Gibberfish VPN Guide

Your Gibberfish server comes with a built-in VPN which can be used to enhance your online privacy. Setup instructions begin on page 3 of this guide.

What is a VPN?

A Virtual Private Network (VPN) is an online service that allows you to create an encrypted “tunnel“ between your computer or mobile device and the VPN server which all of your internet traffic then passes through. This hides your activity from every service provider between you and the VPN server (which may include corporate networks, WiFi access points, or your ISP). Furthermore, the internet sites you visit will see the traffic coming from the VPN server instead of your device, giving you an additional measure of anonymity online.

Why should I use one?

Increasingly, internet providers see your online activities as valuable data which they can sell to third-parties. As such, it‘s likely that they‘re watching and recording everything you do online. Public WiFi providers may also be snooping on your internet traffic, both to profile and track you for advertisers, or for more malicious criminal purposes. Governments and law enforcement may also be eavesdropping on your internet connection directly, or getting this data from your ISP. Websites themselves can see your IP address (your device‘s unique address on the internet) and use it to track you, even when you don‘t log in.

A VPN, in large part, protects you from this sort of passive surveillance; all anyone monitoring your internet connection will see is encrypted (i.e. meaningless) data flowing between you and the VPN server. If you‘re concerned with maintaining your privacy online, using a VPN can help.

There are a few other potential advantages to VPNs which may or may not apply depending on your situation. In some countries (China, for example), the government blocks certain websites that it deems threatening. Connecting to a VPN server outside that country allows you to bypass their filters. Additionally, if internet sites themselves block users coming from particular countries, this can be bypassed by using a VPN server in a country they permit, since they will see the connection coming from the VPN instead of you.

What are the drawbacks and limitations?

VPNs provide a powerful tool for improving your privacy and anonymity online, but like almost everything else, they‘re not perfect. While they can hide your activity from the most pervasive forms of mass-surveillance, with the right resources a determined foe may be able to partially circumvent their protections. For instance, if someone was monitoring both your internet connection *and* the VPN server‘s internet connection, it would be possible for them to infer what sites you‘re using and how, and possibly also intercept that traffic, since it is no longer encrypted once it exits the VPN server (unless you‘re using another encryption layer such as HTTPS).

Websites you visit may also be able to identify you through other means, such as cookies, browser fingerprinting, or malicious javascript. To further aid in protecting your identity, you can use a VPN in tandem with the Tor browser. In either case, if you log in to a site you have an account on, they will know who you are immediately and can easily track you.

Finally, depending on where you live, the very act of using a VPN (and other privacy tools) might attract scrutiny or in itself be considered evidence of wrongdoing. Therefore, we cannot blindly recommend the use of a VPN. It is always important for every individual to make an informed choice based on their situation and personal threat model.

When using a VPN or other privacy tool, one should never assume they are bulletproof, and it is important to remain vigilant and practice good operational security (OpSec).

Gibberfish VPN Setup

Before you begin

Obtain a copy of the VPN client from your Administrator

Your Administrator will have access to a ZIP file via the Management Portal that contains the configuration files as well as a special security key. You will need these to connect to the VPN. Ask them to share this file with you in your Gibberfish cloud.

Create an app password in Nextcloud

You will log in to the VPN using your Gibberfish username, but instead of your normal password, you will use a special securely generated “app password”.

Log in to your Gibberfish account, and go to your personal **Settings** (top-right menu). From here, click on the **Security** tab. In the box labeled “App name”, type something appropriate like “VPN”, then click **Create new app password**.

Your VPN credentials will be displayed below. Please record these somewhere that you won’t lose them because once you hit **Done** you will not be able to see them again. However, if you lose your password you can always to create a new one by repeating these steps.

Setup Instructions

Windows (version 7 and higher)

1. Download the **vpnclient.zip** file provided by your administrator.

2. Download and install the OpenVPN GUI client from here:
https://openvpn.net/index.php/open-source/downloads

Choose the one labeled “Installer, Windows 7 and later”

3. Open **vpnclient.zip** and extract the files to the config folder of your OpenVPN installation. (most likely **C:\Program Files\OpenVPN\config**)

4. Right-click the OpenVPN icon on your system tray and choose **Connect**. You will be prompted for the username and password combo you generated in the previous section. If the connection is successful, the login screen with disappear and you will see the tray icon turn green.

Linux (via Network Manager)

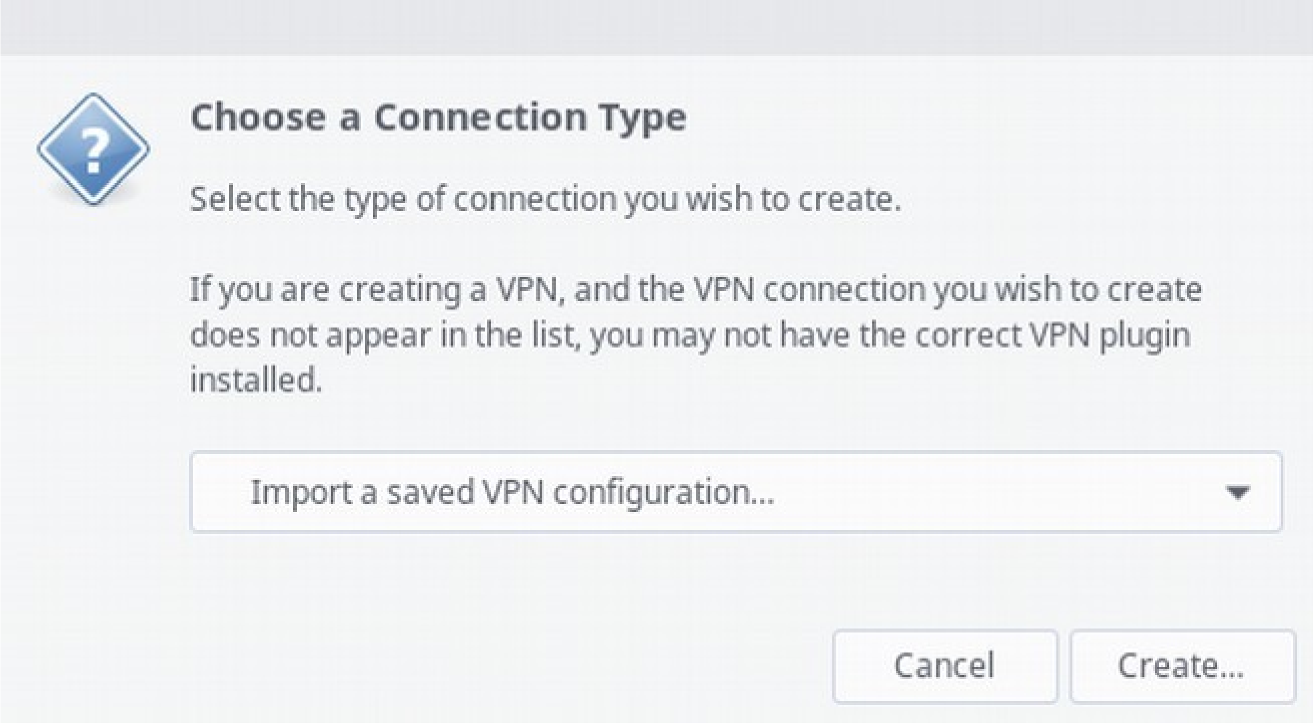
1. Download the **vpnclient.zip** file provided by your administrator and extract it to your home folder.

2. Install the OpenVPN plugin for Network Manager

```
sudo apt-get install network-manager-openvpn
```

3. Right-click the Network Manager icon in your system tray and choose **Network Connections**.

4. Click the plus sign (**+**) to add a new connection and then choose **Import a saved VPN configuration...** from the dropdown menu and click **Create...**



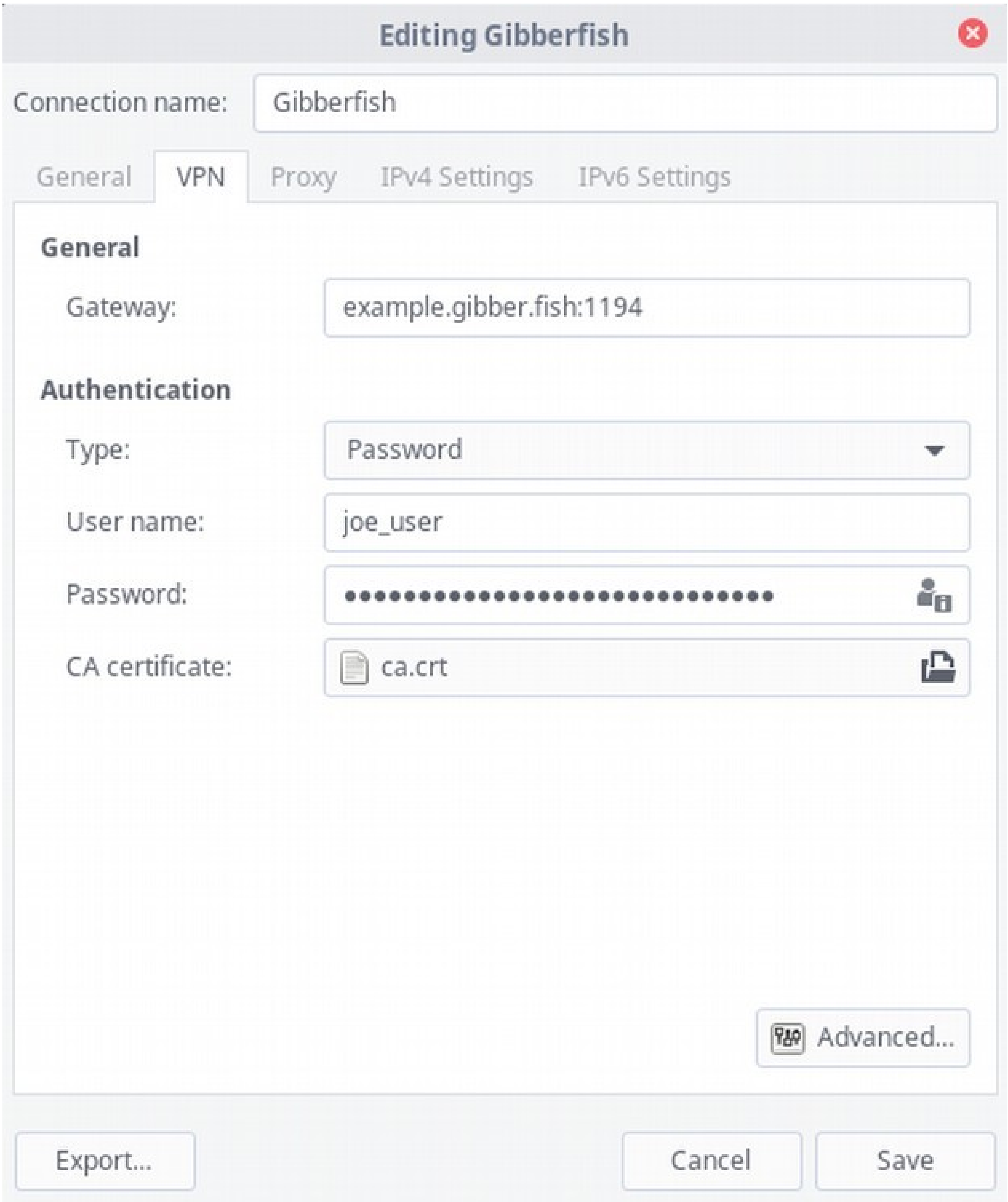
Choose a Connection Type

Select the type of connection you wish to create.

If you are creating a VPN, and the VPN connection you wish to create does not appear in the list, you may not have the correct VPN plugin installed.

Import a saved VPN configuration...

5. Browse to where you extracted the files and open **gibberfish.conf**



Editing Gibberfish

Connection name: Gibberfish

General

Gateway: example.gibber.fish:1194

Authentication

Type: Password

User name: joe_user

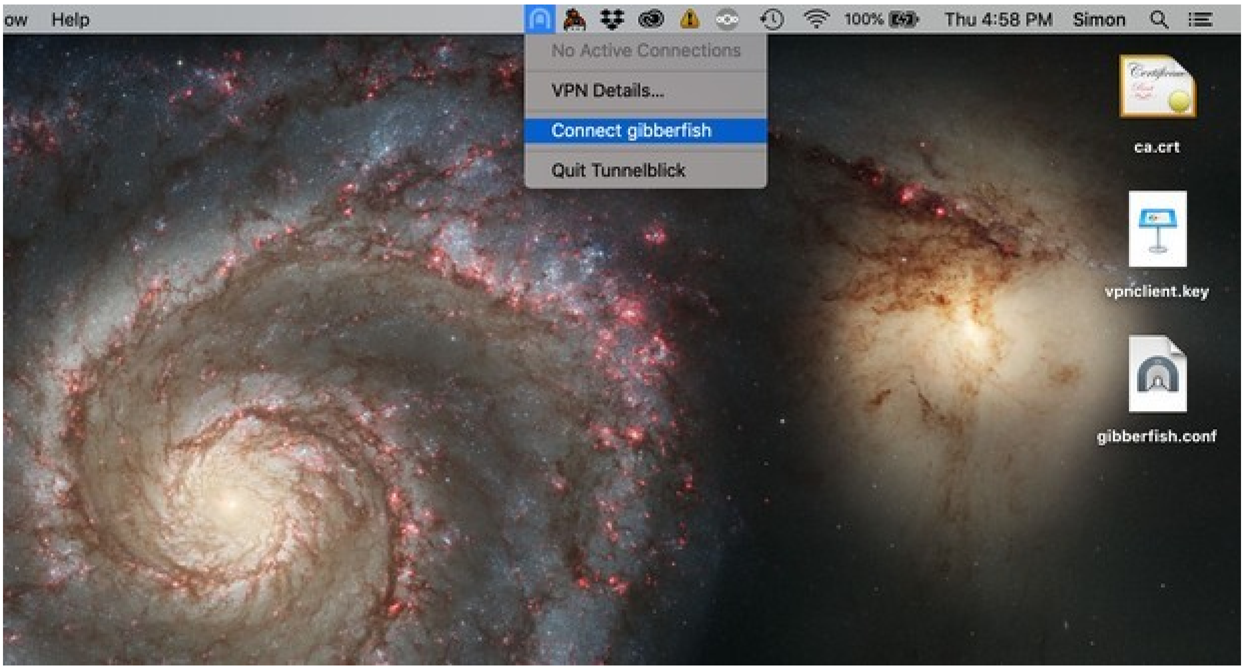
Password: ••••••••••••••••••••••••••••••

CA certificate: ca.crt

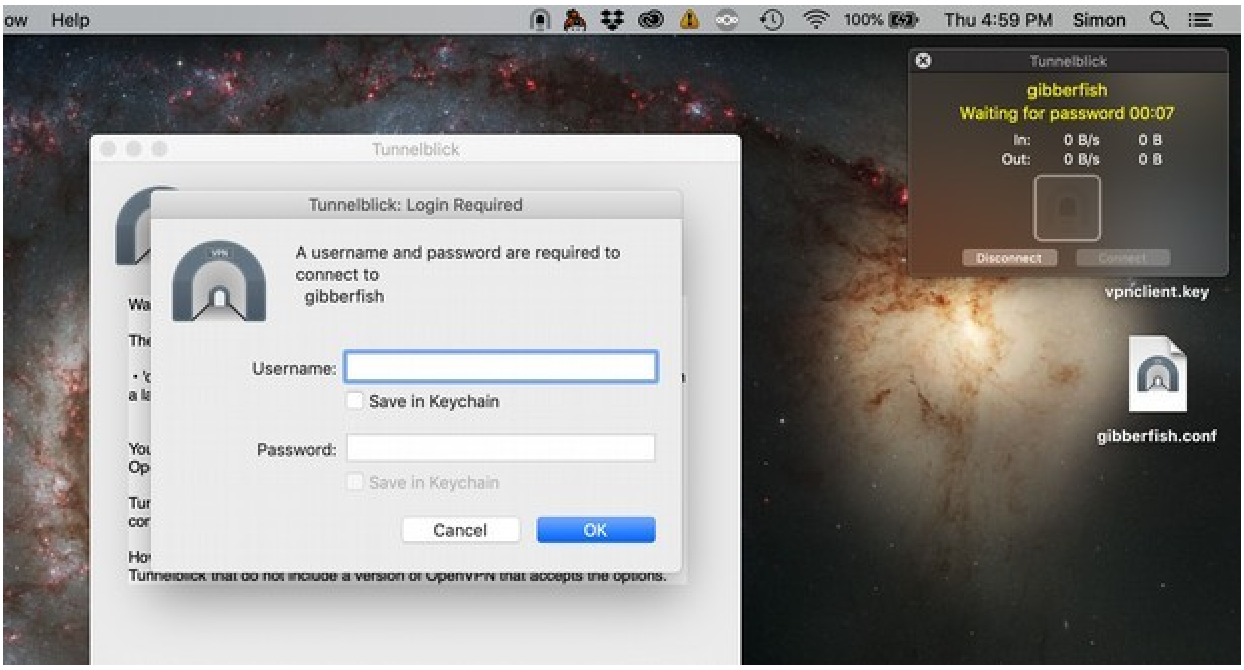
6. Enter your username and password, then click **Save**. You can now connect by right-clicking on the Network Manager tray icon and choosing **gibberfish** under the **VPN Connections** section.

OS X (Mac)

1. Download Tunnelblick from https://tunnelblick.net/ and install it following their instructions.
2. Download the **vpnclient.zip** file provided by your administrator. Extract the files anywhere you like, the desktop works well.
3. Double-click on the .conf file, and it should automatically open with Tunnelblick. If it does not, right click and select: **Open With > Tunnelblick**
4. Tunnelblick will ask if you wish to enable VPN services for yourself or all users of your computer. Choose whichever is your preference.
5. Your computer may then ask for your user password. Typically you must be an administrator or 'root' user of the computer to proceed. A notification will display that Tunnelblick was correctly configured.
6. Navigate to the menu bar and click on the Tunnelblick icon. A drop down menu will appear, click on **Connect gibberfish**.



7. Tunnelblick will ask for your user name and password. Use your Gibberfish username and the “app password” you created earlier.

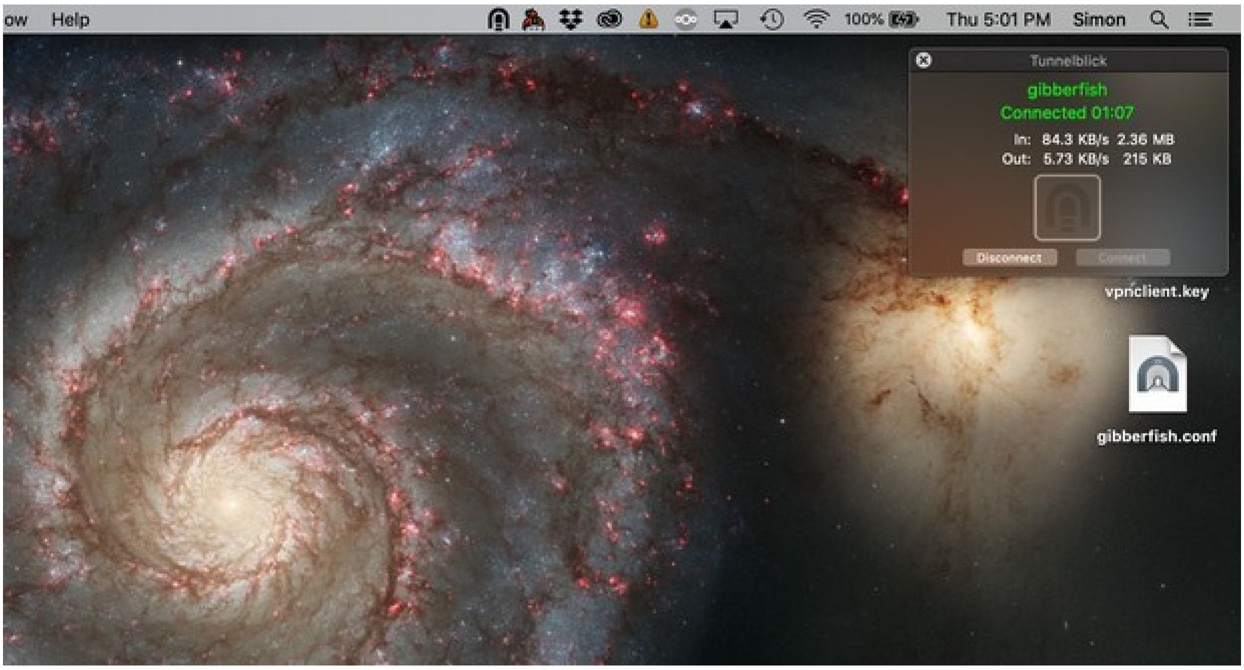


gibberfish
Waiting for password 00:07
In: 0 B/s 0 B
Out: 0 B/s 0 B

A username and password are required to connect to
gibberfish

Tunnelblick that do not include a version of OpenVPN that accepts the options.

8. Tunnelblick should then connect to your VPN. If you hover over the icon in the menu bar, a status window will appear.



gibberfish
Connected 01:07
In: 84.3 KB/s 2.36 MB
Out: 5.73 KB/s 215 KB

9. That’s it! You may delete the VPN files provided by your Gibberfish administrator, they are no longer necessary.

10. If you do not set up Tunnelblick as a login application, you will have to open Tunnelblick and connect each time you wish to use your VPN. However, the installation and configuration will not need to be done again.

Android

1. Download the **vpnclient.zip** file provided by your administrator and extract the files to your local storage.
2. Install **OpenVPN for Android** from F-Droid or the Play store.
3. Run **OpenVPN for Android** and click on the ⬇ icon to import an existing config.
4. Browse to where you extracted the ZIP file and select **gibberfish.conf**
5. Next to **CA Certificate**, tap **Select** and choose the **ca.crt** file.
6. Next to **TLS Auth File**, tap **Select** and choose the **vpnclient.key** file.
7. Click the ✔ icon to save the profile.
8. Return to the main screen and tap the **gibberfish** profile to connect. Enter your username, as well as the app password you previously generated. Optionally select **Save Password**.
9. On the **Profiles** tab, you should now see “Connected: SUCCESS” listed under the **gibberfish** profile.
10. If you want the VPN to start automatically on boot, go to the **Settings** tab, and enable the **Connect on boot** option, then set **Default VPN** to **gibberfish**.