WORKSHOP GARR 2025

NET MAKERS

eduVPN: una soluzione semplice e sicura per l'accesso remoto

Stefano Claut

Università Ca' Foscari Venezia

Abstract

eduVPN è un progetto coordinato da GÉANT che offre una soluzione per il servizio VPN semplice, sicuro e pienamente integrato con l'infrastruttura digitale degli atenei.

Basato su WireGuard/OpenVPN, eduVPN è una soluzione facile da installare, costantemente aggiornata, scalabile, ben documentata e dotata di client per tutti i principali sistemi operativi.

Dal 2023 l'Università Ca' Foscari Venezia ha adottato eduVPN come unico servizio VPN per tutte le tipologie di utenti, integrandolo con il Single Sign-On d'Ateneo (Shibboleth). In questo modo il sistema eredita l'autenticazione a più fattori, l'accesso tramite CIE/SPID e la gestione automatica delle autorizzazioni associate ai vari profili.

Situazione iniziale

Il servizio VPN, inizialmente utilizzato a Ca' Foscari principalmente per l'accesso remoto alle risorse bibliografiche, è poi evoluto con molteplici profili e finalità diverse (anche per l'accesso alla rete WiFi).

Per tutto questo periodo l'implementazione si è basata su soluzioni proprietarie.

Criticità

- configurazione dei profili complessa, sia lato infrastruttura che lato client
- gestione non banale
- necessità di più di un apparato fisico
- mancanza di integrazione con il sistema MFA di Ateneo

Si è resa necessaria la revisione di tutto il sistema VPN

Soluzione

Riorganizzazione dei profili:

- risorse biblioteca digitale (default, ~40.000 account)
- risorse IT per la ricerca (su richiesta, ~4.000 account)
- accesso IoT (su richiesta, tecnici interni/manutentori esterni)

Progetto coordinato da GÉANT

Sviluppato e mantenuto da SURF per fornire una soluzione VPN open source, sicura, moderna e semplice da gestire.

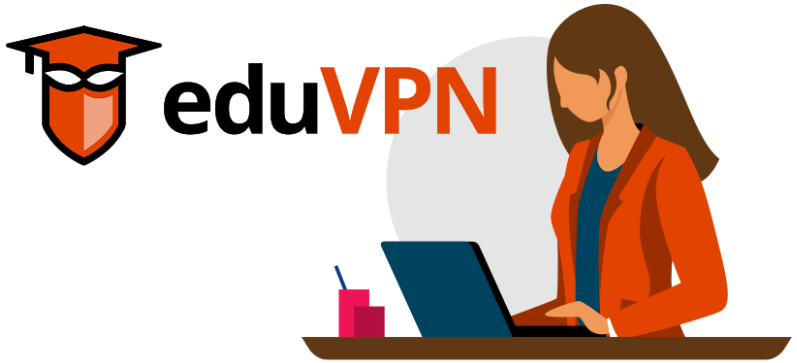
Pensato per università e centri di ricerca

eduVPN

- soluzione multi protocollo che sfrutta diversi componenti già presenti e collaudati nell'ambito opensource come OpenVPN e WireGuard
- installabile e supportata su OS: Debian, Ubuntu, Enterprise Linux
- applicazione client per i principali dispositivi moderni

WireGuard

- semplice e sicuro
- performante
- UDP, con possibilità di usare TCP



Installazione

- inizialmente VM Ubuntu LTS 22.04, poi upgrade a 24.04 LTS
- istruzioni semplici, direttamente dalla documentazione eudvpn.org:

```
$ sudo apt -y install ca-certificates wget
$ wget https://codeberg.org/eduVPN/deploy/archive/v3.tar.gz
$ tar -xzf v3.tar.gz
$ cd deploy
$ sudo -s
# ./deploy_debian.sh
```

- sfrutta soluzioni standard (apache2, php-fpm, nftables)
- aggiornamenti integrati nel sistema di aggiornamento del OS
- principali configurazioni su `/etc/vpn-user-portal/config.php` (dalle ultime release possibile alternativa via JSON)

Configurazione 1/2

- integrazione Shibboleth (SSO di Ateneo)
  - eredita MFA (TOTP gestito su LDAP)
  - accetta SPID/CIE

```
<Location /secure>
    AuthType shibboleth
    ShibRequestSetting requireSession 1
    require shib-attr ou [redacted]
    require shib-attr ou [redacted]
</Location>
```

```
return [
    'styleName' => 'eduVPN',
    'authModule' => 'ShibAuthModule',  // SAML (Shibboleth)
    'ShibAuthModule' => [
        'userIdAttribute' => 'eppn',
        'permissionAttributeList' => ['entitlement'],
        'permissionAttributeList' => ['affiliation'],
        'permissionAttributeList' => ['ou'],
    ],
```

- durata sessioni configurabile (no profile)
- limite connessioni simultanee per user
- opzione TCP, via proxyguard

```
    'sessionExpiry' => 'P5D',
    'Api' => [
        'maxActiveConfigurations' => 3,
    ],
    'WireGuard' => [
        'enableProxy' => true,
        'listenPort' => 51820,
    ],
```

Configurazione 2/2

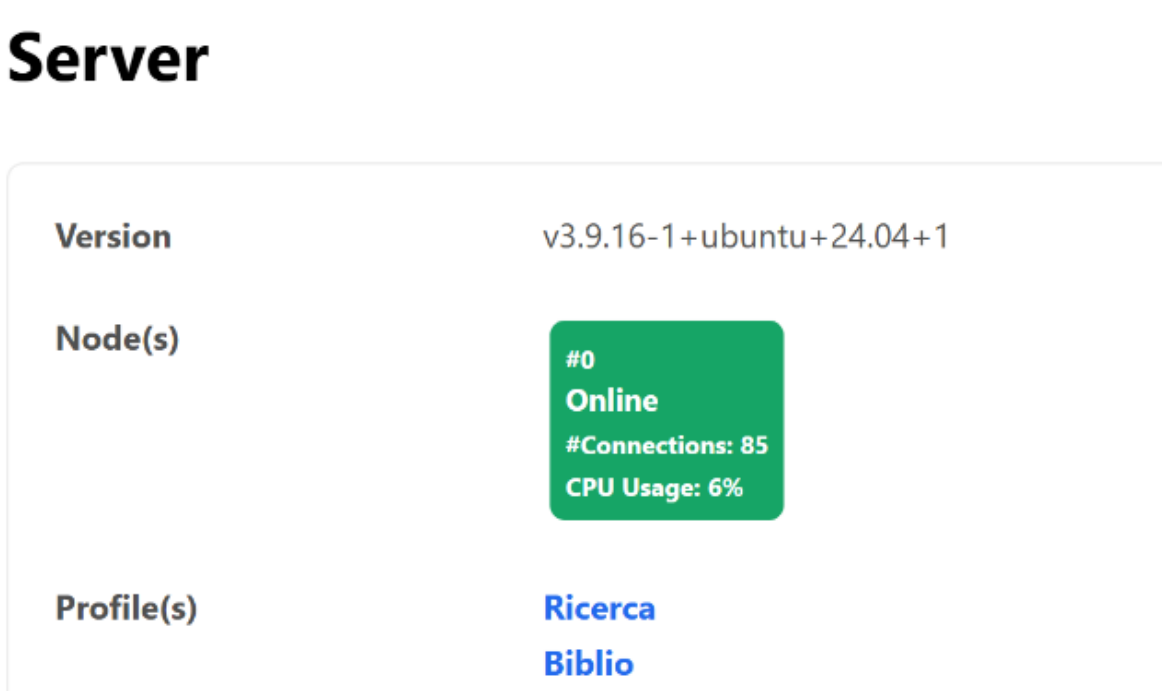
- profilo utente assegnato da attributi SAML ritornati da Shibboleth
- split tunneling / full tunneling

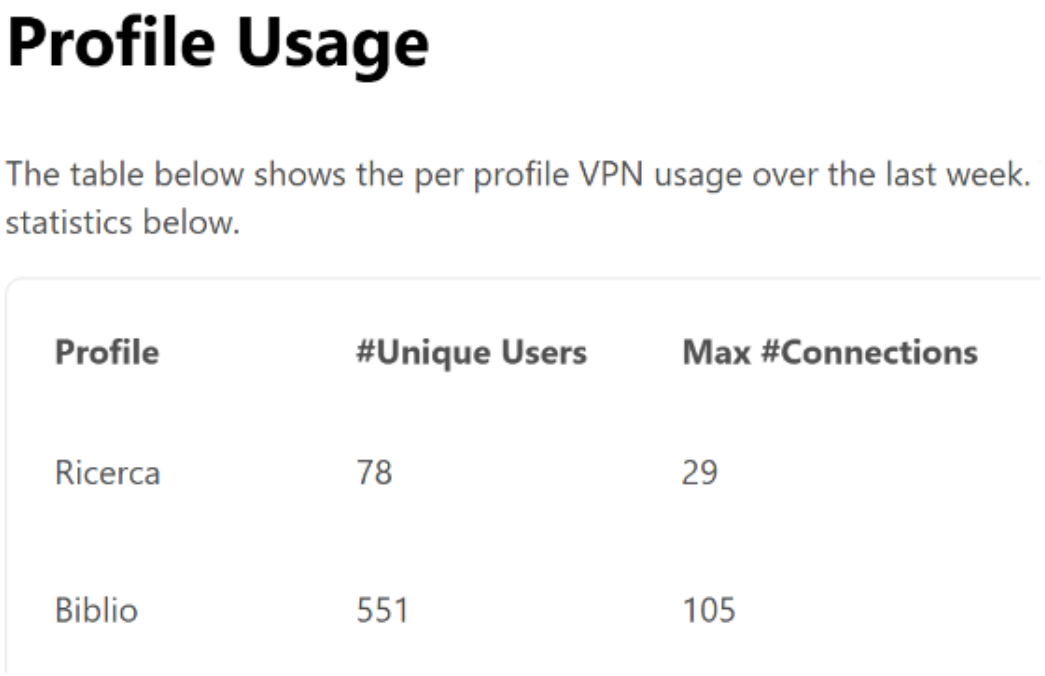
```
'ProfileList' => [
    [
        'profileId' => 'ricerca',
        'displayName' => 'Ricerca',
        'hostName' => 'eduvpn.unive.it',
        'defaultGateway' => false,
        'dnsServerList' => ['157.138.1.8', '157.138.1.9'],
        'dnsSearchDomainList' => ['unive.it'],
        'aclPermissionList' => ['[redacted]'],
        'preferredProto' => 'wireguard',
        'routeList' => ['157.138.[redacted]/24'],
        'wRangeFour' => '157.138.[redacted]/26',
        ...
    ],
```

```
    [
        'profileId' => 'biblio',
        'displayName' => 'Biblio',
        'hostName' => 'eduvpn.unive.it',
        'defaultGateway' => true,
        'dnsServerList' => ['157.138.1.8', '157.138.1.9'],
        'aclPermissionList' => ['[redacted]'],
        'preferredProto' => 'wireguard',
        'wRangeFour' => '157.138.[redacted]/24',
        ...
    ],
```

Dimensionamento

Singola VM (4 vCPU, 4GB RAM) gestita su due data center e migrata in base alle necessità.

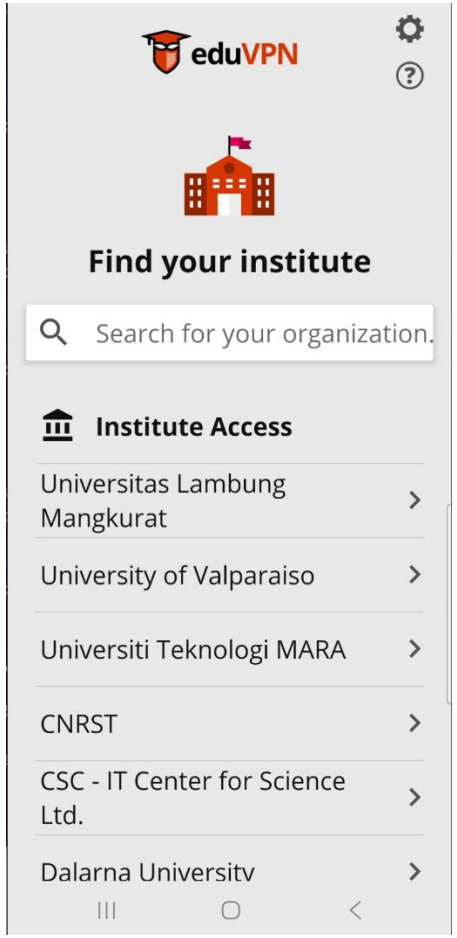


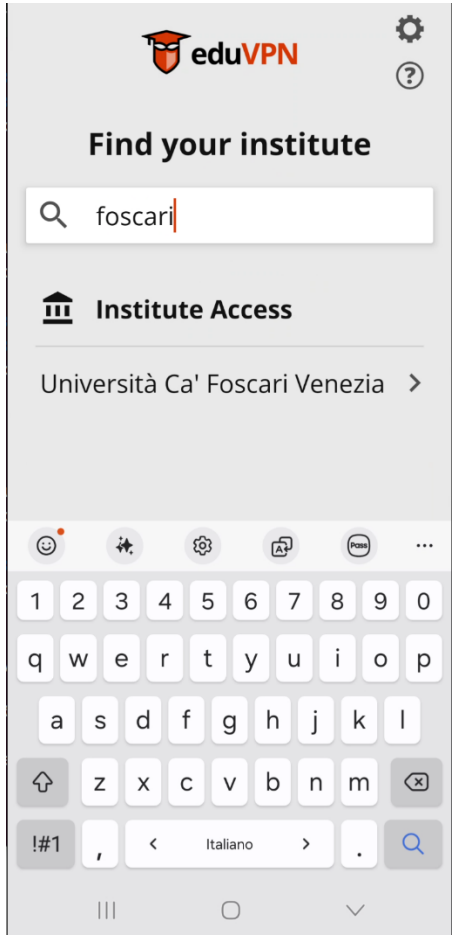


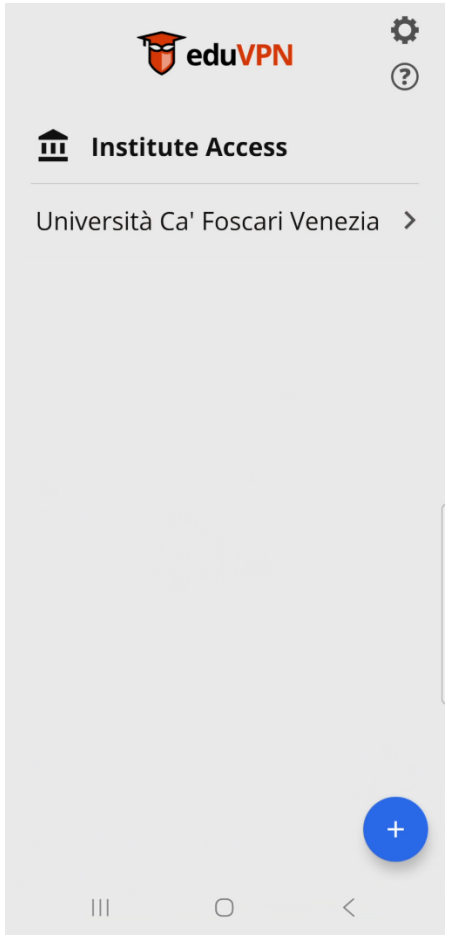
Online

- registrazione «Institute access» su portale eduvpn.org
- client multipiattaforma con configurazione automatica
- configurazione scaricabile per client alternativi (disabilitata)
- migrazione progressiva, ~6 mesi di convivenza con vecchia soluzione

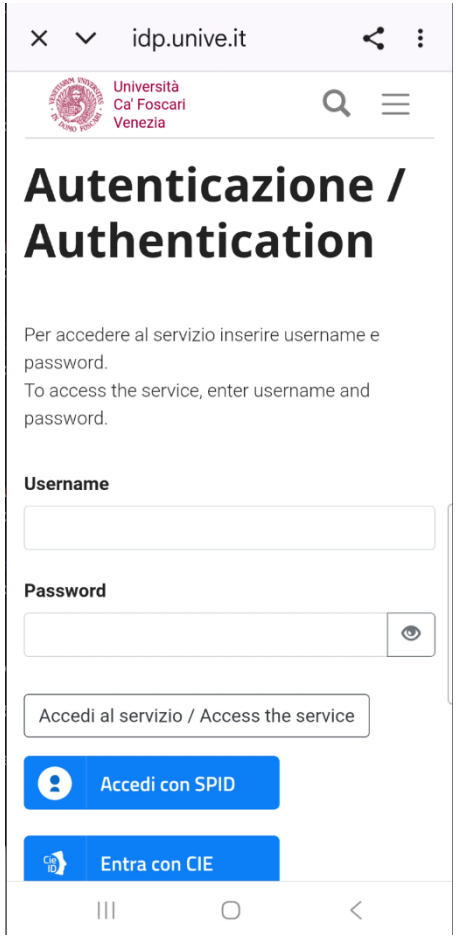
Client 1/2

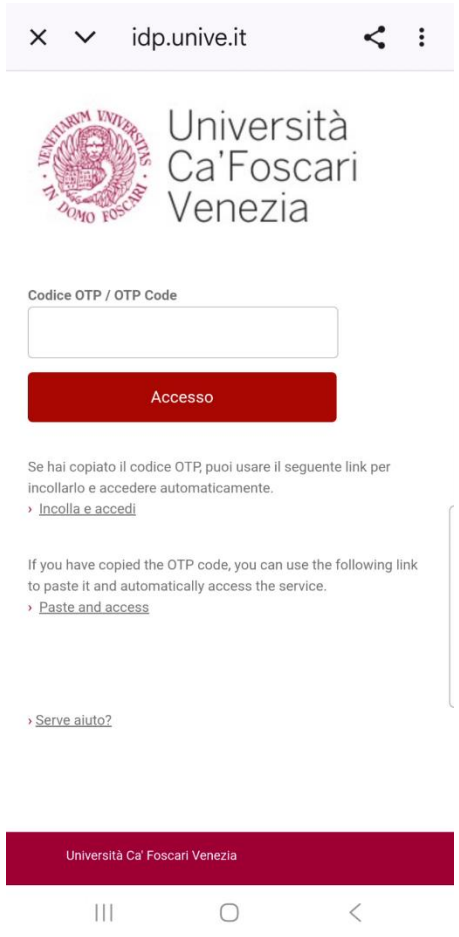

eduVPN
Find your institute
Search for your organization.
Institute Access
Universitas Lambung Mangkurat
University of Valparaiso
Universiti Teknologi MARA
CNRST
CSC - IT Center for Science Ltd.
Dalarna University

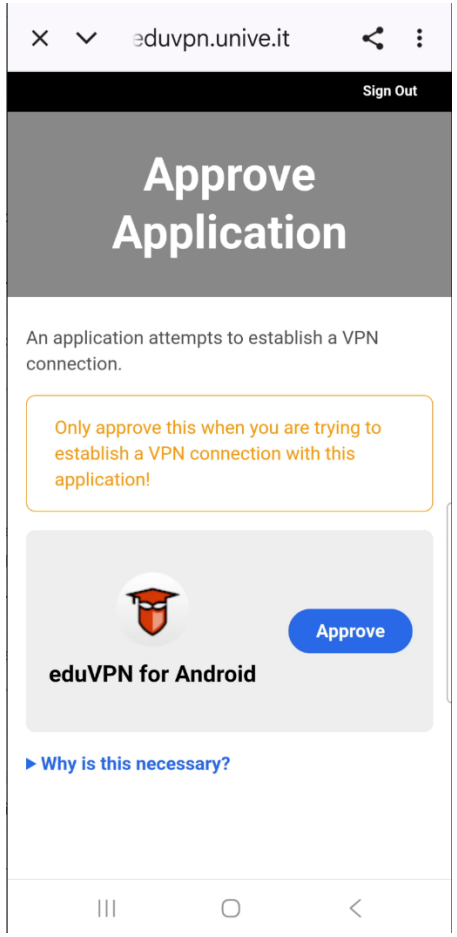

eduVPN
Find your institute
foscari
Institute Access
Università Ca' Foscari Venezia
Italiano

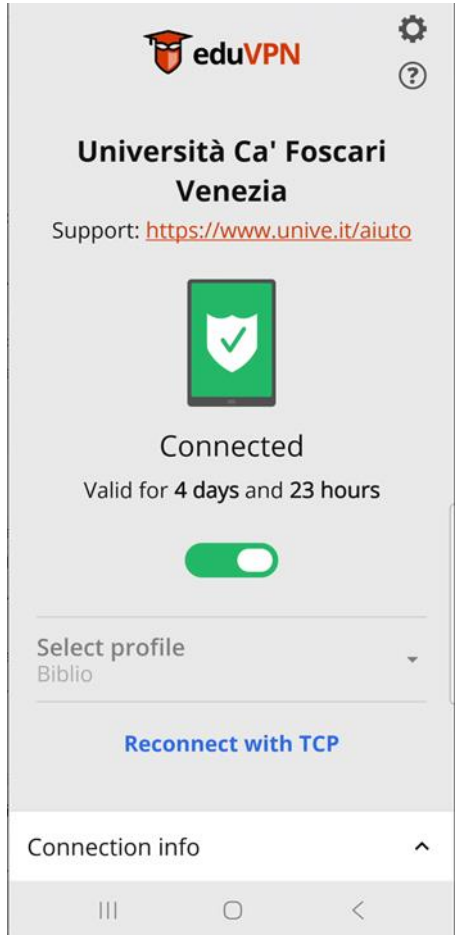

eduVPN
Institute Access
Università Ca' Foscari Venezia

Client 2/2


idp.unive.it
Università Ca' Foscari Venezia
Autenticazione / Authentication
Per accedere al servizio inserire username e password.
To access the service, enter username and password.
Username
Password
Accedi al servizio / Access the service
Accedi con SPID
Entra con CIE


idp.unive.it
Università Ca'Foscari Venezia
Codice OTP / OTP Code
Accesso
Se hai copiato il codice OTP, puoi usare il seguente link per incollarlo e accedere automaticamente.
Incolla e accedi
If you have copied the OTP code, you can use the following link to paste it and automatically access the service.
Paste and access
Serve aiuto?
Università Ca' Foscari Venezia


eduvpn.unive.it
Sign Out
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!
Approve
eduVPN for Android
Why is this necessary?


eduVPN
Università Ca' Foscari Venezia
Support: https://www.unive.it/aiuto
Connected
Valid for 4 days and 23 hours
Select profile
Biblio
Reconnect with TCP
Connection info

Monitoraggio

- interfacce web per carico server, gestione sessioni e ricerca utenti
- log delle connessioni via syslog (diretti a SIEM elastic)

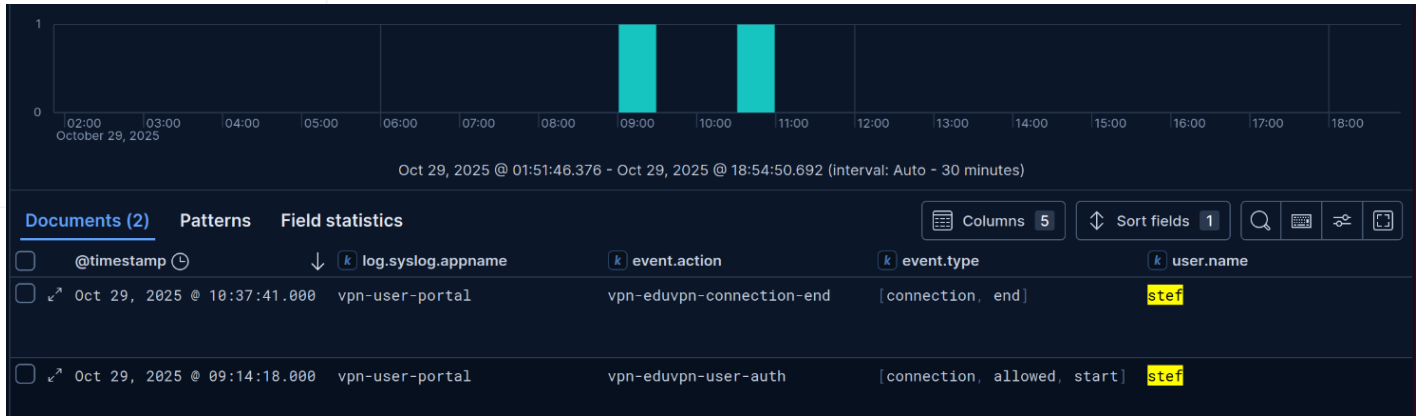
Search

Results

Profile	Biblio
User ID	stef@unive.it
IPs	157.138.[redacted] fc9c:11b5:c7c7:c783::96
Connected	2025-10-29 08:14:18 UTC
Disconnected	2025-10-29 09:37:41 UTC

```
2025-10-29T09:14:18.988485+01:00 eduvpn vpn-user-portal: CONNECT stef@unive.it
(biblio:XaE8irx9lOzvdC3r9QLHotlDBV11SAL9p+YWyAP5+yg=) [* =>
157.138.[redacted],fc9c:11b5:c7c7:c783::96] [AUTH_DATA=]

2025-10-29T10:37:41.707838+01:00 eduvpn vpn-user-portal: DISCONNECT stef@unive.it
(biblio:XaE8irx9lOzvdC3r9QLHotlDBV11SAL9p+YWyAP5+yg=)
```



Risultati

- gestione del server integrata con la gestione delle altre VM (update, backup, HA/DR, log, …)
- scalabile con aggiunta di altre VM dedicate
- facile configurazione dei profili
- assegnazione dei profili integrata nella gestione account
- integrazione con MFA
- azzeramento dei ticket di supporto per la configurazione del client
- soluzione valida per accesso a servizi online soggetti a restrizioni geografiche e/o da paesi con restrizioni locali sulla rete internet

Domande?

wooclap.com
Codice: WSGARR25

Grazie per l’attenzione

stefano.claut@unive.it
Università Ca’ Foscari Venezia

WORKSHOP GARR 2025
NET MAKERS