# X-UI, a multi-user Xray graphical management panel (replacing V2-UI and V2Ray)

📅 2021-10-10

X-UI provides a graphical user interface for managing servers and users. You can visually build servers for Shadowsocks, V2ray, Xray, Trojan, and other popular protocols. You can also monitor VPS performance and traffic usage in real time. X-UI replaces the older V2-UI panel.

## Preparation

Before you begin, you need to do three or four things:

1. Get a virtual private server or VPS. You can get a VPS from many providers. Some popular ones are AWS, Google Cloud, Microsoft Azure, DigitalOcean, Hetzner, and Vultr. In our example we use a Debian 11 VPS, but the X-UI install script supports Ubuntu 16+, Debian 8+, or CentOS 7+. You need to have ports 80 and 443 on your VPS open for TCP input. Also open port 54321 for TCP input.
2. Get a domain name. Some low-cost registrars are Porkbun, Namesilo, and Namecheap.
3. Create a DNS `A` record pointing from your host name to your VPS.
4. Optionally, add your domain to Cloudflare. This will allow you to insert a content distribution network or CDN in between you and your server. However, if you are going to add a CDN, do not turn on proxying in Cloudflare until the end. For now, just use the DNS features of Cloudflare. Adding your domain to Cloudflare is optional, and you can continue to use your domain name registrar's nameservers if you prefer. In any case, not all protocols support the use of CDN proxying.

## Update Server

SSH into your server. On Windows you can use the built-in PowerShell app, or you can install a terminal emulator such as PuTTY or XSHELL.
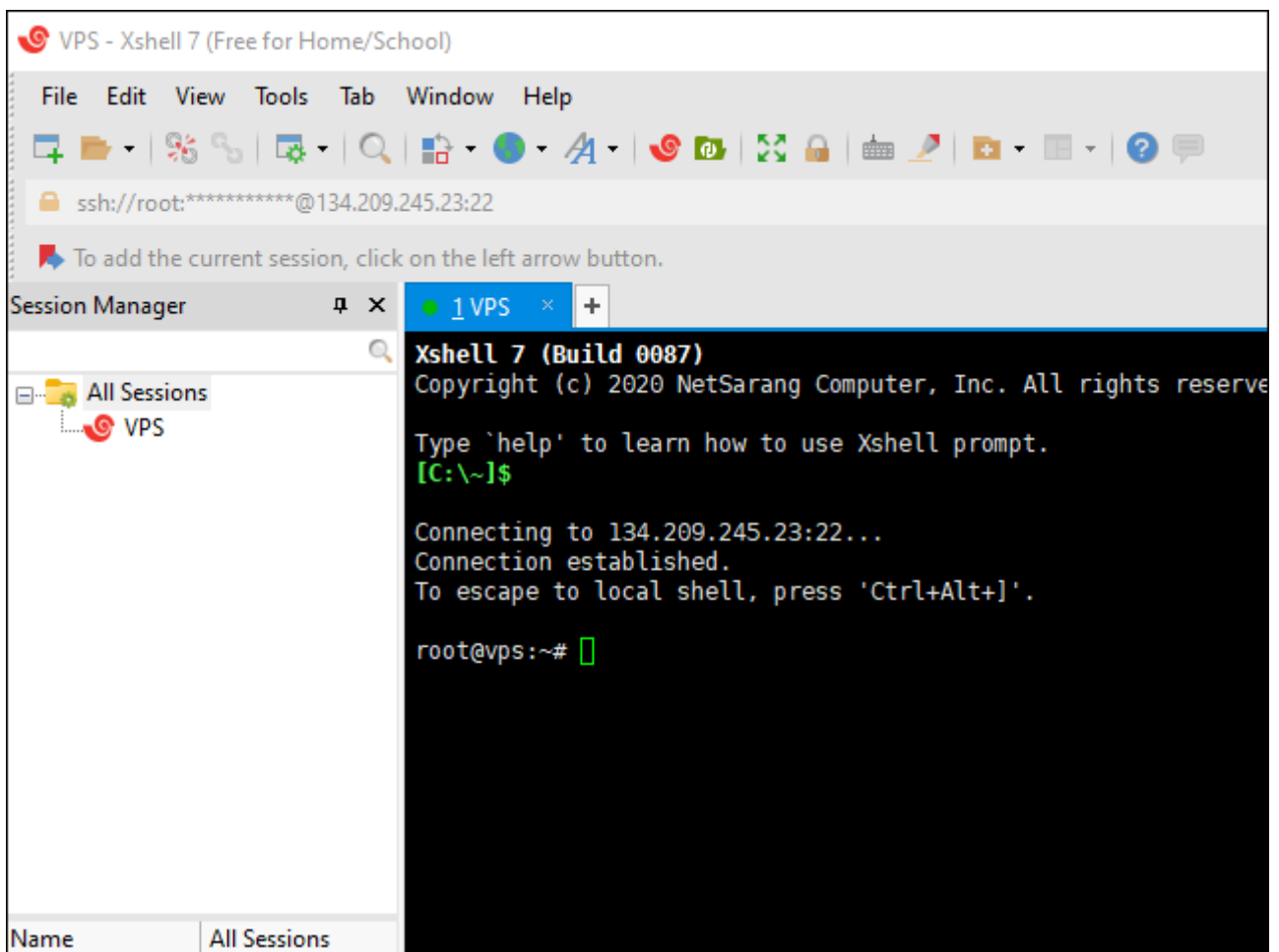


Get your server up to date:

```
1   apt update && apt upgrade -y
```

Also install `curl` and `socat`:

```
1   apt install curl socat -y
```

## Install Acme Script

Download and install the Acme script for getting a free SSL certificate:

```
1   curl https://get.acme.sh | sh
```

## Get Free SSL Certificate

Set the default provider to Let's Encrypt:

```
1   ~/.acme.sh/acme.sh --set-default-ca --server letsencrypt
```

Register your account for a free SSL certificate. In the next command, replace `xxxx@xxxx.com` by your actual email address:

```
1   ~/.acme.sh/acme.sh --register-account -m xxxx@xxxx.com
```

Obtain an SSL certificate. In the next command, replace `host.mydomain.com` by your actual host name:

```
1   ~/.acme.sh/acme.sh --issue -d host.mydomain.com --standalone
```

After a minute or so, the script terminates. On success, you will receive feedback as to the location of the certificate and key:

```
1   Your cert is in: /root/.acme.sh/host.mydomain.com/host.mydomain.com.cer
2   Your cert key is in: /root/.acme.sh/host.mydomain.com/host.mydomain.com.key
3   The intermediate CA cert is in: /root/.acme.sh/host.mydomain.com/ca.cer
4   And the full chain certs is there: /root/.acme.sh/host.mydomain.com/fullchai
```

You cannot use the certificate and key in their current locations, as these may be temporary. Therefore install the certificate and key to a permanent location. In the next command, replace `host.mydomain.com` by your actual host name:

```
1   ~/.acme.sh/acme.sh --installcert -d host.mydomain.com --key-file /root/priva
```

```
Ly9yMy5vLmxlbmNyLm9yZzZAiBggrBgEFBQcwAoYWaHR0cDovL3IzLmkubGVuY3Iu
b3JnLzAcBgNVHREEFTATghF2cHMubXlleGFtcGxlLnh5ejBMBgNVHSAERTBDMAgG
BmeBDAECATA3BgsrBgEEAYLfEwEBATAoMCYGCCsGAQUFBwIBFhpodHRw0i8vY3Bz
LmxldHNlbmNyeXB0Lm9yZzCCAQUGCisGAQQBlnkCBAIEgfYEgfMA8QB2AN+lXqto
gk8fbK3uuF90PlrqzaISpGpejjsSwCBEXCpzAAABfGe+F9EAAAQDAEcwRQIhAIW+
1DN3/Ccgmj+lx2geynHUsfQNR/aWl4EDWTKchKnDAiB7RykHKEkNzbA/Wb5T44Si
ceR2ZSc8tZg5F0eH0Gd07wB3AEalVetl+pEgMLWiiWn0830RLEF0vvlJuIWr8vxw
/m1HAAABfGe+F/oAAAQDAEgwRgIhAIWLbu2jRfcTUwf2qqV72IvP5sYSHDX0RWha
lv8bKrvfAiEAvX0q+K6k/8cid+TyBqgHaq53MBufolaY/yy4Xezdo3IwDQYJKoZI
hvcNAQELBQADggEBAG4Bp7vGN5KcBvTyT3sGHIZMEbW/AimCvgD0Ckwgsdq3XcCG
cvtPnJnsGoUHTiCUn61kEJGKqRWyLxnkWDmtxk/p+ia210yJBtPaUGXjWfRtBBdv
nGRFSBGTDLVuX5NJeWelJCu5PrDz/p3HZ8XDSGT2+v8Lu2+SJ90r0I2MBS8Aiwvk
3VnBBSQtSACGhlFVGkvR5YhpnuCORXvaCXb9vwhTCjl+n3TvMedqD7DB4I+xRKBA
zVlczl2LkQ0twHEd9lhinGETbrMseqURYq3B164yoXdcEfcSs9RzjEqofglF52VE
FT0mTVXdlLpxvoL4WKMcoVlgttWPJtT8Nkd+XTQ=
-----END CERTIFICATE-----
```
```
[Sun Oct 10 01:08:04 UTC 2021] Your cert is in: /root/.acme.sh/vps.myexample.xyz/vps.myexam
er
[Sun Oct 10 01:08:04 UTC 2021] Your cert key is in: /root/.acme.sh/vps.myexample.xyz/vps.my
yz.key
[Sun Oct 10 01:08:04 UTC 2021] The intermediate CA cert is in: /root/.acme.sh/vps.myexample
er
[Sun Oct 10 01:08:04 UTC 2021] And the full chain certs is there: /root/.acme.sh/vps.myexam
ullchain.cer
root@vps:~# ~/.acme.sh/acme.sh --installcert -d vps.myexample.xyz --key-file /root/private.
lchain-file /root/cert.crt
[Sun Oct 10 01:13:08 UTC 2021] Installing key to: /root/private.key
[Sun Oct 10 01:13:08 UTC 2021] Installing full chain to: /root/cert.crt
root@vps:~# ls
cert.crt  private.key
root@vps:~#
```

## Run the X-UI Install Script

Download and run the one-click install script provided by the developer:

```
1   bash <(curl -Ls https://raw.githubusercontent.com/vaxilu/x-ui/master/install
```

## Common Panel Commands

From the command line, you can control the server with various commands:

| Command | Effect |
| --- | --- |
| x-ui | Display the management menu |
| x-ui start | Start the X-UI panel |
| x-ui stop | Stop the X-UI panel |
| x-ui restart | Restart the X-UI panel |

| Command | Effect |
| --- | --- |
| `x-ui status` | View X-UI status |
| `x-ui enable` | Set X-UI to start automatically after boot |
| `x-ui disable` | Cancel X-UI boot from start |
| `x-ui log` | View X-UI log |
| `x-ui update` | Update the X-UI panel |
| `x-ui install` | Install X-UI panel |
| `x-ui uninstall` | Uninstall X-UI panel |

## First Time Login

You can get to the X-UI panel on your PC by opening a browser and typing your server IP address and port `54321`. For example:

```
1   http://123.45.67.89:54321
```

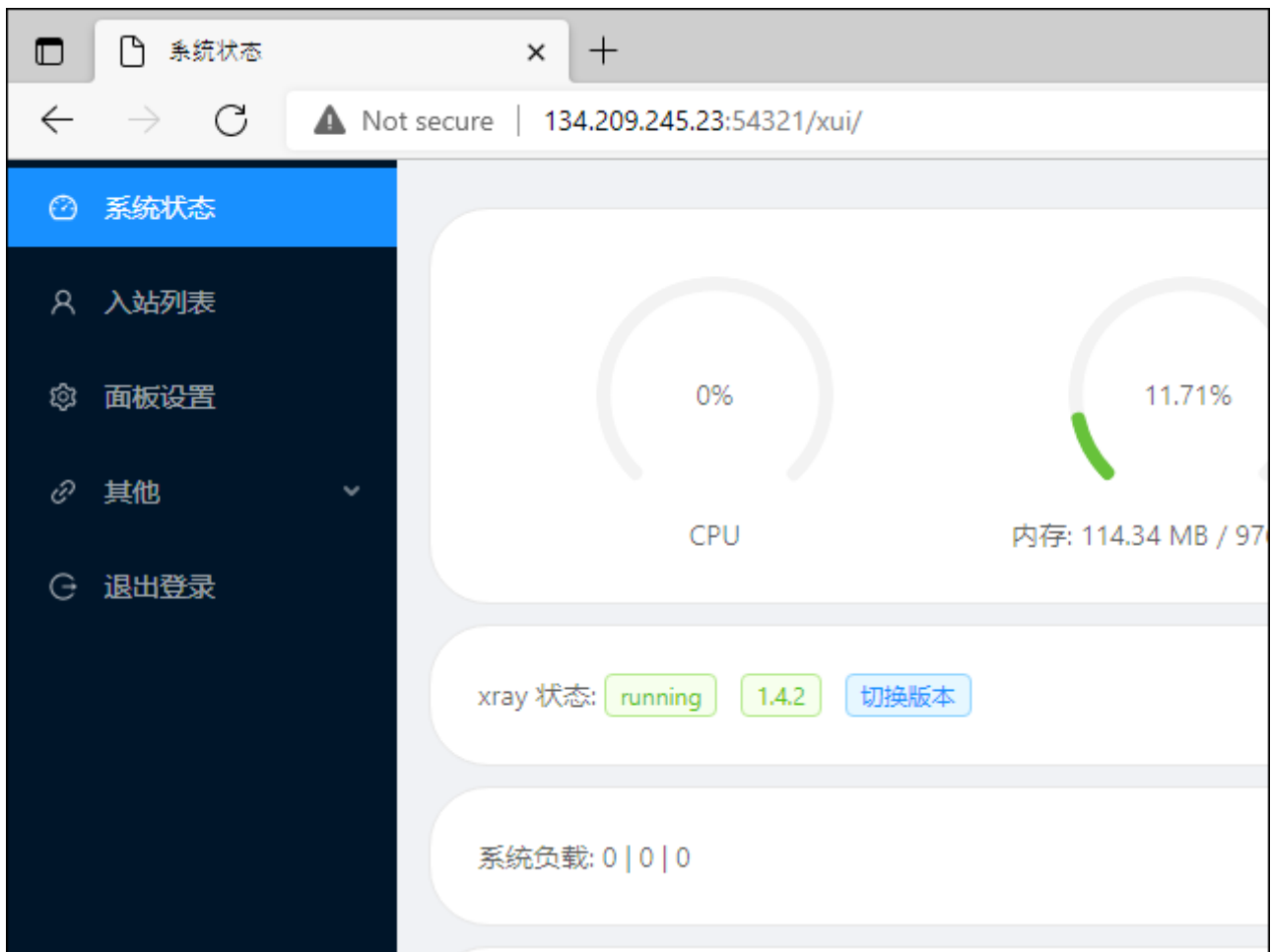By default, the login user name is `admin`, and the password is also `admin`.

## Side Menu

After you have logged in, the side menu offers these options:

| Chinese | English |
| --- | --- |
| 系统状态 | System status |
| 入站列表 | Inbound list |
| 面板设置 | Panel settings |
| 其他 | Other |
| 退出登录 | Sign out |

## Enable HTTPS on Panel

You will notice that, at first, you used plain text HTTP to reach the panel. This is not secure.

To enable HTTPS, choose 面板设置 (Panel settings).

You will need to specify your certificate and key.

```
1    面板证书公钥文件路径
2    填写一个 '/' 开头的绝对路径，重启面板生效
3    Panel certificate public key file path
4    Fill in an absolute path starting with'/', restart the panel to take effect
```

Fill in `/root/cert.crt` .

```
1    面板证书密钥文件路径
2    填写一个 '/' 开头的绝对路径，重启面板生效
3    Panel certificate key file path
     Fill in an absolute path starting with'/', restart the panel to take effect
```
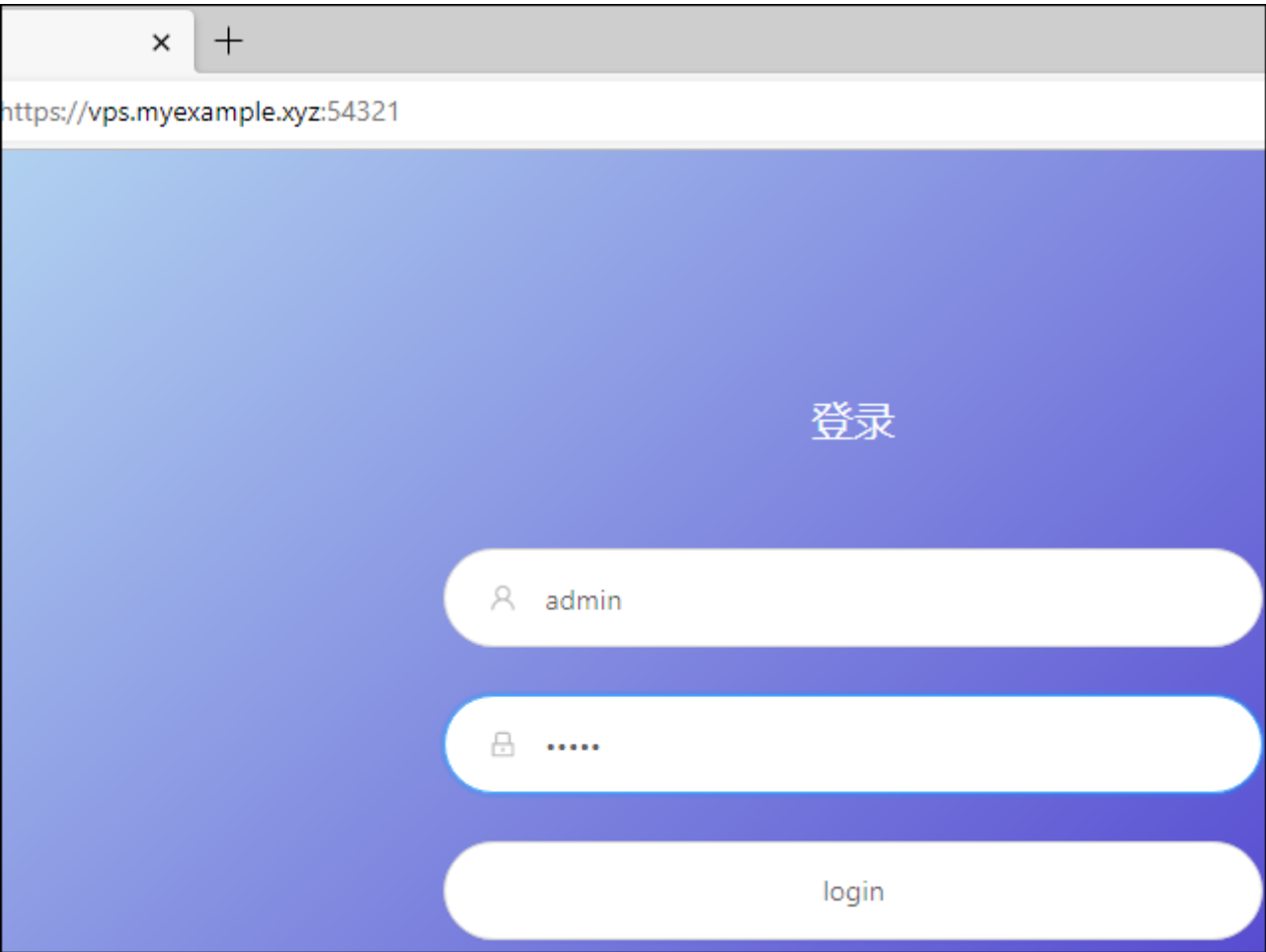
Fill in `/root/private.key` .



Save these options.

Now in your SSH session issue the command:

```
1   x-ui restart
```

Now you can reach the panel using HTTPS. For example:

```
1   https://host.mydomain.com:54321
```

## Change Admin Password

The default admin user name `admin` and password `admin` are the same for all installations. This is not secure. Input the old values of `admin` and `admin`, and choose new, unique values:

| Chinese | English |
| --- | --- |
| 原用户名 | Original user name |
| 原密码 | Old password |
| 新用户名 | New user name |
| 新密码 | New password |

面板配置　　　　用户设置　　　　xray 相关设置　　　　其他设置

原用户名：

admin

原密码：

•••••

新用户名：

neddie

新密码：

••••••••

Save the new values.

Sign out, then sign in again with the new user name and password.

## Add VLESS+XTLS Xray User

We are going to add an inbound user account using VLESS and Xray. VLESS is an an updated version of the older Vmess protocol. After several developers found flaws in Vmess protocol and showed that the Vmess protocol can be detected by deep packet inspection or DPI, VLESS was developed. (Note that it is plain Vmess that can be detected; Vmess+WS+TLS is still secure and supports the use of a CDN.) Xray core was developed as an alternative to the older V2Ray core. According to the Xray developers, Xray is more stable, better for UDP gaming, and 30% faster than V2Ray. XTLS speeds up TLS by reducing double-encryption.

On the side menu, select 入站列表 (Inbound list).

Click the plus sign to add a new inbound user.

The 添加入站 (Add inbound) box appears.

Enter fields as follows.

| Field | Contents |
| --- | --- |
| Remark | Put a unique and meaningful description |
| Enable | On |
| Protocol | `vless` |
| 监听 IP Listening IP | Leave blank |
| 端口 Port | `443` |
| 总流量(GB) Total bandwidth (GB) | `0` means unlimited |
| 到期时间 Expiry date | Blank |
| Id | Leave the generated UUID as is |
| Flow | `xtls-rprx-direct` |
| Fallbacks | None |
| 传输 Transmission | `tcp` |
| HTTP 伪装 masquerading | Off |
| TLS | Off |
| XTLS | On |
| 域名 Domain name | Put your host name, e.g. `host.mydomain.com` |
| 公钥文件路径 Public key file path | `/root/cert.crt` |
| 密钥文件路径 Key file path | `/root/private.key` |
| Sniffing | On |

添加入站

| remark: | VPS | | enable: | ⬤ |

protocol: vless ⌄

监听 IP ❓:

端口: 443        总流量(GB) ❓: 0

到期时间 ❓: Select date 📅

id: 20a79f0e-0123-4512-873ε        flow: xtls-rprx-direct ⌄

fallbacks: ＋

传输: tcp ⌄

http 伪装: ◯

tls: ◯        xtls: ⬤

域名: vps.myexample.xyz

证书: [ certificate file path ]  [ certificate file content ]

公钥文件路径: /root/cert.crt

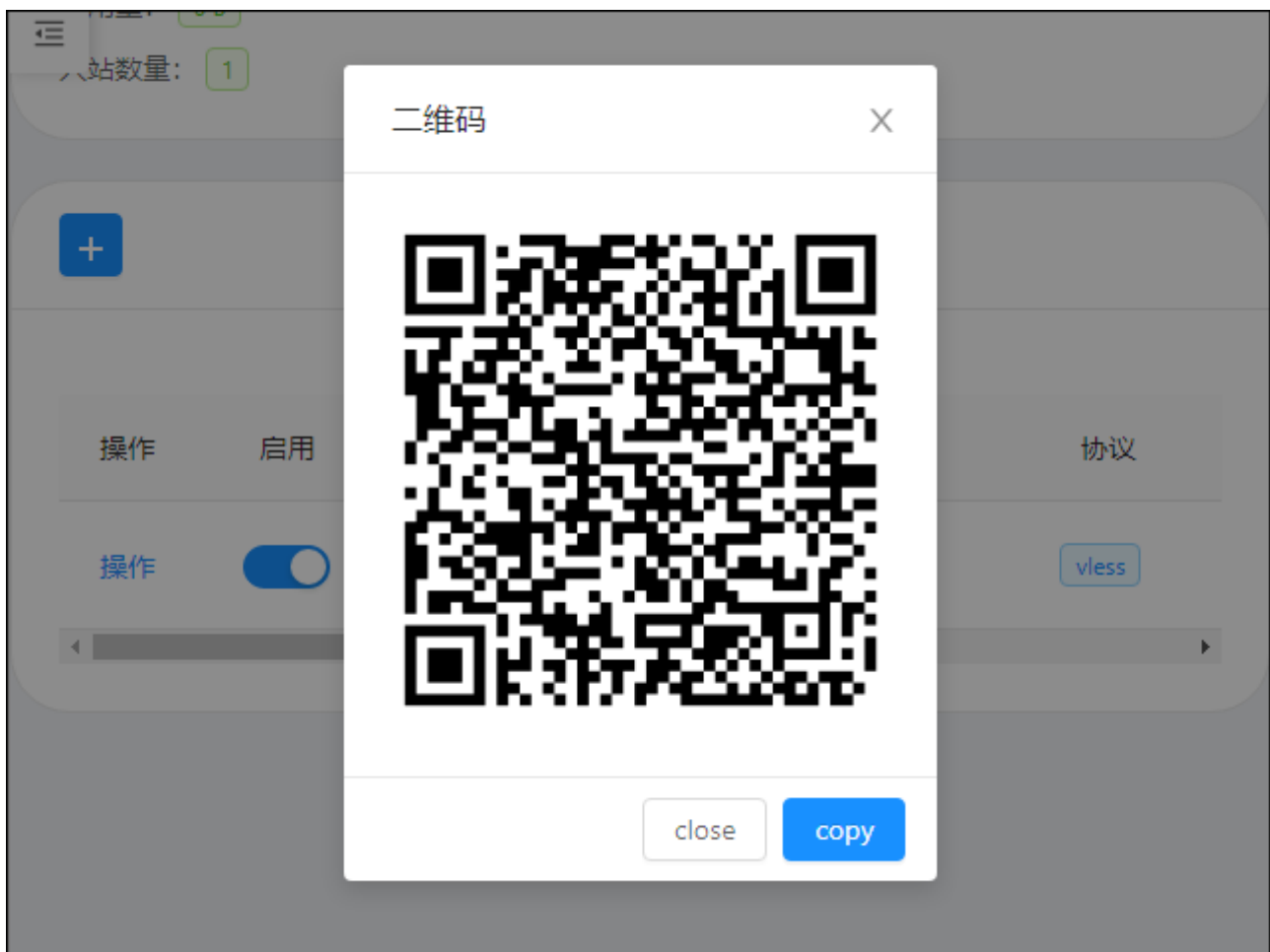密钥文件路径: /root/private.key

sniffing ❓: ⬤

[ close ]  [ 添加 ]

Save the new user.

Click the 操作 (operating) button at the start of its row to display the QR code for the new user.

二维码



close copy

## Client

Clients are available for Android, iOS, Windows, macOS, and Linux. Examples are v2rayNG, Shadowrocket, and Qv2ray.

Add the profile in the QR code to your client.

You can check that your connection is working by opening a browser and going to https://whatismyipaddress.com.
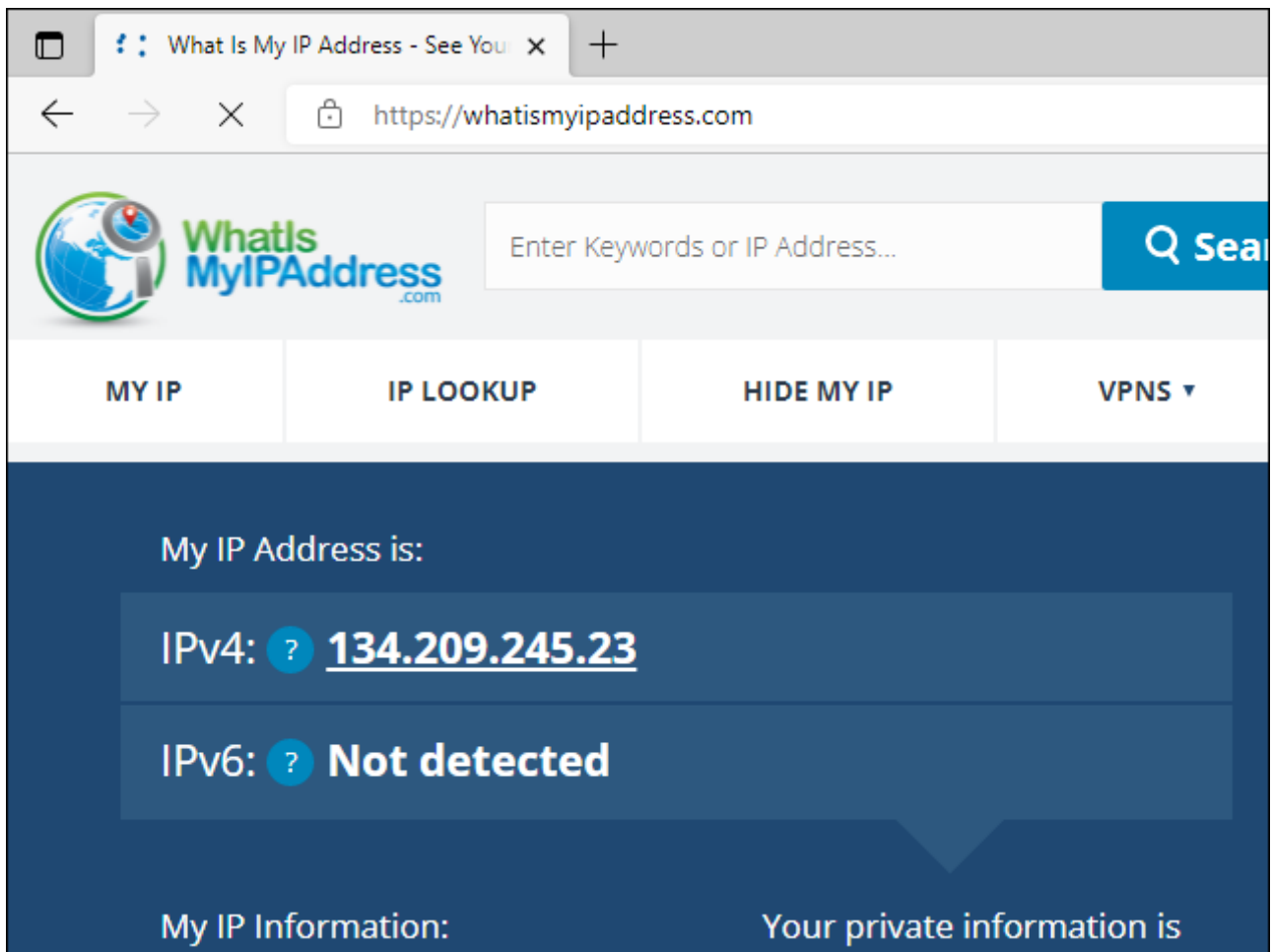
Shadowsocks + V2Ray Plugin with Self-Signed
Certificate

Windows SoftEther VPN Server ›