CISCO
SECURE

Data sheet
Cisco public

Cisco AnyConnect Secure Mobility Client

October 2020

Contents

Easy to use. Highly secure. This is why the Cisco AnyConnect® Secure Mobility Client is so popular around the world. And customers know that with each new release, AnyConnect consistently raises the bar for remote-access across a broad set of desktop and mobile devices.

Product Overview

As mobile workers roam to different locations, an always-on intelligent VPN helps AnyConnect client devices to automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method. This may include voice over IP (VoIP) traffic, TCP-based application access, or Datagram Transport Layer Security (DTLS) protocol for latency-sensitive traffic. Tunneling support is also available for IP Security Internet Key Exchange version 2 (IPsec IKEv2). Select application VPN access may be enforced on Apple iOS, Google Android (5.0 and later), and Samsung Knox with the per-app VPN feature in Release 4.x.

AnyConnect 4.x supports robust, unified endpoint compliance. It protects the integrity of the corporate network by restricting VPN access terminating at the Cisco Adaptive Security Appliance based on an endpoint's security posture. Endpoint posture assessment and remediation across wired and wireless environments validate the status of various antivirus, personal firewall, and antispyware products. Out-of-compliance endpoint enforcement provides options to remediate and implement additional system checks before access is granted.

The AnyConnect Secure Mobility solution has built-in web security, malware threat defense, phishing protection, and command and control callback blocking all on top of remote access for a comprehensive and secure enterprise mobility solution. For web security, choose either the premises-based Cisco Secure Web Appliance or cloud-based Cisco Cloud Web Security for reliable and highly secure employee access to corporate resources and cloud protection services. For protection when the VPN is off, Cisco Umbrella Roaming is a cloud-delivered security service that protects devices anywhere against malware, phishing, and command and control callbacks.

With the Network Visibility Module on Windows, macOS, Linux, and Samsung mobile devices, administrators can monitor endpoint application usage to uncover potential behavior anomalies and to make more informed network-design decisions. Usage data can be shared with NetFlow analysis tools such as Cisco Secure Network Analytics.

With its Cisco Secure Endpoint Enabler, AnyConnect can assist with the deployment of Cisco Secure Endpoint. This capability significantly expands endpoint threat protection to VPN-enabled endpoints or wherever AnyConnect services are in use (for 802.1X network access, posture, etc.). And it further reduces the potential of an attack from enterprise-connected hosts. Secure Endpoint is licensed separately from AnyConnect.

In addition to industry-leading VPN capabilities, the AnyConnect mobility client helps enable IEEE 802.1X capability, providing a single authentication framework to manage user and device identity as well as the network- access protocols required to move smoothly from wired to wireless networks.

Consistent with its VPN functionality, the solution supports IEEE 802.1AE (MACsec) for data confidentiality, data integrity, and data-origin authentication on wired networks safeguarding communication between trusted components of the network.

Figure 1 shows a VPN configuration on Microsoft Windows.

Figure 1. Icon and Sample VPN Configuration on Microsoft Windows

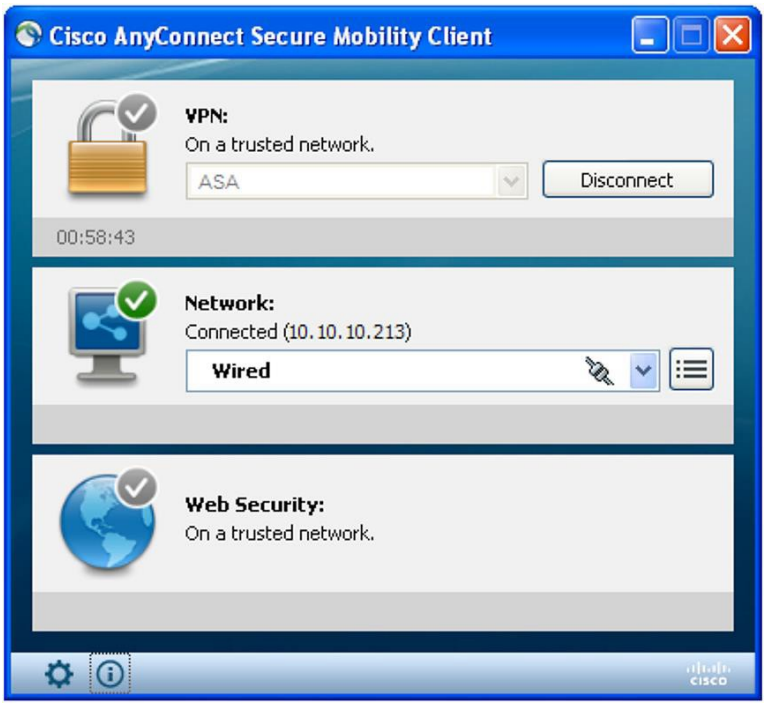
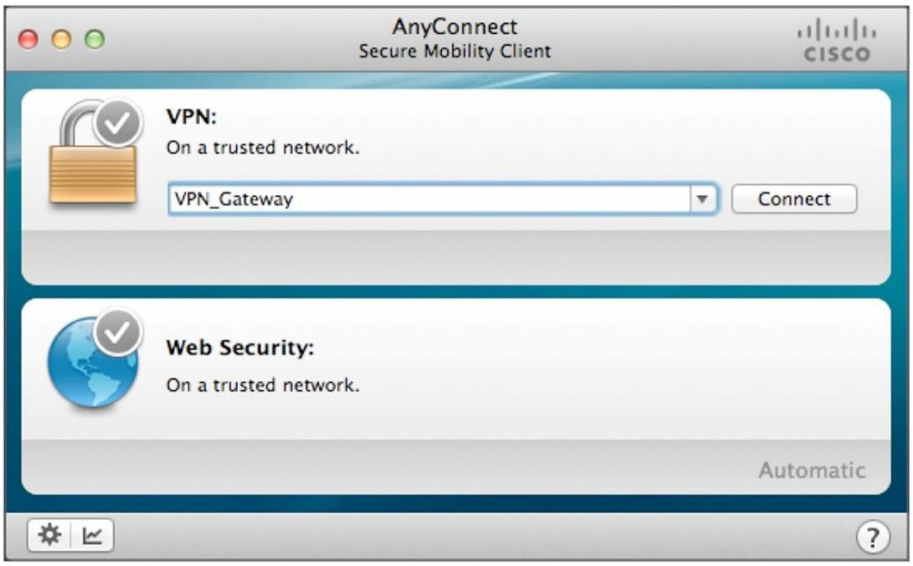


Figure 2 shows a VPN configuration on Apple OS X.

Figure 2. Icon and Sample VPN Configuration on Apple OS X

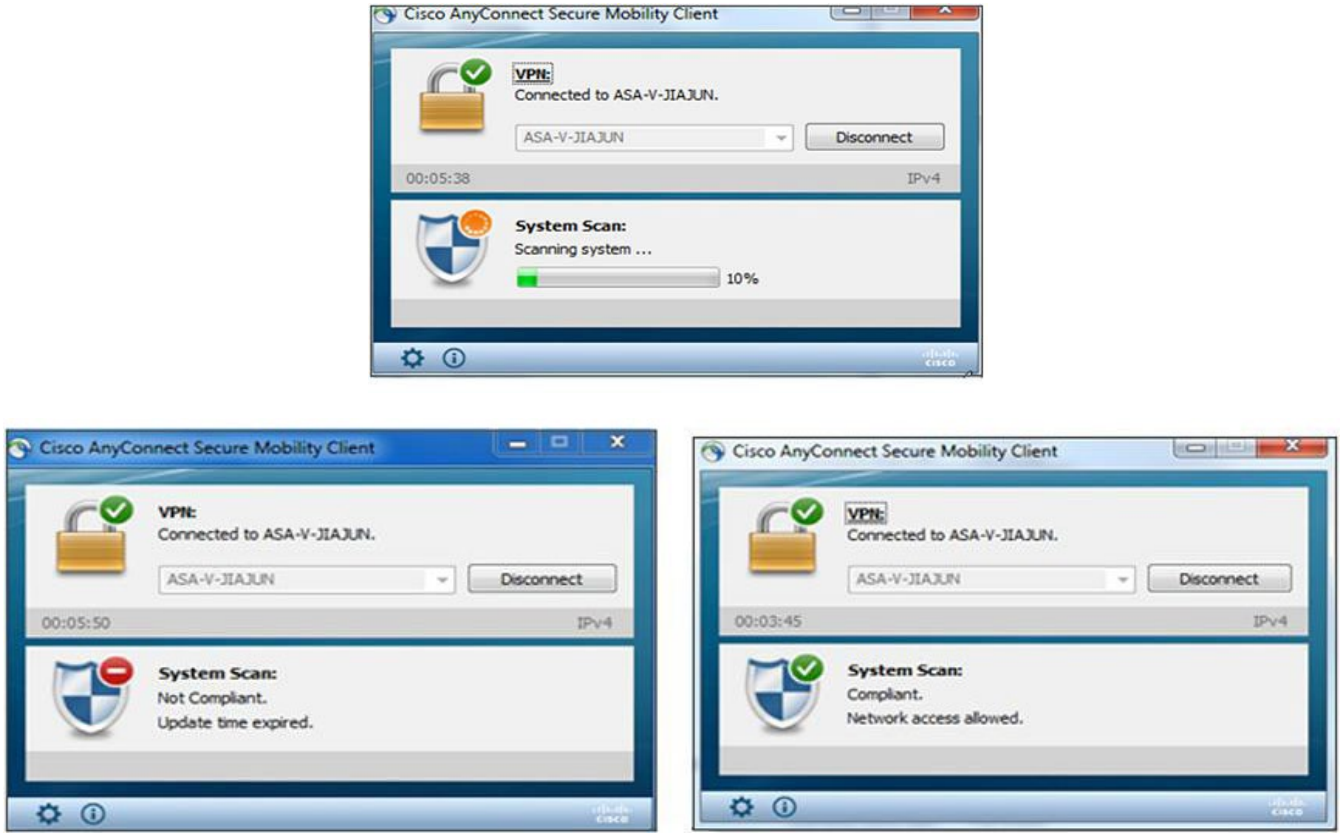


Client Modules

The AnyConnect client is a lightweight, modular security client providing customizable capabilities based on the individual needs of the business. Features such as VPN, 802.1X, compliance check, network visibility, Cisco Umbrella Roaming, integration with Cloud Web Security, and the ability to install or uninstall Secure Endpoint are available in separately deployable modules or services, so organizations can select the features and functionality most applicable to their connectivity needs. This keeps AnyConnect agile and operationally efficient while providing flexibility and benefit to the organization.

Figure 3 shows the AnyConnect unified endpoint compliance across wired and wireless environments.

Figure 3. Endpoint Compliance Checks



Features and Benefits

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

Table 1. Features and Benefits

Feature	Benefits and Details
Remote-Access VPN	
Broad operating system support	• Windows 10, 8.1, 8, and 7 • Mac OS X 10.8 and later • Linux Intel (x64) See the AnyConnect Mobile datasheet for mobile platform information
Software access	• Downloads are available in the Cisco.com Software Center • Technical support and software entitlement for AnyConnect is included with all term-based Plus and Apex licenses, and it can be purchased separately for the Plus perpetual license • The contract number must be linked to Cisco.com ID. See the AnyConnect ordering guide for details
Optimized network access: VPN protocol choice SSL **(TLS and DTLS); IPsec IKEv2**	• AnyConnect provides a choice of VPN protocols, so administrators can use whichever protocol best fits their business needs • Tunneling support includes SSL (TLS 1.2 and DTLS) and next-generation IPsec IKEv2 • DTLS provides an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCP-based application access • TLS 1.2 (HTTP over TLS or SSL) helps ensure availability of network connectivity through locked-down environments, including those using web proxy servers • IPsec IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPsec
Optimal gateway selection	• Determines and establishes connectivity to the optimal network-access point, eliminating the need for end users to determine the nearest location
Mobility friendly	• Designed for mobile users • Can be configured so that the VPN connection remains established during IP address changes, loss of connectivity, or hibernation or standby • With Trusted Network Detection, the VPN connection can automatically disconnect when an end user is in the office and connect when a user is at a remote location
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). Applies only to IPsec IKEv2 connections. An AnyConnect Apex license is required

Feature	Benefits and Details
Wide range of deployment and connection options	**Deployment options:** • Pre-deployment, including Microsoft Installer • Automatic security gateway deployment (administrative rights are required for initial installation) by ActiveX (Windows only) and Java **Connection modes:** • Standalone by system icon • Stealth agent • Temporal agent • Browser-initiated (web launch) • Clientless portal initiated • CLI initiate • API initiated
Wide range of authentication options	• RADIUS • RADIUS with password expiry (MSCHAPv2) to NT LAN Manager (NTLM) • RADIUS one-time password (OTP) support (state and reply message attributes) • RSA SecurID (including SoftID integration) • Active Directory or Kerberos • Embedded certificate authority (CA) • Digital certificate or smartcard (including machine-certificate support), auto- or user-selected • Lightweight Directory Access Protocol (LDAP) with password expiry and aging • Generic LDAP support • 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 • Multiple delivery methods help ensure broad compatibility of AnyConnect • User may defer pushed updates • Customer experience feedback option is available
Centralized policy control and management	• Policies can be preconfigured or configured locally and can be automatically updated from the VPN security gateway • API for AnyConnect eases deployments through webpages or applications • Checking and user warnings are issued for untrusted certificates • Certificates can be viewed and managed locally

Feature	Benefits and Details
Advanced IP network connectivity	• Public connectivity to and from IPv4 and IPv6 networks • Access to internal IPv4 and IPv6 network resources • Administrator-controlled split-tunneling and all-tunneling network access policy • Access control policy • Per-app VPN policy for Apple iOS, Google Android, and Samsung Knox (new in Release 4.0; requires Cisco ASA 5500-X with OS 9.3 or later and AnyConnect 4.0 licenses) **IP address assignment mechanisms:** • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/Lightweight Directory Access Protocol (LDAP)
Robust unified endpoint compliance (Apex license required)	• Endpoint posture assessment and remediation is supported for wired and wireless environments (replacing the Cisco Identity Services Engine NAC Agent). Requires Identity Services Engine (ISE) 1.3 or later with Identity Services Engine Apex license • ISE Posture (working in conjunction with ISE) and Host Scan (VPN only) seeks to detect the presence of anti-malware software, Windows service packs/patching state, and range of other software services 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 • ISE Posture and Host Scan 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, and a range of other capabilities. Additional capabilities are supported for out-of-compliance applications • Functions vary by operating system. See the Host Scan Support charts for detailed information
Client firewall policy	• Provides added protection for split-tunneling configurations • Used in conjunction with the AnyConnect client to allow for local-access exceptions (for example, printing, tethered device support, and so on) • Supports port-based rules for IPv4 and network and IP access control lists (ACLs) for IPv6 • Available for Windows and Mac OS X platforms
Localization	**In addition to English, the following language translations are included:** • Czech (cs-cz) • German (de-de) • Spanish (es-es) • French (fr-fr) • Japanese (ja-jp) • Korean (ko-kr) • Polish (pl-pl) • Simplified Chinese (zh-cn) • Chinese (Taiwan) (zh-tw)

Feature	Benefits and Details
	• Dutch (nl-nl) • Hungarian (hu-hu) • Italian (it-it) • Portuguese (Brazil) (pt-br) • Russian (ru-ru)
Ease of client administration	• Administrators can automatically distribute software and policy updates from the headend security appliance thereby eliminating administration associated with client software updates • Administrators can determine which capabilities to make available for end-user configuration • Administrators can trigger an endpoint script at connect and disconnect times when domain login scripts cannot be utilized • Administrators can fully customize and localize end-user visible messages
Profile editor	• AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM)
Diagnostics	• On-device statistics and logging information are available • Logs can be viewed on device • Logs can be easily emailed to Cisco or an administrator for analysis
Federal Information Processing Standard (FIPS)	• FIPS 140-2 level 2 compliant (platform, feature, and version restrictions apply)

Feature	Benefits and Details
Secure Mobility and Network Visibility	
Web security integration (Cloud Web Security license required)	• Uses Cloud Web Security, the largest global provider of software-as-a-service (SaaS) web security, to keep malware off corporate networks and control and safeguard employee web usage • Supports cloud-hosted configurations and dynamic loading • Gives organizations flexibility and choice by supporting cloud-based services in addition to premises-based services • Integrates with the Web Security Appliance • Supports Trusted Network Detection • Enforces security policy in every transaction, independent of user location • Requires always-on highly secure network connectivity with a policy to permit or deny network connectivity if access becomes unavailable • Detects hotspots and captive portals
Cisco Umbrella Roaming (Cisco Umbrella Roaming license required)	• Enforce security for roaming devices when the VPN is off • Automatically block malware, phishing, and C2 callbacks on roaming devices • Simplest way to protect devices anywhere they go • Utilize endpoint redirection to enforce DNS-based security when the VPN is off or with split tunnels (applies to communication outside tunnel)
Network Visibility module (Apex license required)	• Capture endpoints flows with rich user, endpoint, application, location, and destination context • Flexible collection settings on and off premise • Uncover potential behavior anomalies by monitoring application usage • Allows for more informed network-design decisions • Usage data can be shared with NetFlow analysis tools such as Cisco Network Analytics
Advanced Malware Protection (AMP) for Endpoints Enabler (AMP for Endpoints licensed separately)	• Simplifies the enablement of threat protection services to AnyConnect endpoints by distributing and enabling Secure Endpoint • Extends endpoint threat services to remote endpoints, increasing endpoint threat coverage • Provides more proactive protection to further assure an attack is mitigated at the remote endpoint quickly
Broad operating system support	• Windows 10, 8.1, 8, and 7 • Mac OS X 10.8 and later • See the AnyConnect Mobile data sheet for mobile platform information
Network Access Manager and 802.1X	
Media support	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11)

Feature	Benefits and Details
Network authentication	• IEEE 802.1X-2001, 802.1X-2004, and 802.1X-2010 • Enables businesses to deploy a single 802.1X authentication framework to access both wired and wireless networks • Manages the user and device identity and the network access protocols required for highly secure access • Optimizes the user experience when connecting to a Cisco unified wired and wireless network
Extensible Authentication Protocol (EAP) methods	• EAP-Transport Layer Security (TLS) • EAP-Protected Extensible Authentication Protocol (PEAP) with the following inner methods: • EAP-TLS • EAP-MSCHAPv2 • EAP-Generic Token Card (GTC) • EAP-Flexible Authentication via Secure Tunneling (FAST) with the following inner methods: • EAP-TLS • EAP-MSCHAPv2 • EAP-GTC • EAP-Tunneled TLS (TTLS) with the following inner methods: • Password Authentication Protocol (PAP) • Challenge Handshake Authentication Protocol (CHAP) • Microsoft CHAP (MSCHAP) • MSCHAPv2 • EAP-MD5 • EAP-MSCHAPv2 • Lightweight EAP (LEAP), Wi-Fi only • EAP-Message Digest 5 (MD5), administrative configured, Ethernet only • EAP-MSCHAPv2, administrative configured, Ethernet only • EAP-GTC, administrative configured, Ethernet only
Wireless encryption methods (requires corresponding 802.11 NIC support)	• Open • Wired Equivalent Privacy (WEP) • Dynamic WEP • Wi-Fi Protected Access (WPA) Enterprise • WPA2 Enterprise • WPA Personal (WPA-PSK) • WPA2 Personal (WPA2-PSK) • CCKM (requires Cisco CB21AG Wireless NIC)
Wireless encryption protocols	• Counter mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) using the Advanced Encryption Standard (AES) algorithm • Temporal Key Integrity Protocol (TKIP) using the Rivest Cipher 4 (RC4) stream cipher

Feature	Benefits and Details
Session resumption	• RFC2716 (EAP-TLS) session resumption using EAP-TLS, EAP-FAST, EAP-PEAP, and EAP-TTLS • EAP-FAST stateless session resumption • PMK-ID caching (Proactive Key Caching or Opportunistic Key Caching), Windows XP only
Ethernet encryption	• Media Access Control: IEEE 802.1AE (MACsec) • Key management: MACsec Key Agreement (MKA) • Defines a security infrastructure on a wired Ethernet network to provide data confidentiality, data integrity, and authentication of data origin • Safeguards communication between trusted components of the network
One connection at a time	• Allows only a single connection to the network disconnecting all others • No bridging between adapters • Ethernet connections automatically take priority
Complex server validation	• Supports “ends with” and “exact match” rules • Support for more than 30 rules for servers with no name commonality
Ethernet encryption	• Media Access Control: IEEE 802.1AE (MACsec) • Key management: MACsec Key Agreement (MKA) • Defines a security infrastructure on a wired Ethernet network to provide data confidentiality, data integrity, and authentication of data origin • Safeguards communication between trusted components of the network
One connection at a time	• Allows only a single connection to the network disconnecting all others • No bridging between adapters • Ethernet connections automatically take priority
Complex server validation	• Supports “ends with” and “exact match” rules • Support for more than 30 rules for servers with no name commonality
EAP-Chaining (EAP-FASTv2)	• Differentiates access based on enterprise and non-enterprise assets • Validates users and devices in a single EAP transaction
Enterprise Connection Enforcement (ECE)	• Helps ensure that users connect only to the correct corporate network • Prevents users from connecting to a third-party access point to surf the Internet while in the office • Prevents users from establishing access to the guest network • Eliminates cumbersome blocked listing
Next-generation encryption (Suite B)	• Supports the latest cryptographic standards • Elliptic Curve Diffie-Hellman key exchange • Elliptic Curve Digital Signature Algorithm (ECDSA) certificates

Feature	Benefits and Details
Credential types	• Interactive user passwords or Windows passwords • RSA SecurID tokens • One-time password (OTP) tokens • Smartcards (Axalto, Gemplus, SafeNet iKey, Alladin) • X.509 certificates • Elliptic Curve Digital Signature Algorithm (ECDSA) certificates
Remote desktop support	• Authenticates remote user credentials to the local network when using Remote Desktop Protocol (RDP)

Platform Compatibility

AnyConnect is compatible with all Cisco ASA 5500-X Series Next Generation Firewalls and 5500 Series Enterprise Firewall Edition models running Cisco ASA Software Release 8.0(4) or later. Deploying current appliance software releases is encouraged.

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

Cisco supports AnyConnect VPN access to Cisco IOS® Release 15.1(2)T and later functioning as the security 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

Licensing Options

AnyConnect Plus or Apex licenses are required for AnyConnect 4.x or later.

Information on licensing options and ordering may be found in 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 AnyConnect for Mobile Platforms data sheet: http://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility- client/data_sheet_c78-527494.html
- Cisco ASA 5500-X Series Adaptive Security Appliances: http://www.cisco.com/go/asa
- Cisco Cloud Web Security: http://www.cisco.com/go/cws
- Cisco Secure Endpoint: http://www.cisco.com/c/en/us/products/security/fireamp-endpoints/index.html
- Cisco AnyConnect Secure Mobility Client – License Agreement and Privacy Policy: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyC onnect-SEULA-v4-x.html

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 **https://www.cisco.com/go/offices**.