Avaya VPN Client — Configuration

VPN Client Software
Release 10.06

Document Status: **Standard**

Document Number: **NN46110-509**

Document Version: **05.02**

Date: **June 2012**

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Tables

Preface

This guide helps you install, configure, and use the Avaya VPN Client (AVC) for the Windows XP, Windows Vista, and Windows 7 operating systems. Topics include

- starting Avaya Virtual Private Network Gateway (AVC)
- support for Avaya Virtual Private Network Gateway (AVG)
- Domain logon on Vista and Windows 7 using Pre-Logon Access Provider (PLAP)
- Domain logon on XP using Two-step login
- creating profiles for IPSec and SSL tunnels
- optional configuration settings
- using the client from a script or a third-party application

This guide is intended for network managers who are responsible for setting up client software for the Avaya VPN Router and Avaya VPN Gateway. This guide assumes that you have the following background

- experience with Windows operating systems or graphical user interfaces (GUI)
- familiarity with network management

For more information about configuring and monitoring the VPN Router, see *Avaya VPN Router Configuration — Basic Features* (NN46110-500).

For more information about the AVG, see *Avaya VPN Gateway User Guide* (NN46120-104).

Before you begin

The recommended PC requirements for running the AVC are

- Windows XP, Windows Vista, or Windows 7.
- 1 GHz 32-bit (x86) or 64-bit (x64) processor.
- 1 GB of system memory.
- 40 GB hard drive with 5 GB of available space.

Text conventions

This guide uses the following text conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **ldap-server source {external | internal}**, you must enter either **ldap-server source external** or **ldap-server source internal**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **show ntp [associations]**, you can enter either **show ntp** or **show ntp associations**. Example: If the command syntax is **default rsvp** [**token-bucket** {**depth** | **rate**}], you can enter **default rsvp**, **default rsvp token-bucket depth**, or **default rsvp token-bucket rate**.

ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **more disk***n*:*<directory>/...<file_name>*, you enter **more** and the fully qualified name of the file.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **ping** *<ip_address>*, *ip_address* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Select Status > Health Check.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **terminal paging {off | on}**, you enter either **terminal paging off** or **terminal paging on**, but not both.

Acronyms and terms

This guide uses the following acronyms and terms

API	Application Program Interface
BER	basic encoding rules
CA	Certification Authority
Certification path	Ordered sequence of certificates, leading from a certificate whose public key is known by a client to a certificate whose public key is to be validated by the client

Credential Provider	A module plug-in that handles credential information and communication with an external authentication provider
CRL	Certificate revocation list—list of revoked but unexpired certificates issued by a CA
Digital certificate	Digitally signed data structure defined in the X.509 standard that binds the identity of a certificate holder (or subject) to a public key
DLL	Dynamic Link Library
IKE	Internet Key Exchange
ISAKMP	Internet Security Association and Key Management Protocol
LDAP	Lightweight Directory Access Protocol
MSI	Microsoft Windows Installer
AVC	Avaya VPN client
AVG	Avaya VPN Gateway
AVR	Avaya VPN Router
PLAP	Pre-Logon Access Provider
Public Key Cryptography Standards (PKCS)	Collection of de facto standards produced by RSA covering the use and manipulation of public-private keys and certificates
PKCS #7	Cryptographic Message Standard (Reply with digital certificate)
PKCS #10	Certification Request Syntax Standard
PKCS #12	Personal Information Exchange Syntax
PKI	Public Key Infrastructure
TCP	Transmission Control Protocol
X.509	Standard certificate format

Related publications

For more information about the Avaya VPN Client, Avaya VPN Router and Avaya VPN Gateway, see the following publications:

- *Avaya VPN Client 10.06 Release Notes* provide the latest information, including brief descriptions of the new features, problems fixed in this release, and known problems and workarounds.
- *Avaya VPN Client — Installation and Upgrades* (NN46110-412) provides instructions for installing AVC and upgrading software from previous versions.
- *Avaya VPN Gateway User Guide* (NN46120-104) Describes how to perform basic configuration and maintenance of the Avaya VPN Gateway (AVG).
- *Avaya VPN Gateway VMware Getting Started Guide* (NN46120-302). Provides information on how to configure and deploy the Avaya VPN Gateway (AVG) VMware appliances.
- *Avaya VPN Gateway BBI Application Guide* (NN46120-102). Provides examples to configure the Avaya VPN Gateway for VPN deployment by using the Browser-Based Management Interface (BBI).
- *Avaya VPN Gateway Application Guide for SSL Acceleration*. Provides examples on how to configure SSL Acceleration through the CLI.
- *Avaya VPN Gateway CLI Application Guide for VPN*. Provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway VPN Administrators Guide*. VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway Troubleshooting Guide*. Describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway.
- *Avaya VPN Gateway Release Notes*. Lists new features available in the current version and provides up-to-date product information.
- *Avaya VPN Router Configuration — Basic Features* (NN46110-500) introduces the product and provides information about initial setup and configuration.
- *Avaya VPN Router Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions for configuring authentication services and digital certificates.
- *Avaya VPN Router Security — Firewalls, Filters, NAT, and QoS* (NN46110-601) provides instructions for configuring the Stateful Firewall and Avaya VPN Router and Avaya VPN Gateway interface and tunnel filters.

- *Avaya VPN Router Configuration — Advanced Features* (NN46110-502) provides instructions for configuring advanced LAN and WAN settings, PPP, frame relay, PPPoE, ADSL and ATM, T1CSU/DSU, dial services and demand services, DLSw, IPX, and SSL VPN.
- *Avaya VPN Router Configuration — Tunneling Protocols* (NN46110-503) provides configuration information for the tunneling protocols IPsec, L2TP, PPTP, and L2F.
- *Avaya VPN Router Configuration — Routing* (NN46110-504) provides instructions for configuring BGP, RIP, OSPF, and VRRP, as well as instructions for configuring ECMP, routing policy services, and client address redistribution (CAR).
- *Avaya VPN Router Configuration — Troubleshooting* (NN46110-602) provides information about system administrator tasks such as backup and recovery, file management, and upgrading software, and instructions for monitoring gateway status and performance. This book also provides troubleshooting information and interoperability considerations.
- *Avaya VPN Router Using the Command Line Interface* (NN46110-507) provides syntax, descriptions, and examples for the commands that you can use from the command line interface on the VPN Router.
- *Avaya VPN Router Configuration — TunnelGuard* (NN46110-307) provides information about configuring and using the Avaya Endpoint Access Control Agent feature.

Hard-copy technical manuals

To print selected technical manuals and release notes free, directly from the Internet, go to www.avaya.com/support. Find the product for which you need documentation, then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. For more information about a free copy of the Adobe Reader, go to the Adobe Systems Web site: www.adobe.com.

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to http://www.avaya.com/support or go to one of the pages listed in the following sections.

Navigation

- "Getting technical documentation" on page 13
- "Getting product training" on page 13
- "Getting help from a distributor or reseller" on page 13
- "Getting technical support from the Avaya Web site" on page 13

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to http://www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at http://www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at http://www.avaya.com/support.

Client logon

This chapter describes how you use the Avaya VPN Client (AVC) to launch a VPN tunnel using the Windows XP, Windows Vista, and Windows 7 operating systems.

For information about how to install AVC and the Pre-Logon Access Provider (PLAP), and to customize installation, see *Avaya VPN Client — Installation and Upgrades* (NN46110-412).

Table 1 “AVR and AVG support” on page 15 shows Avaya VPN Router (AVR) and Avaya VPN Gateway (AVG) versions that support the Avaya VPN Client (AVC).

Table 1 AVR and AVG support

AVC Version	AVR	AVG
10.04 and higher (See note)	version 7.xx version 8.xx	version 6.0.13 and higher version 7.xx version 8.xx version 9.xx
Note: AVC version 10.01 supports Windows Vista only.		

Table 2 “AVC IPSec support” on page 16 shows options that are available for IPSec cipher combinations.

Table 2 AVC IPSec support

Version	IPSec cipher combination
10.01 and higher	ESP -256 AES with Sha1 ESP -128 AES with Sha1 ESP - Triple DES with SHA1 ESP - Triple DES with MD5 ESP - 56-BIT DES with SHA1 ESP - 56-BIT DES with MD5 ESP - 40-BIT DES with SHA1 ESP - 40-BIT DES with MD5 ESP - NULL with SHA1 ESP - NULL with MD5

Table 3 “AVC SSL support” on page 16 shows options that are available for SSL cipher combinations.

Table 3 AVC SSL support

Version	SSL cipher combination
10.01 and higher	(DHE_RSA_WITH_3DES_EDE_CBC_SHA, 0x16) (RSA_WITH_3DES_EDE_CBC_SHA, 0x0a) (RSA_WITH_RC4_128_SHA, 0x05) (RSA_WITH_RC4_128_MD5, 0x04) (RSA_EXPORT1024_WITH_RC4_56_SHA, 0x64) (RSA_EXPORT1024_WITH_DES_CBC_SHA, 0x62) (RSA_EXPORT1024_WITH_RC4_56_MD5, 0x60) (DHE_RSA_WITH_DES_CBC_SHA, 0x15) (RSA_WITH_DES_CBC_SHA, 0x09) (DHE_RSA_EXPORT_WITH_DES40_CBC_SHA, 0x14) (RSA_EXPORT_WITH_DES40_CBC_SHA, 0x08)

This chapter includes the following topics:

Starting a VPN tunnel

You start the VPN tunnel through a logon window. Before using AVC, you must ensure you have administrator rights to AVC to use the following functionalities

- creating global profiles
- editing, cloning and deleting options for global profiles
- clearing logs
- modifying log level settings
- Manage Option settings
  - Enable Certificate Revocation List validation for server certificate
  - Display the warning message if the VPN tunnel is still up
  - Disconnect active VPN tunnel

To use the previous functionalities, right-click the Nvc.exe short cut on your desktop, and click **Run as Administrator**.

Start the AVC by performing the following procedure:

1. From Windows, choose **Start, All programs, Avaya VPN Client, Avaya VPN Client.**

   The Connection window appears.

2. Select a connection from the **VPN Connection** list or if this your first logon, you must create a profile.
3. Enter a **user name** and **password** in the **Username** and **Password** fields.
4. Click **Connect**. A status dialog box appears showing the connection status.

After the tunnel is up, a security banner can appear depending on the AVR or AVG setting. If the security banner appears, click **Accept**. The VPN tunnel becomes fully functional. You must accept or the tunnel is taken down. Once the tunnel is fully up, a tray icon appears in the system tray.

Right-click this icon to open up an abbreviated menu. The menu lists the following options:

- Status — opens the **Status** window.
- View Log — opens the **Log Viewer** window.
- View Banner — opens the banner message for the current VPN connection.
- Configuration**s** — opens the **AVC Manage Profiles** window. You can manage profiles and options.
- Help — opens the full Help menu for the AVC.
- About Avaya VPN Client— opens an **About** window showing AVC version information.
- Disconnect VPN — disconnects the VPN with a confirmation.

Logging on using the Pre-Logon Access Provider for Windows Vista and Windows 7

This release provides the Pre-Logon Access Provider (PLAP). A PLAP is a special type of credential provider that allows you to make a network connection before logging on to your PC.

You cannot use the Prelogon Access Provider (PLAP) functionality in conjunction with digital certificate authentication. PLAP doesn't support certificate authentication. When you attempt to make a connection, the error message Failed to connect to following reason: Authentication failure appears.

To ensure security, PLAP does not support PreLaunch and PostLaunch applications and users cannot configure profiles or other AVC settings from PLAP.

You must select Global Profile when configuring an IPSec or SSL profile to enable PLAP.

Log on the AVC with PLAP by performing the following procedure:

1. Log on to your PC by pressing **Ctrl+Alt+Del** to initiate the logon process. A logon window appears.

   The **Ctrl+Alt+Del** keystroke sequence is called a Secure Attention Sequence (SAS). An administrator can enable or disable the SAS.

2. Click **Switch User** to return to the main logon window.

3. Click the **PLAP** icon in the lower right-hand corner of the **Avaya VPN Client** window. One of the following windows appears:

   a. If a tunnel is not connected, the **Establish a VPN Connection** window appears. Go to step 4.

   b. If a tunnel is connected, the **VPN Tunnel is up already** window appears. Go to step 5.

4. If there is not an established tunnel, you are then at the **Establish a VPN Connection** window, perform the following:

   a. Click the submit button (arrow) following **Establish a VPN Connection**. The window displays the message `AVC is starting up, please wait. This may take a few minutes` then changes to `Avc GUI is still running. Waiting for it to finish up`. The **Connection** window appears.

      The first time that you are attempting to launch AVC after a restart you can experience a 20 second or less delay in launching. But you can wait up until 3 minutes. If the AVC PLAP does not connect before 3 minutes, a message stating `Avc Gui didn't respond. Please try again later` appears. You are then returned to the Establish a VPN Connection window.

      Subsequent successful connections reduce the wait time after each attempt when establishing a connection.

   b. Select a preconfigured global profile from the **VPN Connection** list.

   c. Type a password in the **Password** field if it is not saved, and then click **Connect**. The Connect status dialog window appears. The message `VPN Tunnel has been established by AVC` appears on the window and then the **main logon** window appears.

To ensure security, you cannot change the profile, make configurations, or other changes in the pre-logon stage.

d Log on to your PC.

You can click Disconnect beside the PLAP icon to disconnect the VPN connection as well as all other connections brought up by PLAP.

5 If there is an established tunnel and you are at the **VPN Tunnel is up already** window, perform the following:

a Click the submit button (arrow) following **VPN Tunnel is up already**. The main logon window appears.

b Log on to your PC.

You can click Disconnect beside the PLAP icon to disconnect the VPN connection as well as all other connections brought up by PLAP.

Domain logon on XP using Two-step login

AVC provides PLAP feature for domain logon on Vista and Windows 7 operating systems. On XP, domain logon can be achieved through "Two-Step logon" which is explained below:

1 User logs on to the machine using local account

2 Launch AVC in administrator mode

3 Go to **Edit the Profile** dialog and click on **Manage Options** dialog.

4 To set the log-off behavior, check the tab **Display the warning message if the VPN tunnel is still up**

5 Bring up tunnel

6 Manually log-off operating system. Tunnel will be maintained by AVC service component.

7 User logs back in using a domain account. This time, the logon authentication will be done through the tunnel with the Active Directory on the domain

Viewing the Avaya VPN Client Status monitor

The Avaya VPN Client Status monitor shows information regarding the current configuration status such as security, destination IP address, connection statistics and Keepalive parameters. Also on the window are buttons that enable you to configure and monitor the AVC.

To use the Avaya VPN Client Status monitor, perform the following:

1. Log on to the AVC. For more information on logons, see "Starting a VPN tunnel" on page 17.
2. After you successfully connect to a PC over a VPN tunnel, a tray icon appears in the system tray. Clicking on the icon opens the Avaya VPN Client Status window.
3. View the following configuration status information on the left of the window as shown in or click on the following buttons to configure or view further information on the AVC:
   - Close — closes the status window.
   - Disconnect — disconnects the VPN with a confirmation.
   - Configuration — opens the Avaya Client Manage Profiles window. You can manage profiles and options.
   - View Banner — opens the banner message for the current VPN connection.
   - View Log — opens the Log Viewer window.
   - Help— opens the Help window.
   - About — opens an About window showing Avaya VPN Client version information.

The following image shows the Status window.

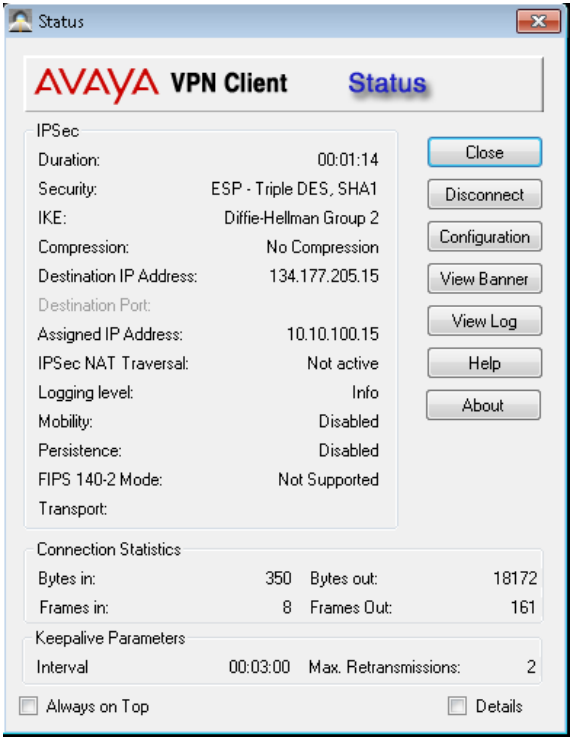


Table 4“Configuration status information” on page 22 lists descriptions of the AVC connection types.

Table 4 Configuration status information

Connection information	Description
Duration	Shows the current connected time for the tunnel
Security	Shows the type of security used for this tunnel
IKE	Shows the type of Diffie-Hellman cipher. Not available for SSL.
Compression	Shows the type of compression used for this tunnel
Destination IP Address	Shows the IP address of the server connecting with the AVC
Destination Port	Shows the connected port number. Not available for IPSec
Assigned IP Address	Shows the IP address assigned for this tunnel
IPSec NAT Transversal	Shows the port number of an active IPSec transmission. Not available for SSL

Table 4 Configuration status information

Connection information	Description
Logging Level	Shows the type of logging level. For more information on logging levels.
Mobility	Shows the type of Mobility enabled for this tunnel
Persistence	Shows if persistent connection is enabled. Not available for SSL.
FIPS 140-2 mode	Shows the type of FIPS 140-2 encryption used for this tunnel. Not available for SSL.
Transport	Shows the type of transport used for this tunnel.
Bytes in Bytes out	Shows the number of bytes ingoing to the AVC and outgoing from the AVC
Frames in Frames out	Shows the number of frames ingoing to the AVC and outgoing from the AVC. Not available for SSL.
Encryption Decryption	Shows the number of errors occurring during encryption or decryption
Intervals Maximum retransmissions	Intervals is the number of milliseconds of wait time before sending keepalive packets Retransmissions is the time in milliseconds between retransmisssions of keepalives after the Keepalive wait time expires
Always on Top	Click to keep the status monitor on top of your other programs
Details	Click to showing connection statistic details

Second instance of AVC GUI

When you launch a second instance of the AVC GUI, a status dialog box appears indicating that an active tunnel is already present on the PC.

Client profile configuration

This chapter provides information about how to configure IPsec and SSL profiles using the Set Up Wizard or with the Manage Profiles dialog box.

For information about how to install the AVC and the Pre-Logon Access Provider (PLAP), and to customize installation, see *Avaya VPN Client — Installation and Upgrades* (NN46110-412).

For information about how to configure split tunneling, mobility and persistence for use with the AVC, see *Avaya VPN Router Configuration — Basic Features* (NN46110-500).

For information about how to configure the AVC to co-exist with Microsoft IPsec Policy Service, see *Avaya VPN Router — Tunneling Protocols* (NN46110-503).

This chapter includes the following topics:

Creating an IPSec profile using the Set Up Wizard

Use the Set Up Wizard to quickly create a standard profile on the Client.

Create a profile data file or user configuration file or machine configuration data using the Set Up Wizard, by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Profile Wizard**.

   The Avaya VPN Client Profile Wizard window appears.

3. Type in a profile name into the **Profile Name** box. You can also enter a description of the profile.
4. Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP. Click **Next**.
5. Click **IPSec Tunnel** as a connection type for this profile. Click **Next**.
6. Type in an IP address or DNS for the VPN into the **Destination** box. Click **Next**.
7. Select one of the following Authentication types, and then click **Next**:
   a. **Username and Password.** Go to step 8.
   b. **Hardware or Software Token Card.** Go to step 9.
   c. **Digital Certificate and Smartcard.** Before using this option, you must import a certificate into the Microsoft Certificate Store. See "Importing and obtaining digital certificates" on page 54. Go to step 9.
8. If you have selected **Username and Password**, perform the following:
   a. Type the username and password as assigned to you by the network administrator into the **Username** and **Password** boxes. Click **Next.**
   b. Click **No** if you do not have a group ID and group password. Click **Yes** if you do, and then type the group ID and group password as assigned to you by the network administrator into the **Group ID** and **Group Password** boxes. Click **Next.** Go to step 10.

If you have selected **Hardware or Software Token Card**, perform the following:

a Select one of the following tokens, and then click **Next**:

— **Challenge Response Token Card**

— **Response Only Token Card**.
Click **Use Passcode** if you are using a passcode.

— **Response Only Software Token**

b Type the user and token group ID, and token group password as assigned to you by the network administrator into the **User ID**, **Token Group ID** and **Token Group Password** boxes. Click **Next.** Go to step 10.

9 If you have selected **Digital Certificate and Smartcard**, perform the following:

a If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate**. Click **Next**.

b If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list. Click **Next**.

10 Click **No** if you do not want to dial first, and then click **Next.** Click **Yes** if you want to make a dial-up connection first. Selecting **Yes** opens the following section**.**

a Select a dial-up from an existing connection from the list or click **Create a new Dial-up entry**. The Set up a new dial-up connection dialog box appears.

b Click the **Dialing Rules** link. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.

c Type the telephone number that the AVC uses to dial up the server into the **Telephone number** box.

d Type a name that identifies the connection into the **Destination** box.

e If you are using a smart card, click **Use a Smart Card**. Click **Create** if you do not want others to use this connection.

f If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.

g Click **Next**. The Type your user name and password section appears.

h Type your user name into the **User name** box.

i Type a password into the **Password** box. You can also select **Show characters** to show the password in the box and **Remember this password** to save the password without having to reenter it again.

j You can optionally type a domain name into the **Domain** box.

k Click **Create** to configure the new dial-up settings. Click **Next**.

11 Click **No** if you do not want to launch an application or **Yes** if you want to launch an application before or after your VPN connection is established. Selecting Yes opens Before and After connection sections.

a In either the **Before connection** or **After connection** section, select the application you want to launch by clicking the **search** button beside the Application box. A Windows box opens from your PC. Search for and click the application executable file to enter it into the **Application** box.

b Type the command line of the application into the **Command line** box.

c For an application that you are starting before a connection, set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box. Click **Next**.

12 Select whether you will define or not define a failover profile. If you click **I will define a failover profile**, a list of previously configured profiles appears. Select a profile from this list, and then click **Next**.

13 Select one of the following Keepalive types then click **Next**:

- **No Keepalives** — disables the Keepalives.
- **Active Keepalives (Dead peer detection)** — determines if a tunnel connection is available.
- **Passive Keepalives (No Dead peer detection)** — maintains state information in the local internet access device.

14 Click **Finish** to complete the creation of the profile.

Creating an IPSec profile using Manage Profiles

Create an IPSec profile, by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.
4. From the **General** tab, choose **IPSec Tunnel** as a connection type for this profile from the **Tunnel Type** list.
5. Type in a profile name into the **Profile** box. You can optionally enter a description of the profile.
6. Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.
7. Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.
8. Type an IP address or DNS for the VPN into the **Destination** box.
9. Select one of the following Authentication types:
   - **Username and Password**
   - **Certificate Authentication**
   - **Group Security Authentication**
10. If you choose **Username and Password** perform the following:
    a. By default **Username and Password** is already selected. Type the username assigned to you by the network administrator into the **Username** box.
    b. Type the password assigned to you by the network administrator into the **Password** box.
    c. Click **Save Password** to save the password.
11. If you choose **Certificate Authentication** perform the following:

a Click **Certificate Authentication** to enable the certificate selection.

b Click **Select**. The Select a certificate window appears. Choose either step c or step d.

c If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate**.

d If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

e Click **OK** to close the window.

f If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.

g Click **Save** to save the new profile.

12 If you choose **Group Security Authentication,** perform the following:

a Click **Group Security Authentication** to enable the group security authentication.

b Select a group authentication type from the list.

— **RADIUS Authentication**

— **Challenge Response Token**

— **Response Only Hardware Token**

— **Response Only Software Token**

The fields in Authentication Information area change according to the type selected. When choosing an authentication type, see Table 1 “IPSec authentication information requirements” on page 31 for the required authentication information.

Table 1 IPSec authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (non modifiable)
RADIUS Authentication	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **Save Password**: click to save the password. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.
Challenge Response Token	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **Save Password**: click to save the password. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.

Table 1 IPSec authentication information requirements

Authentication type	Authentication information
Response Only Hardware Token	**Username**: type the username supplied by your administrator. **PIN**: type the PIN supplied by your administrator. **Save PIN**: click to save the PIN. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator. **Use Passcode**: click to enable a passcode.
Response Only Software Token	**Username**: type the username supplied by your administrator. **PIN**: type the PIN supplied by your administrator. **Save PIN**: click to save the PIN. **Group ID**: type the group identification supplied by your administrator. **Group Password**: type the group password supplied by your administrator.

13 Click **Save** to save the configuration.

Creating a SSL profile using the Set Up Wizard

Use the Set Up Wizard to quickly create a secure profile on the AVC.

Create a profile using the Set Up Wizard, by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Profile Wizard**.

   The Avaya VPN Client Profile Wizard window appears.

3. Type in a profile name into the **Profile Name** box. You can optionally enter a description of the profile.
4. Click **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP. Click **Next**.
5. Click **SSL Tunnel** as a connection type for this profile. Click **Next**.
6. Type in an IP address or DNS name for the VPN into the **Destination** box. Type in the port number assigned to you by your administrator into the **Port** box. Click **Next**.
7. Select one of the following:
   - **a** Click **Use certificate to authenticate** to enable the certificate selection. Click **Next**.
   - **b** Click **Use predefined Login Service to authenticate** to enable Predefined Login Service configuration. Click **Next**.
8. Select one of the following Proxy settings:
   - **a** Click **Don’t Use proxy** if you don’t want to apply proxy settings. This the default setting.
   - **b** Click **Use default browser’s proxy settings** if you want to use your browser proxy settings.
   - **c** Click **Use defined proxy settings** when you want to configure your own. Clicking enables the field information.
   - **d** Type an IP address or DNS into the **Proxy address** box.

e Type the port number supplied by your administrator into the **Port** box. Click **Next**.

To exclude the IP address from being used on the proxy server, type the IP addresses into the box. Be sure to separate the addresses from each other using semicolons.

9 If you selected **Use certificate to authenticate** from step 7, perform the following:

a If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate.** Click **Next**.

b If you want to manually select a certificate, select **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list, Click **Next** and then go to step 11.

10 If you selected **Use predefined Login Service to authenticate** from step 7, perform the following,

a Select a name for the service from the **Login Service Name** list.

b Click **Response Only Software Token** if you want to enable this token. Click **Next**.

c Type the username as assigned to you by the network administrator into the **Username** box. Click **Next**.

11 Click **No** if you do not want to dial first then click **Next.** Click **Yes** if you want to make a dial-up connection first. Selecting Yes opens the following section**.**

a Select an existing dial-up connection from the list or click **Create a new Dial-up entry**. The Set up a new dial-up connection dialog box appears.

b Click the **Dialing Rules** link. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.

c Type the telephone number that the AVC uses to dial up the server into the **Telephone number** box.

d Type a name that identifies the connection into the **Destination** box.

e If you are using a smart card, click **Use a Smart Card**. Click **Create** if you do not want others to use this connection.

f If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.

g Click **Next**. The Type your user name and password section appears.

h Type your user name into the **User name** box.

i Type a password into the **Password** box. You can also select **Show characters** to show the password in the box.

j You can optionally type a domain name into the **Domain** box.

k Click **Create** to configure the new dialup settings. Click **Next**.

12 Click **No** if you do not want to launch an application or **Yes** if you want to launch an application before or after your VPN connection is established. Selecting Yes opens Before and After connection sections.

a In either the **Before connection** or **After connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box opens from your PC. Search for and click the application executive file to enter it into the **Application** box.

b Type the command line of the application into the **Command line** box.

c For an application that you are starting before a connection, set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box. Click **Next**.

13 Select whether you will define or not define a failover profile. If you click **I will define a failover profile**, a list of previously configured profiles appears. Select a profile from this list and then click **Next**.

14 Click **Finish** to complete the creation of the profile.

Creating a SSL profile using Manage Profiles

Create a SSL VPN when you are managing the security of message transmissions.

Create a SSL profile, by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. Click **New** located over the tabs. The information boxes clear to enable you to create a new profile.
4. From the **General** tab, choose **SSL Tunnel** from the **Tunnel Type** list as a connection type for this profile.
5. Type a profile name into the **Profile** box. You can optionally enter a description of the profile into the **Description** box.
6. Click the **Global Profile** if you want this profile to be viewed by all users on the operating system. You must select **Global Profile** to configure PLAP.
7. Type an IP address or DNS for the VPN into the **Destination** box.
8. Type in the port number assigned to you by your Administrator into the **Port** box.
9. Click **Certificate Authentication** to enable the certificate selection.
10. Click **Select**. The Select a certificate window appears. Choose either step a or step b.

    a. If you want to allow the AVC to select a certificate, click **Automatically select a valid certificate**.

    b. If you want to manually select a certificate, click **Please select a certificate from the Microsoft Certificate Store below** to enable the Microsoft Certificate Store list. Highlight a certificate from the list.

11. Click **OK** to close the window.
12. If you want to associate an alternate name with this certificate, select a name from the **Alt Name** list. The default is None.

13 Click **Predefined Login Service** to enable Predefined Login Service configuration.

14 Choose a name for the service from the **Login Service Name** list. See Table 2 “SSL authentication information requirements” on page 37 for authentication information.

15 Type the username into the **Username** box.

16 Click **Response Only Software Token** if you want to enable this token. Type the PIN number into the **PIN** box.

17 Click **Save** to save the configuration.

The fields you select in the Predefined Login Service depend upon the type of Login service that you are using. When choosing an authentication type, see Table 2 “SSL authentication information requirements” on page 37 for the required authentication information.

Table 2 SSL authentication information requirements

Authentication type	Authentication information
Certificate	Certificate (non modifiable)
Login service (second password is not required)	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **PIN**: if you are using a Response Only Software token, type the PIN supplied by your administrator.
Login service (second password is required)	**Username**: type the username supplied by your administrator. **Password**: type the password supplied by your administrator. **PIN**: if you are using a Response Only Software token, type the PIN supplied by your administrator. **Second Password**: type the password supplied by your administrator.

Creating a cloned profile

You can copy a previously configured profile and then edit the information to save you time from completing all the configuration steps.

Create a cloned profile, by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. Under the **Profile Name** found in the profile list at the top of the window, highlight the profile you want to clone.
4. Click **Clone**. The Clone a profile window appears. Type in a profile name and then click **OK**.
5. Highlight the cloned profile from the profile list and then click **Edit**. Edit the information as desired.
6. Click **Save** to save the configuration.

Editing a profile

Once you have a profile completed you may want to add new features to your profile, such as launching an application, or change some feature already configured, such as removing a Failover. Use the edit function to make and then enable these changes.

Edit a profile, by performing the following procedure:

1. Select **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3. Under the **Profile Name** found in the profile list at the top of the window, highlight the profile you want to edit.
4. Click **Edit**. The profile information appears under the **General** tab.

5 Once you have edited the profile, be sure to click **Save** to save the configuration.

Importing profiles or configuration files

You can import existing profile or configuration files from your local file system. You can use this feature to recover the data files in the event that the AVC Client is un-installed and re-installed. Once the files are imported, the Client automatically re-loads the files.

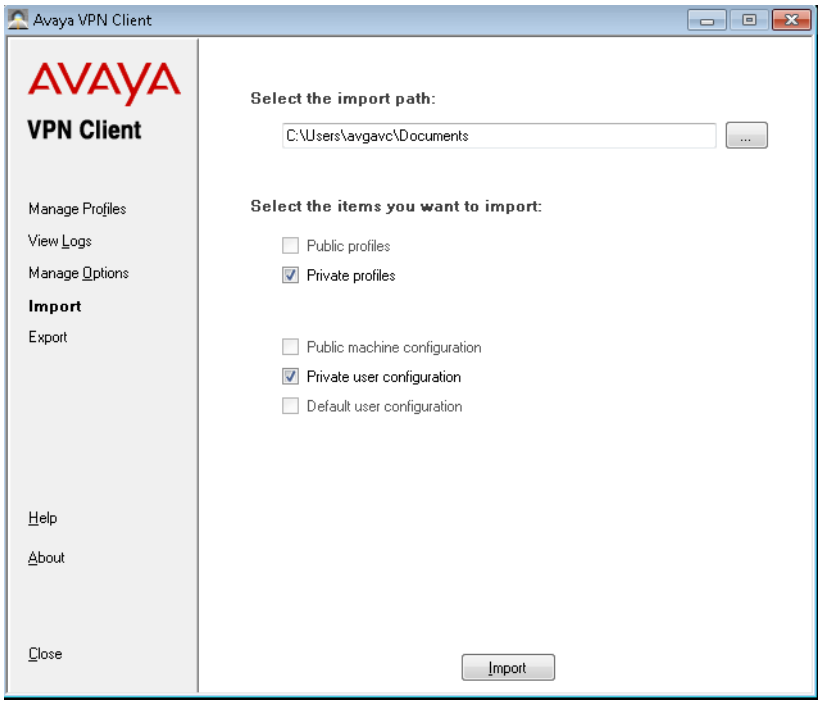
The Import interface is only available when the tunnel is down.

Use the following procedure to import profiles or configuration files:

Caution: You can import profiles and configuration files between different versions of AVC provided the file formats are the same.

1 In the VPN Client navigation pane, select the **Import** option.

The Import user interface (UI) is displayed.



Note: The default location for importing profiles and configuration files from is displayed in the **Select the Import Path** field.

2 If you wish to import files from another location, click the **Browse** button to navigate to the location of the files to be imported.

3 Select one or more of the following import profile file options:

- Public profiles
- Private profiles

Note: Non admin users can select only the Private profile option.

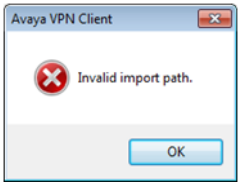
4 Select one or more of the following configuration file options:

- Public machine configuration
- Private user configuration
- Default user configuration

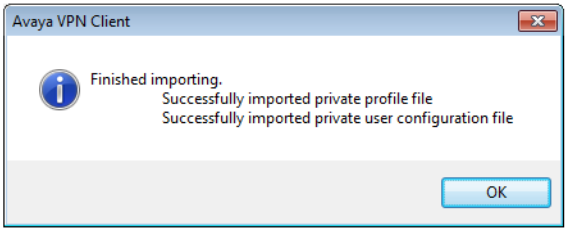
Note: Non admin users can select only the Private user configuration option.

5 Click **Import.**

- If the import path is invalid, a message dialog is displayed, prompting you to click **OK** and correct the filepath specified in step 2.



- If the path is valid, a summary message is displayed.



6 Click **OK**.

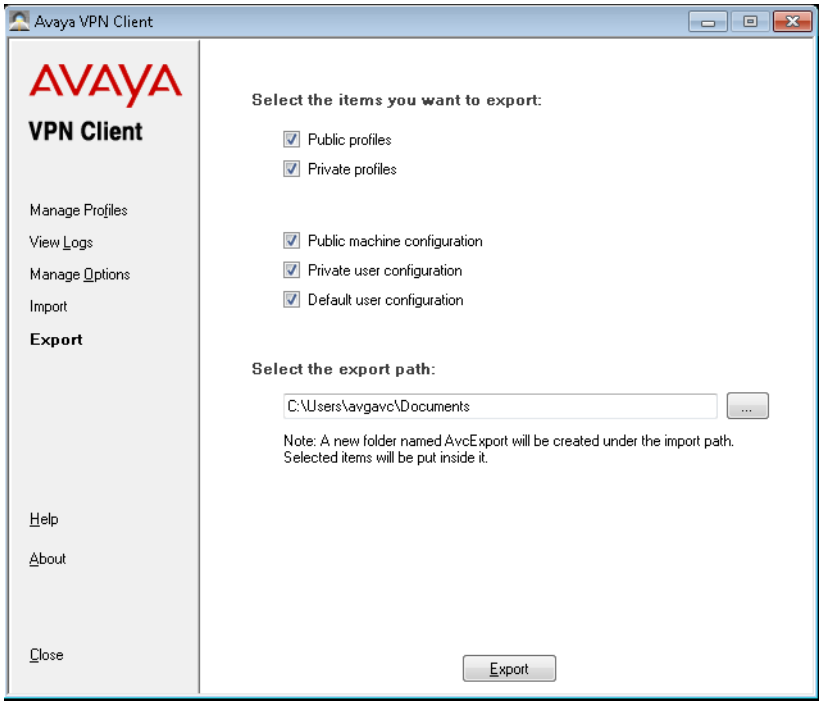
Exporting profiles or configuration files

You can export an existing profile or configuration files to your local file system. You can use this feature to create a back-up of your profile and configuration files.

Use the following procedure to export a profile or configuration file:

1 In the VPN Client navigation pane, select the **Export** option.

The Export UI is displayed.



Note: The default destination for exporting profiles and configuration files is displayed in the **Select the export path** field.

2 If you wish to export files to another destination, click the **Browse** button to navigate to that location.

By default, files will be stored in the directory <filepath>\AvcExport.

Notes:

- A user does not require administrative privileges to export global machine and user configurations and profiles.
- If there are any other users on the same Client machine that have user-defined private profiles or configurations, the export process does not access these files and does not export them.

3 Select one or more of the following profile and configuration options:

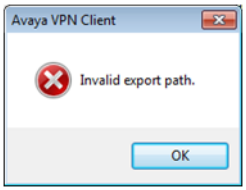
- Public profiles

- Private profiles
- Public machine configuration
- Private user configuration
- Default user configuration

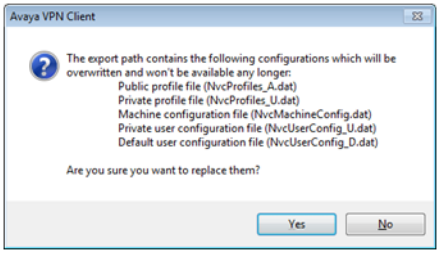
Caution: Exporting will overwrite same-named profile and configuration files present in the destination filepath.

4 Click **Export.**

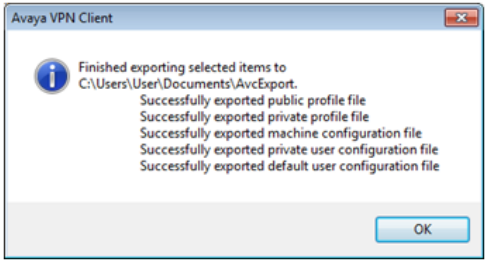
- If the import path is invalid, a message dialog is displayed, prompting you to click **OK** and correct the filepath selected in step 2.



- if the path is valid, an overwrite warning message is displayed.



5 If you wish to overwrite the files specified, click **Yes**.
A success message is displayed.

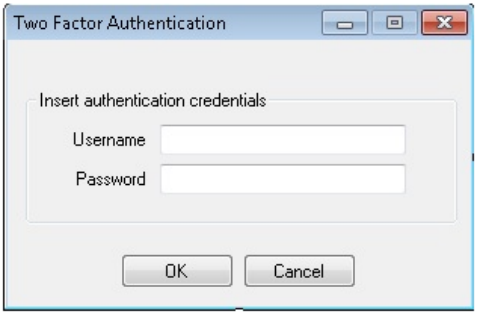


Two Factor Authentication

Beginning with Avaya VPN Client 10.06, Two Factor Authentication is provided in compliance with the security standards of the payment card industry. When the feature is enabled on the server (Avaya VPN Gateway or Avaya VPN Router), the user must provide two sets of credentials (certificate + username/password) to connect to the Avaya VPN Gateway (AVG) or Avaya VPN Router (AVR).

The user creates a certificate-based profile. The user selects this profile and clicks **Connect** to initiate a connection to the VPN.

The user is prompted with the Two Factor Authentication dialog as shown in the following image:



The user enters the secondary Username and Password and clicks **OK**.

- If valid, the VPN connection is established.
- If the credentials supplied are invalid, the server sends a failure message and closes the tunnel.

Client operations configuration

This chapter provides information about how to configure various Avaya VPN Client (AVC) operations such as configuring proxies, launching applications, managing options, importing certificates, and using the third-party API.

This chapter includes the following topics:

Configuring proxy settings

Using a proxy server adds security to the AVC, protecting it from unwanted access to the tunnel. You can configure the AVC to not use a proxy, use default settings, or create your own proxy.

Configure proxy settings for a profile, by performing the following procedure:

1. From a profile you are editing or when creating a new profile, choose **Proxy Settings** tab. The proxy setting information appears.
2. Click **Don't Use proxy** if you do not want to apply proxy settings. This the default setting.
3. Click **Use default browser's proxy settings** if you want to use your browser proxy settings.

Note: AVC collects proxy information from Internet Explorer browser only. Based on the IE browser settings, AVC retrieves proxy information through the following methods:

   a. Automatically detects proxy using Web Proxy Autodiscovery Protocol (WPAD).
   b. Automatically detects proxy using Proxy Auto Configuration (PAC) file specified in the browser.
   c. Retrieves the manually configured proxy information in the browser.

4. Click **Use defined proxy settings** when you want to configure your own. Clicking enables the field information.
   a. Type an IP address into the **Proxy address** box.
   b. Type a port number into the **Port** box.

   To exclude IP addresses from being used on the proxy server, type the IP addresses into the box. Be sure to separate the addresses from each other using semicolons.

5. Click **Save** to save the proxy settings.

Launching an application

You can automatically launch a third party application immediately before or after connecting the AVC.

- "Launching an application before connecting the AVC" on page 47
- "Launching an application after connecting the AVC" on page 47

Launching an application before connecting the AVC

Launch an application before connecting the client, by performing the following procedure.

1. From a profile you are editing or when creating a new profile, choose the **Application Launch** tab. The application launch information appears.
2. In the **Before connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box appears from your PC. Search for and click the application executive file to enter it into the **Application** box.
3. Type the command line of the application into the **Command line** box.
4. Set a tunnel delay start up time by typing between **10** and **120** (seconds) into the **Tunnel Startup Delay** box.
5. Click **Save** to save the configuration.

Launching an application after connecting the AVC

Launch an application after connecting the client, by performing the following procedure:

1. From a profile you are editing or when creating a new profile, choose the **Application Launch** tab. The application launch information appears.
2. In the **After connection** section, select the application you want to launch by clicking the **search** button beside the **Application** box. A Windows box appears from your PC. Search for and click the application executive file to enter it into the **Application** box.
3. Type the command line of the application into the **Command line** box.

4 Click **Save** to save the configuration.

Configuring dial-up

You can program the AVC to automatically use a dial-up connection when connecting the VPN tunnel to a server. You can create a new dial-up, as well as edit or delete an existing number from the Dialup menu.

Create a dialup, by performing the following procedure:

1 From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The dial up information appears.

2 In the **Dialup** section, click on the configuration button beside the **Dialup** list box. A menu appears.

3 Choose **New** from the menu. The Set up a new dial-up connection dialog box appears.

4 Click **Dialing Rules**. The Location Information dialog box appears. Enter the telephone information pertaining to your geographic area. Click **OK** to close.

5 Type the telephone number that the AVC uses to dial-up the server into the **Telephone number** box.

6 Type a name that identifies the connection into the **Destination** box.

7 If you are using a smart card, click **Use a Smart Card**.

8 If you want all users who are using this PC to use this connection, click **Allow other people to use this connection**.

9 Click **Next**. The Type your user name and password section appears.

10 Type your user name into the **User name** box.

11 Type a password into the **Password** box. You can also select **Show characters** to show the password in the box and **Remember this password** to save the password without having to reenter it again.

12 Click **Save password** to keep this password.

13 You can optionally type a domain name into the **Domain** box.

14 Click **Create** to configure the new dial-up settings.

15 Click **Save** to save the configuration.

Setting Keepalives

You set Keepalives to determine if a tunnel connection is available. Because of an issue with Microsoft Windows Vista firewall, for release 10.01 and higher, passive Keepalives for all three Keepalives profiles are sent every 15 seconds from the AVC to prevent the tunnel from being brought down by the Windows operating system.

Set the Keepalive by performing the following procedure:

1. From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The Keepalive information appears.
2. From the **Keepalive option** section, select one of the following Keepalive options to apply to the profile:
   - **No Keepalives** — disables the Keepalives.
   - **Active Keepalives (Dead peer detection)** — determines if a tunnel connection is available.
   - **Passive Keepalives (No Dead peer detection)** — maintains state information in the local internet access device.
3. Click **Save** to save the configuration.

Setting a Failover

When the Server specified in a profile cannot be reached due to various reasons. You can define a failure profile for that profile so that the client will try the failover profile whenever such a situation arises.

Set the Failover by performing the following procedure:

1. From a profile you are editing or when creating a new profile, choose the **Advanced** tab. The failover information appears.
2. From the **Failover** section, select an existing profile from the list to use as the Failover.

3 Click **Save** to save the configuration.

Setting the higher precedence VPN adapter option

The Windows operating systems prioritizes broadband network interface cards (NICs) at a higher priority than standard locally attached NICs. This prioritization supersedes the domain name system (DNS) server information assigned by the Avaya VPN Client (AVC) to the Avaya VPN NIC adapter installed on the host machine. The AVC may not be able to resolve DNS addresses, or fully qualified domain names (FQDN) correctly when used with 3G and 4G broadband adapters.

This option is available only if the registry key exists.

Set the precedence of the AVC adapters ahead of the other adaptors as described in the following sections.

- "Install time method" on page 50
- "Run time method" on page 50
- "Enable the option" on page 51

Install time method

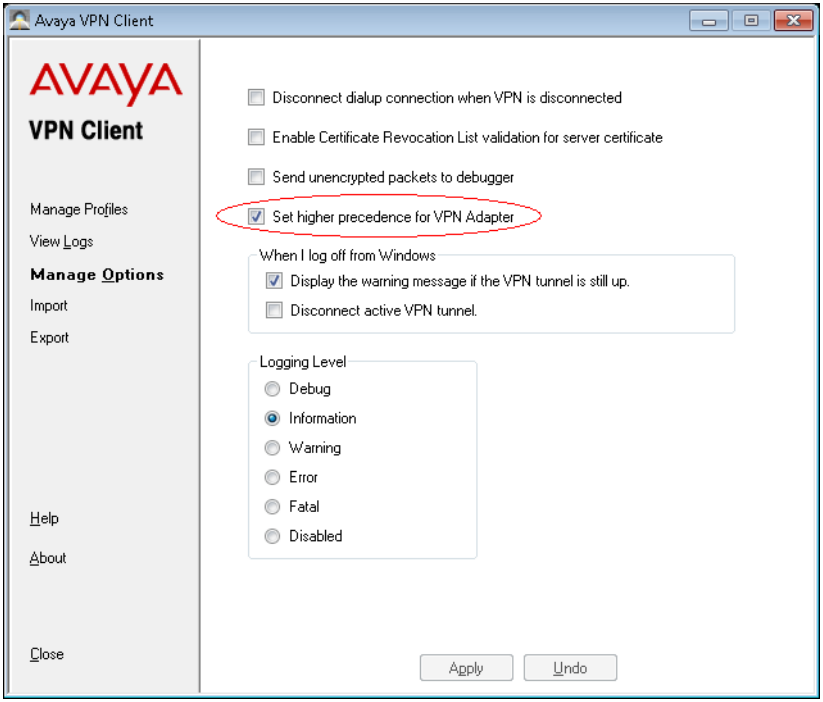
Set the custom install switch `ShowSwapAdapters` to TRUE. The ShowSwapAdapters is a custom install switch, which is used to control whether to show the run time option "Set higher precedence for VPN Adapter".

Run time method

Add a registry key value `SwapAdapters` with DWORD type under `HKLM\Software\Avaya\Avaya VPN Client`.

Enable the option

In the Manage Options pane, enable the option by selecting Set higher precedence for VPN Adaptor.



Setting AVC management options

Use the management options when setting the level of information for log files or to program responses to VPN disconnections.

Set AVC options by performing the following procedure:

1. Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

   The Avaya VPN Client window appears.

2. From the left pane, click **Edit the Profile**.

   The Manage Profiles window appears showing the General tab.

3 From the left pane, click **Manage Options.**

The Manage Options window appears.

4 Choose from the following list of options, and then click the box to enable the option:

- Disconnect dialup connection when VPN is disconnected — the AVC disconnects the dial-up connection when the VPN is disconnected. By default, the dial-up connection is left on.
- Enable Certificate Revocation List validation for server certificate — checks for certificates that have been revoked or are no longer valid.
- Send unencrypted packets to debugger — when enabled, unencrypted packets are sent to system debugger in hex format. The user can use DbgView or other tools to catch and display them. By default, this option is turned off.
- Set higher precedence for VPN adapter — when enabled, the precedence level of the VPN adapter is set higher than other 3G and 4G broadband adaptors. By default, this option is turned off. See Note.
- When I Log off from Windows — enabled by default, the Display the warning message if the VPN tunnel is still up warning message allows you the ability to log off while keeping an active connection. Selecting Disconnect active VPN tunnel removes the warning message and disconnects the tunnel when you log off of Windows.
- Logging Level — select a level to view when using the Log Viewer**.** Default level is Informational.

Note: Introduced in AVC Release 10.06, the *Set higher precedence for VPN adapter* option resolves DNS issues with third party 3G and 4G mobile broadband adaptors. For more information about this option, see "Setting the higher precedence VPN adapter option" on page 50.

Use the information in Table 1 “Logging levels” on page 53 when choosing a logging level .

Table 1 Logging levels

Logging level	Description
Debug	Shows detailed information to help you to debug a problem. Also logs positive events that mark successful milestones.
Information	Shows general type (high level) of information. Logs important and successful milestones of application execution, regardless of whether the application is working properly or not.
Warning	Shows a possible problem has occurred or can occur, but the application still functions correctly. However, it cannot continue to work properly.
Error	Shows that unexpected processing has happened. The application cannot perform a task as expected. However, the application is still up and running.
Fatal	Shows unhandled exceptions where the application has stopped working.
Disabled	The logging level is disabled. No logs are generated.

5 Click **Apply** to save the option.

Viewing log files

Use log files generated by the AVC when determining problems or monitoring the health of a connection. To set the level of a log, go to “Setting AVC management options” on page 51.

View a log file by performing the following procedure:

1 Choose **Start, All programs, Avaya VPN Client, Avaya VPN Client**.

The Avaya VPN Client window appears.

2 From the left pane, click **View Logs**. The Log information window opens.

3 If you want to export a log, click **Export** and then select a folder to save the file.

4 Click **Clear** to clear the log or **Refresh** to update the current log.

SSL tunnel with RSA hardware token

You can bring up the SSL tunnel using RSA hardware token as the authentication mechanism.

Perform the following procedure to bring up the SSL tunnel with RSA hardware token.

1 Launch AVC.
2 Click **Edit the Profile.**
3 Create SSL profile with authentication type **Predefined Login service.**
4 Name the SSL profile as **ssl_rsa_hw_token.**
5 In the **IP Address** field, specify the server IP address.
6 Click **Refresh** and select **Login service** corresponding to RSA authentication.
7 Type the username.
8 Click **Save** to save the profile.
9 Close the ***Edit the Profile*** window.
10 Select the profile ***ssl rsa hw token*** from the main window.
11 Type the passcode in the password field.
12 Click **Connect**.

Note: To get the passcode, append the token number to the pin. For example, if pin is **1234** and token is **55667788**, then passcode is **123455667788**.

Importing and obtaining digital certificates

The AVC supports retrieval of X.509v3 certificates from Microsoft Certificate storage through the Microsoft CryptoAPI (MS CAPI). Microsoft provides a Public Key Infrastructure (PKI) that adheres to the Public-Key Cryptography Standards (PKCS).

You need to import certificates into Personal store of your account. AVC lists all the certificates installed in the Personal store so that you can select a specified certificate while creating a profile.

AVC interacts only with Microsoft certificate store. The smart card vendor software copies certificates available in smart card to the Microsoft certificate store. Once the certificates are copied to Microsoft certificate store, AVC retrieves those certificates using Microsoft CryptoAPI (MS CAPI).

Server certificate validation at client machine

As part of SSL handshake between client and VPN server, VPN server sends a digital certificate to client machine. AVC validates this server certificate received at client machine. In order to validate the server certificate, AVC requires CA certificate of the server certificate under Trusted Root Certification Authority of your account. Windows operating system comes with all well known CA certificates in its MS-CAPI store.

If you try to bring up SSL tunnel through PLAP, CA certificate of server certificate must be available under Trusted Root Certification Authority of computer account.You can create certificate requests with tools that a Certification Authority (CA) supports and are integrated with MS CAPI.

If server certificate is involved in bringing up IPSec tunnels, you need to import CA certificate of server certificate under Trusted Root Certification Authority of your account. If you are trying to bring up tunnel through PLAP, CA certificate of certificate must be available under the Trusted Root Certification Authority of computer account.

Importing a CA certificate

You can import a CA certificate by performing the following procedure:

1. Choose **Start, Run**.
2. Type **mmc.exe.**
3. Press **ENTER.**
4. Choose **Add/Remove Snap-in** from the **File** menu.

The Add/Remove Snap-in window opens.

5 Click **Add.**

The Add Standalone Snap-in window appears.

6 Select **Certificates.**

7 Click **Add.**

The Certificates Snap-in window appears.

8 Select **My user account** or **Computer account.**

9 Click **Finish.**

10 Close the **Add Standalone Snap-in** window.

11 Click **OK** to close the Add/Remove Snap-in window.

12 In the **Console Root** window, right click on **Trusted Root Certification Authorities.**

13 Select **All Task, Import.**

Revocating and validating a server certificate

In the Manage options window, if the **Enable Certificate Revocation List Validation for server certificate** option is checked, then the AVC verifies the server certificate revocation status. Check the CRL database of the certificate authority to perform the server certificate verification. The locations of CRL database are available in the CRL Distribution points field of the certificate.

CRL distribution points must be reachable to the client machine before bringing up the SSL tunnel. You cannot bring up the SSL tunnel if CRL link is inaccessible or server certificate is revoked.

On the other hand, to bring up the IPSec tunnel, the CRL distribution points need to be accessible only after tunnel connection is completed. Once the IPSec tunnel is up, AVC checks the CRL status of server certificate. If AVC detects that server certificate is revoked or CRL Distribution Points are inaccessible, it tears down the tunnel.

For more information about certificate selections after they are in the MS CAPI, see "Creating an IPSec profile using Manage Profiles" on page 29 or "Creating a SSL profile using Manage Profiles" on page 36.

Viewing banners

Banners display security and notification messages. You can receive one of the following types of banner messages:

- "Security banners" on page 58
- "Avaya Endpoint Access Control Agent Notify banner" on page 58

To view a banner, click the Avaya VPN Client icon in the system tray, and choose **View Banners**.

Security banners

A security banner displays a message that is pushed from the server when a VPN tunnel is established, if the banner is configured on the server. All traffic to the server is blocked until the user acknowledges the banner. You have three options:

- Accept/Close — allows traffic to flow and the dialog box closes
- Accept — allows traffic to flow, the security banner remains visible, and all links are clickable
- Cancel — terminates the tunnel immediately

If you enable Dynamic Domain Name System (DNS) at the group level on the server, the DNS registration to the assigned DNS server occurs after you accept the security banner.

The security banner has a timeout. If you do not do anything, the connection terminates after two minutes.

Avaya Endpoint Access Control Agent Notify banner

If Avaya Endpoint Access Control Agent checking is enabled on the server, the server periodically checks for the existence of Avaya Endpoint Access Control Agent. If this check fails, the server sends a message to the AVC. The contents of the message displays in a message box.

For more information about this banner, see *Avaya VPN Router Configuration—TunnelGuard* (NN46110-307) or *Avaya VPN Gateway - Administrator Guide* (NN46120-105).

Using the third-party API

The third-party API provides you with the ability to start, monitor and stop VPN tunnels under a C/C++ program's control.

In this release you can use API on Windows XP, Windows Vista and Windows 7 through both 32-bit and 64-bit systems. The 10.01 version and higher's API is not backward compatible with earlier versions of API.

Table 2 “Third-party API files” on page 59 lists third-party API 32-bit and 64-bit files.

Table 2 Third-party API files

32-bit	64-bit	Description
NvcApi.h	NvcApi.h	Defines the functions of the .dll files
NvcApi32.lib	NvcApi64.lib	Library file
NvcApi32.dll	NvcApi64.dll	Contains the functions.

You can use the following work flow whenever you are working with a third-party API:

1. Start a VPN tunnel with NVCStart (LPWSTR commandline).
2. Monitor the tunnel by polling NVCTunnelStatus() while performing whatever other work is required.

3 Stop the VPN tunnel with NVCStop().

Use the following information in Table 3 “API functions” on page 60 found in the NvcApi.h file to help you use the third-party API.

Table 3 API functions

Function	Synopsis	Arguments	Returns
NVCStart (LPWSTR commandline)	Start a VPN tunnel using the nvc.exe client.	Long Pointer to Wide String (LPWSTR) commandline —A null-terminated string with the command line options for nvc.exe. Do not type the program name, for example, nvc.exe. Type only the command switches.	0 — Successfully started tunnel. –1 — Error starting nvc.exe. other — Error starting tunnel. Error code can be interpreted by NVCGetErrorString()
NVCStop ()	Stops the VPN tunnel.	None	–1 — AVC is not running. 0 — Success, stop command is issued.
NVCTunnelStatus ()	Returns the current status of the VPN tunnel.	None	–1 — AVC is not running. 0 — Tunnel is DOWN. 1 — Tunnel is UP.
NVCTunnelStats (NVC_TUNNELSTATS *statsBuffer)	Returns the tunnel current statistics.	statsBuffer — Points to a NVC_TUNNELSTATS structure that contains the current statistics. The GetSystemTime() is the UTC time when the system collects statistics. The total items are total numbers of bytes and errors the VPN driver processes from the VPN start time. (total for all tunnels). The conn items are the totals for the latest tunnel connection. These items are mirrored in the Avaya VPN Client monitor.	0 — Success other — A Microsoft Window's RPC_STATUS code.
NVCGetErrorString (int errorCode | LPWSTR errorString | DWORD len)	Converts an error code returned by NVCStart() to a readable string.	int errorCode — The error code returned by NVCStart(). LPWSTR errorString— A character buffer where the error string is written upon successful completion of this call. DWORD len — The length, in bytes, of the errorString buffer.	Positive value — Success with string length. 0 — String not available.

Client control—Command line

This chapter tells you how to configure and control the Avaya VPN Client (AVC) using DOS command lines instead of using the AVC GUI. You can create a profile, start and stop the AVC, as well as retrieving Help and banner information.

This chapter includes the following topics:

Starting a tunnel without a profile

You can configure IPsec and SSL tunnels without profiles when you want to create a tunnel to connect to a VPN server.

To configure an IPSec tunnel without a profile, enter the following command:

```
nvc.exe {-ipsec} {-auth <authentication type>} {-serverip <server
ip>} {-user <username>} [-pwd <password>] [-pwd2 <password2>] [-gid
<gid>] [-gpwd <group password>] [-pin <PIN>] [-code <tokenCode>]
[-altname <subj-alt-name>] [-alttype <number>] [-s] [-fs]
[-hidetrayicon]
```

Use the information in Table 1 “Parameters for a tunnel without a profile” on page 62 to configure an IPSec tunnel.

To configure a SSL tunnel without a profile, enter the following command:

```
nvc.exe {-ssl} {-auth <authentication type>} {serverip <server ip>}
{-serverport <server port>} [-proxyip <proxy ip>] [-proxyport
<proxy port>] [-usebrowserproxy] [-loginservice <loginservice
name>] {-user <username>} [-pwd <password>] [-pwd2 <password2>]
[-pin <PIN>] [-code <tokenCode>] [-altname <subj-alt-name>]
[-alttype <number>] [-s] [-fs] [-hidetrayicon]
```

Use the information in Table 1 “Parameters for a tunnel without a profile” on page 62 to configure a SSL tunnel.

Table 1 Parameters for a tunnel without a profile

Switch	Value	Description
–ipsec –ssl	none	Optionally selects the tunnel type. If either type is not stated, IPSec is the default.
-profile -userProfile	Profile name	Specifies an optional preconfigured profile to use. –profile indicates a public profile to load. –userProfile indicates a private or user profile to load.
-auth	0 or userpass	Public or private logon
	1 or challenge	Challenge or response token card.
	2 or securid	SecurId hardware token.
	3 or grouppass	Simple group ID, password with username, or password.

Table 1 Parameters for a tunnel without a profile

Switch	Value	Description
	4 or challengeswtoken	Challenge or response software token.
	5 or softid	SecurID software token.
	6 or loginservice	Login Service name for SSL tunnel
	9 or mscapi	MSCAPI certificate.
	10 or profile	Authentication type comes from the specified profile.
–serverip	Server name or IP address.	Server name or IP address.
–serverport	Server port for ssl connection	Server port number for the SSL tunnel.
–proxyip	Proxy IP address	Proxy IP address.
–proxyport	Proxy port	Port number of the proxy server.
–usebrowserproxy	None	Collects proxy information from the browser.
–loginservice	Login service name	Login service name for SSL tunnel.
–user	User name	Username supplied by an administrator.
–pwd	Password	Password supplied by an administrator.
–pwd2	Password2	Second password for SSL tunnel.
–gid	Group ID	Group ID supplied by an administrator.
–gpwd	Group password	Group password supplied by an administrator.
–pin	PIN	PIN supplied by an administrator when you use Response Only Hardware Token or Response Only Software Token.
–code	Token code	SecurID uses the token code.
–altname	Certificate — alternate name	An alternate name of the certificate.
–alttype	Certificate — alternate type	Alternate type of the certificate.
–s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
–fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If –s and –fs occurs together, then –fs overrides –s.
–hidetrayicon	None	Hides the system tray.

Starting a tunnel with a profile

You can configure IPSec and SSL tunnels with a profile when you want to create a tunnel to connect to a VPN server. Parameters required for the tunnel creation are collected from the profile name specified in the command line switch. At the same time, you have the option to override parameters available in the profile by using command line switches. You cannot override the tunnel type and authentication type in profile based tunnels.

To configure a tunnel with a profile, enter the following command:

```
nvc.exe {-profile <profile name> | -userprofile <profile name>}
{-auth <authentication type>} [-serverip <server ip>] [-user
<username>] [-pwd <password>] [-pwd2 <password2>] [-gid <gid>]
[-gpwd <group password>] [-pin <PIN>] [-code <tokenCode>] [-altname
<subj-alt-name>] [-alttype <number>] [-s] [-fs] [-hidetrayicon]
```

Use the information in Table 2 “Parameters for a tunnel with a profile” on page 64 to tunnel with a profile.

Table 2 Parameters for a tunnel with a profile

Switch	Value	Description
–profile –userProfile	Profile name	Specifies an optional pre-configured profile to use. –profile indicates a public profile to load. –userProfile indicates a private or user profile to load.
–auth	0 or userpass	Public, private logon.
	1 or challenge	Challenge or response token card.
	2 or securid	SecurId hardware token.
	3 or grouppass	Simple group ID, password with username, password.
	4 or challengeswtoken	Challenge or response software token.
	5 or softid	SecurID software token.
	6 or loginservice	Login Service name for SSL tunnel.
	9 or mscapi	MSCAPI certificate.
	10 or profile	Authentication type comes from the specified profile.
–serverip	Server name or IP address.	Server name or IP address.
–user	User name	Username supplied by an administrator.

Table 2 Parameters for a tunnel with a profile

Switch	Value	Description
–pwd	Password	Password supplied by an administrator.
–pwd2	Password2	Second password for SSL tunnel.
–gid	Group ID	Group ID supplied by an administrator.
–gpwd	Group password	Group password supplied by an administrator.
–pin	PIN	PIN supplied by an administrator when you use Response Only Hardware Token or Response Only Software Token.
–code	Token code	SecurID uses the token code.
–altname	Certificate — alternate name	An alternate name of the certificate.
–alttype	Certificate — alternate type	Alternate type of the certificate.
–s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
–fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If –s and –fs occurs together, then –fs overrides –s.
–hidetrayicon	None	Hides the system tray.

Stopping a tunnel

You use the stop tunnel command to disconnect the current tunnel.

To stop a tunnel, use the following command:

```
nvc.exe {-t|-terminate}
```

Use the information in Table 3 “Tunnel parameter for termination” on page 66 to terminate the tunnel.

Table 3 Tunnel parameter for termination

Switch	Value	Description
–terminate –t	None	Terminate current tunnel.

Launching the AVC GUI

You can use the command line to launch the AVC GUI as well as to launch it with a specific profile.

To launch the AVC GUI, enter the following command:

```
nvc.exe
```

To launch the AVC GUI with a profile, enter the following command:

```
nvc.exe {-userprofile <profile name> |-profile <profile name>} [-s]
[-fs] [-hidetrayicon]
```

Use the information in Table 4 “Parameters for launching the AVC GUI” on page 67 to launch the AVC GUI.

Table 4 Parameters for launching the AVC GUI

Switch	Value	Description
–profile –userProfile	Profile name	Specifies an optional preconfigured profile to use. –profile indicates a public profile to load. –userProfile indicates a private or user profile to load.
–s	None	Run in full silent mode, where all popups are suppressed, including the error messages,
–fs	None	Run in full silent mode, where all popups are suppressed, including the error messages, as well as displaying the banner. If –s and –fs occurs together, then –fs overrides –s.
–hidetrayicon	None	Hides the system tray.

Determining tunnel status

Use the tunnel status command whenever you need to view statistics about the state of the tunnel that you are currently using.

To determine the state of a tunnel status, enter the following command:

```
nvc.exe {-status}[-details][-stats]
```

Use the information in Table 5 “Tunnel parameters to determine status” on page 68 to determine the status of the tunnel.

Table 5 Tunnel parameters to determine status

Switch	Value	Description
–status	None	Gives the current tunnel status — Active or No Tunnel found
–details	None	Lists the following details about the tunnel: • Security — type of encryption and hash • IKE — version of Diffie-Helen group • Compression — type of compression • Destination IP Address • Assigned IP Address • IPsec NAT Traversal — active or inactive • Logging — level of logging or disabled • Mobility — enabled or disabled • Persistence— enabled or disabled • FIPS 140-2 Mode — type of mode or disabled • Keepalive Interval — milliseconds of wait time before sending keepalive packets • Maximum retransmissions — milliseconds of time between retransmisssions of Keepalives after the keepalive wait time expires
–stats	None	Lists the following tunnel statistics: • Tunnel active — active or no tunnel found • Duration — time the tunnel has been active • Bytes in — number of bytes entering in to the AVC • Frames in — number of frames entering in to the AVC • Bytes out — number of bytes going out of the AVC • Frames out — number of frame going out of the AVCt • Errors — number of errors.

Retrieving the tunnel banner

View the tunnel banner on the tunnel.

To retrieve the tunnel banner, enter the following command:

```
nvc.exe {-banner}
```

Use the information in Table 6 “Tunnel parameter for banner” on page 69 to retrieve the tunnel banner.

Table 6 Tunnel parameter for banner

Switch	Value	Description
–banner		Retrieves tunnel banner.

Retrieving command line help information

Use the retrieve command line help information command whenever you need to access the help.

To retrieve command line help information, enter the following command:

```
nvc.exe {-h|-help}
```

Use the information in Table 7 “Tunnel parameter for retrieving command line help information” on page 69 to retrieve command line help information.

Table 7 Tunnel parameter for retrieving command line help information

Switch	Value	Description
–h –help		Retrieves the command line help information.

Retrieving AVC version information

You need to know the current version of the AVC whenever you are upgrading to avoid possible software conflicts.

To retrieve the current AVC version information, enter the following command:

```
nvc.exe {-v|-version}
```

Use the information in Table 8 “Tunnel parameter for retrieving current AVC version information” on page 70 to retrieve the current AVC version.

Table 8 Tunnel parameter for retrieving current AVC version information

Switch	Value	Description
–version		Retrieves the client version information