

# Cisco VPN Client

## (Supports the Cisco Unified Client Framework)



### Product Overview

The Cisco VPN Client is software that enables customers to establish secure, end-to-end encrypted tunnels to Cisco remote access VPN devices that support the Cisco Unified Client framework. This thin design, IP Security (IPSec)-compliant implementation is available via Cisco.com for customers with SMARTnet™ support, and is included free of charge with the Cisco VPN 3000 Concentrator. The client can be preconfigured for mass deployments and initial logins require very little user intervention. VPN access policies and configurations are downloaded from the central gateway and pushed to the client when a connection is established, allowing simple deployment and management. The Cisco VPN Client provides support for Windows 95, 98, ME, NT 4.0, 2000, and XP.

The Cisco VPN Client is compatible with the following Cisco product (Cisco Unified Client framework support):

- Cisco VPN 3000 Concentrator Series version 3.0 and later
- Cisco PIX® Firewalls version 6.0 and later
- Cisco VPN 5000 Concentrator Series version 6.2 and later (future availability)
- Cisco IOS® Software-based platforms (future availability)

### Key Features and Benefits

#### Product Highlights

- Support for Windows 95, 98, ME, NT 4.0, 2000, and XP
- Intelligent peer availability detection
- Simple Certificate Enrollment Protocol (SCEP)
- Entrust Entelligence Support (Entrust Ready™)
- Data compression (LZS)
- Command-line options for connecting, disconnecting, and connection status
- Configuration file with option locking
- Support for Microsoft network login (all platforms)
- Domain Name System (DNS), Windows Internet Name Service (WINS), and IP address assignment
- Load balancing and backup server support
- Centrally controlled policies
- Software Update Notification
- Personal Firewall Enforcement for Zone Alarm/Pro and BlackIce

#### Unified Client Framework

The Cisco Unified Client Framework is an initiative that enables consistent VPN client operation between Service Providers and Enterprises and compatibility across various Cisco VPN platforms.

## Specifications

Specifications for the Cisco VPN Client

Description	Specification
Operating Systems	Windows 95, 98, ME, NT 4.0, 2000, and XP
Tunneling Protocols	IPSec Encapsulating Security Payload (ESP), Network Address Translation (NAT) transparent IPSec
Encryption/Authentication	IPSec (ESP) using Data Encryption Standard (DES)/Triple DES (3DES) (56/168-bit) with MD5 or SHA
Key Management	Internet Key Exchange (IKE) - Aggressive and Main Mode (Digital certificates) Diffie-Hellman (DH) Groups 1, 2, and 5 Perfect Forward Secrecy (PFS) Rekeying
Data Compression	Lempel-Ziv standard (LZS) compression
Digital Certificates	The supported enrollment mechanisms are Simple Certificate Enrollment Protocol (SCEP), Entrust Entelligence (Entrust Ready), and Certificates enrolled with Microsoft Internet Explorer. Supported Certificate Authorities (CAs) include: Entrust, GTE Cybertrust, Netscape, Baltimore, RSA Keon, Verisign, and Microsoft.
Authentication	Extended Authentication (XAUTH) Remote Authentication Dial-In User Service (RADIUS) with support for State/Reply-Message attributes (token cards) Security Dynamics (RSA SecurID Ready) Microsoft NT Domain authentication  X.509v3 Digital Certificates
Profile Management	Client can be easily distributed with preconfigured Profile Configuration Files (PCFs)
Policy Management	ISAKMP Configuration Method (Mode-Config) centrally controlled policies including DNS, WINS, IP Address, and Default Domain Name. Ability to save connection password, split tunneling control/networks, LAN access, and remote access load balancing
Personal Firewall Enforcement	Zone Alarm Pro, Zone Alarm, BlackIce Agent, BlackIce Defender

## Ordering Information

### Where to buy Cisco products

Visit [http://www.cisco.com/public/ordering\\_info.shtml](http://www.cisco.com/public/ordering_info.shtml)

### Product and Part Numbers

Available for customers with SMARTnet™ support at <http://www.cisco.com/public/sw-center/sw-vpn.shtml>.

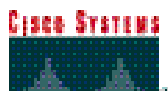
### Part Numbers for the Cisco VPN 3000 Client

Description	Part Number
Cisco VPN Client	CVPN-CLNT-31-K9=

## Documentation

For part numbers for product specific documentation, visit:

[www.cisco.com/univercd/cc/td/doc/pcat/swdo\\_\\_d1.htm](http://www.cisco.com/univercd/cc/td/doc/pcat/swdo__d1.htm)

**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
[www.cisco.com](http://www.cisco.com)  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The  
Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia  
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. PIX and SMARTnet are trademarks, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. All other brands, names, or trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0103R)