



Using the Command-Line Interface

This chapter describes common operations using the command-line interface. You can create your own script files that use the CLI commands to perform routine tasks, such as connect to a corporate server, run reports, and then disconnect from the server.

For more detailed information about using the VPN Client command-line interface, see the *Cisco VPN Client Administrator Guide*. Also, that user guide contains instructions on how to manage the Certificate Manager application from the command line.

Displaying a List of Commands

To display a list of available VPN Client commands, locate the directory that contains the VPN Client software and enter the **vpnclient** command at the command line prompt.

The following example shows the command and the information that is displayed:

```
[root@Linux7_1 unity]# vpnclient
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686

Usage:
  vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
                               [nocertpwd]

  vpnclient disconnect
  vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
  vpnclient notify
```

Establishing a Connection

This section describes how to establish a VPN connection using the **vpnclient connect** command and optional command parameters.



Note

If you are connecting to a VPN device by using Telnet or SSH, check to see if the device allows split tunneling. If it does not, you lose connectivity to your VPN device after making a VPN connection.

To establish a connection, enter the following command:

```
vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
[nocertpwd]
```

The parameters for the **vpnclient connect** command are described in [Table 4-2](#).

Table 4-1 Parameters for the vpnclient connect Command

Parameter	Description
<profile> (required)	The name of the user profile configured for this connection entry (.pcf file). Enter the profile name without the .pcf file extension. If your profile name contains spaces, enclose it in double quotation marks on the command line.
user <username> (optional)	The username configured for this connection entry. If you use this option with the pwd option, the username prompt is suppressed in the authentication dialog box.
{eraseuserpwd pwd <password>} (optional)	<ul style="list-style-type: none"> eraseuserpwd erases the user password that is saved on the VPN Client workstation, forcing the VPN Client to prompt you for a password each time you establish a connection. pwd <password> suppresses the password prompt in the authentication dialog box.
nocertpwd (optional)	Suppresses the prompt for a certificate password and assumes that the password is blank. If you use this option, you cannot set a password for your certificate. For more information, see the "Managing Digital Certificates from the Command Line" in the <i>VPN Client Administrator Guide</i> .



Note

If your user profile is configured with the **SaveUserPassword** keyword set to the default, the password is saved locally.

For more information on profiles, see [Chapter 3, "User Profiles."](#)

Authentication Prompts

Depending on your user profile, you are prompted for the following passwords:

- Group password
- User name
- User password
- Certificate password

If your VPN Client has been configured to use SecurID or RADIUS authentication, you are also prompted for those passwords.

See your administrator for security information.

Rekeying Issues

When the connection is established, the VPN Client window stays in the foreground to allow the VPN Client to be reauthenticated during a rekey by the VPN device. To send the VPN Client window to the background, press **Ctrl-Z** and enter the **bg** command at the command line prompt.

If the VPN device you are connecting to is configured to support rekeying and you send the VPN Client window to the background, the tunnel disconnects when the first rekey occurs.

The VPN Client responds to rekey triggers based on *time*, not *data*. If you want VPN Client connections rekeyed, you must configure the concentrator so that the IKE proposal is set to rekey every 1800 seconds and IPSec parameters are set to rekey every 600 seconds.

DNS Server Settings

You can configure the concentrator to send the IP addresses of DNS servers to the VPN Client to use during tunnel sessions.

If the client receives the DNS server settings, it copies the file `/etc/resolv.conf` to a backup file `/etc/resolv.conf.vpnbackup`. When the tunnel closes, the original contents of `/etc/resolv.conf` are restored.



Note

Refer to the configuration guide for your VPN device for information on DNS server settings.

Disconnecting the VPN Client

This section describes methods for disconnecting the VPN Client.

To disconnect from your session, use one of the following methods:

- Enter the following command:

```
vpnclient disconnect
```

The following example shows the command that disconnects you from your secure connection and the prompts that appear.

```
[root@Linux7_1 clients]# vpnclient disconnect
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686
```

```
Disconnecting the VPN connection.
Your VPN connection has been terminated.
```

- Press **Ctrl-C** while you are in the VPN Client window.

Displaying VPN Client Statistics

This section describes the VPN Client statistics command **vpnclient stat** and its optional parameters.

To generate status information about your connection, enter the following command:

```
vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
```

If you enter this command without any of the optional parameters, the **vpnclient stat** command displays all status information. The optional parameters are described in [Table 4-2](#).

Table 4-2 Optional Parameters for the **vpnclient stat** Command

Parameter	Description
reset	Restarts all connection counts from zero.
traffic	Displays a summary of bytes in and out, packets encrypted and decrypted, and packets bypassed and discarded.
tunnel	Displays IPsec tunneling information.
route	Displays configured routes.
repeat	Provides a continuous display, refreshing it every few seconds. To end the display, press Ctrl-C .

Examples

This section shows examples of output from the different options for the **vpnclient stat** command.

No Options

The following is a sample output from the **vpnclient stat** command with no options.

```
[root@Linux7_1 clients]# vpnclient stat
Cisco Systems VPN Client Version 4.0 (int_84)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.4.2-2 #1 Sun Apr 8 20:41:30 EDT 2001 i686

VPN tunnel information.
Connection Entry: basic
Client address: 10.10.11.214
Server address: 10.200.20.21
Encryption: 168-bit 3-DES
Authentication: HMAC-SHA
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled

VPN traffic summary.
Time connected: 0 day(s), 00:00.01
Bytes in: 0
Bytes out: 0
Packets encrypted: 0
Packets decrypted: 0
Packets bypassed: 17
Packets discarded: 0
```

```
Configured routes.
Secured   Network Destination  Netmask
          0.0.0.0              0.0.0.0
```

Reset Option

To reset all connection counters, use the **vpnclient stat reset** command.

```
vpnclient stat reset
Tunnel statistics have been reset.
```

Traffic Option

The following is a sample output from the **vpnclient stat** command with the traffic option.

```
vpnclient stat traffic

VPN traffic summary
Time connected: 0 day<s>, 00:30:04
Bytes out: 5460
Bytes in: 6090
Packets encrypted: 39
Packets decrypted: 91
Packets bypassed: 159
Packets discarded: 1608
```

Tunnel Option

The following is a sample output from the **vpnclient stat** command with the tunnel option. The **vpnclient stat tunnel** command shows only tunneling information.

```
vpnclient stat tunnel

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
```

Route Option

The following is a sample output from the **vpnclient stat** command with the route option.

```
vpnclient stat route

Configured routes
Secured   Network Destination  Netmask          Bytes
*         10.10.02.02          255.255.255.255  17638
*         0.0.0.0              0.0.0.0          18998
```

**Note**

The maximum size of any VPN client statistics is 4,294,967,296. Once the VPN Client software reaches this limit, the statistics rolls back to zero and starts again.

Event Logging

This section provides information on event logging, including how to capture and view logging information.

Enabling Logging

You must be a system administrator or have access to the global profile (vpnclient.ini) to enable logging.

To enable logging, set **EnableLog=1**. To disable logging, set **EnableLog=0**.

The global profile, located in /etc/CiscoSystemsVPNClient/vpnclient.ini, must include the following parameters:

```
[main]
BinDirPath=/usr/local/bin
EnableLog=1
[LOG.IKE]
LogLevel=15
[LOG.CM]
LogLevel=3
[LOG.CVPND]
LogLevel=3
[LOG.XAUTH]
LogLevel=3
[LOG.CERT]
LogLevel=3
[LOG.IPSEC]
LogLevel=15
[LOG.CLI]
LogLevel=3
[LOG.PPP]
LogLevel=1
[LOG.DIALER]
LogLevel=1
[LOG.FIREWALL]
LogLevel=1
[LOG.GUI]
LogLevel=1
```

The VPN Client for Linux and Solaris supports log levels from 1 (lowest) to 15 (highest).

For more information about the global profile, refer to the *Cisco VPN Client Administrator Guide*.

Viewing Log Files

To view logging information, enter the following command:

```
/usr/local/bin/ipseclog /directory/clientlog.txt
```



Note

If you did not use the default directory `/usr/local/bin` during installation, you must enter logging commands using your chosen path.

When you launch the `ipseclog` application, it appends any previous `ipseclog` files.

To view logging information in real time, enter the following command after you start the `ipseclog`:

```
tail -f /directory/clientlog.txt
```

The `ipseclog` does not automatically go to the background. To send the `ipseclog` to the background, press **Ctrl-Z** and enter the **bg** on the command line, or enter the ampersand symbol (&) at the end of the **view** command, as shown in the following example:

```
/usr/local/bin/ipseclog /directory/clientlog.txt &
```

If the `ipseclog` is in the background, you must send it to the foreground before you end the VPN Client application. To send the `ipseclog` to the foreground, enter **fg** on the command line.

Client Auto Update Messages

When the VPN Client receives an auto-update notification from the VPN remote access device, it logs the notification, but takes no further action.

To receive auto-update messages and other notifications from the network administrator, use the **vpnclient notify** command.

The following example shows the `vpnclient notify` command and an example of an auto-update notification from the VPN device:

```
[root@Linux8 vpnclient]# vpnclient notify
Cisco Systems VPN Client Version 3.7 (Rel)
Copyright (C) 1998-2002 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.18-14 #1 Wed Sep 4 13:35:50 EDT 2002 i686
```

Notification:

```
Your network administrator has placed an update of the Cisco Systems VPN
Client at the following location:
http://fake.cisco.com/
```

```
[root@Linux8 vpnclient]
```

