BitLocker

How to Recover from BitLocker Recovery Mode

Introduction

BitLocker Drive Encryption performs a system integrity check every time an encrypted computer starts up. System integrity is validated by comparing the current configuration of critical components to a baseline taken when **BitLocker Drive Encryption** was first enabled. This validation is done to protect the system from unauthorized tampering and attempts to gain access.

When BitLocker system integrity validation fails while protectors are enabled, the operating system (OS) drive will be locked and the computer will start up in **Recovery Mode**.

Exiting Recovery Mode

In order to exit **Recovery Mode**, the correct recovery key for the encrypted operating system drive must be entered into the field provided. The recovery key can be obtained by using the **Self-Service Portal** or by contacting the **Faculty/Staff Help Center**. The **Self-Service Portal** is accessible from on- or off-campus, and is compatible with any web browser on a desktop, laptop, tablet, or other mobile device.

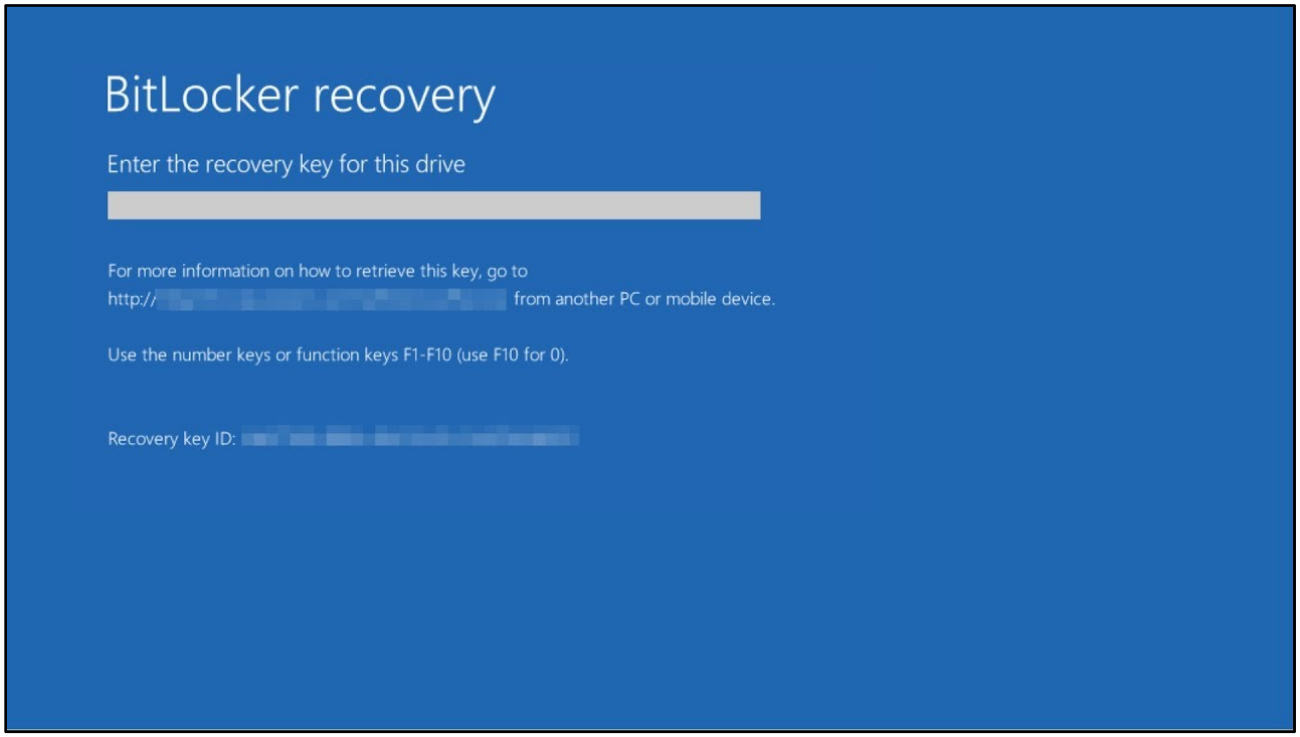

Figure 1

Self-Service Portal

The **Self-Service Portal** can be used by all Towson University faculty and staff to retrieve recovery keys for their own computers and devices. It cannot be used to retrieve recovery keys for other computers and devices that your NetID is not associated with. To retrieve the recovery key from the **Self-Service Portal**:

1. Open your preferred web browser and navigate to **https://bitlocker.towson.edu**.
2. In the **Authentication required** window, type your **Username** (NetID) and **Password**.
3. Click the **Log in** button.

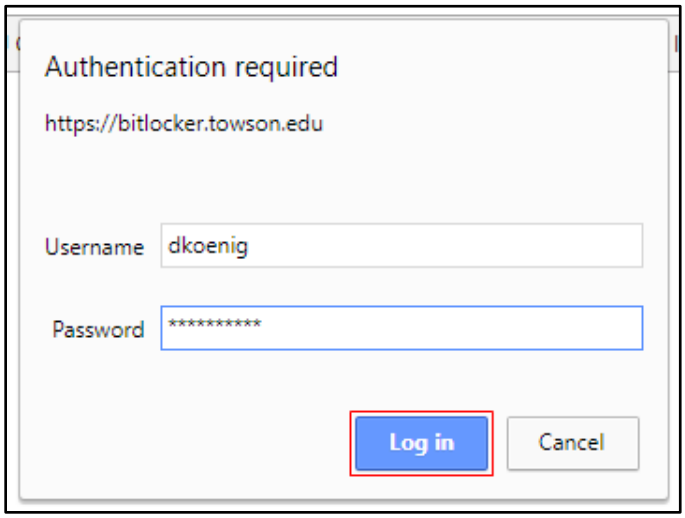

Figure 2

4. Read the notice and check the box beside **I have read and understand the above notice** and then click **Continue** button.

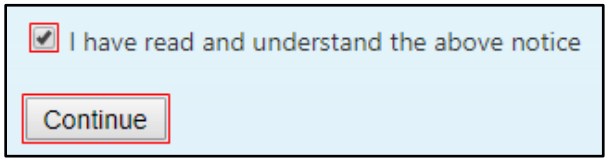

Figure 3

5. Type the **Recovery Key ID** from the device currently locked or in **Recovery Mode**. Note that only the first 8 characters are required. The **Recovery Key ID** can be found on the **BitLocker recovery** screen of the locked device.
6. Select a **Reason** from the drop down menu provided. If you are unsure of the reason, select **OS Files Modified**.
7. Click the **Get Key** button.

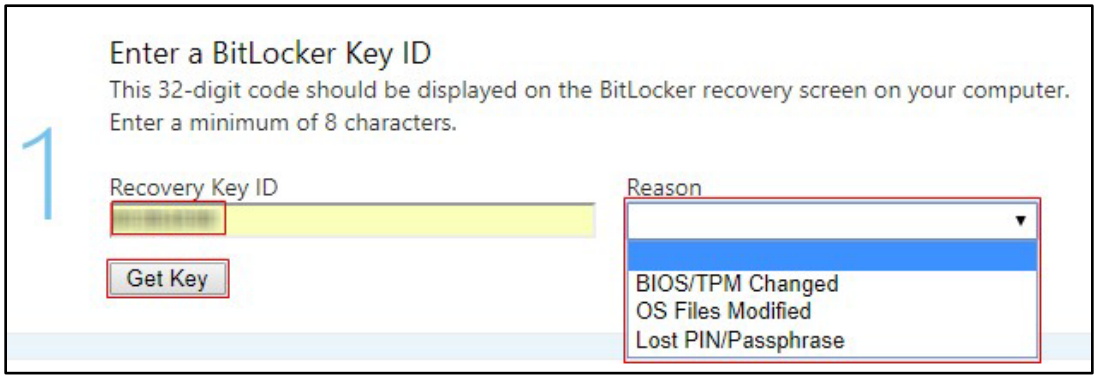

Figure 4

8. Your **BitLocker Recovery Key** will be displayed in the web browser.

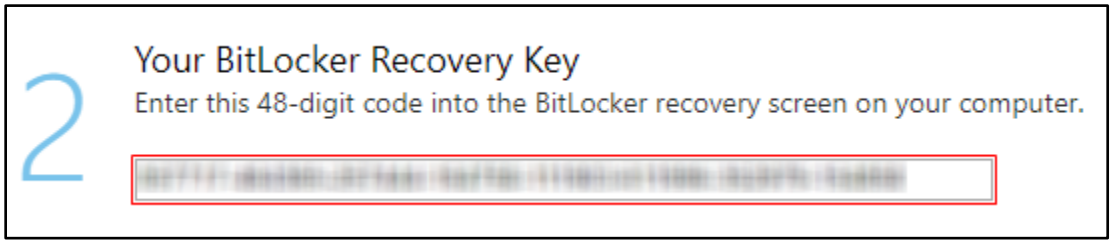

Figure 5

9. Type your **BitLocker Recovery Key** in the text box beneath **Enter recovery key for this drive** on your locked device.

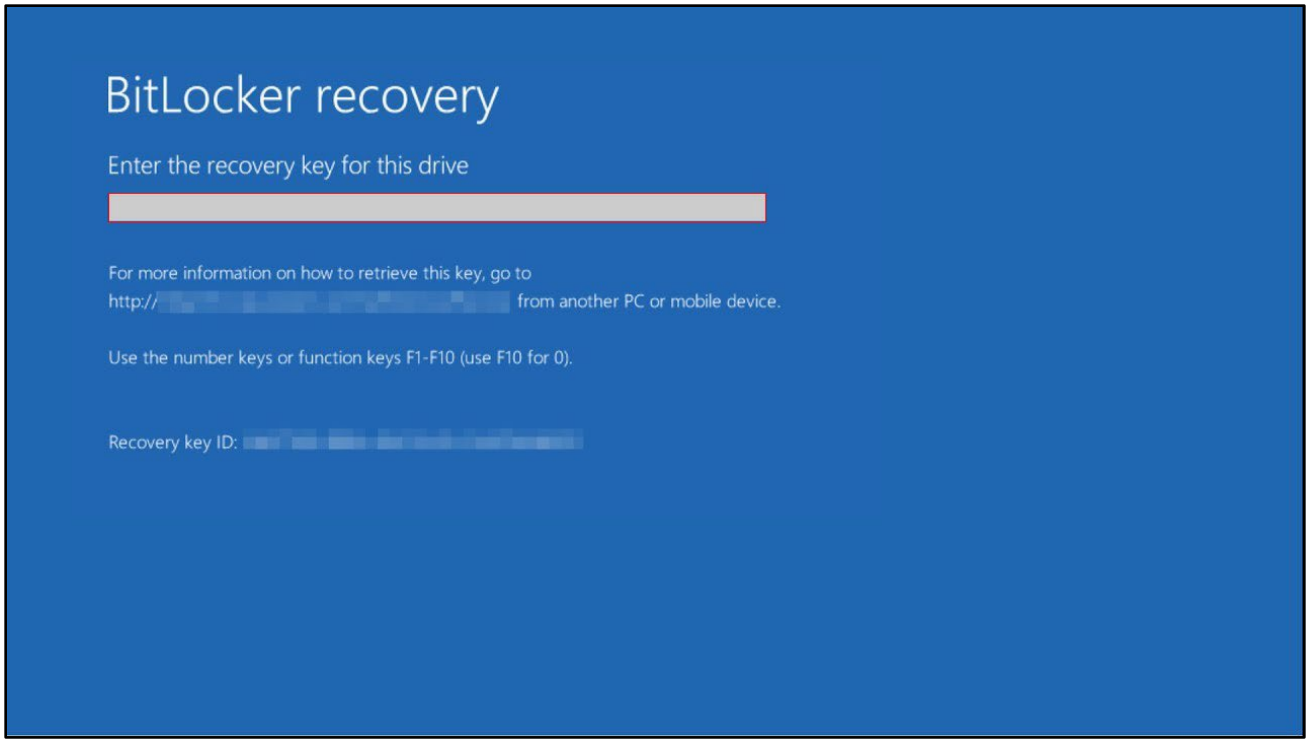

Figure 6

10. Windows will resume starting normally.

Faculty/Staff Help Center

If you are having trouble accessing or using the **Self-Service Portal**, please contact the Faculty/Staff Help Center at 410-704-5151 or submit a **Service Request** by browsing to **https://techhelp.towson.edu**. A technician will be able to retrieve your **Recovery Key** and walk you through the process of unlocking your device.

What should I do after resuming from BitLocker Recovery Mode?

BitLocker protectors on the operating system drive must be reset after resuming from **BitLocker Recovery Mode**. If protectors are not reset, the computer will continue to prompt for the recovery key on startup.

1. Once logged into Windows, and if the computer has an active Internet/network connection, a Microsoft **BitLocker Administration and Monitoring** window will appear stating that the BitLocker disk encryption policy has changed. Click the **Start** button in the window to reset BitLocker protectors on the drive and exit Recovery Mode.

Note: This prompt will not appear without active Internet/network connection, or if you are logged in remotely via Remote Desktop Protocol (RDP). If you are not prompted within a few minutes of logging into Windows, please verify that your computer is connected to the Internet via Ethernet or Wi-Fi and that you have physical access to the computer.

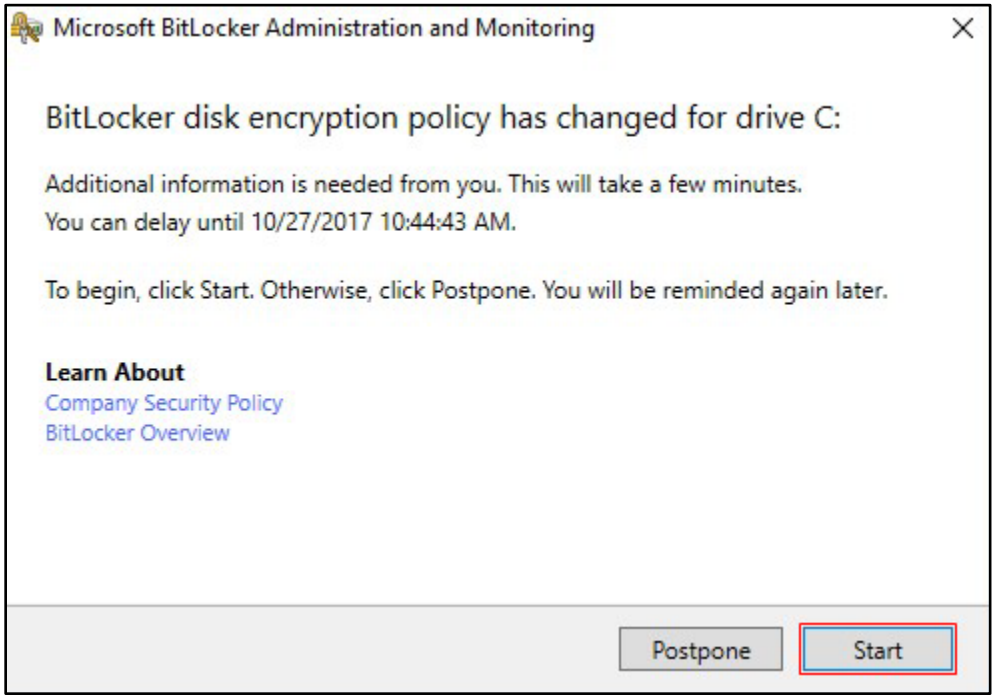

Figure 7