

Risoluzione dei problemi relativi all'errore di accesso sicuro "La funzionalità di definizione della VPN per un utente remoto è disabilitata. Non verrà stabilita una connessione VPN"

Sommario

[Introduzione](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

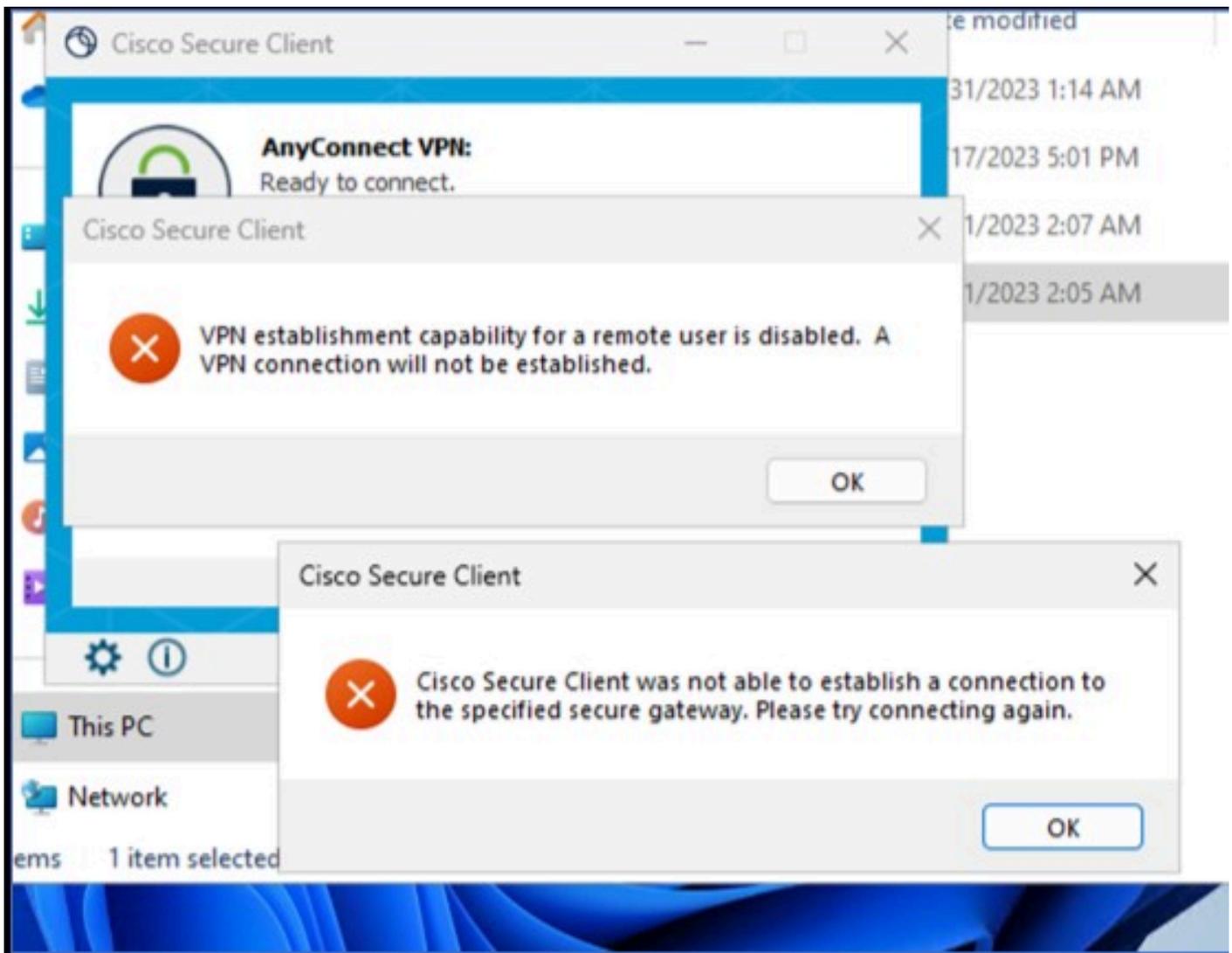
Introduzione

In questo documento viene descritto come risolvere l'errore: "La funzionalità di connessione VPN per un utente remoto è disabilitata. Non verrà stabilita una connessione VPN."

Problema

Quando un utente tenta di connettersi all'headend di Secure Access tramite una VPN ad accesso remoto (RA-VPN), l'errore viene stampato nel popup di notifica di Cisco Secure Client:

- La funzionalità di connessione VPN per un utente remoto è disabilitata. Non verrà stabilita una connessione VPN.
- Cisco Secure Client: impossibile stabilire una connessione con il gateway sicuro specificato. Riprova a connetterti.



Cisco Secure Client - Problema durante la connessione a Cisco Secure Access

L'errore indicato viene generato quando l'utente è connesso tramite RDP al PC Windows e tenta di connettersi a RA-VPN dal PC specificato e **WindowsVPN Establishment** è impostato su **Local Users Only** (default option).

Windows VPN Establishment determina il comportamento di Cisco Secure Client quando un utente che ha eseguito l'accesso remoto al PC client stabilisce una connessione VPN. I valori possibili sono:

- **Local Users Only**

Impedisce a un utente con accesso remoto (RDP) di stabilire una connessione VPN.

- **Allow Remote Users**

Consente agli utenti remoti di stabilire una connessione VPN. Tuttavia, se il routing della connessione VPN configurato provoca la disconnessione dell'utente remoto, la connessione VPN termina per consentire all'utente remoto di riottenere l'accesso al PC client. Gli utenti remoti devono attendere 90 secondi dopo la connessione VPN se desiderano disconnettere la sessione di accesso remoto senza interrompere la connessione VPN.

Soluzione

Passare a Cisco Secure Access Dashboard.

- Fare clic su **Connect > End User Connectivity**
- Fare clic su **Virtual Private Network**
- Scegliere il profilo da modificare e fare clic su **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

Fare clic su **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](#)

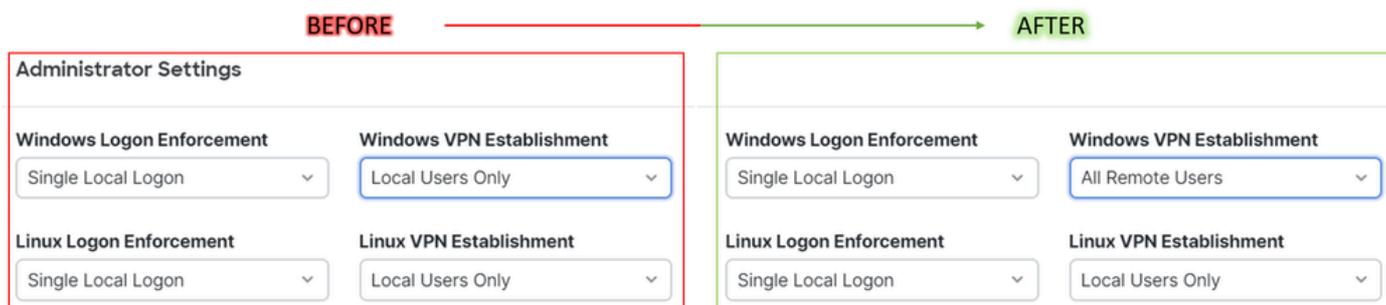
Pre Selected Settings

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](#)

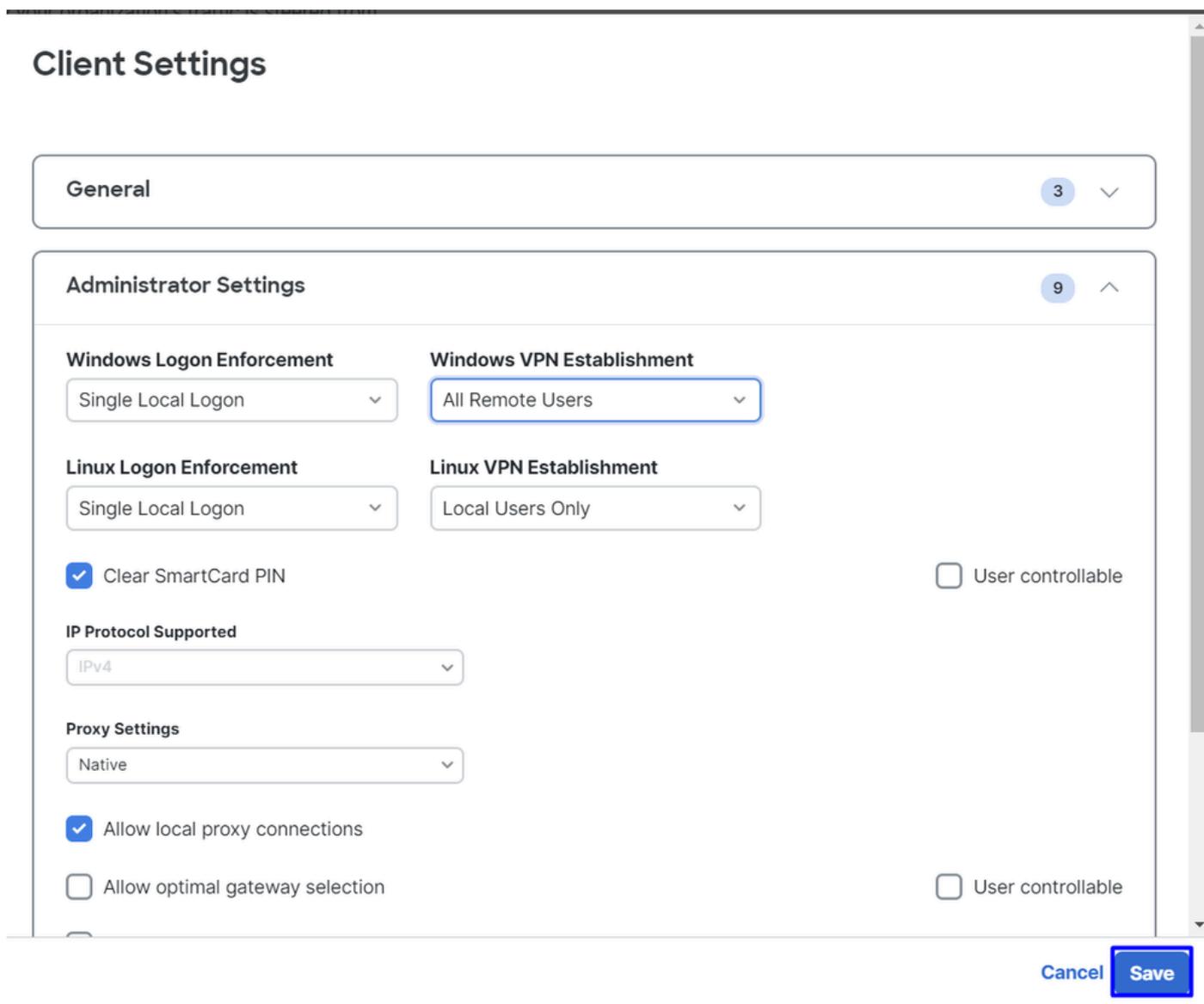
Cisco Secure Access - Configurazione client RA-VPN

Fare clic su **Administrator Settings** e modificare **Windows VPN Establishment** da **Local User Only** a **All Remote Users**



Cisco Secure Access - Installazione di VPN per Windows

E fare clic su Salva



Cisco Secure Access - Windows VPN Establishment 2

Quando si stabilisce la sessione RA-VPN dal PC Windows remoto, è necessario configurare Tunnel Mode come Bypass Secure Access. In caso contrario, si rischia di perdere l'accesso al PC Windows remoto.

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 - Modalità tunnel

Per ulteriori informazioni su Tunnel Mode controlla il prossimo articolo numero articolo 6:

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

Informazioni correlate

- [Guida per l'utente di Secure Access](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).