

VPN

English Version

Per accedere dall'esterno alle risorse della rete d'Ateneo, si utilizza **GlobalProtect** di Palo Alto Networks.

Per motivi di sicurezza, l'accesso alla VPN è consentito solo da client che supportino il set minimo di requisiti di sicurezza:

- Windows: OS Supportato (Windows 8.1 o Windows 10), aggiornamenti automatici attivi, antivirus installato
- MacOSX: OS Supportato (OSX Versione 10.13 o successive), aggiornamenti automatici attivi
- Linux: Aggiornamenti automatici attivi

Dispositivi e sistemi operativi supportati

Il traffico verso internet continuerà ad uscire dalla connessione preesistente (ADSL di casa, altra università, wifi pubblico, ecc...) mentre solo il traffico verso la rete d'Ateneo verrà instradato nel tunnel (modalità **Split Tunnel**).

Qualora sul computer sia già installato il client GlobalProtect di PaloAlto, è possibile aggiungere un secondo profilo di connessione seguendo le istruzioni al seguente link: [Aggiunta nuovo profilo VPN](#).

Download, installazione e prima configurazione

per [Linux](#) e [dispositivi mobili](#) vedi le sezioni dedicate

Windows e MAC

Per MAC OS Catalina vedi le [note](#) a piè di pagina.

Per l'uso della VPN è necessario installare il client GlobalProtect. E' possibile farlo in due modi:

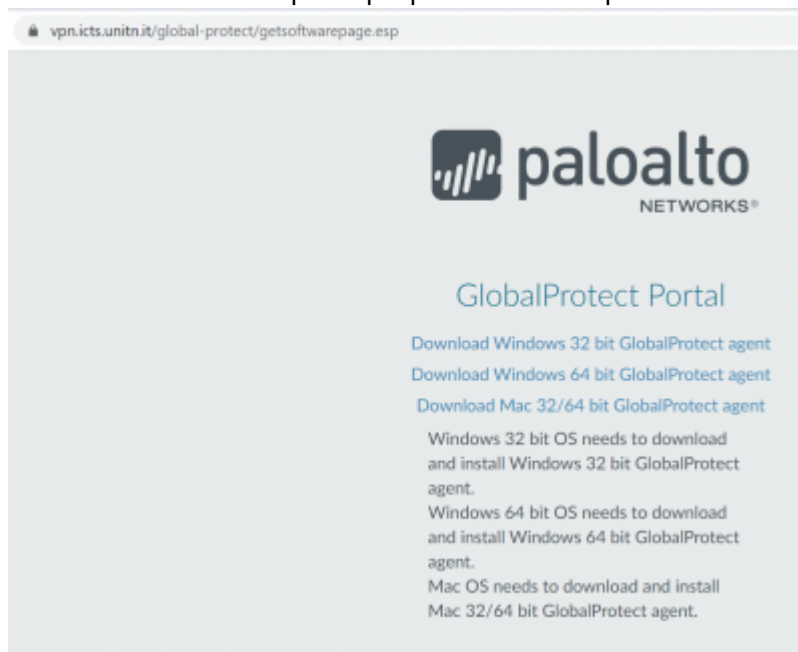
1. collegarsi all' url <https://vpn.icts.unitn.it>

- effettuare il login con le credenziali di Ateneo



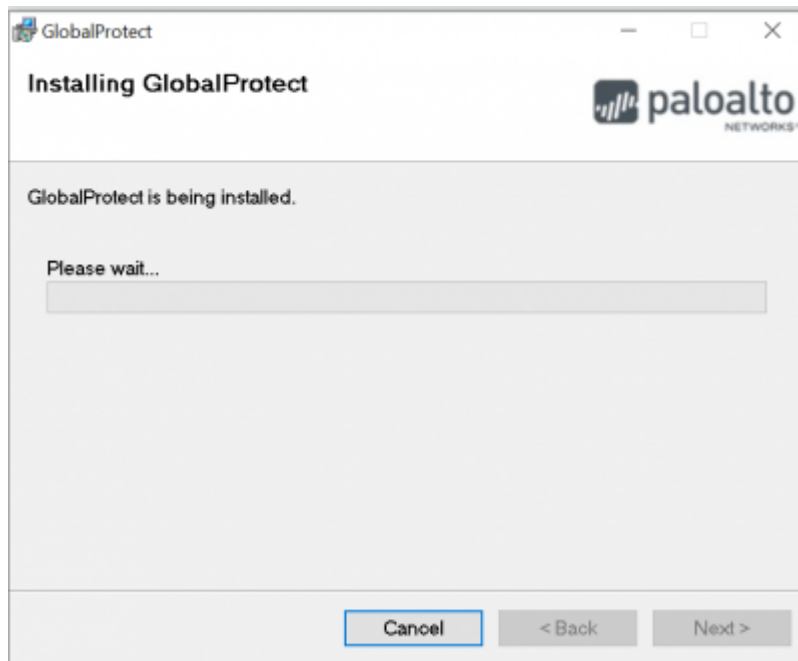
The screenshot shows the login page of the Palo Alto GlobalProtect Portal. The URL in the browser's address bar is `vpn.icts.unitn.it/global-protect/login.esp`. The page features the Palo Alto Networks logo at the top. Below the logo, the text "GlobalProtect Portal" is displayed. There are two input fields: "Name" with the value "nome.cognome@unitn.it" and "Password" with masked characters. A "LOG IN" button is located below the password field.

- scaricare la versione per il proprio Sistema Operativo



The screenshot shows the software download page of the Palo Alto GlobalProtect Portal. The URL in the browser's address bar is `vpn.icts.unitn.it/global-protect/getsoftwarepage.esp`. The page features the Palo Alto Networks logo at the top. Below the logo, the text "GlobalProtect Portal" is displayed. There are three download links: "Download Windows 32 bit GlobalProtect agent", "Download Windows 64 bit GlobalProtect agent", and "Download Mac 32/64 bit GlobalProtect agent". Below these links, there is a section of text providing instructions for each operating system: "Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.", "Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.", and "Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent."

- lanciare l'esecuzione del file appena scaricato e completare l'installazione con le opzioni di default



2. in alternativa è possibile scaricare direttamente da qui il client per il proprio Sistema Operativo ed installarlo

GlobalProtect Download	Note
Windows 7/8/10 (64bit) GlobalProtect	
Windows 7/8/10 (32bit) GlobalProtect	
MACOSX GlobalProtect	Nota per MacOS Catalina

Dopo aver effettuato l'installazione procedere con la prima configurazione (dopo l'installazione il client GlobalProtect parte in automatico):

- nel campo *Portal* inserire **vpn.icts.unitn.it**

GlobalProtect 




Welcome to GlobalProtect

Please enter your portal address

vpn.icts.unitn.it

Connect

- cliccare *Connect*, inserire le credenziali UNITN e poi cliccare su *Sign In*

GlobalProtect 

Sign In

Enter login credentials

Portal: vpn.icts.unitn.it

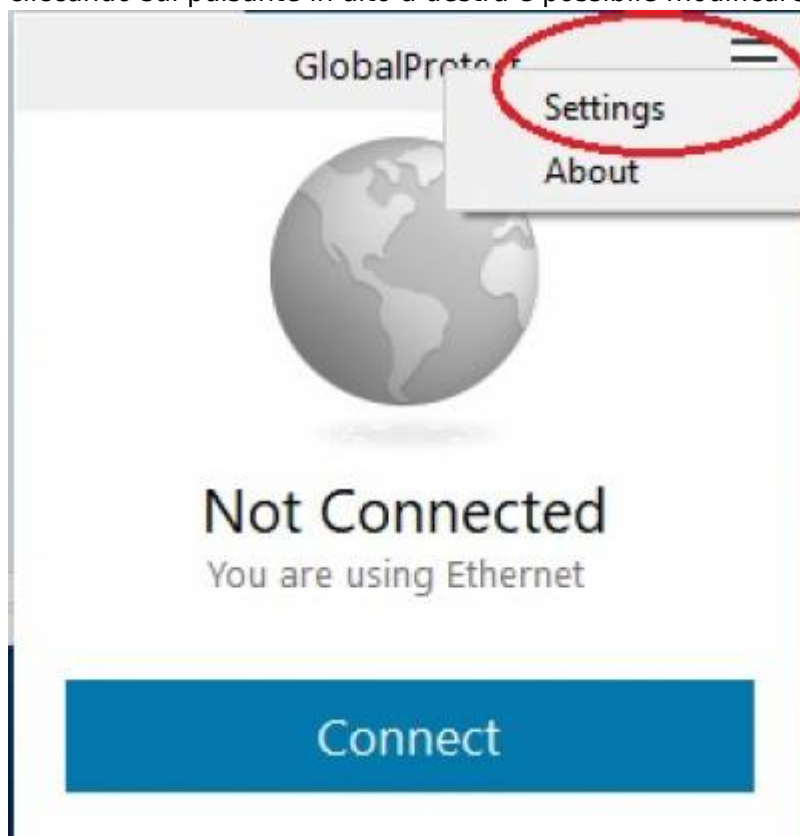
user.name@unitn.it

Password

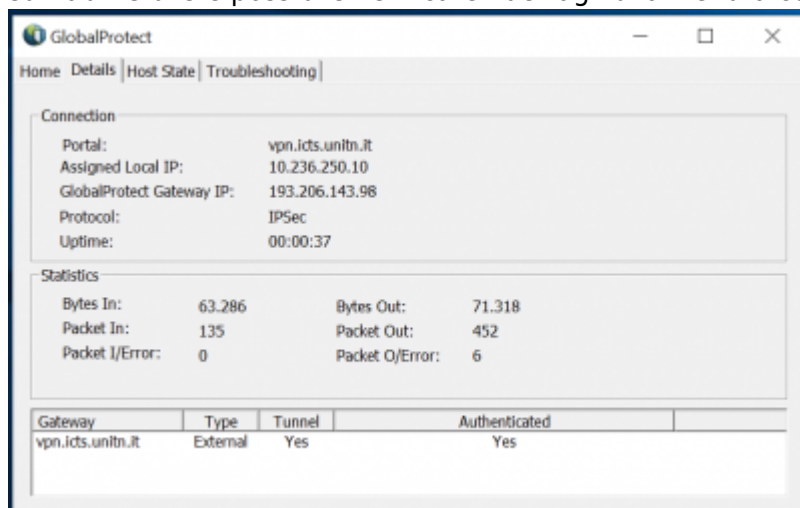
Sign In

Cancel

- attendere che lo Status diventi “Connected”; ora è possibile accedere alle risorse della rete di Ateneo
- cliccando sul pulsante in alto a destra è possibile modificare le impostazioni del client (*Settings*)



- sul tab *Details* è possibile verificare i dettagli di avvenuta connessione



Linux (CentOS, RedHat, Ubuntu)

Scaricare il client GlobalProtect

GlobalProtect Download	Note
Linux GlobalProtect v 5.2.3	
Linux GlobalProtect v 5.3.1	CentOS/RHEL 8

Dopo aver scaricato il pacchetto, estrarre i file con il comando:

```
tar xzfv PanGPLinux-5.2.3-c10.tgz
```

A questo punto è possibile decidere se installare la versione CLI (la VPN verrà attivata da riga di comando) oppure la versione con interfaccia grafica.

Per la versione CLI, procedere con i seguenti comandi (relativi alla propria distribuzione linux):

Debian/Ubuntu

```
dpkg -i GlobalProtect_deb-5.2.3.0-10.deb
```

CentOS/RedHat

```
rpm -ivh GlobalProtect_rpm-5.2.30-10.rpm
```

Dopo l'installazione è possibile utilizzare il comando **globalprotect**.

Per collegarsi:

```
globalprotect connect --portal vpn.icts.unitn.it --username  
user.name@unitn.it
```

Per disconnettersi:

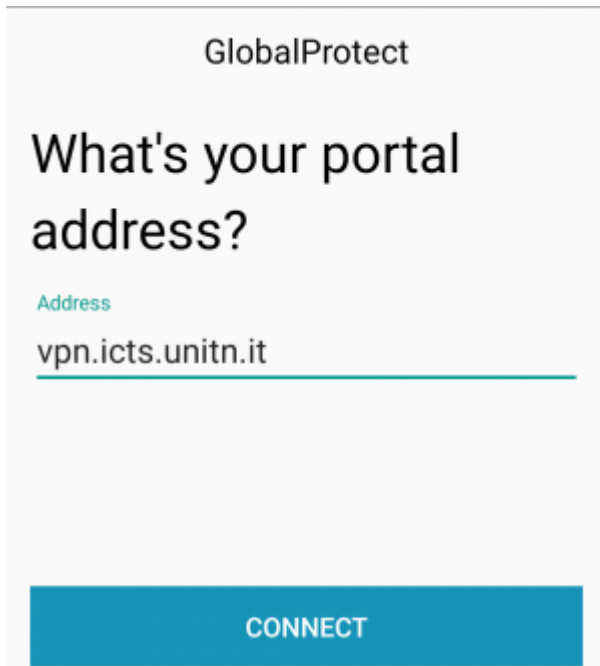
```
globalprotect disconnect
```

Per ulteriori approfondimenti e per l'installazione della versione con interfaccia grafica rimandiamo alle istruzioni del produttore [Istruzioni installazione dal sito Palo Alto](#)

Dispositivi mobili

Per dispositivi mobili scaricare l'app *GlobalProtect* di Palo Alto Networks dal proprio App Store (Android/iOS)

- Scaricare il client tramite Play/App Store, cercando “globalprotect”
- lanciare la app, nella sezione portal inserire *vpn.icts.unitn.it*



GlobalProtect

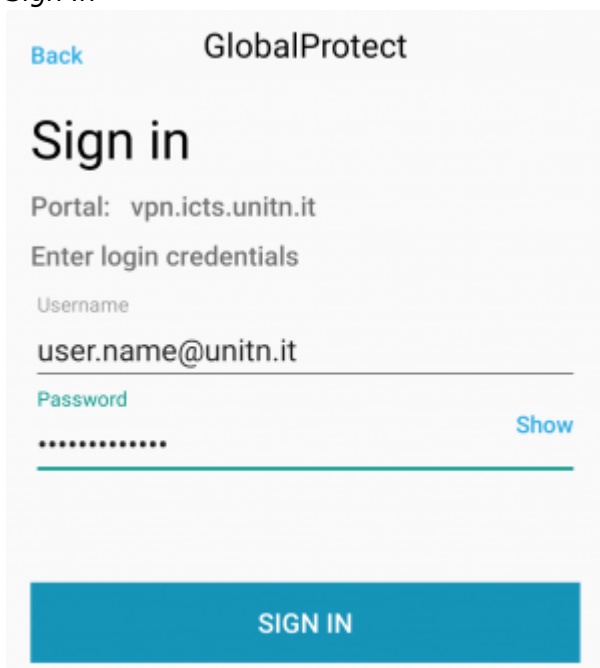
What's your portal address?

Address

vpn.icts.unitn.it

CONNECT

- Quando richiesto, inserire le proprie credenziali in formato *user.name@unitn.it* e cliccare su *Sign In*



Back GlobalProtect

Sign in

Portal: vpn.icts.unitn.it

Enter login credentials

Username

user.name@unitn.it

Password [Show](#)

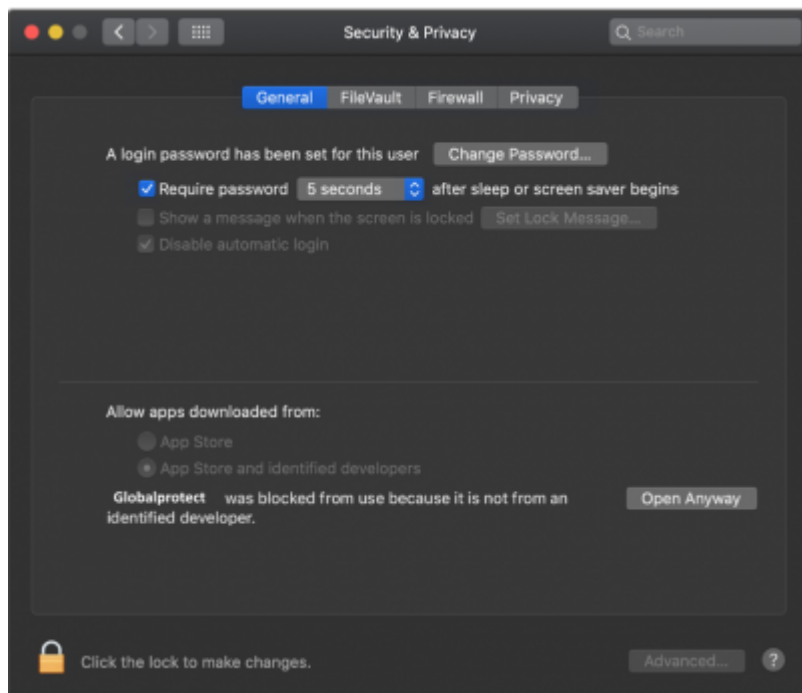
.....

SIGN IN

NOTE

MAC OS Catalina

NB: ci hanno segnalato che in MacOS Catalina, per riuscire a stabilire la connessione, può essere necessario autorizzare manualmente l'applicazione andando in: Impostazioni —> Sicurezza e Privacy —> Generale come da immagine qui sotto e cliccare su “Apri Comunque”



Ritorna alla sezione [Download, installazione e prima configurazione](#)

Risorse bloccate

Gli utenti che si collegano in vpn con sistemi operativi non aggiornati non potranno accedere alle seguenti risorse interne:

alessandria1.unitn.it 192.168.206.42

nx-trento.unitn.it 192.168.132.11

nx-collina.unitn.it 192.168.123.6 192.168.123.5

fluidfs-prod.unitn.it 192.168.123.11

fluidfs-prod2.unitn.it 192.168.123.19 192.168.123.18

f87.unitn.it 192.168.187.25 f85.unitn.it 192.168.187.26

From:

<https://wiki.unitn.it/> - **Wiki UniTn**

Permanent link:

<https://wiki.unitn.it/pub:conf-vpn-paloalto?rev=1639643144>

Last update: **2021/12/16 08:25**

