Removing and Blocking Global Device Identifier (GDID) – A Guide for Better Privacy in Microsoft Windows 10/11

Written by saturniandragon@tumblr

Introduction

Peter Stokes (19), a hacker affiliated with Scattered Spider group was arrested on July 2nd 2026 in Finland and extradited to the US. He was caught despite having a secure connection with a VPN because Microsoft tipped the law enforcement using one information found on his device that is designed to ignore a VPN connection; **Global Device Identifier (GDID)**.

Global Device Identifier or GDID is a permanent, unique digital fingerprint that Microsoft automatically plants in your computer **when you use a Microsoft account to log in/sign** in to Windows. Like mentioned previously, GDID ignores VPN connection and can be read directly by Microsoft. **Microsoft assigns this identifier automatically to your computer without your information and without your consent**.

GDID is **attached to your Microsoft account**. It does not depend on hardware information. If you simply change computers or replace a hardware component but still uses the same MS account, GDID does not change. **This also happens in a virtual machine/VM**.

If you use Windows without using a Microsoft account/use an offline account, you are most likely safe. Your computer should not generate nor store GDID in its settings. If you happen to be one of those people, you can safely skip this guide. Otherwise, keep reading.

If you do use Windows with a Microsoft account, allow me to preface that it is too late. Your GDID has already been sent and recorded in MS servers within 10 seconds of you logging in to your computer for the first time.

This guide does not cover how to delete your GDID information from MS servers. Unless you want to visit MS directly and/or hack into their servers to delete your GDID information, in which case, I won't tell. This guide is about **severing the connection between your computer and MS servers so that GDID can no longer be correlated with your machine**, as well as safely deleting your own GDID from your computer.

Disclaimer

Yes, I hear you all loud and clear. **Just use Linux**. I will not and cannot stop you. In fact, I do encourage you to switch to Linux if you can, and ditch Windows entirely.

This guide is designed for people who **cannot transition to Linux** and must use a Windows operating system. Either they (1) don't have the capability, (2) don't have the means, (3) don't have the technical know-how, (4) don't have the authority, or (5) any of personal reasons that simply summarize into "must use Windows, cannot use Linux."

This guide is NOT SHORT either. This requires careful attention to what you're doing, as well as 30 – 60 minutes of your time. Microsoft will not let you block GDID that easily. But I've made sure I've written this guide as concise and descriptive as I can, without unnecessary details you won't need or care about. My advice? Relax, breathe, take your time, and do not rush through the steps.

Any questions or problems you might have, feel free to contact me on tumblr (@saturniandragon).

With all that said, let's get into it.

What you will lose or break by blocking and deleting GDID

Blocking and deleting GDID is not without consequences. It's tied to your Microsoft account, so Windows services related to Microsoft account may behave improperly or stop functioning. Especially because Windows services that handle GDID also handle a bunch of other stuff too.

Listed below are **features that you can expect to lose or break** by blocking and deleting GDID.

1. Phone Link, Nearby Sharing, some Bluetooth features
2. Potentially slower download speed for Windows Update
3. MS Store, OneDrive, Xbox, etc. (using web browser version of these services should still work)
4. Other MS account-related services (Office 365, Windows Insider, etc) (using web browser version of these services should still work)

If you're okay with those consequences (you most likely are), continue reading.

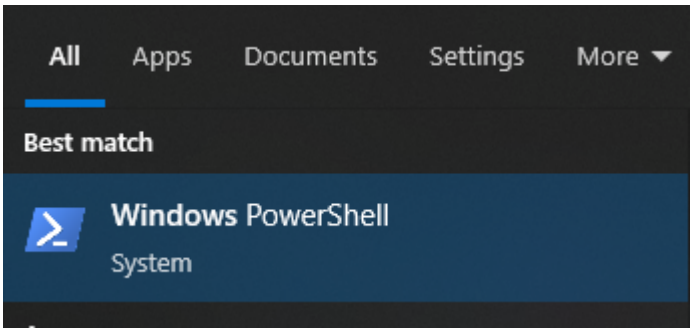
Where is GDID in my computer?

The truth is that **GDID is not hidden or encrypted** in your computer. You can easily read what your GDID is using Windows PowerShell. It is stored in the Registry Editor. **You can even delete it by yourself**. Nothing is stopping you from it, and your computer will continue to function normally without a GDID.

The catch is that when you delete your computer's GDID from the Registry, **Windows automatically requests a backup** from MS servers the moment your computer is connected to the internet. This process does not ask for your permission and does not visibly appear under normal usage. It all happens in the background and takes about 10 seconds to complete.

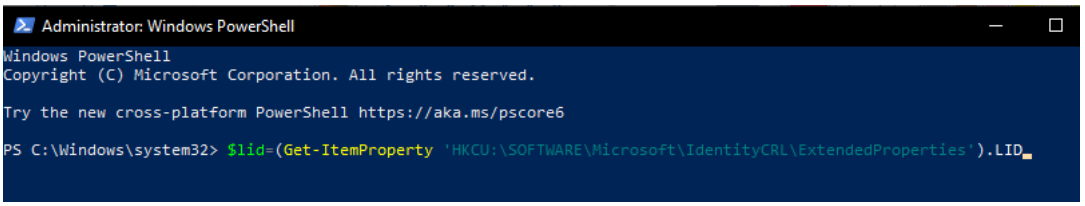
If you're curious about what your GDID reads as, follow these steps.

1. Press the Windows button on your keyboard.
2. Type "powershell" into the search bar. Right click on Windows PowerShell and press "**Run as Administrator**."



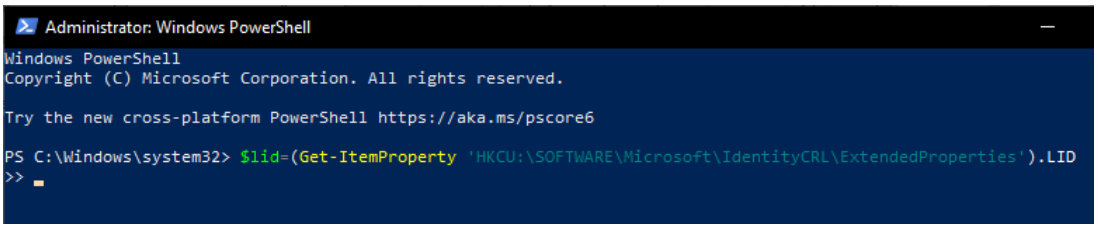
3. First, copy and paste the following command (Ctrl+C to copy and Ctrl+V to paste) into PowerShell but **do not press Enter yet.**

```
$lid=(Get-ItemProperty 'HKCU:\SOFTWARE\Microsoft\IdentityCRL\ExtendedProperties').LID
```



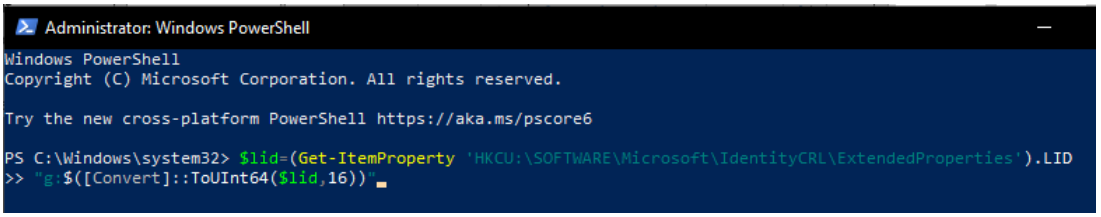
Tip: If you're having trouble reading the small text on the PowerShell terminal, hold Left Ctrl button on your keyboard and use your mouse scroll wheel to make the text bigger.

4. Next, **press Shift and Enter** at the same time (hold Shift and hit Enter) so the typing cursor moves to the next line. If you do it correctly, you should see two chevrons or "higher than" symbols appearing (like this ">>").



5. Next, copy and paste a second command into Windows Powershell. Both quotation marks included.

```
"g:$([Convert]::ToUInt64($lid,16))"
```



6. Now hit Enter and you should see your computer's GDID, beginning with "g:" and a string of 16 seemingly random numbers after it.

   I can't actually show you an example because I have deleted my own GDID. But if you have followed Step 1 to 6 correctly, you should be able to see your own GDID as a string of 16 numbers.

7. Close Windows Powershell for now. We will get back to it later.

Next we will begin **blocking Windows services responsible for handling GDID**, and deleting GDID from the computer afterwards. Read the instructions very carefully.

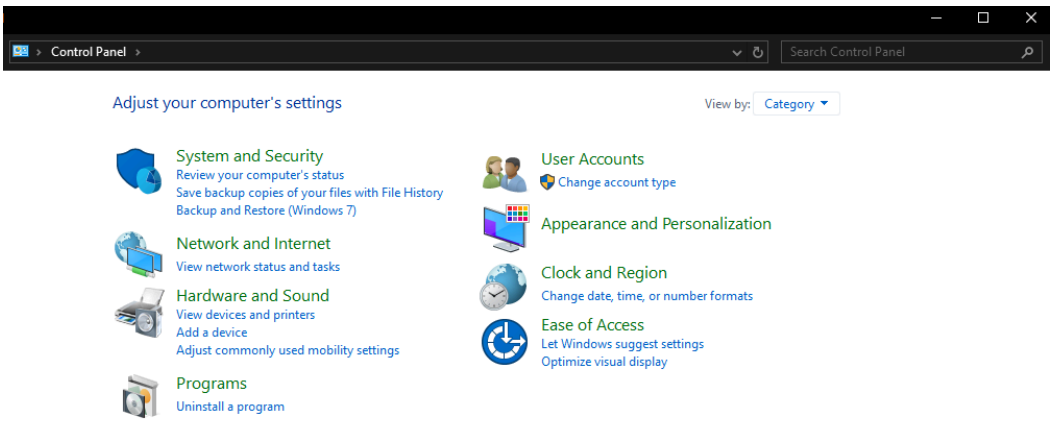
Preparations (optional, but HIGHLY recommended)

While these steps are merely optional and does not directly contribute to blocking and deleting GDID, doing these will tremendously help in our pursuit to block and delete GDID.

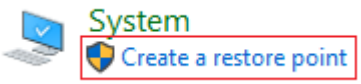
A. Create a system restore point

Restore point function as a "save file" for your computer. It saves numerous settings and information about your computer before doing some drastic changes to the registry, like what we're about to do.

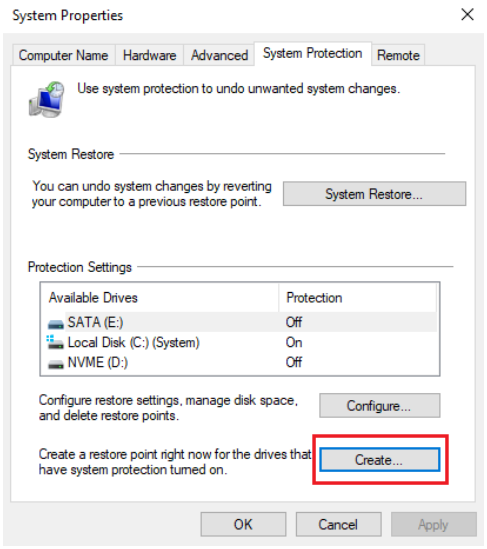
1. Press Windows button on your keyboard, type "control panel" and open it.



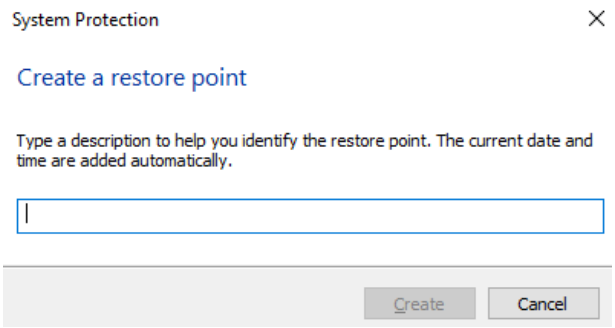
2. On the top right of control panel (under the minimize/maximize/close buttons) is the search bar. Type “restore point” into it.
3. Choose “Create a restore point” under “System”.



4. Click on the “Create” button.



5. Name your restore point with anything you wish, preferably something easily remembered or easily identifiable. Something like “pre-GDID removal” or variants thereof, but all up to you.



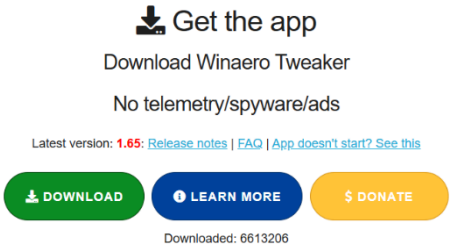
Click “Create” and let Windows do its thing. Should take several minutes.

6. Close restore point when you’re done.

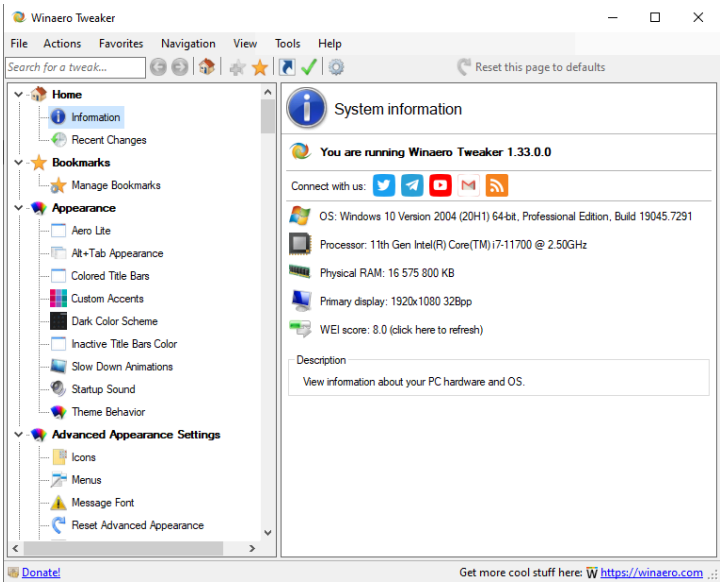
B. Download Winaero Tweaker (free)

Winaero Tweaker is a free software and utility that allows you to change various settings in Windows. Mostly, settings that are not available to the user unless they're willing to dive deep into the Registry. This software automates that.

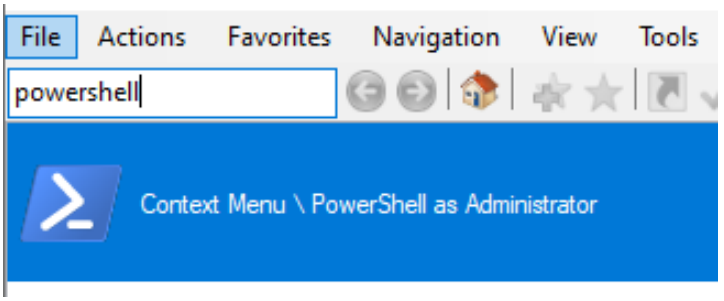
1. Download and install Winaero Tweaker (https://winaerotweaker.com/)



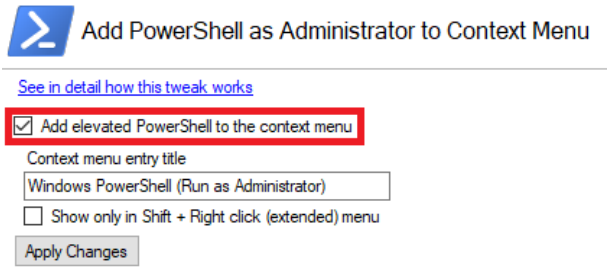
2. Open Winaero Tweaker once installed. You will be presented with this window.



3. There is a search bar on the top left, below File and Actions. Type "powershell" into it.

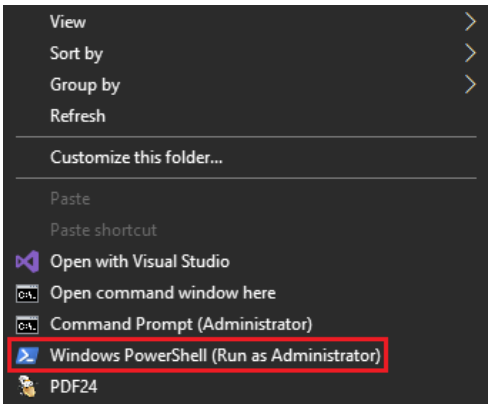


4. Double click on it. Tick the checkbox that says “Add elevated Powershell to the context menu”.



Context menu is a menu that opens when you use right click on your mouse.
Press “Apply Changes” and close Winaero Tweaker.

5. (Optional) You can test if the change works by opening file explorer, going into any folder in your computer, and press right click once.
The option to run Windows Powershell should be visible in the right click menu/context menu.

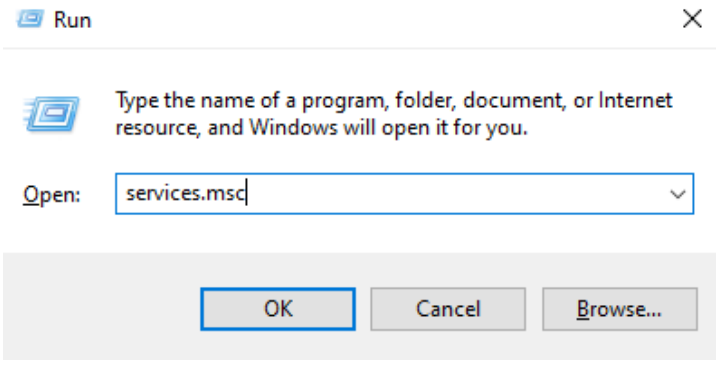


Make sure to right click on an empty area (i.e. Not right-clicking a file or a folder).
If you don’t see this option, try restarting your PC. Usually this change won’t require restart, but just in case.

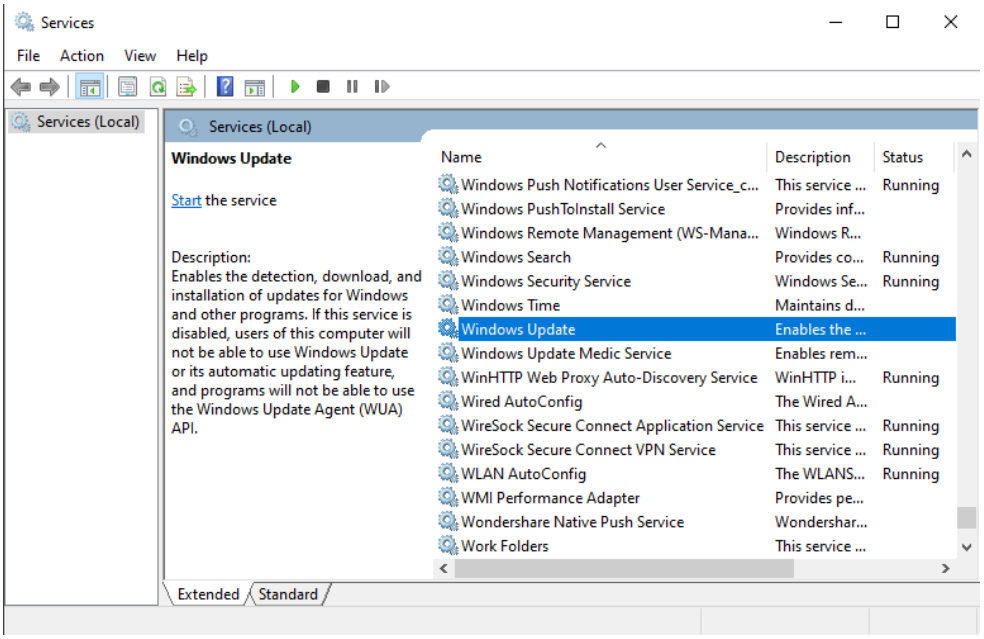
Step 1: Disabling Windows Update

This step is critical. If Windows Update is not disabled, any OS update could potentially undo everything we’re about to do.

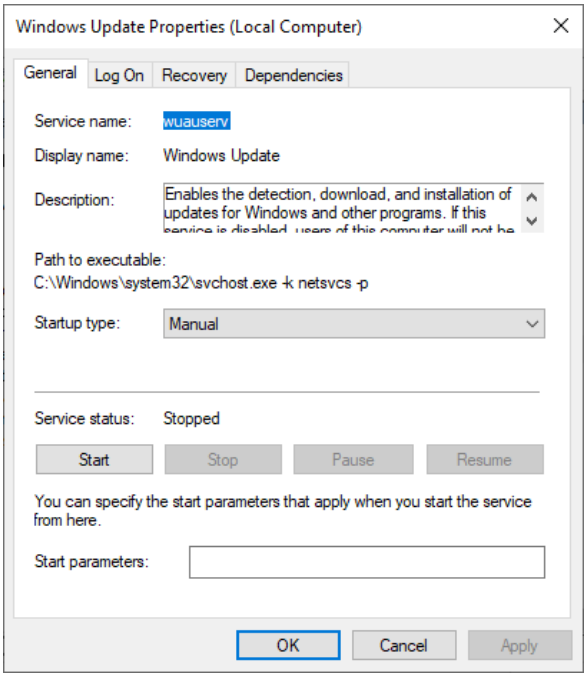
1. On your keyboard, press Windows button and R (Win+R) at the same time.
2. Type “services.msc” into it and hit Enter.



3. In the Services window, scroll down until you find an entry that says Windows Update.

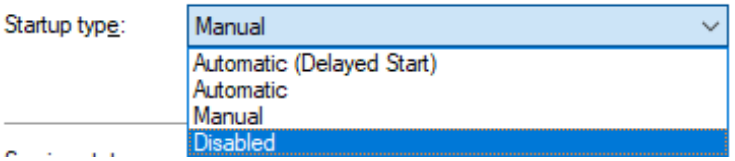


4. Double click on it, you will be presented with this window.

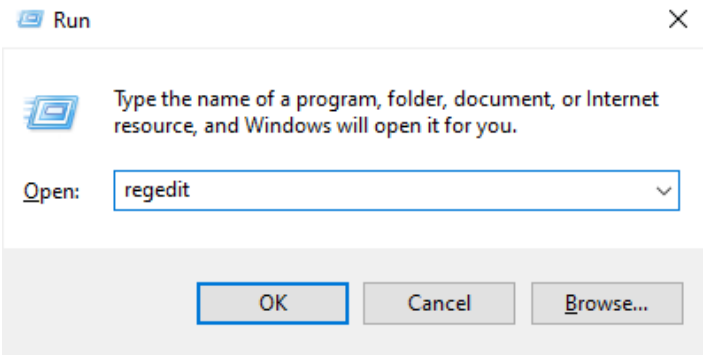


5. Check the field that says “Service status”. If it says “Running” next to it, hit the Stop button under it to stop the service. It will take a few seconds to stop the service.

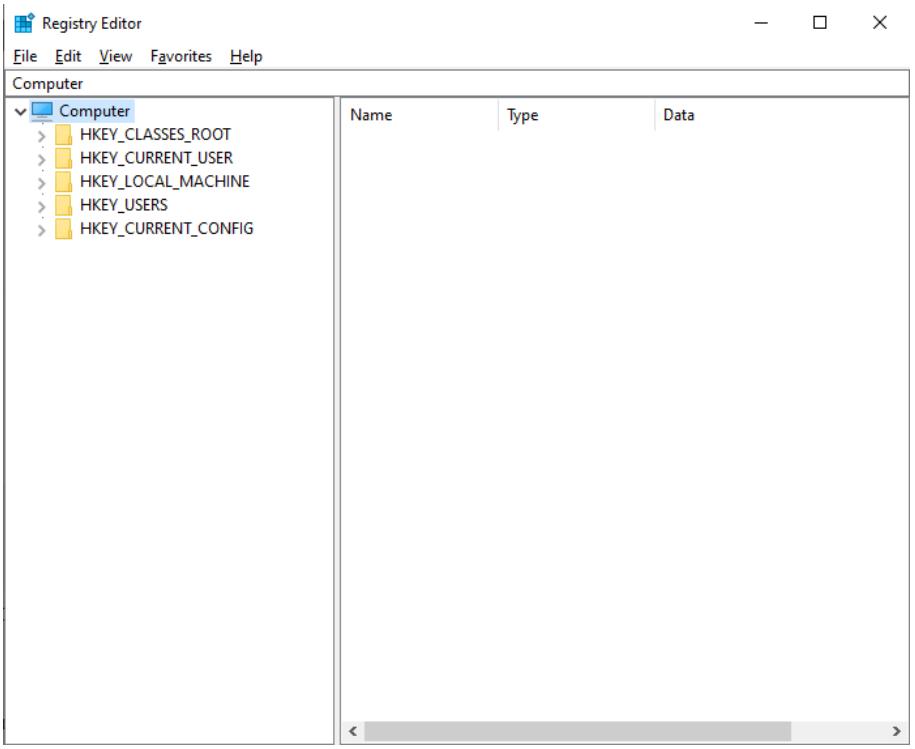
6. Next, change the Startup type, and set it to Disabled. No matter what it says previously.



7. Press Apply to save and OK to close it.
8. To REALLY make sure Windows Update service won't start again, open the Registry Editor by pressing Win+R. Type "regedit" and hit Enter.

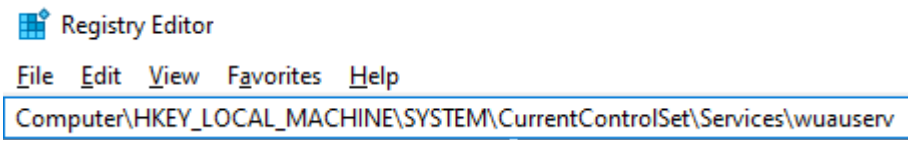


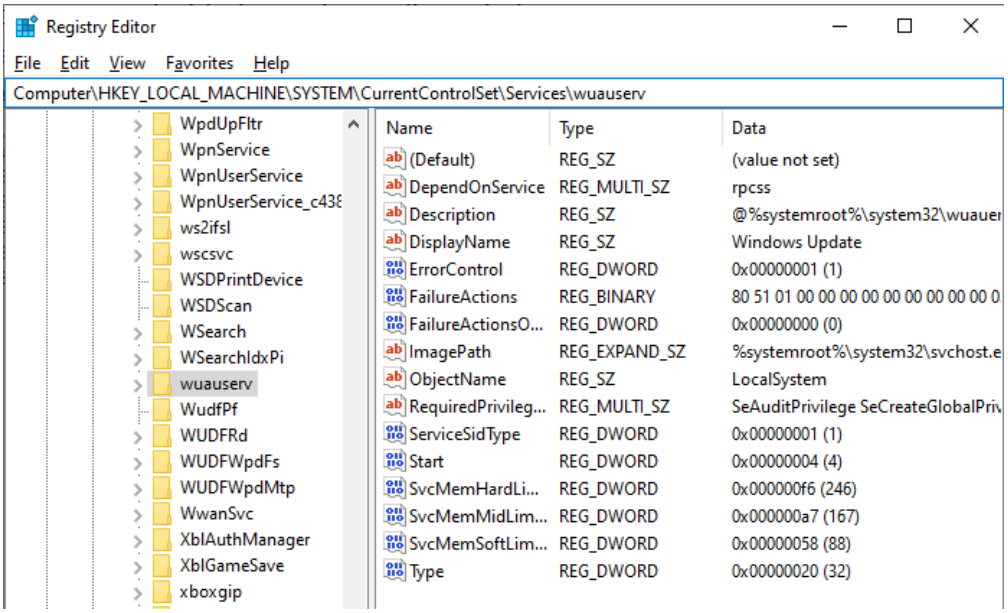
9. You will be presented with the Registry Editor window.



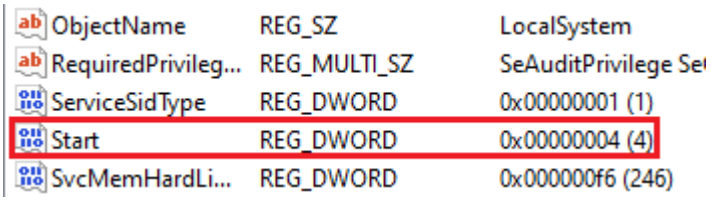
10. Copy the following address, and paste it to the address bar in the registry edit. It's located at the top of the window (below File and Edit). Hit Enter.

    `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv`

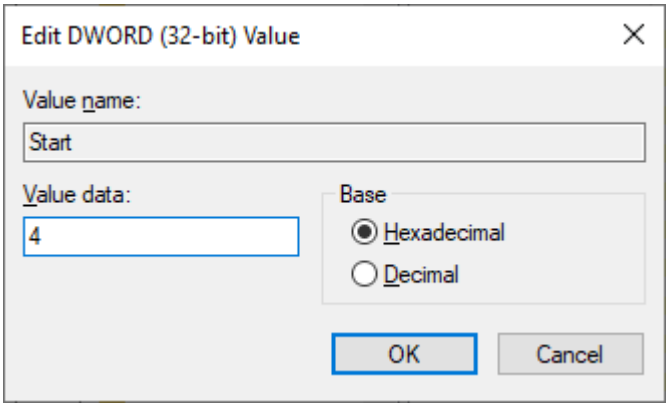




11. On the right side of the window, find an entry that says “Start”. Double click on it.



12. Make sure the box that says “Value data” says “4”, and it’s using Base “Hexadecimal.”



If it already says 4, you’re good to go.
If it doesn’t say 4, change the value to 4.

(1 = Automatic with delayed start, 2 = Automatic, 3 = Manual, 4 = Disabled)

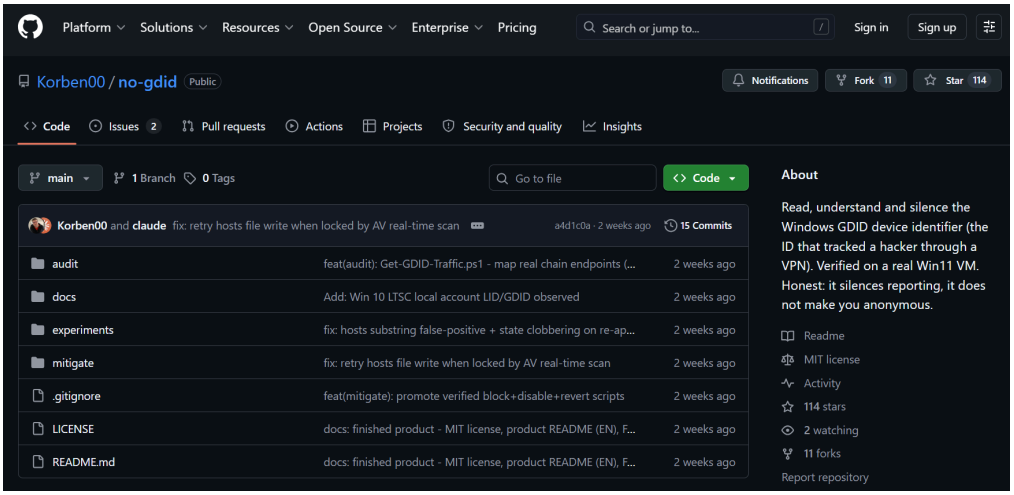
13. Press OK and close the Registry Editor.

Step 2: Blocking GDID host endpoints

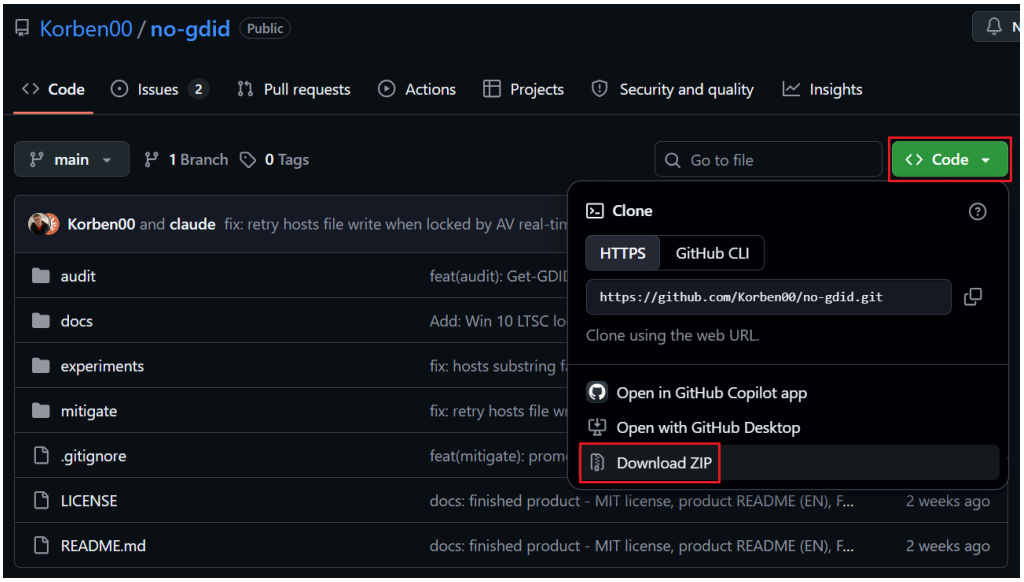
GDID host endpoints are internet addresses (essentially web URLs) that Windows uses to sync its GDID with the one stored in Microsoft servers. We need to sever this connection.

We need PowerShell scripts made by the kind folks at “no-gdid” project on Github. Many thanks to them for making this guide possible.

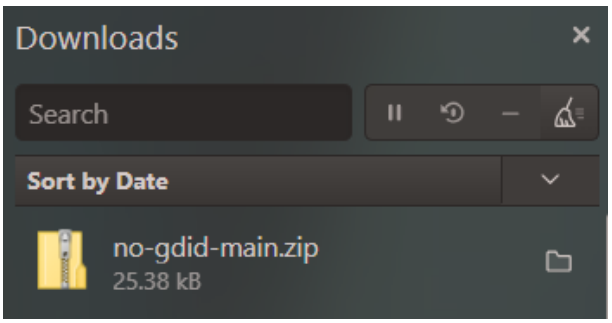
1. Visit the no-gdid project on Github at https://github.com/Korben00/no-gdid



2. Click on the green box that says “Code” and shoose “Download ZIP”.



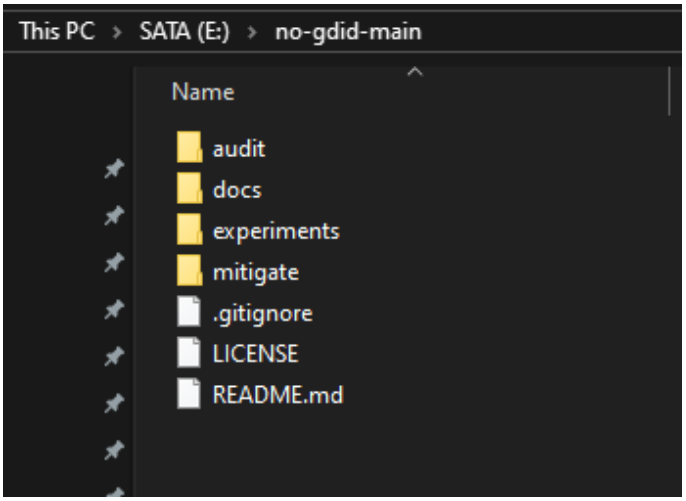
You will download a ZIP file named “no-gdid-main.zip”. It’s only 25 kilobytes.



3. Extract the contents of the ZIP file to a drive in your computer. I recommend your D: drive, E: drive, or in any hard drive you have in your computer.
   Just not the C: drive because that's where Windows installation is located. It may not cause issues if you extract the contents there, but I recommend somewhere else, if you have the option to do so.

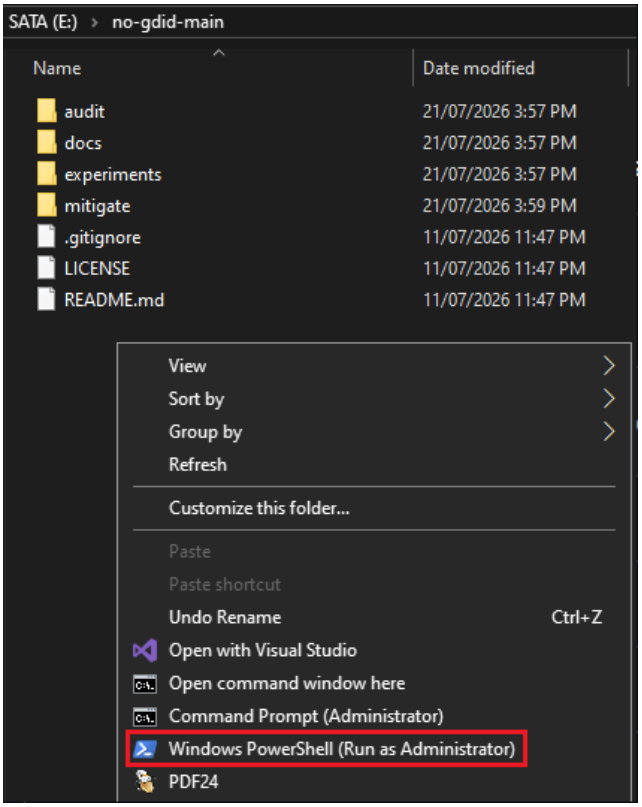
   In my case I will use my E: drive.

   Enter the "no-gdid-main" folder until you see something like this.

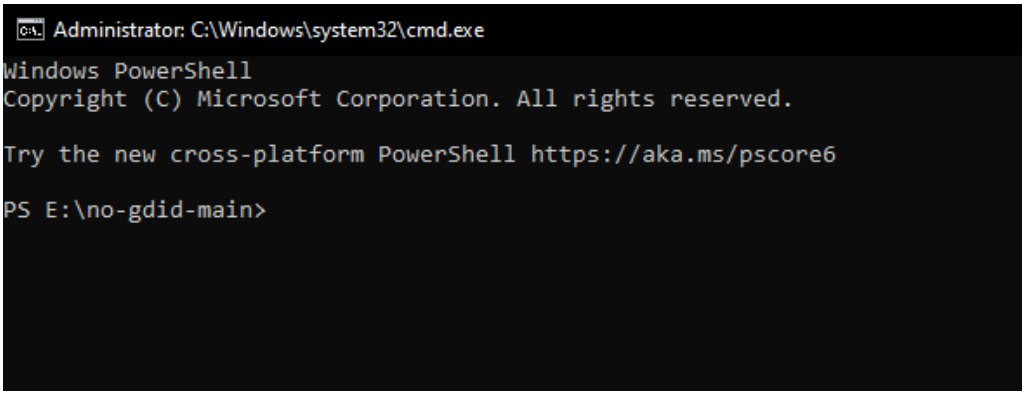


4. Next, if you've already done the optional step previously (enabling Windows PowerShell in context menu), press right click on an empty area inside the folder.
   Make sure not to right click on a file or folder name.

   Choose Windows PowerShell as administrator.



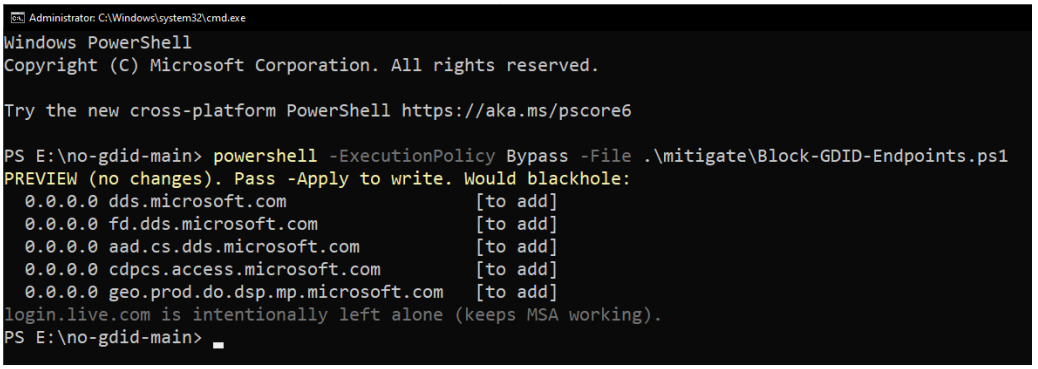
5. A command prompt window will appear.



Tip: If you're having trouble reading the small text on the command prompt, hold Left Ctrl button on your keyboard and use your mouse scroll wheel to make the text bigger.

6. Copy the following command into the command prompt window and hit Enter.

```
powershell -ExecutionPolicy Bypass -File .\mitigate\Block-GDID-Endpoints.ps1
```



This command alone won't block the GDID host endpoints. This shows you a preview of the endpoints/URLs that will be blocked if you proceed.

7. To start the process of blocking the endpoints, enter the same command again but add " -Apply" at the end.

```
powershell -ExecutionPolicy Bypass -File .\mitigate\Block-GDID-Endpoints.ps1 -Apply
```

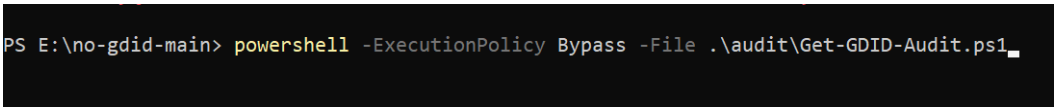
Tip: You can use Up arrow (↑) on your keyboard to bring back the previous command. And then you simply type " -Apply" at the end. Don't forget the space before the hyphen.

Hit Enter to start the process. It will take a moment.

I can't actually show you an example because I have successfully blocked GDID endpoints in my computer, so entering this command again in my computer returns nothing. But it will let you know when it has successfully done so.

8. Let's check and make sure the endpoints have been successfully blocked. To do that, copy the following command and paste it into the command prompt. Then, press Enter.

```
powershell -ExecutionPolicy Bypass -File .\audit\Get-GDID-Audit.ps1
```



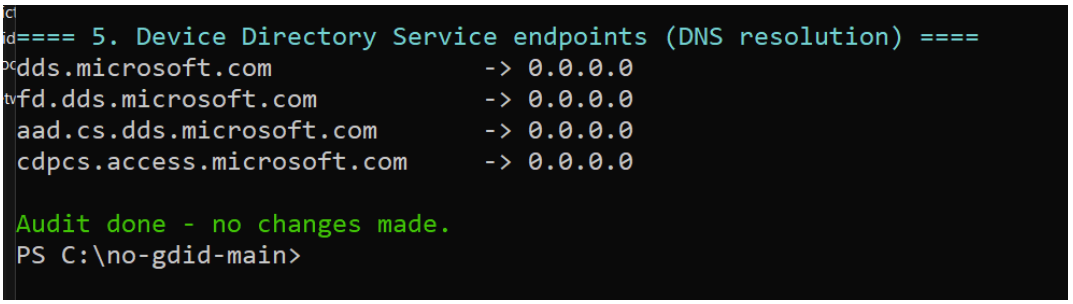
9. If the endpoint names are colored green, that means that endpoint has been successfully blocked.

   If all or some of the endpoint names are colored red, that means that endpoint wasn't successfully blocked. Go back and try again.

   If you have confirmed that all endpoints are colored green (i.e. have been successfully blocked), keep the PowerShell window open to do the next step.

10. (*Added on the 8th of August 2026. Not present in the PDF version of this guide*)

    Certain Windows versions or editions may instead show GDID host endpoints being redirected to 0.0.0.0 address, instead of being colored green or red.



    From a user report, **this appears to be fine**. 0.0.0.0 simply means the respective address can't be recognized or connected to. You can safely continue with the next steps.

Step 3: Blocking Windows services related to GDID

Three Windows services are responsible for handling GDID. These can be viewed in Services (Win + R, services.msc). These services are as follows:

- Connected Device Platform Service (CDPSvc)
- Connected Device Platform User Service_xxxxxx (CDPUserSvc_xxxxxx)*
- Device Optimization (DOsvc)

  * = "xxxxxx" will be different for every computer. Usually a string of numbers and letters such as "1a2b3c".

To disable these services, follow these steps.

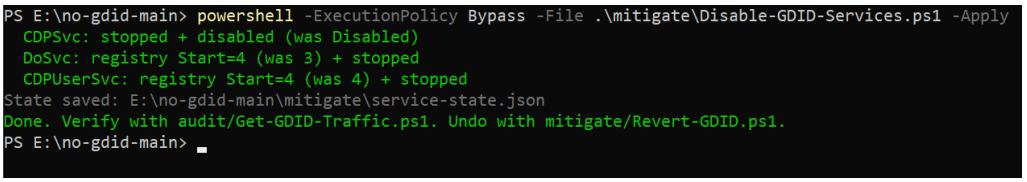
1. Return to the PowerShell window from earlier.
   If you've accidentally closed yours, don't worry. Simply reopen it again with the same steps as before.

2. Copy and paste the following command into PowerShell and hit Enter.

```
powershell -ExecutionPolicy Bypass -File .\mitigate\Disable-GDID-Services.ps1 -Apply
```

   This command will *attempt* to disable all three Windows services mentioned above.

   In my testing however, it failed to disable one (DOsvc). So unlike the previous command that blocks the GDID endpoints, this command that disables GDID services happens to be less reliable, at least on my machine. Your result might vary.
   If all three has been disabled successfully, it should look like this.



   Notice how all three services (CDPSvc, DOsvc and CDPUserSvc) are colored green. That means they have been successfully disabled.

   Keep PowerShell open for now, we will use it to verify in the next step.

3. If you're experiencing my case where one (or multiple) service was not successfully disabled, we need to use Services (`services.msc`) and Registry Edit (`regedit`) to force stop and disable those services.
   Below are the names of the three services, their names in `services.msc` and their address in `regedit`.

Service	**Name in `services.msc`**	**Address in `regedit`**
Connected Device Platform Service (CDPSvc)	Connected Device Platform Service	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDPUserSvc
Connected Device Platform User Service_xxxxxx (CDPUserSvc_xxxxxx)*	Connected Device Platform User Service_xxxxxx*	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDPUserSvc_xxxxxx*
Device Optimization (DOsvc)	Device Optimization	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DoSvc

   * = "xxxxxx" will be different for every computer. Usually a string of numbers and letters such as "1a2b3c".

Scroll back up to page 6 if you need to learn how to open `services.msc` and `regedit` again.

1. Disabling them in `services.msc` can be done the same way as disabling Windows Update. Find the name of the service (listed on the table above), and double click on it.

   If it says "Running", hit the Stop button. And then, change the Startup type to Disabled.

2. Disabling them in `regedit` can be done the same way as disabling Windows Update. Go to the address of the services (listed on the table above). Then find an entry named "Start", double click on it, and make sure the value is "4" and not any other value.

   All of those services will have an entry named "Start" in their registry addresses.

Step 3.1: Blocking additional services related to GDID

Two additional Windows services are related to GDID. They are safe to disable.

Name	**Name in `services.msc`**	**Address in `regedit`**
Connected User Experience and Telemetry (DiagTrack)	Connected User Experience and Telemetry	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DiagTrack
Windows Live ID Sign-in Assistant (wlidsvc)	Windows Live ID Sign-in Assistant ***or*** Microsoft Account Sign-in Assistant*	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wlidsvc

* = may be named one or the other in different Windows versions. Check for both.

Step 4: Verifying that GDID-related services and endpoints have been disabled

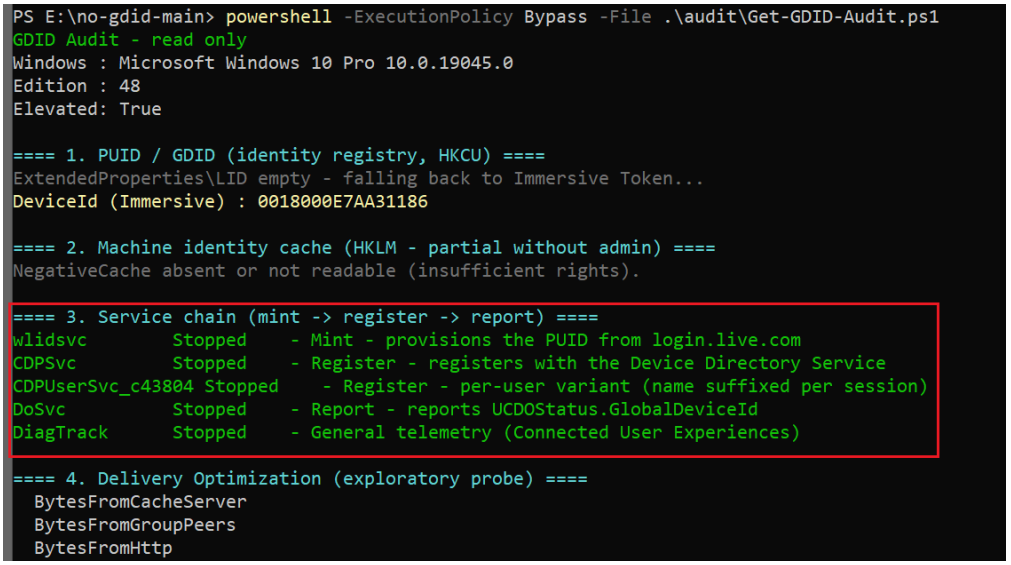
To verify that GDID-related services and endpoints have been disabled, follow these steps.

1. Return to the PowerShell window from earlier.
   If you've accidentally closed yours, don't worry. Simply reopen it again with the same steps as before.

2. Copy and paste the following command into PowerShell, and hit Enter.

   ```
   powershell -ExecutionPolicy Bypass -File .\audit\Get-GDID-Audit.ps1
   ```

3. Scroll up until you find a block of text named "3. Service Chain"

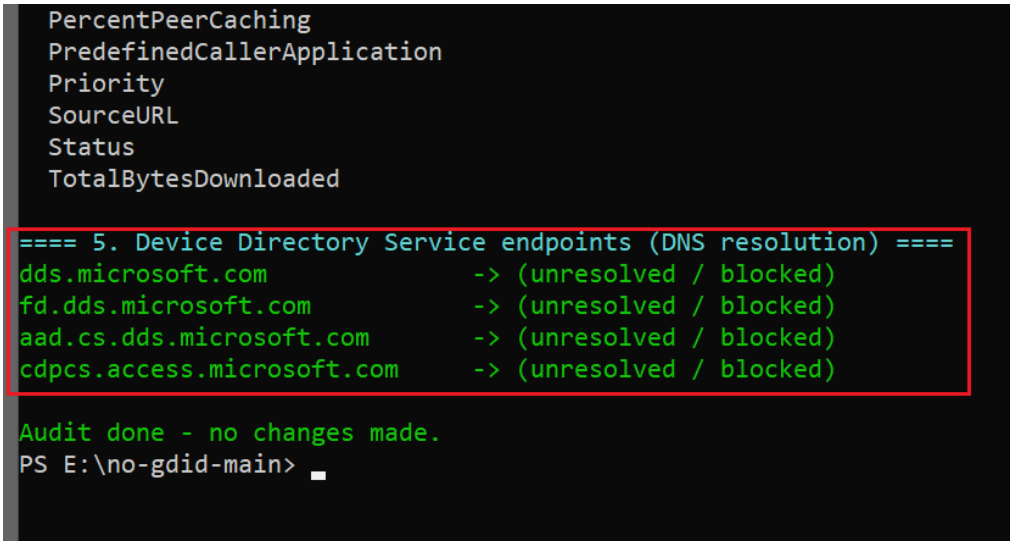


The service chain contains the names of 5 Windows services related to GDID.

If any of them are colored red, it means that service has not been disabled successfully. Go back to *Step 3* (page 13) and *Step 3.1* (page 15) to try again.

If all of them are colored green, you are good to go.

4. Scroll down until you find a block of text named “5. Device Directory Service endpoints.”



These are the endpoints that Windows use to handle GDID.

If any of them are colored red, it means that endpoint was not blocked successfully. Go back to *Step 2* (page 9) to try again.

If all of them are colored green (reads as unresolved/blocked on the right), you are good to go. Proceed to the next step.

Step 5: Deleting GDID from your computer

We are now ready to delete GDID from Windows installation for good. If all previous steps have been done correctly, Windows will not request a GDID backup from Microsoft servers and restore GDID after deletion.

GDID is stored in the Registry Editor. Follow these steps.

1. Open the Registry Editor with Win+R and regedit.
2. Navigate to the following address.

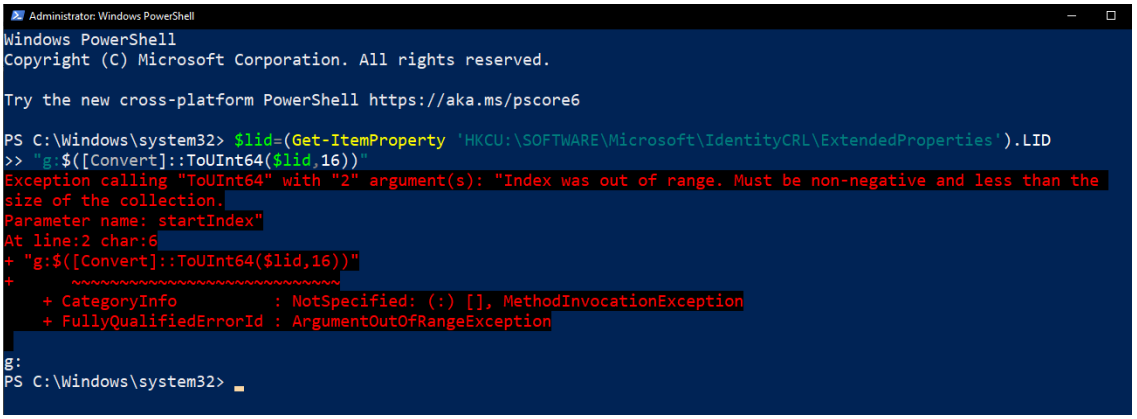
   Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\ExtendedProperties

3. Find an entry named “LID”. This is your GDID.
4. Right click on the entry named “LID” and press “Delete”.

Step 6: Verifying GDID is not being restored

Verifying that GDID is not being restored can be done easily. Go back to page 2, under the “Where is GDID in my computer?” section. Follow the same steps again to attempt viewing your GDID.

Instead of displaying your GDID, PowerShell will return an error code in red text, indicating that the GDID no longer exists in the registry.



Wait another minute, and enter the same command again. Wait another 5 minutes, and enter the same command again.

If it returns the same error code each time, you have **successfully deleted GDID from your computer AND prevented Windows from restoring GDID from Microsoft servers**.

If you’ve made it this far, give yourself a pat on the back for a job well done.

Author note: Issue(s) I had after doing all of these

This section doesn’t contain any step. This is just my own observation/research notes.

When I first completed all these steps, I restarted my machine to verify that GDID was no longer being restored to the registry. Which is indeed the case. It’s been 5 days and I haven’t seen GDID again in the PowerShell terminal or in the registry.

I did, however, experience a weird case of my graphics drivers breaking immediately after the first restart. My RTX 3070 was suddenly not detected, forcing Windows to fall back to Microsoft Basic Renderer Driver.

Eventually I did fix this step by just reinstalling the relevant RTX 3070 drivers obtained from Nvidia. This may or may not happen to you, but it was weird.

My theory is that the graphics drivers are also somehow connected to my MS account in some way via Windows. And doing all these steps to sever GDID connection also severs the link between my graphics driver and Windows' internal working, causing the GPU driver failure.

But that's my theory. A game theory, if you will. I don't know exactly how or why it happened. But in case you experience the same thing after doing all these steps, just know that I had it too. And it was fixed by reinstalling graphics drivers again.

Finally, this guide is not perfect. I've tried my best to make this guide as descriptive and concise as possible, so it can be digested and comprehended by as many people as possible. Despite all of that, the truth is that all computers are built different. You may encounter issues that I didn't. No two computers are the same.

Regardless, if you have questions, feel free to contact me on tumblr (@saturniandragon).

Security/virus/malware concerns: Windows Defender

(Added on 29th of July 2026. Not present in the PDF version of this guide.)

Some people have reached out and expressed concern that disabling Windows Update will prevent security updates. But there is a fix for this. Windows Defender can be updated separately without needing Windows Update.

1. Visit Microsoft Security Intelligence website at https://www.microsoft.com/en-us/wdsi/defenderupdates
2. Scroll down to the download links.


You need to download different security intelligence files for different products and platforms. Select the version that matches your Windows operating system or the environment where you will apply the update.

Note: Starting on Monday October 21, 2019, the Security intelligence update packages will be SHA2 signed.
Please make sure you have the necessary update installed to support SHA2 signing, see 2019 SHA-2 Code Signing Support requirement for Windows and WSUS.

Antimalware solution	Definition version
Microsoft Defender Antivirus for Windows 11, Windows 10, Windows 8.1, and Windows Server	32-bit | 64-bit | ARM
Microsoft Security Essentials	32-bit | 64-bit

3. Download the appropriate version for your computer. Most modern computers are 64-bit. You will download a file named `mpam-fe.exe`. It's around 210 MB.
4. Run the file to update Windows Defender.
5. Do this periodically (e.g. once every few months) to get the latest updates for Windows Defender.

References

Burnel, F. *Windows GDID: Impossible to Delete, But You Can Block It.* Via IT-Connect.Tech. (https://www.it-connect.tech/windows-gdid-impossible-to-delete-but-you-can-block-it/). Accessed July 23rd 2026.

Korben, Claude and Berbe. *"no-gdid" Github project*. Via Github. (https://github.com/Korben00/no-gdid). Accessed July 23rd 2026.

Various users. *Blocking GDID with freeware*. Via The Portable Freeware Collection. (https://www.portablefreeware.com/forums/viewtopic.php?p=110953). Accessed July 23rd 2026.

Microsoft. Microsoft Security Intelligence. Via Microsoft. (https://www.microsoft.com/en-us/wdsi/defenderupdates). Accessed July 29th 2026.