

# AnyConnect VPN-Anmeldung aufgrund von Endpunkt-Statusbedingungen einschließlich Cortex abgelehnt

## Inhalt

---

---

## Problem

Mehrere Benutzer können sich zeitweilig nicht mit Secure Client Remote Access (RAVPN) verbinden und erhalten die Fehlermeldung "AnyConnect VPN Login denied" (AnyConnect VPN-Anmeldung abgelehnt). Ihre Umgebung erfüllt nicht die von Ihrem Administrator definierten Zugriffskriterien." Das Problem betrifft sowohl MacBooks als auch Surface-Laptops, wobei Benutzer häufig mehrere Verbindungsversuche oder Systemneustarts benötigen, um eine erfolgreiche Verbindung herzustellen. Die Verbindungsfehler scheinen auf die Bedingungen zur Validierung des Endpunktstatus zurückzuführen zu sein, insbesondere auf die Anforderungen der MacOS-Version und die Cortex XDR-Statusüberprüfung.

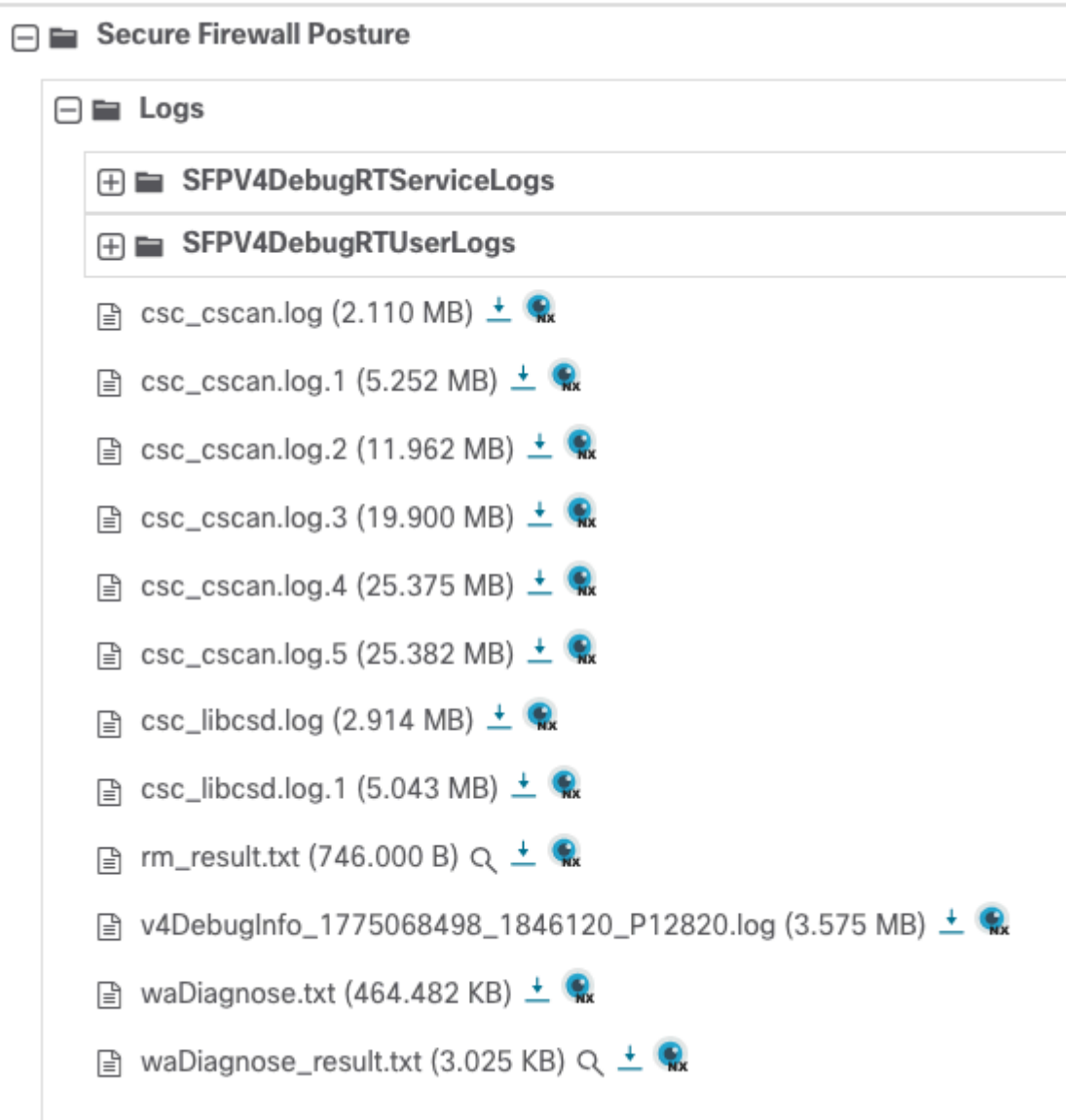
## Umwelt

- Bereitstellung von Secure Client Remote Access (RAVPN) mit Statusüberprüfung
- Gemischte Endgeräteumgebung mit MacBooks und Surface-Laptops
- Statusanforderungen für Endgeräte: macOS Version 26.2 oder höher und Cortex XDR mit
- Lösung für sicheren Zugriff mit DAP-Durchsetzung (Device Access Policy)

## Auflösung

1: DART sammeln.

2: Navigieren Sie zum Ordner Secure Firewall Posture, und laden Sie csc\_scan.log herunter:



inline\_image\_0.png

3: Suchen Sie nach diesen Protokollen:

[Fr Mar 27 13:53:10.419 2026] debug :: Json in als {"input":{"method":1000,"signature":}}

[Fr Mar 27 13:53:10.420 2026] Fehler :: Opswat hat einen Fehler zurückgegeben: -22 und umgewandelt in: 6

[Fr Mar 27 13:53:10.420 2026] Fehler :: Fehler in Bedingung: Status opSuccess !=

[Fr Mar 27 13:53:10.420 2026] debug :: Opswat-Rücksendestatus ist 'Zugriff verweigert'

[Fr Mar 27 13:53:10.420 2026] debug :: mit dem Service den RTP-Status von Antimalware zu

überprüfen.

[Fr Mar 27 13:53:10.420 2026] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Fr Mar 27 13:53:10.420 2026] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Fr Mar 27 13:53:10.420 2026] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Fr Mar 27 13:53:10.420 2026] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Fr Mar 27 13:53:15.060 2026] Fehler :: Antwort empfangen.

[Fr Mar 27 13:53:15.060 2026] debug :: am check rtp.<<<<-----

[Freitag, 27. März 2026, 13:53:15.06] Informationen :: der zurückgegebene RTP-Status ist fehlgeschlagen.

[Freitag, 27. März 2026, 13:53:15.06] Informationen :: Opswat-Rücksendungsdefinitionsdatum ist 1

[Fr Mar 27 13:53:15.060 2026] debug :: mit dem Dienst das Definitionsdatum für Antimalware abrufen.

[Freitag, 27. März 2026, 13:53:15.06] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Freitag, 27. März 2026, 13:53:15.06] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Freitag, 27. März 2026, 13:53:15.06] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Freitag, 27. März 2026, 13:53:15.06] trace :: TCP/IP-Status IPv4(1),IPv6(1)

[Fr Mar 27 13:53:20.079 2026] Fehler :: Antwort empfangen.

[Fr Mar 27 13:53:20.079 2026] debug :: kann keine Malwareschutz-Definitionsdatumsoperation ausführen <<<<<<—

[Fr Mar 27 13:53:20.079 2026] debug :: gefunden Antimalware ==> () (Cortex XDR (Mac)) (9.1.0) () (fehlgeschlagen) .

[Fr Mar 27 13:53:20.084 2026] debug :: Übereinstimmung fehlgeschlagen: Prozessnamen sind 'ciscod' und 'cscan'

[Fr Mar 27 13:53:20.084 2026] debug ::edr Prüfung der Internetverbindung (1)



Anmerkung: Auf dieser Grundlage scheint es entweder eine Einschränkung durch Cortex auf unsere Prozesse oder Einschränkung auf den Internetzugang und die andere Sache, die wir überprüfen können, ob Cortex nicht stört den Prozess. Es könnte die sichere Firewall-Statusüberprüfung blockieren, da der Scan als Malware behandelt werden könnte.

---

## Ausschlussliste von AntiMalware

Cisco Secure Client (CSC): Alle Module - System

1. Windows: C:\Program Files (x86)\Cisco\Cisco Secure Client\\*
2. macOS: /opt/cisco/secureclient/\*
3. Linux: /opt/cisco/secureclient/\*

Cisco Secure Client (CSC): Alle Module - Benutzer

1. Windows: %localappdata%\Cisco\Cisco Secure Client\\*
2. macOS: ~/.cisco/secureclient/\*
3. Linux: ~/.cisco/secureclient/\*

## Ursache

Das Problem wird durch zeitweilige Fehler im Endpunkt-Statusbewertungsprozess verursacht, die speziell mit der Validierung der MacOS-Versionsanforderungen und des Cortex XDR-Status zusammenhängen. Das Statusbewertungssystem erkennt oder validiert inkonsistent die

erforderlichen Sicherheitsbedingungen (macOS 26.2 oder höher und Cortex XDR-Ausführungsstatus), was zu Verbindungsverweigerungen führt, selbst wenn die Endpunkte die angegebenen Kriterien erfüllen. Dies führt dazu, dass Benutzer mehrere Verbindungsversuche oder Systemneustarts durchführen müssen, um eine erfolgreiche Statusüberprüfung und VPN-Verbindung zu erzielen.

## 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.