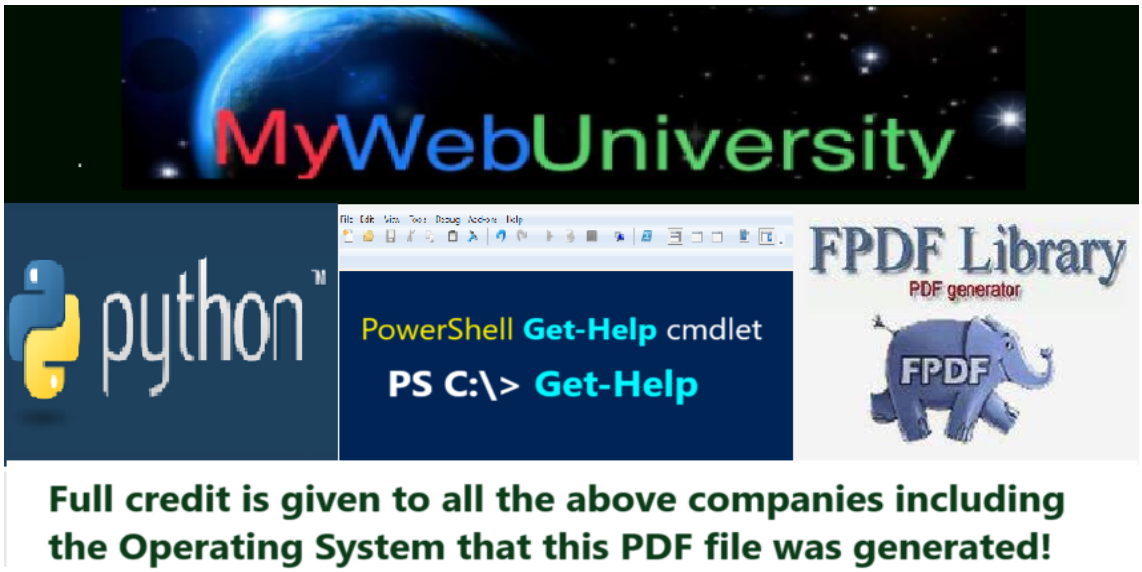

Windows PowerShell Get-Help on Cmdlet 'Enable-BitLocker'

PS:\>Get-HELP Enable-BitLocker -Full

NAME

Enable-BitLocker

SYNOPSIS

Enables BitLocker Drive Encryption for a volume.

SYNTAX

Enable-BitLocker [-MountPoint] <String[]> [-AdAccountOrGroup] <String> -AdAccountOrGroupProtector [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 |

XtsAes256}] [-HardwareEncryption] [-Service] [-SkipHardwareTest] [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [[-Password] <SecureString>] [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption]

-PasswordProtector [-SkipHardwareTest] [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [[-Pin] <SecureString>] [-StartupKeyPath] <String> [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}]

[-HardwareEncryption] [-SkipHardwareTest] -TpmAndPinAndStartupKeyProtector [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [[-Pin] <SecureString>] [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption]
[-SkipHardwareTest] -TpmAndPinProtector [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [-RecoveryKeyPath] <String> [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption]
-RecoveryKeyProtector [-SkipHardwareTest] [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [[-RecoveryPassword] <String>] [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}]
[-HardwareEncryption] -RecoveryPasswordProtector [-SkipHardwareTest] [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [-StartupKeyPath] <String> [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption]
[-SkipHardwareTest] -StartupKeyProtector [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [-StartupKeyPath] <String> [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption]
[-SkipHardwareTest] -TpmAndStartupKeyProtector [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

Enable-BitLocker [-MountPoint] <String[]> [-Confirm] [-EncryptionMethod {Aes128 | Aes256 | XtsAes128 | XtsAes256}] [-HardwareEncryption] [-SkipHardwareTest]
-TpmProtector [-UsedSpaceOnly] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Enable-BitLocker cmdlet enables BitLocker Drive Encryption for a volume.

When you enable encryption, you must specify a volume, either by its drive letter or by its BitLocker volume object.

You must also establish a key protector. BitLocker uses a key protector to encrypt the volume encryption key. When a

user accesses a BitLocker encrypted drive, such

as when starting a computer, BitLocker requests the relevant key protector. For example, the user can enter a PIN or provide a USB drive that contains a key.

BitLocker decrypts the encryption key and uses it to read data from the drive. You can use one of the following methods or combinations of methods for a key protector:

- Trusted Platform Module (TPM): BitLocker uses the computer's TPM to protect the encryption key. If you select this key protector, users can access the encrypted

drive as long as it is connected to the system board that hosts the TPM and system boot integrity is intact. In general, TPM-based protectors can only be

associated to an operating system volume.

- TPM and Personal Identification Number (PIN): BitLocker uses a combination of the TPM and a user-supplied PIN. A PIN is four to twenty digits or, if you allow

enhanced PINs, is four to twenty letters, symbols, spaces, or numbers.

- TPM, PIN, and startup key: BitLocker uses a combination of the TPM, a user-supplied PIN, and input from of a USB memory device that contains an external key.

- TPM and startup key: BitLocker uses a combination of the TPM and a USB flash drive that contains the external key.

- Startup key: BitLocker uses a USB flash drive that contains the external key.

- Password: BitLocker uses a password.

- Recovery key: BitLocker uses a recovery key stored as a specified file.

- Recovery password: BitLocker uses a recovery password.

- Active Directory Domain Services (AD DS) account: BitLocker uses domain authentication.

You can specify only one of these methods or combinations when you enable encryption, but you can use the Add-BitLockerKeyProtector cmdlet to add other protectors.

For a password or PIN key protector, specify a secure string. You can use the ConvertTo-SecureString cmdlet to create a secure string. You can use secure strings in a

script and still maintain confidentiality of passwords.

We strongly recommend specifying the encryption method. By default, BitLocker uses XTS-AES-128. You can opt XTS-AES-256 for stronger security. However, if you are

encrypting a removable media and intend to use it on Windows 8.1 or Windows Server 2012 R2, you must opt either AES-128 or AES-256 for backward compatibility. You may

request hardware encryption but we strongly advise against it. For further guidance, see the ADV180028 Security Advisory

(https://msrc.microsoft.com/update-guide/vulnerability/ADV180028).

This cmdlet returns a BitLocker volume object. If you choose recovery password as your key protector but do not specify a 48-digit recovery password, this cmdlet

generates a random one for you, and stores it in the RecoveryPassword field of the KeyProtector attribute of the BitLocker volume object.

If you use startup key or recovery key as part of your key protector, provide a path to store the key. This cmdlet stores the name of the file that contains the key

in the KeyFileName field of the KeyProtector field in the BitLocker volume object.

If you use the Enable-BitLocker cmdlet on an encrypted volume or on a volume with encryption in process, it takes no action. If you use the cmdlet on a drive that has

encryption paused, it resumes encryption on the volume.

By default, this cmdlet encrypts the entire drive. If you use the UsedSpaceOnly parameter, it only encrypts the used space on the disk. This option can significantly

reduce encryption time.

It is common practice to add a recovery password for an operating system volume using the Add-BitLockerKeyProtector cmdlet, save the recovery password using the

Backup-BitLockerKeyProtector cmdlet, and then enable BitLocker on that volume. This procedure ensures that you have

a recovery option.

For an overview of BitLocker, see the BitLocker Drive Encryption Overview (/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732774(v=ws.11)).

PARAMETERS

-AdAccountOrGroup <String>

Specifies an account using the format Domain\User. This cmdlet adds the account you specify as a key protector for the volume encryption key.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-AdAccountOrGroupProtector [<SwitchParameter>]

Indicates that BitLocker uses an AD DS account as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-EncryptionMethod <BitLockerVolumeEncryptionMethodOnEnable>

Specifies an encryption method for the encrypted drive. For further guidance, see the ADV180028 Security Advisory (https://msrc.microsoft.com/update-guide/vulnerability/ADV180028).

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-HardwareEncryption [<SwitchParameter>]

Indicates that the volume uses hardware encryption. We strongly advise against hardware encryption. For further guidance, see the ADV180028 Security Advisory (https://msrc.microsoft.com/update-guide/vulnerability/ADV180028).

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-MountPoint <String[]>

Specifies an array of drive letters or BitLocker volume objects. This cmdlet enables protection for the volumes specified. To obtain a BitLocker volume object, use the Get-BitLockerVolume cmdlet.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName, ByValue)

Accept wildcard characters? false

-Password <SecureString>

Specifies a secure string object that contains a password. The password specified acts as a protector for the volume encryption key.

Required? false

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PasswordProtector [<SwitchParameter>]

Indicates that BitLocker uses a password as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Pin <SecureString>

Specifies a secure string object that contains a PIN. BitLocker uses the PIN specified, with other data, as a protector for the volume encryption key.

Required? false

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RecoveryKeyPath <String>

Specifies a path to a folder. This cmdlet adds a randomly generated recovery key as a protector for the volume encryption key and stores it in the specified path.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RecoveryKeyProtector [<SwitchParameter>]

Indicates that BitLocker uses a recovery key as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-RecoveryPassword <String>

Specifies a recovery password. If you do not specify this parameter, but you do include the RecoveryPasswordProtector parameter, the cmdlet creates a random

password. You can enter a 48-digit password. The password specified or created acts as a protector for the volume encryption key.

Required? false

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RecoveryPasswordProtector [<SwitchParameter>]

Indicates that BitLocker uses a recovery password as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Service [<SwitchParameter>]

Indicates that the system account for this computer unlocks the encrypted volume.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-SkipHardwareTest [<SwitchParameter>]

Indicates that BitLocker does not perform a hardware test before it begins encryption. BitLocker uses a hardware test as a dry run to make sure that all the key

protectors are correctly set up and that the computer can start without issues.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-StartupKeyPath <String>

Specifies a path to a startup key. The key stored in the specified path acts as a protector for the volume encryption key.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-StartupKeyProtector [<SwitchParameter>]

Indicates that BitLocker uses a startup key as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-TpmAndPinAndStartupKeyProtector [<SwitchParameter>]

Indicates that BitLocker uses a combination of the TPM, a PIN, and a startup key as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-TpmAndPinProtector [<SwitchParameter>]

Indicates that BitLocker uses a combination of the TPM and a PIN as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-TpmAndStartupKeyProtector [<SwitchParameter>]

Indicates that BitLocker uses a combination of the TPM and a startup key as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-TpmProtector [<SwitchParameter>]

Indicates that BitLocker uses the TPM as a protector for the volume encryption key.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-UsedSpaceOnly [<SwitchParameter>]

Indicates that BitLocker does not encrypt unallocated disk space.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

BitLockerVolume[], String[]

OUTPUTS

BitLockerVolume[]

NOTES

---------- Example 1: Enable BitLocker ----------

$SecureString = ConvertTo-SecureString "1234" -AsPlainText -Force

Enable-BitLocker -MountPoint "C:" -EncryptionMethod Aes256 -UsedSpaceOnly -Pin $SecureString -TPMandPinProtector

This example enables BitLocker for a specified drive using the TPM and a PIN for key protector.

The first command uses the ConvertTo-SecureString cmdlet to create a secure string that contains a PIN and saves that string in the $SecureString variable. For more

information about the ConvertTo-SecureString cmdlet, type `Get-Help ConvertTo-SecureString`.

The second command enables BitLocker encryption for the BitLocker volume that has the drive letter C:. The cmdlet specifies an encryption algorithm and the PIN saved

in the $SecureString variable. The command also specifies that this volume uses a combination of the TPM and the PIN as key protector. The command also specifies to

encrypt the used space data on the disk, instead of the entire volume. When the system writes data to the volume in the future, that data is encrypted.

------- Example 2: Enable BitLocker with a recovery key -------

Get-BitLockerVolume | Enable-BitLocker -EncryptionMethod Aes128 -RecoveryKeyPath "E:\Recovery\" -RecoveryKeyProtector

This command gets all the BitLocker volumes for the current computer and passes pipes them to the Enable-BitLocker cmdlet by using the pipe operator. This cmdlet

specifies an encryption algorithm for the volume or volumes. This cmdlet specifies a path to a folder where the randomly generated recovery key will be stored and

indicates that these volumes use a recovery key as a key protector.

-- Example 3: Enable BitLocker with a specified user account --

Enable-BitLocker -MountPoint "C:" -EncryptionMethod Aes128 -AdAccountOrGroup "Western\SarahJones" -AdAccountOrGroupProtector

This command encrypts the BitLocker volume specified by the MountPoint parameter, and uses the AES 128 encryption method. The command also specifies an account and

specifies that BitLocker uses user credentials as a key protector. When a user accesses this volume, BitLocker prompts for credentials for the user account

Western\SarahJones.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/bitlocker/enable-bitlocker?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Disable-BitLocker

Get-BitLockerVolume

Lock-BitLocker

Resume-BitLocker

Suspend-BitLocker