Data sheet
Cisco public

CISCO SECURE

Cisco Secure Client

Formerly Cisco AnyConnect

July 2022

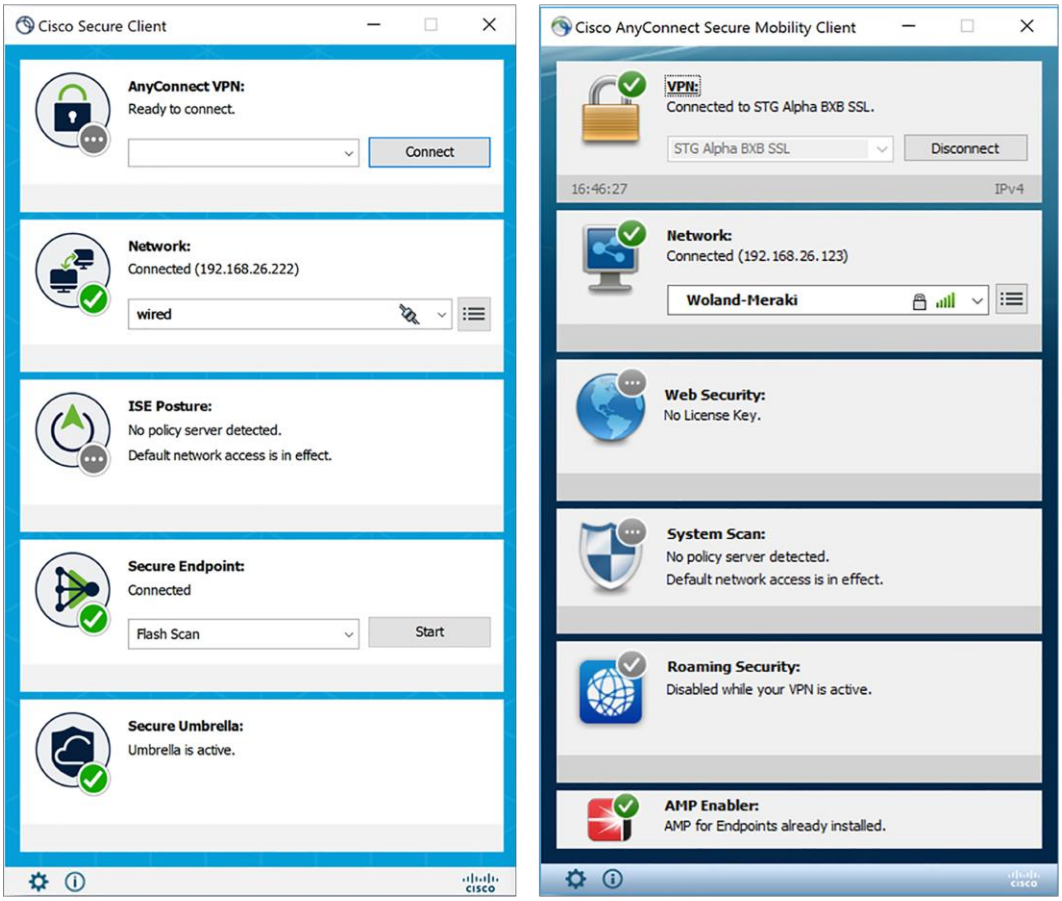
Contents

Overview

Cisco Secure Client, formerly Cisco AnyConnect Secure Mobility Client, is available for Windows 10 and 11. The user interface will be familiar to current AnyConnect users with some updated branding and iconography.

Customers running on macOS and Linux will continue to utilize AnyConnect 4.x until Cisco Secure Client has full OS support.

Cisco Secure Client vs AnyConnect



Cisco Secure Client is the latest version of one of the most widely deployed security clients. Secure Client is built upon Cisco AnyConnect, which provides Remote Access services and a suite of modular security services.

Important to know

AnyConnect is now known as Cisco Secure Client. Additionally, Secure Endpoint is a new optional module of Secure Client that provides customers with integrated advanced Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) capabilities.

New users can install Secure Client by traditional methods and customers looking to adopt the new Cloud Management functions can do so with a packaged installer download from the Secure Endpoint portal.

Cloud Management via SecureX with Device Insights is a new optional capability for Secure Client. This new feature makes deploying, configuring, and monitoring Secure Client simple. Customers are not required to adopt cloud management and can continue to deploy using the current mechanisms; Cisco Secure Firewall, ISE, Software Management tools, i.e., SCCM as an example, or directly using the MSI.

New SecureX screens and tools for Cloud Management include:

- Customizing and generating a network installer for Secure Client
- Creating and downloading custom VPN profiles for Secure Client
- Integrating with Device Insights to monitor and manage an inventory of endpoints with Secure Client installed

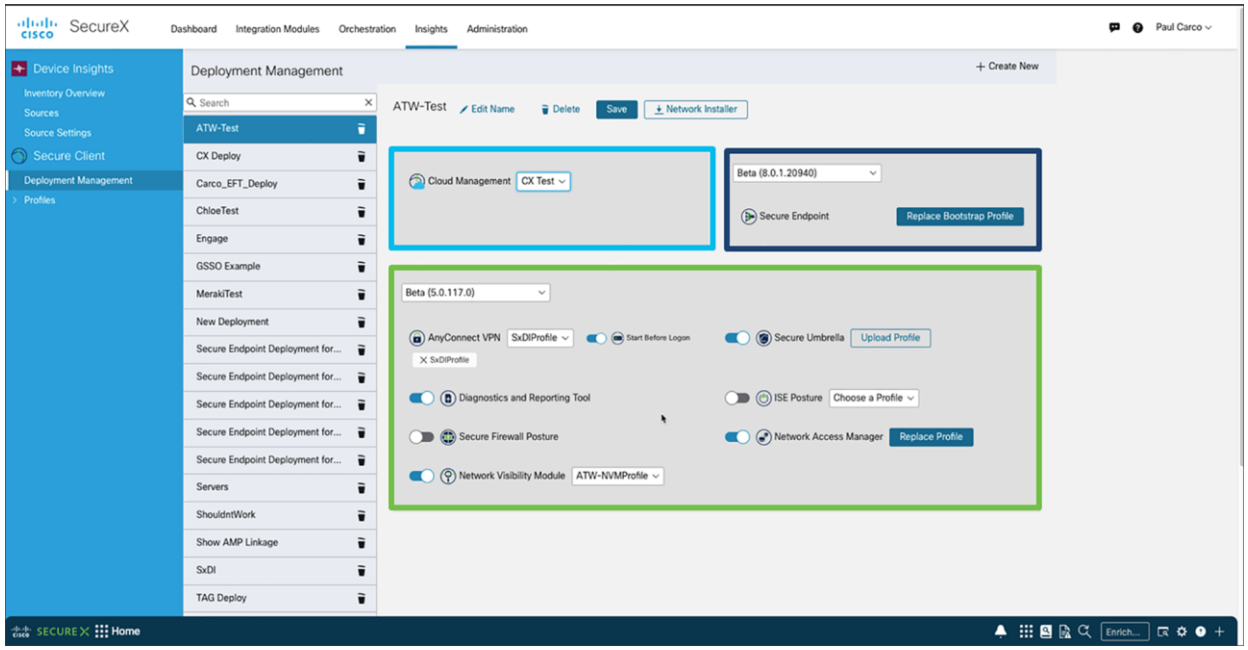


Figure 1.
Cloud Management

Secure Endpoint Module

Secure Client Modules

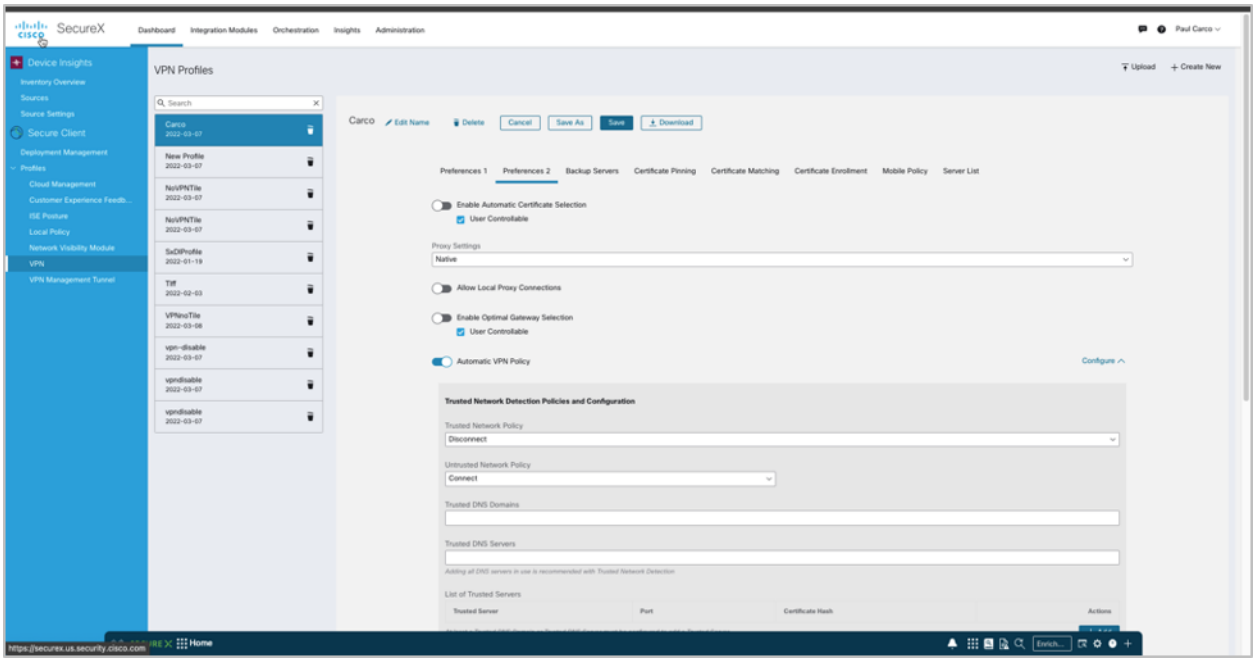


Figure 2.
VPN Profiles

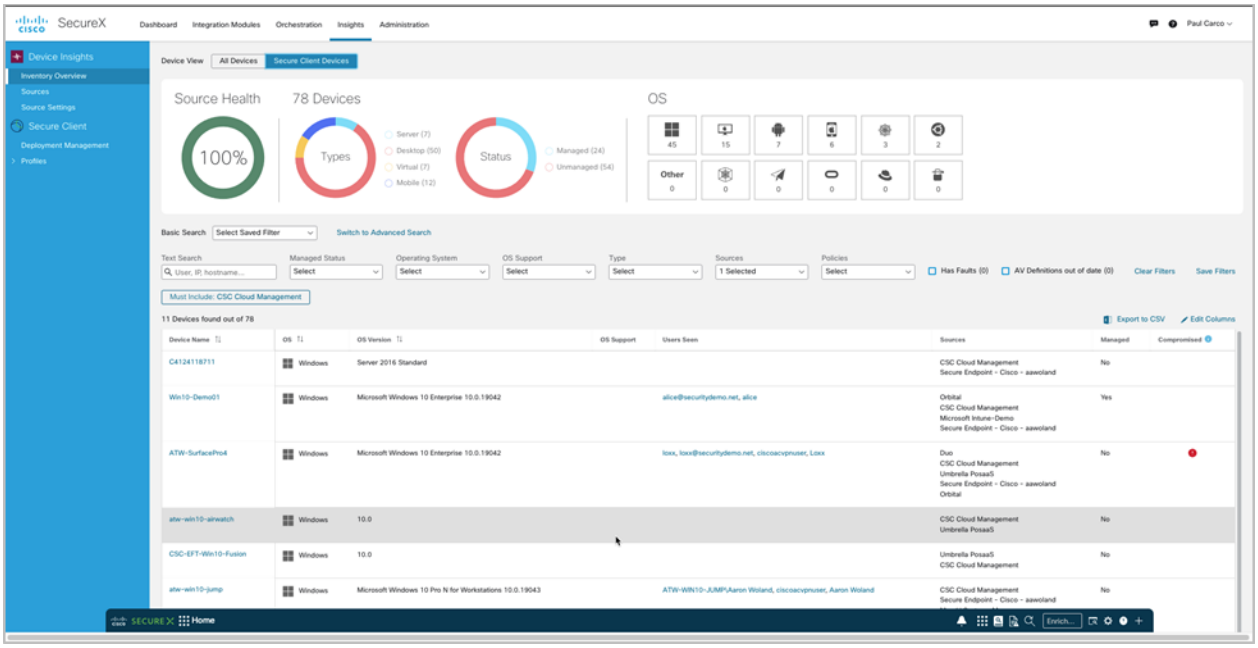


Figure 3.
Device Insights

Modules and Features

AnyConnect VPN/ZTNA User and Management Tunnels

Cisco Secure Client provides many options for automatically connecting, reconnecting, or disconnecting VPN sessions. These options offer a convenient way for your users to connect to your VPN and support your network security requirements. An always-on intelligent VPN helps AnyConnect client devices automatically select the optimal network access point and adapt its tunneling protocol to the most efficient method, including Datagram Transport Layer Security (DTLS) protocol for latency-sensitive traffic, and a path for entering Zero Trust Network 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 and Google Android.

Management VPN tunnel provides connectivity to the corporate network whenever the client system is powered up, not just when the end-user establishes a VPN connection. As a result, you can perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. This feature will also benefit endpoint OS login scripts that require corporate network connectivity. This capability does not have an end-user interface.

Cisco Secure Endpoint

Available with Cisco Secure Client for Windows, Secure Endpoint functions as a module within Cisco Secure Client and is accessible via the Cisco Secure Client user interface. The Cisco Secure Endpoint Cloud can also deploy Cisco Secure Client with Cisco Secure Endpoint, as can SecureX Cloud Management. by taking advantage of this integration, customers can reduce the number of clients under their management.

Cloud Management Module

SecureX Cloud Management Deployment for Cisco Secure Client enables administrators to create cloud-managed deployments of Cisco Secure Client. The deployment configuration generates the option to download a lightweight bootstrapper that contains the information needed by the endpoint to contact the cloud for the specified Cisco Secure Client modules by the deployment with their associated profiles. A full installer is also available. In either case, the installers can be distributed to the endpoints by the administrator using their preferred software method.

Network Visibility Module

The Network Visibility Module delivers a continuous feed of high-value endpoint telemetry, which allows organizations to see endpoint and user behaviors on their networks. It collects flow from endpoints on and off-premises and valuable contexts like users, applications, devices, locations, and destinations. It caches this data and sends it to the Network Visibility Module Collector when it is on a trusted network (the corporate network on-prem or through VPN). Network Visibility Module Collector is a server that receives Internet Protocol Flow Information Export (IPFIX) data and optional filters that are exported to Cisco Secure Network Analytics Endpoint License, Syslog, or a third-party collector. Network Visibility Module Collector processes received messages that adhere to the nvzFlow protocol specification.

NVM sends flow information only when it is on the trusted network. By default, no data is collected. Data is collected only when configured as such in the profile, and the data continues to be collected when the endpoint is connected. If collection is done on an untrusted network, it is cached and sent when the endpoint is on a trusted network. No UI

Umbrella Roaming Security module

To take advantage of Umbrella Roaming Security service, you need the Professional, Insights, Platform, or MSP package subscriptions. Umbrella Roaming Security provides DNS-layer security when no VPN is active and adds an Intelligent Proxy. Additionally, Cisco Umbrella subscriptions provide content filtering, multiple policies, robust reporting, functional directory integration, and more. Use the same Umbrella Roaming Security module regardless of the subscription.

ISE Posture module

ISE Posture is a module you can choose to install as an additional security component of the Cisco Secure Client product. Perform an endpoint posture assessment on any endpoint that fails to satisfy all mandatory requirements and is deemed non-compliant. The other endpoint authorization states are posture unknown or compliant by meeting mandatory requirements. The client receives the posture requirement policy from the headend, collects the posture data, compares the results against the policy, and sends the assessment results back to the headend. Even though ISE determines whether the endpoint is compliant, it relies on Secure Endpoint's policy evaluation.

Network Access Manager

Network Access Manager manages user and device identity and the network access protocols required for secure access. It works intelligently to prevent end-users from making connections that violate administrator-defined policies. It detects and selects the optimal Layer 2 access network by its policies and performs device authentication for access to both wired and wireless networks.

Posture (for Secure Firewall)

Secure Firewall Posture performs server-side evaluation where the Secure Firewall asks only for a list of endpoint attributes such as operating system, IP address, registry entries, local certificates, and filenames, and they are returned by Secure Firewall Posture. Based on the policy's evaluation result, you can control which hosts are allowed to create a remote access connection to the security appliance.

Feature	Benefits and Details
Remote-Access VPN/ZTNA	
Broad operating system support	Windows 11 (64-bit), current Microsoft supported versions of Windows 10 x86 (32-bit) and x64 (64-bit), and Windows 8 Microsoft-supported versions of Windows 11 for ARM64-based Microsoft-supported versions of Windows 10 for ARM64-based PCs **Note:** Cisco Secure Client 5.0 is Windows 10/11 Only. AnyConnect supports all the above. macOS 12, 11.2, 10.15, and 10.14 (all 64-bit) Red Hat Ubuntu SUSE (SLES) See mobile data sheet for Mobile OS support

Feature	Benefits and Details
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 Secure Client 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 1.2) 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	TLS/DTLS 1.2 strong ciphers supported 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. Premier (formerly AnyConnect Apex) is required
Wide range of deployment options	**Deployment options:** Predeploy—New installations and upgrades are done either by the end user or by using an enterprise Software Management System (SMS) Web Deploy—The Cisco Secure Client package is loaded on the headend, which is either a Secure Firewall ASA, Secure Firewall Threat Defense, or an ISE server. When the user connects to a firewall or to ISE, Cisco Secure Client is deployed to the client SecureX Cloud Management Deployment— Cisco Secure Client 5.0 can be deployed from the Cloud using customizable deployments

Feature	Benefits and Details
Wide range of authentication options	**Protocols:** SAML 2.0 with Embedded or Native Browser (SSO) RADIUS LDAP Certificate. TACACS+ HTTP Form SDI Kerberos **Headend Methods** AAA AAA and Certificate Certificate Only SAML Multiple Certificates and AAA
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 client software updates if configured by the Administrator 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 Cisco Secure Client supports deployment and management using the SecureX platform
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 (Network and Dynamic (domain) and full tunnel network access policy Access control policy using Dynamic Access Polices or the identity Services Engine Per-app VPN policy for Apple iOS and Google Android **IP address assignment mechanisms:** Static Internal pool Dynamic Host Configuration Protocol (DHCP) RADIUS/Lightweight Directory Access Protocol (LDAP)

Feature	Benefits and Details
Robust unified endpoint compliance **(Premier formerly 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
Client firewall policy	Provides added protection for split-tunneling configurations Used in conjunction with the AnyConnect and Cisco Secure 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:** cs-CZ Czech (Czech Republic) de-DE German (Germany) es-ES Spanish (Spain) fr-CA French (Canada) fr-FR French (France) hu-HU Hungarian (Hungary) it-IT Italian (Italy) ja-JP Japanese (Japan) ko-KR Korean (Korea) nl-NL Dutch (Netherlands) pl-PL Polish (Poland) pt-BR Portuguese (Brazil) ru-RU Russian (Russia) zh-CN Chinese (China) zh-HANS Chinese (Simplified) zh-HANT Chinese (Traditional) zh-TW Chinese (Taiwan)

Feature	Benefits and Details
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. Cisco Secure Client 5.0 also offers administrators the ability to deploy and manage the client from the SecureX Cloud. 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) Stand-alone Profile Editor SecureX Cisco Secure Client Profile page
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	
Cisco Umbrella Roaming (Cisco Umbrella Roaming license required)	The Umbrella Roaming Security module requires a subscription to a Umbrella Roaming Security service with either the Professional, Insights, Platform, or MSP package. Umbrella Roaming Security provides DNS-layer security when no VPN is active, and a Cisco Umbrella subscription adds Intelligent Proxy. Additionally, Cisco Umbrella subscriptions provide content filtering, multiple policies, robust reporting, active directory integration, and much more. The same Umbrella Roaming Security module is used regardless of the subscription. • 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 (Premier formerly 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

Feature	Benefits and Details
Cisco Secure Endpoint formerly Advanced Malware Protection (AMP) for Endpoints **(Cisco Secure Endpoints licensed separately)**	Cisco Secure Client brings together both AnyConnect VPN/ZTNA and Cisco Secure Endpoint capabilities 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 macOS endpoints can continue to use standalone Secure Endpoint client
Network Access Manager and 802.1X	
Media support	• Ethernet (IEEE 802.3) • Wi-Fi (IEEE 802.11)
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)

Feature	Benefits and Details
Wireless encryption protocols	Counter mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) using the Advanced Encryption Standard (AES) algorithm
Session resumption	RFC2716 (EAP-TLS) session resumption using EAP-TLS, EAP-FAST, EAP-PEAP, and EAP-TTLS EAP-FAST stateless session resumption
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 **(Windows only with Network Access Manager)**	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
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

Platform compatibility

Secure Client is compatible with various Cisco Secure Firewalls, Meraki devices, Cisco Secure Connect Choice, and Cisco Secure Connect Flex. Deploying current appliance software releases is encouraged.

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

Licensing options

Secure Client Advantage, Premium or VPN Only licenses are required. Customers with valid AnyConnect Plus, Apex or VPN Only licenses are eligible to utilize the Cisco Secure Client.

Information on licensing options and ordering may be found in the ordering guide at: https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/secure-client-og.html.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

Learn more

- Cisco Secure Client homepage: https://www.cisco.com/go/secureclient
- Cisco Secure Client (formerly AnyConnect) documentation: https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html
- Cisco Secure Client (formerly AnyConnect) for Mobile Platforms data sheet: https://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: https://www.cisco.com/go/asa
- Cisco Secure Endpoint: https://www.cisco.com/site/us/en/products/security/endpoint-security/secure-endpoints/index.html
- Cisco Secure Client (formerly AnyConnect)– License Agreement and Privacy Policy: https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/license/end_user/AnyConnect-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**.

Printed in USA C78-3117430-00 07/22