# **10-Step Guide to Resolving Windows 11 Upgrade Issues**

Upgrading to Windows 11 can present various challenges, from hardware compatibility to software conflicts. This guide provides ten practical steps to identify and resolve common issues, ensuring a smoother transition to Microsoft's latest operating system.

# Key Takeaways

Step	Action	Purpose
1	Verify System Requirements	Ensure your hardware meets Windows 11's minimum specifications.
2	Update Device Drivers	Prevent compatibility issues by using the latest drivers.
3	Backup Important Data	Protect your files against potential data loss during the upgrade.
4	Disable Non-Essential Startup Programs	Reduce the risk of software conflicts during installation.
5	Check for Software Updates	Ensure all applications are updated to versions compatible with Windows 11.
6	Run Disk Cleanup	Free up space and remove potential sources of conflict.
7	Uninstall VPN Clients	Prevent network-related installation issues.
8	Adjust CPU Voltage	Stabilize system performance during the upgrade process.
9	Check and Replace Faulty RAM	Ensure system stability by identifying and replacing defective memory modules.
10	Run System File Checker (SFC) and DISM	Repair corrupted system files to facilitate a successful upgrade.

# **Step 1: Disable Fast Startup**

Disabling Fast Startup can help resolve the KMODE\_EXCEPTION\_NOT\_HANDLED error by ensuring a complete system shutdown, which prevents potential driver conflicts upon reboot.

- 1. **Open the Control Panel:** 
  - Press the Windows key and type Control Panel.
  - Click on the **Control Panel** app in the search results.
- 2. Navigate to Power Options:
  - In the Control Panel, set the **View by** option to **Large icons** or **Small icons** for easier navigation.
- Click on **Power Options**.
- 3. Access System Settings:
  o In the left-hand menu, click on Choose what the power buttons do.
- 4. Modify Shutdown Settings:
  - If the **Turn on fast startup (recommended)** option is grayed out, click on **Change settings that are currently unavailable** at the top of the window.
- Under the Shutdown settings section, uncheck the box labeled Turn on fast startup (recommended).
   5. Save Changes:

• Click the **Save changes** button at the bottom to apply the new settings.

**Expert Tip:** While Fast Startup aims to reduce boot times by preloading some system information, it can sometimes cause issues with certain drivers or hardware configurations. Disabling this feature ensures that your system performs a full shutdown, which can help in troubleshooting persistent errors like the KMODE\_EXCEPTION\_NOT\_HANDLED. In my experience, I've found that turning off Fast Startup has resolved similar issues for many users, especially when dealing with legacy hardware or drivers.

#### **Step 2: Update or Reinstall Faulty Drivers**

Updating or reinstalling faulty drivers can resolve the KMODE\_EXCEPTION\_NOT\_HANDLED error by ensuring hardware components communicate correctly with the operating system.

#### 1. **Open Device Manager:**

- Press the Windows key + x and select Device Manager.
- 2. Identify Problematic Drivers:
- Look for devices marked with a yellow exclamation mark, indicating issues.
- 3. **Update the Driver:** 
  - Right-click the problematic device and select **Update driver**.
  - Choose **Search automatically for updated driver software**.
- Windows will search and install the latest driver if available.
  4. Reinstall the Driver (if updating doesn't help):
  - Right-click the device and select **Uninstall device**
  - Confirm by clicking Uninstall.
  - Restart your computer; Windows will automatically reinstall the driver upon reboot.

**Expert Tip:** While Windows Update can handle many driver updates, it might not cover all hardware components. For instance, graphics cards often require drivers directly from the manufacturer's website. In my experience, manually updating these drivers can prevent conflicts that automated tools might miss. Additionally, always create a system restore point before making significant driver changes to safeguard your system.

# **Step 3: Install Missing Drivers**

Installing missing drivers is crucial for ensuring that all hardware components function correctly and to prevent errors like the KMODE\_EXCEPTION\_NOT\_HANDLED.

- 1. **Open Device Manager:**
- Press the Windows key + x and select Device Manager.
- 2. Identify Missing Drivers:
   o Look for devices labeled as Unknown Device or those with a yellow exclamation mark, indicating missing drivers.
- 3. Install Drivers Automatically:
- Right-click the device and select **Update driver**.
- Choose **Search automatically for updated driver software**. Windows will attempt to find and install the appropriate driver.
- 4. Install Drivers Manually:
   If Windows cannot find the driver, visit the device manufacturer's website to download the latest driver.
  - Once downloaded, right-click the device in Device Manager and select Update driver.
  - Choose Browse my computer for driver software and navigate to the downloaded driver file to install it.

**Expert Tip:** In some cases, Windows may not detect the necessary drivers, especially for specialized hardware. I've encountered situations where using dedicated driver update tools, such as <u>EaseUS DriverHandy</u>, has been invaluable. These tools can scan your system for missing or outdated drivers and facilitate their installation, ensuring optimal hardware performance. Always ensure that you download drivers to avoid potential security risks.

# **Step 4: Uninstall Incompatible Programs**

Incompatible software can cause system instability, leading to errors like the KMODE\_EXCEPTION\_NOT\_HANDLED. Removing such programs can help maintain system stability.

- 1. Access Programs and Features:
- Press the Windows key, type Control Panel, and press Enter.
- Navigate to Programs > Programs and Features.
   Identify Potentially Incompatible Programs:
- Review the list of installed programs and note any recently installed or unfamiliar applications.
- 3. Uninstall the Problematic Program:o Select the program in question.
- Click on **Uninstall** and follow the on-screen instructions.
- 4. Use Advanced Uninstaller Tools (if necessary):

• If standard uninstallation fails, consider using tools like <u>Revo Uninstaller</u> to remove stubborn programs and residual files.

Expert Tip: In my experience, some programs leave behind residual files and registry entries even after uninstallation. Utilizing advanced uninstaller tools ensures a thorough cleanup, preventing potential conflicts. Always ensure you have backups before making significant system changes.

### **Step 5: Uninstall Third-Party Antivirus Software**

Third-party antivirus programs can sometimes conflict with system processes, leading to performance issues or software incompatibilities. Removing these programs can help maintain system stability.

#### Why Uninstall Third-Party Antivirus Software?

- **System Conflicts:** Multiple security programs can interfere with each other, causing system slowdowns or crashes.
- System Connects: Multiple security programs can interfere with each outer, causing system of a security features, making additional antivirus software unnecessary.
- Resource Consumption: Third-party antivirus programs can consume significant system resources, affecting performance.

# Steps to Uninstall Third-Party Antivirus Software

- 1. Access the Control Panel: Press Win + R, type control panel, and press Enter.
- 2. Navigate to Programs: Click on *Programs* or *Programs and Features*.
- 3. **Select the Antivirus Program:** Find the third-party antivirus software in the list of installed programs.
- 4. **Initiate Uninstallation:** Click on the program and select *Uninstall*. Follow the on-screen prompts to complete the process.
- 5. **Restart Your Computer:** After uninstallation, restart your system to apply changes.

# **Using Specialized Removal Tools**

Some antivirus programs may not uninstall completely through standard methods. In such cases, specialized removal tools provided by the software vendors can be used:

- Avast Uninstall Utility
- <u>AVG Remover Tool</u>
- <u>Bitdefender Uninstall Tool</u>
- <u>Kaspersky Removal Tool</u>
  <u>McAfee Consumer Product Removal Tool</u>

For a comprehensive list of removal tools, refer to this **ESET Knowledgebase article**.

# **Expert Advice**

As an IT professional, I've encountered numerous instances where residual files from uninstalled antivirus programs caused system instability. It's crucial to ensure that all components are thoroughly removed. Utilizing vendor-specific removal tools can help achieve a clean uninstallation.

# **Reactivating Windows Defender**

After uninstalling third-party antivirus software, it's advisable to ensure that Windows Defender (the built-in antivirus for Windows) is active:

- 1. Press Win + I to open Settings.
- 2. Navigate to *Update & Security > Windows Security*.
- 3. Click on *Virus & threat protection*.4. Ensure that Windows Defender is turned on. If not, follow the prompts to activate it.

For more detailed instructions, visit this <u>Microsoft Community thread</u>.

### **Recommended Tool for Thorough Uninstallation**

For a more comprehensive removal of stubborn antivirus programs and their residual files, consider using <u>IObit Uninstaller PRO</u>. This tool can help ensure that all components are completely removed from your system.

# IObit Uninstaller PRO

By following these steps, you can effectively remove third-party antivirus software and maintain your system's performance and security.

# **Step 6: Update BIOS**

Updating the BIOS (Basic Input/Output System) is a critical task that can enhance system stability, compatibility, and performance. However, it should be approached with caution, as an incorrect update can render your system unbootable.

# **Understanding BIOS**

The BIOS is firmware embedded on your motherboard that initializes hardware components during the boot process. Keeping it updated ensures that your system can support new hardware and fix known issues.

# **Preparation Steps**

- 1. Identify Your BIOS Version: Press Windows + R, type msinfo32, and press Enter. In the System Information window, note the BIOS Version/Date.
- 2. **Check for Updates:** Visit your motherboard manufacturer's support page to see if a newer BIOS version is available.
- 3. **Backup Important Data:** Although updating the BIOS doesn't typically affect data on your drives, it's prudent to back up important files. 4. **Ensure Stable Power:** Use an uninterruptible power supply (UPS) to prevent power loss during the update, which could corrupt the BIOS.

# Updating the BIOS

The update process varies by manufacturer. Below is a general guide:

- 1. **Download the Update:** Obtain the latest BIOS file from your motherboard's support page.
- 2. **Prepare a USB Drive:** Format a USB drive to FAT32 and copy the BIOS file to it.
- 3. Enter BIOS Setup: Restart your computer and press the designated key (commonly F2, F12, or Delete) during startup to access the BIOS.
- 4. **Initiate the Update:** Use the BIOS utility to select the BIOS file on your USB drive and follow the on-screen instructions.

For detailed instructions, refer to your motherboard's manual or the manufacturer's website. For example, ASUS provides a comprehensive guide on updating the BIOS using their EZ Flash utility. :contentReference[oaicite:0]{index=0}

#### Expert Advice

As an IT professional, I've encountered systems rendered inoperable due to improper BIOS updates. Always double-check that you're using the correct BIOS file for your specific motherboard model. If you're uncertain, consult with a professional or contact the manufacturer's support.

# **Additional Resources**

- Intel's Guide on Updating BIOS
- Dell BIOS and UEFI Update Guide

Remember, while updating the BIOS can provide benefits, it also carries risks. Ensure you're well-prepared and understand the process before proceeding.

# **Step 7: Uninstall VPN Clients**

Removing VPN clients is essential to prevent potential conflicts and system errors. As an expert in system optimization, I've encountered cases where outdated or incompatible VPN software caused issues like the **KMODE\_EXCEPTION\_NOT\_HANDLED** error, leading to system crashes. To ensure your system runs smoothly, follow these steps to uninstall VPN clients:

# **Uninstalling VPN Clients on Windows**

- 1. **Open Settings:** Press Win + I to open the Settings app.
- 2. Navigate to Apps: Click on Apps.
- 3. Find the VPN Application: Scroll through the list to locate your VPN client.4. Uninstall: Select the VPN application and click *Uninstall*. Confirm when prompted.

For a more thorough removal, especially if you encounter issues during uninstallation, consider using specialized uninstaller tools. These tools can help remove residual files and registry entries that standard uninstallation might miss.

**Removing VPN Connections via Network Settings** 

After uninstalling the VPN client, ensure that any residual VPN connections are removed:

- 1. **Open Network Settings:** Press Win + I, then go to *Network & Internet*.
- 2. **Select VPN:** Click on *VPN* from the left-hand menu.
- 3. **Remove VPN Connection:** Select the VPN connection you wish to remove and click *Remove*.

For advanced users, VPN connections can also be removed using PowerShell:

Get-VpnConnection | Remove-VpnConnection -Force

This command lists all VPN connections and removes them forcefully. Use this method with caution, as it will remove all VPN connections without additional confirmation.

#### **Expert Advice**

In my experience, some VPN clients leave behind network adapters or services that can cause conflicts even after uninstallation. To address this:

- Check Network Adapters: Open Device Manager, expand Network adapters, and uninstall any adapters related to your VPN.
- Clean Up Residual Files: Navigate to the installation directory of the VPN client (usually in C:\Program Files or C:\Program Files (x86)) and delete any remaining files or folders.
- **Registry Cleanup:** Use a reliable registry cleaner to remove leftover entries. Always back up your registry before making changes.

By thoroughly removing VPN clients and their associated components, you can prevent potential system conflicts and ensure optimal performance.

#### **Alternative VPN Solutions**

If you still require VPN services, consider using reputable and well-supported VPN clients. One such option is <u>NordVPN</u>, known for its reliability and extensive server network.

Remember, always download VPN software from official sources and keep them updated to minimize security risks and compatibility issues.

### **Step 8: Adjust CPU Voltage**

Adjusting your CPU's voltage can help resolve the **KMODE\_EXCEPTION\_NOT\_HANDLED** error. However, this process requires caution, as improper voltage settings can lead to system instability or hardware damage.

#### **Understanding CPU Voltage**

The CPU voltage, often referred to as Vcore, is the power supplied to your processor. Adjusting this voltage can stabilize your system, especially if you're experiencing errors or have modified your CPU's performance settings.

#### Steps to Adjust CPU Voltage

1. Access the BIOS/UEFI: • Restart your computer.

- During the boot process, press the designated key (commonly Delete or F2) to enter the BIOS/UEFI settings.
- 2. Navigate to Voltage Settings:
- Within the BIOS/UEFI interface, locate the section related to CPU settings. This might be labeled as "Overclocking," "Advanced CPU Configuration," or similar.
- Find the CPU voltage settings, often listed as "Vcore" or "CPU Core Voltage."
- 3. Adjust the Voltage:
   It's advisable to make small adjustments, typically in increments of 0.01V.
  - After each adjustment, monitor your system's stability. Tools like CPU-Z or HWMonitor can assist in this process.
- 4. Save and Exit:
  - Once you've made the necessary adjustments, save your changes and exit the BIOS/UEFI.
  - Your system will reboot with the new voltage settings.

#### **Expert Advice**

In my experience, adjusting the CPU voltage can be a delicate process. It's essential to monitor your system's temperatures and stability after each change. If you're unsure or uncomfortable with these adjustments, consulting with a professional or referring to your motherboard's manual is recommended.

Remember, while adjusting CPU voltage can help resolve certain errors, it's crucial to proceed with caution to avoid potential system instability.

# **Step 9: Check and Replace Faulty RAM**

Random Access Memory (RAM) is crucial for your computer's performance. Faulty RAM can lead to system instability, crashes, and data corruption. Here's how to identify and replace defective RAM modules.

# Symptoms of Faulty RAM

- Random Blue Screens of Death (BSOD)
- System crashes or restarts
- Operating system freezes Missing memory in system properties

# **Testing Your RAM**

To diagnose RAM issues, you can use built-in or third-party tools:

- 1. Windows Memory Diagnostic:
  - 1. Press Win + R, type mdsched.exe, and press Enter.
  - 2. Choose "Restart now and check for problems."3. Your system will reboot and run the test. Results will be displayed after logging back in.
- 2. MemTest86:
  - 1. Download MemTest86 from the official website.
  - 2. Create a bootable USB drive with the tool.
  - 3. Boot from the USB drive and follow the on-screen instructions to run the test

# **Identifying the Faulty Module**

If you have multiple RAM sticks installed:

- 1. Power off your computer and unplug it.
- 2. Remove all but one RAM module.
- 3. Boot the system and run the memory test.
- 4. If the test passes, repeat with the next module until you identify the faulty one.

# **Replacing Faulty RAM**

Once you've identified the defective module:

- 1. Purchase a replacement module that matches the specifications of your existing RAM (e.g., DDR4, same speed, and latency).
- 2. Install the new module into the appropriate slot, ensuring it's securely seated.
- 3. Boot your system and run a memory test to confirm the new module is functioning correctly.

# **Expert Advice**

In my experience, it's essential to handle RAM modules with care to prevent static damage. Always ground yourself before touching internal components. Additionally, mixing different brands or speeds of RAM can lead to instability. It's best to use matching modules to ensure optimal

#### performance.

# Step 10: Run System File Checker (SFC) and DISM

Over time, Windows system files can become corrupted or go missing, leading to system instability. To address these issues, Windows provides two powerful utilities: **System File Checker (SFC)** and **Deployment Image Servicing and Management (DISM)**. As an IT professional, I've found these tools invaluable for maintaining system integrity.

#### **Understanding SFC and DISM**

- **SFC**: Scans and repairs corrupted or missing system files by replacing them with cached copies stored in the system.
- **DISM**: Repairs the Windows image itself, addressing component store corruption that might prevent SFC from functioning correctly.

#### When to Use These Tools

- 1. System crashes or instability: Unexpected crashes or frequent errors can indicate corrupted system files.
- Failed Windows updates: If updates aren't installing properly, system file corruption might be the cause.
   Application errors: Programs failing to start or crashing unexpectedly can result from underlying system file issues.

# Running DISM and SFC

It's advisable to run DISM before SFC to ensure the system image is healthy, allowing SFC to function effectively. Here's how:

#### 1. Open the **Command Prompt** with administrative privileges:

- Press Windows + x and select **Command Prompt (Admin)** or **Windows PowerShell (Admin)**. 2. Run the DISM tool:
- Type DISM.exe /Online /Cleanup-image /Restorehealth and press Enter. 3. After DISM completes, run the SFC tool:
- Type sfc /scannow and press Enter.

These commands can take some time to complete. Ensure you don't interrupt the process.

#### **Interpreting Results**

After running SFC, you might encounter the following messages:

- No integrity violations found: Your system files are intact.
- Corrupt files repaired: Issues were found and fixed.
  Corrupt files found but unable to fix: Manual repair may be required.

# **Expert Advice**

In my experience, regularly running these tools can preemptively address potential system issues. However, always ensure you have a recent backup before making significant system changes. If SFC and DISM can't resolve the problems, consider restoring from a backup or performing a system reset.

#### **Additional Resources**

For more detailed information, refer to Microsoft's official documentation on using the System File Checker tool to repair missing or corrupted system files. :contentReference[oaicite:0]{index=0}

# **Frequently Asked Questions**

#### 1. What should I do if my computer displays a blue screen error?

A blue screen error, also known as a "stop error," indicates that Windows has encountered a critical issue and must restart. To troubleshoot:

- Note any error codes or messages displayed during the blue screen.
- After the system restarts, check the "Event Viewer" for detailed error logs.
- Ensure all hardware drivers are up-to-date.
  Run diagnostics on your hardware components, especially RAM and storage devices.

In my experience, many blue screen errors are caused by driver conflicts or faulty hardware. Regular system maintenance can prevent these issues.

#### 2. How can I identify and replace faulty RAM?

Faulty RAM can cause system instability, crashes, and data corruption. To diagnose and replace faulty RAM:

- 1. Use the built-in Windows Memory Diagnostic tool:
- Press Win + R, type mdsched.exe, and press Enter.
- Choose to restart and check for problems.
- 2. If errors are detected, power off your computer and open the case.
- 3. Locate the RAM modules and remove them one at a time, testing the system after each removal to identify the faulty module.
- 4. Once identified, replace the faulty RAM with a compatible module.

As an expert, I recommend using high-quality RAM from reputable manufacturers to minimize the risk of future issues.

#### 3. What is the purpose of the System File Checker (SFC) and DISM tools?

The System File Checker (SFC) and Deployment Imaging Service and Management Tool (DISM) are utilities designed to repair corrupted system files:

- **SFC:** Scans and repairs corrupted or missing system files.
- Run it by opening Command Prompt as an administrator and typing sfc /scannow.
- **DISM:** Repairs the system image and can fix issues that SFC cannot.
- Run it by typing DISM /Online /Cleanup-Image /RestoreHealth in Command Prompt as an administrator.

In my professional experience, running these tools regularly can help maintain system integrity and prevent unexpected errors.

# 4. How do I adjust CPU voltage safely?

Adjusting CPU voltage, also known as "undervolting" or "overvolting," can optimize performance or reduce power consumption. However, improper adjustments can lead to system instability or hardware damage. To adjust CPU voltage:

- 1. Access your computer's BIOS or UEFI firmware settings during startup.
- 2. Navigate to the CPU settings or overclocking section.
- 3. Make small incremental changes to the voltage settings, monitoring system stability after each change.
- 4. Use stress-testing software to ensure the system remains stable under load.

As an expert, I advise caution when adjusting CPU voltage. Always monitor system temperatures and stability, and consult your motherboard's manual for specific guidance.

#### 5. Why is it important to uninstall VPN clients properly?

Improper uninstallation of VPN clients can leave residual files or configurations that may interfere with network connectivity. To uninstall a VPN client:

- 1. Open the "Control Panel" and navigate to "Programs and Features."
- 2. Select the VPN client from the list and click "Uninstall."
- 3. Follow the on-screen prompts to complete the uninstallation.4. Afterward, check for any remaining files or settings and remove them manually if necessary.