



Aventail Connect 5.3

Administrator's Guide

©2003 Aventail Corporation. All rights reserved. Aventail, Aventail EX-1500, Aventail ExtraWeb, Aventail Anywhere VPN, Aventail Connect, Aventail ASAP WorkPlace, Aventail Web File Access, Aventail OnDemand, and their respective logos are trademarks, service marks, or registered trademarks of Aventail Corporation. Other product and company names mentioned in this publication are the trademarks of their respective owners.

Last modified 11/20/03 09:15

Table of Contents

Chapter 1

Introduction	1
What is Aventail Connect?	1
How Does Aventail Connect Work?	1
What's New in Aventail Connect 5.3?	2
What is a VPN?	3
Installation	4
Installing the Aventail Connect Client Software	4
System Requirements	4
Installing Aventail Connect on a Single Workstation	5
Network Installation	5
Uninstalling the Aventail Connect Client Software	5
Installing the Aventail Connect Administrator Tools	6
Uninstalling the Aventail Connect Administrator Tools	6

Chapter 2

Configuration	7
The Configuration Tool	8
Networks and Organizations	8
Configuration Files	8
Configuration Setup	9
Starting the Configuration Tool	9
Configuration File Types	9
Creating Standard Aventail Connect 5.x Configuration Files	9
Creating Configuration Update Files	9
Creating Clear-Text Configuration Files	10
Editing Configuration Files	10
Inserting Networks	10
Linking Networks	11
Deleting Networks	12
Exporting Organizations	12
Importing Organizations	12
Network View Options	13
Saving a Network View	13
Loading a Network View	13
Recreating a Network View	13
Organization Settings	13
Configuring Organization Updating Settings	14
Organization Passwords	15
Enabling Password Protection	15
Changing a Password	16
Disabling Password Protection	16
Network Settings	16
Assigning a Network to an Organization	17
Renaming a Network	17



Adding a Logo to Authentication Dialog Boxes	17
Remote Network Access Modes	18
Configuring Remote Network Access Modes	18
Configuring Multiple Remote Network Access Mode	19
Configuring Connection-Termination Options	19
Enabling Internet Proxy Mode	20
Configuring Application Detection	21
Configuring Personal Firewall Integration	22
Personal Firewall Setup	23
Aventail Connect Setup	24
Access Server Settings	25
Specifying a Proxy Server	25
Specifying a Fallback Proxy Server	25
Configuring Internet Access Proxy Detection	26
Authentication Options	27
Enabling Authentication Modules	27
Configuring SSL Options	28
Configuring Advanced SSL Options	29
Configuring Acceptable Ciphers Options	29
Configuring Compression Options	29
Configuring Server Validation Options	30
Configuring Client Certificate Options	31
Configuring Credential Cache Timeout Settings	31
Authentication Realms	32
Visible and Hidden Realms	33
How Realms Work	33
Enabling Realms Support in Connect	33
Configuring Realms Options	35
Domain Options	37
How Microsoft Networking Support Works	37
Configuring Microsoft Networking Support	38
Adding Domains	39
Editing Domains	39
Deleting Domains	40
Adding Hosts	40
Editing Hosts	41
Deleting Hosts	42
Destination Options	42
Defining Destinations	42
Wildcards in Host and Domain Name Definitions	43
Avoiding Conflicts	44
Adding Destinations	44
Excluding Destinations	45
Editing Destinations	46
Deleting Destinations	47

Chapter 3
Deployment 49

Planning a Deployment 49

Customized Configuration and Distribution 51

 Deploying Aventail Connect Packages 51

 Customizer Overview 51

 Starting Customizer 52

 Creating New Packages 53

 Editing Existing Packages 53

 Saving Packages 54

 Specifying Customizer Options 54

 Configuring Installation Prompt Options 54

 Configuring Installation Directory and Automatic Startup Options 55

 Configuring Microsoft Windows Installer Options 56

 Configuring Advanced Installation Options 57

 Configuring Package Information Options 58

 Adding Files to a Package 58

 Configuring Aventail Connect Startup Options 59

 Specifying Configuration File Settings 60

 Configuring Remote Network Access Settings 61

 Configuring Network Settings 62

 Configuring Windows Domain Logon Options 63

 Configuring Advanced Settings for Aventail Connect Software 64

 Configuring Software Updating Options 64

 Configuring Package Signing Options 66

Updating Configurations 68

 Creating Configuration Update Files 68

 Exporting Organizations 68

 Importing Organizations 68

 Enabling Configuration Updating 69

Chapter 4
Troubleshooting 71

Frequently Asked Questions 71

Troubleshooting Aventail Connect Problems 72

 Aventail Connect Installation Problems 72

 Network Connectivity Problems 73

 Aventail Connect Configuration Problems 74

Event Viewer 74

 Opening the Event Viewer 75

 Setting the Logging Level 75

 Filtering Log Messages 76

 Saving Log Messages 77

 Copying Log Messages into Other Applications 77

 Printing Log Messages 77

 Finding a Specific Log Message 78

 Clearing the Event Viewer Window 78

 Closing the Event Viewer Window 78

Running the Diagnostic Utilities 78



Appendix A

Aventail Connect Dialog Boxes 81

Configuration Tool 81

 Link the <x> Network Dialog Box 81

 Configuration Tab 82

 Organization Tab 82

 Organization Updating Dialog Box 83

 Network Tab 83

 Network Advanced Settings Dialog Box 85

 Personal Firewalls Dialog Box 85

 Add Running Application Requirement Dialog Box 85

 Domains Tab 86

 Add/Edit Static Domain Dialog Box 86

 Add Static Host Dialog Box 86

 Destinations Tab 86

 Add/Edit Destination Dialog Box 87

 Access Server Tabs 88

 Authentication Dialog Box 88

 Authentication Realm Options Dialog Box 89

 Authentication Realms Dialog Box 90

 Add Authentication Realm Name Dialog Box 90

 SSL Options Dialog Box 90

 Trusted Roots Dialog Box 91

 PKCS #11 Configuration Dialog Box 92

 Access Server Advanced Settings Dialog Box 92

Customizer Window 92

 Software Installation Pages 93

 Installation Options Page 93

 Windows Installer Options Page 94

 Advanced Installation Options Page 95

 Packaging Options Pages 95

 Package Information Page 95

 Additional Package Files Page 95

 Connect Software Settings Pages 96

 Connect Startup Options Page 96

 Configuration File Settings Page 97

 Remote Network Access Settings Page 97

 Network Settings Page 98

 Username/Password Credentials Page 98

 Advanced Settings Page 98

 Software Update Pages 99

 Software Updates Page 99

 Digital Signature Page 100

Event Viewer Window 101

 Logging Categories Dialog Box 102

Remote Ping Dialog Box 103



Appendix B
Aventail Connect Extensibility Toolkit 105
Entering Command-Line Switches 105
Run-Time Command-Line Switches 106
 One-Click Authentication Integration. 107
Support Command-Line Switches. 109

Glossary 111

Index 119





Chapter 1

Introduction

Welcome to the Aventail® Connect™ 5.3 Administrator's Guide. Aventail Connect, the client component of the Aventail SSL VPN solution, is a secure proxy client based on SOCKS v5, the Internet Engineering Task Force (IETF) standard for authenticated firewall traversal.

What is Aventail Connect?

Aventail's VPN solution provides secure end-user access over the Internet to internal corporate networks and client/server enterprise applications. At the core of the service is the Aventail client/server access service, a circuit-level proxy component that securely brokers end-user access to enterprise applications and network resources. Operating in conjunction with the Aventail client/server access service is the Aventail Connect client.

The Aventail Connect client routes network traffic according to a set of routing directives defined in an Aventail Connect configuration file. When used with Secure Sockets Layer (SSL), Aventail Connect can encrypt inbound and outbound traffic. On larger networks, the Aventail Connect client can address multiple SOCKS v5 servers based on end destination and type of service, allowing you to effectively monitor and direct network traffic.

In most cases, users interact with the Aventail Connect client only when it prompts them to enter authentication credentials for a connection to the remote network.

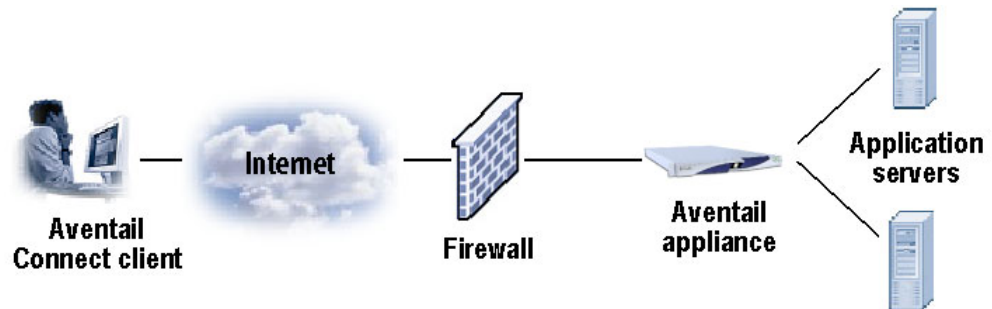
How Does Aventail Connect Work?

Aventail Connect is the client component of Aventail's VPN solution, which enables secure, authorized access to Web-based and client/server applications. The Aventail Connect client allows users to connect to network resources that sit behind the Aventail SSL VPN appliance.

The Aventail Connect client identifies and securely routes application requests to the Aventail appliance. (See diagram below.) The Aventail Connect client automatically routes appropriate network traffic from an application such as an e-mail program or a



Web browser to the Aventail client/server access service on the appliance. The appliance then sends the traffic to the network resources or to the Internet. You can define a set of rules that route this traffic in an Aventail Connect configuration file.



When the Aventail Connect client receives a connection request, it determines whether the connection needs to be redirected to the Aventail appliance 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 Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

SOCKS v5 Overview

SOCKS v5 is a security protocol based on the IETF standards track. SOCKS v5 was designed to allow secure traversal of corporate firewalls. 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 VPN. An application whose traffic is proxied by SOCKS is considered "SOCKSified." Other features of SOCKS include:

- Client authentication: Authentication allows network managers to provide selected user access to internal and external areas of a network.
- Traffic encryption: Encryption ensures that Transmission Control Protocol (TCP) network traffic is private and secure.
- UDP support: SOCKS v5 can proxy User Datagram Protocol (UDP) traffic, which has traditionally been difficult to proxy.
- X.509 client certificate support within SSL.
- Cross-platform support: Unlike many other security solutions, SOCKS can be used on various platforms, such as Windows NT, Windows 2000, Windows Me, Windows 98, and many forms of UNIX.

The Aventail Connect client automates the "SOCKSification" of TCP/IP and NetBIOS client applications, making it simple for workstations to take advantage of the SOCKS v5 protocol.

What's New in Aventail Connect 5.3?

Aventail Connect 5.3 includes the following new features:

- **Personal firewall integration:** You can require that a personal firewall be running on users' computers in order to start Aventail Connect or enable remote network access.

- **Multiple authentication realms support:** Aventail Connect supports the use of multiple authentication realms, which enables a user to log in to different authentication repositories or servers.
- **Enhanced application detection:** You can configure Aventail Connect to validate a required application's Authenticode signature before Aventail Connect will start.

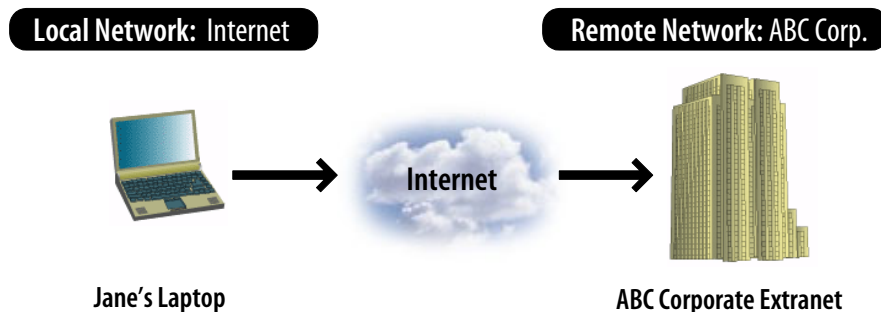
What is a VPN?

Think of a VPN as an extension of your private network. A company can use a VPN to make applications and information available to only authorized users, both inside and outside the company. A VPN provides access to Web-based applications or traditional client/server applications, and encrypts all traffic to make it unreadable to unauthorized users.

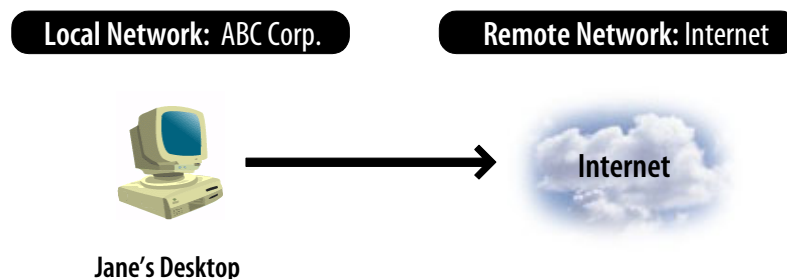
VPNs are an essential tool in managing today's dynamic business relationships. For example, a VPN allows a company to put sales information on the protected network and allow only its sales department and designated customers to access the information.

VPNs consist of a local network and a remote network. The local network is the user's current location, or where the user is connecting from. The remote network is the location that the user is connecting to.

For example, if Jane, an employee of ABC Corporation, wants to connect to the ABC corporate VPN from her laptop while traveling, her local network is the Internet (where she is connecting from) and her remote network is ABC (where she is connecting to).



Some companies use the Aventail Connect client for outbound network access as well. For example, if Jane wants to connect to the Internet from her computer at ABC Corporation's headquarters, her local network is ABC and her remote network is the Internet.



In many cases, the Aventail Connect client can automatically detect users' local network locations. However, Aventail Connect may prompt users to specify their local network locations or remote networks. Specifying the correct local and remote networks ensures that users can successfully access their network resources.

Installation

The Aventail Connect client program and the Aventail Connect administrator tools are two separate installations; each is installed and uninstalled separately. Note that you can install one without the other. The Aventail Connect administrator tools include the Configuration Tool and the Customizer tool. The Configuration Tool is used to create and modify Aventail Connect configuration files, and the Customizer is used to create and modify custom Aventail Connect setup packages.

Typically, users need only the Aventail Connect client program. Aventail recommends not distributing the administrator tools to users unless they specifically need them.

Installing the Aventail Connect Client Software

The Aventail Connect client software is installed and uninstalled using the Microsoft Windows Installer (MSI), an installation and configuration utility that is included with most Microsoft Windows operating systems. Some versions of Microsoft Windows ship without the MSI utility, or with an outdated version of it. If the correct version of MSI is not already installed on users' computers, Aventail Connect can install or upgrade the MSI software on those computers during the Aventail Connect installation process. For more information, see "Configuring Installation Prompt Options" on page 54.

NOTE To install or uninstall the Aventail Connect client software, you must have administrative privileges on the local machine (but not necessarily on the domain).

System Requirements

The Aventail Connect client runs on the following operating systems:

- Windows XP Home Edition and XP Professional
- Windows 2000 Professional
- Windows Millennium (Windows Me)
- Windows 98 (SE)

Aventail Connect also requires Microsoft Internet Explorer 5.0 or later.

The Aventail Connect client runs on x86-based or Pentium personal computers. The following table lists the minimum memory requirements for each of the supported operating systems.

Operating system	Minimum RAM
Windows XP Home Edition and XP Professional	128 MB
Windows 2000 Professional	64 MB
Windows Millennium (Me)	64 MB



Operating system	Minimum RAM
Windows 98 (SE)	32 MB

Installing Aventail Connect on a Single Workstation

This section describes how to install the Aventail Connect client to your own computer. Your users will follow a similar installation procedure after you configure and distribute their Aventail Connect installation packages.

Before installing the Aventail Connect client, close any applications that are running. You must reboot your computer after installing the Aventail Connect client.

► To install the Aventail Connect client

- Installation procedures vary slightly, depending on which media source you use:
 - If you are installing directly from a CD, run *setup.exe* from the Aventail Connect directory.
 - If you are installing from a network-delivered, self-extracting file created with the Aventail Connect Customizer, simply execute the file. This extracts the installation files and automatically launches the Aventail Connect setup program. For more information about the Aventail Connect Customizer tool, see "Customized Configuration and Distribution" on page 51.
- Follow the instructions provided by the Aventail Connect installation program as it guides you through the installation process. At the end of the setup, you are prompted to reboot your computer.

Network Installation

In general, the process of installing the Aventail Connect client to multiple networked workstations involves placing a customized Aventail Connect package—created with the Aventail Connect Customizer tool—in a shared network directory, on a Web server, or in another publicly accessible location and then pointing users to the package file. The most common ways of distributing a setup package are:

- Placing the package on an HTTP or HTTPS server.
- Placing the package on an FTP site.
- Placing the package 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`).

A customized Aventail Connect package automatically extracts the Aventail Connect installation files and initiates setup. You can manually configure this package to suit your network specifications with the Aventail Connect Customizer tool. For more information, see "Customized Configuration and Distribution" on page 51.

Uninstalling the Aventail Connect Client Software

You must reboot your computer after uninstalling the Aventail Connect client software.



► **To uninstall the Aventail Connect client**

1. In the Windows **Control Panel** window, double-click **Add/Remove Programs**.
2. Select **Aventail Connect** from the list of programs, and then click **Remove**.

Installing the Aventail Connect Administrator Tools

The Aventail Connect client program and the Aventail Connect administrator tools are two separate installations; each is installed and uninstalled separately, and you can install one without the other. The Aventail Connect administrator tools include the Configuration Tool and the Customizer tool. The Configuration Tool is used to create and modify Aventail Connect configuration files, and the Customizer is used to create and modify custom Aventail Connect setup packages.

Before installing the Aventail Connect administrator tools, close any applications that are running.

System Requirements

The Aventail Connect administrator tools are supported on the following operating systems:

- Windows XP Home Edition and XP Professional
- Windows 2000 Professional

► **To install the Aventail Connect administrator tools**

1. Run *connectadmin.exe* from the Aventail Connect directory.
2. Follow the instructions provided by the installation program as it guides you through the installation process. You do not need to reboot your computer after the installation.

Uninstalling the Aventail Connect Administrator Tools

You do not need to reboot your computer after uninstalling the Aventail Connect administrator tools.

► **To uninstall the Aventail Connect administrator tools**

1. In the Windows **Control Panel** window, double-click **Add/Remove Programs**.
2. Select **Aventail Connect Administration Tools** from the list of programs, and then click **Remove**.



Chapter 2 Configuration

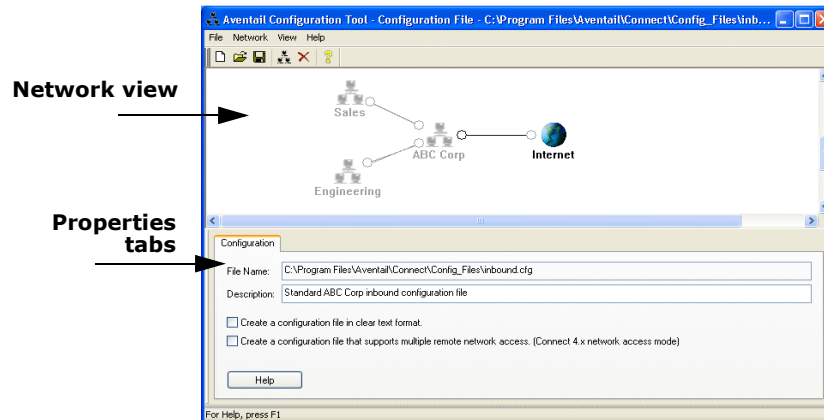
Before running the Aventail Connect client or deploying it to end users, you must determine how VPN traffic will be redirected through the network. Network redirection rules, which determine if and how SOCKS redirection will occur, are defined in the Aventail Connect configuration (.*cfg*) file. You can create and edit configuration files at any time using the Aventail Connect Configuration Tool.

i **NOTE** In the Aventail Connect interface, an ellipsis (...) button is a standard **Browse** button; you can click the ellipsis (...) button to search for files to open or save.

This chapter describes how to configure Aventail Connect client settings.

The Configuration Tool

The Aventail Connect Configuration Tool window is divided into two areas: the network view and the properties tabs.



Networks and Organizations

The Aventail Connect Configuration Tool allows you to define logical groups of networks. A network is defined as a list of destinations and the server attributes that are used to connect to those destinations. Each object in the network view of the Configuration Tool represents one network. You can arrange networks into logical groups called organizations. An organization can contain multiple networks, and you can link the networks to reflect your network topology. Each network, organization, and network link has its own attributes; however, networks inherit certain settings applied to the organizations they belong to.

When you select a network or network link, all of the networks and network links in the organization are highlighted. All networks and network links that are not a part of the organization are grayed out.

Configuration Files

Network redirection settings, which determine if and how network redirection will occur, are defined in the Aventail Connect configuration file. You can add, edit, update, and delete configuration files at any time using the Configuration Tool.

Aventail Connect 5.x includes backward compatibility with configuration files created in Aventail Connect 4.x. You can use Aventail Connect 4.x configuration files to redirect network traffic. However, if you edit a 4.x configuration file in the Aventail Connect 5.x Configuration Tool, the configuration file is saved in the Aventail Connect 5.x format.

Organizations can be saved to configuration update (.cff) files. Configuration update files are used primarily for updating configuration (.cfg) files; merging a configuration update file with a configuration file is the only method for programmatically updating existing configurations that you have already deployed to users. A configuration update file



updates an organization in a configuration file by replacing the old organization settings with the new organization settings. All networks or network links that belong to the organization inherit the organization's settings.

You can create, modify, and delete configuration update files just as you would configuration files.

For more information about updating configuration files, see "Deployment" on page 49.

Configuration Setup

This section describes how to set up Aventail Connect configuration files.

Starting the Configuration Tool

The Configuration Tool is a component of the Aventail Connect administrator tools.

- ▶ **To start the Configuration Tool**
 - From the **Start** menu, point to **Programs**, point to **Aventail Connect 5.30 Administrator Tools**, and then click **Aventail Connect Configuration Tool**.

Configuration File Types

With the Aventail Connect 5.x Configuration Tool, you can create standard binary Aventail Connect 5.x configuration files, clear-text configuration files, and configuration update files.

Creating Standard Aventail Connect 5.x Configuration Files

Standard binary Aventail Connect 5.x configuration files can be viewed and edited only with the Aventail Connect Configuration Tool.

- ▶ **To create a configuration file**
 1. In the Aventail Connect Configuration Tool, on the **File** menu, click **New**.
 2. Configure settings as needed, click **Save** or **Save As** on the **File** menu, and then save the file as a configuration (.*cfg*) file.

Creating Configuration Update Files

Configuration update (.*cff*) files allow you to update existing configuration (.*cfg*) files with new or updated organizations. You can use these configuration update files when performing organization updating. For more information, see "Updating Configurations" on page 68.

- ▶ **To create a configuration update file**
 1. In the Aventail Connect Configuration Tool, on the **File** menu, click **New**.
 2. Configure settings as needed, click **Save** or **Save As** on the **File** menu, and then save the file as a configuration update (.*cff*) file.



Creating Clear-Text Configuration Files

Aventail Connect 5.x supports text-based configuration files that you can view and edit in a text editor such as Notepad. You can also view and edit them in the Aventail Connect Configuration Tool.

- ! **CAUTION** When you edit configuration files in the Configuration Tool, the Configuration Tool performs various types of data validation to ensure the proper operation of configuration files. If you manually edit a text-based configuration file, this data validation is not performed. Aventail recommends not editing configuration files in a text editor unless absolutely necessary.

A clear-text configuration file is “unprotected,” meaning that it can be read with a text editor and its settings cannot be password-protected; all network information (except password information) is displayed in the text editor.

If you do not want users to view or modify an organization’s settings, do not enable the **Create a configuration file in clear text format** option.

► To create a clear-text configuration file

1. In the Aventail Connect Configuration Tool, on the **File** menu, click **New**.
2. On the **Configuration** tab of the Configuration Tool, select the **Create a configuration file in clear text format** check box.
3. Configure settings as needed, and then save the file as a configuration (.*cfg*) or configuration update (.*cff*) file.

Editing Configuration Files

You can edit configuration files and configuration update files in the Aventail Connect Configuration Tool.

► To open a configuration file for editing

1. In the Configuration Tool, on the **File** menu, click **Open**.
2. In the **Open** dialog box, select the configuration file or configuration update file that you want to open, and then click **Open**.
3. Edit the file as needed and then, on the **File** menu, click **Save**.

Note that you can edit “unprotected” configuration files in a text editor, such as Notepad, or in the Configuration Tool.

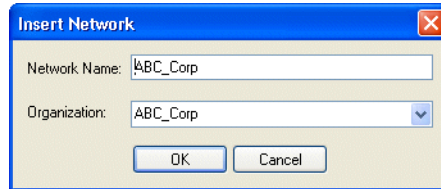
Inserting Networks

Configuration files consist of networks and network links, which you can assign to organizations. You can assign multiple networks to an organization.



► **To insert a network object**

1. In the network view of the **Configuration Tool** window, right-click anywhere in the network view, or on a network that the new network will be linked with, and then click **Insert Network**. The **Insert Network** dialog box appears.



2. In the **Network Name** box, type a descriptive name for the network.
3. In the **Organization** box, type the name of the organization that the network belongs to, or select an organization from the drop-down box, and then click **OK**.

The new network appears in the network view of the Configuration Tool.

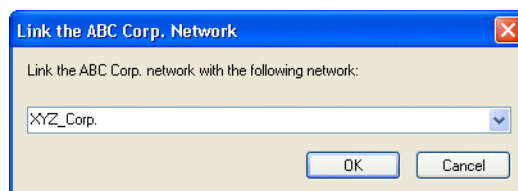
Linking Networks

You can link networks to reflect your network topology. Each network link contains its own attributes, including proxy server definitions and authentication settings.

Network links have a specified direction. For example, in the network view below, the ABC Corp. network is linked to the XYZ Corp. network. If you want two networks to be linked to one another, you must create two network links. In the example below, to link the two networks to one another, you must create one link that links the ABC Corp. network to the XYZ Corp. network, and another link that links the XYZ Corp. network to the ABC Corp. network.

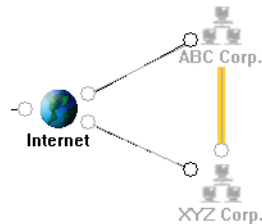
► **To link two network objects**

1. In the network view of the **Configuration Tool** window, right-click the network that you want to create a link to, and then click **Link Network**. The **Link the <x> Network** dialog box appears.



2. In the **Link the <x> network with the following network** box, select the network or organization that you want to link the <x> network to, and then click **OK**.

A network link connects the two networks. (See below.)



Deleting Networks

You can delete networks when they are no longer valid.

► To delete a network object

- In the network view of the **Configuration Tool** window, right-click the network that you want to delete, and then click **Delete Network**.

The network and its network links are removed from the organization.

Exporting Organizations

You can save individual organizations and all of their associated networks and settings. This can be useful when you want to reuse an organization's settings in more than one configuration file, or when you want to update an existing configuration file with a new or updated organization. When you export an organization, it is saved as a configuration update (.cff) file.

► To export an organization

1. In the network view of the **Configuration Tool** window, right-click any network or network link in the organization that you want to export, and then click **Export Organization**.
2. In the **Save As** dialog box, assign a descriptive file name to the organization, and then click **Save**.

Importing Organizations

You can import individual organizations, and all of their associated networks and settings, into a configuration file. This can be useful when you want to reuse an organization's settings in more than one configuration file, or when you want to update an existing configuration file with a new or updated organization.

► To import an organization

1. In the network view of the **Configuration Tool** window, right-click anywhere, and then click **Import Organization**.
2. In the **Open** dialog box, select the organization (.cff file) that you want to import, and then click **Open**.

Network View Options

You can change the network view of the Configuration Tool by dragging network objects to new locations in the network view. Changing the network view does not change the configuration itself. It simply allows you to arrange your network objects in a way that more accurately represents your network topology.

Saving a Network View

You can arrange your network objects in a way that more accurately represents your network topology. If you want to save those settings for future use, you can save the network view as a configuration view (.cfv) file.

► To save a network view

1. In the network view of the **Configuration Tool** window, right-click anywhere, and then click **Save Network View**.
2. In the **Save As** dialog box, assign the network view a descriptive file name, and then save it as a .cfv file.

Loading a Network View

You can load a network view that you saved as a configuration view (.cfv) file. Note that you can load only the network views that are associated with a particular configuration file.

► To load a network view

1. In the network view of the **Configuration Tool** window, right-click anywhere, and then click **Load Network View**.
2. In the **Open** dialog box, select the configuration view file that you want to load, and then click **Open**.

Recreating a Network View

Recreating a network view repositions each network by equally spacing the networks.

► To recreate a network view

- In the network view of the **Configuration Tool** window, right-click anywhere, and then click **Recreate Network View**.

Organization Settings

You can arrange networks into logical groups called organizations. An organization can contain multiple networks, and you can link the networks to reflect your network topology. Each network, organization, and network link has its own attributes.

This section describes how to configure an organization's updating settings and password protection settings.



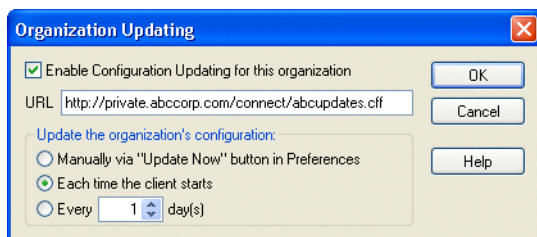
Configuring Organization Updating Settings

You can update existing local configuration files with the Aventail Connect client's configuration updating feature. Updating with configuration update files allows you to update certain parts of a user's configuration file, leaving the other parts of the configuration unchanged. Each organization includes attributes that control its updating behavior, including a URL and an updating frequency. When an organization is updated with a configuration update file, only that organization and the networks that belong to it are modified.

At launch time, the Aventail Connect client checks the configuration file to determine whether updating is required, and then downloads any required updates. Supported updating protocols are HTTP, HTTPS, and FTP. Users may need to authenticate during the updating process if the URL points to a resource that is behind the Aventail appliance. The connection to the designated URL is redirected by the Aventail Connect client according to the settings in the current configuration file. The Aventail Connect client can download updated configuration update information either every time Aventail Connect starts or on a regular, scheduled basis. These settings are managed in the **Organization Updating** dialog box.

► To enable organization updating

1. If redirection through a proxy server is required to reach the Web server, configure the Aventail Connect client to use a configuration file that can access the Web server. If redirection is not required, skip this step.
2. In the network view of the Configuration Tool, select any network or network link in the organization that you want to enable updating for.
3. Click the **Organization** tab, and then click **Updating**. The **Organization Updating** dialog box appears.



4. Select the **Enable configuration updating for this organization** check box.
5. In the **URL** box, type the URL of the location where the configuration update files will be stored.
6. Specify how often the Aventail Connect client will download the updating information:
 - Manually via **Update Now** button
 - Each time the client starts
 - Every <x> days
7. Save the configuration file.

- Place new Aventail Connect configuration update (.cff) files on the specified Web server whenever you need to update the organization.

Organization Passwords

You can enable password protection on a per-organization basis. Protecting an organization with a password prevents unauthorized users from viewing or modifying the organization's settings.

A password is not required to use the organization's configuration file to perform redirection with the Aventail Connect client. However, to view or modify the organization's configuration settings, the correct password must first be specified.



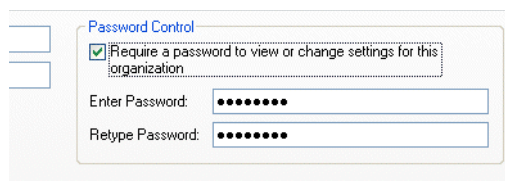
- NOTE** If you edit a configuration file in a text editor, such as Notepad, passwords are stripped from the configuration file to ensure security. For more information, see "Creating Clear-Text Configuration Files" on page 10.

Enabling Password Protection

Enable password protection for an organization when you do not want users to view or modify the organization's configuration information.

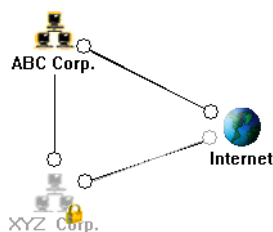
► To enable password protection

- In the network view of the Configuration Tool, select any network or network link in the organization that you want to protect with a password.
- Click the **Organization** tab, and then select the **Require a password to access settings for this organization** check box.



- Type and then retype a password for the organization, and then save the configuration file.

The organization is now password-protected, and a lock icon appears on the organization in the network view.



Changing a Password

Aventail recommends periodically changing an organization's password.

► To change an organization's password

1. Open the configuration file or configuration update file that contains the organization whose password you want to change. Use the current (existing) password to open the file.
2. In the network view of the Configuration Tool, select any network or network link in the organization whose password you want to change.
3. Click the **Organization** tab, and then select the **Require a password to access settings for this organization** check box.
4. Type and then retype a new password for the organization, and then save the configuration file.

Disabling Password Protection

Note that if you disable an organization's password protection, users may be able to view or modify the organization's configuration information.

► To disable password protection

1. Open the configuration file or configuration update file that contains the organization whose password you want to disable. Use the current (existing) password to open the file.
2. In the network view of the Configuration Tool, select any network or network link in the organization whose password you want to change.
3. Click the **Organization** tab, and then clear the **Require a password to access settings for this organization** check box.
4. Save the configuration file.

Network Settings

This section describes how to configure a network's settings.

Assigning a Network to an Organization

You can assign a network to an organization. An organization can include any number of networks.

► To assign a network to an organization

1. In the network view of the Configuration Tool, select the network.
2. On the **Network** tab, in the **Organization** box, click the organization that you want to assign the network to, or type a new organization name.

Renaming a Network

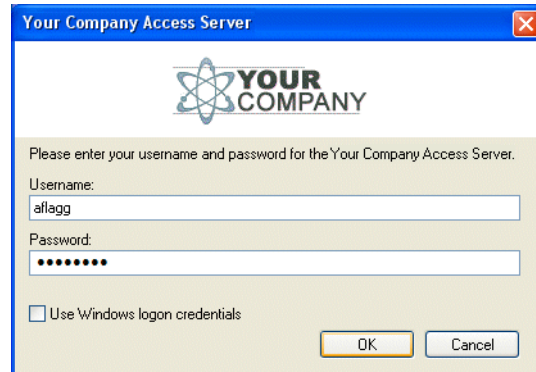
You can change a network's name anytime.

► To change a network's name

1. In the network view of the Configuration Tool, select the network whose name you want to change.
2. On the **Network** tab, in the **Network Name** box, type a new name for the network.

Adding a Logo to Authentication Dialog Boxes

You can add an image, such as a corporate logo, to a network's authentication dialog boxes. When users are prompted to enter authentication credentials for that network, a logo can help identify the network to which they are connecting.



Images must be in bitmap (.*bmp*) format. They must be no larger than 100 x 500 pixels, and it is recommended that they contain no more than 256 colors. You must place the bitmap file in the Aventail Connect directory. (You can do this manually or when creating a custom setup package with the Aventail Connect Customizer tool.)

► To add an image to authentication dialog boxes

1. Place the bitmap file in the Aventail Connect directory.
2. In the network view of the Configuration Tool, select the network whose authentication dialog boxes you want to add the image to.

3. In the **Logo Filename** box, type or browse for the path of the bitmap file.

Remote Network Access Modes

Aventail Connect includes several options for proxying network traffic. The Aventail Connect client can be configured to redirect all network traffic to the Aventail CPE, allowing you to centrally administer the client's "mode," or predefined way of accessing the network resources.

When running in standard mode, users can connect to only one remote network at a time. Traffic for defined destinations is redirected; all other traffic is passed through to the local network or to the Internet.

The two restricted modes prevent users from accessing a local network while the Aventail Connect client is running. This is useful if you want to protect your corporate network from potential vulnerabilities of a home network (such as an open cable or DSL connection).

Mode	Description
Standard: Single network with local access	Connections to remote resources are redirected to the remote network; all other connections are redirected to the local network.
Restricted: Redirect all connections (no local access)	Redirects all network traffic to the Aventail appliance. No local network access is allowed.
Restricted: Refuse non-directed connections (no local access)	Redirects only traffic bound for destinations specified in the configuration file.
Multiple networks with local network access (Connect 4.x mode)	Allows simultaneous connections to multiple networks. Conflicts between destinations are not allowed in this mode. (Configured on the Configuration tab.)

When running in **Multiple networks with local network access** mode, the Aventail Connect client checks the configuration file for network destination conflicts each time a configuration file is created or updated. For more information about destination conflicts, see "Avoiding Conflicts" on page 44.

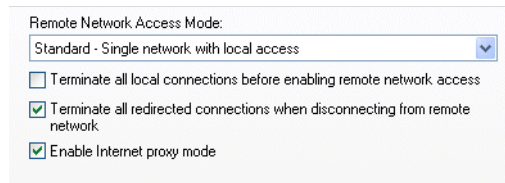
Configuring Remote Network Access Modes

If multiple remote network access mode is enabled (on the **Configuration** tab of the Configuration Tool), the remote network access mode controls on the **Network** tab are disabled.

► To configure remote network access modes (restricted and standard modes)

1. In the network view of the Aventail Connect Configuration Tool, select the network whose connection mode you want to configure.

2. On the **Network** tab of the Configuration Tool, in the **Remote Network Access Mode** box, click the mode that you want the network to run in.



Remote Network Access Mode:
 Standard - Single network with local access
 Terminate all local connections before enabling remote network access
 Terminate all redirected connections when disconnecting from remote network
 Enable Internet proxy mode

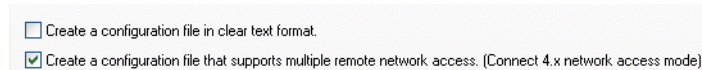
Note that you must configure the **Multiple networks with local network access** mode on the **Configuration** tab of the Configuration Tool. For more information, see "Configuring Multiple Remote Network Access Mode" on page 19.

Configuring Multiple Remote Network Access Mode

The Aventail Connect Configuration Tool allows you to create configuration files that allow simultaneous connections to multiple networks. Note that this setting is configured on the **Configuration** tab.

► To enable multiple remote network access mode

1. In the network view of the Aventail Connect Configuration Tool, select the network whose connection mode you want to configure.
2. On the **Configuration** tab of the Configuration Tool, select the **Create a configuration file that supports multiple remote network access (Connect 4.x network access mode)** check box.



Create a configuration file in clear text format.
 Create a configuration file that supports multiple remote network access. (Connect 4.x network access mode)

3. After you have configured your settings, save the file as a configuration (.cfg) or configuration update (.cff) file.

i **NOTE** If Aventail Connect detects destination conflicts between networks, an error message is displayed. You must resolve the conflict(s) before you can enable the multiple remote network access mode option. For more information, see "Avoiding Conflicts" on page 44.

Configuring Connection-Termination Options

Aventail Connect supports automatic connection termination, which, in standard and restricted modes, increases security by limiting users' connections to other networks. This is useful if you want to protect your corporate network from potential vulnerabilities of a home network (such as an open cable or DSL connection). You can configure the Aventail Connect client to:

- Close non-secure connections before opening a connection to the remote network. When enabled, this ensures that no other connections are open on the user's computer before connecting to the remote network.

- Close secure connections when terminating connections to the remote network. When enabled, this ensures that, when the user disconnects from the remote network, all other open connections to that network are also terminated.

If multiple remote network access mode is enabled (on the **Configuration** tab of the Configuration Tool), the connection-termination options on the **Network** tab are disabled.

► **To enable automatic connection termination**

- In the network view of the Configuration Tool, select the network that you want to configure.
- To close all non-secure connections before connecting to the remote network, on the **Network** tab, select the **Terminate all local connections before enabling remote network access** check box.

Remote Network Access Mode:
 Standard - Single network with local access
 Terminate all local connections before enabling remote network access
 Terminate all redirected connections when disconnecting from remote network
 Enable Internet proxy mode

- To close secure connections when the remote-network connection is terminated, on the **Network** tab, select the **Terminate all redirected connections when disabling remote network access** check box.

Enabling Internet Proxy Mode

When Internet proxy mode is enabled, the Aventail Connect client redirects all unknown traffic (connections that do not match any destinations in the configuration file) to the Internet. When Internet proxy mode is disabled, the Aventail Connect client redirects only those connections that match a defined destination in the configuration file.

► **To enable Internet proxy mode**

1. In the network view of the Configuration Tool, select the network for which you want to enable Internet proxy mode.
2. On the **Network** tab of the Configuration Tool, select the **Enable Internet proxy mode** check box.

Remote Network Access Mode:
 Standard - Single network with local access
 Terminate all local connections before enabling remote network access
 Terminate all redirected connections when disconnecting from remote network
 Enable Internet proxy mode

Notes

- When Internet proxy mode is disabled, you may need to perform additional configuration for any applications that need to access resources on both your network and the Internet. You must configure the application to *not* proxy

connections going to the network resources. You can typically perform this additional configuration where the application's proxy settings are defined, usually in an address exception list.

- When Internet proxy mode is enabled, you must define all local network destinations.

Configuring Application Detection

Aventail Connect supports application detection, which allows you to define applications (such as anti-virus software) that must be running on a user's computer before remote network access is enabled. When you specify these applications in the configuration file, Aventail Connect searches for the defined executable files when a user initiates a connection to the remote network. If the executable files are not running, the user is prompted to start the specified applications before connecting to the remote network.

i **NOTE** To use application detection, the Aventail Connect client must be running as an application (started via the Windows Start menu), and not as a Windows service (started automatically at Windows startup). The applications most useful to detect—personal firewall and anti-virus programs—typically load automatically as Windows services. Because Aventail cannot control the order in which services are loaded during startup, the user must start the Aventail Connect client manually (via the Start menu) to ensure that the necessary applications load properly.

You can configure Aventail Connect to validate a required application's Authenticode signature before Aventail Connect will start. This provides an added level of security as it prevents another application from impersonating the required application.

When you enable Authenticode validation for a required application, if a user is running in Restricted or Standard mode, when the user initiates a connection to the remote network, Connect first ensures that the required application is running. After Connect verifies that the required application is running, it attempts to validate the application's Authenticode signature. If Connect determines that the Authenticode signature is valid, the network connection process continues. If Connect determines that the Authenticode signature is invalid, the network connection will not continue. In addition, if at any time while the user is connected to the remote network Connect detects that the required application quits running, Connect will terminate the network connection.

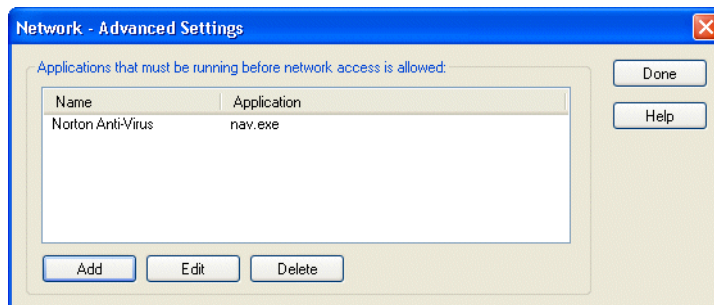
If a user is running in multiple network access mode (4.x mode), at Aventail Connect startup Connect first ensures that the required application is running. After Connect verifies that the required application is running, it attempts to validate the application's Authenticode signature. If Connect determines that the Authenticode signature is valid, Aventail Connect starts. If Connect determines that the Authenticode signature is invalid, Aventail Connect does not start. In addition, if the required application quits running while the user is running Aventail Connect, Connect will shut down.

If application detection is enabled, users can view the status of their required applications on the **Advanced** tab of the **Aventail Connect Options** dialog box.

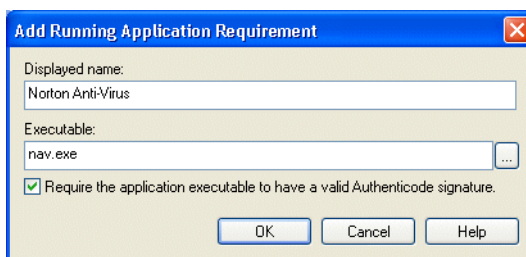
► To enable application detection

1. In the network view of the Aventail Connect Configuration Tool, select the network for which you want to enable application detection.

- Click the **Network** tab, and then click **Advanced**. The **Network Advanced Settings** dialog box appears.



- Click **Add**. The **Add Running Application Requirement** dialog box appears.



- In the **Application Name** box, type an easily recognizable name for the program (for example, *ZoneAlarm Firewall*). This allows users to easily identify the required application.
- In the **Executable** box, type the executable file name, or browse for the executable file (for example, *zonealarm.exe*). This is the file that the Aventail Connect client searches for when verifying that the application is running.
- If you want Aventail Connect to validate the required application's Authenticode signature, select the **Require the application executable to have a valid Authenticode signature** check box.
- Click **OK** to close the **Add Running Application Requirement** dialog box, and then click **Done** to close the **Network Advanced Settings** dialog box.

Configuring Personal Firewall Integration

Aventail Connect supports integration with Sygate and Zone Labs personal firewalls. You can require that a certain personal firewall be running on a user's computer before Aventail Connect will enable remote network access, thus increasing security for the duration of the session.

In addition to verifying that a personal firewall is running before enabling remote network access, Aventail Connect will disable remote network access if it detects that the personal firewall stops running during a session.

Aventail Connect supports integration with the following firewalls:



- Sygate Security Agent v3.5
- Sygate Personal Firewall v5.5
- Zone Labs ZoneAlarm Pro
- All versions of Zone Labs Integrity clients (including Desktop, Agent, and Flex)

Note that Aventail Connect does not support integration with the free (no-cost) versions of the Zone Labs ZoneAlarm personal firewall.

The basic steps for setting up and testing personal firewall integration in Aventail Connect are:

1. Install and configure the applicable personal firewall software on the end user's computer.
2. Using the Aventail Connect 5.3 Configuration Tool, configure personal firewall integration settings. (Create or edit a configuration file.)
3. Using the Aventail Connect 5.3 Customizer tool, create an Aventail Connect 5.3 setup package that includes the new configuration file, and distribute this package to users.

These steps are described in more detail in the following sections.

Personal Firewall Setup

Before you can use the personal firewall integration feature in Aventail Connect, you must install and configure the applicable personal firewall software on the user's computer. The steps will vary depending on whether users are running the Sygate or Zone Labs personal firewall. This section describes how to perform these initial steps for each firewall.

Verify that you have the correct IP address for the destination appliance before configuring the firewall software.

Sygate Setup

To use Aventail Connect with the Sygate personal firewall, you must first install and configure the Sygate personal firewall software on each user's computer.

► To install the Sygate personal firewall

1. Install the Sygate personal firewall software on the user's computer by following the instructions provided by Sygate.
2. Configure the Sygate personal firewall to allow access to your Aventail appliance:
 - a. With Sygate running, right-click the Sygate icon in the taskbar notification area, and then click **Advanced Rules**. The **Advanced Rules** dialog box appears.
 - b. Click **Add**. The **Advanced Rule Settings** dialog box appears.
 - c. On the **General** tab, in the **Rule Description** box, type a brief description for the rule (for example, "Allow all Aventail appliance traffic").
 - d. Under **Action**, click **Allow this traffic**.



- e. Click the **Hosts** tab, click **IP Address(es)**, and then type the IP address of the Aventail appliance.
- f. Click **OK**.

Zone Labs Setup

To use Aventail Connect with the Zone Labs personal firewall, you must install and configure the Zone Labs personal firewall software on each user's computer.

► To install and set up the Zone Labs personal firewall

1. Install the Zone Labs personal firewall software on the user's computer by following the instructions provided by Zone Labs.
2. Configure the Zone Labs personal firewall to allow access to your Aventail appliance.
 - a. Open the Zone Labs Integrity Desktop Control Center, and then click **Trusted**.
 - b. Click **Add**, and then add your protected network to the trusted zone by typing the appliance's DNS name.
 - c. Click **Apply**.

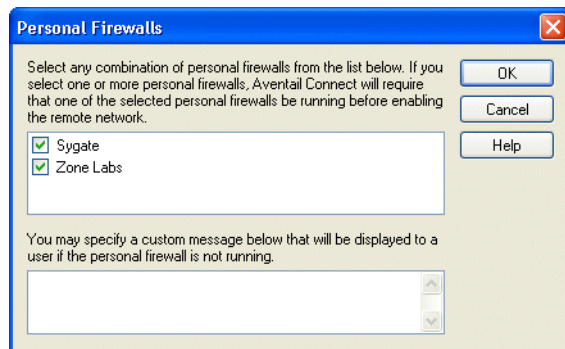
Aventail Connect Setup

To enable personal firewall integration in Aventail Connect, you must create a Connect 5.3 configuration file that requires users to be running a specified personal firewall whenever connecting to your protected network. To do this, you configure personal firewall settings in the Aventail Connect 5.3 Configuration Tool.

- ! **CAUTION** To edit a Connect 5.3 configuration file that includes personal firewall integration settings, you must use the Connect 5.3 Configuration Tool. Opening and then saving a Connect 5.3 configuration file with an earlier (pre-5.3) version of the Configuration Tool will cause all personal firewall settings to be lost.

► To enable personal firewall integration

1. On the **Network** tab, click **Personal Firewalls**. The **Personal Firewalls** dialog box appears.



2. Select any combination of personal firewalls from the list. If you select one or both personal firewalls (Sygate and Zone Labs), Connect will require that one of the selected personal firewalls be running before enabling the remote network.
3. Optionally, type a custom message that will be displayed to users if Aventail Connect detects that a required firewall is not running.
4. Click **OK**.

Access Server Settings

Access server settings are attributes of the network links that connect networks. This section describes how to configure server settings. You can specify secondary (fallback) servers in addition to primary servers. Primary servers and secondary servers have their own separate attributes.

Specifying a Proxy Server

You can specify whether a proxy server is required for network access, and you can define settings for the specified proxy server.

► To specify a primary proxy server

1. In the network view of the Configuration Tool, select the network link that connects the two networks.
2. On the **Access Server** tab for the network where the proxy server sits, under **Network Access**, click **Requires proxy server**.

The screenshot shows the 'Internet Access Server' configuration window. Under the 'Network Access' section, the 'Requires proxy server' radio button is selected. The 'Proxy Server' section contains three fields: 'Hostname or IP Address' with the value 'private.abccorp.com', 'Port' with the value '443', and 'Version' with a dropdown menu set to 'SOCKS v5'. At the bottom of the window, there are three buttons: 'Authentication...', 'Advanced...', and 'Help'.

3. In the **Hostname or IP Address** box, type the server's host name or IP address. If you are using SSL, you must type the server name exactly as it appears in the **Name** field of the server's certificate.
4. In the **Port** box, type the port number on which the server is listening.
5. In the **Type** box, select the server type (SOCKS v4, SOCKS v5, or HTTP).

Specifying a Fallback Proxy Server

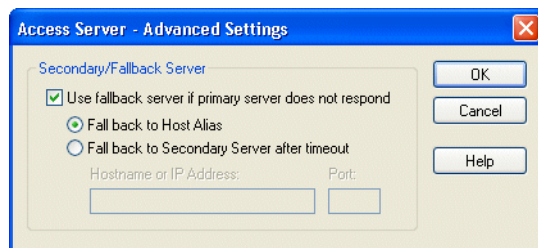
Aventail Connect allows you to define a secondary (fallback) server for any primary server. If the primary server is down or otherwise unable to accept connections, the connection falls back to the secondary server.

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

During normal operation, connections are directed to the primary server. If the primary server does not respond or accept a connection within two minutes, the connection is redirected to the secondary server. If the secondary server accepts the connection, all subsequent connections are automatically 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 direct traffic back to the primary server when it becomes available, you must restart the Aventail Connect client.

► **To specify a fallback proxy server**

1. On the **Access Server** tab for the network where the proxy server sits, click **Advanced**. The **Access Server Advanced Settings** dialog box appears.



2. Select the **Use fallback server if primary server does not respond** check box.
3. Click **Fall back to host alias** (to use DNS records for redundancy) or **Fall back to secondary server after timeout** (to fall back to the secondary server if the primary server times out).
4. If, in step 3, you clicked **Fall back to secondary server after timeout**, type the secondary server's host name or IP address and the port number on which the secondary server is listening. If you are using SSL, you must type the server name exactly as it appears in the **Name** field of the server's certificate. Click **OK**.

NOTE When a connection falls back to a secondary server, the user may be prompted for credentials for the fallback server.

Configuring Internet Access Proxy Detection

Aventail Connect can detect proxy settings in two ways. The two proxy-detection methods are:

- **Static URL:** This checks the URL AutoProxy browser settings in the registry. If a URL is found, it accesses the URL, fetches the configuration script, and then executes it to determine the correct proxy settings to be used to traverse the outbound firewall to connect to the Internet.
- **Dynamic URL:** The URL can be discovered via DHCP or DNS. The client then retrieves the URL via HTTP to fetch the configuration script, and then executes it to determine the proxy settings.

► **To configure Internet access proxy detection**

1. In the network view of the Configuration Tool, select the network link that connects the two networks.
2. On the **Internet Access Server** tab, select the **Network access requires a proxy server** check box.

The screenshot shows the 'Internet Access Server' configuration window. It has three tabs: 'Configuration', 'XYZ_Corp. Access Server', and 'Internet Access Server'. The 'Internet Access Server' tab is active. Under 'Network Access', there are three radio buttons: 'Requires proxy server' (selected), 'Does not require proxy server', and 'No network access available'. Under 'Proxy Server', there are three input fields: 'Hostname or IP Address' (empty), 'Port' (443), and 'Version' (SOCKS v5). A checkbox 'Perform Internet access proxy detection' is checked. At the bottom, there are buttons for 'Authentication...', 'Advanced...', and 'Help'.

3. Select the **Perform Internet access proxy detection** check box.

Authentication Options

Servers often require users to enter authentication credentials before allowing access to network resources. In the Aventail Connect Configuration Tool, you can enable authentication methods that will be offered to the server during the connection process. However, the server ultimately determines which authentication method is used. In the Aventail Connect Configuration Tool, each server has its own authentication settings.

Aventail Connect supports multiple authentication realms, which enables different groups of users to log in to different authentication repositories or servers. Multiple authentication realms can be useful if, for example, you require a more secure method of authentication for vendors and contractors than you do for remote employees.

Authentication options are configured on the **Access Server** tabs in the Configuration Tool. To display the **Access Server** tabs, click the network link that connects the two networks that you want to configure.

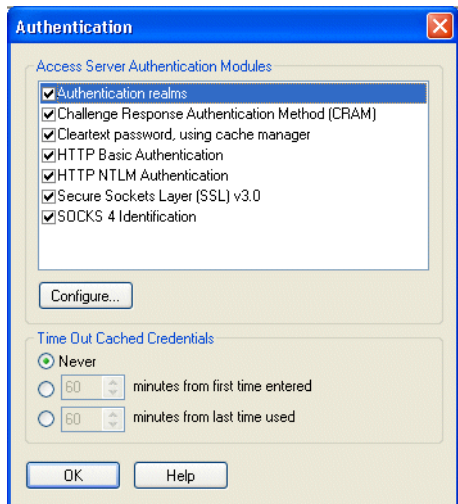
The Aventail Connect client supports multiple authentication methods.

Enabling Authentication Modules

You can enable multiple authentication modules. All enabled methods will be offered to the server during the connection process; however, the server ultimately determines which authentication method is used. For information about enabling authentication realms, see "Enabling Realms Support in Connect" on page 33.

► **To enable an authentication module**

1. On the **Access Server** tab for the network or organization where the proxy server sits, click **Authentication**. The **Authentication** dialog box appears.



2. Select the check box next to the authentication module(s) you want to enable, and then click **OK**.

Configuring SSL Options

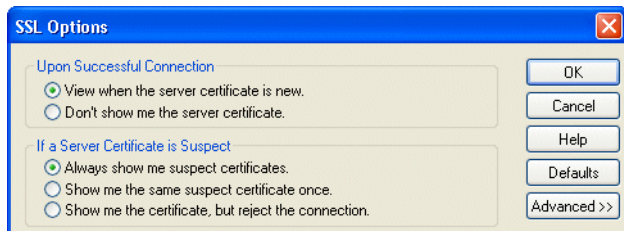
The Aventail Connect client supports Secure Sockets Layer (SSL) v3.0, a session-layer protocol for securing connections in a general, protocol-independent fashion.

This section explains how to configure the basic SSL options. For information about configuring advanced SSL options, see “Configuring Advanced SSL Options” on page 29.

To maintain the highest level of security, Aventail recommends configuring the Aventail Connect client to reject connections to servers that send suspect certificates.

► **To configure basic SSL options**

1. In the **Authentication** dialog box, select (highlight) **SSL v3.0 (domestic strength)**, and then click **Configure**. The **SSL Options** dialog box appears.



2. Under **Upon Successful Connection**, click one of the following:

- **View when the server certificate is new:** Upon successful connection, displays the server certificate if it has not been displayed before.
 - **Do not show me the certificate:** Never displays a valid server certificate.
3. Under **If a Server Certificate is Suspect**, click one of the following:
 - **Always show me suspect certificates:** Each time Aventail Connect suspects that a certificate might not be valid, it displays the certificate.
 - **Show me the suspect certificate once:** Once a suspect certificate has been accepted by the user, Aventail Connect does not display it again.
 - **Show me the certificate, but reject the connection:** Rejects the connection, but displays the suspect certificate.
 4. Click **OK** to finish, or click **Advanced** to configure the advanced SSL options. For more information about configuring advanced settings, see "Configuring Advanced SSL Options" on page 29.

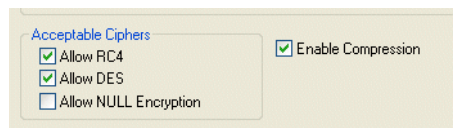
Configuring Advanced SSL Options

Advanced SSL options fall into four general categories: Acceptable ciphers, compression, server validation, and client certificates. This section describes how to configure the advanced SSL options.

For information about configuring basic SSL options, see "Configuring SSL Options" on page 28.

Configuring Acceptable Ciphers Options

The Aventail Connect client can offer the RC4, DES, and NULL encryption ciphers to the server.



► To configure acceptable cipher options

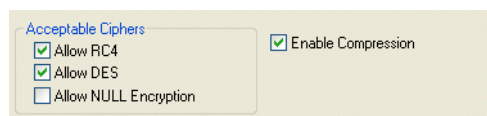
- In the **SSL Options** dialog box, under **Acceptable Ciphers**, click one of the following:
 - **Allow RC4:** Offers the RC4 cipher to the server.
 - **Allow DES:** Offers the DES cipher to the server.
 - **Allow NULL encryption:** Does not encrypt using SSL; uses SSL only to authenticate.

Configuring Compression Options

The Aventail Connect client can enable or disable compression. Compression can be useful when running on slower connections.

► **To configure compression options**

- In the **SSL Options (Advanced)** dialog box, select or clear the **Enable compression** check box.

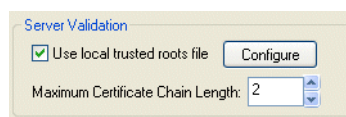


Configuring Server Validation Options

The Aventail Connect client can validate server certificates with trusted roots files. You can also specify a maximum certificate chain length.

► **To configure server validation options**

1. If you want to use a trusted roots file to validate trusted certificate chain roots, in the **SSL Options** dialog box, under **Server Validation**, select the **Use trusted roots file check** box.
2. In the **Maximum certificate chain length** box, specify the maximum allowable certificate chain length.



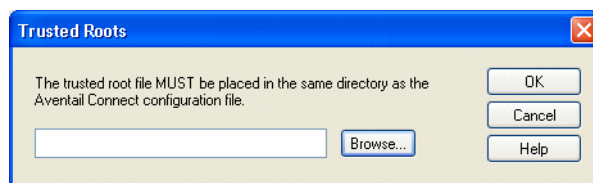
Configuring Trusted Roots Options

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. Under normal circumstances, the server provides the Aventail Connect client with a certificate to match one of Aventail Connect's trusted roots, if any exist.

If you are using a trusted roots file to validate trusted certificate chain roots, you must specify the trusted roots (.rot) file. Note that the trusted roots file must be placed in the Aventail Connect directory.

► **To specify a trusted roots file**

1. In the **SSL Options** dialog box, under **Server Validation**, select the **Use trusted roots file check** box, and then click **Configure**. The **Trusted Roots** dialog box appears.



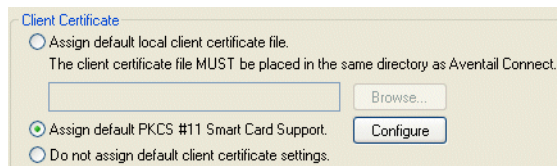
2. Type the path of the trusted roots file, or click **Browse** to locate it, and then click **OK**.

Configuring Client Certificate Options

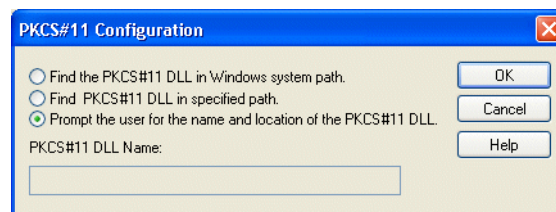
You can configure the Aventail Connect client to use a local client certificate, a certificate stored on a PKCS #11 smart card, or no client certificate.

► To configure client certificate settings

- In the **SSL Options** dialog box, under **Client Certificate**, click one of the three client certificate options:
 - If you plan to use different certificates with different servers, or if you plan to switch from one certificate to another, click **Do not assign default client certificate settings**. Users will be prompted to select an authentication/certificate method (for example, client certificate, PKCS #11 smart card, or no certificate) to use during each initial authentication exchange.
 - If you want the same client certificate to be sent to the server during every initial authentication exchange, click **Assign default local client certificate file** or **Assign default PKCS #11 smart card support**.
 - To load a local client certificate, click **Assign default local client certificate file**.
 - To load a client certificate that is stored on a PKCS #11 smart card, click **Assign default PKCS #11 smart card support**.



- If, in step 1, you clicked **Assign default local client certificate file**, click **Browse**, and then select the client certificate (.cer) file from the Aventail Connect directory. Only the filename, and not the path, of the certificate file loads via the **Browse** button.
- If, in step 1, you clicked **Assign default PKCS #11 smart card support**, click **Configure** and then, in the **PKCS #11 Configuration** dialog box, specify where the PKCS #11 DLL is located.



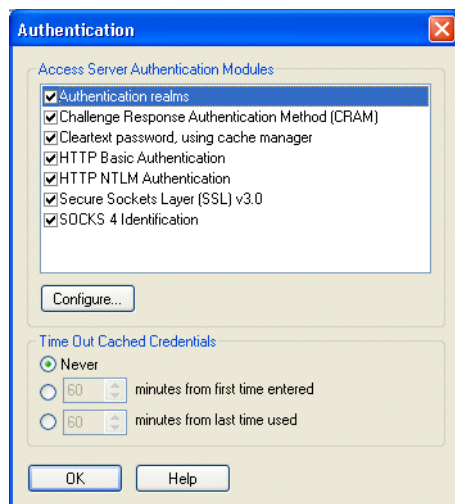
Configuring Credential Cache Timeout Settings

Credential caching retains a user's authentication credentials once the server has accepted them. Using credential caching, a user can enter credentials for a server once per Aventail Connect session, rather than once for each individual connection (a tedious task for applications such as Web browsers).

With the credential cache timeout option, you can control when credentials expire (time out). If a user has not made a connection to the Aventail appliance for the specified length of time, the credentials are automatically deleted from the credential cache. If credentials time out, the user must reauthenticate by entering the proper credentials before regaining access to the network. This feature can help to prevent unauthorized users from gaining access to secured areas.

► **To configure credential cache timeout settings**

1. On the **Access Server** tab for the network or organization where the proxy server sits, click **Authentication**. The **Authentication** dialog box appears.



2. Under **Timeout Cached Credentials**, click **Never**, **<x> minutes from first time entered**, or **<x> minutes from last time used**.
3. If, in step 2, you clicked **<x> minutes from first time entered** or **<x> minutes from last time used**, type the length of time (in minutes) that must pass before credentials expire.
4. Click **OK**.

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

Authentication Realms

An authentication realm is the combination of a directory (LDAP, RADIUS, or Active Directory), an authentication method (username/password, token or smart card, or digital certificate), and other configuration items that make the realm unique (for example, the LDAP search base or the specific directory server).

Visible and Hidden Realms

Realms can be visible or hidden; this setting is configured on the Aventail appliance. Hidden realms can be useful if you have multiple realms for multiple groups of users and you do not want certain groups of users to be aware of specific realms. For example, if you have separate realms for each of your suppliers, but you do not want the suppliers to know about one another, you could configure each of the realms to be hidden.

Any realms that are configured to be visible are displayed to the user as a list in the realm prompt. To log in to one of the visible realms, the user clicks the name of the realm that he or she wants to log in to. Although users can see all visible realms in the prompt, users can successfully connect to only the realms that they belong to.

Hidden realms are not displayed in the realm prompt. To log in to a hidden realm, the user must manually type the name of the appropriate realm at the prompt. If you configure a hidden realm on the appliance, be sure to share the realm name with the appropriate users.

How Realms Work

There are three main scenarios involving authentication realms. This section describes how each scenario would affect a user's Aventail Connect experience.

Scenario	User experience
Appliance configured with single realm	Aventail Connect never prompts the user to select a realm. The user is always automatically logged in to the realm that is configured on the appliance.
Appliance configured with multiple realms, but user belongs to only one realm	<p>After the user specifies a remote network when initiating a network connection, Aventail Connect prompts the user to specify the realm that he or she wants to log in to.</p> <p>When a user is a member of only one realm, the realm prompt is displayed only the first time the user initiates a connection to the remote network. For subsequent connection attempts, Connect will automatically log the user in to the applicable realm.</p>
Appliance configured with multiple realms, and user belongs to multiple realms	<p>Aventail Connect prompts the user to specify a realm each time he or she initiates a connection to the remote network.</p> <p>For any users that fall into this category, you must enable multiple realms support.</p>

Enabling Realms Support in Connect

To allow your users to authenticate to multiple realms, you must enable realms support in Aventail Connect. However, the appliance ultimately determines whether realms are used. To use authentication realms, the associated Aventail appliance must have multiple realms enabled.



Enabling authentication realms support does not enable multiple realms support; it only determines whether the authentication realms method is offered to the server. If your users will be logging in to multiple realms, you must enable multiple realms support in the Aventail Connect Customizer tool.

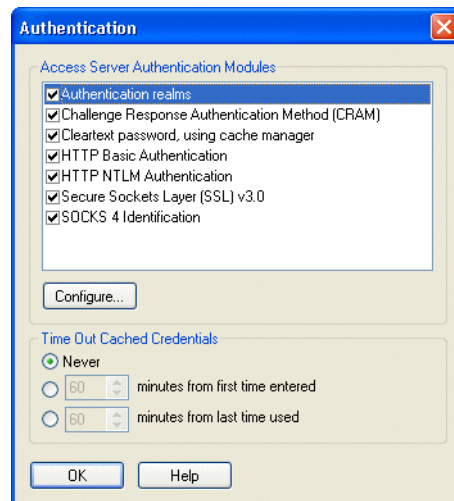
To summarize, enabling multiple realms support in Aventail Connect is a two-part process:

1. Enable realms support in the Aventail Connect Configuration Tool. (In most cases, realms support is enabled by default.)
2. Enable multiple realms in Customizer.

This section describes how to enable realms support. For more information about enabling multiple realms, see "Configuring Aventail Connect Startup Options" on page 59.

► To enable realms support in Connect

1. On the **Access Server** tab for the network or organization where the proxy server sits, click **Authentication**. The **Authentication** dialog box appears.



2. Select the **Authentication realms** check box, and then click **OK**.

Notes

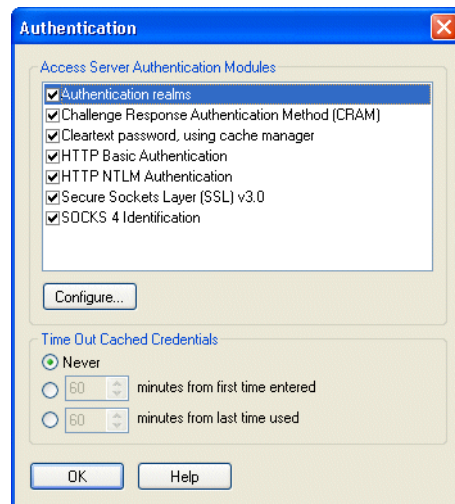
- When you create a new Aventail Connect 5.3 configuration file, authentication realms support is enabled by default. When you use the Aventail Connect 5.3 Configuration Tool to modify a configuration file that was created with the Aventail Connect 5.3 beta or earlier Configuration Tool, the authentication realms method is disabled by default.
- Authentication realms are not supported in Aventail Connect 4.x-mode configuration files.

Configuring Realms Options

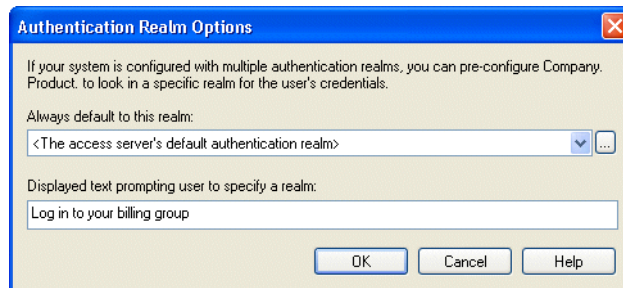
This section describes how to configure realms options in Aventail Connect.

► To configure realms options

1. On the **Access Server** tab for the network or organization where the proxy server sits, click **Authentication**. The **Authentication** dialog box appears.



2. Select (highlight) **Authentication realms**, and then click **Configure**. The **Authentication Realm Options** dialog box appears.



3. In the **Always default to this realm** box, click one of the options:
 - **No default authentication realm** configures no default realm. No default realm is displayed in the realm prompt, so the user must select a realm from the list or type the name of a hidden realm.
 - **The access server's default authentication realm** selects the default realm that is defined on the Aventail appliance. This realm is displayed to users as the default realm; however, users can select a different realm or type the name of a hidden realm. This option can be useful if your users belong to multiple realms but you expect that most users will be logging in to one particular realm most of the time.

- Any specific realm name that you have added to the list of available default realms. If you select one of these realms, the realm that you specify in this field will be displayed to users as the default realm at login. However, users can select a different realm or type the name of a hidden realm. This option can be useful if you are creating a setup package for a group of users who do not belong to the appliance's default realm.

You can click the **Browse** button to add names of any potential default realms to the **Always default to this realm** box. For more information, see "Prepopulating the Realm Name Cache," below.

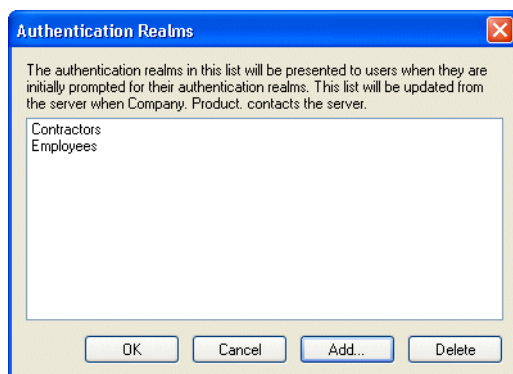
4. In the **Displayed text prompting user to specify a realm** box, type a message that will be displayed to users when they are prompted to specify a realm. For example, you might type "Select or enter your billing group" or "Select or enter your corporate division." If you do not type a message, the default message ("Select or enter your login group") will be displayed to users.
5. Click **OK**.

Prepopulating the Realm Name Cache

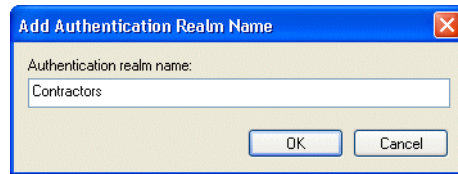
If you know the exact name of the default realm that you want to be displayed to users, you can add it to the list of available default realms in the **Always default to this realm** box in the **Authentication Realm Options** dialog box. Note that the realm name must be typed exactly as it is configured on the Aventail appliance. If you have users who belong to multiple realms, this prepopulates the list of realm names displayed to users the first time they initiate a connection to the remote network. After the first successful remote network connection, the cache of available realm names is updated every time Aventail Connect communicates with the appliance.

► **To add a realm name to the list of available default realms**

1. On the **Access Server** tab for the network or organization where the proxy server sits, click **Authentication**. The **Authentication** dialog box appears.
2. Select (highlight) **Authentication realms**, and then click **Configure**. The **Authentication Realm Options** dialog box appears.
3. To the right of the **Always default to this realm** box, click the **Browse (...)** button. The **Authentication Realms** dialog box appears.



- Click **Add**. The **Add Authentication Realm Name** dialog box appears.



- In the **Authentication realm name** box, type the name of the realm exactly as it is configured on the Aventail appliance, and then click **OK**.
- The realm name now appears in the list of available default realms in the **Authentication Realms** dialog box. Click **OK**.

The realm name now appears in the **Always default to this realm** list in the **Authentication Realm Options** dialog box.

Domain Options

Aventail Connect's Microsoft Networking Support allows you to access mapped Windows drives and work with files (including browsing, opening, copying, moving, and deleting) from remote computers via the Aventail Connect network connection. All interaction with the remote server can be secured. You can specify which local and remote computers are available to users. These computers are visible in the user's **Exploring - Microsoft Windows Network** window. (Domains are also visible in the user's Network Neighborhood if they are defined in the Aventail Connect configuration file.) Each network has its own Microsoft Networking Support settings, which are defined on the **Domains** tab of the Configuration Tool.

Generally, you will use Microsoft Networking Support to connect to a remote network through the Aventail Connect client. For example, you might use Microsoft Networking Support when:

- You are inside the office, on the corporate network, and you connect through the Aventail appliance to your company's remote site, or to another company's network.
- You are outside the office, and you connect your laptop through the Aventail appliance to your internal company network, or to another company's network.

This section explains how Microsoft Networking Support works and how to configure the domain settings.

How Microsoft Networking Support Works

To deliver a secured version of standard Windows browsing, the Aventail Connect client offers a secure alternative to Network Neighborhood. Microsoft Networking Support allows Aventail Connect to authenticate and encrypt TCP/IP traffic on NetBIOS ports in the same way that the Aventail Connect client performs these services for any other applications. This allows Aventail Connect to redirect Windows network traffic based on the settings defined in the Aventail Connect configuration file.

Microsoft Networking Support includes a browsing mode, which allows you to view a dynamic list of available Windows hosts. This eliminates the need to keep an updated static list of hosts. You can also manually specify static hosts in the configuration file.



Configuring Microsoft Networking Support

There are two methods for configuring Microsoft Networking Support:

- **Build a dynamic list of hosts and domains:** Microsoft Networking Support can automatically “browse” available computers and construct a dynamic list of hosts from your local network or a remote network. To use Microsoft Networking Support in browsing mode, you must identify the primary domain controller (PDC) for the domain.

The browsing mechanism can only locate computers that are within the user’s internal network. To search remote networks, you must specify, in the Aventail Connect configuration file, the host name of each remote server or the PDC of the remote network.

- **Create a static list of hosts and domains in the local configuration file:** To use Microsoft Networking Support in the static host list mode, you define, in the Aventail Connect configuration file, the individual hosts in the domain. This allows you to restrict access to those designated hosts. Static hosts are defined by specifying the Windows NetBIOS machine name.

You are not limited to using only one of the above methods for configuring Microsoft Networking Support. For example, if, in a given domain, you have computers that are not necessarily part of that domain, you can logically group them together in the configuration file by defining static hosts and dynamically discovering hosts by defining a PDC.

Choosing a Method

Each of the methods has its advantages and disadvantages, as illustrated in the table below.

Method	Advantages	Disadvantages
Listing individual hosts	You control exactly which hosts the user can view. On slower connections, this method is fastest because you do not need to send a list of servers to the client.	You must update the list of hosts manually if hosts are added to or removed from the domain.
Dynamically browsing hosts	You do not need to update the list of hosts if hosts are added to or removed from the domain.	You cannot control which computers appear in the Domains tab; all computers in the domain are displayed. On slower connections, this method is slower because a list of computers must be sent to the client.

The rest of this section describes how to work with static domains and hosts.

Adding Domains

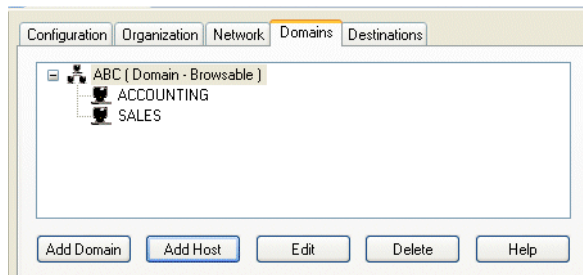
Domains are defined on the **Domains** tab of the Aventail Connect Configuration Tool.

► To define a domain

1. On the **Domains** tab of the Configuration Tool, click **Add Domain**. The **Add Static Domain** dialog box appears.

2. In the **Domain Name** box, type the name of the domain.
3. (Optional) In the **Comment** box, type a descriptive comment about the domain.
4. To enable the Microsoft Networking Support browsing mode, select the **Make domain browsable** check box, and then type the primary domain controller's (PDC) server name and (optionally) the PDC's DNS name or IP address. Click **OK**.

The domain is added to the list on the **Domains** tab.

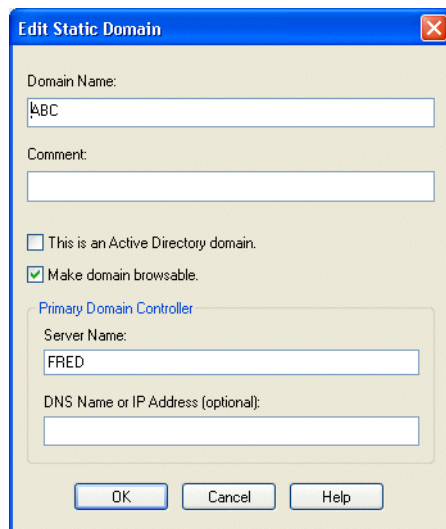


Editing Domains

Domains are defined on the **Domains** tab of the Aventail Connect Configuration Tool.

► **To edit a domain**

1. On the **Domains** tab of the Configuration Tool, select the domain that you want to edit, and then click **Edit Domain**. The **Edit Static Domain** dialog box appears.



The screenshot shows the 'Edit Static Domain' dialog box. It has a title bar with the text 'Edit Static Domain' and a close button. The dialog contains the following fields and options:

- Domain Name: ABC
- Comment: (empty text box)
- This is an Active Directory domain.
- Make domain browsable.
- Primary Domain Controller section:
 - Server Name: FRED
 - DNS Name or IP Address (optional): (empty text box)
- Buttons: OK, Cancel, Help

2. Make any necessary changes, and then click **OK**.

Deleting Domains

Domains are defined on the **Domains** tab of the Aventail Connect Configuration Tool. Before deleting a domain, understand how the deletion will affect the configuration.

► **To delete a domain**

- On the **Domains** tab of the Configuration Tool, select the domain that you want to delete, and then click **Delete**.

Adding Hosts

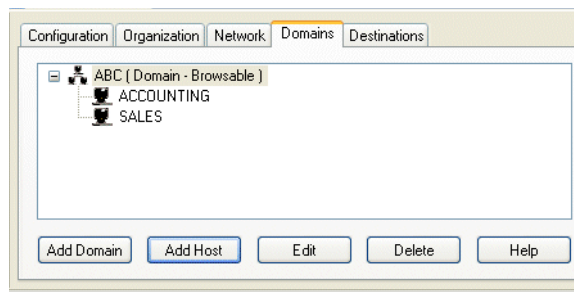
Hosts are defined on the **Domains** tab of the Aventail Connect Configuration Tool.

► **To define a host**

1. Select the appropriate domain in the list on the **Domains** tab, and then click **Add Host**. The **Add Static Host** dialog box appears.

2. In the **Server Name** box, type the Windows NetBIOS name of the host.
3. (Optional) In the **DNS Name or IP Address** box, type the host's DNS name or IP address.
4. (Optional) In the **Comments** box, type a comment that describes the host. Click **OK**.

The host is added to the list on the **Domains** tab.

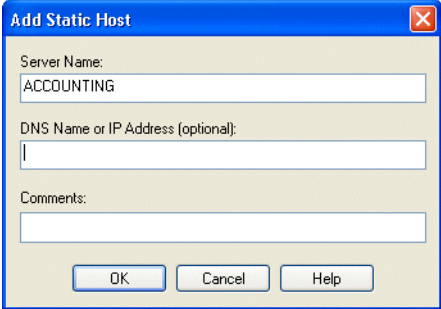


Editing Hosts

Hosts are defined on the **Domains** tab of the Aventail Connect Configuration Tool.

► **To edit a host**

1. On the **Domains** tab of the Configuration Tool, select the host that you want to edit, and then click **Edit Host**. The **Add Static Host** dialog box appears.



2. Make any necessary changes, and then click **OK**.

Deleting Hosts

Hosts are defined on the **Domains** tab of the Aventail Connect Configuration Tool. Before deleting a host, understand how the deletion will affect the configuration.

► **To delete a host**

- On the **Domains** tab of the Configuration Tool, select the host that you want to delete, and then click **Delete**.

Destination Options

You can include specific network destinations to which the Aventail Connect client will route traffic via the Aventail appliance. You can also exclude destinations; Aventail Connect will not route traffic to these excluded destinations.

Note that a network or organization can also have no destinations at all.

Defining Destinations

Destinations specify the network or host addresses that are to be routed via the Aventail Connect client through the Aventail appliance. Destinations are based on either IP address or host/domain name, but not both. Each destination can include a port range and one of the following settings:

- TCP traffic only (redirects only TCP traffic)
- UDP traffic only (redirects only UDP traffic)
- TCP and UDP traffic (redirects both TCP and UDP traffic)

There are five types of destinations, as described in the table below.

Destination type	Example(s)
Host name (fully qualified or unqualified)	bart.private.aventail.com bart b*
Domain name	private.aventail.com aventail.com
IP address	192.168.1.1
IP address/subnet mask	192.168.1.0 / 255.255.255.0
IP address range	192.168.1.60 - 192.168.1.99

When domain destination lookups are performed by name, the Aventail Connect client orders destinations based on how specific they are. The more precise a destination, the higher its priority.

For example, although a lookup for the server private.in.aventail.com would match all three of the destination entries listed below, they are accessed in order of priority.

1. private.in.aventail.com
2. in.aventail.com
3. aventail.com

Wildcards in Host and Domain Name Definitions

The Aventail Connect client supports the use of wildcard characters in destination host and domain names. You can use wildcards when defining named, single-host destinations; however, 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*a.in.aventail.com matches **extra.in.aventail.com**
e?tra.in.aventail.com matches **extra.in.aventail.com**
e?a.in.aventail.com does NOT match **extra.in.aventail.com**

You can use any combination of "?" and "*" characters between each DNS segment. However, each segment 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.??.aventail.com

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**

Avoiding Conflicts

Conflicts occur when destinations from multiple networks overlap. The following table illustrates how conflicts can arise between two example networks, Network 1 and Network 2.

i **NOTE** Conflicts do not occur when running in restricted or standard remote network access modes. The information in this section refers only to configurations running in **Multiple networks with local network access** mode.

Reason for conflict	Network 1	Network 2
Same domain or host name	in.aventail.com	in.aventail.com
Same IP address	192.168.1.1	192.168.1.1
Overlapping IP address ranges or subnets	192.168.1.1 - 192.168.1.100	192.168.1.1 / 255.255.255.0
Unqualified host names	private	private
Unqualified host names with wildcards	p*	private

Adding Destinations

When you include a destination, the Aventail Connect client redirects traffic to that destination via the Aventail appliance.



► **To add a destination**

1. In the Configuration Tool, click the **Destinations** tab, and then click **Add**. The **Add Destination** dialog box appears.

2. In the **Type** box, select the type of destination you want to add.
3. In the **Disposition** box, click **Include Destination**.
4. Fill in the following fields, which vary depending on the type of destination you selected in step 2.
 - (**Host Name** destination type only) In the **Host** box, type the name of the host. Wildcard characters are permitted.
 - (**Domain Name** destination type only) In the **Domain** box, type the name of the domain. Wildcard characters are permitted.
 - (**IP Address** and **IP Address/Subnet Mask** destination types only) In the **Address** box, type the host's IP address.
 - (**IP Address Range** destination type only) In the **From/To** boxes, type the beginning and ending IP addresses of the range.
 - (**IP Address/Subnet Mask** destination type only) In the **Subnet** box, type the host's subnet mask.
 - In the **Protocol** box, select one of the three options.
 - If applicable, under **Ports**, click **Single Port** or **Port Range**.
 - If applicable, type or select the port or port range.
5. (Optional) In the **Comment** box, type a comment that describes the destination, and then click **OK**.

Excluding Destinations

You can exclude specific destinations on the **Destinations** tab in the Configuration Tool. When you exclude a destination, Aventail Connect does not redirect traffic to that destination.

► **To exclude a destination**

1. In the Configuration Tool, click the **Destinations** tab, and then click **Add**. The **Add Destination** dialog box appears.

2. In the **Type** box, select the type of destination you want to exclude.
3. In the **Disposition** box, click **Exclude Destination**.
4. Fill in the following fields, which vary depending on the type of destination you selected in step 2.
 - (**Host Name** destination type only) In the **Host** box, type the name of the host.
 - (**Domain Name** destination type only) In the **Domain** box, type the name of the domain.
 - (**IP Address** and **IP Address/Subnet Mask** destination types only) In the **Address** box, type the host's IP address.
 - (**IP Address Range** destination type only) In the **From/To** boxes, type the beginning and ending IP addresses of the range.
 - (**IP Address/Subnet Mask** destination type only) In the **Subnet** box, type the host's subnet mask.
 - In the **Protocol** box, select one of the three options.
 - If applicable, under **Ports**, click **Single Port** or **Port Range**.
 - If applicable, type or select the port or port range.
5. (Optional) In the **Comment** box, type a comment that describes the destination, and then click **OK**.

Editing Destinations

Destinations are configured on the **Destinations** tab in the Configuration Tool.

► **To edit a destination**

1. On the **Destinations** tab in the Configuration Tool, select the destination that you want to modify, and then click **Edit**. The **Edit Destination** dialog box appears.

2. Modify the settings as necessary, and then click **OK**.

Deleting Destinations

Destinations are configured on the **Destinations** tab in the Configuration Tool. Before deleting a destination, understand how the deletion will affect your configuration.

► **To delete a destination**

- On the **Destinations** tab in the Configuration Tool, select the destination that you want to remove, and then click **Delete**.

The destination is removed from the list.



Chapter 3

Deployment

This chapter describes how to create and distribute custom setup packages with the Aventail Connect Customizer tool, and it explains how to update existing local configuration files that are already deployed to users.

Planning a Deployment

The following tips can help you plan an Aventail Connect deployment more efficiently.

Updating Configurations

If you need to deploy only an updated configuration file to users, you might want to use the Aventail Connect configuration update feature instead of deploying a full Aventail Connect setup package to users. Deploying an Aventail Connect setup package requires users to reboot their computers after package installation, while a configuration update does not require a reboot. In addition, deploying a configuration file update changes only the user's configuration file; all other Aventail Connect settings remain intact. Deploying a full setup package replaces the user's Aventail Connect settings with those specified in the new setup package. For more information, see "Updating Configurations" on page 68.

Updating Aventail Connect Software and Setup Packages

If you want to ensure that users are running the most recent Aventail Connect software or have installed your latest setup packages, enable the Aventail Connect software updating feature. When software updating is enabled, Aventail Connect checks the specified network location for Aventail Connect software or setup package updates at the specified interval.

If you want to ensure that users are running only the most recently released version of the Aventail Connect software, use the default Aventail-provided URL in the **URL to download software updates from** box on the **Software Updates** page of the **Aventail Connect Customizer Tool** window. This updates only the Aventail Connect software; all other Aventail Connect settings and configuration files remain intact.



If, on the other hand, you want to distribute a new or updated Aventail Connect setup package to users, you must specify a URL that you will upload new or updated packages to. Deploying a new or updated setup package replaces the user's Aventail Connect settings with those specified in the new setup package.

For more information, see "Configuring Software Updating Options" on page 64.

Minimizing Setup Package Size

If package size is a concern, select components carefully in the Aventail Connect Customizer tool. For example, including the Microsoft Installer (MSI) software in a setup package will significantly increase the package size. In some cases, you might find that creating two separate, smaller packages is preferable to creating one larger package.

Digitally Signing Setup Packages

To increase security, digitally sign all setup packages, and configure each package to require a digital signature. For more information, see "Configuring Package Signing Options" on page 66.

Customizing the Aventail Connect User Interface

Aventail Connect interface customizations are considered advanced tasks. Familiarize yourself with the Aventail Connect product before performing any customizations to the user interface. To ensure that users can use Aventail Connect properly and can connect to remote networks correctly, use caution when making any interface customizations.

Testing Packages

To ensure that software updating and other features work properly, test each package before distributing it to users.

Minimizing User Interaction

To create an Aventail Connect installation that requires minimal user interaction, follow these guidelines when customizing the setup package:

- Perform a silent installation during which no status dialogs or messages are displayed, and no user interaction is required. For more information, see "Configuring Installation Prompt Options" on page 54.
- Run Aventail Connect automatically when Windows starts. For more information, see "Configuring Installation Directory and Automatic Startup Options" on page 55.
- Disable the Aventail Connect splash screen that is normally displayed when Aventail Connect starts. For more information, see "Configuring Aventail Connect Startup Options" on page 59.
- Disable the dialog box that prompts users to specify a configuration file and local network that is normally displayed at Aventail Connect startup. For more information, see "Configuring Aventail Connect Startup Options" on page 59. In addition, you can specify a default configuration file, and you can configure Aventail Connect to automatically detect each user's local network. For more information, see "Specifying Configuration File Settings" on page 60, "Configuring Network Settings" on page 62, and "Configuring Remote Network Access Settings" on page 61.



- Specify a default remote network. For more information, see "Configuring Remote Network Access Settings" on page 61.
- Enable single sign-on using Windows credentials, which automatically forwards users' Windows credentials to use for Aventail Connect authentication. Note that this feature is supported only when each user's Windows credentials are the same as his or her Aventail Connect credentials. For more information, see "Configuring Windows Domain Logon Options" on page 63.
- Disable the prompt that is normally displayed to users before terminating remote connections at shutdown. For more information, see "Configuring Advanced Settings for Aventail Connect Software" on page 64.
- Disable the prompt that is normally displayed to users before merging configuration fragment (.cff) files. For more information, see "Configuring Advanced Settings for Aventail Connect Software" on page 64 and "Updating Configurations" on page 68.
- If your remote network supports multiple realms, consider creating a separate Aventail Connect setup package for each realm's group of users. In each setup package, set the default realm to be the one used by that group. This will prevent users from needing to know which realm they are in and needing to select the correct realm from a list of possible realms when connecting.

Customized Configuration and Distribution

This section describes how to create and distribute custom Aventail Connect setup packages with the Aventail Connect Customizer tool.

Deploying Aventail Connect Packages

In general, the process of installing the Aventail Connect client to multiple networked workstations involves placing a customized Aventail Connect package—created with the Aventail Connect Customizer tool—in a shared network directory, on a Web server, or in another publicly accessible location and then pointing users to the package file. The most common ways of distributing a setup package are:

- Placing the package on an HTTP or HTTPS server.
- Placing the package on an FTP site.
- Placing the package 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 file automatically extracts an Aventail Connect installation package and initiates setup.

Customizer Overview

The Aventail Connect Customizer tool allows you to customize Aventail Connect installation packages for distribution to multiple networked client workstations. Distributing preconfigured setup packages eliminates the need for users to make installation and setup decisions at their workstations, and gives administrators fine-grained control over how users work with Aventail Connect.



Customizer saves each installation package as a self-extracting executable (.exe) file. Each executable file has an associated *version.ini* file, which is stored in the same directory as the .exe file.

- ! **CAUTION** Do not store more than one custom setup package in any directory. Each package has an associated file named *version.ini*, which is stored in the same directory as the package. A directory cannot contain more than one *version.ini* file. If you create multiple custom setup packages, you must store each package in a separate directory.

You can configure a package to suit your network specifications, and you can easily modify and redistribute an Aventail Connect installation package if your network specifications change.

You can customize a setup package by adding files (such as Aventail Connect configuration files, client certificate files, trusted roots files, or logo bitmap files) to it, or by specifying setup information to meet various client-access needs of individuals or workgroups. You can also customize many of the Aventail Connect user interface components, specify default settings, and configure Aventail Connect software updating options. For more information about the Customizer options, see "Specifying Customizer Options" on page 54.

- i **NOTE** All setup packages created with the Aventail Connect 5.3 Customizer tool include the Aventail Connect 5.3 software. The Aventail Connect 5.3 Customizer tool can modify only Aventail Connect 5.3 packages. You cannot use the Aventail Connect 5.3 Customizer to view or modify packages created with earlier versions of the Aventail Connect Customizer.

Starting Customizer

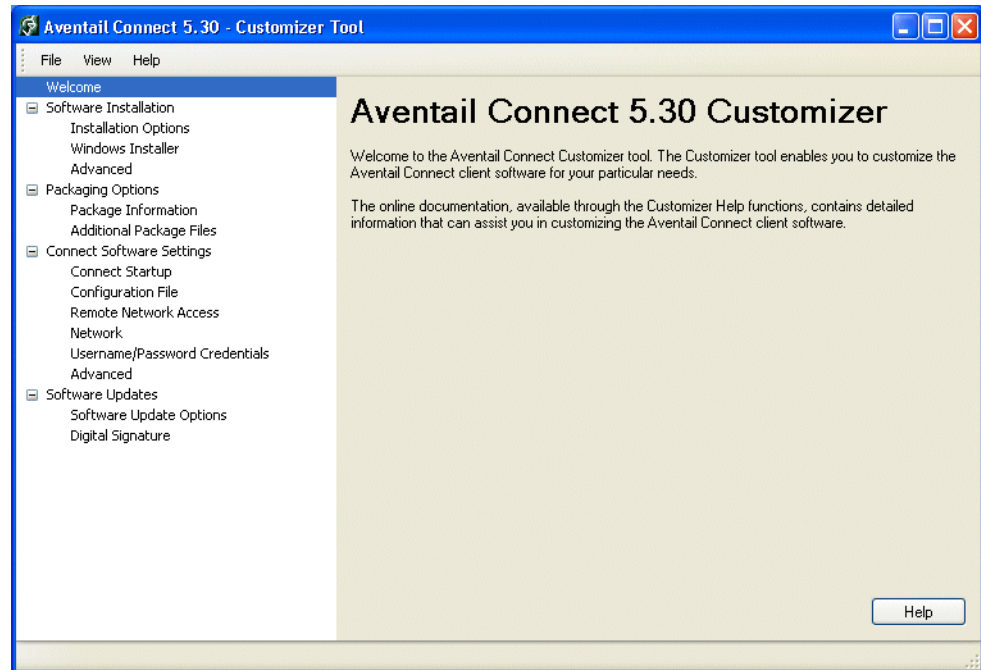
The Customizer tool is used to create and modify custom Aventail Connect setup packages.

► To start Customizer

- From the **Start** menu, point to **Programs**, point to **Aventail Connect 5.30 Administrator Tools**, and then click **Aventail Connect Customizer**.



The **Aventail Connect Customizer Tool** window appears.



Creating New Packages

Most Customizer settings are optional; you can configure settings according to your network requirements.

► To create a new setup package

- In the **Aventail Connect Customizer Tool** window, on the **File** menu, click **New**.

For information about Customizer options, see “Specifying Customizer Options” on page 54.

Editing Existing Packages

You can easily reconfigure and redistribute Aventail Connect setup packages if your network requirements change.

NOTE The Aventail Connect 5.3 Customizer creates Aventail Connect 5.3 setup packages, and it can modify only Aventail Connect 5.3 packages. You cannot use the Aventail Connect 5.3 Customizer to view or modify packages created with earlier versions of the Aventail Connect Customizer.

► To edit an existing setup package

1. In the **Customizer** window, on the **File** menu, click **Open**, select the package that you want to edit, and then click **Open**.

2. Modify the setup package as needed and then, on the **File** menu, click **Save** or **Save As**.

For information about Customizer options, see “Specifying Customizer Options” on page 54.

Saving Packages

Aventail Connect Customizer saves each installation package as a self-extracting executable (.exe) file. Each executable file has an associated *version.ini* file, which is stored in the same directory as the .exe file.

- ! **CAUTION** Do not store more than one custom setup package in any directory. Each package has an associated file named *version.ini*, which is stored in the same directory as the package. A directory cannot contain more than one *version.ini* file. If you create multiple custom setup packages, you must store each package in a separate directory.

► To save a setup package

1. In the **Aventail Connect Customizer Tool** window, on the **File** menu, click **Save** or **Save As**.
2. Type a file name in the **File name** box, and then click **Save**.

Specifying Customizer Options

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 package size is a concern, select options carefully to keep the package size manageable.

This section describes how to configure the settings in the **Aventail Connect Customizer Tool** window.

Configuring Installation Prompt Options

You can specify the level of prompting displayed to users during Aventail Connect installation. You can also disable all installation prompts.

► **To configure the installation prompting level**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Software Installation**, and then click **Installation Options**. The **Installation Options** page appears.

Installation Options

Installation prompting level

Full: All wizard status dialogs, prompts, and error messages are displayed

Reduced: Only wizard status dialogs are displayed; user is prompted to restart the computer upon installation completion

Basic: Only simple progress and error-handling messages are displayed; user is prompted to restart the computer upon installation completion

None: Completely silent installation; computer is not restarted unless the check box below is selected

Restart the computer without prompting the user

NOTE: Aventail cautions against restarting the user's computer without giving the user an opportunity to save any work.

2. Under **Installation prompting level**, click the level of user prompting to perform during Aventail Connect installation.

- **Full:** All wizard status dialog boxes, prompts, and error messages (if errors occur) are displayed during Aventail Connect installation. The user is prompted to restart the computer after installation. This is the default setting.
- **Reduced:** Only wizard status dialog boxes and error messages (if errors occur) are displayed during Aventail Connect installation. The user cannot change the installation directory or automatic-startup settings. The user is prompted to restart the computer after installation.
- **Basic:** Only simple progress and error messages (if errors occur) are displayed during installation. The user cannot change the installation directory or automatic-startup settings. The user is prompted to restart the computer after installation.
- **None:** A "silent" installation is performed. No prompts or messages are displayed during installation. The user cannot change the installation directory or automatic-startup settings.

To automatically restart the user's computer after installation without first displaying a prompt, select the **Restart the computer without prompting the user** check box. If you select this check box, the user is not prompted to save any work before the computer is restarted; the user may lose any unsaved changes. Aventail recommends disabling this option by clearing this check box.

Configuring Installation Directory and Automatic Startup Options

You must specify the directory where the Aventail Connect software and associated files will be installed on users' computers. If you do not specify a directory, the Aventail Connect software and associated files are installed to the default directory of `%ProgramFiles%\Aventail\Connect`, where `%ProgramFiles%` is the system drive and directory where each user's program files are located. (On most systems, this is `C:\Program Files\.`)



You can also configure whether Aventail Connect starts automatically when Windows starts and whether Windows domain logon support is installed. If you enable the **Run Aventail Connect when Windows starts** option, on the Windows 2000 Professional and Windows XP Professional operating systems, the Aventail Connect graphical identification and authentication (GINA) API and Windows domain logon support are installed on users' computers, and Aventail Connect automatically starts at Windows logon time. On Windows XP Home Edition, Windows Me, and Windows 98 operating systems, Aventail Connect automatically starts at Windows logon time; however, the Aventail Connect GINA and Windows domain logon support are not installed.

NOTE To install Windows domain logon support, no other third-party GINA APIs can be installed on the user's computer.

► **To configure installation options**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Software Installation**, and then click **Installation Options**. The **Installation Options** page appears.

2. Under **Installation options**, specify the directory where you want Aventail Connect to be installed. The default install directory is `%ProgramFiles%\Aventail\Connect\`.
3. To configure Aventail Connect to automatically start when Windows starts, select the **Run Aventail Connect when Windows starts** check box. When this option is disabled, users must manually start the Aventail Connect client via the Start menu.

Configuring Microsoft Windows Installer Options

Aventail Connect uses the Microsoft Windows Installer (MSI) utility to install, upgrade, and uninstall the Aventail Connect client software. Some versions of Windows ship without the MSI software, or with an outdated version of it. Aventail Connect can install or upgrade the MSI software on the user's computer during the Aventail Connect installation process. You can bundle the MSI software with the Aventail Connect package or specify a URL from which to download it.



► **To configure Microsoft Windows Installer options**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Software Installation**, and then click **Windows Installer**. The **Windows Installer Options** page appears.

Windows Installer Options

Microsoft Windows Installer

Some versions of Microsoft Windows ship without, or with an older version of, the Microsoft Windows Installer (MSI) software. Aventail Connect may need to upgrade or install the MSI software on some systems.

Do not install Aventail Connect if the correct version of Microsoft Windows Installer is not currently installed

Include Microsoft Windows Installer in the package

Download Microsoft Windows Installer from one of these URLs if needed:

MSI installation for Windows 98 and Windows Me:

<http://update.aventail.com/connect/instmsi.exe>

MSI installation for Windows NT, Windows 2000, and Windows XP:

<http://update.aventail.com/connect/instmsiw.exe>

2. Click one of the MSI options:
 - **Do not install Aventail Connect if the correct version of Microsoft Windows Installer is not currently installed:** If the required version of the MSI software is not already installed on the user's computer, the Aventail Connect installation is canceled and the required MSI software is not installed.
 - **Include Microsoft Windows Installer in the package:** The MSI software is bundled in the Aventail Connect setup package. If the required version of MSI is not installed on the user's computer, the MSI software is installed during the Aventail Connect installation process. Note that including the MSI software in the setup package will significantly increase the size of the package.
 - **Download Microsoft Windows Installer from one of these URLs if needed:** If the required version of MSI is not installed on the user's computer, the MSI software is downloaded from the specified URL and installed during the Aventail Connect installation process. This is the default setting.

If you select this option, you must also specify a URL from which Aventail Connect will download the MSI software. If you do not specify a URL, Aventail Connect will download the MSI software from a default URL provided by Aventail.

Configuring Advanced Installation Options

You can run another command on the user's computer immediately following Aventail Connect installation from the package. You can use this feature to run a system program that is already installed on the user's computer or an executable file that is included in the setup package. For security reasons, this feature is not supported when the user receives the package as the result of an Aventail Connect software update.

The specified command runs only once, immediately following Aventail Connect installation from a custom setup package. The command is executed before the user is prompted to restart the computer.



► **Specifying a command to execute after installation**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Software Installation**, and then click **Advanced**. The **Advanced Installation Options** page appears.

2. In the **Post-installation command** box, type a command to run after the Aventail Connect package is installed.

Configuring Package Information Options

You can assign a company name, author name, or other identifying information to a package. Any information that you specify here is displayed on the **Package Information** page when the package is opened in Customizer; this can be useful if more than one administrator manages setup packages. If you enable software updating, the text that you type in the **Company Name** box is displayed to users in the **Connect Software Update** dialog box when an update is available.

Note that the **Last modified** box displays the date and time, in Greenwich Mean Time (GMT), when the package was last saved; this information cannot be modified.

► **To configure package information**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Packaging Options**, and then click **Package Information**. The **Package Information** page appears.

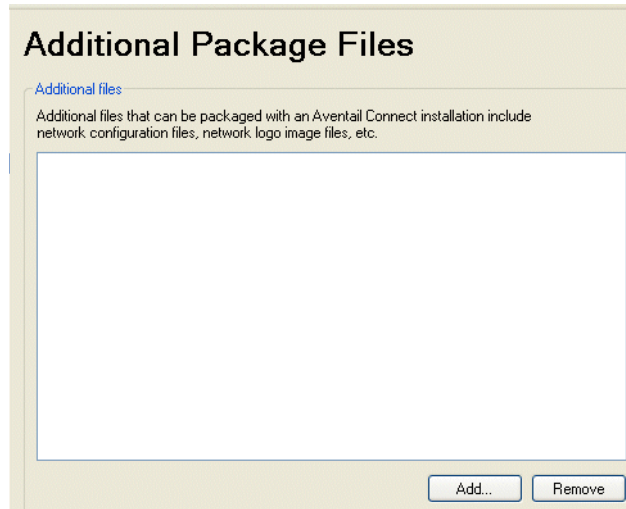
2. In the **Company name** box, type the name of the company issuing the package.
3. In the **Author** box, type the name of the package author.
4. In the **Description** box, type a descriptive comment about the package.

Adding Files to a Package

You can add files—such as configuration files, trusted roots files, or logo image files—to a setup package. Any files that you include in a setup package are automatically installed in the Aventail Connect directory during the Aventail Connect installation process.

► **To add a file to a package**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Packaging Options**, and then click **Additional Package Files**. The **Additional Package Files** page appears.



2. Click **Add**, select any files that you want to add to the package, and then click **Open**.

► **To remove a file from a package**

- On the **Additional Package Files** page, in the **Additional files** box, select the file or files that you want to remove, and then click **Remove**.

Configuring Aventail Connect Startup Options

This section describes how to customize the **Startup Options** section on the **General** tab of the **Aventail Connect Options** dialog box, and how to specify default startup options.

Aventail recommends that you familiarize yourself with the Aventail Connect product before customizing the user interface. Before removing any Aventail Connect interface components, consider how the customization will affect users' ability to connect to their network resources.

► **To configure startup options**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Connect Startup**. The **Connect Startup Options** page appears.

Connect Startup Options

Remove the Startup Options from the General tab of the Aventail Connect Options dialog box

Default startup options

Display the Aventail Connect splash screen at startup

Prompt for configuration file and local network at startup

Enable support for multiple realms

Remove the "Enable support for multiple realms" check box from the Startup Options of the Aventail Connect Options dialog box

2. Configure startup options as necessary:
 - To remove the **Startup Options** section from the **General** tab of the **Aventail Connect Options** dialog box, select the **Remove the Startup Options...** check box.
 - To display the Aventail Connect splash screen each time Aventail Connect starts, under **Default startup options**, select the **Display the Aventail Connect splash screen at startup** check box.
 - To prompt users to specify a configuration file and a local network at startup, select the **Prompt for configuration file and local network at startup** check box.
 - To enable multiple realms support, select the **Enable support for multiple realms** check box. When multiple realms support is enabled, Aventail Connect prompts the user to specify a realm each time he or she initiates a connection to the remote network. Typically, you will need to enable this option only if you have users who belong to multiple realms. For more information, see "Authentication Realms" on page 32.
 - To remove the control that enables and disables multiple realms support from the **Advanced** tab of the **Aventail Connect Options** dialog box, select the **Remove the "Enable support for multiple realms..."** check box. If all of your users belong to a single realm, Aventail recommends removing this control (by selecting this check box). However, if you have users who belong to multiple realms, including this control in the **Aventail Connect Options** dialog box can be useful. For example, if an employee belongs to multiple realms but typically logs in to only one realm, he or she can manually disable the realm prompt; this configures Aventail Connect to automatically log the user in to the default realm.

Specifying Configuration File Settings

You can include or remove the **Network Configuration** section on the **General** tab of the **Aventail Connect Options** dialog box. You can also specify a default configuration file; when users start the Aventail Connect client after installation, the Aventail Connect client runs with this default configuration file.



Aventail recommends that you familiarize yourself with the Aventail Connect product before customizing the user interface. Before removing any Aventail Connect interface components, consider how the customization will affect users' ability to connect to their network resources.

► **To specify configuration file settings**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Configuration File**. The **Configuration File Settings** page appears.

2. To remove the **Network Configuration** settings from the **General** tab of the **Aventail Connect Options** dialog box, select the **Remove the Network Configuration settings...** check box.
3. To specify a default configuration file, select a configuration file in the **Network configuration file** list, or click the **Browse** button to locate it and add it to the setup package.
4. To display a status bar on the **General** tab of the **Aventail Connect Options** dialog box while Aventail Connect is checking for configuration updates, select the **Show configuration updating status** check box.

Configuring Remote Network Access Settings

You can specify default remote network settings, and include or remove selected remote network access options.

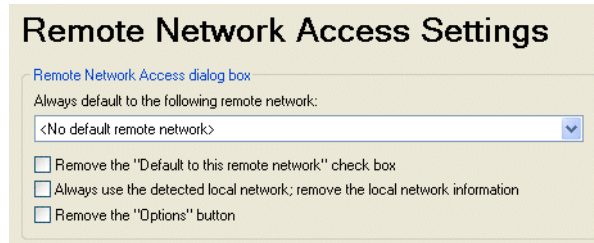
If you specify a default remote network, Aventail Connect attempts to connect to the specified remote network at each startup. If the connection to the default remote network fails, Aventail Connect then prompts the user to specify a remote network.

The list of available default remote networks (in the **Always default to the following remote network** list) is populated with the networks that are defined in the default configuration file. You must specify a default configuration file before you can specify a default remote network. For information about specifying a default configuration file, see "Specifying Configuration File Settings" on page 60.

Aventail recommends that you familiarize yourself with the Aventail Connect product before customizing the user interface. Before removing any Aventail Connect interface components, consider how the customization will affect users' ability to connect to their network resources.

► **To configure remote network access settings**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Remote Network Access**. The **Remote Network Access Settings** page appears.



2. To specify a default remote network, select the remote network name from the **Always default to the following remote network** list.
3. To remove the **Default to this remote network** check box from the **Remote Network Access** dialog box, select the **Remove the "Default to this remote network" check box** check box.
4. To set the default local network to that detected by Aventail Connect, and to remove the local network prompt from the **Remote Network Access** box, select the **Always use the detected local network; remove the local network information** check box. If you select this check box, Aventail recommends also selecting the **Automatically detect local network** check box on the **Network Settings** page. For more information, see "Configuring Network Settings" on page 62.
5. To remove the **Options** button, which opens the **Aventail Connect Options** dialog box from the **Remote Network Access** dialog box, select the **Remove the "Options" button** check box.

Configuring Network Settings

You can configure local network settings, and include or remove selected options on the **Network** tab of the **Aventail Connect Options** dialog box.

Aventail recommends that you familiarize yourself with the Aventail Connect product before customizing the user interface. Before removing any Aventail Connect interface components, consider how the customization will affect users' ability to connect to their network resources.

► **To configure network settings**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Network**. The **Network Settings** page appears.

2. To remove the **Local Network** settings from the **Network** tab of the **Aventail Connect Options** dialog box, select the **Remove the Local Network settings from the Network tab of the Aventail Connect Options dialog box** check box. Note that removing the **Local Network** options from the **Aventail Connect Options** dialog box will prevent users from changing their local networks and could potentially prevent users from connecting to their network resources.
3. To have Aventail Connect automatically detect the user's local network, select the **Automatically detect local network** check box.
4. To remove the **Remote Network** section from the **Network** tab of the **Aventail Connect Options** dialog box, select the **Remove the Remote Network settings...** check box.

Configuring Windows Domain Logon Options

Aventail Connect supports Windows domain logon (single sign-on) functionality, which, when enabled, allows users to automatically log on to Aventail Connect with their Windows credentials. (Windows domain logon functionality is supported on the Windows 2000 and Windows XP Professional operating systems.)

► **To configure Windows domain logon options**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Username/Password Credentials**. The **Username/Password Credentials** page appears.

2. Click one of the Windows domain logon options:

- **Allow the user to choose whether to use Windows credentials for remote network logon:** When users are prompted to provide their username/password credentials for the remote network, they will have the option of selecting the **Use Windows logon credentials** check box in the **Access Server** dialog box. If users select this check box, Aventail Connect will automatically use their Windows logon credentials to authenticate to that remote network for all subsequent connection attempts.
- **Always attempt remote network logon with Windows credentials:** Aventail Connect will always attempt to authenticate to the remote network with the user's Windows logon credentials. If the authentication fails, Aventail Connect prompts the user to provide his or her credentials.
- **Never use Windows logon credentials; remove the "Use Windows logon credentials" check box:** This option disables Windows domain logon support, and removes the **Use Windows logon credentials** check box from the **Access Server** dialog box.

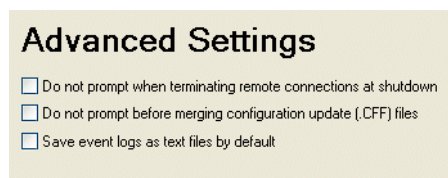
Configuring Advanced Settings for Aventail Connect Software

You can enable or disable prompts that are displayed before connections are terminated and before configuration update files are merged.

You can also configure event logs to always be saved in text format. By default, Aventail Connect log files are saved as binary files; to view these binary files, you must open them in the Aventail Connect Event Viewer. Text files can be displayed in any text editor.

► To configure advanced settings for Aventail Connect software

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Connect Software Settings**, and then click **Advanced**. The **Advanced Settings** page appears.



2. To suppress the prompts that are normally displayed before Aventail Connect terminates remote network connections, select the **Do not prompt when terminating remote connections at shutdown** check box.
3. To suppress the prompts that are normally displayed before Aventail Connect merges configuration update files, select the **Do not prompt before merging configuration update (.CFF) files** check box.
4. To automatically save all event logs as text files, select the **Save event logs as text files by default** check box.

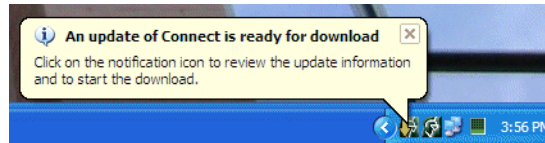
Configuring Software Updating Options

Aventail Connect supports multiple software updating options that can simplify deployment to multiple users and can ensure that users are running the most recent Aventail Connect software or have installed your latest setup package. You can configure



Aventail Connect to automatically check a specified URL for Aventail Connect software updates or new setup packages at specified intervals, or you can allow users to manually check for updates at any time. You can also disable the software updating feature.

If you configure Aventail Connect to automatically check for newer Aventail Connect software or custom setup packages, Aventail Connect will display in the taskbar notification area an updating icon and an update notification message whenever an update is ready for download.



If you configure Aventail Connect to allow manual updates, the Aventail Connect software or setup packages will be updated only when users manually initiate updates via the **Connect Software Update** command on the Aventail Connect system menu.

► To configure Aventail Connect software updating options

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click **Software Updates**. The **Software Updates** page appears.

2. Under **Software updating options**, click one of the software updating options:
 - **Disable software updating:** This option disables the Aventail Connect software updating feature and removes the **Connect Software Update** command from the Aventail Connect system menu.
 - **Allow manual software updates (User initiates software updates):** Users can manually check for Aventail Connect software updates at any time by clicking **Connect Software Update** on the Aventail Connect system menu. This is the default setting.
 - **Check for updates every time Aventail Connect starts:** Aventail Connect checks the specified URL for Aventail Connect software updates or new setup packages at each startup. If a software update or new package is available,

users can download and install the update immediately, or they can temporarily defer the update download by clicking a **Remind Me Later** button.

- **Check for updates at the specified interval:** Aventail Connect checks the specified URL for Aventail Connect software updates or new setup packages at the specified interval. If a software update or new package is available, users can download and install the update immediately, or they can temporarily defer the update download by clicking a **Remind Me Later** button.

Check for software updates every <x> days: Type or select the number of days to wait before checking for new Aventail Connect software or package updates.

3. If you enabled software updating in step 2, in the **URL to download software updates from** box, type the URL from which to download Aventail Connect software updates.

A default URL is provided; Aventail will make any updates for the Aventail Connect software available via this URL. Users can download Aventail Connect software updates, but not custom setup packages, via this URL. This updates only the Aventail Connect software; all other Aventail Connect settings and configuration files remain intact.

If you want to distribute custom setup package updates to your users, you must specify a URL that you will upload new or updated packages to. Deploying a new or updated setup package resets the user's Aventail Connect settings to those specified in the new setup package.

► To configure software update information

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click **Software Updates**.
2. On the **Software Updates** page, under **Software update information**, in the **Software update priority** list, select the update priority level—**Normal** or **Critical**—for the package. This priority level will appear in the **Connect Software Update** dialog box displayed to users when an update is available, and can help to convey to users the urgency of the update.
3. In the **Maximum reminder interval** list, select the maximum time interval that users can select each time they click **Remind Me Later** on the **Connect Software Update** dialog box. This controls how often users will be reminded to download and install an update.
4. In the **Software update message** box, type a message that will appear in the software-updating dialog box displayed to users when an update is available.

Configuring Package Signing Options

Aventail strongly recommends digitally signing all custom setup packages; a digital signature, which is displayed to users in certificate form before they install the package, tells users that a package was created and distributed by a credible source.

The Aventail Connect client software, which is included in every Aventail Connect setup package, is already digitally signed by Aventail Corporation. However, if you want to digitally sign an Aventail Connect setup package, you must do so after creating or modifying the package.



NOTE Modifying a digitally signed package removes the digital signature. If you modify a digitally signed package, you must re-sign the package after saving it.

Package signing is performed using Microsoft Authenticode technology. For more information, visit the Microsoft MSDN Web site at <http://msdn.microsoft.com>.

► **To specify package signing requirements**

1. In the **Aventail Connect Customizer Tool** window, on the main navigation menu, click to expand **Software Updates**, and then click **Digital Signature**. The **Digital Signature** page appears.

Digital Signature

Digital signatures

Aventail recommends that you digitally sign all customized setup packages. A digital signature tells end users that the software they are installing came from a credible source.

Package signing is performed using Microsoft® Authenticode® technology. To learn more about Authenticode technology, visit the Microsoft MSDN Web site at <http://msdn.microsoft.com/>.

Each time you modify a digitally signed package, it loses its digital signature. If you are using digital signatures, you must resign packages after modifying them.

Digital signature handling for software updates

Software updating always validates the digital signatures for the Aventail Connect software that is contained within every package.

The following options offer varying levels of protection for the customized package and for any additional files that are packaged with the Aventail Connect software.

None: No package signature is required. (Least secure)

Standard: Package signature is required. The user is presented with any digital signature problems; the user must then decide whether to install the software update.

Restricted: Package must be signed by the specified software vendor's digital certificate. Any signature problems will cause the software update to fail; the user is not prompted with any signature problems.

Issued to:

Issued by:

2. Under **Digital signature handling for software updates**, click one of the options:

- **None:** A digital signature for the package is not required. This is the least secure option, and is not recommended.
- **Standard:** A digital signature for the package is required. The user is presented with any digital signature problems (such as an expired certificate), and he or she must decide whether to install the package. This is the default setting.
- **Restricted:** A digital signature for the package is required and must be signed by the specified software vendor. The user is not presented with any digital signature problems (such as an expired certificate or an invalid **Issued To** or **Issued By** value); any digital signature problems will automatically cause the update to fail.

If you select the **Restricted** option, you must also type, in the **Issued to** box, the name of the company or person to whom the digital signature was issued and, in the **Issued by** box, the name of the company that issued the digital signature. The **Issued to** and **Issued by** values must match the corresponding fields in the certificate used to sign the package exactly.

Updating Configurations

You can save organizations to configuration update (.*cff*) files. Configuration update files are used primarily for updating configuration (.*cfg*) files; merging a configuration update file with a configuration file is the only method for programmatically updating existing configurations that you have already deployed to users. A configuration update file updates an organization in a configuration file by replacing the old organization settings with the new organization settings. All networks or network links that belong to the organization inherit the organization's settings.

You can create, modify, and delete configuration update files just as you would configuration files.

Creating Configuration Update Files

Configuration update (.*cff*) files allow you to update existing configuration (.*cfg*) files with new or updated organizations.

► **To create a configuration update file**

1. In the Aventail Connect Configuration Tool, click **New** on the **File** menu.
2. After you have configured your settings, click **Save** or **Save As** on the **File** menu, and then save the file as a configuration update (.*cff*) file.

Exporting Organizations

You can save the configuration for individual organizations, including all of their associated networks and settings. This can be useful when you want to reuse an organization's settings in more than one configuration file, or when you want to update an existing configuration file with a new or updated organization. When you export an organization, it is saved as a configuration update (.*cff*) file.

► **To export an organization**

1. In the network view of the **Configuration Tool** window, right-click any network or network link in the organization that you want to export, and then click **Export Organization**.
2. In the **Save As** dialog box, assign a descriptive file name to the organization, and then click **Save**.

Importing Organizations

You can import individual organizations, and all of their associated networks and settings, into a configuration file. This can be useful when you want to reuse an organization's settings in more than one configuration file, or when you want to update an existing configuration file with a new or updated organization.

► **To import an organization**

1. In the network view of the **Configuration Tool** window, right-click any network or network link in the organization that you want to update, and then click **Import Organization**.



- In the **Open** dialog box, select the organization (.cff file) that you want to import, and then click **Open**.

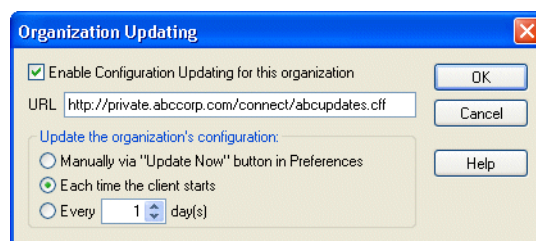
Enabling Configuration Updating

You can update existing local configuration files with the Aventail Connect client's configuration updating feature. Updating with configuration update files allows you to update certain parts of a user's configuration file, leaving the other parts of the configuration unchanged. Each organization includes attributes that control its updating behavior, including a URL and an updating frequency. When an organization is updated with a configuration update file, only that organization and the networks that belong to it are modified.

At launch time, the Aventail Connect client checks the configuration file to determine whether updating is required, and then downloads any required updates. Supported updating protocols are HTTP, HTTPS, and FTP. Users may need to authenticate during the updating process if the URL points to a resource that is behind an Aventail appliance. The connection to the designated URL is redirected by the Aventail Connect client according to the settings in the current configuration file. The Aventail Connect client can download updated configuration update information either every time Aventail Connect starts or on a regular, scheduled basis. These settings are managed in the **Organization Updating** dialog box.

► To enable organization updating

- If redirection through a proxy server is required to reach the Web server, configure the Aventail Connect client to use a configuration file that can access the Web server. If redirection is not required, skip this step.
- In the network view of the Configuration Tool, select any network or network link in the organization that you want to enable updating for.
- Click the **Organization** tab, and then click **Updating**. The **Organization Updating** dialog box appears.



- Select the **Enable configuration updating for this organization** check box.
- In the **URL** box, type the URL of the location where the configuration update files will be stored.
- Specify how often the Aventail Connect client will download the updating information:
 - Manually via **Update Now** button
 - Each time the client starts

- Every <x> days
7. Place new Aventail Connect configuration update (.cff) files on the Web server whenever you want to update the organization.

If you configure organization updating so that users must click **Update Now** (on the **General** tab of the **Aventail Connect Options** dialog box), note that you may need to remind users when it is time to update their configurations. If you anticipate frequent configuration updates, Aventail recommends performing automatic updates each time the client starts or every <x> days.

Chapter 4

Troubleshooting

This chapter describes how to troubleshoot basic Aventail Connect problems and describes how to use the Event Viewer and Remote Ping diagnostic tools.

Frequently Asked Questions

If you are having trouble configuring, deploying, or running the Aventail Connect client, first check the following FAQs to see if your problem is addressed.

Q: What are the limitations to single sign-on with Windows credentials?

- This feature is supported only on the Windows 2000 Professional and Windows XP Professional operating systems. This feature is not supported on the Windows 98 and Windows XP Home Edition operation systems.
- Aventail Connect supports this feature only when Windows domain logon support is enabled, and only on the initial NT logon. If you log off, or if you quit Aventail Connect, the cached credentials are flushed.
- Users can authenticate to Aventail Connect with their Windows logon credentials only when using Username/Password authentication and only if their Windows logon credentials are the same as their Aventail Connect credentials.

Q: What are the Windows domain logon support limitations?

- Aventail Connect supports Windows domain logon functionality on the Windows 2000 Professional and Windows XP Professional operating systems. Windows domain logon functionality is not supported on the Windows XP Home Edition, Windows Me, and Windows 98 operating systems.
- To enable Windows domain logon support, no other third-party Graphical Identification and Authentication (GINA) APIs can be installed on the user's computer.
- When Windows domain logon support is enabled:
 - Aventail Connect does not support Internet Explorer client certificates unless the certificate is already cached.
 - Users cannot switch to a different configuration file when running in multiple remote network access mode.



- Aventail Connect cannot read Internet Explorer proxy settings.
- The **Options** button is disabled in the **Remote Network Access** dialog box displayed at startup.

Q: The Aventail Connect client is physically on a network that is specified in the configuration file, but it is not detecting the local network. Why is Aventail Connect failing to automatically detect the correct local network?

For the Aventail Connect client to successfully detect a network specified in the configuration file, you must define the destination network with the proper domain name and IP address. The computer's current IP configuration must match both its IP address and domain suffix to those of the network for a match to occur.

Q: Why is Remote Ping not working?

Remote Ping functions only if the remote access server has the Remote Ping functionality enabled. For more information, contact the server administrator.

Q: I am using the Aventail Connect client for the first time. Why am I unable to browse the network or map a drive on the network?

During your first use of the Aventail Connect client, you may need to allow the Aventail Connect client to first establish a correlation between corporate domains and resources on each domain before you can browse the domains from Windows Explorer, or before you can successfully map network drives. To establish this correlation:

1. Establish a connection to your Internet service provider (ISP).
2. Start the Aventail Connect client.
3. Double-click the Network Neighborhood icon on your desktop, and then manually browse the NT domains listed in Network Neighborhood.

By browsing these NT domains, the Aventail Connect client can "discover" the information about the domains you will be accessing. After you have completed these steps, you can browse the domains in Windows Explorer and map drives successfully.

Q: Can I reset my corporate NT password through Aventail?

Yes, if the domain is defined in your Aventail Connect configuration file. Just press CTRL+ALT+DEL, and then follow the prompts.

Troubleshooting Aventail Connect Problems

Aventail Connect-related problems tend to fall into three general categories: Installation, Network Connectivity, and Configuration.

Aventail Connect Installation Problems

When installation instructions are followed properly, Aventail Connect installation problems rarely occur. When they do occur, they are often the result of:

- **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 reinstall Aventail Connect, ensuring that the 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 a corrupted Aventail Connect installation CD as the cause of a failed installation, contact Aventail for assistance in determining whether the files on the CD might have been corrupted and whether Aventail or your vendor must supply a replacement CD.

If you suspect a corrupted or incomplete FTP transfer of Aventail Connect installation files obtained over the Internet, retry the transfer, ensuring that the FTP client is in binary mode and confirming that the transfer completes normally. Contact Aventail 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.

- **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 then contact Aventail.

Network Connectivity Problems

Before Aventail Connect can successfully redirect connections, ensure that the TCP/IP connection is functioning properly.

- Basic TCP/IP network connectivity must exist between the client workstation on which Aventail Connect is installed and the Aventail appliance to which it is configured to redirect connections.

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

- Basic TCP/IP network connectivity must exist between the appliance and the network host(s) to which the server is expected to proxy connections.

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



Aventail Connect Configuration Problems

This section explains how to troubleshoot simple Aventail Connect configuration problems. Troubleshooting complex Aventail Connect configuration problems is beyond the scope of this section.

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

i **NOTE** Before troubleshooting Aventail Connect configuration problems, you must know the IP address and port number of the Aventail appliance through which the Aventail Connect client proxies secure traffic. Neither Aventail Connect nor Aventail Support can discover the IP address or port number of the server(s).

► To troubleshoot configuration problems

1. Confirm that the Aventail Connect configuration file that is currently selected on the **General** tab of the **Aventail Connect Options** dialog box is the one intended for testing. Also confirm that the local network and proxy server settings are correct.
2. Open the Aventail Connect Configuration Tool, and then confirm that the Aventail appliance has been correctly identified by IP address.

Click the **Access Server** tab, and compare the address in the **Hostname or IP Address** box with that of the server.

Ensure that the correct version (HTTP, SOCKS v4, or SOCKS v5) is selected.

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

In the **Authentication Modules** dialog box, confirm that the check boxes for all of the authentication modules are selected, indicating that the modules are enabled. Enabling all of the modules configures the Aventail Connect client to attempt any form of authentication demanded by the Aventail appliance. Note the form of authentication demanded by the server and, if necessary, obtain the proper authentication credentials, such as a username and password, from the server administrator.

4. Confirm that the network hosts to which the Aventail appliance is expected to proxy connections are defined within a redirected destination.

On the **Destinations** tab of the Configuration Tool, select the destination that includes the network host to which the Aventail appliance is expected to proxy connections, and then click **Edit**. Confirm that the definition of the destination includes the network host.

5. After making any necessary changes to the Aventail Connect configuration, restart the Aventail Connect client and then test the new configuration.

Event Viewer

The Aventail Connect logging utility, which traces Aventail Connect activity, runs in the background while Aventail Connect is running. The logging utility generates event logs, such as connection alerts and diagnostic messages, as they occur. The Aventail Connect



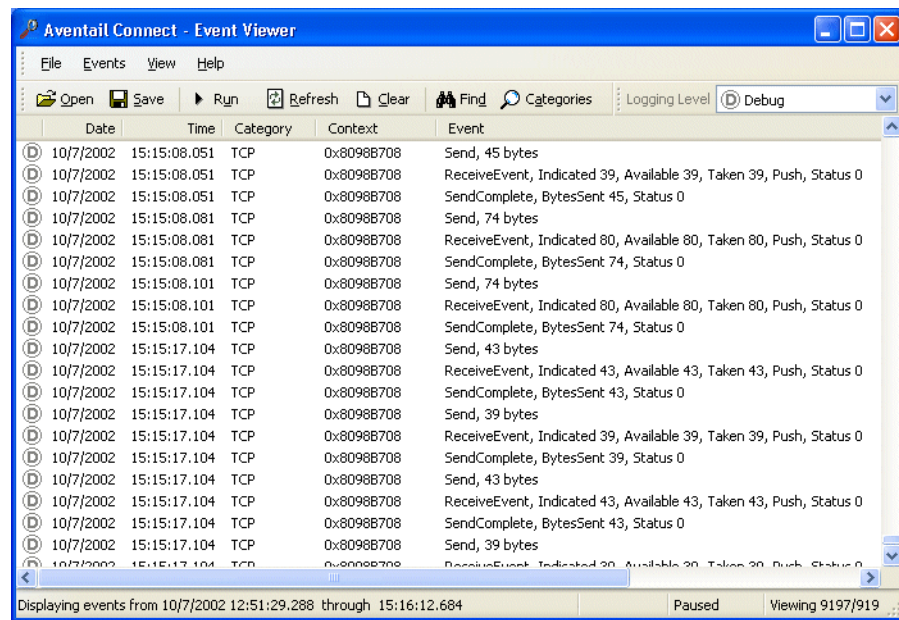
Event Viewer displays those event logs. Users can save the message list to a log file that you can use in troubleshooting technical problems. Log files are also useful when running the Aventail Connect client for the first time, to ensure that network traffic is being routed properly.

Opening the Event Viewer

When the Aventail Connect client is running, the event logger runs in the background. To view the log messages, you must open the **Event Viewer** window.

► **To open the Event Viewer**

- In the taskbar notification area, right-click the Aventail Connect icon, and then click **Event Viewer**. The **Event Viewer** window appears.



Setting the Logging Level

The Event Viewer supports five levels of log messages.

Select	To Log
Fatal	Fatal errors only.
Errors	Errors and fatal errors.
Warnings	Errors and warnings.
Information	Errors, warnings, and information.
Debug	Debugging messages. (For debugging purposes only.)

The Event Viewer also supports multiple logging categories, which specify the types of connections to monitor.

► **To set the logging level**

1. In the **Logging Level** list, click the appropriate log level.
2. On the Event Viewer **Events** menu, click **Categories**. The **Logging Categories** dialog box appears.



3. Select the check boxes of the connection types that you want to log, and clear the check boxes of the connection types you do not want to log. To log all types of connections, click **Select All**. Click **OK**.

The Event Viewer records and displays information at the specified logging level as the Aventail Connect client generates it.

Filtering Log Messages

You can filter the contents of the log window by selecting the types of messages that you want to view. You can exclude or show only certain types of messages.

Message Element	Filtering Options
Category	Show only, exclude
Context	Show only, exclude
Event level	Exclude
Event type	Exclude

► **To filter log messages**

1. In the Event Viewer message list, right-click in the column of an existing message that includes the type of category, context, event level, or event type that you want to include or exclude. For example, if you want to exclude all authentication messages, right-click in the **Category** column of any message that contains "Authentication" in its **Category** column.
2. Click **Show Only...** (for category or context) or **Exclude...** (for event level, category, context, or event).
- To turn off filtering and display all log messages, right-click anywhere in the message list, and then click **Show All Events**.

Saving Log Messages

You can save log messages in text (.txt) or binary (.lgf) format. Binary (.lgf) log files must be viewed in the Aventail Connect Event Viewer. Text-based (.txt) log files can be viewed in a text editor, such as Notepad.

► **To save log messages**

1. Select (highlight) the log messages that you want to save. If you want to save all displayed messages, do not select any messages; if no messages are selected, the contents of the Event Viewer are saved in their entirety.
2. On the Event Viewer **File** menu, click **Save**.
3. In the **Save Connect Log File** dialog box, type or select a file name, select the file format (.txt or .lgf), and then click **Save**.

Copying Log Messages into Other Applications

You can copy Event Viewer log messages to the Windows Clipboard and then paste them into another application, such as an e-mail application or a text editor.

► **To copy selected log messages**

- In the **Event Viewer** window, select (highlight) the log messages that you want to copy, and then click **Copy** on the Event Viewer **Edit** menu.

Printing Log Messages

You can print selected log messages, or you can print the **Event Viewer** window contents in their entirety.

► **To print log messages**

1. Select (highlight) the log messages that you want to print. If you want to print all displayed messages, do not select any messages; if no messages are selected, the contents of the Event Viewer are printed in their entirety.
2. On the Event Viewer **File** menu, click **Print**.

Finding a Specific Log Message

You can find specific log messages or specific types of messages by performing a key word search. Note that only the **Event** column is searched.

► To find a specific log message

1. On the Event Viewer **Events** menu, click **Find**.
2. In the **Find** dialog box, type one or more key words, and then click **Find Next**.

Clearing the Event Viewer Window

Because old log messages are automatically deleted as new ones are generated, you may never need to manually clear the **Event Viewer** window.

► To clear the Event Viewer window

- On the Event Viewer **Events** menu, click **Clear**.

Closing the Event Viewer Window

Closing the **Event Viewer** window does not prevent the event logging utility from generating log messages. Even when the **Event Viewer** window is closed, the event logging utility is always running in the background whenever Aventail Connect is running.

► To close the Event Viewer window

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

Running the Diagnostic Utilities

The Aventail Connect Remote Ping tool is a diagnostic utility that checks connectivity between the Aventail appliance and a host in the remote network. After a response from the host returns, the Aventail appliance relays the data back to the Aventail Connect client and displays it in the **Remote Ping** dialog box. Remote Ping allows you to run 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.

Note that remote network access must be enabled to run Remote Ping, unless you are running in multiple network access mode.

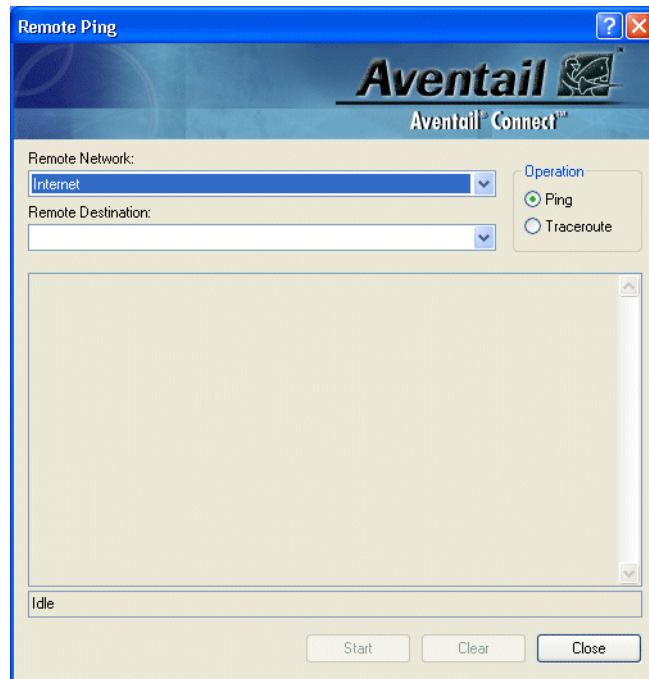
The remote server that you are testing must have ping support enabled for Remote Ping to work correctly.

► To run Remote Ping

1. Right-click the Aventail Connect icon in the taskbar notification area, and then click **Options**.



2. Click the **Network** tab of the **Aventail Connect Options** dialog box.
3. Click **Remote Ping**. The Remote Ping dialog box appears.



4. Select the remote network (the network you are currently logged on to), and then type or select the network destination (the host that you want to ping).
5. Under **Operation**, click **Ping** or **Traceroute**, depending on which utility you want to run, and then click **Start**.

The **Start** button becomes a **Stop** button. When the connection to the host is made, the information returned from the server is displayed in the results window.

► **To stop the ping or traceroute utility**

- Click **Stop**.

This stops the operation and the **Stop** button becomes a **Start** button. The results of the operation remain visible in the **Remote Ping** dialog box.

Notes

- Most ping and traceroute utilities are based on Internet Control Message Protocol (ICMP), which is incompatible with SOCKS v5. In order to proxy a ping or traceroute request, you must use the Aventail Connect Remote Ping tool.
- Some hosts are configured to not respond to ping requests. If Remote Ping tries to contact such a host, Remote Ping will time out.



Appendix A

Aventail Connect Dialog Boxes

This appendix introduces you to the dialog boxes and windows that you are likely to see when configuring and deploying the Aventail Connect client. The appendix describes the dialog box components and provides a brief introduction to the tasks that you can perform in each dialog box. More detailed procedural information is provided in other chapters of this document.

Configuration Tool

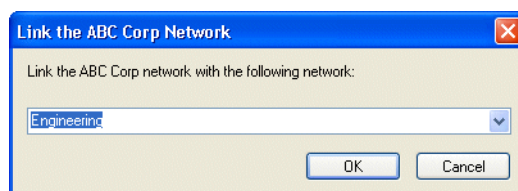
The Aventail Connect Configuration Tool allows you to define logical groups of networks and the network links that connect them. These definitions are saved as configuration (.*cfg*) files or configuration update (.*cff*) files. In the Configuration Tool, you can define a network's destinations, domains, hosts, and remote network access connection modes. You can also define the servers that provide access to those networks, including the servers' authentication and fallback settings.

This section describes the components of the Configuration Tool tabs.

You can also open the **Link the <x> Network** dialog box from the network view of the Configuration Tool. For more information, see "Link the <x> Network Dialog Box" on page 81.

Link the <x> Network Dialog Box

In the **Link the <x> Network** dialog box, you can link the selected network with another existing network in the configuration.



Configuration Tab

You can define basic configuration file settings on the **Configuration** tab of the Configuration Tool.

Field	Description
File Name	Displays the file name of the configuration file or configuration update file.
Description	Allows you to type a comment about the configuration file.
Create a configuration file in clear text format	Determines whether the configuration file can be edited in a text editor. When enabled, the configuration file can be edited with a text editor. When disabled, you can view and edit the configuration file only in the Configuration Tool.
Create a configuration file that supports multiple remote network access (Connect 4.x network access mode)	Specifies whether a configuration file supports multiple remote access mode. When enabled, the configuration file allows simultaneous connections to multiple networks. (Standard and restricted remote network access modes are not supported when this option is enabled.) For more information, see "Remote Network Access Modes" on page 18.

Organization Tab

You can define an organization's settings on the **Organization** tab of the Configuration Tool.

An organization is a logical group of networks. An organization can contain multiple networks, and you can link the networks to reflect your network topology. Each network, organization, and network link has its own attributes; however, networks inherit certain settings applied to the organizations they belong to.

You can open the **Organization Updating** dialog box from the Organization tab. For more information, see "Organization Updating Dialog Box" on page 83.

Field	Description
Organization	Specifies the organization's name.
Description	Assigns a descriptive comment about the organization.
Version	Assign a version number to the organization.
Updating	Specifies organization updating settings.
Import	Imports an existing organization into the selected organization.
Export	Exports the selected organization as a configuration update (.cff) file.

Field	Description
Require a password to view or change settings for this organization	Assigns password protection to an organization.
Enter password	Specifies the password that protects the organization.
Retype password	Specifies the password that protects the organization.

Organization Updating Dialog Box

In the **Organization Updating** dialog box, you can define configuration updating settings for an organization. Organization updating allows you to update individual organizations within a configuration file that has already been deployed to users.

Field	Description
Enable configuration updating for this organization	Enables configuration updating for the organization.
URL	Specifies the URL where the configuration update files are stored. (Supported protocols are HTTP, HTTPS, and FTP.)
Update the organization's configuration	<ul style="list-style-type: none"> • Manually via "Update Now" button in Preferences: Manually updates users' organizations when they click Update Now on the General tab of the Aventail Connect Options dialog box. • Update the organization's configuration each time the client starts: Automatically updates the organization's configuration each time users start the Aventail Connect client. • Update the organization's configuration every <x> day(s): Specifies the interval for updating the organization's configuration.

Network Tab

You can define a network's settings on the **Network** tab of the Configuration Tool.

•

Field	Description
Organization	Specifies which organization the network belongs to (for example, ABC Corporation).
Network Name	Specifies the name of the network (for example, Engineering).
Logo Filename	Specifies an image that will appear in authentication dialog boxes for this network. You can use the browse button to search for the bitmap (.bmp) file.

Field	Description
Remote Network Access Mode	<p>Specifies the remote network access mode for that network. (This option is disabled if the multiple remote network access connection mode is enabled on the Configuration tab.)</p> <ul style="list-style-type: none"> • Standard-Single network with local access: Connections to remote resources are redirected to the remote network; all other connections pass through to the local network. • Restricted-Redirect all connections (no local access): Redirects all network traffic to the remote network. No local network access is allowed. • Restricted-Refuse non-directed connections (no local access): Connections to remote resources are redirected to the remote network; all other connections are refused.
Terminate all local connections before enabling remote network access	Closes all non-secure connections before opening a connection to the remote network. When enabled, this ensures that no other connections are open on the user's computer before connecting to the remote network. (A warning message is displayed first, allowing the user to opt out.)
Terminate all redirected connections when disabling remote network access	Closes all secure connections when terminating connections to the remote network. When enabled, this ensures that, when the user disconnects from the remote network, all other open connections to that network are also terminated. (A warning message is displayed first, allowing the user to opt out.)
Enable Internet proxy mode	Enables Internet proxy mode. When enabled, all unknown traffic (connections that do not match destinations in the configuration file) is directed to the Internet. When disabled, the Aventail Connect client directs unknown connections to the local network.
Personal Firewalls	Click to configure personal firewall integration.
Advanced	Displays the Network Advanced Settings dialog box, which allows you to specify applications that must be running before remote network access is enabled.

Network Advanced Settings Dialog Box

In the **Network Advanced Settings** dialog box, you can specify applications (for example, anti-virus software) that must be running before remote network access is enabled.

Field	Description
Add	Adds a required application.
Edit	Edits a required application.
Delete	Deletes a required application.

Personal Firewalls Dialog Box

Use this dialog box to configure personal firewall integration.

Field	Description
Select firewalls...	Select any combination of personal firewalls from the list by selecting or clearing the check boxes as needed. If you select one or both personal firewalls (Sygate and Zone Labs), Connect will require that one of the selected personal firewalls be running before enabling the remote network
Specify custom message...	Type a custom message that will be displayed to users if Aventail Connect detects that a required firewall is not running. This setting is optional.

Add Running Application Requirement Dialog Box

In the **Running Application** dialog box, you can define applications that must be running before remote network access is enabled.

Field	Description
Displayed Name	Specifies the commonly known name of the application. (Allows users to easily recognize the application.)
Executable	Specifies the executable (.exe) file name of the application.
Require the application executable to have a valid Authenticode signature	Select this check box to configure Aventail Connect to validate a required application's Authenticode signature before Aventail Connect will start. This provides an added level of security as it prevents another application from impersonating the required application.

Domains Tab

You can define a network's static domains and hosts (for Microsoft Networking Support) on the **Domains** tab of the Configuration Tool.

Field	Description
Add Domain	Adds a static domain.
Add Host	Adds a static host to the selected domain.
Edit	Edits the selected domain or host.
Delete	Deletes the selected domain or host.

Add/Edit Static Domain Dialog Box

In the **Add Static Domain** and **Edit Static Domain** dialog boxes, you can define settings for a network's domains.

Field	Description
Domain Name	Specifies the name of the domain.
Comment	Assigns a descriptive comment about the domain.
This is an Active Directory domain	Specifies whether the domain is an Active Directory domain.
Make domain browsable	Enables Microsoft Networking Support browsing mode.
Primary domain controller's server name	Specifies the domain's primary domain controller (PDC) name.
Primary domain controller's DNS name or IP address	Specifies the domain's PDC DNS name or IP address.

Add Static Host Dialog Box

In the **Add Static Host** dialog box, you can define settings for a network's host.

Field	Description
Server Name	Specifies the host's server name.
DNS Name or IP Address	Specifies the host's DNS name or IP address.
Comments	Assigns an optional descriptive comment about the host.

Destinations Tab

You can include and exclude a network's specific destinations on the **Destinations** tab of the Configuration Tool.

You can also open the **Add/Edit Destinations** dialog box from the **Destinations** tab. For more information, see "Add Static Host Dialog Box" on page 86.

Field	Description
Edit	Displays the Edit Destination dialog box, where you can edit the selected destination.
Add	Displays the Add Destination dialog box, where you can include or exclude a destination in the network.
Delete	Deletes the selected destination. (Note that no confirmation prompt is displayed.)

Add/Edit Destination Dialog Box

In the **Add/Edit Destination** dialog box, you can add a destination and define its settings. You can also exclude destinations in this dialog box with the **Exclude Destination** setting in the **Disposition** box.

The fields in the **Add/Edit Destination** dialog box vary depending on the type of destination you select in the **Type** box. All variations of fields are described in the table below.

Field	Description
Type	Specifies type of destination.
Disposition	<ul style="list-style-type: none"> • Include: Traffic can be redirected to this destination. • Exclude: Traffic cannot be redirected to this destination.
Host	(Host Name destination type only) Specifies the name of the host.
Domain	(Domain Name destination type only) Specifies the name of the domain.
Address	(IP Address and IP Address/Subnet Mask destination types only) Specifies the host's IP address.
From/To	(IP Address Range destination type only) Specifies the beginning and ending IP addresses of the range.
Subnet	(IP Address/Subnet Mask destination type only) Specifies the host's subnet mask.
Protocol	Specifies the type of traffic to be redirected (TCP, UDP, or both).
Comment	(Optional) Assigns a descriptive comment about the destination.
Single Port	Specifies a single port.
Port Range	Specifies a range of ports.

Field	Description
Start Port	Specifies the beginning of the port range.
End Port	Specifies the end of the port range.

NOTE You can specify ports and protocol restraints with IP addresses only.

Access Server Tabs

The **Access Server** tabs of the Configuration Tool allow you to specify settings for a network or for the Internet.

Field	Description
Network Access	<p>Defines network access requirements or constraints.</p> <ul style="list-style-type: none"> • Requires proxy server: Specifies that a proxy server is required for access to this network or to the Internet. • Does not require proxy server: Specifies that a proxy server is not required for access to this network or to the Internet. • No network access available: Specifies that no network access is available for this network.
Proxy Server	<p>Specifies proxy server settings.</p> <ul style="list-style-type: none"> • Hostname or IP Address: Specifies the host name or IP address of the proxy server. • Port: Specifies the proxy server's port number. • Version: Specifies the version of proxy server (HTTP, SOCKS v4, or SOCKS v5). • Perform Internet access proxy detection: Enables and disables Internet access proxy detection. (Available only on the Internet Access Server tab.)
Authentication	<p>Opens the Authentication dialog box, where you can define authentication settings for the network access server or the Internet access server.</p>
Advanced	<p>Specifies a fallback server.</p>

Authentication Dialog Box

In the **Authentication** dialog box, you can define which types of authentication the Aventail Connect client can perform.

Field	Description
Authentication modules	Specifies which authentication modules are enabled.

Field	Description
Configure	Configures settings for authentication realms and the SSL authentication module.
About	Displays information about the selected authentication module.
Time out cached credentials	<ul style="list-style-type: none"> • Never: Sets cached authentication credentials to never time out. • Time out cached credentials <x> minutes from first time entered: Sets cached credentials to time out <x> minutes after the first time the user enters them. • Time out cached credentials <x> minutes from last time used: Sets cached credentials to time out <x> minutes after the last time the user enters them.

Authentication Realm Options Dialog Box

Use this dialog box to specify a default realm and configure a custom realm-prompt message.

Field	Description
Always default to this realm	<p>Specifies a default realm:</p> <ul style="list-style-type: none"> • No default authentication realm: Configures no default realm. No default realm is displayed in the realm prompt, so the user must select a realm from the list or type the name of a hidden realm. • The access server's default authentication realm: Selects the default realm that is defined on the Aventail appliance. This realm is displayed to users as the default realm; however, users can select a different realm or type the name of a hidden realm. This option can be useful if your users belong to multiple realms but you expect that most users will be logging in to one particular realm most of the time. • Any specific realm name that you have added to the list of available default realms. If you select one of these realms, the realm that you specify in this field will be displayed to users as the default realm at login. However, users can select a different realm or type the name of a hidden realm. This option can be useful if you are creating a setup package for a group of users who do not belong to the appliance's default realm.

Field	Description
Displayed text prompting user to specify a realm	Type a message that will be displayed to users when they are prompted to specify a realm. For example, you might type "Select or enter your billing group" or "Select or enter your corporate division." If you do not type a message, the default message ("Select or enter your login group") will be displayed to users. This setting is optional.

Authentication Realms Dialog Box

Use this dialog box to view available default authentication realms.

Field	Description
Add	Click to add a realm name to the list of available default realms.
Delete	Click to delete any selected realm names.

Add Authentication Realm Name Dialog Box

Use this dialog box to add a realm name to the list of available default authentication realms.

Field	Description
Authentication realm name	Type the name of the realm that you want to add to the list of available default realms. Type the realm name exactly as it is configured on the Aventail appliance

SSL Options Dialog Box

In the **SSL Options** dialog box, you can define settings for the SSL authentication module. For more detailed instructions about configuring SSL options, see "Configuring SSL Options" on page 28.

Field	Description
Upon Successful Connection	<ul style="list-style-type: none"> • View when the server certificate is new: Upon successful connection, displays the server certificate if it has not been displayed before. • Do not show me the certificate: Never displays a valid server certificate.

Field	Description
If a Server Certificate is Suspect	<ul style="list-style-type: none"> • Always show me suspect certificates: Each time the Aventail Connect client suspects that a certificate might not be valid, it displays the certificate. • Show me the same suspect certificate once: Once a suspect certificate has been accepted by the user, Aventail Connect does not display it again. • Show me the certificate, but reject the connection: Rejects the connection, but displays the suspect certificate.
Acceptable Ciphers	<ul style="list-style-type: none"> • Allow RC4: Offers the RC4 cipher to the server. • Allow DES: Offers the DES cipher to the server. • Allow NULL encryption: Does not encrypt using SSL; uses SSL only to authenticate.
Enable compression	Use SSL compression to improve performance when slower connections are detected.
Server Validation	<ul style="list-style-type: none"> • Use local trusted roots file: Uses a trusted roots file to validate trusted certificate chain roots. Configure opens the Trusted Roots dialog box, where you can specify the trusted roots (.rot) file. For more information, see "Trusted Roots Dialog Box" on page 91. • Maximum certificate chain length: Specifies the maximum allowable certificate chain length.
Client Certificate	<ul style="list-style-type: none"> • Assign a default local client certificate file: Uses a local client certificate. • Assign default PKCS #11 smart card support: Uses a client certificate stored on a PKCS #11 smart card. Configure opens the PKCS #11 Configuration dialog box, where you can configure PKCS #11 settings. • Do not assign default client certificate settings: Does not specify a default client certificate.

Trusted Roots Dialog Box

In the **Trusted Roots** dialog box, you can specify a trusted roots file to validate trusted certificate chain roots with.

PKCS #11 Configuration Dialog Box

You can specify PKCS #11 smart card settings in the **PKCS #11 Configuration** dialog box.

Field	Description
Find the PKCS #11 DLL in Windows system path	Searches for the specified PKCS #11 dynamic link library (DLL) in the Windows system path.
Find PKCS #11 in specified path	Searches for the specified PKCS #11 DLL in the specified path.
Prompt the user for the name and location of the PKCS #11 DLL	Prompts the user to specify the path of the PKCS #11 DLL.
PKCS #11 DLL name	File name or path of PKCS #11 DLL.

You can also open the **Access Server Advanced Settings** dialog box from the **Access Server** tabs of the Configuration Tool. For more information, see "Access Server Advanced Settings Dialog Box" on page 92.

Access Server Advanced Settings Dialog Box

In the **Access Server Advanced Settings** dialog box, you can specify an optional secondary server that the connection will fall back to if the primary server is unable to process the connection.

Field	Description
Use fallback server if primary server does not respond	<p>Falls back to secondary server if the primary server cannot accept the connection.</p> <ul style="list-style-type: none"> • Fall back to host alias: Uses DNS records for redundancy. • Fall back to secondary server after timeout: Falls back to secondary server immediately upon connection timeout. <ul style="list-style-type: none"> • Hostname or IP address: Specifies host name or IP address of secondary server. • Port: Specifies port number of secondary server.

Customizer Window

The Aventail Connect Customizer tool allows you to create and modify custom Aventail Connect setup packages. Distributing preconfigured setup packages eliminates the need for users to make setup decisions when installing Aventail Connect. The Customizer tool allows you to include or exclude specific end-user interface components, specify installation and setup options, specify default settings, and include configuration files and other types of files (such as client certificate files, trusted roots files, or logo bitmap files) in the package.



The installation package is a self-extracting executable (.exe) file. You can distribute the package to multiple users, providing easy access, download, and installation for users. You can easily reconfigure and redistribute the package if your network specifications change.

Each section includes pages that allow you to customize various settings. All of the Customizer settings are optional; you can customize settings according to your network requirements.

Software Installation Pages

Use these pages to specify the level of user input required during Aventail Connect installation, the Aventail Connect installation directory, automatic-startup options, and Microsoft Windows Installer options.

Installation Options Page

Use this page to specify the level of user input required during Aventail Connect installation, the Aventail Connect installation directory, and Aventail Connect startup behavior.

Installation prompting level options

Field	Description
Full	All wizard status dialog boxes, prompts, and error messages (if errors occur) are displayed during Aventail Connect installation. The user is prompted to restart the computer after installation. This is the default setting.
Reduced	Only wizard status dialog boxes and error messages (if errors occur) are displayed during Aventail Connect installation. The user is prompted to restart the computer after installation.
Basic	Only simple progress and error messages (if errors occur) are displayed. The user is prompted to restart the computer after Aventail Connect installation.
None	Performs a "silent" installation of the Aventail Connect client on the user's computer. No prompts or messages are displayed. <ul style="list-style-type: none"> Restart the computer without prompting the user: When this check box is selected, the user's computer automatically restarts after the Aventail Connect installation finishes. The user is not prompted to save any work; any unsaved changes may be lost. <p>Aventail recommends clearing this check box. When this check box is cleared, the user must manually restart the computer after Aventail Connect installation.</p>

Installation options

Field	Description
Install directory	Type the Aventail Connect client installation directory path.
Run Aventail Connect when Windows starts	Starts the Aventail Connect client when Windows starts. If you enable the Run Aventail Connect when Windows starts option, on the Windows 2000 Professional and Windows XP Professional operating systems, the Aventail Connect graphical identification and authentication (GINA) API and Windows domain logon support are installed on users' computers, and Aventail Connect automatically starts at Windows logon time. On Windows XP Home Edition, Windows Me, and Windows 98 operating systems, Aventail Connect automatically starts at Windows logon time; however, the Aventail Connect GINA and Windows domain logon support are not installed.

Windows Installer Options Page

Use this page to specify whether to install the Microsoft Windows Installer (MSI) software on the user's computer if required during Aventail Connect installation; you can also specify the location from which Aventail Connect retrieves the MSI software.

Field	Description
Do not install Aventail Connect if the correct version of Microsoft Windows Installer is not currently installed	If the MSI software is not installed on the user's computer, or if an outdated version of the MSI software is installed, Aventail Connect installation is canceled, and the MSI software is not installed.
Include Microsoft Windows Installer in the package	Includes the MSI software in the current Aventail Connect package, and installs the MSI software on the user's computer during Aventail Connect installation if required. Note that including the MSI software in the setup package will significantly increase the size of the package.
Download Microsoft Windows Installer from one of these URLs if needed	Automatically downloads the MSI software from the specified URL if required, and installs the MSI software on the user's computer during Aventail Connect installation. <ul style="list-style-type: none"> • MSI installation for Windows 98 and Windows Me: Type the URL of the MSI software download location for computers running Windows 98 and Windows Me. • MSI installation for Windows 2000 and Windows XP: Type the URL of the MSI software download location for computers running Windows 2000 and Windows XP.

Advanced Installation Options Page

Use this page to specify a command to execute after Aventail Connect installation is complete. You can use this feature to run a system program that is already installed on the user's computer or an executable file that is included in the setup package.

Field	Description
Post-installation command	Type a command that Aventail Connect will execute after Aventail Connect installation is complete.

Packaging Options Pages

Use these pages to identify a package and add files to a package.

Package Information Page

Use this page to assign a company name, author name, or other identifying information to a package. Any information that you specify here is displayed on the **Package Information** page when the package is opened in Customizer; this can be useful if more than one administrator manages setup packages.

Field	Description
Company name	Type the name of the company issuing the package. If you enable software updating, the text that you type in this box is displayed to users in the Connect Software Update dialog box when an update is available.
Author	Type the name of the person creating or modifying the package.
Last modified	Displays the date and time, in Greenwich Mean Time (GMT), when the package was last saved.
Description	Type a descriptive comment about the package.

Additional Package Files Page

Use this page to add files—such as configuration files, trusted roots files, or logo image files—to a package. You can also use this page to remove files from a package.

Field	Description
Additional files	Displays files that are currently included in the package.
Add	Adds a file to the package.
Remove	Removes any selected files from the package. (Click a file to select it.)

Connect Software Settings Pages

Use these pages to customize the Aventail Connect user interface; specify default configuration files, remote network settings, and local network detection settings; configure Windows domain single sign-on settings; and configure software updating and other advanced settings.

Aventail recommends familiarizing yourself with the Aventail Connect product before performing any of the customizations on these pages.

Connect Startup Options Page

Use this page to include or remove the **Startup Options** section on the **General** tab of the **Aventail Connect Options** dialog box, and to specify default startup options.

Field	Description
Remove the Startup Options from the General tab of the Aventail Connect Options dialog box	Removes all Startup Options from the General tab of the Aventail Connect Options dialog box.
Display the Aventail Connect splash screen at startup	Displays the Aventail Connect splash screen at startup.
Prompt for configuration file and local network at startup	Prompts users to specify a configuration file and a local network at startup.
Remove the "Enable support for multiple realms" check box from the Startup Options of the Aventail Connect Options dialog box	Select this check box to remove the control that enables and disables multiple realms support from the Advanced tab of the Aventail Connect Options dialog box. If all of your users belong to a single realm, Aventail recommends removing this control (by selecting this check box). However, if you have users who belong to multiple realms, including this control in the Aventail Connect Options dialog box can be useful. For example, if an employee belongs to multiple realms but typically logs in to only one realm, he or she can manually disable the realm prompt; this configures Aventail Connect to automatically log the user in to the default realm.

Configuration File Settings Page

Use this page to include or remove the **Network Configuration** section on the **General** tab of the **Aventail Connect Options** dialog box, specify a default configuration file, and specify configuration updating status options.

Field	Description
Remove the Network Configuration settings from the General tab of the Aventail Connect Options dialog box	Removes all Network Configuration options from the General tab of the Aventail Connect Options dialog box.
Network configuration file	Select the path of the default configuration file, or click the Browse button to locate it and add it to the package.
Show configuration updating status	When selected, a status bar is displayed on the General tab of the Aventail Connect Options dialog box during the configuration updating process. When this option is disabled, Aventail Connect does not display a process indicator during configuration updating.

Remote Network Access Settings Page

Use this page to specify default remote network settings, and to include or remove selected remote network access options.

Field	Description
Always default to the following remote network	Type or select the default remote network to connect to.
Remove the "Default to this remote network" check box	Prevents users from specifying a default remote network by removing the Default to this remote network check box from the Remote Network Access dialog box.
Always use the detected local network; remove the local network information	Sets the default local network to that detected by Aventail Connect, and removes the local network prompt from the Remote Network Access dialog box.
Remove the "Options" button	Removes the Options button from the Remote Network Access dialog box.

Network Settings Page

Use this page to configure local network settings, and to include or remove certain options on the **Network** tab of the **Aventail Connect Options** dialog box.

Field	Description
Remove the Local Network settings from the Network tab of the Aventail Connect Options dialog box	Removes all Local Network options from the Network tab of the Aventail Connect Options dialog box.
Automatically detect local network	Automatically detects the user's local network. The user is not prompted to specify a local network.
Remove the Remote Network settings from the Network tab of the Aventail Connect Options dialog box	Removes all Remote Network options from the Network tab of the Aventail Connect Options dialog box.

Username/Password Credentials Page

Use this page to configure Windows domain logon settings.

Field	Description
Allow the user to choose whether to use Windows credentials for network logon	When enabled, users can enable or disable Windows domain logon support on the General tab of the Aventail Connect Options dialog box.
Always attempt remote network logon with Windows credentials	Enables Windows domain logon support, and removes the Enable Windows domain logon support check box from the General tab of the Aventail Connect Options dialog box.
Never use Windows logon credentials; remove the "Use Windows logon credentials" check box	Disables Windows domain logon support, and removes the Enable Windows domain logon support check box from the General tab of the Aventail Connect Options dialog box.

Advanced Settings Page

Use this page to enable or disable prompts that display when terminating connections and merging configuration files, and to configure default event log format settings.

Field	Description
Do not prompt when terminating remote connections at shutdown	Suppresses the prompt that appears before remote connections are terminated when users quit Aventail Connect.

Field	Description
Do not prompt before merging configuration update (.CFF) files	Suppresses the prompt that appears before Aventail Connect merges configuration update files.
Save event logs as text files by default	Saves all event log files in text format instead of binary format.

Software Update Pages

Use these pages to configure software updating settings and specify digital-signature requirements.

Software Updates Page

You can configure Aventail Connect to automatically check a specified URL for newer Aventail Connect setup packages at specified intervals, or you can allow users to manually check for updates at any time via the **Connect Software Update** command on the Aventail Connect system menu. You can also disable the software updating feature.

Software Updating Options

Field	Description
Disable software updating	Disables the Aventail Connect software updating feature and removes the Connect Software Update command from the Aventail Connect system menu.
Allow manual software updates (User initiates software updates)	Users can manually check for and download Aventail Connect software updates or new setup packages at any time by clicking Connect Software Update on the Aventail Connect system menu.
Check for updates every time Aventail Connect starts	Aventail Connect checks the specified URL for an Aventail Connect software update or a new setup package at each startup. If a software update or new setup package is available, users can download and install the update immediately, or they can temporarily defer the update download by clicking a Remind Me Later button.
Check for updates at the specified interval	<p>Aventail Connect checks the specified URL for a newer version of the Aventail Connect software or package at the specified interval. If a newer package or newer version of the Aventail Connect software is available, users can download and install the update immediately, or they can temporarily defer the update download by clicking a Remind Me Later button.</p> <ul style="list-style-type: none"> • Check for software updates every <x> days: Type or select the number of days to wait before checking for new Aventail Connect software or package updates.

Field	Description
URL to download software updates from	Type the URL from which to download Aventail Connect software updates.

Software Update Information

Field	Description
Software update priority	Select the update priority level— Normal or Critical —for the package. This priority level appears in the Connect Software Update dialog box displayed to users, and can help to convey the urgency of the update.
Maximum reminder interval	Select the maximum time interval that users can select each time they click Remind Me Later on the Connect Software Update dialog box.
Software update message	Type a message that will appear in the software-updating dialog box displayed to users.

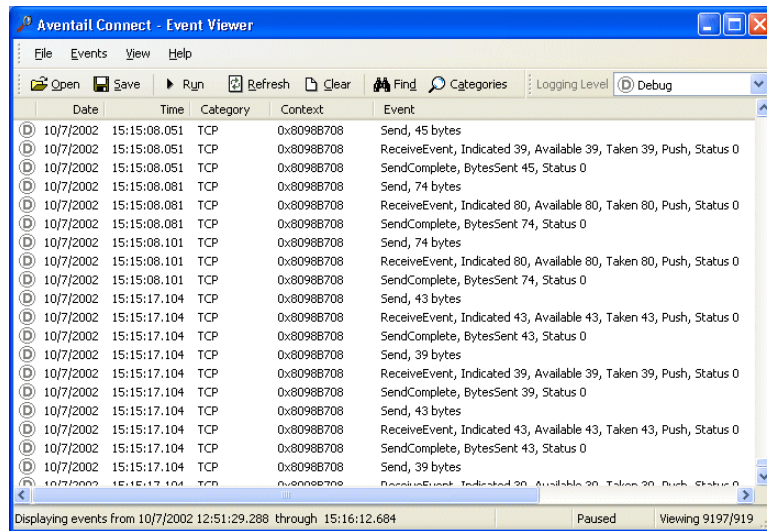
Digital Signature Page

Use this page to specify digital-signature requirements. Aventail strongly recommends signing all custom setup packages; a digital signature tells users that a package was created and distributed by a credible source.

Field	Description
None	A digital signature for the package is not required. This is the least secure option, and is not recommended.
Standard	A digital signature for the package is required. The user is presented with any digital signature problems (such as an expired certificate), and he or she must decide whether to install the package. This is the default setting.
Restricted	A digital signature for the package is required and must be signed by the specified software vendor. The user is not presented with any digital signature problems (such as an expired certificate or an invalid Issued to or Issued by value); any digital signature problems will automatically cause the update to fail. <ul style="list-style-type: none"> • Issued to: Type the name of the company or person to whom the digital signature was issued. • Issued by: Type the name of the company that issued the digital signature.

Event Viewer Window

The Event Viewer is a diagnostic utility for tracing Aventail Connect activity. The Event Viewer, which runs in the background whenever the Aventail Connect client is running, displays errors, warnings, and information as the Aventail Connect client generates them. You can save the message list to a log file that you can use in troubleshooting technical problems. Log files are also useful when running the Aventail Connect client for the first time, to ensure that network traffic is being routed properly.



Field	Description
Open	Opens a saved log file.
Save	Saves a log file in binary or text format.
Pause/Run	Pauses/restarts the logging process.
Refresh	Refreshes the Event Viewer window contents.
Clear	Clears the Event Viewer window contents.
Find	Searches for log messages with key words.
Categories	Displays the Logging Categories dialog box, where you can specify the types of events to be logged.
Logging Level	Specifies the level of logging to perform.
Date	Displays the date on which the log message was generated.
Time	Displays the time of day that the log message was generated.
Category	Displays the type of event.
Context	Displays the context of the connection being made.
Event	Describes the event.

Logging Categories Dialog Box

In the **Logging Categories** dialog box, you can specify the default logging level and the types of events to be logged.

Field	Description
Default Logging Level	Selects the default level of Aventail Connect activity to log.
Category	Displays the available logging categories. A check mark to the left of a category indicates that the category is enabled.
Logging Level	Specifies the level at which each enabled category is being logged.
OK	Saves changes and closes the Logging Categories dialog box.
Cancel	Closes the Logging Categories dialog box without saving changes.
Select All	Enables all logging categories.
Defaults	Applies the default logging-category settings.

Remote Ping Dialog Box

The Aventail Connect Remote Ping tool is a diagnostic utility that is used to test a remote network connection.

Field	Description
Remote Network	Selects the network you are currently logged on to.
Remote Destination	Selects the host on the remote network that you want to test.
Operation	Selects Ping or Traceroute .
Start/Stop	Runs or stops the ping or traceroute utility.
Clear	Clears the Remote Ping results window.
Close	Closes the Remote Ping window.



Appendix B

Aventail Connect Extensibility Toolkit

The Aventail Connect client supports a variety of run-time and support commands. The run-time command-line switches modify the normal run-time behavior of the Aventail Connect client. The support command-line switches allow you to perform certain troubleshooting and diagnostic tasks without using the standard Aventail Connect graphic user interface.

Entering Command-Line Switches

If you enter a support command on the command line, the requested operation is performed and then the DOS command-prompt window closes. While processing support commands, the Aventail Connect client ignores all run-time commands.

► To enter a command-line switch

1. On the Start menu, click **Run**. The **Run** dialog box appears.
2. In the **Open** box, type `cmd`.
3. At the DOS prompt, switch to the Aventail Connect directory by typing `cd` followed by the path. For example, if the Aventail Connect client is installed in the `C:\Program Files\Aventail\Connect` directory, type:

```
cd c:\program files\aventail\connect
```

and then press ENTER.

4. At the Aventail Connect directory, type `as32` followed by a space and the desired command-line switch.

```
as32 [command]
```

For example, if you want to prevent the Aventail Connect splash screen from appearing at startup, type:

```
as32 -nosplash
```



Run-Time Command-Line Switches

The Aventail Connect client supports the following run-time switches.

Command	Description
<code>-cfg=<configuration file></code>	Runs the Aventail Connect client with the specified configuration file. If the Aventail Connect client is already running, the specified configuration file is activated. Note that only one configuration file can be active at a time.
<code>-destination=<network location></code>	Runs the Aventail Connect client with the destination set to the specified network location. If the Aventail Connect client is already running, the specified destination is activated.
<code>-location=<network location></code>	Runs the Aventail Connect client with the specified network location. If the Aventail Connect client is already running, the specified network location is activated.
<code>-runmode=[gina automatic manual]</code>	<p>Sets the run mode for the Aventail Connect client.</p> <ul style="list-style-type: none"> <code>gina</code> configures Aventail Connect to be launched by the GINA and enables Windows domain logon support. <code>automatic</code> configures Aventail Connect to launch automatically when the user's desktop loads. <code>manual</code> configures Aventail Connect to run only when the user manually starts it.
<code>-displaysplash=<seconds></code>	For debugging purposes only. Displays the Aventail Connect client splash screen for a specified number of seconds. The default is 10 seconds.
<code>-merge=<fragment file></code>	Merges the configuration fragment into the current configuration file. If the Aventail Connect client is already running, the merged configuration file is activated.
<code>-nosplash</code>	Suppresses the splash screen from displaying when the Aventail Connect client starts.
<code>-norun</code>	The Aventail Connect client processes the run-time configuration switches and then exits. You can use this switch to change the default configuration file or default network location, or to merge configuration files without running the Aventail Connect client.

Command	Description
<code>-credentials</code>	Specifies user credentials on the command line, which provides authentication integration with other applications, most notably ISP dialers such as iPass.

One-Click Authentication Integration

With the `-credentials` command-line switch, you can specify a user's credentials on the Aventail Connect command line. This provides one-click authentication integration with other applications, most notably ISP dialers such as iPass. Any application that can pass credentials to Aventail Connect can take advantage of this feature.

In most cases, the `-credentials` command will be used in conjunction with existing command-line switches to launch the client, pass credentials, suppress the splash screen, and specify the network location and destination. This provides one-click integration with the iPass dialer, as long as the user credentials are the same for both the dialer client and the Aventail Connect client.

The basic syntax of the command is:

```
-credentials=auth_type:<user_credentials>@server:port[,options]
```

- `auth_type` is the authentication method being used by the Aventail Connect client.
- User credentials include the user's username, password (for UN/PW authentication), token serial number (if applicable), and PIN (if applicable).
- `server` refers to the network access server. The port value defaults to 443 if no port number is specified.

You can specify multiple credentials on the command line. `auth_type` and `server` are required fields; the credentials specified are used only for the associated server and authentication type. Credentials can be passed to the Aventail Connect client upon Aventail Connect startup or after startup by invoking `as32.exe` with the `-credentials` command-line switch.

Note that credentials cannot be passed to a running instance of the Aventail Connect client if remote network access is disabled.

If you click **Clear Credentials** (on the **Network** tab of the **Aventail Connect Options** dialog box), the entire Aventail Connect credential cache is flushed.

The specific command-line syntax for the supported authentication methods is described below.

Username/Password Authentication

```
-credentials=SslUnpw:<username,password>@server:port
```

- Username and password are cached.
- Username/password dialog box will not display.



```
-credentials=SslUnpw:<username>@server:port
```

- Username is cached.
- Username/Password dialog box will display prepopulated with username.

If <username> is '*' (default) then:

- If the specified entry already exists in the cache, the username from that cache entry is used.
- If the cache entry is new, the logged-in Windows username is used.

SecurID Authentication

```
-credentials=SslSecurId:<username>@server:port
```

- Username is cached.
- PIN cannot be cached because passcode is also required.
- CRAM username dialog box will display prepopulated with username.
- CRAM passcode/PIN dialog box will display.

If <username> is '*' (default) then:

- If the specified entry already exists in the cache, the username from that cache entry is used.
- If the cache entry is new, the logged-in Windows username is used.

SoftID Authentication

```
-credentials=SslSoftId:<username,tokenserialnumber,pin>@server:port
```

- Username, token serial number, and PIN are cached.
- SoftID dialog box should not display.

```
-credentials=SslSoftId:<username,tokenserialnumber>@server:port
```

- Username is cached.
- Specified token is used from SoftID.
- SoftID dialog box will display prepopulated with username.

```
-credentials=SslSoftId:<username>@server:port
```

- Username is cached.
- Default token is used from SoftID.
- SoftID dialog will display prepopulated with username.

If <username> is '*' (default) then:

- If the specified entry already exists in the cache, the username from that cache entry is used.
- If the cache entry is new, the logged in Windows username is used.
- There is a default username available within the selected SoftID token; however, specifying this via the command line is currently not supported.



- If <tokenserialnumber> is '*' (default), then the default SoftID token is used.

Manual SoftID

To override SoftID and use regular SecurID, prepopulate the cache using the SecurID authentication syntax.

Support Command-Line Switches

The Aventail Connect client supports the following support commands.

Command	Description
-help or -?	Invokes the Windows Help system for the command-line options.
-readme	Displays the Aventail Connect readme file.
-shutdown	Closes the Aventail Connect client.
-version	Displays Aventail Connect version information in a message box.
-runmode=[gina automatic manual]	<p>Sets the run mode for the Aventail Connect client.</p> <ul style="list-style-type: none"> • <code>gina</code> configures Aventail Connect to be launched by the GINA and enables Windows domain logon support. • <code>automatic</code> configures Aventail Connect to launch automatically when the user's desktop loads. • <code>manual</code> configures Aventail Connect to run only when the user manually starts it.
-displaysplash=<seconds>	For debugging purposes only. Displays the Aventail Connect client splash screen for a specified number of seconds. The default is 10 seconds.



Glossary

access control

A means of limiting access based on a user's identity or credentials. Typically used to control user access to network resources. An access policy is the set of rules that defines the privileges of users on the system. These rules define applications or network resources that users or user groups are allowed to access.

alias

An alternative label or name for an object such as a network, host computer, or network resource. Aliases have significant meaning for the Aventail Web access service; they mask the URLs of the internal network. Because all requests are directed to the Aventail Web access service, the user sees only the incoming URL that contains the alias. The Aventail Web access service matches the alias to a list defined in the AMC, and then translates the URL.

authentication

The practice of validating a user's identification or credentials in order to allow access to resources. Credentials are typically compared to some type of permissions list. There is a variety of authentication methods that dictate what type of credentials the user must have and when authentication should take place.

authorization

Permission granted to a user to use a system, and the data stored on it. Authorization specifies access rights after a user has authenticated.

Aventail ASAP WorkPlace

A dynamically personalized menu that provides access to Web-based resources on your network. After the user authenticates, the ASAP WorkPlace displays a list of Personal Links that provide access to all Web-based resources to which the user has access permissions. ASAP WorkPlace is accessible from any Web browser.

Aventail client/server access service

A server service providing secure, anywhere access to TCP/IP applications on your network, including enterprise client/server applications. The Aventail client/server access service is based on the SOCKS v5 protocol.

Aventail Connect

A configurable 32-bit Windows client that can connect to the Aventail appliance to provide authenticated and encrypted access to network resources. Aventail Connect is installed on the user's computer.

Aventail OnDemand

A secure, lightweight Java applet that can connect to the Aventail appliance to provide authenticated and encrypted access to network resources. Like most Java applets, it is usually configured to download at runtime and is not permanently installed on the user's computer. The only requirement for the user is a browser with a supported Java virtual machine.

Aventail Web access service

A server service on the Aventail appliance that provides clientless access to your Web applications and files, making secure access available from any Internet browser.

back-end

In a client/server application or system, the part of the program that runs on the server. (Note: Servers can also have front and back ends).



CA (Certificate Authority)

A trusted third-party organization that issues, renews, and revokes certificates. The CA guarantees that the individual granted a unique certificate is, in fact, who that individual claims to be (according to the CA's individual policies). A root CA typically issues certificates to intermediate CAs, which in turn issue certificates to users. Certificates are validated by following this hierarchy of trust up the certificate chain to the root.

certificate

A digital certificate that serves to verify a server's or client's identity and binds it to an RSA keypair that can be used to encrypt and sign digital information. A certificate is signed by a CA that vouches for the identity of the individual.

certificate chain

A sequence of certificates that includes the user's certificate (or "leaf") at the bottom, certificates for intermediate CAs (if any) in the middle, and the "root" certificate of the primary CA at the top.

cipher

A type of cryptographic algorithm that uses a key to convert plaintext to ciphertext, and vice versa.

client

The client component of a client/server architecture. It is used to send commands to and receive information from the corresponding server component that carries out the requests.

credentials

The specific information validating a user's permission to access a resource, such as the specific password used to authenticate or the actual information contained in a certificate.

CSR (Certificate Signing Request)

An application to a CA to issue a certificate that contains the user's name and cryptographic keys. The CSR does not contain information that allows the CA to authenticate the user; this is handled separately per the CA's due-diligence policies. The file name for a request usually ends with *.req*.

DES (Data Encryption Standard)

A popular standardized cipher for encrypting data. A common 56-bit key is used to encrypt and decrypt the data. Because 56 bits is inadequate for modern security standards, a common variant is to use DES three times with different keys (Triple DES).

DMZ

The "demilitarized zone" situated between the Internet and a network's firewall. Typically, the DMZ is used to host resources accessible via the Internet while maintaining security to the private network.

DN (distinguished name)

A name made up of a list of attributes and corresponding values that identify a user or group. DNs are used to represent names in certificates, and to look up entries in directory servers. Aventail generally uses the RFC 2253 guidelines when representing DNs.

DNS (domain name system)

The Internet utility that translates alphabetic domain names into numeric IP addresses. Each time a domain name is used, a DNS server must translate it. If one DNS server does not know how to translate a given domain name, it asks another server and so on until the domain name is correctly translated.

DNS server

A computer that answers domain name system (DNS) queries. A DNS server maintains a database of host computers and domain names, and their corresponding IP addresses. When presented with the domain name, it returns the matching IP address.

domain

A group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the Internet, domains are defined by the IP address. All devices sharing a common part of the IP address are said to be in the same domain.

downstream Web server

A private server on your internal network that is secured behind the Aventail Web access service. The Aventail Web access service uses aliases to obscure the URLs on downstream servers. Because all requests are directed to the Aventail Web access service, the user sees only the incoming URL that contains the alias. The Aventail Web access service matches the alias to a list defined in AMC, and then translates the URL.

encryption

The use of a cipher to generate the ciphertext, given the plaintext and a key. Encryption protects data from eavesdropping.

Filter-ID

A RADIUS attribute used to indicate a group to which the user belongs. Through its use, authorization rules may then specify group names, rather than usernames, in setting policy.

firewall

A system that can be implemented in software or hardware and prevents unauthorized access to a network. A firewall examines each message that attempts to pass through and obstructs those that do not meet specified criteria. There are several types of firewall techniques, and it is common to use two techniques together. Firewalls are considered the first line of defense in a security-based architecture.

fully qualified

May also be referred to as "full" or "FQDN" (fully qualified domain name). Used to describe the entire name, address, or path of a computer, host, domain, or file. It refers to a listing of all the components of a hierarchical system that lead to the specific file, IP address, host, or domain. A name, address, or path that is not fully qualified may contain an alias or may be a shortened version.

gateway

A combination of hardware and software that connects two networks using different communications protocols. It converts data exchanged between the networks so that each network can read what has been received from the other.

hash

Also referred to as a "hash value." A number generated by applying a formula to a string of text so that it is unlikely that another string could produce the same number. The hash is always much smaller than the text itself.

host

A computer connected to a TCP/IP network (which includes the Internet) that runs the server programs supplying resources and services to the Internet. Each host has a unique IP address.



host name

The non-numeric name for a specific computer that can be found via the Internet. An example of a host name is private.aventail.com. The host name refers to both the left-most portion of the name (private) and the name in its entirety (private.aventail.com). The remaining two portions are the domain name (aventail) and top-level domain (com).

HTTPS

A commonly used method of securing the HTTP protocol by layering it inside SSL.

IP (Internet Protocol)

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" and then transmitted. For more information, refer to RFC 791.

IP address

A unique ID number that identifies each individual computer on the Internet. Each 32-bit address is represented as four sets of 8-bit numbers, ranging from 0 to 255, separated by periods. A hierarchy from left to right represents a rough organization of the entire Internet, so that some networks can contain other networks. The last number on the right identifies the individual host computer.

key

A piece of information necessary for performing certain cryptographic operations. Keys may be generated randomly, or may be derived from user-friendly representations (such as passwords).

key length

The size of a key, generally measured in bits. When all other things are equal, a longer key length means a more secure but possibly slower algorithm.

key pair

The matching pair of public and private keys used by public-key cryptographic algorithms (for example, RSA). The public and private keys are used for opposing operations (encrypt a message with the public key; decrypt it with the private key).

LAN (local area network)

A network that connects workstations, computers, and other devices within a relatively small area (usually a single building). A LAN allows users to access data on other computers and to share devices such as printers. Multiple LANs can be linked together to create a WAN.

LDAP (Lightweight Directory Access Protocol)

A simplified version of the X.500 directory access protocol (DAP). For more information, refer to RFC 2251.

MD5

A specific message digest algorithm. MD5 is less secure than SHA-1 but is much faster and is often considered "secure enough."

multi-homed

A machine that has more than one NIC (network interface card) and is attached to more than one network.

NAS (Network Access Server)

A server that provides managed connectivity to a set of resources, such as a terminal server handling dial-in modems. A RADIUS client is generally called a NAS.



NAT (Network Address Translation)

An Internet standard that translates internal IP addresses into one external IP address, allowing organizations to present just one IP address to the Internet. NAT hides internal addresses, and also conserves IP addresses by reducing the number of addresses an organization needs.

NIC (network interface card)

A printed circuit board or card installed in clients and servers in a network that enables the computers to exchange data. Also called a network adapter.

Null

In reference to an authentication method, use of Null authentication means that no authentication is required. It is generally not a good idea to require Null (no) authentication in a production environment.

Personal Links

A dynamically generated list of all Web-based resources to which a user has access permissions. Personal Links are displayed in the Aventail ASAP WorkPlace.

ping

A diagnostic tool used to determine connectivity. To "ping" a remote host means to send ICMP ECHO_REQUEST packets and wait for a response. If there is no response, the remote host is down or unreachable; if there is a response, the time delay for the response can be used to determine the Round Trip Time (RTT) necessary for the exchange of data with that host.

plaintext

The unencrypted, readable text of a message.

ports and port numbers

In reference to TCP/IP and UDP networks, a logical channel or channel endpoint. Port numbers are assigned to application programs, and are used to link incoming data to the correct service. Well-known ports are standard port numbers commonly used for certain types of traffic. For instance, port 80 is typically used for HTTP (Web) traffic, while port 20 is typically assigned to FTP transfer.

private key

One half of a key pair used in public-key cryptographic algorithms, known to its owner and never shared. The public key is the other half of the key pair.

protocol

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

proxy server

A firewall component that manages Internet traffic to and from a LAN, serving as a proxy or intermediary between internal resources and external requests for those resources. Proxy servers hide true network addresses (preventing IP addresses from being spoofed or mapped), and secure and manage all application communication. With a proxy server, there is never a direct connection between an outside user and an internal resource. All traffic to and from internal resources is proxied by the proxy server. The Aventail client/server access service is a SOCKS v5 proxy server service.

public key

One half of a key pair used in public-key cryptographic algorithms, known by anybody and included in the user's certificate. The private key is the other half of the key pair.

public-key encryption

A cryptographic algorithm that uses two different keys for encrypting and decrypting data (as opposed to a conventional cipher, which uses the same key for both). Such systems allow key pairs (with one half made public and one half kept private) to be generated and used for digital signatures and key exchanges. Public key systems can be extremely secure and allow communication without the exchange of keys in advance, which facilitates communication among large numbers of unrelated parties (as over the Internet). The idea was invented by Diffie and Hellman, and the most commonly used public key algorithm is RSA.

RADIUS (Remote Authentication Dial-In User Service)

A protocol for communicating with a back-end authentication database. Useful for Username/Password, CHAP, and CRAM authentication mechanisms. The user sends credentials to the Network Access Server, or NAS, which then sends them to a RADIUS server. The RADIUS server performs the checking of the password, and tells the NAS whether to consider the authentication valid. For more information, refer to RFC 2138.

RSA (Rivest-Shamir-Adelman) encryption

The most widely used public-key algorithm today, RSA is named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adelman, who developed it at MIT in 1978. PGP, SSL, and S/MIME are generally used with RSA for key exchanges and digital signatures. RSA was patented in the United States, which limited use, but the patent expired in September of 2000.

SecurID

A two-factor user authentication system developed by RSA Security. The system is based on something you know (a PIN), and something you have (a hardware token). These factors are combined to form a dynamic passcode that the user types in via the authentication mechanism.

server

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

SOCKS v5

A security protocol for handling TCP traffic through a proxy server. SOCKS is the IETF standard for authenticated firewall traversal and can be used with virtually any TCP application. It acts as a proxy mechanism that manages the flow and security of data traffic to and from a LAN, intranet, or extranet. SOCKS uses sockets to represent and track individual connections. There are two main versions of SOCKS—SOCKS v4 and SOCKS v5. SOCKS v5 provides an authentication mechanism, while SOCKS v4 does not. For more information, refer to RFC 1928.

SSL (Secure Sockets Layer)

An authentication and encryption protocol developed by Netscape Communications to secure application protocols such as HTTP over the Internet. SSL uses a key exchange method (RSA is most common) to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. The IETF has generated a successor of SSL, a network standard called Transport Layer Security (TLS). SSL is the most widely deployed security protocol on the Internet today. For more information, refer to RFC 2246.

subnet

A segment of a network. Networks are divided into subnets (or subnetworks) for performance and security reasons. Subnets share a common network address with other parts of the network, even though they may be physically independent. Subnets are distinguished by subnet numbers and are bridged by routers. IP networks are divided using a subnet mask.

subnet mask

The method used to divide IP networks into smaller segments, or subnets. A subnet mask identifies the subnet to which an IP address belongs. Network administrators can divide the host portion of an IP address into two or more subnets. Part of the host address is then reserved to identify the particular subnet.

syslog

The UNIX system log to which logging information can be output.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic protocol suite of the Internet, of which TCP and IP are the foundation. TCP is the transport layer of the suite and correlates to OSI Layer 4, which regulates traffic. IP is the network layer of the suite and correlates to OSI Layer 3, which handles addressing. (TCP/IP uses four layers, in contrast to the OSI networking model's seven layers.) TCP ensures the reliable delivery of packets to their intended destinations, while IP ensures that packets are addressed properly. Other protocols in the TCP/IP suite include SNMP (Simple Network Management Protocol), PPP (Point-to-Point Protocol), SMTP (Simple Mail Transfer Protocol), and UDP (User Datagram Protocol). The TCP/IP protocol suite was developed by the Department of Defense for communications between computers. It has become the de facto standard for data transmission over networks, including the Internet. For more information, refer to RFC 793.

token

A small security device used to generate dynamic passwords. Some tokens display a number that frequently changes; the number is a password that is valid for a short period of time. Others include keypads for typing in a challenge, and compute the appropriate response that will allow successful authentication. Tokens are sometimes called "first-generation smart cards."

trusted roots file

A list of the root certificates an administrator chooses to trust. Every certificate chain ends with a root certificate. There is no "higher" CA to validate the root, so that root must either be trusted or not (if not, the whole chain is untrusted and should be rejected).

UDP (User Datagram Protocol)

A means of sending data over the Internet without guaranteed delivery. Also known as a connectionless protocol. UDP is part of the TCP/IP protocol suite and corresponds to Layer 4 in the OSI networking model (the transport layer). UDP converts data messages generated by an application into packets to be sent over an IP network, but does not guarantee that all of the packets will be delivered or will be in the proper order when they reach their destination. Unlike TCP, UDP provides no error-recovery services and is used primarily for the exchange of very small data units (datagrams) that require little message reassembly. For more information, refer to RFC 768.

virtual private network (VPN)

A secure channel used to access a private network over a public network (such as the Internet). There are two main types of VPNs: *remote access VPNs* provide remote employees with secure access to e-mail, file servers, and other network resources, and *extranet VPNs* provide business partners (such as suppliers or vendors) with secure access to a variety of applications, such as supply chain management (scm) programs.

wildcard

A special symbol that represents one or more characters. Wildcards can be used to identify files and directories, allowing users to select many files with a single specification. In the Windows operating system, for example, the asterisk is a wildcard that represents any combination of letters, so *n** refers to all files that begin with *n*, and *n*.doc* refers to all files that start with *n* and end with *.doc*.

X.500

A set of standards developed by the ITU (International Telecommunication Union) and ISO (International Organization for Standardization) in the mid-1980s that defines how global directories should be structured. The X.509 system of authentication (based on public and private key pairs) and LDAP evolved from the X.500 effort.

X.509

An ITU recommendation used to define digital certificates. The standard has not been officially approved and thus is implemented in different ways by different companies. Virtually all certificates in use today (SSL, S/MIME) are X.509 certificates.

Index

A

- access server settings 25
- adding
 - destinations 44
 - domains 39
 - files to a package 58
 - hosts 40
- advanced installation options 57
- advanced software settings 64
- application detection 21
- authentication
 - configuring options 27
 - credentials 1
 - customized dialogs 17
 - enabling modules 27
 - SSL 28, 90
- authentication realms 32, 89
- Authenticode signatures 21
- automatic startup options 55
- Aventail client/server access service 1
- Aventail Connect
 - advanced software settings 64
 - configuration files 8
 - Configuration Tool 8, 81
 - configuring 7, 74
 - Customizer 51, 92
 - deploying 4, 49
 - Event Viewer 74
 - installation problems 72
 - installing 4, 72
 - new features 2
 - overview 1
 - platform requirements 4
 - Remote Ping 78
 - setup packages 51
 - troubleshooting 71
 - updating configurations 68
 - updating packages 49, 64
 - updating software 49, 64
 - version 4.x 8, 18, 82
- avoiding destination conflicts 44

B

- binary configuration files 9
- bitmaps, authentication dialog 17
- browsing
 - domains 38
 - files 37

C

- cache, credential 31
- categories, event 75
- certificates
 - client 31, 52, 71, 91
 - PKCS #11 31
 - server 28, 30
 - X.509 2
- changing organization passwords 16
- ciphers, encryption 29
- clearing Event Viewer window 78
- clear-text configuration files 10
- client certificates 31, 52, 71, 91
- compression, SSL 29
- configuration file settings 60
- configuration files
 - binary 9
 - clear-text 10
 - creating 9
 - editing 10
 - opening 10
 - overview 8
 - protected 10
 - updating 8, 14, 68
- configuration problems 74
- configuration settings 82
- Configuration Tool
 - overview 8, 81
 - starting 9
- configuration update files
 - creating 9–10, 68
 - overview 8, 14, 68
- configuring
 - access server settings 25
 - authentication options 27
 - Aventail Connect 7, 74
 - Customizer options 54, 92
 - destination options 42
 - domain options 37
 - firewall integration 22
 - Microsoft Networks Support 38
 - multiple networks mode 19
 - network settings 16
 - organization settings 13, 82
 - proxy server settings 25
 - realms 32
 - restricted modes 18
 - standard mode 18
- conflicts, avoiding 44

- connection termination 19
- copying log messages 77
- creating
 - configuration files 9
 - configuration update files 9–10, 68
 - setup packages 53
- credentials
 - caching 31
 - Windows logon 51, 55, 63, 71
- Customizer
 - options 54, 92
 - overview 51, 92
 - starting 52
- D**
- defining destinations 42
- deleting
 - destinations 47
 - domains 40
 - hosts 42
 - networks 12
- deploying Aventail Connect 4, 49
- DES cipher 29
- destinations
 - adding 44
 - avoiding conflicts 44
 - configuring 42
 - defining 42
 - deleting 47
 - editing 46
 - excluding 45
 - including 44
 - types 42, 43
 - wildcards 43
- detecting
 - applications 21
 - local networks 50, 61, 62, 72
 - proxy servers 26
- directory, installation 55
- domain options 37
- domains
 - adding 39
 - browsing 38
 - deleting 40
 - dynamic 38
 - editing 39
 - static 38
- dynamic domains 38
- dynamic hosts 38
- E**
- editing
 - configuration files 10
 - destinations 46
 - domains 39
 - hosts 41
 - setup packages 53
- enabling authentication modules 27
- encryption
 - ciphers 29
 - SSL 1
- event categories 75
- Event Viewer
 - clearing window 78
 - closing window 78
 - copying messages 77
 - event categories 75
 - filtering messages 76
 - finding messages 78
 - logging levels 75
 - opening 75
 - overview 74
 - printing messages 77
 - saving messages 77
- excluding destinations 45
- exporting organizations 12, 68
- F**
- fallback servers 25
- files
 - adding to a package 58
 - browsing 37
 - configuration 8
 - configuration update 8, 14
- filtering log messages 76
- finding log messages 78
- firewall integration 22, 85
- H**
- hosts
 - adding 40
 - deleting 42
 - dynamic 38
 - editing 41
 - static 38
- I**
- images, authentication dialog 17
- importing organizations 12, 68
- inbound network access 3
- including destinations 44
- inserting networks 10
- installation directory options 55
- installation problems 72
- installation prompt options 54
- installing Aventail Connect 4, 72

integrating personal firewalls 22, 85
 Internet access proxy detection 26
 Internet proxy mode 20, 84

L

linking networks 8, 11, 81
 loading network views 13
 local networks
 detecting 50, 61, 62, 72
 overview 3
 specifying 4
 log messages
 copying 77
 filtering 76
 finding 78
 printing 77
 logging levels 75
 logos, authentication dialog 17

M

mapped drives 37
 Microsoft Networking Support 37
 Microsoft Windows Installer options 56
 modes
 Internet proxy 20, 84
 multiple network access 18
 remote network access 18
 restricted 18
 standard 18
 MSI options 56
 multiple realms 32, 89
 multiple networks mode 18, 19

N

NetBIOS 2, 37
 network connectivity problems 73
 network settings 62
 network view options 13
 networks
 configuring settings 16
 connectivity problems 73
 deleting 12
 inbound access 3
 inserting 10
 linking 8, 11, 81
 local 3, 61, 62, 72
 organizations and 8, 17
 outbound access 3
 overview 8
 remote 3
 renaming 17
 security 2
 NULL encryption 29

O

opening
 configuration files 10
 Event Viewer window 75
 setup packages 53
 organizations
 configuring 13, 82
 exporting 12, 68
 importing 12, 68
 networks and 8, 17
 overview 8
 passwords 15
 updating 14, 83
 outbound network access 3

P

package information options 58
 package signing options 66
 packages, setup 51
 passwords, organization 15
 personal firewall integration 22, 85
 ping 78
 PKCS #11 certificates 31
 planning deployments 49
 platform requirements 4
 primary proxy servers 25
 printing log messages 77
 protected configuration files 10
 proxy servers
 detecting 26
 primary 25
 secondary 25
 settings 25
 proxying traffic 18

R

RC4 cipher 29
 realms, authentication 32, 89
 recreating network views 13
 remote network access modes 18
 remote network access settings 61
 remote networks
 overview 3
 specifying 4
 Remote Ping 78
 renaming networks 17
 restricted modes 18

S

saving
 log messages 77
 network views 13
 setup packages 54

- secondary proxy servers 25
- security, network 2
- servers
 - certificates 28
 - fallback 25
 - primary 25
 - secondary 25
 - validating 30
- setup packages
 - adding files to 58
 - creating 53, 92
 - deploying 51
 - editing 53
 - opening 53
 - options 54
 - saving 54
 - updating 49, 64
- signatures, Authenticode 21
- single sign-on 51, 55, 63, 71
- SOCKS overview 2
- software updating options 64
- SSL
 - authentication 28, 90
 - compression 29
 - encryption 1
- standard mode 18
- starting
 - Configuration Tool 9
 - Customizer 52
 - Remote Ping 78
- startup options 59
- startup, automatic 55
- static domains 38
- static hosts 38

T

- TCP traffic 42
- TCP/IP 2, 37
- terminating connections 19
- timeouts, credential cache 31
- traceroute 78
- traffic, proxying 18
- troubleshooting
 - configuration problems 74
 - event logs 74
 - FAQs 71
 - installation problems 72
 - network connectivity 73
 - overview 71
 - ping 78
 - Remote Ping 78
 - traceroute 78
- trusted roots files 30

U

- UDP traffic 2, 42
- updating
 - Aventail Connect software 49, 64
 - configuration files 8, 14, 68
 - organizations 14, 83
 - setup packages 49, 64

V

- validating servers 30
- VPNs 3

W

- wildcard characters 43
- Windows credentials 51, 55, 63, 71
- Windows domain logon support 55, 63, 71

X

- X.509 certificates 2