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

Versione del 25/01/2024

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 WALLIX 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 "WALLIX 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".
L'ICT procede ad abilitare l'operatore e, dall'indirizzo support-noreply@trustelem.com, gli invia una mail contenente n link sicuro che servirà per configurare la procedura sulla app WALLIX.

Attenzione! Nel mese di gennaio 2024 è programmata la riattivazione della VPN a seguito dell'attacco hacker. Gli operatori che prima del 28/11/2023 utilizzavano già la VPN per lo smart working, NON devono richiedere alcuna autorizzazione all'ICT che, automaticamente e in modo progressivo invierà l'e-mail da support-noreply@trustelem.com

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

Solo dopo aver ricevuto l'autorizzazione all'uso della VPN da parte dell'ICT e la mail dall'indirizzo support-noreply@trustelem.com è possibile configurare la App WALLIX Authenticator.

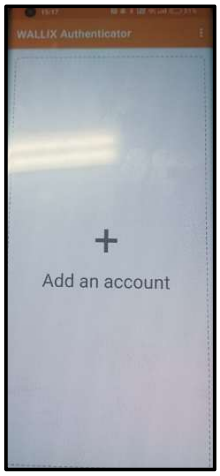
1. Dallo store dello smartphone cerca e installa la app "WALLIX Authenticator". Una volta installata, aprila e consenti l'invio delle notifiche.

2. **Da un PC** accedi alla tua posta aziendale, apri l'e-mail ricevuta da support-noreply@trustelem.com e clicca sul link sicuro presente.

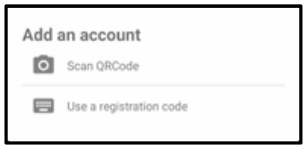
3. Dopo aver cliccato il link nella mail, a video compare la videata a lato.

   Attenzione: il QR Code è nominativo, quindi NON tentare di inquadrare l'esempio di QR a lato.

4. Dalla App WALLIX Authenticator, clicca sul simbolo "+Add Account/Aggiungi un account" che, a seconda del tipo di smartphone (Android/Apple) trovi o al centro dello schermo o in alto a destra.



5. Per precedere con la configurazione clicca:
   - "Scan QRCode" se vuoi scansionare il QR ricevuto via mail
   - oppure su "Use a registration code" se preferisci inserire manualmente il codice di registrazione ricevuto sempre nella stessa mail.

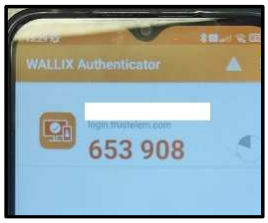


Attenzione!

Se inquadri il QR devi anche consentire all'App di scattare foto e registrare video"

6. Così facendo si completa la creazione dell'account sullo smartphone e l'e-mail ricevuta da support-noreply@trustelem.com si chiude automaticamente.

7. Contemporaneamente sulla app viene generato il codice di 6 cifre necessario a completare la configurazione della app e l'abilitazione dell'utente.



La procedura di configurazione illustrata va eseguita SOLO la prima volta e solo per la configurazione. Chiudere la app.

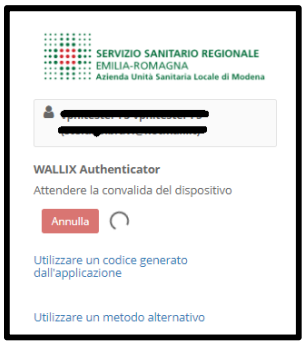
In caso di problemi alla configurazione è possibile richiedere assistenza informatica all'**HelpDesk** tramite i canali indicati sia nella pagina intranet specifica www/vpn sia nella pagina www/faq-ict

Accesso ordinario alla VPN

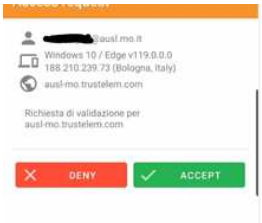
1. Sullo smartphone apri la App WALLIX
2. Dal PC (connesso ad una wi-fi esterna all'Ausl, come ad esempio la rete di casa propria) apri il browser Edge, e vai su **https://vpn.ausl.mo.it**

   Per effettuare il login inserisci le credenziali di dominio e premi il tasto "Sign in".
   Se non ricordi la password clicca su "Password dimenticata" e segui la procedura di recupero illustrata nelle note in calce.

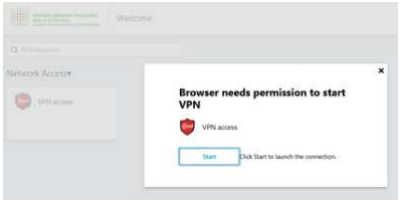
3. Sul monitor del PC si apre automaticamente una schermata simile a quella a lato.



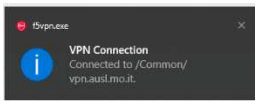
Contemporaneamente la app WALLIX apre sullo smartphone una schermata come quella a lato, sulla quale è necessario cliccare "ACCEPT" per connettere la VPN.



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.

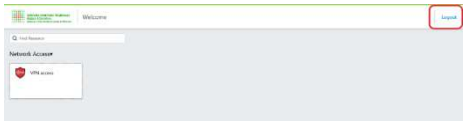


L'avvio della connessione viene confermato da una notifica che comparirà per qualche secondo sul monitor.

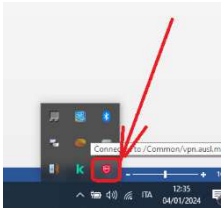


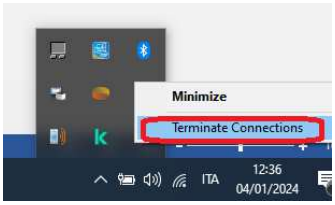
E' ora possibile navigare in intranet, accedere alle cartelle e/o agli applicativi d'uso o connettersi in remoto ad un eventuale PC fisso abilitato in azienda.

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"