BitLocker Drive Encryption with TPM

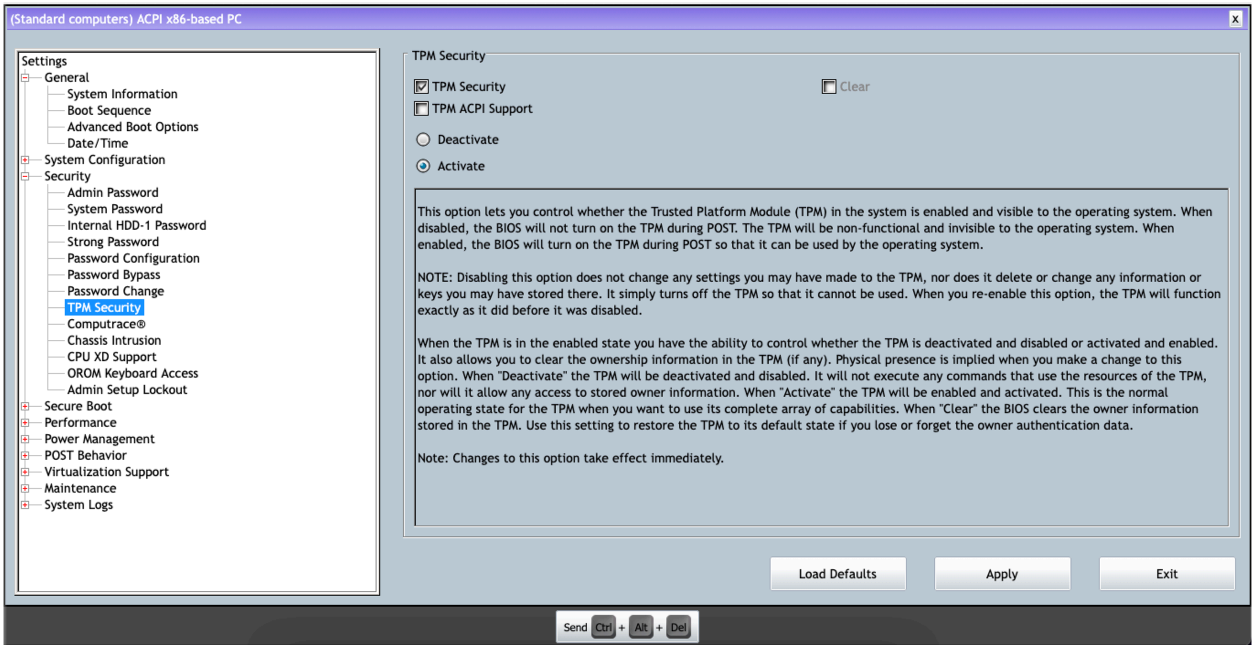
Overview

Configured full-disk encryption on the system drive using BitLocker with TPM support. This included enabling TPM in firmware, activating it, configuring encryption settings, saving a recovery key to a network server, and validating protection with a BitLocker system check.

What I Implemented

1. Enabled and Activated TPM in Firmware

Entered BIOS/UEFI settings and turned on the system's Trusted Platform Module (TPM). This allowed the machine to support hardware-backed key storage, which BitLocker requires for secure boot-time verification.



TPM Security

☑ TPM Security

☐ TPM ACPI Support

☐ Clear

○ Deactivate

● Activate

This option lets you control whether the Trusted Platform Module (TPM) in the system is enabled and visible to the operating system. When disabled, the BIOS will not turn on the TPM during POST. The TPM will be non-functional and invisible to the operating system. When enabled, the BIOS will turn on the TPM during POST so that it can be used by the operating system.

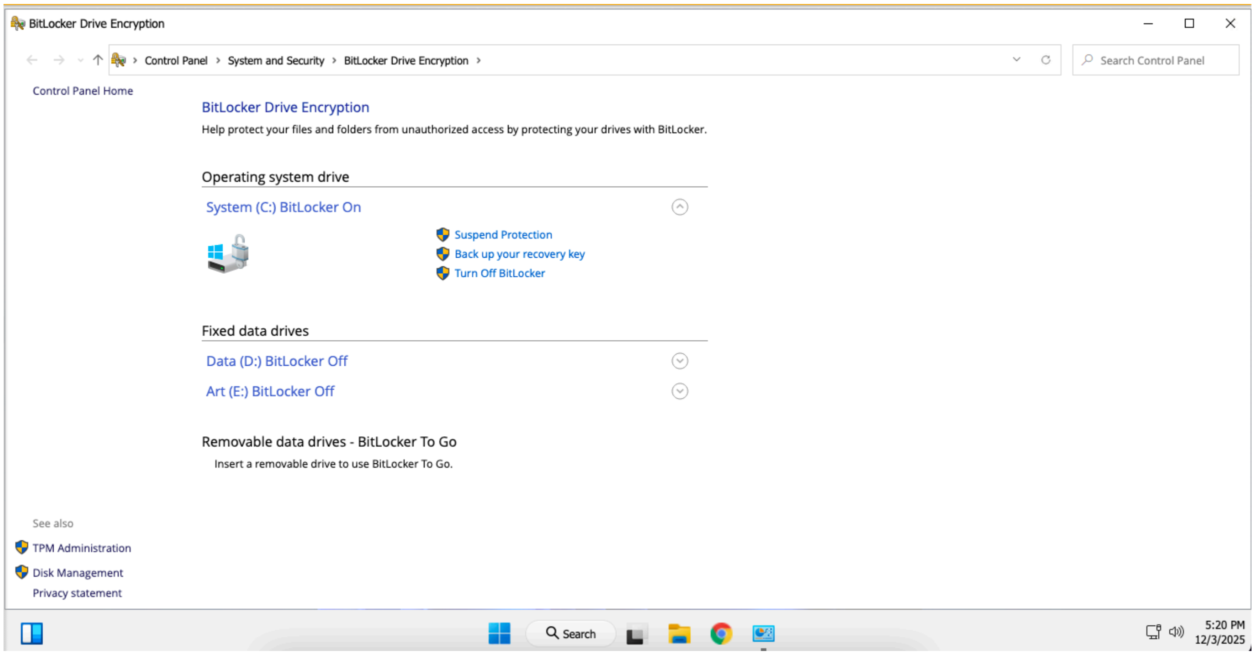
NOTE: Disabling this option does not change any settings you may have made to the TPM, nor does it delete or change any information or keys you may have stored there. It simply turns off the TPM so that it cannot be used. When you re-enable this option, the TPM will function exactly as it did before it was disabled.

When the TPM is in the enabled state you have the ability to control whether the TPM is deactivated and disabled or activated and enabled. It also allows you to clear the ownership information in the TPM (if any). Physical presence is implied when you make a change to this option. When "Deactivate" the TPM will be deactivated and disabled. It will not execute any commands that use the resources of the TPM, nor will it allow any access to stored owner information. When "Activate" the TPM will be enabled and activated. This is the normal operating state for the TPM when you want to use its complete array of capabilities. When "Clear" the BIOS clears the owner information stored in the TPM. Use this setting to restore the TPM to its default state if you lose or forget the owner authentication data.

Note: Changes to this option take effect immediately.

2. Enabled BitLocker on the System Drive

Launched BitLocker Drive Encryption and configured it to protect the **System (C:)** drive. Once TPM was active, BitLocker initialized normally without requiring a USB startup key.



BitLocker Drive Encryption

Control Panel > System and Security > BitLocker Drive Encryption >

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

System (C:) BitLocker On

- Suspend Protection
- Back up your recovery key
- Turn Off BitLocker

Fixed data drives

Data (D:) BitLocker Off

Art (E:) BitLocker Off

Removable data drives - BitLocker To Go

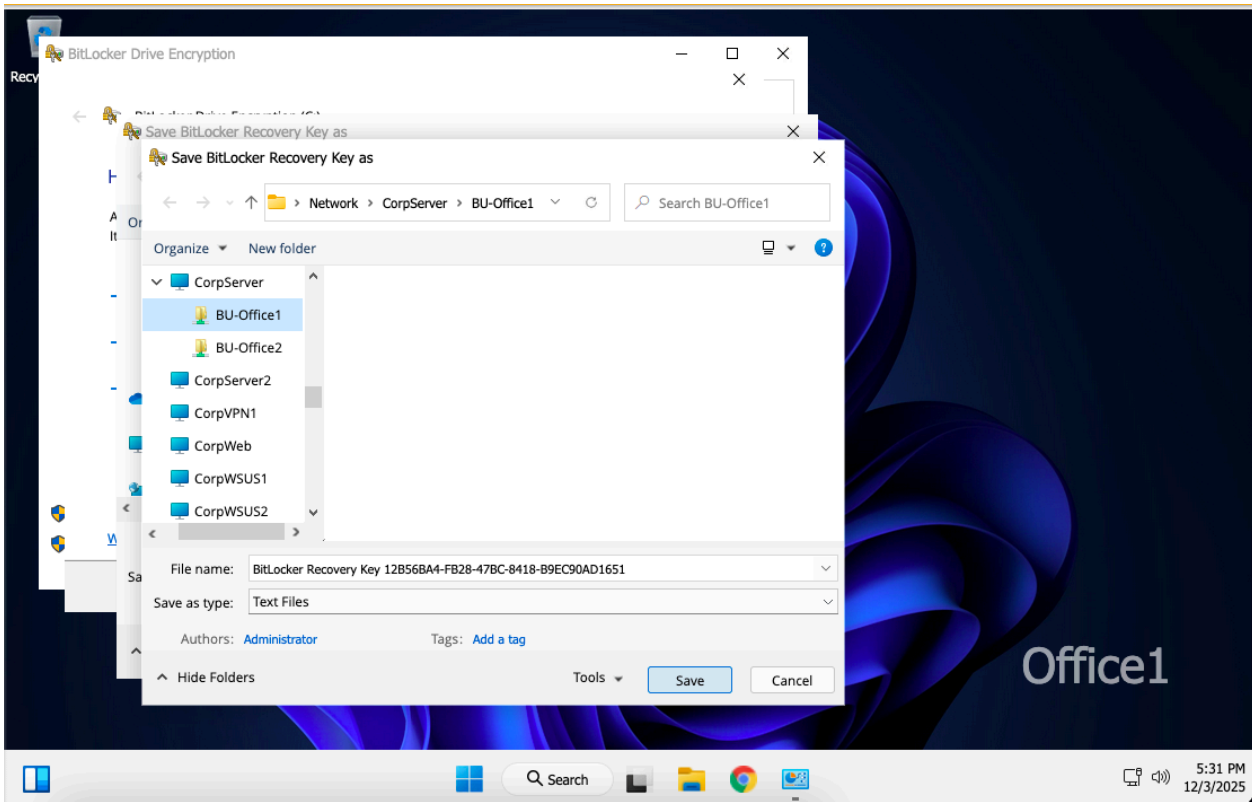
Insert a removable drive to use BitLocker To Go.

See also

- TPM Administration
- Disk Management
- Privacy statement

3. Saved the Recovery Key to a Central Server

Exported the BitLocker recovery key to **CorpServer** → **BU-Office1**, mirroring how enterprises store recovery information for auditability and disaster recovery.



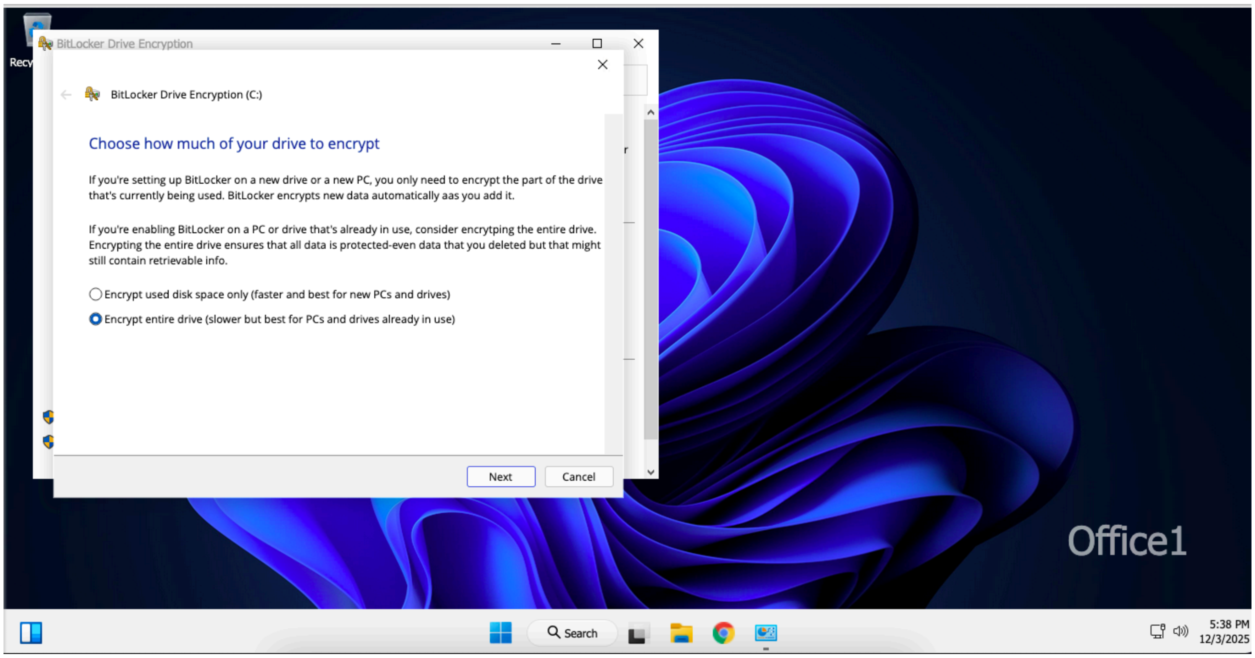
File name: BitLocker Recovery Key 12B56BA4-FB28-47BC-8418-B9EC90AD1651

Save as type: Text Files

Authors: Administrator Tags: Add a tag

4. Encrypted the Entire Drive

Chose full-drive encryption to protect both current and deleted data. Used **New Encryption Mode (XTS-AES)**, the stronger Windows 10+ disk protection standard.



BitLocker Drive Encryption (C:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically aas you add it.

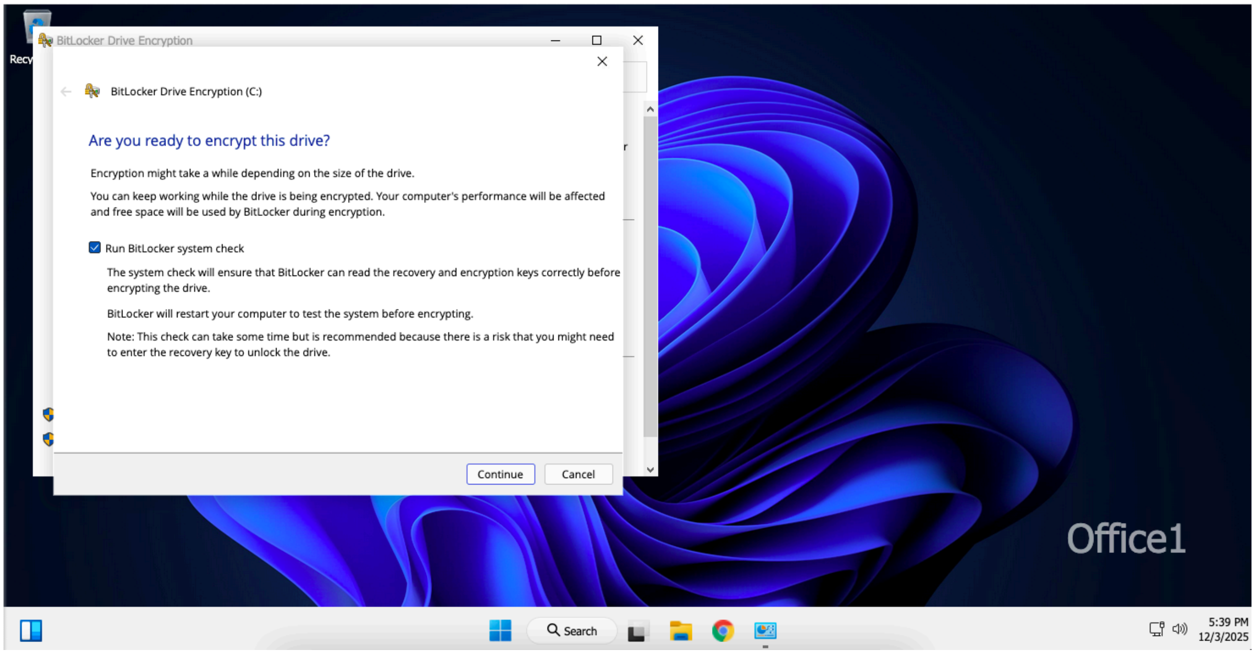
If you're enabling BitLocker on a PC or drive that's already in use, consider encrytping the entire drive. Encrypting the entire drive ensures that all data is protected-even data that you deleted but that might still contain retrievable info.

○ Encrypt used disk space only (faster and best for new PCs and drives)

● Encrypt entire drive (slower but best for PCs and drives already in use)

5. Performed a BitLocker System Check

Ran a pre-boot validation test to ensure TPM integrity, bootloader trust, and disk readiness before encryption. The system rebooted and began full drive encryption automatically.



BitLocker Drive Encryption (C:)

Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

You can keep working while the drive is being encrypted. Your computer's performance will be affected and free space will be used by BitLocker during encryption.

☑ Run BitLocker system check

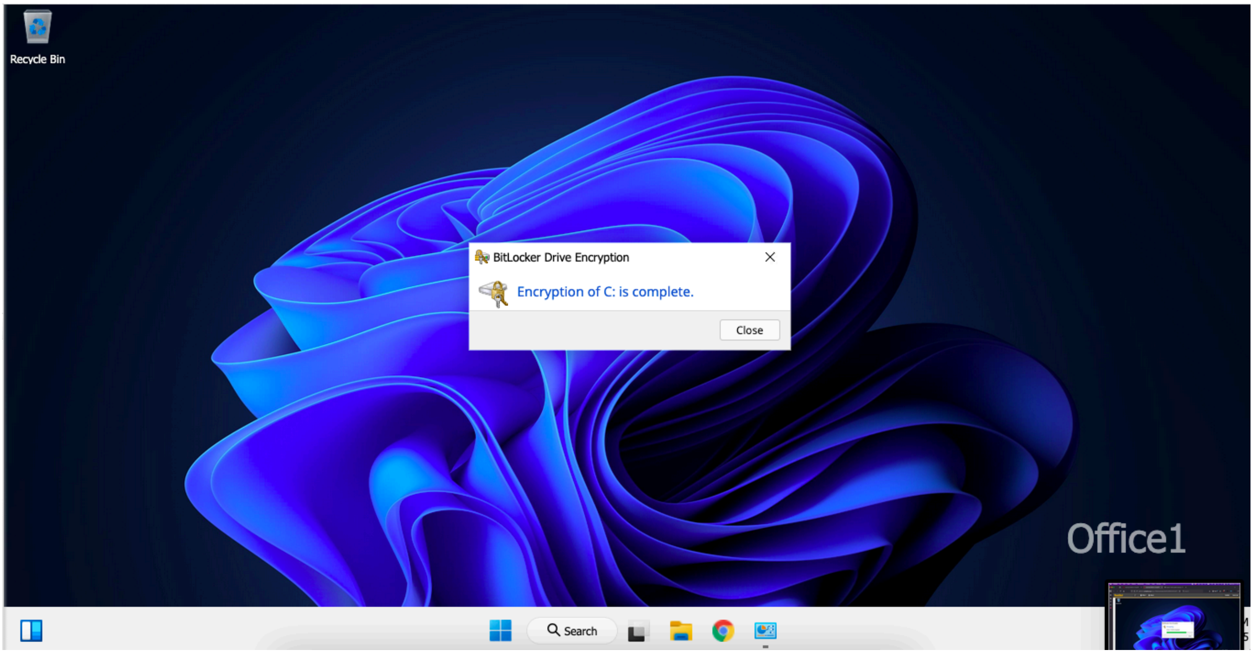
The system check will ensure that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.

BitLocker will restart your computer to test the system before encrypting.

Note: This check can take some time but is recommended because there is a risk that you might need to enter the recovery key to unlock the drive.

6. Verified Active Encryption

Confirmed successful activation by checking the System (C:) drive.



Encryption of C: is complete.

Security Impact

This setup provides strong full-disk protection using hardware-rooted trust. TPM-backed BitLocker ensures stolen devices can’t be booted, tampered with, or accessed without proper authentication while maintaining enterprise-grade recovery procedures.