Broadcast Software International

Frequently Asked Questions

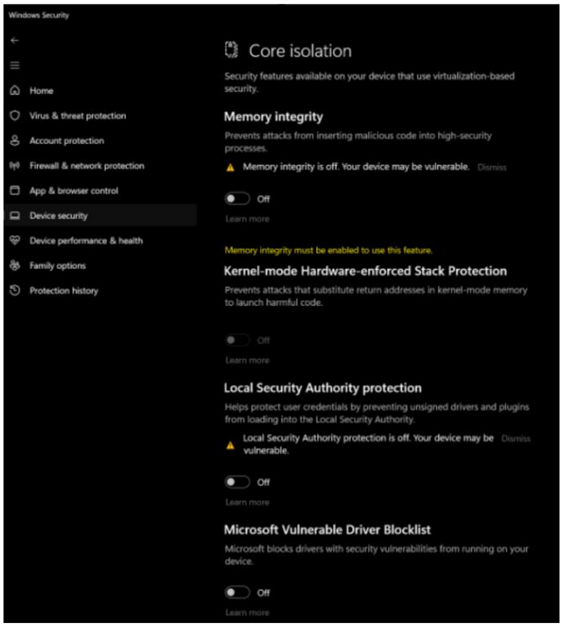
Suggested Windows 11 Pro Configuration for Broadcasting

Operating System:
DO NOT USE HOME VERSION
Windows 11 Pro (64-bit)

Disable All Core Isolation Features

Core Isolation features, including Memory Integrity and the Microsoft Vulnerable Driver Blocklist, protect against malware by isolating critical core processes of Windows from your other processes. Disabling them is critical to avoid audio and hardware key drivers from being falsely flagged.

1. **Open Windows Security:**
   - Click on the **Start Button** and type "Windows Security," then click on the app.
2. **Navigate to Device Security:**
   - In the Windows Security window, click on **Device security** from the left-hand menu.



Core isolation

Security features available on your device that use virtualization-based security.

Memory integrity

Prevents attacks from inserting malicious code into high-security processes.

⚠ Memory integrity is off. Your device may be vulnerable.

Off

Memory integrity must be enabled to use this feature.

Kernel-mode Hardware-enforced Stack Protection

Prevents attacks that substitute return addresses in kernel-mode memory to launch harmful code.

Off

Local Security Authority protection

Helps protect user credentials by preventing unsigned drivers and plugins from loading into the Local Security Authority.

⚠ Local Security Authority protection is off. Your device may be vulnerable.

Off

Microsoft Vulnerable Driver Blocklist

Microsoft blocks drivers with security vulnerabilities from running on your device.

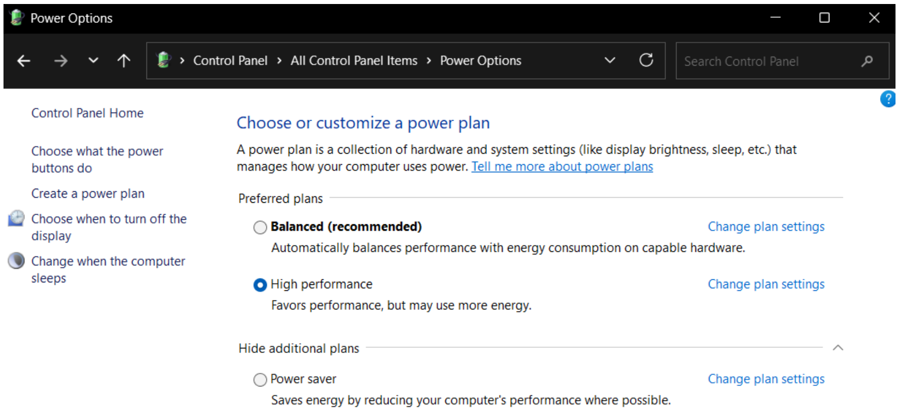
Off

3. **Access Core isolation details:**
   - Under "Core isolation," click on **Core isolation details**.
4. **Disable Memory integrity:**
   - Toggle the switch for **Memory integrity and all other Core Isolation features** to **Off**.
   - If prompted by User Account Control (UAC), click **Yes**.
5. **Restart your computer** for changes to take effect.

Adjust Power Option Plan to High Performance

The High Performance power plan prioritizes performance over power savings, which can be beneficial for demanding applications.

1. **Open Power Options:**
   - Click on the **Start Button** and type "Edit power plan," then select **Edit power plan**.
   - Alternatively, right-click on the **Start Button** and select **Power Options**, then click on **Additional power settings**.
2. **Show additional plans:**
   - In the Power Options window, click on **Show additional plans** to expand the options.
3. **Select High performance:**
   - Choose the **High performance** radio button.



Power Options
Control Panel › All Control Panel Items › Power Options
Search Control Panel
Control Panel Home
Choose what the power buttons do
Create a power plan
Choose when to turn off the display
Change when the computer sleeps

Choose or customize a power plan

A power plan is a collection of hardware and system settings (like display brightness, sleep, etc.) that manages how your computer uses power. Tell me more about power plans

Preferred plans

○ **Balanced (recommended)** Change plan settings

Automatically balances performance with energy consumption on capable hardware.

● High performance Change plan settings

Favors performance, but may use more energy.

Hide additional plans

○ Power saver Change plan settings

Saves energy by reducing your computer's performance where possible.

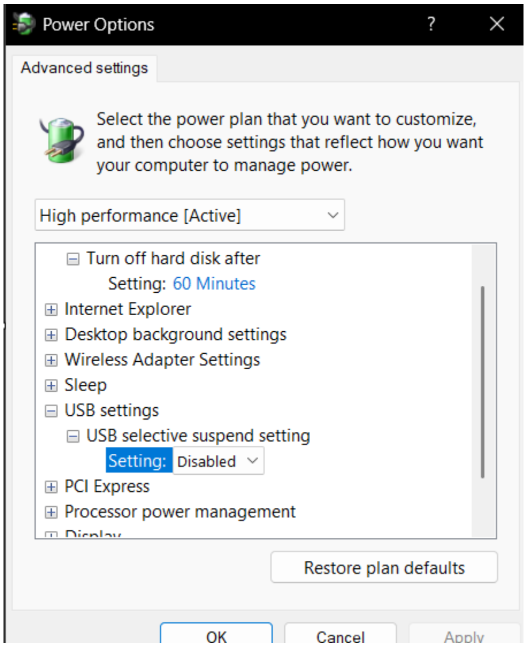
Disable USB Suspend Settings in Power Plan

Disabling USB selective suspend prevents USB devices from entering a low-power state, which can sometimes cause connectivity issues or delays.

1. **Edit Power Plan Settings:**

- Follow the steps in "2. Adjust Power Option Plan to High Performance" to get to the **Edit Plan Settings** window for your selected power plan (e.g., High Performance).

2. **Change advanced power settings:**
   - Click on **Change advanced power settings**.
3. **Disable USB selective suspend setting:**
   - In the Power Options dialog box, expand **USB settings**.
   - Expand **USB selective suspend setting**.
   - Click on the dropdown menu and select **Disabled**.
4. **Apply changes:**
   - Click **Apply**, then **OK**.



Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.

High performance [Active]

- Turn off hard disk after
  - Setting: 60 Minutes
- Internet Explorer
- Desktop background settings
- Wireless Adapter Settings
- Sleep
- USB settings
  - USB selective suspend setting
    - Setting: Disabled
- PCI Express
- Processor power management
- Display

Disable Sleep Button

Disabling the Sleep Button can help to eliminate the possibility of the PC accidentally being put into a sleep state.

1. **From Power Options**, select **Choose What Power Button Do**
   - In the menu, Click on the dropdown menu for **When I Press the Power Button**, and select **Do Nothing.**
2. **Click on the Save Changes** button and close the window.

Disable Core Automatic Update Features in Group Policy

Disabling automatic updates provides more control over when updates are installed. We do recommend that updates be run monthly as part of routine machine maintenance.

1. **Open Group Policy Editor:**
   - Click on the **Start Button** and type "gpedit.msc," then press **Enter**.
2. **Navigate to Windows Update settings:**
   - There are several folders that will need to be accessed for adjusting policies. In the Local Group Policy Editor, navigate to: Computer Configuration > Administrative Templates > Windows Components > Windows Update. The folders you need to focus on are Legacy Policies, Manage end-user experience, and Manage updates offered from Windows Server Update Service.
3. **Legacy Policies:**
   - Disable the “Allow Automatic Updates Immediate Installation” policy.
4. **Manage end-user experience:**
   - Disable the “Configure Automatic Updates” policy.

- Disable the “Allow updates to be downloaded automatically over metered connection” policy.
- Disable the “Always automatically restart at the scheduled time” policy.

5. **Manage updates offered from the Windows Server Update Service:**
   - Disable the “Automatic Updates detection frequency” policy.

Turning Off Notifications

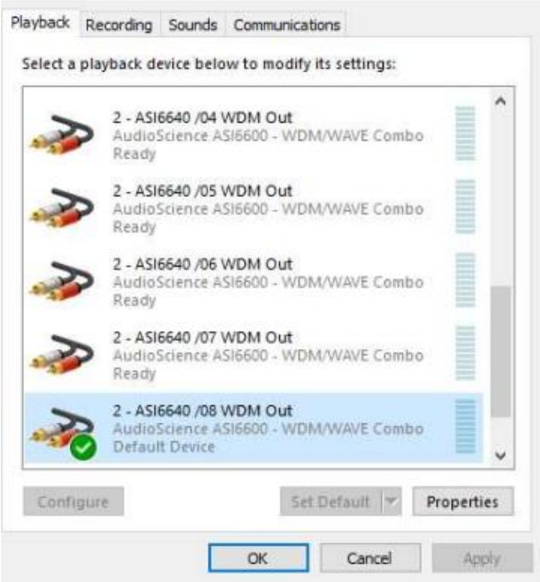
Turning off notifications reduces distractions and system resource usage.

1. **Open Settings:**
   - Click on the **Start Button** and select **Settings** (gear icon).
2. **Navigate to System > Notifications:**
   - In the Settings window, click on **System** from the left-hand menu, then select **Notifications**.
3. **Disable all notifications:**
   - Toggle the main **Notifications** switch to **Off**.
   - Alternatively, you can go through each app and disable notifications individually if you want to keep some.

Turn Off Windows Sounds

Disabling Windows sounds eliminates audio cues for system events.

1. **Open Sound Settings:**
   - Right-click on the **Speaker icon** in the system tray and select **Sound settings**.
2. **More sound settings:**
   - Scroll down and click on **More sound settings** under "Related settings."
3. **Disable sound scheme:**
   - In the Sound dialog box, click on the **Sounds** tab.
   - Under "Sound Scheme," select **No Sounds** from the dropdown menu.
   - Uncheck **Play Windows Startup sound**.
4. **Apply changes:**
   - Click **Apply**, then **OK**.



Select a playback device below to modify its settings:

2 - ASI6640 /04 WDM Out
AudioScience ASI6600 - WDM/WAVE Combo
Ready

2 - ASI6640 /05 WDM Out
AudioScience ASI6600 - WDM/WAVE Combo
Ready

2 - ASI6640 /06 WDM Out
AudioScience ASI6600 - WDM/WAVE Combo
Ready

2 - ASI6640 /07 WDM Out
AudioScience ASI6600 - WDM/WAVE Combo
Ready

2 - ASI6640 /08 WDM Out
AudioScience ASI6600 - WDM/WAVE Combo
Default Device

Turn Off Exclusive Mode on Sound Devices

Exclusive mode allows applications to take exclusive control of the audio device, potentially causing issues with other applications trying to use the same device.

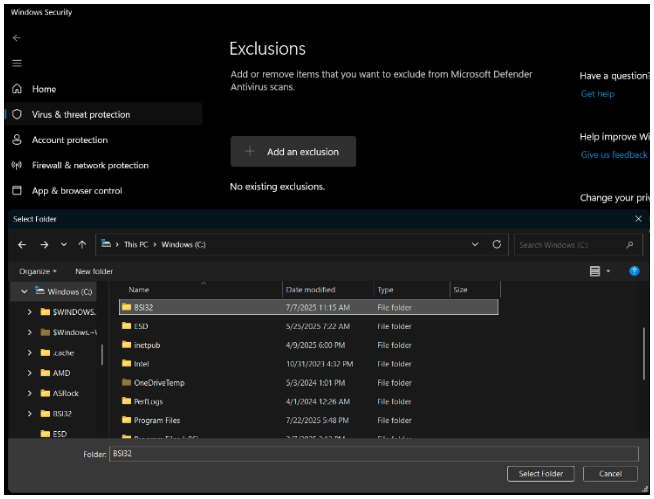
1. **Open Sound Settings:**
   - Right-click on the **Speaker icon** in the system tray and select **Sound settings**.

2. **More sound settings:**
    - Scroll down and click on **More sound settings** under "Related settings."
3. **Access Playback device properties:**
    - In the Sound dialog box, on the **Playback** tab, select your primary audio output device (e.g., Speakers, Headphones) and click **Properties**.
4. **Disable exclusive mode:**
    - In the device's Properties window, click on the **Advanced** tab.
    - Under "Exclusive Mode," uncheck both:
        - **Allow applications to take exclusive control of this device**
        - **Give exclusive mode applications priority**
5. **Apply changes:**
    - Click **Apply**, then **OK**.
6. **Repeat for Recording devices (optional):**
    - Go to the **Recording** tab in the Sound dialog box and repeat the process for your microphone or other recording devices if desired.

Recommended Sound Format for Sound Devices

1. We recommend selecting the following format for all playback and recording devices to be used by our software: 2 channel, 16-bit, 44100 Hz

---



Exclusions

Add or remove items that you want to exclude from Microsoft Defender Antivirus scans.

No existing exclusions.

Name	Date modified	Type	Size
BSI32	7/7/2025 11:15 AM	File folder	
ESD	5/25/2025 7:22 AM	File folder	
inetpub	4/9/2025 6:00 PM	File folder	
Intel	10/31/2023 4:32 PM	File folder	
OneDriveTemp	5/3/2024 1:01 PM	File folder	
PerfLogs	4/1/2024 12:26 AM	File folder	
Program Files	7/22/2025 5:48 PM	File folder	

Folder: BSI32

Create Antivirus Exclusions

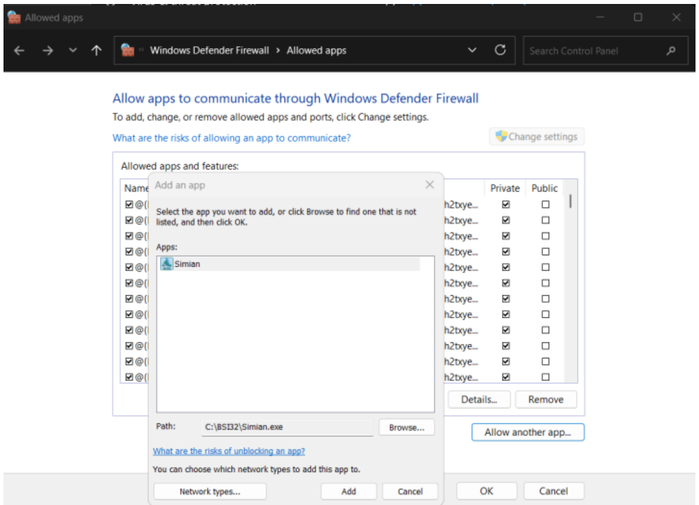
Creating antivirus exclusions can prevent performance issues caused by real-time scanning of specific files or folders, especially for applications with high I/O operations. This should only be done for trusted applications and paths.

1. **Open Windows Security:**
    - Click on the **Start Button** and type "Windows Security," then click on the app.
2. **Navigate to Virus & threat protection:**
    - In the Windows Security window, click on **Virus & threat protection**.
3. **Manage settings for Virus & threat protection settings:**
    - Under "Virus & threat protection settings," click on **Manage settings**.
4. **Add or remove exclusions:**
    - Scroll down to "Exclusions" and click on **Add or remove exclusions**.
5. **Add an exclusion:**
    - Click **+ Add an exclusion** and select the type of exclusion (File, Folder, File type, or Process).
    - **For Folders:** Browse to and select the BSI32 folder in the C:\ path.

Create Firewall Allowances for Applications

Creating firewall rules allows specific applications to communicate through the Windows Defender Firewall.

1. **Open Windows Defender Firewall with Advanced Security:**
   - Click on the **Start Button** and type "Allow an App through firewall" then press **Enter**.
2. **In the Allowed Apps Window:**
   - Click on the **Change settings** button and then on the **Allow another app** button.
   - Select the **Browse button** and navigate to **C:\BSI32 folder** and **select Simian**.
   - Once selected, click on the **Add** button. You will now see Simian listed among the allowed apps. You can then **check the box for both Private and Public networks**.
   - **Repeat** these steps for Info Editor, Sound Hound, Simian Weather Utility, and Simian File Sync.


Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

Add an app

Select the app you want to add, or click Browse to find one that is not listed, and then click OK.

Apps: Simian

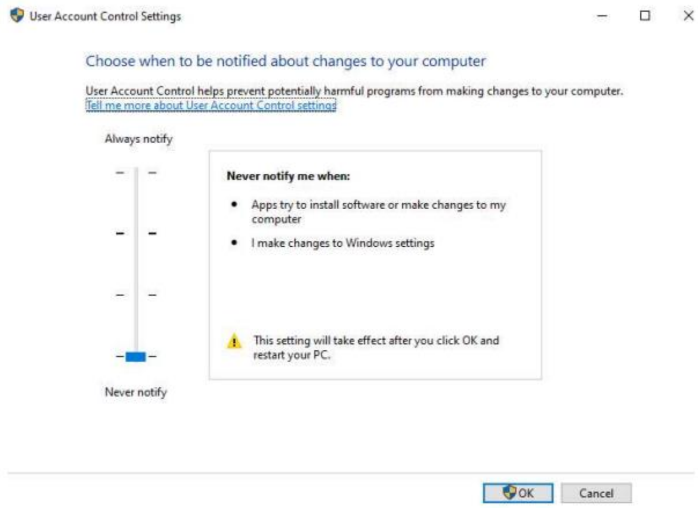
Path: C:\BSI32\Simian.exe

You can choose which network types to add this app to.

Allowed apps
Windows Defender Firewall › Allowed apps
Search Control Panel
What are the risks of allowing an app to communicate?
Change settings
Allowed apps and features:
Name
Private
Public
h2txye...
Browse...
What are the risks of unblocking an app?
Network types...
Add
Cancel
Details...
Remove
Allow another app...
OK
Cancel

Turn Off User Account Control (UAC)

Turning off UAC stops prompts for administrative privileges. This significantly reduces security and is generally **not recommended** for typical use, but can be done in highly controlled environments where security is managed by other means or for specific testing scenarios.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Tell me more about User Account Control settings

Never notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

This setting will take effect after you click OK and restart your PC.

1. **Open User Account Control Settings:**

o Click on the **Start Button** and type "Change User Account Control settings," then click on the result.

2. **Set UAC level:**

o Drag the slider all the way down to **Never notify**.

3. **Apply changes:**

o Click **OK**.

o If prompted by UAC, click **Yes**.

4. **Restart your computer** for the change to take full effect.

Network & Sharing

1. **From Settings, select Network & Internet and scroll down and select Advanced Network Settings.**
2. **Then select advanced sharing settings**.
   - Turn on network discovery and file and printer sharing for both Private and Public networks.
   - Under All Networks, make sure Turn off password protected sharing is selected under Password protected sharing.