

# Leitfaden zur Fehlerbehebung bei AnyConnect VPN-Clients - Häufige Probleme

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Fehlerbehebung](#)

[Probleme bei der Installation und beim virtuellen Adapter](#)

[Verbindungstrennung oder Unmöglichkeit zum Herstellen der ersten Verbindung](#)

[Probleme bei der Weiterleitung von Datenverkehr](#)

[Absturzfehler bei AnyConnect](#)

[Fragmentierung/Übergeben von Datenverkehrsproblemen](#)

[Automatische Deinstallation](#)

[Problem bei der Eingabe des Cluster-FQDN](#)

[Konfiguration der Sicherungsserverliste](#)

[AnyConnect: Beschädigtes Problem mit der Treiberdatenbank](#)

[Reparatur](#)

[Fehlgeschlagene Reparatur](#)

[Analyse der Datenbank](#)

[Fehlermeldungen](#)

[Fehler: Die Sitzungsverwaltungsdatenbank kann nicht aktualisiert werden.](#)

[Lösung 1](#)

[Lösung 2](#)

[Fehler: "Modul c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll konnte nicht registriert werden."](#)

[Lösung](#)

[Fehler: "Beim sicheren Gateway wurde ein Fehler als Antwort auf die VPN-Aushandlungsanfrage gemeldet. Wenden Sie sich an Ihren Netzwerkadministrator."](#)

[Lösung](#)

[Fehler: Die Sitzung konnte nicht eingerichtet werden. Sitzungslimit von 2 wurde erreicht.](#)

[Lösung 1](#)

[Lösung 2](#)

[Fehler: AnyConnect ist auf dem VPN-Server nicht aktiviert, wenn versucht wird, eine Verbindung mit der ASA herzustellen](#)

[Lösung](#)

[Fehler:- %ASA-6-722036: Gruppen-Client-Gruppe Benutzer xxxx IP x.x.x.x Senden eines großen Pakets 1220 \(Schwellenwert 1206\)](#)

[Lösung](#)

[Fehler: Das sichere Gateway hat die VPN-Verbindungs- oder Verbindungsanforderung des Agenten abgelehnt.](#)

[Lösung](#)

Fehler: "Sitzungsmanagement-Datenbank konnte nicht aktualisiert werden"

Lösung

Fehler: "Beim VPN-Client-Treiber ist ein Fehler aufgetreten."

Lösung

Fehler: "Antwort von xxx.xxx.xxx.xxx kann nicht verarbeitet werden."

Lösung

Fehler: "Anmelden verweigert, unberechtigter Verbindungsmechanismus, wenden Sie sich an Ihren Administrator."

Lösung

Fehler: "AnyConnect-Paket nicht verfügbar oder beschädigt. Wenden Sie sich an Ihren Systemadministrator"

Lösung

Fehler: "Das AnyConnect-Paket am sicheren Gateway konnte nicht gefunden werden."

Lösung

Fehler: "Sicheres VPN über Remote-Desktop wird nicht unterstützt."

Lösung

Fehler: "Das empfangene Serverzertifikat oder seine Kette erfüllt nicht FIPS. Eine VPN-Verbindung wird nicht hergestellt."

Lösung

Fehler: "Fehler bei der Zertifikatsvalidierung"

Lösung

Fehler: "Der VPN Agent Service hat ein Problem festgestellt und muss geschlossen werden. Wir entschuldigen uns für die Unannehmlichkeiten."

Lösung

Fehler: "Dieses Installationspaket konnte nicht geöffnet werden. Überprüfen, ob das Paket vorhanden ist"

Lösung

Fehler: "Fehler beim Anwenden von Transformationen. Überprüfen Sie, ob die angegebenen Transformationspfade gültig sind."

Lösung

Fehler: "Beim VPN-Client-Treiber ist ein Fehler aufgetreten."

Lösung

Fehler: "Eine VPN-Verbindung führte zu unterschiedlichen Konfigurationseinstellungen. Die VPN-Netzwerkeinstellung wird neu initialisiert. Anwendungen, die das private Netzwerk nutzen, müssen möglicherweise wiederhergestellt werden."

Lösung

AnyConnect-Fehler bei der Anmeldung

Lösung

Die IE-Proxy-Einstellung wird nach der Trennung von AnyConnect unter Windows 7 nicht wiederhergestellt.

Lösung

Fehler: AnyConnect Essentials kann erst aktiviert werden, wenn alle Sitzungen geschlossen sind.

Lösung

Fehler: Die Verbindungsregisterkarte in der Internetoption von Internet Explorer verbirgt sich nach dem Herstellen der Verbindung mit dem AnyConnect-Client.

Lösung

Fehler: Nur wenige Benutzer erhalten die Meldung "Login Failed" (Anmeldung fehlgeschlagen),

[wenn andere Benutzer erfolgreich eine Verbindung über AnyConnect VPN herstellen können.](#)

[Lösung](#)

[Fehler: Das angezeigte Zertifikat stimmt nicht mit dem Namen der Website überein, die Sie anzeigen möchten.](#)

[Lösung](#)

[AnyConnect kann vom CSD-Vault eines Windows 7-Computers nicht gestartet werden](#)

[Lösung](#)

[Das AnyConnect-Profil wird nach dem Failover nicht auf den Standby-Modus repliziert](#)

[Lösung](#)

[Der AnyConnect-Client stürzt ab, wenn Internet Explorer offline geht](#)

[Lösung](#)

[Fehlermeldung: TLSPROTOCOL\\_ERROR\\_INSUFFICIENT\\_BUFFER](#)

[Lösung](#)

[Fehlermeldung: "Verbindungsversuch ist aufgrund eines ungültigen Hosteintrags fehlgeschlagen."](#)

[Lösung](#)

[Fehler: "Stellen Sie sicher, dass Ihre Serverzertifikate den strikten Modus befolgen können, wenn Sie ein stets verfügbares VPN konfigurieren."](#)

[Lösung](#)

[Fehler: "In Microsoft Windows HTTP Services ist ein interner Fehler aufgetreten."](#)

[Lösung](#)

[Fehler: "Beim SSL-Transport ist ein sicherer Kanalfehler aufgetreten. Möglich ist dies durch eine nicht unterstützte Verschlüsselungskonfiguration auf dem Secure Gateway."](#)

[Lösung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird ein Fehlerbehebungsszenario beschrieben, das auf Anwendungen zutrifft, die nicht über den Cisco AnyConnect VPN-Client ausgeführt werden.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einer Cisco Adaptive Security Appliance (ASA), die Version 8.x ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Fehlerbehebung

Dieses typische Fehlerbehebungsszenario gilt für Anwendungen, die nicht über den Cisco AnyConnect VPN Client für Endbenutzer mit Microsoft Windows-Computern ausgeführt werden. In diesen Abschnitten werden die folgenden Probleme behandelt und Lösungsansätze bereitgestellt:

- [Probleme bei der Installation und beim virtuellen Adapter](#)
- [Verbindungstrennung oder Unmöglichkeit zum Herstellen der ersten Verbindung](#)
- [Probleme bei der Weiterleitung von Datenverkehr](#)
- [Absturzfehler bei AnyConnect](#)
- [Fragmentierung/Übergeben von Datenverkehrsproblemen](#)

## Probleme bei der Installation und beim virtuellen Adapter

Gehen Sie wie folgt vor:

1. Rufen Sie die Geräteprotokolldatei ab:

Windows XP/Windows 2000:

```
\Windows\setupapi.log
```

Windows Vista:

**Hinweis:** Versteckte Ordner müssen sichtbar gemacht werden, damit diese Dateien angezeigt werden können.

```
\Windows\Inf\setupapi.app.log  
\Windows\Inf\setupapi.dev.log
```

Wenn Sie Fehler in der **setupapi**-Protokolldatei sehen, können Sie die Ausführlichkeit auf 0x2000FFFF einstellen, wie in diesem [Windows-Dokument](#) beschrieben. Beachten Sie, dass der Artikel Ihnen empfiehlt, ihn auf 0xFFFF einzustellen, aber wenn Sie den hohen Wert von 0x2 hinzufügen, wird die Protokollierung beschleunigt.

2. Rufen Sie die Protokolldatei des MSI-Installationsprogramms ab:

Wenn es sich um eine erstmalige Installation der Webbereitstellung handelt, befindet sich dieses Protokoll im temporären Verzeichnis für jeden Benutzer.

Windows XP/Windows 2000:

`\Documents and Settings\`

Windows Vista:

`\Users\`

Wenn es sich um ein automatisches Upgrade handelt, befindet sich dieses Protokoll im temporären Verzeichnis des Systems:

`\Windows\Temp`

Der Dateiname hat folgendes Format: **anyconnect-win-x.x.xxx-k9-install-yyyyyyyyyy.log**. Rufen Sie die neueste Datei für die Version des Clients ab, den Sie installieren möchten. Die x.xxx-Änderungen basieren auf der Version, z. B. 2.0.0343, und yyyy-yyyy ist das Datum und die Uhrzeit der Installation.

3. Rufen Sie die Systeminformationsdatei des PCs ab:

Geben Sie in das Feld Eingabeaufforderung/DOS Folgendes ein:

Windows XP/Windows 2000:

`winmsd /nfo c:\msinfo.nfo`

Windows Vista:

```
msinfo32 /nfo c:\msinfo.nfo
```

**Hinweis:** Nachdem Sie diese Eingabeaufforderung eingegeben haben, warten Sie. Es kann zwischen zwei und fünf Minuten dauern, bis die Datei fertig gestellt ist.

Abrufen eines Systeminfo-Dateidumps von einer Eingabeaufforderung:

Windows XP und Windows Vista:

```
systeminfo c:\sysinfo.txt
```

Weitere Informationen finden Sie unter [AnyConnect: Fehler bei der Treiberdatenbank](#), um das Treiberproblem zu beheben.

## Verbindungstrennung oder Unmöglichkeit zum Herstellen der ersten Verbindung

Wenn Verbindungsprobleme mit dem AnyConnect-Client auftreten, z. B. Verbindungstrennung oder die fehlende Möglichkeit zum Herstellen einer Erstverbindung, rufen Sie die folgenden Dateien ab:

- Die Konfigurationsdatei von der ASA, um festzustellen, ob ein Teil der Konfiguration den Verbindungsfehler verursacht:

Geben Sie in der Konsole der ASA Folgendes ein: `write net x.x.x.x:ASA-Config.txt WO x.x.x.x` ist die IP-Adresse eines TFTP-Servers im Netzwerk.

ODER

Geben Sie in der Konsole der ASA Folgendes ein: `show running-config`. Lassen Sie die Konfiguration auf dem Bildschirm abschließen, schneiden Sie sie in einen Texteditor ein, und speichern Sie sie.

- Die ASA-Ereignisprotokolle:

Führen Sie folgende CLI-Befehle aus, um die Protokollierung von Authentifizierungs-, WebVPN-, Secure Sockets Layer (SSL)- und SSL VPN Client (SVC)-Ereignissen auf der ASA zu aktivieren:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```

Erstellen Sie eine AnyConnect-Sitzung, und stellen Sie sicher, dass der Fehler reproduziert werden kann. Erfassen Sie die Protokollausgabe von der Konsole in einen Text-Editor, und speichern Sie sie.

Um die Protokollierung zu deaktivieren, führen Sie folgende Schritte aus: `no logging enable`.

- Das Cisco AnyConnect VPN Client-Protokoll in der Windows Event Viewer des Client-PCs:

Wählen Sie **Start > Ausführen aus**.

Eingabe:

```
eventvwr.msc /s
```

Klicken Sie mit der rechten Maustaste auf das Protokoll **Cisco AnyConnect VPN Client**, und wählen Sie Protokolldatei als **AnyConnect.evt** speichern aus.

**Hinweis:** Speichern Sie die Datei immer im Format **.evt**.

Wenn der Benutzer keine Verbindung zum AnyConnect VPN Client herstellen kann, kann das Problem auf eine auf dem Client-PC aktivierte RDP-Sitzung (Remote Desktop Protocol) oder Fast User Switching zurückzuführen sein. Der Benutzer kann die `AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection will not be established error message` Fehler auf dem Client-PC. Um dieses Problem zu beheben, trennen Sie alle etablierten RDP-Sitzungen, und deaktivieren Sie Fast User Switching. Dieses Verhalten wird vom [Windows](#)-Attribut zur [Durchsetzung](#) der [Anmeldung](#) im Clientprofil gesteuert. Derzeit gibt es jedoch keine Einstellung, die es einem Benutzer ermöglicht, eine VPN-Verbindung herzustellen, während mehrere Benutzer gleichzeitig auf demselben Computer angemeldet sind. [CSCsx15061](#) für Verbesserungsanfrage wurde für diese Funktion abgelegt.

**Hinweis:** Stellen Sie sicher, dass Port 443 nicht blockiert ist, damit der AnyConnect-Client eine Verbindung zur ASA herstellen kann.

Wenn ein Benutzer den AnyConnect VPN Client nicht mit der ASA verbinden kann, kann das Problem durch eine Inkompatibilität zwischen der AnyConnect-Client-Version und der ASA-Software-Image-Version verursacht werden. In diesem Fall erhält der Benutzer die folgende Fehlermeldung: `The installer was not able to start the Cisco VPN client, clientless access is not available.`

Um dieses Problem zu beheben, aktualisieren Sie die AnyConnect-Client-Version, um mit dem ASA-Software-Image kompatibel zu sein. Weitere Informationen zur Überprüfung der Kompatibilität finden Sie im Abschnitt [Security Appliances and Software Supported](#) (Sicherheitslösungen und Software-unterstützte [Anwendungen](#)) der [Versionshinweise](#) des [AnyConnect Client](#).

Wenn Sie sich bei der ersten Anmeldung bei AnyConnect anmelden, wird das Anmeldeskript nicht ausgeführt. Wenn Sie die Verbindung trennen und sich erneut anmelden, läuft das Anmeldeskript einwandfrei. Dies ist das erwartete Verhalten.

Wenn Sie den AnyConnect VPN Client mit der ASA verbinden, wird möglicherweise folgende Fehlermeldung angezeigt: `User not authorized for AnyConnect Client access, contact your administrator.`

Dieser Fehler wird angezeigt, wenn das AnyConnect-Image auf der ASA fehlt. Nachdem das Image auf die ASA geladen wurde, kann AnyConnect ohne Probleme mit der ASA verbunden werden.

Dieser Fehler kann durch Deaktivieren von DTLS (Datagram Transport Layer Security) behoben werden. Gehen Sie zu **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**, und deaktivieren Sie das Kontrollkästchen **Enable DTLS**. Dadurch wird DTLS deaktiviert.

Die Paketdateien zeigen diese Fehlermeldung an, wenn die Verbindung zum Benutzer getrennt wird: `TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE:The secure gateway failed to respond to Dead Peer Detection packets.` Dieser Fehler bedeutet, dass der DTLS-Kanal aufgrund eines DPD-Fehlers (Dead Peer Detection) abgebrochen wurde. Dieser Fehler wird behoben, wenn Sie die DPD-Keepalives anpassen und die folgenden Befehle ausführen:

```
webvpn
svc keepalive 30
svc dpd-interval client 80
svc dpd-interval gateway 80
```

Die Befehle `svc keepalive` und `svc dpd-interval` werden durch die Befehle `anyconnect keepalive` und `anyconnect dpd interval` in ASA Version 8.4(1) und höher ersetzt, wie hier gezeigt:

```
webvpn
anyconnect ssl keepalive 15
anyconnect dpd-interval client 5
anyconnect dpd-interval gateway 5
```

## Probleme bei der Weiterleitung von Datenverkehr

Wenn Probleme beim Weiterleiten des Datenverkehrs an das private Netzwerk mit einer AnyConnect-Sitzung über die ASA festgestellt werden, führen Sie die folgenden Schritte zur Datensammlung aus:

1. Rufen Sie die Ausgabe des Befehls `show vpn-sessiondb detail svc filtername <username>` ASA von der Konsole ab. Wenn die Ausgabe angezeigt wird `Filter Name: XXXXX`, und sammeln Sie dann die Ausgabe für `show access-list XXXXX`. Stellen Sie sicher, dass die Zugriffsliste XXXXX den beabsichtigten Datenverkehrsfluss nicht blockiert.
2. Exportieren Sie die AnyConnect-Statistiken aus **AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt)**.
3. Suchen Sie in der ASA-Konfigurationsdatei nach `nat`-Anweisungen. Wenn Network Address Translation (NAT) aktiviert ist, müssen diese Daten ausnehmen, die nach NAT an den Client



zurückkehren. Um beispielsweise die IP-Adressen aus dem AnyConnect-Pool von NAT (nat 0) auszunehmen, verwenden Sie dies in der CLI:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Bestimmen Sie, ob das getunnelte Standardgateway für die Einrichtung aktiviert werden muss. Das herkömmliche Standard-Gateway ist das Gateway letzter Instanz für nicht entschlüsselten Datenverkehr.

Beispiel:

```
!--- Route outside 0 0 is an incorrect statement.
```

```
route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

Wenn beispielsweise der VPN-Client auf eine Ressource zugreifen muss, die nicht in der Routing-Tabelle des VPN-Gateways enthalten ist, wird das Paket über das Standard-Gateway weitergeleitet. Das VPN-Gateway benötigt zur Lösung dieses Problems keine vollständige interne Routing-Tabelle. Das **getunnelte** Schlüsselwort kann in dieser Instanz verwendet werden.

5. Überprüfen Sie, ob der AnyConnect-Datenverkehr durch die Überprüfungsrichtlinie der ASA verworfen wird. Wenn Sie das modulare Richtlinien-Framework der Cisco ASA implementieren, können Sie die spezifische Anwendung ausnehmen, die vom AnyConnect-Client verwendet wird. Beispielsweise können Sie das Skinny-Protokoll mit diesen Befehlen ausnehmen.

```
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect skinny
```

## Absturzfehler bei AnyConnect

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das Microsoft-Dienstprogramm Dr. Watson aktiviert ist. Wählen Sie dazu **Start > Ausführen**, und führen Sie **Drwtsn32.exe** aus. Konfigurieren Sie dies, und klicken Sie auf **OK**:

```
Number of Instructions      : 25
Number of Errors To Save  : 25
Crash Dump Type           : Mini
```

Dump Symbol Table : Checked  
Dump All Thread Contexts : Checked  
Append To Existing Log File : Checked  
Visual Notification : Checked  
Create Crash Dump File : Checked

Wenn der Absturz auftritt, sammeln Sie die Dateien **.log** und **.dmp** unter **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr**. Wenn diese Dateien scheinbar verwendet werden, verwenden Sie **ntbackup.exe**.

2. Rufen Sie das Cisco AnyConnect VPN Client-Protokoll in der Windows Event Viewer des Client-PCs ab:

Wählen Sie **Start > Ausführen aus**.

Eingabe:

```
eventvwr.msc /s
```

Klicken Sie mit der rechten Maustaste auf das Protokoll **Cisco AnyConnect VPN Client**, und wählen Sie Protokolldatei als **AnyConnect.evt** speichern aus.

**Hinweis:** Speichern Sie die Datei immer im Format **.evt**.

## Fragmentierung/Übergeben von Datenverkehrsproblemen

Einige Anwendungen, z. B. Microsoft Outlook, funktionieren nicht. Der Tunnel ist jedoch in der Lage, anderen Verkehr, wie z. B. kleine Pings, zu passieren.

Dies kann Hinweise auf ein Fragmentierungsproblem im Netzwerk liefern. Die Fragmentierung und Reassemblierung von Paketen durch Consumer-Router ist besonders gering.

Testen Sie eine Skalierung von Pings, um festzustellen, ob diese bei einer bestimmten Größe fehlschlagen. Beispiel: ping -l 500, ping -l 1000, ping -l 1500, ping -l 2000.

Es wird empfohlen, eine spezielle Gruppe für Benutzer zu konfigurieren, die fragmentiert sind, und die SVC Maximum Transition Unit (MTU) für diese Gruppe auf 1200 festzulegen. Auf diese Weise können Sie Benutzer beseitigen, die dieses Problem haben, sich jedoch nicht auf die breitere Benutzerbasis auswirken.

### Problem

TCP-Verbindungen hängen, sobald sie mit AnyConnect verbunden sind.

### Lösung

Um zu überprüfen, ob Ihr Benutzer ein Fragmentierungsproblem hat, passen Sie die MTU für AnyConnect-Clients auf der ASA an.

```
ASA(config)#group-policy <name> attributes
webvpn
svc mtu 1200
```

## Automatische Deinstallation

### Problem

Der AnyConnect VPN Client wird nach Beendigung der Verbindung deinstalliert. Die Client-Protokolle zeigen an, dass die installierte Komponente deaktiviert ist.

### Lösung

AnyConnect deinstalliert sich selbst, obwohl die Option **Keep installed** im Adaptive Security Device Manager (ASDM) aktiviert ist. Um dieses Problem zu beheben, konfigurieren Sie den Befehl **svc Keep-installer installed** unter group-policy.

## Problem bei der Eingabe des Cluster-FQDN

**Problem: Der AnyConnect-Client wird mit dem Hostnamen anstelle des FQDN (Fully Qualified Domain Name) des Clusters vorab ausgefüllt.**

Wenn ein Load Balancing-Cluster für SSL VPN eingerichtet ist und der Client versucht, eine Verbindung zum Cluster herzustellen, wird die Anforderung an den Knoten ASA umgeleitet, und der Client meldet sich erfolgreich an. Nach einiger Zeit, wenn der Client erneut versucht, eine Verbindung zum Cluster herzustellen, wird der Cluster-FQDN nicht mehr in den Einträgen **Verbinden mit** angezeigt. Stattdessen wird der Knoten-ASA-Eintrag angezeigt, zu dem der Client umgeleitet wurde.

### Lösung

Dies liegt daran, dass der AnyConnect-Client den Hostnamen behält, mit dem er zuletzt verbunden wurde. Dieses Verhalten wird beobachtet, und es wurde ein Fehler gemeldet. Vollständige Details zum Fehler finden Sie unter Cisco Bug ID [CSCsz39019](#). Als Problemumgehung wird ein Upgrade von Cisco AnyConnect auf Version 2.5 vorgeschlagen.

## Konfiguration der Sicherungsserverliste

Für den Fall, dass der vom Benutzer ausgewählte Hauptserver nicht erreichbar ist, wird eine Liste der Backup-Server konfiguriert. Dies wird im Bereich **Backup-Server** im AnyConnect-Profil definiert. Gehen Sie wie folgt vor:

1. Laden Sie den [AnyConnect Profile Editor herunter](#) (nur [registrierte](#) Kunden). Der Dateiname ist **AnyConnectProfileEditor2\_4\_1.jar**.
2. Erstellen Sie mit dem AnyConnect Profile Editor eine XML-Datei.

Öffnen Sie die Registerkarte Serverliste.

Klicken Sie auf **Hinzufügen**.

Geben Sie den Hauptserver in das Feld **Hostname ein**.

Fügen Sie den Backup-Server unter der Liste der Backup-Server im Feld **Host-Adresse** hinzu. Klicken Sie anschließend auf **Hinzufügen**.

3. Sobald Sie die XML-Datei haben, müssen Sie sie der Verbindung zuweisen, die Sie auf der ASA verwenden.

Wählen Sie im ASDM **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles (Konfiguration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile** aus.

Wählen Sie Ihr Profil aus, und klicken Sie auf **Bearbeiten**.

Klicken Sie im Abschnitt "Richtlinie der Standardgruppe" auf **Verwalten**.

Wählen Sie Ihre Gruppenrichtlinie aus, und klicken Sie auf **Bearbeiten**.

Wählen Sie **Erweitert** aus, und klicken Sie dann auf **SSL VPN Client**.

Klicken Sie auf **Neu**. Anschließend müssen Sie einen Namen für das Profil eingeben und die XML-Datei zuweisen.

4. Verbinden Sie den Client mit der Sitzung, um die XML-Datei herunterzuladen.

## AnyConnect: Beschädigtes Problem mit der Treiberdatenbank

Dieser Eintrag in der Datei SetupAPI.log legt nahe, dass das Katalogsystem beschädigt ist:

W239-Klassenliste für Treibersignierung "C:\WINDOWS\INF\certclas.inf" was missing or invalid.  
Error 0xfffffde5: Unknown Error., vorausgesetzt, alle Geräteklassen unterliegen der Richtlinie für die Treibersignierung.

Sie können auch die folgende Fehlermeldung erhalten: **Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue.**

Sie können dieses Protokoll auf dem Client erhalten: **"The VPN client driver has encountered an error"**.

### Reparatur

Dieses Problem beruht auf der Cisco Bug-ID [CSCsm54689](#). Um dieses Problem zu beheben, stellen Sie sicher, dass der Routing- und Remote-Zugriffsdienst deaktiviert ist, bevor Sie AnyConnect starten. Wenn das Problem dadurch nicht behoben wird, gehen Sie wie folgt vor:

1. Öffnen Sie auf dem PC eine Eingabeaufforderung als Administrator (erhöhte Eingabeaufforderung unter Vista).

2. Ausführen `net stop CryptSvc`.

3. Ausführen:

```
esentutl /p%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

4. Wenn Sie dazu aufgefordert werden, wählen Sie **OK**, um die Reparatur durchzuführen.

5. Beenden Sie die Eingabeaufforderung.

6. Neustart.

## Fehlgeschlagene Reparatur

Wenn die Reparatur fehlschlägt, gehen Sie wie folgt vor:

1. Öffnen Sie auf dem PC eine Eingabeaufforderung als Administrator (erhöhte Eingabeaufforderung unter Vista).

2. Ausführen `net stop CryptSvc`.

3. Benennen Sie das Verzeichnis `%WINDIR%\system32\catroot2` to `catroot2_old` um.

4. Beenden Sie die Eingabeaufforderung.

5. Neustart.

## Analyse der Datenbank

Sie können die Datenbank jederzeit analysieren, um festzustellen, ob sie gültig ist.

1. Öffnen Sie eine Eingabeaufforderung als Administrator auf dem PC.

2. Ausführen:

```
esentutl /g%systemroot%\System32\catroot2\  
{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb
```

Weitere Informationen finden Sie unter [Systemkatalog-Datenbankintegrität](#).

## Fehlermeldungen

**Fehler: Die Sitzungsverwaltungsdatenbank kann nicht aktualisiert werden.**

Während das SSL VPN über einen Webbrowser verbunden ist, `Unable to Update the Session Management Database`. **Fehlermeldung** wird angezeigt, und die ASA-Protokolle werden angezeigt. `%ASA-3-211001: Memory allocation Error. The adaptive security appliance failed to allocate RAM system memory.`

## Lösung 1

Dieses Problem beruht auf der Cisco Bug-ID [CSCsm51093](#). Um dieses Problem zu beheben, laden Sie die ASA-Software neu oder aktualisieren Sie die ASA-Software auf die im Fehler erwähnte Interimsversion. Siehe Cisco Bug ID [CSCsm51093](#) für weitere Informationen.

## Lösung 2

Dieses Problem kann auch gelöst werden, wenn Sie die Erkennung von Sicherheitsrisiken auf ASA deaktivieren, wenn die Bedrohungserkennung verwendet wird.

## Fehler: "Modul c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll konnte nicht registriert werden."

Wenn Sie den AnyConnect-Client auf Laptops oder PCs verwenden, tritt während der Installation ein Fehler auf:

```
"Module C:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register..."
```

Wenn dieser Fehler auftritt, kann das Installationsprogramm nicht fortfahren, und der Client wird entfernt.

## Lösung

Die folgenden Problemumgehungen können zur Behebung dieses Fehlers durchgeführt werden:

- Der neueste AnyConnect-Client wird von Microsoft Windows 2000 offiziell nicht mehr unterstützt. Es handelt sich um ein Registrierungsproblem mit dem 2000-Computer. Weitere Informationen finden Sie im Abschnitt [Windows-Anforderungen](#) in den [AnyConnect-Versionshinweisen](#).
- Entfernen Sie die VMware-Anwendungen. Nach der Installation von AnyConnect können VMware-Anwendungen wieder zum PC hinzugefügt werden.
- Fügen Sie die ASA ihren vertrauenswürdigen Sites hinzu. Weitere Informationen finden Sie im Abschnitt [Sicherheitsappliance zur Liste der vertrauenswürdigen Sites](#) in den Versionshinweisen zu AnyConnect.
- Kopieren Sie diese Dateien aus dem Ordner `\ProgramFiles\Cisco\CiscoAnyconnect` in einen neuen Ordner und führen Sie die Eingabeaufforderung `regsvr32 vpnapi.dll` aus:

```
vpnapi.dll\npncommon.dll\npncommoncrypt.dll
```

- Erstellen Sie ein neues Image des Betriebssystems auf dem Laptop/PC.

Die Protokollmeldung bezüglich dieses Fehlers auf dem AnyConnect-Client sieht ähnlich aus wie folgt:

```
DEBUG: Error 2911: Could not remove the folderC:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
DEBUG: Error 2911: Could not remove the folder C:\Program Files\Cisco\Cisco AnyConnect
VPN Client\.
The installer has encountered an unexpected error installing this package. This may
indicate a problem with this package. The error code is 2911. The arguments are:
C:\Program Files\Cisco\Cisco AnyConnect VPN Client\, ,
Info 1721. There is a problem with this Windows Installer package. A program required for
this install to complete could not be run. Contact your support personnel or package
vendor. Action: InstallHelper.exe, location: C:\Program Files\Cisco\Cisco AnyConnect VPN
Client\InstallHelper.exe, command: -acl "C:\Documents and Settings\All Users\Application
Data\Cisco\Cisco AnyConnect VPN Client\\" -r
```

**Fehler: "Beim sicheren Gateway wurde ein Fehler als Antwort auf die VPN-Aushandlungsanfrage gemeldet. Wenden Sie sich an Ihren Netzwerkadministrator."**

Wenn Clients versuchen, eine Verbindung zum VPN mit dem Cisco AnyConnect VPN Client herzustellen, wird dieser Fehler ausgegeben.

Diese Nachricht wurde vom sicheren Gateway empfangen:

"Illegal address class" oder "Host or network is 0" oder "Other error" (Anderer Fehler)

## Lösung

Das Problem tritt aufgrund der Erschöpfung des lokalen ASA-IP-Pools auf. Wenn die VPN-Poolressource ausgeschöpft ist, muss der IP-Poolbereich vergrößert werden.

Die Cisco Bug-ID lautet [CSCsl82188](#). Sie wurde zur Behebung dieses Problems gespeichert. Dieser Fehler tritt in der Regel auf, wenn der lokale Pool für die Adresszuweisung erschöpft ist oder eine 32-Bit-Subnetzmaske für den Adresspool verwendet wird. Die Problemumgehung besteht darin, den Adresspool zu erweitern und eine 24-Bit-Subnetzmaske für den Pool zu verwenden.

**Fehler: Die Sitzung konnte nicht eingerichtet werden. Sitzungslimit von 2 wurde erreicht.**

Wenn Sie versuchen, mehr als zwei Clients mit dem AnyConnect VPN Client zu verbinden, erhalten Sie die `Login Failed` Fehlermeldung auf dem Client und eine Warnmeldung in den ASA-Protokollen, die den Status angibt `session could not be established. session limit of 2 reached`. Ich habe die **grundlegende AnyConnect-Lizenz** auf der ASA, die Version **8.0.4** ausführt.

## Lösung 1

Dieser Fehler tritt auf, weil die **grundlegende** Lizenz für **AnyConnect** nicht von der ASA Version 8.0.4 unterstützt wird. Sie müssen ein Upgrade der ASA auf Version 8.2.2 durchführen. Dadurch

wird der Fehler behoben.

**Hinweis:** Unabhängig von der verwendeten Lizenz erhält der Benutzer bei Erreichen des Sitzungslimits die `login failed` Fehlermeldung.

## Lösung 2

Dieser Fehler kann auch auftreten, wenn der Befehl [vpn-sessiondb max-anyconnect-Premium-or-essentials-limit session-limit](#) verwendet wird, um die zulässige Grenze für VPN-Sitzungen festzulegen. Wenn die Sitzungsbeschränkung auf zwei festgelegt ist, kann der Benutzer nicht mehr als zwei Sitzungen einrichten, obwohl die installierte Lizenz mehr Sitzungen unterstützt. Legen Sie das Sitzungslimit auf die Anzahl der erforderlichen VPN-Sitzungen fest, um diese Fehlermeldung zu vermeiden.

## Fehler: AnyConnect ist auf dem VPN-Server nicht aktiviert, wenn versucht wird, eine Verbindung mit der ASA herzustellen

Sie erhalten `anyconnect not enabled on VPN server` Fehlermeldung beim Versuch, AnyConnect mit der ASA zu verbinden.

## Lösung

Dieser Fehler wird behoben, wenn Sie AnyConnect auf der externen Schnittstelle der ASA mit ASDM aktivieren. Weitere Informationen zum Aktivieren von AnyConnect auf der externen Schnittstelle finden Sie unter [Aktivieren des SSL VPN Client Protocol](#).

## Fehler:- %ASA-6-722036: Gruppen-Client-Gruppe Benutzer xxxx IP x.x.x.x Senden eines großen Pakets 1220 (Schwellenwert 1206)

Die `%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x > Transmitting large packet 1220 (threshold 1206)` In den Protokollen der ASA wird eine Fehlermeldung angezeigt. Was bedeutet dieses Protokoll und wie wird es aufgelöst?

## Lösung

In dieser Protokollmeldung wird angegeben, dass ein großes Paket an den Client gesendet wurde. Die Paketquelle kennt die MTU des Clients nicht. Dies kann auch durch die Komprimierung nicht komprimierbarer Daten erfolgen. Die Lösung besteht darin, die SVC-Komprimierung mit dem Befehl [svc komprimierung none](#) zu deaktivieren. Dadurch wird das Problem behoben.

## Fehler: Das sichere Gateway hat die VPN-Verbindungs- oder Verbindungsanforderung des Agenten abgelehnt.

Wenn Sie eine Verbindung mit dem AnyConnect-Client herstellen, tritt dieser Fehler auf: `"The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires re-authentication and must be started manually. Please contact your network administrator if this problem persists. The following message was received from the secure gateway: no assigned address"`.



Dieser Fehler wird auch bei der Verbindung mit dem AnyConnect-Client angezeigt: "The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication. The following message was received from the secure gateway: Host or network is 0".

Dieser Fehler wird auch bei der Verbindung mit dem AnyConnect-Client angezeigt: "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License".

## Lösung

Nach dem Neuladen fehlte dem Router die Pool-Konfiguration. Sie müssen die betreffende Konfiguration wieder zum Router hinzufügen.

```
Router#show run | in pool
```

```
ip local pool SSLPOOL 192.168.30.2 192.168.30.254  
svc address-pool SSLPOO
```

Die "The secure gateway has rejected the agent's vpn connect or reconnect request. A new connection requires a re-authentication and must be started manually. Please contact the network administrator if the problem persists. The following message was received from the secure gateway: No License" tritt ein, wenn die AnyConnect-Mobilitätslizenz fehlt. Sobald die Lizenz installiert ist, wird das Problem behoben.

## Fehler: "Sitzungsmanagement-Datenbank konnte nicht aktualisiert werden"

Wenn Sie versuchen, sich in WebPortal zu authentifizieren, wird folgende Fehlermeldung angezeigt: "Unable to update the session management database".

## Lösung

Dieses Problem betrifft die Speicherzuweisung auf der ASA. Dieses Problem tritt am häufigsten auf, wenn die ASA-Version 8.2.1 ist. Ursprünglich ist hierfür ein 512 MB RAM erforderlich. Weitere Informationen finden Sie im Abschnitt [Speicheranforderungen](#) in den Versionshinweisen.

Als permanente Problemumgehung sollten Sie den Speicher auf 512 MB aufrüsten. Sie können die ["Memory Upgrade Kits"](#) bestellen.

Versuchen Sie, den Speicher als temporäre Problemumgehung mit den folgenden Schritten freizugeben:

1. Deaktivieren Sie die Bedrohungserkennung.
2. Deaktivieren Sie die SVC-Komprimierung.
3. Laden Sie die ASA neu.

## Fehler: "Beim VPN-Client-Treiber ist ein Fehler aufgetreten."

Dies ist eine Fehlermeldung, die auf dem Client-Computer beim Verbindungsversuch mit AnyConnect angezeigt wird.

## Lösung

Führen Sie zur Behebung dieses Fehlers dieses Verfahrens aus, um den AnyConnect VPN-Agenten manuell auf Interaktiv zu setzen:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz > Verwalten > Dienste und Anwendungen > Dienste** > und wählen Sie Cisco AnyConnect VPN Agent aus.
2. Klicken Sie mit der rechten Maustaste auf **Eigenschaften**, melden Sie sich dann an, und wählen Sie **Service zur Interaktion mit dem Desktop zulassen aus**.

Damit wird der Registrierungstyp-Wert DWORD für die HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent auf 110 (Standardwert ist 010) festgelegt.

**Hinweis:** Wenn dies verwendet werden soll, wird die **.MST**-Transformation in dieser Instanz bevorzugt. Dies liegt daran, dass diese Methode bei manueller Einstellung nach jedem Installations-/Upgrade-Prozess festgelegt werden muss. Aus diesem Grund muss die Anwendung identifiziert werden, die dieses Problem verursacht.

Wenn der Routing and Remote Access Service (RRAS) auf dem Windows-PC aktiviert ist, schlägt AnyConnect mit dem `The VPN client driver has encountered an error.` Fehlermeldung. Um dieses Problem zu beheben, stellen Sie sicher, dass Routing und RRAS deaktiviert sind, bevor Sie AnyConnect starten. Weitere Informationen finden Sie unter Cisco Bug ID [CSCsm54689](#).

## Fehler: "Antwort von xxx.xxx.xxx.xxx kann nicht verarbeitet werden."

AnyConnect-Clients können keine Verbindung zu einer Cisco ASA herstellen. Der Fehler im Fenster AnyConnect ist "unable to process response from xxx.xxx.xxx.xxx".

## Lösung

Um diesen Fehler zu beheben, versuchen Sie die folgenden Problemumgehungen:

- Entfernen Sie WebVPN von der ASA, und aktivieren Sie es erneut.<
- Ändern Sie die Port-Nummer des vorhandenen 443 in 444, und aktivieren Sie sie auf 443 erneut.

Weitere Informationen zum Aktivieren von WebVPN und Ändern des Ports für WebVPN finden Sie in dieser [Lösung](#).

## Fehler: "Anmelden verweigert, unberechtigter Verbindungsmechanismus, wenden Sie sich an Ihren Administrator."

AnyConnect-Clients können keine Verbindung zu einer Cisco ASA herstellen. Der Fehler im Fenster AnyConnect ist "Login Denied , unauthorized connection mechanism , contact your administrator".

## Lösung

Diese Fehlermeldung tritt hauptsächlich aufgrund von Konfigurationsproblemen auf, die nicht korrekt oder unvollständig sind. Überprüfen Sie die Konfiguration, und vergewissern Sie sich, dass sie zur Lösung des Problems erforderlich ist.

<

## Fehler: "AnyConnect-Paket nicht verfügbar oder beschädigt. Wenden Sie sich an Ihren Systemadministrator"

Dieser Fehler tritt auf, wenn Sie versuchen, die AnyConnect-Software von einem Macintosh-Client aus zu starten, um eine Verbindung zu einer ASA herzustellen.

## Lösung

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Laden Sie das Macintosh AnyConnect-Paket in den Flash-Speicher der ASA. Weitere Informationen hierzu finden Sie unter [Uploading AnyConnect image](#).
2. Ändern Sie die WebVPN-Konfiguration, um das verwendete AnyConnect-Paket anzugeben.

```
webvpn
svc image disk0:/anyconnect-macosx-i386-2.3.2016-k9.pkg 2
svc image disk0:/anyconnect-macosx-powerpc-2.3.2016-k9.pkg 3
```

Der Befehl **svc image** wird durch den Befehl **anyconnect image** in ASA Version 8.4(1) und höher ersetzt, wie hier gezeigt:

```
hostname(config)#webvpn

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-win-3.0.0527-k9.pkg 1

hostname(config-webvpn)#anyconnect image disk0:/
anyconnect-macosx-i386-3.0.0414-k9.pkg 2
```

## Fehler: "Das AnyConnect-Paket am sicheren Gateway konnte nicht gefunden werden."

Dieser Fehler wird auf dem Linux-Computer des Benutzers verursacht, wenn er versucht, eine Verbindung zur ASA herzustellen, indem er AnyConnect startet. Die vollständige Fehlermeldung lautet:

"The AnyConnect package on the secure gateway could not be located. You may be experiencing network connectivity issues. Please try connecting again."

## Lösung

Um diese Fehlermeldung zu beheben, überprüfen Sie, ob das auf dem Client-Computer verwendete Betriebssystem vom AnyConnect-Client unterstützt wird. Vollständige Informationen zur unterstützten Software finden Sie im Abschnitt [Systemanforderungen](#) in den [AnyConnect-Versionshinweisen](#).

Wenn das Betriebssystem unterstützt wird, überprüfen Sie, ob das AnyConnect-Paket in der WebVPN-Konfiguration angegeben ist. Weitere Informationen finden Sie im Abschnitt [AnyConnect-Paket nicht verfügbar oder beschädigt](#) in diesem Dokument.

## Fehler: "Sicheres VPN über Remote-Desktop wird nicht unterstützt."

Benutzer können keinen Remotedesktopzugriff durchführen. Die `secure VPN via remote desktop is not supported` Fehlermeldung wird angezeigt.

## Lösung

Dieses Problem beruht auf den folgenden Cisco Bug-IDs: [CSCsu22088](#) und [CSCso42825](#). Wenn Sie ein Upgrade des AnyConnect VPN Client durchführen, kann das Problem dadurch gelöst werden. Weitere Informationen finden Sie in diesen Bugs.

## Fehler: "Das empfangene Serverzertifikat oder seine Kette erfüllt nicht FIPS. Eine VPN-Verbindung wird nicht hergestellt."

Wenn Sie versuchen, eine VPN-Verbindung zur ASA 5505 herzustellen, `The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established` Fehlermeldung wird angezeigt.

## Lösung

Um diesen Fehler zu beheben, müssen Sie die Federal Information Processing Standards (FIPS) in der Datei **AnyConnect Local Policy** deaktivieren. Diese Datei finden Sie in der Regel unter `C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml`. Wenn diese Datei nicht in diesem Pfad gefunden wird, suchen Sie die Datei in einem anderen Verzeichnis mit einem Pfad wie `c:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml`. Wenn Sie die XML-Datei gefunden haben, nehmen Sie Änderungen an dieser Datei vor, wie hier gezeigt:

Ändern Sie die Wortgruppe:

```
<fipsMode>true</fipsMode>
```

An:

```
<FipsMode>>false</FipsMode>
```

Starten Sie anschließend den Computer neu. Benutzer müssen über Administratorberechtigungen

verfügen, um diese Datei zu ändern.

## Fehler: "Fehler bei der Zertifikatsvalidierung"

Benutzer können AnyConnect nicht starten und die `certificate validation failure` Fehler.

### Lösung

Die Zertifikatsauthentifizierung funktioniert mit AnyConnect anders als mit dem IPSec-Client. Damit die Zertifikatsauthentifizierung funktioniert, müssen Sie das Clientzertifikat in Ihren Browser importieren und das Verbindungsprofil ändern, um die Zertifikatsauthentifizierung zu verwenden. Sie müssen diesen Befehl auch auf Ihrer ASA aktivieren, damit SSL-Client-Zertifikate auf der externen Schnittstelle verwendet werden können:

### SSL-Schnittstelle zur Zertifikatsauthentifizierung außerhalb des Ports 443

Weitere Informationen zu diesem Befehl finden Sie unter [SSL-Zertifikatsauthentifizierung](#).

## Fehler: "Der VPN Agent Service hat ein Problem festgestellt und muss geschlossen werden. Wir entschuldigen uns für die Unannehmlichkeiten."

Wenn AnyConnect Version 2.4.0202 auf einem Windows XP-PC installiert ist, wird die Aktualisierung der Lokalisierungsdateien beendet, und eine Fehlermeldung zeigt, dass die Datei `vpnagent.exe` fehlschlägt.

### Lösung

Dieses Verhalten wird in der Cisco Bug-ID [CSCsq49102](#) protokolliert. Als Problemumgehung wird empfohlen, den Citrix-Client zu deaktivieren.

## Fehler: "Dieses Installationspaket konnte nicht geöffnet werden. Überprüfen, ob das Paket vorhanden ist"

Beim Herunterladen von AnyConnect wird die folgende Fehlermeldung angezeigt:

```
"Contact your system administrator. The installer failed with the following error: This installation package could not be opened. Verify that the package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer package."
```

### Lösung

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Entfernen Sie alle Virenschutzsoftware.
2. Deaktivieren Sie die Windows-Firewall.
3. Wenn weder Schritt 1 noch 2 helfen, formatieren Sie den Computer und installieren Sie ihn anschließend.

4. Wenn das Problem weiterhin besteht, öffnen Sie ein [TAC-Ticket](#).

## **Fehler: "Fehler beim Anwenden von Transformationen. Überprüfen Sie, ob die angegebenen Transformationspfade gültig sind."**

Diese Fehlermeldung wird beim automatischen Herunterladen von AnyConnect von der ASA erhalten:

```
"Contact your system administrator. The installer failed with the following error:  
Error applying transforms. Verify that the specified transform paths are valid."
```

Dies ist die Fehlermeldung, die bei der Verbindung mit AnyConnect für MacOS angezeigt wird:

```
"The AnyConnect package on the secure gateway could not be located. You may be  
experiencing network connectivity issues. Please try connecting again."
```

## **Lösung**

Führen Sie eine der folgenden Workarounds aus, um dieses Problem zu beheben:

1. Die Ursache für diesen Fehler kann eine beschädigte MST-Übersetzungsdatei (z. B. importiert) sein. Führen Sie folgende Schritte aus, um dies zu beheben:

Entfernen Sie die MST-Übersetzungstabelle.

Konfigurieren Sie das AnyConnect-Image für MacOS in der ASA.

2. Folgen Sie im ASDM dem Pfad **Network (Client) Access > AnyConnect Custom > Install** und löschen Sie die AnyConnect-Paketdatei. Stellen Sie sicher, dass das Paket im **Netzwerk-(Client-)Zugriff > Erweitert > SSL VPN > Client Setting** verbleibt.

Wenn das Problem durch keines dieser Workarounds behoben wird, wenden Sie sich an den [technischen Support von Cisco](#).

## **Fehler: "Beim VPN-Client-Treiber ist ein Fehler aufgetreten."**

Dieser Fehler wird ausgegeben:

```
The VPN client driver has encountered an error when connecting through Cisco  
AnyConnect Client.
```

## **Lösung**

Dieses Problem kann behoben werden, wenn Sie den AnyConnect Client deinstallieren und anschließend die Virenschutzsoftware entfernen. Installieren Sie anschließend den AnyConnect Client neu. Wenn diese Auflösung nicht funktioniert, formatieren Sie den PC neu, um dieses Problem zu beheben.

## **Fehler: "Eine VPN-Verbindung führte zu unterschiedlichen Konfigurationseinstellungen. Die VPN-Netzwerkeinstellung wird neu initialisiert."**

## Anwendungen, die das private Netzwerk nutzen, müssen möglicherweise wiederhergestellt werden."

Dieser Fehler wird beim Start von AnyConnect angezeigt:

```
"A VPN reconnect resulted in different configuration setting. The VPN network setting is being re-initialized. Applications utilizing the private network may need to be restarted."
```

### Lösung

Verwenden Sie zur Behebung dieses Fehlers Folgendes:

```
group-policy <Name> attributes
webvpn
svc mtu 1200
```

Der Befehl **svc mtu** wird durch den Befehl **anyconnect mtu** in ASA Version 8.4(1) und höher ersetzt, wie hier gezeigt:

```
hostname(config) #group-policy
```

```
hostname(config-group-policy) #webvpn
```

```
hostname(config-group-webvpn) #anyconnect mtu 500
```

## AnyConnect-Fehler bei der Anmeldung

### Problem

Der AnyConnect erhält diesen Fehler, wenn er eine Verbindung zum Client herstellt:

```
The VPN connection is not allowed via a local proxy. This can be changed through AnyConnect profile settings.
```

### Lösung

Das Problem kann behoben werden, wenn Sie die folgenden Änderungen am AnyConnect-Profil vornehmen:

Fügen Sie diese Zeile dem AnyConnect-Profil hinzu:

```
<ProxySettings>IgnoreProxy</ProxySettings><
AllowLocalProxyConnections>
false</AllowLocalProxyConnections>
```

**Die IE-Proxy-Einstellung wird nach der Trennung von AnyConnect unter Windows 7 nicht wiederhergestellt.**

## Problem

Wenn in Windows 7 die IE-Proxy-Einstellung für **automatische Erkennung von Einstellungen** konfiguriert ist und AnyConnect eine neue Proxy-Einstellung nach unten drückt, wird die IE-Proxy-Einstellung nicht wieder auf **Einstellungen** nach dem Beenden der AnyConnect-Sitzung **automatisch erkannt**. Dies verursacht LAN-Probleme für Benutzer, die ihre Proxy-Einstellung für die **automatische Erkennung von Einstellungen** konfigurieren müssen.

## Lösung

Dieses Verhalten wird in der Cisco Bug-ID [CSCtj51376](#) protokolliert. Als Problemumgehung wird ein Upgrade auf [AnyConnect 3.0](#) empfohlen.

## Fehler: AnyConnect Essentials kann erst aktiviert werden, wenn alle Sitzungen geschlossen sind.

Diese Fehlermeldung wird auf dem Cisco ASDM angezeigt, wenn Sie versuchen, die AnyConnect Essentials-Lizenz zu aktivieren:

```
There are currently 2 clientless SSL VPN sessions in progress. AnyConnect Essentials can not be enabled until all these sessions are closed.
```

## Lösung

Dies ist das normale Verhalten der ASA. AnyConnect Essentials ist ein separat lizenzierter SSL VPN-Client. Sie ist vollständig auf der ASA konfiguriert und bietet die vollständige AnyConnect-Funktion mit folgenden Ausnahmen:

- Kein Cisco Secure Desktop (CSD) (einschließlich HostScan/Vault/Cache Cleaner)
- Kein Clientless-SSL-VPN
- Optionale Windows Mobile-Unterstützung

Diese Lizenz kann nicht gleichzeitig mit der gemeinsam genutzten SSL VPN Premium-Lizenz verwendet werden. Wenn Sie eine Lizenz verwenden möchten, müssen Sie die andere deaktivieren.

## Fehler: Die Verbindungsregisterkarte in der Internetoption von Internet Explorer verbirgt sich nach dem Herstellen der Verbindung mit dem AnyConnect-Client.

Die **Verbindungsregisterkarte** auf der **Internetoption** von Internet Explorer verbirgt sich, nachdem Sie mit dem AnyConnect-Client verbunden sind.

## Lösung

Dies liegt an der [msie-proxy-Sperrfunktion](#). Wenn Sie diese Funktion aktivieren, wird die Registerkarte Verbindungen in Microsoft Internet Explorer für die Dauer einer AnyConnect VPN-Sitzung ausgeblendet. Wenn Sie die Funktion deaktivieren, bleibt die Anzeige der Registerkarte Verbindungen unverändert.



**Fehler: Nur wenige Benutzer erhalten die Meldung "Login Failed" (Anmeldung fehlgeschlagen), wenn andere Benutzer erfolgreich eine Verbindung über AnyConnect VPN herstellen können.**

Einige Benutzer erhalten die Meldung "Login Failed" (Anmeldung fehlgeschlagen), wenn andere Benutzer erfolgreich über das AnyConnect VPN eine Verbindung herstellen können.

## Lösung

Dieses Problem kann behoben werden, wenn Sie sicherstellen, dass das Kontrollkästchen für die Benutzer **keine Vorabauthentifizierung erfordert** aktiviert ist.

**Fehler: Das angezeigte Zertifikat stimmt nicht mit dem Namen der Website überein, die Sie anzeigen möchten.**

Beim Update des AnyConnect-Profiles wird ein Fehler angezeigt, der besagt, dass das Zertifikat ungültig ist. Dies geschieht nur bei Windows und während der Profilaktualisierungsphase. Die Fehlermeldung wird hier angezeigt:

```
The certificate you are viewing does not match with the name of the site you are trying to view.
```

## Lösung

Dies kann aufgelöst werden, wenn Sie die Serverliste des AnyConnect-Profiles ändern, um den FQDN des Zertifikats zu verwenden.

Dies ist ein Beispiel für das XML-Profil:

```
<ServerList>
```

```
<HostEntry>
```

```
<HostName>vpn1.ccsd.net</HostName>
```

```
</HostEntry>
```

```
</ServerList>
```

**Hinweis:** Wenn ein vorhandener Eintrag für die öffentliche IP-Adresse des Servers vorhanden ist, z. B. entfernen und nur den FQDN des Servers beibehalten (z. B. aber nicht ).

**AnyConnect kann vom CSD-Vault eines Windows 7-Computers nicht gestartet werden**

Wenn AnyConnect vom CSD-Tresor gestartet wird, funktioniert es nicht. Dies wird auf Windows 7-Computern versucht.

## Lösung

Derzeit ist dies nicht möglich, da es nicht unterstützt wird.

## Das AnyConnect-Profil wird nach dem Failover nicht auf den Standby-Modus repliziert

Der AnyConnect 3.0 VPN-Client mit der Software ASA Version 8.4.1 funktioniert einwandfrei. Nach dem Failover gibt es jedoch keine Replikation für die Konfiguration des AnyConnect-Profiles.

### Lösung

Dieses Problem wurde unter der Cisco Bug-ID [CSCtn71662](#) beobachtet und protokolliert. Die temporäre Problemumgehung besteht darin, die Dateien manuell auf die Standby-Einheit zu kopieren.

## Der AnyConnect-Client stürzt ab, wenn Internet Explorer offline geht

In diesem Fall enthält das AnyConnect-Ereignisprotokoll ähnliche Einträge:

```
Description : Function:
CAdapterNetworkStateIfc::SetConnectedStateToConnected
File: .\AdapterNetworkStateIfc.cpp
Line: 147
Invoked Function: InternetSetOption
Return Code: 12010 (0x00002EEA)
Description: The length is incorrect for the option type
```

```
Description : Function: CTransportWinHttp::InitTransport
File: .\CTransportWinHttp.cpp
Line: 252
Invoked Function: CConnectedStateIfc::SetConnectedStateToConnected
Return Code: -25362420 (0xFE7D000C)
Description: CADAPTERNETWORKSTATEIFC_ERROR_SET_OPTION
```

### Lösung

Dieses Verhalten wird unter der Cisco Bug-ID [CSCtx28970](#) beobachtet und protokolliert. Um dies zu beheben, beenden Sie die AnyConnect-Anwendung, und starten Sie erneut. Die Verbindungseinträge werden nach dem Neustart erneut angezeigt.

## Fehlermeldung: TLSPROTOCOL\_ERROR\_INSUFFICIENT\_BUFFER

Der AnyConnect-Client kann keine Verbindung herstellen, und der `unable to establish a connection` Fehlermeldung wird empfangen. Im AnyConnect-Ereignisprotokoll `TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER` Fehler gefunden.

### Lösung

Dies geschieht, wenn das Headend für Split-Tunneling mit einer sehr großen Split-Tunnel-Liste konfiguriert ist (ca. 180-200 Einträge) und ein oder mehrere andere Clientattribute in der Gruppenrichtlinie konfiguriert werden, z. B. dns-server.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Reduzieren Sie die Anzahl der Einträge in der Split-Tunnel-Liste.
2. Verwenden Sie diese Konfiguration, um DTLS zu deaktivieren:

```
group-policy groupName attributes
webvpn
svc dtls none
```

Weitere Informationen finden Sie unter Cisco Bug ID [CSCtc41770](#).

## Fehlermeldung: "Verbindungsversuch ist aufgrund eines ungültigen Hosteintrags fehlgeschlagen."

Die `connection attempt has failed due to invalid host entry` wird eine Fehlermeldung angezeigt, während AnyConnect mithilfe eines Zertifikats authentifiziert wird.

### Lösung

Um dieses Problem zu beheben, versuchen Sie eine der folgenden möglichen Lösungen:

- Aktualisieren Sie AnyConnect auf Version 3.0.
- Deaktivieren Sie Cisco Secure Desktop auf Ihrem Computer.

Weitere Informationen finden Sie unter Cisco Bug ID [CSCti73316](#).

## Fehler: "Stellen Sie sicher, dass Ihre Serverzertifikate den strikten Modus befolgen können, wenn Sie ein stets verfügbares VPN konfigurieren."

Wenn Sie die Always-On-Funktion auf AnyConnect aktivieren, `Ensure your server certificates can pass strict mode if you configure always-on VPN` Fehlermeldung wird empfangen.

### Lösung

Diese Fehlermeldung impliziert, dass Sie, wenn Sie die Always-On-Funktion verwenden möchten, ein gültiges Serverzertifikat benötigen, das auf dem Headend konfiguriert ist. Ohne ein gültiges Serverzertifikat funktioniert diese Funktion nicht. Der strikte Zertifikatmodus ist eine Option, die Sie in der lokalen AnyConnect-Richtliniendatei festlegen, um sicherzustellen, dass die Verbindungen ein gültiges Zertifikat verwenden. Wenn Sie diese Option in der Richtliniendatei aktivieren und eine Verbindung mit einem Scheinzertifikat herstellen, schlägt die Verbindung fehl.

## Fehler: "In Microsoft Windows HTTP Services ist ein interner Fehler aufgetreten."

Dieses Diagnostic AnyConnect Reporting Tool (DART) zeigt einen fehlgeschlagenen Versuch:

```
*****
```

```
Date : 03/25/2014
Time : 09:52:21
Type : Error
Source : acvpnui
```

```
Description : Function: CTransportWinHttp::SendRequest
```

File: .\CTransportWinHttp.cpp  
Line: 1170  
**Invoked Function: HttpSendRequest**  
Return Code: 12004 (0x00002EE4)  
Description: **An internal error occurred in the Microsoft Windows HTTP Services**  
\*\*\*\*\*  
Date : 03/25/2014  
Time : 09:52:21  
Type : Error  
Source : acvpnui

Description : Function: ConnectIfc::connect  
File: .\ConnectIfc.cpp  
Line: 472  
Invoked Function: ConnectIfc::sendRequest  
Return Code: -30015443 (0xFE36002D)  
Description: CTRANSPORT\_ERROR\_CONN\_UNKNOWN  
\*\*\*\*\*  
Date : 03/25/2014  
Time : 09:52:21  
Type : Error  
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode  
File: .\ConnectIfc.cpp  
Line: 2999  
Invoked Function: ConnectIfc::TranslateStatusCode  
Return Code: -30015443 (0xFE36002D)  
Description: CTRANSPORT\_ERROR\_CONN\_UNKNOWN  
**Connection attempt failed. Please try again.**

\*\*\*\*\*

Weitere Informationen finden Sie in den Ereignisanzeige-Protokollen auf dem Windows-Computer.

## Lösung

Dies kann durch eine beschädigte Winsock-Verbindung verursacht werden. Setzen Sie die Verbindung mithilfe dieses Befehls von der Eingabeaufforderung zurück, und starten Sie den Windows-Computer neu:

### Winsock-Reset

Weitere Informationen finden Sie im Artikel [How to determine and to restore from Winsock2 Korruption in Windows Server 2003, in Windows XP und in Windows Vista](#) Knowledge Base ([So ermitteln und beheben Sie die Fehler in Windows Server 2003 und Windows Vista](#)).

**Fehler: "Beim SSL-Transport ist ein sicherer Kanalfehler aufgetreten. Möglich ist dies durch eine nicht unterstützte Verschlüsselungskonfiguration auf dem Secure Gateway."**

Dieses Diagnostic AnyConnect Reporting Tool (DART) zeigt einen fehlgeschlagenen Versuch:

\*\*\*\*\*  
Date : 10/27/2014  
Time : 16:29:09  
Type : Error

Source : acvpnui

Description : Function: CTransportWinHttp::handleRequestError  
File: .\CTransportWinHttp.cpp  
Line: 854

The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto configuration on the Secure Gateway.

\*\*\*\*\*

Date : 10/27/2014  
Time : 16:29:09  
Type : Error  
Source : acvpnui

Description : Function: CTransportWinHttp::SendRequest  
File: .\CTransportWinHttp.cpp  
Line: 1199

Invoked Function: CTransportWinHttp::handleRequestError  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE

\*\*\*\*\*

Date : 10/27/2014  
Time : 16:29:09  
Type : Error  
Source : acvpnui

Description : Function: ConnectIfc::TranslateStatusCode  
File: .\ConnectIfc.cpp  
Line: 3026

Invoked Function: ConnectIfc::TranslateStatusCode  
Return Code: -30015418 (0xFE360046)  
Description: CTRANSPORT\_ERROR\_SECURE\_CHANNEL\_FAILURE  
Connection attempt failed. Please try again.

\*\*\*\*\*

## Lösung

Windows 8.1 unterstützt RC4 gemäß dem folgenden KB-Update nicht:

<http://support2.microsoft.com/kb/2868725>

Konfigurieren Sie entweder DES/3DES-Verschlüsselungen für SSL VPN auf der ASA mithilfe des Befehls "ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1", ODER bearbeiten Sie die Windows-Registrierungsdatei auf dem Client-Computer wie unten beschrieben:

<https://technet.microsoft.com/en-us/library/dn303404.aspx>

## Zugehörige Informationen

- [Cisco Adaptive Security Appliances der Serie ASA 5500](#)
- [Häufig gestellte Fragen zum AnyConnect VPN-Client](#)
- [Häufig gestellte Fragen zu Cisco Secure Desktop \(CSD\)](#)
- [Cisco AnyConnect VPN-Client](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)