



User 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). User profiles reside in the `/etc/CiscoSystemsVPNClient/Profiles/` directory. Leave the permissions for the Profiles folder set at `drwxrwxrwx`. Each profile in the Profiles folder should have the following permissions: **-rw-rw-rw-**.

User profile parameters include the remote server address, IPSec group name and password, use of a log file, use of backup servers, and automatic connect upon startup. Each connection entry has its own user profile.



Note

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

This chapter describes how to create a VPN Client user profile.

To set global profiles for all users, refer to the *Cisco VPN Client Administrator Guide*.

Sample Profile Description

There are two ways to create a user profile:

- Use a text editor to modify the sample profile that comes with the VPN Client installer and rename it.
- Create a unique user profile using a text editor.

There is only one user profile per connection.

The VPN Client software is shipped with a sample user profile. The file is named `sample.pcf`.

The following is an example of a sample user profile that might be shipped with your installer.

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=gawf
SaveUserPassword=0
```


Table 3-1 User Profile Keywords (continued)

Keywords	Description
Host = <i>IP_Address or hostname</i>	The hostname or IP address of the VPN device you want to connect with. The maximum length of the hostname is 255 alphanumeric characters.
AuthType = {1 3 5}	<p>The authentication type that this user is using.</p> <ul style="list-style-type: none"> • 1 is preshared keys. • 3 is a digital certificate using an RSA signature. • 5 is mutual group authentication <p>If you select AuthType 1 or AuthType 5, you must also configure the GroupName and GroupPwd. To use AuthType5, you must have a root certificate on your VPN Client system. For information on how to install a root certificate automatically on your specific platform, see “Installing the VPN Client.”</p>
GroupName = <i>String</i>	The name of the IPSec group configured on the VPN device that contains this user. The maximum length is 32 alphanumeric characters. This keyword is case sensitive.
GroupPwd = <i>String</i>	The password for the IPSec group that contains this user. The minimum length is 4 alphanumeric characters. The maximum is 32. This keyword is case sensitive and entered in clear text.
encGroupPwd = <i>String</i>	Displays the group password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
Username = <i>String</i>	The name that identifies a user as a valid member of the IPSec group specified in GroupName . The VPN Client prompts the user for this value during user authentication. The maximum length is 32 alphanumeric characters. This keyword is case sensitive and entered in clear text.
UserPassword = <i>String</i>	<p>This password is used during extended authentication.</p> <ul style="list-style-type: none"> • If SaveUserPassword is enabled, the first time the VPN Client reads this password, it is saved in the user profile as encUserPassword, and the clear text version is deleted. • If SaveUserPassword is disabled, the VPN Client deletes the clear text version of the user password in the user profile but it does not create an encrypted version.
encUserPassword = <i>String</i>	Displays the user password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
SaveUserPassword = {0 1}	<p>Determines if the user password or its encrypted form are valid in the user profile.</p> <ul style="list-style-type: none"> • 0, the default, displays the user password in clear text in the user profile and is saved locally. • 1 displays the user password in the user profile in its encrypted version, and the password is not saved locally. <p>This value is set in the VPN device, not in the VPN Client.</p>

Table 3-1 User Profile Keywords (continued)


Keywords	Description
EnableBackup = {0 1}	Specifies to use a backup server if the primary server is not available. <ul style="list-style-type: none"> • 0, the default, disables the backup server. • 1 enables the backup server. You must also specify a BackupServer .
BackupServer = <i>IP_Address or hostname</i>	List of IP addresses or hostnames of backup servers. Separate multiple entries by commas. The maximum length of hostname is 255 alphanumeric characters.
EnableLocalLAN = {0 1}	Allows you to configure access to your local LAN. <ul style="list-style-type: none"> • 0, the default, disables local LAN access. • 1 enables local LAN access.  <p>Note To allow local LAN access, it must be enabled on both the VPN Client and the VPN device you are connecting to.</p>
EnableNAT = {0 1}	Specifies whether or not to enable secure transmission between a VPN Client and a VPN device through a router serving as a firewall, which might also be using the NAT protocol. <ul style="list-style-type: none"> • 0, the default, disables IPsec through NAT mode. • 1 enables IPsec through NAT mode.
TunnelingMode = {0 1}	Allows you to select which form of NAT transversal is used. <ul style="list-style-type: none"> • 0, the default, specifies IPsec over UDP for NAT transparency. • 1 specifies IPsec over TCP for NAT transparency. You must also have IPsec through NAT enabled.
TCP TunnelingPort = {0 65535}	Sets which TCP port to use for the cTCP protocol. The default is 10000. You must also have IPsec through NAT enabled and the Tunneling Mode set for IPsec over TCP.
ForceKeepAlives = {0 1}	Allows the VPN Client to keep sending IKE and ESP keepalives for a connection at approximately 20-second intervals so that the port on an ESP-aware NAT/Firewall does not close. <ul style="list-style-type: none"> • 0, the default, disables keepalives. • 1 enables keepalives.
PeerTimeout = <i>Number</i>	The number of seconds to wait before terminating a connection when the VPN device on the other end of the tunnel is not responding. The range is 30 to 480 seconds. The default is 90.
CertStore = {0 1}	Identifies the type of store containing the configured certificate. <ul style="list-style-type: none"> • 0 = default, none. • 1 = Cisco.
CertName = <i>String</i>	Identifies the certificate used to connect to the VPN device. The maximum length is 129 alphanumeric characters.

Table 3-1 User Profile Keywords (continued)

Keywords	Description
CertPath = <i>String</i>	The path name of the directory containing the certificate file. The maximum length is 259 alphanumeric characters.
CertSubjectName = <i>String</i>	The qualified Distinguished Name (DN) of the certificate's owner. You can either <i>not</i> include this keyword in the user profile, or leave this entry blank.
CertSerialHash = <i>String</i>	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. You can either <i>not</i> include this keyword in the user profile, or leave this entry blank.
DHGroup = {1 2 5}	<p>Allows a network administrator to override the configured group value used to generate Diffie-Hellman key pairs on a VPN device.</p> <ul style="list-style-type: none"> • 1 = modp group 1 • 2 = modp group 2 • 5 = modp group 5 <p>The default is 2. The VPN Concentrator configuration for IKE Proposal must match the DHGroup in the VPN Client. If the AuthType is set to 3 (digital certificate), this keyword has no effect on the VPN Client.</p>

