

HiCrypt™ 2.0

Table of Content

1	Introduction
2	Installation
3	Licensing
4	First steps using HiCrypt 2.0
4.1	How to start HiCrypt 2.0
4.2	Connecting Shares
4.3	Encrypt Shares
4.4	Security policies
4.5	User management
4.6	Password-generator
5	Decryption
6	Recovery
7	Repair
8	Further options
9	Using online-storage-server
10	Using Services like Dropbox
A	Technical informations
B	Glossary

1. Introduction

HiCrypt 2.0 restores the key sole ownership warranty. This means the privileg of one responsible person to decide who can see important content and files in a company. Years ago this files were written on paper and were locked in a safe. Nowadays often this secrets are digital files which are saved on a server. This means everybody who has access to the server also has access to this files and can see their content.

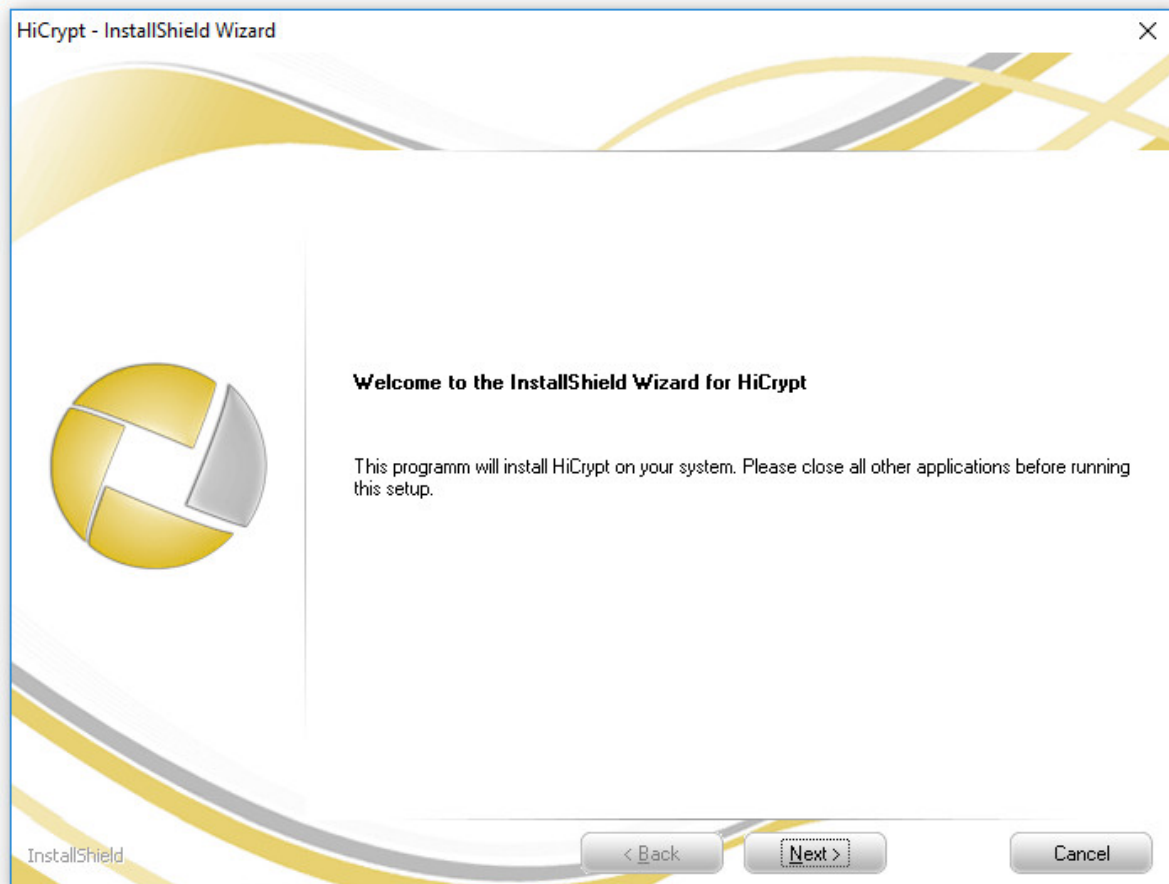
Such access can be still allowed for users if there was made a mistake during the confuration for access rights for sepearte users or administrators, and they also need much more rights to do their work. So HiCrypt 2.0 encrypt the files on the client, before saving them on the server. The responsible person, in HiCrypt a so-called „Manager“, assign the keys needed for the decryption to all the users who should have access to the encrypted files. So the acces permissions given by the operating system won´t were changed so the administrators can do their tasks without having access to files they should not be able to read.

This document gives a step-by-step instruction about the installation and the configuration of HiCrypt 2.0. At least there is a description about some recovery-scenarios and the user management.

Finally you will find the technical details. If you have any questions about HiCrypt 2.0, send us an e-mail to support@digitronic.net. The latest version of HiCrypt 2.0 connected with a standard licence can be find using the following link: <http://www.hicrypt.com/download>.

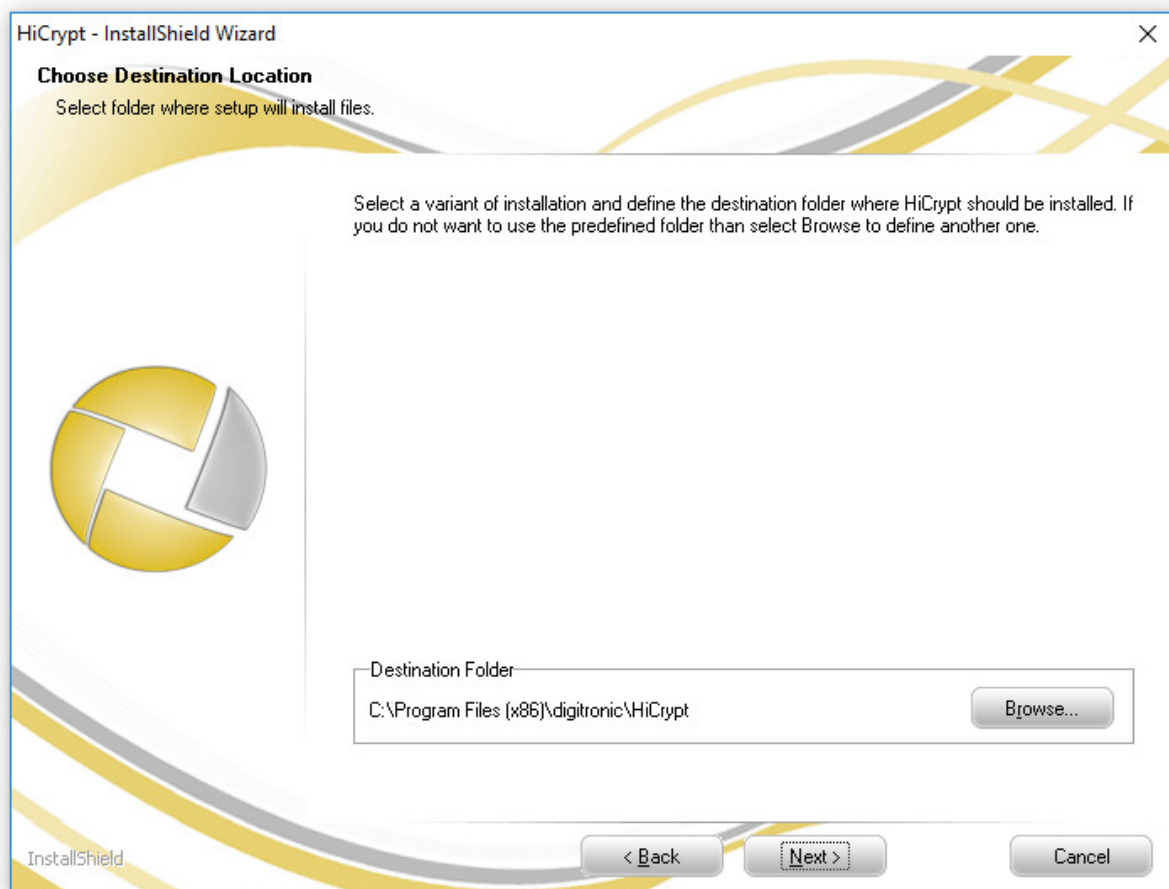
2. Installation

Step 1



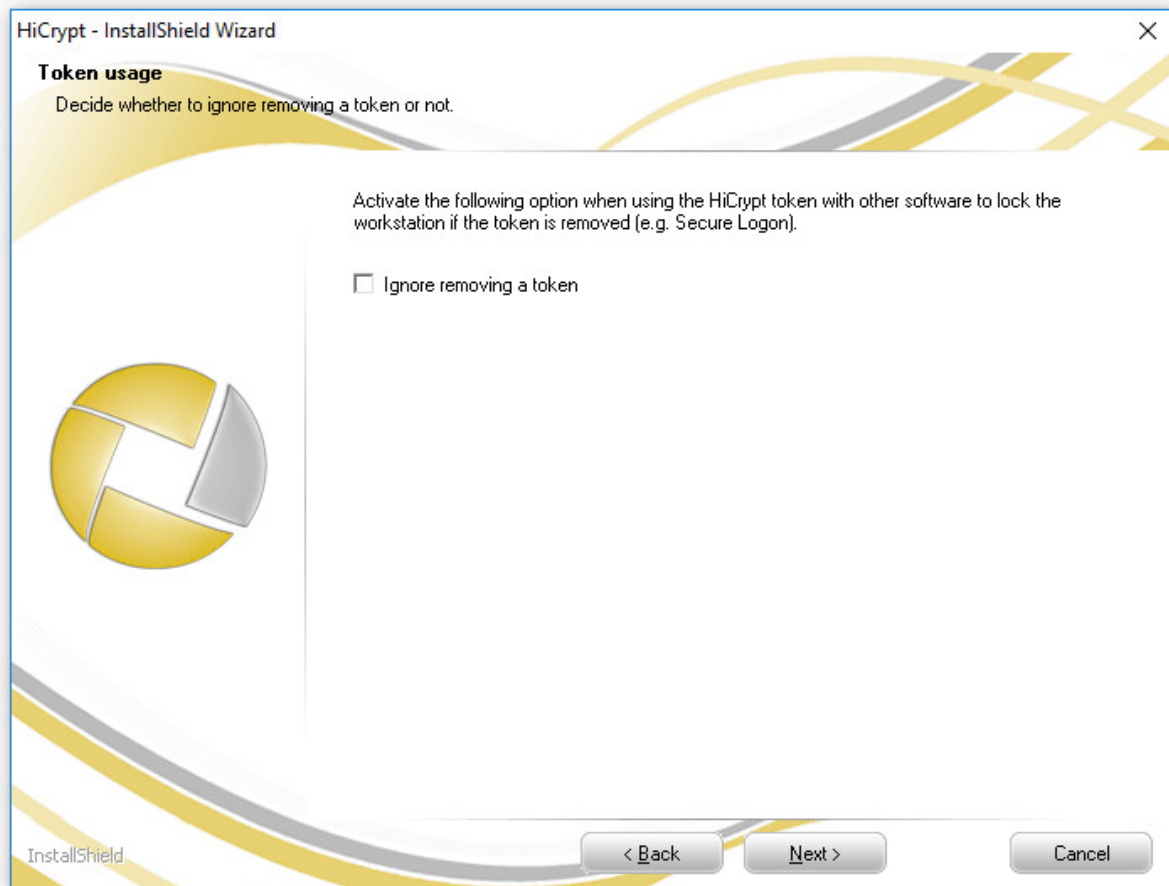
Read the information above and accept by clicking "Next".

Step 2



Choose the directory where HiCrypt 2.0 should be installed and confirm your choice by clicking "Next".

Step 3



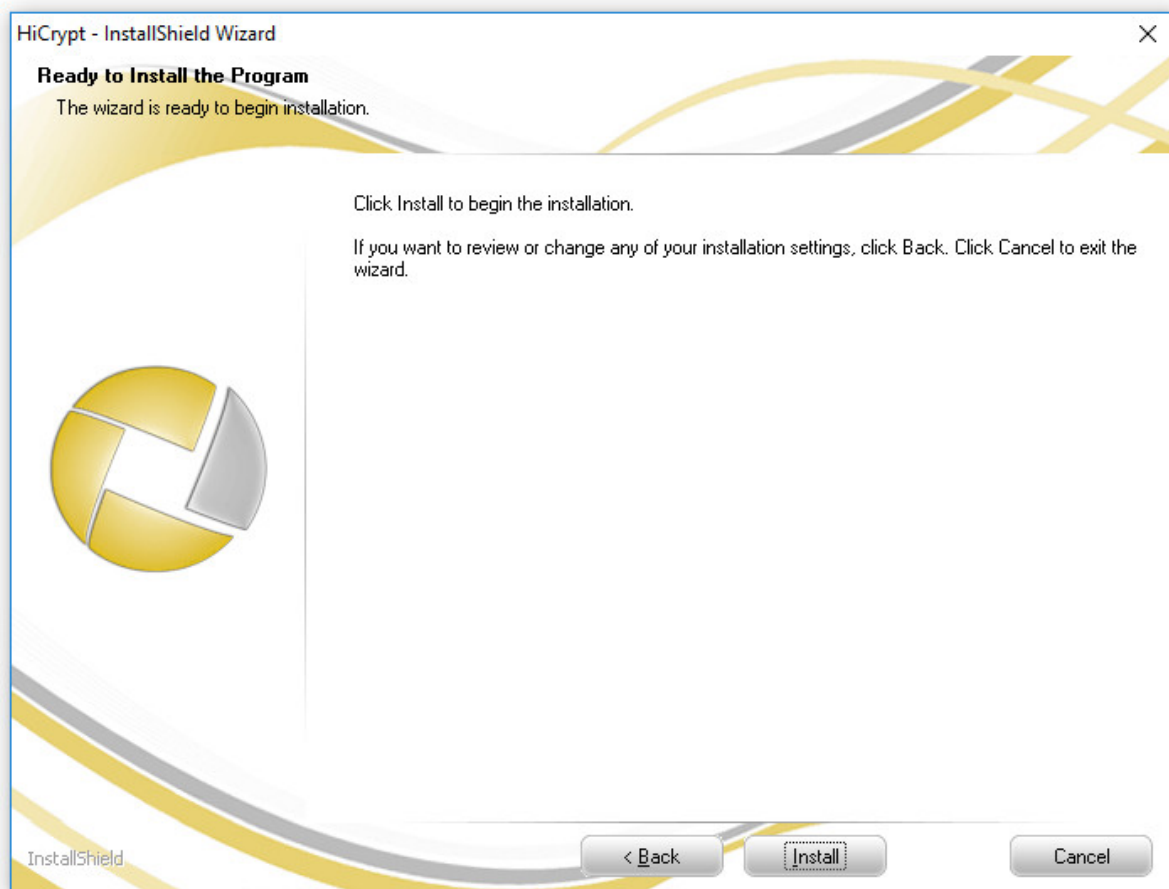
In this dialogue you can choose if HiCrypt 2.0 should not disconnect the shares the actual user is logged in if a SecurityToken is removed.

This could be important if a SecurityToken is used for logging on a windows session, for example Secure Logon 2.0.

If a user would be disconnected if the SecurityToken was removed, a loss of unsaved progress working with files from an encrypted share could **not** be excluded.

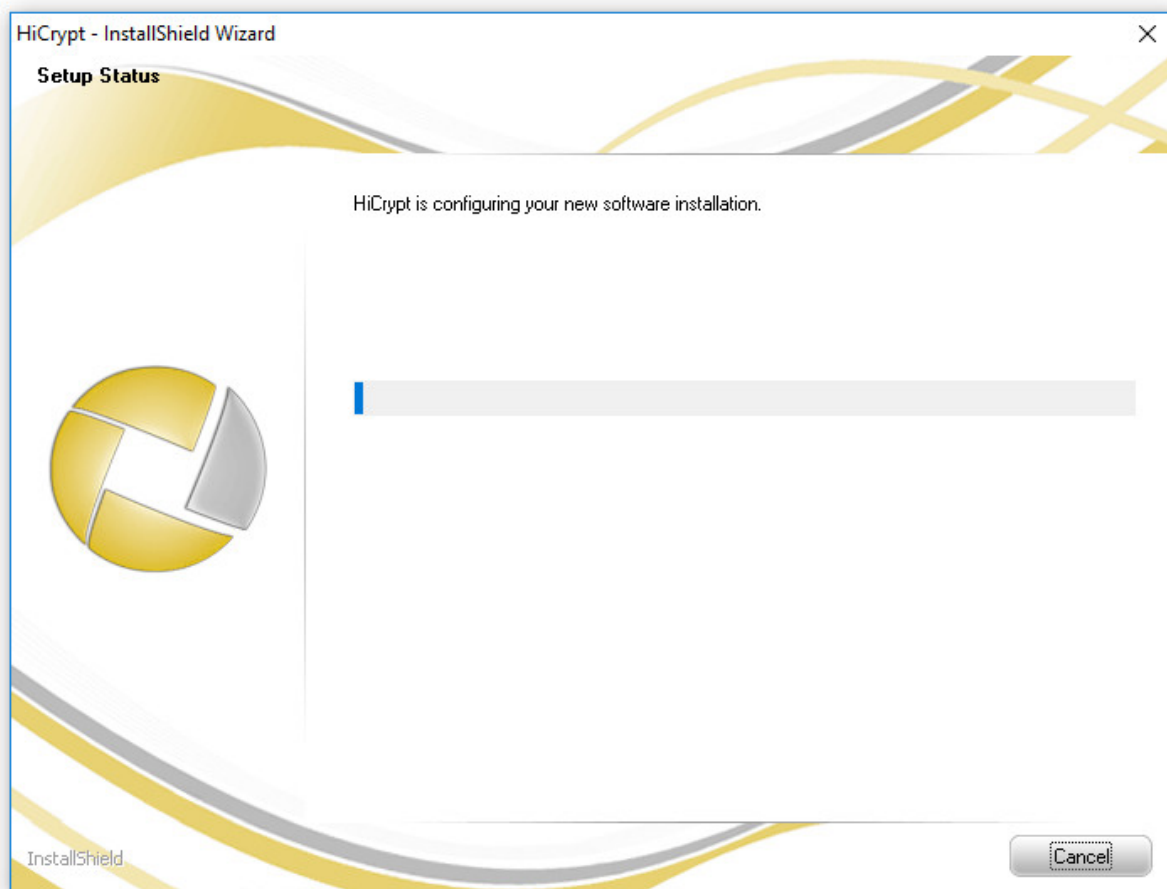
Confirm your choice by clicking "Next".

Step 4



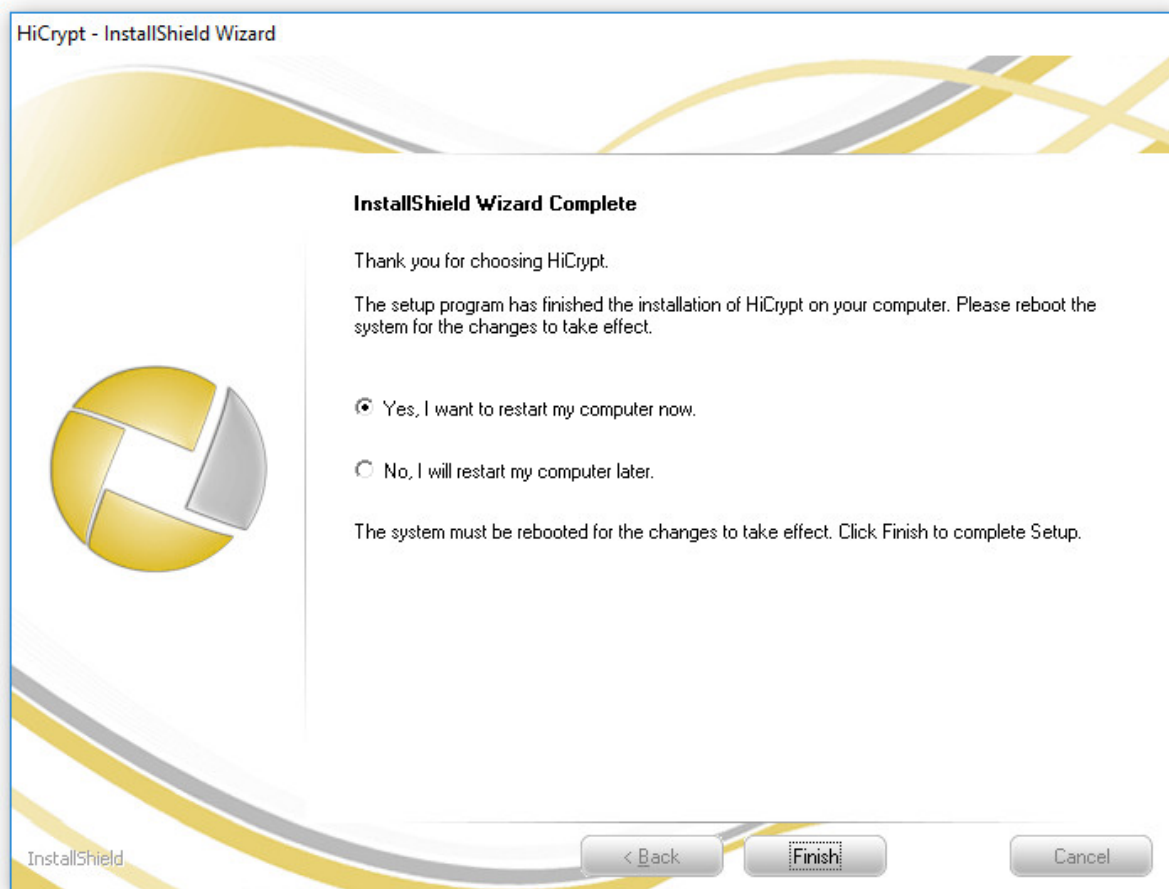
By clicking "Install" the installation will be started.

Step 5



During the installation of HiCrypt 2.0 the needed files were copied and configured on your computer.

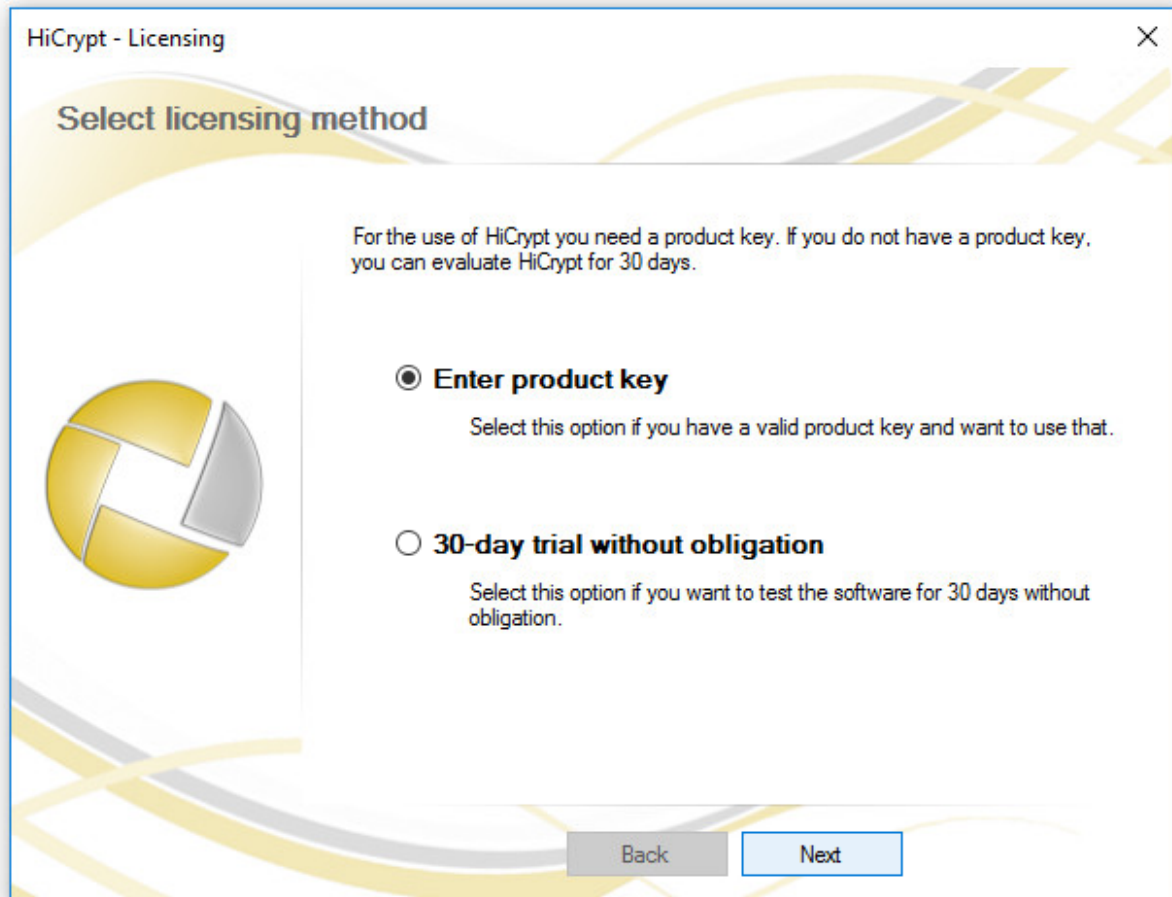
Step 6



To finish the installation, the computer has to be rebooted. You can use HiCrypt 2.0 after rebooting your system so the changes take effect.

3. Licensing

Step 1

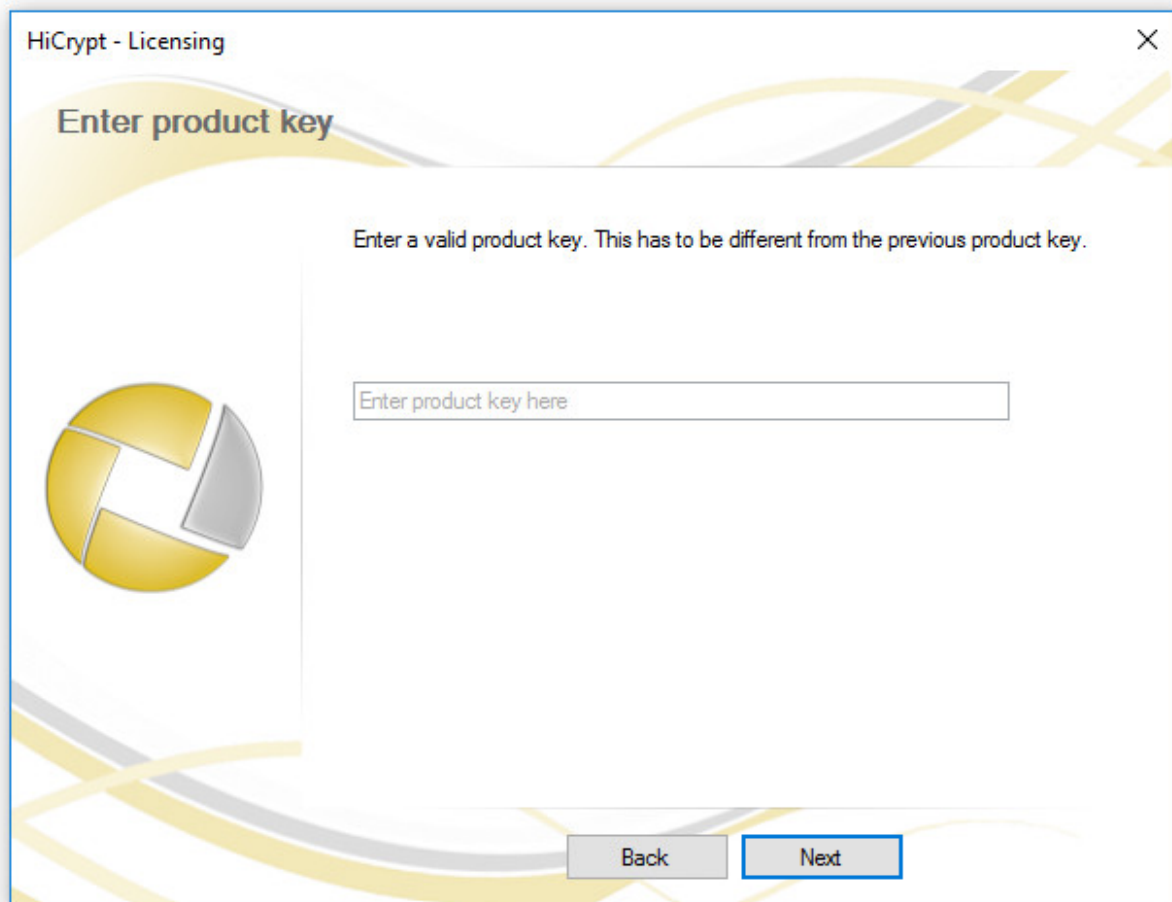


If you have bought a product key, you can choose "Enter product key".

You don't need a product key during your evaluation.
For this option you can choose 30-day trial.

Confirm your choice by clicking "Next".

Step 2



HiCrypt - Licensing

Enter product key

Enter a valid product key. This has to be different from the previous product key.

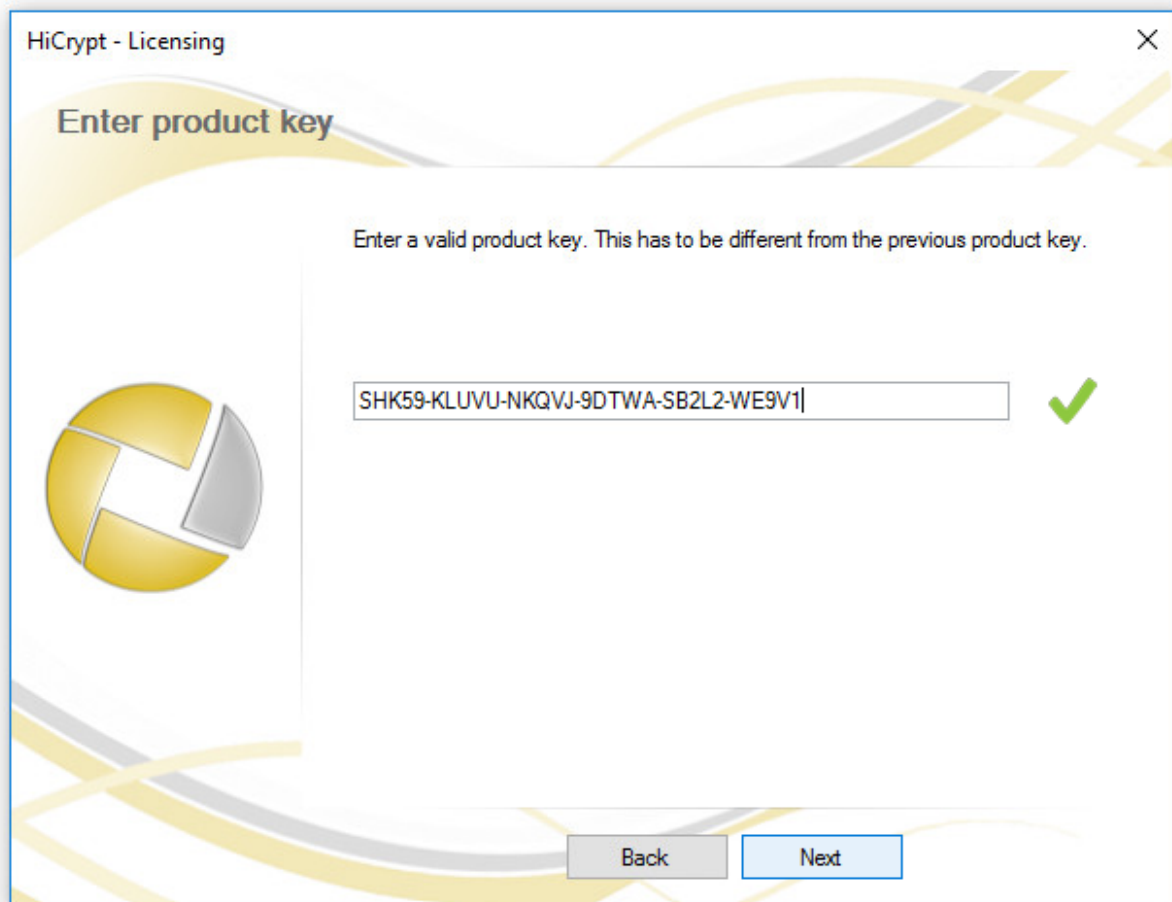
Enter product key here

Back Next

The image shows a software licensing window titled 'HiCrypt - Licensing'. It features a yellow and grey abstract background with a circular logo on the left. The main area contains a text prompt and a text input field. At the bottom, there are 'Back' and 'Next' buttons. The 'Next' button is highlighted with a blue border.

Enter your product key here and confirm by clicking "Next".

Step 3



HiCrypt - Licensing

Enter product key

Enter a valid product key. This has to be different from the previous product key.

SHK59-KLUVU-NKQVJ-9DTWA-SB2L2-WE9V1

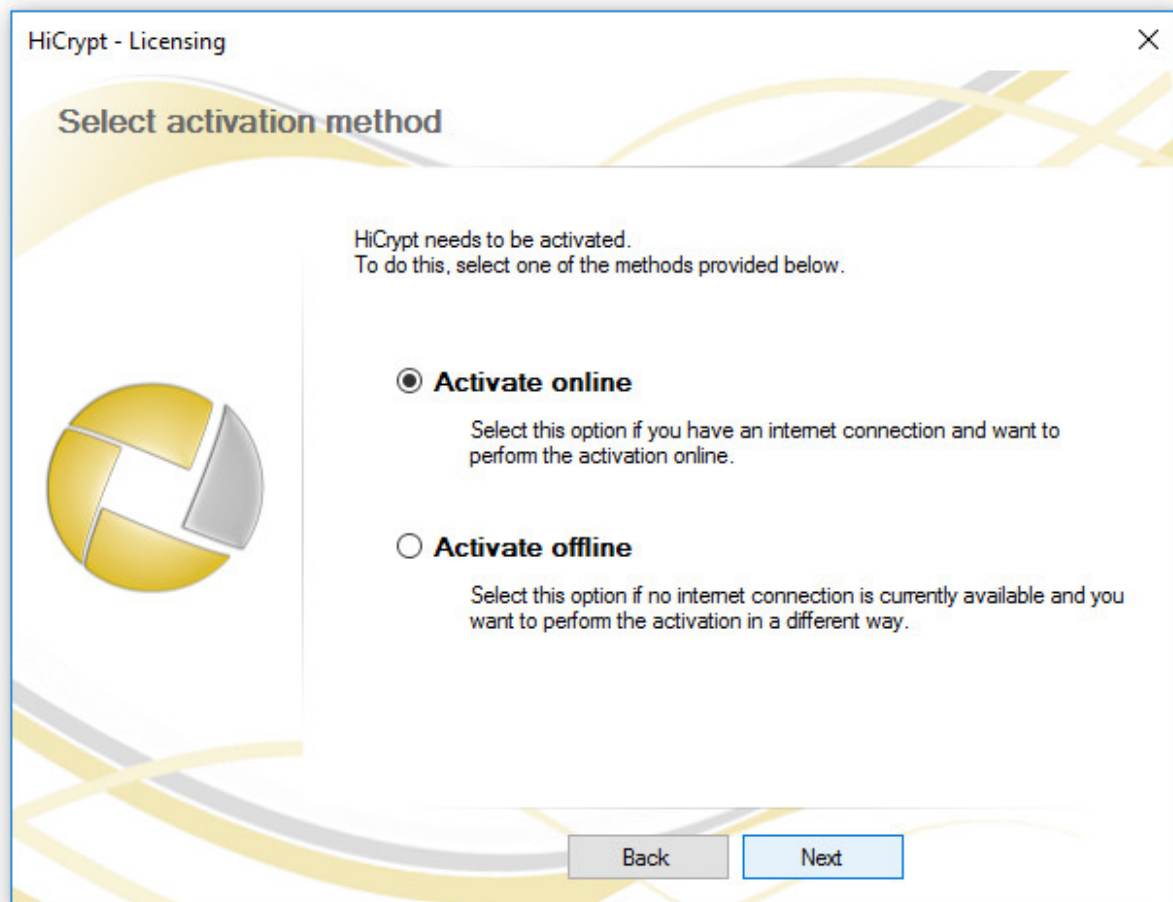
Back Next

The dialog box features a yellow and grey abstract graphic on the left and a green checkmark to the right of the product key input field. The 'Next' button is highlighted with a blue border.

The green tick signals that the product key has a accepted layout.

Confirm by clicking "Next".

Step 4

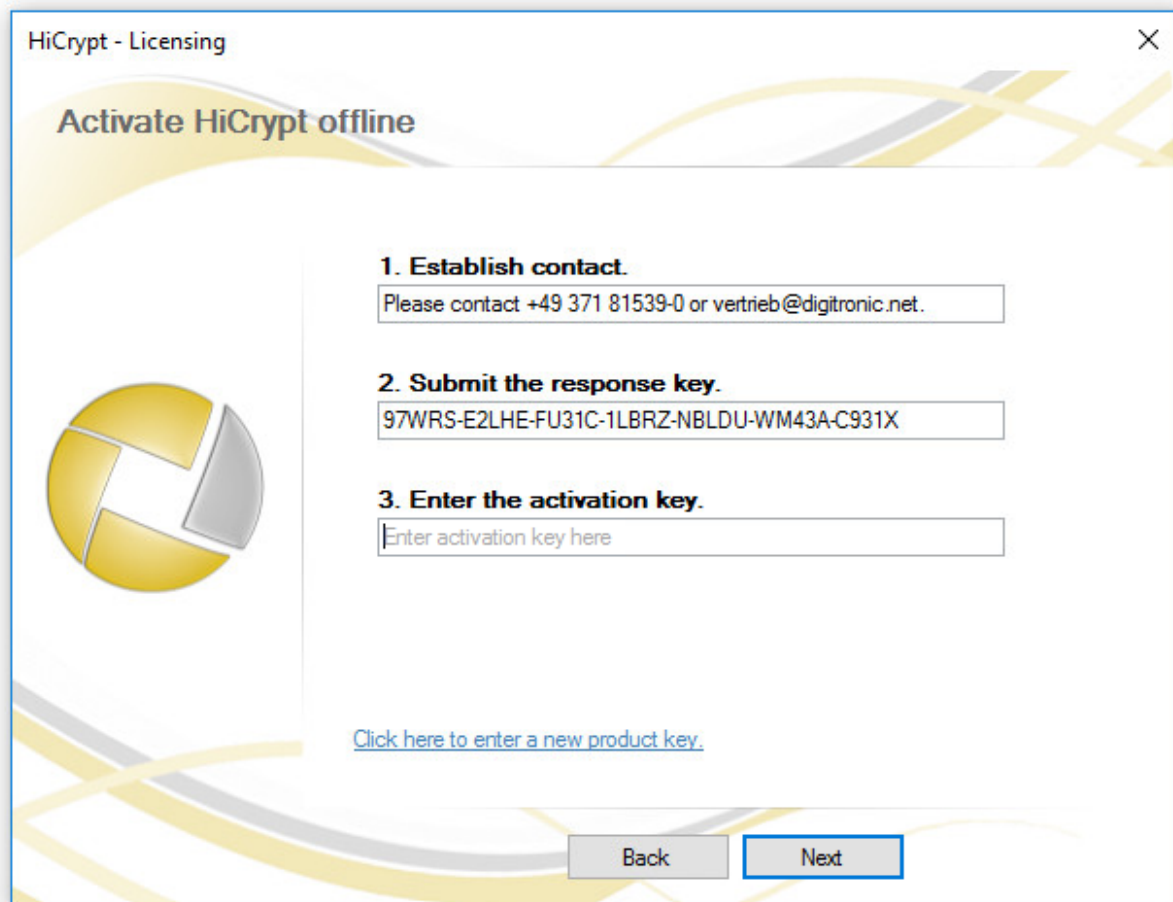


Both choices, "Enter product key" or "30-day trial", need to be activated before you can use it.

This can be done online or offline.
Please consider that an internet connected is required for the online activation.

Choose and confirm by clicking "Next".

Step 5



HiCrypt - Licensing

Activate HiCrypt offline

1. Establish contact.
Please contact +49 371 81539-0 or vertrieb@digitronic.net.

2. Submit the response key.
97WRS-E2LHE-FU31C-1LBRZ-NBLDU-WM43A-C931X

3. Enter the activation key.
Enter activation key here

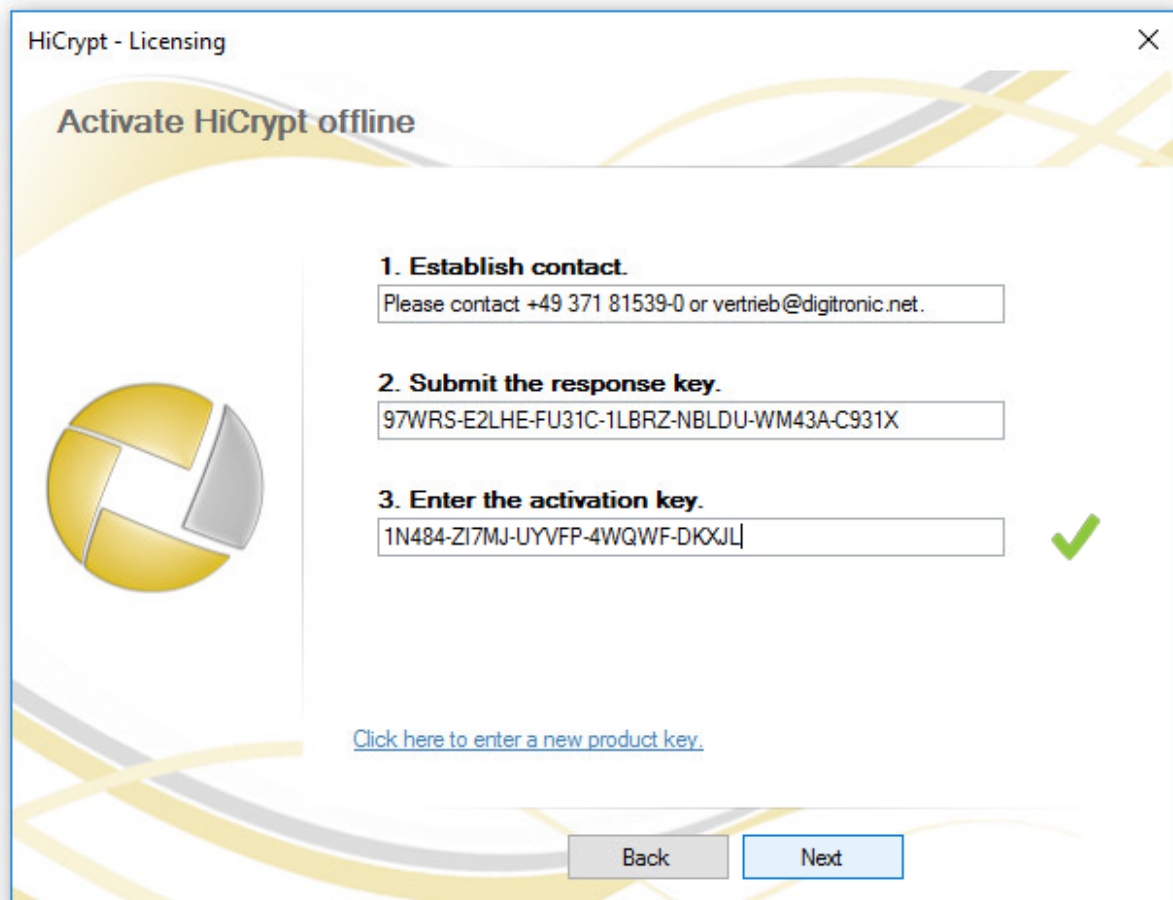
[Click here to enter a new product key.](#)

Back Next

For the offline activation you need a response key. You can enter it on <https://www.digitronic.net/en/service/license-activation-deactivation> or send it via e-mail to vertrieb@digitronic.net.

You will receive an activation key which you have to enter in the last dialogue.

Step 6



HiCrypt - Licensing

Activate HiCrypt offline

1. Establish contact.
Please contact +49 371 81539-0 or vertrieb@digitronic.net.

2. Submit the response key.
97WRS-E2LHE-FU31C-1LBRZ-NBLDU-WM43A-C931X

3. Enter the activation key.
1N484-ZI7MJ-UYVFP-4WQWF-DKXJL ✓

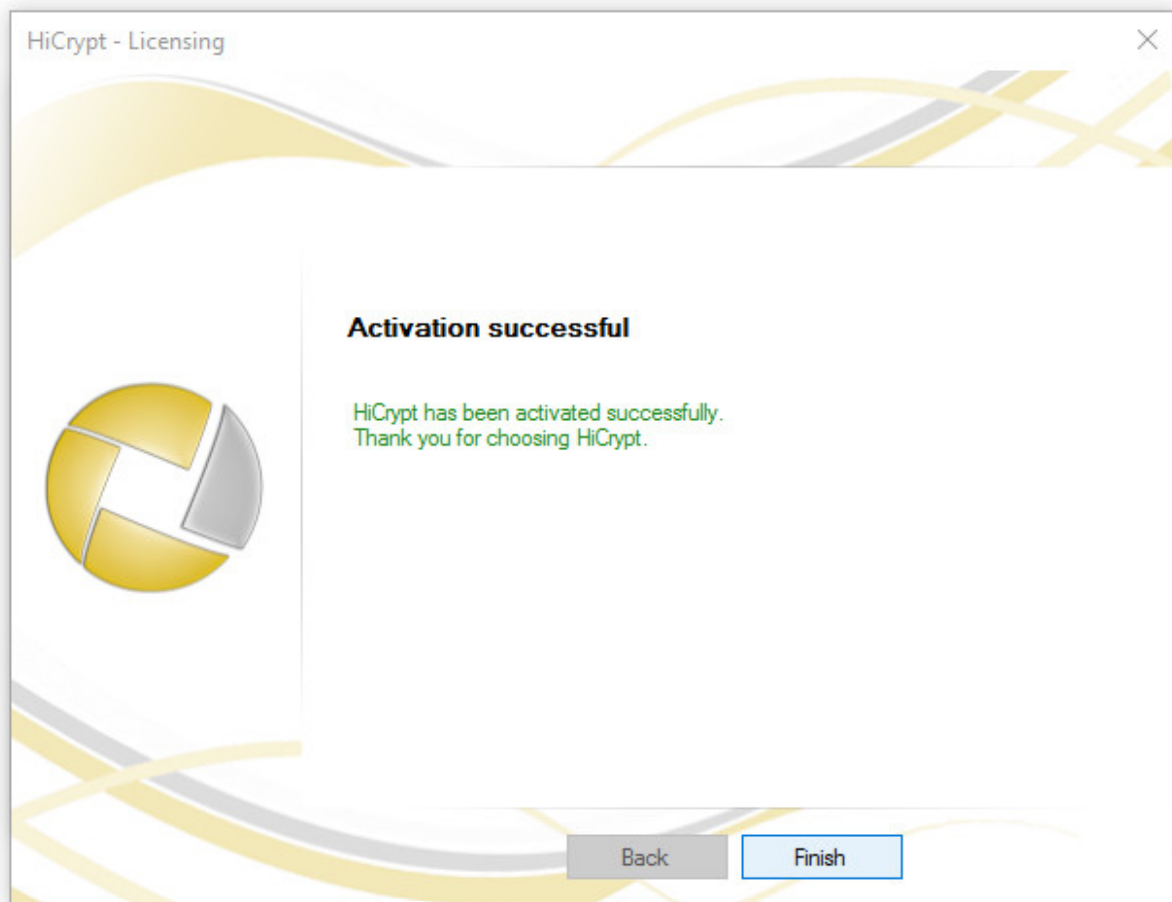
[Click here to enter a new product key.](#)

Back Next

There will be a green tick if the activation key has an accepted layout.

You can now activate the software by clicking "Next". This can take a second.

Step 7



You can close this dialogue by clicking "Finish". HiCrypt 2.0 is now ready for using.

4. First steps

How to start HiCrypt 2.0

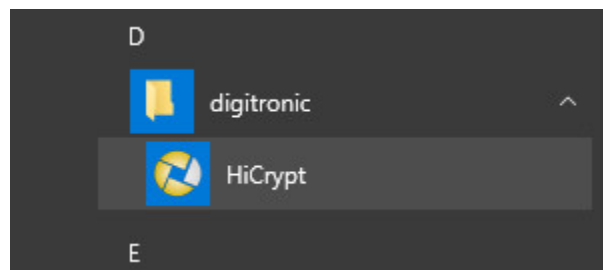
HiCrypt 2.0 will be started automatically when your operating system starts.
There are several ways to open the user interface.



You can open the interface by clicking on the symbol in your systray.



If the Hicrypt 2.0 - symbol is not shown, please use the button on the left side of your systray to show hided objectives.

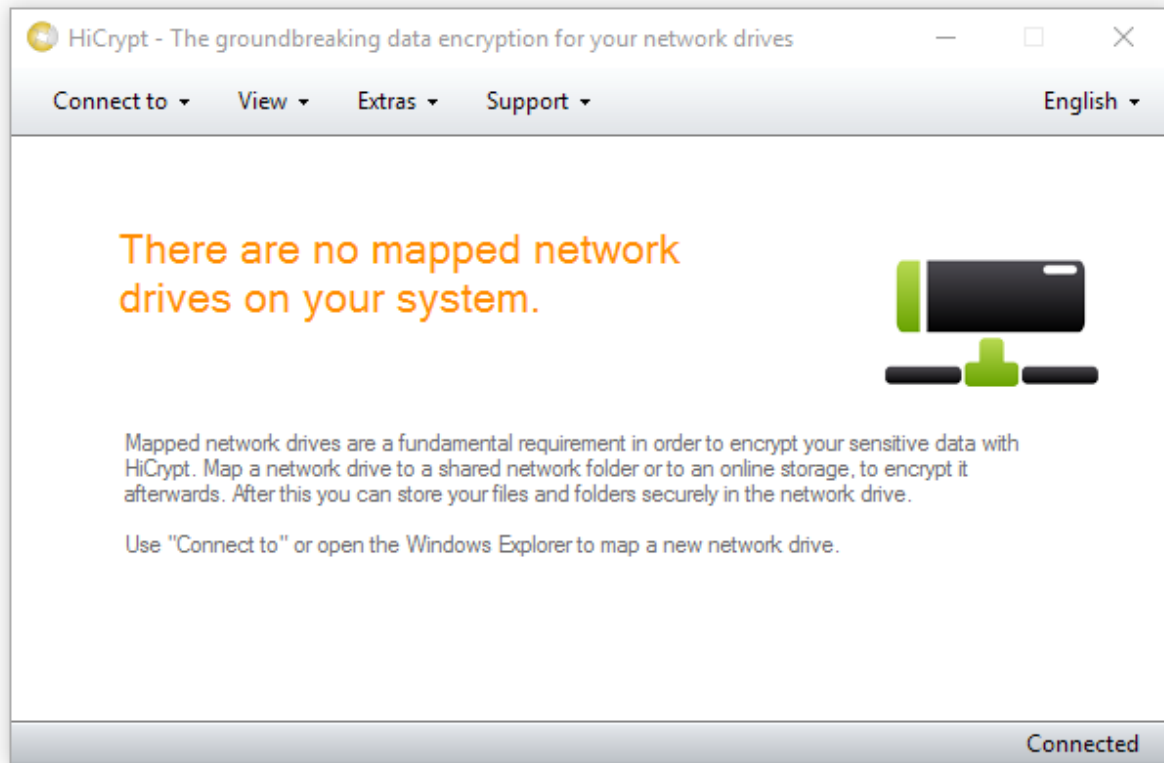


You can also use the shortcut in your **startmenu**.

How to connect network drives

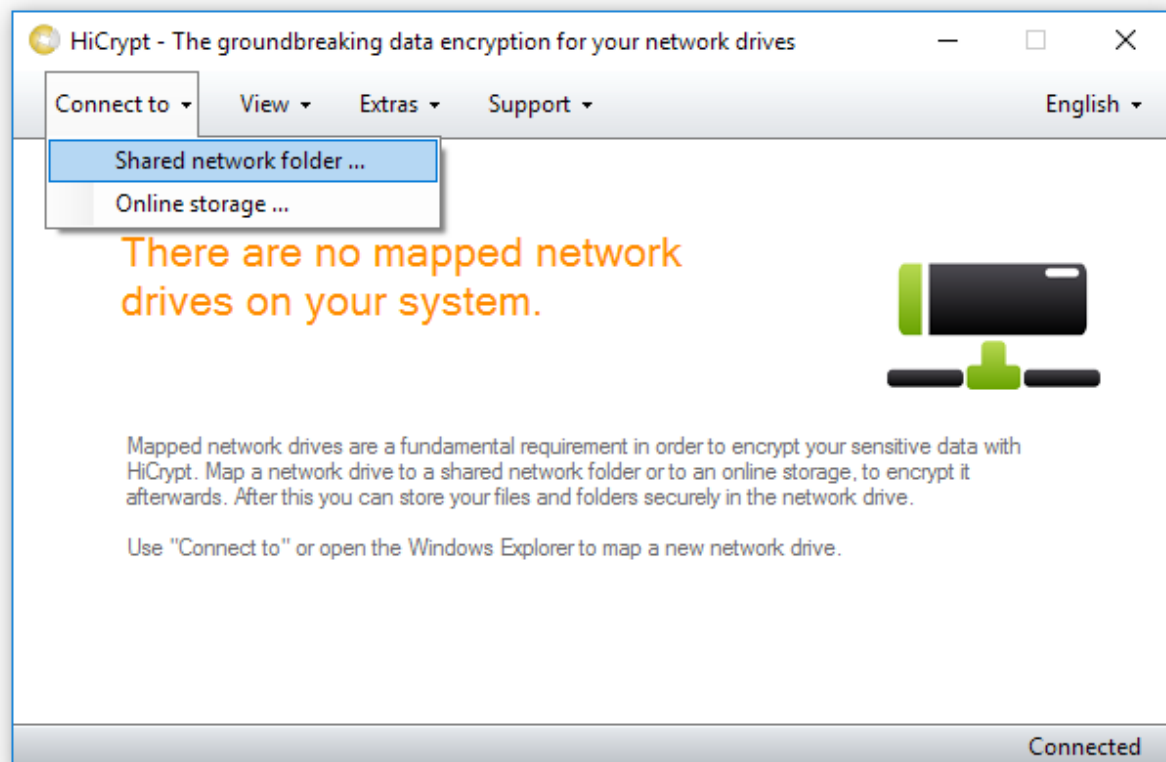
Network drives are essential for encrypt files using HiCrypt 2.0.

Step 1



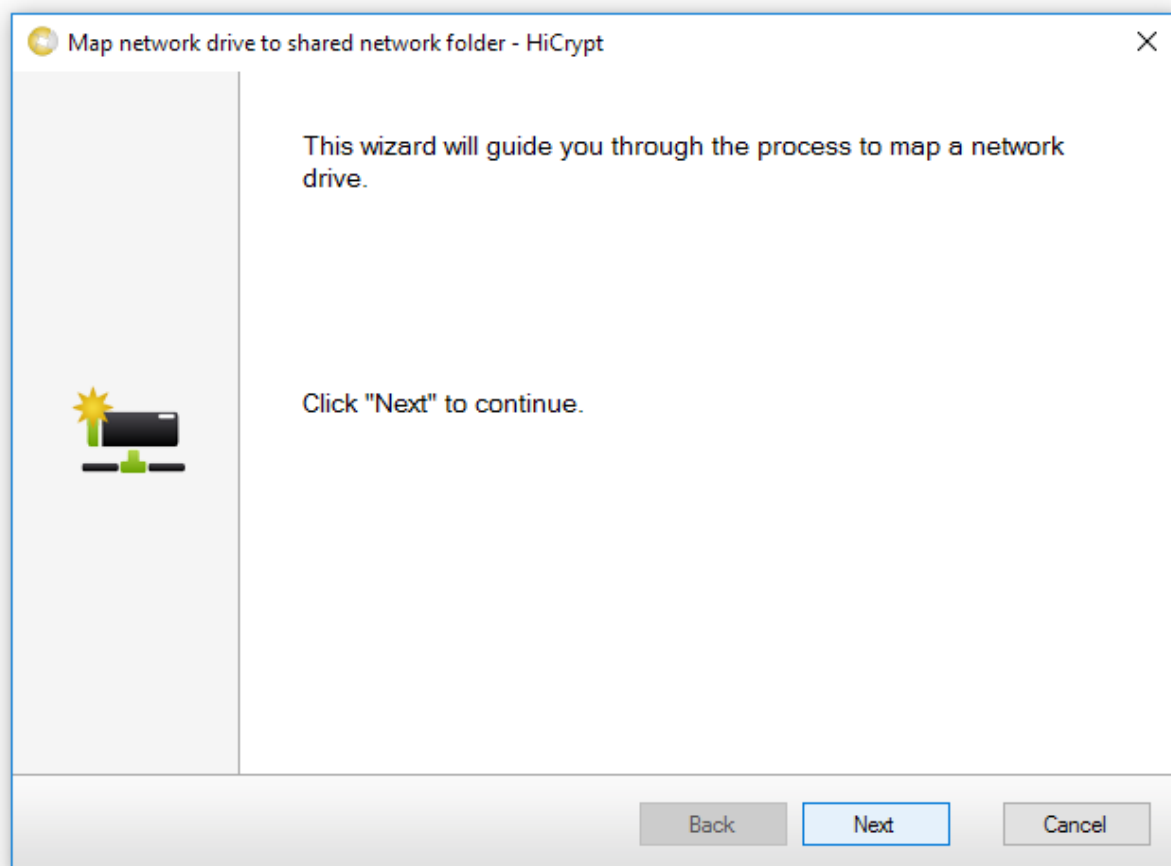
If you haven't connected any network drive yet, you can do this now with the help of HiCrypt 2.0.

Step 2



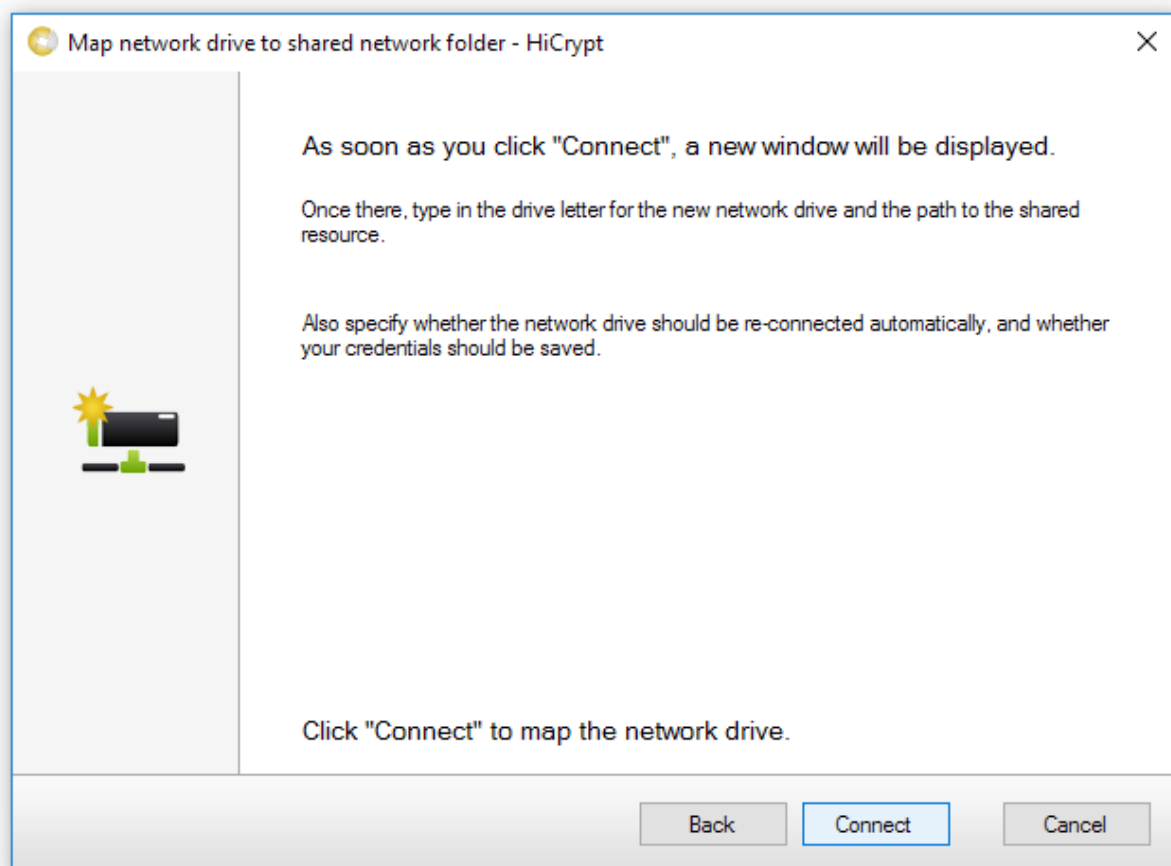
Select "Connect to" and in the next step "Shared network folder..." to connect a new network drive to a shared folder on your fileserver.

Step 3



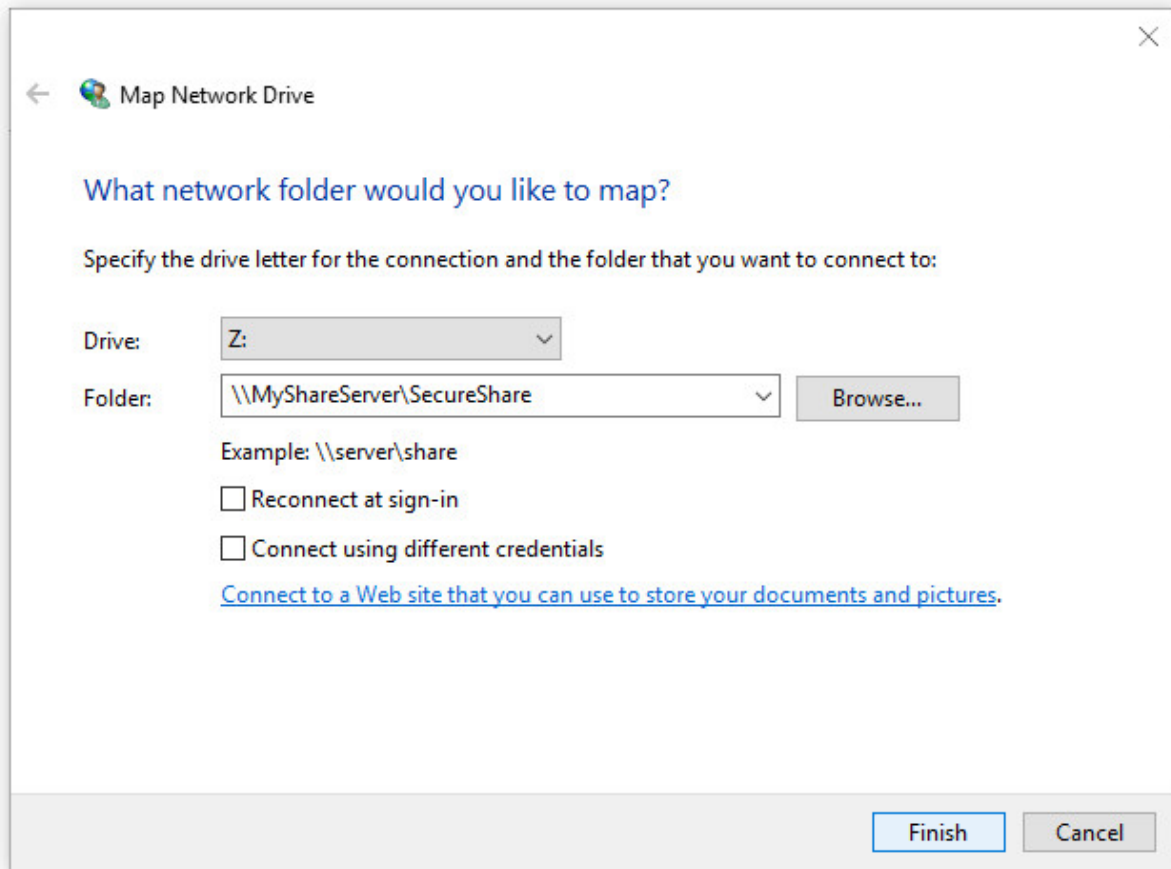
By clicking on "Next" the assistant for configure a new network drive starts.

Step 4



Please read the informations in this dialogue to be informed which kind of configuration you can specify in the following dialogue and continue by clicking on "Connect".

Step 5



← Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Z: ▼

Folder: \\MyShareServer\\SecureShare ▼ Browse...

Example: \\server\\share

☐ Reconnect at sign-in

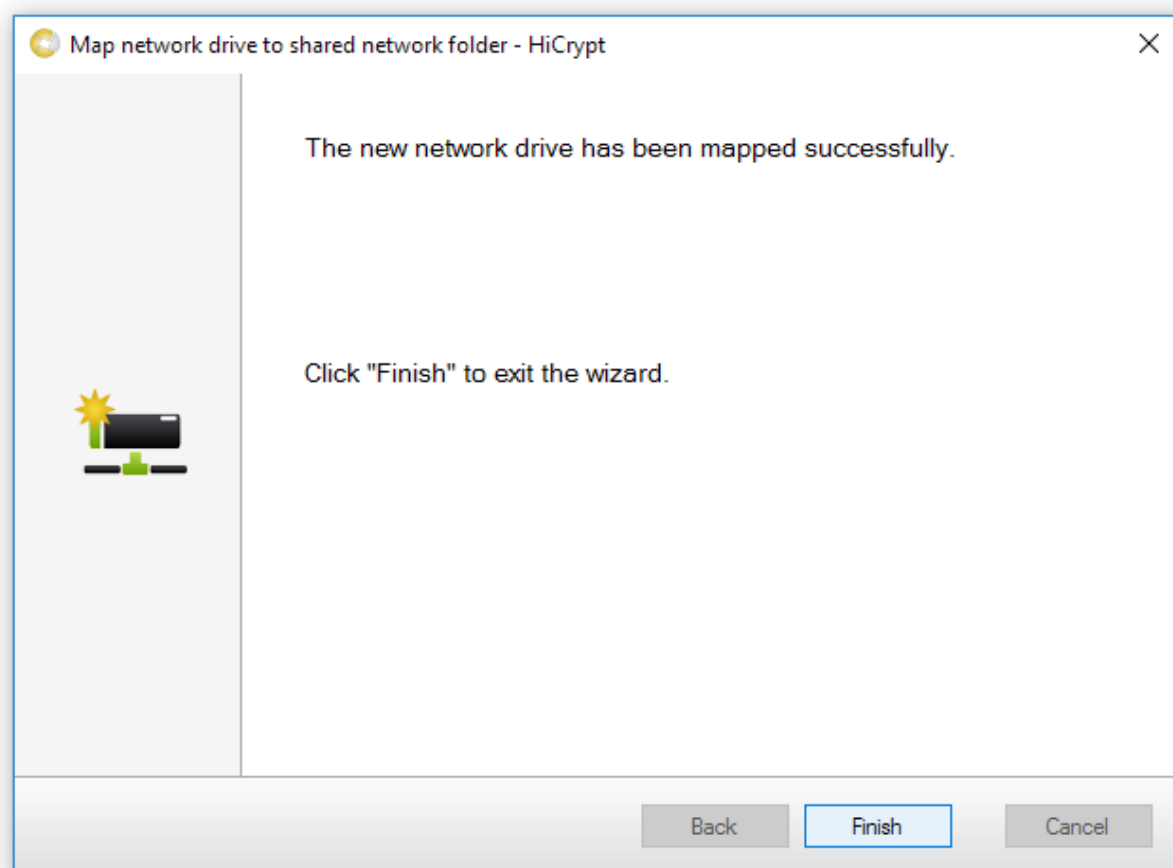
☐ Connect using different credentials

[Connect to a Web site that you can use to store your documents and pictures.](#)

Finish Cancel

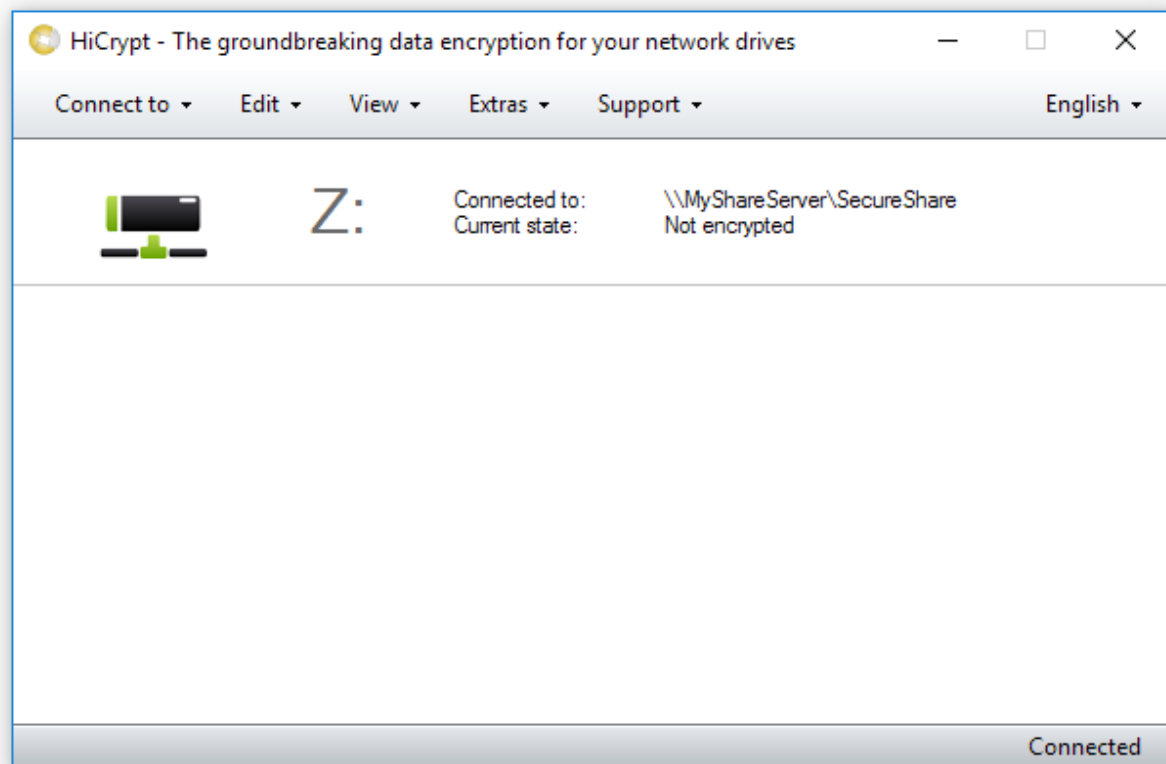
Please select a character for your drive and enter the path to the shared folder which should be connected as a new network drive. Use the options given below to specify your configuration and confirm the choice by clicking on "Finish". The network drive will be connected.

Step 6



You can finish the assistant by clicking on the button below.

Step 7



The connected network drive is now mapped in HiCrypt 2.0.

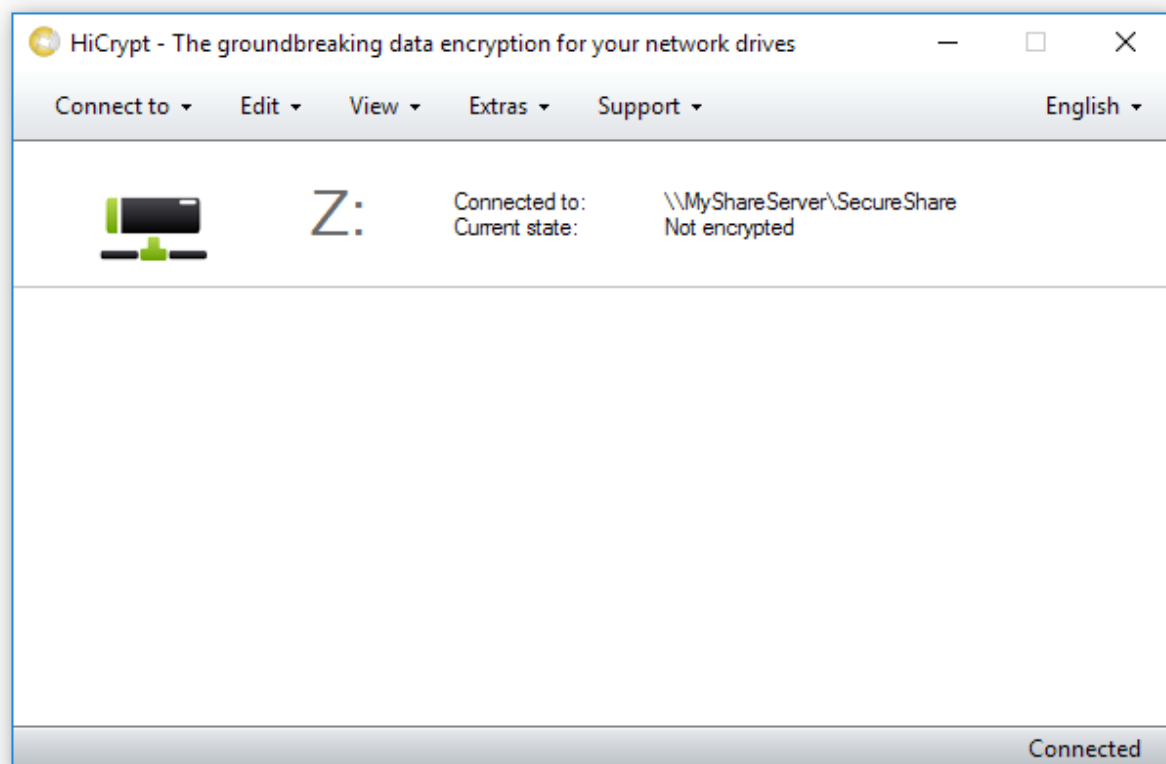
How to encrypt network drives

The status of the network drive is after mapping it is "not encrypted". The following chapter describes how to encrypt the share. Therefor you have to create a manager user which is allowed to manage the share but not to work it.

Please be sure that the connected network drive is empty before it is possible to encrypt the share with HiCrypt 2.0.

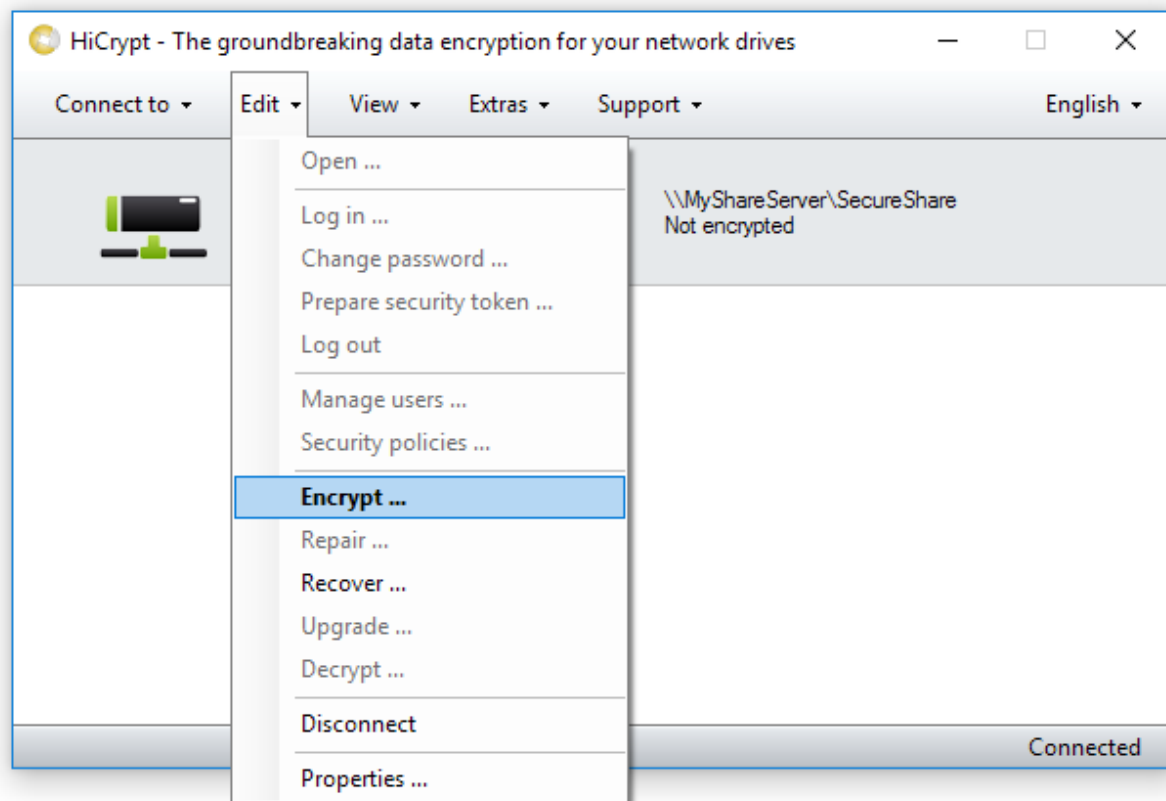
After the encryption you can save your files and directories or create new files and encrypt them automatically.

Step 1



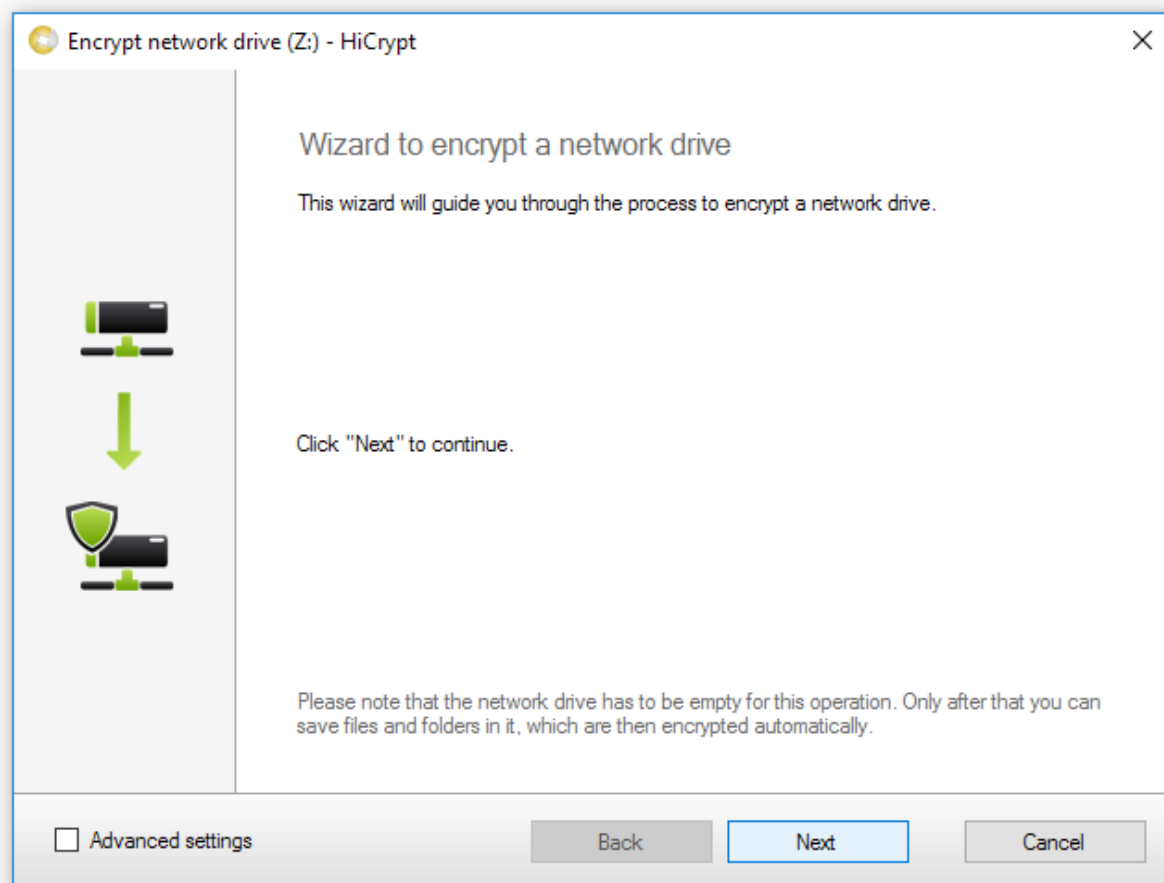
The status of your share is "not encrypted". Just click the network once to mark it.

Step 2



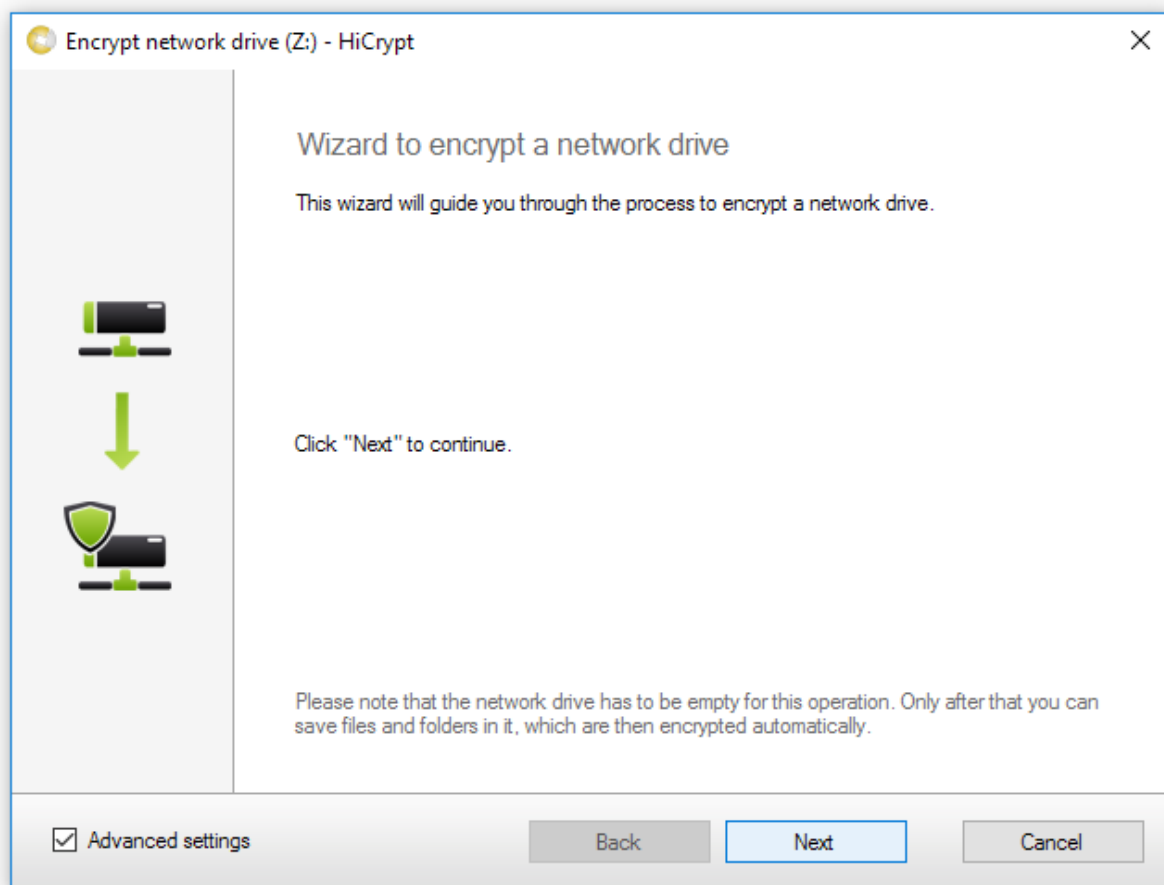
Select in the menu "Edit" and after that "Encrypt..." to encrypt the selected share.

Step 3



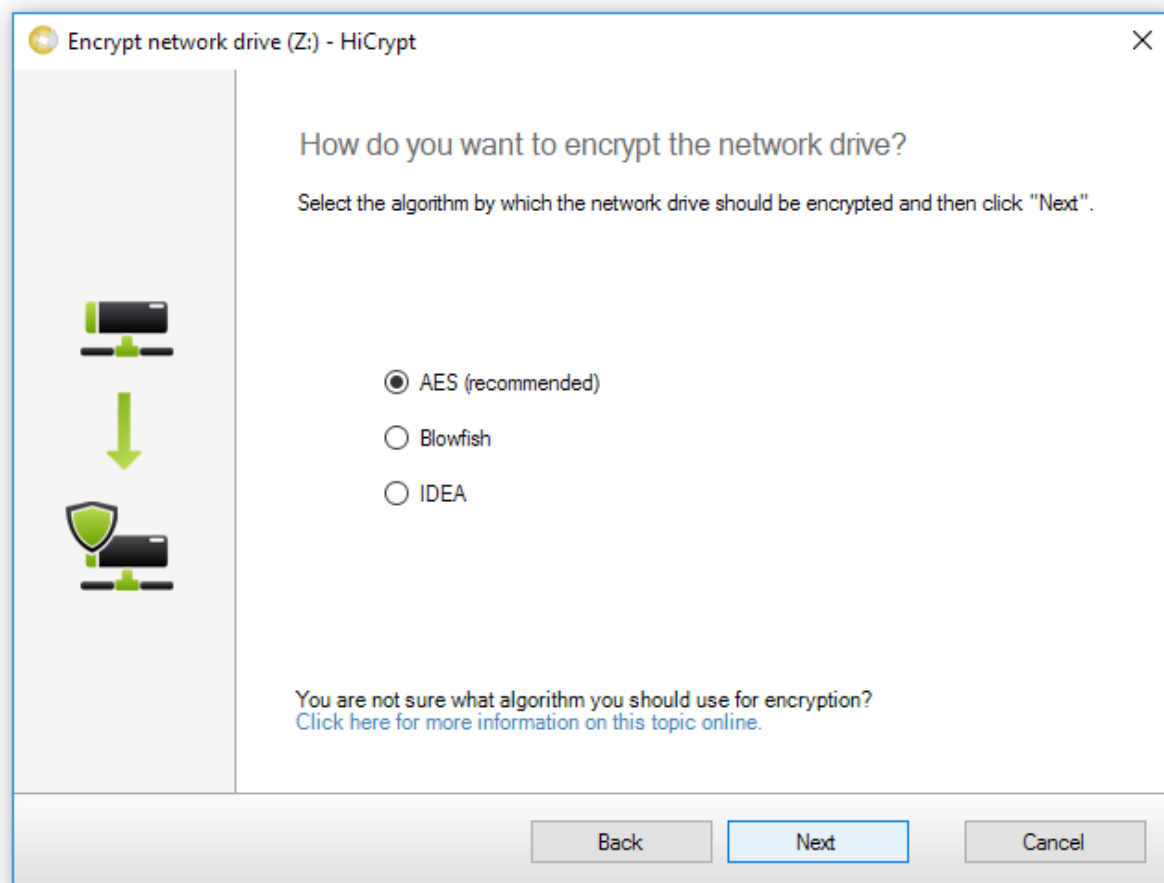
Click "Next" to start the assistant which will lead you through the process of the encryption for your linked share.

Step 3.1



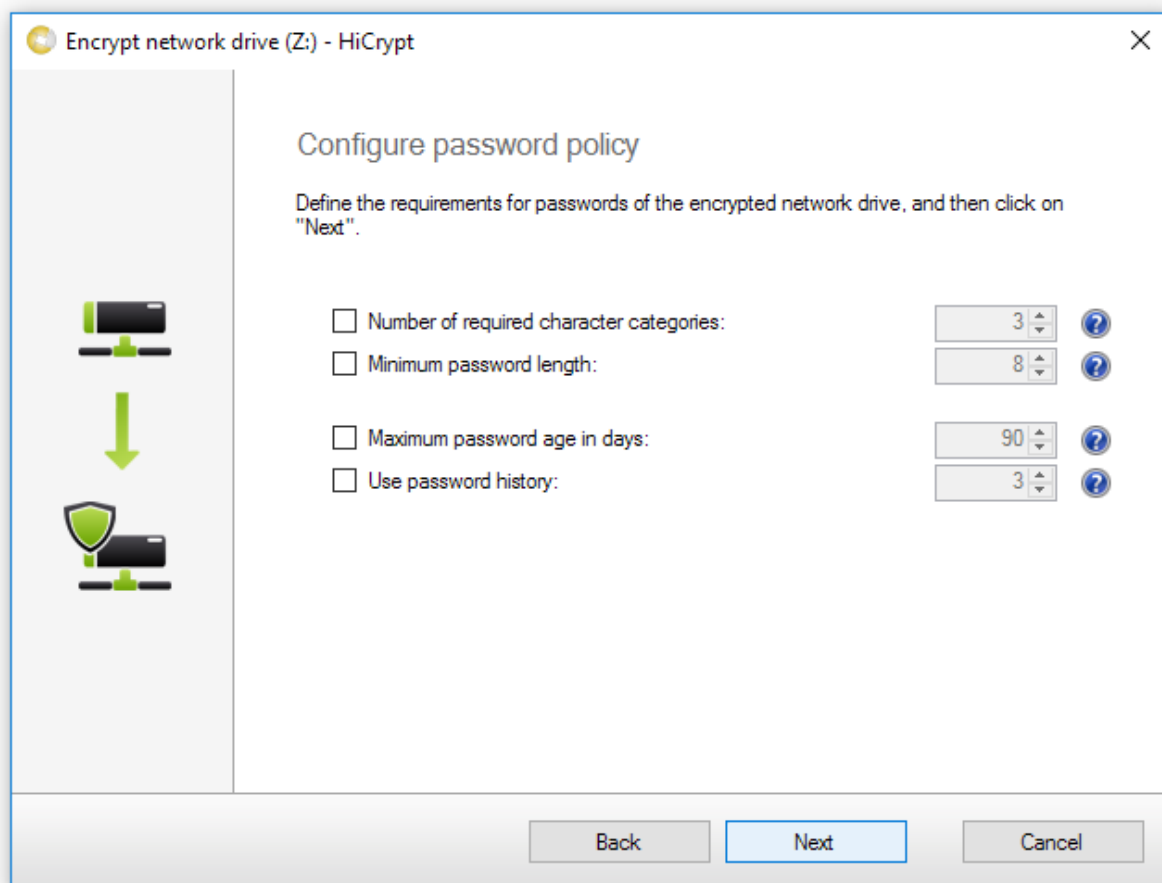
If you want to see advanced settings, please mark this option in the lower left corner. You will have to decide which algorithm will be used. Then click "Next" to continue.

Advanced settings A



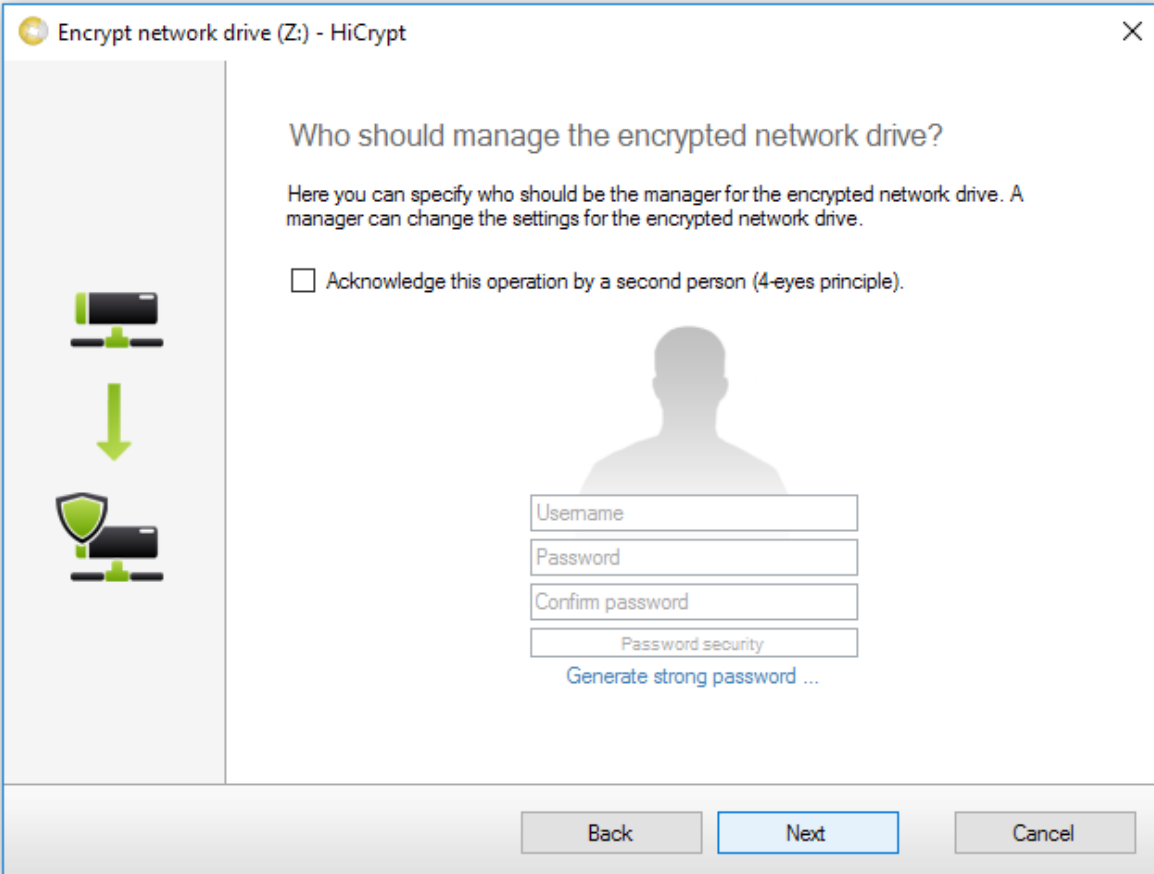
Please choose the algorithm you want to be used for encryption and confirm your choice by clicking "Next".

Advanced settings B



In this dialogue you can configure the password policy. If you use SecurityToken for the authentication against HiCrypt 2.0 and the users should not know their passwords, we recommend you to use no maximum password age in days.

Step 6



Encrypt network drive (Z:) - HiCrypt

Who should manage the encrypted network drive?

Here you can specify who should be the manager for the encrypted network drive. A manager can change the settings for the encrypted network drive.

☐ Acknowledge this operation by a second person (4-eyes principle).

Username

Password

Confirm password

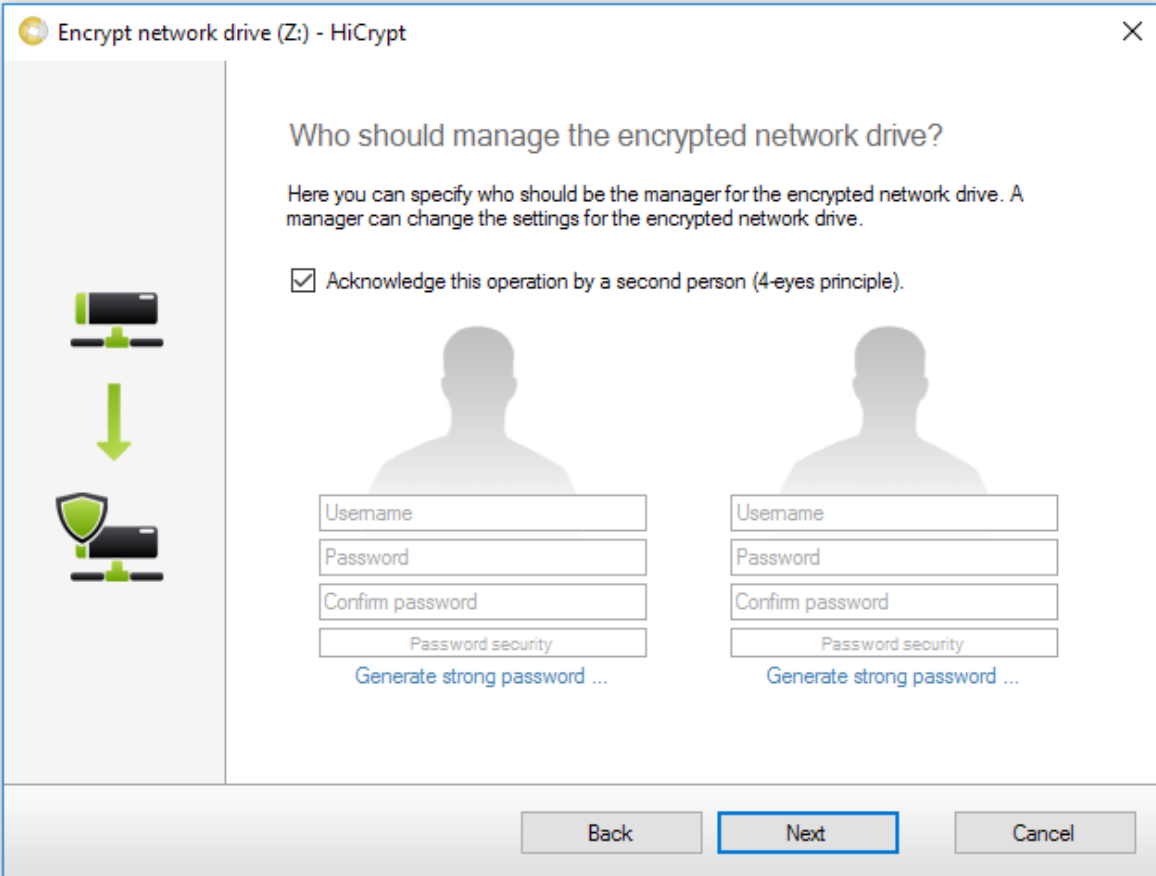
Password security

[Generate strong password ...](#)

Back Next Cancel

In this dialogue you have to decide who will be the manager of the new share. You can enter here any username you want, it has no relation to the actual windows user. You will need this manager account to manage your share, not to have access to the files saved on it.

Four-Eye-Principal



Encrypt network drive (Z:) - HiCrypt

Who should manage the encrypted network drive?

Here you can specify who should be the manager for the encrypted network drive. A manager can change the settings for the encrypted network drive.

☒ Acknowledge this operation by a second person (4-eyes principle).

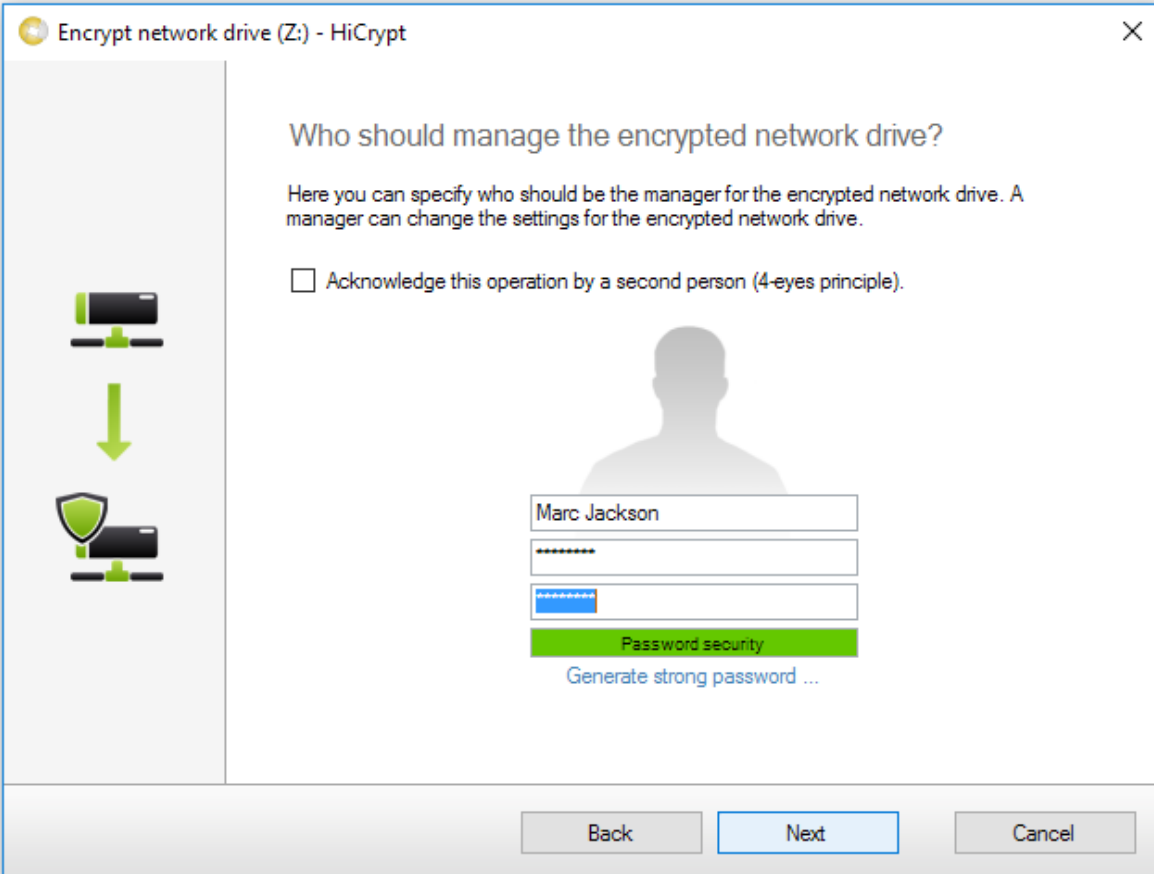
Username
Password
Confirm password
Password security
Generate strong password ...

Username
Password
Confirm password
Password security
Generate strong password ...

Back Next Cancel

There is the possibility to create 2 managers, but have in mind that both will be necessary to change options for your share.

Step 7



Encrypt network drive (Z:) - HiCrypt

Who should manage the encrypted network drive?

Here you can specify who should be the manager for the encrypted network drive. A manager can change the settings for the encrypted network drive.

☐ Acknowledge this operation by a second person (4-eyes principle).

Marc Jackson

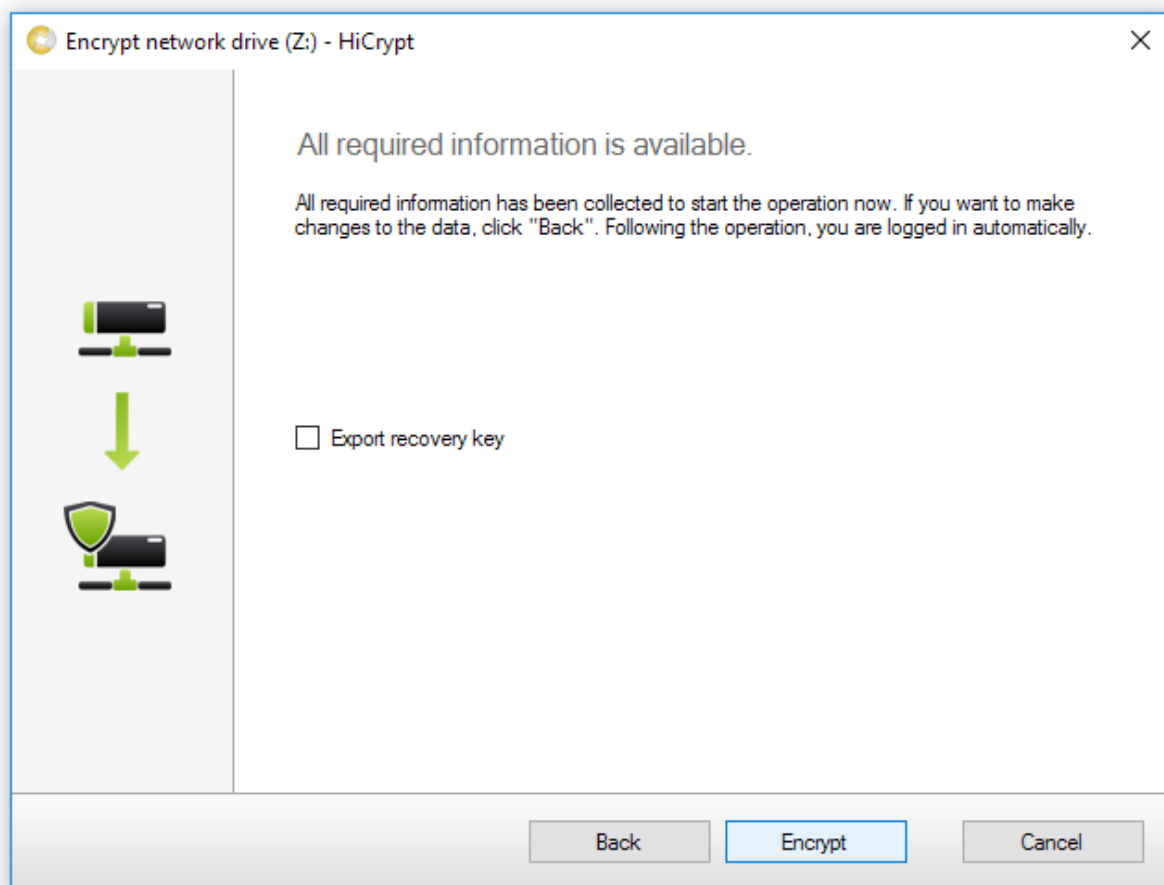
Password security

[Generate strong password ...](#)

Back Next Cancel

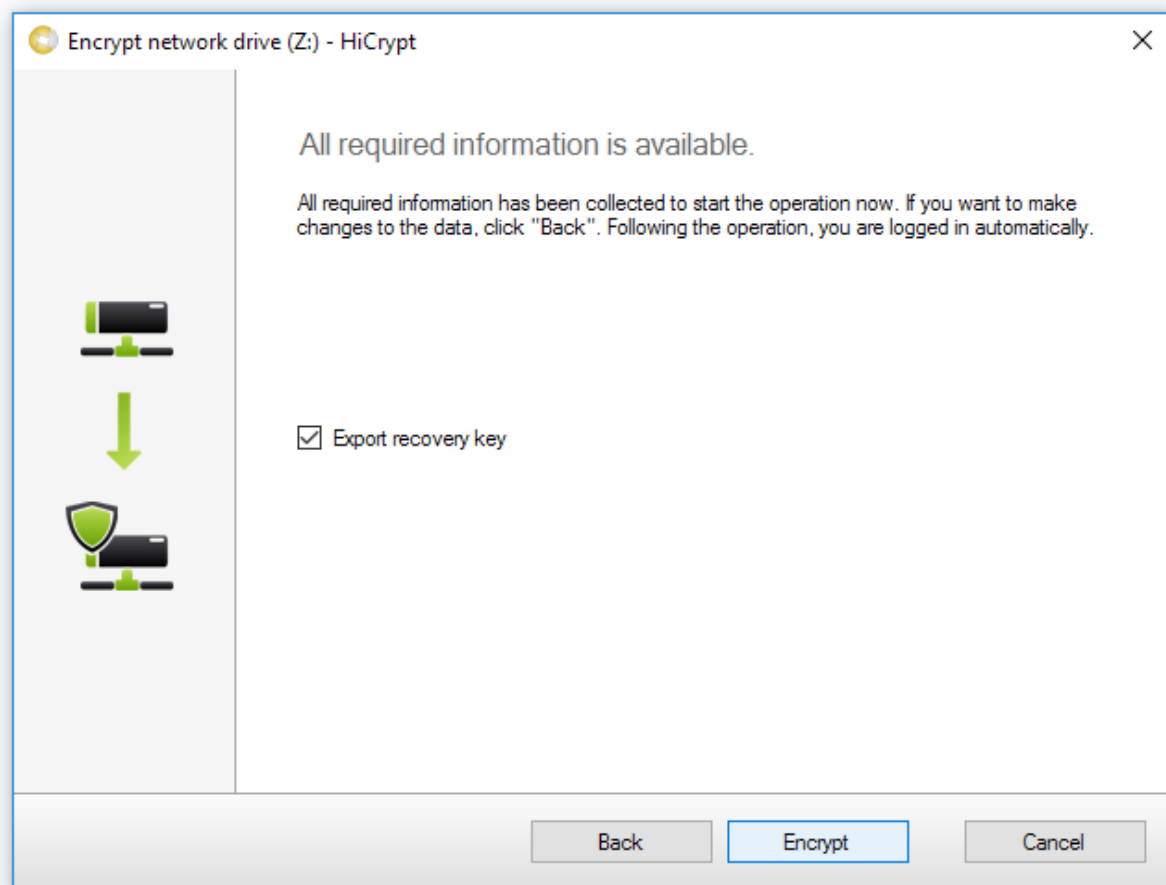
The created manager/-s are able to assign other users access to the files on the share, change the security policies or decrypt the share.
Confirm your input by clicking "Next".

Step 8



Encrypt the network drive by clicking "Encrypt".

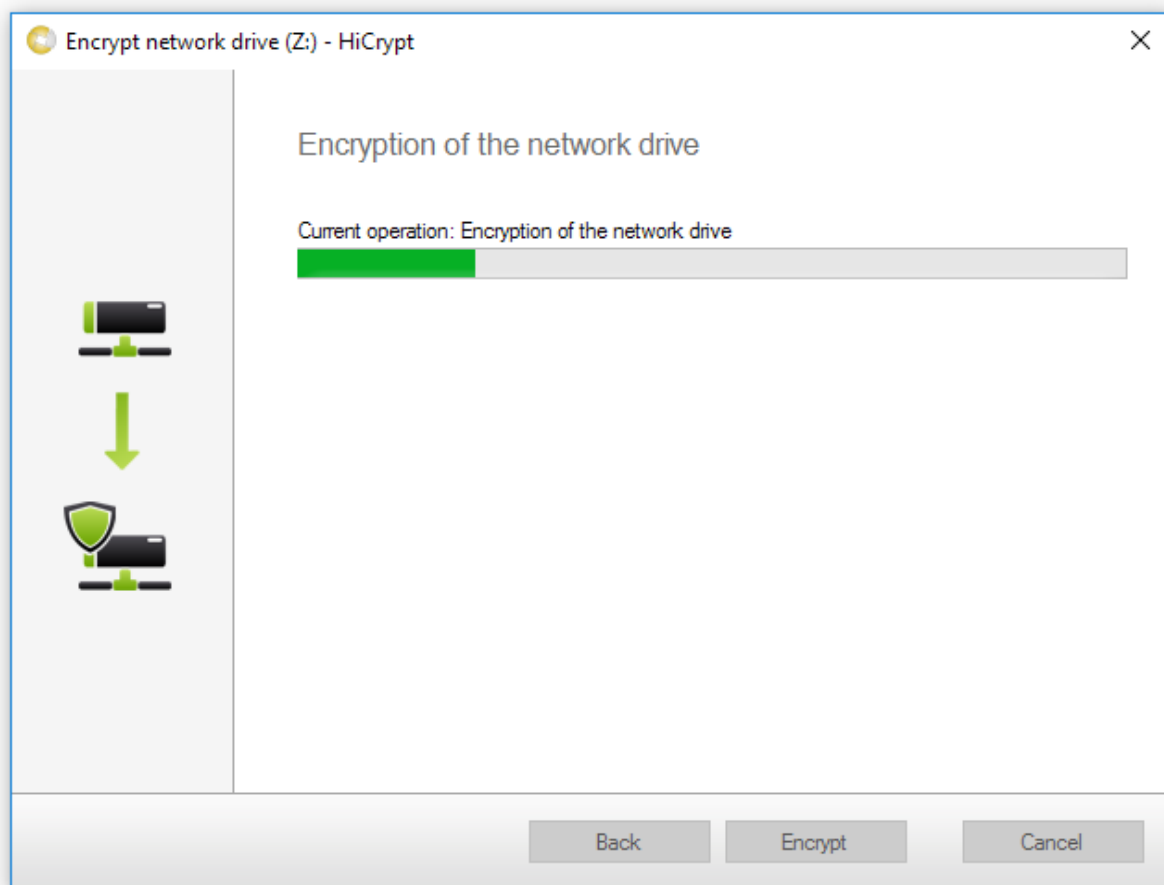
Export the recovery key



Before encrypting your share, you have now and just in this dialogue the option to export your recovery key.

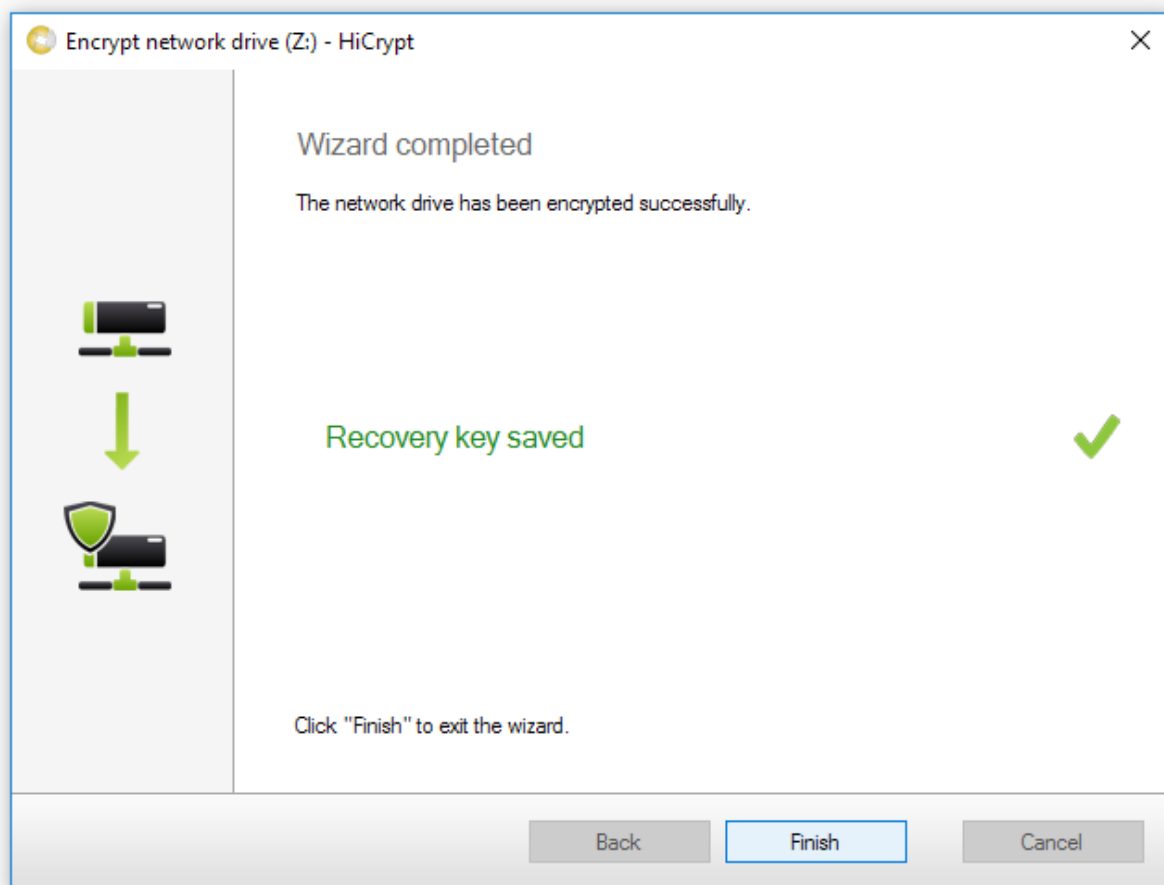
Save this recovery key on an external drive and keep it safe.

Step 9



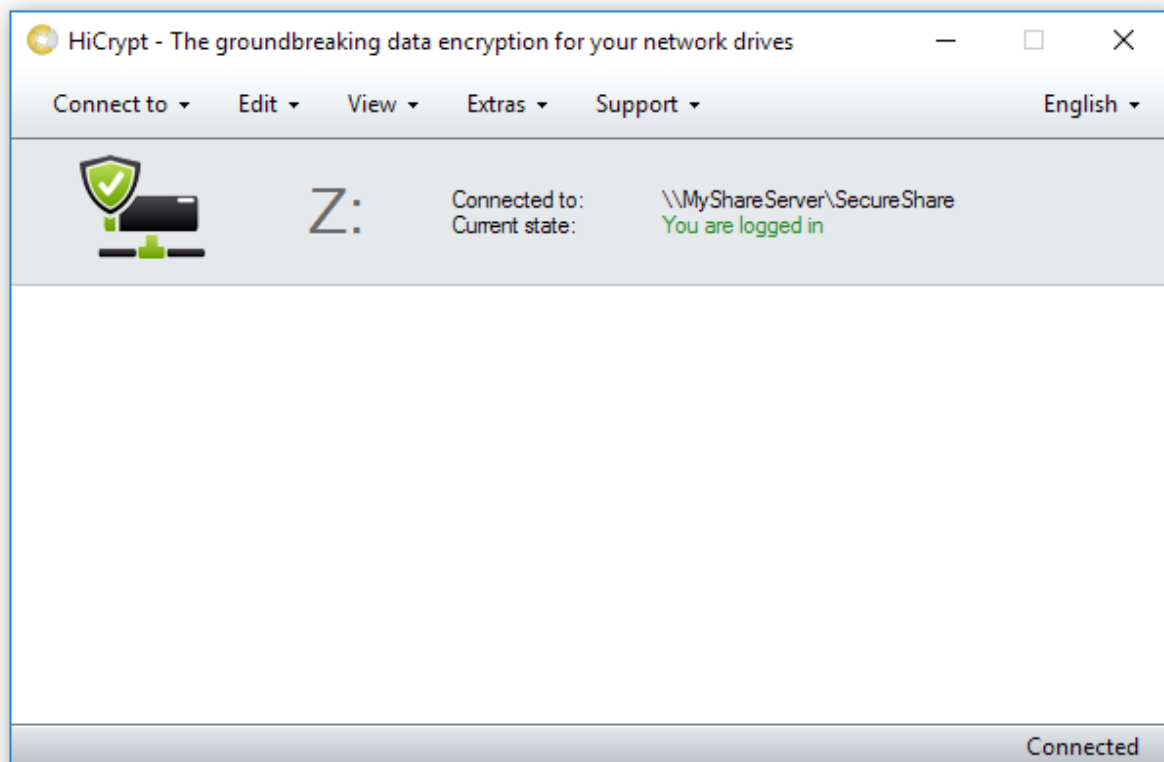
After a successful encryption you will be logged in on the encrypted share automatically.

Step 10



Exit the wizard by clicking "Finish".

Step 11



The network drive is now encrypted. Files you save here will be encrypted without any action you have to do.

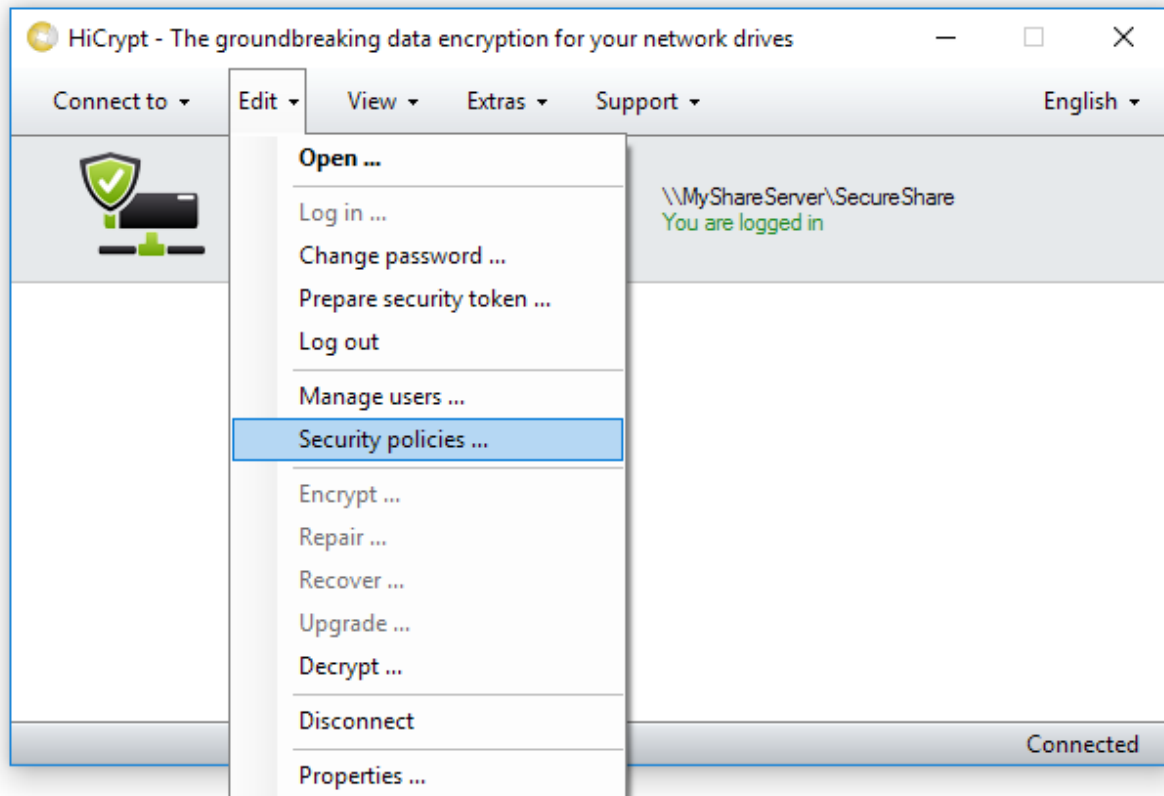
The given instruction to encrypt a network drive has to be repeated for every share you want to encrypt. If an encrypted share will be connected, HiCrypt 2.0 will ask for login informations.

This informations can be saved to be logged on automatically.

Security policies

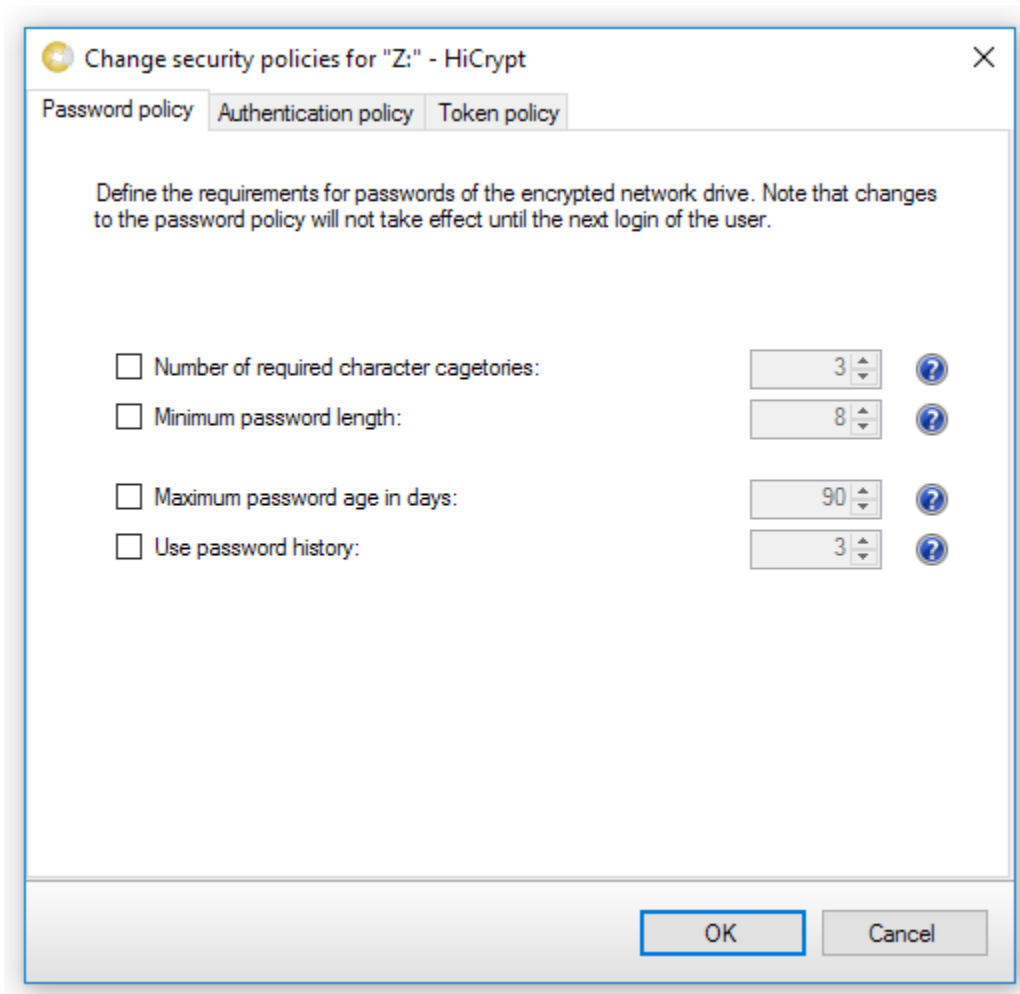
The security policies have to be set for every single share.

Step 1



To open the dialogue of the security policies you have to click in "Edit" and after that on "Security policies".

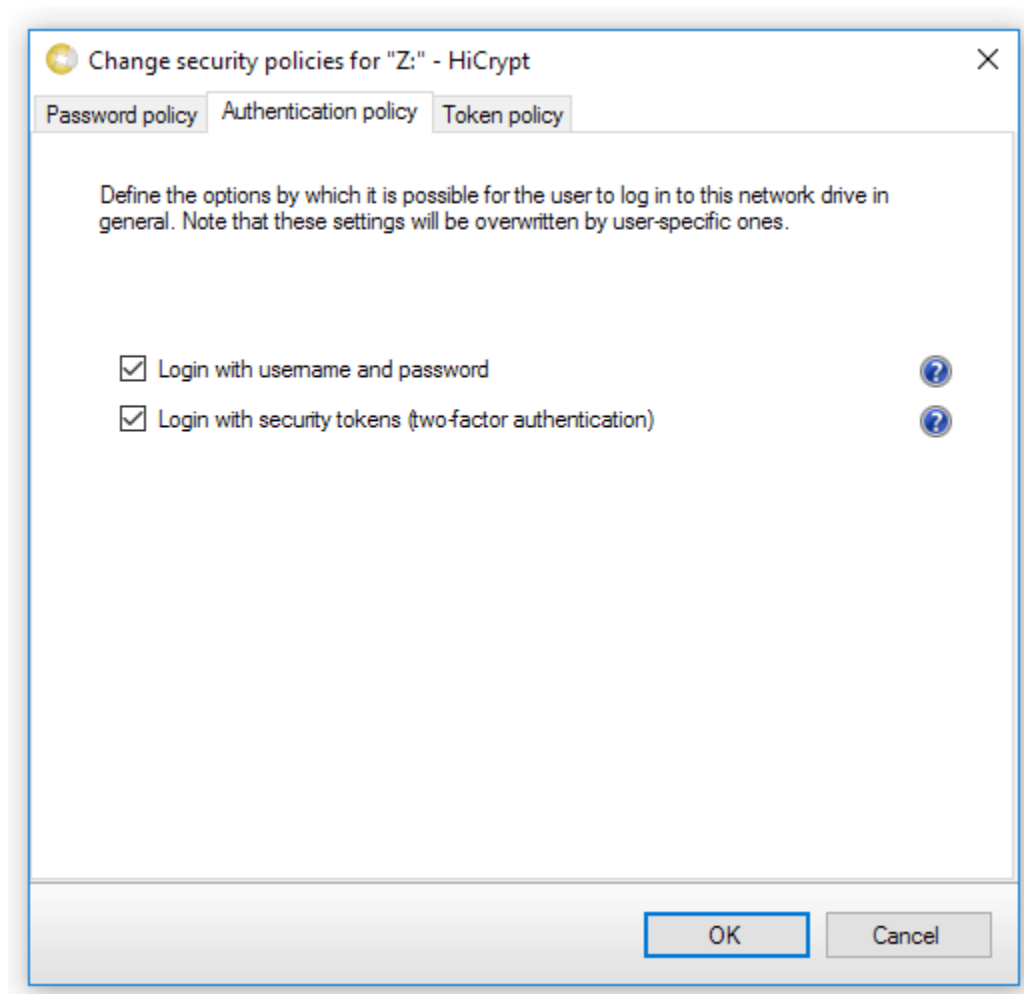
Password policy



You can change the password policies in this dialogue.

If you change the password, please recognize that changes will have no effect until the next change of the password.

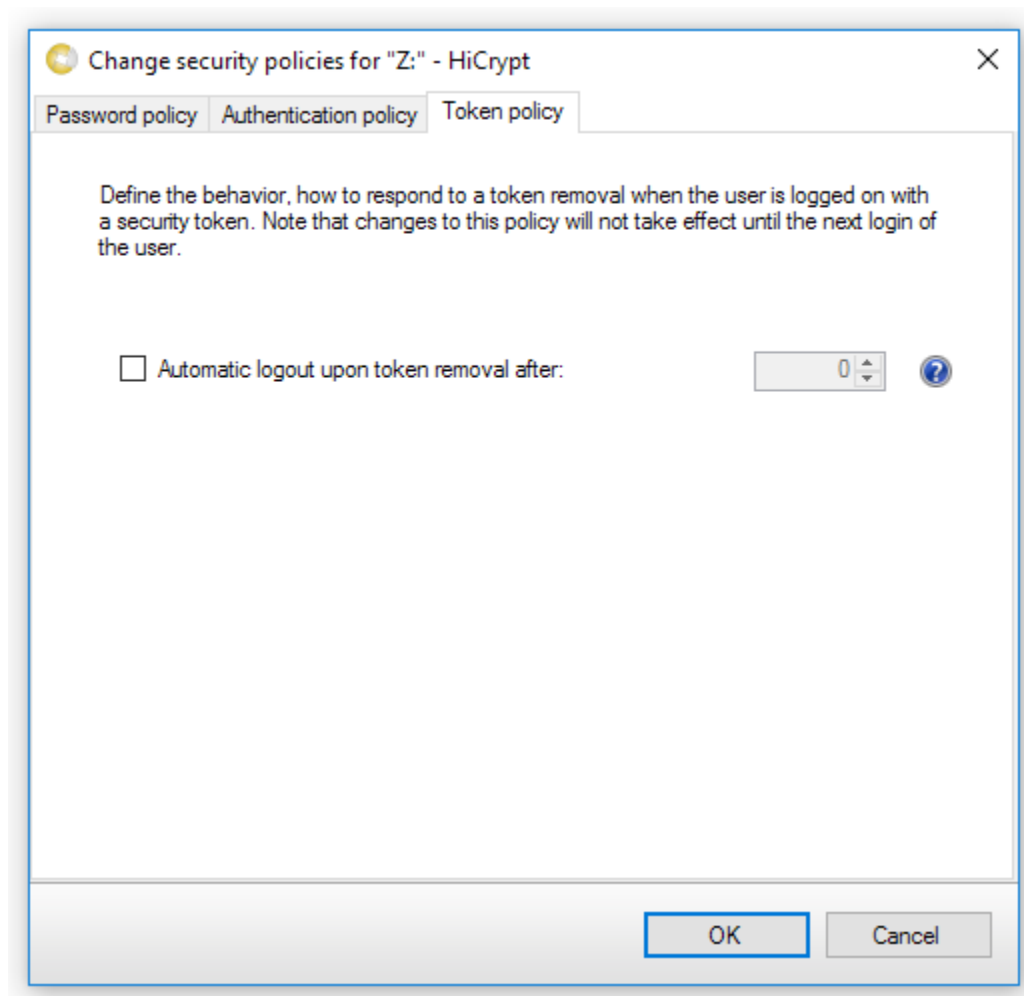
Authentication policy



In this dialogue you can set which kind of login is allowed.

After an encryption the login with username and password is allowed, login with security tokens is forbidden.

Token policy

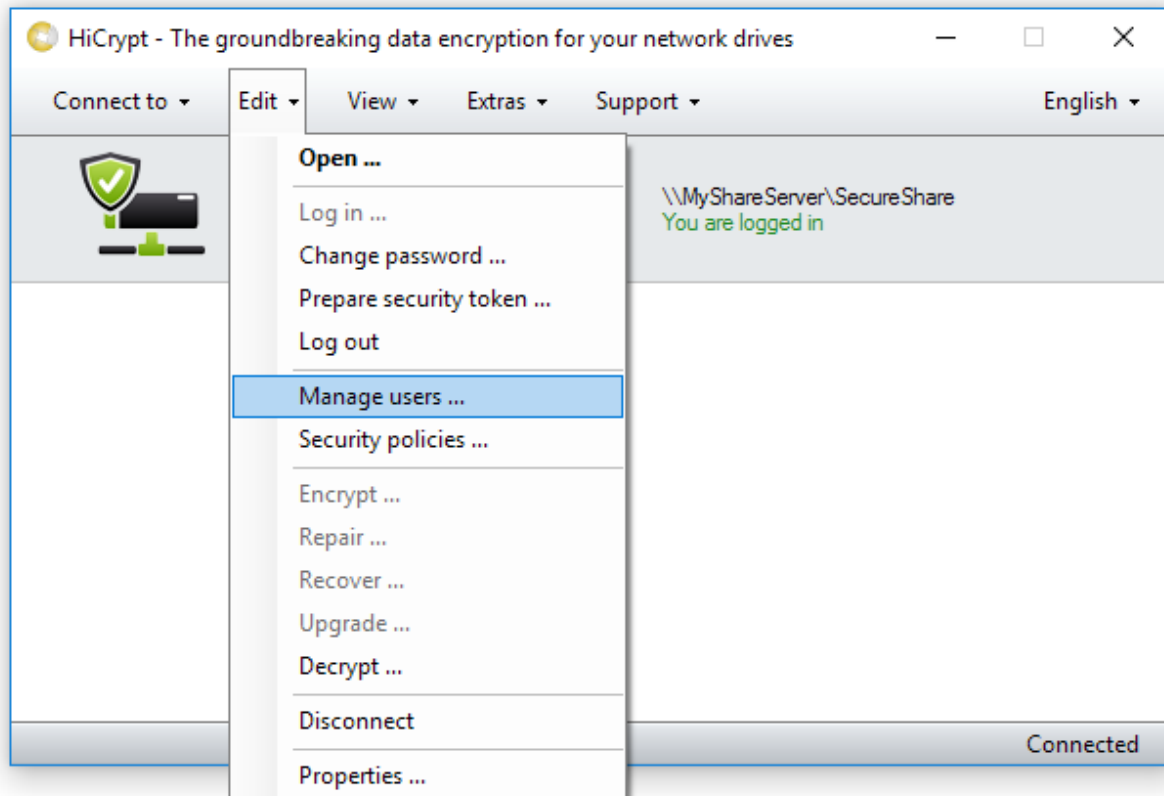


In this dialogue you can set a timer which disconnect all shares after a security token is removed.

User management

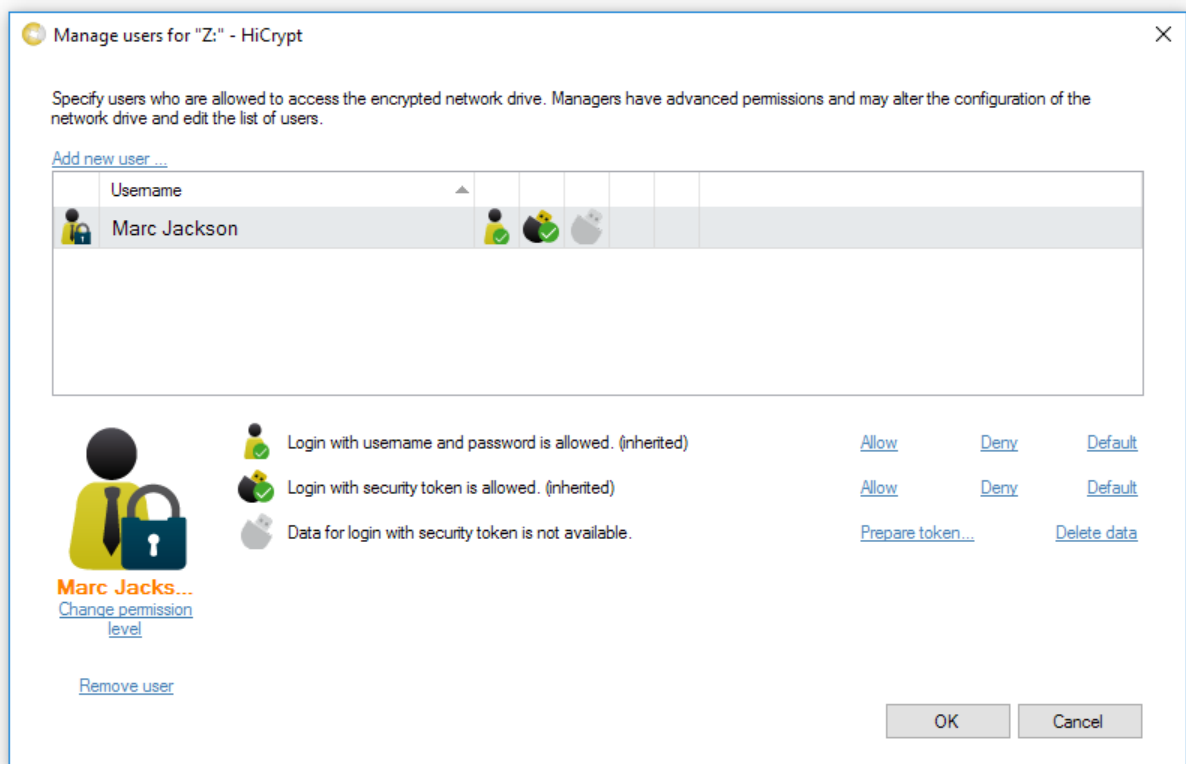
To give other users access to the encrypted share, you can add them following this description.

Step 1



To get to the user management dialogue, click on "Edit" and after that on "Manage users...".

Step 2

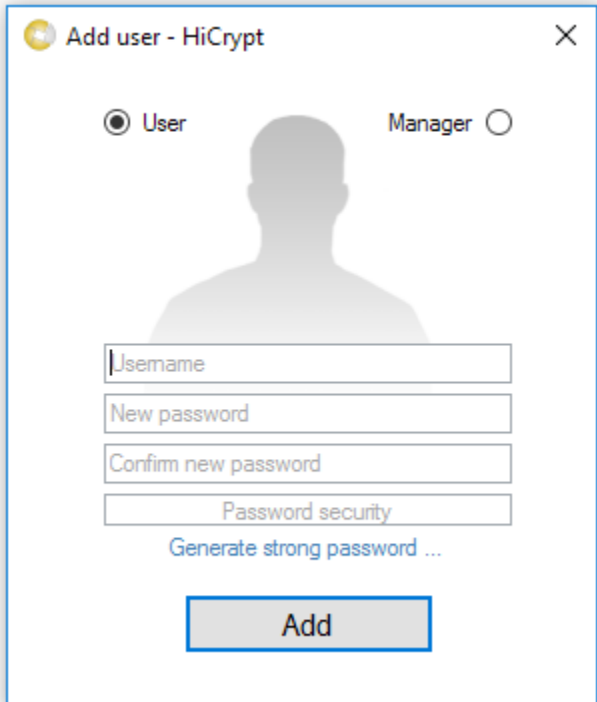


In this dialogue you can add new users to the encrypted share or change the authorization level of an existing user.

The manager who opens this dialogue is protected and his profile can not be changed.

Clicking on "Add new user..." will open the following dialogue.

Add user 1



Add user - HiCrypt

☒ User ☐ Manager

Username

New password

Confirm new password

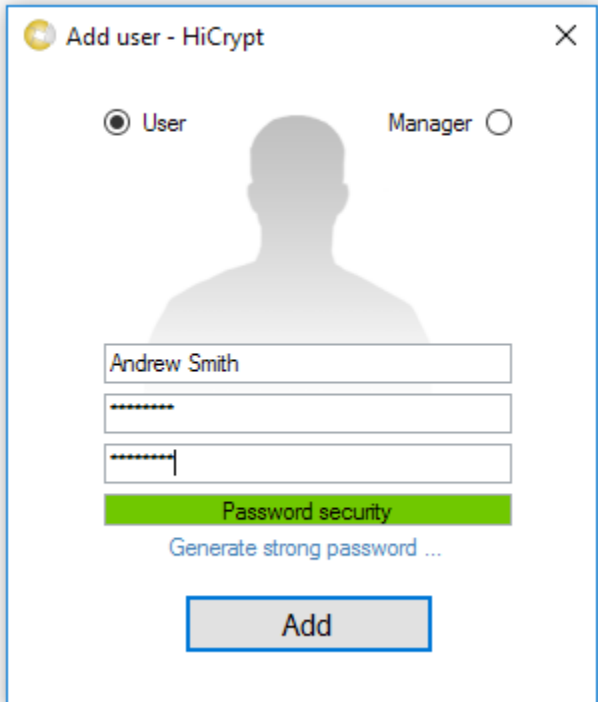
Password security

[Generate strong password ...](#)

Add

A new user is always added by entering a username and a password, it is not important if he can log on with this informations later or not.

Add user 2



Add user - HiCrypt

☒ User ☐ Manager

Andrew Smith

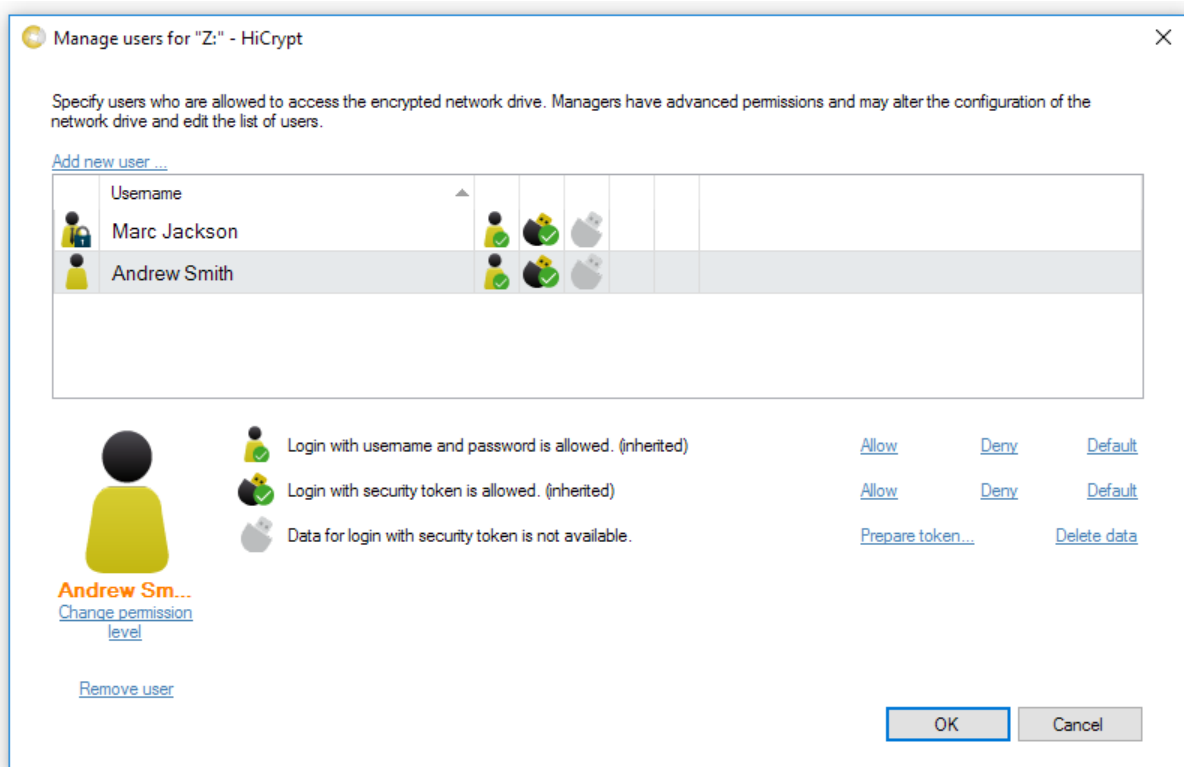
Password security

[Generate strong password ...](#)

Add

When you entered the username and password, you add the new user by clicking on "Add".

Step 5



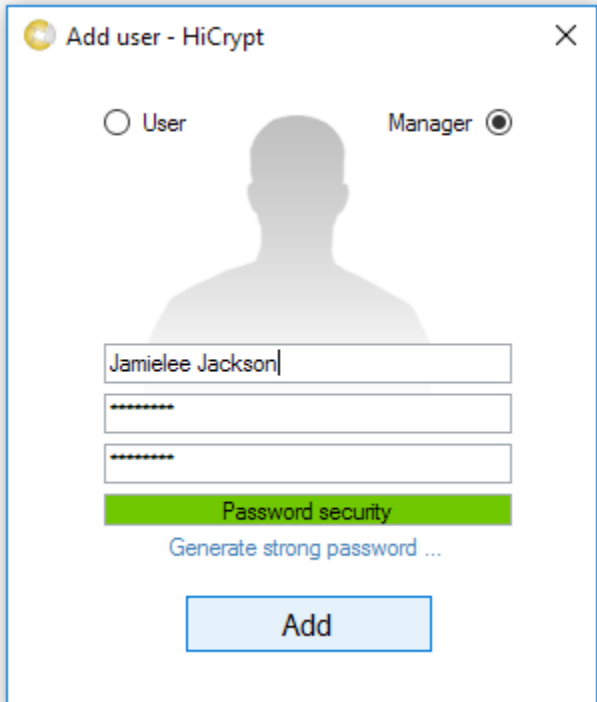
In the overview the new user is added, and he has the permission level "User".

A user is identified by his missing tie.

To create a new manager, you have to add a new user.

Managers are identified by a tie.

Add manager



Add user - HiCrypt

☐ User ☒ Manager

Jamelee Jackson|

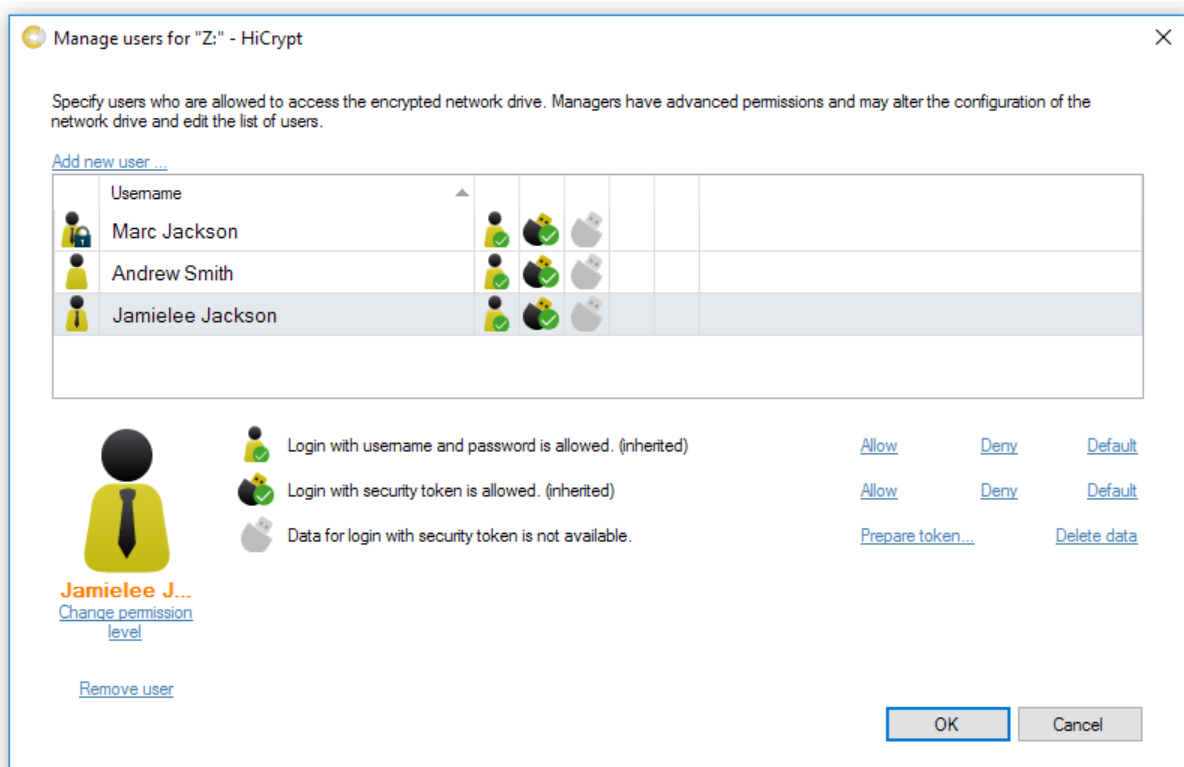
Password security

[Generate strong password ...](#)

Add

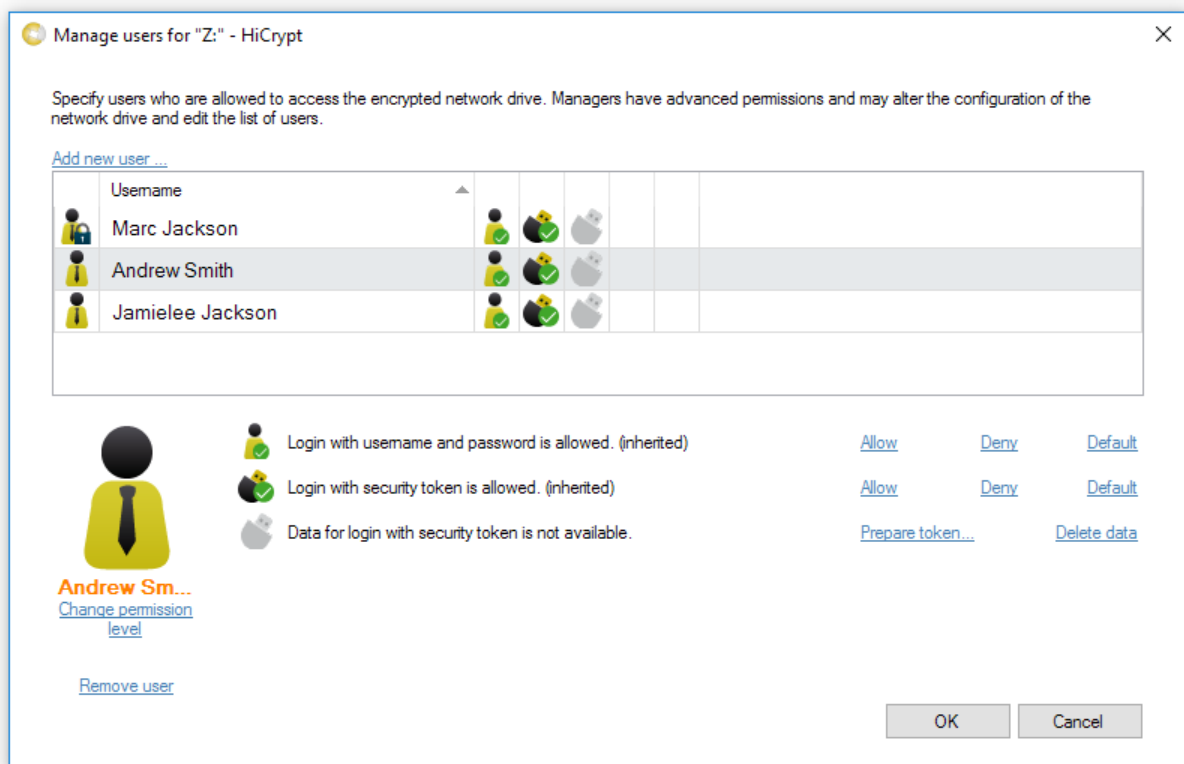
The presetting for creating new users is set to users, but in the upper right corner you can change it to add a new user and give him the permission to manage the share. To add a new manager, enter an username and a password and confirm by clicking "Add".

Step 7



The new manager is added in the overview.

Changing an existing user



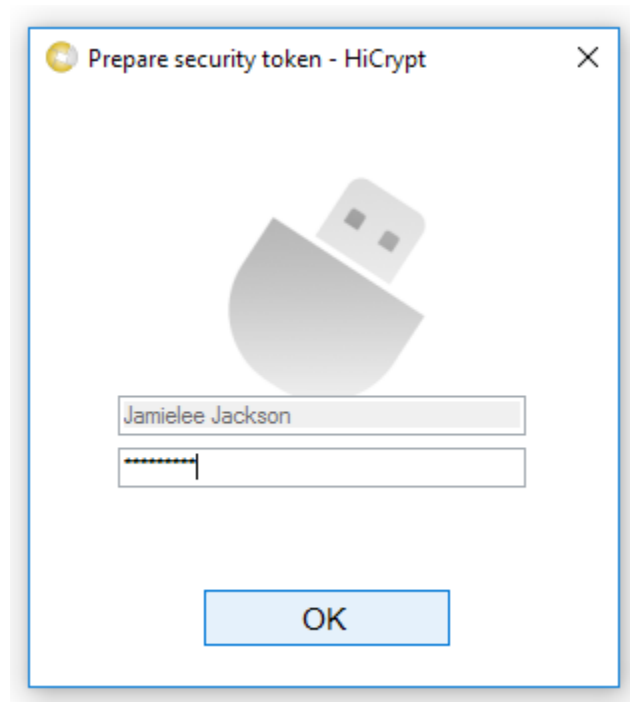
To change the permission of an existing user, you can follow the link "Change permission level".

The changes will be shown instantly in the overview.

To remove a user you have to follow the link "Remove user".

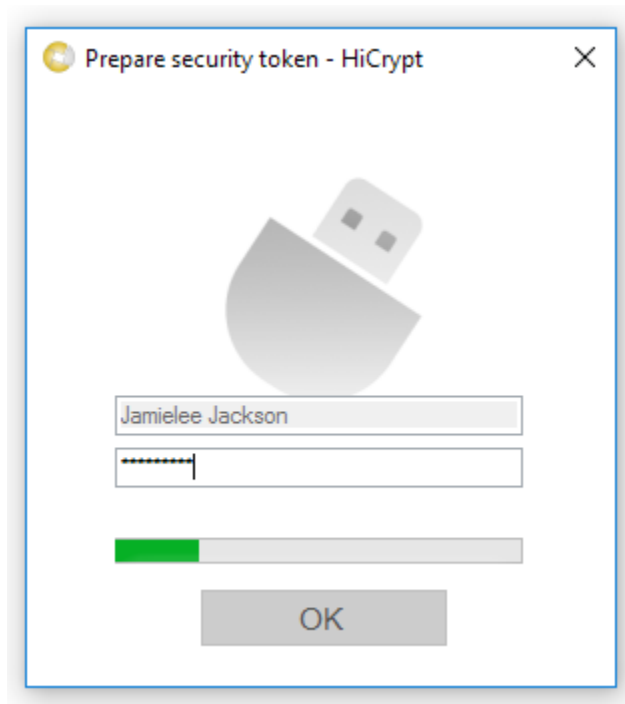
To prepare a security token you have to mark the user you want to connect and follow the link "Prepare token...".

Prepare token 1



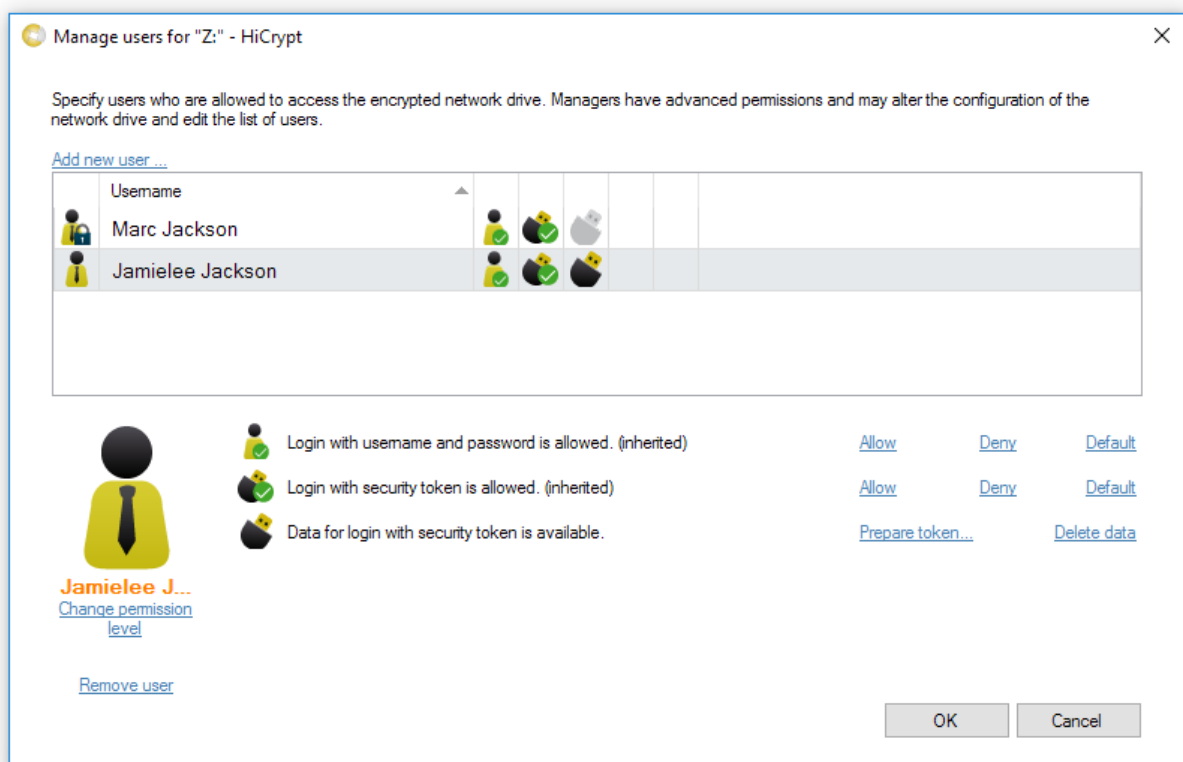
You have to enter the username and the password in this dialogue and confirm by clicking "OK".

Prepare token 2



The security token creates a pair of keys which is connected with the user informations.
This can take a moment.

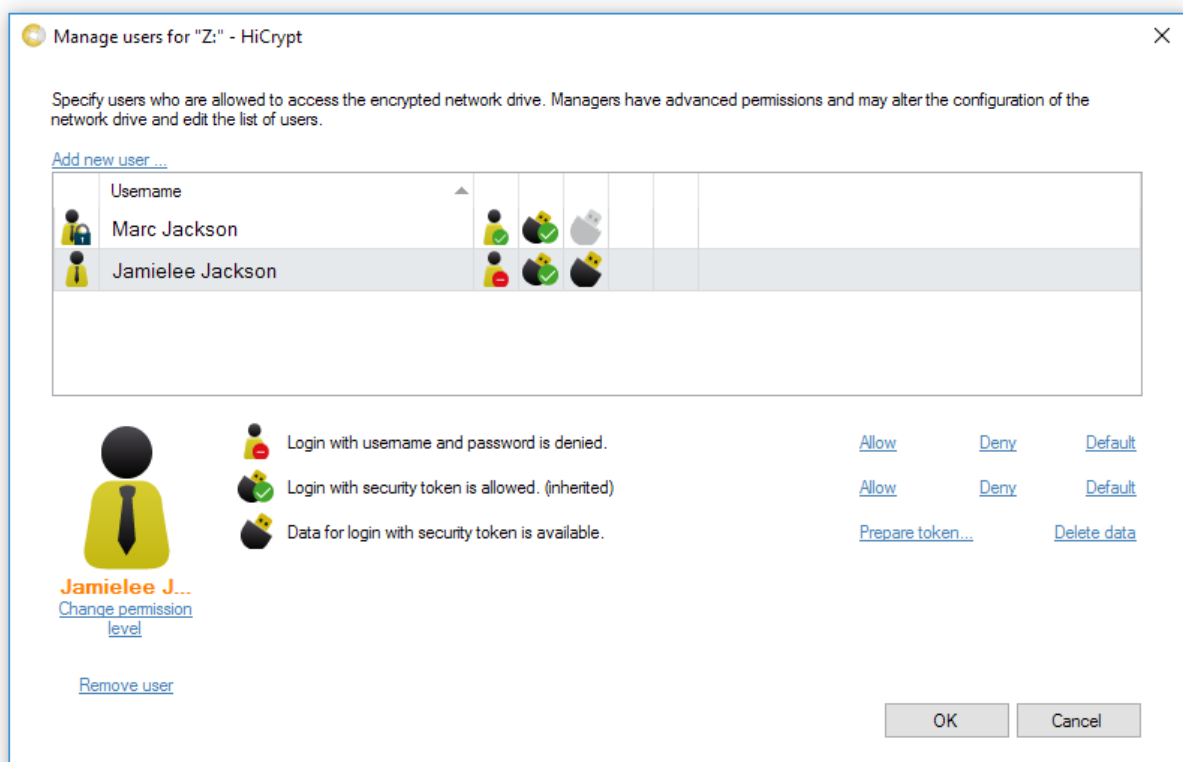
Token activated



After a successful preparation the symbol for the token authentication in the overview is coloured.

"Delete data" just disconnect relation between user and token, but the pair of keys stays on the token.

Log on permissions user



After marking a user, it is possible to change the log in permissions.
 If there is a inherited in brackets behind an option, it means that this setting was defined by the standard settings (security policies).

The red sign in front of the icon means that this log on permission is not allowed.

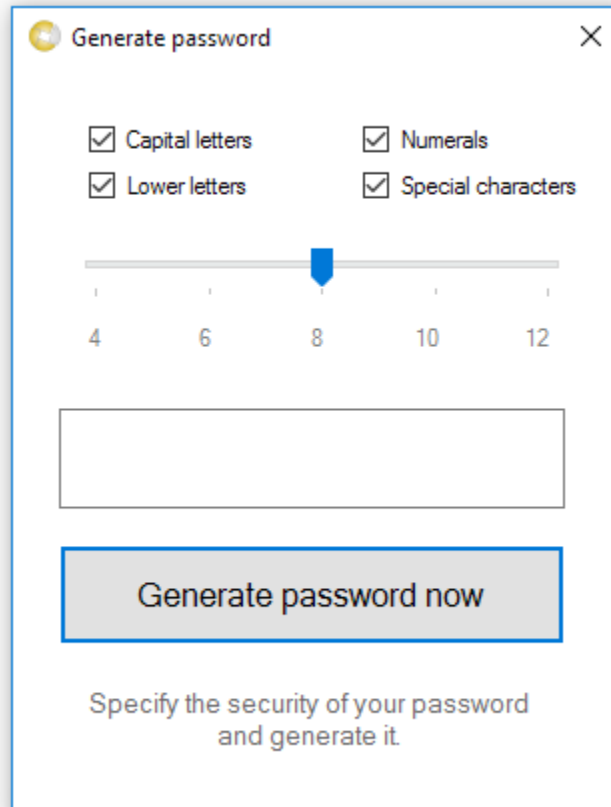
Changes just take effect if you close the dialogue by clicking "OK".

If you change the settings of other users it will take effect after the next log on.
 If a user is removed, but still logged on, he is logged on and has access to the data until he logs off.

Password generator

To make it easier to create safe passwords there is a password generator implemented and you can use it whenever you have to enter a password.

Settings



The screenshot shows a dialog box titled "Generate password" with a close button (X) in the top right corner. Inside the dialog, there are four checked checkboxes arranged in two columns: "Capital letters", "Lower letters", "Numerals", and "Special characters". Below these is a horizontal slider bar with tick marks at 4, 6, 8, 10, and 12. A blue arrow points to the value 8 on the slider. Under the slider is an empty rectangular text box. Below the text box is a button labeled "Generate password now". At the bottom of the dialog, there is a line of text: "Specify the security of your password and generate it."

Select the length of the generated password and specify how the password should be generated.

By clicking "Generate password now" the password will be generated instantly.

Password

Generate password

☒ Capital letters ☒ Numerals
☒ Lower letters ☒ Special characters

4 6 8 10 12

pb;4Vd-@

Generate password now

Transfer the password manually
in the appropriate input box.

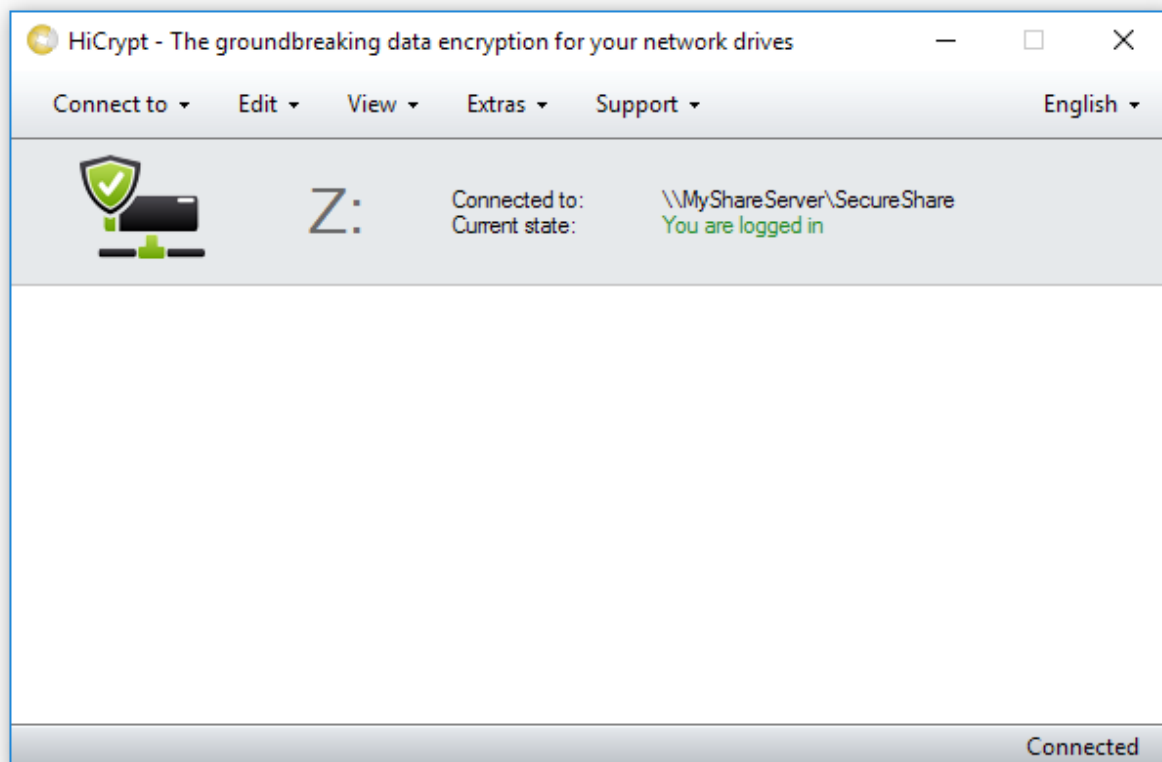
The generated password can not be copied so the user is prompted to write it into the dialogue and remembers that this password is very important.

5. Decryption

Please have in mind that the network drive you want to decrypt has to be empty and all users are disconnected.

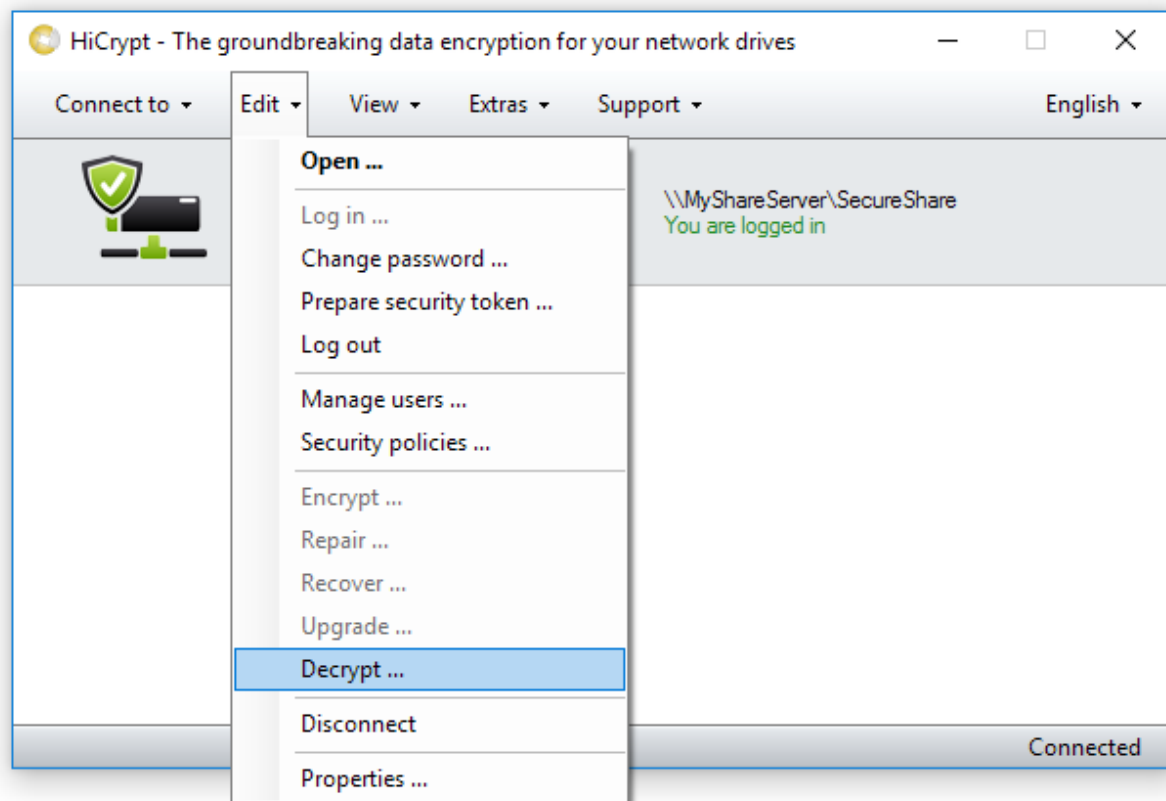
Just the manager who wants to decrypt has to be logged on.

Step 1



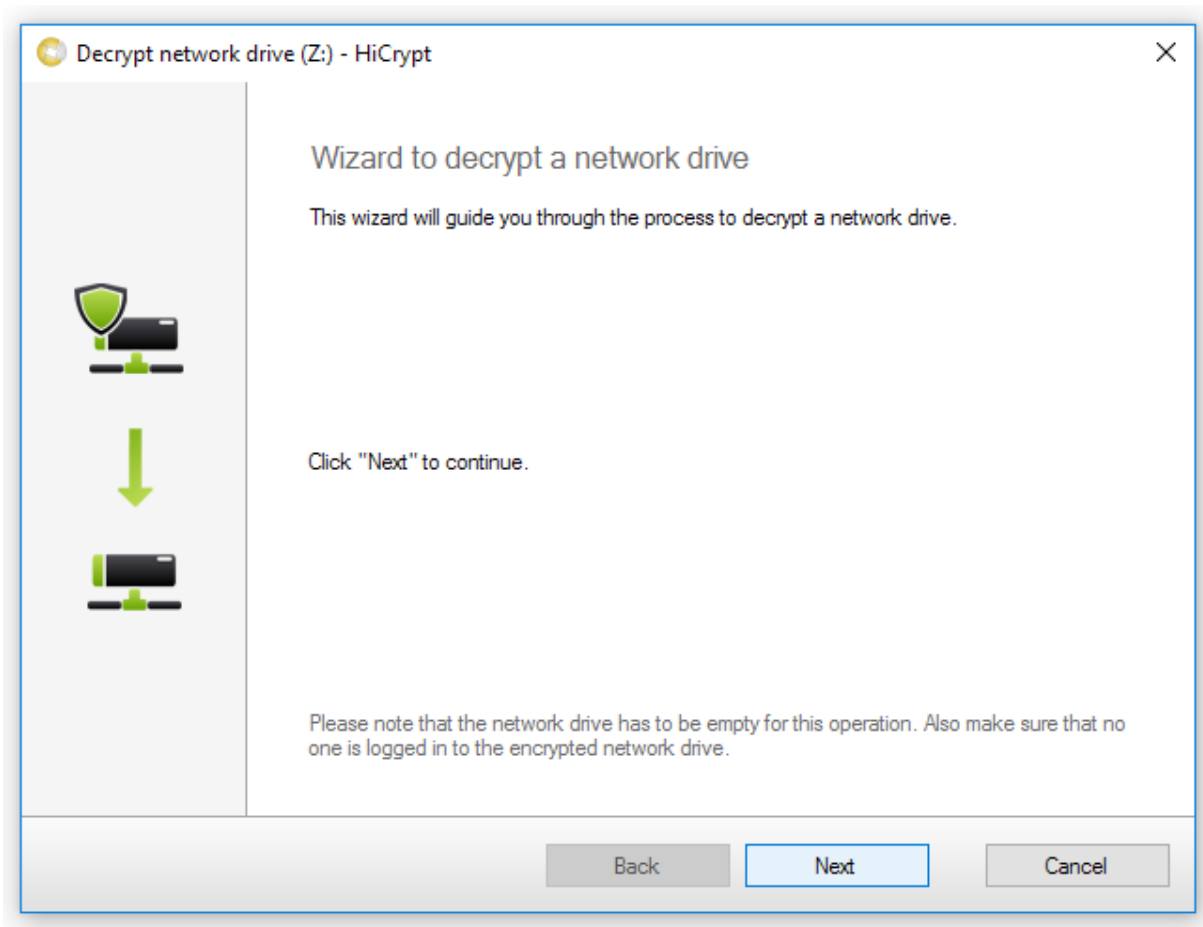
Mark the encrypted share.

Step 2



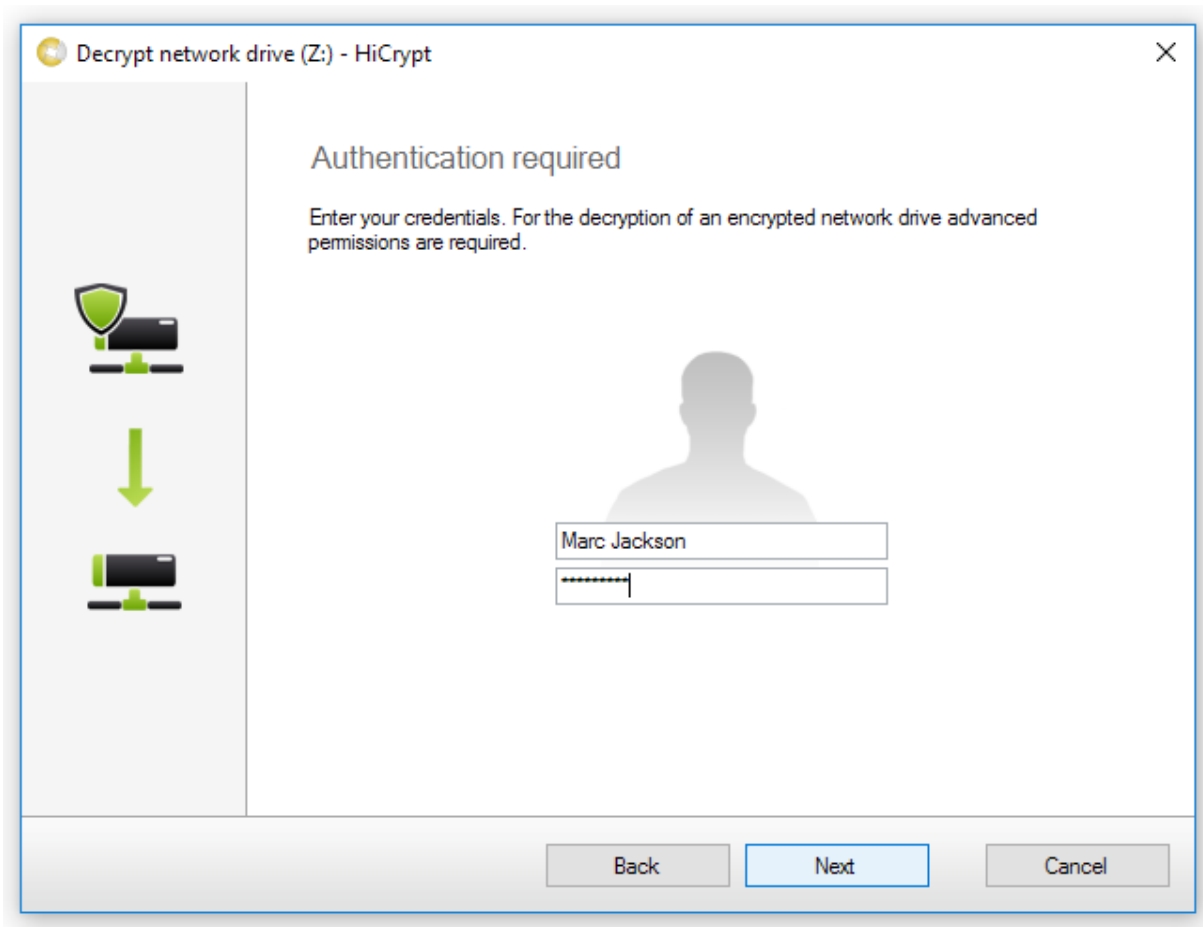
To decrypt the share open the "Edit" - menu and after that click on "Decrypt...".

Step 3



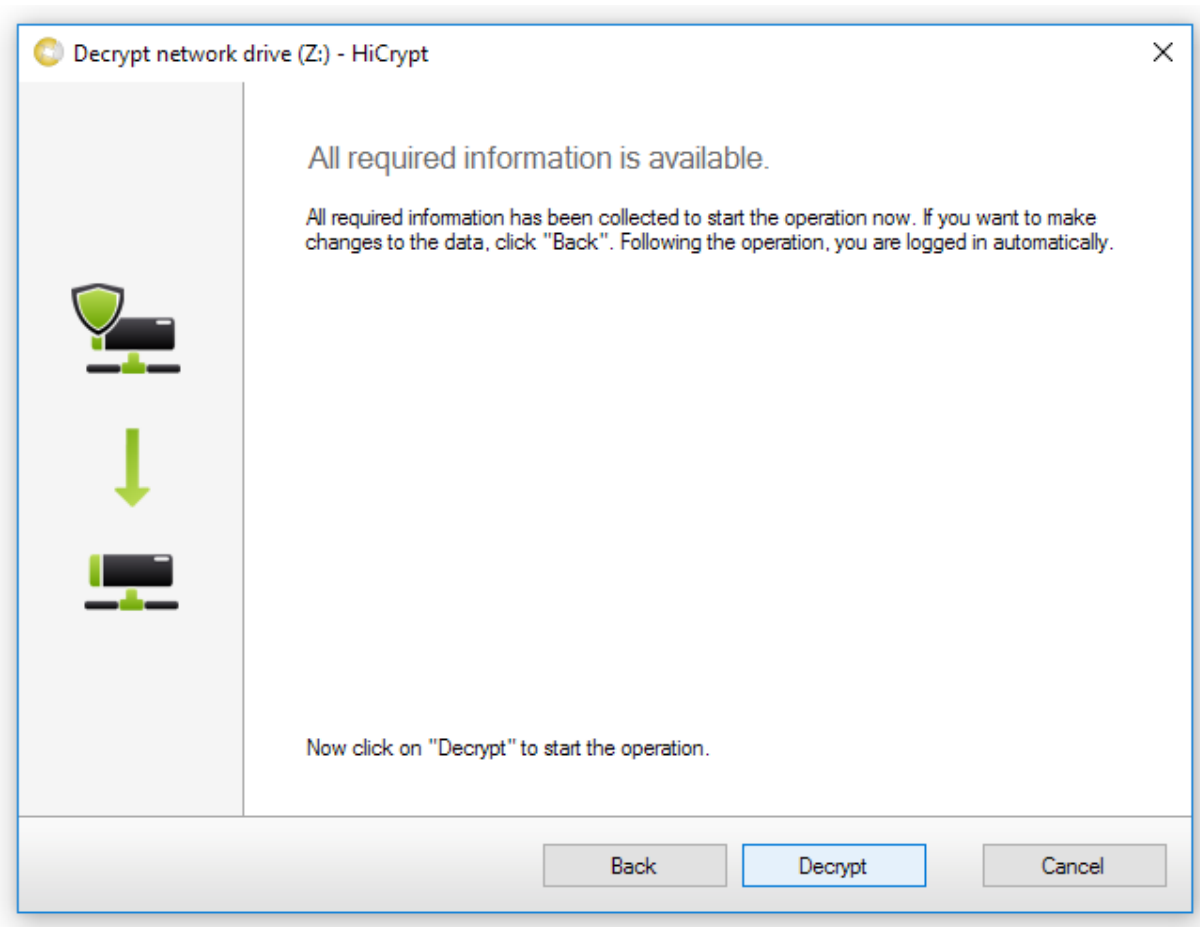
Click "Next" to continue.

Step 4



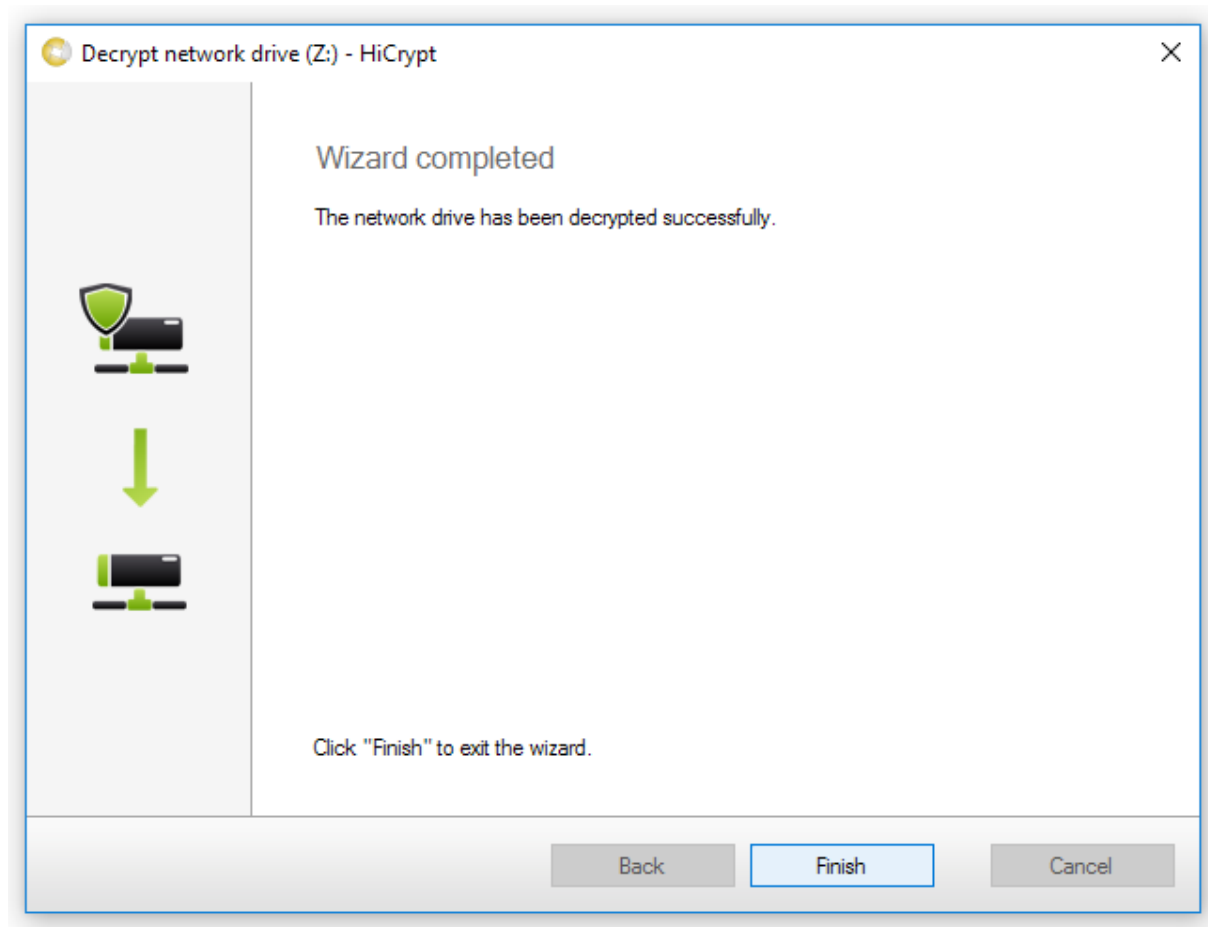
You need to enter a manager username and password to start the decryption. Confirm by clicking "Next".

Step 5



To start the decryption, click "Decrypt".

Step 6

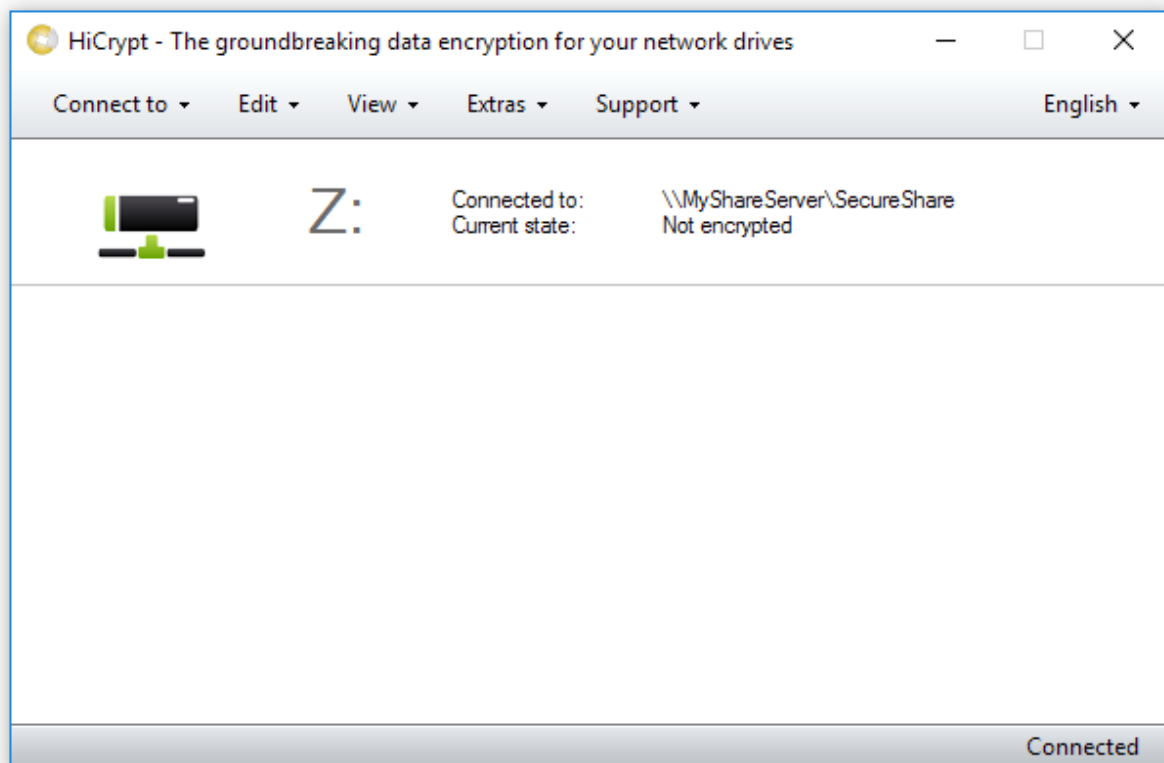


Exit the wizard by clicking "Finish".

6. Recovery

This chapter will lead you through the recovery process. First you need an empty network drive.

Step 1



First mark the share.

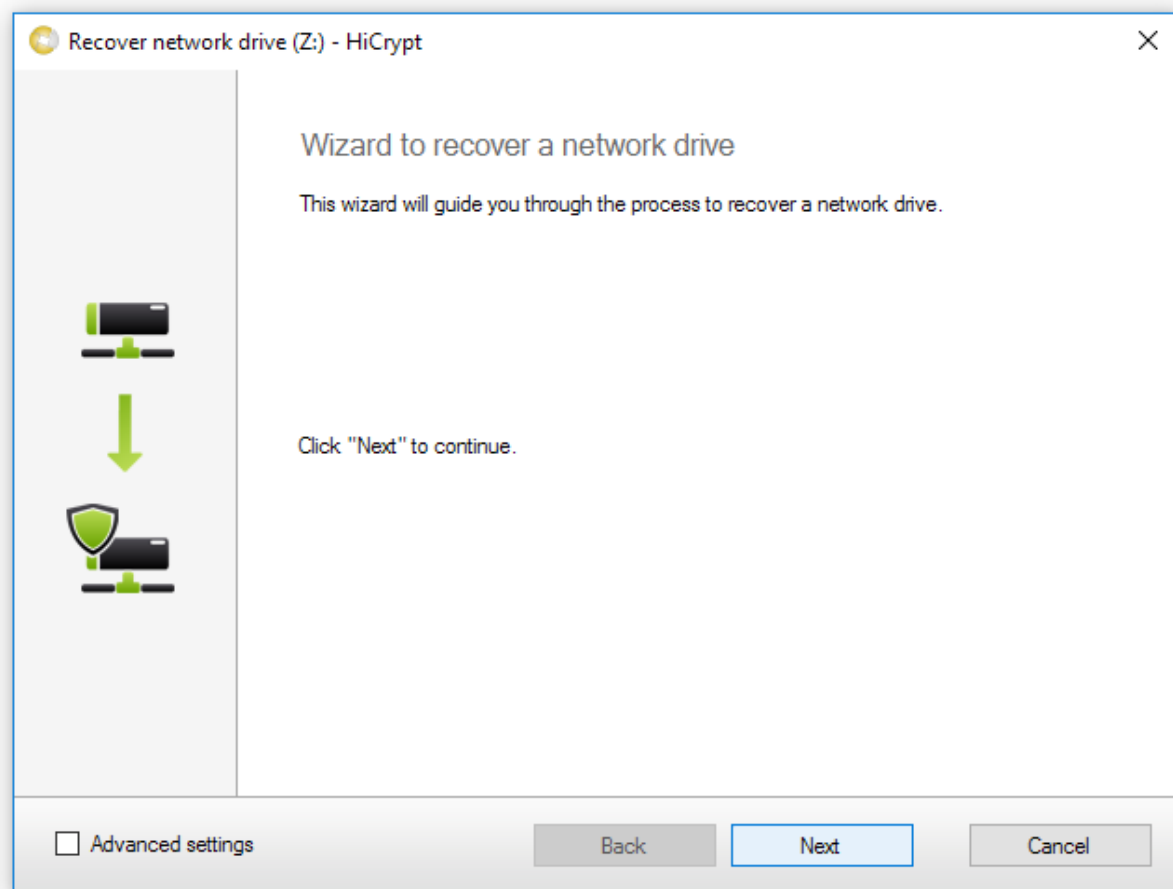
Step 2

<Hier wäre Platz für das richtige Bild>

Open the "Edit" - menu and select "Recover..."

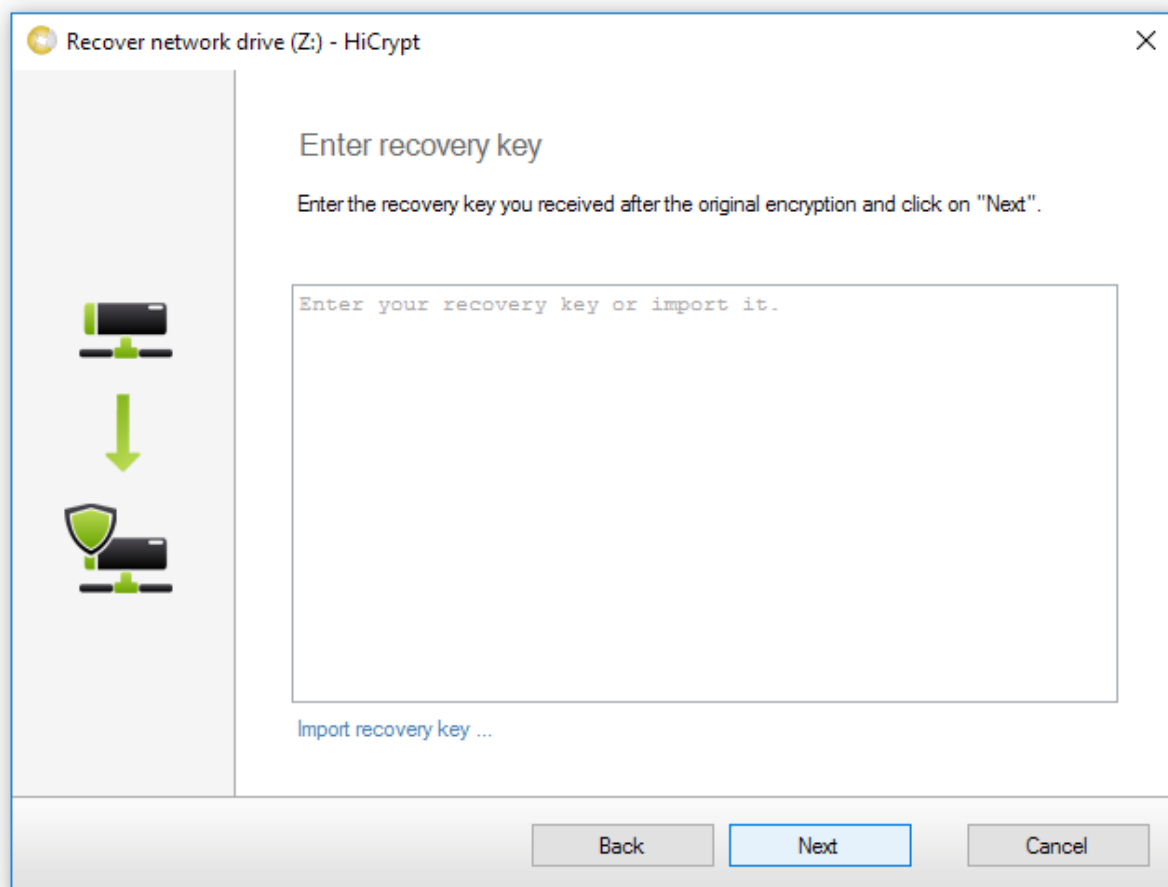


Step 3



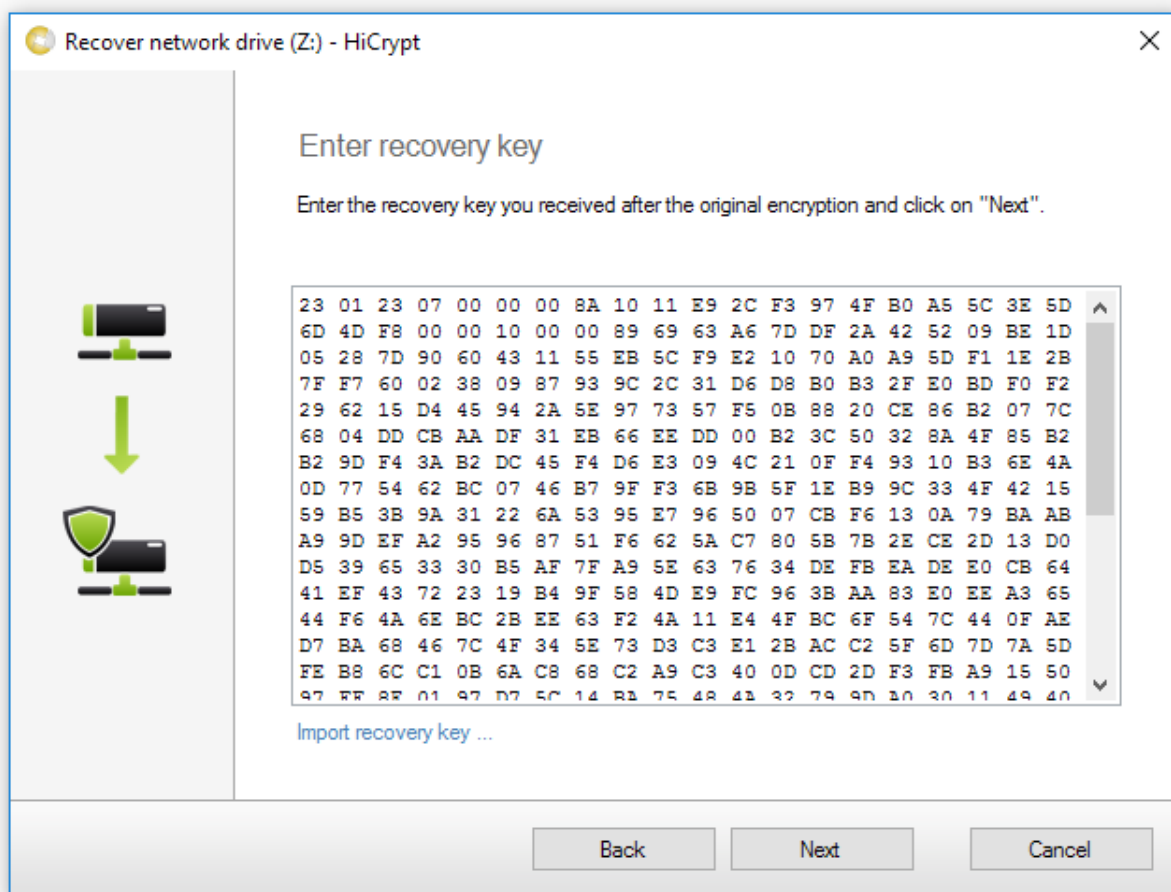
There is the option to define advanced settings or not.
You can just set password policies during a recovery process, because the algorithm which will be used is prompted by the recovery key.

Step 4



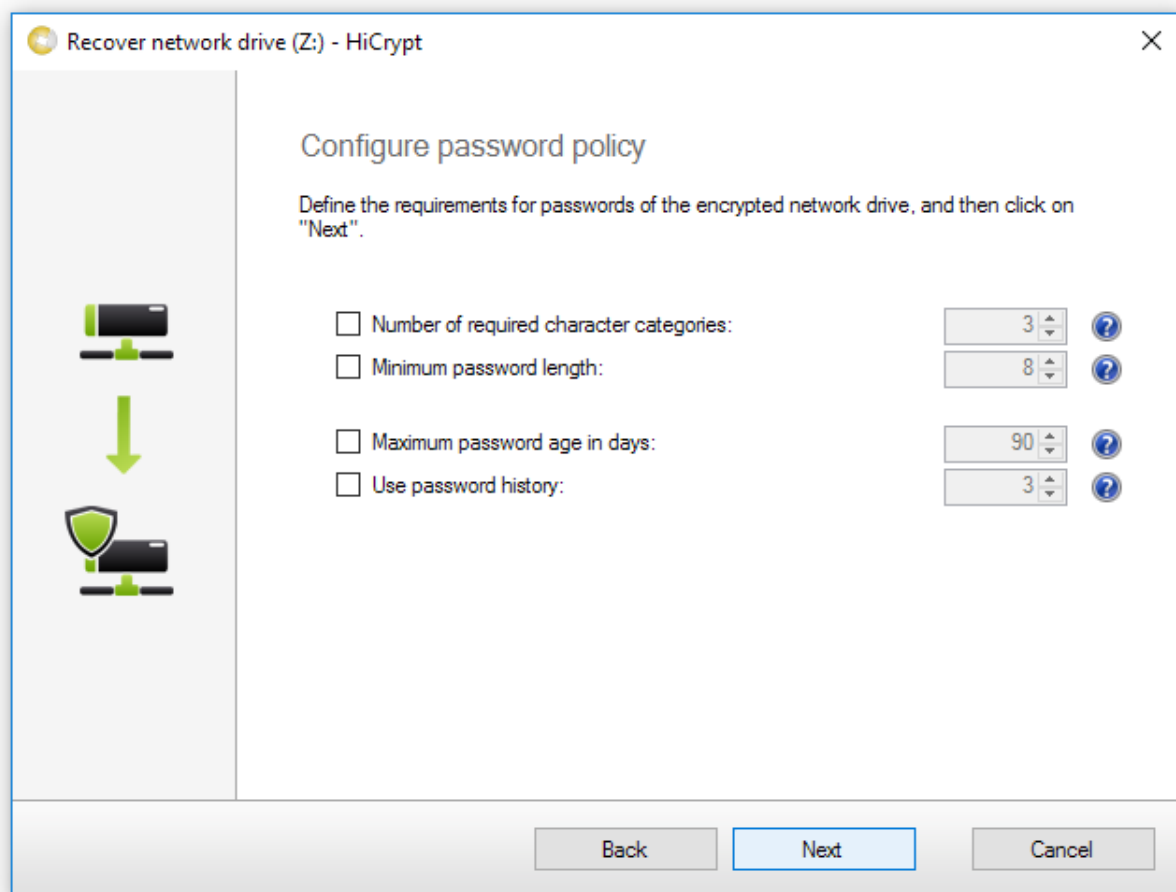
Please enter your recovery key. You can also import the saved *.hrk-file.

Step 5



Confirm the recovery key by clicking "Next".

Step 6



Recover network drive (Z:) - HiCrypt

Configure password policy

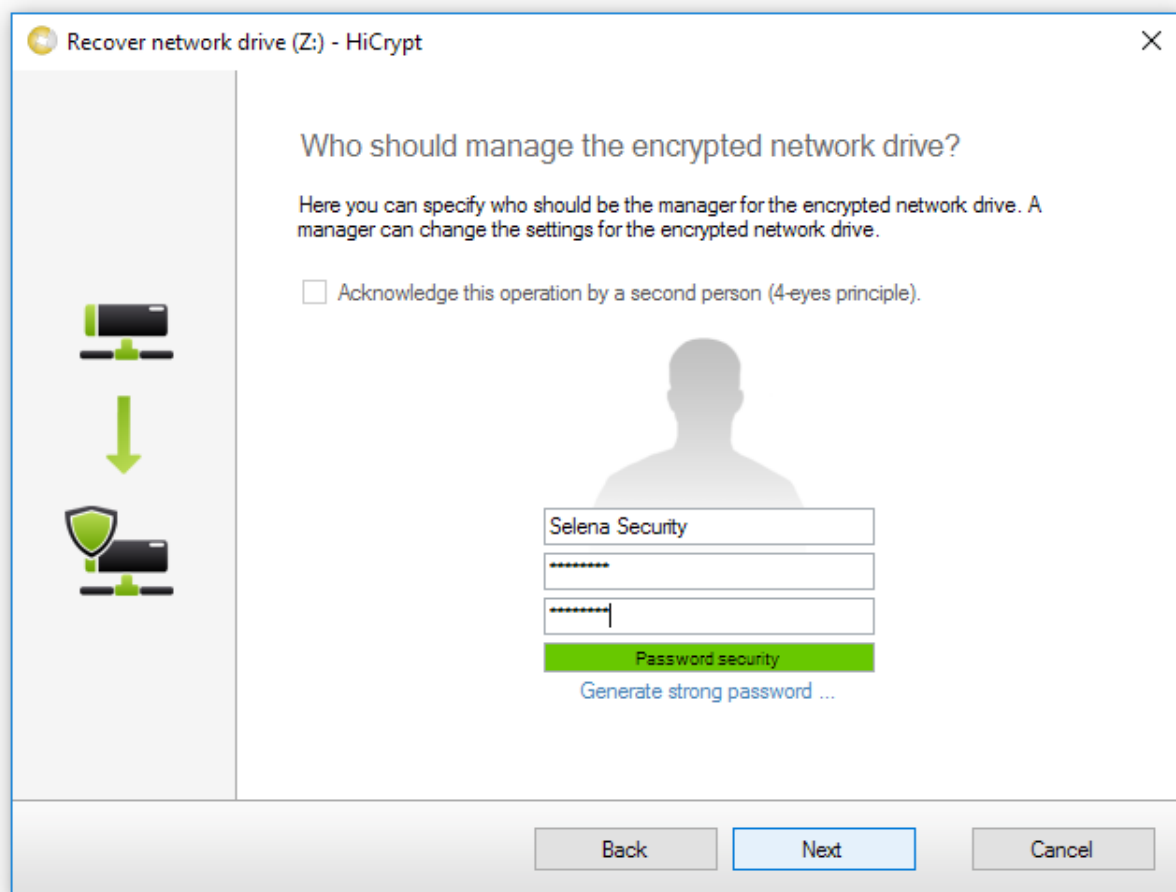
Define the requirements for passwords of the encrypted network drive, and then click on "Next".

- ☐ Number of required character categories: ?
- ☐ Minimum password length: ?
- ☐ Maximum password age in days: ?
- ☐ Use password history: ?

Back Next Cancel

If you selected "Advanced settings" you can now set the password policies.

Step 7



Recover network drive (Z:) - HiCrypt

Who should manage the encrypted network drive?

Here you can specify who should be the manager for the encrypted network drive. A manager can change the settings for the encrypted network drive.

☐ Acknowledge this operation by a second person (4-eyes principle).

Selena Security

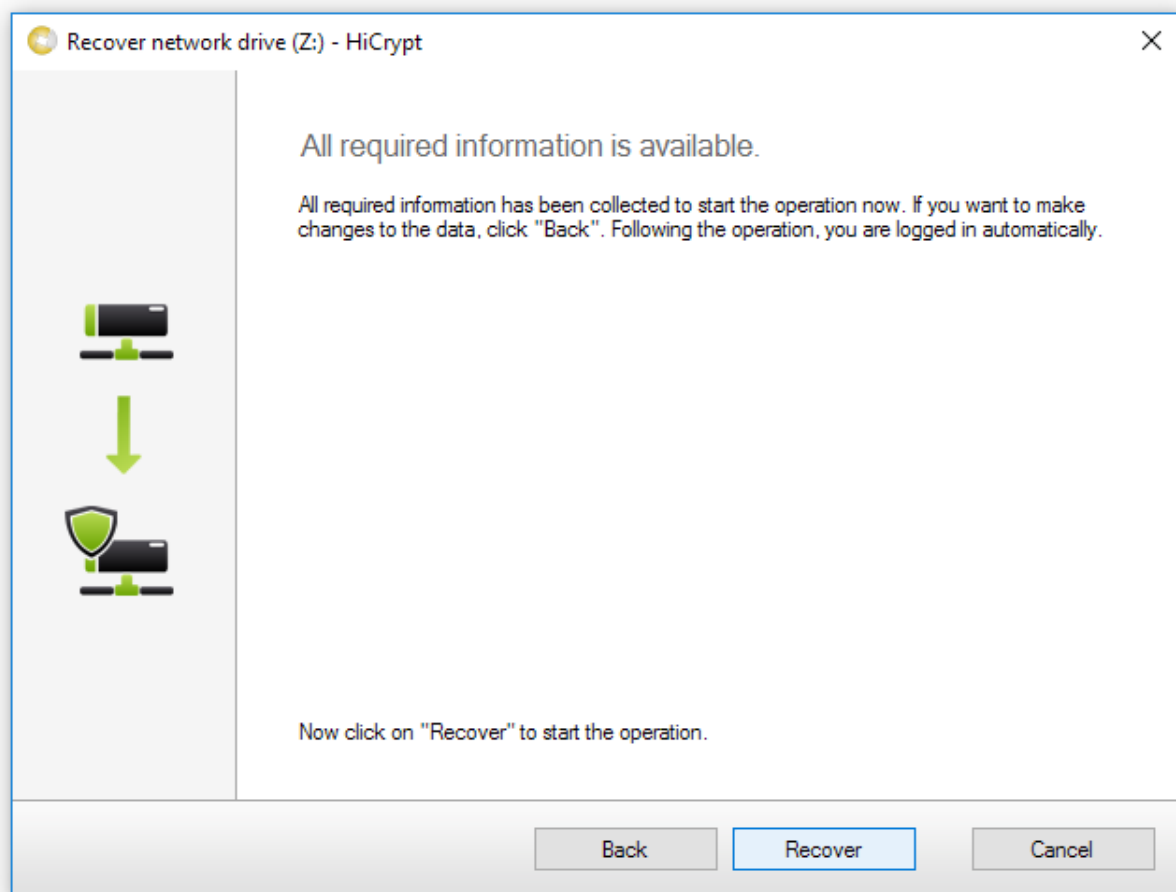
Password security

[Generate strong password ...](#)

Back Next Cancel

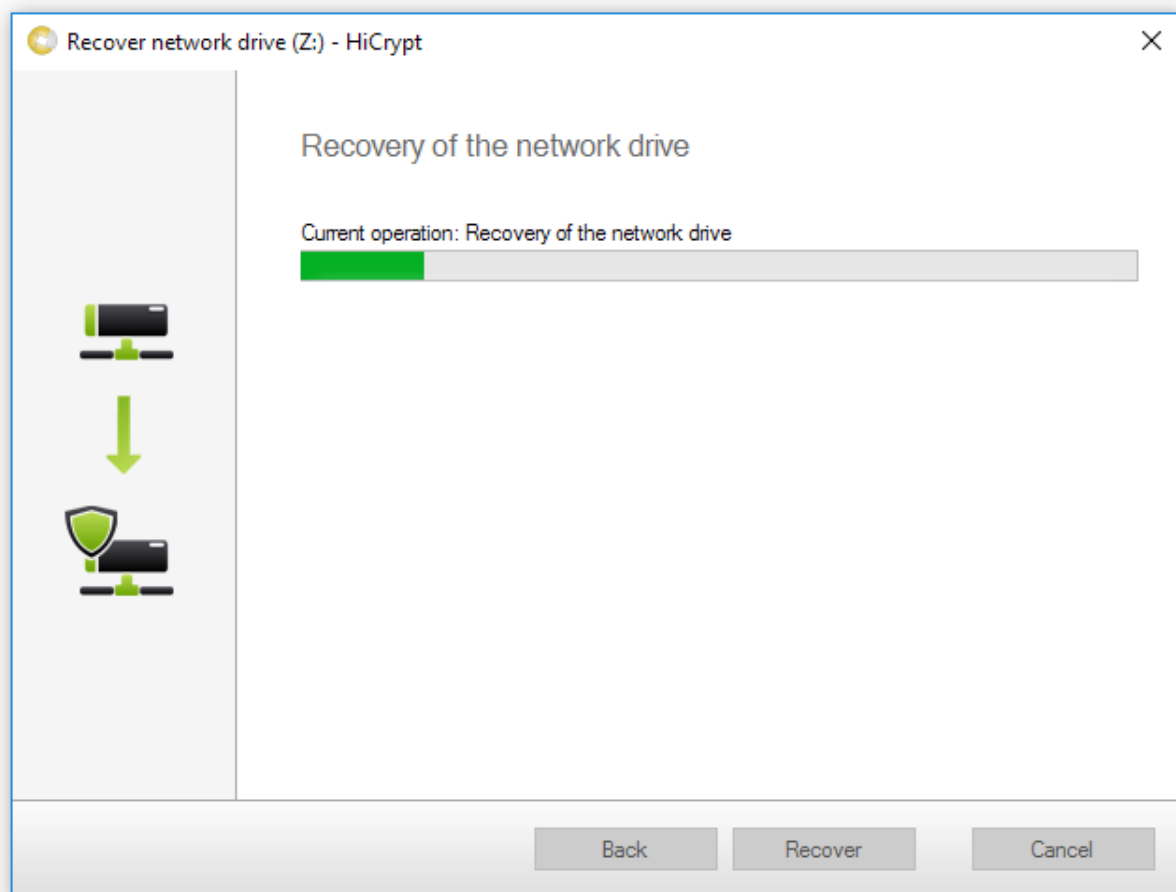
In this dialogue you have to enter the username and password of the new share manager. If the recovered share has been encrypted under usage of the four-eye-principle, you have to use this option here too. Confirm by clicking "Next".

Step 8



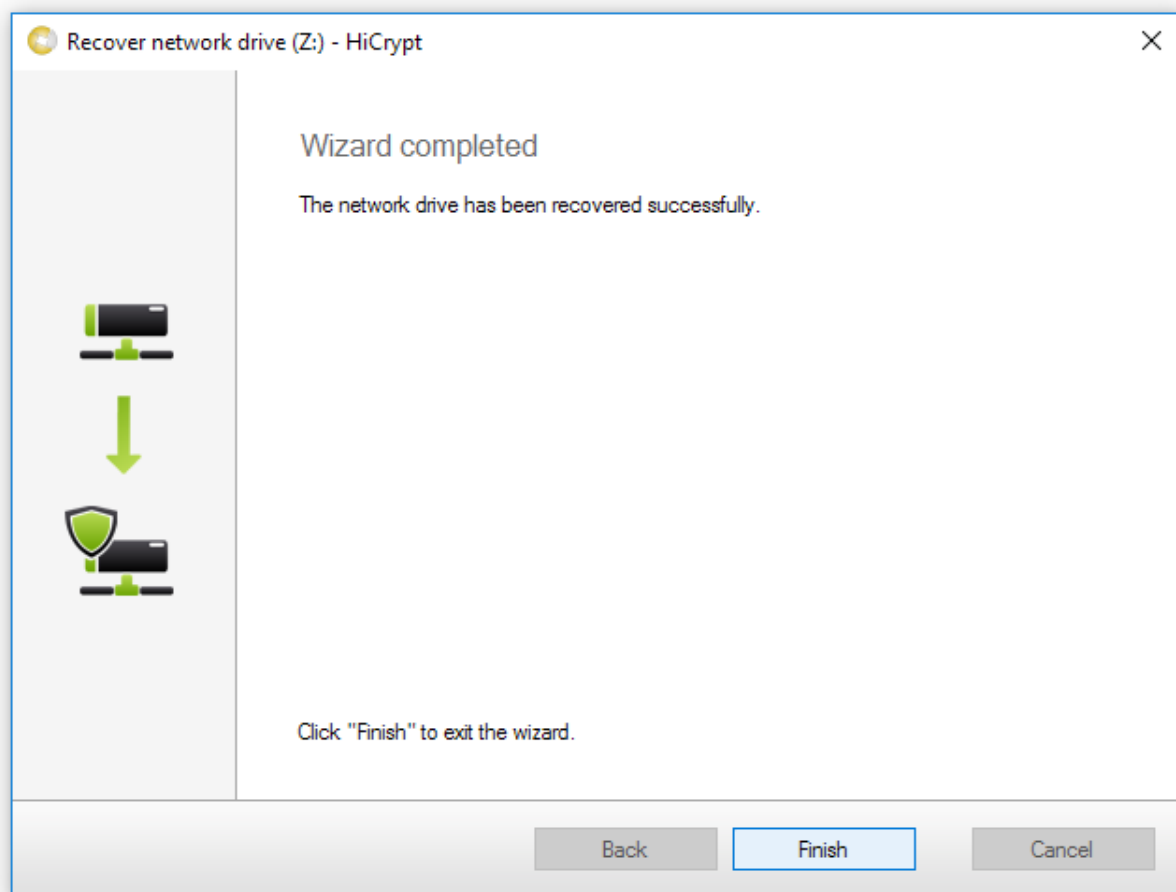
Click on "Recover" to start the operation.

Step 9



Please wait until the recovery was finished.

Step 10



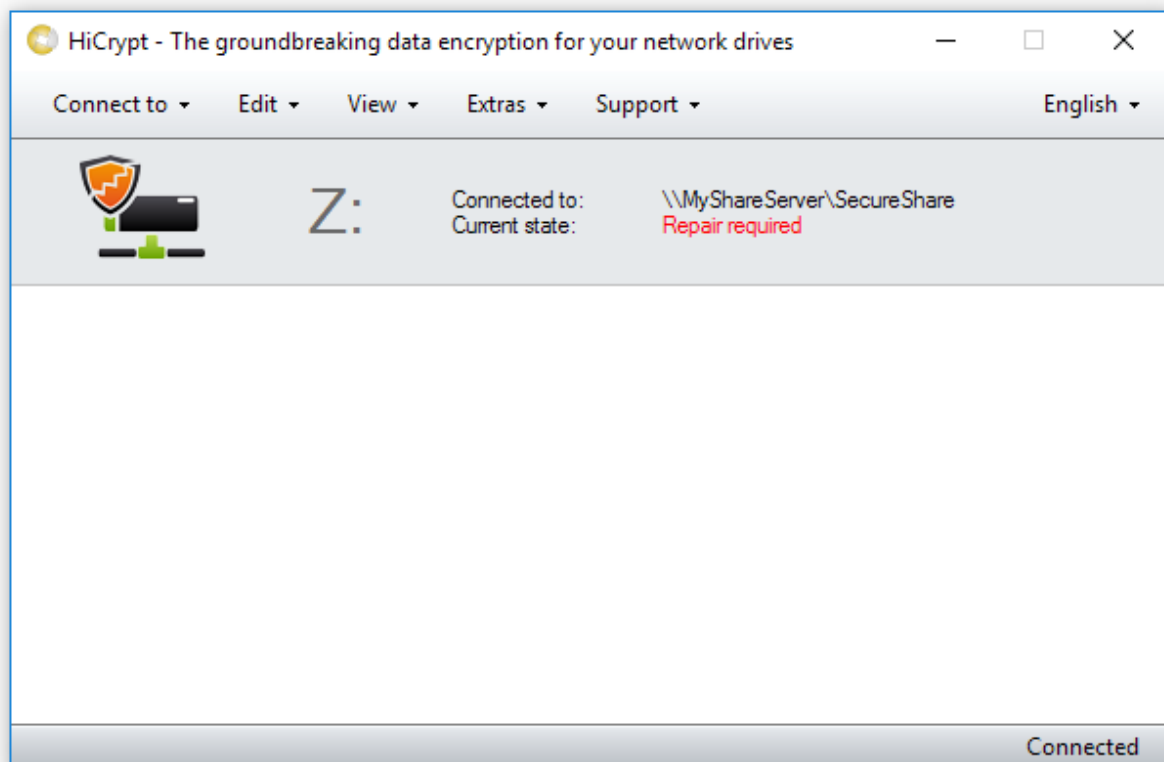
Exit the wizard by clicking "Finish".

Please copy the encrypted files directly on the server from the old directory to the new one.

7. Repair

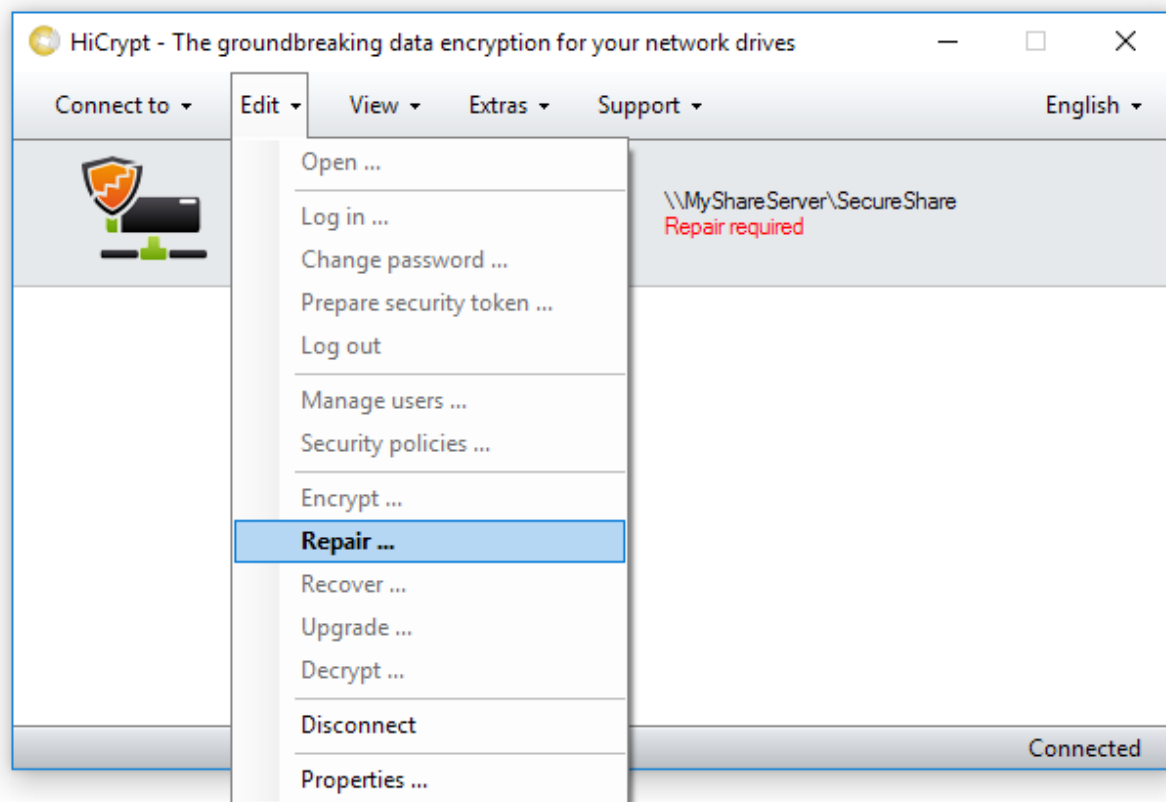
To repair a network drive is needed if the keyfile is damaged. For the repair it is necessary to use an undamaged backupfile.

Step 1



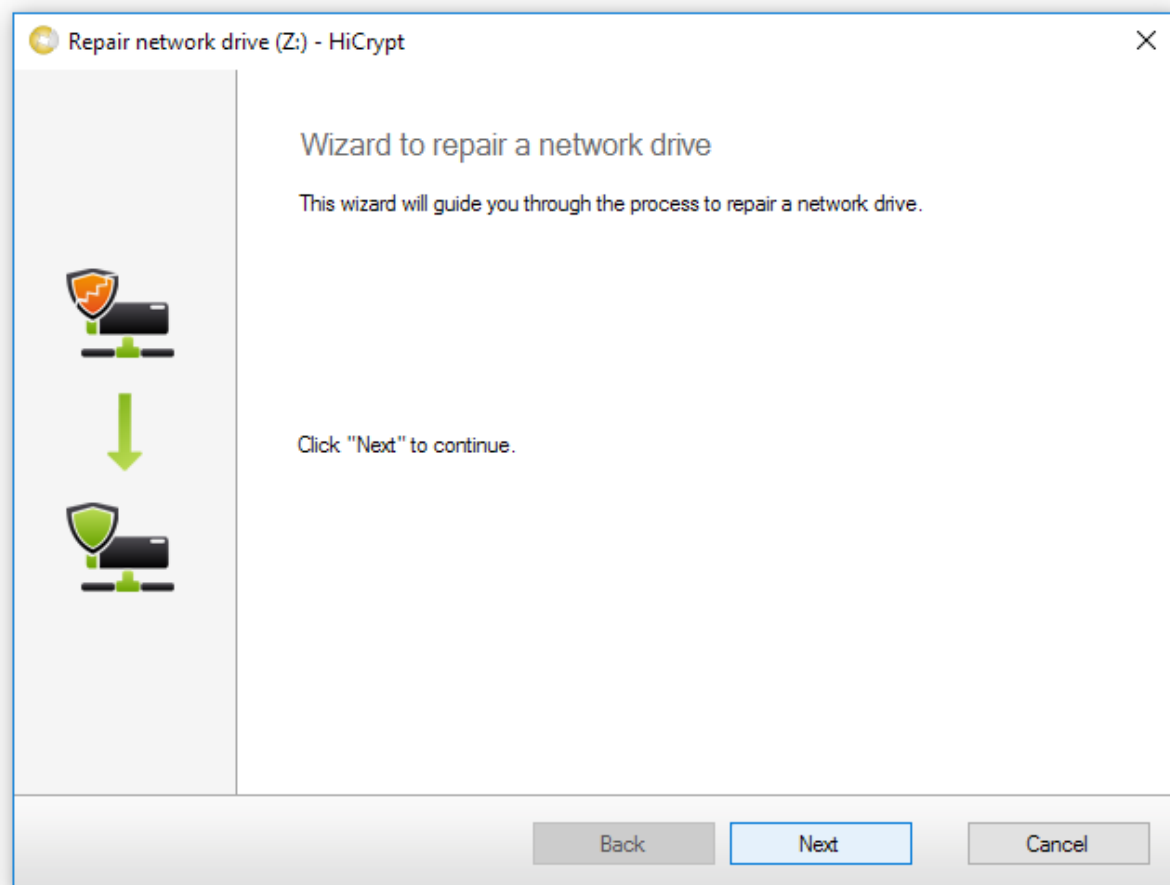
A broken shield in the front of the share means that the share requires a repair.

Step 2



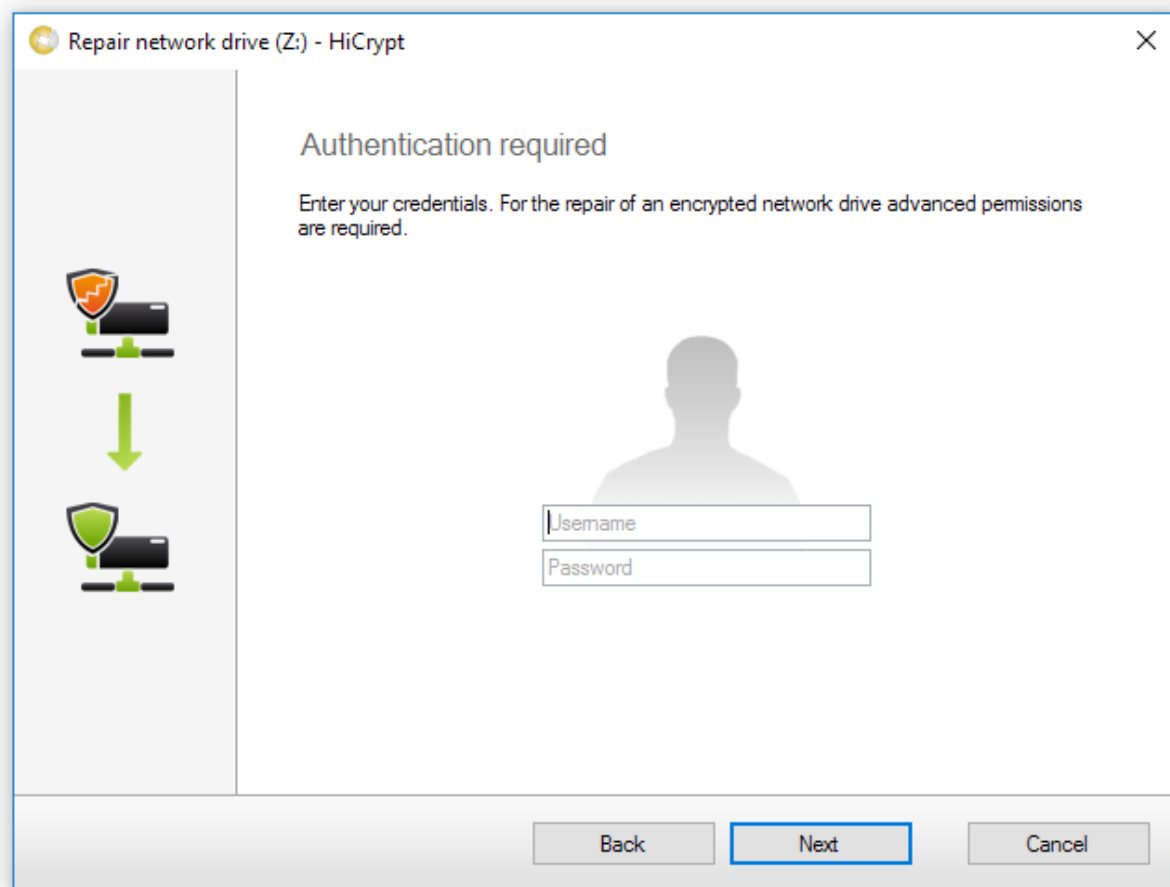
Open the "Edit" - menu and after that click on "Repair...".

Step 3



To start the wizard to repair a network drive click on "Next".

Step 4



Repair network drive (Z:) - HiCrypt

Authentication required

Enter your credentials. For the repair of an encrypted network drive advanced permissions are required.

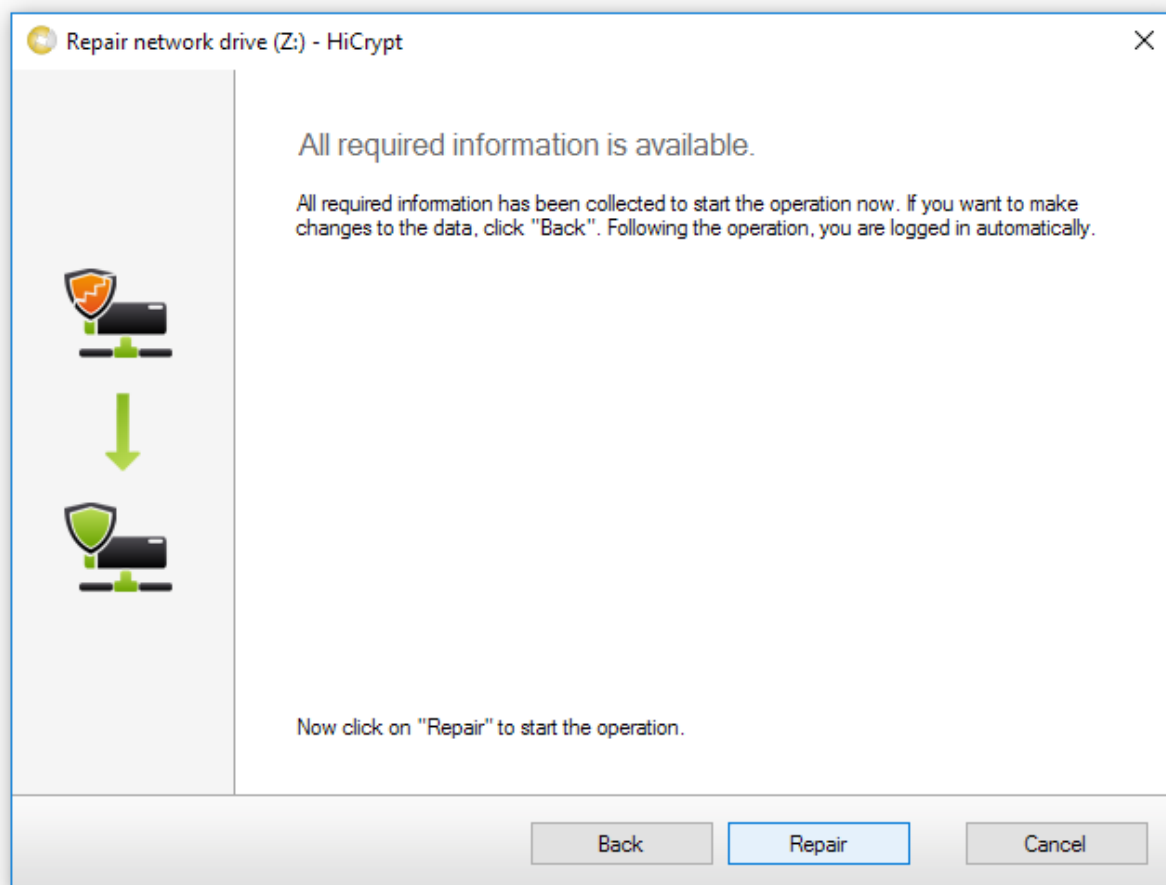
Username

Password

Back Next Cancel

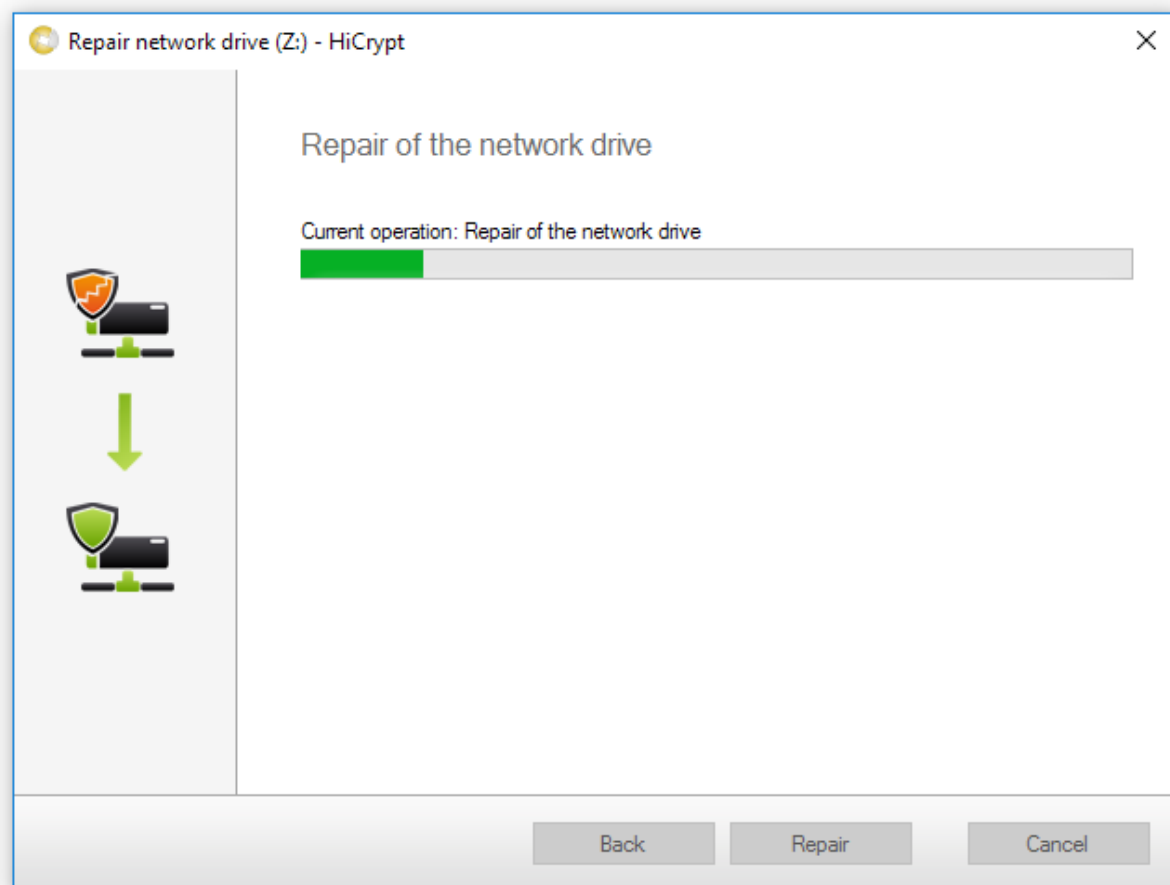
Enter the username and password of a manager here and confirm by clicking "Next".
If you have set the four-eye-principal, the operation has to be confirmed by both managers.

Step 5



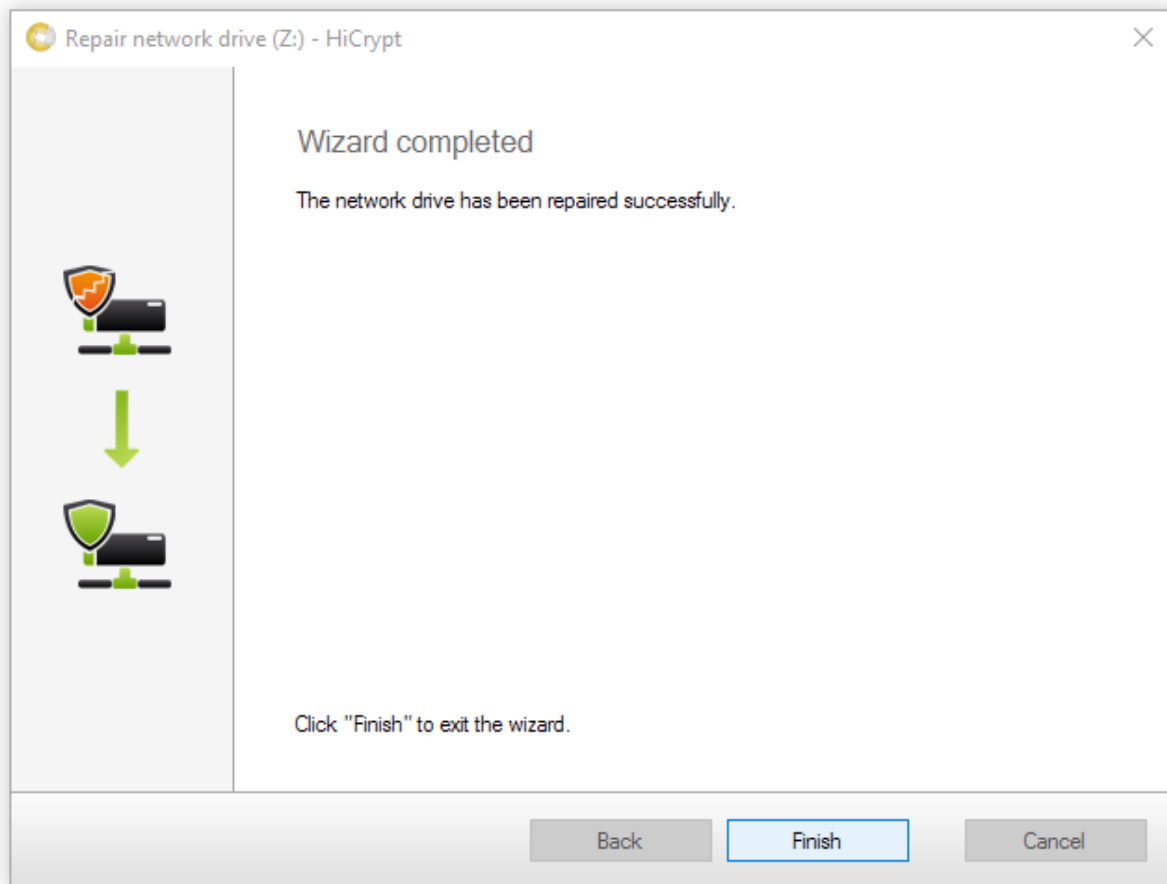
Start the operation by clicking "Repair".

Step 6



Please wait a moment while HiCrypt create a new keyfile under usage of the backupfile.

Step 7



Click "Finish" to exit the wizard.

8. Other settings

This chapter describes the menus which were not described yet.

Properties



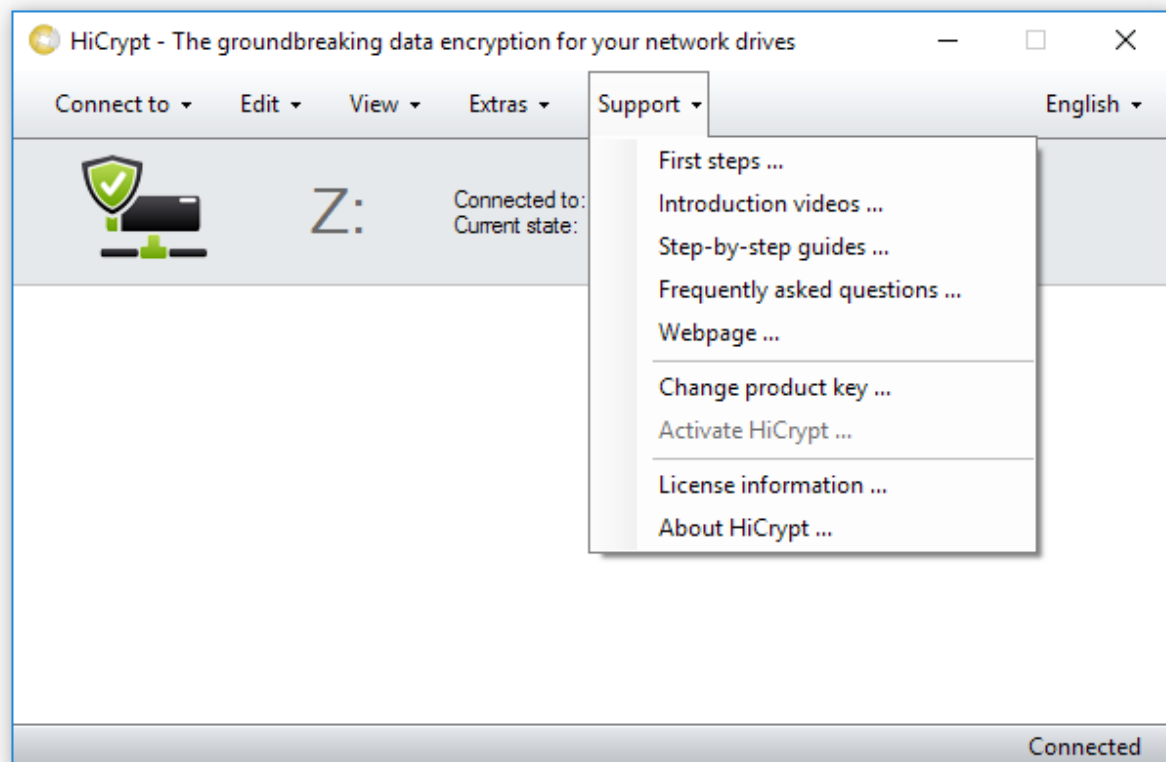
If you have marked a network drive, open the "Edit" - menu and after that click on "Properties".
You will get some informations about the share, like the status or the algorithm which was used for the encryption.

Licence information



This dialogue contains several informations about HiCrypt.
 You can check the state of your licence and feature key, and you are able to update the content of your feature key by clicking on the link.
 You can also enter a new feature key if there is no possibility for an online activation.

Support



The menu "Support" contains some informations about HiCrypt and its configuration.

All links but "First steps ..." refer to online content.

Following "Change product key ..." you can enter a new product key.

Click on "Activate HiCrypt" if you have not activate HiCrypt yet.

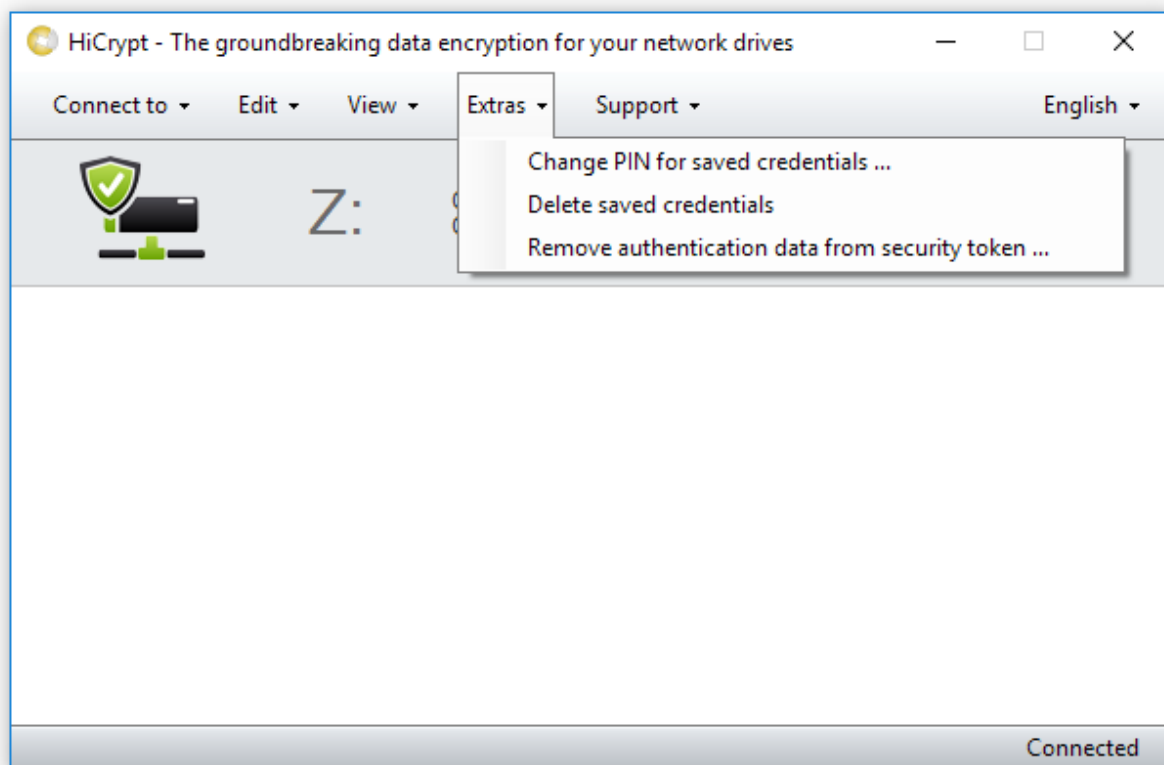
About HiCrypt



If you click on "About HiCrypt", you will get a short overview about the functions of HiCrypt 2.0.

You will find important informations about your version and the contact to the manufacturer.

Extras



If you select the "Extra" -menu, you will find there three points to select.
 "Change PIN for saved credentials ..." gives you the possibility to set a PIN for the saved log in, or change the deposited PIN.

"Delete saved credentials" will delete the saved login credentials.

"Remove authentication data from security token ..." cuts the created pair of keys from the security token.

Setting a PIN could be useful if the user has to log in to multiple network drives and no tokens are used.

9. Technical Data

Supported operating systems	Windows 7, 8, 8.1, 10
Implemented algorithms	AES 256, IDEA, Blowfish
Memory needed (Client)	4 MB
Memory needed (Fileserver)	20 KB HiCrypt 2.0 system files, 4 KB per saved file
Recommended software	Microsoft .net Framework 4.7
Supported token	MiFare DESFire EV1, MiFare DESFire EV2, Java Card OS 2.1.1, 2.2+, 3.0.1, 3.0.4, STARCOS, Multos, TCOS, CardOS, Yubikey, Legic Advant
Supported network protocols	SMB, CIFS, WebDAV