

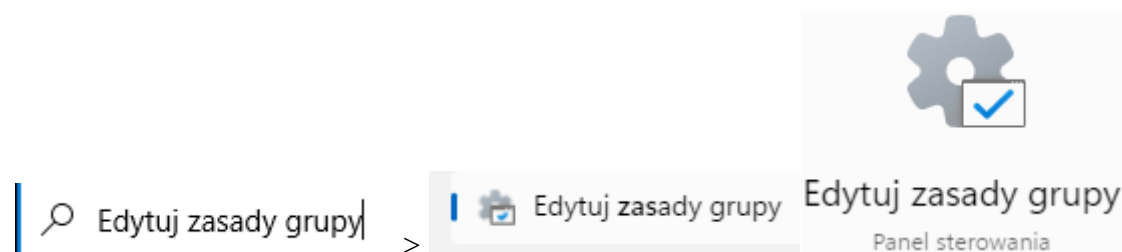
## **Powershell - zaszyfruj dysk za pomocą funkcji Bitlocker i hasła**

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**

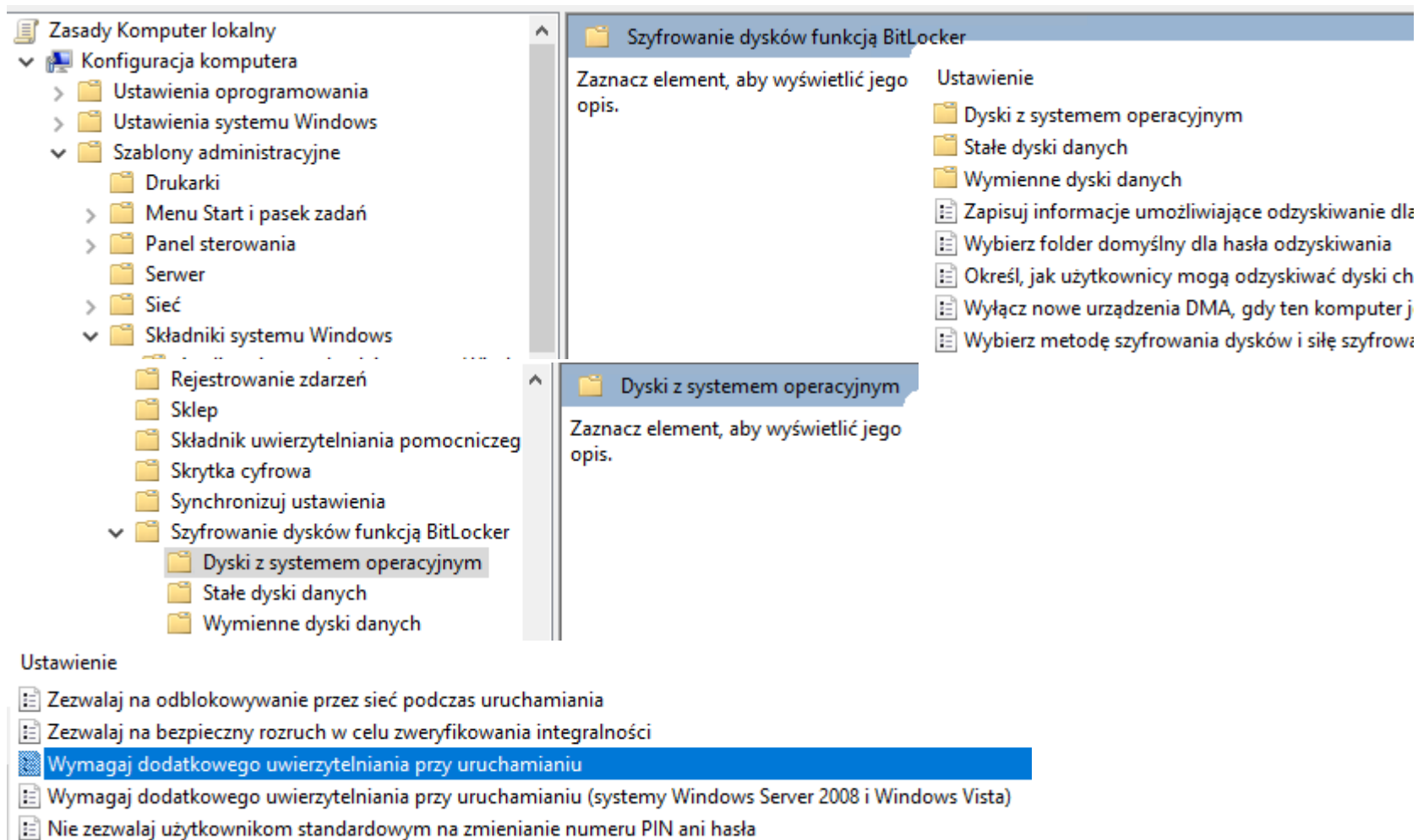
Jako administrator uruchom edytor zasad grupy.



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

Wymagaj dodatkowego uwierzytelniania przy uruchamianiu

Wymagaj dodatkowego uwierzytelniania przy uruchamianiu Poprzednie ustawienie Następne ustawienie

☐ Nie skonfigurowano  
☒ Włączone  
☐ Wyłączone

Komentarz:

Obsługiwane w: System Windows Server 2008 R2 lub nowszy albo system Windows 7

Opcje:

☒ Zezwalaj na używanie funkcji BitLocker bez zgodr (wymaga hasła lub klucza uruchomienia na dysku)

Ustawienia dla komputerów z modulem TPM:

Konfiguruj uruchomienie modułu TPM:

Zezwalaj na używanie modułu TPM

Konfiguruj numer PIN uruchomienia modułu TPM:

Zezwalaj na używanie numeru PIN uruchomienia z r

Konfiguruj klucz uruchomienia modułu TPM:

Zezwalaj na używanie klucza uruchomienia z modu

Konfiguruj klucz i numer PIN uruchomienia modułu

Zezwalaj na używanie klucza i numeru PIN uruchom

Pomoc:

To ustawienie zasad umożliwia określenie, czy funkcja BitLocker będzie wymagać dodatkowego uwierzytelniania przy każdym uruchomieniu komputera i czy funkcja BitLocker ma być używana wraz z modulem TPM, czy bez niego. Jest ono stosowane po włączeniu funkcji BitLocker.

Uwaga: przy uruchamianiu może być wymagana tylko jedna dodatkowa opcja uwierzytelniania. W przeciwnym razie wystąpi błąd zasad.

Aby używać funkcji BitLocker na komputerze bez modułu TPM, zaznacz pole wyboru „Zezwalaj na używanie funkcji BitLocker bez zgodnego modułu TPM”. W tym trybie do uruchomienia potrzebne jest hasło lub dysk USB. W przypadku korzystania z klucza uruchomienia informacje klucza służące do szyfrowania dysku są przechowywane na dysku USB — tworząc klucz USB. Gdy klucz USB zostanie włożony do portu USB, nastąpi uwierzytelnienie dostępu do dysku i dysk stanie się dostępny. Jeśli klucz USB zostanie utracony, będzie niedostępny lub użytkownik zapomni hasła, w celu uzyskania dostępu do dysku trzeba będzie użyć jednej z opcji odzyskiwania funkcji BitLocker.

OK Anuluj Zastosuj

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

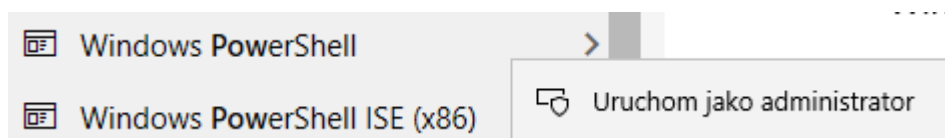
gpupdate /force

**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
ManufacturerVersionFull120 : 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 Point | CapacityGB | VolumeStatus   | Encryption Percentage | KeyProtector | AutoUnlock Enabled | Protection 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 Point      CapacityGB VolumeStatus      Encryption Percentage      KeyProtector      AutoUnlock Enabled      Protection 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.

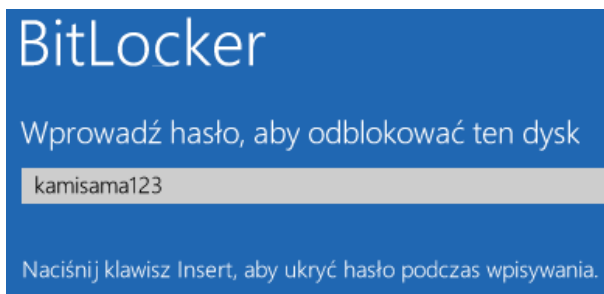
| VolumeType      | Mount Point | CapacityGB | VolumeStatus   | Encryption Percentage | KeyProtector              | AutoUnlock Enabled | Protection Status |
|-----------------|-------------|------------|----------------|-----------------------|---------------------------|--------------------|-------------------|
| 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.