

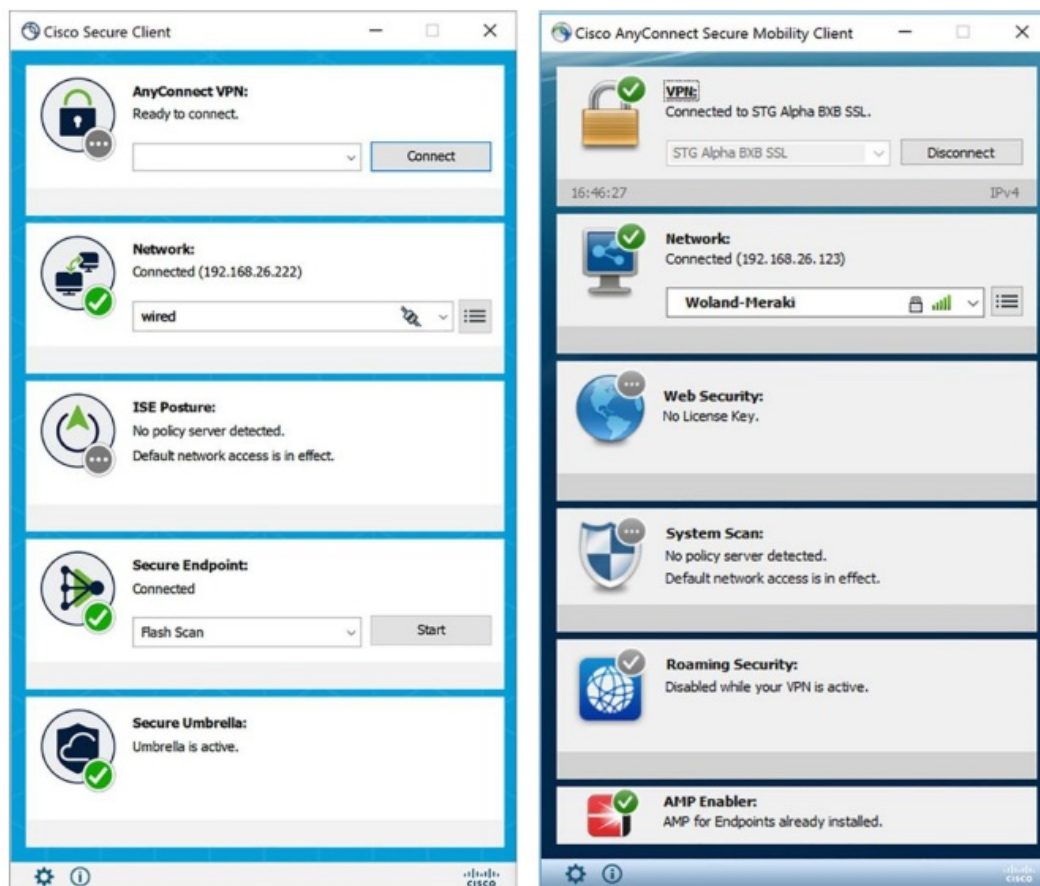


Contents [[hide](#)]

- [1 CISCO Secure Client Including Any Connect](#)
- [2 Product Information](#)
- [3 Supported Operating Systems](#)
- [4 Supported Cryptographic Algorithms](#)
- [5 License Options](#)
- [6 Feature Matrix](#)
- [7 Interfaces](#)
- [8 Documents / Resources](#)
 - [8.1 References](#)



CISCO Secure Client Including Any Connect



Product Information

Specifications

- Product Name: Cisco Secure Client
- Release Version: 5.x
- First Published: 2025-03-31

Cisco Secure Client (including AnyConnect) Features, License, and OSs, Release 5.x

This document identifies the Cisco Secure Client release 5.1 features, license requirements, and endpoint operating systems that are supported in the Secure Client (including AnyConnect). It also includes supported cryptographic algorithms and accessibility recommendations.

Supported Operating Systems

Cisco Secure Client 5.1 supports the following operating systems.

Windows

- Windows 11 (64-bit)
- Microsoft-supported versions of Windows 11 for ARM64-based PCs (Supported only in VPN client, DART, Secure Firewall Posture, Network Visibility Module, Umbrella Module, ISE Posture, and Zero Trust Access Module)
- Windows 10 x86(32-bit) and x64 (64-bit)

macOS (64-bit only)

- macOS 15 Sequoia
- macOS 14 Sonoma
- macOS 13 Ventura

Linux

- **Red Hat:** 9.x and 8.x (except ISE Posture Module, which only supports 8.1 (and later))
- **Ubuntu:** 24.04, 22.04, and 20.04
- **SUSE (SLES)**
 - **VPN:** Limited support. Used only to install ISE Posture.
 - Not supported for Secure Firewall Posture or Network Visibility Module.
 - **ISE Posture:** 12.3 (and later) and 15.0 (and later)
- See the Release Notes for Cisco Secure Client for OS requirements and support notes. See the Offer Descriptions and Supplemental Terms for licensing terms and conditions, and a breakdown of orderability and the specific terms and conditions of the various licenses.
- See the Feature Matrix below for license information and operating system limitations that apply to Cisco Secure Client modules and features.

Supported Cryptographic Algorithms

The following table lists the cryptographic algorithms supported by Cisco Secure Client. The cryptographic algorithms and cipher suites are shown in the order of preference, most to least. This preference order is dictated by Cisco's Product Security Baseline to which all Cisco products must comply. Note that the PSB requirements change from time to time so the cryptographic algorithms supported by subsequent versions of Secure Client will change accordingly.

TLS 1.3, 1.2, and DTLS 1.2 Cipher Suites (VPN)

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

TLS 1.2 Cipher Suites (Network Access Manager)

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA

TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
-------------------------------	--------------

DTLS 1.0 Cipher Suites (VPN)

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

IKEv2/IPsec Algorithms

Encryption

- ENCR_AES_GCM_256
- ENCR_AES_GCM_192
- ENCR_AES_GCM_128
- ENCR_AES_CBC_256
- ENCR_AES_CBC_192

- ENCR_AES_CBC_128

Pseudo Random Function

- PRF_HMAC_SHA2_256
- PRF_HMAC_SHA2_384
- PRF_HMAC_SHA2_512
- PRF_HMAC_SHA1

Diffie-Hellman Groups

- DH_GROUP_256_ECP – Group 19
- DH_GROUP_384_ECP – Group 20
- DH_GROUP_521_ECP – Group 21
- DH_GROUP_3072_MODP – Group 15
- DH_GROUP_4096_MODP – Group 16

Integrity

- AUTH_HMAC_SHA2_256_128
- AUTH_HMAC_SHA2_384_192
- AUTH_HMAC_SHA1_96
- AUTH_HMAC_SHA2_512_256

License Options

- Use of the Cisco Secure Client 5.1 requires that you purchase either a Premier or Advantage license. The license(s) required depends on the Secure Client features that you plan to use, and the number of sessions that you want to support. These user-based licenses include access to support, and software updates that align with general BYOD trends.
- Secure Client 5.1 licenses are used with Cisco Secure Firewall Adaptive Security Appliances (ASA), Integrated Services Routers (ISR), Cloud Services Routers (CSR), and Aggregated Services Routers (ASR), as well as other non-VPN headend such as Identity Services Engine (ISE). A consistent model is used regardless of the headend,

so there is no impact when headend migrations occur.

One or more of the following Cisco Secure licenses may be required for your deployment:

License	Description
Advantage	Supports basic Secure Client features such as VPN functionality for PC and mobile platforms (Secure Client and standards-based IPsec IKEv2 software clients), FIPS, basic endpoint context collection, and 802.1x Windows supplicant.
Premier	Supports all basic Secure Client Advantage features in addition to advanced features such as Network Visibility Module, clientless VPN, VPN posture agent, unified posture agent, Next Generation Encryption/Suite B, SAML, all plus services and flex licenses.
VPN Only (Perpetual)	Supports VPN functionality for PC and mobile platforms, clientless (browser-based) VPN termination on Secure Firewall ASA, VPN-only compliance and posture agent in conjunction with ASA, FIPS compliance, and next-generation encryption (Suite B) with Secure Client and third-party IKEv2 VPN clients. VPN only licenses are most applicable to environments wanting to use Secure Client exclusively for remote access VPN services but with high or unpredictable total user counts. No other Secure Client function or service (such as Cisco Umbrella Roaming, ISE Posture, Network Visibility module, or Network Access Manager) is available with this license.

Advantage and Premier License

- From the Cisco Commerce Workspace website, choose the service tier (Advantage or Premier) and the length of term (1, 3, or 5 year). The number of licenses that are needed is based on the number of unique or authorized users that will make use of Secure Client. Secure Client is not licensed based on simultaneous connections. You can mix Advantage and Premier licenses in the same environment, and only one license is required for each user.
- Cisco Secure 5.1 licensed customers are also entitled to earlier AnyConnect releases.

Feature Matrix

Cisco Secure 5.1 modules and features, with their minimum release requirements, license requirements, and supported operating systems are listed in the following sections:

Cisco Secure Client Deployment and Configuration

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Deferred Upgrades	ASA 9.0 ASDM 7.0	Advantage	yes	yes	yes
Windows Services Lock down	ASA 8.0(4) ASDM 6.4(1)	Advantage	yes	no	no
Update Policy, Software and Profile Lock	ASA 8.0(4) ASDM 6.4(1)	Advantage	yes	yes	yes

Auto Update	ASA 8.0(4) ASDM 6.3(1))	Advantage	yes	yes	yes
Pre-deployment	ASA 8.0(4) ASDM 6.3(1))	Advantage	yes	yes	yes
Auto Update Client Profiles	ASA 8.0(4) ASDM 6.4(1))	Advantage	yes	yes	yes
Cisco Secure Client Profile Editor	ASA 8.4(1) ASDM 6.4(1))	Advantage	yes	yes	yes
User Controllable Features	ASA 8.0(4) ASDM 6.3(1))	Advantage	yes	yes	yes*

* Ability to minimize Secure Client on VPN connect, or block connections to untrusted servers

AnyConnect VPN Core Features

Feature	Minimum ASA/ASDM Release	License Re quired	Window s	macOS	Linux
SSL (TLS & DTLS), including	ASA 8.0(4)	Advantage	yes	yes	yes
Per App VPN	ASDM 6.3(1)				
SNI (TLS & DTLS)	n/a	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Re quired	Window s	macOS	Linux
TLS Compression	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
DTLS fallback to TLS	ASA 8.4.2.8 ASDM 6.3(1)	Advantage	yes	yes	yes

IPsec/IKEv2	ASA 8.4(1) ASDM 6.4(1)	Advantage	yes	yes	yes
Split tunneling	ASA 8.0(x) ASDM 6.3(1)	Advantage	yes	yes	yes
Dynamic Split Tunneling	ASA 9.0	Advantage, Premier, or VPN-only	yes	yes	no
Enhanced Dynamic Split Tunneling	ASA 9.0	Advantage	yes	yes	no
Both dynamic exclusion from and dynamic inclusion into a tunnel	ASA 9.0	Advantage	yes	yes	no
Split DNS	ASA 8.0(4) ASDM 6.3(1)	Advantage	Yes	Yes	No
Ignore Browser Proxy	ASA 8.3(1) ASDM 6.3(1)	Advantage	yes	yes	no
Proxy Auto Config (PAC) file generation	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no

Internet Explorer Connections tab lockdown	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Optimal Gateway Selection	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	no
Global Site Selector (GSS) compatibility	ASA 8.0(4) ASDM 6.4(1)	Advantage	yes	yes	yes
Local LAN Access	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Tethered device access via client firewall rules, for synchronization	ASA 8.3(1) ASDM 6.3(1)	Advantage	yes	yes	yes

Local printer access via client firewall rules	ASA 8.3(1) ASDM 6.3(1)	Advantage	yes	yes	yes
IPv6	ASA 9.0 ASDM 7.0	Advantage	yes	yes	no
Further IPv6 implementation	ASA 9.7.1 ASDM 7.7.1	Advantage	yes	yes	yes
Certificate Pinning	no dependency	Advantage	yes	yes	yes
Management VPN tunnel	ASA 9.0 ASDM 7.10.1	Premier	yes	yes	no

Connect and Disconnect Features

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Fast User Switching	n/a	n/a	yes	no	no

Simultaneous	ASA8.0(4)	Premier	Yes	Yes	Yes
Clientless & Secure Client connections	ASDM 6.3(1)				
Start Before	ASA 8.0(4)	Advantage	yes	no	no
Logon (SBL)	ASDM 6.3(1)				
Run script on connect & disconnect	ASA 8.0(4)	Advantage	yes	yes	yes
connect & disconnect	ASDM 6.3(1)				
Minimize on connect	ASA 8.0(4)	Advantage	yes	yes	yes
connect	ASDM 6.3(1)				
Auto connection	ASA 8.0(4)	Advantage	yes	yes	yes
start	ASDM 6.3(1)				

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
---------	--------------------------	------------------	---------	-------	-------

Auto reconnect	ASA 8.0(4)	Advantage	yes	yes	no
(disconnect on system suspend, reconnect on system resume)	ASDM 6.3(1)				
Remote User	ASA 8.0(4)	Advantage	yes	no	no
VPN Establishment (permitted or denied)	ASDM 6.3(1)				
Logon Enforcement (terminate VPN)	ASA 8.0(4)	Advantage	yes	no	no
	ASDM 6.3(1)				

session if					
another user logs					
in)					
Retain VPN	ASA 8.0(4)	Advantage	yes	no	no
session (when user logs off,	ASDM 6.3(1)				
and then when					
this or another					
user logs in)					
Trusted Network	ASA 8.0(4)	Advantage	yes	yes	yes
Detection (TND)	ASDM 6.3(1)				
Always on (VPN	ASA 8.0(4)	Advantage	yes	yes	no
must be connected to	ASDM 6.3(1)				

access net work)					
Always on	ASA 8.3(1)	Advantage	yes	yes	no
exemption v ia DAP	ASDM 6.3(1)				
Connect Fai lure	ASA 8.0(4)	Advantage	yes	yes	no
Policy (Inter net access allowed	ASDM 6.3(1)				
or disallowe d if					
VPN connection					
fails)					
Captive Por tal	ASA 8.0(4)	Advantage	yes	yes	yes
Detection	ASDM 6.3(1)				

Feature	Minimum A SA/ASDM Release	License Re quired	Windows	macOS	Linux
Captive Por tal	ASA 8.0(4)	Advantage	yes	yes	no

Remediation	ASDM 6.3(1)				
Enhanced Captive Portal Remediation	no dependency	Advantage	yes	yes	no
Dual-home Detection	no dependency	n/a	yes	yes	yes

Authentication and Encryption Features

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Certificate only authentication	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
RSA SecurID /SoftID integration	no dependency	Advantage	yes	no	no
Smartcard support	no dependency	Advantage	yes	yes	no
SCEP (requires Posture Module if Machine ID is used)	no dependency	Advantage	yes	yes	no
List & select certificates	no dependency	Advantage	yes	no	no

FIPS	no dependence	Advantage	yes	yes	yes
SHA-2 for IPsec IKEv2 (Digital Signatures, Integrity, & PRF)	ASA 8.0(4) ASDM 6.4(1)	Advantage	yes	yes	yes
Strong Encryption (AES-256 & 3des-168)	no dependence	Advantage	Yes	Yes	Yes
NSA Suite-B (IPsec only)	ASA 9.0 ASDM 7.0	Premier	yes	yes	yes
Enable CRL check	no dependence	Premier	yes	no	no
SAML 2.0 SSO	ASA 9.7.1 ASDM 7.7.1	Premier or VPN only	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Enhanced SAML 2.0	ASA 9.7.1.24 ASA 9.8.2.28 ASA 9.9.2.1	Premier or VPN only	yes	yes	yes

External Browser SAM L Package for Enhanced Web Authentication	ASA 9.17.1 ASDM 7.17.1	Premier or VPN only	yes	yes	yes
Multiple-certificate authentication	ASA 9.7.1 ASDM 7.7.1	Advantage, Premier, or VPN only	yes	yes	yes

Interfaces

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
GUI	ASA 8.0(4)	Advantage	yes	yes	yes
Command Line	ASDM 6.3(1)	n/a	yes	yes	yes
API	no dependency	n/a	yes	yes	yes
Microsoft Component Object Module (COM)	no dependency	n/a	yes	no	no
Localization of User Messages	no dependency	n/a	yes	yes	yes
Custom MSI transforms	no dependency	n/a	yes	no	no
User-defined resource files	no dependency	n/a	yes	yes	no

Client Help	ASA 9.0 ASDM 7.0	n/a	yes	yes	no
-------------	---------------------	-----	-----	-----	----

Secure Firewall Posture (Formerly HostScan) and Posture Assessment

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Endpoint Assessment	ASA 8.0(4)	Premier	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Endpoint Remediation	ASDM 6.3(1)	Premier	yes	yes	yes
Quarantine	no dependency	Premier	yes	yes	yes
Quarantine status & terminate message	ASA 8.3(1) ASDM 6.3(1)	Premier	yes	yes	yes
Secure Firewall Posture Package Update	ASA 8.4(1) ASDM 6.4(1)	Premier	yes	yes	yes

Host Emulation Detection	no dependency	Premier	yes	no	no
OPSWAT v4	ASA 9.9(1) ASDM 7.9(1)	Premier	yes	yes	yes
Disk Encryption	ASA 9.17(1) ASDM 7.17(1)	n/a	yes	yes	yes
AutoDART	no dependency	n/a	yes	yes	yes

ISE Posture

Feature	Minimum Secure Client Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
ISE Posture CLI	5.0.01xx	no dependency	no dependency	n/a	yes	no	no
Posture State Synchronization	5.0	no dependency	3.1	n/a	yes	yes	yes

Change of Authorization (CoA)	5.0	ASA 9.2 .1 ASDM 7 .2.1	2.0	Advantage	yes	yes	yes
ISE Posture Profile Editor	5.0	ASA 9.2 .1 ASDM 7 .2.1	no dependency	Premier	yes	yes	yes
AC Identity Extensions (ACIDex)	5.0	no dependency	2.0	Advantage	yes	yes	yes

Feature	Minimum Secure Client Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
ISE Posture Module	5.0	no dependency	2.0	Premier	yes	yes	yes
Detection of USB mass storage devices (v4 only)	5.0	no dependency	2.1	Premier	yes	no	no
OPSWAT v4	5.0	no dependency	2.1	Premier	yes	yes	no
Stealth Agent for Posture	5.0	no dependency	2.2	Premier	yes	yes	no

Continuous endpoint monitoring	5.0	no dependency	2.2	Premier	yes	yes	no
Next-generation provisioning and discovery	5.0	no dependency	2.2	Premier	yes	yes	no
Application kill and uninstall capabilities	5.0	no dependency	2.2	Premier	yes	yes	no
Cisco Temporal Agent	5.0	no dependency	2.3	ISE Premier	yes	yes	no
Enhanced SCCM approach	5.0	no dependency	2.3	Premier: Secure Client and ISE	yes	no	no
Posture policy enhancements for optional mode	5.0	no dependency	2.3	Premier: Secure Client and ISE	yes	yes	no
Periodic probe interval in profile editor	5.0	no dependency	2.3	Premier: Secure Client and ISE	yes	yes	no

Visibility into hardware inventory	5.0	no dependency	2.3	Premier: Secure Client and ISE	yes	yes	no
------------------------------------	-----	---------------	-----	-----------------------------------	-----	-----	----

Feature	Minimum Secure Client Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Grace period for noncompliant devices	5.0	no dependency	2.4	Premier: Secure Client and ISE	yes	yes	no
Posture rescanning	5.0	no dependency	2.4	Premier: Secure Client and ISE	yes	yes	no
Secure Client stealth mode notifications	5.0	no dependency	2.4	Premier: Secure Client and ISE	yes	yes	no
Disabling UAC prompt	5.0	no dependency	2.4	Premier: Secure Client and ISE	yes	no	no

Enhanced grace period	5.0	no dependency	2.6	Premier: Secure Client and ISE	yes	yes	no
Custom notification controls and revamp of remediation windows	5.0	no dependency	2.6	Premier: Secure Client and ISE	yes	yes	no
End-to-end agentless posture flow	5.0	no dependency	3.0	Premier: Secure Client and ISE	yes	yes	no

Network Access Manager

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Core	ASA 8.4(1) ASDM 6.4(1)	Advantage	yes	no	no

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
---------	--------------------------	------------------	---------	-------	-------

Wired support IEEE 802.3	no dependency	n/a	yes	no	no
Wireless support IEEE 802.11	no dependency	n/a	yes	no	no
Pre-logon & Single Sign on Authentication	no dependency	n/a	yes	no	no
IEEE 802.1X	no dependency	n/a	yes	no	no
IEEE 802.1AE MAC sec	no dependency	n/a	yes	no	no
EAP methods	no dependency	n/a	yes	no	no
FIPS 140-2 Level 1	no dependency	n/a	yes	no	no
Mobile Broadband support	ASA 8.4(1) ASDM 7.0	n/a	yes	no	no
IPv6	ASDM 9.0	n/a	yes	no	no
NGE and NSA Suite-B	ASDM 7.0	n/a	yes	no	no
TLS 1.2 for VPN connectivity*	no dependency	n/a	yes	no	no

WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support	no dependency	n/a	yes	no	no
--	---------------	-----	-----	----	----

*If you are using ISE as a RADIUS server, note the following guidelines.

- ISE started support for TLS 1.2 in release 2.0. Network Access Manager and ISE will negotiate to TLS 1.0 if you have Cisco Secure Client with TLS 1.2 and an ISE release prior to 2.0. Therefore, if you use Network Access Manager and EAP-FAST with ISE 2.0 (or later) for RADIUS servers, you must upgrade to the appropriate release of ISE as well.
- Incompatibility warning: If you are an ISE customer running 2.0 or higher, you must read this before proceeding!
- The ISE RADIUS has supported TLS 1.2 since release 2.0, however there is a defect in the ISE implementation of EAP-FAST using TLS 1.2 tracked by CSCvm03681. The defect has been fixed in the 2.4p5 release of ISE.
- If NAM is used to authenticate using EAP-FAST with any ISE releases that support TLS 1.2 prior to the above releases, the authentication will fail and the endpoint will not have access to the network.

AMP Enabler

Feature	Minimum ASA/ASDM Release	Minimum ISE Release	License	Windows	macOS	Linux

AMP Enabler	ASDM 7.4.2 ASA 9.4.1	ISE 1.4	Advantage	n/a	yes	n/a
-------------	-------------------------	---------	-----------	-----	-----	-----

Network Visibility Module

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Network Visibility Module	ASDM 7.5.1 ASA 9.5.1	Premier	yes	yes	yes
Adjustment to the rate at which data is sent	ASDM 7.5.1 ASA 9.5.1	Premier	yes	yes	yes
Customization of NVM timer	ASDM 7.5.1 ASA 9.5.1	Premier	yes	yes	yes
Broadcast and multicast option for data collection	ASDM 7.5.1 ASA 9.5.1	Premier	yes	yes	yes
Creation of anonymization profiles	ASDM 7.5.1 ASA 9.5.1	Premier	yes	yes	yes

Broader data collection and anonymization with hashing	ASDM 7.7.1 ASA 9.7.1	Premier	yes	yes	yes
Support for Java as a container	ASDM 7.7.1 ASA 9.7.1	Premier	yes	yes	yes
Configuration of cache to customize	ASDM 7.7.1 ASA 9.7.1	Premier	yes	yes	yes
Periodic flow reporting	ASDM 7.7.1 ASA 9.7.1	Premier	yes	yes	yes
Flow filter	no dependency	Premier	yes	yes	yes
Standalone NVM	no dependency	Premier	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Integration with Secure Cloud Analytics	no dependency	n/a	yes	no	no
Process Tree Hierarchy	no dependency	n/a	yes	yes	yes

Secure Umbrella Module

Secure Umbrella Module	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Secure Umbrella	ASDM 7.6.2	ISE 2.0	Either	yes	yes	no
Module	ASA 9.4.1		Advantage or Premier			
			Umbrella			
			licensing is			
			mandatory			
Umbrella Secure Web Gateway	no dependency	no dependency	n/a	yes	yes	no
OpenDNS IPv6 support	no dependency	no dependency	n/a	yes	yes	no

For information on Umbrella licensing, see <https://www.opendns.com/enterprise-security/threat-enforcement/packages/>

Thousand Eyes Endpoint Agent Module

Feature	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Endpoint Agent	no dependency	no dependency	n/a	yes	yes	no

Customer Experience Feedback

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Customer Experience Feedback	ASA 8.4(1) ASDM 7.0	Advantage	yes	yes	no

Diagnostic and Report Tool (DART)

Log Type	License Required	Windows	macOS	Linux
VPN	Advantage	yes	yes	yes
Cloud Management	n/a	yes	yes	no
Duo Desktop	n/a	yes	yes	no
Endpoint Visibility Module	n/a	yes	no	no

ISE Posture	Premier	yes	yes	yes
Network Access Manager	Premier	yes	no	no
Network Visibility Module	Premier	yes	yes	yes
Secure Firewall Posture	Premier	yes	yes	yes
Secure Endpoint	n/a	yes	yes	no
ThousandEyes	n/a	yes	yes	no
Umbrella	n/a	yes	yes	no
Zero Trust Access Module	n/a	yes	yes	no

Accessibility Recommendations

We are committed to enhancing accessibility and to providing a seamless experience for all users, by adhering to specific Voluntary Product Accessibility Template (VPAT) compliance standards. Our product is designed to integrate effectively with various accessibility tools, ensuring it is both user-friendly and accessible to individuals with specific needs.

JAWS Screen Reader

For Windows users, we recommend using the JAWS screen reader and its capabilities to assist those with disabilities. JAWS (Job Access with Speech) is a powerful screen reader that provides audio feedback and keyboard shortcuts for users with visual impairments. It allows users to navigate through applications and websites using speech output and braille displays. By integrating with JAWS, our product ensures that visually impaired users can efficiently access and interact with all features, enhancing their overall productivity and user experience.

Windows Operating System Accessibility Tools

Windows Magnifier

The Windows Magnifier tool allows users to enlarge on-screen content, improving visibility for those with low vision. Users can zoom in and out easily, ensuring that text and images are clear and readable.

On Windows, set your display resolution to at least 1280px x 1024px. You can zoom to 400% by changing the Scaling on Display setting and view one or two module tiles in Secure Client. To zoom in above 200%, the Secure Client Advanced Window contents may not be fully available (depending on your monitor size). We do not support Reflow, which is typically used on content-based web pages and publications and also known as Responsive Web Design.

Invert Colors

The invert colors feature provides contrast themes (aquatic, dusk, and night sky) and Windows custom themes. The user needs to change Contrast Theme in the Windows setting to apply high contrast mode to Secure Client and make it easier for those with certain visual impairments to read and interact with on-screen elements.

Keyboard Navigation Shortcuts

Because Secure Client is not a content-based web application, it has its own controls and graphics within its UI. For efficient navigation, Cisco Secure Client supports various keyboard shortcuts. By following the below recommendations and using the described tools and shortcuts, users can enhance their interaction with Secure Client, ensuring a more accessible and efficient experience:


- **Tab Navigation:** Use the Tab key for individual panel navigation through the primary (tile) window, DART setup dialogs, and each module's sub dialogs. The Spacebar or Enter trigger the action. An item in focus is indicated as dark blue, and the indication of a shift in focus is portrayed with a frame around the control.
- **Module Selection:** Use the Up/Down arrow keys to navigate through specific modules on the left navigation bar.
- **Module Property Pages:** Use the Left/Right arrow keys to navigate between individual settings tabs, and then use the Tab key for panel navigation.

- **Advanced Window:** Use the Alt+Tab to choose it and Esc to close it.
- **Navigation** of Group Table List: Use PgUp/PgDn or Spacebar/Enter to expand or collapse a specific group.
- **Minimize/Maximize** the active Secure Client UI: Windows Logo key + Up/Down arrow.
- **About Dialog:** Use the Tab key to navigate through this page, and use the Spacebar to launch any available hyperlinks.




Frequently Asked Questions

- **Q: What operating systems are supported by Cisco Secure Client?**
 - A: Cisco Secure Client 5.1 supports Windows operating systems.
- **Q: How can I access licensing terms and conditions for Cisco Secure Client?**
 - A: Refer to the Offer Descriptions and Supplemental Terms provided in the documentation for detailed licensing information.
- **Q: What cryptographic algorithms are supported by Cisco Secure Client?**
 - A: The supported cryptographic algorithms include TLS 1.3, 1.2, and DTLS 1.2 Cipher Suites as well as TLS 1.2 Cipher Suites for Network Access Manager.

Documents / Resources

	<p>CISCO Secure Client Including Any Connect [pdf] User Guide</p> <p>Release 5.1, Secure Client Including Any Connect, Client Including Any Connect, Including Any Connect, Any Connect</p>
---	---

References

-  [Cisco Secure Client \(including AnyConnect\) - Release Notes - Cisco](#)
-  [Offer Descriptions and Supplemental Terms - Cisco](#)
-  [Cisco Umbrella Packages - Cisco Umbrella](#)
- [User Manual](#)

—Previous Post

CISCO Secure Network Analytics Deployment Instruction Manual

Next Post—

CISCO NCS 55A1-24Q6H-SS Crosswork Network Controller User Guide

Leave a comment

Your email address will not be published. Required fields are marked *

Comment *

Name

Email

Website

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search:

e.g. whirlpool wrf535swhz

Search

[Manuals+](#) | [Upload](#) | [Deep Search](#) | [Privacy Policy](#) | [@manuals.plus](#) | [YouTube](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.