CHAPTER 6

Monitoring and Maintaining the AnyConnect Client

This chapter describes some common maintenance and monitoring procedures for network administrators dealing with the Cisco AnyConnect Client. You perform these procedures on the security appliance:

Viewing AnyConnect Client and SSL VPN Sessions

You can view information about active sessions using the **show vpn-sessiondb** command in privileged EXEC mode:

show vpn-sessiondb svc

The following example shows the output of the **show vpn-sessiondb svc** command:

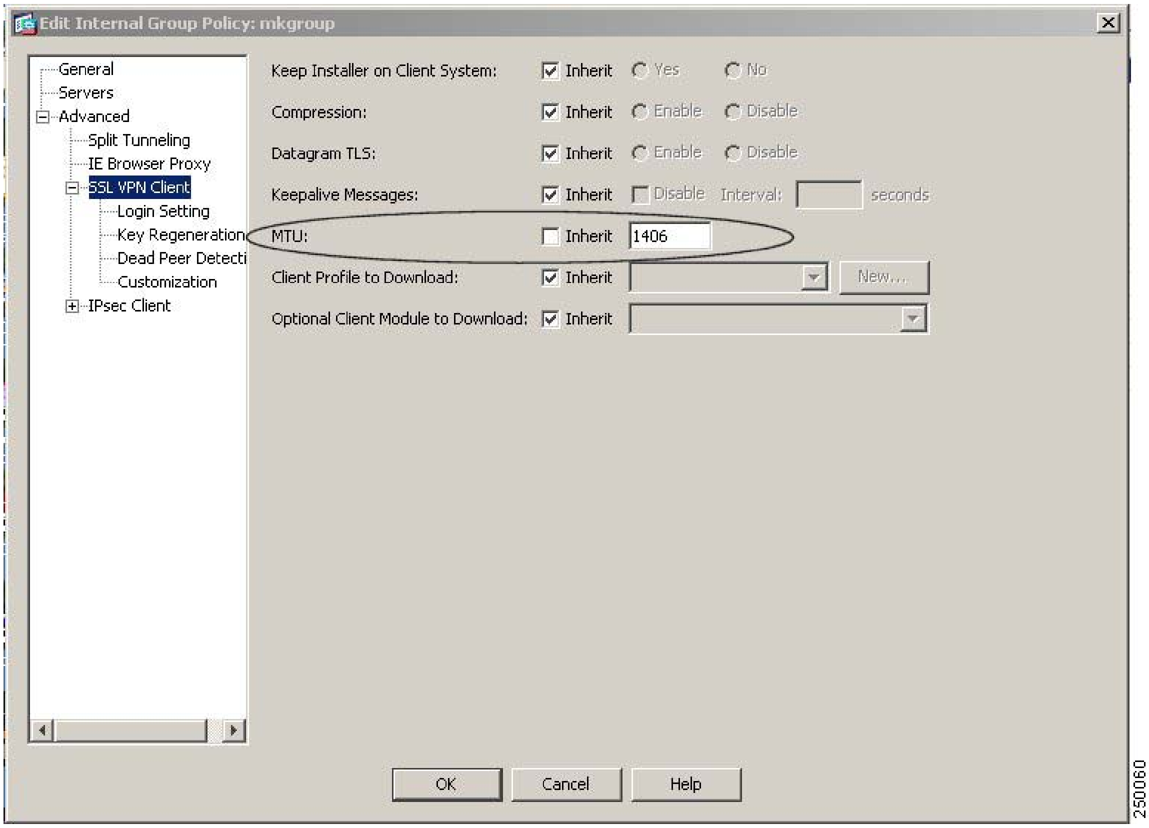
```
hostname# show vpn-sessiondb svc

Session Type: SVC

Username     : testuser               Index        : 17
Assigned IP  : 209.165.200.224        Public IP    : 192.168.23.45
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 17457                  Bytes Rx     : 69502
Group Policy : GroupPolicy            Tunnel Group : CertGroup
Login Time   : 15:19:57 EDT Fri May 25 2007
Duration     : 0h:04m:27s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

To see more detailed information, including the number of AnyConnect (SSL VPN) tunnels, DTLS tunnels, and Clientless tunnels, use the command **show vpn-sessiondb detail svc**.

Adjusting MTU Size Using ASDM

You can adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by the AnyConnect Client by selecting Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add or Edit. The Edit Internal Group Policy dialog box opens (fig).

Figure 6-1 Edit Internal Group Policy Dialog Box



Keep Installer on Client System: ☑ Inherit ○ Yes ○ No

Compression: ☑ Inherit ○ Enable ○ Disable

Datagram TLS: ☑ Inherit ○ Enable ○ Disable

Keepalive Messages: ☑ Inherit □ Disable Interval: seconds

MTU: □ Inherit 1406

Client Profile to Download: ☑ Inherit New...

Optional Client Module to Download: ☑ Inherit

Select Advanced > SSL VPN Client. 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 the AnyConnect Client. The Cisco SSL VPN Client (SVC) is not capable of adjusting to different MTU sizes. This setting affects AnyConnect Client connections established in SSL and those established in SSL with DTLS.

Adjusting MTU Size Using the CLI

You can adjust the Maximum Transmission Unit size (from 256 to 1406 bytes) for SSL VPN connections established by the AnyConnect Client by using the **svc mtu** command from group policy webvpn or username webvpn configuration mode:

[**no**] **svc mtu** *size*

This command affects only the AnyConnect Client. The Cisco SSL VPN Client (SVC) is not capable of adjusting to different MTU sizes.

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 command affects AnyConnect Client connections established in SSL and those established in SSL with DTLS.

The following example configures the MTU size to 1200 bytes for the group policy *telecommuters*:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc mtu 1200
```

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 is used by both the client and the security appliance to set the maximum size of the packet to be transmitted over the tunnel. If an end 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 address the problem.

The client proposes an MTU value that is 94 bytes less than the MTU of the physical adapter used for the SSL and DTLS connection to the security appliance. The security appliance accepts the lesser of the configured MTU or the value proposed by the client. Both the client and the security appliance use the value selected by the security appliance.

For example, if the physical adapter on the PC has been changed to use an MTU of 1300, then the client proposes an MTU of 1206 to the security appliance. If the security appliance is set for a value lower than 1206, both the client and the security appliance use the lower value that was set using the MTU configuration command.

Logging Off AnyConnect Client 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#
```

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 (see Viewing AnyConnect Client and SSL VPN Sessions, page 6-1).

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
```

Updating AnyConnect Client and SSL VPN Client Images

You can update the client images on the security appliance at any time using the following procedure:

Step 1 Copy the new client images to the security appliance using the **copy** command from privileged EXEC mode, or using another method.

Step 2 If the new client image files have the same filenames as the files already loaded, reenter the **svc image** command that is in the configuration. If the new filenames are different, uninstall the old files using the **no svc image** command. Then use the **svc image** command to assign an order to the images and cause the security appliance to load the new images.

Viewing Detailed Statistical Information

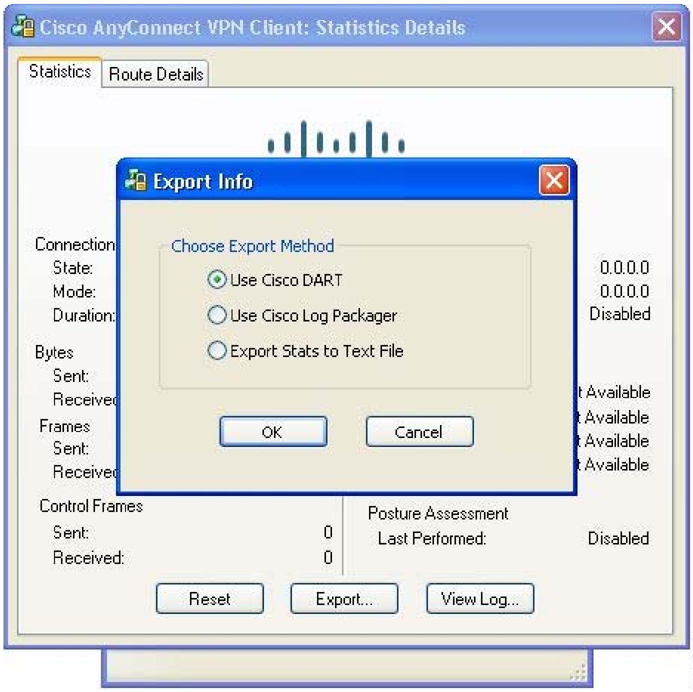
A user can view statistical information for a current AnyConnect client session by clicking the Details button on the GUI (see Figure 1-3).

This opens the Statistics Details window (Figure 1-4). On the Statistics tab in this window, you can reset the statistics, export the statistics, or view an HTML-format log of the statistics for this session. This section describes how to export and view the detailed session statistics.

Exporting Statistics

To export AnyConnect connection statistics to a reporting format, click Export at the bottom of the Statistics Details window. The Export Info dialog box appears (Figure 6-2).

Figure 6-2 Export Info Dialog Box



Choose Export Method

● Use Cisco DART
○ Use Cisco Log Packager
○ Export Stats to Text File

Sent:	0
Received:	0
Last Performed:	Disabled

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:

- Use Cisco DART—DART (Diagnostic AnyConnect Reporting Tool) bundles specified log files and diagnostic information that can be used for analyzing and debugging the AnyConnect client connection. *See Release Notes for Cisco AnyConnect VPN Client, Release 2.3* for information about the DART package.
- Use Cisco Log Packager—Collects log files from compliant Cisco utilities (not just the AnyConnect client) into a particular folder and compresses them into a .zip file. This function is similar to DART, but it uses a different format.
- Export Stats to Text File—Saves the connection statistics to a text file for later analysis and debugging.

Select an option and click OK. The AnyConnect client prompts you for the location to which you want to save the file or bundle. Enter a file name and save the file.

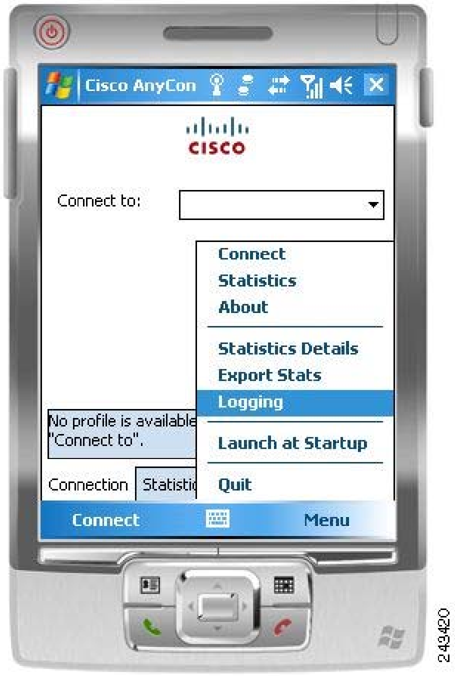
Viewing the Log

To view the log as an HTML file in a browser window, click View Log on the Statistics Detail window. The log information appears in a new browser window, showing the number of message instances, the end-user node name, the event codes and types, the log file name, the event messages, the source of the message, and the time themessage was generated. The browser window might take a short time to appear after you click View Log.

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 6-3).

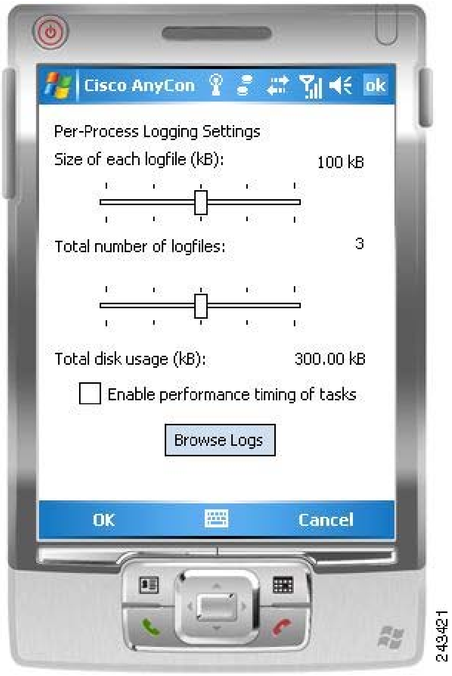
Figure 6-3 Windows Mobile Logging Menu



No profile is available
"Connect to".

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

Figure 6-4 ***Windows Mobile Logging Settings Dialog Box***



Per-Process Logging Settings

Size of each logfile (kB): 100 kB

Total number of logfiles: 3

Total disk usage (kB): 300.00 kB

□ Enable performance timing of tasks

Browse Logs

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.