

# Sprawozdanie z modułu 5

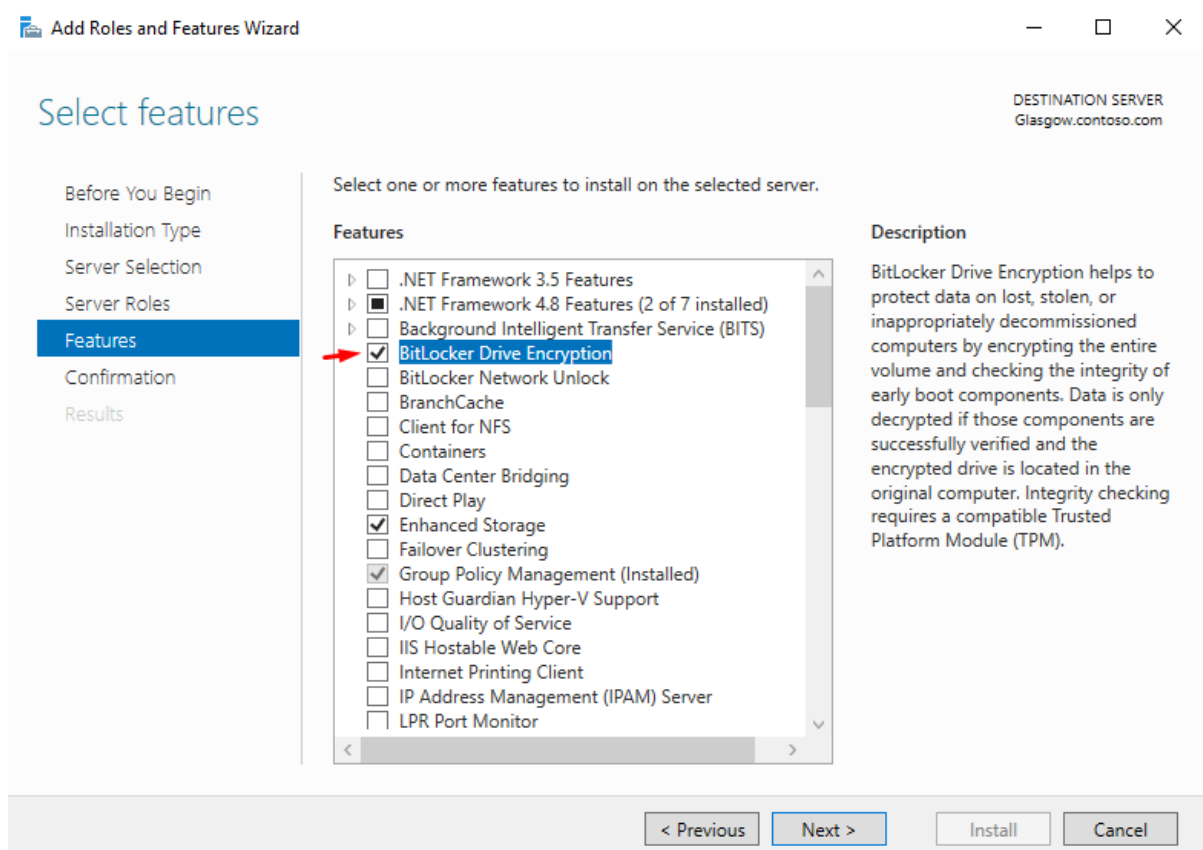
## Zadanie 1

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

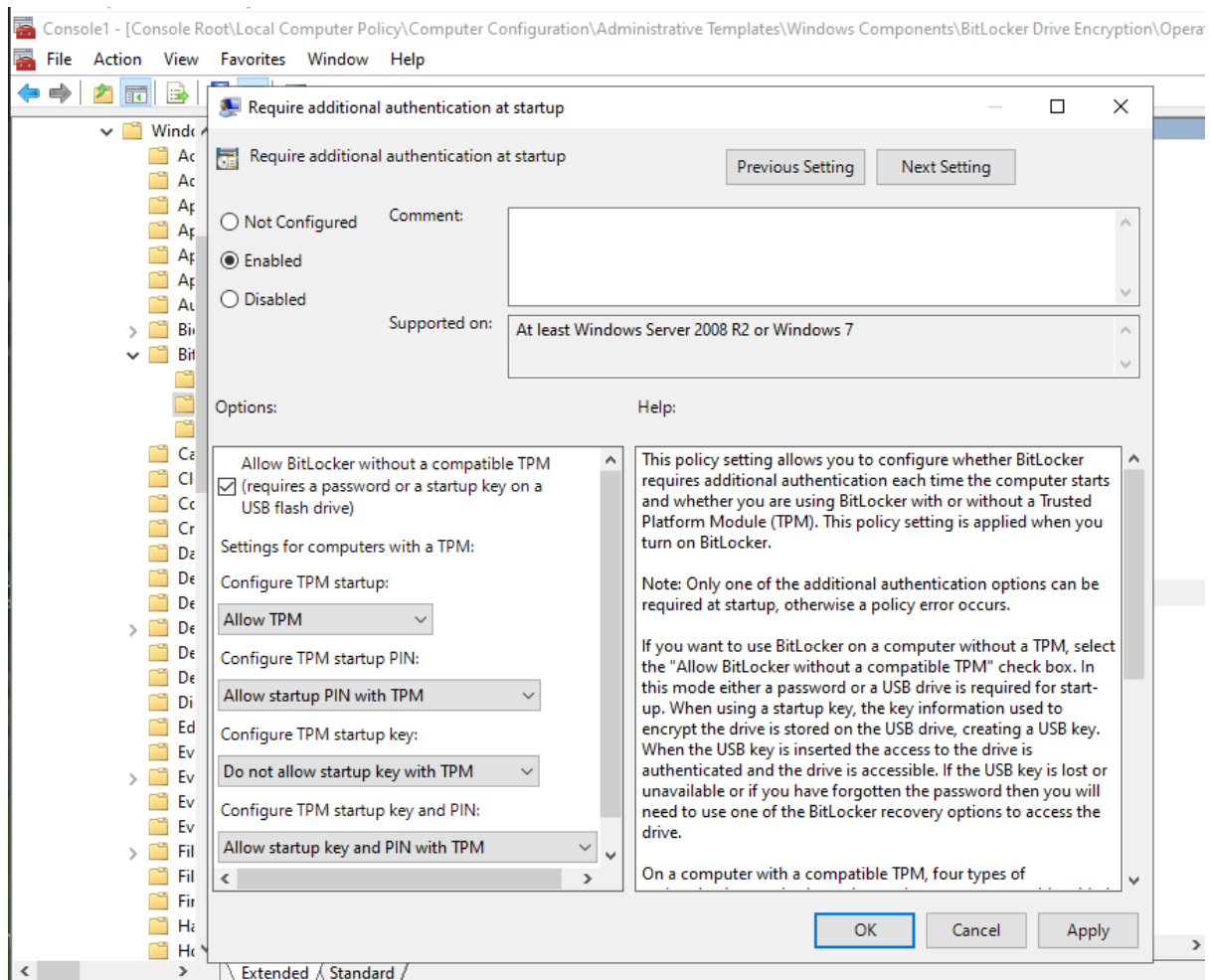
Otrzymałeś zadanie zabezpieczenia dysku serwera Windows Server "Glasgow" z wykorzystaniem wbudowanej funkcji "BitLocker".

Twoim zadaniem jest więc:

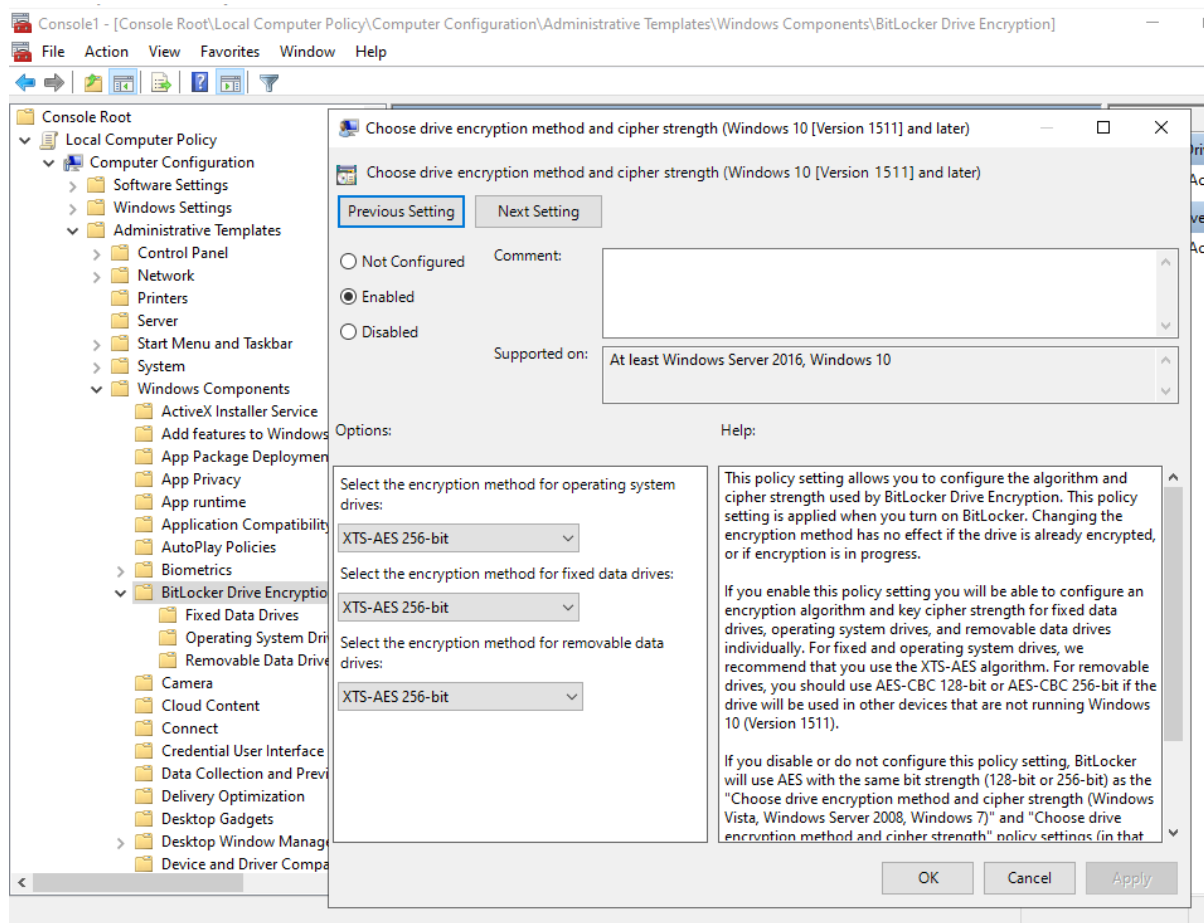
- w systemie Windows Server "Glasgow" zainstalować funkcję *"BitLocker Drive Encryption"*
  - w systemie Windows Server "Glasgow" umożliwić szyfrowanie BitLocker z wykorzystaniem hasła (ze względu na brak modułu TPM), poprzez zaznaczenie opcji *"Allow BitLocker without compatible TPM..."* w lokalnych zasadach grup: *Computer Configuration -> Administrative Templates -> Windows Component -> Bitlocker Drive Encryption -> Operating System Drives -> Require additional authentication at startup*
  - w systemie Windows Server "Glasgow" umożliwić szyfrowanie BitLocker z wykorzystaniem silniejszego klucza symetrycznego "AES256", poprzez zaznaczenie w/w opcji w lokalnych zasadach grup: *Computer Configuration -> Administrative Templates -> Windows Component -> Bitlocker Drive Encryption -> Choose drive encryption method and cipher strength*
  - zaszyfrować systemem BitLocker wolumin C:/ z wykorzystaniem hasła
- 
- w systemie Windows Server "Glasgow" zainstalować funkcję *"BitLocker Drive Encryption"*



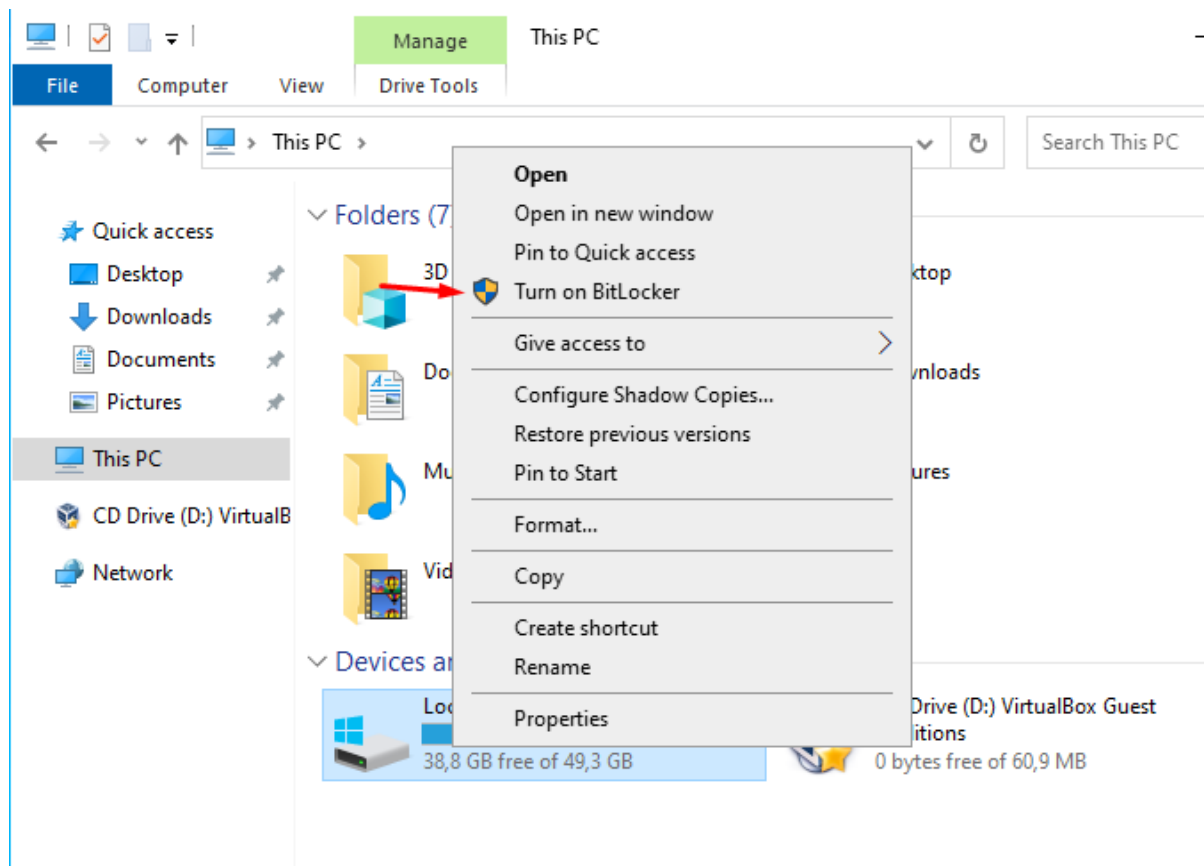
- w systemie Windows Server "Glasgow" umożliwić szyfrowanie BitLocker z wykorzystaniem hasła (ze względu na brak modułu TPM), poprzez zaznaczenie opcji "Allow BitLocker without compatible TPM..." w lokalnych zasadach grup: *Computer Configuration -> Administrative Templates -> Windows Component -> Bitlocker Drive Encryption -> Operating System Drives -> Require additional authentication at startup*



- w systemie Windows Server "Glasgow" umożliwić szyfrowanie BitLocker z wykorzystaniem silniejszego klucza symetrycznego "AES256", poprzez zaznaczenie w/w opcji w lokalnych zasadach grup: *Computer Configuration -> Administrative Templates -> Windows Component -> Bitlocker Drive Encryption -> Choose drive encryption method and cipher strength*



- zaszyfrować systemem BitLocker wolumin C:/ z wykorzystaniem hasła



← BitLocker Drive Encryption (C:)

### Choose how to unlock your drive at startup

**i** Some settings are managed by your system administrator.

To help keep your data more secure, you can have BitLocker prompt you to enter a password or insert a USB flash drive each time you start your PC.


→ Insert a USB flash drive

→ Enter a password



Cancel



←  BitLocker Drive Encryption (C:)

## Create a password to unlock this drive

You should create a strong password that uses uppercase and lowercase letters, numbers, symbols, and spaces.

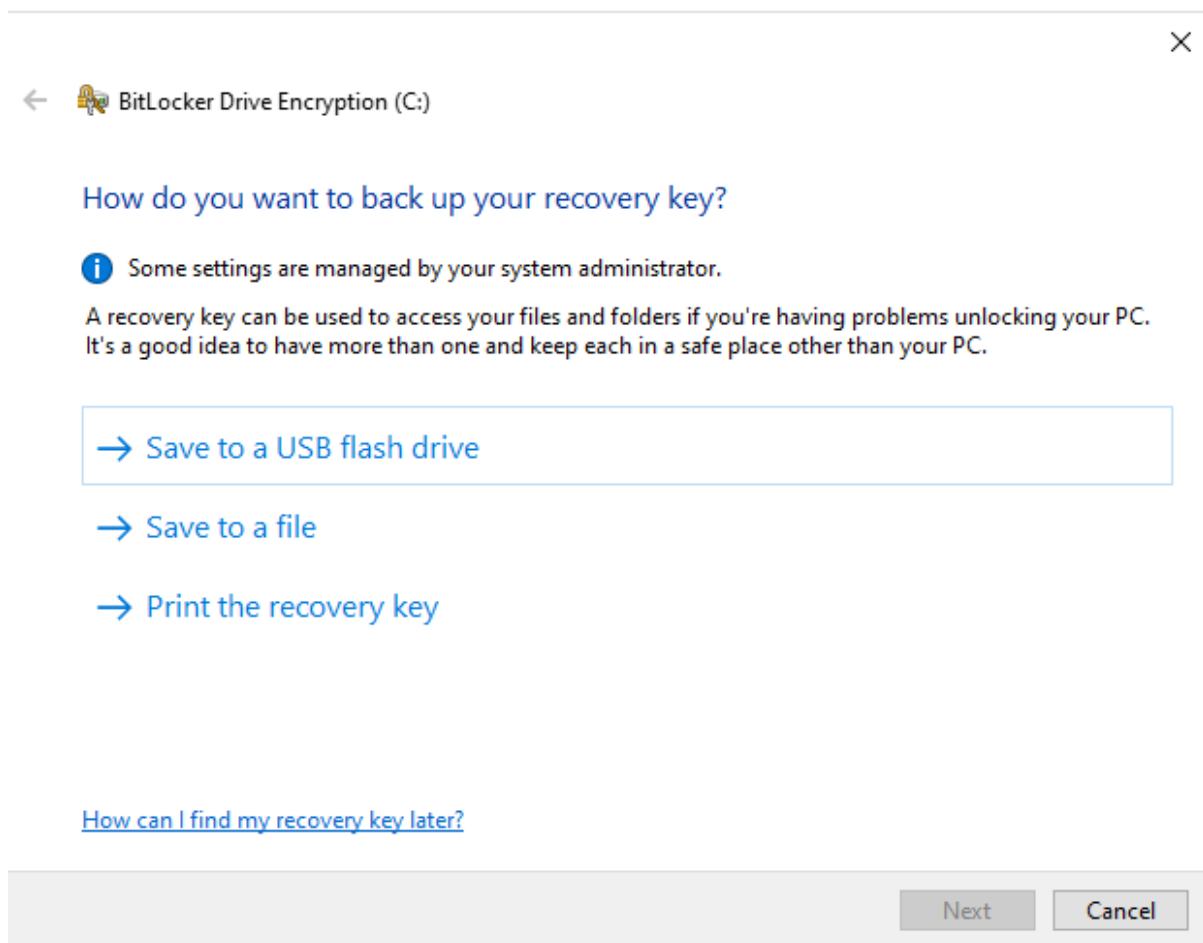
Enter your password

Reenter your password

[Tips for creating a strong password.](#)

Next

Cancel



Zapisałem plik z hasłem odzyskiwania na dysku zewnętrznym.

### 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



## Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

You can keep working while the drive is being encrypted, although your PC might run more slowly.

☒ Run BitLocker system check

The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer before encrypting.

Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.

Continue

Cancel



