What is DNS

The Domain Name System (DNS) is the "phonebook of the internet," transla□ng human-friendly domain. When you type a domain name like **google.com** into your browser, a DNS resolver translates that name into an IP address (for example, 142.251.20.101) so your device knows which server to contact.

Most people use the DNS resolver assigned by their Internet Service Provider (ISP). Switching to 1.1.1.1 gives you a faster, more private alternative. Unlike most DNS resolvers, 1.1.1.1 does not sell user data to advertisers.

DNS over HTTPS (DoH) encrypts your DNS queries by sending them as HTTPS requests. This prevents anyone between your device and the resolver — such as your ISP or a network attacker — from seeing which domains you look up.

Some ISPs/DNS providers block access to our domains. You can bypass this by enabling DNS-over-HTTPS (DoH) in your browser.

Configure DoH on your browser

Several browsers support DNS over HTTPS (DoH), which encrypts your DNS queries to protect them from monitoring and tampering.

Some browsers might already have this setting enabled.

Note

1.1.1.1 for Families provides additional filtering to block malware, phishing, or adult content. To use it, follow the steps below but, instead of choosing the default 1.1.1.1 option, refer to Set up and specify the URL you want to use.

Mozilla Firefox

1. Select the menu button > **Settings**.
2. In the **Privacy & Security** menu, scroll down to the **Enable secure DNS using:**section.
3. Select **Increased Protection** or **Max Protection**. By default, it will use the **Cloudflare** provider.
4. If this is not the case, select **Cloudflare** in the **Choose Provider** dropdown.

Google Chrome

1. Select the three-dot menu in your browser > **Settings**.
2. Select **Privacy and security** > **Security**.
3. Scroll down and enable **Use secure DNS**.
4. Select the **With** option, and from the drop-down menu choose *Cloudflare (1.1.1.1)*.

Microsoft Edge

1. Select the three-dot menu in your browser > **Settings**.
2. Select **Privacy, Search, and Services**, and scroll down to **Security**.
3. Enable **Use secure DNS**.
4. Select **Choose a service provider**.
5. Select the **Enter custom provider**drop-down menu and choose *Cloudflare (1.1.1.1)*.

Brave

1. Select the menu button in your browser > **Settings**.
2. Select **Privacy and security** >**Security**.
3. Under **Advanced**, enable **Use secure DNS**.
4. From the **Select DNS provider** drop-down menu, choose *Cloudflare (1.1.1.1)*.

Check if the browser is configured correctly

Visit 1.1.1.1 help page ↗ and check if Using DNS over HTTPS (DoH) shows Yes

Speed up your online experience with Cloudflare's public DNS resolver.

Most people use the DNS resolver assigned by their Internet Service Provider (ISP). Switching to 1.1.1.1 gives you a faster, more private alternative. Unlike most DNS resolvers, 1.1.1.1 does not sell user data to advertisers.

1.1.1.1 (DNS Resolver)

Copy as MarkdownView as Markdown Agent setupDocs for agents

Available on all plans

1.1.1.1 is Cloudflare's public DNS resolver ↗. When you type a domain name like cloudflare.cominto your browser, a DNS resolver translates that name into an IP address (for example, 104.16.123.96) so your device knows which server to contact.

1.1.1.1 has been measured as thefastest public DNS resolver ↗. It runs on Cloudflare's network in hundreds of cities worldwide ↗ and has access to the addresses of millions of domains on the same servers it runs on.

1.1.1.1 is free. Setting it up takes minutes and does not require any special software.

IP addresses

Copy as Markdown View as Markdown Agent setupDocs for agents

Use the addresses below to configure your device or router. Two addresses are provided for each resolver for redundancy.

For step-by-step instructions, refer to Set up.

1.1.1.1

The standard resolver provides fast, private DNS lookups with no content filtering.

IPv4	IPv6
1.1.1.1 1.0.0.1	2606:4700:4700::1111 2606:4700:4700::1001

Refer to Encryption to learn how to encrypt your DNS queries.

1.1.1.1 for Families

1.1.1.1 for Families adds automatic filtering to block known malware, phishing, and (optionally) adult content.

For more information, refer to 1.1.1.1 for Families set up.

Block malware

IPv4	IPv6
1.1.1.2 1.0.0.2	2606:4700:4700::1112 2606:4700:4700::1002

Block malware and adult content

IPv4	IPv6
1.1.1.3 1.0.0.3	2606:4700:4700::1113 2606:4700:4700::1003