



EGOSECURE AGENT

User 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. OVERVIEW AND BASIC FUNCTIONS	4
1.1. Opening EgoSecure Agent	4
1.2. Agent main elements.....	4
1.3. Changing user on Agent.....	5
1.4. Importing settings	6
1.5. Entering unblocking code	6
1.6. Navigating in popup messages.....	6
2. ACCESS CONTROL	7
2.1. Overview.....	7
2.2. Requesting for access rights change	9
2.3. Controlling the use of keyboards	10
3. ENCRYPTION.....	11
3.1. Overview.....	11
3.2. Encrypting files.....	11
3.3. Using mobile encryption.....	20
3.4. Opening or decrypting encrypted data.....	23
3.5. External access to encrypted files	30
4. ANTIVIRUS	33
4.1. Overview.....	33
4.2. Starting a scan.....	34
4.3. Managing quarantined objects	34
4.4. Defining exclusions	36
4.5. Planning scans	38
4.6. Managing logs.....	39
5. GREEN IT	40
5.1. Overview.....	40
5.2. Performing actions when idle time is out.....	40
5.3. Configuring power profile	41
5.4. Planning tasks.....	42
5.5. Managing exceptions	44
5.6. Changing settings	46
6. SECURE ERASE	46

- 6.1. Overview 46
- 6.2. Deleting files securely 47
- 6.3. Planning secure erase 48
- 7. PASSWORD MANAGER49**
- 7.1. Overview 49
- 7.2. Managing password container 50
- 7.3. Using password container 54


LIST OF FIGURES

- Figure 1. The EgoSecure Agent overview5
- Figure 2. Access control module7
- Figure 3. User specific data filters in the black list mode8
- Figure 4. Generate request code 10
- Figure 5. Keyboard control 10
- Figure 6. Encrypt file in cloud individually 13
- Figure 7. Permanent Encryption 14
- Figure 8. Post-Quantum Encryption with password 15
- Figure 9. Selecting certificates for encryption 16
- Figure 10. Permission for mobile encryption 20
- Figure 11. Specifying the name and password of a mobile key 22
- Figure 12. Overview of available keys 23
- Figure 13. Encrypted files in Windows Explorer 24
- Figure 14. Decrypting permanently encrypted files 26
- Figure 15. Entering mobile password for Cryption Mobile 28
- Figure 16. Cryption Mobile 29
- Figure 17. Access monitoring tab 30
- Figure 18. Information message about access to encrypted data 31
- Figure 19. Confirmation message about access to encrypted data 32
- Figure 20. Access log 33
- Figure 21. Antivirus module 34
- Figure 22. Restoring quarantined objects 35
- Figure 23. Editing exclusion entries 37
- Figure 24. Viewing information about wildcards 37
- Figure 25. Planning automatic scans 38
- Figure 26. Selecting time period 40
- Figure 27. Selecting the action to be performed when idle time is out 40
- Figure 28. Planning tasks for Green IT 43
- Figure 29. Disabling Green IT task 43
- Figure 30. Defining Green IT exceptions 45
- Figure 31. Selecting a secure erase method 47
- Figure 32. Emptying Windows Recycle Bin securely with Secure Erase 48
- Figure 33. Opened password container of Password Manager 50
- Figure 34. Creating a new password container 51
- Figure 35. Entering password for container 51

Figure 36. Creating a new password group in password container54
 Figure 37. New entry for password container.....55
 Figure 38. Copying password to the clipboard.....56

1. OVERVIEW AND BASIC FUNCTIONS

1.1. Opening EgoSecure Agent

Once you start the computers, the **EgoSecure Agent** starts automatically. In the right part of the window task bar the tray icon of the Agent appears .

- ◆ Double-click on  to open the Agent.


1.2. Agent main elements

As a client component of the **EgoSecure Data Protection** software suite, the **EgoSecure Agent** controls your access to devices, data and applications on the computer and on the network. In addition, the **EgoSecure Agent** provides other features that help to securely manage your data.

The layout of the **EgoSecure Agent** interface depends on the modules enabled for the logged in user and/or computer.

The following modules can be activated:

- Access Control
- Encryption
- Antivirus
- Green IT
- Secure Erase
- Password Manager

 INFO	<p>User- and computer-specific functionality</p> <p>This manual describes the full functionality of all modules. Depending on the permission profile, restricted functions can be available.</p>
--	---

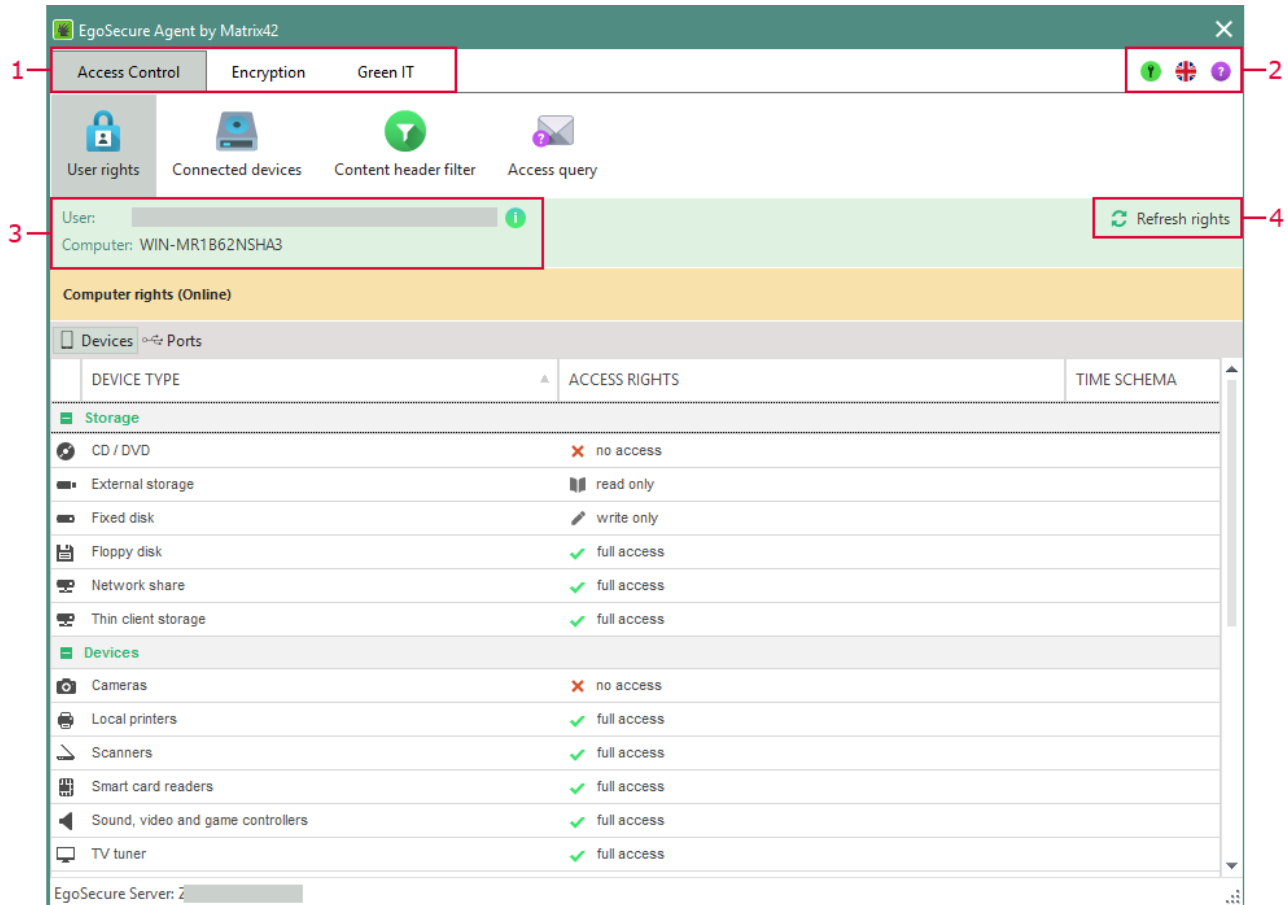


Figure 1. The EgoSecure Agent overview

In the module selection list, you can see, which modules are active (1). If the window is too small to display all modules, >> appears at the end of the bar so that you can access other modules.

With the symbols on the rights edge (2)

- change the language 🇩🇪
- view the version number of the installed Agent ?
- perform the following actions ⓘ:
 - [change user](#), [import settings](#), [enter unblocking code](#).



Below the module selection bar, you can see the credentials of the active user and computer (3).

Via the **Refresh rights** (4) button you can refresh your permission profile.

1.3. Changing user on Agent

By default, the logged in Windows user is logged in to the **EgoSecure Agent**. You can change the user. So, for example, an administrator with more extensive access rights logs in for a short time and uses his permission profile to perform actions that are not allowed to the default user of the computer.

Changing user


1. Click on  in the **EgoSecure Agent** toolbar.
2. Select **Login...** from the context menu.
 - The **Login...** dialog opens.
3. Enter the login data of the Windows user you want to login with.
4. Click **OK** to confirm.
 - A message that the user [name] has successfully logged on to the Agent appears. The permission profile of the newly registered user applies.
5. To return the permission profile of the logged in Windows user, click again on .
6. Select the **Logoff user [name]**.

→ **EgoSecure Agent** resumes the permission profile of the logged in Windows user.

1.4. Importing settings

The administrator can give you a file to update the settings of your permission profile.

Importing settings


1. Click on  in the **EgoSecure Agent** toolbar.
2. Select **Import settings...** from the context menu.
 - The **Open** dialog appears.
3. Select the **EgoSecure** settings file with the **.esd** extension and click **Open**.

→ The imported settings are applied immediately and the permission profile is updated.

1.5. Entering unblocking code

If your **Agent** works offline, you need an unblocking code to apply the rights requested from the administrator. For details, see [Requesting access rights](#).

Entering unblocking code

1. Click on  in the **EgoSecure Agent** toolbar.
2. Select **Enter unblocking code** from the context menu.
 - The **Enter unblocking code** dialog opens.
3. Enter the code which you received from the administrator.
4. Click **OK** to confirm.

→ The success message appears. The new access rights are applied and displayed. New code doesn't replace the previous one.

1.6. Navigating in popup messages

For navigating in EgoSecure Agent popup messages, use [Windows keyboard shortcuts](#).

2. ACCESS CONTROL

2.1. Overview

Access Control controls user access rights to drives, internal and external devices, communication ports and ports on a computer or network. The access to certain file types can be managed. Each user can have different permissions. The permissions may also depend on access rights of the used computer.

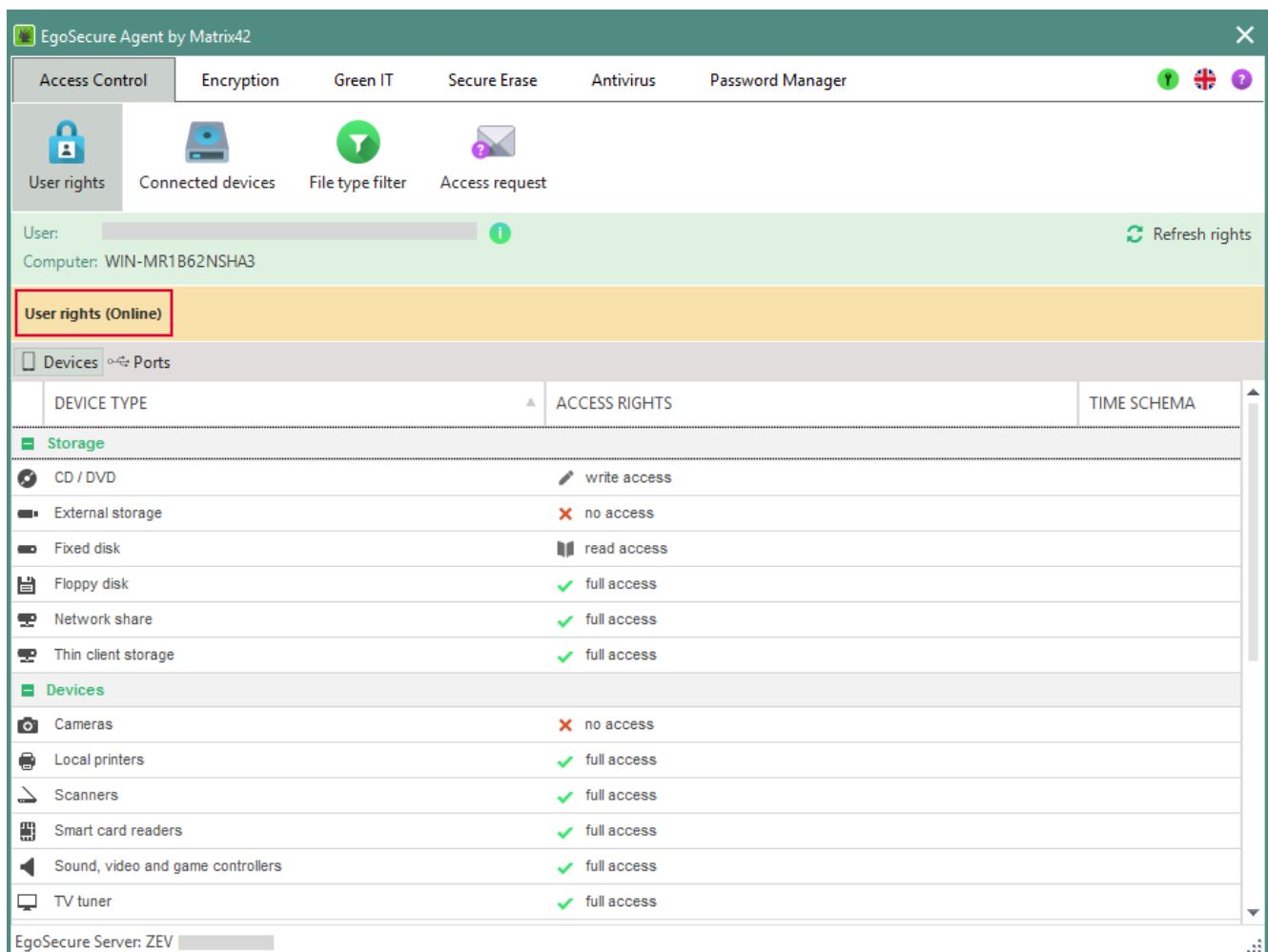


Figure 2. Access control module

User rights tab

Next to the lock icon you can see, whether the active permissions apply to all users of the computer (computer rights) or they are your personal permissions (user rights). What is more, you can see whether you currently have a connection to the EgoSecure Server (online) or not (offline).

In the **Access rights** column, you can see what access rights you have for the device of the **Device type** column.

In der **Time schema** column, you can see if your access rights are limited to a specific time period.

Connected devices tab

In the **Connected devices** tab, you can see all devices currently connected to the computer and access rights to them.

Comments column

If administrator assigns no individual permissions to certain device models, **Computer's rights (User's rights)** are displayed in the **Comments** column. If administrator assigns individual permissions to devices, the **Administrative white list of unique devices** note is shown in the **Comments** column. For example, if **no access** is assigned to the device class (device type) in **User rights**, certain device models can be permitted, and vice versa: if **full access** is assigned to the device class (device type) in **User rights**, certain device models can be forbidden.

Encryption type column

In the **Encryption type** column, the encryption type enabled for this device is displayed. If administrator starts to control hard disks like external media, the **Device encryption** type applies and **DE** is displayed in the column. If hard disks are not controlled like external media or device encryption is not enabled for an Agent, then the **Folder encryption** takes effect and **FE** is displayed in the column.

File type filter tab

In the **File type filter** tab, you can see which data filters are assigned to you.

If the **Blacklist** mode is enabled for filters, you must not access files described in the **File type** column.

If the **Blacklist** mode is enabled for filters, you can only access files described in the **File type** column.

NAME	FILE TYPE	LIMIT
Filter: Office Files (External storage)		
*	Microsoft Access 2007-2016 Database (*.accdb;*.accde;*.accdt)	-
*	Microsoft Word 97-2003 Document (*.doc;*.dot;*.tmp)	-
*	Microsoft Word 2007-2016 Document (*.docm;*.docx;*.dotm;*.dotx;*.tmp)	-
*	Microsoft Access 97-2003 Database (*.mdb)	-
*	Microsoft SQL Server files (*.ldf;*.mdf;*.ndf)	-
*	OpenOffice.org Base Document (*.odb;*.tmp)	-

Figure 3. User specific data filters in the black list mode

Access request tab

In the **Access request** tab, you can contact your administrator and request access rights. For details, see [Requesting access rights](#).

2.2. Requesting for access rights change

You can request access rights for one or more device types from the administrator. The administrator receives the access right request. As soon as he permits the rights, the corresponding permission is displayed in the **Access rights** column of the **User rights** tab. This can also be limited in time. In this case, you see the time restriction near the access right.

If **EgoSecure Agent** has no connection to the **EgoSecure Server** (offline mode), the administrator can give you an unblocking code. As soon as the code is entered, you receive the required permissions. See also: [Entering unblocking code](#)

Requesting for access rights for individual devices

1. In the **User rights** tab, right-click the entry for which you want to change access rights (e.g. **no access**).
2. Select the access right which you want to ask for (e.g. **Request full access**).
→ The **Access request** tab opens. In the **Device** menu, the selected device is listed and in the **Access** menu, the desired permission is listed.
3. In the **Comments** field, enter a message for the administrator.
4. Click **Send**.

→ The administrator receives the right change request. Once the administrator approves or declines your request, you are notified with the popup message.

Requesting for access rights for multiple devices

1. Open the **Access request** tab.
2. In the **Device** drop-down menu, select the device for which you want to request rights.
3. In the **Access** drop-down, select the desired right and click **Add**.
4. Repeat these steps for other devices.
5. In the **Comments** field, enter a message for the administrator
6. Click **Send**.

→ The administrator receives the right change request. Once the administrator approves or declines your request, you are notified with the popup message.

Requesting for access rights for certain device models (offline mode)

1. Open the **Connected devices** tab.

2. Right-click on a device or port entry for which you want to request the access right change.
3. Click **Generate request code**.
 - The **Generate request code** dialog appears.

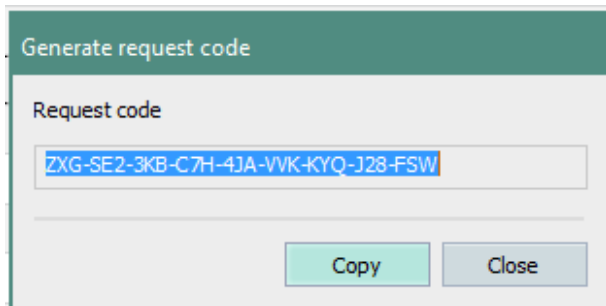


Figure 4. Generate request code

4. Click **Copy**.
 - The code is copied to the clipboard.
 5. Send the code to the administrator.
- The administrator receives the request and sends you the unblocking code, if necessary. For details, see [Entering unblocking code](#).

2.3. Controlling the use of keyboards

The usage of the keyboards other than the ones primarily connected to your computer, may be prohibited. The administrator can grant you the right to control newly connected keyboards on your own. Depending on the permission, a message appears once or every time when a keyboard is connected, where you select whether an additionally connected keyboard will be permitted or not.

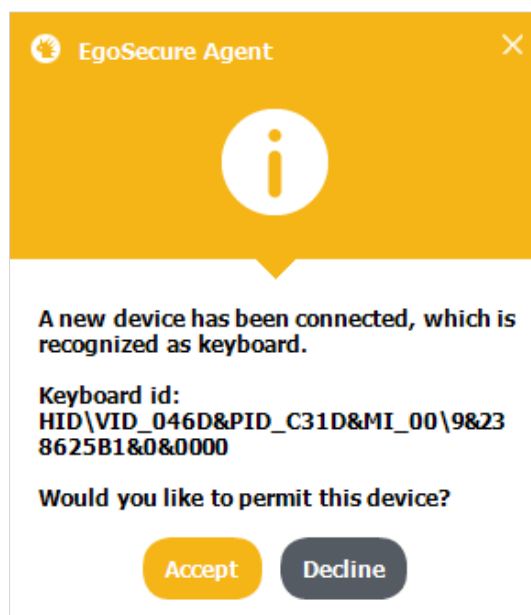


Figure 5. Keyboard control

- ◆ Click **Accept** in the pop-up dialog to permit the connected keyboard.
- ◆ Click **Decline** to block the keyboard. To change your decision later, right-click the keyboard under **Access Control | Connected devices** tab and select **Modify access** from the context menu.

3. ENCRYPTION

3.1. Overview

With encryption, you can encrypt files and folders both on the computer and on the network, as well as on external storage media and in cloud storage. Depending on the selected encryption type, the data is encrypted with a certain key. Depending on the encryption types permitted for you by the administrator, you will see the necessary keys under **Encryption | Encryption keys** tab.

There are five encryption types:

- **Common encryption:** Commonly encrypted data can be decrypted by all users who are registered on the same **EgoSecure Server** and have a 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 to which a group key has been provided.
- **Mobile encryption:** Mobile encrypted data is typically password protected and is used to transport data to external storage or cloud storage. If you have enabled mobile encryption, you can create a mobile key under **Encryption | Encryption keys** tab. For details, see [Using mobile encryption](#).
- **Permanent encryption:** Permanent encryption is used on files and folders and adds the **.espe** file extension. Unlike other encryption types, permanent encryption is preserved when copying or moving the files. For details, see [Encrypting files permanently](#).

There is no separate key for permanent encryption, it uses the keys of the other encryption types.



INFO

Encrypting individual files

Individual files can be encrypted via permanent encryption or via mobile encryption on external and optical storage media and in cloud storage. Entire folders you can encrypt only locally or on the network.

3.2. Encrypting files

If you encrypt folders locally, both included and newly added data are always automatically encrypted. For external and optical storage media as well as for cloud storage, you can set how new data must be encrypted, depending on your permissions.

Encrypting folders locally or on the network

To automatically encrypt files existing in a folder and files newly added there, enable encryption on a folder.

Encrypting local/network folder


1. Right-click a folder in Windows Explorer or on the network.
 2. Select **Define encryption type | [encryption type]** from the context menu.
 - Depending on the permissions, different encryption types are available.
- All files in the folder are automatically encrypted with the selected encryption type and key. Files newly added to the folder are automatically encrypted with the same encryption type.
 - Depending on the type of encryption, a green or yellow lock appears on the file or folder after encryption. For details see: [Identifying an encryption type via an overlay icon](#)
 - All folders encrypted with the **Folder encryption** product locally by you or remotely by the administrator are displayed under **Encryption | Encrypted folders**.

Encrypting files on external storage and in cloud

To automatically encrypt files newly added to a storage medium or cloud, select the encryption type for **external storage**, **CD/DVD encryption** or **cloud storage** encryption.

Encrypting external data

1. In the **External storage**, **CD/DVD encryption** or **Cloud storage** tab, select one of the encryption types:
 - ◆ **Common encryption**
 - ◆ **Group encryption**
 - ◆ **Individual encryption**
 2. To use mobile encryption, enable the **Activate mobile encryption** check box. For details, see: [Using mobile encryption](#)
- Newly added files and existing files that you edit and save are automatically encrypted with the selected encryption type.
 - Depending on the type of encryption, a green or yellow lock appears on the file or folder after encryption. For details see: [Identifying an encryption type via an overlay icon](#)
 - If the mobile encryption has been enabled, the **CryptionMobile.exe** application is automatically copied to the storage medium or to the cloud.

 INFO	<p>Cryption Mobile on CD/DVD disks of UDF format</p> <p>The CryptionMobileCD.exe application (for CD/DVD encryption) performs encryption operations correctly only on the disks of the ISO format. Disks of the UDF format are not supported.</p>
--	---

Encrypting files manually

Encrypt files on storage media and in clouds manually if you selected the **None** encryption type for them.

Encrypting files and folders manually

1. In the External storage, CD/DVD encryption or Cloud storage tab, select the None option.
2. Right-click a folder or a file on an external storage on in a cloud.
3. Select **Encrypt | [encryption type]**.

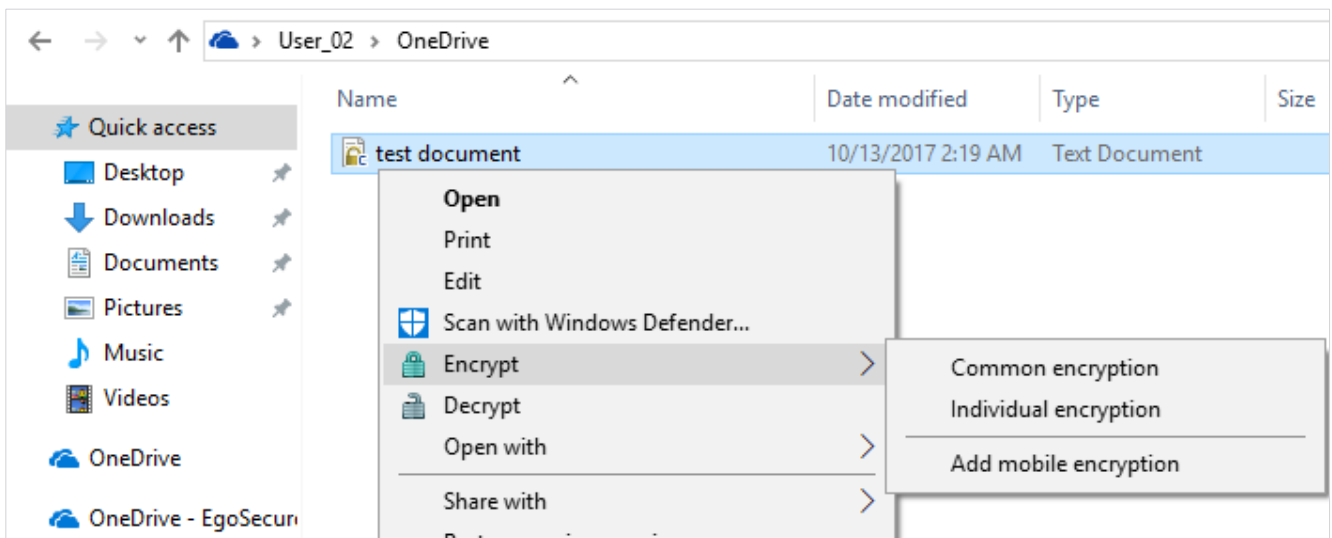


Figure 6. Encrypt file in cloud individually

→ Depending on the permissions, different encryption types are available.

- The file or folder is automatically encrypted with the selected encryption type and key.
- Depending on the type of encryption, a green or yellow lock appears on the file or folder after encryption. For details see: [Identifying an encryption type via an overlay icon](#)
- If the mobile encryption has been enabled, the **CryptionMobile.exe** application is automatically copied to the storage medium or to the cloud.
CryptionMobileCD.exe application (for CD/DVD encryption) is copied only to the disks of the ISO format, and cannot be copied to the disks of the UDF format.

Encrypting files permanently

If you encrypt a file or a folder permanently, the encryption is retained even when copying or moving the encrypted .espe file.

Encrypting files permanently

1. Right-click a file or a folder in Windows Explorer.
2. Select **Encrypt permanently | [encryption type]**.

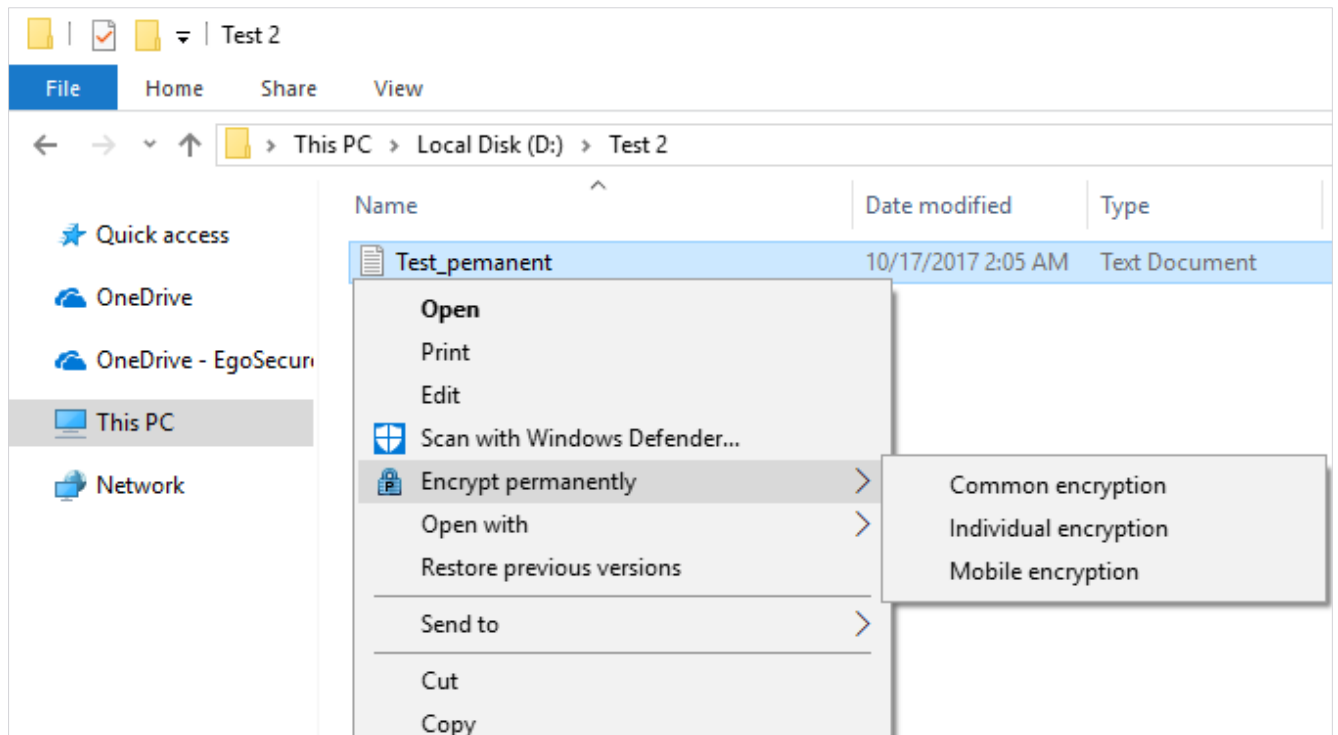


Figure 7. Permanent Encryption

→ If you encrypt a folder, the **Save As** dialog appears.

3. Select a location where to store a zipped .espe file, and then click **Save**.

➤ The file is encrypted permanently and gets the **.espe** extension; the folder is transformed to a zipped .espe archive.

Encrypting files with Post-Quantum Encryption

1. Right-click a file or a folder in the Windows Explorer.
2. Select Encrypt **permanently | Post-Quantum Encryption with password**.

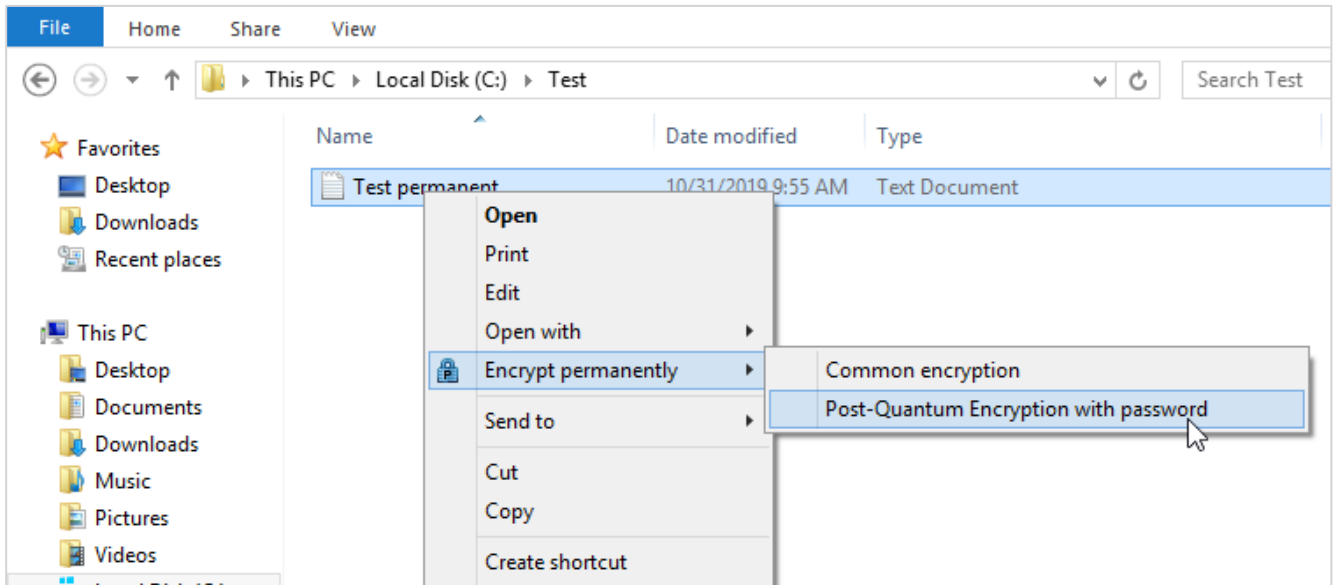




Figure 8. Post-Quantum Encryption with password

- The dialog for creating a password for the file appears.
 - 3.** Create a password and confirm it.
 - 4.** Click **OK**.
 - If you encrypt a folder, the **Save As** dialog appears.
 - 5.** Select a location where to store a zipped **.espe** file, and then click **Save**.
 - A dialog that shows encryption progress appears and encryption starts. Once the encryption finishes successfully, the dialog closes automatically.
- The file is now encrypted with Post-Quantum Encryption and gets the **.espe** extension; the folder is transformed to a zipped **.espe** archive.

Encrypting files permanently with a certificate

- 1.** Preparation: Make sure you have an access to the private key(s) that corresponds to the certificate(s).
- 2.** Right-click a file or a folder in the Windows Explorer.
- 3.** Select **Encrypt permanently | Certificate encryption** from the context menu.
 - The **EgoSecure Encryption by Matrix42** dialog appears. If you previously selected a current encryption certificate, this certificate is now displayed in the right column of the dialog.
- 4.** To encrypt with the current encryption certificate, go to step 8. To encrypt with another certificate(s), select the current certificate in the right column and remove it from the list via clicking .
- 5.** Select where a certificate is stored and click **Search**:
 - a. **Active Directory**: searches for all permitted certificates in the Active Directory. The certificate must be previously generated in the Active Directory.
 - ! When searching by e-mail, the search results show not only the certificates that contain the searched e-mail, but also the certificates of the user to which this e-mail belongs.

- b. **Windows Store:** searches for all available certificates in the Windows Store. The certificate must be previously imported to the local user store of the computer where the EgoSecure Agent is installed.
- ! Certificate requirements: the **Key Usage** field of the certificate details must contain the **Key Encipherment** and/or **Data Encipherment** value.
- 6. Select a certificate from the list. To select multiple certificates, hold down the **Ctrl** key while clicking.
- 7. Click .

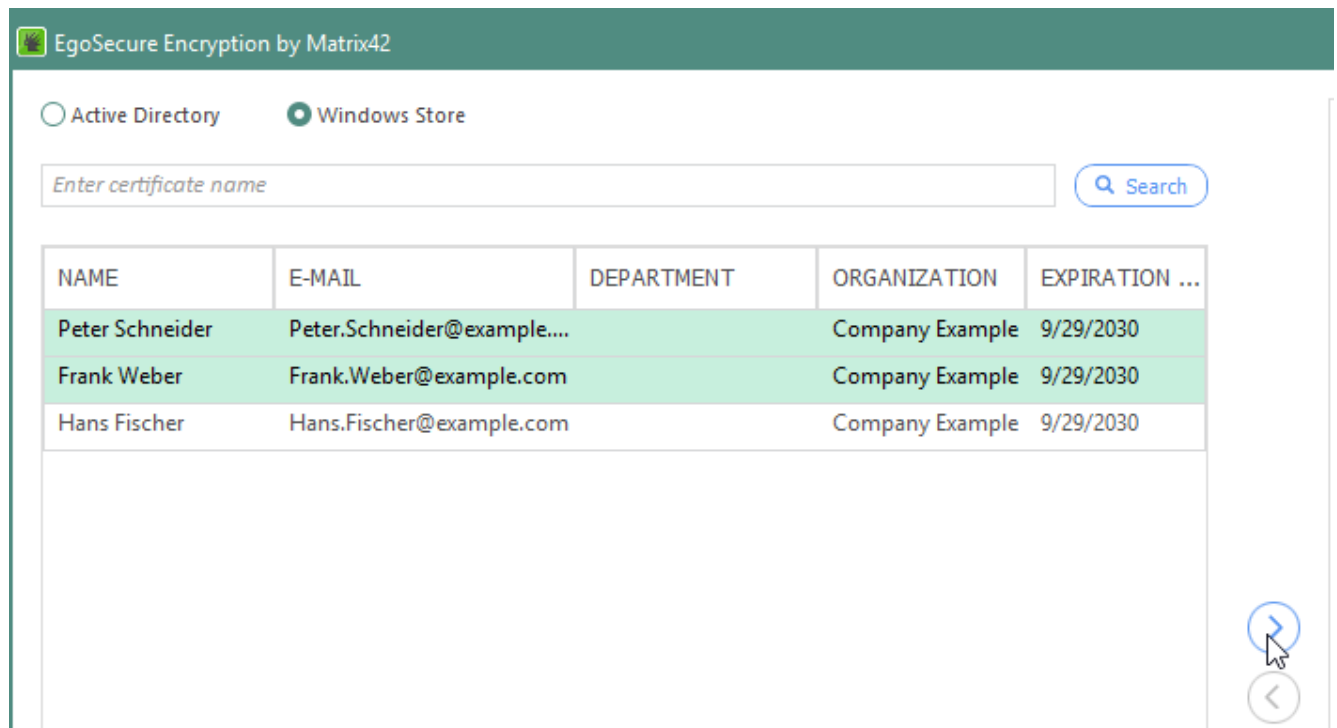


Figure 9. Selecting certificates for encryption

- 8. Click **OK** to confirm.
 - If you encrypt a folder, the **Save As** dialog appears.
- 9. Select where to store an encrypted zipped espe file and define a name for it and then click **Save**.
 - The encryption starts and the smaller **EgoSecure Encryption by Matrix42** dialog appears. Once the encryption finishes successfully, the dialog closes automatically.
- The file is encrypted with the help of the selected certificate(s). The .espe file appears instead of or in addition to the original unencrypted file/folder (depends on your permissions).

Protecting files permanently with a smart card



- 1. Preparation: Select a current signing certificate:
 - a. Go to **Encryption | Certificates**.

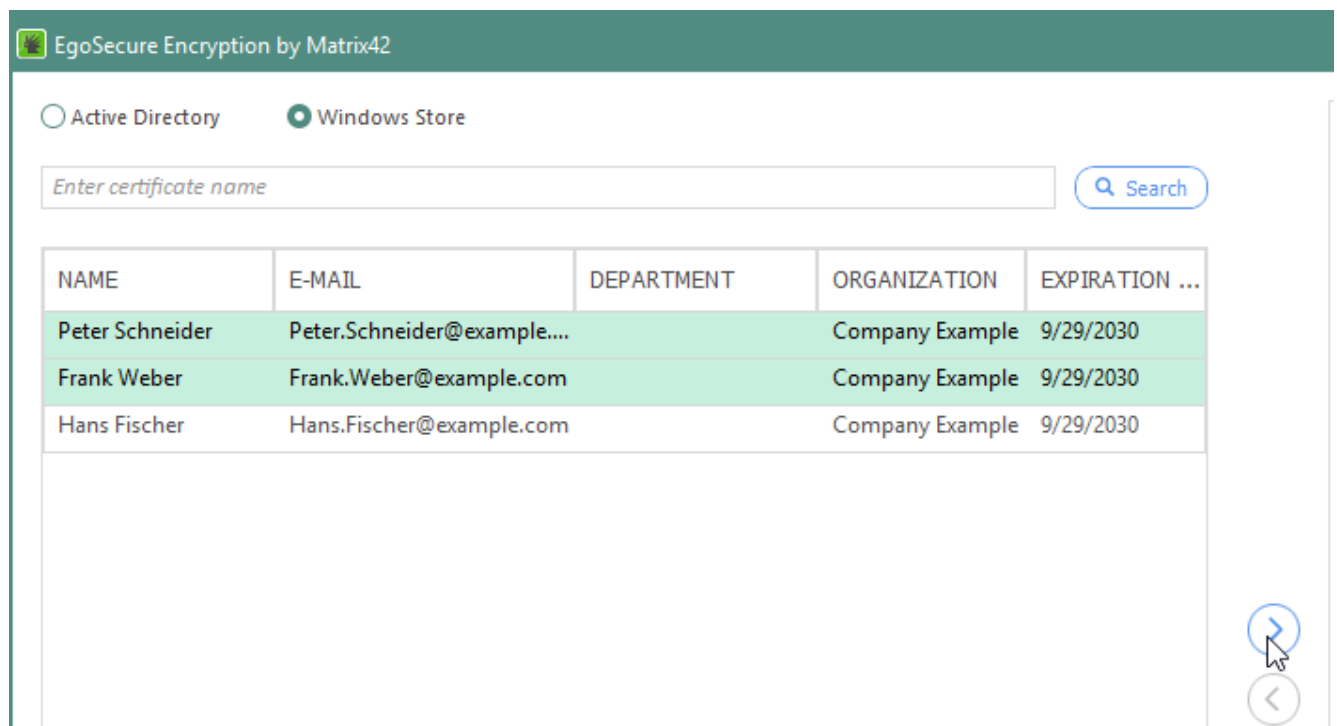
- The certificates stored in the Windows Store are displayed.
 - b. Select a certificate from the list.
The certificate must be suitable for encryption: the **Key Usage** field of the certificate details must contain the **Digital signature** value.
 - c. Click Set as current signing certificate.
2. Preparation: Make sure you have an access to the private key(s) that corresponds to the certificate(s).
 3. Right-click a file or a folder in the Windows Explorer.
 4. Select **Encrypt permanently | Certificate signing** from the context menu.
 - The dialog for providing smart card login data appears.
 5. Provide smart card login data (PIN, password, fingerprint etc.) and confirm the dialog.
 - If you encrypt a folder, the **Save As** dialog appears.
 6. Select where to store an encrypted zipped espe file and define a name for it and then click **Save**.
 - The encryption starts and the **EgoSecure Encryption by Matrix42** dialog appears. Once the encryption finishes successfully, the dialog closes automatically.
- The file is now protected via signing its certificate; the digital signature protects the file from change and spoofing.
The .espe file appears instead of or in addition to the original file/folder (depends on your permissions).
The protected file can be opened, but in case of its change, the signature becomes not valid. To check whether the file signature is verified, use the **Show encryption state** option.

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.

Encrypting files permanently with a certificate and a smart card

1. Preparation: Select a current signing certificate:
 - a. Go to **Encryption | Certificates**.
 - b. The certificates stored in the Windows Store are displayed.
 - c. Select a certificate from the list.
The certificate must be suitable for encryption: the **Key Usage** field of the certificate details must contain the **Digital signature** value.
 - d. Click **Set as current signing certificate**.
2. Preparation: Make sure you have an access to the private key(s) that corresponds to the certificate(s).
3. Right-click a file or a folder in the Windows Explorer.
4. Select **Encrypt permanently | Certificate encryption and signing** from the context menu.

- The **EgoSecure Encryption by Matrix42** dialog appears. If you previously selected a current encryption certificate, this certificate is now displayed in the right column of the dialog.
- 5. To encrypt with the current encryption certificate, go to step 9.
To encrypt with another certificate(s), select the current certificate in the right column and remove it from the list via clicking .
- 6. Select where a certificate is stored and click **Search**:
 - a. **Active Directory**: searches for all permitted certificates in the Active Directory. The certificate must be previously generated in the Active Directory.
 - b. **Windows Store**: searches for all available certificates in the Windows Store. The certificate must be previously imported to the local user store of the computer where the EgoSecure Agent is installed or the certificate must be available on the smart card.
- ! Certificate requirements: The **Key Usage** field of the certificate details must contain the **Key Encipherment** and/or **Data Encipherment** value.
- 7. Select a certificate from the list. To select multiple certificates, hold down the **Ctrl** key while clicking.
- 8. Click .



- 9. Click **OK** to confirm.
 - The dialog for providing smart card login data appears.
- 10. Provide smart card login data (PIN, password, fingerprint etc.) and confirm the dialog.
 - If you encrypt a folder, the **Save As** dialog appears.

11. Select where to store an encrypted zipped espe file and define a name for it and then click **Save**.
 - The encryption starts and the **EgoSecure Encryption by Matrix42** dialog appears. Once the encryption finishes successfully, the dialog closes automatically.
- The file is encrypted with the help of the selected certificate(s), additionally the file is protected via signing its certificate.
The .espe file appears instead of or in addition to the original unencrypted file/folder (depends on your permissions).

Selecting a current encryption certificate

1. Go to **Encryption | Certificates**.
 - The certificates stored in the Windows Store are displayed.
 2. Select a certificate from the list.
 3. Click **Set as current encryption certificate**.
- Now the selected certificate will always be suggested for encryption. For details, see [Encrypting files permanently with a certificate](#) and [Encrypting files permanently with a certificate and a smart card](#).

Adding mobile encryption

1. Right-click a file or a folder on an external storage that was commonly or individually encrypted.
 2. Select **Encrypt | Add mobile encryption**.
- The mobile encryption is added and the icon of the object changes from yellow to green.



INFO

CryptionMobile.exe will not be added

If the **Activate mobile encryption** option is not enabled and the mobile encryption is added via the context menu, the **CryptionMobile.exe** application (or CryptionMobileCD.exe – for CD/DVD encryption), used for decrypting and opening files externally, is not copied to the media. It is not possible to add the application manually, because it will be encrypted and no longer usable.

Encrypt data on storage media with one-time password

You can encrypt on external and optical storage devices independently of a mobile key. To encrypt, assign a password directly when encrypting. The password is not saved by the **EgoSecure Agent**. You can only decrypt the object with the entered password.

Encrypting files with one-time password

1. Right-click a file or a folder.
 2. Select **Encrypt | With password**.
 - A dialog box asking you to enter the password appears.
 3. Enter a password and click **OK** to confirm.
- The object is encrypted. You can decrypt it via the context menu and the entered password again.

3.3. Using mobile encryption

You can encrypt your data in clouds and on external and optical storage media additionally to protect it with a password. If you do not have permission to encrypt data on the fly, the options in the **Mobile encryption** section of the corresponding tab are greyed out and can not be activated.

Via the **CryptionMobile.exe** application or the mobile apps for iOS, Android and MacOS you externally open or decrypt data encrypted with mobile encryption. For details, see [Decrypting mobile files externally](#).

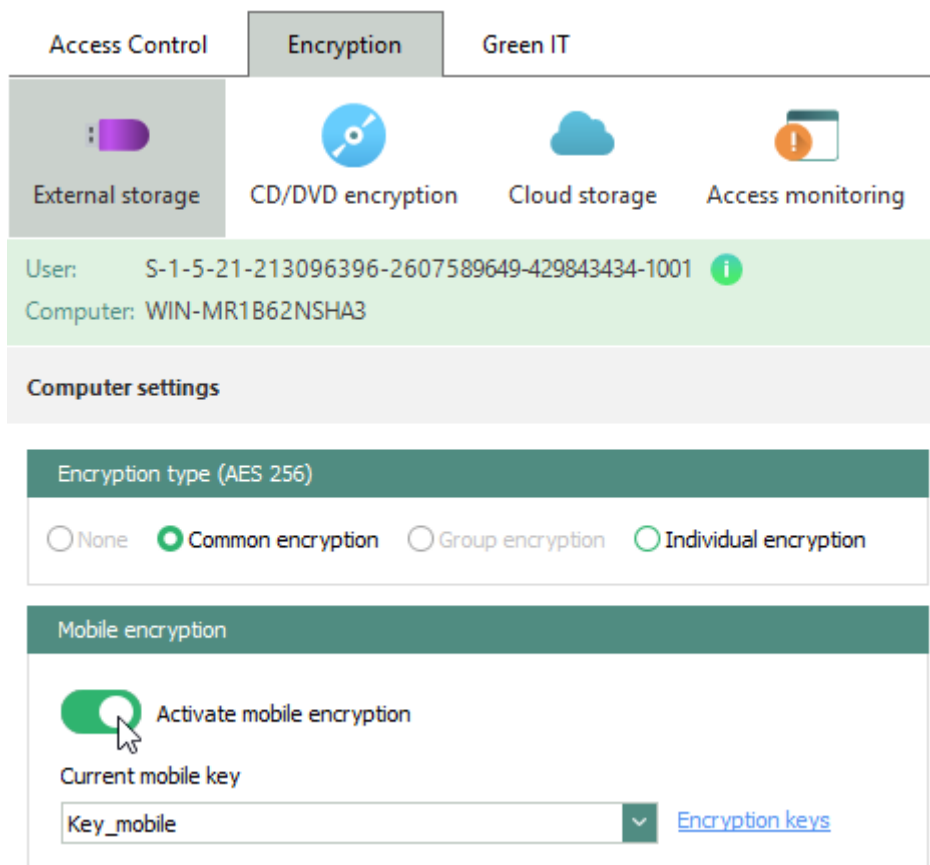


Figure 10. Permission for mobile encryption



INFO

Mobile encryption via certificate

The mobile encryption can also be controlled via a smartcard with a certificate. In this case, no password entry is possible and necessary. Contact your administrator to get the appropriate certificate.

Enabling mobile encryption

1. In the **External storage, CD/DVD encryption** or **Cloud storage** tab, enable the **Activate mobile encryption** check box. For details, see [Encrypting files on external storage and in cloud](#)
 - If you have not yet created a mobile key, the **Edit key** dialog opens.
2. Create a mobile key:
 - a. Select a key owner from the **Owner** drop-down menu (the **Owner** drop-down is available only if one encryption product is activated for a user and the other one is activated for a computer; if all encryption products are activated only for a computer (or only for a user), this menu is greyed out and **Computer** or **User** is selected automatically):
 - **Computer**. The generated key is valid for a computer (all users of a computer) to encrypt using an encryption product activated for the computer. As soon as an encryption product is deactivated on the computer, the key becomes unavailable. The key is displayed in this *Encryption keys* tab for all users of the computer where the key is generated.
 - **User**. The generated key is valid for a user to encrypt using an encryption product activated for the user. As soon as an encryption product is deactivated on the user, the key becomes unavailable. The key is displayed in the *Encryption keys* tab for one user who generated it.
 - b. In the **Title** field, enter a name for the mobile key. If necessary, select a name that can remind you of the associated password. For details, see [Show the password title](#)
 - c. Define and confirm a password for the mobile key. Depending on the configuration, you must use upper- and lower-case letters, numbers and/or special characters, and the password must have a specific minimum length. The configuration is displayed below the field.
3. Click **OK** to confirm.

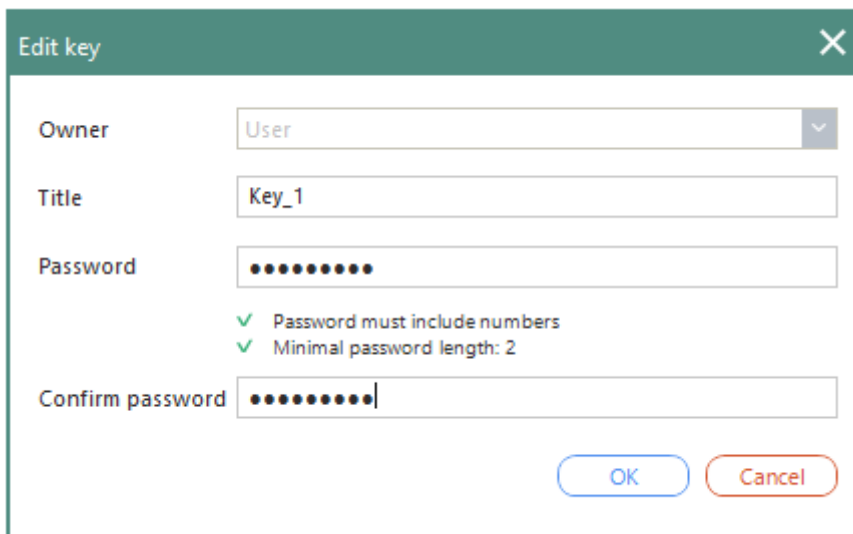


Figure 11. Specifying the name and password of a mobile key

- The new mobile key appears in the **Current mobile password** selection menu and is now used for mobile encryption. You can create any number of additional mobile keys.

Creating a new mobile key

1. Under **Encryption | Encryption keys**, click **Create** in the toolbar.
→ The **Edit key** dialog appears.
2. Select a key owner from the **Owner** drop-down menu (the **Owner** drop-down is available only if one encryption product is activated for a user and the other one is activated for a computer; if all encryption products are activated only for a computer (or only for a user), this menu is greyed out and **Computer** or **User** is selected automatically):
 - a. **Computer**. The generated key is valid for a computer (all users of a computer) to encrypt using an encryption product activated for the computer. As soon as an encryption product is deactivated on the computer, the key becomes unavailable. The key is displayed in this *Encryption keys* tab for all users of the computer where the key is generated.
 - b. **User**. The generated key is valid for a user to encrypt using an encryption product activated for the user. As soon as an encryption product is deactivated on the user, the key becomes unavailable. The key is displayed in the *Encryption keys* tab for one user who generated it.
3. In the **Title** field, enter a name for the mobile key. If necessary, select a name that can remind you of the associated password. For details, see [Show the password title](#)
4. Define and confirm a password for the mobile key. Depending on the configuration, you must use upper- and lower-case letters, numbers and/or special characters, and the password must have a specific minimum length. The configuration is displayed below the field.
5. Click **OK** to confirm.

➤ The generated key appears in the list of the keys.

Edit the password of a mobile key

1. Under **Encryption | Encryption keys**, select the mobile key which password you want to edit.
2. Click **Edit** on the toolbar.
→ The **Edit key** dialog appears.
3. Define a password for the mobile key. Depending on the configuration, you must use upper- and lower-case letters, numbers and/or special characters, and the password must have a specific minimum length. The configuration is displayed below the field.
4. Click **OK** to confirm.
5. In the **Status** column, the **Password is being modified...** entry appears for several seconds.

TITLE	KEY	SIZE	OWNER	STATUS
-	Group key	4096	Software architecture	Ready
-	Group key	4096	GUI development	Ready
-	Group key	4096	Drivers	Ready
-	Group key	4096	123	Ready
-	Group key	4096	Chief development	Ready
-	Group key	4096	Application development	Ready
Key_1	Mobile key	4096	WIN-MR1B62NSHA3	Ready
Key_mobile	Mobile key	4096	WIN-MR1B62NSHA3	Ready

Figure 12. Overview of available keys

➤ The status of the key is now **Ready**. The password has been updated.

3.4. Opening or decrypting encrypted data

Encrypted objects are marked in Windows Explorer with so-called overlay icons. Overlay icons appear on encrypted folders or files in Windows Explorer when **EgoSecure Agent** or **myEgoSecure** is on the computer.

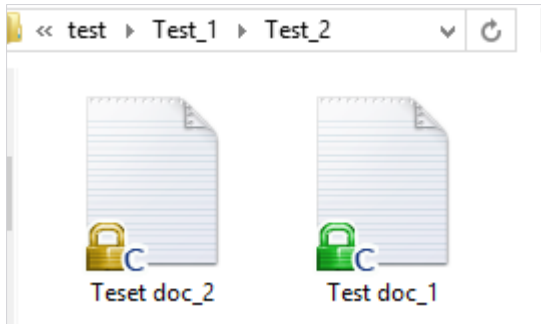


Figure 13. Encrypted files in Windows Explorer

Identifying an encryption type via an overlay icon

Icon	Description
	Encrypted with a common key. The object can be decrypted on any computer that has EgoSecure Agent or myEgoSecure installed and the valid key is available.
	Encrypted with an individual key. The object can be decrypted on any computer that has EgoSecure Agent or myEgoSecure installed and the valid key is available.
	Encrypted with a group key. The object can be decrypted on any computer that has EgoSecure Agent or myEgoSecure installed and the valid key is available.
	Encrypted with a common and a mobile key. The object can be decrypted with the mobile password on the current computer and via password with CryptionMobile.exe (or with CryptionMobileCD.exe) on computers without EgoSecure products.
	Encrypted with an individual and a mobile key. The object can be decrypted with the mobile password on the current computer and via password with CryptionMobile.exe (or with CryptionMobileCD.exe) on computers without EgoSecure products.
	Encrypted with a group and a mobile key. The object can be decrypted with the mobile password on the current computer and via password with CryptionMobile.exe (or with CryptionMobileCD.exe) on computers without EgoSecure products.
	The object was encrypted with a key that is not available on the computer, or a password was used instead of a key to encrypt it.
	Encrypted permanently. The object can be decrypted on all computers, where the EgoSecure Agent is installed and the valid key is available.

Due to the Windows configuration, it may happen that overlay icons on folders in Explorer are not displayed.

Showing encryption state

1. Right-click a folder.

→ The context menu opens. If the **Show encryption state** option is available, the folder is encrypted.

2. Click Show encryption state.

→ The **encryption state** dialog appears. In the **Encryption type** column, you can see with which encryption type the folder was encrypted.

Opening encrypted files

◆ Double-click an encrypted file, for which you have the key.

→ The file opens in its usual application. You can edit and save the file.



INFO

Editing permanently encrypted files

Permanently encrypted files open as read-only.

- ◆ To apply changes to permanently encrypted files, save them in unencrypted original format.

Decrypting files locally

Decrypting encrypted folders

1. Right-click an encrypted folder, for which you have the key.

2. Select Deactivate encryption.

→ The folder is decrypted. Files copied and created there will no longer be automatically encrypted.

Decrypting encrypted folders on external storage

1. Right-click an encrypted object (file or folder), for which you have a valid key or a key is located on a storage medium or in a cloud.

2. Select **Decrypt**.

→ The object is decrypted.

Decrypting permanently encrypted files

1. Right-click a permanently encrypted file with the **.espe** extension.

2. Select **Encrypt permanently | Decrypt** from the context menu.

If you encrypted a file using the **Certificate encryption** or **Certificate encryption and signing** option, make sure you have access to the private part of the certificate used for file encryption.

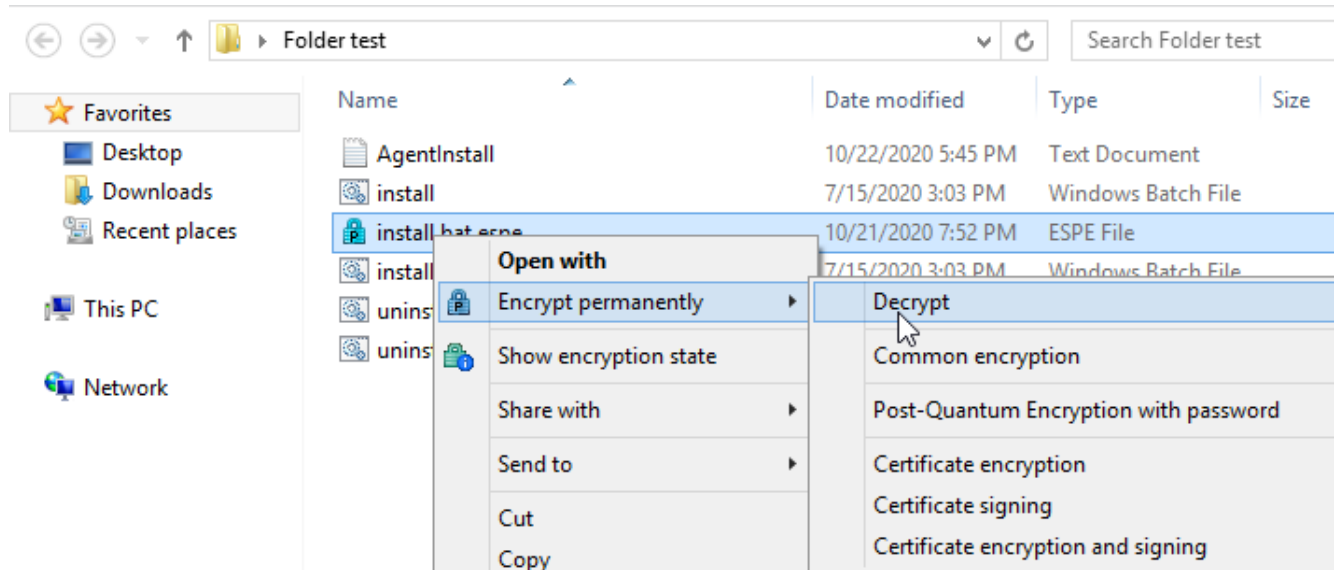



Figure 14. Decrypting permanently encrypted files

→ The decryption starts and the **EgoSecure Encryption by Matrix42** dialog appears. Once the decryption finishes successfully, the dialog closes automatically.

➤ The file is decrypted. The unencrypted file appears in addition to or instead of the **.espe** file (depends on your permissions).



INFO

Editing permanently encrypted files

Permanently encrypted files open as read-only with a double-click.

- ◆ To apply changes to permanently encrypted files, save them in unencrypted original format.

Decrypting permanently encrypted folders

1. Right-click a permanently encrypted file with the **.zip.espe** extension.
 2. Select **Encrypt permanently | Decrypt** from the context menu.
 If you encrypted a file using the **Certificate encryption** or **Certificate encryption and signing** option, make sure you have access to the private part of the certificate used for file encryption.
 - The **Browse For Folder** dialog appears.
 3. Select where to save a decrypted folder.
 4. Click **OK** to confirm.
 - The decryption starts and the **EgoSecure Encryption by Matrix42** dialog appears. Once the decryption finishes successfully, the dialog closes automatically.
- The folder is decrypted and is now stored in the selected location. The encrypted **.zip.espe** file is either automatically deleted or remains (depends on your permissions).



INFO

Editing permanently encrypted folders

Permanently encrypted folders (files with .zip.espe extension) are fully decrypted when opening them with the Cryption Informer.

Decrypting files encrypted with Post-Quantum Encryption

1. Right-click a Post-Quantum-encrypted file with the **.espe** extension.
2. Select **Encrypt permanently | Decrypt Post-Quantum Encryption** from the context menu.
 - The dialog for entering the password that is used to encrypt this file appears.
3. Enter the password.
4. Click **OK**.
 - The password dialog closes. A dialog that shows decryption progress appears and decryption starts. Once the decryption finishes successfully, the dialog closes automatically.

→ The file is decrypted. The **.espe** extension disappears.



INFO

Editing Post-Quantum-encrypted files

Post-Quantum-encrypted files open as read-only.

- ◆ To apply changes to Post-Quantum-encrypted files, save them in an unencrypted original format.

Decrypting mobile files externally

Decrypt the files encrypted with mobile encryption:

- On computers without **EgoSecure** applications: with **CryptionMobile.exe** or **CryptionMobileCD.exe**,
- On computers with **EgoSecure Agent** or **myEgoSecure**: via attaching or importing the mobile key with the same password,
- On iOS and Android devices: via the **EgoSecure Encryption Anywhere** (for iOS und Android) and by attaching the mobile key with the same password.



INFO

Cryption Mobile in connection with others EgoSecure applications

The **CryptionMobile.exe** (and **CryptionMobileCD.exe**) application can NOT be started on computers where the **EgoSecure Agent** or **myEgoSecure** are installed with any encryption module activated.

To open encrypted files via **Cryption Mobile** on an external computer where there is an Agent without its mobile key exists, the Guest encryption must be enabled. Contact the EgoSecure Console administrator for this.

Decrypting mobile files on other computers

1. Double-click *CryptionMobile.exe*

→ The dialog for entering a password opens.

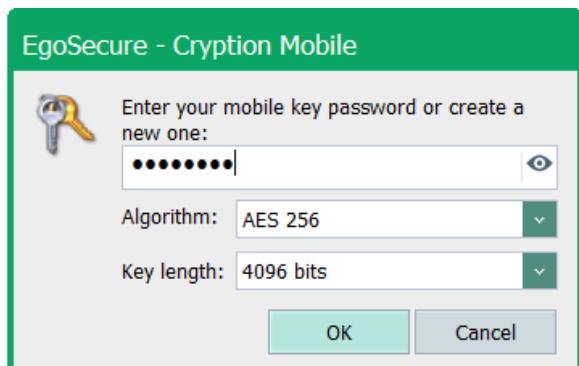


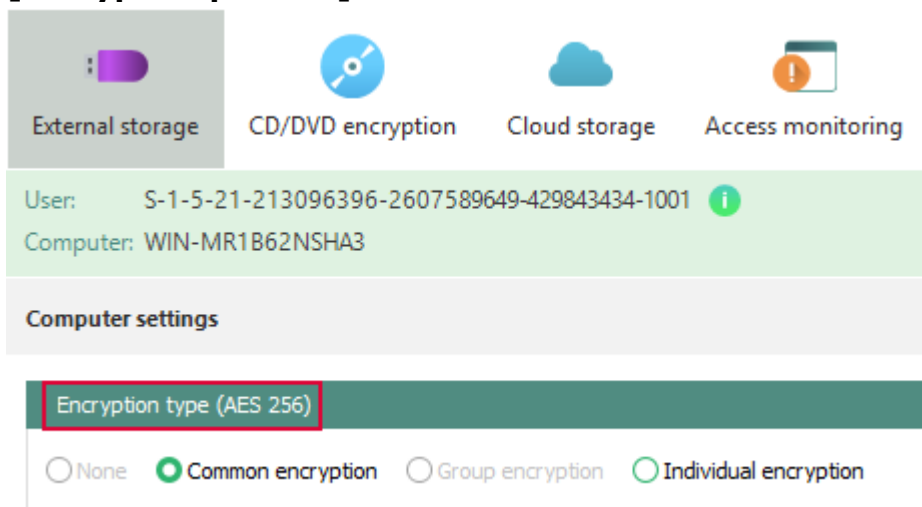
Figure 15. Entering mobile password for Cryption Mobile

2. Enter the mobile password, with which the files were encrypted.

3. In the **Algorithm drop-down, select an encryption algorithm used for file encryption:**

- AES 256.
- AES 256 (OAEP, SHA256).
- Triple DES.
- **Post-Quantum**. Used for files encrypted with **EgoSecure Post-Quantum Encryption** based on the *Kyber-1024* encryption method.
- **GOST**. Used for files encrypted with the *GOST 28147-89* encryption method.
! This method is displayed in the **Key length** drop-down list only if the GOST provider is found on your computer.

Select **Default** to use the encryption algorithm defined by your administrator. The value defined by the administrator is displayed in the Agent under **Encryption | [encryption product]**:



4. In the **Key length** drop-down, select an encryption key length used for file encryption.
 Select **Default** to use the key length defined by your administrator. The value defined by the administrator is displayed in the Agent under **Encryption | Encryption keys** in the **Length** column for the administrator-owned keys (non-editable ones).
5. Click **OK**.
 → **Cryption Mobile** opens.

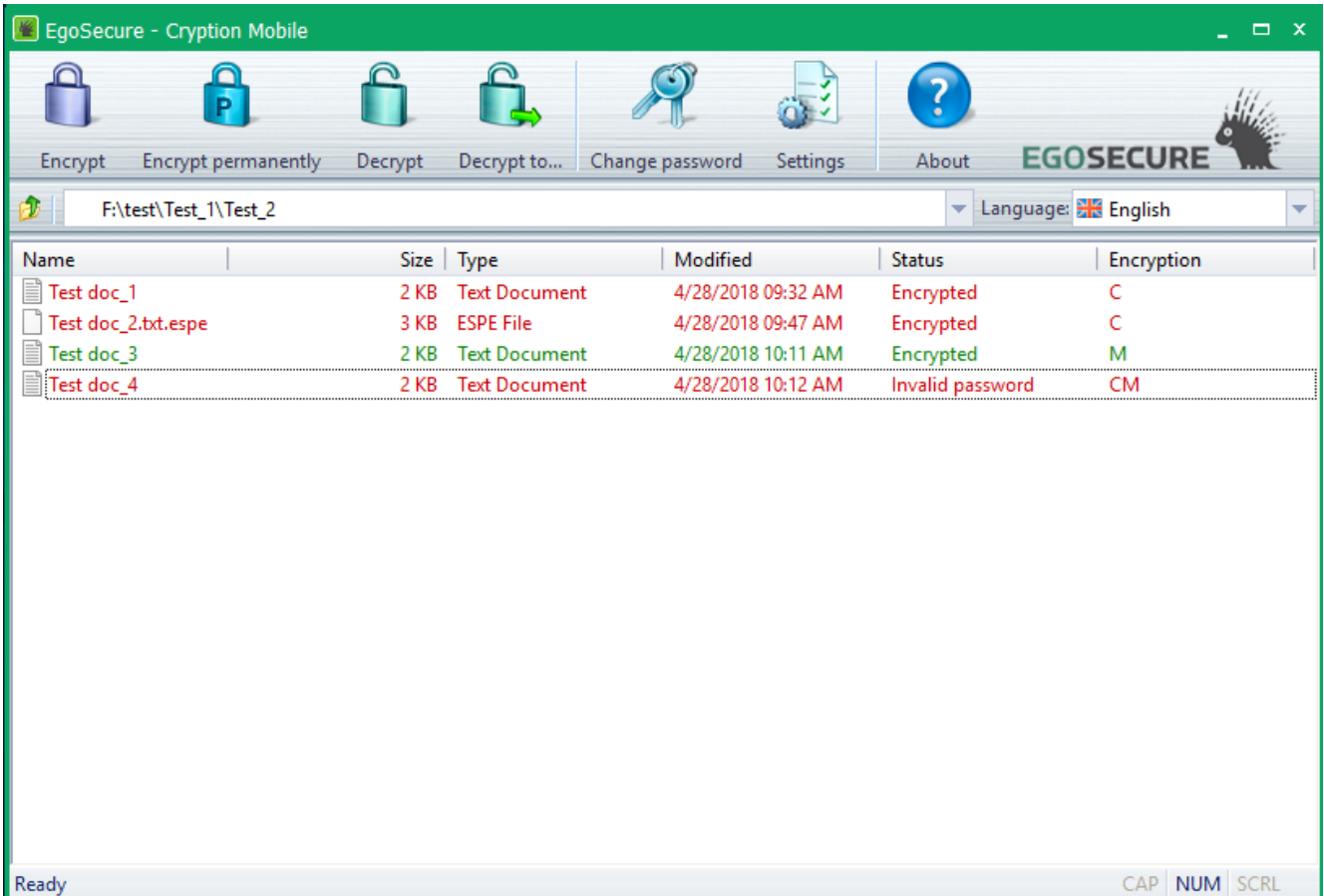


Figure 16. Cryption Mobile

6. Select the files which you want to decrypt.
 7. Click in the toolbar on
 - a. **Decrypt**, to decrypt files on the external storage
 - b. **Decrypt to...**, to save decrypted files to another location.
- The file is decrypted and the file status changes.

Decrypt mobile encrypted files in clouds on iOS or Android device

1. Download the **EgoSecure Encryption Anywhere** (for iOS or for Android). Depending on the configuration, download links can be found in the **External storage** or **Cloud storage** tabs via the Android and iOS buttons.
2. Open the application.

3. Enter the password for the mobile key and the data to access the cloud.

➤ You can now download and decrypt files from the cloud.

Reminding password name of an encrypted file

If you forgot the password of a file encrypted with a mobile key, you can see a reminder of its name.

Showing password name

1. Right-click the encrypted file, for which you forgot a password.
2. Select **Remind password** from the context menu.

➤ A dialog box showing you the name of the used password appears.

3.5. External access to encrypted files

Depending on the configuration, you may receive notifications when another user tries to access your encrypted data. In this case, the **Access monitoring** tab becomes available under **Encryption**.

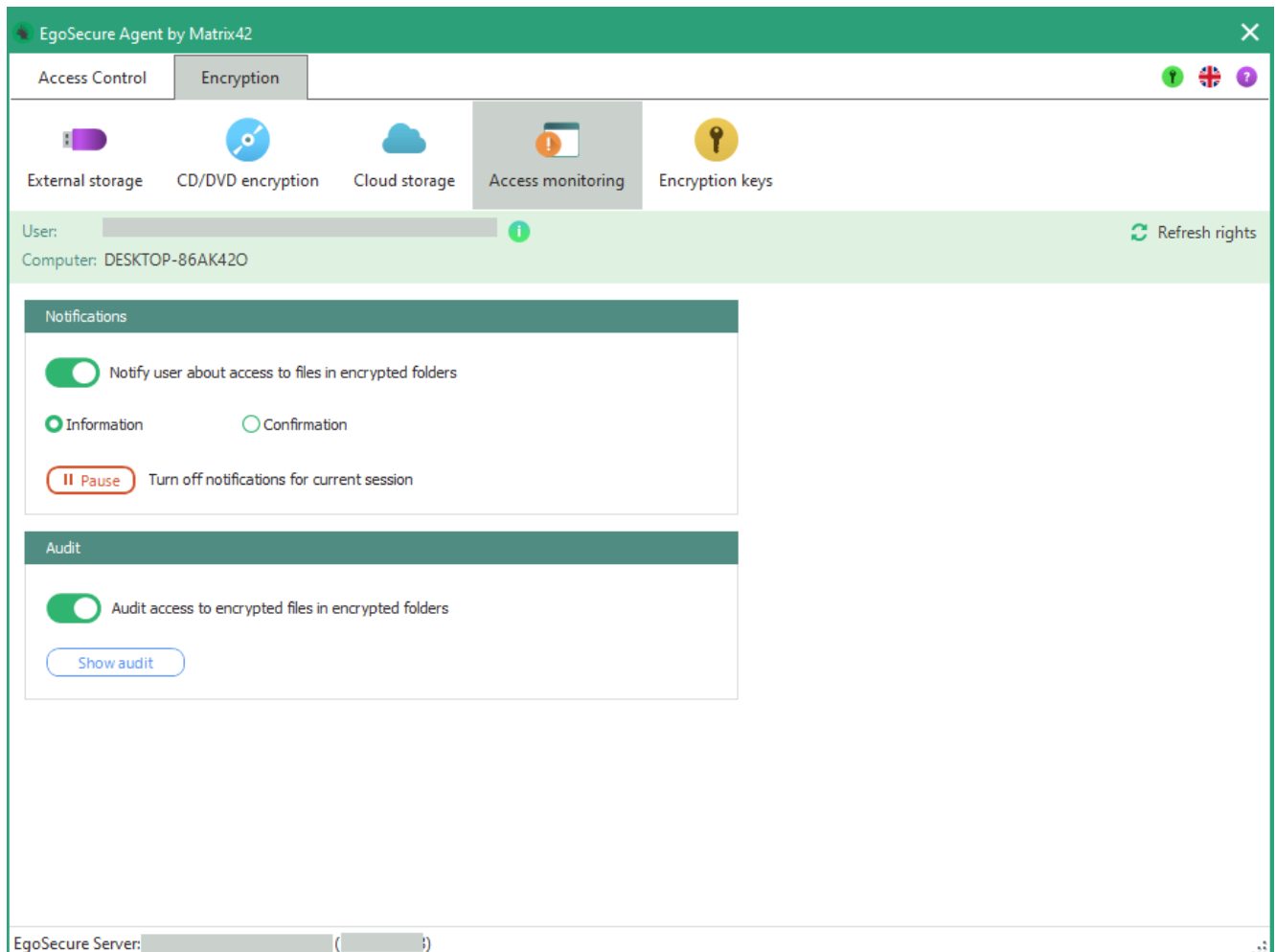


Figure 17. Access monitoring tab

Receiving notifications for third-party access

In the **Access monitoring** tab, you can specify whether and in what form you want to receive messages about external access and whether third-party access should be audited. Only the access from computers where the Agent is installed is monitored. You can also grant access to certain content once or always. For details, see [Showing confirmation messages about data access](#).

Displaying information messages about data access

1. Enable the **Notify users about access to files in encrypted folders** option.
2. Enable the **Information** radio button.
 - The following message appears in case of third-party access:

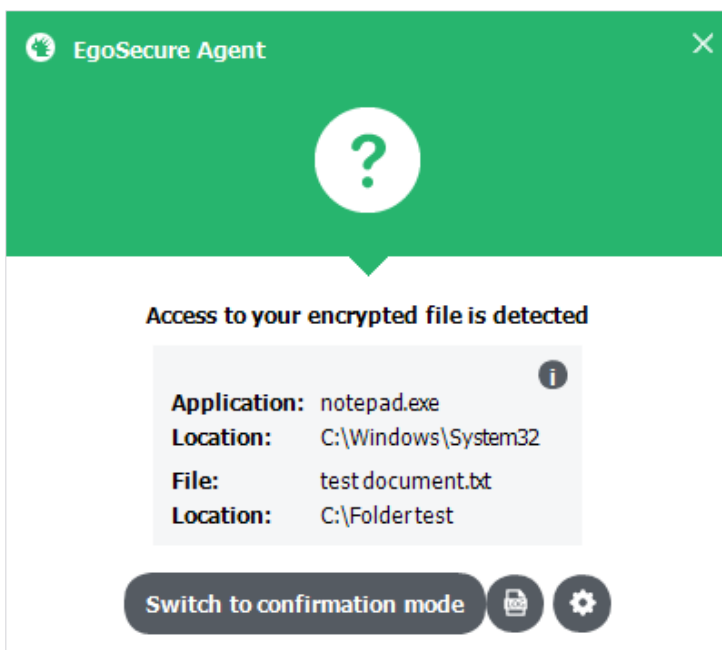


Figure 18. Information message about access to encrypted data

3. Close the message.
 - The access to the file remains blocked and the accessing user is informed. The message appears again when accessing the next time.

Showing confirmation messages about data access

1. Enable the **Notify users about access to files in encrypted folders** option.
2. Enable the **Confirmation** radio button.
 - The following message appears in case of third-party access. If you close the dialog without selection, the access to files is denied once. The accessing user is informed about it. The message appears again when accessing the next time.

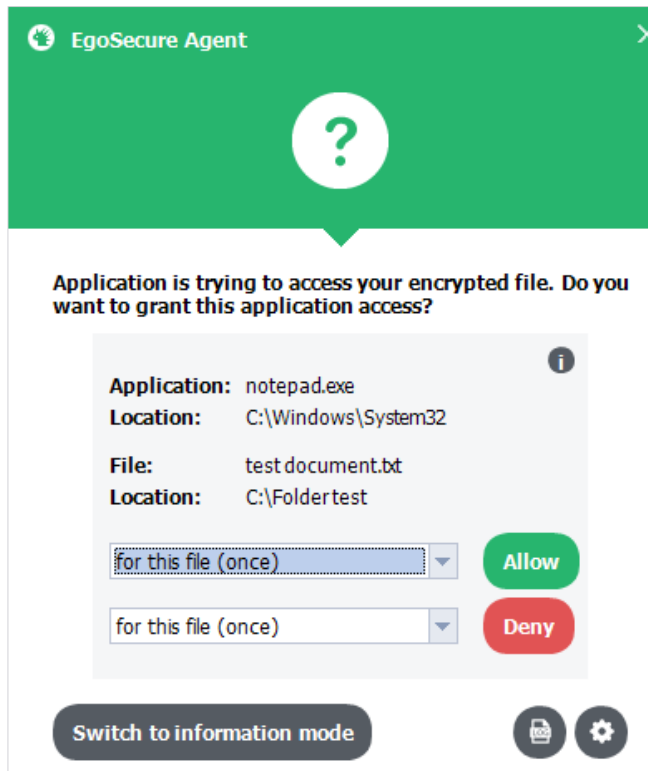



Figure 19. Confirmation message about access to encrypted data

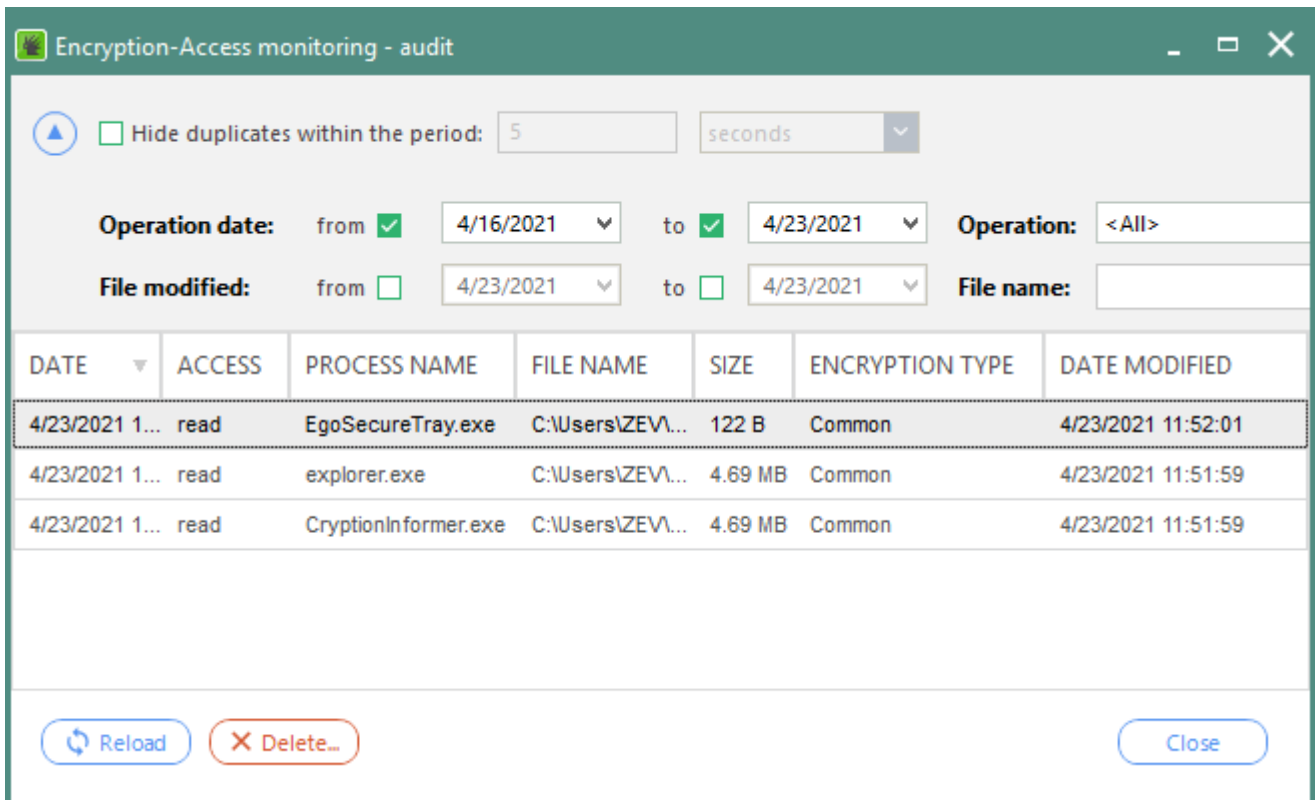
3. Decide about the access:
 - a. Near **Allow**, select in the drop-down menu, whether to permit an unknown user to access the file/whole folder once or permanently and click **Allow**.
 - b. Near **Deny**, select in drop-down menu, whether to forbid an unknown user to access the file/whole folder once or permanently and click **Deny**.

➤ Depending on the selection, the access is granted or denied and the notification dialog closes.

Auditing third-party access

Auditing access

1. Enable the **Audit access to encrypted files in encrypted folders** option.
 2. After a file access, click **Show audit** in the **Access monitoring** tab or click  in the notification message to view the log.
- The **Encryption – Access monitoring – audit** dialog opens. You can filter the log entries by date, access type, file size or file name.



Encryption-Access monitoring - audit

Hide duplicates within the period: seconds

Operation date: from 4/16/2021 to 4/23/2021 Operation:

File modified: from 4/23/2021 to 4/23/2021 File name:

DATE	ACCESS	PROCESS NAME	FILE NAME	SIZE	ENCRYPTION TYPE	DATE MODIFIED
4/23/2021 1...	read	EgoSecureTray.exe	C:\Users\ZEV\...	122 B	Common	4/23/2021 11:52:01
4/23/2021 1...	read	explorer.exe	C:\Users\ZEV\...	4.69 MB	Common	4/23/2021 11:51:59
4/23/2021 1...	read	CryptionInformer.exe	C:\Users\ZEV\...	4.69 MB	Common	4/23/2021 11:51:59

Reload Delete... Close

Figure 20. Access log

4. ANTIVIRUS

4.1. Overview

EgoSecure Antivirus protects the computer from viruses, Trojans and other malware. In the **Antivirus** tab, you can see your protection status. The real-time protection monitors all active processes and identifies potential threats. You can also see the status of the version of the virus signatures and when they were last updated.

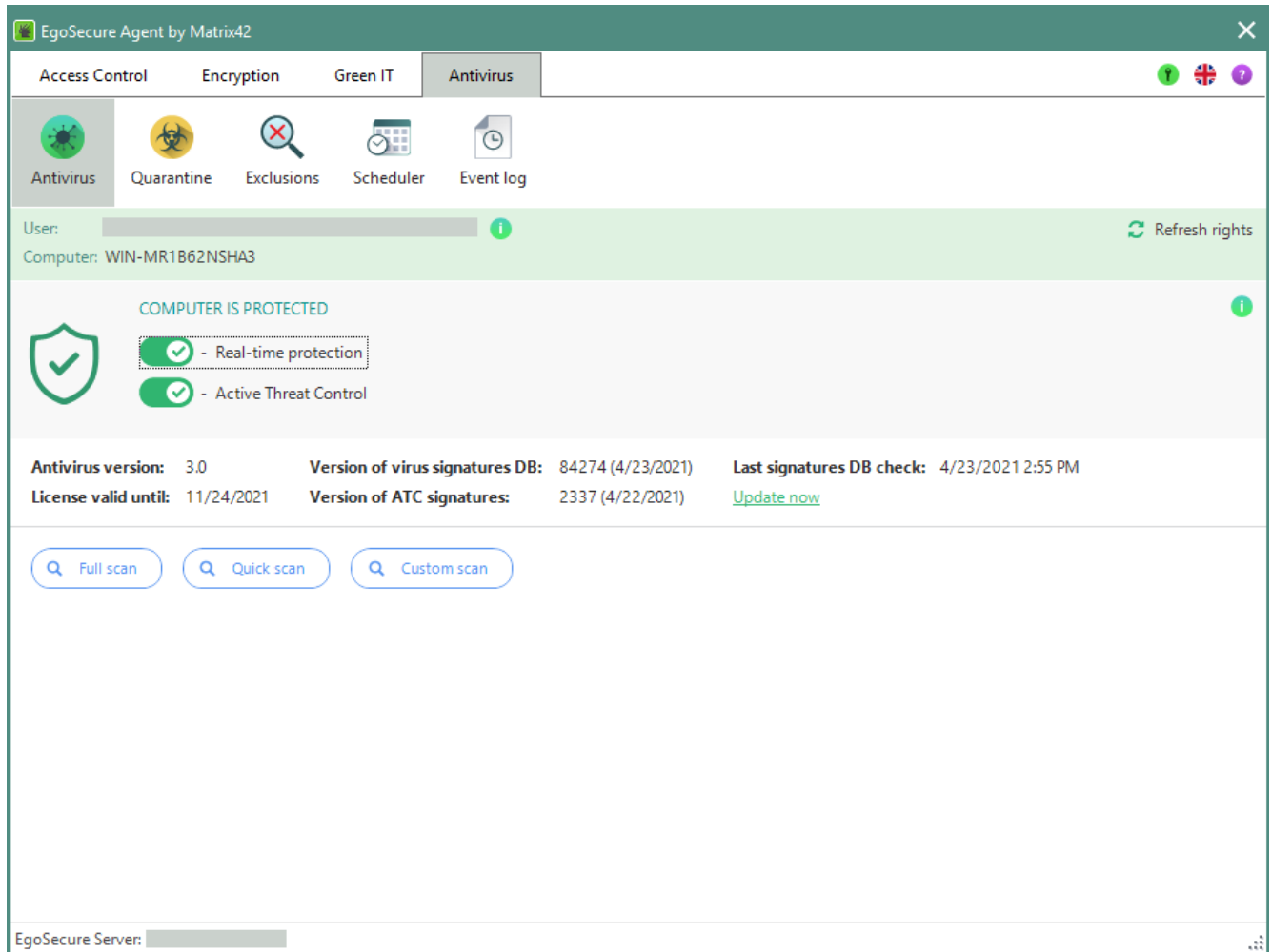


Figure 21. Antivirus module

4.2. Starting a scan

- ◆ Start a manual scan by clicking one of the buttons in the **Antivirus** tab:

Scan type	Description
Full scan	Scans all internal and external drives.
Quick Scan	Scans only system directories.
Custom Scan	Scans all directories, which you select in a dialog window.

- ◆ To scan certain files, right-click the file in Windows Explorer and select **Scan with EgoSecure Antivirus** from the context menu.

4.3. Managing quarantined objects

In the **Antivirus | Quarantine** section you can determine how **Antivirus** handles infected or suspicious objects that have been manually or automatically quarantined.



INFO

Network files not moved to quarantine

Network files are not moved to the quarantine, the access to them is blocked instead.

Restoring quarantined objects to their original location

1. Select an infected or suspicious object.
To select multiple entries at the same time, hold down the **Ctrl** key while clicking.
 2. Click **Restore** on the toolbar.
- The object is moved from the quarantine to its original location.

Restoring quarantined objects to certain location

1. Right-click one or multiple objects.
2. Select **Restore to...** from the context menu.

The screenshot shows the Matrix42 Antivirus interface with the 'Quarantine' tab selected. Below the navigation bar, there is a status bar showing 'User: [redacted]' and 'Computer: WIN-MR1B62NSHA3'. A toolbar contains 'Restore' and 'Delete' buttons. Below the toolbar is a table of quarantined files:

TIME	REASON	NAME	PATH
4/23/2021 3:24:23 PM	spyware.BD.TestSign...	dummyscan_spyware.txt	C:\Users\ZEVI\Desktop
4/23/2021 3:23:43 PM	d		C:\Users\ZEVI\Desktop\
4/23/2021 3:23:43 PM	a		C:\Users\ZEVI\Desktop\
4/23/2021 3:23:41 PM	a		C:\Users\ZEVI\Desktop\
4/23/2021 3:23:35 PM	spyware.BD.TestSign...	dummyscan_spyware.txt	C:\Users\ZEVI\Desktop\

A context menu is open over the first row, showing the following options: Restore, Restore and exclude from scanning, Restore to ..., and Delete. The 'Restore to ...' option is highlighted by the mouse cursor.

Figure 22. Restoring quarantined objects

- The **Browse for folder** dialog appears.
3. Select the location for the quarantined object.
 4. Click **OK** to confirm.
- The objects are moved from the quarantine to the selected location.

Restoring quarantined object and adding to exclusions

1. Right-click an object.
 2. Select **Restore and exclude from scanning**.
- The item is moved from quarantine to the selected location and added to the list of exclusions. See also: [Defining exclusions](#).

Deleting quarantined objects

1. Select an infected or suspicious object.
To select multiple entries at the same time, hold down the **Ctrl** key while clicking.
2. Click **Delete**.

➤ The object is deleted from quarantine and its location on the computer.

4.4. Defining exclusions

In **Antivirus | Exclusions**, specify files which are not scanned by Antivirus.

Excluding a file from Antivirus scan

1. Click **Files and processes** on the toolbar.
2. Click **Add file** on the toolbar.
→ The **Open** dialog appears.
3. Select a file and click **Open**.

➤ The file path appears in the list of exceptions. The file will be excluded from future scans.

Excluding a folder from Antivirus scan

1. Click **Files and processes** on the toolbar.
2. Click **Add folder** on the toolbar.
→ The **Browse for folder** dialog appears.
3. Select a folder.
4. Confirm with **OK**.



➤ The directory path (with an asterisk symbol *) appears in the list of exceptions. The folder will be excluded from future scans.

Excluding a process from Antivirus scan



1. Click **Processes** on the toolbar.
2. Click **Add process** on the toolbar.
→ The **Open** dialog appears.
3. Select a process.
4. Click **Open**.
5. Clear the **Check for certificate** check box if the process doesn't have a valid certificate.

➤ All the files accessed by selected process will be excluded from scans.

Removing items from the exception list

1. Select an entry.
To select multiple entries at the same time, hold down the **Ctrl** key while clicking.
2. Click **Delete** on the toolbar.
You are allowed to delete only your own exclusions with  icon, administrator exclusions  can not be deleted.

Editing the exception list files/paths manually

1. Double-click an entry. You are allowed to edit only your own exclusions with  icon, administrator exclusions  can not be edited.

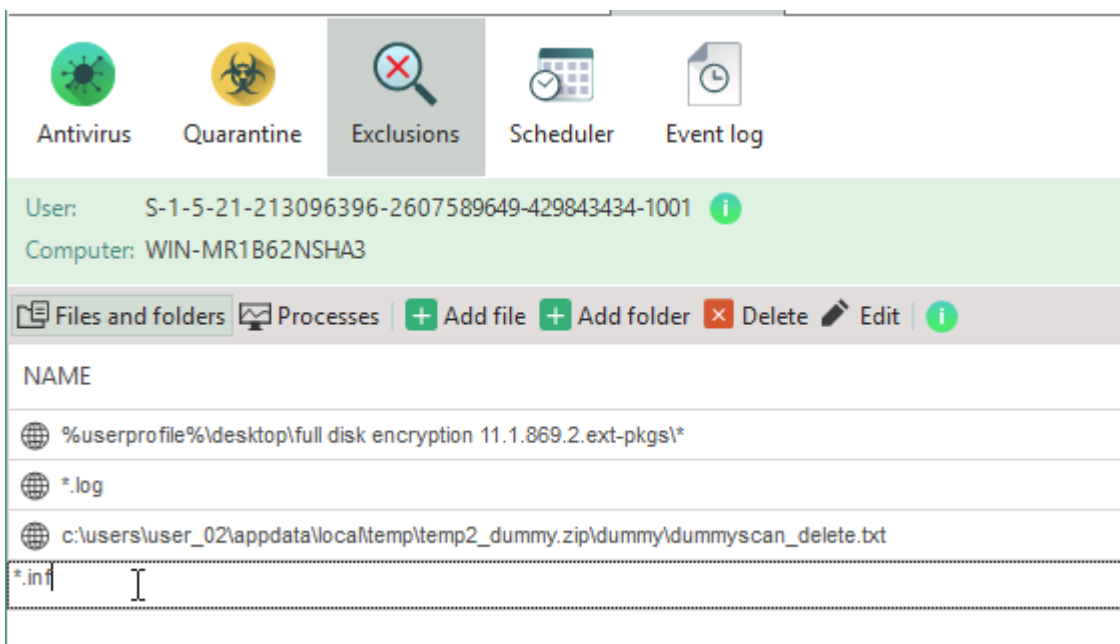


Figure 23. Editing exclusion entries

2. Edit the entry. You can use wildcards and system variables. Click the icon on the toolbar to see examples:

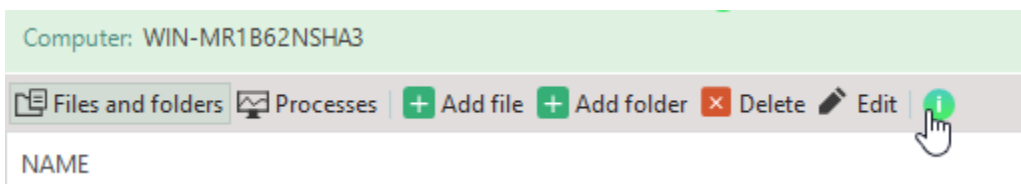



Figure 24. Viewing information about wildcards

3. Click an empty area to apply the changes.
 The files and file paths defined as exclusions will be disregarded from the next scan with **EgoSecure Antivirus**.

4.5. Planning scans

Under **Antivirus | Scheduler** you can perform scans automatically at certain time. You can disable, delete, or edit scheduled scans by adding additional items to scan or by changing the scan time.

Creating a task

1. Click **Create** in the toolbar.
→ The **New task** dialog appears.

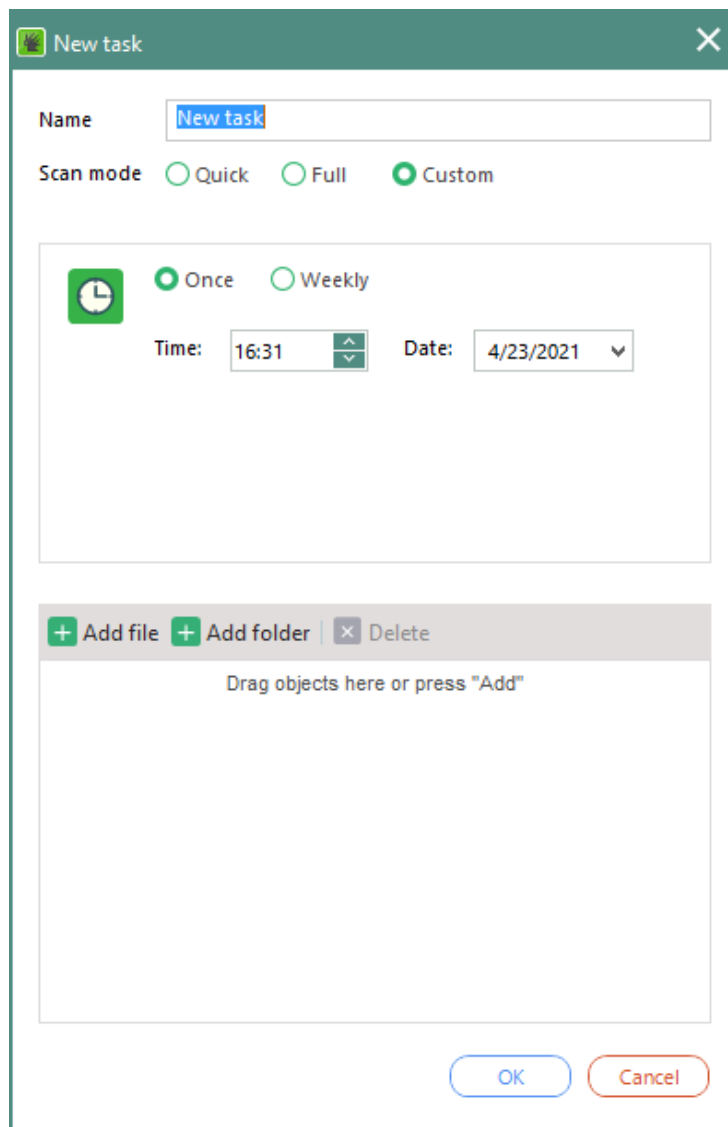


Figure 25. Planning automatic scans

2. In the **Name** field, enter a task name.
3. Select a scan mode. For details, see [Starting a scan](#).
4. Define a time period for a task.
5. If you have selected **Custom**, select the objects which you want to scan. Click **Add file** or **Add folder**.

6. Click **OK** to confirm.

➤ The task appears in the list. In the **Description** column you can see the scan summary.

Editing a task

1. Double-click a task or select a task and click **Edit** on the toolbar.
You are allowed to edit only your own tasks; administrator tasks are greyed out and cannot be edited.
2. Make the changes.
3. Click **OK** to confirm.

Disabling a task

- ◆ Clear the checkbox of the **Active** column of the necessary task.
You are allowed to disable only your own tasks; administrator tasks are greyed out and cannot be edited.

Deleting a task

1. Select an entry.
To select multiple entries at the same time, hold down the **Ctrl** key while clicking.
2. Click **Delete** on the toolbar.
You are allowed to delete only your own tasks; administrator tasks are greyed out and cannot be deleted.

4.6. Managing logs

Under **Antivirus | Event log** you can see logs, created by Antivirus.

Log selection

- **Events**: displays running or failed antivirus databases updates
- **Scans**: shows the list of all antivirus scans
- **Threats**: displays all detected threats and actions performed with them

Clearing event log

1. In the **Log** menu, select which log to display.
2. On the right pane above the list, click **Clear event log**.
OR
3. Right-click an entry and select **Clear event log** from the context menu.
→ The **Delete old data** dialog appears.
4. In the **Delete data older than** menu, select a time period:
 - a. E.g.: select **1 week** to delete all data older than one week.
 - b. Select **All time** to delete all data from logs

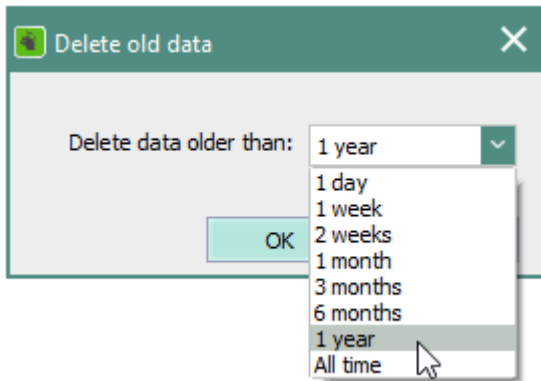


Figure 26. Selecting time period

5. Click **OK** to confirm.

➤ Events data is deleted from all three tabs (events, scans, threats).

5. GREEN IT

5.1. Overview

Green IT lets you configure your computer to consume energy only when the computer is actually in use. You can set and schedule actions that take place at specific time or when the specified idle time is exceeded. In addition, you can configure an energy profile that controls the optimal use of computer resources.

5.2. Performing actions when idle time is out

1. In the **Idle timeout** field, enter the maximum timeout.
2. Near **Idle action**, select what **Green IT** action to perform when the timeout is over.

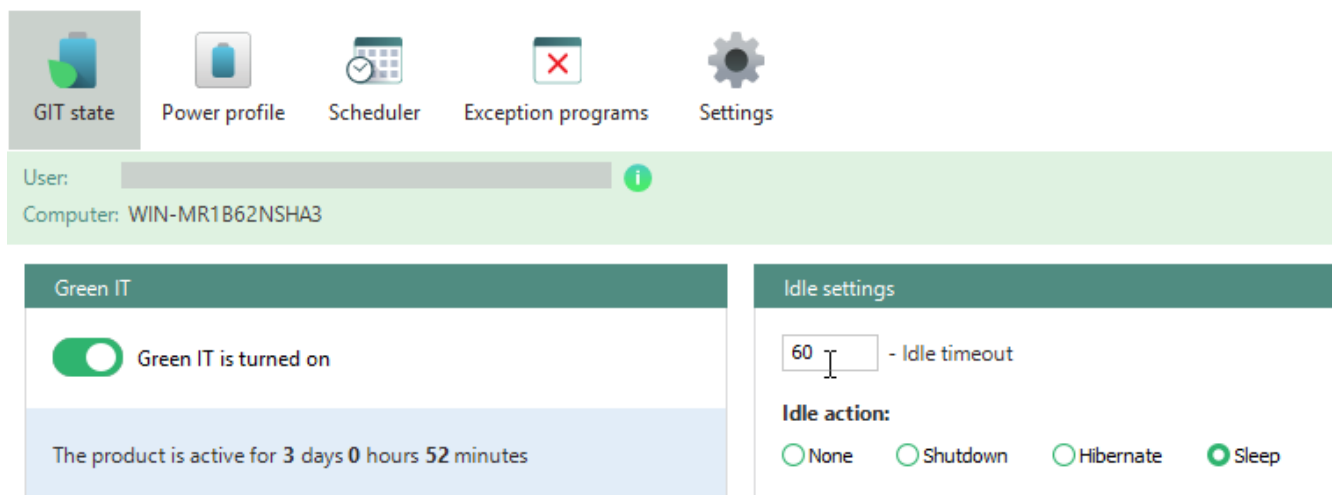


Figure 27. Selecting the action to be performed when idle time is out

5.3. Configuring power profile

In the **Green IT | Power profiles** section, the advanced settings are defined. Green IT actions (hibernate, sleep or shut down) are performed if all conditions defined here are met. If no changes are made in the section, the default values are applied.

For desktop computers powered from the wall socket, only AC (Alternating Current) column is shown.

For laptops (powered from the wall socket or from battery) and desktop computers powered from uninterrupted power supply, both AC and DC (Direct Current) columns are displayed.



INFO

Power settings for predefined exceptions

Power profile performing can be cancelled if a program defined as an exception is functioning. For details, see [Exclusions](#)

Object	Setting group	Setting	Description
Processor	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 done when computer is idle.
	Throttle settings	Throttle policy	Allows Windows to slow down processor speed to reduce power consumption. <ul style="list-style-type: none"> • 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).

			<ul style="list-style-type: none"> • 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	Display timeout		Set how long computer is inactive before the display turns off.
Disk	Spindown timeout		How long the hard drive is inactive before the disk turns off.
Devices	Enable Autoplay	- CD/DVD - USB	Fast way to enable or disable autoplay that appears on each device connection. Please, restart the computer 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.

5.4. Planning tasks

Green IT | Scheduler allows to perform Green IT tasks automatically. In the settings tab, define what actions are performed before executing scheduled tasks. For details, see [Green IT – Settings](#)

Creating a task

1. Click **Create** on the toolbar.
 - The **New task** dialog appears.

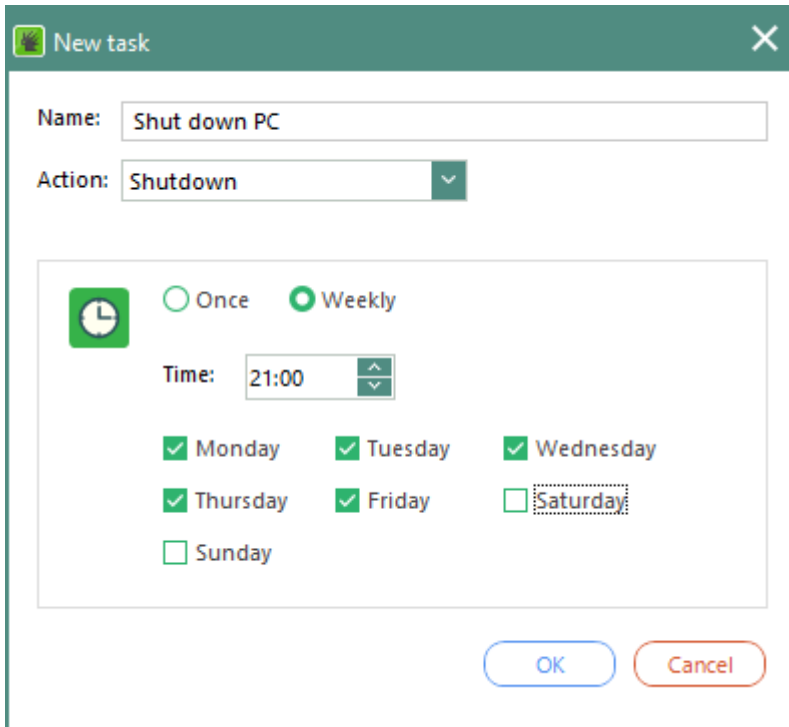


Figure 28. Planning tasks for Green IT

2. In the **Name** field, enter a task name.
3. In the **Action** drop-down menu, select what action to perform. For details about the difference between sleep and hibernate modes, click the external [link to Microsoft help](#).
4. Select when to perform the action (one time or regularly).
5. Click **OK** to confirm.

➤ The new task appears in the **Scheduler** list. In the **Description** column, the summary of the task is shown.

Disabling a task

- ◆ Clear the check box in the **Active** column. You are allowed to disable only your own tasks with 👤 icon, administrator tasks 🌐 can not be disabled.

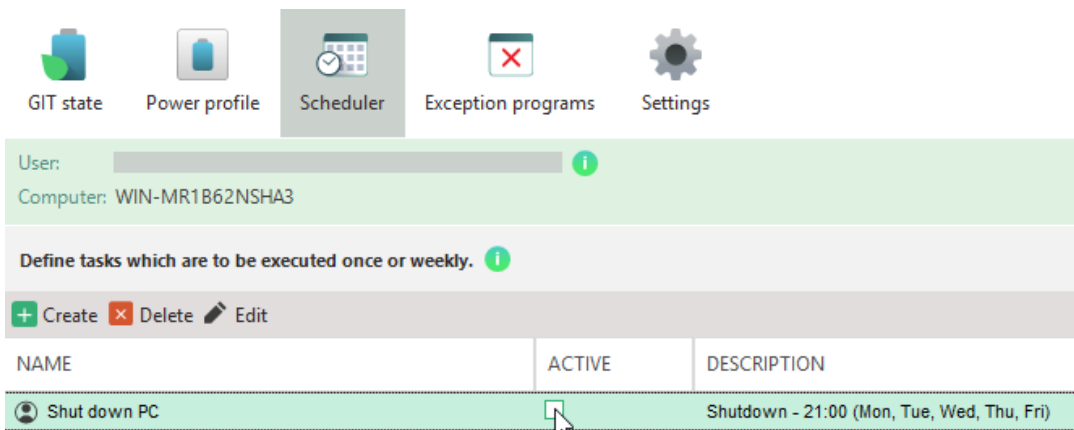




Figure 29. Disabling Green IT task



➤ The task remains disabled till the moment you enable it back.

Editing a task

1. Double-click a task. You are allowed to edit only your own tasks with  icon, administrator tasks  can not be edited.
 - The task dialog opens.
2. Make changes.
3. Click **OK** to confirm.

➤ The text in the **Description** column changes according to the changes made.

Deleting a task

1. Select a task from the list.
To select multiple tasks at the same time, hold down the **Ctrl** key while clicking.
2. Click **Delete** on the toolbar. You are allowed to delete only your own tasks with  icon, administrator tasks  can not be deleted.

➤ The entry is deleted from the list.

5.5. Managing exceptions

In **Green IT | Exception programs** section, define which programs and processes limit the power profile settings. These exceptions are applied only to the power profiles settings. They have no influence on the performing of tasks created in **Scheduler**.

Creating an exception

1. Click **Create** in the toolbar.
 - The **New program** dialog appears. In the **Applications** tab the currently running applications and opened directories are shown. In the **Processes** tab, you can see the currently active processes.

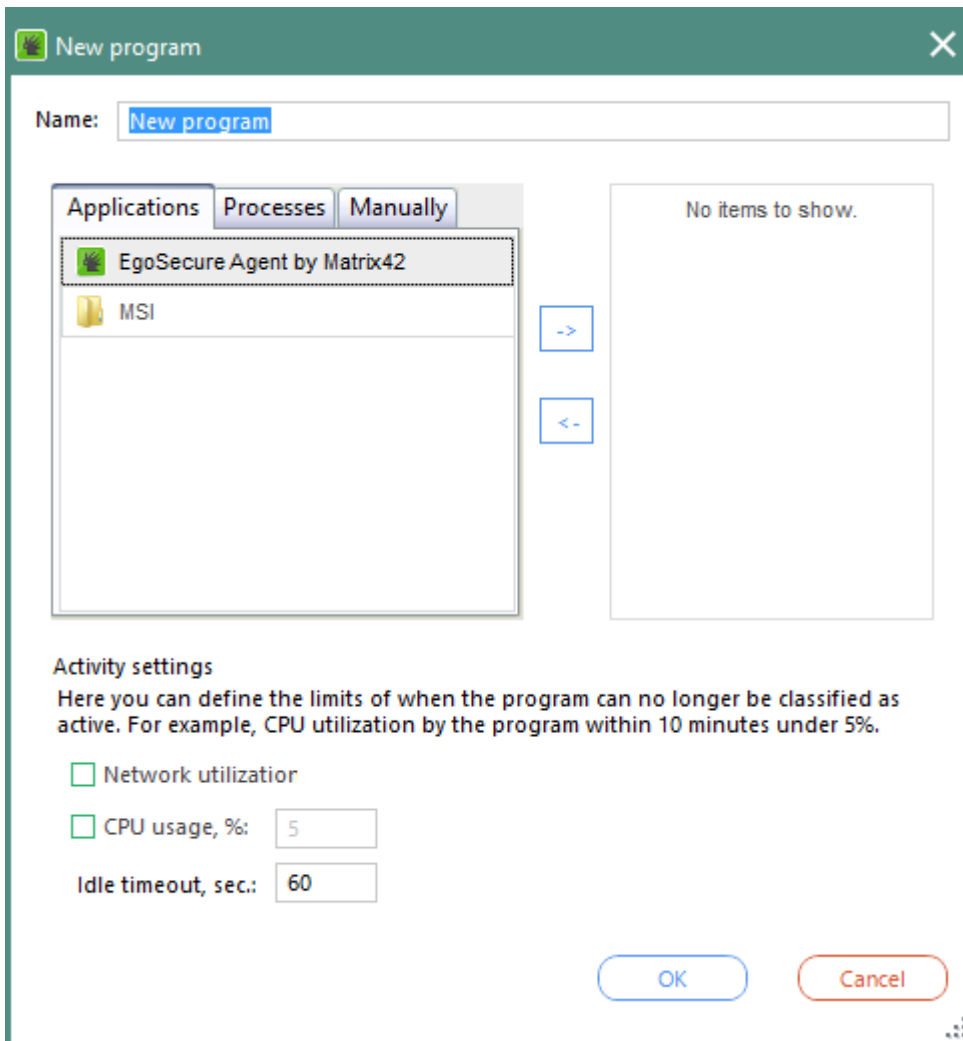







Figure 30. Defining Green IT exceptions

2. Double-click an application/a process.
→ The application/process appears in the right column.
 3. To select a closed program on your computer, click **Open** in the **Manually** tab.
 4. Click .
 5. Define the Activity settings:
 - a. Check **Network utilization** to take network activity into account.
 - b. Specify how much % of CPU a program must use to be considered as an active one.
 6. Click **OK** to confirm.
- The dialog closes. The settings are applied and affect the settings defined in **Power profiles**.



Editing an exception

1. Double-click an exception. You are allowed to edit only your own exceptions with  icon, administrator exceptions  can not be edited.
2. Edit the exception and confirm with **OK**.

Disabling an exception

- ◆ Clear the check box in the **Active** column. You are allowed to disable only your own exceptions with  icon, administrator exceptions  can not be disabled.

Deleting an exception

- ◆ Select an entry and click **Delete** on the toolbar. You are allowed to delete only your own exceptions with  icon, administrator exceptions  can not be deleted.

5.6. Changing settings

In **Green IT | Settings**, define settings for executing Green IT tasks. These settings influence only the performing of the tasks created in **Scheduler**, they do NOT take effect on **Power profile** settings.

Displaying a message before executing a task

1. To display a message with which the action can be postponed to a later date before executing the action, enable the **Show a message before performing a scheduled task** option.
 - The field for defining a time interval appears.
2. Enter the number of minutes before shutdown/sleep/hibernate to display the message or how many minutes the action can be postponed. If you confirm that the action must be postponed, the message will reappear once the time interval expires. The process repeats until the action is finally executed.

Saving documents automatically

- ◆ To automatically save documents opened in Microsoft Office (Excel, Word, Power Point, Access) before executing the action, enable the **Automatic saving of documents** option. If the document hasn't been saved before, it is saved to the **My documents** folder.

6. SECURE ERASE

6.1. Overview

When you delete files from Windows, they are not really deleted from the hard disk. Windows always saves a backup of the file to disk. These backup files are not displayed in Explorer and you can not access them.

With **Secure Erase**, you can safely delete files, folders, and empty areas of your hard disk. You can also delete improperly removed files, which are not deleted when emptying Recycle Bin via Windows. Deleted objects are first overwritten several times and then deleted, so that they can not be restored.

6.2. Deleting files securely

Selecting a secure erase method

- ◆ Select a secure method. By default, is the **Overwrite with random numbers** method is selected.

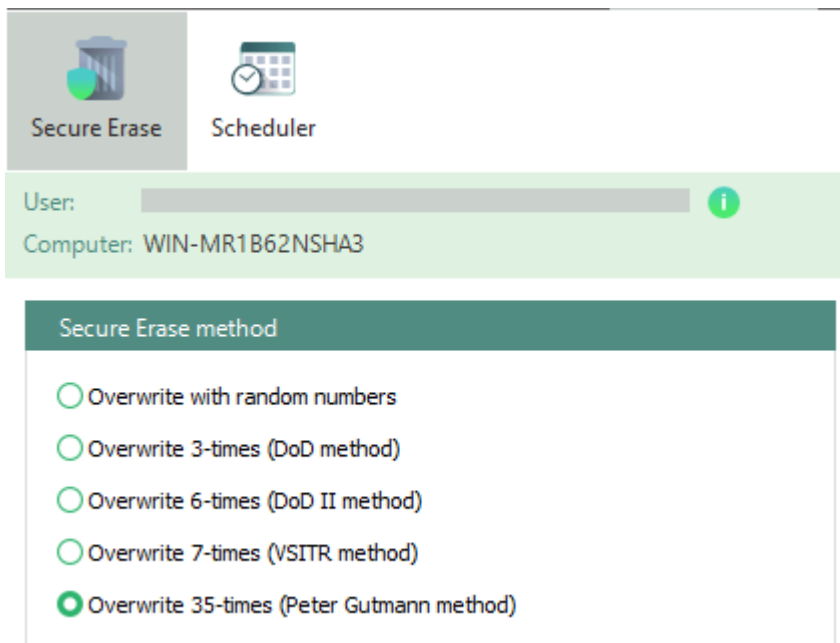


Figure 31. Selecting a secure erase method

- The selected method will be used by **Secure Erase**.

Deleting individual files securely

1. Right-click a file in Windows Explorer.
2. Select **Secure delete** from the context menu.

Emptying the Recycle Bin securely

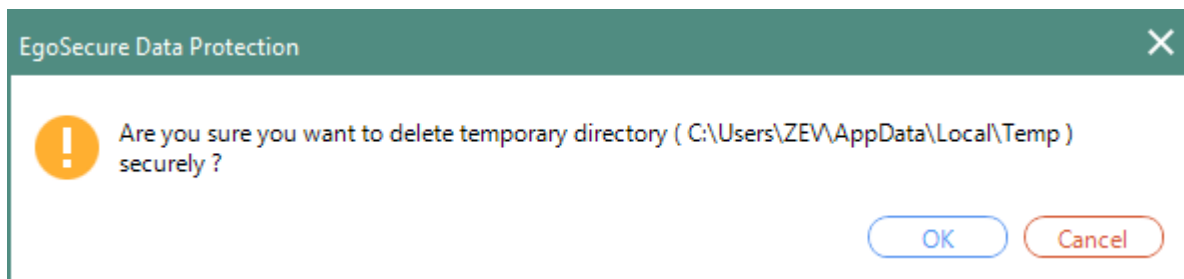
- ◆ Click **Empty Recycle Bin** in the **Secure Erase** tab
OR
- ◆ Right-click the Windows Recycle Bin and select **Empty Recycle Bin securely**.



Figure 32. Emptying Windows Recycle Bin securely with Secure Erase

Deleting temporary directories securely

1. Click **Remove temporary directory** in the **Secure Erase** tab.
 - A dialog asking you whether you want to delete temporary directory. In brackets you can see the path to the directory.



2. Click **OK** to confirm.

6.3. Planning secure erase

You can use the **Scheduler** to automatically execute actions of **Secure Erase**. You can automatically delete files and directories at certain time.

You can also safely delete empty disk sectors. Safely clearing empty sectors cleans up a disk's free space and removes hidden Windows sector backup files.

Creating a task

1. Click **Create**.
 - The **New task** dialog appears.
2. In the **Name** field, enter a task name.
3. To delete files and directories, select **Secure delete** from the **Action** drop-down menu.
 - a. Select a method in the **Secure Erase method** menu.
 - b. Click **Add file...** or **Add folder...** to define objects for deletion.

- c. In the **Open** or in the **Browse for folder** dialog, select the objects for deletion.
 - d. Click **OK** to confirm.
 - The selected objects appear in the **Secure deletion objects list**.
 4. To delete empty sectors of the drives, select **Empty sectors secure delete** from the **Action** drop-down menu. Check the hard drives where you want to delete empty sectors.

Only the free space is cleaned up.
 5. Enable the check boxed, if needed:
 - a. **Empty Recycle Bin securely** to delete the contents of the recycle bin and
 - b. **Delete temporary directories securely** to remove the contents of the temporary directories.
 6. Define a time period or a period for repeating the task.
 7. Click **OK** to confirm.
- The dialog closes and the changes are applied. The new task appears in the list of the **Scheduler** tab.

Editing a task

1. Double-click a task OR select an action and click **Edit** in the toolbar.
2. Make changes.
3. Confirm with **OK**.

Disabling a task

- ◆ Clear the check box in the **Active** column.

Deleting a task

1. Select a task from the list.

To select multiple tasks at the same time, hold down the **Ctrl** key while clicking.
2. Click **Delete** on the toolbar.

- The entry is deleted from the list.

7. PASSWORD MANAGER

7.1. Overview

Password manager allows for saving and managing the passwords of your application and website accounts. Define passwords manually or generate them automatically. The passwords are stored in a password container which is a file with the **.dat** extension. The **.dat** file is automatically encrypted with the **AES 256** encryption algorithm. Access this container via a password for the password manager. The password for the container is required each time you access the **Password manager**.

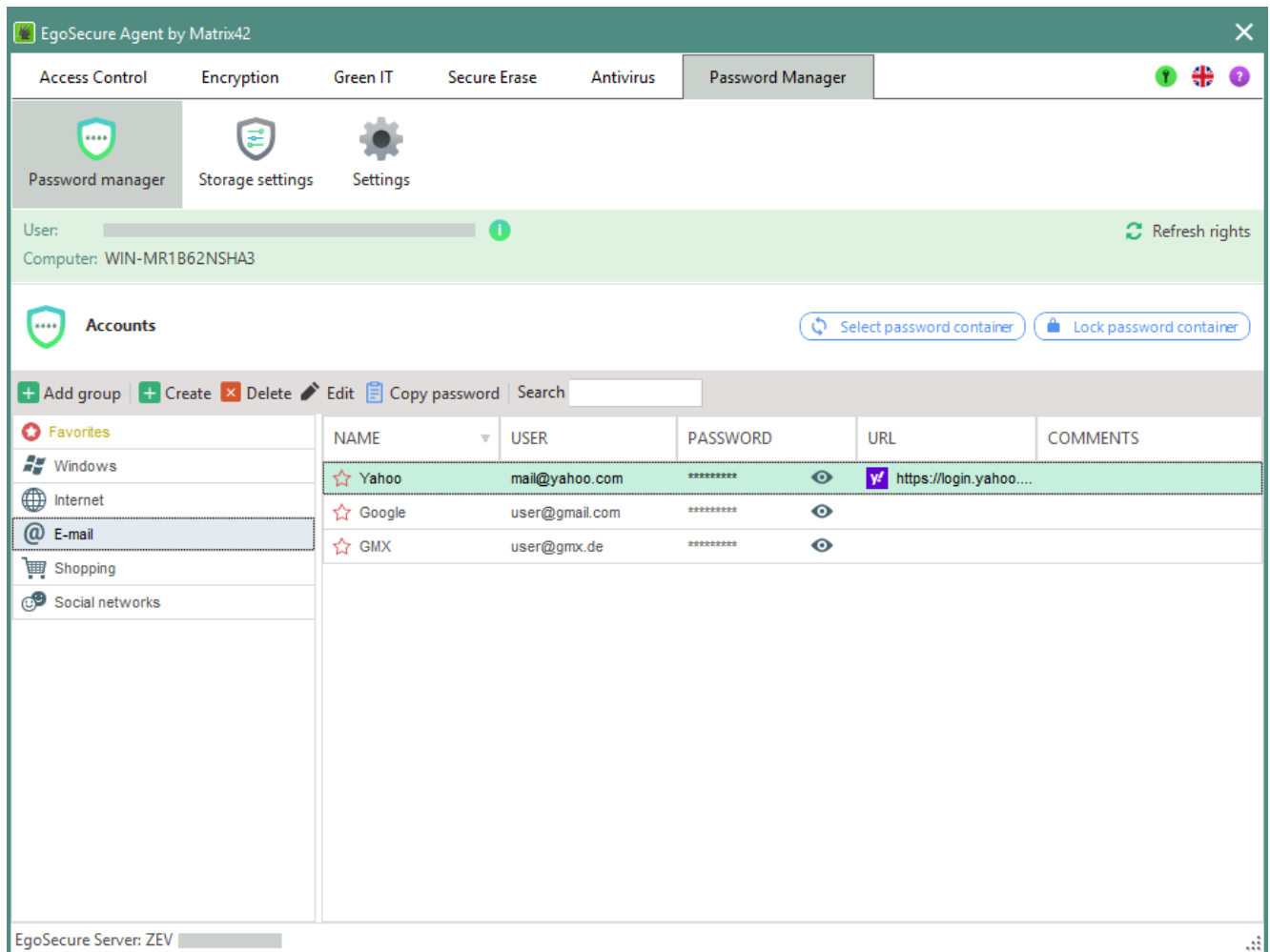


Figure 33. Opened password container of Password Manager

The **Password Manager** tab displays your password entries once the password for the container is entered. For details, see [Using password container](#). The **Storage** settings tab allows for configuring the settings for securing the data of the container. For details, see [Creating a backup copy](#), [Backup settings](#). The **Settings** tab offers to control an access to an opened container. For details, see [Locking access in case of inactivity](#), [Clearing the clipboard](#).

7.2. Managing password container

Creating a password container

1. Near the **Path** field, click to define the location for a password container.
2. In the **File name** field, enter a password container name.
3. In the **Password** field, enter a password. Repeat the password in the **Confirmation** field.
 - The colored bar next to **Password strength** shows you how secure your password is:
dark red = very insecure; dark green = very secure.

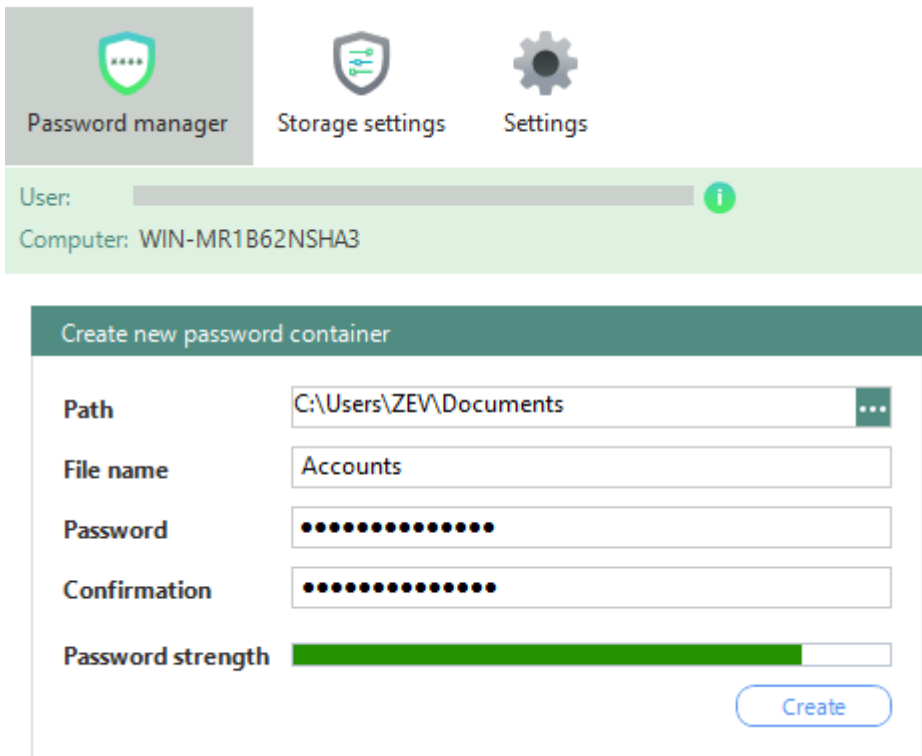


Figure 34. Creating a new password container

4. Click Create.

→ The password container is created and opens.

Opening password container

- ◆ Enter the password for the active container and click **Open**.

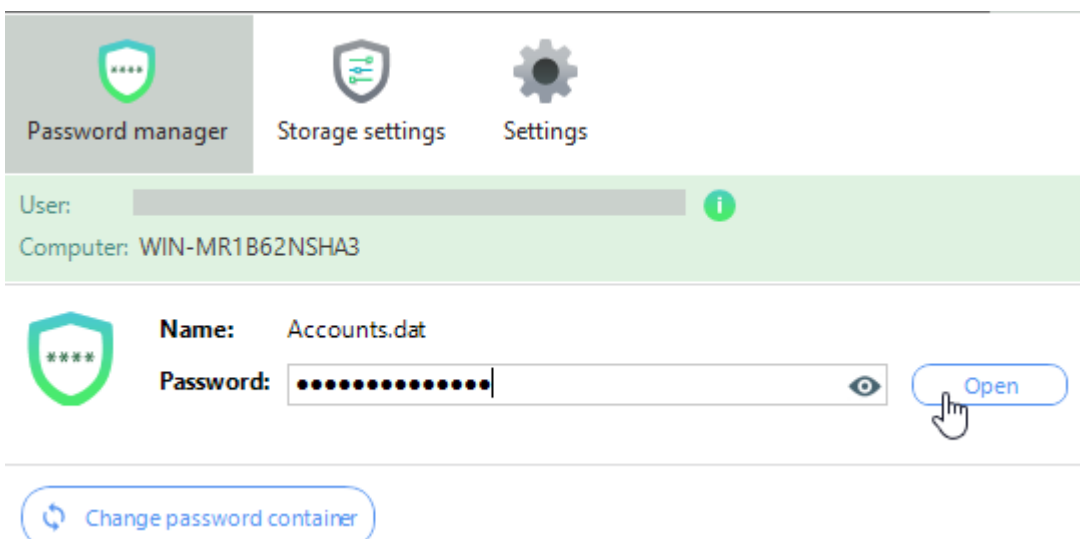


Figure 35. Entering password for container

Changing password container

1. Navigate to the **Password manager** tab.

- If a container is unlocked: click **Select password container** and then click **Open**.
- If a container is locked: click **Change password container** and then click **Open**. If you have already entered the container password and the login view is not displayed, change to another tab and return to the **Password Manager** tab. For details, see [Configuring container locking](#).

→ The **Open** dialog appears.

2. Select a file and click **Open**.

➤ The container is selected, now you need to enter the password for the container and click **OK** to enter it.

Changing a password container path

1. In the **Storage settings** tab, click **Move to** in the toolbar.
 - The **Save as** dialog opens.
2. Define a location for the password container and click **Save**.
 - The **Password Manager** changes the path in Program settings and moves the file on your computer. The success dialog appears.
3. Click **OK** to confirm.

Changing a password for a password container

1. In the **Storage settings** tab, click **Change password** in the toolbar.
 - The **Change password** dialog appears.
2. In the **Old password** field, enter the actual password.
3. In the **Password** field, enter a new password and repeat it in the **Confirmation** field.
4. Click **OK** to confirm.

Creating a backup copy of a password container

1. In the **Storage settings** tab, under **Backup settings**, click ... to specify a location.
 - The **Browse for folder** dialog appears.
2. Select location and click **OK**.
3. Click **Make backup** in the toolbar.
 - The success dialog appears.
4. Click **OK** in the success dialog.

➤ The backup file is saved to the selected location. The file name of the backup copy consists of container name, date and time:

Containername_YYYYMMDDHHMMSS.dat

Restore a password container from a backup

1. In the **Storage settings** tab, click **Restore from backup** in the toolbar.
 - The **Open** dialog appears.
2. Select a backup copy of the password container.

If you manage multiple containers: Make sure to select a backup copy of the active container, because all backup copies are stored in the same folder.

3. Click **Open.**

→ The **Enter password** dialog appears.

4. Enter the password for the selected container.

5. Click **OK.**

→ The **Backup file** dialog appears.

6. Click **Yes.**

→ A message box appears and confirms the successful recovery.

7. Confirm the message box with **OK.**

Defining backup settings

1. In the **Storage settings** tab, under **Backup settings**, click ... to specify a location of a backup copy.
2. In the **Number of backup copies** field, enter how many backup copies can be stored in the specified location. Once the number is reached, the oldest file is deleted.
3. To automatically create a backup copy at regular intervals, check the **Enable automatic backup** box and select the interval in the **Make backup every** drop-down menu.

→ The backup copy will be automatically created from now on.

Set time for locking a container

1. In the **Settings** tab, enable the **Lock password container if idle time more than** option.
2. Enter the number of seconds after which the password container is locked when it is not in use.

Configure locking when changing a tab

1. To temporarily leave the password container open after switching to another tab, enable the **Leave password container opened when switching between modules or windows for** option in the **Settings** tab.
2. Specify for how many seconds the password container can remain open before re-entering the password.

Set the time for emptying the clipboard

- ◆ Enable the **Clear the Clipboard in** box in the **Settings** tab and enter how long a copied password can leave in the clipboard till it is deleted. For details, see: [Copying and using password](#)



ATTENTION

Passwords in the clipboard

If the option is disabled, copied password remain in the clipboard for an unlimited time.

7.3. Using password container

Creating password groups

1. In the opened container, click **Add group** in the toolbar on the left.
→ The **Add group** dialog appears.
2. Enter a name of a group in the **Name** field.
3. Select a symbol for the group.
4. Click **OK** to confirm.

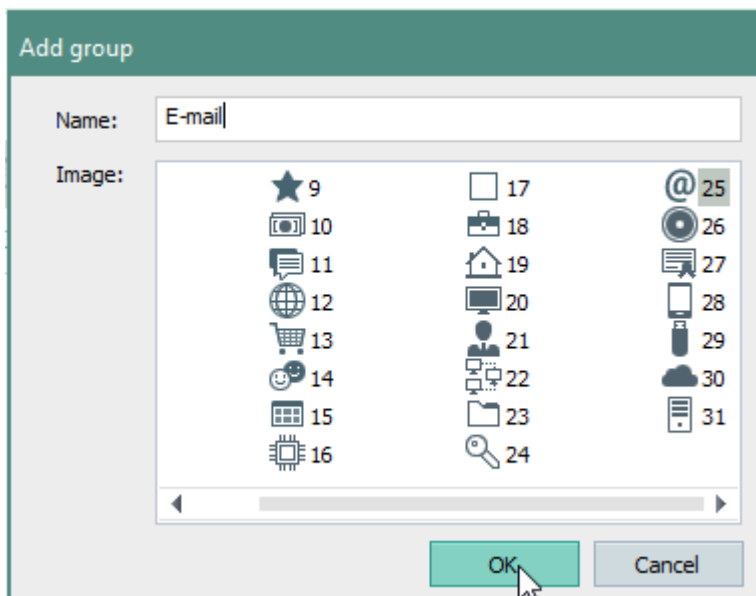



Figure 36. Creating a new password group in password container

- The new group appears in the left column of the **Password manager** tab.

Adding passwords

1. Select a group on the left and click **Create**.
→ The **Add new entry** dialog appears.
2. In the **Name** field, enter a name for the group entry.
3. In the **User** field, enter the user information (e.g.: user name or the e-mail address).
4. In the **URL** field, add the Internet address, where the defined user name and password are used.
5. In the **Password** field, enter the password and repeat in the **Confirmation** field
OR

6. Click on  to generate a password automatically.
 - The colored bar next to **Security** shows you how secure your password is: dark red = very insecure; dark green = very secure.
7. If necessary, enter additional information for a group entry in the **Comments** field.
8. Click **OK** to confirm.

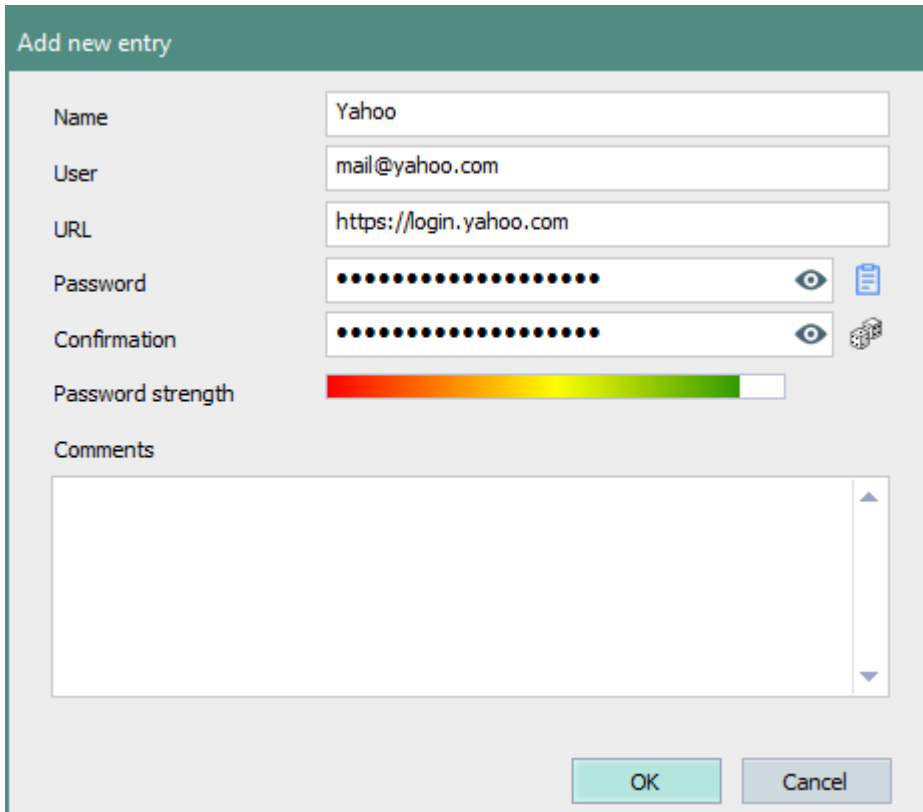




Figure 37. New entry for password container

- The new entry appears in the right column.

 INFO	<p>Showing password</p> <ul style="list-style-type: none"> ◆ Click on  in a password field to make password visible.
--	---

Editing a password entry

1. Double-click an entry.
 - The **Edit entry** dialog opens.
2. Make the changes and click **OK**.

Copying and using password

1. Right-click an entry.
2. Select **Copy password** from the context menu.

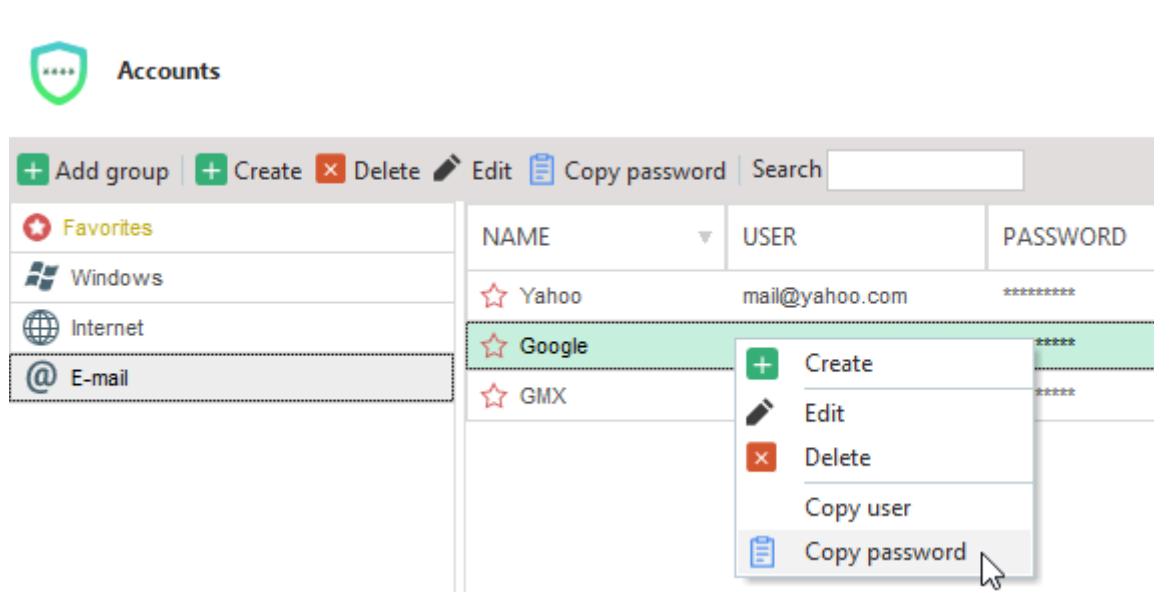


Figure 38. Copying password to the clipboard

➤ The **Password Manager** copies the password to the clipboard.