Zadania do samodzielnej realizacji w domu (Moduł 5)

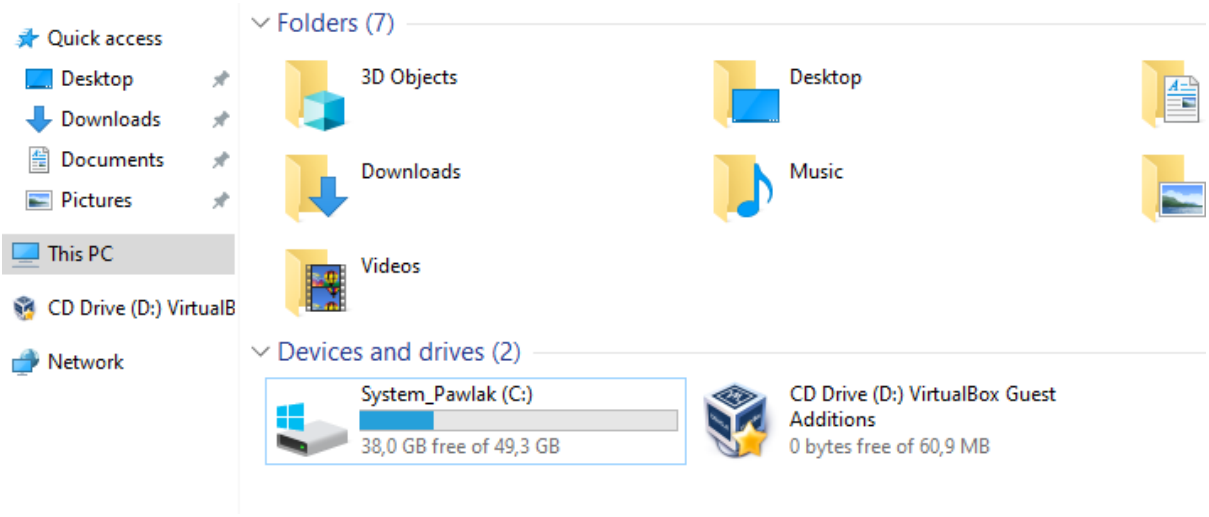
Zadanie 1

Jesteś administratorem systemów w firmie Northwind Traders (nwtraders.msft).

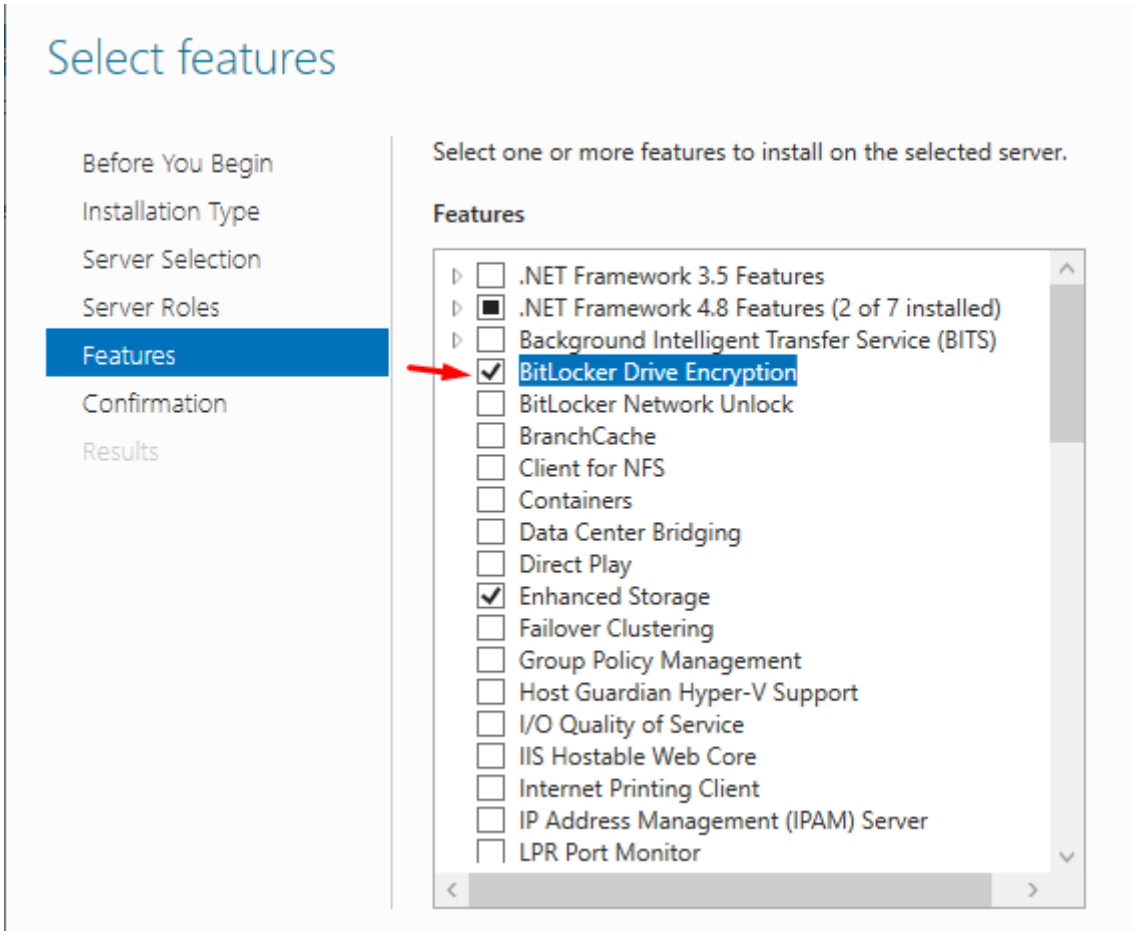
Otrzymałeś zadanie zabezpieczenia dysku serwera Windows Server "Glasgow" oraz firmowego pen-drive'a z wykorzystaniem wbudowanej funkcji "BitLocker".

Twoim zadaniem jest więc:

- zmienić w systemie Windows Server "Glasgow" nazwę woluminu *C:/* na "*System_{Nazwisko}*" (gdzie pod *{Nazwisko)* należy podstawić swoje własne Nazwisko, np. *System_Kowalski*)
- zaszyfrować w systemie Windows Server "Glasgow" z wykorzystaniem systemu *BitLocker* wolumin *C:/* z wykorzystaniem dowolnego hasła
- podłączyć do systemu Windows Server "Glasgow" pen-drive i zaszyfrować go z wykorzystaniem systemu *Bitlocker To G*o, a następnie przetestować czy można prawidłowo go uruchomić w systemie Windows "Nowak"

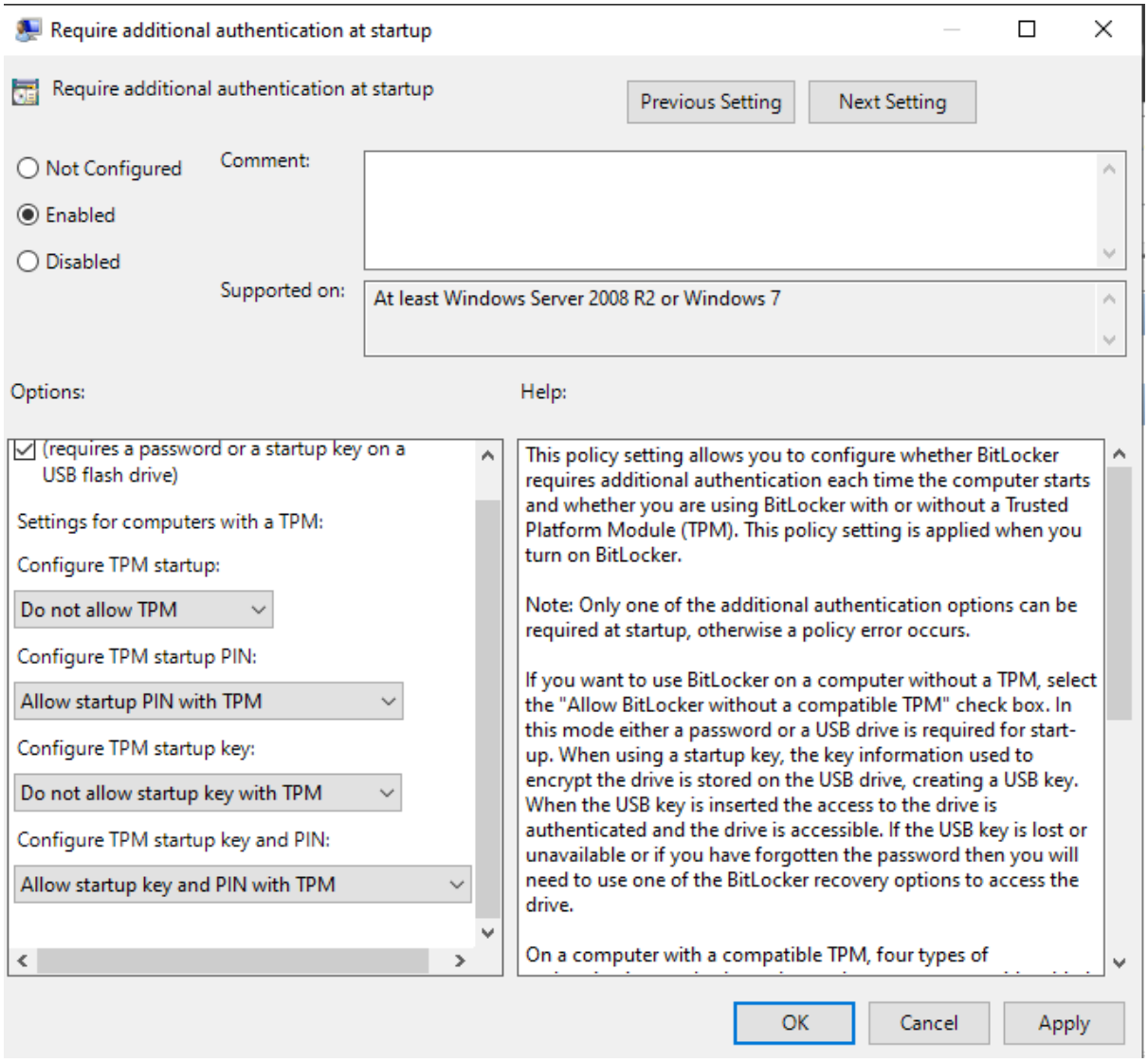


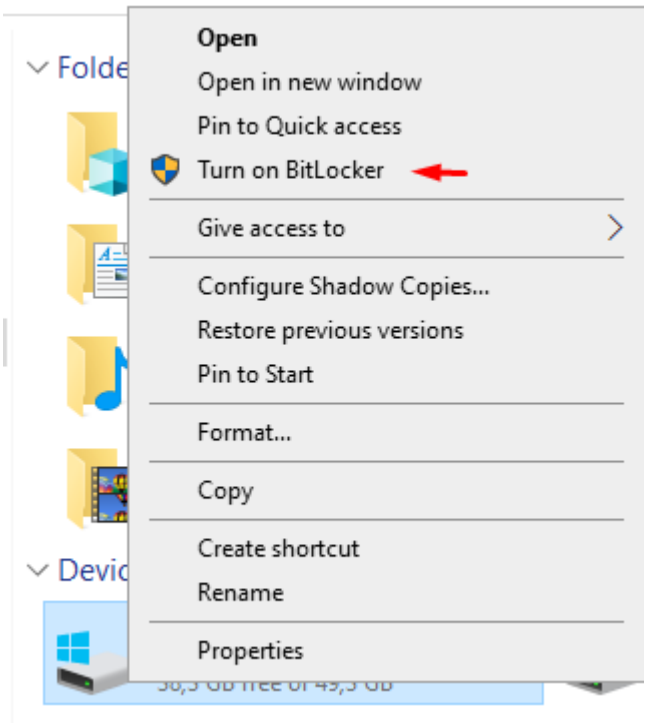
Trzeba pamiętać aby funkcja Bitlocker była zainstalowana:

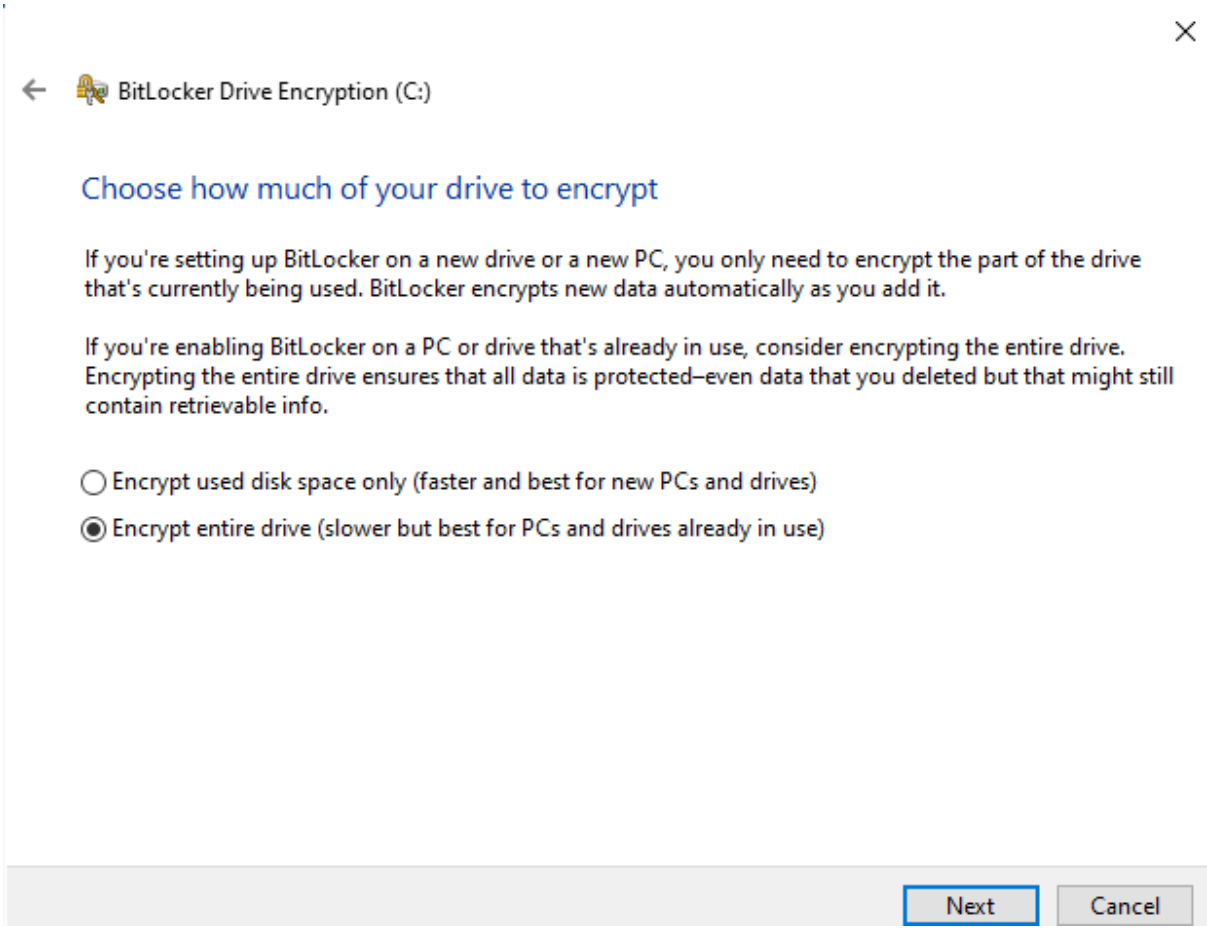


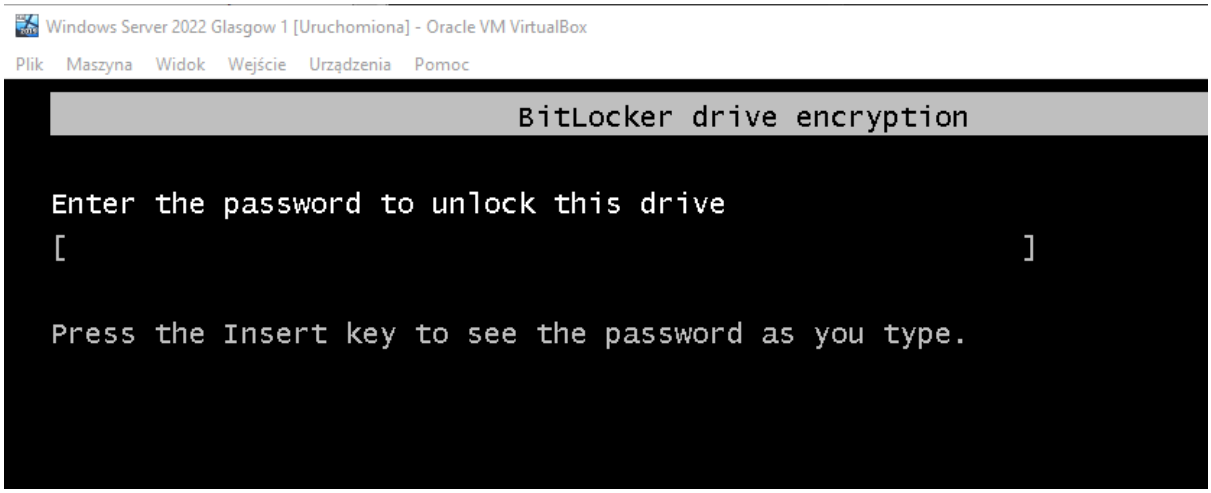
Oraz pozwolić na szyfrowanie bez modułu TPM w lokalnych zasadach grupy:

Computer Configuration -> Administrative Templates -> Windows Component -> Bitlocker Drive Encryption -> Operating System Drives -> Require additional authentication at startup

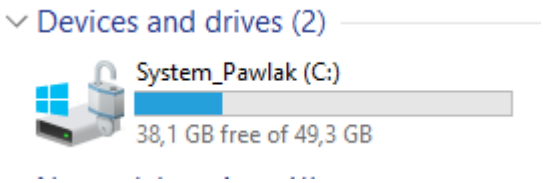

Require additional authentication at startup
Require additional authentication at startup
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2008 R2 or Windows 7
Options:
Help:
(requires a password or a startup key on a USB flash drive)
Settings for computers with a TPM:
Configure TPM startup:
Do not allow TPM
Configure TPM startup PIN:
Allow startup PIN with TPM
Configure TPM startup key:
Do not allow startup key with TPM
Configure TPM startup key and PIN:
Allow startup key and PIN with TPM
This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker.
Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs.
If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive.
On a computer with a compatible TPM, four types of
OK
Cancel
Apply


Open
Open in new window
Pin to Quick access
Turn on BitLocker
Give access to
Configure Shadow Copies...
Restore previous versions
Pin to Start
Format...
Copy
Create shortcut
Rename
Properties

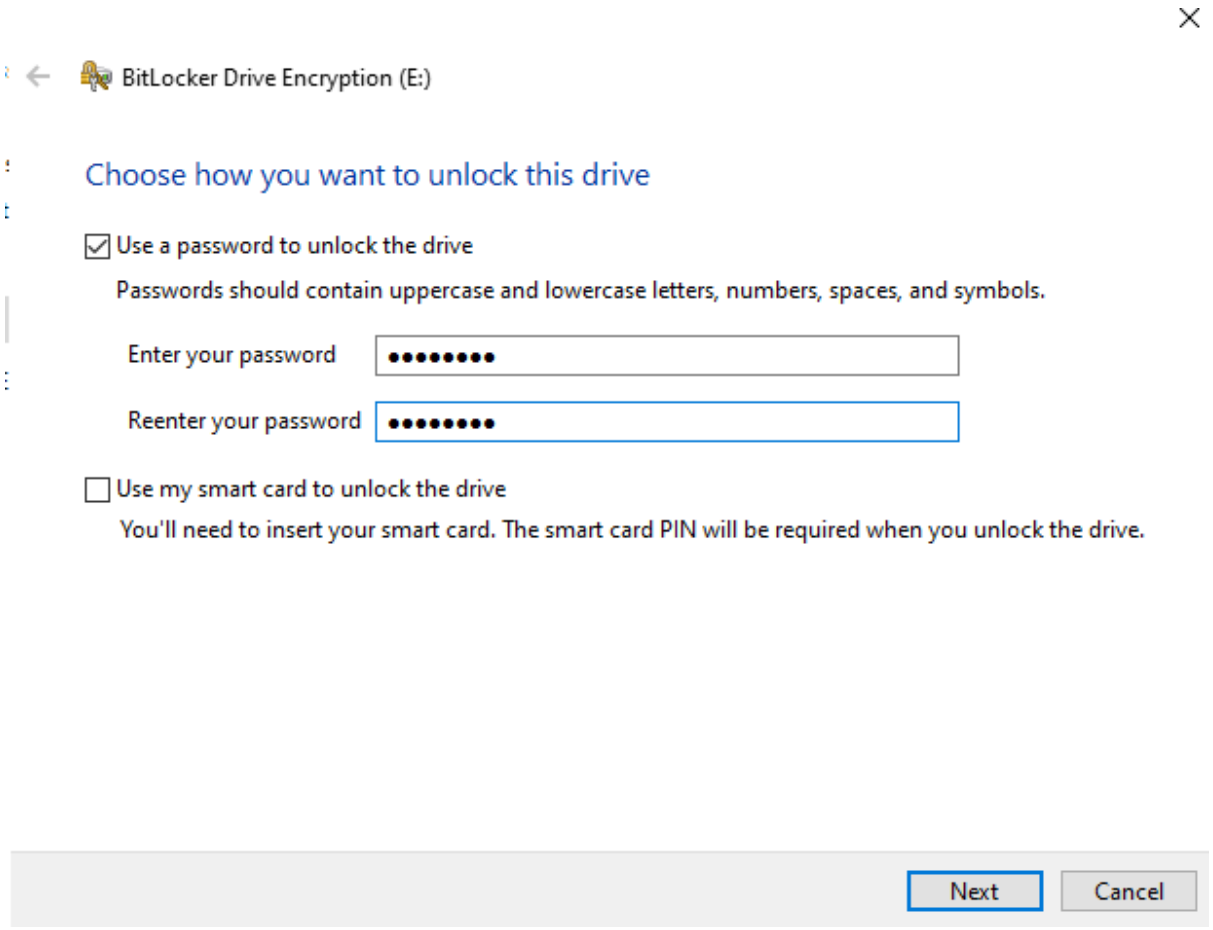

BitLocker Drive Encryption (C:)
Choose how much of your drive to encrypt
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.
Encrypt used disk space only (faster and best for new PCs and drives)
Encrypt entire drive (slower but best for PCs and drives already in use)
Next
Cancel

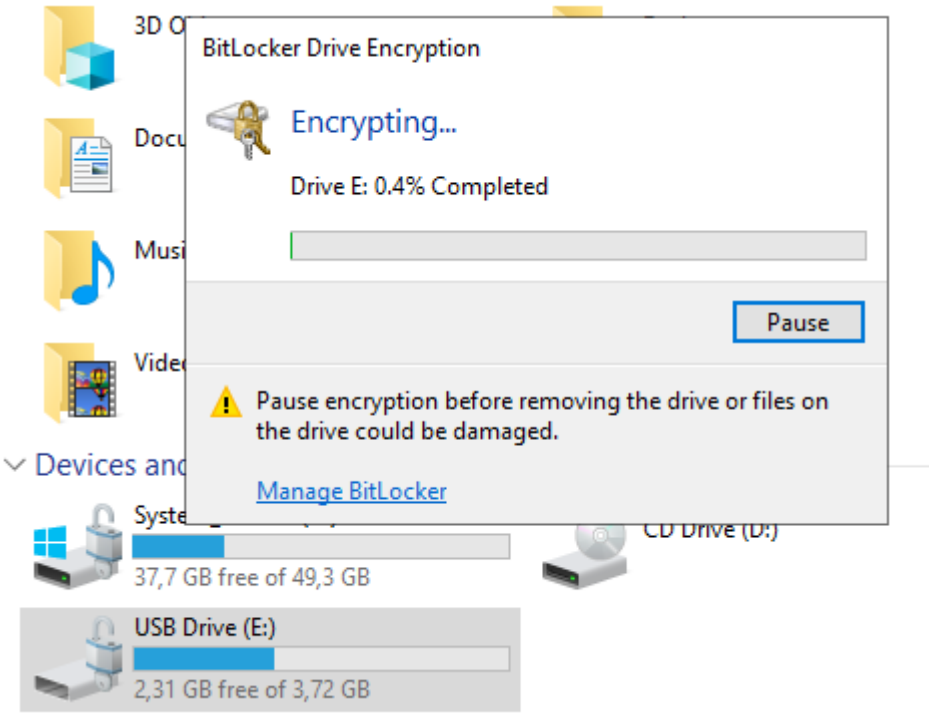


Dysk został zaszyfrowany.

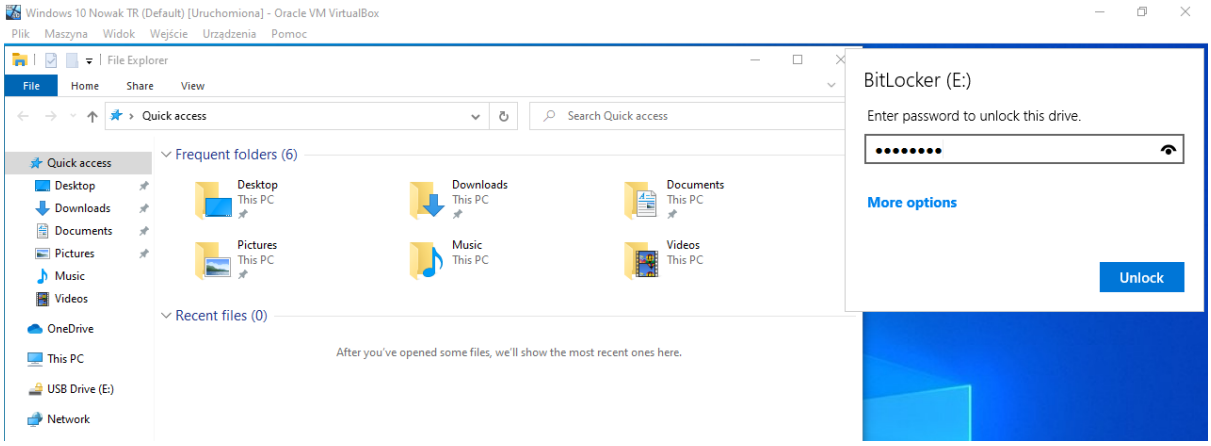


Szyfrowanie dysku usb





Otworzenie dysku na windowsie “Nowak”



Po wpisaniu hasła można zobaczyć zawartość