Cisco AnyConnect Secure Mobility Client for Mobile Platforms

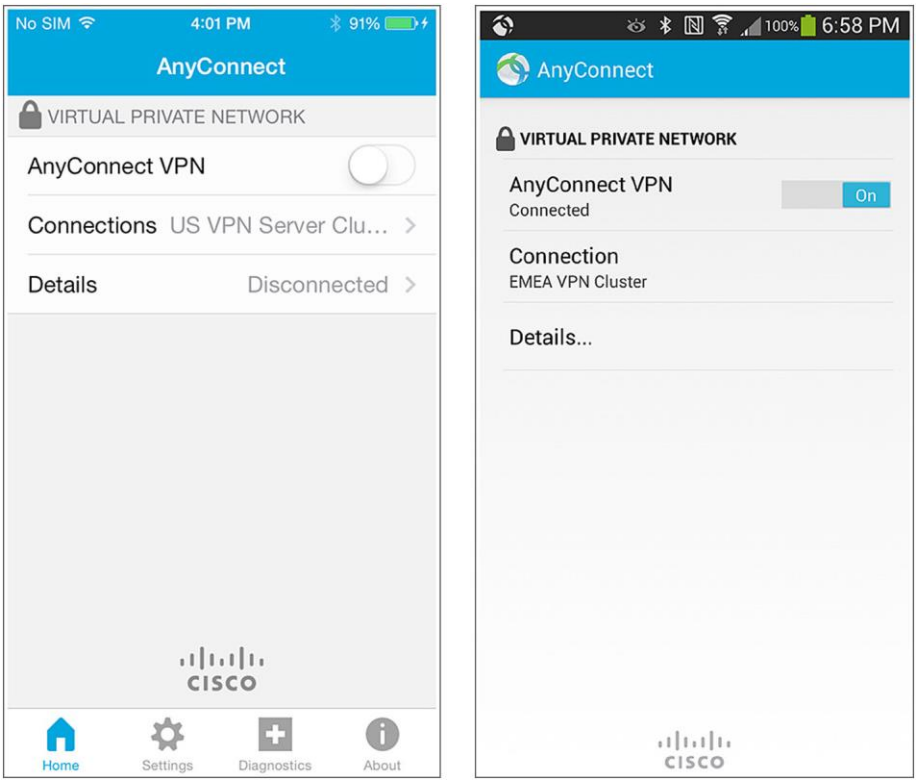
Product Overview

You can now secure employee smartphones and tablets with the Cisco AnyConnect® Secure Mobility Client for Mobile Platforms, available for Apple iOS 6.0+, Android 4.0+, and select Amazon Kindle and Fire Phone devices.

The Cisco AnyConnect Secure Mobility Client for Mobile Platforms provides reliable and easy-to-deploy encrypted network connectivity from smartphones and tablets along with 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 is an easy-to-use interface to business-critical information. The client uses Datagram Transport Layer Security (DTLS), IPsec (IKEv2), and TLS (HTTP over TLS/SSL) to provide business-critical applications, including latency-sensitive applications such as voice over IP (VoIP), with encrypted access to corporate resources. Cisco AnyConnect 4.0 supports per-app VPN functions for iOS 7.0+.

Figure 1 shows a sample Cisco AnyConnect user interface on Apple iOS and Android devices.

Figure 1. Cisco AnyConnect User Interface on Apple iOS and Android Devices



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
Software access and compatibility	**Available on application marketplaces** • **Apple App Store:** Apple iOS 6.0+ devices • **Google Play:** Android 4.0+ devices Note that there are multiple Cisco AnyConnect images available, so it is important that you select the correct image for your device. See the Android release notes for specific requirements • **Amazon Appstore:** Supported on select Kindle and Fire Phone devices
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 help ensure availability of network connectivity through locked-down environments • IPsec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require the use of IPsec (requires ASA 8.4+) • Compatible with Cisco ASA VPN load balancing
Mobility-friendly	• Resumes transparently 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 **Note that 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 and SHA-384). (Available only for IPsec IKEv2 connections. AnyConnect APEX license is required.)
Authentication options	• RADIUS • RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM) • RADIUS onetime 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 • Per-app VPN policy for iOS 7+ (New in Cisco AnyConnect 4.0: Requires Cisco ASA 5500-X with OS 9.3+ and AnyConnect 4.0 licenses) • Access control policy IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/LDAP

Feature	Benefit
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-X Series Adaptive Security Appliance models running Cisco ASA Software Release 8.0(4) and later. Use of current ASA Software releases is advised.

Certain features require later Cisco ASA Software releases or ASA 5500-X models.

Cisco supports Cisco AnyConnect VPN access to Cisco IOS® Release 15.1(2)T and later functioning as the highly secure gateway with certain feature limitations. Please see Features Not Supported on the Cisco IOS SSL VPN for details.

Refer to http://www.cisco.com/go/fn for additional Cisco IOS feature support information.

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

Licensing and ordering: The Cisco AnyConnect Ordering Guide covers licensing for AnyConnect and clientless SSL VPN usage.
http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf

Additional Cisco ASA 5500-X licensing documentation may be found at:
http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html.

For More Information

- Cisco AnyConnect Secure Mobility Client homepage:
  http://www.cisco.com/go/anyconnect
- Cisco AnyConnect documentation:
  http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
- Cisco ASA 5500-X Series Next-Generation Firewalls:
  http://www.cisco.com/go/asa
- 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

Acknowledgments

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.

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 C78-527494-07 12/14