



## Preconfiguring the VPN Client for Remote Users

This chapter explains how to prepare configurations for remote users and how to distribute them. This chapter includes the following sections:

- [User Profiles](#)
- [Creating a Global Profile](#)
- [Creating Connection Profiles](#)

### User Profiles

Groups of configuration parameters define the connection entries that remote users use to connect to a VPN central-site device. Together these parameters form files called profiles. There are two profiles: a global profile and an individual profile.

- A global profile sets rules for all remote users; it contains parameters for the VPN Client as a whole. The name of the global profile file is `vpnclient.ini`.
- Individual profiles contain the parameter settings for each connection entry and are unique to that connection entry. Individual profiles have a `.pcf` extension.

Profiles are created in two ways:

1. When an administrator or a remote user creates connection entries using the VPN Client graphical user interface (Windows and Macintosh only)
2. When you create profiles using a text editor

In the first case, the remote user is also creating a file that can be edited through a text editor. You can start with a profile file generated through the GUI and edit it. This approach lets you control some parameters that are not available in the VPN Client GUI application. For example, auto-initiation or dial-up wait for third-party dialers.

The default location for individual profiles is:

- For Windows platforms—`C:\Program Files\Cisco Systems\VPN Client\Profiles`.
- For the Linux, Solaris, and Mac OS X platforms—`/etc/CiscoSystemsVPNClient/Profiles/`

This chapter explains how to create and edit the `vpnclient.ini` and individual profiles. Both files use the same conventions.

**Note**

The easiest way to create a profile for the Windows platforms is to run the VPN Client and use the VPN Client GUI to configure the parameters. When you have created a profile in this way, you can copy the .pcf file to a distribution disk for your remote users. This approach eliminates errors you might introduce by typing the parameters and the group password gets automatically converted to an encrypted format.

## File Format for All Profile Files

The vpnclient.ini and .pcf files follow normal Windows.ini file format:

- Use a semicolon (;) to begin a comment.
- Place section names within brackets [section name]; they are not case sensitive.
- Use key names to set values for parameters; *keyword = value*. Keywords without values, or unspecified keywords, use VPN Client defaults. Keywords can be in any order and are not case sensitive, although using lower and uppercase makes them more readable.

## Making a Parameter Read Only

To make a parameter read-only so that the client user cannot change it within the VPN Client applications, precede the parameter name with an exclamation mark (!). This controls what the user can do within the VPN Client applications only. You cannot prevent someone from editing the global or .pcf file and removing the read-only designator.

## Creating a Global Profile

The name of the global profile is vpnclient.ini. This file is located in the following directories:

- For Windows platforms—C:\Program Files\Cisco Systems\VPN Client directory
- For the Linux, Solaris, and Mac OS X platforms— /etc/CiscoSystemsVPNClient/vpnclient.ini

These are the default locations created during installation.

## Features Controlled by Global Profile

The vpnclient.ini file controls the following features on all VPN Client platforms:

- Start before logon
- Automatically connect to the default connection entry (default profile) upon startup
- Automatically disconnect upon log off
- Control of logging services by class
- Certificate enrollment
- Identity of a proxy server for routing HTTP traffic
- Identity of an application to launch upon connect
- Missing group warning message
- Logging levels for log classes

- RADIUS SDI extended authentication behavior
- GUI parameters—appearance and behavior of GUI applications

The `vpnclient.ini` file controls the following additional features in the Windows platform:

- Location of the `Entrust.ini` file
- List of GINAs that are not compatible with the VPN Client
- Auto initiation
- Setting of the Stateful Firewall option
- The method to use in adding suffixes to domain names on Windows 2000 and Windows XP platforms
- When working with a third-party dialer, time to wait after receiving an IP address before initiating an IKE tunnel
- Network proxy server for routing HTTP traffic
- Application launching
- DNS suffixes
- Force Network Login, which forces a user on Windows NT, Windows 2000, or Windows XP to log out and log back in to the network without using cached credentials
- Accessibility options setting
- Setting a default connection entry
- Connecting to a default connection entry

### Sample `vpnclient.ini` file



#### Note

---

Profiles for the VPN Client are interchangeable between platforms. Keywords that are specific to the Windows platform are ignored by other platforms.

---

This sample file shows what you might see if you open it with a text editor

```
[main]
IncompatibleGinas=PALGina.dll,theirgina.dll
RunAtLogon=0
EnableLog=1
DialerDisconnect=1
AutoInitiationEnable=1
AutoInitiationRetryInterval=1
AutoInitiationRetryLimit=50
AutoInitiationList=techsupport,admin
[techsupport]
Network=175.55.0.0
Mask=255.255.0.0
ConnectionEntry=ITsupport
[admin]
Network=176.55.0.0
Mask=255.255.0.0
ConnectionEntry=Administration
Connectonopen=1
[LOG.IKE]
LogLevel=1
[LOG.CM]
LogLevel=1
```

```

[LOG.PPP]
LogLevel=2
[LOG.DIALER]
LogLevel=2
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=0
[LOG.IPSEC]
LogLevel=3
[LOG.FIREWALL]
LogLevel=1
[LOG.CLI]
LogLevel=1
[CertEnrollment]
SubjectName=Alice Wonderland
Company=University of OZ
Department=International Relations
State=Massachusetts
Country=US
Email=AliceW@UOZ.com
CADomainName=CertsAreUs
CAHostAddress=10.10.10.10
CACertificate=CAU
[Application Launcher]
Enable=1
Command=c:\apps\apname.exe
[NetLogin]
Force=1
Wait=10
DefaultMsg=For authorized users only
Separator=*****
[GUI]
WindowWidth=578
WindowHeight=367
WindowX=324
WindowY=112
VisibleTab=0
ConnectionAttribute=0
AdvancedView=1
DefaultConnectionEntry=ACME
MinimizeOnConnect=1
UseWindowSettings=1
ShowToolTips=1
ShowConnectHistory=1
AccessibilityOption=1

```

The rest of this section explains the parameters that can appear in the `vpnclient.ini` file, what they mean, and how to use them.

## Global Profile Configuration Parameters

[Table 2-1](#) lists all parameters, keywords, and values. It also includes the parameter name as used in the VPN Client GUI application if it exists, and where to configure it in the application.

Each parameter can be configured on all VPN Client platforms unless specified.

Table 2-1 *vpnclient.ini* File Parameters

<b>.ini Parameter (Keyword)</b>	<b>VPN Client Parameter Description</b>	<b>Values</b>	<b>VPN Client GUI Configuration Location(s)</b>
[main]	Required keyword to identify main section.	[ main ] Enter exactly as shown, as first entry in the file.	Does not appear in GUI
DialupWait	Specifies the number of seconds to wait between receiving an IP address from a third-party dialer such as General Packet Radio Services (GPRS) before initiating an IKE tunnel.  This grants enough time for the connection to go through on the first attempt.	After the keyword and equal sign, enter the number of seconds to wait. For example: DialupWait=1 Default number = 0.	Does not appear in GUI
IncompatibleGinas (Windows-only)	Lists Graphical Identification and Authentication dynamic link libraries (GINA.DLLs) that are not compatible with Cisco's GINA. Adding a GINA to the list causes the VPN Client to leave the GINA alone during installation and use fallback mode. The VPN Client goes into fallback mode only if RunAtLogon = 1. Otherwise, the Client GINA is never installed. (See <a href="#">"Installing the VPN Client Without User Interaction"</a> ).	After the keyword and equal sign, enter the name(s) of the GINAs, separated by commas. For example:  IncompatibleGinas= PALgina.dll, Yourgina.dll, Theirgina.dll  Do not enclose the name in quotes.	Does not appear in GUI
MissingGroupDialog	Controls the pop up window warning that occurs when a user tries to connect without setting the group name in a preshared connection.	0= (default) Do not show the warning message. 1=Show the warning message.	Does not appear in GUI
RunAtLogon (Windows-only)	Specifies whether to start the VPN Client connection before users log on to their Microsoft network. Available only for the Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). This feature is sometimes known as the NT Logon feature.	0 = Disable (default) 1 = Enable	Options > Windows Logon Properties > Enable start before logon
EntrustIni= (Windows-only)	Locates the entrust.ini file if it is in a location that is different from the default.ini file. The default location is the base Windows system directory.	Complete pathname of location	Does not appear in GUI

Table 2-1 vpnclient.ini File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
DialerDisconnect= (Windows-only)	Determines whether to automatically disconnect upon logging off a Windows NT platform (Windows NT 4.0, Windows 2000 and Windows XP). Disabling this parameter lets the VPN connection remain when the user logs off, allowing that user to log back in without having to establish another connection.	0 = Disable 1 = Enable (default disconnect on logoff)	Options > Windows Logon Properties > Disconnect VPN connection when logging off
<p>There are limitations to DialerDisconnect. For example, in the case of MS DUN, the RAS (PPP) connection might go down when the user logs off. For more information about this specific case, see the following URL:</p> <p><a href="http://support.microsoft.com/support/kb/articles/Q158/9/09.asp?LN=EN-US&amp;SD=gn&amp;FR=0&amp;qry=RAS%20AND%20LOGOFF&amp;rnk=2&amp;src=DHCS_MSPSS_gn_SRCH&amp;SPR=NTW40">http://support.microsoft.com/support/kb/articles/Q158/9/09.asp?LN=EN-US&amp;SD=gn&amp;FR=0&amp;qry=RAS%20AND%20LOGOFF&amp;rnk=2&amp;src=DHCS_MSPSS_gn_SRCH&amp;SPR=NTW40</a></p>			
EnableLog=	Determines whether to override log settings for the classes that use the logging services. By default, logging is turned on. This parameter lets a user disable logging without having to set the log levels to zero for each of the classes. By disabling logging you can improve the performance of the client system.	0 = Disable 1 = Enable (default)	Log > Enable/Disable
StatefulFirewall= (Windows-only)	Determines whether the stateful firewall is always on. When enabled, the stateful firewall always on feature allows no inbound sessions from all networks, whether a VPN connection is in effect or not. Also, the firewall is active for both tunneled and nontunneled traffic.	0 = Disable (default) 1 = Enable	Options > Stateful Firewall (Always On)
StatefulFirewallAllow ICMP (Windows only)	Controls whether StatefulFirewall (Always On) allows ICMP traffic.  Some DHCP Servers use ICMP pings to detect if the DHCP client PCs are up so that the lease can be revoked or retained.	0 = Disable (default) 1 = Enable	Does not appear in the GUI.
AutoInitiationEnable	Enables auto initiation, which is an automated method for establishing a wireless VPN connection in a LAN environment. For information on this feature see <a href="#">Updating VPN Client Software</a>	0 = Disable (default) 1 = Enable	Options > Automatic VPN Initiation
AutoInitiationRetry- Interval	Specifies the time to wait, in minutes, before retrying auto initiation after a connection attempt failure.	1 to 10 minutes Default = 1 minute	Options > Automatic VPN Initiation

Table 2-1 *vpnclient.ini* File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AutoInitiationRetry-IntervalType	Changes the retry interval from minutes (the default) to seconds. The range in seconds is 5-600.	0 = minutes (default) 1 = seconds	Options > Automatic VPN Initiation
AutoInitiationRetry-Limit	Identifies the number of consecutive connection failures before automatic initiation gives up and quits trying to connect.	1 to 1000 Default = 0 (no limit)	NA
AutoInitiationList	Identifies auto initiation-related section names within the <i>vpnclient.ini</i> file. The <i>vpnclient.ini</i> file can contain a maximum of 64 auto initiation list entries.	A list of section names separated by commas; for example:  SJWLAN, RTPWLAN, CHWLAN	Does not appear in GUI
[ <i>section name</i> ] (of an item in the AutoInitiationList)	Each section contains a network address, network mask, connection entry name, and a connect flag. The network and mask values identify a subnet. The connection entry identifies a connection profile (.pcf file). The connect flag specifies whether to auto initiate the connection.	<i>Section name in brackets</i> Network = IP address Mask = Subnet mask ConnectionEntry = name of a connection entry (profile) Connect = 1 or 0 0 = Do not auto initiate the connection 1 = Auto initiate the connection (the default)  Example:  [SJWLAN] Network=110.110.110.0 Mask=255.255.0.0 ConnectionEntry=SantaJuan WirelessLAN	Does not appear in GUI

Example of Automatic Initiation configuration for *vpnclient.ini* file:

```
[main]
AutoInitiationEnable = 1—Start automatic initiation.
autoInitiationList = autonet—identifies a section name in the list for automatic initiation.
AutoInitiationRetryInterval = 60—Try to connect every 60 seconds.
AutoInitiationRetryIntervalType = 1—Set retry interval type to seconds.
AutoInitiationRetryLimit = 25—Try to connect 25 times. If connection attempts fail 25 times, stop trying to connect.
[autonet]—Start an entry in the automatic initiation list.
network = 192.168.0.0—Identify the IP address of the connection entry.
mask = 255.255.0.0—Specify the submask
connectionentry = flatirons—Specify the connection entry name s(.pcf file).
```

ConnectOnOpen	Automatically connects to the default user profile set in the DefaultConnectionEntry parameter	0 = Disable (the default) 1 = Enable	Main Menu > Options > Preferences > Enable connect on open
VAEnableAlt	Changes the method for initializing the virtual adapter from the standard method to an alternative method. If your users are experiencing difficulty in initializing the VA, try the alternate method.	0 = Use the alternate method for initializing the VA  1 = Use the standard method for initializing the VA (the default)	NA

Table 2-1 *vpnclient.ini* File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AddDhcpRoute (Windows only)	Adds a route that bypasses all traffic going to the DHCP server. This is the normal behavior. However, if your users do not want the VPN Client to bypass all traffic going to the DHCP server because other services exist on the server, use this parameter to change the default behavior of the software.	0 = Do not add a route to bypass the DHCP server 1 = Add a route to bypass the DHCP server (default)	
For each class that follows, use the LogLevel= parameter to set the logging level			
[LOG.IKE]	Identifies the Internet Key Exchange class for setting the logging level.	[LOG.IKE] Enter exactly as shown.	Log > Settings
[LOG.CM]	Identifies the Connection Manager class for setting the logging level.	[LOG.CM] Enter exactly as shown.	Log > Settings
[LOG.XAUTH]	Identifies the Extend authorization class for setting the logging level.	[LOG.XAUTH] Enter exactly as shown.	Log > Settings
[LOG.PPP] (Windows-only)	Identifies the PPP class for setting the logging level.	[LOG.PPP] Enter exactly as shown.	Log > Settings
[LOG.CVPND]	Identifies the Cisco VPN Daemon class for setting the logging level.	[LOG.CVPND] Enter exactly as shown.	Log > Settings
[LOG.CERT]	Identifies the Certificate Management class for setting the logging level.	[LOG.CERT] Enter exactly as shown.	Log > Settings
[LOG.IPSEC]	Identifies the IPSec module class for setting the logging level.	[LOG.IPSEC] Enter exactly as shown.	Log > Settings
[LOG.FIREWALL] (Windows-only)	Identifies the FWAPI class for setting the logging level.	[LOG.FIREWALL] Enter exactly as shown	Log > Settings
[LOG.CLI]	Identifies the Command-Line Interface class for setting the logging level.	[LOG.CLI] Enter exactly as shown	Log > Settings
[LOG.GUI]	Identifies the Graphical User Interface class for setting the logging level.	[LOG.GUI] Enter exactly as shown	Log > Settings
LogLevel=	Determines the log level for individual classes that use logging services. By default, the log level for all classes is Low. You can use this parameter to override the default setting for the preceding [LOG] parameters.	The VPN Client supports log levels from 1 (lowest) to 15 (highest). Default = 1 To set logging levels, you must first enable logging: <b>EnableLog=1.</b>	Log > Settings

Table 2-1 *vpnclient.ini* File Parameters (continued)

<b>.ini Parameter (Keyword)</b>	<b>VPN Client Parameter Description</b>	<b>Values</b>	<b>VPN Client GUI Configuration Location(s)</b>
[CertEnrollment]	Required keyword to identify the Certificate Enrollment section.	[CertEnrollment] Enter exactly as shown.	Does not appear in GUI
SubjectName=	Identifies the username associated with this certificate.	Maximum of 519 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Company=	Identifies the company or organization of the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Department=	Identifies the department or organizational unit of the certificate owner. If matching by IPsec group in a VPN 3000 Concentrator, must match the group name in the configuration.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
State=	Identifies the state or province of the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Country=	Identifies the two-letter code identifying the country of this certificate owner.	Maximum of 2 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
Email=	Identifies the certificate owner's email address.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
IPAddress	Identifies the IP address of the system of the certificate owner.	Internet address in dotted decimal notation.	Certificates > Enroll Certificate Enrollment form
Domain	Identifies the fully qualified domain name of the host that is serving the certificate owner.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CADomainName=	Identifies the domain name that the certificate authority belongs to; for network enrollment.	Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CAHostAddress=	Identifies the IP address or hostname of the certificate authority.	Internet hostname or IP address in dotted decimal notation. Maximum of 129 alphanumeric characters.	Certificates > Enroll Certificate Enrollment form
CACertificate=	Identifies the name of the self-signed certificate issued by the certificate authority.	Maximum of 519 alphanumeric characters. Note: The VPNClient GUI ignores a read-only setting on this parameter.	Certificates > Enroll Certificate Enrollment form

Table 2-1 *vpnclient.ini* File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
NetworkProxy= (Windows-only)	Identifies a proxy server you can use to route HTTP traffic. Using a network proxy can help prevent intrusions into your private network.	IP address in dotted decimal notation or domain name. Maximum of 519 alphanumeric characters. The proxy setting sometimes has a port associated with it.  Example:10.10.10.10:8080	Does not appear in GUI
[ApplicationLauncher] (Windows-only)	(No VPN Client field) Required keyword to identify Application Launcher section.	[ApplicationLauncher] Enter exactly as shown, as first entry in the section.	Does not appear in GUI
Enable= (Windows-only)	Use this parameter to allow VPN Client users to launch an application when connecting to the private network.	0 = Disabled (default) 1 = Enabled  Disabled means no launching.	Options> Application Launcher
Command= (Windows-only)	The name of the application to be launched. This variable includes the pathname to the command, and the name of the command complete with arguments.	<i>command string</i> Maximum 512 alphanumeric characters.  Example: c:\auth\swtoken.exe.	Options> Application Launcher> Application
[DNS] (Windows-only)	(No VPN Client field) Required keyword to identify DNS section.	[DNS] Enter exactly as shown, as first entry in the section.	Does not appear in GUI.
AppendOriginalSuffix= (Windows-only)	Determines the way the VPN Client treats suffixes to domain names. See “DNS Suffixes and the VPN Client—Windows 2000 and Windows XP Only”, following this table.	0 = do nothing 1 = append the primary DNS suffix to the suffix that the VPN Concentrator supplies. This is the default value. 2 = append the primary and connection-specific DNS suffixes to the suffix that the VPN Concentrator supplies.	Does not appear in GUI.
[RadiusSDI]	Required keyword to identify the RADIUS SDI extended authentication (XAuth) section. Configure this section to enable a VPN Client to handle Radius SDI authentication the same as native SDI authentication, which makes authentication easier for VPN Client users to authenticate using SDI.	Enter exactly as shown.	Does not appear in GUI.

Table 2-1 *vpnclient.ini* File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
QuestionSubStr	Uniquely identifies question-type RADIUS SDI Xauth prompts.	Enter text up to 32 bytes in length. The default text is a question mark.  Example: "Are you prepared to have the system generate your PIN? (y/n):" Response: _____	The question appears in the GUI during extended authentication. It is followed by a Response field.
NewPinSubStr	Uniquely identifies new PIN RADIUS SDI Xauth prompts.	Enter text up to 32 bytes in length. Default text is "new PIN."  Example: "Enter a new PIN of 4 to 8 digits."	Appears in the GUI during extended authentication.
NewPasscodeSubStr	Uniquely identifies new passcode RADIUS Xauth prompts.	Enter text up to 32 bytes in length. Default text is "new passcode."  Example: "PIN accepted. Wait for the token code to change, then enter the new passcode"	Appears in the GUI during extended authentication.
[Netlogin] (windows-only)	Identifies the Force Network Login section of the vpnclient.ini file. This feature forces a user on Windows NT, Windows 2000, and Windows XP to log out and log back in to the network without using cached credentials.	Enter exactly as shown; this is required as part of the feature.	Does not appear in the GUI.
<b>Note</b> If users are connecting via dialup (RAS), you should add the registry key described in the Microsoft article: <a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;Q158909">http://support.microsoft.com/default.aspx?scid=kb;en-us;Q158909</a> . Adding the registry key assures that the RAS connection does not drop when the user gets logged off.			
Force (windows-only)	Specifies what action to take for the Force Network Login feature. This parameter is required for this feature.	0 = (default) Do not force the user to log out and log in. 1 = Force user to log out when the Wait time is reached unless an option is selected. 2 = Disconnect VPN session upon reaching the Wait time unless an option is selected. 3 = Wait for the user to select Connect or Disconnect.	Does not appear in the GUI.

Table 2-1 *vpnclient.ini* File Parameters (continued)

<b>.ini Parameter (Keyword)</b>	<b>VPN Client Parameter Description</b>	<b>Values</b>	<b>VPN Client GUI Configuration Location(s)</b>
Wait (windows-only)	Determines the number of seconds to wait before performing an action specified by the Force parameter. This parameter is optional.	x number of seconds. The default is 5 seconds.	Does not appear in the GUI.
DefaultMsg (windows-only)	Specifies a message to display before performing the action specified by the Force parameter. Message can vary according to setting of Force. This parameter is optional.	Ascii text up to 1023 bytes. Default message = You will soon be disconnected.	Does not appear in the GUI.
Separator (windows-only)	Specifies the separator text that separates banner text from the message. If no banner exists, the separator is not displayed. This parameter is optional.	Ascii text up to 511 bytes. Default separator = -----	Does not appear in the GUI.
[GUI]	Required keyword to identify the section of the file that lets you control features of the Graphical User Interface application.	[GUI] Enter exactly as shown, as first entry in the section.	Does not appear in the GUI.
DefaultConnectionEntry	Specifies the name of the connection entry for the VPN Client to use to initiate a connection, unless otherwise indicated.	<i>ConnectionEntryName</i>	Connection Entries > Add/Modify > Set as default entry.
WindowWidth	Controls the width of the window.	Default = 578 pixels	Manual control
WindowHeight	Controls the height of the window.	Default = 367 pixels	Manual control
WindowX	Controls the X coordinate of the window.	0 to 1024 pixels Default = 324	Where the window appears horizontally relative to your monitor's screen
WindowY	Controls the Y coordinate of the window.	0 to 768 pixels Default = 112	Where the window appears vertically relative to your monitor's screen
VisibleTab	Tracks which tab is currently visible in the advanced mode main dialog; an index.	Connection Entries Certificates Log	VPN Client main dialog
ConnectionAttribute	Indicates the current setting for the status bar display. The status bar is the line area at the bottom of the dialog that shows the state of the connection (connect/not connected), if connected, the name of the connection entry on the left and what the status is on the right.	If you click on the arrow on the right end of the status bar, the right part of the status bar changes. This value records the current display selection.	VPN Client main dialog > status bar

Table 2-1 *vpnclient.ini* File Parameters (continued)

.ini Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client GUI Configuration Location(s)
AdvancedView	Toggles between Advanced and Simple modes of operation.	Simple Mode = 0 Advanced Mode = 1 (default)	Main menu > Options menu > Advanced/Simple Mode
MinimizeOnConnect	Controls whether to minimize to a system tray icon upon connection to a VPN central-site device.	0 = Do not minimize 1 = Do minimize (default)	Main menu > Options > Preferences > Hide upon connect
UseWindowSettings	Controls whether to save windows settings.	0 = No 1 = Yes (default)	Main menu > Options > Preferences > Save window settings
ShowTooltips	Controls whether to display the tool tips .	0 = No 1 = Yes (default)	Main menu > Options > Preferences > Enable tooltips
ShowConnectHistory	Controls whether to display the connection history dialog during connection negotiation.	0 = No (default) 1 = Yes	Main menu > Options > Preferences > Enable Connection History Display
AccessibilityOption	Controls whether to activate 508 accessibility options (Windows only)	0 = No (default) 1 = Yes	Main menu > Options > Preferences > Enable accessibility options

## Creating and Using a Default User Profile

You can configure a default user profile, which is the same as the default connection entry capability in the VPN Client GUI (see *VPN Client User Guide for Windows*, Chapter 4, “Setting a Default Connection Entry” or *VPN Client User Guide for Mac OS X*, Chapter 5, “Connecting to a Default Connection Entry.” The parameter `DefaultConnectionEntry` in the VPN Client .ini file contains the name of the default user profile. Then you can use the Connect on Open feature to configure the VPN Client to connect to the default user profile when it connects to a secure gateway. To activate this configuration, using the parameters in the `vpnclient.ini` file, use the following procedure:

- 
- Step 1** Specify the name of a default connection entry in the `DefaultConnectionEntry` parameter; for example, `DefaultConnectionEntry=myprofile`.
  - Step 2** Enable the `ConnectOnOpen` parameter (`ConnectOnOpen=1`).
- 

## DNS Suffixes and the VPN Client—Windows 2000 and Windows XP Only

When a command or program such as `ping server123` passes a hostname without a suffix to a Windows 2000 or Windows XP platform, Windows 2000/XP has to convert the name into a fully-qualified domain name (FQDN). The Windows operating system has two methods for adding suffixes to domain names: Method 1 and Method 2. This section describes these two methods.

## Method 1—Primary and Connection-Specific DNS Suffixes

A primary DNS suffix is global across all adapters. A connection-specific DNS suffix is only for a specific connection (adapter), so that each connection can have a different DNS suffix.

### Identifying a Primary DNS Suffix

A primary suffix comes from the computer name. To find or assign a primary DNS suffix, use the following procedure according to your operating system:

#### On Windows 2000

- 
- Step 1** On a Windows 2000 desktop, right click the **My Computer** icon, and select **Properties** from the menu. The System Properties dialog displays.
- Step 2** Open the **Network Identification** tab.
- The entry next to *Full Computer Name* identifies the computer's name and DNS suffix on this screen, for example, `SILVER-W2KP.tango.dance.com`. The part after the first dot is the primary DNS suffix, in this example: `tango.dance.com`.
- Step 3** To change the primary DNS suffix, click **Properties** on the Network Identification tab. The Identification Changes dialog displays.
- Step 4** Click **More....**
- This action displays the DNS Suffix and Net BIOS Computer Name dialog. The *Primary DNS suffix of this computer* entry identifies the primary suffix. You can edit this entry.
- 

#### On Windows XP

- 
- Step 1** Right click **My Computer**, and select **Properties** from the menu. The System Properties dialog displays.
- Step 2** Open the **Computer Name** tab.
- The entry next to *Full Computer Name* identifies the computer's name and DNS suffix on this screen (for example, `SILVER-W2KP.tango.dance.com`). The part after the first dot is the primary DNS suffix (in this example: `tango.dance.com`).
- Step 3** To change the primary DNS suffix, click **Change** on the Computer Name tab. The Computer Name Changes dialog displays.
- Step 4** Click **More....**
- This action displays the DNS Suffix and Net BIOS Computer Name dialog. The Primary DNS suffix of this computer entry identifies the primary suffix. You can edit this entry.
- 

### Identifying a Connection-Specific DNS Suffix

You can identify a connection-specific DNS suffix in one of two ways.

1. The connection-specific DNS value is listed as the DNS suffix for the selected connection on the Advanced TCP/IP Settings dialog.

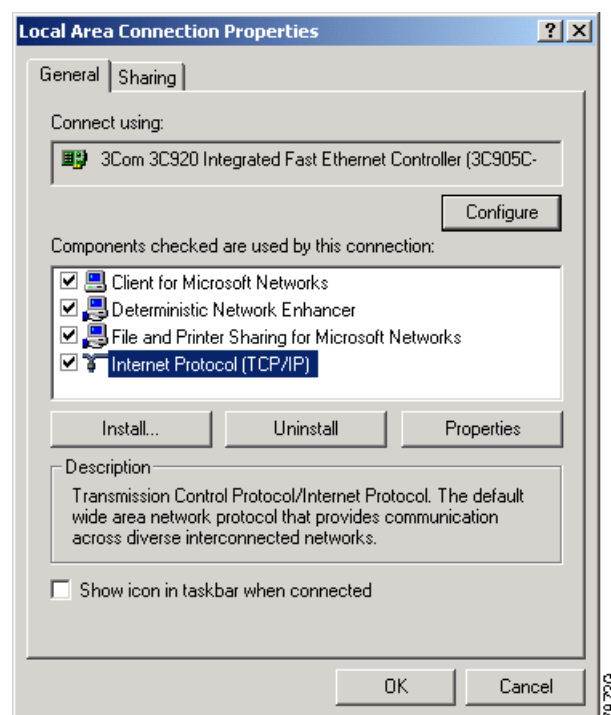
**Note**

The following instructions are for a Windows 2000 platform. There may be slight variations on a Windows XP platform.

To display the Advanced TCP/IP Settings dialog, use the following procedure:

- Step 1** Right click the **My Network Places** icon to display the Properties dialog, which lists your connections.
- Step 2** Double-click on a connection (for example, **local**) to display its Properties dialog. The connection uses the checked components, such as those shown in [Figure 2-1](#), which shows components of a connection named Local Area Connection.

**Figure 2-1** *Displaying Properties for a Connection*



- Step 3** Double-click **Internet Protocol (TCP/IP)** to reveal its properties.
- Step 4** Select **Advanced**.
- Step 5** Display the **DNS** tab and look at `DNS suffix for this connection` box. If the box is empty, you can have it assigned by the DHCP Server.
- a. To identify the connection-specific suffix assigned by the DHCP Server, use the `ipconfig /all` command (Alternative 2, below) and for the DNS Server address.
  2. The connection-specific DNS value is listed in the output from the `ipconfig /all` command, executed at the command-line prompt. Look under Windows 2000 IP Configuration for `DNS Suffix Search List`. Under Ethernet Adapter Connection Name, look for `Connection-specific DNS Suffix`.

## Method 2—User Supplied DNS Suffix

For this method, you can provide specific suffixes. You can view and change suffixes in the DNS tab of the connection properties page. The Append these DNS suffixes (in order) edit box supplies the name that you can edit. The values you provide here are global to all adapters.

## VPN Client Behavior

When the VPN Client establishes a VPN tunnel to the VPN central device (for example, the VPN 3000 Concentrator), the VPN Client uses Method 2 without regard for the method that the Windows platform uses. If the Windows platform is using Method 2, the VPN Client appends the suffix provided by the VPN central device. This is the default behavior and works correctly with no problem.

However if Windows is using Method 1, the VPN Client does not append the primary or connection-specific suffix. To fix this problem, you can set the AppendOriginalSuffix option in the vpnclient.ini file. In [Table 2-1](#), the [DNS] section contains this option:

[DNS]

AppendOriginalSuffix=1:

In this case, the VPN Client appends the primary DNS suffix to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has two suffixes: one provided by the VPN Concentrator and the primary DNS suffix.

AppendOriginalSuffix=2:

In this case, the VPN Client appends the primary and connection-specific DNS suffixes to the suffix provided by the VPN Concentrator. While the tunnel is established, Windows has three suffixes: one provided by the VPN Concentrator, the primary DNS suffix, and the connection-specific DNS suffix.



### Note

---

If Windows is using Method 2, adding these values to the vpnclient.ini file has no effect.

---

The VPN Client sets these values every time a tunnel is established and then restores the original configuration when tearing down the tunnel.

## Setting Up RADIUS SDI Extended Authentication

You can configure the VPN Client to handle RADIUS SDI authentication the same way it handles “native” SDI authentication, which is more seamless and easier to use. With this configuration, users do not have to deal with the RSA SecurID software interface; the VPN Client software directly interfaces with the RSA SecureID software for the user.

To enable intelligent handling of RADIUS SDI authentication, you must configure one profile (.pcf) parameter and possibly three global (vpnclient.ini) parameters:

- In the vpnclient.ini file, enter the following information. (For complete information on these parameters, see [Table 2-1](#).)
  - RadiusSDI—identifies the configuration section for RADIUS SDI
  - A question sub-string to identify question prompts (e.g. “?”)
  - A new PIN sub-string to identify prompts for a new PIN
  - A new passcode sub-string to identify prompts for a new passcode

- In the profile (connection entry) file under the Main section, enter the parameter “RadiusSDI = 1”. (See [Table 2-2](#).)

Now when the request comes in to the VPN Client, the software identifies it as a RADIUS SDI extended authentication request and knows how to process the request.

## Creating Connection Profiles

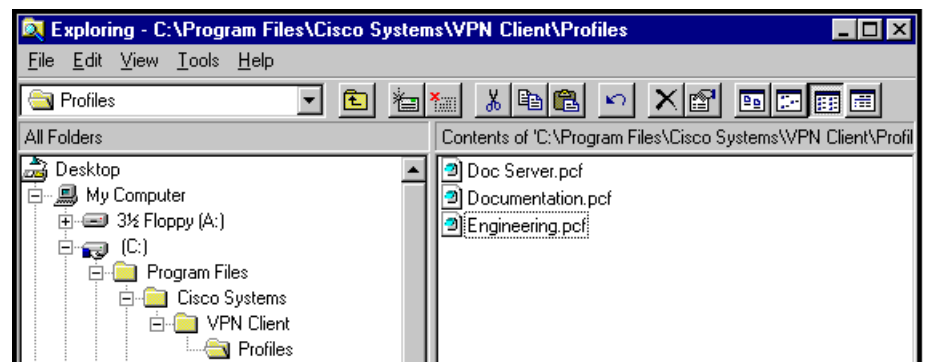
The VPN Client uses parameters that must be uniquely configured for each remote user of the private network. Together these parameters make up a user profile, which is contained in a profile configuration file (.pcf file) in the VPN Client user’s local file system in the following directories:

- For Windows platforms—Program Files\Cisco Systems\VPN Client\Profiles (if the software installed in the default location)
- For the Linux, Solaris, and Mac OS X platforms— /etc/CiscoSystemsVPNClient/Profiles/

These parameters include the authentication type used, remote server address, IPSec group name and password, use of a log file, use of backup servers, and automatic Internet connection via Dial-Up Networking among many other features and requirements. Each connection entry has its own .pcf file. For example, if you have three connection entries, named Doc Server, Documentation, and Engineering, the Profiles directory shows the list of .pcf files.

[Figure 2-2](#) shows the directory structure for the user profile in the Windows platforms.

**Figure 2-2** List of .pcf files



## Features Controlled by Connection Profiles

A connection profile (.pcf file) controls the following features on all platforms):

- Description of the connection profile
- The remote server address
- Authentication type
- Name of IPSec group containing the remote user
- Group password
- Connecting to the Internet via dial-up networking

- Name of remote user
- Remote user's password
- Backup servers
- Split DNS
- Type of dial-up networking connection
- Transparent tunneling
- TCP tunneling port
- Allowing of local LAN access
- Enabling of IKE and ESP keepalives
- Setting of peer response time-out
- Certificate parameters for a certificate connection
- Setting of certificate chain
- Diffie-Hellman group
- Verification of the DN of a peer certificate
- RADIUS SDI extended authentication setting
- Use of SDI hardware token setting
- Split DNS setting
- Use legacy IKE port setting

A connection profile (.pcf file) controls the following additional features on the Windows platform:

- Dial-Up networking phone book entry for Microsoft
- Command string for connecting through an ISP
- NT domain
- Logging on to Microsoft Network and credentials
- Change the default IKE port from 500/4500 (must be explicitly added)
- Enable Force Network Login, which forces a user on Windows NT, Windows 2000, and Windows XP to log out and then log back in to the network without using cached credentials
- Enable/disable the browser proxy setting on the VPN Client for all connection types

### Sample .pcf file



#### Note

Connection profiles for the VPN Client are interchangeable between platforms. Keywords that are specific to the Windows platform are ignored by other platforms.

The sample .pcf profile that follows is a connection entry that uses pre-shared keys. Note that the `enc_` prefix (for example, `enc_GroupPwd`) indicates that the value for that parameter is encrypted and will be filled in by the VPN Client.

```
[main]
Description=connection to TechPubs server
Host=10.10.99.30
AuthType=1
GroupName=docusers
```

```

GroupPwd=
enc_GroupPwd=158E47893BDCD398BF863675204775622C494B39523E5CB65434D3C851ECF2DCC8BD488857EFA
FDE1397A95E01910CABECC4E040B7A77BF
EnableISPCConnect=0
ISPCConnectType=0
ISPCConnect=
ISPCCommand=
Username=alice
SaveUserPassword=0
UserPassword=
enc_UserPassword=
NTDomain=
EnableBackup=1
BackupServer=Engineering1, Engineering2, Engineering 3, Engineering4
EnableMSLogon=0
MSLogonType=0
EnableNat=1
EnableLocalLAN=0
TunnelingMode=0
TCPTunnelingPort=10000
CertStore=0
CertName=
CertPath=
CertSubjectName
SendCertChain=0
VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSURE-OU!*"wonderland"
DHGroup=2
PeerTimeOut=90
ForceNetLogin=1

```

You can configure the VPN Client for remote users by creating a profile configuration file for each connection entry and distribute the .pcf files with the VPN Client software. These configuration files can include all, or only some, of the parameter settings. Users must configure those settings not already configured.

You can also distribute the VPN Client to users without a configuration file and let them configure it on their own. In this case, when they complete their configuration using the VPN Client program, they are in effect creating a .pcf file for each connection entry, which they can edit and share.

To protect system security you should *not* include key security parameters such as the IPsec group password, authentication username, or authentication password in .pcf files for remote users.


**Note**

Whatever preconfiguring you provide, you must supply users with the information they need to configure the VPN Client. See “Gathering Information You Need” in Chapter 2 of the *VPN Client User Guide* for your platform.

## Creating a .pcf file for a Connection Profile

Each user requires a unique configuration file. Use Notepad or another ASCII text editor to create and edit each file. Save as a text-only file with no formatting.

### Naming the Connection Profile

For a Windows platform, you can create profile names that contain spaces. However, if you want to distribute profiles to other platforms (Linux, Mac OS X, or Solaris), the name cannot contain spaces.

## Connection Profile Configuration Parameters

Table 2-2 lists all parameters, keywords, and values. It also includes the VPN Client parameter name (if it exists) that corresponds to the keyword and where it is configured on the VPN Client GUI.

You can configure each parameter on all VPN Client platforms unless specified.

**Table 2-2 .pcf file parameters**

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
[main]	(No VPN Client field) Required keyword to identify main section.	[main] As the first entry in the file, enter exactly as shown.	Does not appear in GUI
Description=	Description A line of text that describes this connection entry. Optional.	Any text. Maximum 246 alphanumeric characters.	Connection Entry > New/Modify
Host=	Remote server address The hostname or IP address of the Cisco remote access server (a VPN central-site device) to which remote users connect.	Internet hostname, or IP address in dotted decimal notation. Maximum 255 alphanumeric characters.	Connection Entry > New/Modify
AuthType=	Authentication type For a description of authentication and authentication types, see the VPN Client user guides for the platform you are using.	The authentication type of this user: 1 = Pre-shared keys (default) 3 = Digital Certificate using an RSA signature. 5 = Mutual authentication (see note below)	Connection Entry > New/Modify > Authentication

**Note** Setting up mutual or hybrid authentication for users:  
To use this authentication method, the VPN central-site device must have an identity certificate installed derived from a root certificate that matches the root certificate installed on the VPN Client system (the credentials used by both sides must match for mutual trust to take place). For information on how to provide a root certificate to a remote user during installation, consult the installation section in the user guide for the platform you are using. For VPN Concentrator configuration information see [Configuring Mutual Authentication](#).

GroupName=	Group Name The name of the IPSec group that contains this user. Used with pre-shared keys.	The exact name of the IPSec group configured on the VPN central-site device. Maximum 32 alphanumeric characters. Case-sensitive.	Connection Entry > New/Modify > Authentication
GroupPwd=	Group Password The password for the IPSec group that contains this user. Used with pre-shared keys. The first time the VPN Client reads this password, it replaces it with an encrypted one (enc_GroupPwd).	The exact password for the IPSec group configured on the VPN central-site device. Minimum of 4, maximum 32 alphanumeric characters. Case-sensitive clear text.	Connection Entry > New/Modify > Authentication

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
encGroupPwd=	The password for the IPsec group that contains the user. Used with pre-shared keys. This is the scrambled version of the GroupPwd.	Binary data represented as alphanumeric text.	Does not appear in GUI.
EnableISPConnect= (Windows-only)	Connect to the Internet via Dial-Up Networking  Specifies whether the VPN Client automatically connects to an ISP before initiating the IPsec connection; determines whether to use PppType parameter.	0 = Disable (default) 1 = Enable  The VPN Client GUI ignores a read-only setting on this parameter.	Connection Entry > New/Modify > Dial-Up > Connect to the Internet via dial-up
ISPConnectType= (Windows-only)	Dial-Up Networking connection entry type  Identifies the type to use: ISPConnect or ISPCommand.	0 = ISPConnect (default) 1 = ISPCommand  The VPN Client GUI ignores a read-only setting on this parameter.	Connection Entry > New/Modify > Dial-Up > (choosing either DUN or Third Party (command))
ISPConnect= (Windows-only)	Dial-Up Networking Phonebook Entry (Microsoft)  Use this parameter to dial into the Microsoft network; dials the specified dial-up networking phone book entry for the user's connection.  Applies only if EnableISPConnect=1 and ISPConnectType=0.	<i>phonebook_name</i>  This variable is the name of the phone book entry for DUN – maximum of 256 alphanumeric characters.  The VPN Client GUI ignores a read-only setting on this parameter.	Connection Entry > New/Modify > Dial-Up > Microsoft Dial-Up Networking > Phonebook
ISPCommand= (Windows-only)	Dial-Up Networking Phonebook Entry (command)  Use this parameter to specify a command to dial the user's ISP dialer.  Applies only if EnableISPConnect=1 and ISPConnectType=1.	<i>command string</i>  This variable includes the pathname to the command and the name of the command complete with arguments; for example:  c:\isp\ispdialer.exe dialEngineering Maximum 512 alphanumeric characters.	Connection Entry > New/Modify > Dial-Up > Third party dialup program > Application
Username=	User Authentication: Username  The name that authenticates a user as a valid member of the IPsec group specified in GroupName.	The exact username. Case-sensitive, clear text, maximum of 32 characters.  The VPN Client prompts the user for this value during user authentication.	Connection Entry > New/Modify > Authentication

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
UserPassword=	<p>User Authentication: Password</p> <p>The password used during extended authentication.</p> <p>The first time the VPN Client reads this password, it saves it in the file as the enc_UserPassword and deletes the clear-text version. If SaveUserPassword is disabled, then the VPN Client deletes the UserPassword and does not create an encrypted version.</p> <p>You should only modify this parameter manually if there is no GUI interface to manage profiles.</p>	Maximum of 32 alphanumeric characters, case sensitive.	Connection Entry > New/Modify > Authentication
encUserPassword	Scrambled version of the user's password	Binary data represented as alphanumeric text.	Does not appear in GUI.
SaveUserPassword	<p>Determines whether or not the user password or its encrypted version are valid in the profile.</p> <p>This value is pushed down from the VPN central-site device.</p>	<p>0 = (default) do not allow user to save password information locally.</p> <p>1 = allow user to save password locally.</p>	Does not appear in GUI.
NTDomain= (Windows-only)	<p>User Authentication: Domain</p> <p>The NT Domain name configured for the user's IPsec group. Applies only to user authentication via a Windows NT Domain server.</p>	<p>NT Domain name.</p> <p>Maximum 14 alphanumeric characters. Underbars are not allowed.</p>	Connection Entry > New/Modify
EnableBackup=	<p>Enable backup server(s)</p> <p>Specifies whether to use backup servers if the primary server is not available.</p>	<p>0 = Disable (default)</p> <p>1 = Enable</p>	Connection Entry > New/Modify > Backup Servers
BackupServer=	<p>(Backup server list)</p> <p>List of hostnames or IP addresses of backup servers.</p> <p>Applies only if EnableBackup=1.</p>	<p>Legitimate Internet hostnames, or IP addresses in dotted decimal notation.</p> <p>Separate multiple entries by commas. Maximum of 255 characters in length.</p>	Connection Entry > New/Modify > Backup Servers
EnableMSLogon= (Windows-only)	<p>Logon to Microsoft Network.</p> <p>Specifies that users log on to a Microsoft network.</p> <p>Applies only to systems running Windows 9x.</p>	<p>0 = Disable</p> <p>1 = Enable (Default)</p>	<p>Connection Entry &gt; New/Modify &gt; Microsoft Logon</p> <p>This is available only on Windows 98 and Windows ME.</p>

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
MSLogonType= (Windows-only)	Use default system logon credentials.  Prompt for network logon credentials.  Specifies whether the Microsoft network accepts the user's Windows username and password for logon, or whether the Microsoft network prompts for a username and password.  Applies only if EnableMSLogon=1.	0 = (default) Use default system logon credentials; i.e., use the Windows logon username and password. 1 = Prompt for network logon username and password.	Connection Entry > New/Modify > Microsoft Logon  This is available only on Windows 98 and Windows ME.
EnableNat=	Enable Transparent Tunneling.  Allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing NAT or PAT.	0 = Disable 1 = Enable (default)	Connection Entry > New/Modify > Transport
TunnelingMode=	Specifies the mode of transparent tunneling, over UDP or over TCP; must match that used by the secure gateway with which you are connecting.	0 = UDP (default) 1 = TCP	Connection Entry > New/Modify > Transport
TCP TunnelingPort=	Specifies the TCP port number, which must match the port number configured on the secure gateway.	Port number from 1 through 65545  Default = 10000	Connection Entry > New/Modify > Transport
EnableLocalLAN=	Allow Local LAN Access.  Specifies whether to enable access to resources on a local LAN at the Client site while connected through a secure gateway to a VPN device at a central site.	0 = Disable (default) 1 = Enable	Connection Entry > New/Modify > Transport
PeerTimeout=	Peer response time-out  The number of seconds to wait before terminating a connection because the VPN central-site device on the other end of the tunnel is not responding.	Number of seconds  Minimum = 30 seconds Maximum = 480 seconds Default = 90 seconds	Connection Entry > New/Modify > Transport

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
CertStore=	Certificate Store Identifies the type of store containing the configured certificate.	0 = No certificate (default) 1 = Cisco 2 = Microsoft The VPN Client GUI ignores a read-only (!) setting on this parameter. (See note)	Windows GUI Does not appear in GUI. You can view on Certificates tab. Mac OS X GUI Connection Entry > New/Modify > Transport
<b>Note</b> Normally, if a parameter is marked as read only, the GUI disables the checkbox or edit box so users can not change the value of the parameter. However, this is not true for Certificate parameters. These values cannot be overwritten in the file. Users can change them in the GUI display, but these changes are not saved.			
CertName=	Certificate Name Identifies the certificate used to connect to a VPN central-site device.	Maximum 129 alphanumeric characters The VPN Client GUI ignores a read-only setting on this parameter.	Certificates > View
CertPath=	The complete pathname of the directory containing the certificate file.	Maximum 259 alphanumeric characters The VPN Client GUI ignores a read-only setting on this parameter.	Certificates > Import
CertSubjectName	The fully qualified distinguished name (DN) of certificate's owner. If present, the VPN Dialer enters the value for this parameter.	Either do not include this parameter or leave it blank. The VPN Client GUI ignores a read-only setting on this parameter.	Certificates > View
CertSerialHash	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. If present, the VPN Dialer enters the value for this parameter.	Either do not include this parameter or leave it blank. The VPN Client GUI ignores a read-only setting on this parameter.	Certificates > View
<b>Note</b> When processing certificate authentication, the software uses the following fields in priority order: CertSerialHash CertSubjName CertName If there are two certificates with the same DN or CN, the software chooses the first certificate.			
SendCertChain	Sends the chain of CA certificates between the root certificate and the identity certificate plus the identity certificate to the peer for validation of the identity certificate.	0 = disable (default) 1 = enable	<ul style="list-style-type: none"> <li>• Connection Entry &gt; New/Modify</li> <li>• Certificates &gt; Export</li> </ul>

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
VerifyCertDN	Prevents a user from connecting to a valid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.	Include any certificate DN values of both subject and issuer:  You can use all valid ASCII characters including <code>-_@&lt;&gt;().,</code> , as well as wildcards. See example:	Does not appear in GUI
<p>Example: <code>VerifyCertDN=CN="ID Cert",OU*"Cisco",ISSUER-CN!="Entrust",ISSUER-OU!*"wonderland"</code>  <code>CN="ID Cert"</code>—Specifies an exact match on the CN.  <code>OU*"Cisco"</code>—Specifies any OU that contains the string "Cisco".  <code>ISSUER-CN!="Entrust"</code>—Specifies that the Issuer CN must not equal "Entrust".  <code>ISSUER-OU!*"wonderland"</code>—Specifies that the Issuer OU must not contain "wonderland".</p>			
DHGroup	Allows a network administrator to override the default group value on a VPN device used to generate Diffie-Hellman key pairs.	1 = modp group 1 2 = modp group 2 (default) 5 = modp group 5  Note: This value is preset only for pre-shared keys; for a certificate-authenticated connection, the DHGroup number is negotiated.	Does not appear in GUI
RadiusSDI	Tells the VPN Client to assume that Radius SDI is being used for extended authentication (XAuth).	0 = No (default) 1 = Yes	If this parameter is enabled, the prompts in the GUI for SDI authentication are from Radius SDI and configured using parameters in the <code>vpnclient.ini</code> file.
SDIUseHardwareToken	Enables a connection entry to avoid using RSA SoftID software.	0 = Yes, use RSA SoftID (default) 1 = No, ignore RSA SoftID software installed on the PC.	Does not appear in GUI
EnableSplitDNS	Determines whether the connection entry is using splitDNS, which can direct packets in clear text over the Internet to domains served through an external DNS or through an IPSec tunnel to domains served by a corporate DNS. This feature is configured on the VPN 3000 Concentrator and is used in a split-tunneling connection.  <b>Note</b> You must also enable this feature on the VPN central-site device you are connecting to.	0 = No 1 = Yes (default)	Does not appear in GUI

Table 2-2 .pcf file parameters (continued)

.pcf Parameter (Keyword)	VPN Client Parameter Description	Values	VPN Client Configuration Location(s)
UseLegacyIKEPort	Changes the default IKE port from 500/4500 to dynamic ports to be used during all connections. You must explicitly enter this parameter into the .pcf file.	0 = Turn off the legacy setting; use dynamic ports with cTCP.  1 = (default) Maintain the legacy setting 500/4500. This lets TCP/UDP work easily with VPN central-site devices that support cTCP. This setting enables interoperability with VPN central-site devices that expect the VPN Client to use static port assignments. Enabling this parameter inhibits interoperability with certain versions of Windows.	Does not appear in GUI
ForceNetlogin (windows-only)	Enables the Force Net Login feature for this connection profile.	0 = Do not force the user to log out and log in (default). 1 = Force user to log out when the Wait time is reached unless an option is selected. 2 = Disconnect VPN session upon reaching the Wait time unless an option is selected. 3 = Wait for the user to select Connect or Disconnect.	Does not appear in GUI

## Distributing Configured VPN Client Software to Remote Users

When you have created the VPN Client profile configuration file, you can distribute it to users separately or as part of the VPN Client software.

### Separate Distribution

To distribute the configuration file separately and have users import it to the VPN Client after they have installed it on their PCs, follow these steps:



#### Note

For the Mac OS X platform, the configuration file is placed in the Profiles folder before the VPN Client is installed. See Chapter 2 of the *VPN Client User Guide for Mac OS X* for more information.

- 
- Step 1** Distribute the appropriate profile files to users on whatever media you prefer.
- Step 2** Supply users with necessary configuration information.

- Step 3** Instruct users to:
- a. Install the VPN Client according to the instructions in the *VPN Client User Guide* for your platform.
  - b. Start the VPN Client and follow the instructions in Chapter 5 of the *VPN Client User Guide* for your platform. See the section “Importing a VPN Client Configuration File.” (Windows-only)
  - c. Finish configuring the VPN Client according to the instructions in Chapter 4 of the *VPN Client User Guide* for your platform.
  - d. Connect to the private network, and enter parameters according to the instructions in Chapter 5 of the *VPN Client User Guide* for your platform.
- 

## Distribution with the VPN Client Software

If the `vpnclient.ini` file is bundled with the VPN Client software when it is first installed, it automatically configures the VPN Client during installation. You can also distribute the profile files (one `.pcf` file for each connection entry) as preconfigured connection profiles for automatic configuration.

To distribute preconfigured copies of the VPN Client software to users for installation, perform the following steps:

- 
- Step 1** Copy the VPN Client software files from the distribution CD-ROM into each directory where you created an `vpnclient.ini` (global) file and separate connection profiles for a set of users.



**Note** For the Mac OS X platform, preconfigured files are placed in the Profiles and Resources folders before the VPN Client is installed. The `vpnclient.ini` file is placed in the installer directory. You must place custom `vpnclient.ini` files in the VPN Client Installer directory at the same level as the Profiles and Resources folders. See Chapter 2 of the *VPN Client User Guide for Mac OS X* for more information.

---

- Step 2** Prepare and distribute the bundled software.
- CD-ROM or network distribution:* Be sure the `vpnclient.ini` file and profile files are in the same directory with all the CD-ROM image files. You can have users install from this directory through a network connection; or you can copy all files to a new CD-ROM for distribution; or you can create a self-extracting ZIP file that contains all the files from this directory, and have users download it, and then install the software.
- Step 3** Supply users with any other necessary configuration information and instructions. See Chapter 2 of the *VPN Client User Guide* for your platform.
-

