Cisco AnyConnect Secure Mobility Client for Mobile Platforms

Product Overview

The Cisco AnyConnect® Secure Mobility Client for Mobile Platforms enables enterprises to enhance employee productivity by securing their employees' smartphones and tablets. The client is available for Apple iOS and Android 4.0 and later (Ice Cream Sandwich and Jelly Bean) operating systems, as well as a growing number of Android devices from HTC, Lenovo, Motorola, and Samsung. The client may also be used on Android platforms where root access is available.

The Cisco AnyConnect Secure Mobility Client for Mobile Platforms provides reliable and easy-to-deploy encrypted network connectivity from smartphones and tablets by delivering persistent corporate access for employees on the go. Whether an employee is accessing business email, a virtual desktop session, or other enterprise applications, the Cisco AnyConnect client offers an easy-to-use interface to business-critical information. The client uses Datagram Transport Layer Security (DTLS) and Transmission Control Protocol (TCP) to provide business-critical applications, including latency-sensitive applications such as voice-over-IP (VoIP), with encrypted access to corporate resources.

Figure 1 shows a sample Cisco AnyConnect VPN configuration on Apple iOS.

Figure 1. Cisco AnyConnect Icon and Sample VPN Configuration on Apple iOS

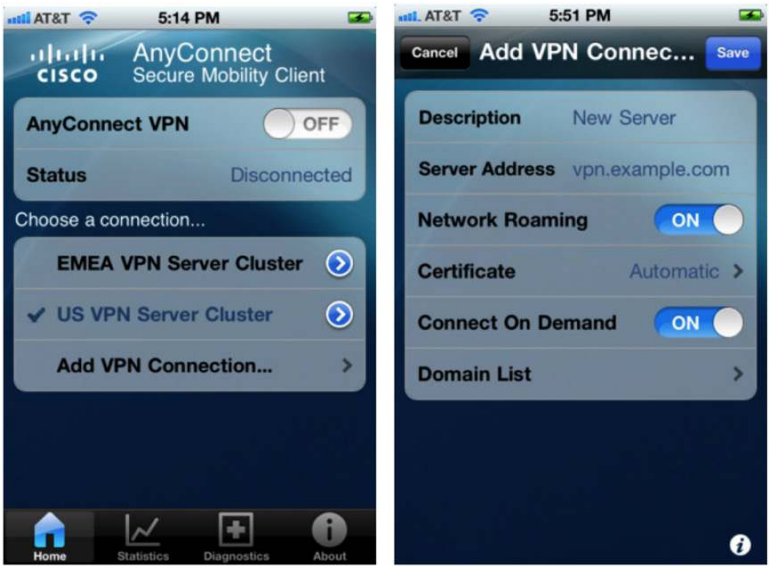
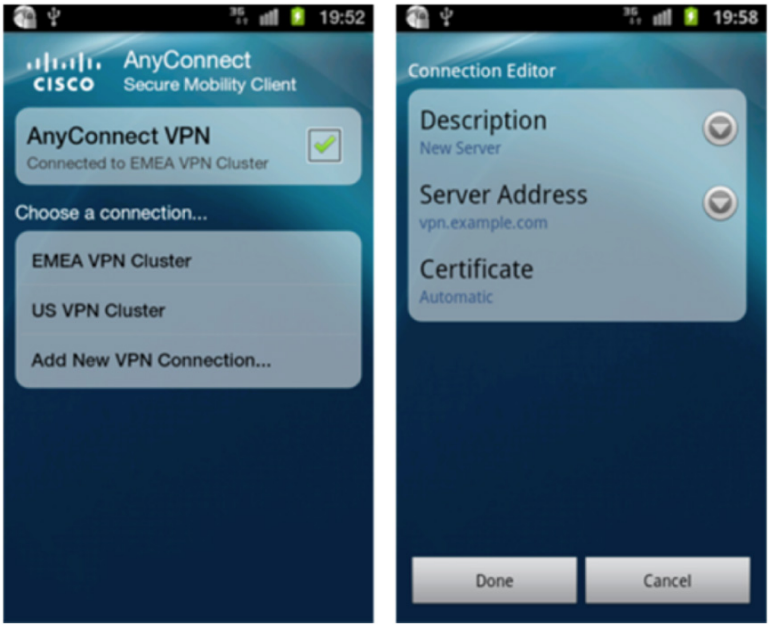


Figure 2 shows a sample Cisco AnyConnect VPN configuration on Google Android.

Figure 2. Cisco AnyConnect Icon and Sample VPN Configuration on Google Android



Features and Benefits

Table 1 lists the features and benefits of the Cisco AnyConnect Secure Mobility Client for Mobile Platforms.

Table 1. Features and Benefits

Feature	Benefit
Compatibility	**Apple iOS:** Apple iPhone® 3G, 3GS, 4, 4S, and 5; Apple iPod touch® (second, third, and fourth generations); and Apple iPad™, iPad™ 2, the iPad™ HD, and the iPad™ mini **Google Android:** tuntap (tun.ko) support is required • Generic Android VPN Framework (4.0+/Ice Cream Sandwich and Jelly Bean) • HTC: For the latest list of supported devices, see: http://www.htcpro.com/enterprise/VPN • Lenovo • Motorola • Samsung • Generic Google Android with root privileges (2.3+/Gingerbread, Honeycomb, ICS, and Jelly Bean)[1] ◦ Please note that additional supported devices are frequently added. ◦ For a current list of supported Android devices, please see the AnyConnect for Android Release Notes or the Google Play description for the appropriate image. Certain platform restrictions apply, including requirements for minimum device software versions. ◦ Certain features may not be available on all platforms due to OS restrictions. Please read the Release Notes for specific feature availability details.
Software Access	**Available on application marketplaces:** • **Apple:** iTunes App Store℠: Apple iOS 4.1+ devices • **Google Play:** Multiple Cisco AnyConnect images are available. It is important to select the correct image for your device.

[1] Requires root access, tuntap, and iptables. Root access is not available by default in Android without modification of the OS.

Feature	Benefit
Optimized Network Access	• Automatically adapts its tunneling to the most efficient method possible based on network constraints • Uses DTLS to provide an optimized connection for TCP-based application access and latency-sensitive traffic, such as VoIP traffic • Uses TLS (HTTP over TLS/SSL) to ensure availability of network connectivity through locked-down environments • IPsec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPsec (new in Cisco AnyConnect 3.0 for Mobile Platforms) • Compatible with Cisco ASA VPN load balancing
Mobility-Friendly	• Resumes seamlessly after IP address change, loss of connectivity, or device standby • Trusted Network Detection (TND) pauses or disconnects VPN sessions when connected to corporate trusted networks ◦ *Due to platforms limitations, TND is not available for generic Android or Apple iOS.*
Battery-Friendly	• Compatible with Apple iOS device sleep operation
Encryption	• Supports strong encryption, including AES-256 and 3DES-168 (The security gateway device must have a strong-crypto license enabled.) • Next-generation encryption, including NSA Suite B algorithms, ESPv3 with IKEv2, 4096-bit RSA keys, Diffie-Hellman group 24, and enhanced SHA2 (SHA-256 & SHA-384). (Only available for IPsec IKEv2 connections. A Premium ASA license is required.)
Authentication Options	• RADIUS • RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM) • RADIUS one-time password (OTP) support (state/reply message attributes) • RSA SecurID • Active Directory/Kerberos • Digital certificate (compatible with Cisco AnyConnect integrated SCEP for credential deployment) • Generic Lightweight Directory Access Protocol (LDAP) support • LDAP with Password Expiry and Aging • Combined certificate and username/password multifactor authentication (double authentication)
Consistent User Experience	• Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience
Centralized Policy Control and Management	• Policies can be preconfigured or configured locally, and can be automatically updated from the VPN security gateway • Universal Resource Indicator (URI) handler for Cisco AnyConnect eases deployments through URLs embedded in webpages or applications • Certificates can be viewed and managed locally
Advanced IP Network Connectivity	• Administrator-controlled split- or all-tunneling network access policy • Access control policy IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP
Localization	In addition to English, the following language translations are included: • Canadian French (fr-ca) • Czech (cs-cz) • German (de-de) • Japanese (ja-jp) • Korean (ko-kr) • Latin American Spanish (es-co) • Polish (pl-pl) • Simplified Chinese (zh-cn)
Diagnostics	• On-device statistics and logging information • View logs on device • Logs can be easily emailed to Cisco or an administrator for analysis

Platform Compatibility

The Cisco AnyConnect Secure Mobility Client is compatible with all Cisco ASA 5500 Series Adaptive Security Appliance models running Cisco ASA Software Release 8.0(4) and later.

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

Cisco AnyConnect Secure Mobility Client Licensing Options

Table 2 lists licensing options for the Cisco AnyConnect Secure Mobility Client.

Table 2. Cisco AnyConnect Secure Mobility Client Licensing Options

License Requirements *(each license below is required)*	Description
Cisco ASA Platform License	**Cisco AnyConnect Essentials**[2] (P/N: (L-ASA-AC-E-55**=) 5, 10, 20, 40, 50, 80, 85) • Highly secure remote-access connectivity • Single license per ASA device model (not a per-user license); enables maximum simultaneous users on platform • Full-tunneling access to enterprise applications
	Cisco AnyConnect Premium[3] (P/N: (L-ASA-SSL-***=) 10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10,000) • Also provides support for clientless SSL VPN and capabilities available on desktop Cisco AnyConnect platforms, including Cisco HostScan and Always-On VPN connectivity • License is based on number of simultaneous users and is available as a single device or shared license
Cisco AnyConnect Mobile License[5] **P/N: (L-ASA-AC-M-55*=)** **5, 10, 20, 40, 50, 80, 85**	• Enables mobile OS platform compatibility • Required (single license) per security gateway device, in addition to Essentials or Premium licenses • No per-user license required

Electronic License Delivery

Most licenses are available for electronic delivery; this significantly speeds up license fulfillment time. To order a license electronically, be sure to order part number(s) that begin with "L-." If you have any questions regarding licensing or would like evaluation licenses, please contact ac-mobile-license-request (AT) cisco.com and include a copy of the results of the “show version” command from your Cisco ASA appliance.

If you already have an Essentials or Premium ASA license, you may use the automated license request tool at https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=717.

Warranty Information

Find warranty information at the Cisco Product Warranties page.

[2] Replace ** with the appropriate last two digits of the ASA model number.
[3] Replace *** with the number of total number of license seats.

Ordering Information

To place an order for a security gateway license, visit the Cisco Ordering Home Page. See Table 1 for compatible platforms and software access information.

Security gateway licenses are required to enable connectivity. Please refer to the Cisco AnyConnect Licensing Options section for additional information on the available options. For a list of available licensing options that enable connectivity with the Cisco AnyConnect Secure Mobility Client, please refer to the Cisco AnyConnect Secure Mobility Client Features, Licenses, and OSs webpage.

Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

This product includes cryptographic software written by Eric Young.

This product includes software written by Tim Hudson.

This product incorporates the libcurl HTTP library: Copyright © 1996-2006, Daniel Stenberg.

For More Information

Cisco AnyConnect Secure Mobility Client homepage:
http://www.cisco.com/go/anyconnect.

Cisco AnyConnect 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.

Cisco AnyConnect License Agreement and Privacy Policy:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/eula-seula-privacy/AnyConnect_Supplemental_End_User_License_Agreement.htm.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV 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.

Printed in USA C78-678242-02 05/13