

Troubleshoot Secure Access Error "VPN Establishment Capability for a Remote User Is Disabled. A VPN Connection Will Not Be Established"

Contents

[Introduction](#)

[Problem](#)

[Solution](#)

[Related Information](#)

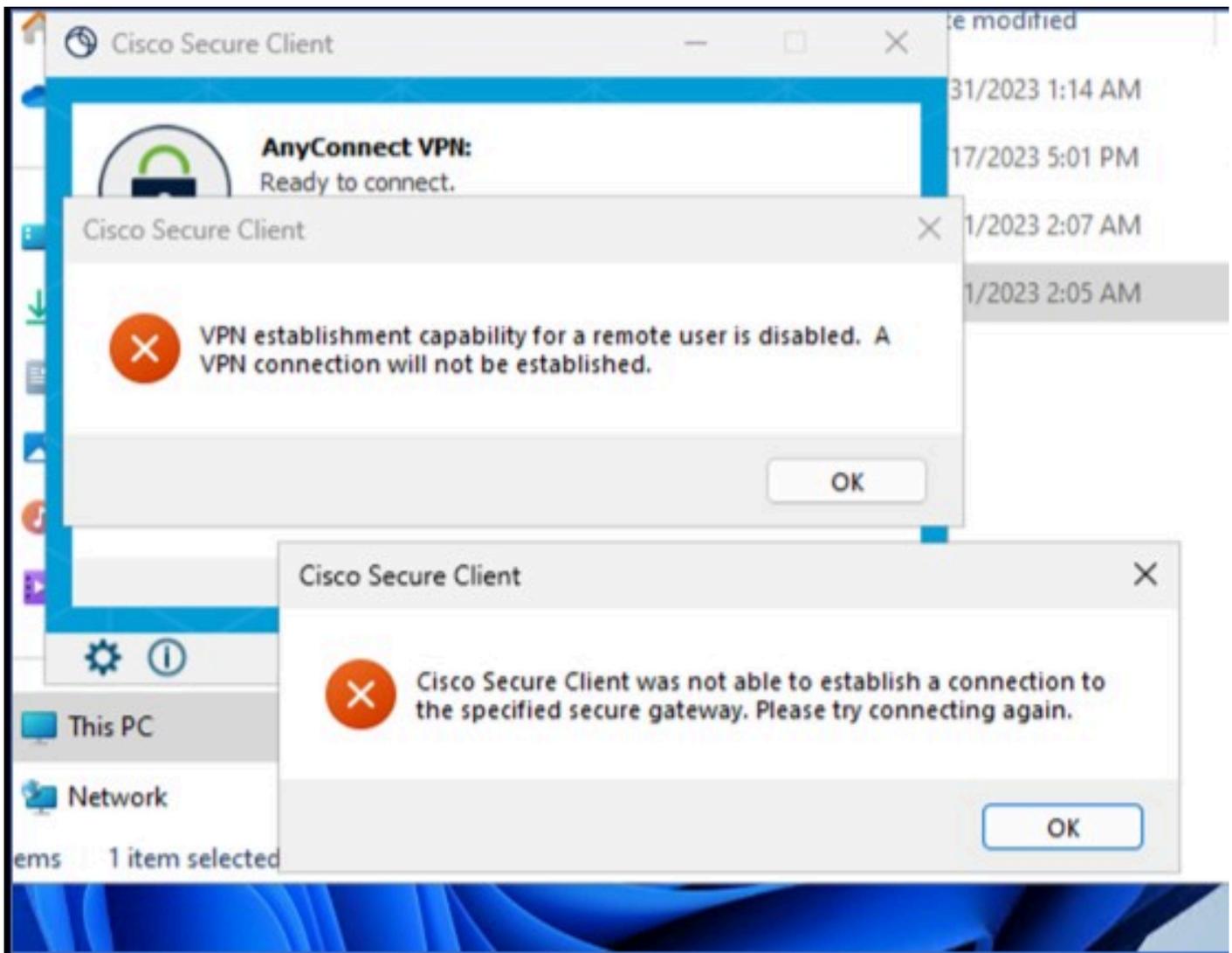
Introduction

This document describes how to resolve error: "VPN establishment capability for a remote user is disabled. A VPN connection will not be established."

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:

- **VPN establishment capability for a remote user is disabled. A VPN connection will not be established.**
- **Cisco Secure Client was not able to establish a connection to the specified secure gateway. Please try connecting again.**



Cisco Secure Client - Problem connecting to Cisco Secure Access

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 **WindowsVPN Establishment** is set to **Local Users Only** (default option).

Windows VPN Establishment determines the behavior of the Cisco Secure Client when a user who is remotely logged on to the client PC establishes a VPN connection. The possible values are:

- **Local Users Only**

Prevents a remotely logged-on (RDP) user from establishing a VPN connection.

- **Allow Remote Users**

Allows remote users to establish a VPN connection. However, if the configured VPN connection routing causes the remote user to become disconnected, the VPN connection terminates to allow the remote user to regain access to the clients PC. Remote users must wait 90 seconds after VPN establishment if they want to disconnect their remote login session without causing the VPN connection to be terminated.

Solution

Navigate to 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](#)

⚠ New Service Provider Certificate
Download the new service provider certificate and upload in your identity provider (IdP) to avoid user Authentication failures. The certificate will expire on date 11/8/2023. Download and update the certificate now from [Certificate Management](#)

Q Search + Add

name	General	Authentication	Traffic Steering	Secure Client Configuration	Profile URL	Download XML
CiscoSSPT1	ciscospt.es TLS, IKEv2	SAML	Connect to Secure Access 1 Exception(s)	12 Settings	fb57.vpn.sse.cisco.com/CiscoSSPT1	Download XML

Edit
Duplicate
Delete

Cisco Secure Access - RA-VPN

Click on **Cisco Secure Client Configuration > Client Settings > Edit**

← End User Connectivity
VPN Profile

General settings
Default Domain: ciscospt.es | DNS Server: Umbrella (208.67.222.222, 208.67.222.220) | Protocol: TLS / DTLS, IKEv2

Authentication
SAML

Traffic Steering (Split Tunnel)
Connect to Secure Access | 1 Exceptions

Cisco Secure Client Configuration

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

Session Settings **3** **Client Settings 12** Client Certificate Settings **4** [Download XML](#)

Pre Selected Settings

Use Start before Logon	Enabled
Minimize on connect	Enabled
Autoreconnect	Enabled
Windows Logon Enforcement	Single Local Logon
Linux Logon Enforcement	Single Local Logon
Windows VPN Establishment	All Remote Users
Linux VPN Establishment	Local Users Only
Clear SmartCard PIN	Enabled
IP Protocol Supported	IPv4
Proxy Settings	Native
Allow local proxy connections	Enabled
Authentication Timeout	30

Back Save

Cisco Secure Access - RA-VPN Client Configuration

Click on **Administrator Settings** and **modify** Windows VPN Establishment **from** Local User Only **to** All Remote Users

BEFORE
→
AFTER

Administrator Settings

Windows Logon Enforcement Single Local Logon	Windows VPN Establishment Local Users Only
Linux Logon Enforcement Single Local Logon	Linux VPN Establishment Local Users Only

Windows Logon Enforcement Single Local Logon	Windows VPN Establishment All Remote Users
Linux Logon Enforcement Single Local Logon	Linux VPN Establishment Local Users Only

Cisco Secure Access - Windows Windows VPN Establishment

And click on **Save**

The screenshot displays the 'Client Settings' window. At the top, there is a 'General' tab with a count of 3 and a downward arrow. Below it is the 'Administrator Settings' tab, which is expanded to show 9 settings and an upward arrow. The settings are organized into several sections:

- Windows Logon Enforcement:** A dropdown menu set to 'Single Local Logon'.
- Windows VPN Establishment:** A dropdown menu set to 'All Remote Users'.
- Linux Logon Enforcement:** A dropdown menu set to 'Single Local Logon'.
- Linux VPN Establishment:** A dropdown menu set to 'Local Users Only'.
- Clear SmartCard PIN:** A checked checkbox.
- User controllable:** An unchecked checkbox.
- IP Protocol Supported:** A dropdown menu set to 'IPv4'.
- Proxy Settings:** A dropdown menu set to 'Native'.
- Allow local proxy connections:** A checked checkbox.
- Allow optimal gateway selection:** An unchecked checkbox.
- User controllable:** An unchecked checkbox.

At the bottom right of the window, there are two buttons: 'Cancel' and 'Save'.

Cisco Secure Access - Windows Windows VPN Establishment 2

When you establish the RA-VPN session from the remote Windows PC, you must configure the **Tunnel Mode** as **Bypass Secure Access**. Otherwise, you risk losing access to the remote Windows PC.

Traffic Steering (Split Tunnel)

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

Tunnel Mode

Bypass Secure Access 

All traffic is steered outside the tunnel.



Cisco Secure Access - Tunnel Mode

For more information about Tunnel Mode check the next article item number **6**:

<https://docs.sse.cisco.com/sse-user-guide/docs/add-vpn-profiles>

Related Information

- [Secure Access UserGuide](#)
- [Cisco Technical Support & Downloads](#)