



UNIVERSITÀ
DEGLI STUDI
DI TORINO

unito.it

L'UNIVERSITÀ DI TORINO ON LINE

VPN UNITO GLOBAL PROTECT

versione 1 | 07-2018

Direzione
Sistemi Informativi,
Portale, E-learning

VPN UNITO: cos'è e perché usarla

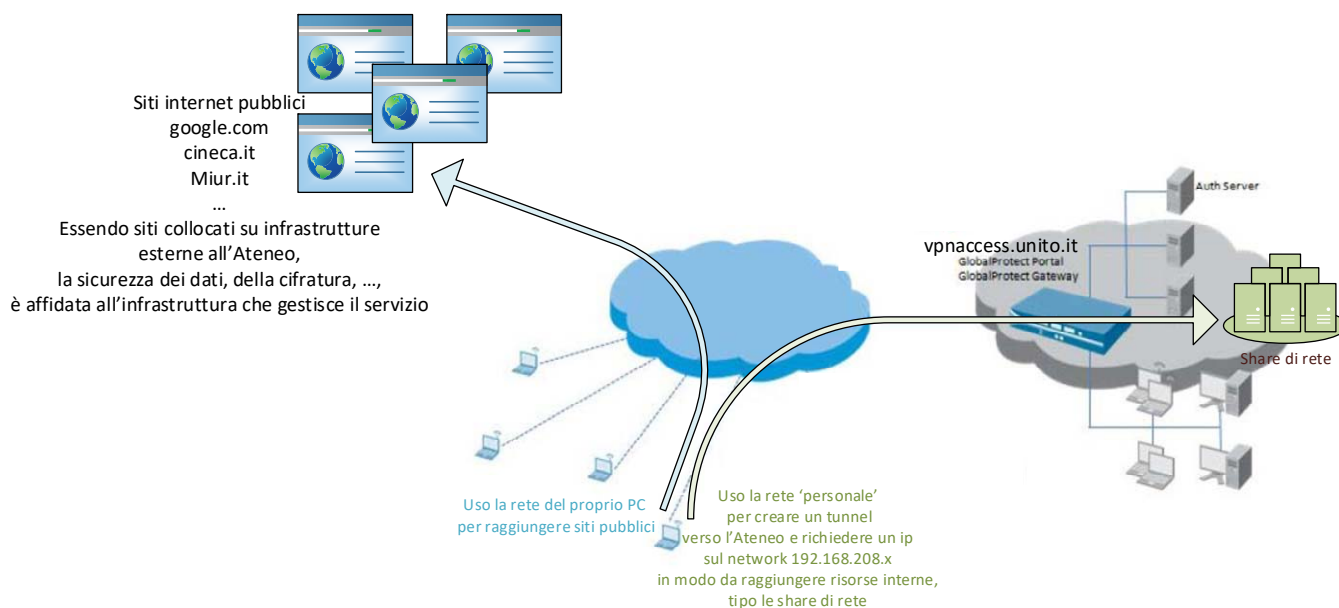
La VPN o Virtual Private Network è un particolare tipo di connessione che permette a un client (come ad esempio il proprio computer di casa o il proprio tablet) di collegarsi in modo sicuro alle risorse presenti all'interno della rete informatica dell'Ateneo. Normalmente a queste risorse è possibile accedere solo se ci si collega da postazioni che sono fisicamente connesse all'interno della rete di Unito, ma tramite una connessione VPN è possibile accedere anche se il client o device utilizzato è connesso a una rete esterna.

Una rete VPN garantisce la sicurezza rispetto ai dati scambiati durante la connessione utilizzando sistemi di codifica opportuni. Inoltre, il servizio VPN di Ateneo richiede l'autenticazione degli utenti tramite le credenziali SCU, si basa su regole di accesso in modo da garantire l'utilizzo ai soli dipendenti e assicura un maggiore livello di affidabilità.

Tutti gli accessi saranno definiti da regole di carattere generale impostate dalla Direzione Sistemi Informativi Portale e E-learning di Ateneo con lo scopo di rendere utilizzabile il servizio con un livello di accesso base, che ci si augura possa rispondere alla maggior parte delle esigenze degli utenti.

La VPN di Ateneo si basa sulla soluzione VPN Global Protect di Palo Alto.

Il device connesso in VPN, tramite l'applicazione Global Protect, utilizzerà un indirizzo IP di Unito per collegarsi alle risorse interne all'Ateneo e manterrà quello originale quando dovrà navigare su Internet o utilizzare le risorse della sua rete locale (domestica o aziendale che sia).



Direzione Sistemi Informativi, Portale, E-learning

Via Verdi, 8 - 10124 Torino - Tel. +39 011.6702037 - Fax. +39 011/2364478 - 011/6709111
e-mail: spo@unito.it

Questa modalità di connessione è valida solo per i dispositivi su cui è possibile installare il client Global Protect messo a disposizione da Palo Alto (tutti i device con sistemi operativi Windows e Mac a 32 e 64 bit, come verrà illustrato nel dettaglio nelle pagine seguenti del documento).

Il servizio VPN è implementato e gestito dalla Sezione Networking e dalla Sezione Sistemi dell'Area Infrastrutture ICT della Direzione Sistemi Informativi, Portale e E-Learning di Ateneo.

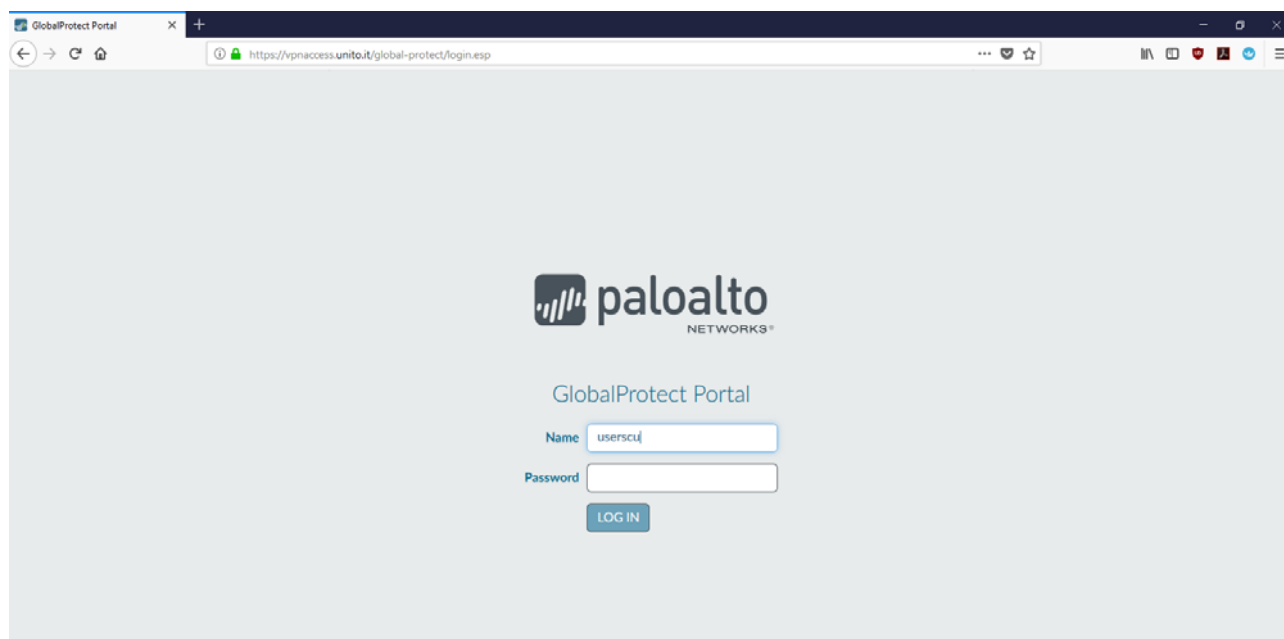
Per eventuali segnalazioni o richieste di informazioni inerenti con questo servizio si invita ad aprire un ticket tramite il service Desk di Ateneo, disponibile al link <https://help.unito.it/> selezionando la voce VPN (Virtual Private Network).

1. SISTEMI OPERATIVI WINDOWS E MAC

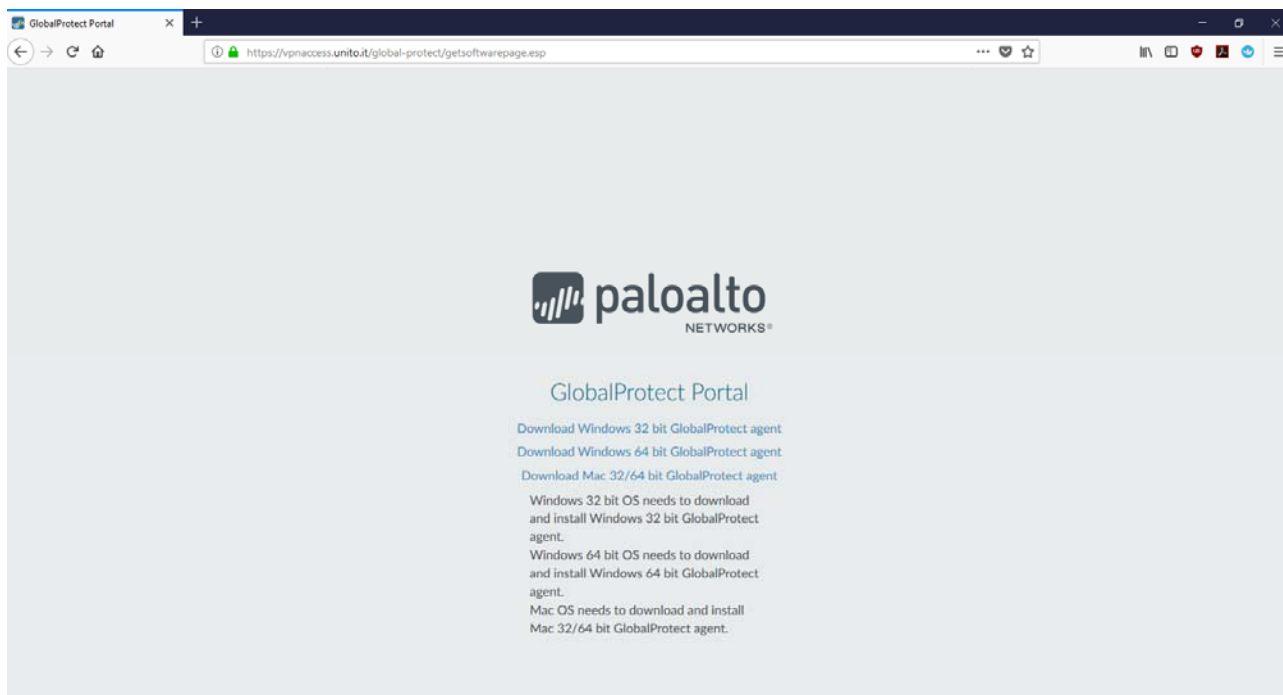
Per i sistemi operativi Windows e Mac a 32 e 64 bit è disponibile un applicazione o agent dedicato denominato Global Protect che facilita la configurazione e la gestione della VPN di Ateneo. L'agent VPN attiva in automatico uno *split tunnel*, grazie al quale, mentre la connessione VPN è attiva, soltanto il traffico diretto verso l'Ateneo passerà attraverso la connessione VPN, mentre tutto il resto del traffico utilizzerà la connessione originale del dispositivo dell'utente (quale ad esempio la connessione domestica nel caso in cui ci si stia collegando da casa).

1.1. Download dell'agent

Per poter scaricare l'agent GlobalProtect è necessario aprire un browser e digitare l'url <https://vpnaccess.unito.it>






Nella pagina che si presenterà bisognerà inserire le credenziali SCU, cliccare su “LOG IN” e scegliere il pacchetto da scaricare più indicato al sistema operativo in uso sul proprio dispositivo (Windows 32 o 64 bit oppure Mac 32/64 bit).



1.2. Installazione dell'agent

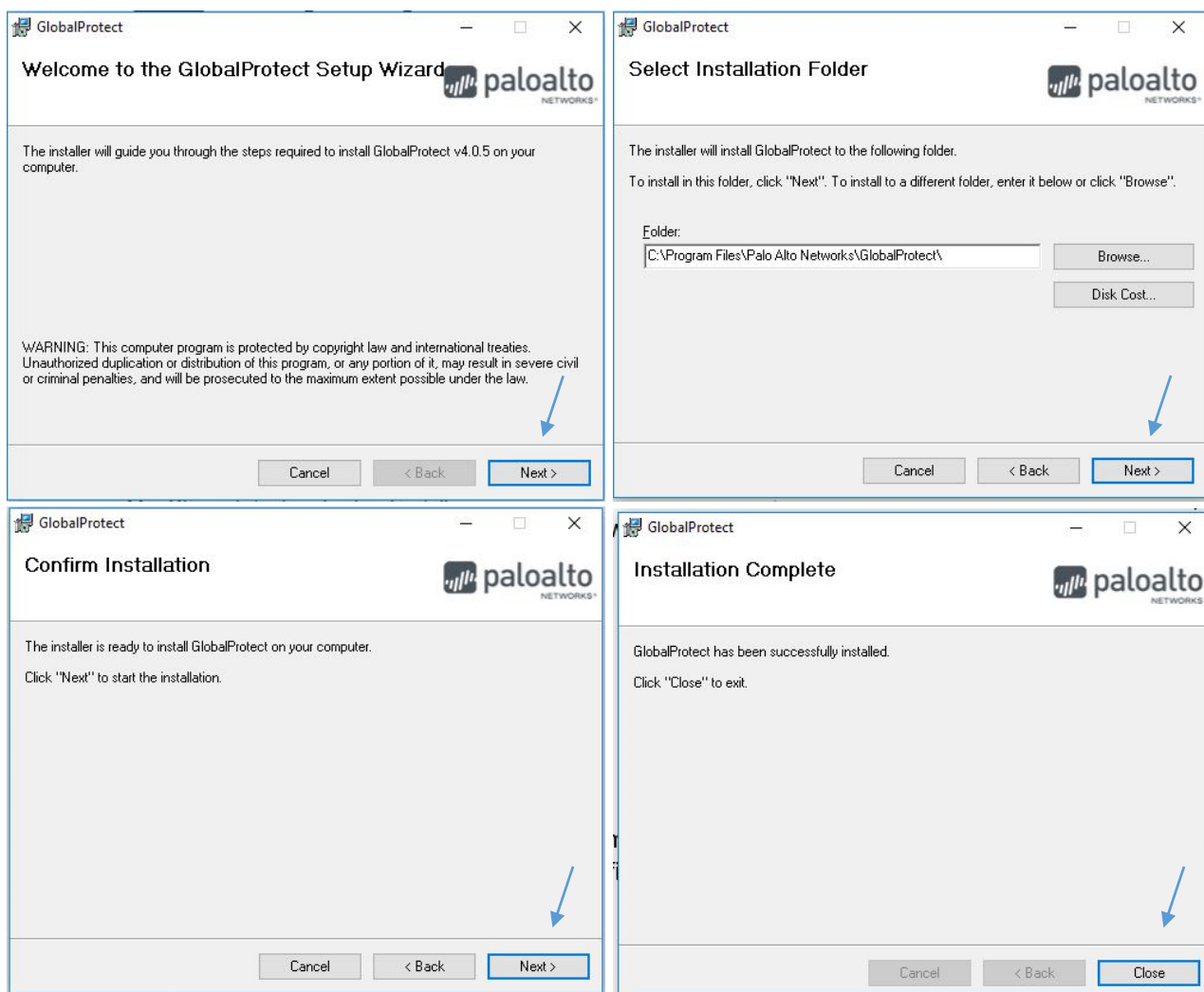
Dopo aver terminato il download, aprire la cartella dove è stato scaricato il file.

All'interno della directory troverete uno dei seguenti file (il nome varia in base al tipo di pacchetto scaricato).

 GlobalProtect.msi
 GlobalProtect.pkg
 GlobalProtect64.msi

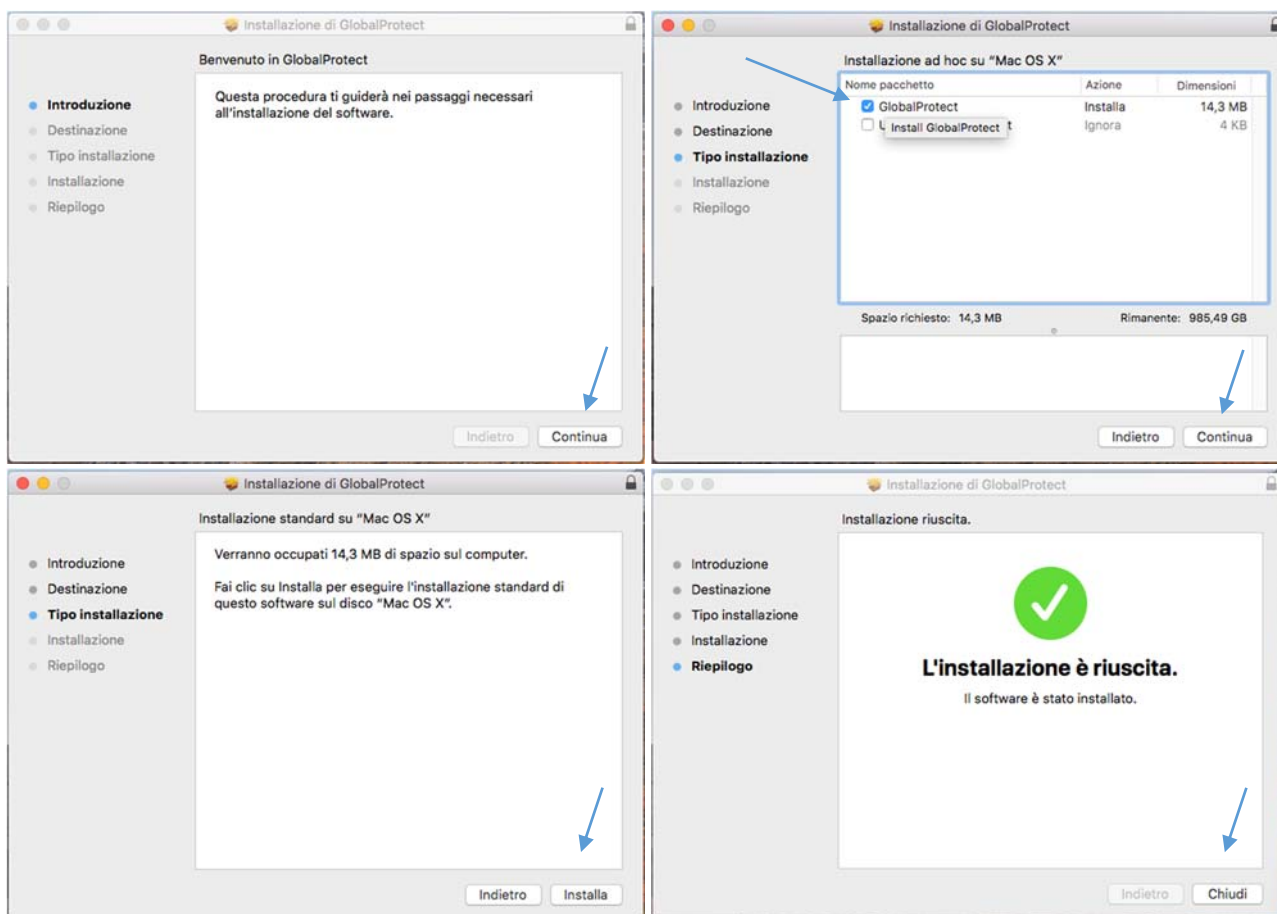
Lanciare l'installazione eseguendo un doppio click sul file GlobalProtect e procedere con l'installazione secondo le modalità standard proposte direttamente dal software, illustrate nelle pagine seguenti.

1.2.1. Installazione Windows



Attenzione: tra la videata di *“Confirm Installation”* e *“Installation Complete”* verrà visualizzato un pop-up di Windows all’interno del quale si dovrà cliccare *“SI”* per poter autorizzare il software a scrivere sui registri del sistema. Diversamente l’installazione non andrà a buon fine.

1.2.2. Installazione Mac



Attenzione: tra la videata di "Installazione standard su Mac OS X" e "Installazione riuscita" verrà visualizzato un pop-up come questo



dove sarà necessario inserire le credenziali di un amministratore della macchina e cliccare su "Installa software". Diversamente l'installazione non andrà a buon fine.

1.3. Configurazione dell'agent

Terminata l'installazione, se l'applicazione non si è aperta automaticamente,

su Windows: fare doppio click con il tasto sinistro del mouse sull'icona di "GlobalProtect"



che si trova nella barra di stato in basso a destra (probabilmente sarà necessario cliccare su "Mostra icone nascoste").

su Mac: cliccare sull'icona "GlobalProtect"  che si trova nelle Applicazioni.

A questo punto configurare la VPN inserendo nel riquadro bianco "Portal":
vpnaccess.unito.it.

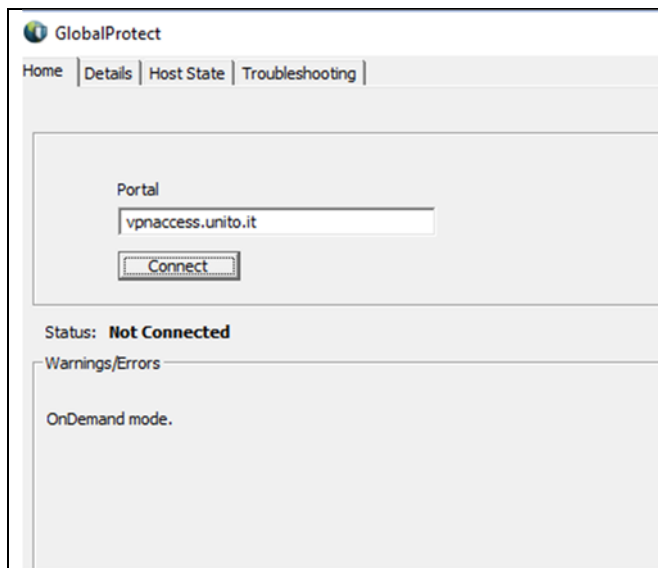


Figura 1- Sistema Operativo Windows

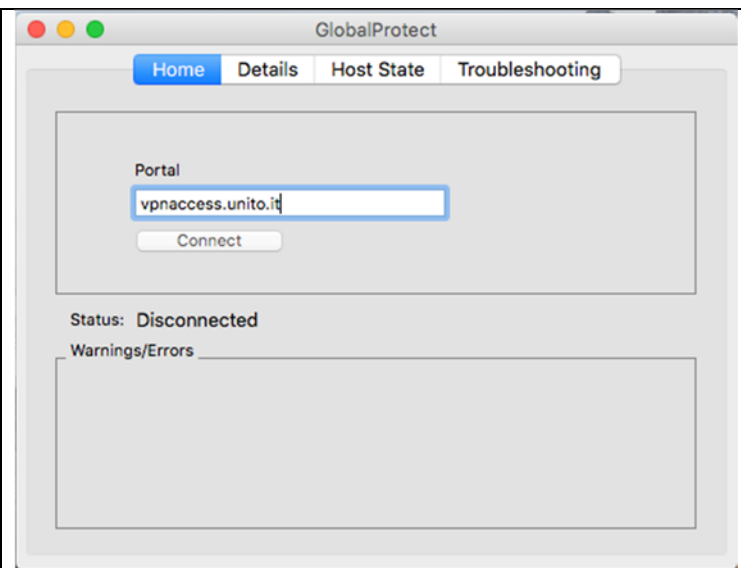
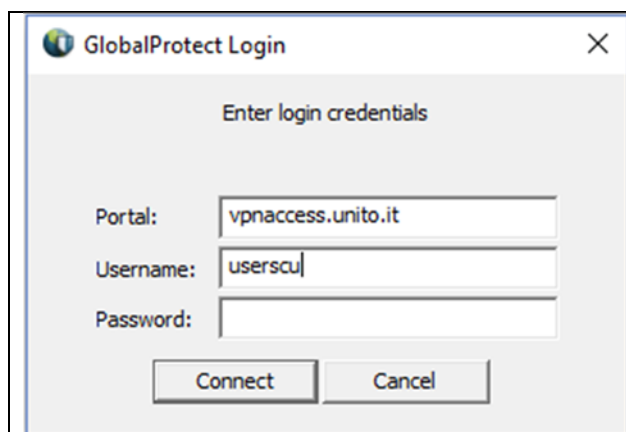


Figura 2- Sistema Operativo Mac

Per collegarsi alla VPN cliccare su "Connect" e inserire le proprie credenziali SCU.



GlobalProtect Login

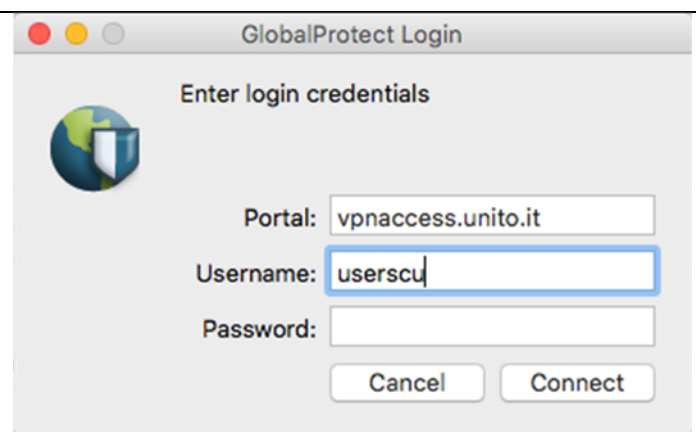
Enter login credentials

Portal: vpnaccess.unito.it

Username: userscu

Password:

Connect Cancel

Figura 3- Login Sistema Operativo Windows

GlobalProtect Login

Enter login credentials

Portal: vpnaccess.unito.it

Username: userscu

Password:

Cancel Connect

Figura 4- Login Sistema Operativo Mac

2. INSTALLAZIONE E CONFIGURAZIONE VPN UNITO SU SISTEMI OPERATIVI LINUX

I sistemi operativi Linux non utilizzano l'agent Global Protect di Palo Alto disponibile per Windows e Mac.

Per utilizzare la VPN occorre installare alcuni software e configurare la connessione VPN.

Si prende ad esempio il caso in cui si utilizzi l'ambiente desktop Gnome.

É necessario installare prima i pacchetti ***vpnc - network-manager-vpnc - vpnc-scripts - network-manager-vpnc-gnome***

Ad esempio, su Ubuntu, è possibile installare questi pacchetti usando il comando:

```
sudo apt-get install vpnc network-manager-vpnc vpnc-scripts network-manager-vpnc-gnome
```

Per verificare se i pacchetti sopra citati sono stati installati correttamente o se siano già installati occorre lanciare il comando:

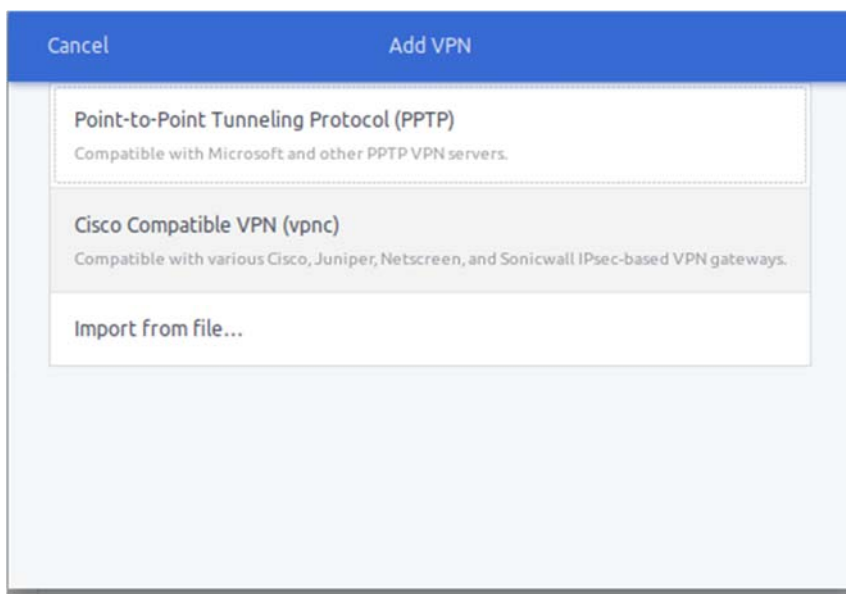
```
apt list --installed | grep vpnc
```

Se sono installati l'output dovrebbe essere simile a questo:

```
network-manager-vpnc/bionic-updates,bionic-security,now 1.2.4-6ubuntu0.1 amd64 [installed]  
network-manager-vpnc-gnome/bionic-updates,bionic-security,now 1.2.4-6ubuntu0.1 amd64 [installed]  
vpnc/bionic,now 0.5.3r550-3 amd64 [installed]  
vpnc-scripts/bionic,bionic,now 0.1~git20171005-1 all [installed]
```

Dopo l'installazione dei pacchetti è necessario aggiungere una *VPN connection* cliccando sul simbolo della rete.

Scegliere VPN-Connections → VPN Configuration → Add → Cisco VPN-Client (vpnc) (o Cisco Compatible VPN)



Procedere con la configurazione come riportata sotto, mettendo come *Group name* e *Group password* "vpnunito" (senza virgolette).

3. CONFIGURAZIONE VPN UNITO PER SISTEMI ANDROID E APPLE

Sugli app store delle piattaforme Android e Apple è disponibile l'app di GlobalProtect di Palo Alto. Attualmente l'Ateneo non ha ancora deciso di dotarsi di tale app e, di conseguenza, per attivare una connessione VPN dai dispositivi mobile Android e Apple occorre utilizzare e configurare manualmente il client VPN integrato presente su questi sistemi.

ATTENZIONE: vale quanto indicato in precedenza per i sistemi operativi Linux e cioè che con questo tipo di configurazione la funzionalità di "*split tunnel*" non verrà attivata, per tanto tutto il traffico passerà attraverso la connessione VPN di Ateneo.

Nelle pagine seguenti viene descritto come configurare manualmente i dispositivi mobili su piattaforma Android e Apple.

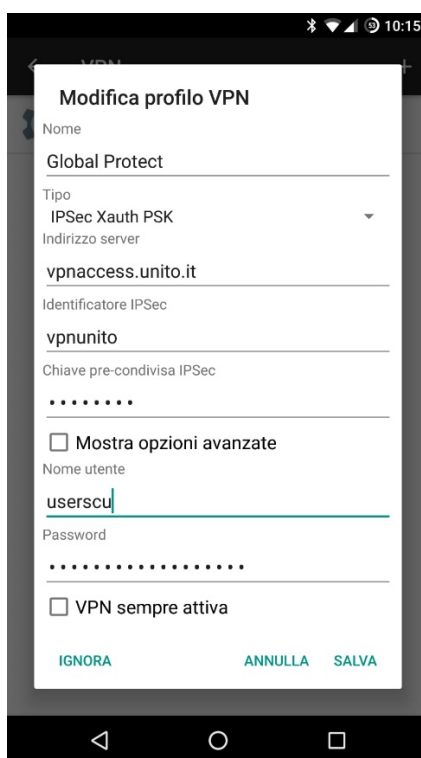
3.1. Android

ATTENZIONE: le immagini seguenti si riferiscono a una particolare versione di Android installata su uno specifico modello di smart phone, per tanto potrebbero differire a seconda della versioni di Android in uso e del modello di smart phone utilizzato.

Tipicamente, sui sistemi Android la configurazione VPN si trova al seguente percorso:

Impostazioni → Nella sezione relativa alla connettività scegliere Altro → VPN → Aggiungi rete VPN

Arrivati questo punto configurare come riportato nella figura seguente:



Come chiave pre-condivisa IPsec utilizzare “vpnunito” (senza virgolette).

3.2. Apple

Nei sistemi Apple, il client VPN da configurare si trova seguendo il percorso:

Impostazioni → Generale → VPN → Aggiungi Configurazione VPN

È importante impostare subito il Tipo di VPN, mettendo IPsec, in modo che venga visualizzato il client corretto. A questo punto procedere con il resto della configurazione come riportato nella figura seguente:

The screenshot shows the configuration screen for a VPN on an Apple device. At the top, there are three buttons: "Annulla" (Cancel), "Global Protect UniTO" (Title), and "Fine" (Done). Below the title is the Cisco logo. The main configuration area includes:

- Tipo:** IPsec
- Descrizione:** Global Protect UniTO
- Server:** vpnaccess.unito.it
- Account:** userscu
- Password:** Chiedi ogni volta
- Usa certificato:** A toggle switch that is currently turned off.
- Nome gruppo:** vpnunito
- Segreto:** A field with ten black dots representing a password.

At the bottom, there is a "PROXY" section with three buttons: "No" (selected), "Manuale", and "Automatico".

Come "Segreto" utilizzare "vpnunito" (senza virgolette).