

How to build a local DNS to prevent tracking from ISPs

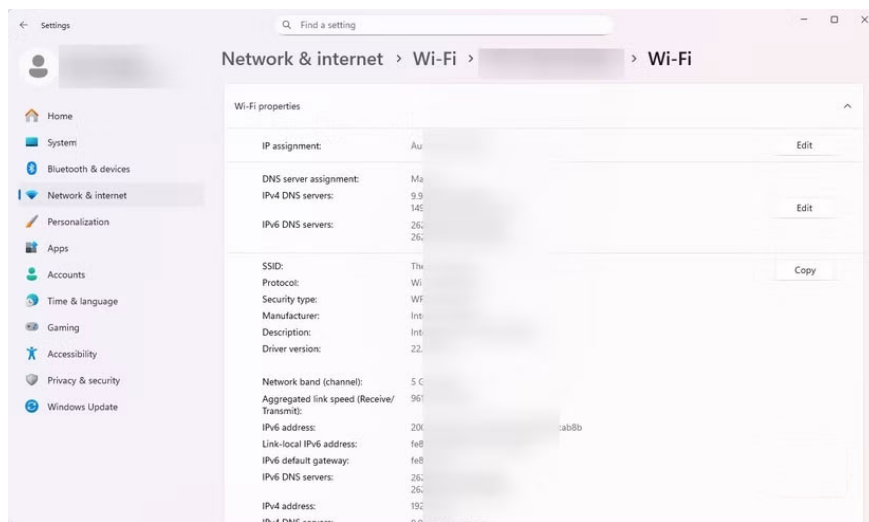
Nowadays, most people think that using a good VPN service is the only way to protect their privacy online. However, there is another solution: local DNS.

Your Internet Service Provider (ISP) is the first point of connection between you and the Internet . Every time you connect, you pass information to your ISP, including your domain name, IP address , connection timestamp, and any unencrypted HTTP traffic. While this is mostly fine, you may want a little more security and privacy for your online activities.

Nowadays, most people think that using a good VPN service is the only way to protect their privacy online. However, there is another solution: local DNS.

Control DNS with local configuration

A new layer of flexible control



DNS is one of those services that most people outsource by default. Most people either use their ISP's default DNS settings or turn to a third-party DNS provider like Google or Cloudflare. The only problem is that these third parties can see your requests.

However, one of the most effective ways to change this is to run DNS locally. This way, a small DNS service running on your computer becomes your trusted resolver.

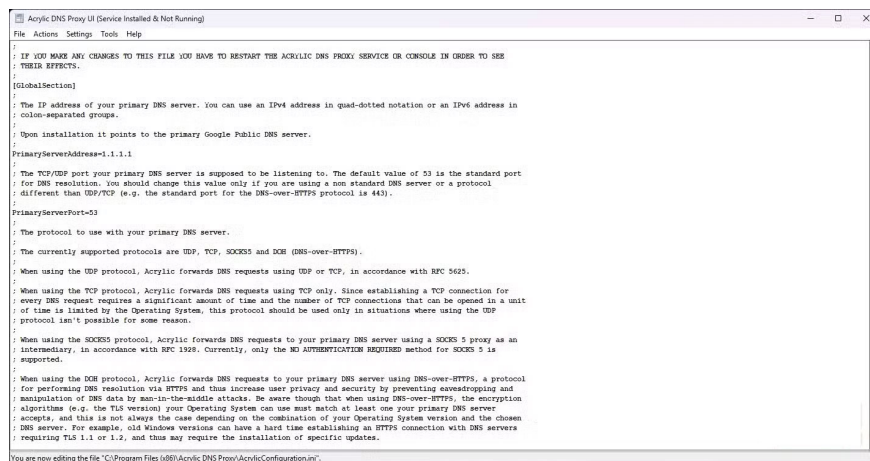
Note : The resolver receives requests for a website and finds the appropriate IP address. This process is usually handled by your ISP's resolver, but if you're setting up local DNS, you'll have control.

This autonomy change allows you to decide how to handle your requests. You can resolve them yourself by querying authoritative servers directly or forward them to a trusted resolver. However, requests sent from your computer will not be encrypted and can still be seen by your ISP or upstream resolver if your local DNS setup does not use DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT). You do not have complete privacy without encrypted DNS; you only have control over the cache, filters, and upstream services you trust.

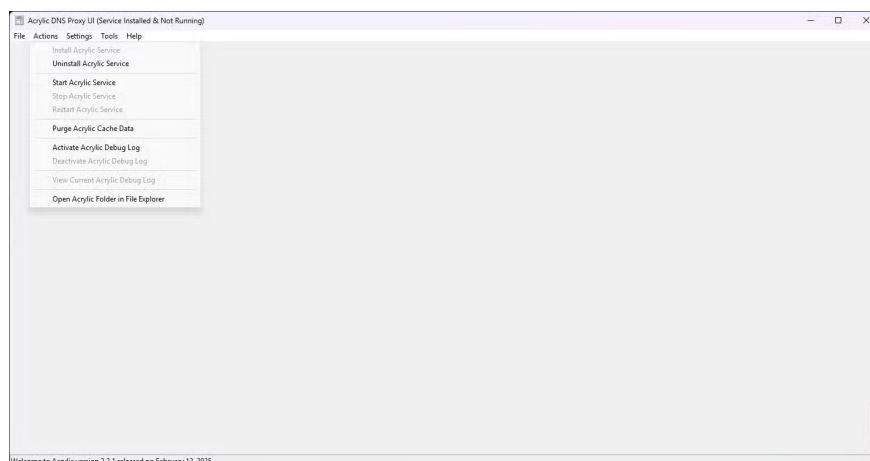
This is a powerful control that allows you to apply caching and custom rules to block specific websites from your child's device or get faster access to frequently visited domains. You can even add a hosts file to block known trackers.

How to create local DNS

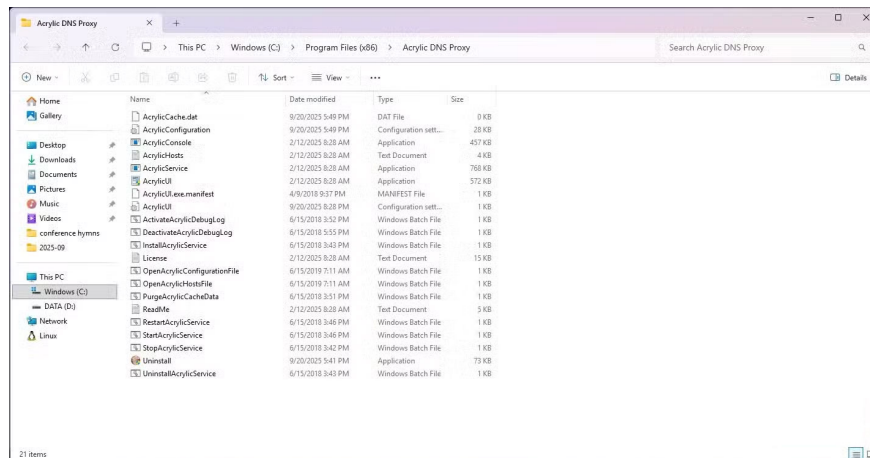
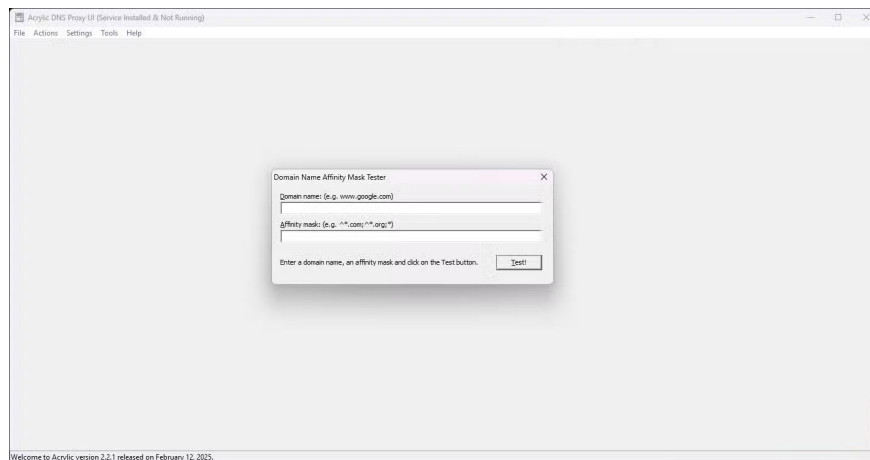
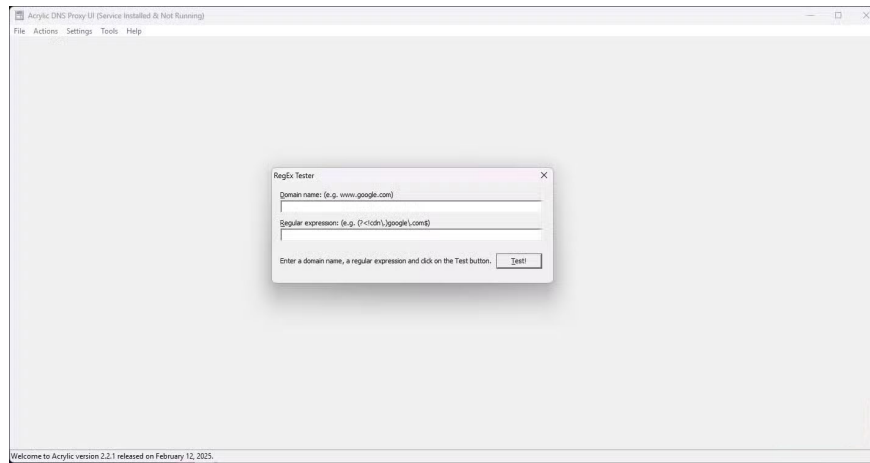
Free Local DNS on Windows 11



```
Acrylic DNS Proxy UI (Service Installed & Not Running)
File Actions Settings Tools Help
:
: IF YOU MAKE ANY CHANGES TO THIS FILE YOU HAVE TO RESTART THE ACRYLIC DNS PROXY SERVICE OR CONSOLE IN ORDER TO SEE
: THEIR EFFECTS.
:
[GlobalSection]
:
: The IP address of your primary DNS server. You can use an IPv4 address in quad-dotted notation or an IPv6 address in
: colon-separated groups.
:
: Upon installation it points to the primary Google Public DNS server.
:
PrimaryServerAddress=1.1.1.1
:
: The TCP/UDP port your primary DNS server is supposed to be listening to. The default value of 53 is the standard port
: for DNS resolution. You should change this value only if you are using a non standard DNS server or a protocol
: different than UDP/TCP (e.g. the standard port for the DNS-over-HTTPS protocol is 443).
:
PrimaryServerPort=53
:
: The protocol to use with your primary DNS server.
:
: The currently supported protocols are UDP, TCP, SOCKS5 and DOH (DNS-over-HTTPS).
:
: When using the UDP protocol, Acrylic forwards DNS requests using UDP or TCP, in accordance with RFC 5625.
:
: When using the TCP protocol, Acrylic forwards DNS requests using TCP only. Since establishing a TCP connection for
: every DNS request requires a significant amount of time and the number of TCP connections that can be opened in a unit
: of time is limited by the Operating System, this protocol should be used only in situations where using the UDP
: protocol isn't possible for some reason.
:
: When using the SOCKS5 protocol, Acrylic forwards DNS requests to your primary DNS server using a SOCKS 5 proxy as an
: intermediary, in accordance with RFC 1928. Currently, only the NO AUTHENTICATION REQUIRED method for SOCKS 5 is
: supported.
:
: When using the DOH protocol, Acrylic forwards DNS requests to your primary DNS server using DNS-over-HTTPS, a protocol
: for performing DNS resolution via HTTPS and thus increase user privacy and security by preventing eavesdropping and
: manipulation of DNS data by man-in-the-middle attacks. Be aware though that when using DNS-over-HTTPS, the encryption
: algorithms (e.g. the TLS version) your Operating System can use must match at least one your primary DNS server
: accepts, and this is not always the case depending on the combination of your Operating System version and the chosen
: DNS server. For example, old Windows versions can have a hard time establishing an HTTPS connection with DNS servers
: requiring TLS 1.1 or 1.2, and thus may require the installation of specific updates.
:
You are now editing the file "C:\Program Files\j080\Acrylic DNS Proxy\AcrylicConfiguration.ini".
```



```
Acrylic DNS Proxy UI (Service Installed & Not Running)
File Actions Settings Tools Help
:
: Install Acrylic Service
: Uninstall Acrylic Service
: Start Acrylic Service
: Stop Acrylic Service
: Restart Acrylic Service
:
: Purge Acrylic Cache Data
:
: Activate Acrylic Debug Log
: Deactivate Acrylic Debug Log
: View Current Acrylic Debug Log
: Open Acrylic Folder in File Explorer
:
Welcome to Acrylic version 2.2.1 released on February 12, 2023.
```



When deciding to set up a DNS server, what people are looking for is something practical and free. So no Raspberry Pi and subscription required – just something that works on Windows 11. Here's exactly what to do:

1. Download Acrylic DNS Proxy from the Mayakron website , then install it using the default options. Acrylic is a great choice because it's free and lightweight, and doesn't require any complicated configuration. Note, however, that Acrylic doesn't encrypt your DNS traffic—it just forwards your requests. To encrypt, you'll need a resolver or tool that supports DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT).

2. Next, open the network connection settings in Control Panel. Here, right-click on the active connection (Wi-Fi or Ethernet) and select **Properties** .
3. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties** . Then, select **Use the following DNS server addresses** and set **the Preferred DNS server** to **127.0.0.1** . This way, Windows will always send DNS lookups to Acrylic running locally.
4. Then, set Quad9 as the upstream resolver that Acrylic forwards requests to by launching Acrylic, clicking **File** , then selecting **Open Acrylic Configuration** and setting the parameters below to the following values:
 1. Primary Server Address: 9.9.9.9
 2. Primary Server Port: 53
 3. Secondary Server Address: 149.112.112.112
 4. Secondary Server Port: 53

Note : Quad9 is an ideal upstream resolver because it proactively blocks some known malicious domains, but you will need to add a free hosts file or filter list to Acrylic to block known advertising/tracking domains. Of course, you can also use any other DNS server that prioritizes online safety.

This setting makes a real difference. Cached DNS queries are answered locally, which speeds up domain resolution times, especially on slow internet connections, as cached DNS lookups bypass the initial problem. You can also choose to add a free hosts file to block domains known to be used by ad trackers, so intrusive requests don't reach your browser.

Each DNS will have different levels of success. Some are too technical, some are too time-consuming to return results. However, setting up a local DNS is different. It gives you control, filtering, and some speed benefits—but it won't prevent your ISP from seeing the IP address you're connecting to. To do that, you'll need to pair your local configuration with an encrypted DNS, or you can use one of our recommended VPN services to secure your entire connection.

You finished reading the article "**How to build a local DNS to prevent tracking from ISPs**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.