

Fehler beim sicheren Zugriff "Die VPN-Verbindung wurde von einem Remotedesktop-Benutzer gestartet, dessen Remote-Konsole getrennt wurde"

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

[Zugehörige Informationen](#)

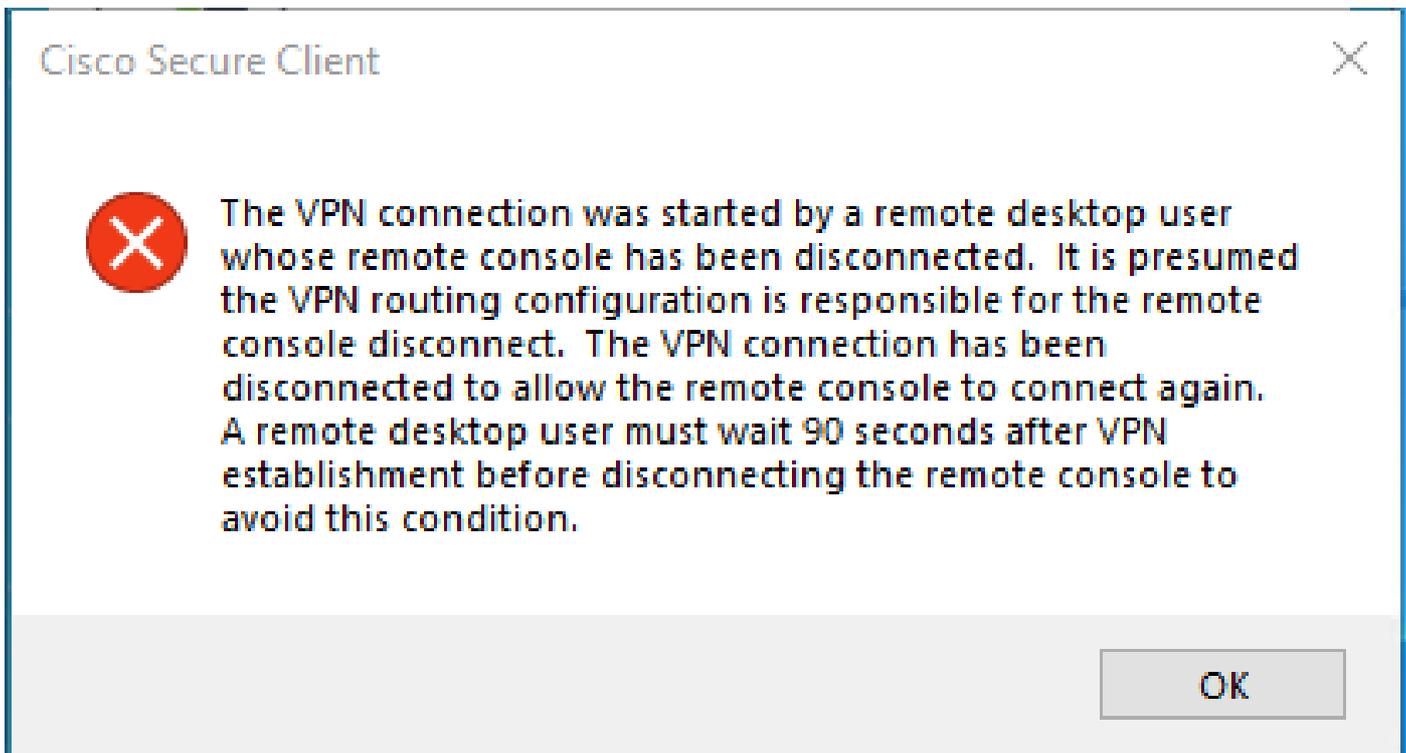
Einleitung

In diesem Dokument wird beschrieben, wie Sie den Fehler beheben: "Die VPN-Verbindung wurde von einem Remote-Desktop-Benutzer gestartet, dessen Remote-Konsole getrennt wurde."

Problem

Wenn ein Benutzer versucht, eine Verbindung mit RA-VPN (Remote Access VPN) zum Secure Access-Headend herzustellen, wird der Fehler im Benachrichtigungs-Popup-Fenster von Cisco Secure Client angezeigt:

- The VPN connection was started by a remote desktop user whose remote console has been disconnected. It is presumed the VPN routing configuration is responsible for the remote console disconnect. The VPN connection has been disconnected to allow the remote console to connect again. A remote desktop user must wait 90 seconds after VPN establishment before disconnecting the remote console to avoid this condition.



Der genannte Fehler wird generiert, wenn der Benutzer über das RDP mit dem Windows-PC verbunden ist, versucht, eine Verbindung zum RDP-VPN vom angegebenen PC herzustellen, und Tunnel Mode im VPN-Profil auf festgelegt ist **Connect to Secure Access (default option)** und die Quell-IP-Adresse der RDP-Verbindung nicht zu Ausnahmen hinzugefügt wird.

Für **Traffic Steering (Split Tunnel)** können Sie ein VPN-Profil konfigurieren, um eine vollständige Tunnelverbindung zu sicherem Zugriff aufrechtzuerhalten, oder das Profil so konfigurieren, dass es eine Split-Tunnel-Verbindung verwendet, um den Datenverkehr nur bei Bedarf durch das VPN zu leiten.

- Wählen Sie für **Tunnel Mode** eine der folgenden Optionen:
 - **Connect to Secure Access** den gesamten Verkehr durch den Tunnel zu leiten oder
 - **Bypass Secure Access** um den gesamten Verkehr außerhalb des Tunnels zu leiten.
- Je nach Ihrer Auswahl können Sie den Verkehr innerhalb oder außerhalb des Tunnels **Add Exceptions** steuern. Sie können durch Kommata getrennte IPs, Domänen und Netzwerkbereiche eingeben.

Lösung

Rufen Sie das Cisco Secure Access Dashboard auf:

- Klicken Sie **Connect > End User Connectivity**

- Klicken Sie Virtual Private Network
- Wählen Sie das zu ändernde Profil aus, und klicken Sie auf **Edit**

VPN Profiles
A VPN profile allows for configuration of remote user connections through a VPN. [Help](#)

Q Search + Add

name	General	Authentication	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
...iVPNprofile	sspt: ...ft.com TLS, IKEv2	SAML	Connect to Secure Access 2 Exception(s)	13 Settings	6f1...iVPNprofile	

Edit
 Duplicate
 Delete

- Klicken Sie **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**

General settings
Default Domain: sspt: ...ft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2

Authentication
SAML

3 Traffic Steering (Split Tunnel)
Connect to Secure Access | 2 Exceptions

Cisco Secure Client Configuration

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#)

Tunnel Mode
Connect to Secure Access

All traffic is steered through the tunnel.

Add Exceptions
Destinations specified here will be steered OUTSIDE the tunnel. + Add

Destinations	Exclude Destinations	Actions
proxy-8...3.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sseposture-routing-commercial.posture.duosecure	-	-

Cancel Back Next

- Fügen Sie die IP-Adresse hinzu, von der Sie die RDP-Verbindung hergestellt haben.

Add Destinations

Comma seperated IPs, domains, and network spaces

Cancel

Save

- Klicken Sie auf **Save** Im **Add Destinations** Fenster

TCP	127.0.0.1:62722	0.0.0.0:0	LISTENING
TCP	127.0.0.1:62722	127.0.0.1:49794	ESTABLISHED
TCP	172.30.1.7:139	0.0.0.0:0	LISTENING
TCP	172.30.1.7:3389	185.15[REDACTED]:12974	ESTABLISHED
TCP	172.30.1.7:49687	52.16.166.193:443	ESTABLISHED
TCP	172.30.1.7:49745	20.42.72.131:443	TIME_WAIT
TCP	172.30.1.7:49755	40.113.110.67:443	ESTABLISHED
TCP	172.30.1.7:49757	23.212.221.139:80	ESTABLISHED
TCP	172.30.1.7:49758	23.48.15.164:443	ESTABLISHED



Hinweis: Die IP-Adresse kann aus der Ausgabe des Befehls `cmd` ermittelt werden. **netstat -an**; Beachten Sie die IP-Adresse, von der eine Verbindung zur lokalen IP-Adresse des Remote-Desktops zu Port 3389 besteht.

-
- Klicken Sie **Next** nach dem Hinzufügen der Ausnahme auf:

- ✓ **General settings**
Default Domain: ssp[redacted]oft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2
- ✓ **Authentication**
SAML
- 3 Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. [Help](#)

Tunnel Mode

Connect to Secure Access

All traffic is steered through the tunnel.

Add Exceptions + Add

Destinations specified here will be steered OUTSIDE the tunnel.

Destinations	Exclude Destinations	Actions
185.15[redacted]/32	+ Add	...
proxy-8179183.zpc.sse.cisco.com, ztna.sse.cisco.com, acme.sse.cisco.com, devices.api.umbrella.com, sseposture-routing-commercial.k8s.5c10.org, sse		

Cancel
Back
Next

- Klicken Sie auf **Save** Änderungen im VPN-Profil:

- ✓ **General settings**
Default Domain: ssp[redacted]oft.com | DNS Server: UmbrellaDNS2 (208.67.222.222, 208.67.220.220) | Protocol: TLS / DTLS, IKEv2
- ✓ **Authentication**
SAML
- ✓ **Traffic Steering (Split Tunnel)**
Connect to Secure Access | 2 Exceptions
- 4 Cisco Secure Client Configuration**

Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings 3
Client Settings 13
Client Certificate Settings 4
Download XML

Banner Message

Require user to accept a banner message post authentication

Session Timeout

days

Session Timeout Alert

minutes before

Maximum Transmission Unit ⓘ

Cancel
Back
Save

Zugehörige Informationen

-

[VPN-Profil hinzufügen](#)

- [Secure Access - Benutzerhandbuch](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.