

# Secure Client VPN trennt die Verbindung mit dem Ursachencode 7 für die Terminierung unter Ubuntu 24.04

## Inhalt

---

---

## Problem

Cisco Secure Client unter Ubuntu 24.04 stellt erfolgreich eine VPN-Verbindung her, trennt die Verbindung jedoch innerhalb von Sekunden. Die Trennung wird konsequent von Termination Ursachencode 7 begleitet und stürzt mit libvpnapl.so, verhindert stabile VPN-Konnektivität für den normalen Geschäftszugang erforderlich.

Die Verbindungssequenz zeigt an, dass der Client den Status "Verbunden" erreicht hat, dann aber sofort wieder in den Status "Getrennt" übergeht, wenn der Status überprüft wird. Der VPN-Client zeigt den Code "Terminierungsgrund 7: Der Agent wurde angehalten" in den Protokollen sowie Tunnelzustandsänderungseinträge und Meldungen, die darauf hinweisen, dass DTLS/SSL-Verbindungen mit Warnungen über das Schließen der Verbindung abgebrochen werden.

Diese Befehlssequenz zeigt das Problem:

```
/opt/cisco/secureclient/bin/vpn connect
```

Die Verbindungsausgabe zeigt eine erfolgreiche Herstellung an:

```
Cisco Secure Client (version 5.1.12.146) release.  
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.  
>> state: Unknown  
>> state: Disconnected  
>> state: Disconnected  
>> notice: Ready to connect.  
>> registered with local VPN subsystem.  
>> contacting host (vpn.sse.cisco.com) for login information...  
>> notice: Contacting vpn.sse.cisco.com.  
>> Your client certificate will be used for authentication  
Group:  
>> state: Connecting
```

```
>> notice: Establishing VPN session...
The Cisco Secure Client - Downloader is analyzing this computer. Please wait...
Initializing the Cisco Secure Client - Downloader...
The Cisco Secure Client - Downloader is performing update checks...
The Cisco Secure Client - Downloader update checks have been completed.
>> notice: The Cisco Secure Client - Downloader is performing update checks...
>> notice: Checking for profile updates...
>> notice: Checking for customization updates...
>> notice: Performing any required updates...
>> notice: The Cisco Secure Client - Downloader update checks have been completed.
Please wait while the VPN connection is established...
>> state: Connecting
>> notice: Establishing VPN session...
>> notice: Establishing VPN - Initiating connection...
>> notice: Establishing VPN - Examining system...
>> notice: Establishing VPN - Activating VPN adapter...
>> notice: Establishing VPN - Configuring system...
>> notice: Establishing VPN...
>> state: Connected
```

Wenn Sie jedoch den Status unmittelbar nach der Verbindung überprüfen:

```
/opt/cisco/secureclient/bin/vpn status
```

Der Client zeigt den Status "Getrennt" an:

```
Cisco Secure Client (version 5.1.12.146) release.
Copyright (c) 2004 - 2025, Cisco Systems, Inc. All rights reserved.
>> state: Unknown
>> state: Disconnected
>> state: Disconnected
>> state: Disconnected
>> notice: Ready to connect.
>> registered with local VPN subsystem.
VPN>
```

## Umwelt

- Betriebssystem: Ubuntu 24,04
- Version des Cisco Secure Client: 5.1.12.146
- Authentifizierungsmethode: Authentifizierung von Client-Zertifikaten

- Virtuelle Schnittstelle: cscotun0 (oder ähnliche virtuelle Cisco Secure Client-Schnittstelle)
- Umgebung umfasst Automatisierungsskripte für das Systemmanagement

## Auflösung

Das Problem konnte durch die Identifizierung und Korrektur eines Automatisierungsskripts behoben werden, das die virtuelle Cisco Secure Client-Schnittstelle (cscotun0) falsch als neues physisches Gerät identifizierte, und indem eine HTTP-/transparente Proxykonfiguration darauf angewendet wurde. In den folgenden Schritten wird der Problemlösungsprozess beschrieben.

### Schritt 1: Erfassen von Diagnoseinformationen

Generieren Sie DART-Pakete (Diagnose- und Reporting-Tool) vom betroffenen Endpunkt, um detaillierte VPN-Client-Protokolle und Systeminformationen zu erfassen:

```
Generate DART bundle from Cisco Secure Client interface or command line
```

Die DART-Pakete enthalten Protokolleinträge des VPN-Agenten, in denen die Schritte zur Schnittstellen- und Profilkonfiguration aufgeführt sind, einschließlich der DNS-Einstellungen für die Schnittstelle cscotun0, der Konfiguration des VPN-Adapters und der Änderungen der Routing-Tabelle.

```
Mar 13 16:41:08 Message type information sent to
> the user: Contacting vpn.sse.cisco.com.
> Mar 13 16:41:08 : VPN SESSION START: Initiating
> VPN connection to the secure gateway hvpn.sse.cisco.com
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy server configuration from
> the operating system: http://x.x.x.x:3128/
> Mar 13 16:41:08 The Cisco Secure Client -
> AnyConnect VPN has obtained the following proxy exception list from the
> operating system: localhost,127.0.0.0/8,::1
> Mar 13 16:41:11 Termination reason code 7: The
> agent has been stopped.
```

## Phase 2: Automatisierungsskriptverhalten analysieren

Lokale Automatisierungsskripts untersuchen, die Netzwerkschnittstellen und Proxy-Konfigurationen verwalten. Suchen Sie nach Skripten, die neue Netzwerkschnittstellen automatisch erkennen und Konfigurationsrichtlinien anwenden.

### Schritt 3: Problem mit der Proxy-Zuweisung identifizieren

Stellen Sie fest, ob Automatisierungsskripts die virtuelle Cisco Secure Client-Schnittstelle als neues physisches Gerät behandeln und unangemessene Proxyeinstellungen anwenden. Auf die virtuelle Schnittstelle (cscotun0 oder ähnlich) kann keine HTTP/transparente Proxykonfiguration angewendet werden.

### Schritt 4: Entfernen der Proxykonfiguration von der virtuellen Schnittstelle

Entfernen oder korrigieren Sie die Proxy-Zuweisung, die vom Automatisierungsskript automatisch auf die virtuelle Cisco Secure Client-Schnittstelle angewendet wurde. Dadurch wird verhindert, dass der Proxy den VPN-Datenverkehrsfluss stört.

### Schritt 5: Automatisierungsskriptlogik aktualisieren

Ändern Sie das Automatisierungsskript, um virtuelle Cisco Secure Client-Schnittstellen (in der Regel cscotun0, cscotun1 genannt) von den Richtlinien für die automatische Proxy-Konfiguration auszuschließen. Fügen Sie Logik hinzu, um virtuelle VPN-Schnittstellen während automatisierter Netzwerkkonfigurationsprozesse zu identifizieren und zu überspringen.

### Schritt 6: Überprüfung der VPN-Verbindungen

Testen Sie die VPN-Verbindung, nachdem Sie die Proxy-Konfiguration entfernt haben, um eine stabile Verbindung zu bestätigen:

```
/opt/cisco/secureclient/bin/vpn connect vpn.sse.cisco.com
```

Überprüfen Sie den Status der Verbindung nach dem Verbindungsaufbau, um sicherzustellen, dass die Verbindung stabil bleibt:

```
/opt/cisco/secureclient/bin/vpn status
```

## Alternative Schritte zur Fehlerbehebung

Wenn das Problem weiterhin besteht oder in ähnlichen Umgebungen auftritt, sollten Sie zusätzlich folgende Ansätze zur Fehlerbehebung in Betracht ziehen:

- Testen des Cisco Secure Client auf einem neuen Linux-Endgerät ohne Automatisierungsskripts
- Deaktivieren Sie vorübergehend Dienste von Drittanbietern, die mit libvpngapi oder dem VPN-Agenten interferieren können.
- Upgrade von Cisco Secure Client auf die neueste verfügbare Version
- Überprüfung der Systemprotokolle auf Konflikte bei der Erstellung und Konfiguration virtueller VPN-Schnittstellen

## Ursache

Die Ursache dafür war ein internes Automatisierungsskript, das die virtuelle Schnittstelle des Cisco Secure Client (cscotun0 oder ähnlich) falsch als neues physisches Netzwerkgerät identifizierte. Das Skript wandte die HTTP/Transparent-Proxy-Konfiguration automatisch auf diese virtuelle Schnittstelle an, was den VPN-Datenverkehrsfluss beeinträchtigte und dazu führte, dass die Verbindung mit dem Ursachencode 7 beendet wurde.

Wenn der VPN-Client eine Verbindung herstellt, erstellt er eine virtuelle Netzwerkschnittstelle, um verschlüsselten Datenverkehr zu verarbeiten. Das Automatisierungsskript erkannte diese Schnittstellenerstellung als neues Netzwerkgerät, das dem System beiträgt, und wandte Standardproxyrichtlinien für physische Netzwerkschnittstellen an. Diese Proxy-Konfiguration beeinträchtigte die Fähigkeit des VPN-Tunnels, verschlüsselten Datenverkehr ordnungsgemäß

weiterzuleiten, was nach dem erfolgreichen Verbindungsaufbau zu einer sofortigen Trennung der Verbindung führte.

Der Terminierungsgrund Code 7 ("Der Agent wurde gestoppt") und libvpnapl.so Abstürze waren Symptome der zugrunde liegenden Proxy-Interferenz und nicht direkte VPN-Client-Software-Probleme.

## Verwandte Inhalte

- [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.