



# CHAPTER 11

## Troubleshooting and Programmer Notes

---

This chapter contains information to help you resolve problems installing or running the VPN Client. It also contains notes helpful for writing programs for special needs.

This chapter includes the following main topics:

- [Troubleshooting the VPN Client](#)
- [Changing the MTU Size](#)
- [Delete With Reason](#)
- [Start Before Logon and GINAs—Windows Only](#)
- [Programmer Notes](#)
- [IKE Proposals](#)

## Troubleshooting the VPN Client

This section describes how to perform the following tasks:

- [Gathering VPN Client Logs](#)
- [Getting Information About Severity 1 Events](#)
- [Gathering System Information for Customer Support](#)
- [Solving Common Problems](#)
- [Changing the MTU Size](#)

## Gathering VPN Client Logs

The Logs folder in the VPN Client install directory stores log files of VPN Client sessions. Log files are text files with names in the format Log-yyyy-MM-dd-hh-mm-ss.txt. For information on log files and logging, refer to *VPN Client User Guide for Windows*, Chapter 7 “Managing the VPN Client” or *VPN Client User Guide for Mac OS X*, Chapter 7, “Managing the VPN Client.”

You can obtain these log files for analysis and send them to Customer Support, when necessary.

## Getting Information About Severity 1 Events

When severity 1 events occur, the VPN Client logs them in a text file named `faultlog.txt`. This file exists in the installation directory of the VPN Client. This event logging occurs whether the logviewer application is running or not. For example errors occurring during service initialization cannot be logged to the log viewer, because these errors occur before the service has attached itself to the log viewer. Therefore, you can open the `faultlog.txt` file to read these severity 1 events. This log file provides a useful tool to help you analyze what is happening and gives you information to report to customer support if you need to contact your customer support representative.

## Gathering System Information for Customer Support

If you are having problems running the VPN Client on your PC, you can gather system information that is helpful to a customer support representative and e-mail it to us. We recommend that you do the following *before* you contact us.

### If Your Operating System is Windows 98, 98 SE, ME, 2000, or XP



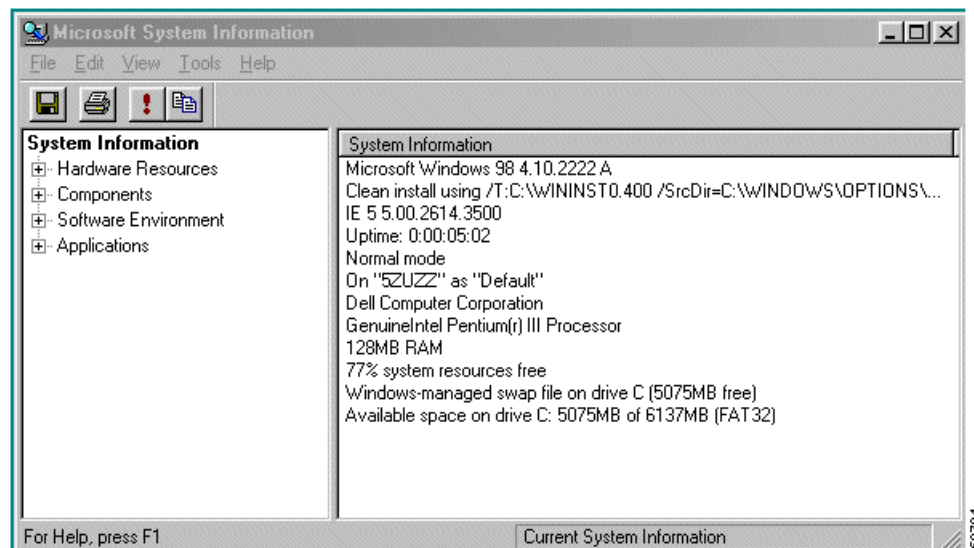
#### Note

The VPN Client no longer officially supports Windows 95, Windows 98, and Windows ME.

Go to the **Start** menu and select **Programs > Accessories > System Tools > System Information**.

Windows displays the Microsoft System Information screen, such as the one in [Figure 11-1](#).

**Figure 11-1** System Information Screen on Windows 98



Select a category and the screen displays details for that category. You can then execute the **Export** command and choose a name and destination. Windows creates a text file, which you can attach to an e-mail message and send to the support center.

## If Your Operating System is Windows NT or Windows 2000

On the Windows NT or Windows 2000 operating system, you can run a utility named `WINMSD` from a command-line prompt. `WINMSD` generates a file containing information about your system configuration, and the software and drivers installed.

To use this utility, perform the following steps:

---

**Step 1** Go to the **Start** menu and select **Programs > Command Prompt**.

This action displays a window with a DOS prompt, such as `c:\`.

**Step 2** Type the following command at the DOS prompt:

```
c: \>winmsd /a /f
```

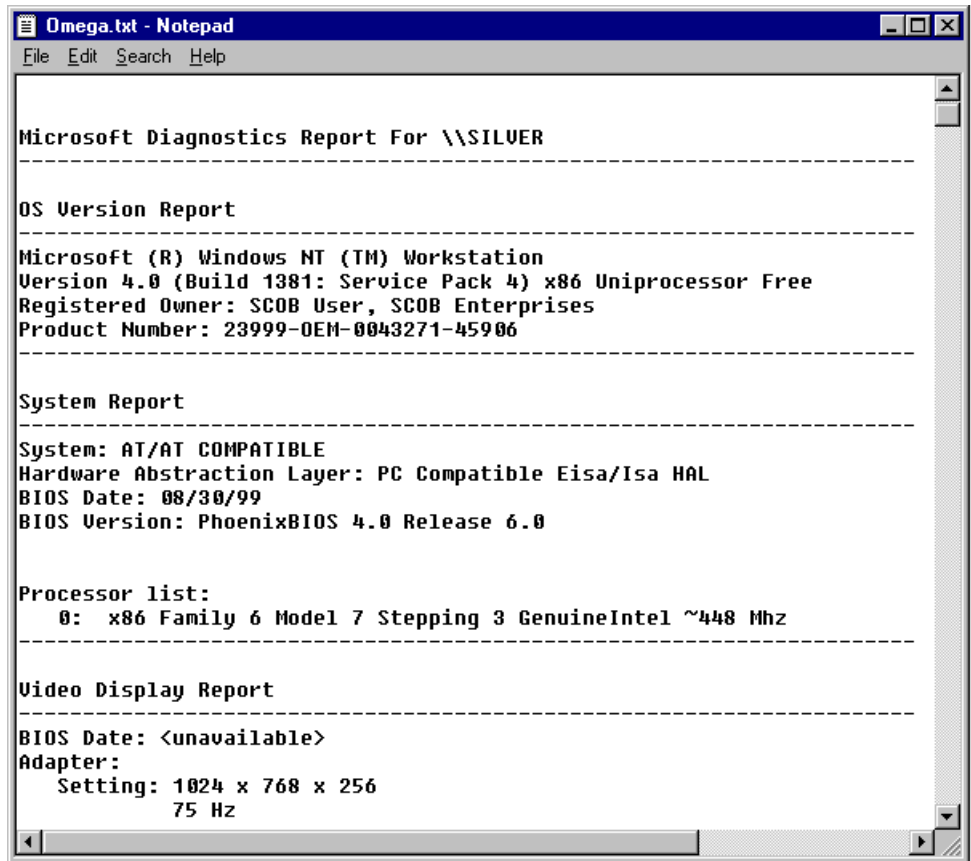
where **/a** = all and **/f** = write to file.

This command generates a text (.txt) file with the name of your computer and places the file in the directory from which you run the command. For example, if the name of your machine is `SILVER` and you execute the command from the `c:` drive (as shown above), the text file name is `silver.txt`.

---

If you open the file with a text editor, such as Notepad, you see a file such as the one shown in [Figure 11-2](#), which was from a Windows NT system.

Figure 11-2 System Text File



You can attach this file to an e-mail message and send it to the support center.

## If Your Operating System is Mac OS X

**Step 1** From the command line, execute the following commands:

```

ifconfig -a
uname -a
kextstat
  
```

Copy the output from the above commands, paste it into an e-mail message, and send it to Support.

## Solving Common Problems

This section describes some common problems and what to do about them.

### Shutting Down on Windows 98

You may experience a problem with your Windows 98 system shutting down when the VPN Client software is installed. If so, you need to disable the fast shutdown feature, as follows:

- 
- Step 1** At the Microsoft System Information screen (shown in [Figure 11-1](#)), select **Tools > System Configuration**. Microsoft displays a **Properties** page.
  - Step 2** From the **General** page, select the **Advanced** button.
  - Step 3** Choose the **Disable Fast Shutdown** option.
- 

### Booting Automatically Starts up Dial-up Networking on Windows 95

Some versions of Internet Explorer silently control startup options in Windows 95 so that every time you start your system, Dial-Up Networking launches. If this occurs, as it does in Internet Explorer 3.0, go to **View > Options > Connections** and uncheck the option **Connect to the Internet as needed**.

## Changing the MTU Size

The Set MTU option is used primarily for troubleshooting connectivity problems.

**Note**

---

The VPN Client automatically adjusts the MTU size to suit your environment, so running this application is not recommended.

---

The maximum transmission unit (MTU) parameter determines the largest packet size in bytes that the client application can transmit through the network. If the MTU size is too large, the packets may not reach their destination. Adjusting the size of the MTU affects all applications that use the network adapter. Therefore the MTU setting you use can affect your PC's performance on the network.

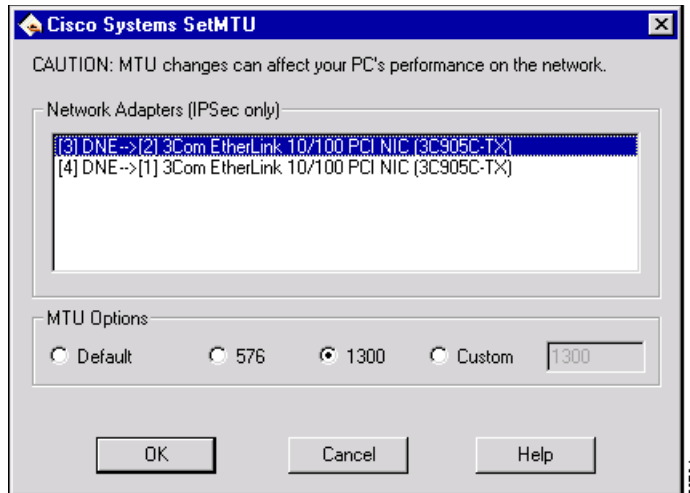
MTU sizing affects fragmentation of IPsec and IPsec through NAT mode packets to your connection destination, because IPsec encapsulation increases packet size. A large size (for example, over 1300) can increase fragmentation. Using 1300 or smaller usually prevents fragmentation. Fragmentation and reassembly of packets at the destination causes slower tunnel performance. Also, many firewalls do not let fragments through.

## Changing the MTU Size—Windows

To change the size of the MTU for Windows, use the following procedure:

- 
- Step 1** Select **Start > Programs > Cisco Systems VPN Client > SetMTU**.  
The Set MTU window appears.

Figure 11-3 Setting MTU Size on Windows NT



**Step 2** Click a network adapter on the list of network adapters.

**Step 3** Click one of the following choices under MTU Options:

Default	The factory setting for this adapter type.
576 (in bytes)	The standard size for dial-up adapters.
1300 (in bytes)	The choice recommended for both straight IPsec and IPsec through NAT. Using this value guarantees that the client does not fragment packets under normal circumstances.
Custom	Enter a value in the box. The minimum value for MTU size is 68 bytes.

**Step 4** Click **OK**.

*You must restart your system for your change to take effect.*

## Changing the MTU Size—Linux, Solaris, and Mac OS X

To change the MTU size:

**Step 1** Open a terminal (Mac OS X-only).

**Step 2** Type the following command:

```
sudo ifconfig en0 mtu 1200
```

(Replace the en0 with the appropriate interface, and replace 1200 with the desired mtu.)

**Step 3** The changes take effect immediately.

## Setting the MTU from the Command Line

You can use the SetMTU command at the command-line prompt to set the MTU size. The syntax of the SetMTU command follows:

**setmtu** */switch value*

where switch can be one of the following:

Switch	Description
<i>/s value</i>	Set the MTU for all adapters to <i>value</i> . This sets the MTU at the IP layer. This action requires a reboot.
<i>/r</i>	Reset the MTU for all adapters to the operating system default at the IP layer. This action requires a reboot.
<i>/va value</i>	Set the MTU for the virtual adapter to <i>value</i> . This sets the MTU at the MAC layer. This action does not require a reboot.
<i>/vaReset</i>	Reset the MTU for the virtual adapter to the default (1500) at the MAC layer. This action does not require a reboot.
<i>/?</i>	Display help on the SetMTU switches.

The new setting remains in effect the next time a tunnel is established.

## Delete With Reason

When a disconnect occurs, the VPN Client displays a reason code or reason text. The VPN Client supports the delete with reason function for client-initiated disconnects, secure-gateway-initiated disconnects, and IPsec deletes.

- If you are using a GUI VPN Client, a pop-up message appears stating the reason for the disconnect, the message is appended to the Notifications log, and is logged in the IPsec log (Log Viewer window).
- If you are using a command-line client, the message appears on your terminal and is logged in the IPsec log.
- For IPsec deletes, which do not tear down the connection, an event message appears in the IPsec log file, but no message pops up or appears on the terminal.



### Note

The secure gateway you are connecting to must be running software version 4.0 or later to support delete with reason functionality.

Table 11-1 describes the reason codes and the corresponding messages.

**Table 11-1** Delete with Reason Codes

Reason Code	Translated Text
IKE_DELETE_SERVER_SHUTDOWN	Peer has been shut down
IKE_DELETE_SERVER_REBOOT	Peer has been rebooted.
IKE_DELETE_MAX_CONNECT_TIME	Maximum configured connection time exceeded.

**Table 11-1 Delete with Reason Codes**

Reason Code	Translated Text
IKE_DELETE_BY_USER_COMMAND	Manually disconnected by administrator.
IKE_DELETE_BY_ERROR	Connectivity to Client lost.
IKE_DELETE_NO_ERROR	Unknown error.
IKE_DELETE_IDLE_TIMEOUT	Maximum idle time for session exceeded.
IKE_DELETE_P2_PROPOSAL_MISMATCH	Policy negotiation failed
IKE_DELETE_FIREWALL_MISMATCH	Firewall policy mismatch.
IKE_DELETE_CERT_EXPIRED	Certificates used with this connection entry have expired.
IKE_DELETE_BY_EXPIRED_LIFETIME	Maximum configured lifetime exceeded.

All text messages for client-initiated disconnects begin with “Secure VPN Connection terminated terminated locally by the client”.

All text messages for secure-gateway-initiated disconnects begin with “Secure VPN Connection terminated by Peer X.X.X.X”, where X.X.X.X is the IP address of the secure gateway.

The translated reason code or the reason text follows.

## Configuring Delete with Reason on a VPN Concentrator

To receive disconnect information from a 4.0 or greater VPN Concentrator, you must configure the feature as follows:

- 
- Step 1** Go to Configuration | Tunneling | IPsec | Alerts
  - Step 2** Check **Alert when disconnecting**.
  - Step 3** Click **Apply**.
  - Step 4** Save the configuration.
- 

## Start Before Logon and GINAs—Windows Only

The VPN Client can load prior to logging in to a Windows NT platform (Windows NT 4.0, Windows 2000, and Windows XP). This feature lets remote users establish a VPN connection to a private network where they can successfully log in to a domain. When start before logon (SBL) is enabled on a Windows NT platform, the VPN Client tries to replace the standard Microsoft logon dialog box (the same one that appears after you press Ctrl+Alt+Del when booting your PC, called a GINA). The name of the Microsoft GINA is msgina.dll and you can find it in the registry at the location:

```
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
GinaDLL = msgina.dll
```

The VPN Client replaces the msgina.dll with the VPN Client's GINA (csgina.dll), and then points to it so that you can still see and use the MS GINA. When you start your PC and press Ctrl+Alt+Del, you are launching the VPN Client Dialer application and the MS logon dialog box. The VPN Client detects whether the necessary Windows services are running and if not, displays a message asking you to wait.

If you look in the VPN Client registry, you see the following parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 1
PreviousGinaPath = msgina.dll
```



#### Note

When you enable start before logon for the first time, you must reboot for the system to load csgina.

## Fallback Mode

In some cases a third-party program replaces the MS GINA, and in some of these cases the VPN Client works with the third-party program, while in other cases, it does not. The VPN Client maintains a list of incompatible GINAs that it does not work with, and does not replace the GINA file in use. This is called *fallback* mode. The list of incompatible GINAs resides in the vpnclient.ini file, and the VPN Client refers to the list only during installation. The following entry is an example.

```
IncompatibleGinas=PALgina.dll,nwgina.dll,logonrem.dll,ngina.dll
```

In fallback mode, the VPN Client performs differently when start before logon is in use. Instead of loading when you press Ctrl+Alt+Del, the VPN Dialer loads as soon as the VPN service starts. When operating in fallback mode, the VPN Client does not check to see if the necessary Windows services have started. As a result, the VPN connection could fail if initiated too quickly. In fallback mode, when the VPN connection succeeds, you then press Ctrl+Alt+Del to get to the Microsoft logon dialog box. In this mode, you see the following VPN Client registry parameters and values:

```
HKLM\Software\Cisco Systems\VPN Client\
GinaInstalled = 0
PreviousGinaPath = msgina.dll
```

## Incompatible GINAs

If a new problem GINA is discovered after the VPN Client is released, you can add the GINA to the incompatible GINA list in the vpnclient.ini file. Adding the GINA to this list places it in the IncompatibleGinas list in the registry when you install the VPN Client and puts the VPN Client into fallback mode, thus avoiding possible conflicts (see section [Start Before Logon and GINAs—Windows Only, page 11-8](#)).

## Disabling the Firewall Dialogs

You can disable firewall dialogs that display to the user during the SBL period when firewalls are not running. The registry key DisableSBLFirewallCheck controls this function.

The registry location is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\VPN Client\Secure
```

The key is DisableSBLFirewallCheck, with the following values:

- 0 (FALSE)—Do not disable firewall checking. Firewall dialogs appear to users.
- 1- (TRUE)—Disable firewall checking. Firewall dialogs *do not* appear to users.

## Programmer Notes

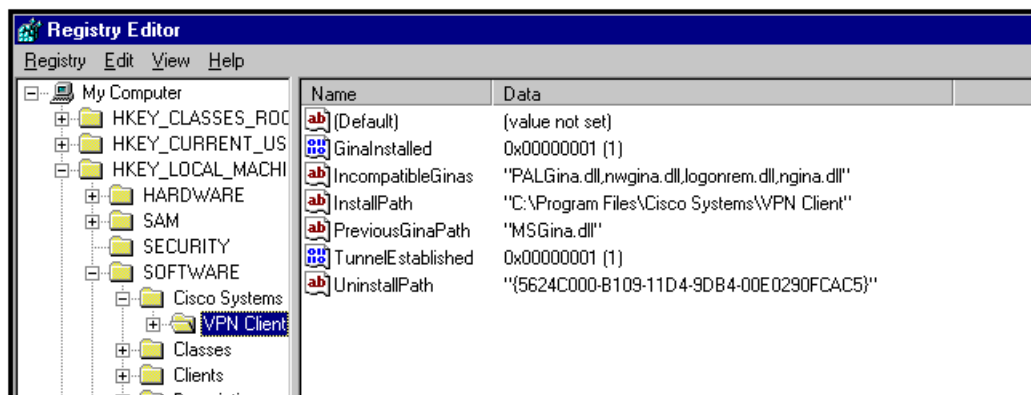
This section contains information to aid a programmer in writing programs that perform routine tasks.

## Testing the Connection

As part of a program, you might want to test a connection to see if it is active before performing the tasks that are the purpose of the program. To test the connection, you can poll the TunnelEstablished entry in the HKEY\_LOCAL\_MACHINE registry.

To see this entry, bring up the Registry Editor and go to SOFTWARE > Cisco Systems > VPN Client. (See [Figure 11-4](#).) In the list of entries, you see TunnelEstablished. This entry can have only two values: 1 or 0. If the connection is working, the value is 1; if not, the value is 0.

**Figure 11-4** Cisco Systems VPN Client Registry Entries



## Command Line Switches for vpngui Command—Windows Only

The vpngui command starts a connection from the command line by bringing up the VPN Client GUI application. You can use switches to specify parameters with this command. You must precede a switch with a forward slash (/) or hyphen (-). Non-Windows platforms allow only a hyphen prefix.

[Table 11-2](#) lists the switches you can include in the vpngui command and describes the task that each switch performs. If the connection entry name contains spaces or other special characters, you must enclose the name in quotes. In the following examples, towork is the name of the connection entry.

**Table 11-2**      **Command Line Switches**




Switch	Parameter	Description
/c	Auto-connect	<p>Starts the VPN Client application for the specified connection entry and displays the authentication dialog. If no connection entry is specified, then the VPN Client uses the default connection entry. The c and sc switches are mutually exclusive.</p> <p>Example: <b>vpngui /c towork</b></p>
/eraseuserpwd	Erase User Password	<p>Erases the user password saved on the Client PC thereby forcing the VPN Client to prompt for a password.</p> <p>Example: <b>vpngui /c /eraseuserpwd towork</b></p> <p> <b>Note</b> A connection entry may have been configured with Saved Password to suppress a password prompt when connecting using a batch file. Use the eraseuserpwd option to return to require password input from the console when connecting. You cannot combine this switch with the pwd switch. You may use it only with the /c or the /sc switch.</p>
/user	Username	<p>Specifies a username for authentication. Suppresses the username prompt in authentication dialog. Used with the pwd switch, it suppresses the authentication dialog entirely. Updates the username in the .pcf file. You can use this parameter only with the /c or the /sc switch.</p> <p>Example: <b>vpngui /c /user robron /pwd siltango towork</b></p> <p> <b>Note</b> If the name supplied is not valid, the VPN Client displays the authentication dialog on a subsequent authentication request.</p>

Table 11-2 Command Line Switches (continued)

Switch	Parameter	Description
/pwd	Password	<p>Specifies a password for authentication. Suppresses the password prompt in authentication dialog. Used with the <code>pwd</code> switch, it suppresses the authentication dialog entirely. Updates the password in the <code>.pcf</code> file during authentication and then clears the password from the <code>.pcf</code> file. You can use this switch only with the <code>/c</code> or the <code>/sc</code> switch.</p> <p>Example: <b><code>vpngui /c /user robron /pwd siltango towork</code></b></p> <hr/> <p> <b>Note</b> If the password supplied is not valid, the VPN Client displays the authentication dialog on a subsequent authentication request. After encrypting and using the password for the connection, the VPN Client clears the password in the <code>.pcf</code> file. Using this option on the command line compromises security and is not recommended.</p> <hr/>
/sd	Silent disconnect	<p>Suppresses connection terminating messages, such as “Your IPsec connection has been terminated.” You can use this parameter to improve the automatic connection process. You can use this switch only with the <code>/c</code> or the <code>/sc</code> switch.</p> <p>Example: <b><code>vpngui /sd towork</code></b></p>

# IKE Proposals

Table 11-3 lists the IKE proposals that the VPN Client supports.

**Table 11-3** Valid VPN Client IKE Proposals

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-3DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-3DES-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
CiscoVPNClient-AES128-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES128-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5	Preshared Keys (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA	Preshared Keys (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-3DES-MD5	Preshared Keys	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA	Preshared Keys	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-DES-MD5	Preshared Keys	MD5/HMAC-128	DES-56	Group 2 (1024 bits)
IKE-AES128-MD5	Preshared Keys	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA	Preshared Keys	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES256-MD5	Preshared Keys	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA	Preshared Keys	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-3DES-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
CiscoVPNClient-DES-MD5-RSA-DH1	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	DES-56	Group 1 (768 bits)
CiscoVPNClient-AES128-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)

Proposal Name	Authentication Mode	Authentication Algorithm	Encryption Algorithm	Diffie- Hellman Group
CiscoVPNClient-AES128-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
CiscoVPNClient-AES256-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
CiscoVPNClient-AES256-SHA-RSA	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
CiscoVPNClient-3DES-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-3DES-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
CiscoVPNClient-AES128-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES128-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
CiscoVPNClient-AES256-MD5-RSA-DH5	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
CiscoVPNClient-AES256-SHA-RSA-DH5	RSA Digital Certificate (XAUTH)	SHA/HMAC-160	AES-256	Group 5 (1536 bits)
CiscoVPNClient-3DES-MD5-RSA	RSA Digital Certificate (XAUTH)	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
HYBRID-3DES-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
HYBRID-DES-MD5-RSA-DH1	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	DES-56	Group 1 (768 bits)
HYBRID-AES128-MD5-RSA	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
HYBRID-AES128-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
HYBRID-AES256-MD5-RSA	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
HYBRID-AES256-SHA-RSA	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
HYBRID-3DES-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
HYBRID-3DES-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
HYBRID-AES128-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
HYBRID-AES128-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
HYBRID-AES256-MD5-RSA-DH5	RSA Digital Certificate (HYBRID)	MD5/HMAC-128	AES-256	Group 5 (1536 bits)

<b>Proposal Name</b>	<b>Authentication Mode</b>	<b>Authentication Algorithm</b>	<b>Encryption Algorithm</b>	<b>Diffie- Hellman Group</b>
HYBRID-AES256-SHA-RSA-DH5	RSA Digital Certificate (HYBRID)	SHA/HMAC-160	AES-256	Group 5 (1536 bits)
IKE-3DES-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 2 (1024 bits)
IKE-3DES-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 2 (1024 bits)
IKE-AES128-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 2 (1024 bits)
IKE-AES128-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 2 (1024 bits)
IKE-AES256-MD5-RSA	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 2 (1024 bits)
IKE-AES256-SHA-RSA	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 2 (1024 bits)
IKE-DES-MD5-RSA-DH1	RSA Digital Certificate	MD5/HMAC-128	DES-56	Group 1 (768 bits)
IKE-3DES-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	3DES-168	Group 5 (1536 bits)
IKE-3DES-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	3DES-168	Group 5 (1536 bits)
IKE-AES128-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-128	Group 5 (1536 bits)
IKE-AES128-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-128	Group 5 (1536 bits)
IKE-AES256-MD5-RSA-DH5	RSA Digital Certificate	MD5/HMAC-128	AES-256	Group 5 (1536 bits)
IKE-AES256-SHA-RSA-DH5	RSA Digital Certificate	SHA/HMAC-160	AES-256	Group 5 (1536 bits)

Table 11-4 lists phase 2 proposals that the VPN Client sends.

**Table 11-4 Phase 2 Proposals**

AES256	MD5	IPCOMPRESSION
AES256	SHA	IPCOMPRESSION
AES128	MD5	IPCOMPRESSION
AES128	SHA	IPCOMPRESSION
AES256	MD5	
AES256	SHA	
AES128	MD5	
AES128	SHA	
3DES	MD5	IPCOMPRESSION
3DES	SHA	IPCOMPRESSION
3DES	MD5	
3DES	SHA	
DES	MD5	IPCOMPRESSION
DES	MD5	
NULL	MD5	
NULL	SHA	

## VPN Client Application Program Interface

The VPN Client software includes an API that customers can use to perform VPN Client tasks without using the standard command-line or graphical interfaces that Cisco provides. The API comprises a shared library that programmers can link into their application, which allows it to:

- Connect and disconnect VPN tunnels
- Authenticate users
- Receive notifications when tunnels open and close
- Retrieve tunnel statistics, such as byte and packet counts

The API comes with a programmer's user guide *VPN Client: API Overview*. This guide contains information enabling a programmer not familiar with the code base to use the API. The programmer's guide describes functions and data types, an overview of how to accomplish specific tasks, and easy to follow example programs.