

# ISTRUZIONI PER LAVORO AGILE

*last update: 1.8 del 12/08/2024*

## Indice

<b>Posta Elettronica .....</b>	<b>2</b>
<b>Accesso al proprio PC Aziendale (Lavoro Agile) .....</b>	<b>3</b>
<b>Istruzioni Connessione VPN .....</b>	<b>4</b>
<b>Risoluzione Problemi .....</b>	<b>9</b>
<b>VideoConferenza .....</b>	<b>11</b>
<b>Scopia .....</b>	<b>11</b>
<b>Webex.....</b>	<b>12</b>

## Posta Elettronica

Per utilizzare la posta elettronica aziendale utilizzare il link di Zimbra da un qualsiasi browser del proprio PC

<https://webmail.sanita.toscana.it>

## Accesso al proprio PC Aziendale (Lavoro Agile)

La modalità di lavoro agile consiste nel collegarsi dal PC di casa al desktop del PC aziendale, in modo da poter utilizzare **tutti i programmi e i dati** in esso contenuti come se si fosse in ufficio.

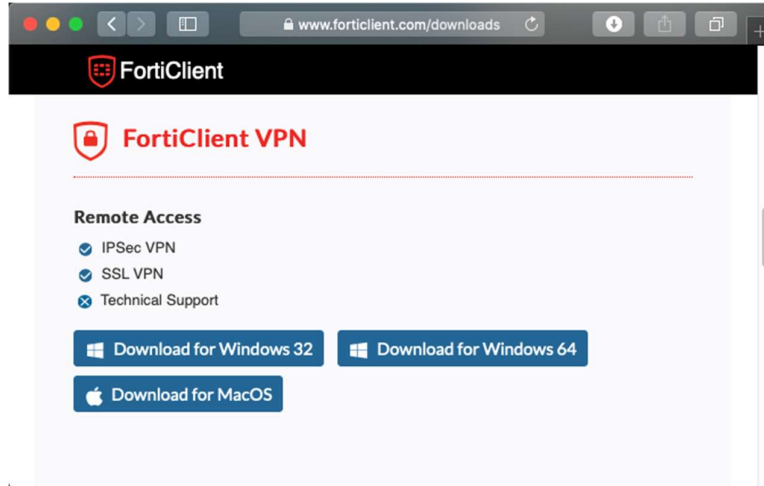
A tal proposito, assicurarsi che siano soddisfatti i seguenti prerequisiti:

1. Il PC d'ufficio deve essere lasciato **acceso**, assicurarsi che lo standby sia disabilitato
2. Nelle impostazioni Windows del PC ISPRO a cui collegarsi, sia **abilitato l'accesso remoto per l'utente aziendale** (es. *m.meoni*). Se non si dispone dei diritti di amministratore per cambiare tale impostazione, aprire un ticket al numero verde HelpDesk. La mancata abilitazione del servizio di accesso remoto genera l'errore documentato nella sezione **Risoluzione Problemi** della presente guida.
3. Sia inviato per email all'indirizzo email **accessiextranet@estar.toscana.it**, debitamente compilato negli spazi gialli, il modulo "Gestione Richieste Accesso Remoto" in calce alla presente guida (pagine 15-18). Nella stessa email mettere in copia l'indirizzo **ict@ispro.toscana.it**.
4. Sia installato sul proprio PC di casa il programma FortciClient VPN, come da istruzioni che seguono.

## Istruzioni Connessione VPN

1) Scaricare il software “FortiClient VPN” dal seguente sito, scegliendo la versione per il vostro sistema operativo:

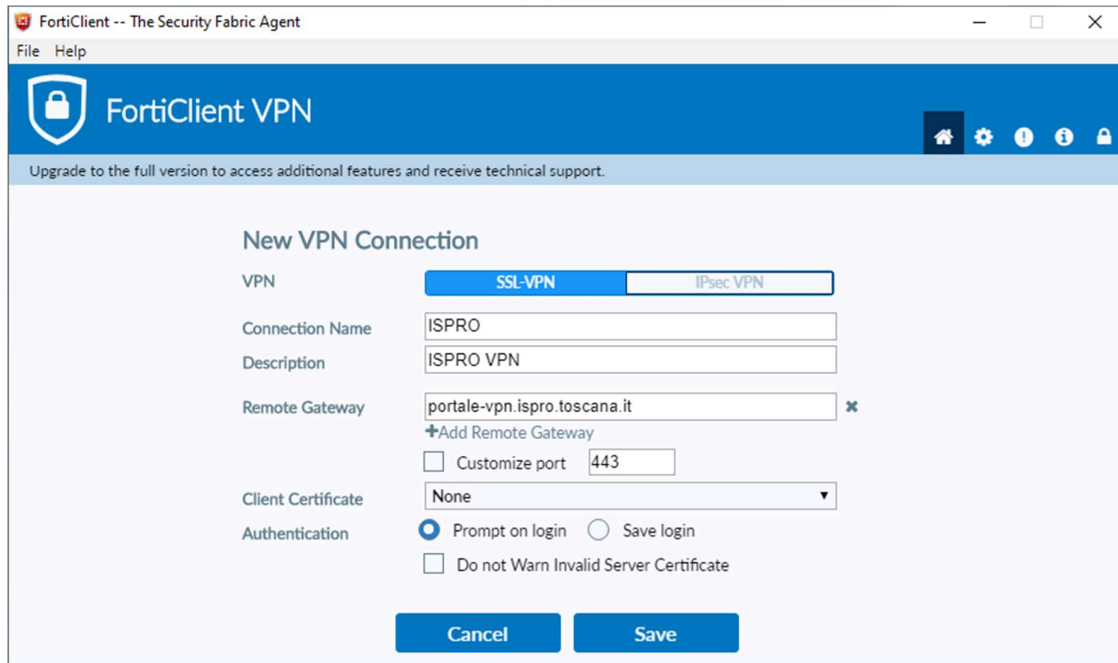
<https://forticlient.com/downloads>



2) Installare ed eseguire il software



3) Impostare al primo accesso i parametri della VPN e salvare la configurazione

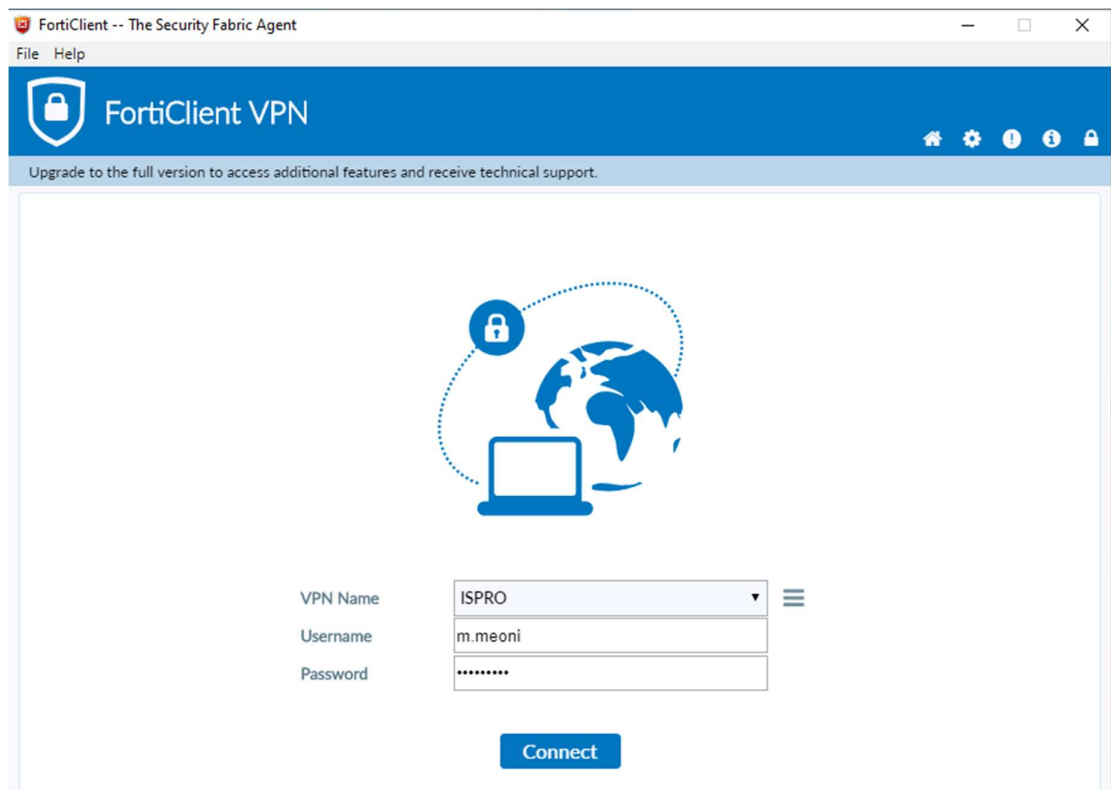


The screenshot shows the 'New VPN Connection' window in FortiClient. The window has a blue header with the FortiClient logo and title. Below the header, there's a message: 'Upgrade to the full version to access additional features and receive technical support.' The main area is titled 'New VPN Connection'. It has two tabs: 'SSL-VPN' (selected) and 'IPsec VPN'. The fields are as follows:

- VPN: SSL-VPN (selected)
- Connection Name: ISPRO
- Description: ISPRO VPN
- Remote Gateway: portale-vpn.ispro.toscana.it (with a dropdown arrow and a plus icon to add more)
- +Add Remote Gateway
- ☐ Customize port: 443
- Client Certificate: None (dropdown menu)
- Authentication: ☒ Prompt on login, ☐ Save login
- ☐ Do not Warn Invalid Server Certificate

At the bottom, there are 'Cancel' and 'Save' buttons.

4) avviare la VPN inserendo nei campi login e password le credenziali di dominio

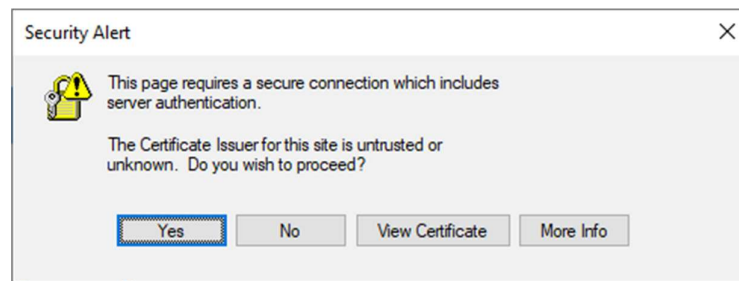


The screenshot shows the main interface of the FortiClient VPN application. It has a blue header with the FortiClient logo and title. Below the header, there's a message: 'Upgrade to the full version to access additional features and receive technical support.' The main area features a large graphic of a globe with a laptop and a lock icon, representing a secure connection. Below the graphic, there are three input fields:

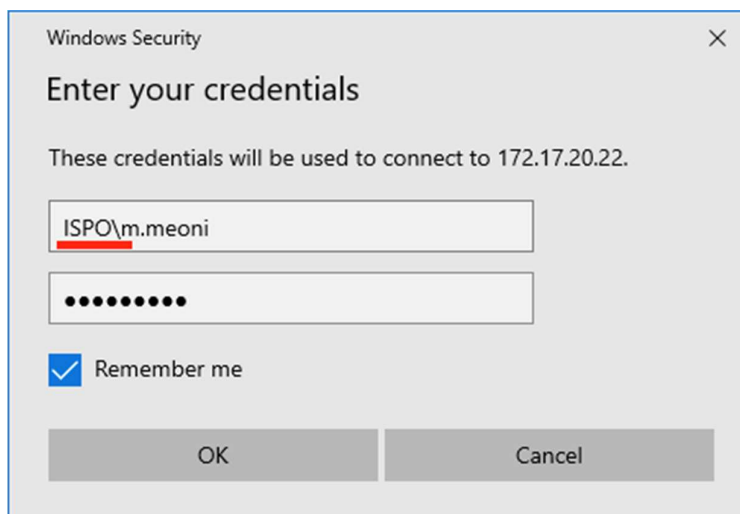
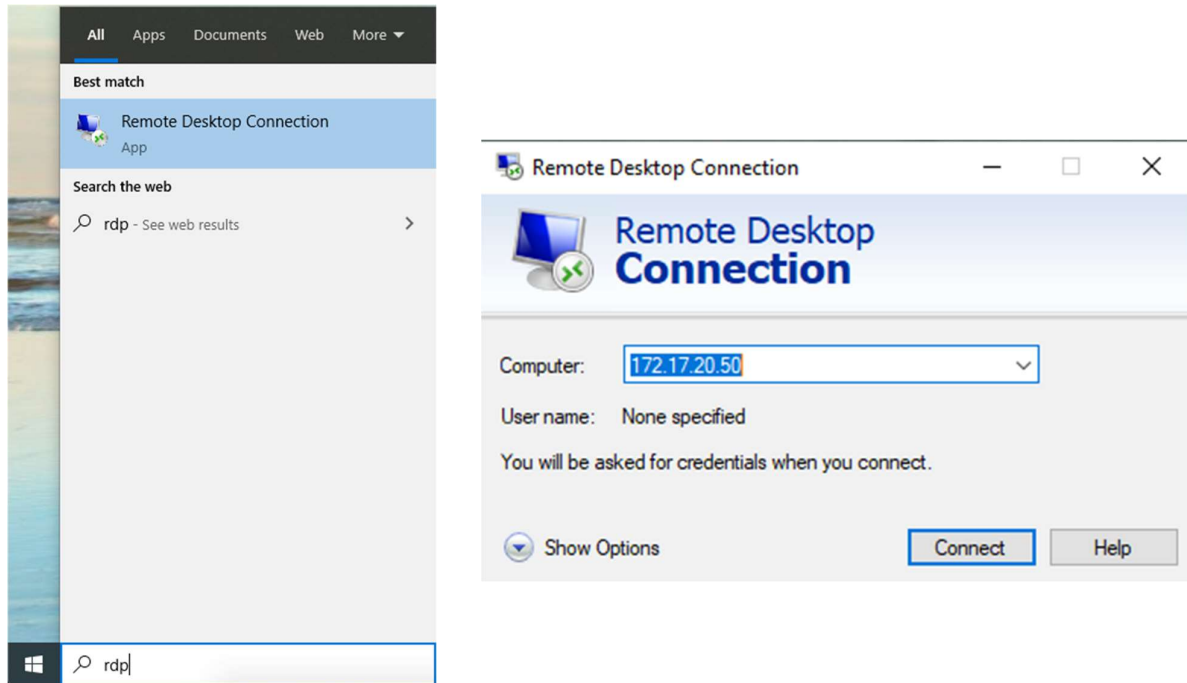
- VPN Name: ISPRO (dropdown menu)
- Username: m.meoni
- Password: (masked with dots)

At the bottom, there is a 'Connect' button.

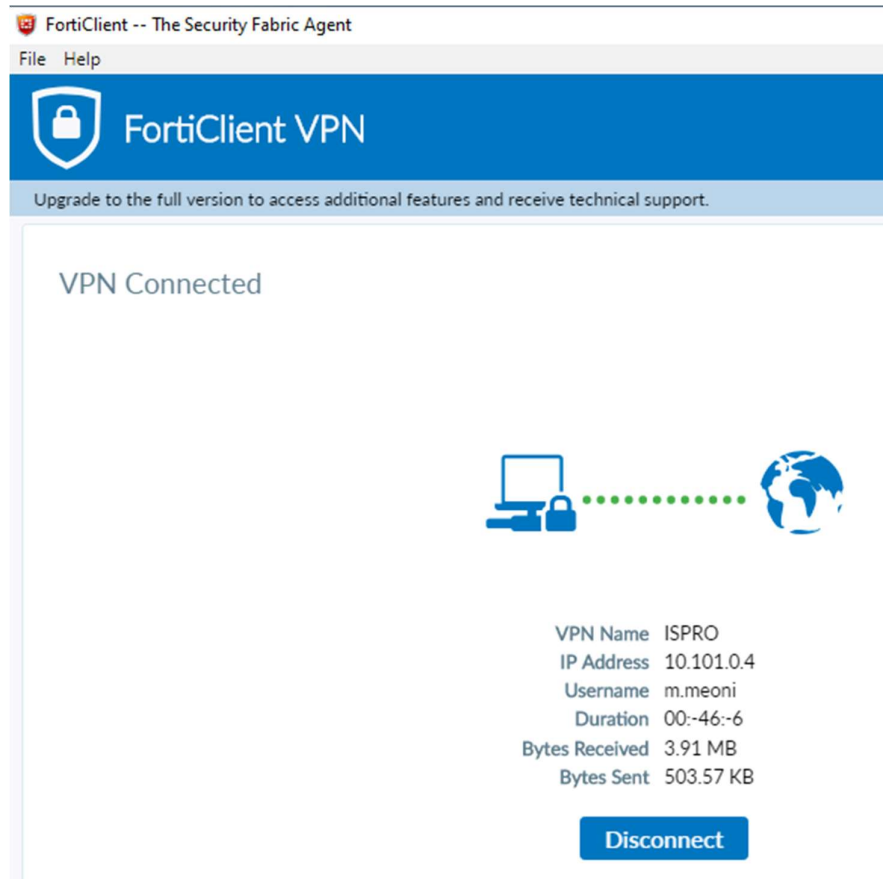
5) se richiesto, accettare la richiesta di certificato:



6) Quando la VPN è connessa, collegarsi mediante programma RDP al desktop remoto



7) Al termine della sessione di lavoro disconnettere la VPN



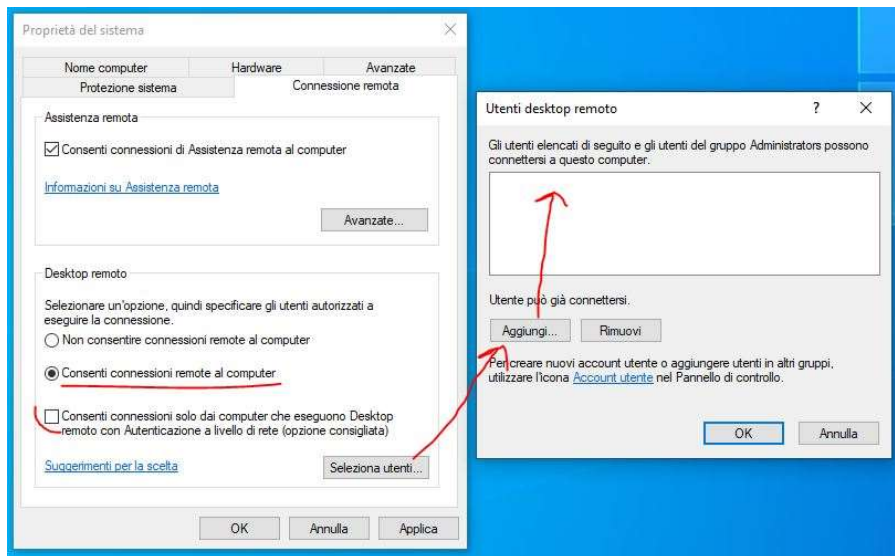


## Risoluzione Problemi



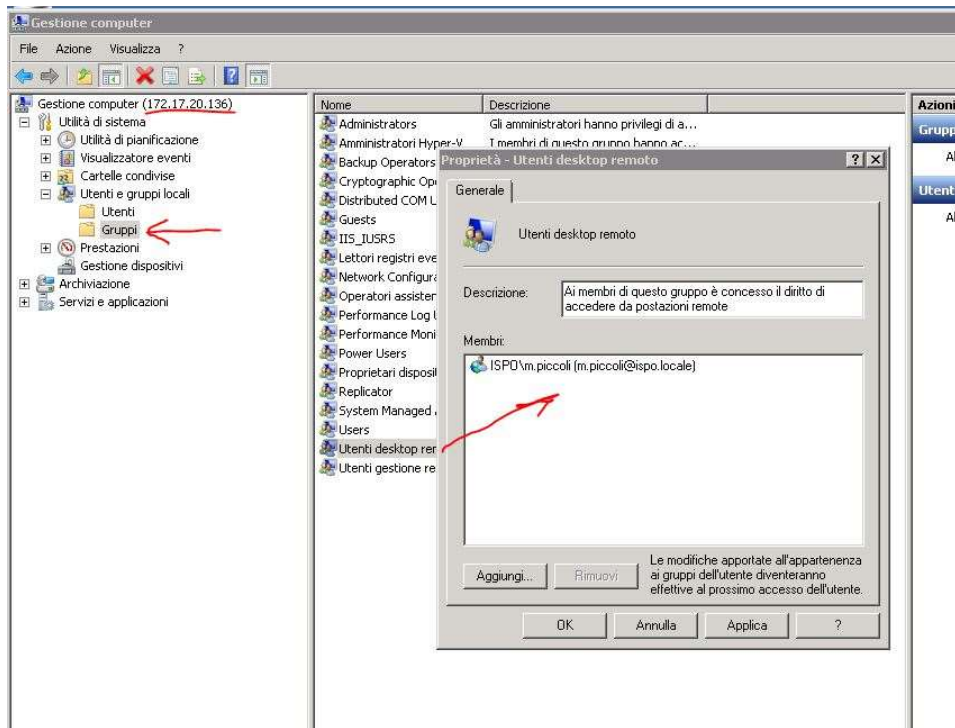
Se la connessione al proprio Desktop non funziona e appare il seguente messaggio significa che il PC in ufficio non è abilitato alla connessione remota. Procedere come segue:

1. Aprire il Pannello di Controllo di Windows > Sistema > Impostazioni Remote > Remoto e



abilitare la voce "Consenti connessioni remote su questo PC".

2. Aprire il Pannello di Controllo di Windows > Strumenti di Amministrazione > Gestione



Computer e aggiungere l'utente nel gruppo "Utenti desktop remoto"

**Se non si hanno i diritti per cambiare le due impostazioni sopra, richiedere l'intervento dell'helpdesk.**

## VideoConferenza

In modalità smartworking sono incoraggiate tutte le forme di videoconferenza individuali e di gruppo (whatsapp, skype, facetime, etc).

ISPRO mette a disposizione due piattaforme di videoconferenza, Scopia e WebEx.

### Scopia

E' possibile utilizzare la piattaforma Regionale di Web Conferenza per "incontrarsi" in Sala Incontri VdR. Tale piattaforma non ha bisogno della VPN attiva ma richiede di coordinarsi preventivamente con la Direzione Aziendale per la disponibilità.

- Per l'utilizzo da PC collegarsi all'indirizzo <https://webconference.e.toscana.it> e seguire le istruzioni (WebCam e set audio necessari)
- Per l'utilizzo da smartphone/tablet installare la app Scopia (da Play Store o App Store) e impostare 159.213.234.37 come Dekstop Server.



A questo punto indicare il numero di stanza virtuale (meeting ID) della Sala Incontri: 6825

## Webex

Cisco Webex permette di organizzare conferenze Web in autonomia con funzionalità più avanzate di Scopia. La programmazione della sala virtuale è condivisa tra tutti i dipendenti ISPRO, è buona norma pertanto programmare una conferenza con durata circoscritta alle reali necessità per non impegnare l'agenda delle prenotazioni Webex se non necessario.

Mentre per la partecipazione a un meeting è sufficiente fare click sull'invito ricevuto per email, per la programmazione e l'avvio di una riunione di cui si è organizzatori occorre seguire le seguenti istruzioni.

Cliccare il seguente link:

<https://estar-toscana.webex.com/webappng/sites/estar-toscana/dashboard?siteurl=estar-toscana>

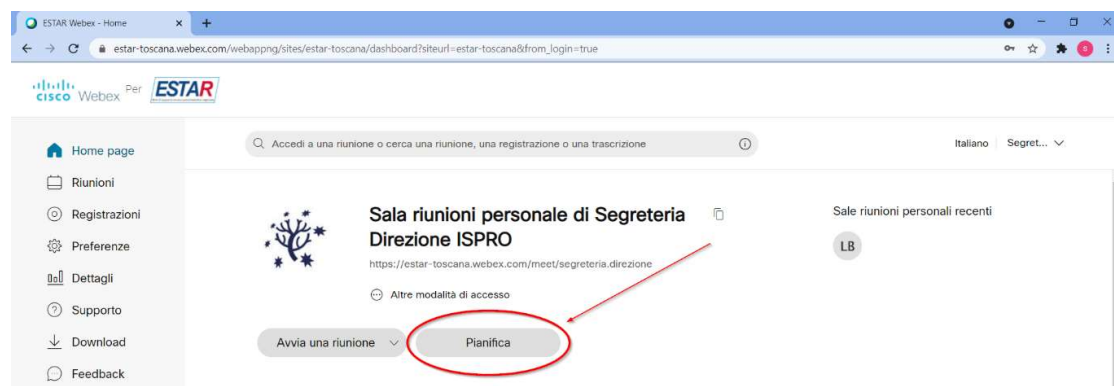
Si aprirà una pagina Internet, cliccare su **Accedi** e nei campi d'login inserire le credenziali:

-Email: webconference@ispro.toscana.it

-Password: WebEx2021#



A questo punto avrete accesso alla dashboard di Webex, cliccare sul tasto **Pianifica** per programmare la riunione:



Adesso potrete inserire i dati relativi alla riunione che volete pianificare, nello specifico:

- Argomento della riunione (a)
- Password (b) [non occorre inserire niente, la password di accesso alla riunione viene generata automaticamente dal sistema]

- Data, orario e durata della riunione (c) [cliccando sopra l'orario si apre una mascherina di inserimento]
- Partecipanti (d) [indicare gli indirizzi email dei partecipanti, che riceveranno l'invito al termine della procedura]

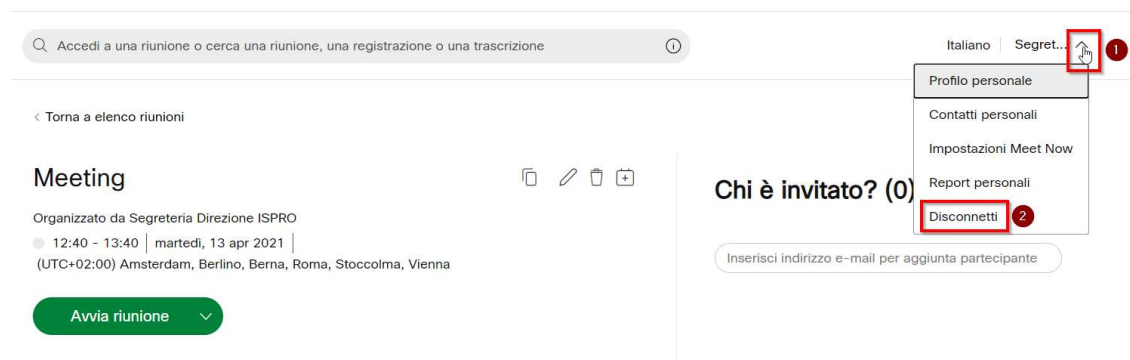
Adesso cliccare sul tasto **Pianifica** (se avete programmato una riunione in prossimità dell'orario attuale il tasto si chiamerà **Avvia**)


In seguito si verrà reindirizzati ad una pagina dove tramite semplici comandi è possibile avviare, modificare o annullare la riunione (con automatica notifica tramite email ai partecipanti).

- Cliccare il tasto “Avvia riunione” se si vuole avviare la riunione
- Cliccare il tasto “Copia” per fare una copia della riunione appena creata

- Cliccare il tasto “Modifica” per modificare i parametri precedentemente impostati
- Cliccare Il tasto “Elimina” per cancellare la riunione (con automatica notifica tramite email di annullamento ai partecipanti)

Una volta terminata la riunione eseguire il logout cliccando sull’opzione disconnetti del menu a tendina che si apre sotto il nome utente “Segreteria Direzione ISPRO”



	Ente per i Servizi Tecnico-Amministrativi Regionale	Allegato 2 PA 90/2020 TI  <b>REV00</b>  Pag. 1 di 4
	GESTIONE RICHIESTE ACCESSO REMOTO (modulo dedicato alle richieste trasmesse dai dipendenti)	

ATTENZIONE : LA PRESENTE RICHIESTA, DEVE ESSERE COMPILATA CON STRUMENTI DI VIDEOSCRITTURA (Word, LibreOffice, etc) ; TUTTI I DATI SONO OBBLIGATORI - NON SARANNO EVASE RICHIESTE INCOMPLETE E/O NON COMPILATE CON STRUMENTI DI VIDEOSCRITTURA

Al Resp.le

Area/UOC/UOS/Ref.te ICT ASL

\_\_\_\_\_  
 \_\_\_\_\_

Oggetto: Richiesta accesso remoto

Il sottoscritto \_\_\_\_\_

dipendente assegnato alla Area/UOC/UOS

\_\_\_\_\_

Recapiti per eventuali contatti:

Tel. ....

Indirizzo Posta Elettronica \_\_\_\_\_

Matricola e codice fiscale \_\_\_\_\_

### **RICHIEDE**

di essere autorizzato ad accedere attraverso connessione remota ai server/sistemi/applicativi e per le necessità di seguito elencati:

<i>server/sistema/applicativo</i>	<i>necessità di collegamento da remoto su indirizzo IP</i>
ACCESSO VPN	172.17. .

Tabella 1

In relazione ai server/sistemi/applicativi ai quali si richiede l'accesso remoto, fornisce le seguenti informazioni:

<i>server/sistema/ applicativo</i>	<i>Indirizzo IP</i>	<i>Hostname</i>	<i>Porte di accesso</i>	<i>Localizzato presso</i>

Tabella 3

Nel caso in cui la risorsa da raggiungere sia un applicativo web o una risorsa condivisa all'interno della rete, in alternativa e in mancanza di uno o più dei dati riportati nella tabella precedente, è possibile indicare il Link da raggiungere:

<i>sistema/applicativo</i>	<i>Link</i>


Tabella 4

Il personale autorizzato all'accesso remoto si impegna a:

- Non consentire a terzi, a nessun titolo, l'utilizzo dell'accesso alla rete Aziendale.
- Comunicare immediatamente a questa struttura la disdetta del servizio di accesso remoto alla rete aziendale, per qualsiasi causale, incluse, a titolo puramente indicativo e non esaustivo, l'eventuale compromissione della riservatezza delle credenziali di accesso o il decadere delle condizioni per cui si era reso necessario il servizio.
- Non immettere, trasmettere, utilizzare, diffondere qualsiasi dato che non può essere legalmente distribuito via telematica.
- Evitare attività che producano deliberatamente: abuso di risorse di rete o computazionali anche in termini di tempo dedicato da parte del personale addetto alla sua gestione, danneggiamento o compromissione di dati inclusa la loro diffusione o comunicazione a terzi, violazione della riservatezza di altri utenti, interferenze sul lavoro di altri utenti, altri usi impropri, quali l'introduzione di malware o altri meccanismi di vulnerabilità.
- Garantire di aver installato e debitamente aggiornato sul proprio dispositivo un antivirus o comunque verificato l'assenza di malware, prima di connettersi alla rete.
- Mantenere indenne l'Azienda e l'ESTAR da qualsiasi danno, perdita, costo, responsabilità, e dagli oneri di spesa che dovessero derivare da atti, fatti, comportamenti, omissioni, derivanti dal proprio accesso alla rete Aziendale.

Riconosce, inoltre, al personale ICT di ESTAR:




	Ente per i Servizi Tecnico-Amministrativi Regionale	Allegato 2 PA 90/2020 TI  <b>REV00</b>  Pag. 3 di 4
	GESTIONE RICHIESTE ACCESSO REMOTO (modulo dedicato alle richieste trasmesse dai dipendenti)	

- La possibilità di procedere in qualsiasi momento a controllare la corretta utilizzazione dell'accesso alla rete, attraverso la ricostruzione dei percorsi telematici effettuati.
- Di interrompere il servizio prestato all'utente per la mancata osservanza degli obblighi assunti, ivi compresa la palese violazione della normativa vigente in tema di uso dei dati e degli strumenti della P.A., fatta salva la possibilità di sua esposizione a sanzioni disciplinari e la facoltà, per ESTAR, di richiedere il risarcimento degli eventuali danni

Data

Il richiedente

	Ente per i Servizi Tecnico-Amministrativi Regionale	Allegato 2 PA 90/2020 TI
	GESTIONE RICHIESTE ACCESSO REMOTO (modulo dedicato alle richieste trasmesse dai dipendenti)	<b>REV00</b> Pag. 4 di 4

Al Resp.le

UOC Reti e Sistemi

*Modulo da compilare  
ad opera del resp.le  
struttura/ref.te ICT*

ESTAR – Regione Toscana

Il sottoscritto MEONI MARCO in qualità di responsabile della struttura/ref.te ICT per ISPRO

### **AUTORIZZA**

la UOC Reti e Sistemi a procedere con le attività di competenza finalizzate alla realizzazione del collegamento oggetto della presente richiesta.

VISTO SI AUTORIZZA