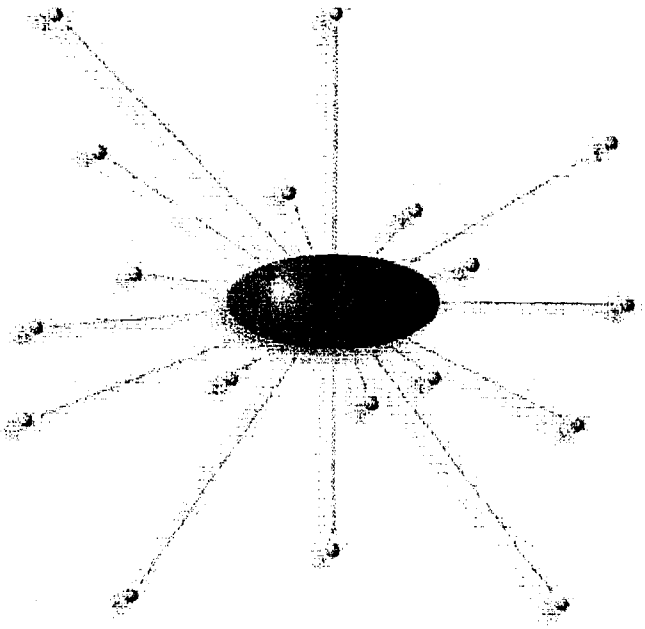
Aventail

CONNECT

v3.1/v2.6



Administrator's Guide

Windows

Aventail

AVENTAIL CONNECT 3.1/2.6 ADMINISTRATOR'S GUIDE

808 Howell Street, Second Floor
Seattle, WA 98101
USA

http://www.aventail.com/

Printed in the United States of America.

TRADEMARKS AND COPYRIGHTS

Table of Contents

UTILITIES REFERENCE GUIDE

TROUBLESHOOTING

Introduction

Welcome to the Aventail Connect 3.1/2.6 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. (For more information about WinSock, TCP/IP, and general network communications, see "Getting Started.")

On larger networks, Aventail Connect can address multiple SOCKS 5 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 (LSP) applications in Windows 98, and Windows NT 4.0, and WinSock 1.1 and WinSock 2 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

NOTE: *Not all versions of Aventail Connect have encryption enabled.*

About This Document

This *Administrator's Guide* provides basic information about Aventail Connect. It includes entry-level data for non-technical users, plus installation, setup, and configuration information for network administrators. 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 three main sections: *Administrator's Guide*, *Utilities Reference Guide*, and *Troubleshooting*.

The *Administrator's Guide* describes procedures for setting up, installing, and configuring Aventail Connect for individual and multiple networked workstations. It also describes how to create a customized Aventail Connect package for distribution to multiple users.

The *Utilities Reference Guide* describes the Aventail Connect system menu commands and utility programs. It contains detailed information about using the S5 Ping utility and the Logging Tool, and documents the authentication/encryption modules and settings.

The document concludes with *Troubleshooting* and the *Glossary*.

You can also use the Quick Start Card, a short document designed to help you install Aventail Connect to an individual workstation, and the Aventail Connect flowchart, at **http://www.aventail.com/contents/solutions/presentations/quickstart/vpnclient.pdf**.

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.
Bold	Dialog box controls (**Edit...** buttons), e-mail addresses (**support@aventail.com**), URLs, (**www.aventail.com**), and IP addresses (**165.121.6.26**).
Italic	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**, or the Aventail Knowledge Base, at **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 *Administrator's Guide*.

Aventail Technical Support:
Web site: **http://www.aventail.com/index.phtml/support/index.phtml**
E-mail: **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

An aventail is a piece of chainmail armor worn around the neck area. In the 14th 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.

Administrator's Guide

This section includes procedural and background information on installing Aventail Connect on both single and networked workstations. It includes:

- "Getting Started," with brief explanations of network security and communications
- Definitions of SOCKS and Aventail Connect
- Aventail Connect platform and installation requirements, with an introduction to WinSock 2 and LSP architecture
- "Installing Aventail Connect," which includes network diagrams of Aventail ExtraNet Center and SOCKS v4-based server configurations
- Directions on how to create and edit configuration files, and an introduction to the Aventail Customizer

NOTE: *Aventail understands the importance of a flexible, easy-to-use installation process. If you have feedback regarding the Aventail Connect installation procedures, or if there are additional features you want to see implemented, please e-mail comments to* **support@aventail.com**. *Your input is appreciated.*

GETTING STARTED

If you are new to Aventail Connect technology, the following section will help you understand what Aventail Connect is and does, and its relationship to network security in general.

NETWORK SECURITY IN A NUTSHELL

Escalating security threats are forcing companies to seek ways to safeguard their corporate networks and the information they exchange. The first response to these concerns has been the development of security firewalls—software barriers that control the flow of information. But firewalls are not designed to handle complex security issues, such as monitoring network usage, providing private communication over public networks, and enabling remote users to gain secure access to internal network resources.

Enter SOCKS v5, an Internet Engineering Task Force (IETF)-approved security protocol targeted at securely traversing corporate firewalls. SOCKS was originally developed in 1990, and is now maintained by NEC. SOCKS acts as a circuit-level proxy mechanism that manages the flow and security of data traffic to and from your local area network (LAN) or extranet. An application whose traffic

is proxied by SOCKS is considered "socksified." SOCKS is more than a standard security firewall. Other features:

- Client Authentication: (SOCKS v5 only) Authentication allows network managers to provide selected user access to internal and external areas of a network.
- Traffic Encryption: (SOCKS v5 only) Encryption ensures that network traffic is private and secure.
- UDP Support: (SOCKS v5 only) User Datagram Protocol (UDP) traffic has traditionally been difficult to proxy, with the exception of SOCKS v5.
- Aventail Connect supports X.509 client certificates within SSL.
- Cross-Platform Support: Unlike many other security solutions, SOCKS can be used on various platforms, such as Windows NT, Windows 95, Windows 98, and various forms of UNIX.

NOTE: *Not all versions of Aventail Connect include the SSL module for encryption.*

WHAT IS AVENTAIL CONNECT?

Aventail Connect is the client component of the Aventail ExtraNet Center. Aventail Connect works with the Aventail ExtraNet Server, the SOCKS 5 server component of the Aventail ExtraNet Center. You can use Aventail Connect as a simple proxy client for managed outbound access, and for secure inbound access.

Aventail Connect automates the "socksification" of Transmission Control Protocol/Internet Protocol (TCP/IP) client applications, making it simple for workstations to take advantage of the SOCKS v5 protocol. When you run Aventail Connect on your system, it automatically routes appropriate network traffic from a WinSock (Windows sockets) application to an extranet (SOCKS) server, or through successive servers. (WinSock is a Windows component that connects a Windows PC to the Internet using TCP/IP.) The SOCKS server then sends the traffic to the Internet or the external network. Network administrators can define a set of rules that route this traffic.

Aventail Connect is designed to run transparently on each workstation, without adding overhead to the user's desktop. In most cases, users will interact with Aventail Connect only when it prompts them to enter authentication credentials for a connection to a secure extranet (SOCKS) server. Users may also occasionally need to start and exit Aventail Connect, although network administrators often configure it to run automatically at startup. Aventail Connect does not require administrators to manually establish an encrypted tunnel; Aventail Connect can establish an encrypted tunnel automatically.

To understand Aventail Connect, you first need to understand a few basics of TCP/IP communications.

TCP/IP Communications

Windows TCP/IP networking applications (such as telnet, e-mail, Web browsers, and ftp) use WinSock to gain access to networks or the Internet. WinSock is the core component of TCP/IP under Windows, and is the interface that most Windows applications use to communicate to TCP/IP.

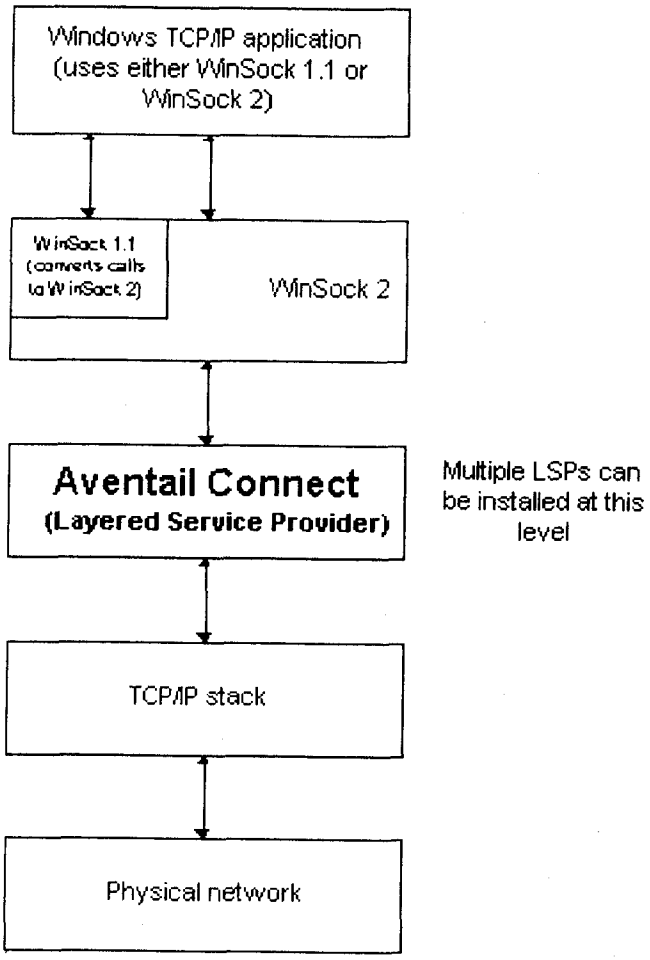
WinSock Connection to a Remote Host

Via WinSock, an application goes through the following steps to connect to a remote host on the Internet or corporate extranet:

1. The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address or, in rare cases, it will do a reverse DNS lookup to convert the IP address into a hostname. If the application already knows the IP address, this step is skipped.
2. The application requests a connection to the specified remote host. This causes the underlying stack to begin the TCP handshake, when two computers initiate communication with each other. When the handshake is complete, the application is notified that the connection is established, and data can then be transmitted and received.
3. The application sends and receives data.

WHAT DOES AVENTAIL CONNECT DO?

Aventail Connect slips in between WinSock and the underlying TCP/IP stack. (See diagram below.) As an application that sits between WinSock and the TCP/IP stack, Aventail Connect 3.1 is a Layered Service Provider (LSP). Aventail Connect can change data (compressing it or encrypting it, for example) before routing it to the TCP/IP stack for transport over the network. The routing is determined by the rules described in the configuration file.



Windows TCP/IP applications and Aventail Connect have no direct contact with one another; instead, each of them communicates through WinSock. Multiple LSP applications can be installed at the LSP level.

NOTE: Aventail Connect does not alter or replace WinSock or any other core TCP/IP components (files) provided by the operating system.

When the Aventail Connect LSP receives a connection request, it determines whether or not the connection needs to be redirected (to an Aventail ExtraNet Server) and/or encrypted (in SSL). When redirection and encryption are not necessary, Aventail Connect simply passes the connection request, and any subsequent transmitted data, to the TCP/IP stack.

The two most popular versions of WinSock are versions 1.1 and 2. Aventail Connect 3.1, like all LSPs, requires WinSock 2; WinSock 1.1 does not support LSPs. WinSock 2 includes backward-compatibility with all WinSock 1.1 applications. Not every platform supports WinSock 2 and its LSP structure.

- Windows 98 and Windows NT 4.0 support WinSock 2 natively. (Windows NT 4.0 requires Service Pack 3 or above, available from Microsoft.)
- Windows 95 supports WinSock 1.1. Windows 95 can also support WinSock 2, but you must install a patch (available from Microsoft) to add support for WinSock 2.
- Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51 do not support WinSock 2; they support only WinSock 1.1.

For those platforms that do not support WinSock 2 and LSP applications, Aventail includes Aventail Connect 2.6 on the Aventail Connect 3.1/2.6 CD. Aventail Connect 2.6 was designed for operating systems that support only WinSock 1.1. On Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51 operating systems, setup will install Aventail Connect 2.6. If you are working on a Windows 95 operating system, setup will detect whether you have installed the Microsoft Windows 95 WinSock 2 Update. If setup detects the Microsoft update, which upgrades Windows 95 to support WinSock 2, setup will install Aventail Connect 3.1. If setup does not detect the Microsoft update, it will install Aventail Connect 2.6.

The Aventail Connect 2.6 user interface is identical to that of Aventail Connect 3.1; however, Aventail Connect 3.1 includes MultiProxy functionality (see "Multiple Firewall Traversal"). Aventail Connect 2.6 does not include MultiProxy.

In the future, more Windows applications may require WinSock 2.

During installation, setup determines which version of Aventail Connect to install. On WinSock 2 platforms, Aventail Connect 3.1 is installed. On WinSock 1.1 platforms, Aventail Connect 2.6 is installed. The following table shows how setup determines which version of Aventail Connect to install.

Operating System	WinSock Support	Aventail Connect Version Installed
Windows 98, Windows NT 4.0	WinSock 2	Aventail Connect 3.1
Windows 95	With Microsoft patch: WinSock 2	Aventail Connect 3.1
	Without Microsoft patch: WinSock 1.1	Aventail Connect 2.6
Windows 3.1, Windows for Workgroups 3.11, Windows NT 3.51	WinSock 1.1	Aventail Connect 2.6

You can create custom packages that include one or both versions of Aventail Connect (3.1 and 2.6). Setup will determine which version to install on each workstation. (For more information, see "Customizer.")

WINDOWS 95 AND WINSOCK

The Microsoft Windows 95 WinSock 2 Update upgrades WinSock 1.1 to WinSock 2 in Windows 95. This patch (filename `w95ws2setup.exe`) is available from the Microsoft Web site, at **http://www.microsoft.com/Windows95/downloads/contents/wuadmintools/s_wunetworkingtools/W95Sockets2/default.asp**. Unless you need specific Aventail Connect 3.1 features, Aventail recommends that you do not upgrade from WinSock 1.1 to WinSock 2. If you do not upgrade to WinSock 2, Aventail Connect 2.6 will be installed on Windows 95 systems.

If you do need to install the Microsoft Windows 95 WinSock 2 Update, follow the instructions provided by Microsoft. Reboot your computer after upgrading, prior to installing Aventail Connect.

HOW DOES AVENTAIL CONNECT WORK?

The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

1. The application does a DNS lookup to convert the hostname to an IP address or, in rare cases, it will do a reverse DNS lookup to convert the IP address to a hostname. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:
   - If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running.

- If the destination hostname matches a redirection rule domain name (i.e., the host is part of a domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.
- If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a false DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

CAUTION: *The reverse DNS process can create unexpected delays, causing Aventail Connect to behave unpredictably. Aventail recommends that you do not enable this option unless you specifically require the Reverse DNS functionality.*

2. The application requests a connection to the remote host. This causes the underlying stack to begin the TCP handshake. When the handshake is complete, the application is notified that the connection is established and that data may now be transmitted and received. Aventail Connect does the following:

   a. Aventail Connect checks the connection request.

      - If the request contains a false DNS entry (from step 1), it will be proxied.
      - If the request contains a routable IP address, and the rules in the configuration file say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.
      - If the request contains a real IP address and the configuration file rule says that it does not need to be proxied, the request will be passed to WinSock and processing jumps to step 3 as if Aventail Connect were not running.

   b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.

      - It sends the list of authentication methods enabled in the configuration file.
      - Once the server selects an authentication method, Aventail Connect executes the specified authentication processing.
      - It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

   c. When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS

negotiation, including the authentication negotiation, is merely the TCP handshaking.

3. The application transmits and receives data.

   If an encryption module is enabled and selected by the SOCKS server, Aventail Connect encrypts the data on its way to the server on behalf of the application. If data is being returned, Aventail Connect decrypts it so that the application sees cleartext data.

AVENTAIL CONNECT PLATFORM REQUIREMENTS

The following table lists the minimum system requirements for each of the platforms that Aventail Connect supports.

Platform	Processor	RAM	SOCKS Server
Windows 98; Windows NT 4.0 (requires Microsoft Service Pack 3 or above)	x86-based or Pentium personal computer	16 MB	Network-accessible SOCKS v4 or v5 compliant server
Windows 95; Windows NT 3.51	x86-based or Pentium personal computer	8 MB	Network-accessible SOCKS v4 or v5 compliant server
Windows 3.1; Windows for Workgroups 3.11	x86-based or Pentium personal computer	4 MB	Network-accessible SOCKS v4 or v5 compliant server

Aventail Connect 3.1 runs on the following operating systems:

- Windows 98
- Windows NT 4.0 (with Service Pack 3 or above, available from Microsoft)
- Windows 95, with the Microsoft WinSock 2 update (To install Aventail Connect 3.1, you must upgrade Windows 95 with the Microsoft WinSock 2 update prior to Aventail Connect installation and setup. If you do not install the Microsoft patch, Aventail Connect 2.6 will be installed. For more information, see "What Does Aventail Connect Do?".)

Aventail Connect 2.6 runs on the following operating systems:

- Windows 3.1
- Windows for Workgroups 3.11
- Windows NT 3.51
- Windows 95, without the Microsoft WinSock 2 update (If you do not upgrade Windows 95 with the Microsoft WinSock 2 update, Aventail Connect 2.6 will be installed. For more information, see "What Does Aventail Connect Do?".)

NOTE: A WinSock-compatible 16- or 32-bit TCP/IP application must be installed and configured prior to running Aventail Connect. This can be the Microsoft-provided TCP/IP stack or a third-party TCP/IP stack.

INTERFACE FEATURES

The following table lists the interface features for each platform. Each of these features is discussed in greater detail later in the *Administrator's Guide*.

Platform	Start Aventail Connect	Display System Menu	Open Secure Extranet Explorer	View Program Icon	Hide Program Icon
Windows 95, Windows 98, Windows NT 4.0	Start\Programs \Aventail Connect menu	Right-click **Aventail Connect** icon in system tray	Double-click **Extranet Neighborhood** icon on desktop	In system tray	Not available
Windows 3.1, Windows for Workgroups 3.11, Windows NT 3.51	**Aventail Connect** icon in Aventail Connect program group window	Click **Aventail Connect** icon in Aventail Connect program group window	Not available	Minimized on desktop	Configure during setup

INSTALLATION SOURCE MEDIA

Regardless of platform, Aventail Connect can be delivered on CD or as a network-delivered, self-extracting archive file.

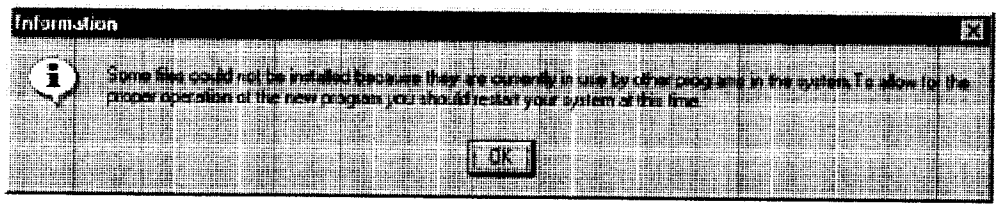
- **CD**: The CD contains the Aventail Connect setup program, `setup.exe`. The setup program allows for an administrative setup. It also contains the *Administrator's Guide* and the *User's Guide* in the `\docs` directory, formatted for Adobe® Acrobat Reader.
- **Network-delivered Source Media**: The network-delivered source media is a self-extracting archive containing the required disk/directory structure within the archive file. The executable automatically extracts the Aventail Connect installation files and initiates setup. The archive filename will be similar to `as31s.exe`. This archive, or package, will also be available on the CD (located in the **Utilities** directory) to be used with the Customizer application. For more information, see the "Customizer" section.

INSTALLING AVENTAIL CONNECT

After your Aventail ExtraNet Server is set up, Aventail Connect can be installed to a single workstation or to multiple networked workstations. In either case, you must perform an initial installation of the software and create one or more configuration (.cfg) files. This procedure is described under "Individual Installation." Once the initial installation is complete, you can then install to a series of networked computers using the instructions and information described under "Network Installation."

NOTE: *To install or uninstall Aventail Connect on Windows NT machines, you must have administrative privileges on the machine (but not necessarily on the domain).*

If you are upgrading from an earlier version of Aventail Connect (Aventail VPN Client or Aventail AutoSOCKS), the following message may appear on your screen if you install a custom setup package using Aventail Customizer. This is not an error message. If this message appears, click **OK** and reboot your computer.



CONFIGURATION FILES

Integral to the initial installation of Aventail Connect is deciding how SOCKS traffic will be redirected through the network. Network redirection rules (used to determine if and how SOCKS redirection will occur) are defined in the Aventail Connect configuration (.cfg) file. Configuration files are initially created at the end of the installation process; however, you can add, edit, and remove configuration files at any time using the Config Tool (in Windows 95, Windows 98, or Windows NT 4.0 via the **Aventail** icon in the system tray on the taskbar; in Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51 via the Aventail Program Group). The process of creating one or more configuration files is described under "Configuring Aventail Connect."

If you are installing Aventail Connect on multiple networked workstations, refer to "Network Installation" to determine the best method for maintaining and distributing configuration files. You can then proceed through the initial installation. The Installation Wizard will guide you through the steps, culminating with the option to create a configuration file.

CUSTOMIZED CONFIGURATION AND DISTRIBUTION

The Aventail Customizer is a utility that allows network administrators to customize Aventail Connect installation packages for distribution to multiple client workstations. Giving network administrators control over how setup packages are configured eliminates the need for end users to make installation and setup decisions at their workstations. The installation package is a self-extracting executable file. You can customize this file by adding license file, configuration file, or setup information for different authentication and encryption policies to meet various client-access needs of individuals or workgroups. You can customize configurations for multiple users and then distribute the package, providing easy access, download, and installation for users. You can reconfigure the Aventail Connect installation package anytime your network topology or security profiles change.

For more information about the Aventail Customizer, see the "Customizer" section.

INDIVIDUAL INSTALLATION

Before running setup, close all open Windows applications.

To install Aventail Connect

1. Installation procedures vary slightly, depending on which media source you use:
   - If you are installing directly from CD-ROM, run `setup.exe` from the Aventail Connect directory.
   - If you are installing from a network-delivered self-extracting archive, simply execute the archive file. This will extract the installation files and automatically launch the setup program.

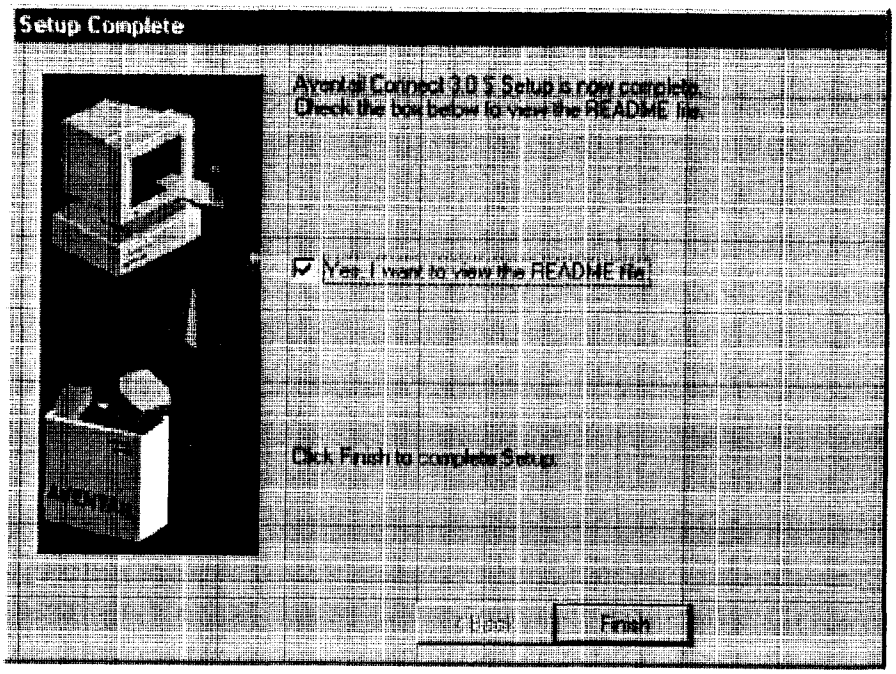
   The Aventail Connect Installation Wizard then guides you through the process of installing the Aventail Connect application.

NOTE: *You will be asked during the installation procedure if you would like Aventail Connect to be run automatically during startup. In most cases, you will select* ***yes****. Exceptions to this can be determined by the network administrator.*

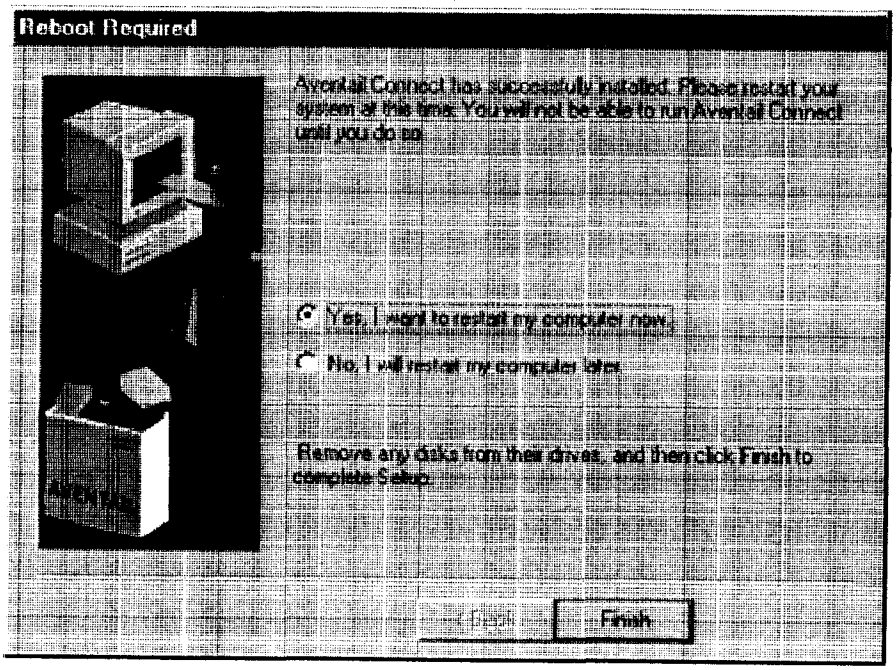
2. At the end of the setup program, you can select **Yes, I want to view the README file** in the **Setup Complete** dialog box. This opens the `readme.txt` file, which contains the latest information on Aventail Connect.

-OR-

Simply click **Finish** in the **Setup Complete** dialog box to complete the setup program.



3. The setup program will then ask you if you want to restart your machine now or later.



4. After restarting your PC, Aventail Connect will launch automatically if, during installation, you selected **Yes** when asked if Aventail Connect should be added to your startup directory. (If, during installation, you specified that Aventail Connect *not* be added to the startup directory, start Aventail Connect from the **Programs** menu.)
5. Aventail Connect will ask you if you want to run the configuration wizard.

   If you click **Yes,** then the configuration wizard will launch to help you create a new configuration file.

   If you click **No**, then Aventail Connect will ask you to select a configuration file.
6. After creating or selecting a configuration file, Aventail Connect will finish its installation procedure.

To uninstall Aventail Connect

The procedure to uninstall (remove) Aventail Connect varies depending on whether you are running a 16- or 32-bit Windows operating system.

- To uninstall Aventail Connect from Windows 95, Windows 98, and Windows NT 4.0, double-click **Add/Remove Programs** in the **Control Panel** window, click **Aventail Connect** on the list of programs on the **Install/Uninstall** tab, and then click **Add/Remove**.
- To uninstall Aventail Connect on Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51, use the **Uninstall** icon in the Aventail Connect program group.

NETWORK INSTALLATION

In general, the process of installing Aventail Connect to multiple networked workstations involves selecting a file server to use, creating a staging area for the Aventail Connect software, and placing the Aventail Connect package in a shared network directory or other publicly accessible location. Additional options include adding a default configuration file, license file, certificate and roots files, and SEEHosts files. You must place Aventail Connect files on a network drive that can be accessed as a mapped drive or, for Microsoft networks, via a UNC path name (`\\computer name\share name\Connect`).

An executable archive file (with a filename similar to `as31s.exe`) automatically extracts the Aventail Connect installation files and initiates setup. This archive, or package, is located in the Utilities directory of the CD and can be used in conjunction with the Customizer application. (For more information, see "Customizer.") The package can also be manually configured to suit your network specifications. The default package includes all of the core Aventail Connect files, but does not include the custom network information.

NETWORKED CONFIGURATION FILE SETUP

There are a number of ways to set up networked client configuration files. These are the most common:

- **Remote UNC:** Remote client configuration file on a Windows share using UNC path and filename (e.g., `\\internal\common\a.cfg`)
- **Local Configuration File:** Local client configuration file common for all users, but distributed via a locally stored Aventail Connect package
- **Remote Web Server:** Remote configuration files stored on a Web server using URL (e.g., **http://internal/a.cfg**)

Configuration file setup method	Location	Advantages	Disadvantages
Remote UNC	Windows share using UNC path and filename	• Configuration file can be centrally maintained. • No local caching required.	• File server must be on local network. If file server is unavailable, Aventail Connect will not function.
Local Configuration File	Locally stored setup package	• Does not require network connection; configuration file is always available.	• Configuration files cannot be centrally maintained.
Remote Web Server	Web server	• Configuration file can be centrally maintained. • Connection to Web server can be made across the Internet, and can traverse proxies. • Supports authentication and encryption. • If Web server is unavailable, locally cached copy can be used.	• Requires Web server. • Requires network connection for updates.

ADMINISTRATOR-MAINTAINED SHARED CONFIGURATION FILES

This is the most desirable configuration method—multiple workstations sharing one or more administrator-maintained configuration files located in a common directory. The network administrator maintains the configuration file, and the administrator can quickly adapt any changes to network topology through a single configuration file. For example:

- A single networked (usually read-only) configuration file is shared by more than one client workstation. This method is appropriate when multiple workstations share identical traffic routing rules.
- Multiple configuration files are shared by multiple workstations. This option is useful when you have workstations organized into functional groups (engineering, marketing, accounting, etc.) with group-specific redirection rules.

Shared Configuration File Distribution

Shared configuration files can be easily distributed and, if necessary, updated via the network or a Web server. Aventail recommends that you test all configuration files before distribution.

You can distribute shared configuration files with the Aventail Customizer. This automated wizard allows you to create custom setup packages for multiple users and then store the packages in a networked directory, providing easy access, download, and installation for users. You can include multiple local and/or remote configuration files. For more information, refer to the "Customizer" section.

To distribute a shared configuration file

There are three methods for distributing shared configuration files.

- **Remote UNC:** Copy the file to a Microsoft or Novell network drive accessible by all users, or to a Microsoft Windows workstation supporting UNC-sharing for file resources. (Both the 16- and 32-bit versions of Aventail Connect support specification of the configuration file using the Microsoft UNCs.) If you copy the file to a network drive, make sure that users configure Aventail Connect to load the configuration file located on the mapped drive. You can preconfigure this information for users from a package install.

-OR-

- **Local Configuration File:** Create a shared configuration file to be installed on workstations during the standard Aventail Connect installation/upgrade process. Whenever Aventail Connect is installed or updated, it will automatically copy the shared configuration file to the user's workstation and set Aventail Connect to use it.

-OR-

- **Web Server:** Copy the file to a Web server. The Web server can be directly accessible to the workstation, or it can be behind a proxy server. To keep configuration files secure, you can redirect the configuration file connection, authenticated and encrypted, across firewalls.

Storing Remote Configuration Files on a Web Server

When you specify the remote configuration file in Aventail Connect, include the entire URL (e.g., http://aventail.com/server1/config.cfg). You can specify this URL in the **Aventail Connect Configuration File** dialog box, or with Customizer.

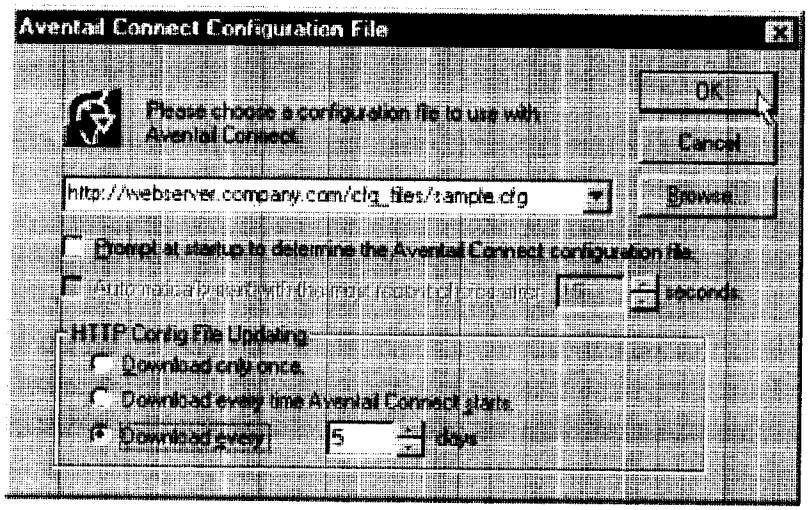
Aventail Connect keeps a temporary local copy of the remote configuration file in its program directory, with the filename _ashttpX.cfg, where X is a number between 0 and 9. Keeping a local copy of the remote configuration file allows the connection to the Web server to be proxied (with authentication and encryption) if necessary. Whenever the remote configuration file needs to be downloaded, Aventail Connect will check the cached copy of the configuration file to determine whether redirection is necessary.

Aventail Connect can download remote configuration files either every time Aventail Connect starts or on a scheduled basis. You can configure this setting in the **Aventail Connect Configuration File** dialog box, or when adding a remote configuration file to a custom installation package with Customizer. When you add a remote configuration file with Customizer, a cached copy of the file can automatically be added to the package.

To store remote configuration files on a Web server

1. Place an Aventail Connect configuration file on a Web server.
2. If redirection through a proxy server is required to reach the Web server, configure Aventail Connect to use a configuration file that can access the Web server. If redirection is not required, skip this step.
3. With Aventail Connect running, select **Configuration File** from the system tray menu.

   The **Aventail Connect Configuration File** dialog box will open.
4. Enter the URL and filename of the configuration file, e.g., **http://webserver.company.com/cfg_files/sample.cfg**. Click **OK**.



5. Under "HTTP Config File Updating," specify how often Aventail Connect will download the configuration file. Click **OK**.

   The configuration file will automatically be downloaded, and Aventail Connect will begin using it immediately. A local copy of the configuration file will be cached in the Aventail Connect program directory.

ADMINISTRATIVE SETUP

There are two ways to install Aventail Connect: from the setup program (`setup.exe`), or from a setup package that you create using the Aventail Customizer. The setup program (`setup.exe`) allows you to manually install Aventail

Connect. With the Aventail Connect setup package, you can select options that will customize setup based on your unique network environment. You can customize the setup package through the Customizer Editor or the Customizer Wizard. The Customizer *Editor* is a dialog box that allows you to manually enter or modify information about your custom installation package. The Customizer *Wizard* walks you through each step of creating a custom installation package. Aside from the user-interface differences, the Customizer Wizard and the Customizer Editor are identical. You can use both the Customizer Wizard and the Customizer Editor to create or modify a setup package. For example, you can create a package using the Customizer Wizard, then modify it with the Customizer Editor.

CUSTOMIZER

The Aventail Customizer simplifies and customizes the installation and setup process. Network administrators can reconfigure the self-extracting executable installation package (included in the Customizer directory of the distribution CD) to meet the various client-access needs of individuals or workgroups. Customizer offers a centralized approach to network configuration; network administrators can select the *unattended setup mode*, which eliminates the need for individual users to answer any setup configuration questions. Specifying unattended mode will cause the setup program to automatically install using default values for any options not explicitly specified.

The setup program (`setup.exe`) allows users to select any available setup options during installation of Aventail Connect. Customizer modifies the setup control file of a custom package; this file controls all of the settings within the setup package, before users receive the setup package. With a customized package, users will receive an installation package based on the administrator's defined settings. (For more information, see "Network Installation.")

As Customizer allows you to select various options to suit your setup and installation needs, the size of the setup package will vary, depending on which options you select. If size of the setup package is a concern, select setup options carefully to keep the package size manageable.

The Aventail Connect CD includes both versions of Aventail Connect (3.1 and 2.6). You can create custom packages that include one or both versions of Aventail Connect; setup will determine which version to install on each workstation. (For more information, see "What Does Aventail Connect Do?")

Aventail Connect requires a valid Aventail license file (`aventail.alf`) and one or more configuration (`.cfg`) files in order to function properly. Before installing Aventail Connect, make sure that users have these files. If users do not have a valid license file and/or configuration file(s), Aventail recommends that you include them in the installation package.

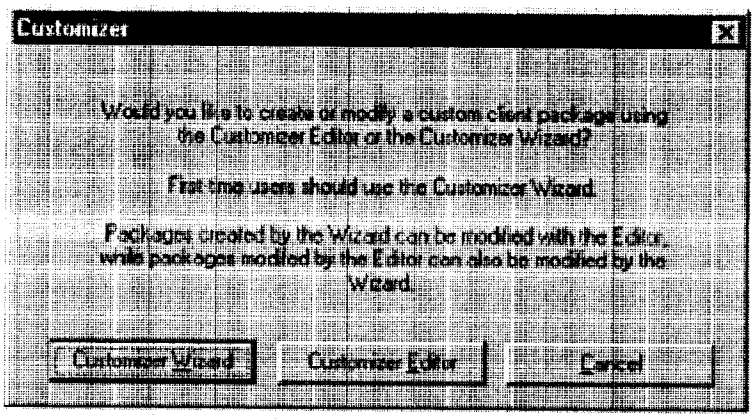
RUNNING CUSTOMIZER

The Customizer and the Aventail Connect installation package are included in the Customizer directory on the Aventail Connect CD. Before running Custom-

izer, you must copy Customizer from the Aventail Connect CD to the local drive. You must also modify the Customizer attributes so it is not read-only.

To run Customizer, double-click the **Customizer** icon in the Customizer directory. To run Customizer from your hard drive, copy the Customizer and Aventail Connect directories into a common folder on the hard drive.

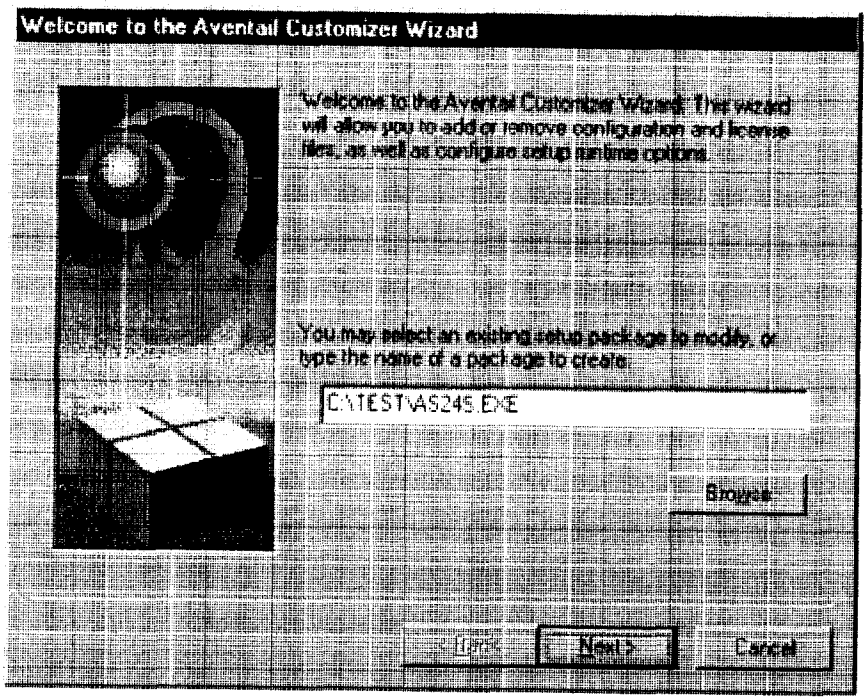
When you run Customizer, you will be prompted to select either the Customizer Wizard or the Customizer Editor.



- **Customizer Wizard:** This automated wizard walks you through the process of creating a new installation package or modifying an existing package. If you are unsure about which method to use, Aventail recommends that you use the Customizer Wizard.
- **Customizer Editor:** The Customizer Editor is a dialog box that allows you to manually enter information about the package you are creating or modifying.

CUSTOMIZER WIZARD

If you are using the Customizer Wizard to create a new setup package or modify an existing package, the Customizer Wizard will display a **Welcome...** screen, and will prompt you to enter the pathname of the package that you will be creating or modifying.



After you have specified the pathname of the package, the Customizer Wizard will prompt you to:

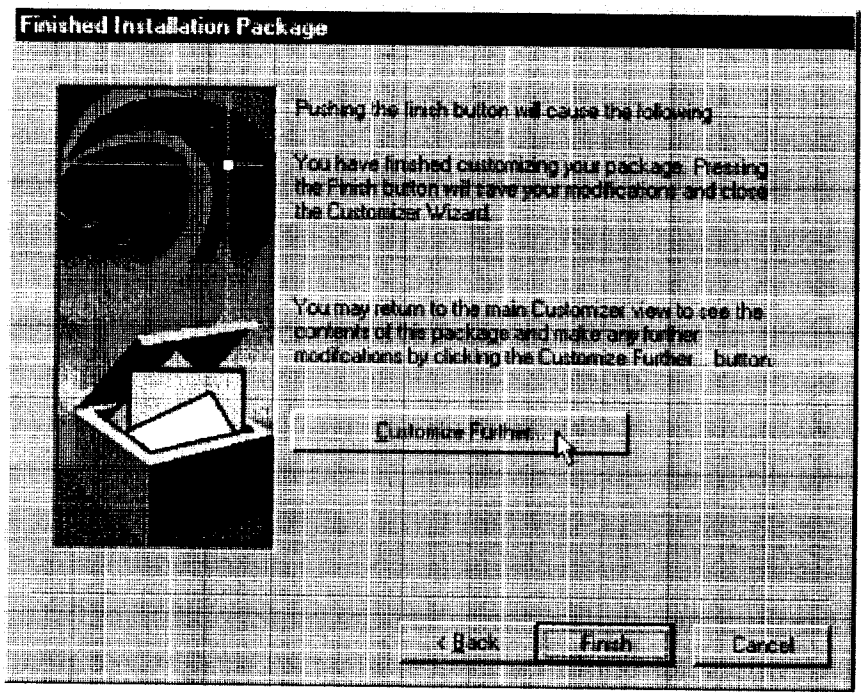
- Specify which platform(s) to support
- Add a license file, or leave an existing license file in the package
- Add or remove configuration files
- Select X.509 certificate files
- Select an extranet hosts (SEEHosts) file
- Specify a custom destination directory
- Specify whether or not to put program icons in a custom folder
- Enter command-line switches
- Specify whether or not to run setup in unattended mode
- Specify whether or not to add Aventail Connect to the startup directory
- Select any, all, or none of the following Aventail Connect components:
  - Extranet Neighborhood (Secure Extranet Explorer)
  - Configuration Tools (Config Tool and Configuration File command)
  - Diagnostic Tools (Logging Tool and S5 Ping)
  - Certificate Tools

- Install 32-bit support only (on Windows NT 3.51)

- Select any, all, or none of the following authentication modules:
  - SSL (Secure Sockets Layer)
  - CRAM (Challenge Response Authentication Method)
  - CHAP (Challenge Handshake Authentication Protocol)
  - UNPW (Username/Password)
  - SOCKS 4
  - HTTP Basic (username/password)
- Specify whether or not to run a command after setup

All of the features listed above are optional.

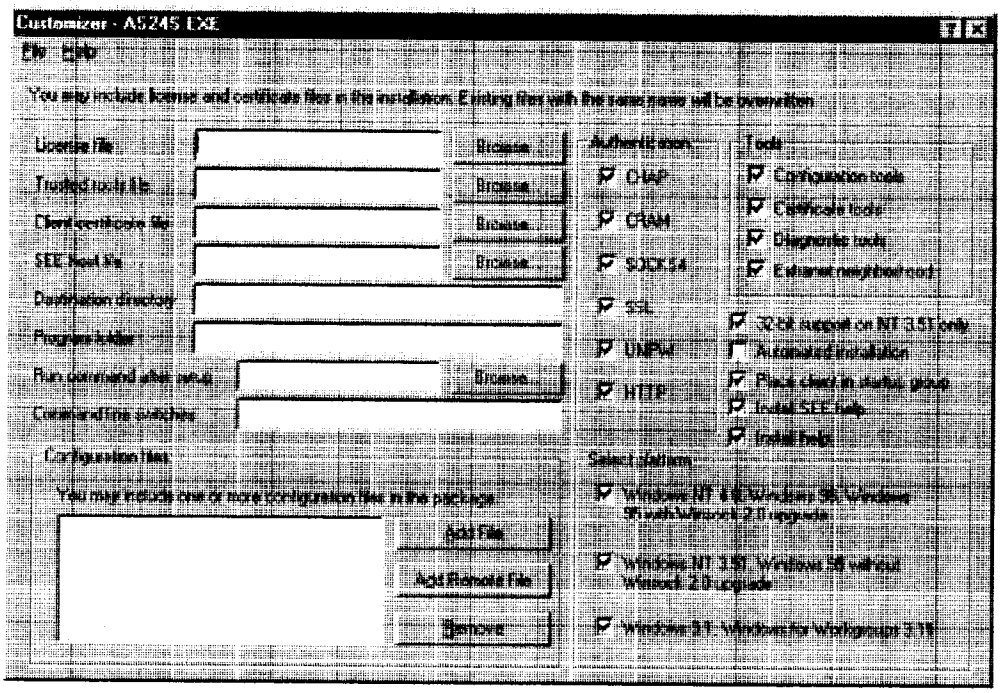
After entering or modifying the package information, the **Finished Installation Package** dialog box appears.



Clicking **Finish** saves your specifications and closes the Customizer Wizard. Clicking **Customize Further** allows you to view the **Customizer Editor** dialog box, where you can manually edit any of the information about your custom installation package.

CUSTOMIZER EDITOR

If you select the Customizer Editor as your tool to create a new setup package or modify an existing package, the **Customizer Editor** dialog box will appear. In this dialog box, you can manually enter or modify information about your custom installation package.



NOTE: *To view a list of tips on creating custom setup packages, click* ***Tips*** *on the* ***Help*** *menu in the* ***Customizer Editor*** *dialog box.*

After entering or editing your setup package information in the Customizer Editor, click **Save** (or **Save As**) on the **File** menu to save your changes. To close the **Customizer Editor** window, click **Exit** on the **File** menu.

The options in the Customizer Editor are identical to the options in the Customizer Wizard. These options are explained in the following paragraphs and tables.

Option	Settings	Default Setting
Pathname	Enter pathname	None
License file	Enter name of Aventail license file (must use `aventail.alf`)	None
Trusted roots file	Enter name of trusted roots file	None
Client certificate file	Enter name of file that contains certificate	None
Extranet (SEE) Hosts File	Enter name of extranet (SEE) hosts file	None
Destination directory	Enter name of destination directory	None
Program folder	Enter name of program folder	None
Run command after setup	Enter command to be run after setup	None
Command line switches	Enter command line switches	None
Configuration Files	Enter name(s) of local and/or remote configuration file(s) that Aventail Connect will use	None
Authentication Modules	SSL, CRAM, CHAP, UNPW, S4, or HTTP Basic	All
Tools	Configuration tools, Certificate tools, Diagnostic tools, or Extranet Neighborhood	All
32-bit support only, on Windows NT 3.51	Yes/No	Yes
Unattended setup mode/automated installation	Yes/No	No
Add to Startup Directory	Yes/No	Yes
Install SEE help	Yes/No	Yes
Install help	Yes/No	Yes
Select platform	Windows NT 4.0, Windows 98, Windows 95 with WinSock 2 upgrade, Windows 95 without WinSock 2 upgrade, Windows NT 3.51, Windows 3.1, or Windows for Workgroups 3.11	All

The setup package options are discussed below.

- **Specify path for installation:** You can specify a path for installation, or you can select the default path. The default path for 32-bit operating systems is `c:\Program Files\Aventail\Connect`.
  For 16-bit-only operating systems, the default is `c:\Connect`.

NOTE: *If you are upgrading from an earlier version of Aventail Connect, Aventail Connect will install to the same directory that the earlier version of it was installed to.*

- **Platforms:** You must specify which operating systems need to be supported in the setup package. Aventail Connect 3.1 supports Windows 95 (with the Microsoft WinSock 2 update), Windows 98, and Windows NT 4.0 (with Service Pack 3 or above, available from Microsoft). Aventail Connect 2.6 supports Windows 95 (without the Microsoft WinSock 2 update), Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51. For more information, refer to "What Does Aventail Connect Do?"
- **Trusted Roots File and Certificate File:** If you want to use server certificates, you must include the trusted roots file that contains those certificates. If you want to use client certificates, you must specify the location of the file that contains the X.509 certificate.
- **Running Setup in Unattended Mode:** Unattended setup mode simplifies distribution of numerous client configuration files. The network administrator specifies all settings before users receive the Aventail Connect setup package file. No end-user input is required because the network administrator has already selected the setup options; users simply open the package file, which will automatically install on their workstations.

NOTE: *Specifying unattended setup mode will cause the setup package to automatically install using default values for any options not explicitly specified.*

- **Adding Aventail Connect to the Startup Directory:** If you choose to add Aventail Connect to the startup directory, Aventail Connect will automatically start when Windows starts.
- **Select Tools:** Aventail Connect gives you the option to install various components, including Extranet Neighborhood/Secure Extranet Explorer (SEE), configuration tools (Config Tool and Configuration File command), or diagnostic tools (Logging Tool and S5 Ping). The default value is to install all package components.
  - **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. Extranet Neighborhood functions much like Network Neighborhood, except Extranet

Neighborhood allows you to browse, copy, move, and delete files from secured remote computers via an extranet, while Network Neighborhood displays all computers on your local network.

- **Config Tool:** The Aventail Connect Config Tool allows you to create configuration files that determine how network requests will be routed and which authentication protocols will be enabled. You can add, remove, or edit configuration files at any time. If necessary, you can create several configuration files for different users or user groups. If you want to prohibit end users from editing configuration files, do not include the Config Tool in the installation package.
- **S5 Ping:** S5 Ping allows you to use the ping and traceroute utilities, two diagnostic tools. 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.
- **Logging Tool:** The Logging Tool is a diagnostic utility that traces Aventail Connect activity. When running a trace, the Logging Tool displays errors, warnings, and information as Aventail Connect generates them. If necessary, the message list can be saved to a log file that can be used by Aventail Technical Support in troubleshooting technical problems. These traces are also useful when running Aventail Connect for the first time to ensure that network traffic is being routed appropriately.

- **Select Authentication Modules:** Aventail Connect lets you select any, all, or none of the following authentication modules: SSL, CRAM, CHAP, UN/PW, SOCKS v4, or HTTP Basic (username/password).
  - **Secure Sockets Layer:** Secure Sockets Layer (SSL) is a session-layer protocol for securing connections in a general, protocol-independent fashion.

NOTE: *In versions of Aventail Connect that do not include encryption, the Secure Sockets Layer (SSL) authentication module is not included.*

  - **CRAM:** The Challenge Response Authentication Method (CRAM) sends your username and password as clear text between extranet (SOCKS) servers, but encrypted between servers that support CRAM. Typically, CRAM subauthenticates within SSL, which provides both encryption and credential caching options.

NOTE: *In versions of Aventail Connect that do not include encryption, the CRAM authentication module is not included.*

- **CHAP:** The Challenge Handshake Authentication Protocol (CHAP) sends your username and password encrypted across the network to the destination server.
- **Username/Password:** The RFC 1928 (Internet standards document) Username/Password (UNPW) authentication protocol sends your username and password in clear text across the network to the destination server.
- **SOCKS 4 Identification:** Aventail Connect includes backward compatibility for the SOCKS 4 protocol. SOCKS 4 does not support password authentication, so only your username is sent, unencrypted, to the SOCKS server along with your connection request.
- **HTTP Basic (Username/Password):** The HTTP Basic authentication module enables username/password authentication against HTTP proxies that implement the RFC 2068 HTTP Basic authentication protocol.

NOTE: *Not all versions of Aventail Connect have encryption enabled.*

- **Configuration Files:** Aventail Connect needs at least one configuration (`.cfg`) file in order to function properly. The configuration file contains all of the authentication and traffic routing instructions that you specify. You can include one or more configuration files in the setup package; however, each configuration file must have a different name. If you include only one configuration file in a setup package, Aventail Connect will automatically use that configuration file. If, however, you include multiple configuration files, Aventail Connect will prompt users to select a configuration file at startup.

  You can include local configuration files, remote configuration files, or a combination of both. Local configuration files are included in the setup package and are installed on users' machines. If you include remote configuration files, pointers to those files are included in the package; the remote configuration files remain in their original location on the network, where they can be shared by multiple users.

  If your setup package does not already contain a configuration file, you can add a configuration file to the package. If your setup package contains one or more configuration files, you can remove or replace any or all of the existing configuration files, or you can leave them, unchanged, in the package. If you are upgrading from an earlier version of Aventail Connect, you may not need a new configuration file.
- **License Files:** Aventail Connect requires a valid license file in order to function properly. If your setup package contains a license file, you can remove or replace the existing license file, or you can leave it, unchanged, in the package. If your setup package does not contain a

license file, you can add one to the packaged Aventail license file, `aventail.alf`.

CAUTION: Aventail Connect 3.1 and 2.6 use a different license (`.alf`) file format than earlier versions of Aventail Connect (VPN Client or AutoSOCKS) did. If you are upgrading from an earlier version of Aventail Connect (v2.42 or earlier), you must include a new Aventail license file.

- **Extranet (SEE) Hosts Files:** Secure Extranet Explorer (SEE) allows you to browse remote computers using Extranet Neighborhood. SEE requires a hosts file that specifies which Windows domains, WINS servers, and other computers are available in Extranet Neighborhood. The extranet hosts (SEEHosts) file is contained in the setup package. If you install SEE, this file is placed in the target directory. If you do not include a hosts file in the setup package, Aventail Connect will automatically create a hosts file on users' machines the first time they open Extranet Neighborhood. (Available only in Windows 95, Windows 98, and Windows NT 4.0.)

CREATING, LOADING, AND SAVING PACKAGES

You can create, load, or save custom setup packages through either the Customizer Editor or the Customizer Wizard.

To create a new package

There are two ways to create a new custom setup package:

- In the **Customizer Editor** window, select **File | New**.

-OR-

- Type the filename of a new package in the first window of the Customizer Wizard and click **Next**.

To load a package

There are two ways to load an existing setup package:

- In the **Customizer Editor** window, select **File | Open**, and then enter the filename of the package you want to load

-OR-

- Type the filename of the package in the first window of the Customizer Wizard and then click **Next**.

When you load a package, Customizer reads the setup control file to determine what information the package contains. Customizer uses this information to populate the **Customizer Editor** window. Customizer also reads the configuration file(s) into memory; configuration files are stored in memory to facilitate adding them to and removing them from a package.

To save changes to a package

There are two ways to save changes to a setup package:

- After making the desired changes to the package, click **Save** (or **Save As**) on the **File** menu in the **Customizer Editor** window

-OR-

- Click **Save Package** in the final window of the Customizer Wizard.

CUSTOMIZER TIPS

The following tips will help you use the Aventail Customizer more efficiently.

- **Keep the package size small:** You can control the size of your custom setup packages by selecting components carefully. To keep the package as small as possible, include only the options that you need, and support only the platforms (e.g., Windows 98, Windows NT 4.0, etc.) that your users work with. You may find that creating two separate, smaller packages is preferable to creating one larger package. For example, you might create one package that supports Windows 98 and Windows NT 4.0 operating systems, and another separate package that supports Windows 3.1 and Windows 95 operating systems.
- **Use descriptive package names:** When naming setup packages, assign descriptive, recognizable names that will help users identify the setup packages.
- **Select components carefully:** If you include the Config Tool in the package, users will be able to view and modify the settings in the Config Tool. Aventail recommends that, in most cases, you do not include the Config Tool in your custom setup package(s). Excluding options such as the Config Tool will eliminate users' ability to modify your settings, and will keep the package size smaller. However, the S5 Ping and Logging Tool utilities are useful diagnostic tools, and Aventail recommends including these options in the setup package whenever possible.
- **Install Aventail Connect 2.6 on Windows 95:** By default, Windows 95 does not support WinSock 2, but you can upgrade it to support WinSock 2 with a Microsoft patch. (The patch, `w95ws2setup.exe`, is available from Microsoft, at **http://www.microsoft.com/Windows95/downloads/contents/wuadmintools/s_wunetworkingtools/W95Sockets2/default.asp**. However, this procedure adds an extra step to the installation and setup process. Unless users need the MultiProxy feature, which is available only in Aventail Connect 3.1, Aventail recommends that you install Aventail Connect 2.6 rather than 3.1 on machines running the Windows 95 operating system.
- **Include a hosts file:** If you install Secure Extranet Explorer (SEE) without also installing a corresponding hosts file, SEE will automatically create a hosts file the first time that users open SEE. If you want to control which hosts users can view, Aventail recommends that you include a hosts file in the custom setup package.

- **Include a license file:** Aventail Connect requires a valid license file (`aventail.alf`) to function properly. Aventail Connect 3.1/2.6 uses a different license file than earlier versions of Aventail Connect (VPN Client or AutoSOCKS) did. If you are upgrading from an earlier version of Aventail Connect (v2.42 or earlier), you must use the new Aventail license file, `aventail.alf`. Including this license file in the custom setup package is a simple way to install the license file.
- **Test each custom package:** Aventail recommends that you thoroughly test each custom setup package before distribution to users.

CONFIGURING AVENTAIL CONNECT

Create configuration files using the Config Tool or the Configuration wizard. You can launch either during the Aventail Connect installation or any time you want to add, modify, or remove a configuration file.

The steps for creating a new configuration file are:

1. Define the SOCKS servers
2. Define the destinations (networks and hosts)
3. Specify redirection rules
4. Enter Name Resolution information (optional)
5. Manage authentication modules
6. Enable password protection (optional)

These procedures are described in the text below.

To launch the Config Tool

The Config Tool opens with the **Open Aventail Connect Configuration File** dialog box. After you select a configuration file or enter a new file name, the main window of the Config Tool appears.

1. Select the **Yes, I want to configure Aventail Connect** box in the **Setup Complete** dialog box (during installation).

-OR-

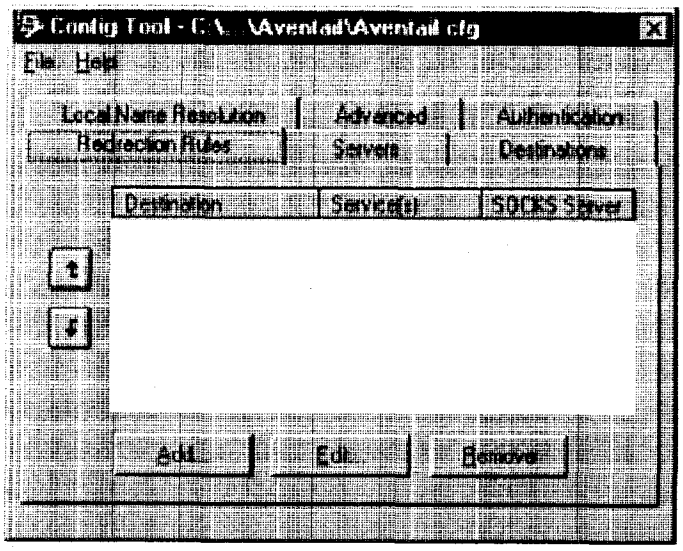
Right-click the **Aventail Connect** icon in the taskbar and click **Config Tool** (Windows 95, Windows 98, or Windows NT 4.0 programs menu option), or double-click the **Config Tool** icon in the Aventail Connect program group (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).

2. If you are creating a new configuration file, enter a name for the configuration file

-OR-

Select the configuration file you want to open.

This displays the main window of the Config Tool.



The **Config Tool** window contains six tabs. The properties defined on each tab can be edited at any time.

Tab	Function
Servers	Defines the extranet (SOCKS) server(s).
Destinations	Specifies the network and host addresses that will be routed through the SOCKS server(s).
Redirection Rules	Specifies how network requests are routed to the SOCKS server(s).
Name Resolution	(Optional) Specifies hostnames that will be resolved by the local workstation.
Authentication	Enables, disables, and sets properties for the authentication modules.
Advanced	Enables/disables extranet (SOCKS) traffic through successive SOCKS servers, enables/disables the Application Exclusion/ Inclusion List, secures selected applications, and sets credential cache timeouts.

You can change the width of any of the fields on the tabs by positioning the cursor over the dividing line between the fields on the field bar. When the cursor changes to a double-headed arrow, click and drag to resize the field.

Aventail Connect 3.1 allows you to create or modify a configuration file and then immediately use it, without needing to restart Aventail Connect and any Aventail-processed applications. When you modify a configuration file, Aventail Connect can re-read the updated configuration file; all applications being processed by

Aventail Connect will then immediately begin using the new configuration information.

When you make a modified configuration file active, Aventail Connect will save the current (modified) configuration file, update the registry, and load the selected configuration file. Aventail Connect will begin using the modified configuration file with any subsequent TCP connection requests, and/or any subsequent UDP activity.

NOTE: *The configuration file "refresh" feature is supported in Aventail Connect 3.1 only. It is not supported in Aventail Connect 2.6. To activate modified configuration files in Aventail Connect 2.6, you must first shut down and restart Aventail Connect and all applications being processed through Aventail Connect.*

To load a modified configuration file for immediate use

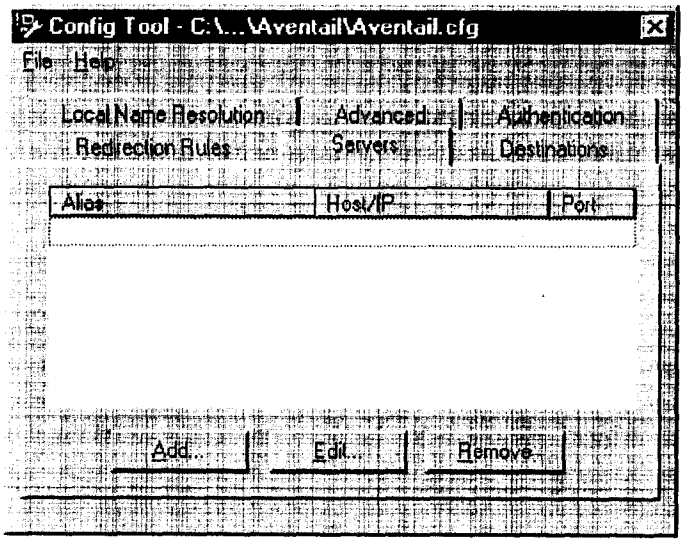
- With the newly modified configuration file open, select **Make Active** from the **File** menu of the Config Tool

  -OR-

- From the system tray menu, select **Configuration File**, and select (or enter the name of) the configuration file that you want to use. Click **OK**.

DEFINE AN EXTRANET (SOCKS) SERVER

SOCKS servers are defined on the **Servers** tab in the Config Tool.



Field	Definition
Alias	The name you assign to the server.
Host/IP	The hostname or IP address of the server.
Port	The port on which the server is listening.

Aventail Connect 3.1 allows you to set a server fallback timeout for every Aventail ExtraNet Server. If a primary SOCKS server is down, or otherwise unable to accept connections, Aventail Connect can fall back to a secondary server. You can set the server fallback timeout, in seconds, on a server-by-server basis. If you do set a server fallback timeout, each connection to a primary server must be completed within the specified length of time or else the connection will fall back to the secondary server.

NOTE: *Server fallback timeouts are supported in Aventail Connect 3.1 only. You cannot set a server fallback timeout in Aventail Connect 2.6; you must let the TCP/IP stack time out.*

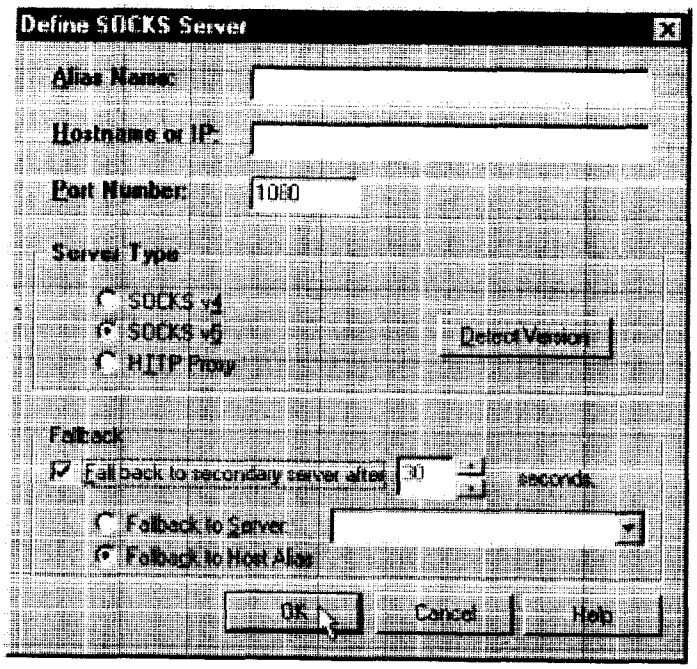
NOTE: *Aventail Connect can fall back to only one server. For example, Aventail Connect could fall back from Server A (primary server) to Server B (secondary server). Aventail Connect could not, however, fall back from Server A to Server B to Server C.*

During normal operation, if you configure Aventail Connect to fall back to a secondary server, connections will be directed to the primary server. If the primary server does not respond or accept the connection by the end of the fallback timeout period, the connection will be redirected to the secondary server. If the secondary server accepts the connection, all subsequent connections will automatically be directed to the secondary server. The secondary server is generally meant to be used only when the primary server is unable to accept connections. To prevent the secondary server from automatically becoming the default server for all subsequent connection, Aventail Connect will check the primary server's status every ten minutes. If the primary server is back up and able to accept connection, all subsequent connections will be routed through the primary server.

CAUTION: *Do not enable the server fallback option if you are using plug gateways.*

To add an extranet (SOCKS) server

1. On the **Servers** tab, click **Add...**. The **Define SOCKS Server** dialog box appears.



Field	Definition	
Alias Name	User-friendly alias for extranet (SOCKS) server.	
Hostname or IP	Actual hostname or full numeric IP address for SOCKS server.	
Port Number	SOCKS server port. Default value is 1080.	
Server Type	SOCKS v4	SOCKS Version 4.0.
	SOCKS v5	SOCKS Version 5.0.
	HTTP Proxy	HTTP proxy server.
	Detect Version	Detect SOCKS version number.
Fallback	Fall back to secondary server after x seconds	Server fallback timeout period (in seconds).
	Fall back to Server:	SOCKS server alias for redundant server.
	Fall back to Host Alias	Use DNS records for redundancy.

2. In the **Alias Name** box, type a user-friendly alias for the extranet (SOCKS) server. Do not leave this box blank.
3. In the **Hostname or IP address box**, type the actual hostname of the SOCKS server or its IP address.
4. In the **Port Number** box, type the extranet server's port number. If you do not enter a value, it defaults to the standard SOCKS port 1080.
5. Under "Server Type," select the version of SOCKS supported by the server. If you are unsure of the version, click **Detect Version**.

NOTE: *Typically you should select **SOCKS v5** unless the server can support only SOCKS v4.*

6. If you want to use a fallback server, select **Fall back to secondary server after...** under "Fallback." Either select **Fall back to server** and directly specify an extranet server for redundancy, or select **Fall back to host alias**. Select or enter, in seconds, the fallback timeout period. Click **OK**.

To edit extranet (SOCKS) server properties

- Select the extranet server you want to edit and click **Edit**.

  The **Define SOCKS server** dialog box appears with the selected server data filled in. Edit any of the information, and then click **OK**.

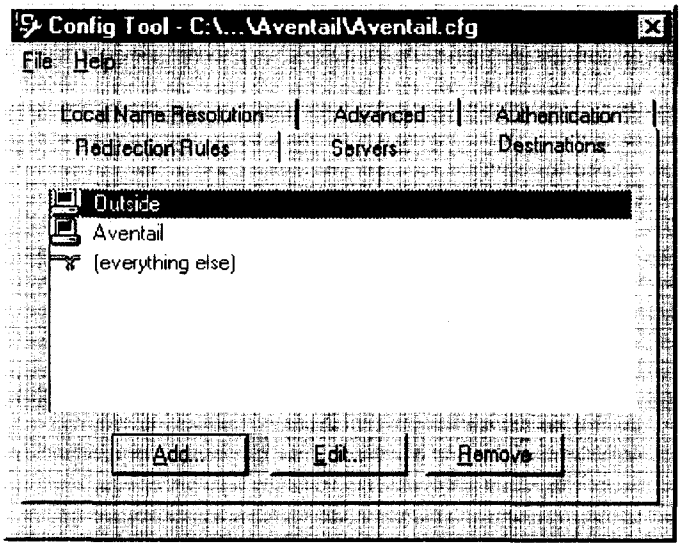
To remove an extranet (SOCKS) server definition

- Select the extranet server you want to remove and click **Remove**.

  The server is deleted from the list. Corresponding redirection rules will also be deleted.

DEFINE A DESTINATION

Destinations are defined on the **Destinations** tab in the Config Tool.



After one or more SOCKS servers are defined, add destinations to be routed through them.

NOTE: *The "(everything else)" destination refers to all network and host addresses not otherwise defined. You cannot delete or modify "(everything else)."*

WILDCARDS IN HOSTNAME DEFINITIONS

Aventail Connect supports the use of wildcard characters in destination hostnames. You can use wildcards when defining named destinations (hostnames); you cannot use wildcards when defining numerical destinations, such as IP addresses or subnet masks.

Acceptable wildcard characters are "?" and "*" (where "?" represents one character, and "*" represents any number of characters). For example:

`e*tra.in.aventail.com` **matches** `extra.in.aventail.com`
`e?tra.in.aventail.com` **matches** `extra.in.aventail.com`
`e?ra.in.aventail.com` **does NOT match** `extra.in.aventail.com`

You can use any combination of "?" and "*" characters between each set of periods. However, each section must contain at least one non-wildcard character. For example, the following destination names would be allowed:

```
e?t?a.in.aventail.com
*xtr?.in.aventail.com
e???a.in.ave*.com
e*.in.*tail.com
```

The following destination names, however, would not be allowed:

```
extra.*.aventail.com
*.*.aventail.com
extra.in.*.com
```

CAUTION: *You cannot use a wildcard character, or a series of wildcard characters, to represent multiple sections. Any wildcard character in a section can represent characters within that section only. For example:*

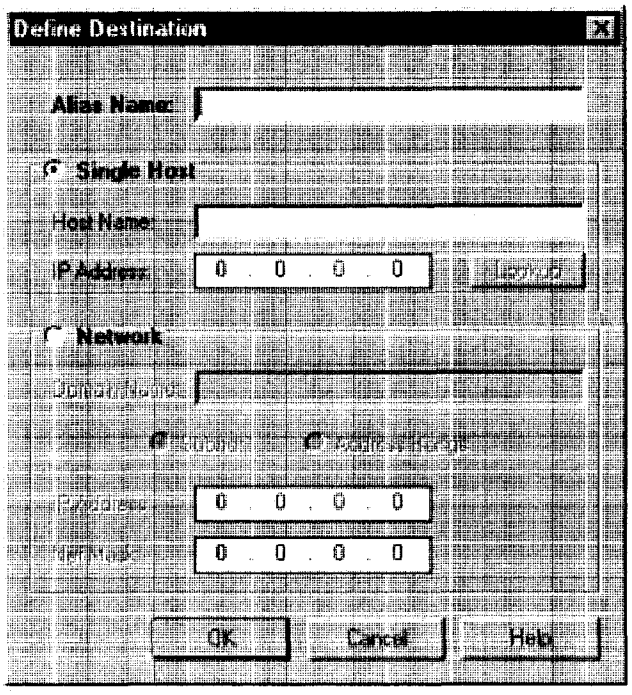
`e*.in.aventail.com` ***matches*** `extra.in.aventail.com`
`e*.aventail.com` ***does NOT match*** `extra.in.aventail.com`

To add a destination

In the **Define Destination** dialog box, you can define subnets, individual host computers, or IP address ranges, and set up rules about redirecting some or none of the IP traffic to these defined destinations.

1. On the **Destinations** tab, click **Add...**.

The **Define Destination** dialog box appears.



Field	Definition	
Alias Name	User-friendly alias for destination network or host	
Single Host	A specific destination computer	
	Hostname	Actual name of destination network or host
	IP Address (*optional*)	Full numeric IP address
	Lookup	Look up IP address
Network	One or more computers in a network	
	Domain Name	Domain of the network
	Subnet (*optional*)	IP address and netmask address
	Address Range (*optional*)	Beginning and ending IP addresses From Starting IP address To Ending IP address

CAUTION: *The **IP Address**, **Subnet**, and **Address Range** fields are all optional. However, in order to apply redirection rules when connecting by IP address, you must enter IP address and subnet information.*

2. In the **Alias Name** box, type a user-friendly alias for the destination network or host.
3. Select either the **Single Host** or **Network** option:
   - Under "Single host," type the actual name of the host system and/or its full, numeric IP address. If you do not know the host's IP address, click **Lookup** to search for it.

-OR-

   - Under "Network," type the domain of the network and then, if applicable, select either **Address Range** or **Subnet**.

Use	To
Address Range	Enter a starting and ending IP address. All addresses between the two will be included as part of the destination. For example, a starting IP address of 192.1.1.0 and an ending IP address of 192.1.1.255 would include all hosts of the 192.1.1.x subnet.
Subnet	Enter an IP address and a netmask address. This is another way to specify a group of destinations. For example, an IP address of 192.1.1.0 and a net mask of 255.255.255.0 defines the same address range as shown above.

To edit a destination

- Select the destination you want to edit and click **Edit...**.

  The **Define Destination** dialog box appears with the selected destination data filled in. Edit the data as necessary.

To remove a destination

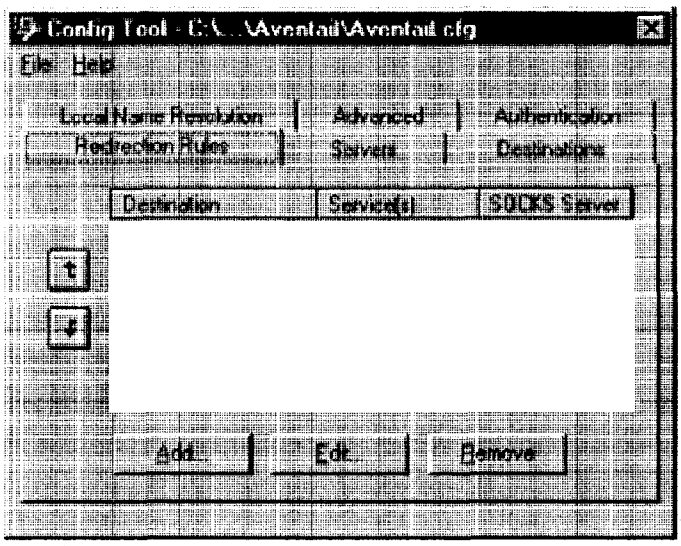
- Select the destination you want to remove and click **Remove**.

  The destination is deleted from the list. The corresponding redirection rules will also be deleted.

ENTER REDIRECTION RULES

Once servers and destinations are defined, you can specify how you want Aventail Connect to redirect (or deny) access to various hosts and services such as e-mail, FTP, and HTTP.

Redirection rules are specified on the **Redirection Rules** tab in the Config Tool.



Field	Definition
Destination	Destinations defined on the **Destinations** tab
Service	Type of Internet traffic
Proxy Redirection	Specify how to redirect traffic

You can change the width of any of the three fields by moving the cursor to the dividing line between the fields on the field bar. When the cursor changes to a double-headed arrow, click and drag to resize the field.

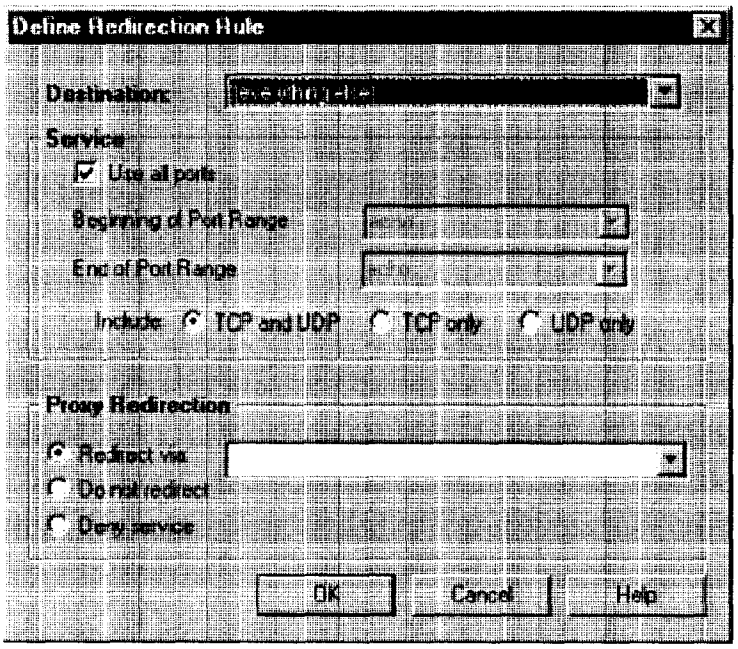
To add a redirection rule

As you add destinations, use the arrow buttons to prioritize them. List the most specific rules first and the general rules last.

NOTE: *Aventail Connect scans the list from the top down and uses the first matching rule it finds, so it is important to list the most specific rules first.*

1. On the **Redirection Rules** tab, click **Add**.

The **Define Redirection Rule** dialog box appears.



Field	Definition	
Destination	Host or server destination for message traffic.	
Service	Type of Internet traffic	
	Use all ports	Apply the defined rule to all ports.
	Beginning of port range	Apply the defined rule to this range of ports.
	End of port range	
	TCP and UDP	Apply the defined rule to both TCP and UDP traffic.
	TCP only	Apply the defined rule to TCP traffic only.
	UDP only	Apply the defined rule to UDP traffic only.
Proxy Redirection	Specify how to redirect traffic.	
	Redirect via	Redirect all traffic through the extranet server selected from the list.
	Do not redirect	Route traffic directly to the specified destination without being redirected through SOCKS.
	Deny service	Deny access to the specified destination. The network connection is blocked locally instead of at the server level.

2. Select a destination from the **Destination** list.
3. Under "Service," select the **Use all ports** box to apply the rule to all services. Otherwise, select a range of ports. To select a single port, enter that port number in both the **Beginning of port range** and **End of port range** boxes.
4. Under "Proxy Redirection," select one of three redirection options.

*CAUTION: If you select **Deny Service** and the user has edit control of the configuration file, the option can be circumvented by quitting Aventail Connect or by changing the option in the dialog box.*

To edit a redirection rule

- Select the redirection rule you want to edit and click **Edit...**.

  The **Define Redirection Rule** dialog box appears with the selected data filled in. Edit any of the information.

To remove a redirection rule

- Select the redirection rule you want to remove and click **Remove**.

  The redirection rule is deleted from the dialog box.

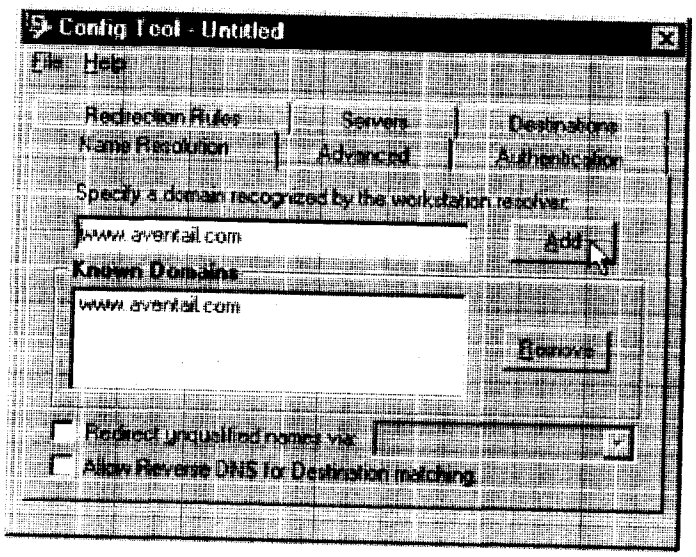
DEFINE NAME RESOLUTION

Name Resolution instructs Aventail Connect to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how Aventail Connect performs name resolution.

The local workstation resolver is the name resolution component of the local TCP/IP stack. This feature acts as a shortcut; hostnames matching the strings defined in the **Name Resolution** dialog box are passed to the local resolver for name resolution instead of being proxied through the SOCKS v5 server.

For example, if **aventail.com** is added to the Defined Strings list, then a workstation attempting to connect to **www.aventail.com** would perform hostname resolution using the local TCP/IP stack.

Name Resolution is specified on the **Name Resolution** tab in the Config Tool.



Field	Definition
Specify a domain recognized by the workstation resolver	New domain name
Known Domains	List of domain names that can be resolved locally
Redirect unqualified names via	Pass through unqualified hostnames to the local resolver
Allow Reverse DNS for destination matching	Enable Reverse DNS (converts IP addresses into hostnames)

To add a local domain name

- On the **Name Resolution** tab, type the new name in the **Specify a domain** box and click **Add...**.
- If necessary, select **Allow Reverse DNS for destination matching**.

  The new name is moved into the **Known Domains** box. It is now active.

CAUTION: *The reverse DNS process can create unexpected delays, causing Aventail Connect to behave unpredictably. Aventail recommends that you do not enable this option unless you specifically require the Reverse DNS functionality.*

To remove a local domain name

- Select the domain name you want to remove from the **Known Domains** box and click **Remove**.

  The domain name is removed from the list.

MANAGE AUTHENTICATION MODULES

SOCKS v5 servers often require user authentication before allowing access. Aventail Connect authentication modules display dialog boxes that prompt users to enter username and password information as well as other authentication credentials.

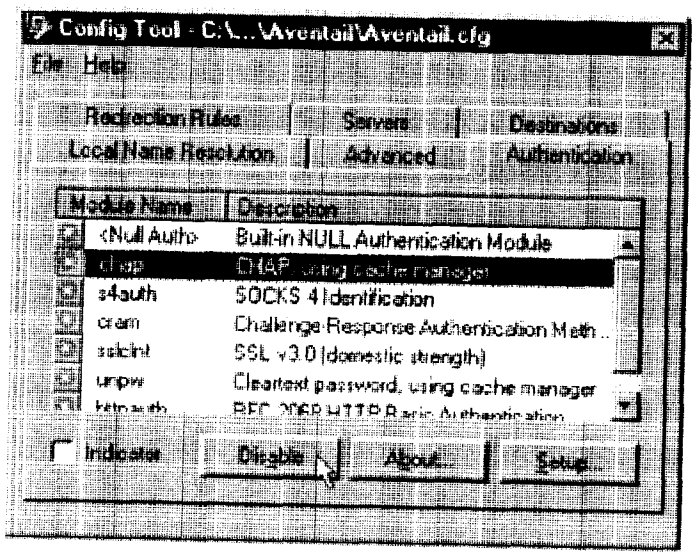
NOTE: *Not all versions of Aventail Connect have encryption enabled.*

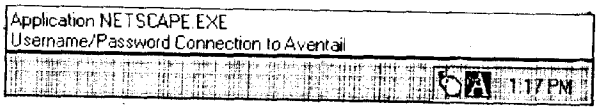
The current Aventail Connect authentication modules are SOCKS v4 Identification, Username/Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Each of these authentication modules supports an Aventail Connect feature known as credential caching. Credential caching retains your authentication credentials once the extranet server has accepted them. Using credential caching, you can enter your credentials for an extranet server once per Aventail Connect session, rather than once for each individual connection (a tedious task for applications such as WWW browsers).

Aventail Connect can cache authentication credentials in memory, based on the option you select in the **Authentication** dialog box. Memory caching stores the credentials for the current session only. When you restart Aventail Connect or Windows, the memory cache is flushed and you must reenter your credentials as prompted.

SEE ALSO: *For additional information on credential caching, see "Credential Cache Timeouts" in the "Advanced Tab Options" section of this Administrator's Guide.*

Authentication modules are managed and configured through the **Authentication** tab in the Config Tool.



Field	Definition
Module Name	The name of the authentication module on disk. `<Null Auth>` indicates that no authentication module will be used.
Description	The description of the authentication method.
Indicator	Check this option to display network traffic passing through a selected authentication/encryption module. See the example below (for Windows 95, Windows 98, and Windows NT 4.0). 

Each authentication module includes its own module-specific configuration. To view or edit a module's configuration, select the module from the list on the **Authentication** tab and then click **Setup**. An options dialog box for the specific module will appear.

Enable and disable authentication modules with the **Disable/Enable** button. By default, the modules are all enabled. The green button next to the module name indicates an active module. This is the default state of all the modules. The green button changes to red when you disable the module.

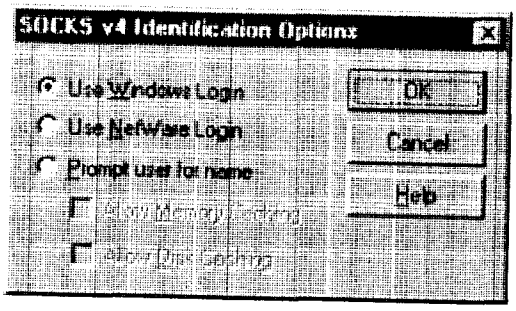
To configure the SOCKS 4 Identification module

Aventail Connect includes backward compatibility for the SOCKS 4 protocol. SOCKS 4 does not support password authentication, so only your username is sent unencrypted to the extranet (SOCKS) server along with your connection request.

Your username is determined by entries in the **SOCKS 4 Identification Module Configuration** dialog box.

1. On the **Authentication** tab in the Config Tool, click **s4auth** (SOCKS v4 Identification) and click **Setup**.

   The **SOCKS 4 Identification Options** dialog box appears.



Field	Description	
Use Windows Login	Identify users by their Windows Login names.	
Use NetWare Login	Identify users by their Novell NetWare Login names.	
Prompt user for name	Identify users by the names they enter for this specific purpose.	
	Allow Memory Caching	Stores credentials in memory for this session only. Cache is flushed upon restart; credentials must be reentered as prompted.
	Allow Disk Caching	This option is currently unavailable. (Stores credentials on disk for future sessions.)

2. When you select the **Prompt user for name** option, you must also select the desired caching option. (Currently only Memory Caching is available.)
3. After making appropriate selections, click **OK**.

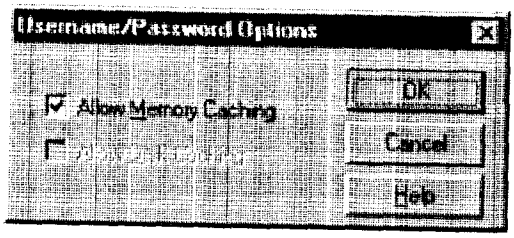
   The dialog box closes and the Config Tool reappears.

To configure the Username/Password authentication module

Aventail Connect supports the RFC 1928 (Internet standards document) username and password authentication protocol. This authentication method sends your username and password *in cleartext* across the network to the destination server. The **Username/Password authentication module** dialog box contains only credential caching options.

1. On the **Authentication** tab in the Config Tool, select **unpw** and click **Setup**.

   The **Username/Password Options** dialog box appears.



Field	Description
Allow memory caching	Stores credentials in memory for this session only. Cache is flushed upon restart; credentials must be reentered as prompted.
Allow Disk Caching	This option is currently unavailable. (Stores encrypted credentials on disk for future sessions.)

2. The selection defaults to **Allow Memory Caching**. Click **OK**.

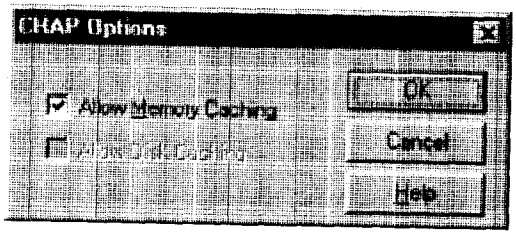
   The dialog box closes and the Config Tool reappears.

To configure the CHAP authentication module

Aventail Connect supports the Challenge Handshake Authentication Protocol (CHAP). This authentication method sends your username and password *encrypted* across the network to the destination server. The **CHAP authentication module** dialog box contains only credential caching options.

1. On the **Authentication** tab in the Config Tool, select **chap** and click **Setup**.

The **CHAP Options** dialog box appears.



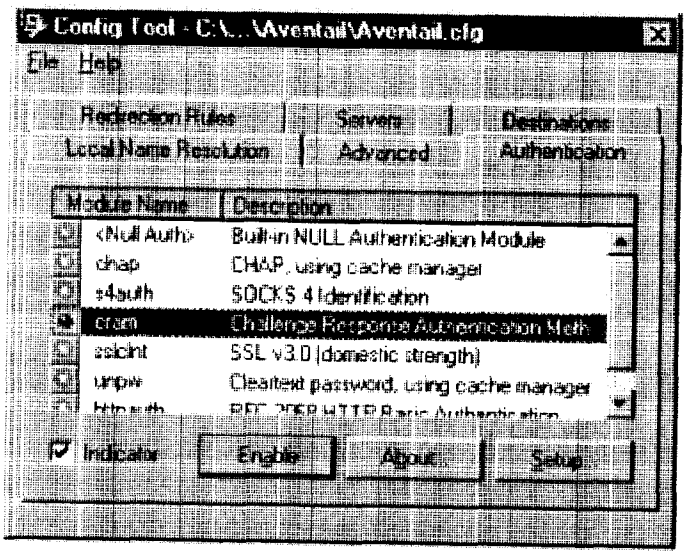
Field	Description
Allow memory caching	Stores credentials in memory for this session only. Cache is flushed upon restart; credentials must be reentered as prompted.
Allow disk caching	This option is currently unavailable. (Stores encrypted credentials on disk for future sessions.)

2. The selection defaults to **Allow Memory Caching**. Click **OK**.

   The dialog box closes and the Config Tool reappears.

To configure the CRAM authentication module

Aventail Connect supports the Challenge Response Authentication Method (CRAM). This authentication method sends your username and passcode as cleartext between extranet (SOCKS) servers, but *encrypted* between servers that support CRAM. Typically, CRAM subauthenticates within SSL, which provides both encryption and credential caching options.



You do not need to configure the CRAM authentication module. You can enable/disable it, by clicking on the **Disable/Enable** button. The button at the left of the module name will change from green to red, accordingly.

To configure the SSL security module

Aventail Connect supports Secure Sockets Layer (SSL) v3.0, a session-layer protocol for securing connections in a general, protocol-independent fashion.

NOTE: *Currently, SSL is a TCP-only enhancement. When using SSL with User Datagram Protocol (UDP) applications, bulk data is passed without encryption.*

Normally SSL servers are required to have an RSA key pair and a certificate. Aventail uses an RSA algorithm to create a cryptographic system: a private key (which, as the name suggests, is kept absolutely private and never shared) and a public key (which is widely published).

NOTE: *In versions of Aventail Connect that do not include encryption, SSL is not available.*

However, as the client, you normally must then establish some kind of relationship between your RSA public key and the identity of the server, so that somebody else cannot create their own RSA key information and use it to impersonate your server. *Certificates* establish this relationship. A certificate is essentially an electronic "statement" that verifies that a certain RSA public key is associated with a particular name.

Certificates are issued by a Certification Authority (CA), and are linked together to form a construct called a certificate *chain of authorities*, each one having a previous entity vouching for its identity. In practice, chains generally include two certificates: one confirming the identity of the server, and the other—a "root" certificate—containing the identity and public key of the CA.

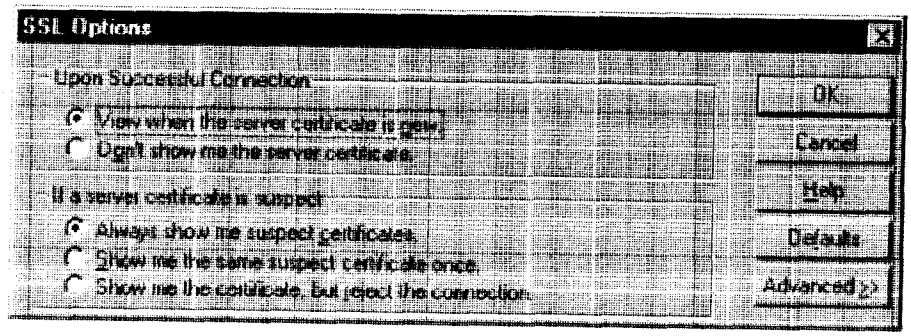
Certificates contain special integrity checks and electronic signatures that verify that the certificate is genuine, was issued by a certification authority, and was not tampered with. Anybody can issue a certificate that says anything; the client must know who issued the certificate, and have some trust relationship in order to believe that it is in fact true. The client has a list of trusted CAs. A set of certificate chains can be structured as a tree, with new certificates stemming from old ones. A base CA is sometimes called the "root" or "trusted root" of this tree.

It is becoming common practice for both clients and servers to exchange certificate information. However, in Aventail Connect the client-side of this exchange is transparent. The client only needs to deal with the information from the server certificate and this is done through the SSL module.

The **SSL module** dialog box contains an initial set of options regarding the viewing of certificates.

1. On the **Authentication** tab in the Config Tool, select **sslclnt** (SSL v3.0) and click **Setup**.

   The **SSL Options** dialog box appears.



Field		Description
Upon Successful Connection		The certificate is valid.
	View when the server certificate is new.	Upon successful connection, display the server certificate if it has not been displayed during the current session.
	Do not show me the certificate.	Never display a valid server certificate.
If a server certificate is suspect		The certificate may not be valid.
	Always show me suspect certificates.	Each time Aventail Connect suspects a certificate may not be valid, show the certificate.
	Show me the same suspect certificate once.	Once a suspect certificate has been accepted by the user, do not display it again.
	Show me the certificate, but reject the connection.	Reject the connection, but display the suspect certificate.

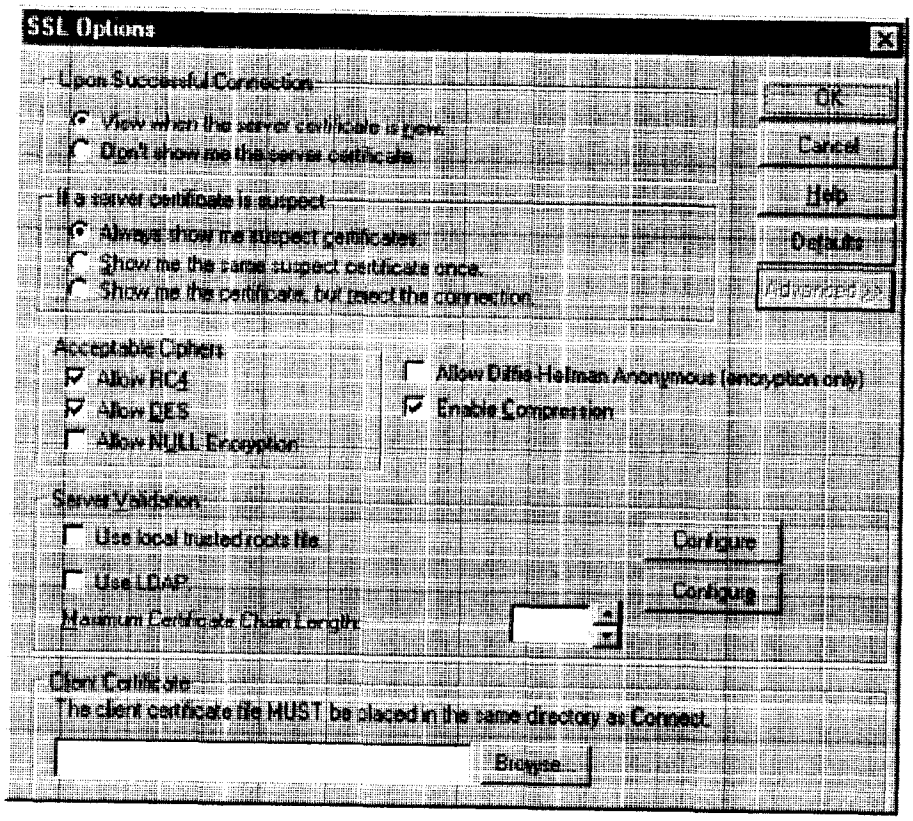
2. Select an action that Aventail Connect must take once it accepts the validity of the server certificate. (Under normal circumstances, the server will provide Aventail Connect with a certificate to match one of Aventail Connect's trusted roots, if any exist):
   - **View when the server certificate is new:** Aventail Connect displays the certificate the first time it is seen. The certificate will not appear on subsequent connections to the same extranet server.
   - **Do not show me the server certificate:** Aventail Connect will never display a valid certificate.
3. Select an action that Aventail Connect must take if it receives a server certificate that is suspect:
   - **Always show me suspect certificates**: Aventail Connect will display suspect certificates each time they are received. The **Certificate** dialog box will appear for each new connection to the server(s) sending a suspect certificate. (This option allows you to continue the connection despite the fact that the certificate is questionable.) The SSL module authenticates the server's certificate based on the following questions:
     - Is the certificate valid?
     - Did a trusted certificate authority (CA) issue the certificate?
     - Is the name established by the certificate the same as the name of the server for this connection?

   If a certificate does not pass all three tests, it is considered a suspect certificate.
   - **Show me the same certificate once:** Aventail Connect will display a suspect certificate the first time that it is received. If you choose to

maintain the connection, the questionable certificate will not be displayed again during the current session.

- **Show me the certificate, but reject the connection:** Aventail Connect will reject a connection if the certificate is suspect. It will display the certificate to allow you to view it.

4. Click **Advanced** in the dialog box to show the acceptable cipher (a cryptographic algorithm used to encrypt the data stream) options.



Field	Description	
Acceptable Ciphers		
Allow RC4	Offer the RC4 cipher to the server.	
Allow DES	Offer the DES cipher to the server.	
Allow NULL Encryption	Do not encrypt using SSL. SSL will be used to authenticate only.	
Allow Diffie-Hellman Anonymous	Do not authenticate the server; only do encryption.	
Enable Compression	Use SSL compression to improve performance when slower connections are detected.	
Server Validation		
Trusted Roots	Use a trusted roots file to validate trusted certificate chain roots. *NOTE: The trusted roots file MUST be placed in the same directory as the Aventail Connect configuration file.*	
	Configure	Configure trusted roots
LDAP	Use an LDAP server to validate trusted certificates.	
	Configure	Configure LDAP
Maximum Chain Length	Specify the maximum allowable certificate-chain length.	
Client Certificate	Select a client certificate file. *NOTE: The client certificate MUST be placed in the same directory that Aventail Connect was installed to.*	
	Browse	Select the specific file

During the initial SSL connection, the client and the server negotiate which cipher to use. Checking a particular cipher in the dialog box does not mean that it will be used. Instead, each checked cipher is *offered* to the server, but the server determines which cipher to use. If the server requires a cipher that is not selected in this dialog box, the authentication will fail.

Any or all of the acceptable cipher options can be selected:

- **Allow RC4:** Aventail Connect encrypts the information using the RC4 cipher.
- **Allow DES:** Aventail Connect encrypts the information using the DES cipher.
- **Allow NULL Encryption:** Aventail Connect allows the server to select *no* encryption. Message integrity is still assured, but the data will be sent in cleartext.
- **Allow Diffie-Hellman Anonymous:** Aventail Connect will be able to communicate with the extranet (SOCKS) server without requiring a

server certificate. The client and server will not exchange certificates, so there will be no authentication. The encryption will still be negotiated, and the data stream will still be encrypted (unless NULL encryption is chosen by the server).

- **Enable Compression**: To speed the encryption process and enhance overall performance, Aventail Connect will automatically compress encryption when a narrow bandwidth and/or slow modem are detected.

5. If necessary, add (or delete) a trusted roots (`*.rot`) file and/or an LDAP server definition.

To add or remove a trusted root

a. In the **SSL Options—Advanced** dialog box, under "Server Validation," select **Use local trusted roots file**, and then click **Configure**.

The **Trusted Roots** dialog box will appear.

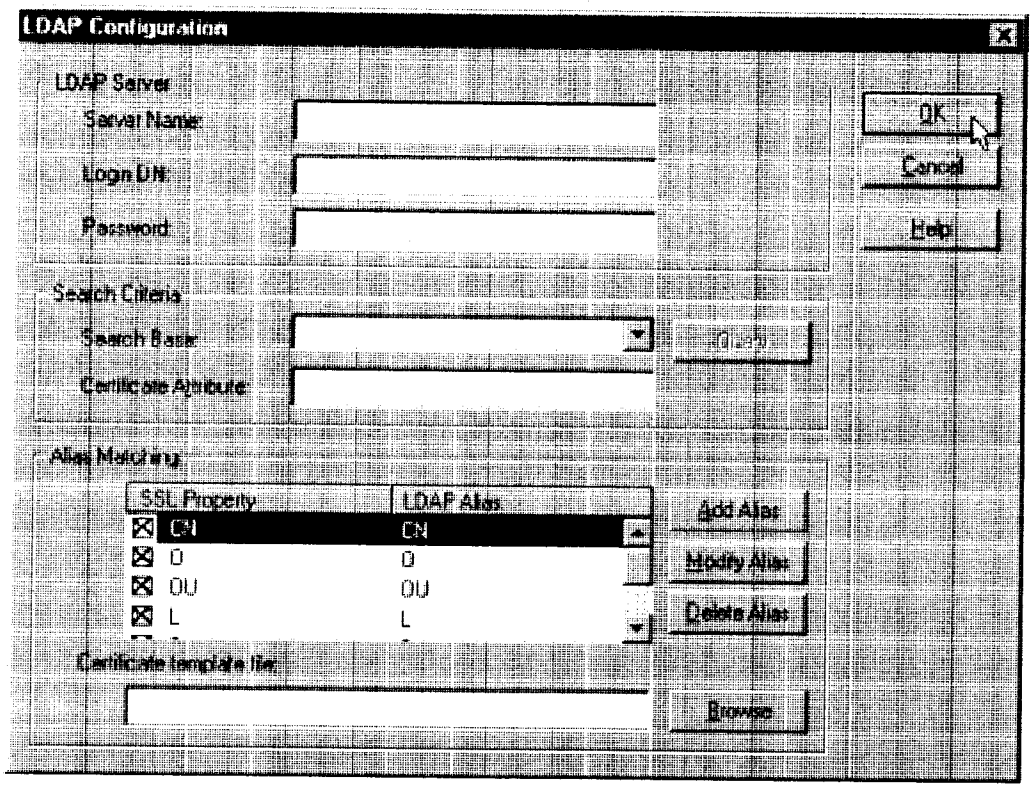
b. Enter the name of the trusted roots file, or click **Browse** to search for the file, and then click **OK**.

CAUTION: The trusted root file must be in the same directory as the Aventail Connect configuration file.

To configure LDAP

a. In the **SSL Options—Advanced** dialog box, under "Server Validation," select **Use LDAP**, and then click **Configure**.

The **LDAP Configuration** dialog box appears.



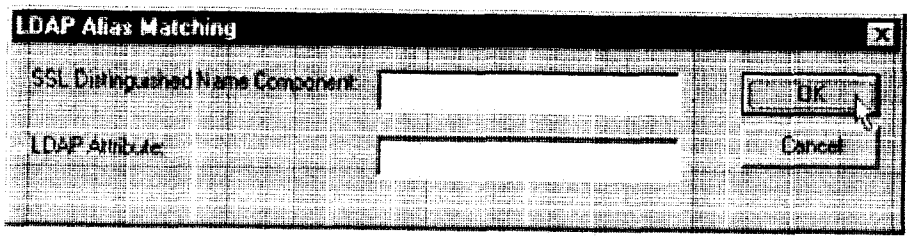
Field	Description	
LDAP Server		
Server Name	Enter the LDAP server hostname.	
Login DN	Enter the login DN (distinguished name) for the LDAP server.	
Password	Enter the password for the LDAP server.	
Search Criteria		
Search Base	Enter the DN to use as the search base.	
	Query	Search available DNs to use as search base.
Certificate Attribute	Enter the certificate attribute.	
Alias Matching		
SSL Property/LDAP Alias	Names of SSL property and corresponding LDAP alias.	
Add Alias	Add an LDAP alias/SSL property.	
Modify Alias	Modify an LDAP alias.	
Delete Alias	Delete an LDAP alias/SSL property.	
Certificate template file:	*(Optional)* Enter name of certificate file to use as template.	
	Browse	Search available certificate files.

b. Under "LDAP Server," enter the LDAP server name, and the DN and password that you want to log in under.

c. Under "Search Criteria," enter or select the DN to use as the search base, and enter the certificate attribute. (In most cases, the certificate attribute will be "usercertificate.")

d. Under "Alias Matching," select the SSL properties that you want to use as search criteria.

   If necessary, you can modify any of the LDAP aliases to map to the SSL properties. To modify an LDAP alias, click **Modify Alias**. In the **LDAP Alias Matching** dialog box, enter the LDAP Attribute that will map to the SSL Distinguished Name Component. You can also **Add** or **Remove** an SSL property/LDAP alias in the **LDAP Alias Matching** dialog box.



In the **Certificate template file:** box, you can specify a certificate file to use as a template. If you specify a certificate template file, Aventail Connect will automatically populate the "SSL Property/LDAP Alias" box with the attributes used in the specified certificate template file.

e. Click **OK**.

6. If Aventail Connect sends a client certificate to the server during the initial authentication exchange, it sends the certificate identified in the **Client Certificate** window. To load the client certificate, press **Browse** and then select the client certificate (`*.cer`) from the Aventail Connect directory. Only the filename of the certificate file loads via the **Browse** button, and not the pathname.

CAUTION: *The client certificate file must be placed in the Aventail Connect directory.*

When Aventail Connect receives a certificate from a server, it looks at the root of the certificate chain and matches it against the Aventail Connect list of trusted roots.

You can specify the maximum number of certificates in a certificate chain. The default maximum length is two certificates. In most instances, Aventail recommends allowing no more than two certificates to form a chain, although you can specify up to ten. The longer the certificate chain, the less secure the chain is.

CAUTION: *In most instances, Aventail recommends allowing no more than two certificates in a certificate chain. Allowing more than two certificates can compromise security.*

7. After making appropriate selections, click **OK**.

PKCS #12 Certificates for User Authentication

Aventail Connect supports PKCS #12-formatted X.509 client certificates for SSL authentication. PKCS #12-formatted certificates are stored in a portable format for easy exchange between applications. You can generate client certificates by enrolling with a public-key infrastructure (PKI), such as VeriSign OnSite. You can then use your Web browser to export the client certificate to a PKCS #12 file in

the Aventail program directory. When users connect to an Aventail ExtraNet Server for the first time, they will be prompted to select a certificate.

To export a PKCS #12-formatted X.509 certificate

1. Using a Web browser and a CA, such as VeriSign Onsite, obtain a client certificate.
2. Export the certificate to a file in the Aventail program directory. You can use any filename. This step varies from browser to browser.

   Microsoft Internet Explorer 4.01

   a. Select **View|Internet Options...|Content|Certificates|Personal...**.
   b. Select the certificate that you want to export, and click **Export...**.
   c. Specify a password to protect the certificate.
   d. Save the file to the Aventail Connect program directory.

CAUTION: On Windows NT, Microsoft Internet Explorer 4.01 does not export PKCS #12 certificates properly. This problem was corrected in Microsoft Internet Explorer 5.0.

   Microsoft Internet Explorer 5.0

   a. Select **Tools|Internet Options...|Content|Certificates|Personal...**.
   b. Select the certificate that you want to export, and click **Export...**.
   c. In the Certificate Export Wizard, click **Export the Private Key**.
   d. Specify a password to protect the certificate.
   e. Select the PKCS #12 format.
   f. Select **Include all certificates in the certificate path if possible**.
   g. Save the file to the Aventail Connect program directory.

   Netscape Navigator 4.5

   a. Click the Lock icon in the lower-left corner of the main Netscape Navigator window.
   b. Select **Certificate|Yours**.
   c. Select the certitficate that you want to export, and click **Export**.
   d. Specify a password to protect the certificate.
   e. Save the file to the Aventail Connect program directory.

3. Use an Aventail Connect configuration file and server setup that forces the user to authenticate using client certificates. Configure the Aventail ExtraNet Server.
4. Initiate a connection that forces the user to authenticate. You will be prompted for a certificate file. Select the certificate that you just exported, and then click **OK**.

PKCS #11 Smart Cards for User Authentication

Aventail Connect can use client certificates that are stored on PKCS #11-compatible smart cards for SSL authentication. Currently, Aventail Connect supports the DataKey and Spyrus Rosetta smart cards.

Aventail Connect will be prompted for a file (or smart card) containing certificate information only when the SOCKS server requests client authentication using a certificate. If a SOCKS server requests client authentication with a certificate, and no certificate is already specified for that host, the user will be prompted to select a certificate. You can configure passwords or PINs to be cached to memory, or you can specify that users enter passwords or PINs each time they use a smart card to authenticate.

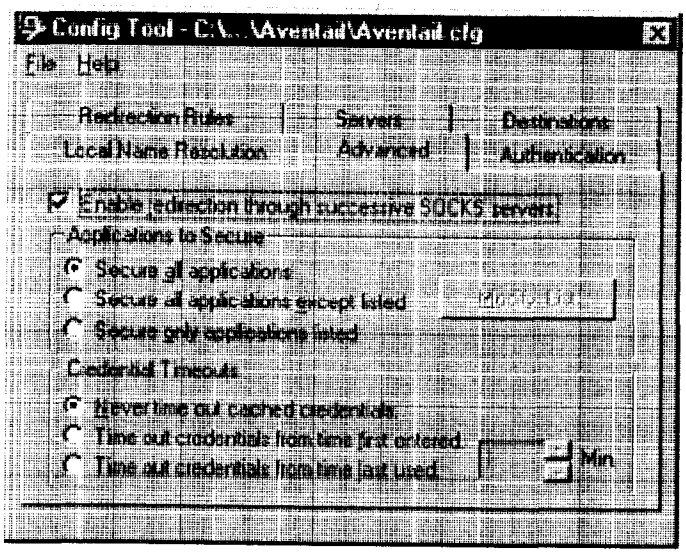
To configure PKCS #11 smart-card user authentication

1. Use a smart card with an X.509 certificate stored on it.
2. Install the appropriate smart card software on the user's computer.
3. Include the public certificates of the CA (and any intermediary CAs) for the client certificate in the trusted roots file that Aventail Connect is configured to use.
4. Configure Aventail Connect to redirect to an Aventail ExtraNet Server that requires client certificates.
5. Initiate a connection.
6. When prompted, specify whether you want to authenticate with a client certificate that is stored in a file, a client certificate that is stored on a smart card, or no client certificate at all.
7. Aventail Connect will prompt you for the path of the dynamic link library (DLL) for the smart card's PKCS #11 module. This is the same DLL that is used with Netscape Navigator. Enter the DLL pathname and click **OK**.
8. Aventail Connect will display a list of all detected smart cards on the system. If you have not yet inserted your smart card into the appropriate reader, insert it and click **Refresh List**.
9. Select your smart card and click **OK**.
10. If the smart card is protected with a PIN, you will be prompted to enter it.
11. Select the private key you want to use, and click **OK**.

NOTE: *Once you specify a smart card token or client certificate to be used with a server, this setting will be remembered indefinitely. To reset the setting, select* ***Credentials*** *from the Aventail Connect system tray menu, select (highlight) the credentials, and click* ***Delete****. Your PIN will not be remembered.*

ADVANCED TAB OPTIONS

The **Advanced** tab in the Config Tool contains three advanced options. In the **Advanced** tab, you can allow SOCKS tunneling through successive extranet (SOCKS) servers, secure selected applications, and set credential cache time-outs.



ALLOW SOCKS TUNNELING THROUGH SUCCESSIVE EXTRANET SERVERS

Once servers and destinations are defined, you can direct SOCKS traffic through successive extranet (SOCKS) servers.

On the **Advanced** tab in the Config Tool, select the **Enable redirection...** box to allow credential information to forward to successive extranet servers.

SECURE SELECTED APPLICATIONS

This option allows you to:

- secure all applications except those listed,
- secure only the applications that are listed,
- or secure all applications, enabling neither exclusion nor inclusion.

NOTE: *You can exclude and include only 32-bit applications. You cannot exclude and include 16-bit applications.*

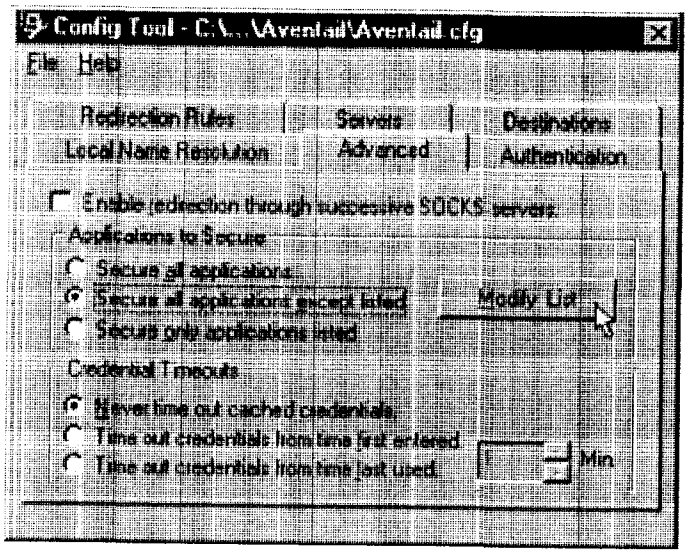
You can exclude or include specified applications in the Exclusion/Inclusion List. With the Exclusion/Inclusion List, you can secure all applications *except* those on the list, or you can secure *only* those applications on the list. The default setting is to secure (hook) *all* network applications.

Excluding Applications

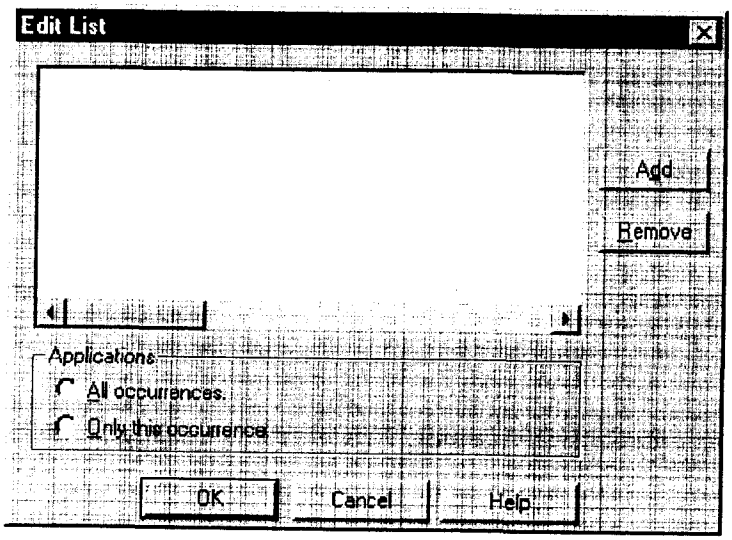
You can exclude specific applications through the Exclusion/Inclusion List. When you enable the "Secure all applications except listed" option, Aventail Connect will not proxy any applications that are on the Exclusion/Inclusion List.

To exclude an application

1. Under "Applications to Secure," select **Secure all applications except listed** and click **Modify List**.

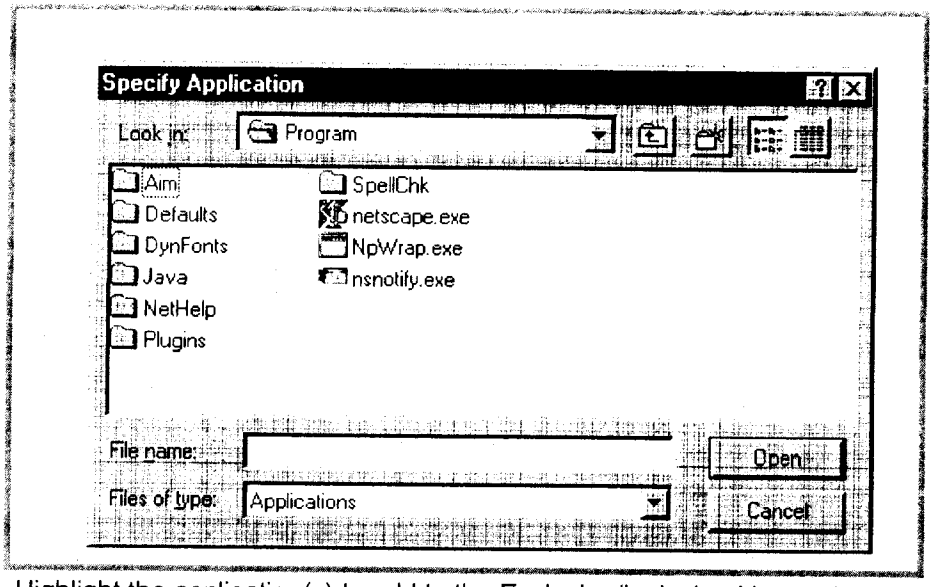


The **Edit List** dialog box appears.



2. Click **Add...**.

The **Specify Application** dialog box appears.



3. Highlight the application(s) to add to the Exclusion/Inclusion List, and then click **Open**.

   The **Specify Application** dialog box disappears and the applications are now in the **Edit List** dialog box.

4. In the **Edit List** dialog box, select **All occurrences** or **Only this occurrence**.

NOTE: *You may have more than one path (instance) of a specified filename (e.g.,* `ftp.exe`*). You can choose to exclude one specified application, with a fully qualified pathname (e.g.,* `C:\Windows\Sys32\ftp.exe`*), or all instances of a specified filename (e.g., all instances of* `ftp.exe`*).*

- **Only this occurrence:** Selecting this option excludes only the specified application.
- **All occurrences:** Selecting this option excludes all applications with the specified filename.

To undo application exclusion

1. Under "Applications to secure," select **Secure all applications except listed**, and then click **Modify List**.

   The **Edit List** dialog box appears.

2. Highlight the application you want to remove from the Exclusion/Inclusion List, and then click **Remove**.

   The application is removed from the Exclusion/Inclusion List.

Including Applications

You can include specific applications through the Exclusion/Inclusion List. When you enable the "Secure only applications listed" option, Aventail Connect will hook only those applications that are on the Exclusion/Inclusion List.

To include an application

1. Under "Applications to secure," select **Secure only applications listed**, and then click **Modify List**.

   The **Edit List** dialog box appears.

2. Click **Add**.

   The **Specify Application** dialog box appears.

3. Highlight the application(s) to add to the Exclusion/Inclusion List, and then click **Open**.

   The **Specify Application** dialog box disappears and the applications are now in the **Edit List** dialog box.

4. In the **Edit List** dialog box, select **All occurrences** or **Only this occurrence**.

NOTE: *You may have more than one instance of a specified application (e.g., `ftp.exe`). You can choose to include one specified application, with a fully qualified pathname (e.g., `C:\Windows\Sys32\ftp.exe`), or all instances of a specified application (e.g., all instances of `ftp.exe`).*

- **Only this occurrence:** Selecting this option excludes only the specified application.
- **All occurrences:** Selecting this option excludes all applications with the specified filename.

To undo application inclusion

1. Under "Applications to secure," select **Secure only applications listed**, and then click **Modify List**.

   The **Edit List** dialog box appears.

2. Highlight the application you want to remove from the Exclusion/Inclusion List, and then click **Remove**.

The application is removed from the Exclusion/Inclusion List.

Securing all Applications

You can secure *all* applications, enabling neither exclusion nor inclusion. When you secure all applications, Aventail Connect ignores any applications on the Exclusion/Inclusion List.

To secure all applications

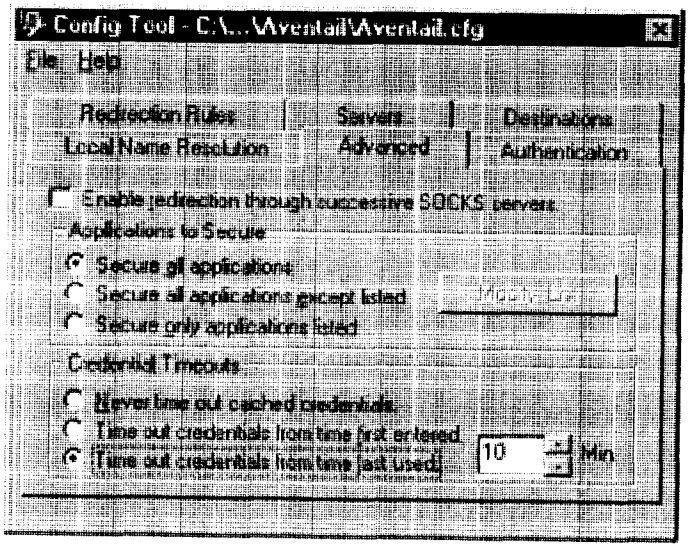
- On the **Advanced** tab, under "Applications to Secure," select **Secure all applications**.

*NOTE: Aventail Connect secures all applications by default. Unless you need to exclude or include specific applications, Aventail recommends that you use the default **Secure all applications** setting.*

CAUTION: Microsoft Internet server products (including Microsoft Internet Information Server (IIS) and Microsoft Peer Web Server) include inetinfo.exe, which conflicts with Aventail Connect 3.1. To eliminate this conflict, exclude inetinfo.exe through the Application Exclusion/Inclusion List in the Config Tool.

CREDENTIAL CACHE TIMEOUTS

With the credential cache timeout feature, you can control when credentials expire (time out). If a user has not made a connection to the extranet (SOCKS) server for a certain length of time (determined by the administrator), then the credentials will automatically be deleted from the credential cache. If a credential times out, the user must reauthenticate by entering the proper credentials before regaining access to the extranet. This feature can help to prevent unauthorized users from gaining access to secured areas.



There are three credential cache timeout options.

- **Never time out cached credentials:** Credentials never time out.

- **Time out credentials from time first entered:** Credentials time out ***x*** minutes after the user first entered the credentials (where "***x***" is the number of minutes you enter in the **Min.** box).
- **Time out credentials from time last used:** Credentials time out ***x*** minutes after the user last connected through the extranet server (where "***x***" is the number of minutes you enter in the **Min.** box).

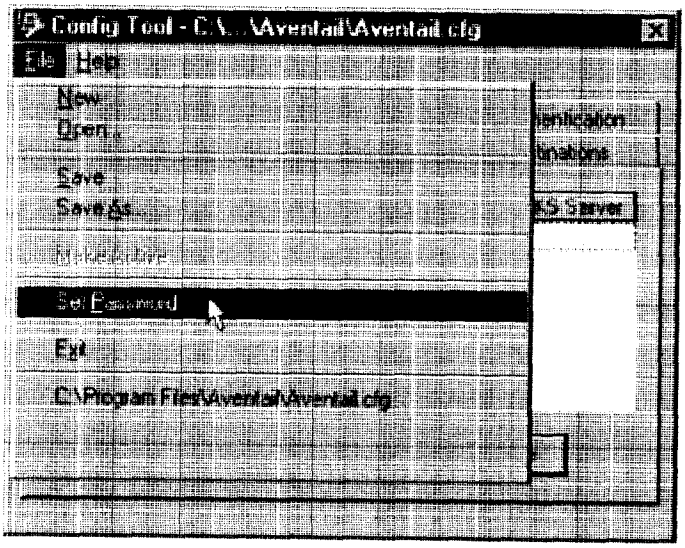
CAUTION: *If your mail program is configured to check for e-mail at regular intervals, the mail-checking frequency must be longer than the credential cache timeout. For example, if your mail program is configured to check for mail every ten minutes, you should set the credential cache to less than ten minutes.*

ENABLE PASSWORD PROTECTION

You can enable password protection for a configuration file. If you enable password protection, users will not be able to view or modify the configuration file without the assigned password. A password is not required to use the configuration file with Aventail Connect.

To enable password protection

1. From any tab of the Config Tool, select **File | Set Password**.



The **Configuration File Password** dialog box will appear.

2. Enter the desired password.
3. Reenter the password to confirm, and then click **OK**.

To disable password protection

1. From any tab of the Config Tool, select **File | Set Password**.

   The **Configuration File Password** dialog box will appear.

2. Clear the password from both boxes, and then click **OK**.

NOTE: *If you save an existing configuration file using the* ***Save As*** *command, Aventail Connect will prompt you to enter the correct password for the configuration file.*

MULTIPLE FIREWALL TRAVERSAL

To gain access to your extranet, users may need to traverse multiple firewalls. In the simplest case, this involves an employee at a partner company gaining access to the Internet via an outbound proxy server at the partner company, and having an authenticated, encrypted, and controlled connection to your internal network via an Aventail ExtraNet Server. This capability is provided in Aventail Connect 3.1 by the Aventail MultiProxy feature. Aventail Connect can open connections through SOCKS servers, through HTTP proxies, or through proxy chaining.

- **MultiProxy with SOCKS Server:** Uses a SOCKS server to control outbound access.
- **MultiProxy with HTTP Proxy:** Uses an HTTP proxy to control outbound access.
- **Proxy Chaining:** Uses two Aventail ExtraNet Servers, where one Aventail ExtraNet Server acts as a client to another Aventail ExtraNet Server.

AVENTAIL MULTIPROXY

The Aventail MultiProxy feature allows Aventail Connect to traverse multiple firewalls by making connections through successive proxy servers. Aventail Connect makes a connection with each proxy server individually. Each proxy server forms a link in a chain that connects Aventail Connect to the final destination. Any or all of the proxy servers can apply authentication and access control rules. Proxies can be Aventail ExtraNet Servers, other SOCKS 5 servers, SOCKS 4 servers, or HTTP proxies.

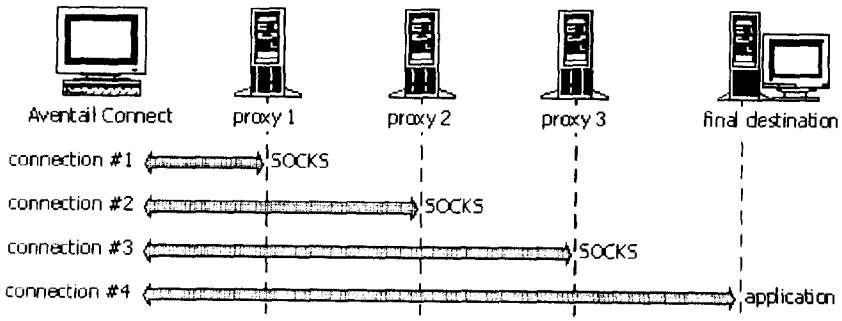
Using an HTTP proxy server to control outbound traffic eliminates the need to install a separate SOCKS server. This HTTP proxy can filter outbound connection requests and route those requests to the specified servers. MultiProxy supports RFC 2068 HTTP Basic (username/password) authentication. If your proxy uses HTTP Basic (username/password) authentication, Aventail Connect will store the username and password information in the credential cache, as it does with SOCKS servers.

NOTE: *The MultiProxy feature supports the use of HTTP proxies in Aventail Connect 3.1 only. HTTP proxies cannot be used in Aventail Connect 2.6.*

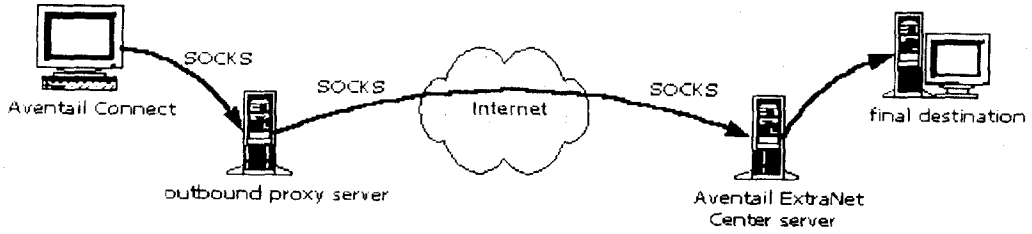
The steps for making a connection using MultiProxy are:

1. The client application requests access to the destination server.
2. Aventail Connect establishes a connection with the outbound server (SOCKS server or HTTP proxy). Aventail Connect then sends the access request to the outbound server, specifying the Aventail ExtraNet Server as the destination. The user authenticates with the outbound server, if necessary.
3. Aventail Connect instructs the outbound server to establish a connection with the Aventail ExtraNet Server on the specified port. The user authenticates with the Aventail ExtraNet Server, if necessary.
4. Aventail Connect instructs the Aventail ExtraNet Server to proxy its connection to the final destination.
5. Once the connection between the client and the Aventail ExtraNet Server is established, the outbound server simply relays the data.

The following example illustrates the connections made during a MultiProxy connection through three proxy servers.



In the following diagram, the Aventail ExtraNet Server acts as both a *destination* and a *server*. It is a destination because a proxy server routes traffic to it. It is a server because it routes traffic to the final destination.



CAUTION: If using an HTTP proxy, you must configure your HTTP proxy and firewall to allow HTTPS/SSL connections to port 1080, **OR** *you must run the Aventail ExtraNet Server on port 443 or port 563.*

Configuring Aventail MultiProxy

You have two options for configuring MultiProxy. You can configure Aventail Connect 3.1 to redirect all Internet traffic (including extranet traffic) through your outbound proxy, or you can configure Aventail Connect 3.1 to redirect only extranet traffic through your outbound proxy.

To configure Aventail MultiProxy

1. Create a destination ("Final destination").
2. Create a server ("Extranet server").
3. **To redirect only extranet traffic:** Create a destination ("Extranet server"), using the same information from step 2, above.

   -OR-

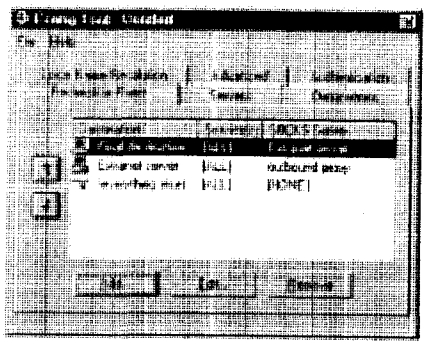
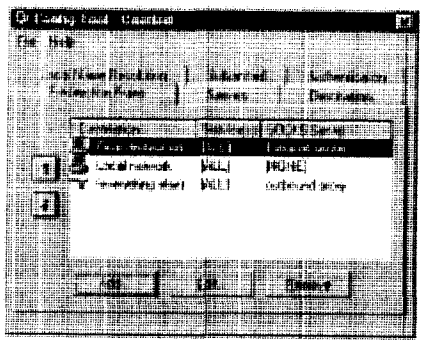
   To redirect all Internet traffic (including extranet traffic): Create a destination ("Local network," the network local to Aventail Connect).

NOTE: If you have multiple domains or subnets, you may need to create multiple destinations.

4. Create a server ("Outbound proxy"). This can be a SOCKS 5, SOCKS 4, or HTTP proxy server.
5. Create a redirection rule (Redirect "Final destination" through "Extranet server").
6. **To redirect only extranet traffic:** Create a redirection rule (Redirect "Extranet server" through "Outbound proxy"). Do not redirect "(everything else)."

   -OR-

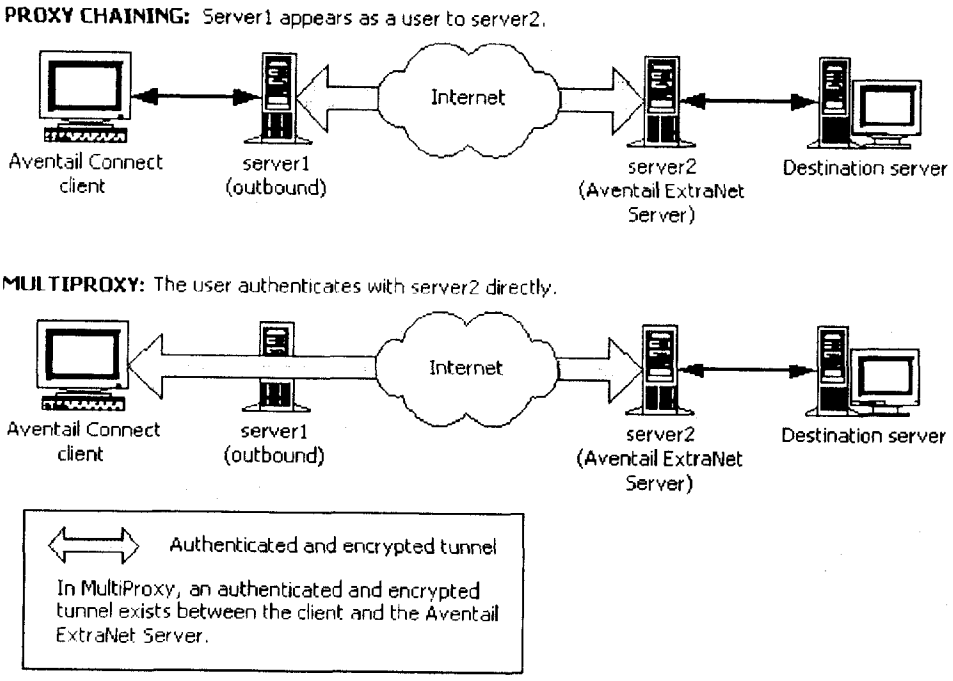
   To redirect all Internet traffic (including extranet traffic): Create a redirection rule (Do not redirect "Local network"). Redirect "(everything else)" through the outbound proxy. (**NOTE:** Your outbound proxy must belong to "Local network.")

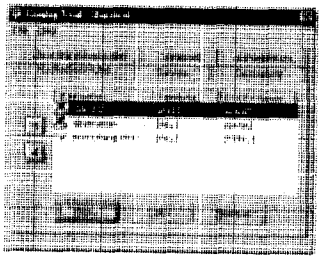
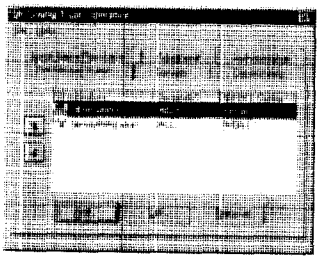
Redirect only extranet traffic	Redirect all Internet traffic (including extranet traffic)
	
Redirect only the extranet traffic through the outbound proxy. Leave all other traffic alone.	Redirect all Internet traffic through the outbound proxy. Leave only "Local network" traffic alone.

PROXY CHAINING

Proxy chaining is an Aventail ExtraNet Server feature. With proxy chaining, Aventail ExtraNet Servers forward connections for certain destinations to other proxy servers.

The following diagram and table illustrate the differences between MultiProxy and proxy chaining. In many cases, MultiProxy is the preferred method for traversing multiple firewalls. With MultiProxy, *each* proxy server can provide authentication, access control, and encryption.



Criteria	MultiProxy	Proxy Chaining
Server 1	Can be Aventail ExtraNet Server, other SOCKS 5 server, SOCKS 4 server, or HTTP proxy.	Must be Aventail ExtraNet Server.
Server 2	Must be Aventail ExtraNet Server.	Must be Aventail ExtraNet Server.
Authentication to Server 1	User authenticates (if necessary).	User authenticates.
Authentication to Server 2	User authenticates.	Server 1 authenticates automatically.
Trust model for Server 2	Not inherited. Each user must individually authenticate with Server 2.	Inherited from Server 1. Server 2 trusts everyone who authenticates to Server 1 equally.
Access control rules	Can be for specific users.	Treats everyone who authenticates to Server 1 equally.
Client configuration redirection rules		
Advantages	• Server 1 can be an Aventail ExtraNet Server, other SOCKS 5 server, SOCKS 4 server, or HTTP proxy. • Most secure, because no security policy is inherited from Server 1.	• Client is aware of Server 1 only. • User authenticates only once, to Server 1.
Disadvantages	• User may need to authenticate more than once. • Client must be aware of Server 1 and Server 2.	• All users connecting through Server 1 appear as a single user to Server 2.

HTTP Proxies and Web Browsers

Extranets often include Web pages that must be viewed with a Web browser. When a Web browser uses an HTTP proxy server, Aventail Connect sees connections being made to the HTTP proxy rather than to the final destination. Therefore, Aventail Connect cannot redirect the connections to the Aventail ExtraNet Server or provide authentication and encryption. For Aventail Connect to function properly, the Web browser cannot use the HTTP proxy to connect with sites protected in the extranet; this is because Aventail Connect must redirect and encrypt connections. The Web browser can still use the HTTP proxy to connect to sites that are not protected in the extranet.

If access to Web pages behind the Aventail ExtraNet Server requires users to connect through a Web browser (e.g., Microsoft Internet Explorer or Netscape Navigator), you must configure the Web browser to not use the HTTP proxy in the Web browser for those sites protected in the extranet.

When users need to access Web pages behind an Aventail ExtraNet Server, you must properly configure the Web browser.

Configuring Aventail Connect and the Web Browser

There are two approaches to configuring Aventail Connect for use with a Web browser.

- Configure the Web browser to not use the HTTP proxy for any traffic. (Aventail Connect redirects all connections through the outbound proxy.)

-OR-

- Configure the Web browser to not use the HTTP proxy for only those sites that are protected in the secure extranet. (Aventail Connect redirects only extranet connections through the outbound proxy.)

To use either approach, you must first configure Aventail Connect. The Aventail Connect configuration is the same for both approaches, whether you are configuring your browser to not use the HTTP proxy for all traffic or for protected sites only.

To configure Aventail Connect for use with a Web browser

1. In the **Servers** tab of the Config Tool, add the HTTP proxy as a server.
2. In the **Destinations** tab of the Config Tool, add the HTTP proxy as a destination.
3. In the **Redirection Rules** tab of the Config Tool, edit the "(everything else)" rule to redirect all traffic to the HTTP proxy server.
4. In the **Redirection Rules** tab, select the HTTP proxy and select the **Do not redirect** option.

CAUTION: *Make sure you do not redirect the outbound proxy. Redirecting the outbound server or proxy will instruct the outbound proxy to redirect traffic to itself, causing Aventail Connect to behave unpredictably.*

To configure the Web browser to not use the HTTP proxy for all traffic

After you have configured Aventail Connect by following the instructions above, configure the Web browser by using one of the following procedures.

- **Microsoft Internet Explorer**
  a. On the **View** menu, click **Internet Options.**
  b. Click the **Connection** tab.
  c. Click to clear the **Access the Internet using a proxy server** check box.
- **Netscape Navigator**
  a. On the **Edit** menu, click **Preferences**.
  b. Under "Category," click to expand **Advanced**, and then click **Proxies**.
  c. Select **Direct Connection to the Internet**, and then click **OK**.

To configure the Web browser to not use the HTTP proxy for protected sites only

After you have configured Aventail Connect, configure the Web browser by using one of the following procedures.

- **Microsoft Internet Explorer**
  a. On the **View** menu, click **Internet Options**.
  b. Click the **Connection** tab.
  c. Under "Proxy Server," click **Advanced**.
  d. In the **Exceptions** box, type the URL of each site that is in the protected extranet.
- **Netscape Navigator**
  a. On the **Edit** menu, click **Preferences**.
  b. Under "Category," click to expand **Advanced**, and then click **Proxies**.
  c Select **Manual Proxy Configuration**, and then click **View**.
  d. In the **Exceptions** box, type the URL of each site that is in the protected extranet.

CONFIGURING THE HTTP PROXY

To allow SSL connections to destination ports other than 443 (https) and 563 (snews), you may need to configure your HTTP proxy. Typically, if you plan to connect to a SOCKS server on port 1080 using an HTTP proxy, you must change the HTTP proxy configuration.

To avoid changing the HTTP proxy configuration, you must run the destination Aventail ExtraNet Server on port 443 or port 563, and configure Aventail Connect accordingly.

Most HTTP proxies can allow connections to port 1080. The following instructions describe how to configure the Microsoft Proxy Server, Netscape Proxy Server, or Apache Web Server to allow port 1080 connections.

- **Microsoft Proxy Server 2.0:** Follow the Microsoft instructions at **http://support.microsoft.com/support/kb/articles/q184/0/28.asp**. You must modify a registry setting with `regedt32.exe`. (`regedit.exe` will not work; you must use `regedt32.exe`.)
- **Netscape Proxy Server 3.5:** Add the following to your `obj.conf` file:
  `<Object ppath="connect://*">` (*all ports*)
  `Service fn="connect" method="CONNECT"`
  `</Object>`
  To specify a particular port, add the following to your `obj.conf` file:
  `<Object ppath="connect://*:1080"`
- **Apache Web Server 1.3.2 (Linux) with Proxy Support:** The following two lines must be included in the `httpd.conf` file:

  ```
  Proxy Requests On
  ```

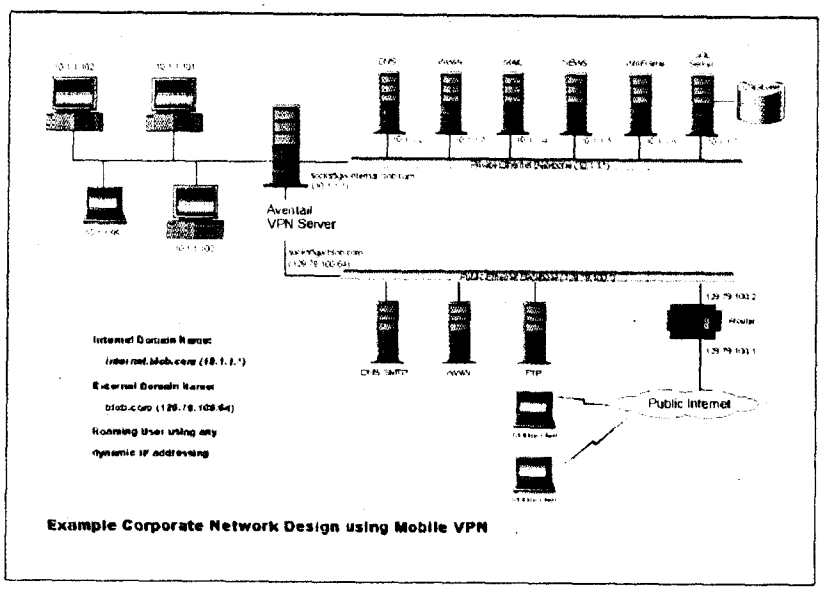
  `AllowCONNECT <port list>` (***NOTE:*** This feature is available only on version 1.3.2 and greater.)

EXAMPLE NETWORK CONFIGURATION

The following section describes the setup of Aventail Connect in an example network configuration using the Aventail ExtraNet Server.

CONFIGURATION USING AVENTAIL EXTRANET SERVER

The following example network configurations show the Aventail ExtraNet Server configured for a Mobile Extranet environment and a Partner Extranet environment. This example emphasizes simplicity to facilitate easy adaptation to real world network designs.



Example Corporate Network Design using Mobile VPN

The design used in the example above consists of two individual Ethernet segments, one public and one private. The public segment is used to host anonymous services available to the general public. The public access is provided through a router that is connected to the public Internet. The private segment is used to house all of the corporation's private network resources and data to be used only by internal company employees. The Aventail ExtraNet Server depicted in this example is used to provide secure and monitored access to the private LAN for mobile employees and partners. For security reasons the Aventail ExtraNet Server is configured such that operating system routing is disabled. Therefore, no direct network connections between the public LAN and the private LAN can be created without being securely proxied through the Aventail ExtraNet Server.

The mobile user workstations connected to the public Internet are the client workstations, onto which, Aventail Connect will be deployed. Due to the routing restrictions described above, these clients will have no network access beyond the Aventail ExtraNet Server unless they are running Aventail Connect. Depending on the security policy and the Aventail ExtraNet Server configuration, Aventail Connect will automatically proxy their allowed application traffic into the private network. In this situation, Aventail Connect will forward traffic destined for the private internal network to the Aventail ExtraNet Server. Then, based on the security policy, the Aventail ExtraNet Server will proxy mobile user traffic into the private network but only to those resources allowed. The client workstations we focus on in this section are Microsoft Windows based PCs.

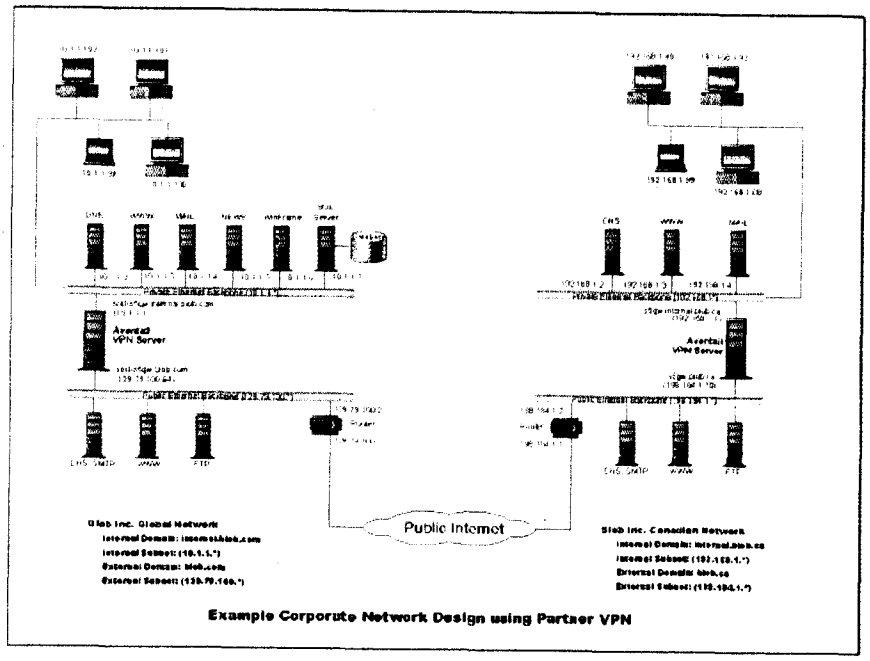
The Aventail ExtraNet Server in our example, has two network adapters configured to use the internal IP address of 10.1.1.1 and an external address of 129.79.100.64.

CAUTION: *Since the internal network address space is part of the IANA reserved address space (per BCP RFC 1918) routing MUST be disabled on this host and routing advertisements for this internal network MUST NOT be propagated to the outside world.*

User authentication and encryption on the Aventail ExtraNet Server require all users to use Aventail Connect to authenticate and encrypt their sessions before any connection to the internal private network(s). For this example, the Aventail ExtraNet Server encrypts all sessions with SSL.

SEE ALSO: *For additional information on how to configure the Aventail ExtraNet Server product, consult the* Aventail ExtraNet Server Administrator's Guide.

Installing and using Aventail Connect for remote access purposes differs a bit from its installation and use within a corporate network. First, configuration files need to be kept locally on the workstation or laptop. This is due to the inability to share a file server that allows direct access outside the perimeter of the private network. Second, not all traffic passes through to the Aventail ExtraNet Server. Only traffic destined for the internal network is authenticated and encrypted; all other traffic passes through Aventail Connect unchanged. For instance, browsing the Internet from the mobile user workstation occurs as if Aventail Connect is not even running in the background. Large sites with many mobile users will want to set up an internal file server for a network installation for all mobile users to easily install and configure Aventail Connect. For more information, refer to "Network Installation."



Example Corporate Network Design using Partner VPN

Utilities Reference Guide

This section explains:

- Commands on the System menu, including Close, Hide Icon (in Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51), Help, About, Credentials, and Configuration File
- How to use the Aventail Connect utilities, including the Config Tool, the Logging Tool, and S5 Ping, all displayed through the Utility Programs menu.
- How to use Secure Extranet Explorer (SEE)/Extranet Neighborhood.

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 **Aventail Connect** icon from view. Not available in Windows 95, Windows 98, and Windows NT 4.0.
Help	Accesses Help.
About	Displays Aventail Connect **About** box.
Credentials	Displays authentication credentials.
Configuration File	Selects new configuration file via **Aventail Connect Configuration File** dialog box.

Each of the commands is discussed below.

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.

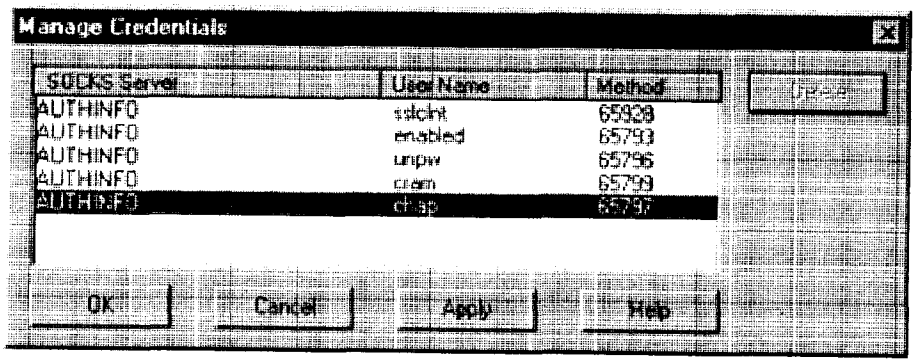
ABOUT

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. 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-

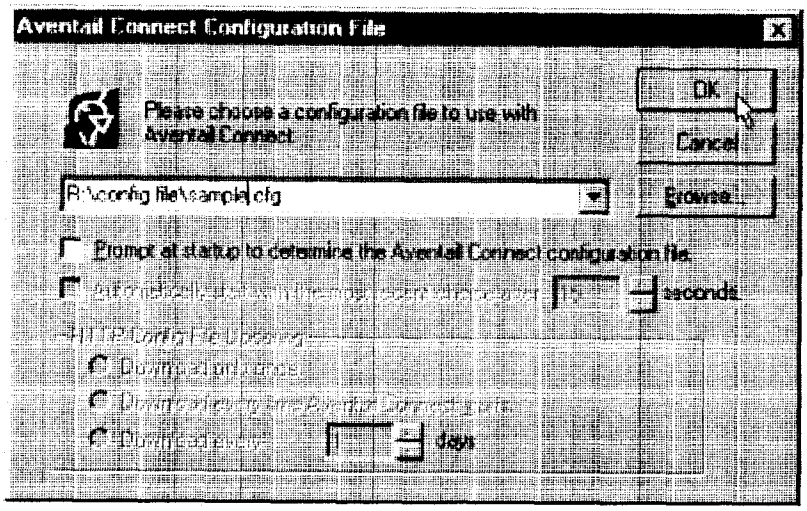
- Click **Cancel** to close the dialog box without accepting any changes you might have entered.

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 Configuration File** dialog box. Aventail Connect 3.1 allows you to use a new or modified configuration file immediately, without needing to restart Aventail Connect and any Aventail-processed applications.

For more information about the configuration file, refer to "Configuring Aventail Connect."



To load a configuration file

- 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...** checkbox.

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.

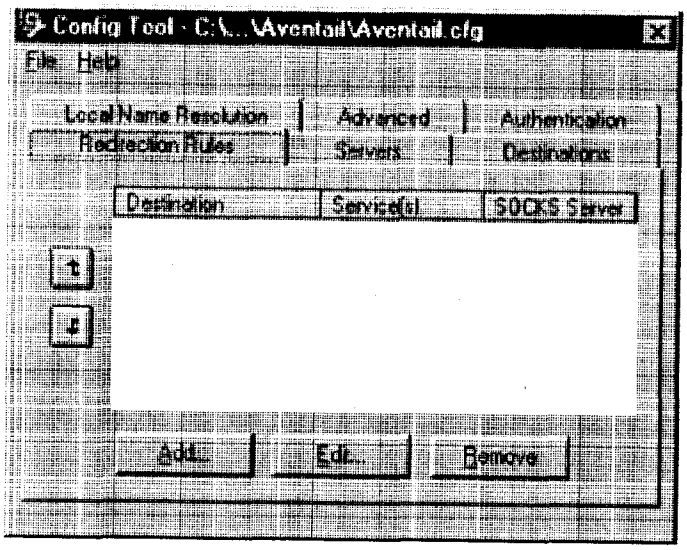
Menu Command	Function
Config Tool	Runs the Config Tool. (Optional)
Logging Tool	Runs the Logging Tool. (Optional)
S5 Ping	Runs the ping and traceroute utilities. (Optional)

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 a custom setup package. They are discussed in the sections "Config Tool," "Logging Tool," and "S5 Ping."*

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. *(This option may not be available to all users if the network administrator has chosen not to install it.)*



Network administrators generally create configuration files during Aventail Connect installation. However, you can add, remove, or modify configuration files at any time. If necessary, you can create several configuration files for different users or user groups. Some configuration files may reside on a networked drive, accessible by multiple users. Other configuration files may be tailored to a specific user on an individual workstation. "Configuring Aventail Connect" discusses the Config Tool in detail.

LOGGING TOOL

The Logging Tool is an optional diagnostic utility for tracing 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, including Aventail Connect network, extranet (SOCKS) server, and WinSock application interoperability problems. Aventail Technical Support engineers may request that you perform a verbose trace, log it to a file,

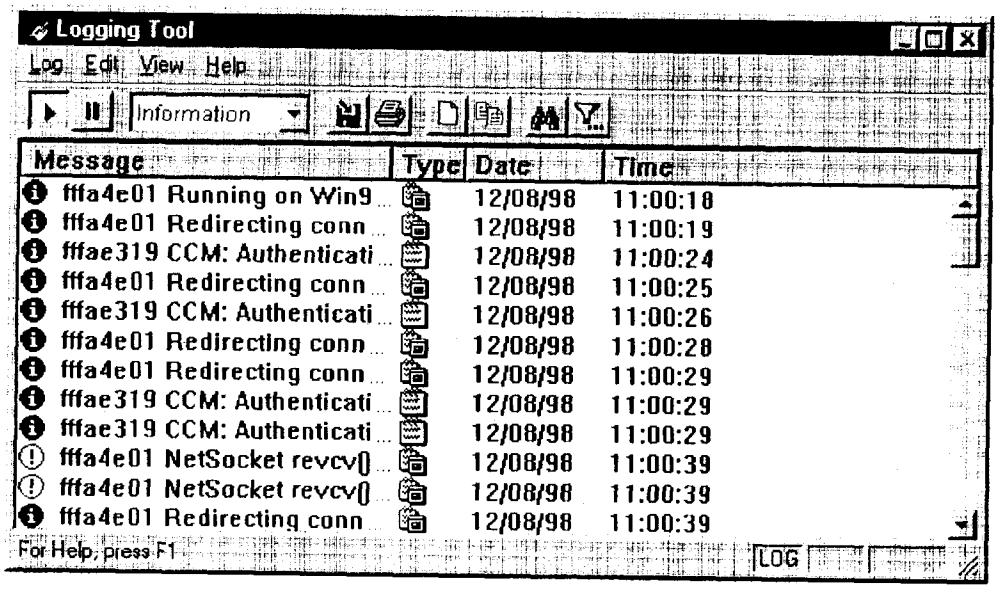
and e-mail it to them as an attachment. Log files are also useful when running Aventail Connect for the first time, to ensure that network traffic is being routed properly.

To trace Aventail Connect activity

1. Windows 95, Windows 98, or Windows NT 4.0: Either right-click the **Aventail Connect** icon (in the system tray on the taskbar) and click **Logging Tool**, or select **Start | Programs | Aventail Connect | Logging Tool**.

-OR-

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



2. In the **Log** menu, click **Level** and select one of the five levels of information you want to trace.

-OR-

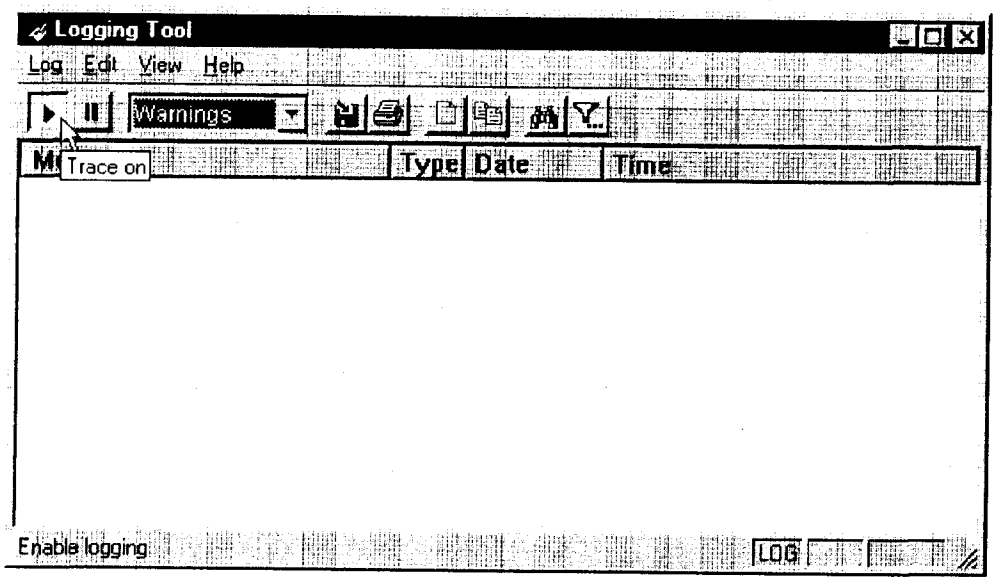
Select one of the five levels from the drop-down list on the toolbar.

Select	To Log
Fatal Errors	Fatal errors only
Errors	Errors and fatal errors only
Warnings	Errors and warnings only
Information	Errors, warning, and information
Verbose	All of the above, and more descriptive information on progress of connections

3. On the **Log** menu, click **Trace.**

-OR-

Click the **Trace On** button on the toolbar (shown below).

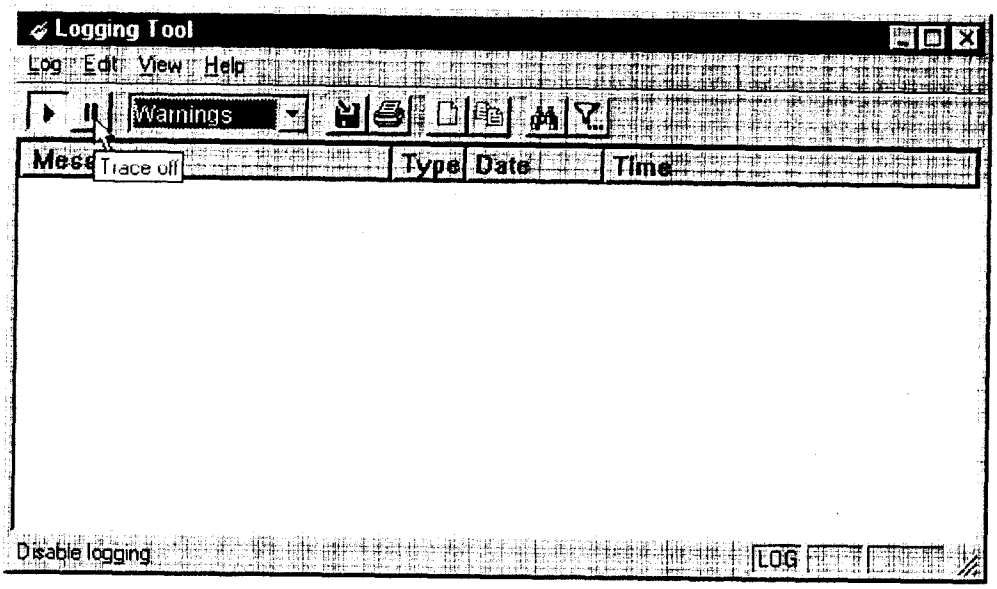


The log window will now record and display trace information as it is generated by Aventail Connect. You can tell when the trace function is active because messages are scrolling down the screen and the **Trace On** button is depressed.

4. When you are ready to stop the Trace function, click **Trace** on the **Log** menu.

-OR-

Click the **Trace Off** button on the toolbar (shown below).



The Trace function stops. You can now scroll through the results, print them, and/or save them to a file.

To save a log file

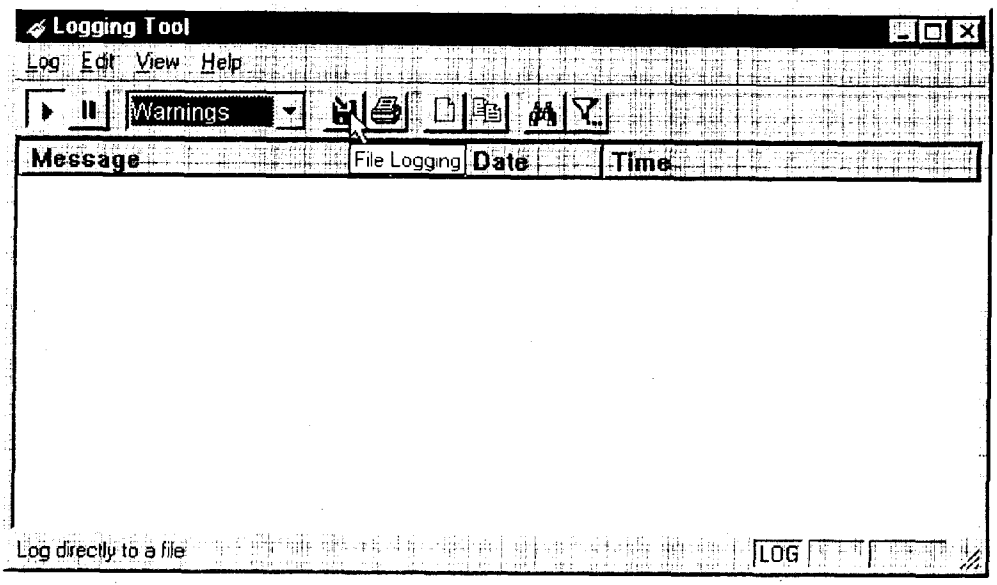
The Logging Tool allows you to append each new message to the end of a .LOG file during the trace, or save the contents of the log window at any time. If you save during a trace, Aventail Connect will append messages to the log file until you stop the log function. You must save data in the log window to retain it.

You cannot open a preexisting log file from within the log window. To open a pre-existing log file, you must open it in a text editor such as Notepad.

1. To save a log file as the data is being generated, click **Log to File** on the **Log** menu. Enter the filename in the **Select Log File** dialog box.

-OR-

Click the **File Logging** button on the toolbar (shown below).



2. Enter the filename in the **Select Log File** dialog box.

   - To save the contents of the log window at any time, click **Save As** on the **Log** menu and then enter the filename.

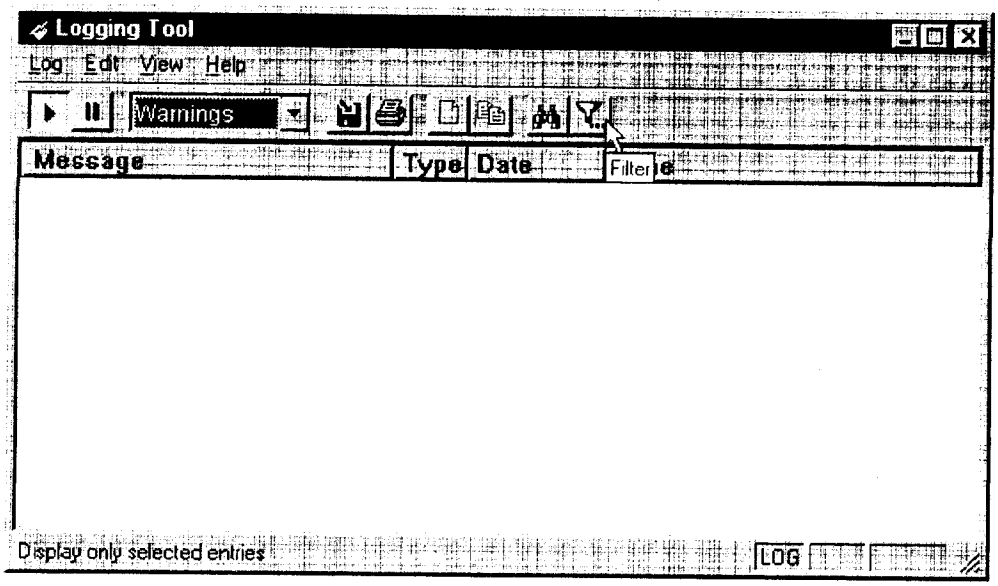
To filter messages in the log window

You can filter the contents of a log window by selecting the types of messages you want to view. By selecting a specific type of message, you can easily scan the information on-screen. If you save data to a log file, a view filter will not affect the file contents; it merely adjusts the screen display of those contents.

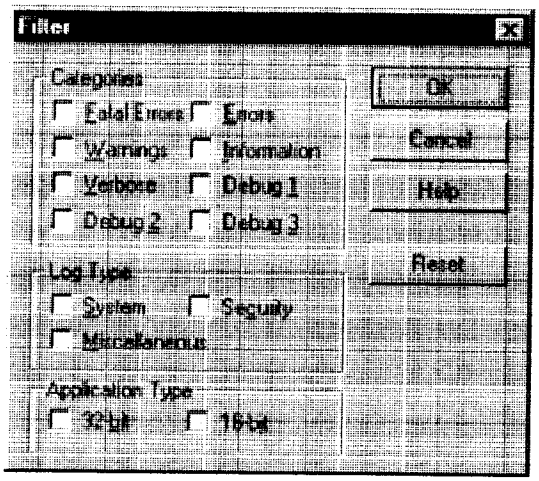
1. On the **View** menu, click **Filter Messages** to display the **Filter** dialog box

-OR-

Click the **Filter** button on the toolbar (shown below) to display the **Filter** dialog box.



NOTE: *The **Filter** function is an on/off toggle. If the filter is enabled, select **Filter Messages** to turn it off, then select it again to display the **Filter** dialog box.*



Field	Definition	
Categories	Select any of the five filters to display errors, fatal errors, warnings, information and/or verbose information in the log window.	
Log Type	Select the type of log to be filtered. (Currently, the only valid log type used in Aventail Connect is Miscellaneous.)	
Application Type*	32-bit	Show messages from 32-bit applications.
	16-bit	Show messages from 16-bit applications.
	*These options are disabled if you are running 16-bit Windows.	

2. Under "Categories," select one or more of the five filter check boxes. The log window will adjust the display based on your selection(s).
3. Under "Log Type," select the log type to filter.
4. Under "Application Type," select one or both of the check boxes.

To change the view parameters

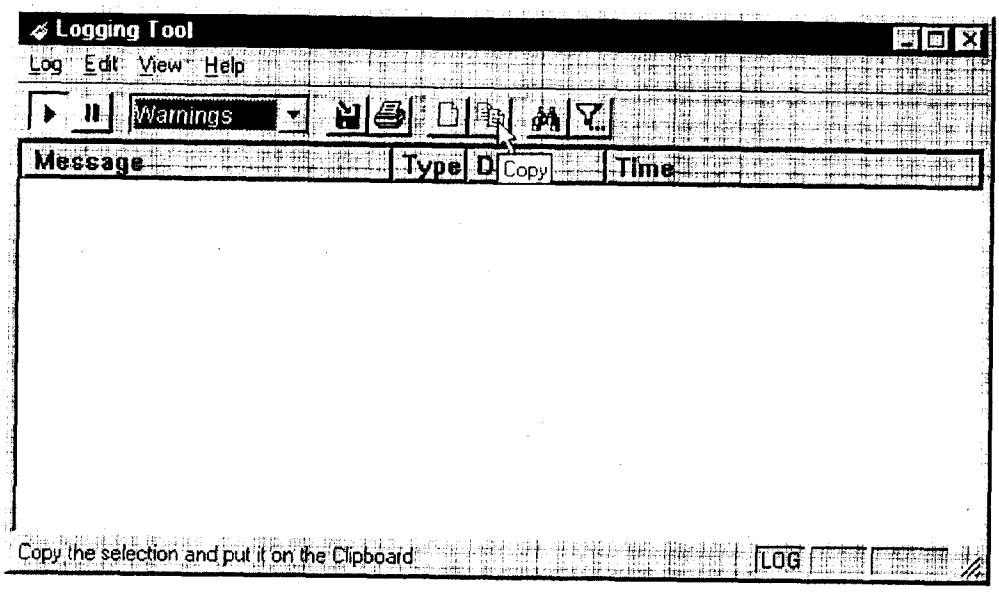
The display font and window options can be customized as follows:

- On the **View** menu, click **Font**. Enter your font preferences into the standard **Windows Font** dialog box.
- To display or hide the toolbar and status bar, click **Toolbar** and/or **Status Bar** on the **View** menu.

To copy the log window

You can copy the log window contents to the Windows Clipboard.

- To copy all of the log window contents to the Windows Clipboard, click **Select All** on the **Edit** menu. Then click **Copy** on the **Edit** menu, or click the **Copy** button on the toolbar.
- To copy selected messages to the Windows Clipboard, drag the mouse over the messages to highlight them. Then select **Copy** on the **Edit** menu or click the **Copy** button on the toolbar.



To print the log window

You can print the contents of the log window can be printed only in its entirety.

- On the **Log** menu, click **Print**.

-OR-

Click the **Print** button on the toolbar.

The entire contents of the window will print, regardless of whether you have specific messages selected. If you have filtered the display, only the filtered messages will print.

To find a specific message

The **Find** command will only work with data displayed in the window. If the display has been filtered, only the filtered messages will be searched. The **Find** dialog box remains active until you close it.

- On the **Edit** menu, click **Find**.

-OR-

Click the **Find** button on the toolbar.

Then enter your search parameters in the **Find** dialog box.

To clear the log window

Clear the log window contents when you are ready to execute a new trace.

- On the **Edit** menu, click **Clear All**.

-OR-

Click the **Clear All** button on the toolbar.

To close the log window

When you are ready to close the log window, make sure you have saved the contents of the trace for later reference. All settings are saved when you exit.

- On the **File** menu, click **Exit**.

S5 PING

Two of the most useful diagnostic tools in an administrator's arsenal are the ping and traceroute utilities.

- 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.

Ping and traceroute both use Internet Control Message Protocol (ICMP). SOCKS v5 is designed to handle TCP and UDP protocols; however, SOCKS v5 does not support ICMP. Because ping and traceroute are based on ICMP, there is no way to directly proxy a ping or traceroute request. To circumvent this problem, Aventail Connect provides a utility called S5 Ping.

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.

To launch S5 Ping

You can use S5 Ping whether or not Aventail Connect is running. However, if the server that you are connecting through requires authentication, you must load Aventail Connect before reconnecting.

- Windows 95, Windows 98, or Windows NT 4.0: Select **Start | Programs | Aventail Connect | S5 Ping**.

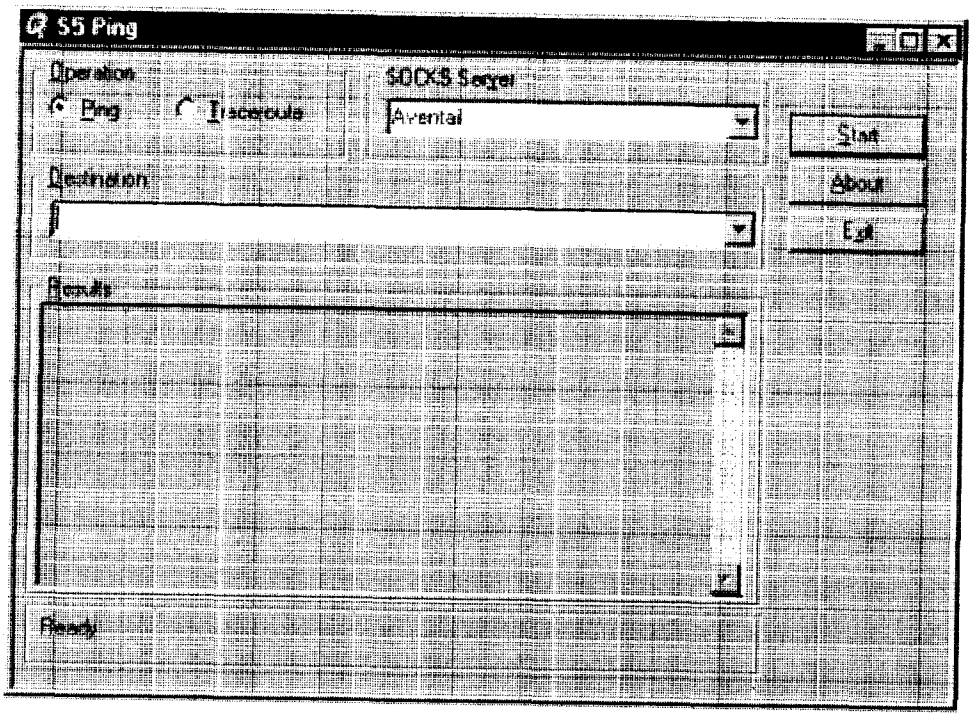
-OR-

Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51: From the Aventail Connect program group, double-click the **S5 Ping** program icon.

-OR-

If Aventail Connect is already running, right-click the **Aventail Connect** icon on the taskbar and click **S5 Ping** (Windows 95, Windows 98, or Windows NT 4.0), click the minimized **Aventail Connect** icon in the System menu (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).

The **S5 Ping** dialog box appears.



NOTE: *S5 Ping will function without a properly configured Aventail Connect; however, the user will be required to type the information about the target extranet server and target host into the* ***SOCKS Server*** *and* ***Destination*** *boxes.*

Field	Definition
Operation	Select ping or traceroute.
SOCKS Server	The Extranet (SOCKS) server that will execute the operation. If Aventail Connect is already configured, this list will be preloaded with extranet servers from the configuration file.
Destination	The extranet server you want to ping (or traceroute). If Aventail Connect is already configured, this list will be preloaded with single host destinations defined in the configuration file. (See "Configuring Aventail Connect.")
Results	The results of successful connection. The format of the results will vary based upon the extranet server platform.

S5 Ping can be used whether or not Aventail Connect is running. However, if the server that you are connecting through requires authentication, you must load

Aventail Connect before connecting. The network administrator may or may not make S5 Ping available to users during installation. In some cases, the **S5 Ping** command will not appear on the Aventail Connect System menu or in the program group.

Once the **S5 Ping** dialog box opens, you can execute a ping or traceroute network operation.

To run ping or traceroute using S5 Ping

S5 Ping has two modes of operation: ping and traceroute.

1. Under "Operation," select one of the two options, **Ping** or **Traceroute**.
2. Under "SOCKS Server," select an Aventail ExtraNet Server to carry out the operation. If no servers are listed (because S5 Ping did not locate an Aventail Connect configuration file), type the extranet server's hostname or IP address.
3. Under "Destination," select a single host destination to ping or traceroute. If no hosts are listed (because S5 Ping did not locate an Aventail Connect configuration file), type the hostname or IP address of the host you want to ping or traceroute.
4. Click **Start** to execute the operation. **Start** then changes to **Stop**. Results from any previous operation are cleared from the window.
5. If the extranet server requires authentication, you may be prompted with a server certificate or required to enter a username and password. (For more information about server certificates and username/password authentication, see "Manage Authentication Modules" in the *Administrator's Guide*.)
6. Once the connection to the host has been made, the information returned from the server will be displayed in the **Results** window.

To stop ping or traceroute

- Click **Stop**.

  This stops the operation and changes **Stop** to **Start**. The results of the operation remain displayed in the **S5 Ping** dialog box.

To exit S5 Ping

- Click **Exit**.

  This clears the results and closes 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.*

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. You can include a SEEHosts file with the Aventail Customizer tool. If users install a custom package that does not include a SEEHosts file, then the first time they open Extranet Neighborhood, SEE will create a SEEHosts file. For more information, see the "Customizer" section in the *Administrator's Guide*.

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.

How Extranet Neighborhood Works

Typically, with Windows networking, the Microsoft Windows Explorer and Network Neighborhood browse files using NetBIOS (NBT), over TCP. Network Neighborhood does not use the standard WinSock programming interface. This prevents Aventail Connect from redirecting TCP connections. Since Aventail Connect redirects only WinSock calls, it cannot redirect NBT calls.

To deliver a secured version of standard Windows browsing, Aventail Connect redirects NBT calls to WinSock. This allows Aventail Connect to redirect this traffic based on a set of redirection rules, as defined in the Aventail Connect configuration file.

Extranet Neighborhood can use either hosts files or Windows Internet Naming Service (WINS) servers to map a computer's Internet (host) name to its Windows machine name. Without a hosts file or a WINS server, Extranet Neighborhood cannot associate a computer's Internet name with its Windows machine name.

Extranet Neighborhood includes a browsing mode, which allows you to view a dynamic list of available Windows hosts. Hosts files provide a static list of hosts.

There are two basic methods for configuring Extranet Neighborhood.

- **Listing WINS Servers:** List only WINS servers for the domain(s) in the hosts file. You do not need to list individual hosts within the domain.
- **Listing Individual Hosts:** List every individual host in the hosts file that will be accessible to users.

Listing WINS Servers

To use Extranet Neighborhood in the browsing mode, you must configure Extranet Neighborhood to use WINS, and you must identify the IP address (hostname) of the WINS server(s) and, possibly, the primary domain controller (PDC) for the domain. If you do not specify a WINS server, you will not be able to use Extranet Neighborhood in the browsing mode.

The PDC for the domain is required only if the destination network is not accessible by UDP. (For example, when using MultiProxy, the destination network is not UDP-accessible.) When Extranet Neighborhood is in browsing mode, it must be able to resolve the name of the host. If the destination network is UDP-accessible, then the WINS server is used to map a computer's Internet (host) name to its Windows machine name. If the destination network is not UDP-accessible, then Extranet Neighborhood uses the PDC and DNS to determine the host's address.

LISTING INDIVIDUAL HOSTS

To use Extranet Neighborhood in the static host list mode, you must define, in the hosts file, each individual host in the domain. This allows you to restrict access to designated hosts only. In the hosts file, you must specify the host's IP address or DNS name along with the Windows machine name. WINS and PDC are not used in this method.

INSTALLING EXTRANET NEIGHBORHOOD

When installed, Extranet Neighborhood appears on your desktop as an icon, and in Windows Explorer. You can open, move, copy, and delete files in Extranet Neighborhood just as you would in Network Neighborhood.

If you need to install Extranet Neighborhood, install it from the Aventail Connect CD. Or, if you downloaded your copy of Aventail Connect, run the downloaded executable package. When the **Installation Components and Sub-components** dialog box appears, select **Extranet Neighborhood** (located under **Components**). Continue with the installation process.

The default installation directory is `\Program Files\Aventail\Connect`.

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

CONFIGURING EXTRANET NEIGHBORHOOD

You can include a SEEHosts file with the Aventail Customizer tool. Only by installing a custom package will users have a local or remote hosts file automatically configured. If users install a custom package that does not include a SEEHosts file, the SEE Configuration wizard will run when users open Extranet Neighborhood for the first time. The SEE Configuration wizard walks you through the process of defining local or remote hosts files. Aventail recommends that you use the Customizer tool to distribute Extranet Neighborhood, bundled with a hosts file, in a custom setup package.

Extranet Neighborhood can automatically construct a hosts file from your local network or a remote network. Using the Search feature, Extranet Neighborhood can automatically "browse" available computers and build the local hosts file. The Search feature is available through the **Extranet Neighborhood Properties | Local** tab. Alternatively, you can enter the names of the available computers manually. The Search feature browses only those computers that are within your internal network. To search remote networks, you must manually enter the fully qualified hostname of each remote WINS server that is outside your Aventail ExtraNet Server. When using the Search feature, the same UDP restrictions described in "Listing WINS Servers" apply.

NOTE: *To use the Search feature, Aventail Connect must be running and configured correctly.*

Do not use the Search feature if you are using the WINS-browsing mode. The Search feature builds the local hosts file for all of the computers, which is not necessary with WINS. Use Search when creating a local hosts file using the "listing individual hosts" method.

NOTE: *When you click* ***Search****, you may see more than one domain in the resulting local hosts file. This is because Search includes trusted domains.*

To create a hosts file

Use this procedure if you have not yet created a hosts file.

1. Decide which method, listing WINS servers or listing all individual hosts, to use.
2. If no hosts file exists, launch Extranet Neighborhood (Extranet Neighborhood will prompt you automatically if you are running Extranet Neighborhood for the first time),

-OR-

Right-click the **Extranet Neighborhood** icon on your desktop and then click **Properties**.

3. Follow the on-screen instructions to create the hosts file.
4. To distribute the new hosts file, include the SEEHosts file in your custom setup package, if using the Customizer tool.

After creating the hosts file, users can browse only those domains and machines that the network administrator has included in that list of hosts. This list may be a local hosts file called "SEEHosts" and/or a remote host list, which is identified by `[share]\[path]\[filename]`.

NOTE: *To use the browsing mode, you must specify the domain's WINS server(s) in the local hosts file.*

CAUTION: *SEE cannot recognize share names that contain special characters (e.g., é) or multiple spaces (e.g.,* Aventail Custom Computer*). SEE also will not recognize hidden one-letter share names (e.g.,* C$ *or* D$*).*

SEE CONFIGURATION METHODS

There are numerous methods for configuring SEE. The three most common methods are described below.

Local Hosts File Method

With this method, the hosts file contains a list of all domains and servers in the local hosts file. Every host is listed.

There are two ways to configure SEE using this method.

- In the **Extranet Neighborhood Properties | Local** tab, manually add each domain and host to the local hosts file

-OR-

- On the **Local** tab, click **Search**, click **Search Local Network**, and then search any remote networks, if necessary. SEE automatically builds a list of all hosts. You may delete hosts from the local hosts file if you do not want users to view them.

NOTE: *To view your domains, double-click the* ***Extranet Neighborhood*** *icon on your desktop. If you make changes to the hosts file, you can reload the* ***Extranet Neighborhood domains*** *window by pressing the* F5 *key.*

Remote Hosts File Method

With this method, the local hosts file contains the path of the remote hosts file, and the remote hosts file contents are determined by which configuration method you use.

To use this method, first create the remote hosts file, and then create a local hosts file that points to the remote hosts file.

To configure SEE using the remote hosts file method

1. Create a local hosts file, using one of the methods listed above, and copy it to a central location. (This creates a remote hosts file; this file is not distributed with Aventail Connect.)
2. On the **Remote** tab, click **Add**, and then add a pointer to the remote hosts file that you created in Step 1. (This file is distributed with Aventail Connect.)

NOTE: *You can point to multiple remote hosts files on a single list.*

WINS Browsing Method

With this method, the hosts file contains a list of all domains, and the WINS servers for each domain. You do not need to list all of the computers.

To use this method, add each domain in the **Local** tab, specifying the primary WINS server and, if applicable, the secondary WINS server, and then select the **Make domain browsable** check box in the **Windows Domain** dialog box.

Choosing a Method

Each of the three methods has advantages and disadvantages. The table below lists pros and cons for each of the three methods.

Method	Advantages	Disadvantages
Local hosts file with individual computers	The administrator controls exactly which hosts the users can see. On slower connections, this method is fastest since you do not need to send a list of servers to the client.	The administrator must update the local hosts file if file servers are added to or removed from the domains.
Remote hosts file	• The administrator can edit the centrally stored hosts file whenever necessary. • If the hosts file is stored behind a firewall, SEE can go through an extranet server (using encryption and authentication) to reach it.	• Users are immediately prompted to enter authentication credentials upon opening SEE (because SEE must load the remote hosts file). • If a user loses network connectivity to the hosts file, SEE will not display the list of hosts/computers.
Local hosts file with WINS browsing	The administrator does not need to update the hosts file if new computers are added or removed.	• The administrator must update the local hosts file if domains are added or removed. • The administrator cannot control which computers appear in SEE; all computers in the NT domain are displayed. • On slower connections, this method is slower than other methods because a list of computers must be sent to the client.

You are not limited to using only one method for configuring SEE. You can use a combination of the various methods. For example:

- Use WINS browsing for some domains, and explicitly list hosts for other domains

-OR-

- Use multiple remote hosts files

-OR-

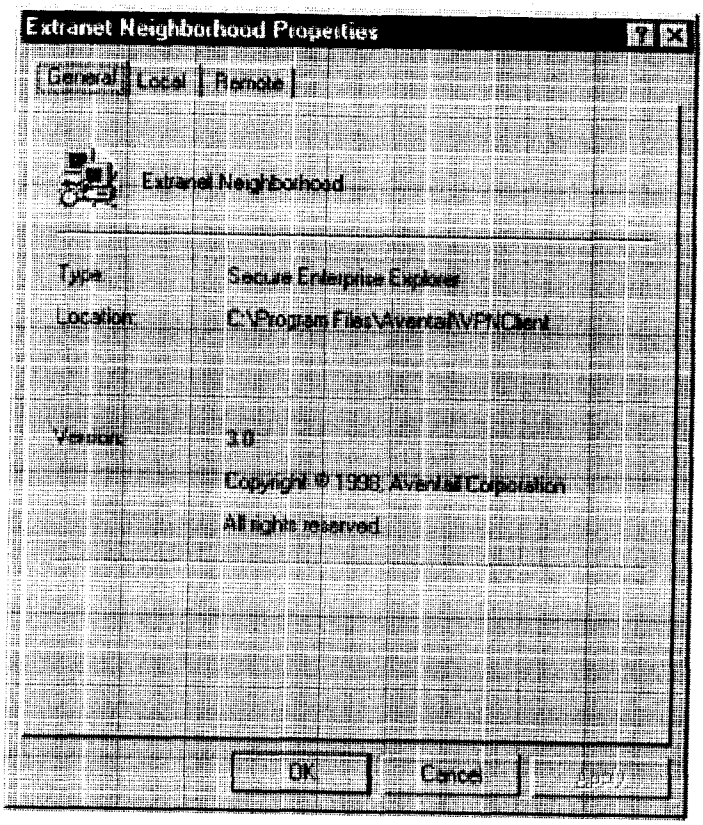
- Specify some computers in a local hosts file and others in a remote hosts file.

SEE PROPERTIES

To access information about the current configuration of SEE, or to make changes to that configuration, right-click the **Extranet Neighborhood** icon and click **Properties**, or click **View | Options** in any open **SEE** window. The **Extranet Neighborhood Properties** window will appear with the **General** tab selected.

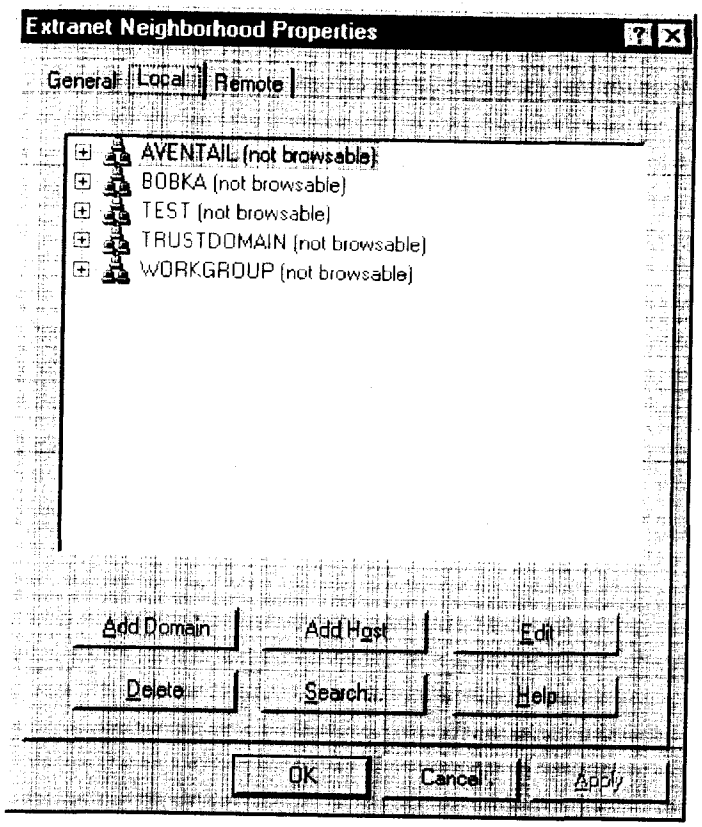
THE GENERAL TAB

The **General** tab displays information about the current configuration of SEE.



THE LOCAL TAB

The **Local** tab displays the computers that are listed in the local hosts file.



If you have specified a host in the local hosts file, you can add, edit, or remove computers or domains that appear in the **Local** tab. If you have specified hosts in the remote hosts file, they will not appear in this tab. To edit hosts in the remote hosts file, you must copy the file to your Aventail Connect directory, edit it, and then replace it in the remote hosts directory.

If you are using the WINS browsing mode, the individual computer names will not appear. Any hosts specified in remote hosts files, including WINS servers, will not appear in this tab.

The **Add Host** and **Add Domain** buttons allow you to add additional computers or domains in the **Add Host to Aventail** dialog box and the **Windows Domain** dialog box.

If no computers or domains appear in your **Local** tab, check the **Remote** tab. It is possible that your network administrator has configured Extranet Neighborhood with only a remote hosts file.

The Search feature can automatically browse available computers in local or remote domains and populate your local hosts file. Alternatively, you can enter the names of the hosts files manually.

NOTE: *To view your domains, double-click the* ***Extranet Neighborhood*** *icon on your desktop. To reload the hosts files in the* ***Extranet Neighborhood domains*** *window, press the* F5 *key.*

NOTE: *In the* **Local** *tab, "browsable" domains do not show individual computers in them.*

Hosts File Locking

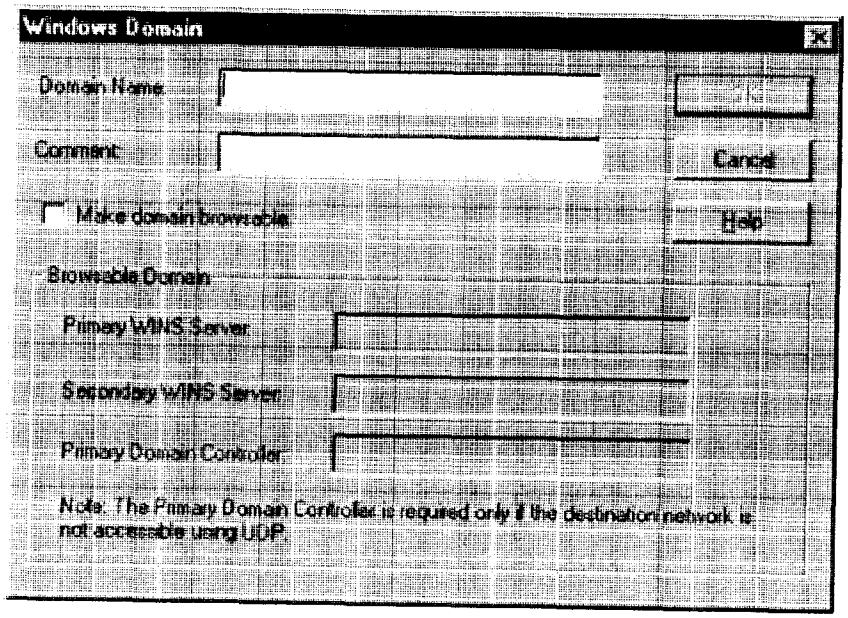
If the controls in this window are disabled (dimmed), then the hosts file has been "locked." The network administrator determines which, if any, hosts files are locked.

You can lock and unlock files from any **Extranet Neighborhood Properties** tab.

- To lock a file, use the **Ctrl+L** command.
- To unlock a file, use the **Ctrl+U** command.

Windows Domain Dialog Box

To open the **Windows Domain** dialog box, click **Add Domain** in the **Extranet Neighborhood Properties | Local** tab.



For each domain, you can either specify the WINS server names or specify each individual host that should appear in the domain. Listing WINS servers will result in a smaller, more manageable hosts file. You must add a domain before you can add hosts to that domain.

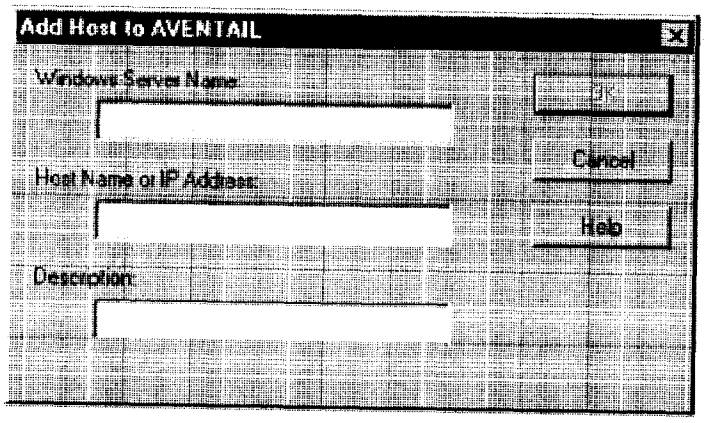
To make the specified domain "browsable," enter WINS server information in the **Primary WINS Server** box and, if desired, the **Secondary WINS Server** box. In both of these boxes, you can enter either the server's IP address or its fully qualified host name. You must also select the **Make domain browsable** check box. If you do not select the **Make domain browsable** check box, Extranet Neighborhood will display only those computers in the local or remote hosts file, even if you have specified a WINS server.

NOTE: *To use the browsing mode for a domain, you must specify the domain's WINS server(s) in the hosts file. You must specify the WINS server(s) only if you want to use the browsing mode.*

To view your domains, double-click the **Extranet Neighborhood** icon on your desktop. To reload the hosts files in this screen, press the F5 key.

Add Host to Aventail Dialog Box

To open the **Add Host to Aventail** dialog box, click **Add Host** on the **Extranet Neighborhood Properties | Local** tab.

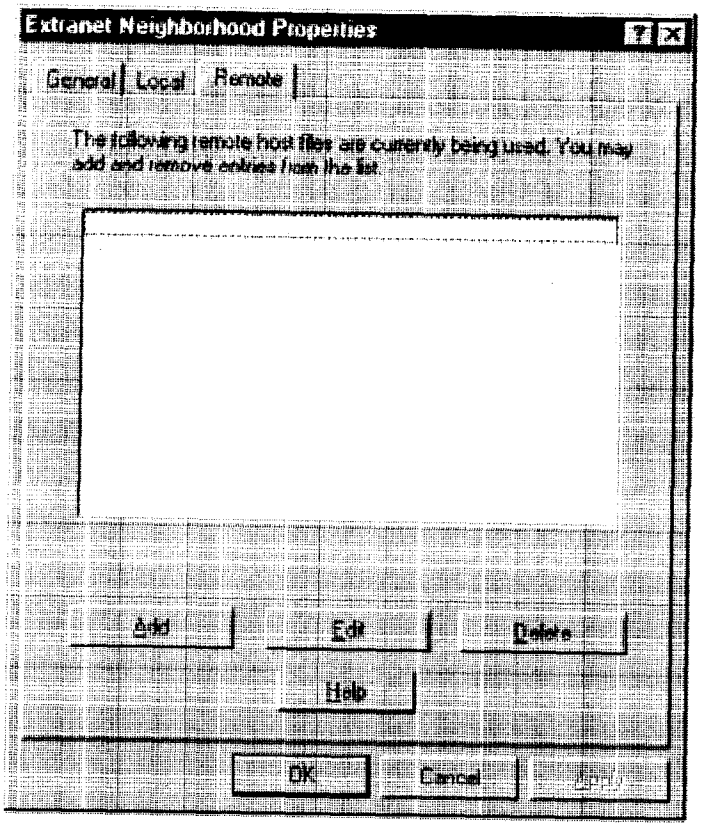


Aventail Connect automatically places hosts within the domain that is selected when you click **Add Host**. Select the correct domain before clicking **Add Host**. You must specify a domain before you can add hosts to that domain.

In the **Host name or IP address** box, be sure to enter the server's Internet address, not its Windows machine name.

THE REMOTE TAB

If the network administrator has configured Extranet Neighborhood to use a remote hosts file, this tab displays the information about the currently configured remote hosts file(s). Server name, host name or address, pathname, and username are all configurable through the **Remote** tab.



Remote hosts files are always used in conjunction with a local hosts file. When you add a remote hosts file to the list, Extranet Neighborhood adds the path to the local hosts file. Extranet Neighborhood always has a single local hosts file; this file can include references to multiple remote hosts files.

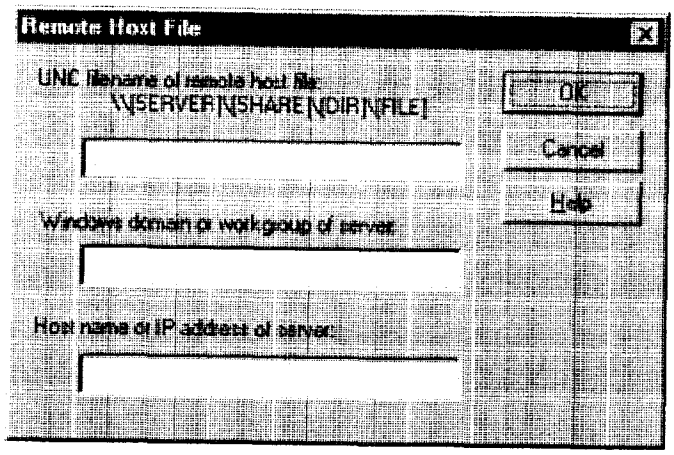
The most common configuration is one remote hosts file (with all domains and hosts in the remote hosts file) and one local hosts file that contains a pointer to the remote hosts file. If you want users to share a common hosts file, and if you want to simplify administration, use a remote hosts file.

To add entries to the list of remote hosts files, click **Add**. The **Remote Hosts File** dialog box appears, and you can type the names of the remote hosts file(s) you want to add.

NOTE: *To access remote hosts files, Aventail Connect must be running and configured correctly.*

Remote Hosts File Dialog Box

To open the **Remote Hosts File** dialog box, click **Add** on the **Remote** tab.



When entering the Universal Naming Convention (UNC) filename of the remote hosts file that you are adding, note that the [SERVER] name is the Windows machine name, not its IP address or hostname.

In the **Host name or IP address of Server** box, be sure to enter the server's Internet address, not its Windows machine name.

NOTE: *Extranet Neighborhood ignores any remote hosts files that it cannot access.*

Troubleshooting

Aventail Connect-related problems tend to fall into four categories: Installation, Network Connectivity, Configuration, and Application and TCP/IP Stack Interoperability.

AVENTAIL CONNECT INSTALLATION PROBLEMS

When the instructions in "Installing" in the *Administrator's Guide* are followed, Aventail Connect installation problems rarely occur. When they do occur, they are often the result of:

- **Toolbars, virus-checking utilities, or other Windows applications running during the installation**

  If any of these are running during a failed installation, close them, uninstall Aventail Connect, reboot, and then re-install Aventail Connect, ensuring that the toolbars, virus-checking utilities, or applications are not automatically restarted when the system reboots.

- **Insufficient RAM or free space on the volume to which Aventail Connect is being installed**

  If you suspect either of these as the cause of a failed installation, increase the available resources and retry the installation.

- **Corrupted Aventail Connect installation media, or corrupted or incomplete FTP of Aventail Connect self-extracting, executable installation file**

  If you suspect corrupted Aventail Connect installation diskettes as the cause of a failed installation, contact Aventail Technical Support (206.215.0078) for assistance in determining whether the files on the diskettes may have been corrupted and whether Aventail or your vendor must supply replacement diskettes.

  If you suspect a corrupted or incomplete FTP transfer of Aventail Connect installation files obtained over the Internet, retry the transfer, taking care to ensure that the FTP client is in binary mode and confirm that the transfer completes normally. Contact Aventail Technical Support to confirm that the byte size of the transferred installation file is correct.

- **Installation to a workstation on which Aventail Connect was running or from which a previous version of Aventail Connect was not completely uninstalled**

  If you suspect either of these circumstances as the cause of a failed installation, contact Aventail Technical Support.

- **Installation script errors**

  Aventail Connect is installed with InstallShield. If InstallShield reports errors during a failed installation, note the text of the error messages and the specific circumstances in which they occurred and contact Aventail Technical Support.

NETWORK CONNECTIVITY PROBLEMS

Before Aventail Connect can successfully redirect WinSock application connections:

1. The workstation on which Aventail Connect is installed must also have a properly installed, WinSock-compatible, TCP/IP stack running on it.

   This installation can be confirmed by successfully pinging the IP address of the workstation, from the workstation itself, using a WinSock ping application. If this test fails, the failure must be corrected before Aventail Connect can be tested and before Aventail Technical Support can provide assistance.

2. Basic TCP/IP network connectivity must exist between the client workstation on which Aventail Connect is installed and the extranet (SOCKS) server(s) to which it is configured to redirect connections.

   This connectivity can be confirmed by successfully pinging the extranet server(s) by IP address, from the client workstation. If this test fails, the failure must be corrected before Aventail Connect can be tested and before Aventail Technical Support can provide assistance.

3. Basic TCP/IP network connectivity must also exist between the extranet server(s) and the network host(s) to which the extranet server(s) are expected to proxy connections.

   This connectivity can be confirmed by successfully pinging the network host(s), by IP address, from the extranet server(s). If this test fails, the failure must be corrected before Aventail Connect can be tested and before Aventail Technical Support can provide assistance.

AVENTAIL CONNECT CONFIGURATION PROBLEMS

This section addresses troubleshooting of simple Aventail Connect configuration problems. Troubleshooting complex Aventail Connect configuration problems is beyond the scope of this section.

It is easiest to troubleshoot Aventail Connect configuration problems by creating and testing simple Aventail Connect configuration files, such as those that may be created with the Aventail Connect configuration wizard. However, all references to host and domain names must be removed from configuration files created with the wizard, before testing, to defer possible name resolution complications until the files can be demonstrated to work with IP addresses alone.

NOTE: The IP address and SOCKS port number of the extranet (SOCKS) server(s) to which Aventail Connect must connect must be known before troubleshooting Aventail Connect configuration problems. Neither Aventail Connect, nor Aventail Technical Support, can discover the IP address or port number of the extranet server(s).

When troubleshooting Aventail Connect configuration problems, confirm that the Aventail Connect configuration file that is currently selected in the **Configuration File** dialog box is the one intended for testing.

After selecting a configuration file to test, open the Aventail Connect Config Tool and:

1. Confirm that the extranet server has been correctly identified by IP address.

   Click the **Servers** tab, select the server alias and then click **Edit...**. Compare the IP address in the **Hostname or IP** box with that of the extranet server.

   If the extranet server is a SOCKS v5 server, click **SOCKS v4** in the "SOCKS Version" area of the **Servers** tab. Then click **Detect Version**. The selection will revert to **SOCKS v5**, indicating that Aventail Connect detected a SOCKS v5 server running at the IP address specified in the **Hostname or IP** box.

   If, on the other hand, the extranet server is a SOCKS v4 server, click **SOCKS v5** in the "SOCKS Version" area. Then click **Detect Version**. The selection will revert **SOCKS v4**, indicating that Aventail Connect detected a SOCKS v4 server running at the IP address specified in the **Hostname or IP** box.

   If **Detect Version** fails to detect an extranet server of either version, it is possible that no extranet server is running on the host identified in the **Hostname or IP** box. Contact your extranet server administrator to confirm that the extranet server is running at the address specified.

2. Confirm that all Aventail Connect authentication modules are enabled.

   Click the **Authentication** tab and confirm that the "traffic light" icons for all of the authentication Modules are green, indicating that the modules are enabled. Enabling all the modules configures Aventail Connect to attempt any form of authentication demanded by the extranet server or null (no) authentication. Note the form of authentication demanded by the extranet server and, if necessary, obtain the proper authentication credentials, such as an extranet server username and password, from the extranet server administrator.

3. Confirm that the network hosts to which the extranet server is expected to proxy connections are within a redirected destination.

   Click the **Destinations** tab, select the destination that includes the network host to which the extranet server is expected to proxy connections, and then click **Edit...**. Confirm that the definition of the Destination includes the network host.

   Next, click the **Redirection Rules** tab. Confirm that connections to the Destination are configured to be redirected by the extranet server.

After making any necessary changes to the Aventail Connect configuration, restart Aventail Connect and then restart any WinSock applications before testing the new configuration.

Application and TCP/IP Stack Interoperability Problems

Aventail Connect is intended to "automatically socksify" all "well-behaved" WinSock applications. Occasionally, you may find WinSock applications that Aventail Connect does not socksify, due to interoperability problems with the application.

Aventail Connect is also intended to run on all WinSock-compliant Microsoft Windows TCP/IP stacks. Aventail Connect does not alter or replace WinSock or any other core TCP/IP components (files) provided by the operating system. Occasionally, you may find WinSock stacks on which Aventail Connect does not run as expected, due to interoperability problems with the stack.

If you suspect an application or stack interoperability problem, report it to Aventail Technical Support. Aventail will make every reasonable effort to resolve interoperability problems.

Aventail Connect Trace Logging

Aventail Connect includes a Logging Tool for tracing Aventail Connect and WinSock activity. Aventail Connect traces are often useful in troubleshooting Aventail Connect network, extranet server, and WinSock application interoperability problems. Aventail Technical Support engineers may request that you perform a verbose trace, log it to a file, and e-mail it to them as an attachment.

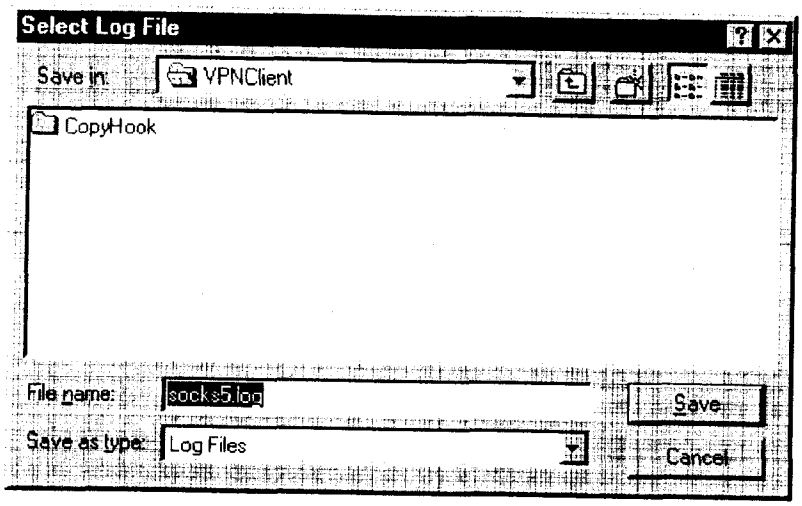
To run an Aventail Connect trace

1. Close any WinSock applications that are running on the workstation.
2. If Aventail Connect is running, close it and then restart it.
3. Start an Aventail Connect trace.

   In Windows 95, Windows 98, and Windows NT 4.0, right-click the minimized **Aventail Connect** icon in the system tray, and click **Logging Tool**. In Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51, double-click the **Logging Tool** icon in the Aventail program group. The Aventail Connect **Logging Tool** window will open, as illustrated in Figure 1, below.
4. On the **Log** menu, confirm that the **Trace** command is checked. If it is not, click **Trace** to enable it.

To save an Aventail Connect trace to a file

1. On the **Log** menu, confirm that the **Log To File** command is checked. If it is not, click **Log To File** to enable it.
2. The **Select Log File** dialog box (shown below) appears. Enter a file name and click **Save**.



ERROR MESSAGES

Occasionally, you may see an error message while running Aventail Connect. The following table explains some of the more common Aventail Connect error messages.

Error Message	Meaning
Setup has determined that your computer does not have this support and needs the WinSock 2 patch, available from Microsoft.	SETUP: To install Aventail Connect 3.1, you must first install the Microsoft WinSock 2 upgrade.
The patch is available for download on the Microsoft Web site, at http://www.microsoft.com/Windows95/downloads/contents/wuadmintools/s_wunetworkingtools/W95Sockets2/default.asp.	SETUP: Location of the Microsoft WinSock 2 upgrade.

Error Message	Meaning
You must have administrator privileges to install.	SETUP: On Windows NT machines, you must have administrative privileges to install or uninstall Aventail Connect.
Setup has detected that a previous installation of (....) is present. Would you like to continue and upgrade to (....)? Pressing NO will leave your existing installation intact and will cause Setup to terminate.	SETUP: Retain the previous installation of Aventail Connect by pressing NO. Replace with the newer installation by pressing YES.
The package does not contain the necessary 3.1 files. Please contact your administrator.	SETUP: Setup cannot find the necessary Aventail Connect 3.1 files.
The package does not contain the necessary 2.6 files. Please contact your administrator.	SETUP: Setup cannot find the necessary Aventail Connect 2.6 files.
The file you have selected is not a valid Aventail setup file. Would you like to create it?	CUSTOMIZER: Create a new setup file, or retain a previous setup file.
Customizer must be run from a valid Customize directory. Your changes will not be saved.	CUSTOMIZER: Must run Customizer from a valid Customize directory.
The Connect executable does not have a valid Aventail digital signature.	The specified signature is not valid.
Connect cannot find your license file, aventail.alf.	Aventail Connect cannot find a valid Aventail license file, aventail.alf.
Connect cannot load because your license file does not contain a license.	The license file exists, but it contains no license.
This version of Connect does not support HTTP servers.	Aventail Connect 2.6 does not support HTTP servers.

Reporting Aventail Connect Problems

Report Aventail Connect problems to Aventail Technical Support by completing and submitting an Online Support form on the Support page of the Aventail Web site, **http://www.aventail.com**.

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 it's 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.