Issue How to Fix CrowdStrike Blue Screen Issue

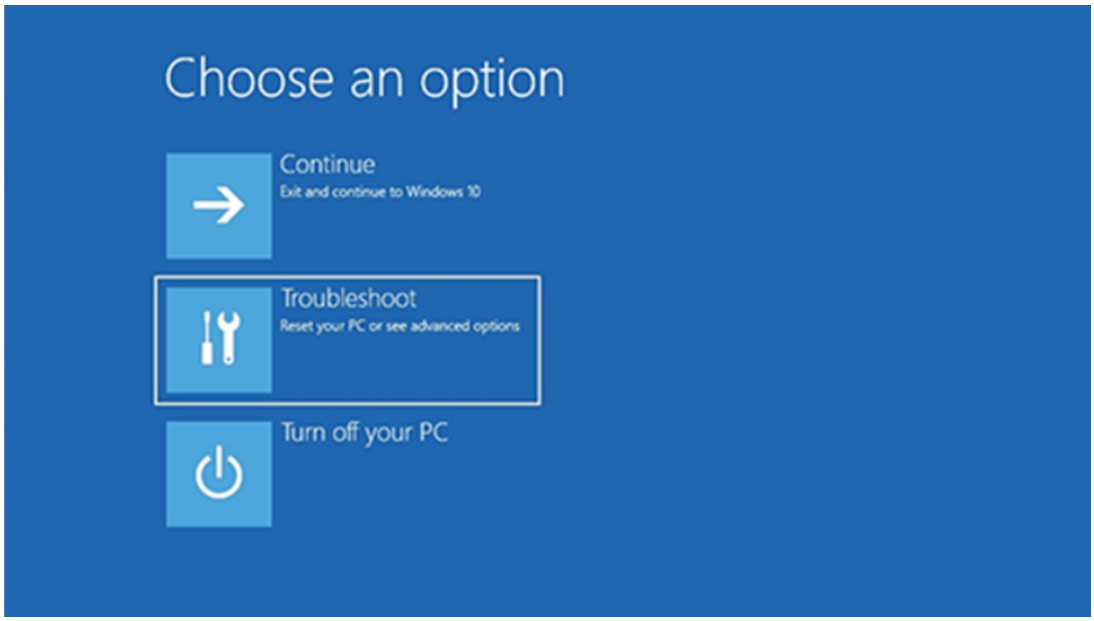
Jeffrey Pierce - 2024-07-23 - Comments (0) - Security

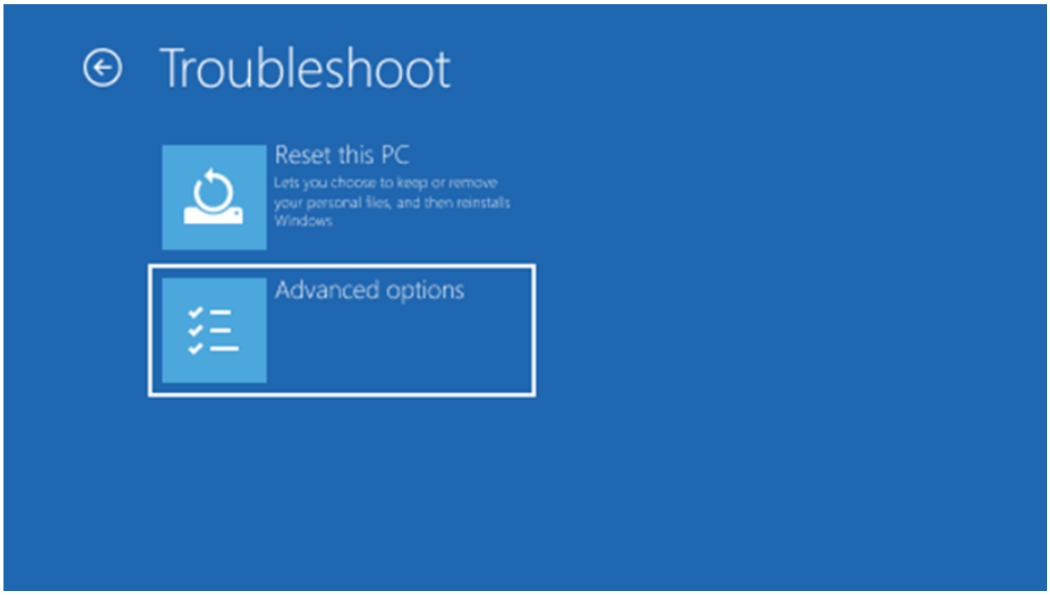
To restore a Windows machine to full working condition perform the following steps:

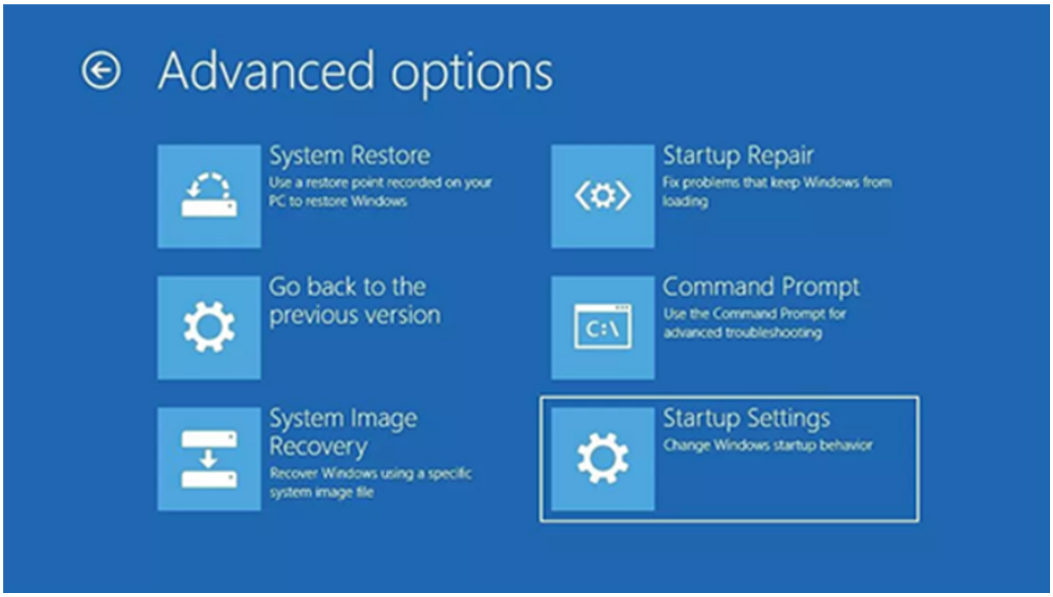
1. Boot Windows into Safe Mode/Windows Recovery Environment by following these steps in this article.

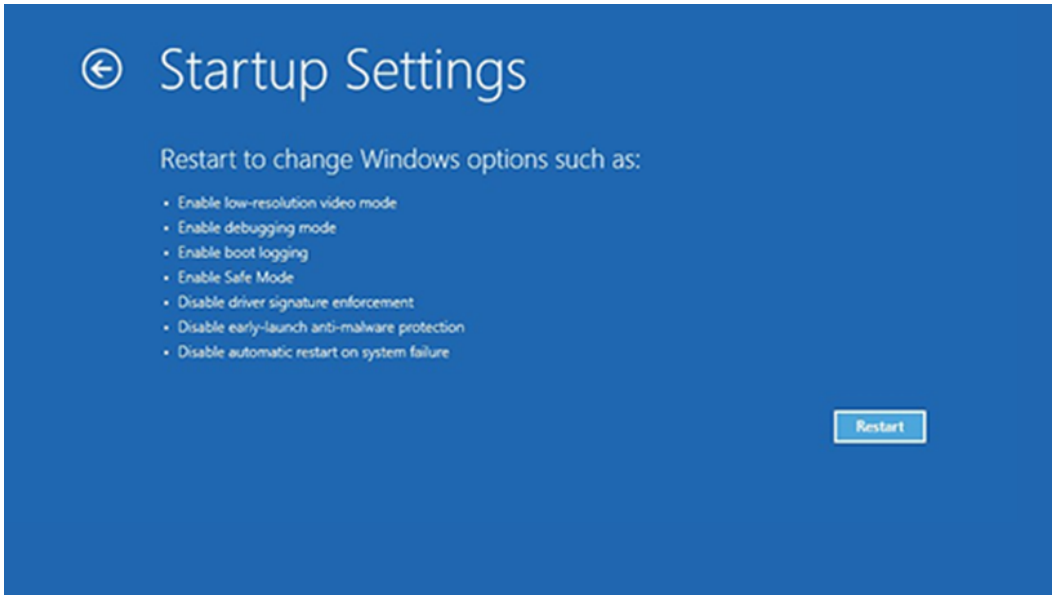
You may see an option on your screen to select **Advanced options**.

On the Choose an option screen, select **Troubleshoot > Advanced options > Startup Settings > Restart**.




Troubleshoot
Reset this PC
Lets you choose to keep or remove your personal files, and then reinstalls Windows
Advanced options


Advanced options
System Restore
Use a restore point recorded on your PC to restore Windows
Startup Repair
Fix problems that keep Windows from loading
Go back to the previous version
Command Prompt
Use the Command Prompt for advanced troubleshooting
C:\
System Image Recovery
Recover Windows using a specific system image file
Startup Settings
Change Windows startup behavior


Startup Settings
Restart to change Windows options such as:
Enable low-resolution video mode
Enable debugging mode
Enable boot logging
Enable Safe Mode
Disable driver signature enforcement
Disable early-launch anti-malware protection
Disable automatic restart on system failure
Restart

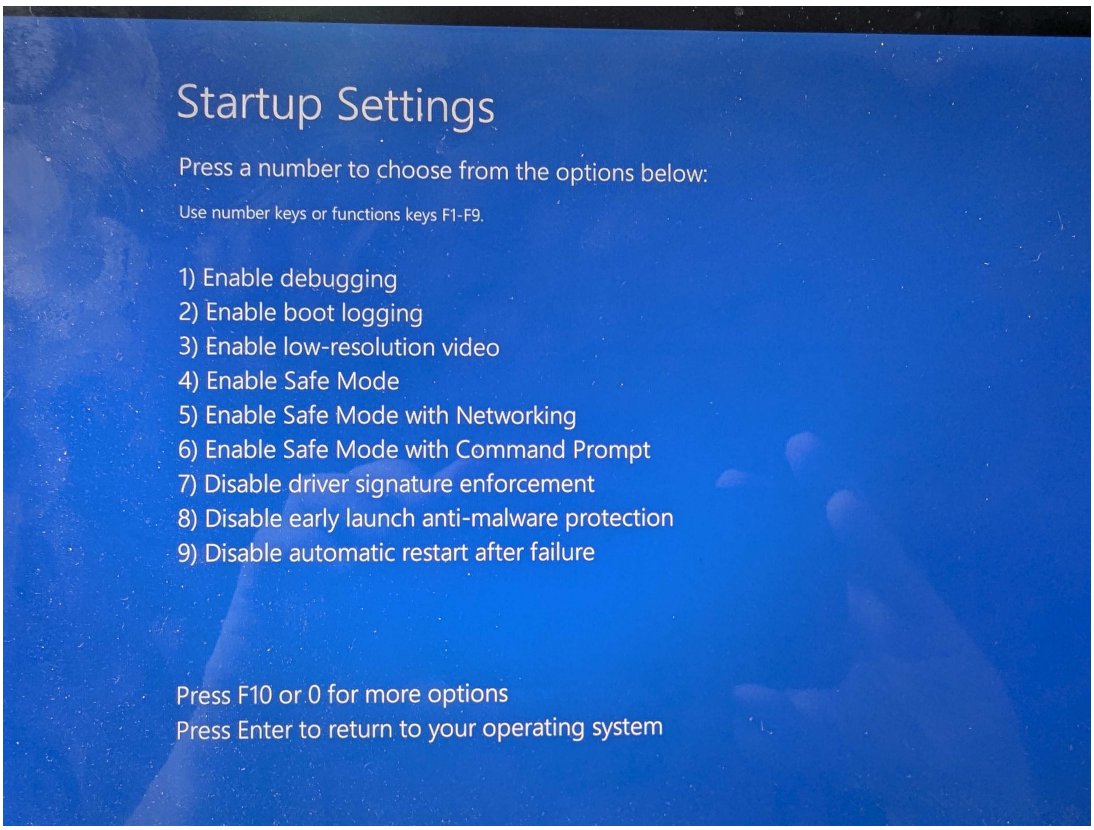
Microsoft has a detailed technical article on the process at: https://support.microsoft.com/en-us/windows/start-your-pc-in-safe-mode-in-windows-92c27cff-db89-8644-1ce4-b3e5e56fe234

1a. If your computer is prompting you for a Bitlocker key, please reach out to Brown IT support staff by calling the OIT Help Desk:

- Chat: https://helpchat.brown.edu
- Email: help@brown.edu
- Phone: (401) 863-4357
- Submit a ticket: https://ithelp.brown.edu/new-ticket

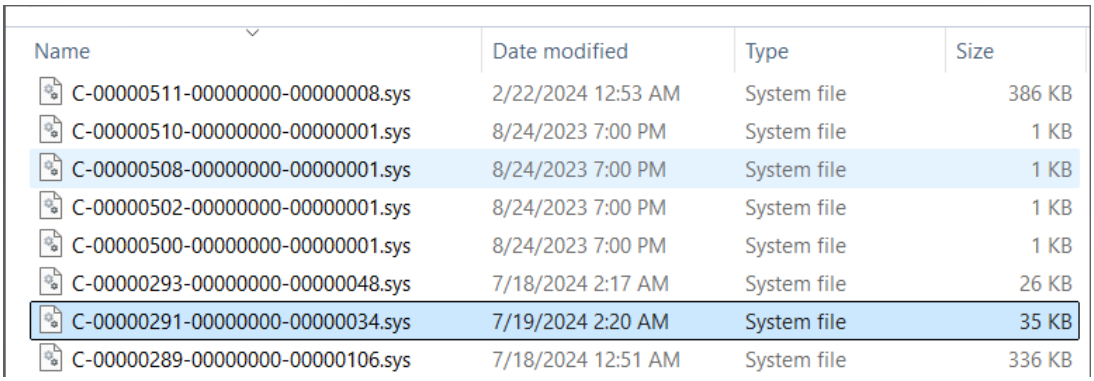
1b. Enter the **recovery key** to continue the Safe Mode boot process.

2. Press **4** to **Enable Safe Mode**. Once you have successfully started your computer in Safe Mode, continue to Step 3.



3. Once you are at the desktop in safe mode, there are files to be deleted that will help to clear the issue. Press the **Windows Key + E** and navigate to the "C:\Windows\System32\drivers\CrowdStrike" directory.

4. Locate the file(s) matching “C-00000291*.sys”, and delete them. A file time timestamp of 7/19/24 1:27AM or later is a good version. Previous timestamps may cause bluescreen.



Name	Date modified	Type	Size
C-00000511-00000000-00000008.sys	2/22/2024 12:53 AM	System file	386 KB
C-00000510-00000000-00000001.sys	8/24/2023 7:00 PM	System file	1 KB
C-00000508-00000000-00000001.sys	8/24/2023 7:00 PM	System file	1 KB
C-00000502-00000000-00000001.sys	8/24/2023 7:00 PM	System file	1 KB
C-00000500-00000000-00000001.sys	8/24/2023 7:00 PM	System file	1 KB
C-00000293-00000000-00000048.sys	7/18/2024 2:17 AM	System file	26 KB
C-00000291-00000000-00000034.sys	7/19/2024 2:20 AM	System file	35 KB
C-00000289-00000000-00000106.sys	7/18/2024 12:51 AM	System file	336 KB

5. Boot the host normally.