** tab, enable the **Use alternate loader** option in the **Alternate loader** area.
3. Click **Save**.
4. Initialize FDE again.

17.3. Using FDE

Requirements for encryption

Hard disk encryption applies to IDE, SATA, and SCSI hard disks formatted using the NTFS file system under Windows. Hard disks formatted using the FAT file system are not supported.

EgoSecure Full Disk Encryption supports the integrated power management mechanisms of Windows 'Suspend to RAM' and 'Suspend to Disk' with enabled, as well as disabled, PBA.
If your hard disk is already encrypted using a third-party product, please, decrypt it BEFORE re-encryption with **EgoSecure Full Disk Encryption**.
You cannot apply hard disk encryption to the following:

- Disks formatted with FAT
- A remote (network) hard disk
- A drive that uses software BIOS, for example: EZ-Drive, Drive-Pro or Disk Manager.

WARNING

Possible data loss

To avoid data loss, follow the points below:

- Do not encrypt drives that are already encrypted.

  If your hard drive is already encrypted with a third-party product, decrypt it BEFORE encryption with **EgoSecure Full Disk Encryption.**

- Do not encrypt system logical drives where the operating system is installed.

- Make sure that you close, or stop, applications that perform hard disk intensive operations before you start the initial encryption.

	- Do not turn off the computer or work on the computer while the initial encryption is in progress. Doing so would result in data corruption.

Emergency recovery

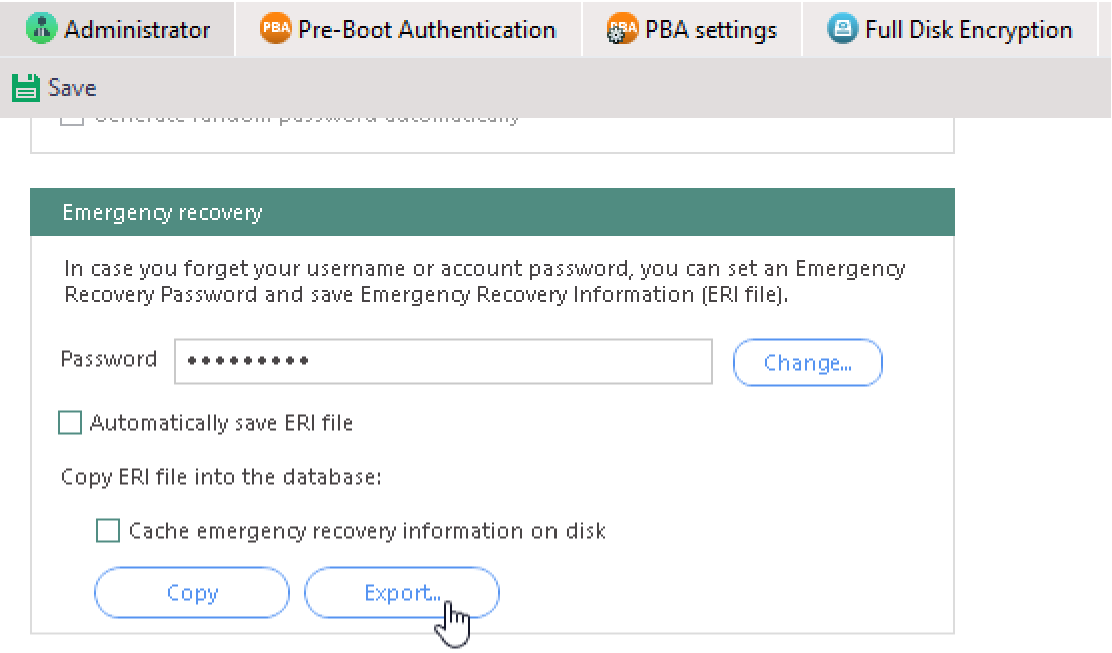
Below is described why emergency recovery is needed and how to get the emergency recovery file. For details about performing emergency recovery, see the EgoSecure FDE – Administration and usage guide, chapter 1.13.

Why ERI file is needed? ERI file is used to decrypt an encrypted disk if, for example, administrator password is forgotten.

How to create ERI file? ERI file is created automatically during a disk encryption. Click Change to specify a password for the ERI file before the disk encryption. If the password is not specified the disk encryption fails.

How to export ERI file?

- If **Automatically save ERI file** option was checked before the disk encryption, the ERI file is copied to the **EgoSecure database** automatically and, therefore, can be saved as a file via the **Export** button.



Emergency recovery

In case you forget your username or account password, you can set an Emergency Recovery Password and save Emergency Recovery Information (ERI file).

Password: •••••••••• [Change...]

□ Automatically save ERI file

Copy ERI file into the database:

□ Cache emergency recovery information on disk

- If **Automatically save ERI file** option was NOT checked before encryption, ERI file is not copied to the **EgoSecure database** automatically and, therefore, can NOT be saved as a file via the **Export** button. In this case, copy ERI file to the **EgoSecure database** manually by clicking **Copy** and then click **Export**.

Storing data for emergency recovery in cache. To store data for emergency recovery in cache of the computer where FDE is installed, enable **Cache emergency recovery information on disk**. This data is stored on the FDE partition in an encrypted form. That allows for administrator to load emergency recovery information directly from computer cache when it is needed.

Encrypting a disk

1. Define settings to decrypt a disk in case of emergency.
2. Read the requirements for encryption.
3. Under **Computer management | FDE**, in the **Full Disk Encryption** tab, select one of the encryption options:

- **Encrypt the whole drive**. Encrypting all sectors of the drive provides more security because even such things as already deleted data will be encrypted. Select this option to encrypt all the sectors of the partition.
- **Encrypt just used parts of the drive**. When a drive is initially encrypted, either all the sectors (regardless of whether they contain data or not) or only those sectors that contain data, can be encrypted. Encrypting only those portions of the drive that are used is much faster in most of the cases. Select this option to encrypt only the currently used sectors during the initial encryption.

4. Select an encryption algorithm:

Algorithm	Description
Blowfish	A strong, fast, and compact algorithm that supports key lengths of up to 448 bits.
DESX	A widely used cryptosystem and uses a key length of up to 128 bits.
DES	A widely used cryptosystem and uses a key length of up to 56 bits.
AES	Provides the most effective protection using a 256-bit key. The AES (Advanced Encryption Standard) provides the highest security coupled with fast encryption speed. This algorithm is the optimal choice for most users.

5. Define a key length if the selected algorithm supports several key lengths. Use the slider to define the preferred key length for the selected algorithm. The key that will be generated out of the password will be of this length.
6. Generate a random key automatically or define a key password:

- With **generating random key** option, you do not have to enter an encryption password. The encryption key will be generated randomly when encryption takes place.
- With defining a **key password**, the encryption key will be generated from (but is not a copy of) the password you enter (and confirm) here. The encryption password should be different to the EgoSecure Full Disk Encryption administration password.

7. Click **Save**.

8. Right-click a computer where FDE is initialized.
9. Select **Encrypt | [disk letter]** from the context menu.

    → The dialog where you agree with a possible reboot of computer where encryption is performed appears.

10. Click **OK** to confirm.

    → The encryption starts: the entry in the FDE status column changes to **Executing script** and the icon 🔒 appears on a user side. When the user clicks this icon, the **EgoSecure FDE** dialog appears, where the encryption progress is shown. Once the disk is encrypted, the **Script executed successfully** status is displayed in **Console**.

11. Export and save the emergency recovery file to external storage or a network folder. For details, see How to export ERI?.

Improving encryption security

Enable an additional layer of security to the disk encryption key (DEK).
The HKEK option utilizes unique hardware-based information from the client to generate an additional hardware-based key encryption key (HKEK).
The TKEK option uses uses unique TPM information from the client for generating a TPM-based key encryption key (TKEK). Check TPM system requirements before enabling the option.
The options protect against moving the encrypted drive into another computer within the same network, where the same KEK is used.
You can use both options at a time for the protection.

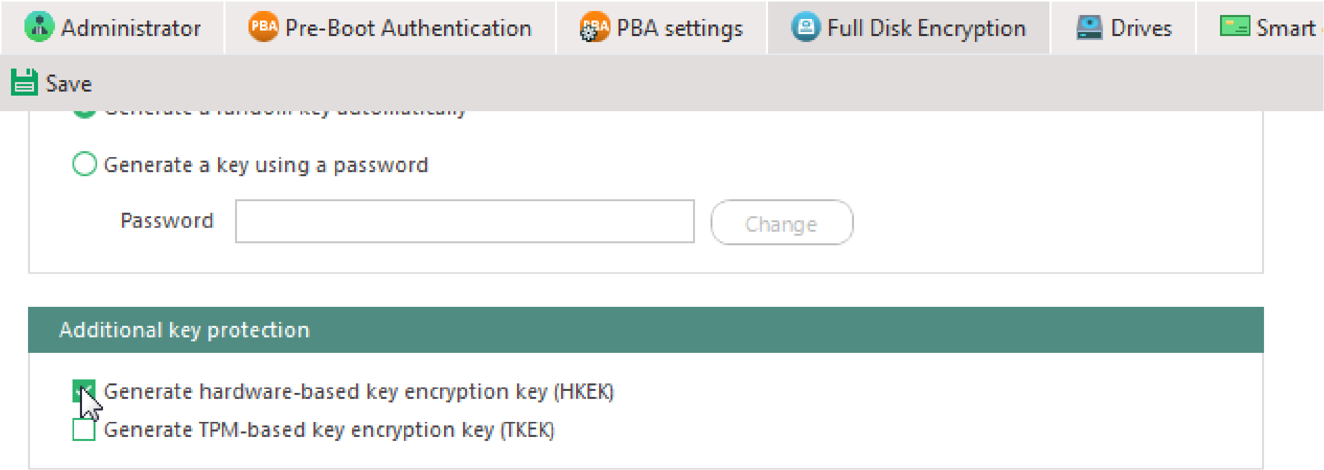
ATTENTION

Before updating BIOS or replacing hardware

- When updating BIOS or replacing hardware, the information used for key generation changes and disk recovery will no longer be possible. That is why, please, follow the steps below to avoid it:
    1. Decrypt the disk.
    2. Update BIOS or replace hardware.
    3. Encrypt the disk.

Improving security by enabling hardware-based key generation (compatible only with FDE 14.1 and higher)

1. Navigate to **Computer management | FDE**.
2. Select a computer.
3. In the lower work area, under **Full Disk Encryption** tab, enable the **Generate hardware-based key encryption key (HKEK)** option.



Administrator | Pre-Boot Authentication | PBA settings | Full Disk Encryption | Drives | Smart

Save

Generate a random key automatically

○ Generate a key using a password

Password [ ] Change

Additional key protection

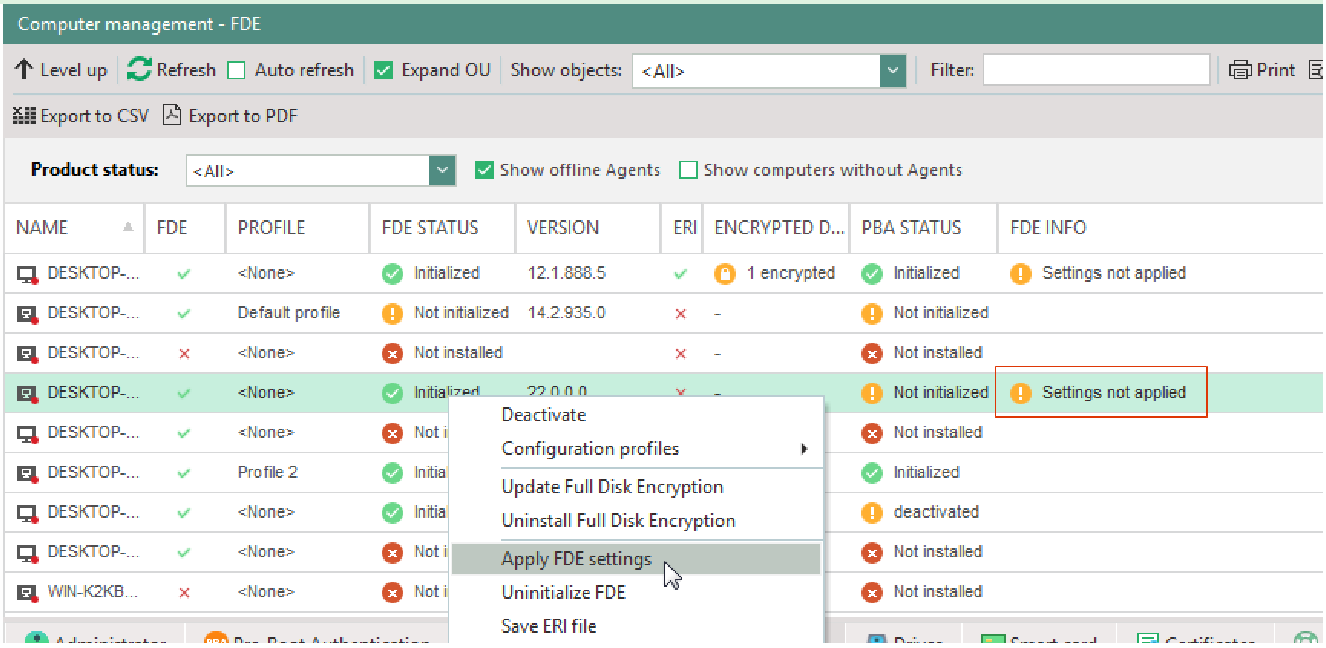
☑ Generate hardware-based key encryption key (HKEK)

□ Generate TPM-based key encryption key (TKEK)

4. Click **Save**.

   → In the **FDE info** column, the **Settings not applied** entry appears.

5. Right-click a computer and select **Apply FDE settings**.



Computer management - FDE

Level up | Refresh | □ Auto refresh | ☑ Expand OU | Show objects: <All> | Filter: | Print

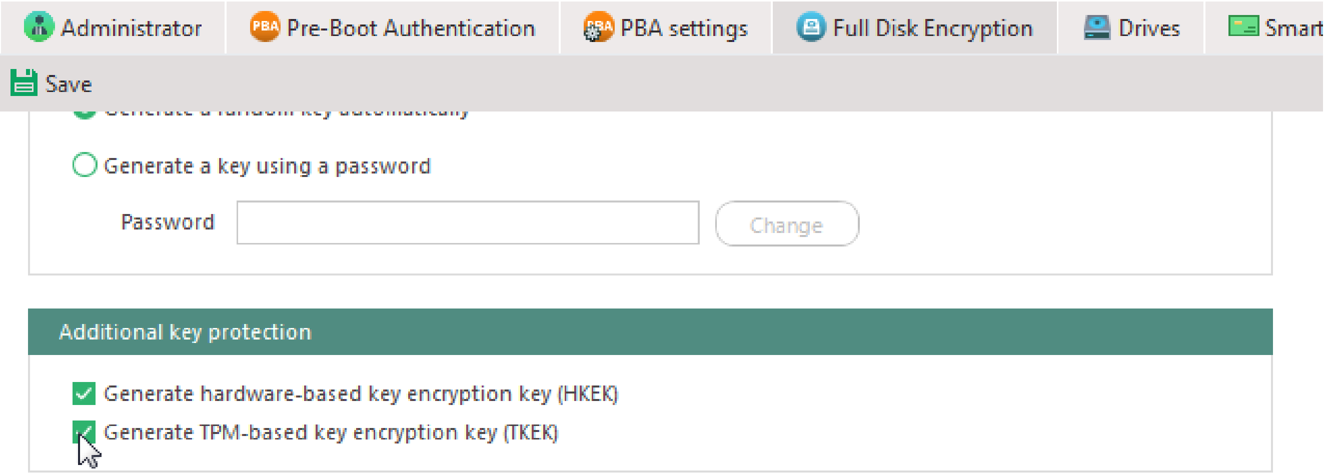
Export to CSV | Export to PDF

Product status: <All> ☑ Show offline Agents □ Show computers without Agents

NAME	FDE	PROFILE	FDE STATUS	VERSION	ERI	ENCRYPTED D...	PBA STATUS	FDE INFO
DESKTOP-...	✓	<None>	Initialized	12.1.888.5	✓	1 encrypted	Initialized	Settings not applied
DESKTOP-...	✓	Default profile	Not initialized	14.2.935.0	✕	-	Not initialized	
DESKTOP-...	✕	<None>	Not installed		✕	-	Not installed	
DESKTOP-...	✓	<None>	Initialized	22.0.0.0	✕	-	Not initialized	Settings not applied
DESKTOP-...	✓	<None>	Not i				Not installed	
DESKTOP-...	✓	Profile 2	Initia				Initialized	
DESKTOP-...	✓	<None>	Initia				deactivated	
DESKTOP-...	✓	<None>	Not i				Not installed	
WIN-K2KB...	✕	<None>	Not i				Not installed	

Improving security by enabling TPM key generation (compatible only with FDE 22.0.0 and higher)

1. Navigate to **Computer management | FDE**.
2. Select a computer.
3. In the lower work area, under **Full Disk Encryption** tab, enable the **Generate TPM-based key encryption key (TKEK)** option.



Generate a random key automatically

○ Generate a key using a password

Password

Additional key protection

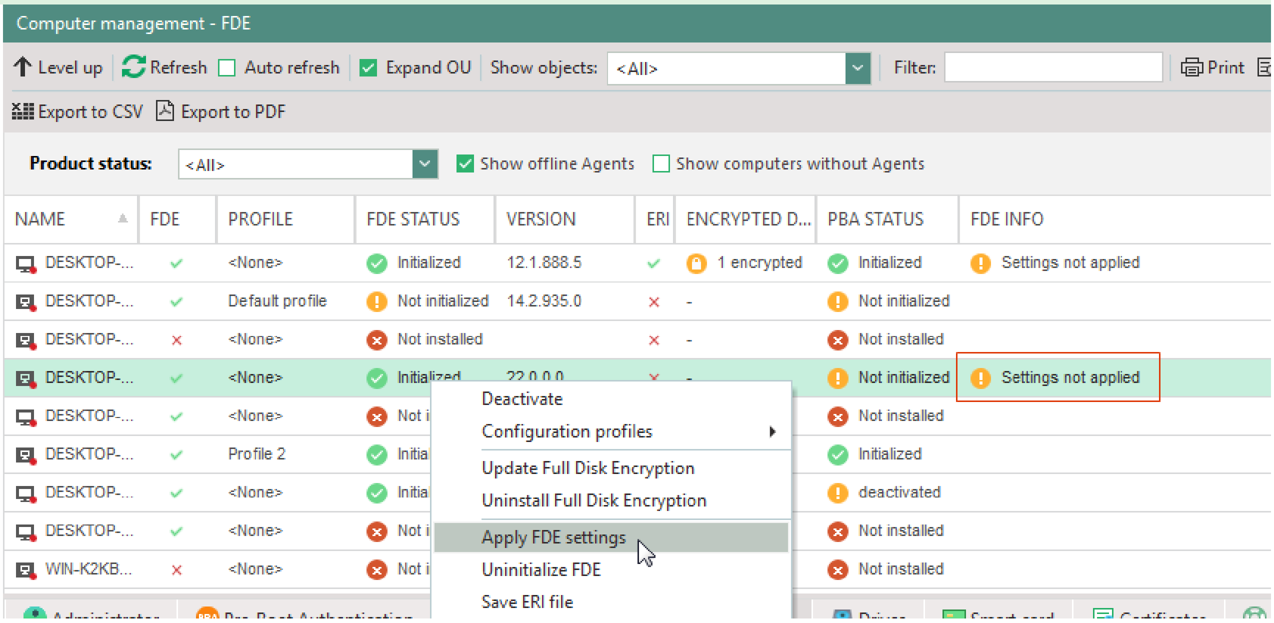
☑ Generate hardware-based key encryption key (HKEK)

☑ Generate TPM-based key encryption key (TKEK)

4. Click **Save**.

   → In the **FDE info** column, the **Settings not applied** entry appears.

5. Right-click a computer and select **Apply FDE settings**.



□ Auto refresh ☑ Expand OU Show objects: <All> Filter:

Product status: <All> ☑ Show offline Agents □ Show computers without Agents

NAME	FDE	PROFILE	FDE STATUS	VERSION	ERI	ENCRYPTED D...	PBA STATUS	FDE INFO
DESKTOP-...	✓	<None>	Initialized	12.1.888.5	✓	1 encrypted	Initialized	Settings not applied
DESKTOP-...	✓	Default profile	Not initialized	14.2.935.0	✕	-	Not initialized	
DESKTOP-...	✕	<None>	Not installed		✕	-	Not installed	
DESKTOP-...	✓	<None>	Initialized	22.0.0.0	✕	-	Not initialized	Settings not applied
DESKTOP-...	✓	<None>	Not i				Not installed	
DESKTOP-...	✓	Profile 2	Initia				Initialized	
DESKTOP-...	✓	<None>	Initia				deactivated	
DESKTOP-...	✓	<None>	Not i				Not installed	
WIN-K2KB...	✕	<None>	Not i				Not installed	

f

18. APPENDIX

18.1. DLP – syntax of lexical expressions

You can use simple expressions, predefined and user-defined regular expressions to define search patterns in DLP. These expressions can be connected to each other by operators.

Simple expressions

A simple expression searches exactly for the entered string. Any number of other characters can appear before or after the character string, but no letters, otherwise the expression will no longer find it.

For example, the simple expression **credit** is found or not found in the following strings:

String	"Credit" will be found?
Credit xy	Yes
Credit!	Yes
Credit,	Yes
Creditcard	No
Creditcardnumber	No

User-defined expressions

User-defined expressions are regular expressions that you can create in the editor and save for using later. The following sections tell you what syntax you need to use to define regular expressions.

Syntax for regular expressions

Use the **.PERL.** expression operator with a keyword or phrase to indicate a regular expression:

.PERL.regular_expression

Operators

You can insert operators in the **Expression editor** using the buttons and don't have to enter them manually. With operators, you can link several strings together. E.g.:

.PERL.regular_Expression1.AND.regular_Expression2
.PERL.regular_Expression1.OR.regular_Expression2

The following operators are available:

Operator	Description
AND	Both keywords or phrases must be present.
OR	One or both keywords or phrases must be present.
XOR	One or the other keyword or phrase must be present but not both.
BEFORE	Both keywords or phrases must be present and the keyword or phrase that precedes the operator must occur before the keyword or phrase that follows the operator.
AFTER	Both keywords or phrases must be present and the keyword or phrase that precedes the operator must occur after the keyword or phrase that follows the operator.
FOLLOWED BY	Both keywords or phrases must be present and the keyword or phrase that follows the operator must be within x words of the one that precedes the operator.
NEAR	Both keywords or phrases must be present and they must be within ten words of one another. The expressions may occur in either order.
ANDNOT	The keyword or phrase that precedes the operator must be present and the keyword or phrase that follows the operator must not be present.

Symbols

With certain placeholders, you can define any single character or combine several characters into sub-expressions within a character string:

Character	Description	Example
.	Any single character except line breaks.	.name. matches "1name!", " name@", "nnamee" but not "name"
()	Subexpression, substring.	**(ab)+** matches ab, abab, …
|	Or operator. Matches either the expression preceding or succeeding the operator	a|b matches either "a" or "b".

Anchor characters

Anchor characters indicate a character or a string to appear at the beginning or end of the search string:

Character	Description	Example
^	Matches the start of a line. Returns all strings, which start with the expression after ^expression.	**^Beginning** finds all strings where line starts with "Beginning"
$	Matches the end of a line.	**End$** finds all strings that end with "Ende"

Character sets

A set of characters specifies a predefined selection of characters and is enclosed in square brackets. To negate a set, insert the ^ character before the string.

Character	Description	Example
[ac]	a or c	**1[ac]** finds 1a or 1c, but not 1b
[a-c]	a or b or c	**1[a-c]** finds 1a, 1b or 1c
[14]	1 or 4	**[14]a** finds 1a or 4a, but not 2a or 3a
[1-4]	1 or 2 or 3 or 4	**[1-4]a** finds 1a, 2a, 3a or 4a
[^1-4]	not 1, 2, 3 or 4	**[^1-4]a** finds 5a, 6a, …, bit not 1a, 2a, 3a or 4a
[a-zA-Z]	All upper- and lowercase letters from A-Z	**1[a-zA-Z]** finds 1a, 1b, 1c, … and also 1A, 1B, 1C, …

Character classes

Character classes define the type of characters, which are searched (digits, letters, special characters or spaces).

Character class	Description	Example
\d	Finds only digits.	0, 1, … 9
\D	Finds all characters except digits.	A, B, … Z, @, €, …
\l	Finds all lowercase characters in case sensitive expressions that have uppercase / lowercase letters. When used in a case-insensitive expression, this character set will also match uppercase characters.	a, b, … z
\L	Finds all characters that are not lowercase in expressions, which are case sensitive.	A, B, … Z, 0, 1, … 9, @, €, …
\s	Finds only whitespace characters (spaces, tabs, line breaks).	
\S	Finds all characters that is not whitespace.	A, B, … Z, 0, 1, … 9, @, €, …
\u	Finds all uppercase letters in expressions that are case sensitive.	A, B, … Z
\U	Finds all characters that are not uppercase in expressions which are case-sensitive.	a, b, … z, 0, 1, … 9, @, €, …
\w	Finds only digits or letters.	A, B, … Z, 0, 1, … 9

\W	Finds all characters except digits or letters.	@, €, …

Quantifiers

Quantifiers indicate how often certain characters occur in a string. Digits are places in brackets after an atom or expression.

Quantifiers	Description	Example
*	Zero or more occurrences of the preceding atom	**Zo*** finds Z, Zo, Zoo, …
+	One or more occurrences of the preceding atom	**Zo+** finds Zo, Zoo, …
?	Zero or one occurrence of the preceding atom	**Zo?** finds Z and Zo

Quantifiers can also specify precisely how many times a character or a string may appear:

Quantifiers	Description	Example
X{n}	Bounded repeat. Matches exactly 'x' occurrences of the preceding atom.	**A{5}** finds AAAAA
X{n,m}	Matches between 'x' and 'y' (inclusive) occurrences of the preceding atom.	**A{1,5}** finds A, AA, AAA, AAAA, AAAAA
X{n,}	Matches 'x' or more (inclusive) occurrences of the preceding atom	**A{5,}** finds AAAAA, AAAAAA, …

Usually quantifiers are greedy, which means they try to find as many characters as possible. This behavior changes from greedy to hesitant when following the quantifier with a question mark.
The greedy quantifier searches in a string from left to right and stops only at the first character, where the condition of the search pattern is no longer satisfied. It searches until the pattern matches and provides a minimal search result.
The hesitant quantifier looks in a string from left to right and stops at the first character where the condition of the search pattern is met. It searches as long as the pattern matches and returns a maximum search result.
Which quantifier to use depends on the result to be achieved.
Quantifiers can also specify how often a character or string is allowed to occur.

Example 1: The search pattern or the regular expression in the first example starts with the characters A, B or C, which can appear 1-n times. These characters can be followed by 0-n of any characters. The characters A, B or C are to be output (the contents in the round brackets in the regular expression).

Text	Regular expression with greedy quantifier	Result with greedy quantifier	Regular expression with hesitant quantifier	Result with hesitant quantifier
ACBAXXACA	([A-C]+).*	ACBA	([A-C]+?).*	A
015A63	([0-9]+).*	015	([0-9]+?).*	0

- *The greedy quantifier* outputs as many characters as possible and stops only at the character X, which no longer satisfies the condition.
- *The hesitant quantifier* outputs as many characters as necessary and stops after the character A satisfying the condition.

Example 2:
The use of multiple quantifiers in an expression can sometimes lead to incorrect results. In the following example, the first numeric value after the M is to be read out of the character string M 14x52:

String	Regular expression with greedy quantifier	Result with greedy quantifier	Regular expression with hesitant quantifier	Result with hesitant quantifier
M 14x52	.*([0-9]+)x.*	4	.*?([0-9]+)x.*	14

The number you look for consists of 1-n digits between 0 and 9: [0-9] +
In front of the number you are looking for, there is any number of characters in any quantity: .*
The number you look for is followed by an x and any other characters: x.*
This first quantifier at the beginning of the regular expression now searches for as many characters as possible, which results that the first digit of the searched number is included in its search result. When adding a hesitant quantifier at the beginning, only the most necessary characters appear in the search result and the next quantifier fully reads the searched numerical value.

Masks

Predefined characters, such as brackets, can be recognized as normal characters if the backslash is set before them. The backslash symbol \ turns a predefined character into a normal character and a normal character into a special character (e.g. \s searches for a whitespace character). For details, see Character classes
To search for a character that represents a predefined character within regular expressions, add a backslash before the character:

String	Searches for
\\	Backslash \
\t	Tabulator

\{	An opened curly brace {

18.2. EgoSecure Antivirus default exclusions

```
C:\Windows\SoftwareDistribution\Datastore\tmp.edb
C:\Windows\SoftwareDistribution\Datastore\DataStore.edb
C:\Windows\SoftwareDistribution\Datastore\Logs\Res*.log
C:\Windows\SoftwareDistribution\Datastore\Logs\Edb*.jrs
C:\Windows\SoftwareDistribution\Datastore\Logs\Edb.chk
C:\Windows\SoftwareDistribution\Datastore\Logs\Tmp.edb
C:\Windows\Security\Database\*.edb
C:\Windows\Security\Database\*.sdb
C:\Windows\Security\Database\*.log
C:\Windows\Security\Database\*.chk
C:\Windows\Security\Database\*.jrs
C:\Windows\System32\GroupPolicy\Registry.pol
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\*.*
C:\ProgramData\NTUser.pol
C:\Windows\Ntds\Ntds.dit
C:\Windows\Ntds\Ntds.pat
C:\Windows\Ntds\EDB*.log
C:\Windows\Ntds\Res*.log
C:\Windows\Ntds\Edb*.jrs
C:\Windows\Ntfrs\jet\sys\*.*
C:\Windows\Ntfrs\jet\*.*
C:\Windows\Ntfrs\jet\log\*.*
C:\Windows\Ntfrs\Edb*.log
C:\Windows\Ntfrs\FRS\Jet\Log\Edb*.jrs
C:\Windows\Sysvol\Staging areas\Nntfrs_cmp*.*
C:\Windows\Sysvol\Domain\*.adm
C:\Windows\Sysvol\Domain\*.admx
C:\Windows\Sysvol\Domain\*.adml
C:\Windows\Sysvol\Domain\Registry.pol
C:\Windows\Sysvol\Domain\*.aas
C:\Windows\Sysvol\Domain\*.inf
C:\Windows\Sysvol\Domain\Fdeploy.inf
C:\Windows\Sysvol\Domain\Scripts.ini
C:\Windows\Sysvol\Domain\*.ins
C:\Windows\Sysvol\Domain\Oscfilter.ini
C:\Windows\Ntfrs\DO_NOT_REMOVE_NtFrs_PreInstall_Directory\Ntfrs*.*
C:\Windows\Ntfrs\DO_NOT_REMOVE_NtFrs_PreInstall_Directory\*\Ntfrs*.*
C:\System Volume Information\DFSR\$db_normal$
C:\System Volume Information\DFSR\FileIDTable_*
C:\System Volume Information\DFSR\SimilarityTable_*
```

C:\System Volume Information\DFSR\*.xml
C:\System Volume Information\DFSR\db_dirty
C:\System Volume Information\DFSR\db_lost
C:\System Volume Information\DFSR\Dfsr.db
C:\System Volume Information\DFSR\Fsr.chk
C:\System Volume Information\DFSR\*.frx
C:\System Volume Information\DFSR\*.log
C:\System Volume Information\DFSR\Fsr*.jrs
C:\System Volume Information\DFSR\Tmp.edb
C:\System Volume Information\DFSR\*\db_normal
C:\System Volume Information\DFSR\*\FileIDTable_*
C:\System Volume Information\DFSR\*\SimilarityTable_*
C:\System Volume Information\DFSR\**.xml
C:\System Volume Information\DFSR\*\db_dirty
C:\System Volume Information\DFSR\*\db_lost
C:\System Volume Information\DFSR\*\Dfsr.db
C:\System Volume Information\DFSR\*\Fsr.chk
C:\System Volume Information\DFSR\**.frx
C:\System Volume Information\DFSR\**.log
C:\System Volume Information\DFSR\*\Fsr*.jrs
C:\System Volume Information\DFSR\*\Tmp.edb
C:\System Volume Information\tracking.log
C:System32\DHCP\*.mdb
C:System32\DHCP\*.pat
C:System32\DHCP\*.log
C:System32\DHCP\*.chk
C:System32\DHCP\*.edb
C:System32\DHCP\**.mdb
C:System32\DHCP\**.pat
C:System32\DHCP\**.log
C:System32\DHCP\**.chk
C:System32\DHCP\**.edb
C:System32\Dns\*.log
C:System32\Dns\*.dns
C:System32\Dns\BOOT
C:System32\Dns\**.log
C:System32\Dns\**.dns
C:System32\Dns\*\BOOT
C:System32\Wins\*.chk
C:System32\Wins\*.logF
C:System32\Wins\*.mdb
C:System32\Wins\**.chk
C:System32\Wins\**.log
C:System32\Wins\**.mdb

18.3. Supported Ethernet manufacturers for Friendly Network

3Com devices
Adaptec devices
Agere devices
Alteon devices
Altera Triple-Speed Ethernet MAC devices
AMD devices
ARC devices
Atheros devices
Aurora VLSI devices
Beckhoff CX5020 EtherCAT master devices
Broadcom devices
Cadence devices
Cavium ethernet drivers Chelsio devices
Cisco devices
Dave ethernet (DNET) devices
Digital Equipment devices
D-Link devices
Emulex devices
Exar devices
EZchip devices
Fujitsu devices
HP devices
Intel devices
JMicron® PCI-Express Gigabit Ethernet devices
Marvell devices
Mellanox devices
Micrel devices
Myricom devices
Myson MTD-8xx PCI Ethernet devices
National Semi-conductor devices
Netronome® devices
NVIDIA devices
OKI Semiconductor devices
OpenCores 10/100 Mbps Ethernet MAC devices
Packet Engine devices
QLogic BR-series devices
QLogic devices
Qualcomm devices
RDC devices
Realtek devices
Renesas devices
Rocker devices
Samsung Ethernet devices

SEEQ devices
Silan devices
Silicon Integrated Systems (SiS) devices
SMC (SMSC)/Western Digital devices
Solarflare SFC4000/SFC9000/SFC9100-family devices
STMicroelectronics devices
Sun devices
Synopsys devices
Tehuti devices
Texas Instruments (TI) devices
VIA devices
WIZnet devices
Xircom devices

18.4. XML import format

You can import the user and computer management settings via XML (**Access Control** access rights, product activation). To import, define the respective rights externally in an XML file and import the file to the **Console**. For details, see: Importing settings via XML file

XML file format for importing access rights

The basic structure of the XML files with which you can import settings is as follows:

```
<?xml version="1.0"?>
<xml>
            <header></header>
            <body>
             <schema>1</schema>
            </body>
</xml>
```

Below the `<schema>` element (inside the `<body>`), define the access rights or the settings for the product activation that you want to import.

Definition of access rights

The access rights for **Access Control** occurs on several levels. First determine the device or port for which to apply the rights, and then assign rights for this device to specific users and/or computers.
Example: An XML file for assigning the access rights looks as follows:

```
<?xml version="1.0"?>
<xml>
```

```
            <header></header>
            <body>
             <schema>1</schema>
             <DC id="7" name="Bluetooth">
                 <SD prf="0">
                     <ACE
guid="d0acaf5d1e474b3cb047f313ba2c5e60" ar="0"></ACE>
                 </SD>
             </DC>
            </body>
</xml>
```

First of all, the device or port for which rights are to be assigned is addressed (in example: via the `<DC>` element (device class) with the `id="7"` (Bluetooth)). After that, a security descriptor (element `<SD>`) is used that contains the entries for the access rights (element `<ACE>`). The `<SD>` element contains the attribute `prf="0"`, which specifies the access rights for online profile of the device. The `<ACE>` element contains the attribute `guid`, which specifies the default rights for new user, computer or unknown user to whom the rights of this element to apply. In the example, the value `guid="d0acaf5d1e474b3cb047f313ba2c5e60"` assigns the default rights to all new computers. The `<ACE>` element also has the attribute `ar="0"`. This attribute specifies the actual access rights of the user/computer for the respective device. The value 0 stands for no access.

To see all elements and attributes for the definition of access rights, click on Elements and attributes.

Definition of product activations

In addition to defining access rights, you can also use XML to activate products for specific users and/or computers. The example code for this looks as follows:

```
<?xml version="1.0"?>
<xml>
            <header></header>
            <body>
             <schema>1</schema>
             <ACCNT name="PC-NAME" addons="256"></ACCNT>
            </body>
</xml>
```

The settings for the product activation are defined in the `<ACCNT>` element. Specify the directory service object for which to activate the products (in the example, the corresponding computer is addressed via the attribute `name = "PC-NAME"`) and then enter a value in the `addons` attribute that corresponds to the products to be activated

(in the example, the value 256 stands for the **Green IT** product). You can also store a number of optional settings via attributes in the <ACCNT> element.
To see all elements and attributes for the definition of product activation, click on Elements and attributes.

Elements and attributes

Elements for device definition

To define access rights for a device or a port, define them via the corresponding element. Depending on the device and application, the following elements are available:

Element	Description	Attribute
DP (device port)	Defines access rights for a specific port type. You can find the available port types under **User management | Control** or **Computer management | Control**.	- type: ID for identifying the port type (for details, see: Available port types and device classes) - name (optional): port name; used for identifying if no type is specified
DC (device class)	Defines access rights for a specific device type. You can find the available device types under **User management | Control** or **Computer management | Control**.	- id: ID for identifying the device class (for details, see: Available port types and device classes) - name (optional): name of the device class; used for identifying if no id is specified
DM (device model)	Adds certain device groups under **Permitted devices | Permitted device models** to the whitelist.	- hwid: Windows hardware identifier of a device. Add symbols * and ? to use this field as a mask. - cert: is device certified (whitelist), can have value 1 - port (optional): device port - class (optional): device class - name (optional): device group name
DN (device node)	Adds individual devices under Permitted devices | Individual device permissions to the whitelist.	- Instance id: Windows device instance unique identifier (hardware id + serial number) - name: device name - port (optional): device port - class (optional): device class

Available port types and device classes

To address a device or a port via the elements `<DC>` / `<DP>`, the attribute `id` (for device classes) or `type` (for port types) must be assigned to it. The individual device classes and port types have certain IDs, which can be used to assign them during import. The following tables give an overview of the values of the `type` and `id` attributes that you must assign to the respective elements:

Port type (<DP>)	Type
Parallel port	3
Serial port	4
FireWire	9
PCMCIA	10
USB (without keyboards, mouses…)	14
Thunderbolt	29

Device class (<DC>)	ID
Unknown	0
CD / DVD	1
Floppy disk	2
External storage	5
Infrared	6
Bluetooth	7
WiFi	8
Scanners	11
TV Tuner	12
Local printers	13
Portable devices (Android, PDA, Windows Mobile, MTP- & PTP-Devices)	15
Blackberry	16
Modem	17
ISDN cards	18
Sound, video and game controllers	19
Fixed disk	20
Thin client storage	21
Network share	22
Apple (iPhone, iPad etc.)	23

Smart card readers	24
USB network adapter	27
Cameras	28
NFC	30

Elements for defining access rights

Element	Description	Attribute
SD (security descriptor)	Container for the access rights of a device/port; contains one or more ACE elements.	■ prf: defines whether the rights apply to online (value 0) or offline (value 1) profile
ACE (access control entry)	Contains the access rights for a specific directory service object or default rights for new/unknown users or computers.	■ sid: Windows SID (security identifier). ■ guid: unique object identifier from Active Directory (guid is not used when importing permitted device models and individual device permissions, use object sid or name instead). ■ name: Fully Qualified Host Name of the directory service objects (used only if there is no sid/guid attribute) ■ ar: access rights; see the next table ■ host (optional): computer on which the rights apply to specific user/group ■ del (optional): Value 1 to remove the corresponding access rights entry (e.g. from a whitelist).

The values for the `ar` attribute within an `<ACE>` element define the respective access rights. The attributes for the different access types are the following:

Access right	Attribute
No access	`ar="0"`
Read access	`ar="1"`
Print access (only printers)	`ar="1"`

Playback access (only Sound, video and game controllers)	ar="1"
Block virtual adapters (only Bluetooth)	ar="1"
Write access	ar="2"
Full access	ar="3"
Not controlled	ar="8"

The attributes guid or sid within an <ACE> element can not only be used to address individual users or computers, but also all objects in the directory using special, predefined values. In addition, default rights for new users/computers in the directory or for unknown users can also be defined in this way. The attributes and values for this are the following:

Description	Attribute
All computer/user (used when adding devices under Permitted devices | Permitted device models and under Permitted devices | Individual device permissions)	sid="S-1-1-0"
Default rights for new user	guid="9a20eff0a9d74646aa1ccc4d91354b31"
Default rights for new computer	guid="d0acaf5d1e474b3cb047f313ba2c5e60"
Default rights for unknown user	guid="4f691245707843EC91aace235478c647"

Elements for activating products

To activate products for certain users and / or computers, use the <ACCNT> element. Make all the settings using attributes within this element.

Element	Description	Attribute
ACCNT	Contains the settings for activating products for a specific directory object.	■ sid: ID assigned by Windows (for users and groups) ■ name: object name (for computer) ■ addons: sum of numbers in decimal format, showing which products to activate. See the table below for details

		■ other option settings; see optional attributes for <ACCNT> elements

To determine the correct value of the addons attribute, add the values for all products that you want to activate from the following table:

Product	Value for addon attribute
Secure Audit	1
Removable Device Encryption	2
Shadowcopy	4
Cloud Storage Encryption	8
Application Control	16
Local Folder Encryption	32
Full Disk Encryption	64
Access Control	128
Green IT	256
Secure Erase	512
BitLocker Management	1024
EgoSecure Antivirus	2048
MDM	4096
Insight Analysis	8192
Inventory	16384
Network Share Encryption	32768
Permanent Encryption	65536
Password Manager	131072
IntellAct Automation	262144
DLP Data in Use	1048576
DLP Data at Rest	2097152

Optional attributes for <ACCNT> elements

In addition to the addons attribute, you can also assign other optional attributes to the <ACCNT> element that define certain settings for clients and users. For each of these attributes, you can assign a value of **1** to activate the respective option or a value of **0** to deactivate it. You can also assign the value **inherit**, which has the priority over values **0** and **1** within one section.

E.g.: `allowThinClientControl="1" allowHddFullControl="inherit"` results in enabling the inheritance for the section **Computer management | Settings | Client settings**.

Setting type	Attribute
Client settings	allowPrinterControl allowNetworkSharesControl allowThinClientControl allowHddFullControl denyLowLevelDiskAccess denyStorageExecuteAccess restrictKbdAccess restrictMouseAccess checkAccountExpiration agentWindowsLog agentSyslog enablePRESENSE autoKbdRegister agentPollingMode (0 – disable, 1 – enable, 2 – auto)
User settings	disableFileDownloads disableClipboard allowAdditionalKeyboards askAccessByEachConnection archivesScanning officeFilesScanning

Examples

- Setting user access rights for three device classes
- Setting default user rights for three device classes
- Setting user and computer access rights for device port
- Setting computer access rights for two device ports and two device classes
- Adding two device models of different device classes into whitelist
- Adding an external storage device in Console under Permitted devices | Individual device permissions for user and computer with readonly right
- Adding an external storage device in Console globally under Permitted devices | Individual device permissions
- Removing one user from CD security descriptor in Console under Permitted devices | Individual device permissions
- Activating products 'Access Control' and 'Secure Audit' for the user with SID="S-1-5-21-760337890-188976374-1171351706-1000"
- Activating 'Access Control' for the computer with Name="PC-NAME"

- Activating network shares control, printer control and disable hard drive full control for default rights
- Restricting access to one keyboard and allow printer control for computer with Name = "PC-NAME"
- Enabling the inheritance of settings for computer with Name = "PC-NAME"
- Disabling file downloads and clipboard for user with Sid = "S-1-5-21-2024135453-3835937584-2321026569-1000"

Setting user access rights for three device classes

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DC Id="1" Name="CD / DVD">
            <SD>
                  <ACE sid="S-1-5-21-3757206099-4223034928-3177353085-1003"
ar="0"></ACE>
            </SD>
            </DC>
            <DC Id="5" Name="External Storage">
            <SD>
                  <ACE sid="S-1-5-21-3757206099-4223034928-3177353085-1003"
ar="1"></ACE>
            </SD>
            </DC>
            <DC Id="8" Name="WiFi">
            <SD>
                  <ACE sid="S-1-5-21-3757206099-4223034928-3177353085-1003"
ar="3"></ACE>
            </SD>
            </DC>
      </Body>
</Xml>
```

Setting default user rights for three device classes

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DC Id="1" Name="CD / DVD">
            <SD>
                  <ACE GUID="9a20eff0a9d74646aa1ccc4d91354b31" ar="0"></ACE>
            </SD>
            </DC>
            <DC Id="5" Name="External Storage">
            <SD>
                  <ACE GUID="9a20eff0a9d74646aa1ccc4d91354b31" ar="1"></ACE>
            </SD>
            </DC>
            <DC Id="8" Name="WiFi">
            <SD>
```

```
                  <ACE GUID="9a20eff0a9d74646aa1ccc4d91354b31" ar="3"></ACE>
            </SD>
            </DC>
      </Body>
</Xml>
```

Setting user and computer access rights for device port

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DP Type="14" Name="USB">
            <SD>
                  <ACE host="computer.damain.in" sid="S-1-5-21-3757206099-
4223034928-3177353085-1003" ar="3"></ACE>
            </SD>
            </DP>
      </Body>
</Xml>
```

Setting computer access rights for two device ports and two device classes

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DP Type="9" Name="FireWire">
            <SD>
                  <ACE host="hostname.domain.at" ar="0"></ACE>
            </SD>
            </DP>
            <DP Type="10" Name="PCMCIA">
            <SD>
                  <ACE host="hostname.domain.at" ar="3"></ACE>
            </SD>
            </DP>
            <DC Id="7" Name="Bluetooth">
            <SD>
                  <ACE host="hostname.domain.at" ar="0"></ACE>
            </SD>
            </DC>
            <DC Id="8" Name="WiFi">
            <SD>
                  <ACE host="hostname.domain.at" ar="3"></ACE>
            </SD>
            </DC>
      </Body>
</Xml>
```

Adding two device models of different device classes into whitelist

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DM Class="1" Cert="1" HwId="IDE\\CDROMLITE-ON_DVDRW_SHM-
165P6S________________MS0F____"></DM>
            <DM Port="14" Class="5" Cert="1" HwId="USB\\VID_0835&PID_0835"></DM>
      </Body>
</Xml>
```

Adding an external storage device into Console under Permitted devices | Individual device permissions for user and computer with readonly right

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DN Port="14" Class="5"
InstanceId="USB\\VID_08EC&PID_0020\\0DE0F8613363AA02&0" Name="Intuix U3 USB
Device">
            <SD>
                  <ACE host="comp1" sid="S-1-5-21-3757206099-4223034928-
3177353085-1003" ar="1"></ACE>
            </SD>
            </DN>
      </Body>
</Xml>
```

Adding an external storage device in Console globally under Permitted devices | Individual device permissions

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DN Port="14" Class="15"
InstanceId="USB\\VID_0BB4&PID_0BCE\\5&1C5E86F8&0&1" Name="Windows Mobile-based
Device">
            <SD>
                  <ACE sid="S-1-1-0" ar="3"></ACE>
            </SD>
            </DN>
      </Body>
</Xml>
```

Removing one user from CD security descriptor in Console under Permitted devices | Individual device permissions

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
            <DN InstanceId="IDE\\CDROMLITE-ON_DVDRW_SHW-
16H5S_________________LS0N____\\5&23126E32&0&0.1.0" Name="LITE-ON DVDRW SHW-
16H5S">
            <SD>
```

```
                  <ACE Del="1" sid="S-1-5-21-3757206099-4223034928-3177353085-
1003"></ACE>
            </SD>
            </DN>
      </Body>
</Xml>
```

Activating products 'Access Control' and 'Secure Audit' for the user with SID="S-1-5-21-760337890-188976374-1171351706-1000"

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Sid="S-1-5-21-760337890-188976374-1171351706-1000"
Addons="129"></ACCNT>
      </Body>
</Xml>
```

Activating 'Access Control' for the computer with Name="PC-NAME"

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Name="PC-NAME" Addons="128"></ACCNT>
      </Body>
</Xml>
```

Activating network shares control, printer control and disable the control of hard disks like external media for *default rights*.

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Guid = "d0acaf5d1e474b3cb047f313ba2c5e60">
                  <ClientSettings allowNetworkSharesControl="1"
allowHddFullControl="0" allowPrinterControl="1">
                  </ClientSettings>
                  </ACCNT>
      </Body>
</Xml>
```

Restricting access to one keyboard and allow printer control for computer with Name = “PC-NAME”

```
<?xml version="1.0"?>
<Xml>
```

```
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Name = "PC-NAME" >
                  <ClientSettings restrictKbdAccess="1" allowPrinterControl="1">
                  </ClientSettings>
                  </ACCNT>
      </Body>
</Xml>
```

Enabling the inheritance of settings for computer with Name = “PC-NAME”

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Name = "PC-NAME" >
                  <ClientSettings inheritSettings="1" >
                  </ClientSettings>
                  </ACCNT>
      </Body>
</Xml>
```

Disabling file downloads and clipboard for user with Sid = "S-1-5-21-2024135453-3835937584-2321026569-1000"

```
<?xml version="1.0"?>
<Xml>
      <Header></Header>
      <Body>
            <Schema>1</Schema>
                  <ACCNT Sid = "S-1-5-21-2024135453-3835937584-2321026569-1000">
                  <UserSettings disableFileDownloads="1" disableClipboard="1">
                  </UserSettings>
                  </ACCNT>
      </Body>
</Xml>
```