Cisco Secure Client（AnyConnect を含む）リリース 5 の機能、ライセンス、および OS

このマニュアルでは、Cisco Secure Client リリース 5 の機能、ライセンス要件、および Secure Client（AnyConnect を含む）がサポートするエンドポイント オペレーティング システムについて説明します。

サポートされているオペレーティングシステム

Cisco Secure Client 5 は、次のオペレーティングシステムをサポートします。

Windows

- Windows 11（64 ビット）
- ARM64 ベースの PC 用に Microsoft 社がサポートしているバージョンの Windows 11 および Windows 10（VPN クライアント、DART、Cisco Secure Firewall ポスチャ、Network Visibility Module でのみサポート）
- Windows 10 x86（32 ビット）および x64（64 ビット）

macOS（64 ビットのみ）

- macOS 13 Ventura
- macOS 12 Monterey
- macOS 11.x Big Sur

Linux

- Red Hat
  - 9.x
  - 8.x

* 8.1 以降のみをサポートする ISE ポスチャモジュールを除く。

- Ubuntu
  - 22.04
  - 20.04
- SUSE（SLES）
  - VPN：制限付きのサポート。ISE ポスチャのインストールにのみ使用されます。
  - Cisco Secure Firewall ポスチャまたは Network Visibility Module ではサポートされていません。
  - ISE ポスチャ：12.3（以降のバージョン）および 15.0（以降のバージョン）

OS の要件およびサポートノートについては、『*Release Notes for Cisco Secure Client*』を参照してください。ライセンス契約条件については、『*Supplemental End User Agreement (SEULA)*』を参照してください。発注の詳細と各種ライセンスに特有の契約条件については、『*Cisco Secure Client Ordering Guide*』を参照してください。

Cisco Secure Client モジュールおよび機能に適用されるライセンス情報とオペレーティングシステムの制限については、下記の機能マトリクスを参照してください。

サポートされている暗号アルゴリズム

次の表に、Cisco Secure Client でサポートされている暗号アルゴリズムを示します。暗号アルゴリズムと暗号スイートは、優先度の高いものから順に示されています。この優先度は、すべてのシスコ製品が準拠する必要があるシスコの製品セキュリティベースラインによって決定されます。PSB の要件は随時変更されるため、以降のバージョンの Secure Client でサポートされる暗号アルゴリズムはそれに応じて変更されます。

TLS 1.3、1.2、および DTLS 1.2 暗号スイート（VPN）

表 1　　TLS 1.3、1.2、および DTLS 1.2 暗号スイート（VPN）

標準 RFC 命名規則	OpenSSL 命名規則
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	

表 1　TLS 1.3、1.2、および DTLS 1.2 暗号スイート（VPN）（続き）

標準 RFC 命名規則	OpenSSL 命名規則
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 暗号スイート（ネットワーク アクセス マネージャ）

表 2　TLS 1.2 暗号スイート（ネットワーク アクセス マネージャ）

標準 RFC 命名規則	OpenSSL 命名規則
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 暗号スイート（VPN）

表 3　DTLS 1.0 暗号スイート（VPN）

標準 RFC 命名規則	OpenSSL 命名規則
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

表 3　　DTLS 1.0 暗号スイート（VPN）（続き）

標準 RFC 命名規則	OpenSSL 命名規則
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

IKEv2/IPsecアルゴリズム

暗号化

ENCR_AES_GCM_256

ENCR_AES_GCM_192

ENCR_AES_GCM_128

ENCR_AES_CBC_256

ENCR_AES_CBC_192

ENCR_AES_CBC_128

疑似ランダム関数

PRF_HMAC_SHA2_256

PRF_HMAC_SHA2_384

PRF_HMAC_SHA2_512

PRF_HMAC_SHA1

Diffie-Hellman グループ

DH_GROUP_256_ECP：グループ 19

DH_GROUP_384_ECP：グループ 20

DH_GROUP_521_ECP：グループ 21

DH_GROUP_3072_MODP：グループ 15

DH_GROUP_4096_MODP：グループ 16

整合性

AUTH_HMAC_SHA2_256_128

AUTH_HMAC_SHA2_384_192

AUTH_HMAC_SHA1_96

AUTH_HMAC_SHA2_512_256

ライセンス オプション

Cisco Secure Client 5 を使用するには、Premier または Advantage ライセンスを購入する必要があります。必要なライセンスは、使用する予定の Secure Client の機能と、サポートするセッションの数によって異なります。これらのユーザベースのライセンスには、一般的な BYOD のトレンドに合わせたサポートとソフトウェア更新へのアクセスが含まれます。

Secure Client 5 ライセンスは Cisco Secure Firewall 適応型セキュリティアプライアンス（ASA）、サービス統合型ルータ（ISR）、クラウドサービスルータ（CSR）、および Aggregated Services Router（ASR）と、Identity Services Engine（ISE）などのその他の非 VPN ヘッドエンドで使用されます。ヘッドエンドに関係なく一貫したモデルが使用されるため、ヘッドエンドの移行が発生した場合も影響はありません。

導入には次の Cisco Secure ライセンスが 1 つまたは複数必要になる場合があります。

ライセンス	説明
Advantage	PC やモバイルプラットフォーム（Secure Client および標準ベースの IPsec IKEv2 ソフトウェアクライアント）の VPN 機能、FIPS、基本的なエンドポイント コンテキスト コレクション、および 802.1x Windows サプリカントなどの基本的な Secure Client 機能をサポートします。
Premier	Network Visibility Module、クライアントレス VPN、VPN ポスチャエージェント、統一されたポスチャエージェント、次世代暗号化/スイート B、SAML、すべての Plus サービスと Flex ライセンスなどの高度な機能に加えて、すべての基本的な Secure Client Advantage 機能もサポートします。
VPN のみ（永久）	PC およびモバイルプラットフォームのための VPN 機能、Secure Firewall ASA でのクライアントレス（ブラウザベース）VPN ターミネーション、ASA と連携した VPN 専用コンプライアンスおよびポスチャエージェント、FIPS コンプライアンス、ならびに Secure Client およびサードパーティ IKEv2 VPN クライアントでの次世代暗号化（スイート B）をサポートします。VPN のみのライセンスは、Secure Client をリモートアクセス VPN サービス専用に使用したい場合で、総ユーザー数が多い、または予測できない環境に最も適しています。Secure Client のその他の機能またはサービス（Cisco Umbrella Roaming、ISE ポスチャ、Network Visibility Module、または Network Access Manager など）は、このライセンスでは使用できません。

Cisco Secure Client Advantage または Premier ライセンス

Cisco Commerce Workspace Web サイトから、サービス階層（Advantage または Premier）と期間（1、3、または 5 年）を選択します。必要なライセンスの数は、Secure Client を使用する一意のユーザーまたは承認ユーザーの数に基づきます。Secure Client のライセンスは同時接続に基づいて付与されるものではありません。同じ環境に Advantage ライセンスと Premier ライセンスを混在させることができ、ユーザーごとに必要なライセンスの数は 1 つのみです。

Cisco Secure 5 のライセンスをお持ちのお客様は、以前のリリースの AnyConnect もご利用になれます。

機能マトリクス

Cisco Secure 5 のモジュールおよび機能と、最小リリース要件、ライセンス要件、およびサポートされるオペレーティングシステムを次の項に示します。

Cisco Secure Client の展開と構成

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
遅延アップグレード	ASA 9.0 ASDM 7.0	Advantage	はい	はい	はい
Windows サービスのロックダウン	ASA 8.0(4) ASDM 6.4(1)	Advantage	はい	いいえ	いいえ
ポリシー、ソフトウェア、プロファイル ロックの更新	ASA 8.0(4) ASDM 6.4(1)	Advantage	はい	はい	はい
自動更新	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
Web 起動 （32 ビット ブラウザのみ）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
事前展開	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
クライアント プロファイルの自動更新	ASA 8.0(4) ASDM 6.4(1)	Advantage	はい	はい	はい
Cisco Secure Client プロファイルエディタ	ASA 8.4(1) ASDM 6.4(1)	Advantage	はい	はい	はい
ユーザ制御可能な機能	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	○*

* VPN 接続で Secure Client を最小化する機能、または信頼できないサーバーへの接続をブロックする機能

AnyConnect VPN

コア機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
SSL（TLS および DTLS）（アプライアンスごとの VPN を含む）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
SNI（TLS および DTLS）	適用対象外	Advantage	はい	はい	はい
TLS 圧縮	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
DTLS の TLS へのフォールバック	ASA 8.4.2.8 ASDM 6.3(1)	Advantage	はい	はい	はい
IPsec/IKEv2	ASA 8.4(1) ASDM 6.4(1)	Advantage	はい	はい	はい
スプリット トンネリング	ASA 8.0(x) ASDM 6.3(1)	Advantage	はい	はい	はい
ダイナミック スプリット トンネリング	ASA 9.0	Advantage、Premier、または VPN のみ	はい	はい	いいえ
強化されたダイナミック スプリット トンネリング	ASA 9.0	Advantage	はい	はい	いいえ
スプリット DNS	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
ブラウザ プロキシの無視	ASA 8.3(1) ASDM 6.3(1)	Advantage	はい	はい	いいえ
Proxy Auto Config（PAC）ファイルの生成	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
Internet Explorer の [接続（Connections）] タブのロック	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
最適ゲートウェイ選択	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
Global Site Selector（GSS）の互換性	ASA 8.0(4) ASDM 6.4(1)	Advantage	はい	はい	はい
ローカル LAN へのアクセス	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
同期化のためのクライアント ファイアウォール ルールによるテザーデバイスのアクセス	ASA 8.3(1) ASDM 6.3(1)	Advantage	はい	はい	はい
クライアント ファイアウォール ルールによるローカル プリンタのアクセス	ASA 8.3(1) ASDM 6.3(1)	Advantage	はい	はい	はい
IPv6	ASA 9.0 ASDM 7.0	Advantage	はい	はい	いいえ
さらなる IPv6 の実装	ASA 9.7.1 ASDM 7.7.1	Advantage	はい	はい	はい
証明書のピン留め	依存関係なし	Advantage	はい	はい	はい
管理 VPN トンネル	ASA 9.0 ASDM 7.10.1	Premier	はい	はい	いいえ

接続機能および切断機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
高速ユーザースイッチング	適用対象外	適用対象外	はい	いいえ	いいえ
クライアントレス接続と Secure Client 接続の同時使用	ASA8.0(4) ASDM 6.3(1)	Premier	はい	はい	はい
Start Before Logon（SBL）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
接続時および切断時のスクリプト実行	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
接続時の最小化	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
起動時の自動接続	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
自動再接続（システムの一時停止で切断、システムの再開で再接続）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
リモート ユーザ VPN 確立（許可または拒否）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
ログオン実行（別のユーザがログインすると、VPN セッションを終了）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
VPN セッションの維持（ユーザがログオフし、その後このユーザまたは別のユーザがログインした場合）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	いいえ	いいえ
Trusted Network Detection（TND）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
常時オン（ネットワークにアクセスするには、VPN を接続する必要がある）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
DAP による常時オン除外	ASA 8.3(1) ASDM 6.3(1)	Advantage	はい	はい	いいえ
接続障害ポリシー（VPN 接続に障害が発生した場合、インターネット アクセスを許可または不許可）	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
キャプティブ ポータルの検出	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
キャプティブ ポータルの修復	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	いいえ
強化されたキャプティブ ポータル修復	依存関係なし	Advantage	はい	はい	いいえ

認証および暗号化機能

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
証明書のみの認証	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
RSA SecurID/SoftID の統合		Advantage	はい	いいえ	いいえ
スマートカードのサポート		Advantage	はい	はい	いいえ
SCEP（マシン ID を使用する場合はポスチャ モジュールが必要）		Advantage	はい	はい	いいえ
証明書の一覧表示および選択		Advantage	はい	いいえ	いいえ
FIPS		Advantage	はい	はい	はい
IPsec IKEv2 の SHA-2（デジタル署名、整合性、および PRF）	ASA 8.0(4) ASDM 6.4(1)	Advantage	はい	はい	はい
強力な暗号化（AES-256 およびトリプル DES 168）		Advantage	はい	はい	はい
NSA Suite-B（IPsec のみ）	ASA 9.0 ASDM 7.0	Premier	はい	はい	はい
CRL チェックの有効化	適用対象外	Premier	はい	いいえ	いいえ
SAML 2.0 SSO	ASA 9.7.1 ASDM 7.7.1	Premier または VPN のみ	はい	はい	はい
強化された SAML 2.0	ASA 9.7.1.24 ASA 9.8.2.28 ASA 9.9.2.1	Premier または VPN のみ	はい	はい	はい
拡張 Web 認証用の外部ブラウザ SAML パッケージ	ASA 9.17.1 ASDM 7.17.1	Premier または VPN のみ	はい	はい	はい
複数の証明書の認証	ASA 9.7.1 ASDM 7.7.1	Advantage、Premier、または VPN のみ	はい	はい	はい

インターフェイス

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
GUI	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
コマンド ライン			はい	はい	はい
API			はい	はい	はい
Microsoft コンポーネント オブジェクト モジュール（COM）			はい	いいえ	いいえ
ユーザ メッセージのローカリゼーション			はい	はい	いいえ
カスタム MSI トランスフォーム			はい	いいえ	いいえ
ユーザ定義リソース ファイル			はい	はい	いいえ
クライアント ヘルプ	ASA 9.0 ASDM 7.0		はい	はい	いいえ

Cisco Secure Client モジュール

Cisco Secure Firewall ポスチャ（旧称 HostScan）とポスチャアセスメント

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
エンドポイント アセスメント	ASA 8.0(4) ASDM 6.3(1)	Premier	はい	はい	はい
エンドポイント修復		Premier	はい	はい	はい
検疫		Premier	はい	はい	はい
検疫のステータスおよび中止メッセージ	ASA 8.3(1) ASDM 6.3(1)	Premier	はい	はい	はい
Cisco Secure Firewall ポスチャパッケージの更新	ASA 8.4(1) ASDM 6.4(1)	Premier	はい	はい	はい
ホスト エミュレーション検出		Premier	はい	いいえ	いいえ
OPSWAT v4	ASA 9.9(1) ASDM 7.9(1)	Premier	はい	はい	はい

ISE ポスチャ

機能	最低限の AnyConnect リリース	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
ISE ポスチャ CLI	5.0.01xxx	適用対象外	適用対象外	適用対象外	はい	いいえ	いいえ
認可変更（CoA）	4.0	ASA 9.2.1 ASDM 7.2.1	2.0	Advantage	はい	はい	はい
ISE ポスチャ プロファイル エディタ	4.0	ASA 9.2.1 ASDM 7.2.1	適用対象外	Premier	はい	はい	はい
AC Identity Extensions（ACIDex）	4.0	適用対象外	2.0	Advantage	はい	はい	はい
ISE ポスチャ モジュール	4.0	適用対象外	2.0	Premier	はい	はい	はい
USB 大容量ストレージ デバイス（v4 のみ）の検出	4.3	適用対象外	2.1	Premier	はい	いいえ	いいえ
OPSWAT v4	4.3	適用対象外	2.1	Premier	はい	はい	いいえ
ポスチャのステルス エージェント	4.4	適用対象外	2.2	Premier	はい	はい	いいえ
エンドポイントの継続的モニタリング	4.4	適用対象外	2.2	Premier	はい	はい	いいえ
次世代のプロビジョニングおよびディスカバリ	4.4	適用対象外	2.2	Premier	はい	はい	いいえ
アプリケーションの強制終了およびアンインストール機能	4.4	適用対象外	2.2	Premier	はい	はい	いいえ
Cisco Temporal Agent	4.5	適用対象外	2.3	ISE Premier	はい	はい	いいえ
強化された SCCM アプローチ	4.5	適用対象外	2.3	Premier：Secure Client および ISE	はい	いいえ	いいえ
オプション モードのポスチャ ポリシー拡張機能	4.5	適用対象外	2.3	Premier：Secure Client および ISE	はい	はい	いいえ
プロファイル エディタでの定期的なプローブの間隔	4.5	適用対象外	2.3	Premier：Secure Client および ISE	はい	はい	いいえ
ハードウェア インベントリの可視性	4.5	適用対象外	2.3	Premier：Secure Client および ISE	はい	はい	いいえ

機能	最低限の AnyConnect リリース	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
非準拠デバイスの猶予期間	4.6	適用対象外	2.4	Premier: Secure Client および ISE	はい	はい	いいえ
ポスチャの再スキャン	4.6	適用対象外	2.4	Premier: Secure Client および ISE	はい	はい	いいえ
Secure Client のステルスモード通知	4.6	適用対象外	2.4	Premier: Secure Client および ISE	はい	はい	いいえ
UAC プロンプトの無効化	4.6	適用対象外	2.4	Premier: Secure Client および ISE	はい	いいえ	いいえ
猶予期間の拡張	4.7	適用対象外	2.6	Premier: Secure Client および ISE	はい	はい	いいえ
カスタム通知制御と修復ウィンドウの revamp	4.7	適用対象外	2.6	Premier: Secure Client および ISE	はい	はい	いいえ
エンドツーエンドのエージェントレス ポスチャ フロー	4.9	適用対象外	3.0	Premier: Secure Client および ISE	はい	はい	いいえ

Network Access Manager

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
コア	ASA 8.4(1) ASDM 6.4(1)	Advantage	はい	いいえ	いいえ
IEEE 802.3 の有線サポート			○		
IEEE 802.11 の無線サポート			○		
事前ログオンおよびシングル サインオン認証			○		
IEEE 802.1X			○		
IEEE 802.1AE MACsec			○		
EAP メソッド			○		
FIPS 140-2 レベル 1			○		
モバイル ブロードバンドのサポート	ASA 8.4(1) ASDM 7.0		○		
IPv6	ASA 9.0 ASDM 7.0		○		
NGE および NSA Suite-B			○		
VPN 接続の TLS 1.2*	適用対象外		はい	いいえ	いいえ

* RADIUS サーバとして ISE を使用する場合は、次のガイドラインに注意してください。

ISE は、リリース 2.0 で TLS 1.2 のサポートを開始しています。TLS 1.2 を使用した Cisco Secure Client と 2.0 より以前の ISE リリースを使用する場合、Network Access Manager と ISE は TLS 1.0 とネゴシエートします。そのため、Network Access Manager をアップグレードし、RADIUS サーバーに ISE 2.0（またはそれ以降）を使用した EAP-FAST を使用する場合は、適切な ISE リリースへのアップグレードも必要になります。

警告：
非互換性警告：2.0 以上を実行している ISE のお客様は、次に進む前にこちらをお読みください。

ISE RADIUS はリリース 2.0 以降 TLS 1.2 をサポートしてきましたが、CSCvm03681 により追跡される TLS 1.2 を使用した EAP-FAST の ISE 導入に不具合が見つかりました。ISE の 2.4p5 リリースで不具合が修正されました。

上記のリリースより以前の TLS 1.2 をサポートする ISE の EAP-FAST を使用して、NAM が認証に使用される場合、認証は失敗し、エンドポイントはネットワークにアクセスできません。

AMP イネーブラ

機能	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
AMP イネーブラ	ASDM 7.4.2 ASA 9.4.1	ISE 1.4	Advantage	適用対象外	対応	適用対象外

ネットワーク可視性モジュール

機能	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
ネットワーク可視性モジュール	ASDM 7.5.1 ASA 9.5.1	ISE 依存関係なし	Premier	対応	対応	対応
データ送信レートへの調整	ASDM 7.5.1 ASA 9.5.1	ISE 依存関係なし	Premier	対応	対応	対応
NVM タイマーのカスタマイズ	ASDM 7.5.1 ASA 9.5.1	ISE 依存関係なし	Premier	対応	対応	対応
データ収集のブロードキャストおよびマルチキャスト オプション	ASDM 7.5.1 ASA 9.5.1	ISE 依存関係なし	Premier	対応	対応	対応
匿名プロファイルの作成	ASDM 7.5.1 ASA 9.5.1	ISE 依存関係なし	Premier	対応	対応	対応
より広範囲なデータ収集とハッシュによる匿名化	ASDM 7.7.1 ASA 9.7.1	ISE 依存関係なし	Premier	対応	対応	対応
コンテナとしての Java のサポート	ASDM 7.7.1 ASA 9.7.1	ISE 依存関係なし	Premier	対応	対応	対応
カスタマイズするキャッシュの設定	ASDM 7.7.1 ASA 9.7.1	ISE 依存関係なし	Premier	対応	対応	対応
定期的なフロー レポート	ASDM 7.7.1 ASA 9.7.1	ISE 依存関係なし	Premier	対応	対応	対応
フロー フィルタ	適用対象外	ISE 依存関係なし	Premier	対応	対応	対応
スタンドアロン NVM	適用対象外	適用対象外	Premier	対応	対応	対応

Umbrella ローミング セキュリティ モジュール

機能	最低限の ASA/ASDM リリース	最低限の ISE リリース	必要なライセンス	Windows	macOS	Linux
Umbrella ローミング セキュリティ モジュール	ASDM 7.6.2 ASA 9.4.1	ISE 2.0	Advantage または Premier のいずれか Umbrella のライセンスが必須	対応	対応	非対応
Umbrella セキュア Web ゲートウェイ	適用対象外	適用対象外	Umbrella の SIG Essential パッケージ	対応	対応	非対応
OpenDNS IPv6 のサポート	適用対象外	適用対象外	適用対象外	対応	対応	非対応

Umbrella のライセンスの詳細については、
https://www.opendns.com/enterprise-security/threat-enforcement/packages/ を参照してください。

レポート モジュールおよびトラブルシューティング モジュール

カスタマー エクスペリエンスのフィードバック

機能	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
カスタマー エクスペリエンスのフィードバック	ASA 8.4(1) ASDM 7.0	Advantage	はい	はい	いいえ

Diagnostic and Reporting Tool（DART）

ログ タイプ	最低限の ASA/ASDM リリース	必要なライセンス	Windows	macOS	Linux
VPN	ASA 8.0(4) ASDM 6.3(1)	Advantage	はい	はい	はい
ネットワーク アクセス マネージャ	ASA 8.4(1) ASDM 6.4(1)	Premier	はい	いいえ	いいえ
ポスチャ アセスメント	ASA 8.4(1) ASDM 6.4(1)	Premier	はい	はい	はい
ネットワーク可視性モジュール	ASA 8.4(1) ASDM 6.4(1)	Premier	はい	はい	はい

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。