Cisco Secure Client (including AnyConnect) Features, Licenses, and OSs, Release 5

This document identifies the Cisco Secure Client release 5 features, license requirements, and endpoint operating systems that are supported in the Secure Client (including AnyConnect).

Supported Operating Systems

Cisco Secure Client 5 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, and ISE Posture)
- 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
  - 8.x*

* Except ISE Posture Module, which only supports 8.1 (and later).

- Ubuntu
  - 24.04
  - 22.04
  - 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 *Supplemental End User Agreement (SEULA)* for licensing terms and conditions. See the *Cisco Secure Client Ordering Guide* for 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)

Table 1 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

Table 1 TLS 1.3, 1.2, and DTLS 1.2 Cipher Suites (VPN)

Standard RFC Naming Convention	OpenSSL Naming Convention
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
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)

Table 2 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)

Table 3 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
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 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 to align with general BYOD trends.

Secure Client 5 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.

Cisco Secure Client Advantage and Premier Licenses

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 licensed customers are also entitled to earlier AnyConnect releases.

Features Matrix

Cisco Secure 5 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
  - Core Features
  - Connect and Disconnect Features
  - Authentication and Encryption Features
  - Interfaces
- Cisco Secure Client Modules
  - Secure Firewall Posture
  - ISE Posture
  - Network Access Manager
  - AMP Enabler
  - Network Visibility Module
  - Umbrella
  - ThousandEyes Endpoint Agent
- Reporting and Troubleshooting
  - Customer Experience Feedback
  - Diagnostics and Reporting Tool (DART)

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 Lockdown	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
Web Launch (32 bit browsers only)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Pre-deployment	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
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 Required	Windows	macOS	Linux
SSL (TLS & DTLS), including Per App VPN	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
SNI (TLS & DTLS)	n/a	Advantage	yes	yes	yes
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 Clientless & Secure Client connections	ASA8.0(4) ASDM 6.3(1)	Premier	yes	yes	yes
Start Before Logon (SBL)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Run script on connect & disconnect	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
Minimize on connect	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
Auto connect on start	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
Auto reconnect (disconnect on system suspend, reconnect on system resume)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	no
Remote User VPN Establishment (permitted or denied)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Logon Enforcement (terminate VPN session if another user logs in)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Retain VPN session (when user logs off, and then when this or another user logs in)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	no	no
Trusted Network Detection (TND)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
Always on (VPN must be connected to access network)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	no
Always on exemption via DAP	ASA 8.3(1) ASDM 6.3(1)	Advantage	yes	yes	no
Connect Failure Policy (Internet access allowed or disallowed if VPN connection fails)	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	no
Captive Portal Detection	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Captive Portal Remediation	ASA 8.0(4) ASDM 6.3(1)	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 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
RSA SecurID /SoftID integration		Advantage	yes	no	no
Smartcard support		Advantage	yes	yes	no
SCEP (requires Posture Module if Machine ID is used)		Advantage	yes	yes	no
List & select certificates		Advantage	yes	no	no
FIPS		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)		Advantage	yes	yes	yes
NSA Suite-B (IPsec only)	ASA 9.0 ASDM 7.0	Premier	yes	yes	yes
Enable CRL check	n/a	Premier	yes	no	no
SAML 2.0 SSO	ASA 9.7.1 ASDM 7.7.1	Premier or VPN only	yes	yes	yes
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 SAML 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) ASDM 6.3(1)	Advantage	yes	yes	yes
Command Line			yes	yes	yes
API			yes	yes	yes
Microsoft Component Object Module (COM)			yes	no	no
Localization of User Messages			yes	yes	yes
Custom MSI transforms			yes	no	no
User defined resource files			yes	yes	no
Client Help	ASA 9.0 ASDM 7.0		yes	yes	no

Cisco Secure Client Modules

Secure Firewall Posture (Formerly HostScan) and Posture Assessment

Feature	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
Endpoint Assessment	ASA 8.0(4) ASDM 6.3(1)	Premier	yes	yes	yes
Endpoint Remediation		Premier	yes	yes	yes
Quarantine		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		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)		yes	yes	yes
AutoDART	n/a	n/a	yes	yes	yes

ISE Posture

Feature	Minimum AnyConnect Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
ISE Posture CLI	5.0.01xxx	n/a	n/a	n/a	yes	no	no
Posture State Synchronization	5.0	n/a	3.1	n/a	yes	yes	yes
Change of Authorization (CoA)	4.0	ASA 9.2.1 ASDM 7.2.1	2.0	Advantage	yes	yes	yes
ISE Posture Profile Editor	4.0	ASA 9.2.1 ASDM 7.2.1	n/a	Premier	yes	yes	yes
AC Identity Extensions (ACIDex)	4.0	n/a	2.0	Advantage	yes	yes	yes
ISE Posture Module	4.0	n/a	2.0	Premier	yes	yes	yes
Detection of USB mass storage devices (v4 only)	4.3	n/a	2.1	Premier	yes	no	no
OPSWAT v4	4.3	n/a	2.1	Premier	yes	yes	no
Stealth Agent for posture	4.4	n/a	2.2	Premier	yes	yes	no

Feature	Minimum AnyConnect Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Continuous endpoint monitoring	4.4	n/a	2.2	Premier	yes	yes	no
Next-generation provisioning and discovery	4.4	n/a	2.2	Premier	yes	yes	no
Application kill and uninstall capabilities	4.4	n/a	2.2	Premier	yes	yes	no
Cisco Temporal Agent	4.5	n/a	2.3	ISE Premier	yes	yes	no
Enhanced SCCM approach	4.5	n/a	2.3	Premier: Secure Client and ISE	yes	no	no
Posture policy enhancements for optional mode	4.5	n/a	2.3	Premier: Secure Client and ISE	yes	yes	no
Periodic probe interval in profile editor	4.5	n/a	2.3	Premier: Secure Client and ISE	yes	yes	no
Visibility into hardware inventory	4.5	n/a	2.3	Premier: Secure Client and ISE	yes	yes	no
Grace period for noncompliant devices	4.6	n/a	2.4	Premier: Secure Client and ISE	yes	yes	no
Posture rescan	4.6	n/a	2.4	Premier: Secure Client and ISE	yes	yes	no
Secure Client stealth mode notifications	4.6	n/a	2.4	Premier: Secure Client and ISE	yes	yes	no
Disabling UAC prompt	4.6	n/a	2.4	Premier: Secure Client and ISE	yes	no	no

Feature	Minimum AnyConnect Release	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Enhanced grace period	4.7	n/a	2.6	Premier: Secure Client and ISE	yes	yes	no
Custom notification controls and revamp of remediation windows	4.7	n/a	2.6	Premier: Secure Client and ISE	yes	yes	no
End-to-end agentless posture flow	4.9	n/a	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
Wired support IEEE 802.3			yes		
Wireless support IEEE 802.11			yes		
Pre-logon & Single Sign on Authentication			yes		
IEEE 802.1X			yes		
IEEE 802.1AE MACsec			yes		
EAP methods			yes		
FIPS 140-2 Level 1			yes		
Mobile Broadband support	ASA 8.4(1) ASDM 7.0		yes		
IPv6	ASA 9.0 ASDM 7.0		yes		
NGE and NSA Suite-B			yes		
TLS 1.2 for VPN connectivity*	n/a		yes	no	no
WPA3 Enhanced Open (OWE) and WPA3 Personal (SAE) support	n/a		yes	no	no

* If you are using ISE as a RADIUS server, note the following guideline:

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 Network Access Manager and use EAP-FAST with ISE 2.0 (or later) for RADIUS servers, you must upgrade to the appropriate release of ISE as well.

Warning!
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 Required	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	Minimum ISE Release	License Required	Windows	macOS	Linux
Network Visibility Module	ASDM 7.5.1 ASA 9.5.1	no ISE dependency	Premier	Yes	Yes	Yes
Adjustment to the rate at which data is sent	ASDM 7.5.1 ASA 9.5.1	no ISE dependency	Premier	Yes	Yes	Yes
Customization of NVM timer	ASDM 7.5.1 ASA 9.5.1	no ISE dependency	Premier	Yes	Yes	Yes
Broadcast and multicast option for data collection	ASDM 7.5.1 ASA 9.5.1	no ISE dependency	Premier	Yes	Yes	Yes
Creation of anonymization profiles	ASDM 7.5.1 ASA 9.5.1	no ISE dependency	Premier	Yes	Yes	Yes
Broader data collection and anonymization with hashing	ASDM 7.7.1 ASA 9.7.1	no ISE dependency	Premier	Yes	Yes	Yes
Support for Java as a container	ASDM 7.7.1 ASA 9.7.1	no ISE dependency	Premier	Yes	Yes	Yes
Configuration of cache to customize	ASDM 7.7.1 ASA 9.7.1	no ISE dependency	Premier	Yes	Yes	Yes
Periodic flow reporting	ASDM 7.7.1 ASA 9.7.1	no ISE dependency	Premier	Yes	Yes	Yes
Flow filter	n/a	no ISE dependency	Premier	Yes	Yes	Yes
Standalone NVM	n/a	n/a	Premier	Yes	Yes	Yes
Integration with Secure Cloud Analytics	n/a	n/a	n/a	Yes	No	No

Secure Umbrella Module

Feature	Minimum ASA/ASDM Release	Minimum ISE Release	License Required	Windows	macOS	Linux
Secure Umbrella Module	ASDM 7.6.2 ASA 9.4.1	ISE 2.0	Either Advantage or Premier Umbrella licensing is mandatory	Yes	Yes	No
Umbrella Secure Web Gateway	n/a	n/a	SIG Essential package from Umbrella	Yes	Yes	No
OpenDNS IPv6 support	n/a	n/a	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	n/a	n/a	n/a	Yes	Yes	No

Reporting and Troubleshooting Modules

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	Minimum ASA/ASDM Release	License Required	Windows	macOS	Linux
VPN	ASA 8.0(4) ASDM 6.3(1)	Advantage	yes	yes	yes
Network Access Manager	ASA 8.4(1) ASDM 6.4(1)	Premier	yes	no	no
Posture Assessment	ASA 8.4(1) ASDM 6.4(1)	Premier	yes	yes	yes
Network Visibility Module	ASA 8.4(1) ASDM 6.4(1)	Premier	yes	yes	yes

Accessibility Improvements

We addressed specific Voluntary Product Accessibility Template (VPAT) compliance standards to benefit those who are disadvantaged and to drive productivity through digital transformation:

- High contrast theme, which fixed invisible hyperlinks in the About dialog and tile title
- Minimum contrast ratio which increased contrast by adjusting the text colors of the tile submenu and DART menu description
- Keyboard navigation with Windows common shortcut keys (Tab, Enter, Spacebar)
- Navigation and selection of Advanced Window with Menu buttons(using Up/Down and Left/Right arrow keys)
- Keyboard access to Preference/About/DART windows from the Advanced Window
- Keyboard navigation with PgUp/PgDn to expand/collapse the statistics group
- Navigation and selection focus visibility for DART and Cisco Secure Client UIs
- Mismatch between screen reader of log settings and JAWS announcement was adjusted
- Mismatch between screen reader of DART encryption menu and JAWS announcement was adjusted
- Appropriate JAWS announcement for label in name