File Encryption migration steps

SafeGuard Enterprise

SafeGuard Enterprise ("SGN") is a security suite from Sophos. It consists of several modules, with Data Exchange (DX), Cloud Storage (CS) and File Encryption (FE) all providing file-level encryption. The entire software suite is being discontinued. Users run the risk of losing access to their encrypted documents. Migrating from one security product to another can be a hassle and an added risk, especially if the process involves the decryption of data. This is not the case when migrating to conpal LAN Crypt.

conpal LAN Crypt and Sophos SafeGuard Enterprise are fully compatible

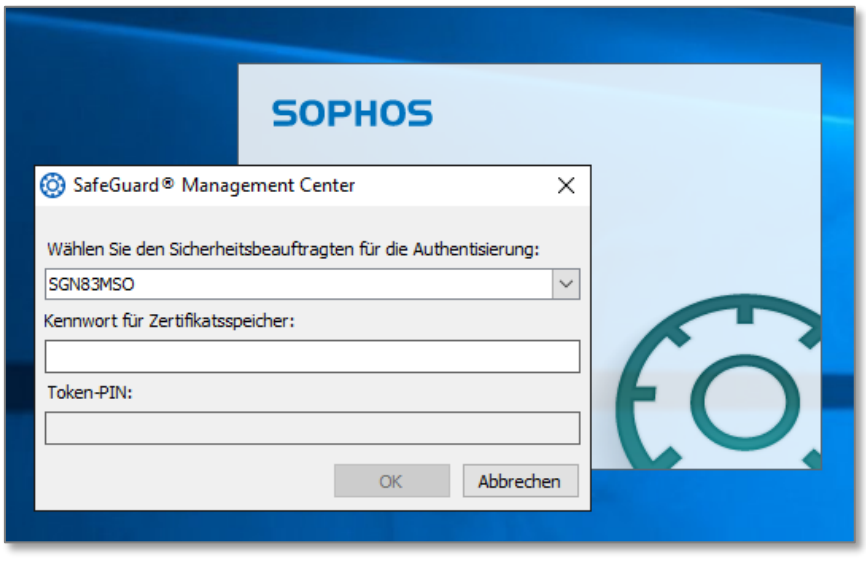
Sophos SafeGuard Enterprise and conpal LAN Crypt share the same technical foundation and file-encryption subsystem. As a consequence, files encrypted in SafeGuard Enterprise are fully compatible with and can be read natively by conpal LAN Crypt. The encryption keys are specific for each installation, and only those need to be migrated.

Export Keys from SafeGuard Enterprise

The export of the encryption keys can be done on any machine capable of logging in to the Sophos SafeGuard Enterprise console. You'll need an account with security officer privileges to be able to manage the keys you want to export. Depending on your security officer configuration, not all security officer accounts might be able to manage all available keys of your environment.

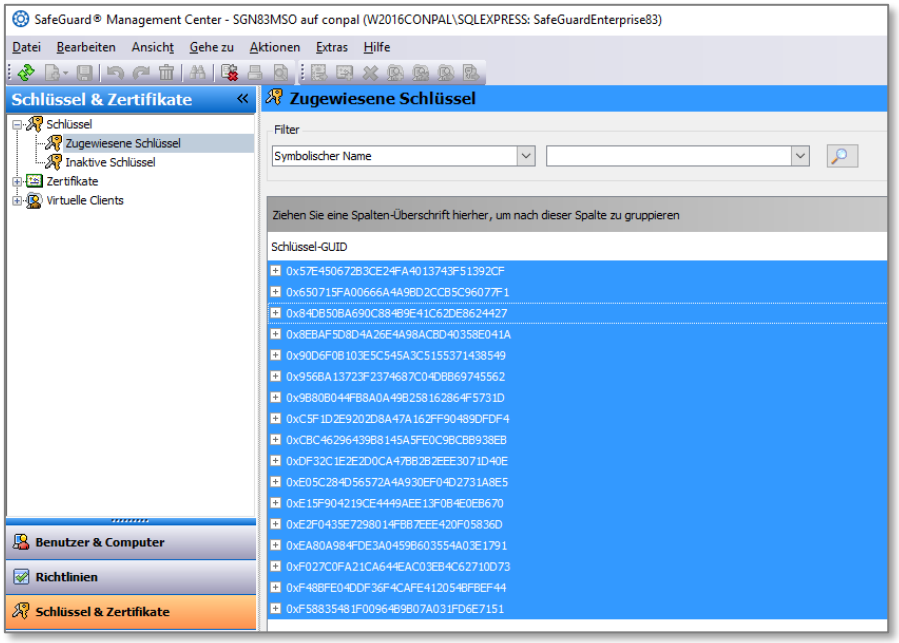
Login with your Security Officer account

Typically, there's a so-called master security officer with global rights. If you want to export every available key, that account would be the right one.



Identify keys you want to export / migrate to conpal LAN Crypt

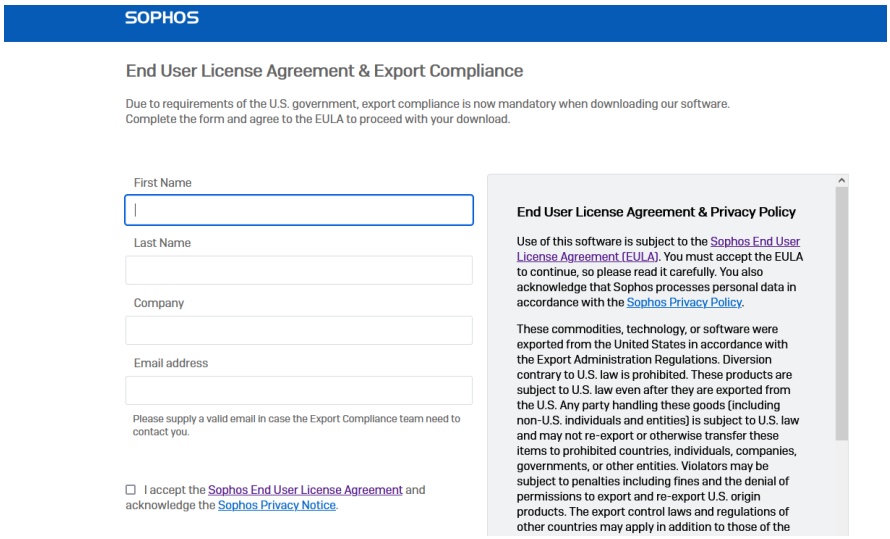
If you are unsure which keys to export it would be best to export all of them, but this also depends on how key generation has been configured in SafeGuard Enterprise. There might be a number of available keys that have not been used for file encryption but rather for other purposes.
You will only need the keys used for file encryption

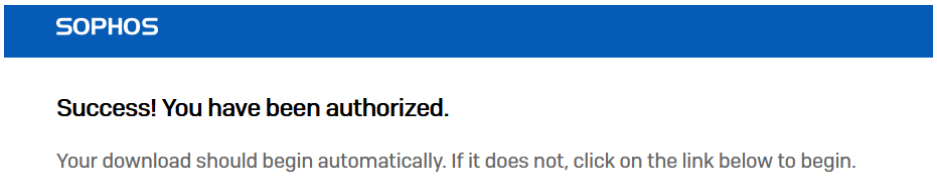


If you require assistance on this, please contact conpal support at support@conpal.de.

Get the ‘KeyExporter’ tool

Sophos provides a key exporter tool to customers that are (planning) to migrate.
The release is part of the SafeGuard Decryption Tools and now available for Download.
The Link will be provided by conpal, your partner, or Sophos.
Please don’t forward or publish this link.
In order to use the tool, Sophos requires the EULA and export policy to be agreed to.





Extract the keyexporter.exe and the runtime environment from that package.

Run the ‘KeyExporter’ tool

In this example, we will export all keys from the SafeGuard environment.

Open a Windows Terminal/command line and run `keyexporter.exe`, no admin elevation needed:

```
C:\tmp\Keyexporter>KeyExporter.exe SGN83MSO -o c:\tmp\keyexport.json -a -e
Enter certificate store password: *********
Performing export of SGN keys:
  Officer:     SGN83MSO
  Input path:
  Output path: c:\tmp\keyexport.json

Exporting all keys...

17 keys found in the SGN database...

Keyfile created, password is:
152904-560876-245403-559805-273930-347985-880268-409332

C:\tmp\Keyexporter>
```

You need to provide your SafeGuard Enterprise Account name and a path to the keyexport.json file. There’s a parameter to export all:

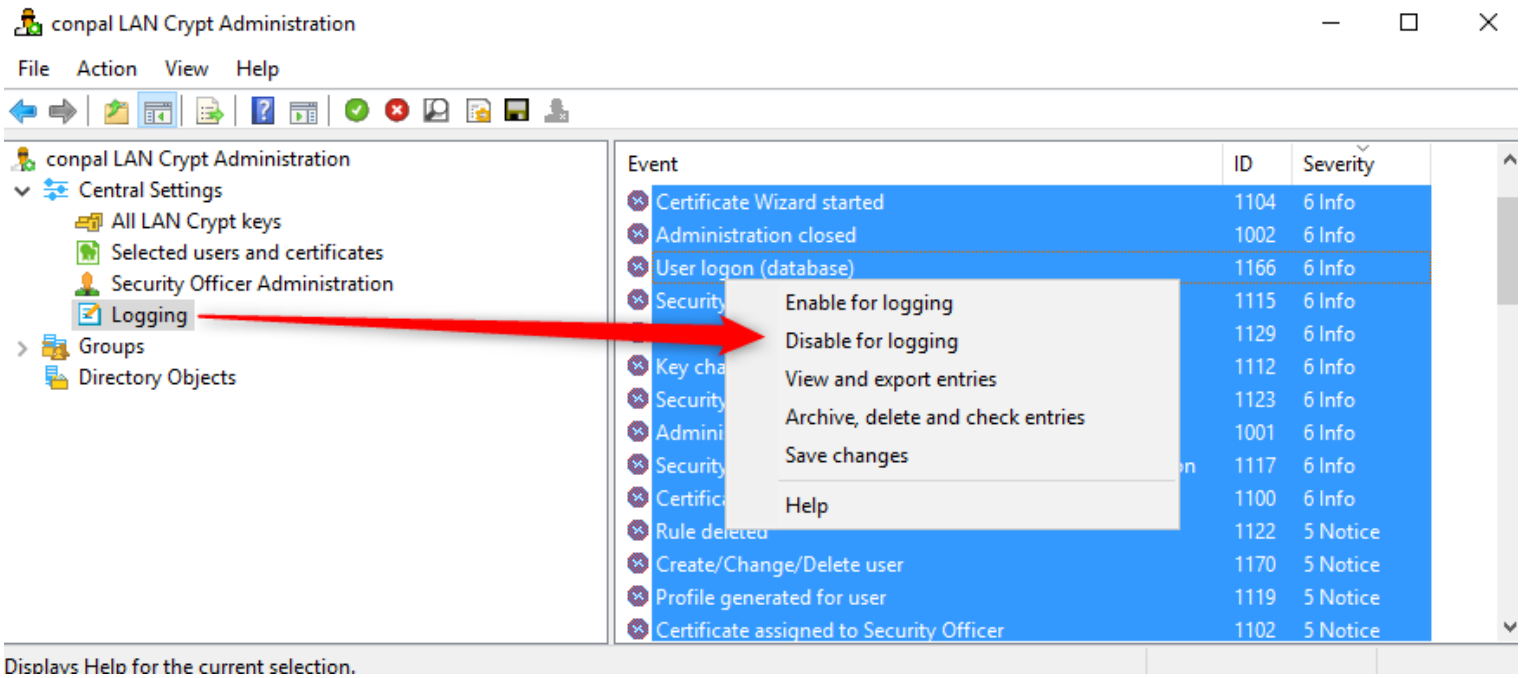
```
c:\tmp\SGN\KeyExporter.exe SGN83MSO -o c:\temp\keyexport.json -a
```

You will then be asked for the security officer's certificate store password (the login password to the SafeGuard console). Next, the export will start.
The export file itself will be encrypted, so no plaintext encryption values will be exposed at any point. This is the reason it will take a while to export if there are a lot of keys, so please be patient.
Towards the end, you will be given a password you need to pin down / copy. This password is needed to import the encryption keys to conpal LAN Crypt in the next step.

Import Keys to conpal LAN Crypt

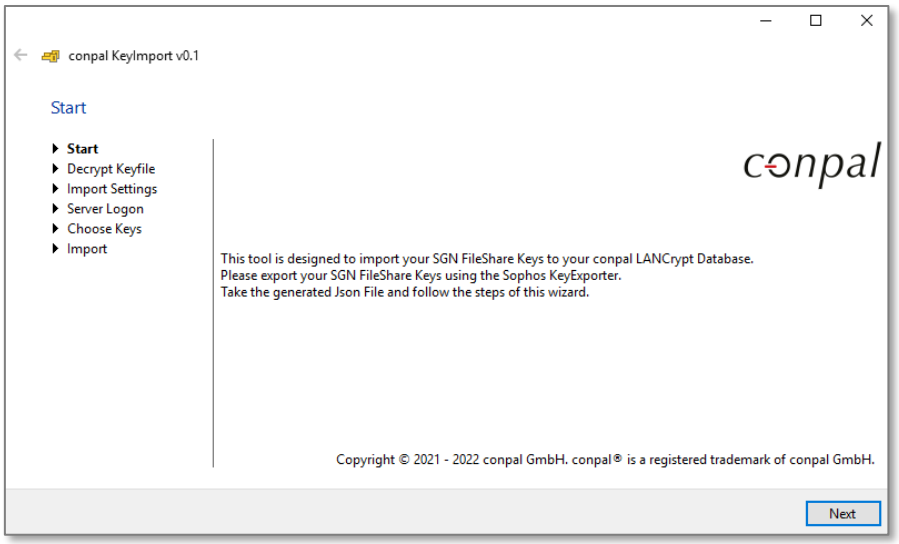
Once the keys have been exported successfully from SafeGuard Enterprise, you can migrate them to conpal LAN Crypt by importing them into the conpal LAN Crypt Administration.

Attention:
For the import process, logging in the admin console has to be deactivated, you can reactivate it right after the import process:



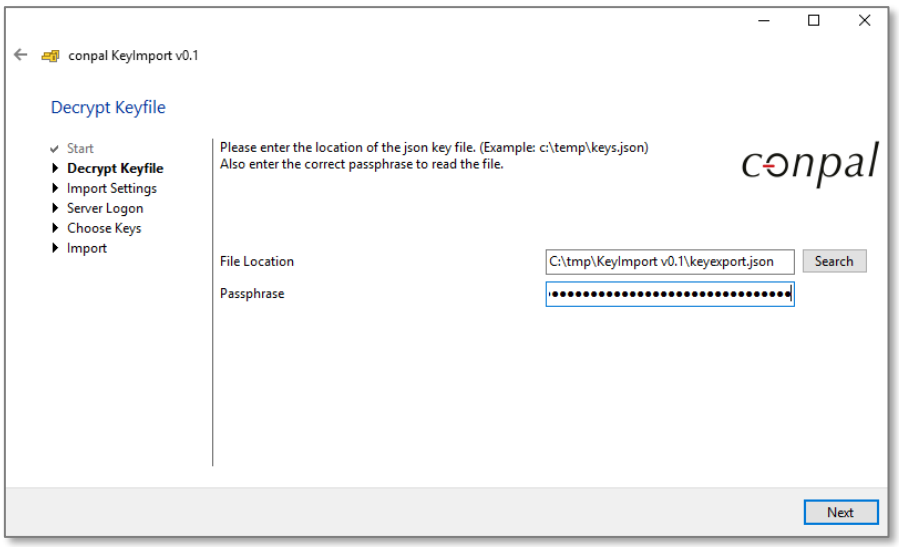
Run the ‘KeyImporter’ tool

On a machine capable of logging in to the conpal LAN Crypt administration console, run `KeyImporter.exe`. A wizard will guide you through the import process.



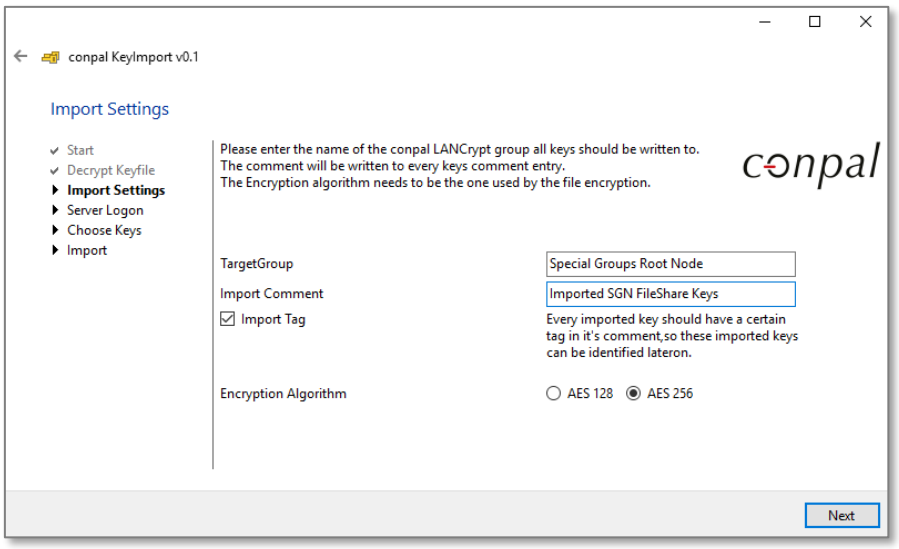
Select import-file

Choose your previously exported `keyexport.json` file and enter the password:



Adjust import options

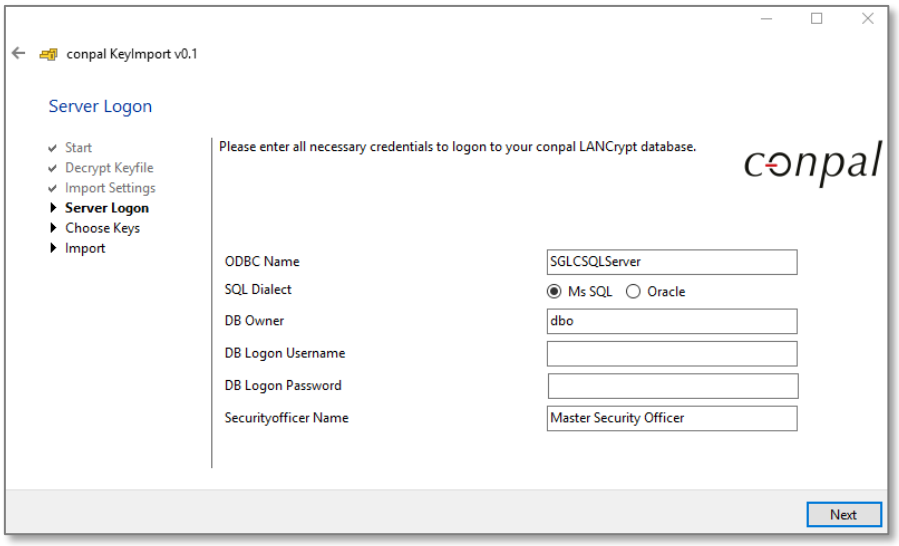
In conpal LAN Crypt, encryption keys are linked to a group, but you can link them to any group you like later on. In this step you should choose a group to which all the imported keys will be saved.
The “Special Groups Root Node” is the root group of conpal LAN Crypt. At your discretion, create a “SGN-Import” group in the conpal LAN Crypt administration and choose that group as target.
It makes sense to use the comment field of the key to document which keys were imported, regardless of which group they will be in.



Provide conpal LAN Crypt authorization information

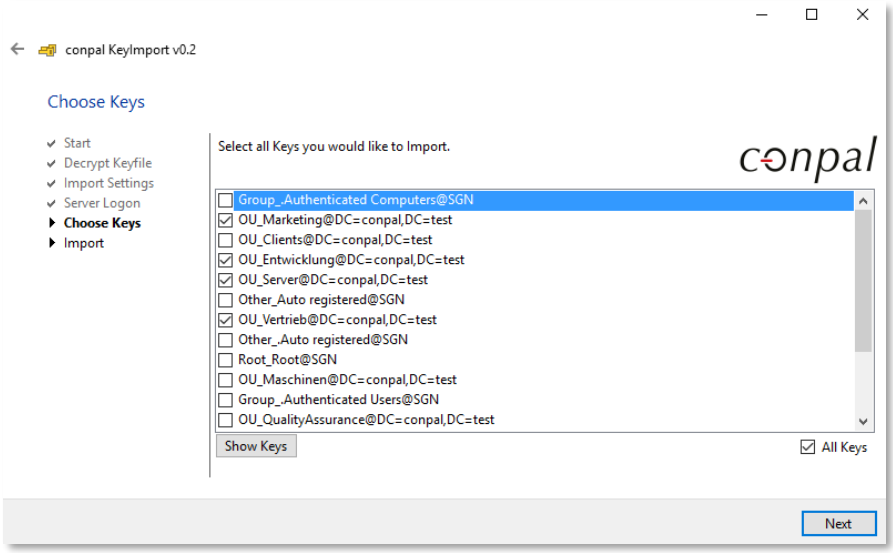
The next UI asks for your login credentials. When importing the keys, the importer will log in to the conpal LAN Crypt database just as you would log in to the admin console, so please enter the name of a master security officer. You need to have access to this officer's certificate and private key to be able to import the keys. If you are able to log on to the admin console on this machine, it will also work with the key importer.

Once you've logged in to the SQL database with a local SQL Account, please enter the SQL credentials: If you're authorized with your Windows credentials, just leave it blank.

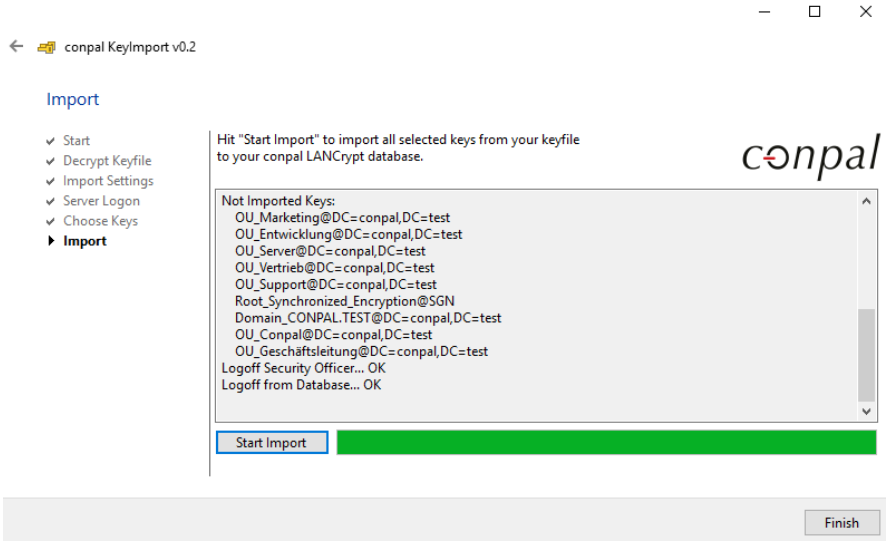


Select keys to be imported

In the final step before the actual import operation, you can select the keys you want to import, or alternatively just import all (this makes sense in cases where you've already picked specific keys in SGN):

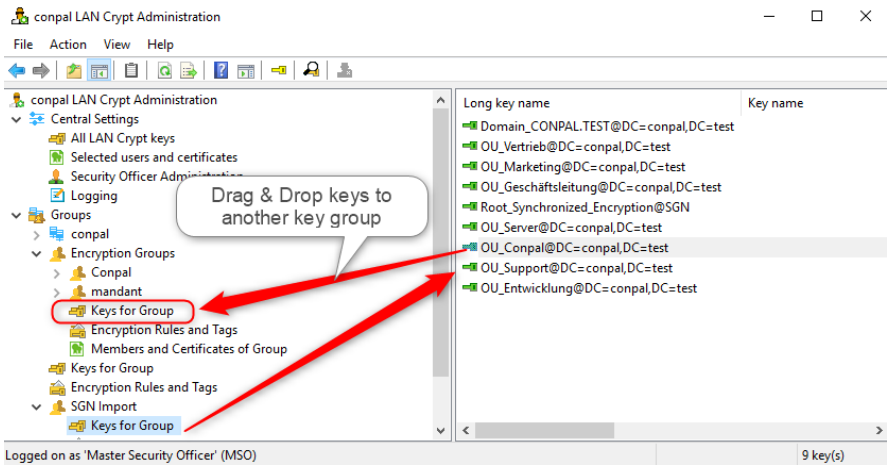


After the keys have been imported, you will receive a message confiming the transfer. All keys are available in conpal LAN Crypt, and you can terminate the tool at this point.



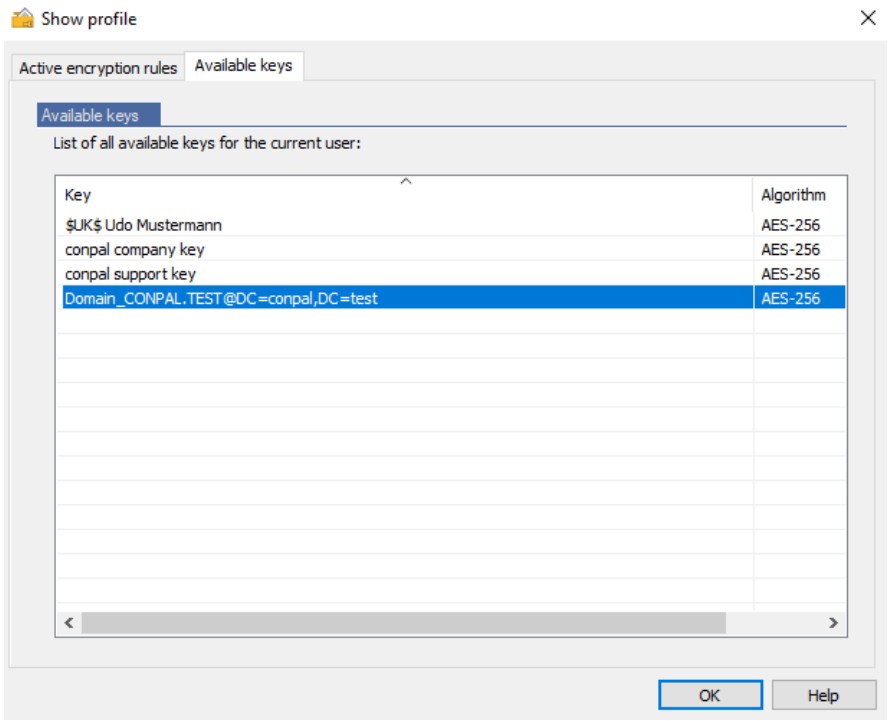
Assign Keys

The last step is to make the keys available to your users. This heavily depends on whether you already have a conpal LAN Crypt environment to simply add keys from SGN to, or whether you're doing a fresh migration from SGN to conpal LAN Crypt.
In the first case, just add the keys to existing groups or create a few new ones. In the latter case, it makes sense to re-create your encryption structure in conpal LAN Crypt.



Assigning a key to another group can be done by drag & drop.

If you require assistance on this, please contact conpal support at support@conpal.de.
After re-assingning the keys, you can build a user's profile and verify whether access to the SafeGuard encrypted files is possible. On the client side, you can also verify whether the imported key found its way into the user's profile:



Don't't forget to reenable loggin the console if it's still switched off!

And that's it. You're done. All SafeGuard encrypted files are now accessible with conpal LAN Crypt.

VE1.1