



CSI

Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

Titolo	Nome file
Accesso remoto autorizzato mediante VPN per il personale A.O.U. "Federico II"	Smart_Working_AOU_VPN_manuale_progetto_CSI_2020_v1.0.docx

	Nome	Data
Redatto da	Divisione Networking	19-11-2020



CSI

Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

Accesso remoto autorizzato mediante VPN per il personale A.O.U. “Federico II”

Indice

1. Premessa	3
2. Come richiedere il servizio	3
3. Come collegarsi	3
4. Download del client	4
5. Configurazione del client per MS Windows	5
6. Suggerimenti per la collaborazione interpersonale	8



CSI

Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

1. PREMESSA

Sulla base dei DPCM susseguiti nell'attuale periodo emergenziale Covid-19 e su richiesta dell'AOU "Federico II", al fine di agevolare il ricorso al lavoro agile, il CSI ha reso disponibile, per il solo personale dell'AOU autorizzato dal Direttore Generale, il Servizio di Accesso Remoto Autorizzato per l'accesso alla Rete Telematica Ospedaliera ed ai Sistemi Sanitari aziendali.

Il Servizio è in deroga agli attuali accordi convenzionali tra C.S.I. ed A.O.U. e, quindi, è da intendersi temporaneo fino alla fine dello stato emergenziale.

2. COME RICHIEDERE IL SERVIZIO

Per richiedere il servizio, è necessario:

1. prendere visione dell'attuale documentazione in merito alla procedura aziendale di attivazione dello [Smart Working](#)
2. compilare, in ogni sua parte, la [Richiesta di accesso sicuro \(VPN\) alle procedure aziendali](#) allegandole **copia di un documento di identità** in corso di validità
3. inviare la richiesta all'indirizzo sistemainformativo.aou@pec.it e, per conoscenza, a csi@pec.unina.it
4. attendere l'autorizzazione del Direttore Generale aziendale.

Una volta autorizzata, la richiesta verrà presa in carico dal C.S.I. per la generazione delle credenziali che saranno inviate via pec al richiedente all'indirizzo presente sulla richiesta.

3. COME COLLEGARSI

Il servizio VPN utilizza una connessione di tipo SSL e richiede l'utilizzo di un programma dedicato, denominato FortiClient, da installare sulla propria postazione di lavoro remota. Tale programma, se correttamente configurato, consentirà all'utente di [collegarsi sulla propria postazione di lavoro aziendale](#) ed utilizzare tutti i Servizi come se fosse fisicamente presente in Azienda. Per tale motivo, non è necessario installare sulla propria postazione di lavoro remota tutti i programmi aziendali.



CSI

Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

Il client è disponibile nelle versioni per Microsoft Windows, Mac OS, Linux, iOS e Android.

4. DOWNLOAD DEL CLIENT

In base al proprio Sistema Operativo, **effettuare il download del software FortiClient 6.0** da uno dei seguenti indirizzi ed installarlo:

Windows (versioni dalla 7 in poi):

https://filestore.fortinet.com/forticlient/downloads/FortiClientOnlineInstaller_6.0.exe

Mac OSX (versioni dalla 10.12 Sierra in poi):

https://filestore.fortinet.com/forticlient/downloads/FortiClientOnlineInstaller_6.0.dmg

Linux (versioni Ubuntu dalla 16.04 in poi, RedHat e CentOS dalla 7.4 in poi): far riferimento alle istruzioni disponibili alla pagina <https://www.forticlient.com/repoinfo> per la versione **FortiClient 6.0**

iOS (versioni dalla 9.0.0 in poi): <http://itunes.apple.com/md/app/forticlient/id525600370?mt=8>

Android (versioni dalla 4.1 in poi): <https://play.google.com/store/apps/details?id=com.fortinet.forticlient>

Chromebook: <https://chrome.google.com/webstore/detail/forticlient-chromebook-we/igbgpehnbmhdgjbhkkpedommgmfbeao>



CSI

Centro di Ateneo per i Servizi Informativi

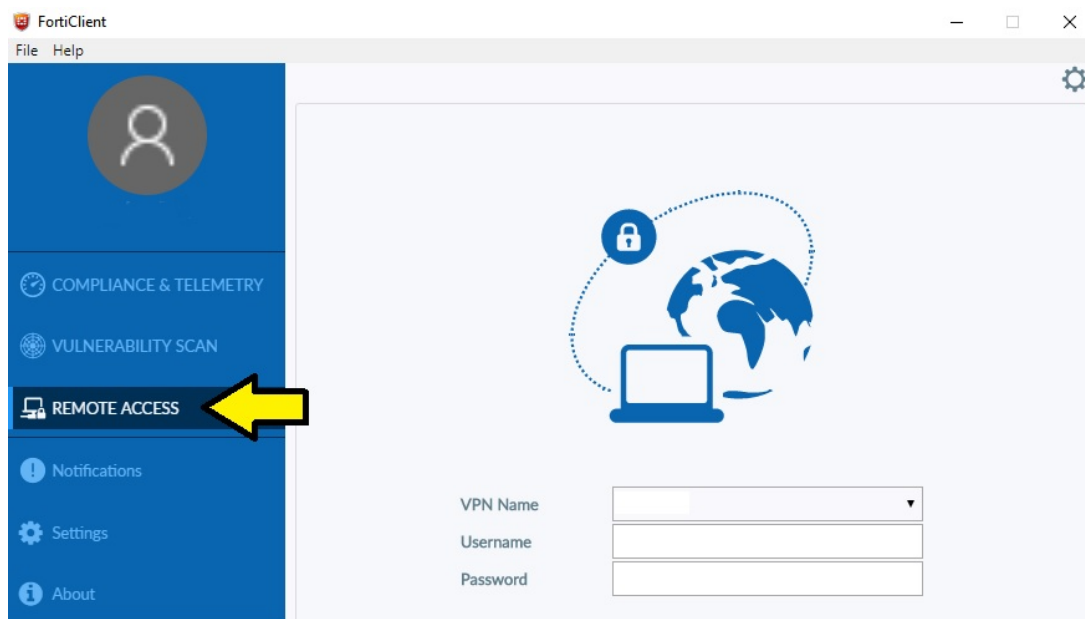


UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

5. CONFIGURAZIONE DEL CLIENT

Una volta installato il software, cliccare sull'icona FortiClient per far partire il programma e procedere con i seguenti passi per la configurazione:

1. **selezionare Remote Access** sulla colonna di sinistra





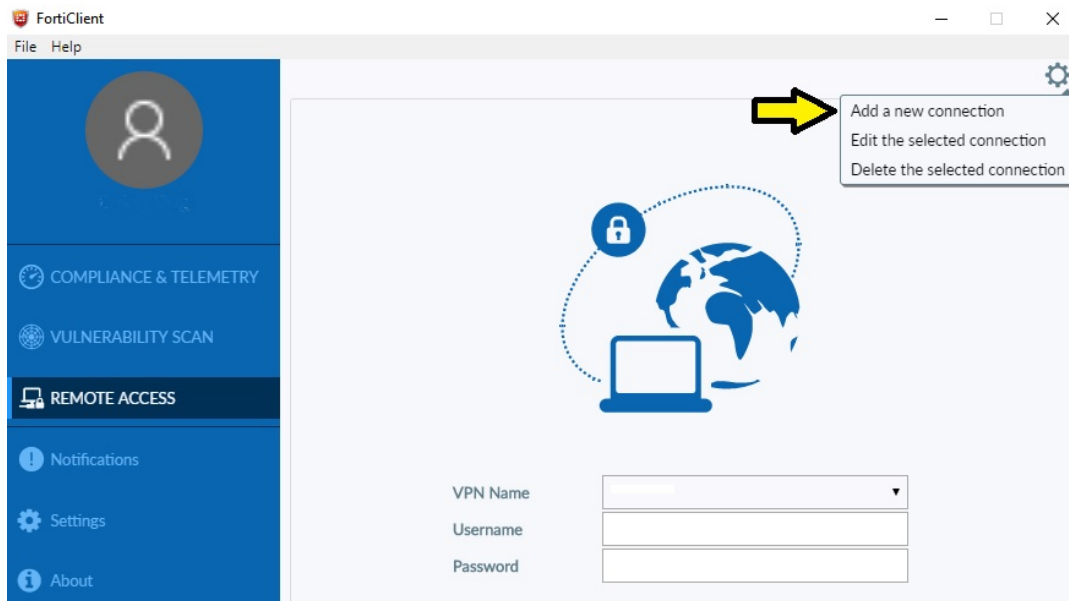
CSI

Centro di Ateneo per i Servizi Informativi

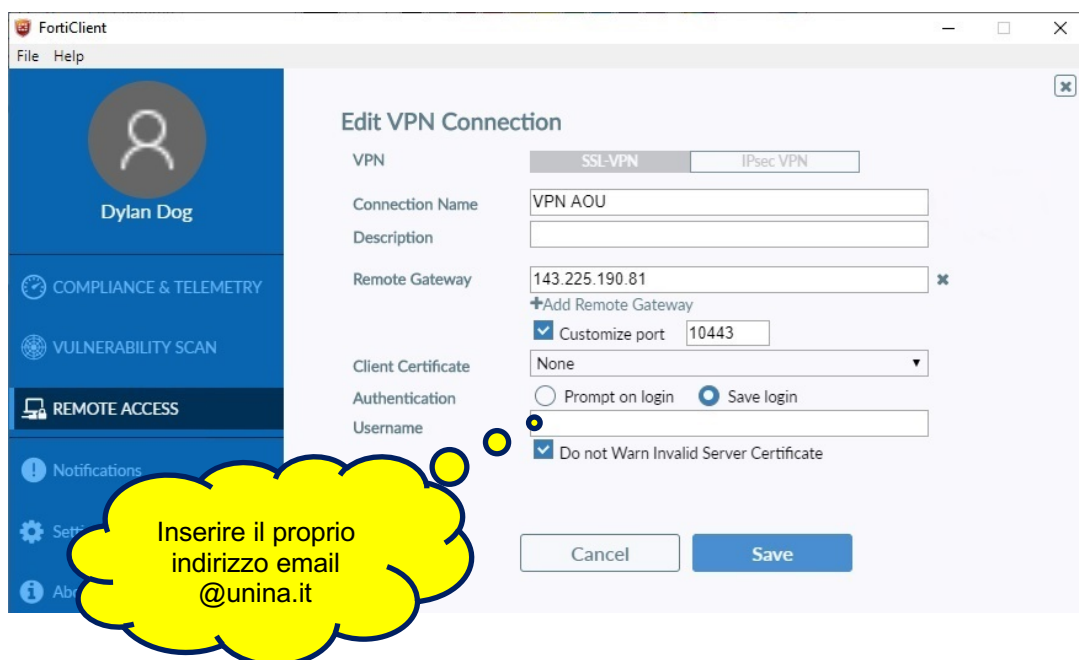


UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

2. Cliccare sull'icona **Impostazioni** in alto a destra. Selezionare **'Add a new connection'**.



3. Configurare la connessione **come in figura allegata**.





CSI

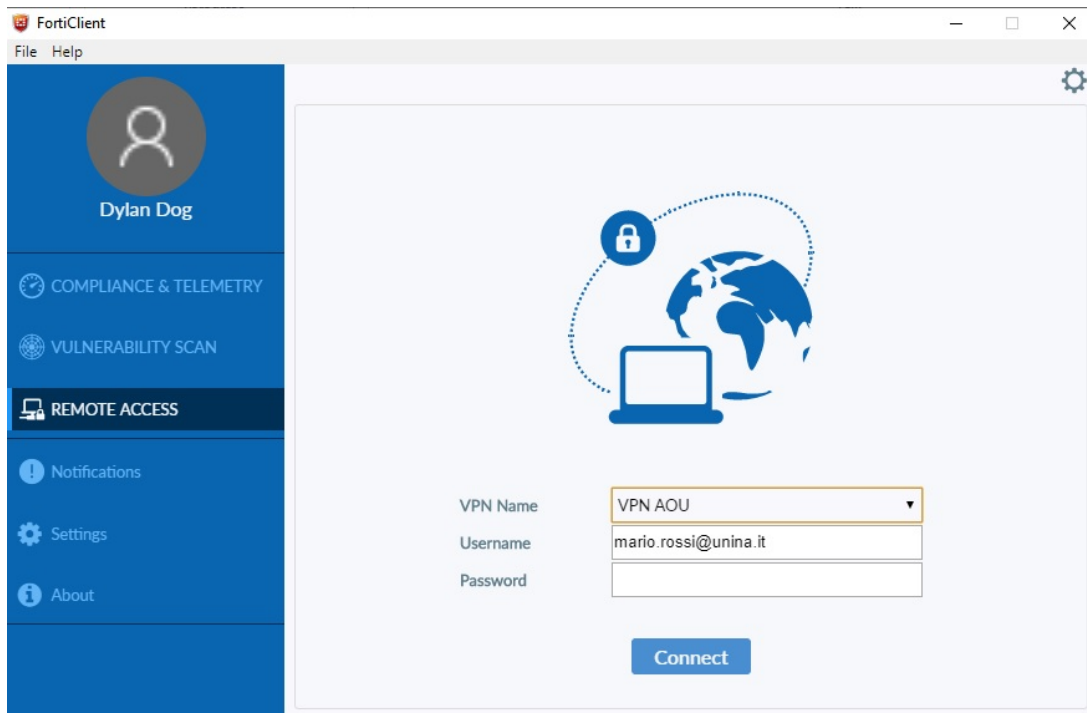
Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

4. Cliccando su **Save**, si verrà riportati nella finestra principale nella quale basterà semplicemente selezionare, nel campo **VPN Name**, il nome della connessione creata, inserire la password e cliccare su **Connect**.

Ovviamente, il campo **Username** andrà riempito con il **proprio indirizzo di posta elettronica Unina**.



Nel momento in cui il programma avvertirà, con una notifica, dell'avvenuta connessione, sarà possibile utilizzare qualsiasi software di controllo remoto per connettersi alla propria postazione di lavoro aziendale (es. Desktop Remoto) e lavorare come se si fosse presenti fisicamente in ufficio.



CSI

Centro di Ateneo per i Servizi Informativi



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

6. SUGGERIMENTI PER LA COLLABORAZIONE INTERPERSONALE

Per eventuali **call** o **riunioni virtuali** per la collaborazione interpersonale, è possibile utilizzare Teams dal proprio computer di casa (si rimanda alla documentazione relativa <http://www.csi.unina.it/teams> per la configurazione) oppure, dalla stessa postazione casalinga, è possibile utilizzare **OpenMeet** e **EduMeet**, servizi **gratuiti e senza registrazione** messi a disposizione dal GARR per le pubbliche amministrazioni, ai seguenti indirizzi:

OpenMeet: <https://www.servizi.garr.it/videoevoce/openmeet>

EduMeet: <https://www.servizi.garr.it/videoevoce/edumet>