Cisco Secure Client Features, Licenses, and OSs, Release 5.x

First Published: 2025-06-27

Last Modified: 2026-06-25

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 crytographic algorithms and accessibility recommendations.

Supported Operating Systems

Cisco Secure Client 5.1 supports the following operating systems.

Windows

- Current Microsoft supported versions of Windows 11 and Windows 10
- Microsoft-supported versions of Windows 11 for ARM64-based PCs (Not supported in Network Access Manager or ThousandEyes Endpoint Agent)
- Windows Server 2022: Supported for Network Visibility Module on-prem and XDR

macOS (64-bit only)

- macOS 27 Golden Gate: 5.1.20.333+
- macOS 26 Tahoe: 5.1.12.146+
- macOS 15 Sequoia: 5.1.6.103+

Linux (for x86_64)

- Red Hat: 10.x, 9.x, and 8.x
- Ubuntu: 26.04, 24.04, and 22.04
- SUSE supported versions of SLES 15
  - VPN: Limited support. Used only to install ISE Posture.
  - Not supported for Secure Firewall Posture, Network Visibility Module, or Zero Trust Access.

Linux (for ARM64)

- Red Hat 9.x and 8.x

- Ubuntu 24.04 and 22.04

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 cryptographical 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	ECDHA-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

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
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

Standard RFC Naming Convention	OpenSSL Naming Convention
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
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

Encyption

- 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 headends 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	Miniumum ASA/ASDM Release	License Required	Windows	macOS	Linux
Deferred Upgrades	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Windows Services Lockdown	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Update Policy, Software and Profile Lock	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Auto Update	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Pre-deployment	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Auto Update Client Profiles	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Cisco Secure Client Profile Editor	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
User Controllable Features	ASA 9.16 ASDM 7.16	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 Required	Windows	macOS	Linux
SSL (TLS & DTLS), including Per App VPN	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
SNI (TLS & DTLS)	n/a	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
TLS Compression	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
DTLS fallback to TLS	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
IPsec/IKEv2	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Split tunneling	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Dynamic Split Tunneling	ASA 9.16	Advantage, Premier, or VPN-only	yes	yes	no
Enhanced Dynamic Split Tunneling	ASA 9.16	Advantage	yes	yes	no
Both dynamic exclusion from and dynamic inclusion into a tunnel	ASA 9.16	Advantage	yes	yes	no
Split DNS	ASA 9.16 ASDM 7.16	Advantage	Yes	Yes	No
Ignore Browser Proxy	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Proxy Auto Config (PAC) file generation	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Internet Explorer Connections tab lockdown	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Optimal Gateway Selection	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Global Site Selector (GSS) compatibility	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Local LAN Access	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Tethered device access via client firewall rules, for synchronization	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Local printer access via client firewall rules	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
IPv6	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Further IPv6 implementation	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Certificate Pinning	no dependency	Advantage	yes	yes	yes
Management VPN tunnel	ASA 9.16 ASDM 7.16	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 Clientless & Secure Client connections	ASA 9.16 ASDM 7.16	Premier	Yes	Yes	Yes
Start Before Logon (SBL)	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Run script on connect & disconnect	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Minimize on connect	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Auto connect on start	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Auto reconnect (disconnect on system suspend, reconnect on system resume)	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Remote User VPN Establishment (permitted or denied)	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Logon Enforcement (terminate VPN session if another user logs in)	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Retain VPN session (when user logs off, and then when this or another user logs in)	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Trusted Network Detection (TND)	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Always on (VPN must be connected to access network)	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Always on exemption via DAP	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Connect Failure Policy (Internet access allowed or disallowed if VPN connection fails)	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
Captive Portal Detection	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Captive Portal Remediation	ASA 9.16 ASDM 7.16	Advantage	yes	yes	no
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 9.16 ASDM 7.16	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 dependency	Advantage	yes	yes	yes
SHA-2 for IPsec IKEv2 (Digital Signatures, Integrity, & PRF)	ASA 9.16 ASDM 7.16	Advantage	yes	yes	yes
Strong Encryption (AES-256 & 3des-168)	no dependency	Advantage	Yes	Yes	Yes
NSA Suite-B (IPsec only)	ASA 9.16 ASDM 7.16	Premier	yes	yes	yes
Enable CRL check	no dependency	Premier	yes	no	no
SAML 2.0 SSO	ASA 9.16 ASDM 7.16	Premier or VPN only	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Enhanced SAML 2.0	ASA 9.16	Premier or VPN only	yes	yes	yes
External Browser SAML Package for Enhanced Web Authentication	ASA 9.16 ASDM 7.16	Premier or VPN only	yes	yes	yes
Multiple-certificate authentication	ASA 9.16 ASDM 7.16	Advantage, Premier, or VPN only	yes	yes	yes

Interfaces

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
GUI	ASDM 7.16	Advantage	yes	yes	yes
Command Line	ASA 9.16	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 9.16 ASDM 7.16	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 9.16	Premier	yes	yes	yes
Endpoint Remediation	ASDM 7.16	Premier	yes	yes	yes
Quarantine	no dependency	Premier	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Quarantine status & terminate message	ASA 9.16 ASDM 7.16	Premier	yes	yes	yes
Secure Firewall Posture Package Update	ASA 9.16 ASDM 7.16	Premier	yes	yes	yes
Host Emulation Detection	no dependency	Premier	yes	no	no
OPSWAT v4	ASA 9.16 ASDM 7.16	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	5.0.01xxx	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 9.16 ASDM 7.16	2.0	Advantage	yes	yes	yes
ISE Posture Profile Editor	5.0	ASA 9.16 ASDM 7.16	no dependency	Premier	yes	yes	yes
AC Identity Extensions (ACIDex)	5.0	no dependency	2.0	Advantage	yes	yes	yes
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

Feature	Minimum Secure Client Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
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
Grace period for noncompliant devices	5.0	no dependency	2.4	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
Posture rescan	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
Continuous Reassessment	5.1.17	no dependency	3.5	n/a	yes	yes	yes

Network Access Manager

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Core	ASA 9.16 ASDM 7.16	Advantage	yes	no	no
Wired support IEEE 802.3	no dependency	n/a	yes	no	no

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
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 MACsec	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 9.16 ASDM 7.16	n/a	yes	no	no
IPv6	ASDM 9.0	n/a	yes	no	no
NGE and NSA Suite-B	ASDM 7.16	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.

Network Visibility Module

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Network Visibility Module	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Adjustment to the rate at which data is sent	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Customization of NVM timer	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Broadcast and multicast option for data collection	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Creation of anonymization profiles	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Broader data collection and anonymization with hashing	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Support for Java as a container	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Configuration of cache to customize	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Periodic flow reporting	ASDM 7.16 ASA 9.16	Premier	yes	yes	yes
Flow filter	no dependency	Premier	yes	yes	yes
Standalone NVM	no dependency	Premier	yes	yes	yes
Integration with Secure Cloud Analytics	no dependency	n/a	yes	yes	yes
Process Tree Hierarchy	no dependency	n/a	yes	yes	yes
Extension of Linux Kernel Capabilities	no dependency	n/a	n/a	n/a	yes
Interoperability with Zero Trust Access	no dependency	n/a	Yes	Yes	No

Secure Umbrella Module

Secure Umbrella Module	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Secure Umbrella Module	ASDM 7.16 ASA 9.16	ISE 2.0	Either Advantage or Premier Umbrella licensing is mandatory	yes	yes	no
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/

ThousandEyes 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

Zero Trust Access Module

Feature	Windows	macOS	Linux
Enrollment: SAML	Yes	Yes	Yes
Enrollment: Zero Trust	Yes (5.1.9+)	Yes (5.1.9+)	Yes
Posture: Basic ACIDEX	Yes	Yes	Yes
Posture: Duo Desktop Integration	Yes	Yes	No
Traffic Steering: SPA (CIDR/FQDN)	Yes	Yes	Yes
Traffic Steering: SPA (DNS)	Yes (5.1.11+)	Yes (5.1.11+)	Yes
Traffic Steering: UZTNA (1: cloud or local)	Yes (5.1.11+)	Yes (5.1.11+)	Yes

Feature	Windows	macOS	Linux
Traffic Steering: UZTNA (2: local only)	Yes (5.1.11+)	Yes (5.1.11+)	Yes
Traffic Steering: SIA-Lite (CIDR/FQDN)	Yes	Yes	Yes
Traffic Steering: SIA-Lite (CIDR/DNS)	Yes (5.1.11+)	Yes (5.1.11+)	Yes
Step-up Authentication	Yes	Yes	Yes
TND for SPA/SIA	Yes (5.1.10+)	Yes (5.1.10+)	Yes
TND: Criteria - DNS Server/Domain	Yes (5.1.10+)	Yes (5.1.10+)	Yes
TND: Criteria - Trusted Server	Yes (5.1.10+)	Yes (5.1.10+)	Yes
TND: Virtual interface detection	Yes (5.1.13+)	Yes (5.1.13+)	Yes
TND: Multiple interface evaluation	Yes (5.1.10+)	Yes (5.1.10+)	Yes
User Pause for SPA/SIA	Yes (5.1.13+)	Yes (5.1.13+)	Yes
Localized strings	Yes	Yes	Yes

Customer Experience Feedback

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Customer Experience Feedback	ASA 9.16 ASDM 7.16	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

Log Type	License Required	Windows	macOS	Linux
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	yes

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.

© 2026 Cisco Systems, Inc. All rights reserved.