

セキュアアクセスエラーのトラブルシューティング"; リモートユーザのVPN確立機能が無効になっている。VPN接続が確立されない(&C)

内容

[はじめに](#)

[問題](#)

[解決方法](#)

[関連情報](#)

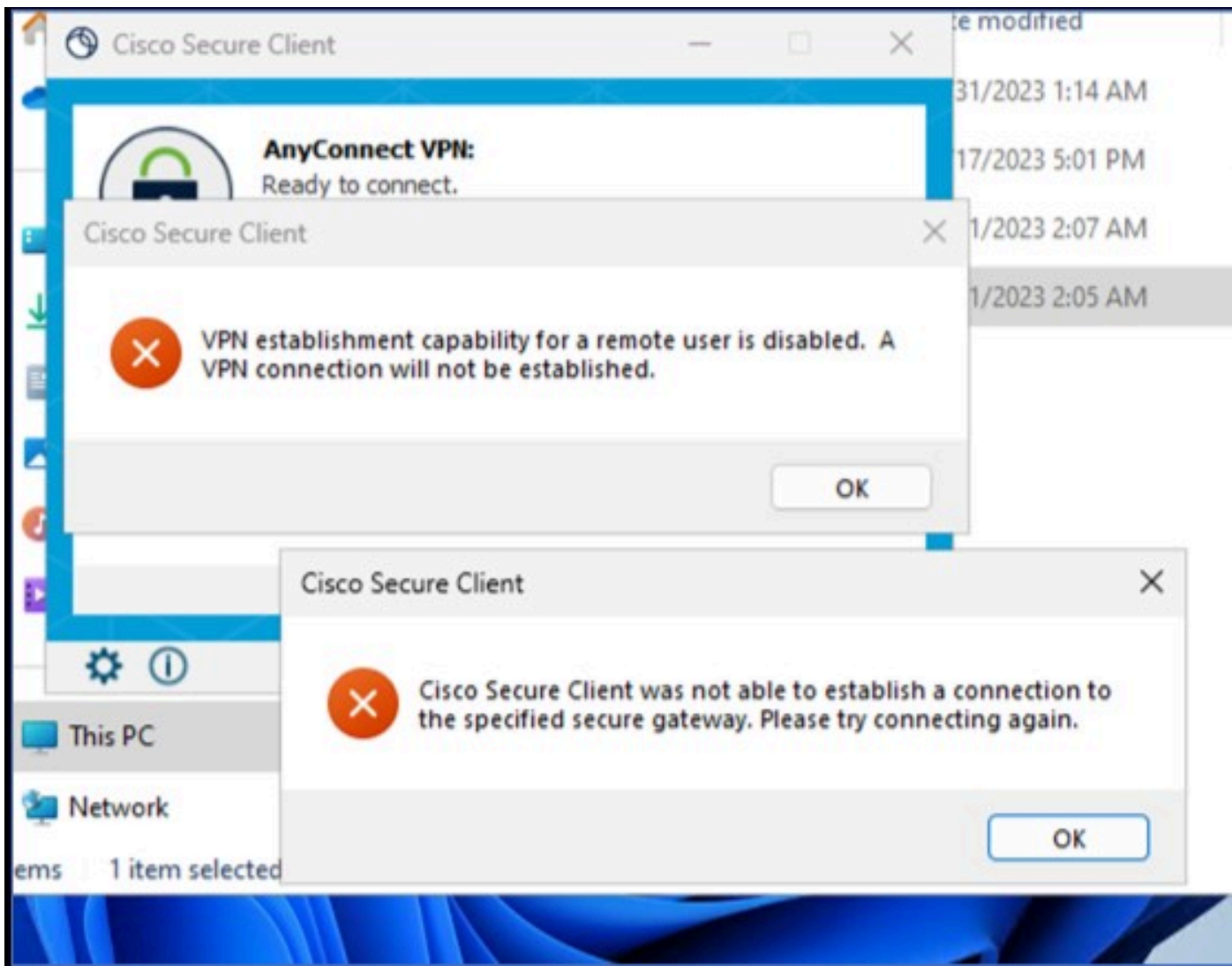
はじめに

このドキュメントでは、エラー「VPN establishment capability for a remote user is disabled」を解決する方法について説明します。A VPN connection will not be established.」

問題

ユーザがRA-VPN (リモートアクセスVPN) を使用してセキュアアクセスヘッドエンドに接続しようとする、Cisco Secure Client通知ポップアップにエラーが表示されます。

- リモートユーザのVPN確立機能が無効になっている。A VPN connection will not be established。
- Cisco Secure Clientは、指定されたセキュアゲートウェイへの接続を確立できませんでした。接続を再試行してください。



Cisco Secure Client:Cisco Secure Accessへの接続に関する問題

ユーザがRDPを介してWindows PCに接続し、特定のPCからRA-VPNに接続しようとするすると、上記のエラーが生成されます。 WindowsVPN Establishment に設定されている Local Users Only (default option)を参照。

Windows VPN Establishment クライアントPCにリモートでログオンしているユーザがVPN接続を確立するときのCisco Secure Clientの動作を指定します。可能な値は次のとおりです。

- Local Users Only

リモートログイン(RDP)ユーザによるVPN接続の確立を防止します。

- Allow Remote Users

リモートユーザはVPN接続を確立できます。ただし、設定されたVPN接続ルーティングによってリモートユーザが接続解除された場合、VPN接続は終了し、リモートユーザがクライアントPCにアクセスできるようになります。リモートユーザがVPN接続を終了させずにリモートログインセッションを切断するには、VPNの確立後90秒間待機する必要があります。

解決方法

Cisco Secure Access Dashboardに移動します。

- クリックして **Connect > End User Connectivity**
- クリックして **Virtual Private Network**
- 変更するプロファイルを選択し、**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](#)

シスコセキュアアクセス - RA-VPN

クリックして **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 1

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](#) 3

[Cancel](#) [Back](#) [Save](#)

Cisco Secure Access - RA-VPNクライアントの設定

クリックして **Administrator Settings** および変更 **Windows VPN Establishment** 変更前 **Local User Only** から **All Remote Users**

BEFORE → **AFTER**

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

Cisco Secure Access - Windows Windows VPNの確立

次に、Saveをクリックします

Client Settings

General 3

Administrator Settings 9

Windows Logon Enforcement Single Local Logon	Windows VPN Establishment All Remote Users
Linux Logon Enforcement Single Local Logon	Linux VPN Establishment 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確立2

リモートWindows PCからRA-VPNセッションを確立する場合は、 Tunnel Mode as Bypass Secure Accessを参照。そうしないと、リモートのWindows PCへのアクセスが失われる危険性があります。

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 – トンネルモード

シナリオとセットアップの詳細については、 [Tunnel Mode](#) 次の記事の項目6を確認してください。

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

関連情報

- [セキュアアクセスユーザガイド](#)
- [シスコテクニカルサポートおよびダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。