

Cisco VPN Client Version 3.1

(Unified Client Framework)



Frequently Asked Questions

Q. What is the Cisco VPN Client?

A. The Cisco VPN Client is software for use with Cisco Virtual Private Networking (VPN)-enabled products that support the Unified Client framework. It provides support for Windows 95, 98, ME, NT 4.0, 2000, and XP (Whistler).

Q. What is the Cisco Unified Client framework?

A. 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.

Q. How does the Cisco VPN Client benefit customers?

A. The Cisco VPN Client is simple to deploy and operate. It enables customers to establish secure, end-to-end encrypted tunnels to Unified Client framework-compliant Cisco remote access VPN devices. The thin design, IPSec implementation is available via www.cisco.com for use with any Cisco central site VPN product, and is included free of charge with the Cisco VPN 3000 Concentrator Series.

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, as well as high scalability.

Q. Which devices support the Unified Client framework? The following devices support the Unified Client framework:

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

Q. Can I use the Cisco VPN Client with a non-Cisco device?

A. No. The Cisco VPN Client is permitted only for use with Cisco devices.

Q. What operating systems does the Cisco VPN Client run on?

A. Windows 95, 98, ME, NT 4.0, 2000, and XP (Whistler).

Q. What type of encryption does the Cisco VPN Client support?

A. The Cisco VPN Client supports Data Encryption Standard (DES) and Triple DES (3DES). The central site VPN device controls the type of encryption used by the client.



- Q.** Which Diffie-Hellman (DH) Groups does the Cisco VPN Client support?
- A.** The client supports DH Groups 1, 2, and 5. Not all central site concentrators support Group 5.
- Q.** Does the client support Perfect Forward Secrecy (PFS)?
- A.** Yes.
- Q.** Does the Cisco VPN Client support Data Compression?
- A.** Yes.
- Q.** What type of user authentication can the Cisco VPN Client support?
- A.** The Cisco VPN Client supports up to two phases of authentication. For the first phase, the client can use a group name and preshared secret or a Digital Certificate. For the second phase, the client can support a username/password (RADIUS, NT, and so forth), token cards (Reply and State-Message) or Native SDI for central site devices with this support.
- Q.** Can the client work through a Port Address Translation (PAT) device?
- A.** Yes. The client can work with an IPsec ESP-aware PAT device. For non ESP-aware PAT devices, the client has IPsec over User Datagram Protocol (UDP) capabilities if permitted by the administrator. IPsec over UDP attaches a UDP header before the ESP (Protocol 50) data to allow IPsec to function in these environments.
- Q.** Can the client perform split tunneling?
- A.** Yes. However, the administrator of the VPN device must decide whether this is permitted. By default, a client must tunnel all data back to the central site concentrator.
- Q.** What information is “pushed” to the Cisco VPN Client?
- A.** The Cisco VPN Client uses push technology to set all non connection-entry policies. Policies are set at the central site and are pushed to the Cisco VPN Client. Items pushed to the Cisco VPN Client from the central site concentrator include:
- Domain Name System (DNS)
 - Windows Internet Naming System (WINS)
 - Split tunneling networks, LAN access permission
 - Default domain name
 - IP address
 - Ability to save a password for the VPN connection
- The client is free of charge when used with Cisco products for customers with SMARTnet™ contracts. The Client can be obtained from www.cisco.com in the SW CENTER/VPN SOFTWARE/CISCO VPN CLIENT area. For customers without SMARTnet, the client can be purchased for a US \$50 media charge (part no. CVPN-CLNT-31-K9=). The client ships on CD with the purchase of a Cisco VPN 3000 Concentrator.
- Q.** Where can I find the documentation and release notes for the Cisco VPN Client?
- A.** Documentation and release notes are at <http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/index.htm>.
- Q.** Can the Cisco VPN Client be preconfigured?
- A.** Yes. The Client can be preconfigured and distributed with Profile Configuration Files (PCFs). Refer to the Cisco VPN Client Administrator Guide for more details.
- Q.** Can the client be “branded”?
- A.** Yes. The Cisco VPN Client Administrator Guide describes how to create an OEM.INI file in order to change client icons and names.



Q. How does the client support certificates?

A. The client can support exportable certificates in the Microsoft store (Internet Explorer, and so forth), certificates that are enrolled in to the Cisco store (imported or Simple Certificate Enrollment Protocol [SCEP]), or the Entrust Entelligence client Entrust Ready™).

Q. Can the Cisco VPN Client connect to a Cisco VPN Concentrator with load balancing?

A. Yes. The Cisco VPN Client supports load balancing with a Cisco VPN 3000 Concentrator. When the client connects to a load balancing server, it is transparently redirected to the least loaded concentrator.

Q. Does the Cisco VPN Client support logging in to the Microsoft network (Drive Mappings or Logon Scripts)?

A. Yes. You must enable the “Log on to Microsoft Network” option in the client. For Windows 2000, XP and NT operating systems, use the “Start Before Logon” option. This enables the client to run either as a GINA or a Service. You log in to the VPN Client prior to logging in to your system in the normal way.

Q. Does the Cisco VPN Client work with my GINA?

A. You must determine if your GINA supports GINA chaining. If your GINA does not, follow the instructions in the Cisco VPN Client documentation on adding your GINA to the Incompatible GINA list. This causes the Client to use “fallback” mode and run as a service. As a service, the client is preempted by other system tasks and may take longer than usual for the client to start when the machine loads.

Q. Where can I find a list of known issues regarding the Cisco VPN Client?

A. Issues can be found in the Bug Navigator system at <http://cco.cisco.com/support/bugtools/bugtool.shtml>. Follow the path Cisco Software --> Cisco Security Components --> Cisco VPN Client

In addition, for each major release, the release notes are updated with a list of known issues at release time.

Q. Does the Cisco VPN Client have a command line?

A. Yes. You can connect, disconnect, and check connection status using the client's vpnclient.exe command line, as described in the documentation.

Q. Is the Cisco VPN Client compatible with PPPoE-based DSL?

A. Yes. The Client has been tested with NTS Enternet, Wind River WinPoET, and RASPPPoE.

Q. Is the Cisco VPN Client Entrust Ready™?

A. Yes, the VPN Client works in conjunction with the Entrust Entelligence client for certificate lifecycle management.

Q. Can I notify my users when a new software version is available?

A. Yes, client version 3.1 or greater can be notified of software updates.

Q. Can I enforce the use of a Personal Firewall when connecting with the VPN client?

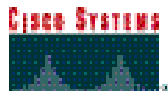
A. Yes, you can enforce the use of Zone Alarm PRO, Zone Alarm, BlackIce Agent or Defender when using VPN.

Q. Can I provide my users access to only LAN addresses while tunneled in?

A. Yes, v3.1 provides the ability to configure LAN permission access for tunneled users.

Q. Does the Entrust Entelligence client work in conjunction with the Cisco VPN Client?

A. Yes, client v3.1 and greater are Entrust Ready™ and support the Entrust Entelligence client.

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
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
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
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
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.

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, SMARTnet, and Unity 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)