SYNACKTIV

DLP bypass for boomers

Antoine Cervoise

Sthack 2023

2023/05/12

DLP

- Data Loss Prevention
  - Sur le poste
  - Au niveau des passerelles

DLP

- Data Loss Prevention
  - → Sur le poste ←
  - ~~Au niveau des passerelles~~

Solutions techniques

- Durcissement Windows
- Logiciels spécialisés
  - Intégré dans un endpoint (antivirus, firewall…)
  - Ou bien une solution à part

Pourquoi les contourner ?

- Ramener nos outils
- Récupérer nos traces pour les rapports
- Et parce qu’on peut !

Email

- **ZIP / 7zip chiffré**
  - **Souvent bloqué en reception mais pas en émission**

File upload

- Sur Internet
- Sur le réseau local
  - Si le firewall limite l’accès au réseau local
    - → héberger l’application sur la passerelle
  - Exemple :
    - https://gist.github.com/taterbase/2688850

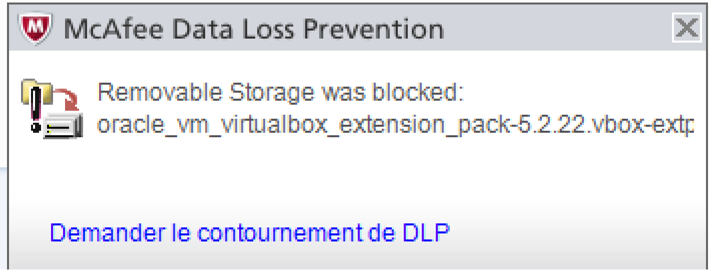
    -
      ```
      mkdir uploads && chmod 777 upload && docker run -it
      --rm --name uploader -p 9091:80 -v
      YOURPATH:/var/www/html php:7.2-apache
      ```

La machine virtuelle

- Méthode
  - Partager un répertoire avec la VM
  - Monter la clé USB sur la VM
- Limite
  - Avoir un système de virtualisation préinstallé
  - Ou des droits d'admin local

Enregistrer sous ?

- Lors de la copie vers une clé USB



McAfee Data Loss Prevention

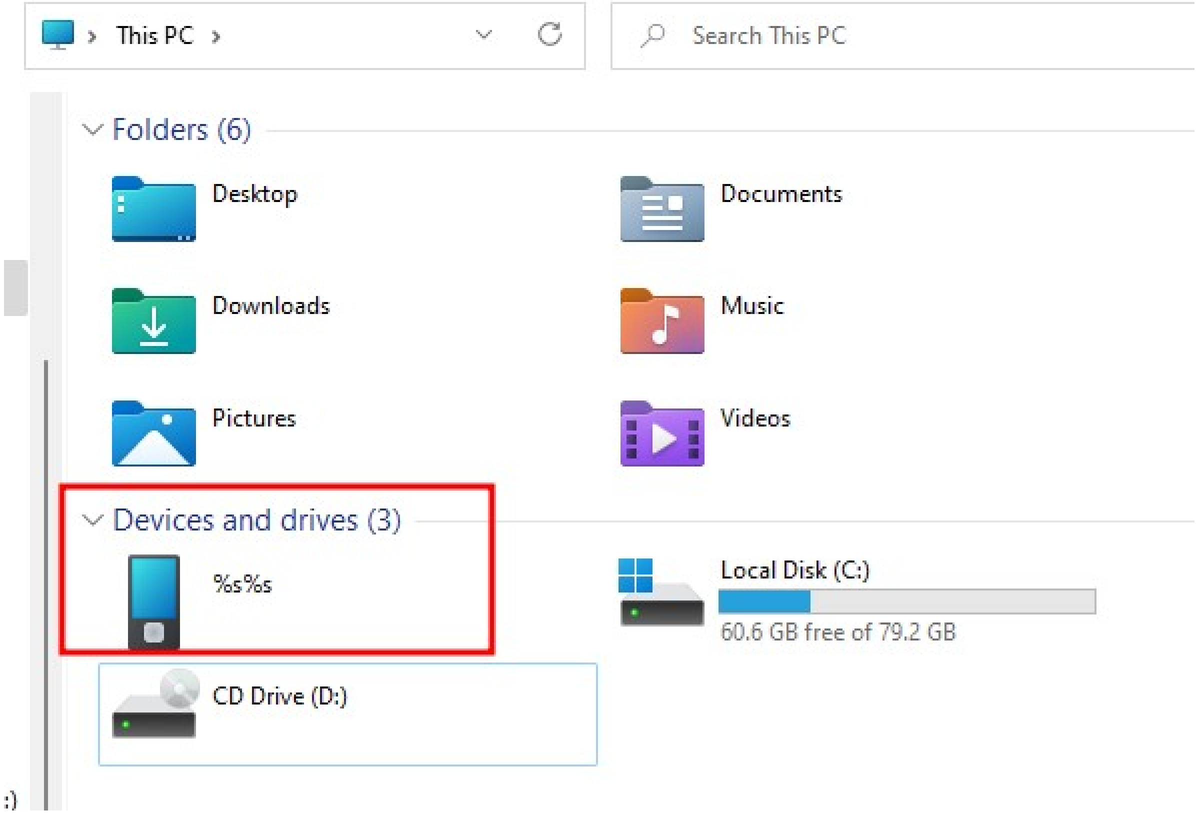
Removable Storage was blocked:
oracle_vm_virtualbox_extension_pack-5.2.22.vbox-extp

Demander le contournement de DLP

- Contournement magique
  - Ouvrir le fichier dans Notepad++ → Enregistrer sous → Clé USB

Chercher dans vos poches

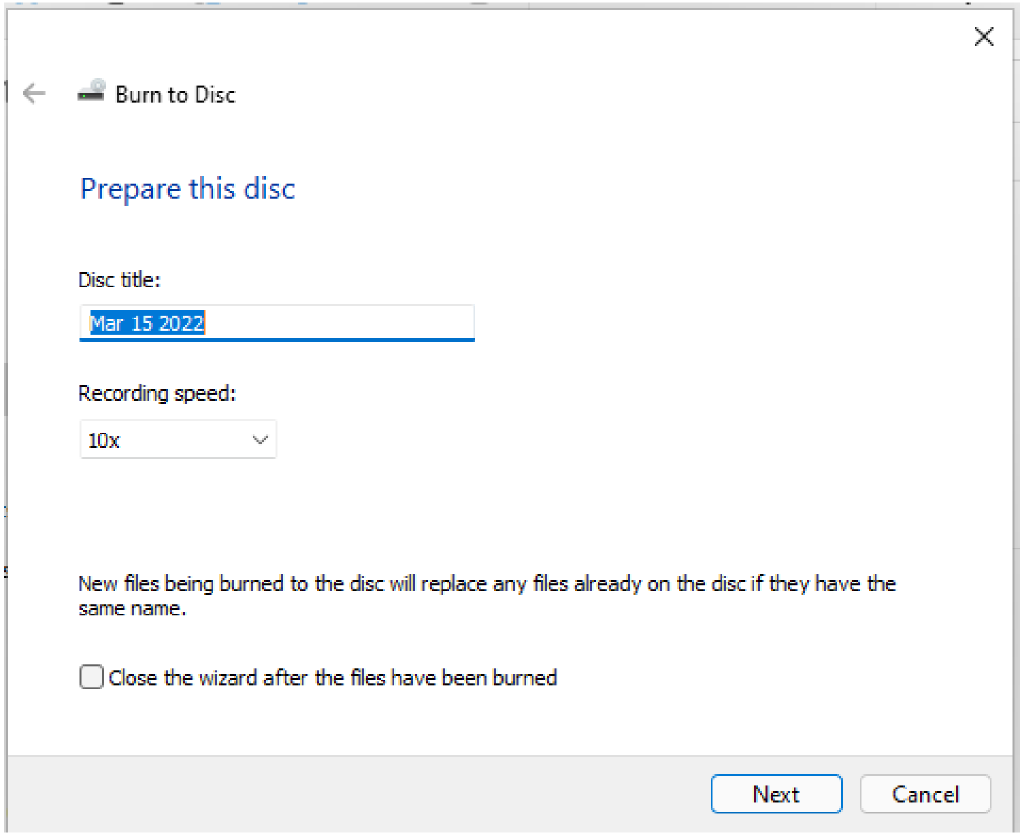
- WPD (Windows Portable Device)



Truc de vieux #1

- Lecteur/Graveur de CD
  - Pour Windows un lecteur/graveur CD en USB n'est pas un média amovible !

- *Fun fact*
  - Certains EDR tente de supprimer le fichier avant de le bloquer



Burn to Disc

Prepare this disc

Disc title: Mar 15 2022

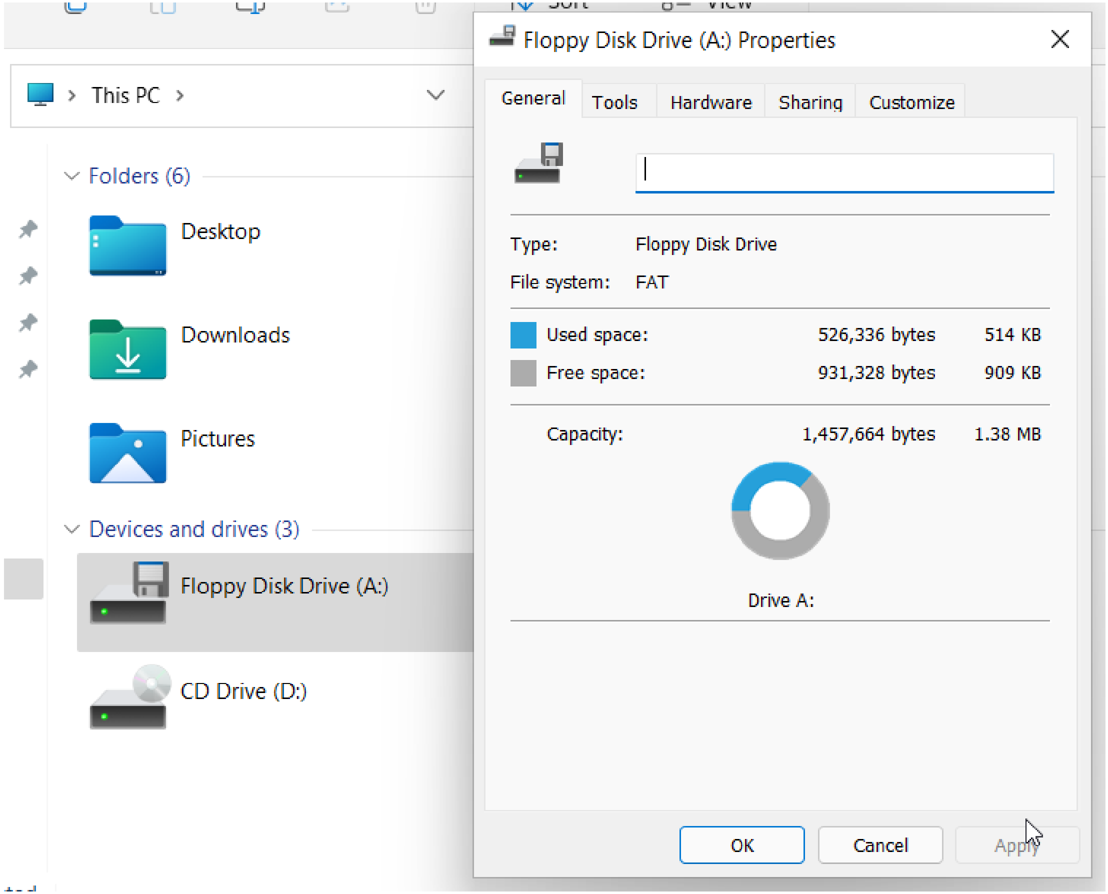
Recording speed: 10x

New files being burned to the disc will replace any files already on the disc if they have the same name.

☐ Close the wizard after the files have been burned

Truc de vieux #2

- **Lecteur de disquette**
  - **Comme pour les CD/DVD**
  - **Limité à 1,44 Mo**



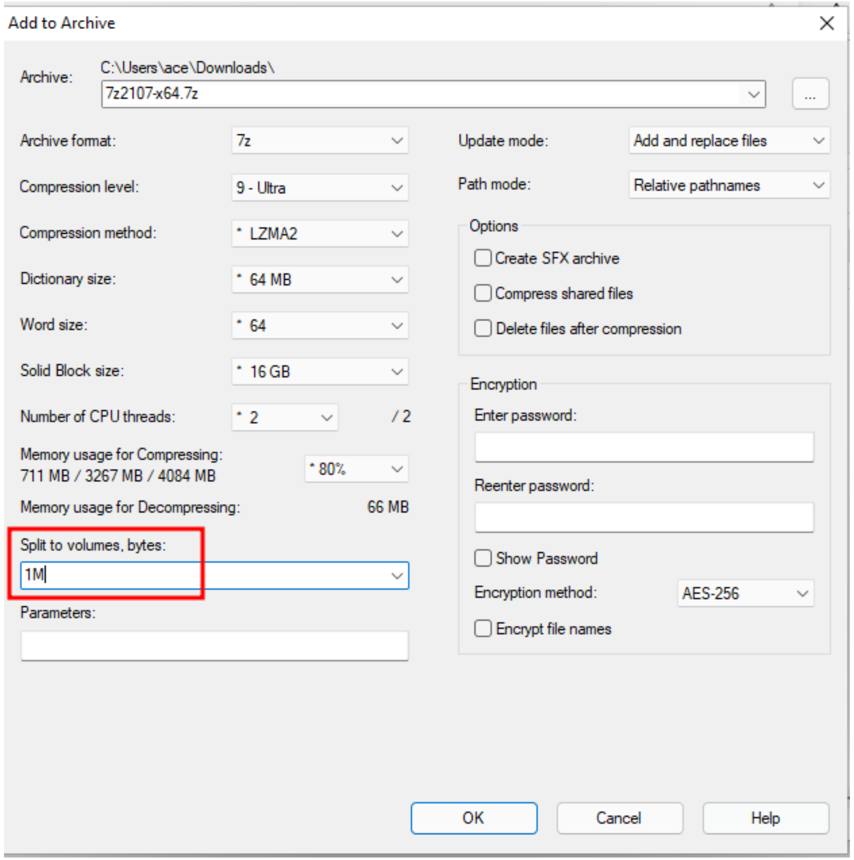
Floppy Disk Drive (A:) Properties

Type: Floppy Disk Drive

File system: FAT

🟦 Used space:	526,336 bytes	514 KB
▨ Free space:	931,328 bytes	909 KB
Capacity:	1,457,664 bytes	1.38 MB

Truc de vieux #2



Add to Archive

Archive: C:\Users\ace\Downloads\ 7z2107-x64.7z

Archive format: 7z

Compression level: 9 - Ultra

Compression method: * LZMA2

Dictionary size: * 64 MB

Word size: * 64

Solid Block size: * 16 GB

Number of CPU threads: * 2 / 2

Memory usage for Compressing: 711 MB / 3267 MB / 4084 MB * 80%

Memory usage for Decompressing: 66 MB

Split to volumes, bytes: 1M

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

☐ Create SFX archive

☐ Compress shared files

☐ Delete files after compression

Encryption

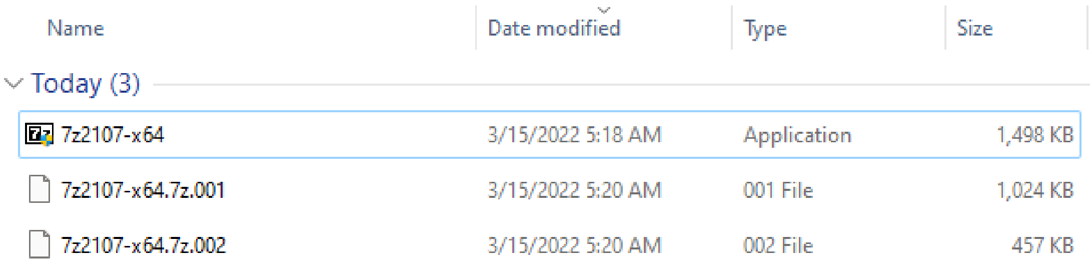
Enter password:

Reenter password:

☐ Show Password

Encryption method: AES-256

☐ Encrypt file names

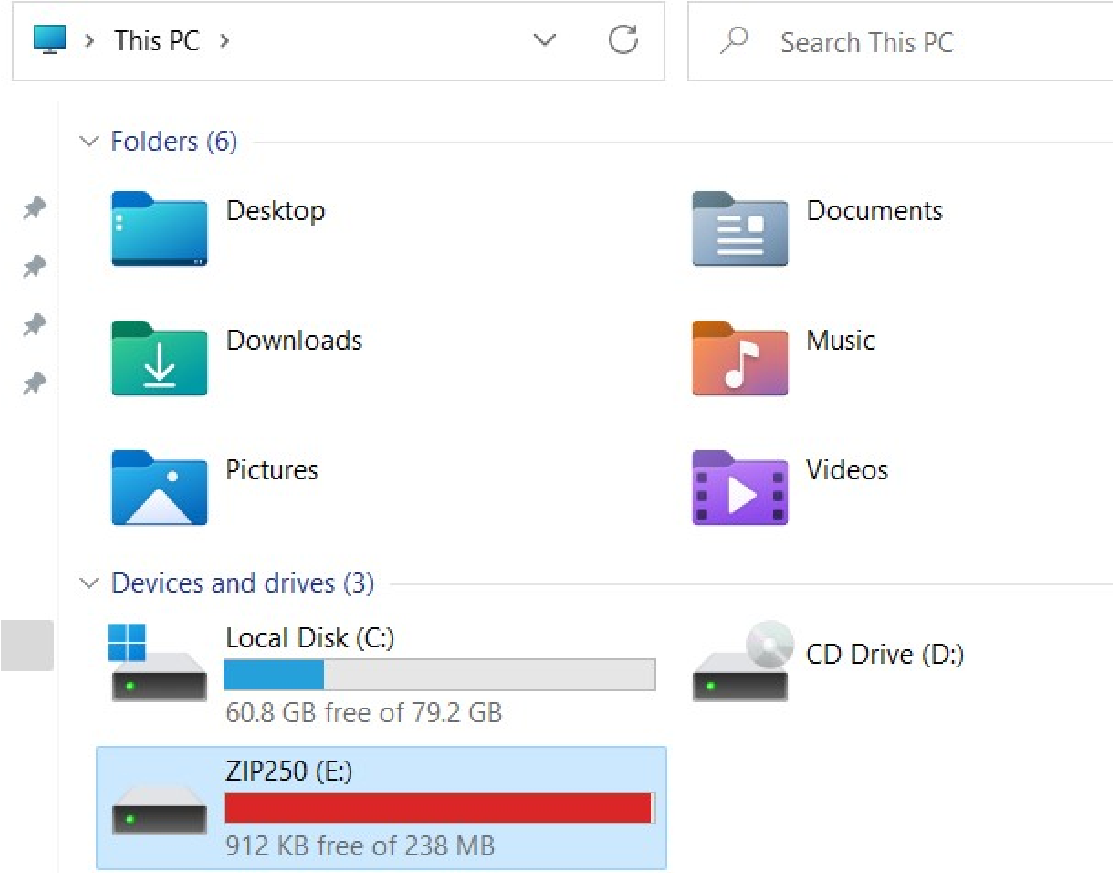


Today (3)

Name	Date modified	Type	Size
7z2107-x64	3/15/2022 5:18 AM	Application	1,498 KB
7z2107-x64.7z.001	3/15/2022 5:20 AM	001 File	1,024 KB
7z2107-x64.7z.002	3/15/2022 5:20 AM	002 File	457 KB

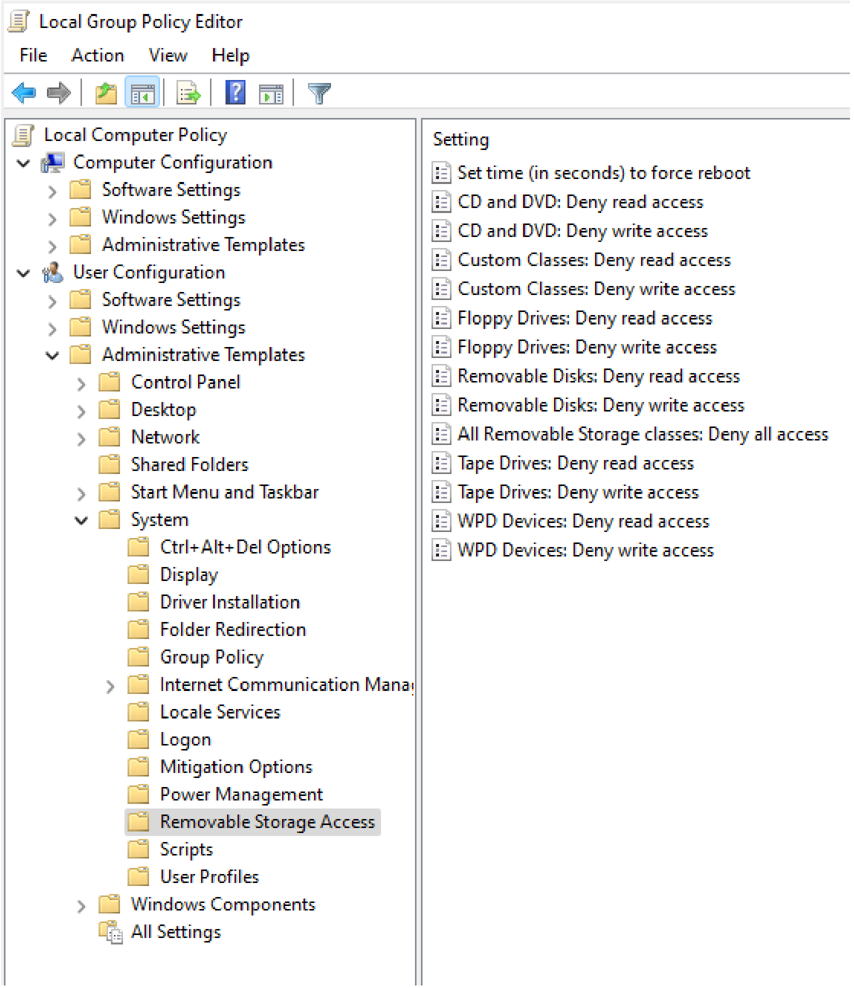
Truc de vieux #2bis

- **Disquettes ZIP**
  - **Branché en IDE ce n'est pas considéré comme un lecteur de disquette**



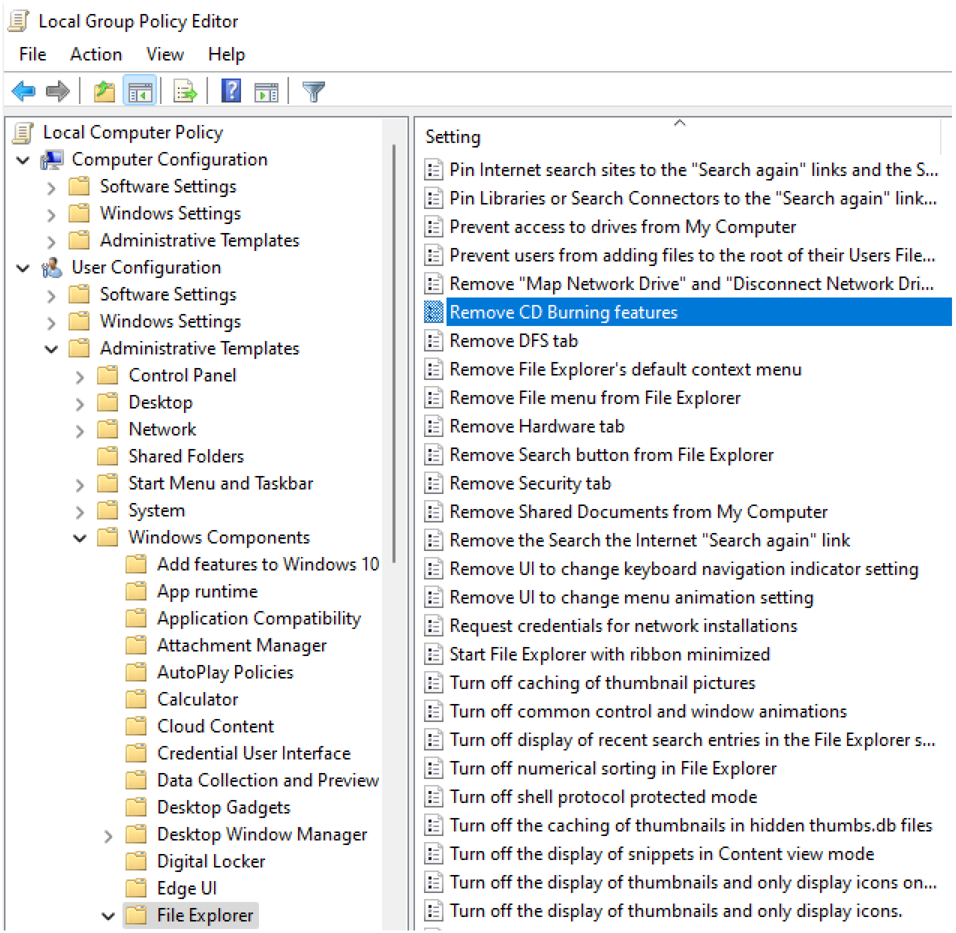
Local Disk (C:)
60.8 GB free of 79.2 GB
CD Drive (D:)
ZIP250 (E:)
912 KB free of 238 MB

Blocage dans Windows 11



Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Desktop
    - Network
    - Shared Folders
    - Start Menu and Taskbar
    - System
      - Ctrl+Alt+Del Options
      - Display
      - Driver Installation
      - Folder Redirection
      - Group Policy
      - Internet Communication Mana
      - Locale Services
      - Logon
      - Mitigation Options
      - Power Management
      - Removable Storage Access
      - Scripts
      - User Profiles
    - Windows Components
    - All Settings

Setting
- Set time (in seconds) to force reboot
- CD and DVD: Deny read access
- CD and DVD: Deny write access
- Custom Classes: Deny read access
- Custom Classes: Deny write access
- Floppy Drives: Deny read access
- Floppy Drives: Deny write access
- Removable Disks: Deny read access
- Removable Disks: Deny write access
- All Removable Storage classes: Deny all access
- Tape Drives: Deny read access
- Tape Drives: Deny write access
- WPD Devices: Deny read access
- WPD Devices: Deny write access



Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Desktop
    - Network
    - Shared Folders
    - Start Menu and Taskbar
    - System
    - Windows Components
      - Add features to Windows 10
      - App runtime
      - Application Compatibility
      - Attachment Manager
      - AutoPlay Policies
      - Calculator
      - Cloud Content
      - Credential User Interface
      - Data Collection and Preview
      - Desktop Gadgets
      - Desktop Window Manager
      - Digital Locker
      - Edge UI
      - File Explorer

Setting
- Pin Internet search sites to the "Search again" links and the S...
- Pin Libraries or Search Connectors to the "Search again" link...
- Prevent access to drives from My Computer
- Prevent users from adding files to the root of their Users File...
- Remove "Map Network Drive" and "Disconnect Network Dri...
- Remove CD Burning features
- Remove DFS tab
- Remove File Explorer's default context menu
- Remove File menu from File Explorer
- Remove Hardware tab
- Remove Search button from File Explorer
- Remove Security tab
- Remove Shared Documents from My Computer
- Remove the Search the Internet "Search again" link
- Remove UI to change keyboard navigation indicator setting
- Remove UI to change menu animation setting
- Request credentials for network installations
- Start File Explorer with ribbon minimized
- Turn off caching of thumbnail pictures
- Turn off common control and window animations
- Turn off display of recent search entries in the File Explorer s...
- Turn off numerical sorting in File Explorer
- Turn off shell protocol protected mode
- Turn off the caching of thumbnails in hidden thumbs.db files
- Turn off the display of snippets in Content view mode
- Turn off the display of thumbnails and only display icons on...
- Turn off the display of thumbnails and only display icons.

SYNACKTIV

https://www.linkedin.com/company/synacktiv
https://twitter.com/synacktiv
Nos publications sur : https://synacktiv.com