Managing, Monitoring, and Troubleshooting AnyConnect Sessions

This chapter explains these subjects and tasks:

Disconnecting All VPN Sessions

To log off all SSL VPN sessions, including Cisco AnyConnect Secure Mobility client sessions, use the **vpn-sessiondb logoff anyconnect** command in global configuration mode:

vpn-sessiondb logoff anyconnect

In response, the system asks you to confirm that you want to log off the VPN sessions. To confirm press **Enter** or type **y**. Entering any other key cancels the logging off.

The following example logs off all SSL VPN sessions:

```
hostname# vpn-sessiondb logoff anyconnect
INFO: Number of sessions of type "svc" logged off : 1
Do you want to logoff the VPN session(s)? [confirm]
```

```
INFO: Number of sessions logged off : 6
hostname#
```

Disconnecting Individual VPN Sessions

You can log off individual sessions using either the **name** option or the **index** option:

vpn-sessiondb logoff name *name*

vpn-sessiondb logoff index *index*

For example, to log off the user named tester, enter the following command:

```
hostname# vpn-sessiondb logoff name tester
Do you want to logoff the VPN session(s)? [confirm]
INFO: Number of sessions with name "tester" logged off : 1
hostname#
```

You can find both the username and the index number (established by the order of the client images) in the output of the **show vpn-sessiondb anyconnect** command.

The following example terminates that session using the **name** option of the **vpn-sessiondb logoff command**:

```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

Viewing Detailed Statistical Information

You or the user can view statistical information for a current AnyConnect session. On Windows navigate to **Advanced Window > VPN drawer > Statistics**. Alternatively, on Linux click the **Details** button on the user GUI.

This opens the Statistics Details dialog. On the Statistics tab in this window, you can reset the statistics, export the statistics, and gather files for the purpose of troubleshooting.

The options available in this window depend on the packages that are loaded on the client computer. If an option is not available, its button is not active and a "(Not Installed)" indicator appears next to the option name in the dialog box. The options are as follows:

- Clicking **Reset** resets the connection information to zero. AnyConnect immediately begins collecting new data.
- Clicking **Export Stats...** saves the connection statistics to a text file for later analysis and debugging.
- Clicking **Troubleshoot...** Launches the AnyConnect Diagnostics and Reporting Tool (DART) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the client connection. See the "Using DART to Gather Troubleshooting Information" section on page 13-4 for information about the DART package.

Resolving VPN Connection Issues

Use the following sections to resolve VPN connection issues.

Adjusting the MTU Size

Many consumer-grade end user terminating devices (for example, a home router) do not properly handle the creation or assembly of IP fragments, particularly UDP. Because DTLS is a UDP-based protocol, it is sometimes necessary to reduce the MTU to prevent fragmentation. The MTU parameter sets the maximum size of the packet to be transmitted over the tunnel for the client and ASA. If a VPN user is experiencing a significant amount of lost packets, or if an application such as Microsoft Outlook is not functioning over the tunnel, it might indicate a fragmentation issue. Lowering the MTU for that user or group of users may resolve the problem.

To adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by AnyConnect,

Step 1 From the ASDM interface, select **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add** or **Edit**.

The Edit Internal Group Policy dialog box opens.

Step 2 Select **Advanced > SSL VPN Client**.

Step 3 Uncheck the **Inherit** check box and specify the appropriate value in the MTU field.

The default size for this command in the default group policy is 1406. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

This setting affects only AnyConnect connections established in SSL and those established in SSL with DTLS.

Optimal MTU (OMTU)

Use the Optimal MTU (OMTU) function to find the largest endpoint MTU at which the client can successfully pass DTLS packets. Implement OMTU by sending a DPD packet that is padded to the maximum MTU. If a correct echo of the payload is received back from the head end, the MTU size is accepted. Otherwise, the MTU is reduced and the probe is sent again until the minimum MTU allowed for the protocol is reached.

Note Using OMTU does not interfere with the existing tunnel DPD function.

To use this feature, DPD on the ASA must be enabled. This feature does not work with IPsec, since DPD is based on the standards implementation that does not allow padding.

Using DART to Gather Troubleshooting Information

DART is the AnyConnect Diagnostics and Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect installation and connection problems. DART supports Windows 7, Windows Vista, and Windows XP, Mac OS X v10.6, v10.7, and v10.8, and Red Hat Enterprise Linux 5.x (32-bit) or 6.x (64-bit).

The DART wizard runs on the computer that runs AnyConnect. DART assembles the logs, status, and diagnostic information for Cisco Technical Assistance Center (TAC) analysis. DART does not require administrator privileges.

DART does not rely on any component of the AnyConnect software to run, though you can launch DART from AnyConnect, and DART does collect the AnyConnect log file, if it is available.

DART is currently available as a standalone installation, or the administrator can push this application to the client computer as part of the AnyConnect dynamic download infrastructure. Once installed, the end user can start the DART wizard from the Cisco folder available through the Start button.

Note DART bundles cannot be unzipped by Achieve Utility on Mac OS X v10.6.

Getting the DART Software

You can install DART on the client using either the web-deployment or pre-deployment method of AnyConnect.

Any version of DART works with any version of AnyConnect; the version numbers of each are no longer synchronized.

Table 13-1 provides the AnyConnect downloads (both files and packages) containing DART for the pre-deploy and web deploy (downloaded) installer. Before release 3.0.3050, the DART component was a separate download (a .dmg, .sh, or .msi file) for web deploy. With release 3.0.3050 or later, the DART component is included in the .pkg file.

Table 13-1 DART File or Package Filenames for ASA or Pre-Deployment

DART	Web-Deploy Filenames and Packages (Downloaded)	Pre-Deploy Installer
Windows	*Release 3.0.3050 or later:* anyconnect-win-(ver)-k9.pkg	anyconnect-win-(ver)-pre-deploy-k9.iso
	Before release 3.0.3050: anyconnect-dart-win-(ver)-k9.msi*	anyconnect-dart-win-(ver)-k9.msi*
Mac OS X	*Release 3.0.3050 or later:* anyconnect-macosx-i386-(ver)-k9.pkg	anyconnect-macosx-i386-(ver)-k9.dmg
	Before release 3.0.3050: anyconnect-dartsetup.dmg	anyconnect-dart-macosx-i386-(ver)-k9.dmg
Linux	*Release 3.0.3050 or later:* anyconnect-linux-(ver)-k9.pkg	anyconnect-predeploy-linux-(ver)-k9.tar.gz
	Before release 3.0.3050: anyconnect-dartsetup.sh	anyconnect-dart-linux-(ver)-k9.tar.gz

Table 13-1 DART File or Package Filenames for ASA or Pre-Deployment

DART	Web-Deploy Filenames and Packages (Downloaded)	Pre-Deploy Installer
Linux-64	*Release 3.0.3050 or later:* anyconnect-linux-64-(ver)-k9.pkg	anyconnect-predeploy-linux-64-(ver)-k9.tar.gz
	Before release 3.0.3050: anyconnect-dartsetup.sh	anyconnect-dart-linux-64-(ver)-k9.tar.gz

The web-deploy and predeployment packages are contained in an ISO image (.iso). The ISO image file contains the programs and MSI installer files to deploy to user computers. Refer to the "Predeployment Package File Information" section on page 2-20 for more information about the .iso image and its contents.

Installing DART

The administrator can include DART as part of the AnyConnect installation.

When AnyConnect downloads to a computer running Windows, a new version of DART, if available, downloads along with it. When a new version of the AnyConnect downloads as part of an automatic upgrade, it includes a new version of DART if there is one.

Note If the **dart** keyword is not present in the group-policy configuration (configured through the **anyconnect modules** command or the corresponding ASDM dialog), then the AnyConnect download does not install DART, even if it is present in the package.

Installing DART with AnyConnect

This procedure downloads DART to the remote-user's machine the next time the user connects.

Step 1 Load the AnyConnect package containing DART to the ASA, just as you would any other Cisco software package.

Step 2 After installing the AnyConnect .pkg file containing DART on the security appliance, you must specify DART in a group policy, in order for it to be installed with AnyConnect. You can do this using ASDM or the CLI, as follows:

If using ASDM:

a. Begin by clicking **Configuration** and then click **Remote Access VPN > Network (Client) Access > Group Policies**.

b. Add a new group policy or edit an existing group policy. In the group policy dialog box, expand **Advanced** and click **SSL VPN Client**.

c. In the SSL VPN Client dialog box, uncheck **Inherit** for the **Optional Client Modules to Download** option. Select the **dart** module in the option's drop-down list.

d. If the version of ASDM that you are using does not have the DART option checkbox, enter the keyword **dart** in the field. If you want to enable both DART and Start Before Logon, enter both **dart** and **vpngina** in that field, in either order, separated by a comma.

Click **OK** and then click **Apply**.

If using CLI, use the **anyconnect modules value dart** command.

Note If you later change to **anyconnect modules none** or if you remove the DART selection in the **Optional Client Modules to Download** field, DART remains installed. The security appliance cannot cause DART to be uninstalled. However, you can remove DART by using the Windows Add/Remove Programs in the Control Panel. If you do remove DART in this way, then it is reinstalled automatically when the user reconnects using AnyConnect. When the user connects, DART is upgraded automatically when an AnyConnect package with a higher version of DART is uploaded and configured on the ASA.

To run DART, see the "Running DART on Windows" section on page 13-7.

Manually Installing DART on a Windows Device

Follow these steps to install DART on a Windows device.

Step 1 Store anyconnect-dart-win-(ver)-k9.msi locally. If you are installing with release 3.0.3050 or later, this DART component is included with the anyconnect-win-(ver)-k9.pkg download.

Step 2 Double-click the **anyconnect-dart-win-(ver)-k9.msi** file to launch the **DART Setup Wizard**.

Step 3 Click **Next** at the Welcome screen.

Step 4 Select **I accept the terms in the License Agreement** to accept the end user license agreement and click **Next**.

Step 5 Click **Install** to install DART. The installation wizard installs **DartOffline.exe** in the <System Drive>:\Program Files\Cisco\Cisco DART directory.

Step 6 Click **Finish** to complete the installation.

To run DART, see the "Running DART on Windows" section on page 13-7.

Manually Installing DART on a Linux Device

Follow these steps to install DART on a Linux device.

Step 1 Store anyconnect-dart-linux-(ver)-k9.tar.gz locally. If you are installing with release 3.0.3050 or later, this DART component is included with the anyconnect-linux-(ver)-k9.pkg download.

Step 2 From a terminal, extract the tar.gz file using the **tar -zxvf** ***<path to tar.gz file including the file name>*** command.

Step 3 From a terminal, navigate to the extracted folder and run dart_install.sh using the **sudo ./dart_install.sh** command.

Step 4 Accept the license agreement and wait for the installation to finish.

Note You can only uninstall DART using **/opt/cisco/anyconnect/dart/dart_uninstall.sh**.

Manually Installing DART on a Mac OS X Device

Follow these steps to install DART on a Mac OS X device.

Step 1 Store anyconnect-dart-macosx-i386-(ver)-k0.dmg locally. If you are installing with release 3.0.3050 or later, this DART component is included with the anyconnect-macosx-i386-(ver)-k9.pkg download.

Step 2 When the download finishes, the .dmg file is automatically mounted to the desktop, and the DART install wizard starts automatically. To start the install wizard manually, go to the download folder, double click the downloaded .dmg file to mount it to the desktop, and double click dart.pkg from the mounted device.

The install wizard displays a "This package will run a program to determine if the software can be installed" message.

Step 3 Click **Continue**. The license agreement displays on the wizard.

Step 4 Click **Continue** and **Accept** to agree to the license agreement.

Step 5 You are prompted to change the install location. Make the necessary changes and click **Continue**.

Step 6 You must enter the administrator credentials for the installation to begin. Click **Continue** after entering the credentials. The installation begins.

Step 7 Wait for the installation to complete and click **Cancel** to exit the program.

Note You can only uninstall DART using **/opt/cisco/anyconnect/bin/dart_uninstall.sh**.

Running DART on Windows

To run the DART wizard and create a DART bundle for Windows, follow these steps:

Step 1 Launch the AnyConnect GUI if you are running on a Windows device.

Step 2 Click the **Statistics** tab and then click the **Details** button at the bottom of the dialog box. This opens the Statistics Details dialog box.

Step 3 Click **Troubleshoot** at the bottom of the Statistics Details window.

Step 4 Click **Next** at the Welcome screen. This brings you to the Bundle Creation Option dialog box.

Step 5 In the Bundle Creation Options area, select **Default** or **Custom**.

- The **Default** option includes the typical log files and diagnostic information, such as the AnyConnect and Cisco Secure Desktop log files, general information about the computer, and a summary of what DART did and did not do.

  By selecting **Default,** and then clicking **Next** at the bottom of the dialog box, DART immediately begins creating the bundle. The default name for the bundle is DARTBundle.zip, and it is saved to the local desktop.

- If you choose **Custom,** the DART wizard will present you with more dialog boxes, after you click **Next**, so that you can specify what files you want to include in the bundle and where to store the bundle.

Tip By selecting **Custom**, you could accept the default files to include in the bundle and then only specify a different storage location for the file.

Step 6 If you want to encrypt the DART bundle, in the **Encryption Option** area check **Enable Bundle Encryption**; then, enter a password in the **Encryption Password** field. Optionally, select **Mask Password** and the password you enter in the **Encryption Password** and **Reenter Password** fields will be masked with astericks (*).

Step 7 Click **Next**. If you selected **Default,** DART starts creating the bundle. If you selected **Custom**, the wizard continues to the next step.

Step 8 In the **Log File Selection** dialog box, select the log files and preference files to include in the bundle. You have an option to include the Network Access Manager, Telemetry, Posture, and Web Security logs. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

Step 9 In the Diagnostic Information Selection dialog box, select the diagnostic information to include in the bundle. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

Step 10 In the Comments and Target Bundle Location dialog box, configure these fields:

- In the **Comments** area, enter any comments you would like included with the bundle. DART stores these comments in a comments.txt file included with the bundle.
- In the **Target Bundle Location** field, browse for a location in which to store the bundle.

Click **Next**.

Step 11 In the Summary dialog box, review your customizations and click **Next** to create the bundle or click **Back** to make customization changes.

Step 12 Click **Finish** after DART finishes creating the bundle.

Tip In some instances, customers have reported that DART has run for more than a few minutes. If DART seems to be taking a long time to gather the default list of files, click **Cancel** and then re-run the wizard choosing to create a **Custom** DART bundle and only select the files you need.

Running DART on Linux or Mac OS X

To run the DART wizard and create a DART bundle for Linux or Mac, follow these steps:

Step 1 For a Linux device, you will launch DART from ->Applications -> Internet-> Cisco DART or /opt/cisco/anyconnect/dart/dartui.

For a Mac device, you will launch DART from ->Applications ->Cisco -> Cisco DART.

Step 2 Click the **Statistics** tab and then click the **Details** button at the bottom of the dialog box. This opens the Statistics Details dialog box.

Step 3 In the Bundle Creation Options area, select **Default** or **Custom**.

- The **Default** option includes the typical log files and diagnostic information, such as the AnyConnect and Cisco Secure Desktop log files, general information about the computer, and a summary of what DART did and did not do.

  By selecting **Default,** and then clicking **Next** at the bottom of the dialog box, DART immediately begins creating the bundle. The default name for the bundle is DARTBundle.zip, and it is saved to the local desktop.

  Note Default is the only option for Mac OS X. You cannot customize which files to include in the bundle.

- If you choose **Custom,** the DART wizard will present you with more dialog boxes, after you click **Next**, so that you can specify what files you want to include in the bundle and where to store the bundle.

Tip By selecting **Custom**, you could accept the default files to include in the bundle and then only specify a different storage location for the file.

Step 4 Click **Next**. If you selected **Default,** DART starts creating the bundle. If you selected **Custom**, the wizard continues to the next step.

Step 5 In the **Log File Selection** dialog box, select the log files and preference files to include in the bundle. You have an option to include the Network Access Manager, Telemetry, Posture, and Web Security logs. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

Step 6 In the Diagnostic Information Selection dialog box, select the diagnostic information to include in the bundle. Click **Restore Default** if you want to revert to the default list of files typically collected by DART. Click **Next**.

Step 7 In the Comments and Target Bundle Location dialog box, configure these fields:

- In the **Comments** area, enter any comments you would like to be included with the bundle. DART stores these comments in a comments.txt file included with the bundle.
- In the **Target Bundle Location** field, browse for a location in which to store the bundle.

Click **Next**.

Step 8 If you want to encrypt the DART bundle, in the **Encryption Option** area check **Enable Bundle Encryption**; then, enter a password in the **Encryption Password** field. Optionally, select **Mask Password** and the password you enter in the **Encryption Password** and **Reenter Password** fields will be masked with astericks (*).

Note Masking the password is not an option for Mac OS Xoperating systems.

Step 9 Click **Finish** to close the wizard.

Tip In some instances, customers have reported that DART has run for more than a few minutes. If DART seems to be taking a long time to gather the default list of files, click **Cancel** and then re-run the wizard choosing to create a **Custom** DART bundle and only select the files you need.

Installing the AnyConnect Client

If you configure the AnyConnect images with the **anyconnect image xyz** command, you must issue the **anyconnect enable** command. Without issuing this command, AnyConnect does not function as expected, and **show webvpn anyconnect** states that the "SSL VPN client is not enabled," instead of listing the installed AnyConnect packages.

Installing the Log Files

The log files are retained in the following files:

- \Windows\setupapi.log — Windows XP and Windows 2000
- \Windows\Inf\setupapi.app.log — Windows 7 and Windows Vista
- \Windows\Inf\setupapi.dev.log —Windows 7 and Windows Vista

Note In Windows 7 and Windows Vista, you must make the hidden files visible.

If registry information is missing from the setupapi.log file, enable verbose logging on a Windows XP-based computer. Follow these steps to enable verbose logging on a Window XP-based computer:

Note Serious problems could result if the registry is modified incorrectly. For added protection, back up the registry before you modify it.

Step 1 Click **Start > Run**.

Step 2 Type **regedit** in the Open field and click **OK**.

Step 3 Locate and double click **LogLevel** in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup registry subkey.

Step 4 Choose **Hexadecimal** on the Base pane of the Edit DWORD Value window.

Step 5 Type **0x2000FFFF** in the Value data box.

Step 6 Click **OK**.

Note When you enable verbose logging, the size of the Setupapi.log file grows to approximately 4 megabytes (MB). Follow these steps again to reset the registry value but instead set the DWORD value (in Step 5) to 0.

Web Install of Log Files

If this is an initial web deployment install, the log file is located in the per-user temp directory:

%TEMP%\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log.

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

%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-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.

Standalone Install of Log Files

To turn on MSI logging and capture logs of the install, run the following:

MSIExec.exe/i anyconnect-win-3X.xxxx-pre-deploy-k9.msi/lvx* c:\AnyConnect.log

where *anyconnect-win-3.X.xxxx-pre-deplay-k9.msi* is the full name of the actual msi file that you want to install.

The log appears in the following locations:

- \Documents and Settings\<username>\Local Settings\Temp —on Windows XP and Windows 2000.
- \Users\<username>\AppData\Local\Temp —on Windows 7 and Windows Vista.
- \Windows\Temp —if an automatic upgrade

If you intend to use standalone only (or you do not want ActiveX control installed on your system), perform one of the following:

Note Without these actions, you may receive a Cisco AnyConnect VPN Error 1722 indicating a problem with the Windows Installer package.

- Create an MSI transform to set the ActiveX property to disabled (NOINSTALLACTIVEX=1):

```
MISExec /i anyconnect-win-x.x.xxxxx-pre-deploy-k9.msi NOINSTALLACTIVEX=1
```

- Perform a quiet install without a reboot:

```
msiexec /quiet /i "anyconnect-gina-x.x.xxxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
msiexec /quiet /norestart /i "anyconnect-gina-x.x.xxxxx-pre-deploy-k9.msi
```

- Perform a quiet uninstall without a reboot:

```
msiexec /quiet /x "anyconnect-gina-x.x.xxxxx-pre-deploy-k9.msi" REBOOT=ReallySuppress
```

Note The value of *x.x.xxxxx* depends on the version being installed.

Problems Disconnecting AnyConnect or Establishing Initial Connection

If you experience problems disconnecting the AnyConnect client or establishing an initial connection, follow these suggestions:

1. Obtain the config file from the ASA to look for signs of a connection failure:
   - From the 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 ASA console, type **show running-config**. Cut and paste the config into a text editor and save.

2. View the ASA event logs.
   a. At the 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
```

   b. Attempt an AnyConnect client connection, and when the connect error occurs, cut and paste the log information from the console into a text editor and save.
   c. Type **no logging enable** to disable logging.
3. On the client computer, get the Cisco AnyConnect VPN client log from the Windows Event Viewer.
   a. Choose **Start > Run** and type **eventvwr.msc /s**.
   b. Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows Vista and Win7) and choose **Save Log File As..**.
   c. Assign a filename like AnyConnectClientLog.evt. You must use the .evt file format.
4. Attach the vpnagent.exe process to the Windows Diagnostic Debug Utility if you are having problems with disconnecting or closing the AnyConnect GUI. Refer to the WinDbg documentation for additional information.
5. If a conflict with the IPv6/IPv4 IP address assignment is identified, obtain sniffer traces and add additional routing debugs to the registry of the client computer being used. These conflicts may appear in the AnyConnect 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
```

   Route debugging can be enabled on a one-time basis for a connection by adding a specific registry entry (Windows) or file (Linux and Mac OS X) prior to making the VPN connection.

   On 32-bit Windows: the DWORD registry value must be:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```

   On 64-bit Windows the DWORD registry value must be:

```
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility
Client\DebugRoutesEnabled
```

   On Linux or Mac OS X, create a file in the followin path using the **sudo touch** command:

```
/opt/cisco/anyconnect/debugroutes
```

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

When a tunnel connection is started and 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 /tmp on Mac or Linux). The two files (debug_routechangesv4.txt4 and debug_routechangesv6.txt) are overwritten if they already exist.

Problems Passing Traffic

If the AnyConnect client cannot send data to the private network once connected, follow these suggestions:

1. 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.
2. Obtain the DART file or the output from AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt). Observe the statistics, interfaces, and routing table.
3. Check the 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 AnyConnect 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
   ```

4. 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 0.0.83.145.50.1
   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 83.145.50.1 as a last resort, while traffic coming from the VPN routes to 10.0.4.2 and is decrypted.
5. Collect a text dump of ipconfig /all and a route print output before and after establishing a tunnel with AnyConnect.
6. Perform a network packet capture on the client or enable a capture on the 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 -l 500, ping -l 1000, ping -l 1500, and ping -l 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.

Problems with AnyConnect Crashing

When a crash in the UI occurs, the results are written to the %temp% directory (such as C:\DOCUME~1\jsmith\LOCALS~1\Temp). If you receive a "The System has recovered from a serious error" message after a reboot, gather the .log and .dmp generated files from C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson or a similar application. Either copy them or follow the steps below to back up the files.

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 computer, get the Cisco AnyConnect VPN client log from the Windows Event Viewer by entering **eventvwr.msc /s** at the Start > Run menu.

Step 4 Locate the **Cisco AnyConnect VPN Client** in the Applications and Services Logs (of Windows Vista and Win7) and choose **Save Log File As..**. Assign a filename such as AnyConnectClientLog.evt in the .evt file format.

Step 5 If a driver crash occurs in VPNVA.sys, check for any intermediate drivers that are bound to the Cisco AnyConnect Virtual Adapter and uncheck them.

Step 6 If a driver crash occurs in vpnagent.exe, attach the vpnagent.exe process to the debugging tools for Windows. After the tools are installed, perform the following:

a. Create a directory called c:\vpnagent.

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

c. 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.

d. Type **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst**, where *PID* is the number determined in Step b.

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

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

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

Problems Connecting to the VPN Service

If you receive an "Unable to Proceed, Cannot Connect to the VPN Service" message, the VPN service for AnyConnect is not running. Most likely, the VPN agent exited unexpectedly. To troubleshoot whether another application conflicted with the service, follow these steps:

Step 1 Check the services under the Windows Administration Tools to ensure that the Cisco AnyConnect 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, rebooted, and retested.

Step 2 Try to start the Cisco AnyConnect VPN Agent. This determines if the conflict is with the initialization of the server at boot-up or with another running service (because the service failed to start).

Step 3 Check the AnyConnect logs in the Event Viewer for any messages stating that the service was unable to start. Notice the time stamps 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 the AnyConnect 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

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. After rebooting, 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.

Responding to Security Alert in Microsoft Internet Explorer

A security alert window may appear when you establish a Microsoft Internet Explorer connection to an ASA that is not recognized as a trusted site. In response to this alert, install a self-signed certificate as a trusted root certificate on a client. The upper half of the Security Alert window shows 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.
```

Note We do not recommend using a self-signed certificate because of the possibility that a user could inadvertently configure a brower 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.

Detailed Steps

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 Click **Next**.

Step 8 Click **Finish**.

Step 9 At the Security Warning window prompt, click **Yes**. The Certificate Import Wizard window indicates the import is successful.

Step 10 Click **OK** to close this window.

Step 11 Click **OK** to close the Certificate window.

Step 12 Click **Yes** to close the Security Alert window. The ASA window opens, signifying the certificate is trusted.

Responding to "Certified by an Unknown Authority" Alert

A "Web Site Certified by an Unknown Authority" alert window may appear when you establish a Netscape, Mozilla, or Firefox connection to an ASA that is not recognized as a trusted site. In response to this alert, install a self-signed certificate as a trusted root certificate on a client. 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.
```

Note We do not recommend using a self-signed certificate because of the possibility that a user could inadvertently configure a brower 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.

Detailed Steps

Step 1 Click **Examine Certificate** in the "Web Site Certified by an Unknown Authority" window. The Certificate Viewer window opens.

Step 2 Click the **Accept this certificate permanently** option.

Step 3 Click **OK**. The ASA window opens, signifying the certificate is trusted.

Obtaining the Computer System Information

Type the following and wait about two minutes to obtain the computer's system info:

- **winmsd /nfo c:\msinfo.nfo** — on Windows XP or 2K
- **msinfo32 /nfo c:\msinfo.nfo** —on Vista

Obtaining a Systeminfo File Dump

On Windows XP or Vista, type the following at a command prompt to obtain a systeminfo file dump:

systeminfo >> c:\sysinfo.txt

Checking the 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.

Conflicts with Third-Party Applications

Some third-party applications prohibit the installation of AnyConnect's Virtual Adapter drivers. This can result in blue screens and a failure to update the routing table. Using the DART tool (described in the "Using DART to Gather Troubleshooting Information" section on page 13-4), you can gather a customer's operating system environment. Based upon this diagnosis, Cisco has identified the following conflicts with third-party applications and can recommend the following resolutions.

Adobe and Apple—Bonjour Printing Service

- Adobe Creative Suite 3
- BonJour Printing Service
- iTunes

Symptom Unable to successfully verify the IP forwarding table.

Possible Cause The AnyConnect event logs indicate a failure to identify the IP forwarding table and indicate the following entries in the routing table:

```
Destination 169.254.0.0
Netmask 255.255.0.0
Gateway 10.64.128.162
Interface 10.64.128.162
Metric 29
```

Recommended Action 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.

AT&T Communications Manager Versions 6.2 and 6.7

Symptom A failure to connect or pass traffic occurs when a customer has an AT&T Sierra Wireless 875 card on several computers. Versions 6.2 to 6.7 seem to conflict with AnyConnect.

Possible Cause CSTP transport failure indicates that the transport layer is compromised by the AnyConnect Virtual Adapter.

Recommended Action 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**.

AT&T Global Dialer

Symptom The client operating system sometimes experiences a blue screen, which causes the creation of a mini dump file.

Possible Cause The AT&T Dialer intermediate driver failed to handle pending packets correctly and caused the operating system to crash. Other NIC card drivers (such as Broadcom) do not exhibit this problem.

Recommended Action Upgrade to the latest 7.6.2 AT&T Global Network Client.

Citrix Advanced Gateway Client Version 2.2.1

Symptom The following error may occur when disconnecting the AnyConnect session:

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

Possible Cause During the freeing of memory, the crash occurs as a result of the Citrix CtxLsp.dll, which gets loaded into every process using Winsock.

Recommended Action Remove the Citrix Advanced Gateway Client until Citrix can resolve this generic problem with CtxLsp.dll.

Firewall Conflicts

Third-party firewalls can interfere with the firewall function configured on the ASA group policy.

Juniper Odyssey Client

Symptom When wireless suppression is enabled, the wireless connection drops if a wired connection is introduced. With wireless suppression disabled, the wireless operates as expected.

Possible Cause The Odyssey Client should not manage the network adapter.

Recommended Action Configure the Odyssey Client with the steps below:

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.
2. Open the registry and go to HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual.
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 are pushed down to other clients.

Kaspersky AV Workstation 6.x

Symptom When Kaspersky 6.0.3 is installed (even if disabled), AnyConnect connections to the 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.).
```

Possible Cause A known incompatibility exists between Kaspersky AV Workstation 6.x and AnyConnect.

Recommended Action Uninstall Kaspersky and refer to their forums for additional updates.

McAfee Firewall 5

Symptom A UDP DTLS connection cannot be established.

Possible Cause McAfee Firewall defaults to blocking incoming IP fragments and thus blocking DTLS if fragmented.

Recommended Action In the McAfee Firewall central console, choose **Advanced Tasks > Advanced options and Logging** and uncheck the **Block incoming fragments automatically** check box in McAfee Firewall.

Microsoft Internet Explorer 8

Symptom You cannot install AnyConnect from the WebVPN portal when using Internet Explorer 8 with Windows XP SP3.

Possible Cause The browser crashes with the installation.

Recommended Action As recommended by Microsoft, remove MSJVM. Refer to Microsoft Knowledge Based Article KB826878.

Microsoft Routing and Remote Access Server

Symptom When AnyConnect attempts to establish a connection to the host device, the following termination error is returned to the event log:

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service "Routing and Remote Access" is incompatible with the Cisco
AnyConnect VPN Client.
```

Possible Cause RRAS and AnyConnect conflict over the routing table. With RRAS, the computer acts as an Ethernet router and therefore modifies the routing table the same way as AnyConnect does. The two cannot run together since AnyConnect depends on the routing table to properly direct traffic.

Recommended Action Disable the RRAS service.

Microsoft Windows Updates

Symptom The following message is encountered when trying to establish a VPN connection:

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

Possible Cause A recent Microsoft update to the certclass.inf file has occurred. The following error appears in the C:\WINDOWS\setupapi.log:

```
#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.
```

Recommended Action Check which updates have recently been installed by entering **C:\>systeminfo** at the command prompt or checking the C:\WINDOWS\WindowsUpdate.log. To attempt a repair, use the following steps:

1. Open a command prompt as an admin.
2. Enter **net stop CryptSvc**.
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.
4. When prompted, choose **OK** to attempt the repair. Exit the command prompt and reboot.

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.

Microsoft Windows XP Service Pack 3

Symptom You cannot install the AnyConnect client. The following error message appears:

```
This application has failed to start because dot3api.dll was not found.
Re-installing the application may fix this problem.
```

Possible Cause The missing dot3api.dll file is a known issue.

Recommended Action Reinstall regsvr32 dot3api.dll and reboot the operating system.

OpenVPN Client

Symptom An error indicates that the version of TUN is already installed on this system and is incompatible with the AnyConnect client.

Possible Cause The Mac OS X Shimo VPN Client can cause this.

Recommended Action Uninstall the Viscosity OpenVPN Client.

Load Balancers

Symptom The connection fails due to lack of credentials.

Possible Cause While the browser may cache the DNS results, additional applications such as the port forwarder and smart tunnels may not. If you log into X.4 and the DNS resolver is set to use x.15, the PF applet or smart tunnel application resolves the DNS and connects to X.15. Since no sessions were established, the connection fails due to lack of credentials.

Recommended Action The third-party load balancer has no insight into the load on the 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 ASA load balancing.

Wave EMBASSY Trust Suite

Symptom The AnyConnect client fails to download and produces the following error message:

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

Possible Cause If you gather the mdmp file, the decode of the crash mdmp file indicates that a third-party dll is resident.

Recommended Action Upload the patch update to version 1.2.1.38 to resolve all dll issues.

Layered Service Provider (LSP) Modules and NOD32 AV

Symptom When AnyConnect attempts to establish a connection, it authenticates successfully and builds the ssl session, but then the AnyConnect client crashes in the vpndownloader.

Possible Cause The LSP component imon.dll has incompatibility issues.

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

LSP Symptom 2 Conflict

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

Possible Cause An Intel Mobile Bandwidth LSP Module such as impbw.dll may have caused a fault on the Intel code.

Recommended Action Uninstall the LSP module.

LSP Slow Data Throughput Symptom 3 Conflict

Symptom Slow data throughput may occur with the use of NOD32 V4.0.

Possible Cause The conflict involves Cisco AnyConnect and NOD32 Antivirus 4.0.468 x64 using Windows 7.

Recommended Action Go to **Protocol Filtering > SSL** in the Advanced Setup and enable SSL protocol scanning. Now go to **Web access protection > HTTP, HTTPS** and check **Do not use HTTPS protocol checking**. When the setting is enabled, go back to **Protocol filtering > SSL** and disable **SSL protocol scanning.**

EVDO Wireless Cards and Venturi Driver

Symptom A client disconnect occurred and produced the following in the event log:

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

Possible Cause Check the Application, System, and AnyConnect event logs for a relating disconnect event and determine if a NIC card reset was applied at the same time.

Recommended Action Ensure that the Venturi driver is up to date. Disable **Use Rules Engine** in the 6.7 version of the AT&T Communications Manager.

DSL Routers Fail to Negotiate

Symptom DTLS traffic was failing even though it was successfully negotiated.

Possible Cause The DSL routers were blocking return DTLS traffic. No settings on the Air Link would allow a stable DTLS connection.

Recommended Action Connecting to a Linksys router with factory settings allowed a stable DTLS session and no interruption in pings. Add a rule to allow DTLS return traffic.

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

Symptom The AnyConnect log indicates a failure to fully establish a connection to the secure gateway.

Possible Cause The client logs indicate multiple occurrences of NETINTERFACE_ERROR_INTERFACE_NOT_AVAILABLE. These errors occur when the client is attempting to retrieve operating system information on the computer's network interface used to make the SSL connection to the secure gateway.

Recommended Action If you are uninstalling the Integrity Agent and then installing AnyConnect, enable TCP/IP. 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 AnyConnect adapter appears in the Device Manager. If there is only one instance, authenticate with AnyConnect, and after 5 seconds, manually enable the adapter from the Device Manager. If any suspect drivers have been enabled within the AnyConnect adapter, disable them by unchecking them in the Cisco AnyConnect VPN Client Connection window.

Performance Issues with Virtual Machine Network Service Drivers

Symptom When using AnyConnect on some client computers, performance issues have resulted.

Possible Cause The virtual machine network driver virtualizes a physical network card or connection. When binding other Virtual Machine Network Services to the Cisco AnyConnect VPN Client Connection network adapter, performance issues occurred. The client device became infected with some malware and introduces a delay around SSL_write().

Recommended Action Uncheck the binding for all IM devices within the AnyConnect 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 AnyConnect results.

Kaspersky AntiVirus and Telemetry Module

Symptom When the Telemetry module is installed, AnyConnect may delete the main executable of the Kaspersky AntiVirus 8 suite (avp.exe).

Possible Cause Using Windows 7 64-bit German language with AnyConnect 3.0.5080 or later and Kaspersky AV 8 causes conflict.

Recommended Action Remove the Telemetry module.