



**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

Oggetto: Istruzioni configurazione client VPN per piattaforma Windows

Data: 13/05/2025

Versione: 2.01

Sommario

1. PREMESSA	2
2. INSTALLAZIONE SOFTWARE VPN CLIENT	2
3. PRIMO AVVIO E CONFIGURAZIONE DEL CLIENT VPN DI TIPO SSL	6
4. ATTIVAZIONE DEL TUNNEL VPN	9
5. CREDENZIALI E ABILITAZIONI ALL'USO DEL SERVIZIO	12



Politecnico di Torino

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

1. PREMESSA

Il presente documento contiene le istruzioni per accedere alle risorse di rete e agli host della rete locale del Politecnico di Torino tramite servizio di VPN (Virtual Private Network).

L'accesso in VPN permette agli utenti istituzionali del Politecnico di Torino di realizzare una connessione sicura da qualsiasi parte del mondo (Internet) verso l'interno della rete dell'Ateneo, permettendo l'accesso alle risorse informatiche e telematiche interne come se ci si trovasse all'interno dell'Ateneo. Tutto il traffico verso la rete del Politecnico è protetto mentre non lo è quello diretto verso Internet, permettendo il massimo della sicurezza dei propri dati e delle risorse informatiche del Politecnico e contemporaneamente sfruttando al massimo la connessione locale verso Internet. Inoltre l'accesso in VPN permette di realizzare connessioni protette dalla rete wireless del Politecnico consentendo anche l'accesso a share di rete, stampanti ed altre risorse informatiche altrimenti non raggiungibili.

Nota – L'accesso tramite VPN di tipo SSL permette di creare un tunnel usando la porta standard 443, ovvero la medesima utilizzata per la navigazione HTTPS o "Web Sicuro".

2. INSTALLAZIONE SOFTWARE VPN CLIENT

È possibile scaricare le ultime versioni del client direttamente dal sito della Fortigate®.

<http://www.forticlient.com>

Si prega di notare che, dalle pagine di download del suddetto sito, esistono più prodotti scaricabili liberamente, quello che dovrà essere installato è quello della sezione "**FortiClient VPN-only**" presente a fondo pagina, come indicato nell'immagine della seguente figura:

FortiClient VPN

La versione solo VPN di FortiClient offre VPN SSL e VPN IPSec, ma non include alcun supporto. Scarica il miglior software VPN per più dispositivi.

Accesso remoto

- VPN SSL con MFA
- VPN IPSec con MFA



SCARICA
VPN per Windows



SCARICA
VPN per MacOS



SCARICA
VPN per Linux .rpm



SCARICA
VPN per iOS



SCARICA
VPN per Android



SCARICA
VPN per Linux .deb

Direzione Infrastrutture Servizi Informatici e Amministrazione Digitale

Servizio Infrastrutture

Ufficio Reti e Data Center

Politecnico di Torino - Corso Duca degli Abruzzi 24, 10129 - Torino, Italia

wifi@polito.it - www.polito.it



**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

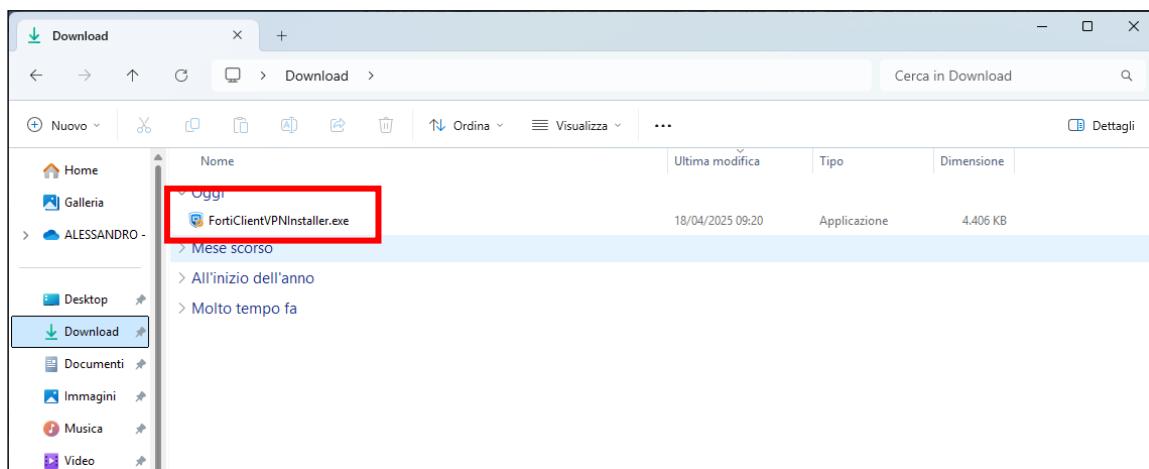
Ufficio Reti e Data Center

NOTA: Si consiglia sempre di tenere aggiornato il programma di connessione FortiClient scaricando regolarmente l'ultima versione disponibile nel sito.

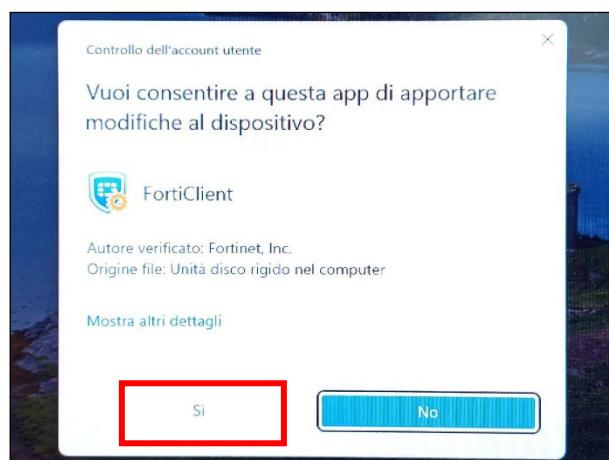
NOTA: Si consiglia sempre di disinstallare la versione vecchia dell'applicativo prima di installare quella nuova onde evitare conflitti nell'installazione.

Di seguito si riporta come esempio l'installazione del software FortiClient su piattaforma Windows 11.

1. Lanciare il file eseguibile “FortiClientVPNInstaller.exe”



2. Nel caso in cui sia attivato il controllo dell'account utente (UAC) cliccare su “SI” per procedere con l'installazione.



Direzione Infrastrutture Servizi Informatici e Amministrazione Digitale

Servizio Infrastrutture

Ufficio Reti e Data Center

Politecnico di Torino - Corso Duca degli Abruzzi 24, 10129 - Torino, Italia

wifi@polito.it - www.polito.it

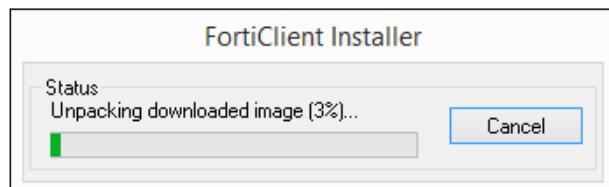
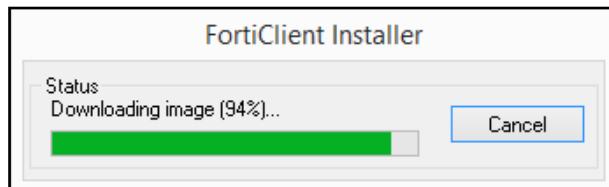


**Politecnico
di Torino**

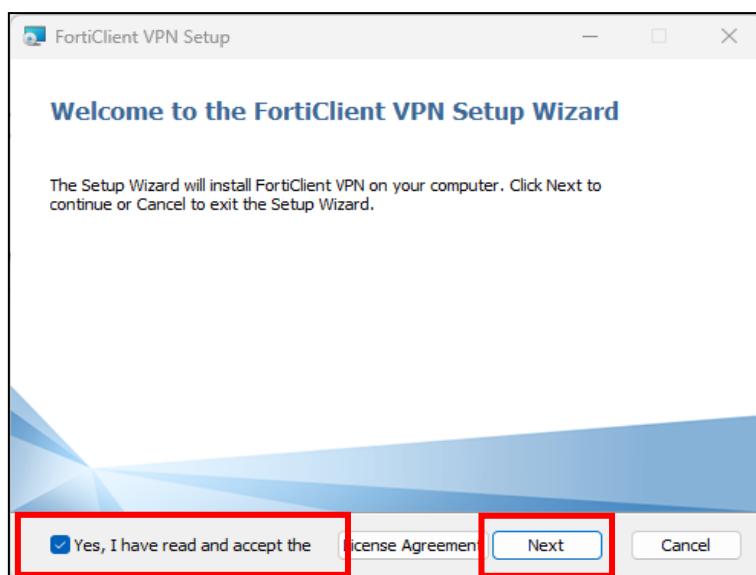
Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

3. Attendere che l'installer completi l'attività di downloading e di unpacking dei file.



4. Accettare il License Agreement e cliccare su "Next" per continuare.



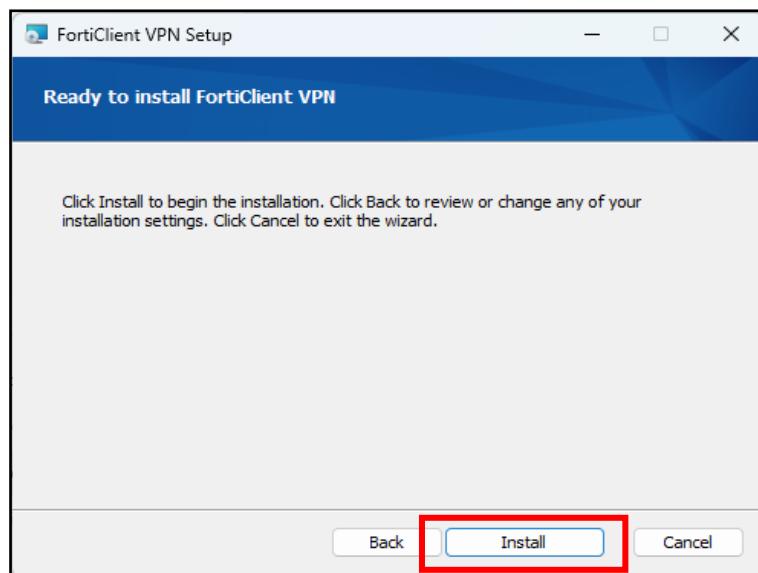


**Politecnico
di Torino**

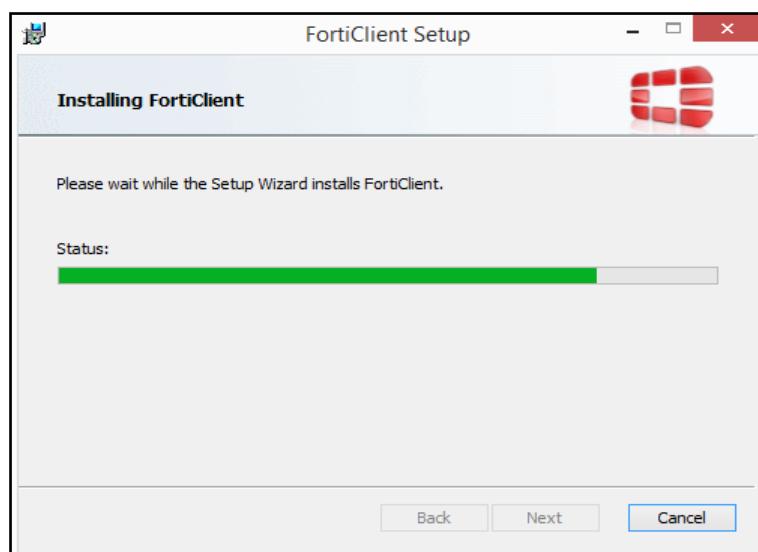
Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

5. Cliccare su "Install" per procedere con l'installazione.



6. Attendere il completamento dell'installazione.



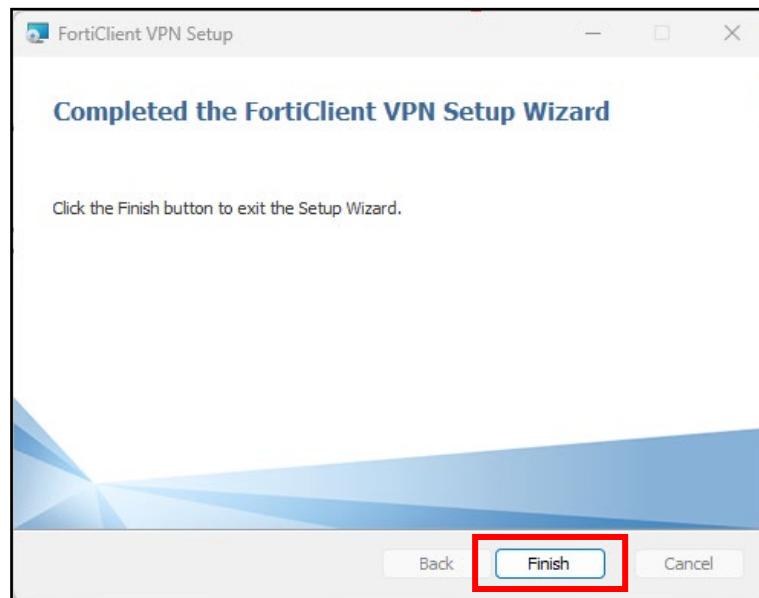
7. Se l'installazione è stata completata correttamente apparirà una schermata come quella mostrata di seguito. Per proseguire cliccare su "Finish".



**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center



3. PRIMO AVVIO E CONFIGURAZIONE DEL CLIENT VPN DI TIPO SSL

1. Avviare il client cliccando ad esempio sull'icona presente sul desktop



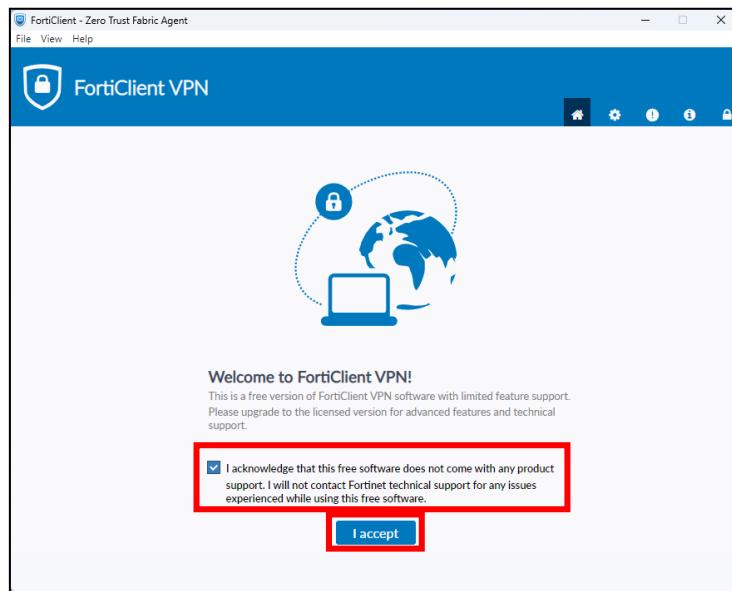


**Politecnico
di Torino**

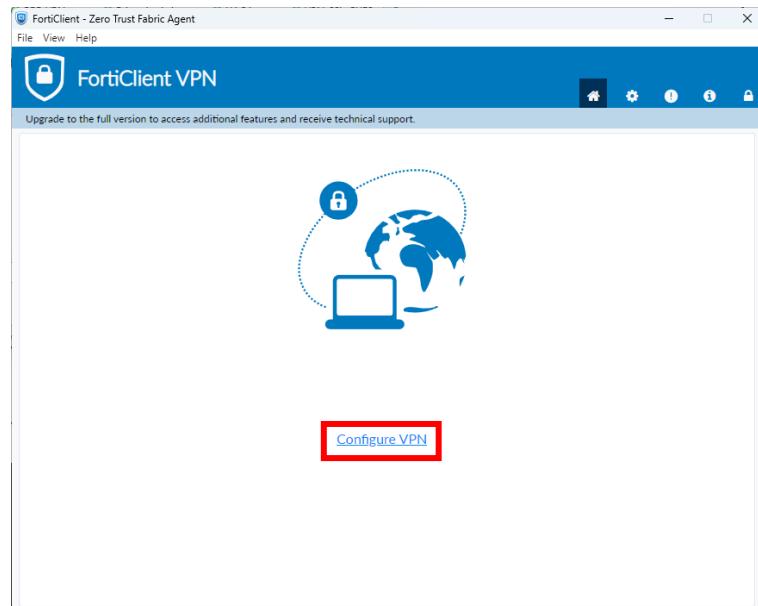
Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

2. Al primo avvio il client VPN presenta la seguente schermata. Mettere la spunta sull'accettazione d'uso e cliccare su "I accept"



3. Cliccare quindi su "Configure VPN"



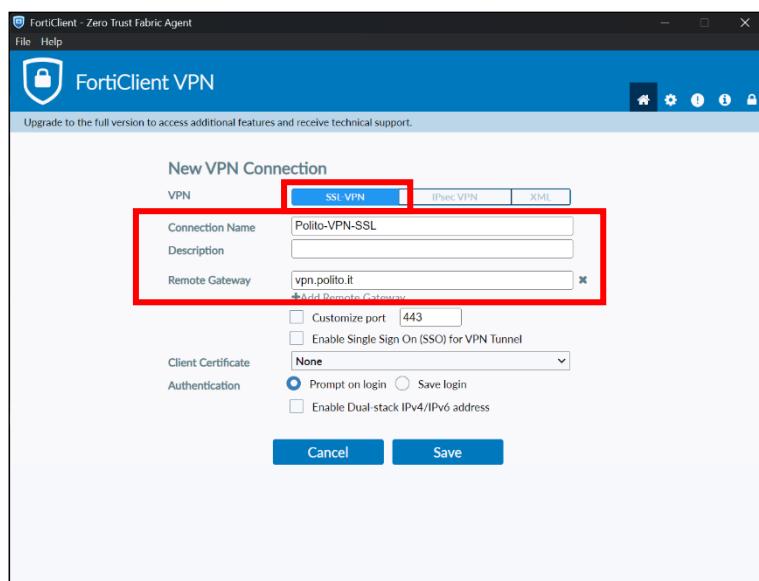


**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

4. Verificare che sia selezionata la sezione “SSL-VPN” e compilare i campi come indicato qui sotto



5. Si riportano di seguito le impostazioni da inserire negli appositi campi.

- **Connection Name:** POLITO VPN SSL
- **Description:** Connessione VPN con Polito
- **Remote Gateway:** vpn.polito.it
- Aggiungere la spunta nella casellina corrispondente a “Enable Single Sign On (SSO) for VPN Tunnel”
- La schermata si modificherà leggermente, spariranno le voci “Client Certificate” e “Authentication” e apparirà una nuova casellina di spunta “Use external browser as user-agent for saml user authentication” che andrà spuntata (vedi la figura seguente)

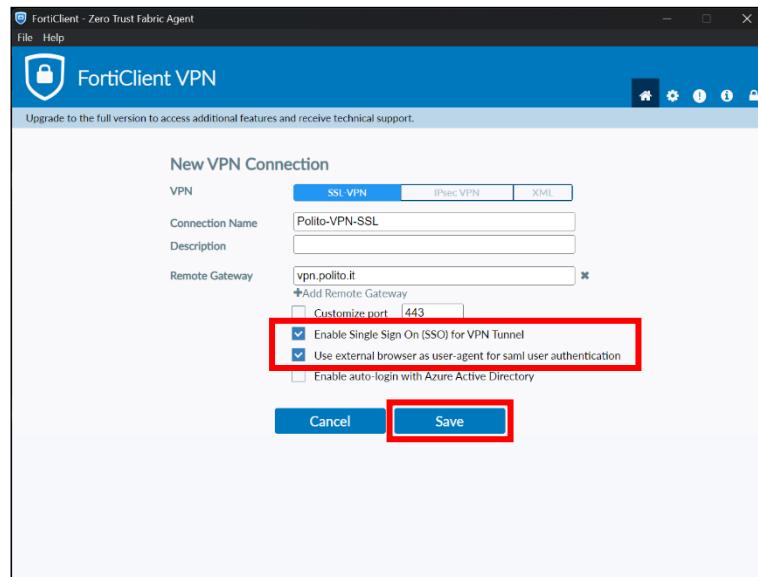


**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

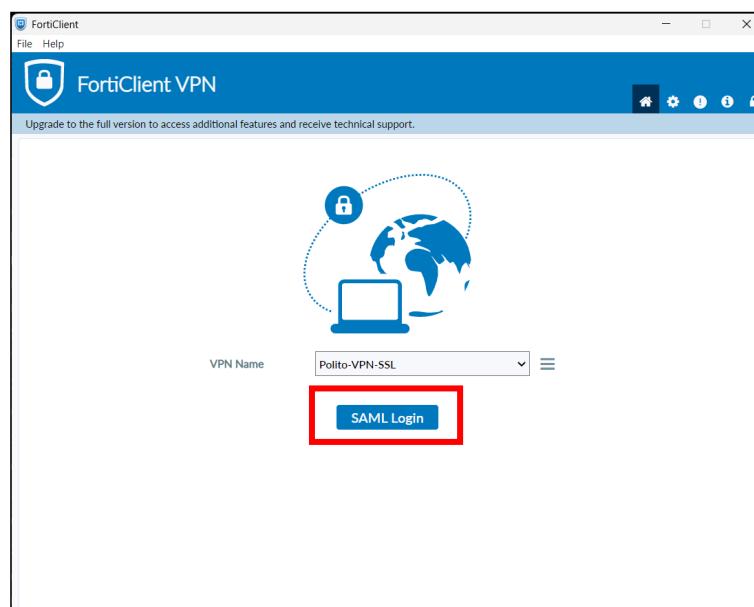
Ufficio Reti e Data Center

6. Salvare la nuova configurazione.



4. ATTIVAZIONE DEL TUNNEL VPN

1. Dopo aver configurato la connessione, il client presenterà la seguente schermata. Per connettersi è necessario cliccare su "SAML Login" oppure "Connect".





**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

2. Premendo tale tasto verrà aperta una nuova pagina del browser predefinito sul proprio dispositivo e verrà presentata la pagina di autenticazione idp.polito.it che già usiamo per accedere a MyPoli, in questa pagina andremo a fare accesso con le credenziali unificate.

The screenshot shows a web browser window titled "Servizio di autenticazione". The address bar shows the URL idp.polito.it. The page content is the Politecnico di Torino authentication interface. It features the university's logo at the top right. Below the logo, there are four buttons: "@Poli", "CIE", "SPID", and "eIDAS". A text input field asks for "Nome utente" (User name) and a password input field ask for "Password". There is a checkbox for "Non ricordare l'accesso". Below these fields are three blue buttons: "Accedi" (Log in), "Oppure" (Or), and "Accedi con Passkey". Another "Oppure" (Or) button is shown below the Passkey button, followed by a "Accedi con certificato" (Log in with certificate) button. At the bottom left, there is a link for "Password dimenticata?" (Forgot password?). The top right of the page has language links "ITA | ENG".

Nota: Nel caso esista già una sessione attiva su idp.polito.it sul nostro browser, l'autenticazione avverrà senza la richiesta delle credenziali come già avviene per l'accesso ai siti web istituzionali con autenticazione unificata.

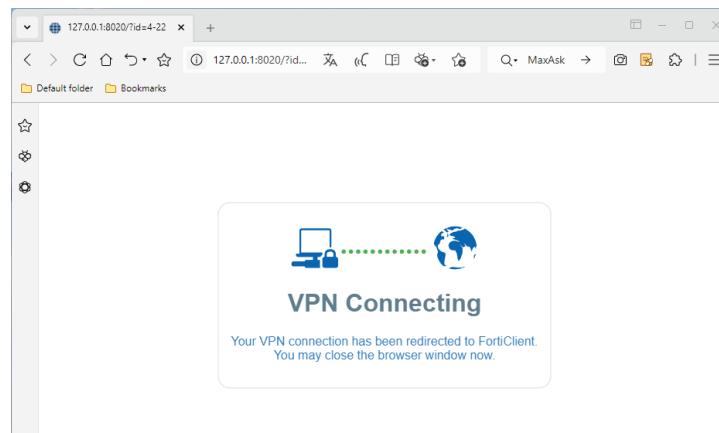


**Politecnico
di Torino**

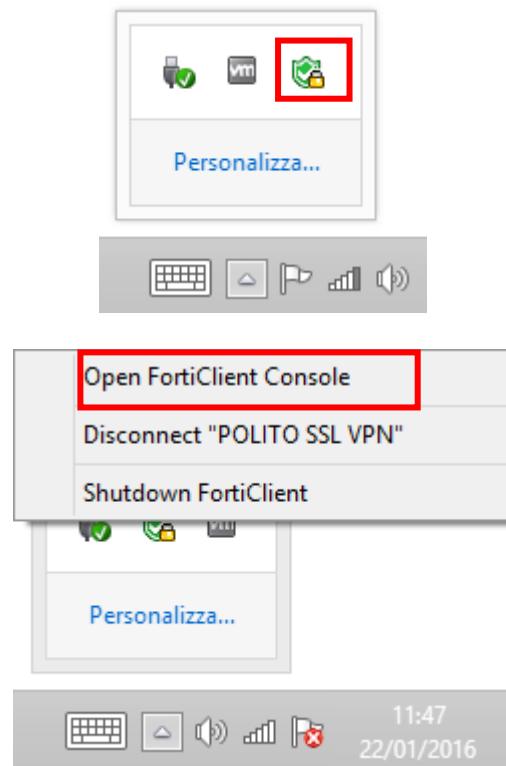
Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center

3. Dopo aver effettuato l'accesso sul browser apparirà il messaggio



4. L'autenticazione è avvenuta con successo, la pagina del browser può esser chiusa
5. È possibile verificare sempre lo stato del client tramite la System Tray. Cliccando col tasto destro del mouse sull'apposita icona e poi su selezionando "Open FortiClient Console"

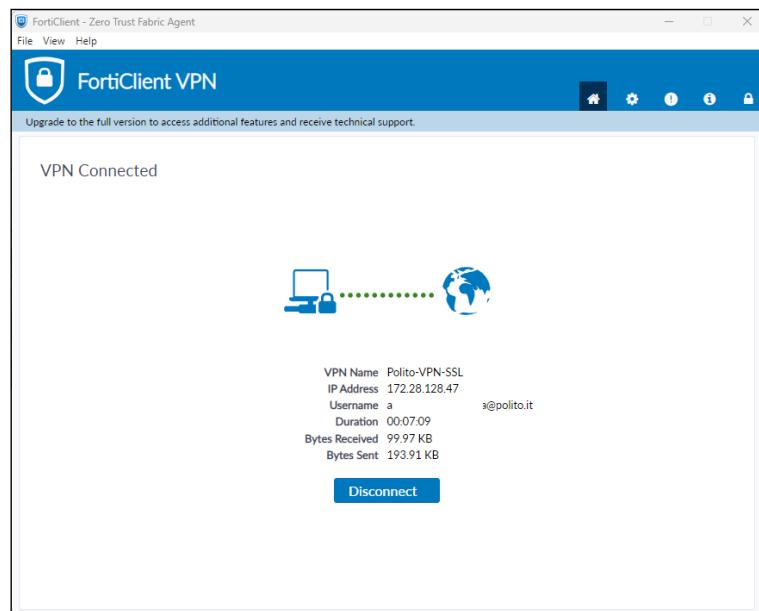




**Politecnico
di Torino**

Direzione Infrastrutture
Servizi Informatici e
Amministrazione Digitale

Ufficio Reti e Data Center



6. Vengono visualizzate informazioni relative alla durata della sessione VPN e i byte trasmessi e ricevuti.

5. CREDenziali E ABilitazioni ALL'uso DEL SERVIZIO

Le credenziali da usare per l'accesso in VPN sono le stesse utilizzate dall'utente per l'accesso a tutti i servizi gestiti da ISIAD, ovvero il Portale Mypoli, le connessioni WiFi (politow ed eduroam), la Mail istituzionale, il Portale della Didattica, le postazioni Windows appartenenti al dominio polito.it, etc...).

Per qualsiasi problema nella configurazione del FortiClient sul proprio dispositivo, si prega di contattare il Service Desk di ISIAD al numero +39-011-090.5050 o via email: 5050@polito.it