GSD. Hardware - How to enable Bitlocker on a device

Article ID: KB0039793
Created: 2024-12-19 14:03:36
Updated: 2024-12-19 14:03:36
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/ea439c04c3ca1a100acd3300150131d2', 'value': 'ea439c04c3ca1a100acd3300150131d2'}

General Information:

Possible symptoms/errors:

How to enable Bitlocker on a device.

Alternative names of the system:

N/A

IMPORTANT NOTICE:

If the user needs a manual password reset, he needs to be authenticated

Solution:

User Authentication for manual reset: Ask the user for his manager and compare the data with the entered manager in Service Now. The password can only be reset manually if this detail match.

Bitlocker helps to protect user’s data by encrypting their device. It's part of Windows and can be enabled by users themselves.

Note: Notebooks, being deployed in Germany and notebooks being ordered for Sweden and Denmark come with activated and preset Bitlocker encryption.

The following article describes how to enable Bitlocker and how to unlock the device afterwards.

1. Enable Bitlocker for a drive

The easiest way to enable BitLocker for a drive is to right-click the drive in a File Explorer window, and then choose the “Turn on BitLocker” command. If user doesn’t see this option on their context menu, then they likely don’t have a Pro or Enterprise edition of Windows and they will need to seek another encryption solution.

It’s just that simple. The wizard that pops up walks user through selecting several options, which we’ve broken down into the sections that follow.

2. Choose an unlock method

The first screen user will see in the “BitLocker Drive Encryption” wizard lets them choose how to unlock their drive. User can select several different ways of unlocking the drive.

If user is encrypting their system drive on a computer that doesn’t have a TPM, they can unlock the drive with a password, or a USB drive that functions as a key. Advise the user to select their unlock method and follow the instructions for that method (enter a password or plug in your USB drive).

If user’s computer does have a TPM, they will see additional options for unlocking their system drive. For example, they can configure automatic unlocking at start-up (where the computer grabs the encryption keys from the TPM and automatically decrypts the drive). User could also use a PIN instead of a password, or even choose biometric options like a fingerprint.

If user is encrypting a non-system drive or removable drive, they will see only two options (whether they have a TPM or not). User can unlock the drive with a password or a smart card (or both).

3. Backup a recovery key

BitLocker provides user with a recovery key that they can use to access their encrypted files should they ever lose their main key—for example, if user forgets their password or if the PC with TPM dies and they must access the drive from another system.

User can save the key to their Microsoft account, a USB drive, a file, or even print it. These options are the same whether they’re encrypting a system or non-system drive.

If user backs up the recovery key to their Microsoft account, they can access the key later at https://onedrive.live.com/recoverykey. If they use another recovery method, advise them to ensure to keep this key safe—if someone gains access to it, they could decrypt user’s drive and bypass encryption.

User can also back up their recovery key multiple ways if they want. In order to do this, they need to click each option they want to use in turn, and then follow the directions. When they’re done saving their recovery keys, advise them to click “Next” to move on.

Note: If user is encrypting a USB or other removable drive, they won’t have the option of saving their recovery key to a USB drive. They can use any of the other three options.

4. Encrypt and unlock the device

BitLocker automatically encrypts new files as user adds them, but they must choose what happens with the files currently on their drive. They can encrypt the entire drive—including the free space—or just encrypt the used disk files to speed up the process. These options are also the same whether user is encrypting a system or non-system drive.

If user is setting up BitLocker on a new PC, advise them to encrypt the used disk space only—it’s much faster. If they’re setting BitLocker up on a PC they’ve been using for a while, they should encrypt the entire drive to ensure no one can recover deleted files.

When user has made their selection, advise them to click the “Next” button.

5. Choose an encryption mode (Windows 10 only)

If user is using Windows 10, they’ll see an additional screen letting them choose an encryption method. If they’re using Windows 7 or 8, advise them to skip ahead to the next step.

Windows 10 introduced a new encryption method named XTS-AES. It provides enhanced integrity and performance over the AES used in Windows 7 and 8. If user knows the drive they’re encrypting is only going to be used on Windows 10 PCs, they can go ahead and choose the “New encryption mode” option. If user thinks they might need to use the drive with an older version of Windows at some point (especially important if it’s a removable drive), advise them to choose the “Compatible mode” option.

Whichever option user chooses (and again, these are the same for system and non-system drives), advise them to go ahead and click the “Next” button when they’re done, and on the next screen, ask them to click the “Start Encrypting” button.

6. Finish

The encryption process can take anywhere from seconds to minutes or even longer, depending on the size of the drive, the amount of data user is encrypting, and whether they chose to encrypt free space.

If user is encrypting their system drive, they'll be prompted to run a BitLocker system check and restart their system. Advise the user to make sure the option is selected, to click the "Continue" button, and then to restart their PC when asked. After the PC boots back up for the first time, Windows encrypts the drive.

If user is encrypting a non-system or removable drive, Windows does not need to restart, and encryption begins immediately.

Whatever type of drive user is encrypting, they can check the BitLocker Drive Encryption icon in the system tray to see its progress, and they can continue using their computer while drives are being encrypted—it will just perform more slowly.

Unlock the device

If user's system drive is encrypted, unlocking it depends on the method they chose (and whether user' PC has a TPM). If they do have a TPM and selected to have the drive unlocked automatically, they won't notice anything different—they'll just boot straight into Windows like always. If user chose another unlock method, Windows prompts them to unlock the drive (by typing their password, connecting their USB drive, or whatever).

And if user has lost (or forgotten) their unlock method, they need to press Escape on the prompt screen to enter their recovery key.

If user has encrypted a non-system or removable drive, Windows prompts them to unlock the drive when they first access it after starting Windows (or when they connect it to their PC if it's a removable drive). Advise the user to type their password or insert their smart card, and the drive should unlock so they can use it.

In File Explorer, encrypted drives show a gold lock on the icon (on the left). That lock changes to grey and appears unlocked when user unlocks the drive (on the right).

User can manage a locked drive—change the password, turn off BitLocker, back up their recovery key, or perform other actions—from the BitLocker control panel window. Advise the user to right-click any encrypted drive, and then to select "Manage BitLocker" to go directly to that page.

In case of any issues with the Bitlocker, gather the information from the user as per below and assign the ticket to the Ext_WW_Physical-Workplace_SLS_Capgemini team in Service Now:

The affected machine's hostnameProblem descriptionUsernameUser's contact numberUser's location details

Assignment Group:

Ext_WW_Physical-Workplace_SLS_Capgemini

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/A