eduVPN 3.0

François Kooman

77. Betriebstagung @DFN

19.10.2022

About Me

François Kooman, MSc

Software Engineer @DeiC (DK)

Previously: Technical Product Manager @SURF (NL)

Overview

- What is eduVPN?
- Why eduVPN?
- What’s new in 3.0?
- How to eduVPN

Why VPN?

- In 2022 we *still* need a VPN
  - Services are often (still) not secure enough to directly expose to the Internet
  - Hide existence of (certain) services from the Internet
  - If you don’t care about the above, it is *still* an extra line of defense…

What is eduVPN?

- A Commons Conservancy (TCC) program supported by GÉANT, SURF, NORDUnet and others
- Offering a complete VPN solution
  - Server Software
  - Apps
  - Supporting organizations deploying eduVPN
- Facilitating “Work from Home” (WFH)

Why eduVPN? (I)

- Easy to integrate in your own infrastructure
  - Just Linux networking
- Multiple authentication mechanisms
  - LDAP, RADIUS, SAML, local, …
- Full IPv6 (and IPv4) support
- Authorization
  - Assigning attribute (values) to VPN "profiles"

Why eduVPN? (II)

- Admin interface
  - View connections, users, configuration, manage users
- Open Source (Free Software)
  - Server *and* apps
- No dependencies on "Big Tech" (infrastructure)
  - *Technological sovereignty*

Why eduVPN? (III)

- Community project tailored specifically to R&E community
- No license fees *at all*
- Scales from a single Raspberry Pi to many core servers with 10GB+ network connectivity
- Host it on premises on your own hardware, or in “the cloud”
- No commercial vendor comes even close to matching eduVPN on costs, reliability, security, privacy and ease of deployment :-)

Who’s using it?

- In Germany (in no particular order)
  - Hochschule Trier, DKRZ, Hochschule Osnabrück, IFW Dresden, University of Augsburg, University of Erfurt, University of Hildesheim, University of Osnabrück
  - Managed by LRZ: Bavarian Academy of Sciences and Humanities, Leibniz Supercomputing Centre, Munich Scientific Network, Technical University of Munich, University of Applied Sciences Munich, University of Munich, Weihenstephan-Triesdorf University of Applied Sciences
- Worldwide
  - 114 servers
  - See https://status.eduvpn.org for a full list

History (I)

```
commit bd61496d2ff6c33d41aaa0b9c768434603e316e3
Author: François Kooman <fkooman@tuxed.net>
Date:   Mon Oct 13 12:09:04 2014 +0200

    initial commit
```

History (II)

Version	Release Date
1.0	2017-07-13
2.0	2019-04-02
3.0	2022-05-25
4.0	2025?

Server – OS Support (2.x)

- Debian >= 10
- EL 7 (CentOS, RHEL)
- Fedora >= 35

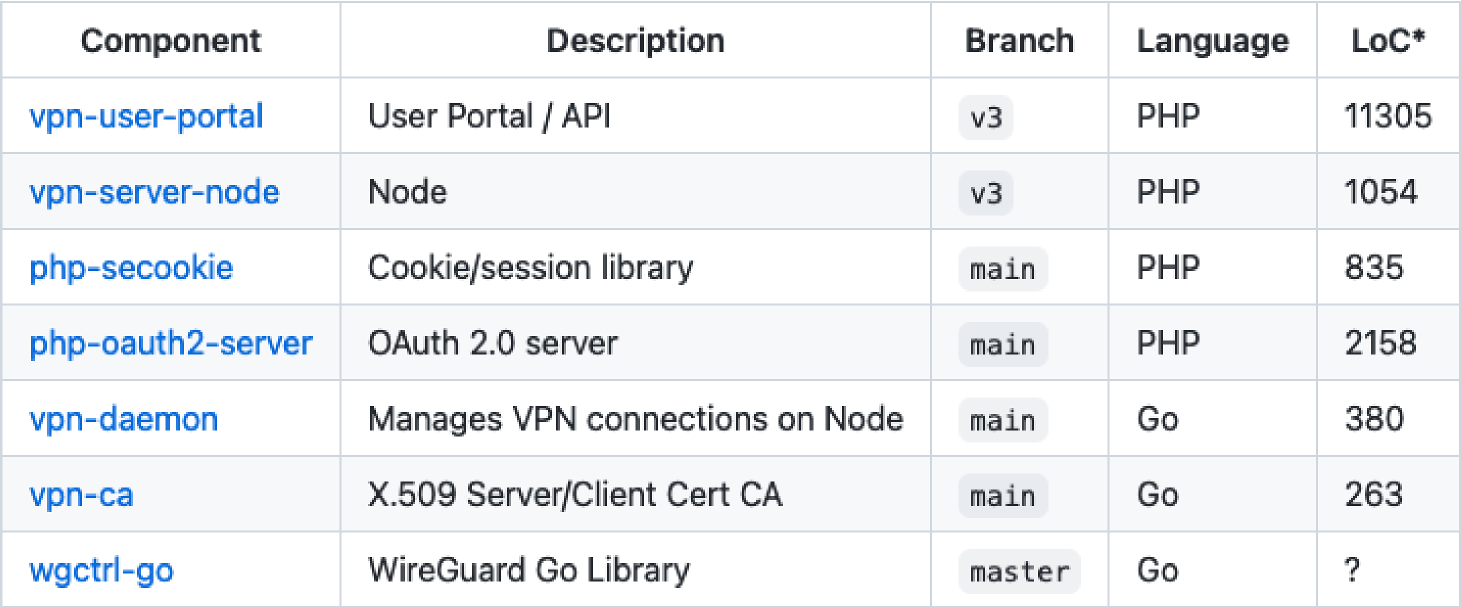
Server – OS Support (3.x)

- Debian >= 11
- EL 9 (AlmaLinux, Rocky Linux, RHEL)
- Ubuntu >= 22.04
- Fedora >= 36

Server “Stack”

- PHP
  - Web interface, API
- Go
  - VPN daemon, X.509 certificate CA

SBOM



Component	Description	Branch	Language	LoC*
vpn-user-portal	User Portal / API	`v3`	PHP	11305
vpn-server-node	Node	`v3`	PHP	1054
php-secookie	Cookie/session library	`main`	PHP	835
php-oauth2-server	OAuth 2.0 server	`main`	PHP	2158
vpn-daemon	Manages VPN connections on Node	`main`	Go	380
vpn-ca	X.509 Server/Client Cert CA	`main`	Go	263
wgctrl-go	WireGuard Go Library	`master`	Go	?

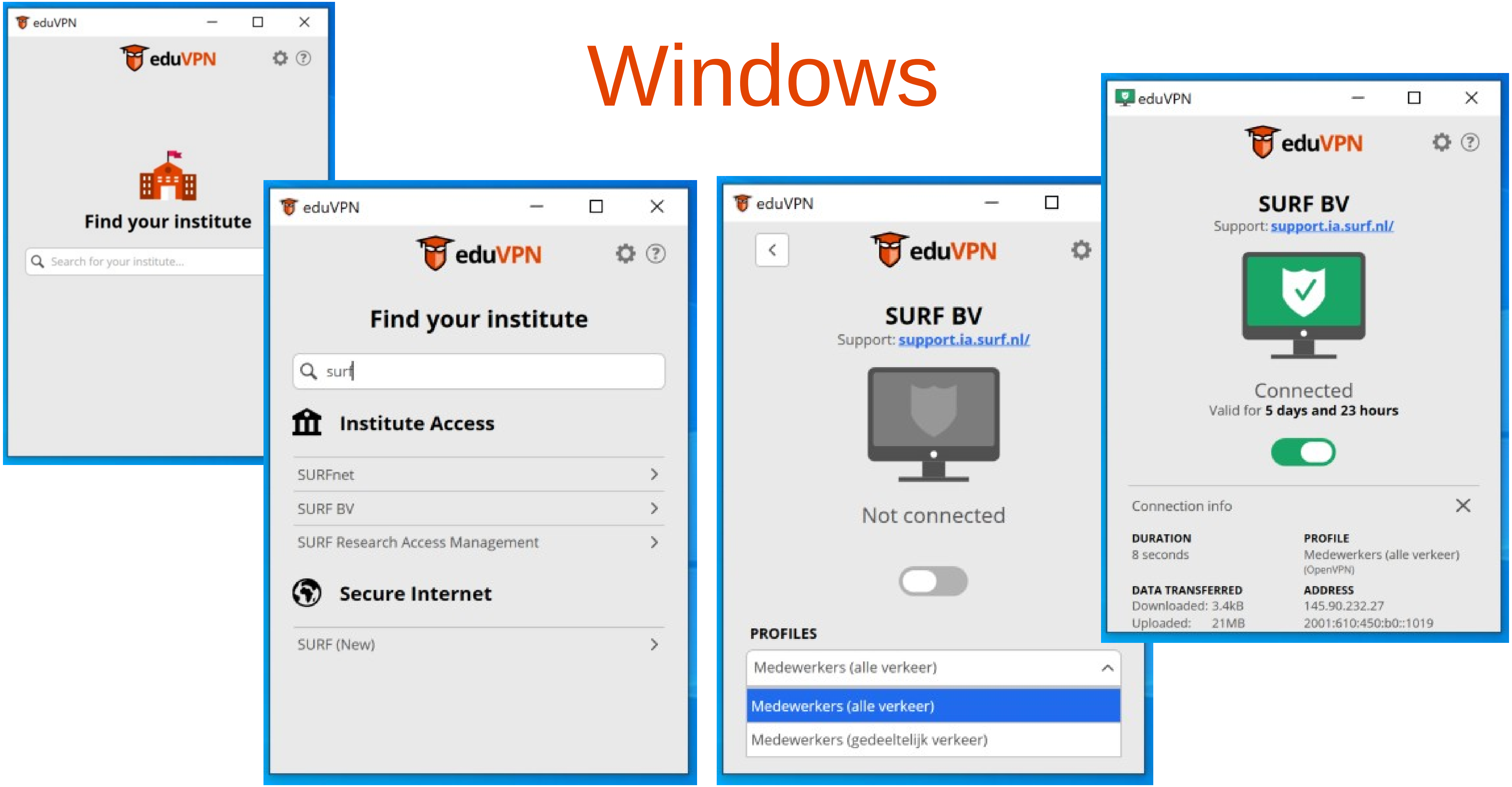
Server – Deployment

- Full extensive documentation provided
- Install on *bare metal*, or in virtual environment
- “Deploy” scripts provided for supported server operating systems
- Updates handled through OS update mechanism (package repository)

Apps – OS Support

- Windows
- macOS
- Android
- iOS
- Linux (NetworkManager)

Windows



Find your institute

Search for your institute...

Find your institute

surf

Institute Access

- SURFnet
- SURF BV
- SURF Research Access Management

Secure Internet

- SURF (New)

SURF BV

Support: support.ia.surf.nl/

Not connected

PROFILES

Medewerkers (alle verkeer)

- Medewerkers (alle verkeer)
- Medewerkers (gedeeltelijk verkeer)

SURF BV

Support: support.ia.surf.nl/

Connected

Valid for **5 days and 23 hours**

Connection info

DURATION
8 seconds

PROFILE
Medewerkers (alle verkeer)
(OpenVPN)

DATA TRANSFERRED
Downloaded: 3.4kB
Uploaded: 21MB

ADDRESS
145.90.232.27
2001:610:450:b0::1019

What is new in 3.0?

- WireGuard VPN protocol (next to OpenVPN)
- Full “HA” deployment
- APIv3
- Limit number of active client connections
- Support OpenID Connect (OIDC)
- Delegated 2FA/MFA to SAML/OIDC IdP
- Lots of refactoring…
  - Reduce dependencies, remove unused features, …

WireGuard (I)

- (Relatively) new VPN Protocol
  - Integrated in Linux/BSD kernels
  - Very simple
  - Modern cryptography
  - High performance

WireGuard (II)

- UDP *only*
  - Does not work on all networks
    - UDP blocked/mangled, MTU issues

→ In 3.x we keep OpenVPN support

WireGuard (III)

- A VPN *profile* can support both OpenVPN and WireGuard at the same time
- A profile can be configured to *prefer* either OpenVPN, or WireGuard

OpenVPN

- Modernize OpenVPN configuration
  - Only Ed25519 for X.509 certificates
  - AES-256-GCM and ChaCha20-Poly1305

API

- Applications use API to talk to VPN server
  - Simplified API to only have 3 calls
    - *Info*
    - *Connect*
    - *Disconnect*
  - Allows app to indicate VPN technology support
- To simplify app development, also made available in 2.x servers

Connection Limits

- To avoid abuse, we allow limiting number of active VPN configurations/connections *per user*
- Apps
  - (default) maximum of 3 active connections, 4th connection will disconnect the oldest one first
- Portal
  - (default) maximum of 3 downloaded configuration files, for a 4th one, one of the previous ones must be deleted first

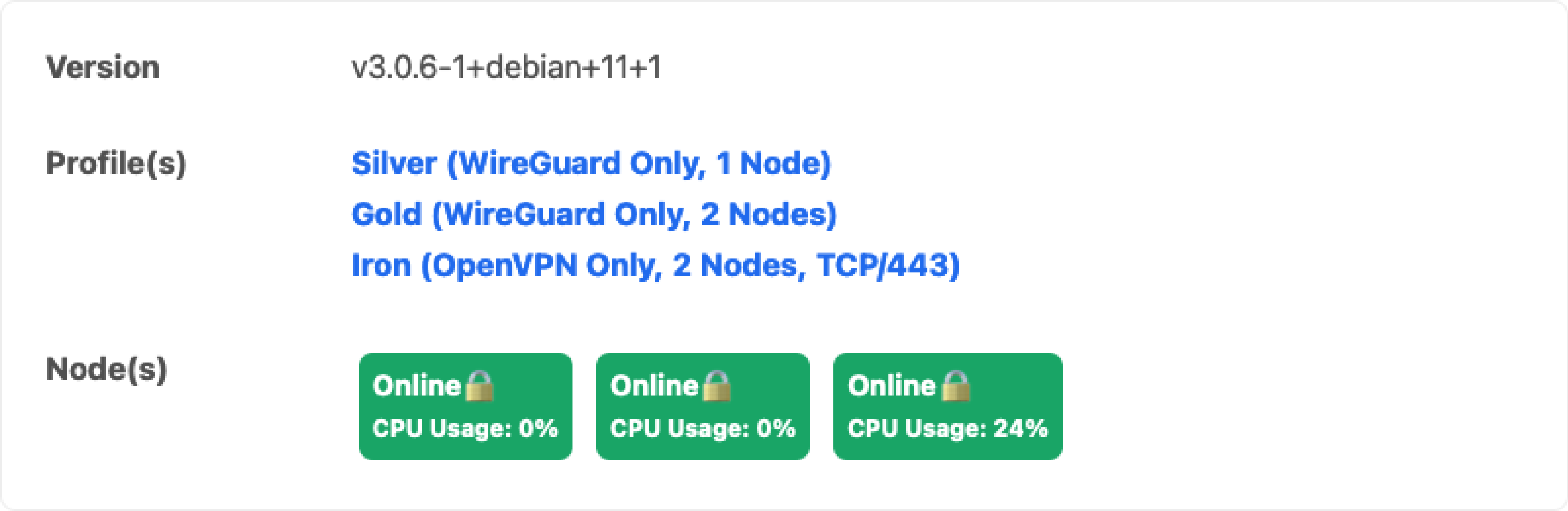
App Authorization

- Update OAuth to 2.1 “draft” specification
  - “refresh tokens” can’t be reused anymore
  - Implement “iss” (RFC 9207)

High Availability (HA)

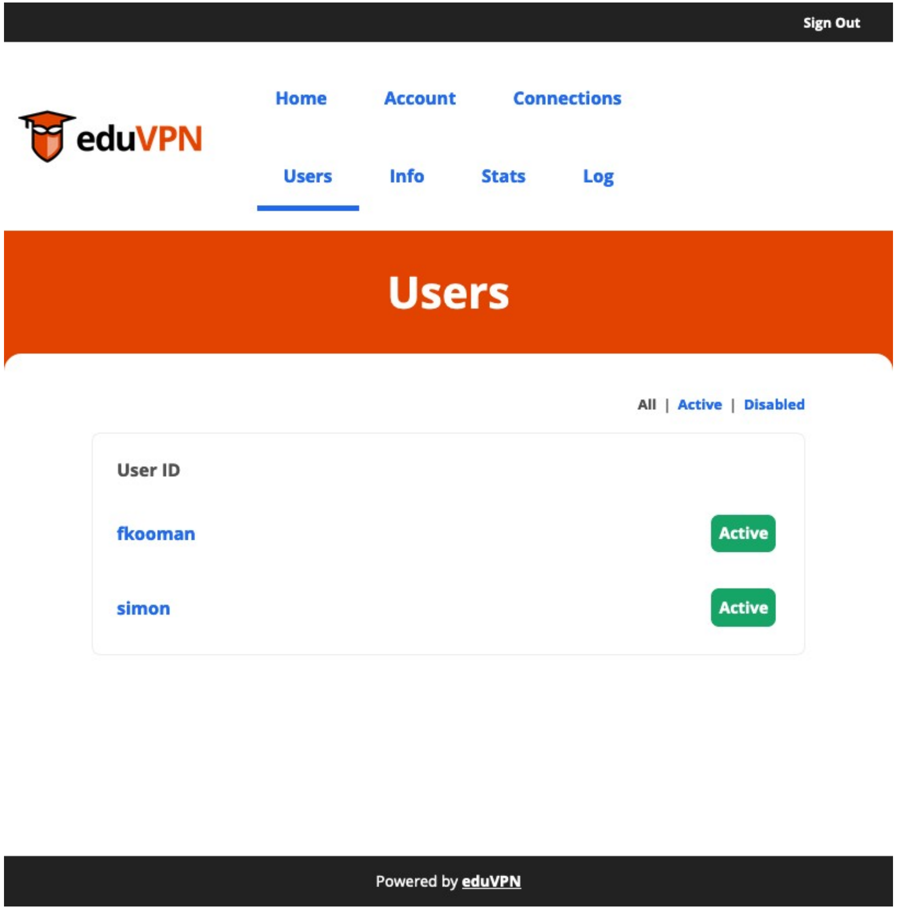
- Multiple *Portals*
  - PostgreSQL, memcached, keepalived
- Multiple *Nodes*
  - Portal determines which node to use
    - Pick at random, but first makes sure node is up

Multi Node



Version	v3.0.6-1+debian+11+1
Profile(s)	Silver (WireGuard Only, 1 Node) Gold (WireGuard Only, 2 Nodes) Iron (OpenVPN Only, 2 Nodes, TCP/443)
Node(s)	Online 🔒 CPU Usage: 0%
	Online 🔒 CPU Usage: 0%
	Online 🔒 CPU Usage: 24%

Admin Interface

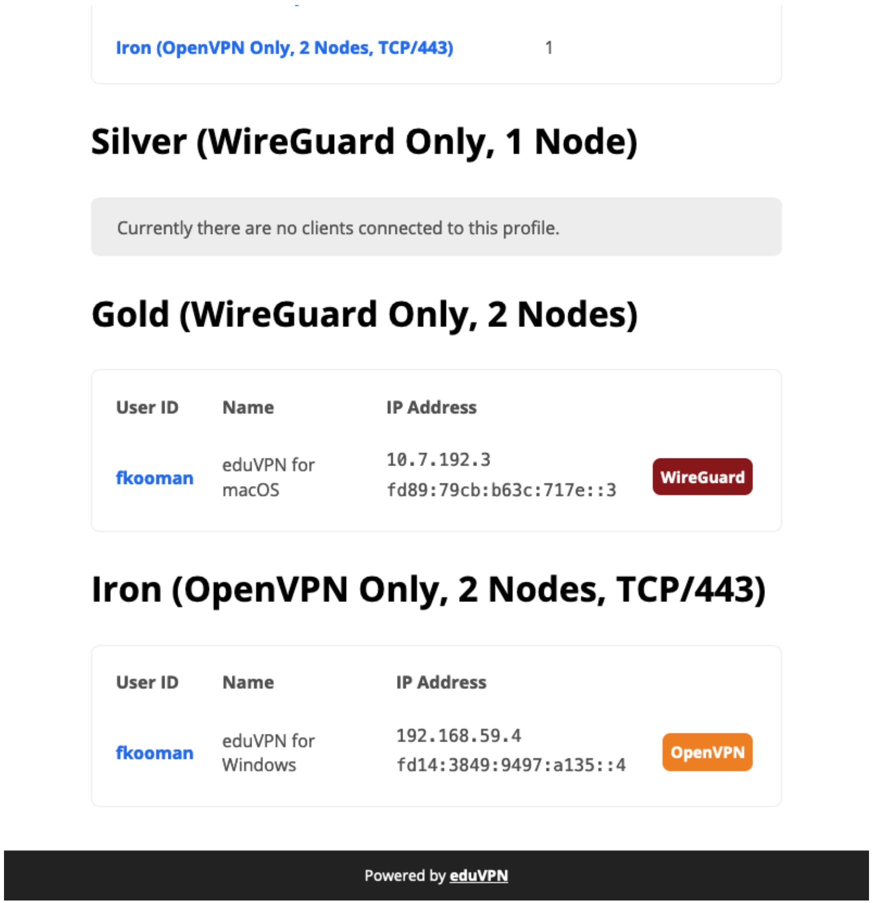


Users

All | Active | Disabled

User ID	
fkooman	Active
simon	Active

Powered by eduVPN



Iron (OpenVPN Only, 2 Nodes, TCP/443)	1

Silver (WireGuard Only, 1 Node)

Currently there are no clients connected to this profile.

Gold (WireGuard Only, 2 Nodes)

User ID	Name	IP Address	
fkooman	eduVPN for macOS	10.7.192.3 fd89:79cb:b63c:717e::3	WireGuard

Iron (OpenVPN Only, 2 Nodes, TCP/443)

User ID	Name	IP Address	
fkooman	eduVPN for Windows	192.168.59.4 fd14:3849:9497:a135::4	OpenVPN

Powered by eduVPN

Profile Configuration

- *Assumption*: users have proper UDP connectivity (true, most of the time for WFH)
  - Deploy with WireGuard as default
  - Offer OpenVPN (TCP) fallback
- *Otherwise*: deploy with OpenVPN as default

Audits

Date	**Type**	**By**
Q4-2016	Server audit	Radically Open Security
Q4-2017	Windows app audit	Fox-IT
Q1-2018	Server audit	Radboud University
Q3-2018	Android app audit	GÉANT
Q4-2018	iOS/macOS app audit	Radically Open Security
Q4-2019	TunnelKit (iOS/macOS) library “fuzzing”	Guido Vranken
Q4-2020	SAML (php-saml-sp) audit	Cure53
Q1-2021	iOS/macOS app audit	Midnight Blue
Q4-2022	3.x Server audit	Cure53

→ Audit documents available on request

Future Development (3.x)

- Improve VPN “online detection” to be able to automatically fallback to OpenVPN+TCP if WireGuard connectivity is broken
- Make WireGuard work over TCP
- Look into properly supporting “duplicate” nodes (failover configuration)
- Integrate shared “eduvpn-common” library in all apps
- “Pre-provisioning”, i.e. have eduVPN client be active before user authenticates
  - When e.g. AD server is behind VPN

Future Development (4.x)

- Drop OpenVPN support
- Store all server/profile configuration in the database
- Allow “user defined” VPNs
  - Create a private network for your own devices/servers (P2P)

Questions?

- eduVPN Team: eduvpn-support@lists.geant.org
- Web: https://www.eduvpn.org
- Me: fkooman@deic.dk
- Deploying eduVPN? https://github.com/eduvpn/documentation

Bonus Slides

- “Secure Internet”
- OAuth

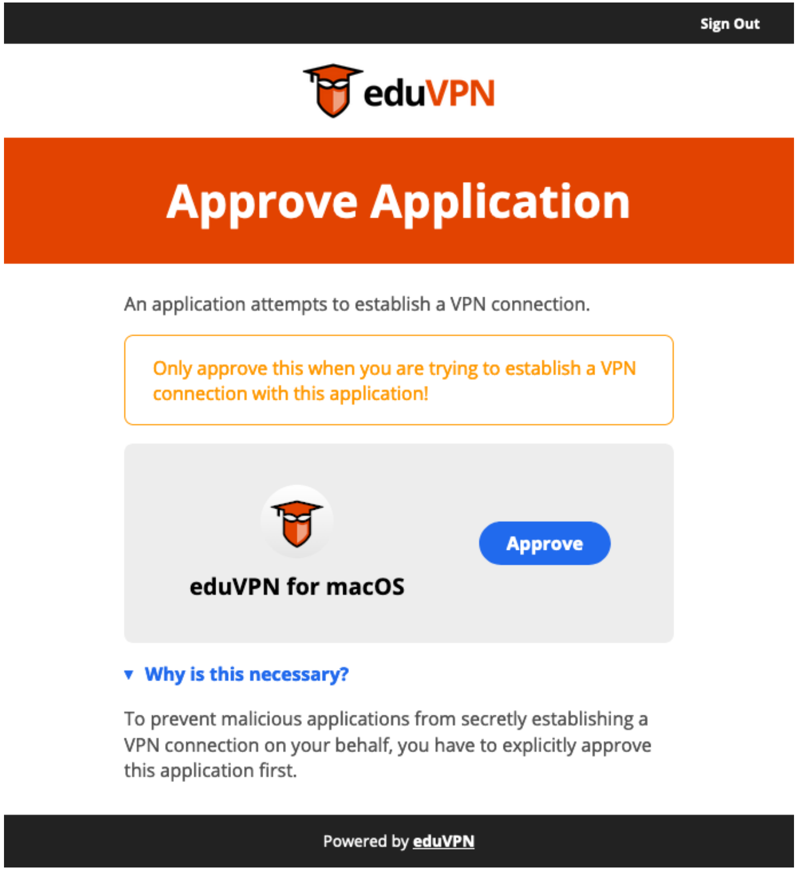
“Secure Internet”

- NREN hosted server, only giving (unfiltered) Internet access
  - No access to “restricted resources”
- If a user has access to one NREN hosted server, they have access to *all* of them
  - For example: authenticate in Germany, use server in Denmark

OAuth

- Mechanism to allow *app* to act on behalf of *user*
- App obtains *token* that can be used to talk to API
- User does NOT authenticate to the app!
- Involves (annoying) excursion to user’s web browser to perform OAuth *authorization* (UX disaster)

OAuth



Approve Application

An application attempts to establish a VPN connection.

Only approve this when you are trying to establish a VPN connection with this application!

eduVPN for macOS

▾ Why is this necessary?

To prevent malicious applications from secretly establishing a VPN connection on your behalf, you have to explicitly approve this application first.

Powered by eduVPN