Troubleshoot Cisco Secure Client VPN Common Problems

Contents

- Introduction
- Prerequisites
  - Requirements
  - Components Used
- Troubleshoot Process
- Gather Information for Troubleshooting
  - Client — Statistics and DART
  - Headend — ASA
  - Headend — FTD
  - Installation and Virtual Adapter Issues
  - Disconnection or Inability to Establish Initial Connection
  - Problems with Passing Traffic
  - AnyConnect Crash Issues
  - Fragmentation / Passing Traffic Issues
  - Uninstall Automatically
  - Issue Populating the Cluster FQDN
  - Backup Server List Configuration
- Cisco Secure Client: Corrupt Driver Database Issue
  - Repair
  - Failed Repair
  - Analyze the Database
- Error Messages
  - Error: Unable to Update the Session Management Database
  - Solution 1
  - Solution 2
  - Error: "Module failed to register" during Cisco Secure Client install
  - Solution
  - Error: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator"
  - Solution
  - Error: AnyConnect not enabled on VPN server while trying to connect anyconnect to ASA
  - Solution
  - Error:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)
  - Solution
  - Error: The secure gateway has rejected the agent's vpn connect or reconnect request.
  - Solution
  - Error: "The VPN client driver has encountered an error"

Solution

Error: "Unable to process response from xxx.xxx.xxx.xxx"

Solution

Error: "Login Denied, unauthorized connection mechanism, contact your administrator"

Solution

Error: "Anyconnect package unavailable or corrupted. Contact your system administrator"

Solution

Error: "The AnyConnect package on the secure gateway could not be located"

Solution

Error: "Secure VPN via remote desktop is not supported"

Solution

Error: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"

Solution

Error: "Certificate Validation Failure"

Solution

Error: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience"

Solution

Error: "This installation package could not be opened. Verify that the package exists"

Solution

Error: "Error applying transforms. Verify that the specified transform paths are valid."

Solution

Error: "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 restored."

Solution

Cisco Secure Client Error While Logging In

Solution

Error: AnyConnect Essentials can not be enabled until all these sessions are closed.

Solution

Error: Few users getting Login Failed Error message when others are able to connect successfully through AnyConnect VPN

Solution

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

Solution

AnyConnect Profile Does Not Get Replicated to the Standby After Failover

Solution

Error Message: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Solution

Error Message: "Connection attempt has failed due to invalid host entry"

Solution

Error: "Ensure your server certificates can pass strict mode if you configure always-on VPN"

Solution

Error: "An internal error occurred in the Microsoft Windows HTTP Services"

Solution

Error: "The SSL transport received a Secure Channel Failure. May be a result of a unsupported crypto

configuration on the Secure Gateway."

Solution

Related Information

Introduction

This document describes Cisco Secure Client issues with app failures and disconnects on Windows, macOS, and Linux.

Prerequisites

Requirements

Before you use this document, ensure that you have:

- **Cisco Secure Client 5.x** on the endpoint (or the version your headend supports).
- Ability to collect a **DART** bundle or client logs.
- Administrative access to the VPN headend (ASA or FTD).

Components Used

The information in this document is based on:

- **Client:** Cisco Secure Client 5.x (AnyConnect VPN module).
- **Headend:** Cisco ASA 9.x or Cisco Secure Firewall Threat Defense (FTD) with Remote Access VPN.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Review the Troubleshoot Cisco Secure Client in the product administrator guide.

Troubleshoot Process

This document details Cisco Secure Client VPN issues (including AnyConnect) including application failures, unexpected disconnects, and common errors on Windows, macOS, Linux, and Cisco ASA/FTD headend configurations.

- Applications that do not work through the VPN tunnel.
- Clients connect/disconnect unexpectedly.

- Common error messages appearing on the client or headend.

This covers the VPN client on Windows, macOS, and Linux including headend configuration on Cisco ASA and Cisco Secure Firewall Threat Defense (FTD) Remote Access. VPN.



Tip: Before troubleshooting, collect a Cisco Secure Client DART bundle. You can analyze DART outputs with the DART Analyser BDB task.

Review these sections to address common problems and solutions:

- Gather Information for Troubleshooting
- Installation and Virtual Adapter Issues
- Disconnection or Inability to Establish Initial Connection
- Problems with Passing Traffic
- AnyConnect Crash Issues
- Fragmentation / Passing Traffic Issues
- Uninstall Automatically
- Issue Populating the Cluster FQDN
- Backup Server List Configuration

Gather Information for Troubleshooting

Collect client and headend data before you change configuration. TAC typically requests a **DART** bundle.

Client — Statistics and DART

1. **Export Connection Statistics**
   - **Windows: Gear Icon > Advanced Window > Statistics > AnyConnect VPN > Export Stats**
   - **macOS: Statistics Icon > Export Stats**
   - **Linux: Details** on the client GUI
2. **Run DART**
   - **Windows / Linux: Gear Icon > Advanced Window > Diagnostics**
   - **macOS: Application Menu > Generate Diagnostic Report**

   Attach the bundle to your TAC case or use **Upload to TAC** with the SR number and token.
3. **Embedded browser issues: Advanced Window > General > Web Browser > Clear Data**.

Headend — ASA

- **show running-config**
- **show vpn-sessiondb detail anyconnect filter name <username>**
- Debug example:

```
configure terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

Reproduce the failure, capture output, then **no logging enable**.

Headend — FTD

From FMC/CDO, export Remote Access VPN policy and connection profile settings. Collect FTD SSL VPN / connection logs for the failure window.

Installation and Virtual Adapter Issues

If installation or virtual adapter setup fails, collect:

1. **Windows setup logs:**

```
%SystemRoot%\Inf\setupapi.dev.log
%SystemRoot%\Inf\setupapi.setup.log
```

2. **MSI installer log: %LOCALAPPDATA%\Temp** or **%SystemRoot%\Temp** — filename **cisco-secure-client-win-*-install-*.log** (most recent for your version).
3. **Verbose MSI (if needed):**

```
msiexec /i cisco-secure-client-win-<version>-predeploy-k9.msi /lvx %TEMP%\ac-install.log
```

4. **System info: msinfo32 /nfo %TEMP%\msinfo.nfo** and **systeminfo > %TEMP%\sysinfo.txt**

For driver database errors, see Cisco Secure Client: Corrupt Driver Database Issue and the administrator guide section **VPN Client Driver Encounters Error (after a Microsoft Windows Update)**.

Disconnection or Inability to Establish Initial Connection

If you experience connection problems with the **Cisco Secure Client**, collect data per Gather Information for Troubleshooting before changing the configuration.

- **Headend Configuration: show running-config** or export policy from FMC/CDO for FTD.
- **Client Logs:** Collect a **DART** bundle (see Gather Information). Do not rely on the legacy Event Viewer **.evt** exports.
- **ASA Debug (if needed):** Enable **logging class auth**, **webvpn**, **ssl**, and **anyconnect** at debugging;

reproduce the failure; capture console output; then **no logging enable**.

If the user cannot connect, the issue can be related to Remote Desktop Protocol (RDP) or Fast User Switching. The user can see: **AnyConnect profile settings mandate a single local user, but multiple local users are currently logged into your computer. A VPN connection cannot be established**.

Disconnect the RDP session(s) and disable Fast User Switching. **Multiple simultaneous local users are not supported** on the same machine for VPN establishment.

Note: Ensure Port 443 (and UDP 443 for DTLS) is not blocked so the client can reach the headend.

When a user cannot connect, the issue can be caused by incompatibility between the **Cisco Secure Client** version and the headend software. The user can receive: **The installer was not able to start the Cisco VPN client, clientless access is not available**. Upgrade the client to a version supported by your ASA or FTD Remote Access VPN deployment.

When you log in the first time to Cisco Secure Client, the log in script can have issues. If you disconnect and log in again, the login script often runs as expected. This can be expected behavior depending on the profile and script timing.

When you connect, you can receive: **User not authorized for AnyConnect Client access, contact your administrator**. This is often seen when the Secure Client image is missing on the headend. Upload the correct client image and reference it in the RA VPN / WebVPN configuration.

DART can show **TUNNELPROTOCOLDPDMGR_ERROR_NO_DPD_RESPONSE** when the DTLS channel is torn down due to Dead Peer Detection (DPD) failure. Tune keepalives on ASA:

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

Disable DTLS only as a temporary test (ASDM: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**, uncheck **Enable DTLS**, or FMC equivalent). Prefer fixing DPD timing and allowing UDP 443.

Problems with Passing Traffic

When problems are detected with passing traffic to the private network with a Cisco Secure Client session through the ASA, complete these data-gathering steps:

1. Obtain the output of **show vpn-sessiondb detail anyconnect filter name <username>** from the ASA console. If the output shows **Filter Name: XXXXX**, gather **show access-list XXXXX**. Verify the

access list does not block intended traffic.

2. Export connection statistics: **Cisco Secure Client > Gear > Advanced Window > Statistics > AnyConnect VPN > Export Stats**.

3. Check the ASA configuration for **nat** statements. If Network Address Translation (NAT) is enabled, exempt traffic that returns to the client. Example to NAT-exempt an AnyConnect pool:

```
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. Determine if the tunneled default gateway must be enabled. Example:

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

   If the client must reach resources not in the VPN gateway routing table, the **tunneled** keyword routes that traffic through the VPN tunnel.

5. Verify whether the inspection policy drops application traffic. You can exempt a protocol under the Modular Policy Framework. Example for skinny:

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

AnyConnect Crash Issues

Complete these data-gathering steps:

1. Collect **DART** immediately after the crash.
2. Note Windows Error Reporting entries for **vpnagent.exe** / **acvpnui.exe**.
3. Client logs: **%LOCALAPPDATA%\Cisco\Cisco Secure Client\Logs** (verify the path for your version).

Fragmentation / Passing Traffic Issues

Some applications, such as Microsoft Outlook, do not work while the tunnel passes smaller traffic like small pings. This can indicate fragmentation on the path. Consumer routers are often poor at fragmentation and reassembly.

Try a scaling set of pings: **ping -l 500**, **ping -l 1000**, **ping -l 1500**, **ping -l 2000**.

Configure a dedicated group policy for affected users and set a lower MTU:

```
group-policy <name> attributes
 webvpn
  anyconnect mtu 1200
```

Uninstall Automatically

Problem

Cisco Secure Client uninstalls itself after the connection terminates even though **keep installed** appears selected in ASDM/FMC.

Solution

```
group-policy <name> attributes
 webvpn
  anyconnect keep-installer installed
```

Issue Populating the Cluster FQDN

Problem: AnyConnect client is pre-populated with the hostname instead of the cluster Fully Qualified Domain Name (FQDN).

When you have a load-balancing cluster for SSL VPN and the client connects, the request can redirect to a cluster node and login succeeds. On a later connect attempt, the cluster FQDN does not appear in **Connect to**; the last node hostname can appear instead.

Solution

The client caches the last successful hostname. Clear cached entries or set the cluster FQDN in the profile server list. Verify on **Cisco Secure Client 5.x**. See Cisco bug ID CSCsz39019 for platform-specific notes.

Backup Server List Configuration

A backup server list is configured when the primary server is unreachable. Define it in the **Backup Server** pane of the client profile. Complete these steps:

1. Edit the profile with the **Profile Editor** from your headend Secure Client package or per the Secure Client 5.1 Profile Configuration Guide. Assign the profile in ASDM or FMC.

2. Create or edit the XML profile:
    1. Go to the server list tab.
    2. Click **Add**.
    3. Enter the primary server **Hostname**.
    4. Add backup servers under the backup server list, then click **Add**.
3. Assign the profile to the connection on the ASA:
    1. In ASDM: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.
    2. Select your profile and click **Edit**.
    3. Click **Manage** from the Default Group Policy section.
    4. Select your group-policy and click **Edit**.
    5. Select **Advanced** and then **SSL VPN Client**.
    6. Click **New**, name the profile, and assign the XML file.
4. Connect the client to download the profile.

Cisco Secure Client: Corrupt Driver Database Issue

This entry in the SetupAPI.log file suggests the catalog system is corrupt:

W239 driver signing class list **"C:\WINDOWS\INF\certclas.inf" was missing or invalid. Error 0xfffffde5: Unknown Error.**, assuming all device classes are subject to the driver signing policy. You can also receive: **Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue**.

And you can receive this log on the client: **"The VPN client driver has encountered an error".**

Repair

This issue is related to Cisco bug ID CSCsm54689. Disable Routing and Remote Access Service (RRAS) before starting Cisco Secure Client. If the issue persists:

1. Open a command prompt as **Administrator** on Windows.

2. Run **net stop CryptSvc**.

3. Run:

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

4. When prompted, choose **OK** to attempt the repair.
5. Exit the command prompt.

6. Reboot.

Failed Repair

If the repair fails:

1. Open a command prompt as **Administrator** on Windows.
2. Run **net stop CryptSvc**.
3. Rename **%WINDIR%\system32\catroot2** to **catroot2_old**.
4. Exit the command prompt.
5. Reboot.

Analyze the Database

You can analyze the database at any time to determine if it is valid.

1. Open a command prompt as **Administrator** on Windows.
2. Run:

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

Refer to System Catalog Database Integrity for more information.

Error Messages

Error: Unable to Update the Session Management Database

This error can appear during browser-based SSL VPN or Web Portal authentication. The client or portal shows **Unable to Update the Session Management Database**. The ASA can log **%ASA-3-211001: Memory allocation Error. The adaptive security appliance failed to allocate RAM system memory.**

Solution 1

Related to Cisco bug ID CSCsm51093. Reload the ASA or upgrade to a fixed release per the bug. On FTD,

verify the platform memory and RA VPN session limits.

Solution 2

Free headend memory:

1. Disable the threat-detection if enabled.
2. Disable AnyConnect compression: **anyconnect compression none** under the group-policy **webvpn** section.
3. Reload the ASA.
4. On older ASA platforms with 256 MB RAM, upgrade to 512 MB if memory exhaustion persists.

Error: "Module failed to register" during Cisco Secure Client install

During installation on Windows, the installer reports that a module (for example **vpnapi.dll**) failed to register and rolls back.

Solution

- Remove conflicting VMware virtual network adapters temporarily; reinstall Secure Client; add VMware back.
- Add the headend FQDN to trusted sites if using web deploy.
- From **C:\Program Files\Cisco\Cisco Secure Client**, run elevated: **regsvr32 vpnapi.dll** (and **vpncommon.dll**, **vpncommoncrypt.dll** if present).
- Collect MSI verbose log (see Installation section) and DART if the install still fails.
- As a last resort, repair Windows or redeploy from a clean Secure Client uninstall.

Error: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator"

When clients connect with **Cisco Secure Client**, the gateway returns an error such as **"Illegal address class"**, **"Host or network is 0"**, or **"Other error"**.

Solution

The ASA or FTD local IP pool is exhausted or misconfigured. Expand the VPN address pool and use an appropriate mask (for example /24 instead of a /32-only pool). See Cisco bug ID CSCsl82188.

Error: AnyConnect not enabled on VPN server while trying to connect anyconnect to ASA

The client reports that AnyConnect / Secure Client is not enabled on the VPN server.

Solution

Enable Remote Access VPN and deploy a Secure Client image on the headend. On ASA: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**. On FTD: configure RA VPN and client image in FMC. Use a Remote Access VPN guide — not clientless WebVPN-only configuration.

Error:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

The **%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)** message appears in ASA logs.

Solution

A large packet was sent to the client (MTU or non-compressible data). Disable the compression for the group policy:

```
group-policy <name> attributes
 webvpn
  anyconnect compression none
```

Error: The secure gateway has rejected the agent's vpn connect or reconnect request.

Examples include **no assigned address**, **Host or network is 0**, or **No License** in the gateway message.

Solution

Verify the headend has a configured IP local pool and group-policy address assignment after reload or failover:

```
show running-config | include pool
ip local pool SSLPOOL 192.168.30.2 192.168.30.254
 anyconnect address-pool SSLPOOL
```

For **No License**, install or enable the required Secure Client mobility license on the headend.

Error: "The VPN client driver has encountered an error"

Usually, the virtual adapter failure, RRAS conflict, or post–Windows Update driver issue.

Solution

1. Disable **Routing and Remote Access Service (RRAS)** before starting Secure Client.
2. Complete the Cisco Secure Client: Corrupt Driver Database Issue steps if the setupapi shows catalog errors.
3. After the Windows Update, use **Repair VPN Client Driver Error** in the Secure Client 5.1 Administrator Guide.
4. Collect DART and contact TAC if needed. See Cisco bug ID CSCsm54689.

Error: "Unable to process response from xxx.xxx.xxx.xxx"

The Cisco Secure Client fails to connect with **Unable to process response from <gateway>**.

Solution

- Disable and reenable Remote Access VPN / WebVPN on the affected interface.
- Temporarily move the SSL VPN to another Port (for example 444), then restore 443.

See SSL VPN client configuration on ASA. Collect DART if the error persists.

Error: "Login Denied, unauthorized connection mechanism, contact your administrator"

Cisco Secure Client shows **Login Denied, unauthorized connection mechanism, contact your administrator**.

Solution

Review the connection profile and authentication on the headend (ASA or FTD). Ensure the client auth method (RADIUS, SAML, certificate, and so on) matches the profile. Verify the group-policy and tunnel-group assignment.

Error: "Anyconnect package unavailable or corrupted. Contact your system administrator"

This error can appear when launching **Cisco Secure Client** from a Macintosh client.

Solution

1. Upload the macOS Secure Client package to headend flash.
2. Reference it on the WebVPN configuration:

```
webvpn
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

Error: "The AnyConnect package on the secure gateway could not be located"

On Linux (or other platforms), the client cannot download the package from the headend.

<#root>

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

Solution

Verify the client OS is supported and the correct image is configured on the headend:

```
webvpn
 anyconnect image disk0:/cisco-secure-client-win-<version>-predeploy-k9.pkg 1
 anyconnect image disk0:/cisco-secure-client-macos-<version>-predeploy-k9.pkg 2
```

See AnyConnect Package Unavailable or Corrupted for the related steps.

Error: "Secure VPN via remote desktop is not supported"

Users see **Secure VPN via remote desktop is not supported**.

Solution

Upgrade to a supported **Cisco Secure Client 5.x** release. See Cisco bug ID CSCsu22088 and Cisco bug ID CSCso42825.

Error: "The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established"

The client reports the server certificate or chain does not comply with FIPS.

Solution

If FIPS is required on the endpoint, use the FIPS-compliant certificates on the headend. If it is not required, edit the **C:\ProgramData\Cisco\Cisco Secure Client\AnyConnectLocalPolicy.xml** and set **<FipsMode>false</FipsMode>**, then reboot (admin rights required).

Error: "Certificate Validation Failure"

Users cannot launch Cisco Secure Client and receive **Certificate Validation Failure**.

Solution

For certificate authentication, import the client certificate, configure the profile for certificate auth, and on ASA enable:

```
ssl certificate-authentication interface outside port 443
```

Ensure the server certificate matches the FQDN in the profile server list.

Error: "VPN Agent Service has encountered a problem and needs to close. We are sorry for the inconvenience"

The **vpnagent.exe** service fails during install, upgrade, or connect.

Solution

1. Restart **Cisco Secure Client - AnyConnect VPN Agent** in Windows Services.
2. Repair or reinstall from headend web deploy.
3. Collect DART if the service fails repeatedly. For Citrix conflicts, see Cisco bug ID CSCsq49102.

Error: "This installation package could not be opened. Verify that the package exists"

Web deploy fails with a Windows Installer error that the package could not be opened.

Solution

1. Verify the MSI downloaded completely; retry from the headend portal.
2. Temporarily disable aggressive AV on the download folder; collect verbose MSI log.
3. Ensure Windows Installer service is running.
4. If the issue persists, collect DART/MSI logs and open a TAC Case.

Error: "Error applying transforms. Verify that the specified transform paths are valid."

Auto-download from the headend fails, sometimes due to a corrupted MST transform.

Solution

1. Remove the custom MST transform from the headend AnyConnect custom install definition.
2. Re-upload the correct Secure Client image on the headend.
3. In ASDM: **Network (Client) Access > AnyConnect Custom > Installs** — Remove duplicate entries; keep the active image under client settings.

Error: "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 restored."

This message can appear after reconnect when headend Pushed settings change.

Solution

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

Cisco Secure Client Error While Logging In

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

Solution

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

Error: AnyConnect Essentials can not be enabled until all these sessions are closed.

ASDM shows clientless SSL VPN sessions in-progress when enabling AnyConnect Essentials.

Solution

AnyConnect Essentials cannot run concurrently with the premium shared SSL VPN license. End clientless SSL VPN sessions before enabling Essentials. Essentials does not include clientless SSL VPN.

Error: Few users getting Login Failed Error message when others are able to connect successfully through AnyConnect VPN

Some users receive **Login Failed** while others can connect.

Solution

Ensure **do not require pre-authentication** (or equivalent) is set correctly for affected users. Compare group-policy and connection profile mapping.

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

During profile update on Windows, certificate validation fails against the connection URL.

Solution

```
<ServerList>
 <HostEntry>
    <HostName>vpn1.example.com</HostName>
 </HostEntry>
</ServerList>
```



Note: Remove <HostAddress> entries that use the public IP if the certificate is FQDN-only.

AnyConnect Profile Does Not Get Replicated to the Standby After Failover

After ASA failover, Secure Client profile-related files are missing on the standby unit.

Solution

See Cisco bug ID CSCtn71662. Workaround: manually copy profile files to the standby. Verify stateful failover config sync for RA VPN profiles.

Error Message: TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER

Cisco Secure Client fails to connect with **Unable to establish a connection**. The event log shows **TLSPROTOCOL_ERROR_INSUFFICIENT_BUFFER**.

Solution

This occurs with a very large split-tunnel list (approximately 180–200 entries) plus, other group-policy attributes (for example, **dns-server**).

1. Reduce split-tunnel list entries.
2. Temporarily disable DTLS:

```
group-policy groupName attributes
 webvpn
  anyconnect ssl dtls none
```

See Cisco bug ID CSCtc41770.

Error Message: "Connection attempt has failed due to invalid host entry"

Connection attempt has failed due to invalid host entry during certificate authentication.

Solution

- Use a valid **HostName** (FQDN) in the profile server list.
- Use supported **Cisco Secure Client 5.x**.
- Remove deprecated Cisco Secure Desktop (CSD) policy if still present.

See Cisco bug ID CSCti73316.

Error: "Ensure your server certificates can pass strict mode if you configure always-on VPN"

When Always-On is enabled, the client can report that server certificates must pass strict mode.

Solution

Always-On requires a valid headend certificate matching the connection URL. **Strict Certificate Mode** in local policy causes failure if the certificate is untrusted or mismatched.

See **Certified by an Unknown Authority** in the Secure Client 5.1 Administrator Guide.

Error: "An internal error occurred in the Microsoft Windows HTTP Services"

DART can show **HttpSendRequest** failures and **An internal error occurred in the Microsoft Windows HTTP Services** with **CTransportWinHttp** errors.

Solution

This can be caused by corrupted Winsock state. From an elevated command prompt: **netsh winsock reset**

Restart Windows and see Microsoft Guidance on Resetting Winsock.

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

Cisco Secure Client DART can show **CTransportWinHttp** errors and **CTransPORT_ERROR_SECURE_CHANNEL_FAILURE** when TLS or cipher negotiation fails between the client and headend.

Solution

1. On the headend, use **TLS 1.2+** and modern cipher suites only. Do **not** enable DES, 3DES, or RC4.
2. ASA example:

```
ssl cipher tlsv1.2 custom "AES256-GCM-SHA384:AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-R
```

3. Check the server certificate validity and FQDN match.
4. Upgrade the client and headend to supported releases.
5. On Windows, keep Schannel at TLS 1.2+; do not weaken the client crypto for obsolete headends.

Related Information

- Troubleshoot Cisco Secure Client (Administrator Guide 5.1)
- AnyConnect VPN Client Troubleshooting Guide - Common Problems External
- Cisco Secure Client / AnyConnect FAQ