EXHIBIT E1

DECLARATION OF CHRIS HOPEN

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent No. 6,502,135	)		
	)		
Munger et al.	)	Group Art Unit:	Central Reexamination Unit
	)		
Filed: February 15, 2000	)		
	)		
For: AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	)	Examiner:	Not assigned.
	)		
	)	Confirmation No.:	n/a
	)		
	)		
	)		

DECLARATION OF CHRIS A. HOPEN UNDER 37 C.F.R. § 1.132

I, CHRIS HOPEN, do hereby declare and state:

1. I am a citizen of the United States, and reside in 19805 15th Avenue NW, Shoreline, Washington.

2. I am presently the Chief Executive Officer of HomePipe Networks, Inc., based in Seattle, Washington.

3. Prior to HomePipe, I was affiliated with Aventail, Inc., until that company was acquired by SonicWall, Inc. in 2007. I helped co-found Aventail in 1996, and served as its Chief Technical Officer and Vice-President of Engineering from 1996 to 2007.

4. While I was affiliated with Aventail, I was involved in the design, development and distribution of all of Aventail's network security products.

5. In 1997, Aventail released a set of SOCKS v5 compliant VPN software products including AutoSOCKS, MobileVPN and PartnerVPN. AutoSOCKS was a client-based software product that ran on user's computers, while Mobile VPN and Partner VPN were server-based products.

6. When paired with Aventail MobileVPN or PartnerVPN server products, Aventail AutoSOCKS would automatically establish a VPN to give the remote user access to secured network resources on a private network. The AutoSOCKS client and the server would automatically authenticate the remote user and encrypt all communications with the remote user.

7. Version 2.1 of the AutoSOCKS product was publicly distributed in the summer of 1997. Exhibit A is a copy of a May 2, 1997 Aventail press release announcing the AutoSOCKS, MobileVPN and PartnerVPN products. Exhibit B is a copy of a June 23, 1997 article in InfoWorld reviewing the AutoSOCKS v2.1 and MobileVPN v2.0 products.

8. Aventail included printed manuals with the software packages that it distributed. Exhibit C is a copy of the Aventail AutoSOCKS v2.1 Administrator's Guide that was distributed with the AutoSOCKS v2.1 software. This document was distributed without any confidentiality restrictions.

9. I estimate that thousands of copies of the Aventail AutoSOCKS v2.1 software that included the AutoSOCKS v2.1 Administrator's Guide were distributed to customers during 1997 and 1998.

10. In the fall of 1998, Aventail announced a product called the Aventail Extranet Center ("AEC"). Exhibit D is a copy of an October 12, 1998 Aventail press release announcing the Aventail Extranet Center product.

11. The AEC product had three components: (i) the Extranet Server (which resided and ran on a server), (ii) the Aventail Management Server and Config Tool (which was used to configure server and client installations), and (iii) the Aventail Connect client software (which resided and ran on client computers).

12. Like the earlier Aventail VPN solution, Aventail Connect would, when paired with the Extranet Server, automatically establish a VPN between a remote user and a private network to give the remote user access to secured network resources on a private network. The Aventail Connect client and the Extranet Server would automatically authenticate the remote user and encrypt all communications with the remote user.

13. The initial release version of the AEC product was version 3.0. The AEC v3.0 product included version 3.01/2.51 of Aventail Connect and version 3.0 of the Aventail Extranet Server.

14. The AEC v3.0 product with its client and server components was publicly distributed during no later than January of 1999.

15. Exhibit E is a copy of the Aventail Connect v3.01/2.51 Administrator's Guide that was distributed with the Aventail Connect v3.01/2.51 software. Exhibit F is a copy of the Aventail Extranet Server v3.0 Administrator's Guide that was distributed with the Aventail Extranet Server software. Both of these documents were distributed without any confidentiality restrictions.

16. I estimate that Aventail distributed thousands of copies of the AEC v3.0 product (including the Administrator Guides for Aventail Connect and Extranet Center) during the first six months of 1999.

17. Aventail announced version 3.1 of the Aventail Extranet Center product in May of 1999. This version of AEC included Aventail Extranet Server v3.1 and Aventail Connect v3.1/v2.6. Exhibit G is a May 26, 1999 Aventail press release announcing the AEC v3.1 product. Exhibit H is copy of an August 9, 1999 Aventail press release reporting that Aventail had begun shipping the AEC v3.1 product to customers.

18. I recall that Aventail began distributing the AEC v3.1 product to its larger customers in June and July of 1999. Two such customers that I recall having received the AEC v3.1 product in June or July of 1999 were IBM and Morgan Stanley.

19. Exhibit I is a copy of the Administrator's Guide for the Aventail Connect v3.1/v2.6 product that was distributed with the Aventail Connect v3.1/v2.6 client software. This document was distributed without any confidentiality restrictions.

20. Aventail customers were not required to accept any obligations limiting their ability to use or disseminate the information contained in or associated with the AutoSOCKS v2.1 product, the Aventail Connect 3.01/2.51 product or the AEC v3.1 product, or the printed materials that accompanied each of these products.

21. I recall that between April and May of 1999, Aventail distributed pre-release versions of the AEC v3.1 product to organizations that conduct and report on the testing of network security products. I recall that Michael Fratto of Network World was one of the individuals who received a copy of the pre-release version of AEC v3.1 for testing and review between April and June of 1999. Mr. Fratto's review of the pre-release AEC v3.1 product was published in Network World on June 28, 1999. A copy of his review is provided in Exhibit J.

22. The pre-release version of AEC v3.1 provided to Mr. Fratto included a stable and feature complete version of Extranet Server component of the AEC v3.1 package. While I recall that certain bug fixes and other minor changes were made to this pre-release version of the server component of the AEC v3.1 package before it was distributed to customers, none of those changes significantly altered the features or functionality of the Extranet Server component that was later distributed to customers.

23. The Aventail Connect client in the pre-release version of AEC v3.1 product provided to Mr. Fratto, by contrast, was the same version of the Aventail Connect client that was later distributed to customers with the AEC v3.1 product in the summer of 1999.

24. The copy of the Aventail Connect v3.1/v2.6 Administrator's Guide that Mr. Fratto was provided with the pre-release version of the AEC v3.1 product is the same as the copy of this guide shown in Exhibit I. This printed Administrator's Guide did not change between the date it was given to Mr. Fratto and the date the final version of the AEC v3.1 product was distributed to customers.

25. The AEC v3.1 software and the Aventail Connect v3.1/v2.6 Administrator's Guide that were provided to Mr. Fratto between April and June of 1999 were provided without any restrictions or limitations on their use. Mr. Fratto was not required to enter into a agreement restricting his ability to disclose information about the pre-release AEC v3.1 product or the Aventail Connect v3.1/v2.6 Administrator's Guide as a condition of receiving and using these materials. Instead, I recall that it was Aventail's practice to simply provide recommendations to reviewers about installation and use of a pre-release version of a product, and information about the intended release date for the product.

****

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the patent subject to this reexamination proceeding.

Chris A. Hopen

05-27-11
Date

Exhibit A

May 2, 1997 Aventail Press Release

"Aventail Ships the First Standards-Based Virtual Private Network Software Solution," PR Newswire, PR Newswire Association LLC. May 2, 1997

Aventail Ships the First Standards-Based Virtual Private Network Software Solution

Publication: PR Newswire Publish date: May 2, 1997

Aventail MobileVPN and PartnerVPN Include Granular Access Controls and Support For Multiple Authentication and Encryption Methods

SEATTLE, May 2 /PRNewswire/ -- Aventail Corporation announced today the availability of the industry's only standards-based Virtual Private Network (VPN) software solutions. Aventail MobileVPN and Aventail PartnerVPN for Windows NT will begin shipping today and pricing starts at $4,995. UNIX versions will be available at the end of this month.

Aventail MobileVPN and Aventail PartnerVPN enable organizations to securely communicate over the Internet, allowing companies to extend the reach of their corporate intranet to customers, partners, remote offices, and mobile employees. Aventail's adherence to standards simplifies VPN deployment, enables interoperability, and leverages corporations' existing network investments.

"Aventail has moved the concept of a VPN to the next level. They are the only company providing a highly secure circuit-level solution that is deployable over existing network infrastructure and has the ability to work with a variety of authentication and encryption technologies," says Ira Machefsky, vice president at Giga Information Group.

The Only Standards-Based VPN Product

Aventail MobileVPN and Aventail PartnerVPN are the first VPN solutions based on SOCKS v5, an open Internet Engineering Task Force (IETF) standard. SOCKS is a distributed network security standard that represents the next-generation of Internet security. The SOCKS protocol has received widespread support from leading Internet vendors, including Netscape (Nasdaq: NSCP), Microsoft (Nasdaq: MSFT), IBM (NYSE: IBM), Sterling Software (NYSE: SSW), NetManage (Nasdaq: NETM), FTP Software (Nasdaq: FTPS), and Pointcast. NEC USA, Incorporated has been the driving force behind SOCKS with the vision that it would be the most important communication technology for the Internet.

Powerful Security and Management Tools

Aventail MobileVPN and Aventail PartnerVPN are the only products to support all of the popular authentication and encryption methods, such as SSL, DES, TripleDES, CHAP, RC4, MD4, MD5, and RADIUS. Other features include:

* Access Control Tool allows the IS administrator to specify access based on destination, source, application usage, type of encryption and/or authentication, and specific filtering profiles.

* Protocol Filtering blocks specific JAVA, ActiveX or any other application that could demand too much bandwidth or infect the network with a virus.

* Content Filtering blocks out objectionable content that may interfere with employee productivity.

* Traffic Monitor shows real-time inbound and outbound traffic through a graphical interface.

* Reporting and Logging Tool monitors and logs server activity so that reports can easily be produced from any SQL supported database.

* Administration Tool enables IS managers to easily configure the server and add or modify security or management modules.

Product Demonstrations at Networld+Interop

Aventail will be conducting product demonstrations in Booth 1710 at Networld+Interop in Las Vegas from May 6th to 8th.

About Aventail

Aventail Corporation is the leading developer of Virtual Private Network (VPN) solutions. Aventail software allows organizations to build session- layer VPNs so corporations can privately communicate with mobile employees, remote offices, and business partners. Aventail's standards-based products represent the next-level of secure communication by providing strong authentication and encryption, customizable access controls, comprehensive monitoring, logging and reporting capabilities.

Aventail offers four security solutions: Aventail MobileVPN, Aventail PartnerVPN, Aventail Internet

Policy Manager (IPM), and Aventail AutoSOCKS. Aventail MobileVPN enables mobile or remote employees to have secure and managed access into the corporate network. Aventail PartnerVPN allows a company to extend their network to customers, suppliers, remote offices or corporate partners. Aventail IPM allows corporations to control and implement their Internet security policies. Aventail AutoSOCKS enables client TCP/IP applications to securely traverse existing SOCKS-based firewalls and servers.

The company has offices in Seattle, Washington and can be contacted by phone: 888-SOCKSV5 (762-5785), fax: 206-777-5656, or email: info@aventail.com. Aventail's Web address is www.aventail.com.

NOTE: Aventail, MobileVPN, and PartnerVPN are trademarks of Aventail Corporation. All other brands, products, and service names mentioned are trademarks or registered service marks of their respective owners.

SOURCE Aventail Corporation

-0- 05/02/97

/CONTACT: Deanna Leung of Aventail Corporation, 206-777-5617, or deanna@aventail.com; or Jessica Maco of Reed, Revell-Pechar, Inc., 206-462-4777, or jmaco@rrp.com/

CO: Aventail Corporation ST: Washington IN: CPR MLM SU: PDT

DC-KW -- SFF006 -- 9928 05/02/97 08:01 EDT http://www.prnewswire.com

Exhibit B

InfoWorld June 23, 1997 Article

"Aventail delivers highly secure, flexible VPN solution,"
InfoWorld, page 64D (June 23, 1997)

[available at http://books.google.com/books?id=6TsEAAAAMBAJ&pg=PA70-IA6&lpg=PA70-IA6&dq=autosocks+v2.1&source=bl&ots=qpNSIifDny&sig=J-lO0yOnzsoezG3en5dJP5Rxr6s&hl=en&ei=HPLdTeT6C5D4swOxu9WNBw&sa=X&oi=book_result&ct=result&resnum=7&ved=0CEwQ6AEwBg#v=onepage&q=autosocks&f=false]

InfoWorld

June 23, 1997

SECTION: NETWORKING: Product Reviews; Pg. 64d

LENGTH: 1067 words

HEADLINE: Aventail delivers highly secure, flexible VPN solution

BYLINE: By Lai-Han Szeto

BODY:
For secure remote-access needs, Aventail's MobileVPN 2.0 and AutoSocks 2.1 comprise a virtual private network (VPN) software solution that lets you monitor and maintain access to your central site via application-level proxies.

Most VPN products, such as Microsoft's Steelhead technology, Digital's AltaVista Tunnel, and Data Fellow's F-Secure, do not address security issues beyond initial log-ins, tending to be server-centric. Aventail has engineered a solution that is user-centric, taking a more in-depth approach to VPN implementation.

Boasting nearly unmatched interoperability with other security protocols, MobileVPN and AutoSocks succeed as a VPN solution, but not without drawbacks: Unidirectional data flow prohibits broadcasting and remote administration, and the system requires third-party products for specific IP-layer features, such as IPX encapsulation.

High level of security

Aventail has developed its own connectivity protocol, Socks 5, which represents the next step in the evolution of the well-known Socks 4 protocol. The addition of security protocols makes Socks 5 a viable VPN tool and a contender to Microsoft's Point to Point Tunneling Protocol (PPTP). Aventail implements the Socks 5 protocol in the Aventail Server, the engine of its VPN package. Socks 5 is based on directed architecture, as opposed to the tunneled architecture one usually associates with VPN technology.

The server establishes a unidirectional connection with a remote client (AutoSocks) or second host site. A secured user can read, write, and execute to the host Server site according to the user's permission profile, but the host cannot likewise carry out transactions on the user's machine. This

setup prevents an intruder from accessing both sites.

Unlike IP-based protocols such as IP Security Architecture (IPSec), a tunneling protocol currently in the draft stage, Socks 5 compels a user to pass permission requirements once that user passes the system perimeter. Once users traverse firewalls, Socks 5 limits access to specific parts of your host system. The system locks out users from directories and applications according to their permission profile.

Socks 5 performs encryption and authentication at the session layer (Layer 5) of the IP packet, enabling an interoperability unmatched by most of Aventail's competitors.

Aventail products support Challenge Handshake Authentication Protocol, Secure Sockets Layer, and Remote Access Dial-In User Service authentication. In addition, Aventail deploys an open architecture to further enhance the flexibility of its products. Key management is compliant with Public Key Cryptography Standards. Encryption is DES and triple-DES enabled. Recently, Aventail announced Socks 5 capability with the IPSec, PPTP, and Layer 2 Tunneling Protocol security protocols.

Outside authority

MobileVPN represents an achievement in usability. I ran my VPN server on Windows NT 4.0 and used a Windows 95 client unit running AutoSocks.

MobileVPN carries handy administrative tools such as Proxy Chaining and Credential Caching, as well as myriad conventional utilities for alias tables, filtering, and session parameters.

AutoSocks acts as the remote-access agent that intercepts application requests between the client application itself and the WinSock interface. It offers logging and configuration GUIs that resemble a miniature version of MobileVPN, minus the high-level host controls.

I installed both pieces with minimal hassle, minus a certificate authority component. Aventail has no plans to become a certificate authority vendor, leaving the task to third parties, such as VeriSign. Unfortunately, this extra service can cost from $290 to as much as $2,000 per year per server.

Add this to Aventail's tiered licensing scheme, and the bottom line becomes a little steeper than that of most conventional VPN solutions. Whether it is worth the cost depends on the complexity of your security policies.

Fluctuating protocols

Implementing VPNs is not for the faint of heart or pocketbook. Tunneling protocols are maturing even as I write. The key to maintaining a foothold in the market is flexibility. In general, developers are building modular products in anticipation of the Internet Engineering Task Force's final draft of IPSec. It is hard to say what will become of Socks 5 (or Socks 6), but for now it has found a little-explored niche in secured connectivity.

Although MobileVPN and AutoSocks lack bidirectional communication and IP-layer features, their open architecture makes them compatible with multiple standards and provides a high level of security.

Lai-Han Szeto (laihan_szeto@infoworld.com) is a contract analyst at the InfoWorld Test Center.

THE BOTTOM LINE: EXCELLENT

MobileVPN 2.0 and AutoSocks 2.1

This virtual private network (VPN) software combination offers a secure and easy-to-manage remote-access solution.

Pros: Excellent proxy-level management; flexible architecture that complements other VPN and security products.

Cons: Third-party products required for specific IP-layer features such as IPX encapsulation; no broadcasting or remote administration.

Aventail Corp., Seattle; (888) 762-5785 (toll-free), (206) 777-5600; fax: (206) 777-5656; http://www.aventail.com.

Price: $4,999 per server for fewer than 25 connections; $66 per client seat for fewer than 25 seats. (Tiered pricing available.)

Platforms: MobileVPN: Unix, Windows NT; AutoSocks: Unix, Windows 3.x, Windows 95, Windows NT.

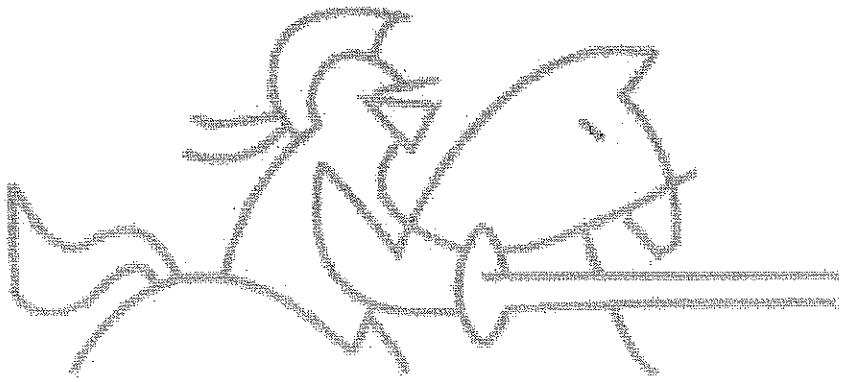
LOAD-DATE: June 23, 1997

Exhibit C

Aventail AutoSOCKS v2.1 Administrator's Guide

2.1 Aventail AutoSOCKS

ADMINISTRATION & USER'S GUIDE



AVENTAIL

Aventail AutoSOCKS v2.1 *Administration and User's Guide*

117 South Main Street
4th Floor
Seattle, WA 98104-2540
USA

Printed in the United States of America.

Trademarks and Copyrights

Table of Contents

Introduction

Welcome to the AutoSOCKS™ v2.1 secure Windows client for 16- and 32-bit Windows applications. AutoSOCKS v2.1 is the first commercial application to incorporate the SOCKS v5 security protocol standard, simplifying SOCKS deployment for end users and network managers.

AutoSOCKS transparently intercepts WinSock communication requests issued by TCP/IP applications and processes them based upon a set of routing directives (rules) assigned when AutoSOCKS is configured. (For more information about WinSock, TCP/IP, and general network commuuications, see "Getting Started.")

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

Features of AutoSOCKS v2.1:

- Supports both SOCKS v4 and SOCKS v5 standards
- Supports RFC1928 and RFC1929 SOCKS v5 standards
- Network-based setup provides a single configuration point with a simple user interface
- Transparently route connections from Windows applications to external networks through any SOCKS-based firewall system
- Logging utility to troubleshoot problems with network connections
- Enables internal network connections to pass through without interference
- Enables network redirection through multiple SOCKS servers
- Supports multiple authentication methods including SOCKS v4 Identification, username/password, CHAP, and SSL 3.0. Other authentication modules can be added
- Supports 16-bit WinSock 1.1 applications under Windows 3.1 and Windows for Workgroups 3.11
- Supports both 16- and 32-bit applications under Windows 95, Windows NT 3.51, and Windows NT 4.0
- Provides automated installation and uninstallation
- WinSock interoperability tested at Stardust WinSock Labs

About This Document

The AutoSOCKS v2.1 *Administration and User's Guide* provides basic information about AutoSOCKS v2.1. It is designed to iuclude entry-level data for non-technical users as well as more advanced installation, setup, and configuration information for network administrators.

This information is also available via online AutoSOCKS Help and the Aventail web site at **http://www.aventail.com/**.

Document Organization

This document is divided into two primary sections: the Administrator's Guide and the AutoSOCKS *Utilities Reference Guide*. The Administrator's Guide describes procedures for setting up, installing, and configuring AutoSOCKS for individual and multiple networked workstations.

The AutoSOCKS *Utilities Reference Guide* describes the AutoSOCKS system menu commands and utility programs. It contains detailed information about using Ping and Traceroute utilities and documents the autheutication/encryption modules and settings.

In addition to the AutoSOCKS v2.1 *Administration and User's Guide* and the AutoSOCKS *Utilities and Reference Guide*, this document includes a removable AutoSOCKS User's Supplement which describes screen displays and features that end-users may encounter while running AutoSOCKS in their client workstations. The document concludes with Appendix 1: Troubleshooting and a Glossary.

Check the Quick Start Card, a short document designed to help you install AutoSOCKS to an individual workstation.

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
ALL CAPITALS	Filenames and extensions, directory names, keynames, and pathnames.
Bold	Anything the user types, including command-line commands, addresses or URLs, options, and portions of syntax that must be typed exactly as shown. Dialog box controls (**Destination** field), e-mail addresses (**support@aventail.com**), URLs (**http://www.aventail.com/**), and IP addresses (**165.121.6.26**) are also bold.
Italic	Placeholders that represent information the user must insert.
"To Do" Procedures	Underlined *To Do* headings indicate procedures and step-by-step directions. Multi-step procedures are numbered; single-step procedures are bulleted.

Technical Support

If you experience problems installing, configuring, or running AutoSOCKS refer to any of the following:

- The Aventail web site, **http://www.aventail.com/**, for the latest list of known problems.
- The README.TXT documentation for additional information not contained in the manual.

If necessary, report problems to Aventail using the Bug Report form at the Aventail web site.

Aventail Technical Support:

Web site: **http://www.aventail.com/**

E-mail: **support@aventail.com**

Phone: 206.777.5640

Fax: 206.777.5656

About Aventail Corporation

Aventail Corporation is the leading vendor of next-generation Internet security systems. Its software allows organizations to secure their networks, manage their employees' access to the Internet and build Virtual Private Networks (VPNs). Creating a VPN gives organizations the ability to dynamically create a private communication or data channel over the Internet. Aventail's adherence to open security standards simplifies VPN deployment, enables interoperability, and leverages corporations' existing network investments. Its VPN solutions allow companies to extend the reach of their corporate Intranets to customers, partners, remote offices, and worldwide employees.

Aventail Corporation

117 South Main Street

4th Floor

Seattle, WA 98104-2540

Phone: 206.777.5600

Fax: 206.777.5656

http://www.aventail.com/

info@aventail.com

AutoSOCKS v2.1 *Administration and User's Guide*

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

- Getting Started with brief explanations of network security and communications
- Definitions of SOCKS and AutoSOCKS
- AutoSOCKS platform and installation requirements
- Installing AutoSOCKS, including network diagrams of Aventail VPN, Aventail Internet Policy Manager, and SOCKS v4-based server configurations
- Creating and editing configuration files

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

Getting Started

If you're new to AutoSOCKS technology, the following section will help you understand what AutoSOCKS is and does, as well as its relationship to network security in general.

Network Security in a Nutshell

Escalating threats of computer viruses and increased potential for unwelcome hackers 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 can't easily be configured 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. It 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 or intranet. A workstation whose traffic is proxied by SOCKS is considered "socksified." SOCKS is more than a standard security firewall. It also features:

- Client Authentication: (SOCKS v5 only) Authentication allows network managers to provide selected 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) has traditionally been difficult to proxy with the exception of SOCKS v5.
- Cross-Platform Support: Unlike most UNIX security solutions, SOCKS code can easily be ported to platforms such as Windows NT, Windows 95, and Macintosh systems.

What is AutoSOCKS?

AutoSOCKS automates the "socksification" of client applications, making it simple for workstations to take advantage of the SOCKS v5 protocol. When you run AutoSOCKS on your system, it automatically routes appropriate network traffic from a WinSock application to the SOCKS server. (WinSock is a Windows component that connects a Windows PC to the Internet using Transmission Control Protocol/Internet Protocol—TCP/IP.) The SOCKS server then sends the traffic to the Internet or the external network. Your network administrator defines sets of rules by which this traffic is to be routed.

AutoSOCKS is designed to run transparently on each workstation. In most cases, you'll interact with AutoSOCKS only when it prompts you to enter authentication information for a connection to a secure SOCKS server. You may also occasionally need to start and exit AutoSOCKS, although network administrators often configure it to run automatically at startup.

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

TCP/IP Communications

Windows TCP/IP networking applications such as e-mail or ftp use WinSock to gain access to the network or the Internet. WinSock (Windows Sockets) is the core component of TCP/IP under Windows. (TCP/IP is a suite of protocols that the Internet uses to provide for services such as e-mail, ftp, and telnet.)

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 intranet:

1. The application executes a Domain Name System (DNS) lookup to convert the hostname into an Internet Protocol (IP) address. 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. (The TCP handshake is the process by which two computers initiate communication with each other.) When the handshake is

complete, the application is notified that the connection is established, and that data may now be transmitted and received.

3. The application sends and receives data.

What Does AutoSOCKS Do?

AutoSOCKS slips in between the Windows TCP/IP application and the single access point—WinSock. In simple terms, AutoSOCKS redirects WinSock calls (both parameters and data) and reroutes them through a SOCKS-based server when required. The routing is determined by the rules described in the configuration file created when AutoSOCKS is installed. (See "Configuring AutoSOCKS.")

Because AutoSOCKS intercepts calls to WinSock, AutoSOCKS must duplicate WinSock functionality. Since AutoSOCKS also makes calls directly into WinSock, it must behave as a typical WinSock application as well. (See Figure 1.)

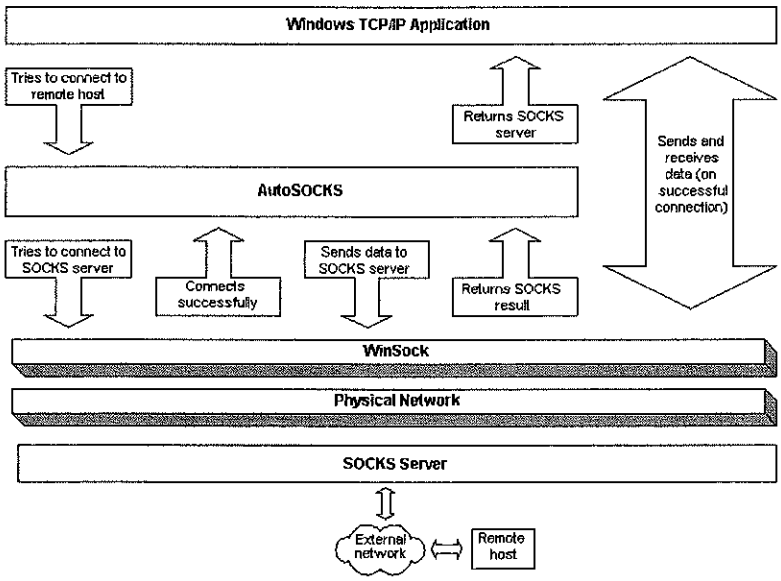


Figure 1. Network application calls intercepted by AutoSOCKS

With AutoSOCKS running, an application executes additional steps in order to connect to a remote host through WinSock. These steps must be transparent to the application so that it cannot differentiate between when AutoSOCKS is running and when it is not. The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by AutoSOCKS.

1. The application does a DNS lookup to convert the hostname to an IP address. However, if the application already knows the IP address, this entire step is skipped. Otherwise, AutoSOCKS does the following:

   - If the hostname matches a local domain string or does not match a redirection rule, AutoSOCKS passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack then performs the lookup as if AutoSOCKS is not running.
   - If the DNS proxy option is disabled, AutoSOCKS allows the request to go through unchanged.
   - 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 AutoSOCKS creates a false DNS entry (HOSTENT) that it can recognize during the connection request. AutoSOCKS will forward the hostname to the 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, AutoSOCKS creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells AutoSOCKS that the DNS lookup should be proxied, and that it should send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

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. AutoSOCKS does the following:

   a. AutoSOCKS checks the connection request.

      - If the request contains a false DNS entry (from step 1) it will be proxied.
      - If the request contains a real IP address and the rules in the configuration file say it should be proxied, AutoSOCKS calls WinSock to begin the TCP handshake with the server designated in the config file.
      - If the request contains a real IP address and the configuration file rules says that it should *not* be proxied, the request is passed to WinSock and processing jumps to step 3 as if AutoSOCKS is not running.

   b. When the connection is completed, AutoSOCKS begins the SOCKS negotiation.

      - It sends the list of authentication methods enabled in the configuration file.
      - Once the server chooses an authentication method, AutoSOCKS executes the specified authentication processing.
      - It then sends the proxy request to the 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, AutoSOCKS 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, AutoSOCKS encrypts the data on its way to the server on behalf of the application. If data is being returned, AutoSOCKS decrypts it so that the application sees clear text data.

AutoSOCKS Platform Requirements

AutoSOCKS runs under Windows 3.1, Windows for Workgroups 3.11, Windows 95, and Windows NT 3.51 and 4.0. These five platforms can be divided into two groups. Operating requirements and interface features unique to each group are described below.

Windows 95 and Windows NT 4.0

Windows 95 and Windows NT 4.0 have virtually identical interfaces. AutoSOCKS commands are accessed in the Programs list located on the Start menu and from the minimized AutoSOCKS icon on Taskbar tray.

System Requirements

AutoSOCKS system requirements for Windows 95 and Windows NT 4.0 include the following:

- Pentium-based personal computer
- Windows 95 or Windows NT 4.0
- 16 MB application RAM (8 MB on Windows 95)
- 3.5 MB hard disk space
- 16- or 32-bit WinSock-based TCP/IP application(s)
- Network-accessible SOCKS v4 or SOCKS v5 compliant server
- A WinSock compatible TCP/IP stack needs to be installed and configured prior to running AutoSOCKS. This can be the Microsoft-provided TCP/IP stack or a third-party TCP/IP stack.

Interface Features

- The AutoSOCKS program icon can be accessed via the Start menu, Programs option, and Aventail AutoSOCKS menu command.
- When AutoSOCKS is running in the background, the AutoSOCKS icon is visible in the system tray (unless the Hide Icon command is enabled).
- The AutoSOCKS system menu can be displayed by right-clicking the AutoSOCKS icon located in the Taskbar tray.
- AutoSOCKS can be uninstalled via the Start menu by using the **Add/Remove Programs** icon in the Control Panel folder.

Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51

Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51 have similar interfaces. AutoSOCKS commands are accessible from the Aventail AutoSOCKS program group and from the minimized icon's System menu when AutoSOCKS is running.

System Requirements

AutoSOCKS system requirements for Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51 include the following:

- 486-based personal computer
- 4 MB application RAM for Windows 3.1 and Windows for Workgroups 3.11; 16 MB for Windows NT
- 3.5 MB hard disk space
- 16- or 32-bit WinSock-based TCP/IP application(s)
- Network-accessible SOCKS v4 or SOCKS v5 compliant server
- A WinSock compatible TCP/IP stack needs to be installed and configured prior to running AutoSOCKS. This can be the Microsoft-provided TCP/IP stack or a third-party TCP/IP stack.

Interface Features

- The AutoSOCKS program icon is accessed via the AutoSOCKS program group window in Program Manager.
- The AutoSOCKS system menu is displayed by clicking the AutoSOCKS icon located in the AutoSOCKS program group.
- AutoSOCKS can be uninstalled using the Uninstall icon in the AutoSOCKS program group window.
- When AutoSOCKS is running in the background, the AutoSOCKS icon is minimized on the desktop (unless the Hide Icon command is enabled)

Installation Source Media

Regardless of platform, AutoSOCKS can be delivered on CD; in a network-delivered, self-extracting archive file; or on diskette.

This runs SETUP.EXE and installs AutoSOCKS. You can specify an installation directory, or AutoSOCKS will install in the default AutoSOCKS directory.

- CD: The CD contains the AutoSOCKS installation program, SETUP.EXE. It also contains in the \DOCS directory the AutoSOCKS v2.1 *Administration and User's Guide* formatted for 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 archive filename will be similar to AS21ED.EXE.
- **Diskette Based Source Media.** The diskette based source media is composed of two separate disks (labeled Disk 1 and Disk 2) that contain all of the AutoSOCKS installation files.

Installing AutoSOCKS

AutoSOCKS 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 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 instrnctions and information described under "Network Installation."

Note: Check the Quick Start Card for an easy-to-follow guide to individual workstation installation.

Configuration Files

Integral to the initial installation of AntoSOCKS is deciding how SOCKS traffic should be redirected through the network. Network redirection rules (used to determine if and how SOCKS redirection should occur) are defined in the AutoSOCKS configuration file. Configuration files are initially created at the end of the installation process; however; they can be added, edited, and removed at any time using the Config Tool (in Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51 via the System menu in the Aventail Program Group; in Windows 95 or Windows NT 4.0 via the Aventail icon in the Taskbar tray). The process of creating one or more configuration files is described under "Configuring AutoSOCKS."

If you are installing AutoSOCKS 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. An Installation Wizard will guide you through the steps, culminating with the option to create a configuration file.

Individual Installation

To install AutoSOCKS

Before running Setup, it is advisable to close all open Windows applications.

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 AutoSOCKS directory (\AS_v21).
   - If you are installing directly from diskette, run SETUP.EXE on disk 1.

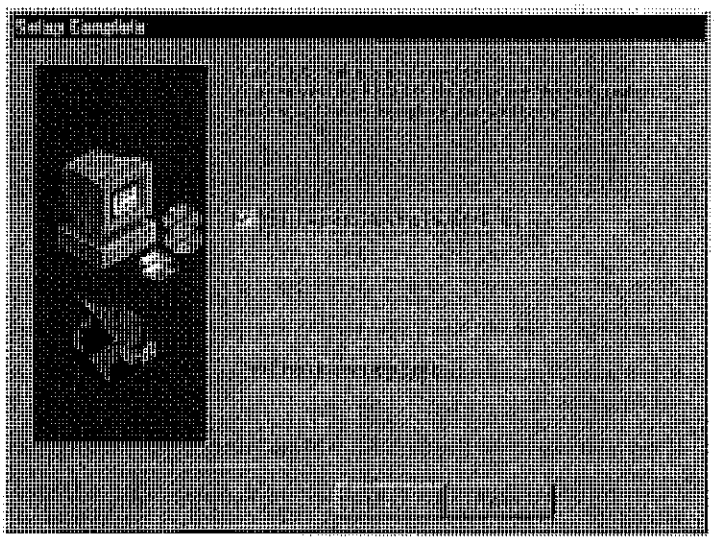
- If you are installing from a network-delivered self-extracting archive, simply run the archive file. This will extract the installation files and automatically launch the setup program.

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

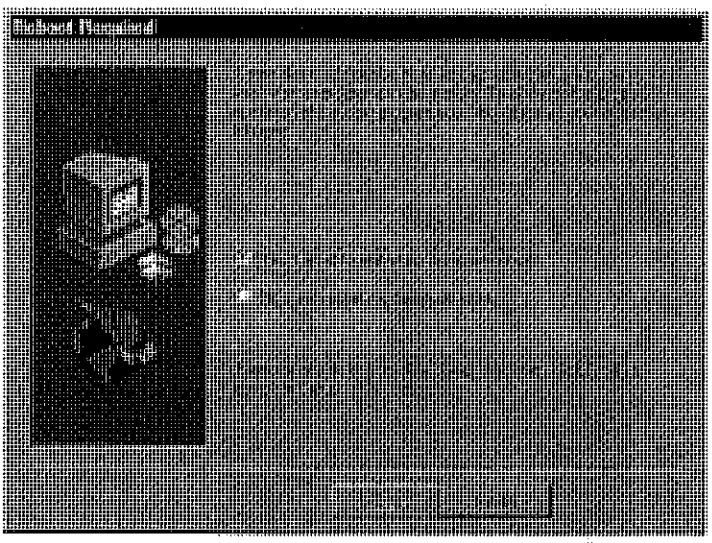
2. At the end of the Setup Program you can click the **Yes, I want to view the README file** box in the Setup Complete dialog box. This opens the README file for the latest information on AutoSOCKS.

   -OR-

   Simply click the **Finish** button to complete the Setup Program.



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



4. After restarting your PC, start AutoSOCKS for the first time.
5. AutoSOCKS will ask you if you want to run the Configuration Wizard.

   If you select **Yes,** then the Configuration Wizard will launch to help you create a new configuration file.

   If you select **No,** then AutoSOCKS will ask you to select a configuration file to use.
6. After creating or selecting a configuration file, AutoSOCKS will now be finished installing.

To uninstall AutoSOCKS

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

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

Network Installation

In general, the process of installing AutoSOCKS to multiple networked workstations involves selection of a file server to use, creation of a staging area for the AutoSOCKS software, and copying the AutoSOCKS files to a shared network directory from the source media. Additional

options include adding a default configuration file, and creating a universal batch/script file that specifies required default command line options wheu executed by the end user or installation personnel. AutoSOCKS files should be placed in a network drive which can be accessed as a mapped drive or, for Microsoft networks, via a UNC path name (**\\computer_name\share_name\AutoSOCKS**).

Networked Configuration File Setup

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

- Client configuration file distributed via a mapped network drive (Novell or Microsoft)
- Client configuration file distributed via a Microsoft UNC path and filename
- Local client configuration file common for all users, but distributed via the standard AutoSOCKS installation and upgrade program

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. It is an easily managed configuration because the configuration file is maintained by the network administrator and changes to network topology can be reflected quickly via network distribution. For example:

- A single-networked (usually read-only) configuration file is shared by more than one client workstation. This method is appropriate when workstations share identical message 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 message traffic routing rules.

Shared Configuration File Distribution

Shared configuration files can be easily distributed and, if necessary, updated via the network. All configuration files should be tested first before being distributed.

To distribute a shared configuration file

There are three methods for distributing shared configuration files.

- Copy the file to a Microsoft or Novell network mapped drive accessible by all users. Make sure that end users configure their AutoSOCKS clients to load the configuration file located on the mapped drive.

-OR-

- Copy the file to a Microsoft Windows workstation supporting UNC-sharing for file resources. (Both the 16- and 32-bit AutoSOCKS clients support specification of the configuration file using the Microsoft UNCs.)

This distribution method has all the benefits of placing the file on a network mapped drive with the added bonus of convenience—end users don't have to actually map the network drive.

-OR-

- Create a shared configuration file, AUTOSOCK.CFG, to be installed on workstations during the standard AutoSOCKS installation/upgrade process. (Place the shared configuration file into the DISK1 directory.) Whenever the AutoSOCKS client is installed or updated, it will to automatically copy AUTOSOCK.CFG to the end user's workstation and set AutoSOCKS to use it.

  Note: If a configuration file is specified as a command line option in the Setup program, installation of the AUTOSOCK.CFG configuration file will be overridden.

Setup Command Line Options

The AutoSOCKS setup program accepts several command line options which allow you to customize the installation process. By using options on the command line, installation can either run entirely unattended, or it can be used to specify a network-based AutoSOCKS configuration file. Each of the command line options are listed in the following table along with a brief explanation. Specifying any of the options that support unattended mode will cause the setup program to perform an automatic installation using default values for any options not explicitly specified.

Option	Explanation	Default Value	Unattended
config=*path*	Specifies the location of the AutoSOCKS configuration file. The destination can be either a local file, or can be specified with a UNC filename or common mapped drive.	Nothing	No
dir=*path*	Specifies the directory containing AutoSOCKS installation files.	**C:\Program Files\Aventail\ AutoSOCKS**	Yes
autostart	If specified, moves the AutoSOCKS application into the Startup group; otherwise AutoSOCKS must be started manually.	Don't put in startup	Yes
nocfg	Specifies that none of the configuration tools should be installed. This option will keep the Config Tool and Configuration Wizard from being installed.	Configuration tools are installed	No
nt=16|32|both	Selects the type of WinSock applications supported by AutoSOCKS: 16-bit, 32-bit or both. This option is only valid for Windows NT	Both	Yes

Configuring AutoSOCKS

Configuration files are created using the Config Tool application. This application can be launched during AutoSOCKS installation or any time you wish 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 Local Name Resolution (optional)
5. Manage authentication modules

These procedures are described in the text below.

To launch the Config Tool

The Config Tool opens with the Open AutoSOCKS Configuration File dialog box. After a configuration file is selected or a new file name is entered, the main window of the Config Tool appears.

1. Click the **Yes, I want to configure AutoSOCKS** box in the Setup Complete dialog box (during installation).

   -OR-

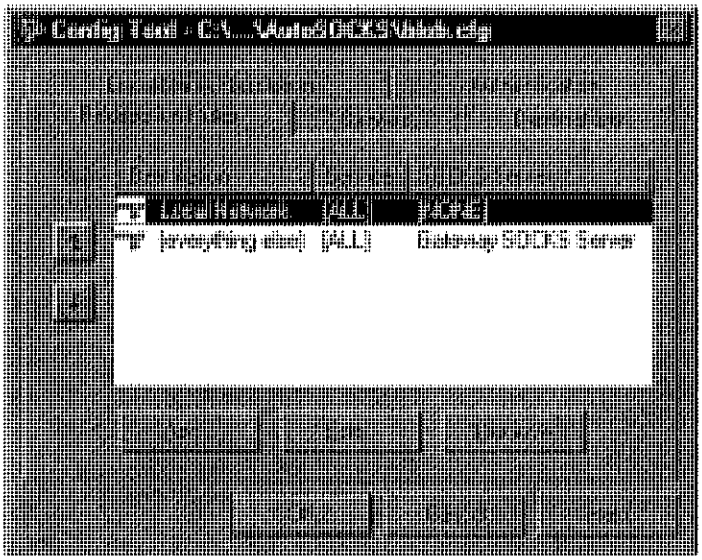
   Select Config Tool from the Aventail AutoSOCKS program group (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51) or the Aventail AutoSOCKS menu (Windows 95 or Windows NT 4.0 Programs menu option).

2. If you are creating a new configuration file, enter a name for the configuration file. (AutoSOCKS defaults to AUTOSOCK.CFG).

   -OR-

   Select the configuration file you wish to open.

   This displays the main window of the Config Tool.



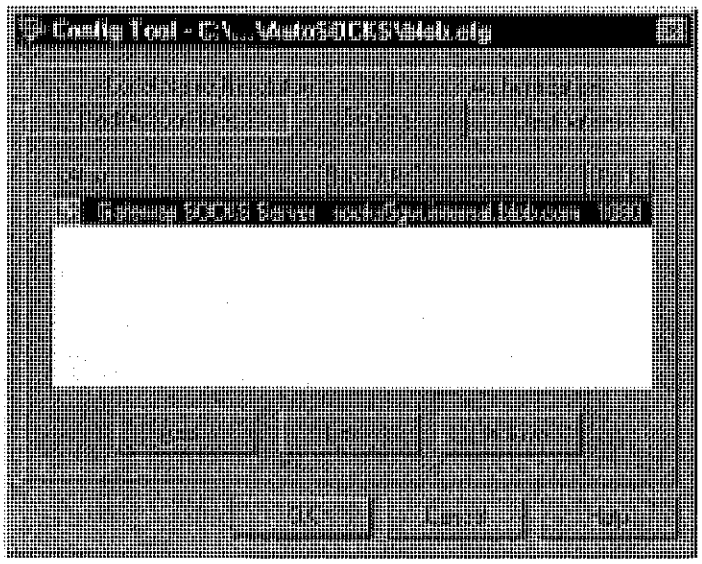
   The Config Tool window contains five tabs. The properties defined on each tab can be edited at any time.

Tab	Function
Redirection Rules	Specifies how network requests are routed to the SOCKS servers.
Servers	Defines the SOCKS servers.
Destinations	Specifies the network and host addresses that should be routed through SOCKS servers.
Local Name Resolution	(Optional) Specifies hostnames that will be resolved by the local workstation.
Authentication	Enables, disables, and sets properties for the authentication modules.

You can change the width of any of the fields on the tabs 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.

Define a SOCKS Server

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

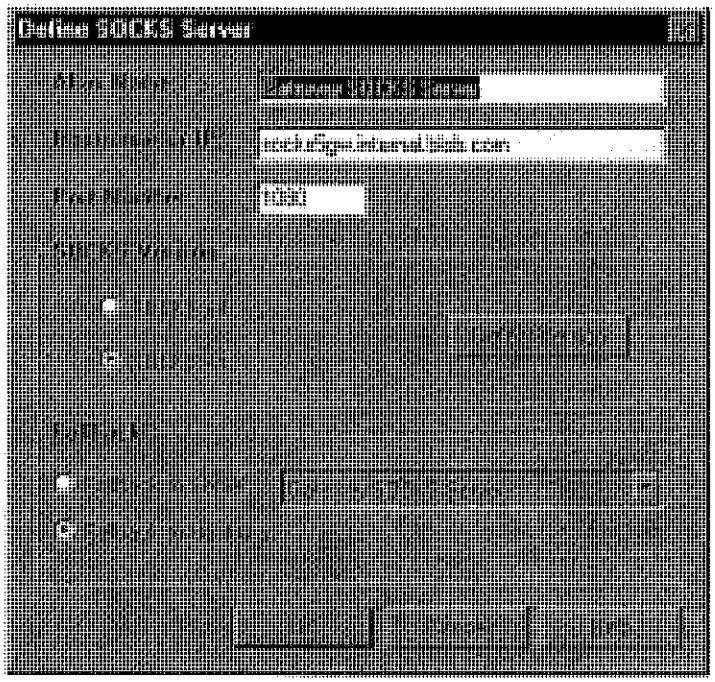


Field	Definition
Alias	The descriptive name you assign to the server. (The number is the SOCKS version.)
Host/IP	The hostname and/or IP address of the server.
Port	The port on which the server is listening.

To add a SOCKS server

1. On the Server tab, click the **Add** button.

   The Define SOCKS Server dialog box appears.



Field	Definition	
Alias Name	User-friendly alias for SOCKS server.	
Hostname or IP	Actual hostname or full numeric IP address for SOCKS server.	
Port Number	SOCKS server port. Default value is 1080.	
SOCKS Version	SOCKS v4:	SOCKS Version 4.0
	SOCKS v5:	SOCKS Version 5.0
	Detect Version:	Detect SOCKS version number.
Fallback	Fallback to Server:	SOCKS server alias for redundant server
	Fallback to Host Alias:	Use DNS records for redundancy

2. In the Alias Name box, type a user-friendly alias for the SOCKS server.
3. In the Hostname or IP box, type the actual hostname of the SOCKS server or its IP address.
4. In the Port Number box, type the SOCKS server's port number. If you don't enter a value, it defaults to the standard SOCKS port 1080.
5. Under SOCKS Version, select the version of SOCKS supported by the server. If you're unsure of the version, click the **Detect** button.

   Note: Typically you should select SOCKS v5 unless the server can only support SOCKS v4.
6. Under Fallback, directly specify a SOCKS server for redundancy or use the Host Alias to specify a SOCKS server.

To edit SOCKS server properties

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

  The Define SOCKS Server dialog box appears with the selected server data filled in. Edit any of the information.

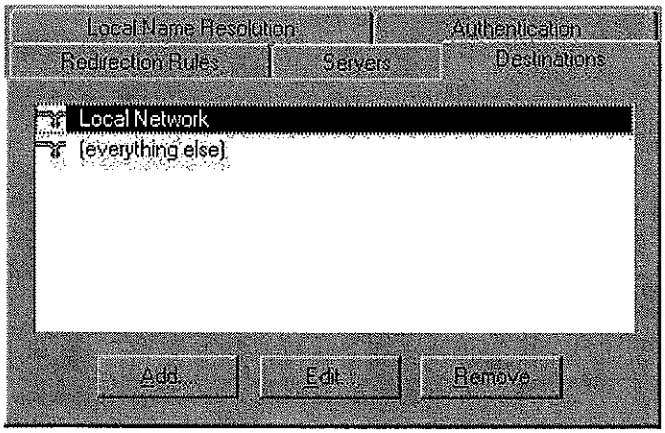
To remove a SOCKS server definition

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

  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.



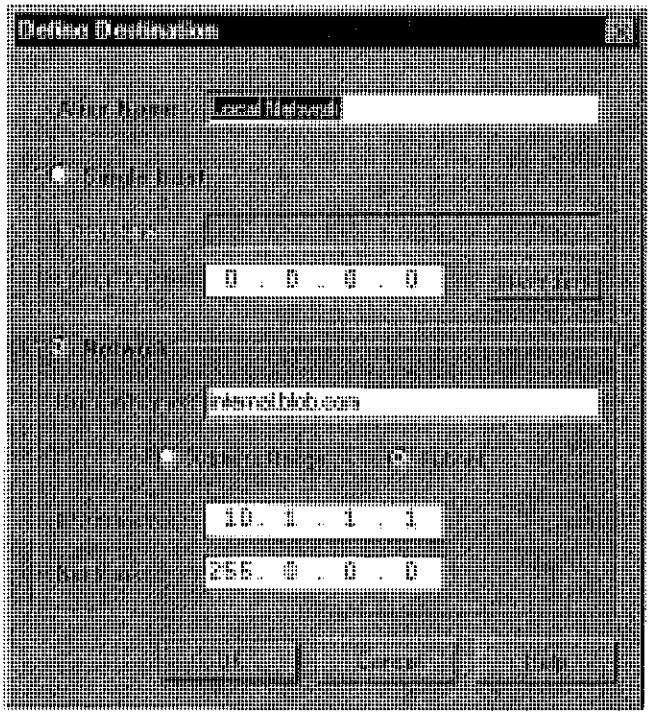
After one or more SOCKS servers are defined, destinations to be routed through them should be added.

Note: The **(everything else)** destination refers to all network and host addresses not otherwise defined.

To add a destination

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

   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:	Full numeric IP address
	Lookup:	Look up IP address
Network	One or more computers in a network	
	Domain Name:	Domain of the network
	Address Range:	Beginning and ending IP addresses
	Subnet:	IP address and netmask
	From:	Address Range: Starting IP address. Subnet: IP address
	To:	Address Range: Ending IP address. Subnet: Net mask

2. In the Alias Name box, type a user-friendly alias to use for the destination network or host.

3. Choose 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 don't know the Host's IP address, the **Lookup** button will help you locate it.

   -OR-

   Under Network, type the domain of the network and choose either the Address Range or Subnet options:

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 192.168.1.0 and an ending IP address of 192.168.1.255 would include all hosts on the 192.168.1 subnet.
Subnet	Enter an IP address and a net mask. This is another way to specify a group of destinations. For example, an IP address of 192.168.1.0 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 the **Edit** button.

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

To remove a destination

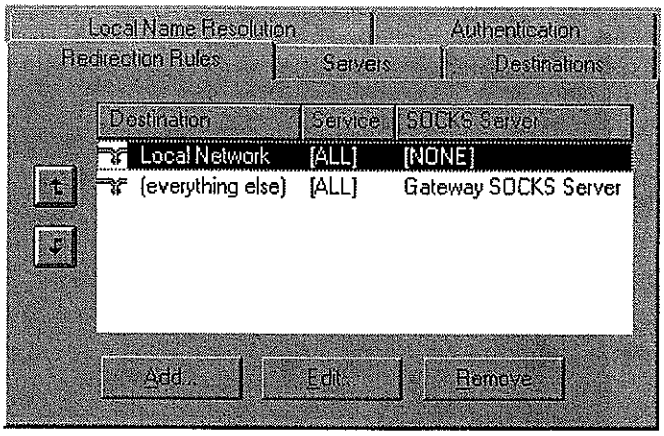
- Select the destination you want to remove and click the **Remove** button.

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

Enter Redirection Rules

Once servers and destinations are defined, you can then specify how you want AutoSOCKS 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.



In the above example, the redirection rules specify that network traffic on the Local Network will not be redirected throngh a SOCKS server. All traffic not directed to the Local Network will be proxied through the Gateway SOCKS Server.

Field	Definition
Destination	Destinations defined on the Destination tab
Service	Type of Internet traffic
SOCKS Server	Servers defined on the Server tab

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.

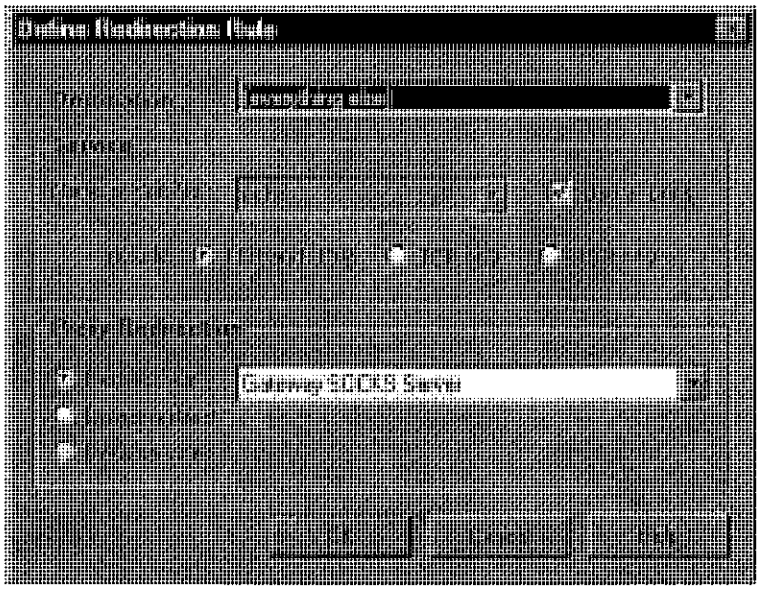
To add a redirection rule

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

Note: AutoSOCKS 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 the **Add** button.

The Define Redirection Rule dialog box appears.



Field	Definition	
Destination	Host or server destination for message traffic.	
Service	Type of Internet traffic.	
	Name or Port No.:	Select from a list of common service ports or enter a new port.
	Use all ports:	Apply the rule to all services.
	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 SOCKS 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, check the **Use all ports** box to apply the rule to all services. Otherwise, select an individual service from the **Name or Port No.** list.
4. Under Proxy Redirection, select one of three redirection options:

   Note: If you select Deny Service and the user has edit control of the Config file, the option can be circumvented by quitting AutoSOCKS or by changing the option in the dialog box.

To edit a redirection rule

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

  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 the **Remove** button.

  The redirection rule is deleted from the dialog box.

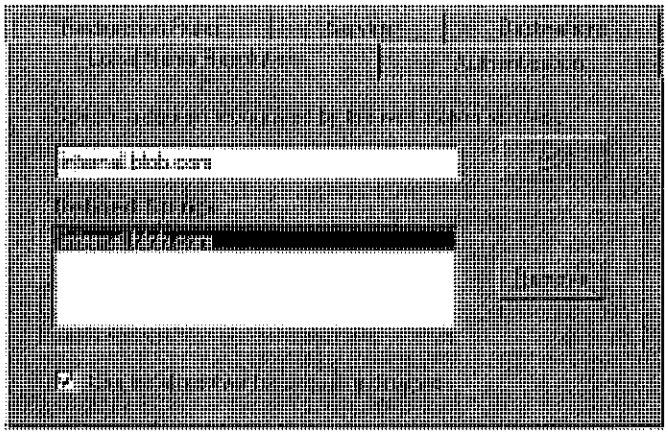
Define Local Name Resolution

Local Name Resolution instructs AutoSOCKS to resolve hostnames locally without needing to venture on to the Internet. This optional feature offers you another level of control over how AutoSOCKS 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 Local 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 **internal.blob.com** is added to the Defined Strings list, then a workstation attempting to connect to **www.internal.blob.com** would perform hostname resolution using the local TCP/IP stack.

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



Field	Definition
Specify Domain	New domain name
Defined Strings	List of domain names that can be resolved locally
Use local resolver	Pass through unqualified hostnames to the local resolver

To add a local domain name

- On the Local Name Resolution tab, type the new name in the Specify Domain text box and click the **Add** button.

  The new name is moved into the Defined Strings text box. It is now active.

To remove a local name

- Select the domain name you want to remove from the Defined Strings text box and click the **Remove** button.

  The domain name is removed from the list.

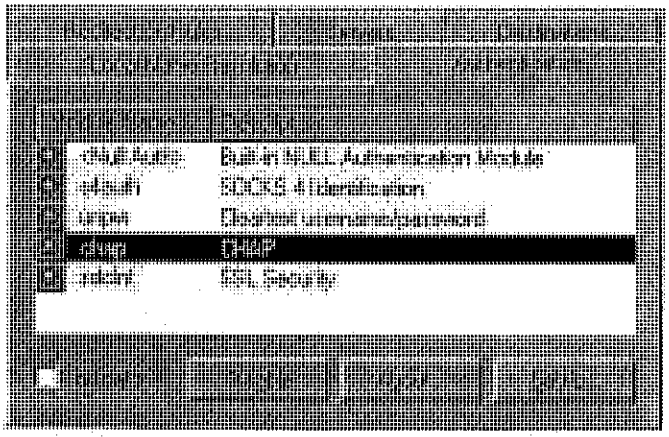
Managing Authentication Modules

SOCKS v5 servers often require user authentication before allowing access. AutoSOCKS authentication modules facilitate this process by displaying dialog boxes which ask for username and password information as well as other authentication credentials.

The current AutoSOCKS authentication modules (SOCKS v4 Identification, Username/Password, Challenge Handshake Authentication Protocol, and Secure Socket Layer) support an AutoSOCKS feature known as credential caching. Credential caching is the process of retaining your authentication credentials once they've been accepted by the SOCKS server. Using credential caching, you can enter your credentials for a SOCKS server once per AutoSOCKS session, rather than once for each individual connection (a tedious task for applications such as WWW browsers).

AutoSOCKS 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 AutoSOCKS or Windows, the memory cache is flushed and you must renter your credentials as prompted.

Authentication modules are managed and configured on 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 a visual indication of the authentication/encryption being used as network traffic is generated.

Each authentication module includes its own module-specific configuration. To view or edit a module's configuration dialog box, select the module from list ou the Authentication tab and then click the **Setup** button.

Authentication modules can be selectively enabled and disabled using the Disable/Enable button. By default, the modules are all enabled. This is indicated by the green button next to the module name. When a module is disabled, the button is red.

To configure the SOCKS v4 Identification module

AutoSOCKS includes backward compatibility for the SOCKS v4 protocol. SOCKS v4 does not support password authentication; only your username is sent unencrypted to the SOCKS server along with your connection request. Your username is determined by entries in the SOCKS v4 Identification Module configuration dialog box.

1. On the Authentication tab in the Config Tool, select **sv4auth** (SOCKS v4 Authentication) and click the **Setup** button.

   The SOCKS v4 Identification 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 the option **Prompt user for name** is selected, choose the desired caching option. (Currently only Memory Caching is available.)
3. After making appropriate selections, click **OK**.

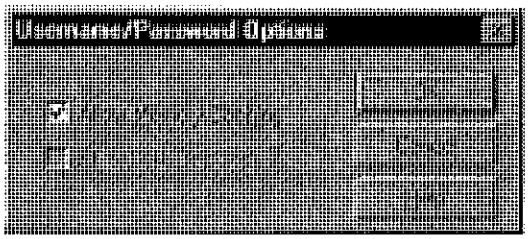
   The dialog box closes and the Config Tool is displayed.

To configure the Username/Password authentication module

AutoSOCKS supports the RFC 1928 (Internet standards document) username and password authentication protocol. This authentication method sends your username and password *in clear text* 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** (Clear text username/password) and click the **Setup** button.

   The Username/Password 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 is displayed.

To configure the CHAP Authentication module

AutoSOCKS 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** (CHAP) and click the **Setup** button.

   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	Currently Unavailable. (Stores encrypted credentials on disk for future sessions.)

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

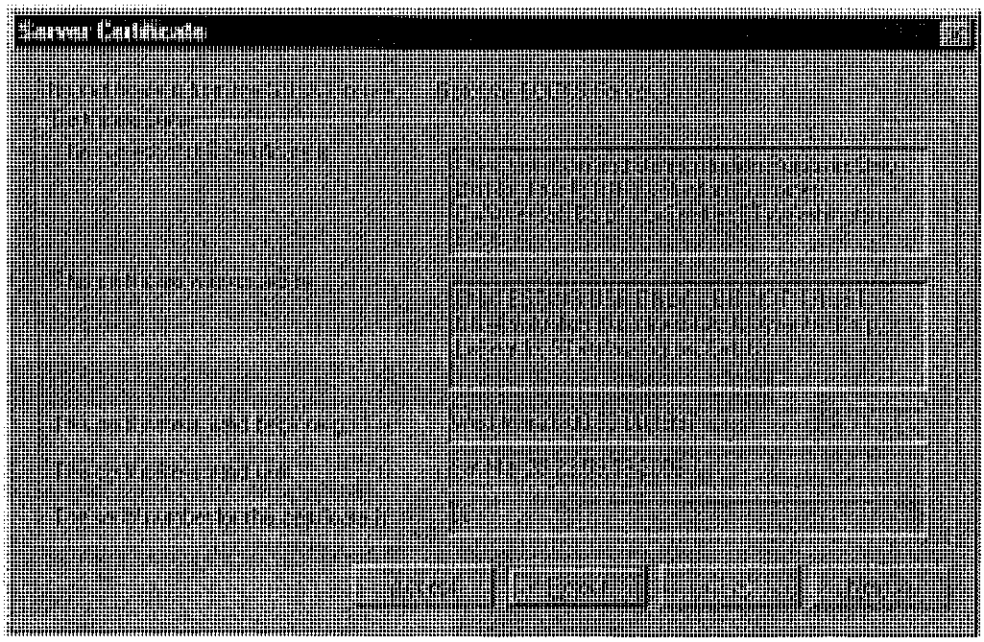
The dialog box closes and the Config Tool is displayed.

To configure the SSL security module

AutoSOCKS supports Secure Socket Layer (SSL) v3.0, a session-layer protocol for securing connections in a general, protocol-independent fashion. At this time, SSL is a TCP-only enhancement; when using SSL with UDP associations, the bulk data is passed without protection.

Normally SSL servers are required to have an RSA key pair and a certificate. RSA is a public/private-key cryptographic system; it creates a key pair: a private key (which, as the name suggests, is kept absolutely private and never shared) and a public key (which is widely published.)

However, 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 esseutially an electronic "statement" which verifies that a certain RSA public key is associated with a particular name.



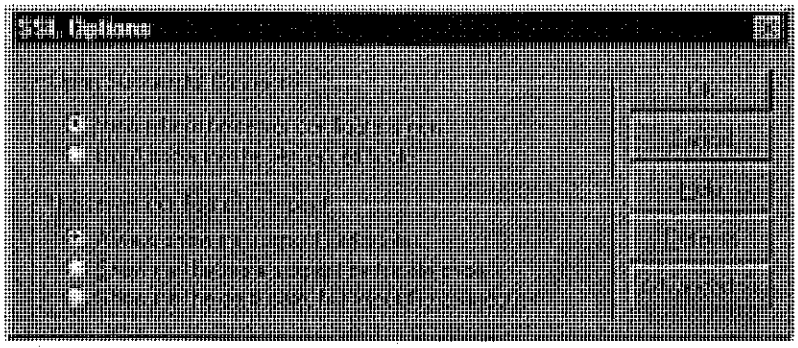
Certificates are issued by a Certification Authority (CA), and are linked together to form a construct called a certificate *chain of authorities*, each one having a previous entity vouching for its identity. In practice, chains generally include two certificates: one confirming the identity of the server,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

Certificates contain special integrity checks and electronic signatures which verify that the certificate is genuine, was issued by some 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.

The SSL module dialog box contains an initial set of options regarding the viewing of certificates. It expands into more detail when the **Advanced** button is clicked.

1. Ou the Authentication tab in the Config Tool, select **sslclnt** (SSL Security) and click the **Setup** button.

   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 hasn't been displayed during the current session.
	Don't show me the certificate.	Never display the server's certificate if it is deemed valid.
If a server certificate is suspect:		The certificate may not be valid.
	Always show me suspect certificates.	Each time a certificate is deemed suspect by AutoSOCKS, display it.
	Show me the same suspect certificate once.	Once a suspect certificate has been accepted by the user, don't display it again.
	Show me the certificate, but reject the connection.	Reject the connection, but display the suspect certificate.

2. Select an action that AutoSOCKS should take once it deems the server certificate acceptable. (Under normal circumstances, the server will provide AutoSOCKS with a certificate to match with one of AutoSOCKS' trusted roots, if any exist):

   - **View when the server certificate is new:** AutoSOCKS displays the certificate the first time it's seen. Subsequent connections to the same SOCKS server will not cause the certificate to be redisplayed.
   - **Don't show me the server certificate:** AutoSOCKS will never display a valid certificate.

3. Select an action that AutoSOCKS should take if it receives a server certificate that is suspect:

   - **Always show me suspect certificates**: AutoSOCKS 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?

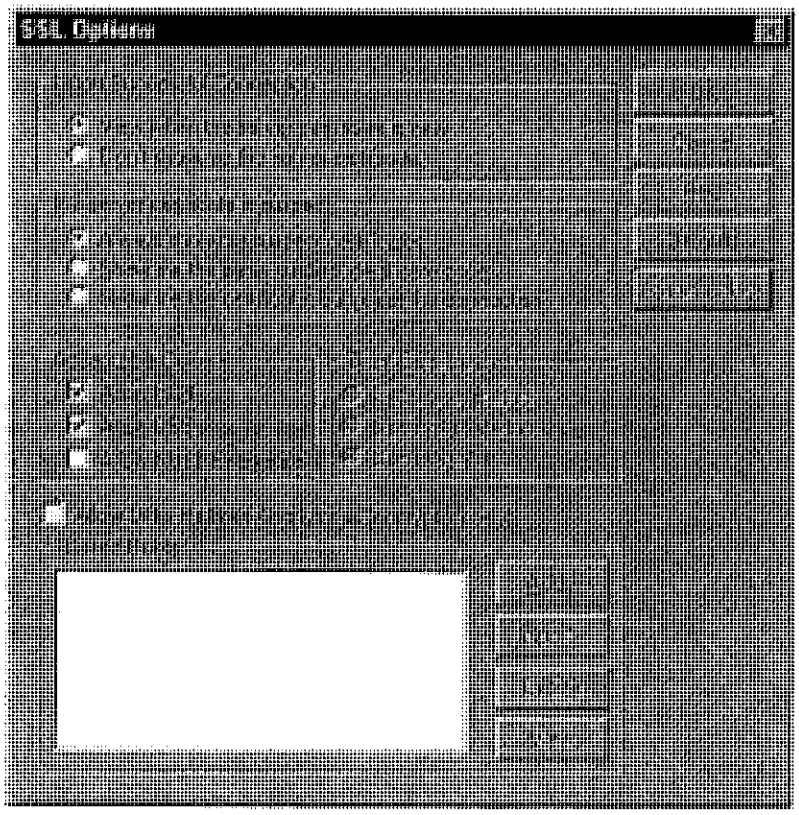
Did a trusted certificate authority (CA) issue the certificate?

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:** AutoSOCKS 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:** AutoSOCKS will reject a connection if the certificate is suspect. It will display the certificate to allow you to view it.

4. Clicking the **Advanced** button in the dialog box to expand the dialog box into acceptable cipher (a cryptographic algorithm used to encrypt the data stream) options.



Field	Description	
Allow RC4	Offer the RC4 cipher to the server.	
Allow DES	Offer the DES cipher to the server.	
Allow NULL Encryption	Do no encryption. SSL will be used to authenticate, not encrypt.	
Allow Diffie-Hellman Anonymous	Don't authenticate the server; only do encryption.	
Trusted roots	Choose a file with a certificate that specifies certificate chain roots that are to be trusted.	
	Add	Add a new trusted root.
	Import	Import a trusted root.
	Delete	Delete a trusted root.
	View	View a trusted root certificate file.

During the initial SSL connection negotiation, the client and the server negotiate which cipher to use. Checking a particular cipher in the dialog box doesn't mean that it will be used. Instead, each checked cipher is *offered* to the server, but the server must make the final determination. If the server requires a cipher that isn't selected in this dialog box, the authentication will fail.

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

- **Allow RC4:** AutoSOCKS encrypts the information using the RC4 cipher.
- **Allow DES:** AutoSOCKS encrypts the information using the DES cipher.
- **Allow Null Encryption:** AutoSOCKS allows the server to choose *no* encryption. Message integrity is still assured, but the data will be sent in the clear.
- **Allow Diffie-Hellman Anonymous:** AutoSOCKS will be able to communicate with the 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).

5. If necessary, add a trusted root to the list of trusted roots by pressing the **Add** button, and selecting a file that contains a trusted root certificate.

   When AutoSOCKS receives a certificate from a server, it looks at the root of the certificate chain and matches it against AutoSOCKS' list of trusted root certificates.

6. After making appropriate selections, click OK.

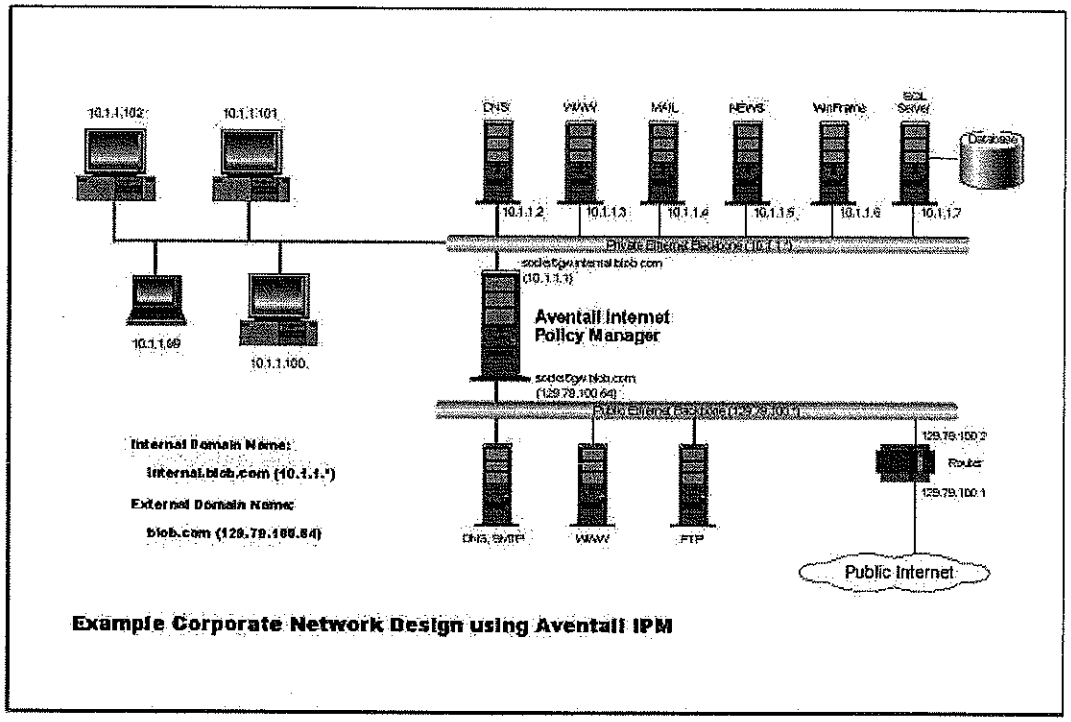
   The dialog box closes and the Config Tool is displayed.

Example Network Configurations

The following sections describe the setup of AutoSOCKS in an example network configuration using the Aventail Internet Policy Manager (IPM) and the Aventail VPN Server.

Configuration Using Aventail Internet Policy Manager

To better describe how to get started configuring AutoSOCKS for use with the Internet Policy Manager, we have created an example network configuration that will be used in all examples throughout this section. Below is an example network topology architecture that emphasizes simplicity to facilitate easy adaptation to real world network designs.



AutoSOCKS in an Aventail Internet Policy Manager Environment

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. To provide protection of the private LAN from unwanted external access, the Aventail IPM 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 proxied through the Aventail IPM.

The end user workstations (10.1.1.99 through 10.1.1.102) illustrate client workstations, onto which, AutoSOCKS will be deployed. Due to the routing restrictions described above, these clients will have no network access beyond the Aventail IPM unless they are running AutoSOCKS, which will automatically proxy their application traffic. In this situation, AutoSOCKS will forward traffic destined for the Internet to the Aventail IPM. Then, based on the administrative configuration, the Aventail IPM will proxy end user traffic out beyond the boundary on which the Aventail IPM is located. The client workstations used in this example are Microsoft Windows based PC's.

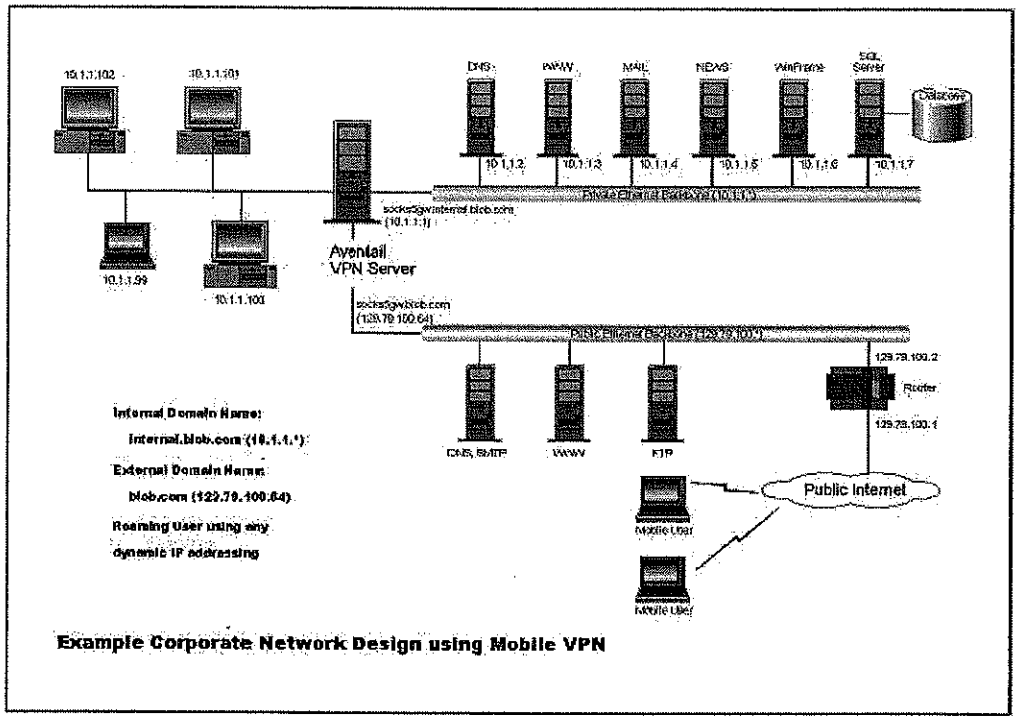
The other servers on the private segment are "internal" or private servers that contain information and tools that are not intended for public use or consumption. If these individual hosts require access beyond the Aventail IPM they can also be configured to use AutoSOCKS. As in the client workstation case, AutoSOCKS will allow applications running on these hosts to traverse the Aventail IPM public/private boundary. In most situations, for more stringent security, these hosts don't have access to the public network at all.

The Aventail IPM 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. 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. End user authentication has been enabled on the Aventail IPM server, which will require that users present their credentials before being allowed to have any connectivity to the external public network(s). For this example, Aventail IPM is configured to use RFC1929 Username/Password for authenticating connections AutoSOCKS forwards to it. For additional information on how to configure the Aventail IPM product, consult the Aventail IPM *Administration Guide*.

Subsequently, in most Aventail IPM environments there are large numbers of clients that require installation and configuration. For completeness we will illustrate how to install and configure AutoSOCKS on a large number of client workstations. The easiest and best mechanism for installatiou of AutoSOCKS to many client workstations is to follow the AutoSOCKS network installation procedures. For our example, we will be installing the base AutoSOCKS client distribution to a network file server that will be used to pull the AutoSOCKS software and client configuration to the desktops. It is often the case that MIS personnel install single copies of AutoSOCKS for testing and evaluating prior to mass deployment. The configuration file that is created through the testing phases will then be copied to a shared file server for group access. This way each client workstation maintains the exact same configuration as determined by the network security policy.

Configuration Using Aventail VPN Server

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



Example Corporate Network Design using Mobile VPN

AutoSOCKS in an Aventail Mobile VPN Environment

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 VPN 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 VPN 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 VPN server.

The mobile user workstations connected to the public Internet are the client workstations, onto which, AutoSOCKS will be deployed. Due to the routing restrictions described above, these clients will have no network access beyond the Aventail VPN Server unless they are running AutoSOCKS. Depending on the security policy and the Aventail VPN Server configuration, AutoSOCKS will automatically proxy their allowed application traffic into the private network. In this is situation, AutoSOCKS will forward traffic destined for the private internal network to the Aventail VPN Server. Then, based on the security policy, the Aventail VPN

Server will proxy mobile end 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 PC's.

The Aventail VPN 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. 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. End user authentication and encryption has been enabled on the Aventail VPN Server, which will require all end users to use AutoSOCKS to enable authentication and encryption of their sessions before being allowed to have any connectivity to the internal private network(s). For this example, the Aventail VPN Server is configured to use SSL for encryption of all sessions. For additional information on how to configure the Aventail VPN Server product, consult the Aventail VPN Server *Administration Guide*.

Installation and use of AutoSOCKS for remote access purposes differs a bit from its installation and use with the Aventail IPM product. First, configuration files need to be kept locally on the end user workstation or laptop. This is due to the inability to have a shared file server that allows direct access outside the perimeter of the private network. Second, not all traffic is passed through to the Aventail VPN Server. Only traffic that is destined for the internal network is authenticated and encrypted, all other traffic passes through AutoSOCKS unchanged. For instance, browsing the Internet from the mobile user workstation occurs as if AutoSOCKS was not even running in the background. Large sites with many mobile users will want to setup an internal file server and perform a network installation for use by all of the mobile users to install and configure AutoSOCKS easily. For more information, consult the "Network Installation."

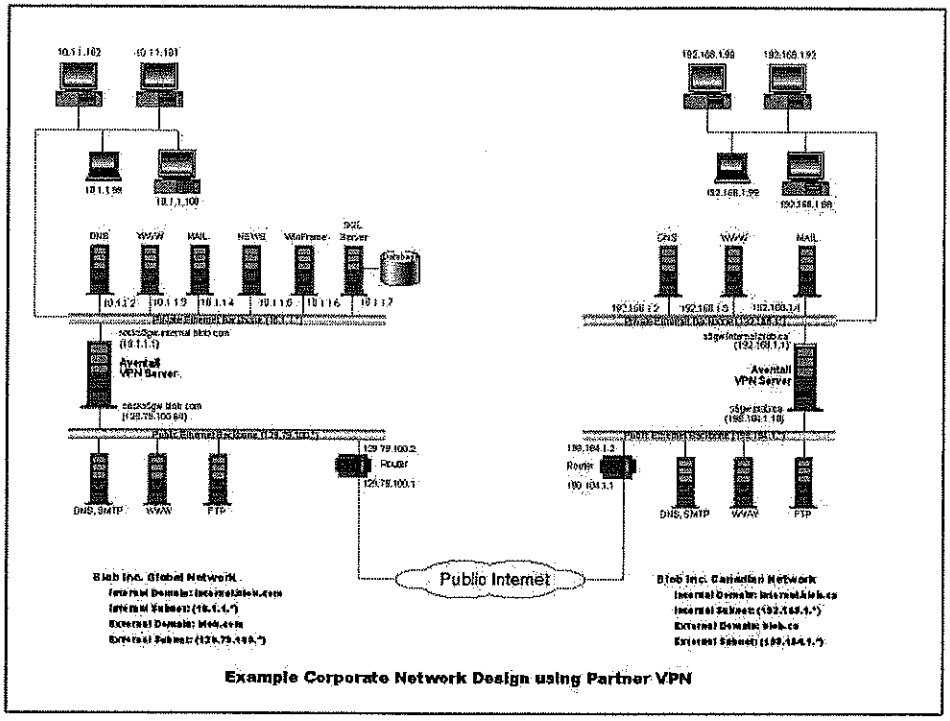


Figure 4. AutoSOCKS in a Partner VPN Environment

AutoSOCKS *Utilities Reference Guide*

Section II, the AutoSOCKS *Utilities Reference Guide*, covers the utilities available from the AutoSOCKS system menu. This section explains:

- Using commands in the System menu including Close, Hide Icon, Help, About, Credentials, Configuration File, Config Tool
- Using the Logging Tool to track AutoSOCKS activity and S5 Ping to check network connectivity

System Menu Commands

Even though AutoSOCKS requires little to no interaction with the end user, there are functions available by way of the AutoSOCKS System menu. To display the System menu, right-click the minimized AutoSOCKS icon (Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.1) or click the AutoSOCKS icon in the Taskbar tray (Windows 95 and Windows NT 4.0).

AutoSOCKS System Menu Commands

Menu Command	Function
Close	Closes AutoSOCKS.
Hide Icon	Hides the AutoSOCKS icon from view.
Help	Accesses online Help.
About	Displays Aventail AutoSOCKS About box.
Credentials	Displays authentication credentials.
Configuration File	Selects a new configuration file.
Config Tool	Runs the Config Tool.
Logging Tool	Runs the Logging Tool.
S5 Ping	Runs the ping and traceroute utilities.

Each of the commands are discussed in the paragraphs below.

Note: The Config Tool, Logging Tool, and S5 Ping commands are optional components and will only appear when they have been installed by the

network administrator. They are discussed in the sections "Logging Tool" and "S5 Ping" below.

Close

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

Hide Icon

This command hides the AutoSOCKS icon from view. AutoSOCKS will be running the background; however, the icon won't be visible in the system tray (Windows 95, Windows NT 4.0) or minimized on the desktop (for Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51).

Help

This command accesses AutoSOCKS online Help menu.

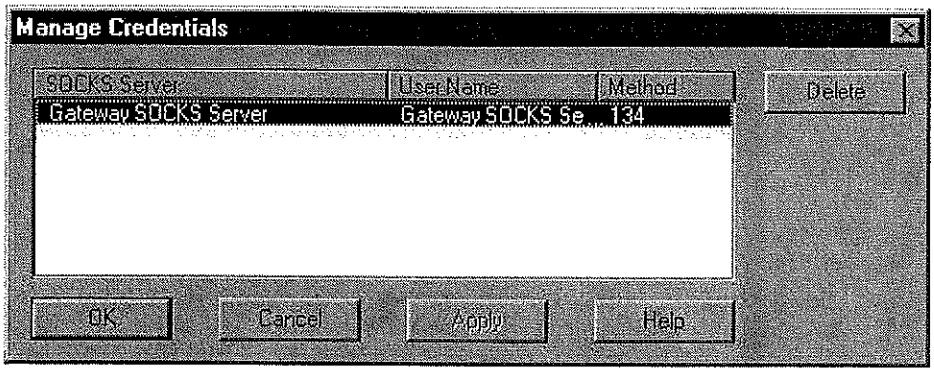
About

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

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 a SOCKS server requiring user authentication. (AutoSOCKS prompts you with an authentication dialog box.) As long as your credentials are in memory, you can establish connections to associated SOCKS servers without needing to re-enter the authentication information.

Currently, there is no way to edit credential data fields; you can only delete the entire credential entry or clear the password portion of it. In either case, AutoSOCKS will prompt you to enter updated authentication information when you re-establish a connection to the associated SOCKS server.



Field	Definition
SOCKS Server	SOCKS server name
User Name	User name for the SOCKS server
Method	Numeric identifier of authentication method (2=username/password, 3=CHAP, 134=SSL)

To delete a credential entry

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

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

  This deletes the credential information.

To exit the Manage Credentials dialog box

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

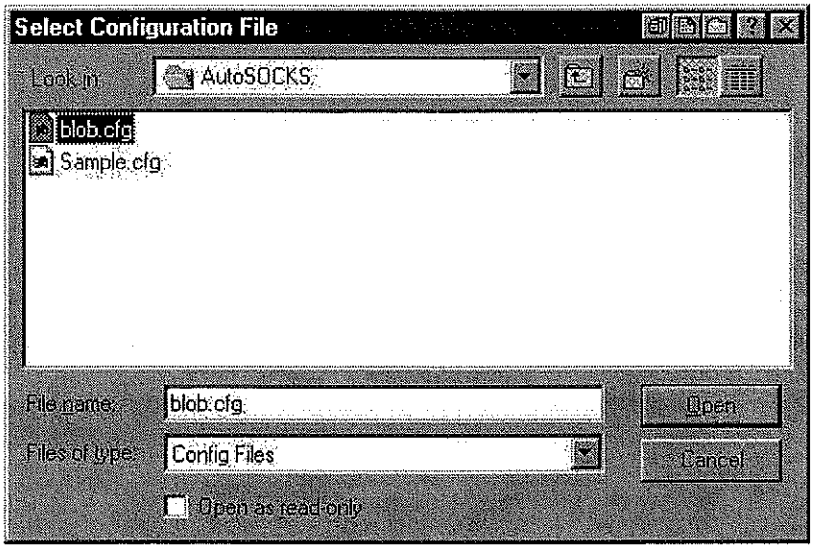
  -OR-

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

  Note: The **Apply** button makes changes permanent but keeps the dialog box open so you can keep working.

Configuration File

This command lets you load a different configuration file from the Select Configuration dialog box. AutoSOCKS defaults to AUTOSOCKS.CFG.



For more information about the configuration file, refer to "Creating Configuration Files."

To load a configuration file

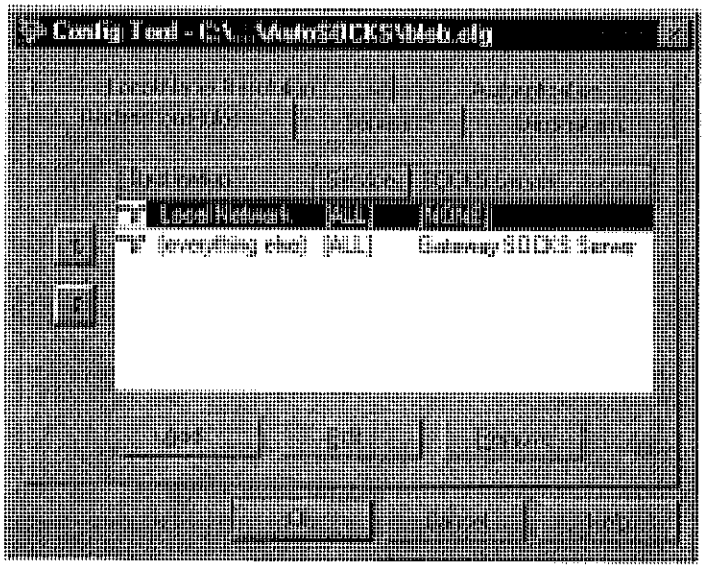
Check with the network administrator before making any changes to the configuration.

- Select the configuration file you wish to load and click the **Open** button.

  The new configuration file is transparently loaded into AutoSOCKS. AutoSOCKS must be restarted for the new configuration parameters to take effect.

Config Tool

The AutoSOCKS Config Tool creates configuration files used to determine how network requests should be routed and which authentication protocols should be enable. (This option may not be available to all users.)



Configuration files should be set up by a network administrator. They are usually created during AutoSOCKS installation but they can also be added, removed, or modified at any time. If necessary, several configuration files can be created 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. The Config Tool dialog box is discussed in detail under "Creating Configuration Files."

Logging Tool

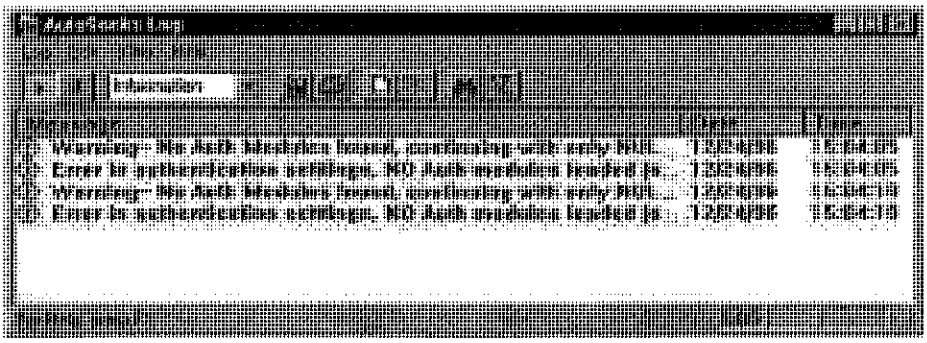
The Logging Tool is a diagnostic utility used to trace AutoSOCKS activity. (This option may not be available to all users.) When running a trace, the Logging Tool displays errors, warnings, and information messages as AutoSOCKS generates them. If desired, the message list can be saved to a log file for later study. Log files can be used to troubleshoot technical problems. They are also useful when running AutoSOCKS for the first time to ensure that network traffic is being routed appropriately.

To trace AutoSOCKS activity

1. Windows 95 or Windows NT 4.0: From the Programs command in the Start menu, point to Aventail AutoSOCKS and click Logging Tool.

   -OR-

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



2. In the Log menu, select **Level** and then click one of the three levels of information you wish to trace.

   -OR-

   Select one of the three levels from the list on the toolbar.

Choose	To Log
Errors	Errors only
Warnings	Errors and warnings only
Information	Errors, warnings, and information

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

   -OR-

   Click the **Trace On** button on the toolbar.

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

5. When you're ready to stop the Trace function, click **Trace** in the Log menu

   -OR-

   Click the **Trace Off** button on the toolbar.

   The Trace function is stopped. 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 as the trace is executed, or save the contents of the log window at any time. If you save as the trace is being executed, AutoSOCKS will append messages to the log file until you stop the log function. Data in the log window will not be retained unless it is saved.

There is no way to open a log file from within the log window. You must open a log file using a text editor such as Notepad.

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

  -OR-

  Click the **File Logging** button on the toolbar. Enter the filename in the Select Log File dialog box.

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

To filter messages in the log window

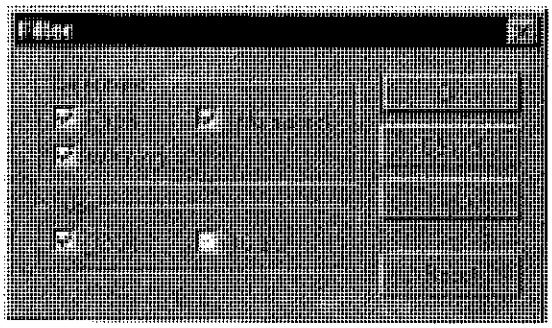
The contents of a log window can be filtered by selecting the types of messages you wish to view. Selecting a specific type of message can make it easier to scan the information onscreen. If the data has been saved to a log file, a view filter will not affect the file contents; it merely adjusts the screen display of those contents.

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

   -OR-

   Click the **Filter** button on the toolbar.

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



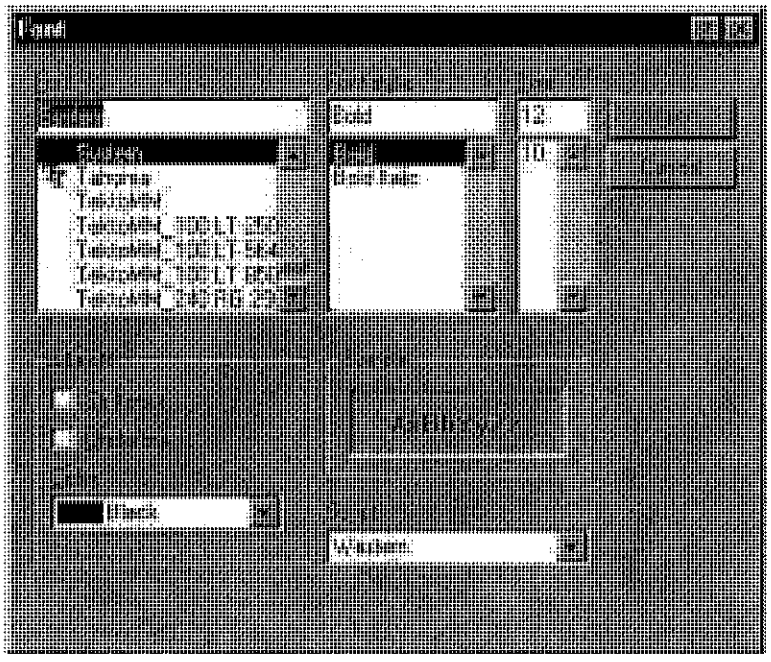
Field	Definition	
Categories	Select any of the three filters to display errors, warnings, and/or information in the log window.	
Type*	32-bit:	Show messages from 32-bit applications.
	16-bit:	Show messages from 16-bit applications.
	*These options are disabled if you're running 16-bit Windows.	

2. Under Categories, select one or more the three filter check boxes. The Log window will adjust the display based on your selection(s).
3. Under 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:

- In the View menu, click **Font**. Enter your font preferences into the standard Windows Font dialog box.



- To display and hide the toolbar and status bar, click **Toolbar** and/or **Status Bar** in the View menu.

To copy the log window

The log window contents can be copied to the Windows Clipboard.

- To copy all of the window contents to the Windows Clipboard, click **Select All** in the View menu. Then click **Copy** in 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 click **Copy** in the Edit menu or click the **Copy** button on the toolbar.

To print the log window

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

- To print the log window contents, click **Print** in the log menu.

  -OR-

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

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

To find a specific message

The Find function 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.

- In the Edit menu, select **Find.**

  -OR-

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

  Then enter your search parameters into the Find dialog box.

To clear the log window

Log window contents should be cleared when you're ready to execute a new trace, and you no longer need to see the old data.

- In the Edit menu, select **Clear All.**

  -OR-

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

To close the log window

When you're ready to close the Log window, make sure you've saved the contents of the trace for later reference if necessary. All settings are saved when you exit.

- In the File menu, select **Exit.**

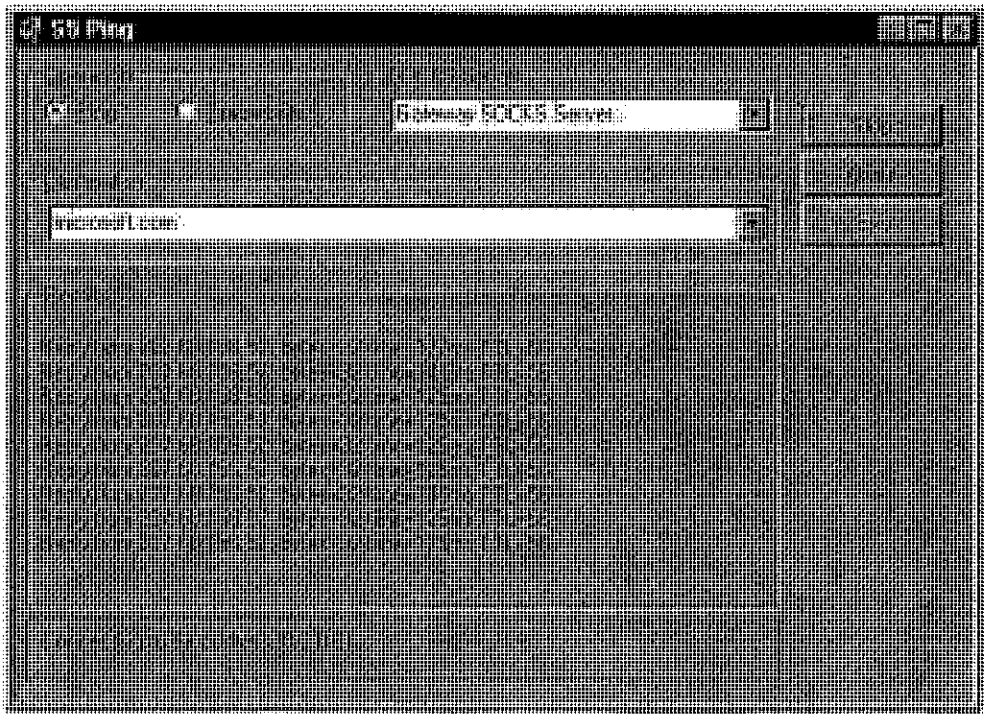
S5 Ping

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

- 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 ronters 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, ICMP is not supported. Because ping and traceroute are based on ICMP, there's no way to directly proxy a ping or traceroute request. To circumvent this problem, AutoSOCKS provides a utility called S5 Ping.

S5 Ping will ping (or traceroute to) a host outside of a SOCKS server by having the client reqnest the SOCKS v5 server to ping the host in question. When a response from the host is returned, the SOCKS server relays the data back to the client and displays it in the S5 Ping window.



Field	Definition
Operation	Select the program you wish to run.
SOCKS Server	The SOCKS server which will execute the operation. If AutoSOCKS is already configured, this list will be preloaded with SOCKS servers from the configuration file.
Destination	The SOCKS server you wish to ping (or traceroute). If AutoSOCKS is already configured, this list will be preloaded with single host destinations defined in the configuration file. (See "Configuring AutoSOCKS.")
Results	The results of the operation once the connection succeeds. The format of the results will vary based upon the SOCKS server platform.

S5 Ping can be used whether or not AutoSOCKS is running. However, if the server that you're connecting through requires authentication, AutoSOCKS must be loaded. The availability of S5 Ping is determined by the network administrator when AutoSOCKS is first installed. In some cases, the S5 Ping command won't appear on the AutoSOCKS System menu or in the program group.

To run ping or traceroute using S5 Ping:

1. Launch S5 Ping.
2. Select the network operation to use (ping or traceroute).
3. Choose which SOCKS server will carry out the ping or traceroute operation.
4. Select the host to ping or traceroute.
5. Click the **Start** button to start the operation.

These procedures are described in the text below.

To launch S5 Ping

S5 Ping can be used whether or not AutoSOCKS is running.

1. Windows 95 or Windows NT 4.0: From the Programs command in the Start menu, point to Aventail AutoSOCKS and click **S5 Ping**.

   -OR-

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

   -OR-

   If AutoSOCKS is already running, choose the S5 Ping menu item from the AutoSOCKS tray icon menu (Windows 95, Windows NT 4.0) or from the minimized AutoSOCKS

icon System menu (Wiudows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51).

The S5 Ping window appears.

Note: S5 Piug will function without a properly configured AutoSOCKS; however, the user will be required to type the information about the target SOCKS server and target host into the SOCKS Server and Destinatiou text boxes.

Once the S5 Ping window 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 a SOCKS server to carry out the operation. If no servers are listed (because S5 Piug did not locate an AutoSOCKS configuration file), type the SOCKS server's hostname or IP address.
3. Under Destination, select a siugle host destination to ping or traceroute. If no hosts are listed (because S5 Ping did not locate an AutoSOCKS configuration file), type the hostname or IP address of the host you wish to ping or traceroute.
4. Click the **Start** button to execute the operation. The **Start** button then changes to **Stop**. Results from any previous operation are cleared from the window.
5. If the SOCKS 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 "Managing Authentication Modules" in the AutoSOCKS v2.1 *Administration and User'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 the **Stop** button.

  This stops the operation and changes the **Stop** button back to **Start**. The results of the operation remain displayed in the S5 Ping window.

To exit S5 Ping

- Click the **Exit** button.

  This clears the results and closes the S5 Ping window.

AutoSOCKS *User Supplement*

AutoSOCKS automatically routes appropriate network traffic from a WinSock-compatible TCP/IP application such as an e-mail program or a web browser to a SOCKS-based server. (WinSock is a Windows TCP/IP interface that connects a Windows PC to the Internet.) The SOCKS server then sends the traffic to the Internet or the network. Your network administrator defines sets of rules by which this message traffic is to be routed.

This AutoSOCKS *User Supplement* is designed to familiarize you with aspects of the AutoSOCKS interface. Because AutoSOCKS is designed to run transparently, in most cases you'll interact with AutoSOCKS only when it prompts you to enter authentication information for a connection to a secure SOCKS server on the Internet or corporate intranet. You may also occasionally need to start and exit AutoSOCKS although network administrators often configure it to run automatically at startup.

If you have questions about how AutoSOCKS is running on your system, contact your network administrator. Details about other AutoSOCKS commands and utilities are described in the AutoSOCKS v2.1 *Administration and User's Guide*. You might find the section, "Getting Started" to be helpful.

How to Start and Close AutoSOCKS

Because network administrators often set up AutoSOCKS to run minimized at startup, you may never need to actually launch the AutoSOCKS application. When AutoSOCKS is started, it loads a default configuration file, AUTOSOCKS.CFG. This file contains the rules AutoSOCKS uses to properly route network traffic to and from your individual workstation. Your network administrator will inform you if the configuration file name should be different.

Closing AutoSOCKS may limit access to certain remote hosts or prevent you from using certain WinSock applications. Before closing AutoSOCKS it's a good idea to check with your network administrator.

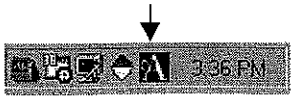
To start AutoSOCKS

- Windows 95 and Windows NT 4.0: From the Programs command in the Start menu, point to Aventail AutoSOCKS and click AutoSOCKS v2.1.

  -OR-

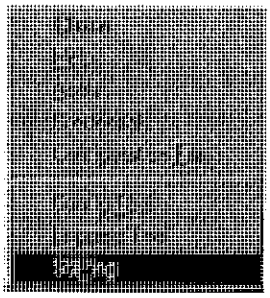
  Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51: In the Aventail AutoSOCKS program group, double-click the AutoSOCKS v2.1 program icon.

  You'll see a minimized AutoSOCKS icon indicating that AutoSOCKS is running in the background. In Windows 95 and Windows NT 4.0, this icon is located in the system tray on the Task bar.



To close AutoSOCKS

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



-OR-

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

Note: The Config Tool, Logging Tool, and S5Ping may not appear on the Aventail System menu in the program group. This is a configuration option determined when AutoSOCKS is first installed.

How to Enter Authentication Credentials

Some SOCKS servers ask you to authenticate yourself before you are allowed to access them. If you try to connect to a secure SOCKS server, AutoSOCKS may display a dialog box asking you to enter authentication credentials. (For some types of authentication methods, your input isn't required.) Credentials can be as simple as your username or password, or they can be more complicated information. Credentials are assigned to you by your network administrator.

Note: Never talk about credentials over cellular or cordless phones. These lines are not secure and you could be compromising system integrity. If you've mistakeuly done so, be sure to let your network administrator know so that you can be assigned a new password.

Currently, AutoSOCKS supports four kinds of user authentication protocols: Username/Password, Challenge Handshake Authentication Protocol (CHAP), Secure Socket Layer (SSL), and SOCKS v4 Identification. To read more about these protocols, see "Managing Authentication Modules" in the AutoSOCKS v2.1 *Administration and User's Guide*.

Once you enter your credentials, AutoSOCKS will save them in memory. This is known as memory caching. Memory caching stores the credentials for the current session only. When

you restart AutoSOCKS or Windows, the memory cache is flushed. If you reconnect to the secure SOCKS server, you must again enter your credentials as prompted.

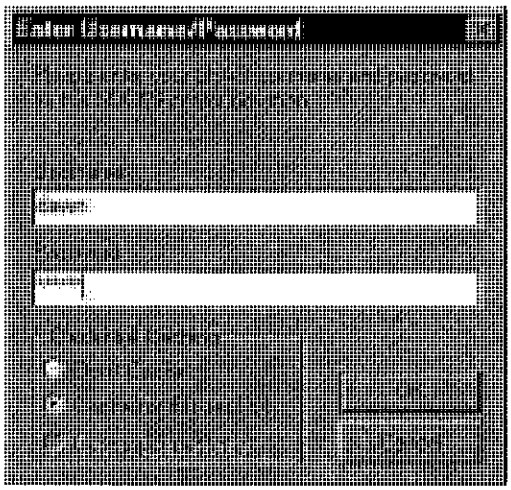
The following discussion includes Username/Password, CHAP, and SSL authentication. SOCKS v4 authentication does not require user interaction and therefore is not covered in this supplement.

Username/Password and CHAP Authentication

Username/Password and CHAP authentication use basically the same dialog boxes.

To enter authentication credentials

If the secure SOCKS server to which you're connecting uses Username/Password or CHAP authentication, you'll see a dialog box similar to the following:



Note: If you don't know what to enter into the dialog box fields, check with your network administrator.

1. In the Username text box, type your user name.

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

2. In the Password text box, type your password.

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

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

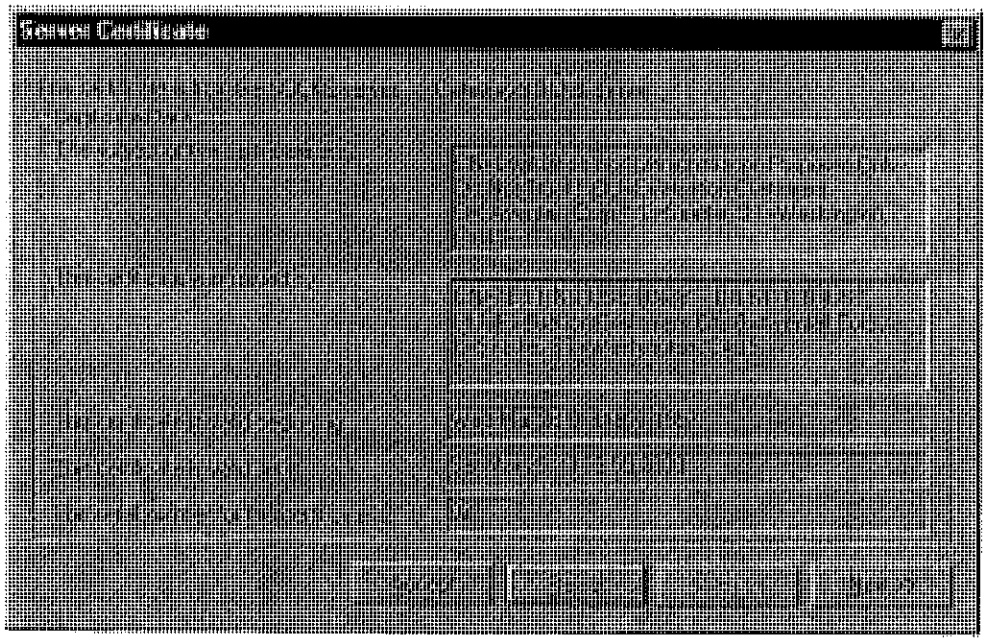
   When you click OK, your credentials are sent to the secure SOCKS server and if they are accepted, you'll continue your processing without hindrance.

If your credentials are refused by the server, the application will display an alert stating that the message traffic didn't go through. Try the transaction again, reentering your username/password. If problems persist, contact your network administrator.

SSL Authentication

SSL authentication, originally developed by Netscape for secure Web communications, uses *authentication certificates* to identify authorized users. A certificate is essentially an electronic "statement" which verifies the integrity of a connection. When you attempt to connect to an SSL server, AutoSOCKS may display the SSL certificate sent by the server. This may not always be the case, depending on how your network administrator has configured the system.

Note: It isn't the mission of this supplement to explain the intricacies of authentication or the components of SSL certificates. If you're interested in learning more about them, talk to your system administrator or read about them in the AutoSOCKS v2.1 *Administration and User's Guide* under "Managing Authentication Modules."



To accept an SSL certificate

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

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

   If you click **Reject**, your connection won't be established. If you click **Next**, you see a second "page" of the certificate data with the same Accept and Reject buttons.

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

2. In the **Username** text box, type your user name.

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

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

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

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

   When you click OK, your credentials are sent to the secure SOCKS server and if they are accepted, you'll continue your processing without hindrance.

Appendix I:
Troubleshooting

AutoSOCKS-related problems tend to fall into four categories: Installation, Network Connectivity, Coufiguration, and Application and TCP/IP Stack Iuteroperability.

AutoSOCKS Installation Problems

When the instructious in Installiug AutoSOCKS in the AutoSOCKS v2.1 *Administration and User's Guide* are followed, problems installing AutoSOCKS are rare. When they occur, they are often the result of:

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

If any of these are found to have been running during a failed installation, close them, uninstall AutoSOCKS, reboot, and then re-install AutoSOCKS, taking care to ensure that the toolbars, virus-checking utilities, or applications were not automatically restarted when the system was rebooted.

Insufficient RAM or free space on the volume to which AutoSOCKS is being installed

If either of these is suspected as the cause of a failed installation, increase the available resources according to the System Requirements of the AutoSOCKS v2.1 *Administration and User's Guide* and retry the installatiou.

Corrnpted AutoSOCKS installation media or corrupted or incomplete FTP of AutoSOCKS self-extracting, executable installation file

If corrupted AutoSOCKS installation diskettes are suspected causes of a failed installation, contact Aventail Technical Support for assistance in determiuing whether the files on the diskettes may have been corrupted and whether replacement diskettes must be obtained from Aventail or your vendor.

If corrupted or incomplete FTP transfer of AutoSOCKS installation files obtained over the Internet is suspected, 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 AutoSOCKS was running or from which a previous version of AutoSOCKS was not completely uninstalled

If either of these circumstances is suspected causes of a failed installation, contact Aventail Technical Support.

Installation script errors

AutoSOCKS 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 AutoSOCKS can be used to successfully redirect WinSock application connections:

1. The workstation on which AutoSOCKS 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 AutoSOCKS 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 AutoSOCKS is installed and the SOCKS server(s) to which it is configured to redirect connections.

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

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

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

AutoSOCKS Configuration Problems

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

It is easiest to troubleshoot AutoSOCKS configuration problems by creating and testing simple AutoSOCKS configuration files, such as those that may be created with the AutoSOCKS Configuration Wizard. However, all references to host and domain names should 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 SOCKS server(s) to which AutoSOCKS must connect must be known, before troubleshooting AutoSOCKS configuration problems. Neither AutoSOCKS, nor Aventail

Technical Support, can discover the IP address or port number of the SOCKS server(s).

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

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

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

Click on the Servers tab, click on the server alias, and then click on the **Edit** button. Compare the IP address in the Hostname or IP: field with that of the SOCKS server.

If the SOCKS server is a SOCKS v5 server, click on the SOCKS v4 radio button in the SOCKS Version section of the Servers tab. Then click on the **Detect Version** button. The selection should revert to the SOCKS v5 radio button, indicating that AutoSOCKS detected a SOCKS v5 server running at the IP address specified in the Hostname or IP: field.

If, on the other hand, the SOCKS server is a SOCKS v4 server, click on the SOCKS v5 radio button in the SOCKS Version panel. Then click on the **Detect Version** bntton. The selection should revert to the SOCKS v4 radio button, indicating that AutoSOCKS detected a SOCKS v4 server running at the IP address specified in the Hostname or IP: field.

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

2. Confirm that all AutoSOCKS Authentication Modules are enabled.

Click on 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 AutoSOCKS to attempt any form of authentication demanded by the SOCKS server or null (no) authentication. Note the form of authentication demanded by the SOCKS server and, if necessary, obtain the proper authentication credentials, such as a SOCKS server username and password, from the SOCKS server administrator.

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

Click on the Destinations tab, click on the Destination which includes the network host to which the SOCKS server is expected to proxy connections, and then click on the Edit button. Confirm that the definition of the Destination includes the network host.

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

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

Application and TCP/IP Stack Interoperability Problems

AutoSOCKS is intended to "automatically socksify" all "well-behaved" Winsock applications. Occasionally, Winsock applications are found which AutoSOCKS does not socksify, due to interoperability problems with the application.

AutoSOCKS is also intended to run on all WinSock-compliant Microsoft Windows TCP/IP stacks. Occasionally, WinSock stacks are found on which AutoSOCKS does not run as expected, due to interoperability problems with the stack.

If an application or stack inter-operability problem is suspected, report it to Aventail Technical Support. Aventail will make every effort to resolve interoperability problems.

AutoSOCKS Trace Logging

AutoSOCKS includes a Logging Tool for doing traces of AutoSOCKS and Winsock activity. AutoSOCKS traces are ofteu useful in troubleshooting AutoSOCKS network, SOCKS server, and Winsock application interoperability problems. Aventail Technical Support engineers may request that you perform a debug-level trace, log it to file, and e-mail it to them.

Before Starting an AutoSOCKS Trace:

1. Close any WinSock applications that are running on the workstation.

2. Close AutoSOCKS, if it is running.

3. Start an AutoSOCKS Trace.

4. Click on the Windows Start | Programs | Aventail AutoSOCKS | Logging Tool menu bar item. The AutoSOCKS Logging Tool window should open, as illustrated in Figure 1, below.

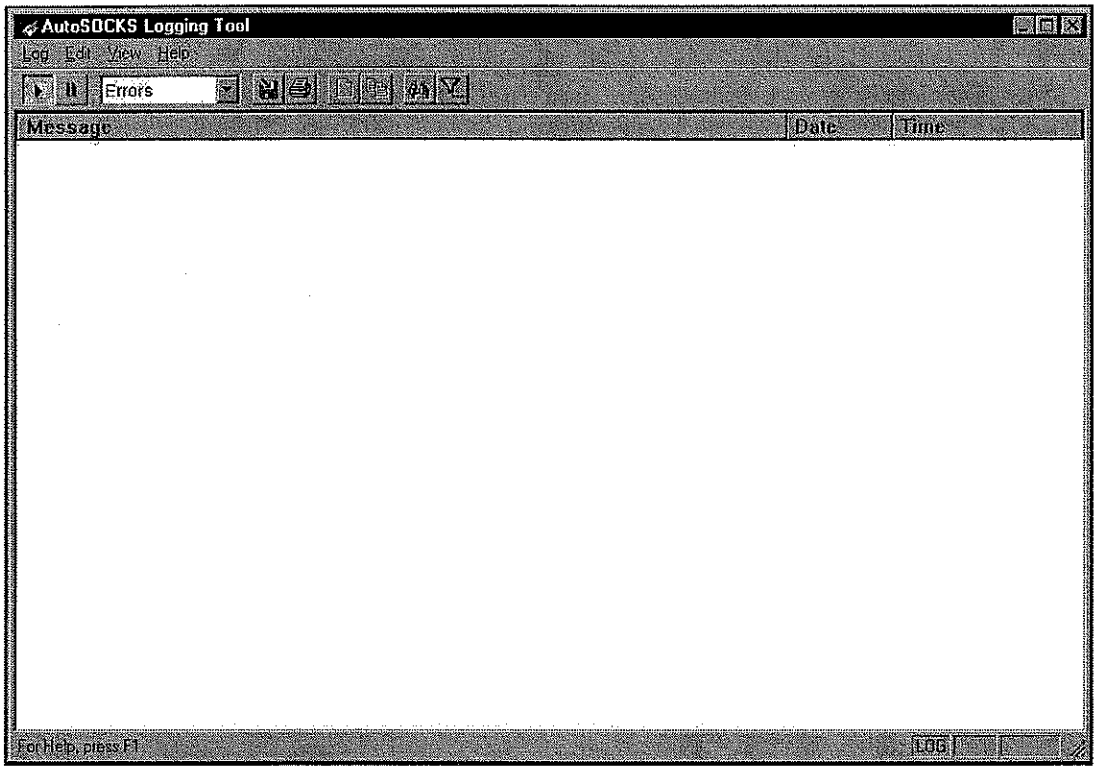


Figure 1

5. In the Logging Tool window Log menu, confirm that the Trace option is checked. If it is not, click on the Trace option, to check it.

Saving an AutoSOCKS Trace to a File:

1. In the AutoSOCKS Logging Tool window Log menu, confirm that the Log To File... option is checked. If it is not, click on the Log To File... option, to check it. The AutoSOCKS Logging Tool window Log menu should appear as illustrated in Figure 2, below.

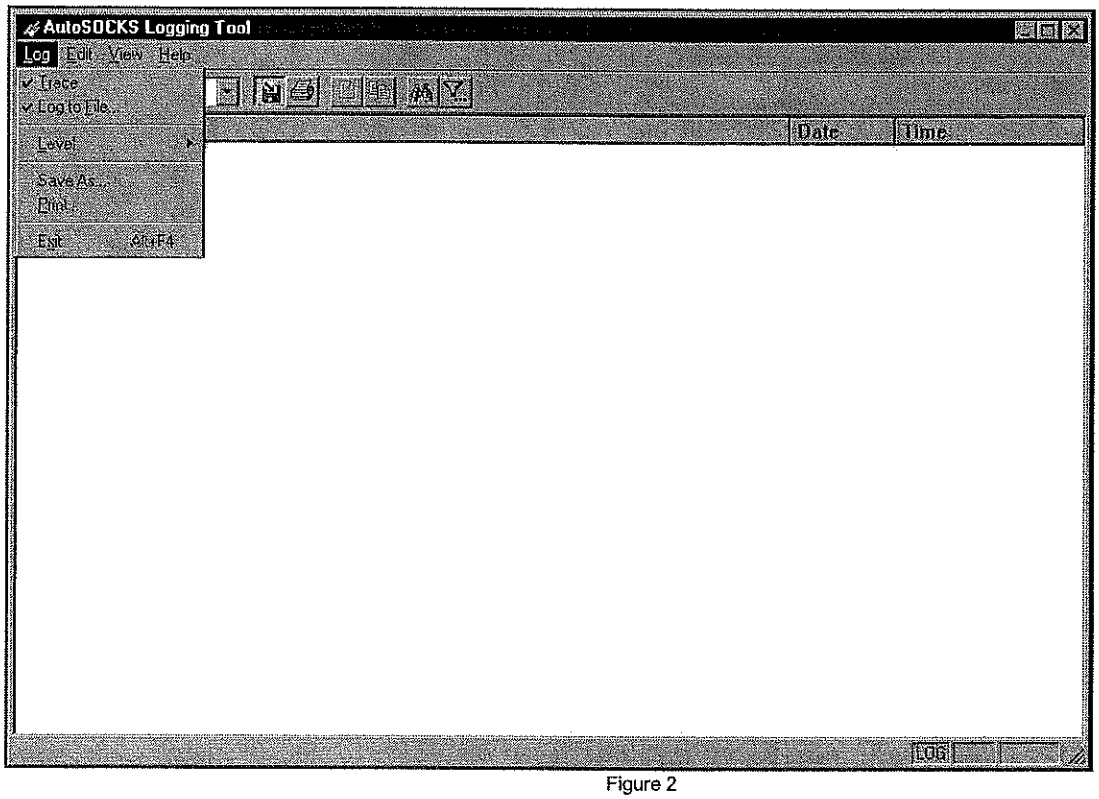


Figure 2

2. A Select Log File dialog box should appear, as illustrated in Figure 3, below. Enter a file name appropriate to later identify the file and click Save.

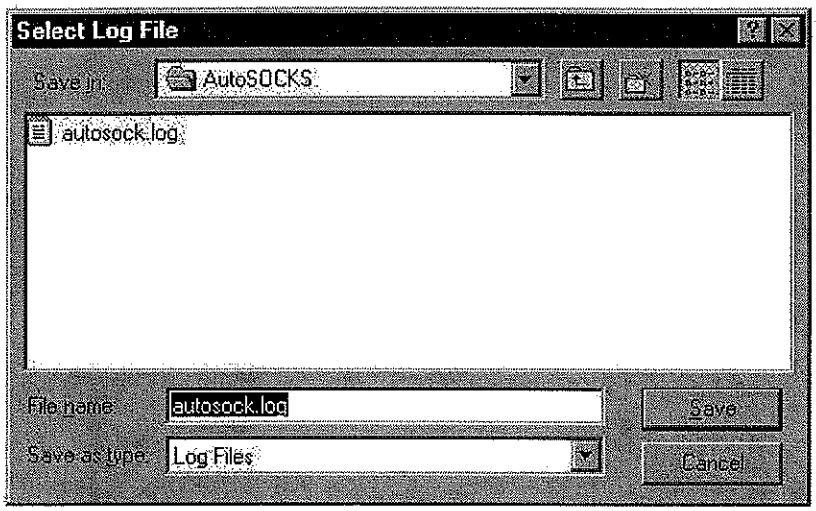


Figure 3

Setting the AutoSOCKS Trace Level to Debug:

1. Click on the AutoSOCKS Logging Tool window and then press <Ctrl><4>."Debug" should appear in the drop-down text box in the AutoSOCKS Logging Tool toolbar, as illustrated in Figure 4, below.

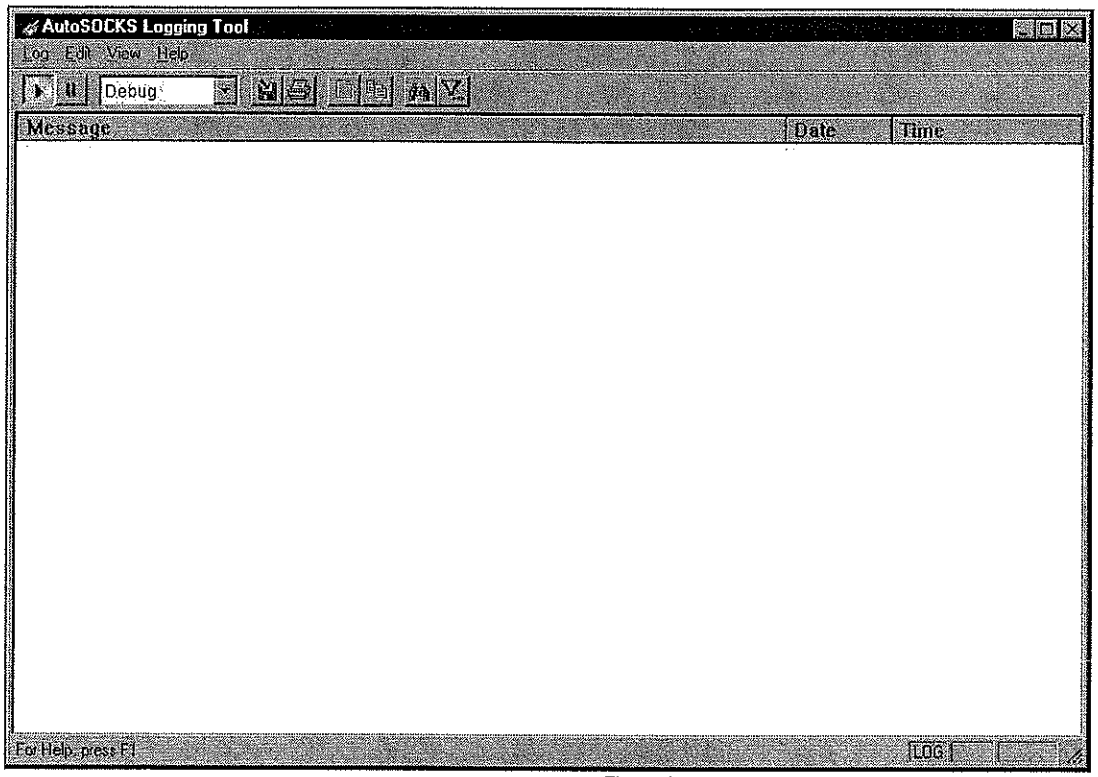


Figure 4

Note that, when tracing in Debug mode, not all messages that are displayed are indicative of error.

Logging Trace Data:

1. Start AutoSOCKS.
2. Start the Winsock application.
3. Reproduce the problem and only the problem.
4. Close the trace log file and confirm that it was saved.

Reporting AutoSOCKS Problems

Report AutoSOCKS problems to Aventail Technical Support, ideally by completing and submitting an AutoSOCKS Problem Report on the Support page of the Aventail website.

Glossary

alias
User-friendly name for destination uetwork 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.

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

host
A server connected to the 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.

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

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

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

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 protocol.

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.

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.

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.)

WinSock
(Windows Socket) A Windows component that connects a Windows PC to the Internet using TCP/IP.

workstation
Any computer connected to a network.

Index

Exhibit D

October 12, 1998 Aventail Press Release

"Aventail Introduces The First Extranet-Ready Platform; Aventail Previews its Latest Solution, Aventail ExtraNet Center, at Networld+Interop in Atlanta." PR Newswire. PR Newswire Association LLC (October 12, 1998).

HighBeam™ RESEARCH

PR Newswire

Aventail Introduces The First Extranet-Ready Platform; Aventail Previews its Latest Solution, Aventail ExtraNet Center, at Networld+Interop in Atlanta.

Publication: **PR Newswire** Publish date: **October 12, 1998**

SEATTLE, Oct. 12 /PRNewswire/ -- With a strong reputation for providing easy-to-manage security software solutions, Aventail Corporation today announced the introduction of Aventail ExtraNet Center(TM).

Aventail ExtraNet Center enables corporations to securely extend their enterprise applications to business partners, suppliers, and customers over the Internet and other public networks. It is the only extranet-ready platform that delivers the necessary security, centralized management, and application and network integration for building an extranet, eliminating the barriers that have previously deterred the widespread deployment of extranets.

"Businesses are realizing that in order to stay competitive in this global market, they must constantly evaluate and improve their business processes. It is imperative that they think of innovative ways to improve the delivery of information to key individuals," said Evan Kaplan, president & CEO of Aventail Corporation. "Aventail ExtraNet Center enables corporations to improve customer relations, facilitate collaborative projects with partners, and increase employee productivity."

Today's Extranet Challenges Addressed

Aventail Extranet Center is a client/server software solution that addresses the specific security, management, and deployment issues that many corporations face when designing a system to share information with extranet users.

Tha complete solution provides the following:

* Sophisticated Security and Access Controls Aventail ExtraNet Center not only provides strong encryption and authentication, but also granular access controls that enable administrators to define user privileges based on a broad range of parameters, including authentication/encryption method, user ID, information resource, group affiliation, and day and time. This provides corporations with the flexibility to build custom access profiles to reflect the unique business relationship of each partner.

* Application Independent

Currently, many corporations are deploying extranets with products that only support Web-based applications, greatly limiting the functionality of the extranet. Aventail ExtraNet Center supports all IP-based applications including legacy host, Web, JAVA, ActiveX, CORBA, DCOM+, custom corporate, and client/server applications from corporations such as SAP, BAAN and PeopleSoft.

* Simple User Management

Aventail ExtraNet Center makes deployment easy for the administrator, even if there are thousands or millions of users. Through the Aventail Policy Console, a single intuitive interface, administrators can easily create, delete, or modify extranet users' profiles. Using the Aventail Management Console, these functionalities can also be securely administered from any remote or desktop workstation.

* Infrastructure Independent

Aventail ExtraNet Center runs on most operating systems and works with any firewall, encryption and authentication method, and proxy server. The ability to seamlessly integrate into any existing infrastructure allows corporations to leverage their existing and future network and security infrastructure investments. In addition, it makes it easy for corporations and their business partners to select "best-of-breed" technologies that address their specific business requirements.

* Transparent Client

Designed for non-technical users, Aventail Extranet Client is a highly functional piece of software that is completely transparent to the end user. It can be installed in minutes, makes no technical modifications to the desktop, and can securely traverse any firewall without administrator intervention. Aventail Extranet Client includes Extranet Neighborhood, a revolutionary application that enables users to browse selected 32-bit

Windows-based file systems. Using the popular and well-known Microsoft Windows Explorer user interface, Extranet Neighborhood does not require any end-user training.

* Automated Client Configuration and Distribution

Network administrators can create up to tens of thousands of custom Aventail Extranet Clients in one easy step with the Aventail Customizer. With this tool, network administrators can easily distribute clients and make them available in a central, networked directory for easy access, download, and installation.

"Information Systems (IS) decision makers charged with protecting core business information and the brand-equity of the enterprise will want to look at Aventail ExtraNet Center," said Jim Hurley, managing director of the information security practice with Aberdeen Group. "Our clients are wrestling with how to safely deploy and maintain enterprise commerce activities with key customers, partners and suppliers. Aventail ExtraNet Center is positioned to meet this need."

Real-Life Extranet Deployments

To date, many organizations in the healthcare, financial services, consulting, manufacturing, insurance, and high technology industries have benefited greatly from successful extranet deployments using Aventail solutions.

For example, Ari Friedman, a network engineer at University Health Systems, uses Aventail to provide doctors, medical students, and staff members at The University of Texas Health Science Center in San Antonio with secure access to patient billing, scheduling, and lab results. By deploying Aventail's extranet solution, the users at the Health Science Center can be more productive and spend more time with their patients, giving them better care.

"I evaluated several VPN hardware products and firewall solutions. The hardware products were unacceptable because the client would have been a nightmare to deploy, and it meant managing and purchasing another device. Firewalls were out of the question because they provided terrible performance," said Friedman. "Aventail meets all of my requirements. Their solution is dependable, versatile, and something that scales well."

Pricing and Availability

Aventail ExtraNet Center will be available in November through Aventail's worldwide sales team and Aventail's Extranet Advantage VAR partners. Pricing details will be available at the time of product release.

About Aventail

Aventail is at the forefront of providing extranet security and management software solutions that allow organizations to securely extend their enterprise applications to strategic partners, suppliers, customers, consultants, and other key individuals. Aventail's extranet solutions enable organizations to increase their competitive advantage, raise profits, and leverage their investments in existing and future enterprise systems. With a strong reputation for providing highly secure and easy-to-manage software solutions, Aventail has received numerous industry awards from publications such as InfoWorld, Network Computing, LAN Times, BYTE Magazine, Software Digest, and Computer Reseller News.

Aventail Corporation is a privately held company headquartered in Seattle, Washington. For more information on the company and its products, please visit the company's Web site at www.aventail.com, or contact the company directly at 206-215-1111, 877-AVENTAIL, or info@aventail.com.

Aventail and Aventail ExtraNet Center are trademarks of Aventail Corporation. All other trademarks are the property of their respective owners.

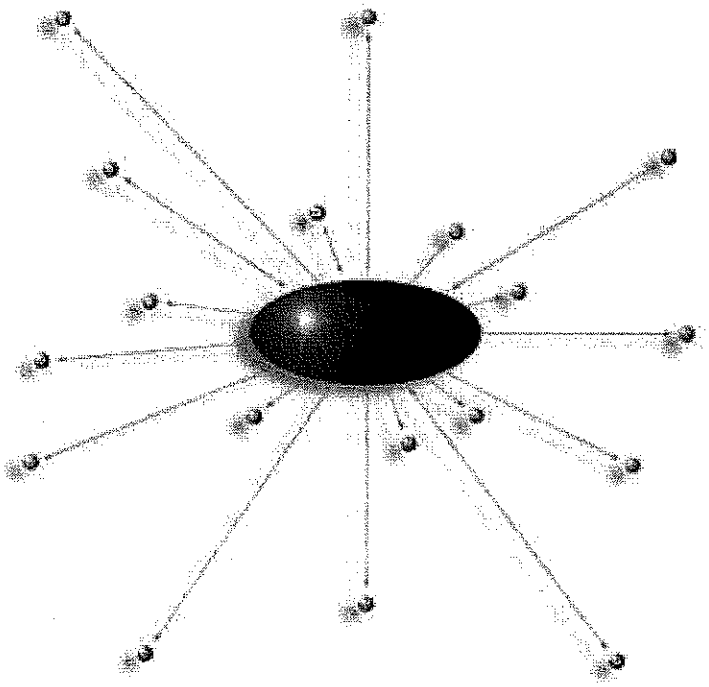
Exhibit E

Aventail Connect v3.01/2.51 Administrator's Guide

Aventail

CONNECT

v3.01/v2.51



Administrator's Guide

Windows

Aventail

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

Aventail Connect redirects WinSock calls and reroutes them based upon a set of routing directives (rules) assigned when Aventail Connect is configured. (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 2.0 (LSP) applications in Windows 98, and Windows NT 4.0, and WinSock 1.1 and WinSock 2.0 applications in Windows 95
- Supports WinSock 1.1 applications in Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51
- MultiProxy feature allows you to use a SOCKS server or an HTTP proxy to control outbound access
- Allows the use of port ranges for redirection rules
- Provides integration with SoftID™ and SecurID™ tokens
- Provides automated installation and uninstallation
- Credential cache timeout feature allows administrators to specify when credentials expire
- Provides optional password protection for configuration files
- Supports both SOCKS v4 and SOCKS v5 (RFC 1928 and RFC 1929) standards

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

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

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

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 2.0 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: Includes a Certificate wizard for generating and processing client certificate requests.
- 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 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 (Windows Sockets) 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.

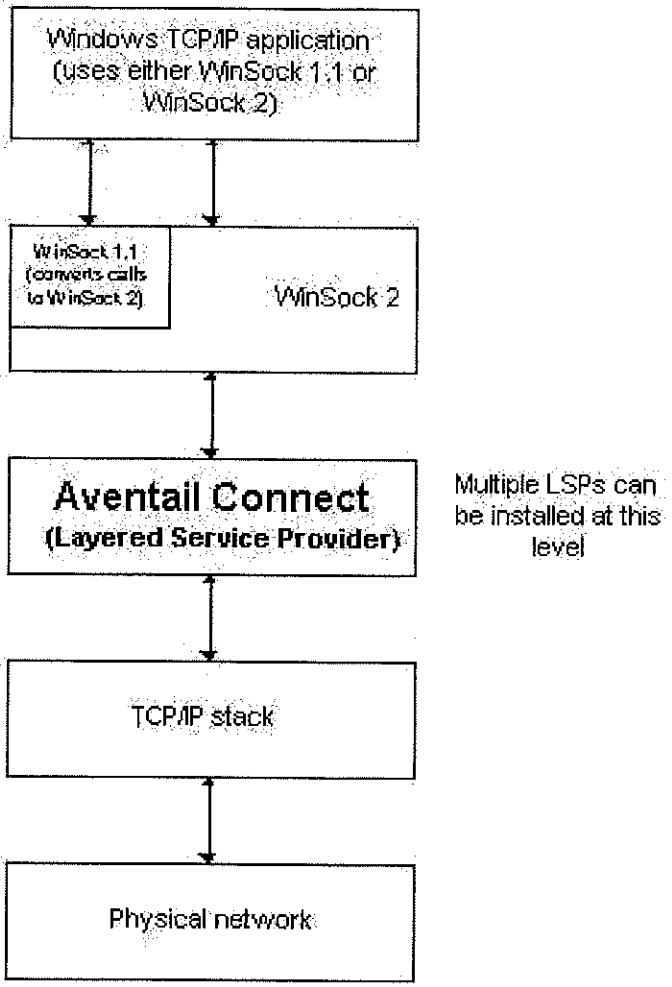
WinSock Connection to a Remote Host

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. 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 3.01 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 version 1.1 and version 2. Aventail Connect 3.01, like all LSPs, requires WinSock 2.0; WinSock 1.1 does not support LSPs. WinSock 2.0 includes backward-compatibility with all WinSock 1.1 applications. Not every platform supports WinSock 2.0 and its LSP structure.

- Windows 98 and Windows NT 4.0 support WinSock 2.0 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 2.0, but you must install a Microsoft patch to add support for WinSock 2.0.
- Windows 3.1, Windows for Workgroups 3.11, and Windows NT 3.51 do not support WinSock 2.0; they support only WinSock 1.1.

For those platforms that do not support WinSock 2.0 and LSP applications, Aventail includes Aventail Connect 2.51 on the Aventail Connect 3.01/2.51 CD. Aventail Connect 2.51 was designed for operating systems that support only WinSock 1.1. For Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51 operating systems, setup will install Aventail Connect 2.51. If you are working on a Windows 95 operating system, setup will detect whether you have installed the Microsoft Windows 95 WinSock 2.0 Update. If setup detects the Microsoft update, which upgrades Windows 95 to support WinSock 2.0, setup will install Aventail Connect 3.01. If setup does not detect the Microsoft update, it will install Aventail Connect 2.51.

The Aventail Connect 2.51 user interface is identical to that of Aventail Connect 3.01; however, Aventail Connect 3.01 includes MultiProxy (see "Multiple Firewall Traversal"). Aventail Connect 2.51 does not include MultiProxy.

In the future, more Windows applications may require WinSock 2.0.

During installation, setup determines which version of Aventail Connect to install. On WinSock 2.0 platforms, Aventail Connect 3.01 is installed. On WinSock 1.1 platforms, Aventail Connect 2.51 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 2.0	Aventail Connect 3.01
Windows 95	With Microsoft patch: WinSock 2.0	Aventail Connect 3.01
	Without Microsoft patch: WinSock 1.1	Aventail Connect 2.51
Windows 3.1, Windows for Workgroups 3.11, Windows NT 3.51	WinSock 1.1	Aventail Connect 2.51

You can create custom packages that include one or both versions of Aventail Connect (3.01 and 2.51) Setup will determine which version to install on each workstation. (For more information, see "Customizer.")

WINDOWS 95 AND WINSOCK

The Microsoft Windows 95 WinSock 2.0 Update upgrades WinSock 1.1 to WinSock 2.0 in Windows 95. This patch (filename `w95ws2setup.exe`) is available from the Microsoft Web site, at **http://www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp**. Unless you need specific Aventail Connect 3.01 features, Aventail recommends that you do not upgrade from WinSock 1.1 to WinSock 2.0. If you do not upgrade to WinSock 2.0, Aventail Connect 2.51 will be installed.

If you do need to install the Microsoft Windows 95 WinSock 2.0 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. 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 fake 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.

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	Extranet (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 3.01 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 2.0 update (To install Aventail Connect 3.01, you must upgrade Windows 95 with the Microsoft WinSock 2.0 update prior to Aventail Connect installation and setup. If you do not install the Microsoft patch, Aventail Connect 2.51 will be installed. For more information, see "What Does Aventail Connect Do?".)

Aventail Connect 2.51 runs on the following operating systems:

- Windows 3.1
- Windows for Workgroups 3.11
- Windows NT 3.51
- Windows 95, without the Microsoft WinSock 2.0 update (If you do not upgrade Windows 95 with the Microsoft WinSock 2.0 update, Aventail Connect 2.51 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.

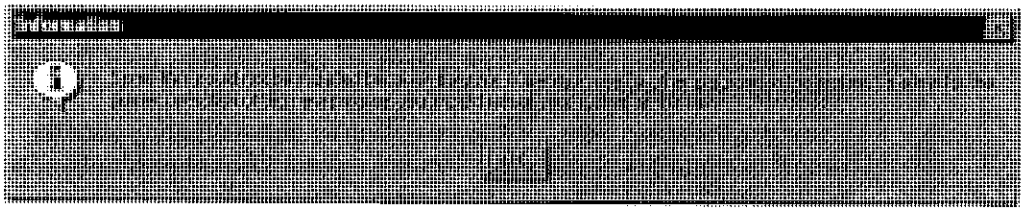
- **CD**: The CD contains the Aventail Connect setup program, `setup.exe`. The setup program allows for an administrative setup. It also contains the *Administrator's Guide* and the *User's Guide* in the `\docs` directory, formatted for Adobe® Acrobat Reader.
- **Network-delivered Source Media**: The 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 `as30s.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 (VPN Client or 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 work-

stations. 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.

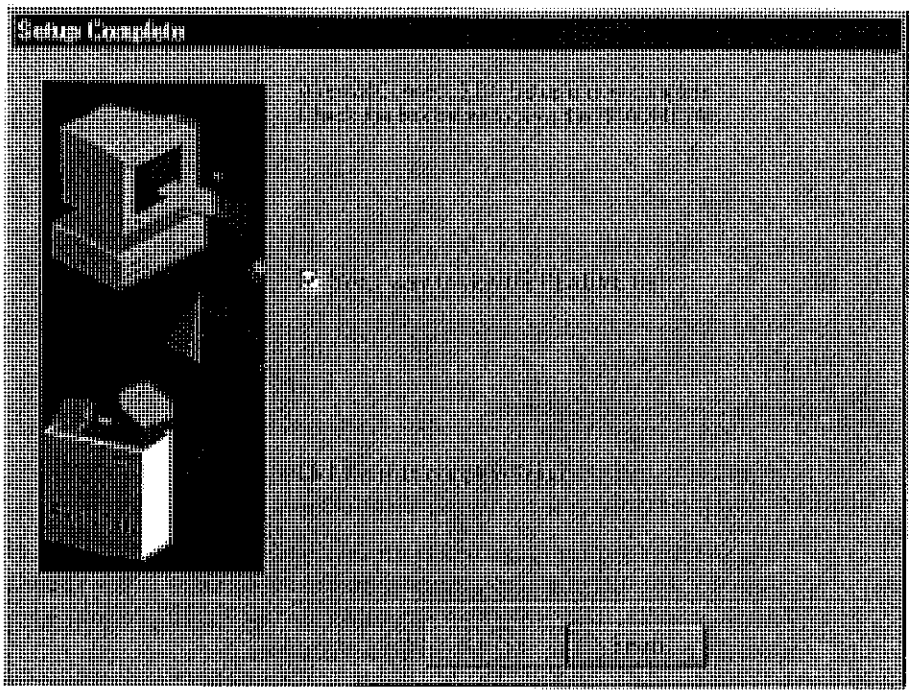
   The Aventail Connect installation wizard then guides you through the process of installing the Aventail Connect application.

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 the* ***yes*** *option. Exceptions to this can be determined by the network administrator.*

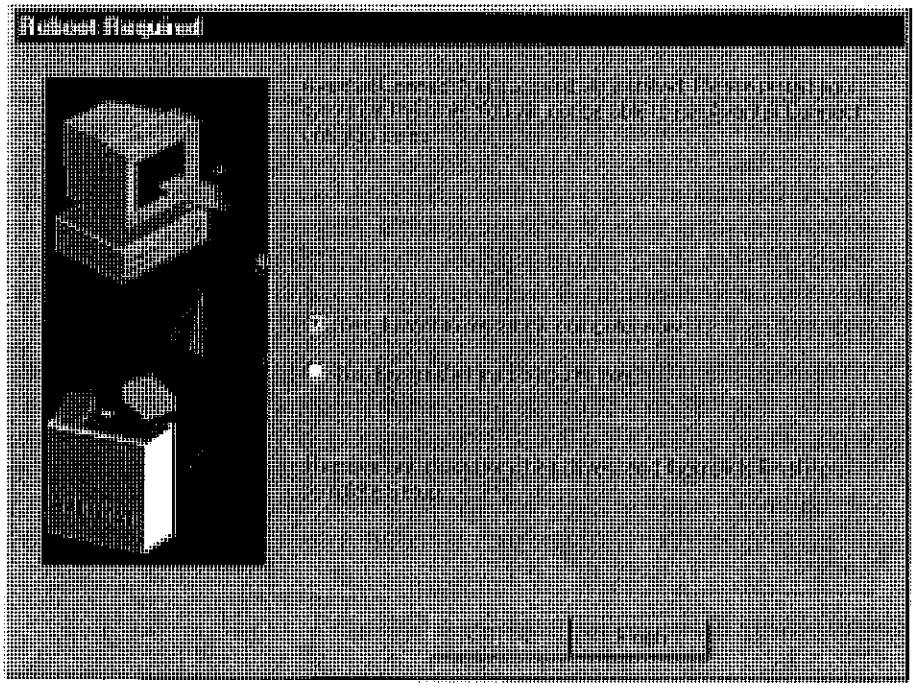
2. At the end of the setup program you can select the **Yes, I want to view the README file** box in the **Setup Complete** dialog box. This opens the `readme.txt` file, which contains the latest information on Aventail Connect.

-OR-

Simply click **Finish** 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 chose "yes" when asked if Aventail Connect should be added to your startup directory. (If you selected the **no** option during installation, 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 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 `as30s.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. 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:

- Client configuration file shared on a mapped network drive (Novell or Microsoft)
- Client configuration file distributed via a Microsoft UNC path and file-name
- Local client configuration file common for all users, but distributed via an Aventail Connect package

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. Aventail recommends that you test all configuration files before distribution.

To distribute a shared configuration file

There are three methods for distributing shared configuration files.

- Copy the file to a Microsoft or Novell network drive accessible by all users. 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-

- Copy the file 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.) This distribution method has all the benefits of placing the file on a network mapped drive with the added bonus of convenience—users do not need to actually map the network drive.

-OR-

- Create a shared configuration file to be installed on workstations during the standard Aventail Connect installation/upgrade process. (You can build the configuration file into a package with Customizer.) 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.

You can create and 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.

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 may 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.

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 (3.01 and 2.51). 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?")

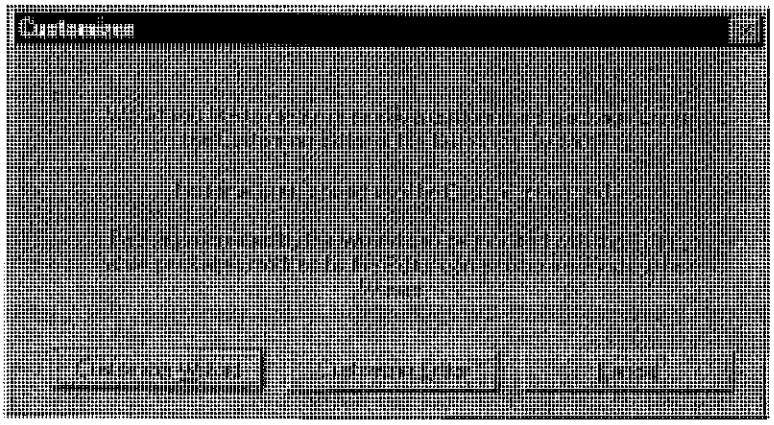
Aventail Connect requires a valid Aventail license file (`aventail.alf`) and one or more configuration (`.cfg`) files in order to function properly. Before installing Aventail Connect, make sure that users have these files. If users do not have a valid license file and/or configuration file(s), Aventail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

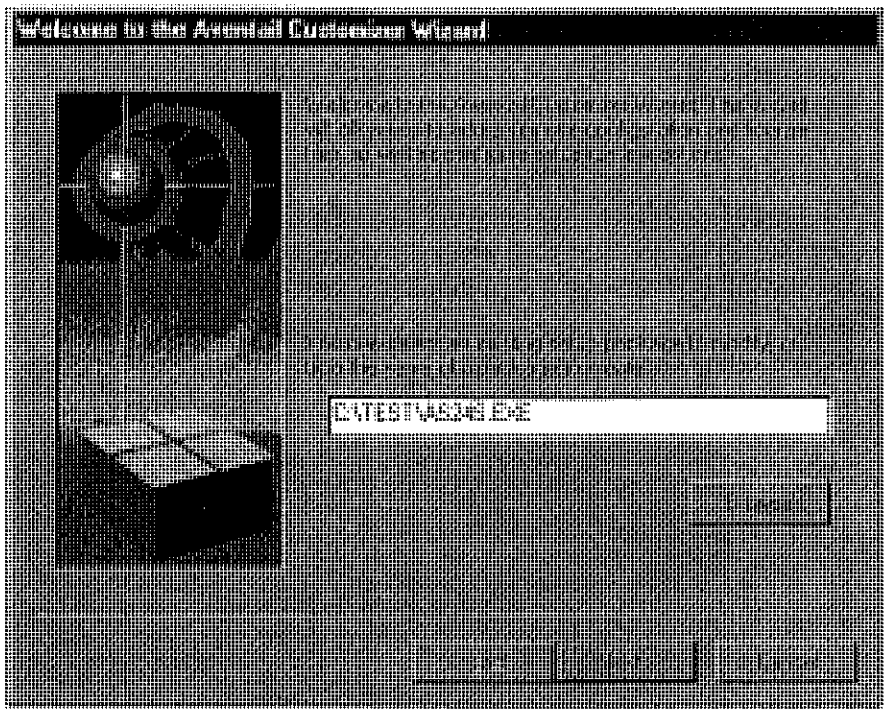
When you run Customizer, you will be prompted to select either the Customizer Wizard or the Customizer Editor.



- **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.



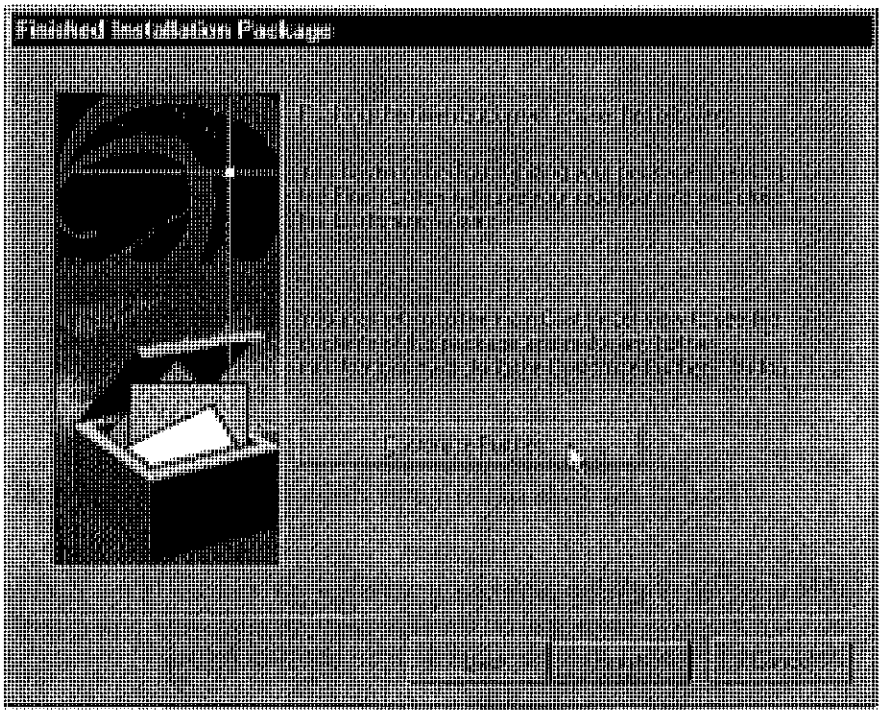
After you have specified the pathname of the package, the Customizer Wizard will prompt you to:

- 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.

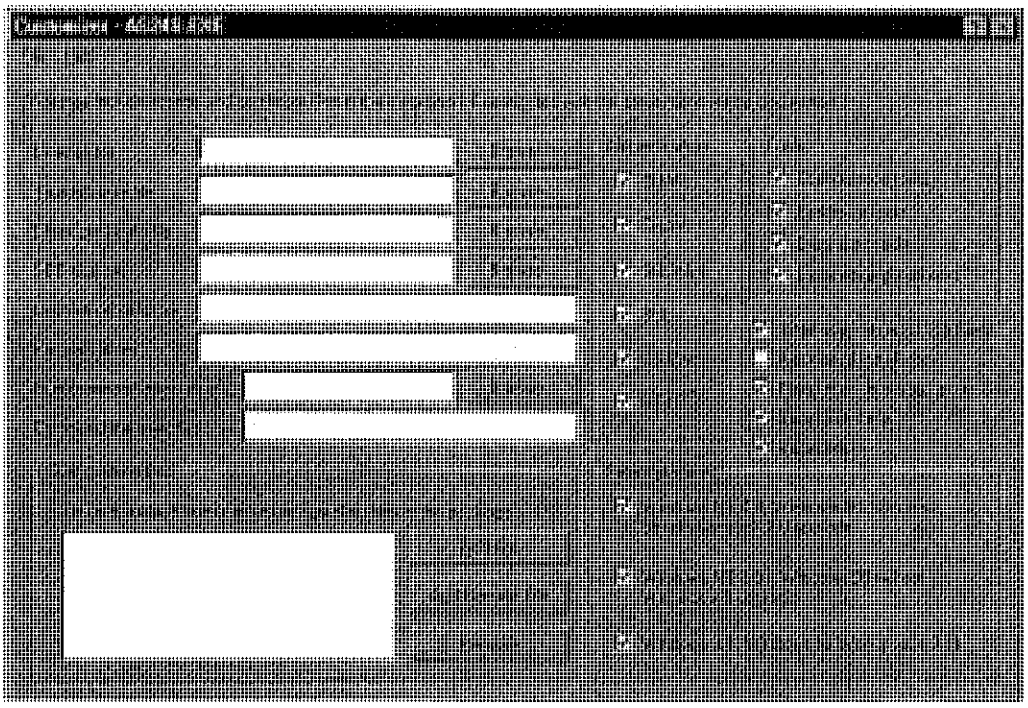
After entering or modifying the package information, the **Finished Installation Package** dialog box appears.



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 2.0 upgrade, Windows 95 without WinSock 2.0 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 3.01 supports Windows 95 (with the Microsoft WinSock 2.0 update), Windows 98, and Windows NT 4.0 (with Service Pack 3 or above, available from Microsoft). Aventail Connect 2.51 supports Windows 95 (without the Microsoft WinSock 2.0 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 3.01 and 2.51 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 (2.42 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 2.51 on Windows 95:** By default, Windows 95 does not support WinSock 2.0, but you can upgrade it to support WinSock 2.0 with a Microsoft patch. (The patch, `w95ws2setup.exe`, is available from Microsoft, at **http://www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp**. However, this procedure adds an extra step to the installation and setup process. Unless users need the Multi-Proxy feature, which is available only in Aventail Connect 3.01, Aventail recommends that you install Aventail Connect 2.51 rather than 3.01 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 3.01/2.51 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 (2.42 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 extranet (SOCKS) servers
2. Define the destinations (networks and hosts)
3. Specify redirection rules
4. Enter Local 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-

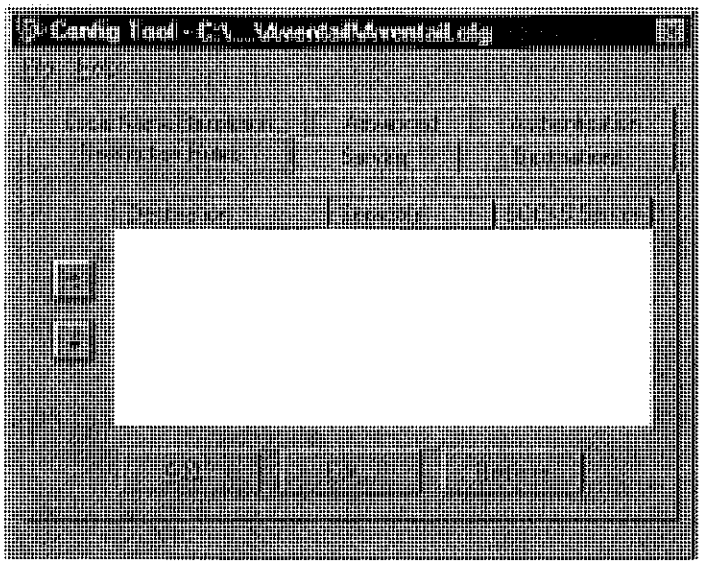
Right-click the **Aventail Connect** icon in the taskbar and click **Config Tool** (Windows 95, Windows 98, or Windows NT 4.0 programs menu option), or double-click the **Config Tool** icon in the Aventail Connect program group (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).

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.



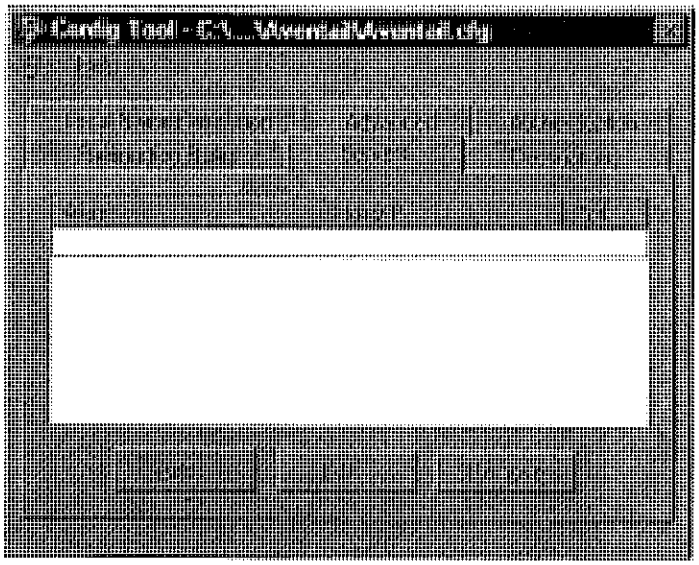
The **Config Tool** window contains six tabs. The properties defined on each tab can be edited at any time.

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).
Local 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.

DEFINE AN EXTRANET (SOCKS) SERVER

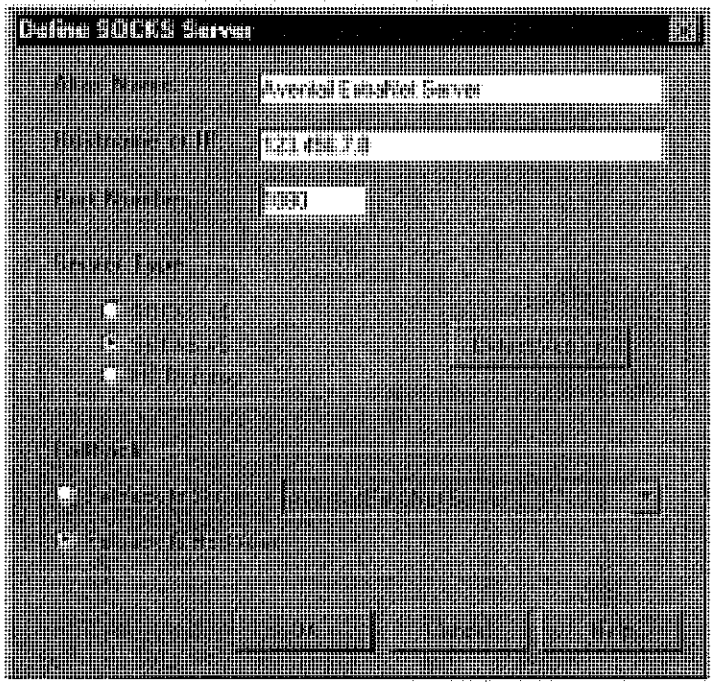
SOCKS servers are defined on the **Servers** tab in the Config Tool.



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.

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	Fallback to Server:	SOCKS server alias for redundant server.
	Fallback 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. Under "Fallback," directly specify an extranet server for redundancy or use the Host Alias to specify an extranet server.

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.

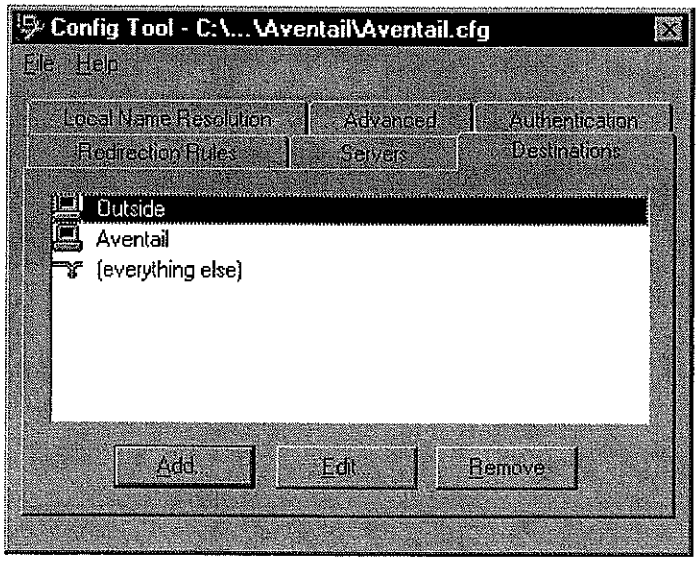
To remove an extranet (SOCKS) server definition

- 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 extranet servers are defined, add destinations to be routed through them.

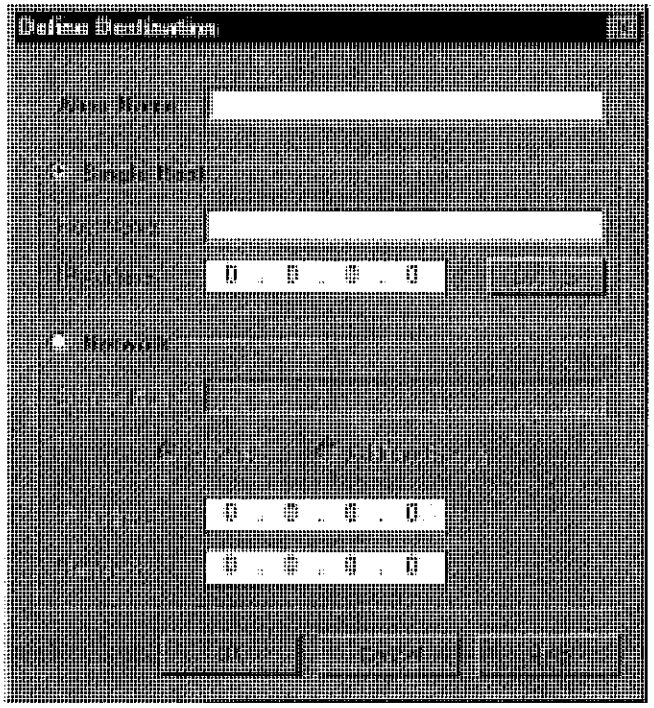
NOTE: *The "(everything else)" destination refers to all network and host addresses not otherwise defined. You cannot delete or modify "(everything else)".*

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	Full numeric IP address
	Lookup	Look up IP address
Network	One or more computers in a network	
	Domain Name	Domain of the network
	Subnet	IP address and netmask address
	Address Range	Beginning and ending IP addresses From Starting IP address To Ending IP address

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 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

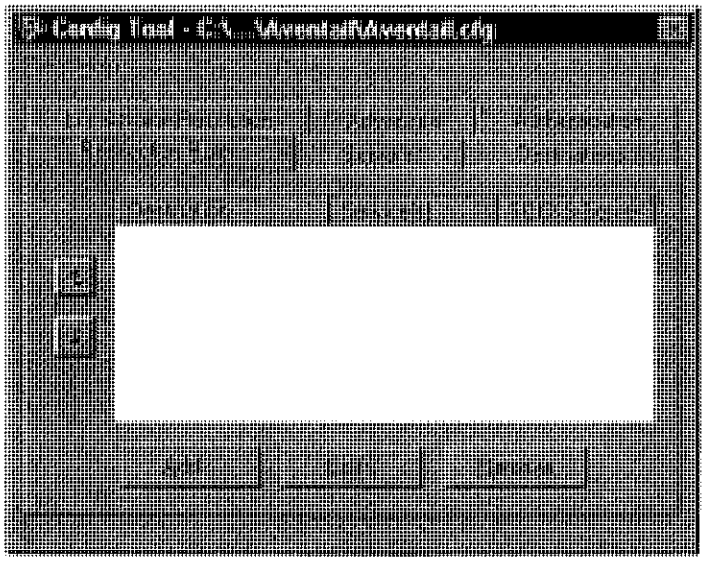
- Select the destination you want to remove and click **Remove**.

  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.

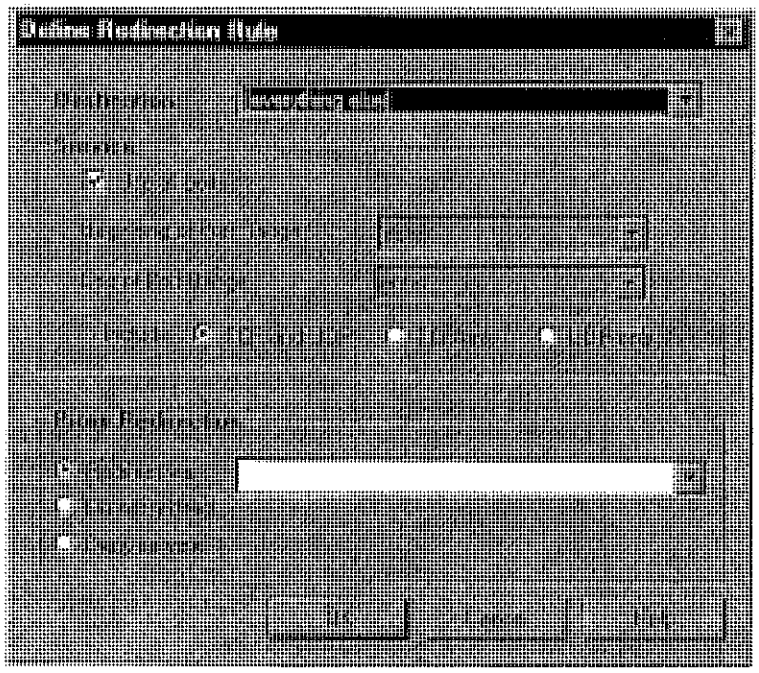
To add a redirection rule

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.

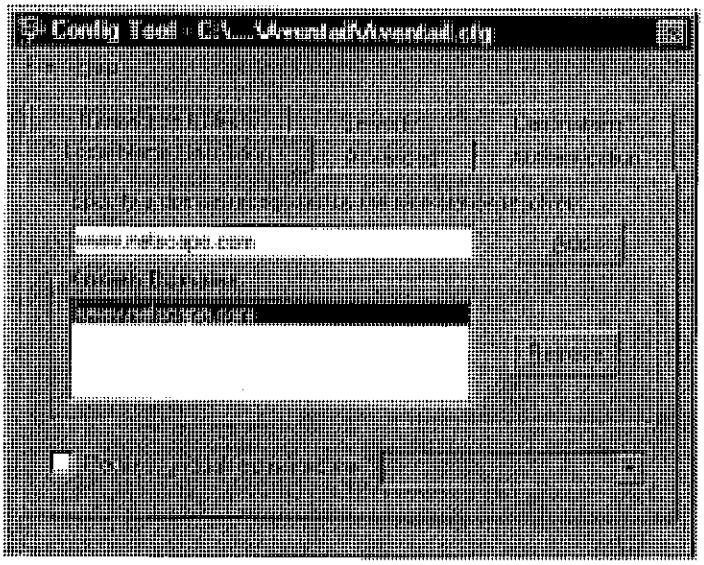
DEFINE LOCAL NAME RESOLUTION

Local 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 **Local 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.

Local Name Resolution is specified on the **Local 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

To add a local domain name

- On the **Local Name Resolution** tab, type the new name in the **Specify a domain** box and click **Add...**.

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

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.*

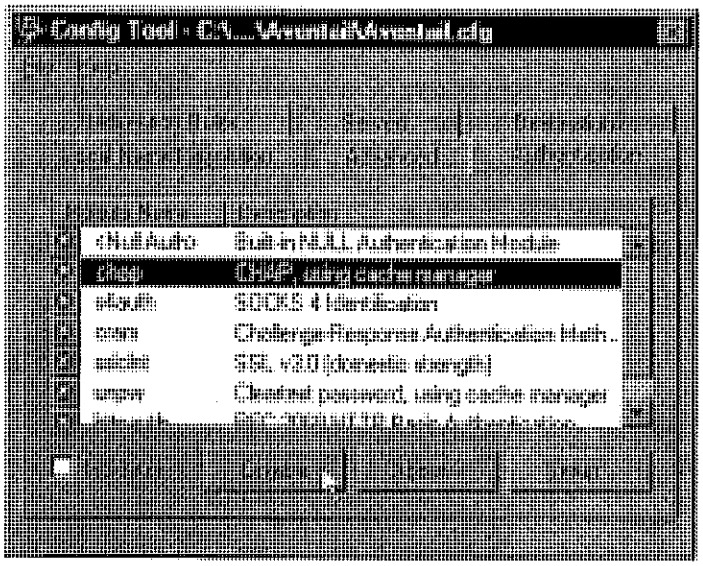
The current Aventail Connect authentication modules are SOCKS v4 Identification, Username/Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Each of these authentication modules 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.

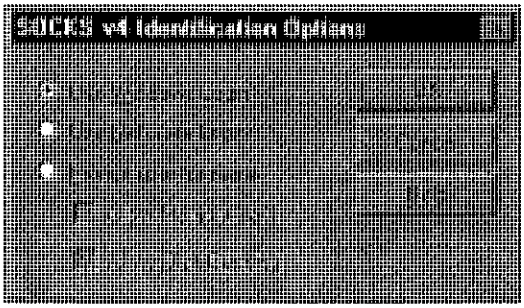
To configure the SOCKS 4 Identification module

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.

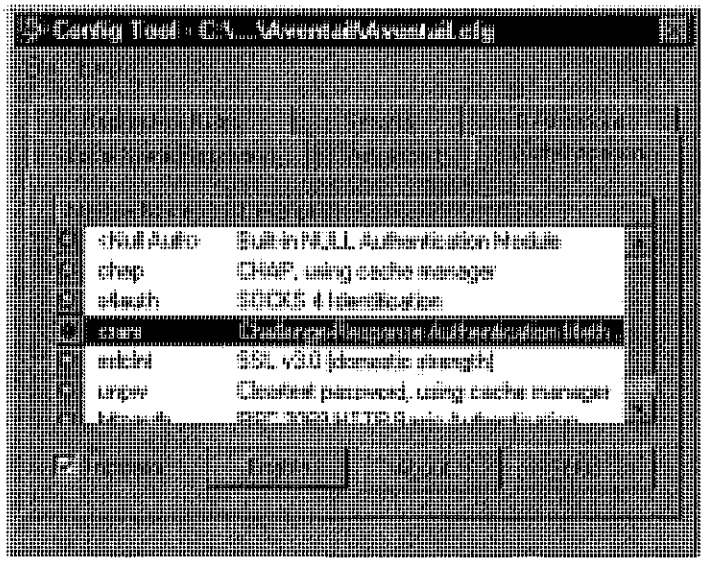
Field	Description
Allow memory caching	Stores credentials in memory for this session only. Cache is flushed upon restart; credentials must be reentered as prompted.
Allow disk caching	This option is currently unavailable. (Stores encrypted credentials on disk for future sessions.)

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) 3.0, 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.

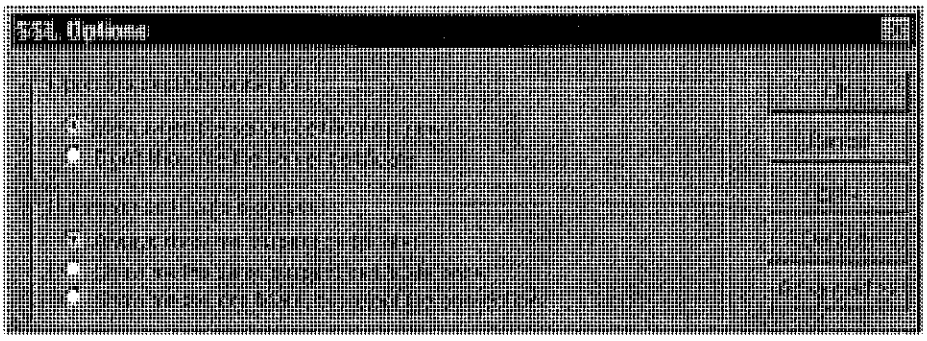
Certificates contain special integrity checks and electronic signatures that verify that the certificate is genuine, was issued by a certification authority, and was not tampered with. Anybody can issue a certificate that says anything; the client must know who issued the certificate, and have some trust 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 3.0) and click **Setup**.

   The **SSL Options** dialog box appears.



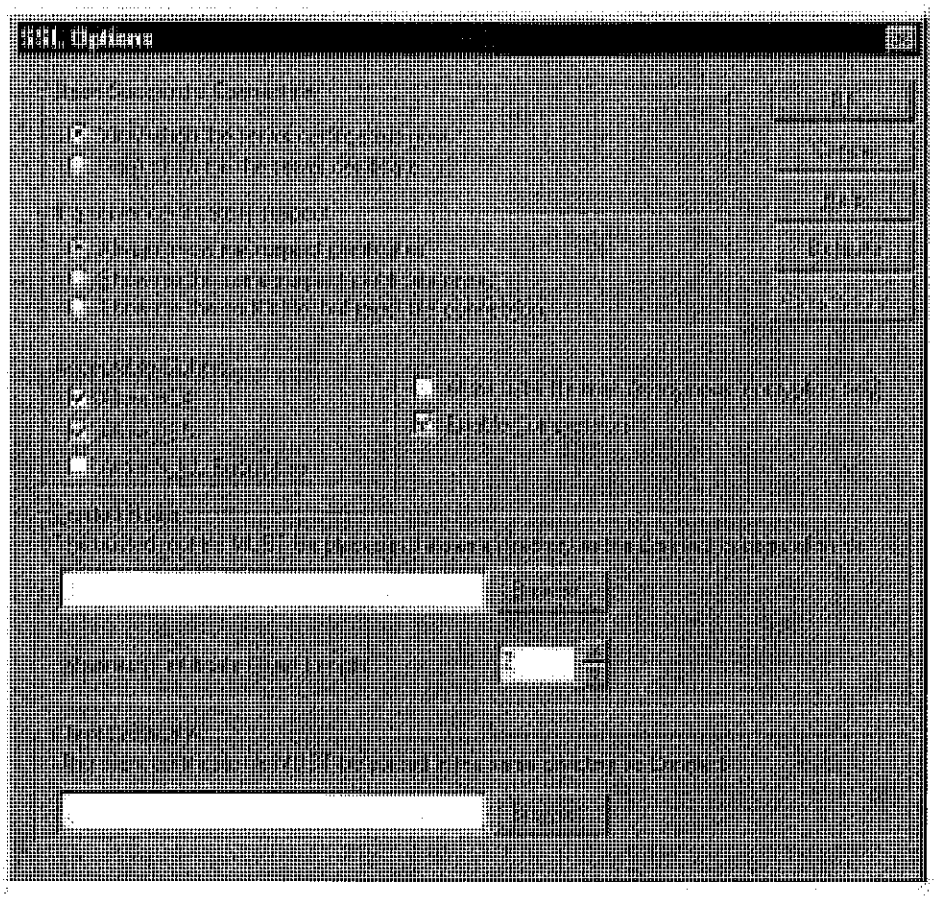
Field		Description
Upon Successful Connection		The certificate is valid.
	View when the server certificate is new.	Upon successful connection, display the server certificate if it has not been displayed during the current session.
	Do not show me the certificate.	Never display a valid server certificate.
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.	
Trusted Roots	Select a certificate file that specifies trusted certificate chain roots, and specify the maximum allowable certificate-chain length. *NOTE: The trusted root file MUST be placed in the same directory as the Aventail Connect configuration file.*	
	Browse	Select the specific file
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 root (`*.rot`) to (or from) the list of trusted roots by clicking **Browse**. Only the filename of the roots file loads via the **Browse** button, and not the pathname.

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

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.

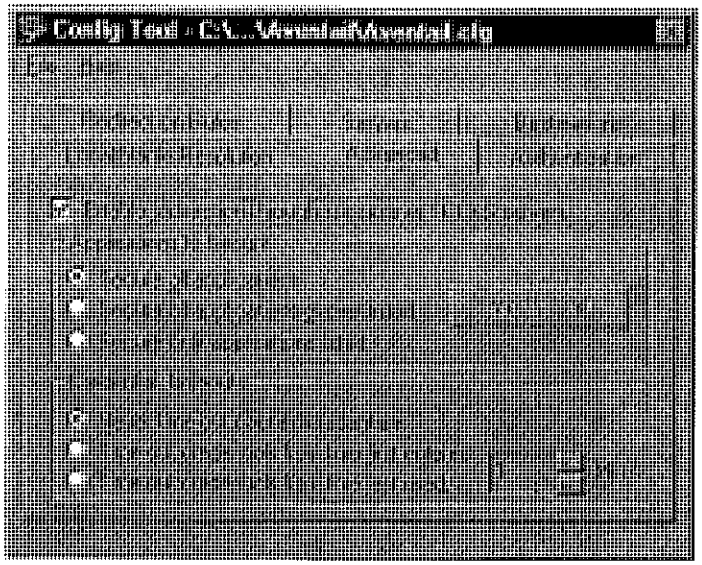
CAUTION: *In most instances, Aventail recommends allowing no more than two certificates in a certificate chain. Allowing more than two certificates can compromise security.*

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

   The dialog box closes and the Config Tool reappears.

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 timeouts.



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.*

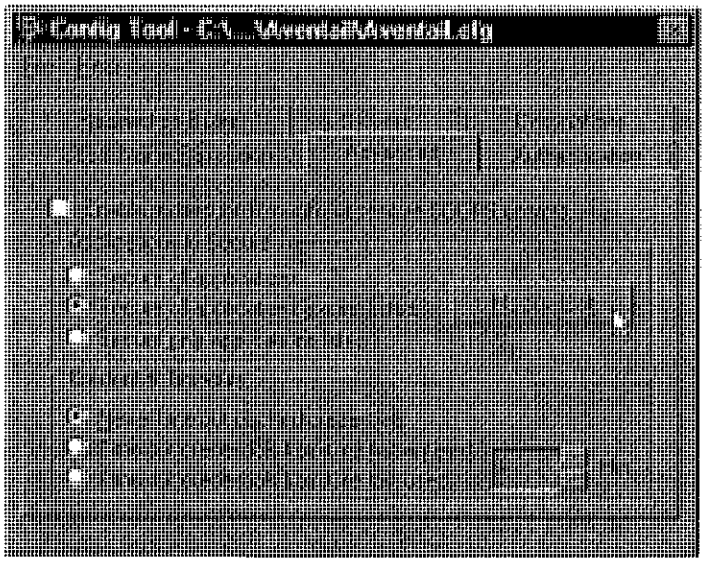
You can exclude or include specified applications in the Exclusion/Inclusion List. With the Exclusion/Inclusion List, you can secure all applications *except* those on the list, or you can secure *only* those applications on the list. The default setting is to secure (hook) *all* network applications.

Excluding Applications

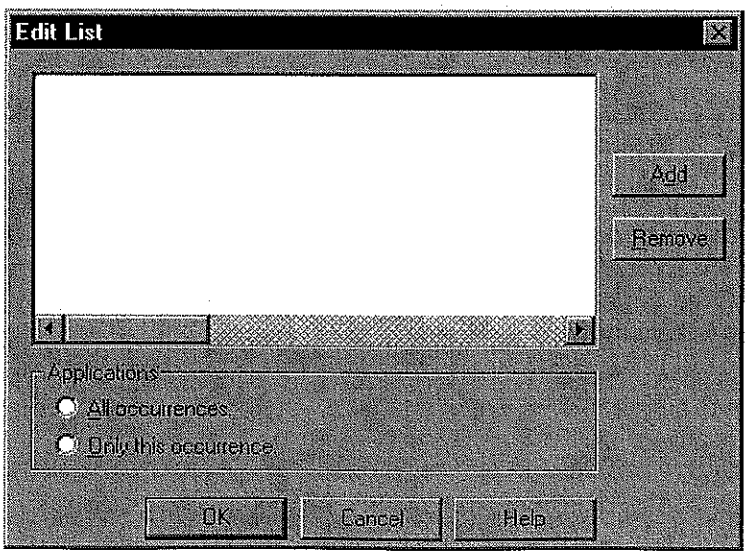
You can exclude specific applications through the Exclusion/Inclusion List. When you enable the "Secure all applications except listed" option, Aventail Connect will not proxy any applications that are on the Exclusion/Inclusion List.

To exclude an application

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

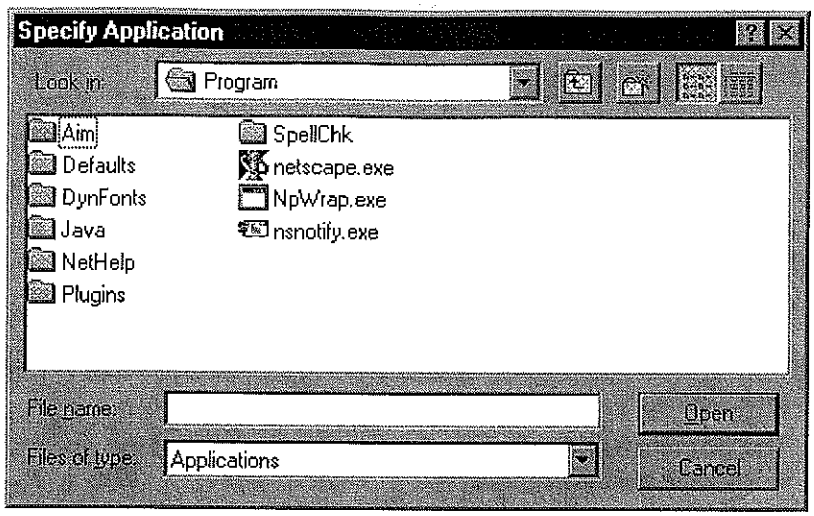


The **Edit List** dialog box appears.



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

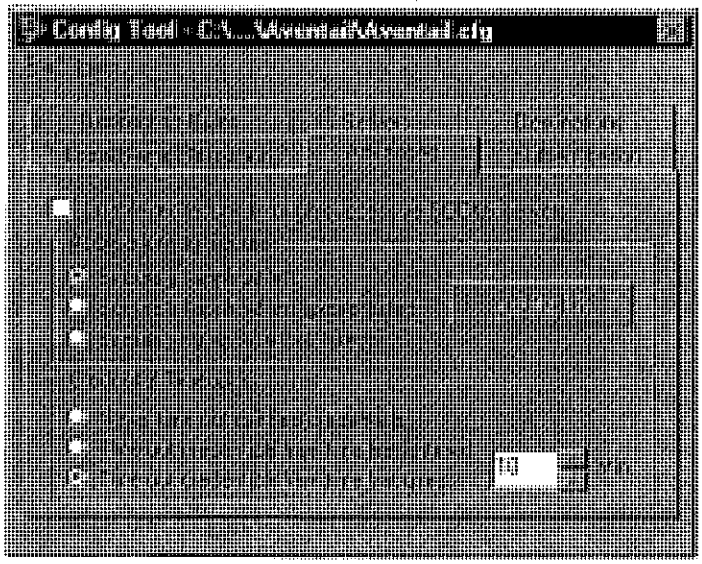
- On the **Advanced** tab, under "Applications to Secure," select **Secure all applications**.

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 3.01. 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).

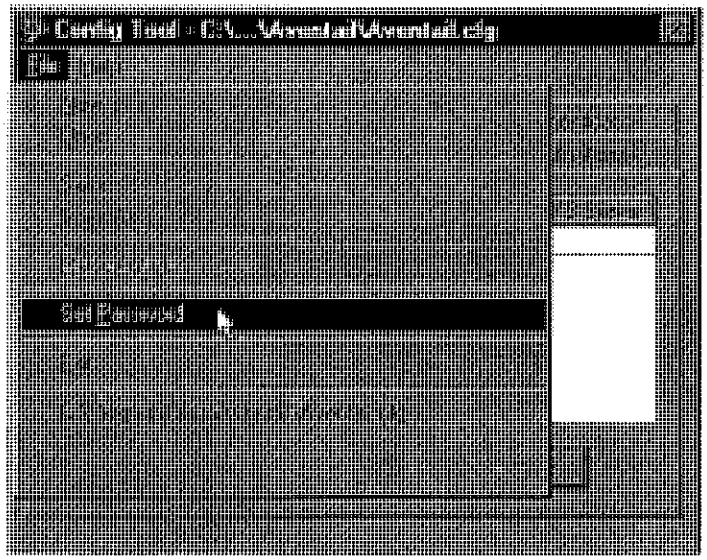
CAUTION: *If your mail program is configured to check for e-mail at regular intervals, the mail-checking frequency must be longer than the credential cache timeout. For example, if your mail program is configured to check for mail every ten minutes, you should set the credential cache to less than ten 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 3.01 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.

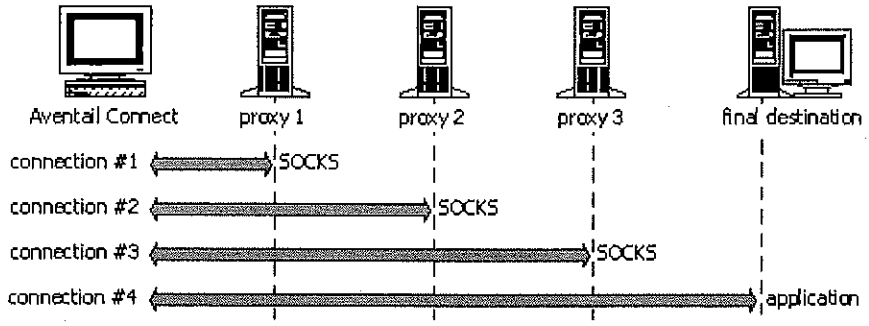
Using an HTTP proxy server to control outbound traffic eliminates the need to install a separate SOCKS server. This HTTP proxy can filter outbound connection requests and route those requests to the specified servers. MultiProxy supports RFC 2068 HTTP Basic (username/password) authentication. If your 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 3.01 only. HTTP proxies cannot be used in Aventail Connect 2.51.*

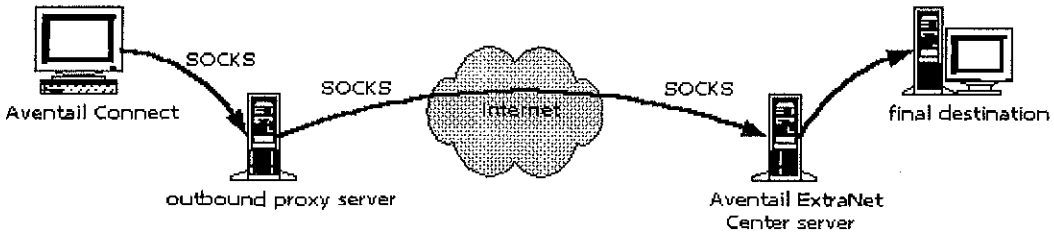
The steps for making a connection using MultiProxy are:

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 3.01 to redirect all Internet traffic (including extranet traffic) through your outbound proxy, or you can configure Aventail Connect 3.01 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-

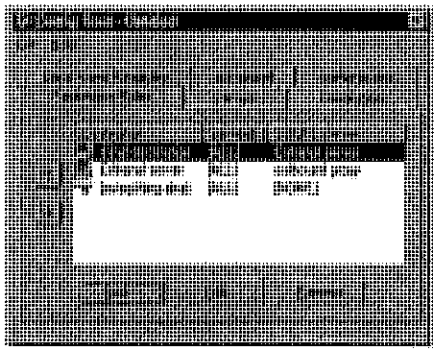
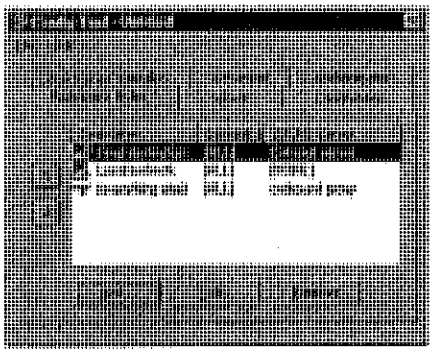
   To redirect all Internet traffic (including extranet traffic): Create a destination ("Local network," the network local to Aventail Connect).

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-

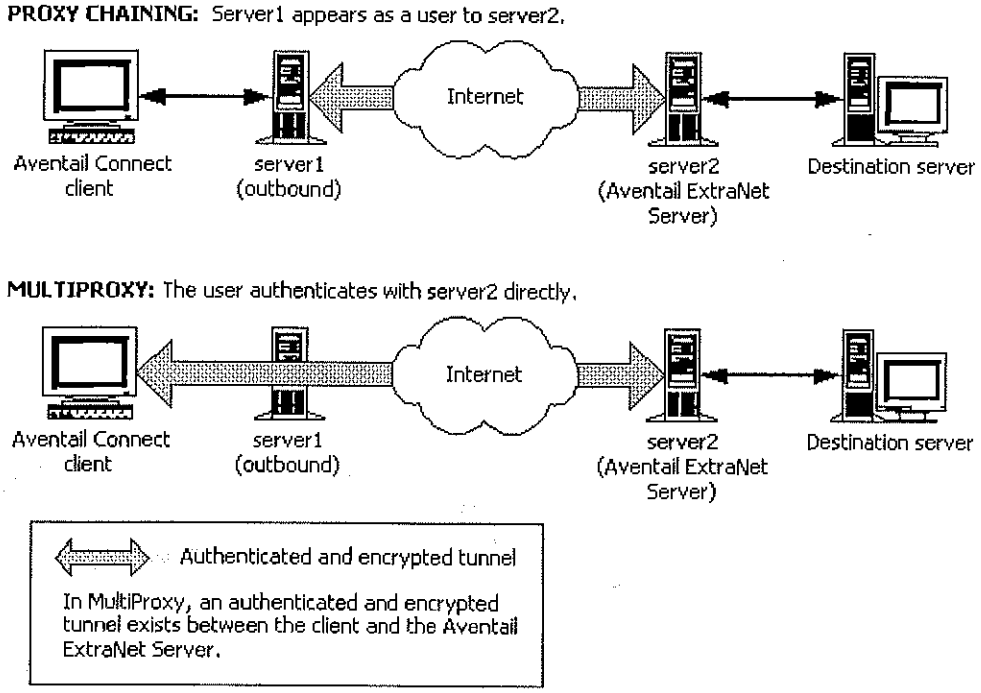
   To redirect all Internet traffic (including extranet traffic): Create a redirection rule (Do not redirect "Local network"). Redirect "(everything else)" through the outbound proxy. (**NOTE:** Your outbound proxy must belong to "Local network.")

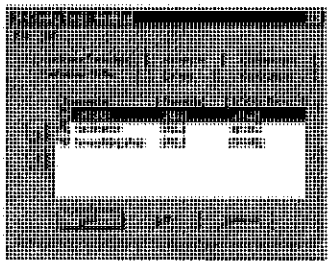
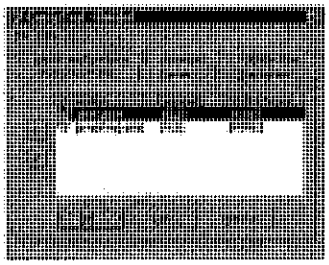
Redirect only extranet traffic	Redirect all Internet traffic (including extranet traffic)
	
Redirect only the extranet traffic through the outbound proxy. Leave all other traffic alone.	Redirect all Internet traffic through the outbound proxy. Leave only "Local network" traffic alone.

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.)

THE CERTIFICATE WIZARD

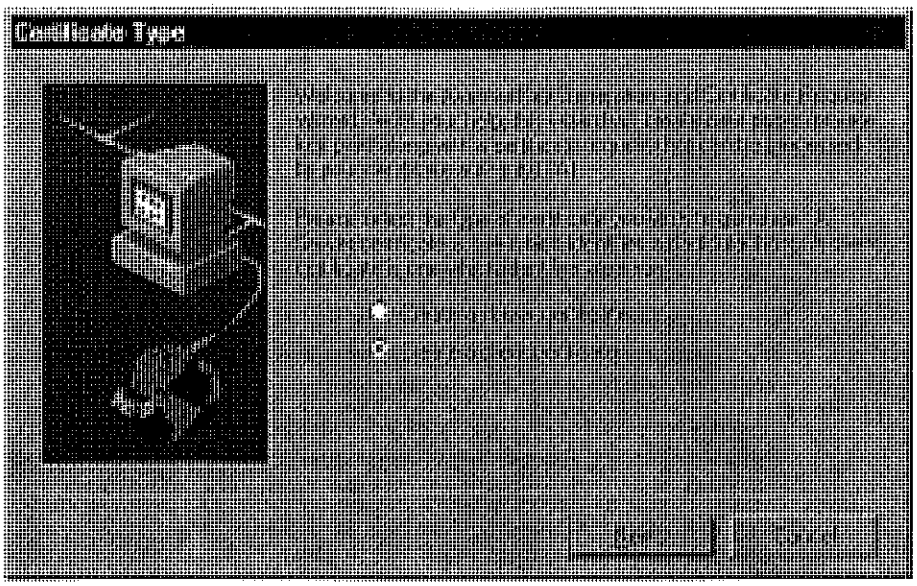
Aventail Connect supports client certificates and provides you with a certificate wizard to help *generate* and *process* a certificate. You start the certificate wizard through the Aventail Connect program group (via the **Start** button or Program Manager).

The Certificate wizard can create certificates for clients and servers. In this case, you are only interested in creating a client certificate. However, whether for client or server, you will need to run this wizard twice: Once to *generate* a Certificate Signing Request (CSR) to submit to your Certificate Authority (CA); the second time, to *process* the certificate file. If this is your first time in generating a certificate request, Aventail recommends that you complete the second step immediately after the first.

To generate the client key pair and Certificate Signing Request (CSR)

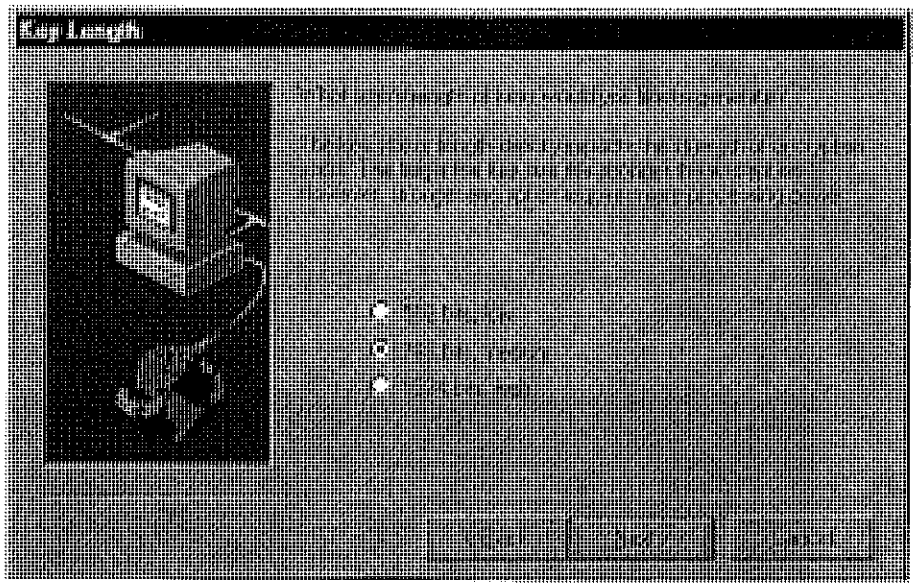
1. Select the certificate wizard from the Aventail Connect program group.

2. In the **Certificate Type** dialog box, select the **client certificate** option, and then click **Next**.

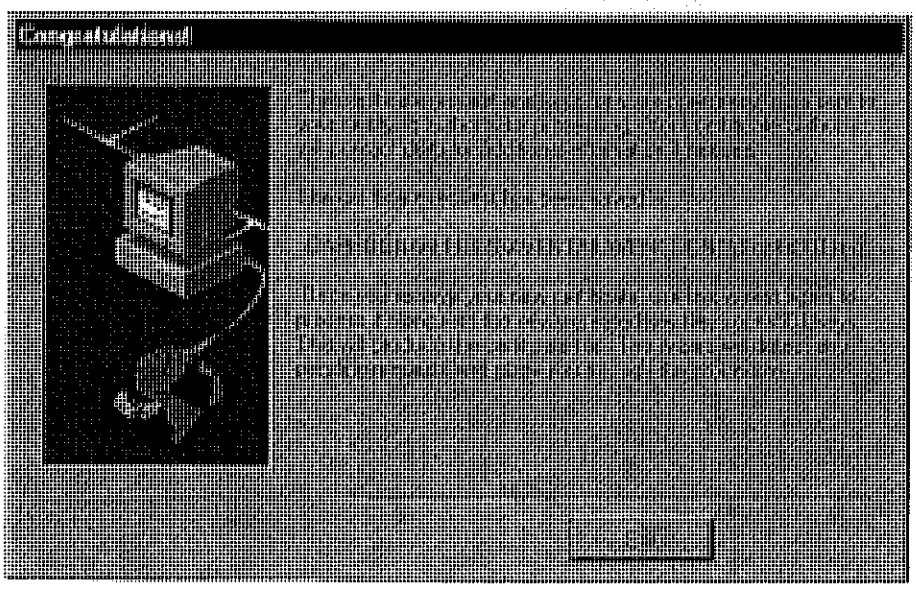


3. Provide the requested information by following the prompts in the subsequent dialog boxes.
4. In the **Key Length** dialog box, select the size of your key.

NOTE: *Not all CAs accept keys larger than 512 bits. It is prudent to know which key lengths your CA accepts prior to generating your key pair. For testing purposes use 512 bits.*



5. Once you have generated the random data, continue through the screen prompts until the **Congratulations!** screen, where you will see the name and path to the new certificate request.



To submit the Certificate Signing Request (CSR)

1. You are now ready to submit the CSR (the `*.req` file) to your CA (usually via e-mail).

   Aventail works with many certificate servers and certification authorities. Companies such as VeriSign (**www.verisign.com**) issue both client and server

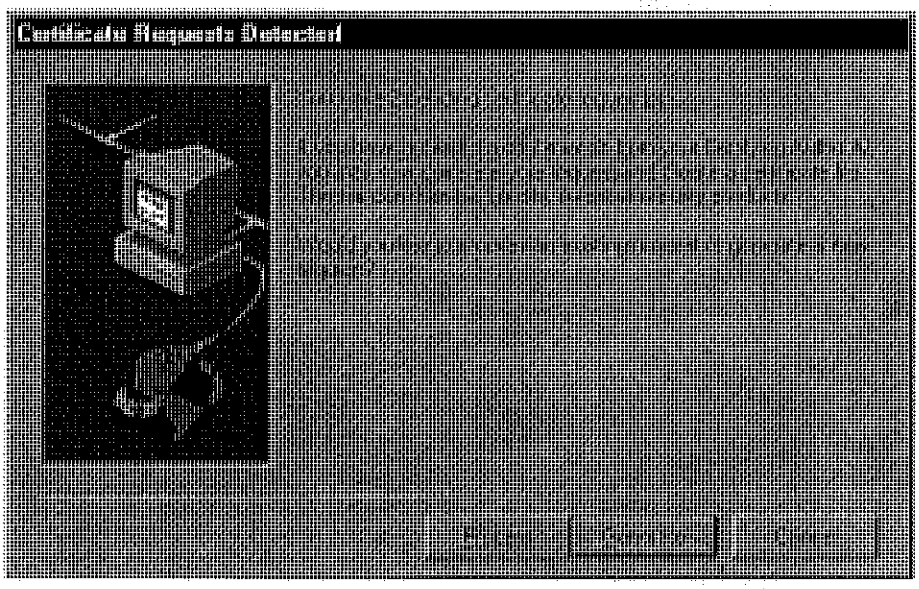
certificates. The Aventail Web site (**www.aventail.com**) gives concise instructions (see "TechNotes") on how to use these programs with Aventail's certificate wizard. Aventail CSRs are generated in a standard PKCS #10 format.

The CA will create a certificate file and issue a trusted roots file.

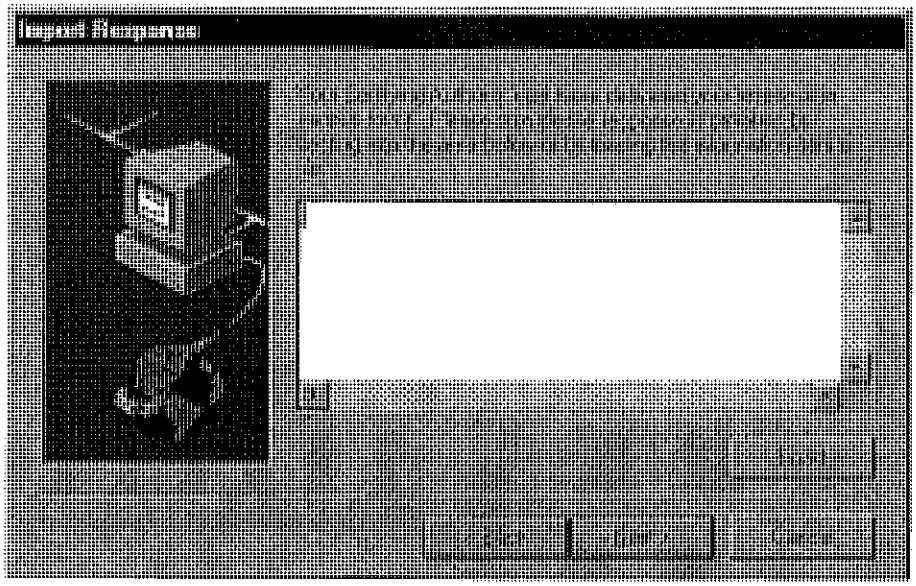
2. On receipt, copy (or place) the trusted roots file into the same directory as the configuration file, and the certificate file into the Aventail Connect directory.

To process the CSR

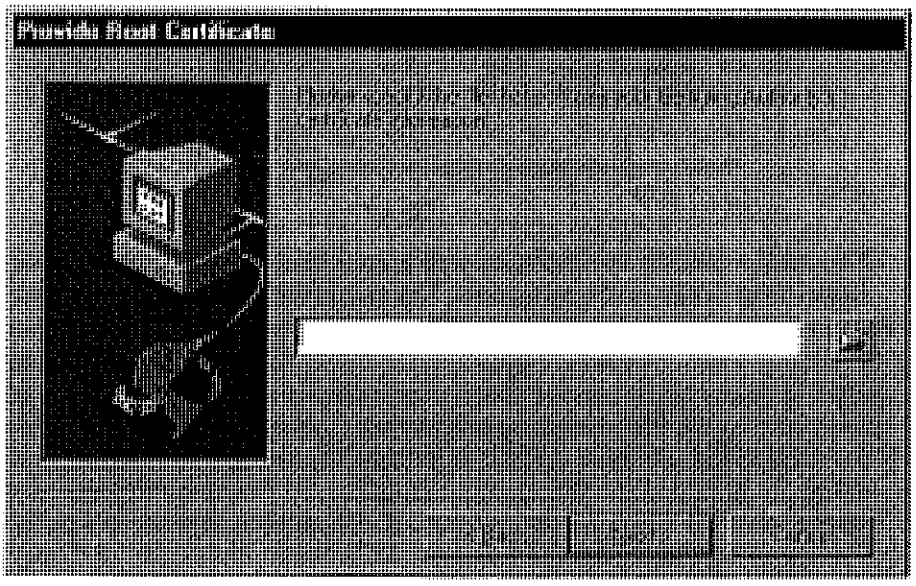
1. Run the certificate wizard, again. The wizard will detect the pending requests. Click **Process**.



2. Follow the prompts on the following screens. You will be asked to paste or load the certificate response information in a window area. Click **Next**.



3. Provide the root certificate file name in the **Root Certificate** screen. The root certificate is your "trusted" root file. Click **Next**.



4. The **Summary** screen will identify the pathnames to your key file, and certificate.

   Verify that the roots file is in the same directory as the configuration file and that the certificate file is in the Aventail Connect directory.

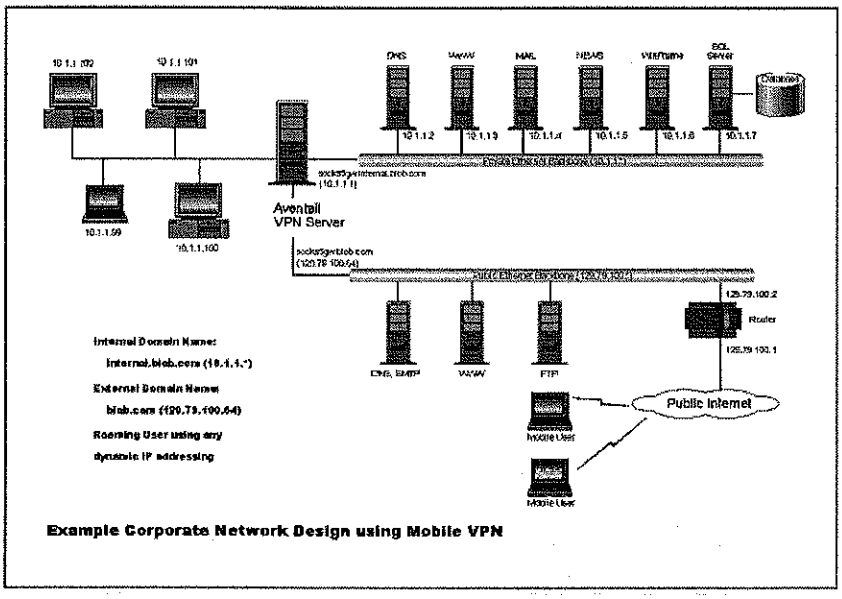
   You have successfully created a client certificate and key pair.

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.

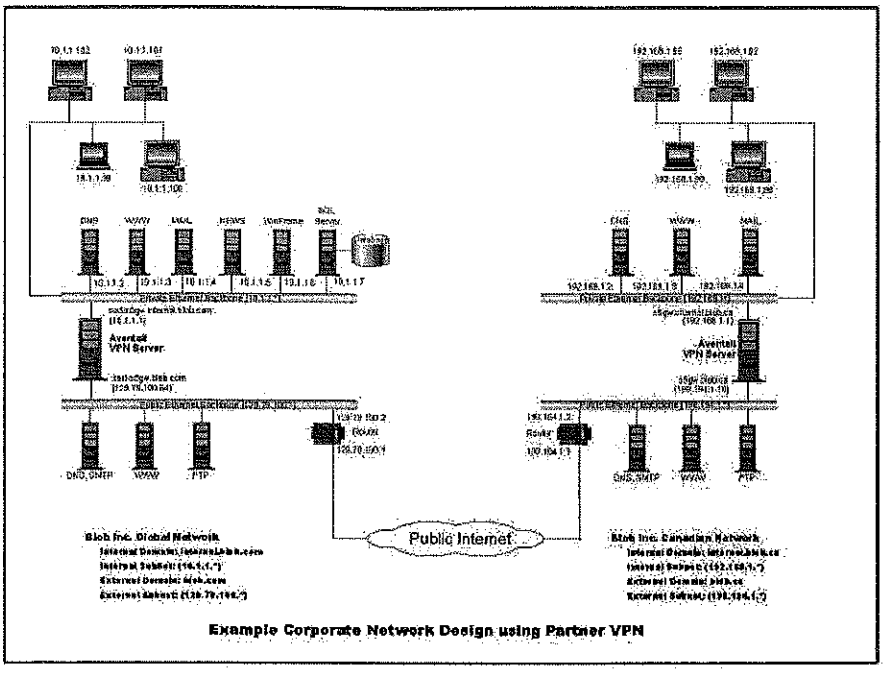
The Aventail ExtraNet Server in our example, has two network adapters configured to use the internal IP address of 10.1.1.1 and an external address of 129.79.100.64.

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 a new configuration file via **Startup Options** 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.

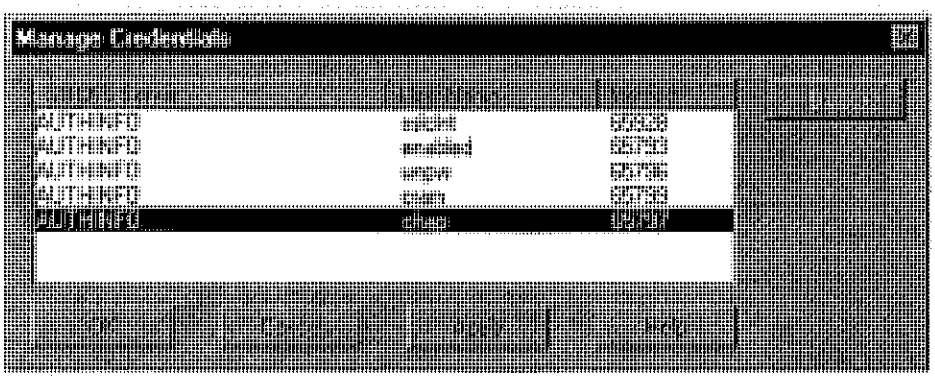
ABOUT

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.

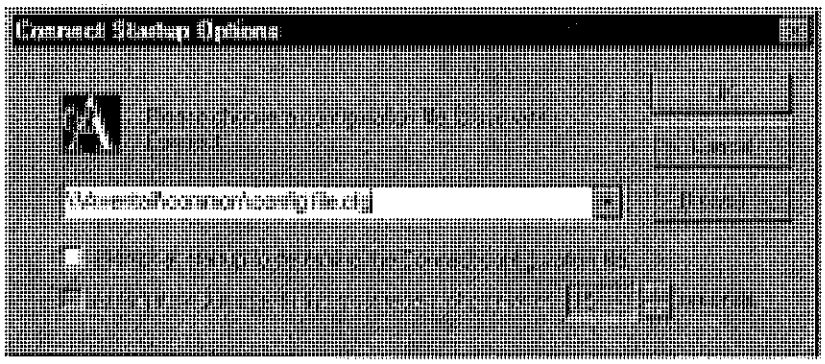
-OR-

- 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 **Startup Options** dialog box.



For more information about the configuration file, refer to "Creating Configuration Files."

To load a configuration file

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

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

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

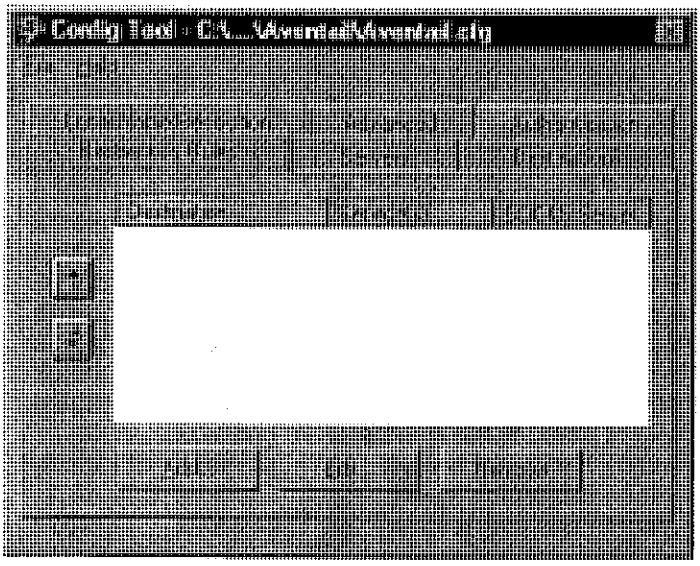
Menu Command	Function
Config Tool	Runs the Config Tool. (Optional)
Logging Tool	Runs the Logging Tool. (Optional)
S5 Ping	Runs the ping and traceroute utilities. (Optional)

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. "Creating Configuration Files" 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,

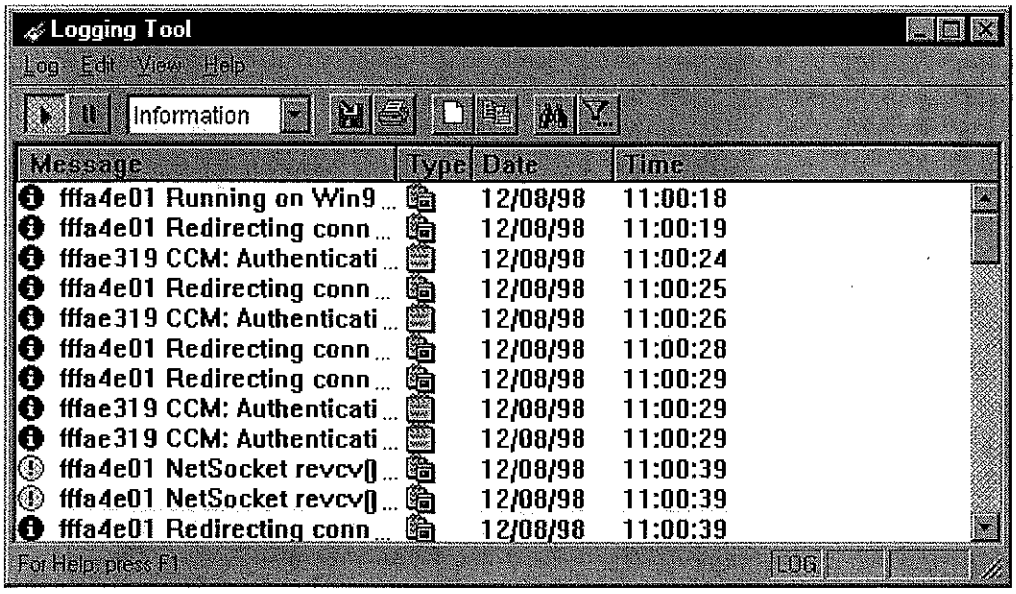
and e-mail it to them as an attachment. Log files are also useful when running Aventail Connect for the first time, to ensure that network traffic is being routed properly.

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-

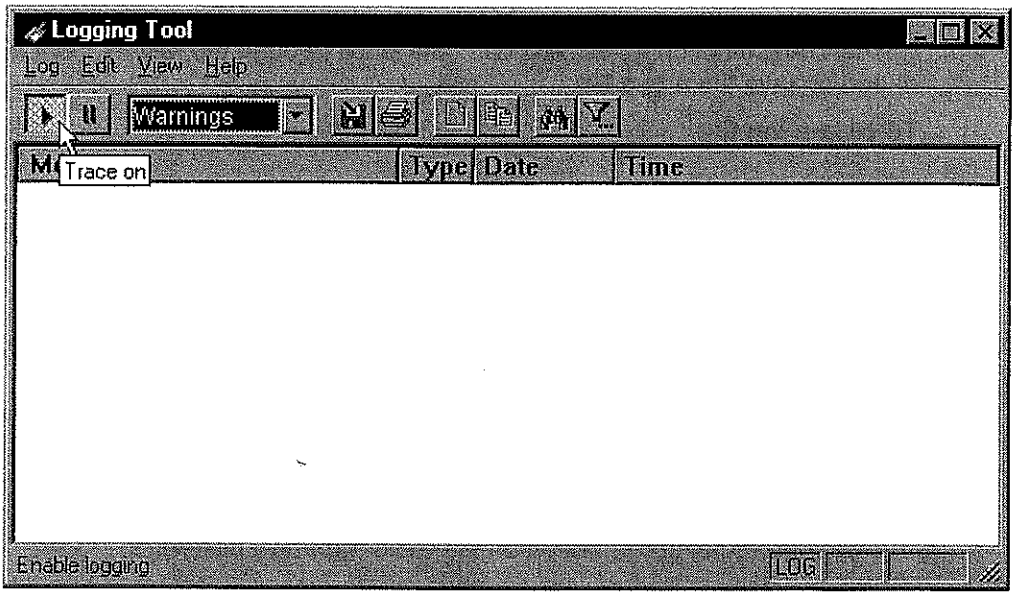
Select one of the five levels from the drop-down list on the toolbar.

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).

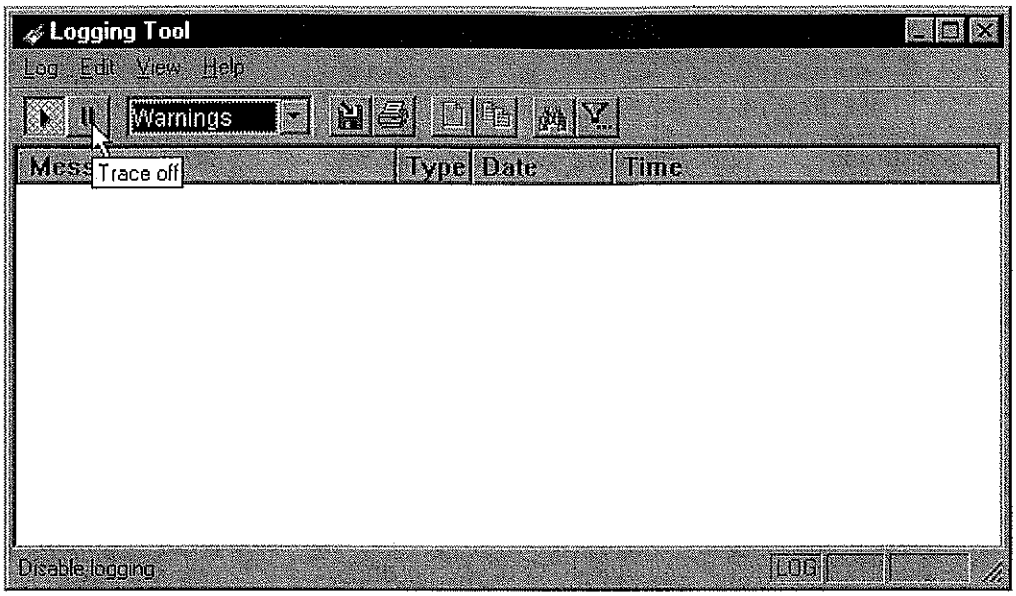


The log window will now record and display trace information as it is generated by Aventail Connect. You can tell when the trace function is active because messages are scrolling down the screen and the **Trace On** button is depressed.

4. When you are ready to stop the **T**race 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

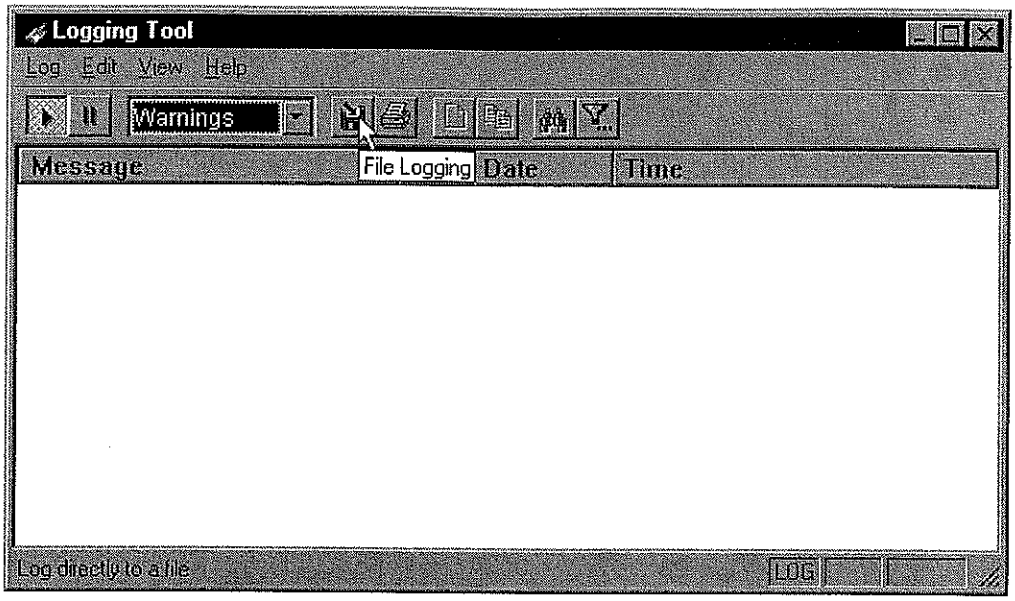
The Logging Tool allows you to append each new message to the end of a `.LOG` file during the trace, or save the contents of the log window at any time. If you save during a trace, Aventail Connect will append messages to the log file until you stop the log function. You must save data in the log window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

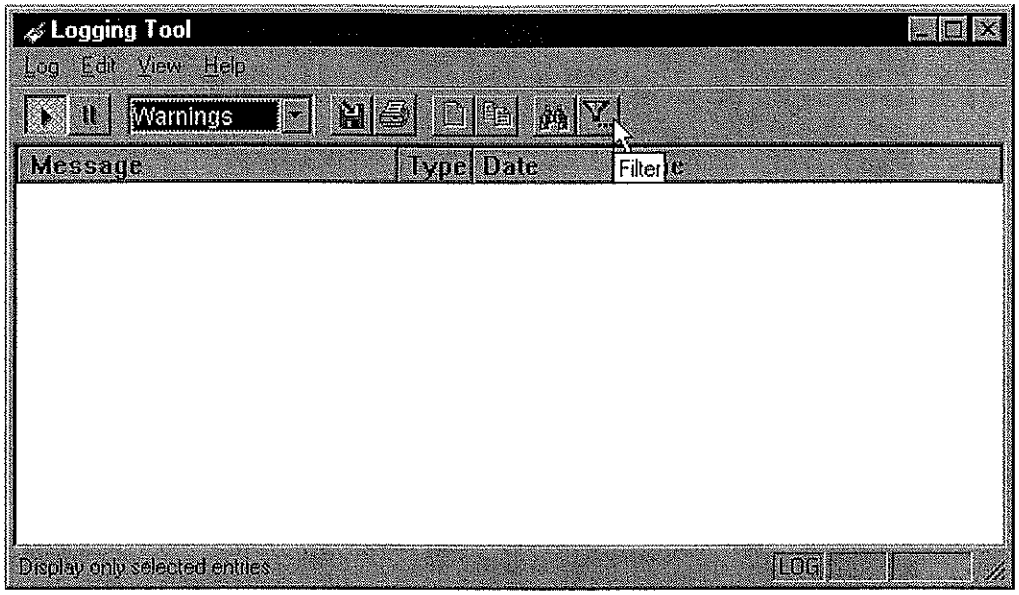
To filter messages in the log window

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.

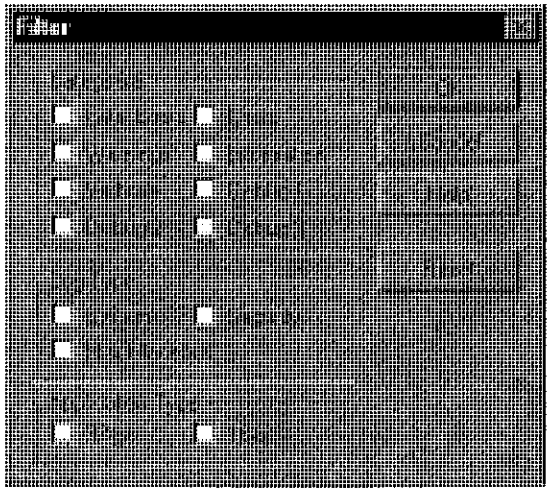
1. On the **View** menu, click **Filter Messages** to display the **Filter** dialog box

-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

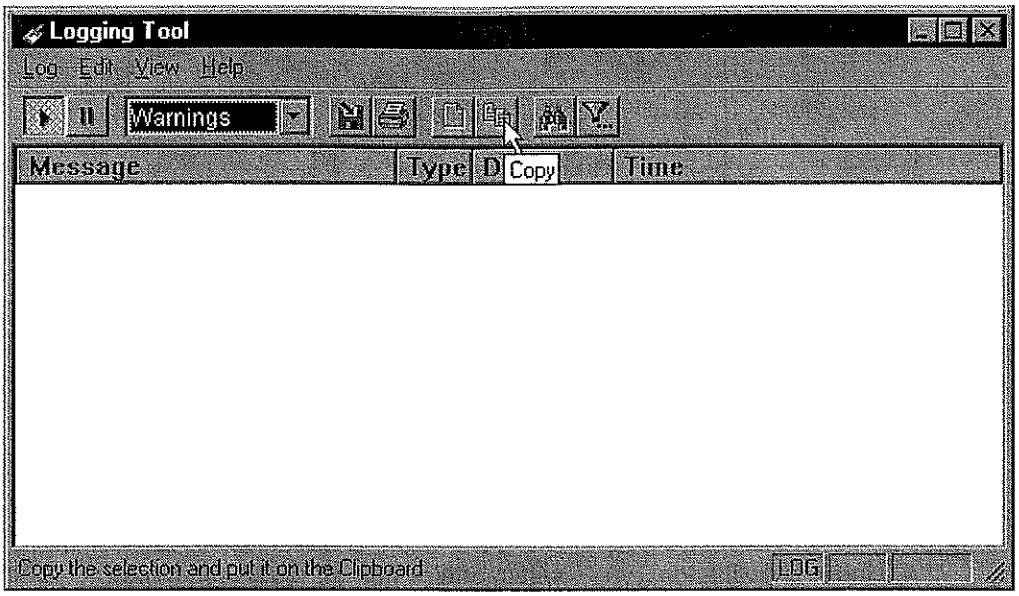
The display font and window options can be customized as follows:

- 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**.

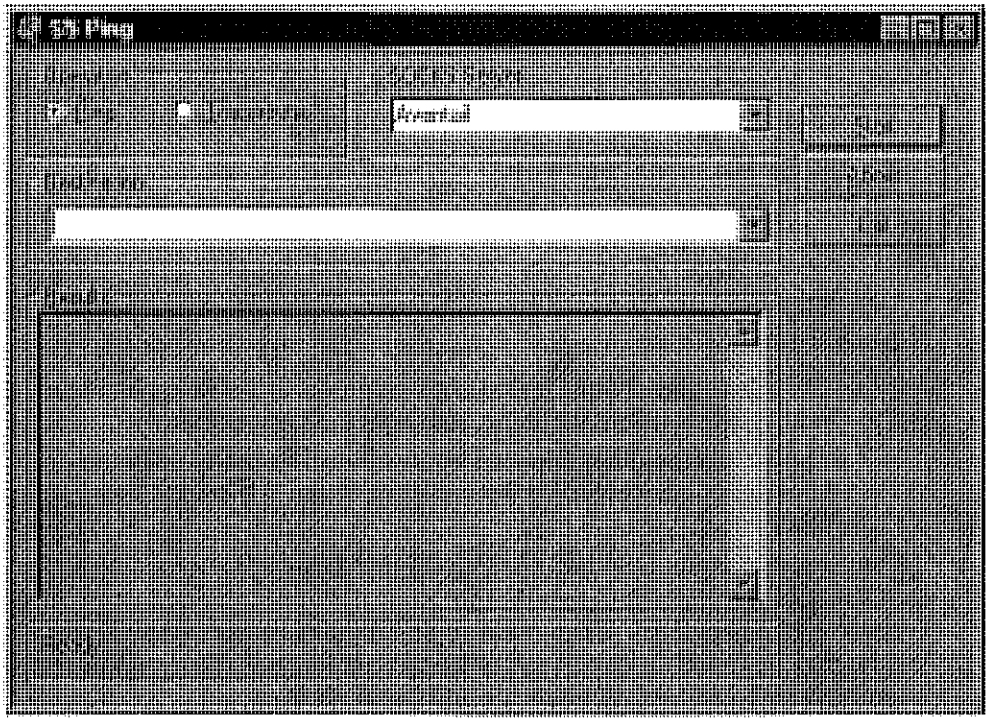
-OR-

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-

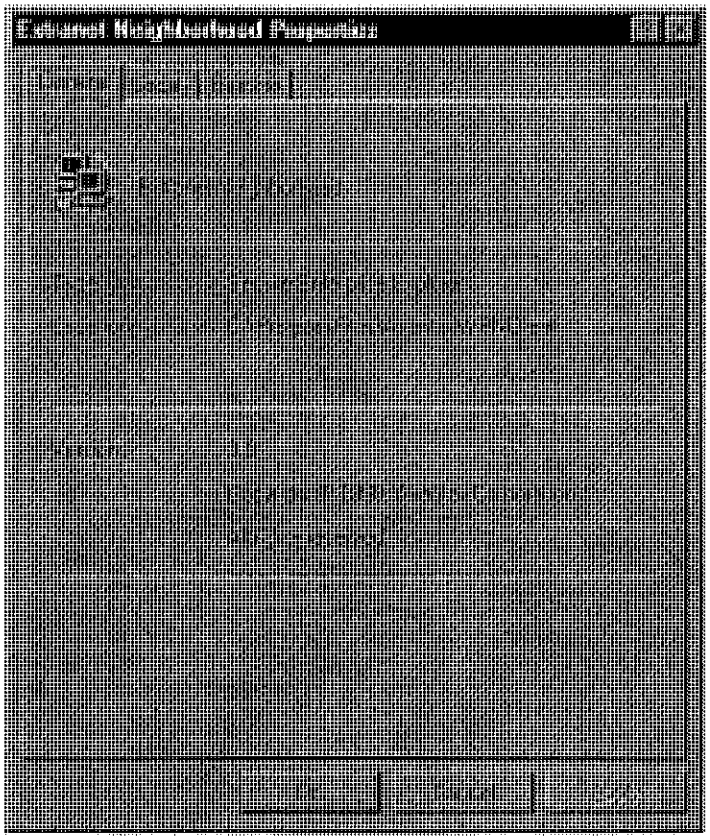
- Specify some computers in a local hosts file and others in a remote hosts file.

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 I Options** in any open **SEE** window. The **Extranet Neighborhood Properties** window will appear with the **General** tab selected.

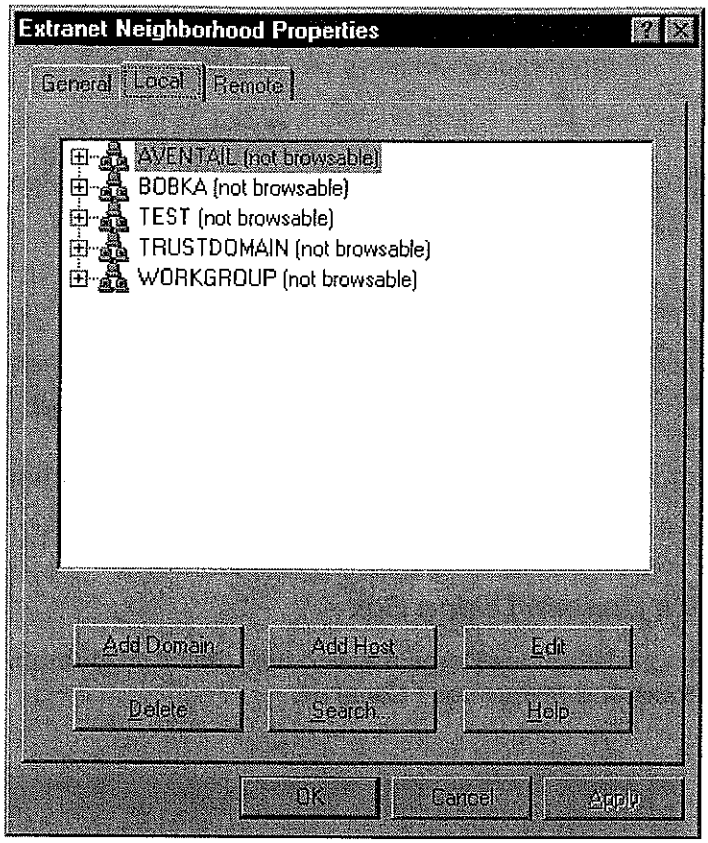
THE GENERAL TAB

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

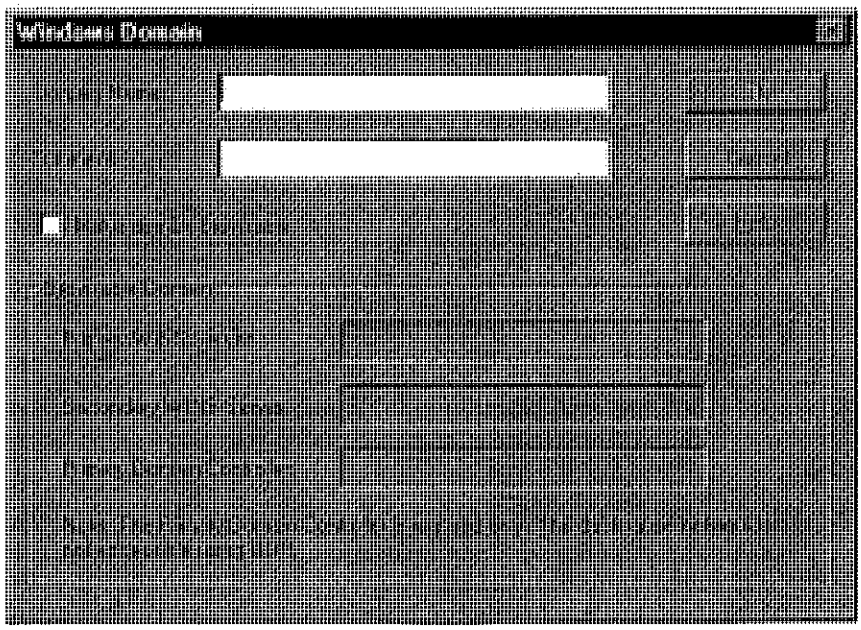
If the controls in this window are disabled (dimmed), then the hosts file has been "locked." The network administrator determines which, if any, hosts files are locked.

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 I 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.

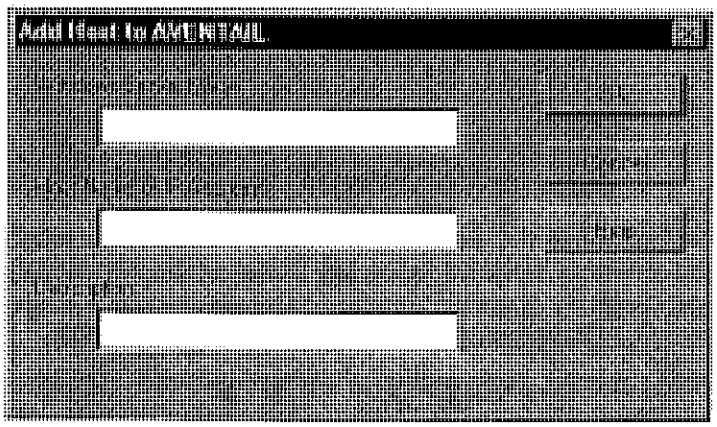
To make the specified domain "browsable," enter WINS server information in the **Primary WINS Server** box and, if desired, the **Secondary WINS Server** box. In both of these boxes, you can enter either the server's IP address or its fully qualified host name. You must also select the **Make domain 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.

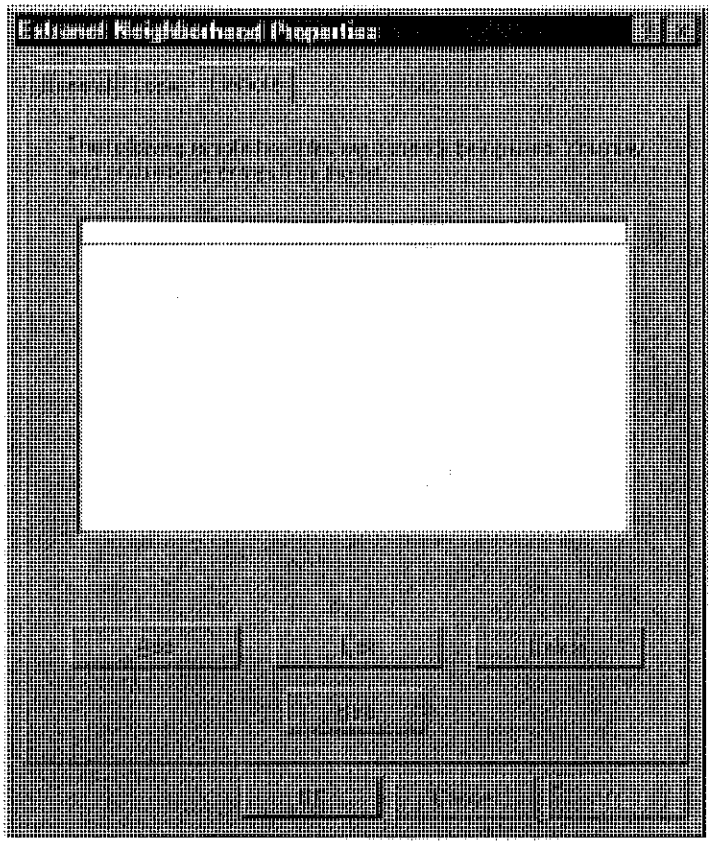


Aventail Connect automatically places hosts within the domain that is selected when you click **Add Host**. Select the correct domain before clicking **Add Host**. You must specify a domain before you can add hosts to that domain.

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.

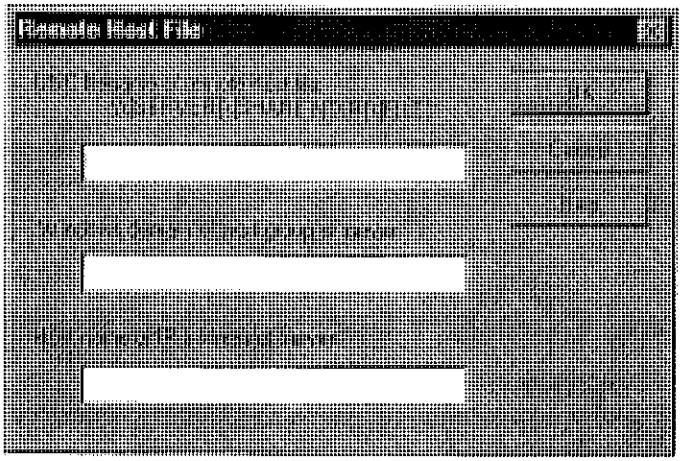
The most common configuration is one remote hosts file (with all domains and hosts in the remote hosts file) and one local hosts file that contains a pointer to the remote hosts file. If you want users to share a common hosts file, and if you want to simplify administration, use a remote hosts file.

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.

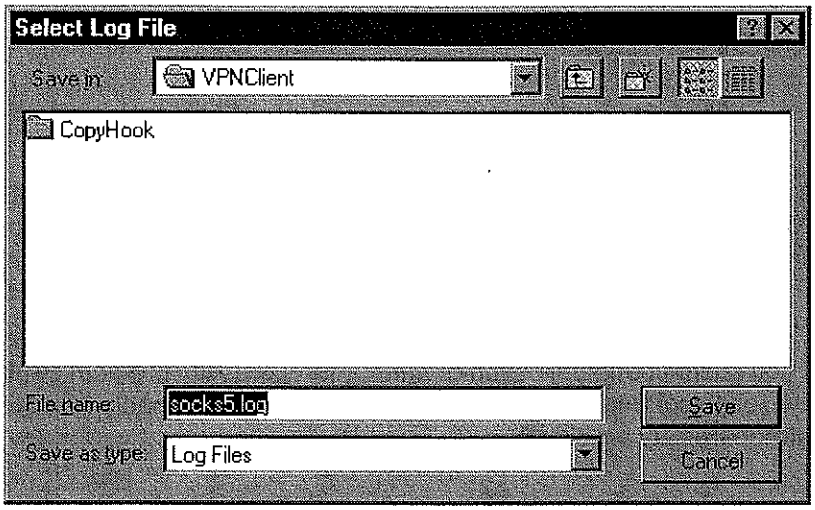
To run an Aventail Connect trace

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 2.0 patch, available from Microsoft.	SETUP: To install Aventail Connect 3.01, you must first install the Microsoft WinSock 2.0 upgrade.
The patch is available for download on the Microsoft Web site, at **www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp**.	SETUP: Location of the Microsoft WinSock 2.0 upgrade.
You must have administrator privileges to install.	SETUP: On Windows NT machines, you must have administrative privileges to install or uninstall Aventail Connect.

Error Message	Meaning
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 3.01 files. Please contact your administrator.	SETUP: Setup cannot find the necessary Aventail Connect 3.01 files.
The package does not contain the necessary 2.51 files. Please contact your administrator.	SETUP: Setup cannot find the necessary Aventail Connect 2.51 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 2.51 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 2.0, allowing two-way communication between the WinSock 2.0-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.

Exhibit F

Aventail Extranet Server v3.0 Administrator's Guide

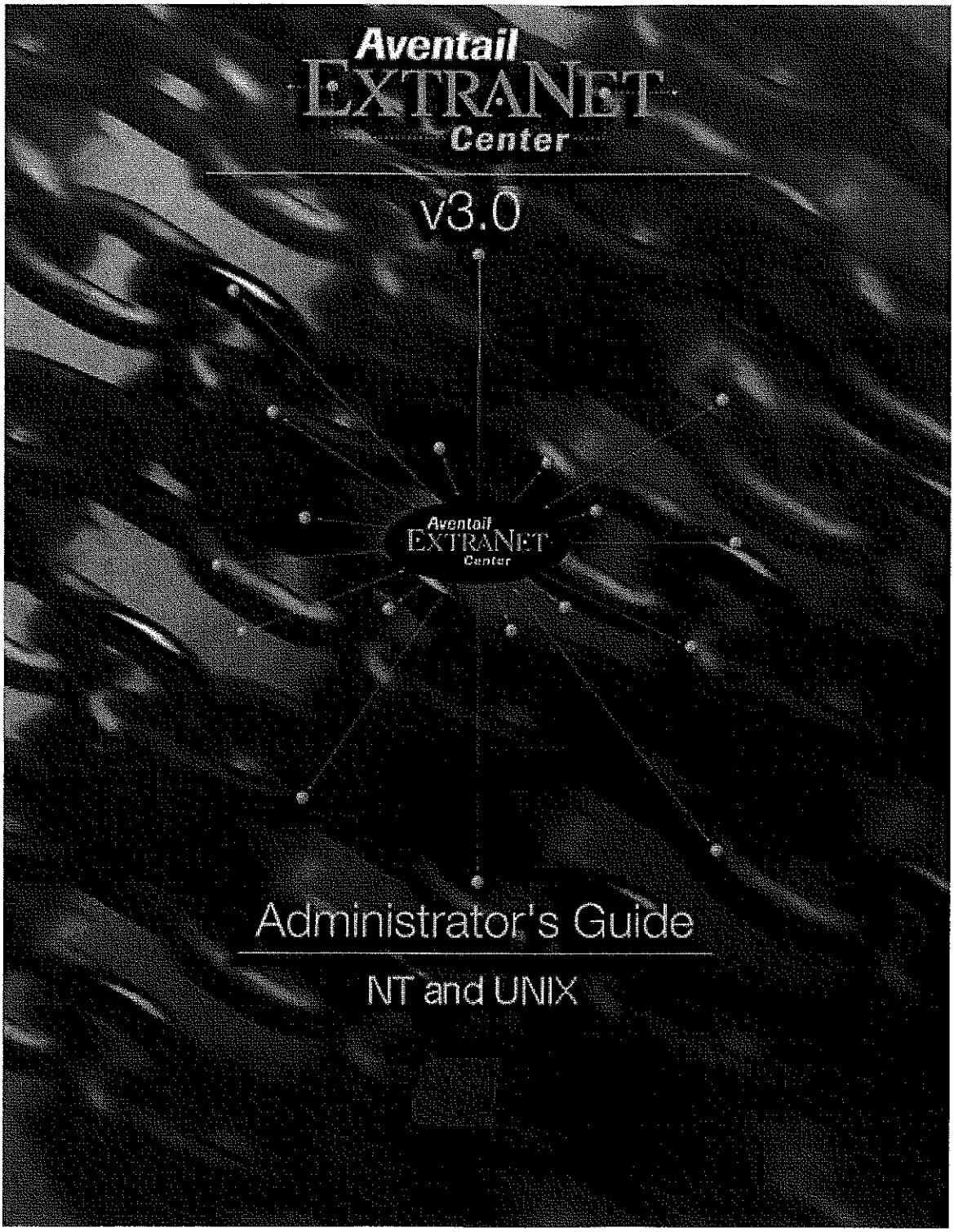


Table of Contents

AVENTAIL EXTRANET CENTER QUICK START GUIDE

POLICY CONSOLE

CONFIGURATION FILE FORMAT

Aventail ExtraNet Server Quick Start Guide

Welcome to the Aventail ExtraNet Server Quick Start Guide.

Aventail ExtraNet Server is the server component of the Aventail ExtraNet Center, a client/server solution for management of sophisticated extranets. Setup of the Aventail ExtraNet Center requires that installation on both a server and multiple client machines. Setup of the Aventail ExtraNet Server consists of installing several components.

AVENTAIL EXTRANET CENTER COMPONENTS

The following are the components of the Aventail ExtraNet Center.

- **Aventail ExtraNet Server:** The primary component of Aventail ExtraNet Center is the ExtraNet Server. This is a SOCKS v5 proxy server that manages the authentication of users and processes all of the connection requests. Aventail ExtraNet Server can manage traffic for both incoming (external users attempting to reach internal network resources) and outgoing (internal users attempting to reach external network resources) network traffic.
- **Aventail Policy Console:** The Aventail Policy Console is the graphical administrative tool for creating, viewing and managing the policies for your extranet. It can also be used for starting and stopping the ExtraNet Server as well as viewing log and license files.

  The Policy Console provides a graphical front-end for the configuration file that the Aventail ExtraNet Server uses. The Policy Console can be run locally on the machine that the ExtraNet Server is installed on or remotely to manage a server that resides on another machine. When the Policy Console is being run remotely, it will establish a secure LAN, WAN or Internet connection via the Management Server (see below). A remote Policy Console running on a Windows NT machine can configure a UNIX Aventail ExtraNet Server and vice versa.
- **Aventail Management Server:** The Aventail Management Server is an optional service that allows administrators to remotely manage an ExtraNet Server. The Management Server and Policy Console communicate via a secure, encrypted connection.

  The Management Server must be installed on the same machine as the ExtraNet Server.
- **Aventail Management Server Config Tool:** The Aventail Management Server Config Tool is the administrative utility that establishes a policy specific to the Management Server. This policy will determine which administrators can manage the ExtraNet Server, how they must authenticate and which network interfaces the server will accept traffic from. The policy also defines the specific directories that can be browsed remotely.
- **Aventail Connect:** Aventail Connect is the client component of the Aventail ExtraNet Center solution.

AVENTAIL EXTRANET SERVER INSTALLATION

The following instructions will get the Aventail ExtraNet Server up and running in a very basic configuration.

Windows NT

The general Aventail ExtraNet Server configuration will require encrypted sessions only and force all users to authenticate against the accounts in the Windows NT Server username/password database. This configuration provides unrestricted access for both outbound and inbound traffic. A sample X.509 certificate is supplied and configured during installation and should be used for non-secure testing purposes only.

Instructions on tightening access controls, configuration as a dual-homed server, obtaining "real" digital certificates, configuring the Aventail Management Server, and changing other parameters may be found in the "Aventail ExtraNet Center Administration Guide" located in the "`\docs`" directory.

1. **Installation:** Run `setup.exe` from the Aventail ExtraNet Center directory of the CD-ROM or run the downloaded distribution file.
2. **License File:** Copy the `aventail.alf` license file into the `C:\Aventail\etc` directory. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Run the Policy Console:** Start | Programs | Aventail ExtraNet Center | Policy Console.
4. **Modify Default Configuration File:** From the Access Control tab, click on the red box to the left of the Action column to change the rule from Deny to Permit. The box color will turn green and the text under the Action column will change to Permit.
5. **Start the Aventail ExtraNet Server**:
   - From Policy Console menu bar, select File | Save.
   - Select Services | Configure.
   - Select "Aventail ExtraNet Server."
   - Click "Start."

UNIX

The general configuration will require encrypted sessions only and force all users to authenticate against the accounts in the UNIX "`/etc/passwd`" file. This configuration provides unrestricted access for both outbound and inbound traffic. A sample X.509 certificate is supplied and configured during installation and should be used for non-secure testing purposes only.

Instructions on tightening access controls, configuration as a dual-homed server, obtaining "real" digital certificates, configuring the Aventail Management Server, and changing other parameters may be found in the "Aventail ExtraNet Center Administrator's Guide" located in the "`/docs`" directory.

1. **Installation:** Run the `install.sh` script from the Aventail ExtraNet Center directory of the CD-ROM or install the downloaded distribution file.

NOTE: *This will install into the default directory,* `/usr/local/aventail`. *If you wish to install into a different location, specify by executing the* `install.sh` *script with the "prefix" switch. For example:*
`install.sh --prefix=/<install directory>/`
where `<install directory>` *is the location to install.*

2. **License File:** Copy the `aventail.alf` license file into the `/etc` directory of the installation root. The default is `/usr/local/aventail/etc`. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Run the Policy Console:** At the command line, type:
   `<install directory>/bin/apc`
4. **Modify Default Configuration:** File From the Access Control tab, click on the red box to the left of the Action column to change the rule from Deny to Permit. The box color will turn green and the text under the Action column will change to Permit.
5. **Start the Aventail ExtraNet Server**:
   - From the Policy Console menu bar, select File I Save.
   - Select Services I Configure.
   - Select "Aventail ExtraNet Server."
   - Click "Start."

   - OR -

   From the command line, type:

   `<install directory>/bin/socks5`

   `-s for log to stderr -p <port>` for port values other than 1080

CLIENT INSTALLATION

These installation steps will get the client component of Aventail ExtraNet Center, Aventail Connect, up and running in a basic configuration. Instructions covering advanced configuration options, public certificates, and troubleshooting may be found in the "Aventail Connect Administrator's Guide" and in the online Help.

NOTE: *Leave all settings not described below as DEFAULTS.*

1. **Installation:** Run `setup.exe` from the Aventail Connect directory of the CD-ROM or run the downloaded distribution file.
2. **License File:** Copy the `aventail.alf` license file into the `C:\Program Files\Aventail\Connect` directory. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Create a Configuration File**:
   - Select Programs I Aventail Connect I Configuration Tool.
   - Select File I New.

4. **Add Server Definition**:
   - From the Servers tab, click Add.
   - Type in Alias name ="Aventail ExtraNet Server."
   - Hostname or IP address = public DNS hostname or IP address of machine with Aventail ExtraNet Server installed and running. This host must be reachable by TCP/IP (i.e., ping test).
   - Click OK.
5. **Define Destinations**:
   - From the Destinations tab, click Add.
   - Type in Alias name = "Private Network."
   - Select "Network."
   - Domain Name = <internal DNS Domain name for private network>.
   - Select "Subnet."
   - Enter network IP Address/Subnet mask.
   - Click OK.
6. **Specify Redirection Rules**:
   - From the Redirection Rules tab, click Add.
   - Select Destination "Private Network."
   - Select Redirect via "Aventail ExtraNet Server."
   - Click OK.
   - Click Add.
   - Select Destination "Everything Else."
   - Do not Redirect.
   - Click OK.
7. **Save Client Configuration File**:
   - From the Config Tool menu bar, select File | Save.
   - Type `aventail.cfg`.
   - Click OK.
   - Select File | Select Make Active.
   - Select File.
   - Select Exit.
8. **Start Aventail Connect**:
   - Start | Programs | Aventail Connect | Connect.
   - Point to new configuration file `aventail.cfg`.
   - Select OK.

- Start any TCP application to initiate the connection. The ExtraNet Server or other SOCKS proxy server must be running.

Essential Concepts for Aventail ExtraNet Server Policies

It is important to understand the primary components of the Aventail Policy Manager that are used to build an extranet policy. There are four types of rules that can be used to build an Aventail ExtraNet Server policy:

Access Control Rules

Access control rules define the network resources and services that are accessible to users and groups based on where they are coming from, what day or time it is, how they authenticated, and what their encryption strength is.

The following are the parameters that make up an access control rule:

- **Active/Inactive:** Temporarily disables a rule without having to delete it.
- **Permit/Deny:** Defines whether the rule will permit or deny access based on the criteria selected.
- **Source Networks:** Defines the originating source of the connection for the rule to be applicable.
- **Source Ports:** Defines the originating ports (services) of the connection for the rule to be applicable.
- **Destination Networks:** Defines which network resource(s) the rule will permit or deny access to.
- **Destination Ports:** Defines which services on the Destination Networks can be used by the rule.
- **Users and Groups:** Defines which users and groups the rule applies to.
- **Times:** Defines the times or days the rule is active.
- **Authentication Matching:** Defines the authentication methods to be used for the rule to be applicable.
- **Key Length:** Specifies the encryption strength required for the rule to be applicable.
- **Commands:** Defines the commands that can be used on the specified Destination Networks.

Authentication Rules

Authentication rules define the authentication options available to users or groups based on where they are coming from.

The following are the parameters that make up an authentication rule:

- **Source Networks:** Defines the originating source of the connection for the rule to be applicable.
- **Authentication:** Defines the authentication methods available.

Filter Rules

Filters can be applied to network traffic based on the same parameters as an access control rule. This means that you can apply filters on a very granular level, such as only apply them to specific users, traffic between two locations, or during certain times.

- **Filter Type:** Defines which of the loaded (and configured) filters should be used for the rule.
- All other components used for access control rules except permit and deny.

Proxy Chaining Rules

Defines the methods for accessing network destinations located behind other ExtraNet Servers.

- **Destination Networks:** Specifies which network resources the rule will permit or deny access to.
- **Proxy Server:** Specifies the IP address or hostname of the ExtraNet Server that secures the intended network destination.

NOTE: *In order to use proxy chaining, server-to-server authentication methods must be loaded first. Please reference the Aventail ExtraNet Center Administrator's Guide for more information.*

Objects Used to Build Aventail ExtraNet Server Policies

- **Groups:** These can be made up from six different types of user databases: Windows NT, Novell NDS, UNIX passwd, Host, SSL User (X.509), and Single User. Only SSL Users and Single Users can be created and deleted by the administrator. Administrators can select any combination of these six types of users and groups and apply them to rules. Administrators can also select any combination of users and groups and place them in a folder for easy re-use in multiple rules.
- **Source or Destination Networks and Ports:** Network resources can be a host, domain, IP range or subnet. Administrators can select any combination of network resources they have created to use in rules. Administrators can also select any combination of network resources and place them in a folder for easy re-use in multiple rules. Combinations of single ports and port ranges can be applied to source and destination networks to restrict the available services a user can access.
- **Time:** Days of the week and hours during those days or date range for which a rule is applicable.
- **Authentication method:** Available methods include SSL which can use any of the following methods to sub-authenticate users. These methods can also be used individually but will not provide encryption unless used with SSL for sub-authentication. Client certificates can be used in conjunction as well.
  - Username/Password back-ended to Windows NT, NetWare bindery/ NDS, RADIUS, File, Crypt file, UNIX passwd file.

  - CRAM back-ended to RADIUS or ACE/Server.
  - CHAP back-ended to RADIUS or file.
- **Key length requirements:** Can be set to any, 40-bit or higher, 56-bit or higher, or 128-bit or higher.
- **Filters:** Available filters include an HTTP filter and an authentication forwarder filter.
- **Commands:** Available commands include any, traceroute, ping, UDP, connect and bind

Policy Console

Introduction

The Aventail Policy Console is the graphical administrative tool for creating, viewing, and managing the policies for your extranet. You can also use the Policy Console to start and stop the Aventail ExtraNet Server, or to view log files and license files. The Policy Console provides a graphical front-end for the configuration file that the Aventail ExtraNet Server uses to handle connection requests. There are no major differences between the Windows NT and UNIX Policy Consoles.

The first section of this chapter covers the server settings. These are server-level settings that specify, among other settings, which port to run on, logging, and starting and stopping the Aventail ExtraNet Server. The next section covers the policy part of the server. These various rules consist of access-control rules, authentication rules, filter rules, proxy-chaining rules, and network rules. The Policy Console Tools are covered at the end of this chapter.

For more information on using the Policy Console to manage a remote Aventail ExtraNet Server, refer to the "Management Server" chapter.

Running the Policy Console

On Windows NT:

Start | Programs | Aventail ExtraNet Center | Policy Console

On UNIX:

At the command line, type `<install directory>/bin/apc`

Server Settings

(Add some introductory content here)

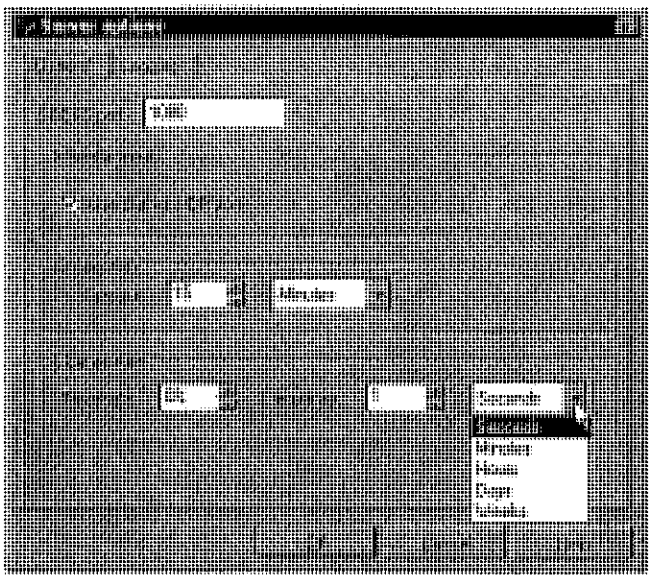
SERVER OPTIONS

(Add some introductory content here)

General

The Aventail ExtraNet Server requires fundamental licensing and connection information prior to a specific network configuration: how to handle UDP, connection timeouts, concurrent connections, etc.

To open the Server options dialog box, at the Policy Console menu select View | Server Options.



SOCKS PORT

This is the port on which the server wil listen for incoming connections. The default is 1080.

USE THE CLIENT'S UDP PORT

Checking this enables support for unknown UDP connections. If enabled, the Aventail ExtraNet Server relays packets from hosts to which it has not previously sent data.

SETTING THE CONNECTION TIMEOUT

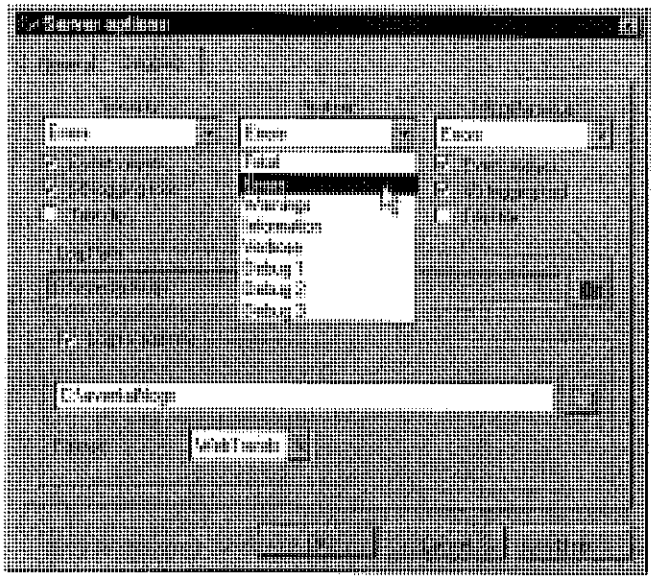
Controls the duration of client connections. If there is no activity after a specified period, the client connection will timeout. You can establish a timeout interval of seconds to weeks.

CONFIGURING THE LICENSE ALERT

The license alert will create logging information at predetermined intervals that you are at "X" percentage of your license limit. For example, if you have an Aventail license for 1,000 users and you establish a threshold of 80%, alerts will be sent to your logging at the intervals you determine every time concurrent connections exceed 800.

Logging and Auditing

Logging is an essential part of diagnosing and maintaining server function. With logging you can track user activity, diagnose failed connections, repair system failures, and configure the logging output for Aventail or WebTrends formats.



LOGGING

You can select one of three logging methods, one of eight levels of information, and three output options.

LOG METHODS

- Security- Security information will consist of failed authentication attempts and methods. Select the logging level from the drop-down menu and check the desired output option. The default filename is security.log.
- System- System information will point out network problems as they affect the Aventail ExtraNet Server; i.e., low memory, timing out, a SOCKS server crashing, etc. Select the logging level from the drop-down menu and check the desired output option. The default filename is system.log.
- Miscellaneous- Miscellaneous information will consist of everything else not covered by the two prior methods. Select the logging level from the drop-down menu and check the desired output option. The default filename is misc.log.

LOG LEVELS

NOTE: *Processing large amount of information may impact the server's performance for brief periods of time.*

- Fatal- Fatal error information only.
- Error- Critical error information only.
- Warning- Non-critical warning information, as well as Error level information.
- Information- Detailed logging information, including all previous level data.
- Verbose- All previous level data, but less data than Debug 1.

- Debug 1, Debug 2, and Debug 3- Debugging programs of increasing debug information. This can be a large amount of data, and should be used only when troubleshooting.

OUTPUT OPTIONS

- Event Viewer- Logging information will output to the Windows NT Event Viewer's Application Log. Note that the server will always log startup information to the Event Viewer, regardless of settings at the Logging tab.
- (S5) Logging Tool (Windows only)- The (S5) Logging Tool is the dynamic logging tool for all (Windows) Aventail ExtraNet Server activity. Start the (S5) Logging Tool via the Tools I Logging Tool menu of the Policy Console.
- Plain-text file- Aventail ExtraNet Server activity information will output to the default logging file, server.log in the Aventail ExtraNet Server installation directory

AUDITING

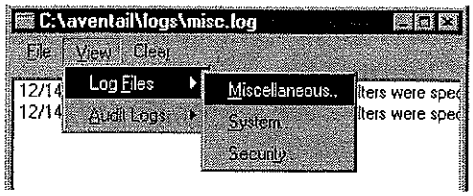
Enabling this option will direct exportable logging information to the audit log.

OUTPUT FORMATS

- Aventail- outputs information into the Aventail format.
- Webtrends- Outputs audit log information in the Webtrends format. For more information on Webtrends, contact http://www.webtrends.com.

Tips: - To debug the server, use the (S5) Logging Tool (Windows only), and set the Debug level to 3.
- For normal operations, either log to the system log, or log to file.
-To archive traffic through the server, and process reports on it, use the audit log. There are maximum no log settings. However, logging at one of the Debug levels could exhaust server memory.

LOG VIEWER



NOTE: *At the Policy Console menu, select View I Server Options...to configure the level of information the server will generate for Log files.*

Opening the Log Viewer

Via the ViewlLog Files... menu command on the Policy Console, you can view the Miscellaneous, System and Security Log files, and the Error, Accounting and Security Audit logs.

NOTE: *Select ViewlServer Options...lLogging tab to configure the level of information the server will generate for Log files.*

CLEARING LOG AND AUDIT FILES

You can clear the logging or auditing information from a selected file, whether you are viewing it or not. At the Log Viewer, select and:

- the type of log or audit file,
- Current (the file you are viewing), or
- All (files).

RELOADING LOG AND AUDIT FILES

At the Log Viewer, for any log or audit file you are viewing, you can refresh the window with the latest information the server generates for that specific log. You can do this in one of three ways:

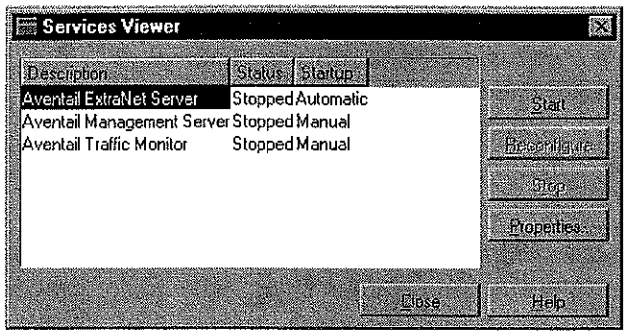
- By cursor, select File I Reload at the Log Viewer menu,
- by the keystroke, Ctrl+R, or
- by clicking the Reload button at the bottom of the Log Viewer.

NOTE: *More than one Log Viewer can be opened at one time.*

CONFIGURING SERVICES

The Aventail ExtraNet Server has three services (ExtraNet Server, Management Server, and Traffic Monitor) that you can start, stop, and reconfigure. The difference between Start/Stop and Reconfigure is that reconfiguration refreshes your configuration file "on the fly" without having to stop and restart server connections.

This means existing client connections will not be lost and will continue to use the old policy. New incoming connections will use the new policy.



NOTE: *You cannot stop the Management Server remotely.*

Configuring server services

Select Services | Configure... from the Policy Console menu to display the Services Viewer. The Services Viewer displays available services, whether they are running or not, and the buttons for managing the services.

Viewing available services

The window of the Services Viewer contains the description (name) of the service, it status, and its startup configuration (whether automatic, manual or disabled). You can adjust the column width of the Description-Status-Startup bar by dragging the separator bars to the desired width.

Starting a service

Select the service in the Services Viewer and click **Start**.

Changing startup properties

To configure a service to start automatically or manually, or to disable it, select that service in the Service Viewer and click **Properties**. The Properties dialog box will appear. Select one of the three options and click **OK**.

NOTE: *If you want to run the (S5) Logging Tool, you must check the "Interact with desktop" box at the Properties dialog box*

Reconfiguring a service

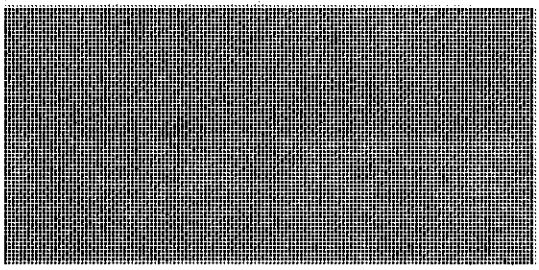
If you've made modifications to your configuration file but are actively using the Aventail ExtraNet Server, you can refresh the configuration file by clicking **Reconfigure**, and the server will use the new configuration file for all new incoming connections, but continue to use the old one for existing connections.

Viewing server status

Select Services I Status from the Policy Console menu to view the activity status of the Aventail ExtraNet Server, Management Server, and Traffic Monitor.

CONNECT TO REMOTE

With proper configuration, the Management Server can establish a connection with another Host, domain, or subnetwork.



Connecting to a remote server

Click Connect on the Policy Console; the Establish Remote Connection dialog box appears. Two text boxes on the dialog box, Host and Port, let you specify the remote server to which you want to connect.

- Host -- enter the IP or host name of the remote ExtraNet
- Port -- enter port on which the Management server is listed. The default port is 2080

After the connection is established the Policy Console is automatically populated with the remote server configuration file. The name of the remote server appears in the titlebar of the Policy console. Browsing in the remote Files, Users, and Groups can now be accomplished from your Policy Console.

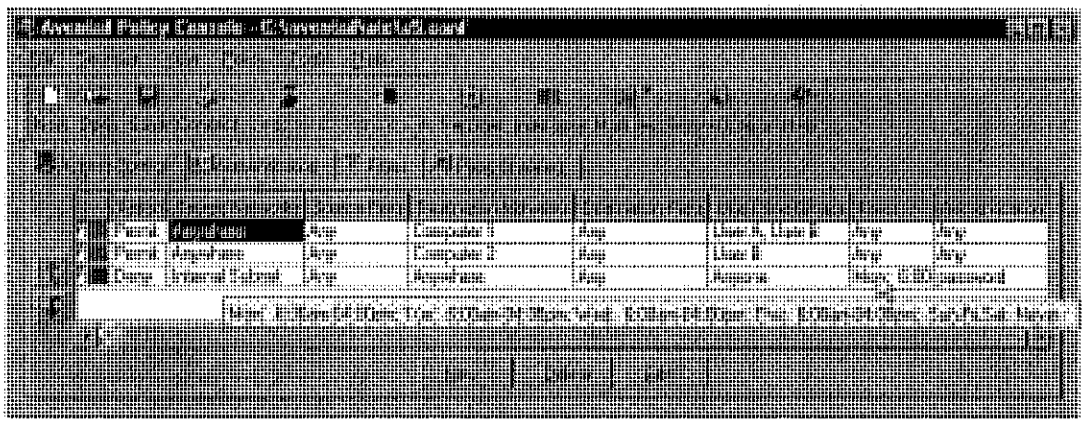
To end the remote browsing session, click Disconnect on the Policy Console.

Access Control

Access Control rules determine which people and groups can access what machines and services based on where they came from, the time of day, how they authenticated, and encryption strength, etc.

Access Control Tab

The Access Control tab is where you define the rules for specifying which people and groups can access what machines and services. Rule elements include: where they came from, the time of day, how they authenticated, and encryption strength, etc. Rules for machine and services appear on the Access Control tab as row in a grid.



Column headings (definitions)

When you create an access control rule, by either adding or editing, the information appears beneath the column headings of that rule.

How to adjust column width and display cell contents

- To adjust the width of the columns, click on the separator bar between column headings (the cursor will change to arrows), and drag the separator bar, left or right, to the desired width.
- To view the contents of a cell populated with information that runs beyond the cell width, place your cursor in the cell and a ToolTip will display all configured properties for that cell.

You create access control rules with the Access Control Builder. Every access control rule is populated by rule elements located under each column on the grid of the Access Control tab. The server checks client access requests against the access control rules, starting with rule #1, and continues down the list seeking a match between the request and the access requirements of each rule. It does this by comparing any combinations of rule elements. At the first instance of a match, the server stops searching and permits (or denies) access to the client. For this reason you must be sure to create a logical flow to your access rules, from the top down. This is known as rule order.

Changing rule order

- To establish the order of a rule, select the entire rule or a cell of that rule. Use the up/down arrows located on the left side of the Access Control tab to move the rule to its new position in rule order.
  -OR-
- Right-click a selected cell of the rule you want to reorder, and select the "move up" or "move down" arrow commands from the shortcut menu.

Adding rules

- On the Access Control tab, click **New...**
  -OR-
- Right-click anywhere in the white area of the Access Control tab grid and select **New...** from the shortcut menu
  -OR-
- Double-click anywhere in the white area of the Access Control tab grid. Any of these actions will open the Access Control Builder.

Editing rules

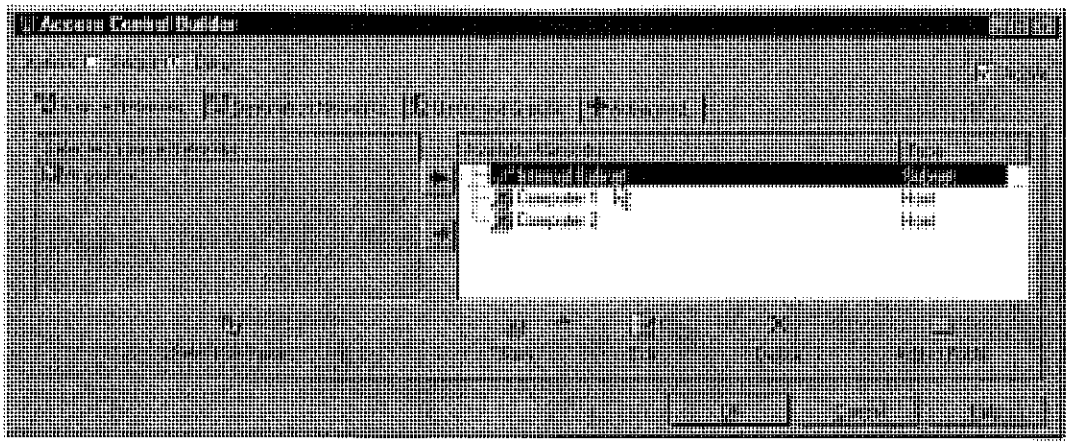
- On the Access Control tab, select the cell in a rule that you want to modify, and click **Edit...**
  -OR-
- Select the cell in a rule that you want to modify, right-click and select **Edit...** from the shortcut menu.
  -OR-
- Double-click any cell of a rule.
  Any of these actions will open the Access Control Builder at the appropriate tab for the selected cell, with the rule number of the selected cell displayed in the title bar.

Deleting rules

- On the Access Control tab, select the entire rule or any cell in that rule. Click **Delete**,
  -OR-
- Right-click the selected rule or cell, and select **Delete** from the shortcut menu.

ACCESS CONTROL BUILDER

The Access Control Builder gives you access to all the tools necessary to build your access rules: Source and destination networks, users and groups, time-based access limits, authentication matching, key length requirements, commands, etc.



Creating access control rules

Click the appropriate tab on the Access Control Builder to configure that part of the new rule you are creating or existing rule you want to edit:

- Source Networks -- This is where you create or identify your source network for this rule, as well as assign services (ports).
- Destination Networks -- This is where you create or identify your destination network for this rule, and assign services (ports).
- Users and Groups -- You can select a user or group from the Available Users pane or create a new user or group.
- Advanced -- It is at the Advanced tab that you can configure time constraints for the rule, select loaded authentication methods for the rule, require specific key lengths or none, and/or assign network commands (traceroute, ping, UDP, etc.) to the rule.

Assigning a "permit" or "deny" status to a rule

As you create a rule, select either Action: option before you click **OK**. If you select Permit, the server evaluates the rule according to the rule order and offers it to client requests for access to that specific network. If you select deny, the server will evaluate the rule, but not offer it to client requests. You can also assign a permit or deny status to the rule at any time via the Policy Console.

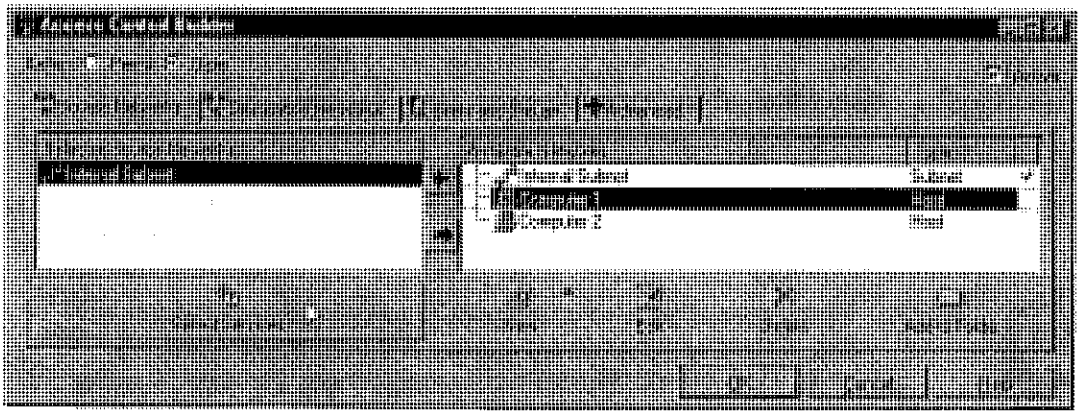
Making a rule active or inactive

Check the Active: box to make the access control rule active, if it is not. This puts the rule in the rule order queue for server evaluation. If you make the rule inactive, the server will

not evaluate the rule or offer it to client requests. You can also make the rule active or inactive at any time via the Policy Console.

Source networks

For your Extranet, traffic starts from a source and travels to a destination, either on the same network, or another network, by way of address protocols. Any host machine on any network has a unique address and can send and receive message traffic, hence it can be both a source and a destination. However, when you need to control message traffic, you must identify source networks and determine where you will allow their message traffic to go. For example, your company (ABC, Inc.) has a relationship with a development team at an XYZ, Inc. office, and all members (groups and users) of that team need to communicate with all members of the product development team from your company. You can assign authentication attributes to the network, create a folder, add the XYZ network to the folder, and select that folder as an active, source network. Once you select the XYZ network as a source network, you can then refine the access rights of anyone coming from that network, e.g., by limiting access to only a specific destination network (Destination Networks tab), during certain times of the day (Advanced tab I Time Editor).



AVAILABLE NETWORKS

The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. You must move the network object to the Selected Source Networks pane to make it a part of an access control rule.

The checkbox located above the right pane indicates whether the access control rule for the selected network is active or disabled.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

SELECTED SOURCE NETWORKS

In order to add a source network object to an access control rule (or filter rule), you must move network objects from the right pane into the left pane. The network objects then become Selected Source Networks.

NOTE: *A check mark appears in the Available pane to the right of objects and/or folders to indicate they are active in the Selected pane.*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available Networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Source Networks pane, the Select Services and New tools remain functional, but the Edit, Delete and Add to Folder tools become unusable.

CREATING A NEW (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

- To add a network object to an Available Networks pane, either right-click anywhere in the Policy Console window and select New... from the shortcut menu,
  -OR-
  click **New...**at the Policy Console, then click **New...** in the Access Control Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**. You may also enter Optional Information.

NOTE: *If you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders allow you to group similar network objects under a common name. You can create folders in the Available Networks pane, into or out of which you can move selected networks and groups (only while that folder is in the Available Networks pane). To make that folder an active source network, move it from the Available Networks pane to the Selected Source networks pane, using the arrows, or you can also double-click the network object (folder) to move it back and forth, from one pane to another.

ADDING OBJECTS TO A FOLDER

To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Access Control Builder and select **Add**

to from the shortcut menu-OR-Select the objects and click the **Add to Folder** tool. This will open the **Add to Folder** dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the Shift key down as you click the first and last objects of a continuous list, or by holding the Control key to select individual, non-adjacent objects.*

EDITING A SOURCE NETWORK/OBJECT

Right-click a cell under the Source Network column on the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. Either action will open the Access Control Builder at the Source Networks tab. Select the network object you want to edit from the Available pane . Then click the Edit tool on the Access Control Rule. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to the Source Network is global.

DELETING A SOURCE NETWORK/OBJECT

To delete a source network object from an access control rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the access control rules that will be disabled due to the security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

ADDING OR EDITING SERVICES (PORTS)

- You can only add or edit ports for networks or network objects in the Selected Source networks pane. Right-click an object in that pane and select Edit Services from the shortcut menu,
  -OR-
- Select the object in that pane and click Select Services. Either action will open the Selected Services dialog box where you can add or edit network services (ports) to your selected network object.

NOTE: *By allowing only selected services you will restrict the port on which that the client can make the initial access request.*

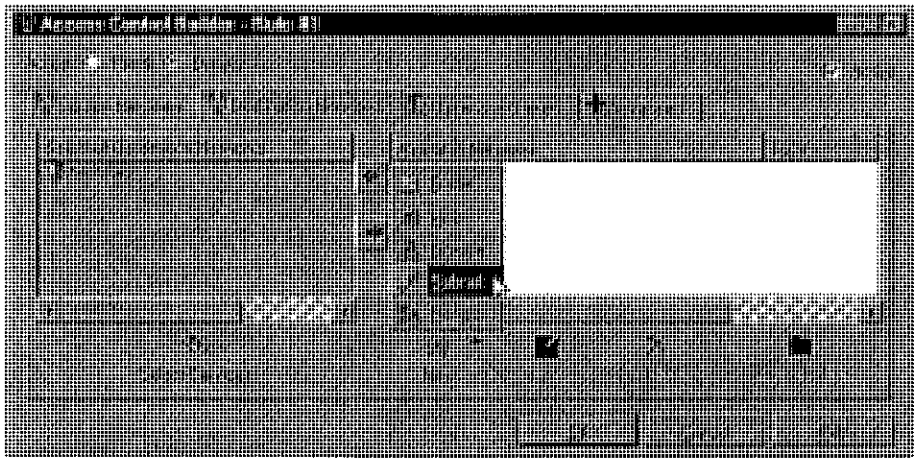
Destination networks

On an extranet, message traffic starts from a source and travels to a destination, either on the same network, or another network, by way of address protocols. Any host machine on any network has a unique address and can send and receive message traffic, hence it can be both a source and a destination. However, when you need to control message traffic, you must identify destination networks to direct message traffic. For example, your company (ABC, Inc.) has a relationship with a development team at an XYZ, Inc. office, and all members of that team need to communicate with all members of the product development team from your company. You can configure your network with authentication to match theirs. Once you add the XYZ network as a destination network,

you can then refine the access rights of anyone going to that network, e.g., limiting access to a destination network during certain times of the day. In doing so, you create an access control rule with the Destination Network information as an integral part of that rule.

AVAILABLE NETWORKS

You can create and edit network objects only in the Available Networks pane.To access the Destination Networks tab, at the Policy Console select a cell under the Destination Networks column and double-click, or click **New...** or **Edit...**. Any of these actions will open the Access Control Builder at the Destination Networks tab.



The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. You must move the network object to the Selected Destination Networks pane to make it a part of an access control rule. The checkbox located above the right pane indicates whether the access control rule for the selected network is active or disabled.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

SELECTED DESTINATION NETWORKS

In order to add a destination network object to an access control, filter, or proxy servers rule, you must move network objects from the right pane into

the left pane. The network objects then become Selected Destination Networks.

NOTE: *A check mark appears in the Available pane directly to the right of objects and/or folders to indicate they are active in the Selected pane.*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Destination networks pane, the Select Services and New tools remain functional, but the Edit, Delete and Add to Folder tools become unusable.

CREATING A NEW... (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

- To add a network object to an Available Networks pane, either right-click anywhere in the Policy Console window and select **New...** from the shortcut menu,
  -OR-
- click **New...**at the Policy Console, then click **New...** in the Access Control Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**.

You may also enter Optional Information.

NOTE: *If you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders are a convenience that allow you to group similar network objects under a common name. You can create folders (which function like aliases) to appear in the Available Networks pane, into or out of which you can move selected networks (only while that folder is in the Available Networks pane). To make that folder an active destination network, move it from the Available Networks pane to the Selected Destination Networks pane, using the arrows, or you can double-click the network object (folder) to move it back and forth, from one pane to another.

ADDING OBJECTS TO A FOLDER

- To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Access Control Builder and select Add to from the shortcut menu
  -OR-

- Select the objects and click the Add to Folder tool. This will open the Add to Folder dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the SHIFT key down as you click the first and last objects of a continuous list, or by holding the CONTROL key to select individual, non-continuous objects.*

EDITING A NETWORK/OBJECT

Either right-click a cell under the Destination Networks column on the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. The Access Control Builder will appear. Select from the Available Networks pane the network object you want to edit. Then click the Edit tool on the Access Control Builder. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to that Destination Network is global.

DELETING A DESTINATION NETWORK/OBJECT

To delete a destination network object from an access control rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the rules that will be disabled due to security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

ADDING AND/OR EDITING SERVICES (PORTS)

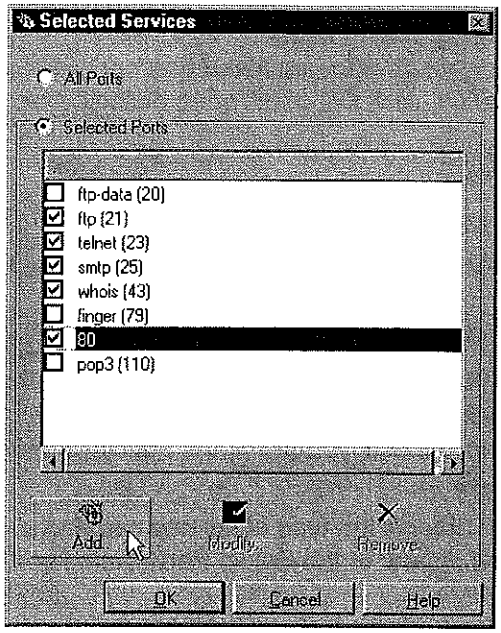
- You can only add or edit network services (ports) to network objects in the Selected Destination Networks pane. Right-click an object in that pane and select Edit Services from the shortcut menu
  -OR-
- Select the object in that pane and click Select Services. Either action will open the Selected Services dialog box where you can add or edit network services (ports) to your selected network object.

SERVICES (PORTS)

The port number is an identifier for the type of service that runs on that network; e.g. e-mailers send and receive on port 25 (the SMTP port), Web servers send and receive on port 80 (the HTTP port), and telnet is on port 23. On the Aventail ExtraNet Server, you can assign any number to any service on a network. However, the industry standard is for servers to use the commonly accepted port numbers (up to 1024) for specific services.

SELECTED PORTS

By allowing only selected services you will restrict the services that the clients can access on the destination machine.



DEFAULT CONFIGURATION

Prior to configuring your ports, the Aventail ExtraNet Server's default will be to allow any (all) ports for an access control rule. The Selected Services dialog box will present eight commonly used services/ports when you initially open it. You may add or delete ports via the Add/Modify Ports dialog box to build a suite of your most commonly used ports.

ADDING A SERVICE (PORT)

To add a service (port) to a rule:

1. In the Policy Console, double-click the Access Control rule that contains the network to which you want to add a port, then click Select Services at the bottom of the Selected pane,
   -OR-
   Click Add
2. Select the source or destination network to which you want to add a port. Make certain the network is in the Selected pane.
3. Click the Edit Ports tool.
4. Choose either the All Ports or Selected Ports option on the Select Ports dialog box. If you choose Selected Ports check the port number you want to assign to the network,
   -OR-
   If you choose Selected Ports, click the Add tool at the bottom of the Select Ports dialog box, and the Add Port dialog box will appear. You have the option of selecting a port name (service) from the Port: list box, or entering a from-to port range.
5. After entering your information, click **OK** on all open dialogs until you return to the Policy Console.

EDITING A PORT

1. To modify a port, follow steps 1 and 2 from above.
2. Select **Edit...**. The Edit Ports dialog box appears.
   The selected port number or port range appears in the appropriate boxes.
3. After entering your new information, click **OK** on all open dialog boxes until you return to the Policy Console.

DELETING A PORT

To delete a port from your suite of commonly used ports:

1. Select that port in the Select Ports dialog box, and click Delete (at the bottom of the Select Ports dialog box).
2. Click **OK** on the successive windows until you are at the Policy Console.

To simply remove the port from its access control rule without removing the port:

1. Clear the check box in the Select Ports dialog box.
2. Click **OK** on the successive windows until you are at the Policy Console.

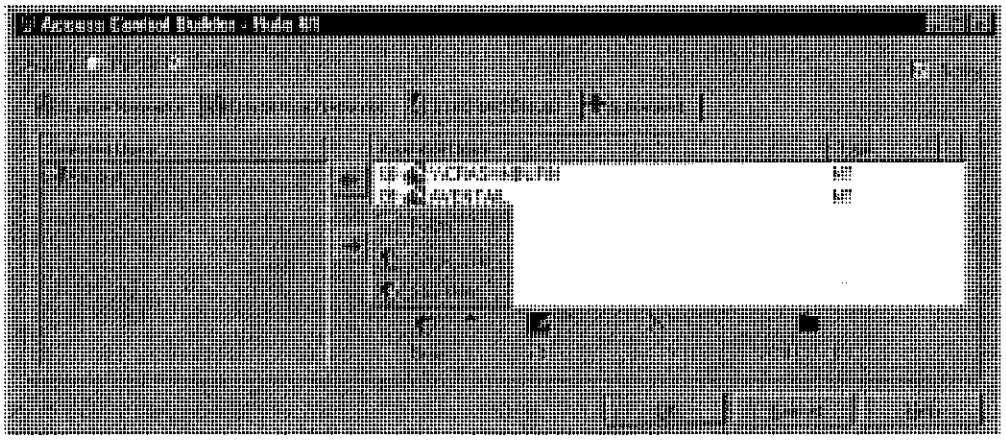
WHAT SERVICES ARE ON WHICH PORTS

When the Aventail ExtraNet Server detects the type of service carrying a client request, the service name will appear in the Select Ports dialog box.

NOTE: *The Port: list box in the Add/Modify dialog box will list the suite of ports available on your machine.*

Users and Groups

The Aventail ExtraNet Server will automatically populate the Policy Console with available (browseable) NT and NDS users and groups, as well as UNIX populations, depending on your network setups. You can add non-browseable users and edit these users. You cannot manually add groups.



You can add new single users, new SSL users, and folders. You can create these entities only in the Available Users pane of the Users and Groups tab. To add these entities to an access control rule, you must move them to the Selected pane.

ADDING USERS OR GROUPS

To add a single or SSL user, from the Access Control tab, either:

1. At the Policy console, select a cell in the Users and Groups column and double-click to open the Access Control Builder
   -OR-
   Click **Add....**
   The Users and Groups tab will appear as the active tab. The Available Users pane displays your NT, NDS and UNIX (depending on your platforms) users and groups.
2. Select New | SSL, Single User, or Folder.

EDITING USERS OR GROUPS

NOTE: *You can only edit users that you manually create.*

At the Users and Groups tab, select the entity you want to modify In the Available Users pane, and either

- Right-click and select **Edit...** from the shortcut menu,
  -OR-
- Click Edit.

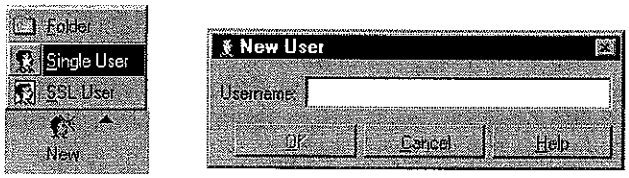
Either action will open the New User dialog box where you can enter your changes. When you finish entering your changes, click **OK**. Your changes now appear in the Available Users pane. To make those changes active in an access control rule, move the entity to the Selected pane and click **OK**.

REMOVING USERS OR GROUPS

Select the entity you want to remove (delete) in the Available Users pane, and click Delete or right-click and select Delete from the shortcut menu. Depending on your User and Groups setup, a Delete Confirmation dialog box will open stating that the user or group will be deleted from the "following rules" or that specific rules will be deactivated due to security risks. Click **OK**. The Delete Confirmation dialog closes. Then click **OK** at the Access Control Builder.

SINGLE USER

The Aventail ExtraNet Server will automatically populate the Policy Console with available (browseable) NT and NDS users and groups, as well as UNIX populations, depending on your network setups. You can add single users (non-browseable; i.e., RADIUS, text file), and edit or delete them.



ADDING A SINGLE USER

To add a new, single user,

1. click **Add...** at the bottom of the Policy Console

-OR-

Double-click an access control rule in the Users and Groups column.The Access Control Builder will appear with the Users and Groups tab active.

2. Select New I Single User in the toolbar,

-OR-

Right-click the white space in the Available Users pane and select New I Single User from the shortcut menu. The New User dialog box appears.

3. Enter the appropriate information and click **OK**. The new user appears in the "plain" directory in the Available Users and Groups pane of the Access Control Rule.To add the new user to a rule, you must move the new user to the Selected Users pane.

DELETING A SINGLE USER

To delete a single user, make certain the single user's name shows in the Available Users and Groups pane of the Access Control Builder, select it, and click Delete in the toolbar. The Delete Confirmation dialog box will open, with the rule number and type of rule displaying in the dialog window. It warns you that either,

- the rule(s) affected by the deletion will be deactivated because of a security risk

  -OR-

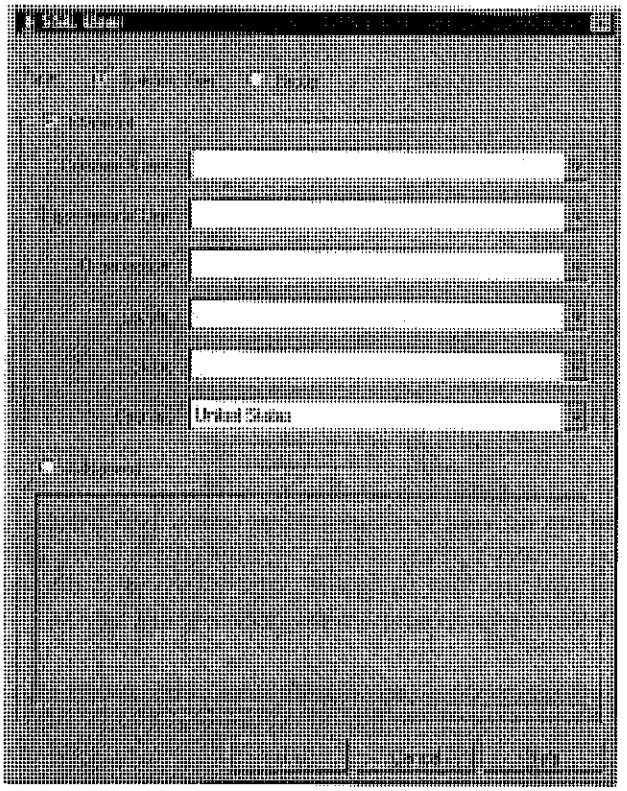
- it will notify you of all the rules affected by deleting the single user.

Click **OK**. If the deletion will cause a security risk, the check mark at the beginning of that rule on the Policy Console/Access Control tab will disappear, as will the check mark in the upper right-hand corner of the Access Control Builder. The ACL rule will be unavailable to the server until you reactivate it. Whether or not the deletion causes a security warning, that single user will no longer appear in the Available Users pane.

SSL USER

You can organize and maintain certificate information (RFC 1485) for users and groups via the SSL User dialog. How you organize that information depends on your certificate format, information, and the number of users requiring certificates. Once you enter certificate information into the SSL User dialog box, you can add the SSL user to Available users and groups

To organize standard or advanced SSL certificate information by specific users or by groups, click New at the Users and Groups tab and select SSL User, or right-click in the Available pane at the users and Groups tab and select New I SSL User from the shortcut menu.



You can enter distinguished name information through either the Standard or Advanced sections of the SSL User dialogs.

ENTERING STANDARD CERTIFICATE INFORMATION

You must type appropriate certificate information into each text box. The text boxes will populate as you add information for successive SSL users. This will allow you to use the "pull-down" features of the text boxes.

ENTERING ADVANCED CERTIFICATE INFORMATION

You can cut distinguished name information from a certificate via a text viewer, and paste it into the Advanced window of the SSL User dialog.

ENTERING OPTIONAL INFORMATION

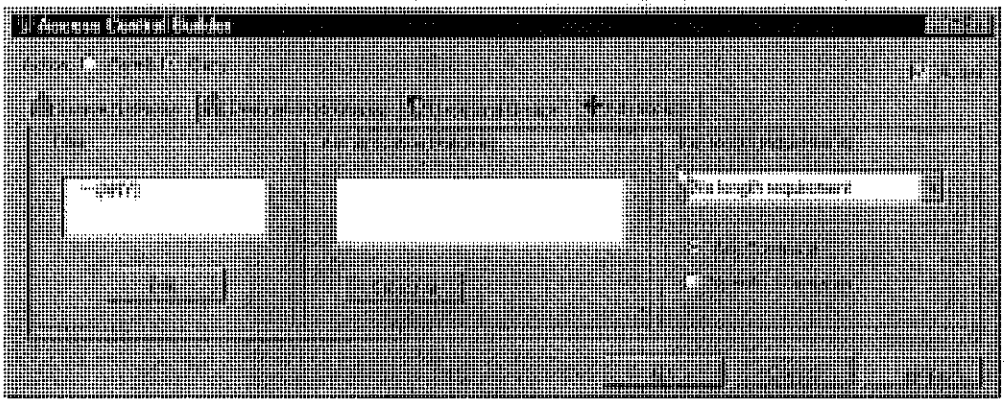
If you enter an optional name, it will appear in the Available pane on the Users and Groups tab after you click **OK** to close the SSL User dialog box. Otherwise, the distinguished name will appear in the SSL User tree.

Advanced

You can access the Advanced tab via the Access Control Builder and Filter Builder. On the Advanced tab, you can:

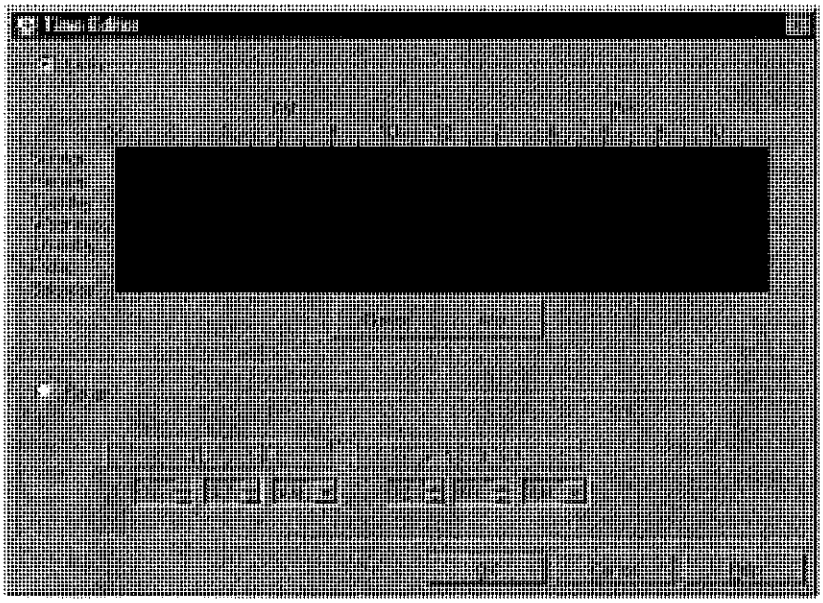
- add time-based restrictions to access rules,
- match authentication between client and server,
- establish a required key length for client access,

- and configure the network commands for the Aventail ExtraNet Server.



TIME ATTRIBUTES

In addition to controlling access by destinations, users and groups, and authentication, you can also control access by days of the week and hours of the day. This means you can limit people to coming in only during business hours, or, limit a contractor to coming for only a two-week period.



TIME EDITOR

You modify the default time-based rule of "Any" via the Time Editor. To do that, select the Access Control Rule | Advanced tab. You will see the default configuration Any in the Time pane of the Advanced tab. To change that configuration, select Edit on the Advanced tab and the Time Editor appears. The Time Editor will display the Shifts (24-hour/7-day) grid as completely blue.

- To completely limit access by time-based rules, click Never. The 24-hour/7-day grid clears to grey.
  -OR-
- Select (either or both?) the Shift or Range options on the Time Editor to configure a limited, time-based rule.

CONFIGURING SHIFTS

1. Click on any number of squares in the 24/7 grid to designate access hours and day(s),
   -OR-
   Click and drag your cursor to include start/end access times from a specific start day to end day of the week.
2. Click **OK** on the Time Editor and the access days/hours appear in the Time window of the Advanced tab.
3. Click **OK** and the days/hours appear on the Policy Console in the Times cell of the rule to which you applied time-access constraints.

Range

1.Upon selecting the Range option on the Time Editor, the 24/7 grid clears to grey.

2. Click the starting date button (left side) and a calendar dialog box opens.
3. Select your starting date and time.
4. The calendar closes and the starting date appears on the starting date button.
5. Repeat the process with the ending date button (right side) and calendar.
6. Click **OK** on the Time Editor and the start/end dates/times appear in the Time window of the Advanced tab.
7. Click **OK** and the start/end dates appear in the Times cell of the rule to which you applied time-access constraints.

ADDING AUTHENTICATION MATCHING

Authentication matching simply means that you configure an access control rule to offer a specific or several authentication methods to match an incoming or outgoing access request. In order to match authentication requirements between client and server, you must first load and assign the authentication method(s) to a source network. You can load the authentication modules via the Add/Edit button of the Authentication Methods tab on the Authentication Builder. Once you configure and load the modules, they appear in the windows of the Authentication Methods tab and the Authentication Matching window on the Advanced tab. However, they are not enabled.

- Click Select All to enable all the loaded modules,
  -OR-
- Check specific modules to enable them.
- Click **OK**.

ADDING KEY LENGTH REQUIREMENTS

This is a new feature in the ExtraNet Center. The key length requirement can force 128-bit encryption to certain resources when a client allows a combination of null, 56-bit and 128-bit encryption. You do this via the

Advanced tab. If you allow 40-, 56-, and 128-bit encryption, the server will always try to establish a 128-bit session, but if the client is restricted to 40-bit strength due to export restrictions, the server will "dumb down" to the 40-bit session. You can restrict access to sensitive information to 128-bit uses with

Adding network commands

To enable basic network commands (Traceroute, Ping, UDP, Bind, and Connect) select the Any Commands option on the Advanced tab. To enable specific commands, select the Specific Commands option which will make the commands available, then check the desired commands in the Authentication Matching window.

Authentication

When the server receives an incoming client request, it will poll its suite of authentication rules in descending order to match the user's source (IP, host name, domain name, range, or subnet) to a source in an authentication rule. When the server finds a match, it then compares authentication methods available to the client source against methods the client offers the server. The server then selects the appropriate method for the client if it is in the Config file.

- If the source of the client request is "Anywhere," the server will match this rule and look no further.
- If the server cannot match a client source, it will deny the connection.
- If the client cannot use any source the server specifies in an authentication rule, the server will deny the connection.

NOTE: *The Aventail ExtraNet Server will not start without authentication rules.*

Each authentication rule consists of two configurable elements:

- the source networks,
- and the authentication method(s) assigned to those networks.

As an example (see above), rule #1 requires a user coming from the company's internal subnet to authenticate with a username and password. Rule #2 requires the user to subauthenticate with username/password; i.e., if the client comes from anywhere other than the internal subnet, it must first establish an SSL (encrypted) session, then authenticate with, in this case, username/password as a secondary method. You must first select a source network before you can apply an authentication method to it.

Changing rule order

- To establish the order of a rule, select the entire rule or a cell of that rule. Use the up/down arrows located on the left side of the Authentication tab to move the rule to its new position in rule order.
  -OR-

Right-click a selected cell of the rule you want to reorder, and select the "move up" or "move down" arrow commands from the shortcut menu.

Adding authentication rules

- On the Authentication tab, click New...
  -OR-
- Right-click anywhere in the white area of the Authentication tab and select New... from the shortcut menu.
  -OR-
- Double-click anywhere in the white area of the Authentication tab.Any of these actions will open the Authentication Builder.

Editing authentication rules

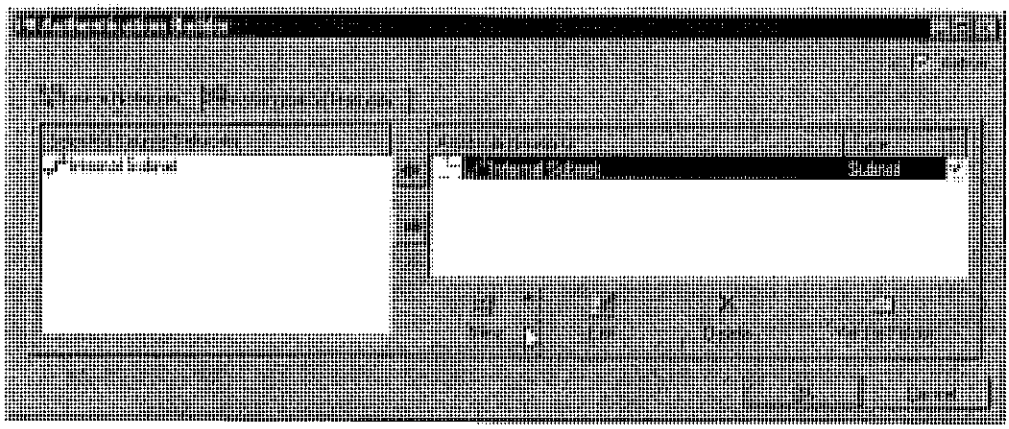
- At the Authentication tab, select the cell in a rule that you want to modify, and click Edit...
  -OR-
- Select the cell in a rule that you want to modify, right-click and select Edit... from the shortcut menu.
  -OR-
- Double-click any cell of a rule.
  -OR-
- Use the arrow keys to move the highlighted focus to a desired cell, then click **Enter.**
- Any of these actions will open the Authentication Builder at the appropriate tab for the selected cell, with the rule number of the selected cell displayed in the title bar.

Deleting authentication rules

- At the Authentication tab, select the entire rule or any cell in that rule. Click **Delete.**
  -OR-
  Right-click the selected rule or cell, and select Delete from the shortcut menu.
  -OR-
  Use the arrow keys to move the highlighted focus to a desired cell, then click **Delete.**

AUTHENTICATION BUILDER

You can configure and view authentication rules via the Authentication Builder. The configurable properties of the Source Networks tab plus the contents of the Authentication Methods tab constitute an authentication rule.



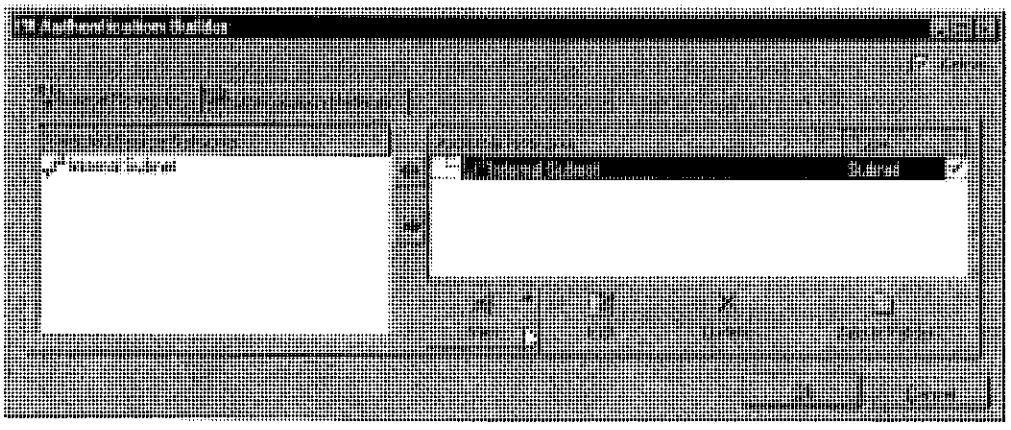
"Active" checkbox in the upper right-hand corner of the Authentication Builder will temporarily deactivate rules without having to delete them.

Via the Source Networks tab you can configure the network information for your authentication rule.

Via the Authentication Methods tab of the Authentication Builder, you can configure, load and enable the authentication method for your authentication rules.

Source Networks

The Aventail ExtraNet Server uses two, integral, configurable elements to create authentication rules. The source network is one part, and authentication method is the other.



AVAILABLE NETWORKS

The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. In order to assign an authentication method to the source network, you must move the network object to the Selected Source Networks pane.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

SELECTED SOURCE NETWORKS

In order to add a source network object to an authentication rule, you must move network objects from the right pane into the left pane. The network objects then become Selected Source Networks.

NOTE: *A check mark appears in the Available pane to the right of objects and/or folders to indicate they are active in the Selected pane. (See above).*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available Networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Source Networks pane, the **New** tools remain functional, but the **Edit**, **Delete** and **Add to Folder** tools become unusable.

CREATING A NETWORK/OBJECT... (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

To add a network object to an Available Networks pane, either right-click anywhere in the Available pane and select New... from the shortcut menu,
-OR-
click **New...** at the Source Networks tab of the Authentication Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**.You may also enter Optional Information.

NOTE: *If you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders are a convenience that allow you to group similar network objects under a common name. You can create folders (which function like aliases) that will appear

in the Available Networks pane, into or out of which you can move selected networks and groups (only while that folder is in the Available Networks pane). To make that folder an active source network, move it from the Available Networks pane to the Selected Source networks pane, using the arrows, or you can also double-click the network object (folder) to move it back and forth, from one pane to another.

ADDING OBJECTS TO A FOLDER

To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Source Networks tab and select **Add to** from the shortcut menu
-OR-
Select the objects and click the **Add to Folder** tool. This will open the Add to Folder dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the SHIFT key down as you click the first and last objects of a continuous list, or by holding the CONTROL key to select individual, non-continuous objects.*

EDITING AN AUTHENTICATION SOURCE NETWORK/OBJECT

Right-click a cell under the Source Network column on the Authentication tab of the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. Either action will open the Authentication Builder at the Source Networks tab. Select from the Available pane the network object you want to edit.

Then click the **Edit** tool. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to that Source Network is global.

DELETING A SOURCE NETWORK/OBJECT

To delete a source network object from an authentication rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the access control rules that will be disabled due to the security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

Authentication Methods

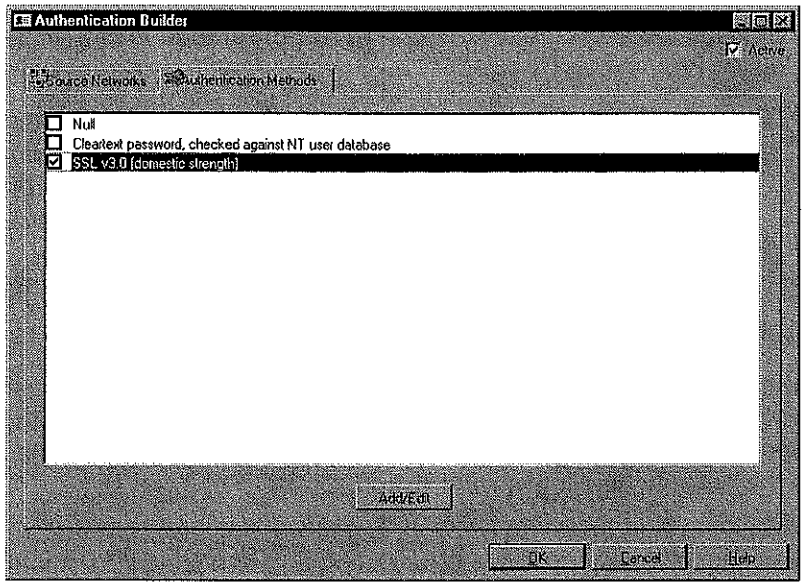
The Authentication Methods tab is where you select an acceptable authentication method for a source network. This tab displays all loaded authentication modules. To apply an authentication method to a source network, check the box of the desired method. You can also add (load) or edit authentication modules via the Authentication Methods tab.

If you select more than one method and the client can authenticate with any of them, the server will select the first authentication rule (#1 of the ordered list of authentication rules). You can configuring the Aventail ExtraNet Server to offer multiple authentication methods.

You can also configure the server to require encrypted messages, or SSL, without requiring authentication, or to require only authentication without encryption. Customarily,

you will require subauthentication when using SSL, which means that you specify an authentication method within the SSL module.

NOTE: *Loading and checking both SSL and an additional authentication method at the Authentication Methods tab DOES NOT mean that the authentication will automatically encrypted. You MUST identify the authentication you want to encrypt (called "subauthentication" via the SSL module if you want to assure that the server will encrypt your authentication*



ADDING OR EDITING AUTHENTICATION MODULES

To load, configure and edit an authentication module, click **Add/Edit** (at the Authentication Methods tab of the Authentication Builder) to open the Authentication Modules dialog box. Once you have loaded and configured your authentication modules, and they appear at the Authentication Methods tab, you can.

NOTE: *You must first select a source network before you can apply an authentication method to it.*

- Click Select All to make all loaded authentication available for the source network
  -OR-
- Check only specific method(s) for the selected source network.
- Click **OK** to close the Authentication Builder. This puts you back at the Policy Console. You will see the new rule on the Authentication tab.

SUBAUTHENTICATING (WITH SSL)

If you select only CHAP, CRAM or password for an authentication method, clients will authenticate but the traffic that matches the specific rule will be in the clear; i.e., not encrypted. If you select SSL (encryption) and you do not specify a secondary

authentication method within the SSL module, the server will encrypt that traffic but not require authentication.

CONFIGURE SSL

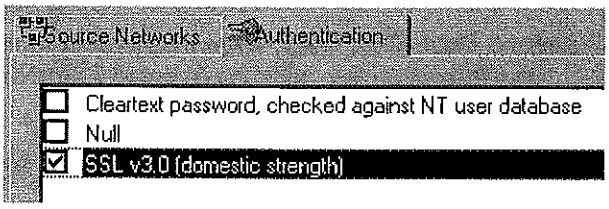
To both encrypt and authenticate traffic, you must correctly configure SSL:

1.First, load the desired authentication methods (CHAP, CRAM, or password).
2.Begin the process of loading SSL, and at the Authentication Modules dialog box select the Client Auth. tab of the SSL module.

3.Enable "Require Client Authentication," and the Secondary Authentication window will become active and display the loaded secondary authentication methods.

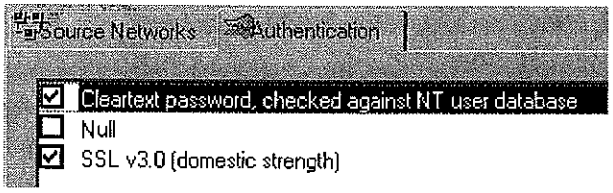
4.Select the desired secondary authentication method, and click OK. Return to the Authentication Methods tab of the Authentication Builder. You will see the secondary methods and SSL as available authentication methods.

If you select SSL as the only method for your authentication rule, the server will encrypt (transparently) and require authentication based on the secondary authentication method.



This means that clients only have the option of SSL (encryption) and must subauthenticate with the NT username and password (when coming from a specified source).

If you select SSL and a secondary method, you are efffectively giving the server a choice of methods.



This means the clients have the option of using SSL (encryption) and must subauthenticate with NT username and password,

-OR-

Clients can use the NT username and password without encryption (when coming from a specified source).

Authentication Modules

The Aventail ExtraNet Server used authentication rules to check incoming (server) and outgoing (client) requests for access. An authentication module is one of two integral, configurable elements of any authentication rule. The source network is the other.

LOADING A MODULE

Select a CHAP, CRAM, cleartext password, or SSL module from the Add Module dialog box, then click **OK**. This loads the module into, and opens, the Authentication Modules dialog box for configuration. The configurable properties of each module are explained below:

CHAP, CHECKED AGAINST A RADIUS SERVER

Incoming module that uses the CHAP protocol for transmission.

Password checking is against a RADIUS user database.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CHAP, CHECKED AGAINST A PLAIN TEXT FILE

Incoming module that uses the CHAP protocol with MD5. Password checking is against a specified password file.

- Password File: Verification is against this password file. The file must contain one username/password combination, separated by whitespace, per line.

CRAM, CHECKED AGAINST A RADIUS SERVER

Incoming module that uses the Challenge-Response Authentication Method against a RADIUS database.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.
- Always prompt for password without consulting RADIUS server:

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.

- Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CRAM, CHECKED AGAINST AN ACE SERVER

Incoming module that uses the Challenge-Response Authentication Method via SecurID tokens against a user/token database on an ACE server. Requires no configuration.

CLEARTEXT PASSWORD, CHECKED AGAINST NT USER DATABASE

Incoming module that applies cleartext-password checking against the Windows NT user database. The server authenticates against LognUser value, for both member and trusted domains.

WARNING: *You must disable the NT Guest Account on the NT server. If you do not, the NT logon module will authenticate any user.*

AUTHORIZATION SCOPE

- SOCKS Server Only: Default value. Verifies password with only the local user database on the server.
- SOCKS Server and Windows NT domains: Verifies the password with the local user database on the server as well as on any trusted domains. If you check Let User Specify Domain, the users can specify which domain to use for authentication. This is an appropriate option when users have accounts on several domains, but different access rights. The format for a user-specified domain is domain\\username.
- Allow user password update: Prompts user to update their password (check on this).
- Export additional user information: Forwards authentication information to another server. It eliminates having to enter authentication information at every server.

CLEARTEXT PASSWORD, CHECKED AGAINST NETWARE

Incoming module applied to NetWare servers using either NDS (NetWare Directory Services) or Bindery NetWare function calls. Because this module needs to make NetWare C Interface Library function calls, the NetWare client for Windows NT must be installed on the same server as the Aventail ExtraNet Server.

NDS (NetWare Directory Services) Authorization: If you check this, the ExtraNet Server will perform authentication against the local

- Novell NDS server on the network. The Aventail ExtraNet Server will always attempt Novell NDS before any specific bindery servers listed in the NetWare Bindery section.
  - Name-Enter user name (and context); e.g., kevin.xena.fox.
  - Password-Enter required password.
  - Tree-Select appropriate tree from pulldown menu.
- NetWare Bindery Servers: If checked, the Aventail ExtraNet Server will attempt authentication of clients against one or more Novell NetWare bind-

ery-based servers. The Aventail ExtraNet Server will attempt to authenticate users against each listed server until 1) one is found that positively authenticates the user or 2) the list of servers is exhausted. You dictate the server order in the listbox, which you can rearrange via the up and down arrows.

Export additional user information: Forwards authentication information to another server.

CLEARTEXT PASSWORD, CHECKED AGAINST A RADIUS SERVER

Incoming module that checks passwords against a RADIUS user database, caches credentials, and forwards user authentication information.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Export additional user information: Forwards authentication information to another server. It eliminates having to enter authentication information at every server.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.

CACHING TAB

- Cache Credentials: Check to enable cache file.
- Cache file: Name of RADIUS caching file.
- Lifetime (hours): Number of hours cache retains credential information.

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.
- Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CLEARTEXT PASSWORD, CHECKED AGAINST A PLAIN TEXT FILE

The module applies password checking against a specified password file.

Filename: Verification is against this password file. The file must contain one username/password combination, separated by whitespace, per line.

Export additional user information: Forwards authentication information to another server.

SSL v3.0

Incoming module that applies one or more encryption algorithms to message traffic, plus compression.

GENERAL TAB

- Acceptable Ciphers: RC4, DES, NULL (no encryption), Diffie-Hellman (not recommended except for testing).
  Advanced... button: See below.

- Credentials Cache
  SSL session resumption requires that you store certificate information. This box allows to specify where the file will be stored via the browse button.
  Cache file: Specifies the storage file for certificate information. If you do not specify a file, the default is sslsrvdata in the temp directory.
  Lifetime (hours): Specifies how long to keep data before considering it stale.
- Miscellaneous
  Max. Certificate Chain Length: You specify the maximum length for a certificate chain, starting with not less
  than two certificates.
  Enable Compression: Transparently compresses encrypted data, depending on available network bandwidth.

ADVANCED BUTTON

The Advanced SSL Server Option Dialog box allows combinations of encryption strengths plus various encryption standards. Its default configuration allows 40- to 128-bit encryption modes.

- Advanced RC4 Options
  RC4 with MD5 (default cipher suite, combining excellent security with speed).
  RC4 with SHA (a more secure suite, but considerably slower).
  RC4 exportable (40-bit) with MD5 Legal encryption strength for U.S. export (clearing checkbox disables 40-bit encryption).
- Advanced DES Options
  DES with SHA (very secure but slow cipher suite).
  Triple DES with SHA (more secure suite than above, but even slower).
  DES exportable (40-bit) with SHA (legal encryption strength for U.S. export) (clearing checkbox disables 40-bit encryption).
  NULL with SHA-Offers stronger protection to authenticated (not encrypted) traffic.
  NULL with MD5-Offers faster protection to authenticated (not encrypted) traffic.
  Reset Defaults Restores all Advanced RC4 and DES option to fully enabled state.

CERTIFICATES TAB

- Certificate File Specifies the filename which contains the certificate information created by the Certificate Wizard. Note that this is optional. It is only needed if client-side authentication is required.
- Certificate information: Displays information about the specified certificate file.
  Password-Password for certificate file.
  Reset- Clears the Certificate File and Certificate Information fields.

CERTIFICATE AUTHORITIES TAB

- Roots File - Specifies a filename containing the root(s) CAs that the client trusts. If no file is specified, any/all roots are allowed.
  Add: Reads a file containing trusted roots and adds its contents to the roots

file.
Remove - Deletes the highlighted trusted root from the roots file.
Describe - Pops up a box displaying more information about the highlighted root.
Reset - Clears the Roots File field.

CLIENT AUTHENTICATION TAB

- Require Client Authentication: Enables client authentication.
- Cache File - Specifies the file in which the user information associated with client authentication will be stored. If you do not specify a file, the default is *sslsrvdata* in the temp directory.
- Client certificates are:- "Never asked for" (a secondary authentication method must be used since the client certificates will not be used), optional (secondary authentication may be used in addition to the optional client certificates), "required" (secondary authentication may be used in addition to the required client certificates).
- Secondary Authentication Methods:- NULL (default), SSL (specifies the client authenticate itself with its own certificate as part of the SSL handshake). Other methods, like password, CRAM and CHAP specify that specific method as the secondary method, over the SSL-encrypted channel.

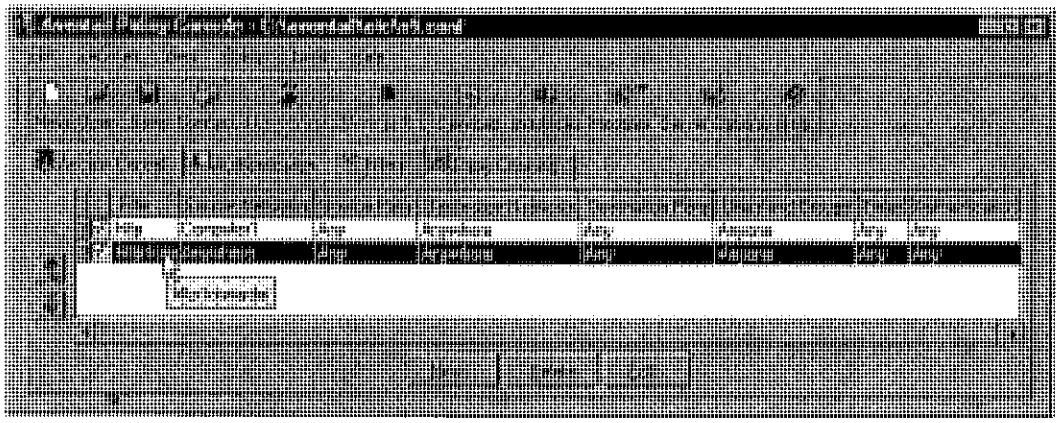
If you select both SSL and other methods (other methods only appear if you load them prior to subauthenticating), the server will attempt SSL first, and attempt to authenticate with other methods only when SSL authentication fails.

Filtering

HTTP content filtering can be an integral part of your access control rules for any network in your system. With the Filter Builder you can use HTTP filtering to control URL content for Source/Destination Network, and Group/User access. For example, you can apply HTTP filtering with time-based parameters, to a group (Marketing).

Marketing will not have HTTP access to:

- URLs of dating and introduction services, extreme/gross/indecent content, gambling or gambling
- information, sex content, or UseNet news sites,
- from 8 a.m. to 6 p.m., Monday through Friday.



CAUTION: *You cannot apply two filters to the same rule. The server will apply the first filter it finds for a rule and look no further.*

HTTP Content Filter

The HTTP Content filter offers both fine-grained, text-editable content control (Aventailfilter), as well as a predefined definition file (SmartFilter) of "deny" categories. Usually, you will use the text-editable filter only when content gets past the SmartFilter and continues to the end user.

HTTP Authentication Forwarding filter

The HTTP Authentication Forwarding filter allows you to forward user credentials in the HTTP header to an IIS Web server or any Web server that supports the same protocol(s) used by the Aventail ExtraNet server. This eliminates the need to repeatedly enter authentication information.

NOTE: *The forwarding filter does not require configuration.*

Adding Filtering Rules

At the filters tab of the Policy Console,

- Double-click in the white space of the Filters tab,
  -OR_
- Right-click and select New,
  -OR-
- Click New.

Any of these actions will open the Filter Builder. It is with the Filter Builder that you configure and enable a filter.

Editing Filtering Rules

At the Filters tab, select the appropriate cell of the rule you want to edit:

1. Right-click and select **Edit...** from the shortcut menu,
   -OR-
2. Click **Edit...**Either of these actions will open the Filter Builder where you can make your changes.

Removing Filtering Rules

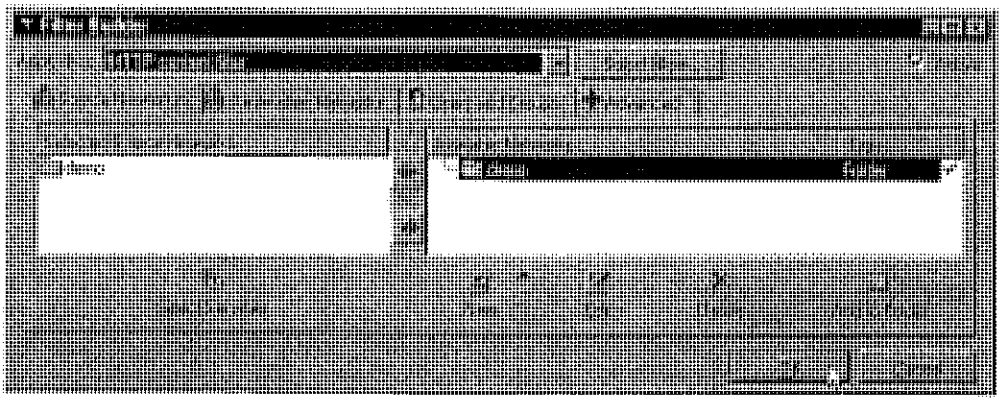
At the Filters tab, select the whole rule or a cell of the rule you want to delete.

1. Right-click and select **Delete** from the shortcut menu,
   -OR-
2. Click **Delete**.Either action will remove the rule.

FILTER BUILDER

With the filter builder you can apply HTTP content filtering, HTTP authentication forwarding, and packet printer filtering to

- Source Networks
- Destination Networks
- Users and Groups
- and content available through the Advanced tab of the Filter Builder.



ADDING FILTERING TO A NETWORK, USER/GROUP, OR TIME-BASED RULE

1. At the Filter Builder, select the appropriate tab and network or user/group object to which you will apply filtering.

NOTE: *Make certain that the object appears in the "Selected" pane.*

2. Once you select your object, click Select Filters.... This opens the Filters... dialog box.
3. Enable the appropriate filter and click **OK**.The enabled filter now appears in the Apply Filter... text box of the Filter Builder.

NOTE: *Checking the HTTP Content filter activates the Configure... button.*

The new filter rule appears on the Filters tab.

EDITING FILTERING FOR A NETWORK, USER/GROUP, OR TIME-BASED RULE

At the Filter tab, select the whole rule or a cell of the rule you want to edit.

- Right-click and select Edit... from the shortcut menu,
  -OR-
- Click Edit...,
  -OR-
  Double-click the selected cell.
- Any of these actions will open the Filter Builder. Make the appropriate changes, and

- click **OK**. The changes will appear at the Filters tab.

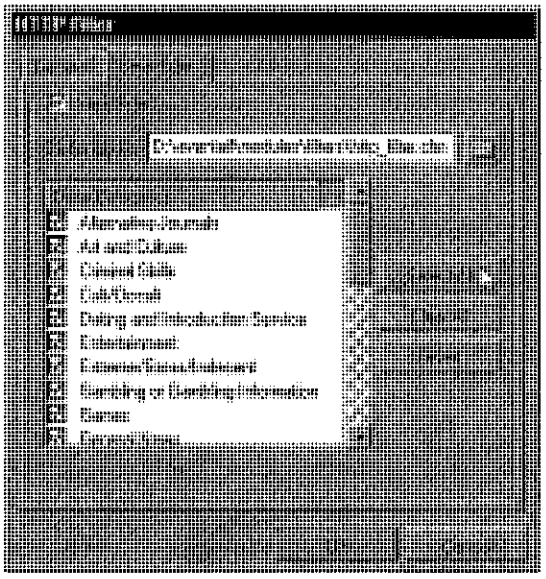
DELETING FILTERING FROM A NETWORK, USER/GROUP, OR TIME-BASED RULE

At the Filters tab, select the rule you want to delete, and

- Click Delete,
  -OR-
- Right-click and select Delete from the shortcut menu.This removes the rule from the Filters tab.

HTTP Content Filter

The HTTP filter will allow you to make sophisticated policy decisions, not just "user X can (or cannot) connect to host Y." In addition to controlling URL access, you can remove content, strip HTML tags, and deny JAVA and ActiveX controls. The HTTP filter currently consists of two filters:



- SmartFilter -- SmartFilter blocks URLs based on deny categories in a definition file supplied with the HTTP filter. You must load the dictionary file to enable the SmartFilter to block URLs.
- General tab (Aventail) -- The Aventail filter offers fine-grained, text-based control to block Netscape Plug-ins, JAVA applets, and ActiveX controls. You must load the filter configuration file to block HTTP content.

CONFIGURING AND LOADING THE HTTP CONTENT FILTER

To configure and enable the SmartFilter module, select the SmartFilter tab of the HTTP Filter dialog box.

1. Check the SmartFilter box. Browse for the dictionary file

`(aventail\modules\filters\http_filter.mod),`

2. select and load it into the text box.

3. At the Deny Categories window, check the categories you want to exclude,
   -OR-
   click Select All.

NOTE: *The Invert button reverses "deny" selections within the Deny Categories window. It does not clear them.*

4. Click **OK**. This returns you to the Filters dialog box.
5. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to deny access to the URLs in the selected categories. You can apply it to any network, user, group or time-based rule.

To configure and enable the Aventail filter (General tab), select the General tab of the HTTP Filter dialog box.

1. Check the Aventail box.
2. Browse for and select the filter file:

`(aventail\modules\filters\http_filter.cfm)`. text-editable file.

3. Click **OK**. This returns you to the Filters dialog box.
4. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to remove Netscape plugins, JAVA applets, ActiveX controls, etc. from HTTP content. You can apply it to any network, user, group or time-based rule.

To configure and enable the Aventail filter (General tab), select the General tab of the HTTP Filter dialog box.

1. Check the Aventail box.
2. Browse for and select the filter file

`(aventail\modules\filters\http_filter.cfm)`. text-editable file.

3. Click **OK**. This returns you to the Filters dialog box.
4. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to remove Netscape plugins, JAVA applets, ActiveX controls, etc. from HTTP content. You can apply it to any network, user, group or time-based rule.

Proxy Chaining

Proxy chaining is when one SOCKS server acts as a gatekeeper to route requests for information that resides behind another SOCKS server. In this capacity, the gatekeeper server evaluates its security policies to authenticate the user (client) request and determine if the user has access to the requested destination. If the user request is valid, the gatekeeper server acts as a client and proxies the user request to another SOCKS server by authenticating to the secondary SOCKS server. If the secondary server has access to the destination, the user passes through to the destination.

You can assign a destination to a server's address, so all requests to this destination will be proxied (forwarded) to that server. Additionally, you can prioritize proxy servers.

To proxy chain a server, you configure the proxy server name and address, the name of a fallback server (optional), the destination network, and the network services (ports).

Adding a Proxy

At the Proxy Servers tab on the Policy Console,

- Double-click in the white space
  -OR-
- click New...,
  -OR-
- Right-click and select New... from the shortcut menu.

Any of these actions will open the Proxy Chain Builder.

Editing a Proxy

At the Proxy Servers tab, select a cell of a rule that you want to edit, and

- right-click and select Edit... from the shortcut menu,
  -OR-
- click Edit....

Either action will open the Proxy Chain Builder at the appropriate tab.

Deleting a Proxy

At the Proxy Servers tab, select the proxy rule you want to delete, and

- Right-click and select Delete from the shortcut menu,
  -OR-
- click Delete.

Proxy Chain Builder

The Server tab allows you to identify and configure the proxy and fallback servers for the destination network. The default status of the Server tab is to allow a direct connection, not proxied.

To proxy a server, you will need to

- select the Proxy option on the Server tab of the Proxy Chain Builder,
- enter host and port information for the proxy server,
- and enter host and port information for the fallback server, if you use a fallback server.

Additionally, you need to select a SOCKS version.

Adding a primary/fallback host and port

Select the Proxy option on the Server tab. If you will use a fallback server, enable the Use Fallback option. Enter a qualified name, fully qualified name or IP address for the primary (and fallback) host. Enter a single port.

Editing a primary/fallback host and port

At the Proxy Servers tab on the Policy Console, select the cell containing the information you want to edit, and either right-click and select Edit,
-OR-
Click Edit. The Proxy Server Builder will open at the correct tab for your edits. When you finish entering the new information, click **OK** to return to the Policy Console.

Determining SOCKS version

Select a SOCKS version option or click Detect, then click **OK**.

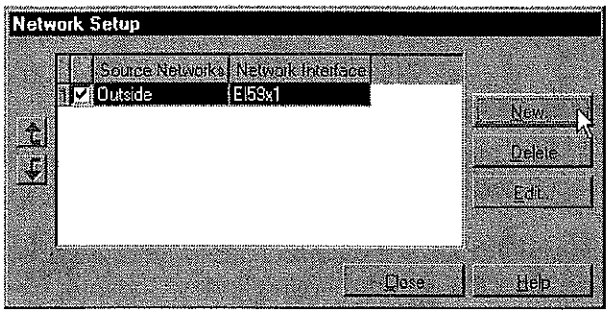
Active/disabled (checkbox)

The checkbox in the right-hand corner of the Proxy Chain Builder indicates the enabled/ disabled status of the proxy rule. This information corresponds to the checkmark at the beginning of each Access Control rule.

Network Setup

Network Setup is for "multihomed" servers (a server with two or more installed network interface cards). To properly configure your network setup you must specify what internal and external network traffic goes to which network interface cards (NIC). You do this with "routing rules."

NOTE: *To neutralize IP spoofing attacks you must properly configure multihomed servers.*

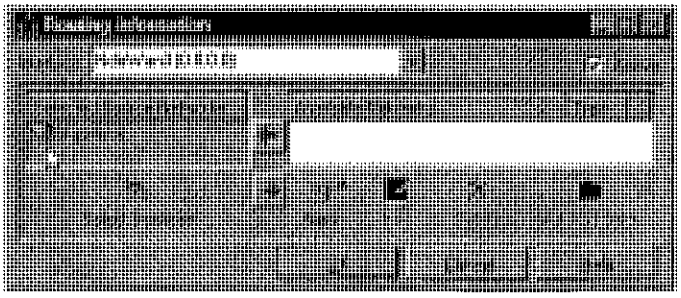


To correctly configure your routing rules, you must identify a source network available to any specific interface card. The Aventail ExtraNet Server transparently detects installed network cards. This information appears at the Routing information dialog box.

Routing Rules

Routing rules specify what internal and external network traffic goes to which network interface cards (NIC) on a server. Routing rules work only for multihomed servers (a server with two or more installed network interface cards), and are not necessary for the server to properly function. However, you must properly configure multihomed servers in order to proxy chain and neutralize IP spoofing attacks.

The Aventail ExtraNet Server transparently detects installed network cards and available networks. This information appears in the Routing information dialog box where you can configure your routing rules.



Adding a route

At the Routing information dialog box,

1. Select the appropriate card that appears in the Interface: list box.
2. From the Available Networks pane, select the target network and move it to the Selected Source Networks pane.

Click **OK**. The new routing rule will appear in the Network Setup dialog box.

NOTE: *If you do not select a network but click* **OK**, *all network traffic will route through the card displayed in the Interface: text box.*

Editing a route

At the Routing information dialog box, either:

1. Select a new network in the Available Networks pane.
2. Move that network to the Selected Source Networks pane
   -OR-
   Move the Selected Source Network to the Available pane,
   -AND/OR-
   Select a different card in the Interface: text box
3. Click **OK**. The edited routing rule will appear in the Network Setup dialog box.

Deleting a route

You can delete a route at the Network Setup dialog box.

Adding a routing rule

1. At the Policy Console, click Network Setup at the toolbar
   -OR-
   select View | Network Setup from the menu. Either action opens the Network Setup dialog box.
2. Click New... to open the Routing Information dialog box where you will configure your new routing setup.

Editing a routing rule

From the Policy Console menu,

1. select View | Network Setup...
   -OR-
   Click Network Setup on the tool bar. Either action opens the Network Setup dialog box.
2. At the Network Setup dialog box, Double-click in the white space of the Network Setup window,
   -OR-
   Right-click and select Edit... from the shortcut menu,
   -OR-
   Click Edit...to open the Routing Information dialog box where you can reconfigure your routing setup.

Deleting a routing rule

From the Policy Console menu,

1. select View I Network Setup...
   -OR-
   Click Network Setup on the tool bar. Either action opens the Network Setup dialog box.
2. At the Network Setup dialog box, select the rule you want to delete, and Right-click and select Delete from the shortcut menu,
   -OR-
   Click Delete. Either action removes the rule from the Network Setup dialog box.

Configuration File Format

INTRODUCTION

The configuration file `s5.conf` controls all aspects of the Aventail ExtraNet Server. By default, this file is located in `<prefix>/etc/s5.conf`, where `<prefix>` is the directory the Aventail ExtraNet Server was installed to (typically `/usr/local/aventail`). You can edit this file using a text editor.

The Aventail ExtraNet Server reads this configuration file the first time the server is started, and each time the process is restarted. This file contains all the policy information that the Aventail ExtraNet Server needs to handle a connection.

GENERAL SYNTAX

All entries in the configuration file are of the following format:

```
type name {
  key = value;
  key = value;
}
```

Case, new lines, and spacing are not significant, unless referring to an object name, or data within a quoted string. The name of the object is not significant, as long as it is unique within the configuration file.

The type of object determines which keys are within the block. The order of keys within the block is significant only in the Policy Object. In the Policy Object, the server reads each line, from top to bottom, until it makes a match; for a line to match, each entry within the line must match. For more information, refer to the "Policy" section.

DATA TYPES

There are five basic data types in the configuration file: tokens, booleans, integers, simple strings, and strings. The following object is used as an example in the definitions below:

```
installation @converted_installation
{
  comment = "Automatically converted from v2.x file:socks5.conf";
  port = 1080;
  reversedns = TRUE;
}
```

Tokens

Tokens are the internal keywords that the parser recognizes. Tokens determine the type of data that can come after them. In the example above, `installation`, `comment`, `port`, `reversedns`, and `TRUE` are all tokens.

Tokens are not case-sensitive. Tokens should never be contained within quotation marks.

Booleans

Booleans can be either `TRUE` or `FALSE`. `TRUE` and `FALSE` are tokens that the parser recognizes internally. In the example above, `TRUE` is a boolean.

Booleans are not case-sensitive. Booleans should never be contained within quotation marks.

Integers

An integer can be any sequence of numbers. In the example above, `1080` is an integer.

Numbers cannot be negative, and floating point numbers are not allowed.

Simple Strings

A simple string must start with an "@" symbol, and must contain only alphabetic characters (a-z or A-Z), digits (0-9), and/or underscores (_). In the example above, `@converted_installation` is a simple string.

Strings

To avoid parse errors, a typical string is usually contained within quotation marks; this can reduce confusion between strings and tokens that otherwise appear identical.

In cases where quotation marks must be included within the string, basic escape mechanisms are available. To include a quotation mark within a string, type `'\''`. To include a literal backslash character, type `'\\'`. Placing any other character directly after a backslash (\) simply inserts that character. In the example above, `"Automatically converted from v2.x file:socks5.conf"` is a string in quotation marks.

Common Attributes

Any object(s) can have the `comment = STRING` attribute included within the object body. This freeform string can contain information about the object. It is not parsed by the server or the graphic user interface (GUI) administration tool in any way. It is strictly for informational purposes.

ORDER OF OBJECTS

You must define all objects before using them. (This limitation will be removed in a future release of the Aventail ExtraNet Server.) The following example would result in a parse error because "Second Group" is used before it is defined.

```
group "First Group"
{
  local group "Second Group";
}
group "Second Group"
{
}
```

MODULES

All filters and authentication methods (except NULL) are defined in loadable modules so that, if desired, only the necessary functionality can be loaded into memory. Loadable modules also allow for in-house development of custom authentication methods or content filters.

You must complete three steps before a server will actually use a module. You must load the module, apply the module to a specific installation, and use the module in an access-control, authentication, or filter rule.

Loading a Module

You must load each module individually, in the module section. The module section also contains all configuration information for the module. The following example is used in the definitions below:

```
module "http_filter"
{
comment = "HTTP content filter";
filename = "modules/filters/http-filter.mod";
stub = "http_filter";
option "aventail" = "/usr/local/aventail/etc/avfilter.conf";
}
```

Parameter	Description
filename	Specifies where the loadable module can be found. This can be a fully qualified pathname (e.g., `/usr/local/aventail/modules/authentication/test.mod`), or relative to the installation directory (e.g., `modules/authentication/test.mod`).

Parameter	Description
stub	The unique identifier for the module. It is used to find all of the functions that the server needs. This is typically the name of the module, without the `.mod` suffix. All `'-'` characters will be converted to `'_'`.
option	All configuration information for the module includes any number of "option" statements. Options are module-specific.

Including a Module in an Installation

You must use a module in an installation before you can use it in the installation's ACL, filter, or authentication rule. To include a module in an installation, use the "module" keyword. For example:

```
installation "Converted"
{
  module "http_filter";
}
```

Referencing a Module in a Rule

Once you have loaded and included a module in an installation, any rule in that installation can reference the module. The type of module determines which referencing method to use.

- **Client-side Authentication:** Client-side modules are used only when proxy chaining, and do not need to be explicitly used in a rule. If the server you are chaining to requires authentication, all configured authentication methods will be offered in the negotiation phase, and the remote server will select the most appropriate method.
- **Server-side Authentication:** Server-side modules are used to force clients to authenticate in a certain way. Authentication methods are referenced by a short, unique string, which maps to a specific authentication method. The Aventail ExtraNet Center includes the following authentication methods by default: SSL, Username/Password, CHAP, CRAM, and Null. Other methods can be installed by third parties or local system administrators. If you are unsure of which authentication methods are available in your installation, contact your local system administrator.

  To configure the server to require a certain authentication method, include that method in an authentication rule and, if necessary, in any access control or filtering rules that might require greater control than an authentication rule can provide.
- **Content Filters:** Content filters are referenced by a short, unique string, which maps to a specific filter method. Content filters are used only in filter rules. The Aventail ExtraNet Center includes the following filters by default: http, http-forwarder, and print. Other methods can be installed by third parties or local system administrators. If you are unsure of which filters are available in your installation, contact your local system administrator.

- **Access Control:** Access-control modules do not need to be explicitly used in a rule. Access-control modules are used in the order in which you load them. If a module refuses a connection, none of the subsequent modules will be consulted.

  The Aventail ExtraNet Center does not ship with any access-control modules by default; however, other methods can be installed by third parties or local system administrators. If you are unsure of which access-control methods are available in your installation, contact your local system administrator.

DEFINING USERS AND GROUPS

You do not need to explicitly define users and groups before using them in a rule or group definition; the users and groups are self-describing.

The standard user/group notation is "`backend:name`" where "`backend`" is a string that uniquely identifies a backend where the actual authentication information is stored, and "`name`" is the user/group name. Specifying the special backend "`any`" means that any backend should match the username.

To use a user or group in a rule or group, use the group or user keywords. For example:

```
access permit @ac10
{
   .
   .
   .
   user "unix:root";
   group "unix:wheel";
   user "unix:dhdore";
   user "any:ichabod";
}
```

When using the same set of users in many rules, it is easier to put them into a group locally and use those groups in the rules. The "group" object defines a local group. You can include users, groups, and other local groups in a local group. You can also mix and match backends. For example:

```
group "Special Users"
{
   user "unix:root";
   group "unix:wheel";
   user "unix:dhdore";
   user "any:ichabod";
}
access permit @ac11
{
   .
   .
   .
   local group "Special Users;
}
```

DEFINING NETWORKS

To define networks and hosts, use the network object. There are four types of networks; they all follow the same pattern in the configuration file:

```
network <TYPE> "name
{
  key1 = value 1;
  key2 = value 2;
}
```

The <TYPE> determines which keys are valid.

- **Domain:** This type of network is used to match an entire domain of machines. The domain keyword is used to define the domain. For example:

  ```
  network domain "GNU Domain"
  {
     domain = "gnu.org";
  }
  ```

  Any machine name that ends with the domain matches. Examples of matches and mismatches:

  `www.aventail.com` **IS** in `.aventail.com`
  `www.aventail.com` **IS NOT** in `.bob.aventail.com`
  `patrick.in.aventail.com` **IS** in `.aventail.com`

- **Host:** This matches a specific machine. You can match the host machine with either the IP address or the hostname keywords. The IP address should be in dotted-decimal notation, and the hostname should be a string. For example:

  ```
  network host "Mythical machine"
  {
     ipaddress = "123.456.7.8";
  }
  network host "Another Mythical machine"
  {
     hostname = "test.test.ick.bin.org";
  }
  ```

  Hostname comparisons are case-insensitive; therefore, `WWW.AvEnTAiL.com` matches `www.aventail.com`, and vice versa.

- **Subnet:** You can define an entire subnet with this type of network. The IP address and netmask keywords recognized and should be in the standard dotted-decimal notation. For example:

  ```
  network subnet "123.456.7.8.xxx Subnet"
  {
  ipaddress = "123.456.7.1";
  netmask = "255.255.255.0":
  }
  ```

- **Range:** Occasionally, a grouping of machines cannot easily be described with a subnet mask. A network can also be a consecutive range of IP addresses.

The from and to keywords specify the beginning and end of a range in dotted-decimal notation. For example:

```
network range "Subrange of 123.456.7.xxx"
{
from = "123.456.7.5";
to = "123.456.7.25";
}
```

The range is inclusive, which means that the endpoints are included in the range. In the example above, "`123.456.7.5`" and "`123.456.7.25`" would match the specified range.

DEFINING SOCKS SERVERS

SOCKS server definitions are used in proxy chaining rules. The following table explains the attributes that you can specify.

Parameter	Description
hostname	The hostname of the SOCKS server. If you specify the hostname, you do not need to specify the IP address.
ipaddress	The hostname of the SOCKS server in dotted-decimal notation. If you specify the IP address, you do not need to specify the hostname.
port	The port number that the server is listening on.
version	The SOCKS protocol version the server speaks. Valid version numbers are "4" and "5."

An example of a SOCKS server definition is:

```
server "slow";
{
  hostname = "slow";
  port = 1080;
  version = 5;
}
```

RULES

There are five types of rules that determine how a connection will be handled: Authentication, Access-control, Filters, Routing Entries, and Proxy-chaining. Rules are evaluated in the order in which you list them in the installation object. The server applies the first matching rule to the connection, then the second matching rule, and so on.

Rule	Description
Authentication Rule	Determines how a client will be allowed to authenticate to the server.
Access-control Rule	Specifies the class(es) of connection allowed through the server. Connections can be accepted or rejected.
Filter Rule	Determines whether or not a content filter needs to be applied to the data stream. This is the final decision made before starting to proxy data.
Routing Entries	Specifies which network interface each machine can use.
Proxy-chaining Rule	Controls which traffic (if any) will be directed through subsequent servers. This is typically used for access to partners' networks where individual users in the company do not have accounts but the company as a whole does.

Common Attributes of Rules

You can use the following attributes in any of the rule types. If you specify multiple networks, network groups, users, or groups, this becomes an "OR" operation. For example, the user could be "Deb" *or* "Dale" *or* "Eric," etc.

Attribute	Description
enabled	Controls whether or not the rule will actually be considered when the server looks for matches. If FALSE, it will be skipped completely. This is useful for temporarily disabling a certain set of access rights.
network source name	Specifies that the user's connection must originate from the network source for the rule to apply.
network group source name	Specifies that the user's connection must originate from the network source for the rule to apply.
source services	Specifies that the user's connection must originate from any of the listed ports for the rule to apply. You can list either single services or ranges of services.
methods	Specifies that the user must authenticate using one of the methods listed for the rule to apply. For information about which authentication modules are supported, refer to "Authentication."

Attribute	Description
keylength	Specifies that the session must be encrypted with a key of a certain minimum length for the rule to apply. Valid key lengths are 0, 40, 56, or 128 bits.
user backend	Specifies that the authenticated user must be the named user according to the backend in order for the rule to apply.
group backend	Specifies that the authenticated user must be in the named group according to backend in order for the rule to apply.
local group name	Specifies that the authenticated user must be in the locally defined group name in order for the rule to apply.
DAY	One of Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday. The right-hand side is a list of one or more time ranges, in 24-hour format. The granularity of the times is on the half hour only. Time ranges are inclusive.
startdate	Start date in mm/dd/yyyy notation.
enddate	End date in mm/dd/yyyy notation.
starttime	Start time in hh:mm notation.
endtime	End time in hh:mm notation.

Authentication

The methods keyword determines which authentication method(s) will be accepted from different networks. There are no new keywords available for this object type. For example:

```
authentication @ac10
{
  enabled = TRUE;
  network source = "Anywhere";
  methods = "password " "cram" "ssl";
}
```

Access Control

Access-control rules determine who can go where, and when, through the server. An access-control rule specifies, in the object definition, whether it will permit or deny access to the listed resources. Each entry on the line must match for the entire line to match. For example:

```
access permit @ac10
{
  enabled = TRUE;
```

```
  network source  "Anywhere";
  network destination "Anywhere";
}
access deny @acl1
{
  enabled = TRUE
  network source "Anywhere";
  network destination "Anywhere";
}
```

You can apply the following new attributes to access-control rules.

Attribute	Description
commands	Specifies that the user can use only the commands listed. Recognized commands are "connect," "bind," udp," "ping," or "traceroute." The commands correspond to the SOCKS commands for proxying different types of traffic.
network destination name	Specifies that the user must be attempting to reach the network name for the rule to apply.
network group destination name	Specifies that the user must be attempting to reach any of the networks in name for the rule to apply.
source services	Specifies that users must be attempting to reach any of the listed ports for the rule to apply. You can list either single services or ranges of services.

Filters

Filter rule objects can have any of the common attributes and access-control attributes, and include the following attributes:

- **`module = filtername;`**

  This attribute specifies the name of the filter to apply if the connection matches this rule. For more information on content filters, refer to "Filters."

- **`filter @filter0`**

```
{
   enabled = TRUE
   module = "http";
   SUNDAY = 00:00-24:00
   MONDAY = 00:00-24:00
   TUESDAY = 00:00-24:00
   WEDNESDAY = 00:00-24:00
   THURSDAY = 00:00-24:00
   FRIDAY = 00:00-24:00
   SATURDAY = 00:00-24:00
}
```

Routing Entries

On machines with multiple network interfaces (i.e., IP addresses), it is important to ensure that the machines use certain network interfaces in conjunction with certain addresses. This prevents IP spoofing (where machines outside the network pretend to be machines inside the network) by ensuring that inside machines use the inside network and outside machines use the outside network. This is also used by SOCKS servers in determining which network interface to bind on when accepting a BIND request, or when issuing a SENDTO request. If no entry matches, the SOCKS server uses INADDR_ANY to bind, and a connection can be received on any interface. Single-homed hosts do not need routing entries; they are necessary only when machines have more than one network interface. The format for the routing-entry object is:

```
card = string;
```

Proxy Chaining

Proxy-chaining entries describe the addresses of SOCKS proxy servers. There lines tell the server how to contact a given host. If no lines match a host, the server contacts the host directly. The format for the proxy-chaining object is:

```
noproxy = boolean;
server = name;
```

INSTALLATION

The following table describes the attributes of the installation object.

Attribute	Description
port	Specifies the port number that the server should listen on for incoming connections.
identd	Specifies whether to use the IDENTD protocol when using NULL authentication. (This attribute is not supported in v3.0.)
reversedns	Specifies whether to attempt reverse DNS. This is a legacy option. The server does reverse DNS only when necessary (e.g., when a rule needs to check it against a domain-based network, etc.).
udprestrict	Specifies whether the server should accept UDP traffic from anyone, or only from machines that it has previously talked to.
udpclientsport	Specifies whether the server should try to use the same port number on its external interface that the client has used internally. This can improve the performance of some UDP applications.
udpbind	This attribute is no longer used.

Attribute	Description
timeout	Specifies how long idle connections are allowed to stay active. This attribute is used in conjunction with the time-unit attribute (below).
timeunit	Used in conjunction with the timeout attribute (above) to specify how long idle connections are allowed to stay active.
secout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `security.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
sysout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `system.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
miscout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `misc.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
seclevel	Specifies the error level for logging security messages. For more information, refer to "Logging."
syslevel	Specifies the error level for logging system messages. For more information, refer to "Logging."
misclevel	Specifies the error level for logging miscellaneous messages. For more information, refer to "Logging."
logroot	Specifies the directory that will contain the log files.
auditlog	Specifies whether to keep an audit log of all connections processed by the server.
auditpath	Specifies the directory that will contain the audit files. Three files are created in this directory: *accounting*, which contains the main audit trail; *security*, which contains additional security information; and *errors*, which contains information about failed connections (due to network errors, etc.).

Attribute	Description
auditformat	Specifies which format to log the auditing information in. Currently supported formats are the WebTrends Enhanced Log Format (WELF) and a flat text file specific to Aventail, which is easily imported into spreadsheets or databases.
buffersize	Specifies how much data to attempt to read from the network at one time. Larger sizes may improve throughput, but will increase memory usage.
maxchildren	Maximum number of connections to allow at any one time. The license should do this automatically.
servicenames	Specifies whether to look up service names to use in logging messages and audit files.
backlog	Specifies how many pending connections to allow to "stack up." The default value is "5." On some versions of Unix, the TCP/IP stack ignores this value. Once the maximum allowable number of connections is in the queue, the server will reject new connections.
pidfile	*(Unix only)* Specifies where to store the process ID. This file is used by the stopsocks script. You usually do not need to specify this attribute.
ipspoofing	Specifies whether to watch for IP spoofing attacks, and reject potentially bad connections. If this option is activated (TRUE), the server will reject any connection that originates from a network interface that it would not use in talking to that host. In complicated network setups, this can cause problems, and should probably not be activated (set to FALSE).
alertfrequency	
alertthreshold	
traceroutеprogram	Specifies which program to execute when a "traceroute" command is proxied. This should be the executable name by itself, or a fully qualified pathname to the executable (if it is not in the default path for the user the server is running as).
pingprogram	Specifies which program to execute when a "ping" command is proxied. This should be the executable name by itself, or a fully qualified pathname to the executable (if it is not in the default path for the user the server is running as).

Attribute	Description
nlsdirectory	Specifies where to find the NLS catalogs for the server. In most cases, this attribute should not be set. The server will automatically determine where the catalogs are installed.
module module_name	Use the module module_name in this installation. This means that the module will be loaded and available for use in any rules in the Policy section (see below).

POLICY

The policy object is where you arrange all of the rules and give them a specific ordering. The ordering of similar attributes is important, and can significantly affect the policy enforced by the server. Be sure to order or reorder rules carefully.

The following table describes the additional attributes that are valid in a policy object.

Attribute	Description
interface string	Imports the routing rule named "*string*" into the current policy.
authentication string	Imports the authentication rule named "*string*" into the current policy.
proxy string	Imports the proxy chaining rule named "*string*" into the current policy.
filter string	Imports the filter rule named "*string*" into the current policy.
access string	Imports the access-control rule named "*string*" into the current policy.

An example of a policy object is:

```
policy "Converted"
{
  interface @route0;
  authentication @auth0;
  proxy @proxy0;
  proxy @proxy1;
  filter @filter0;
  access @ac10;
  access @ac12;
}
```

LOGGING

Logging is an essential part of maintaining server function. With logging, you can track user activity, diagnose failed connections, repair system failures, and configure the logging output for Aventail or WebTrends formats.

Logging options include three logging methods, eight levels of information, four output options, and two output formats.

Log Methods

There are three log methods: Security, System, and Miscellaneous. When logging server activity, select one of the three methods.

- **Security:** Security information consists of failed authentication attempts and methods. When logging to LOGFILE, the filename is `security.log`.
- **System:** System information identifies and displays network problems as they affect the ExtraNet Server. Examples of network problems include low memory, timing out, a SOCKS server crash, etc. When logging to LOGFILE, the filename is `system.log`.
- **Miscellaneous:** Miscellaneous information consists of everything else not included in the Security and System methods. When logging to LOGFILE, the filename is `misc.log`.

Log Levels

There are eight log levels: Fatal, Error, Warning, Information, Verbose, Debug1, Debug2, and Debug3. When logging server activity, select one of the eight methods.

NOTE: *Processing large amounts of information by logging at the Verbose level or higher can impact the server's performance for brief periods of time.*

NOTE: *Logging at a certain level includes all levels below that level as well. For example, logging at the Warning level includes Fatal and Error messages as well.*

Log Level	Description
Fatal	Fatal error information only.
Error	Critical error information only.
Warning	Non-critical warning information.
Information	Detailed logging information.

Log Level	Description
Verbose	More detailed logging information than the Information level, but not as detailed as the Debug-level information.
Debug1, Debug2, Debug3	Debugging levels of increasing verbosity. This can cause large amounts of data to be written, and should be used only when troubleshooting.

Log Output Options

There are three log-output options: SYSTEM, LOGTOOL, and LOGFILE. You can specify multiple output options at once.

- **SYSTEM:** Selecting this log-output option will cause logging information to output to the system logger. Under Unix, the system logger is syslog, and under Windows NT it is the Event Viewer Application Log. Under Windows NT, the server will always log startup information to the Event Viewer.
- **LOGTOOL:** This option is currently valid only under Windows NT. The Logging Tool is the dynamic logging tool for all Aventail ExtraNet Server activity. The Logging Tool can dynamically filter out certain types of log messages and is useful for debugging quickly without having to bring the server up and down to change log levels.
- **LOGFILE:** Selecting this log-output option will cause logging information to log to the appropriate flat file in the logroot directory.

Auditing

The auditing subsystem tracks where users are going, and how much bandwidth they are using. Auditing can be useful for fine-tuning policy if certain types of traffic start using too much bandwidth.

Audit Log Types

There are three audit log types: Error Audit Log, Accounting Audit Log, and Security Audit Log.

- **Error Audit Log:** The Error Audit Log records failed connections that result from system or hardware lapses or failures.
- **Accounting Audit Log:** The Accounting Audit Log records successful system and authentication connections.
- **Security Audit Log:** The Security Audit Log records failed connections that result from authentication lapses or failures.

Information Types

Log entries can contain varying amounts of information, depending on the type of log and the connection status of each entry. Log entries are in a text-only, space-delimited format (with date and time within quotation marks). Log entries allow administrators to track

- Traffic date and time
- Source and destination

- Connection duration
- Authentication methods
- Commands
- Bytes received
- Exit status

Output Formats

The two valid output formats are the Aventail format and the WebTrends Enhanced Log Format (WELF).

- **Aventail:** This is a flat text file format specific to Aventail, which is easily imported into spreadsheets or databases. Below is an example entry format.

  ```
  bob.bp.aventail.com:1234 null dhdore "15 May 1998
  09:20:57" v4 connect www.gnu.org:http 0 19252 1195 38
  ```

- **WebTrends Enhanced Log Format (WELF):** With WebTrends products, you can save, FTP, or e-mail reports in Microsoft Word, Microsoft Excel, HTML, text, or comma-delimited text formats. For more information about WebTrends, contact WebTrends at `http://www.webtrends.com`.

Exhibit G

May 26, 1999 Aventail Press Release

HighBeam™ RESEARCH

AVENTAIL: Aventail announces new directory-enabled extranet solution.

Publication: **M2 Presswire** Publish date: **May 26, 1999**

M2 PRESSWIRE-26 May 1999-AVENTAIL: Aventail announces new directory-enabled extranet solution (C)1994-99 M2 COMMUNICATIONS LTD

RDATE:250599

* Aventail ExtraNet Center Supports Leading LDAP Directories from Netscape, IBM, and Lotus

For the rapid deployment of secure extranets, Aventail has announced a new version of its award-winning Extranet Management and Security (EMS) solution, Aventail ExtraNet Center v3.1. This latest offering simplifies extranet user management by including broader support for Public Key Infrastructure (PKI) and Lightweight Directory Access Protocol (LDAP)-enabled directories and automatic client updating. With these enhancements. large multi-enterprise organisations can quickly and easily deploy and manage powerful and secure extranet applications.

"Extranets are rapidly evolving into a mainstream technology as the Fortune 1 000 begin to implement strategic business plans around extranets to improve communication, reduce supplier costs, increase customer response time, improve quality and decrease inventory," says Colin Tankard, European managing director at Aventail. This view is supported by a recent report from Giga Information Group that states that the cornerstone of extranets will be the directory services that provide authorisation access to applications and data.

Currently, less than 1 0 percent of corporations deploying extranets today use a directory service, but by the end of 2000, Giga predicts that 70 percent of corporations will be utilising directories within their extranet infrastructure.

Simplifying User Management

Aventail ExtraNet Center's latest features enable deployments that are easily scalable for any number of extranet users. These new features include:

LDAP-enabled Authentication and Authorisation: Aventail ExtraNet Center v3.1 allows companies implementing various LDAP directories, including Netscape Directory Server, IBM SecureWay Directory and Lotus Domino, to authorise users and groups from an authoritative directory.

Aventail's LDAP implementation complements its existing support for NDS and Bindery, RADIUS, Windows NT Domain, UNIX Password Files and Security Dynamics' ACE/Server.

Increased Support for Emerging PKI Standards: Adding broader PKI support gives users more choices when using digital certificates. These include the ability to acquire a certificate via a browser (PKCS #1 2) and support for smart card and other device- based authentication (PKCS #1 1). Expanded support for PKI standards enhances Aventail's current support of authentication methods including RADIUS, CHAP, Windows NT Domain, NDS, Security Dynamics' SecurID, Hewlett-Packards' Authorization Server and x.509 certificates from VeriSign, Netscape, GTE and Microsoft.

Automated Configuration Updates: Utilising Aventail Customizer, Administrators can easily configure and distribute prepackaged clients via e-mail, FTP, HTTP or application deployment products such as Microsoft's SMS. After deployment, Aventail's AutoUpdate allows new configuration files to be installed automatically without user intervention at an interval set by the administrator.

"Aventail focuses on the needs of major enterprises building production-ready extranets," said Aventail's Colin Tankard. "Directory and PKI are large investments with strategic implications; we allow organisations to bring those investments to bear when collaborating with their extranet partners."

Pricing and Availability

Exhibit H

August 9, 1999 Aventail Press Release

HighBeam RESEARCH

Aventail Ships Directory-enabled Extranet Solution; Aventail Extranet Center V3.1 Available At www.aventail.com.

Publication: **Business Wire** Publish date: **August 9, 1999**

SEATTLE--(BUSINESS WIRE)--Aug. 9, 1999--

Aventail Corporation, the leading provider of Extranet Management and Security (EMS) solutions, announced today that they have shipped the latest versions of its award-winning product, Aventail ExtraNet Center(tm).

This latest offering simplifies extranet user management by including broader support for Public Key Infrastructure (PKI) and Lightweight Directory Access Protocol (LDAP)-enabled directories as well as automatic client updating. With these enhancements, Aventail has greatly simplified how large multi-enterprise organizations deploy and manage world-class extranets.

"I was quite impressed with the latest version of Aventail ExtraNet Center and its ability to seamlessly integrate with various LDAP directories and PKI environments," stated Ken Aull, Technical Fellow for TRW. "Aventail ExtraNet Center is a perfect tool for any enterprise organization conducting business-to-business commerce and collaboration. Aventail's standards-based solution reassures corporations that their extranet will work now as well as in the future."

Simplifying User Management

Aventail ExtraNet Center's latest features enable deployments that are easily scalable for any number of extranet users. These new features include:

-- LDAP-enabled Authentication and Authorization: Aventail ExtraNet

Center v3.1 allows corporations implementing various LDAP

directories, including Netscape (NYSE:AOL) Directory Server, IBM

(NYSE:IBM) SecureWay Directory, and Lotus Domino, to authorize

users and groups from an authoritative directory. Aventail's LDAP

implementation complements its existing support for NDS and

Bindery, RADIUS, Windows NT Domain, UNIX Passwrd Files, and

Security Dynamics' ACE/Server. -- Increased Support for Emerging PKI Standards: Adding broader PKI

support gives users more choices when using digital certificates.

These include the ability to acquire a certificate via a browser

(PKCS #12) and support for smart card and other device-based

authentication (PKCS #11) such as SPYRUS' Rosetta Smart Card. The

expanded suppourID, Hewlett-Packards' (NYSE:HWP) Authorization Server, and

x.509 certificates from VeriSign (Nasdaq:VRSN), Netscape

(Nasdaq:NSCP), GTE (Nasdaq:GTE), and Microsoft (Nasdaq:MSFT). -- Automated Configuration Updates: Aventail ExtraNet Center also

includes the ability to easily configure, distribute, and

automatically update client configuration files. Utilizing

Aventail Customizer(tm), administrators can easily configure and distribute pre-packaged clients via e-mail, FTP, HTTP, or application deployment products such as Microsoft's SMS. After deployment, Aventail's AutoUpdate(tm) allows new configuration files to be automatically installed without user intervention at an interval set by the administrator. This easy-to-use administrative tool reiterates Aventail's efforts in providing a transparent client for business partners, suppliers, consultants, and customers.

Pricing and Availability

Aventail ExtraNet Center is currently shipping on Windows NT and Solaris. Additional platform support will be available at the end of August.

Aventail ExtraNet Center is available through Aventail's worldwide sales team and Aventail Extranet Advantage VAR partners as well as leading security vendors such as Hewlett-Packard and BullSoft. Pricing begins at $10,000 depending on client requirements.

A Comprehensive Solution for Extranet Management and Security

Aventail ExtraNet Center is a client/server software solution that includes integrated encryption, authentication and authorization services using the popular IETF standards SSL and SOCKS v5.

Aventail ExtraNet Center has the ability to seamlessly integrate into any existing infrastructure, making it less costly to install and easier to implement and support than other extranet solutions. Aventail ExtraNet Center works with any IP-based application, including legacy host, mainframe, Java, CORBA-based, custom corporate, and client/server applications from vendors such as SAP (NYSE:SAP), BAAN (Nasdaq:BAANF), Oracle (Nasdaq:ORCL), and PeopleSoft (Nasdaq: PSFT). Aventail ExtraNet Center can also traverse any firewall, such as Check Point Software Ltd.'s (Nasdaq:CHKP) Firewall-1/VPN-1, AXENT Technologies' (Nasdaq:AXNT) Raptor Firewall, and IBM's (NYSE:IBM) eNetwork Firewall.

About Aventail Corporation

Founded in 1996, Aventail has quickly emerged as the leading provider of EMS solutions for the Global 2000. Aventail's solutions allow organizations to securely extend their enterprise resources to strategic partners, suppliers, customers, consultants and other key individuals over public IP networks.

Leading corporations are using Aventail's solutions to help them increase their competitive advantage, raise profits, and leverage investments in existing and future enterprise systems. Aventail's solutions are currently deployed at companies such as Aetna, Bear Stearns, Kodak, Hewlett-Packard, IBM, IKON, Marriott, and Xerox. With a strong reputation for providing highly secure and easy-to-manage software solutions, Aventail has received numerous industry awards from publications and industry analyst firms such as Giga Information Group, InfoWorld, Network Computing, LAN Times, BYTE Magazine, Software Digest, and Computer Reseller News.

Aventail Corporation is privately held and headquartered in Seattle, Washington. For more information on the company or to download a trial version of Aventail ExtraNet Center, please visit www.aventail.com, or contact the company directly at 206-215-1111, 877-AVENTAIL, or info@aventail.com. Information on Aventail can also be obtained through Yahoo (Nasdaq:YHOO), Infoseek (Nasdaq:SEEK), Lycos (Nasdaq:LCOS), and Excite (Nasdaq:XCIT).

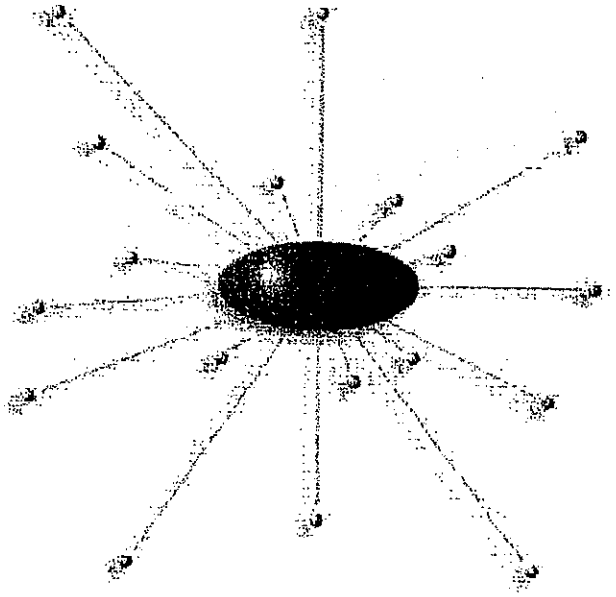
Aventail is a registered trademark of Aventail Corporation. Aventail ExtraNet Center, Aventail Customizer and Aventail AutoUpdate are trademarks of Aventail Corporation. All other trademarks are the property of their respective owners.

EXHIBIT I

AVENTAIL CONNECT ADMINISTRATOR'S GUIDE
v3.1/v2.6

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.

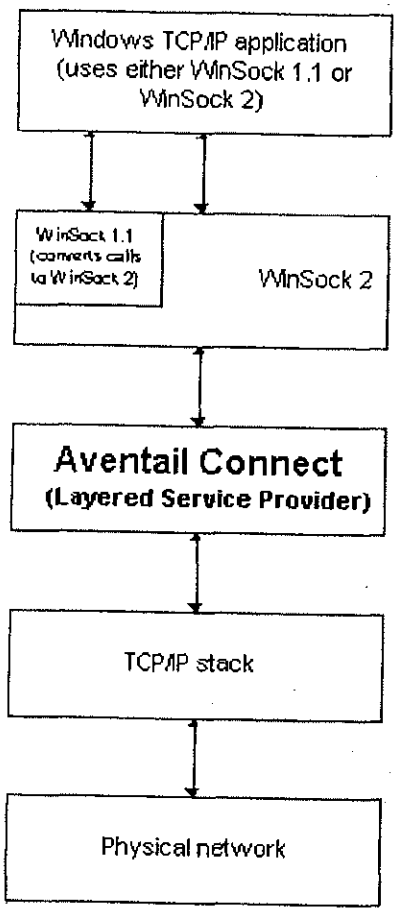
WinSock Connection to a Remote Host

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.

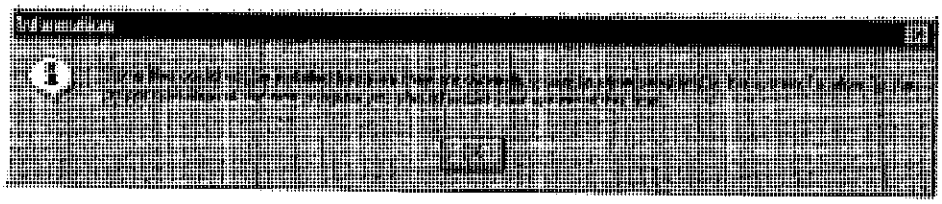
- **CD**: The CD contains the Aventail Connect setup program, `setup.exe`. The setup program allows for an administrative setup. It also contains the *Administrator's Guide* and the *User's Guide* in the `\docs` directory, formatted for Adobe® Acrobat Reader.
- **Network-delivered Source Media**: The 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.

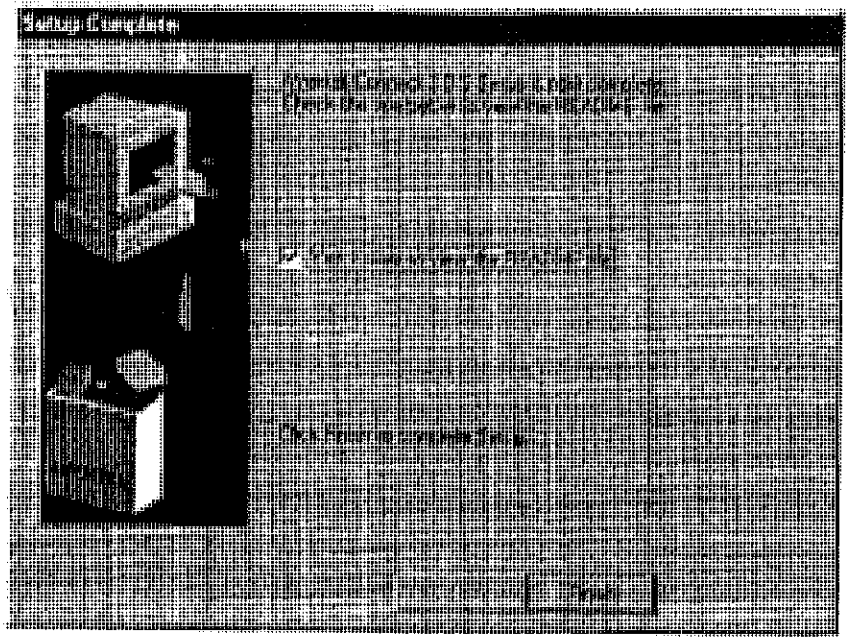
   The Aventail Connect Installation Wizard then guides you through the process of installing the Aventail Connect application.

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.*

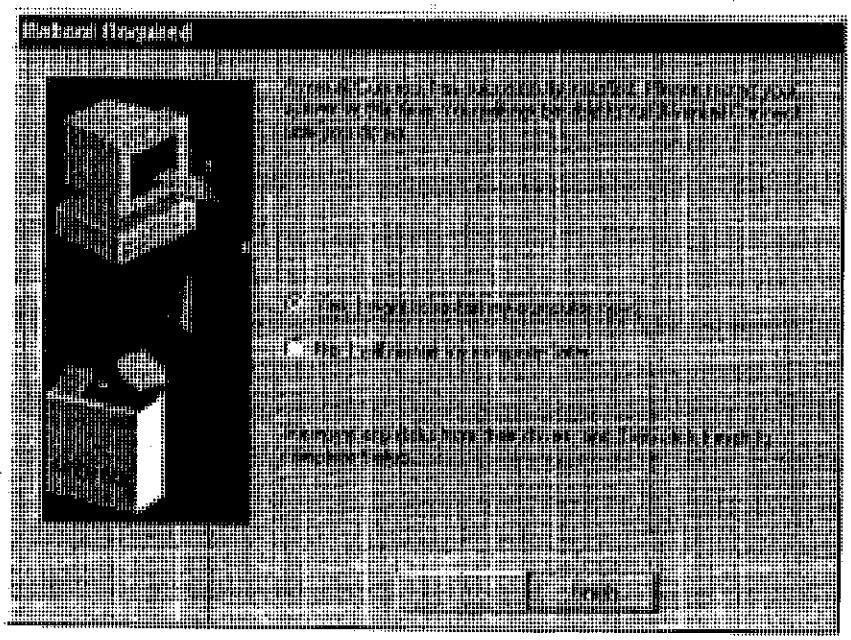
2. At the end of the setup program, you can select **Yes, I want to view the README file** in the **Setup Complete** dialog box. This opens the `readme.txt` file, which contains the latest information on Aventail Connect.

-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.

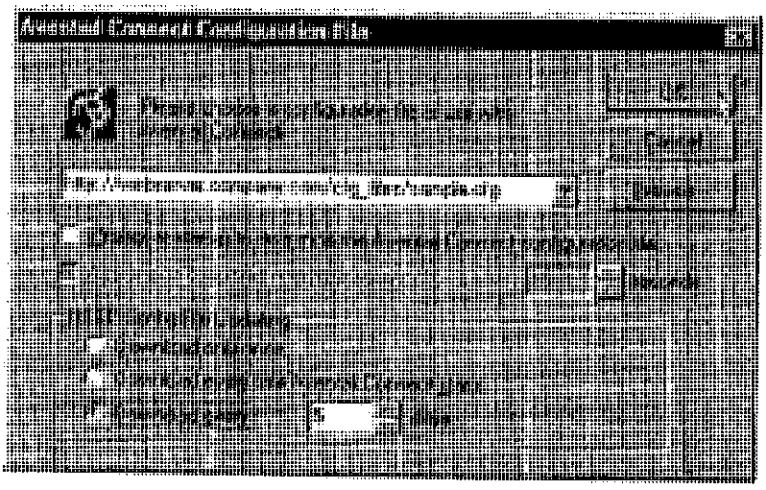
Aventail Connect keeps a temporary local copy of the remote configuration file in its program directory, with the filename _ashttpX.cfg, where X is a number between 0 and 9. Keeping a local copy of the remote configuration file allows the connection to the Web server to be proxied (with authentication 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.

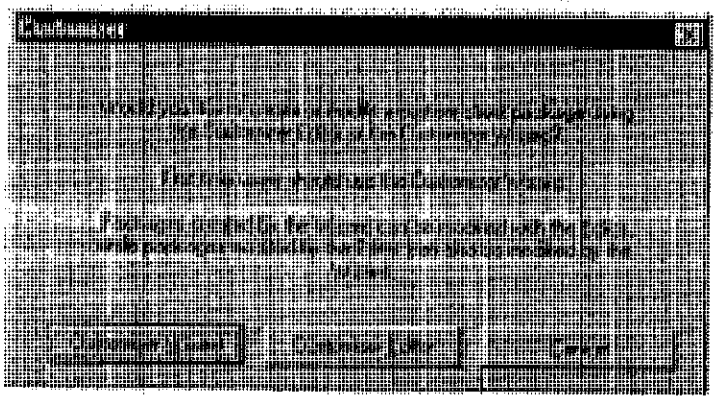
RUNNING CUSTOMIZER

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.

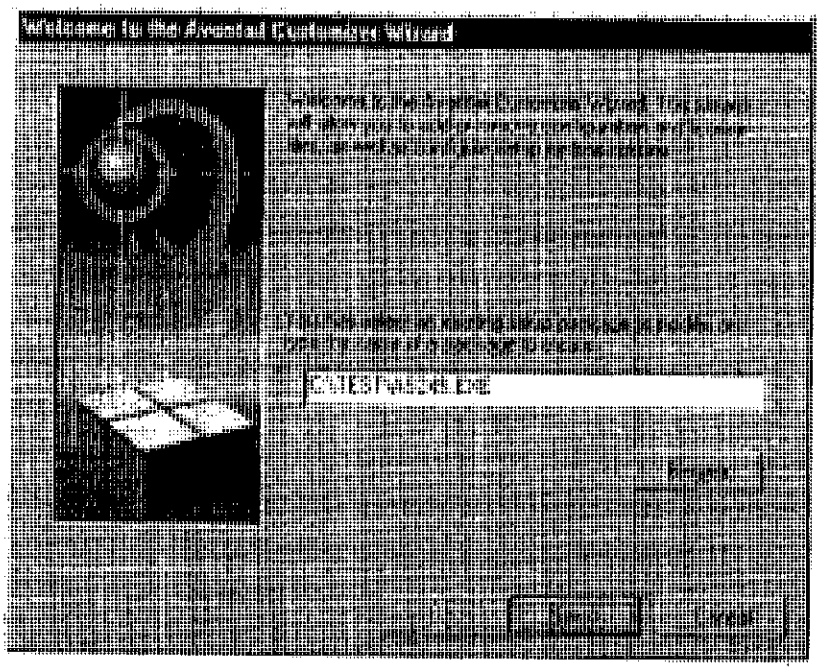
When you run Customizer, you will be prompted to select either the Customizer Wizard or the Customizer Editor.



- **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.



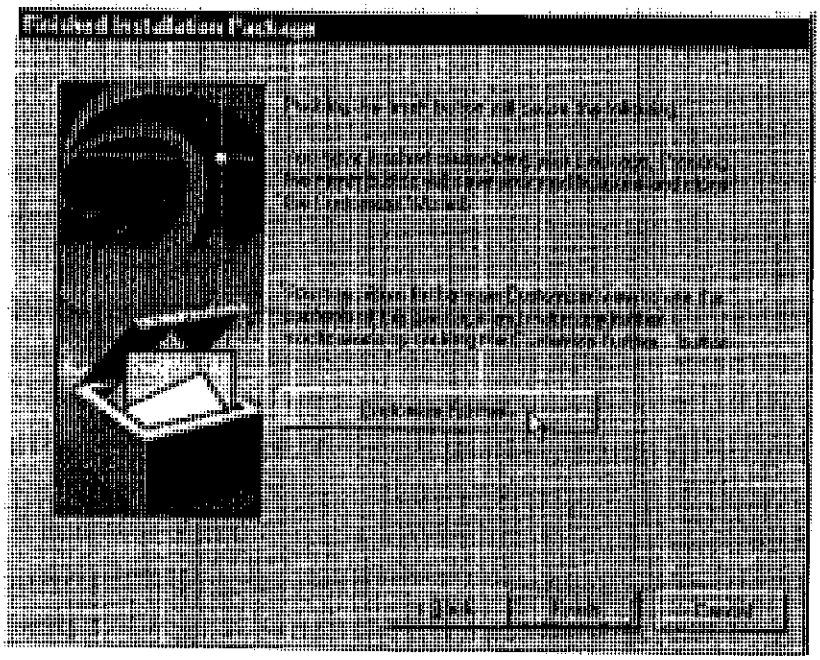
After you have specified the pathname of the package, the Customizer Wizard will prompt you to:

- 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.

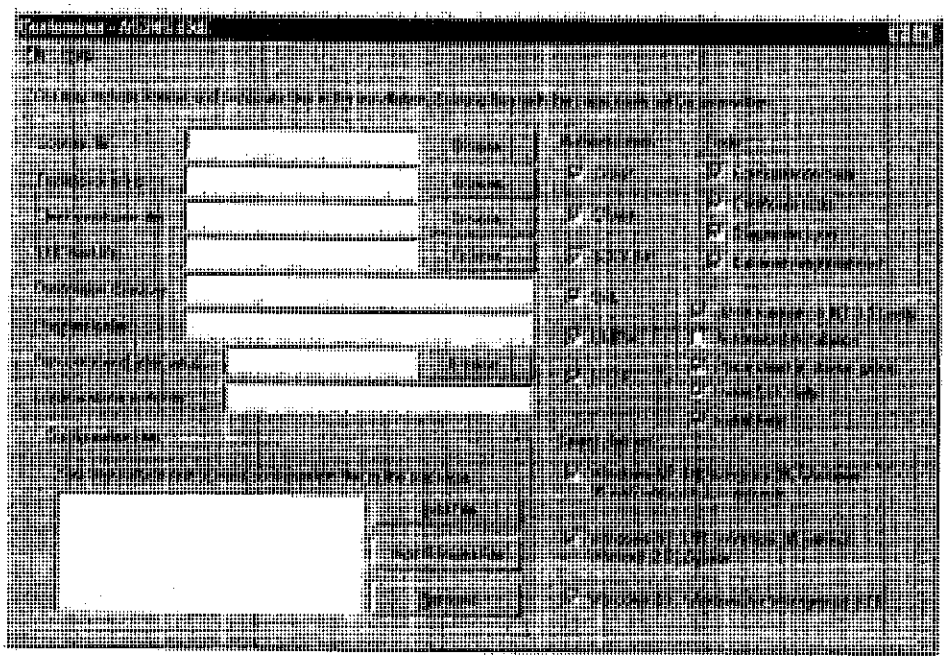
After entering or modifying the package information, the **Finished Installation Package** dialog box appears.



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-

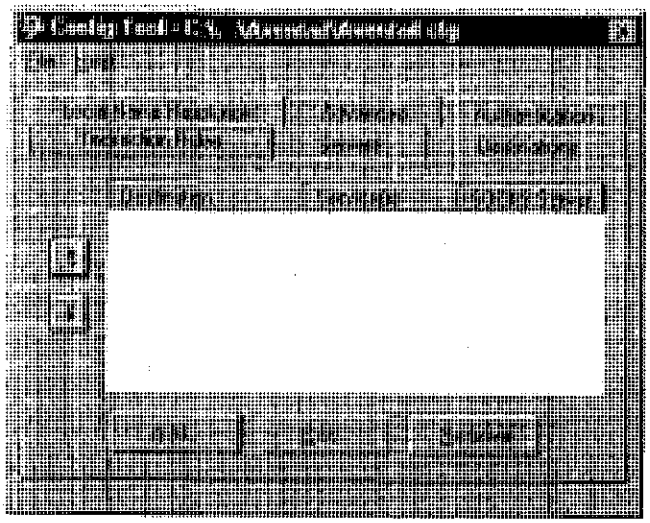
Right-click the **Aventail Connect** icon in the taskbar and click **Config Tool** (Windows 95, Windows 98, or Windows NT 4.0 programs menu option), or double-click the **Config Tool** icon in the Aventail Connect program group (Windows 3.1, Windows for Workgroups 3.11, or Windows NT 3.51).

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

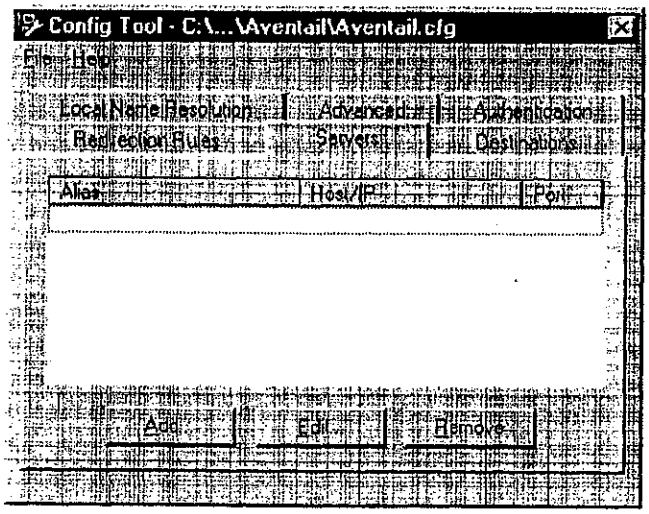
- With the newly modified configuration file open, select **Make Active** from the **File** menu of the Config Tool

  -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.*

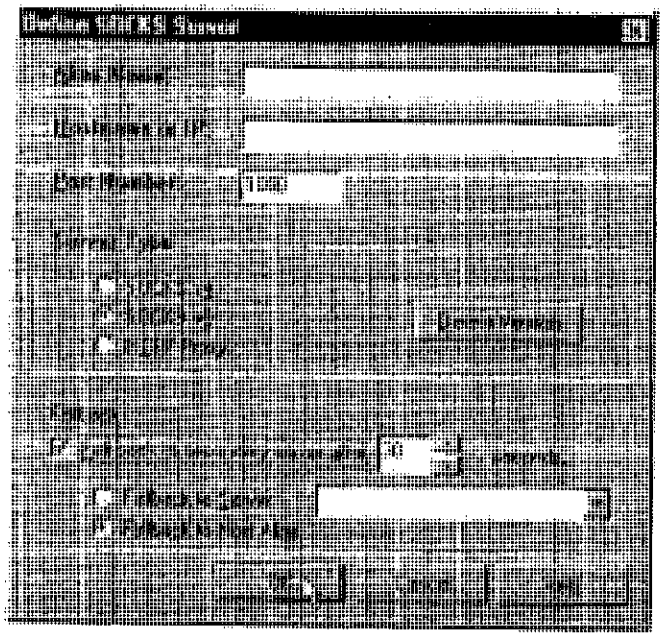
NOTE: *Aventail Connect can fall back to only one server. For example, Aventail Connect could fall back from Server A (primary server) to Server B (secondary server). Aventail Connect could not, however, fall back from Server A to Server B to Server C.*

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**.

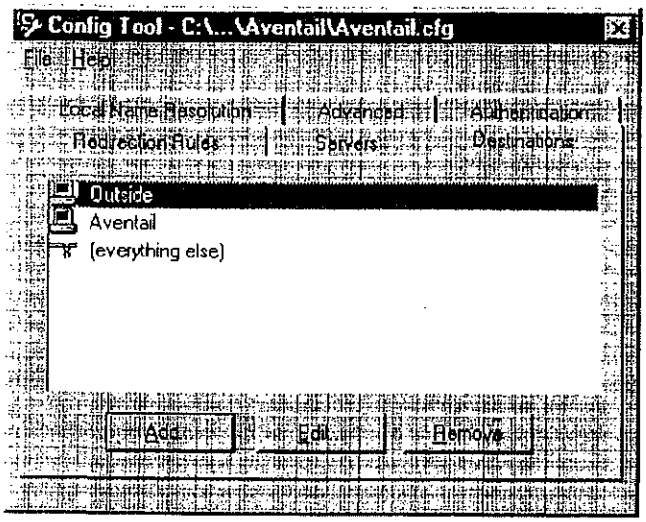
To remove an extranet (SOCKS) server definition

- 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:

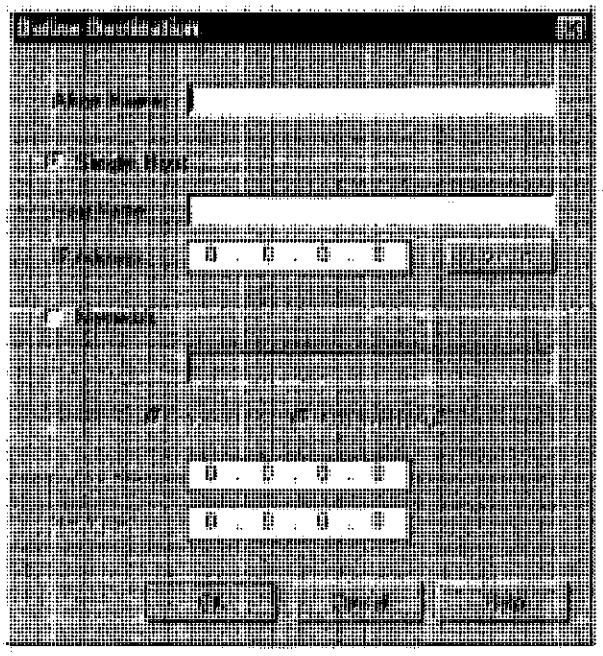
*`e*.in.aventail.com` **matches** `extra.in.aventail.com`*
*`e*.aventail.com` **does NOT match** `extra.in.aventail.com`*

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

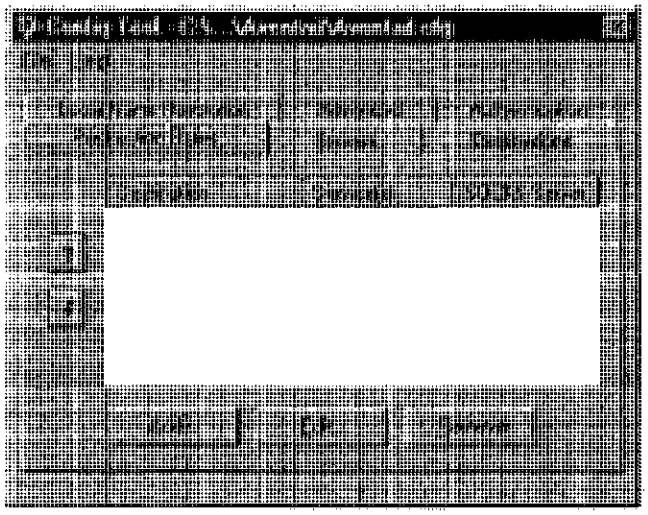
- Select the destination you want to remove and click **Remove**.

  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.

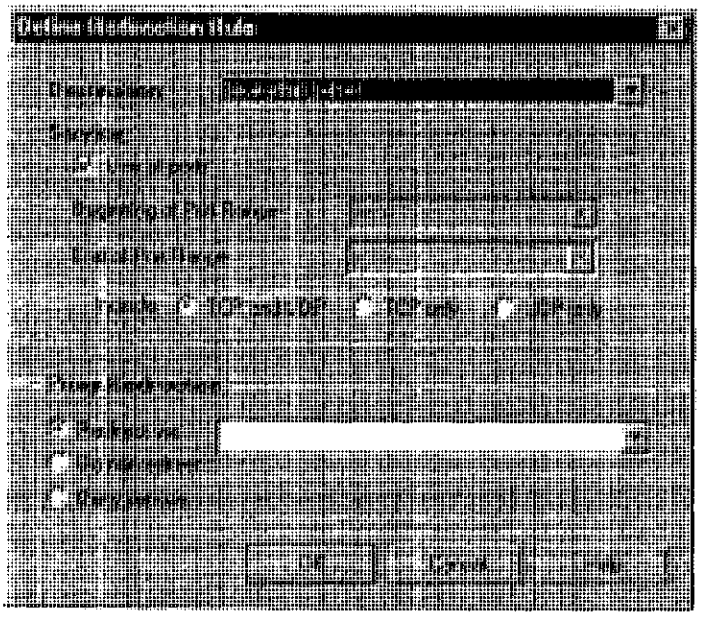
To add a redirection rule

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.

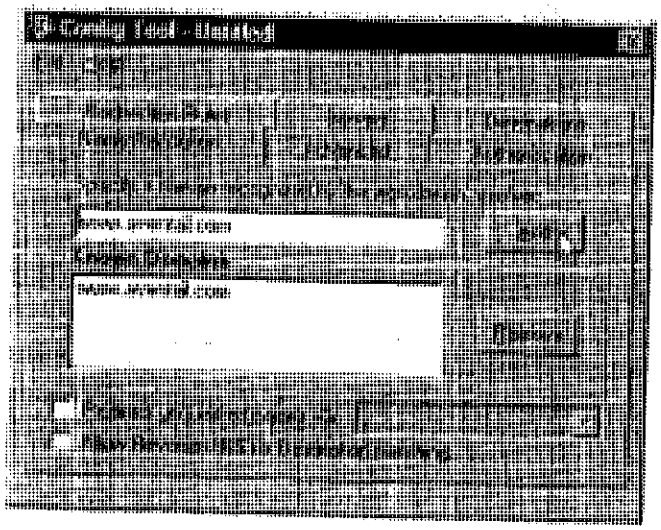
DEFINE NAME RESOLUTION

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.

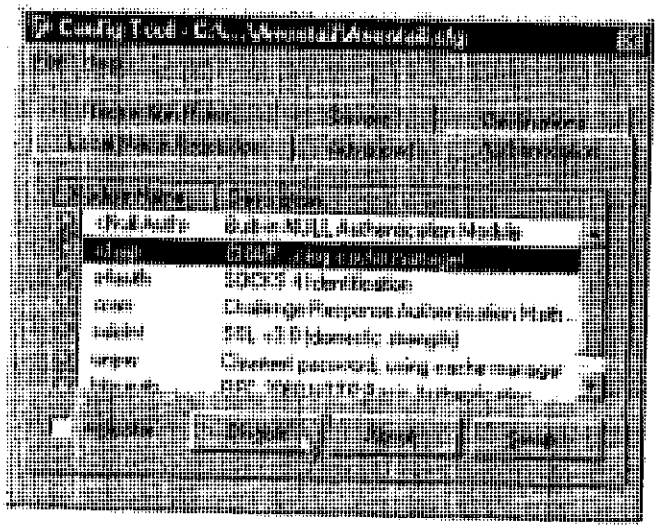
NOTE: Not all versions of Aventail Connect have encryption enabled.

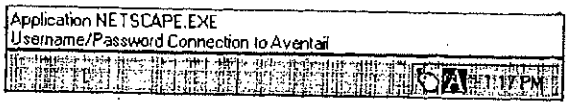
The current Aventail Connect authentication modules are SOCKS v4 Identification, Username/Password, Challenge Handshake Authentication Protocol (CHAP), Challenge Response Authentication Method (CRAM), Secure Sockets Layer (SSL), and HTTP Basic (username/password). Each of these authentication modules 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.

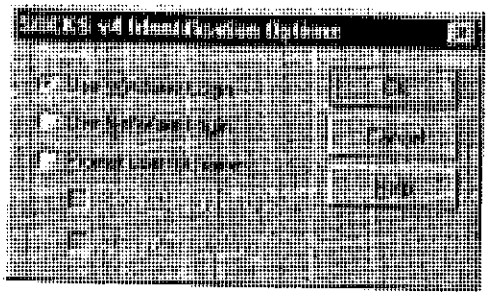
To configure the SOCKS 4 Identification module

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**.

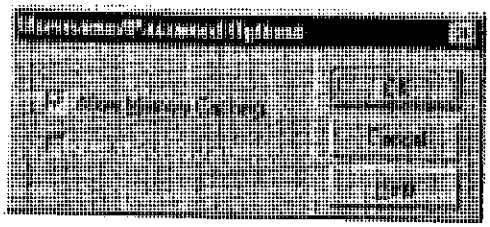
   The dialog box closes and the Config Tool reappears.

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**.

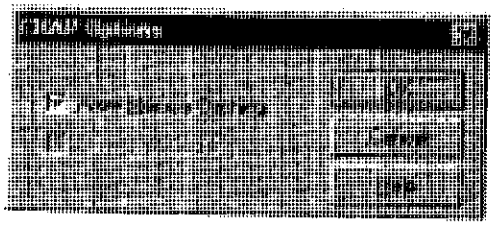
   The dialog box closes and the Config Tool reappears.

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.



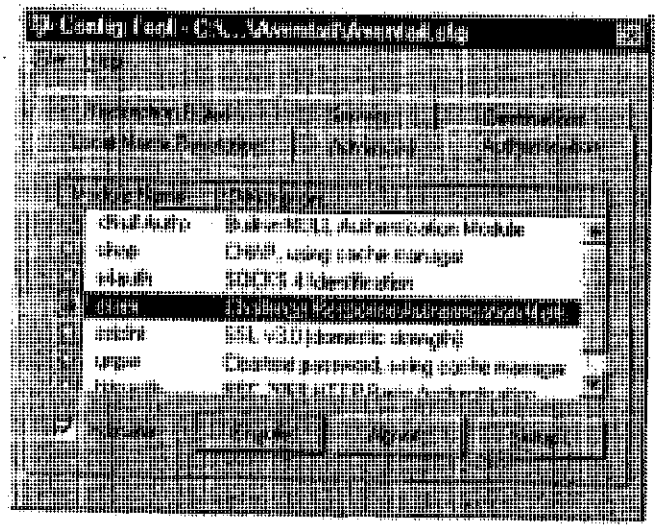
Field	Description
Allow memory caching	Stores credentials in memory for this session only. Cache is flushed upon restart; credentials must be reentered as prompted.
Allow disk caching	This option is currently unavailable. (Stores encrypted credentials on disk for future sessions.)

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.

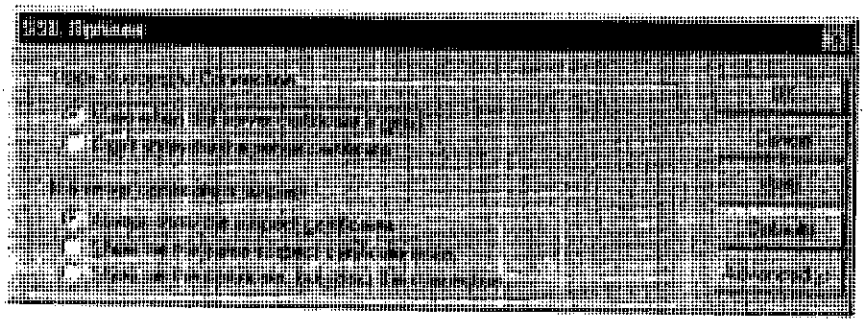
Certificates contain special integrity checks and electronic signatures that verify that the certificate is genuine, was issued by a certification authority, and was not tampered with. Anybody can issue a certificate that says anything; the client must know who issued the certificate, and have some trust 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 **sslcInt** (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.

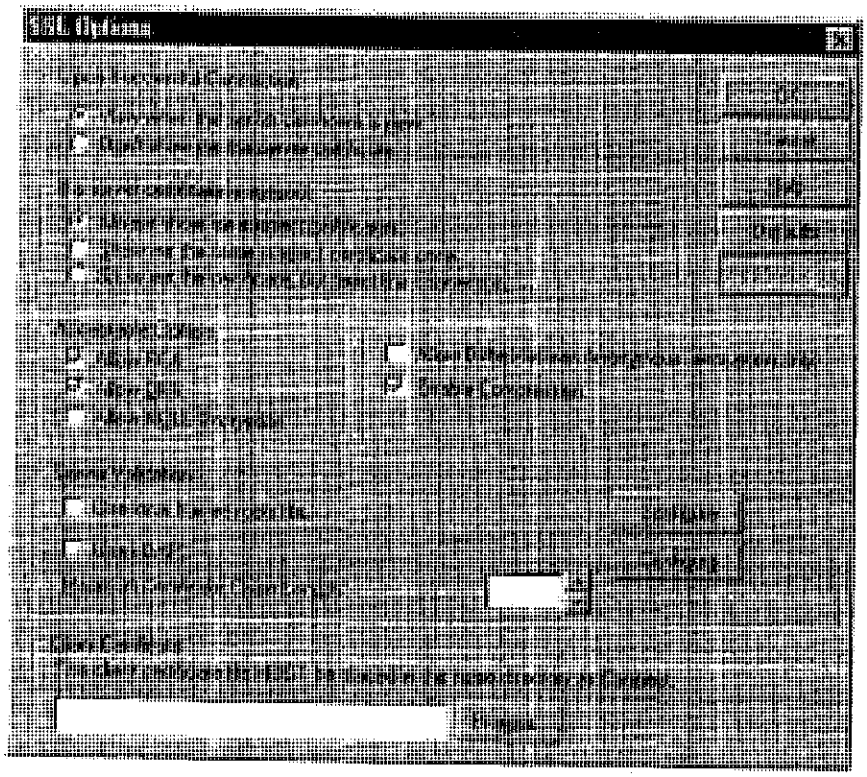
2. Select an action that Aventail Connect must take once it accepts the validity of the server certificate. (Under normal circumstances, the server will provide Aventail Connect with a certificate to match one of Aventail Connect's trusted roots, if any exist):
   - **View when the server certificate 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.

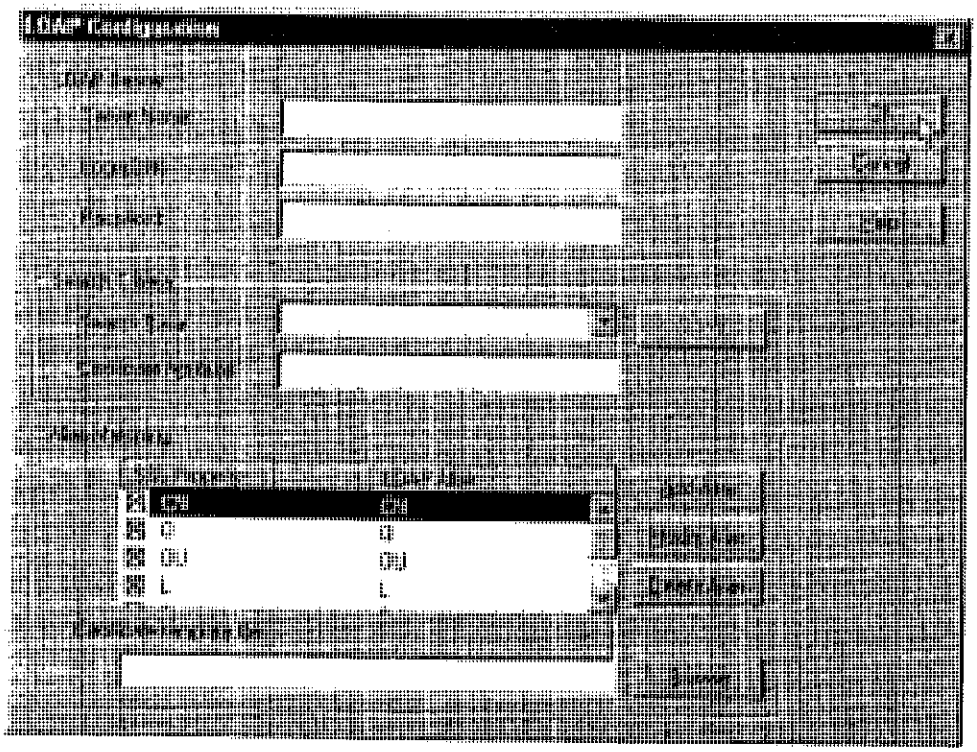
b. Enter the name of the trusted roots file, or click **Browse** to search for the file, and then click **OK**.

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.

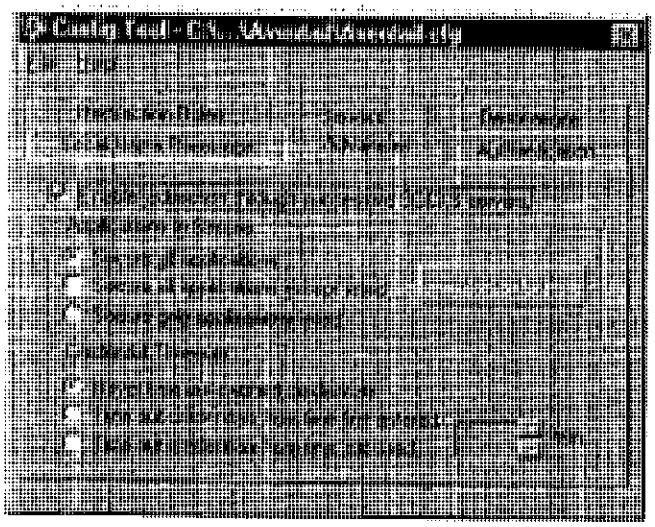
To configure PKCS #11 smart-card user authentication

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.

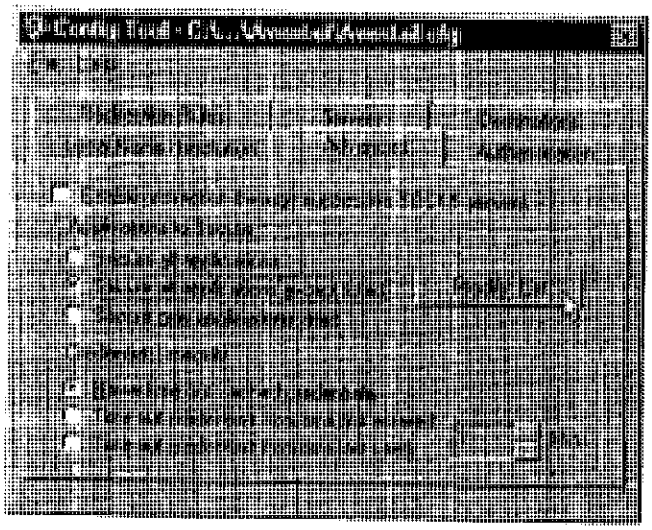
You can exclude or include specified applications in the Exclusion/Inclusion List. With the Exclusion/Inclusion List, you can secure all applications *except* those on the list, or you can secure *only* those applications on the list. The default setting is to secure (hook) *all* network applications.

Excluding Applications

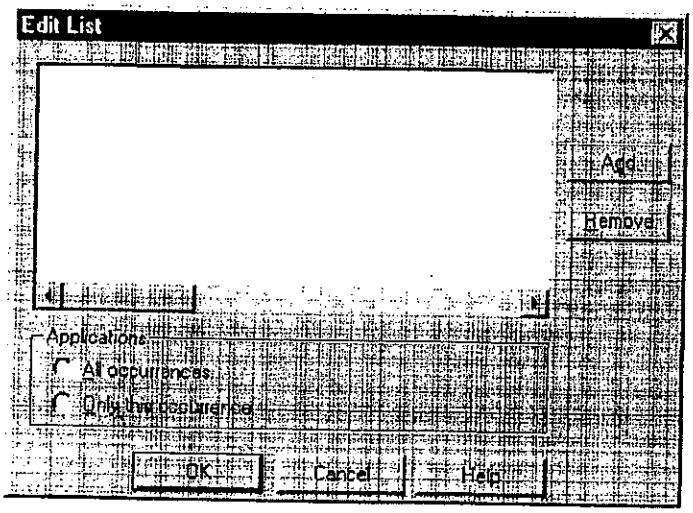
You can exclude specific applications through the Exclusion/Inclusion List. When you enable the "Secure all applications except listed" option, Aventail Connect will not proxy any applications that are on the Exclusion/Inclusion List.

To exclude an application

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

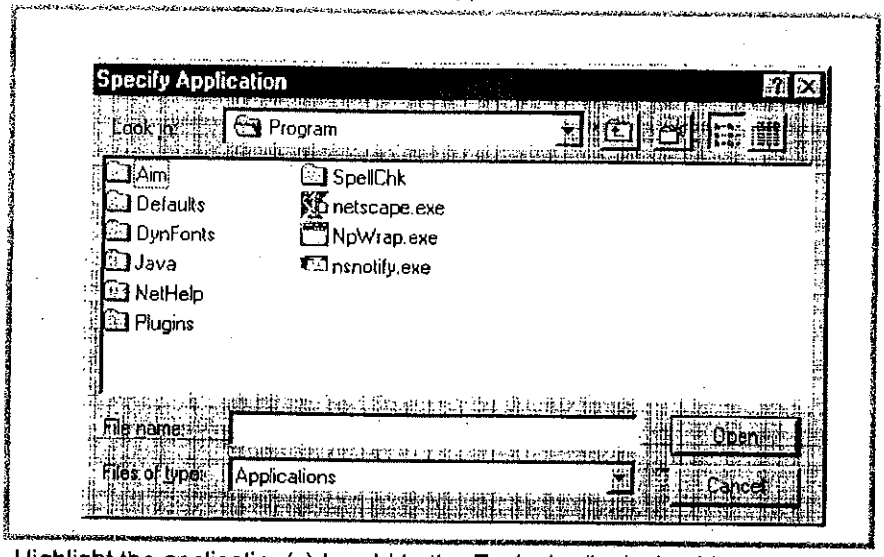


The **Edit List** dialog box appears.



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

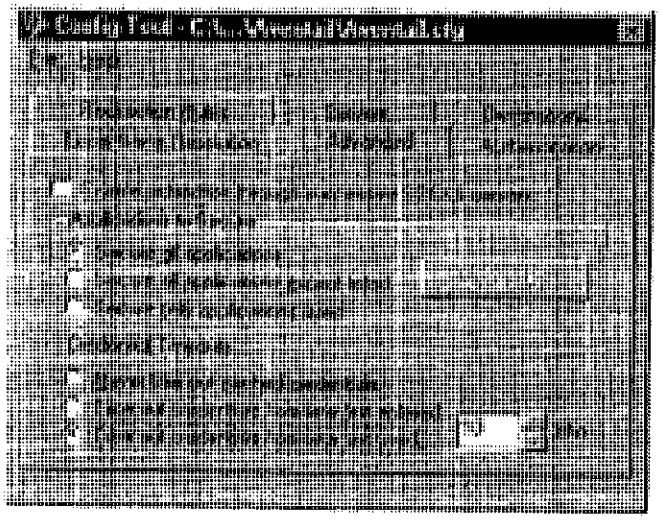
- On the **Advanced** tab, under "Applications to Secure," select **Secure all applications**.

*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).

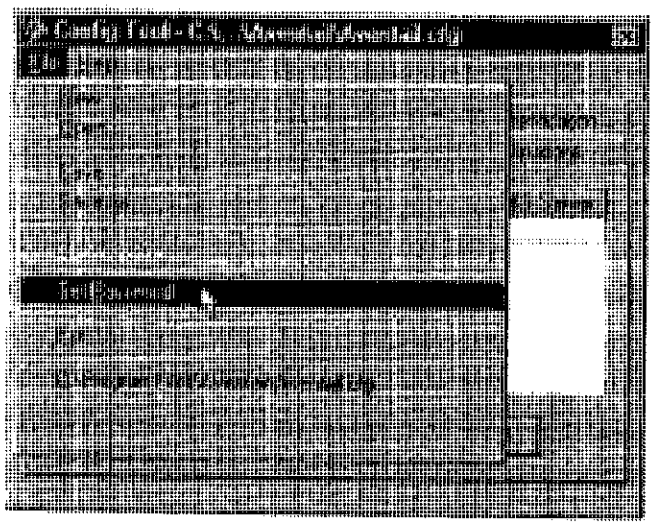
CAUTION: If your mail program is configured to check for e-mail at regular intervals, the mail-checking frequency must be longer than the credential cache timeout. For example, if your mail program is configured to check for mail every ten minutes, you should set the credential cache to less than ten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

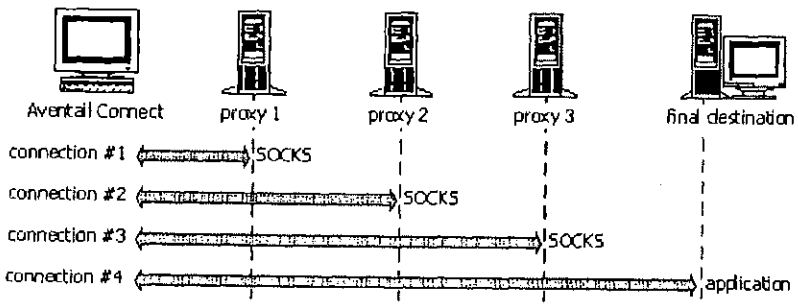
Using an HTTP proxy server to control outbound traffic eliminates the need to install a separate SOCKS server. This HTTP proxy can filter outbound connection requests and route those requests to the specified servers. MultiProxy supports RFC 2068 HTTP Basic (username/password) authentication. If your 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.

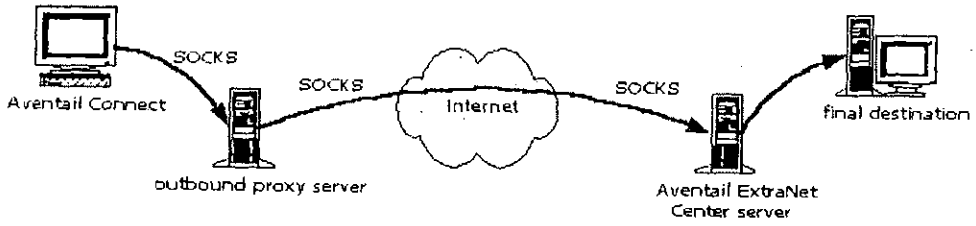
The steps for making a connection using MultiProxy are:

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-

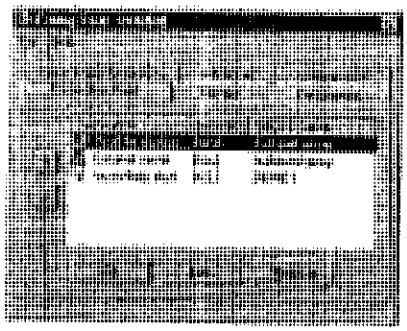
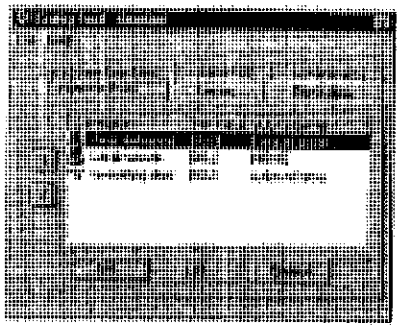
   To redirect all Internet traffic (including extranet traffic): Create a destination ("Local network," the network local to Aventail Connect).

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.")

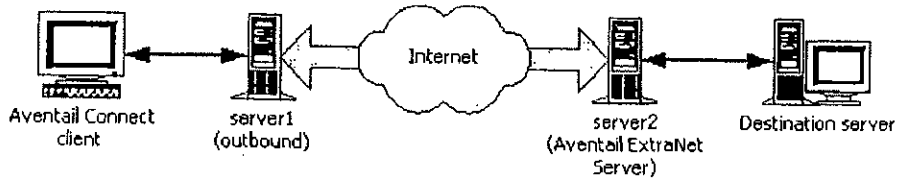
Redirect only extranet traffic	Redirect all Internet traffic (including extranet traffic)
	
Redirect only the extranet traffic through the outbound proxy. Leave all other traffic alone.	Redirect all Internet traffic through the outbound proxy. Leave only "Local network" traffic alone.

PROXY CHAINING

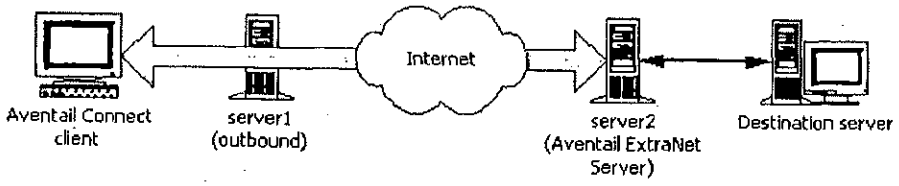
Proxy chaining is an Aventail ExtraNet Server feature. With proxy chaining, Aventail ExtraNet Servers forward connections for certain destinations to other proxy servers.

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.

PROXY CHAINING: Server1 appears as a user to server2.

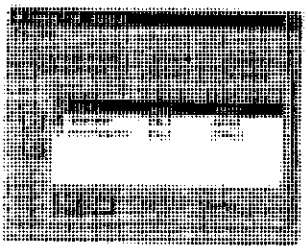
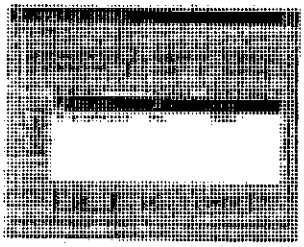


MULTIPROXY: The user authenticates with server2 directly.




Authenticated and encrypted tunnel

In MultiProxy, an authenticated and encrypted tunnel exists between the client and the Aventail ExtraNet Server.

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.

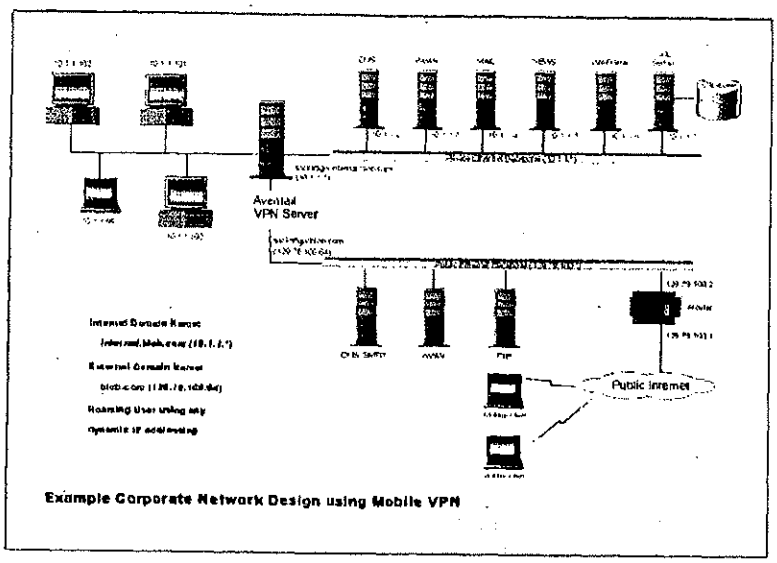
- **Microsoft Proxy Server 2.0:** Follow the Microsoft instructions at **http://support.microsoft.com/support/kb/articles/q184/0/28.asp**. You must modify a registry setting with `regedt32.exe`. (`regedit.exe` will not work; you must use `regedt32.exe`.)
- **Netscape Proxy Server 3.5:** Add the following 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.

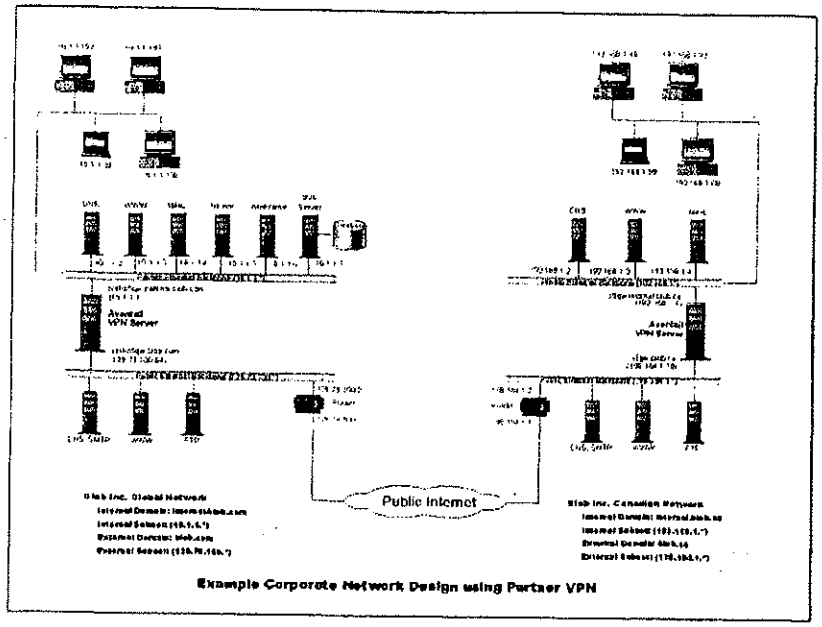
The Aventail ExtraNet Server in our example, has two network adapters configured to use the internal IP address of 10.1.1.1 and an external address of 129.79.100.64.

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.

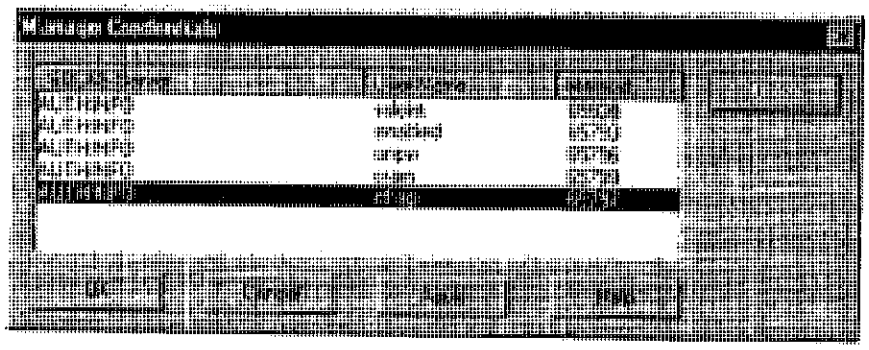
ABOUT

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-

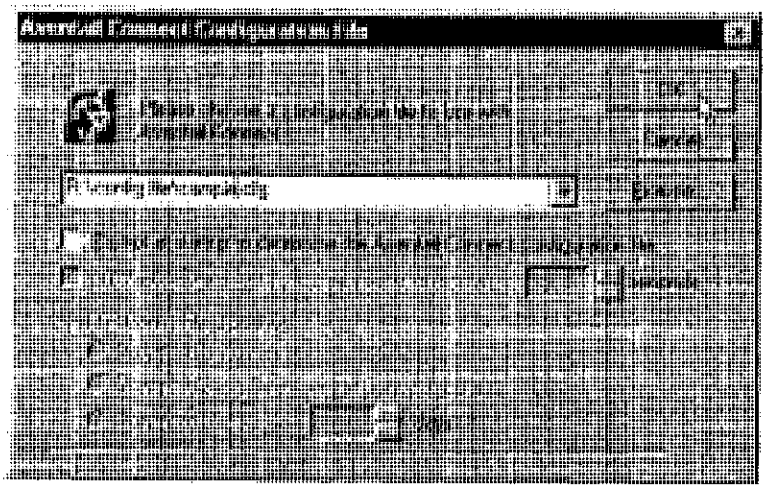
- Click **Cancel** to close the dialog box without accepting any changes you might have entered.

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.

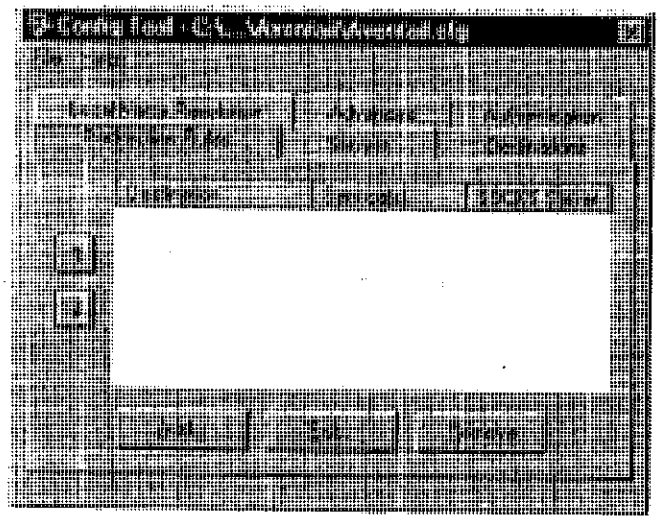
Menu Command	Function
Config Tool	Runs the Config Tool. (Optional)
Logging Tool	Runs the Logging Tool. (Optional)
S5 Ping	Runs the ping and traceroute utilities. (Optional)

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,

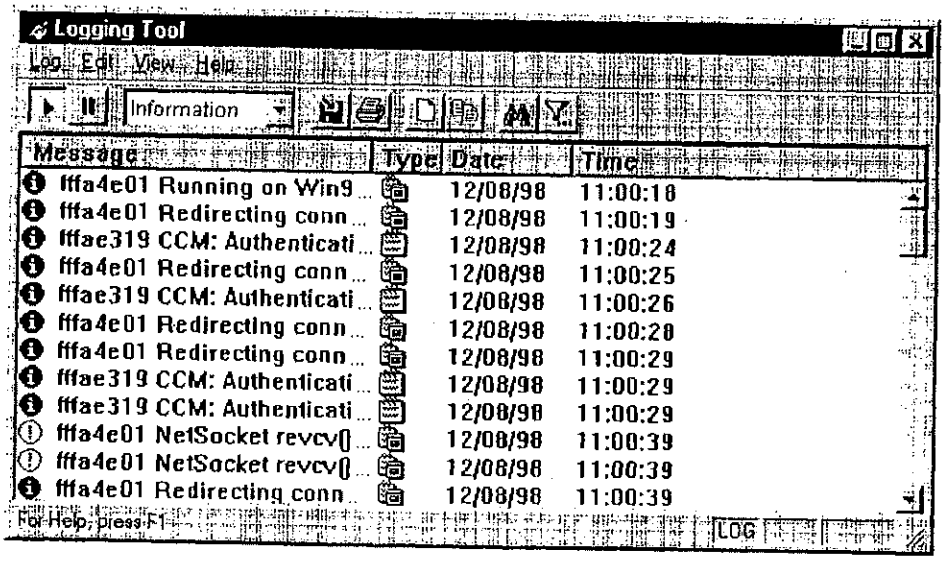
and e-mail it to them as an attachment. Log files are also useful when running Aventail Connect for the first time, to ensure that network traffic is being routed properly.

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-

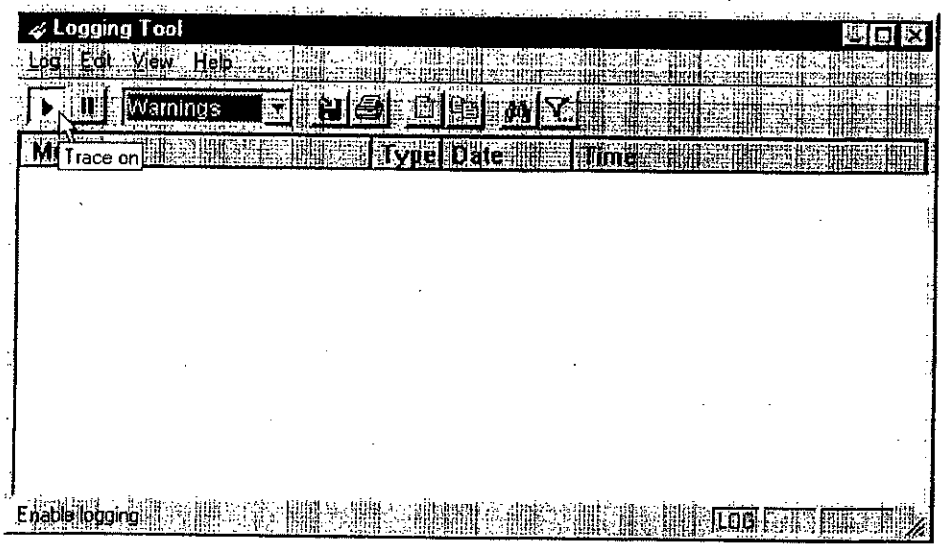
Select one of the five levels from the drop-down list on the toolbar.

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).

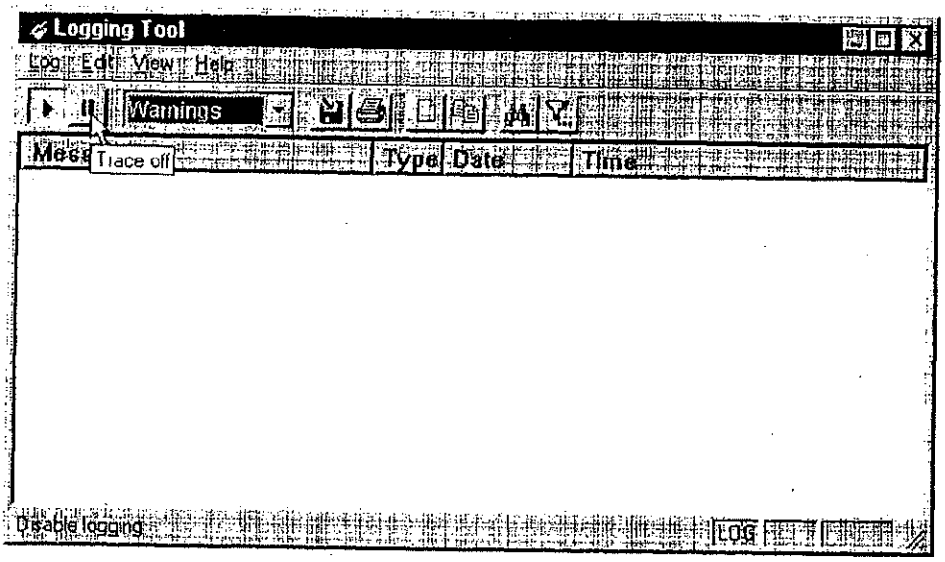


The log window will now record and display trace information as it is generated by Aventail Connect. You can tell when the trace function is active because messages are scrolling down the screen and the **Trace On** button is depressed.

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

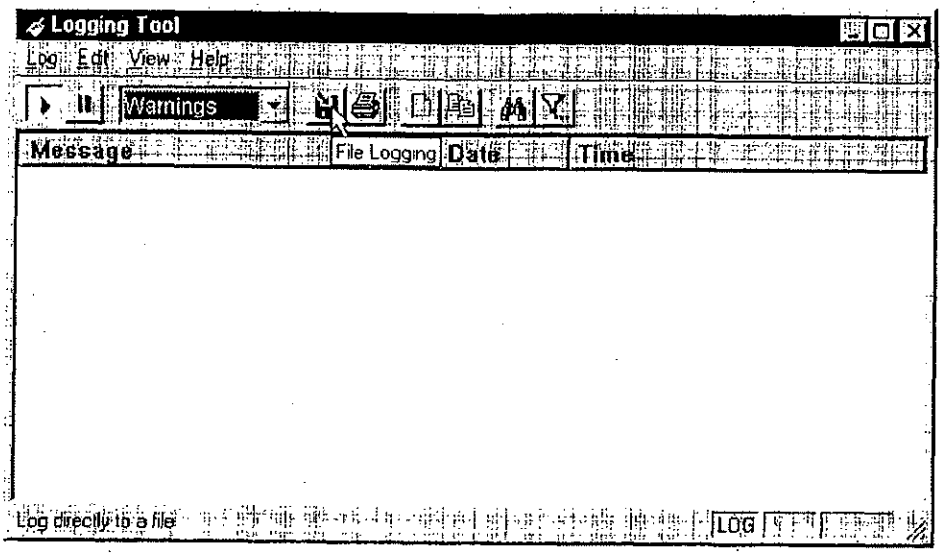
The Logging Tool allows you to append each new message to the end of a .LOG file during the trace, or save the contents of the log window at any time. If you save during a trace, Aventail Connect will append messages to the log file until you stop the log function. You must save data in the log window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

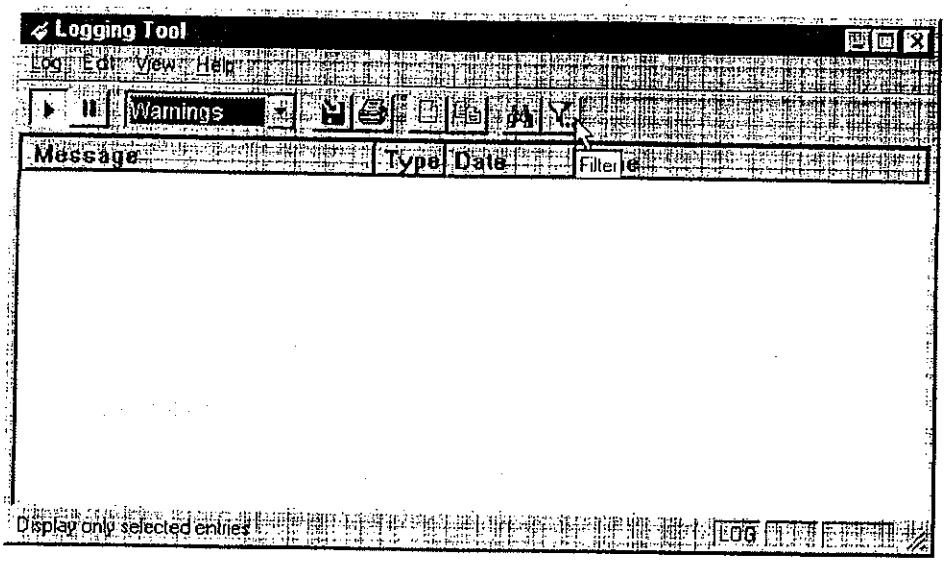
To filter messages in the log window

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.

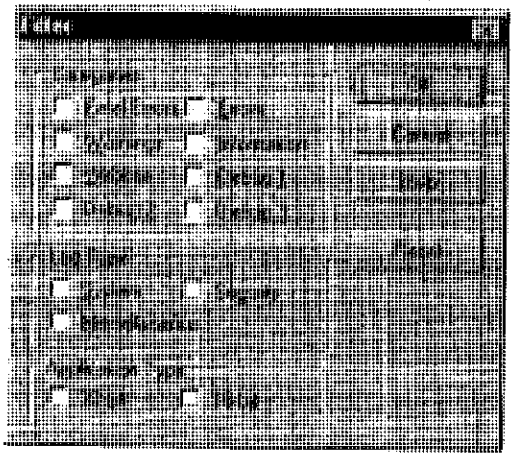
1. On the **View** menu, click **Filter Messages** to display the **Filter** dialog box

-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

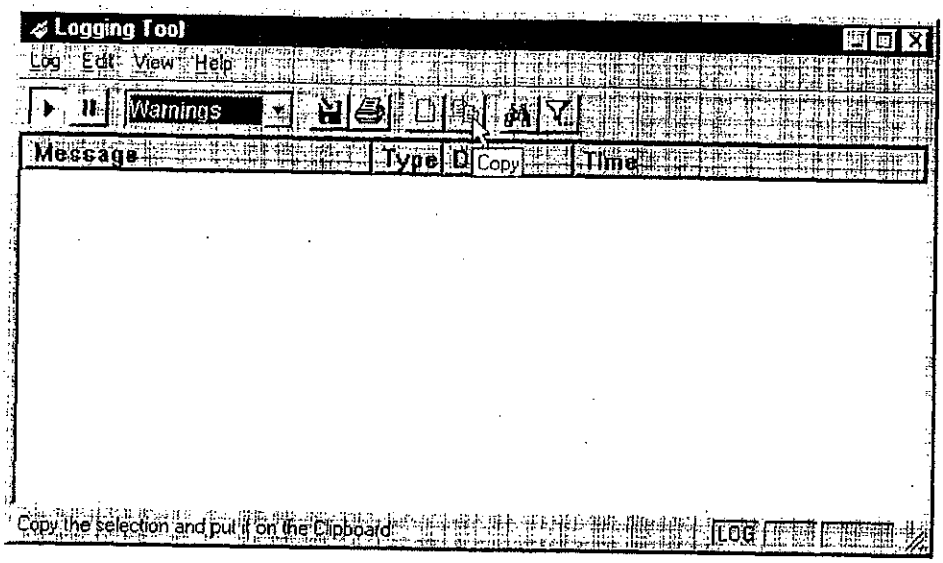
The display font and window options can be customized as follows:

- 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**.

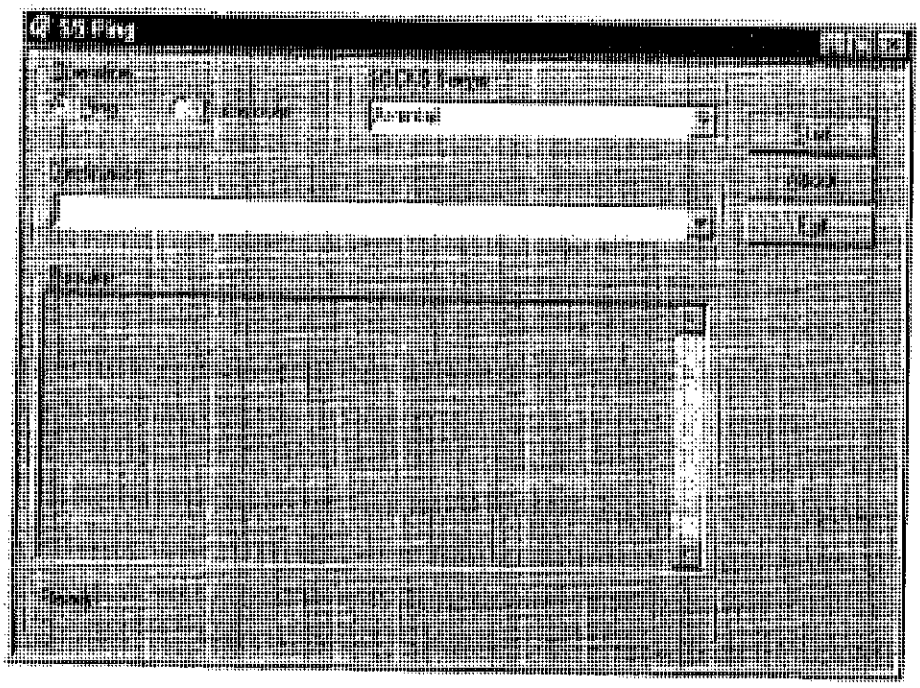
-OR-

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., ė) 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-

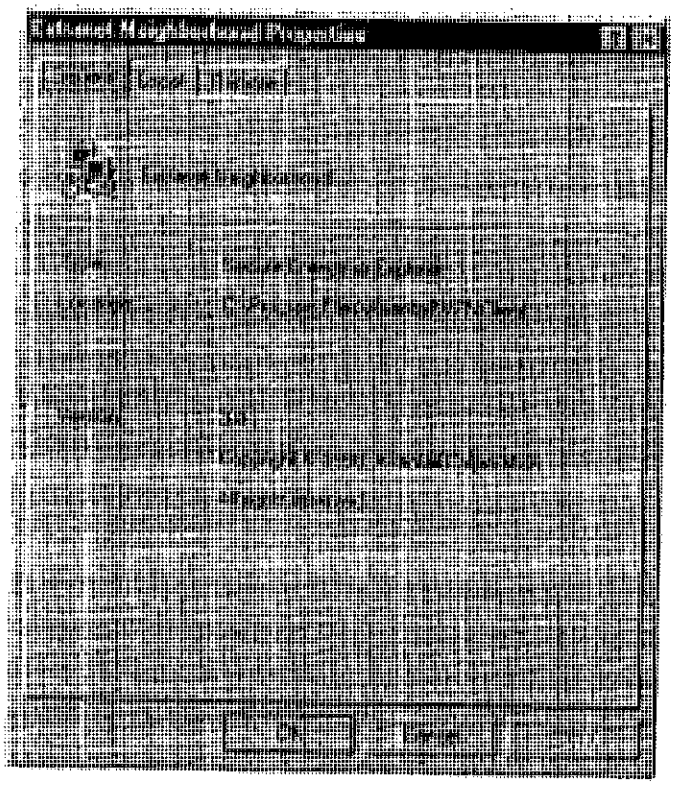
- Specify some computers in a local hosts file and others in a remote hosts file.

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.

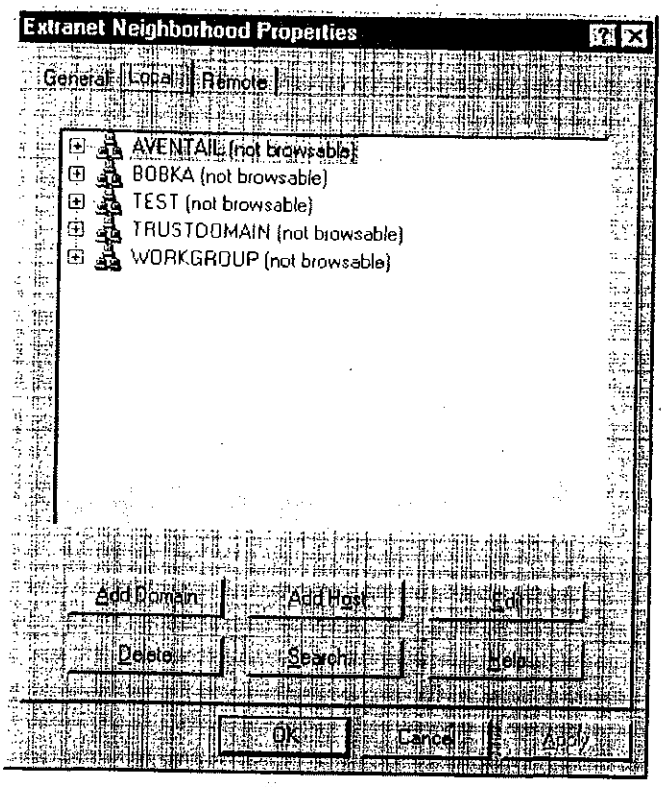
THE GENERAL TAB

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

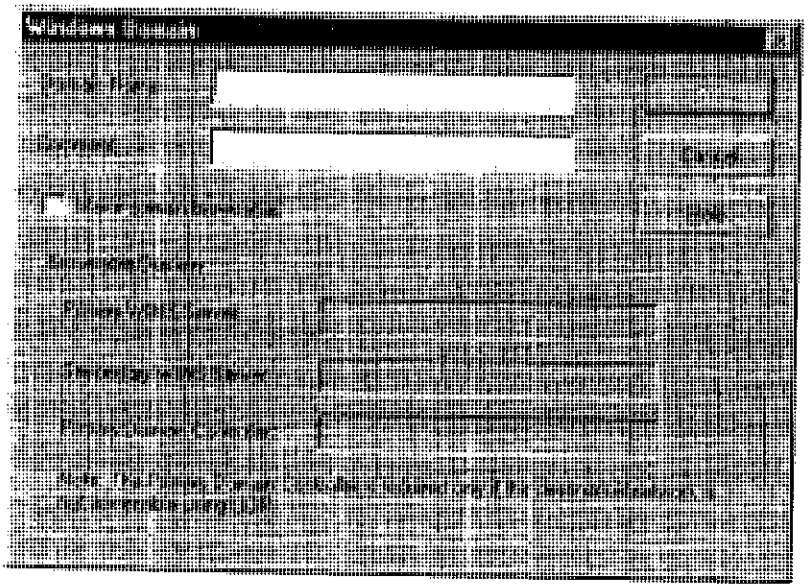
If the controls in this window are disabled (dimmed), then the hosts file has been "locked." The network administrator determines which, if any, hosts files are locked.

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.

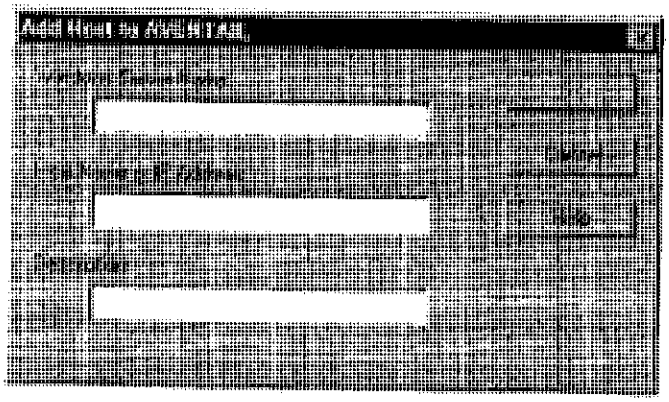
To make the specified domain "browsable," enter WINS server information in the **Primary WINS Server** box and, if desired, the **Secondary WINS Server** box. In both of these boxes, you can enter either the server's IP address or its fully qualified host name. You must also select the **Make domain 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.

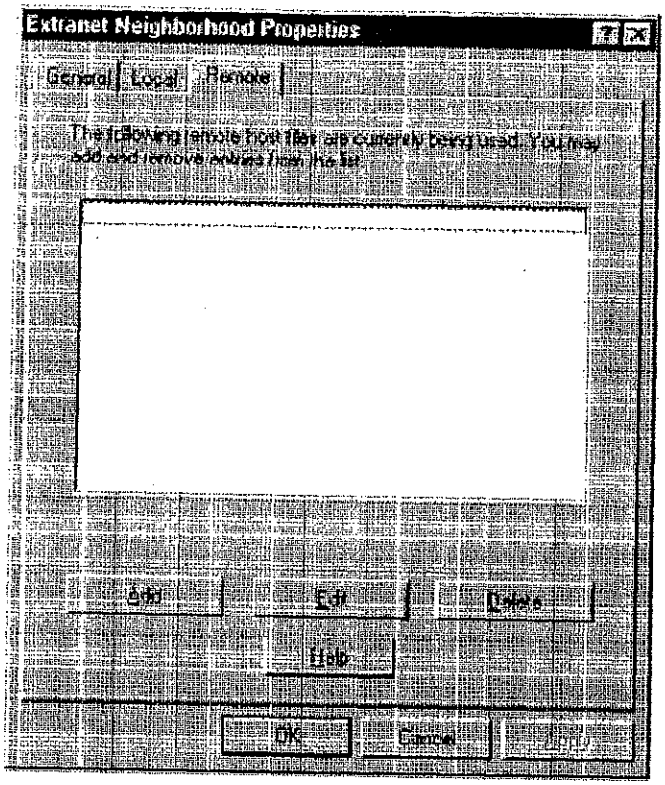


Aventail Connect automatically places hosts within the domain that is selected when you click **Add Host**. Select the correct domain before clicking **Add Host**. You must specify a domain before you can add hosts to that domain.

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.

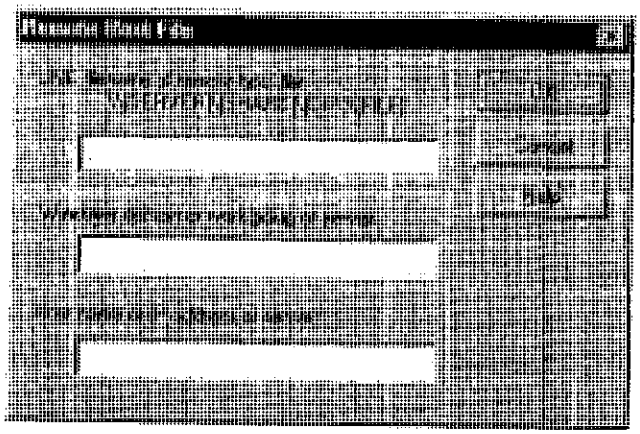
The most common configuration is one remote hosts file (with all domains and hosts in the remote hosts file) and one local hosts file that contains a pointer to the remote hosts file. If you want users to share a common hosts file, and if you want to simplify administration, use a remote hosts file.

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.

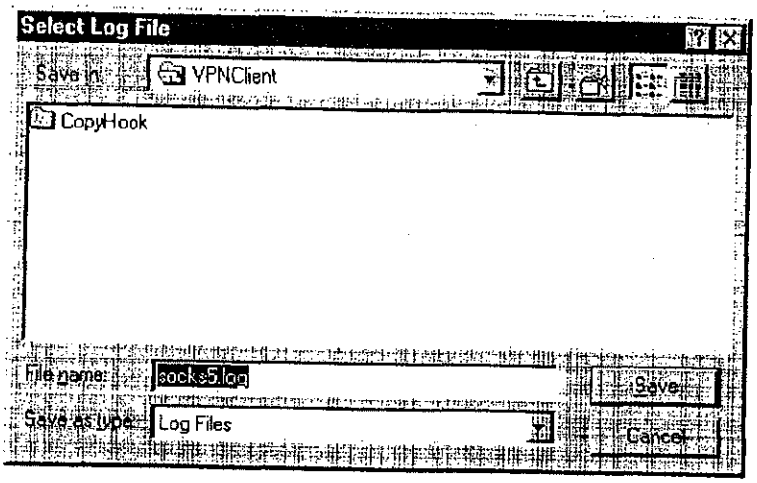
To run an Aventail Connect trace

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.

Exhibit J

"Aventail ExtraNet Center 3.1: Security With Solid Management, Network Computing (June 28, 1999)

Network Computing

Aventail ExtraNet Center 3.1: Security With Solid Management.(Aventail's remote access/network security software)(Software Review)(Evaluation)

Network Computing | June 28, 1999 | Fratto, Mike

I've always thought that Aventail Corp. had a great solution for providing secure remote access and building extranets; it combines fine-grained access control, strong authentication support and detailed auditing. The problem with previous versions of its Aventail ExtraNet Center (AEC) was the absence of strong management functions.

AEC 3.1 addresses these concerns with support for remote server management, LDAP authentication, and NT Domain and NDS user password management. Connect 3.1, Aventail's client, also provides LDAP and client-side SSL (Secure Sockets Layer) support, remote configuration file-loading and a customizable application setup utility.

The AEC is a Socks 5-based proxy server with several components. Its AEC Server runs on Windows NT or Unix servers and proxies connection requests from Aventail Connect clients. Using a modular approach, the AEC secures communications via SSL and authenticates users through existing services, including Windows domains, Novell's NDS, RADIUS (Remote Authentication Dial-In User Service) server and SecurID. The AEC is managed both locally and remotely via the Aventail Management Server using the product's Policy Console. The Aventail Connect client securely redirects network connections from the user's desktop to the AEC server.

Network Computing conducted an exclusive test of AEC 3.1 and Connect 3.1 betas in our Real-World Labs(R) at Syracuse University. I was impressed with the improvements in both the AEC Server and the Connect client, though Aventail still needs to refine the new features.

Aventail presents a highly customizable pricing model based on the number of required servers and clients, as well as the number of site or individual licenses. Starting at $10,000, AEC provides granular, secure access control to internal and external network resources.

Remote Management, Finally!

Remote management is an important, long-awaited aspect of AEC 3.1. Remote AEC Servers can be managed through Policy Console as if they were local, but you must be using NT; Policy Console will not run on Windows 95/98. When AEC installs, three services are added to NT: AEC Server, Management Server and Traffic Monitor Server. Only the AEC Server installs to run automatically. I set the Management Server startup profile to automatic, so remote management was always available.

Aventail's default installation of AEC and Management Servers denies all access. I used the Management Server Console to allow access only from my remote-management workstation, and only if I could authenticate into my Windows NT Domain. This configuration process is similar to configuring the access rules on the AEC Server. I then stopped and started the Management Server with the new rule.

Using the Policy Console from my remote workstation, I configured the AEC with my preferred authentication methods: SSL with NT authentication, and with access rules allowing only *HTTP traffic* through the extranet. Once the new configuration was created and saved, I used the Policy Console Services window to issue a reconfigure command; according to Aventail, this reconfigures the AEC

Server on the fly. But the command didn't work, so I had to stop and start the AEC Server. Stopping the AEC Server remotely can take up to three minutes, and the Policy Console and the Service Applet on the AEC Server were inaccessible while I waited for the Stop command to end. Aventail is aware of this problem and says it has fixed it in a later beta.

I learned from my tests that a local and a remote administrator can simultaneously configure the AEC Server and overwrite each other's changes, which easily leads to misconfigurations. For example, I ran Policy Console remotely and locally on the AEC Server, and neither Policy Console was aware of the other. In addition, changes made through one console were not reflected on the other console. To alleviate this problem, don't install the Policy Console on the same server as the AEC Server. Regardless, server management should be locked to only one manager at a time. Don't worry if you have multiple remote managers because they can't simultaneously configure an AEC Server.

Improved Authentication

AEC 3.1 adds enhanced authentication support, which proved very useful during our tests. Configuring the AEC to use Netscape's Directory Server for LDAP authentication was a snap. I simply entered the addressing information for the LDAP server and assigned the appropriate field name for authentication matching. Aventail's other authentication enhancement can request new passwords on behalf of NT or NDS, such as when a user's password expires. This makes password management enforceable even for remote Aventail users.

Among the more interesting features in Aventail Connect 3.1 is the ability to preconfigure the client and on-the-fly reconfigurations. These two features greatly simplify remote management.

I first built a Connect configuration file on my management station. The Customizer wizard application stepped me through the creation of an executable installation file. I pointed the wizard to the required files, such as the license and server's roots file. I chose not to include client applications because I wanted to restrict user access. I selected only one configuration file, but I liked having the ability to include multiple configuration files in the distribution; in this way, I could create configuration files for use inside or outside the local network. With previous versions of Connect, if you had to change your configuration, it meant restarting the client. With version 3.1, you can reconfigure Connect without restarting.

Send your comments on this article to Mike Fratto at mfratto@nwc.com.

Aventail ExtraNet Center 3.1. Available: Now. Starts at $10,000. Aventail, (206) 215-1111, (817) 283-6824; fax (206) 215-1120. www.aventail.com

Fratto, Mike

http://business.highbeam.com/4113/article-1G1-55009142/aventail-extranet-center-31-security-solid-management