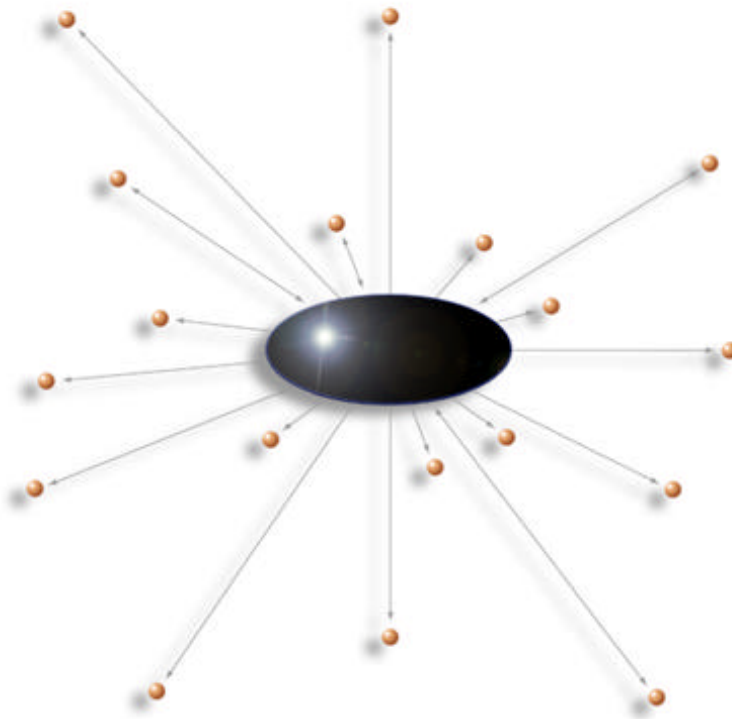




---

v3.01/v2.51



---

User's Guide  
Windows



# **AVENTAIL CONNECT 3.01/2.51 USER'S GUIDE**

© 1996-1999 Aventail Corporation. All rights reserved.

808 Howell Street, Second Floor  
Seattle, WA 98101  
USA

<http://www.aventail.com/>

Printed in the United States of America.

## **TRADEMARKS AND COPYRIGHTS**

Aventail is a registered trademark of Aventail Corporation. AutoSOCKS, Internet Policy Manager, Aventail VPN, Aventail VPN Client, Aventail ExtraNet Center, and Aventail ExtraNet Server are trademarks of Aventail Corporation.

Socks5Toolkit is a trademark of NEC Corporation. MD4 Message-Digest Algorithm and MD5 Message-Digest Algorithm are trademarks of RSA Data Security, Inc. Microsoft, MS, Windows, Windows 95, Windows 98, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation. RealAudio is a trademark of RealNetworks. SecurID, SoftID, ACE/Server, and SDTI are either registered trademarks or trademarks of Security Dynamics Technologies, Inc.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

© 1995-1996 NEC Corporation. All rights reserved.

© 1990-1992 RSA Data Security, Inc. All rights reserved.

© 1996 Hi/fn Inc., including one or more U.S. patents: 4701745, 5016009, 5126739, and 5146221, and other patents pending.

© 1996-1997 Consensus Development Corporation. All rights reserved.

# Table of Contents

Trademarks and Copyrights .....	i
<b>INTRODUCTION</b>	
About This Document .....	3
Document Organization .....	3
Document Conventions .....	4
Aventail Technical Support .....	5
About Aventail Corporation .....	5
<b>USER'S GUIDE</b>	
Start and Close Aventail Connect .....	6
Enter Authentication Credentials .....	8
Username/Password and CHAP Authentication .....	9
CRAM Authentication .....	10
Integration with SoftID .....	10
SSL Authentication .....	11
System Menu Commands .....	13
Close .....	13
Hide Icon .....	14
Help .....	14
About .....	14
Credentials .....	14
Configuration File .....	16
Utilities .....	17
Config Tool .....	17
Logging Tool .....	18
S5 Ping .....	19
Secure Extranet Explorer .....	20
<b>GLOSSARY</b> .....	22
<b>INDEX</b> .....	26

## Introduction

Welcome to the Aventail Connect 3.01/2.51 secure Windows client for 16- and 32-bit Windows applications. The client component of the Aventail ExtraNet Center, Aventail Connect is a secure proxy client based on SOCKS 5, the IETF standard for authenticated firewall traversal. Aventail Connect delivers enhanced security and simplifies SOCKS deployment for users and network managers.

Aventail Connect redirects WinSock calls and reroutes them based upon a set of routing directives (rules) assigned when Aventail Connect is configured. Aventail Connect is designed to run transparently in the background as you work in any TCP/IP applications. (For more information about WinSock, TCP/IP, and general network communications, see "Getting Started.")

On larger networks, Aventail Connect can address multiple SOCKS v5 servers based on end destination and type of service. This feature enables network administrators to effectively monitor and direct network traffic.

Aventail Connect is a proxy client, but when used with SSL it provides the ability to encrypt inbound or outbound information.

Features of Aventail Connect:

- Aventail Connect supports X.509 client certificates for strong authentication with SSL (when encryption is enabled)
- Automated Customizer utility simplifies client configuration, distribution, and installation
- SSL compression detects low bandwidth connections and compresses encrypted data (when encryption is enabled)
- Secure Extranet Explorer (via **Extranet Neighborhood** icon on desktop) allows users to securely access Windows or SMB hosts over an extranet connection (Windows 95, Windows 98, and Windows NT 4.0 only)
- Supports WinSock 2.0 (LSP) applications in Windows 98, and Windows NT 4.0, and WinSock 1.1 and WinSock 2.0 applications in Windows 95
- Supports WinSock 1.1 applications in Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51
- MultiProxy feature allows you to use a SOCKS server or an HTTP proxy to control outbound access
- Allows the use of port ranges for redirection rules
- Provides integration with SoftID™ and SecurID™ tokens
- Provides automated installation and uninstallation
- Credential cache timeout feature allows administrators to specify when credentials expire
- Provides optional password protection for configuration files
- Supports both SOCKS v4 and SOCKS v5 (RFC 1928 and RFC 1929) standards

- Enables network redirection through successive extranet (SOCKS) servers
- Includes a logging utility to troubleshoot problems with network connections
- Includes a Configuration wizard for simplified step-by-step creation of configuration files
- Allows internal network connections to pass through without interference
- Supports multiple authentication methods including SOCKS v4 identification, username/password, CHAP, CRAM, HTTP Basic (username/password), and SSL 3.0



**SEE ALSO:** *For more information on the differences between Aventail Connect 3.01 and Aventail Connect 2.51, see “What Does Aventail Connect Do?” in the Administrator’s Guide.*



**NOTE:** *Not all versions of Aventail Connect have encryption enabled. For more information, see your network administrator.*

## ABOUT THIS DOCUMENT

This *User's Guide* provides basic information about Aventail Connect. It includes entry-level data for end users. This information is also available via Aventail Connect Help and the Aventail Web site at <http://www.aventail.com/content/products/docs/>.

## DOCUMENT ORGANIZATION

This document is divided into two main sections: *User's Guide* and *Utilities Reference Guide*.

The *User's Guide* describes screen displays and features that users may encounter while running Aventail Connect on their client workstations.

The *Utilities Reference Guide* describes the Aventail Connect system menu commands and utility programs. It contains detailed information about using the S5 Ping and the Logging Tool utilities, and Extranet Neighborhood/Secure Extranet Explorer (SEE).

The document concludes with the *Glossary*.

## DOCUMENT CONVENTIONS

The following typographic conventions are used in this document. Exceptions may be made for online material; for instance, italics may be difficult to read online.

Convention	Usage
Courier font	Filenames, extensions, directory names, keynames, and pathnames. Command-line commands, options, and portions of syntax that must be typed exactly as shown.
<b>Bold</b>	Dialog box controls ( <b>Edit...</b> buttons), e-mail addresses ( <b>support@aventail.com</b> ), URLs, ( <b>www.aventail.com</b> ), and IP addresses ( <b>165.121.6.26</b> ).
<i>Italic</i>	Placeholders that represent information the user must insert.



**SEE ALSO:** *A reference to additional useful information.*



**NOTE:** *Information the user should be aware of to increase understanding and/or efficiency of the software.*



**CAUTION:** *An operational item that the user should be aware of to avoid a network policy/software conflict, or lapse, which may create a MINOR security flaw.*



**WARNING:** *An operational item that the user should be aware of to avoid a network policy/software conflict, or lapse, which may create a SERIOUS security flaw.*

## AVENTAIL TECHNICAL SUPPORT

Contact Aventail Technical Support if you have questions about installation, configuration, or general usage of Aventail Connect. Refer to the Aventail Support Web site, at [http://www.aventail.com/index.phtml/support/online\\_support.phtml](http://www.aventail.com/index.phtml/support/online_support.phtml), or the Aventail Knowledge Base, at [http://www.aventail.com/index.phtml?page\\_id=03110000](http://www.aventail.com/index.phtml?page_id=03110000), for the latest technical notes and information. Refer to the `readme.txt` documentation for additional information not included in the *User's Guide*.

Aventail Technical Support:

Web site: <http://www.aventail.com/index.phtml/support/index.phtml>

E-mail: [support@aventail.com](mailto:support@aventail.com)

Phone: 206.215.0078

Fax: 206.215.1120

## ABOUT AVENTAIL CORPORATION

Aventail Corporation is the leading vendor of extranet software. Its extranet solutions allow organizations to secure their networked communications and manage their employees' access to the Internet. Building an extranet gives organizations the ability to dynamically create a private communication or data channel over the Internet. Aventail's adherence to open security standards simplifies extranet deployment, enables interoperability, and leverages corporations' existing network investments. Its extranet solutions allow companies to extend the reach of their corporate extranets to customers, partners, remote offices, and worldwide employees.

Aventail Corporation  
808 Howell Street, Second Floor  
Seattle, WA 98101  
Phone: 206.215.1111  
Fax: 206.215.1120  
<http://www.aventail.com/>  
[info@aventail.com](mailto:info@aventail.com)



An aventail is a piece of chainmail armor worn around the neck area. In the 14<sup>th</sup> century, knights wore an aventail to protect themselves while in combat. Today, Aventail continues the tradition of protection by allowing organizations to securely communicate over the Internet.



## User's Guide

For outbound traffic, Aventail Connect automatically routes appropriate network traffic from a WinSock-compatible TCP/IP application such as an e-mail program or a Web browser to a SOCKS-based server. (WinSock is a Windows TCP/IP interface that connects a Windows PC to the Internet.) The extranet (SOCKS) server then sends the traffic to the Internet or the network. Your network administrator defines routing rules for this traffic.

This *User's Guide* is designed to familiarize you with aspects of the Aventail Connect interface. Because Aventail Connect is designed to run transparently in the background, in most cases you will interact with Aventail Connect only when it prompts you to enter authentication information for connections to resources secured by an Aventail ExtraNet Server. You may also occasionally need to start and close Aventail Connect, although network administrators often configure it to run automatically at startup.

If you have questions about how Aventail Connect is running on your system, contact your network administrator. Details about other Aventail Connect commands and utilities are described in the *Administrator's Guide*. You might find the "Getting Started" section helpful.

## START AND CLOSE AVENTAIL CONNECT

Because network administrators often set up Aventail Connect to run minimized at startup, you may never need to actually launch the Aventail Connect application. When Aventail Connect starts, it loads a default configuration file. This file contains the rules Aventail Connect uses to properly route network traffic to and from your individual workstation.

Aventail Connect may prompt you at startup to select a configuration file. If you are unsure of which configuration file to use, contact your network administrator.

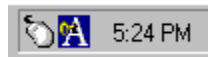
Closing Aventail Connect may limit access to certain remote hosts or prevent you from using certain WinSock applications. Before closing Aventail Connect, check with your network administrator.

### To start Aventail Connect

- Windows 95, Windows 98, and Windows NT 4.0: Select **Start | Programs | Aventail Connect | Aventail Connect**.

-OR-

- Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51: In the Aventail Connect program group, double-click the **Aventail Connect** program icon.



You will see a minimized **Aventail Connect** icon indicating that Aventail Connect is running in the background. In Windows 95, Windows 98, and Windows NT 4.0, this icon is located in the system tray on the taskbar.

#### To close Aventail Connect

---

- Windows 95, Windows 98, and Windows NT 4.0: In the system tray on the taskbar, right-click the minimized **Aventail Connect** icon to display the Aventail System menu, and click **Close**.



-OR-

- Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51: Click the minimized **Aventail Connect** icon to display the Windows System menu, and click **Close**.



**NOTE:** The availability of the **Help**, **Credentials**, **Configuration File**, **Config Tool**, **Logging Tool**, and **S5 Ping** commands depends on whether or not your network has included them in your Aventail Connect installation package. For more information, refer to "System Menu Commands" and "Utilities."

## ENTER AUTHENTICATION CREDENTIALS

Most extranet (SOCKS) servers require you to enter authentication credentials before you are granted access to them. If you try to connect to resources through a secure extranet server, Aventail Connect may display a dialog box asking you to enter authentication credentials. (For some types of authentication methods, your input is not required.) Credentials can be as simple as your username or password, or as elaborate as a client certificate plus username and password. Your network administrator assigns credentials to users.



**NOTE:** *Not all versions of Aventail Connect have encryption enabled. For more information, contact your network administrator.*

Aventail Connect supports the following authentication protocols:

- Username/Password
- Challenge Handshake Authentication Protocol (CHAP)
- Challenge Response Authentication Method (CRAM)
- Secure Sockets Layer (SSL)
- SOCKS 4 Identification
- HTTP Basic (username/password)

Aventail Connect also supports X.509 client certificates with SSL.



**SEE ALSO:** *To read more about these protocols, see "Manage Authentication Modules" in the Administrator's Guide.*

Once you enter your credentials, Aventail Connect will save them in memory. This is known as *memory caching*. Memory caching stores the credentials for the current session only. When you restart Aventail Connect or Windows, the memory cache is flushed. If you reconnect to a resource requiring access through an extranet server, you must again enter your credentials as prompted.

The following section explains how to authenticate using these modules: Username/Password, CHAP, CRAM, SSL authentication, and client certificates. SOCKS v4 identification does not require user interaction and therefore is not covered in this guide.

## USERNAME/PASSWORD AND CHAP AUTHENTICATION

Username/Password and CHAP authentication use similar dialog boxes.

### To enter authentication credentials

If the secure extranet server to which you are connecting uses Username/Password or CHAP authentication, you will see a dialog box similar to the following:



**NOTE:** If you do not know what to enter in the dialog box fields, check with your network administrator.

1. In the **Username** box, type your username.  
Press the **TAB** key to move to the next field, or click in the **Password** box to place the insertion point. Be sure to type your username and password accurately.
2. In the **Password** box, type your password.  
Your password is concealed as you type it; it displays on-screen as a series of asterisk (\*) characters.
3. Under "Credential Caching," use the default option, **Cache for this session**. Click **OK**.

When you click **OK**, your credentials are sent to the secure extranet server and if they are accepted, the connection will continue.

If your credentials are refused by the server, the application will display an alert stating that the connection could not be established. Try the transaction again, reentering your username/password. If problems persist, contact your network administrator.

## CRAM AUTHENTICATION

In Aventail Connect, the CRAM authentication module is used to support challenge response authentication systems such as SecurID and other token-based authentication systems. The SecurID system uses a two-part process comprised of a user's Personal Identification Number (PIN) and a token that generates a time-based code. This client code mirrors the Pseudo Random Number (PRN), which typically changes each minute, generated by the server.

There are several ways to use the PIN-token process. The specific method you use will be determined by your network administrator.

Subauthenticated through SSL, SecurID's CRAM provides an additional layer of security, plus session resumption capabilities to mobile/remote users.



**NOTE:** *Without SSL subauthentication, users will be required to log on every time they need to access the corporate intranet, extranet, or Internet.*

## INTEGRATION WITH SOFTID

In addition to the Security Dynamics SecurID tokens, Aventail Connect supports the Security Dynamics SoftID token system. SoftID is similar to SecurID, except that SecurID uses a hand-held token while SoftID uses a "virtual" token that you view on-screen. When authenticating with SecurID, a physical token displays the six-digit Pseudo Random Number (PRN). When authenticating with SoftID, the PRN appears in the on-screen token. With both the SecurID and SoftID tokens, the PRN typically changes each minute. You can install multiple SoftID tokens, although typically you will have just one.

The following platforms support SoftID:

- Windows 98
- Windows NT 4.0
- Windows 95 (See note below)



**NOTE:** *When running Aventail Connect 2.51 on the Windows 95 operating system, SoftID is compatible with 32-bit applications only. When running Aventail Connect 3.01 on Windows 95, SoftID is compatible with both 16- and 32-bit applications.*

SoftID is not supported by Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51.

For Aventail Connect to integrate with SoftID on the Windows 95 and Windows 98 operating systems, you must install a Security Dynamics patch. This patch consists of three files: `stauto.dll`, `stauto16.dll`, and `stauto.dll`. You can download the patch from:

**<http://www.securid.com/products/datasheets/sofidata.html>.**

With SoftID integration, the Aventail Connect CRAM module can automatically “read” the PRN from the on-screen SoftID token, eliminating the need for you to manually enter the PRN. Aventail Connect determines whether or not you are running SoftID on your computer. If you are authenticating with CRAM and Aventail Connect determines that you are running SoftID, Aventail Connect will display a dialog box asking if you want to use the SoftID token to authenticate. (If you have multiple SoftID tokens on your computer, the Aventail Connect CRAM module will prompt you to specify which token you want to use.) If you choose to authenticate with SoftID, Aventail Connect will “read” the six-digit PRN and automatically enter it for you; however, you must still manually enter your four-digit PIN. If you choose not to authenticate with SoftID, you will be prompted to enter the six-digit PRN that is visible on your SecurID token.

The Aventail Connect CRAM module will store your username and the serial number of your SoftID token in the credential cache, eliminating the need for you to enter this information every time you authenticate with SoftID.

If you authenticate with SoftID, you can also use a password for added security, if desired. If you choose to protect your token with an optional password, you must enter the correct password before the SoftID user interface is displayed; the password “unlocks” the SoftID user interface so you can view the SoftID token on-screen.

## SSL AUTHENTICATION

SSL authentication, originally developed by Netscape for secure Web communications, uses *authentication certificates* to identify authorized users. A certificate is essentially an electronic “statement” that verifies the integrity of a connection. When you attempt to connect to an SSL server, Aventail Connect may display the SSL certificate sent by the server.

This may not always be the case, depending on how your network administrator has configured the system.



**SEE ALSO:** *For more information on authentication or SSL certificates, contact your network administrator, or go to <http://www.aventail.com>.*

### To accept an SSL certificate

---

Because anyone can issue a certificate that says anything, accept certificates only from trusted sources. Otherwise, the information you receive may be invalidated. If you have any concerns about whether or not to accept a certificate, talk with your network administrator.

1. When you see a trusted certificate display on-screen, click **Accept**.

If you click **Reject**, your connection will not be established. If you click **Next**, you see a second “page” of the certificate data with the same **Accept** and **Reject** commands.

If you click **Accept**, the certificate is accepted as valid and Aventail Connect may display a **Username/Password** dialog box for you to fill in. The Username/Password dialog will only display if sub-authentication is being negotiated. With SSL authentication, the network administrator has the additional option of requiring you to perform a second (sub) level of authentication.



2. In the **Username** box, type your username.

Press the **TAB** key to move to the next field, or click in the **Password** box to place the insertion point. Be sure to type your username and password accurately.

3. In the **Password** box, type your password.

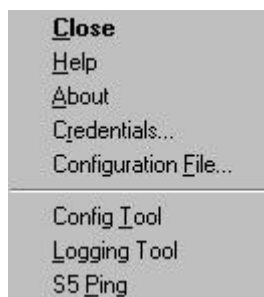
Your password is concealed as you type it; it displays on-screen as a series of asterisk (\*) characters.

4. Under "Credential Caching," use the default option, **Cache for this session**. Click **OK**.

When you click **OK**, your credentials are sent to the secure extranet server and if they are accepted, you will continue your processing without hindrance.

## SYSTEM MENU COMMANDS

Even though Aventail Connect requires little to no interaction with the user, there are commands on the Aventail Connect System menu. To display the System menu, right-click the **Aventail Connect** icon in the system tray on the taskbar (Windows 95, Windows 98, and Windows NT 4.0) or click the minimized **Aventail Connect** icon (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).



### Aventail Connect System Menu Commands

Menu Command	Function
Close	Closes Aventail Connect.
Hide Icon	Hides the <b>Aventail Connect</b> icon from view. Not available in Windows 95, Windows 98, and Windows NT 4.0.
Help	Accesses Help.
About	Displays Aventail Connect <b>About</b> box.
Credentials	Displays authentication credentials.
Configuration File	Selects a new configuration file via <b>Startup Options</b> dialog box.

Each of the commands is discussed below.



**NOTE:** Not all installations of Aventail Connect include the optional **Hide Icon**, **Help**, **Credentials**, and **Configuration File** commands. These components are available only when network administrators include them in a custom setup package. For more information, contact your network administrator.

## CLOSE

This command closes Aventail Connect. Exiting Aventail Connect may limit access to certain remote hosts or prevent you from using certain WinSock applications.



## HIDE ICON

This command hides the **Aventail Connect** icon from view (Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51 only). Aventail Connect will run in the background. *The **Hide Icon** command is not available in Windows 95, Windows 98, and Windows NT 4.0.*

## HELP

This command accesses Aventail Connect Help.

## ABOUT

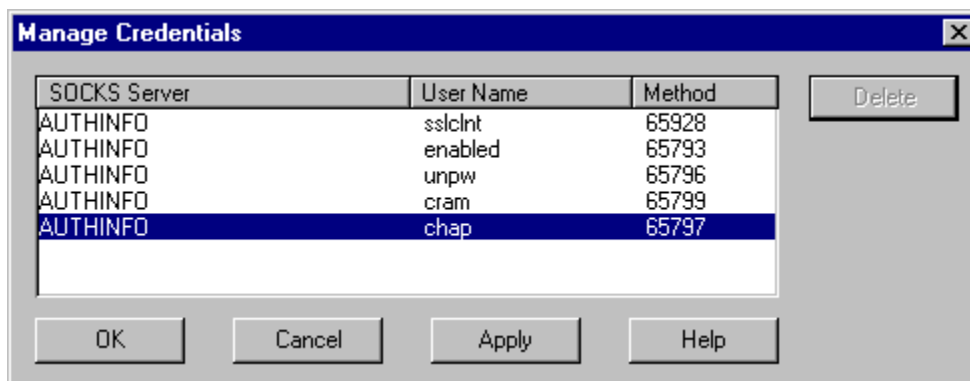
This command displays the Aventail Connect **About** box, which includes Aventail Connect software copyright notification, version information, and so on. Clicking **More** displays a list of files used by the current version of Aventail Connect.

## CREDENTIALS

This command displays the **Manage Credentials** dialog box. The availability of the **Credentials** command depends on whether or not your network administrator has included it in your Aventail Connect installation package.

Credentials include the information (such as username/password) that you enter when establishing a connection to an extranet (SOCKS) server requiring user authentication. (Aventail Connect prompts you with an authentication dialog box.) As long as your credentials are in memory, you can establish connections to associated extranet servers without needing to reenter your authentication information.

You cannot edit credential data fields; you can, however, delete individual credential entries. Aventail Connect will prompt you to enter updated authentication information when you reestablish a connection to the associated extranet server.





**NOTE:** You cannot edit the “AUTHINFO” entries in the **Manage Credentials** dialog box. This information is for diagnostic purposes only.

Field	Definition
SOCKS Server	Extranet (SOCKS) server name.
User Name	User name for the extranet server.
Method	Authentication method.

#### To delete a credential entry

Delete authentication credentials when they are no longer correct. After the credentials are deleted, you will be prompted to reenter them the next time you connect to the associated extranet server.

- Select the credential entry you want to delete and click **Delete**.

This deletes the credential information.

#### To exit the Manage Credentials dialog box

- Click **OK** to accept changes to the credentials and close the dialog box.

-OR-

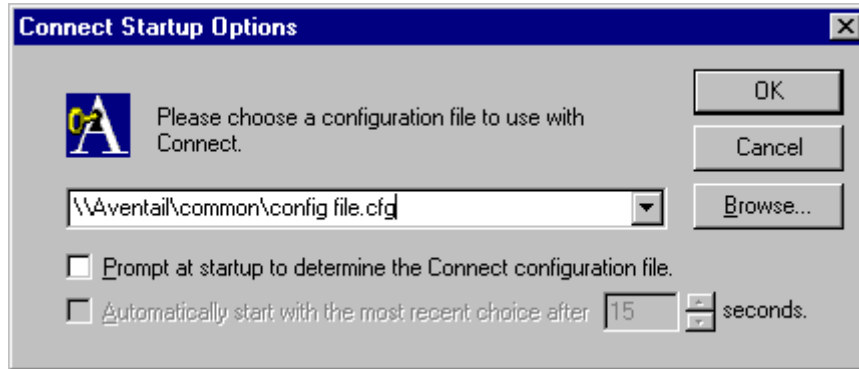
- Click **Cancel** to close the dialog box without accepting any changes you might have entered.



**NOTE:** Clicking **Apply** saves changes but keeps the dialog box open so you can keep working.

## CONFIGURATION FILE

This command lets you load a different configuration file via the **Aventail Connect Startup Options** dialog box.



### To load a configuration file

Check with your network administrator before making any changes to the configuration.

- Select the configuration file you want to load (use the **Browse** button), and then click **OK**.
- If you want Aventail Connect to start automatically with your most recent choice of configuration file, select the **Automatically start...** check box, and then select the start delay (in seconds).

The new configuration file transparently loads into Aventail Connect. You can close and restart Aventail Connect for your change to take effect, or wait the specified length of time if you selected the **Automatically start...** check box.

## UTILITIES

To display the Utility Programs menu, right-click the **Aventail Connect** icon in the system tray on the taskbar (Windows 95, Windows 98, or Windows NT 4.0) or click the minimized **Aventail Connect** icon (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).

### Aventail Connect Utility Program Menu Commands.

Menu Command	Function
Config Tool	Runs the Config Tool. (Optional)
Logging Tool	Runs the Logging Tool. (Optional)
S5 Ping	Runs the ping and traceroute utilities. (Optional)

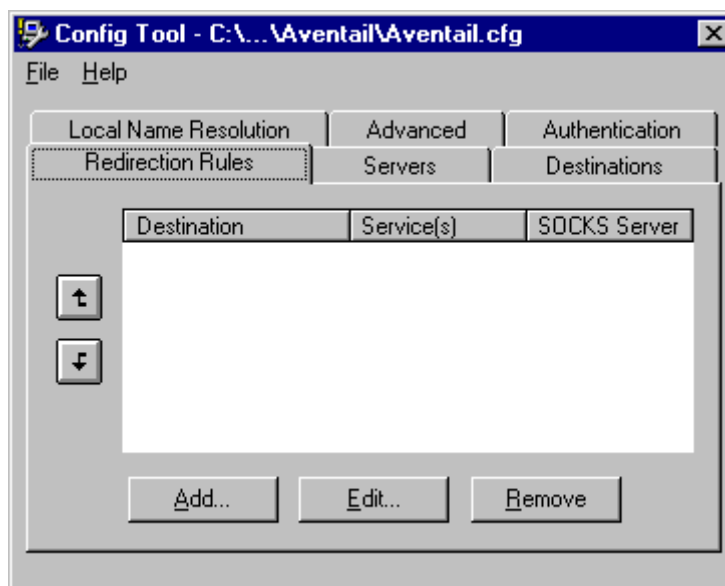
Each of the commands is discussed below.



**NOTE:** The **Config Tool**, **Logging Tool**, and **S5 Ping** commands are optional components and will only appear when the network administrator has included them in an installation package. These commands are discussed in detail in the *Administrator's Guide*.

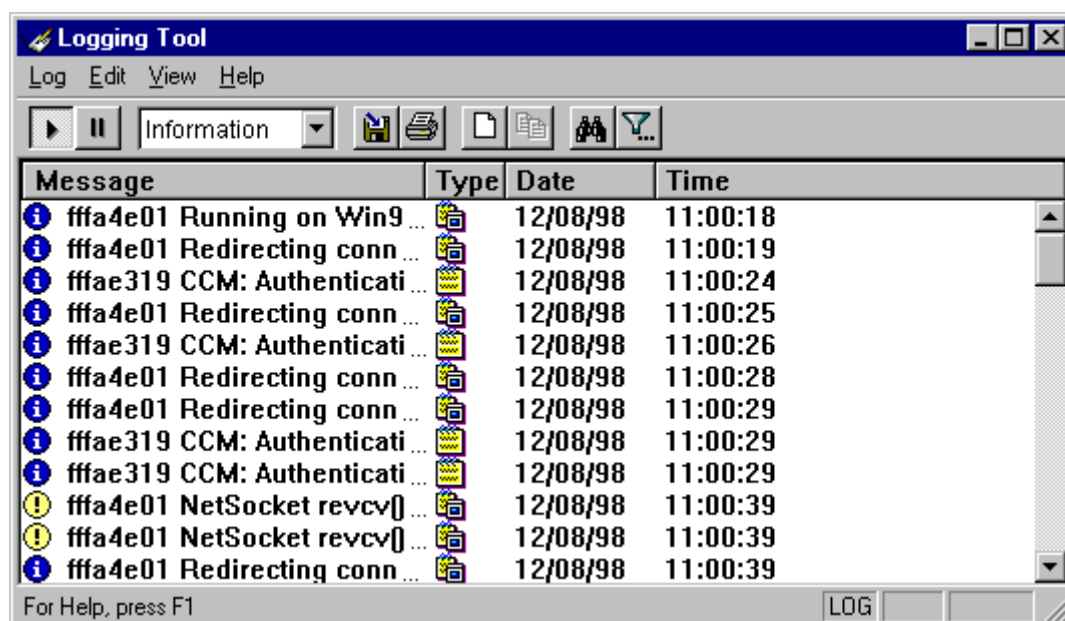
## CONFIG TOOL

The Aventail Connect Config Tool creates configuration files that determine how network requests will be routed and which authentication protocols will be enabled. Network administrators generally create configuration files during Aventail Connect installation. The availability of the Config Tool depends on whether or not your network administrator has included it in your Aventail Connect installation package.



## LOGGING TOOL

The Logging Tool is an optional diagnostic utility that traces Aventail Connect and WinSock activity. When running a trace, the Logging Tool displays errors, warnings, and information as Aventail Connect generates them. You can save the message list to a log file that Aventail Technical Support can use in troubleshooting technical problems. Log files are also useful when running Aventail Connect for the first time, to ensure that network traffic is being routed properly. The availability of the Logging Tool depends on whether or not your network administrator has included it in your Aventail Connect installation package.

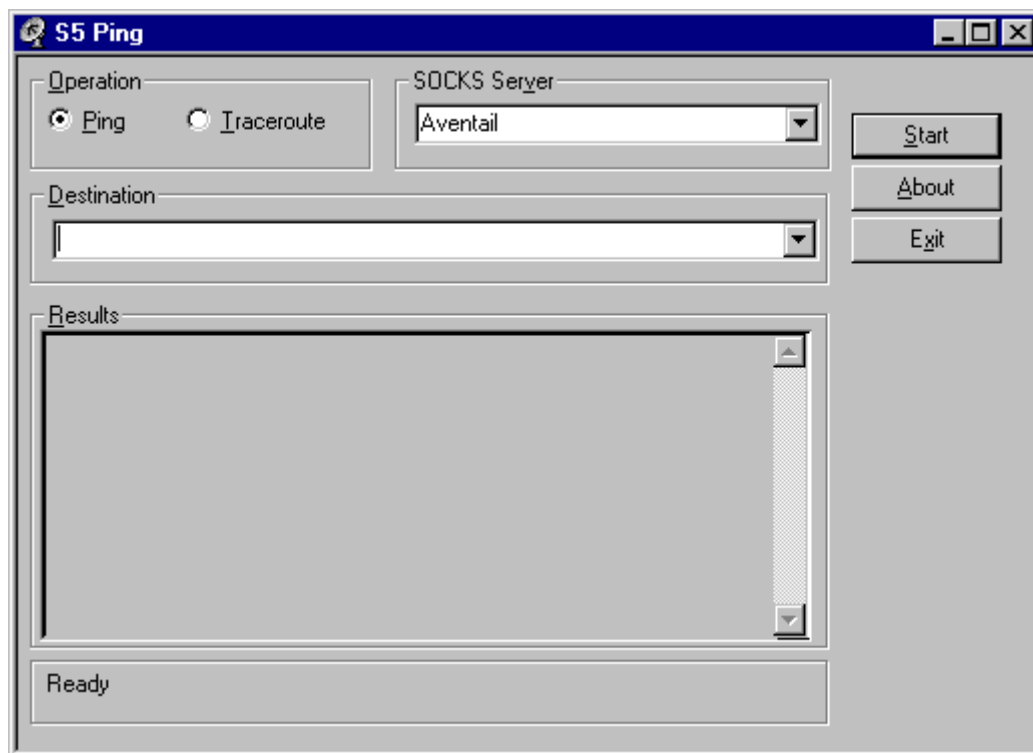


## S5 Ping

This command allows you to run the ping and traceroute utilities. The availability of the S5 Ping command depends on whether or not your network administrator has included it in your Aventail Connect installation package.

- The ping utility checks for network connectivity between two hosts and returns information about the quality of the connection.
- The traceroute utility checks for network connectivity by displaying information about routers between two hosts. It displays information for each hop.

S5 Ping determines whether a host outside of an extranet server is active. After a response from the host returns, the extranet server relays the data back to the client and displays it in the **S5 Ping** dialog box.



## SECURE EXTRANET EXPLORER

Secure Extranet Explorer (SEE) allows you to view your Extranet Neighborhood, which is accessed through the **Extranet Neighborhood** icon on your desktop. The Extranet Neighborhood user interface resembles that of Network Neighborhood. However, while Network Neighborhood displays all computers on your local network, Extranet Neighborhood allows you to browse, copy, move, and delete files from remote computers via the Aventail Connect extranet connection. With Extranet Neighborhood, all interaction with the remote server can be secured. Network administrators determine which local and remote computers are available to users.



**NOTE:** Some installations of Aventail Connect may not include SEE. Network administrators can decide whether or not to include SEE in a custom setup package.



**NOTE:** Secure Extranet Explorer/Extranet Neighborhood is available only on Windows 95, Windows 98, and Windows NT 4.0 operating systems.

Extranet Neighborhood, a Windows Explorer shell extension, is a collection of Windows file servers and Windows NT domains. Network Neighborhood displays only those remote computers that the network administrator has specified. SEE requires a hosts file (SEEHosts) that determines which Windows file servers and NT domains are available. If you install a custom setup package that does not include a SEEHosts file, then the first time you open Extranet Neighborhood, SEE will create a SEEHosts file. For more information, contact your network administrator.

Extranet Neighborhood offers Aventail Connect users a secure alternative to traditional file-browsing methods. Users can securely access computers from the desktop through Extranet Neighborhood (see icon below), or through Windows Explorer.



Generally, you will use Extranet Neighborhood to connect to a remote network through Aventail Connect. For example, you will use Extranet Neighborhood when:

- you are inside the office, on the corporate network, and you connect through an Aventail ExtraNet Server to your company's remote site, or to another company's network.

- you are outside the office, and you connect your laptop through an Aventail ExtraNet Server to your internal company network, or to another company's network.



**NOTE:** *To use Extranet Neighborhood with remote hosts, Aventail Connect must be running and configured correctly.*



**CAUTION:** *Always check with your network administrator before making any changes to your Extranet Neighborhood/SEE configuration.*



# Glossary

**ALIAS**

User-friendly name for destination network or host computer.

**AUTHENTICATION**

A method for identifying a user in order to establish access to a system resource or network. Authentication information such as username/password is entered via prompts.

**CERTIFICATE**

A certificate is essentially an electronic "statement" which verifies that a certain RSA public key is associated with a particular name. Certificates are issued by a Certification Authority (CA).

**CLIENT**

A program or Internet service that sends commands to and receive information from a corresponding program known as a server. Most Internet services run as client/server programs.

**CONFIGURATION FILE**

A file of information containing traffic redirection rules used to determine if and how SOCKS redirection should occur.

**CREDENTIALS**

Credentials include the information (such as username/password) that you enter when establishing a connection to a SOCKS server requiring user authentication.

**DOMAIN**

Internet name for a network or computer system.

**ENCRYPTION**

A security procedure that converts data into a format which can be read only by the intended recipient computer.

**EXTRANET**

A network that is partially accessible to outsiders.

**FIREWALL**

Software or hardware barriers that control the flow of information to Private networks.

**GATEWAY**

A communications device/program that passes data between networks.

**HACKER**

A person who enjoys using computers and has a thorough understanding of how they work, as well as the networks they run on. Often used to mean "cracker," the correct term for someone who accesses computer systems without authorization.

**HOST**

A server connected to the Internet.

**IETF**

Internet Engineering Task Force: An open community of network designers, vendors, etc. who resolve protocol and architectural issues for the quickly evolving Internet.

**INTERNET PROTOCOL (IP)**

The basic data transfer protocol used for the Internet. Information such as the address of the sender and the recipient is inserted into an electronic "packet" which is then transmitted.

**INTRANET**

A network that is internal to a company or organization.

**LAN**

Local area network

**LAYERED SERVICE PROVIDER (LSP)**

A program that is installed just below WinSock 2, allowing two-way communication between the WinSock 2-compatible application and the underlying TCP/IP stack. An LSP can redirect and/or change data before sending the data to the operating system's TCP/IP stack for transport over the network.

**LOG WINDOW**

The window of the Logging Tool which shows alerts, messages, and warnings generated by Aventail Connect.

**PING**

A utility that determines if a remote host computer is up. ping sends data packets to the host. If the packets are not returned, the host is down.

**PROTOCOL**

Rules and procedures used to exchange information between networks and computer systems.

## **REDIRECTION RULES**

Rules defined in the configuration file which specify how network requests are routed to SOCKS servers.

## **ROUTER**

A device that transmits traffic between networks

## **SERVER**

A networked computer that shares resources with other computers. Servers “serve up” information to clients.

## **SMB**

Server Message Block. A message format used by DOS and Windows for sharing files, directories, and other resources.

## **SOCKS**

SOCKS is a security protocol. It acts as a proxy mechanism that manages the flow and security of data traffic to and from your local area network or intranet.

## **SSL**

Security Sockets Layer. An authentication and encryption protocol.

## **TRACEROUTE**

A utility that traces the routing of data over the Internet to a specific computer. Traceroute sends a data packet and then lists the intermediate host computers that it traverses on its way to the destination machine.

## **TRANSMISSION CONTROL PROTOCOL (TCP)**

A means of sending data over the Internet with guaranteed delivery.

## **TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP)**

A suite of protocols the Internet uses to provide for services such as e-mail, ftp, and telnet.

## **USER DATAGRAM PROTOCOL (UDP)**

A means of sending data over the Internet without guaranteed delivery. Also known as “connectionless” protocol, it is used for data such as RealAudio®.

## **UNIVERSAL NAMING CONVENTION (UNC)**

A way of accessing a file or directory on another computer. For example: // host/share/directory/file (“share” refers to the alias used to make the resource available.)

## **VIRUS**

A self-replicating code segment that can infect a computer or network, causing minor to major damage

**VPN**

Virtual Private Network: A secure channel used to transmit data over a public network

**WinSock**

Windows Sockets. A Windows component that connects a Windows PC to the Internet using TCP/IP.

**WORKSTATION**

Any computer connected to a network.

**X.509**

An ISO format standard for client and server certificates.

**A**

- About command 13
- accepting an SSL certificate 11
- applications
  - TCP/IP 6
- authentication
  - certificates 11
  - CHAP 9
  - CRAM 10
  - entering credentials 9
  - modules 8
  - tokens 10
  - UNPW 9
- Aventail Connect
  - closing 6
  - Config Tool 17
  - configuration files 6
  - features 1
  - Logging Tool 17
  - S5 Ping 17
  - starting 6
- Aventail Corporation, about 5
- Aventail ExtraNet Server 21
- Aventail Technical Support 5

**C**

- caching 8, 12
- certificates
  - authentication 11
  - SSL 11
- CHAP 9
- Close command 13
- closing Aventail Connect 6
- commands
  - About 13
  - Close 13
  - Configuration File 13
  - Credentials 13
  - Help 13
  - Hide Icon 13
- Config Tool 17
- Configuration File command 13
- configuration files 6
- CRAM 10
- credential caching 8, 12
- credentials
  - deleting 15
  - managing 15
- Credentials command 13

**D**

- deleting
  - credential entries 15
- document
  - conventions 4
  - organization 3

**E**

- encryption 8
- Extranet Neighborhood
  - icon 20
  - overview 20
  - remote access and 20
- Extranet servers 8, 15

**F**

- files
  - configuration 6
  - hosts 20

**G**

- Glossary 22

**H**

- Help command 13
- Hide Icon command 13
- hosts files
  - SEEHosts 20

**I**

- icon 20

**L**

- Logging Tool 17

**M**

- managing credentials 15
- menu commands 13

**N**

- Network Neighborhood 20

**P**

- ping 19
- platform requirements 20

**R**

- rejecting an SSL certificate 11
- remote access 20

**S**

- S5 Ping 17, 19
- Secure Extranet Explorer
  - overview 20
  - platform requirements 20
- Secure Socket Layer (SSL) 10
- SecurID 10
- servers
  - Extranet 8, 15
  - SOCKS 15
  - SSL 11
- SOCKS 15
- SoftID 10
- SSL certificates 11
- SSL servers 11
- SSL subauthentication 10
- starting Aventail Connect 6
- system menu commands 13

**T**

- TCP/IP applications 6
- Technical Support 5
- tokens 10
- traceroute 19

**U**

- UNPW 9
- utilities
  - Config Tool 17
  - Logging Tool 17
  - S5 Ping 17

**W**

- Windows Explorer 20
- WinSock 6