

Risoluzione dei problemi relativi a errore accesso sicuro "La connessione VPN è stata avviata da un utente di Desktop remoto la cui console remota è stata disconnessa"

Sommario

[Introduzione](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

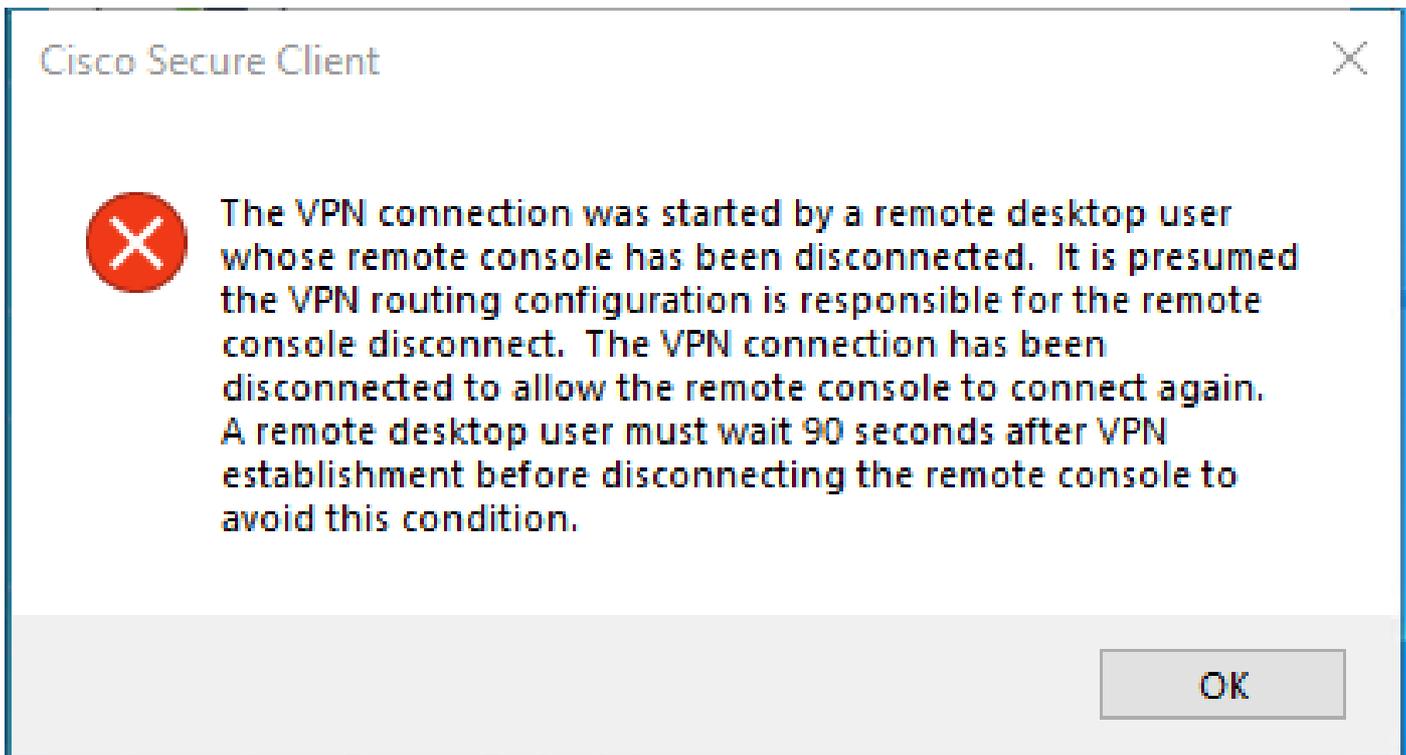
Introduzione

In questo documento viene descritto come correggere l'errore: "La connessione VPN è stata avviata da un utente desktop remoto la cui console remota è stata disconnessa".

Problema

Quando un utente tenta di connettersi all'headend di Secure Access tramite una VPN ad accesso remoto (RA-VPN), l'errore viene stampato nel popup di notifica di Cisco Secure Client:

- 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.



L'errore indicato viene generato quando l'utente è connesso tramite RDP al PC Windows, tenta di connettersi a RA-VPN dal PC specificato e Tunnel Mode in Profilo VPN è impostato su **Connect to Secure Access (default option)** e l'indirizzo IP di origine della connessione RDP non viene aggiunto a Eccezioni.

Ad esempio, **Traffic Steering (Split Tunnel)** è possibile configurare un profilo VPN per mantenere una connessione tunnel completa ad Accesso sicuro oppure configurare il profilo in modo che utilizzi una connessione tunnel divisa per indirizzare il traffico attraverso la VPN solo se necessario.

- Per **Tunnel Mode**, scegliere:
 - **Connect to Secure Access** dirigere tutto il traffico attraverso la galleria; oppure
 - **Bypass Secure Access** per indirizzare tutto il traffico all'esterno del tunnel.
- A seconda della selezione effettuata, è possibile indirizzare **Add Exceptions** il traffico all'interno o all'esterno del tunnel. È possibile immettere indirizzi IP, domini e spazi di rete separati da virgole.

Soluzione

Passare al Cisco Secure Access Dashboard:

- Fare clic su **Connect > End User Connectivity**

- Fare clic su Virtual Private Network
- Scegliere il profilo da modificare e fare clic su **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

- Fare clic su **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

- Aggiungere l'indirizzo IP da cui è stata stabilita la connessione RDP

Add Destinations

Comma separated IPs, domains, and network spaces

Cancel

Save

- Fare clic su **Save** In **Add Destinations** window

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



Nota: l'indirizzo IP può essere trovato dall'output del comando **netstat -ancmd.**; Notare l'indirizzo IP da cui è stata stabilita una connessione all'indirizzo IP locale del desktop remoto alla porta 3389.

-
- Fare clic su **Next** dopo aver aggiunto l'eccezione:

- 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

- Fare clic su **Save Changes** (Modifiche) nel profilo VPN:

- 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

-

[Aggiungi profili VPN](#)

- [Guida per l'utente di Secure Access](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).