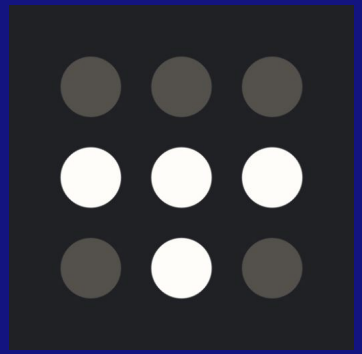
VPNs in 2023



Ondřej Šika

ondrej@sika.io
@ondrejsika

jOpenSpace 2023,
Telč, 7. 10. 2023

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.

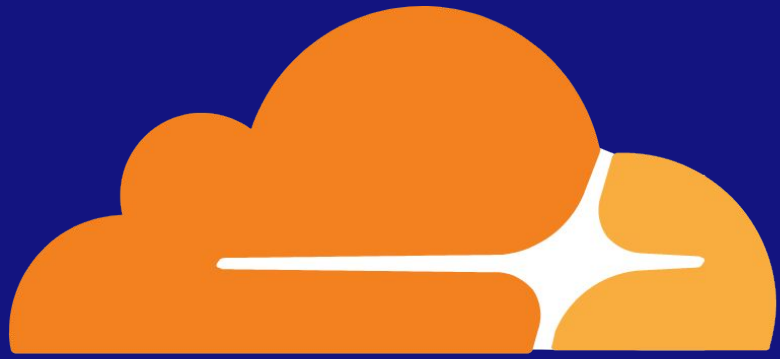
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

Do you need a VPN? 🤔

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

You don't!

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

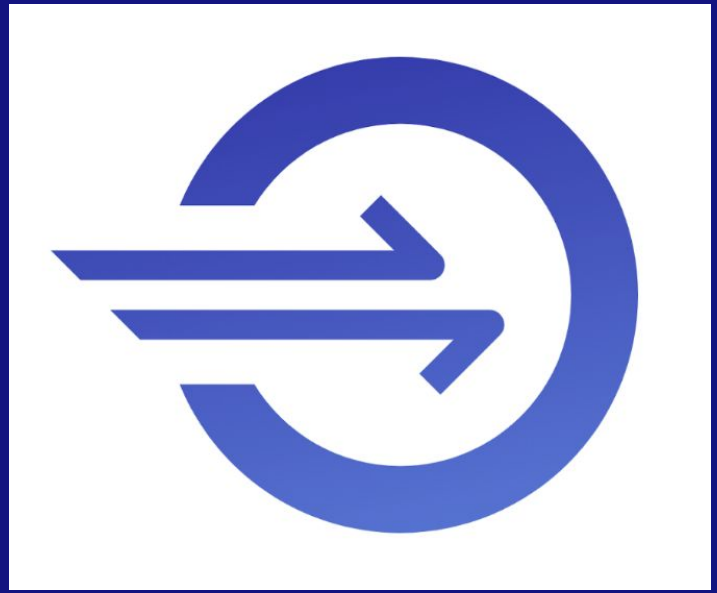


CLOUDFLARE®

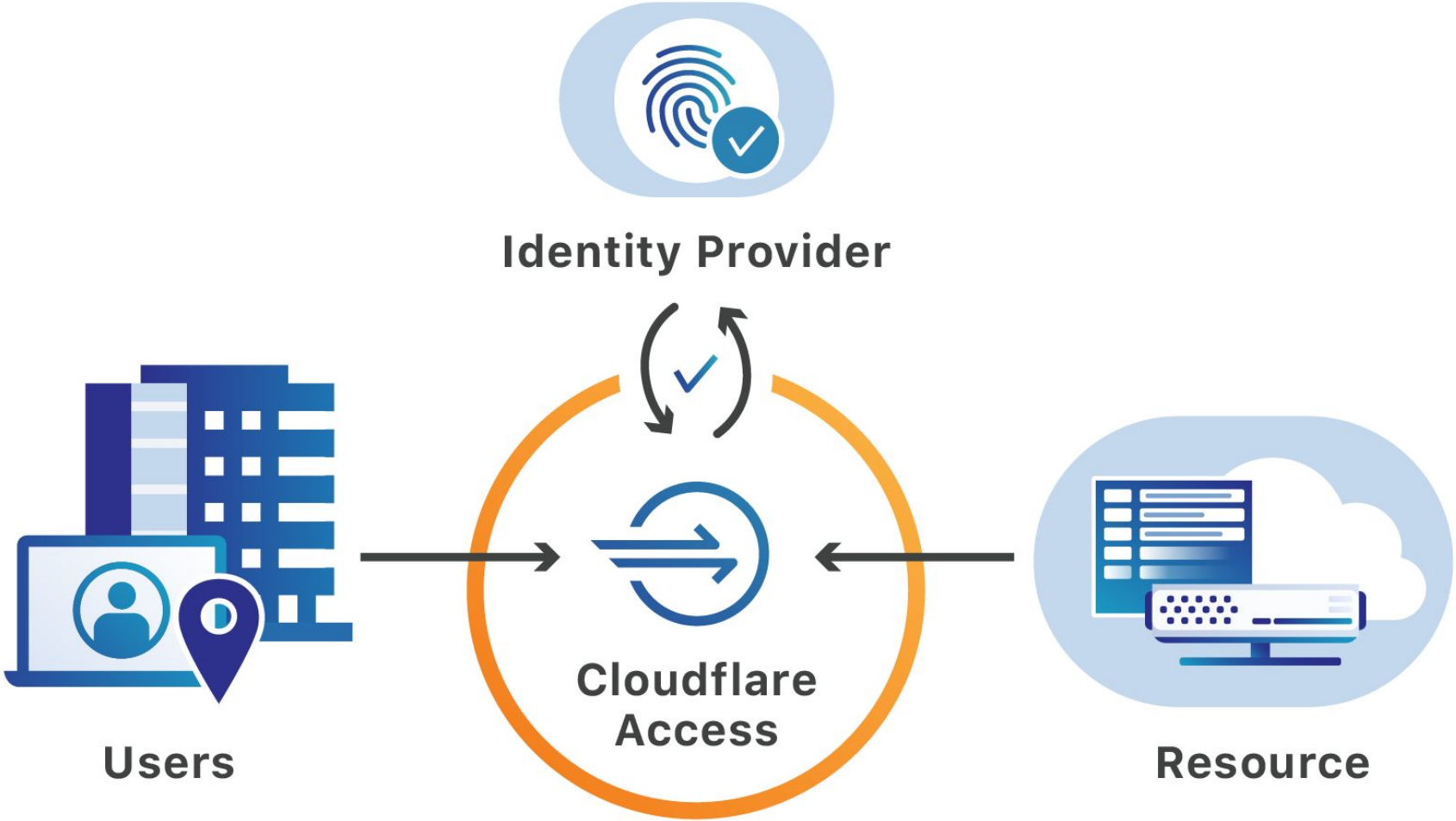
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

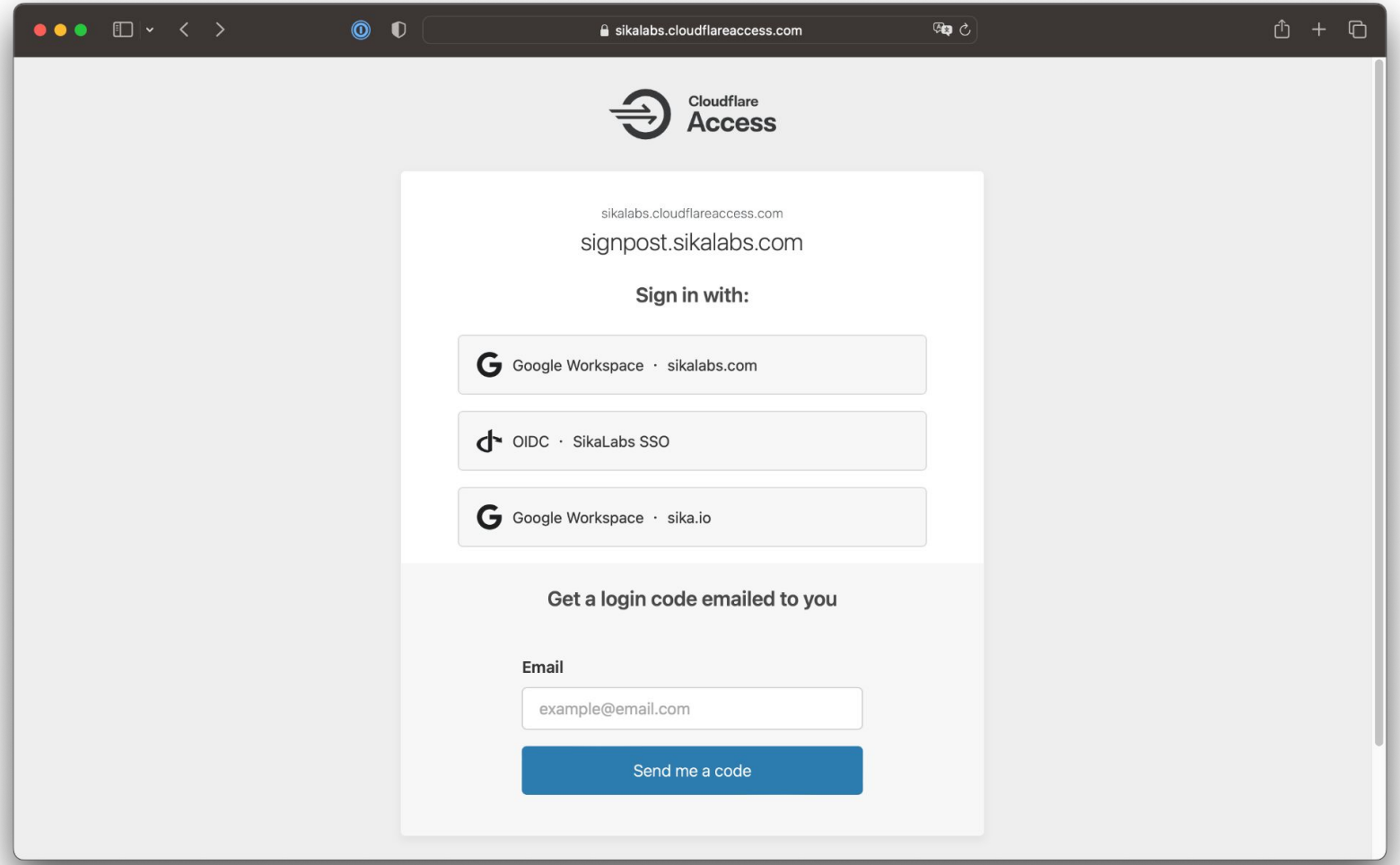
Cloudflare Access

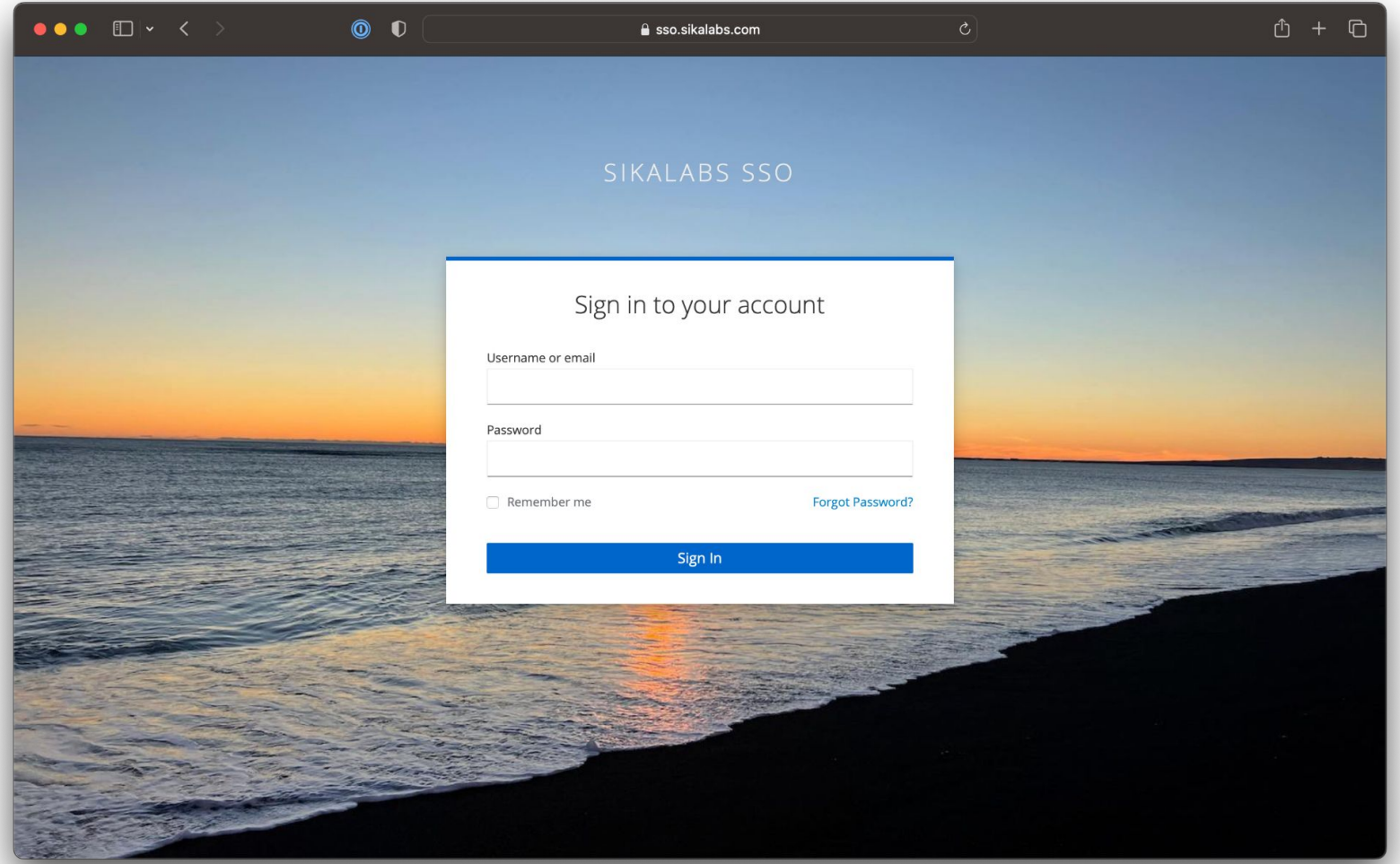
- Secure VPN alternative
- Identity based Cloudflare Proxy
- Zero trust model
- Identity based authentication
  - OIDC (Okta, Keycloak)
  - Google, Microsoft
  - Email



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


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


sso.sikalabs.com
SIKALABS SSO
Sign in to your account
Username or email
Password
Remember me
Forgot Password?
Sign In

Open Source alternatives?

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

- HashiCorp Boundary
- oidc2-proxy

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

What if we really need a VPN?

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

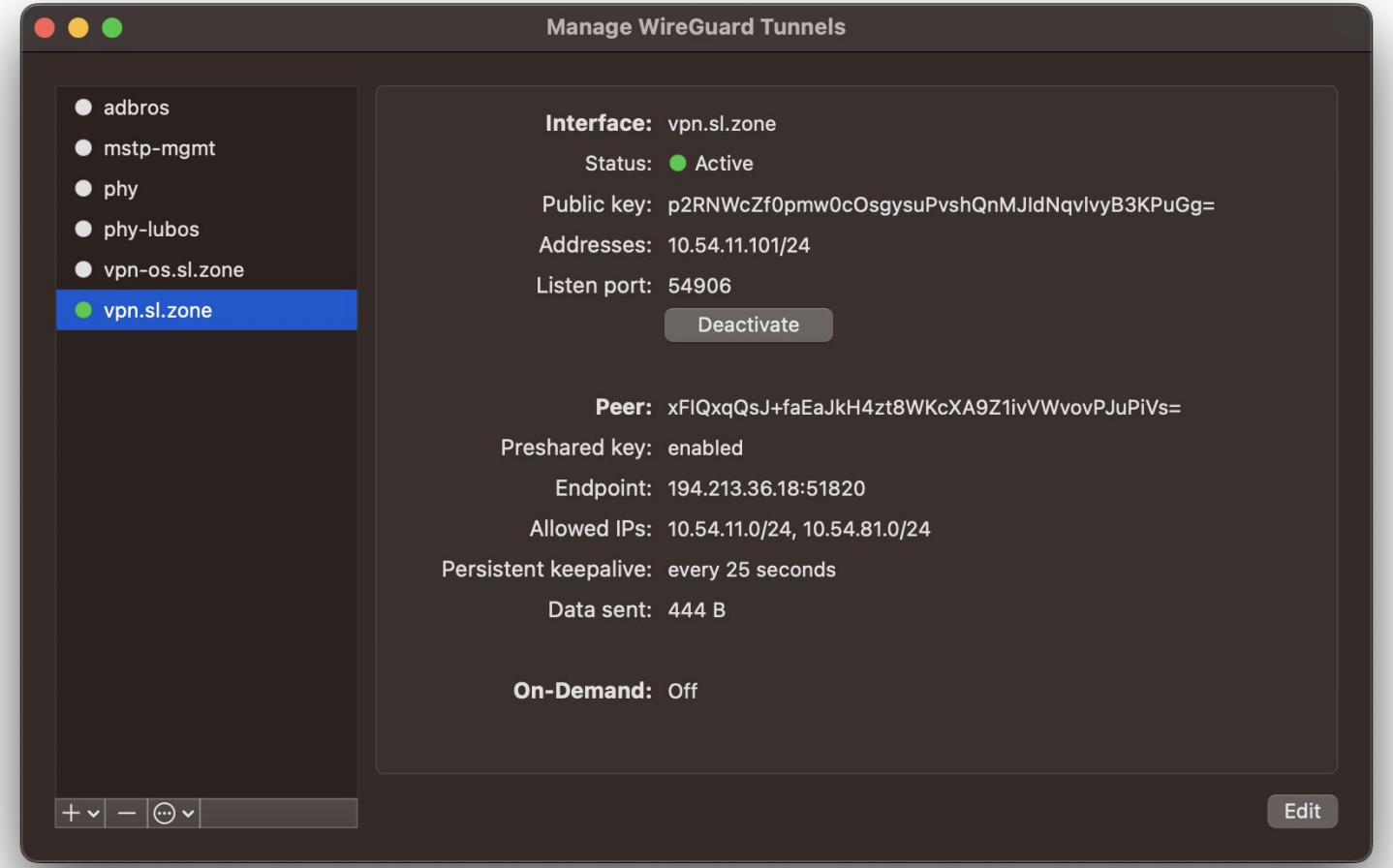
WireGuard

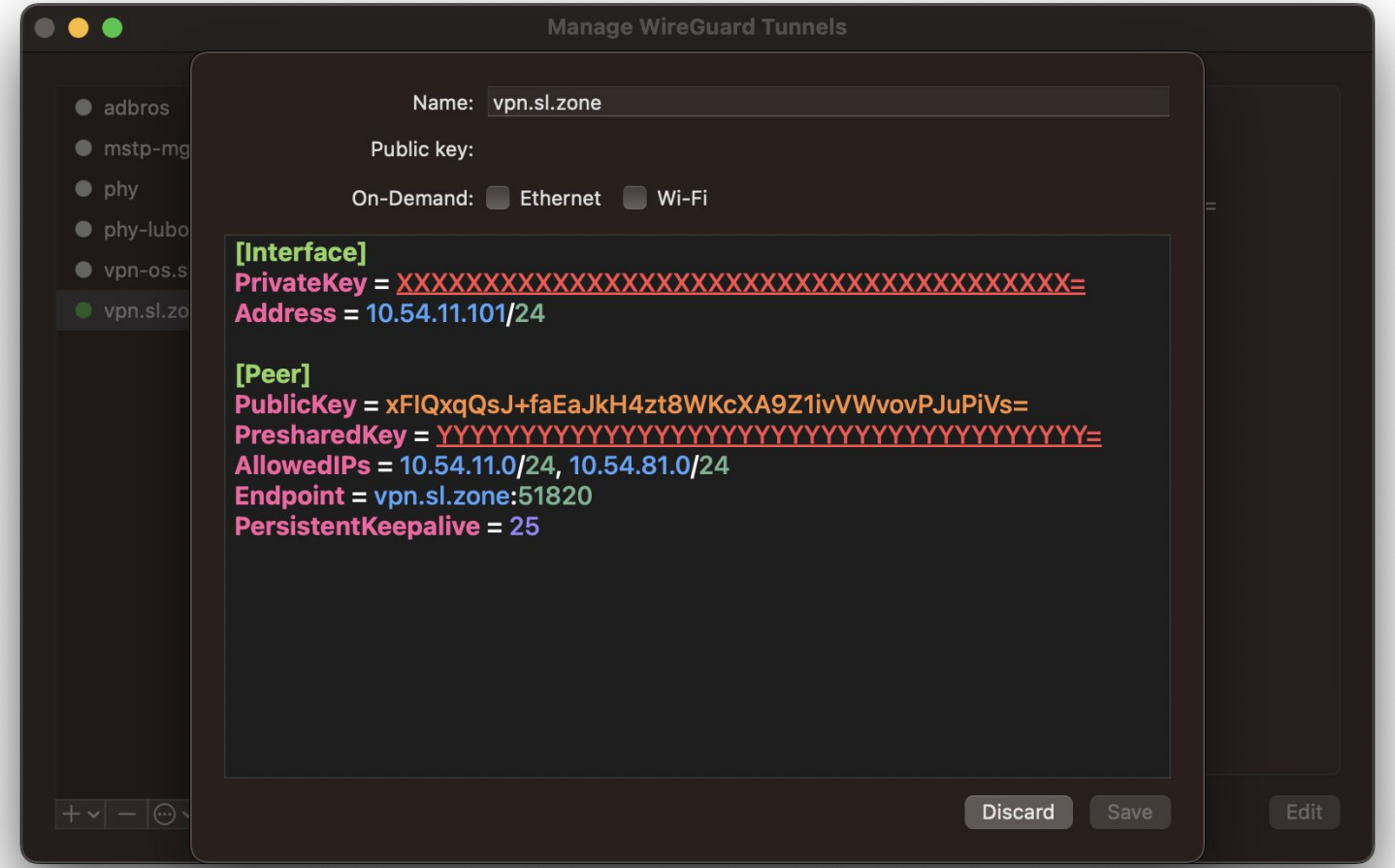
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

What is WireGuard?

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

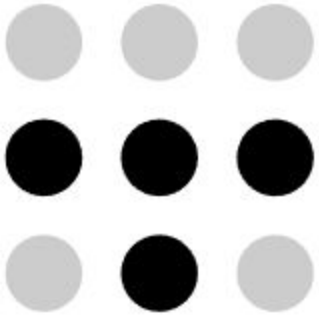
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika


Manage WireGuard Tunnels
adbros
mstp-mgmt
phy
phy-lubos
vpn-os.sl.zone
vpn.sl.zone
Interface: vpn.sl.zone
Status: Active
Public key: p2RNWcZf0pmw0cOsgysuPvshQnMJldNqvlvyB3KPuGg=
Addresses: 10.54.11.101/24
Listen port: 54906
Deactivate
Peer: xFlQxqQsJ+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
Edit


Manage WireGuard Tunnels
adbros
mstp-mg
phy
phy-lubo
vpn-os.s
vpn.sl.zo
Name: vpn.sl.zone
Public key:
On-Demand: Ethernet Wi-Fi
[Interface]
PrivateKey = XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX=
Address = 10.54.11.101/24
[Peer]
PublicKey = xFlQxqQsJ+faEaJkH4zt8WKcXA9Z1ivVWvovPJuPiVs=
PresharedKey = YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY=
AllowedIPs = 10.54.11.0/24, 10.54.81.0/24
Endpoint = vpn.sl.zone:51820
PersistentKeepalive = 25
Discard
Save
Edit

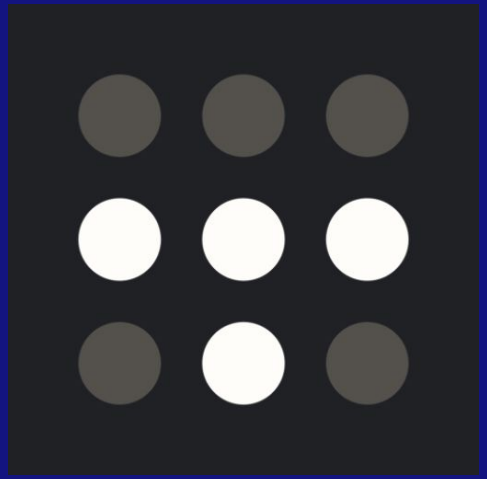
But WireGuard is not so user friendly... 😔

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



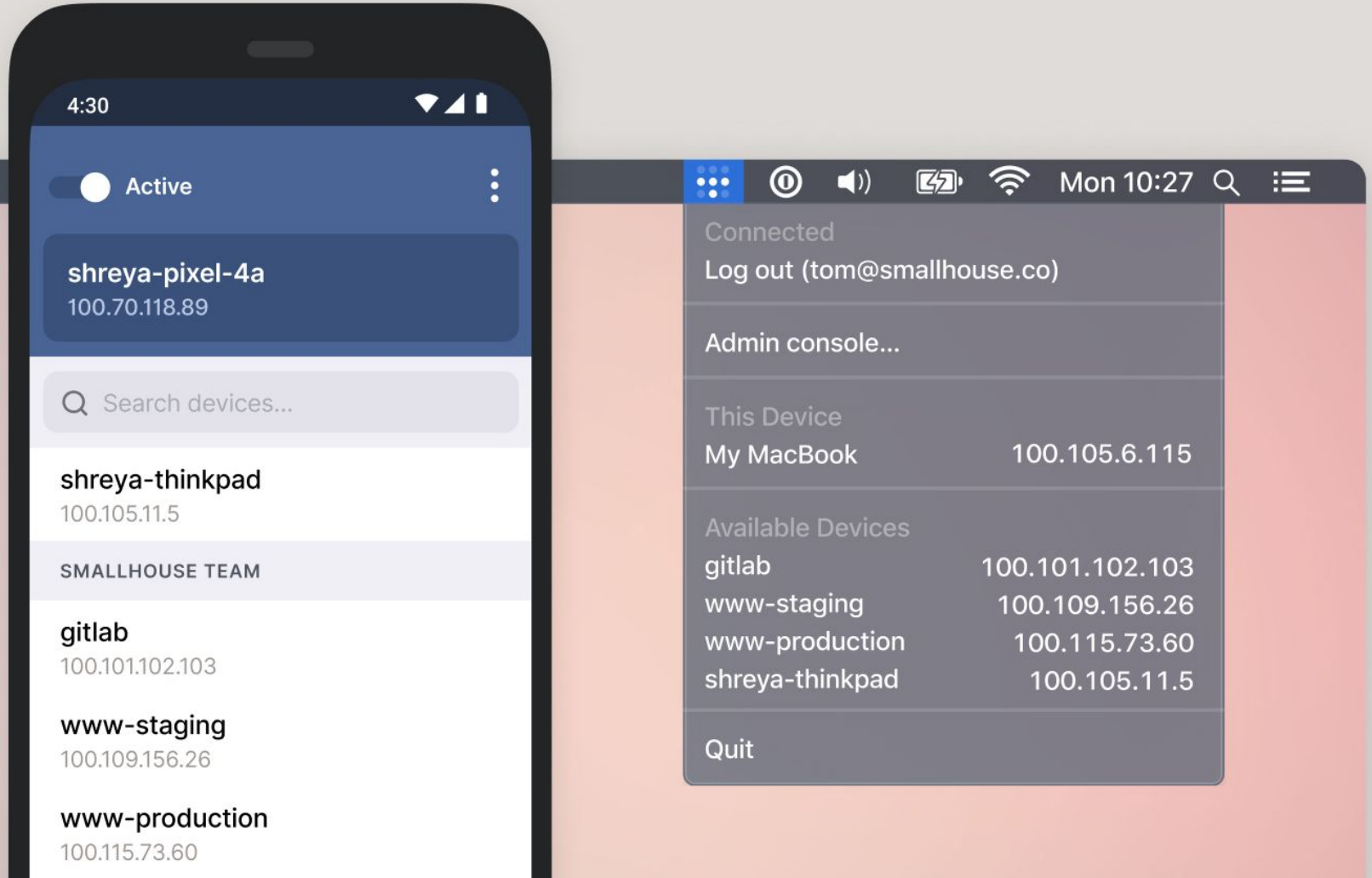
tailscale

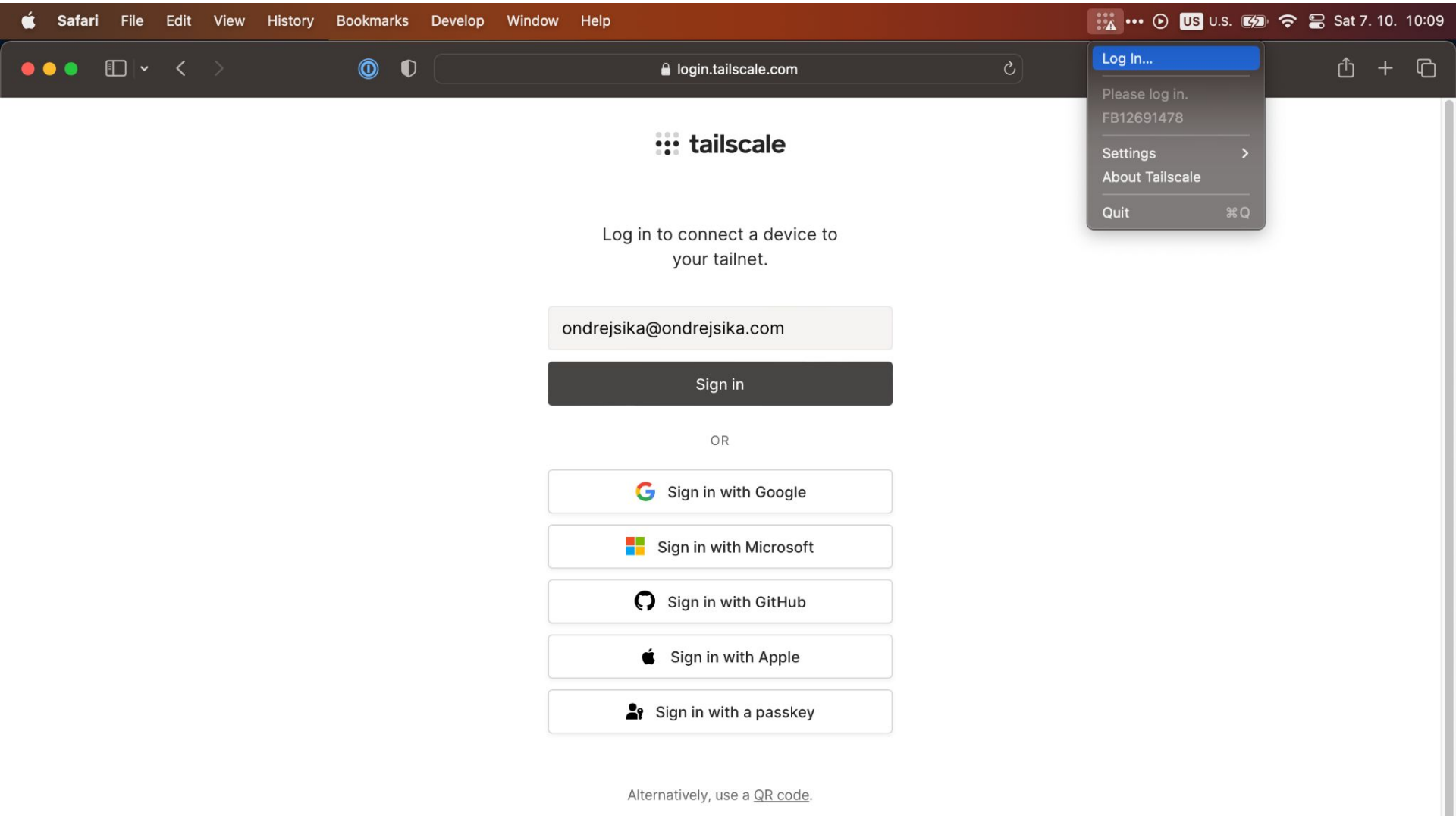
What is Tailscale

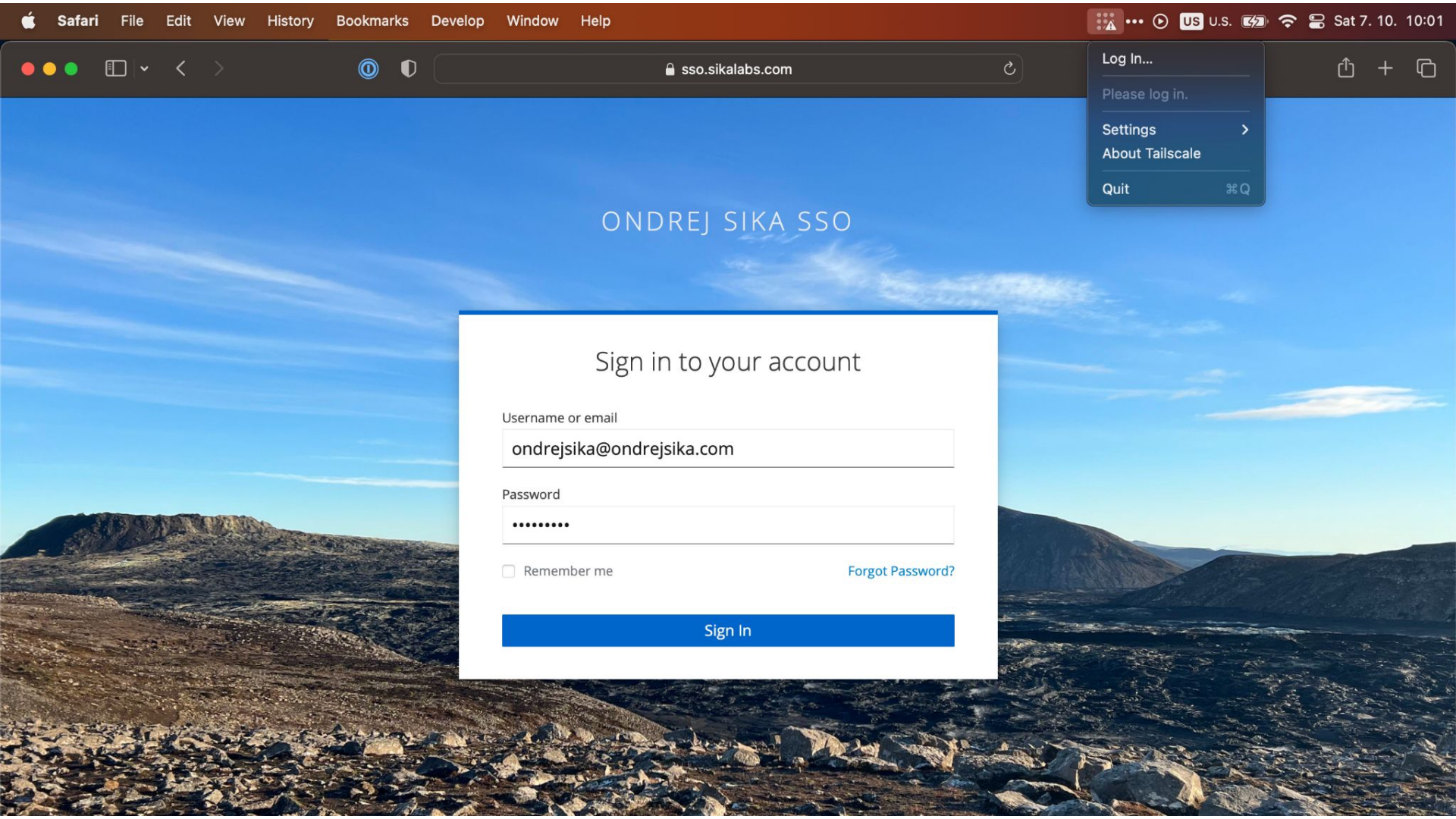


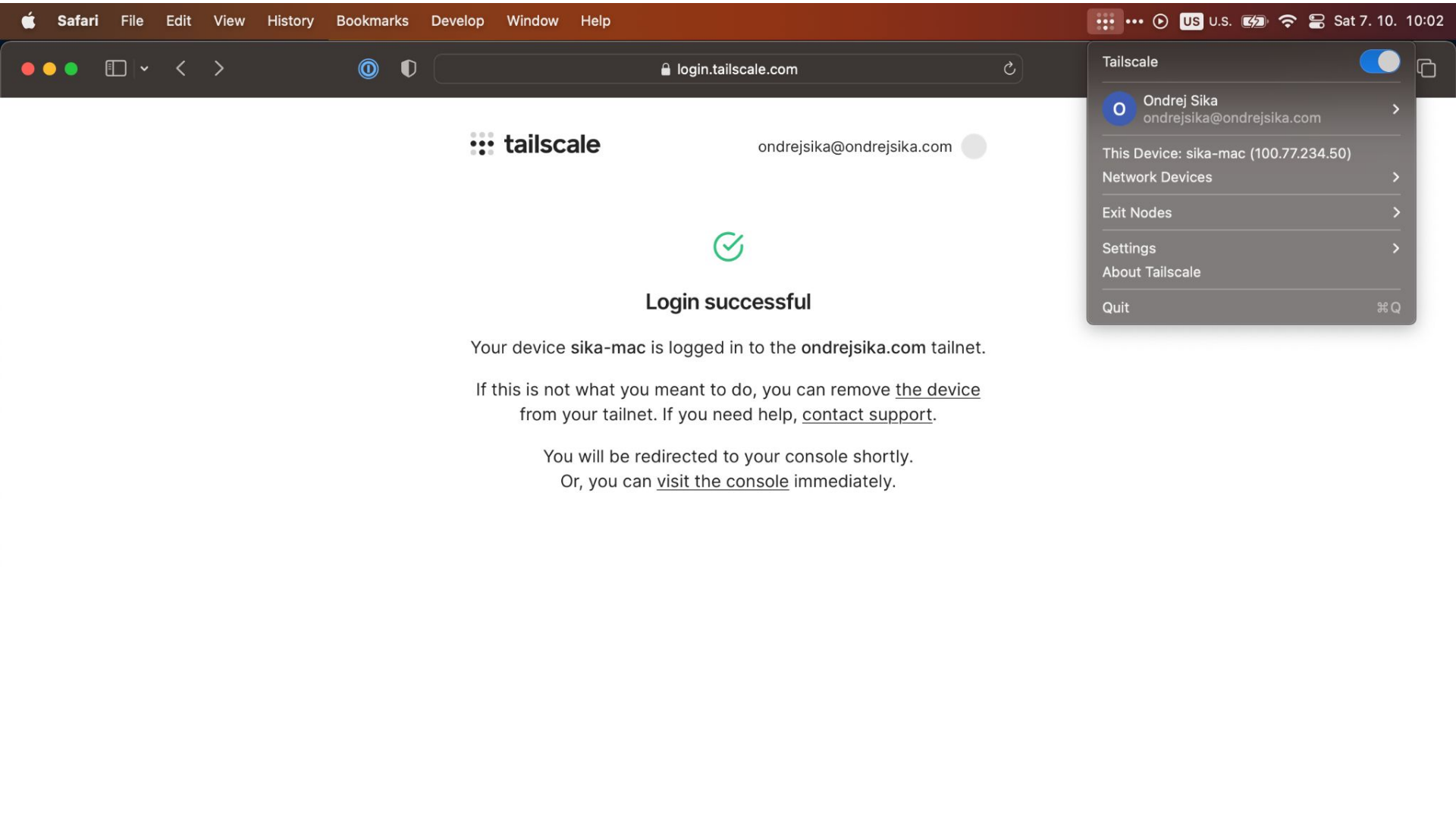
- Modern managed VPN solution
- WireGuard based
- Identity based authentication
- 6 USD / user / mo (3 free users, 100 devices)
- Serverless VPN (managed relay servers)
- ACL
- API & Terraform
- Open Source Clients, Open Communication
- Great Docs & Blog

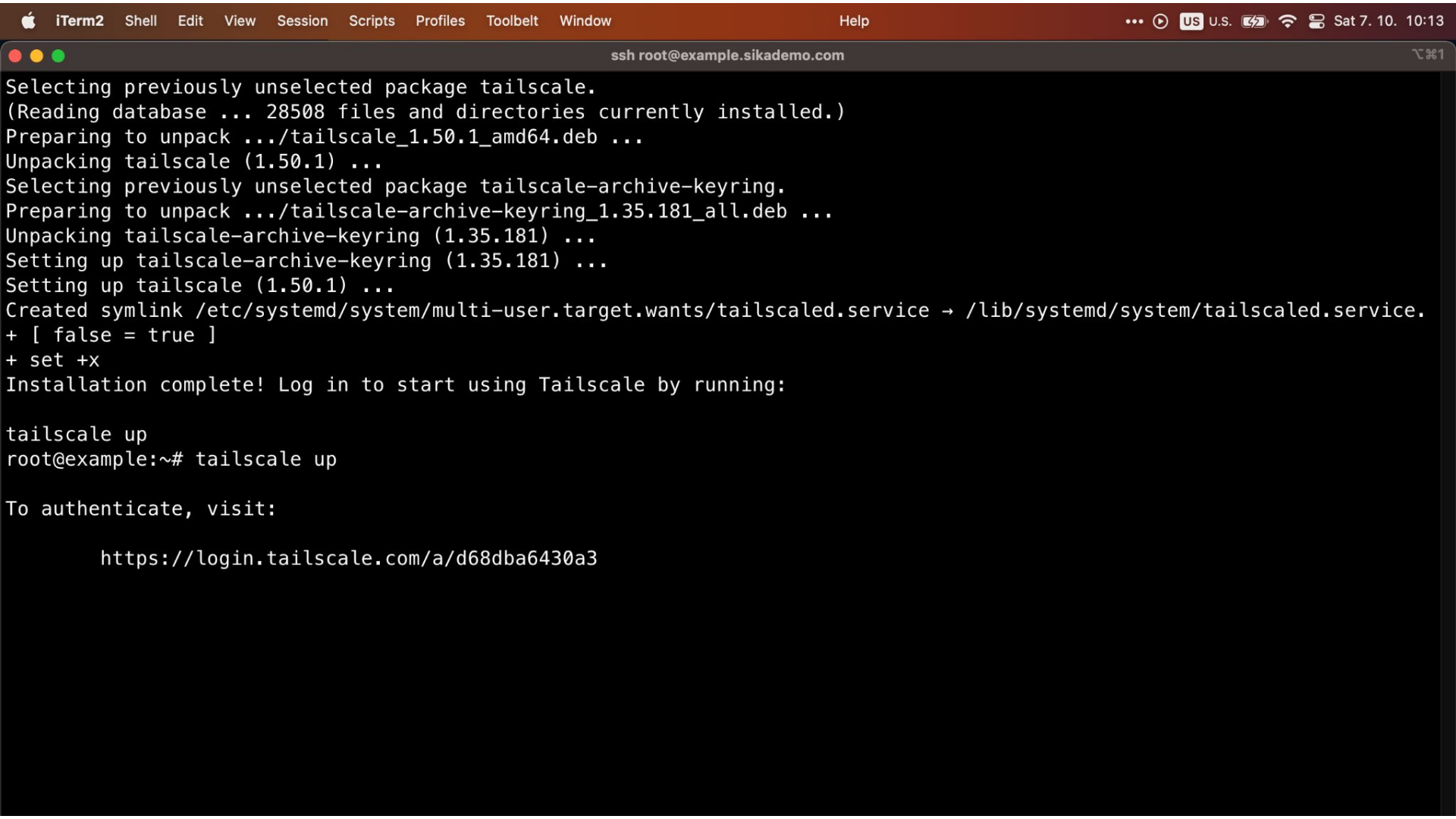
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika

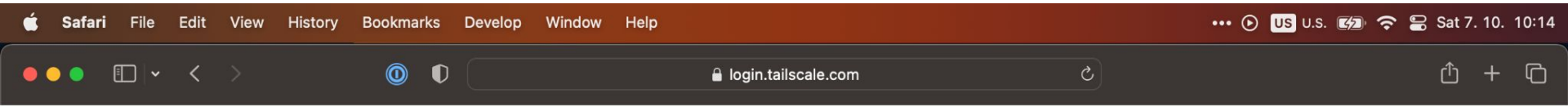

4:30
Active
shreya-pixel-4a
100.70.118.89
Search devices...
shreya-thinkpad
100.105.11.5
SMALLHOUSE TEAM
gitlab
100.101.102.103
www-staging
100.109.156.26
www-production
100.115.73.60
Mon 10:27
Connected
Log out (tom@smallhouse.co)
Admin console...
This Device
My MacBook 100.105.6.115
Available Devices
gitlab 100.101.102.103
www-staging 100.109.156.26
www-production 100.115.73.60
shreya-thinkpad 100.105.11.5
Quit


Safari File Edit View History Bookmarks Develop Window Help
US U.S. Sat 7. 10. 10:09
login.tailscale.com
Log In...
Please log in.
FB12691478
Settings
About Tailscale
Quit ⌘Q
tailscale
Log in to connect a device to your tailnet.
ondrejsika@ondrejsika.com
Sign in
OR
Sign in with Google
Sign in with Microsoft
Sign in with GitHub
Sign in with Apple
Sign in with a passkey
Alternatively, use a QR code.


Safari File Edit View History Bookmarks Develop Window Help
Sat 7. 10. 10:01
sso.sikalabs.com
Log In...
Please log in.
Settings
About Tailscale
Quit ⌘Q
ONDREJ SIKA SSO
Sign in to your account
Username or email
ondrejsika@ondrejsika.com
Password
Remember me
Forgot Password?
Sign In


Safari File Edit View History Bookmarks Develop Window Help
US U.S. Sat 7. 10. 10:02
login.tailscale.com
Tailscale
Ondrej Sika
ondrejsika@ondrejsika.com
This Device: sika-mac (100.77.234.50)
Network Devices
Exit Nodes
Settings
About Tailscale
Quit ⌘Q
tailscale
ondrejsika@ondrejsika.com
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.


iTerm2 Shell Edit View Session Scripts Profiles Toolbelt Window Help
US U.S. Sat 7. 10. 10:13
ssh root@example.sikademo.com
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



tailscale

ondrejsika@ondrejsika.com

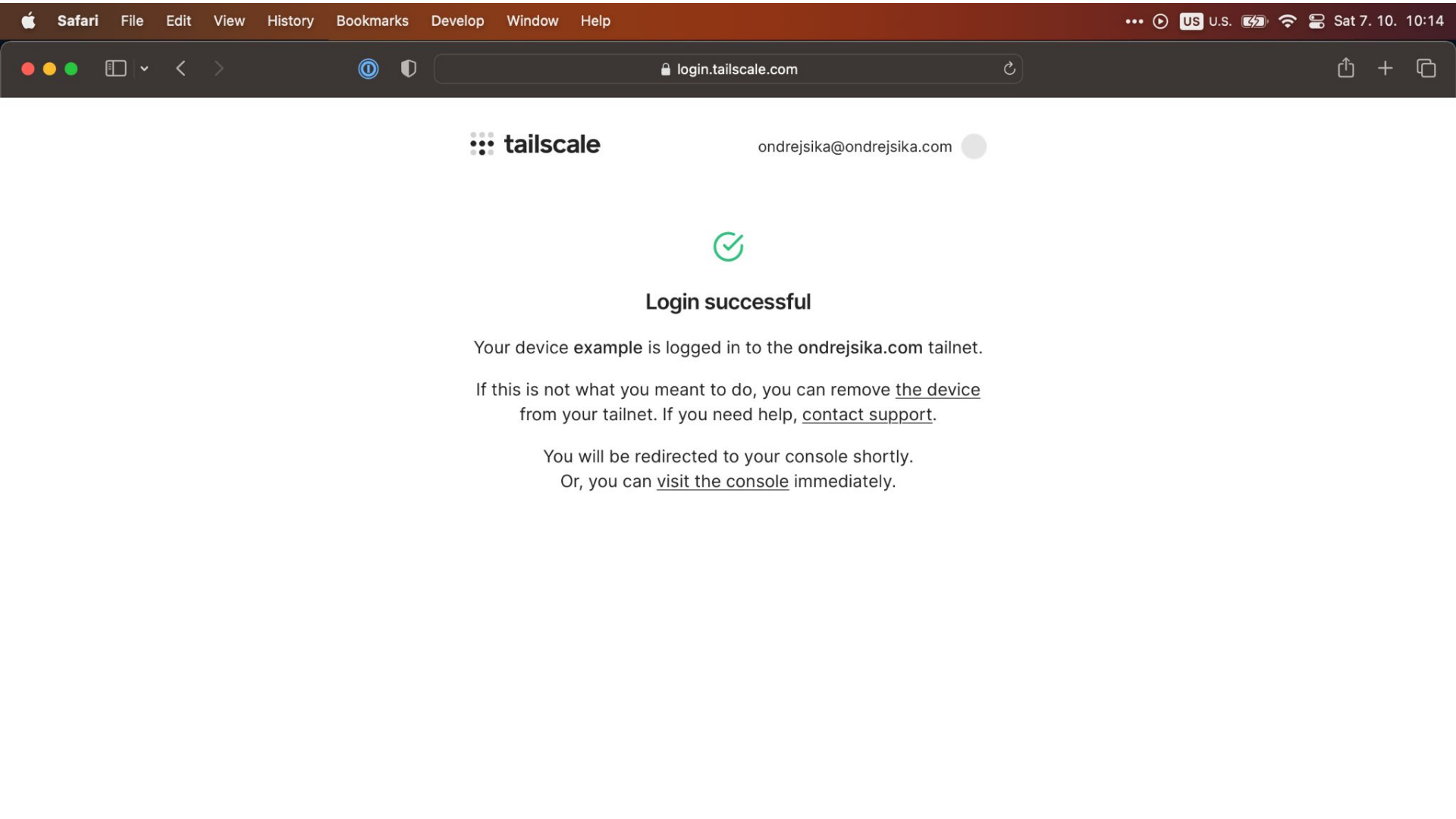
Connect device

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

Connect

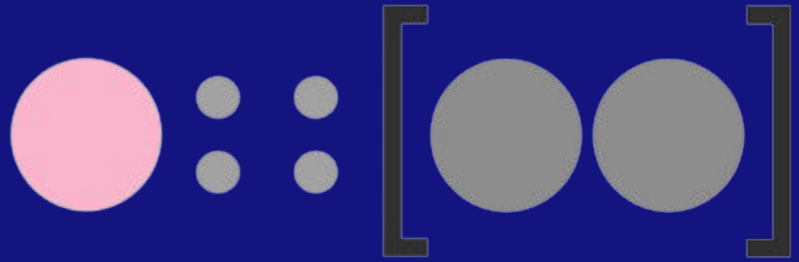
▼ Device details

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


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

Open Source Tailscale?

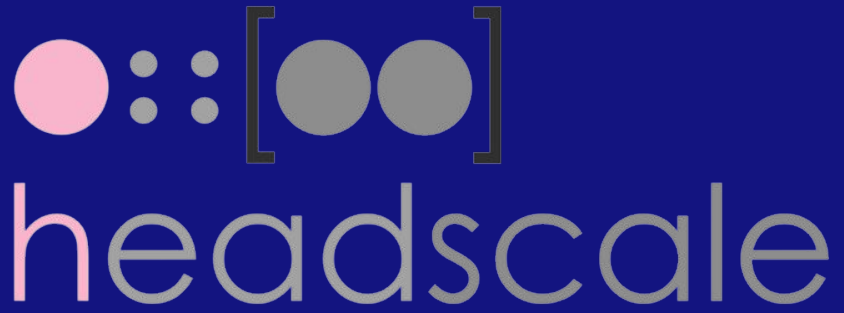
@ondrejsika ondrej@sika.io sika.io /in/ondrejsika



headscale

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

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
```

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

Díky za pozornost

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

Otázky?

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

Email

ondrej@sika.io

Twitter

@ondrejsika

LinkedIn

/in/ondrejsika

Slides

sika.link/slides