



CHAPTER 8

Managing, Monitoring, and Troubleshooting AnyConnect Sessions

This chapter explains these subjects and tasks:

- [Disconnecting All VPN Sessions, page 8-1](#)
- [Disconnecting Individual VPN Sessions, page 8-1](#)
- [Viewing Detailed Statistical Information, page 8-2](#)
- [Resolving VPN Connection Issues, page 8-4](#)
- [Using DART to Gather Troubleshooting Information, page 8-5](#)

Disconnecting All VPN Sessions

To log off all AnyConnect Client and SSL VPN sessions, use the **vpn-sessiondb logoff svc** command in global configuration mode:

vpn-sessiondb logoff svc

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 svc
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 svc** command.

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

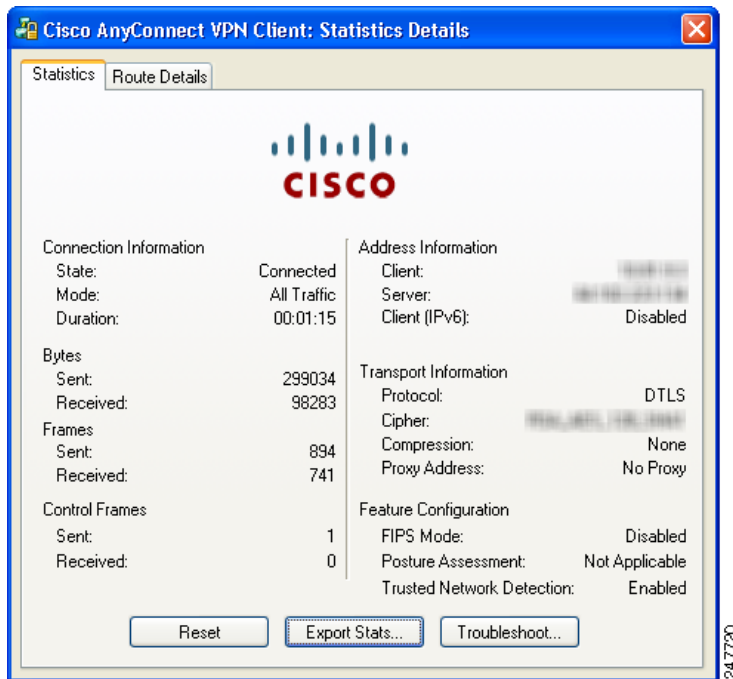
```
hostname# vpn-sessiondb logoff name testuser
INFO: Number of sessions with name "testuser" logged off : 1
```

Viewing Detailed Statistical Information

You or the user can view statistical information for a current AnyConnect client session by clicking 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.

Figure 8-1 AnyConnect VPN Client Statistics Details Dialog



The options available in this window depend on the packages that are loaded on the client PC. If an option is not available, its radio 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 DART (Diagnostic AnyConnect Reporting Tool) wizard which bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. See [Using DART to Gather Troubleshooting Information](#), page 8-5 for information about the DART package.

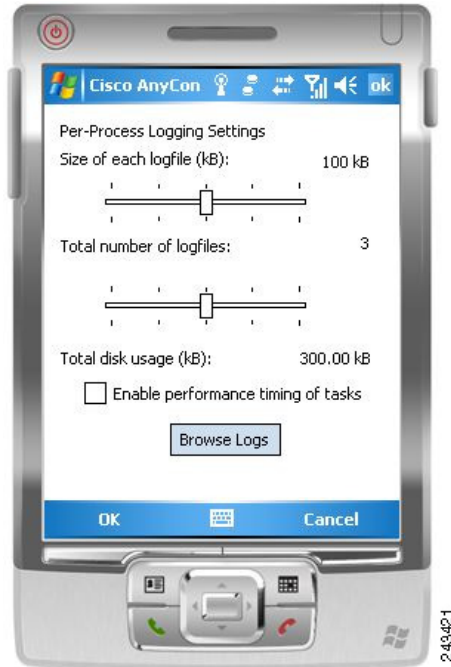
Viewing Statistics on a Windows Mobile Device

An AnyConnect user with a Windows Mobile device can also use the statistical details export and logging functions by clicking Menu on the lower-right corner of the screen and selecting the desired function from the menu that appears (Figure 8-2).

Figure 8-2 Windows Mobile Logging Menu



Clicking on Logging opens the logging settings dialog box (Figure 8-3).

Figure 8-3 Windows Mobile Logging Settings Dialog Box

Move the sliders on this dialog box to control the total number of log files and the size of each log file and to enable performance timing of tasks.

Click Browse Logs to display an HTML list of the log messages in a separate browser window.

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. This is particularly true of 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 security appliance. 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 the AnyConnect Client,

-
- 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 Client connections established in SSL and those established in SSL with DTLS.

Eliminating Compression to Improve VPN Performance and Accommodate Windows Mobile Connections

On low-bandwidth connections, compression increases the communications performance between the security appliance and the client by reducing the size of the packets being transferred. By default, compression for all SSL VPN connections is enabled on the security appliance, both at the global level and for specific groups or users. For broadband connections, compression might result in poorer performance.



Note

The AnyConnect client for Windows Mobile does not support compression.

You can configure compression globally using the CLI command **compression svc** command from global configuration mode.

Using DART to Gather Troubleshooting Information

DART is the Diagnostic AnyConnect Reporting Tool that you can use to collect data useful for troubleshooting AnyConnect install and connection problems. DART supports Windows 7, Windows Vista, and Windows XP.

The DART wizard runs on the computer that runs AnyConnect Client. 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.

Any version of DART works with any version of AnyConnect; the version numbers of each are no longer synchronized. To optimize DART, we recommend downloading the most recent version available on the Cisco AnyConnect VPN Client Software Download site, regardless of the AnyConnect version you are using.

DART is currently available as a standalone installation, or the administrator can push this application to the client PC 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

Cisco has made DART available to its customers so that they may have a convenient method of gathering important troubleshooting information; however, be aware that DART is in the “Beta” phase of its release cycle.

Getting the DART Software

DART is available as part of the AnyConnect client download and installation package or as a standalone .msi file.

Any version of DART works with any version of AnyConnect; the version numbers of each are no longer synchronized. To optimize DART, we recommend downloading the most recent version available on the Cisco AnyConnect VPN Client Software Download site, regardless of the AnyConnect version you are using.

These are the AnyConnect downloads, containing DART, on Cisco.com. Refer to the Release Notes for Cisco AnyConnect VPN Client for the latest version numbers:

- **anyconnect-all-packages-2.4.version-k9.zip** — Contains all AnyConnect packages.
- **anyconnect-dart-win-2.4.version-k9.pkg** — Contains *only* the DART installation package, not the AnyConnect or vpngina software. Use this when installing DART as a standalone application.

Installing DART

The administrator can include DART as part of the AnyConnect installation, or registered users of Cisco.com can download the file from <http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect>, as described in [Getting the DART Software](#), and install it manually on the PC.

When the user downloads the AnyConnect client, a new version of DART, if available, is also automatically downloaded to the user's PC. When a new version of the AnyConnect client is downloaded as part of an automatic upgrade, that download 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 **svc 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 security appliance, 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, begin by clicking **Configuration** and then click **Remote Access VPN > Network (Client) Access > Group Policies**.

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

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.

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 **svc modules value dart** command.

**Note**

If you later change to **svc modules none** or if you remove the DART selection in the **Optional Client Modules to Download** field, DART remains installed. There is no way for the security appliance to 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 the AnyConnect client. When the user connects, DART is upgraded automatically when an AnyConnect package with a higher version of DART is uploaded and configured on the security appliance.

To run DART, see [Running DART on a Windows PC, page 8-7](#).

Manually Installing DART on the Host

- Step 1** Get the DART software from Cisco.com. See, [Getting the DART Software, page 8-6](#), and store **anyconnect-dart-win-2.4.version-k9.pkg** locally.
- Step 2** Using a file compression utility such as WinZip®, extract the contents of the **anyconnect-dart-win-2.4.version-k9.pkg** and maintain the directory structure.
- Step 3** Open the **binaries** directory created from extracting the contents of the **anyconnect-dart-win-2.4.version-k9.pkg** file.
- Step 4** Double-click the **anyconnect-dart-win-2.4.version-k9.msi** file to launch the **DART Setup Wizard**.
- Step 5** Click **Next** at the Welcome screen.
- Step 6** Select **I accept the terms in the License Agreement** to accept the end user license agreement and click **Next**.
- Step 7** Click **Install** to install DART. The installation wizard installs **DartOffline.exe** in the <System Drive>\Program Files\Cisco\Cisco DART directory.
- Step 8** Click **Finish** to complete the installation.

To run DART, see [Running DART on a Windows PC, page 8-7](#).

Running DART on a Windows PC

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

- Step 1** Launch the AnyConnect client GUI.
- 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. 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 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 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.