

# Cisco AnyConnect Secure Mobility Client for Mobile Platforms

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.

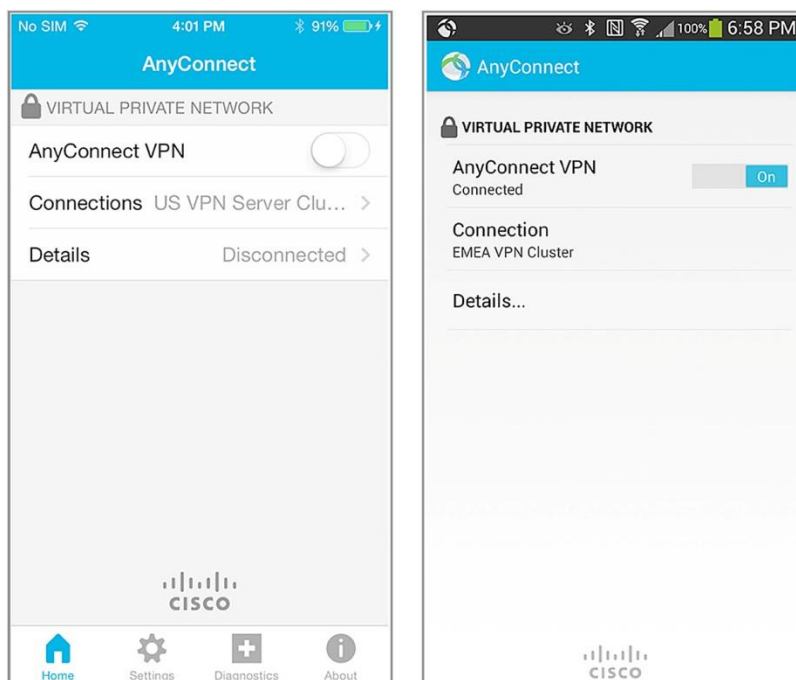
## Product Overview

You can now safeguard employee smartphones and tablets with the Cisco AnyConnect Secure Mobility Client for Mobile Platforms, available for Apple iOS, Android, Windows Phone 8.1 and later, BlackBerry 10.3.2 and later, select Amazon Kindle and Fire Phone devices, and Google Chrome OS (early preview version).

Whether an employee is accessing business email, a virtual desktop session, or other enterprise applications, the AnyConnect client is an easy-to-use interface for business-critical information. The client uses Datagram Transport Layer Security (DTLS), IP Security Internet Key Exchange version 2 (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. AnyConnect 4.x supports per-app VPN functions for iOS 8.3 and later.

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

**Figure 1.** User Interface on Apple iOS and Android Devices



## Features and Benefits

Table 1 lists the features and benefits of the AnyConnect Secure Mobility Client for Mobile Platforms. Feature availability varies by platform. Please see the [platform release notes](#) and [documentation](#) for specific supported feature details for a particular operating system.

**Table 1.** Features and Benefits

Feature	Benefit
<b>Software access and compatibility</b>	<p><b>Available on application marketplaces:</b></p> <ul style="list-style-type: none"> <li>• <b>Apple App Store:</b> for Apple iOS 6.0 and later</li> <li>• <b>Google Play:</b> for Android 4.0 and later</li> </ul> <p>Note that there are multiple AnyConnect images available, so it is important that you select the correct image for your device. See the Android release notes for specific requirements.</p> <ul style="list-style-type: none"> <li>• <b>Windows Store:</b> for Windows Phone 8.1 Update 1 and later</li> <li>• <b>BlackBerry App World:</b> for BlackBerry 10.3.2 and later</li> <li>• <b>Google Chrome OS:</b> for Chrome OS 43 and later (early preview)</li> <li>• <b>Amazon Appstore:</b> for select Kindle and Fire Phone devices</li> </ul>
<b>Optimized network access</b>	<ul style="list-style-type: none"> <li>• Automatically adapts its tunneling to the most efficient method possible based on network constraints</li> <li>• Uses DTLS to provide an optimized connection for TCP-based application access and latency-sensitive traffic, such as VoIP traffic</li> <li>• Uses TLS (HTTP over TLS/SSL) to help ensure availability of network connectivity through locked-down environments</li> <li>• IPsec IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require the use of IPsec (requires Cisco Adaptive Security Appliance 8.4 or later)</li> <li>• Compatible with ASA VPN load balancing</li> </ul>
<b>Network Visibility</b>	<ul style="list-style-type: none"> <li>• Mobile visibility from the Network Visibility module</li> <li>• Capture endpoint flows with rich user, endpoint, application, location and destination context</li> <li>• Available on select Samsung mobile devices</li> </ul>
<b>Mobility friendly</b>	<ul style="list-style-type: none"> <li>• Resumes transparently after IP address change, loss of connectivity, or device standby</li> </ul>
<b>Battery friendly</b>	<ul style="list-style-type: none"> <li>• Compatible with device sleep operation</li> </ul>
<b>Encryption</b>	<ul style="list-style-type: none"> <li>• Supports strong encryption, including AES-256 and 3DES-168. (The security gateway device must have a strong-crypto license enabled.)</li> <li>• 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. An AnyConnect Apex license is required.</li> </ul>
<b>Authentication options</b>	<ul style="list-style-type: none"> <li>• RADIUS</li> <li>• RADIUS with Password Expiry (MSCHAPv2) to NT LAN Manager (NTLM)</li> <li>• RADIUS onetime password (OTP) support (state and reply message attributes)</li> <li>• RSA SecurID</li> <li>• Active Directory or Kerberos</li> <li>• Digital certificate (compatible with AnyConnect integrated Simple Certificate Enrollment Protocol, or SCEP, for credential deployment)</li> <li>• Generic Lightweight Directory Access Protocol (LDAP) support</li> <li>• LDAP with password expiry and aging</li> <li>• Combined certificate and username-password multifactor authentication (double authentication)</li> <li>• SAML support for iOS and Android</li> </ul>
<b>Consistent user experience</b>	<ul style="list-style-type: none"> <li>• Full-tunnel client mode supports remote-access users requiring a consistent LAN-like user experience</li> </ul>
<b>Centralized policy control and management</b>	<ul style="list-style-type: none"> <li>• Policies can be preconfigured or configured locally and can be automatically updated from the VPN security gateway</li> <li>• Universal Resource Indicator (URI) handler for AnyConnect eases deployments through URLs embedded in webpages or applications</li> <li>• Certificates can be viewed and managed locally</li> </ul>

Feature	Benefit
<b>Advanced IP network connectivity</b>	<ul style="list-style-type: none"> <li>• Administrator-controlled split- or all-tunneling network access policy</li> <li>• Per-app VPN policy for iOS 8.3 and later (requires Cisco ASA 5500-X with OS 9.3.2 or later and AnyConnect Plus or Apex license)</li> <li>• Access control policy</li> </ul> <p><b>IP address assignment mechanisms:</b></p> <ul style="list-style-type: none"> <li>• Static</li> <li>• Internal pool</li> <li>• Dynamic Host Configuration Protocol (DHCP)</li> <li>• RADIUS/LDAP</li> </ul>
<b>Localization</b>	<p><b>In addition to English, the following language translations are included:</b></p> <ul style="list-style-type: none"> <li>• Canadian French (fr-ca)</li> <li>• Czech (cs-cz)</li> <li>• German (de-de)</li> <li>• Japanese (ja-jp)</li> <li>• Korean (ko-kr)</li> <li>• Latin American Spanish (es-co)</li> <li>• Polish (pl-pl)</li> <li>• Simplified Chinese (zh-cn)</li> </ul>
<b>Diagnostics</b>	<ul style="list-style-type: none"> <li>• On-device statistics and logging information are available.</li> <li>• Logs can be viewed on device.</li> <li>• Logs can be easily emailed to Cisco or an administrator for analysis.</li> </ul>

## Platform Compatibility

The AnyConnect Secure Mobility Client is compatible with all [Cisco ASA 5500-X Series Next-Generation Firewalls and Cisco 5500 Series Enterprise Firewall Edition](#) models running ASA Software Release 8.0(4) or later. Use of current ASA software releases is advised.

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

Cisco supports AnyConnect VPN access to Cisco IOS® Release 15.1(2)T or later functioning as the highly secure gateway with certain feature limitations. Refer to <http://www.cisco.com/go/fn> for additional Cisco IOS Software feature support information.

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

## Licensing Options and Ordering Information

The AnyConnect Ordering Guide covers licensing and ordering information for AnyConnect, clientless SSL VPN, and third-party IKEv2 remote-access VPN usage. AnyConnect Plus or Apex licenses are required for full platform and feature support. Customers with existing Essentials or Premium and Mobile licenses are permitted to use the iOS and Android versions (excluding per-app VPN functions) until April 30, 2016. All other mobile platforms require Plus or Apex licenses. AnyConnect VPN connectivity to non-Cisco headend equipment is never permitted.

For more information, see the ordering guide at <http://www.cisco.com/c/dam/en/us/products/security/anyconnect-og.pdf>.

---

## Cisco Capital

### Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more.](#)

### 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/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect40/license/end\\_user/AnyConnect-SEULA-v4-x.html](http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-SEULA-v4-x.html).

### 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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1110R)