PowerShell Get-Help on command 'Add-BitLockerKeyProtector'

PS C:\Users\wahid> Get-Help Add-BitLockerKeyProtector

```
NAME
    Add-BitLockerKeyProtector


SYNOPSIS
    Adds a key protector for a BitLocker volume.



SYNTAX
    Add-BitLockerKeyProtector [-MountPoint] <String[]> [-ADAccountOrGroup]
    <String> -ADAccountOrGroupProtector [-Confirm] [-Service] [-WhatIf]
    [<CommonParameters>]

    Add-BitLockerKeyProtector [-MountPoint] <String[]> [[-Password]
    <SecureString>] [-Confirm] -PasswordProtector [-WhatIf] [<CommonParameters>]

    Add-BitLockerKeyProtector [-MountPoint] <String[]> [[-Pin] <SecureString>]
    [-StartupKeyPath] <String> [-Confirm] -TpmAndPinAndStartupKeyProtector
    [-WhatIf] [<CommonParameters>]

    Add-BitLockerKeyProtector [-MountPoint] <String[]> [[-Pin] <SecureString>]
    [-Confirm] -TpmAndPinProtector [-WhatIf] [<CommonParameters>]
```

```
Add-BitLockerKeyProtector [-MountPoint] <String[]> [-RecoveryKeyPath] <String>
[-Confirm] -RecoveryKeyProtector [-WhatIf] [<CommonParameters>]

Add-BitLockerKeyProtector [-MountPoint] <String[]> [[-RecoveryPassword]
<String>] [-Confirm] -RecoveryPasswordProtector [-WhatIf] [<CommonParameters>]

Add-BitLockerKeyProtector [-MountPoint] <String[]> [-StartupKeyPath] <String>
[-Confirm] -StartupKeyProtector [-WhatIf] [<CommonParameters>]

Add-BitLockerKeyProtector [-MountPoint] <String[]> [-StartupKeyPath] <String>
[-Confirm] -TpmAndStartupKeyProtector [-WhatIf] [<CommonParameters>]

Add-BitLockerKeyProtector [-MountPoint] <String[]> [-Confirm] -TpmProtector
[-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The Add-BitLockerKeyProtector cmdlet adds a protector for the volume key of the volume protected with BitLocker Drive Encryption.

When a user accesses a drive protected by BitLocker, 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 retrieves 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 specify this protector, users can access the encrypted drive as long as it is connected to the system board that hosts the TPM and the 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, 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 input from of a USB memory device. - Startup key. BitLocker uses input from of a USB memory device that contains the external key. - Password. BitLocker uses a password. - Recovery key. BitLocker uses a recovery key stored as a specified file in a USB memory device. - Recovery password. BitLocker uses a recovery password. - Active Directory Domain Services (AD DS) account. BitLocker uses domain authentication to unlock data volumes. Operating system volumes cannot use this type of key protector.

You can add only one of these methods or combinations at a time, but you can run this cmdlet more than once on a volume.

Adding a key protector is a single operation; for example, adding a startup key protector to a volume that uses the TPM and PIN combination as a key protector results in two key protectors, not a single key protector that uses TPM, PIN, and startup key. Instead, add a protector that uses TPM, PIN, and startup key and then remove the TPM and PIN protector by using the Remove-BitLockerKeyProtector cmdlet.

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.

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 creates a random 48-digit recovery password. The cmdlet stores the password as 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.

For an overview of BitLocker, see BitLocker Drive Encryption Overview (https://technet.microsoft.com/en-us/library/cc732774.aspx)on TechNet.

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.

-ADAccountOrGroupProtector [<SwitchParameter>]

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

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-MountPoint <String[]>

Specifies an array of drive letters or BitLocker volume objects. This cmdlet adds a key protector to the volumes specified. To obtain a BitLocker volume object, use the Get-BitLockerVolume cmdlet.

-Password <SecureString>

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

-PasswordProtector [<SwitchParameter>]

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

-Pin <SecureString>

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

-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.

-RecoveryKeyProtector [<SwitchParameter>]

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

-RecoveryPassword <String>

Specifies a recovery password. If you do not specify this parameter, the cmdlet creates a random password. You can enter a 48 digit password. The cmdlet adds the password specified or created as a protector for the volume encryption key.

-RecoveryPasswordProtector [<SwitchParameter>]

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

-Service [<SwitchParameter>]

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

-StartupKeyPath <String>

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

-StartupKeyProtector [<SwitchParameter>]

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

-TpmAndPinAndStartupKeyProtector [<SwitchParameter>]

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

-TpmAndPinProtector [<SwitchParameter>]

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

-TpmAndStartupKeyProtector [<SwitchParameter>]

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

-TpmProtector [<SwitchParameter>]

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

-WhatIf [<SwitchParameter>]

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

<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).

----------------- Example 1: Add key protector -----------------

```
PS C:\>$SecureString = ConvertTo-SecureString "1234" -AsPlainText -Force
PS C:\>Add-BitLockerKeyProtector -MountPoint "C:" -Pin $SecureString
-TPMandPinProtector
```

This example adds a combination of the TPM and a PIN as key protector for the BitLocker volume identified with the drive letter C:.

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 adds a protector to the BitLocker volume that has the drive letter C:. The command specifies that this volume uses a combination of the TPM and the PIN as key protector and provides the PIN saved in the $SecureString variable.

--- Example 2: Add a recovery key for all BitLocker volumes ---

```
PS C:\>Get-BitLockerVolume | Add-BitLockerKeyProtector -RecoveryKeyPath
"E:\Recovery\" -RecoveryKeyProtector
```

This command gets all the BitLocker volumes for the current computer and passes them to the Add-BitLockerKeyProtector cmdlet by using the pipe operator. 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: Add credentials as a key protector --------

```
PS C:\>Add-BitLockerKeyProtector -MountPoint "C:" -AdAccountOrGroup
"Western\SarahJones" -AdAccountOrGroupProtector
```

This command adds an AD DS account key protector to the BitLocker volume specified by the MountPoint parameter. The command 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.

REMARKS

To see the examples, type: "get-help Add-BitLockerKeyProtector -examples".

For more information, type: "get-help Add-BitLockerKeyProtector -detailed".

For technical information, type: "get-help Add-BitLockerKeyProtector -full".

For online help, type: "get-help Add-BitLockerKeyProtector -online"