

# ASA 8.x: AnyConnect VPN Client Troubleshooting Tech Note

Document ID: 100597

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### Troubleshooting Process

- 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
- AnyConnect Latency Issues
- Issue Populating the Cluster FQDN
- Backup Server List Configuration

#### AnyConnect: Corrupt Driver Database Issue

- Repair
- If Repair Fails
- Analyze the Database

#### Error Messages

- Error: Unable to Update the Session Management Database
  - Solution 1
  - solution 2
- Error: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"
  - Solution
- Error: "An error was received from the secure gateway in response to the VPN negotiation request. Please contact your network administrator"
  - Solution
- Error: Session could not be established. Session limit of 2 reached.
  - Solution 1
  - Solution 2
- 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: "Unable to update the session management database"
  - 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: "The VPN client driver has encountered an error"

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

AnyConnect Error while login

Solution

IE Proxy setting is not restored after AnyConnect disconnect on Windows 7

Solution

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

Solution

Error: Connection tab on Internet option of Internet Explorer hides after getting connected to the AnyConnect client.

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

Cannot launch AnyConnect from the CSD vault from a Windows 7 machine

Solution

AnyConnect profile not getting replicated to the standby after failover

Solution

Problem: AnyConnect client crashes if Internet Explorer goes offline

Solution

## **Related Information**

# **Introduction**

This troubleshooting scenario applies to applications that do not work through the Cisco AnyConnect VPN Client.

# Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

The information in this document is based on ASA Security Appliance that runs version 8.x.

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, make sure that you understand the potential impact of any command.

## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Troubleshooting Process

This typical troubleshooting scenario applies to applications that do not work through the Cisco AnyConnect VPN Client for end-users with Microsoft Windows-based computers. These sections address and provide solutions to the problems:

- Installation and Virtual Adapter Issues
- Disconnection or Inability to Establish Initial Connection
- Problems with Passing Traffic
- AnyConnect Crash Issues
- Fragmentation / Passing Traffic Issues
- AnyConnect Latency Issues

## Installation and Virtual Adapter Issues

Complete these steps:

1. Obtain the device log file:

- ◆ Windows XP / Windows 2000:

`\windows\setupapi.log`

- ◆ Windows Vista:

**Note:** Hidden folders must be made visible in order to see these files.

`\windows\Inf\setupapi.app.log`

`\windows\Inf\setupapi.dev.log`

If you see errors in the setupapi log file, you can turn up verbosity to 0x2000FFFF as described in this Windows KB article . Note the article says to set it to 0xFFFF, but if you add the high order value of 0x2, it makes the logging faster.

2. Obtain the MSI installer log file:

If this is an initial web deploy install, this log is located in the per-user temp directory.

- ◆ Windows XP / Windows 2000:

```
\Documents and Settings\\Local Settings\Temp\
```

- ◆ Windows Vista:

```
\Users\\AppData\Local\Temp\
```

If this is an automatic upgrade, this log is in the temp directory of the system:

```
\Windows\Temp
```

The filename is in this format:

anyconnect-win-x.x.xxxx-k9-install-yyyyyyyyyyyyyy.log. Obtain the most recent file for the version of the client you want to install. The x.xxxx changes based on the version, such as 2.0.0343, and yyyy-yyyy is the date and time of the install.

3. Obtain the PC system information file:

- a. From a Command Prompt/DOS box, type this:

- ◇ Windows XP / Windows 2000:

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

- ◇ Windows Vista:

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

**Note:** After you type this prompt, wait. It can take between two to five minutes for the file to complete.

- b. Obtain a systeminfo file dump from a Command Prompt:

Windows XP and Windows Vista:

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

See AnyConnect: Corrupt Driver Database Issue in order to debug the driver issue.

## Disconnection or Inability to Establish Initial Connection

If you experience connection problems with the AnyConnect client, such as disconnections or the inability to establish an initial connection, obtain these files:

- The configuration file from the ASA in order to determine if anything in the configuration causes the connection failure:

From the console of the ASA, type `write net x.x.x.x:ASA-Config.txt` where x.x.x.x is the IP address of a TFTP server on the network.

OR

From the console of the ASA, type `show running-config`. Let the configuration complete on the screen, then cut-and-paste to a text editor and save.

- The ASA event logs:

1. In order to enable logging on the ASA for auth, webvpn, ssl, and svc events, issue these CLI commands:

```
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
```

2. Originate an AnyConnect session, and ensure that the failure can be reproduced. Capture the logging output from the console to a text editor and save.
  3. In order to disable logging, issue `no logging enable`.
- The Cisco AnyConnect VPN Client log from the Windows Event Viewer of the client PC:

1. Choose **Start > Run**.
2. Enter:

```
eventvwr.msc /s
```

3. Right-click the **Cisco AnyConnect VPN Client** log, and select Save Log File as **AnyConnect.evt**.

**Note:** Always save it as the **.evt file** format.

If the user cannot connect with the AnyConnect VPN Client, the issue might be related to an established RDP session or Fast User Switching enabled on the client PC. The user can see the 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 error on the client PC. In order to resolve this issue, disconnect any established RDP sessions and disable Fast User Switching.

**Note:** Make sure that port 443 is not blocked so the AnyConnect client can connect to the ASA.

When a user cannot connect the AnyConnect VPN Client to the ASA, the issue might be caused by an incompatibility between the AnyConnect client version and the ASA software image version. In this case, the user receives this error message: The installer was not able to start the Cisco VPN client, clientless access is not available.

In order to resolve this issue, upgrade the AnyConnect client version to be compatible with the ASA software image. In order to verify the compatibility, refer to the Security Appliances and Software Supported section of AnyConnect Client Release notes.

When a user cannot connect to the AnyConnect VPN Client from the PC, the issue can be caused by the Antivirus software present on the PC.

**Note:** AnyConnect must be installed on the computer before you install any third party firewall/anti-virus softwares. If AnyConnect is installed after any third-party firewall/anti-virus softwares, then the AnyConnect will fail to connect. In order to resolve this issue, disable all the features of the personal firewall/AV. Then, make a small change on the AnyConnect virtual adapter and try to re-connect the AnyConnect. For more information, refer to Cisco bug IDs CSCsj91840 (registered customers only) and CSCti16453 (registered customers only).

When you login the first time to the AnyConnect, the login script does not run. If you disconnect and login again, then the login script runs fine. This is the expected behavior.

When you connect the AnyConnect VPN Client to the ASA, you might receive this error: User not authorized for AnyConnect Client access, contact your administrator.

This error is seen when the AnyConnect image is missing from the ASA. Once the image is loaded to the

ASA, AnyConnect can connect without any issues to the ASA.

This error can be resolved by disabling Datagram Transport Layer Security (DTLS). Go to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles** and uncheck the **Enable DTLS** check box. This disables DTLS.

The dartbundle files show this error message when the user gets disconnected:

TUNNELPROTOCOLDPDMGR\_ERROR\_NO\_DPD\_RESPONSE:The secure gateway failed to respond to Dead Peer Detection packets. This error means that the DTLS channel was torn due to dpd failure. This error is resolved by tweaking the dpd keepalives and issuing these commands:

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

The **svc keepalive** and **svc dpd-interval** commands are replaced by the **anyconnect keepalive** and **anyconnect dpd-interval** commands respectively in ASA version 8.4(1) and later as shown here:

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

## Problems with Passing Traffic

When problems are detected with passing traffic to the private network with an AnyConnect session through the ASA, complete these data gathering steps:

1. Obtain the output of the **show vpn-sessiondb detail svc filter name <username>** ASA command from the console. If the output shows **Filter Name: XXXXX**, then gather the output for **show access-list XXXXX**. Verify that the access-list XXXXX does not block the intended traffic flow.
2. Export the AnyConnect statistics from AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt).
3. Check the ASA configuration file for **nat** statements. If NAT is enabled, these must exempt data that returns to the client as a result of NAT. For example, to NAT exempt (nat 0) the IP addresses from the AnyConnect pool, use this on the 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. Determine if the tunneled default gateway needs to be enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic.

### Example

```
!--- 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
```

For example, if the VPN Client needs to access a resource which is not in the routing table of the VPN Gateway, the packet is routed through the standard default gateway. The VPN gateway does not need the complete internal routing table in order to resolve this. The **tunneled** keyword can be used in this instance.

5. Verify if the AnyConnect traffic is being dropped by the inspection policy of the ASA. You could exempt the specific application that is used by AnyConnect client by implementing the Modular Policy Framework of Cisco ASA. For example, you could exempt the skinny protocol from exemption using the following commands.

```
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. Ensure that the Microsoft Utility Dr Watson is enabled. In order to do this, choose Start > Run, and run **Drwtsn32.exe**. Configure this and click **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
```

When the crash occurs, gather the .log and .dmp files from **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson**. If these files appear to be in use, then use **ntbackup.exe**.

2. Obtain the Cisco AnyConnect VPN Client log from the Windows Event Viewer of the client PC:
  - a. Choose **Start > Run**.
  - b. Enter:

```
eventvwr.msc /s
```

- c. Right-click the **Cisco AnyConnect VPN Client** log, and select **Save Log File As AnyConnect.evt**.

**Note:** Always save it as the **.evt** file format.

## Fragmentation / Passing Traffic Issues

Some applications, such as Microsoft Outlook, do not work. However, the tunnel is able to pass other traffic such as small pings.

This can provide clues as to a fragmentation issue in the network. Consumer routers are particularly poor at packet fragmentation and re-assembly.

Try a scaling set of pings to see if it fails at a certain size. For example, ping 1 500, ping 1 1000, ping 1 1500, ping 1 2000.

It is recommended that you configure a special group for users that experience fragmentation, and set the **svc mtu** for this group to 1200. This allows you to remediate users who experience this issue, but not impact the broader user base.

**Problem:**

TCP connections hang once connected with AnyConnect.

### **Solution:**

In order to verify if your user has a fragmentation issue, adjust the mtu for AnyConnect clients on the ASA.

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

## **Uninstall Automatically**

### **Problem:**

The AnyConnect VPN Client uninstalls itself once the connection terminates.

The client logs show that keep installed is set to disabled.

### **Solution:**

AnyConnect uninstalls itself despite that the **keep installed** option is selected on the Adaptive Security Device Manager (ASDM). In order to resolve this issue, configure the **svc keep-installer installed** command under group-policy.

## **AnyConnect Latency Issues**

### **Problem:**

Latency issues are seen with the AnyConnect VPN Client.

### **Solution:**

Datagram Transport Layer Security (DTLS) avoids latency and bandwidth problems associated with some SSL-only connections, including AnyConnect connections, and improves the performance of real-time applications that are sensitive to packet delays. DTLS allows the AnyConnect client that establishes an SSL VPN connection to use two simultaneous tunnels, an SSL tunnel and a DTLS tunnel.

If you use DTLS, it avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays. DTLS is a standards-based SSL protocol that provides a low-latency data path that uses UDP. DTLS can be enabled with the **svc dtls enable** command, as shown:

```
hostname(config)#group-policy sales attributes
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)#svc dtls enable
```

Also, if you disable compression and df-bit-ignore, latency and bandwidth problems are reduced. df-bit-ignore can be enabled and compression can be disabled as shown here:

```
hostname(config)#group-policy <name> attributes
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)#svc df-bit-ignore enable
hostname(config-group-webvpn)#svc routing-filtering-ignore enable
hostname(config-group-webvpn)#svc mtu 1200
```

```
hostname(config-group-webvpn)#svc compression none
```

Also, modifying outside ACLs on ASA to allow UDP port 443 will resolve the latency issue.

### **Problem:**

Anyconnect is taking a very long time to connect.

### **Solution:**

The proxy configuration in the browser is a known issue that would cause slowness problems. One of the workarounds is to set the client to ignore it. Enable the "bypass proxy" in the Anyconnect profile so that the problem could be eliminated.

Add the following line to the AnyConnect profile.

```
<ProxySettings>IgnoreProxy</ProxySettings>
```

## **Issue Populating the Cluster FQDN**

**Problem: AnyConnect client is pre-populated with the hostname instead of the cluster fqdn.**

When you have a load balancing cluster set up for SSL VPN and the client attempts to connect to cluster, the request is redirected to the node ASA and the client logs in successfully. After some time, when the client tries again to connect to the cluster, the cluster fqdn is not seen in the "Connect to" entries. Instead, the node ASA entry to which the client has been redirected is seen.

### **Solution**

This occurs because the AnyConnect client is retaining the host name to which it last connected. This behavior is observed and a bug has been filed. For complete details about the bug, refer to Cisco bug ID **CSCsz39019** (registered customers only) . Upgrading the Cisco AnyConnect to 2.5 is the suggested workaround.

## **Backup Server List Configuration**

A backup server list is configured in case the main server selected by the user is not reachable. This is defined in the "Backup Server" pane in the AnyConnect profile. Complete these steps:

1. Download the AnyConnect Profile Editor (registered customers only) . The file name is AnyConnectProfileEditor2\_4\_1.jar.
2. Create an XML file using the AnyConnect Profile Editor.
  - a. Go to the server list tab.
  - b. Click **Add**.
  - c. Type the main server on the *Hostname* field.
  - d. Add the backup server below the backup server list on the *Host address* field. Then, click **Add**.
3. Once you have the XML file, you need to assign it to the connection you are using on the ASA.
  - a. In ASDM, choose **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.
  - b. Select your profile and click **Edit**.
  - c. Click **Manage** from the Default Group Policy section.

- d. Select your group-policy and click **Edit**.
  - e. Select **Advanced** and then click **SSL VPN Client**.
  - f. Click **New**. Then, you need to type a name for the Profile and assign the XML file.
4. Connect the client to the session in order to download the XML file.

## AnyConnect: Corrupt Driver Database Issue

This entry in the SetupAPI.log file suggests that 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 driver
signing policy.
```

You can also receive this error message: Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue.

And this log on the client: "The VPN client driver has encountered an error"

### Repair

This issue is due to Cisco bug ID CSCsm54689 (registered customers only) . In order to resolve this issue, make sure that Routing and Remote Access Service is disabled before you start AnyConnect. If this does not resolve the issue, complete these steps:

1. Open a command prompt as an Administrator on the PC (elevated prompt on Vista).
2. Run `net stop CryptSvc`.
3. Run `esentutl /p`  
`%systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catd`
4. When prompted, choose **OK** to attempt the repair.
5. Exit the command prompt.
6. Reboot.

### If Repair Fails

If the repair fails, complete these steps:

1. Open a command prompt as an Administrator on the PC (elevated prompt on Vista).
2. Run `net stop CryptSvc`.
3. Rename the `%WINDIR%\system32\catroot2` to `catroot2_old` directory.
4. Exit the command prompt.
5. Reboot.

### Analyze the Database

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

1. Open a command prompt as an Administrator on the PC.
2. Run `esentutl /g`  
`%systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catd`

Refer to System Catalog Database Integrity for more information.

**Note:** Refer to asapedia for more information.

# Error Messages

## Error: Unable to Update the Session Management Database

While the SSL VPN is connected through a web browser, the Unable to Update the Session Management Database. error message appears, and the ASA logs show %ASA-3-211001: Memory allocation Error. The adaptive security appliance failed to allocate RAM system memory..

### Solution 1

This issue is due to Cisco bug ID CSCsm51093 (registered customers only) . In order to resolve this issue, reload the ASA or upgrade the ASA software to the interim release mentioned in the bug. Refer to Cisco bug ID CSCsm51093 (registered customers only) for more information.

### solution 2

This issue can also be resolved by disabling threat-detection on ASA if threat-detection is being used.

## Error: "Module c:\Program Files\Cisco\Cisco AnyConnect VPN Client\vpnapi.dll failed to register"

When using the AnyConnect client on laptops or PCs, an error occurs during the install:

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

When this error is encountered, the installer cannot move forward and the client is removed.

### Solution

These are the possible workarounds to resolve this error:

- The latest AnyConnect client is no longer officially supported with Windows 2000. It is a registry problem with the 2000 computer. Refer to the Windows requirements section from the AnyConnect Release Notes.
- Remove the vmware applications. Once AnyConnect is installed, vmware applications can be added back to the PC.
- Add the ASA to their trusted sites. For more information, refer to the Adding Security Appliance to List of Trusted Sites section from the AnyConnect Release Notes.
- Copy these files from the \ProgramFiles\Cisco\CiscoAnyconnect folder to a new folder and run the **regsvr32 vpnapi.dll** command prompt:
  - ◆ vpnapi.dll
  - ◆ vpncommon.dll
  - ◆ vpncommoncrypt.dll
- Re-imaging the operating system on the laptop/PC.

The log message related to this error on the AnyConnect client looks similar to this:

```
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\, ,
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
```

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

When clients try to connect to the VPN using the Cisco AnyConnect VPN Client, this error is received:

This message was received from the secure gateway:

*"Illegal address class" or "Host or network is 0" or "Other error"*

### **Solution**

The issue occurs because of the ASA local IP pool depletion. As the VPN pool resource is exhausted, the IP pool range needs to be enlarged.

A bug is filed for this issue. The Cisco bug ID is CSCsl82188 (registered customers only) . This error usually occurs when the local pool for address assignment is exhausted, or if 32 bit subnet mask is used for the address pool. The workaround is to expand the address pool and use 24 bit subnet mask for the pool.

## **Error: Session could not be established. Session limit of 2 reached.**

When I try to connect more than two clients using the AnyConnect VPN Client, I receive the Login Failed error message on the Client and a warning message in the ASA logs that states `Session could not be established. Session limit of 2 reached`. I have the **AnyConnect essential** license on the ASA, which runs version **8.0.4**.

### **Solution 1**

This error occurs because the **AnyConnect essential** license is not supported by ASA version 8.0.4. You need to upgrade the ASA to version 8.2.2. This resolves the error.

**Note:** Regardless of the license used, if the session limit is reached the user will receive the `login failed` error message.

### **Solution 2**

This error can also occur if the `vpn-sessiondb max-anyconnect-premium-or-essentials-limit session-limit` command is used to set the limit of VPN sessions permitted to be established. If the `session-limit` is set as 2, then the user cannot establish more than two sessions even though the license installed supports more sessions. Set the `session-limit` to the number of VPN sessions required to avoid this error message.

## **Error: Anyconnect not enabled on VPN server while trying to connect anyconnect to ASA**

I receive the Anyconnect not enabled on VPN server error message when trying to connect AnyConnect to the ASA.

### **Solution**

This error is resolved by enabling AnyConnect on the outside interface of the ASA using ASDM. For more information on how to enable AnyConnect on the outside interface, refer to Enabling the SSL VPN Client Protocol.

## **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) error message appears in the logs of the ASA. What does this log mean and how is this resolved?

### **Solution**

This log message states that a large packet was sent to the client. The source of the packet is not aware of the MTU of the client. This can also be due to compression of non-compressible data. The workaround is to turn off the SVC compression with the **svc compression none** command. This resolves the issue.

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

When connecting to the AnyConnect Client, this error is received: "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".

This error is also received when connecting to the AnyConnect Client: "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".

This error is also received when connecting to the AnyConnect Client: "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".

### **Solution**

The router was missing pool configuration after reload. You need to add the concerned configuration back to the router.

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

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

The "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" error occurs when the AnyConnect mobility license is missing. Once the license is installed the issue gets resolved.

## **Error: "Unable to update the session management database"**

When trying to authenticate in WebPortal, this error message is received: "Unable to update the session management database".

### **Solution**

This problem is related to memory allocation on the ASA. This issue is mostly seen when the ASA version is 8.2.1. Originally, this requires a 512MB RAM for its complete functionality. Refer to the Memory requirements section in the release notes.

As a permanent workaround, upgrade the memory to 512MB. You can order the "Memory Upgrade kits".

As a temporary workaround, try to free the memory by performing these steps:

1. Disable the threat-detection.
2. Disable svc compression.
3. Reload the ASA.

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

This is an error message obtained on the client machine when trying to connect to the AnyConnect.

### **Solution**

In order to resolve this error, complete this procedure to manually set the AnyConnect VPN agent to Interactive:

1. Right click on **My Computer > Manage > Services and Applications > Services** > Select the Cisco AnyConnect VPN Agent.
2. Right click **Properties**, then log on and select Allow service to interact with the desktop.

This sets the registry Type value DWORD to 110 (default is 010) for the HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\vpnagent.

**Note:** If this is to be used, then the preference would be to use the .MST transform in this instance. This is because setting this manually using the following methods requires that this be set after every install/upgrade process. Therefore, the need to identify the application that is causing this.

When Routing and Remote Access Service (RRAS) is enabled on the Windows PC, AnyConnect fails with the The VPN client driver has encountered an error. error message. In order to resolve this issue, make sure that Routing and RRAS is disabled before starting AnyConnect.

Refer to Cisco bug ID CSCsm54689 (registered customers only) for more information.

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

AnyConnect clients are failing to connect to a Cisco ASA. The error in the AnyConnect window is "Unable to process response from xxx.xxx.xxx.xxx".

### Solution

In order to resolve this error, try these workarounds:

- Remove the webvpn from the ASA and re-enable it.
- Change the port number to 444 from the existing 443 and re-enable it on 443 again.

For more information on enabling the webvpn and changing the port for webvpn, refer to this Solution.

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

AnyConnect clients are failing to connect to a Cisco ASA. The error in the AnyConnect window is "Login Denied , unauthorized connection mechanism , contact your administrator".

### Solution

This error message occurs mostly because of configuration issues that are improper or an incomplete configuration. Check the configuration and make sure it is as required to resolve the issue.

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

This error occurs when you try to launch the AnyConnect software from a MAC client to connect to an ASA.

### Solution

In order to resolve this, complete these steps:

1. Upload the MAC AnyConnect package to the flash of the ASA. For more information on this, refer to [Uploading AnyConnect image](#).
2. Modify the webvpn configuration to specify the AnyConnect package that will be used.

```
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
```

The **svc image** command is replaced by the **anyconnect image** command in ASA version 8.4(1) and later as shown here:

```
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.p
```

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

This error is caused on the user's linux machine when trying to connect to the ASA by launching AnyConnect. The complete error looks like this:

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

### **Solution**

In order to resolve this error message, verify whether the Operating System (OS) being used on the client machine is supported by the AnyConnect client. For complete information on supported software, refer to the System Requirements section in the AnyConnect Release Notes.

If the OS is supported, then verify if the AnyConnect package is specified in the WebVPN configuration or not. See the Anyconnect package unavailable or corrupted section of this document for more information.

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

Users are unable to perform a remote desktop access. The Secure VPN via remote desktop is not supported error message appears.

### **Solution**

This issue is due to these Cisco bug IDs: CSCsu22088 (registered customers only) and CSCso42825 (registered customers only) . Upgrading the AnyConnect VPN Client can resolve the issue. Refer to these bugs for more information.

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

When attempting to VPN to the ASA 5505, the The server certificate received or its chain does not comply with FIPS. A VPN connection will not be established error message occurs.

### **Solution**

In order to resolve this error, you need to disable the FIPS in the **AnyConnect Local Policy** file. This file can usually be found at C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\AnyConnectLocalPolicy.xml. If this file is not found in this path, then locate the file at a different directory having path such as C:\Documents and Settings\All Users\Application Data\Cisco AnyConnectVPNClient\AnyConnectLocalPolicy.xml. Once you locate the xml file, make changes to this file as shown here:

Change the phrase:

```
<FipsMode>true</FipsMode>
```

To:

`<FipsMode>>false</FipsMode>`

Then, restart the computer. The users will need to have administrative permissions to modify this file.

## **Error: "Certificate Validation Failure"**

Users are unable to launch the AnyConnect and receive the Certificate Validation Failure error.

### **Solution**

Certificate authentication works differently with AnyConnect compared to the IPSec client. In order for certificate authentication to work, you need to import the client certificate to your browser and change the connection profile to use certificate authentication. You also need to enable this command on your ASA to allow SSL client-certificates to be used on the outside interface:

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

For more information about this command, refer to SSL Certificate authentication.

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

When AnyConnect 2.4.0202 is installed on a Windows XP PC, it stops at updating localization files and an error message shows that the vpnagent.exe fails.

### **Solution**

This behavior is logged in Cisco bug ID CSCsq49102 (registered customers only) . The suggested workaround is to disable the Citrix client.

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

When AnyConnect is downloaded, this error message is received:

"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. "

### **Solution**

Complete these steps in order to fix this issue:

1. Remove any anti-virus software.
2. Disable the Windows firewall.
3. If neither step 1 or 2 helps, then format the machine and then install.
4. If the problem still persists, open a TAC Case (registered customers only) .

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

This error message is received during the auto-download of AnyConnect from the ASA:

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

This is the error message received when connecting with AnyConnect for MacOS:

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

## **Solution**

Complete one of these workarounds in order to resolve this issue:

1. The root cause of this error might be due to a corrupted MST translation file (for example, imported). Perform these steps to fix this:
  - a. Remove the MST translation table.
  - b. Configure the AnyConnect image for MacOS in the ASA.
2. From the ASDM, follow the *"Network (Client) Access" > "AnyConnect Custom" > "Installs"* path and delete the AnyConnect package file. Make sure the package remains in *"Network (Client) Access" > "Advanced" > "SSL VPN" > "Client Setting"*.

If neither of these workarounds resolve the issue, contact Cisco TAC (registered customers only) .

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

This error is received:

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

## **Solution**

This issue can be resolved when you uninstall the AnyConnect Client, then remove the anti-virus software. After this, re-install the AnyConnect Client. If this resolution does not work, then reformat the PC in order to fix this issue.

## **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 error is received when trying to launch AnyConnect:

```
"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."
```

## Solution

In order to resolve this error, use this:

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

The **svc mtu** command is replaced by the **anyconnect mtu** command in ASA version 8.4(1) and later as shown here:

```
hostname(config)#group-policy <Name> attributes
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)#anyconnect mtu 500
```

## AnyConnect Error while login

### Problem:

The AnyConnect receives this error when connecting to the Client:

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

## Solution

The issue can be resolved by making these changes to the AnyConnect profile:

Add this line to the AnyConnect profile:

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

## IE Proxy setting is not restored after AnyConnect disconnect on Windows 7

### Problem:

In Windows 7, if the IE proxy setting is configured for **Automatically detect settings** and AnyConnect pushes down a new proxy setting, the IE proxy setting is not restored back to **Automatically detect settings** after the user ends the AnyConnect session. This causes LAN issues for users who need their proxy setting configured for **Automatically detect settings**.

## Solution

This behavior is logged in Cisco bug ID CSCtj51376 (registered customers only) . The suggested workaround is to upgrade to AnyConnect 3.0.

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

This error message is received on Cisco ASDM when attempting to enable the AnyConnect Essentials license:

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

## Solution

This is the normal behavior of the ASA. AnyConnect Essentials is a separately licensed SSL VPN client. It is entirely configured on the ASA and provides the full AnyConnect capability, with these exceptions:

- No CSD (including HostScan/Vault/Cache Cleaner)
- No clientless SSL VPN
- Optional Windows Mobile Support

This license cannot be used at the same time as the shared SSL VPN premium license. When you need to use one license, you need to disable the other.

## Error: Connection tab on Internet option of Internet Explorer hides after getting connected to the AnyConnect client.

The **connection** tab on the **Internet** option of Internet Explorer hides after getting connected to the AnyConnect client.

## Solution

This is due to the msie-proxy lockdown feature. Enabling this feature hides the Connections tab in Microsoft Internet Explorer for the duration of an AnyConnect VPN session. Disabling the feature leaves the display of the Connections tab unchanged.

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

A few users receive the Login Failed Error message when others can connect successfully through the AnyConnect VPN.

## Solution

This issue can be resolved by making sure the **do not require pre-authentication** checkbox is checked for the users.

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

During the AnyConnect profile update, an error is shown that says the certificate is invalid. This occurs with Windows only and at the profile update phase. The error message is shown here:

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

## Solution

This can be resolved by modifying the server list of the AnyConnect profile to use the FQDN of the certificate.

This is a sample of the xml profile:

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

**Note:** If there is an existing entry for the Public IP address of the server such as <HostAddress>, then remove it and retain only the FQDN of the server (for example, <HostName> but not <Host Address>).

## Cannot launch AnyConnect from the CSD vault from a Windows 7 machine

When the AnyConnect is launched from the CSD vault, it does not work. This is attempted on Windows 7 machines.

### Solution

Currently, this is not possible because it is not supported.

## AnyConnect profile not getting replicated to the standby after failover

The AnyConnect 3.0 VPN client with ASA 8.4.1 software works fine. However, after failover, there is no replication for the AnyConnect profile related configuration. How is this resolved?

### Solution

This problem has been observed and logged under Cisco bug ID CSCtn71662 (registered customers only). The temporary workaround is to manually copy the files to the standby unit.

## Problem: AnyConnect client crashes if Internet Explorer goes offline

When this occurs, the AnyConnect event log contains entries similar to these:

```
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
```

## Solution

This behavior is observed and logged under Cisco bug ID CSCtx28970 (registered customers only) . In order to resolve this, quit the AnyConnect application and re-launch. The connection entries reappear after re-launch.

## Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
  - [AnyConnect VPN Client FAQ](#)
  - [Cisco Secure Desktop \(CSD\) FAQ](#)
  - [Cisco AnyConnect VPN Client](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Sep 16, 2011

Document ID: 100597

---