對安全訪問錯誤進行故障排除"；VPN連線由遠端控制檯已斷開連線的遠端案頭使用者啟動"；

目錄

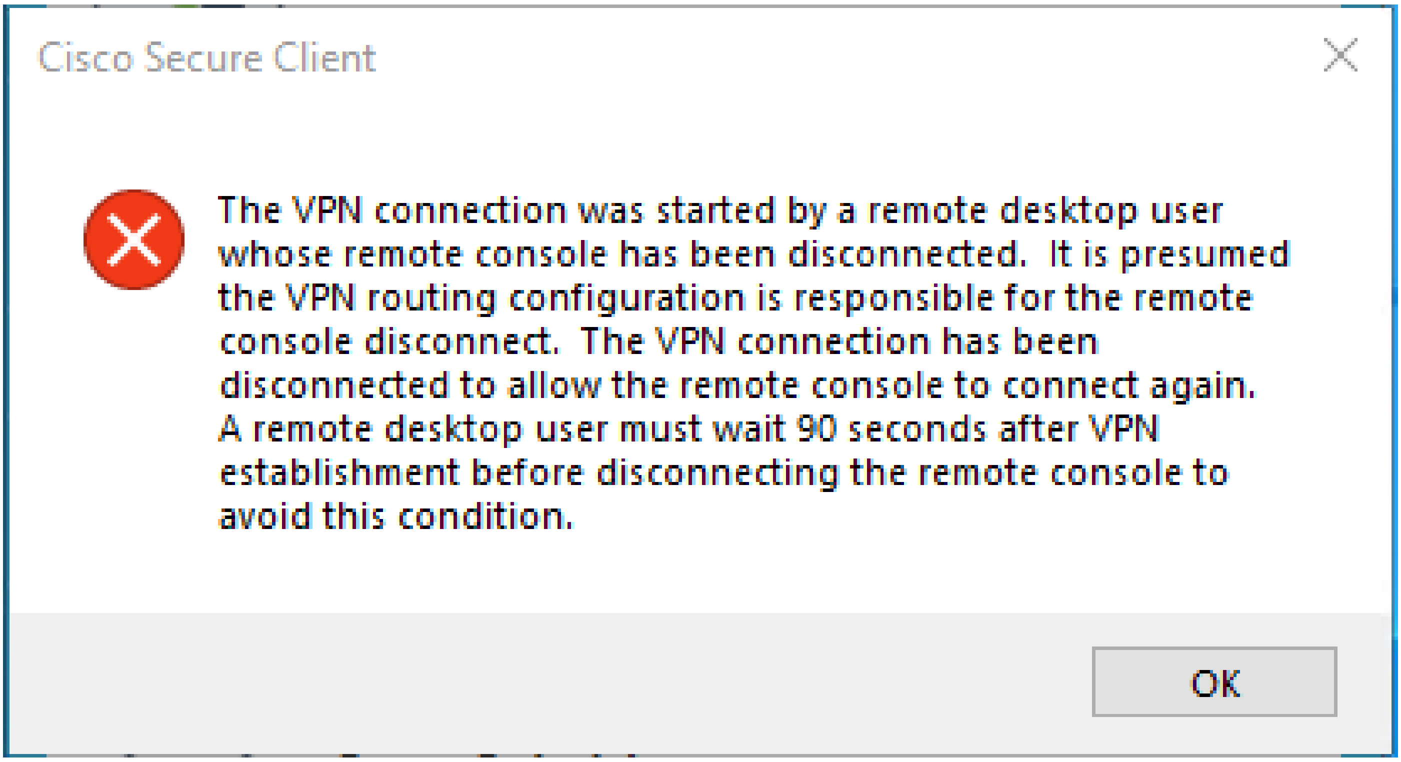
簡介

本文檔介紹如何修復錯誤：「VPN連線由遠端控制檯已斷開連線的遠端案頭使用者啟動」。

問題

當使用者嘗試透過RA-VPN（遠端接入VPN）連線到安全接入頭端時，會在Cisco Secure Client通知彈出窗口中顯示以下錯誤：

- 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.



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.

當使用者透過RDP連線到Windows PC，嘗試從給定的PC連線到RA-VPN，並且VPN配置檔案中的Tunnel Mode設定為 **Connect to Secure Access (default option)** 且RDP連線的源IP未增加到「例外」時，將生成上述錯誤。

對於 **Traffic Steering (Split Tunnel)**，您可以配置VPN配置檔案以維護到安全訪問的完整隧道連線，或配置配置檔案以使用分割隧道連線，僅在必要時引導資料流透過VPN。

- 對於**Tunnel Mode**，請選擇以下任一項：
  - **Connect to Secure Access** 透過隧道轉發所有流量；或者，
    - **Bypass Secure Access** 將所有流量引向隧道外部。

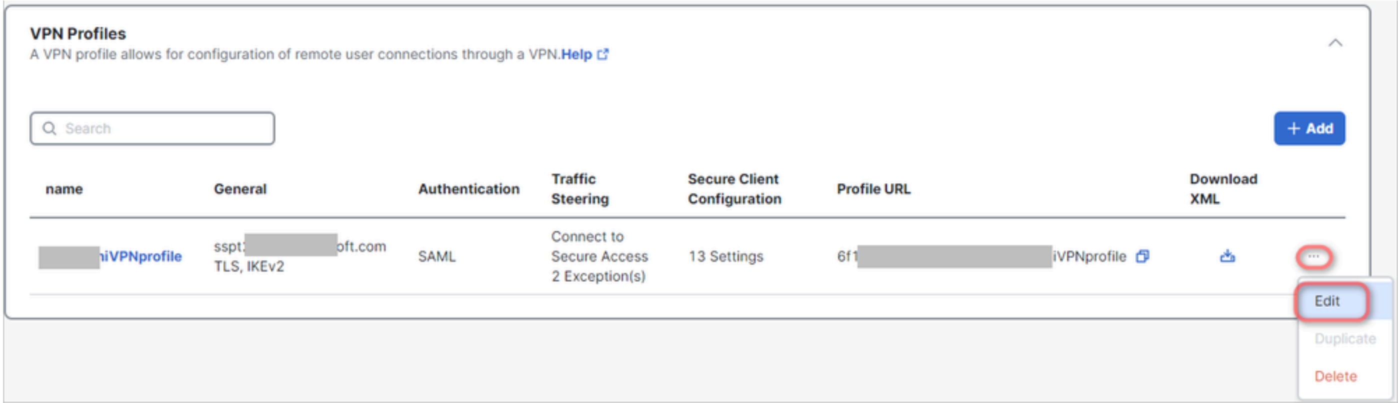
- 根據您的選擇，您可以**Add Exceptions** 控制隧道內部或外部的流量。您可以輸入逗號分隔的IP、域和網路空間。

解決方案

導航到Cisco Secure Access Dashboard：

- 按一下 **Connect** > **End User Connectivity**
- 按一下 Virtual Private Network

- 選擇要修改的設定檔，然後按一下 **Edit**



VPN Profiles

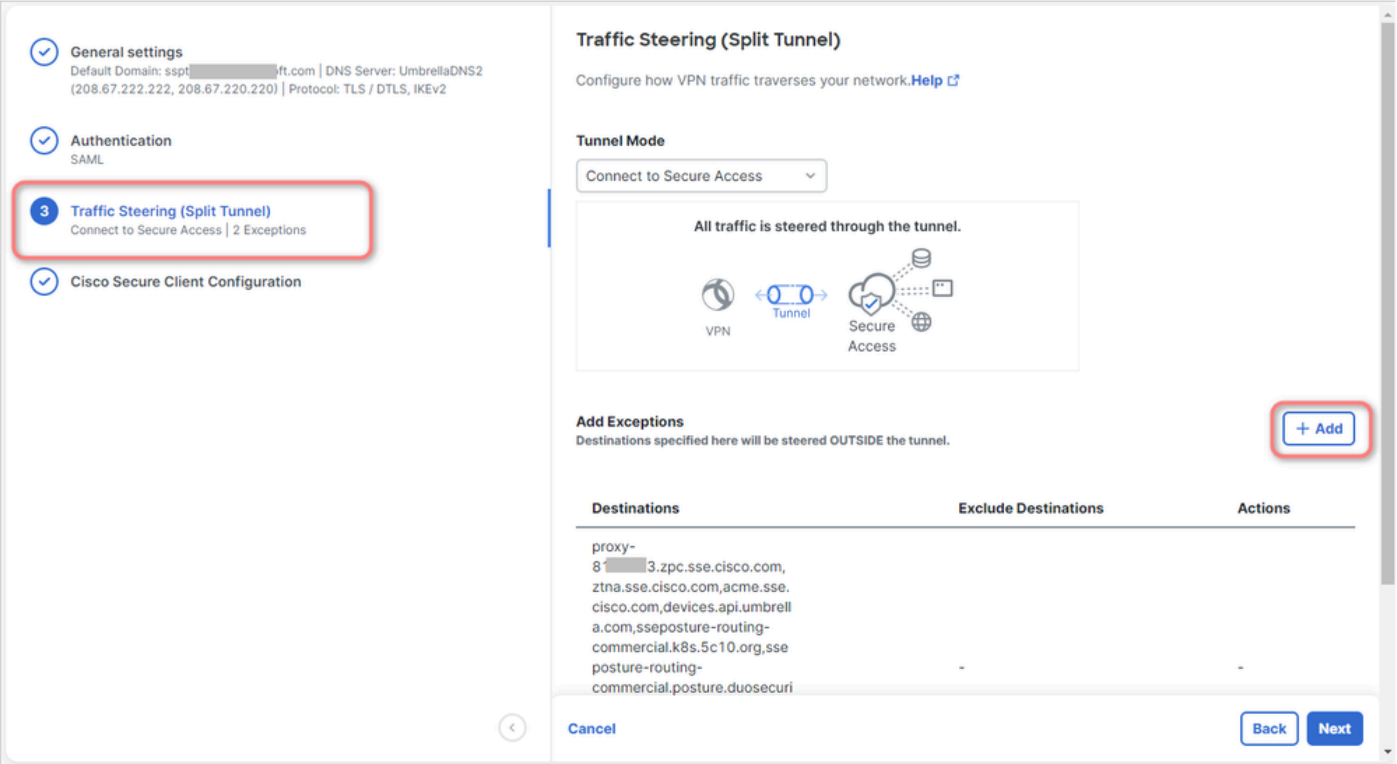
A VPN profile allows for configuration of remote user connections through a VPN. Help

Search

+ Add

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

- 按一下 **Traffic Steering (Split Tunnel) > Add Exceptions > + Add**



General settings
Default Domain: sspt[redacted]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.

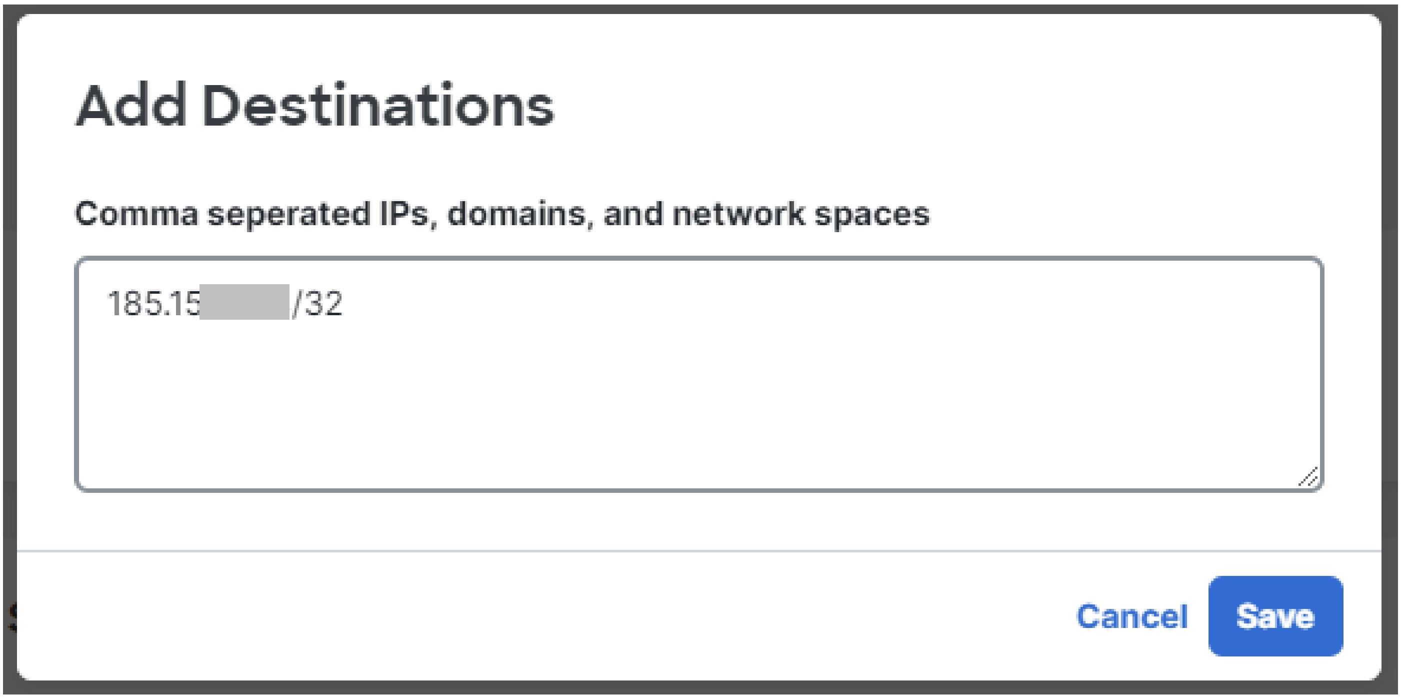
Add Exceptions

Destinations specified here will be steered OUTSIDE the tunnel.

+ Add

Destinations	Exclude Destinations	Actions
proxy-8[redacted]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.duosecuri	-	-

- 增加用於建立RDP連線的IP地址

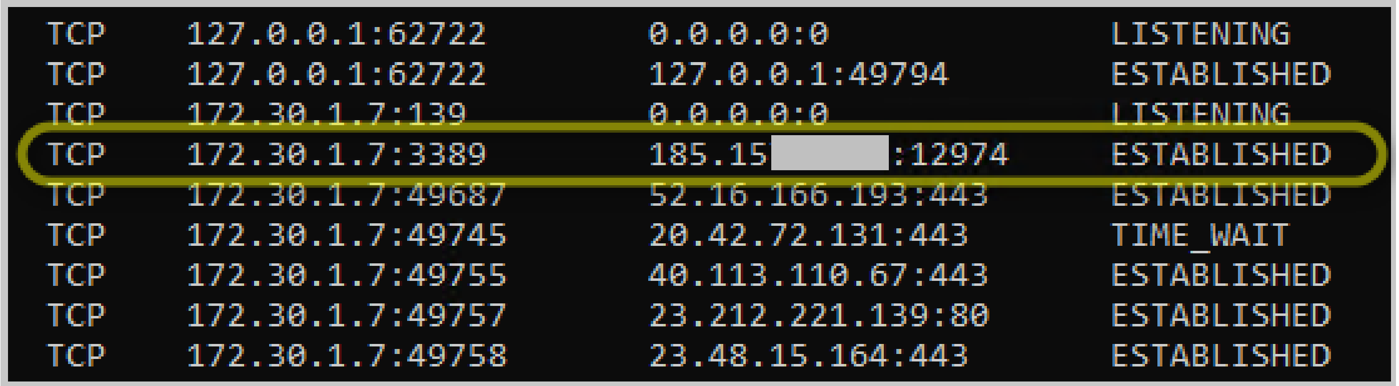


Add Destinations

Comma seperated IPs, domains, and network spaces

185.15[redacted]/32

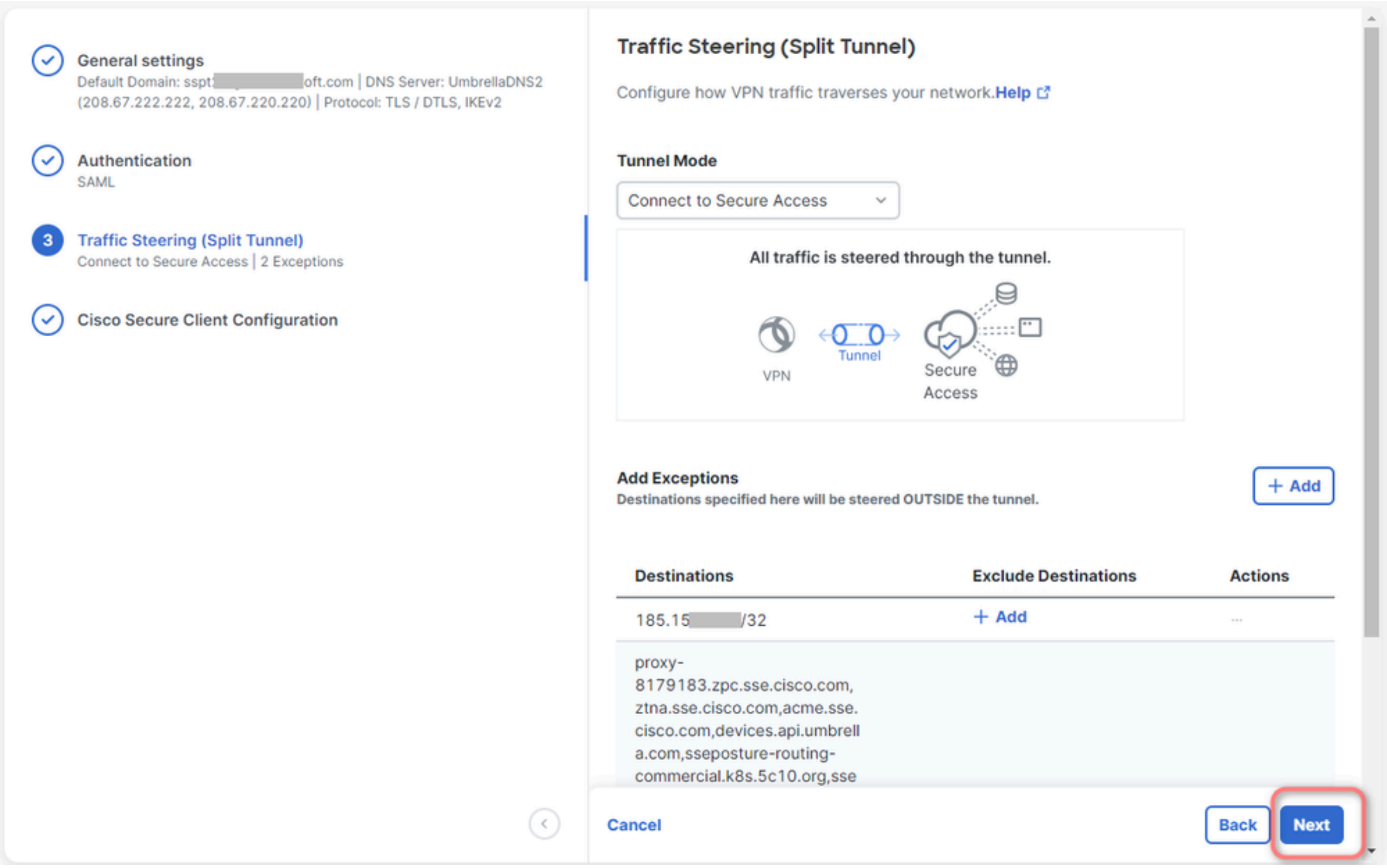
- 按一下**Save** 在 **Add Destinations** 視窗中



```
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
```

注意：可以從cmd命令 **netstat -an**的輸出中找到IP地址。注意IP地址，從該地址到埠3389的遠端案頭本地IP地址已建立連線。

- 新增例外後 **Next** 按一下：



General settings
Default Domain: sspt[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

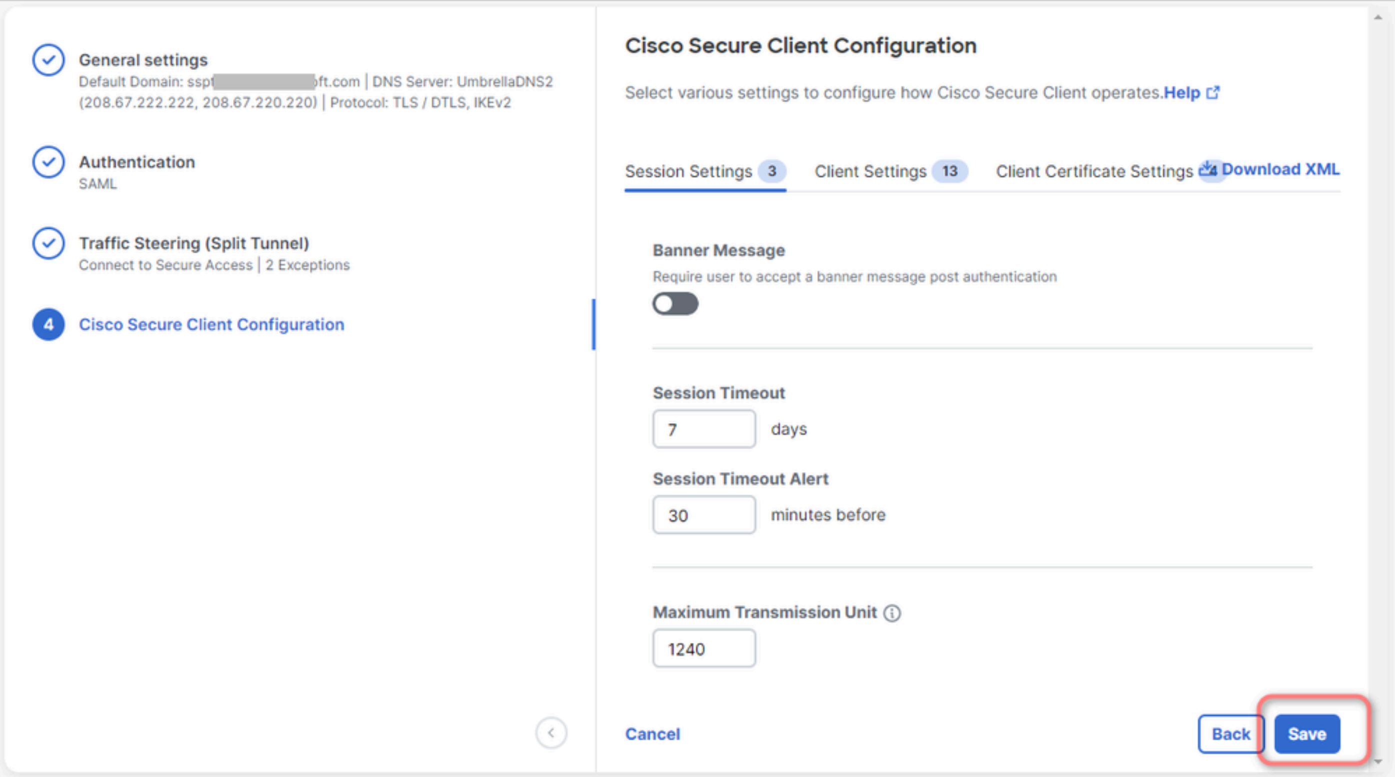
Connect to Secure Access

All traffic is steered through the tunnel.

Add Exceptions
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		

- 按一下VPN配置檔案中的 **Save** 更改：



General settings
Default Domain: sspt[redacted]ft.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

Banner Message
Require user to accept a banner message post authentication

Session Timeout
7 days

Session Timeout Alert
30 minutes before

Maximum Transmission Unit
1240

相關資訊

-

增加VPN配置檔案

- 安全訪問使用手冊
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。