Cisco Secure Client

Formerly Cisco AnyConnect

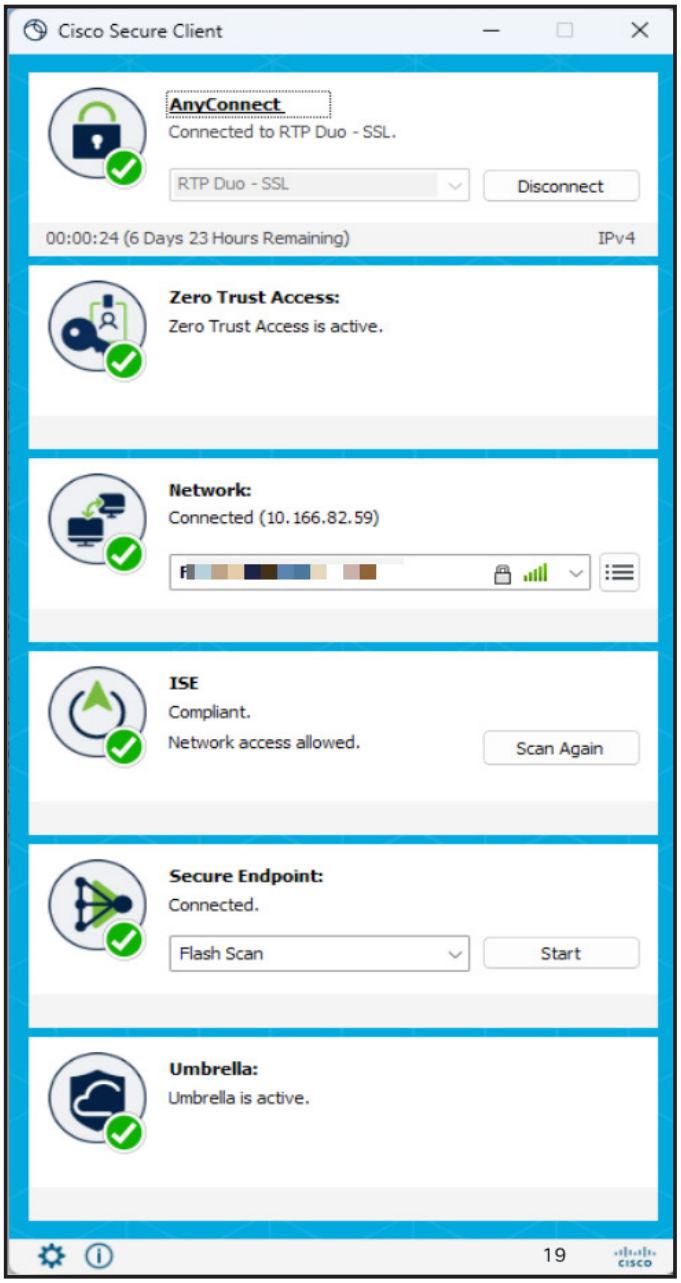
September 2024

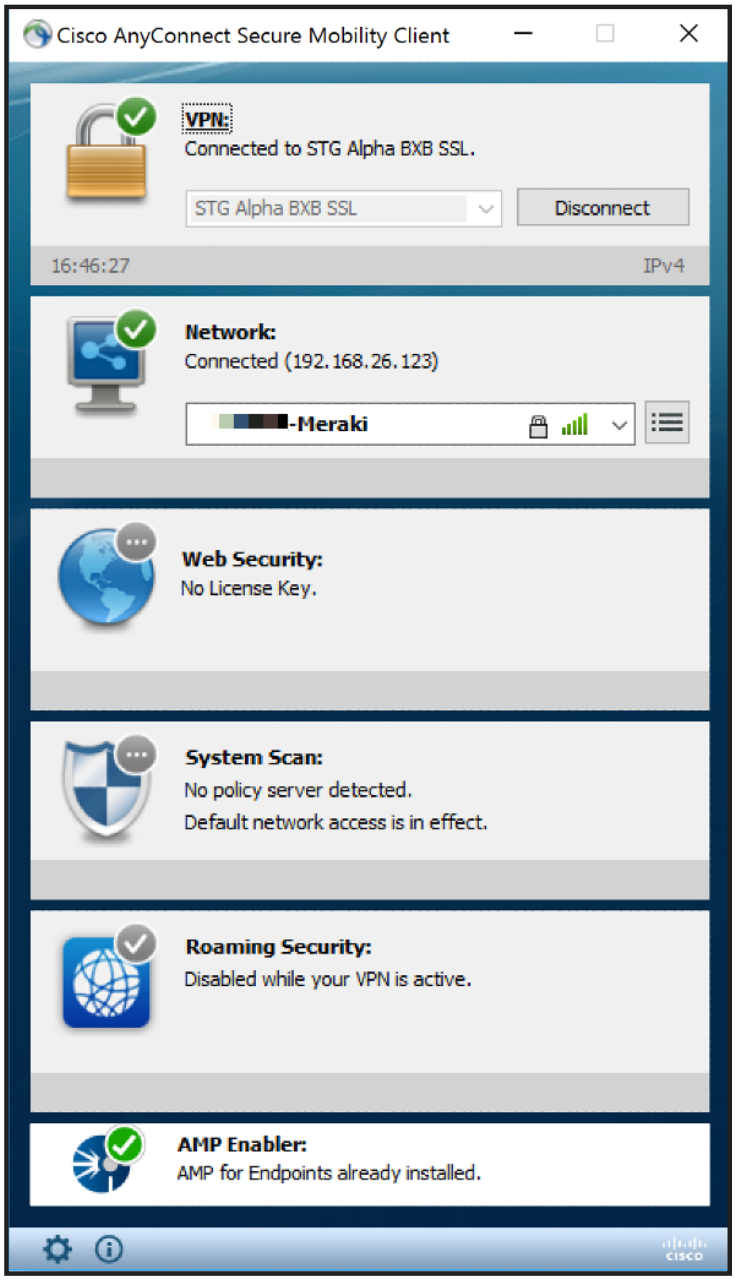
Contents

Overview

Cisco Secure Client version 5, previously known as Cisco AnyConnect Secure Mobility Client, is compatible with Windows, macOS, and Linux platforms. Users familiar with the current AnyConnect interface will find the Cisco Secure Client user interface similar, with the main differences being the new branding and updated icons.

Cisco Secure Client 5 vs. AnyConnect 4.10





Cisco Secure Client is the rebranded version of one of the most widely deployed security clients. While Cisco AnyConnect is most known as a VPN client, it has evolved significantly over the years. Today, it is more accurately described as a comprehensive security client that offers a suite of security services through its modular approach.

Important to know

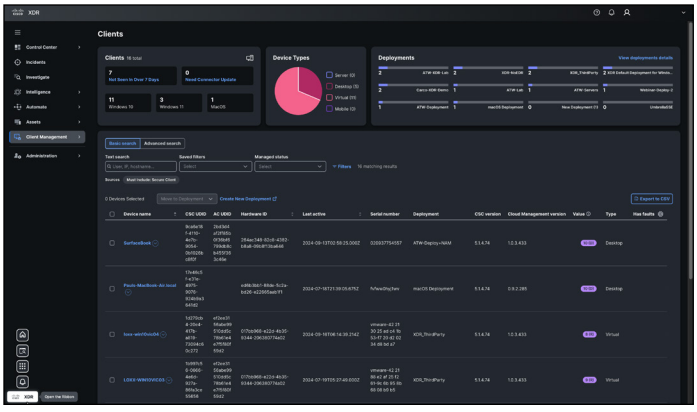
AnyConnect rebranding to Secure Client (including major version increment to 5)

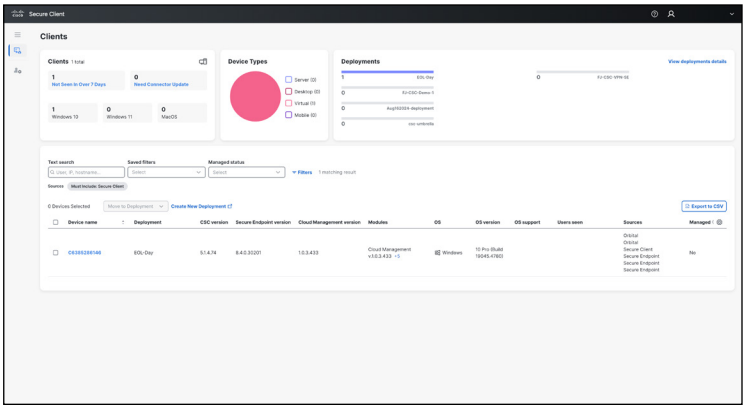
- Introduction of Secure Endpoint within Cisco Secure Client as a fully functioning module
- Software maintenance for 4.x software releases ended on **March 31, 2024**. Maintenance releases and patches are no longer provided for AnyConnect 4.x, customers should migrate to Cisco Secure Client
- Application software support (AnyConnect 4.x) will not be available for the stated software versions beyond **March 31, 2027**. Software maintenance and application software support requires an active term license or active service contract for perpetual licenses. After these dates, all support services for the product are unavailable, and the product becomes obsolete. Migration path is Cisco Secure Client 5
- Cloud deployment and management of Cisco Secure Client 5 and later versions available standalone in Cisco Secure Client Cloud Management or via Cisco XDR

Note: : Customers have the flexibility to continue using their existing deployment methods, including options like Cisco Secure Firewall ASA, Cisco Firepower (NGFW) , ISE, MDM/EMM, or software management tools such as SCCM. Alternatively, they can also choose to deploy using the MSI installer directly.

Screens and tools for Cloud Management including:

- Capability to customize and generate a network installer for Secure Client
- Option to create, upload, and download custom profiles for Secure Client
- Leverage the visibility provided by the Client Inventory for clients deployed via the cloud
- Available in XDR: The Client Management feature with Secure Client is the next-generation Secure Mobility Client, integrating the functionalities of both AnyConnect and Secure Endpoint with a Cloud Management solution into a single, unified end-user interface.
- Available in a Stand-alone interface: Cisco Secure Client Cloud Management is the next-generation Secure Mobility Client, merging the capabilities of both AnyConnect and Secure Endpoint with a Cloud Management solution into a single, unified end-user interface.





Modules and Features

AnyConnect VPN User and Management Tunnels

Cisco Secure Client offers various options for automatically connecting, reconnecting, or disconnecting VPN sessions. These options make it convenient for users to connect to your VPN while supporting your network security needs. An always-on intelligent VPN allows AnyConnect client devices to automatically select the best network access point and adapt its tunneling protocol to the most efficient method. This can include the 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 can be enforced on Apple iOS, Google Android and Samsung Knox with the per-app VPN.

The management VPN tunnel ensures connectivity to the corporate network whenever the client system is powered up, not just when a VPN connection is established by the end user. This feature allows for patch management on out-of-office endpoints, especially devices infrequently connected by users via VPN to the office network. Endpoint OS login scripts requiring corporate network connectivity will also benefit from this feature.

Zero Trust Access module

The Zero Trust Access module is now available for Secure Client deployments 5.1.3.62 or later. Zero Trust Access reduces the attack surface by hiding applications, and expands your level of knowing, understanding, and controlling who and what is on your network.

Cisco Secure Endpoint

With Cisco Secure Client 5, the former AMP for Endpoints client has been unified into Cisco Secure Client, functioning as a full module and leveraging the same user interface as other modules. The Cisco Secure Endpoint Cloud, XDR Client Management, and stand-alone Cisco Secure Client Cloud Management can all deploy Cisco Secure Client with Cisco Secure Endpoint. This integration enables customers to reduce the number of clients they need to manage.

Cloud Management Module

XDR Client Management and stand-alone Cisco Secure Client Cloud Management for Cisco Secure Client 5 and greater enable administrators to create cloud managed deployments of Cisco Secure Client. This deployment configuration offers the option to download a lightweight bootstrapper, containing only the necessary information for the endpoint to connect to the cloud and receive the specified Cisco Secure Client and modules along with their associated profiles. A full installer is also available. In either case, administrators distribute the installers to the endpoints using their preferred software distribution method.

Network Visibility Module

The Network Visibility Module (NVM) provides a continuous stream of high-value endpoint telemetry, enabling organizations to monitor endpoint and user behaviors on their networks. It gathers flow data from endpoints both on- and off-premises, along with essential context such as users, applications, devices, locations, and destinations. This data is cached and sent to the Network Visibility Module Collector when the endpoint is connected to a trusted network (either the corporate network on-premises or via VPN).

The Network Visibility Module Collector is a server that receives Internet Protocol Flow Information Export (IPFIX) data, optionally filters it, and then exports it to Cisco Secure Network Analytics Endpoint License, syslog, or collectors like Splunk for on-premises collection. It processes received messages that adhere to the nvzFlow protocol specification and sends flow information only when on a trusted network. By default,

no data is collected; data is collected only when configured in the profile. If collection occurs on an untrusted network, the data is cached and sent once the endpoint connects to a trusted network.

NVM is a core component of Cisco XDR. By installing the XDR Default Deployment on your endpoints, you can send telemetry directly to Cisco XDR without the need for an on-premises collector. Cisco XDR uses this data to create new detections, correlate multiple events into a single incident, and fill visibility gaps in your network.

Umbrella Roaming Security module

The Umbrella Roaming Security module requires a subscription to an Umbrella Roaming Security service, available with the Professional, Insights, Platform, or MSP package. This module provides DNS-layer security when no VPN is active, and a Cisco Umbrella subscription includes Intelligent Proxy. Additionally, Cisco Umbrella subscriptions offer content filtering, multiple policies, robust reporting, Active Directory integration, and more. The same Umbrella Roaming Security module is used regardless of the subscription level.

ISE Posture module

ISE Posture conducts a client-side evaluation. The client receives the posture requirement policy from the headend, gathers the necessary posture data, compares the results against the policy, and sends the assessment results back to the headend. Although ISE ultimately determines the endpoint's compliance status, it depends on the endpoint's own evaluation of the policy.

Network Access Manager

Network Access Manager is client software exclusively for Windows that ensures a secure Layer 2 network in line with its policies. It detects and selects the optimal Layer 2 access network and performs device authentication for access to both wired and wireless networks. Network Access Manager handles user and device identity as well as the network access protocols necessary for secure access. It operates intelligently to prevent end users from making connections that violate administrator-defined policies.

Secure Firewall Posture

Secure Firewall Posture, previously known as HostScan, is a package that installs on the remote device after the user connects to the Secure Firewall ASA but before the user logs in. Secure Firewall Posture can include any combination of the basic module, the endpoint assessment module, and the advanced endpoint assessment module. Note that Secure Firewall Posture is not supported on mobile devices such as Android, iOS, ChromeOS, or UWP.

Thousand Eyes

The ThousandEyes Endpoint Agent is an application that gathers network and application-layer performance data when users access specific websites from within monitored networks. It enhances customers' ability to gain a comprehensive view of their application health, enabling them to make better-informed decisions and resolve issues more quickly. When ThousandEyes is installed within Secure Client, its version is displayed in the Secure Client About box upon detection. The ThousandEyes agent, as part of Cisco Secure Client, is installed using the pre-deployment method.

Remote-Access VPN	
Feature	Benefits and Details
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: Initial CISCO SECURE CLIENT5.0 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
Software access	• Downloads are available in the Cisco.com Software Center • Technical support and software entitlement for Cisco Secure Client is included Premier and Advantage licensing • The contract number must be linked to Cisco.com ID. See the Secure Client Ordering Guide
Optimized network access: VPN protocol choice SSL (TLS and DTLS); IPsec IKEv2	• Cisco Secure Client 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

Remote-Access VPN	
Feature	Benefits and Details
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	Pre-deploy—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 XDR and Cisco Secure Client Cloud Management: Cisco Secure Client 5.0 can be deployed from the cloud using customizable deployment options
Wide range of authentication options	**Protocols:** • SAML 2.0 with Embedded or Native Browser (SSO) • RADIUS • LDAP • Certificate • TACACS+ • HTTP Form

Remote-Access VPN	
Feature	Benefits and Details
	Headend Methods AAA AAA and Certificate Certificate Only SAML Multiple Certificates and AAA • Multiple Certificates
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
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
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, Google Android, and Samsung Knox

Remote-Access VPN	
Feature	Benefits and Details
	IP address assignment mechanisms: • Static • Internal pool • Dynamic Host Configuration Protocol (DHCP) • RADIUS/Lightweight Directory Access Protocol (LDAP)
Robust unified endpoint compliance	• 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) with Identity Services Engine Premier 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 Secure Firewall Posture (Formerly HostScan) Support Charts for detailed information
Client firewall policy	• Provides added protection for split-tunneling configurations • Used in conjunction with the AnyConnect module 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 macOS platforms

Remote-Access VPN	
Feature	Benefits and Details
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)
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 also offers Administrators the ability to deploy and manage via Client Management (available via Cisco XDR or standalone) • 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

Remote-Access VPN	
Feature	**Benefits and Details**
Profile editor	• AnyConnect policies may be customized directly from Cisco Adaptive Security Device Manager (ASDM) • Stand-alone Profile Editor • XDR Client Management or Cisco Secure Client Cloud Management: The profile configuration page includes settings for Cloud Management functionality and various client modules, such as ISE Posture, Network Visibility Module, Cisco Secure Endpoint, Customer Experience Feedback, and VPN
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	
Feature	**Benefits and Details**
Cisco Umbrella Roaming (Cisco Umbrella Roaming license required)	• The Umbrella Roaming Security module requires a subscription to the Umbrella Roaming Security service, which can be obtained through DNS Security Essentials, DNS Security Advantage, SIG Essentials, or SIG Advantage plans. This module offers DNS-layer security when no VPN is active. A Cisco Umbrella subscription enhances this with Intelligent Proxy capabilities. Additionally, Cisco Umbrella subscriptions offer features such as content filtering, multiple policy management, comprehensive reporting, Active Directory integration, and more. The same Umbrella Roaming Security module is utilized across all subscription plans • 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)

Secure Mobility and Network Visibility	
Feature	Benefits and Details
Network Visibility Module	▪ Capture endpoint flows with detailed information about users, endpoints, applications, locations, and destinations ▪ Enable flexible collection settings for both on-premises and off-premise environments ▪ Monitor application usage to uncover potential behavioral anomalies ▪ Facilitate more informed network design decisions ▪ Share usage data with NetFlow analysis tools, such as Cisco Network Analytics
Cisco Secure Endpoint (Cisco Secure Endpoints licensed separately)	▪ Cisco Secure Client 5 is a unified agent that integrates the functionalities of the former AnyConnect and AMP for Endpoints, now known as Cisco Secure Endpoint. In its initial release, available exclusively for Windows, administrators can leverage a single agent to deliver both Cisco Secure Client and Cisco Secure Endpoint functionalities through a unified client and user interface ▪ 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
ThousandEyes	▪ Licensed separately the Endpoint Agent is an application designed to collect performance data at both the network and application layers when users access specific websites within monitored networks ▪ This tool enhances customers' ability to gain a comprehensive view of their application health, enabling them to make more informed decisions and resolve issues more swiftly ▪ When ThousandEyes is installed within the Secure Client, its version is displayed in the Secure Client About box upon detection

Network Access Manager and 802.1X	
Feature	Benefits and Details
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
Wireless encryption protocols	• WEP: (Wired Equivalent Privacy • WPA: (Wi-Fi Protected Access) • WPA2: Advanced Encryption Standard (AES) for encryption support • WPA3: CCMP-128 and GCMP-256 support • Enhanced Open: Provides unauthenticated data encryption to users, an improvement over traditional open networks with no protection at all. It is based on Opportunistic Wireless Encryption (OWE) Please refer to the Cisco Secure Client Release Notes for the latest support information.
Session resumption	• RFC2716 (EAP-TLS) session resumption using EAP-TLS, EAP-FAST, EAPPEAP, 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	• Allows only a single connection to the network disconnecting all others • No bridging between adapters • Ethernet connections automatically take priority

Network Access Manager and 802.1X	
Feature	**Benefits and Details**
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

Zero Trust Access (ZTA Module)	
Feature	**Benefits and Details**
Zero Trust Access Module	• When you see “Enrolled in Zero Trust Access” in the Cisco Secure Client Tile, it indicates that Zero Trust Access is enabled and running • This access model focuses on knowing, understanding, and controlling who and what is on your network. By definitively identifying users, the appropriate level of access is granted based on their role or function, and the network rights associated with those roles

Zero Trust Access (ZTA Module)	
Feature	**Benefits and Details**
	• Beyond the traditional AnyConnect VPN, Zero Trust Access offers more granular control and a secure user experience for a comprehensive network solution. Unlike VPNs, which may trust any entity that passes network control, the Zero Trust Access approach does not trust any user or device until it is verified. No one is automatically trusted; once verified, users are granted limited access and are subject to continuous re-verification • This model extends the zero-trust principle beyond the network, reducing the attack surface by concealing applications from the internet and ensuring that only authenticated and authorized users can access network resources
ZTNA Support	• Currently supported by the Cisco Secure Access solution.
System Requirements	• Supported on Windows 10 and 11 (TPM-enabled devices) and macOS 11, 12, 13, and 14 (TPM-enabled devices) • Windows devices must be running on systems that include Trusted Platform Module version 2.0 • macOS devices must be running on systems that include a Secure Enclave such as MacBook Pro computers with Touch Bar (2016 and 2017) that contain the Apple T1 chip • Intel-based Mac computers that contain the Apple T2 Security chip, or Mac computers with Apple silicon • You must have Windows WebView2 installed if you are going to use the Zero Trust Access Module, and you must deploy it out of band • If you are pre-deploying Zero Trust Access on macOS 11 or greater, refer to Additional Duo Desktop Requirements on macOS 11 (and later) for additional requirements • iOS/iPadOS 17.2 (or later) • Samsung device running Android version 14+ and Samsung Knox 3.10 or higher
Cisco Secure Client	• Please refer to the Cisco Secure Client Release Notes for the latest support information Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1 - Cisco

Platform compatibility

Cisco Secure Client compatibility with Cisco Secure Firewall ASA
Cisco Secure Firewall ASA Compatibility - Cisco

Cisco Secure Client compatibility with Cisco Secure Firewall Threat Defense
Cisco Secure Firewall Threat Defense Compatibility Guide - Cisco

Cisco Secure Client compatibility with Meraki
AnyConnect on the MX Appliance - Cisco Meraki Documentation

Cisco Secure Client compatibility with Cisco IOS
Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1 - Cisco

Limitations of Cisco Secure Client on Cisco IOS
Features Not Supported on the Cisco IOS SSL VPN

Cisco IOS Feature Navigator

Licensing options

Cisco Secure Client requires Premier or Advantage licensing.

Please see the Secure Client Ordering Guide
Products - Cisco Secure Client Ordering Guide - Cisco

Cisco Capital

Cisco Capital payment solutions

Cisco Capital flexible payment solutions offer choices so you get the tech you need and the business outcomes you want. Faster.

Cisco Capital Finance and Flexible Payment Solutions - Cisco

For more information

- Cisco Secure Client Homepage: Secure Client (including AnyConnect) - Cisco
- Cisco Secure Client documentation: Cisco Secure Client 5 - Cisco
- Cisco Secure Client Release Notes: Release Notes for Cisco Secure Client (including AnyConnect), Release 5.1 - Cisco
- Privacy information and Licensing https://trustportal.cisco.com/c/r/ctp/home.html

C78-4684586-00 09/24