BitLocker recovery without recovery keys

Published Date: Jul 20, 2024

Objective

This is an experimental runbook to consider when you need to access the disk in Windows Recovery mode to delete the offending channel file when Bitlocker Recovery keys are not available.

Applies To

- Supported versions of the Falcon sensor for Windows
- Supported versions of Microsoft Windows
- May require a physical or virtual Trusted Platform Module (TPM)

Procedure

Caution: If the affected system is configured to use RAID, the Storage Controllers within the BIOS of a system must first be changed from RAID to **AHCI**. During boot, load the BIOS options and adjust as appropriate.

Cycle through the blue-screen error (when the host continues to crash) until you get to the recovery screen. Perform the steps below:

1. Navigate to **Troubleshoot > Advanced Options > Startup Settings**
2. Press **Restart**
3. Skip the first Bitlocker recovery key prompt by pressing **Esc**
4. Skip the second Bitlocker recovery key prompt by selecting **Skip This Drive** in the bottom right
5. Navigate to **Troubleshoot > Advanced Options > Command Prompt**
6. Type `bcdedit /set {default} safeboot minimal`, then press **Enter**
7. Close the command prompt window by clicking the X in the top right. This will return you back to the blue screen (WinRE main menu)
8. Select **Continue**.

Your PC will now reboot; it may cycle 2-3 times. Your PC should now boot into safe mode.

1. Select **Other User** from the bottom left-hand side of the screen
2. At the Login screen: Login with your local Admin credentials (normal credentials)

   NOTE: If your device is company owned, you may have to consult your IT helpdesk to gain access to Admin credentials

3. Select **Login**

4. Open Windows Explorer and navigate to **C:\Windows\System32\drivers\Crowdstrike**
5. Delete the offending file (starts with C-00000291*. sys file extension)
6. Open command prompt (as administrator)
7. Type `bcdedit /deletevalue {default} safeboot`, then press **Enter**
8. Restart as normal, confirm normal behaviour

NOTE: Some hosts may have slightly different options and you may not be able to follow these steps exactly. Configurations may exist where these steps will not work.

In the event you are unsuccessful remediating through these steps, please open a CrowdStrike Technical Support case.