SOPHOS

Cybersecurity made simple.

Sophos Connect

Hilfe

Inhalt

1 Über Sophos Connect

Sophos Connect ist ein VPN-Client, der auf Windows und Macs installiert werden kann. Er ermöglicht es Ihnen, sich von einem Remote-Standort, z. B. Ihrem Firmennetzwerk, mit Netzwerken hinter der XG zu verbinden. Ihr Firewall-Administrator konfiguriert die Verbindungsdaten auf der XG und stellt für Sie das Installationspaket und die Verbindungskonfigurationsdateien bereit.

In dieser Anleitung finden Sie Hinweise zur Verwendung von Sophos Connect:

- Hinweise zur Installation und Deinstallation von Sophos Connect finden Sie unter Installation von Sophos Connect (Seite 1).
- Hinweise zum Import von Verbindungsdateien und zur Verwaltung der Verbindungen finden Sie unter Verbindungen (Seite 2).
- Informationen zu Ereignissen und zur Behebung von ereignisbezogenen Fehlern finden Sie unter Ereignisse (Seite 11).
- Hinweise zur Behebung von Fehlern, die nicht im Abschnitt Ereignisse aufgeführt sind, finden Sie unter Allgemeine Fehlerbehebung (Seite 18).

1.1 Installation von Sophos Connect

Installation von Sophos Connect unter Windows

- Öffnen Sie den Installer.
- Stimmen Sie der Lizenzvereinbarung zu und klicken Sie auf **Installieren**.
- Klicken Sie nach Abschluss der Installation auf **Fertigstellen**. Sie können auswählen, dass Sophos Connect nach dem Beenden gestartet wird.

Installation von Sophos Connect auf Mac

- Öffnen Sie den Installer.
- Wählen Sie das Installationsziel aus. Stellen Sie sicher, dass auf dem gewählten Ziel, z. B. das Systemlaufwerk, genügend freier Speicherplatz vorhanden ist.
- Klicken Sie auf **Installieren**.
- Klicken Sie nach Abschluss der Installation auf **Fertigstellen**.

1.2 Deinstallation von Sophos Connect

Deinstallation von Sophos Connect unter Windows

- Gehen Sie zur **Systemsteuerung** und klicken Sie unter **Programme** auf **Programm deinstallieren**.
- Klicken Sie mit der rechten Maustaste auf Sophos Connect und wählen Sie **Deinstallieren**.

Deinstallation von Sophos Connect auf Mac

- Öffnen Sie das Terminal.
- Erhöhen Sie die Berechtigung auf Root und führen Sie das Script in dem Verzeichnis aus, in dem Sophos Connect installiert ist:

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

Bei erfolgreicher Deinstallation wird folgende Meldung angezeigt:

```
Sophos Connect has been uninstalled
```

1.3 Verbindungen

Sie können Verbindungen importieren, Verbindungen herstellen und Verbindungen anzeigen und bearbeiten.

Sophos Connect unterstützt SSL VPN und IPsec VPN.

1.3.1 Verbindungen importieren

Der Sophos Connect-Client kann sich über SSL- oder IPsec-VPN-Verbindungen mit der XG-Firewall verbinden. Sie können Verbindungen in den Sophos Connect-Client importieren.

Einleitung

Bei Version 2.0 des Sophos Connect-Clients können Sie sowohl SSL- als auch IPsec-VPN-Verbindungen importieren. Wenn Sie eine frühere Version des Sophos Connect-Clients verwenden, können Sie nur IPsec-Verbindungen importieren.

Diese Seite beschreibt Folgendes:

- Importieren Sie eine IPsec-Verbindung mithilfe einer Datei, die Ihnen von Ihrem Administrator bereitgestellt wurde.
- Importieren Sie eine SSL-Verbindung mithilfe einer Datei, die Ihnen von Ihrem Administrator bereitgestellt wurde.
- Importieren Sie eine SSL-Verbindung, indem Sie eine Datei aus dem Benutzerportal herunterladen.

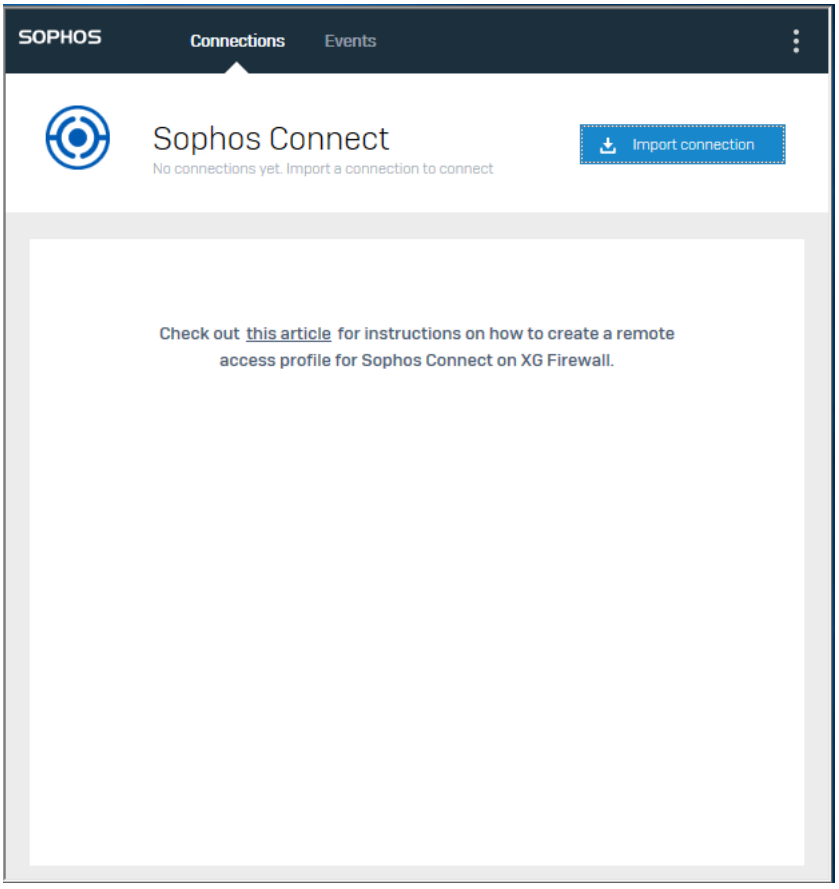
IPsec-Verbindung importieren

Ihnen wurde eine Verbindungsdatei bereitgestellt. Die Datei hat die Endung `tgb`, z. B. `Company_connection.tgb`.

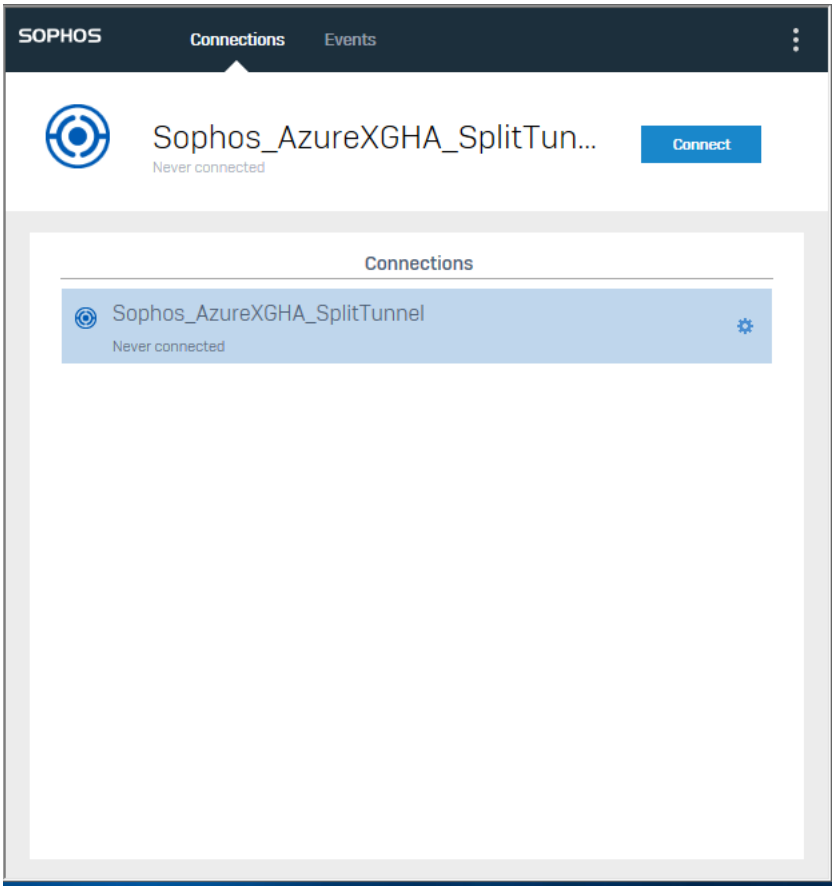
So importieren Sie eine Verbindung:

1. Klicken Sie auf der Seite **Verbindungen** auf **Verbindung importieren**.

   Wenn bereits Verbindungen vorhanden sind, klicken Sie auf die Menüschaltfläche und wählen Sie im Dropdown-Menü **Verbindung importieren** aus.



2. Suchen Sie nach der `.tgb`-Datei und doppelklicken Sie darauf.
   Die Verbindung wird unter **Verbindungen** angezeigt.



Sie können die Verbindung jetzt herstellen.

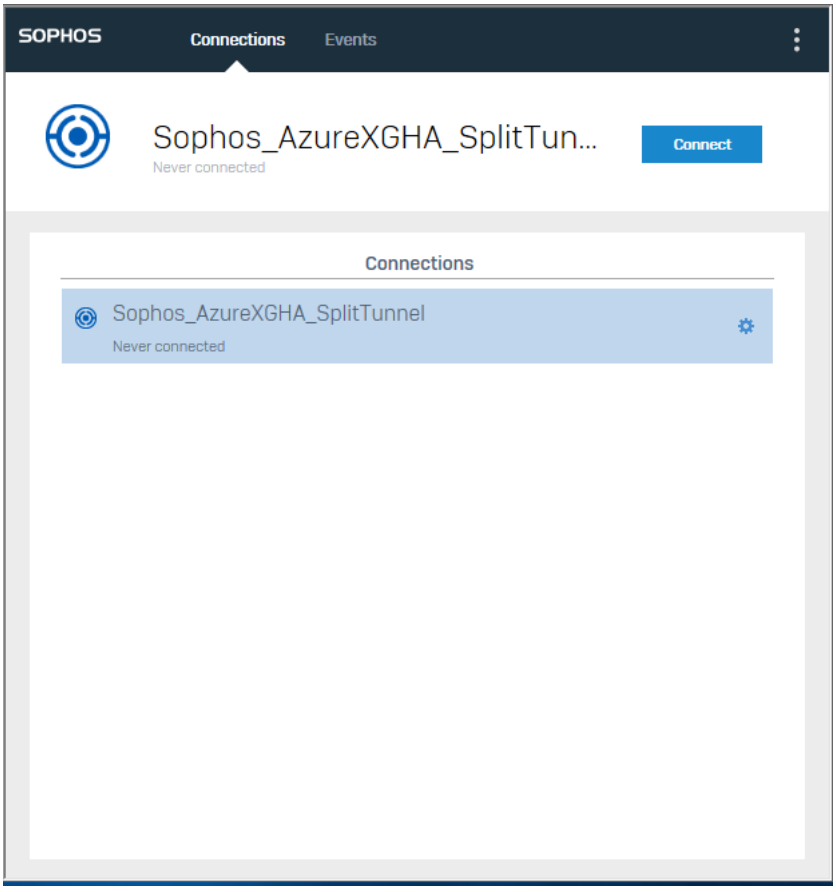
Hinweis
Sie können mehrere Verbindungen importieren.

Importieren einer SSL-Verbindung

Ihnen wurde eine Verbindungsdatei bereitgestellt. Die Datei hat die Endung `pro`, z. B. `Company_connection.pro`.

So importieren Sie eine Verbindung:

Suchen Sie nach der `.pro`-Datei und doppelklicken Sie darauf.
Die Verbindung wird automatisch importiert und Sophos Connect wird geöffnet. Die Verbindung wird unter **Verbindungen** angezeigt.



Sie können die Verbindung jetzt herstellen.

Hinweis
Sie können mehrere Verbindungen importieren.

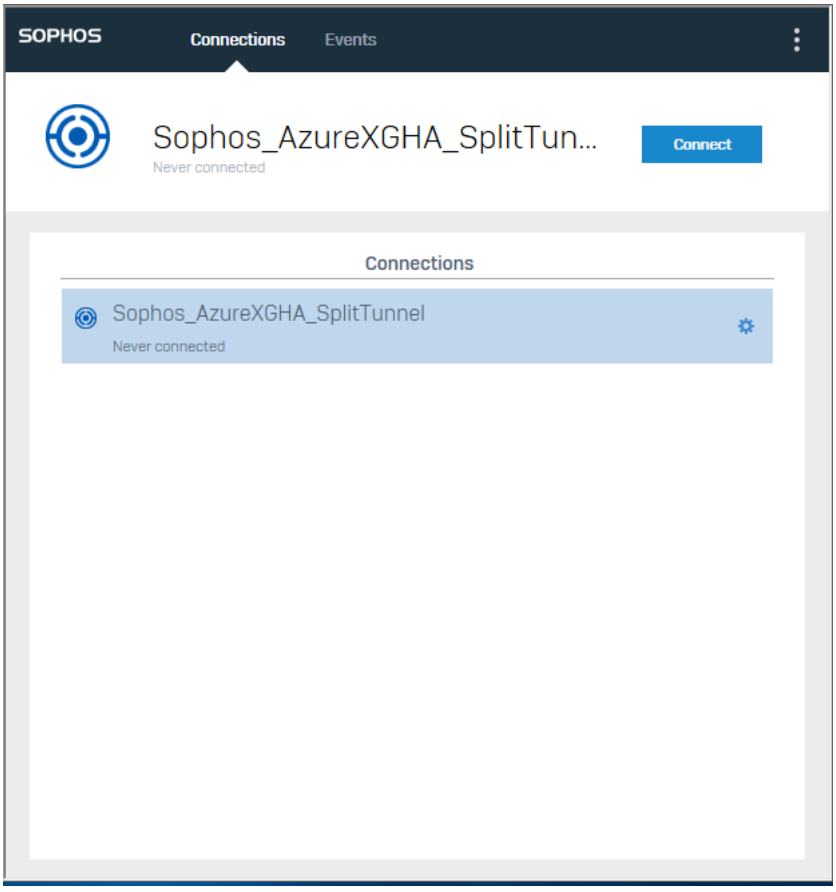
Importieren einer SSL-Verbindung aus dem Benutzerportal

So importieren Sie eine Verbindung:

1. Melden Sie sich beim Benutzerportal an.
2. Gehen Sie zu **SSLVPN** und klicken Sie auf **Konfiguration für andere Betriebssysteme herunterladen**.
3. Öffnen Sie den Sophos Connect-Client.
4. Klicken Sie auf der Seite **Verbindungen** auf **Verbindung importieren**.

   Wenn bereits Verbindungen vorhanden sind, klicken Sie auf die Menüschaltfläche und wählen Sie im Dropdown-Menü **Verbindung importieren** aus.
5. Suchen Sie nach der `.ovpn`-Datei und öffnen Sie sie.

Die Verbindung wird unter **Verbindungen** angezeigt.



Sie können die Verbindung jetzt herstellen.

Hinweis
Sie können mehrere Verbindungen importieren.

1.3.2 Verbinden

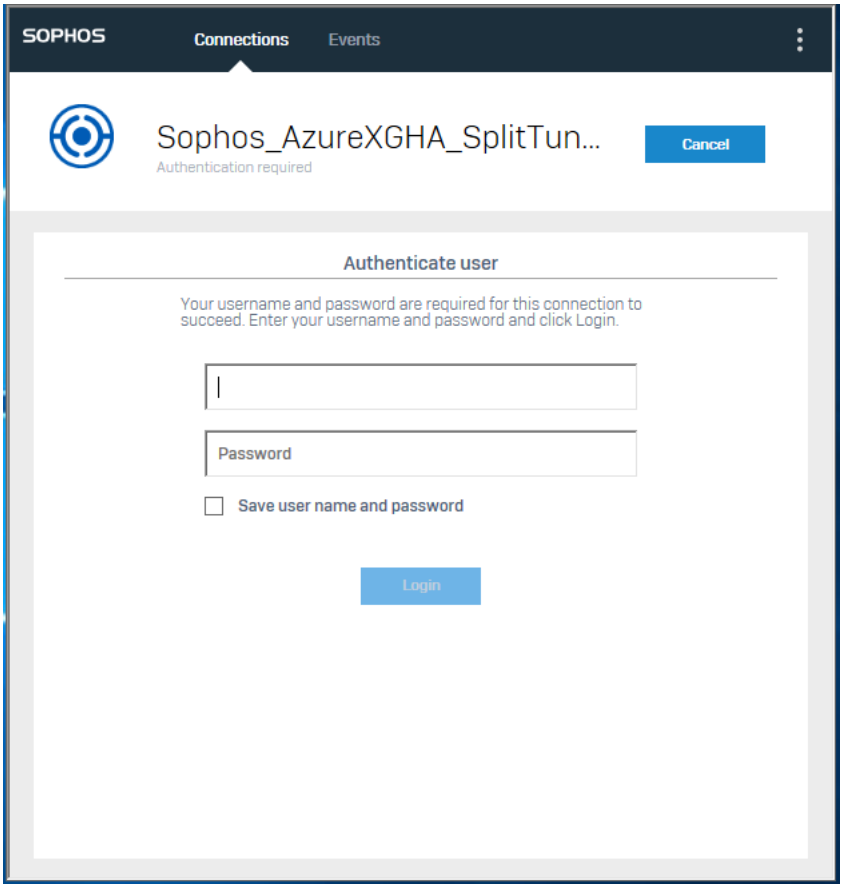
Stellen Sie sicher, dass mindestens eine importierte Verbindung verfügbar ist und die erforderlichen Zugangsdaten vorliegen.

So stellen Sie eine Verbindung her:

1. Wählen Sie auf der Seite **Verbindungen** eine Verbindung aus.
2. Doppelklicken Sie auf die Verbindung.

   Sie können auch auf **Verbinden** klicken.

   Daraufhin öffnet sich der Anmelde-Bildschirm.

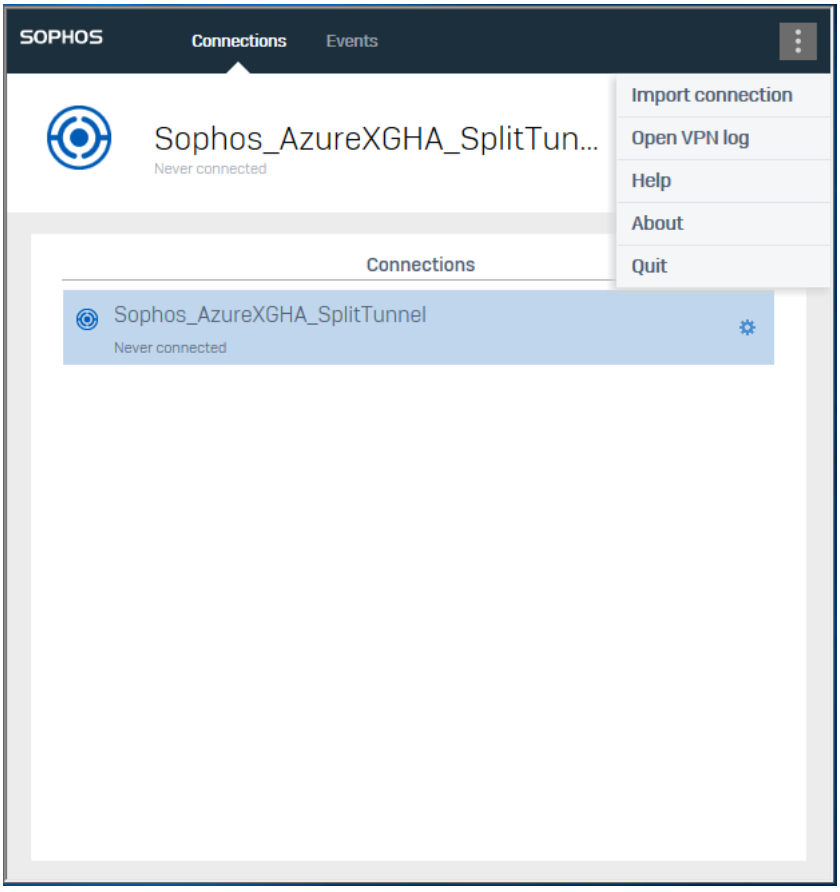


3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein und klicken Sie auf **Anmelden**.
   Ihr Administrator hat möglicherweise eine Zwei-Faktor-Authentifizierung konfiguriert.
   - Wenn Ihr Administrator OTP konfiguriert hat, müssen Sie zusätzlich zu Ihrem Benutzernamen und Kennwort auch Ihren 6-stelligen OTP-Passcode eingeben.
   - Wenn Ihr Administrator die DUO-Authentifizierung konfiguriert hat, erhalten Sie möglicherweise eine oder zwei DUO-Aufforderungen während des Verbindungsvorgangs.

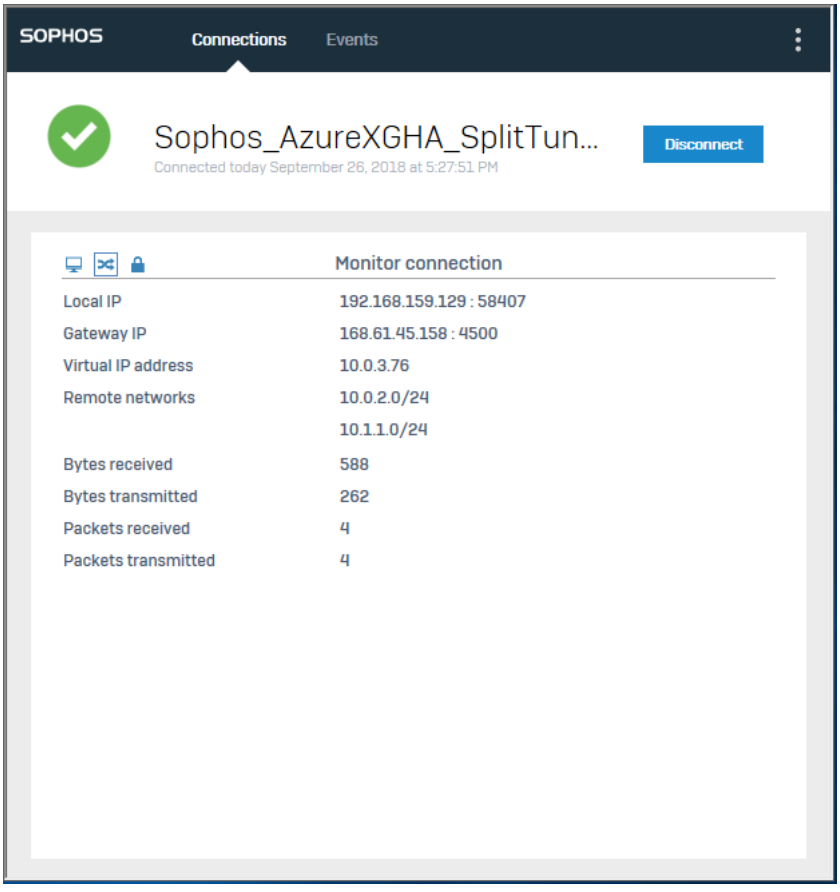
   Hinweis
   Wenn Sie die Verbindung mithilfe einer Bereitstellungsdatei importiert haben, erhalten Sie eine Warnung, dass das Serverzertifikat nicht verifiziert werden kann. Klicken Sie auf **OK**, um fortzufahren. Wenn diese Meldung nicht mehr angezeigt werden soll, wenden Sie sich an Ihren Administrator.

   Sophos Connect versucht, eine Verbindung herzustellen und Sie zu authentifizieren.

   Hinweis
   Bei Verbindungsproblemen überprüfen Sie die Seite **Ereignisse** und wenden Sie sich an Ihre IT-Abteilung. Sie können auch die VPN-Protokolle überprüfen, indem Sie auf das Menüsymbol klicken und diese auswählen.



Die Verbindung zum Remote-Server ist hergestellt.



Wurde die Verbindung erfolgreich hergestellt, wird folgendes Symbol in der Taskleiste angezeigt:

Konnte die Verbindung nicht hergestellt werden, wird folgendes Symbol in der Taskleiste angezeigt:

Hinweis
Wenn Sie die Verbindung umbenannt haben, wird der ursprüngliche Name (der Ihnen von Ihrem Firewall-Administrator mitgeteilt wurde) weiterhin in den Verbindungsdetails angezeigt. Hinweise zum Umbenennen von Verbindungen finden Sie unter Verbindungsoptionen (Seite 9).

1.3.3 Verbindungsoptionen

Sie können verschiedene Änderungen der Verbindungen in Sophos Connect vornehmen. Klicken Sie dazu auf das Symbol für die Einstellungen rechts neben der Verbindung.

1. Mit **Automatisch verbinden** wird versucht, eine Verbindung herzustellen, sobald Sophos Connect gestartet wird.
2. Mit **Löschen** wird die Verbindung gelöscht. Wenn Sie die Verbindung wiederherstellen möchten, müssen Sie sie erneut importieren.
3. Mit **Umbenennen** können Sie Ihre Verbindung umbenennen.
4. Mit **Anmeldeinformationen löschen** werden zuvor gespeicherte Anmeldeinformationen gelöscht.
5. **Richtlinie aktualisieren** (nur verfügbar, wenn die Verbindung mit einer Bereitstellungsdatei erstellt wurde). Hiermit können Sie bei Bedarf die neueste Richtlinie von der XG-Firewall abrufen.

Tipp
Wenn die Verbindung nach mehreren Versuchen fehlschlägt, initiieren Sie eine Richtlinienaktualisierung und versuchen Sie erneut, eine Verbindung herzustellen.

1.4 Ereignisse

Hier sehen Sie alle Aktionen in Sophos Connect und die Ergebnisse dieser Aktionen. Dazu gehören Probleme aufgrund von Maßnahmen der Benutzer sowie mit der IKE-Aushandlung. Hinweise zur Behebung von ereignisbezogenen Fehlern finden Sie unter Behebung von Ereignissen (Seite 12).

- Wenn zur Behebung eines Problems nähere Fehlerinformationen erforderlich sind, klicken Sie auf **VPN-Protokoll öffnen**.
- Um Ereignisse aus der Liste zu entfernen, klicken Sie auf **Ereignisse löschen**.

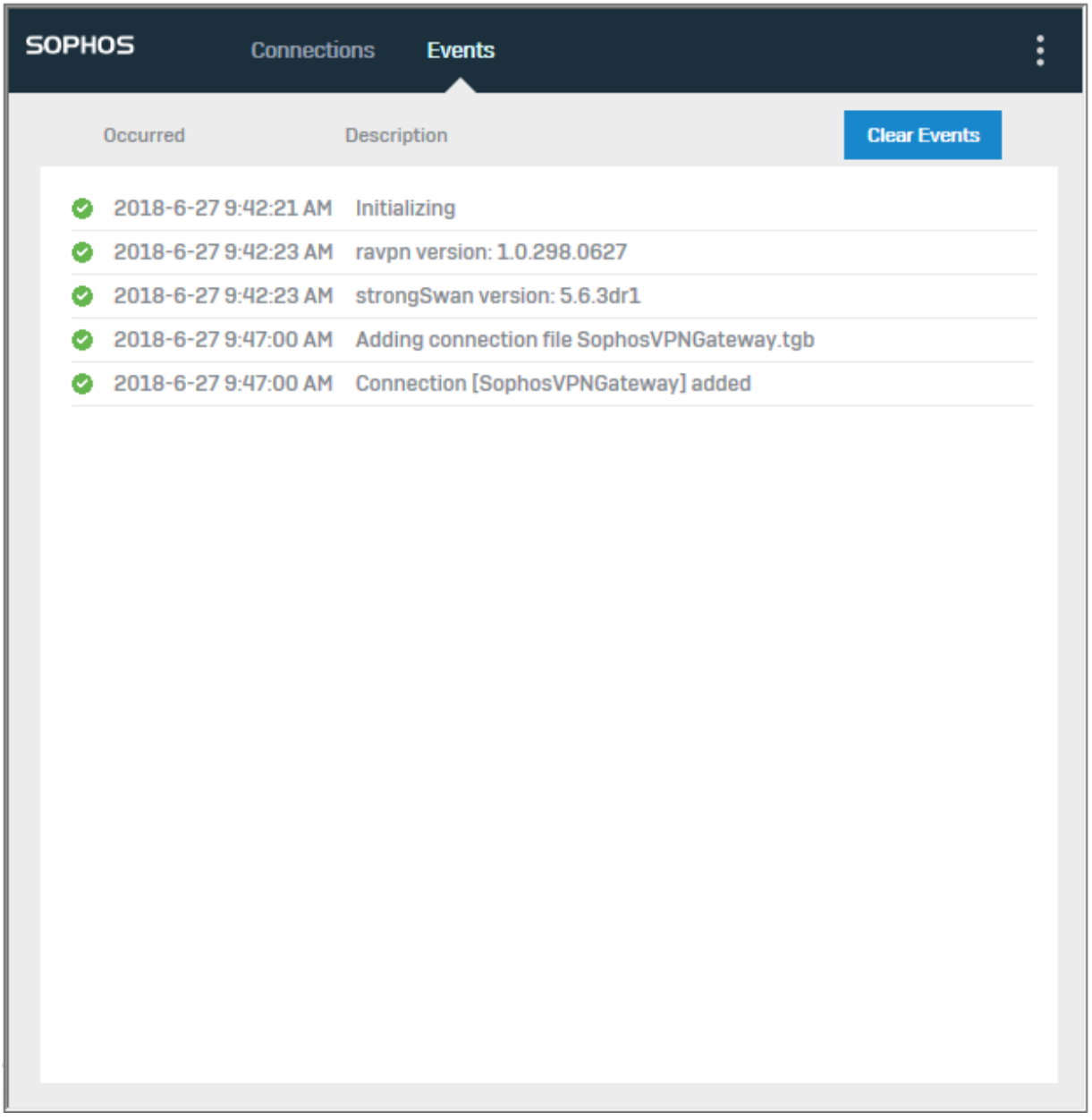


Abbildung 1: Ereignisse

1.4.1 Behebung von Ereignissen

Wenn Sie Probleme beim Herstellen der Verbindung haben, klicken Sie auf **Ereignisse**, suchen nach dem Zeitstempel des Verbindungsversuchs und dann nach dem betreffenden Fehler.

In diesem Abschnitt werden die Fehlermeldungen, mögliche Fehlerursachen und Maßnahmen beschrieben. Wenn bei Ihnen ein Problem aufgetreten ist, das unten nicht beschrieben ist, lesen Sie unter Allgemeine Fehlerbehebung nach.

Wenn Sie weitergehende Hilfe benötigen, kontaktieren Sie den Sophos Support.

Keine Netzwerkverbindung

Ursache: Der Netzwerkadapter (Ethernet oder WLAN) hat keine IP-Adresse.

Maßnahme: Stellen Sie sicher, dass Sie eine gültige IP-Adresse haben und dass Ihre vorhandene Netzwerkverbindung funktioniert.

DNS-Auflösung fehlgeschlagen

Ursache: Der Client kann den Hostnamen des Gateways nicht auflösen.

Maßnahme: Überprüfen Sie, ob der Netzwerkschnittstelle ein DNS-Server zugewiesen ist. Führen Sie `nslookup` über die Eingabeaufforderung (Windows) oder über das Terminal (Mac) für einen öffentlichen Host aus, z. B. www.sophos.com, und überprüfen Sie, ob eine Auflösung in eine IP-Adresse erfolgt. Falls nicht, wenden Sie sich an Ihren Internetprovider.

UDP-Ports 500/4500 blockiert

Ursache: Die Firewall oder der Router blockiert die UDP-Ports 500 und 4500.

Maßnahme: Überprüfen Sie die Konfiguration Ihrer lokalen Firewall oder Ihres Routers und erlauben Sie Datenverkehr an diesen Ports. Wenn Sie keinen Zugriff auf die Firewall oder den Router haben, z. B. wenn Sie sich in einem Hotel aufhalten, verbinden Sie sich über Ihren mobilen Hotspot und versuchen erneut, eine Verbindung herzustellen.

Keine Antwort von Gateway: <gateway FQDN or IP specified in connection>

Ursache: Das Gateway antwortet nicht auf IKE-Aushandlungsmeldungen. Dies kann daran liegen, dass:

- Das Remote-Gateway (Firewall oder Router) heruntergefahren wurde.
- Die WAN-Adresse am Remote-Gateway nicht direkt mit dem Internet verbunden ist.

Maßnahme: Kontaktieren Sie Ihren Firewall-Administrator und melden Sie das Problem.

Meldung NO_PROPOSAL_CHOSEN erhalten von Gateway

Ursache: Das Remote-Gateway hat auf IKE-Aushandlungen von Sophos Connect mit dieser Fehlermeldung geantwortet. Dies kann daran liegen, dass:

- Keine Sophos Connect-Richtlinie auf der Firewall eingerichtet wurde oder aktiviert ist.
- Der Firewall-Administrator die IKE-Proposals der Phase 1, die für die Sophos Connect-Richtlinie auf der Firewall verwendet werden, geändert hat und die neue Konfiguration nicht exportiert und zum Client übertragen wurde.

Maßnahme: Kontaktieren Sie Ihren Firewall-Administrator und melden Sie das Problem.

Server erwartete Remote-ID <erwarteter ID-Wert>, erhielt aber <tatsächlicher ID-Wert>

Ursache: Der Typ oder Wert der lokalen ID, wie er in der Sophos Connect-Richtlinie auf der Firewall konfiguriert ist, ist ein anderer als der für diese Verbindung verwendete Wert. Das kann daran liegen, dass der Firewall-Administrator die lokale ID auf der Firewall geändert hat und die neue Konfigurationsdatei nicht in Sophos Connect importiert wurde.

Maßnahme: Kontaktieren Sie Ihren Firewall-Administrator und melden Sie das Problem.

Möglicherweise stimmt der Pre-Shared Key nicht mit <Verbindungsname> überein

Ursache: Der Pre-Shared Key auf der Firewall stimmt nicht mit dem für diese Verbindung verwendeten PSK überein. Das kann daran liegen, dass der Firewall-Administrator den PSK auf der Firewall geändert hat und die neue Konfigurationsdatei nicht zu Sophos Connect übertragen wurde.

Maßnahme: Kontaktieren Sie Ihren Firewall-Administrator und melden Sie das Problem.

Benutzerauthentifizierung von <eingegebener Benutzername> fehlgeschlagen

Ursache: Benutzername oder Kennwort ist nicht korrekt.

Maßnahme: Versuchen Sie es erneut – möglicherweise lag ein Eingabefehler vor. Wenn Sie es mehrere Male versucht haben und immer wieder dieselbe Fehlermeldung erhalten, hat sich möglicherweise auf der Firewall das Kennwort geändert oder es wurde deaktiviert. Wenden Sie sich in diesem Fall an Ihren Firewall-Administrator und melden Sie das Problem.

Route [Netzwerk/Maske] konnte nicht hinzugefügt werden, daher konnte Phase 2 nicht abgeschlossen werden

Hinweis
Die unten beschriebenen Schritte zur Fehlerbehebung gelten nur für Windows.

Ursache: Nachdem eine SA der Phase 2 angelegt wurde, ist `route add` zum Remote-Netzwerk fehlgeschlagen. Das kann daran liegen, dass der strongSwan-Dienst abgestürzt ist, während der Tunnel aktiv war.

Maßnahme: Deaktivieren Sie den TAP-Adapter und aktivieren ihn erneut. Öffnen Sie die Befehlszeile als Administrator und geben Sie die folgenden Befehle ein:

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

Die Verbindungsdaten konnten nicht hinzugefügt werden. Eine Verbindung mit dem Namen <Verbindungsname> ist bereits vorhanden.

Ursache: Es wurde bereits eine Verbindung mit diesem Namen importiert.

Maßnahme: Löschen Sie die vorhandene Verbindung aus Sophos Connect. Stellen Sie vorher sicher, dass Sie die vorhandene Verbindung wirklich löschen möchten. Wenden Sie sich andernfalls an Ihren Administrator, um die Fehlerbehebung weiter durchzuführen.

Dienst ist nicht verfügbar

Hinweis
Die unten beschriebenen Schritte zur Fehlerbehebung gelten nur für Windows.

Ursache: Der Sophos Connect-Dienst (scvpn) wird nicht ausgeführt.

Maßnahme: Öffnen Sie die Befehlszeile als Administrator und geben Sie den folgenden Befehl ein:

```
net start scvpn
```

Verbindungsinformationen konnten nicht in strongSwan geladen werden

Hinweis
Die unten beschriebenen Schritte zur Fehlerbehebung gelten nur für Windows.

Ursache: Der strongSwan-Dienst wird nicht ausgeführt (Dienstname: charon-svc.exe).

Maßnahme: Öffnen Sie die Befehlszeile als Administrator und geben Sie den folgenden Befehl ein:

```
net start strongswan
```

SA durch Gateway deaktiviert oder gelöscht

Ursache: Das Gateway hat eine IKE-Löschanfrage gesendet, dann wurde der Tunnel gelöscht. Dies kann daran liegen, dass:

- Der Firewall-Administrator die Richtlinie auf der Firewall geändert hat. Dadurch wird eine IKE-Löschanfrage an alle aktiven SAs auf der Firewall gesendet.
- Der Firewall-Administrator manuell alle IPsec-Verbindungen für diesen Benutzer auf der Firewall gelöscht hat.

Maßnahme: Versuchen Sie, erneut eine Verbindung herzustellen. Wenn es immer noch nicht funktioniert, wenden Sie sich für die weitere Problembehebung an Ihren Administrator.

DNS-Auflösung fehlgeschlagen für Gateway: <Gateway-Name:Port>

Ursache: Dieser Fehler ist auf einen ungültigen Hostnamen zurückzuführen.

Maßnahme:

- Wenn die Verbindung mithilfe einer Bereitstellungsdatei hinzugefügt wurde, überprüfen Sie den angegebenen Hostnamen.
- Wenn die Verbindung durch Importieren einer `ovpn`-Datei hinzugefügt wurde, überprüfen Sie die SSL VPN-Einstellungen auf der XG Firewall.

Serverzertifikat kann nicht verifiziert werden: <Gateway-Name>. Möchten Sie fortfahren?

Ursache: Der Sophos Connect-Client importiert die SSL VPN-Konfiguration, indem er über die Eigenschaften in der Bereitstellungsdatei eine Verbindung zum Benutzerportal der XG Firewall herstellt. Das Benutzerportal verwendet ein selbstsigniertes Zertifikat, das vom Sophos Connect-Client nicht verifiziert werden kann.

Maßnahme: Akzeptieren Sie die Sicherheitswarnung, um eine Verbindung herzustellen und die `ovpn`-Konfigurationsdatei vom Benutzerportal herunterzuladen. Damit die Aufforderung in Zukunft nicht mehr angezeigt wird, verwenden Sie eine der folgenden Optionen:

- Stellen Sie ein neues, von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat für die XG Firewall aus. Importieren Sie auf der XG Firewall das Zertifikat und wählen Sie dann das Zertifikat in den **Admin-Einstellungen** für die Anmeldung bei der Web-Admin-Konsole aus.
- Verschieben Sie das Standard-CA-Zertifikat von der XG Firewall in den vertrauenswürdigen Speicher auf den Remote-Computern.

Verbindung zum nicht vertrauenswürdigen Server: <gateway>

Ursache: Sie haben die Zertifikatwarnung abgebrochen und die Verbindung wurde beendet.

Maßnahme: Akzeptieren Sie die Sicherheitswarnung, um eine Verbindung herzustellen und die SSL VPN-Richtlinie von der XG Firewall herunterzuladen. Damit die Aufforderung nicht mehr angezeigt wird, wenn die SSL VPN-Richtlinie heruntergeladen wird, verwenden Sie eine der folgenden Optionen:

- Stellen Sie ein neues, von einer öffentlichen Zertifizierungsstelle signiertes Zertifikat für die XG Firewall aus. Importieren Sie auf der XG Firewall das Zertifikat und wählen Sie dann das Zertifikat in den **Admin-Einstellungen** für die Anmeldung bei der Web-Admin-Konsole aus.
- Übertragen Sie das Standard-CA-Zertifikat von der XG Firewall in den vertrauenswürdigen Speicher auf den Remote-Computern.

Importdatei enthält eine doppelte Verbindung: <Verbindungsname>

Ursache: Die aus einer Bereitstellungsdatei importierte Verbindung hat einen doppelten Anzeigenamen.

Maßnahme: Überprüfen Sie das Attribut `display_name` in der Bereitstellungsdatei und benennen Sie alle doppelten Namen um.

Verbindung mit Richtlinien-Gateway nicht möglich: <Gateway-Name>

Ursache: Die Bereitstellungsdatei ist falsch konfiguriert. Dies könnte die folgenden Gründe haben:

1. Ungültiger Gateway-Hostname oder ungültige IP-Adresse.
2. Ungültiger Port oder blockierter Port für ausgehenden Datenverkehr.

3. Das Richtlinien-Gateway ist nicht erreichbar, da es deaktiviert ist.

Maßnahme:

Überprüfen Sie die Bereitstellungsdatei auf Folgendes:

1. Stellen Sie sicher, dass der dem Attribut `gateway` zugewiesene Wert korrekt ist.
2. Stellen Sie sicher, dass der dem Attribut `user_portal_port` zugewiesene Wert mit der HTTPS-Porteinstellung des Benutzerportals auf der XG Firewall übereinstimmt.
3. Wenn die Bereitstellungsdatei korrekt konfiguriert ist, wenden Sie sich für die weitere Problembehebung an Ihren Administrator.

Für diesen Benutzer ist keine SSL VPN-Richtlinie definiert: <Benutzername>

Ursache: Die SSL VPN-Richtlinie (Remotezugriff) der XG Firewall enthält keine Richtlinienmitglieder.

Maßnahme: Wenden Sie sich an Ihren Administrator.

Komprimierungsfehler (fehlende Übereinstimmung). Versucht erneut, die Verbindung herzustellen.

Ursache: Eine SSL VPN-Richtlinie wird zum ersten Mal von der XG Firewall heruntergeladen und mit ihr der SSL VPN-Tunnel eingerichtet.

Maßnahme: Die Fehlerbehebung erfolgt anhand dessen, wie die Verbindung konfiguriert ist:

- Mit einer Bereitstellungsdatei: Sophos Connect versucht automatisch erneut, eine Verbindung herzustellen.
- Mit einer `ovpn`-Datei: Manuelle erneute Verbindung.

Richtlinienfehler (fehlende Übereinstimmung). Lädt die Richtlinie herunter und versucht erneut, die Verbindung herzustellen.

Ursache: Der Sophos Connect-Client hat versucht, eine SSL VPN-Verbindung mit einer vorhandenen Richtlinie herzustellen, die er für diese Verbindung gespeichert hat.

Der Administrator hat die SSL VPN-Einstellungen auf der XG Firewall geändert, nachdem eine SSL VPN-Verbindung hergestellt und von Sophos Connect gespeichert wurde.

Maßnahme: Die Verbindung wurde mithilfe einer Bereitstellungsdatei erstellt. Sophos Connect lädt die neue Richtlinie automatisch herunter und stellt den SSL VPN-Tunnel wieder her.

Hinweis
Wenn der Administrator die SSL VPN-Richtlinie auf der XG Firewall ändert, während der Tunnel verbunden ist, und es sich um einen SSL VPN über TCP-Tunnel handelt, erkennt der Sophos Connect Client die neue Richtlinie und lädt sie sofort herunter. Wenn es sich um einen SSL VPN über UDP-Tunnel handelt, müssen Sie warten, bis der Inaktivitäts-Timer den Tunnel löscht. Sophos Connect lädt dann die neue Richtlinie herunter, um den Tunnel wiederherzustellen.

Fehler wegen Richtlinienabweichung. Importieren Sie eine neue Richtlinie für diese Verbindung.

Ursache: Der Sophos Connect-Client hat versucht, eine SSL VPN-Verbindung mit einer vorhandenen Richtlinie herzustellen, die er für diese Verbindung gespeichert hat.

Der Administrator hat die SSL VPN-Einstellungen auf der XG Firewall geändert, nachdem eine SSL VPN-Verbindung hergestellt und von Sophos Connect gespeichert wurde.

Maßnahme: Die Verbindung wurde durch den Import einer ovpn-Datei hergestellt. Der Benutzer muss eine neue ovpn-Datei aus dem XG Firewall-Benutzerportal herunterladen und importieren, um den SSL VPN-Tunnel wiederherzustellen.

Hinweis
Wenn der Administrator die SSL VPN-Richtlinie auf der XG Firewall ändert, während der Tunnel verbunden ist, und es sich um einen SSL VPN über TCP-Tunnel handelt, erkennt der Sophos Connect Client den Tunnel und trennt ihn mit einem Fehler. Wenn es sich um einen SSL VPN über UDP-Tunnel handelt, müssen Sie warten, bis der Inaktivitäts-Timer den Tunnel löscht. Der Benutzer muss eine neue ovpn-Datei aus dem XG Firewall-Benutzerportal herunterladen und importieren, um den SSL VPN-Tunnel erfolgreich wiederherzustellen.

Zeitüberschreitung beim Warten auf Serverantwort.

Ursache: Die SSL VPN-Richtlinie ist in der XG Firewall falsch konfiguriert. Mögliche Gründe für den Fehler sind:

1. „Hostname überschreiben“ ist konfiguriert, es erfolgt aber keine Auflösung in die richtige oder gültige öffentliche IP-Adresse.
2. DDNS ist konfiguriert, es erfolgt aber keine Auflösung in die richtige oder gültige öffentliche IP-Adresse.
3. Sowohl **Hostname überschreiben** als auch DDNS sind nicht konfiguriert und der WAN-Port verfügt nicht über eine öffentliche IP-Adresse.

Maßnahme: Wenn Sie zum Importieren der Verbindung eine Bereitstellungsdatei verwendet haben, aktualisieren Sie das Menü für die Verbindungseinstellungen der Richtlinie (auf dem Sophos Connect-Client). Wenn Sie zum Erstellen der Verbindung eine ovpn-Datei verwendet haben, exportieren Sie eine neue ovpn-Datei aus dem Benutzerportal und importieren Sie sie erneut in den Sophos Connect-Client.

1.5 Allgemeine Fehlerbehebung

In diesem Abschnitt ist die Behebung von Fehlern beschrieben, die nicht auf der Seite Ereignisse aufgeführt sind.

Wenn Sie weitergehende Hilfe benötigen, kontaktieren Sie den Sophos Support.

Datenverkehr stoppt bei Passieren des VPN-Tunnels

Ursache: Wenn Sie mit einer Firmware-Version arbeiten, die älter ist als v17.5, kann es sein, dass der Client eine neue virtuelle IP nach dem Rekeying der Phase 1 erhalten hat.

Maßnahme: Trennen Sie die Verbindung und stellen Sie sie wieder her. Eine dauerhafte Lösung wäre die Aktualisierung auf v17.5.

Das Sophos Connect Dashboard öffnet sich nicht

Ursache: Wenn sich das Sophos Connect Dashboard nicht öffnet oder nicht reagiert, wenn Sie auf das Systray-Symbol klicken, bedeutet dies, dass sich die Sophos Connect GUI in einer Endlosschleife befindet und nicht auf externe Eingaben reagieren kann.

Maßnahme (Windows): Öffnen Sie den Task-Manager und wählen Sie die Registerkarte „Details“. Suchen Sie nach scgui.exe und klicken Sie mit der rechten Maustaste darauf, um den Task zu beenden. Starten Sie die Anwendung über die Desktop-Verknüpfung neu.

Maßnahme (Mac): Öffnen Sie die Aktivitätsanzeige und suchen Sie nach dem Sophos Connect-Prozess. Öffnen Sie diesen Prozess und wählen Sie „Sofort beenden“. Starten Sie die Anwendung über das Launchpad neu.

Das Surfen im Internet funktioniert nicht mehr, wenn der Tunnel getrennt wird

Hinweis
Diese Meldung betrifft hauptsächlich Macs.

Ursache: Wenn eine Verbindung getrennt wird, bei der alles getunnelt wird, werden die DNS-Server nicht von den physischen Netzwerkadaptern wiederhergestellt. Das bedeutet, dass die internen DNS-Server, die verwendet wurden, als Sie über das VPN verbunden waren, weiterhin verwendet werden. Da der Tunnel nicht mehr existiert, funktioniert die Namensauflösung nicht.

Maßnahme: Trennen Sie die Verbindung zum lokalen Netzwerk und stellen Sie dann die Verbindung wieder her.

Sophos Connect GUI meldet „Dienst nicht verfügbar“

Hinweis
Diese Meldung betrifft hauptsächlich Macs.

Ursache: Wenn die Trennung der Verbindung zum Tunnel initiiert wird, gerät der strongSwan IPsec-Daemon in eine Endlosschleife. Das führt dazu, dass die GUI keine Antwort für den Trennungsvorgang erhält und es zu einem Timeout kommt. Der Fehler wird dann als „Dienst nicht verfügbar“ angezeigt.

Maßnahme (Mac):

1. Öffnen Sie die Aktivitätsanzeige und suchen Sie nach dem Sophos Connect GUI-Prozess.
2. Öffnen Sie das Terminal und führen Sie die folgenden Befehle aus:

   ```
   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. Öffnen Sie Sophos Connect und überprüfen Sie, ob der Fehler „Dienst nicht verfügbar“ nun behoben ist.

Maßnahme (Windows):

1. Öffnen Sie `cmd` als Administrator und führen Sie die folgenden Befehle aus:

   ```
   net stop scvpn
   ```

   ```
   net start scvpn
   ```

2. Öffnen Sie Sophos Connect und überprüfen Sie, ob der Fehler „Dienst nicht verfügbar“ nun behoben ist.

Sophos Connect kann keinen Tunnel aufbauen

Ursache: Vermutlich haben Sie zuerst den Sophos Connect-Client und dann den Sophos SSL VPN-Client installiert.

Maßnahme: Deinstallieren Sie beide Clients. Installieren Sie zuerst den Sophos SSL VPN-Client und dann den Sophos Connect-Client.

Hinweis
Die Clients müssen in dieser Reihenfolge installiert werden.

Anfrage zum Zurücksetzen der Verbindung vom Gateway empfangen: <Gateway-Name>

Diese Meldung wird in der Datei `scvpn.log` im Installationsordner protokolliert.

Ursache: SSL VPN-Einstellungen werden an der XG Firewall geändert, ein Benutzer wird manuell getrennt oder die XG Firewall wird neu gestartet. Wenn die Verbindung SSL VPN über TCP verwendet, sendet die XG Firewall eine Anfrage zum Zurücksetzen der Verbindung. Wenn die Verbindung SSL VPN über UDP verwendet, kann es sein, dass die Verbindung je nach Leerlaufzeit automatisch wieder hergestellt wird.

Maßnahme: Importieren Sie eine neue Konfigurationsdatei in den Sophos Connect-Client und stellen Sie dann die Verbindung wieder her. Wenn Ihnen der Administrator die Datei nicht gesendet hat, rufen Sie das Benutzerportal auf und laden Sie sie herunter. Andernfalls rufen Sie das Benutzerportal auf und laden Sie die `ovpn`-Datei herunter.

Bei der SSL VPN-Verbindung sind die Menüelemente für die automatische Verbindung und Aktualisierung der Richtlinie ausgegraut.

Ursache: Wenn die SSL VPN-Verbindung durch Importieren einer `ovpn`-Datei erstellt wird, sind diese Optionen nicht verfügbar.

Maßnahme: Um diese Optionen zu aktivieren, müssen Sie eine Verbindung mit einer Bereitstellungsdatei erstellen. Fügen Sie diese Optionen zur Bereitstellungsdatei hinzu. **Richtlinie aktualisieren** ist verfügbar, nachdem Sie die erste Verbindung hergestellt haben. Um **Automatisch verbinden** zu aktivieren, müssen Sie einen `Auto_Connect_Host` definieren, auf den nur im internen Netzwerk zugegriffen werden kann.

Beispiel für eine Bereitstellungsdatei mit Mindestanforderungen für die Aktivierung der automatischen Verbindung:

```
[
 {
```

```
  "display_name": "<Verbindungsname eingeben>",
  "gateway": "<Gateway-Hostname oder IP eingeben>",
  "auto_connect_host":" <Hostname oder IP der internen Netzwerkressource
 eingeben>"
 }
]
```

SSL VPN-Fehler

Ursache: Ein vom OpenVPN-Dienst generierter Fehler.

Maßnahme: Stellen Sie die Verbindung wieder her. Wenn dies nicht funktioniert, starten Sie das Gerät neu und versuchen Sie es erneut.

Management-Port ist nicht verfügbar

Ursache: Sophos Connect kann den TCP-Port 25340 nicht anfordern, der für die Kommunikation mit OpenVPN erforderlich ist.

Maßnahme: Überprüfen Sie, ob auf dem Gerät, das diesen Port verwendet, eine andere Anwendung ausgeführt wird. Beenden Sie die Anwendung, wenn möglich. Wenn Sie dieses Problem nicht beheben, kann Sophos Connect 2.0 nicht auf Ihrem Gerät ausgeführt werden. Wenn keine andere Anwendung diesen Port verwendet, kann dies ein vorübergehendes Problem sein. Das Problem sollte durch erneutes Herstellen der Verbindung behoben sein.

Temporäre Datei konnte nicht erstellt werden

Ursache: Sophos Connect verwendet eine temporäre Datei, um die Verbindungsattribute an den OpenVPN-Dienst zu übergeben. Sophos Connect konnte die Datei auf diesem Gerät nicht erstellen.

Maßnahme: Starten Sie das Gerät neu.

Der OpenVPN-Dienst ist nicht verfügbar

Ursache: Der OpenVPN-Dienst wurde möglicherweise nicht gestartet.

Maßnahme: Wenn der Starttyp des OpenVPN-Dienstes auf **deaktiviert** gesetzt ist, ändern Sie ihn auf **manuell** und starten Sie den Sophos Connect-Dienst neu.

Schreiben in Pipe fehlgeschlagen

Ursache: Vom Sophos Connect-Client wurde ein Fehler generiert.

Maßnahme: Stellen Sie die Verbindung wieder her. Wenn dies nicht funktioniert, starten Sie das Gerät neu und versuchen Sie es erneut.

2 Über Sophos Connect Admin

In Sophos Connect Admin können Sie Konfigurationsdateien (`.tgb`) importieren und verschiedene Optionen für Ihr VPN-Setup konfigurieren.

Hinweis
Informationen zum Konfigurieren und Exportieren einer tgb-Datei auf der XG finden Sie im Abschnitt Sophos Connect Client der XG-Hilfe: Sophos Connect Client.

Die Installations- und Deinstallationsprozesse für Sophos Connect Admin sind mit den Prozessen für Sophos Connect identisch. Weitere Informationen finden Sie unter Installation in der Sophos Connect-Hilfe.

2.1 Bearbeiten von Konfigurationsdateien

Sie können Ihre Konfigurationsdateien (`.tgb`) in Sophos Connect Admin bearbeiten. Dort stehen Ihnen granularere VPN-Konfigurationsoptionen zur Verfügung.

Öffnen Sie die `.tgb`-Datei, die Sie aus der XG zu Sophos Admin exportiert haben. Sie haben folgende Möglichkeiten:

- Aktivieren Sie **Alles tunneln**, um den gesamten Datenverkehr über die VPN-Verbindung zu senden.
- Aktivieren Sie **Security Heartbeat senden**, damit Sophos Endpoint einen Heartbeat an die XG senden kann. Dies funktioniert nur, wenn der Benutzer den Sophos Endpoint-Client auf seinem Computer installiert hat.
- Aktivieren Sie **Kennwort speichern zulassen**, damit Benutzer ihren Benutzernamen und ihr Kennwort auf ihrem Computer speichern können. Die Anmeldeinformationen des Benutzers werden mithilfe von Schlüsselbund-Diensten sicher gespeichert.
- Aktivieren Sie die **Eingabeaufforderung für 2FA**, wenn Sie die Zwei-Faktor-Authentifizierung für die VPN-Benutzer auf der XG konfiguriert haben.
- Aktivieren Sie **Tunnel automatisch verbinden**, um die Verbindung automatisch zu aktivieren, nachdem sich der Benutzer auf seinem Computer bei Sophos Connect angemeldet hat. Sophos Connect initiiert die Verbindung nicht automatisch, wenn der Benutzer bereits mit dem Firmennetzwerk verbunden ist.

  Für die automatische Verbindung ist ein zusätzlicher Konfigurationsparameter erforderlich: **DNS Suffix/Monitoring Host**, der verwendet werden kann, um festzustellen, ob sich das lokale System des Benutzers innerhalb oder außerhalb des Unternehmensnetzwerks befindet. Verwenden Sie einen der folgenden Werte:

  — Eine IP-Adresse.

  — Einen vollständigen Domainnamen (FQDN). Der Hostname darf nur aufgelöst werden, wenn der interne DNS-Server verwendet wird.

  — Ein DNS-Suffix.

Hinweis
Wenn Sie eine IP-Adresse oder einen FQDN konfigurieren, muss ICMP auf diesem Host zugelassen sein.

- Sie können **Netzwerke** hinzufügen, ändern und löschen, zu denen der Benutzer eine Verbindung herstellen kann. Das Hinzufügen bestimmter Netzwerke zur Liste ermöglicht Split Tunneling, da der Benutzer über die VPN-Verbindung auf Ressourcen in diesen Netzwerken zugreifen kann, aber direkt über sein Remote-Gateway auf Internetressourcen zugreift.

  Hinweis
  Wenn Sie alle Netzwerke löschen, wird **Alles tunneln** aktiviert, d. h. der gesamte Datenverkehr wird über die VPN-Verbindung geleitet.

- Ändern Sie den **Verbindungsnamen** und den **Zielhost**.

  Wenn Sie die Konfiguration **löschen**, müssen Sie die `.tbg`-Datei erneut importieren.

  Wenn Sie die Konfiguration **speichern**, wird sie als `.scx`-Datei gespeichert.

  Hinweis
  Sie können `.scx`-Dateien importieren und erneut bearbeiten.

Wenn Sie die Konfigurationsdatei gespeichert haben, können Sie sie an den Benutzer senden, der sie in Sophos Connect importiert. Weitere Informationen finden Sie unter Sophos Connect.

3 Rechtliche Hinweise