



## COMUNE di PISA

Direzione 05  
Programmazione e controllo – Sistemi  
Informativi – Patrimonio

Ufficio Sistemi Informativi

via S. Martino, 108

56125 Pisa

[si.gestione@comune.pisa.it](mailto:si.gestione@comune.pisa.it)

### **ACCESSO AL PC DELL'UFFICIO DAL COMPUTER DI CASA CON CLIENT VPN**

02 maggio 2023

Per particolari esigenze lavorative i dipendenti del Comune di Pisa possono accedere al proprio computer di ufficio dal computer di casa. Il dipendente deve essere autorizzato dal proprio dirigente ed abilitato dai Sistemi Informativi.

#### REQUISITI

- **PC DELL'UFFICIO**

*(chi già si collega da casa in Desktop Remoto con il browser non deve fare niente)*

1. Il PC dell'ufficio deve essere lasciato acceso, il monitor può essere spento
2. Il PC dell'ufficio deve essere abilitato alla connessione in Desktop Remoto (\*)
3. Il PC dell'ufficio deve avere Windows Firewall disabilitato (\*)
4. Il PC dell'ufficio deve avere l'autosospensione del PC (power safe) disabilitata (\*)
5. L'utente con cui si accede a Windows deve essere abilitato al Desktop Remoto (\*)
6. Prendere nota dell'indirizzo IP del PC dell'ufficio

**(\*)** Queste impostazioni possono essere richieste all'Ufficio Sistemi Informativi inviando una mail a [si.gestione@comune.pisa.it](mailto:si.gestione@comune.pisa.it) – **vedi anche istruzioni in Appendice**

- **PC DI CASA**

7. Il PC di casa deve avere installato un antivirus con scansioni schedate. L'antivirus deve essere aggiornato ed aver eseguito scansioni recenti
8. Il PC di casa deve avere una connessione Internet; la qualità di tale connessione influisce in maniera determinante sulla stabilità del collegamento al PC dell'ufficio
9. Il PC di casa deve avere installato uno dei Sistemi Operativi supportati (**Windows XP e Windows Vista non sono supportati**):

#### FORTICLIENT

##### Supported Operating Systems\*

Microsoft Windows 7 (32-bit and 64-bit)

Microsoft Windows 8, 8.1 (32-bit and 64-bit)

Microsoft Windows 10 (32-bit and 64-bit)

Microsoft Windows 11 (64-bit)

Microsoft Windows Server 2012 or later

macOS 11+, 10.15, 10.14

iOS 9.0 or later

Android 5.0 or later

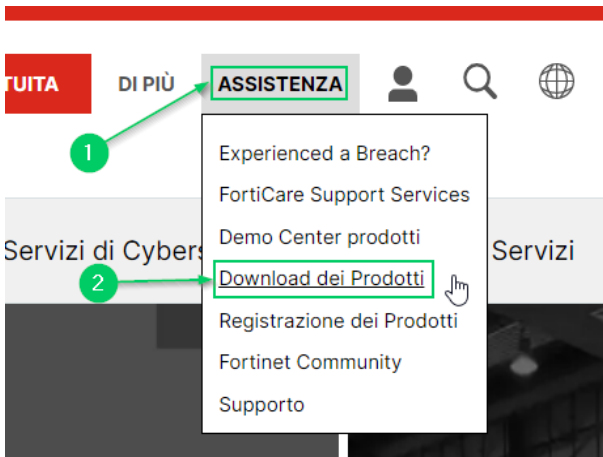
Linux Ubuntu 16.04 and later, Red Hat 7.4 and later, CentOS 7.4 and later with KDE or GNOME

## LA PRIMA VOLTA CHE SI ACCEDE DA CASA

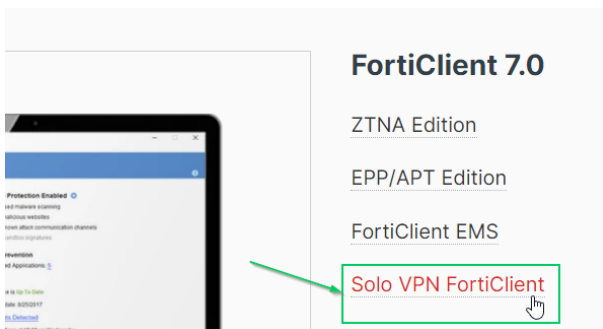
Per configurare il computer di casa è necessario seguire la procedura seguente (solo la prima volta):

10. Aprire un browser web (es. *Chrome, Firefox, Edge*)

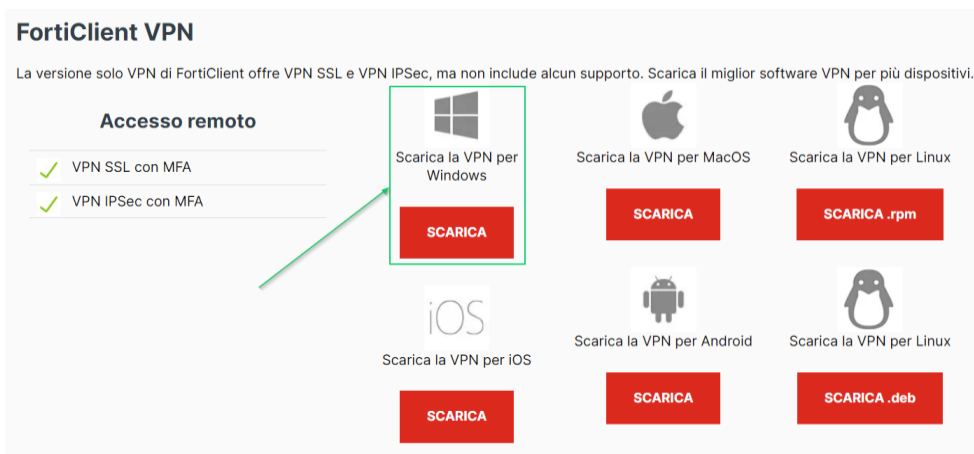
11. Andare all'indirizzo <https://www.fortinet.com/it>, spostarsi sulla voce di menu "ASSISTENZA" in alto a destra, poi nel sottomenu cliccare su "Download dei Prodotti":



12. Nella pagina che si aprirà scorrere in basso e cliccare su "Solo VPN FortiClient":



13. Per scaricare il software, cliccare sul pulsante "SCARICA" corrispondente al sistema operativo installato nel computer di casa, nell'esempio Windows (**Windows XP e Windows Vista non sono supportati**; per chi ha uno di questi sistemi operativi seguire le istruzioni "Guida per l'accesso alla postazione clientless").



14. Installare il software scaricato

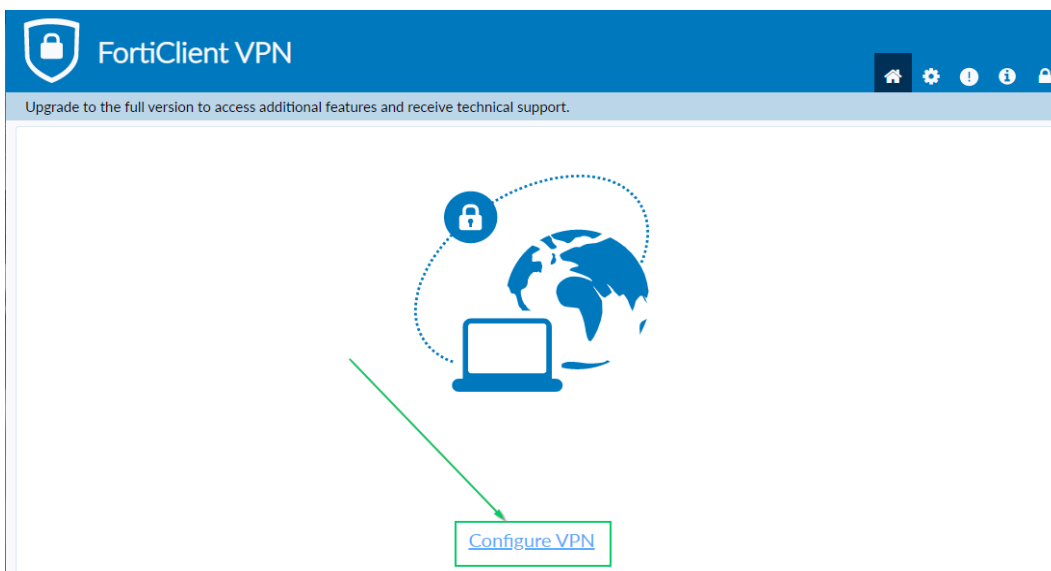
15. Lanciare il software appena installato, riconoscibile dall'icona seguente:



16. Nella finestra successiva **spuntare la checkbox** e poi cliccare sul pulsante **“I accept”**



17. Nella finestra seguente cliccare su **“Configure VPN”**:



18. Configurare come mostrato nell'immagine seguente e poi cliccare sul pulsante **"Save"**:  
(selezionando l'opzione **Save login** anziché **Prompt on login**, sarà possibile memorizzare la username – non la password – senza digitarla ogni volta che si stabilisce una connessione vpn)

**New VPN Connection**

VPN: **SSL-VPN** | IPsec VPN | XML

Connection Name: **VPN Comune Pisa**

Description:

Remote Gateway: **vpn.comune.pisa.it** ✕

+Add Remote Gateway

Customize port: 443

Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: None

Authentication:  Prompt on login  **Save login**

Enable Dual-stack IPv4/IPv6 address

Cancel Save

## DOPO LA PRIMA VOLTA

Terminata la procedura di configurazione del client, ogni volta che si vorrà effettuare l'accesso al PC dell'ufficio si dovrà seguire la procedura di seguito descritta.

19. Lanciare il software **FortiClient VPN**
20. Nella finestra che si aprirà selezionare **VPN Comune Pisa** e, nei campi *username* e *password*, digitare rispettivamente nome utente e password utilizzati per accedere a Windows dal PC dell'ufficio, poi cliccare sul pulsante **"Connect"**:

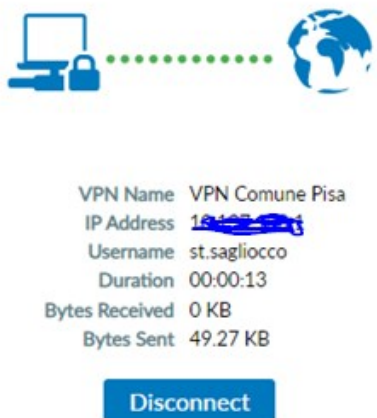
VPN Name: **VPN Comune Pisa**

Username: **st.sagliocco**

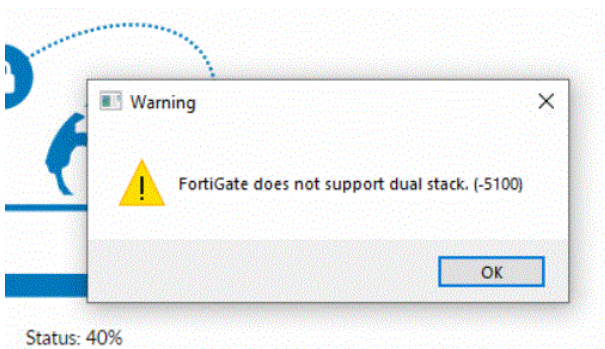
Password: .....

Connect

21. Dopo alcuni secondi verrà stabilita la connessione ed apparirà la seguente finestra informativa:



Potrebbe accadere, nel caso di utilizzo di una vecchia versione di FortiClient VPN su sistema operativo Windows 11, che il software, nel tentativo di stabilire la connessione di rete, restituisca il messaggio di errore **“FortiGate does not support dual stack (-5100)”**



In questo caso è necessario prima disinstallare FortiClient VPN dal proprio computer, dopo scaricare e installare l'ultima versione rilasciata di FortiClient VPN e ripetere la procedura di configurazione descritta nella sezione **“LA PRIMA VOLTA CHE SI ACCEDE DA CASA”**.

## 22. **A QUESTO PUNTO LA CONNESSIONE DI RETE È STABILITA**

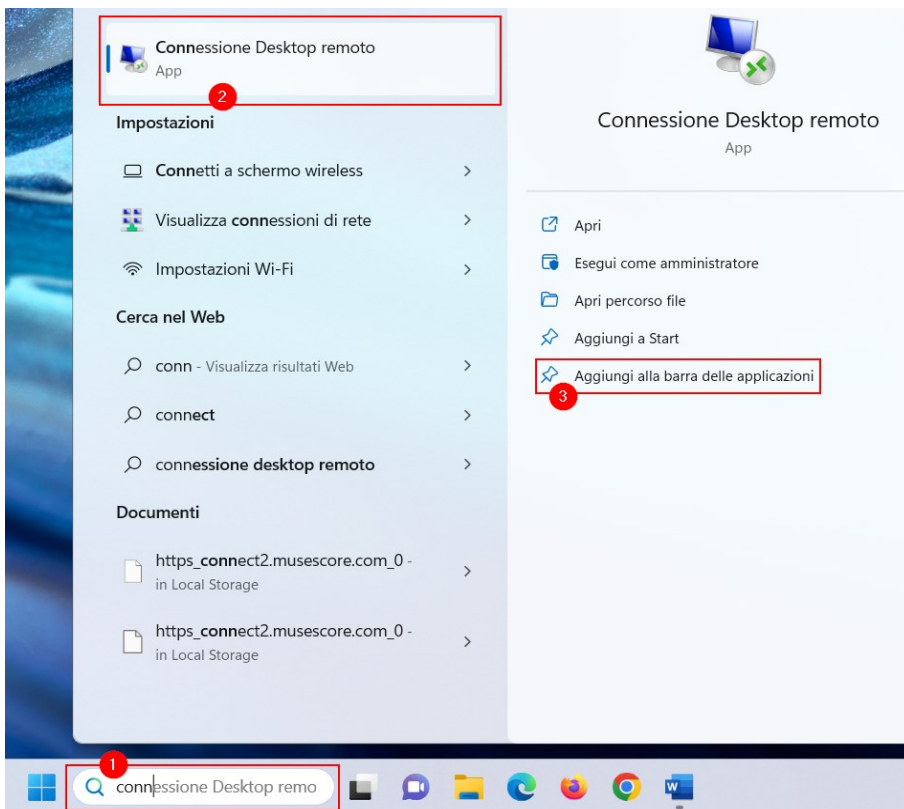
23. Se per qualche motivo la connessione si interrompesse, inserire nuovamente username e password nelle relative caselle di testo e cliccare sul pulsante **“Connect”**

## 24. **ORA SI PUO' APRIRE UN DESKTOP REMOTO SUL PC DELL'UFFICIO**

25. Nel PC di casa cercare ed eseguire l'app **Connessione Desktop Remoto**. Gli screenshot seguenti mostrano come procedere per Windows 7, Windows 10 e Windows 11:

### **Windows 11**

Nella casella **“Cerca”** (1) posta a fianco del pulsante Start, iniziare a digitare **“connes...”**, grazie all'autocompletamento verrà visualizzata l'app **“Connessione Desktop Remoto”** (2): cliccare su questa per eseguirla.

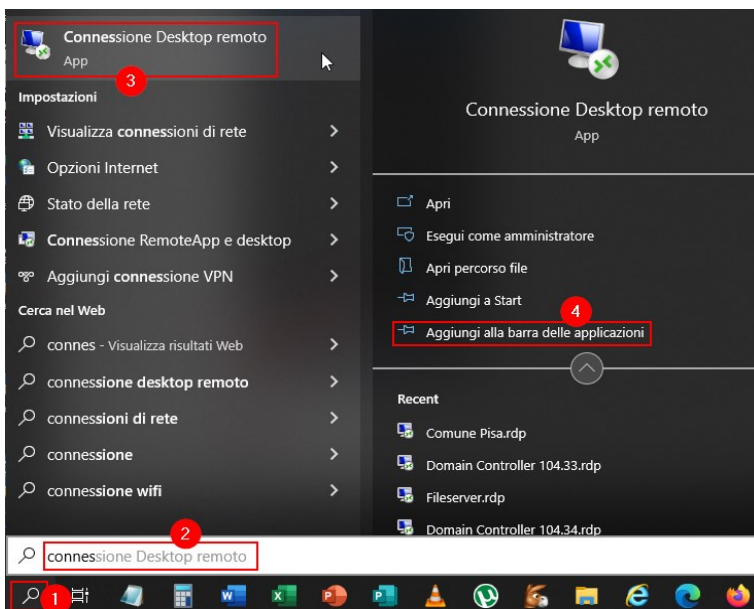


Facendo click su **“Aggiungi alla barra delle applicazioni”** (3) verrà creato, nella barra delle applicazioni, un nuovo collegamento alla app:



## Windows 10

Cliccare sul pulsante **“Cerca”** (1), iniziare a digitare nella relativa casella di testo (2) “connes...”, grazie all’autocompletamento verrà visualizzata l’app **“Connessione Desktop Remoto”** (3): cliccare su questa per eseguirla.

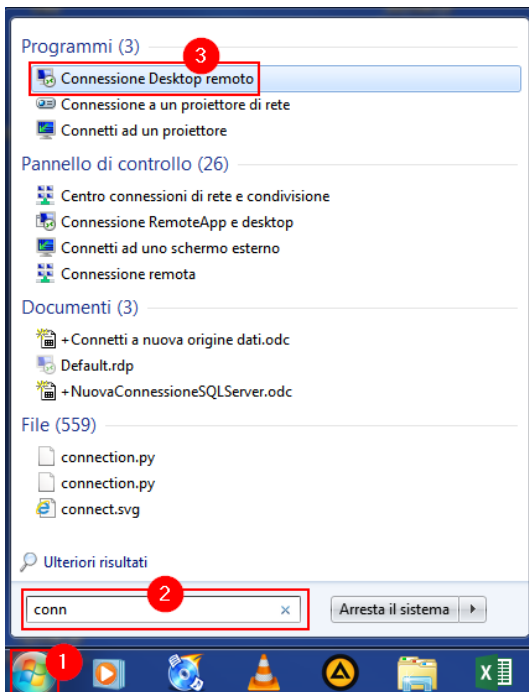


Facendo click su **“Aggiungi alla barra delle applicazioni”** (4) verrà creato, nella barra delle applicazioni, un nuovo collegamento alla app:

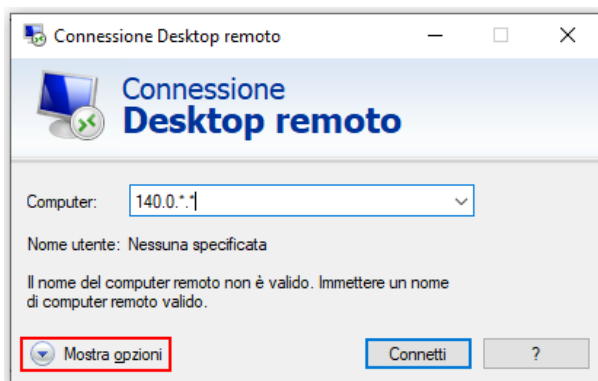


## Windows 7

Cliccare sul pulsante **“Start”** (1), iniziare a digitare nella casella di testo (2) **“conn...”**, grazie all’autocompletamento verrà visualizzata l’app **“Connessione Desktop Remoto”** (3): cliccare su questa per eseguirla.

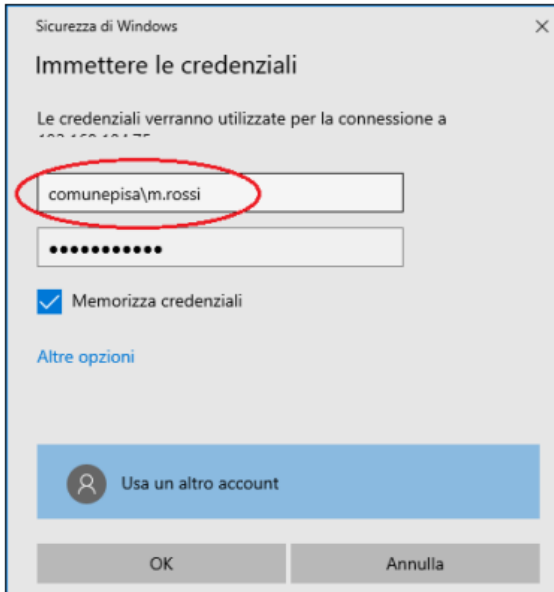


26. Una volta lanciata l’app Connessione Desktop remoto, si apre la seguente finestra, nella quale nella casella Computer deve essere inserito l’indirizzo IP del PC dell’ufficio (per semplicità, si tratta di quattro numeri compresi tra 0 e 255). Cliccando su **“Mostra opzioni”** sarà possibile salvare la connessione sul desktop.

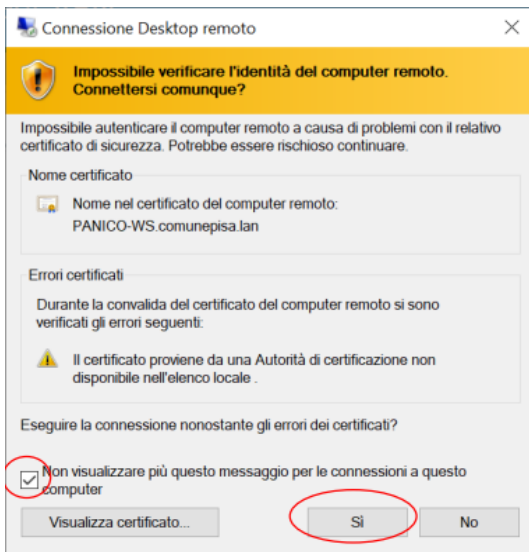


Inserire username e password (sono quelli utilizzati per accedere a Windows dal PC dell’ufficio) e cliccare sul pulsante **“OK”**.

**ATTENZIONE:** la username deve essere inserita con il prefisso comunepisa\ come indicato nell'immagine seguente:



Se viene visualizzata la finestra seguente spuntare la checkbox **“Non visualizzare più questo messaggio per le connessioni a questo computer”** e cliccare sul pulsante **“SI”**:



A questo punto si aprirà il desktop del PC dell'ufficio, sul quale si potrà operare proprio come se fisicamente ci trovassimo in ufficio.

Al termine della sessione di lavoro, è necessario disconnetterci, chiudendo dapprima la finestra del Desktop Remoto e successivamente cliccando sul pulsante **“Disconnect”** dell'app FortiClient VPN:





VPN Name VPN Comune Pisa  
IP Address ~~192.168.1.1~~  
Username st.sagliocco  
Duration 00:00:16  
Bytes Received 0.49 KB  
Bytes Sent 55.08 KB



## APPENDICE

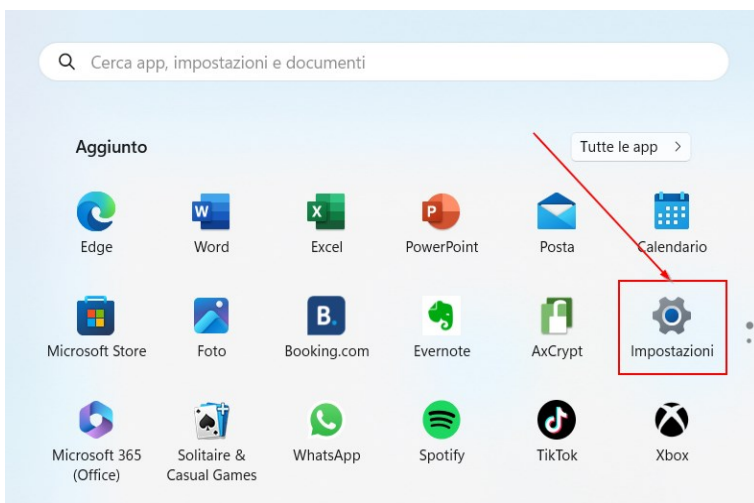
### Verifica dei requisiti

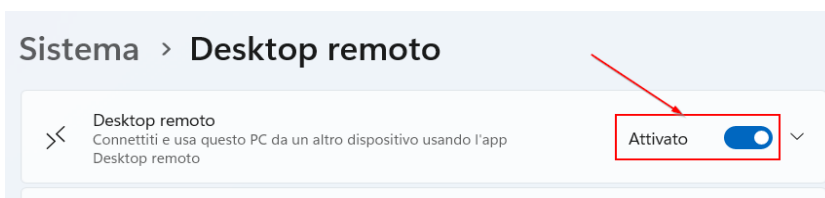
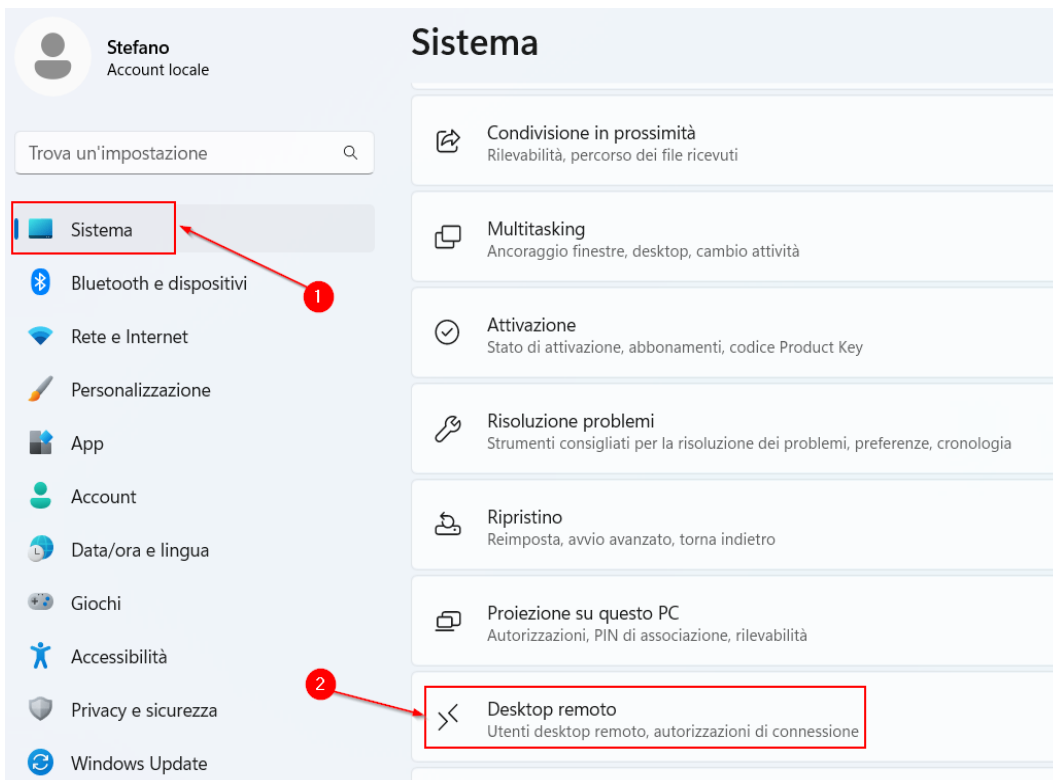
*(chi già si collega da casa in Desktop Remoto con il browser non deve fare niente)*

1. Il PC dell'ufficio deve essere abilitato alla connessione in Desktop Remoto:

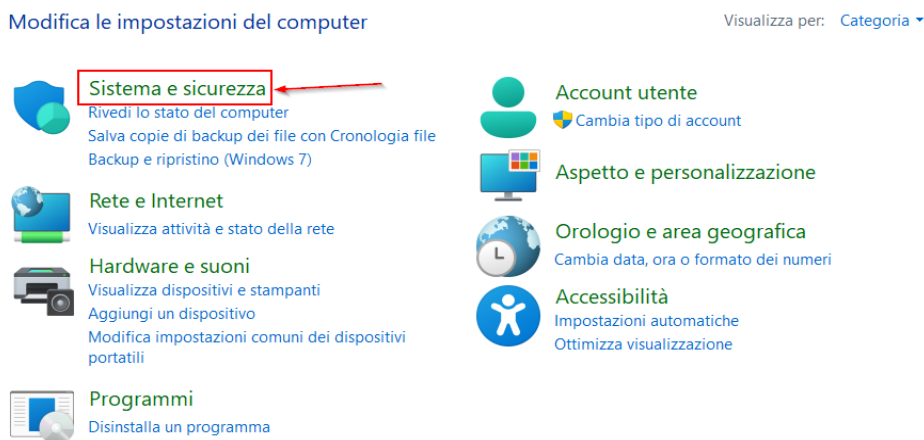
#### Windows 11

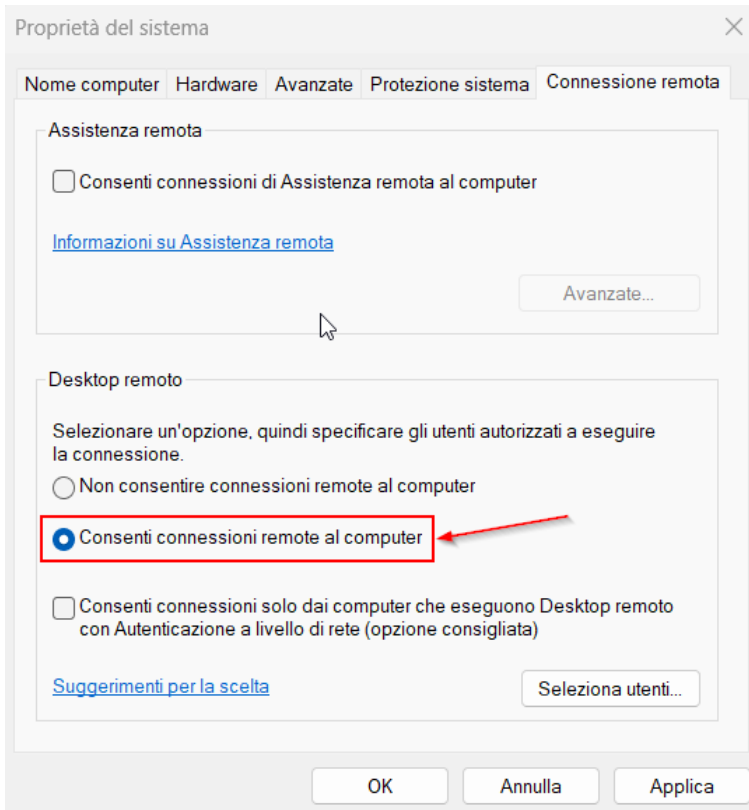
Per verificare: **Impostazioni -> Sistema -> Desktop Remoto**





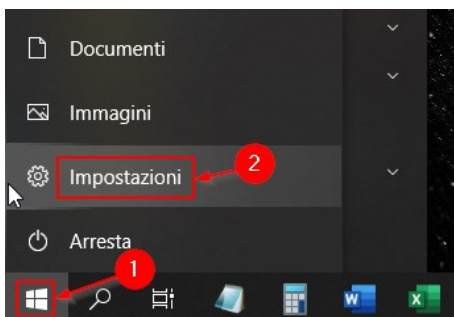
Oppure: **Pannello di controllo -> Sistema e sicurezza -> Consenti accesso remoto**

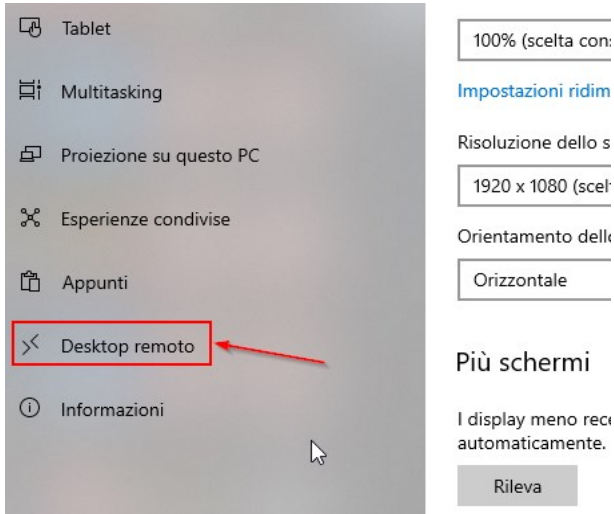
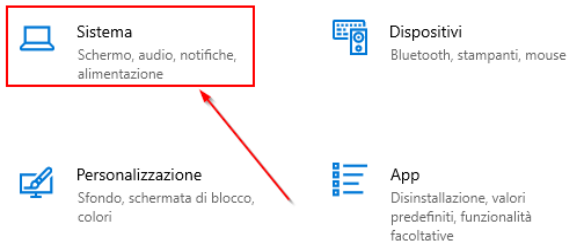




## Windows 10

Per verificare: **Impostazioni -> Sistema -> Desktop Remoto**





## Desktop remoto

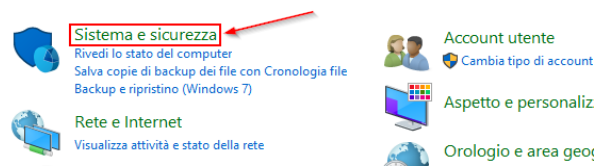
Desktop remoto ti consente di connetterti a questo PC e di controllarlo da un dispositivo remoto mediante un client Desktop remoto (disponibile per Windows, Android, iOS e macOS). Potrai lavorare su un altro dispositivo come se stessi utilizzando direttamente questo PC.

Abilita Desktop remoto



## Oppure: Pannello di controllo -> Sistema e sicurezza -> Consenti accesso remoto

Modifica le impostazioni del computer

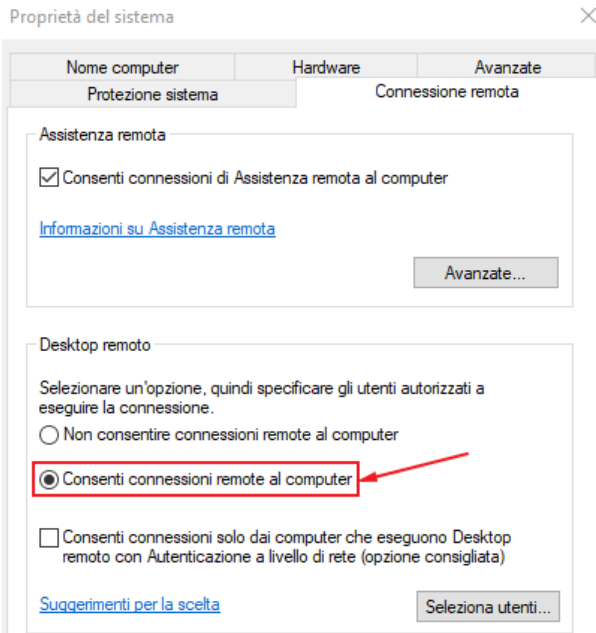


Sicurezza e manutenzione  
Controlla lo stato del computer e risolvi i problemi |  
Modifica le impostazioni di Controllo dell'account utente |  
Risoluzione dei problemi comuni relativi al computer

Windows Defender Firewall  
Controlla stato del firewall | Consenti app attraverso Windows Firewall

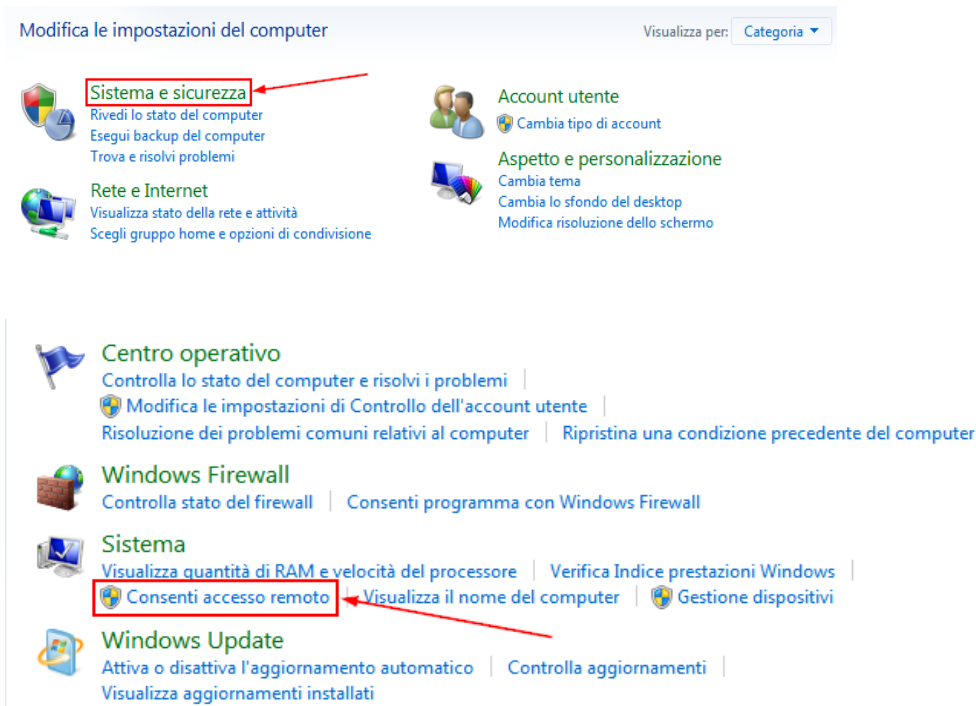
Sistema  
Visualizza quantità di RAM e velocità del processore | Consenti accesso remoto |  
Avvia Assistenza remota | Visualizza il nome del computer

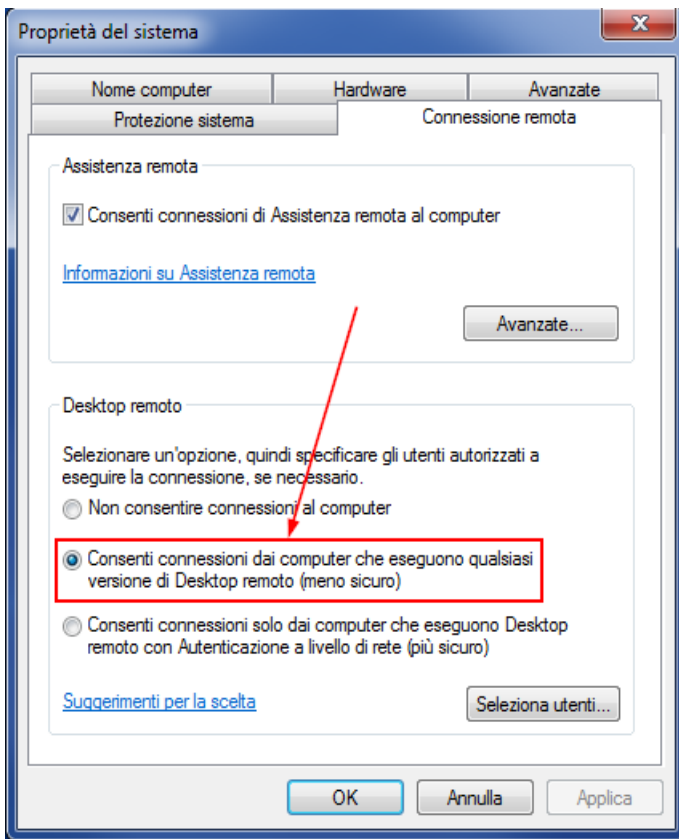
Opzioni risparmio energia  
Cambia comportamento dei pulsanti di alimentazione |  
Modifica impostazioni di sospensione del computer



## Windows 7

Per verificare: **Pannello di controllo -> Sistema e sicurezza -> Consenti accesso remoto**





## 2. Il PC dell'ufficio deve avere Windows Firewall disabilitato:

Per verificare: **Pannello di controllo -> Sistema e sicurezza -> Windows Defender Firewall** (ATTENZIONE: sui sistemi Windows 7 la denominazione utilizzata è "Windows Firewall")

Poi cliccare su **Attiva/Disattiva Windows Defender Firewall**:



## E disattivare **Windows Defender Firewall**:

### Personalizzazione impostazioni per ogni tipo di rete

È possibile modificare le impostazioni del firewall per ogni tipo di percorso di rete in uso.

[Informazioni sui percorsi di rete](#)

#### Impostazioni percorso di rete di dominio

- Attiva Windows Firewall
- Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco dei programmi consentiti
  - Notifica quando Windows Firewall blocca un nuovo programma

- Disattiva Windows Firewall (scelta non consigliata)

#### Impostazioni percorso di rete domestica o aziendale (privata)

- Attiva Windows Firewall
- Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco dei programmi consentiti
  - Notifica quando Windows Firewall blocca un nuovo programma

- Disattiva Windows Firewall (scelta non consigliata)

#### Impostazioni percorso di rete pubblica

- Attiva Windows Firewall
- Blocca tutte le connessioni in ingresso, incluse quelle nell'elenco dei programmi consentiti
  - Notifica quando Windows Firewall blocca un nuovo programma

- Disattiva Windows Firewall (scelta non consigliata)

## 3. Il PC dell'ufficio deve avere l'autosospensione del PC (power safe) disabilitata:

Per verificare: **Pannello di controllo -> Sistema e sicurezza -> Opzioni risparmio energia: Modifica impostazioni di sospensione del computer**

**Sicurezza e manutenzione**  
Controlla lo stato del computer e risolvi i problemi |  
Modifica le impostazioni di Controllo dell'account utente |  
Risoluzione dei problemi comuni relativi al computer

**Windows Defender Firewall**  
Controlla stato del firewall | Consenti app attraverso Windows Firewall

**Sistema**  
Visualizza quantità di RAM e velocità del processore | Consenti accesso remoto |  
Avvia Assistenza remota | Visualizza il nome del computer

**Opzioni risparmio energia**  
Cambia comportamento dei pulsanti di alimentazione |  
**Modifica impostazioni di sospensione del computer**

**Cronologia file**  
Salva copie di backup dei file con Cronologia file | Ripristina file con Cronologia file

### Scegliere o personalizzare una combinazione per il risparmio di energia

Una combinazione per il risparmio di energia è un insieme di impostazioni hardware e di sistema (relative ad esempio a luminosità dello schermo, sospensione e così via) che gestiscono l'utilizzo dell'energia da parte del computer. [Ulteriori informazioni sulle combinazioni per il risparmio di energia](#)

Combinazione selezionata

- Bilanciato** [Modifica impostazioni combinazione](#)
- Consente di bilanciare automaticamente le prestazioni e il consumo di energia sull'hardware compatibile.

#### Modifica le impostazioni per la combinazione: Bilanciato

Specificare le impostazioni desiderate per la sospensione e per lo schermo.

A batteria Alimentazione da rete elettrica

Disattivazione schermo: 3 minuti 5 minuti

Sospensione computer: Mai Mai

Cambia impostazioni avanzate risparmio energia

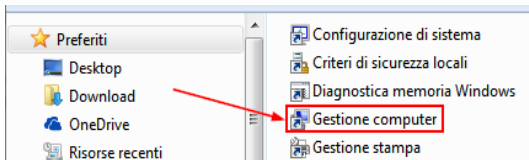
Ripristina impostazioni predefinite per questa combinazione

Salva cambiamenti Annulla

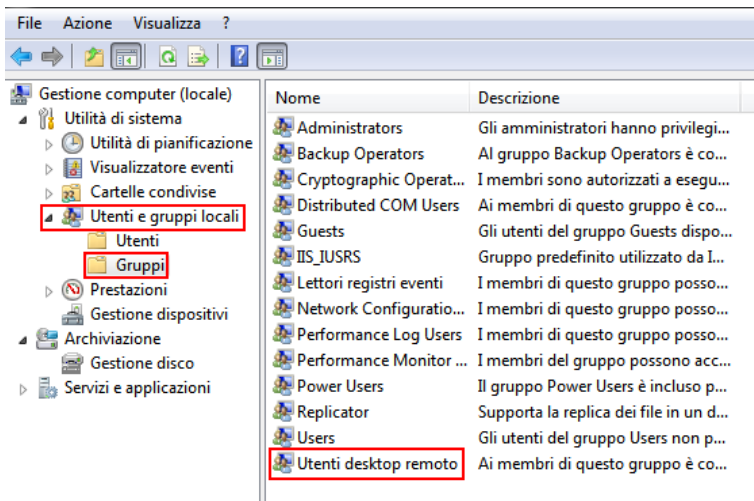
#### 4. L'utente con cui si accede a Windows deve essere abilitato al Desktop Remoto:

Per verificare: **Pannello controllo -> Sistema e sicurezza -> Strumenti di amministrazione**

Doppio click su **Gestione Computer**



**Utenti e gruppi locali -> Gruppi:** verificare che nel gruppo **"Utenti desktop remoto"** ci sia il proprio utente, oppure ci sia "Domain user" o "Utenti di Dominio"



#### 5. Prendere nota dell'indirizzo IP del PC dell'ufficio:

Doppio click sull'icona presente sul desktop del PC dell'ufficio **"Visualizza Indirizzo IP"**:

