SELF-SERVICE CROWDSTRIKE RECOVERY GUIDE

OBJECTIVE

This guide is provided to assist users with devices that are impacted by the CrowdStrike Blue Screen of Death (BSOD) issue to recover their devices themselves

IMPORTANT NOTE: *self-service recovery requires Local Administrator privileges on the device. Typically if you are able to download and install new applications on the device by yourself, this would indicate that you have Local Administrator privileges.*

HOW TO USE THIS GUIDE

This guide has been formatted into three sections with page breaks between each section to enable you to easily print out, or share, just the relative sections of this document to avoid end-user confusion around what scenario applies to them.

SECTIONS

The following sections are available in this guide, for the common scenarios that users may find themselves in. All scenarios require Local Administrator privileges.

1. Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue for devices without Bitlocker
2. Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue with Bitlocker AND without your Bitlocker recovery key
3. Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue with Bitlocker AND with your Bitlocker recovery key

If you are unsure what scenario applies to you, please contact your support team

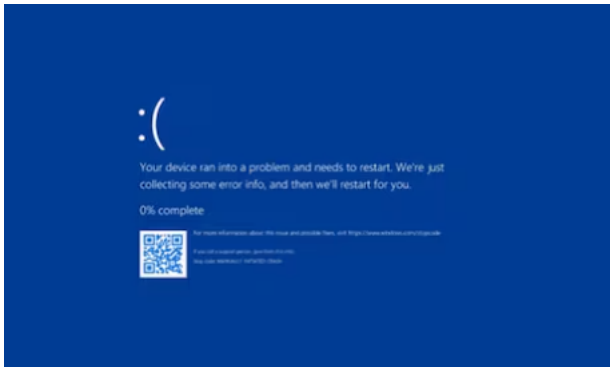
Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue for devices without Bitlocker

If you're experiencing blue screen issues on your workstation due to the recent Crowdstrike outage, please try the below steps to recovery as provided by Crowdstrike.

***IMPORTANT NOTE:** self-service recovery requires Local Administrator privileges on the device. Typically if you are able to download and install new applications on the device by yourself, this would indicate that you have Local Administrator privileges.*

Initial steps

If your PC is now sitting at this screen since Friday 19th July 24, you have most likely been affected by this issue:

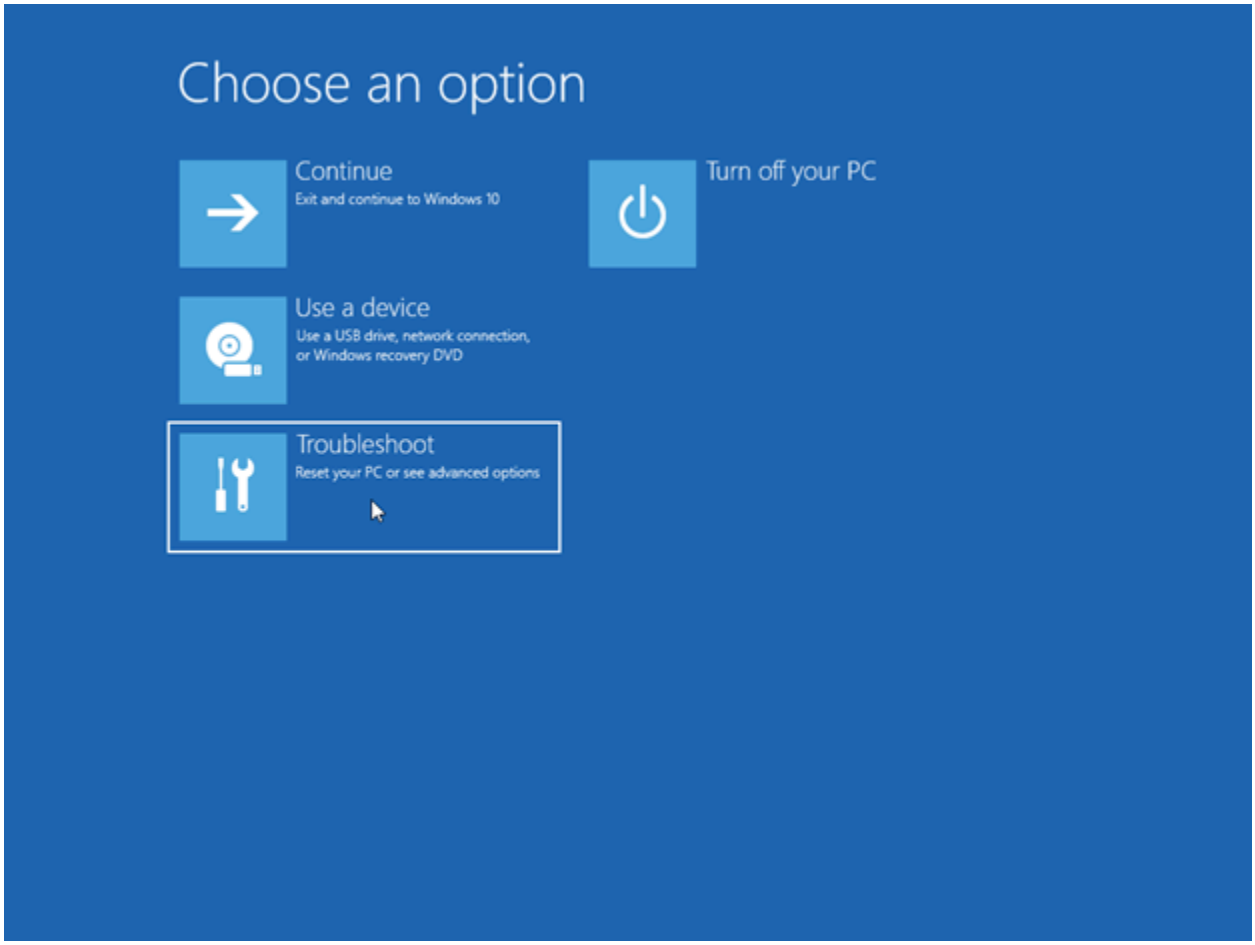


1. If possible, ensure your machine is connected to a wired network (as opposed to using Wi-Fi)
2. Initially, try to reboot the device 2-3 times. If the machine continues to crash or goes into a boot loop, then attempt the following procedure

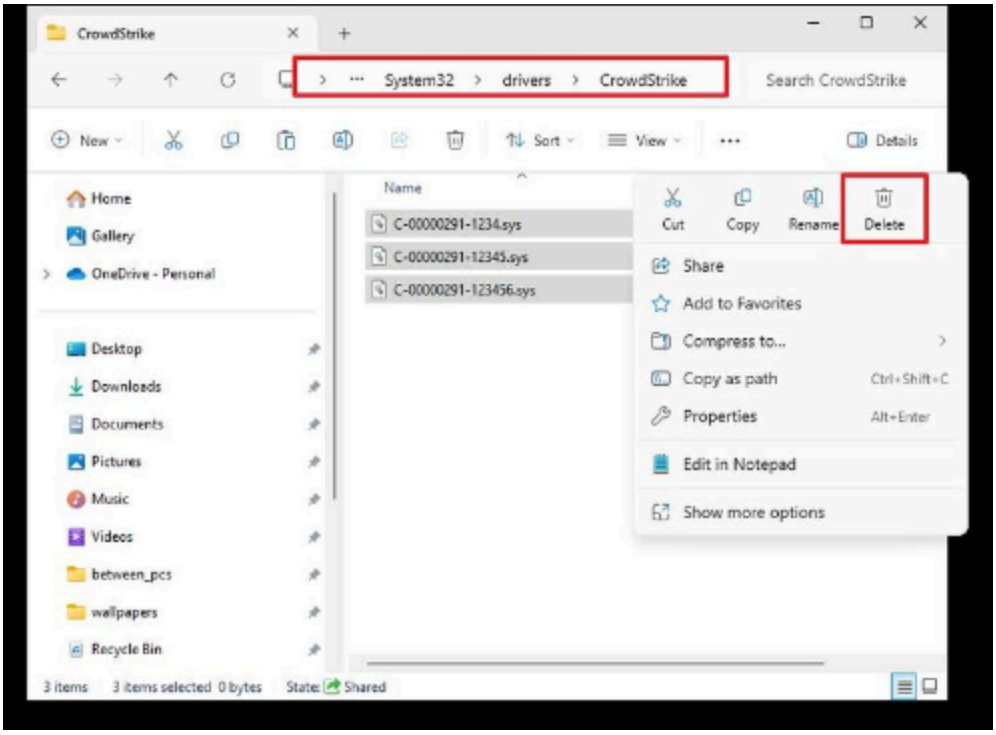
Procedure

1. Hold the power button for 10 seconds to turn off your device and then press the power button again to turn on your device.
2. On the Windows sign-in screen, press and hold the **Shift** key while you select **Power > Restart.**

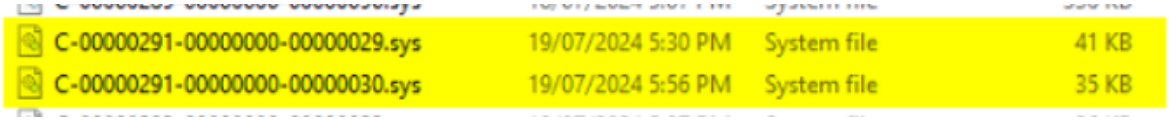
3. After your device restarts to the **Choose an option** screen, select **Troubleshoot**.



4. On the **Troubleshoot** screen, select **Advanced options** > **Startup Settings** > **Enable safe mode**.
5. Press **Restart**
6. At the Login screen, login with your normal credentials
7. Once in Safe Mode and logged on, click on Start and search for Run
8. Open **Run** and enter *%WINDIR%\System32\drivers\CrowdStrike* into the address bar and hit **Enter**. You will see a screen similar to the following:



9. Here, you will need to locate the system file matching “C-00000291” and delete them. File names will be in the format C-X-X-X.sys, where X denotes a string of numbers. You will need to locate and delete any files that have the above string of numbers after C-. Please refer to the screenshot below for example. In some cases there may be more than one file that requires deletion.



10. Once the file is deleted, restart your machine normally and confirm normal behaviour

If issues persist please contact the Service Desk for further assistance.

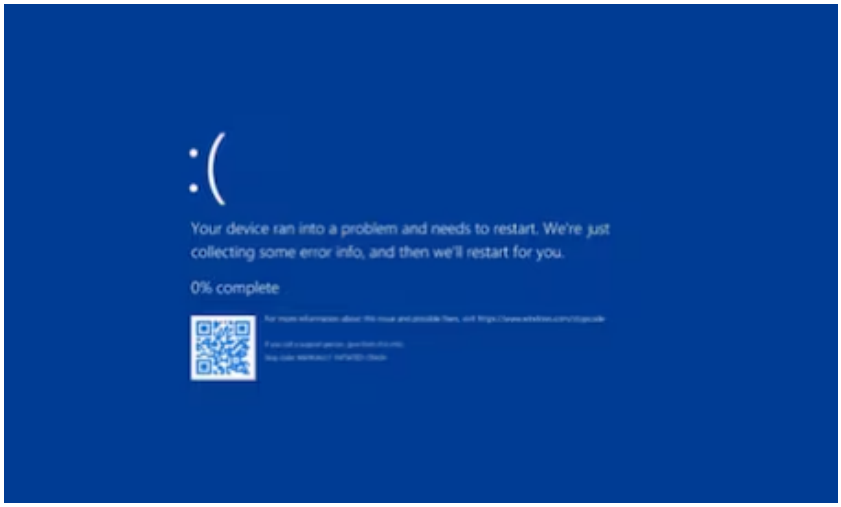
Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue with Bitlocker AND without your Bitlocker recovery key

If you're experiencing blue screen issues on your workstation due to the recent Crowdstrike outage, please try the below steps to recovery as provided by Crowdstrike.

***IMPORTANT NOTE:** self-service recovery requires Local Administrator privileges on the device. Typically if you are able to download and install new applications on the device by yourself, this would indicate that you have Local Administrator privileges.*

Initial steps

If your PC is now sitting at this screen since Friday 19th July 24, you have most likely been affected by this issue:

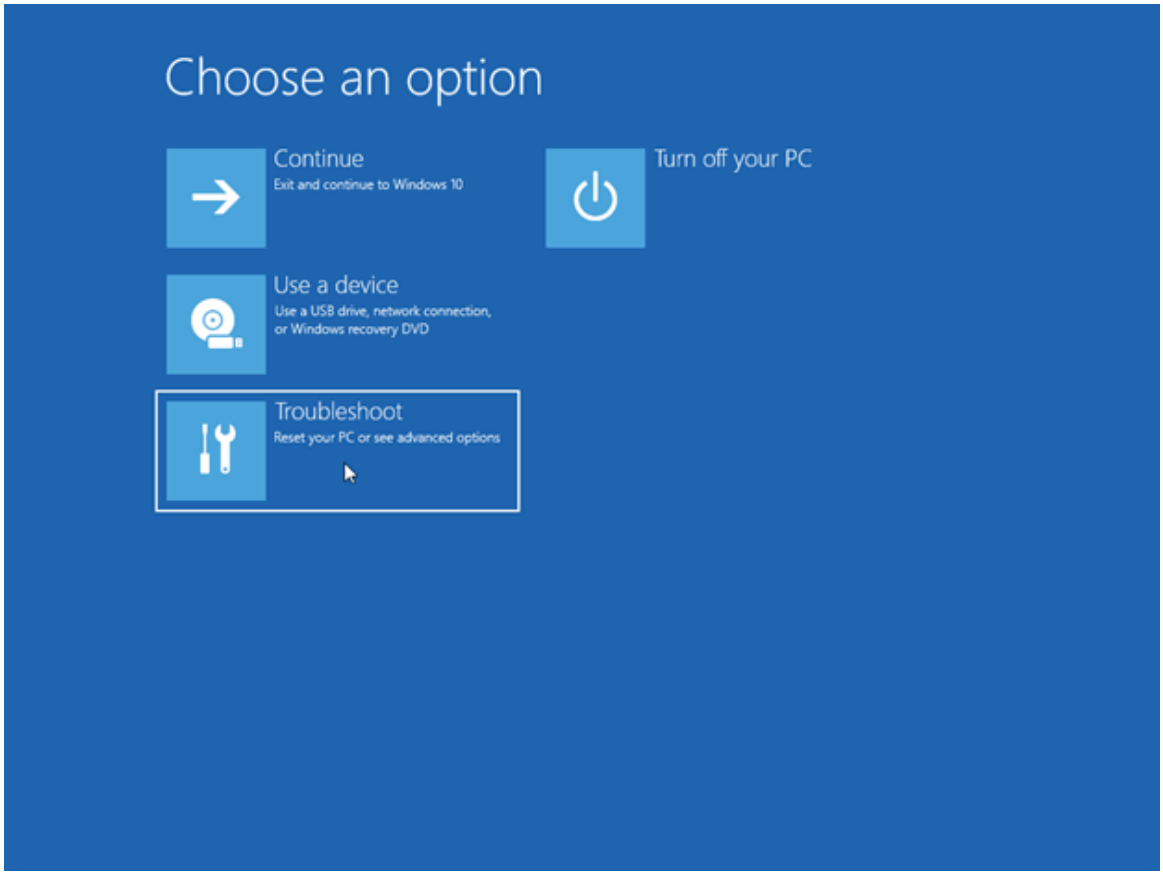


1. If possible, ensure your machine is connected to a wired network (as opposed to using Wi-Fi)
2. Initially, try to reboot the device 2-3 times. If the machine continues to crash or goes into a boot loop, then attempt the following procedure

Procedure

1. Hold the power button for 10 seconds to turn off your device and then press the power button again to turn on your device.
2. On the Windows sign-in screen, press and hold the **Shift** key while you select **Power > Restart.**

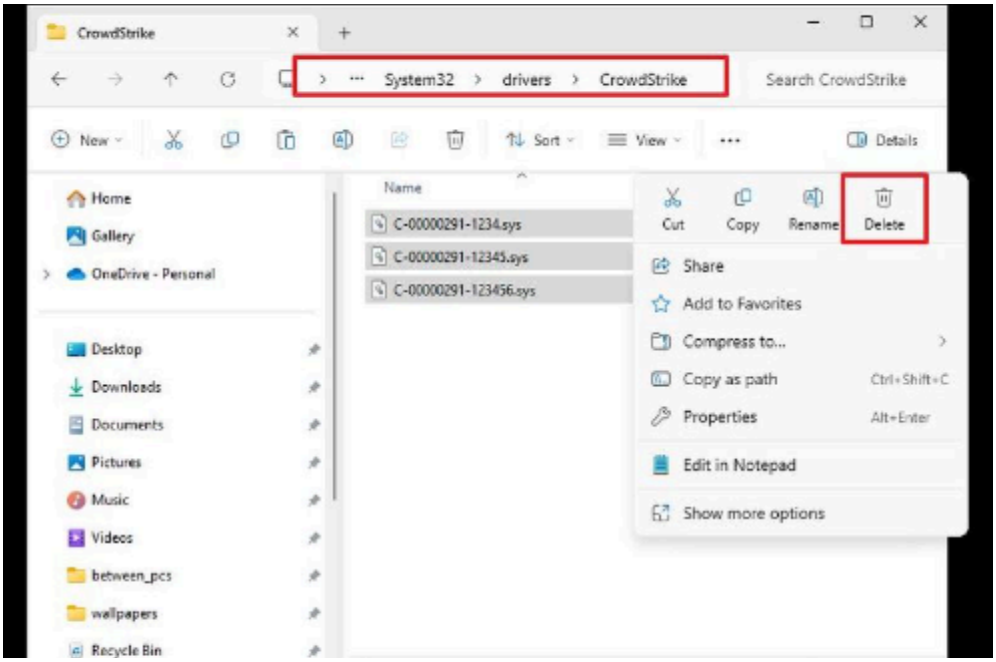
3. After your device restarts to the **Choose an option** screen, select **Troubleshoot**.



4. Navigate to **Troubleshoot > Advanced Options > Startup Settings**
5. Press **Restart**
6. Skip the first Bitlocker recovery key prompt by pressing **Esc**
7. Skip the second Bitlocker recovery key prompt by selecting **Skip This Drive** in the bottom right
8. Navigate to **Troubleshoot > Advanced Options > Command Prompt**
9. Type *bcdedit /set {default} safeboot minimal* then press **Enter**
10. 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)
11. Select **Continue**.

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

12. At the Login screen, login with your normal credentials.
13. Open **Run** and enter *%WINDIR%\System32\drivers\CrowdStrike* into the address bar and hit **Enter**. You will see a screen similar to the following:



14. Here, you will need to locate the system file matching "C-00000291" and delete them. File names will be in the format C-X-X-X.sys, where X denotes a string of numbers. You will need to locate and delete any files that have the above string of numbers after C-. Please refer to the screenshot below for example. In some cases there may be more than one file that requires deletion.

15. Open command prompt (as administrator)
16. Type *bcdedit /deletevalue {default} safeboot* then press **Enter**
17. 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.

If issues persist please contact the Service Desk for further assistance.

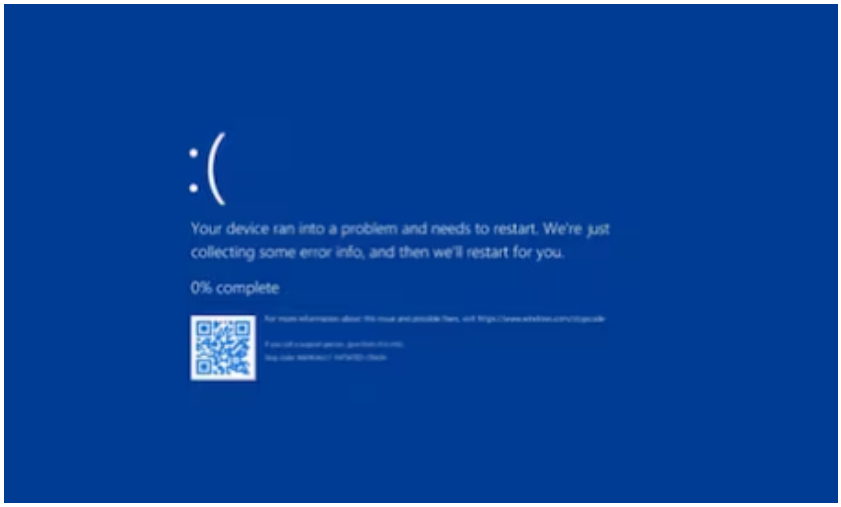
Self-Service Recovery for CrowdStrike Blue Screen of Death (BSOD) issue with Bitlocker AND with your Bitlocker recovery key

If you're experiencing blue screen issues on your workstation due to the recent Crowdstrike outage, please try the below steps to recovery as provided by Crowdstrike.

***IMPORTANT NOTE:** self-service recovery requires Local Administrator privileges on the device. Typically if you are able to download and install new applications on the device by yourself, this would indicate that you have Local Administrator privileges.*

Initial steps

If your PC is now sitting at this screen since Friday 19th July 24, you have most likely been affected by this issue:

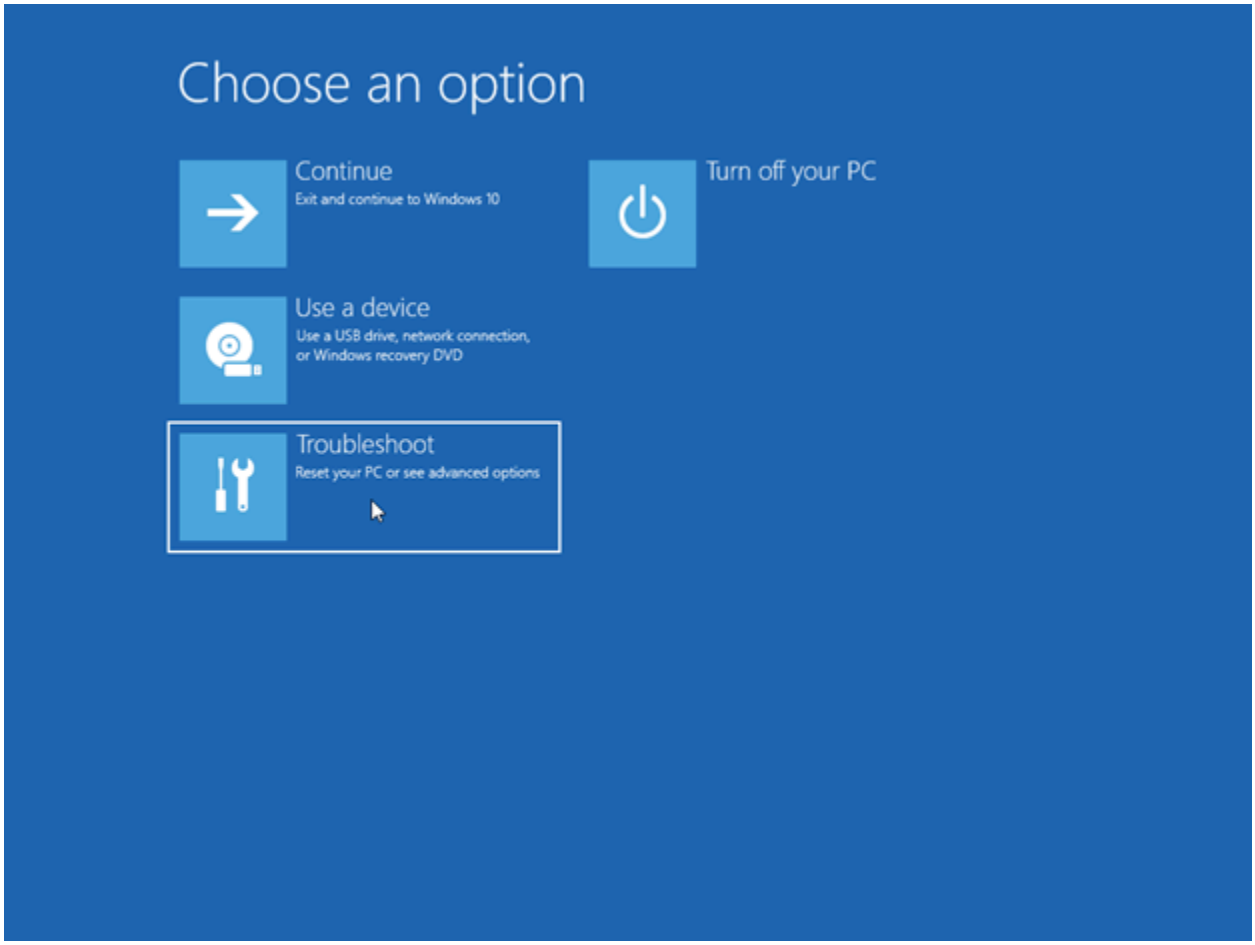


3. If possible, ensure your machine is connected to a wired network (as opposed to using Wi-Fi)
4. Initially, try to reboot the device 2-3 times. If the machine continues to crash or goes into a boot loop, then attempt the following procedure

Procedure

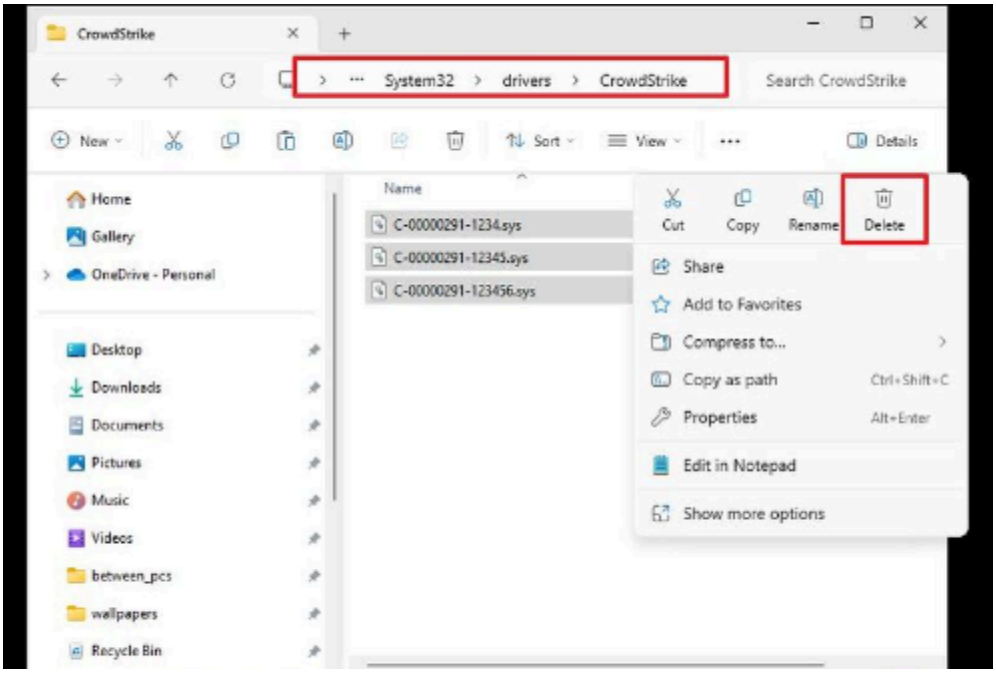
1. Hold the power button for 10 seconds to turn off your device and then press the power button again to turn on your device.
2. On the Windows sign-in screen, press and hold the **Shift** key while you select **Power > Restart.**

3. After your device restarts to the **Choose an option** screen, select **Troubleshoot**.



4. On the **Troubleshoot** screen, select **Advanced options** > **Startup Settings** > **Enable safe mode**.
5. Press **Restart**
6. Upon restart, if you're prompted for a bit locker key please refer to the additional steps below to obtain this from your Microsoft Account.
7. Navigate to and login to https://account.microsoft.com/devices/recoverykey with your company email address and password using a working device
   Important notes:
   a. If you're accessing this on a shared computer please ensure to use a new Incognito or a Private Browsing window and close the window once completed
   b. Bitlocker is used for data encryption and as such these keys should not be shared with anyone.
8. Once logged in, click on **Manage Devices** and you will be able to see the device allocated to you.

9. Click on the drop down arrow to expand and you will see “View Bitlocker Keys”. Click on this and then click on “Show Recovery Key” to view your device recovery key.
10. Enter the recovery key into your impacted device and proceed to Restart
11. At the Login screen login with your normal credentials
12. Open **Run** and enter *%WINDIR%\System32\drivers\CrowdStrike* into the address bar and hit **Enter**. You will see a screen similar to the following:



13. Here, you will need to locate the system file matching “C-00000291” and delete them. File names will be in the format C-X-X-X.sys, where X denotes a string of numbers. You will need to locate and delete any files that have the above string of numbers after C-. Please refer to the screenshot below for example. In some cases there may be more than one file that requires deletion.

14. 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.

If issues persist please contact the Service Desk for further assistance.