

DriveLock und Thin Clients

USB-Laufwerkskontrolle in Citrix-Umgebungen





INHALT

1.	Einleitung	2
2.	USB-Laufwerkskontrolle in Citrix-Umgebungen	2
2.1.	Die Citrix-Sicht	2
2.2.	Die DriveLock-Sicht	6
2.3.	DriveLock Virtual Channel	
3.	Temporäre Freigabe von USB-Laufwerken	
4.	Verschlüsselung von externen USB-Laufwerken	
5.	Weiterführende Informationen	



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

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).



ITC00E0C519B784				>
✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	nDesktop / XenApp 🕨 HDX / IC	A Global 🕨 Native USB Redir	ection	
Configuration	Enable native USB Redire	ection		
Sessions	Default rule		wollA	٣
Global Session Options	Class Rules			8 6 / 0
Citrix XenDesktop / XenApp Citrix XenDesktop / XenApp HDX / ICA Global Server Location Local Logon Window	Rule	Class ID	Name	
► Keyboard ► Mapping	Device Rules			🗄 🖻 🗡 🗋
FireWall Options Natve USB Redirection Fabulach USB Redirection HDX Multimedia Codec United Communications Legacy ICA Sessions Cirk: StorFontWeb Interface Cirk: Set/Service RDP Horizon Client Appliance Node Caradigm Leostream Search	Rule	Vendor ID	ProductID	Name
			Apply and send to thi	n client <u>S</u> ave <u>C</u> ancel

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":

🌀 Citrix V	Vorkspace	e - Preferences				×			
<u>D</u> evic	es	<u>F</u> ile Access	<u>C</u> onnections	Di <u>s</u> play <u>M</u>	onitor Layout				
You can use devices on your local machine and the remote session, depending on the virtual channel support for the device (optimized or generic) and policy restrictions.									
Learn r Device	Policy R	estrictea	Current Connection	Redirect to Sessio	n Virtual Channel	^			
	Dell In Policy R	c. HID Device (V estricted	Local machine	Redirect					
	Dell Ine Policy R	c. HID Device (V estricted	Local machine	Redirect					
	Logited Policy R	ch USB Receiver estricted	Local machine	Redirect					
2 2 0 0	USB Di Optimiz	sk 2.0 ed	Local machine Remote session	Redirect	Switch to generic				
Refres	;h			OK	Cancel Ap	ply			



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:

Music SharE	DriveLock Mobile.app	23/01/2020 13:46 06/12/2019 17:50	File folder 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)				
> 👌 Music				
👳 Network Drive (V: on SUP-MUC-WIN10)				
> E Pictures				
Removable Disk (F: on SUP-MUC-WIN10)				
> 📕 Videos				
> LocalTsVolume (D:)				

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:

🎯 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>	onitor Layout	
You ca channe	n use devices on your local I support for the device (op	machine and the remo otimized or generic) an	ote session, depen d policy restriction	ding on the virtual ns.	
Learn r Device	nore Policy Kestricted	Current Connection	Redirect to Sessio	on Virtual Channel	^
1	Dell Inc. HID Device (V Policy Restricted	Local machine	Redirect		ł
₹ [™]	Dell Inc. HID Device (V Policy Restricted	Local machine	Redirect		
1	Logitech USB Receiver Policy Restricted	Local machine	Redirect		
\$	USB Disk 2.0 Generic	Remote session	Redirect	Switch to optimized	
Refres	h		OK	Cancel App	ly

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.



> 🔝 Documents	- Detrees 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-WINTO)
> 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)	VendorColISB (Fr)	33,3 60 1100 61 53,0 60	
> Fictures			
> 📓 Videos	4,00 MB free of 7,50 GB		
> 🏪 Local Disk (C:)			
> 👝 LocalTsVolume (D:)			
> 🔉 VendorCoUSB (F:)			
✓ 🥩 Network			

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):

1		Line cachee	
	Settings	Floppy disk drives	Locked
	User Interface settings	OCD-ROM drives	Locked
	Server connections	USB bus connected drives	Locked
	File storage	i Firewire (1394) bus connected devices	Locked
	File storage Multilingual potification messages	👼 SD card drives (SD-bus)	Locked
		The removable drives	Locked
	> CA Self-service groups	Fixed disks (eSATA and other non-removable, non-system har	Not configured (Not locked)
>	R EDR	Encrypted volumes	Not configured (Not locked)
v	Drives	Network 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
	> Trive whitelist rules	🚾 Citrix XenApp (ICA) client drive mappings	Locked
	> 🗟 File filter templates		
	Drive collections		

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



Citrix XenAp	p (ICA) client dr	ive mapping	s Propert	ties	?	\times				
Permissions	Filter / Shadow	Encryption	Options	Drive sca	an					
Citrix XenApp (ICA) client drive mappings Allow (default)										
U	ser or group		Read	Write	Exec					
	Add	Remove								
	[OK	Ca	incel	Арр	ly				

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:



ITC00E0C519B784			×
X Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y Y	evices 🕨 Storage Hotplug		
Configuration Sessions Accessories User interface Network Devices Storage Devices Storage Devices UsB access control Security System Secarch	Default permission Enable dynamic client drive mapping Number of storage holplug devices Private drive letter for each storage drive Start storage drives with this drive letter. ICA Read Access for storage holplug devices ICA Write Access for storage holplug devices ICA Write Access for storage holplug beep Show storage holplug message Message timeout	Read/Write 2 H yes yes 15	 Related Configurations HCX/ICA Global - Drive Mapping RDP Global - Drive Mapping Its Removal Its Removal Its Ression Control Bar USB access USB access
		Apply and send to thir	in client Save Cancel

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

📢 DriveLock						- 0	×
File Action View Window Help							×
	200						
🗢 🗠 🔽 🗙 🗉 🔄 🖪 🛏 😁 🚺	1 1 1 1 1 1						
📑 INC07206-iPhone-canNotBeAccessed-LkrMir ^	Vendor ID / Rule type	Module name	Serial number	Status	Rule type	Comment	
 Global configuration 	Enter text here	Enter text here	T Enter text here	Enter text h_ 7	Enter text h 🍸	Enter text here	
Settings	CD-ROM drives			Locked with exc.	Base rule	Amt 53: Röntge	n-DVDs
User interface settings	USB bus connected drives			Locked with exc	Base rule	Standard: USB-	Anschluss f
Server connections	CD-ROM drives			Locked with exc	Base rule	Standard-Rege	1
Trusted certificates	Philips	DPM4-Harddisk		Locked with exc	Drive rule	Digitale Diktier	geräte
File storage	generic	flash disk		Locked	Drive rule		,
Configuration filters	Terminal services drive ma	F		Locked with exc	Terminal servic	Block TeminalS	ervice Drive
Self-service groups	2 generic	flash disk	5fee5daa	Locked with exc	Drive rule		
> Service groups							
 © Drives 							
Settings							
Removable drive locking							
✓							
Whitelist template rules							
USB-Sticks							
> 🖄 File filter templates							
Drive collections							
④ Authorized media							
> 면 Devices							
> ** Network profiles							
> [G] Applications							
>							
P Defender Management							
D Inventory and yulperability scan							
> - Operating system management							
< > >	<						>

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:



New drive exce	ption Prop	perties				?	\times
Encryptic General	on Permis	C	ptions Filter /	Shade	D	rive sca) Time	n e limits
Rule ap The rule Use you for spec	oplies to ten e is based o ur thin clien cific device	minal serv on the driv t manage types.	ices client e letter wit ment softv	drive r hin the vare to	mappings e termina define f	s. Il sessio ixed driv	n. e letters
Drive le	tter	F	~				
Client p	orotocols	⊠ RDP ⊡ ICA	(Windows (Citrix Xen/	s Term App)	inal Serv	ices)	
⊠ Active Comme	e ent						
Block 1	TeminalSen	vice Drive	F				
		(ОК	С	ancel		Apply

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:

New drive exce	ption Properties				?	×	
Encryptio	Encryption Options Driv						
General	Permissions	Filte	r / Shade	wo	Time lim	nits	
Drive locking be	havior						
⊖ Allow							
⊖ Deny (lo	ck) for all users						
Deny (lo	ck), but allow acce	ess for defir	ned users	s and grou	lps		
User	or group		Read	Write	Exec		
💄 s	UP\citrixUserFC		✓	~	✓		
A	d Rei	move					
		OK	С	ancel	App	bly	



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:



Temporarily unlock agent			×
Temporarily unlock agent Please select users for terminal s	ervice unlock		R
Select users for terminal service unlo	ck		
Users			
🙎 citrix User			
Add Remove			
1	< <u>B</u> ack	<u>N</u> ext >	Cancel

Anschließend wählt man den oder die Citrix-Server. Diese Einstellung wird gespeichert, so dass

man hier nur einmalig alle Server der Farm auswählen muss.

Unlock multiple computers			×
Select computers to unlock Select all computers you want t	o unlock temporarily.		R
Create a list of computers and grou	ps to be unlocked:		
Computer			
SUP-MUC-TS01			
Add v Remove			
	< <u>B</u> ack	Next >	Cancel

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:

aral Settings Encryption Volume creation word settings Interpret of the settings Interpret of the settings Image: Use administrative password, don't prompt user Image: Prompt user for encryption password Image: Prompt user for encryption password Image: Prompt to mount using administrative password first Image: Disable any administrative password for new containers Image: Users can disable administrative password for new containers The administrative password is set using DriveLock Encryption Container password recovery space usage Image: entire drive for encrypted container	s ers
word settings	s ers
to or create encrypted drives using these settings Use administrative password, don't prompt user Prompt user for encryption password Attempt to mount using administrative password first Disable any administrative password for new containers Users can disable administrative password for new container. Users can disable administrative password for new container. The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container.	ers
 Use administrative password, don't prompt user Prompt user for encryption password ☑ Attempt to mount using administrative password first □ Disable any administrative password for new containers □ Users can disable administrative password for new container □ Users can disable administrative password for new container □ Users can disable administrative password for new container □ bisable administrative password for new container 	ers
Prompt user for encryption password Attempt to mount using administrative password first Disable any administrative password for new containers Users can disable administrative password for new container The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container	ers
Attempt to mount using administrative password first Disable any administrative password for new container. Users can disable administrative password for new container. The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container	ers
Disable any administrative password for new container: Users can disable administrative password for new contain. The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container	ers 2-Gol
□ Users can disable administrative password for new contain The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container	ers
The administrative password is set using DriveLock Encryption Container password recovery space usage e entire drive for encrypted container	2-Go
space usage	12.00
e entire drive for encrypted container	
□ Fill any remaining empty space on drives	
□ Leave empty space of 0	
ave unencrypted space on drives	
Unencrypted space 0 0 MB opercent	of drive
aximum size of encrypted container 100 + MB	
OK Cancel	

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.



Properties				?	×
General Settings	Encryption	Volume creat	ion		
Encryption algorithm	AES	3		~	
Hash algorithm	SHA	\ -1		~	
File system	FAT			~	
Cluster size	Defa	ault		~	
Volume label					
Perform quick form	at (do not e	ncrypt complet	e container)		
		OK	Cancel		Apply

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.

Properties	;					?	×
General	Settings	Encryption	Volume crea	tion			
Preserv	e existing	data (move e	existing data in	to encryp	ted contai	ner)	
Copy D	riveLock N	Nobile Encryp	otion to unencr	ypted por	tion		
	py Mac OS	S X version					
✓ Cre	ate autoru	n file (AUTO	RUN.INF)				
	Use custor	mized autoru	n settings				
							^
							~
Use cus	stom local	temporary fo	lder during vol	ume crea	tion		
By de	fault temp	orary files wil	l be stored in th	ne user's	profile.		
□ Hide en	ncrypted co	ontainer file					
⊡ Automa (default	atically refo t) or NTFS	rmat file syst	ems not suppo	orting mo	re than 4 (GB to ex	FAT
Per	form quick	-format					
For	mat to NTI	FS instead of	fexFAT				
Let use	r decide a	bout reforma	tting				
			OK	Can	cel	Арр	ly

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:

Citrix XenAp	p (ICA) client dri	ve mapping	is Propert	ies	?	×
Permissions	Filter / Shadow	Encryption	Options	Drive scan		
Require dr	ive to be encrypte	d				
⊡ Auton	natically encrypt un	encrypted me	edia			
	checking for encry	oted media (n	o non-Driv	eLock files a	allowed)	
🗆 Do no	t automatically mo	ount encrypted	d media			
	[ОК	Ca	ncel	Appl	у

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

Recycle Bin Host Name: OS Version: Mindows Server 20171 MB IP Address: T2.20.8.3 Image: Celevic Files Image: Celevic Files Image: Celevic Files Image: Celevic Files	L	~
Chris Files Calibration 11 * A * IF IF IE * IE * IE * IE * IE * IE * I	2016	
Firefox S 1 + 2 + + 1 + + 2 + + 1 + + 2 Lautwerk Verschlussein -14 + 12 15 + + 16 + + + 17 + + + Das angeschlossene Laufwerk ist nicht verschlusselv. verschlussellog ist für	Ŷ	
Notepad Notepad Vogescheben. Vogescheben. Determine Austern Negeter Se durch die Schrite, die rölig and um das Laufwerk zu verschlussen. Determine Seter richt mehr anzeigen		
C:\Users\citrixuser>	~	

•••



wird	s Laufwerk wird Sie, während das	d formatiert verschlüsselte La	ufwerk formatiert		
Mobile	Encryption Applica	ation wird kopiert.	**		
)	E			
	of Decals	Minister and	Contract	Links	
	< <u>B</u> ack	Next >	Cancel	Help	
	< <u>B</u> ack	<u>N</u> ext >	Cancel	Help	
₽ ∎ ▼ Home Share	View Magaz	Next >	Cancel	Help	-
✓ v I Home Share → v ↑ ▲ → This	View Manage SPC > Removable Disk	Next >	Cancel	Help – C	- ,
Image Share Image Share This Home Share This Devnloads Local Disk (D: en SUP Masic	View Diver Tools View Larage RC > Removable Disk -MUC-WIN10) -MUC-WIN10)	Next > Removable Disk (G) (G) Name	Cancel	Help – c Search Removable Disk (0 Date modified der is empty.	1 31)
Hone Share Hone Share → ↑ → 1 hit Downloads Local Disk (D. on SUP Local Disk (D. on SUP Music Network Drive (V. on 1 Pictures Pictures Pictures	View Direct Book View Larage PC - Removable Disk -MUC-WIN(0) SUP-MUC-WIN(0) sUP-MUC-WIN(0)	Next > Removable Disk (G) Go) Name	Cancel	Help – C Search Removable Disk (0 Date modified der is empty.	30)
	VIIIV VIIIV Anage PC + Removable Disk -MUC-WINTO SUP-MUC-WINTO SUP-MUC-WINTO	Next > Removable Disk (G:) (G:) Name	Cancel	Help – D Search Removable Disk (0 Date modified der is empty.	2 3)

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



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.

© 2022 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.