



# Software Product Description

---

**PRODUCT NAME:** AltaVista Tunnel Personal Edition Version 1.1

**SPD 56.14.01**

## DESCRIPTION

The AltaVista Tunnel allows you to use the public Internet as a secure, cost-effective extension or alternative to your private network.

There are two types of AltaVista Tunnel products offered: the Workgroup Edition and Personal Edition. The Personal Edition enables you to securely connect a client personal computer to a server in a private network via the Internet. In addition, the Workgroup Edition lets you connect two servers or two private networks to support confidential organization-to-organization communications.

Thus, there are two possible configurations: 1) Workgroup Edition to Workgroup Edition configuration and 2) a Workgroup Edition to Personal Edition configuration. Note that in both, one end point of the connection(s) must be a Workgroup Edition for tunnel authorization, authentication, and management.

This Software Product Description (SPD) covers the AltaVista Tunnel Personal Edition. See SPD 56.13.01 for the AltaVista Tunnel Workgroup Edition. The name AltaVista Tunnel, tunnel, or tunneling, will be used when referring to both the Personal and Workgroup Editions.

### Tunneling:

Tunneling in this application allows information to be securely passed between one computer and another over a public network as if the two were connected by a single physical wire. The process of sending information through tunnels is simple and straightforward. After authenticating the tunnel client and the tunnel server, information is encrypted by its sender, encapsulated into TCP/IP data packets, and sent across the Internet as unreadable and unrecognizable data. Once they reach their final destination, the packets are reconstituted, and decrypted into a readable form. Note that a system running the Workgroup or Personal Edition software

may be a client, while only a system running the Workgroup Edition may be a server (tunnel management station).

### Authentication and Encryption:

The AltaVista Tunnel employs RSA Public Key Cryptosystem (512 bit) for authentication and session key exchange, and RSA RC4 Symmetric Stream Cipher for bulk data encryption. Cryptographic identity and keys are tied to the user, leaving the IP address free to be dynamically assigned. Once the authenticated tunnel session is created, the tunnel server and tunnel client automatically switch from public key encryption to RC4-based secret key encryption to perform bulk data encryption and transmission. At 30-minute intervals, the tunnel client and server pass new session keys back and forth to decode transmitted data. During data packet transmission, each packet is integrity protected and authenticated by MD5.

In conformance with federal export regulations, the U.S. version of the AltaVista Tunnel employs a 128-bit RC4 key, while the international version supports a 40-bit RC4 key. When creating a multinational tunnel, automatic arbitration reconciles this key discrepancy transparently, enabling both the tunnel client and server to operate in common key mode.

### Firewall Independence:

Most Internet-connected companies and organizations employ firewalls to protect the information on their private networks from Internet invaders. Because the AltaVista Tunnel uses encryption and authentication to protect that information as it is transmitted across the Internet, it is a natural complement to any firewall. However, a firewall is not a prerequisite for the AltaVista Tunnel which delivers a highly flexible firewall-independent solution. The AltaVista Tunnel Workgroup Edition can run on a system with the AltaVista Firewall or it can run on a separate system behind a firewall that protects it from the Internet.

Primary Components of The AltaVista Tunnel Personal Edition for Windows 95 are:

- Microsoft[R] Windows 95 GUI-based tunnel setup and administration
- Windows 95 pseudo-adapter device driver
- Key Manager
- Online Help
- Native Windows 95 installation and tunnel management capabilities

Primary Components of The AltaVista Tunnel Personal Edition for Windows NT are:

- Microsoft[R] Windows NT GUI-based tunnel setup and administration
- Windows NT pseudo-adapter device driver
- Key Manager
- Online Help
- Native Windows NT installation and tunnel management capabilities

The Personal Edition is based on Microsoft's TCP/IP stack - an integral part of the Windows 95 and Windows NT[TM] operating systems

The Personal Edition Version 1.1 is compatible with the AltaVista Tunnel Workgroup Edition V1.0.

#### HARDWARE REQUIREMENTS

Processors Supported: 80486 or higher

Other Hardware Required:

In general, the AltaVista Tunnel Personal Edition provides enhanced security to TCP/IP network transmissions over the Internet. Thus, all the hardware (e.g. modems) necessary to implement a remote TCP/IP networking environment should already be in place. The tunnel requires no additional hardware or software besides the tunnel product itself.

For installation, the system must have a 3.5" floppy disk drive.

Disk Space Requirements: 5 MB free disk space

Memory Requirements:

Windows 95: 8 MB  
Windows NT: 16 MB

#### SOFTWARE REQUIREMENTS:

Operating System: Microsoft Windows 95, Windows NT 3.51, or Windows NT 4.0.

Other software requirements:

As stated above, the AltaVista Tunnel Personal Edition provides enhanced security to TCP/IP network transmissions over the Internet. Thus, all the software (e.g. dialup networking) necessary to implement a TCP/IP networking environment should already be in place.

#### GROWTH CONSIDERATIONS:

The minimum hardware/software requirements for any future version of this product may be different from the requirements for the current version.

#### DISTRIBUTION MEDIA

The Personal Edition is available on 3.5" floppy disk.

The printed documentation for this product may be ordered separately.

#### ORDERING INFORMATION

##### Windows 95

	<u>Win95 US/Can</u>	<u>Win95 International</u>
License, Software, Documentation	QB-4W2AA-SA	QB-4W3AA-SA
Documentation	QA-4W2AA-GZ	QA-4W3AA-GZ
Version upgrade	QB-4W2AA-MA	QB-4W3AA-MA

##### Windows NT

	<u>WinNT US/Can</u>	<u>WinNT International</u>
License, Software, Documentation	QB-4W2AB-SA	QB-4W3AB-SA
Documentation	QA-4W2AA-GZ	QA-4W3AA-GZ
Version upgrade	QB-4W2AB-MA	QB-4W3AB-MA

#### SOFTWARE LICENSING

This software is furnished under the licensing provisions of Digital Equipment Corporation's Standard Terms and Conditions. For more information about Digital's licensing terms and policies, contact your local Digital office. Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from Digital or an authorized sublicensor.

## SOFTWARE PRODUCT SERVICES

In addition to standard Software Product Services (SPS) remedial services, consulting services for planning, designing, and implementing a custom security system are also available. For more information, contact your local Digital office.

## SOFTWARE WARRANTY

Warranty for this software product is provided by Digital with the purchase of this software package.

This product is intended to assist customers in maintaining an appropriately secure systems environment when used in conjunction with customers' vigilant operational security practices. Digital does not guarantee or warrant that the use of this product will provide complete security protection for customers' systems.

© 1996 Digital Equipment Corporation. All rights reserved.

- ™ The DIGITAL Logo, AltaVista, AlphaServer, AlphaStation, DEC, DECnet, and Digital are trademarks of Digital Equipment Corporation.
- ™ Windows95 and Windows NT are trademarks of Microsoft Corporation.
- ™ Intel is a trademark of Intel Corporation.
- ™ RSA and RSA Public Key Cryptosystem are trademarks of RSA Data Security, Inc.
- ™ UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Ltd.

