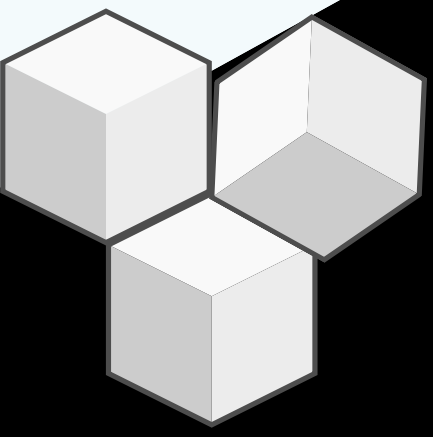
Documentation

Cloudflare WARP 1.1.1.1



Prepared By
Sakshi Kashyap

Basket Hunt
BETA

Table of Contents

	Contents	Pg No.
1.	Introduction to Cloudflare	3
2.	Introduction to Cloudflare WARP 1.1.1.1	4 - 5
3.	Cloudflare WARP 1.1.1.1 v/s OpenVPN Connect	6 - 7
4.	WARP Modes	8 - 9
5.	Installing and Setting up of Cloudflare WARP 1.1.1.1	10 - 16
6.	Privacy with WARP 1.1.1.1	17 - 18
7.	Encryption with 1.1.1.1	19

1. Introduction to Cloudflare

Cloudflare is a large network of servers that can improve the security, performance, and reliability of anything connected to the Internet. Cloudflare does this by serving as a reverse proxyOpen external link for your web traffic. Every request to and from your origin passes through Cloudflare, where we can apply a number of rules and optimizations to enhance security, speed, and dependability.

When your traffic is proxied through Cloudflare before reaching your origin server, your application gets additional security, performance, and reliability benefits.

Security

Along with blocking harmful traffic before it reaches your origin web server, Cloudflare also masks your origin's IP address from potential attackers. Using our WAF and DDoS defence, Cloudflare automatically reduces security concerns.

*** A Web Application Firewall or WAF creates a shield between a web app and the Internet. This shield can help mitigate many common attacks.*

*** HTTP DDoS attack protection. Included in all Cloudflare plans for zones onboarded to Cloudflare (zones with their traffic routed through the Cloudflare network).*

Performance

Cloudflare also functions as a Content Delivery Network (CDN) for proxied traffic, caching static resources and otherwise streamlining the delivery of assets.

Reliability

Requests from website visitors are forwarded to the closest Cloudflare data centre through the company's internationally dispersed Anycast network. Our network assists in keeping your application online when used in conjunction with our CDN and DDoS defence.

2. Introduction to Cloudflare WARP 1.1.1.1

1.1.1.1 is a free Domain Name System (DNS) service by American company Cloudflare in partnership with APNIC. The service functions as a recursive name server providing domain name resolution for any host on the Internet. The service was announced on April 1, 2018.

DNS resolver translate domains like cloudflare.com into the IP addresses necessary to reach the website (like 104.16.123.96).

1.1.1.1 is a recursive DNS resolver. It's important to say at the outset that 1.1.1.1 is not a Virtual Private Network (VPN).

A VPN encrypts all your device's data and sends that information to a server controlled by the VPN company. This process hides your true IP address and prevents your ISP—or any spy on your network—from monitoring your traffic.

A secure DNS resolver only secures DNS requests, the wide adoption of HTTPS means that much of your online activity is already encrypted.

Cloudflare runs an authoritative DNS resolver with a network of over 20 million Internet properties. With the recursor and the resolver on the same network, some DNS queries can be answered directly. With the release of the 1.1.1.1 mobile application in November 2018, Cloudflare added the ability for users to encrypt their DNS queries over HTTPS (DoH) or TLS (DoT).

In September 2019, Cloudflare released a VPN service called WARP which is built into the 1.1.1.1 mobile app.

Combined with the power of 1.1.1.1 (the world's fastest public DNS resolver), WARP keeps your traffic secure, private and fast. Cloudflare prevents snooping or selling the personal data of its customers. And if DNS-over-HTTPS (DoH) or DNS-over-TLS (DoT) is used to the 1.1.1.1 resolver, the DNS request will be sent over a secure channel.

The VPN will operate on a freemium model, allowing customers to upgrade to Warp+ for faster performance with a "low monthly fee."

The WARP Client application uses a VPN profile and/or service that enables to intercept and secure the DNS queries and to transmit data from the device through the Cloudflare network, depending on the services enabled. Only limited DNS queries are collected and traffic data (excluding payload) that is sent to cloudflare network when the app is enabled on the device. Although 1.1.1.1 uses VPN technology, it isn't a VPN. But because it needs to create a VPN connection, you can't use a separate VPN at the same time.

3. Cloudflare WARP 1.1.1.1 v/s OpenVPN Connect

- WARP establishes a secure link between your personal devices (such as laptops, smartphones) and the online services used.
- Combined with the power of 1.1.1.1, WARP keeps your traffic secure, private and fast. It prevents snooping or selling the personal data of its customers.
- The basic 1.1.1.1 DNS resolution app and Warp VPN service are free. It is paid-for extra features of Cloudflare's existing 1.1.1.1 app, offering fast DNS resolution while also helping to keep your browsing activity hidden from your broadband provider and safeguarding you against potential man-in-the-middle attacks.
- 1.1.1.1 with WARP prevents anyone from snooping on you by encrypting more of the traffic leaving your device.

- OpenVPN is one of the VPN implementations which uses SSL/TLS protocol to safeguard connections.
- Unlike other SSL based VPNs, OpenVPN can be configured to preshared keys and also X.509 certificates.
- Most at times OpenVPN is free to download irrespective of platforms. You can connect to a VPN server without paying anything by using OpenVPN. Therefore, OpenVPN offers free access whenever VPN connections from a certain server are received. Due to this, OpenVPN is affordable.
- With the usage of OpenSSL along with HMAC packet authentication, the network can be ensured of maximum safety and from Man In the Middle Attacks.

- Cloudflare will retain only the limited transaction and debug log data (“Public Resolver Logs”) for the legitimate operation of the Public Resolver and research purposes, and Cloudflare will delete the Public Resolver Logs within 25 hours. There are three categories of data being collected: Account Data, Operational Data, and DNS Resolver Information.

- Cloudflare Warp is supported over the platforms - Android, iOS, Linux, macOS, Windows.

- Each time a user connects to the Private Tunnel service, openVPN retain the following data for 14-30 days: the user's source IP address, the Private Tunnel IP address used by the user, connection start and stop time and total number of bytes used.

- OpenVPN is supported over the platforms - Windows, iOS, OS X, Linux.

4. WARP Modes

The WARP client has several modes to better suit different connection needs –

1.1.1.1

1.1.1.1 is Cloudflare's public DNS resolver. It offers a fast and private way to browse the Internet. It also offers a DNS encryption service through DNS over HTTPS (DoH) or DNS over TLS (DoT) for increased security and privacy.

1.1.1.1 with WARP

The WARP application uses BoringTun to encrypt and secure the traffic from your device, and send it directly to Cloudflare's edge network. This ensures Internet traffic between your device and the Internet is secure and private, while also preventing third parties from accessing your traffic. If the site you are visiting is already a Cloudflare customer, the content is immediately sent to your device. If not, Cloudflare uses its global network of data centers to devise the shortest path to the site.

WARP via local proxy

Currently, this mode is available on desktop clients only. When WARP is configured as a local proxy, only the applications that you configure to use the proxy (HTTPS or SOCKS5) will have their traffic sent through WARP. This allows you to pick and choose which traffic is encrypted — for example, your web browser or a specific application. Everything else will not be encrypted and will be sent over a regular Internet connection.
Because this feature restricts WARP to just applications configured to use the local proxy, leaving all other traffic over the Internet unencrypted by default, we have hidden it in the Advanced menu. To turn it on:
1. Navigate to Preferences > Advanced and select Configure Proxy.
2. On the window that opens, check the box and configure the port you want to listen on.
This will enable the WARP via Local Proxy option in the WARP Settings menu.

WARP+

WARP+ will route your traffic around congested Internet routes and improve overall end-to-end performance. You can purchase WARP+ via iOS and Android devices, and use it both with Cloudflare's mobile and desktop apps. WARP+ runs on a limited data plan — the more people you refer, the more MBs of data you can use with WARP+.

WARP unlimited

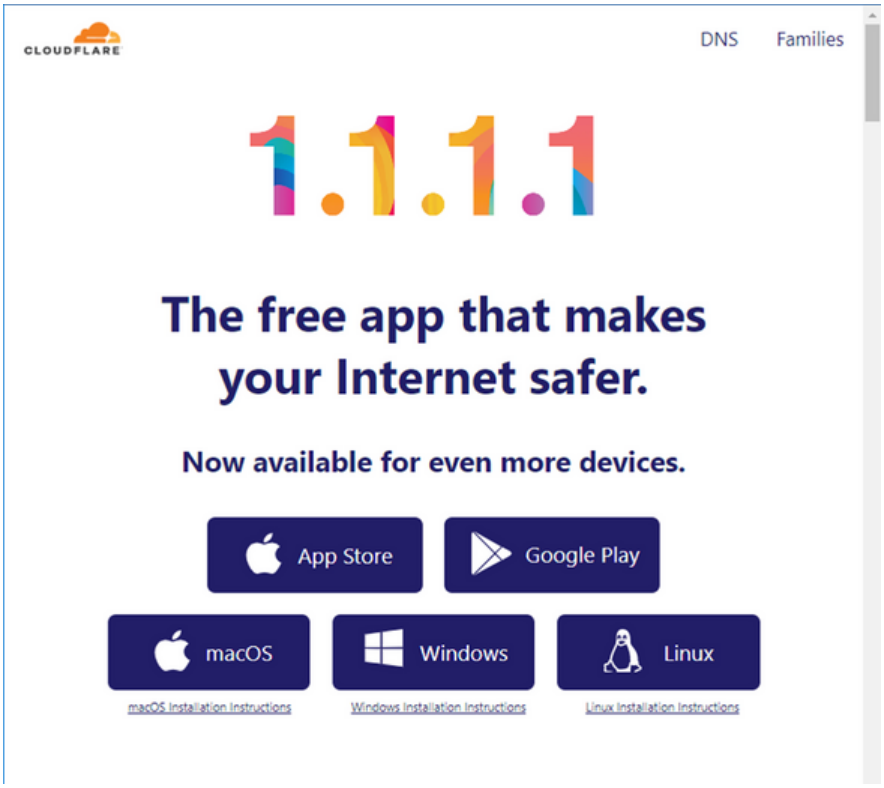
If you would like to secure all your mobile traffic without any data limits, you can get WARP+ Unlimited by buying their monthly subscription.
Here we are going to discuss about the Cloudflare Warp 1.1.1.1 in detail.

In this Documentation, we are going to discuss Cloudflare WARP 1.1.1.1 version in detail.

5. Installing & Setting up of Cloudflare WARP 1.1.1.1

Download link for Cloudflare WARP 1.1.1.1 :
https://1.1.1.1/

This window appears -

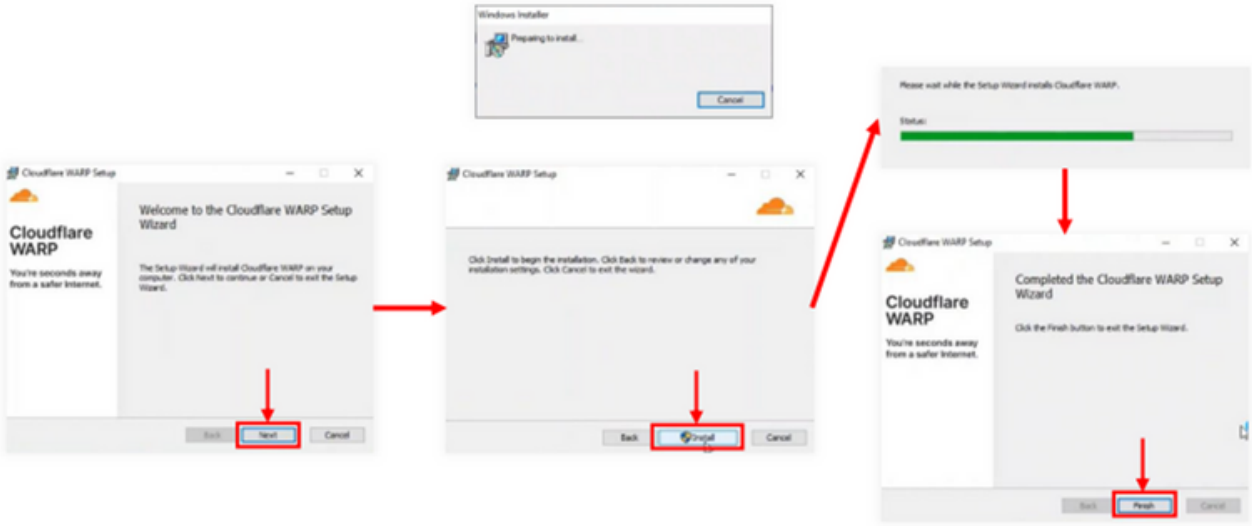


Now Select the suitable version for desktop your device uses.

For Windows -

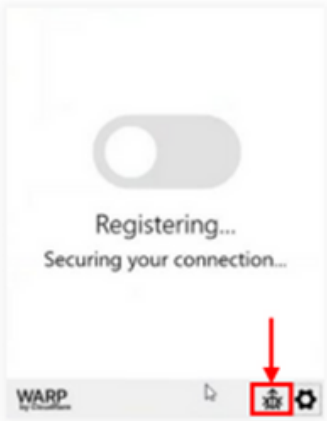
It will start downloading at the bottom of the window. Once completed, click on the download to open it.

The installer will launch. It will then guide you through the installation.

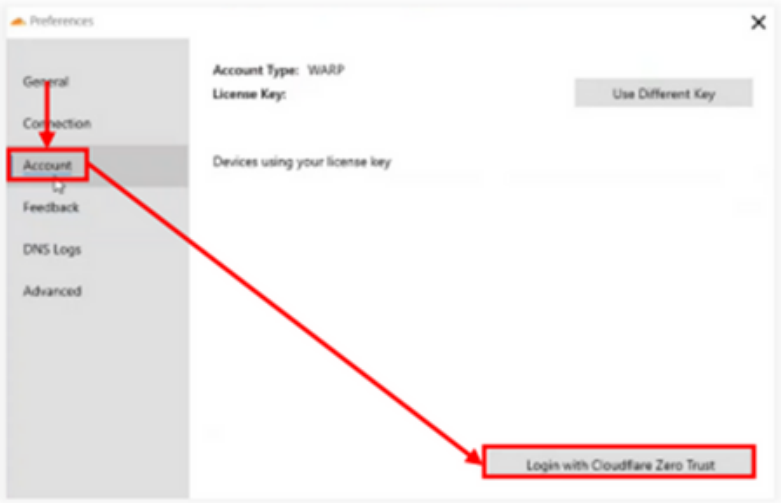


A pop-up for the application will open on the bottom right of the screen. Click “Next” and then click “Accept”.

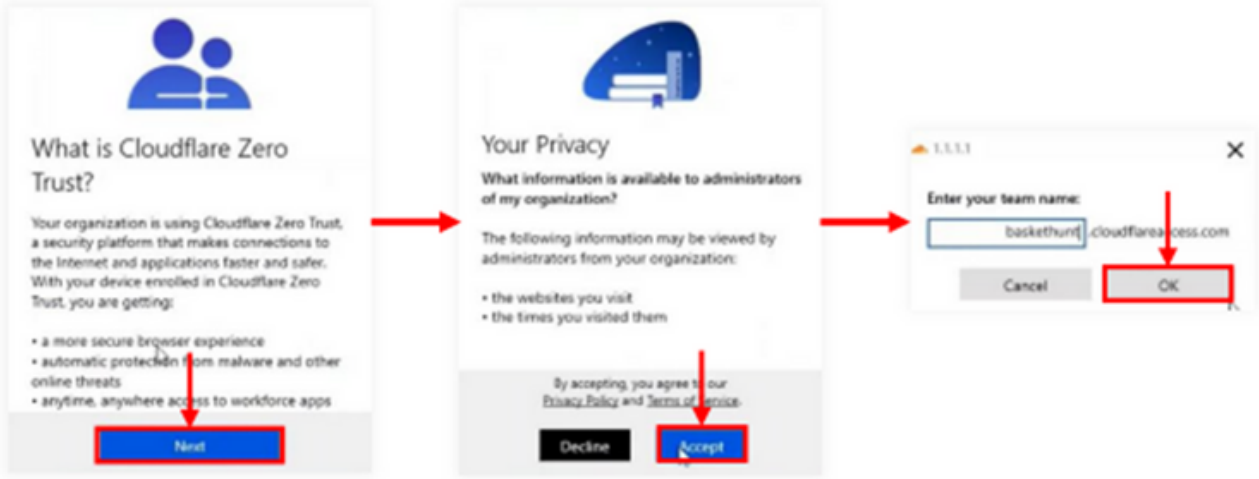
On the pop-up, click the bug-shaped icon.



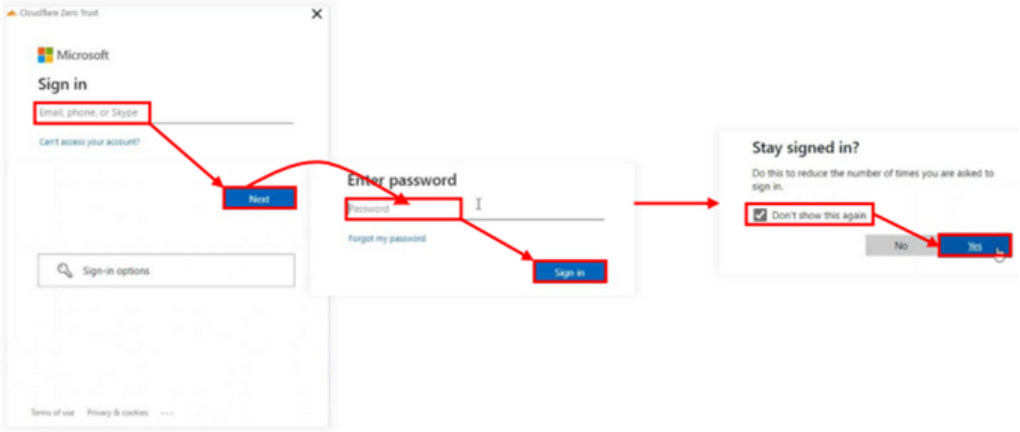
This will open a window. Here, you will click “Account” -> “Login with Cloudflare Zero Trust”.



On the pop-up click “Next” -> “Accept”. Under team name, enter “baskethunt” then click “OK”.



A window will prompt you to enter your Microsoft Credentials (Make sure you are using the Organization Microsoft account).



After the “successful sign in”, go to the application (It will be located in the bottom right of your screen) and turn it on.

You are all set to use the Warp 1.1.1.1 service.

WARP modes available -

The WARP app has two main modes of operation: WARP and 1.1.1.1.

In WARP mode, all traffic leaving your computer is encrypted and sent over WARP, including DNS traffic. In 1.1.1.1 mode, the WARP app only encrypts DNS traffic to the 1.1.1.1 resolver.

WARP mode is the default and the recommended mode of operation. However, if you only want to use the 1.1.1.1 resolver mode:

1. Click the WARP app icon.
2. Click the cog icon, and choose your preferred mode of operation for WARP.

WARP Options -

Beyond the two modes of operation, the WARP app lets you configure additional options to better suit your needs. You can change the protocol used to connect to Cloudflare or enable 1.1.1.1 for Families, for example.
To access these options:

1. Click the WARP app icon.
2. Click the cog icon > Preferences.

The following is a list of options you can configure in the Connection tab:

- **Disable for all Wi-Fi / wired networks:** Check the box corresponding to the network where you want to prevent WARP from working on.
- **DNS Protocol:** The available options depend on the WARP mode you have enabled:
  - **WARP:** Only available when you have the WARP mode enabled. All DNS traffic encrypted and sent to Cloudflare's edge.
  - **HTTPS:** All DNS traffic is sent outside the tunnel via DNS over HTTPS.
  - **TLS**: All DNS traffic is sent outside the tunnel via encrypted TLS.
- **1.1.1.1 for Families:** Allows you to enable 1.1.1.1 for Families and choose between blocking malware, or blocking malware and adult content.

Cloudflare WARP GUI -

This is the main GUI application that you interact with. You can find it in:

- Start menu > Cloudflare.
- On your disk, in C:\Program Files\Cloudflare\Cloudflare WARP\Cloudflare WARP.exe.

Cloudflare WARP Service -

This is the Windows service that is responsible for establishing the wireguard tunnel and all interaction between Cloudflare's service endpoint and the client application. You can find it in C:\Program Files\Cloudflare\Cloudflare WARP\warp-svc.exe.

Log Files -

The Windows application places log files in two locations based on what part of the application is logging information. These logs are included during feedback submission when you check Feedback > Share debug information. You can find the logs for:

- WARP Service: C:\ProgramData\Cloudflare.
- Application GUI Logs: C:\Users\<your username>\AppData\Local\Cloudflare.

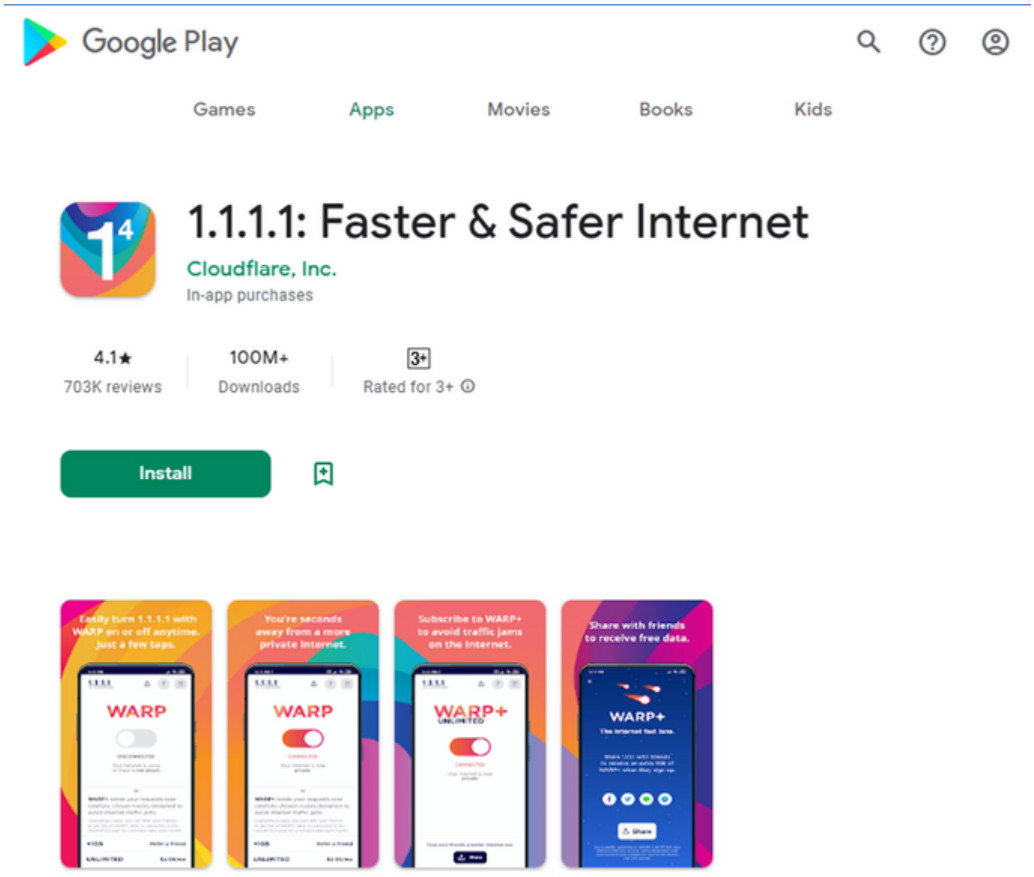
Steps to remove the application -

1. Click the Start menu and search for Settings. You can also press ⊞ Win + i).
2. Select Apps > App & Features.
3. Scroll down to Cloudflare WARP and select Uninstall.

For Android -

By default, 1.1.1.1:Faster Internet is configured to WARP mode. You can also configure it to only encrypt your DNS queries and leave the remaining traffic unencrypted.

1. Download 1.1.1.1: Faster Internet from Google Play for free.



2. Launch 1.1.1.1: Faster Internet and accept the Terms of Service.
3. Toggle the WARP button to Connected.
4. Install the VPN profile that allows your phone to connect securely to 1.1.1.1.

Your connection to the Internet and your DNS queries are now protected.

Enable only DNS queries -

After installing 1.1.1.1: Faster Internet, you may want to only encrypt your DNS queries and leave the remaining traffic unencrypted.

1. Open 1.1.1.1: Faster Internet.
2. Toggle the WARP button and choose Switch to DNS only mode.
3. If the WARP toggle is disconnected, tap the menu button.
4. You will see two options: 1.1.1.1 and WARP. Select 1.1.1.1.

You are now using encryption only for your DNS queries.

Enable 1.1.1.1 for Families -

1. Open 1.1.1.1: Faster Internet.
2. Tap the menu button.
3. Select Advanced > Connection options.
4. In DNS settings > 1.1.1.1 for Families, select the option you want to use.

Steps to remove the application -

1. Find the application on the home screen.
2. Touch and hold on the application tile.
3. Select Remove App.
4. Select Delete App.

For iOS follow the link below -

https://developers.cloudflare.com/warp-client/get-started/ios/

For Linux follow the link below -

https://developers.cloudflare.com/warp-client/get-started/linux/

For Linux follow the link below -

https://developers.cloudflare.com/warp-client/get-started/macos/

6. Privacy with WARP 1.1.1.1

Depending on the services you have enabled, the WARP Client application employs a VPN profile and/or service that enables us to intercept and secure your DNS requests as well as transfer data from your device across the Cloudflare network. When you have the app active on your device, we merely gather a small amount of DNS query and traffic data (excluding payload) that is delivered to our network.

Check out the below link to know about the privacy policy of WARP 1.1.1.1 in detail :
https://www.cloudflare.com/application/privacypolicy/

What does Cloudflare do with the user's data -

The very least amount of information that seems necessary to deliver the service is stored by Cloudflare. Except as required to deliver the services or as otherwise specified in the Privacy Policy, they claim not to sell, rent, distribute, or otherwise disclose your personal information to anyone without first giving you notice and the opportunity to consent.
They do not use the data to identify who you are or what you are doing on the Internet beyond the exceptions mentioned. Such data may include: your app installation ID, the amount of data transferred through Cloudflare's network, and your average speed when you are using the WARP Client application.

How Cloudflare uses user data -

Registration ID
Cloudflare uses a random identifier generated when you install the app to give you referral bonuses for referring the app to others.

Data Transferred
Cloudflare tracks the amount of data your WARP installation has transferred to keep track of your WARP+ usage. When you refer friends to WARP, this quota is increased.

Average Speed

Cloudflare uses this data to understand how much faster the WARP Client application is making your Internet connection. Knowing this information helps us improve the application in your region and on your mobile carrier or Internet provider.

Aggregate Usage

Cloudflare tracks the aggregate amount of traffic by website and by region. Knowing this information helps Cloudflare plan better when we should build future data centers.

Check out the below link to know about the Application Terms of Service:

hhttps://www.cloudflare.com/application/terms/

Check out the below link to know about the Third party licenses:

https://developers.cloudflare.com/warp-client/legal/3rdparty/

7. Encryption with 1.1.1.1

Traditionally, DNS queries and replies are performed over plaintext. Even when you are viewing a secured website, they are sent across the Internet without any encryption or security. This has a significant impact on security and privacy since hostile actors, advertisers, ISPs, and others may monitor, spoof, and trace these searches.

To prevent this and secure your connections, 1.1.1.1 supports DNS over TLS (DoT) and DNS over HTTPS (DoH), two standards developed for encrypting plaintext DNS traffic. This prevents untrustworthy entities from interpreting and manipulating your queries.

DNS over HTTPS -

DNS requests and replies are sent via the HTTP or HTTP/2 protocols while using DNS over HTTPS (DoH). DoH ensures that a ttackers cannot spoof or modify DNS traffic. DoH encapsulates the DNS query in an HTTPS request using port 443, which is the default port for HTTPS transmission. Due to the fact that all HTTPS traffic originates and ends on the same port, DNS requests and responses are masked by other HTTPS traffic.

DNS over TLS -

DNS over TLS (DoT) is one way to send DNS queries over an encrypted connection. Cloudflare supports DNS over TLS on standard port 853 and is compliant with RFC7858. With DoT, the encryption happens at the transport layer, where it adds TLS encryption on top of the user datagram protocol (UDP).

There are many other ways to use 1.1.1.1 beyond the traditional set up in operating systems and routers.

- DNS in **Google Sheets** (https://developers.cloudflare.com/1.1.1.1/other-ways-to-use-1.1.1.1/dns-in-google-sheets/)
- DNS over **Discord** (https://developers.cloudflare.com/1.1.1.1/other-ways-to-use-1.1.1.1/dns-over-discord/)
- DNS over **Telegram** (https://developers.cloudflare.com/1.1.1.1/other-ways-to-use-1.1.1.1/dns-over-telegram/)
- DNS over **Tor** (https://developers.cloudflare.com/1.1.1.1/other-ways-to-use-1.1.1.1/dns-over-tor/)