Cisco AnyConnect Secure Mobility Client Data Sheet

Product Overview

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, Cisco AnyConnect consistently raises the bar in remote access technology. The Cisco AnyConnect Secure Mobility Client provides a secure connectivity experience across a broad set of PCs and mobile devices. As mobile workers roam to different locations, an always-on intelligent VPN enables the Cisco AnyConnect Secure Mobility Client to automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method. That may include Datagram Transport Layer Security (DTLS) protocol for latency-sensitive traffic, voice over IP (VoIP) traffic, or TCP-based application access. 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 with the Cisco AnyConnect 4.0 per-app-VPN feature.

Cisco AnyConnect 4.0 supports robust unified endpoint compliance. It protects the integrity of the corporate network by restricting Cisco Adaptive Security Appliance (ASA) VPN access 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 anti-spyware products. Out-of-compliance endpoint enforcement provides options to remediate and implement additional system checks before access is granted.

Cisco AnyConnect Secure Mobility Solution has built-in web security and malware threat defense. Choose either the premises-based Cisco® Web Security Appliance (WSA) or cloud-based Cisco Cloud Web Security (CWS) for reliable and highly secure employee access to corporate resources. Web security, malware threat defense, and remote access are brought together in a comprehensive and highly secure enterprise mobility solution. Consistent, context-aware security policies help ensure a protected and productive work environment.

In addition to industry-leading VPN capabilities, the Cisco AnyConnect Secure 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 Cisco AnyConnect Secure Mobility Client 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 sample Cisco AnyConnect VPN configuration on Microsoft Windows.

Figure 1. Cisco AnyConnect Icon and Sample VPN Configuration on Microsoft Windows

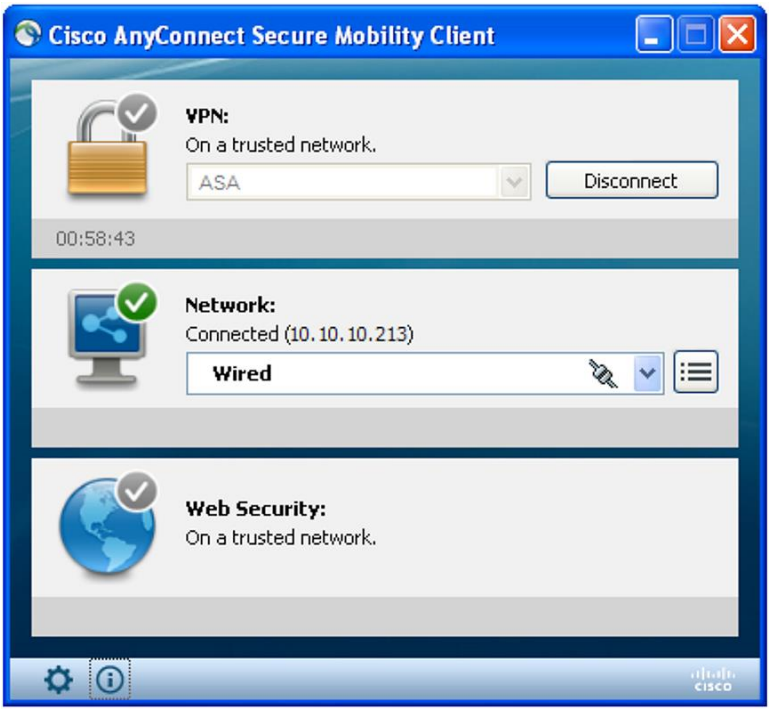
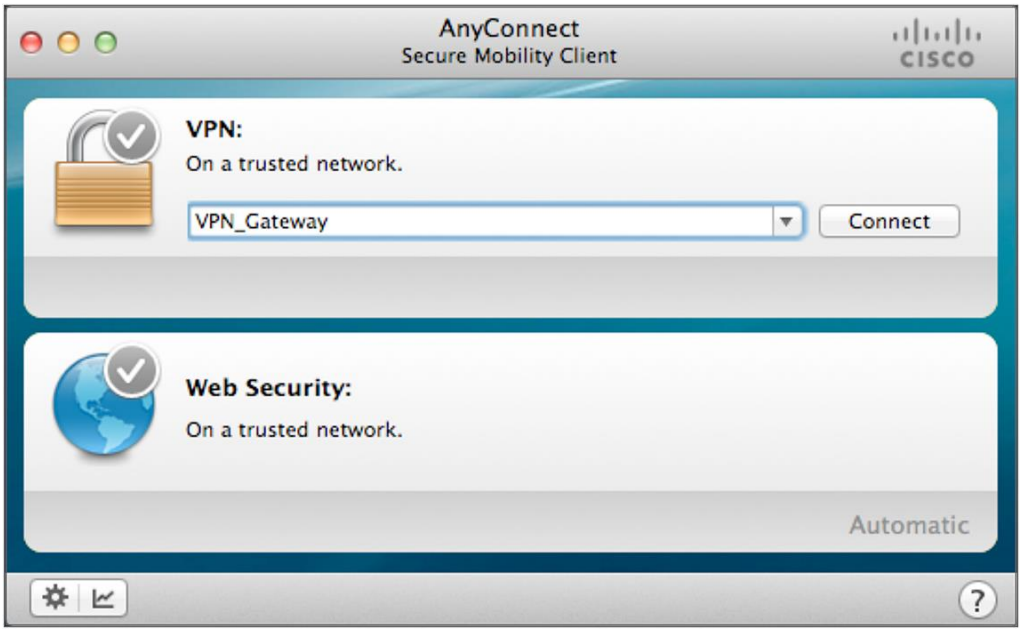


Figure 2 shows a sample Cisco AnyConnect VPN configuration on Apple OS X.

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

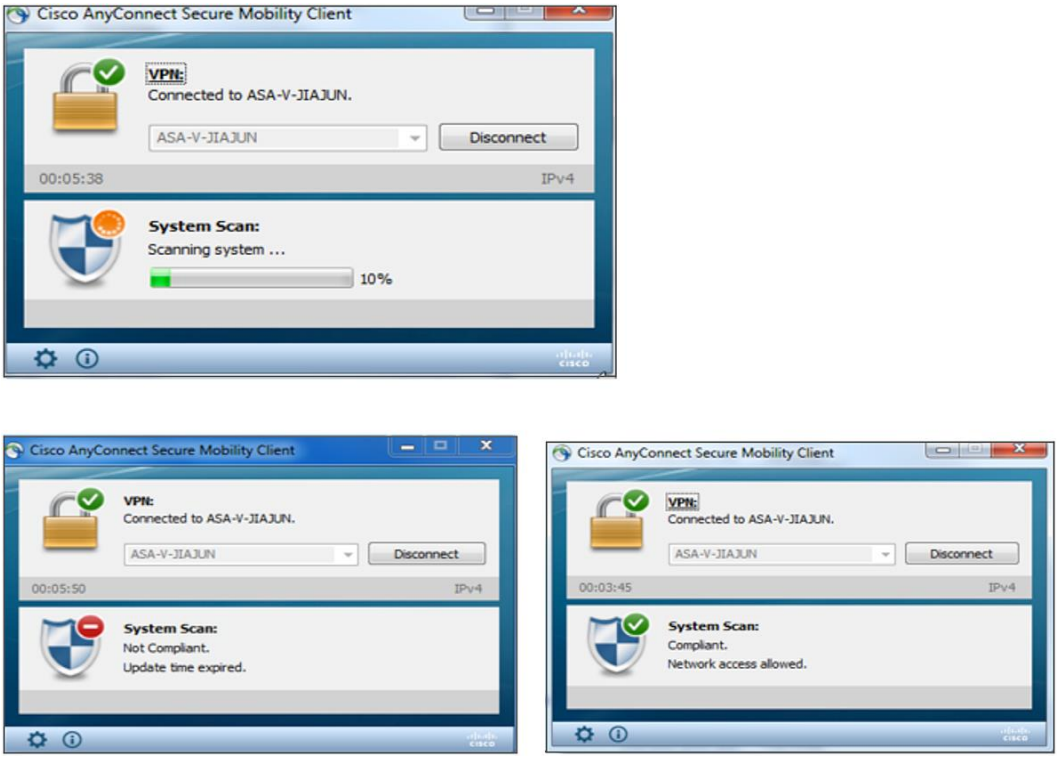


Cisco AnyConnect Secure Mobility Client Modules

The Cisco AnyConnect Secure Mobility Client is a lightweight, highly modular security client providing easily customizable capabilities based on the individual needs of the business. Features such as VPN, 802.1X, compliance check, and integration with Cisco CWS are available in separately deployable modules, allowing organizations to select the features and functionality most applicable to their secure connectivity needs. This keeps Cisco AnyConnect nimble and operationally efficient, while providing flexibility and benefit to the organization.

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

Figure 3. Cisco AnyConnect 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 Virtual Private Networking	
Broad operating system support	• Windows 8 and 8.1 • Windows 7 32-bit (x86) and 64-bit (x64) • Mac OS X 10.8 and later • Linux Intel (x64)
Software access	• 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

Feature	Benefits and Details
Optimized network access: VPN protocol choice SSL (TLS and DTLS); IPsec IKEv2	• AnyConnect provides a choice of VPN protocols, allowing administrators to use whichever protocol best fits their business needs • Tunneling support includes SSL (TLS 1.2 and DTLS) and next-generation IPsec (Internet Key Exchange version 2) • 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. Cisco AnyConnect Apex license required.)
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 • Browser-initiated (web launch) • Clientless portal initiated • CLI initiated • 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 or 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 Cisco AnyConnect • User may defer pushed updates to Cisco AnyConnect • Customer experience feedback option
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 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 iOS 7 and later (new in Cisco AnyConnect 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 **(AnyConnect Apex license required)**	• **New in Cisco AnyConnect 4.0:** Endpoint posture assessment and remediation for wired and wireless environments (replacing the Cisco Identity Service Engine NAC Agent). Requires ISE 1.3 or later with ISE Apex license. • Cisco Hosts can 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 Hosts 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 or to matching • Additional capabilities are supported for out-of-compliance applications
Client firewall policy	• Added protection for split-tunneling configurations • Used in conjunction with Cisco AnyConnect Secure Mobility 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 7, 8, 8.1, and Mac OS X 10.8 and later
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) • Dutch (nl-nl) • Hungarian (hu-hu) • Italian (it-it) • Portuguese (Brazil) (pt-br) • Russian (ru-ru)
Ease of client administration	• Allows an administrator to automatically distribute software and policy updates from the head-end 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
AnyConnect profile editor	• AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM).
Diagnostics	• On-device statistics and logging information • View logs 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	
Web security integration	• Uses Cisco CWS, 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 • Cloud-hosted configurations and dynamic loading • Gives organizations flexibility and choice by supporting cloud-based services in addition to premises-based services • Cisco WSA integration • 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 • Hotspot and captive portal detection
Broad operating system support	• Windows 8 and 8.1 • Windows 7 32-bit (x86) and 64-bit (x64) • Mac OS 10.8 and later
Network Access Manager and 802.1X	
Media support	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11a/b/g/n)
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
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 blacklisting
Next-generation encryption (Suite B)	• Supports the latest cryptographic standards • Elliptic Curve Diffie-Hellman key exchange • Elliptic Curve Digital Signature Algorithm (ECDSA) certificates
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	• Authenticate remote user credentials to the local network when using Remote Desktop Protocol (RDP)
Operating systems supported	• Windows 8 and 8.1 • Windows 7 (32-bit and 64-bit)

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. Deploying current ASA Software releases is encouraged.

Cisco supports Cisco 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.

Cisco AnyConnect Secure Mobility Client Licensing Options

- Information on Cisco AnyConnect licensing options and ordering may be found in the Cisco AnyConnect Ordering Guide at: 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/en/US/products/ps6120/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 Adaptive Security Appliances: 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.

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 C78-733184-00 10/14