DriveLock
securing your digital tomorrow

DriveLock und Thin Clients

USB-Laufwerkskontrolle in Citrix-Umgebungen

INHALT

1. Einleitung

Eine typische virtualisierte Umgebung besteht oft aus einer gemischten Infrastruktur von Endgeräten: FAT-Client-Systeme (z. B. Desktop- oder Notebook-Computer) werden in der Regel von Mitarbeitern verwendet, um zusätzlich auf Anwendungen zuzugreifen, die nicht auf ihren PCs, sondern zentral (z.B. auf Terminal Servern) ausgeführt werden. Thin Clients werden in der Regel eingesetzt, um den Benutzern eine vollständige virtualisierte Arbeitsumgebung zu bieten, die zentral gesteuert und verwaltet wird.

Dieses Dokument gibt einen Überblick über die verschiedenen Möglichkeiten, DriveLock in virtualisierten Umgebungen zusammen mit Citrix einzusetzen. Dabei ist ein grundsätzliches Verständnis für den Einsatz und die Konfiguration von DriveLock hilfreich. Weitere Informationen zur Nutzung und Konfiguration von DriveLock finden Sie online unter https://drivelock.help.

2. USB-Laufwerkskontrolle in Citrix-Umgebungen

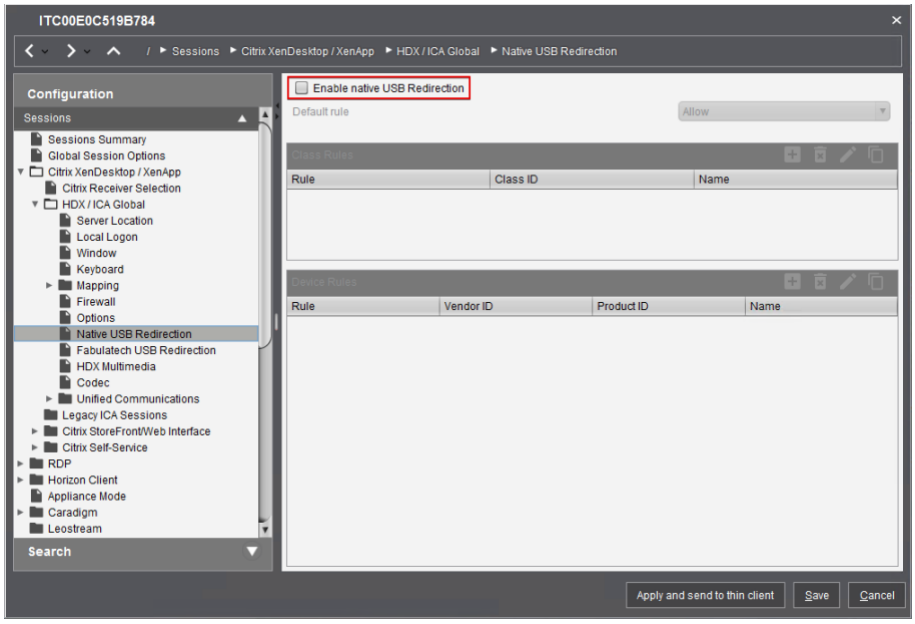
Der in DriveLock integrierte Support von Terminal Server Sessions ermöglicht eine sichere und flexible Steuerung der Nutzung von Laufwerken innerhalb von Terminal Services Client-Sitzungen, einschließlich lokaler Fest- und Wechsellaufwerke auf Client-Rechnern und Thin Clients.

Um die Möglichkeiten der UBS-Schnittstellenkontrolle besser zu verstehen, ist es hilfreich, sich die technischen Gegebenheiten einmal aus zwei verschiedenen Perspektiven genauer anzusehen. Einmal von der Citrix-Seite und anschließend aus der technischen Sicht des DriveLock Agenten.

2.1. Die Citrix-Sicht

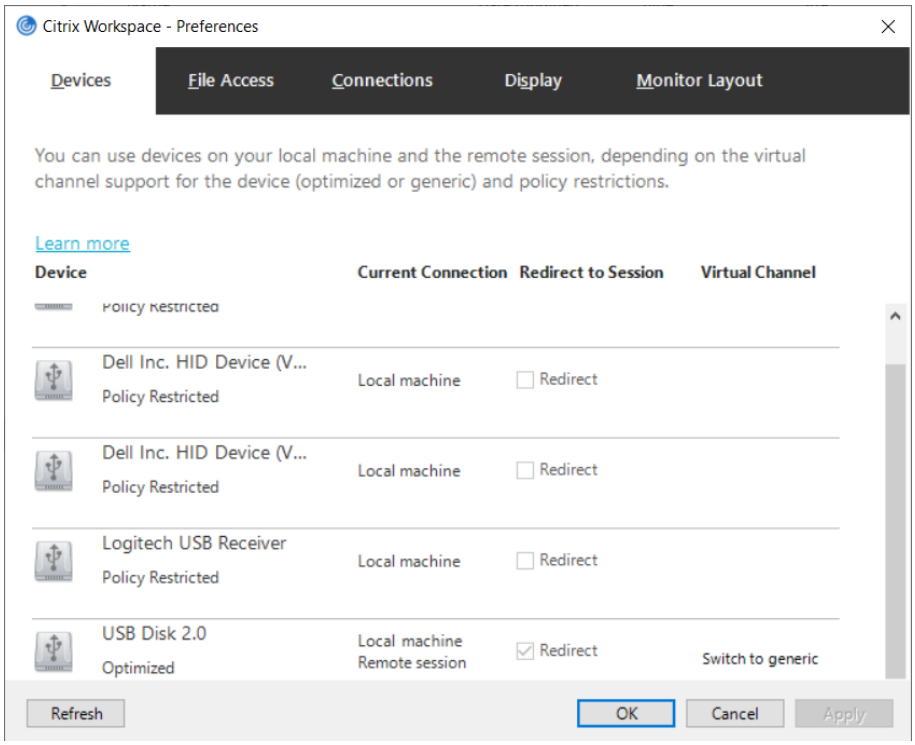
Citrix Workspace erlaubt zwei verschiedene Arten von Verbindungen von Laufwerken in eine Terminalsession: ICA-Client Drive Mapping und USB Redirection (Generic). Ob und welche der beiden Arten zur Verfügung stehen (es können auch beide sein), wird in der Citrix-Richtlinie in Citrix Studio festgelegt.

Darüber hinaus kann eine entsprechende Konfiguration z.B. auch über eine Verwaltungsoberfläche für die Thin Clients eingestellt werden (z.B. in Igel UMS).



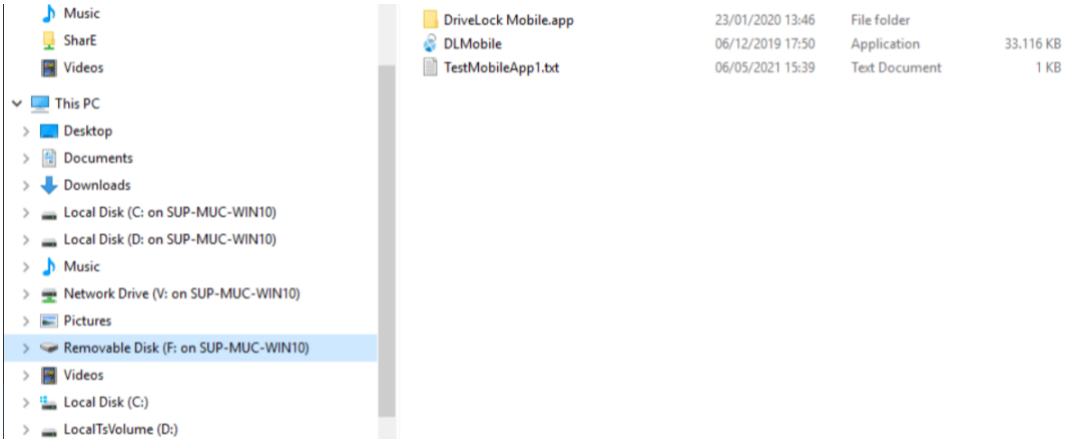
1.1.1 ICA-Dateiumleitung / ICA-Client drive mapping

In Citrix Workspace wird diese Methode als “Optimized” bezeichnet. Im Citrix Studio dagegen als „Dateiumleitung“. In Citrix Workspace erkennt man die entsprechende Umleitung in die Citrix-Session anhand des markierten „Redirect“:



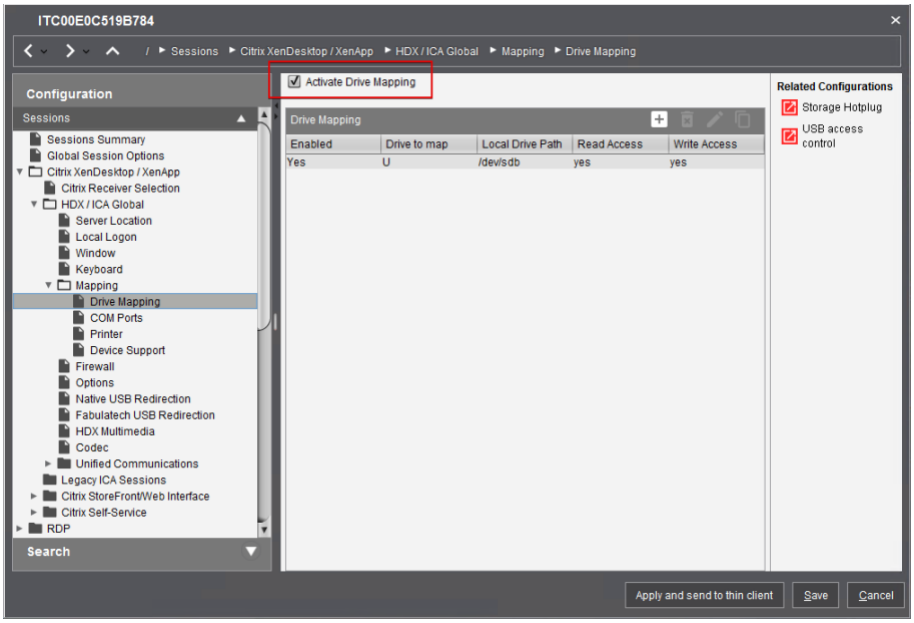
Dort kann man auch mit Click auf „Switch to generic“ (bzw. „Switch to optimized“) zwischen den beiden Methoden umschalten.

Die “Optimized”-Variante benutzt ein Citrix-eigenes Protokoll, um im virtuellen Desktop des Benutzers ein virtuelles Netzwerklaufwerk zur Verfügung zu stellen:



Aus Sicht des Anwenders erscheint das Laufwerk in der Session als „Removable Disk“ mit dem Zusatz „Laufwerksbuchstabe on Thinclient-Name“. Technisch handelt es sich um ein virtuelles Netzwerklaufwerk, ein sogenanntes Client Drive Mapping.

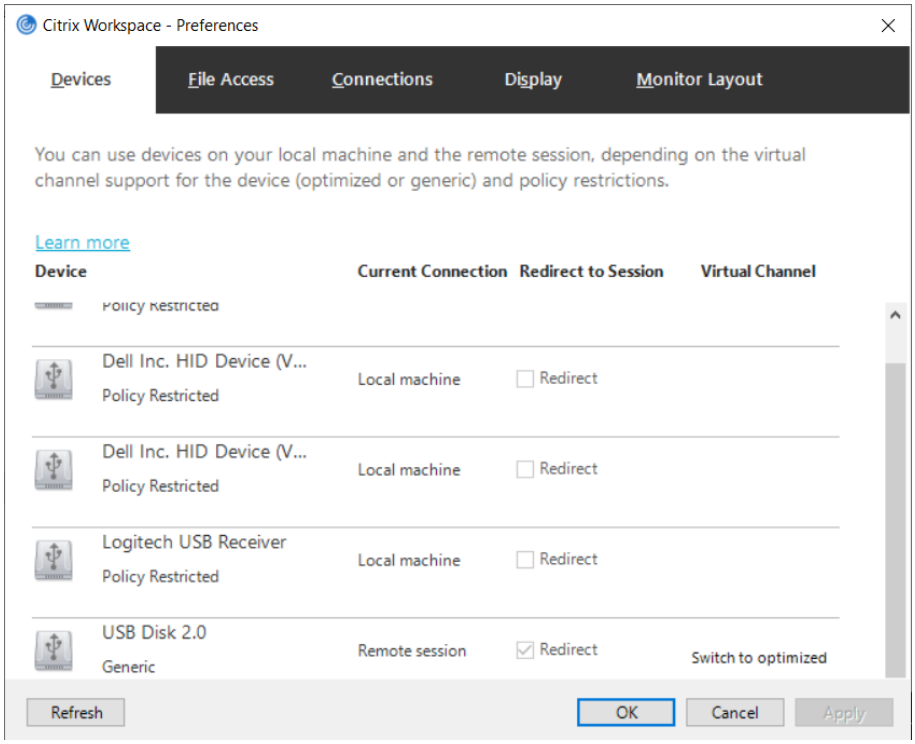
Auch über die Verwaltungsoberfläche des Thin-Client-Herstellers für die Thin Clients können Einstellungen dazu vorgenommen werden (z.B. in Igel UMS):



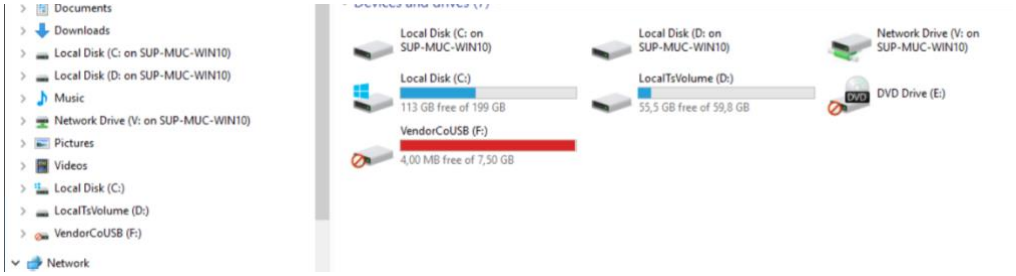
Bei dieser Art der Laufwerksfreigabe gibt es diverse technische Beschränkungen, wie eine maximale Dateigröße und auch eine maximale Größe des gesamten Datenträgers, die je nach Version des Citrix Workspace bzw. Citrix Receiver und der Version der Serversoftware variieren. Diese Einschränkungen sind auf der Citrix-Webseite dokumentiert. Der Vorteil, Laufwerke auf diese Weise freizugeben, liegt darin, dass ein Zugriff auf Dateien schnell durchgeführt wird und etwaige Netzwerk-Latenzzeiten (Verzögerungen) praktisch keine Rolle spielen.

1.1.2 USB Redirection

Die zweite Methode der Freigabe wird von Citrix „Generic“ genannt und in Citrix Workspace auch entsprechend dargestellt:



Bei dieser Variante handelt es sich um eine sogenannte USB-Weiterleitung, d.h. die Netzwerkleitung fungiert als (sehr) langes USB-Kabel und das USB-Gerät wird mit Hilfe der Citrix-Software quasi direkt am Server angeschlossen. Dadurch ist es auch im Gerätemanager von Windows sichtbar und verhält sich aus Benutzersicht wie ein USB-Stick, den man an einen Windows PC anschließt.

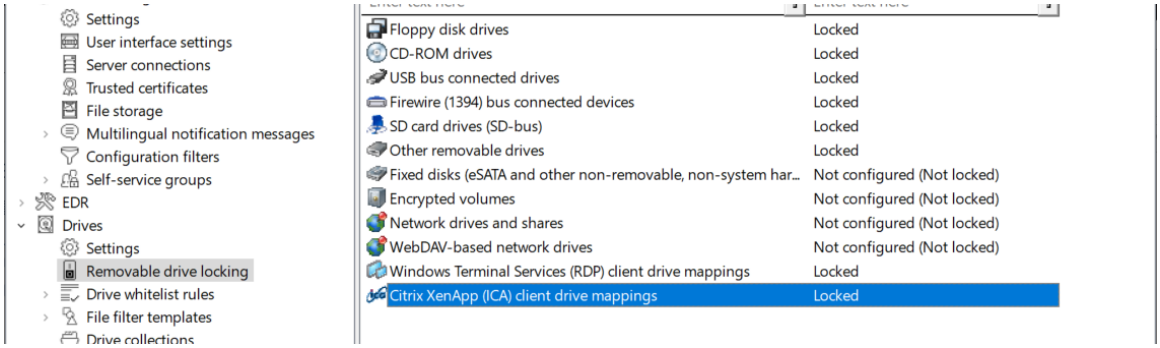


2.2. Die DriveLock-Sicht

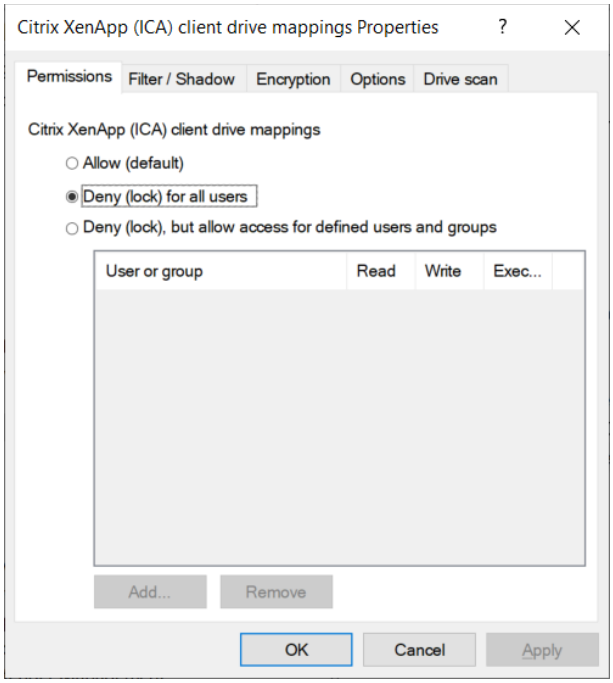
DriveLock kann sowohl mit einem ICA Client Drive Mapping als auch mit USB Redirection umgehen und Laufwerke entsprechend sperren oder freigeben. Da es sich jedoch um verschiedene Technologien handelt, erfolgt die Kontrolle innerhalb der DriveLock-Richtlinie an unterschiedlichen Stellen mit verschiedenen Whitelist-Regeln.

Laufwerke, die über die „Generic“-Methode angeschlossen werden, werden aus DriveLock-Sicht wie „normale“ USB-Geräte behandelt und entsprechend auch kontrolliert.

Laufwerke, die über die „Optimized“-Methode angeschlossen werden, sind keine USB-Geräte im eigentlichen Sinne, sondern werden in DriveLock über die Gerätekategorie „Citrix XenApp (ICA) client drive mappings“ kontrolliert (bzw. „Windows Terminal Services (RDP) client drive mappings“, falls das RDP-Protokoll zum Einsatz kommen sollte):

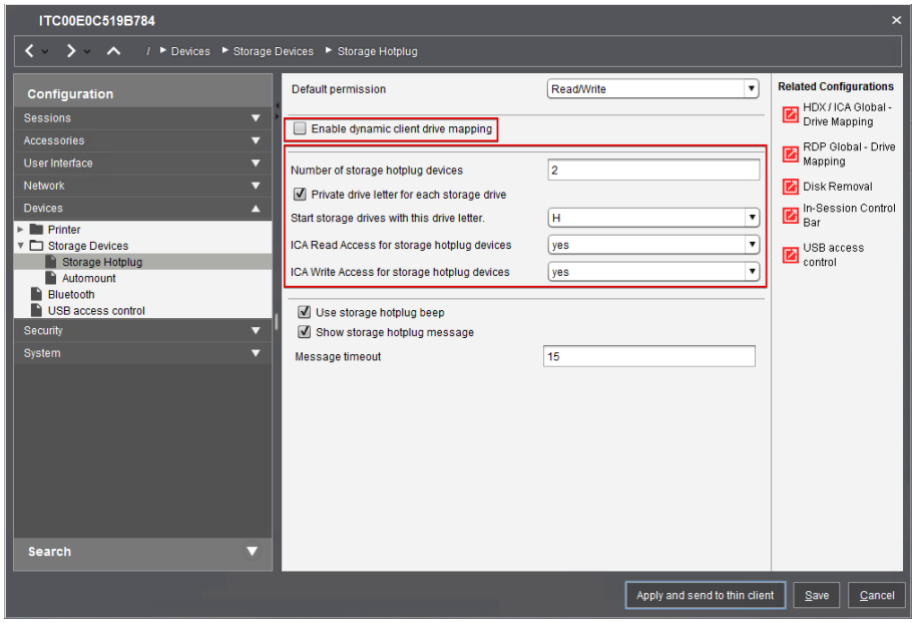


Unter „Removable drive locking“ kann dort – wie üblich – der Grundzustand für diese Laufwerke eingestellt werden:

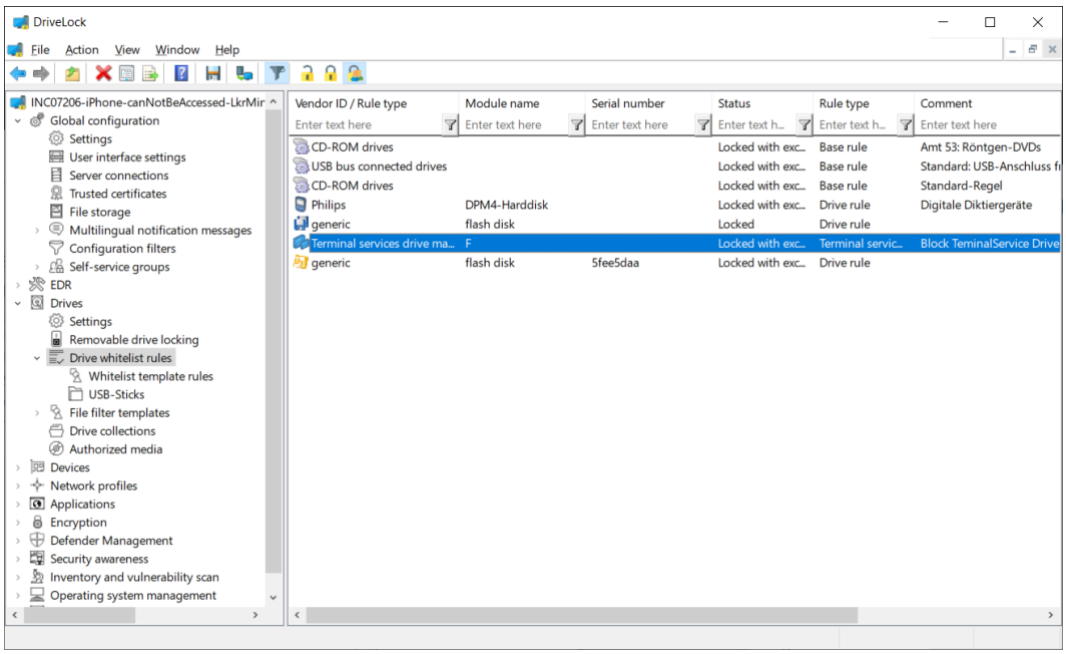


Einen wichtigen Unterschied gibt es hier im Vergleich zu „normalen“ USB-Sticks: das „Optimized“-Protokoll kennt keine Hardwaredaten. D.h. es gibt – da dies nicht in der ICA Protokoll-Spezifikation vorgesehen ist – keine Informationen, welcher konkrete USB-Stick sich hinter einem solchen Laufwerk verbirgt. Abhilfe schafft hier der „DriveLock Virtual Channel“ (wird im Abschnitt 2.3 näher beschrieben).

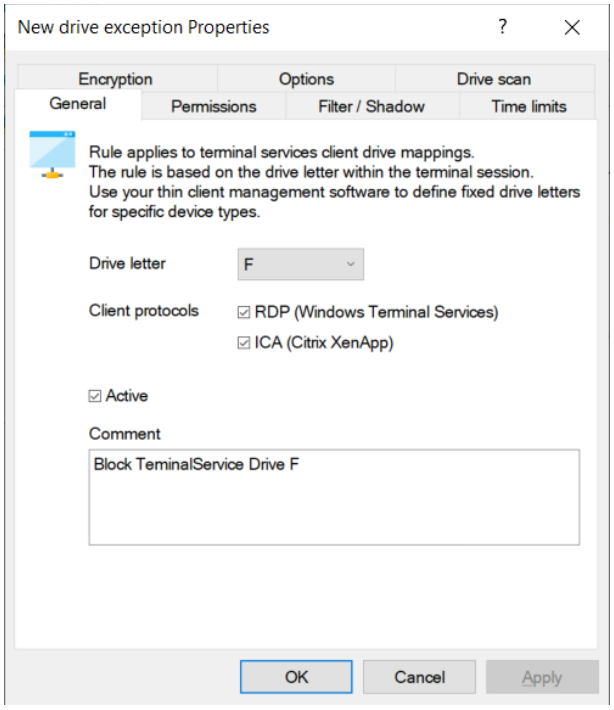
Wenn kein Virtual Channel im Einsatz ist, kann daher die Freigabe von Ausnahmen nur anhand des ICA-Laufwerksbuchstabens erfolgen, welcher i.d.R. durch die Thin-Client-Administrationssoftware vorgegeben werden kann:



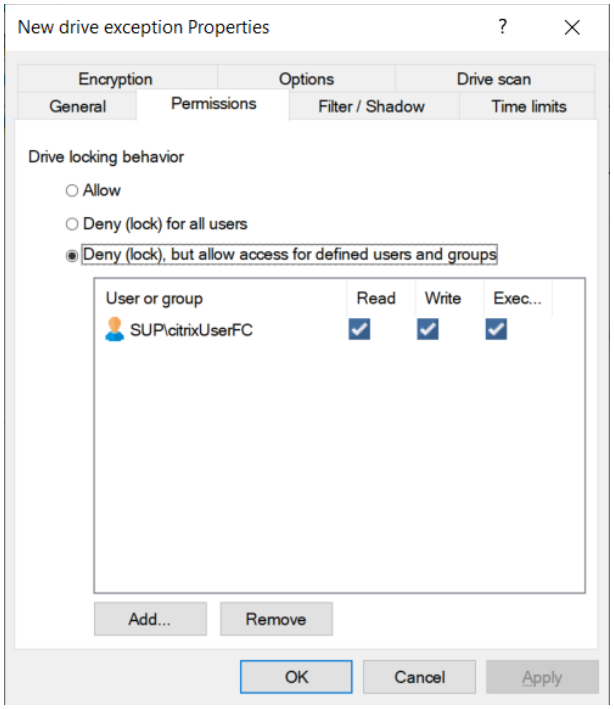
Eine „Terminal services drive mapping rule" ist die richtige Art von Laufwerksregel für eine solche Ausnahme in der DriveLock-Richtlinie.



Dort können die üblichen Optionen für Whitelist-Regeln eingestellt werden, die Identifikation der Regel erfolgt aber eben nicht anhand von Vendor- und Product-ID, sondern anhand von Protokoll und virtuellem Laufwerksbuchstaben:



Die restlichen Einstellungen entsprechen der in anderen Regeln gegebenen Möglichkeiten, man kann also z.B. bestimmte Benutzer(gruppen) für den Zugriff auf so ein Laufwerk berechtigen:

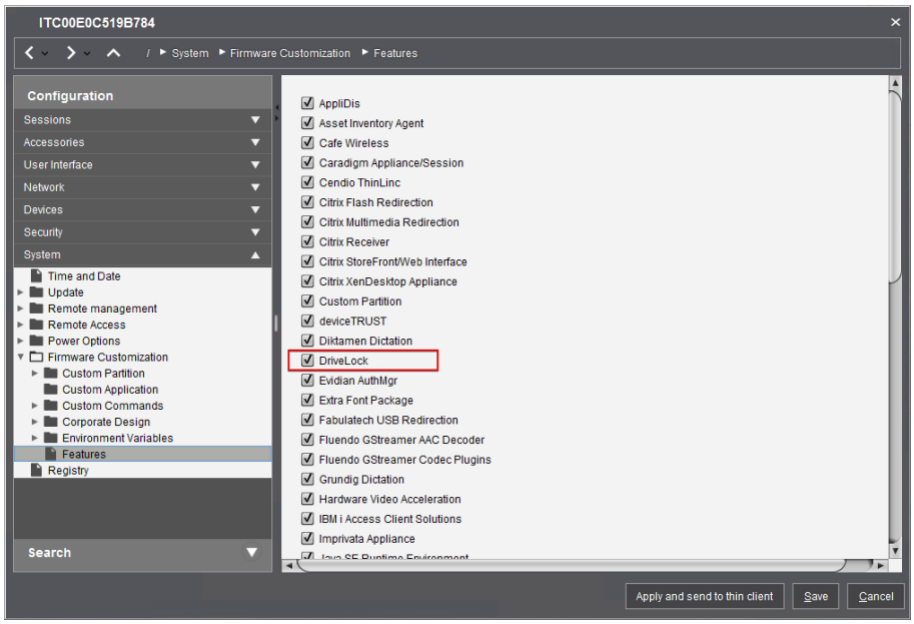


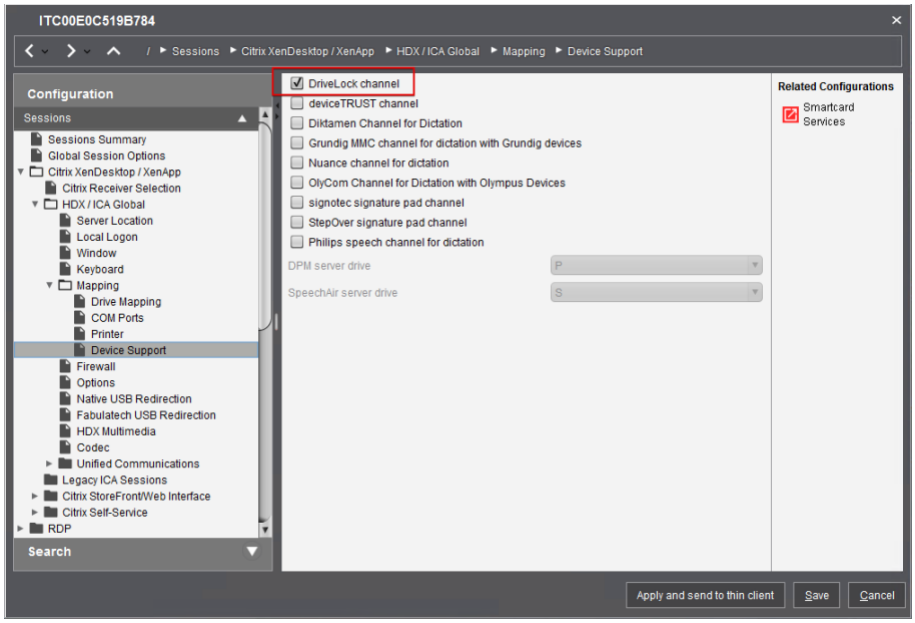
2.3. DriveLock Virtual Channel

Das „Optimized“ Protokoll erlaubt, wie oben erläutert, keine Übertragung von Hardwaredaten. Um eine Identifikation dieser Daten trotzdem zu ermöglichen, wurde der DriveLock Virtual Channel entwickelt. Dieser Virtual Channel ist eine Software, die auf dem Thin Client läuft, dort die benötigten Hardwaredaten sammelt und diese an den Server übermittelt (innerhalb eines sogenannten „Virtual Communication Channel“ im ICA-Protokoll – daher der Name).

Hiermit ist es dem DriveLock Agenten möglich zu erkennen, welche Hardware zu welchem Laufwerksbuchstaben innerhalb einer ICA-Session gehört.

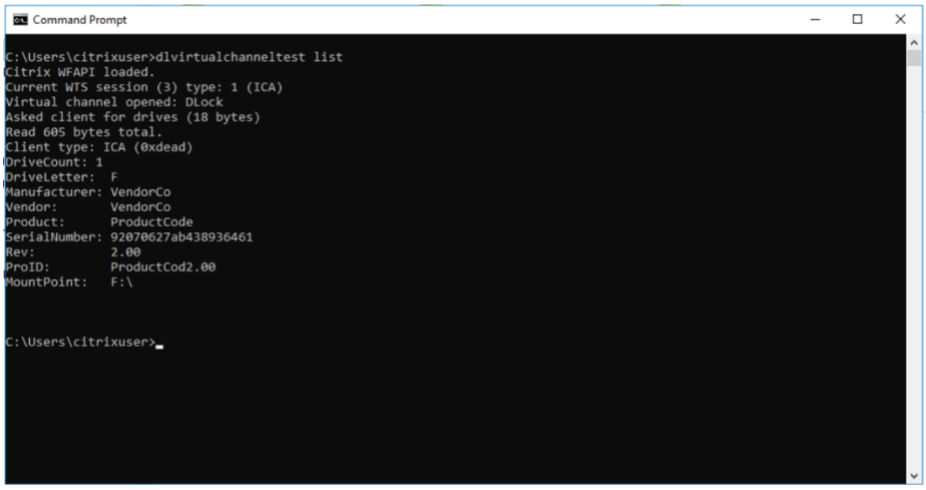
Der DriveLock Virtual Channel ist auf IGEL-Geräten bzw. in IgelOS bereits vorinstalliert und muss über die IGEL-Administrations-Oberfläche nur aktiviert werden.





Für Windows-basierte Thin Clients steht er zum Download zur Verfügung. Für andere Thin Clients kontaktieren Sie bitte den Thin Client-Hersteller.

Um die Verfügbarkeit des Virtual Channel zu testen, verbindet man sich in einer ICA-Session mit dem Server. Anschließen schließt man ein USB-Gerät am Thin Client an und öffnet einen Command Prompt in der ICA-Session. Mit der Ausführung des Befehls „dlvirtualchanneltest list“ werden die Hardwaredaten angezeigt, die mit Hilfe des Virtual Channel übermittelt wurden.

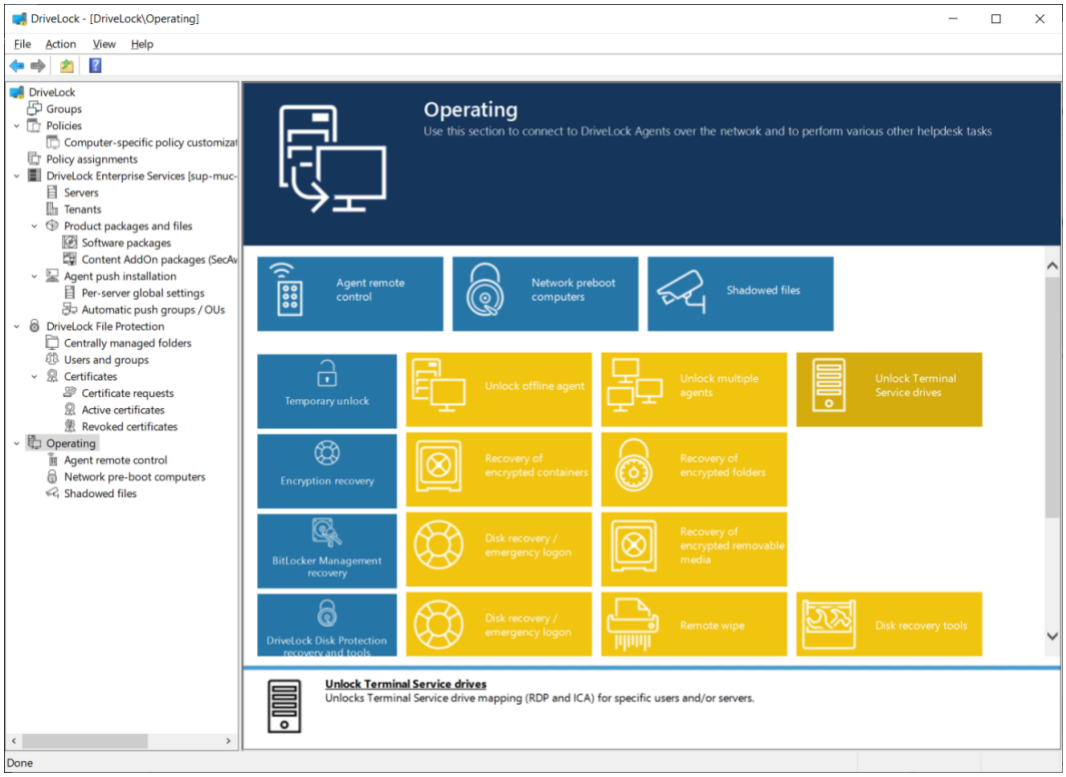


Ist der Virtual Channel korrekt eingerichtet, können innerhalb der DriveLock-Richtlinie „normale“ USB-Whitelist-Regeln auch für die ICA-Dateiumleitungen benutzt werden. Geräte werden dann anhand der übermittelten Hardwaredaten freigegeben.

Ist der Virtual Channel nicht verfügbar, kann die Freigabe wiederum nur über den Laufwerksbuchstaben erfolgen.

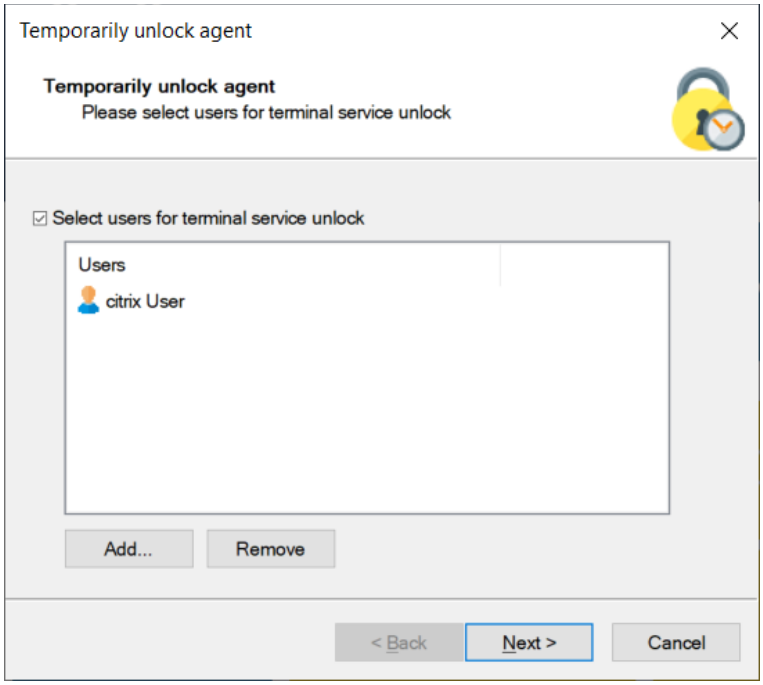
3. Temporäre Freigabe von USB-Laufwerken

Für Terminal-Server steht in DriveLock eine zusätzliche Funktion der temporären Gerätefreigabe zur Verfügung: „Unlock Terminal Services drives“.

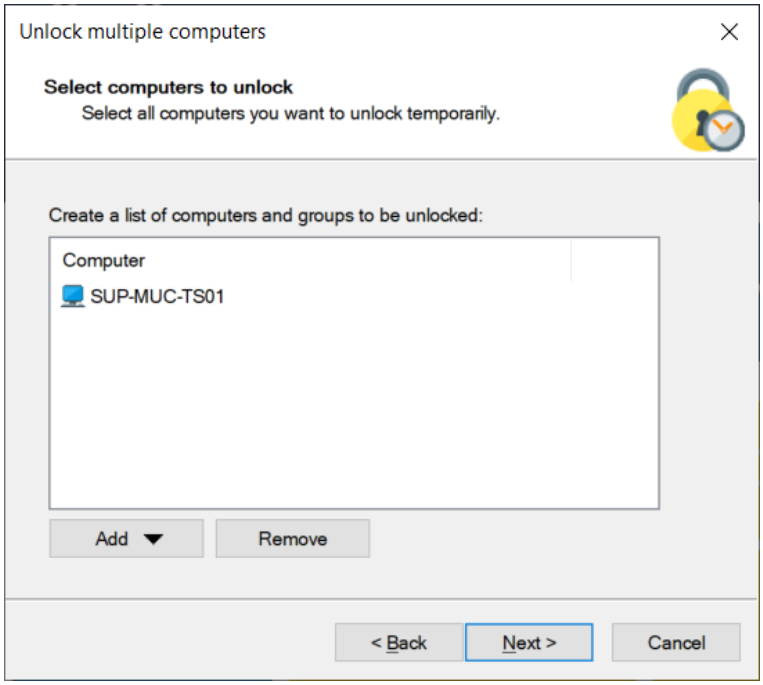


Über diese Funktion ist es möglich, auf dem Terminal Server bzw. einer Terminal Server Farm nur für bestimmte Benutzersitzungen eine Freigabe zu machen.

In dem entsprechenden Assistenten wird daher zunächst der freizugebende Benutzer ausgewählt:



Anschließend wählt man den oder die Citrix-Server. Diese Einstellung wird gespeichert, so dass man hier nur einmalig alle Server der Farm auswählen muss.



Nach der Auswahl der weiteren Optionen und Zeitdauer der Freigabe werden auf allen Servern Sitzungen des ausgewählten Benutzers gesucht und diese temporär freigegeben. D.h.

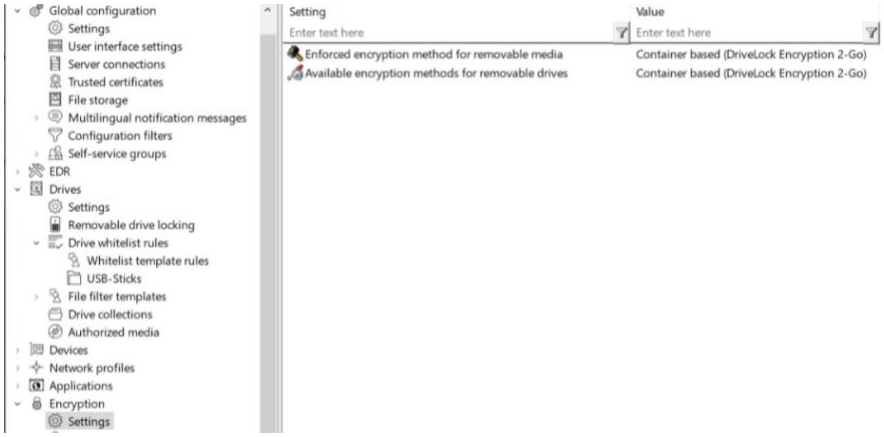
der Benutzer kann dann innerhalb seiner Sitzung z.B. USB-Laufwerke benutzen. Für andere Benutzer, die gerade auf dem Server angemeldet sind, gilt die Freigabe dagegen nicht.

4. Verschlüsselung von externen USB-Laufwerken

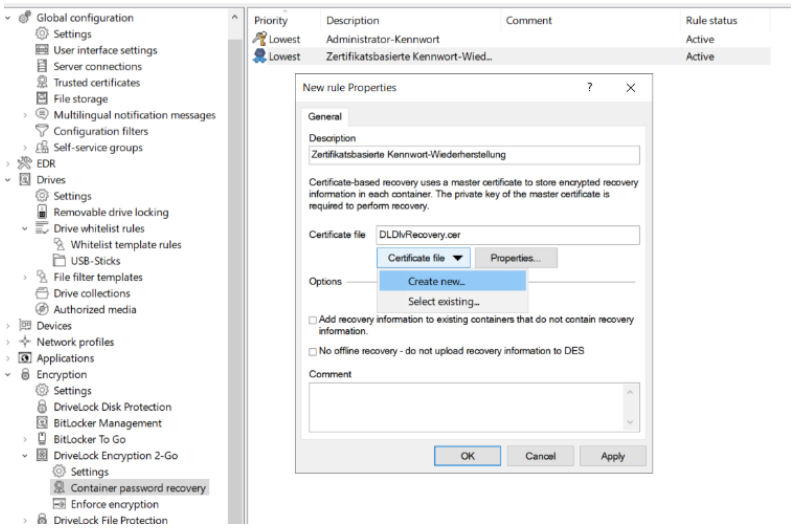
Wenn man „Generic“ verwendet, dann funktioniert die Verschlüsselung von Laufwerken mit allen Features so wie auf einem lokalen Rechner (da das Laufwerk ja unter Windows „ganz normal“ vorhanden ist).

Wenn man „Optimized“ verwendet, dann gibt es einige technischen Einschränkungen für die manuelle Verschlüsselung. Die automatische Verschlüsselung funktioniert aber wie gewohnt.

Notwendige Einstellungen dazu:

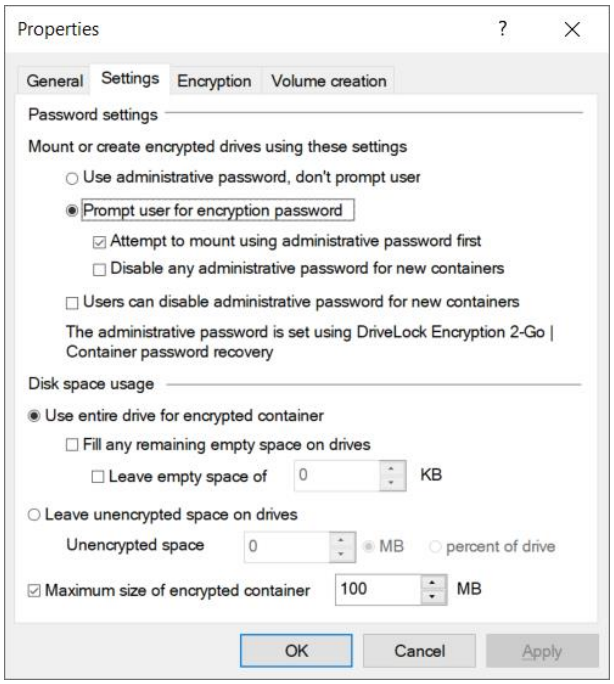


Verschlüsselungsart auswählen: nur „Container-based“ sollte verfügbar sein.

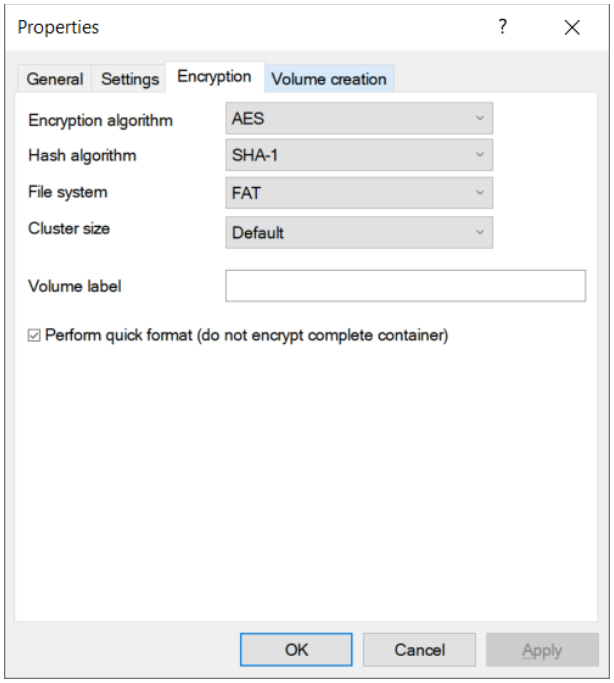


Recovery-Informationen anlegen für die Containerverschlüsselung.

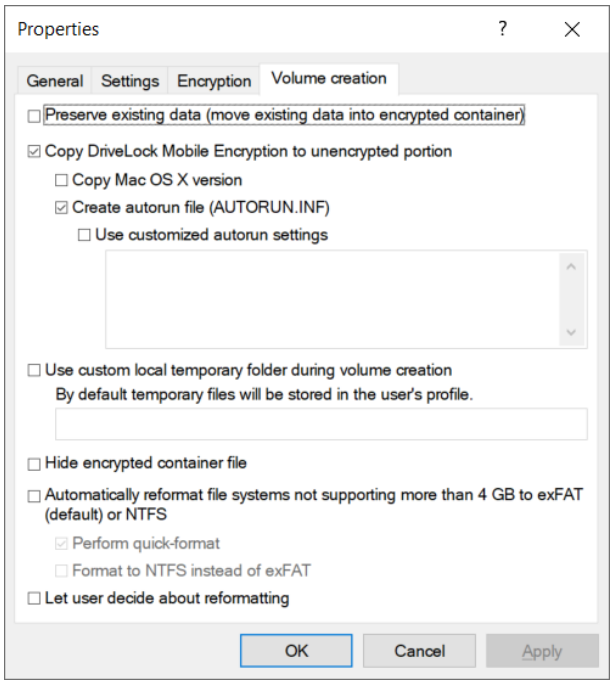
Unter „Enforced encryption“ die Einstellungen bearbeiten. Folgende Einstellungen sind empfohlen:



Die maximale Containergröße kann gesetzt werden, falls es für die benutzten Thin-Clients oder ICA-Protokolle/Citrix-Receiver Einschränkungen gibt. Die üblichen ICA-Einschränkungen (2 bzw. 4 GB maximale Dateigröße) sind dem DriveLock Agenten bekannt.

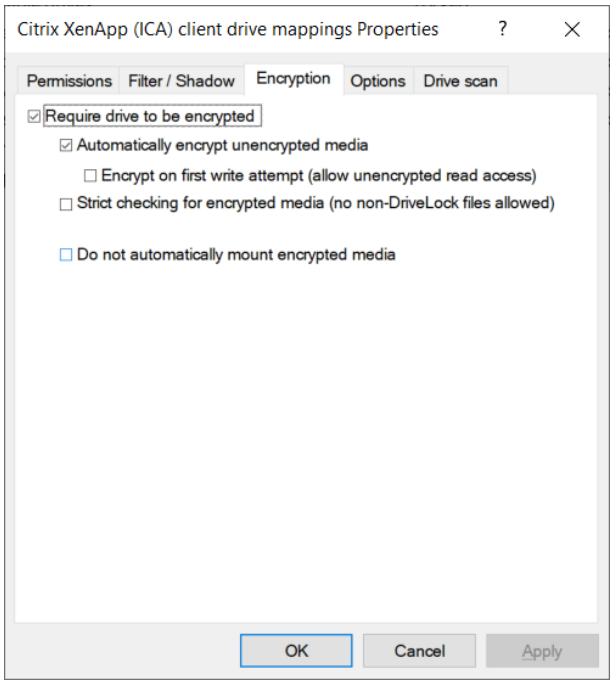


Quick Format sollte gewählt werden, sonst dauert die initiale Verschlüsselung sehr lang. Bei IGEL Thin Clients gibt es hier eine Beschleunigung über den DriveLock Virtual Channel.

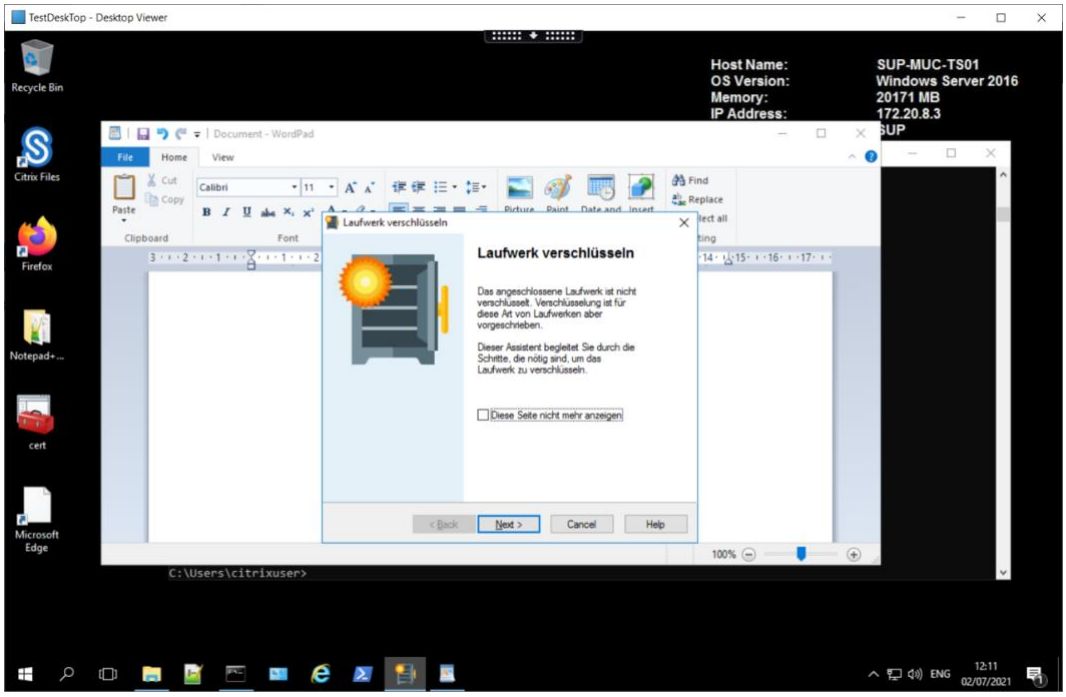


Bestehende Daten sollte wenn möglich nicht gerettet werden (aus Performancegründen). Das Kopieren von großen Datenmengen über die ICA Optimized Methode ist nicht sonderlich performant.

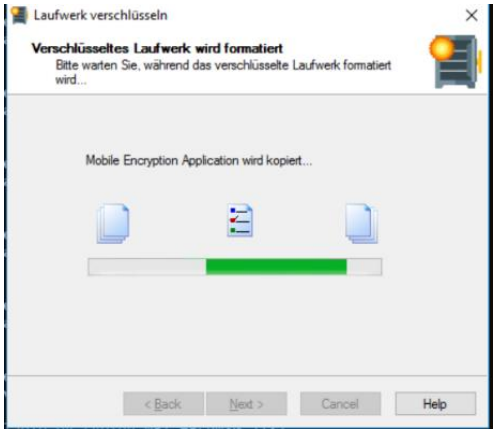
Wenn diese Einstellungen gemacht sind, kann unter „Removable drive locking“– wie üblich – der Grundzustand für die erzwungene Verschlüsselung eingestellt werden:



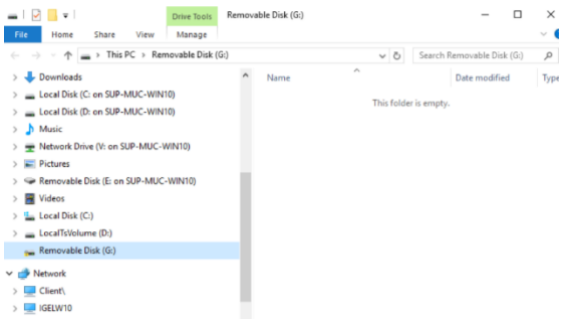
In der ICA-Session sieht das dann wie gewohnt aus:



…

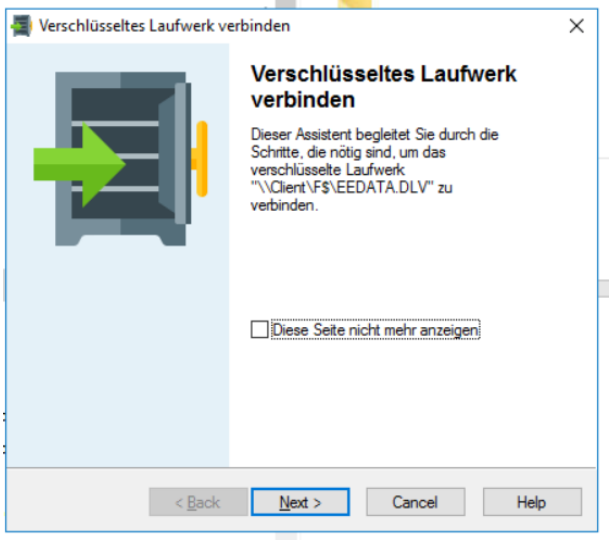


...



Am Ende hat man ein neues verschlüsseltes Laufwerk in der ICA-Session verbunden.

Wenn man das Laufwerk dann an eine andere ICA-Session anschließt, erscheint auch der Mount-Dialog:



Es ist zu beachten, dass je nach verwendetem ICA-Receiver/Citrix-Workspace man manchmal auf das Client-Drive-Mapping klicken muss, damit der Mount- bzw. Anlegen-Dialog erscheint. Bei Thin Clients gibt es dieses Problem normalerweise nicht, aber bei manchen Versionen unter Windows tritt dieses auf.

5. Weiterführende Informationen

Weitere technische Artikel bzw. Whitepaper bzw. auch die vollständige Dokumentation der DriveLock Zero Trust Plattform steht unter https://drivelock.help zur Verfügung.