Anleitung File Encryption Migration

SafeGuard Enterprise

SafeGuard Enterprise („SGN") ist eine Sicherheitssuite von Sophos. Sie besteht aus mehreren Modulen, wobei Data Exchange (DX), Cloud Storage (CS) und File Encryption (FE) alle eine Verschlüsselung auf Dateiebene bieten. Die gesamte Software-Suite wird nun eingestellt. Die Benutzer laufen Gefahr, den Zugriff auf ihre verschlüsselten Dokumente zu verlieren. Die Migration von einem Sicherheitsprodukt zu einem anderen kann mühsam sein und ein zusätzliches Risiko darstellen, vor allem wenn der Prozess die Entschlüsselung der Daten beinhaltet. Dies ist bei der Migration zu conpal LAN Crypt nicht der Fall.

conpal LAN Crypt und Sophos SafeGuard Enterprise sind voll kompatibel

Sophos SafeGuard Enterprise und conpal LAN Crypt verfügen über die gleiche technische Basis und das gleiche System zur Dateiverschlüsselung. Daher sind in SafeGuard Enterprise verschlüsselte Dateien vollständig kompatibel mit conpal LAN Crypt und können von diesem gelesen werden. Die Verschlüsselungsschlüssel sind spezifisch für jede Installation, und nur diese müssen migriert werden.

Schlüssel aus SafeGuard Enterprise exportieren

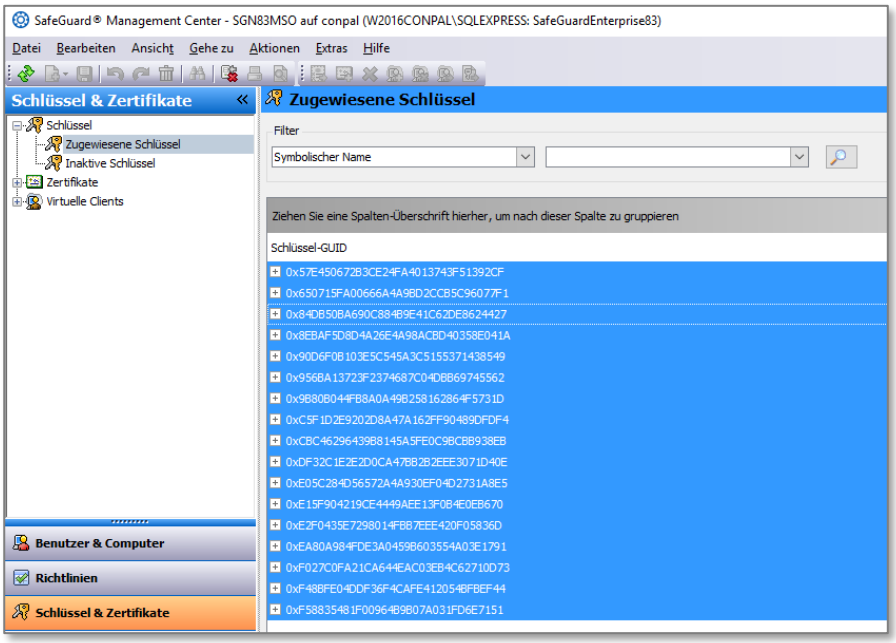
Der Export der Schlüssel kann auf jedem Rechner erfolgen, der sich an der Sophos SafeGuard Enterprise Konsole anmelden kann. Sie benötigen ein Konto mit Security Officer-Rechten, um die zu exportierenden Schlüssel verwalten zu können. Je nach Konfiguration Ihrer Security Officer Berechtigungen können möglicherweise nicht alle Security Officer alle verfügbaren Schlüssel Ihrer Umgebung verwalten.

Am Security Officer-Konto anmelden

In der Regel gibt es einen so genannten Master Security Officer mit globalen Rechten. Wenn Sie alle verfügbaren Schlüssel exportieren möchten, wäre dieses Konto das geeignete.

Legen Sie fest, welche Schlüssel Sie exportieren und nach conpal LAN Crypt migrieren wollen

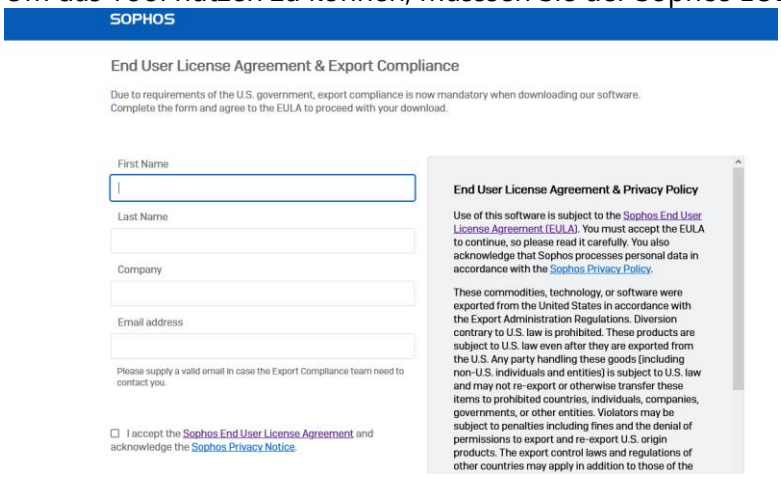
Wenn Sie nicht sicher sind, welche Schlüssel Sie exportieren sollen, empfiehlt es sich der Export aller Schlüssel. Dies hängt auch davon ab, wie die Schlüsselgenerierung in SafeGuard Enterprise konfiguriert wurde. Möglicherweise gibt es eine Reihe von Schlüsseln, die nicht für die Dateiverschlüsselung, sondern für andere Zwecke verwendet wurden.
Sie benötigen nur die für die Dateiverschlüsselung verwendeten Schlüssel

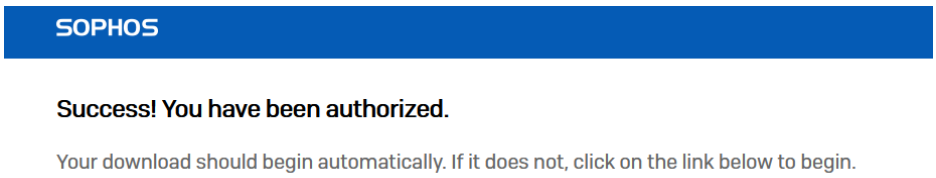


Wenn Sie hierbei Hilfe benötigen, nehmen Sie mit dem conpal Support unter support@conpal.de Kontakt auf.

Bezug des ‘KeyExporter’ Tools

Sophos stellt Kunden, die eine Migration (planen), ein Key-Exporter-Tool zur Verfügung.
Das Release ist Teil der SafeGuard Decryption Tools und steht ab sofort zum Download bereit.
Der Link wird von conpal, Ihrem Partner oder Sophos zur Verfügung gestellt.
Bitte leiten Sie diesen Link nicht weiter und veröffentlichen Sie ihn nicht.
Um das Tool nutzen zu können, müsssen Sie der Sophos EULA und den Exportrichtlinien zustimmen



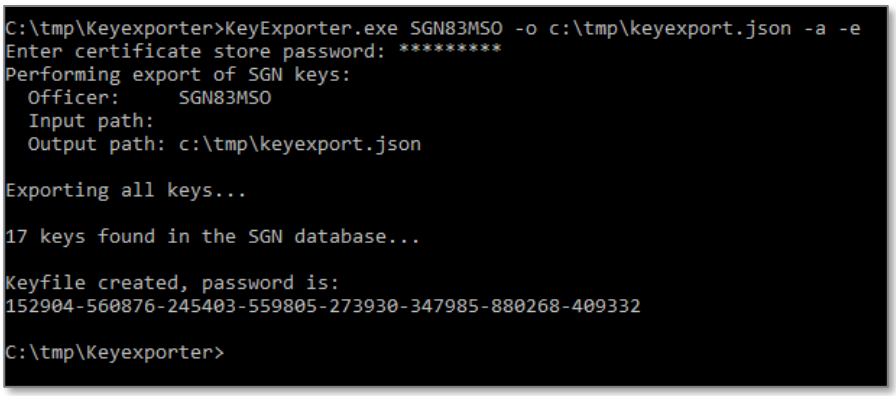


Extrahieren Sie die Datei keyexporter.exe und die Laufzeitumgebung aus diesem Paket.

Benutzung des ‘KeyExporter’ Tools

In diesem Beispiel werden wir alle Schlüssel aus der SafeGuard-Umgebung exportieren.

Öffnen Sie Windows Terminal/Kommandozeile und führen Sie `keyexporter.exe` aus, dazu müssen Sie nicht über Administratorenrechte verfügen:



Sie müssen nun Ihren SafeGuard Enterprise Kontonamen und den Pfad zur keyexport.json Datei angeben. Es gibt einen Parameter um alle zu exportieren:

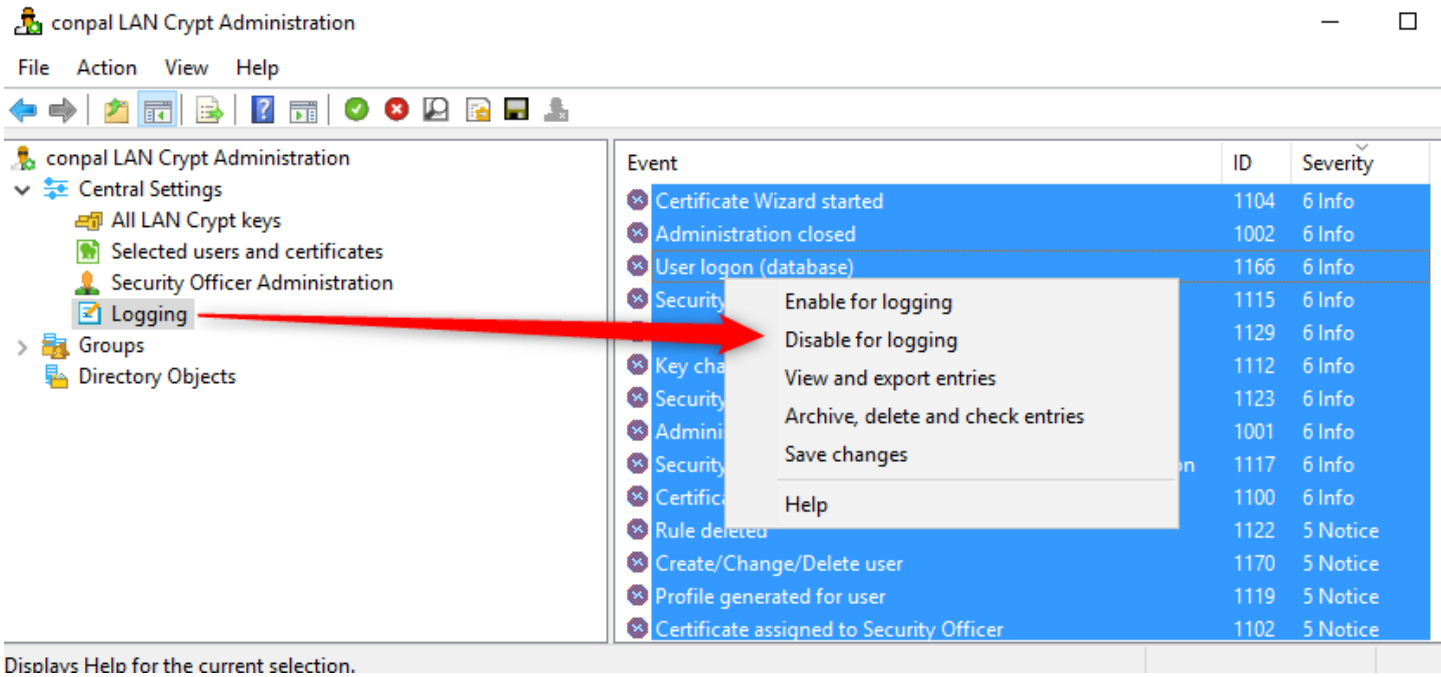
```
c:\tmp\SGN\KeyExporter.exe SGN83MSO -o c:\temp\keyexport.json -a
```

Sie werden dann nach dem Passwort für den Zertifikatspeicher des Security Officer gefragt (das Anmeldepasswort für die SafeGuard-Konsole). Anschließend wird der Export gestartet.
Die Exportdatei selbst wird verschlüsselt, so dass zu keinem Zeitpunkt Klartext sichtbar ist.
Aus diesem Grund kann der Export bei einer großen Zahl an Schlüsseln einige Zeit in Anspruch nehmen, haben Sie also bitte etwas Geduld.
Am Ende wird Ihnen ein Passwort angezeigt, das Sie sich merken/kopieren müssen. Dieses Passwort wird benötigt, um im nächsten Schritt die Schlüssel in conpal LAN Crypt zu importieren.

Schlüssel in conpal LAN Crypt importieren

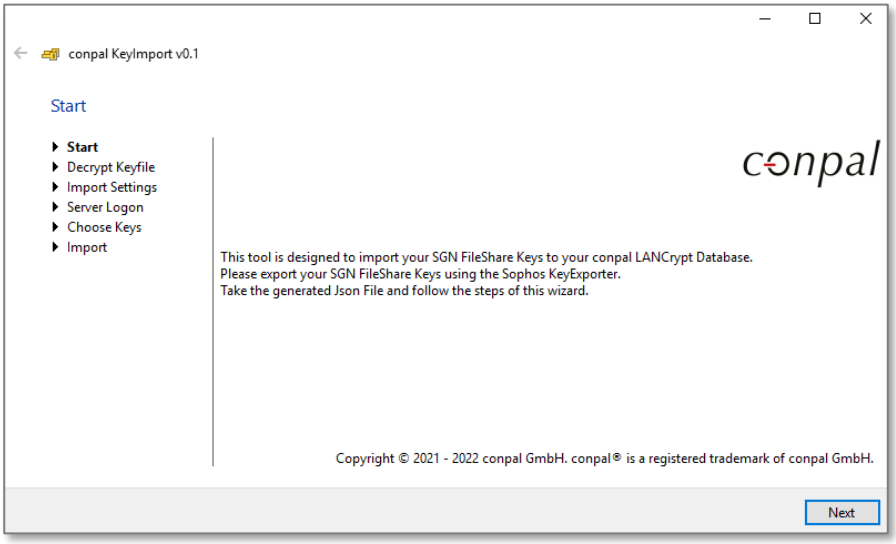
Nachdem die Schlüssel erfolgreich aus SafeGuard Enterprise exportiert wurden, können Sie sie nach conpal LAN Crypt migrieren, indem Sie sie in die conpal LAN Crypt Administration importieren.

Wichtig:
Für den Importvorgang der Schlüssel muss in der LAN Crypt Admin Konsole das Logging deaktiviert werden, dies kann nach dem Importvorgang wieder aktiviert werden:



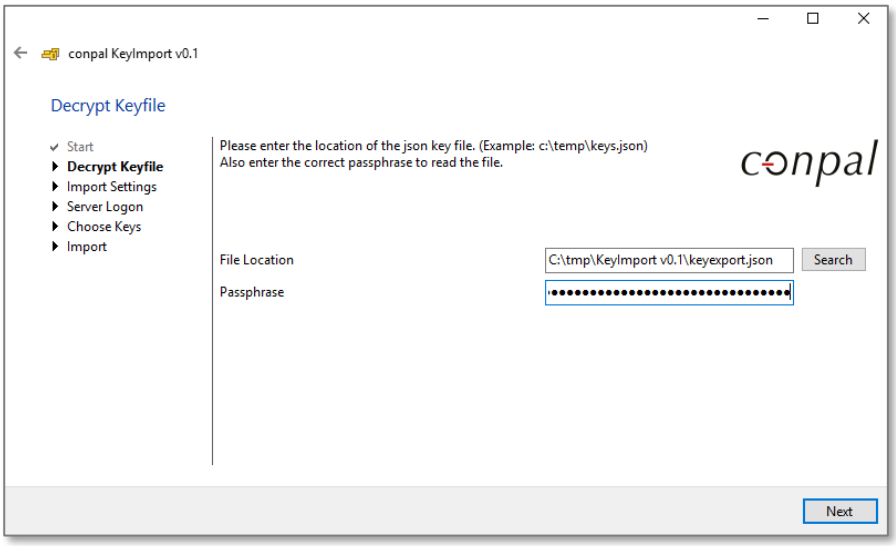
Benutzung des 'KeyImporter' Tools

Führen Sie auf einem Rechner, der in der Lage ist, sich bei der Verwaltungskonsole von conpal LAN Crypt anzumelden, `KeyImporter.exe`. Ein Assistent wird Sie durch den Importvorgang führen.



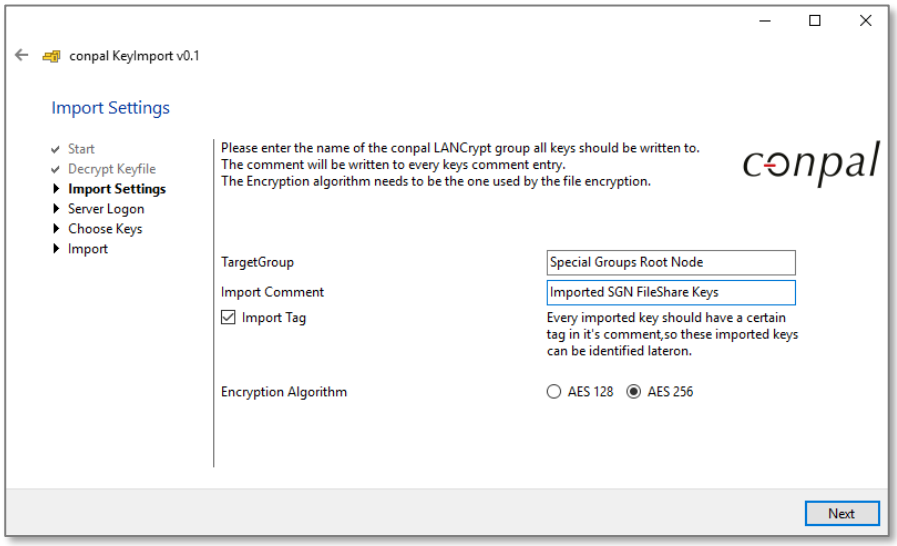
Zu importierende Datei auswählen

Wählen Sie die zuvor exportierte `keyexport.json` Datei aus und geben Sie das Passwort ein:



Importoptionen anpassen

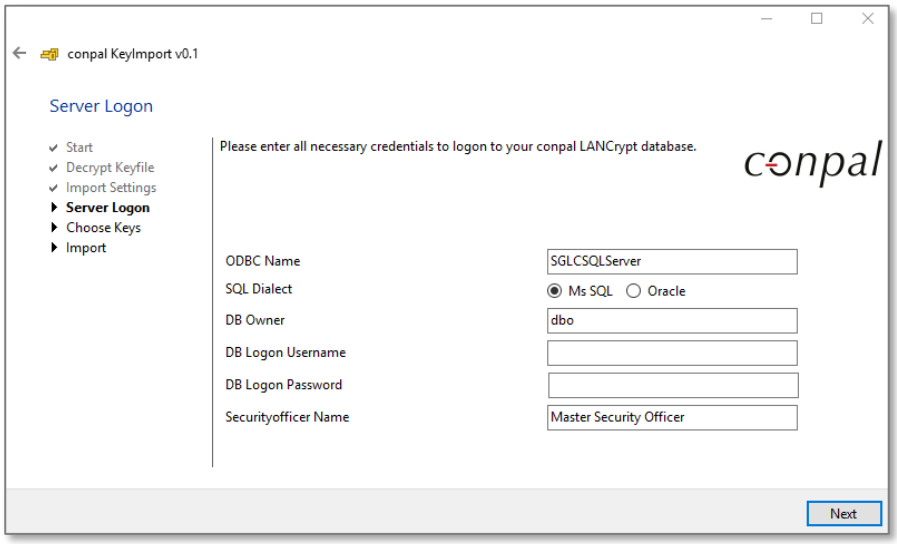
In conpal LAN Crypt sind die Schlüssel mit einer Gruppe verknüpft, aber Sie können sie auch zu einem späteren Zeitpunkt mit jeder beliebigen Gruppe verknüpfen. In diesem Schritt sollten Sie eine Gruppe auswählen, in der alle importierten Schlüssel gespeichert werden sollen.
Die "Special Groups Root Node" ist die Stammgruppe von conpal LAN Crypt. Legen Sie nach eigenem Ermessen eine Gruppe "SGN-Import" in der conpal LAN Crypt-Administration an und wählen Sie diese Gruppe als Ziel.
Es ist sinnvoll, das Kommentarfeld des Schlüssels zu verwenden, um zu dokumentieren, welche Schlüssel importiert wurden, unabhängig davon, in welcher Gruppe sie sich befinden.



conpal LAN Crypt mit den nötigen Informationen zur Authentisierung versehen

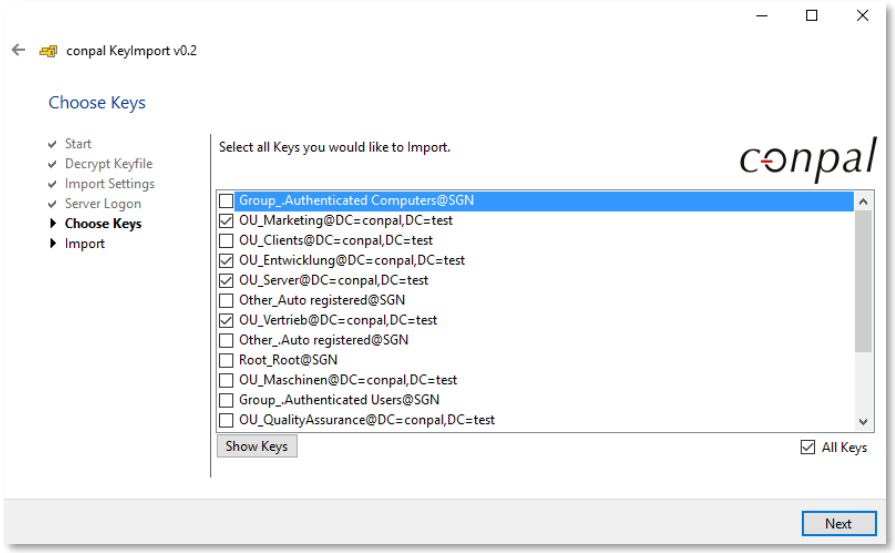
Die nächste Benutzeroberfläche fragt Sie nach Ihren Anmeldedaten. Beim Importieren der Schlüssel meldet sich der Importer bei der conpal LAN Crypt-Datenbank genauso an, wie Sie sich bei der Verwaltungskonsole anmelden würden. Geben Sie also den Namen eines Master Security Officer ein. Um die Schlüssel zu importieren, müssen Sie Zugriff auf das Zertifikat und den privaten Schlüssel dieses Beauftragten haben. Wenn Sie sich auf diesem Rechner an der Verwaltungskonsole anmelden können, funktioniert der Schlüsselimport auch mit diesem Rechner.

Sobald Sie sich mit einem lokalen SQL-Konto bei der SQL-Datenbank angemeldet haben, geben Sie bitte die SQL-Anmeldedaten ein: Wenn Sie mit Ihren Windows-Zugangsdaten autorisiert sind, lassen Sie das Feld einfach leer.

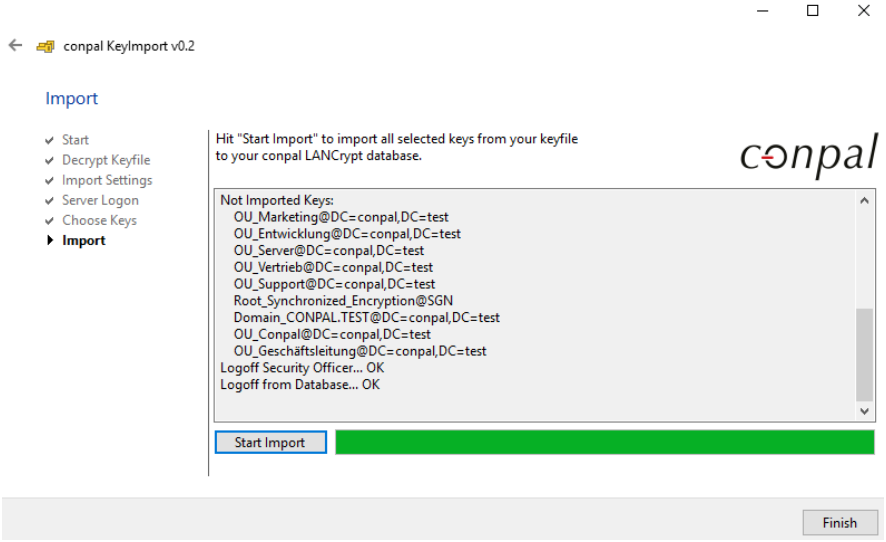


Schlüssel für den Import festlegen

Im letzten Schritt vor dem eigentlichen Importvorgang können Sie die Schlüssel auswählen, die Sie importieren möchten, oder alternativ einfach alle importieren (dies ist sinnvoll, wenn Sie bereits bestimmte Schlüssel im SGN ausgewählt haben):

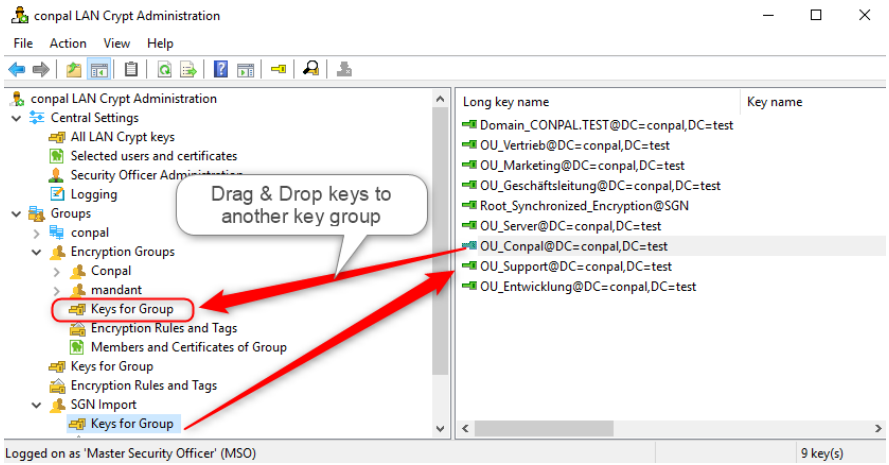


Nachdem die Schlüssel importiert wurden, erhalten Sie eine Meldung, die die Übertragung bestätigt. Alle Schlüssel sind in conpal LAN Crypt verfügbar, und Sie können das Tool nun beenden.



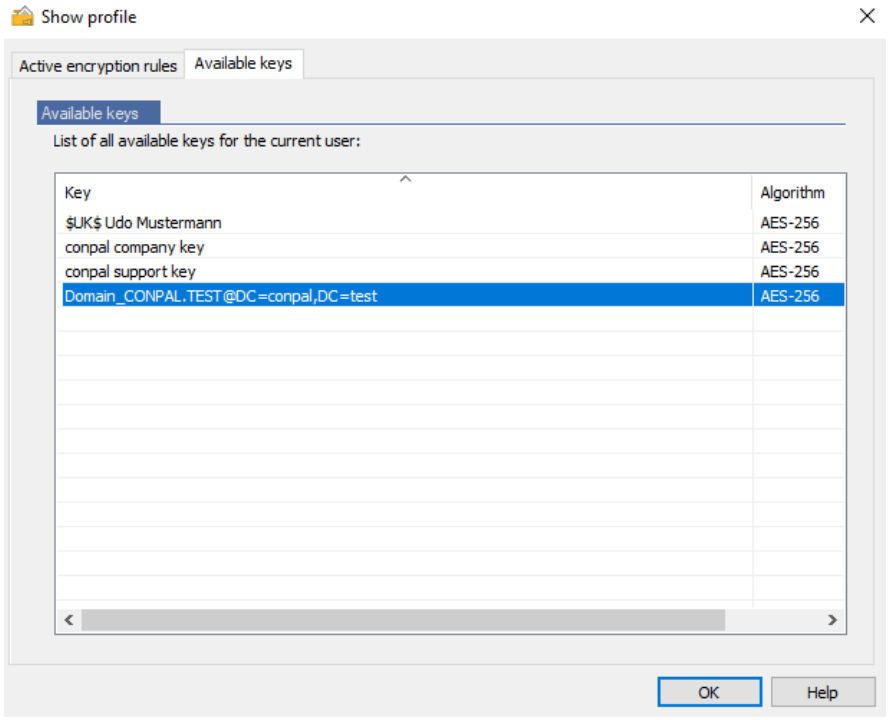
Schlüssel zuweisen

Der letzte Schritt besteht darin, die Schlüssel für Ihre Benutzer verfügbar zu machen. Dies hängt stark davon ab, ob Sie bereits eine conpal LAN Crypt-Umgebung haben, zu der Sie einfach Schlüssel von SGN hinzufügen können, oder ob Sie eine neue Migration von SGN zu conpal LAN Crypt durchführen.
Im ersten Fall fügen Sie die Schlüssel einfach zu bestehenden Gruppen hinzu oder erstellen ein paar neue Gruppen. Im zweiten Fall ist es sinnvoll, Ihre Verschlüsselungsstruktur in conpal LAN Crypt neu zu erstellen.



Die Zuweisung eines Schlüssels zu einer anderen Gruppe erfolgt per Drag & Drop.

Wenn Sie hierbei Hilfe benötigen, nehmen Sie mit dem conpal Support unter support@conpal.de Kontakt auf.
Nach der Neuzuordnung der Schlüssel können Sie ein Benutzerprofil erstellen und überprüfen, ob der Zugriff auf die von SafeGuard verschlüsselten Dateien möglich ist. Auf der Client-Seite können Sie auch überprüfen, ob der importierte Schlüssel seinen Weg in das Profil des Benutzers gefunden hat:



Bitte denken Sie daran das Logging in der Admin Konsole wieder zu aktivieren!

Und das wäre alles. Sie haben es geschafft. Alle mit SafeGuard verschlüsselten Dateien sind jetzt mit conpal LAN Crypt zugänglich.