

WireGuard Setup



WireGuard Setup

Prod URI: [https://\[your.mamori.server\]/](https://[your.mamori.server]/)

Access is authenticated via a digital identity and multi-factored with mamori.io

This guide covers :

1. Pre-requisites
2. Client Setup
3. First time portal login – setup 2FA & get WireGuard device key

Overview

To follow this guide you will need the following three items:

WireGuard Setup

Pre-requisites

- Login credentials
- Mobile 2FA App
- Laptop WireGuard client

1. A Mamori Login Account

If you don't have one, then contact your administrator. Your login could be your existing AD login.

2. Install Mamori.io 2FA mobile application

iOS App Store: search for mamori 2FA

Android App Store: search for mamori.io

3. Install Wireguard Client on your laptop

Link: <https://www.wireguard.com/install>

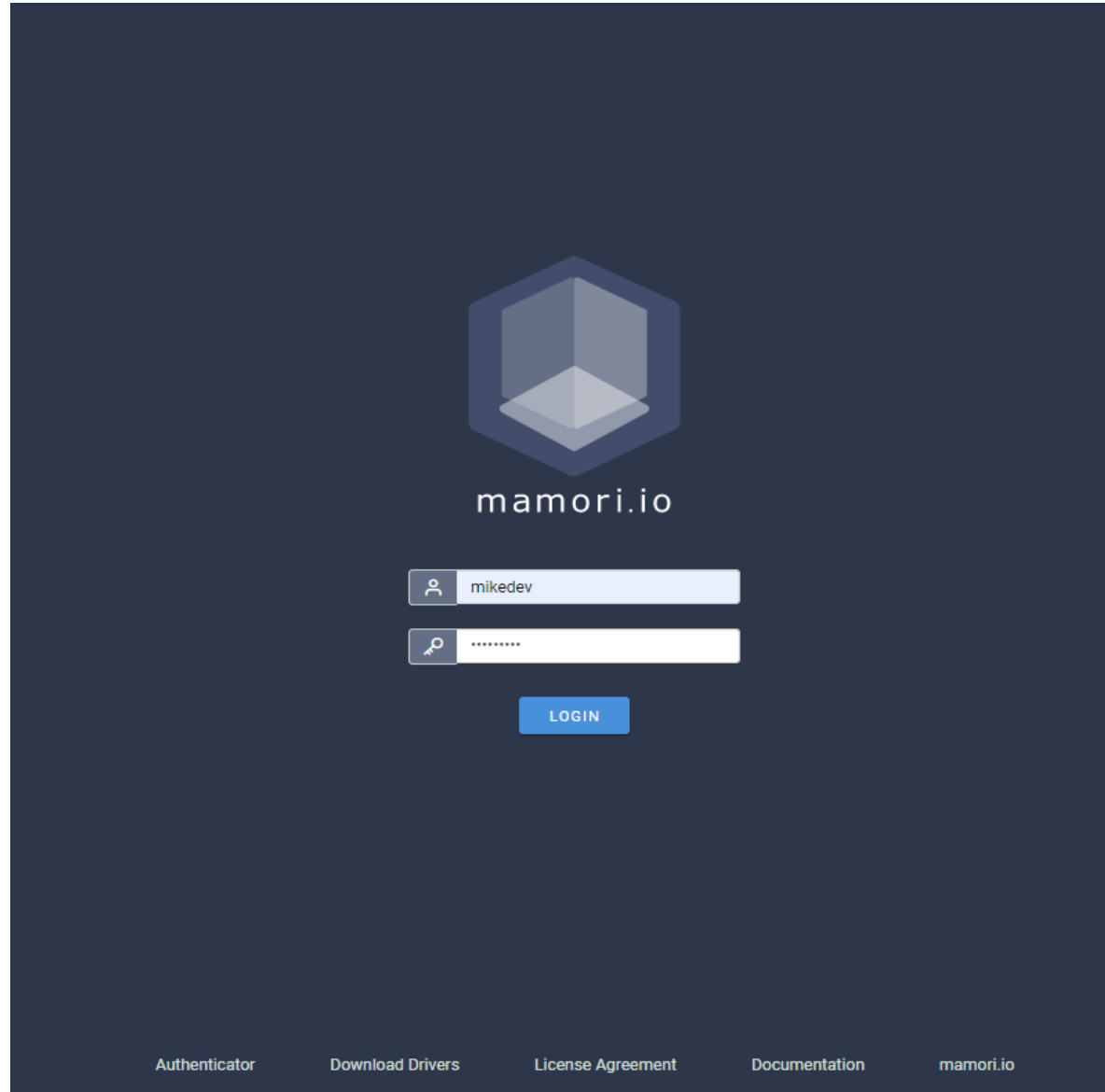
Login to [https://\[your.mamori.server\]/](https://[your.mamori.server]/)
with your provided credentials

WireGuard Setup

Portal Login

Step 1/7

- 1. Login with your credentials**
2. Scan 2FA QR Code
3. Login & 2FA
4. Copy WireGuard client details
5. Start WireGuard & add empty tunnel
6. Paste in details
7. Activate WireGuard



The screenshot shows the login page for mamori.io. At the top center is the mamori.io logo, a stylized hexagon with a 3D effect. Below the logo is the text "mamori.io". There are two input fields: the first is for the username, containing "mikedev", and the second is for the password, containing ".....". Below the password field is a blue "LOGIN" button. At the bottom of the page, there are five links: "Authenticator", "Download Drivers", "License Agreement", "Documentation", and "mamori.io".



Scan the displayed QRCode with the mamori mobile app

WireGuard Setup

Portal Login

Step 2/7

1. Login with your credentials
- 2. Scan 2FA QR Code**
3. Login & 2FA
4. Record WireGuard client details
5. Start WireGuard & add empty tunnel
6. Paste in details
7. Activate WireGuard


mamori.io


This code will only be shown once.
Please make sure you scan it with your authenticator app on your phone.

Once you have scanned the code above with your authenticator app, click [here](#) to log in to Mamori.

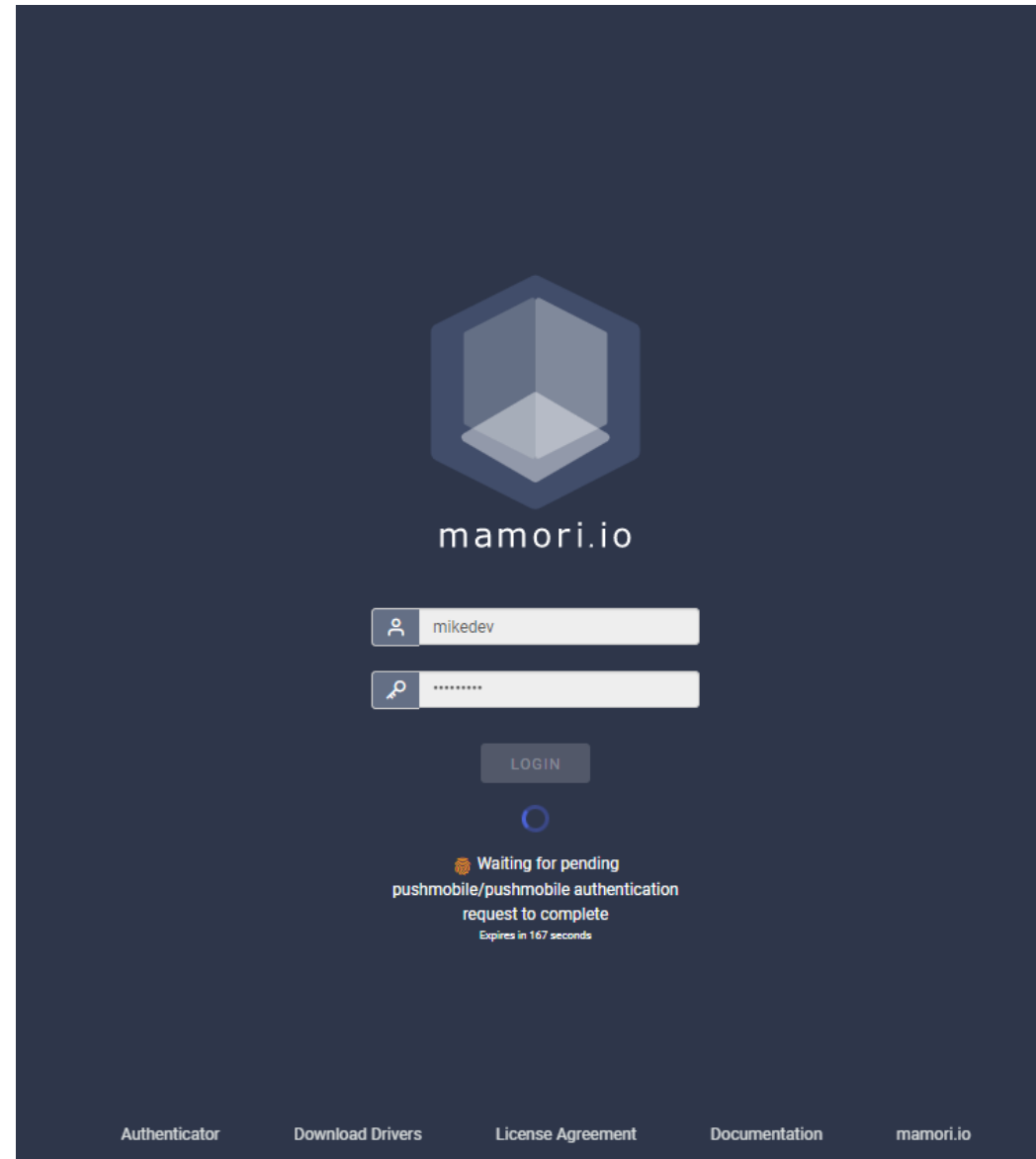
Login to [https://\[your.mamori.server\]/](https://[your.mamori.server]/) again with your credentials and click **Accept** on the mobile app

WireGuard Setup

Portal Login

Step 3/7

1. Login with your credentials
2. Scan 2FA QR Code
- 3. Login & 2FA**
4. Record WireGuard client details
5. Start WireGuard & add empty tunnel
6. Paste in details
7. Activate WireGuard



mamori.io

mikedev

LOGIN

Waiting for pending
pushmobile/pushmobile authentication
request to complete
Expires in 167 seconds

Authenticator Download Drivers License Agreement Documentation mamori.io

Copy the config and add it to your WireGuard desktop client.

NEW WIREGUARD PEER DETAILS

A default wireguard peer has been created for you on your first login to Mamori.

! This configuration information will only be shown once.

Paste the following into your Wireguard client

```
[Interface]
PrivateKey = QPFwDAaBBTbFQpBWnsjiOk+GexwPLkIgsr17/pis+XE=
Address = 10.11.0.58

[Peer]
PublicKey = PSCXKnsT5ssYfnYSyVoKzrEFs3WPc5MLPUDXrGY+9FE=
AllowedIPs = 10.11.0.1/32,10.0.0.0/24
Endpoint = test.mamori.io:51871
```

or scan the QR code with you mobile device



i An email has been sent with the information above. Please check your inbox

WireGuard Setup

Portal Login

Step 4/7

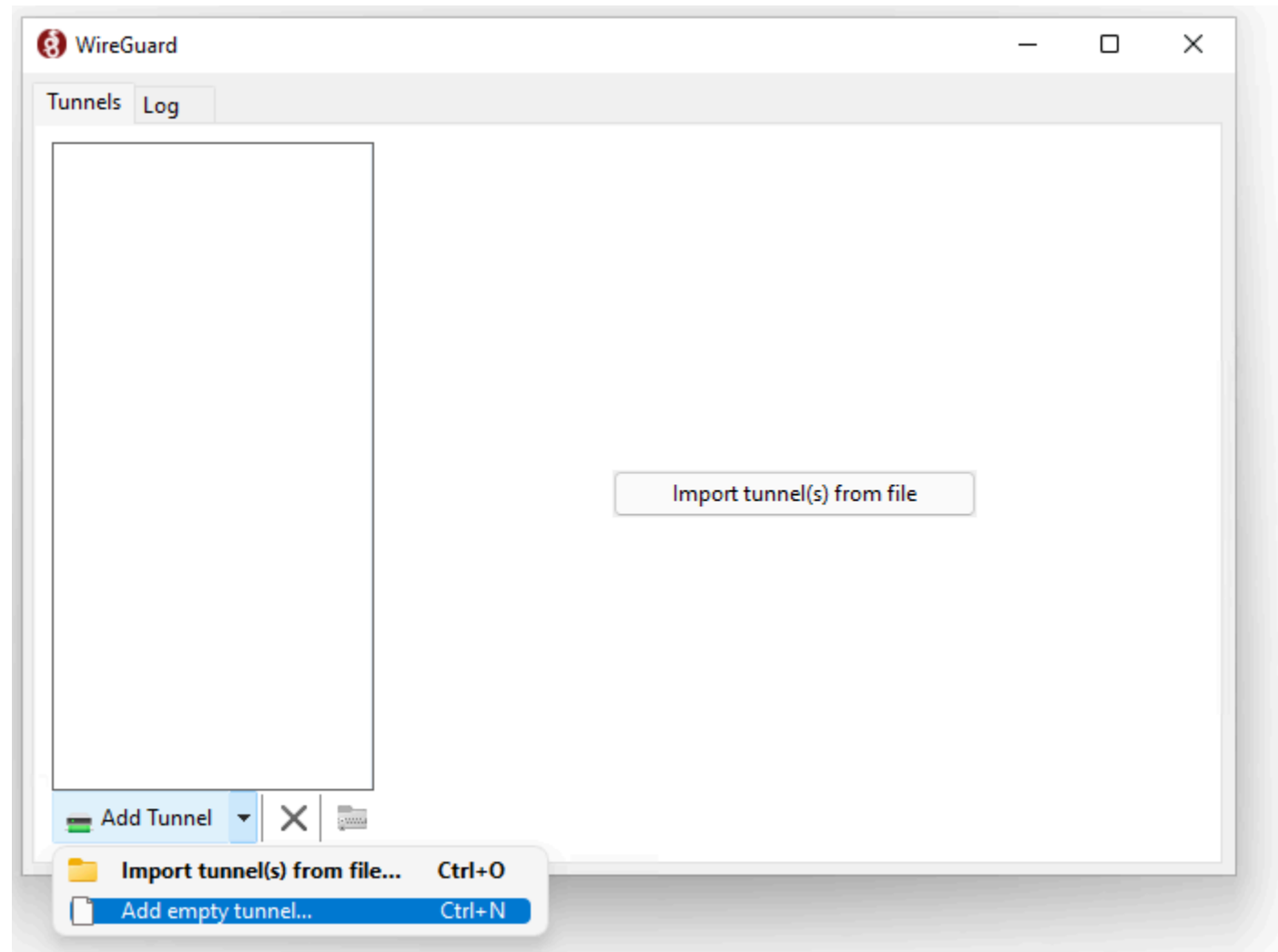
1. Login with your credentials
2. Scan 2FA QR Code
3. Login & 2FA
- 4. Record WireGuard client details**
5. Start WireGuard & add empty tunnel
6. Paste in details
7. Activate WireGuard

Start WireGuard client & add empty tunnel

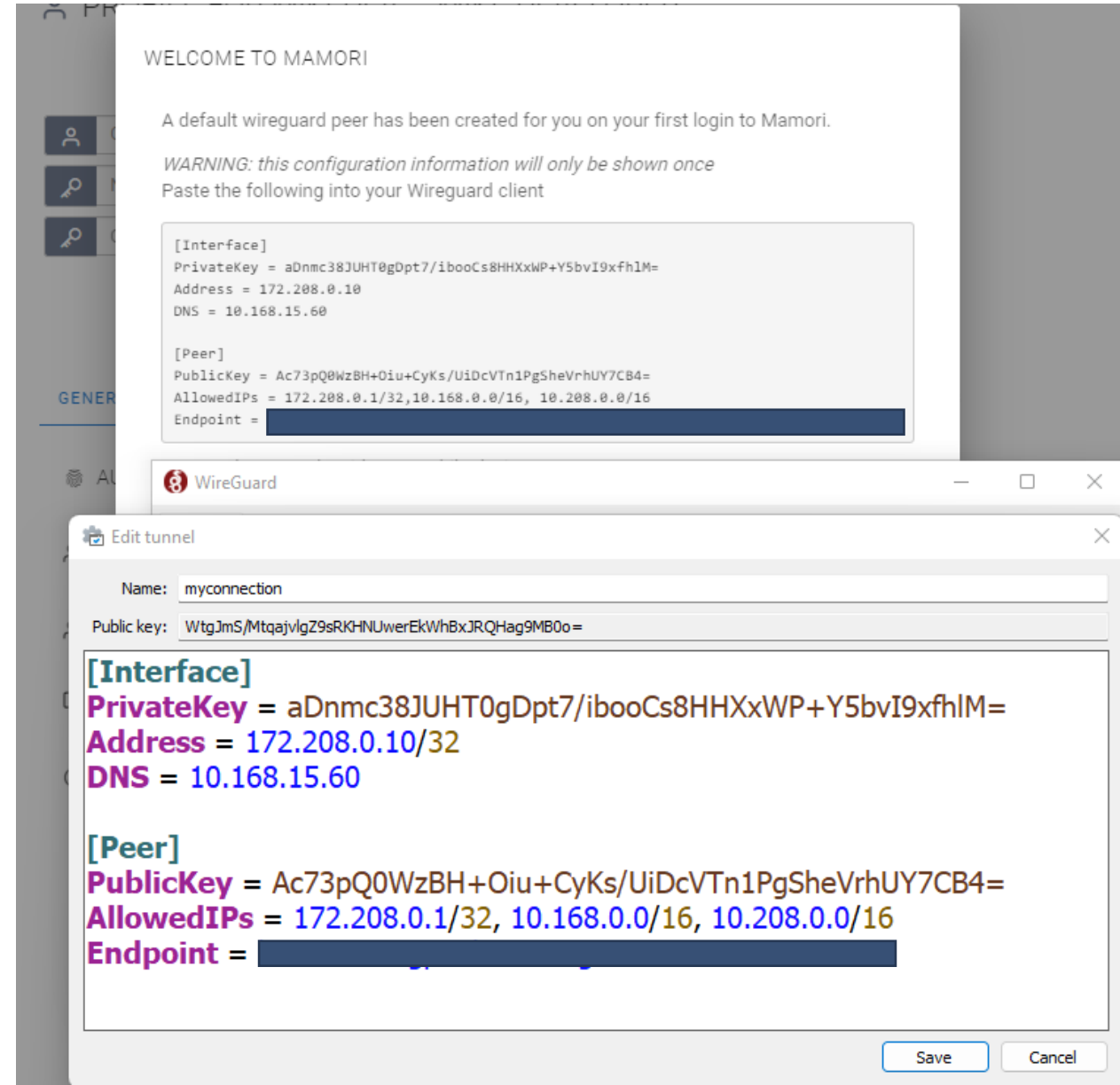
WireGuard Setup Client Setup

Step 5/7

1. Login with your credentials
2. Scan 2FA QR Code
3. Login & 2FA
4. Record WireGuard client details
- 5. Start WireGuard & add empty tunnel**
6. Paste in details
7. Activate WireGuard



Paste details & click save



The screenshot shows the Mamori web interface with a 'WELCOME TO MAMORI' message. A warning states: 'WARNING: this configuration information will only be shown once. Paste the following into your Wireguard client'. Below this is a code block containing the configuration details. In the foreground, the WireGuard application window is open, showing the 'Edit tunnel' dialog. The 'Name' field is 'myconnection' and the 'Public key' field contains 'WtgJmS/MtqajvlgZ9sRKHNUwerEkWhBxJRQHag9MB0o='. The configuration details from the web interface are pasted into the 'Edit tunnel' dialog, with the following text:

```
[Interface]
PrivateKey = aDnmc38JUHT0gDpt7/ibooCs8HHXxWP+Y5bvI9xfhIM=
Address = 172.208.0.10/32
DNS = 10.168.15.60

[Peer]
PublicKey = Ac73pQ0WzBH+Oiu+CyKs/UiDcVTn1PgSheVrhUY7CB4=
AllowedIPs = 172.208.0.1/32, 10.168.0.0/16, 10.208.0.0/16
Endpoint = [REDACTED]
```

The 'Edit tunnel' dialog has 'Save' and 'Cancel' buttons at the bottom right.

WireGuard Setup Client Setup

Step 6/7

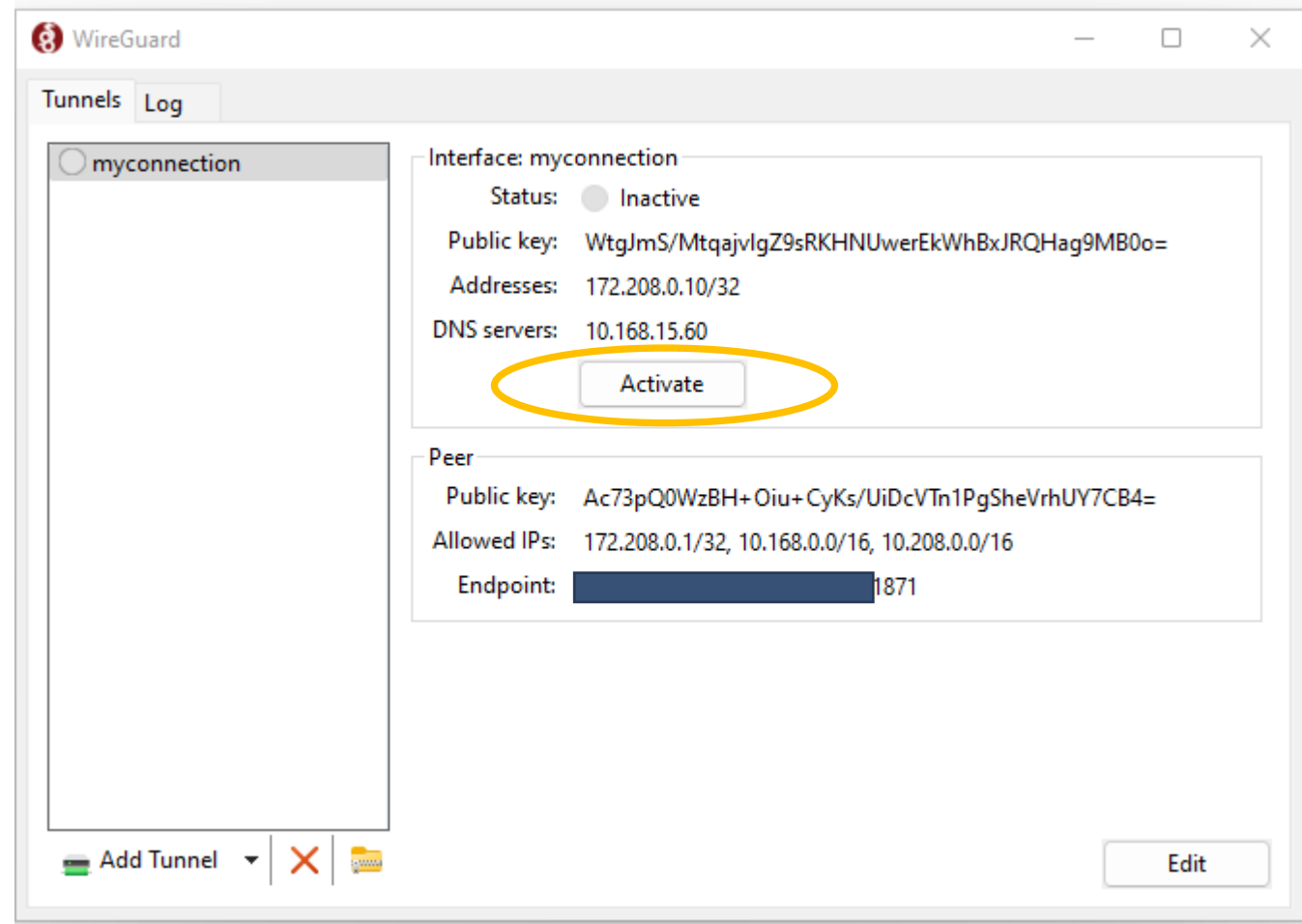
1. Login with your credentials
2. Scan 2FA QR Code
3. Login & 2FA
4. Record WireGuard client details
5. Start WireGuard & add empty tunnel
- 6. Paste in details**
7. Activate WireGuard

Activate Connection

WireGuard Setup Client Setup

Step 7/7

1. Login with your credentials
2. Scan 2FA QR Code
3. Login & 2FA
4. Record WireGuard client details
5. Start WireGuard & add empty tunnel
6. Paste in details
7. **Activate WireGuard**



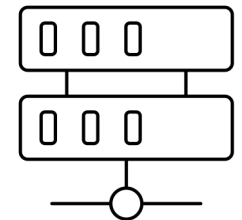
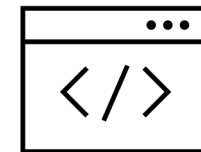
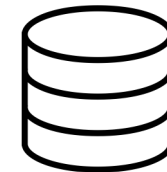
WireGuard Setup

Done

Your 2FA and WireGuard client setup is complete.

Access resources like you normally do. The only difference is that you will be multi-factored on resource access.

Web browser
Developer IDE
SQL tool
SSH tool
RDP tool
Terminal
etc..



Access Resources