VPNs in 2024

Ondřej Šika

ondrej@sika.io
@ondrejsika

LinuxDays 2024,
Praha, 12. 10. 2024

Ondřej Šika

I'm a DevOps engineer and consultant from Prague.

I help companies to set up or improve DevOps to deliver easier, faster and more reliable software products.

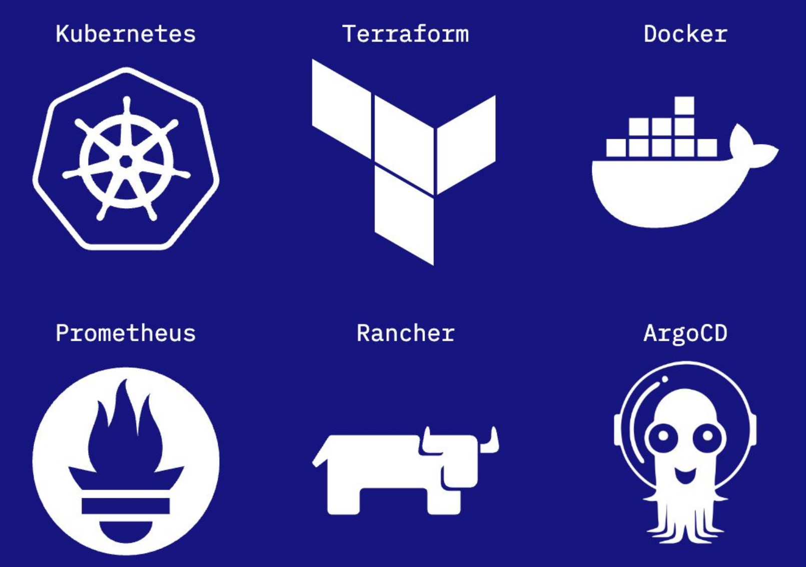
I have also popular DevOps training and DevOps company SikaLabs.

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

My DevOps Training

I have popular training sessions where I share my knowledge in a way that allows you to do everything yourself, without unnecessary mistakes and dead ends.

- Docker
- Kubernetes
- ArgoCD
- Prometheus



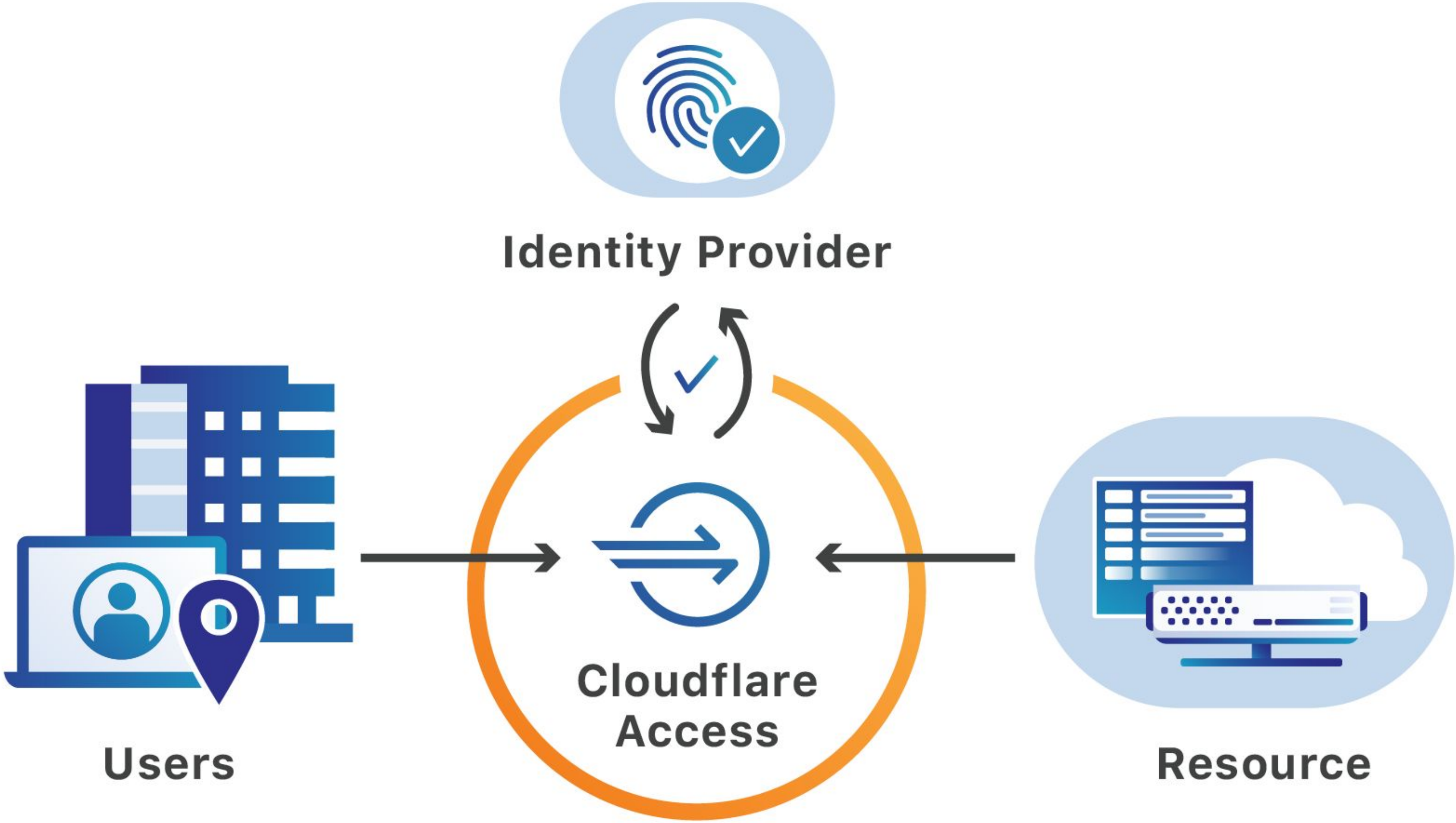
Do you need a VPN? 🤔

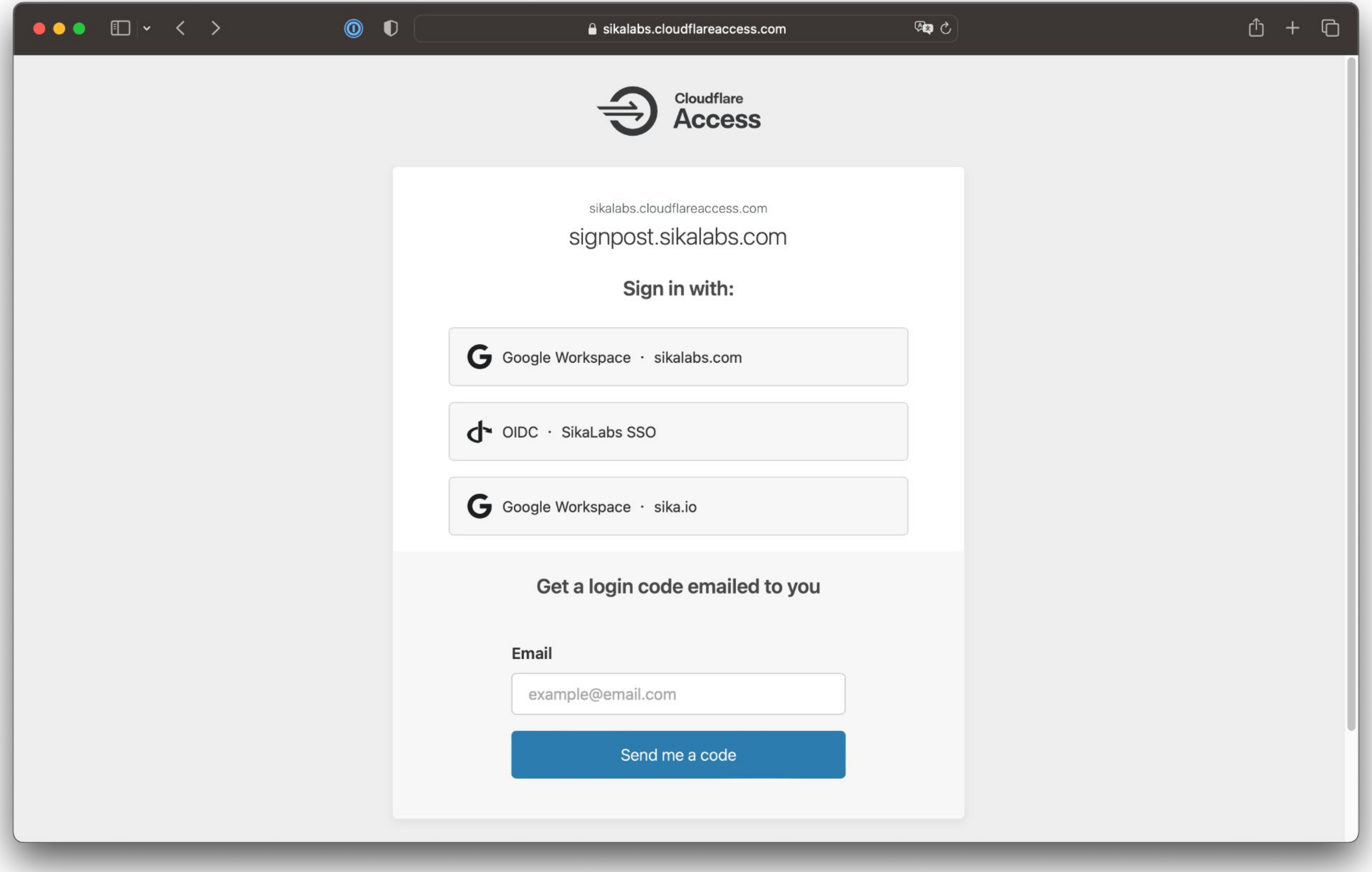
You don't!

CLOUDFLARE®

Cloudflare Access

- Secure VPN alternative
- Identity based Cloudflare Proxy
- Zero trust model
- Identity based authentication
  - OIDC (Okta, Keycloak)
  - Google, Microsoft
  - Email


Identity Provider
Users
Cloudflare Access
Resource



sikalabs.cloudflareaccess.com

Cloudflare Access

sikalabs.cloudflareaccess.com

signpost.sikalabs.com

Sign in with:

Google Workspace · sikalabs.com

OIDC · SikaLabs SSO

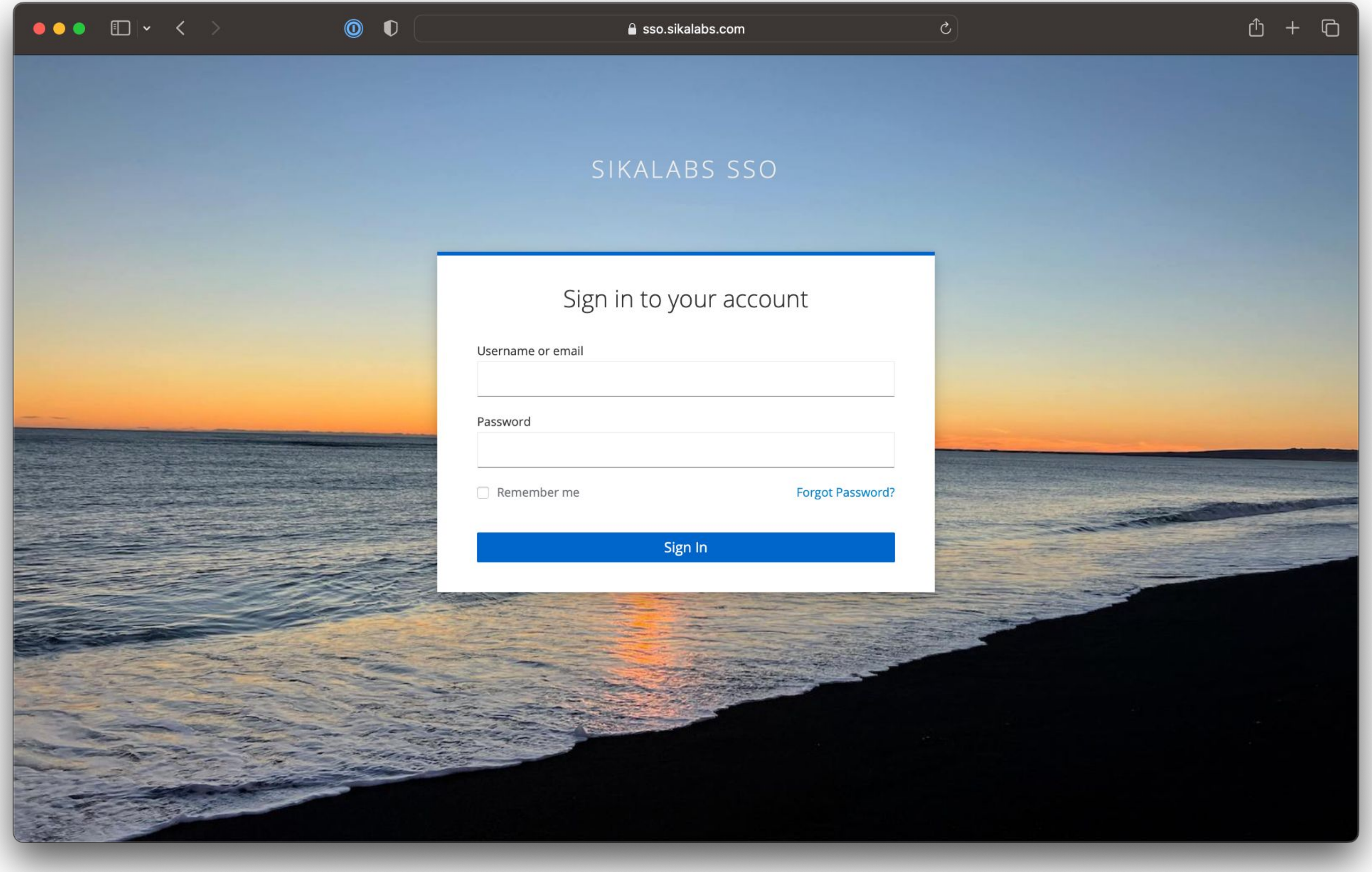
Google Workspace · sika.io

Get a login code emailed to you

Email

example@email.com

Send me a code



SIKALABS SSO

Sign in to your account

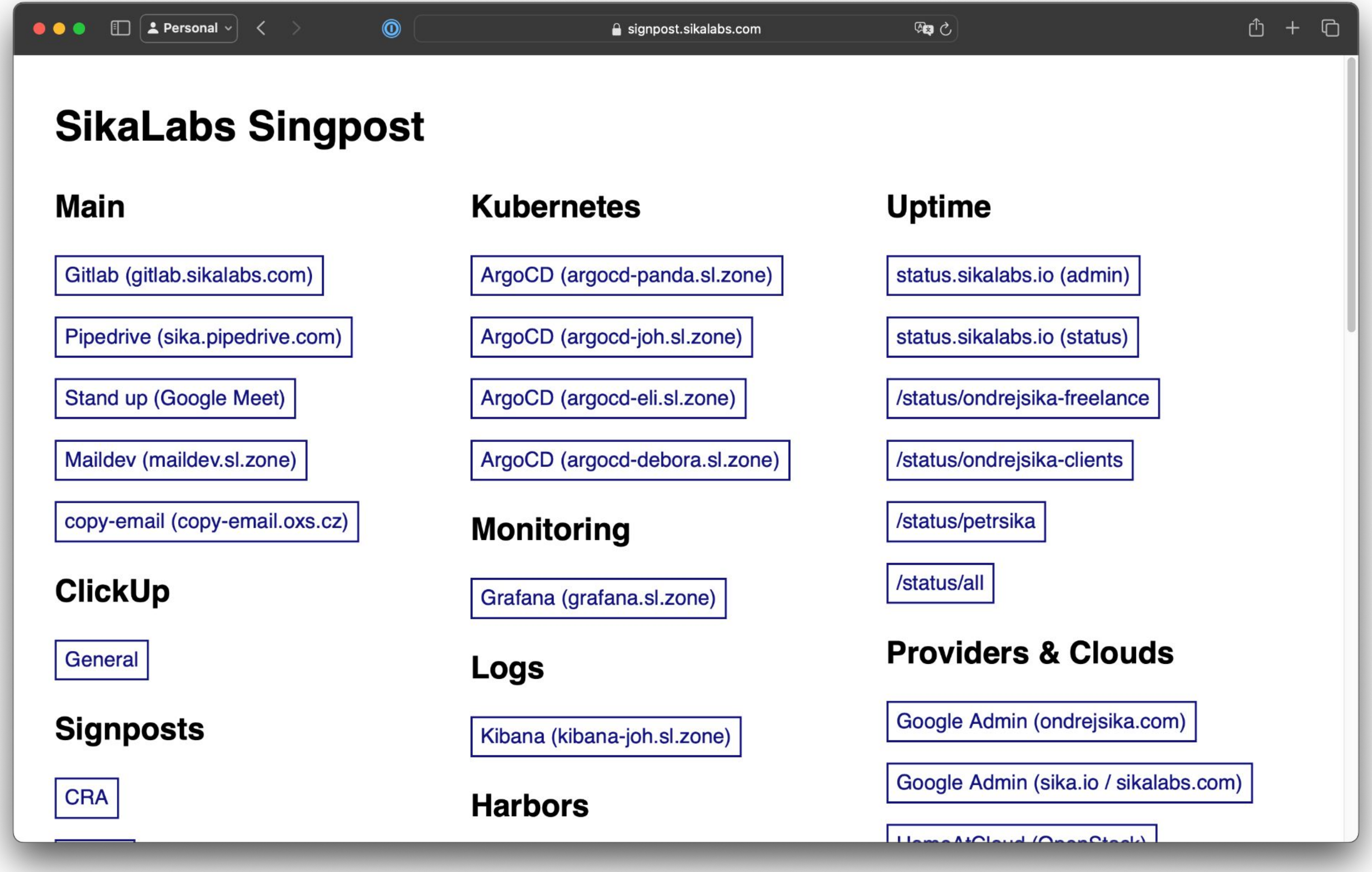
Username or email

Password

□ Remember me

Forgot Password?

Sign In



SikaLabs Singpost

Main

- Gitlab (gitlab.sikalabs.com)
- Pipedrive (sika.pipedrive.com)
- Stand up (Google Meet)
- Maildev (maildev.sl.zone)
- copy-email (copy-email.oxs.cz)

ClickUp

- General

Signposts

- CRA

Kubernetes

- ArgoCD (argocd-panda.sl.zone)
- ArgoCD (argocd-joh.sl.zone)
- ArgoCD (argocd-eli.sl.zone)
- ArgoCD (argocd-debora.sl.zone)

Monitoring

- Grafana (grafana.sl.zone)

Logs

- Kibana (kibana-joh.sl.zone)

Harbors

Uptime

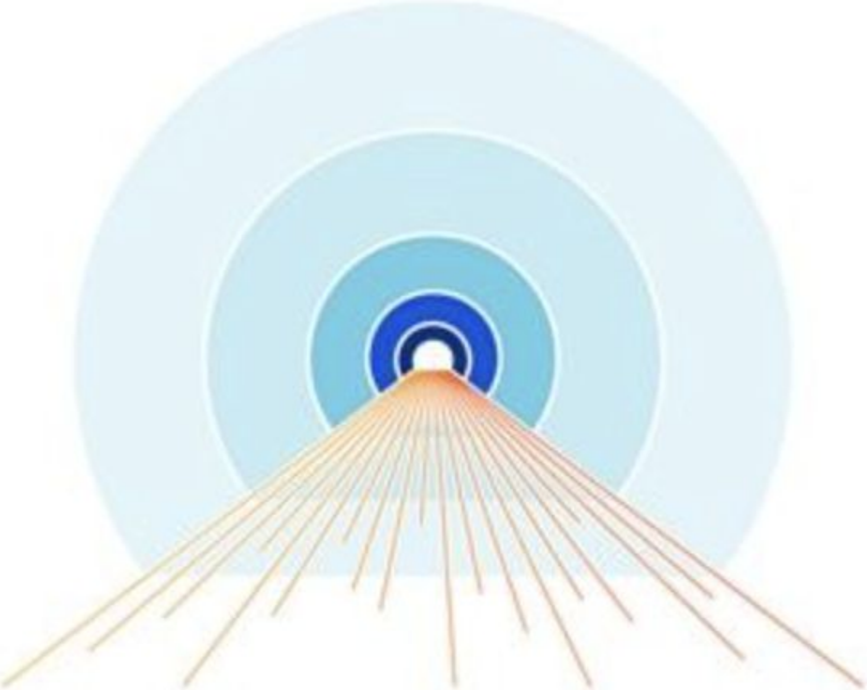
- status.sikalabs.io (admin)
- status.sikalabs.io (status)
- /status/ondrejsika-freelance
- /status/ondrejsika-clients
- /status/petrsika
- /status/all

Providers & Clouds

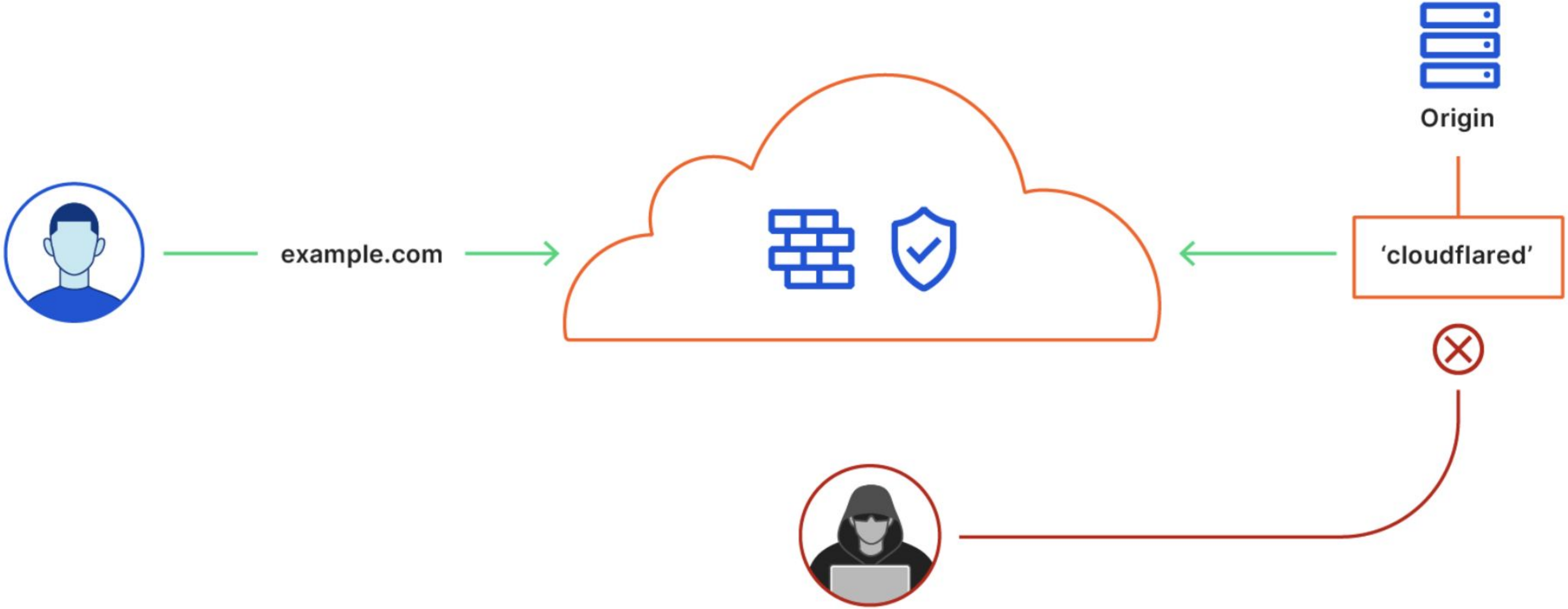
- Google Admin (ondrejsika.com)
- Google Admin (sika.io / sikalabs.com)
- HomeAtCloud (OpenStack)

DEMO TIME 🚀🚀

But I don't have public or static IP ... 😔



Cloudflare Tunnel


example.com
Origin
'cloudflared'

DEMO TIME 🚀🚀

Open Source alternatives?

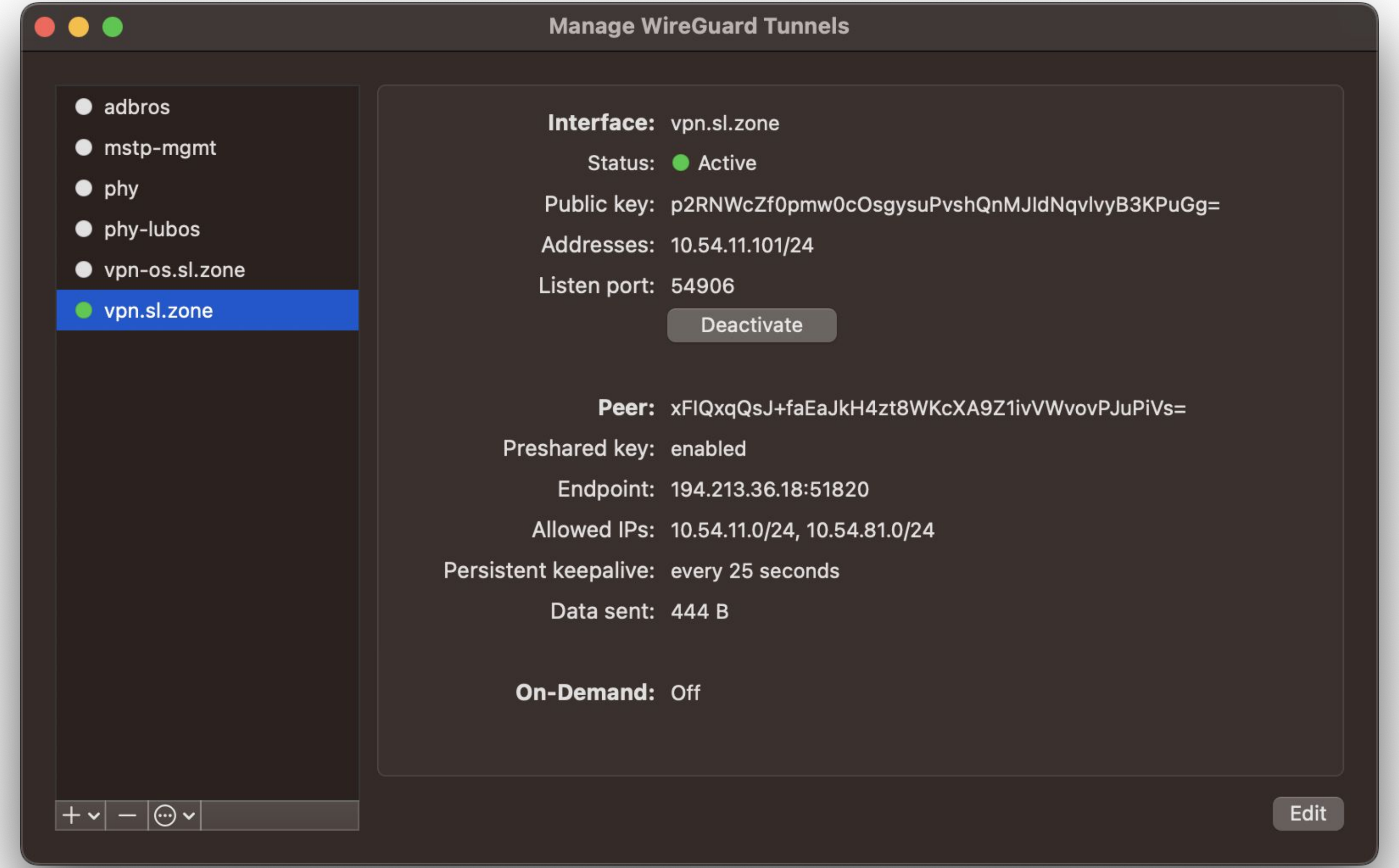
- HashiCorp Boundary
- oidc2-proxy

What if we really need a VPN?

WireGuard

What is WireGuard?

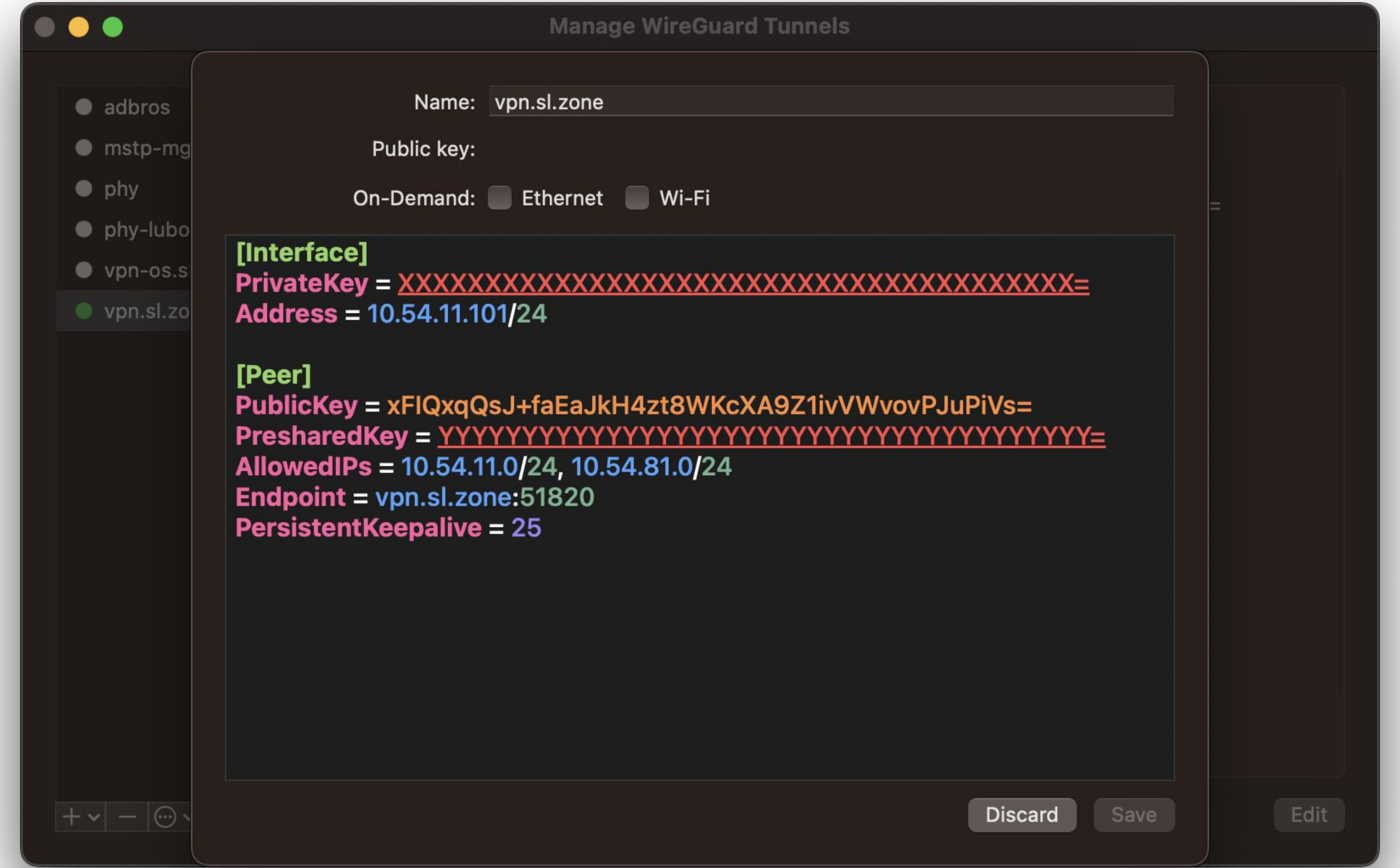
- Great alternative to OpenVPN & IPSec
- Modern, Simple & Robust
- Cross Platform
- Roaming support
- Open Source GPLv3



Interface: vpn.sl.zone
Status: ● Active
Public key: p2RNWcZf0pmw0cOsgysuPvshQnMJIdNqvlvyB3KPuGg=
Addresses: 10.54.11.101/24
Listen port: 54906

Peer: xFIQxqQsJ+faEaJkH4zt8WKcXA9Z1ivVWvovPJuPiVs=
Preshared key: enabled
Endpoint: 194.213.36.18:51820
Allowed IPs: 10.54.11.0/24, 10.54.81.0/24
Persistent keepalive: every 25 seconds
Data sent: 444 B

On-Demand: Off



Name: vpn.sl.zone

Public key:

On-Demand: □ Ethernet □ Wi-Fi

```
[Interface]
PrivateKey = XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX=
Address = 10.54.11.101/24

[Peer]
PublicKey = xFIQxqQsJ+faEaJkH4zt8WKcXA9Z1ivVWvovPJuPiVs=
PresharedKey = YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY=
AllowedIPs = 10.54.11.0/24, 10.54.81.0/24
Endpoint = vpn.sl.zone:51820
PersistentKeepalive = 25
```

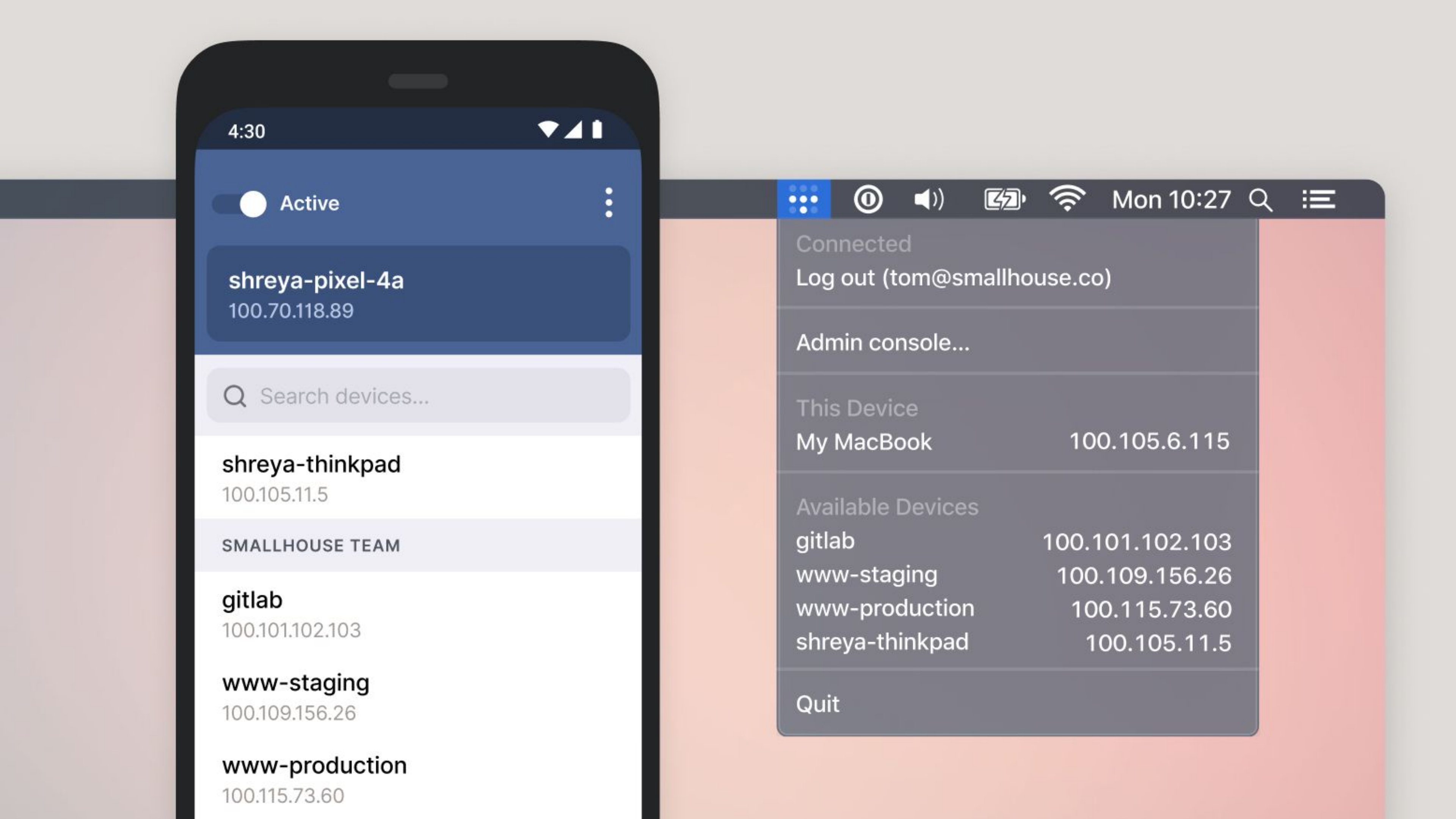
DEMO TIME 🚀🚀

But WireGuard is not so user friendly... 😔

tailscale

What is Tailscale

- Modern managed VPN solution
- WireGuard based
- Identity based authentication
- 6 USD / user / mo (3 free users, 100 devices)
- Serverless VPN (managed relay servers)
- ACL
- API & Terraform
- Open Source Clients, Open Communication
- Great Docs & Blog



shreya-pixel-4a
100.70.118.89

shreya-thinkpad
100.105.11.5

SMALLHOUSE TEAM

gitlab
100.101.102.103

www-staging
100.109.156.26

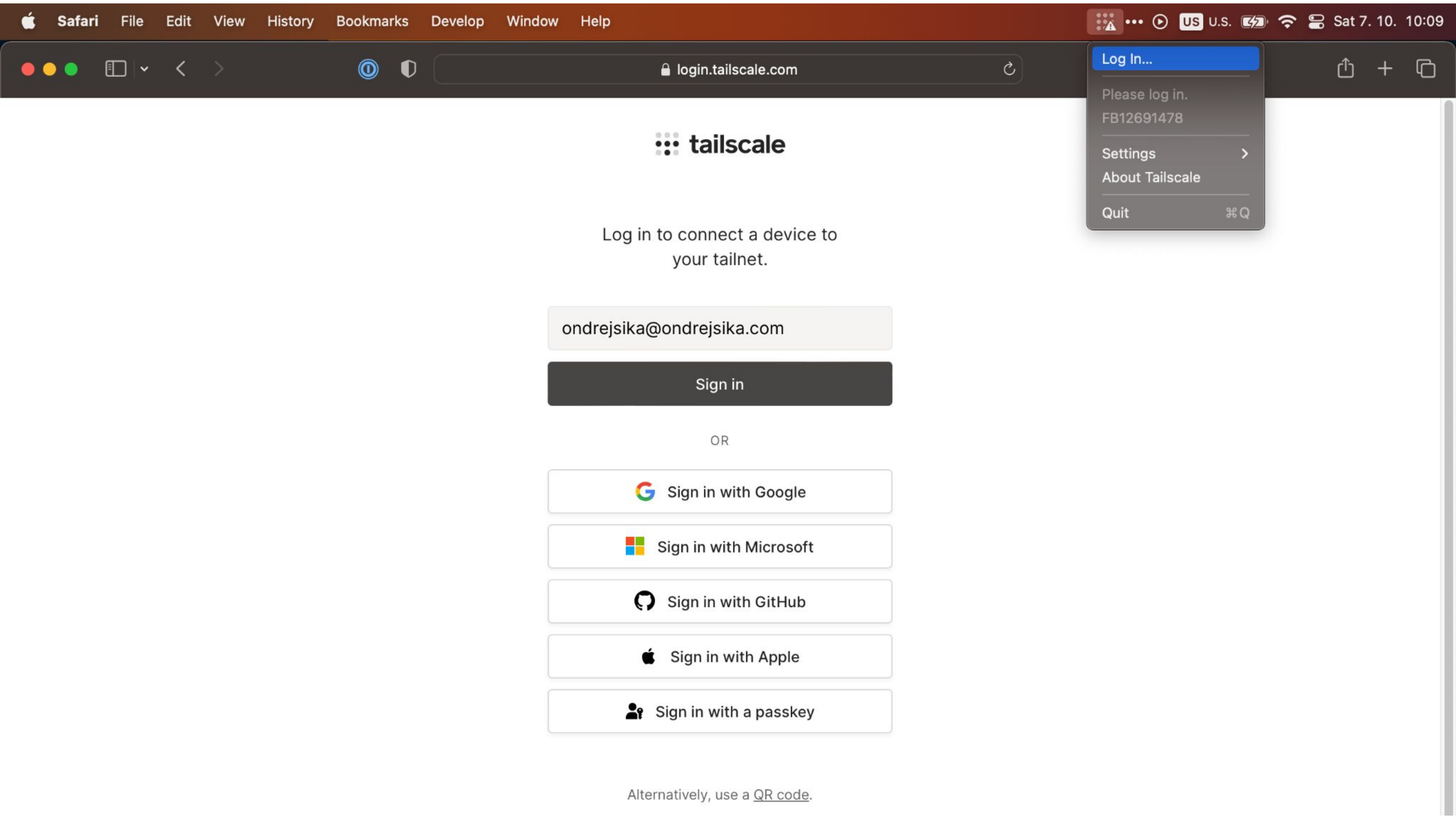
www-production
100.115.73.60

This Device

My MacBook	100.105.6.115

Available Devices

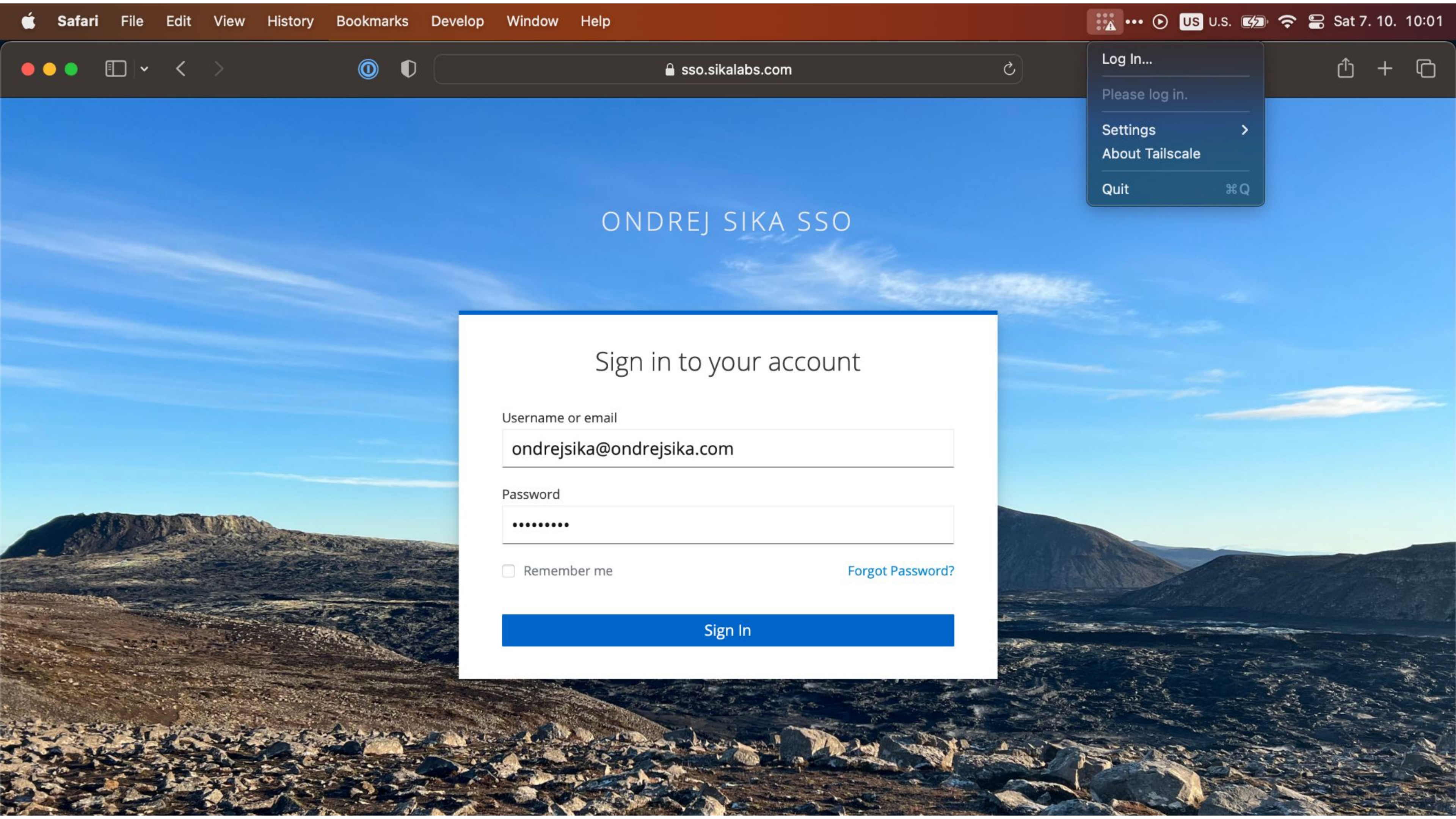
gitlab	100.101.102.103
www-staging	100.109.156.26
www-production	100.115.73.60
shreya-thinkpad	100.105.11.5



Log in to connect a device to your tailnet.

ondrejsika@ondrejsika.com

Alternatively, use a QR code.



Please log in.

sso.sikalabs.com

ONDREJ SIKA SSO

Sign in to your account

Username or email

ondrejsika@ondrejsika.com

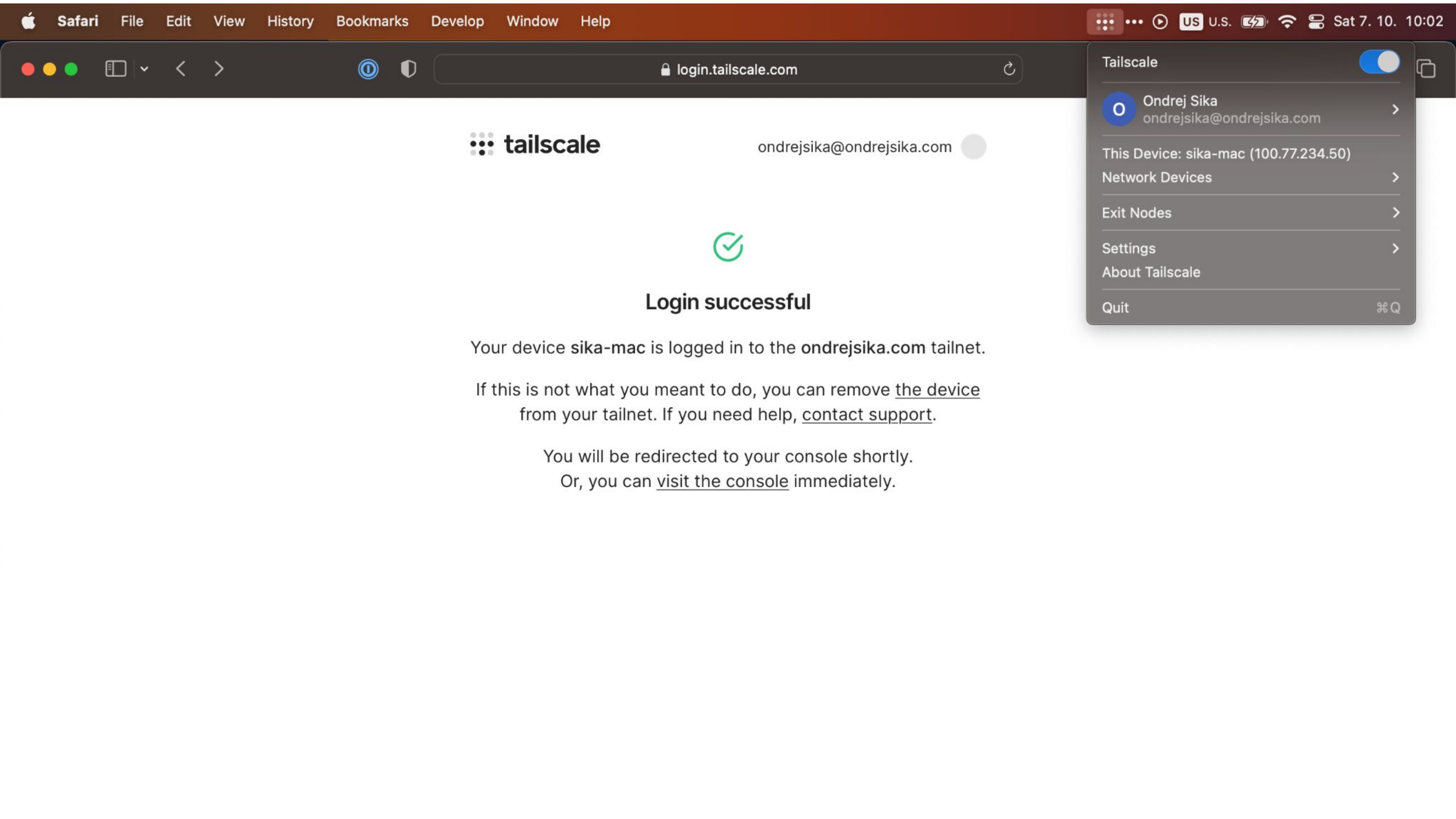
Password

••••••••••

□ Remember me

Forgot Password?

Sign In

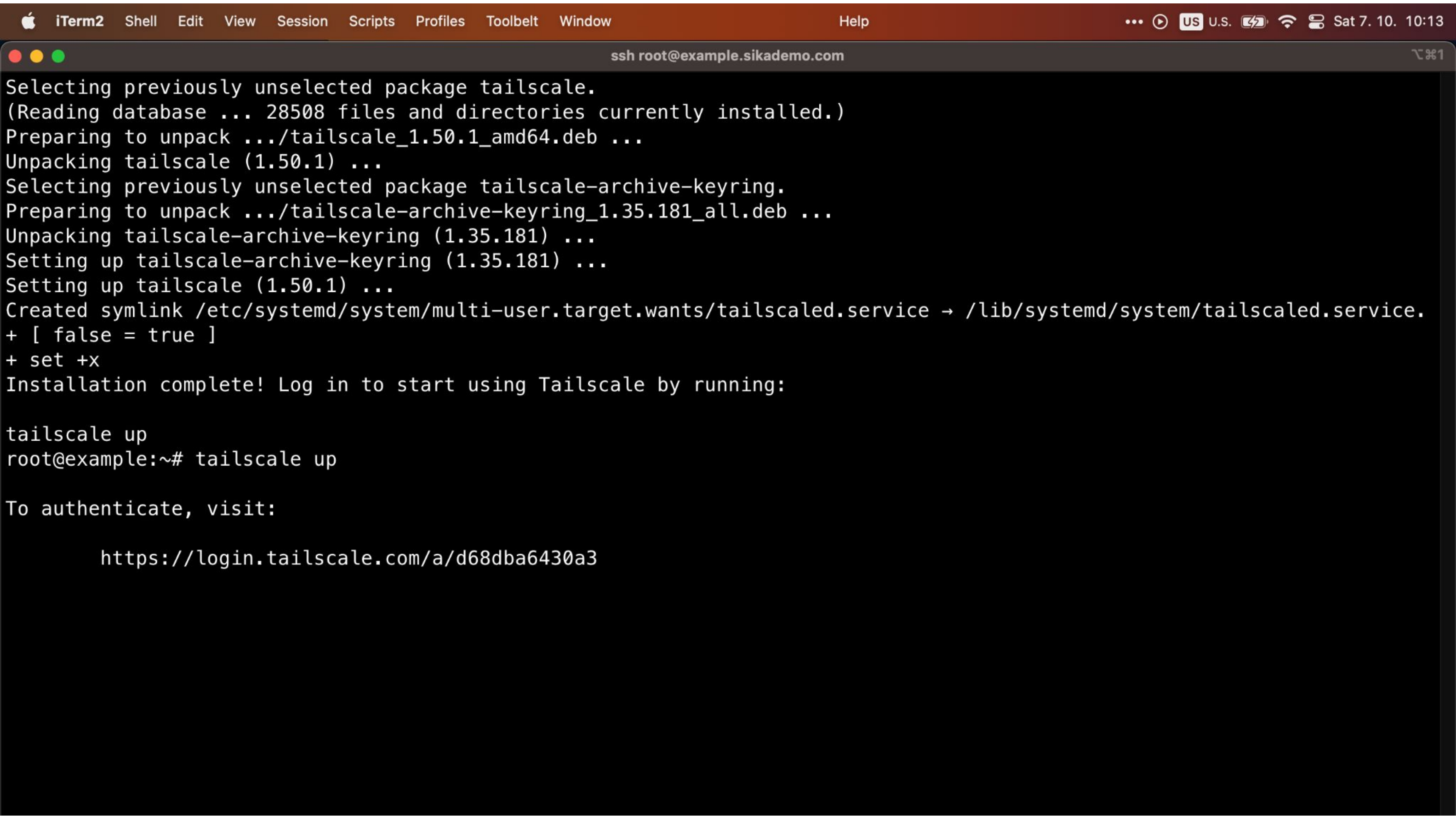


Login successful

Your device **sika-mac** is logged in to the **ondrejsika.com** tailnet.

If this is not what you meant to do, you can remove the device from your tailnet. If you need help, contact support.

You will be redirected to your console shortly.
Or, you can visit the console immediately.

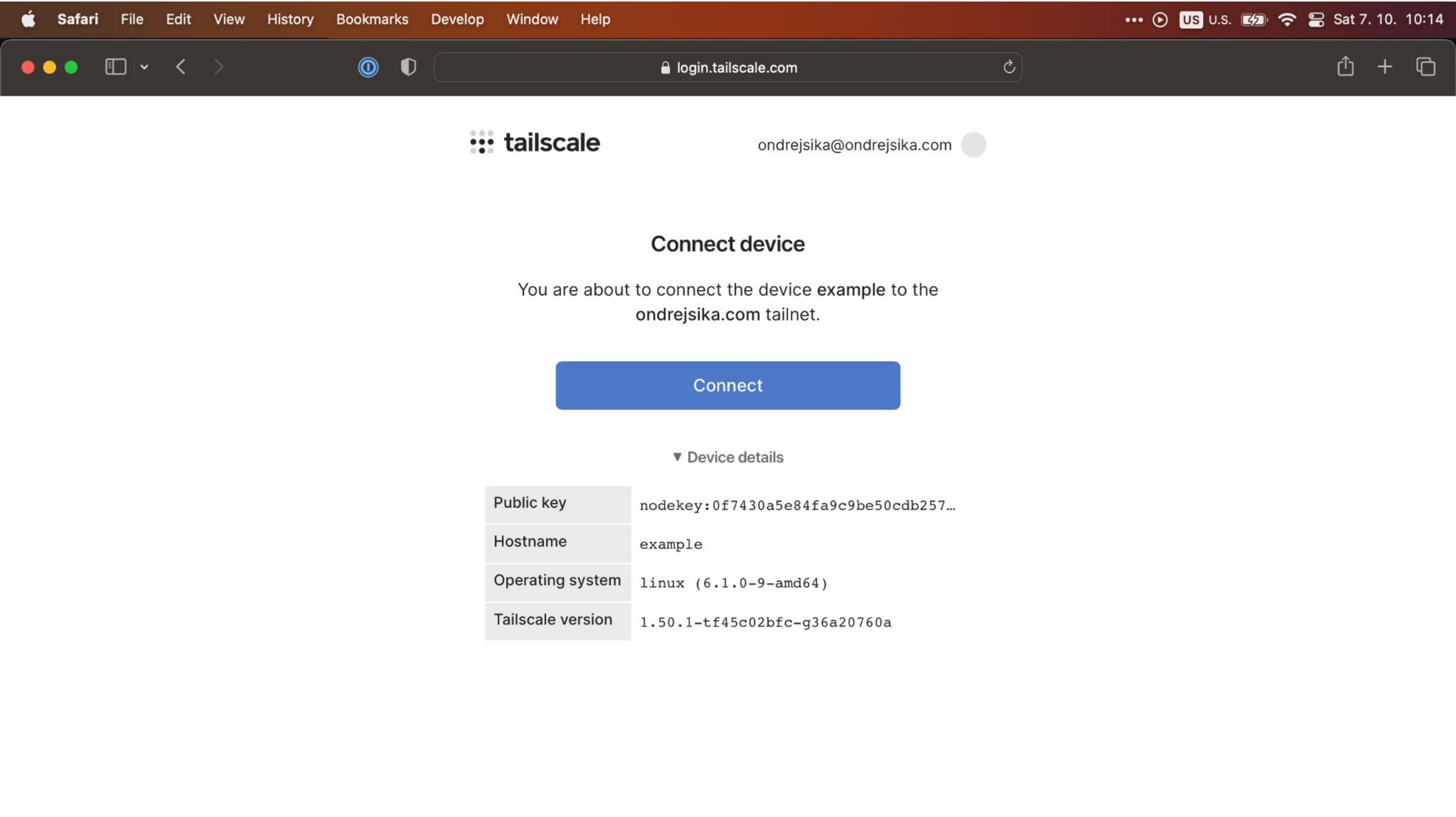


```
Selecting previously unselected package tailscale.
(Reading database ... 28508 files and directories currently installed.)
Preparing to unpack .../tailscale_1.50.1_amd64.deb ...
Unpacking tailscale (1.50.1) ...
Selecting previously unselected package tailscale-archive-keyring.
Preparing to unpack .../tailscale-archive-keyring_1.35.181_all.deb ...
Unpacking tailscale-archive-keyring (1.35.181) ...
Setting up tailscale-archive-keyring (1.35.181) ...
Setting up tailscale (1.50.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/tailscaled.service → /lib/systemd/system/tailscaled.service.
+ [ false = true ]
+ set +x
Installation complete! Log in to start using Tailscale by running:

tailscale up
root@example:~# tailscale up

To authenticate, visit:

        https://login.tailscale.com/a/d68dba6430a3
```

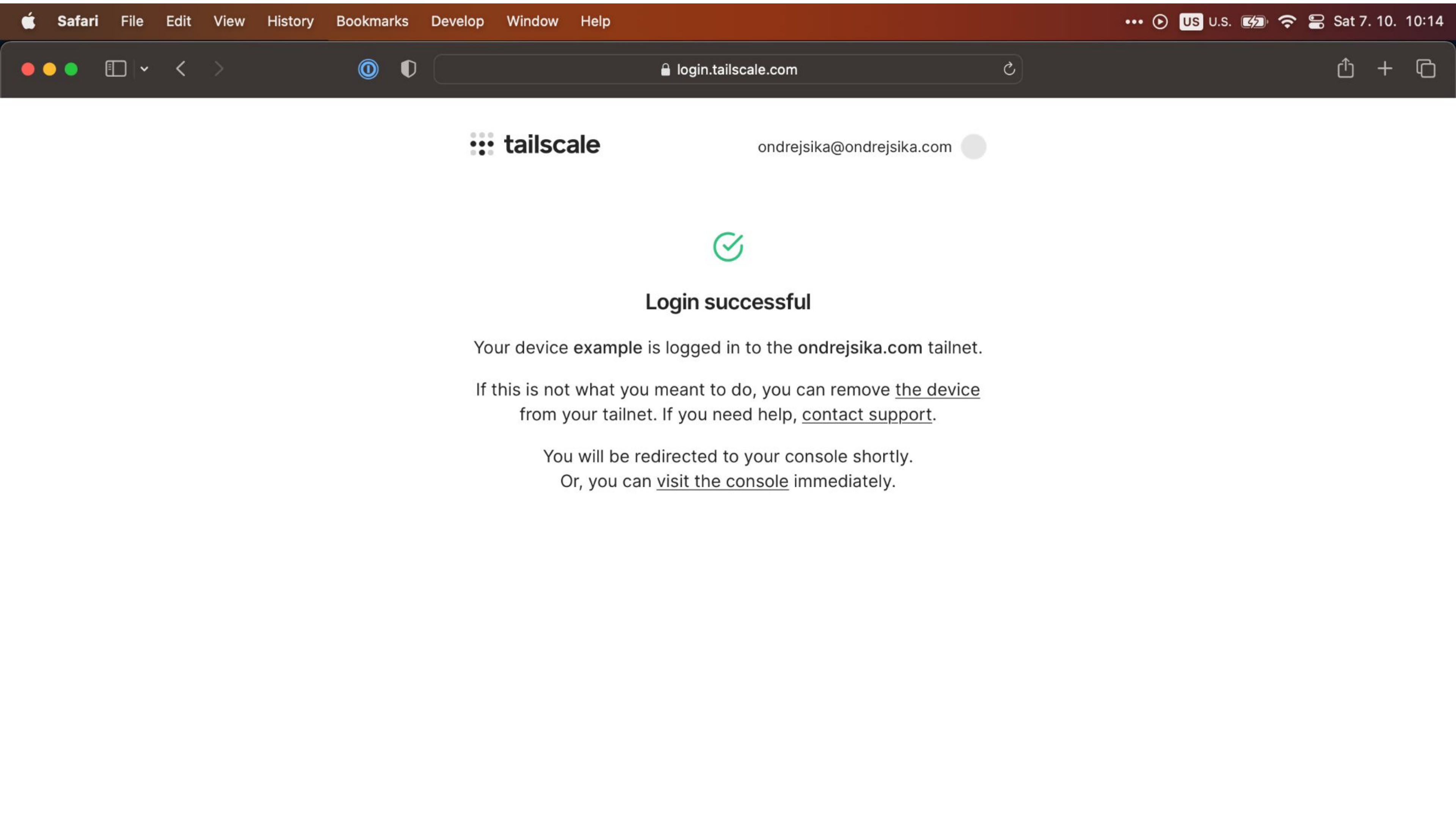

Safari File Edit View History Bookmarks Develop Window Help
US U.S. Sat 7. 10. 10:14
login.tailscale.com
tailscale
ondrejsika@ondrejsika.com
Connect

Connect device

You are about to connect the device **example** to the **ondrejsika.com** tailnet.

▼ Device details

Public key	`nodekey:0f7430a5e84fa9c9be50cdb257…`
Hostname	`example`
Operating system	`linux (6.1.0-9-amd64)`
Tailscale version	`1.50.1-tf45c02bfc-g36a20760a`



ondrejsika@ondrejsika.com

Login successful

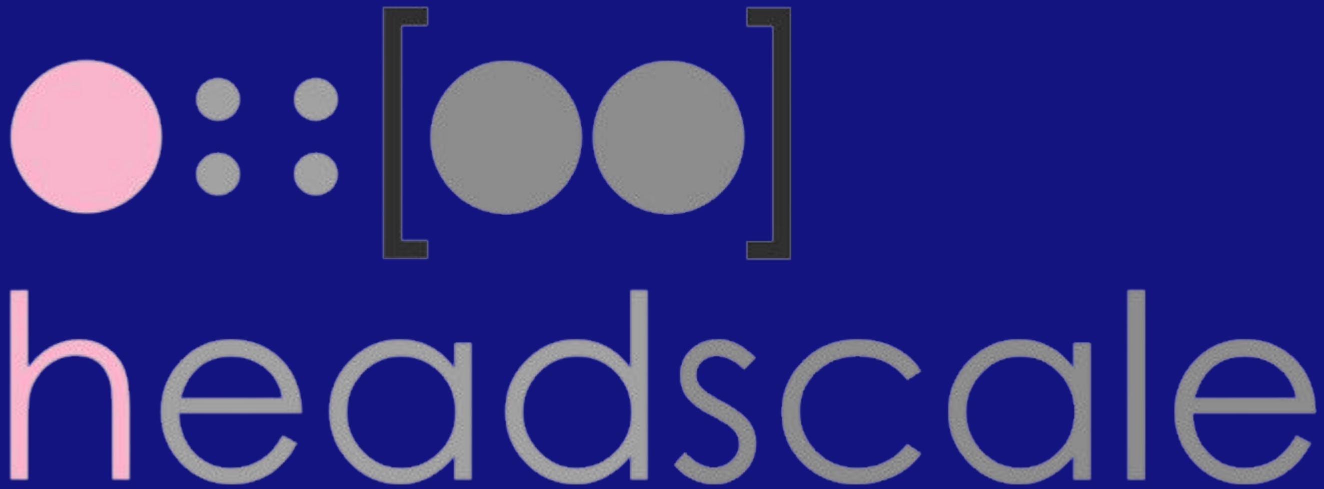
Your device **example** is logged in to the **ondrejsika.com** tailnet.

If this is not what you meant to do, you can remove the device from your tailnet. If you need help, contact support.

You will be redirected to your console shortly.
Or, you can visit the console immediately.

DEMO TIME 🚀🚀

Open Source Tailscale?


headscale

What is Headscale

- Open Source management server for Tailscale
- Same features like Tailscale (except for relays)
- No UI (but there are third party UI projects)
- Use official Tailscale clients

```
tailscale up --login-server https://vpn.sl.zone
```

DEMO TIME 🚀 🚀

Thanks for your attention

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Questions?

@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Email

ondrej@sika.io

Twitter

@ondrejsika

LinkedIn

/in/ondrejsika

Slides

sika.link/slides

github.com/ondrejsika/linuxdays24-vpn