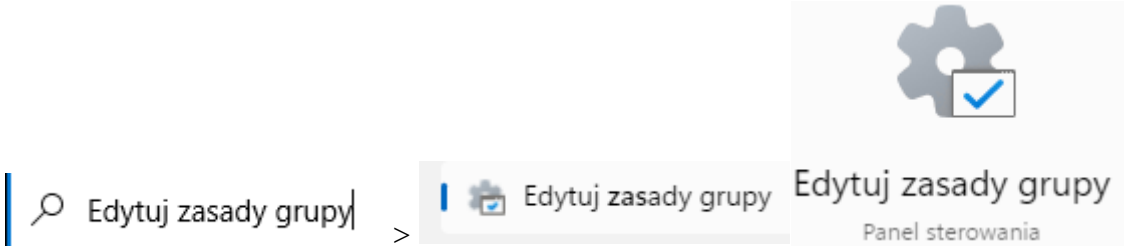
Powershell - zaszyfruj dysk za pomocą funkcji Bitlocker i hasła

Chcesz dowiedzieć się, jak używać funkcji Bitlocker do szyfrowania dysku systemu operacyjnego za pomocą hasła?

Jak zaszyfrować dysk za pomocą funkcji Bitlocker na komputerze bez układu TPM?

1. Bitlocker - Włącz korzystanie z szyfrowania hasła

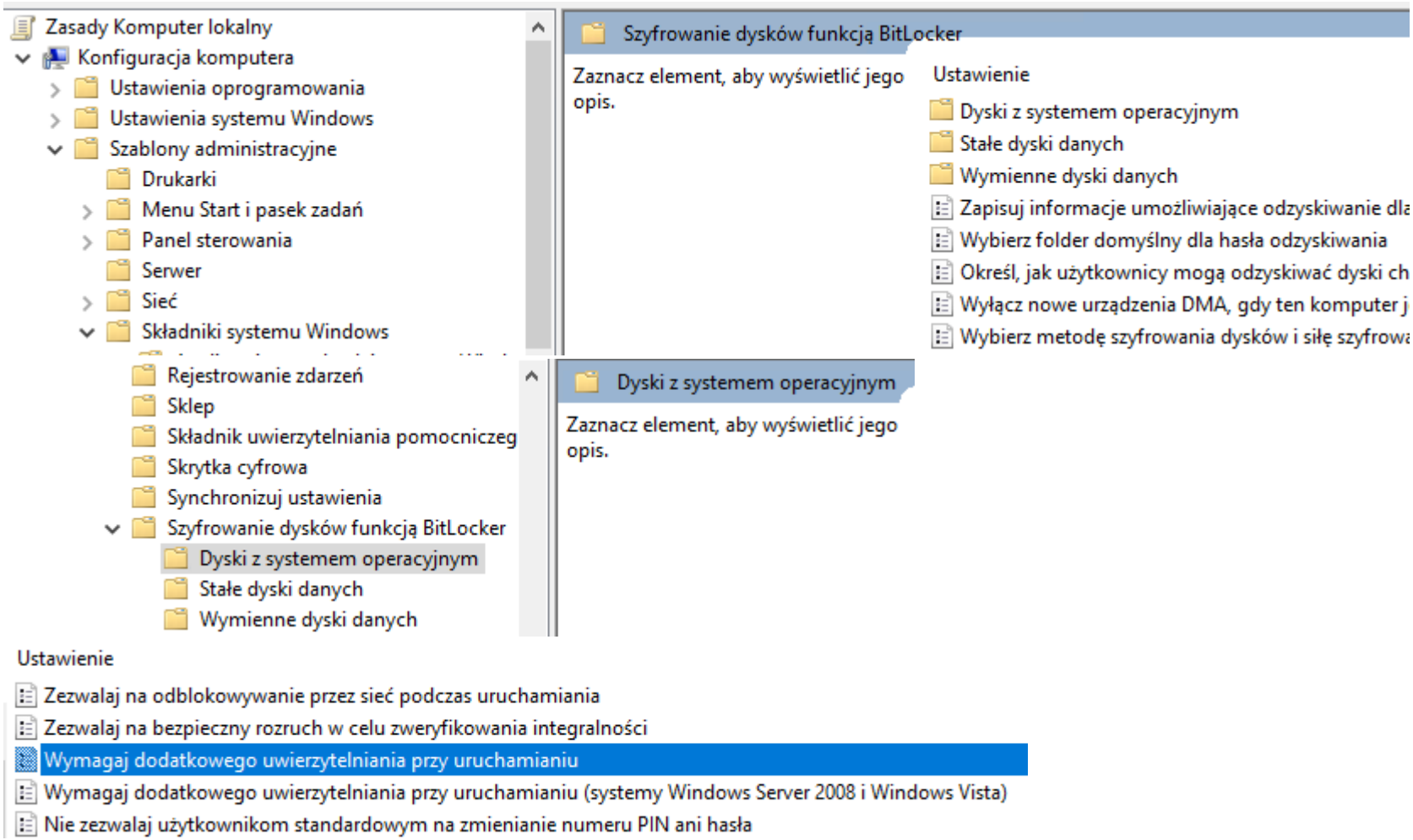
Jako administrator uruchom edytor zasad grupy.



Na ekranie edytora zasad grupy rozwiń folder Konfiguracja komputera i zlokalizuj następujący element.

Konfiguracja komputera > Szablony administracyjne > Składniki systemu Windows > Szyfrowanie dysków funkcją BitLocker > Dyski z systemem operacyjnym

Uzyskaj dostęp do folderu o nazwie Dyski z systemem operacyjnym.



Włącz element o nazwie: Wymagaj dodatkowego uwierzytelniania podczas uruchamiania.

Opcje:

• Zezwalaj na użycie funkcji Bitlocker bez zgodnego modułu TPM - ☑ tak.

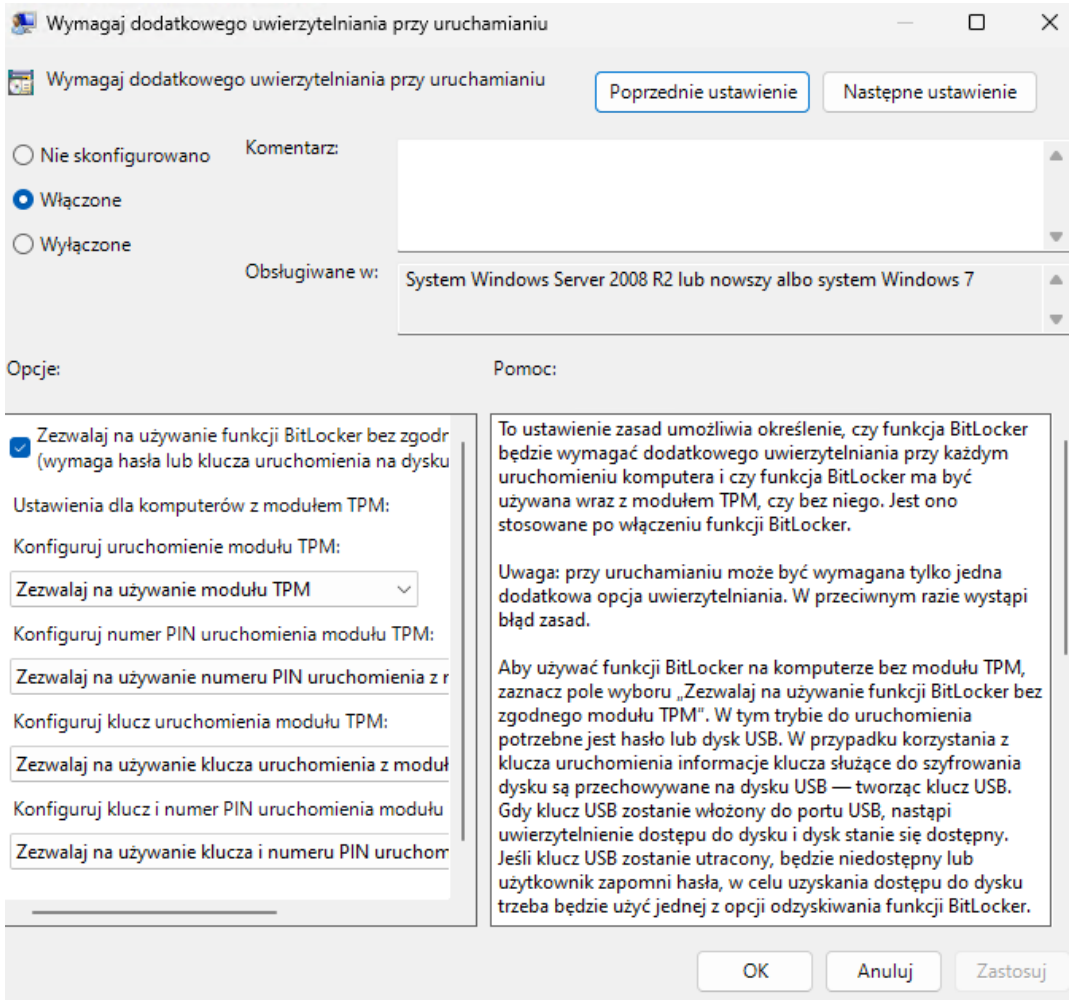
Ustawienia dla komputerów z modułem TPM:

• Konfiguruj uruchamianie modułu TPM: - Zezwalaj na używanie modułu TPM.

• Konfiguruj numer PIN uruchamiania modułu TPM: - Zezwalaj na używanie numeru PIN uruchamiania za pomocą modułu TPM.

• Konfiguruj klucz uruchomienia modułu TPM: - Zezwalaj na używanie klucza uruchomienia z modułem TPM.

• Konfiguruj klucz i numer PIN uruchomienia modułu TPM: - Zezwalaj na używanie klucza i numer PIN uruchomienia z modułem TPM.



Aby zapisać konfigurację zasad grupy, musisz zamknąć edytor zasad grupy.

gpupdate /force

Zrestartuj komputer.

Gratulacje! Zakończyłeś konfigurację GPO.

2. Powershell - zaszyfruj dysk za pomocą funkcji Bitlocker i hasła

Jako administrator uruchom wiersz polecenia programu Powershell z podwyższonym poziomem uprawnień.

Sprawdź, czy komputer ma włączony układ TPM.

Get-tpm

Dane wyjściowe komputera z układem TPM.

```
TpmPresent                 : True
TpmReady                   : True
TpmEnabled                 : True
TpmActivated               : True
TpmOwned                   : True
RestartPending             : False
ManufacturerId             : 1297303124
ManufacturerIdTxt          : MSFT
ManufacturerVersion        : 8213.275.21.18466
ManufacturerVersionFull20  : 8213.275.21.18466

ManagedAuthLevel           : Full
OwnerAuth                  :
OwnerClearDisabled         : False
AutoProvisioning           : Enabled
LockedOut                  : False
LockoutHealTime            : 10 minutes
LockoutCount               : 1
LockoutMax                 : 31
SelfTest                   : {}
```

Wymień dostępne dyski.

Get-BitlockerVolume

Oto dane wyjściowe polecenia:

```
VolumeType      Mount CapacityGB VolumeStatus            Encryption KeyProtector             AutoUnlock Protection
                Point                                    Percentage                          Enabled    Status
----------      ----- ---------- ------------            ---------- ------------             ---------- ----------
OperatingSystem C:      1 023,12 FullyDecrypted          0          {}                                  Off
```

Zaszyfruj dysk systemu operacyjnego za pomocą funkcji Bitlocker i hasła.

$PASSWORD = ConvertTo-SecureString "kamisama123" -AsPlainText -Force

```
PS C:\Windows\system32> $PASSWORD = ConvertTo-SecureString "kamisama123" -AsPlainText -Force
```

Zmień wartość hasła.

Enable-BitLocker -MountPoint "C:" -UsedSpaceOnly -EncryptionMethod Aes256 -Password $PASSWORD -PasswordProtector

Oto dane wyjściowe polecenia.

```
PS C:\Windows\system32> Enable-BitLocker -MountPoint "C:" -UsedSpaceOnly -EncryptionMethod Aes256 -Password $PASSWORD -PasswordProtector
WARNING: ACTIONS REQUIRED:

1. Restart the computer to run a hardware test.
    (Type: get-help Restart-Computer for command line instructions.)


   ComputerName: STACJA

VolumeType      Mount CapacityGB VolumeStatus            Encryption KeyProtector             AutoUnlock Protection
                Point                                    Percentage                          Enabled    Status
----------      ----- ---------- ------------            ---------- ------------             ---------- ----------
OperatingSystem C:      1 023,12 FullyDecrypted          0          {Password}                          Off
```

Utwórz hasło odzyskiwania.

Add-BitlockerkeyProtector C: -RecoveryPasswordProtector

```
PS C:\Windows\system32> Add-BitlockerkeyProtector C: -RecoveryPasswordProtector
```

Zanotuj hasło odzyskiwania funkcji Bitlocker - "kamisama123".

OSTRZEŻENIE: WYMAGANE DZIAŁANIA:

Zapisz to numeryczne hasło odzyskiwania w bezpiecznym miejscu z dala od komputera:

```
WARNING: ACTIONS REQUIRED:

1. Save this numerical recovery password in a secure location away from your computer:

064801-269808-233244-670472-692505-296219-620884-131241

To prevent data loss, save this password immediately. This password helps ensure that you can unlock the encrypted volume.
```

Aby zapobiec utracie danych, natychmiast zapisz to hasło. To hasło pomaga zapewnić odblokowanie zaszyfrowanego woluminu.

Oto dane wyjściowe polecenia.

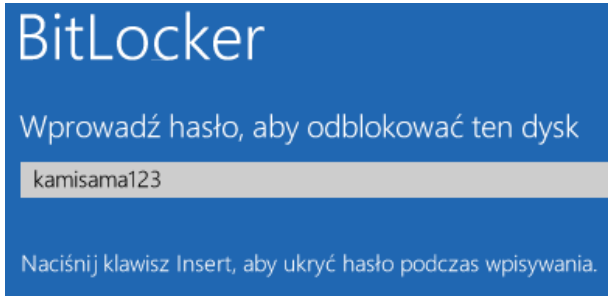
```
VolumeType      Mount Point CapacityGB VolumeStatus            Encryption Percentage KeyProtector            AutoUnlock Enabled Protection Status
----------      ----------- ---------- ------------            --------------------- ------------            ------------------ ----------
OperatingSystem C:            1 023,12 FullyDecrypted          0                     {Password, RecoveryPas...                  Off
```

Zrestartuj komputer.

Restart-Computer

```
Restart-Computer
```

Komputer poprosi o hasło, aby rozpocząć.



Zaszyfrowałeś dysk systemowy za pomocą funkcji Bitlocker i hasła.