Troubleshoot Cisco Secure Client

Gather Information for Troubleshooting

View Statistical Details

An administrator or end user can view statistical information for a current Cisco Secure Client session.

Procedure

Step 1 On Windows, choose the gear icon on the left of the UI and then navigate to **Advanced Window** > **Statistics** > **AnyConnect VPN drawer**. On macOS, choose the **Statistics** icon next to the gear. On Linux, click the **Details** button on the user GUI.

Step 2 Choose from the following options, depending upon the packages that are loaded on the client computer.

- **Export Stats**—Saves the connection statistics to a text file for later analysis and debugging.
- **Reset**—Resets the connection information to zero so Cisco Secure Client begins collecting new data.
- **Diagnostics**—Launches the Cisco Secure Client Diagnostics and Reporting Tool (DART) wizard which bundles specified log files and diagnostic information for analyzing and debugging the client connection. On macOS, you must choose **Generate Diagnostic Report** from the Cisco Secure Client application menu to start the DART.

Clear Embedded Cache (Windows and macOS)

You can clear embedded cache if you are having issues related to the embedded browser. The Secure Client Web Browser stores information about websites in its cache and cookies. Typically, if you're experiencing issues with website loading or formatting within the Secure Client, clearing its browser cache and cookies may help resolve these problems.

On the Secure Client Advanced Window,

For macOS—Navigate to Statistics > General > Web Browser tab and click **Clear Data**.

For Windows—Navigate to Advanced Window > General > Web Browser tab and click **Clear Data**.

You will see a popup that the browser caches successfully cleared.

Run DART to Gather Data for Troubleshooting

DART is the Cisco Secure Client Diagnostics and Reporting Tool that you can use to collect data for troubleshooting Cisco Secure Client installation and connection problems. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis. Note that by default, data collection is based on U.S. region format (MM/DD/YY).

After the DART bundle collection is completed and collected, you have a choice to **Email Bundle** or **Upload to TAC**. If you choose the Upload to TAC option, you will need to include an SR number (the TAC case number) and a Token, which TAC provides. Then click **Upload to TAC**. The SR number will also be the username when signing in to view the TAC case.

The DART wizard runs on the device that runs Cisco Secure Client. You can launch DART from Cisco Secure Client, or by itself without Cisco Secure Client.

Note DART requires administrator privileges on macOS, Ubuntu 18.04, and Red Hat 7 to collect logs.

Also, for ISE posture only, you can automatically collect DART, if configured, as soon as an ISE posture crash occurs or when an endpoint goes to non-compliant. To enable Auto-DART, set the DARTCount to any non-zero value. When set to 0, the feature is disabled. Enabling Auto-DART prevents data loss due to time lapse. Gather the auto-collected DARTS at the following locations:

- **Windows:** %LocalAppData%\Cisco\Cisco Secure Client
- **macOS:** ~/.cisco/iseposture/log

The following operating systems are supported:

- Windows
- macOS
- Linux

Procedure

Step 1 Launch DART:

- For a Windows device, launch the Cisco Secure Client.
- For a Linux device, choose **Applications** > **Internet** > **Cisco DART**

  or /opt/cisco/anyconnect/dart/dartui.
- For a macOS device, choose **Applications** > **Cisco** > **Cisco DART**

Step 2 Click the gear icon and then **Diagnostics**.

Step 3 Choose **Default** or **Custom** bundle creation.

- Default—Includes the typical log files and diagnostic information, such as the Cisco Secure Client log files, general information about the computer, and a summary of what DART did and did not do. The default name for the bundle is `DARTBundle.zip`, and it is saved to the local desktop.
- Custom—Allows you to specify what files you want to include in the bundle (or the default files) and where to store the bundle.

  Successful route and filtering changes for Linux and macOS will be kept out of the log so that you can better notice important events. Otherwise, with syslog event rate limiting, important events might drop off and be overlooked. Also, capture filtering settings enable you to see the system configuration file for macOS as well as the Cisco Secure Client filtering configuration files. For Linux, iptables and ip6tables outputs are visible in DART even though access to most of these configuration is restricted unless the DART tool is run via sudo.

Note

Default is the only option for macOS. You cannot customize which files to include in the bundle.

Note

If you select **Custom**, you can configure which files to include in the bundle, and specify a different storage location for the file.

Step 4 If DART seems to be taking a long time to gather the default list of files, click **Cancel**, re-run DART, and choose **Custom**, selecting fewer files.

Step 5 If you chose **Default**, DART starts creating the bundle. If you chose **Custom**, continue following the wizard prompts to specify logs, preference files, diagnostic information, and any other customizations.

Expose UDID in DART

Within the DART CLI, you can display the client's unique device identifier (UDID). For example, with Windows, go to the folder containing dartcli.exe (C:\Program Files\Cisco\Cisco Secure Client) and enter **dartcli.exe -u** or **dartclie.exe -udid**.

Collect Logs to Gather Data for Install or Uninstall Issues (for Windows)

If you have an install or uninstall failure with Cisco Secure Client, you need to collect logs, because the DART collection does not have diagnostics for this.

Run the msiexec command in the same directory where you unzipped Cisco Secure Client files:

- For install failures, enter

  ```
  C:\Windows\temp>msiexec /i cisco-secure-client-win-version-predeploy-k9.msi /lvx
  ac-install.log
  ```

  where *ac-install.log* can be a filename of your choice.

- For uninstall failures, enter

  ```
  C:\Windows\temp>msiexec /x cisco-secure-client-win-version-predeploy-k9.msi /lvx
  ac-uninstall.log
  ```

  where *ac-uninstall.log* can be a filename of your choice.

Note For uninstall failures, you should use the MSI specific to the version currently installed.

You can alter the same commands above to capture information about any module on Windows which is not installing or uninstalling correctly.

Get Computer System Info

For Windows type **`msinfo32 /nfo c:\msinfo.nfo`**.

Get Systeminfo File Dump

For Windows use the **`systeminfo`** command to gather info and store it in the txt file `systeminfo > c:\temp\sysinfo.txt`.

Check Registry File

An entry in the SetupAPI log file as below indicates a file cannot be found:

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

Make sure the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce registry key exists. Without this registry key, all INF install packages are forbidden.

Location of Cisco Secure Client Log Files

The logs are retained in the following files:

- Windows—`\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log`

Note In Windows, you must make the hidden files visible.

Because the deployment is manual, you can choose to download the installer file on the web portal and assign your own log filename.

If an upgrade was pushed from the gateway, the log file is in the following location:

```
%WINDIR%\TEMP\cisco-secure-client-win-<version>-core-vpn-webdeploy-k9-install-yyyyyyyyyyyyyy.log.
```

Obtain the most recent file for the version of the client you want to install. The *xxx* varies depending on the version, and the *yyyyyyyyyyyyyy* specifies the date and time of the install.

- macOS (10.12 and later)—the logging database; use Console app or log command to query logs for VPN, DART, or Umbrella
- macOS (legacy file based log)—`/var/log/system.log` for all other modules
- Linux Ubuntu—`/var/log/syslog`
- Linux Red Hat—`/var/log/messages`

Activating Logging for Docker Deployments

In Docker deployments, thre is no systemd; therefore, you can't log into a system journal. To activate logging on the screen (standard ouput) of the user, you can add the following line to the Docker file, which enables logging:

```
ENV CSC_LOGGING_OUTPUT=STDOUT
```

Run DART to Clear Troubleshooting Data

In Windows, you can use the DART wizard to clear the generated logs.

Procedure

Step 1 Launch DART with administrator privileges.

Step 2 Click **Clear All Logs** to start the clearing of the logs.

Cisco Secure Client Connection or Disconnection Issues

Cisco Secure Client Not Establishing Initial Connection or Not Disconnecting

Problem: Cisco Secure Client will not establish initial connection, or you get unexpected results when you click **Disconnect** on the Cisco Secure Client window.

Solution: Check the following:

- You can experience intermittent connectivity issues because the network or WiFi adapter drivers are ooutdated. Upgrade those drivers and retry.
- If you are using Citrix Advanced Gateway Client Version 2.2.1, remove the Citrix Advanced Gateway Client until the CtxLsp.dll issue is resolved by Citrix.
- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
  1. Disable acceleration on the Aircard.
  2. Launch **AT&T communication manager** > **Tools** > **Settings** > **Acceleration** > **Startup**.
  3. Type **manual**.
  4. Click **Stop**.
- Obtain the config file from the Secure Firewall ASA to look for signs of a connection failure:
  - From the Secure Firewall ASA console, type **write net x.x.x.x:ASA-Config.txt**, where *x.x.x.x* is the IP address of the TFTP server on the network.
  - From the Secure Firewall ASA console, type **show running-config**. Cut and paste the config into a text editor and save.
- View the Secure Firewall ASA event logs:
  1. At the Secure Firewall ASA console, add the following lines to look at the ssl, webvpn, anyconnect, and auth events:

     ```
     config 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
     ```

  2. Attempt connection to Cisco Secure Client, and when the connect error occurs, cut and paste the log information from the console into a text editor and save.
  3. Type **`no logging enable`** to disable logging.
- Obtain the Cisco Secure Client log from the client computer using the Windows Event Viewer.
  1. Choose **Start** > **Run** and type **`eventvwr.msc /s`**.
  2. Locate the Cisco Secure Client in the Applications and Services Logs (of Windows 7) and choose **Save Log File As..**.
  3. Assign a filename, for example, `CiscoSecureClientLog.evt`. You must use the `.evt` file format.
- Modify the Windows Diagnostic Debug Utility.
  1. Attach the vpnagent.exe process as shown in the WinDbg documentation.
  2. Determine if there is a conflict with the IPv6/IPv4 IP address assignments. Look in the event logs for any idenfied conflicts.
  3. If a conflict was identified, add additional routing debugs to the registry of the client computer being used. These conflicts may appear in the Cisco Secure Client event logs as follows:

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

4. Enable route debugging on a one-time basis for a connection by adding a specific registry entry (Windows) or file (Linux and macOS).
   - On 32-bit Windows, the DWORD registry value must be `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client\DebugRoutesEnabled`
   - On 64-bit Windows, the DWORD registry value must be `HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco Secure Client\DebugRoutesEnabled`
   - On Linux or macOS, create a file in the following path using the sudo touch command: `/opt/cisco/secureclient/vpn/debugroutes`

Note The key or file is deleted when the tunnel connection is started. The value of the key or content of the file is not important as the existence of the key or file is sufficient to enable debugging.

Start a VPN connection. When this key or file is found, two route debug text files are created in the system temp directory (usually C:\Windows\Temp on Windows and /opt/cisco/secureclient/vpn on macOS or Linux). The two files (debug_routechangesv4.txt4 and debug_routechangesv6.txt) are overwritten if they already exist.

Cisco Secure Client Not Passing Traffic

Problem: Cisco Secure Client cannot send data to the private network once connected.

Solution: Check the following:

- If you are using AT&T Communication Manager Version 6.2 or 6.7 with an AT&T Sierra Wireless 875 card, follow these steps to correct the problem:
  1. Disable acceleration on the Aircard.
  2. Launch AT&T communication manager > Tools > Settings > Acceleration > Startup.
  3. Type **manual**.
  4. Click **Stop**.
- Obtain the output of the **show vpn-sessiondb detail anyconnect filter name <username>** command. If the output specifies Filter Name: XXXXX, get the output for the show access-list XXXXX command as well. Verify that the ACL is not blocking the intended traffic flow.

- Obtain the DART file or the output from Cisco Secure Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt). Observe the statistics, interfaces, and routing table.
- Check the Secure Firewall ASA config file for NAT statements. If NAT is enabled, you must exempt data returning to the client from network address translation. For example, to NAT exempt the IP addresses from the Cisco Secure Client pool, the following code would be used:

```
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
```

- Verify whether the tunneled default gateway is enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic:

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  If a VPN client needs to access a resource that is not in the routing table of the VPN gateway, packets are routed by the standard default gateway. The VPN gateway does not need to have the whole internal routing table. If you use a tunneled keyword, the route handles decrypted traffic coming from IPsec/SSL VPN connection. Standard traffic routes to 209.165.200.225 as a last resort, while traffic coming from the VPN routes to 10.0.4.2 and is decrypted.

- Collect a text dump of ipconfig /all and a route print output before and after establishing a tunnel with Cisco Secure Client.
- Perform a network packet capture on the client or enable a capture on the Secure Firewall ASA.

Note If some applications (such as Microsoft Outlook) do not operate with the tunnel, ping a known device in the network with a scaling set of pings to see what size gets accepted (for example, ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000). The ping results provide clues to the fragmentation issues in the network. Then you can configure a special group for users who might experience fragmentation and set the anyconnect mtu for this group to 1200. You can also copy the Set MTU.exe utility from the old IPsec client and force the physical adapter MTU to 1300. Upon reboot, see if you notice a difference.

Connectivity Issues with VM-based Subsystems

If you experience connectivity issues with Windows Subsystem for Linux (WSL2) or VMware Fusion VM when the AnyConnect VPN is active on the host (Windows 10 or macOS 11 (and later), follow these steps to configure Local LAN split exclude tunneling restricted to only virtual adapter subnets.

Procedure

Step 1 In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** to configure a new custom attribute type.

Step 2 Choose **Add** and set the following in the Create Custom Attribute pane:

a) Enter **BypassVirtualSubnetsOnlyV4** for IPv4 or **BypassVirtualSubnetsOnlyV6** for IPv6 as the new type.
b) Optionally, enter a description.
c) Set the name and value to *true* in **AnyConnect Custom Attributes Names**.

If the local LAN wildcard split exclude is already configured in the group policy for a certain IP protocol, it is restricted by the client to only virtual subnets, provided that the custom attribute is enabled for the same IP protocol. If the local LAN wildcard split exclude is not configured in the group policy, it is added by the client for the IP protocol(s) with the custom attribute enabled, resulting in restricted local LAN split exclude being enforced accordingly. With no other split-exclude networks configured, all physical adapter traffic is tunneled, similar to the tunnel-all configuration.

Step 3 Attach the previously created custom attribute type and name to a group policy via **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Group Policies** > **Edit** >**Advanced** > **AnyConnect Client** > **Custom Attributes**.

What to do next

To verify if the attribute value was set correctly, check the Cisco Secure Client logs for a message starting with "Received VPN Session Configuration." It should say that local LAN Wildcard is limited to virtual subnets.

VPN Service Failures

VPN Service Connection Fails

Problem: You receive an “Unable to Proceed, Cannot Connect to the VPN Service” message. The VPN service for Cisco Secure Client is not running.

Solution: Determine if another application conflicted with the service. See Determine What Conflicted With Service, page 11-7.

Determine What Conflicted With Service

The following procedure determines if the conflict is with the initialization of the server at boot-up or with another running service, for example, because the service failed to start.

Procedure

Step 1 Check the services under the Windows Administration Tools to ensure that the Cisco Secure Client VPN Agent is *not* running. If it is running and the error message still appears, another VPN application on the workstation may need disabled or even uninstalled. After taking that action, reboot, and repeat this step.

Step 2 Try to start the Cisco Secure Client VPN Agent.

Step 3 Check the Cisco Secure Client logs in the Event Viewer for any messages stating that the service was unable to start. Notice the timestamps of the manual restart from Step 2, as well as when the workstation was booted up.

Step 4 Check the System and Application logs in the Event Viewer for the same general time stamps of any messages of conflict.

Step 5 If the logs indicate a failure starting the service, look for other information messages around the same time stamp which indicate one of the following:

- a missing file—reinstall Cisco Secure Client from a standalone MSI installation to rule out a missing file.

- a delay in another dependent service—disable startup activities to speed up the workstation's boot time.
- a conflict with another application or service—determine whether another service is listening on the same port as the port the vpnagent is using or if some HIDS software is blocking our software from listening on a port.

Step 6 If the logs do not point directly to a cause, use the trial and error method to identify the conflict. When the most likely candidates are identified, disable those services (such as VPN products, HIDS software, spybot cleaners, sniffers, antivirus software, and so on) from the Services panel.

Step 7 Reboot. If the VPN Agent service still fails to start, start turning off services that were not installed by a default installation of the operating system.

VPN Client Driver Encounters Error (after a Microsoft Windows Update)

Problem: If you recently updated the Microsoft certclass.inf file, the following message is encountered when trying to establish a VPN connection:

```
The VPN client driver has encountered an error.
```

If you check the C:\WINDOWS\setupapi.log, you can see the following error:

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
 policy.
```

Solution: Check which updates have recently been installed by entering **C:\>systeminfo** at the command prompt or checking the C:\WINDOWS\WindowsUpdate.log. Follow the instructions to repair the VPN driver.

Repair VPN Client Driver Error

Even though the steps taken above may indicate that the catalog is not corrupt, the key file(s) may still have been overwritten with an unsigned one. If the failure still occurs, open a case with Microsoft to determine why the driver signing database is being corrupted.

Procedure

Step 1 Open a command prompt as an admin.

Step 2 Enter **net stop CryptSvc**.

Step 3 Analyze the database to verify its validity by entering **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** or rename the following directory: %/WINDIR%\system32\catroot2 to catroot2_old.

Step 4 When prompted, choose **OK** to attempt the repair. Exit the command prompt and reboot.

Driver Crashes

Fix Driver Crashes in VPNVA.sys

Problem: VPNVA.sys driver crashes.

Solution: Find any intermediate drivers that are bound to the Cisco Secure Client Virtual Adapter and uncheck them.

Fix Driver Crashes in vpnagent.exe

Procedure

Step 1 Create a directory called c:\vpnagent.

Step 2 Look at the Process tab in the Task Manager and determine the PID of the process in vpnagent.exe.

Step 3 Open a command prompt and change to the directory where you installed the debugging tools. By default, the debugging tools for Windows are located in `C:\Program Files\Debugging Tools`.

Step 4 Type **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**, where *PID* is the PID of **vpnagent.exe**.

Step 5 Let the open window run in minimized state. You cannot log off of the system while you are monitoring.

Step 6 When the crash occurs, collect the contents of c:\vpnagent in a zip file.

Step 7 Use **!analyze -v** to further diagnose the crashdmp file.

Link/Driver Issues with Network Access Manager

If the Network Access Manager fails to recognize your wired adapter, try unplugging your network cable and reinserting it. If this does not work, you may have a link issue. The Network Access Manager may not be able to determine the correct link state of your adapter. Check the Connection Properties of your NIC driver. You may have a "Wait for Link" option in the Advanced Panel. When the setting is On, the wired NIC driver initialization code waits for auto negotiation to complete and then determines if a link is present.

Note Certain older Intel NIC do not support WPA3. If you attempt to create a WPA3 network using one of these cards (Intel 72xx and 82xx), Network Access Manager will not be able to complete the connection.

Other Crashes

Cisco Secure Client Crashes

Problem: You received a “the system has recovered from a serious error” message after a reboot.

Solution: Gather the .log and .dmp generated files from the %temp% directory (such as C:\DOCUME~1\jsmith\LOCALS~1\Temp). Copy the files or back them up. See How to Back Up .log or .dmp Files, page 11-9.

How to Back Up .log or .dmp Files

Procedure

Step 1 Run the Microsoft utility called Dr. Watson (Drwtsn32.exe) from the Start > Run menu.

Step 2 Configure the following 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
```

Step 3 On the client device, get the Cisco Secure Client VPN client log from the Windows Event Viewer by entering **eventvwr.msc /s** at the Start > Run menu.

Step 4 Locate the Cisco Secure Client in the Applications and Services Logs (of Windows) and choose **Save Log File As..**. Assign a filename such as CiscoSecureClientLog.evt in the .evt file format.

Cisco Secure Client Crashes in vpndownloader (Layered Service Provider (LSP) Modules and NOD32 AV)

Problem: When Cisco Secure Client attempts to establish a connection, it authenticates successfully and builds the ssl session, but then it crashes in the vpndownloader if using LSP or NOD32 AV.

Solution: Remove the Internet Monitor component in version 2.7 and upgrade to version 3.0 of ESET NOD32 AV.

Blue Screen (AT & T Dialer)

Problem: If you are using an AT&T Dialer, the client operating system sometimes experiences a blue screen, which causes the creation of a mini dump file.

Solution: Upgrade to the latest 7.6.2 AT&T Global Network Client.

Security Alerts

Microsoft Internet Explorer Security Alert

Problem: A security alert window appears in Microsoft Internet Explorer with the following text:

```
Information you exchange with this site cannot be viewed or changed by others. However,
there is a problem with the site's security certificate. The security certificate was issued
 by a company you have not chosen to trust. View the certificate to determine whether you
want to trust the certifying authority.
```

Solution: This alert may appear when connecting to a Secure Firewall ASA that is is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See Install Trusted Root Certificates on a Client, page 11-10.

"Certified by an Unknown Authority" Alert

Problem: A "Web Site Certified by an Unknown Authority" alert window may appear in the browser. The upper half of the Security Alert window shows the following text:

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

Solution: This security alert may appear when connecting to a Secure Firewall ASA that is not recognized as a trusted site. To prevent this alert, install a trusted root certificate on a client. See Install Trusted Root Certificates on a Client, page 11-10.

Install Trusted Root Certificates on a Client

Before you begin

Generate or obtain the certificate to be used as the trusted root certificate.

Note You can avoid security certificate warnings in the short term by installing a self-signed certificate as a trusted root certificate on the client. However, we do not recommend this because of the possibility that a user could inadvertently configure a browser to trust a certificate on a rogue server and because of the inconvenience to users of having to respond to a security warning when connecting to your secure gateway.

Procedure

Step 1 Click **View Certificate** in the Security Alert window.

Step 2 Click **Install Certificate**.

Step 3 Click **Next**.

Step 4 Select **Place all certificates in the following store**.

Step 5 Click **Browse**.

Step 6 In the drop-down list, choose **Trusted Root Certification Authorities**.

Step 7 Continue following the Certificate Import wizard prompts.

Dropped Connections

Wireless Connection Drops When Wired Connection is Introduced (Juniper Odyssey Client)

Problem: When wireless suppression is enabled on an Odyssey client, the wireless connection drops if a wired connection is introduced. With wireless suppression disabled, the wireless operates as expected.

Solution: Configure the Odyssey Client, page 11-11.

Configure the Odyssey Client

Procedure

Step 1 In Network Connections, copy the name of the adapter as it appears in its connection properties. If you edit the registry, perform a backup before making any changes and use caution as serious problems can occur if modified incorrectly.

Step 2 Open the registry and go to HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual.

Step 3 Create a new string value under virtual. Copy the name of the adapter from Network properties into the registry portion. The additional registry settings, once saved, are ported over when a customer MSI is created and is pushed down to other clients.

Connections to the Secure Firewall ASA Fail (Kaspersky AV Workstation 6.x)

Problem: When Kaspersky 6.0.3 is installed (even if disabled), Cisco Secure Client connections to the Secure Firewall ASA fail right after CSTP state = CONNECTED. The following message appears:

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy
 authentication, handshake, bad cert, etc.).
```

Solution: Uninstall Kaspersky and refer to their forums for additional updates.

No UDP DTLS Connection (McAfee Firewall 5)

Problem: When using McAfee Firewall 5, a UDP DTLS connection cannot be established.

Solution: In the McAfee Firewall central console, choose **Advanced Tasks** > **Advanced options and Logging** and uncheck the **Block incoming fragments automatically** checkbox in McAfee Firewall.

Connection to the Host Device Fails (Microsoft Routing and Remote Access Server)

Problem: If you are using RRAS, the following termination error is returned to the event log when Cisco Secure Client attempts to establish a connection to the host device:

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the Cisco Secure Client.
```

Solution: Disable the RRAS service.

Failed Connection/Lack of Credentials (Load Balancers)

Problem: The connection fails due to lack of credentials.

Solution: The third-party load balancer has no insight into the load on the Secure Firewall ASA devices. Because the load balance functionality in the ASA is intelligent enough to evenly distribute the VPN load across the devices, we recommend using the internal Secure Firewall ASA load balancing instead.

Installation Failures

Do Not Edit Windows Registry Without Root Cause

If you are receiving a failure while installing, uninstalling, or upgrading Cisco Secure Client, we do not recommend modifying the Windows Installer registry keys directly, because it can lead to undesired consequences. Microsoft-provided tools can troubleshoot installer issues after proper root cause is determined.

Cisco Secure Client Fails to Download (Wave EMBASSY Trust Suite)

Problem: Cisco Secure Client fails to download and produces the following error message:

```
“Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close.”
```

Solution: Upload the patch update to version 1.2.1.38 to resolve all dll issues.

Incompatability Issues

Interoperability with Third-Party Products Using Layer 4 Network Flow

You may experience issues with Secure Client Zero Trust Access or Umbrella Secure Web Gateway modules interoperating with third-party security networking products that use layer 4 network flow. You may need to configure the third-party product to intercept very specific resources, and not the ones that overlap with those intercepted by the Zero Trust Access or Umbrella Secure Web Gateway modules.

Embedded Browser Changes After Deprecation of IE11

With the deprecation of IE11, Secure Client embedded browser defaults to WebView2, as long as the runtime is installed. If you need to revert back to the legacy embedded browser control, add a DWORD registry value UseLegacyEmbeddedBrowser set to *1* to the following Windows registry key:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client

Failure to Update the Routing Table (Bonjour Printing Service)

Problem: If you are using Bonjour Printing Services, the Cisco Secure Client event logs indicate a failure to identify the IP forwarding table.

Solution: Disable the BonJour Printing Service by typing **net stop “bonjour service”** at the command prompt. A new version of mDNSResponder (1.0.5.11) has been produced by Apple. To resolve this issue, a new version of Bonjour is bundled with iTunes and made available as a separate download from the Apple web site.

Version of TUN is Incompatible (OpenVPN Client)

Problem: An error indicates that the version of TUN is already installed on this system and is incompatible with the Cisco Secure Client.

Solution: Uninstall the Viscosity OpenVPN Client.

Winsock Catalog Conflict (LSP Symptom 2 Conflict)

Problem: If an LSP module is present on the client, a Winsock catalog conflict may occur.

Solution: Uninstall the LSP module.

Slow Data Throughput (LSP Symptom 3 Conflict)

Problem: Slow data throughput may occur with the use of NOD32 Antivirus V4.0.468 x64 using Windows.

Solution: Disable SSL protocol scanning. See Disable SSL Protocol Scanning.

Disable SSL Protocol Scanning

Procedure

Step 1 Go to **Protocol Filtering** > **SSL** in the Advanced Setup and enable SSL protocol scanning.

Step 2 Go to **Web access protection** > **HTTP, HTTPS** and check **Do not use HTTPS protocol checking**.

Step 3 Go back to **Protocol filtering** > **SSL** and disable **SSL protocol scanning.**

DPD Failure (EVDO Wireless Cards and Venturi Driver)

Problem: If you are using a EVDO wireless card and Venturi driver while a client disconnect occurred, the event log reports the following:

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

Solution:

- Check the Application, System, and Cisco Secure Client event logs for a relating disconnect event and determine if a NIC card reset was applied at the same time.
- Ensure that the Venturi driver is up to date. Disable **Use Rules Engine** in the 6.7 version of the AT&T Communications Manager.

DTLS Traffic Failing (DSL Router)

Problem: If you are connecting with a DSL router, DTLS traffic may fail even if successfully negotiated.

Solution: Connect to a Linksys router with factory settings. This setting allows a stable DTLS session and no interruption in pings. Add a rule to allow DTLS return traffic.

NETINTERFACE_ERROR (CheckPoint and other Third-Party Software such as Kaspersky)

Problem: When attempting to retrieve operating system information on the computer’s network used to make the SSL connection, the Cisco Secure Client log may indicate a failure to fully establish a connection to the secure gateway.

Solution:

- If you are uninstalling the Integrity Agent and then installing Cisco Secure Client, enable TCP/IP.
- Ensure that if you disable SmartDefense on Integrity agent installation, TCP/IP is checked.
- If third-party software is intercepting or otherwise blocking the operating system API calls while retrieving network interface information, check for any suspect AV, FW, AS, and such.
- Confirm that only one instance of the Cisco Secure Client adapter appears in the Device Manager. If there is only one instance, authenticate with Cisco Secure Client, and after 5 seconds, manually enable the adapter from the Device Manager.
- If any suspect drivers have been enabled within the Cisco Secure Client adapter, disable them by unchecking them in the Connection window of Cisco Secure Client.

Performance Issues (Virtual Machine Network Service Drivers)

Problem: When using Cisco Secure Client on some Virtual Machine Network Service devices, performance issues have resulted.

Solution: Uncheck the binding for all IM devices within the Cisco Secure Client virtual adapter. The application dsagent.exe resides in C:\Windows\System\dgagent. Although it does not appear in the process list, you can see it by opening sockets with TCPview (sysinternals). When you terminate this process, normal operation of Cisco Secure Client returns.

Known Third-Party Application Conflicts

The following third-party applications have known complications with Cisco Secure Client:

- Adobe and Apple—Bonjour Printing Service
    - Adobe Creative Suite 3
    - BonJour Printing Service
    - iTunes
- AT&T Communications Manager Versions 6.2 and 6.7
    - AT&T Sierra Wireless 875 card
- AT&T Global Dialer
- CheckPoint and other Third-Party Software such as Kaspersky
- Cisco Secure Client for Apple iOS on Apple M1 devices running the same time as Cisco Secure Client on macOS
- Cisco Secure Client on Universal Windows Platform
- Citrix Advanced Gateway Client Version 2.2.1
- DSL routers
- EVDO Wireless Cards and Venturi Driver
- Firewall Conflicts
    - Third-party firewalls can interfere with the firewall function configured on the Secure Firewall ASA group policy.
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- Layered Service Provider (LSP) Modules and NOD32 AV
- Load balancers
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- Microsoft VPN
- OpenVPN client
- Pulse Secure

- Virtual Machine Network Service Drivers
- Wave EMBASSY Trust Suite