Troubleshoot Secure Access Error "The VPN Connection Was Started by a Remote Desktop User Whose Remote Console Has Been Disconnected"

Contents

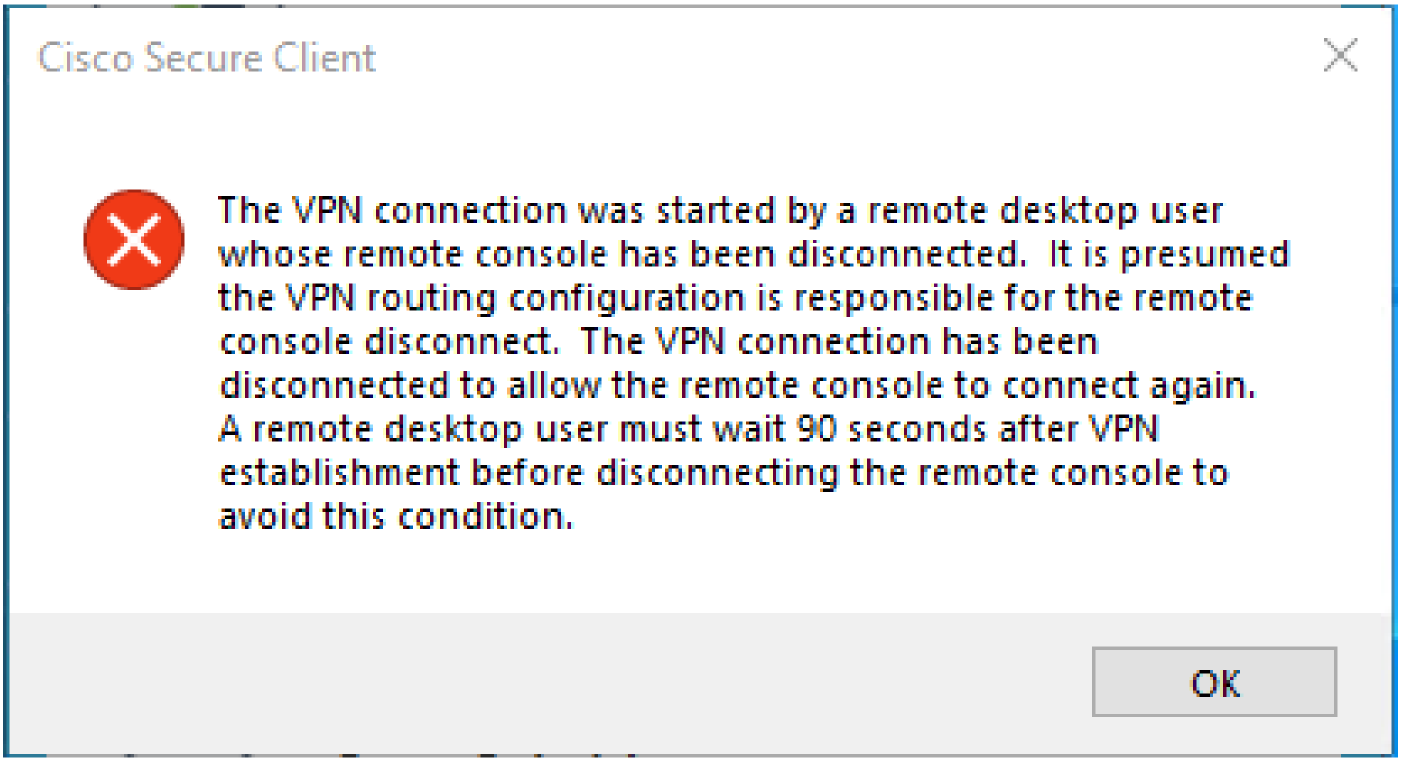
Introduction

This document describes how to fix the error: "The VPN connection was started by a remote desktop user whose remote console has been disconnected".

Problem

When a user tries to connect with RA-VPN (Remote Access VPN) to the Secure Access headend, the error is printed in the Cisco Secure Client notification popup:

- 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.

The mentioned error is generated when the user is connected via the RDP to the Windows PC, tries to connect to RA-VPN from the given PC, and Tunnel Mode in VPN Profile is set to **Connect to Secure Access (default option)** and source IP of the RDP connection is not added to Exceptions.

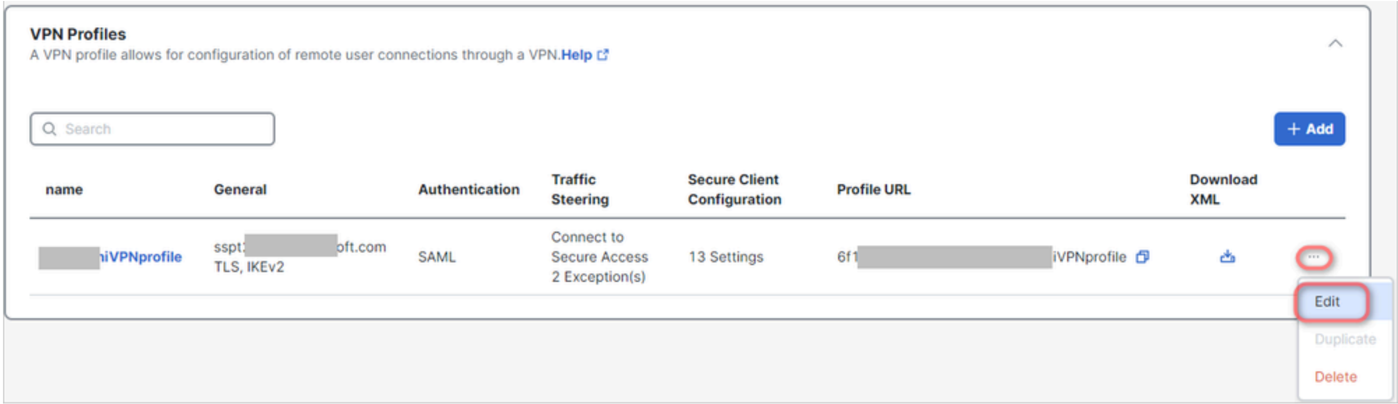
For **Traffic Steering (Split Tunnel)**, you can configure a VPN profile to maintain a full tunnel connection to Secure Access or configure the profile to use a split tunnel connection to direct traffic through the VPN only if necessary.

1. For **Tunnel Mode**, choose either:
   - **Connect to Secure Access** to direct all traffic through the tunnel; or,
   - **Bypass Secure Access** to direct all traffic outside the tunnel.
2. Depending on your selection, you can **Add Exceptions** to steer traffic inside or outside the tunnel. You can enter comma-separated IPs, domains, and network spaces.

Solution

Navigate to the Cisco Secure Access Dashboard:

- Click on **Connect** > **End User Connectivity**
- Click on Virtual Private Network
- Choose the profile that you want to modify and click **Edit**

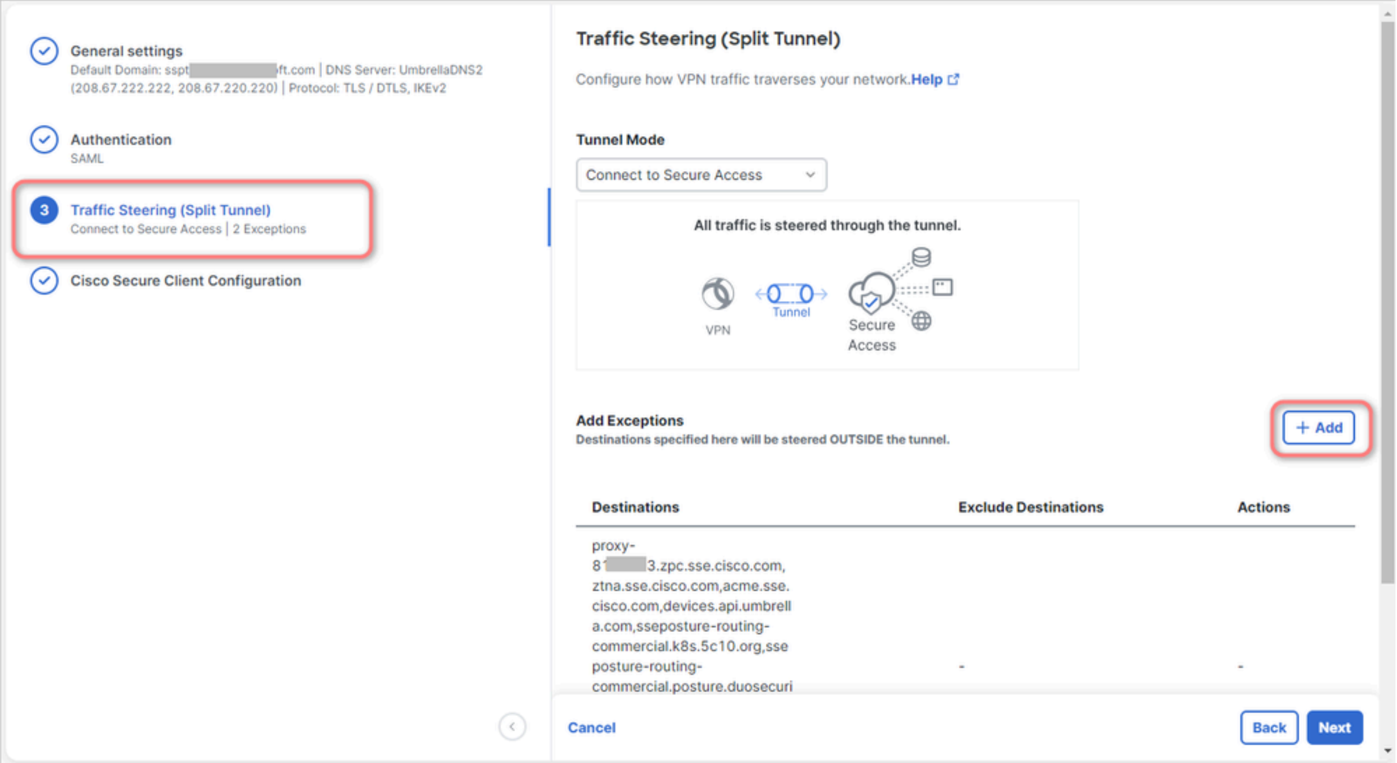


VPN Profiles

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

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	

- Click on **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

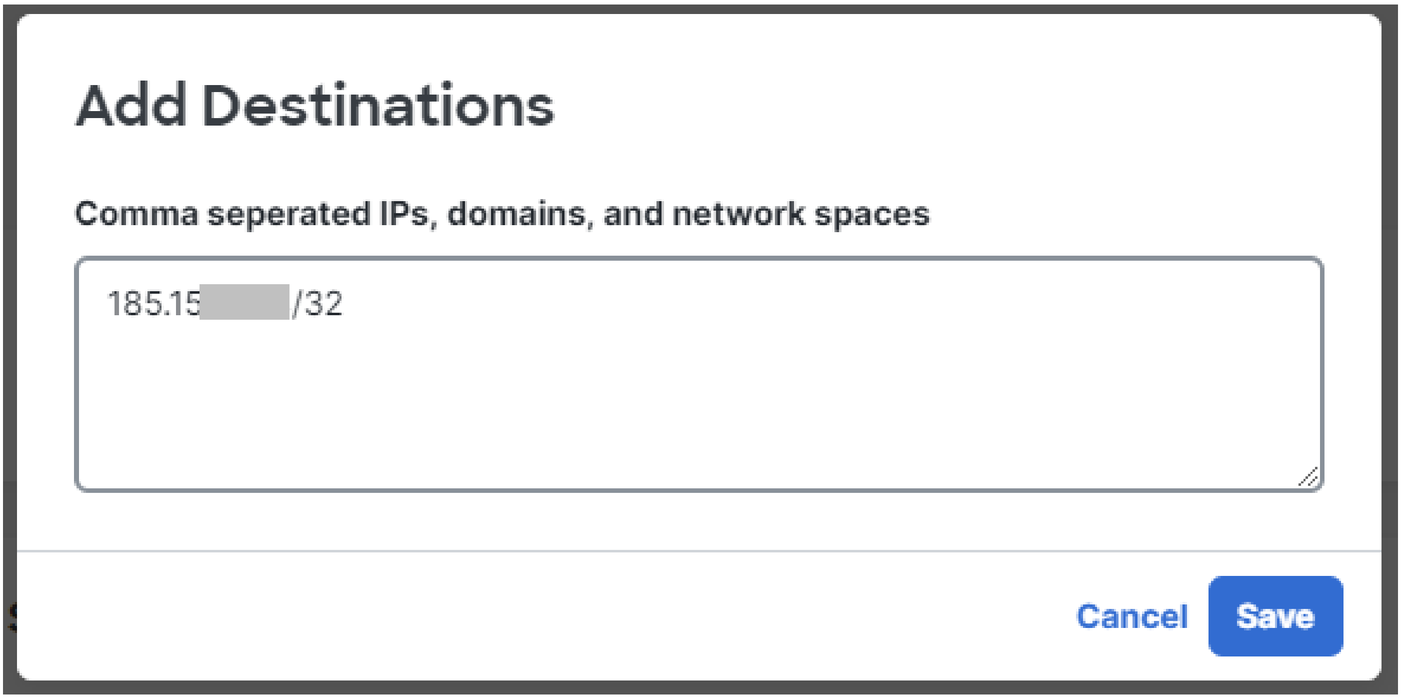
All traffic is steered through the tunnel.

Add Exceptions

Destinations specified here will be steered OUTSIDE the tunnel.

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	-	-

- Add your IP address from which you established the RDP connection

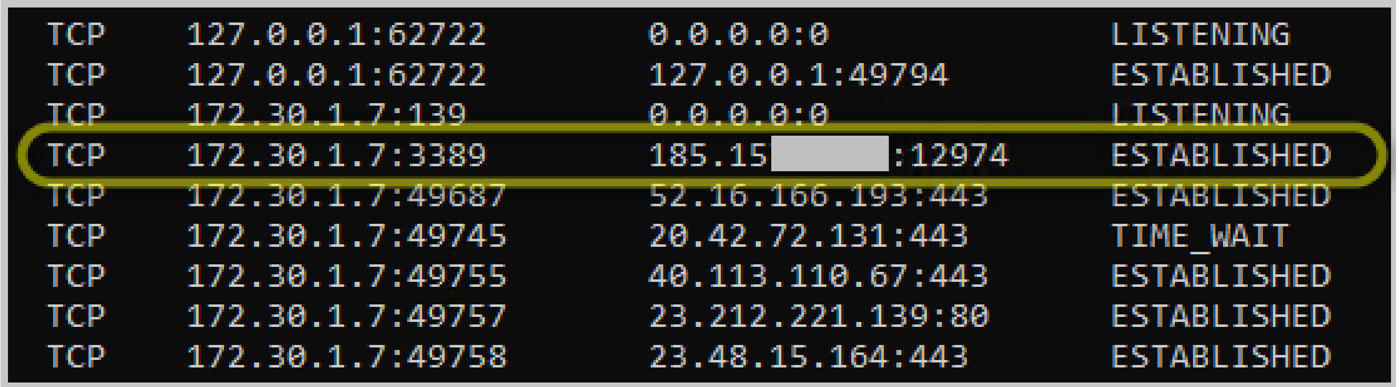


Add Destinations

Comma seperated IPs, domains, and network spaces

185.15[redacted]/32

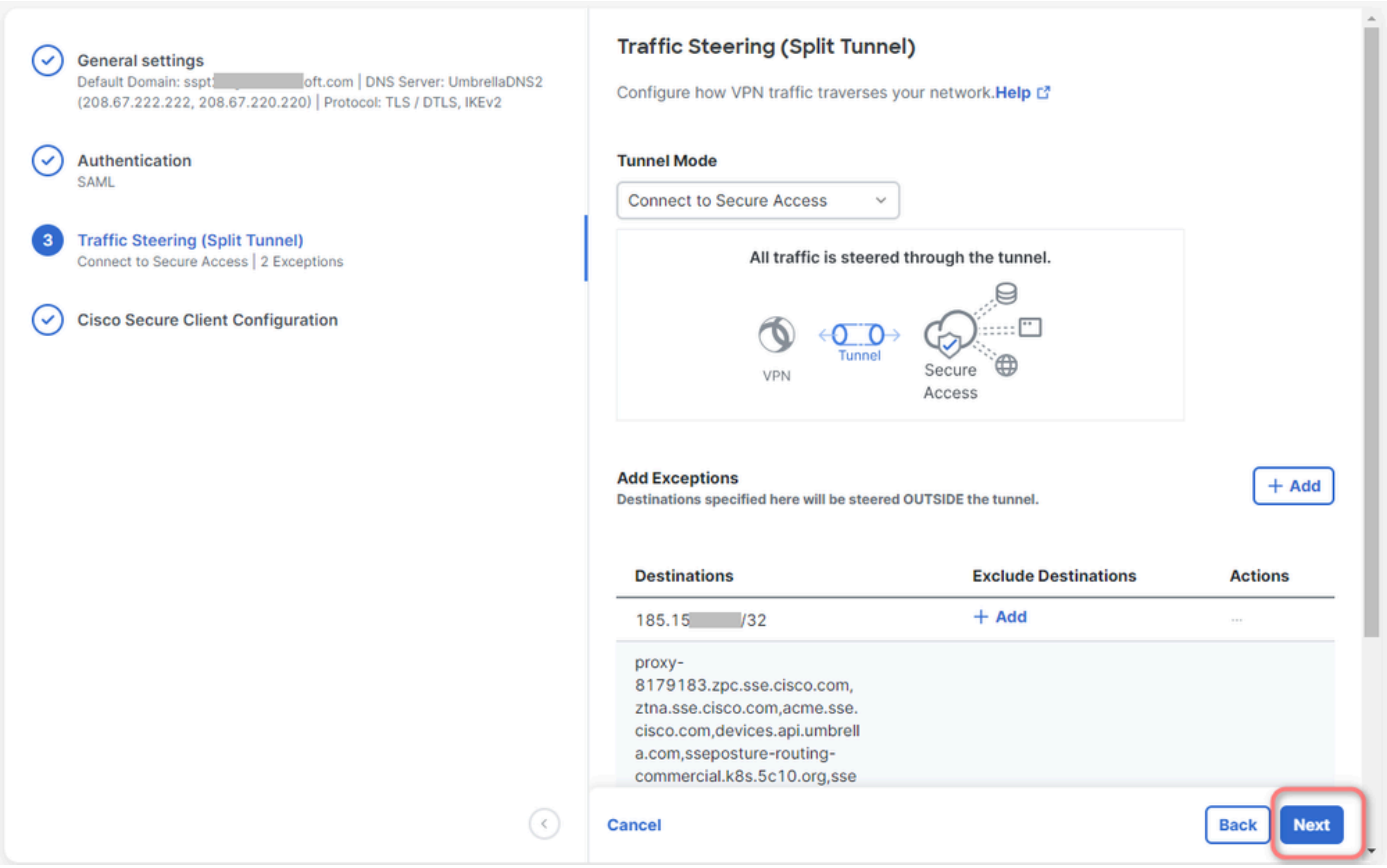
- Click on **Save** In **Add Destinations** window



```
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
```

Note: The IP address could be found from the output of cmd command **netstat -an.**; Note the IP address from which there is an established connection to the local IP address of the remote desktop to port 3389.

- Click **Next** after adding the exception:



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

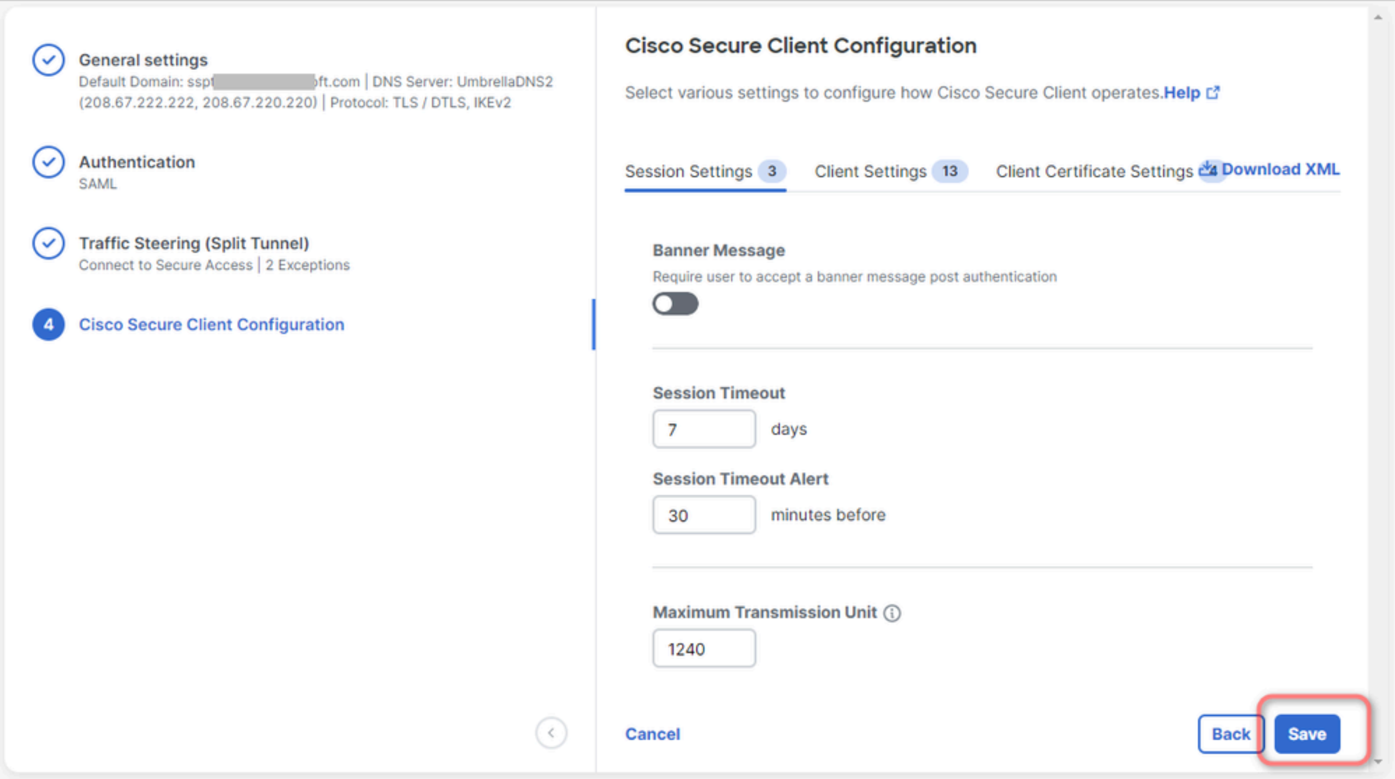
Tunnel Mode: Connect to Secure Access

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		

- Click **Save** changes in the VPN profile:



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

Related Information

- Add VPN Profiles

- Secure Access UserGuide
- Cisco Technical Support & Downloads