VSClient VPN User's Guide

Revision A: VSClient Version 5.1e

Sören R. Olsen

Security Perimeter Design

12 September, 2002

Boeing Copyright Release

The Boeing VSClient 5.1e User's Guide is based on the VSClient 4.0 User's Guide, Rev. 5.42, copyright 1999 by InfoExpress, Inc. InfoExpress has given Boeing a copyright release, with these rights:

- The right to reproduce the material for Boeing and non-Boeing users of the Boeing InfoExpress system.
- The right to reproduce only portions of the material, omitting material that does not apply to our implementation.
- The right to incorporate the material into a document with other Boeing-specific information added.
- The right to modify the InfoExpress material to correct errors and enhance understanding.

Trademarks

InfoExpress, VTCP/Secure, VSGate, and VSClient are trademarks of InfoExpress, Inc.

All other names are trademarks or registered trademarks of their respective companies.

Contents

Chapter One

Boeing VSClient VPN Overview

. . . . . .

This user's guide specifically supports the Boeing VSClient Virtual Private Network (VPN) Implementation. We have modified the documentation (with the permission of InfoExpress) to fit the needs of our Boeing employees and non-Boeing partners.

Revision A has been updated to include a new Boeing-developed Connections Preferences Editor, which simplifies configuration of VSClient. We have also added scripts that automatically launch Z_Token software for you.

These document conventions are used are used to show Boeing-specific comments: informational material, recommended choices, and not-recommended choices. Additionally, we have added new sections specific to Boeing. For more information, go to the VSClient VPN web site:

http://compsec.web.boeing.com/products/access/vpn/altvpn/?pid=altvpn

Product overview

VTCP/Secure extends the corporate network to remote computers that use untrusted networks like the Internet or are connected through proxies or firewalls on remote networks. VTCP/Secure creates a remote VPN that authenticates, authorizes, and encrypts all data between the remote computer and the corporate network.

VTCP/Secure consists of VSClient software, which is installed on the remote computer, and VSGate software, which is installed on the server. VSGate links the remote computers on the untrusted network to the computers on the secure network.

System requirements

The minimum configuration for using VSClient 5.1e software is as follows:

- Windows 95, Windows 98, Windows 2000 Pro, and Windows NT 4.0 operating systems.
- Windows TCP/IP networking software.
- Direct or indirect connectivity to a server running VSGate 5.1 software through a supported proxy.
- Supported network applications.

Supported applications include most TCP and UDP applications, Microsoft networking, and file sharing.

What's new in version 5.1e

Integration with Z_Token

Several of the VSClient login scripts automatically launch the Z_Token software for you. While this is primarily intended to support Z_Token users in a pre-GINA environment (see ch. 3), everyone who uses the Z_Token authentication software will appreciate the ease of login these scripts provide for the Z_Token user.

The scripts which launch the "Z_Token" application include "& Z_Token" in the script name. Chapter 2 describes these scripts in detail.

Connection Preferences Editor dialog box

The Boeing VSClient Connection Preferences Editor enables you to maintain your personal information as well as information that may change depending on your remote location. When you select the Connection Preferences Editor script in the list and click **Connect**, you go to the **Connection Preferences Editor** dialog box, where you can configure your information. When you fill in the information in this dialog box, you are not prompted for it during the login process.

VSClient features

The following sections describe product features that you will use when you connect to Boeing resources using VSClient.

Connect to Boeing Resources

You can use VSClient to connect to Boeing resources through a tunnel from your local host network, Boeing laptop, or home computer. You use some of the following features to establish the settings necessary to create and monitor the connection.

Map Shares

Use Map Shares to set up the connections you require. This feature enables you to add and delete shares and view them in a list. You can also specify how to map shares when logging on and out.

Use Smart Tunnel Mode

When you use the Smart Tunnel mode, you can access network-based resources from your local host network and the VPN tunnel network simultaneously (also called "split tunneling"). For example, you can read your Boeing Outlook e-mail and print it on your local network printer without starting or stopping the VPN connection or changing the configuration for your tunnel session. Chapter 4 describes how to use this mode.

Use Always Tunnel Mode

Use Always Tunnel Mode for certain applications (such as Windows NetMeeting) that do not make their connections in Smart Tunnel mode. In these cases, you must switch from Smart Tunnel to Always Tunnel Mode and back. Chapter 4 describes how to use this mode.

Use Bypass Mode

Bypass Mode directs all traffic, such as connection requests, to the local network rather than down the tunnel. At that point, the network protocol stack sends the request normally. You maintain your tunnel connections, but cannot make new ones. Chapter 4 describes how to use this mode.

View Session Information

When you open the Session Information window, you can review your assigned IP address and domain and the addresses of the WINS, DNS, and NBDG servers available to your session. You should gather this information before you contact your local help desk. Chapter 6 describes how to find session information.

Record Traces

You can use the Trace feature to record connection activity so that any problems are documented. When you enable traces, you have a record that you can send to your local help desk to quickly solve your problem. Chapter 6 describes how to set Traces.

Compatibility with your applications

Use of VSClient can affect the software on your computer. These issues fall into two broad categories: features that are independent of the Microsoft Windows operating system and features that are dependent on the Microsoft Windows operating system. These issues are discussed in more detail in chapter 4.

Independent of Microsoft Windows authentication

The vast majority of applications used at Boeing are independent of the Windows operating system. This list of applications includes browsers, X-Windows, NetMeeting, Telnet, and FTP. Use of applications like these requires no special setup other than having both VSClient 5.1e and the application itself installed on the computer.

Dependent on Microsoft Windows authentication

These two features have authentication issues that affect your ability to gain access to Microsoft features:

- Microsoft Outlook (Exchange) checks the underlying NT logon credentials for authentication.
- The Map Network Drives feature requires accessing the underlying NT logon credentials for authentication.

How you approach gaining access to the Microsoft-dependent features depends on the function of your client platforms. Your approach may differ based on whether you are using a Boeing laptop, a computer belonging to another company, or a personally owned computer.

Installing VSClient 5.1e

This section describes the process for installing and configuring VSClient 5.1e software.

Before you begin

Before you can use VSClient software, you must have a Boeing DDA account and use your DES Gold card or your Z_Token to generate a one-time password for each session.

IMPORTANT: If you do not have a Boeing DDA account, go to the http://compsec.boeing.com/products/access/cass/external/?pid=cass.external web site to request one.

Downloading the VSClient 5.1e software

The method that you choose (or have chosen for you) determines your installation experience. The installation process is documented in a separate VSClient Install Guide on the VSClient VPN web site. These are the methods available for downloading and installing the software:

- Software Express
- NOS depot
- SMS push
- Web download

For more information

For more information about VSClient VPN, read these documents, all of which are available on the VSClient web site:

http://compsec.web.boeing.com/products/access/vpn/altvpn/?pid=altvpn

Quick Reference Card. This 2-pg procedure describes how to install and configure VSClient software. Available for Windows platforms.

Install Guide. Describes in depth how to install and configure VSClient software. This guide is available for Windows, Linux/Solaris, and Macintosh operating systems.

Tip sheets. List techniques for using VSClient VPN effectively.

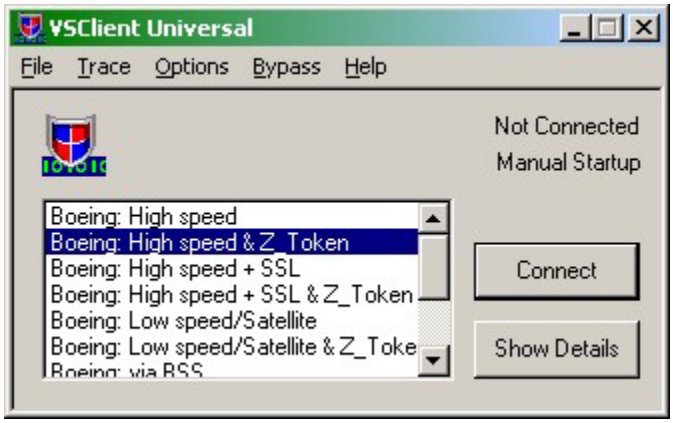
Troubleshooting Guide. Explains how to solve problems related to using VSClient software in the Boeing environment.

Chapter Two

Configuring Your Connection and Choosing the Right Script

. . . . . .

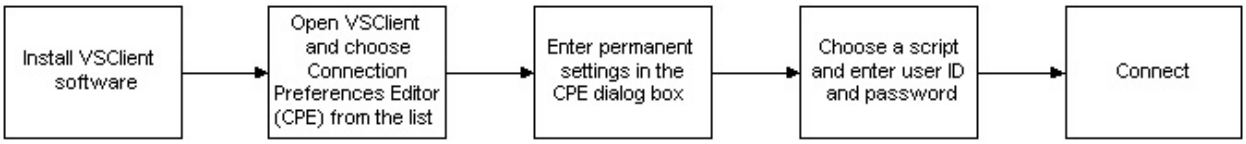
This chapter describes how to select a script from the logon scripts used for the Boeing implementation of VSClient VPN. As you can see in the following **VSClient Universal** dialog box, you connect by highlighting a script in the list box and then clicking the **Connect** button. A number of Boeing-specific scripts are available in the scrolling list box. This illustration shows the VSClient Universal window. Note the scripts in the list box.



These scripts cover most remote environments that you will encounter while traveling or working on site at a customer or supplier location. The last script in the list box launches the Boeing-specific **Connection Preferences Editor** dialog box, which enables you to enter your most-used connection preferences once rather than enter them each time you connect.

Process for configuring your connection

This illustration shows the steps you'll follow in this chapter:

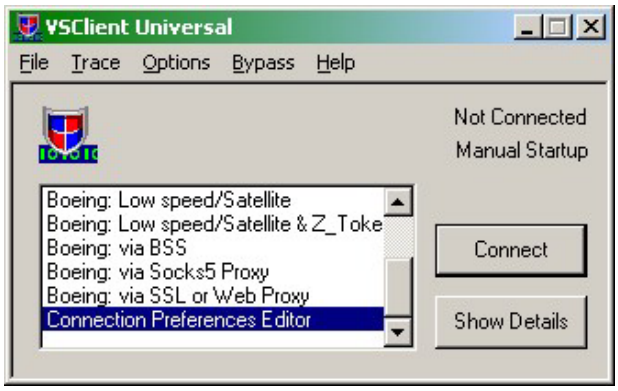


Chapter 3 describes how to connect after configuration is complete and Chapter 4 describes how to adapt your work patterns to using the VSClient VPN.

Configuring your connection

Follow these steps:

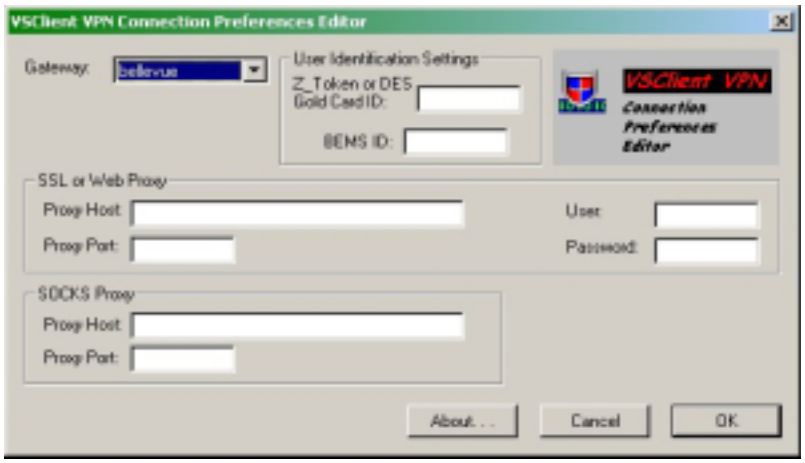
1. In the VSClient Universal window, click the **Connection Preferences Editor** script at the bottom of the list.



2. In the **Connection Preferences Editor** dialog box, enter the information needed for your connection. Boeing added this feature so that you do not have to enter these settings each time you connect.

   - In the **Gateway** box, select a location.
   - In the **User Identification Settings** group box, enter your Z_Token or DES Gold Card ID and your BEMSID.
   - **Note:** Your BEMSID is optional now, but it will be used in the future for authentication.
   - If you are a consultant or customer on a LAN, you may need to fill out the **SSL or Web Proxy** group box and the **SOCKS Proxy** group box. If you are uncertain about this information, contact your computing focal.

   Note: Read chapter 5 for detailed descriptions of all the fields in the **Connection Preferences Editor** dialog box.



3. Click **OK** to return to the **VSClient VPN Universal** window.

4. In the **VSClient VPN Universal** window, use the following table to select a script from the scrolling list box.

If you…	And you…	Then choose this script
Connect from home	dial in	Low speed/Satellite
	have DSL or a cable modem	High speed
	have a satellite-based ISP	Low speed/Satellite
	use DSL or a cable modem and you have a firewall such as Microsoft ISA with port 443 open	High speed+SSL
Work at BSS	are physically located at BSS	via BSS
Connect from a partner company	use DSL or a cable modem and port 443 is enabled; or on a customer LAN and port 443 passthrough is enabled on the firewall	High speed+SSL
	need to traverse a web proxy on the local firewall before connecting to VSGate over the Internet	via SSL or Web Proxy
	need to traverse a SOCKS5 proxy on the local firewall before connecting to VSGate over the Internet	via SOCKS5 Proxy
Connect from a hotel, etc.	can only use a dialup line	Low speed/Satellite
	have high-speed Internet access available	High speed
Use Z_Token		Choose a script with & Z_Token in the name

5. Click the **Connect** button.

6. Following the prompts, enter the required information, which may vary by script.

7. Click **OK**.

8. When you are connected, the VSClient Universal window status area changes from **Not Connected** to **Connected**, and then the window minimizes to the system tray.

If not connected, you will see a message box with the next instructions.

More about the logon scripts

The following table offers a technical explanation of each script family, with recommendations for the applicability of each script to your situation.

Script name	How it works	When to use it
Boeing: High Speed Boeing: High Speed & Z_Token	With this script, data is transferred over a single TCP connection without compression. This script supports one or more hops between the client and gateway, such as transparent proxies and address translation devices. *The option with "& Z_Token" also automatically launches the Boeing Z_Token application and waits for you to completely respond to all Z_Token prompts before proceeding with the connection process.*	From home with a cable or DSL ISP. From a hotel with high-speed Internet access.
Boeing: High Speed + SSL Boeing: High Speed + SSL & Z_Token	This script encapsulates the encrypted TCP datastream with the SSL protocol to connect to the gateway through a transparent SSL portal (e.g., at a customer site). This is not a proxy script and requires availability of port 443 from end to end. The encapsulation of the datastream with SSL adds overhead. Response is slower when using this option than it is when you use the standard High Speed option.	When you connect to Boeing via a customer site using a DSL line or when the site has enabled port 443 passthrough on their firewall.
Boeing: Low speed / Satellite Boeing: Low speed / Satellite & Z_Token	With this script, data is transferred over a single TCP connection using data compression. This script supports one or more hops between the client and gateway, such as transparent proxies and address translation devices.	From home with a dialup or satellite-based ISP. From any place where the only Internet access is via a dialup-based ISP.
Boeing: via BSS	This script connects to the gateway when you are physically working at the BSS sites in Anaheim, California, and surrounding areas.	This is the only choice if you are physically at BSS.
Boeing: via SOCKS5 Proxy	This script connects to the gateway through an SOCKS5 proxy. This is useful when connecting to the gateway through a remote firewall (e.g., at a customer site). You must provide the name of the SOCKS server and the port number that the client is to use. The default SOCKS port is 1080.	When you are physically at a site that requires using a SOCKS5 proxy for firewall egress (e.g., at IBM).
Boeing: via SSL or Web Proxy	This script connects to the gateway through an SSL proxy. This is useful when connecting to the gateway through a remote firewall (e.g., at a customer site). To use these scripts, you need the DNS name or IP address and port number of the SSL (or web) proxy. You may also be required to enter a user name and password for the SSL or Web proxy.	When you are physically at a site that provides a Web or SSL proxy for Internet browser access.

Chapter Three

Getting Connected With VSClient VPN

. . . . . .

This chapter describes how to connect to the Boeing network using the VSClient VPN.

Before you begin

The Boeing implementation uses strong authentication. You must have a Boeing DDA account and use your DES Gold card or Z_Token to generate a one-time password for each session.

VSClient for NT Logon (the pre-GINA panel)

When you select the **Add VSClient Logon for NT and Win2000** check box when you install VSClient on your computer, the **VSClient for NT Logon** box appears when you press CTRL+ALT+DEL to log on to your computer.

This box enables you to start a tunnel before logging on to your computer. When this tunnel is created, you log in using the Boeing domain controllers instead of locally cached credentials.

You have these options:

- To log on without starting the tunnel first, click the **Logon to NT** button without selecting the check box, and then proceed to your normal NT logon panel. **This is the default!**
- To start the tunnel before logging on, select the **Start VSClient VPN before NT logon** check box before clicking the **Logon to NT** button.
- To return to the CTRL+ALT+DEL security panel, click **Cancel**.
- To use the VSClient RAS dialing agent, VSDial, select the **Start Dial-up Networking for VPN Logon** check box. **Do not select this setting.**

Important: If you change the default setting, and you encounter one of the following conditions, you will be unable to receive help desk support and may not be able to use your workstation at all until you can connect your workstation directly to the Boeing network.

Specific support issues require this panel to be installed on your workstation. These specific issues are:

- Allows tunnel establishment before NT login, which can be necessary if you are connecting for the first time on a remotely located machine.
- Authenticates directly to the domain instead of to local cached credentials, which enables password expiration notification when you work remotely.
- Allows your local help desk to assist with remote password reset for local lockout conditions; otherwise, you must wait until you return to Boeing to access the computer in any way.
- Supports the Worldwide Site Operations (WWSO) Remote Domain Join requirement to create or rebuild "new" Boeing machines in a remote location.

VSClient integration with Z_Token

When you use one of the & Z_Token scripts, follow these steps:

1. When you click the **Connect** button, the Z_Token application is automatically launched and you go directly to the **Z_Token** dialog box.

2. Type your pin number and press **Enter** to go to the confirmation screen:

3. Click **OK** to continue the connection.

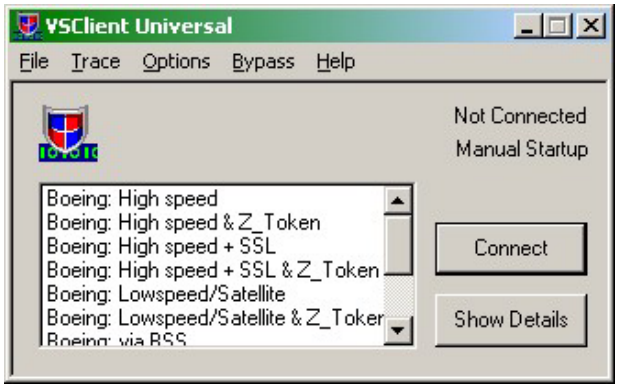
Connecting to the Boeing Intranet

Follow these steps:

1. On the **Start** menu, select **VSClient** from the **Programs** menu.

2. In the **VSClient Universal** window, select a logon script from the scrolling list box and then click the **Connect** button.

   Note: For more information about choosing scripts, read chapter 2.

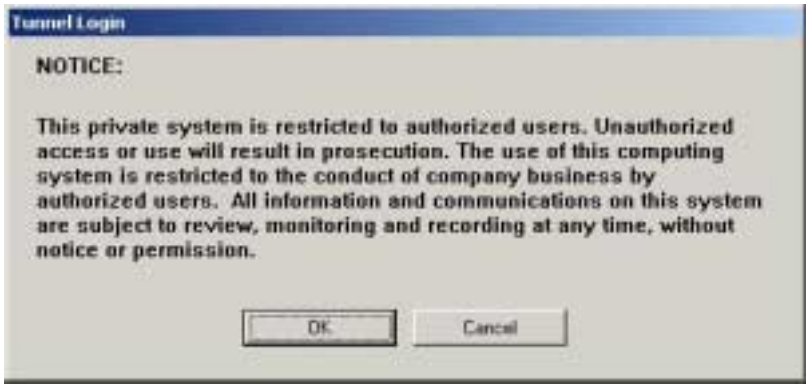


3. In the **Tunnel Login** screen, select the preferred Gateway location, and type your DESGold or Z_Token user name in the field provided. Click **OK** to continue or **Cancel** to end the login.

   Note: When you use the **Connections Preferences Editor** dialog box to configure all information that a particular login panel requires, you will *not see* that panel during the login process. The following panel is an example of one of these panels.

4. If you selected one of the scripts that includes **& Z_Token**, then you will go to the **Z_Token** dialog box. Respond to both Z_Token panels, and then the connection process can continue.

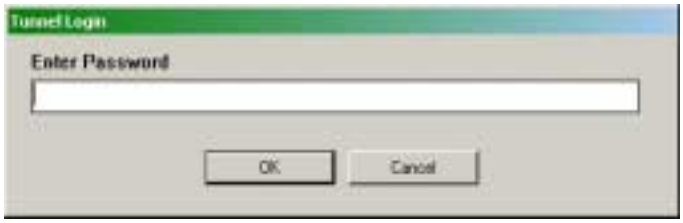
5. When the connection is first established with the gateway, you are presented with the following privacy notice. Legal requirements make it mandatory to present this dialog to everyone who logs in. Click **OK** to continue or **Cancel** to end the login.



6. When you are prompted for your password, enter the one-time password generated by your token, and then click **OK**.

   If you use a DES Gold card, you must type the one-time password in this panel.

   If you use Z_Token, you can use the CTRL+V command to paste the generated password from the clipboard.



7. When you are connected, the dialog box closes and the VSClient icon appears in the system tray at the bottom of your screen. This icon is animated when you are connected and static when you are not connected.

   If you are connecting in a pre-GINA environment, then you will see the NT Domain Login Panel at this point. If you are connecting from an established local session, you will see your normal desktop.

Chapter Four

Smart Tunnel Survivor's Guide

. . . . . .

This chapter describes how to use VSClient 5.1e in a Smart Tunnel environment. Even more important than learning how to deal with the Smart Tunnel mode of VSClient is learning VPN basics that give you the foundation you need to be successful when working at a remote location.

Living with the VPN environment

This section describes new work strategies you may need to learn when you use a VPN to connect to Boeing resources.

Know your own ISP

You need to learn the characteristics of your own ISP or LAN environment. The services that you receive at this level have tremendous impact on your overall experience. Know the DNS servers your ISP provides. Learn the normal responsiveness of each of them.

It takes longer to upload files than to download them

You will probably have a slower upload speed than download speed. In a VPN environment, this is very important. A number of "normal" network operations that you perform are bidirectional in their construction. They are slower (sometimes significantly) in sending data back to Boeing resources than in retrieving data from Boeing. Encryption only makes this situation worse.

The architecture of your VPN affects performance

One of the first things to consider is the architecture of the application that you use to provide your connectivity.

We refer to several applications as Layer 3 or Layer 2 applications. These applications ride very close to the physical architecture; therefore, there is little "translation" of protocols for them to do. This architecture includes PPTP, IPSec, and L2TP. As a result of this architecture, certain low-level protocols, such as Microsoft Networking, may perform significantly better.

Further, we refer to several more applications as Layer 5 applications. These applications are much farther removed from the physical architecture; therefore, with more protocol translation to perform, they are not as efficient at the low-level protocols and can show moderate to significant performance degradation compared to a Layer 3 application. VSClient is a Layer 5 application.

Network topology

We tend to think in geographical terms when determining what is "closest" to us. When determining the best server gateway to use from a particular location, that is not always the best approach. With access to the Internet, you should perform a traceroute to determine which server gateway is the fewest number of "network hops" from your location. This will show the best choice for a gateway selection. Contact the VSClient VPN group mailbox (VSClientVPN@boeing.com) if you require assistance in performing this for your location.

Rethinking working on shared file servers

Based on the way a VPN works, it may be best to rethink some work strategies when it comes to accessing documents located on shared file servers. It is much more efficient to copy a file to your local workstation, make the changes, then copy the file back to the server than it is to open the file on the server and make the changes over the network.

One method that seems to work fairly well is to use the **Briefcase** folder type in Windows and link your network documents to the briefcase. You can keep the document in sync by monitoring changes made to both the briefcase and network versions of the document.

What is a Smart Tunnel?

Smart Tunnel is the InfoExpress term for the split tunnel operating mode of their VPN product. Smart Tunnel allows a workstation simultaneously to access network-based resources from the local host network and from the VPN tunnel network. This capability enables you to read your Boeing Outlook e-mail and print it on your local network printer without starting and stopping the VPN or changing the configuration to the tunnel.

Some applications cannot make connections in Smart Tunnel mode

Certain applications cannot make connections in Smart Tunnel mode. To use these applications, you must switch the VPN to Always Tunnel mode. Once you make your connection, you can switch back to Smart Tunnel mode. Here is the list:

- NetMeeting (needed to make the initial connection).
- TLM Backup (entire backup session).
- McAfee ePO agent.
- CISCO IP SoftPhone.

Am I then "stuck" in Always Tunnel mode when I use these applications?

Maybe. Currently the only application that requires constant Always Tunnel mode is the TLM Backup tool. The other applications function normally after the initial connection is made. One of the notable features of VSClient is its flexibility to adapt to a changing environment. It does require learning as much as you can about your environment.

During the course of a normal day, there are times when you need to be in Always Tunnel mode and times when you need to be in Smart Tunnel mode. Times are dependent on the applications you must access and when you must access them.

Smart Tunnel "weight"

Depending on the settings you choose in the **For Smart Tunnel** group box in the **Session Settings** dialog box, VSClient gives "weight" for certain operations to the VPN tunnel or to the local network. These operations include, but are not limited to, mapping shares, Telnet, FTP, and X-Windows. Specific operations that are not affected by these settings are Outlook and Web browsing.

Configuring tunnel weight to the Boeing network

For the result results in accessing your Boeing network shares, follow these steps:

1. From the **Options** menu, select **Session Settings** (see ch. 6 for a full description of this dialog box).
2. In the **For Smart Tunnel** group box, make these selections:
   - Deselect **Use Downloaded Routes**.
   - Select **Use Dynamic Routes**.
   - Select **Always Tunnel WINS**.
   - Select **Always Tunnel NetBT**.

The **Use Dynamic Routes** option allows the client to tunnel everything with a boeing.com or mdc.com DNS suffix, which is what you want your client to do. This option also attempts to tunnel downloaded IP subnets as well as the DNS suffixes. Because we cannot send a valid list of IP subnets to the client at this time, having the client use the default information would lead to unpredictable and, most likely, undesirable results.

Selecting the two **Always Tunnel** options allows the WINS and NetBT protocols to automatically use the tunnel, allowing clean, smooth connections to your Boeing network resources at all times. It causes timeouts with any network resources on the host intranet from which you are tunneling.

Configuring weight to your local network

To give your local network prime consideration for the affected operations, use these settings in the **For Smart Tunnel** group box:

- Deselect **Use Downloaded Routes**.
- Select **Use Dynamic Routes**.
- Deselect **Always Tunnel WINS**.
- Deselect **Always Tunnel NetBT**.

Thoughts on Telnet, FTP, and X-Windows

The Telnet, FTP, and X-Windows protocols are greatly affected by the "weight" of the tunnel. When the tunnel is weighted towards the local network and you attempt to make a Telnet or FTP connection into Boeing, it will result in a DNS timeout.

When operating in this mode, follow this procedure to make a new Telnet or FTP connection. The assumption is made that you already have a VSClient connection.

1. Double-click the VSClient icon in the system tray.
2. On the **Options** menu, select **Always Tunnel**.
3. Launch your Telnet, FTP, or X-Windows application.
4. On the **Options** menu, select **Smart Tunnel**.
5. Minimize the **VSClient Universal** window.

If the tunnel is weighted towards the VPN tunnel, then Telnet or FTP connection requests are smooth and clean. Generally, when using X-Windows over a VPN connection, you should configure your X-server to use settings that minimize the amount of traffic sent over the network. For example, when using HcL Exceed, you would use Multiple Window mode so that Microsoft Windows is your Windows manager rather than a remote Windows manager. Using passive connection mode on the X-server and starting sessions via an initial Telnet connection also help to reduce network traffic. Using a configuration like this allows use of X-clients without having to change operating modes in the VPN.

The issue with Outlook

You may find that your e-mail does not flow smoothly through Outlook. Mail may only seem to appear when you click on your Inbox, and mail only appears to be sent when you click on your Outbox. Actually clicking on anything within Outlook may cause mail to be received or sent when you are suffering this condition. Finally, you may find that Outlook receives and sends your e-mail; however, it can take 30 minutes or more for this to occur without some intervention.

To fix this condition, follow these steps:

1. VSClient must not have a session connection.
2. From the **Start** button, select **VSClient** from your **Programs** menu.
3. On the VSClient **Options** menu, select **Session Settings**.
4. Select the checkbox for **Include Gateway Address Locally**.
5. Click the **OK** button.

Outlook will now function properly, with your e-mail smoothly flowing in and out as you would expect.

The perils of PDAs

Most people with PDAs have them synchronize data with Outlook, including the Calendar, Contacts, and possibly the Inbox. When working in a VPN environment, docking your PDA requires attention to detail; otherwise, you can lock up your session, your Outlook client, or both. Always make sure that your Outlook client is connected to the server when you dock your PDA. Also, always properly undock your PDA properly before you close down your Outlook client connection to the server. Never leave your PDA docked during a reboot.

The perils of mapping shares

It is probably easier to "hang" a Windows-based workstation by clicking on an unavailable network mapped share than any other single method available. There is really no way to protect you from this situation from a system level. When you are in a VPN environment, this type of problem can become even more common.

General notes on mapped shares in the VSClient environment

Success in mapping network shares depends on a number of issues, including the settings on your workstation for DNS, DHCP, the NT domain/username you are logged in to, and the settings within your VSClient configuration. Your workstation settings directly affect the ability of your workstation to locate and authenticate to the resources that you must access, and your VSClient settings directly affect the ability of the client to work seamlessly with these resources when it is in Smart Tunnel mode.

Note: Earlier versions of VSClient (5.1 and earlier) have a known issue with Windows 2000 authentication. You can resolve these issues by upgrading your client to 5.1e.

Methods of mapping shares

There are two basic ways to map network shares when you are in a VSClient VPN environment. These methods are either to use VSClient methods or standard Windows methods. The following sections discuss both options.

Mapping shares using the VSClient methodology

This method involves using tools available within the VSClient application itself. This method works best for non-Boeing workstations where you do not want persistent connections. All shares are mapped using Universal Naming Convention (UNC) format.

Mapping shares using the standard Windows methodology

The most familiar method for most people is to establish access through the My Computer or Windows Explorer. The actual work is done through the Windows **Map Network Drive** interface. This interface allows the user to easily establish persistent shares that reconnect when the user logs on. This method works best for Boeing workstations where you want to keep persistent connections. All shares are mapped using UNC format.

Mapping Boeing resources on Boeing workstations

If you have your tunnel mode set to Always Tunnel or set to Smart Tunnel with the Tunnel-weighted configuration, you can map Boeing resources as you would if you were directly connected to the Boeing Intranet.

If you are in Smart Tunnel mode with the Local-weighted configuration, you will see the following error:

Mapping resources on your host Intranet with a Boeing Windows 2000 laptop

There are several scenarios to address in this arena. These include making the initial connection to a resource on your host Intranet and reconnecting to a persistent connection on your host Internet environment.

Making the initial connection to a resource

To make the initial connection to a network resource on your local host network, follow these guidelines:

- You must be connected to the Boeing network, so the workstation can talk to a domain controller.
- VSClient must be in Smart Tunnel mode, and in the **Session Settings** dialog box, the **For Smart Tunnel** group box must have these settings:
    - **Always Tunnel WINS** is deselected.
    - **Always Tunnel NetBT** is deselected.
- You *may* have to make your local connections using IP addresses instead of names; for example, instead of \\hostname\sharename, you may need to use: \\123.456.78.9\sharename.

Reconnecting to a persistent connection with the same Windows 2000 laptop

The method you choose for reconnecting to a persistent connection may be dictated by whether you log on to your laptop locally using cached credentials before making the VPN connection to Boeing, or you start the VPN tunnel into Boeing and log on via the domain controller to get credentials.

Log on to NT locally first

When you log on locally using cached credentials, follow these steps:

1. Log on to your NT account.
2. Right-click **My Computer**, and then click **Explore.**
3. In succession, click each local network share you must access and type passwords, as necessary.

Log on to NT via VPN tunnel

When you log on via the VPN Tunnel, follow these steps:

1. Log on to your NT account.
2. Double-click the VSClient icon in the system tray.
3. On the **Bypass** menu, toggle to put the tunnel into Bypass mode.
4. Right-click **My Computer**, and then click **Explore**.
5. In succession, click each local network share you must access and type passwords, as necessary.
6. Select **Bypass** on the **VSClient Universal** window to return the tunnel **to Smart Tunnel** mode.
7. Minimize the **VSClient Universal** window.

   Note: As you work with the recommended settings, you will find that the connections to your local network shares time out. When this occurs, you should repeat this procedure, beginning with step 3.

Mapping to Boeing resources with a non-Boeing computer

Mapping Boeing network shares on your own computer is a different matter, and the following sections describes instructions for Windows 9x, Windows 2000, and NT 4.0 operating systems.

Windows 9x

If you use a Windows 9x operating system, you must follow additional steps to set up your computer to log on to your Boeing domain:

1. Configure the computer to appear to belong to a proper Boeing domain (see app. A for procedures related to Windows 98SE).
2. Configure the user on the computer to match their Boeing user ID.
3. Set the password on the computer to match the Boeing domain password.

Logging on using Windows 9x

After you have set up your shares, follow the normal logon procedure (see ch. 3). For smooth performance, set the tunnel weight for the VPN tunnel (see previous sec.) or set the tunnel mode to **Always Tunnel**.

1. In the **VSClient Universal** window, select a script, and then click the **Connect** button.
2. Begin a normal session.
3. If your computer was not properly configured, you will see a dialog box like this:

   This box does not provide a way to enter your Domain or user ID, so go to step 4.

4. Click the **Cancel** button and allow the logon to proceed without mapping the share. Repeat this process for each share that you attempt to map.
5. Log off and correct the configuration problems.
6. Repeat the logon procedure until the shares are mapped properly.
7. Begin a normal session.

Windows 2000 and NT 4.0

If you use the Windows 2000 or NT 4.0 operating system, then you can use the **Connect As** feature to supply the Boeing domain/user ID and password necessary to connect to the resource.

It is recommended that you use the VSClient Methodology (see previous sections) to map shares when you map Boeing resources on a non-Boeing workstation. This ensures that your computer is connected to Boeing resources only when the VPN tunnel is established.

To set up your list of shares to map, open the **VSClient Universal** window and, on the **Options** menu, select **Map Shares**. For each share, follow these steps:

1. In the text box, enter the name of the share.
2. Click the **Add to List** button.
3. Repeat step 1 and 2 for each share that you want to map.
4. No changes are necessary in the **First Mappable Drive Letter (C-Z)** and **First Mappable Printer Number (1-8)** boxes for this process.
5. Check the **Map Shares in List when Logging on** box.
6. Check the **Unmap Shares when Logging Out** box.
7. Click the **Done** button.

Logging on using Windows 2000 or NT 4.0

After you have set up your shares, follow the normal logon procedure (see ch. 3). For smooth performance, you should set the tunnel weight for the VPN tunnel or set the tunnel mode to **Always Tunnel**.

1. In the **VSClient Universal** window, select a script, and then click the **Connect** button.
2. Select a gateway from the list and then click **OK**.
3. When you see the Warning notice, click **OK**.

4. Enter your one-time password and then click **OK**.
5. For each of the shares you map, you will see the **Enter Network Password** dialog box.

6. In the **Connect As** box, type your user ID for Domain/User ID.
7. In the **Password** box, type your password.
8. When the **Enter Network Password** dialog box appears for each share you have mapped, repeat steps 2 and 3.
9. Begin a normal session.

Logging off

When you click **Disconnect** to end your session, VSClient automatically unmaps each share and returns you to your nontunneled configuration.

Chapter Five

VSClient 5.1e Screens and Menu Commands

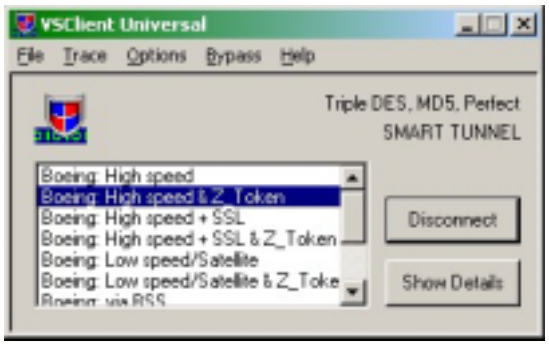
. . . . . .

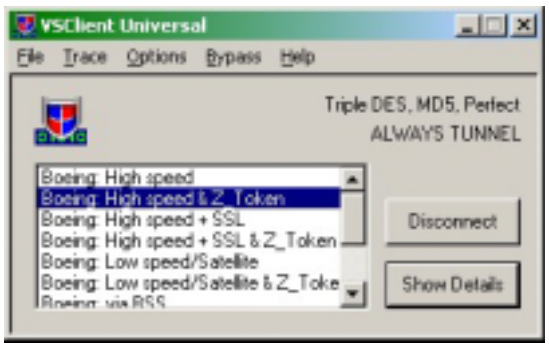
This chapter includes descriptions of a all product screens and commands.

VSClient Universal window

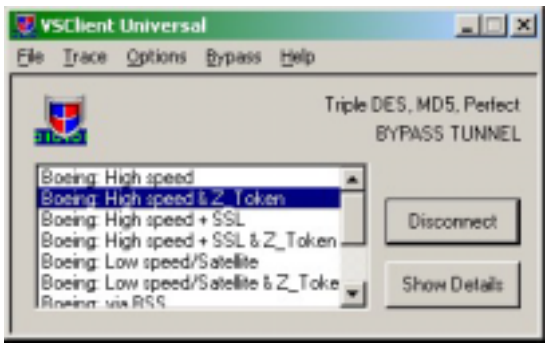
This section describes the screens, menus, and commands in the **VSClient Universal** window. In addition to the list of scripts and connection button, the **VSClient Universal** window displays the current state of your tunnel.

When the connection is active, you see one of these two messages:





When in Bypass mode, you see this flashing message:

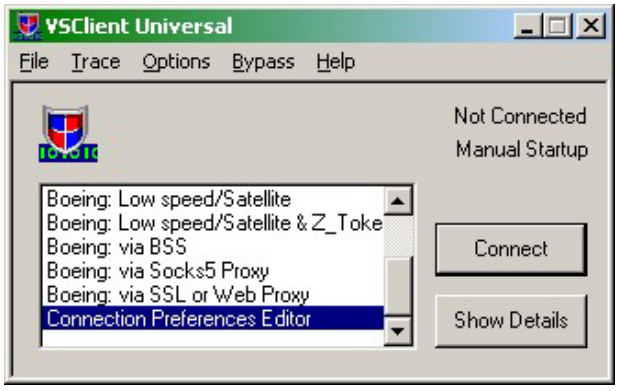


This table explains the elements of the **VSClient Universal** window. Menu items and dialog boxes are described in detail in the following sections.

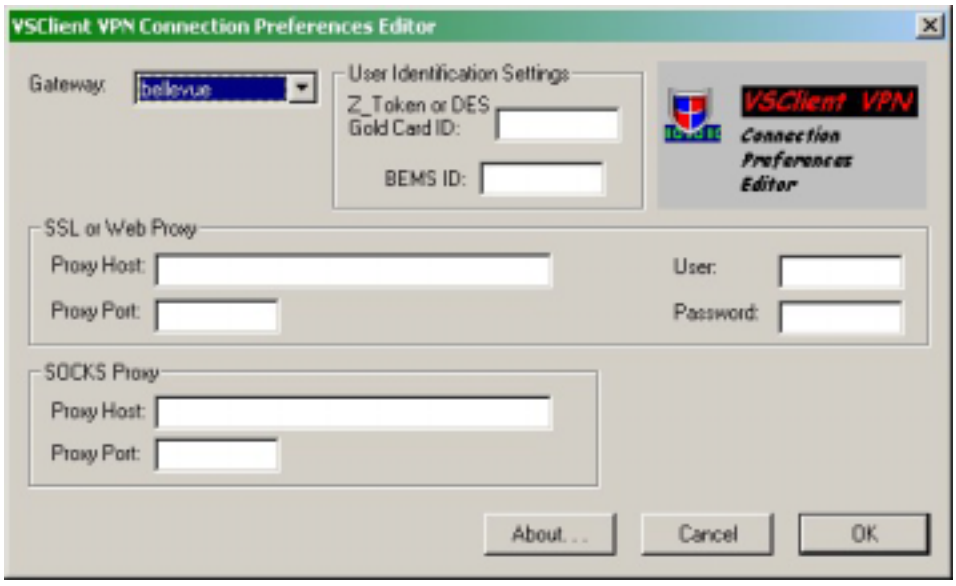
Element	Function
Script scrolling list box	Shows different scripts for connecting to the gateway. The scripts provide methods for connecting to the gateway over direct Internet connections or though port address translation (PAT) or network address translation (NAT) devices at the remote user's location. Several standard logon scripts are included for your convenience.
Connect button	Runs the highlighted logon script to start a tunnel. If the tunnel is already running, this terminates the session.
Show Details button	Displays a trace window that shows information about the current logon session. This is useful when troubleshooting the system. Changes to a **Hide Details** button when the trace window is open.
File menu	Includes commands related to connection, session information, shares, and script options.
Trace menu	Includes commands for recording and showing trace data.
Options menu	Includes commands for setting Smart Tunnels and mapping network shares.
Bypass menu	Includes the command for toggling between tunneling and using your usual network.
Help menu	Lists commands for reaching online help and the **About** box.
Status area	Shows the current connection state and specified type of startup.

Boeing Connection Preferences Editor dialog box

The Boeing VSClient Connection Preferences Editor enables you to maintain your personal information as well as information that may change depending on your remote location. To use this dialog box, select the **Connection Preferences Editor** script from the list, and click **Connect**. This should be done when you are not connected to a VPN session.



When you go to the **Connection Preferences Editor** dialog box, you can configure your own information into your VSClient installation. When you complete all the information, you are **not** be prompted for this information each time you log on.



Use the **Connections Preferences Editor** dialog box to configure your default gateway and external access user ID for authentication to the Boeing network. You can also maintain specific proxy information for gaining access to the Internet from behind a partner company's firewall environment.

Element	Function
Gateway dropdown list box	Establishes your default gateway. The three gateways for access are ***bellevue***, ***sealbeach***, and ***stlouis***. These are the only three options on the dropdown list box. This is only a starting point for access. When the client is unable to connect to either server on the perimeter you choose, it tries servers from the other two perimeters until it has connected you to Boeing or has failed to connect to all six servers.
Z_Token or DES Gold Card ID text box	Configures your Boeing standard external access account name into your VSClient installation. Enter either a user ID associated with a DES Gold card or the Z_Token software token.
BEMS ID text box	Configures your BEMSID into your VSClient installations. This field is currently not used; however is available for a future migration to certificate-based authentication.
SSL or Web Proxy group box	Enables you to configure information for use by a SSL or Web proxy to gain Internet connectivity from within a partner's firewall environment. All locations need the **Proxy Host** and **Proxy Port** entries. Some require the **User** and **Password** fields.
SOCKS Proxy group box	Configures information for use by a SOCKS5 proxy to gain Internet connectivity from within a partner's firewall environment. You must complete the **Proxy Host** and **Proxy Port** fields. The standard default SOCKS port is 1080.

File menu

Use the **File** menu to reach settings related to connection and information about the session.

Element	Function
Connect	Executes the currently highlighted logon script.
Disconnect	Terminates the current session. Closes all connections established through the tunnel.
Suspend	Suspends the current session. Does not close connections; however, you must log on again before data can be sent. Data can be received by applications in suspend mode, but not sent.
Session Info	Shows server settings for the current session or, if not logged on, for the last session.
Share Info	Shows shares currently in use on this computer.
Script	Offers several script options, including creating, copying, editing, and deleting the highlighted script on the **VSClient Universal** window. **This option is disabled.**

Trace menu

Use the **Trace** menu to establish settings for displaying, saving, and clearing trace data.

Element	Function
Show Trace Data	Shows (or hides) the Trace Display. The trace display is normally hidden other than during a logon session. This command can be used to show the Trace Display for the last logon session.
Trace Logon	Shows events associated with logging on.
Trace Data	Shows network data transfers during a session. Data transfers through the tunnel are preceded with a *V*.
Trace Session	Displays session information such as compression ratios and key updates.
Clear Trace	Clears the trace display.
Save Trace	Saves the information in the trace display to a file.

Options menu

Use the **Options** menu to make session settings, map shares, and define tunneling options.

Element	Function
Always On Top	Places VSClient on top of other open windows on the desktop.
Session Settings	Configures tunnel startup, selective tunneling, and other options pertaining to a tunnel session.

Driver Settings	Configures device sharer options. **This option is disabled.**
Map Shares	Configures the shares that are added after logging on to VSGate.
SMART Tunnel	Selectively tunnels data according to the options specified in the **Session Settings** dialog box.
Always Tunnel	Tunnels all data. Even if this option is selected, VSGate may still elect to reject data requests that do not meet the user's access privileges.
Bypass Tunnel	Does not tunnel any new connections. Existing connections will continue to run. This mode lets users who are not allowed to use the Smart Tunnel to bypass the tunnel temporarily without terminating the current session.

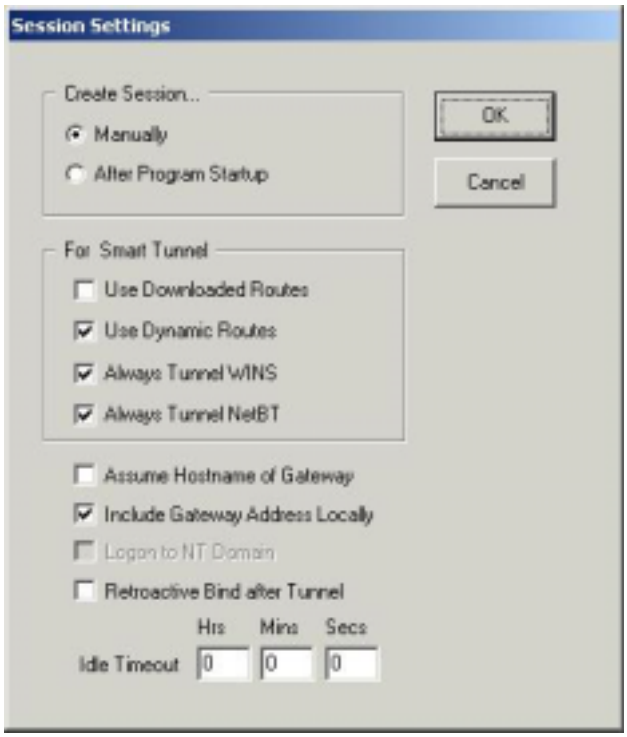
Bypass menu

Use the **Bypass** menu to toggle between the current tunnel mode and the **Bypass Tunnel** mode.

Element	Function
Bypass	Toggles VSClient between the current tunnel mode (Smart or Always) and the Bypass tunnel mode.

Session Settings dialog box

This section describes the elements of the **Session Settings** dialog box.



Create Session group box

This section describes settings that specify when a session is initiated.

Element	Function
Manually radio button	Establishes a session only when you click the **Connect** button. **(You should select this option.)**
Program Startup radio button	Establishes a session immediately after starting VSClient. This mode is useful when the command line options or script launches other applications automatically.

For Smart Tunnel group box

These options specify the methods that VSClient uses to determine when to tunnel data.

Element	Function
Use Downloaded Routes checkbox	Uses the DNS suffixes and IP routing information downloaded from VSGate to determine which IP addresses should be tunneled**. (Do NOT select this option.)**
Use Dynamic Routes checkbox	Uses the DNS suffixes downloaded from VSGate to deduce which IP addresses should be tunneled. For example, if the tunneling suffix is acme.com, a connection to a host called server.acme.com would be sent through the tunnel because the suffix matches the domain name, which in turn is resolved to a specific IP address, which is tunneled. **(You should select this option.)**
Always Tunnel WINS checkbox	Always tunnels WINS and NETBios datagrams, which Windows uses to resolve computer names into IP addresses for Microsoft Networking services. **(You should select this option.)**
Always Tunnel NetBT checkbox	Always tunnels NETBios over TCP data. NETBios over TCP is used to provide Microsoft Networking services such as browsing, file sharing, and printing. **(You should select this option.)**

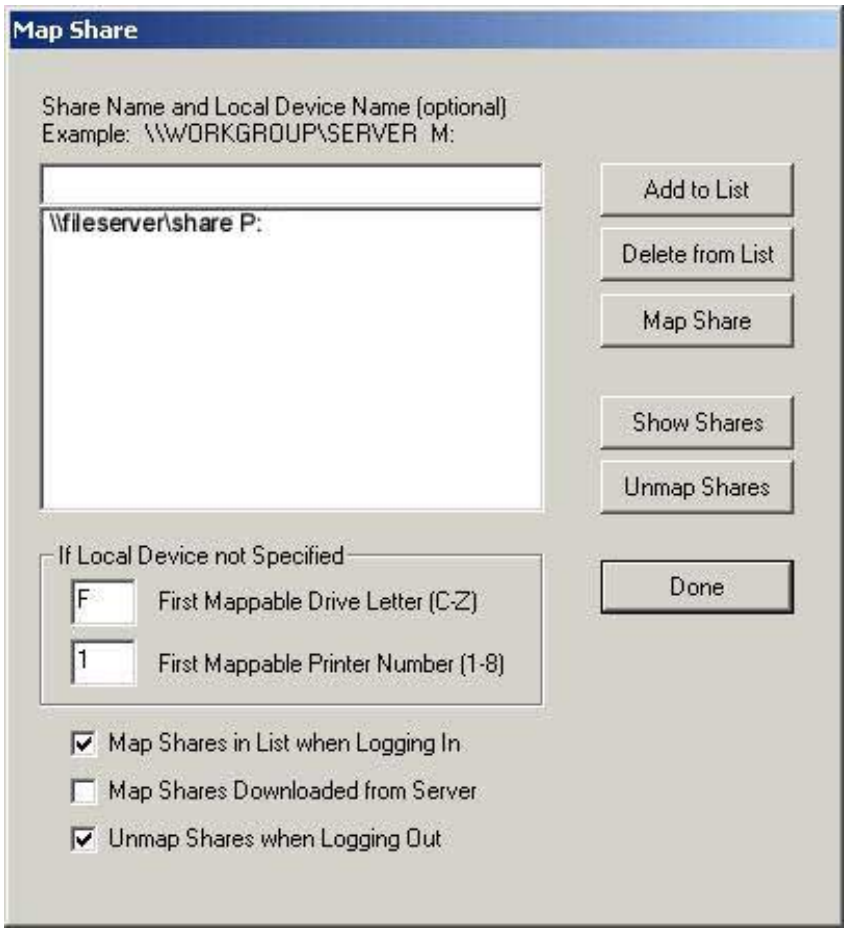
Other items

Element	Function
Assume Hostname checkbox	Assumes the hostname of VSGate while the tunnel is up. This provides better compatibility with some applications that use the hostname of the computer to determine its IP address. This also causes the system to assume the domain name of the gateway for non fully qualified domain names. This feature enables Outlook to work properly; however, it causes DNS problems with non-fully-qualified domain names. This option is **not recommended**.
Include Gateway Address Locally checkbox	Enables Outlook to work properly without many of the DNS issues associated with the **Assume Hostname of Gateway** option. **This is a recommended option.**
Automatic Logon	Logs on to the NT Domain Controller after the tunnel is up. This option only

checkbox	works on Windows 95 and 98 operating systems and is ignored on Windows NT. **Use only for a Boeing computer.**
Retroactive Bind checkbox	Enables data to be tunneled to server applications that were running before tunnel startup. Server applications normally "bind" to a port to listen for incoming connections. **(Recommend that this be left unchecked.)**
Idle Timeout checkbox	Terminates the tunnel after the specified seconds of user inactivity, which is detected by monitoring the use of the mouse. Setting this value to 0 means that idle timeouts are disabled.

Map Share dialog box

The VSClient VPN team has not worked to date on mapping shares or accessing Boeing Outlook e-mail on computers owned by other companies.



Note: This dialog box is not required to support standard Microsoft networking operations. You can use **Explorer**, **Network Neighborhood**, **My Computer**, and all other Windows methods to access resources on the corporate network.

You can use this screen to specify the shares that VSClient should connect to. This screen provides the option of manually connecting to individual shares or automatically connecting to all shares during a tunneling session.

The remote share name field can contain a share name like \\server\d optionally followed by a local device name. For example: \\SERVER\PUBLIC P:

If the share is a share and the local name is omitted, the share is assigned to the next unused share letter; if the local name is included, it is used when it is available. The list can contain a combination of resources that include and omit the local name.

If the share is a printer, the local name is required and must have the format LPT#.

The following table describes the commands in the **Map Share** dialog box.

Element	Function
Add to List button	Adds the share in the text box to the list of shares underneath.
Delete from List button	Deletes the share in the text box from the list of shares underneath.
Map Share button	Maps the share in the **Edit** box.
Show Shares button	Shows the currently mapped shares on this computer.
Unmap Shares button	Unmaps all shares that were mapped from this dialog box.
Done button	Saves your settings and closes the **Map Share** dialog box.
First Mappable Drive Letter [C-Z] text box	Specifies the first share that will be assigned when automatically mapping shares from the local list or downloaded from VSGate where a local share letter has not been provided.
First Mappable Printer Number [1-8] text box	Specifies the first printer that will be assigned when automatically mapping printer shares from the local list or downloaded from VSGate.
Map Shares in List when Logging on checkbox	Automatically maps shares in the list after logging onto VSGate. **(If you are mapping shares, this is recommended!)**
Map Shares Downloaded from Server checkbox	Automatically maps shares that have been downloaded from VSGate after logging on. **(Do not select this option. Shares are not available from the server!)**
Unmap Shares when Logging Out checkbox	Automatically unmaps all shares that were mapped while logging on from the **Map to Shares** options. **(If you are mapping shares, this is recommended!)**

Chapter Six

Getting Information from VSClient 5.1e

. . . . . .

When you have successfully connected to the Boeing Intranet, VSClient downloads its configuration settings, and then becomes an icon in your system tray. Follow these steps to get information about your session:

1. To open the **VSClient Universal** window, double-click the VSClient icon in the system tray.

2. In the VSClient window, on the **File** menu, select **Session Information**.
3. In the **Session Information** window, review this information:
    - Your assigned IP address.
    - The assigned domain.
    - The addresses of the WINS, DNS, and NBDG servers available to your session.
    - Encryption strength details.
    - Your available access list names.

Showing the current mapped shares

To see all the current mapped shares, on the **File** menu, select **Share Info**.

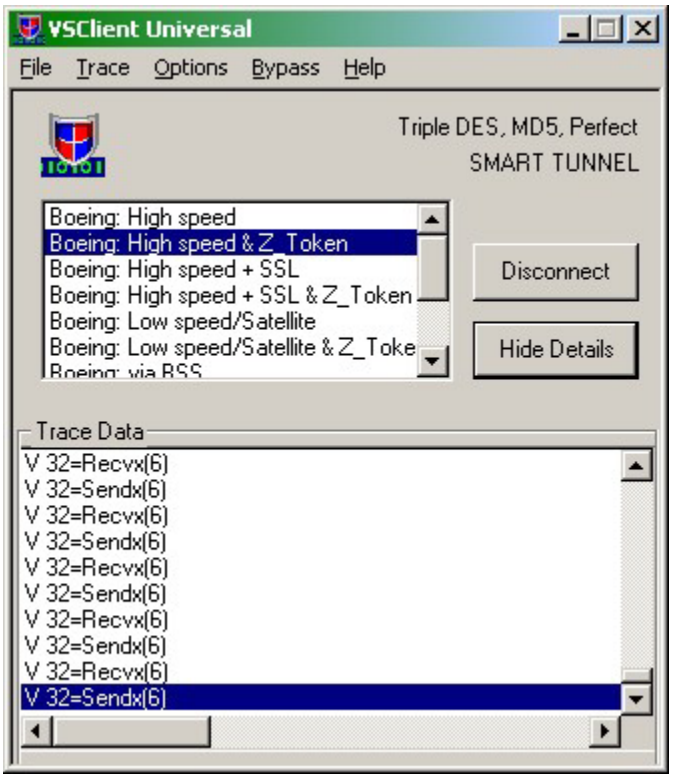
Using trace data to solve problems

For most problems, the first step is for you to enable the traces to display the events on a trace list during login and the application session. You can also select **Display-Show Trace** to see events from the previous session when VSClient is off. Although the number of events logged to the trace display is limited (older events are overwritten with newer ones), the trace display can be saved to disk and sent to your system administrator.

Viewing trace data

To save traces, follow these steps:

1. On the **Trace** menu, select **Trace Login**, **Trace Network**, and **Trace Session**.
2. To view the traces as you work, click the **Show Details** button, which then toggles to a **Hide Details** button you click to close the trace data.

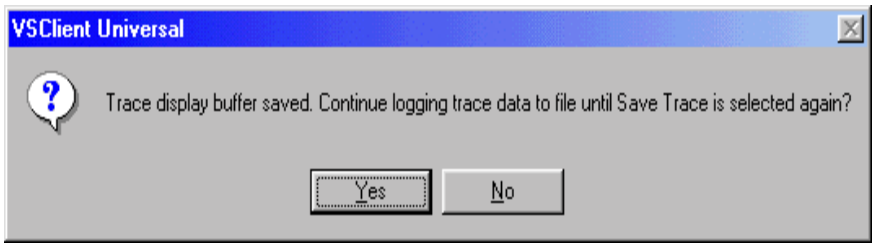


Saving trace data

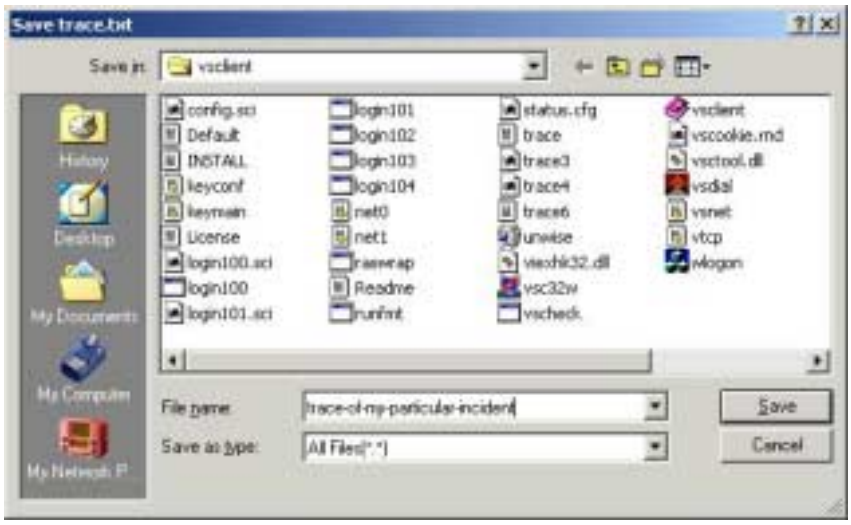
To save traces, follow these steps:

1. On the **Trace** menu, select **Save Trace Data**.

   You are prompted to choose whether you want to continue to log trace data after saving this trace data. If you click the **Yes** button, you do not see the second dialog box until you choose to save trace data again. If you click the **No** button, you go to the second dialog box immediately.



2. In the **Save trace.txt** dialog box, specify the location where you want to save the trace data and then click **Save**.



Filenames are by default in the format *trace#.txt*. The default filename is ***trace.txt***. Do not choose the default filename, as this can be easily overwritten. Choose a filename that you can find again so that you can provide it to the analyst you contact for assistance.

If you see the dialog box that asks you if you want to continue logging, and you need to find the trace file to send to the support analyst, look for the filename in the default filename format for the date/time stamp that matches your save time. You see the basic contents of the install VSClient directory above, after several trace files have been saved. A distinctive filename stands out when you want to find it later.

Appendix A

Configuring a Windows 98 Node To Connect to Boeing

. . . . . .

Before you begin

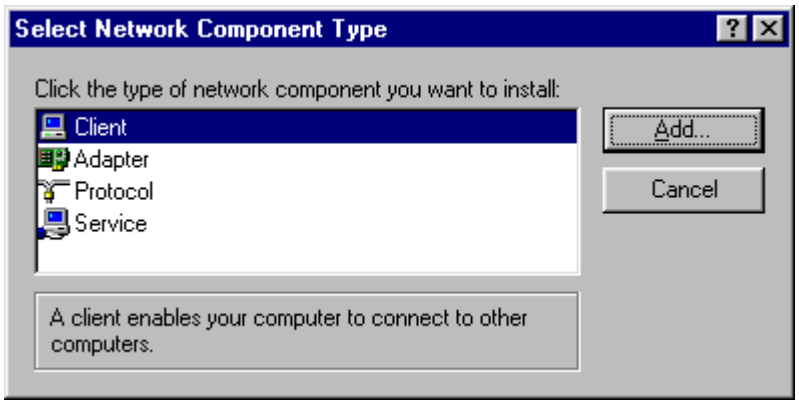
To find out whether Client for Microsoft Networks is installed on your computer, follow these steps:

1. On the Windows desktop, click the **Start** button, and then select **Settings**.
2. In the **Settings** dialog box, select **Control Panel**.
3. In the **Control Panel** dialog box, select **Network**.
4. Look for **Client For MS Networks** in the list.

Installing Client For Microsoft Networks

Follow these steps:

1. On the Windows desktop, click the **Start** button, and then select **Settings**.
2. In the **Settings** dialog box, select **Control Panel**.
3. In the **Control Panel** dialog box, select **Network**.
4. Click the **Add** button.
5. Choose **Client** from the list, and then click the **Add** button.



6. From the list of manufacturers (on the left side), select **Microsoft.**
7. Under **Network Clients**, choose **Client For Microsoft Networks**.
8. Click **OK** to finish.

Configuring a Windows 9x computer to connect to Boeing

Follow these steps:

1. Configure your machine to log on to a Boeing domain.
2. Create a user on your system that matches the user you use at Boeing.
3. Set the password to be the same as your Boeing user password.

Enabling authentication

To configure Client for Microsoft Networks to provide the proper information to Boeing domain controllers so that authentication can occur, follow these steps:

1. From the **Network** dialog box in the **Control Panel**, be sure that **Client For Microsoft Networks** is highlighted.
2. Click the **Properties** button.
3. In the **Properties** window, check the **Log onto Windows NT Domain** box.
4. In the text box, type your domain in the area that is provided.

   Example: NTMSEA1, NW
5. Under **Network Logon Options**, check the **Quick Logon** box.
6. Click **OK**.

   During the process of copying and updating Windows system files, you may be prompted for the Windows 98 Media. If you receive a **Version Conflicts Errors**, message, select **Yes** to keep the existing file.
7. Click **OK** to restart your system.

   At this point, your Win9x computer opens the Domain Login panel. If you actually connect to Boeing at this point, you will see the standard Boeing logon warning about using Boeing resources for business use only.
8. From the Windows desktop, from the **Start** button, select **Settings**.
9. In the **Control Panel** dialog box, select **Network**.
10. Select **Client for Microsoft Networks** from the list.
11. Click the **Properties** tab.
12. Uncheck the **Log on to Windows NT domain** check box.
13. Click **OK** to close the **Properties** tab.
14. Click **OK** to close the **Network** dialog box.

15. Click **OK** to restart your computer.

    You will not see the Domain Login panel at this point; however, you will be able to map network shares and use Outlook when you connect to Boeing.

Changing the workgroup value

Follow these steps:

1. In the Control Panel, select **Networks**, and then select the **Identifications** tab.
2. Type your Windows NT domain name in the **Workgroup** text box, and then click **OK**.