Protecting your data with Windows 10 BitLocker

**Customization note:** This document contains guidance and/or step-by-step installation instructions that can be reused, customized, or deleted entirely if they do not apply to your organization’s environment or installation scenarios. The yellow highlighted text indicates either customization guidance or organization-specific variables. All of the highlighted text in this document should either be deleted or replaced prior to distribution.

Microsoft BitLocker Drive Encryption technology uses the strongest publicly available encryption to protect your computer’s data. It also prevents others from accessing your disk drive(s) without authorization. BitLocker To Go prevents unauthorized access to your portable storage drives, including USB flash drives.

When you install Windows 10, you can use the Setup program to enable BitLocker. If you did not enable BitLocker during the installation process, you can use this guide to walk you through the process. You can also use this guide to learn how to suspend BitLocker, retrieve or print a BitLocker recovery key, or encrypt portable drives with BitLocker To Go.

# Preparing to turn BitLocker on

All new systems that <your organization name> provides are ready for BitLocker. However, before you turn BitLocker on, connect to the corporate network and join your computer to a domain (if it is not already joined).

# Turning BitLocker on

After you join your computer to the corporate network and connect to the domain, you can turn BitLocker on. BitLocker then turns on your computer’s Trusted Platform Module (TPM) chip, which is a microchip that enables your computer to utilize advanced security features.

Initially, when you start BitLocker, you can create a personal identification number (PIN) that you can use each time you start your computer. A PIN is required on devices that use DirectAccess for remote access. It’s optional for other devices. If you are using a Slate PC, you are not required to create a PIN.

## Turn BitLocker on

1. On the **Start** menu, type **Control Panel**, and then select **Control Panel** to open it.
2. In Control Panel, select **System and Security**, and then select **BitLocker Drive Encryption**.
3. On the **BitLocker Drive Encryption** page, under **Operating** system drive, select **Turn on BitLocker**.

On the **Choose how to unlock your drive at startup** page, select **Enter a PIN (recommended)**.

NOTE: If the TPM chip on your computer has not been turned on, you may see additional pages that walk you through the process of turning on the TPM chip. In this case, you must also reboot your device.

1. On the **Enter a PIN** page, enter a PIN, re-enter it to confirm it, and then select **Set PIN**.
2. On the **How do you want to back up your recovery key?** page, select **Save to a file**, and then browse to a secure location (for example, a hardened file share, secure removable drive, or Microsoft OneDrive for Business) that is not on your computer.

 

1. On the **Choose how much of your drive to encrypt** page, pick one of the options, and then select **Next**.

NOTE: We recommend that you choose the Encrypt used disk space only option for fast encryption. There is no risk of data loss.



1. In the **Are you ready to encrypt this drive?** page, select **Continue**.
2. When you are prompted to restart your computer, select **Restart** **now**.
3. After your computer restarts, enter your BitLocker PIN, and then press **Enter**.
4. Slide the Lock screen up, and then log on using your domain password.

NOTES:

* You can continue to use your computer during the encryption process.
* After BitLocker is enabled and if a startup PIN was used, each time that you attempt to log on to your computer, you must enter your BitLocker PIN before Windows starts. If you are not prompted for your PIN or have any issues when accessing your computer, contact <your IT department> at <link or phone number>.

# Turning BitLocker on for a secondary fixed data drive

1. On the **Start** menu, type **Control** **Panel**, and then select **Control Panel** to open it.
2. In **Control** **Panel**, select **System** **and** **Security**, and then select **BitLocker Drive Encryption**.
3. On the **BitLocker Drive Encryption** page, under **Fixed data drives**, select **Turn on BitLocker**.



NOTE: The Fixed data drives area is blank if your computer does not have a secondary fixed data drive.

1. On the **Choose how you want to unlock this drive** page, select a form of protection for the fixed data drive. At a minimum, you must select the **Automatically unlock this drive on this** **computer** check box. Requiring a password or smart card is optional.



1. On the **How do you want to back up your recovery key?** page, select **Save to a file**, and then browse to a secure location (for example, a hardened file share, secure removable drive, or OneDrive for Business) that is not on your computer.
2. After saving your recovery file, on the **Choose how much of your drive to encrypt** page, pick one of the options, and then select **Next**.

NOTE: We recommend that you choose the Encrypt used disk space only option for fast encryption. There is no risk of data loss.

1. On the **Are you ready to encrypt this drive?** page, select **Continue**.
2. When you are prompted to restart your computer, select **Restart now**.

NOTE: You can continue to use the computer and drive during the encryption process.

# Suspending BitLocker protection

On occasion, you may need to suspend BitLocker. For example, you might need to do a hardware upgrade or install a new operating system. When you suspend BitLocker, Windows disables protection on your system for one reboot. Your drive is still encrypted, however, and protection will be turned on again automatically after the first reboot.

You can perform all updates and system changes by suspending BitLocker protection. You typically do not need to turn BitLocker off for any reason other than to decrypt your drive.

## Suspend BitLocker

1. Open Control Panel, and then select **System and Security**.
2. Select **BitLocker Drive Encryption**, and then select **Suspend protection**.



1. When prompted to confirm, select **Yes**.

## Resume BitLocker

1. Open Control Panel, and then select **System and Security**.
2. Select **BitLocker Drive Encryption**, and then select **Resume protection**.

NOTE: After one reboot, BitLocker is turned on again automatically.

## Decrypt your drive

1. Open Control Panel, and then select **System** **and** **Security**.
2. Select **BitLocker Drive Encryption**, and then select **Turn off BitLocker**.

NOTE: You can continue to use your computer during the decryption process.

# Encrypting a portable drive with BitLocker To Go

When you encrypt a portable drive with BitLocker To Go, you can set it to unlock by using a password or your smart card.

Password encryption requires that you enter an 8-character password during the setup process. <Your organization name> recommends a 12-character password to minimize the risk of someone reading or modifying data on a lost or stolen device. This password does not expire. You can also use the auto-unlock feature to avoid having to enter a password each time you use the portable drive. For more information, see “Managing BitLocker To Go” later in this guide.

Smart card encryption is more secure than password encryption and requires additional steps. To use smart card encryption, you encrypt the device using your smart card and a PIN. You share this information only with someone who has a smart card reader, and you must insert your smart card and enter your PIN to unlock the portable drive.

## Turn on BitLocker To Go

1. Connect to the corporate network.
2. Open Control Panel, select **System and Security**, and then select **BitLocker Drive Encryption**.
3. If you have not already done so, insert the portable drive (such as a USB drive or SD/MMC card) into the appropriate slot.
The name of the portable drive appears on the **BitLocker Drive Encryption** page, in the **Removable Data Drives** area.
4. Select **Turn on BitLocker**.
5. On the Choose how you want to unlock this drive page, select the option you want:
* Use a password to unlock the drive check box to use a password to unlock the drive. Enter your password twice, and then select **Next**.
* Use my smart card to unlock the drive check box to unlock the drive instead. Insert your smart card, and then select **Next**.
1. On the **How do you want to back up your recovery key?** page, select **Save to a file**, and then browse to a secure location (for example, a hardened file share, secure removable drive, or OneDrive for Business) that is not on your computer.
2. Select **Save**, and then select **Next**.
3. On the **Choose how much of your drive to encrypt** page, select the option you want, and then select **Next**.

TIP: We recommend choosing the Encrypt used disk space only option for fast encryption. There is no risk of data loss.

1. On the **Are you ready to encrypt this drive?** page, select **Start encrypting**.

An encryption progress box appears, followed eventually by a completion notice.

1. If you remove the portable drive and then reinsert it, do one of the following:
* If you chose password protection, respond to the prompt for your password.

– OR –

* If you chose smart card protection, insert your smart card in your smart card reader and enter your smart card PIN.

NOTES:

* The time required to encrypt a portable drive with BitLocker To Go varies depending on the drive size, your connection speed, and the technology you use. You can continue to use your computer during the encryption process.
* Each time you attempt to use the drive you must enter the password or smart card, unless you set up BitLocker To Go to unlock the drive automatically. If you have any issues accessing your drive, contact <your IT department> at <<link or phone number>>.
* If you want to change the password for a portable drive or change the auto-unlock feature, see the “Managing BitLocker To Go” section of this guide.

# Managing BitLocker To Go

After you encrypt a portable drive, you may want to back up your recovery key, change a password, remove a password, add a smart card to unlock the drive, enable or disable the auto-unlock feature, or turn BitLocker off.

To do any of these tasks, follow these steps:

1. Open Control Panel, select **System and Security**, and then select **BitLocker Drive Encryption**.
2. On the **BitLocker Drive Encryption** page, select the appropriate BitLocker option.



# Saving a BitLocker recovery key

A BitLocker recovery key is created when you turn on BitLocker for the first time. You can use the recovery key to gain access to your computer if the drive that Windows is installed on is encrypted and BitLocker detects a condition that prevents it from unlocking the drive when the computer starts up. You can also use a recovery key to gain access to a secondary fixed data drive or a removable data drive encrypted with BitLocker To Go, if you forget the password or your computer cannot access the drive.

You can save your recovery key as a file on a computer that you are not encrypting. You cannot save the recovery key for a removable data drive to removable media. Make sure to store the recovery key separate from your computer.

TIP: If you print your recovery key to a file and store it on OneDrive for Business, you can access your recovery key from your Windows Phone if you need it.

## Save your recovery key

If you are a business travelers who is often away from the domain (and cannot access the MBAM Recovery Portal), you may find it helpful to keep a recovery key stored on OneDrive for Business, stored on a removable drive, or printed on a piece of paper.

1. Open the Control Panel.
2. On the **Programs and features** page, select **BitLocker Drive Encryption**. Select **Back up your recovery key**, and then select how you want to save your key.

TIP: Do not keep both your computer and your recovery key together in the same container.

# For more information

### Microsoft IT

<http://www.Microsoft.com/ITShowcase>

### Windows 10

https://www.microsoft.com/en-us/windows/windows-10-upgrade

© 2016 Microsoft Corporation. All rights reserved. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.