



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

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

NAME

Unlock-BitLocker

SYNOPSIS

Restores access to data on a BitLocker volume.

SYNTAX

Unlock-BitLocker [-MountPoint] <String[]> -AdAccountOrGroup [-Confirm] [-WhatIf] [<CommonParameters>]

Unlock-BitLocker [-MountPoint] <String[]> [-Confirm] -Password <SecureString> [-WhatIf] [<CommonParameters>]

Unlock-BitLocker [-MountPoint] <String[]> [-Confirm] -RecoveryKeyPath <String> [-WhatIf] [<CommonParameters>]

Unlock-BitLocker [-MountPoint] <String[]> [-Confirm] -RecoveryPassword <String> [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Unlock-BitLocker cmdlet restores access to encrypted data on a volume that uses BitLocker Drive Encryption. You can use the Lock-BitLocker cmdlet to prevent

access.

In order to restore access, provide one of the following key protectors for the volume:

- Active Directory Domain Services (AD DS) account
- Password
- Recovery key
- Recovery password

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

PARAMETERS

-AdAccountOrGroup [<SwitchParameter>]

Indicates that BitLocker requires account credentials to unlock the volume. In order to use this parameter, the account for the current user must be a key protector for the volume.

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

-MountPoint <String[]>

Specifies an array of drive letters or BitLocker volume objects. The cmdlet unlocks 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 that contains a password. The password specified acts as a protector for the volume encryption key.

Required?	true
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-RecoveryKeyPath <String>

Specifies the path to a folder where recovery keys are stored. The key stored in the specified path, if found, acts as a protector for the volume encryption.

Required?	true
Position?	named

Default value None
Accept pipeline input? False
Accept wildcard characters? false

-RecoveryPassword <String>

Specifies a recovery password. The password specified acts as a protector for the volume encryption key.

Required? true
Position? named
Default value None
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: Unlock a volume -----

```
PS C:\> $SecureString = ConvertTo-SecureString "fjuksAS1337" -AsPlainText -Force
```

```
PS C:\> Unlock-BitLocker -MountPoint "E:" -Password $SecureString
```

This example unlocks a specified BitLocker volume by using a password.

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

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

The second command unlocks the specified BitLocker volume by using the password saved in the \$SecureString variable.

RELATED LINKS

Online

Version:

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

Disable-BitLocker

Enable-BitLocker

Get-BitLockerVolume

Lock-BitLocker

Resume-BitLocker

Suspend-BitLocker

