SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Modena

Guida per la richiesta, installazione e accesso della VPN aziendale con autenticazione multi-fattore.

L'Ausl ha attivato una modalità di accesso alla rete interna tramite VPN tramite un sistema di autenticazione multi fattore. Tale sistema consente **l'accesso alla VPN tramite due step di inserimento:**

1. le credenziali di dominio del singolo operatore, cioè lo **username e la password di dominio personali** (le stesse utilizzate per accedere al PC e agli applicativi, come ad esempio il portale WHR)

2. **un "secondo fattore" di autenticazione** che viene **generato da una specifica App configurata su uno smartphone**.

Questo sistema risponde a **livelli di sicurezza informatica più elevati** ed evita, in caso di furto delle credenziali personali, che un malintenzionato possa accedere alla rete aziendale usando la password rubata (a meno che l'utente non abbia salvato impropriamente anche il proprio username e la password aziendale sul telefono).

Questo documento è suddiviso in **3 aree tematiche**, con l'obiettivo di spiegare e accompagnare l'utente passo passo; dalla fase di abilitazione e configurazione del sistema fino all'accesso ordinario alla VPN:

1) Prerequisiti obbligatori. Cosa deve possedere l'utente prima di accedere alla VPN
2) Configurazione della App Microsoft Authenticator e del PC all'uso della VPN
3) Accesso ordinario alla VPN

Prerequisiti obbligatori. Cosa deve possedere l'utente prima di accedere alla VPN:

1) **Credenziali di dominio personali**: cioè username e password aziendali personali utilizzati per accedere al proprio PC aziendale.

2) Impostare una **password di dominio sicura**: la password per considerarsi sicura deve essere scelta e impostata dall'utente, secondo la policy aziendale, combinando più elementi in questo modo:
   > **lunga**: deve avere **almeno 8 caratteri** (ma anche di più)

   > **mista**: deve contenere **caratteri alfanumerici maiuscoli e minuscoli** (cioè sia numeri che lettere scritte sia in maiuscolo che in minuscolo) e **caratteri speciali** (esempio: ! & # ? ^ ecc...)

   > **senza senso**: **evita nomi e/o parole comuni (**come ad esempio il nome di un figlio o le stagioni), date di nascita a te affini che potrebbero essere facilmente scoperte dagli hacker

> **sempre diversa**: non usare la stessa password di dominio aziendale per altri siti esterni all'Ausl o applicativi che non siano quelli aziendali/regionali automaticamente riconosciuti dal sistema

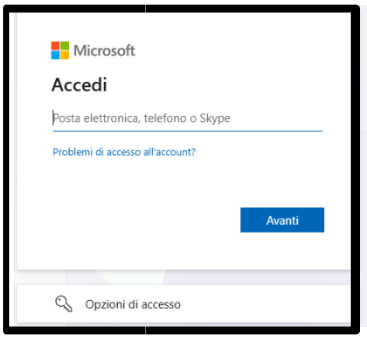
3) Uno **smartphone personale** (cioè NON un cellulare condiviso con altre persone) che può essere sia privato che aziendale. Su tale dispositivo è necessario installare la App "Microsoft Authenticator" che, collegata al proprio username aziendale, assicura il "secondo fattore di autenticazione" per completare l'accesso alla VPN.

4) **Autorizzazione all'uso della VPN**: è necessario chiedere l'abilitazione alla VPN al Servizio ICT secondo la procedura aziendale disponibile alla pagina intranet www/faq-ict alla FAQ n.13 "Richiesta di abilitazione alla VPN aziendale".

Configurazione della App Microsoft Authenticator e del PC all'uso della VPN

1) Collegarsi al sito https://access.ausl.mo.it

Si aprirà la pagina di login Microsoft:

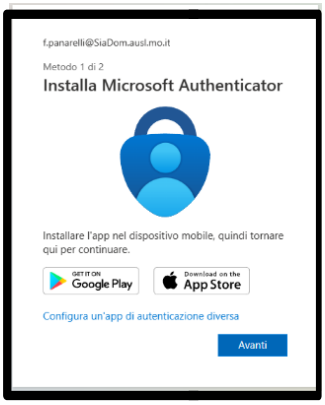


2) Inserire le proprie credenziali di dominio.
N.B il nome utente deve essere seguito dal suffisso "**@siadom.ausl.mo.it**". Una volta inserita la password cliccare su "**Accedi**"

3) A questo punto ti verrà richiesta di installare l'app **Microsoft Authenticator** sul tuo smartphone.
Clicca su "**Avanti**"

4) Installa **l'App**: Scarica e installa l'App Microsoft Authenticator sul tuo dispositivo mobile dall'App Store (iOS) o Google Play Store (Android).

5) Una vota installata l'app sullo smartphone Selezionare "**Avanti**".

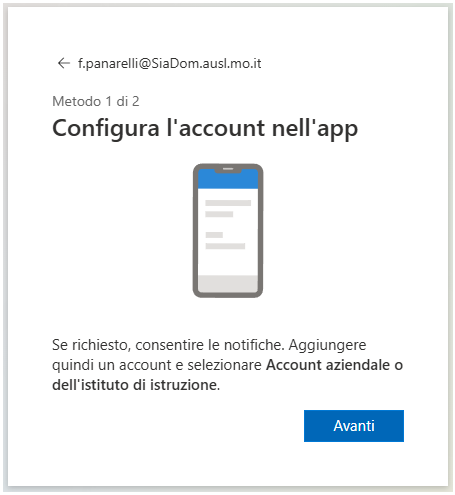


6) Apri l'App Microsoft Authenticator sul tuo telefono.

Metodo 1 - Collega il dispositivo Manualmente

Seleziona +: Tocca l'icona del segno più (+) per aggiungere un nuovo account.

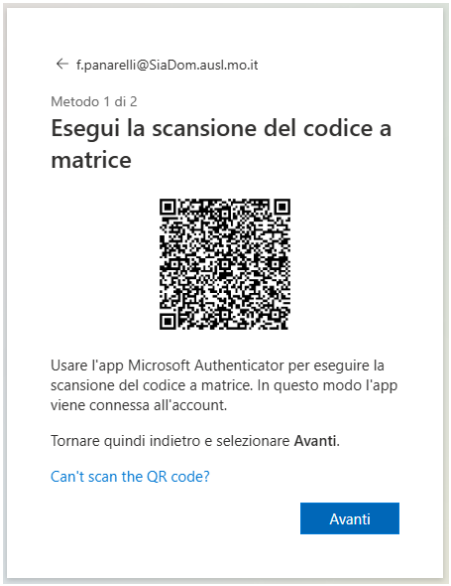
Scegli il tipo di account: Seleziona "Account aziendale o dell'istituto di istruzione" o "Account personale" se stai configurando un account Microsoft personale.



Selezionare “Avanti”.

Metodo 2 - Collega il dispositivo tramite scansione QR

Scansiona il codice QR: Sul tuo computer, accedi alla sezione "Informazioni di sicurezza" del tuo account (ad esempio, account.microsoft.com/security) e segui le istruzioni per "Aggiungi un nuovo modo per accedere" o "Aggiungi metodo" selezionando "Microsoft Authenticator". Ti verrà mostrato un codice QR da scansionare.

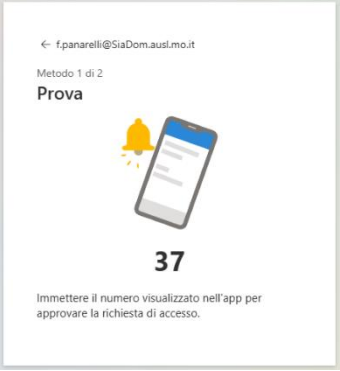


Inquadra il codice: Usa l'App Microsoft Authenticator per scansionare il codice QR visualizzato sullo schermo del tuo computer. Se non riesci a usare la fotocamera, puoi toccare "Non riesco a scansionare il codice" per inserire il codice manualmente.

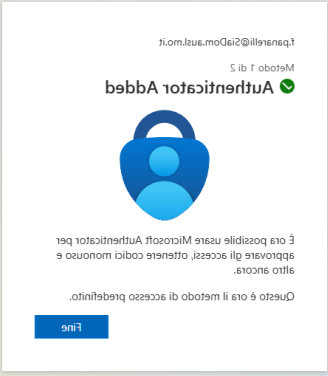
Conferma sul telefono: Una volta scansionato il codice, l'account verrà aggiunto all'app. Potrebbe apparire un messaggio di conferma che ti chiede di approvare la notifica push.

Selezionare “Avanti”.

Inserisci il Codice che compare sullo schermo del tuo computer nello smartphone

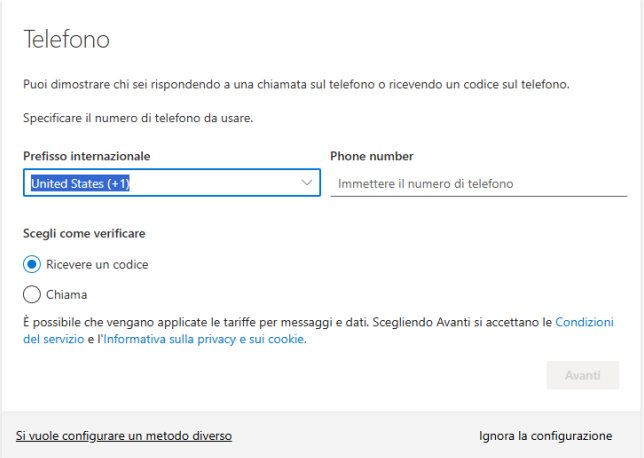


Una volta inserito il codice sullo smartphone la configurazione e terminata.

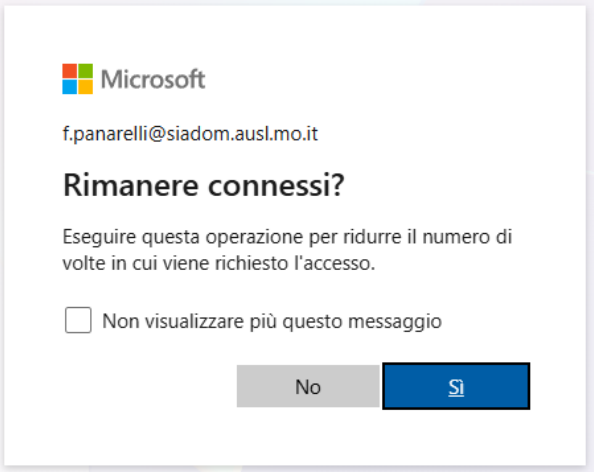


Cliccando su Fine, verrà richiesto di aggiungere il proprio numero di telefono per la verifica:

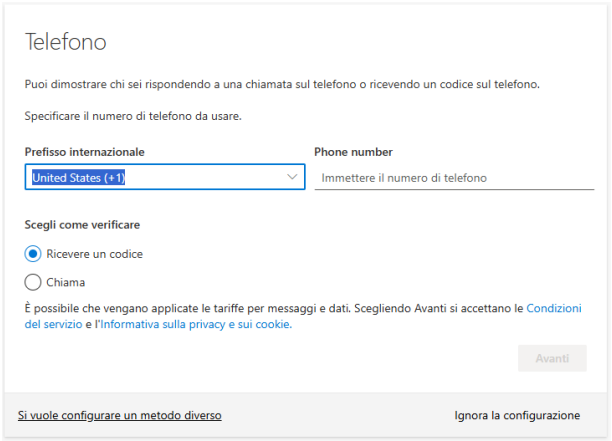
- Selezionare il prefisso del paese;
- Inserire il proprio numero di cellulare;



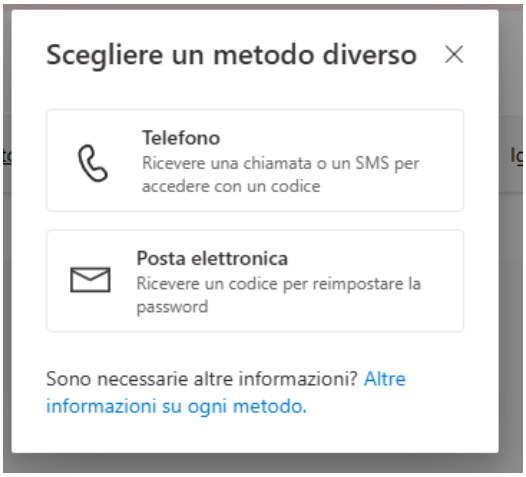
Selezionare "**Sì**".



In alternativa cliccando in basso a sinistra su “**Si vuole configurare un metodo diverso**”



Si può ricevere il codice di verifica sulla propria casella di posta elettronica cliccando su “Posta elettronica”



Controlla il risultato: Verifica che l'account sia stato aggiunto con successo e che ora appaia nell'App.

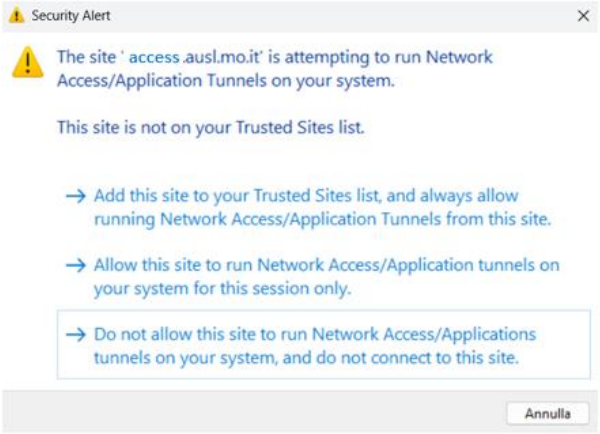
Dopo l'avvenuta autenticazione è possibile avviare il componente F5 come da cliccano su "Start".

Comparirà un popup che chiederà conferma dell'avvio del componente, mettere la spunta su "Consenti sempre a access.ausl.mo.it di aprire link di questo tipo n.."

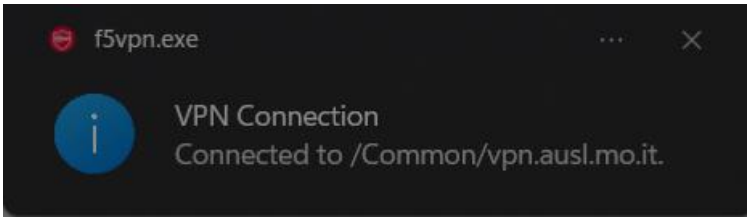
E chiederà conferma dell'aggiunta nei siti attendibili.

Cliccare sulla prima opzione:

" → Add this site to your. Trusted Site List, and allow running Network Access/Application Tunnel from this site."



In seguito, si avvierà l'effettiva connessione VPN come al solito. L'avvio della connessione viene confermato da una notifica che comparirà per qualche secondo sul monitor iIn basso a sinistra.



SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Modena

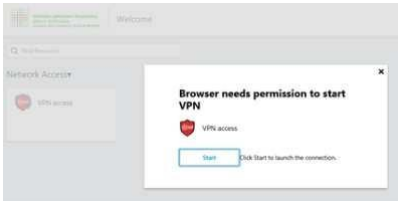
Accesso ordinario alla VPN

1. Dal PC (connesso ad una wi-fi esterna all'Ausl, come ad esempio la rete di casa propria) apri il browser Edge, e vai su **https://access.ausl.mo.it**

2. Sul monitor del PC si apre automaticamente una schermata simile a quella a lato. Inserire le proprie credenziali di dominio seguite dal suffisso "@siadom.ausl.mo.it" e cliccare su **accedi**.

3. Sarà quindi sufficiente approvare la richiesta di accesso dal proprio smartphone inserendo nell'app Microsoft Authenticator il numero visualizzato nella schermata.

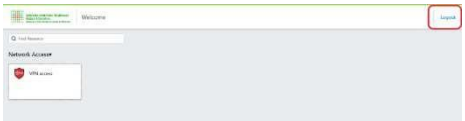
4. Ecco che sul monitor del PC si apre la schermata di collegamento: clicca su Start per completare l'accesso e avviare il collegamento VPN.



L'avvio della connessione viene confermato da una notifica che comparirà per qualche secondo sul monitor.

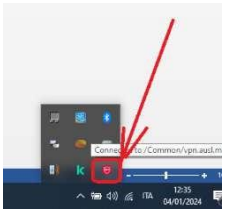
E' ora possibile navigare in intranet, accedere alle cartelle e/o agli applicativi d'uso o connettersi in remoto ad un eventuale PC fisso abilitato in azienda.

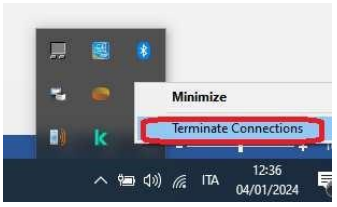
5. Una volta terminata l'attività, per disconnettersi (o uscire) dalla VPN ci sono 2 possibilità:



- clicca su Logout (in alto a destra della pagina di accesso alla VPN)

- oppure clicca con il tasto destro del mouse sull'icona che trovi in basso a destra monitor e, di nuovo, clicca su "Terminate Connections"





NOTE UTILI

➢ Accesso alle directory di rete

Dopo aver cliccato sulla directory (o cartella di rete) da aprire, è necessario inserire le proprie credenziali di dominio (utente e password aziendali) nella maschera che appare a video. Nel campo "nome utente" è necessario inserire il proprio user name preceduto da "SIADOM\", ad esempio "SIADOM\rossim"