

Cisco AnyConnect VPN Client

Product Overview

Cisco® AnyConnect VPN Client provides remote users with full network access to virtually any corporate application. It automatically adapts its tunneling protocol to the most efficient method based on network constraints. Cisco AnyConnect VPN Client is the first VPN product to use the Datagram Transport Layer Security (DTLS) protocol to provide an optimized connection for latency-sensitive traffic, such as voice over IP (VoIP) traffic or TCP-based application access.

Features and Benefits

Table 1 lists the features and benefits of Cisco AnyConnect VPN Client.

Table 1. Features and Benefits

Feature	Benefit
Optimized Network Access	<ul style="list-style-type: none"> Automatically adapts its tunneling to the most efficient method possible based on network constraints. Uses DTLS to provide an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access. Uses HTTP over SSL to ensure availability of network connectivity through locked-down environments, including those using Web proxy servers.
Mobility Friendly	<ul style="list-style-type: none"> Designed for mobile users. Can be configured so that the VPN connection remains established during IP address changes, loss of connectivity, and/or hibernation or standby. Trusted Network detection enables the VPN connection to automatically disconnect when an end user is in the office and connect when a user is at a remote location.
Encryption	<ul style="list-style-type: none"> Supports strong encryption, including AES-256 and 3DES-168. (The headend device must have a strong-crypto license enabled.)
Broad Operating System Support	<ul style="list-style-type: none"> XP 32-bit (x86) and 64-bit (x64) Windows Vista 32-bit (x86) and 64-bit (x64), including Service Pack 1 and 2 (SP1/SP2) Windows 7 32-bit (x86) and 64-bit (x64) Mac OS X 10.5 and 10.6.x Linux Intel (2.6.x kernel) <i>Windows 2000 & Mac OS X 10.4 are no longer validated / supported as of AnyConnect 2.4.</i> <p>Cisco AnyConnect Mobile (requires optional AnyConnect Mobile license)</p> <ul style="list-style-type: none"> Windows Mobile 5.0, 6.0, and 6.1 (Professional and Classic)
Wide Range of Deployment and Connection Options	<p>Deployment options:</p> <ul style="list-style-type: none"> Pre-deployment, including Microsoft Installer Automatic headend deployment (administrative rights are required for initial installation) via ActiveX (Windows only) and Java <p>Connection modes:</p> <ul style="list-style-type: none"> Standalone via system icon Browser-initiated (Weblaunch) Clientless portal initiated Command-line interface (CLI) initiated API initiated
Wide Range of Authentication Options	<ul style="list-style-type: none"> RADIUS RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM) RADIUS one-time password (OTP) support (state/reply message attributes) RSA SecurID (including SoftID integration) Active Directory/Kerberos Embedded Certificate Authority (CA) Digital Certificate/Smartcard (including Machine Certificate support) – auto or user selected

Feature	Benefit
	<ul style="list-style-type: none"> Lightweight Directory Access Protocol (LDAP) with Password Expiry and Aging Generic LDAP support Combined certificate and username/password multifactor authentication (double authentication)
Ease of Client Administration	<ul style="list-style-type: none"> Allows an administrator to automatically distribute software and policy updates from the headend security appliance, thereby eliminating administration associated with VPN client software updates. Administrators can determine which capabilities to make available for end user configuration. Administrators can trigger an endpoint script at connect/disconnect time when domain login scripts cannot be utilized.
Consistent User Experience	<ul style="list-style-type: none"> Full tunnel client mode supports remote-access users requiring a consistent LAN-like user experience. Multiple delivery methods and small download size help ensure broad compatibility and rapid download of the Cisco AnyConnect VPN Client.
Pre-connection Posture Assessment (Premium license required)	<ul style="list-style-type: none"> In conjunction with Cisco Secure Desktop, host integrity verification checking seeks to detect the presence of antivirus software, personal firewall software, and Windows service packs on the endpoint system prior to granting network access. Administrators also have the option of defining custom posture checks based on the presence of running processes. Cisco Secure Desktop can detect the presence of a watermark on a remote system. The watermark can be used to identify assets that are corporate-owned and provide differentiated access as a result. The watermark checking capability includes system registry values, file existence matching a required CRC32 checksum, IP address range matching, and certificate issued by/to matching. An advanced endpoint assessment option is available to automate the process of repairing out-of-compliance applications.
Advanced IP Network Connectivity	<ul style="list-style-type: none"> Access to internal IPv4 and IPv6 network resources Centralized split tunneling control for optimized network access IP address assignment mechanisms: <ul style="list-style-type: none"> Static Internal pool Dynamic Host Configuration Protocol (DHCP) RADIUS/LDAP

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
<http://www.openssl.org>.

Platform Compatibility

The Cisco AnyConnect VPN Client is compatible with all [Cisco ASA 5500 Security Appliance](#) models (running Cisco ASA Software Release 8.0.3 and later) and various [Cisco IOS® Software-based routers](#).

The Cisco AnyConnect VPN Client is not compatible with Cisco PIX® security appliances or Cisco VPN 3000 Series concentrators.

Additional compatibility information may be found at <http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html>.

Cisco AnyConnect Licensing Options

Table 2 lists licensing options for Cisco AnyConnect.

Table 2. Cisco AnyConnect Licensing Options

License Option	Description
Platform Licenses	
AnyConnect Essentials	<ul style="list-style-type: none"> Highly secure, remote-access connectivity. Single license per device model. Full Tunneling access to Enterprise applications.
AnyConnect Premium	<ul style="list-style-type: none"> Includes clientless SSL VPN and Cisco Secure Desktop capabilities (including Host Scan). Optionally provides Full Tunneling access to Enterprise applications. License is based on number of simultaneous users, and is available as a single device or shared license.

License Option	Description
Optional Feature Licenses	
AnyConnect Mobile	<ul style="list-style-type: none"> Enables Mobile OS platform compatibility. Required per-device, in addition to Essentials or Premium licenses.
Advanced Endpoint Assessment	<ul style="list-style-type: none"> Enables advanced endpoint assessment capabilities (such as auto-remediation). Required per-device, in addition to Premium licenses. (not available with AnyConnect Essentials).
FIPS 140-2 Level1 Validation	<ul style="list-style-type: none"> ASA license which allows use of a FIPS validated version of AnyConnect.

Warranty Information

Find warranty information at the [Cisco Product Warranties](#) page.

Ordering Information

To place an order, visit the [Cisco Ordering Home Page](#). To download software, visit the [Cisco Software Center](#) (a Cisco SMARTnet[®] contract is required).

Any Cisco SMARTnet customer may download the latest Cisco AnyConnect VPN Client software from Cisco.com, but a headend license is required in order to support more than two simultaneous connections. Please refer to the AnyConnect Licensing Options section above for additional information on the available options.

For a list of available licensing options that enable connectivity with AnyConnect, please refer to the Cisco Secure Remote Access: VPN Licensing Overview.

For More Information

Cisco AnyConnect VPN Client documentation

http://www.cisco.com/en/US/products/ps8411/tsd_products_support_series_home.html

Cisco ASA 5500 Series Adaptive Security Appliances <http://www.cisco.com/go/asa>

Cisco ASA 5500 Series Adaptive Security Appliance Licensing Information:

http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems (Europe) B.V.
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, CCSP, Cisco IaaS, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nexus Connect, Cisco Prime, Cisco ScanSense, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Halo for Cisco, Halo Mini, Hiperlane (Design), Hip Ultra, Hip Video, Hip Video (Design), Incident Broadband, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play and Learn, Cisco Capital, Cisco Capital (Design), Cisco Financial (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks, and Access Register, Almond, All built, AsyncOS, Bringing the Meeting to You, Catalyst, CCDA, CCDE, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumina, Cisco Nexus, Cisco Prime, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, Fireport, IronSwitch, Event Center, Explorer, Follow Me Browsing, GainMedia, IYX, OS, iPhone, IronPort, the IronPort logo, iLearn Link, LightStream, Linksys, MeetingPlace, MeetingPlace Online Sound, MGX, Network, Networking Academy, PCNow, PX, PowerKEY, PowerPanel, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROBA, ScanSense, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910)