UNIVERSITÀ DEGLI STUDI DI MILANO
Ufficio Cybersecurity, Protezione Dati e Conformità
Direzione Generale

VPN Lavoro da Remoto – Manuale Utente

Sommario

Descrizione Generale

Il servizio di VPN Lavoro da Remoto permette a utenti strutturati e abilitati di connettersi dall'esterno dell'Ateneo ai servizi interni e navigare su Internet utilizzando un indirizzo IP di Ateneo in maniera analoga a qualunque postazione presente all'interno dell'Ateneo. Il servizio è disponibile per sistemi Windows, Mac OSX e per i principali sistemi Linux.

Il servizio si compone di:

- Un client per effettuare la connessione al servizio.
- Un portale di accesso dove è anche possibile scaricare il client Global Protect per Windows e Mac OSX
- Uno o più server di erogazione del servizio (*gateway*).

L'accesso al servizio è autenticato attraverso le credenziali istituzionali di Ateneo.

Installazione

Sistemi Windows e Mac OSX

Dopo essere stati abilitati al servizio, è possibile connettersi al portale di accesso tramite le proprie credenziali di Ateneo e scaricare il client adatto al proprio sistema operativo.

Per installare il client Global Protect è necessario avere i privilegi di amministratore di sistema.

Scaricare il client Global Protect

Per connettersi al portale occorre aprire il browser preferito e inserire come indirizzo:

https://telelavoro.unimi.it

Inserire nel campo **Name** il proprio indirizzo di posta elettronica completo e nel campo **Password** la propria password (Figure 1); le credenziali sono le stesse utilizzate per accedere ai servizi di Ateneo per il personale.

mario.rossi@uni

mario.rossi@uni
mi.it

Figure 1: Autenticazione del portale di accesso

Dopo l'accesso viene presentata una schermata dove è possibile scaricare i client *Global Protect* per Windows 32bit e 64bit e Mac OSX (Figure 2):

Figure 2: Portale di accesso

Si può verificare che tipo di sistema operativo Windows si possiede (se 32bit o 64 bit) accedendo al pannello di controllo e cliccando sul icona *Sistema.*

Una volta scaricato il client Global Protect è possibile installarlo seguendo le procedure specifiche del sistema operativo a disposizione ed accettando le opzioni di *default*.

Sistemi Linux

Sui sistemi operativi Linux è possibile utilizzare qualunque client IPSEC con autenticazione X-Auth. Il client consigliato è **vpnc,** disponibile nel *repository* di *default* delle principali distribuzioni Linux. Per l'assistenza in fase d'installazione e i parametri di configurazione del client occorre rivolgersi all'ufficio Sicurezza ICT di Ateneo (sicurezza @unimi.it).

Connettersi al servizio VPN Lavoro da Remoto

Sistemi Windows

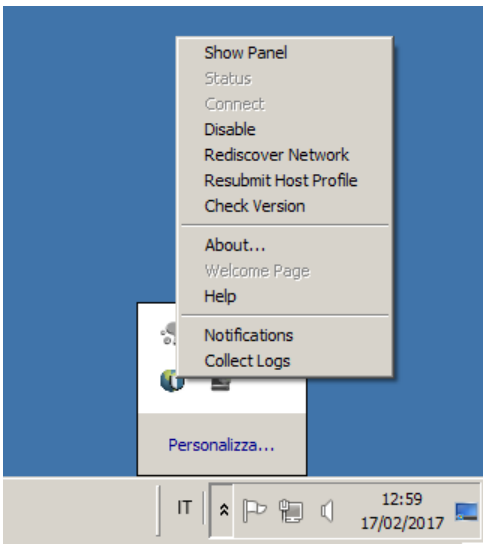
Una volta installato il client e una volta effettuato il login nel proprio profilo, è possibile verificare lo stato della connessione VPN ed accedere ai settaggi del client attraverso le icone di notifica (Figure 3).

Figure 3: Icona Global Protect Windows

L'icona indica anche lo stato della connessione:

-  Croce Rossa: client disabilitato o servizio VPN non funzionante (password errata, server non raggiungibile, servizio non disponibile)
-  Scudo fermo: client attivo e funzionante
-  Scudo rotante intorno al mondo: Client in fase di connessione

Attraverso il tasto destro del mouse è possibile accedere al menu contestuale del client:



Pannello di controllo Global

Abilita/Disabilita il

Ripeti la fase di

Figure 4: Menu Contestuale Windows

Per eseguire la connessione al servizio VPN Lavoro da Remoto occorre:

- Aprire il pannello di controllo attraverso la voce "**Show Panel**" del menù contestuale (Figure 9)
- Inserire l'indirizzo del portale di accesso: **telelavoro.unimi.it** (Figure 5)
- Premere il tasto **Connect** sul pannello di controllo
- Inserire le proprie credenziali di Ateneo (Figure 11)
- Premere il tasto **Connect** sul pannello di inserimento delle credenziali

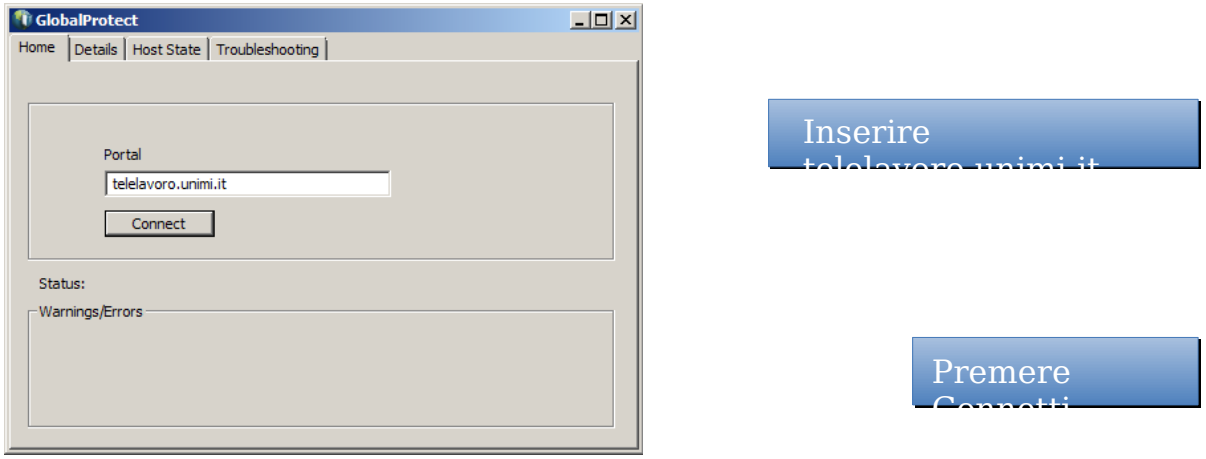


Figure 5: Pannello di controllo Global Protect

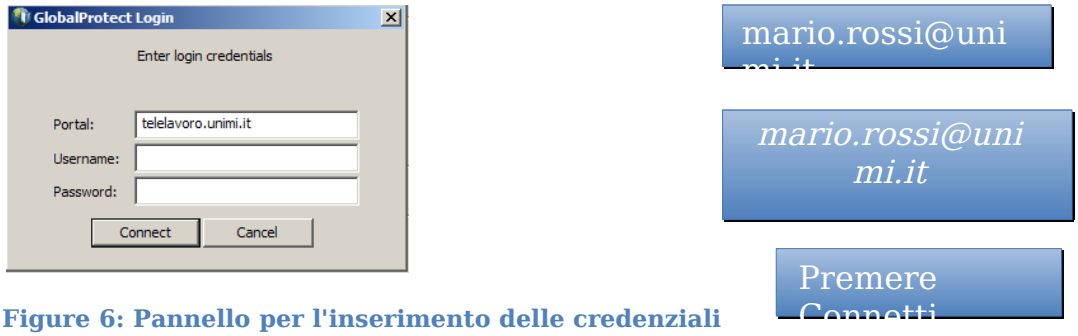


Figure 6: Pannello per l'inserimento delle credenziali

Le credenziali sono memorizzate dal client per i successivi accessi. E' possibile cancellare le credenziali memorizzate e disconnettere il client cliccando sulla croce dell'icona delle credenziali presente sul pannello di controllo (Figure 12).

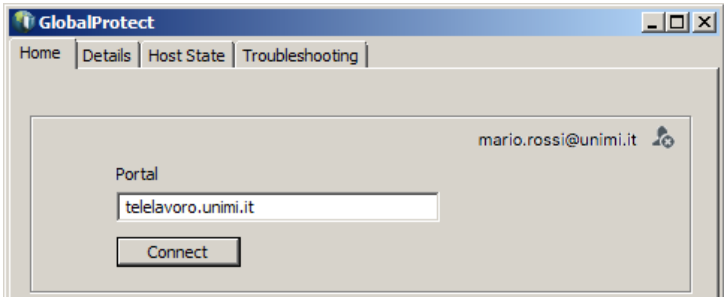


Figure 7: Icona delle credenziali

Sistemi Mac OSX

Una volta installato il client ed una volta effettuato il login nel proprio profilo, è possibile verificare lo stato della connessione VPN ed accedere ai settaggi del client attraverso le icone di notifica sullo schermo in alto.

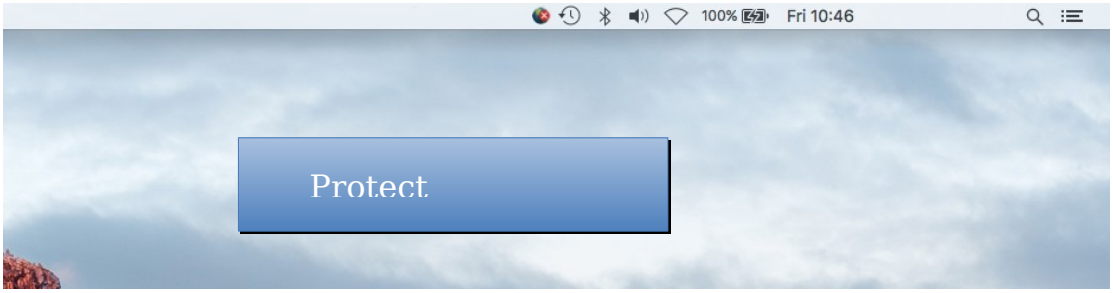
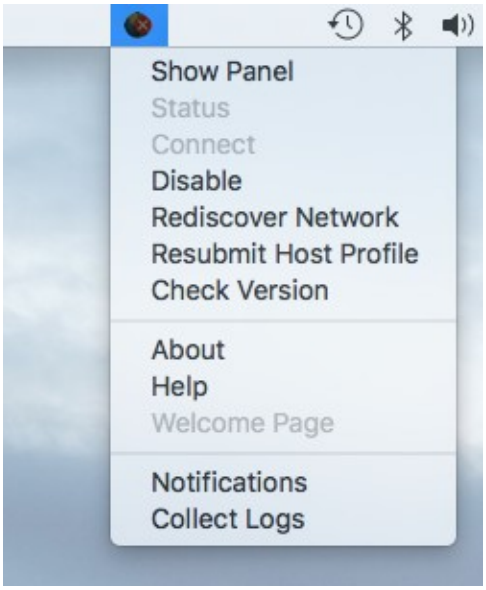


Figure 8: Icona di stato Global Protect

L'icona indica anche lo stato della connessione (Figure 8):

-  Croce Rossa: client disabilitato o servizio VPN non funzionante (password errata, server non raggiungibile, servizio non disponibile)
-  Scudo fermo: client attivo e funzionante
-  Scudo rotante intorno al mondo: Client in fase di connessione

Attraverso il tasto destro del mouse è possibile accedere al menù contestuale del client:



Mostra il pannello di controllo del client

Abilita/Disabilita il client

Ripeti la fase di connessione

Figure 9: Menù Contestuale

Per eseguire la connessione al servizio VPN Lavoro da Remoto occorre:

- Aprire il pannello di controllo attraverso la voce "**Show Panel**" del menù contestuale (Figure 9)
- Inserire l'indirizzo del portale di accesso: **telelavoro.unimi.it** (Figure 10)
- Premere il tasto **Connect** sul pannello di controllo
- Inserire le proprie credenziali di Ateneo (Figure 11)
- Premere il tasto **Connect** sul pannello di inserimento delle credenziali

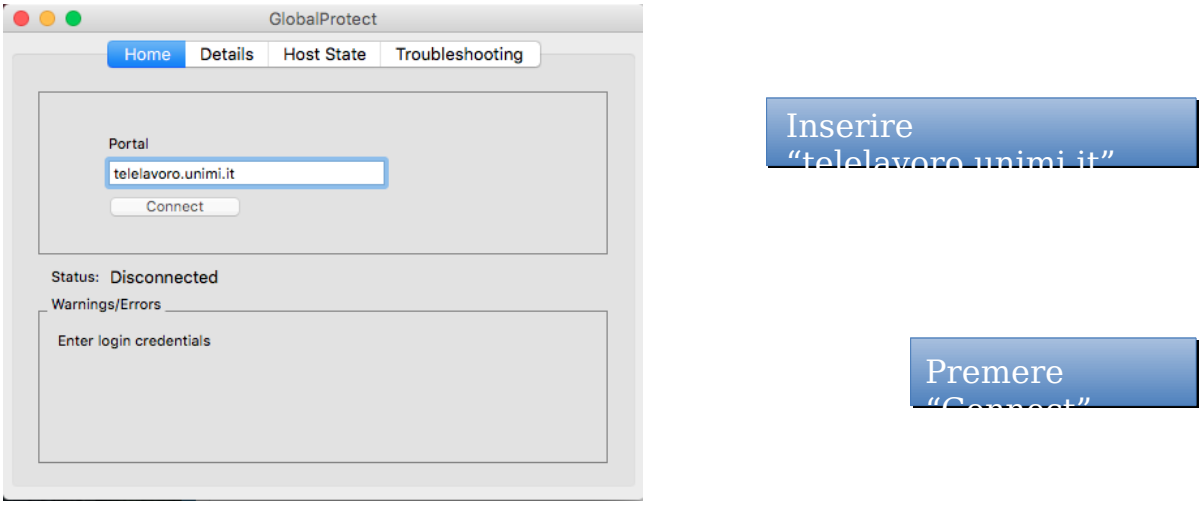


Figure 10: Pannello di controllo Global Protect

Figure 11: Pannello per l'inserimento delle credenziali

Le credenziali sono memorizzate dal client per i successivi accessi. E' possibile cancellare le credenziali memorizzate e disconnettere il client cliccando sulla croce dell'icona delle credenziali presente sul pannello di controllo (Figure 12).

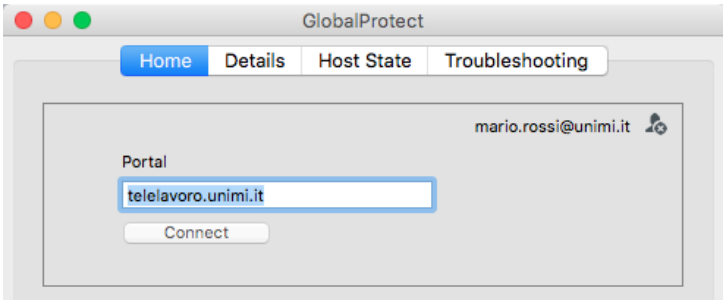


Figure 12: Icona delle credenziali

Verifica della connessione al servizio VPN Lavoro da Remoto

Sistemi Windows

Se la connessione è stabilita correttamente, il pannello di controllo si presenterà in maniera simile alla Figure 15:

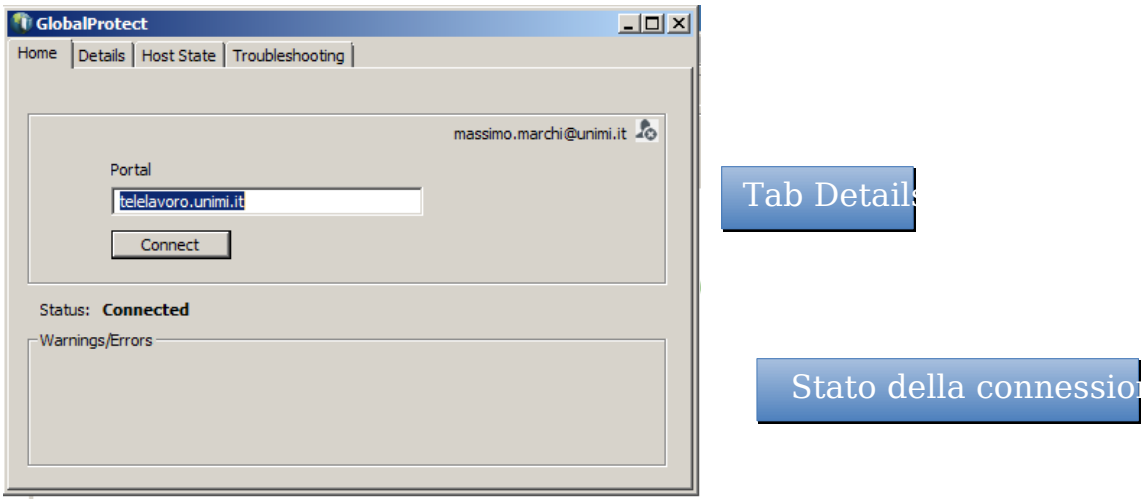
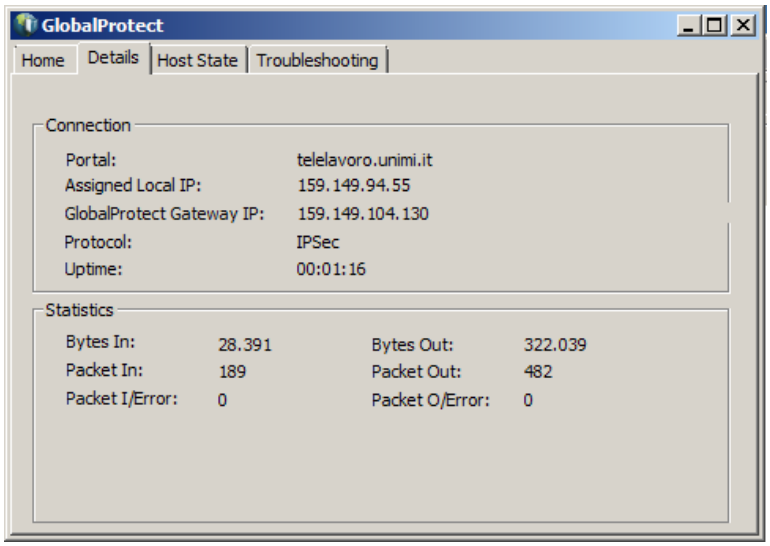


Figure 13: Connessione stabilita correttamente

Per verificare i dettagli della connessione è possibile consultare il tab "**Details**" (Figure 15):



IP assegnato alla

Server che sta erogando il servizio (gateway)

Figure 14: Dettaglio della connessione

Sistemi Mac OSX

Se la connessione è stabilita correttamente, il pannello di controllo si presenterà in maniera simile alla Figure 15:

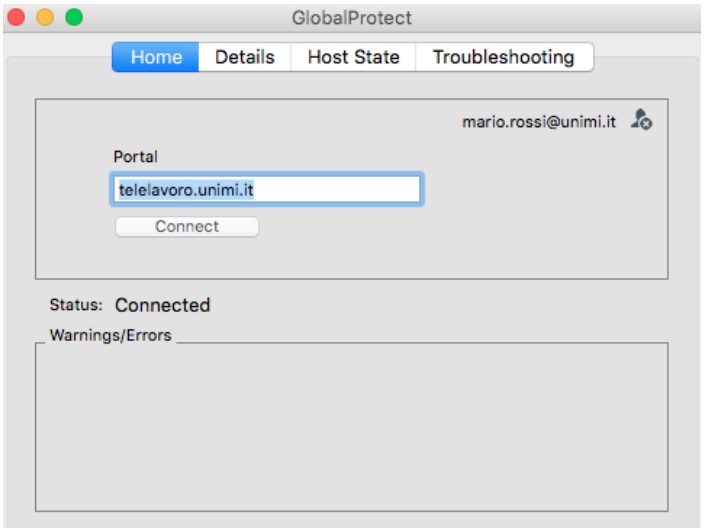


Figure 15: Connessione stabilita correttamente

Per verificare i dettagli della connessione è possibile consultare il tab "**Details**" (Figure 15):

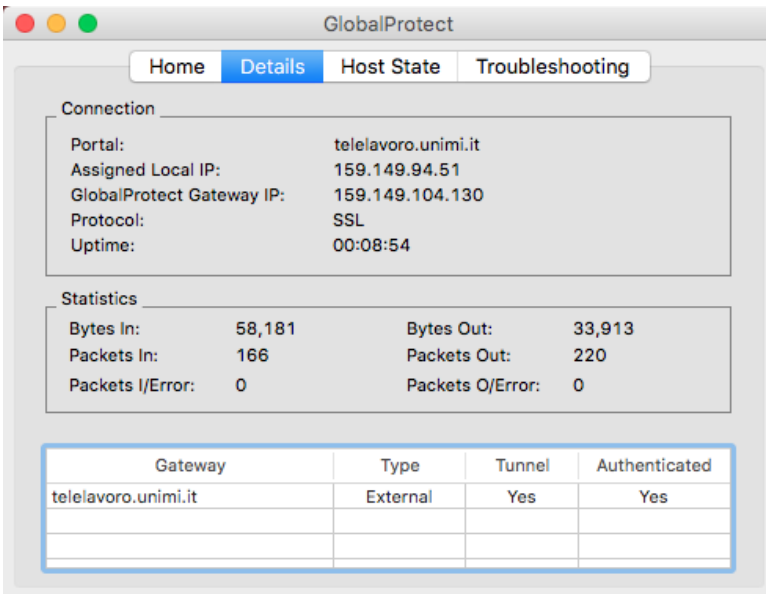


Figure 16: Dettaglio della connessione

Disinstallare il Client Global Protect

Sistemi Windows

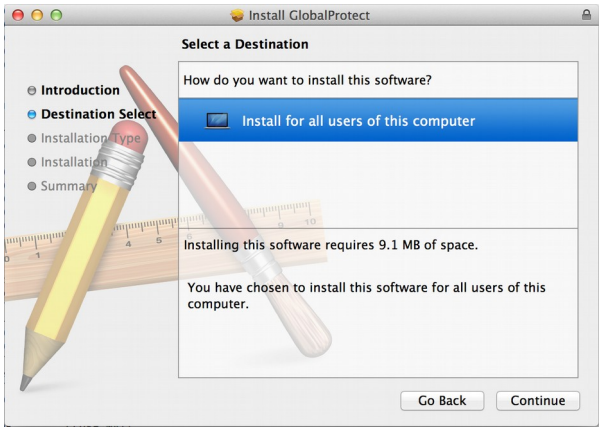
La disinstallazione del client Global Protect avviene come tutte le altre applicazioni Windows accedendo alla voce *Programmi e Funzionalità* del pannello di controllo.

Sistemi Mac OSX

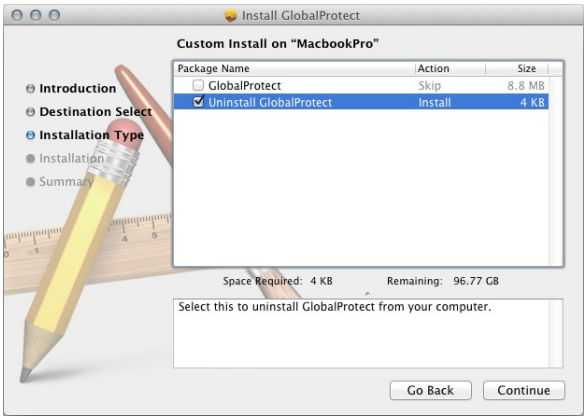
Disinstallare il client via package .pgk file

Per disinstallare il Global Protect in modalità grafica occorre scaricare il file di installazione ed eseguirlo, selezionando la voce apposita quando richiesto:

- Scaricare dal portale il file di installazione .pkg per Mac OSX
- Selezionare **Continue** nell'introduzione
- in **Destination Select**, selezionare **Install for all users of this computer** e quindi selezionare **Continue**



- Deselezionare 'GlobalProtect', selezionare 'Uninstall GlobalProtect', e quindi selezionare **Continue**



- Selezionare **Install**

Disinstallare il client via CLI

Per disinstallare il Global Protect via terminale occorre avere i privilegi di root sul dispositivo. Da linea di comando:

$ sudo /Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh