

1. *Introduzione.*

La seguente procedura per l'utilizzo di una connessione VPN da casa si basa sul protocollo SSL (Secure Socket Layer) che viene utilizzato per garantire la protezione a livello di applicazione delle comunicazioni basate su web che avvengono attraverso la rete Internet.

Grazie a un sistema di crittografia e autenticazione, il protocollo SSL consente comunicazioni in modalità protetta tra due dispositivi, in genere un server web e un PC client.

Per utilizzare la modalità VPN SSL bisogna eseguire i seguenti passi:

1. Scaricare ed installare un piccolo programma che farà da client per la connessione. (Questo passo dovrà essere effettuato solo la prima volta o ad ogni cambio di computer)
2. Eseguire il programma inserendo le proprie credenziali

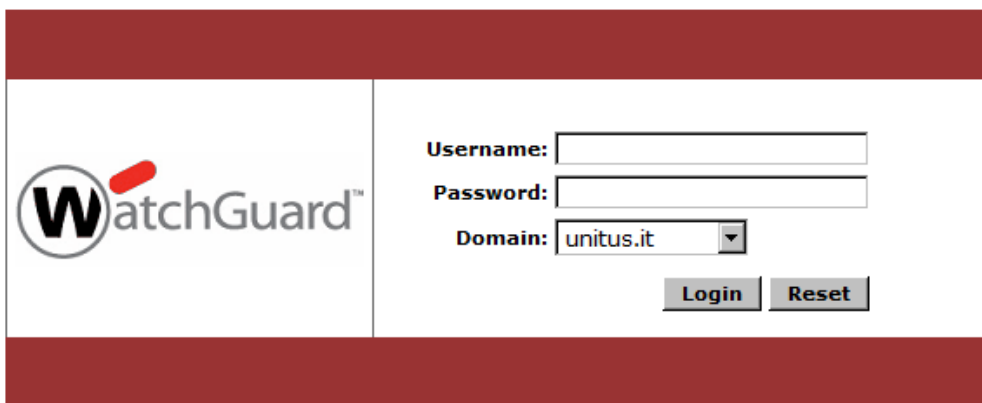
Sono disponibili client per Windows e MAC OS-X

Passo 1 Scaricare ed installare il client. (solo la prima volta)

- Aprire il proprio browser e digitare l'indirizzo:

<https://sslvpn.unitus.it/sslvpn.html>

- Accettare il certificato digitale e proseguire. Si ottiene la seguente pagina:



The screenshot shows a web interface with a dark red header and footer. On the left, there is the WatchGuard logo. On the right, there is a login form with the following fields:

- Username:
- Password:
- Domain: (dropdown menu)

Below the form are two buttons: "Login" and "Reset".

- Inserire le vostre credenziali (le stesse del servizio di posta elettronica).
- **ATTENZIONE:** Il personale **docente e non docente** di UNITUS dovrà lasciare nella casella Domain “**unitus.it**”, mentre gli **studenti** dovranno selezionare il dominio “**Studenti.local**”
- Si ottiene la seguente pagina dalla quale è possibile scegliere il client da installare (prime due opzioni)
- Cliccare su download: (per windows o per Mac).

Items available to download**Mobile VPN with SSL client software for Windows**

Use this client to make a secure VPN connection to the company network from a Windows computer.

[Download](#)**Mobile VPN with SSL client software for Mac**

Use this client to make a secure VPN connection to the company network from a Mac computer.

[Download](#)**Mobile VPN with SSL client profile**

Import this profile to enable a secure VPN connection from any SSL VPN client that supports .ovpn configuration files.

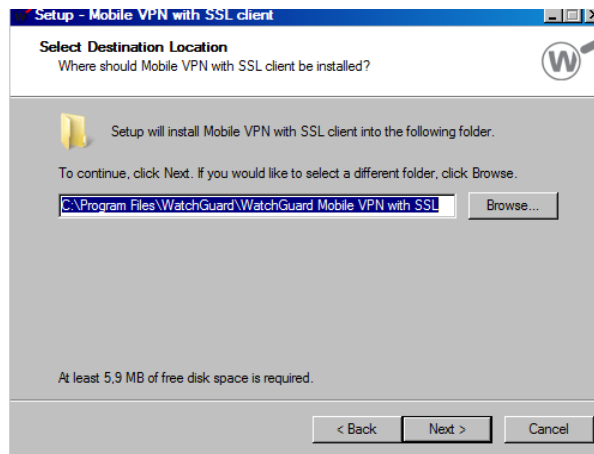
[Download](#)[Logout](#)

- Salvare e successivamente eseguire il file

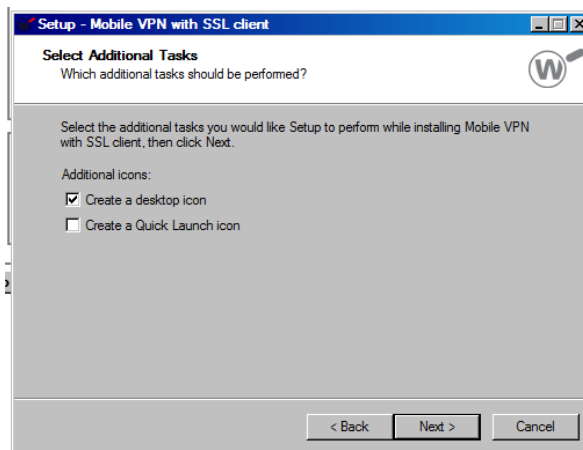
(Per i client windows)

- Accettate le impostazioni di default per le schermata successive.





- Alla fine potete scegliere di aggiungere un'icona sul desktop.

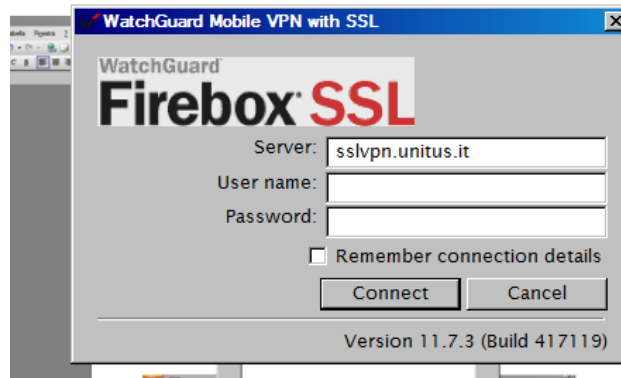


(Per i client MAC)

- fare doppio click su **WG-MVPN-SSL.dmg**.
Un volume chiamato WatchGuard Mobile VPN verrà creato sul desktop.
- All'interno del volume WatchGuard Mobile VPN volume, doppio-click su **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
L'installazione partirà.
- Accettate le impostazioni di default per le schermata successive.
- Completate l'installazione.

Passo 2 Eseguire la connessione VPN

Dopo aver scaricato e installato il software client, esso si conatterà automaticamente al server, presentando la seguente maschera:



Le volte successive per avviare la connessione basterà lanciare il programma:

(Per i client windows)

1. Utilizzare uno di questi tre metodi per avviare il software client:
 - Dal menu Start, selezionare Tutti i programmi> WatchGuard> Mobile VPN con client SSL> Mobile VPN con client SSL.
 - Fare doppio clic sul Mobile VPN con SSL icona sul desktop.
 - Fare clic sul VPN cellulare con l'icona SSL nella barra di avvio veloce.
2. Nel campo server appare il nome *sslvpn.unitus.it* ; nei campi successivi si devono inserire le proprie credenziali
3. Fare clic su Connetti.

Per Mac OS X:

1. Aprire una finestra del Finder. Andare su Applicazioni> WatchGuard e fare doppio clic sul WatchGuard Mobile VPN con applicazioni SSL.
Un'icona "WatchGuard Mobile VPN con SSL" verrà visualizzata nella barra dei menu.
2. Fare clic sull'icona nella barra dei menu e selezionare Connetti
3. Nel campo server appare il nome *sslvpn.unitus.it*; nei campi successivi bisogna inserire le proprie credenziali
4. Fare clic su Connetti.

ATTENZIONE

Nel campo **Username** il personale docente e non docente di Unitus dovrà inserire semplicemente le stesse credenziali che usa per il servizio di posta elettronica senza indicare "@unitus.it" precedute dal suffisso *unitus.it* es.:




username: *unitus.it\marirossi*
password: *della posta elettronica*

Gli studenti di Unitus invece dovranno inserire il proprio *Codice Fiscale* e come password il *PIN* assegnato in fase di iscrizione es.:

username: *codicefiscale*
password: *PIN*

Quando la connessione VPN è stabilita, viene visualizzata un'icona nella barra di avvio rapido vicino all'orologio in basso a destra del monitor (windows) o sul lato destro della barra dei menu (Mac OS X).

Lo stato della connessione VPN è indicato dall'iconcina:

-  Connessione VPN non stabilita.
-  Connessione VPN stabilita. Ora ci si può connettere con sicurezza alle risorse della propria rete.
-  Il client è ancora in fase di connessione o disconnessione

4.. Terminare la connessione VPN

Facendo click con il mouse sull'iconcina del programma si può visualizzare il menu dei comandi:

- Per terminare la connessione VPN fare click su **disconnetti**
- Se si vuole anche chiudere il client fare click su **Exit (windows)** o **Quit (MAC)**

ATTENZIONE

È importante sapere che:

- La connessione VPN può essere stabilita da qualsiasi linea adsl, rete cellulare o altra tipologia di connessione ad Internet.
- Non è necessaria alcuna procedura burocratica: gli utenti verranno autenticati tramite le stesse credenziali con cui accedono al servizio di posta elettronica.
- La connessione VPN va utilizzata soltanto se è necessario accedere a risorse che sono riservate soltanto ai computer direttamente connessi alla rete d'Ateneo (ricerca bibliografica, banche dati, abbonamenti a riviste, ecc.).
- Utilizzare la connessione VPN per la navigazione ordinaria (posta elettronica, web, ecc.) è fortemente sconsigliato perché introduce un rallentamento, sebbene quasi impercettibile, e rischia di sovraccaricare inutilmente il server impedendo ad altri utenti di usufruire del servizio.