AnyConnect セキュア モビリティ クライアント リリース 4.10 の機能、ライセンス、および OS

このマニュアルでは、AnyConnect リリース 4.10 の機能、ライセンス要件、および AnyConnect 機能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 AnyConnect セキュア モビリティ クライアント 4.10 は、次のオペレーティングシステムをサポートします。

オペレーティング システム	バージョン
Windows	ARM64 ベースの PC 用に Microsoft がサポートしているバージョンの Windows 10（VPN クライアント、DART、ISE ポスチャ、および HostScanのみ）
	現在のMicrosoftWindows10x64（64ビット）のバージョンのサポート
	Windows 8.1 x86（32 ビット）および x64（64 ビット）
macOS	macOS13、macOS12.x、macOS11.x（64ビット）、10.15（64ビット）、および 10.14（64 ビット）
Linux	Red Hat 8 および 7（64 ビット）
	Ubuntu 20.04、18.04、および 16.04（すべて 64 ビット）

(注) Windows 7 の限定的な拡張サポートは、Microsoft とアクティブな Windows 7 の拡張サポート契約を結んでいるお客様に提供されます。シスコは Windows 7 で実質的な品質保証テストを実施しなくなりましたが、可能な限り問題は解決します。セキュリティ強化機能を利用するには、AnyConnect および Windows の最新バージョンにアップグレードすることを強く推奨します。シスコでは、現在 Windows XP 用の AnyConnect リリースをサポートしていません。

OS の要件およびサポート ノートについては、『*Release Notes for Cisco AnyConnect Secure Mobility 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 AnyConnect Ordering Guide*』を参照してください。

AnyConnect モジュールおよび機能に適用されるライセンス情報およびオペレーティング 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。

AnyConnect 4.3(およびそれ以降)は Visual Studio(VS)2015 ビルド環境に移行しており、その Network Access Manager モジュールが機能するためには VS 再頒布可能ファイルが必要です。これらのファイルは、インストール パッケージの一部としてインストールされます。.msi ファイルを使用して、4.3(またはそれ以降)にネットワーク アクセス マネージャ モジュールをアップグレードできますが、最初に AnyConnect セキュア モビリティ クライアントをアップグレードし、リリース 4.3(またはそれ以降)を実行する必要があります。

また、AnyConnect Umbrella ローミング セキュリティ モジュールの追加には、Microsoft .NET 4.0 が必要です。

サポートされている暗号アルゴリズム

次の表に、AnyConnect 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 AnyConnect 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 1.2 および DTLS 1.2 暗号スイート（VPN）

表 1　TLS 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_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
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

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)(続き)

標準 RFC 命名規則	OpenSSL 命名規則
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
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

AnyConnect セキュア モビリティ クライアント 4.10 を使用するには、AnyConnect Plus ライセンスまたは AnyConnect Apex 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 AnyConnect VPN Client および Secure Mobility 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。

AnyConnect 4.10 ライセンスは Cisco ASA 5500 シリーズ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 AnyConnect 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
AnyConnect Plus	PC やモバイルプラットフォーム（AnyConnect および標準ベースのIPsecIKEv2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 AnyConnect 機能をサポートします。Plus ライセンスは、以前に AnyConnect Essentials ライセンスで提供されていた環境と、Network Access Manager Module のユーザに最適です。

ライセンス	説明
AnyConnect Apex	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/SuiteB、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 AnyConnect Plus 機能もサポートします。Apex ライセンスは、以前に AnyConnect Premium、Shared、Flex、および Advanced Endpoint Assessment ライセンスで提供されていた環境に最適です。
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、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 にともなう VPN のみの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AnyConnectおよびサードパーティIKEv2VPNクライアントでの次世代暗号化（SuiteB）をサポートします。VPNのみのライセンスは、AnyConnectをリモートアクセス VPN サービスのみに使用する必要があるものの、ユーザの総数が多かったり予測不能であったりする環境に最適です。AnyConnectのその他の機能またはサービス（CiscoUmbrellaローミング、ISEポスチャ、ネットワーク可視性モジュール、またはネットワークアクセスマネージャなど）は、このライセンスでは使用できません。

AnyConnect Plus および Apex ライセンス

Cisco Commerce Workspace Web サイトから、サービス階層（Apex または Plus）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、AnyConnect を使用する一意のユーザまたは許可されたユーザの数に基づきます。AnyConnect 4.10 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 Apex ライセンスと Plus ライセンスを混在させることができ、ユーザごとに必要なライセンスの数は 1 つのみです。

AnyConnect 4.10 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

AnyConnect 4.10 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。

- AnyConnect の導入および設定
- *VPN 接続で AnyConnect を最小化する機能、または信頼できないサーバへの接続をブロックする機能
  - コア機能
  - 接続機能および切断機能
  - 認証および暗号化機能
  - インターフェイス
- AnyConnect ネットワーク アクセス マネージャ
- * 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。
  - Hostscan およびポスチャ アセスメント
  - ISE ポスチャ
- カスタマー エクスペリエンスのフィードバック
  - カスタマー エクスペリエンスのフィードバック
  - Diagnostic and Reporting Tool（DART）

- AMP イネーブラ
- ネットワーク可視性モジュール
- Umbrella ローミング セキュリティ モジュール

AnyConnect の導入および設定

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	Plus	○	○	○
Windows サービスのロックダウン	ASA 8.0(4) ASDM 6.4(1)	Plus	○	×	×
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)	Plus	○	○	○
自動更新	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
Web 起動 （32 ビット ブラウザのみ）	ASA 8.0(4) ASDM 6.3(1)	Plus	○	×	×
事前展開	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
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)	Plus	○	○	○
AnyConnect プロファイル エディタ	ASA 8.4(1) ASDM 6.4(1)	Plus	○	○	○
ユーザ制御可能な機能	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○*

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

AnyConnect のコア VPN クライアント

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)	Plus	○	○	○
SNI(TLS および DTLS)	適用対象外	Plus	○	○	○
TLS 圧縮	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
DTLS の TLS へのフォールバック	ASA 8.4.2.8 ASDM 6.3(1)	Plus	○	○	○
IPsec/IKEv2	ASA 8.4(1) ASDM 6.4(1)	Plus	○	○	○
スプリット トンネリング	ASA 8.0(x) ASDM 6.3(1)	Plus	○	○	○
ダイナミック スプリット トンネリング	ASA 9.0	Plus、Apex、または VPN のみ	○	○	×
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	Plus、Apex、または VPN のみ	○	○	×
スプリット DNS	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	×
ブラウザ プロキシの無視	ASA 8.3(1) ASDM 6.3(1)	Plus	○	○	×
Proxy Auto Config(PAC)ファイルの生成	ASA 8.0(4) ASDM 6.3(1)	Plus	○	×	×
Internet Explorer の [接続(Connections)] タブのロック	ASA 8.0(4) ASDM 6.3(1)	Plus	○	×	×
最適ゲートウェイ選択	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	×
Global Site Selector (GSS)の互換性	ASA 8.0(4) ASDM 6.4(1)	Plus	○	○	○
ローカル LAN へのアクセス	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
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)	Plus	○	○	○

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 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)	Plus	○	○	○
IPv6	ASA 9.0 ASDM 7.0	Plus	○	○	×
さらなる IPv6 の実装	ASA 9.7.1 ASDM 7.7.1	Plus	○	○	○
証明書のピン留め	依存関係なし	Plus、Apex、または VPN のみ	○	○	○
管理 VPN トンネル	ASA 9.0 ASDM 7.10.1	Apex	○	×	×

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
クライアントレス接続と AnyConnect 接続の同時使用	ASA8.0(4) ASDM 6.3(1)	Apex	○	○	○
StartBeforeLogon（SBL）	ASA 8.0(4) ASDM 6.3(1)	Plus	○	×	×
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)	Plus	○	○	○
接続時の最小化	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
起動時の自動接続	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
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)	Plus	○	○	×
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)	Plus	○	×	×
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)	Plus	○	×	×
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)	Plus	○	×	×
Trusted Network Detection（TND）	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
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)	Plus	○	○	×
DAP による常時オン除外	ASA 8.3(1) ASDM 6.3(1)	Plus	○	○	×
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)	Plus	○	○	×
キャプティブ ポータルの検出	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	○
キャプティブ ポータルの修復	ASA 8.0(4) ASDM 6.3(1)	Plus	○	○	×
強化されたキャプティブ ポータル修復	依存関係なし	Plus	○	○	×

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)	Plus	○	○	○
RSA SecurID/SoftID の統合		Plus	○	×	×
スマートカードのサポート		Plus	○	○	×
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)		Plus	○	○	×
証明書の一覧表示および選択		Plus	○	×	×
FIPS		Plus	○	○	○
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)	Plus	○	○	○
強力な暗号化 (AES-256 およびトリプル DES 168)		Plus	○	○	○
NSA Suite-B(IPsec のみ)	ASA 9.0 ASDM 7.0	Apex	○	○	○
CRL チェックの有効化	適用対象外	Apex	○	×	×
SAML 2.0 SSO	ASA 9.7.1 ASDM 7.7.1	Apex または VPN のみ	○	○	○
強化された SAML 2.0	ASA 9.7.1.24 ASA 9.8.2.28 ASA 9.9.2.1	Apex または VPN のみ	○	○	○
複数の証明書の認証	ASA 9.7.1 ASDM 7.7.1	Plus、Apex、または VPN のみ	○	○	○

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)	Plus	○	○	○
コマンド ライン			○	○	○
API			○	○	○
Microsoft コンポーネント オブジェクト モジュール(COM)			○	×	×
ユーザ メッセージのローカリゼーション			○	○	×
カスタム MSI トランスフォーム			○	×	×
ユーザ定義リソース ファイル			○	○	×
クライアント ヘルプ	ASA 9.0 ASDM 7.0		○	○	×

AnyConnect ネットワーク アクセス マネージャ

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)	Plus	○	×	×
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		○	×	×

* 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 AnyConnect 4.7(およびそれ以降)のバージョンと 2.0 より前の ISE リリースを使用する場合、ネットワーク アクセス マネージャと ISE は TLS 1.0 とネゴシエートします。そのため、AnyConnect ネットワーク アクセス マネージャを 4.7(およびそれ以降)にアップグレードし、RADIUS サーバに 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、ISE リリース 2.4p5 にアップグレードする必要があります。

AnyConnect Secure Mobility のモジュール

Hostscan およびポスチャ 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)	Apex	○	○	○
エンドポイント修復		Apex	○	○	○
検疫		Apex	○	○	○
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)	Apex	○	○	○
HostScan パッケージの更新	ASA 8.4(1) ASDM 6.4(1)	Apex	○	○	○
ホスト エミュレーション検出		Apex	○	×	×
OPSWAT v4	ASA 9.9(1) ASDM 7.9(1)	Apex	○	○	○

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
認可変更(CoA)	4.0	ASA 9.2.1 ASDM 7.2.1	2.0	Plus	○	○	○
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	Apex	○	○	○
AC Identity Extensions(ACIDex)	4.0	適用対象外	2.0	Plus	○	○	○
ISE ポスチャ モジュール	4.0	適用対象外	2.0	Apex	○	○	○
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	Apex	○	×	×
OPSWAT v4	4.3	適用対象外	2.1	Apex	○	○	×
ポスチャのステルス エージェント	4.4	適用対象外	2.2	Apex	○	○	×
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	Apex	○	○	×
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	Apex	○	○	×
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	Apex	○	○	×

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
Cisco Temporal Agent	4.5	適用対象外	2.3	ISE Apex	○	○	×
強化された SCCM アプローチ	4.5	適用対象外	2.3	AC Apex および ISE Apex	○	×	×
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	AC Apex および ISE Apex	○	○	×
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	AC Apex および ISE Apex	○	○	×
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	AC Apex および ISE Apex	○	○	×
非準拠デバイスの猶予期間	4.6	適用対象外	2.4	AC Apex および ISE Apex	○	○	×
ポスチャの再スキャン	4.6	適用対象外	2.4	AC Apex および ISE Apex	○	○	×
AnyConnect ステルス モード通知	4.6	適用対象外	2.4	AC Apex および ISE Apex	○	○	×
UAC プロンプトの無効化	4.6	適用対象外	2.4	AC Apex および ISE Apex	○	×	×
猶予期間の拡張	4.7	適用対象外	2.6	AC Apex および ISE Apex	○	○	×
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	AC Apex および ISE Apex	○	○	×
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	AC Apex および ISE Apex	○	○	×

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 4.7(以降)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	Plus	対応	対応	非対応

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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	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	Apex	対応	対応	対応
スタンドアロン NVM	適用対象外	適用対象外	Apex	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	Plus または Apex 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	Plus	○	○	×

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)	Plus	○	○	○
ネットワーク アクセス マネージャ	ASA 8.4(1) ASDM 6.4(1)	Apex	○	×	×
ポスチャ アセスメント			○	○	○

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。