Get to Know the Cisco AnyConnect Secure Mobility Client

Objective

This article focuses on the features, specifications, and benefits of using Cisco AnyConnect. For information on AnyConnect licensing on the RV340 series routers, please see the article AnyConnect Licensing for the RV340 Series Routers .

Software Version

4.2.03013 (Release Notes)

Features and Specifications

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 data sheet for mobile platform information.
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	AES-256 and 3DES-168. (The security gateway device must have a strong-crypto license enabled.) 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.
Wide range of deployment and connection options	**Deployment options:** Predeployment, 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-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.
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 Google Android (Lollipop) 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/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 1.3

	or later with Identity Services Engine Apex license. Cisco Hostscan 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. Hostscan detects 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 certificates issued by or to a matching certificate authority. 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) 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)
Secure Mobility and Network Visibility	
Web security integration (Cloud Web Security license required)	Uses Cloud Web Security, the largest global provider of S oftware-as-a- S ervice (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.
Network Visibility module (Apex license required)	Uncover potential behavior anomalies by monitoring application usage. Allows for more informed network-design decisions. Can share usage data with a growing number of Internet Protocol Flow Information Export (IPFIX)-capable network-analysis tools.
Advanced Malware Protection (AMP) for Endpoints Enabler (AMP for Endpoints licensed separately)	Simplifies the enablement of threat services to AnyConnect endpoints by distributing and enabling CiscoAMP for Endpoints. 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
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
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	Authenticates remote user credentials to the local network when using Remote Desktop Protocol (RDP).
Operating systems supported	Windows 10, 8.1, 8 and 7