

Fehler beim sicheren Zugriff "VPN-Einrichtungsfunktion für einen Remote-Benutzer ist deaktiviert. Eine VPN-Verbindung wird nicht hergestellt"

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

[Zugehörige Informationen](#)

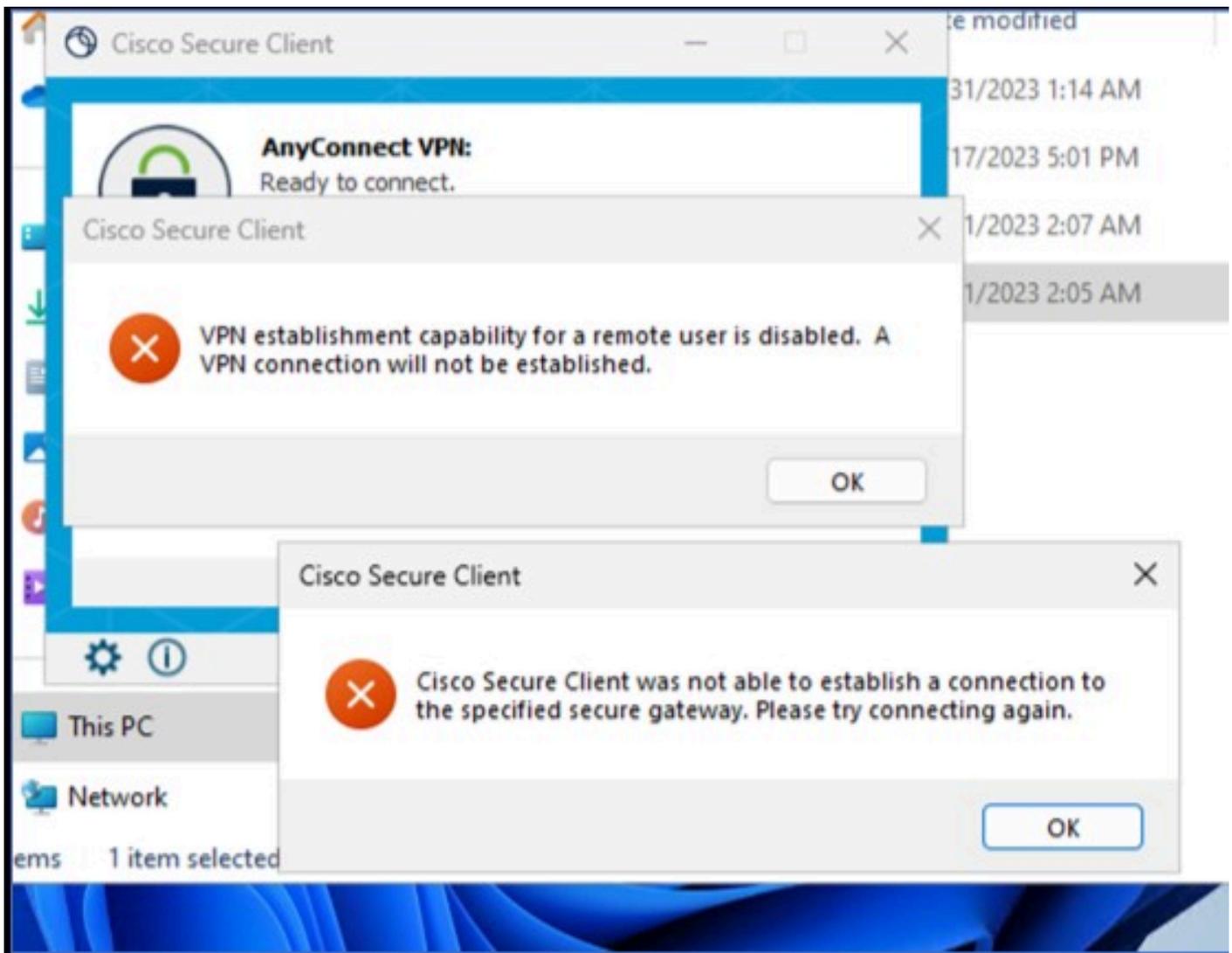
Einleitung

In diesem Dokument wird die Fehlerbehebung beschrieben: "Die VPN-Einrichtungsfunktion für einen Remote-Benutzer ist deaktiviert. Es wird keine VPN-Verbindung hergestellt."

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:

- Die VPN-Einrichtungsfunktion für einen Remote-Benutzer ist deaktiviert. Es wird keine VPN-Verbindung hergestellt.
- Der Cisco Secure Client konnte keine Verbindung mit dem angegebenen sicheren Gateway herstellen. Versuchen Sie erneut, eine Verbindung herzustellen.



Cisco Secure Client - Verbindungsproblem mit Cisco Secure Access

Der genannte Fehler wird generiert, wenn der Benutzer über das RDP mit dem Windows-PC verbunden ist, versucht, eine Verbindung zum RA-VPN vom angegebenen PC herzustellen, und **WindowsVPN Establishment** ist auf **Local Users Only** (default option).

Windows VPN Establishment bestimmt das Verhalten des Cisco Secure Client, wenn ein Benutzer, der remote am Client-PC angemeldet ist, eine VPN-Verbindung herstellt. Folgende Werte sind gültig:

- Local Users Only

Verhindert, dass ein remote angemeldeter (RDP) Benutzer eine VPN-Verbindung herstellt.

- **Allow Remote Users**

Ermöglicht Remote-Benutzern, eine VPN-Verbindung herzustellen. Wenn jedoch die konfigurierte VPN-Verbindungsweiterleitung dazu führt, dass die Verbindung des Remote-Benutzers getrennt wird, wird die VPN-Verbindung beendet, damit der Remote-Benutzer wieder Zugriff auf den Client-PC erhält. Remote-Benutzer müssen nach der VPN-Einrichtung 90 Sekunden warten, wenn sie ihre Remote-Anmeldesitzung trennen möchten, ohne dass die VPN-Verbindung beendet wird.

Lösung

Navigieren Sie zum Cisco Secure Access Dashboard.

- 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](#)

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

Klicken Sie **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

Edit

Cancel Back Save

Cisco Secure Access - Konfiguration des RA-PVN-Clients

Klicken Sie **Administrator Settings** und zu ändern **Windows VPN Establishment** von **Local User Only** ZU **All Remote Users**

BEFORE

AFTER

BEFORE		AFTER	
Administrator Settings			
Windows Logon Enforcement	Windows VPN Establishment	Windows Logon Enforcement	Windows VPN Establishment
Single Local Logon	Local Users Only	Single Local Logon	All Remote Users
Linux Logon Enforcement	Linux VPN Establishment	Linux Logon Enforcement	Linux VPN Establishment
Single Local Logon	Local Users Only	Single Local Logon	Local Users Only

Cisco Secure Access - Windows-VPN-Einrichtung

und klicke auf "Speichern".

Client Settings

General 3 ▾

Administrator Settings 9 ▲

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

Clear SmartCard PIN User controllable

IP Protocol Supported

IPv4

Proxy Settings

Native

Allow local proxy connections User controllable

Allow optimal gateway selection

Cancel **Save**

Cisco Secure Access - Windows Windows VPN Establishment 2

Wenn Sie die RA-VPN-Sitzung vom Remote-Windows-PC aus einrichten, müssen Sie die **Tunnel Mode** als **Bypass Secure Access**. Andernfalls riskieren Sie, den Zugriff auf den Windows-Ferncomputer zu verlieren.

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 - Tunnelmodus

Weitere Informationen über Tunnel Mode Überprüfen Sie den nächsten Artikel Nummer 6:

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

Zugehörige Informationen

- [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.