SOPHOS

Cybersecurity made simple.

Sophos Connect
ヘルプ

目次

(2020/05/15)

1 Sophos Connect について

Sophos Connect は、Windows および Mac にインストール可能な VPN クライアントです。Sophos Connect を使用して、企業ネットワークなど、XG Firewall の内側にあるネットワークに外部から接続することができます。ファイアウォール管理者は、XG Firewall 上で接続の詳細を設定し、インストールパッケージと接続設定ファイルをユーザーに配布します。

このガイドでは、Sophos Connect の使用方法について説明しています。

- Sophos Connect のインストールやアンインストールを行う方法については、Sophos Connect のインストール (p. 1)を参照してください。
- 接続ファイルのインポートや接続の管理を行う手順については、接続 (p. 2)を参照してください。
- イベントの概要や、イベントエラーのトラブルシューティングを行う方法については、イベント (p. 11)を参照してください。
- 「イベント」セクションに表示されない問題のトラブルシューティングについては、一般的なトラブルシューティング (p. 18)を参照してください。

1.1 Sophos Connect のインストール

Windows への Sophos Connect のインストール

- インストーラを起動します。
- 使用許諾契約に同意して、「**インストール**」をクリックします。
- インストールが終了したら、「**完了**」をクリックします。終了後に Sophos Connect を起動するオプションを選択できます。

Mac への Sophos Connect のインストール

- インストーラを起動します。
- インストール先を選択します。選択したインストール先 (システムドライブなど) に十分な空き容量があることを確認します。
- 「**インストール**」をクリックします。
- インストールが終了したら、「**完了**」をクリックします。

1.2 Sophos Connect のアンインストール

Windows からの Sophos Connect のアンインストール

- 「**コントロールパネル**」を開き、「**プログラム**」の下の「**プログラムのアンインストール**」をクリックします。
- Sophos Connect を右クリックして、「**アンインストール**」を選択します。

Mac からの Sophos Connect のアンインストール

- 「ターミナル」を開きます。
- 権限を root に変更し、Sophos Connect をインストールしたフォルダからアンインストール用スクリプトを実行します。

  sudo /Library/Sophos Connect/uninstall.sh

アンインストールに成功すると、次のメッセージが表示されます。

Sophos Connect has been uninstalled

1.3 接続

接続は、インポートおよび確立したり、表示および編集できます。

Sophos Connect は、SSL VPN および IPsec VPN をサポートしています。

1.3.1 接続のインポート

Sophos Connect クライアントは、SSL VPN または IPsec VPN 接続を使用して XG Firewall に接続できます。Sophos Connect クライアントに接続をインポートすることもできます。

はじめに

バージョン 2.0 の Sophos Connect クライアントでは、SSL VPN および IPsec VPN 接続のどちらでもインポートできます。以前のバージョンの Sophos Connect クライアントを使用している場合は、IPsec 接続のみをインポートできます。

このページでは、次の操作方法について説明しています。

- 管理者配布のファイルを使用した、IPsec 接続のインポート。
- 管理者配布のファイルを使用した、SSL 接続のインポート。
- ユーザーポータルからダウンロードしたファイルを使用した、SSL 接続のインポート。

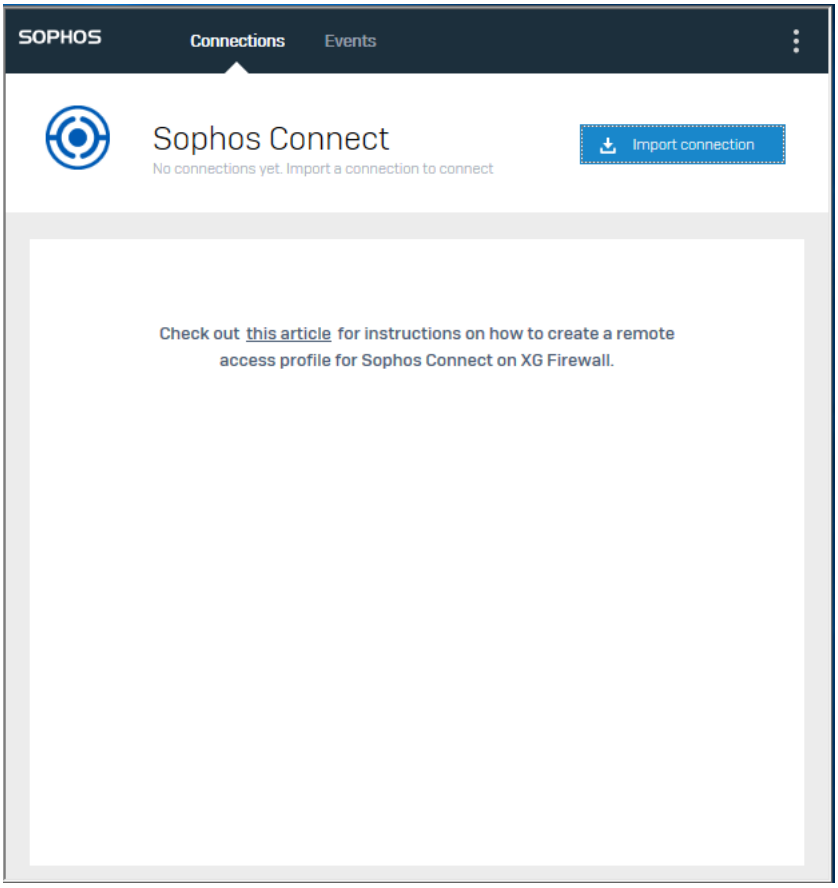
IPsec 接続のインポート

管理者から接続ファイルが配布されています。ファイルには「tgb」という拡張子が付いています。例: Company_connection.tgb

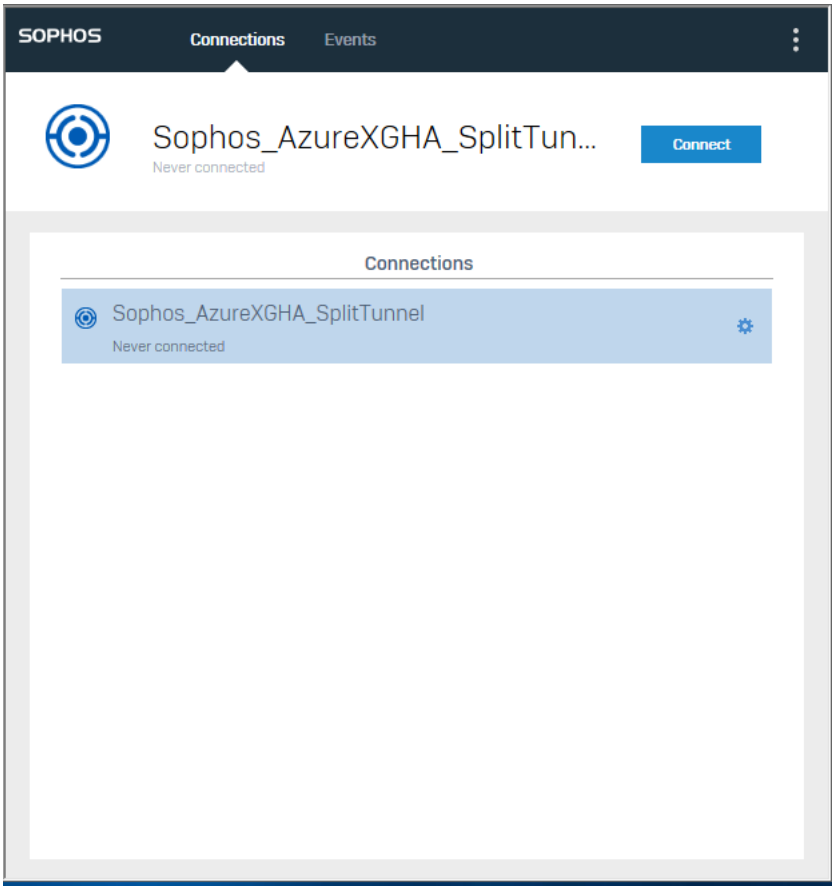
接続をインポートする方法は次のとおりです。

1. 「**接続**」ページの「**接続のインポート**」をクリックします。

   既存の接続がある場合は、メニューボタンをクリックして、ドロップダウンメニューから「**接続のインポート**」を選択します。



2. .tgb ファイルを参照してダブルクリックします。
「**接続**」の下に、インポートした接続が表示されます。



これで、接続を確立できるようになります。

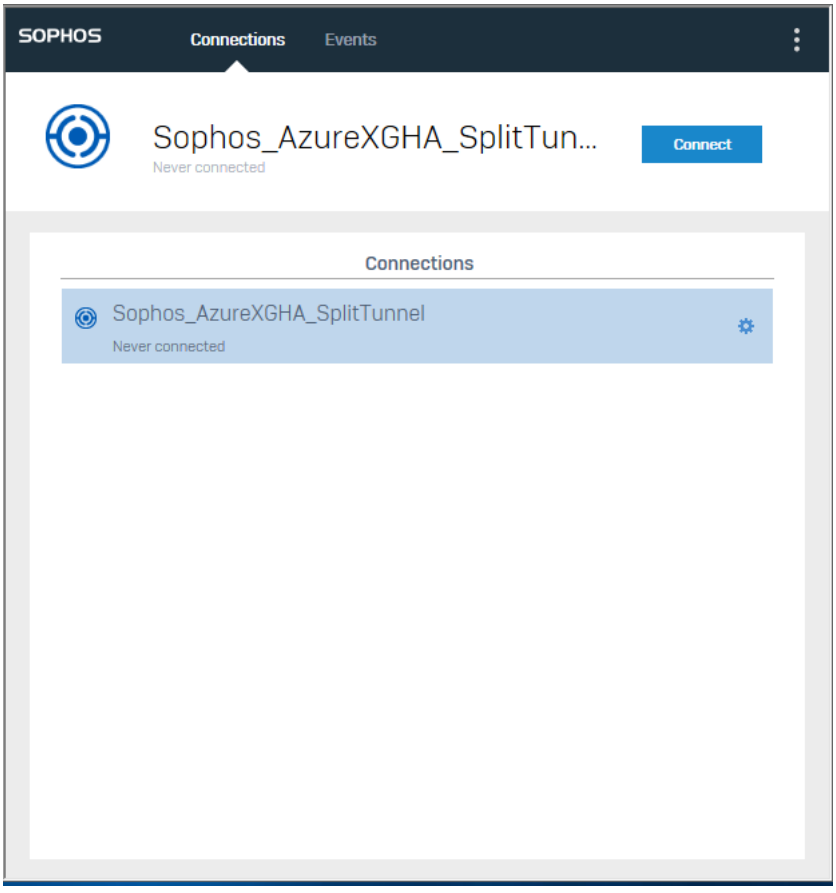
注
複数の接続をインポートできます。

SSL 接続のインポート

管理者から接続ファイルが配布されています。ファイルには、「pro」という拡張子が付いています。例: Company_connection.pro

接続をインポートする方法は次のとおりです。

.pro ファイルを参照してダブルクリックします。
接続は自動的にインポートされ、Sophos Connect が開きます。「**接続**」の下に、インポートした接続が表示されます。



これで、接続を確立できるようになります。

注
複数の接続をインポートできます。

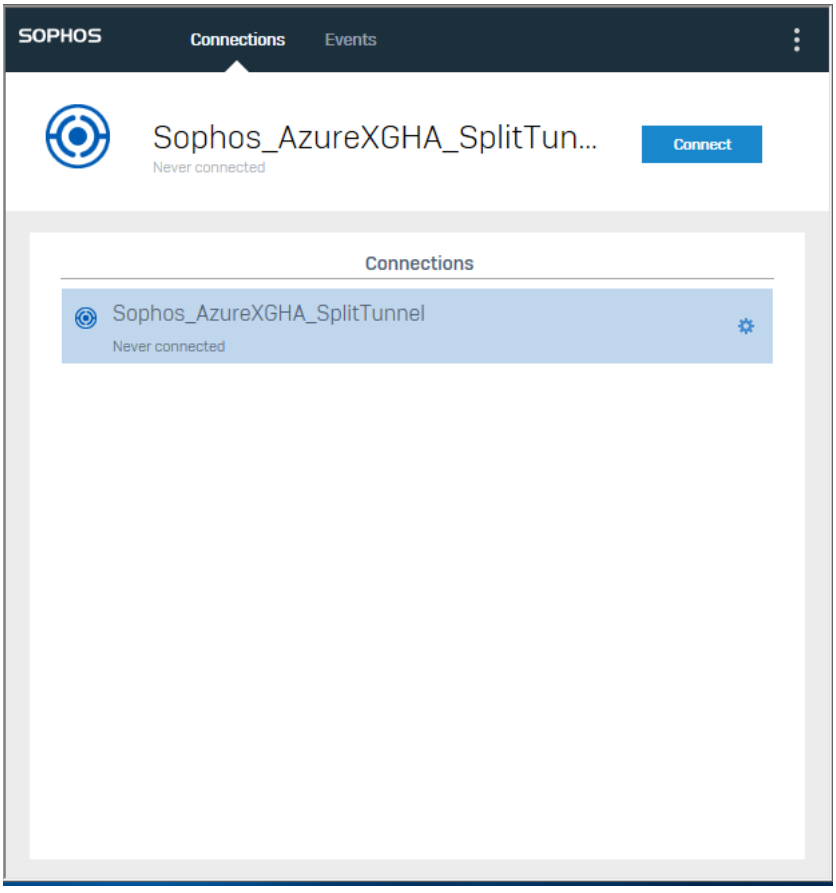
ユーザーポータルからの SSL 接続のインポート

接続をインポートする方法は次のとおりです。

1. ユーザーポータルにサインインします。
2. 「**SSL VPN**」に移動し、「**その他の OS 向け設定のダウンロード**」をクリックします。
3. Sophos Connect クライアントを開きます。
4. 「**接続**」ページで「**接続のインポート**」をクリックします。

   既存の接続がある場合は、メニューボタンをクリックして、ドロップダウンメニューから「**接続のインポート**」を選択します。
5. .ovpn ファイルを参照して開きます。

「**接続**」の下に、インポートした接続が表示されます。



これで、接続を確立できるようになります。

注
複数の接続をインポートできます。

1.3.2 接続

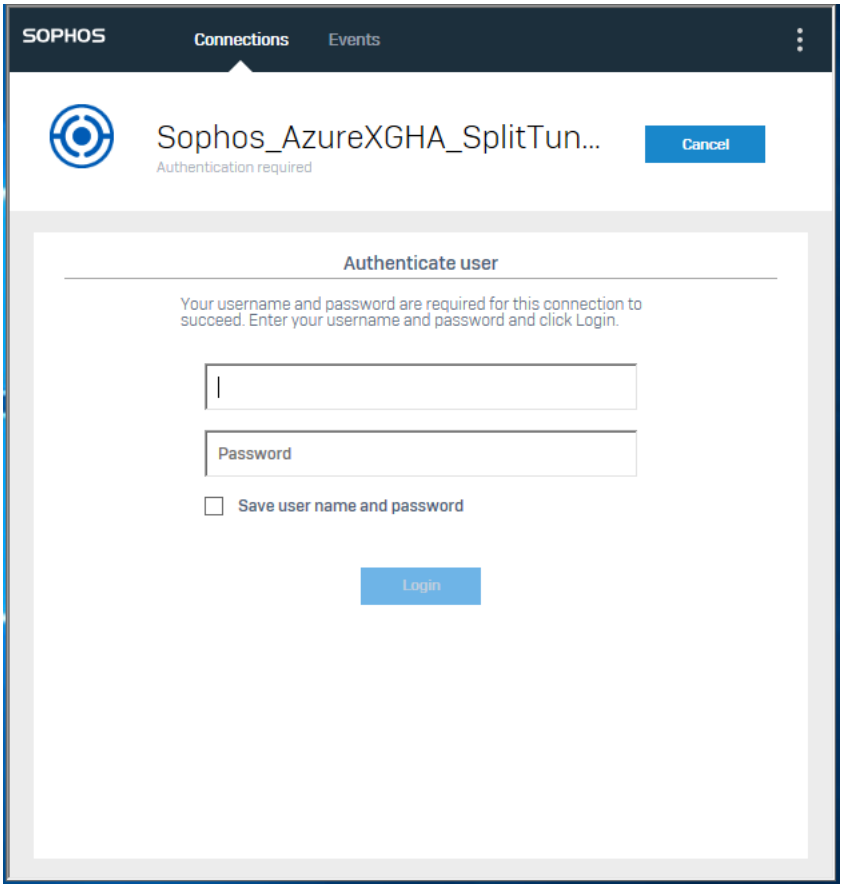
少なくとも 1つのインポートされた接続が利用できる状態であり、かつ必要な認証情報が手元にある必要があります。

接続を確立する方法は次のとおりです。

1. 「**接続**」ページで対象の接続を選択します。
2. 接続をダブルクリックします。

   「**接続**」をクリックすることもできます。

   サインイン画面が表示されます。

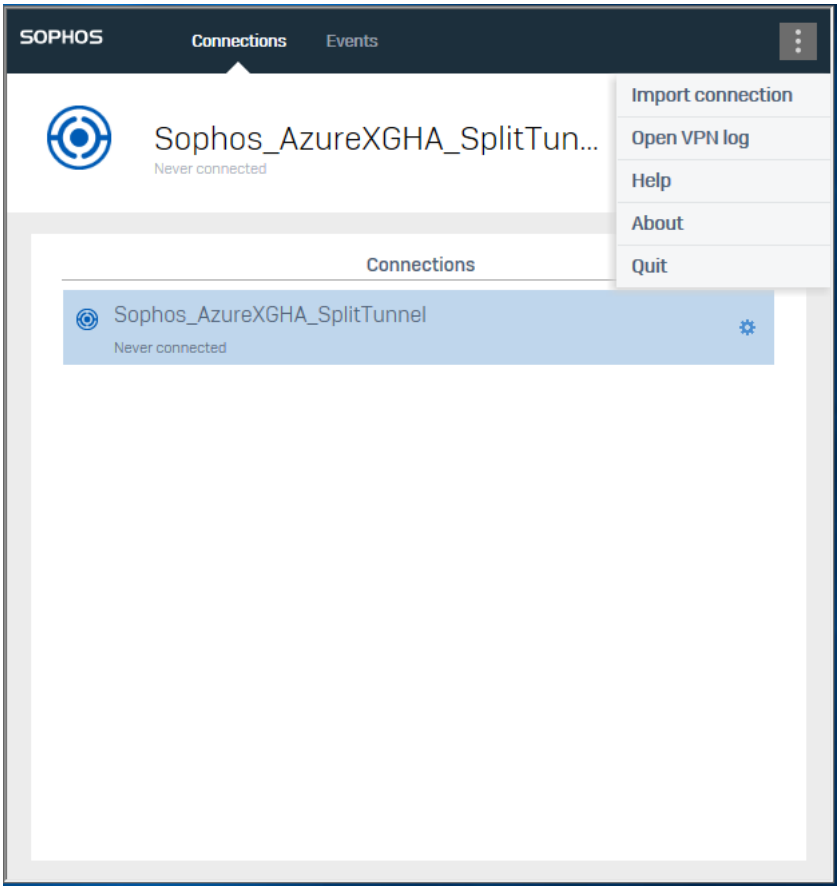


3. ユーザー名とパスワードを入力し、「**ログイン**」をクリックします。
   管理者によって、二要素認証が設定されている場合があります。
   - 管理者によって OTP が設定されている場合は、ユーザー名とパスワードの入力に加え、6桁の OTP パスコードを入力する必要があります。
   - 管理者によて Duo 認証が設定されている場合は、接続プロセス中に 1つまたは 2つの Duo プロンプトが表示されることがあります。

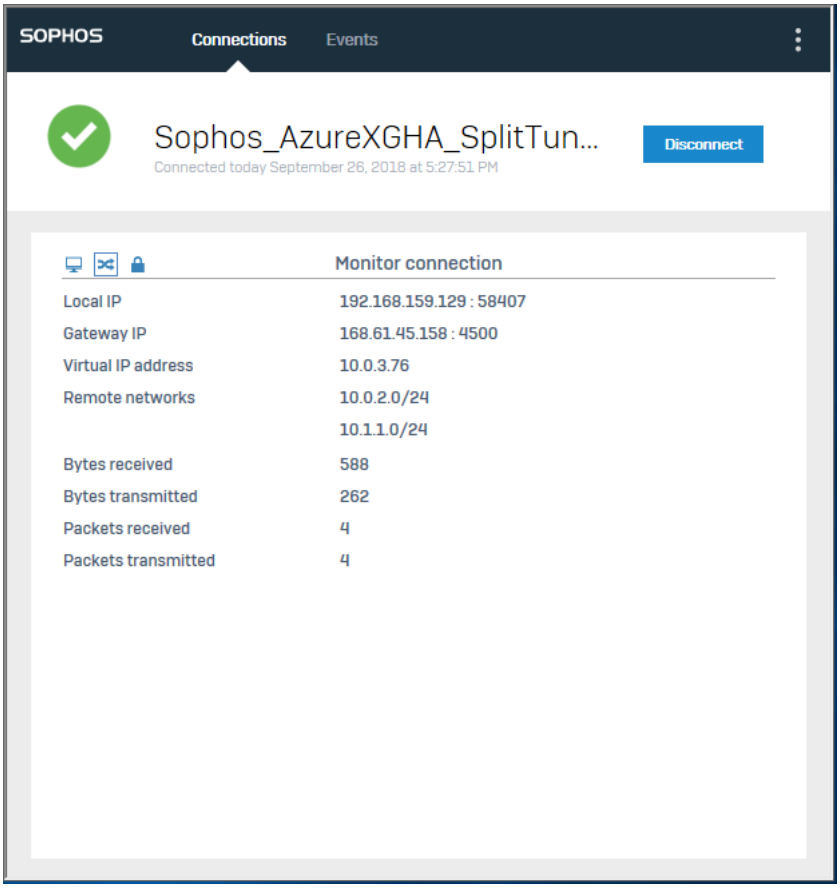
   注
   プロビジョニングファイルを使用して接続をインポートした場合は、サーバー証明書を検証できない、という警告が表示されますが、「**OK**」をクリックして続行できます。このメッセージを非表示にするには、管理者に問い合わせてください。

   Sophos Connect で、接続の確立とユーザーの認証が実行されます。

   注
   接続エラーが発生した場合は、「**イベント**」ページを確認して、社内の IT 部門に問い合わせてください。VPN ログは、メニューアイコンをクリックして、「VPN ログを開く」を選択して確認できます。



リモートサーバーへの接続が確立されます。



接続に成功した場合は、次のアイコンがタスクバーに表示されます。

接続に失敗した場合は、次のアイコンがタスクバーに表示されます。

注
接続名を変更しても、ファイアウォール管理者から配布されたときの元の接続名が、接続の詳細に表示されます。名前の変更方法については、接続オプション (p. 10)を参照してください。

1.3.3 接続オプション

Sophos Connect で、各接続の右端にある設定アイコンをクリックすると、接続に関するさまざまな変更を行うことができます。

1. **自動接続**: Sophos Connect の起動時に接続を確立します。
2. **削除**: 接続を削除します。接続を再度有効にするには、もう一度インポートする必要があります。
3. **名前の変更**: 接続名を変更できます。
4. **認証情報のクリア**: 以前に保存した認証情報を消去します。
5. **ポリシーの更新**: (プロビジョニングファイルを使用して接続を作成した場合のみに使用可能)。XG Firewall から最新のポリシーをオンデマンドで取得できます。

ヒント
何度再試行しても接続に失敗する場合は、ポリシーを更新後、再度接続を試みてください。

1.4 イベント

Sophos Connect で実行されたアクションとその結果を確認できます。これには、ユーザーがアクションを実行した結果発生したエラーや、IKE ネゴシエーションエラーなどが含まれます。イベントエラーのトラブルシューティングを行う方法については、イベントのトラブルシューティング (p. 12)を参照してください。

- トラブルシューティングに詳細なログが必要な場合は、「**VPN ログを開く**」クリックします。
- イベントをリストから削除するには、「**イベントのクリア**」をクリックします。

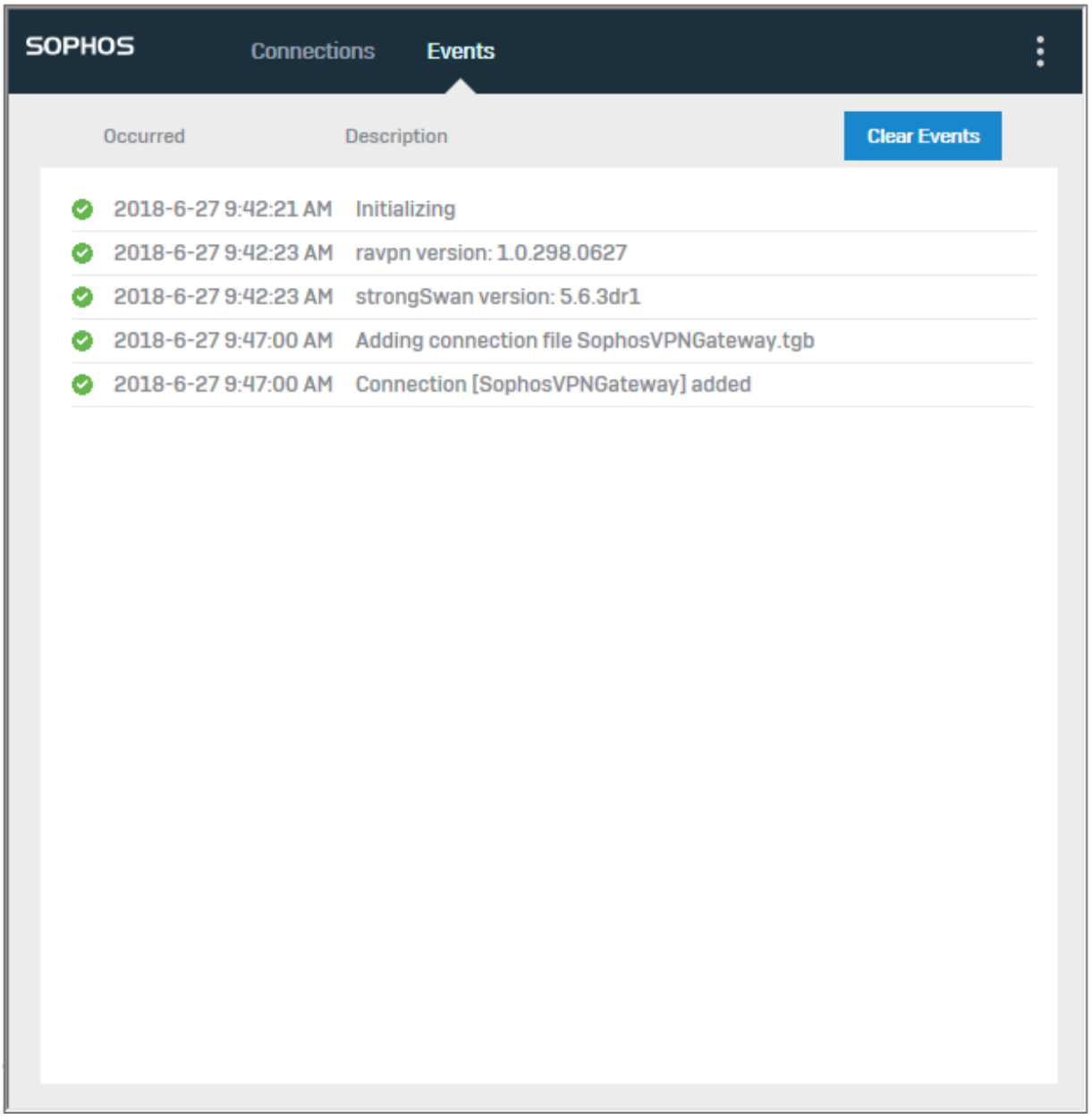


図 1：イベント

1.4.1 イベントのトラブルシューティング

接続に関する問題が発生した場合は、「**イベント**」をクリックし、接続を試みた際のタイムスタンプを確認して該当するエラーを見つけ出します。

このセクションには、エラーメッセージ、エラーの考えられる原因、および対処方法に関する情報が表示されます。以下に記載されていない問題が発生した場合は、一般的なトラブルシューティングを参照してください。

さらにご不明な点は、ソフォス サポートへお問い合わせください。

ネットワーク接続がありません

原因: ネットワークアダプタ (イーサネットまたは Wi-Fi) に IP アドレスがありません。

対策・説明: IP アドレスが有効であることと、ネットワークに正常に接続していることを確認します。

DNS 解決に失敗しました

原因: クライアントがゲートウェイのホスト名を名前解決できません。

対策・説明: DNS サーバーがネットワークインターフェースに割り当てられていることを確認します。パブリックホスト (例: www.sophos.co.jp) に対して、コマンドプロンプト (Windows) またはターミナル (Mac) で nslookup を実行し、IP アドレスが表示されることを確認します。名前解決されない場合は、ご利用の ISP にお問い合わせください。

UDP ポート 500/4500 がブロックされています

原因: ファイアウォールまたはルーターが UDP ポート 500 および 4500 をブロックしています。

対策・説明: ローカルのファイアウォールやルーターの構成を確認し、これらのポートでトラフィックを許可します。たとえば宿泊先などで、ファイアウォールやルーターにアクセスできない場合は、携帯電話のポットスポットを通じて接続し、もう一度接続し直してみてください。

ゲートウェイから応答がありません: <ゲートウェイの FQDN または接続で指定されている IP アドレス>

原因: ゲートウェイが IKE ネゴシエーションのメッセージに応答していません。次の原因が考えられます。

- リモートゲートウェイ (ファイアウォールまたはルーター) がシャットダウンされた。
- リモートゲートウェイの WAN の IP アドレスが直接インターネットに接続されていない。

対策・説明: 社内のファイアウォール管理者に問題を報告して対応を依頼してください。

ゲートウェイから通知 NO_PROPOSAL_CHOSEN を受信しました

原因: Sophos Connect からの IKE ネゴシエーションに対して、リモートゲートウェイが上記のエラーで応答した状態です。次の原因が考えられます。

- ファイアウォールで、Sophos Connect のポリシーが定義されていない、または有効な状態になっていない。
- ファイアウォール管理者が、ファイアウォールで、Sophos Connect のポリシーで使用される IKE フェーズ 1 のプロポーザルを変更し、変更後の設定内容をエクスポートしてクライアントにアップロードしていない。

対策・説明: 社内のファイアウォール管理者に問題を報告して対応を依頼してください。

サーバーはリモート ID <予期していた ID の値> を予期していたが、<実際の ID の値> を受信した

原因: 当該の接続で使用されている値が、ファイアウォールの Sophos Connect のポリシーで設定されているローカル ID の種類または値と異なります。ファイアウォール管理者が、ファイアウォールでローカル ID を変更し、変更後の設定ファイルを Sophos Connect にインポートしていないことが原因である可能性があります。

対策・説明: 社内のファイアウォール管理者に問題を報告して対応を依頼してください。

事前共有鍵の不一致の可能性がある <接続名>

原因: 当該の接続で使用されている事前共有鍵が、ファイアウォールの事前共有鍵と一致しません。ファイアウォール管理者が、ファイアウォールで事前共有鍵を変更し、変更後の設定ファイルを Sophos Connect にアップロードしていないことが原因である可能性があります。

対策・説明: 社内のファイアウォール管理者に問題を報告して対応を依頼してください。

<入力されたユーザー名> のユーザー認証に失敗した

原因: ユーザー名またはパスワードが一致しませんでした。

対策・説明: もう一度やり直して入力ミスでないかどうかを確認します。何回か試しても同じエラーが表示される場合は、パスワードが変更されているか、ファイアウォールで無効に設定されている可能性があります。その場合は、社内のファイアウォール管理者に問題を報告して対応を依頼してください。

ルート [ネットワーク/サブネットマスク] の追加に失敗したため、フェーズ 2 を完了できませんでした

注
次のトラブルシューティングの手順は、Windows のみを対象にしています。

原因: フェーズ 2 SA が確立された後、リモートネットワークに対する route add の実行に失敗しました。トンネルがアクティブな状態のときに、strongSwan サービスが異常終了したことが原因である可能性があります。

対策・説明: TAP アダプタを無効にした後、有効にします。管理者権限でコマンドプロンプトを開き、次のコマンドを実行します。

net stop scvpn

net start scvpn

接続データを追加できませんでした。名前が <接続名> の接続は既に存在します

原因: 同じ名前の接続が既にインポートされています。

対策・説明: Sophos Connect から既存の接続を削除します。削除する前に、既存の接続を削除してもよいかを確認してください。それ以外の場合は、社内の管理者に連絡して対応を依頼してください。

サービスを使用できません

注
次のトラブルシューティングの手順は、Windows のみを対象にしています。

原因: Sophos Connect サービス (scvpn) が実行されていない状態です。

対策・説明: 管理者権限でコマンドプロンプトを開き、次のコマンドを実行します。

net start scvpn

strongSwan への接続情報の読み込みに失敗した

注
次のトラブルシューティングの手順は、Windows のみを対象にしています。

原因: strongSwan サービスが実行されていない状態です (サービス名: charon-svc.exe)。

対策・説明: 管理者権限でコマンドプロンプトを開き、次のコマンドを実行します。

net start strongswan

ゲートウェイによって SA が無効化または削除された

原因: ゲートウェイが IKE の削除要求を送信後、トンネルが削除されました。次の原因が考えられます。

- ファイアウォール管理者がファイアウォールでポリシーを変更した。これにより、IKE の削除要求が、ファイアウォール上のすべてのアクティブな SA に送信されます。
- ファイアウォール管理者が、ファイアウォールで、当該のユーザーに対する、すべての IPsec 接続を手動で削除した。

対策・説明: もう一度接続し直してください。それでも問題が解消しない場合は、社内の管理者に連絡して対応を依頼してください。

ゲートウェイで DNS 解決に失敗しました: <ゲートウェイ名: ポート>

原因: このエラーは、無効なホスト名が原因です。

対策・説明:

- プロビジョニングファイルを使用して接続を追加した場合は、指定されたホスト名を確認します。
- ovpn ファイルをインポートして接続を追加した場合は、XG Firewall の SSL VPN 設定を確認します。

サーバー証明書を検証できません: <ゲートウェイ名>。続行しますか？

原因: Sophos Connect クライアントは、プロビジョニングファイル内のプロパティを使用して XG Firewall ユーザーポータルに接続することによって、SSL VPN 設定をインポートします。ユーザーポータルは自己署名証明書を使用しますが、これは Sophos Connect クライアントでは検証できません。

対策・説明: セキュリティ警告を受け入れて接続し、ユーザーポータルから ovpn 設定ファイルをダウンロードします。今後プロンプトが表示されないようにするには、次のいずれかのオプションを使用します。

- パブリック CA によって署名された XG Firewall の新しい証明書を発行します。XG Firewall で証明書をインポートし、Web 管理コンソールにサインインするために、「**管理の設定**」で証明書を選択します。
- デフォルトの CA 証明書を、XG Firewall からリモートコンピュータの信頼できるストアにプッシュします。

信頼できないサーバーに接続できませんでした: <ゲートウェイ>

原因: 証明書の警告プロンプトをキャンセルしたため、接続が終了しました。

対策・説明: セキュリティ警告を受け入れて接続し、XG Firewall から SSL VPN ポリシーをダウンロードします。SSL VPN ポリシーのダウンロード中ににプロンプトが表示されないようにするには、次のいずれかのオプションを使用します。

- パブリック CA によって署名された XG Firewall の新しい証明書を発行します。XG Firewall で証明書をインポートし、Web 管理コンソールにサインインするために、「**管理の設定**」で証明書を選択します。
- デフォルトの CA 証明書を、XG Firewall からリモートコンピュータの信頼できるストアにプッシュします。

インポートファイルに重複した接続が含まれています: <接続名>

原因: プロビジョニングファイルからインポートした接続に、重複した表示名があります。

対策・説明: プロビジョニングファイルの display_name 属性をチェックし、重複する名前を変更します。

ポリシーゲートウェイに接続できません: <ゲートウェイ名>

原因: プロビジョニングファイルが正しく設定されていません。次のような状況が原因になっている可能性があります。

1. ゲートウェイのホスト名または IP アドレスが無効。
2. ポートが無効、または送信ポートがブロックされている。
3. ポリシーゲートウェイがオフになっているため到達不能。

対策・説明:

プロビジョニングファイルで次の事柄を確認します。

1. gateway 属性に正しい値が割り当てられていることを確認します。

2. user_portal_port 属性に割り当てられている値が、XG Firewall のユーザーポータル HTTPS ポート設定と一致することを確認します。
3. プロビジョニングファイルが正しく設定されている場合は、社内の管理者に連絡して対応を依頼してください。

このユーザーに対して SSL VPN ポリシーが定義されていません: <ユーザー名>

原因: XG Firewall の SSL VPN (リモートアクセス) ポリシーに、ポリシーメンバーが含まれていません。

対策・説明: 管理者に問い合わせてください。

圧縮の不一致エラー。接続を再試行します。

原因: SSL VPN ポリシーが XG Firewall からはじめてダウンロードされ、SSL VPN トンネルがそのポリシーとともに確立されます。

対策・説明: このエラーは、接続の設定方法に基づいて次のように解決されます。

- プロビジョニングファイルの場合: Sophos Connect は自動的に再接続を試みます。
- ovpn ファイルの場合: 手動で再接続します。

ポリシーの不一致エラー。ポリシーをダウンロードし、接続を再試行します。

原因: Sophos Connect クライアントは、この接続用に保存された既存のポリシーに基づいて、SSL VPN 接続を確立しようとしました。

Sophos Connect によって SSL VPN 接続が確立、保存された後、管理者が XG Firewall の SSL VPN 設定を変更しました。

対策・説明: プロビジョニングファイルを使用して接続が作成されました。Sophos Connect は自動的に新しいポリシーをダウンロードし、SSL VPN トンネルを再確立します。

注
TCP 経由の SSL VPN トンネルが接続している状態で、管理者が XG Firewall の SSL VPN ポリシーを変更すると、Sophos Connect クライアントは新しいポリシーを直ちに検出してダウンロードします。UDP 経由の SSL VPN トンネルの場合は、「操作なしタイマー」がトンネルを削除するまで待機する必要があります。Sophos Connect は、その後、トンネルを再確立するために新しいポリシーをダウンロードします。

ポリシーの不一致エラー。この接続用に新しいポリシーをインポートします。

原因: Sophos Connect クライアントは、この接続用に保存された既存のポリシーに基づいて、SSL VPN 接続を確立しようとしました。

Sophos Connect が SSL VPN 接続を確立して保存した後、管理者が、XG Firewall の SSL VPN 設定を変更しました。

対策・説明: 接続は、ovpn ファイルをインポートして作成されました。ユーザーは、XG Firewall ユーザーポータルから新しい ovpn ファイルをダウンロードしインポートして、SSL VPN トンネルを再確立する必要があります。

注
TCP 経由の SSL VPN トンネルが接続している状態で、管理者が XG Firewall の SSL VPN ポリシーを変更すると、Sophos Connect クライアントはトンネルを検出し、切断して、エラーを表示します。UDP 経由の SSL VPN トンネルの場合は、「操作なしタイマー」がトンネルを削除するまで待機する必要があります。ユーザーは、XG Firewall ユーザーポータルから新しい ovpn ファイルをダウンロードしインポートして、SSL VPN トンネルを再確立する必要があります。

サーバーの応答を待機中、タイムアウトしました。

原因: SSL VPN ポリシーが XG Firewall で正しく設定されていません。障害の原因として、次のような事柄が考えられます。

1. 上書きホスト名が設定されているが、正しいまたは有効なパブリック IP アドレスに解決されない。
2. DDNS が設定されているが、正しいまたは有効なパブリック IP アドレスに解決されない。
3. 「**上書きホスト名**」と DDNS の両方が未設定で、WAN ポートにパブリック IP アドレスが設定されていない。

対策・説明: プロビジョニングファイルを使用して接続をインポートした場合は、(Sophos Connect クライアントで) ポリシー接続設定メニューを更新します。ovpn ファイルを使用して接続を作成した場合は、ユーザーポータルから新しい ovpn ファイルをエクスポートし、Sophos Connect クライアントに再度インポートします。

1.5 一般的なトラブルシューティング

ここでは、「イベント」ページに表示されないトラブルシューティングの項目について説明します。

さらにご不明な点は、ソフォス サポートへお問い合わせください。

VPN トンネルを通る際にトラフィックが停止する

原因: v17.5 よりも古いバージョンのファームウェアを実行している場合、フェーズ 1 のリキー (暗号鍵の交換) が行われた後に、クライアントが新しい仮想 IP アドレスを取得する可能性があります。

対策・説明: 接続を切断して再接続する必要があります。恒久的な解決策は、v17.5 にアップグレードすることです。

Sophos Connect のダッシュボードが開かない

原因: トレーアイコンをクリックしても Sophos Connect のダッシュボードが開かない場合や、応答がない場合は、Sophos Connect GUI が無限ループに入ったため、外部からのインプットに応答できなくなっている状態です。

対策・説明 (Windows): タスクマネージャを開き、詳細タブを開きます。scgui.exe を見つけ出し、右クリックして「タスクの終了」を選択します。デスクトップのショートカットからアプリケーションを再起動します。

対策・説明 (Mac): アクティビティモニタを開き、Sophos Connect のプロセスを見つけ出します。このプロセスを開き、「強制終了」を選択します。LaunchPad からアプリケーションを再起動します。

トンネルが切断されると、Web 閲覧が停止する

注
この問題は Mac でより多く見られます。

原因: すべてをトンネル経由にした接続が切断されると、DNS サーバーは物理ネットワークアダプタから復元されません。つまり、VPN 経由で接続したときに使用されていた内部 DNS サーバーが引き続き使用されます。トンネルが存在しなくなったため、名前解決は機能しません。

対策・説明: ローカルネットワークから切断し、再接続します。

Sophos Connect GUI に「サービスを使用できません」と表示される

注
この問題は Mac でより多く見られます。

原因: トンネルの切断が開始した際に、strongSwan Ipsec デーモンが無限ループに入った場合に発生します。これにより、GUI で切断に対する応答を取得できず、最終的にタイムアウトとなり、「サービスを使用できません」というエラーが表示されます。

対策・説明 (Mac):

1. アクティビティモニタを開き、Sophos Connect GUI のプロセスを終了させます。
2. ターミナルを開き、次のコマンドを実行します。

   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. Sophos Connect を開き、「サービスを使用できません」エラーが解決されたことを確認します。

対策・説明 (Windows):

1. 管理者権限で cmd を開き、次のコマンドを実行します。

   net stop scvpn

   net start scvpn
2. Sophos Connect を開き、「サービスを使用できません」エラーが解決されたことを確認します。

Sophos Connect がトンネルを確立できない

原因: 先に Sophos Connect クライアントをインストールし、その後に Sophos SSL VPN クライアントをインストールしたことが原因である場合があります。

対策・説明: 両方のクライアントをアンインストールして、Sophos SSL VPN クライアントを再インストールしてから、Sophos Connect クライアントを再インストールします。

注
両クライアントは、この順序でインストールする必要があります。

ゲートウェイから接続リセットを受信しました: <ゲートウェイ名>

このメッセージは、(インストールフォルダ内の) scvpn.log ファイルに記録されます。

原因: SSL VPN 設定が XG Firewall で変更されると、ユーザーが手動で切断されるか、または XG Firewall が再起動します。接続が TCP 経由で SSL VPN を使用している場合、XG Firewall は接続リセット要求を送信します。接続が UDP 経由で SSL VPN を使用している場合は、アイドルタイムアウトに応じて、接続が自動的に再接続されることがあります。

対策・説明: 新しい設定ファイルを Sophos Connect クライアントにインポートしてから再接続します。管理者がそのファイルを提供していない場合は、ユーザーポータルにアクセスしてダウンロードします。それ以外の場合は、ユーザーポータルに移動して ovpn ファイルをダウンロードします。

SSL VPN 接続で、自動接続およびポリシーの更新のメニュー項目がグレーアウト表示されている。

原因: ovpn ファイルをインポートして SSL VPN 接続を作成した場合、このようなオプションは使用できません。

対策・説明: オプションを有効にするには、プロビジョニングファイルを使用して接続を作成する必要があります。該当するオプションをプロビジョニングファイルに追加します。「**ポリシーの更新**」は、はじめて接続した後に使用可能になります。「**自動接続**」を有効にするには、内部ネットワークのみでアクセス可能な auto_connect_host を定義する必要があります。

自動接続を有効にするための最低要件を満たしたプロビジョニングファイルの例:

```
[
 {
  "display_name": "<接続名を入力>",
  "gateway": "<ゲートウェイのホスト名または IP を入力>",
  "auto_connect_host":"<内部ネットワークリソースのホスト名または IP を入力>"
 }
]
```

SSL VPN エラー

原因: OpenVPN サービスによって生成されたエラー。

対策・説明: 接続を再確立します。それでも問題が解決しない場合は、デバイスを再起動して、もう一度やり直してください。

管理ポートを使用できない

原因: Sophos Connect は、OpenVPN との通信に必要な TCP ポート 25340 を要求できません。

対策・説明: このポートを使用して実行中の別のアプリケーションがデバイスにないかどうかを確認します。可能であれば、そのアプリケーションを終了します。この問題を解決しないと、Sophos Connect 2.0 をご使用のデバイスで実行することはできません。他のアプリケーションがこのポー

トを使用していない場合は、一時的な状態によって発生した問題である可能性もあります。接続を再確立すると問題が解決するはずです。

一時ファイルの作成に失敗しました

原因: Sophos Connect は一時ファイルを使用して、接続の属性を OpenVPN サービスに渡します。Sophos Connect はこのデバイスでそのファイルを作成できませんでした。

対策・説明: デバイスを再起動します。

OpenVPN サービスを使用できません

原因: OpenVPN サービスが開始されていない可能性があります。

対策・説明: OpenVPN サービスのスタートアップタイプが「**無効**」に設定されている場合は、「**手動**」に変更し、Sophos Connect サービスも再起動します。

パイプへの書き込みに失敗しました

原因: Sophos Connect クライアントによって生成されたエラー。

対策・説明: 接続を再確立します。それでも問題が解決しない場合は、デバイスを再起動して、もう一度やり直してください。

2 Sophos Connect Admin について

Sophos Connect Admin では、設定 (.tgb) ファイルをインポートして、VPN 設定用のさまざまなオプションを設定できます。

注
XG Firewall で .tgb ファイルを設定およびエクスポートする方法の詳細は、XG Firewall ヘルプの Sophos Connect クライアントのセクションを参照してください。

Sophos Connect Admin のインストールおよびアンインストールのプロセスは、Sophos Connect のプロセスと同じです。詳細は、Sophos Connect ヘルプのインストールを参照してください。

2.1 設定ファイルの編集

Sophos Connect Admin で、より詳細な VPN 設定オプションを提供する設定 (.tgb) ファイルを編集できます。

XG Firewall からエクスポートした .tgb ファイルを Sophos Connect Admin で開きます。次の操作を行うことができます。

- すべてのトラフィックを VPN 接続を介して送信するには、「**Tunnel All**」(すべてをトンネル経由にする) を有効にします。
- Sophos Endpoint がハートビートを XG Firewall に送信できるようにするには、「**Send Security Heartbeat**」(セキュリティハートビートを送信する) を有効にします。これは、ユーザーのマシンに Sophos Endpoint クライアントがインストールされている場合のみに機能します。
- ユーザーが自分のマシンに自分のユーザー名とパスワードを保存できるようにするには、「**Allow Password Saving**」(パスワード保存を許可する) を有効にします。ユーザーの認証情報は、鍵チェーンサービスを使用して安全に保管されます。
- XG Firewall 上の VPN ユーザーに対して二要素認証を設定している場合は、「**Prompt for 2FA**」(二要素認証を要求する) を有効にします。
- ユーザーが自分のマシンから Sophos Connect にログオン後、接続を自動的に有効にするには、「**Auto-Connect Tunnel**」(自動接続トンネル) を有効にします。ユーザーが既に企業ネットワークに接続している場合、Sophos Connect は接続を自動的に開始しません。

  自動接続には、追加の設定パラメータ「**DNS Suffix/Monitoring Host**」(DNS サフィックス/モニタリングホスト) が必要です。これは、ユーザーのローカルシステムが社内ネットワークの内部にあるか外部にあるかを判断するために使用できます。次のいずれかの値を使用してください。

  — IP アドレス。

  — 完全修飾ドメイン名 (FQDN)。ホスト名は、内部 DNS サーバーを使用する場合のみに名前解決する必要があります。

  — DNS サフィックス。

注
IP アドレスまたは FQDN を設定する場合は、このホストで ICMP を許可する必要があります。

- ユーザーが接続できる「**Networks**」(ネットワーク) を追加、変更、および削除します。特定のネットワークをリストに追加すると、スプリットトンネリングが有効になります。つまり、ユーザーは、指定されたネットワークにあるリソースには VPN 接続を介してアクセスしますが、インターネットリソースには、リモートゲートウェイを介して直接アクセスします。

  注
  すべてのネットワークを削除すると、「**Tunnel All**」(すべてをトンネル経由にする) モードがアクティブになり、すべてのトラフィックが VPN 接続を介して転送されます。

- 「**Connection Name**」(接続名) と「**Target Host**」(ターゲットホスト) を変更します。

  設定を「**Clear**」(クリア) した場合は、.tbg ファイルを再度インポートする必要があります。

  「**Save**」(保存) をクリックすると、設定は .scx ファイルとして保存されます。

  注
  .scx ファイルは、インポートして、再編集できます。

設定ファイルを保存したら、ユーザーに送信できます。ユーザーはそれを Sophos Connect にインポートできます。詳細は、Sophos Connect を参照してください。

3 利用条件