What is a HWID

Every component in your computer has it's so called "**Hardware ID**", also referred to as "**HWID**". Every operating system needs to know your component's HWID to register it and talk to it correctly. You can think of it as a digital fingerprint for your operating system to distinguish it from other components in your PC. Note that the term "HWID" only applies to the Windows operating system, but other operating systems have different terms for this device fingerprint.

There are two types of "HWIDs" on Windows:

- System HWID
- Device HWID

System HWID

A **System HWID** is an identifier that identifies your operating system and it's composed of multiple devices, like from your motherboard's firmware, MAC addresses, disk serials etc. It doesn't change with each installation of Windows unless you swap your motherboard.

Example: `12345678-1234-1234-1234-1234567890AB`

Device HWID

However the **Device HWID** is different for each physical component in your computer. For example, your CPU and GPU will have different UUIDs.

Example: `PCI\VEN_10DE&DEV_1C82&SUBSYS_1C821043&REV_A1`

What are FiveM Identifiers

FiveM Identifiers are generally just the IDs related to your linked accounts. For example, the **discord** identifier is just `discord:<your discord account id>`. FiveM supports these identifiers:

- **CFX** (`fivem:`) - Your CFX.re account you linked in settings (*optional*)
- **Rockstar** (`license:`) - Your Rockstar account hash, every player needs this identifier to play FiveM
- **Steam** (`steam:`) - Your Steam account that's fetched if Steam is running on your PC along with FiveM
- **Xbox Live** (`xbl:`) - Your Xbox account that's fetched if Xbox Gaming Services are installed
- **Microsoft** (`live:`) - Your Microsoft account PUID (if you have Windows Local Account you don't have this identifier)
- **IP Address** (`ip:`) - Your IPv4 address

> Note: There's also a `license2:` identifier: "This identifier is the ROS license for people who use Steam, this identifier can be the same value as `license` "

Read more here

How do AntiCheats remember they banned you?

Before an AntiCheat completely bans you and disconnects your from a server, it first fetches your account data on the server side. That includes your FiveM identifiers but also your HWID. You can grab partial HWID "tokens" in FiveM through the `GetPlayerToken()` native. This native does the following:

> "Gets a player's token. Tokens can be used to enhance banning logic, however are specific to a server."

That means your HWID tokens will be different on each server, this is because the tokens are just unique identifiers composed from your actual HWIDs but are hashed using a specific value that's different for each server.

Why are the tokens different on each server? It might be so creators can't create a "global ban system" shared across multiple servers, but I don't really know.

Then the AntiCheat saves your identifiers, most of the time they use a database or a plain JSON file with all player bans, for example the JSON file could look like this:

```
[
    "bannedPlayer1": {
        playerName: "player123",
        license: "license:123",
        discord: "discord:123",
        ipAddress: "127.0.0.1"
        banReason: "cheating",
        hwid: [
            1: "hwid123",
            2: "hwid345",
            3: "hwid0000"
        ]
        // and so on...
    }
]
```

After that it finally disconnects you from the server and prevents you from connecting again. But when you try to connect again, how does it know that you've been banned before?

Simple, when you try to join a server, you first fire a `playerConnecting` event to the server. Resources on the server can listen for this event. This event includes some arguments, and with these arguments the resources can obtain your player data again - so identifiers and HWID tokens. After that the server just looks in the database and compares your current identifiers and HWID tokens with the ones saved in the database.

If you want to know more about this event, read here

So how does the actual spoofing process work??

Now that we know the basics of HWIDs, FiveM identifiers and how AntiCheats work, we can use this knowledge to bypass the AntiCheat's system that prevents banned players from joining again. See, device HWIDs are just some data that your computer reads from somewhere - that means that if we

figure out where the OS reads those values from, we can tamper with these values and make the OS think our HWIDs have changed. And since the OS thinks we have a different HWIDs, every application that requests these HWIDs values from the OS will receive the changed values.

So the spoofer doesn't do anything else than just tampering with your HWID values. This tricks your OS into thinking you have a different hardware components.

So basically:

- You have a GPU with the following HWID: `gpu:123456`
- An AntiCheat banned you and saved this HWID - you cannot connect to that server anymore with the same GPU
- But you have a spoofer, so you spoof your HWID and now your GPU has the following HWID: `gpu:567890`
- The AntiCheat compares the HWID you had when you got banned, and the HWID you have now
- The HWIDs doesn't match, so it thinks you're a completely different player and let's you in!

And that's all! It's this simple.

> Please note that the actual spoofing process is way more complicated, as you have to also acquire completely new Rockstar accounts, uninstall Xbox Gaming Services, optionally get a new Discord account and so on. Current AntiCheat systems are way more strict when it comes to saving banned player data so it requires more effort to actually evade the ban.

> Also note that the HWID spoof is not permanent and your new HWID will only last until the next system restart

Sources

- https://www.unknowncheats.me/forum/alternative-online-mods/687133-getplayertoken-track.html
- https://docs.fivem.net/docs/scripting-reference/events/list/playerConnecting/
- https://docs.fivem.net/natives/?_0x54C06897
- https://docs.fivem.net/docs/scripting-reference/runtimes/lua/functions/GetPlayerIdentifiers/
- https://learn.microsoft.com/en-us/windows-hardware/drivers/install/hardware-ids