DriveLock
securing your digital tomorrow

DriveLock and Thin Clients

USB drive control in Citrix environments

CONTENTS

Note: This article is machine translated from German!

1. Introduction

A typical virtualized environment often consists of a mixed infrastructure of end devices: FAT client systems (e.g. desktop or notebook computers) are usually used by employees to additionally access applications that are not executed on their PCs but centrally (e.g. on terminal servers). Thin clients are generally used to provide users with a complete virtualized working environment that is centrally controlled and managed.

This document provides an overview of the various options for using DriveLock in virtualized environments together with Citrix. A basic understanding of the use and configuration of DriveLock is helpful. Further information on the use and configuration of DriveLock can be found online at https://drivelock.help.

2. USB drive control in Citrix environments

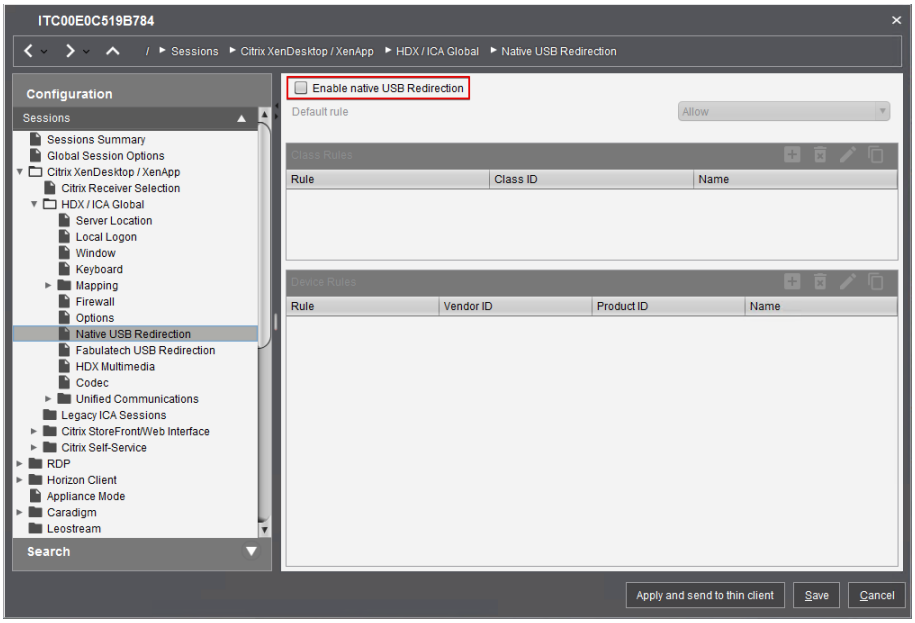
DriveLock's built-in support for Terminal Server sessions enables secure and flexible control of drive usage within Terminal Services client sessions, including local fixed and removable drives on client computers and thin clients.

In order to better understand the possibilities of UBS interface control, it is helpful to take a closer look at the technical conditions from two different perspectives. Firstly, from the Citrix side and then from the technical perspective of the DriveLock agent.

2.1. The Citrix view

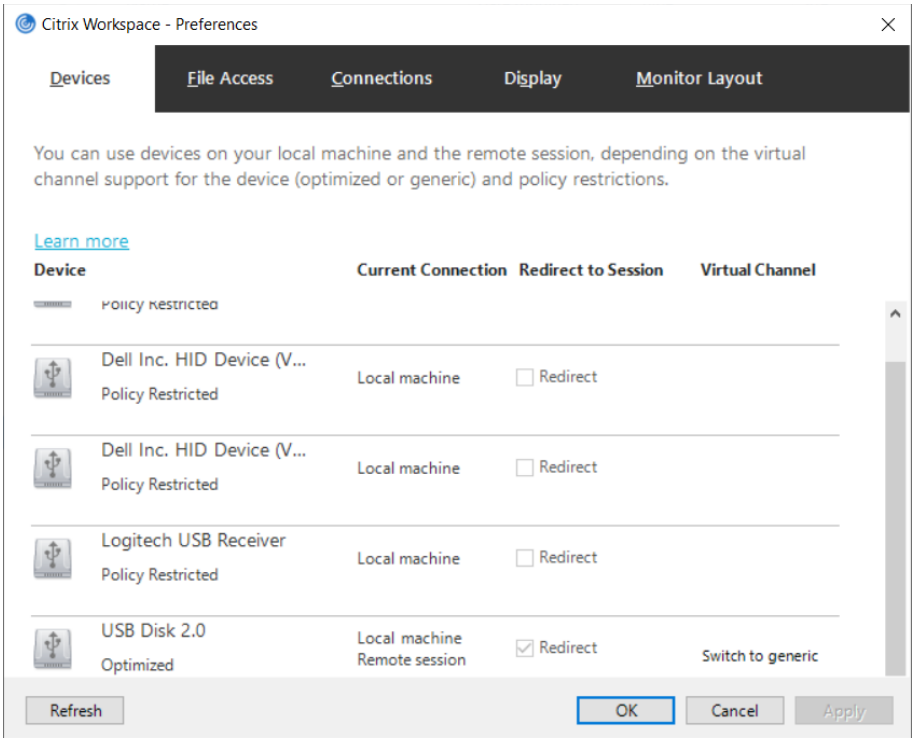
Citrix Workspace allows two different types of drive connections into a terminal session: ICA Client Drive Mapping and USB Redirection (Generic). Whether and which of the two types are available (it can also be both) is defined in the Citrix policy in Citrix Studio.

In addition, a corresponding configuration can also be set via an administration interface for the thin clients (e.g. in Igel UMS).



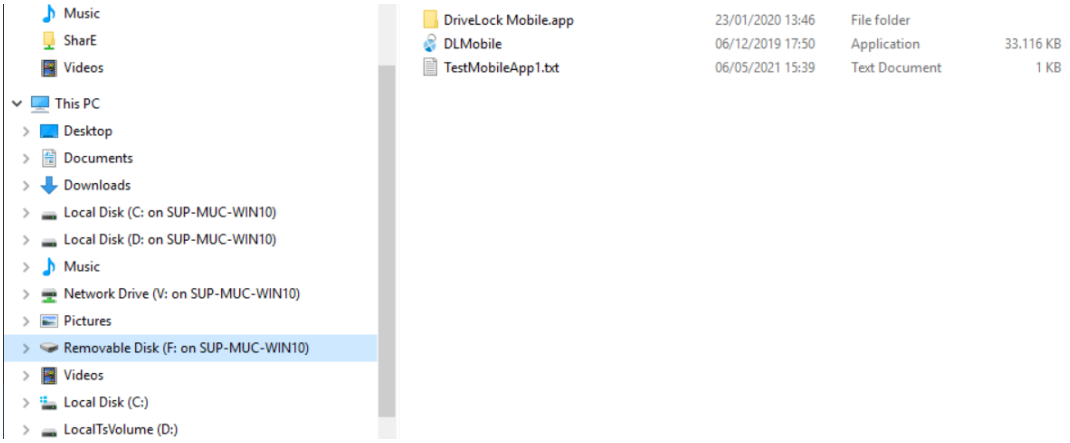
1.1.1 ICA file redirection / ICA client drive mapping

In Citrix Workspace, this method is called "Optimized". In Citrix Studio, on the other hand, it is called "File redirection". In Citrix Workspace, you can recognize the corresponding redirection in the Citrix session by the marked "Redirect":



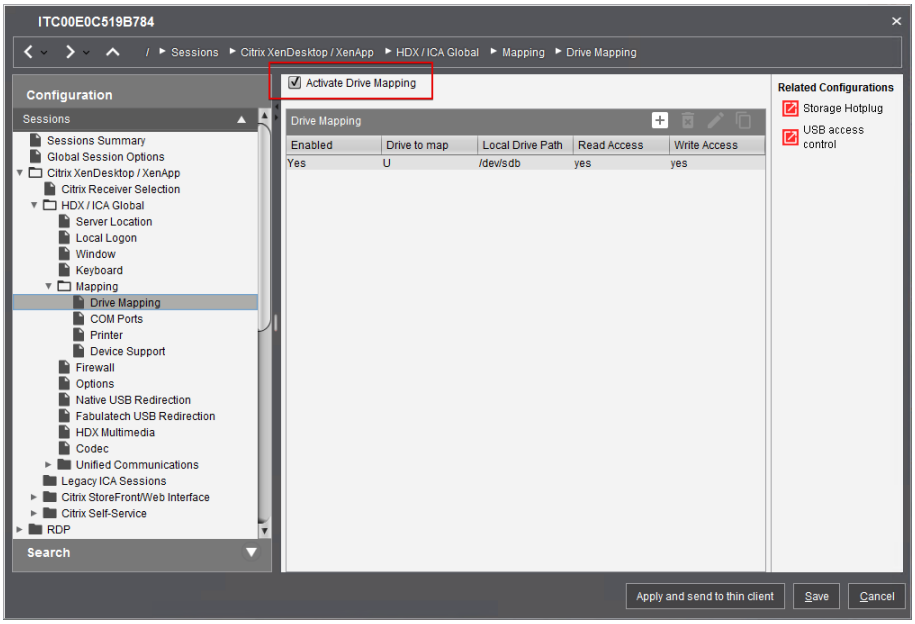
There you can also switch between the two methods by clicking on "Switch to generic" (or "Switch to optimized").

The "Optimized" variant uses Citrix's own protocol to provide a virtual network drive in the user's virtual desktop:



From the user's perspective, the drive appears in the session as a "Removable Disk" with the addition "Drive letter on Thinclient-Name". Technically, this is a virtual network drive, a so-called client drive mapping.

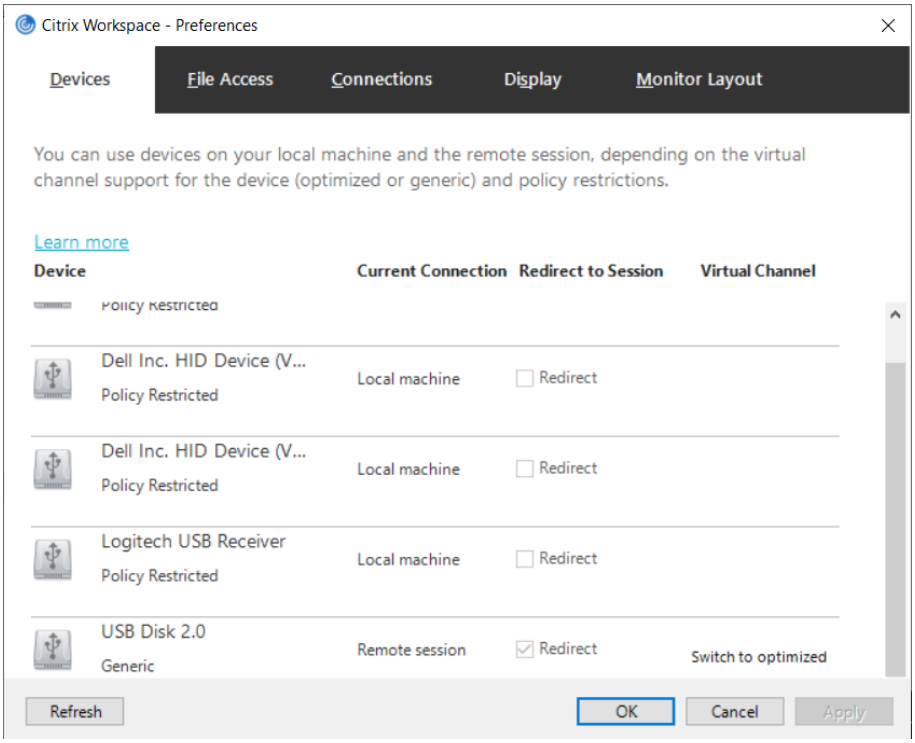
Settings can also be made via the administration interface of the thin client manufacturer for the thin clients (e.g. in Igel UMS):



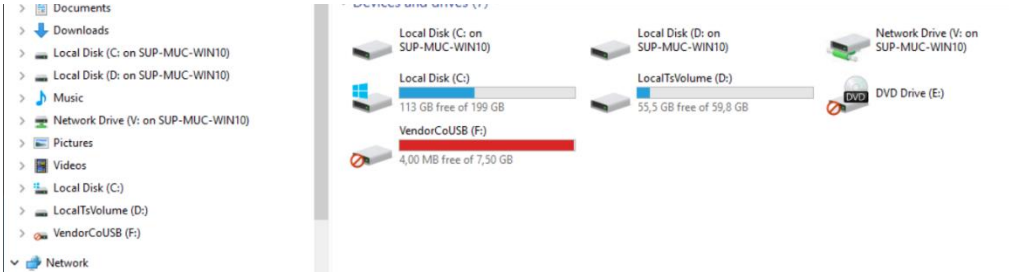
With this type of drive sharing, there are various technical restrictions, such as a maximum file size and a maximum size of the entire data carrier, which vary depending on the version of Citrix Workspace or Citrix Receiver and the version of the server software. These restrictions are documented on the Citrix website. The advantage of sharing drives in this way is that files can be accessed quickly, and any network latency (delays) are practically irrelevant.

1.1.2 USB Redirection

The second method of sharing is called "Generic" by Citrix and is also displayed accordingly in Citrix Workspace:



This variant is a so-called USB forwarding, i.e. the network cable acts as a (very) long USB cable and the USB device is connected directly to the server with the help of the Citrix software. As a result, it is also visible in the Windows device manager and behaves like a USB stick connected to a Windows PC from the user's perspective.

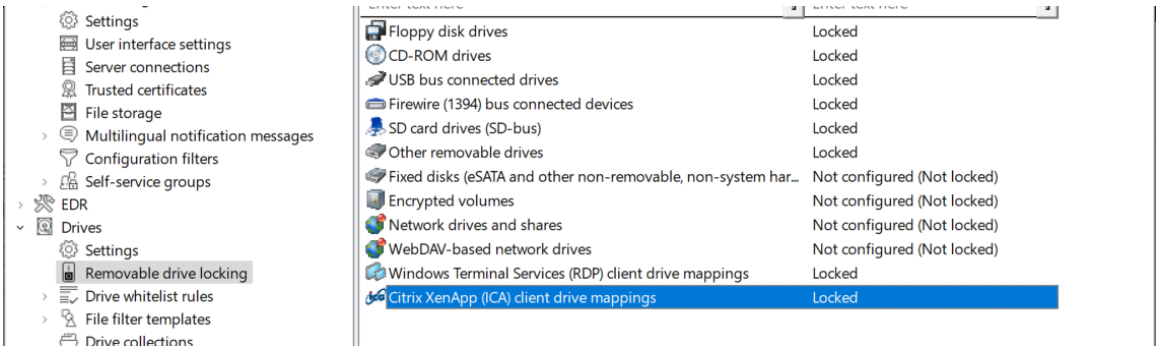


2.2. The DriveLock view

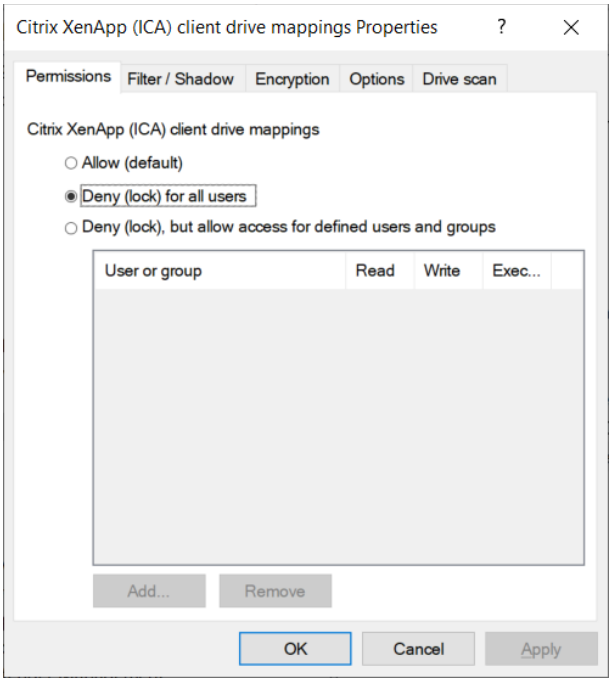
DriveLock can handle both ICA client drive mapping and USB redirection and lock or unlock drives accordingly. However, as these are different technologies, control within the DriveLock policy takes place in different places with different whitelist rules.

Drives that are connected using the "Generic" method are treated as "normal" USB devices from DriveLock's point of view and controlled accordingly.

Drives that are connected via the "Optimized" method are not USB devices as such, but are controlled in DriveLock via the device category "Citrix XenApp (ICA) client drive mappings" (or "Windows Terminal Services (RDP) client drive mappings" if the RDP protocol is used):

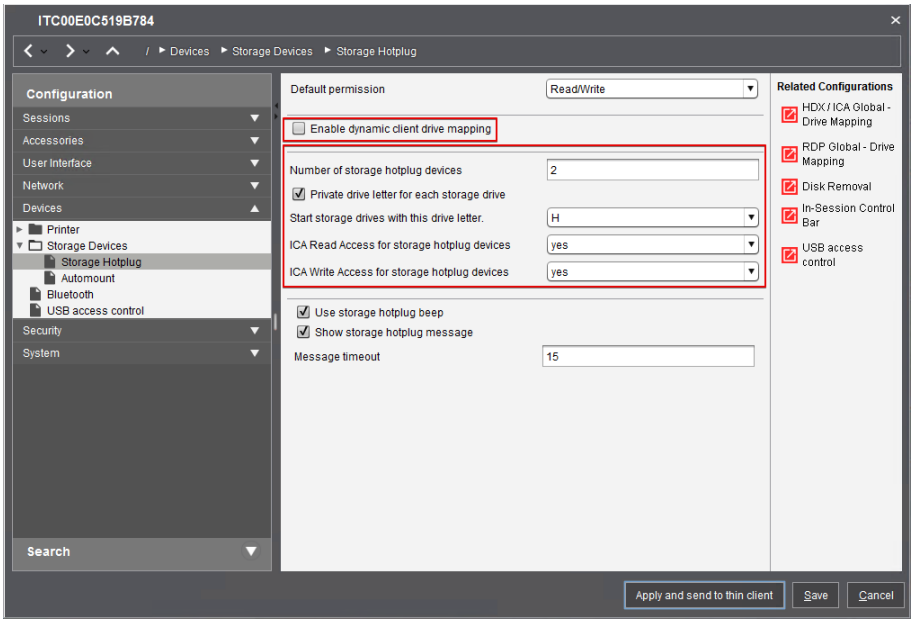


Under "Removable drive locking", the default status for these drives can be set as usual:

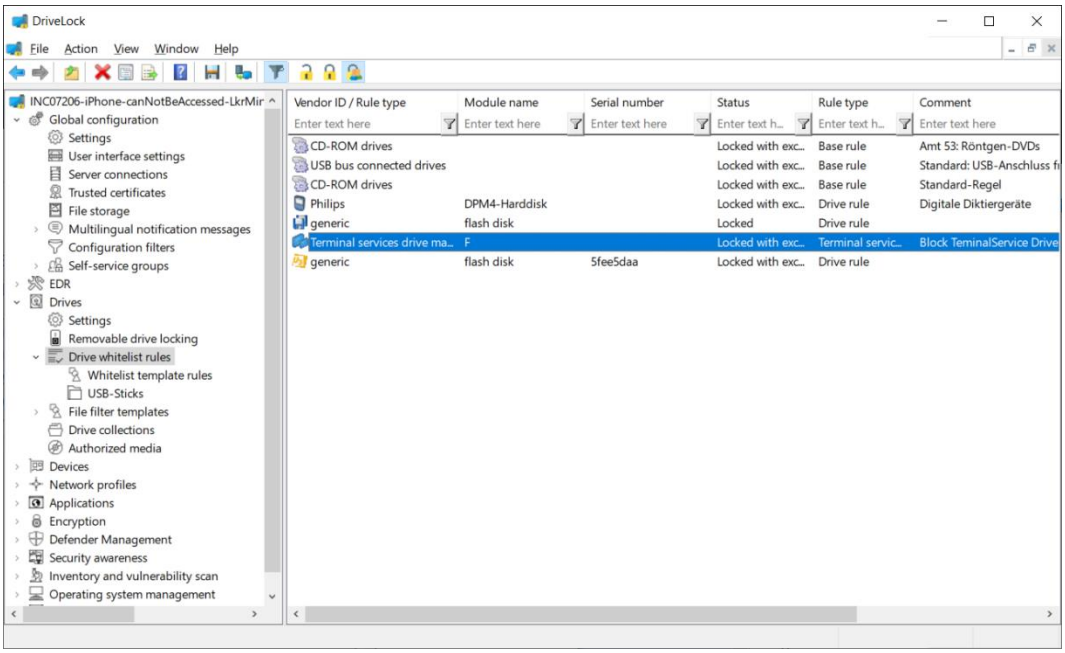


There is an important difference here compared to "normal" USB sticks: the "Optimized" protocol does not know any hardware data. This means that - as this is not provided for in the ICA protocol specification - there is no information about which specific USB stick is hidden behind such a drive. This is remedied by the "DriveLock Virtual Channel" (described in section 2.3 described in more detail).

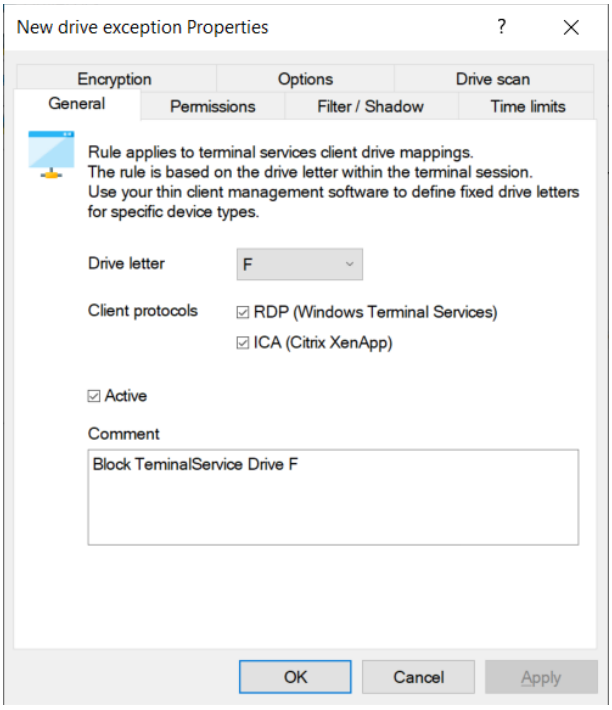
If no Virtual Channel is in use, exceptions can therefore only be released using the ICA drive letter, which can usually be specified by the thin client administration software:



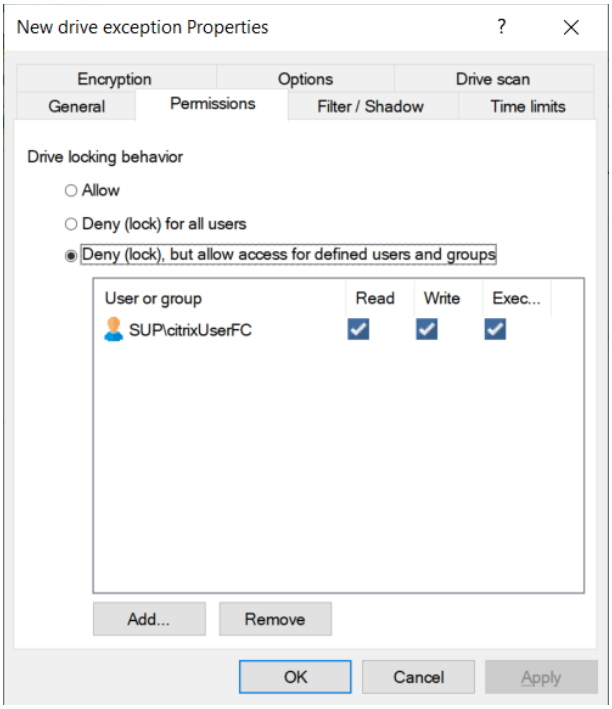
A "Terminal services drive mapping rule" is the correct type of drive rule for such an exception in the DriveLock policy.



The usual options for whitelist rules can be set there, but the rule is not identified by vendor and product ID, but by protocol and virtual drive letter:



The remaining settings correspond to the options given in other rules, e.g. you can authorize certain users (groups) to access such a drive:

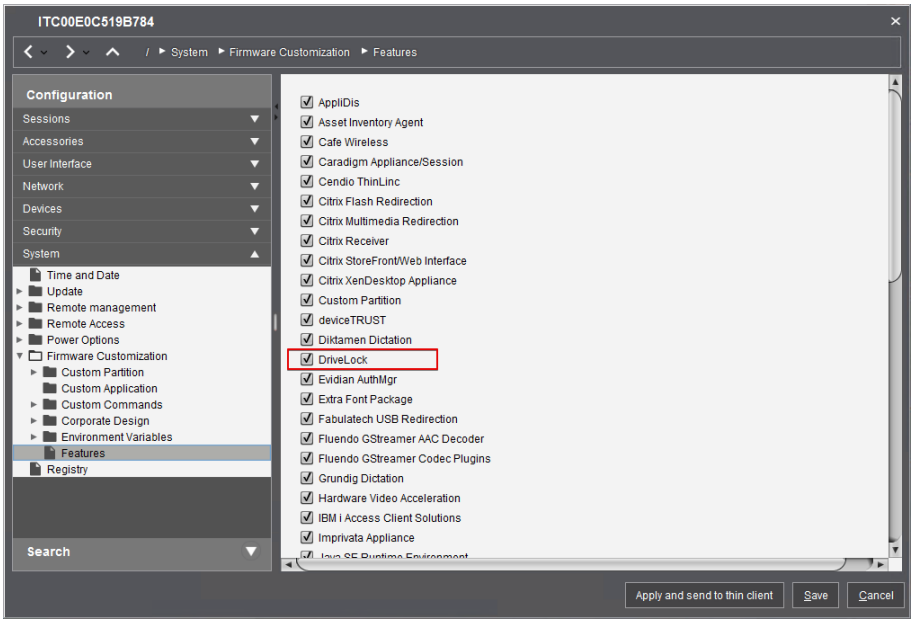


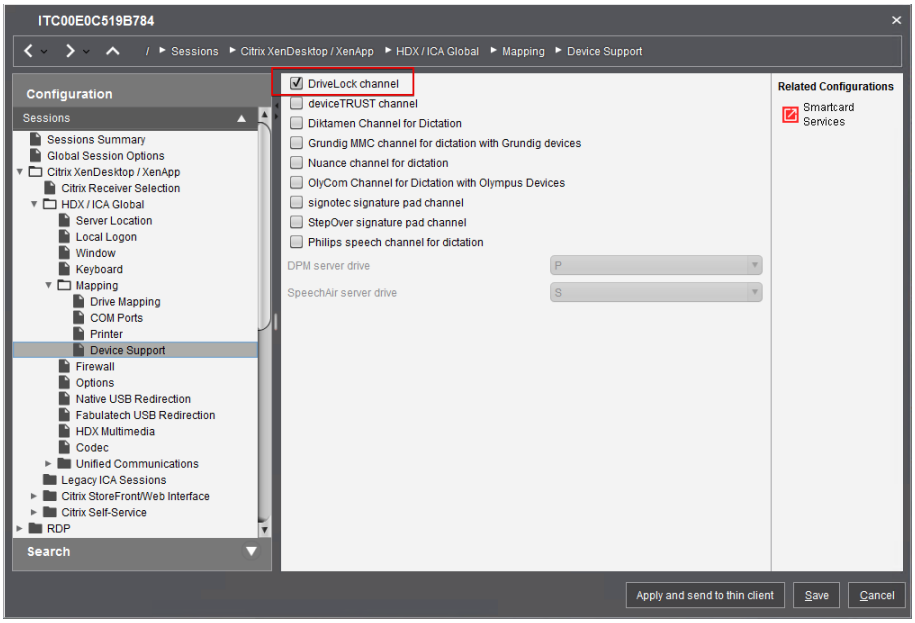
2.3. DriveLock Virtual Channel

As explained above, the "Optimized" protocol does not allow the transfer of hardware data. The DriveLock Virtual Channel was developed to enable this data to be identified anyway. This Virtual Channel is software that runs on the thin client, collects the required hardware data there and transmits it to the server (within a so-called "Virtual Communication Channel" in the ICA protocol - hence the name).

This enables the DriveLock agent to recognize which hardware belongs to which drive letter within an ICA session.

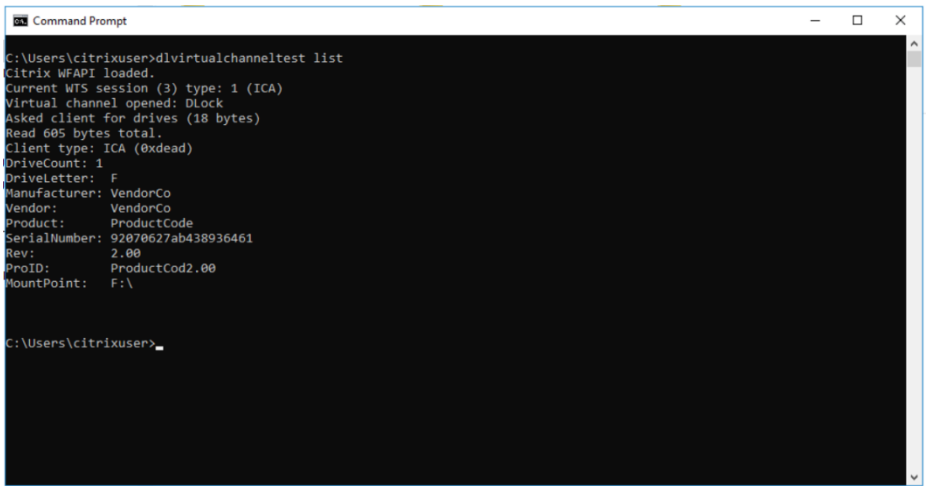
The DriveLock Virtual Channel is already pre-installed on IGEL devices or in IgelOS and only needs to be activated via the IGEL administration interface.





It is available for download for Windows-based thin clients. For other thin clients, please contact the thin client manufacturer.

To test the availability of the Virtual Channel, connect to the server in an ICA session. Then connect a USB device to the thin client and open a command prompt in the ICA session. Executing the command "dlvirtualchanneltest list" displays the hardware data that was transmitted using the Virtual Channel.

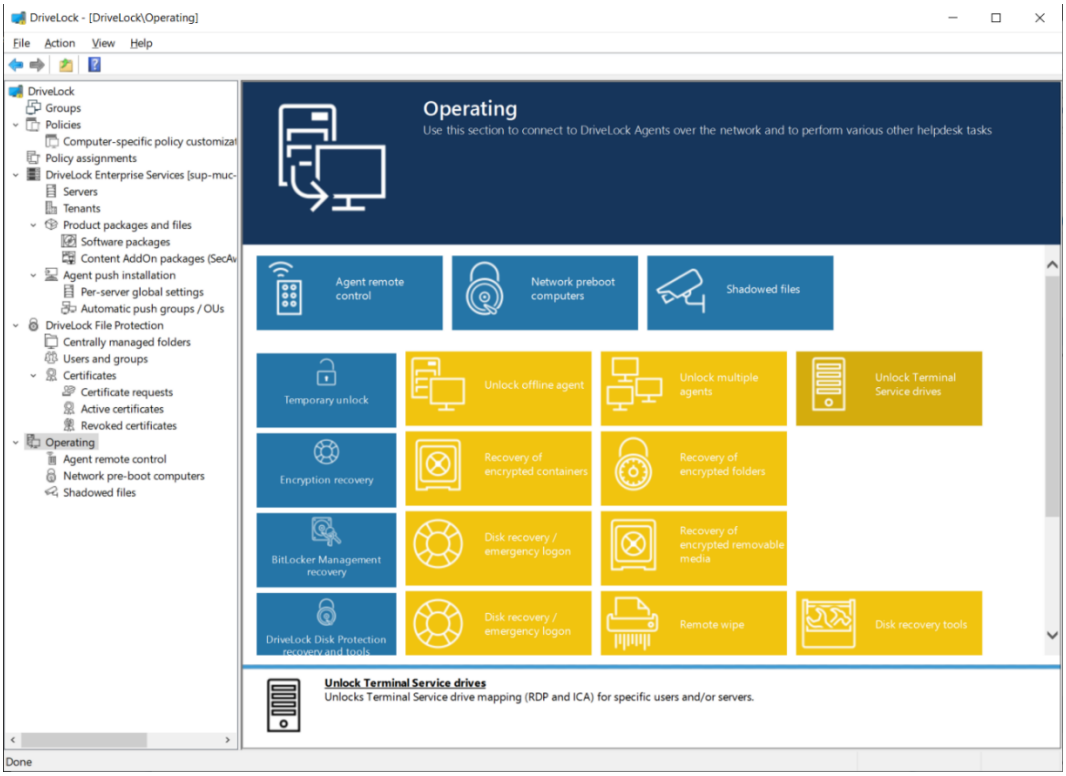


If the Virtual Channel is set up correctly, "normal" USB whitelist rules can also be used for ICA file redirection within the DriveLock policy. Devices are then released based on the transmitted hardware data.

If the Virtual Channel is not available, it can only be shared via the drive letter.

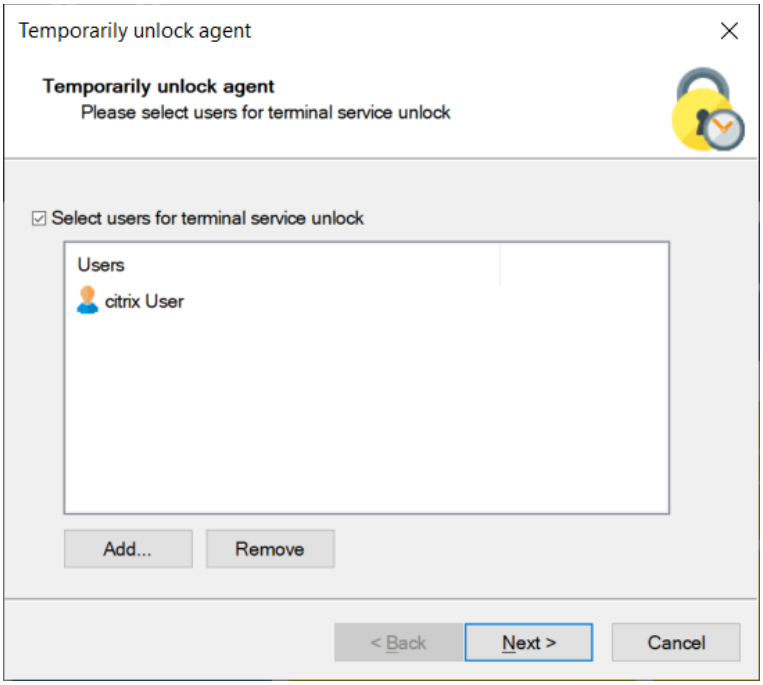
3. Temporary sharing of USB drives

An additional function for temporary device release is available in DriveLock for terminal servers: "Unlock Terminal Services drives".

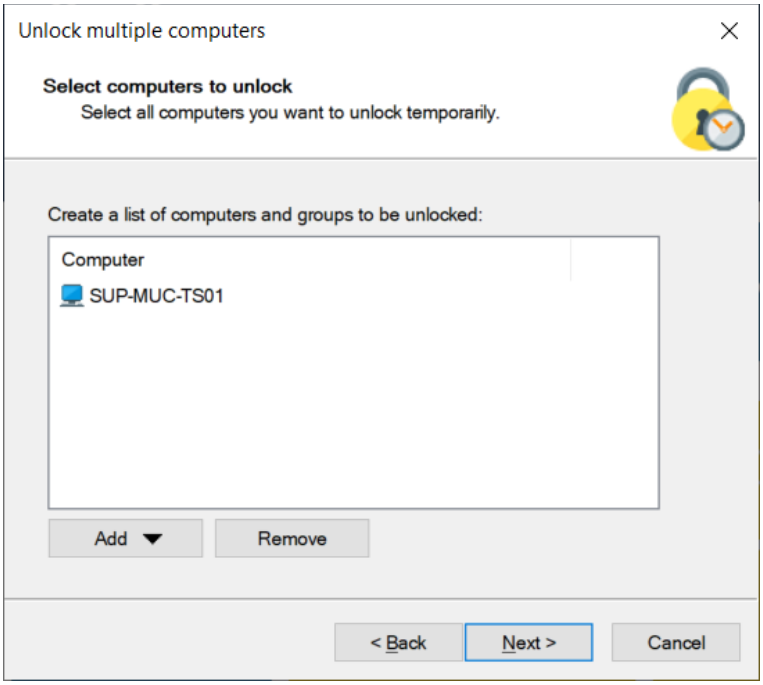


Using this function, it is possible to make a release on the terminal server or a terminal server farm only for certain user sessions.

The user to be released is therefore first selected in the corresponding wizard:



Then select the Citrix server(s). This setting is saved so that you only have to select all servers in the farm once.



After selecting the other options and the duration of the release, sessions of the selected user are searched for on all servers and these are temporarily released. This means that the user

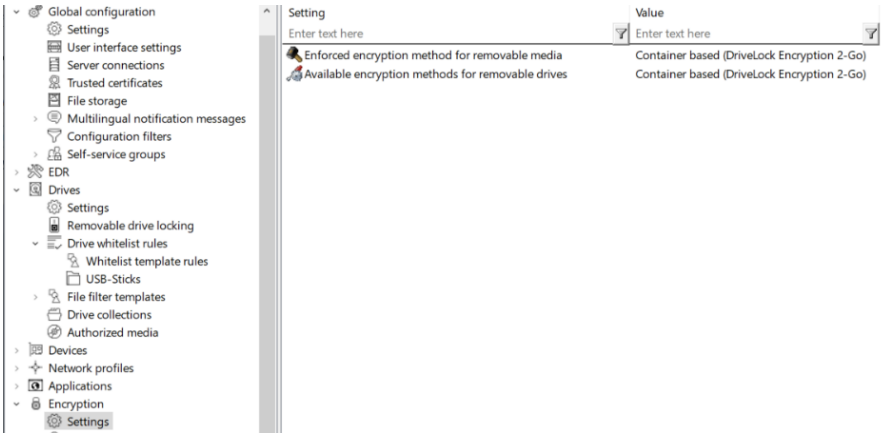
can then use USB drives within their session, for example. However, the share does not apply to other users who are currently logged on to the server.

4. Encryption of external USB drives

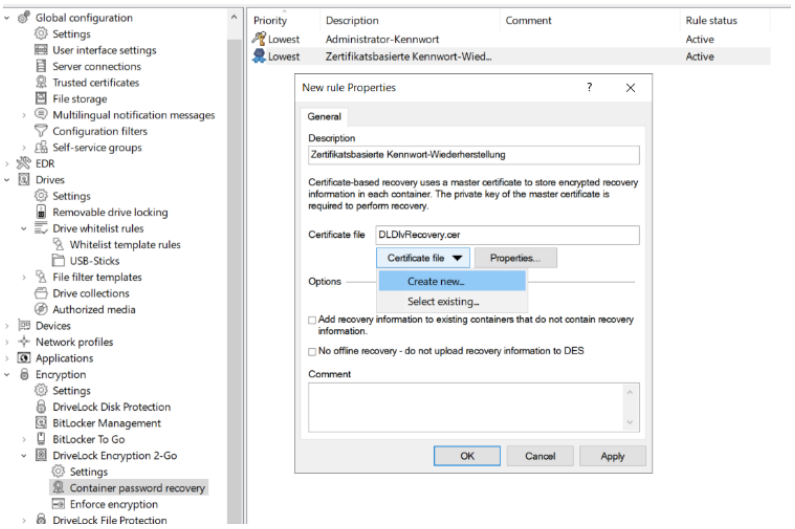
If you use "Generic", the encryption of drives with all features works in the same way as on a local computer (since the drive is "normally" available under Windows).

If you use "Optimized", there are some technical restrictions for manual encryption. However, automatic encryption works as usual.

Necessary settings for this:

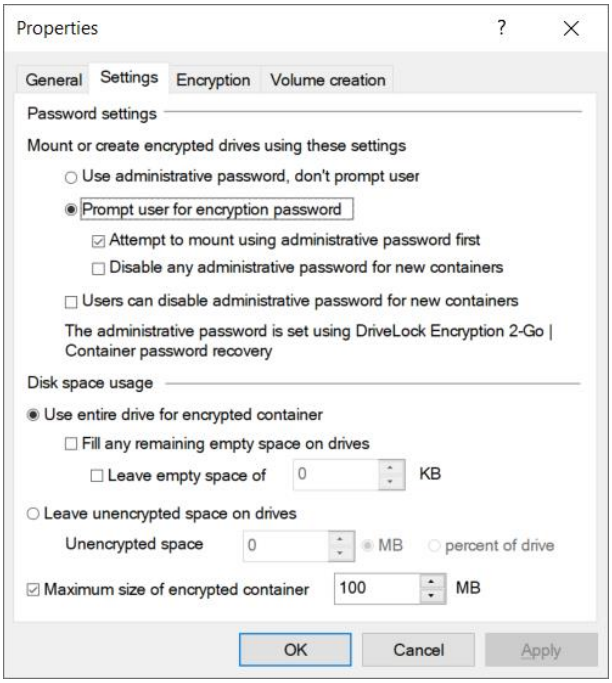


Select encryption type: only "Container-based" should be available.

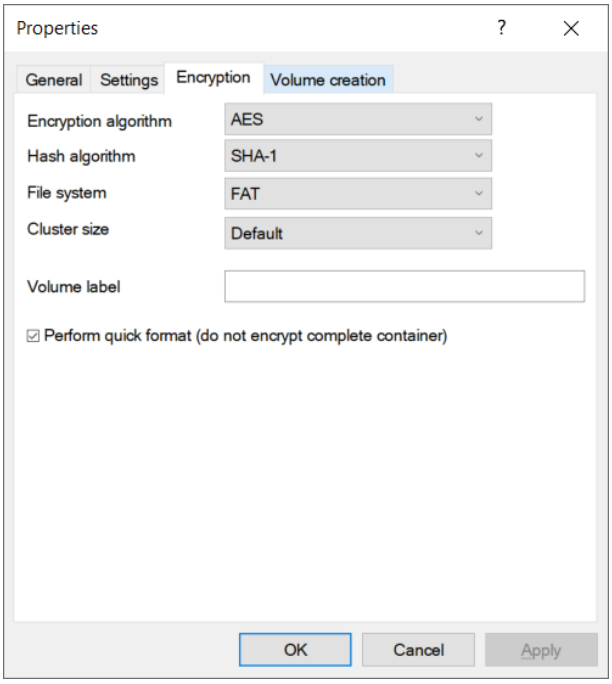


Create recovery information for container encryption.

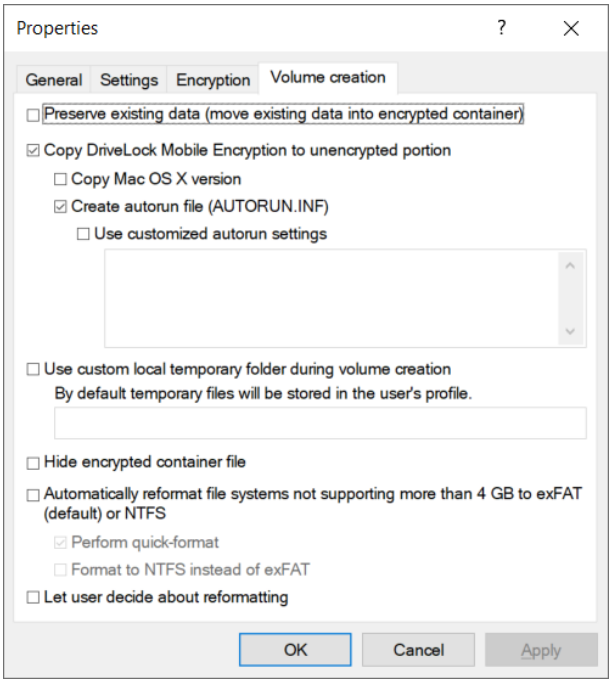
Edit the settings under "Enforced encryption". The following settings are recommended:



The maximum container size can be set if there are restrictions for the thin clients or ICA protocols/Citrix receivers used. The usual ICA restrictions (2 or 4 GB maximum file size) are known to the DriveLock agent.

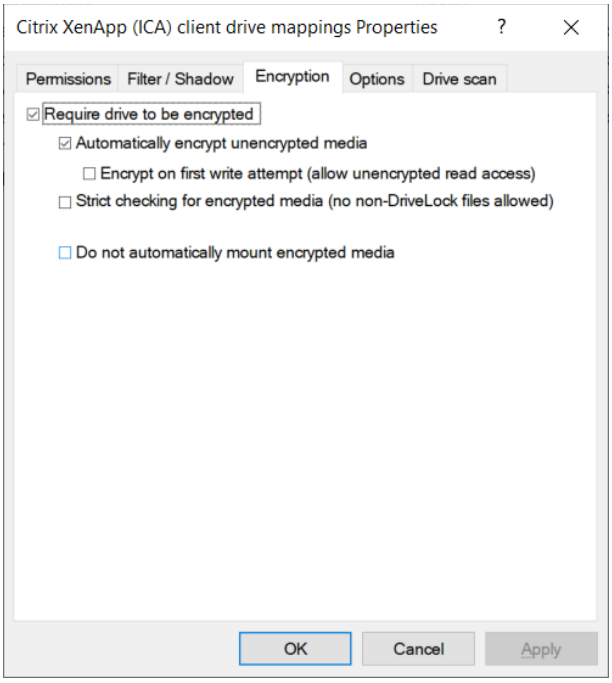


Quick Format should be selected, otherwise the initial encryption will take a very long time. IGEL thin clients can be accelerated here via the DriveLock Virtual Channel.

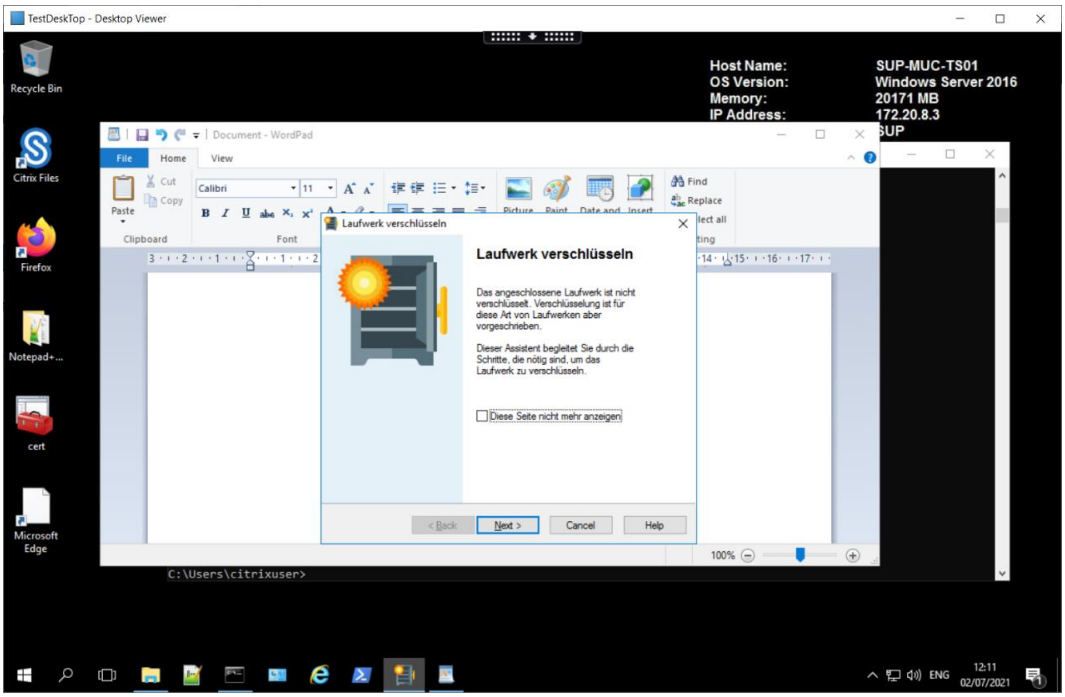


Existing data should not be saved if possible (for performance reasons). Copying large amounts of data using the ICA Optimized method is not very performant.

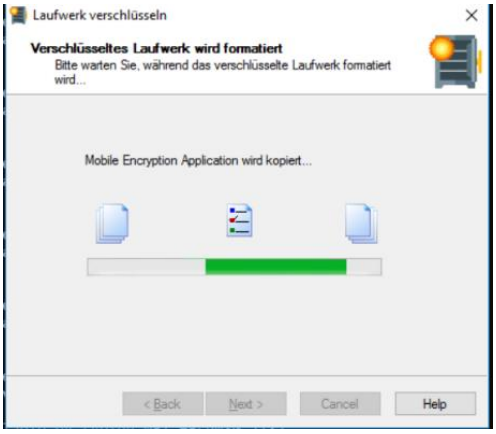
Once these settings have been made, the default state for forced encryption can be set under "Removable drive locking" - as usual:



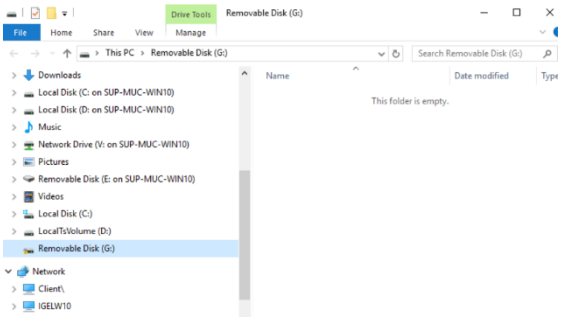
In the ICA session, this then looks as usual:



...

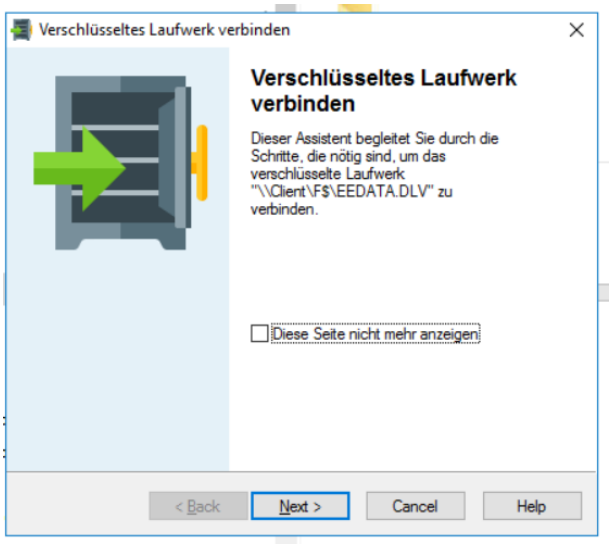


...



At the end, you have connected a new encrypted drive in the ICA session.

If you then connect the drive to another ICA session, the mount dialog also appears:



Please note that, depending on the ICA receiver/Citrix workspace used, you sometimes have to click on the client drive mapping for the mount or create dialog to appear. This problem does not normally occur with thin clients, but it does occur with some versions of Windows.

5. Further information

Further technical articles and white papers as well as the complete documentation of the DriveLock Zero Trust platform are available at https://drivelock.help.