

# DriveLock and Thin Clients

# USB drive control in Citrix environments



#### CONTENTS

1.	Introduction	2
2.	USB drive control in Citrix environments	2
2.1.	The Citrix view	.2
2.2.	The DriveLock view	.6
2.3.	DriveLock Virtual Channel	10
3.	Temporary sharing of USB drives	12
4.	Encryption of external USB drives	14
5.	Further information	19

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).



ITC00E0C519B784				>
✓ ✓ ✓ ✓ ✓ / ► Sessions ► Citrix Xer	n Desktop / Xen App 🕨 HDX / IC	A Global 🕨 Native USB Redire	ection	
Configuration	Enable native USB Redire	ction		
Sessions	Default rule		Allow	Ŧ
Global Session Options	Class Rules			🕂 🖬 🖊 🗋
Cltrix XenDesktop / XenApp     Cltrix XenDesktop / XenApp     Cltrix Receiver Selection     FHOX / ICA Global     Server Location     Local Logon     Window	Rule	Class ID	Name	
► Keyboard ► Mapping	Device Rules			🗄 🗟 🖊 🗋
Firewall  Options  Native USB Redirection  Fabulatch USB Redirection  HDX Multimedia  Codec  United Communications  Legacy ICA Sessions  Critix Self-Service  Critix Self-Service  Critics Client  Appliance Mode  Caradigm  Leostream  Search	Rule	Vendor iD	ProductID	Name
			Apply and send to th	in client <u>S</u> ave <u>C</u> ancel

#### 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":

🌀 Citrix V	Vorkspace - P	references				×
<u>D</u> evi	ces	<u>F</u> ile Access	<u>C</u> onnections	Di <u>s</u> play <u>I</u>	<u>M</u> onitor Layout	
You ca channe	n use devic el support fo	es on your local r or the device (opt	nachine and the remo imized or generic) and	ote session, depe d policy restrictio	ending on the virtual ons.	
Learn r Device	Policy Kestr	ictea	Current Connection	Redirect to Sess	ion Virtual Channel	^
	Dell Inc. H Policy Restr	ID Device (V	Local machine	Redirect		
	Dell Inc. H Policy Restr	ID Device (V	Local machine	Redirect		
	Logitech l Policy Restr	JSB Receiver icted	Local machine	Redirect		
	USB Disk a	2.0	Local machine Remote session	✓ Redirect	Switch to generic	
Refre	sh			OK	Cancel App	ply



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:

👌 Music	DriveLock Mobile.app	23/01/2020 13:46	File folder
📮 SharE	DLMobile	06/12/2019 17:50	Application
Videos	TestMobileApp1.txt	06/05/2021 15:39	Text Document
📃 This PC			
> 🔜 Desktop			
Documents			
Downloads			
Local Disk (C: on SUP-MUC-WIN10)			
Local Disk (D: on SUP-MUC-WIN10)			
h Music			
Network Drive (V: on SUP-MUC-WIN10)			
Pictures			
Removable Disk (F: on SUP-MUC-WIN10)			
🙀 Videos			
> 🚘 LocalTsVolume (D:)			

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):

ITC00E0C519B784						×
	nDesktop / XenApp	HDX / ICA Glob	al 🕨 Mapping 🍽 I	Drive Mapping		
Configuration Sessions Clobal Session Options Clobal Session Options Clobal Session Options Clobal Session Options Clobal Senser Detection Clobal Senser Location Clobal Senser Location Clobal Senser Location Clobal Clobal Senser Location Clobal Clobal Clobal Senser Clobal Senser Clobal Senser Clobal Section Clobal Secti	Activate Drive     Drive Mapping     Enabled     Yes	Mapping Drive to map U	Local Drive Path /dev/sdb	yes	Virte Access yes	Related Configurations Storage Hotplug USB access control
				Apply	y and send to thin clier	t <u>S</u> ave <u>C</u> ancel



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:

🎯 Citrix V	Vorkspace - Preferences				×
<u>D</u> evic	es <u>F</u> ile Access	<u>C</u> onnections	Di <u>s</u> play <u>M</u> oni	itor Layout	
You ca channe	n use devices on your local r el support for the device (opt	nachine and the remo imized or generic) and	ote session, dependin d policy restrictions.	g on the virtual	
Learn r Device	Policy Restricted	Current Connection	Redirect to Session	Virtual Channel	~
1.00 A	Dell Inc. HID Device (V Policy Restricted	Local machine	Redirect		
100 m	Dell Inc. HID Device (V Policy Restricted	Local machine	Redirect		
100 A	Logitech USB Receiver Policy Restricted	Local machine	Redirect		
12	USB Disk 2.0 Generic	Remote session	✓ Redirect	Switch to optimized	
Refres	sh		OK	Cancel Apply	

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.



> 😰 Documents	· Derices and arres (7)		
> 🕹 Downloads	Local Disk (C: on	Local Disk (D: on	Network Drive (V: on
Local Disk (C: on SUP-MUC-WIN10)	SUP-MUC-WIN10)	SUP-MUC-WIN10)	SUP-MUC-WIN10)
> Local Disk (D: on SUP-MUC-WIN10)	Local Disk (C:)	LocalTsVolume (D:)	
> 🁌 Music	113 GB free of 199 GB	55.5 GB free of 59.8 GB	DVD Drive (E:)
> 🛫 Network Drive (V: on SUP-MUC-WIN10)	VendorCoUSB (E)		
> 📰 Pictures			
> 🔛 Videos	4,00 MB free of 7,50 GB		
> 🏪 Local Disk (C:)			
> 👝 LocalTsVolume (D:)			
> 👧 VendorCoUSB (F:)			
✓ → Network			

#### 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):

Settings.		
Settings	🖬 Floppy disk drives	Locked
Service settings	OCD-ROM drives	Locked
Server connections     Trusted certificates	✓ USB bus connected drives	Locked
	🚍 Firewire (1394) bus connected devices	Locked
Image     I	👼 SD card drives (SD-bus)	Locked
	The removable drives	Locked
	Fixed disks (eSATA and other non-removable, non-system har.	. Not configured (Not locked)
Service groups	Encrypted volumes	Not configured (Not locked)
<ul> <li>         Image: A state of the state of t</li></ul>	Setwork drives and shares	Not configured (Not locked)
Settings	WebDAV-based network drives	Not configured (Not locked)
Removable drive locking	Windows Terminal Services (RDP) client drive mappings	Locked
> Drive whitelist rules	Citrix XenApp (ICA) client drive mappings	Locked
> 🖄 File filter templates		
Drive collections		

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



Citrix Xen/	App (ICA) client	drive mapping	gs Proper	ties	?	×
Permission	Filter / Shado	w Encryption	Options	Drive sca	an	
Citrix Xen/ O All © De	App (ICA) client dr ow (default) eny (lock) for all us eny (lock), but allo	rive mappings sers w access for def	ined users	and group	os	
[	User or group		Read	Write	Exec	
	Add	Remove				
		OK	Ca	ancel	Арр	ły

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:



ITC00E0C519B784					×
✓ ✓ ✓ ✓ ✓ / ► Devices ► Storage D	evices 🕨 Storage Hotplug				
Configuration       Sessions       Accessories       User Interface       Network       Devices       Storage Devices       Storage Hotplug       Automount       Bluetooth       Security       System	Lence → Course + Coping     Default permission     Enable dynamic client drive mapping     Number of storage hotplug devices     I' Private drive letter for each storage drive     Start storage drives with this drive letter.     ICA Read Access for storage hotplug devices     I'A Write Access for storage hotplug message     Message timeout	ReadWrite       2       H       yes       yes       15	v           v           v           v           v	Related Config HDX/ICA Drive Map RDP Glob Mapping Polsk Rem Bar USB acce control	urations Global - Jing al - Drive oval n Control SS
			Apply and send to thin clien	t <u>S</u> ave	<u>C</u> ancel

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

📢 DriveLock						0 <b>—</b> 0		>	×
🚅 Eile Action View Window Help								- 6	×
♦ ♦ 2 × □ ► 2 H ► ▼	🔒 🔒 🚨								
<ul> <li>INCO7206-iPhone-canNotBeAccessed-LkrMir</li> <li>Global configuration</li> <li>Settings</li> <li>User interface settings</li> <li>Server connections</li> <li>Trusted certificates</li> <li>File storage</li> <li>Multilingual notification messages</li> <li>Multilingual notification messages</li> <li>Multilingual notification</li> <li>Self-service groups</li> <li>Settings</li> <li>Removable drive locking</li> <li>Drive shitelist rules</li> <li>Multilingual</li> <li>Whitelist rules</li> <li>Multilingual</li> <li>Whitelist rules</li> <li>Multilingual</li> <li>Settings</li> <li>Removable drive locking</li> <li>Drive shitelist rules</li> <li>Multilingual</li> <li>Multilingual</li> <li>Multilingual</li> </ul>	<ul> <li>a a a a a a a a a a a a a a a a a a a</li></ul>	Module name Enter text here Ves DPM4-Harddisk flash disk flash disk	Serial number          Image: Serial number         Image: Serial number         Image: Serial number         Sfee5daa	Status Enter text h. Locked with exc Locked with exc Locked with exc Locked with exc Locked with exc	Rule type Enter text h_ \[ Base rule Base rule Drive rule Terminal servic- Drive rule	Comment Enter text Amt 53: R Standard: Standard Digitale D Block Tem	t here jöntgen USB-A Regel jiktiergu	-DVDs nschlu eräte vice D	s uss fi
Pill     Devices       →     Network profiles       ③     Applications       ○     B Encryption       >     ⊕       Defender Management       >     ∰ Security awareness       >     ½ Inventory and vulnerability scan       >     ⊖       ⊖     Operating system management	4								
								_	-

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:



New drive exc	eption Pro	perties			?	×
Encrypt General	Encryption Options			Drive sca Tim	an e limits	
Rule a The ru Use y for spi	rminal serv on the driv nt manage types.	vices client ve letter wit ment softv	drive mappi thin the term vare to defir	ings. ninal sessio ne fixed dri	on. ve letters	
Drive	letter	F	~			
Client	protocols	⊠ RDF ⊡ ICA	? (Windows (Citrix Xen	s Terminal S App)	Services)	
⊠ Acti Comr	ve nent					
Block	TeminalSer	vice Drive	F			
			OK	Cape		Apply
			OK	Cance		Apply

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

New drive exc	eption Pro	perties				?	$\times$
Encryp	ion	C	Options		Dr	ive scan	
General	ral Permissions Filter / Shadow				Time lin	nits	
Drive locking b	ehavior						
⊖ Allow							
⊖ Deny	lock) for all u	users					
Deny	ock), but all	ow access	for defin	ed users	s and grou	ups	
Us	er or group			Read	Write	Exec	
2	SUP\citrixUserFC					~	
	Add	Remo	ove				
		(	ОК	С	ancel	App	ply



#### 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.





ITC00E0C519B784			×
	enDesktop / XenApp 🕨 HDX / ICA Global 🕨 Mapping	g 🕨 Device Support	
Configuration Sessions Sessions Summary Global Session Options Citrix Receiver Selection Citrix Receiver Selection Citrix Receiver Selection Citrix Receiver Selection Citrix Receiver Selection Citrix Receiver Selection Citrix Receiver Selection Com Porte Printer Device Support Frewall Options Native USB Redirection Fabulach USB Redirection HDX Multimedia Code United Communications Legacy ICA Sessions Citrix Self-Service Citrix Self-Service Citrix Self-Service	DriveLock channel     deviceTRUST channel     Diktamen Channel for Dictation     Grundig MMC channel for dictation with Grundig     Nuance channel for dictation     O(Com Channel for Dictation with Olympus Dec     signotec signature pad channel     StepOver signature pad channel     Philips speech channel for dictation     DPM server drive     SpeechAir server drive	devices Aces P y S y	Related Configurations Smartcard Services
		Apply and send to thin clies	nt <u>S</u> ave <u>C</u> ancel

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:



Temporarily unlock agent			×				
Temporarily unlock agent Please select users for terminal service unlock							
☑ Select users for terminal service unk	ock						
Users							
💄 citrix User							
Add Remove							
	< <u>B</u> ack	<u>N</u> ext >	Cancel				

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

#### in the farm once.

Unlock multiple computers		×
Select computers to unlock Select all computers you want	to unlock temporarily.	R
Create a list of computers and gro	ups to be unlocked:	
Computer		
General SUP-MUC-TS01       Add ▼		
	< <u>B</u> ack <u>N</u> ext >	Cancel

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:

roperties					?	×
General Settings	Encryption	Volum	e creation			
Password settings	-					
Mount or create en	crypted drives	s using th	ese settings	8		
⊖ Use admin	istrative passv	vord, dor	n't prompt us	er		
Promot use	ar for encountin	n nacew	ord			
	t to mount up	ing admit		award fire		
	any administ	rative pa	seword for p	ew conta	iners	
		iauve pa	SSWOID IDI II	ew conta	iners	
Users can	disable admin	istrative p	bassword for	new con	tainers	
The administr Container pas	ative passwo ssword recove	rd is set u ery	using DriveLo	ock Encry	ption 2-G	0
Disk space usage	-					
Use entire drive	for encrypted	containe	r			
🗌 Fill any rem	aining empty	space or	n drives			
🗆 Leave e	empty space of	of 0	-	KB		
	ted space on	drives				
Leave unencrypt	ten opene en	anvoo				
⊖ Leave unencrypt Unencrypted	space 0	anves	* ® MB	⊖ per	cent of dr	ive
○ Leave unencrypt Unencrypted ☑ Maximum size o	space 0	ontainer	‡ ◎ MB 100	⊖ per	cent of dr B	ive

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.

Properties				1	?	×
General Settings E	ncryption	Volume creation	on			
Encryption algorithm	AES	6		$\sim$		
Hash algorithm	SH	<del>\</del> -1		~		
File system	FAT			~		
Cluster size	Def	ault		~		
Volume label						
Perform quick format	t (do not e	ncrypt complete	container)			
		OK	Cancel		Арр	ly



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.

Propertie	s				?	×
General	Settings	Encryption	Volume creation	on		
Preser	ve existing	data (move e	existing data into	encrypted	container)	
☑ Copy	DriveLock N	Nobile Encryp	tion to unencry	ted portion	1	
	opy Mac OS	S X version				
⊡ Cr	eate autoru	ın file (AUTO	RUN.INF)			
	Use custo	mized autoru	n settings			
						^
						~
□ Use α	ustom local	temporary fo	lder during volu	me creation	1	
By d	efault temp	orary files wil	be stored in the	e user's prot	file.	
🗆 Hide e	encrypted co	ontainer file				
□ Autom (defau	natically refo lt) or NTFS	ormat file syst	ems not suppor	ting more th	nan 4 GB to e	exFAT
⊡ Pe	erform quick	-format				
- Fo	rmat to NT	FS instead of	f exFAT			
□ Let us	er decide a	bout reforma	tting			
			OK	Cancel	Ap	ply

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:



Citrix XenApp (ICA) client drive mappings Properties $\qquad ? \qquad \times$								
Permissions Filter / Shadow Encryption Options Drive scan								
☑ Require drive to be encrypted								
Automatically encrypt unencrypted media								
□ Encrypt on first write attempt (allow unencrypted read access)								
□ Strict checking for encrypted media (no non-DriveLock files allowed)								
Do not automatically mount encrypted media								
OK Cancel Apply								

In the ICA session, this then looks as usual:



•••



Laufwerk verschlüsseln Verschlüsseltes Laufwerk wire Bite waten Sie, während das v wird	<b>d formatiert</b> verschlüsselte La	aufwerk formatiert	×	
Mobile Encryption Applica	ation wird kopiert	***		
	E			
< <u>B</u> ack	Next >	Cancel	Help	
File Home Share View Manage	Removable Disk (G:		- L	× L
← → · · · ↑ → This PC → Removable Disk (	(G:)	× õ	Search Removable Disk (G	c) _0
> ↓         Devenloads           > ↓         Load Disk (C: on SUP-MUC-VIN10)           > ↓         Maxie           > ↓         Load Disk (C: ()           > ↓         Load Disk (C: ()	• Name	↑ This folde	Date modified	Туре

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:

Verschlüsseltes Laufwerk ve	erbinden	×
	Verschlüsseltes Laufwerk verbinden Dieser Assistent begleitet Sie durch die Schritte, die nötig sind, um das verschlüsselte Laufwerk "\Client\F\$\EEDATA.DLV" zu verbinden.	
< <u>B</u> ack	Next > Cancel Help	



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 <u>https://drivelock.help.</u>



#### Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2024 DriveLock SE. All rights reserved.

DriveLock and others are either registered trademarks or trademarks of DriveLock SE or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.