

# Windows

## Get Bitlocker Encryption Status with manage-bde

Manage-bde is the command to manage everything Bitlocker related. To view your encryption status:

From an elevated command prompt (right click, run as administrator):

```
manage-bde -status
```

Here's the full program syntax and options from Microsoft:

### Syntax

```
manage-bde [-status] [-on] [-off] [-pause] [-resume] [-lock] [-unlock] [-autounlock]
  [-protectors] [-tpm]
  [-setidentifier] [-forcerecovery] [-changepassword] [-changePIN] [-changekey] [-key
  ackage] [-upgrade] [-wipefreespace] [{-?|/?}] [{-help|-h}]
```

### Parameters

Parameter	Description
<a href="#">manage-bde status</a>	Provides information about all drives on the computer, whether or not they are BitLocker-protected.
<a href="#">manage-bde on</a>	Encrypts the drive and turns on BitLocker.
<a href="#">manage-bde off</a>	Decrypts the drive and turns off BitLocker. All key protectors are removed when decryption is complete.
<a href="#">manage-bde pause</a>	Pauses encryption or decryption.
<a href="#">manage-bde resume</a>	Resumes encryption or decryption.
<a href="#">manage-bde lock</a>	Prevents access to BitLocker-protected data.
<a href="#">manage-bde unlock</a>	Allows access to BitLocker-protected data with a recovery password or a recovery key.
<a href="#">manage-bde autounlock</a>	Manages automatic unlocking of data drives.
<a href="#">manage-bde protectors</a>	Manages protection methods for the encryption key.
<a href="#">manage-bde tpm</a>	Configures the computer's Trusted Platform Module (TPM). This command isn't supported on computers running Windows 8 or <b>win8_server_2</b> . To manage the TPM on these computers, use either the TPM Management MMC snap-in or the TPM Management cmdlets for Windows PowerShell.
<a href="#">manage-bde setidentifier</a>	Sets the drive identifier field on the drive to the value specified in the <b>Provide the unique identifiers for your organization</b> Group Policy setting.
<a href="#">manage-bde ForceRecovery</a>	Forces a BitLocker-protected drive into recovery mode on restart. This command deletes all TPM-related key protectors from the drive. When the computer restarts, only a recovery password or recovery key can be used to unlock the drive.

# Windows

Parameter	Description
<a href="#">manage-bde changepassword</a>	Modifies the password for a data drive.
<a href="#">manage-bde changepin</a>	Modifies the PIN for an operating system drive.
<a href="#">manage-bde changekey</a>	Modifies the startup key for an operating system drive.
<a href="#">manage-bde KeyPackage</a>	Generates a key package for a drive.
<a href="#">manage-bde upgrade</a>	Upgrades the BitLocker version.
<a href="#">manage-bde WipeFreeSpace</a>	Wipes the free space on a drive.
-? or /?	Displays brief Help at the command prompt.
-help or -h	Displays complete Help at the command prompt.

Unique solution ID: #1104

Author: n/a

Last update: 2021-06-29 12:54