



EGOSECURE DATA PROTECTION

Quick Start Guide

Version 23.0.3

Updated: January 2024

Matrix42 GmbH
Elbinger Street 7
60487 Frankfurt am Main

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

CONTENTS

1. Starting Console	4
1.1. Authenticating	4
1.2. Creating a supervisor if not created during installation	5
1.3. Activating a license	6
1.4. Console areas overview	7
2. Performing AD- / NDS- / LDAP- synchronization	8
2.1. Specifying connection settings	8
2.2. Setting up synchronization	10
2.3. Performing synchronization	12
3. Defining administrators	13
3.1. Creating administrators or super administrators in Console	14
3.2. Granting administrative (super administrative) privileges to users from directory service	15
3.3. Creating and assigning administrative roles	16
4. Managing tenants	20
4.1. Creating a tenant	20
4.2. Assigning a tenant to an administrator or a super administrator	22
4.3. Switching between tenants	22
5. Installing EgoSecure Agents	24
5.1. Adjusting Windows settings	25
5.2. Adjusting client settings	26
5.3. Generating an MSI package	27
5.4. Installing EgoSecure Agents via Console	28
6. Activating products	30
6.1. Activating products for computers	31
6.2. Activating products for users	32
7. Configuring default rights	32
7.1. Customizing settings for users	36
7.2. Customizing permissions for computer	39

8. Managing user groups

40

1. STARTING CONSOLE

- 1.1. Authenticating
- 1.2. Creating a supervisor
- 1.3. Activating a license
- 1.4. Console areas overview

1.1. Authenticating

1. Click the **EgoSecureConsole.exe** file or its shortcut on the desktop.

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

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. Leave the **Login** and **Password** fields as is if a supervisor password has not been specified during the Server installation.
The fields are available for editing, because in this step the program doesn't check,

whether the specified server contains administrators, super administrators or supervisors in its database.

- 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**.

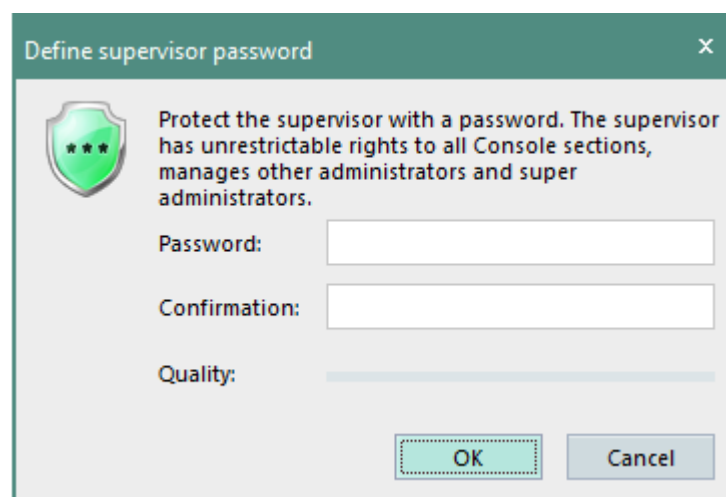
5. Click **OK** to continue.

- The **Define supervisor password** dialog appears if a supervisor password has not been specified during the Server installation (see chapter 1.2 for further steps).

1.2. Creating a supervisor if not created during installation

Once you have connected to the Server, the dialog for defining a supervisor password appears if the supervisor without a password has been created during the EgoSecure Server installation.

Supervisor has all permissions to Console, which can not be restricted. Supervisor password can be defined or edited later in **Administration | Administrators & scopes**.

A screenshot of a dialog box titled "Define supervisor password" with a close button (X) in the top right corner. On the left is a green shield icon with three stars. The main text reads: "Protect the supervisor with a password. The supervisor has unrestrictable rights to all Console sections, manages other administrators and super administrators." Below this text are three input fields: "Password:" (a text box), "Confirmation:" (a text box), and "Quality:" (a progress bar). At the bottom right are two buttons: "OK" (highlighted with a dashed border) and "Cancel".

Creating a password-protected supervisor

1. Define a password and confirm it.
2. Click **OK**.

- The supervisor protected with a password is created. This password is used each time when logging in to the **EgoSecure Data Protection Console**. Note down this password, because it is not saved to the EgoSecure database and cannot be restored if you forget it.



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](#)).

Creating a supervisor with no password protection

1. Leave the **Password** and **Confirmation** fields blank.
2. Click **OK**. Supervisor password can be defined later in **Administration | Administrators & scopes**.

➡ The supervisor without a password protection is created.



ATTENTION

No password protection

With no supervisor password the console authentication is available for every person. It makes the company data vulnerable and allows to take control over Agents.

1.3. Activating a license

Once you have created the supervisor, the dialog for activation product licenses appears. You can change the license information after the first activation in **Administration | Licenses | License management**.

EgoSecure Data Protection - product activation

☐ License file
☒ Activation code

User name:

E-mail:

Organization:

Code:

Products:

☐ Use proxy server

1. If you bought licenses, upload a license file or enter an activation code.
2. If you want to test the EgoSecure trial version for 30 days, leave the **Activation code** field with the predefined activation code.

For details about licensing, see the article [Activating product licenses](#).

3. Click **OK**.

➤ You have activated the product licenses. The EgoSecure Data Protection Console opens. Depending on the scope of the license, different products and functions are available to you.

1.4. Console areas overview

Console is divided into three main areas:

Navigation pane

Work area

Directory service structure

The screenshot shows the EgoSecure Data Protection by Matrix42 console. The interface is divided into three main areas:

- Navigation pane (3):** Located on the left, it contains a search bar, 'Default policies', 'Favorites', and 'All Domains'.
- Top menu bar (1):** Located at the top, it includes tabs for 'User management', 'Computer management', 'Permitted devices', 'Product settings', 'Administration', 'Installation', 'Reports', and 'Insight Analysis'.
- Main work area (2):** The central area displaying 'Computer management'. It includes a table of 'Default rights (computer)' and a 'Devices and ports' section showing storage devices with full access rights.

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			

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 individual 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**, **Data Loss Prevention** 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). If you use Active Directory or another directory service, you can synchronize it with the Console. For details, see [AD- /NDS-/LDAP-Synchronization](#).

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

2. PERFORMING AD- / NDS- / LDAP- SYNCHRONIZATION

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.

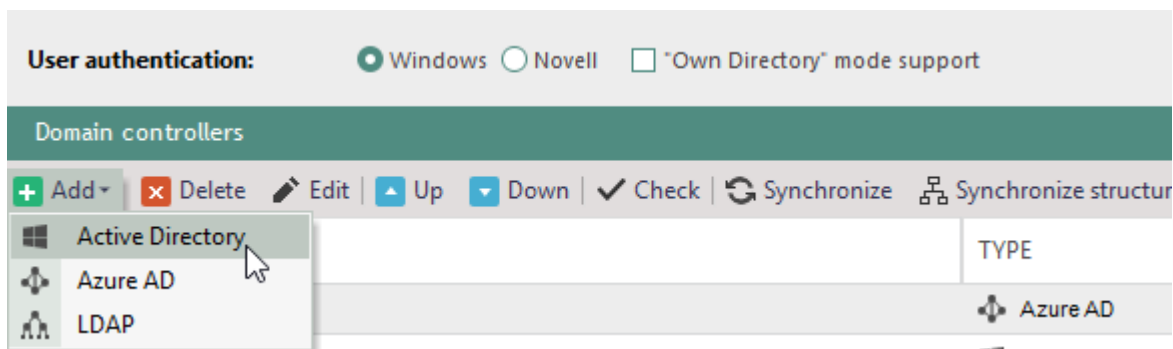
Synchronization of domains or organizational units refers to objects (users, computers, groups) that physically exist locally. Synchronization of groups, on the other hand, only applies to the group membership, but the group members / objects (users, computers, groups) do not physically exist locally.

- 2.1. Specifying connection settings
- 2.2. Setting up synchronization
- 2.3. Performing synchronization

2.1. Specifying connection settings

Synchronization requires account information of the domain controller/server 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**.



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](#) in the [EgoSecure Console Manual](#).
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. Click **Check**.
8. Once the connection is tested successfully, click **OK** to confirm and close the dialog.
9. Click **Save** to save the changes.
10. Click **Synchronize** to perform the synchronization of the selected domain controller with the settings defined under **Administration | Synchronization | Synchronization**.

2.2. 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

The following synchronization settings are available:

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 [number] 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 [number] days	Removes deleted directory service objects from the console after a certain period of time (Administration AD Synchronization Deleted objects). This option is available only if the option Synchronize only changes in AD for the last [number] 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 settings

Automatic product activation takes care about activating and deactivating products for users and computers shortly after each synchronization according to defined settings. The following settings are available:

Option	Description
Activate products for new users/computers a) all selected products b) only group-matching products	Activates all selected products for new users/computers. Activates only the products both selected in the list and already activated for a group. ! A group must be synchronized with server before adding new users/computers there. Otherwise, users/computers in this group are not considered as new ones. The option is available only if the options Synchronize directory structure only and Match product activation

	<p>with the activated products of the group are not enabled.</p>
Deactivate products for inactive users/computers	<p>Deactivates products for inactive users/computers. <i>Inactive users/computers</i> are the objects of a directory service, for which the disable account operation has been performed.</p> <p>The option is available only if the options Synchronize only active users/computers and Synchronize directory structure only are not checked.</p>
Match product activation with the activated products of the group	<p>Automatically activates only the products, which are already enabled for a group. Products are activated for both new and existing users/computers.</p> <p>Groups are:</p> <ul style="list-style-type: none"> ■ Groups imported from the Active directory. ■ EgoSecure groups created in a domain under User management/Computer management Directory service structure. <p><i>EgoSecure groups created in the domain</i> can contain only AD users/computers while <i>EgoSecure groups created in the Own directory</i> can contain only local users/computers.</p> <p>! Products previously enabled for a user/computer become disabled if they are not enabled for a group.</p> <p>The option is available only if the options Synchronize directory structure only and Activate products for new users/computers are not enabled.</p>

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** section.
 - 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 **esSyncIgnored** attribute with the value **0** for directory objects directly in the Active Directory.

4. In the **Directory service structure** section, 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 the structure (Domains, OUs and folders) of the directory service

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. Click **Add**.
 - b. Select the directory objects and click **OK**.
 - The excluded objects appear in the **Objects to exclude from synchronization** area.
6. Click **Save**.

2.3. Performing synchronization

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

Performing synchronization manually

1. Go to **Administration | AD(NDS/LDAP) Synchronization | Synchronization**.


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**.

Edit the settings. For details see [Setting up synchronization](#).

Click **Start**.

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

Performing synchronization at a 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.

3. DEFINING ADMINISTRATORS

- 3.1. Creating administrators or super administrators in Console
- 3.2. Granting administrative (super administrative) privileges to users from directory service
- 3.3. Creating and assigning administrative roles

There are three types of administrators in the Console:

■ Supervisor

Can be created during the Server installation. If not, can be created during the first Console login ([Creating a supervisor](#)). Has all permissions which cannot be restricted.

■ Super administrator

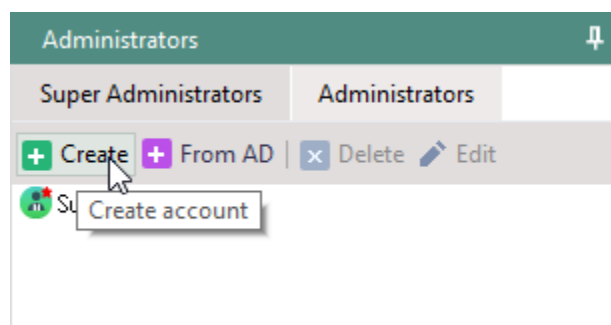
A super administrator is created by the supervisor. He owns all rights. The rights can be restricted by the supervisor by hiding console commands for the super administrator. Any number of super administrators can be created. A Windows user account can also act as a super administrator.

■ 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 administrator.

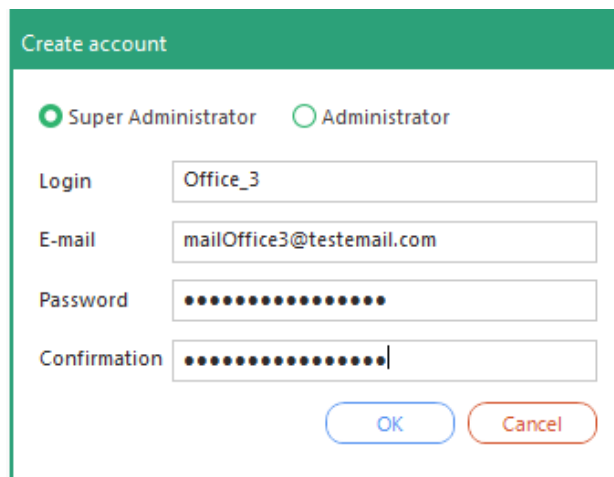
3.1. Creating administrators or super administrators in Console

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. In the **Administrators** work area, click **Create**.



→ The **Create account** dialog appears.

3. Select whether to create an administrator or a super administrator.
4. Define login and password.
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.
With activated **IntellAct Automation** product, this email is used to inform respective tenant admins and super admins about Server events.



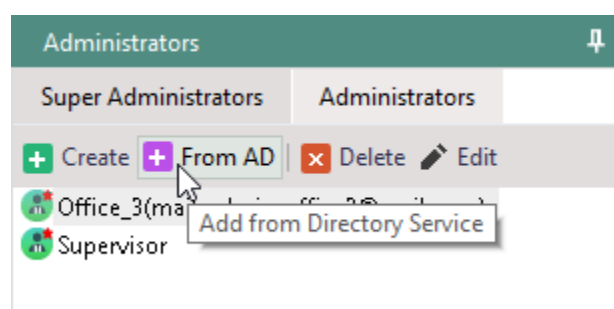
The 'Create account' dialog box has a green header. It contains two radio buttons: 'Super Administrator' (selected) and 'Administrator'. Below are four input fields: 'Login' with the value 'Office_3', 'E-mail' with 'mailOffice3@testemail.com', 'Password' with masked characters, and 'Confirmation' with masked characters. At the bottom right are 'OK' and 'Cancel' buttons.

6. Click **OK**.

➔ New administrator (super administrator) appears in the **Administrators** section.

3.2. Granting administrative (super administrative) privileges to users from directory service

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




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

3. Select a user from the list and click the right arrow. You can select several Windows user accounts as console administrators at once.
4. Click **OK**.

- New user appears in the **Administrators** section under the **Administrators** or **Super administrators** tab. Now he can login to console using Windows account.

To login to Console as a user with granted administrative (super administrative) privileges:

1. Click  in the top right corner of the Console window.
→ The **Connect to EgoSecure server** dialog appears.
2. Clear the Use EgoSecure authentication box.
3. Click **OK** to login.

- Login to Console occurs successfully if the user with granted administrative (super administrative) privileges is currently logged in to the operating system.

3.3. 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.

There are two types of roles:

- **Global**
- **Scope specific**

Criteria	Global	Scope specific
Role purpose	Permit access to defined Console sections. Permitted sections are defined in Administration Superadmin Administrative roles Operations work area.	
Role scope	Admin manages a directory structure on the whole without distinction (all users and computers of a domain, for example). It means that he, for example, cannot assign a filter to one user of the directory structure, because he is not permitted to see directory objects contained within the domain.	One of the permitted directory objects.

Creating a role

1. Go to **Administration | Superadmin | Administrative roles**.
2. In the **Global roles** or **Scope specific** roles tab, click **Add**.

Administration » Superadmin » Administrative roles

Administrative roles - Global roles

Global roles | Scope specific roles

Save | Add | Delete

NAME

Role for group 1

- Specify a role name.
- In the **Operations – [role name]** work area, set check boxes to permit operations.

Operations - Role for group 1		
NAME	VIEW	MODIFY
<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/>	<input type="checkbox"/>
Inheritance settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application-dependent settings	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Default policies	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Permitted devices	<input type="checkbox"/>	<input type="checkbox"/>
Permitted device models	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Challenge-response unblocking code	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Devices list for encryption	<input type="checkbox"/>	<input type="checkbox"/>

- Click **Save**.

Assigning a global role to an administrator

- Go to **Administration | Superadmin | Administrators & scopes**.
- Select an administrator in the **Administrators** work area -> **Administrators** tab.

Administrators

Super Administrators | Administrators

Create | Add | Delete | Edit

Admin 1

Admin2(mailAdmin2@mail.com)

- In the **Administrative roles - [admin name] | Global roles** tab, select a role created in **Administration | Superadmin | Administrative roles**.

Administrative roles - Admin 1

Tenants

Global roles

Scope specific roles

Save

<input checked="" type="checkbox"/>	NAME
<input checked="" type="checkbox"/>	Role for group2
<input type="checkbox"/>	Audit
<input type="checkbox"/>	Antivirus

4. Click **Save**.

Assigning a scope specific role to an administrator

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. Select an administrator in the **Administrators** work area | **Administrators** tab.

Administrators

Super Administrators

Administrators

Create

Add

Delete

Edit

Admin 1

Admin2(mailAdmin2@mail.com)

3. In the **Administrative roles – [admin name] | Scope specific roles** tab, click a scope (directory objects that can be managed by the administrator to whom the role is assigned).
4. In the **Administrative roles selection** work area, enable the roles. Once roles are enabled, the selected directory object changes its color.

Administrative roles - Admin 1

Tenants Global roles Scope specific roles

Save

All Domains

- TEST_WORKGROUP
- WORKGROUP
 - OU 1
 - OU2
 - Unsorted (30)
 - 1
 - Management group
 - User_100
 - AMD 32
- cit

Administrative roles selection

<input checked="" type="checkbox"/>	NAME
<input checked="" type="checkbox"/>	Cloud
<input checked="" type="checkbox"/>	Audit

5. Click **Save**.

- The administrator receives the rights of the role for the selected section of the directory service structure.

4. MANAGING TENANTS

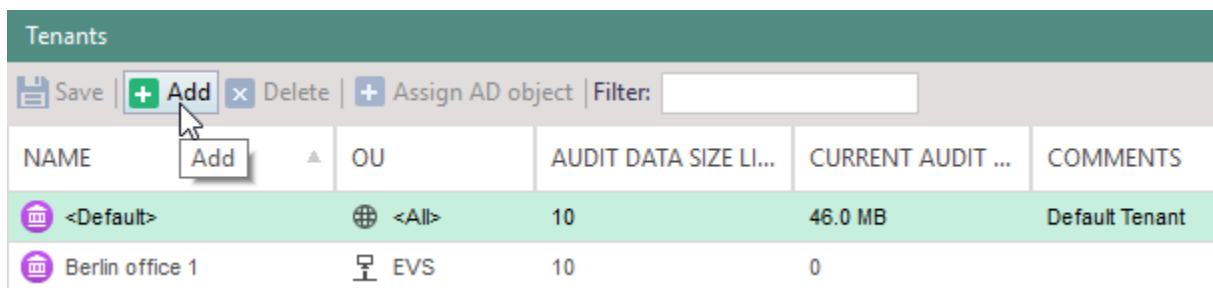
Tenants are used to divide and isolate EgoSecure Data Protection Console settings (except [Common console branches](#)) and directory objects of several united organizations or several departments of one organization which have one server and database. If no tenants are created, the **<Default>** tenant is used, which includes all elements of the directory service structure.

- 4.1. Creating a tenant
- 4.2. Assigning a tenant to an administrator or a super administrator
- 4.3. Switching between tenants

4.1. Creating a tenant

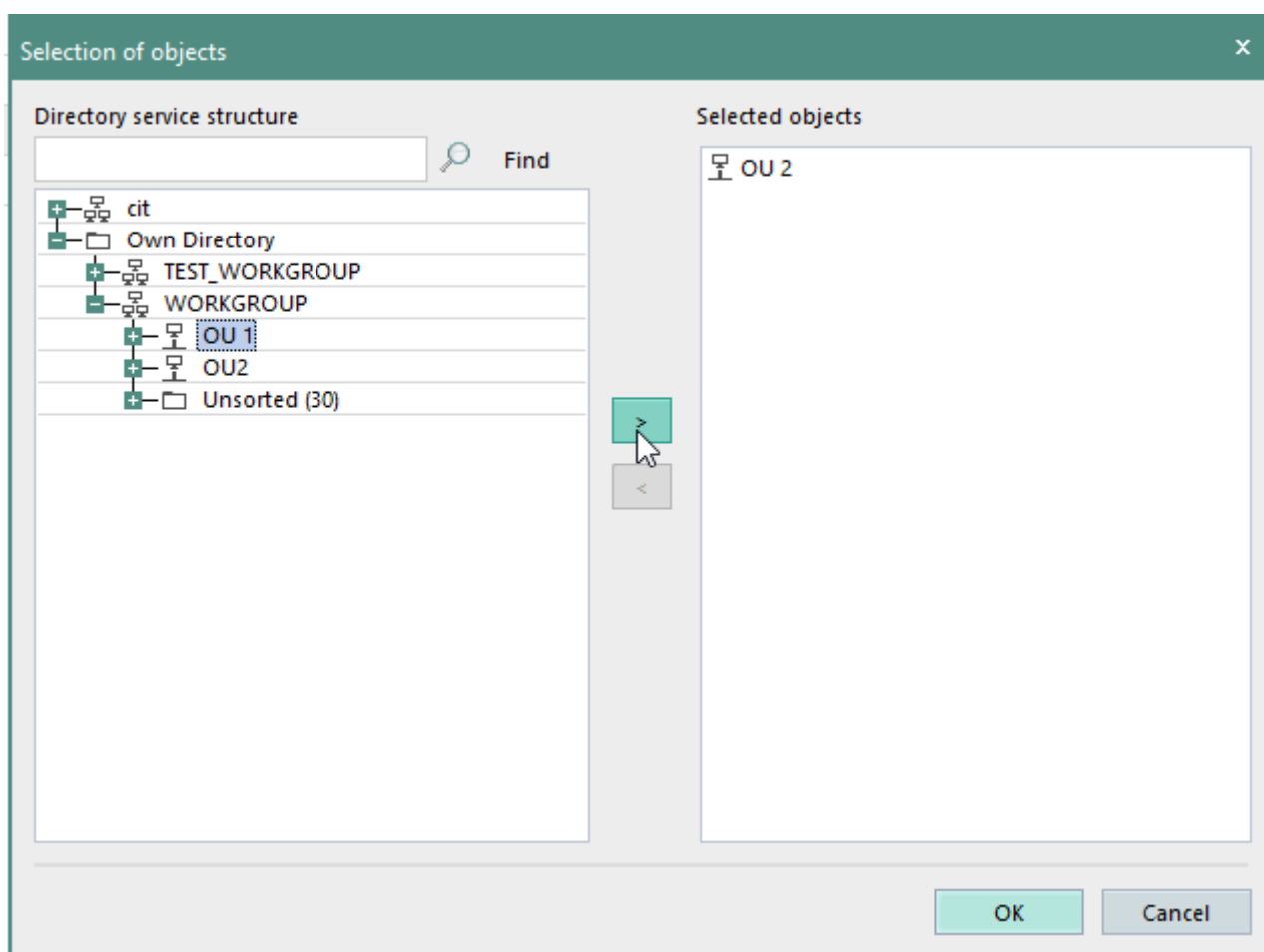
A tenant is created to assign objects of the directory (domains and OUs) which can be managed by an admin or a super admin who logs in to this tenant.

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



Tenants					
Save + Add x Delete + Assign AD object Filter: <input type="text"/>					
NAME	OU	AUDIT DATA SIZE LI...	CURRENT AUDIT ...	COMMENTS	
<Default>	<All>	10	46.0 MB	Default Tenant	
Berlin office 1	EVS	10	0		

- A new entry appears in the list with the *New tenant* name.
3. Change the name if necessary and click **Assign AD object** (or click in the area of the OU column).
 - The **Selection of objects** dialog appears.



4. Select objects and click **OK**.

→ The selected objects appear in the **OU** column divided with semicolon (;).

Tenants			
<div> Save Add Delete Assign AD object Filter: <input type="text"/> </div>			
NAME	OU	AUDIT DATA SIZE LI...	CURRENT AUDIT
<Default>	<All>	10	46.0 MB
Berlin office 1	EVS	10	0
Berlin office 2	OU 1; OU 2	10	0

5. Click **Save**.



ATTENTION

Directory objects in tenants

One directory object can only belong to one tenant.
Objects deleted from a tenant or objects which do not belong to any tenant, receive the settings of the **Default** tenant.

4.2. Assigning a tenant to an administrator or a super administrator

1. Go to **Administration | Superadmin | Administrators & scopes**.
2. Select an administrator or a super administrator in the **Administrators** work area | **Administrators (Super Administrators)** tab.
3. In the **Tenants** tab, enable tenants.

Administrators

Super Administrators

Administrators

+ Create

+ Add

✕ Delete

✎ Edit

Admin 1

Admin 2

Admin 3

DESKTOP-7CDTHEJ\user win10

DESKTOP-B2270UD\User_02

Administrative roles - Admin 3

Tenants

Global roles

Scope specific roles

Save

<input checked="" type="checkbox"/>	NAME	OU
<input type="checkbox"/>	Hamburg	No objects selected
<input checked="" type="checkbox"/>	Berlin office 2	OU 1; OU 2
<input checked="" type="checkbox"/>	Berlin office 1	EVS
<input type="checkbox"/>	<Default>	<All>

4. Click **Save**.



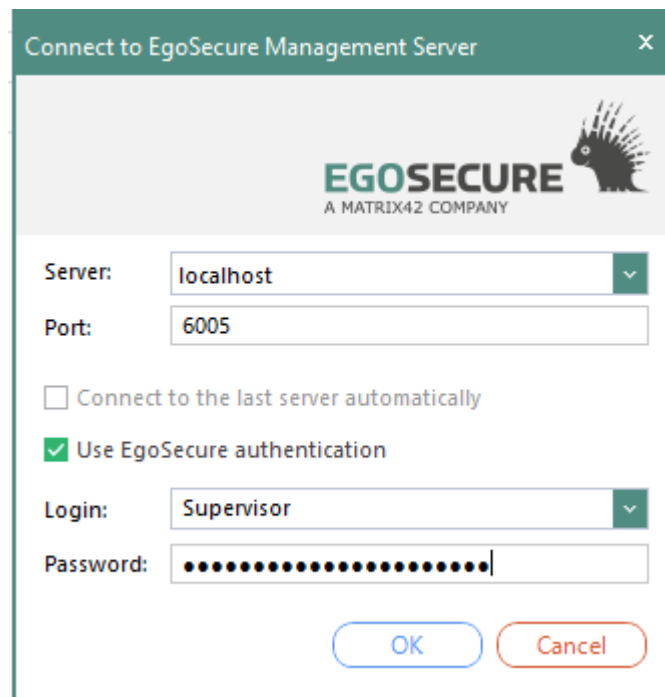
INFO

Tenant management

One tenant can be managed by several administrators and super administrators and the supervisor.

4.3. Switching between tenants

1. Logon to the **EgoSecure Server**.

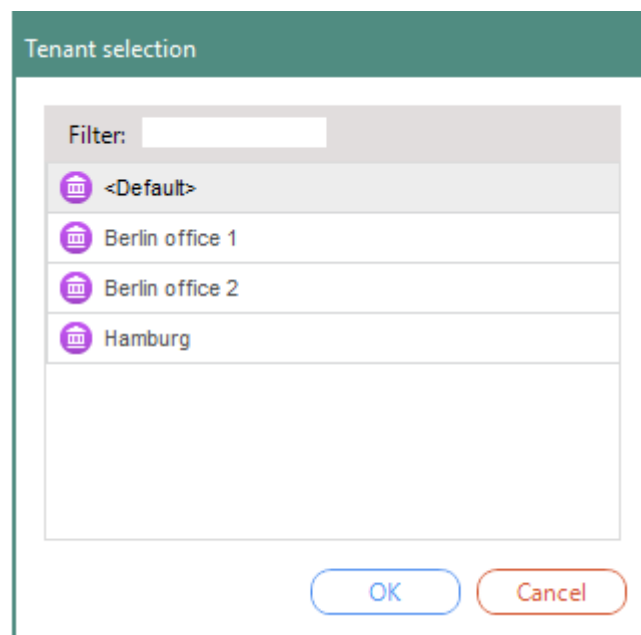


The dialog box is titled "Connect to EgoSecure Management Server". It features the EgoSecure logo (a porcupine) and the text "A MATRIX42 COMPANY". The form includes the following fields and options:

- Server:** A dropdown menu with "localhost" selected.
- Port:** A text input field containing "6005".
- ☐ Connect to the last server automatically
- ☒ Use EgoSecure authentication
- Login:** A dropdown menu with "Supervisor" selected.
- Password:** A text input field filled with 15 dots.
- Buttons:** "OK" (blue outline) and "Cancel" (red outline).

2. Click **OK**.

→ The **Tenant selection** dialog appears.



The dialog box is titled "Tenant selection". It includes a "Filter:" text input field at the top. Below it is a list of tenants, each preceded by a purple icon of a building:

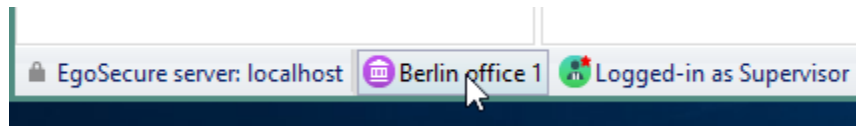
- <Default>
- Berlin office 1
- Berlin office 2
- Hamburg

At the bottom of the dialog are "OK" (blue outline) and "Cancel" (red outline) buttons.

3. Selects one of the tenants and click **OK**.

→ The Console is opened in the same state and with the settings defined for this tenant. The tenant name is displayed on the bottom left part of console window. Click the tenant

name to login to another tenant. Administrators and super administrators can see and login only to permitted tenants.



Common console branches

Although console settings and branches are divided and isolated, the following sections are common for all tenants:

■ Administration:

- 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.

■ Admin tool and its settings;

■ Product settings:

- Audit | Shadowcopy | Shadowcopy server.
- EgoSecure Antivirus | Update settings | Server settings.

■ Installation:

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

5. INSTALLING EGOSECURE AGENTS

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

**INFO****Agent installation without directory service**

If you do not use a directory service, but use the **Own Directory**, the Clients appear in the Console after the Agent installation.

- ◆ Install Agents in this case using a different way (e.g. via software distribution or local installation).

Before generating an MSI package, adjust the client settings, if necessary.

- 5.1. Adjusting Windows settings
- 5.2. Adjusting client settings
- 5.3. Generating an MSI package
- 5.4. Installing EgoSecure Agents via Console

5.1. Adjusting Windows settings

Enable the TCP ports on Server and Client so that **EgoSecure Agent** and **EgoSecure Server** can communication with each other. If you use the Windows Firewall, create the rules under **Advanced settings**.

If you install **EgoSecure Agents** via the Console, customize the group policies in addition.

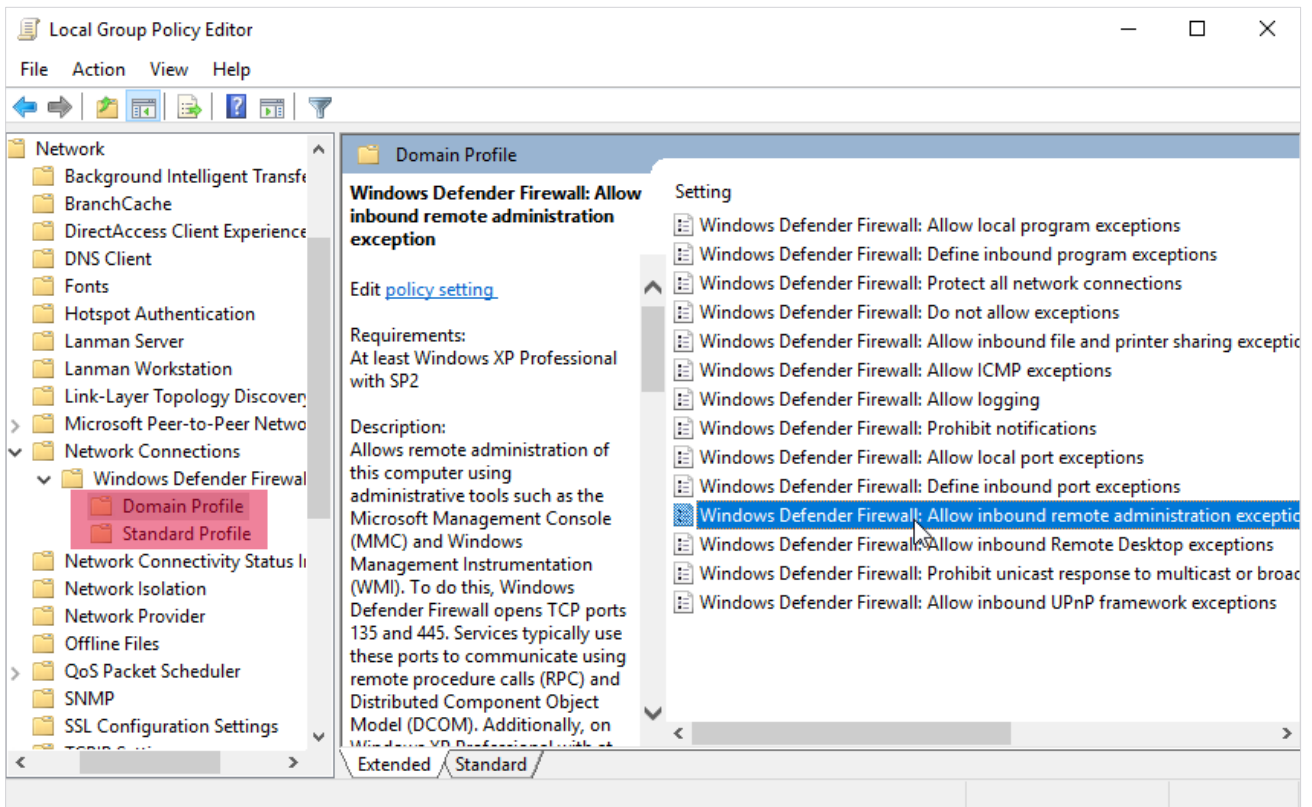
Enabling TCP ports

1. On the computer with **EgoSecure Server**, create a new incoming rule for **EgoSecure**: TCP port 6005, Allow the connection.
2. On the computer with **EgoSecure Agent**, create a new incoming rule for **EgoSecure**: TCP port 6006, Allow the connection.
3. If the outgoing connections in your system environment are not opened by default, create the following additional rules:
 - a. On the Server: new outgoing rule for **EgoSecure** TCP port 6006, Allow the connection.
 - b. On the Client: new outgoing rule for **EgoSecure** TCP port 6005, Allow the connection.

Customizing group policy

Group policy for an Agent can be customized via GPO or, as described below, locally for each Agent.

1. Open the Group Policy Editor via the Windows Settings or by running the gpedit.msc file.
2. On the computer with **EgoSecure Agent**, 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**.



5.2. Adjusting client settings

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

Showing settings

1. Go to **Administration | Clients | Client settings**.
2. To see the description of a setting at the bottom of the **Client settings** section, click the table entry.

Adjusting settings

1. To forbid users to ask for the change of the access rights via **EgoSecure Agents**, disable the **Allow requests for access rights** check box.
2. To avoid conflicts between network drive and external media when external storage gets the same drive letter a network drive, set the **Drive letter assignment** option.
3. Define further settings if needed and click **Save**.

5.3. Generating an MSI package

Defining package settings

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



INFO

Restrictions on using MSI generation options

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

3. To see the description of settings at the bottom of the window, click the table entry.
4. To forbid users with administrative rights to stop the **EgoSecure Server** service, set the **Protect EgoSecure Agent service and files** check box.
5. To forbid users with administrative rights to uninstall or update the EgoSecure Agents, set the **Check the password on uninstall** (update) box.
6. If you are going to use SSL in the company, you can include an SSL certificate for the Agent to the MSI package via enabling the **Add SSL certificate and its private key** option and defining a password for certificate protection.

- The certificate for the Agent with its private key is added to the MSI package if the certificate with its private key is provided under **Administration | Administrator | SSL configuration**. There are also other ways of distributing SSL certificate to Agents (for details, see the [SSL implementation](#) whitepaper).



WARNING

Possible data loss with immediate installation of the WLAN control

If you select **Immediately** for the option **Install network driver for WLAN control**, the WLAN on the client side will be temporary interrupted during the installation. This may lead to a data loss.

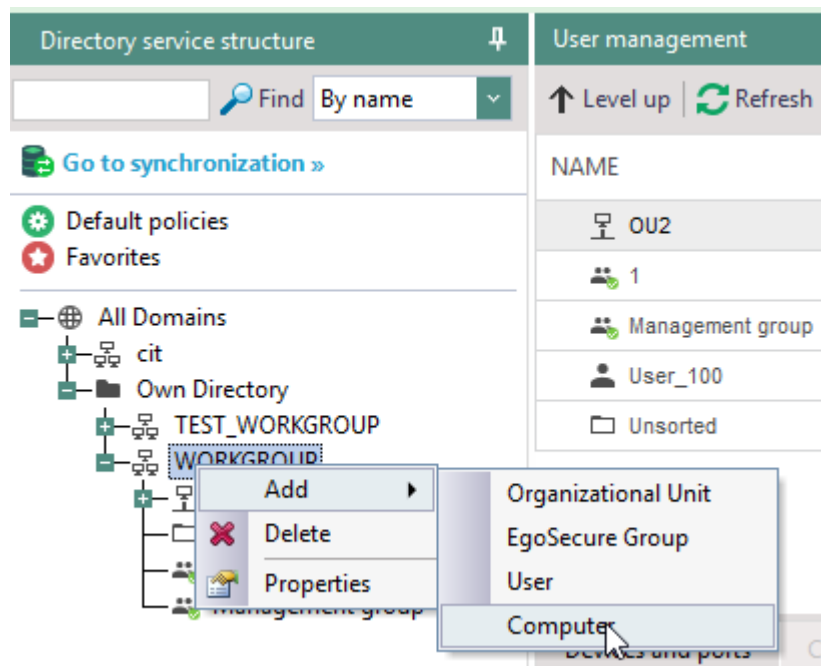
- ◆ To install WLAN control after the **EgoSecure Agent** restart, select the **After restart** option from the drop-down list.

Generating a package

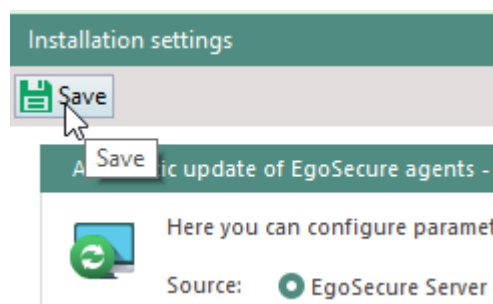
1. In the **Path to the MSI package** area, in the **Folder** field, define the folder where to store the MSI package.
2. In the **Create MSI package** area, click **Generate**.
 - On the right side of the **Create MSI package** area, the details whether the package was generated and where it was generated are displayed.
3. Click **Open folder** to open the location of the MSI package.

5.4. Installing EgoSecure Agents via Console

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



- c. Enter a name of a computer where to install the Agent.
- d. Set up WMI on the computer where the Agent will be installed to provide an access to administrative shares for the administrator specified in step 5.
4. Go to **Installation | EgoSecure agents | Installation settings**.
5. In the **Remote installation settings** area, specify the login data of the administrator who has enough rights for installing the EgoSecure Agent on the devices.
6. In the **Installation settings** main area, click **Save**.



7. Go to **Installation | EgoSecure agents | Install/Update**.
8. In the **Show** drop-down menu, select the **Only computers without agents** option.
9. Select the clients, where to install the **EgoSecure Agents**.
10. Click **Install/Update**.

➡ The Agents are now installed and activated on client.
To test the connection between Agent and Server, use Telnet.

Testing connection

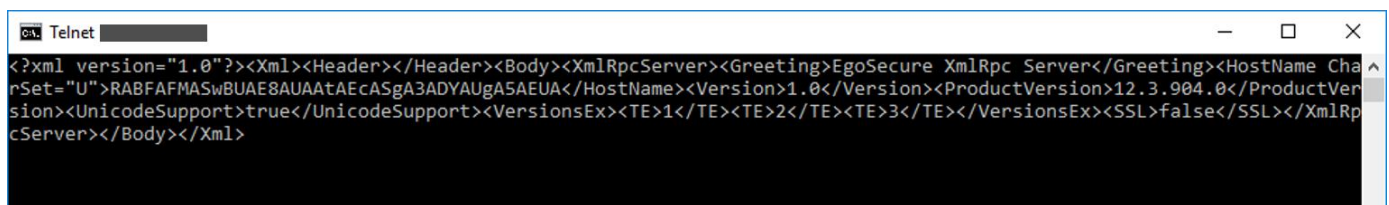
1. To enable Telnet, enter **OptionalFeatures** in the Windows search box and enable the **Telnet Client** check box in the **Windows Features** dialog window.
2. Enter the following commands in the Windows command prompt:
3. To test the connection from Server to Client:

```
telnet [client IP address] 6006
```

4. To test the connection from Client to Server:

```
telnet [Server IP Address] 6005
```

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



```

c:\ Telnet
<?xml version="1.0"?><Xml><Header></Header><Body><XmlRpcServer><Greeting>EgoSecure XmlRpc Server</Greeting><HostName>CharSet="U">RABFAFMASwBUAE8AUAAAtAEcASgA3ADYAUGA5AEUA</HostName><Version>1.0</Version><ProductVersion>12.3.904.0</ProductVersion><UnicodeSupport>true</UnicodeSupport><VersionsEx><TE>1</TE><TE>2</TE><TE>3</TE></VersionsEx><SSL>false</SSL></XmlRpcServer></Body></Xml>
  
```

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

6. ACTIVATING PRODUCTS

For each Agent and computer, where the product will be used, activate the product in the Console. For every activated product the license is required. The number of available licenses and their usage you can see in **Administration | Licenses | License management**.

If users and computers appear in Console via a synchronization of the directory service structure, you can specify, which products are automatically activated for new users and computers. For details, see [Setting up synchronization](#).

If you activate a product for a group, the product is automatically activated for all group members. For every group member the license is required. You can cancel a license or deactivate a product for certain group members.



INFO

Activating Secure Audit and Encryption

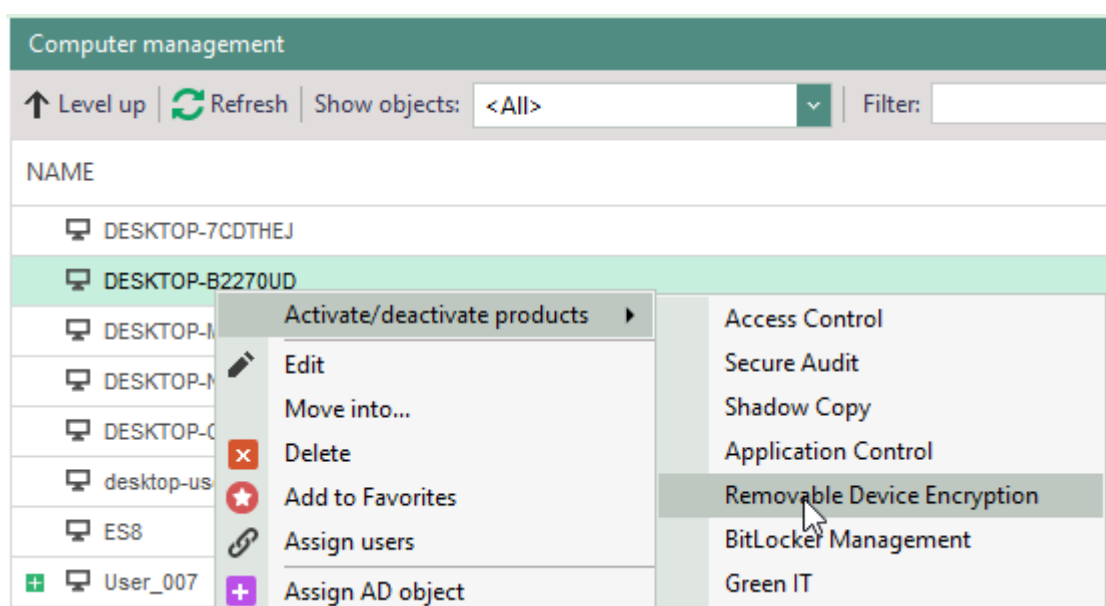
To activate **Secure Audit** and encryption products for a user, a computer or groups, you must first activate audit and encryption.

- ◆ To activate **Secure Audit**, go to **Product settings | Secure Audit | Audit**.

- ◆ To activate encryption, go to **Product settings | Encryption | Encryption options**.

Activating products

1. Navigate to the User management/Computer management menu.
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** work area.
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.

6.1. Activating products for computers

To apply the permissions to a computer and affect all users, enable the product for the computer. In spite of the products and rights activated for the user, the settings of the computer take effect.

The following products are activated only for computers:

- BitLocker Management
- Full Disk Encryption
- Green IT
- Inventory
- EgoSecure Antivirus
- DLP – Data at Rest

6.2. Activating products for users

If a product is activated for a user, he can use this product on any (network) computer. If the product is activated for the user, but not for the used computer, the permissions set for a user take effect. These can be either the default rights of users, group rights or individual user rights.

You can grant special permissions for certain users on certain computers. For details, see [Assign user to computer](#).

7. CONFIGURING DEFAULT RIGHTS

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** and encryption products for a user, a computer or groups, you must first activate audit and encryption.

- ◆ To activate **Secure Audit**, go to **Product settings | Audit | Audit**.
- ◆ To activate encryption, go to **Product settings | Encryption | Encryption options**.

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.

The screenshot shows the 'User management' interface. At the top, there's a header bar with 'User management' and navigation links like 'Level up', 'Refresh', 'Show objects: <All>', and 'Filter:'. Below this is a table with columns 'NAME' and 'ACTIVE PRODUCTS'. The first row is 'Default rights (user)' and the second is 'Unknown users'. The 'Default rights (user)' row is highlighted with a red box.

Below the table, there's a toolbar with tabs: 'Devices and ports', 'Cloud storage', 'Firewall', and 'Revision'. The 'Devices and ports' tab is active. In the toolbar, there are buttons for 'Save', 'Emergency', 'Devices', 'Ports', 'Profile: Online', and 'Summary'. The 'Devices' and 'Ports' buttons are highlighted with a red box, and the 'Profile: Online' dropdown is also highlighted with a red box.

Below the toolbar is a table with columns 'DEVICE TYPE', 'ACCESS RIGHTS', and 'TIME SCHEMA'. The first row is 'Storage'. The second row is 'CD / DVD' with a green checkmark and 'full access'. The third row is 'External storage' with a green checkmark and 'full access'.

4. In the toolbar of the product area, click **Save**.
 - The settings are applied to default users in online mode.
5. In the **Profile** drop down, select **Offline**.
6. Change the settings for offline default users.
7. Click **Save** in the toolbar.

→ The rights are assigned to default users in online and offline mode and 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. For details, see [Defining access rights](#).
3. Click **Save**.
4. In the **Profile** combo box, select **Offline**.
5. Define the offline settings and click **Save** again.

➤ The customizable default rights are automatically assigned for every unknown user, who logs on to the server. Additionally, if global filters have been created under **Product settings | Filters | Content filter definition**, they are applied to unknown users.

Customizing default settings for users

1. Navigate to **User management | Settings | Default policies**.
2. Select **Default rights (user)**.
3. In the lower part of the work area, click the **User settings** tab.
4. To prohibit the downloading of files via the Internet Explorer, enable the check box in the **Internet** work area.
5. To prohibit the usage of the clipboard, set the checkbox in the **Clipboard** area.
6. To disable file transfer via Skype, check the box in the **Communication** section.
7. To scan archives or MS Office by filters, check the corresponding checkbox in the **Content filter** section. The checkboxes are only available if the options under **Product Settings | Filters | Settings** are enabled.
8. Click **Save**.

Adjusting computer default rights

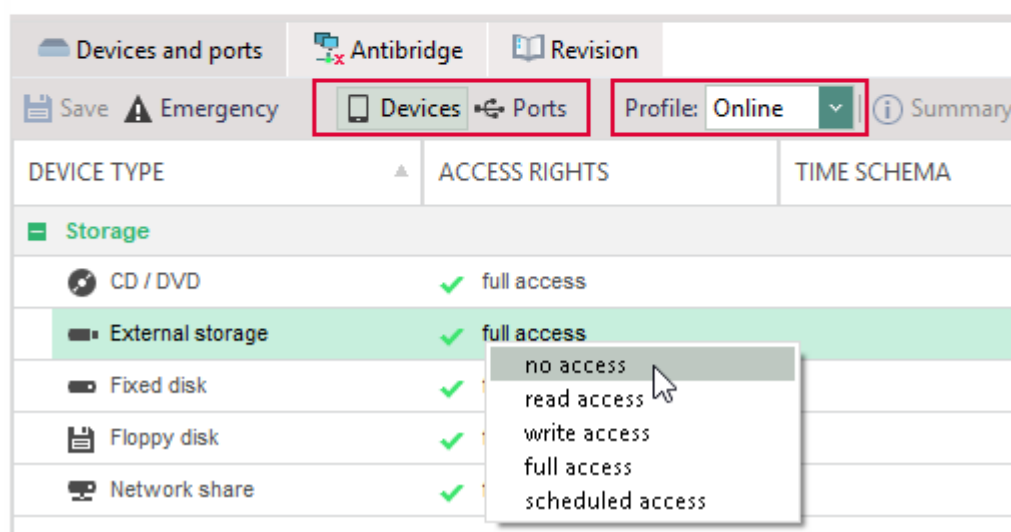
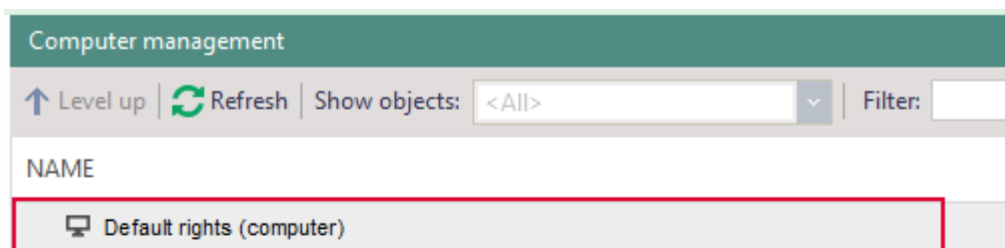


INFO

Rights priority for computers

If some products are also activated for computers or only for computers, restrictions defined for computers always have priority. For details, see [Activating products](#).

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:



4. Click **Save**.
5. In the **Profile** combo box, select **Offline**.
6. Define the settings for the offline profile and again click **Save**.

➡ The rights are assigned to default computers in online and offline mode and automatically inherited by all known computer 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](#).

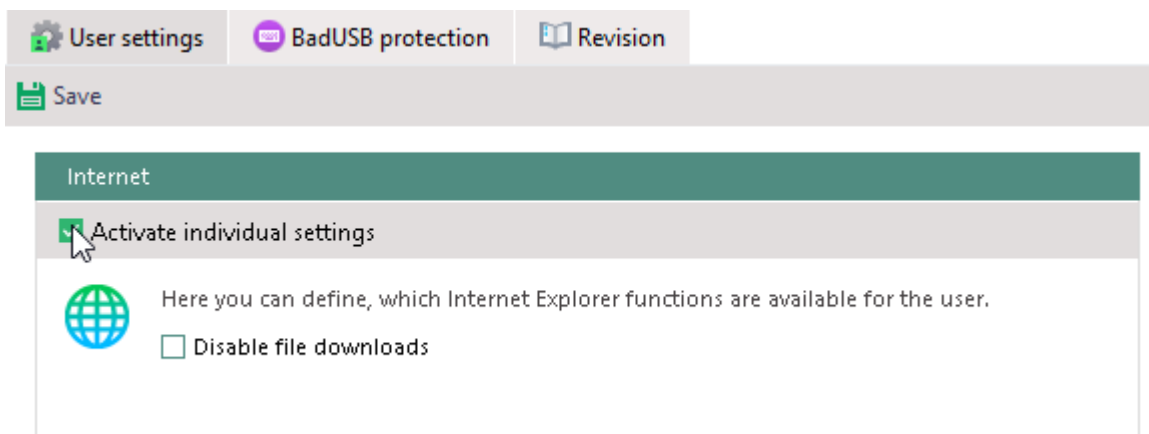
These client settings are inherited by every computer and can be customized for individual computers. For details, see: [Defining settings for computer](#).

7.1. Customizing settings for users

By default, users inherit the rights and settings from the default user. You can disable the inheritance and assign individual rights and settings to each user. User rights take effect only if the product is activated for the user and not for the computer. For details, see [Activating products](#).

Customizing 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 **Content filter** area are available only when options under **Product settings | Filters | Settings** are enabled.
2. Click on the **Activate individual settings** check box to deactivate inheritance and change the settings.



3. Click **Save**.

→ The selected user now has 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 lower part of the work area, click the tab where you want to make changes.

3. Enable the **Activate individual settings** option.
If the option is greyed out and cannot be edited, the product is not activated. For details, see [Activating products](#).
4. Edit the settings and click **Save**.

Defining access rights



INFO

Product activation required

For the access rights configuration to work, activate the **Access Control** product for the selected object (user/computer/group).

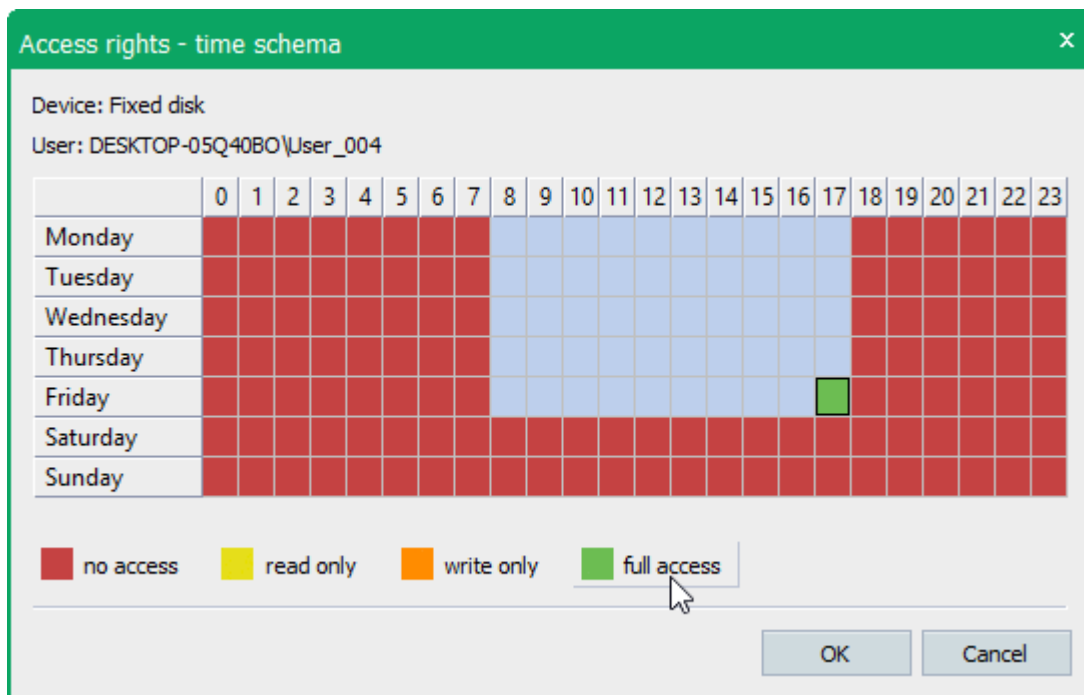
Permitting/restricting access to certain devices

1. Go to **User management/Computer management | Control**.
2. Click on the **Devices and ports** tab.
3. In the **Profile** drop-down menu, select whether the permissions will be applied to online or offline computers. *Offline* profile means that connection cannot be established with the **EgoSecure Server**.
4. Right-click a device.
5. Select an access right. See also [Configuring a scheduled access](#), [Configuring a temporary access](#).
6. Click **Save**.

➡ New permissions are transferred and applied on the Agent.

Configuring a scheduled access

1. Right-click a device and select **Scheduled access**.
→ The **Access rights – time schema** dialog appears.
2. Select a time period by hovering over the area.
3. Click on an access right.



4. Click **OK** to confirm.
5. In the **Devices and ports** tab, click **Save** on the toolbar.

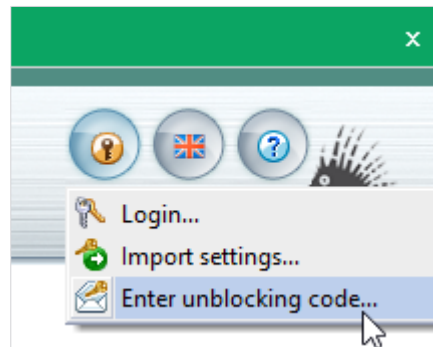
Configuring a temporary access

1. Right-click a device and select **Temporary right access**.
 - The **Temporary right access** dialog appears.
2. Select an access type and specify a type period.
3. Click **OK** to confirm.
4. In the **Devices and ports** tab, click **Save** on the toolbar.


Configuring an unblocking code for offline clients

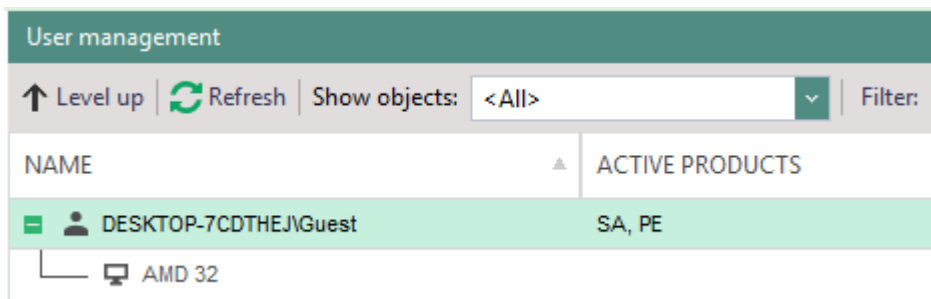
1. Right-click a device and select **Generate unblocking code**.
 - The **Unblocking code generation** dialog appears.
2. Select an access type and access duration and click **Generate**.
 - The generated code appears in the **Code** field.
3. Copy the code and send it to the client (e.g. by mail).

→ Via the **EgoSecure Agent** the client can enter the code and get the access rights:



Assigning special permissions to a user on certain computers

1. Right-click a user in **User management**.
2. Select **Assign computers** from the context menu.
 - The **Selection of computers** dialog appears.
3. Select a computer from the directory service structure and click on .
 - The computer appears in the **Selected computers** field.
4. Click **OK** to confirm.
 - In **User management**, the computer appears under the user.



5. Click on the computer and edit the user-specific permissions for the computer in the lower area.
6. Click **Save**.

7.2. Customizing permissions for computer

The settings that you define for a computer under **Computer management | Settings** are connected with the client settings of the **Administration** menu. For details, see [Adjusting client settings](#).

If you want to customize the individual settings of a computer, you can only deactivate but not activate the options defined in the client settings.

Defining settings for computer

1. Select a computer under **Computer management | Settings**.
2. Enable the **Activate individual settings** box.
3. Disable the necessary settings and click **Save**.


Defining rights for Secure Audit, Filters, Encryption and Application Control products

1. Select a computer in the **Computer management** menu.
2. In the lower part of the work area, click on the tab where you want to change the settings.
3. Enable the **Activate individual settings** check box.
If the option is greyed out and cannot be edited, the product is not activated. For details, see [Activating products](#).
4. Edit the settings and click **Save**.

8. MANAGING USER GROUPS

A group is a directory object, which consists of users and/or computer. The group receives for its members the default rights for users and computers. These rights can be changed. The members of a group can inherit the different permissions of the group. Individual permissions of users and computers have priority over the group rights.

Viewing and adding group members

1. Right-click a group in the **Directory service structure**.
2. Select **Group members** from the context menu.
→ The **Group members** dialog appears. The group members are shown in the right part of the dialog.
3. Select a user or a computer from the directory service structure and click .
→ The new group member appears in the right part of the dialog.
4. Click **OK** to confirm.

Editing group rights


1. In the **User management/Computer management** menu, in the **Directory service structure** area, click on the element (e.g. domain or OU) that contains the group.

2. Click on the group in the User management/Computer management area.
3. In the lower part of the **User management/Computer management** area, edit the group rights.
4. Click **Save**.

If a user is a member of more than one group, the rights of the group may differ. In this case, you should define whether restrictions or permissions have priority.

Rights priority of group members in multiple groups

1. Go to the **Product settings** menu.
2. Edit the **Inheritance settings** area, edit the rights priority:
3. To grant priority to permissions, which were defined for the **Access Control** product, select the **Access permissions have priority** radio button. Otherwise, select the **Access restrictions have priority** radio button.
4. To grant priority to permissions, which were defined for the **Encryption** product, select the **Encryption permissions have priority** radio button. Otherwise, select the **Encryption restrictions have priority** radio button.
5. Define the rights of which groups must be inherited by the user:
 - a. **EgoSecure groups**: only EgoSecure groups inherit the rights.
 - b. **AD/Novell groups**: only directory service groups inherit the rights.
 - c. **EgoSecure groups and AD/Novell groups**: all groups inherit rights.
6. Click **Save**.

 The inheritance settings are applied.