BitLocker Drive Encryption End User Guide

(Revision Date: 09/11/2020)

Table of Contents

Introduction

The Connecticut State Colleges and Universities (CSCU) is securing the confidentiality of sensitive data on Connecticut Community College (CCC) and System Office (SO) owned laptop computers by implementing BitLocker Drive Encryption. Every content on a computer that ends up lost or stolen is vulnerable to unauthorized access, which can present a security risk to both yourself and CSCU. BitLocker provides protection for the laptop's operating system as well as the data stored on it; ensuring the data remains encrypted and inaccessible to unauthorized users. The configuration for BitLocker requires users to provide a PIN, in form of a password, to unlock the drive before making the operating system available for regular use.
When a new file is added to a drive that is encrypted, BitLocker encrypts it automatically. Files remain encrypted only while they are stored in the encrypted drive. Files that are copied to another drive or computer are decrypted. If you share files with other users, such as through a network, these files are encrypted while stored on the encrypted drive, but they can be accessed normally by authorized users.

This guide will provide instructions for changing the BitLocker PIN and performing machine recovery.

Intended Audience

The intended audience for this procedure is:

- CCC Employees
- SO Employees

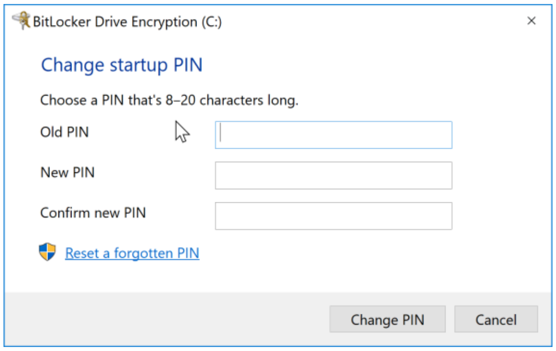
Procedure

Create the Initial Enhanced PIN for BitLocker

The first time you are assigned a laptop, the Helpdesk technician will guide you in setting up the initial enhanced PIN. The PIN is enhanced to accept letters, numbers, and special characters. All enhanced PINs must meet CSCU's Password Standard. The requirements are summarized here.

1. Setup a time to work with a Helpdesk staff to receive your laptop.

2. The technician will sign into the laptop and open the program, Manage BitLocker, for you to create a new PIN.



BitLocker Drive Encryption (C:)

Change startup PIN

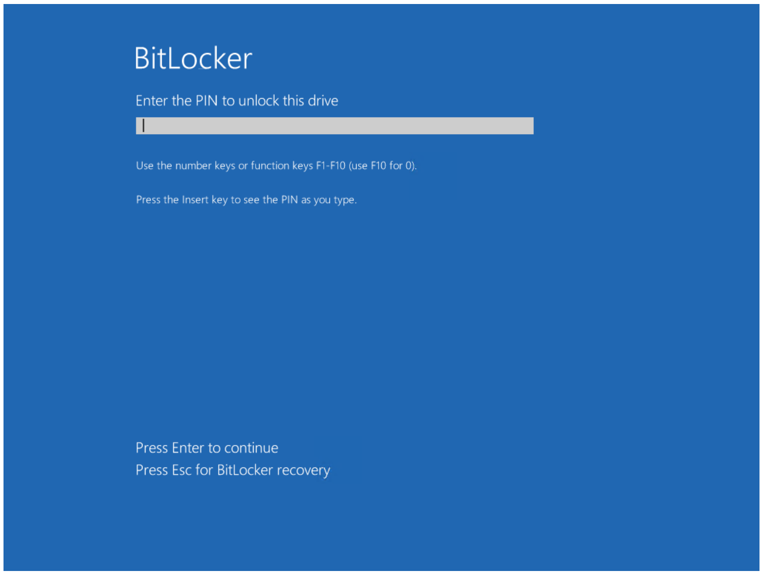
Choose a PIN that's 8–20 characters long.

The technician will enter the **Old PIN**. You will then enter the **New PIN** and **Confirm new PIN**. The PIN you create must NOT be the same as the current Windows password. Doing so will result in a violation of CSCU's Acceptable Use Policy. Do not write the PIN on paper to avoid misplacing it and do not share it with anyone, including your helpdesk staff.

3. Click **Change PIN** to submit the change.

4. Restart the laptop to test the new PIN.

5. Upon reboot, the BitLocker pre-boot authentication screen will prompt for the PIN. This screen will always present itself when the laptop is rebooted or powered on.



BitLocker

Enter the PIN to unlock this drive

Use the number keys or function keys F1-F10 (use F10 for 0).

Press the Insert key to see the PIN as you type.

Press Enter to continue
Press Esc for BitLocker recovery

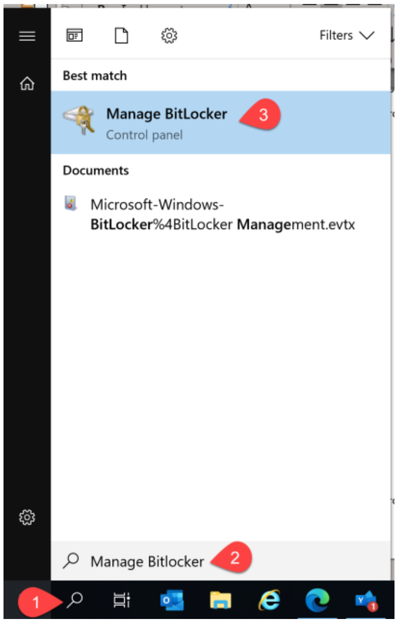
Enter the PIN and press **Enter** to continue.

6. The Windows operating system will load and prompt you for netID and Password to login.

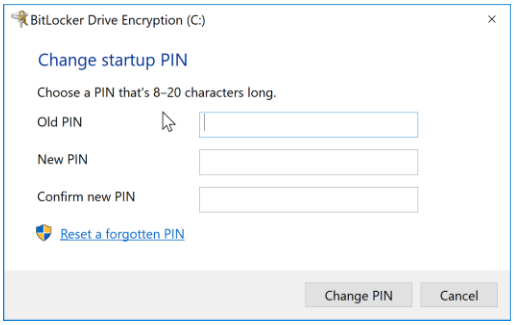
Changing Your BitLocker PIN

You are not required to change the PIN periodically and you will not be prompted to do so. However, if your PIN was mistakenly shared with someone else you must change it right away. You may also choose to change the PIN at any time you prefer.

1. From the Windows **Start Menu** or **Search** bar, type “Manage BitLocker” without quotes.



2. Create your new PIN.



BitLocker Drive Encryption (C:)

Change startup PIN

Choose a PIN that's 8–20 characters long.

Old PIN

New PIN

Confirm new PIN

Reset a forgotten PIN

Enter the **Old PIN** or current PIN. Enter the **New PIN** and then confirm it. Click **Change PIN** to submit changes.

NOTE: If you do not know the old PIN, contact the local Helpdesk. An Administrator will guide you in setting up a new PIN.

3. Restart the computer to confirm the new PIN is working at the BitLocker pre-boot authentication screen.

Machine Recovery

Because BitLocker is designed to protect your computer from numerous attacks, there are various reasons why BitLocker could require machine recovery.

Machine recovery is necessary when one of the following conditions occur:

- You forgot the PIN and BitLocker will not accept your entry.
- A major hardware / software update from your IT department changed system files.
- When an attack is detected, the device will immediately reboot and enter BitLocker recovery mode.
- Docking or undocking a portable computer. If a certain manufacturer laptop is connected to its docking station when BitLocker was enabled, then it might also need to be connected to the docking station when it is unlocked.

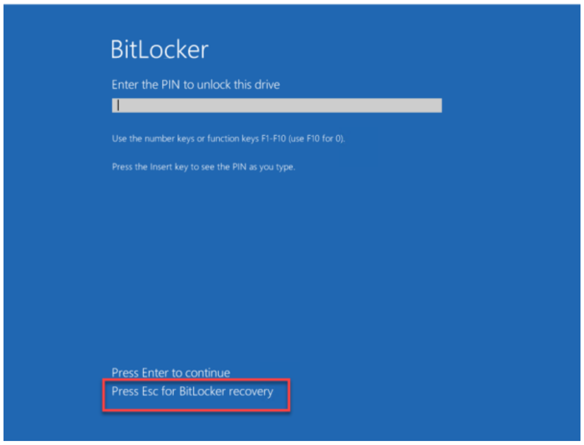
If you forgot the BitLocker PIN, contact the local Helpdesk for recovery and PIN reset:

1. Call the Helpdesk phone number for your institution. You may visit your institution's website and navigate to the *Contact* section and find the number to call.

2. Verify your identity by confirming first and last name, birthdate and the last four digits of your SSN. State that you need recovery due to forgotten PIN. It is important to clearly state why recovery is needed.

3. Turn on the laptop.

4. Press the **Esc** key on the keyboard to enter BitLocker Recovery.



BitLocker

Enter the PIN to unlock this drive

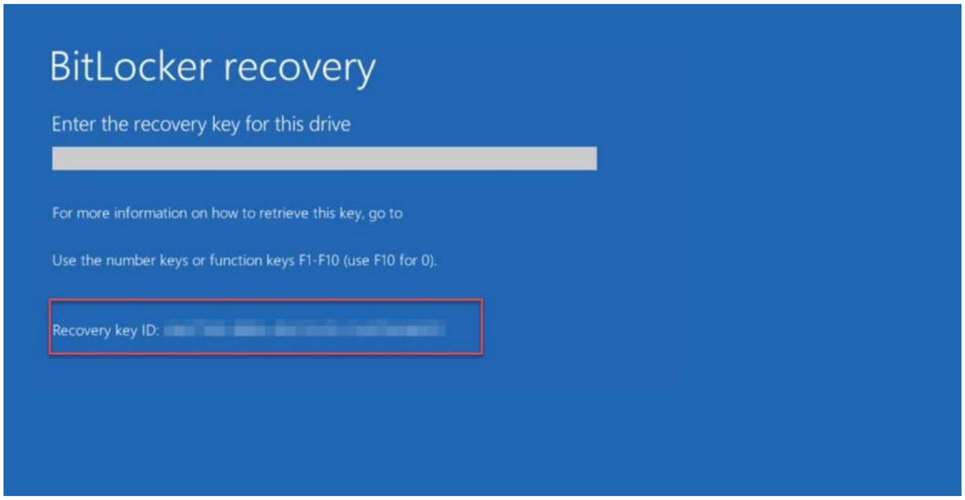
Use the number keys or function keys F1-F10 (use F10 for 0).

Press the Insert key to see the PIN as you type.

Press Enter to continue

Press Esc for BitLocker recovery

5. Provide the Recovery Key ID to the technician.



BitLocker recovery

Enter the recovery key for this drive

For more information on how to retrieve this key, go to

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID: [redacted]

NOTE: A security measure is in place to shutdown the laptop if this screen is inactive for one (1) minute. Move the mouse cursor or press the arrow keys on the keyboard to keep the screen alive. If the laptop shuts down due to inactivity, turn it back on and start over from step 4.

6. After verifying the information, the technician will read your recovery key. The key is 48 digits long. Use the number keys or function keys on your keyboard to enter the numbers provided by the technician. Press **Enter** when finished.

   NOTE: You may write down the key on a piece of paper if you are having trouble. After completing the recovery, the key will become invalid. A different key will be needed for future recoveries.

7. If the process was successful, the laptop will complete initialization and load the Windows operating system.

8. Login to Windows with your netID and password.

9. Since the PIN was forgotten, you will need assistance from the helpdesk technician to create a new PIN. Failing to do so will result in consecutive requests for Machine Recovery each time your laptop is rebooted.

   a) If you are present at the institution, the technician will connect to your laptop remotely and use the *Manage BitLocker* program to help create a new PIN. You may also visit the IT Department in person to receive assistance with creating the PIN.

   b) If you are working off-site, the technician may have the ability to remotely connect to your laptop and create the PIN. In most cases, you will have to bring the laptop to the IT Department for in-person support.

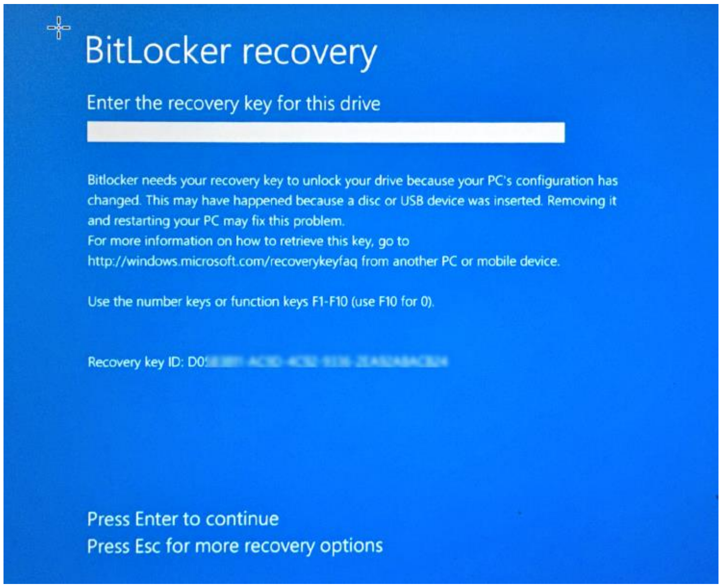
10. Restart the laptop to confirm if BitLocker accepts the PIN. If you are successful, the PIN will remain as is for the length of time the laptop is at your possession.

Machine Recovery due to System Changes

BitLocker is programmed to detect any firmware or hardware changes to the laptop. This measure is in place to prevent malicious users from finding a way to break into the system.

The following scenarios may prevent themselves after you turn on the laptop:

A. When BitLocker detects a configuration change, the screen below will be presented at boot.



BitLocker recovery

Enter the recovery key for this drive

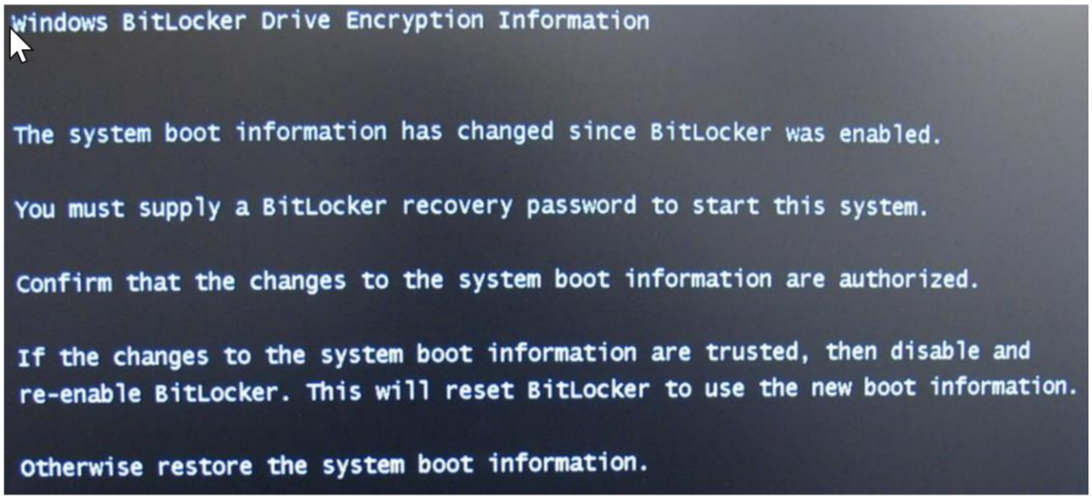
Bitlocker needs your recovery key to unlock your drive because your PC's configuration has changed. This may have happened because a disc or USB device was inserted. Removing it and restarting your PC may fix this problem.
For more information on how to retrieve this key, go to http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device.

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID: D0[redacted]

Press Enter to continue
Press Esc for more recovery options

B. When BitLocker detects a change in the BIOS or boot files, the following screen will be presented at boot.

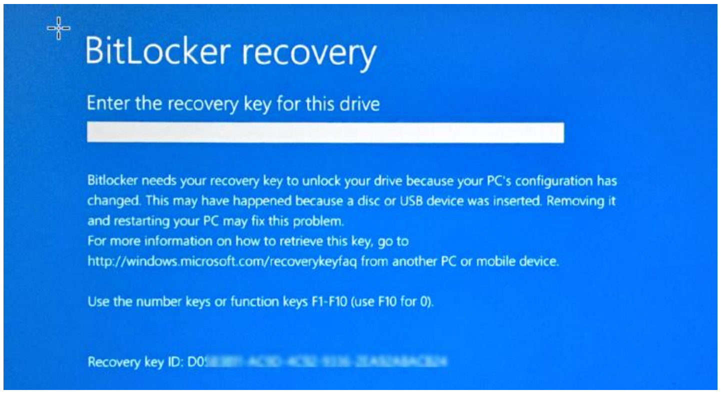


```
Windows BitLocker Drive Encryption Information

The system boot information has changed since BitLocker was enabled.

You must supply a BitLocker recovery password to start this system.

Confirm that the changes to the system boot information are authorized.

If the changes to the system boot information are trusted, then disable and
re-enable BitLocker. This will reset BitLocker to use the new boot information.

Otherwise restore the system boot information.
```

1. You will need to perform recovery for both scenarios. Call the Helpdesk phone number for your institution to receive assistance. You may visit your institution's website and navigate to the *Contact* section and find the number to call.

2. Verify your identity by confirming first and last name, birthdate and the last four digits of your SSN. State the reason why you need recovery. It is important to clearly state why recovery is needed.

   Scenario A – Provide the recovery key ID to the helpdesk technician. The technician will confirm the information and, in turn, read you the recovery key. Enter the 48-digit key and press **Enter.**



BitLocker recovery

Enter the recovery key for this drive

Bitlocker needs your recovery key to unlock your drive because your PC's configuration has changed. This may have happened because a disc or USB device was inserted. Removing it and restarting your PC may fix this problem.
For more information on how to retrieve this key, go to
http://windows.microsoft.com/recoverykeyfaq from another PC or mobile device.

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID: D0[redacted]

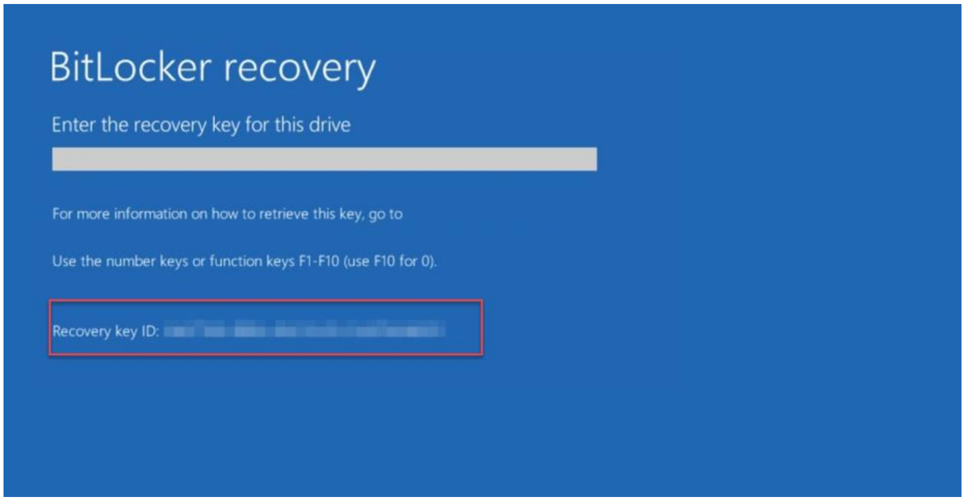
3. If the key entry is successful, Windows will load and prompt for your netID and password.

4. Login and reboot the laptop after 60 seconds. Confirm that you are able to sign in with the current PIN you have. (Note: no changes were made to the PIN and it does not need to be changed after this kind of recovery).

5. BitLocker will acknowledge whatever the system change may have been and no longer prompt for recovery.

Scenario B – BitLocker detected changes with boot files. Boot files provide the order necessary for your computer to turn on, initialize and load the operating system.

Repeat from step 1. The recovery screen will look similar to the image below.



BitLocker recovery

Enter the recovery key for this drive

For more information on how to retrieve this key, go to

Use the number keys or function keys F1-F10 (use F10 for 0).

Recovery key ID: [redacted]

Release History

□	09/11/2020	Initial Release