SOPHOS

Cybersecurity made simple.

Sophos Connect

Guida in linea

Sommario

Informazioni su Sophos Connect....1
Installazione di Sophos Connect....1
Disinstallazione di Sophos Connect....1
Connessioni....2
Eventi....11
Risoluzione generale dei problemi....18
Informazioni su Sophos Connect Admin....22
Modifica dei file di configurazione....22
Note legali....24

1 Informazioni su Sophos Connect

Sophos Connect è un client VPN che può essere installato su Windows e Mac. Permette agli utenti di connettersi da una posizione remota alle reti protette da XG, come ad es. la rete aziendale. L'amministratore del firewall configurerà i dettagli della connessione nel firewall e fornirà all'utente il pacchetto di installazione e i file di configurazione.

Questa guida fornisce informazioni su come utilizzare Sophos Connect:

- Per istruzioni su come installare e disinstallare Sophos Connect, vedere Installazione di Sophos Connect (pagina 1).
- Per istruzioni sull'importazione dei file di connessione e sulla gestione delle connessioni, vedere Connessioni (pagina 2).
- Per istruzioni sugli eventi e su come risolvere gli errori degli eventi, vedere Eventi (pagina 11).
- Per risolvere problemi che non sono elencati nella sezione Eventi, vedere Risoluzione generale dei problemi (pagina 18).

1.1 Installazione di Sophos Connect

Installazione di Sophos Connect su Windows

- Aprire il programma di installazione.
- Accettare il contratto di licenza e cliccare su **Installa**.
- Una volta completata l'installazione, cliccare su **Fine**. È possibile scegliere di avviare Sophos Connect dopo la chiusura del programma di installazione.

Installazione di Sophos Connect su Mac

- Aprire il programma di installazione.
- Selezionare la destinazione dell'installazione. Verificare che sia presente sufficiente spazio disponibile nella destinazione selezionata, ad es. l'unità di sistema.
- Cliccare su **Installa**.
- Una volta completata l'installazione, cliccare su **Fine**.

1.2 Disinstallazione di Sophos Connect

Disinstallazione di Sophos Connect da Windows

- Aprire il **Pannello di controllo** e sotto **Programmi** cliccare su **Disinstalla un programma**.
- Cliccare con il tasto destro del mouse su Sophos Connect e selezionare **Disinstalla**.

Disinstallazione di Sophos Connect da Mac

- Aprire il terminale.
- Elevare le autorizzazioni a livello root e disinstallare lo script dal percorso su cui è installata Sophos Connect:

  ```
  sudo /Library/Sophos Connect/uninstall.sh
  ```

Se la disinstallazione viene completata correttamente, verrà visualizzato il seguente messaggio:

```
Sophos Connect has been uninstalled
```

1.3 Connessioni

È possibile importare connessioni, stabilire connessioni e visualizzare e modificare connessioni.

Sophos Connect supporta VPN SSL e VPN IPsec.

1.3.1 Importazione delle connessioni

Sophos Connect Client può connettersi a XG Firewall utilizzando connessioni VPN SSL o IPsec. È possibile importare connessioni in Sophos Connect Client.

Introduzione

Per la versione 2.0 di Sophos Connect Client, è possibile importare sia connessioni VPN SSL che IPsec. Se si utilizza una versione meno recente di Sophos Connect Client, è possibile importare solo connessioni IPsec.

Questa pagina fornisce informazioni su come eseguire le seguenti operazioni:

- Importare una connessione IPsec utilizzando un file fornito dall'amministratore.
- Importare una connessione SSL utilizzando un file fornito dall'amministratore.
- Importare una connessione SSL scaricando un file dal portale utenti.

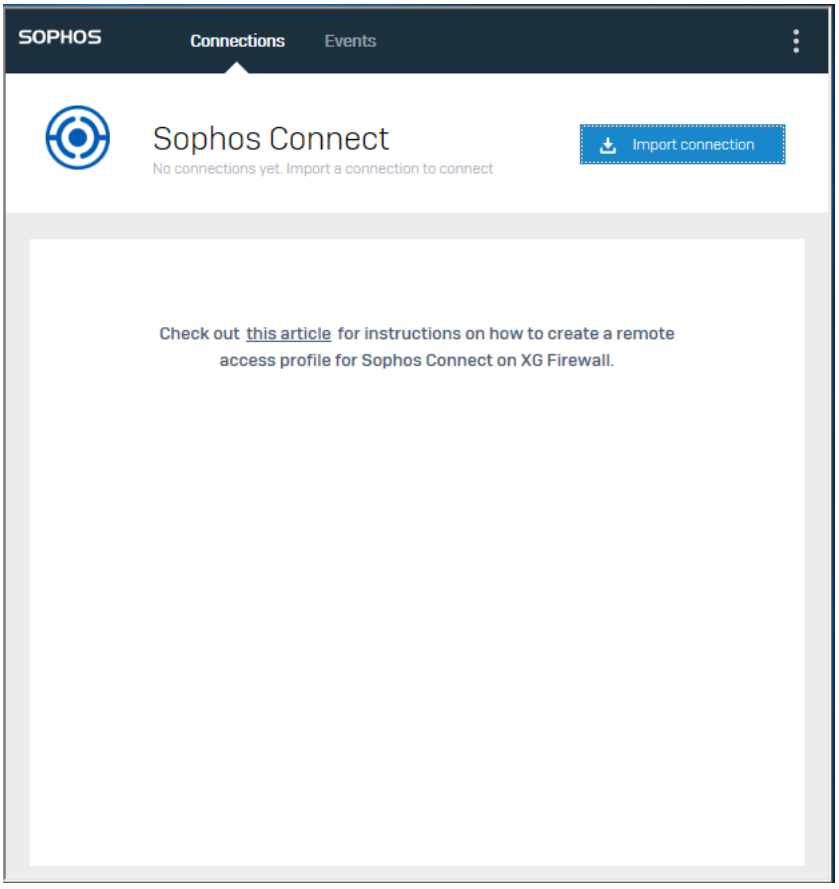
Importazione di una connessione IPsec

È stato fornito un file di connessione. Ha l'estensione `tgb`, ad es. `Connessione_azienda.tgb`.

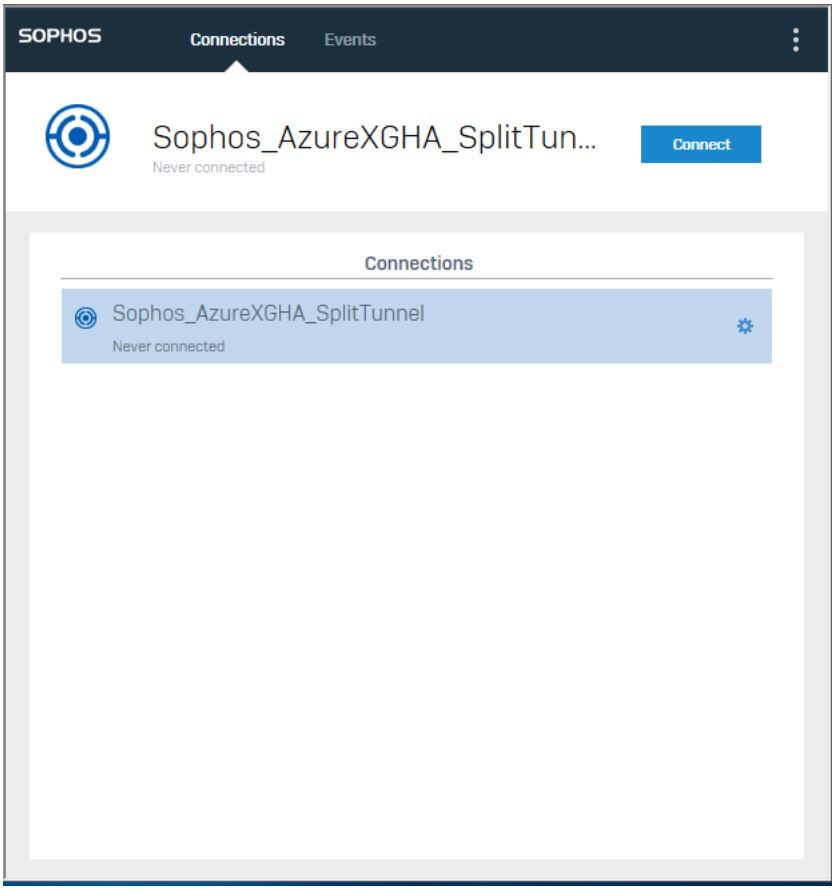
Per importare una connessione:

1. Cliccare su **Importa connessione** nella pagina **Connessioni**.

   Se sono già presenti connessioni, cliccare sul pulsante del menu e selezionare **Importa connessione** dal menu a discesa.



2. Cercare e fare doppio clic sul file `.tgb`.
   La connessione verrà visualizzata sotto **Connessioni**.



Sarà ora possibile stabilire la connessione.

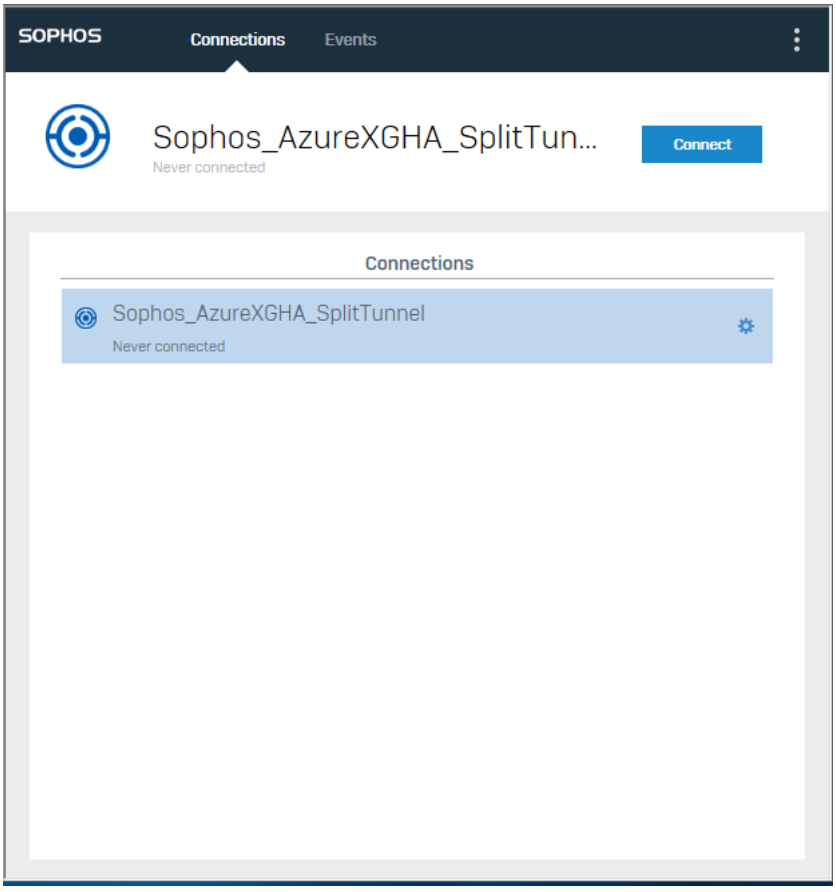
Nota
È possibile importare connessioni multiple.

Importazione di una connessione SSL

È stato fornito un file di connessione. Ha l'estensione `pro`, ad es. `Connessione_azienda.pro`.

Per importare una connessione:

Cercare e fare doppio clic sul file `.pro`.
La connessione sarà importata automaticamente e Sophos Connect verrà aperta. La connessione verrà visualizzata sotto **Connessioni**.



Sarà ora possibile stabilire la connessione.

Nota
È possibile importare connessioni multiple.

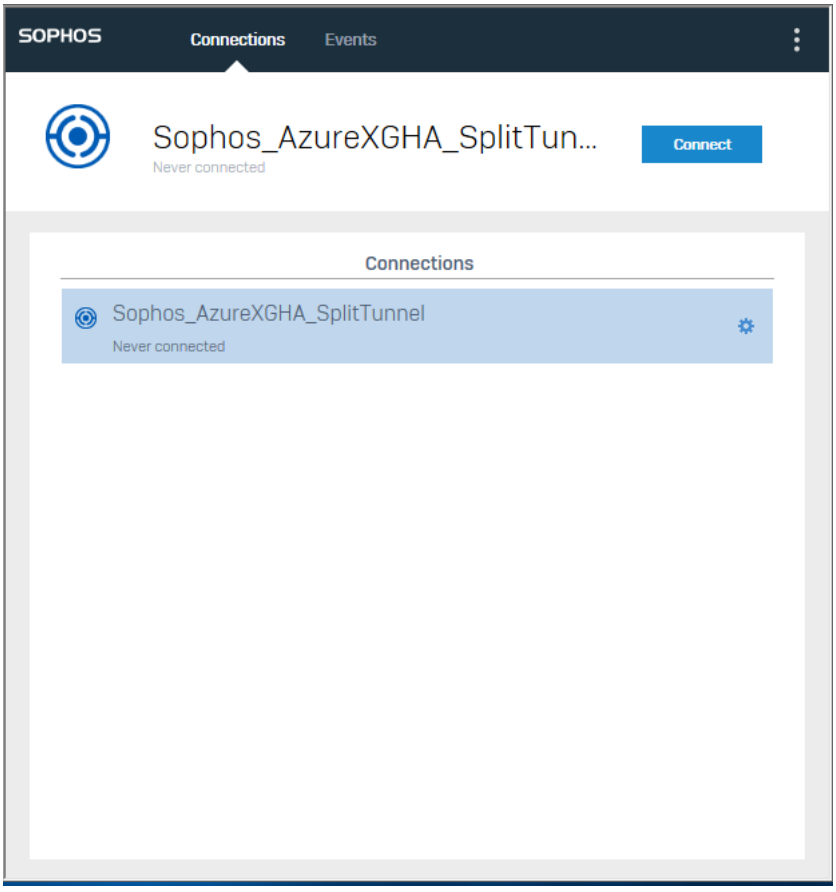
Importazione di una connessione SSL dal portale utenti

Per importare una connessione:

1. Accedere al portale utenti.
2. Selezionare **SSLVPN** e cliccare su **Scarica configurazione per altri sistemi operativi**.
3. Aprire Sophos Connect Client.
4. Cliccare su **Importa connessione** nella pagina **Connessioni**.

   Se sono già presenti connessioni, cliccare sul pulsante del menu e selezionare **Importa connessione** dal menu a discesa.
5. Cercare e aprire il file `.ovpn`.

La connessione verrà visualizzata sotto **Connessioni**.



Sarà ora possibile stabilire la connessione.

Nota
È possibile importare connessioni multiple.

1.3.2 Connetti

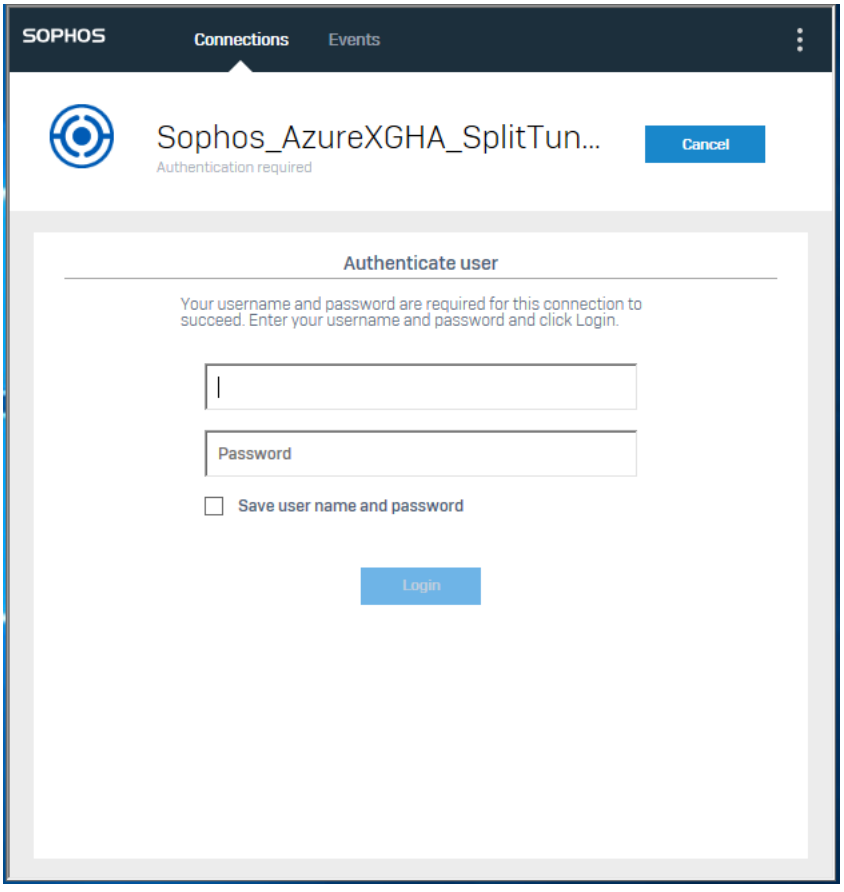
Verificare che sia disponibile almeno una connessione importata e accertarsi di disporre delle credenziali richieste.

Per stabilire una connessione:

1. Selezionare una connessione nella pagina **Connessioni**.
2. Fare doppio clic sulla connessione.

   È anche possibile cliccare su **Connetti**.

   Verrà visualizzata la schermata di accesso.



3. Inserire nome utente e password e cliccare su **Accedi**.

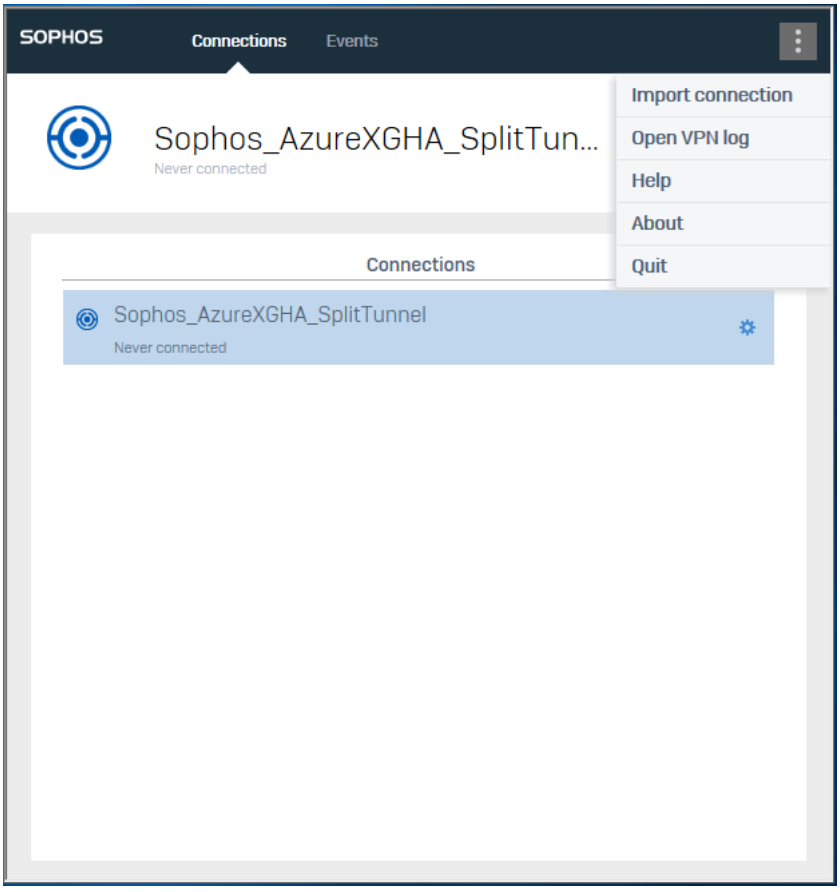
   L'amministratore potrebbe aver configurato l'autenticazione a due fattori.

   - Se l'amministratore ha configurato OTP (one-time password), oltre a nome utente e password, occorrerà immettere anche il passcode OTP a 6 cifre.
   - Se l'amministratore ha configurato l'autenticazione DUO, si potrebbero ricevere uno o due messaggi di DUO durante il processo di connessione.

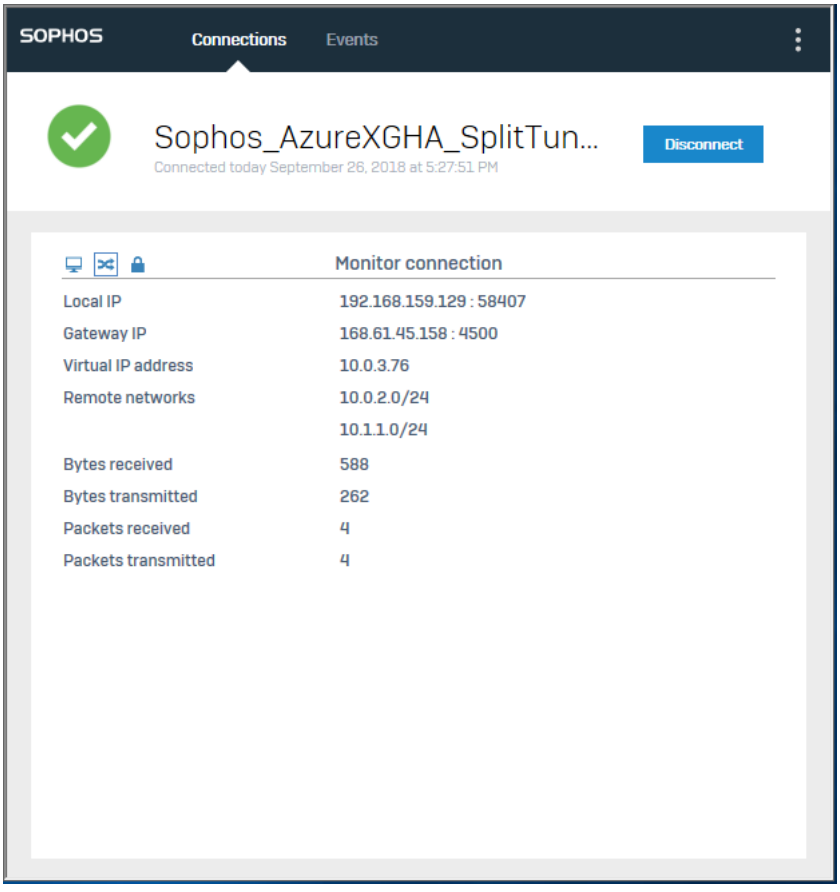
   Nota
   Se la connessione è stata importata utilizzando un file di provisioning, verrà visualizzato un avviso che indicherà che non è possibile verificare il certificato del server. Cliccare su **OK** per continuare. Se non si desidera visualizzare il messaggio, contattare l'amministratore.

   Sophos Connect tenta di stabilire la connessione ed effettuare l'autenticazione.

   Nota
   Se si dovessero riscontrare problemi di connessione, consultare la pagina **Eventi** e contattare il proprio reparto IT. È anche possibile controllare i log della VPN cliccando sull'icona del menu e selezionandoli.



La connessione al server remoto è stata stabilita.



Se la connessione viene stabilita correttamente, verrà visualizzata questa icona nella barra delle applicazioni:

Se la connessione non viene stabilita correttamente, verrà visualizzata questa icona nella barra delle applicazioni:

Nota
Se il nome della connessione è stato modificato, nei dettagli della connessione verrà visualizzato il nome originale, fornito dall'amministratore del firewall. Per istruzioni su come modificarne il nome, vedere Opzioni di connessione (pagina 9).

1.3.3 Opzioni di connessione

In Sophos Connect è possibile effettuare varie modifiche alle connessioni, cliccando sull'icona delle impostazioni, a destra della connessione.

1. **Connessione automatica** effettua un tentativo di connessione quando viene avviata Sophos Connect.
2. **Elimina** elimina la connessione, pertanto se si desidera riattivarla, occorrerà effettuarne nuovamente l'importazione.
3. **Rinomina** offre l'opzione di modificare il nome della connessione.
4. **Cancella credenziali** cancella le credenziali memorizzate in passato.
5. **Aggiorna criterio** (disponibile solo se la connessione è stata creata utilizzando un file di provisioning) consente di recuperare su richiesta il criterio più recente da XG Firewall.

Consiglio
Se dopo vari tentativi non fosse possibile stabilire la connessione, avviare un aggiornamento dei criteri e ritentare la connessione.

1.4 Eventi

È possibile visualizzare tutte le azioni all'interno di Sophos Connect e verificarne i risultati. Sono inclusi gli errori derivati dalle azioni degli utenti e gli errori delle negoziazioni IKE. Per risolvere gli errori degli eventi, vedere Risoluzione degli eventi (pagina 12)

- Se per la risoluzione di un problema è richiesta una descrizione dettagliata dell'errore, cliccare su **Apri log VPN**.
- Per rimuovere eventi dall'elenco, cliccare su **Cancella eventi**.

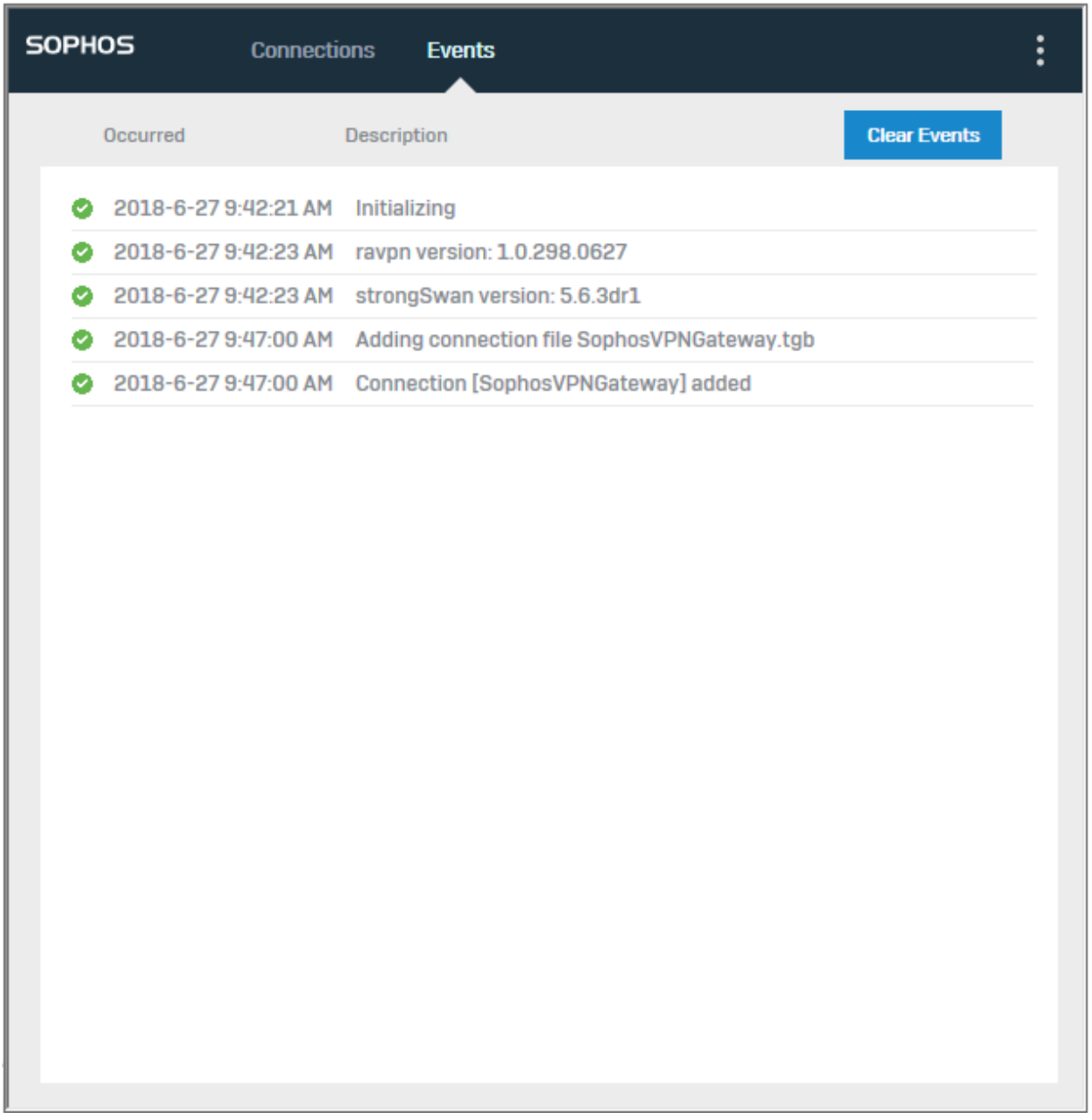


Figura 1: Eventi

1.4.1 Risoluzione degli eventi

Se si dovessero riscontrare problemi di connessione, cliccare su **Eventi**, cercare la data e l'ora di un tentativo di connessione e individuare l'errore pertinente.

Questa sezione descrive i messaggi di errore e le loro potenziali cause, fornendo informazioni utili su come procedere. Se si dovessero riscontrare problemi che non sono elencati di seguito, consultare l'argomento Risoluzione generale dei problemi.

Per ulteriore assistenza, contattare il Supporto tecnico Sophos.

Nessuna connessione di rete

Causa: la scheda di rete (Ethernet o Wi-Fi) non ha alcun indirizzo IP.

Come procedere: verificare di avere un indirizzo IP valido e controllare il funzionamento della connessione di rete attuale.

Non è stato possibile risolvere il DNS

Causa: il client non è in grado di risolvere il nome host del gateway.

Come procedere: verificare che sia presente un server DNS assegnato all'interfaccia di rete. Eseguire `nslookup` dal prompt dei comandi (Windows) o dal Terminale (Mac) per un host pubblico, ad esempio www.sophos.com, e verificare che si risolva a un indirizzo IP. Se non dovesse risolversi, contattare il proprio ISP.

Porte UDP 500/4500 bloccate

Causa: il firewall o il router blocca le porte UDP 500 e 4500.

Come procedere: verificare la configurazione locale del firewall o del router e autorizzare il traffico su queste porte. Se non si dovesse avere accesso al firewall o al router, ad esempio nel caso in cui ci si trovi in un hotel, connettersi con l'hotspot mobile e ritentare.

Nessuna risposta dal gateway: <FQDN o IP del gateway specificato nella connessione>

Causa: il gateway non risponde ai messaggi di negoziazione IKE. I motivi potrebbero essere:

- Il gateway remoto (firewall o router) è stato arrestato.
- L'indirizzo WAN del gateway remoto non è connesso direttamente a internet.

Come procedere: contattare il proprio amministratore del firewall e segnalare il problema per ulteriori attività di risoluzione.

Ricevuta notifica NO_PROPOSAL_CHOSEN dal gateway

Causa: il gateway remoto ha risposto alle negoziazioni IKE provenienti da Sophos Connect restituendo questa notifica di errore. I motivi potrebbero essere:

- Il criterio di Sophos Connect non è definito o attivato nel firewall.
- L'amministratore del firewall ha modificato le proposte IKE di Fase 1 utilizzate per il criterio di Sophos Connect nel firewall e la nuova configurazione non è stata esportata e caricata sul client.

Come procedere: contattare il proprio amministratore del firewall e segnalare il problema per ulteriori attività di risoluzione.

Il server aveva previsto l'ID remoto <valore ID previsto>, ma ha ricevuto <valore ID effettivo>

Causa: il tipo di ID locale o il valore configurato nel criterio di Sophos Connect nel firewall è diverso dal valore utilizzato per questa connessione. Questo potrebbe essere perché l'amministratore del firewall ha modificato l'ID locale nel firewall e il nuovo file di configurazione non è stato importato in Sophos Connect.

Come procedere: contattare il proprio amministratore del firewall e segnalare il problema per ulteriori attività di risoluzione.

Possibile mancata corrispondenza della chiave precondivisa <nome connessione>

Causa: la chiave precondivisa nel firewall non corrisponde alla chiave utilizzata per questa connessione. Questo potrebbe essere perché l'amministratore del firewall l'ha modificata nel firewall e il nuovo file di configurazione non è stato caricato in Sophos Connect.

Come procedere: contattare il proprio amministratore del firewall e segnalare il problema per ulteriori attività di risoluzione.

Autenticazione utente di <nome utente immesso> non riuscita

Causa: il nome utente o la password non hanno trovato corrispondenza.

Come procedere: ritentare, per verificare se ciò sia dovuto a un errore dell'utente durante l'immissione. Se dopo tentativi ripetuti viene visualizzato lo stesso errore, è possibile che la password sia stata modificata o disattivata nel firewall. In tale eventualità, contattare il proprio amministratore del firewall e segnalare il problema per ulteriori attività di risoluzione.

L'errore nell'aggiunta della route [rete/maschera] ha impedito il completamento della Fase 2

Nota
La procedura di risoluzione dei problemi indicata di seguito è valida solo per Windows.

Causa: una volta stabilita la SA (Security Association) di Fase 2, non è stato possibile eseguire `route add` sulla rete remota. Questo potrebbe essere perché il servizio strongSwan ha subito arresto anomalo mentre il tunnel era attivo.

Come procedere: disattivare e abilitare l'adattatore TAP. Aprire il prompt dei comandi con privilegi di amministratore e digitare i seguenti comandi:

```
net stop scvpn
net start scvpn
```

Non è stato possibile aggiungere i dati di connessione. Esiste già una connessione denominata <nome connessione>

Causa: è già stata importata una connessione con lo stesso nome.

Come procedere: eliminare la connessione esistente da Sophos Connect. Assicurarsi di voler veramente eliminare la connessione esistente prima di eliminarla. In caso contrario, contattare l'amministratore per ulteriori attività di risoluzione.

Il servizio non è disponibile

Nota
La procedura di risoluzione dei problemi indicata di seguito è valida solo per Windows.

Causa: il servizio Sophos Connect (scvpn) non è in esecuzione.

Come procedere: aprire il prompt dei comandi con privilegi di amministratore e digitare il seguente comando:

```
net start scvpn
```

Non è stato possibile caricare informazioni relative alla connessione su strongSwan

Nota
La procedura di risoluzione dei problemi indicata di seguito è valida solo per Windows.

Causa: il servizio strongSwan non è in esecuzione (nome servizio: charon-svc.exe).

Come procedere: aprire il prompt dei comandi con privilegi di amministratore e digitare il seguente comando:

```
net start strongswan
```

SA disattivata o eliminata dal gateway

Causa: il gateway ha inviato una richiesta di eliminazione dell'IKE e il tunnel è stato eliminato. I motivi potrebbero essere:

- L'amministratore del firewall ha modificato il criterio nel firewall. Questa operazione invia una richiesta di eliminazione dell'IKE a tutte le SA (Security Association) nel firewall.
- L'amministratore del firewall ha eliminato manualmente tutte le connessioni IPsec per questo utente nel firewall.

Come procedere: ritentare la connessione. Se questa situazione dovesse persistere, contattare l'amministratore per ulteriori attività di risoluzione.

Non è stato possibile risolvere il DNS per il gateway: <nome gateway:porta>

Causa: questo errore è dovuto a un nome host non valido.

Come procedere:

- se la connessione è stata aggiunta utilizzando un file di provisioning, verificare il nome host fornito.
- Se la connessione è stata aggiunta importando un file `ovpn`, controllare le impostazioni della VPN SSL in XG Firewall.

Impossibile verificare il certificato del server: <nome del gateway>. Continuare?

Causa: Sophos Connect Client importa la configurazione della VPN SSL connettendosi al portale utenti di XG Firewall utilizzando le proprietà nel file di provisioning. Il portale utenti utilizza un certificato autofirmato che non può essere verificato da Sophos Connect Client.

Come procedere: accettare l'avviso di sicurezza per la connessione e scaricare il file di configurazione `ovpn` dal portale utenti. Per evitare che il prompt venga visualizzato in futuro, utilizzare una delle seguenti opzioni:

- Emettere un nuovo certificato per XG Firewall, firmato da una CA pubblica. In XG Firewall, importare il certificato e selezionarlo nelle **Impostazioni di amministrazione** per l'accesso alla console Web Admin.
- Inviare tramite push il certificato CA predefinito da XG Firewall all'archivio dati attendibile dei computer remoti.

Non è stato possibile connettersi al server non attendibile: <gateway>

Causa: il prompt dell'avviso del certificato è stato annullato e la connessione è stata interrotta.

Come procedere: accettare l'avviso di sicurezza per la connessione e scaricare il criterio VPN SSL da XG Firewall. Per evitare che il prompt venga visualizzato in futuro quando viene scaricato il criterio VPN SSL, utilizzare una delle seguenti opzioni:

- Emettere un nuovo certificato per XG Firewall, firmato da una CA pubblica. In XG Firewall, importare il certificato e selezionarlo nelle **Impostazioni di amministrazione** per l'accesso alla console Web Admin.
- Inviare tramite push il certificato CA predefinito da XG Firewall all'archivio dati attendibile dei computer remoti.

Il file di importazione contiene una connessione duplicata: <nome connessione>

Causa: la connessione importata da un file di provisioning ha un nome visualizzato duplicato.

Come procedere: Controllare l'attributo `display_name` nel file di provisioning e rinominare eventuali nomi duplicati.

Impossibile stabilire la connessione al gateway dei criteri: <nome del gateway>

Causa: Il file di provisioning non è configurato correttamente. Possibili cause:

1. Nome host o indirizzo IP del gateway non valido.
2. Porta non valida o porta in uscita bloccata.
3. Il gateway dei criteri non è raggiungibile perché è disattivato.

Come procedere:

controllare il file di provisioning per verificare quanto segue:

1. Assicurarsi che il valore assegnato all'attributo `gateway` sia corretto.
2. Assicurarsi che il valore assegnato all'attributo `user_portal_port` corrisponda all'impostazione della porta HTTPS del portale utenti in XG Firewall.
3. Se il file di provisioning è configurato correttamente, contattare l'amministratore per ulteriori attività di risoluzione.

Nessun criterio VPN SSL definito per questo utente: <nome utente>

Causa: il criterio VPN SSL (accesso remoto) in XG Firewall non contiene alcun membro del criterio.

Come procedere: contattare l'amministratore.

Errore di compressione non corrispondente. Verrà effettuato un nuovo tentativo di connessione.

Causa: un criterio VPN SSL viene scaricato per la prima volta da XG Firewall e il tunnel VPN SSL viene stabilito con esso.

Come procedere: l'errore viene risolto in base alla configurazione della connessione:

- Con un file di provisioning: Sophos Connect effettua automaticamente un nuovo tentativo di connessione.
- Con un file `ovpn`: occorre riconnettersi manualmente.

Errore di criterio non corrispondente. Il criterio verrà scaricato e sarà effettuato un nuovo tentativo di connessione.

Causa: Sophos Connect Client ha effettuato il tentativo di stabilire una connessione VPN SSL con un criterio esistente salvato per questa connessione.

L'amministratore ha modificato le impostazioni VPN SSL in XG Firewall dopo che una connessione VPN SSL è stata stabilita e salvata da Sophos Connect.

Come procedere: la connessione è stata creata utilizzando un file di provisioning. Sophos Connect scaricherà automaticamente il nuovo criterio e ristabilirà il tunnel VPN SSL.

Nota
Se l'amministratore modifica il criterio VPN SSL in XG Firewall mentre il tunnel si trova in stato connesso e si tratta di una VPN SSL su TCP, Sophos Connect Client rileverà e scaricherà immediatamente il nuovo criterio. Se si tratta di un tunnel VPN SSL su UDP, è necessario attendere che il timer di inattività elimini il tunnel. Sophos Connect scaricherà quindi il nuovo criterio per ristabilire il tunnel.

Errore di criterio non corrispondente. Importa un nuovo criterio per questa connessione.

Causa: Sophos Connect Client ha effettuato il tentativo di stabilire una connessione VPN SSL con un criterio esistente salvato per questa connessione.

L'amministratore ha modificato le impostazioni VPN SSL in XG Firewall dopo che una connessione VPN SSL è stata stabilita e salvata da Sophos Connect.

Come procedere: la connessione è stata creata importando un file `ovpn`. L'utente deve scaricare e importare un nuovo file `ovpn` dal portale utenti di XG Firewall per ristabilire il tunnel VPN SSL.

Nota
Se l'amministratore modifica il criterio VPN SSL in XG Firewall mentre il tunnel si trova in stato connesso e si tratta di una VPN SSL su tunnel TCP, Sophos Connect Client rileverà e disconnetterà immediatamente il tunnel, restituendo un errore. Se si tratta di un tunnel VPN SSL su UDP, è necessario attendere che il timer di inattività elimini il tunnel. L'utente deve scaricare e importare un nuovo file `ovpn` dal portale utenti di XG Firewall per ristabilire correttamente il tunnel VPN SSL.

Si è verificato un timeout durante l'attesa della risposta del server.

Causa: il criterio VPN SSL non è configurato correttamente in XG Firewall. Le possibili cause del problema sono le seguenti:

1. È configurato Override hostname (override del nome host), ma non si risolve all'indirizzo IP pubblico corretto o valido.
2. È configurato il DDNS, ma non si risolve all'indirizzo IP pubblico corretto o valido.
3. Sia **Override hostname** che il DDNS non sono configurati e la porta WAN non dispone di un indirizzo IP pubblico.

Come procedere: se è stato utilizzato un file di provisioning per importare la connessione, aggiornare il menu delle impostazioni di connessione dei criteri (su Sophos Connect Client). Se è stato utilizzato un file `ovpn` per creare la connessione, esportare un nuovo file `ovpn` dal portale utenti e reimportarlo in Sophos Connect Client.

1.5 Risoluzione generale dei problemi

Questo argomento descrive i problemi che non sono elencati nella pagina degli eventi.

Per ulteriore assistenza contattare il Supporto tecnico Sophos.

Il traffico non viene incanalato nel tunnel VPN

Causa: se si esegue una versione del firmware precedente alla v17.5, è possibile che il client abbia ricevuto un nuovo IP virtuale dopo la reimpostazione della chiave di fase 1.

Come procedere: occorrerà effettuare prima la disconnessione e successivamente la riconnessione. La soluzione permanente è l'upgrade alla v17.5.

La dashboard di Sophos Connect non si apre

Causa: se la dashboard di Sophos Connect non dovesse aprirsi, o se non dovesse rispondere quando si clicca sull'icona nell'area di notifica, significa che l'interfaccia grafica è bloccata in un ciclo infinito e non è in grado di rispondere a input esterni.

Come procedere (Windows): aprire Gestione attività e selezionare la scheda Dettagli. Individuare scgui.exe e cliccarci sopra con il tasto destro del mouse per terminare l'attività. Riavviare l'applicazione dal collegamento sul desktop.

Come procedere (Mac): aprire Monitoraggio attività e individuare il processo Sophos Connect. Aprire il processo e selezionare Uscita forzata. Riavviare l'applicazione dal LaunchPad.

La navigazione web smette di funzionare quando il tunnel viene disconnesso

Nota
Questo problema è più comune sui Mac.

Causa: quando viene disconnessa una connessione di tipo Tunnel all, i server DNS non vengono ripristinati dalle schede di rete fisiche. Ciò significa che i server DNS interni utilizzati durante la connessione tramite VPN sono ancora in uso. Poiché il tunnel non esiste più, la risoluzione dei nomi non funzionerà.

Come procedere: disconnettersi dalla rete locale e riconnettersi.

L'interfaccia grafica di Sophos Connect visualizza il messaggio "Servizio non disponibile"

Nota
Questo problema è più comune sui Mac.

Causa: quando viene avviata la disconnessione di un tunnel, il daemon IPsec di strongSwan rimane bloccato in un ciclo infinito. Di conseguenza, l'interfaccia grafica non otterrà risposta per la disconnessione, si verificherà un timeout e verrà visualizzato l'errore "Server non disponibile".

Come procedere (Mac):

1. aprire il Monitoraggio attività e uscire dal processo dell'interfaccia grafica di Sophos Connect.
2. Aprire Terminal ed eseguire nuovamente i seguenti comandi:

```
sudo /bin/launchctl unload -w /Library/LaunchDaemons/
com.sophos.connect.scvpn.plist
```

```
sudo /bin/launchctl load -w /Library/LaunchDaemons/
com.sophos.connect.scvpn.plist
```

3. Aprire Sophos Connect e verificare che l'errore "Servizio non disponibile" sia ora risolto.

Come procedere (Windows):

1. Aprire `cmd` con privilegi di amministratore ed eseguire il seguente comando:

   ```
   net stop scvpn
   ```

   ```
   net start scvpn
   ```

2. Aprire Sophos Connect e verificare che l'errore "Servizio non disponibile" sia ora risolto.

Sophos Connect non è in grado di stabilire un tunnel

Causa: è probabile che l'installazione del client di Sophos Connect sia avvenuta prima di quella del client della VPN SSL Sophos.

Come procedere: disinstallare entrambi i client e successivamente reinstallare prima il client VPN SSL Sophos e poi il client di Sophos Connect.

Nota
Devono essere installati in questo ordine.

Ricevuto ripristino della connessione dal gateway: <nome del gateway>

Questo messaggio viene registrato nel file `scvpn.log` (nella cartella di installazione).

Causa: modifica delle impostazioni VPN SSL in XG Firewall, disconnessione manuale di un utente, oppure riavvio di XG Firewall. Se la connessione utilizza VPN SSL su TCP, XG Firewall invierà una richiesta di ripristino della connessione. Se la connessione utilizza VPN SSL su UDP, a seconda del periodo di timeout di inattività, la connessione potrebbe riconnettersi automaticamente.

Come procedere: importare un nuovo file di configurazione in Sophos Connect Client e riconnettersi. Se l'amministratore non ha inviato il file, visitare il portale utenti e scaricarlo. Altrimenti è anche possibile visitare il portale utenti per scaricare il file `ovpn`.

La connessione VPN SSL presenta voci disattivate nei menu Connessione automatica e Aggiorna criterio.

Causa: se la connessione VPN SSL viene creata importando un file `ovpn`, queste opzioni non sono disponibili.

Come procedere: per attivare queste opzioni occorre creare una connessione utilizzando un file di provisioning. Aggiungere queste opzioni al file di provisioning. **Aggiorna criterio** sarà disponibile dopo la prima connessione. Per attivare la **Connessione automatica**, è necessario definire un `auto_connect_host` a cui è possibile accedere solo nella rete interna.

Esempio di file di provisioning con requisiti minimi per l'attivazione della connessione automatica:

```
[
 {
  “display_name": "<Enter connection name>",
  "gateway": "<Enter your gateway hostname or IP>",
  "auto_connect_host":" <Enter hostname or IP of internal network resource>"
```

```
 }
]
```

Errore VPN SSL

Causa: errore generato dal servizio OpenVPN.

Come procedere: stabilire nuovamente la connessione. Se non dovesse funzionare, riavviare il dispositivo e ritentare.

Porta di gestione non disponibile

Causa: Sophos Connect non riesce a richiedere la porta TCP 25340, che è obbligatoria per comunicare con OpenVPN.

Come procedere: controllare se nel dispositivo è in esecuzione un'altra applicazione che utilizza questa porta. Se possibile, uscire dall'applicazione. Se questo problema non viene risolto, Sophos Connect 2.0 non potrà eseguirsi sul dispositivo. Se nessun'altra applicazione utilizza questa porta, si potrebbe trattare di una condizione temporanea. Una volta ristabilita la connessione, il problema dovrebbe risolversi.

Creazione del file temporaneo non riuscita

Causa: Sophos Connect utilizza un file temporaneo per passare gli attributi di connessione al servizio OpenVPN. Sophos Connect non ha potuto creare il file su questo dispositivo.

Come procedere: riavviare il dispositivo.

Il servizio OpenVPN non è disponibile

Causa: il servizio OpenVPN potrebbe non essere stato avviato.

Come procedere: se il tipo di avvio del servizio OpenVPN è impostato su **disabled**, impostarlo su **manual** e riavviare anche il servizio Sophos Connect.

Scrittura sulla pipe non riuscita

Causa: errore generato dal Sophos Connect Client.

Come procedere: stabilire nuovamente la connessione. Se non dovesse funzionare, riavviare il dispositivo e ritentare.

2 Informazioni su Sophos Connect Admin

Sophos Connect Admin consente di importare file di configurazione (`.tgb`) e di configurare varie opzioni per l'impostazione della VPN.

Nota
Per informazioni su come configurare ed esportare un file .tgb in XG, vedere la sezione Sophos Connect Client della Guida in linea di XG: Sophos Connect Client.

I processi di installazione e disinstallazione di Sophos Connect Admin sono identici a quelli di Sophos Connect. Per ulteriori informazioni, vedere la sezione Installazione nella Guida in linea di Sophos Connect.

2.1 Modifica dei file di configurazione

È possibile modificare i file di configurazione (`.tgb`) in Sophos Connect Admin, che offre opzioni di configurazione VPN più dettagliate.

Aprire il file `.tgb` esportato da XG in Sophos Admin. È possibile:

- Attivare **Tunnel All** per indirizzare tutto il traffico attraverso la connessione VPN.
- Attivare **Send Security Heartbeat** per consentire a Sophos Endpoint di inviare un Heartbeat a XG Firewall. Questo sarà possibile solo se nel computer dell'utente è installato Sophos Endpoint.
- Abilitare **Allow Password Saving** per consentire agli utenti di salvare nome utente e password nel proprio computer. Le credenziali dell'utente vengono archiviate in modo sicuro utilizzando i servizi keychain.
- Attivare **Prompt for 2FA** se è stata configurata l'autenticazione a due fattori per gli utenti VPN in XG.
- Attivare **Auto-Connect Tunnel** per attivare automaticamente la connessione dopo che l'utente accede a Sophos Connect sul proprio computer. Sophos Connect non avvia automaticamente la connessione se l'utente è già connesso alla rete aziendale.

  La connessione automatica richiede un parametro di configurazione aggiuntivo: **DNS Suffix/ Monitoring Host**, che può essere utilizzato per determinare se il sistema locale dell'utente si trova all'interno o all'esterno della rete aziendale. Utilizzare uno dei seguenti valori:

  — Un indirizzo IP.

  — Un nome di dominio completo (fully qualified domain name, FQDN). Il nome host deve risolversi solo quando si utilizza il server DNS interno.

  — Un suffisso DNS.

  Nota
  Se si configura un indirizzo IP o un FQDN, è necessario che ICMP sia autorizzato sull'host.

- Aggiungere, modificare ed eliminare le **Networks** a cui l'utente può connettersi. L'aggiunta di reti specifiche all'elenco abilita lo split tunneling, in quanto l'utente accede alle risorse su tali reti tramite la connessione VPN, ma effettua l'accesso alle risorse Internet direttamente tramite il gateway remoto.

Nota
Se si eliminano tutte le reti, verrà attivata la modalità **Tunnel All**, il che significa che tutto il traffico verrà indirizzato attraverso la connessione VPN.

- Modificare **Connection Name** e **Target Host**.

  Se si seleziona **Clear** per cancellare la configurazione, sarà necessario importare nuovamente il file `.tbg`.

  Se si seleziona **Save** per salvare la configurazione, verrà salvata come file `.scx`.

  Nota
  È possibile importare file `.scx` e modificarli nuovamente.

Una volta salvato il file di configurazione, è possibile inviarlo all'utente, che lo importerà in Sophos Connect. Per maggiori informazioni, vedere Sophos Connect.

3 Note legali