



Windows Vista™

## Windows BitLocker Drive Encryption Step-by-Step Guide

---

Microsoft Corporation

Published: September 2006

### **Abstract**

Microsoft® Windows® BitLocker™ Drive Encryption is a new hardware-enhanced feature in the Microsoft Windows Vista™ operating system that provides better off-line data protection for your computer. This guide includes system requirements and step-by-step instructions on how to use BitLocker Drive Encryption in a test lab environment.

**Microsoft**

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release, and is the confidential and proprietary information of Microsoft Corporation. It is disclosed pursuant to a non-disclosure agreement between the recipient and Microsoft. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Active Directory, BitLocker, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

References to any third-party products or their hardware identifiers are for illustrative purposes only. These products are not endorsed by Microsoft Corporation.

All other trademarks are property of their respective owners.

# Contents

---

Windows BitLocker Drive Encryption Step-by-Step Guide .....	5
What is BitLocker Drive Encryption? .....	5
Who should use BitLocker Drive Encryption? .....	5
In this guide .....	6
Requirements for BitLocker Drive Encryption.....	6
Hardware and software requirements .....	6
Scenario 1: Partitioning a Hard Disk for BitLocker Drive Encryption.....	7
Partition a disk with no operating system for BitLocker .....	7
Scenario 2: Turn On BitLocker Drive Encryption.....	9
Before you start .....	9
Scenario 3: Turning on BitLocker Drive Encryption on a Computer Without a Compatible TPM.....	11
Before you start .....	11
Scenario 4: Recovering Data Protected by BitLocker Drive Encryption.....	13
Scenario 5: Turning off BitLocker Drive Encryption.....	15
Before you start .....	15
Logging Bugs and Feedback .....	16
Additional Resources .....	16



# Windows BitLocker Drive Encryption Step-by-Step Guide

---

This step-by-step guide provides the instructions you need to use Microsoft® Windows® BitLocker™ Drive Encryption in a test environment. We recommend that you first use the steps provided in this guide in a test lab environment. Step-by-step guides are not necessarily meant to be used to deploy Microsoft® Windows Vista™ operating system features without accompanying documentation (as listed in the Additional Resources section) and should be used with discretion as a stand-alone document.

## What is BitLocker Drive Encryption?

BitLocker Drive Encryption is an integral new security feature in the Windows Vista operating system that provides considerable protection for the operating system on your computer and data stored on the operating system volume. BitLocker ensures that data stored on a computer running Windows Vista remains encrypted even if the computer is tampered with when the operating system is not running. This helps protect against "offline attacks," attacks made by disabling or circumventing the installed operating system, or made by physically removing the hard drive to attack the data separately.

BitLocker uses a Trusted Platform Module (TPM) to provide enhanced protection for your data and to assure early boot component integrity. This helps protect your data from theft or unauthorized viewing by encrypting the entire Windows volume.

BitLocker is designed to offer a seamless user experience. It is designed for systems that have a compatible TPM microchip and BIOS. A compatible TPM is defined as a version 1.2 TPM. A compatible BIOS must support the TPM and the Static Root of Trust Measurement as defined by the Trusted Computing Group. For more information about TPM specifications, visit the TPM Specifications section of the Trusted Computing Group's Web site (<http://go.microsoft.com/fwlink/?LinkId=72757>).

The TPM interacts with BitLocker to help provide seamless protection at system startup. This is transparent to the user, and the user logon experience is unchanged. However, if the TPM is missing or changed, or if the startup information has changed, BitLocker will enter recovery mode, and you will need a recovery password to regain access to the data.

## Who should use BitLocker Drive Encryption?

This guide is intended for the following audiences:

- IT planners and analysts who are evaluating the product
- Early adopters
- Security architects

## In this guide

The purpose of this guide is to help administrators become familiar with the BitLocker Drive Encryption feature of Windows Vista. The sections below provide basic information and procedures that administrators need to start configuring and deploying BitLocker within their networks.

Scenario 1 provides instructions for creating the two partitions required for BitLocker Drive Encryption. Scenario 2 explains how to encrypt a drive using BitLocker and a TPM. Scenario 3 describes using BitLocker on a computer without a TPM. Scenario 4 describes how to access encrypted data after lockdown, and how to test BitLocker by generating a lockdown. Scenario 5 guides you through turning off BitLocker.

- [Requirements for BitLocker Drive Encryption](#)
- [Scenario 1: Partitioning a Hard Drive for BitLocker Drive Encryption](#)
- [Scenario 2: Turning on Basic BitLocker Drive Encryption](#)
- [Scenario 3: Turning on BitLocker Drive Encryption on a Computer Without a Compatible TPM](#)
- [Scenario 4: Recovering Data Protected by BitLocker Drive Encryption](#)
- [Scenario 5: Turning off BitLocker Drive Encryption](#)
- [Logging Bugs and Feedback](#)
- [Additional Resources](#)

## Requirements for BitLocker Drive Encryption

These steps are for testing only. This guide should not be the only resource you use to deploy Microsoft Windows Server® Code Name "Longhorn" or Windows Vista features.

### Note

We strongly recommend that you do not run a debugger when BitLocker is enabled. Running a debugger on your BitLocker-enabled computer requires you to follow the recovery process every time you restart the computer.

## Hardware and software requirements

- A computer that meets the minimum requirements for Windows Vista.

- A TPM microchip, version 1.2, turned on. (Scenarios 2 and 3).
- A Trusted Computing Group (TCG)-compliant BIOS (Scenarios 2 and 3).
- Two NTFS drive partitions, one for the system volume and one for the operating system volume. The system volume partition must be at least 1.5 gigabytes (GB) and set as the active partition (Scenario 1).
- A BIOS setting to start up first from the hard drive, not the USB or CD drives.

 **Note**

For any test that includes the USB flash drive, your BIOS must support reading USB flash drives at startup

## Scenario 1: Partitioning a Hard Disk for BitLocker Drive Encryption

For BitLocker to work, you must have at least two partitions on your hard disk. The first partition is the system volume and labeled S in this document. This volume contains the boot information in an unencrypted space. The second partition is the operating system volume and labeled C in this document. This volume is encrypted and contains the operating system and user data.

The partitions must be created before installing Windows Vista.

 **Note**

In some situations, a volume can involve multiple partitions. This document discusses only simple volumes, where a volume and a partition are functionally equivalent. BitLocker works with volumes, a logical structure; but many disk tools are concerned with physical disk partitions.

Scenario 1 describes how to create the two partitions required for BitLocker. This procedure assumes that you have backed up any data on the disk.

- If you have an unused disk with a single partition, follow the steps in [Partition a drive with no operating system for BitLocker](#).

 **Note**

Make sure that you have backed up any data and that you have your product key for Windows Vista.

### Partition a disk with no operating system for BitLocker

In this procedure you start the computer from the product DVD and then enter a series of commands to do the following:

- Create a new 1.5 GB primary partition.

- Set this partition as active.
- Create a second primary partition using the rest of the space on the disk.
- Format both new partitions so they can be used as Windows volumes.
- Install Windows Vista on the larger volume (drive C).

 **Note**

You must create a second active partition for BitLocker to work properly.

Your drive letters might not correspond to those in this example. In this example, the operating system volume is labeled C, and the system volume is labeled S (for system volume). In this example, we also assume that the system has only one physical hard disk drive.

 **To partition a disk with no operating system for BitLocker**

1. Start the computer from the Windows Vista product DVD.
2. In the initial **Install Windows** screen, choose your **Installation language, Time and currency format**, and **Keyboard layout**, and then click **Next**.
3. In the next **Install Windows** screen, click **System Recovery Options**, located in the lower left of the screen.
4. In the **System Recovery Options** dialog box, choose your keyboard layout, and then click **Next**.
5. In the next **System Recovery Options** dialog box, make sure no operating system is selected. To do this, click in the empty area of the **Operating System** list, below any listed entries. Then click **Next**.
6. In the next **System Recovery Options** dialog box, click **Command Prompt**.
7. Use Diskpart to create the partition for the operating system volume. At the command prompt, type **diskpart**, and then press ENTER.
8. Type **select disk 0**.
9. Type **clean** to erase the existing partition table.
10. Type **create partition primary size=1500** to set the partition you are creating as a primary partition.
11. Type **assign letter=S** to give this partition the S designator.
12. Type **active** to set the new partition as the active partition.
13. Type **create partition primary** to create another primary partition. You will install Windows on this larger partition.
14. Type **assign letter=C** to give this partition the C designator.
15. Type **list volume** to see a display of all the volumes on this disk. You will see a

listing of each volume, volume numbers, letters, labels, file systems, types, sizes, status, and information. Check that you have two volumes and that you know the label used for each volume.

16. Type **exit** to leave the diskpart application.
17. Type **format c: /y /q /fs:NTFS** to properly format the C volume.
18. Type **format s: /y /q /fs:NTFS** to properly format the S volume.
19. Type **exit** to leave the command prompt.
20. In the **System Recovery Options** window, use the close window icon in the upper right (or press ALT+F4) to close the window to return to the main installation screen. (Do not click **Shut Down** or **Restart**.)
21. Click **Install now** and proceed with the Windows Vista installation process. Install Windows Vista on the larger volume, C: (the operating system volume).

## Scenario 2: Turn On BitLocker Drive Encryption

Scenario 2 outlines the procedures for turning on BitLocker Drive Encryption protection on a system with a TPM. After the volume is encrypted, the user logs onto the computer normally.

Use the following procedure to turn on BitLocker Drive Encryption.

### Before you start

- You must be logged on as an administrator.
- You can configure a printer to print recovery passwords.

### To turn on BitLocker Drive Encryption

1. Click **Start**, click **Control Panel**, click **Security**, and then click **BitLocker Drive Encryption**.
2. If the **User Account Control** message appears, verify that the proposed action is what you requested, and then click **Continue**. For more information, see "Additional Resources" later in this document.
3. On the **BitLocker Drive Encryption** page, click **Turn On BitLocker** on the operating system volume.  
If your TPM is not initialized, you will see the **Initialize TPM Security Hardware** wizard. Follow the directions to initialize the TPM and restart your computer.
4. On the **Save the recovery password** page, you will see the following options:

- **Save the password on a USB drive.** Saves the password to a USB flash drive.
- **Save the password in a folder.** Saves the password to a network drive or other location.
- **Print the password.** Prints the password.

Use one or more of these options to preserve the recovery password. For each option, select the option and follow the wizard steps to set the location for saving or printing the recovery password.

When you have finished saving the recovery password, click **Next**.



#### **Important**

The recovery password will be required in the event the encrypted drive must be moved to another computer, or changes are made to the system startup information. This password is so important that it is recommended that you make additional copies of the password stored in safe places to assure you access to your data. You will need your recovery password to unlock the encrypted data on the volume if BitLocker enters a locked state (see [Scenario 4: Recovering Data Protected by BitLocker Drive Encryption](#)). This recovery password is unique to this particular BitLocker encryption. You cannot use it to recover encrypted data from any other BitLocker encryption session.



#### **Important**

Store recovery passwords apart from the computer for maximum security.

5. On the **Encrypt the selected disk volume** page, confirm that the **Run BitLocker System Check** check box is selected, and then click **Continue**.  
Confirm that you want to restart the computer by clicking **Restart Now**. The computer restarts and BitLocker verifies if the computer is BitLocker-compatible and ready for encryption. If it is not, you will see an error message alerting you to the problem.
6. If it is ready for encryption, the **Encryption in Progress** status bar is displayed. You can monitor the ongoing completion status of the disk volume encryption by dragging your mouse cursor over the BitLocker Drive Encryption icon in the tool bar at the bottom of your screen. .

By completing this procedure, you have encrypted the operating system volume and created a recovery password unique to this volume. The next time you log on, you will see no change. If the TPM ever changes or cannot be accessed, if there are changes to key system files, or if someone tries to start the computer

from a disk to circumvent the operating system, the computer will switch to recovery mode until the recovery password is supplied.

## Scenario 3: Turning on BitLocker Drive Encryption on a Computer Without a Compatible TPM

Use the following procedure to change your computer's Group Policy settings so that you can turn on BitLocker Drive Encryption without a TPM. Instead of a TPM, you will use a startup key to authenticate yourself. The startup key is located on a USB flash drive inserted into the computer before the computer is turned on. For this scenario, you must have a BIOS that will read USB flash drives in the pre-operating system environment (at startup). Your BIOS can be checked by the Hardware Test at the end of the BitLocker wizard.

### Before you start

- You must be logged on as an administrator.
- You must have a USB flash drive to save the recovery password.
- We recommend a second USB flash drive to store the startup key separate from the recovery password.

### ▶ To turn on BitLocker Drive Encryption on a computer without a compatible TPM

1. Click **Start**, type **gpedit.msc** in the **Start Search** box, and then press ENTER.
2. If the **User Account Control** dialog box appears, verify that the proposed action is what you requested, and then click **Continue**. For more information, see "Additional Resources" later in this document.
3. In the **Group Policy Object Editor** console tree, click **Local Computer Policy**, click **Administrative Templates**, click **Windows Components**, and then double-click **BitLocker Drive Encryption**.
4. Double-click the setting **Control Panel Setup: Enable Advanced Startup Options**. The **Control Panel Setup: Enable Advanced Startup Options** dialog box appears.
5. Select the **Enabled** option, select the **Allow BitLocker without a compatible TPM** check box, and then click **OK**.

You have changed the policy setting so that you can use a startup key instead of a TPM.

6. Close the **Group Policy Object Editor**.
7. To force Group Policy to apply immediately, you can click **Start**, type **gpupdate.exe /force** in the **Start Search** box, and then press ENTER.
8. Click **Start**, click **Control Panel**, click **Security**, and then click **BitLocker Drive Encryption**.
9. If the **User Account Control** message appears, verify that the proposed action is what you requested, and then click **Continue**. For more information, see "Additional Resources" later in this document.
10. On the **BitLocker Drive Encryption** page, click **Turn On BitLocker**. This will only appear under the on the operating system volume.
11. On the **Set BitLocker Startup Preferences** page, select the **Require Startup USB Key at every startup** option. This is the only option available for non-TPM configurations. This key must be inserted each time before you start the computer.
12. Insert your USB flash drive in the computer, if it is not already there.
13. On the **Save your Startup Key** page, choose the location of your USB flash drive, and then click **Save**.
14. On the **Save the recovery password** page, you will see the following options:
  - **Save the password on a USB drive**. Saves the password to a USB flash drive.
  - **Save the password in a folder**. Saves the password to a network drive or other location.
  - **Print the password**. Prints the password.

Use one or more of these options to preserve the recovery password. For each option, select the option and follow the wizard steps to set the location for saving or printing the recovery password.

When you have finished saving the recovery password, click **Next**.

#### **Important**

The recovery password will be required in the event the encrypted drive must be moved to another computer, or changes are made to the system startup information. This password is so important that it is recommended that you make additional copies of the password stored in safe places to assure you access to your data. You will need your recovery password to unlock the encrypted data on the volume if BitLocker enters a locked state (see [Scenario 4: Recovering Data Protected by BitLocker Drive Encryption](#)). This recovery password is unique to this particular BitLocker encryption. You cannot use it to

recover encrypted data from any other BitLocker encryption session.

 **Important**

Store recovery passwords apart from the computer for maximum security.

15. On the **Encrypt the selected disk volume** page, confirm that the **Run BitLocker System Check** check box is selected, and then click **Continue**.  
Confirm that you want to restart the computer by clicking **Restart Now**. The computer restarts and BitLocker ensures that the computer is BitLocker-compatible and ready for encryption. If it is not, you will see an error message alerting you to the problem before encryption starts.
16. If it is ready for encryption, the **Encryption in Progress** status bar is displayed. You can monitor the ongoing completion status of the disk volume encryption by dragging your mouse cursor over the BitLocker Drive Encryption icon in the tool bar at the bottom of your screen or clicking on the Encryption balloon.  
By completing this procedure, you have encrypted the operating system volume and created a recovery password unique to that volume. The next time you turn your computer on, the USB flash drive must be plugged into a USB port on the computer. If it is not, you will not be able to access data on your encrypted volume. Store the startup key away from the computer to increase security.  
If you do not have the USB flash drive containing your startup key, then to access the data, you will need to use recovery mode and supply the recovery password.

## Scenario 4: Recovering Data Protected by BitLocker Drive Encryption

Scenario 4 describes the process for recovering your data after BitLocker has entered recovery mode. BitLocker locks the computer when a disk encryption key is not available. The following is a list of likely causes:

- An error related to TPM occurs.
- One of the early boot files is modified.
- The TPM is inadvertently turned off and the computer is turned off.
- The TPM is inadvertently cleared and the computer is turned off.

When a computer is locked, the startup process is interrupted very early, before the operating system starts. You must use the recovery password from a USB flash drive, or use the function keys to enter the recovery password. F1 through F9 represent the digits 1 through 9, and F10 represents 0.

Because recovery happens so early in the startup process, the accessibility features of Windows are not available. If you require accessibility features, consider what you will do in the event of recovery.

This scenario includes two steps:

- Testing data recovery
- Recovering data

▶ **To test data recovery**

1. Click **Start**, click **All Programs**, click **Accessories**, and then click **Run**.
2. Type **tpm.msc** in the **Open** box, and then click **OK**. The **TPM Management Console** is displayed.
3. Under **Actions**, click **Turn TPM Off**.
4. Provide the TPM owner password, if required.
5. When the **Status** panel in the **TPM Management on Local Computer** task panel reads "Your TPM is off and ownership of the TPM has been taken," close that task panel.
6. Close all open windows.
7. If the USB flash drive that contains your recovery password is plugged into the system, use the **Safely Remove Hardware** icon in the notification area to remove it from the system.
8. Click the **Start** button, and then click the **Shutdown** button to turn off your computer.

When you restart the computer, you will be prompted for the recovery password, because the startup configuration has changed since you encrypted the volume.

▶ **To recover access to data using BitLocker Drive Encryption**

1. Turn on your computer.
2. If the computer is locked, the **BitLocker Drive Encryption Recovery Console** will appear.
3. You will be prompted to insert the USB flash drive that contains the recovery password.
  - If you have the USB flash drive with the recovery password, insert it, and then press **ESC**. Your computer will restart automatically. You do not need to enter the recovery password manually.
  - If you do not have the USB flash drive with the recovery password, press **ENTER**.

You will be prompted to enter the recovery password.

If you know the recovery password, type it and then press ENTER.

If you do not know the recovery password, press ENTER twice and turn off your computer.

 **Note**

If you saved your recovery password in a file in a folder away from this computer, or on removable media, you can use another computer to open the file that contains the password. To locate the correct file, find **Password ID** on the recovery console display on the locked computer, and record this number. The file containing the recovery key uses this Password ID as the file name. Open the file and locate the recovery password in the file.

## Scenario 5: Turning off BitLocker Drive Encryption

Scenario 5 describes how to turn off BitLocker Drive Encryption and decrypt the volume. The procedure is the same for all BitLocker Drive Encryption configurations on TPM-equipped computers and computers without a compatible TPM.

When you turn off BitLocker, you can choose to either disable BitLocker temporarily, or to decrypt the drive. Disabling BitLocker allows TPM changes and operating system upgrades. Decrypting the drive means that the volume will once again be readable, and that all the keys are discarded. Once a volume is decrypted, you must generate new keys by going through the encryption process again.

### Before you start

- You must be logged on as an administrator.
- The drive must be encrypted.

### To turn off BitLocker Drive Encryption

1. Click **Start**, click **Control Panel**, click **Security**, and then click **BitLocker Drive Encryption**.
2. From the **BitLocker Drive Encryption** page, find the volume on which you want BitLocker Drive Encryption turned off, and click **Turn Off BitLocker Drive Encryption**.
3. From the **What level of decryption do you want** dialog box, click either **Disable**

**BitLocker Drive Encryption** or **Decrypt the volume** as needed.

By completing this procedure, you have either disabled BitLocker or decrypted the operating system volume.

## Logging Bugs and Feedback

Because BitLocker Drive Encryption is a new feature of Windows Vista, we are very interested in your feedback on your experiences with BitLocker, problems you encountered, and the usefulness of the documentation.

If you are part of a managed beta or the Technology Adoption Program (TAP), please follow the process provided by your coordinator to file bugs using the appropriate Web site or the reporting tool, or send e-mail to the address specific to your program.

All users are invited to participate in the Windows Vista Beta Security area of TechNet Forums (<http://go.microsoft.com/fwlink/?LinkId=71217>). You may also send general comments to [bdeinfo@microsoft.com](mailto:bdeinfo@microsoft.com).

## Additional Resources

The following resources provide additional information about BitLocker Drive Encryption:

- If you need product support, see the Microsoft Connect Web site (<http://go.microsoft.com/fwlink/?LinkId=49779>).
- To access newsgroups for BitLocker Drive Encryption, follow the instructions that are provided on the Microsoft Connect Web site (<http://go.microsoft.com/fwlink/?LinkId=50067>).

For more information about the User Account Control feature, see User Account Control on the Microsoft Web site (<http://go.microsoft.com/fwlink/?LinkId=66018>).