Cisco Secure Client の導入

はじめる前に

次の箇条書きは、AnyConnect セキュア モビリティ クライアント 4.x リリースとは異なる主要なサポート、命名、および機能の変更を示しています。リリース 5 では、AnyConnect セキュア モビリティ クライアントは、名前が Cisco Secure Client に変更されました。

- Network Access Manager は Cisco Secure Client 5.0 の一部ですが、SecureX 内の Network Access Manager プロファイルエディタはリリース 5 では使用できません。
- Windows 用 Cisco Secure Client は Cisco Secure Endpoint（旧 AMP for Endpoints）との完全な統合を提供するため、AMP イネーブラは Cisco Secure Client 5 での macOS 専用です。
- 一部の AnyConnect モジュールも、Cisco Secure Client 5 リリースで新しい名前が付けられています。HostScan（VPN Posture）は Secure Firewall Posture に変更されます。ASDM UI では、リモートアクセス VPN ウィンドウでポスチャ（Cisco Secure Firewall 用）として参照されます。同様に、Cisco.com からダウンロードした hostscan.pkg の名前は、secure-firewall-posture-version-k9.pkg に変更されます。
- ドキュメントと ASDM UI で AnyConnect への参照に気付くでしょう。ASDM は Cisco Secure Client 5 プロファイルを設定するために完全にサポートされていますが、現在、これらの参照を新しい Cisco Secure Client 名に変更する予定はありません。Cisco Secure Firewall ASA は、バージョン 9.18 以降では新しい ASA 名になります。

- Umbrella クラウド インフラストラクチャにインストールされたすべての AnyConnect モジュールの自動更新を提供する Umbrella ローミング セキュリティ モジュールの機能は、リリース 5 で削除されました。
- AnyConnect の Apex および Plus ライセンスは、Cisco Secure Client の Premier および Advantage ライセンスに変更されました。

Cisco Secure Client 展開の概要

Cisco Secure Client の展開は、Cisco Secure Client と関連ファイルのインストール、設定、アップグレードを意味します。

Cisco Secure Client は、次の方法によってリモート ユーザに展開できます。

- 事前展開：新規インストールとアップグレードは、エンドユーザによって、または社内のソフトウェア管理システム（SMS）を使用して実行されます。この展開オプションでは、クラウド管理は提供されません。
- Web 展開：Cisco Secure Client パッケージは、ヘッドエンド（Secure Firewall Threat Defense または ISE サーバー）にロードされます。ユーザーがファイアウォールまたは ISE に接続すると、Cisco Secure Client がクライアントに展開されます。この展開オプションでは、クラウド管理は提供されません。
  - 新規インストールの場合、ユーザーはヘッドエンドに接続して Cisco Secure Client をダウンロードします。クライアントは、手動でインストールするか、または自動（Web 起動）でインストールされます。
  - アップデートは、Cisco Secure Client がすでにインストールされているシステムで Cisco Secure Client を実行すること、またはユーザーを Cisco Secure Firewall ASA クライアントレスポータルに誘導することによって行われます。
- SecureX のクラウド管理の展開：有効にする Cisco Secure Client オプションを選択したら（Start Before Login、Diagnostics and Reporting Tool、Secure Firewall Posture、Network Visibility Module、Secure Umbrella、ISE Posture、Network Access Manager など）、SecureX UI の [展開管理（Deployment Management）] ページにある [ネットワークインストーラ（Network Installer）] ボタンをクリックします。この操作により、csc-deployment.exe ファイルがダウンロードされ、コマンドプロンプトで実行してクラウド管理サービスをインストールできます。クラウド管理サービスは、設定されたモジュールを自動的にダウンロードし、SecureX クラウドに接続します。その後、パッケージまたはプロファイル管理なしでクラウド登録を行うか、完全なクラウド管理を利用するかを選択できます。Cisco Secure Client は、クラウド管理の有無にかかわらず使用できます。
- XDR 内では、[クライアント管理（Client Management）]>[展開（Deployments）] に移動して Cisco XDR 組織内のすべての Secure Client 展開のリストを確認でき、ユーザーは、組織内の特定の展開ですべてのコンピュータにインストールする必要があるすべてのパッケージと関連プロファイルのリストを定義できます。詳細については、XDR のマニュアルを参照してください。

AnyConnect VPN を展開する場合に、追加機能を含めるオプションの Cisco Secure Client モジュール、および AnyConnect VPN やオプションの Cisco Secure Client 機能を設定するクライアントプロファイルを含めることができます。

Cisco Secure Firewall ASA、IOS、Microsoft Windows、Linux、および macOS のシステム、管理、およびエンドポイントの要件については、Cisco Secure Client のリリースノートを参照してください。

（注） 一部のサードパーティのアプリケーションおよびオペレーティングシステムにより、ISE ポスチャエージェントおよびその他のプロセスによる必要なファイルアクセスおよび権限昇格が制限される場合があります。Cisco Secure Client インストールディレクトリ（Windows の場合は C:\Program Files (x86)\Cisco または macOS の場合は /opt/cisco）がエンドポイントのウイルス対策、マルウェア対策、スパイウェア対策、データ損失防止、権限マネージャ、またはグループポリシーオブジェクトの許可/除外/信頼リストで信頼されていることを確認します。

また、サードパーティのセキュリティアプリケーション（ウイルス対策、スパイウェア対策、マルウェア対策、データ漏洩防止）により、エンドポイントでのライブラリの欠落が生じてコンプライアンスモジュールのアップグレードに失敗する可能性があります。この問題を回避するには、コンプライアンスモジュールのバージョンをアップグレードし、（サードパーティのセキュリティアプリケーションで）それを除外するように設定してから、コンプライアンスモジュールをアップグレードします。

```
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k0.pkg
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.exe
-cisco-secure-client-win-4.3.xxxx.xxxx-isecompliance-webdeploy-k9.msi
-opswat.msi
```

コンプライアンスモジュールは、SecureX Cloud Management デプロイメントの一部ではありません。

Cisco Secure Client のインストール方法の決定

Cisco Secure Client は、ISE 2.0（またはそれ以降）および Cisco Secure Firewall ASA ヘッドエンドによる Web 展開または事前展開が可能です。Cisco Secure Client をインストールするには、最初に管理者権限が必要です。

Web 展開

Cisco Secure Client をアップグレードする、または（ASA/ISE/Secure Firewall Threat Defense クラウドとダウンローダーからの）Web 展開を使用して追加のモジュールをインストールするには、管理者権限は必要ありません。

- Cisco Secure Firewall ASA または Secure Firewall Threat Defense からの Web 展開：ユーザーは、ヘッドエンドデバイス上の Cisco Secure Client クライアントレスポータルに接続して、Cisco Secure Client のダウンロードを選択します。Cisco Secure Firewall ASA は Cisco Secure Client ダウンローダーをダウンロードします。Cisco Secure Client ダウンローダーがクライアントをダウンロードし、クライアントをインストールし、VPN 接続を開始します。

- ISE からの Web 展開：ユーザーは、Cisco Secure Firewall ASA、ワイヤレスコントローラ、またはスイッチなどのネットワーク アクセス デバイス（NAD）に接続します。NAD はユーザを許可し、ISE ポータルにユーザをリダイレクトします。Cisco Secure Client ダウンローダーがクライアントにインストールされ、パッケージの抽出およびインストールを管理します。ただし、VPN 接続は開始しません。

事前展開

Cisco Secure Clientをアップグレードするか、事前展開（手動またはSCCM を使用したアウトオブバンド展開）を使用して追加のモジュールをインストールするには、管理者権限が必要です。

- 社内のソフトウェア管理システム（SMS）を使用します。
- Cisco Secure Client ファイルのアーカイブを手動で配布し、インストール方法に関する指示をユーザーに提供します。ファイルのアーカイブ形式は、zip（Windows）、DMG（macOS）、gzip（Linux）です。

システム要件およびライセンスの依存関係の詳細については、『Cisco Secure Client Features, License, and OS Guide』[英語] を参照してください。

（注） macOS または Linux プラットフォームでルート権限のアクティビティを実行するために Secure Firewall ポスチャを使用している場合は、Secure Firewall ポスチャ を事前展開することを推奨します。

Cisco Secure Client のインストールに必要なリソースの決定

Cisco Secure Client 展開は、複数の種類のファイルで構成されています。

- Cisco Secure Client パッケージに含まれている AnyConnect VPN。
- 追加機能をサポートするモジュール。Cisco Secure Client パッケージに含まれています。
- Cisco Secure Client および追加機能を設定するクライアントプロファイル。自分で作成します。
- 言語ファイル、画像、スクリプト、およびヘルプ ファイル（展開をカスタマイズまたはローカライズする場合）。
- ISE ポスチャおよびコンプライアンスモジュール（OPSWAT）。

Cisco Secure Client のためのエンドポイントの準備

Cisco Secure Client とモバイル ブロードバンド カードの使用方法

一部の 3G カードには、Cisco Secure Client を使用する前に必要な設定手順があります。たとえば、VZAccess Manager には次の 3 種類の設定があります。

- モデム手動接続（modem manually connects）
- ローミング時を除くモデム自動接続（modem auto connect except when roaming）
- LAN アダプタ自動接続（LAN adapter auto connect）

[LAN アダプタ自動接続（LAN adapter auto connect）] を選択した場合は、プリファレンスを NDIS モードに設定します。NDIS は、VZAccess Manager が終了されても接続を続行できる、常時接続です。VZAccess Manager では、Cisco Secure Client をインストールする準備が整うと、自動接続 LAN アダプタをデバイス接続のプリファレンスとして表示します。Cisco Secure Client インターフェイスが検出されると、3G マネージャはインターフェイスをドロップし、Cisco Secure Client 接続を許可します。

優先順位の高い接続に移動する場合（有線ネットワークが最も優先順位が高く、次に WiFi、モバイルブロードバンドの順になります）、Cisco Secure Client は古い切断を解除する前に新しい接続を確立します。

Internet Explorer でのプロキシ変更のブロック

ある条件下では、Cisco Secure Client によって Internet Explorer の [ツール（Tools）] > [インターネットオプション（Internet Options）] > [接続（Connections）] タブが非表示にされます（ロックされます）。このタブが表示されている場合、ユーザーはプロキシ情報を設定できます。このタブを非表示にすると、ユーザーが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックダウン設定は、接続を解除するときに反転します。タブのロックダウンは、そのタブに適用されている管理者定義のポリシーによって上書きされます。ロックダウンは、次の場合に適用されます。

- Cisco Secure Firewall ASA の設定で、[接続（Connections）] タブのロックダウンが指定されている
- Cisco Secure Firewall ASA の設定で、プライベート側プロキシが指定されている
- Windows のグループ ポリシーにより、以前に [接続（Connections）] タブがロックされている（no lockdown Cisco Secure Firewall ASA グループポリシー設定の上書き）

Windows 10 バージョン 1703（またはそれ以降）では、Cisco Secure Client は、Internet Explorer の [接続（Connections）] タブを非表示にすることに加えて、設定アプリのシステムプロキシタブも非表示に（ロックダウン）し、ユーザーが意図的または偶発的にトンネルを迂回しないようにします。このロックダウンは、接続を解除するときに反転します。

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 ナビゲーション ペインで、**[詳細（Advanced）] > [ブラウザ プロキシ（Browser Proxy）]** に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4 **[プロキシ ロックダウン（Proxy Lockdown）]** をクリックして、その他のプロキシ設定を表示します。

ステップ 5 [継承（Inherit）] をオフにし、次のいずれかを選択します。

- [はい（Yes）] を選択して、Cisco Secure Client セッションの間、プロキシのロックダウンを有効にし、Internet Explorer の [接続（Connections）] タブを非表示にします。
- [いいえ（No）] を選択して、Cisco Secure Client セッションの間、プロキシのロックダウンを無効にし、Internet Explorer の [接続（Connections）] タブを公開します。

ステップ 6 [OK] をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7 [適用（Apply）] をクリックして、グループ ポリシーの変更を保存します。

Cisco Secure Client による Windows RDP セッションの処理方法の設定

Cisco Secure Client は、Windows RDP セッションからの VPN 接続を許可するように設定できます。デフォルトでは、RDP によりコンピュータに接続されているユーザーは、Cisco Secure Client を使用して VPN 接続を開始できません。次の表に、RDP セッションからの VPN 接続のログインとログアウトのオプションを示します。これらの設定は、VPN クライアントプロファイルで設定されます。

[Windows ログインの強制（Windows Logon Enforcement）]：**SBL モードで使用可能**

- [シングルローカルログイン（Single Local Logon）]（デフォルト）：（ローカル：1、リモート：制限なし）VPN 接続全体で、ログインできるローカルユーザは 1 人だけです。また、クライアント PC に複数のリモート ユーザーがログインしている場合でも、ローカル ユーザーが VPN 接続を確立することはできます。この設定は、VPN 接続を介した企業ネットワークからのリモート ユーザー ログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

- [シングルログイン（Single Logon）]：（ローカル＋リモート：1）VPN 接続全体で、ログインできるユーザは1人だけです。VPN接続の確立時に、ローカルまたはリモートで複数のユーザがログインしている場合、接続は許可されません。VPN接続中にローカルまたはリモートで第 2 のユーザがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

（注） 複数同時ログオンはサポートされません。

- [シングルログイン（リモートなし）（Single Logon No Remote）]：（ローカル：1、リモート：0）VPN 接続全体で、ログインできるローカルユーザは 1 人だけです。リモートユーザは許可されません。VPN接続の確立時に、複数のローカルユーザまたはリモートユーザがログインしている場合、接続は許可されません。VPN接続中に第2のローカルユーザまたはリモートユーザがログインすると、VPN 接続が終了します。

[Windows VPN確立（Windows VPN Establishment）]：**SBL モードでは使用できません**

- [ローカルユーザのみ（Local Users Only）]（デフォルト）：リモート ログインしたユーザは、VPN 接続を確立できません。これは、以前のバージョンの AnyConnect と同じ機能です。
- [リモートユーザーを許可（Allow Remote Users）]：リモート ユーザーは VPN 接続を確立できます。ただし、設定された VPN 接続ルーティングによってリモート ユーザが接続解除された場合は、リモートユーザがクライアントPCに再アクセスできるように、VPN接続が終了します。リモートユーザがVPN接続を終了せずにリモートログインセッションを接続解除するには、VPN を確立した後、90 秒間待つ必要があります。

Cisco Secure Client による Linux SSH セッションの処理方法の設定

Cisco Secure Clientは、Linux SSHセッションからのVPN接続を許可するように設定できます。デフォルトでは、SSH によりコンピュータに接続されているユーザーは、Cisco Secure Client を使用して VPN 接続を開始できません。次の表に、SSH セッションからの VPN 接続のログインとログアウトのオプションを示します。これらのオプションは、VPN クライアントプロファイルで設定されます。

Linux ログイン適用：[シングルローカルログイン（Single Local Logon）]（デフォルト）：VPN 接続全体で、ログインできるローカル ユーザーは 1 人だけです。また、クライアント PC に複数のリモート ユーザーがログインしている場合でも、ローカル ユーザーが VPN 接続を確立することはできます。この設定は、VPN接続を介した企業ネットワークからのリモートユーザーログインに対しては影響を与えません。

（注） VPN 接続が排他的トンネリング用に設定されている場合、VPN 接続用のクライアント PC のルーティング テーブルが変更されるため、リモート ログインは接続解除されます。VPN 接続がスプリット トンネリング用に設定されている場合、リモート ログインが接続解除されるかどうかは、VPN 接続のルーティング設定によって異なります。

シングルログイン：VPN 接続全体で、ログインできるユーザーは 1 人だけです。VPN 接続の確立時に、（ローカルまたはリモートで）複数のユーザーがログインしている場合、接続は許可されません。（ローカルまたはリモートで）VPN 接続中に第 2 のユーザーがログインすると、VPN 接続が終了します。VPN 接続中の追加のログインは許可されません。そのため、VPN 接続によるリモート ログインは行えません。

Linux VPN の確立：

- [ローカルユーザーのみ（Local Users Only）]（デフォルト）：リモートログインしたユーザーは VPN 接続を確立できません。
- [リモートユーザーを許可（Allow Remote Users）]：リモート ユーザーは VPN 接続を確立できます。

Windows での DES-only SSL 暗号化

デフォルトでは、Windows は DES SSL 暗号化をサポートしません。Cisco Secure Firewall ASA に DES-only を設定した場合、Cisco Secure Client 接続は失敗します。これらのオペレーティングシステムの DES 対応設定は難しいため、Cisco Secure Firewall ASA には、DES-only SSL 暗号化を設定しないことをお勧めします。

Linux での Network Visibility Module の使用

Network Visibility Module を Linux 上で使用する場合は、事前にカーネル ドライバ フレームワーク（KDF）をセットアップする必要があります。Cisco Secure Client カーネルモジュールを事前構築するか、ターゲット上にドライバを構築するか、選択できます。ターゲット上に構築する場合、アクションは不要です。構築は、展開時またはリブート時に自動的に処理されます。

Cisco Secure Client カーネルモジュールを構築するための前提条件

ターゲット デバイスを準備します。

- GNU Make Utility がインストールされていることを確認します。
- 次のカーネル ヘッダー パッケージをインストールします。
  - RHEL の場合は、kernel-devel-2.6.32-642.13.1.el6.x86_64 などのパッケージ **kernel-devel-$(uname -r)** をインストールします。

- Ubuntu の場合は、linux-headers-4.2.0-27-generic などのパッケージ **linux-headers-$(uname -r)** をインストールします。
- Linux には、必要な libelf devel パッケージをインストールします。

- GCC コンパイラがインストールされていることを確認します。インストールされた GCC コンパイラの *major.minor* バージョンが、カーネルの構築に使用されている GCC のバージョンと一致している必要があります。これは、/proc/version ファイルで確認できます。

NVM の構築済み Cisco Secure Client Linux カーネルモジュールとのパッケージ化

始める前に

「Cisco Secure Client カーネルモジュールを構築するための前提条件 （8 ページ）」に記載されている前提条件を満たす必要があります。

Cisco Secure Client Network Visibility Module は、構築済みの Cisco Secure Client Linux カーネルモジュールとパッケージ化することができます。こうすると、特にターゲットデバイスの OS カーネルバージョンが同一である場合、すべてのターゲットデバイスに構築する必要がなくなります。事前構築の選択肢を使用しない場合、構築は展開時またはリブート時に、管理者による入力がなくても自動的に実行され、ターゲット上で使用できるようになります。また、展開がすべてのエンドポイントにおけるカーネルの前提条件を満たしていない場合は、事前作成オプションを使用できます。

（注） 構築済み Cisco Secure Client Linux カーネルモジュールでは、Web 展開はサポートされていません。

ステップ 1 Cisco Secure Client 事前展開パッケージ、cisco-secure-client-linux64-<*version*>-predeploy-k9.tar.gz を解凍します。

ステップ 2 nvm ディレクトリに移動します。

ステップ 3 次のスクリプトを呼び出します。**$sudo ./build_and_package_ac_ko.sh**

次のタスク

スクリプトを実行すると、構築済みの Cisco Secure Client Linux カーネルモジュールを含む cisco-secure-client-linux64-<*version*>**-ac_kdf_ko-k9.tar.gz** が作成されます。セキュアブートが有効になっているシステムでは、セキュアブートによって許可された秘密キーを使用してモジュールに署名します。このファイルは、事前展開にのみ使用することができます。

ターゲットデバイスの OS カーネルがアップグレードされたら、更新された Linux カーネルモジュールで Cisco Secure Client Network Visibility Module を再展開する必要があります。

Cisco Secure Client の事前展開

Cisco Secure Client は、SMS を使用した手動による事前展開が可能です。この場合、エンドユーザーがインストールできるファイルを配布するか、Cisco Secure Client ファイルアーカイブにユーザーが接続できるようにします。

Cisco Secure Client をインストールするためのファイルアーカイブを作成する場合、「Cisco Secure Client プロファイルを事前展開する場所 （13 ページ）」で説明するように、アーカイブのディレクトリ構造が、クライアントにインストールされるファイルのディレクトリ構造と一致する必要があります。

始める前に

- SecureX でプロファイルを作成または展開するときは、次の 2 つの要件が満たされていることを確認してください。
  - プロファイル名（VPN または任意の Cisco Secure モジュールプロファイルの場合）は、ASA/FTD ヘッドエンドや ISE で作成および設定されたプロファイルの名前と正確に一致する必要があります。
  - すべてのエンドポイントと展開でプロファイルの同期を維持するには、SecureX で作成されたプロファイルも ASA/FTD ヘッドエンドや ISE にインポートする必要があります。

    上記の要件に従わない場合、すべての環境でプロファイルの同期が維持されず、既存の展開で現在構成されている特定の機能が無効になる可能性があります。たとえば、VPN の使用時にリモートデスクトップ機能が必要な場合は、1) SecureX の VPN プロファイルでリモートデスクトップ機能を有効にし、2) ASA/FTD または ISE 環境で設定されたプロファイルでリモートデスクトップ機能を有効にします。

    Cisco Secure Firewall ASA で Cisco Secure Client プロファイル（旧名は AnyConnect）を設定せずに、アウトオブバンドで（SCCM、MDM、SecureX Cloud Management などを使用して）プロファイルを配布する場合は、UseLocalProfileAsAlternative カスタム属性を使用できます。このカスタム属性を設定すると、クライアントは設定とプリファレンスに (通常のデフォルトではなく) ローカル（ディスク上）の Cisco Secure Client プロファイルを使用します。ローカルプロファイルを使用したセッションの確立は、1) UseLocalProfileAsAlternative が有効に設定されている場合、および 2) ASA グループポリシープロファイルが設定されていない場合にのみ発生します。このカスタム属性を設定し、ASA のグループポリシー構成から Cisco Secure Client プロファイルを元に戻したり削除したりしない場合、グループポリシーで構成された Cisco Secure Client プロファイルが維持され、カスタム属性の設定が無視される各接続で使用されます。詳細については、『Cisco Secure Firewall ASA Series VPN ASDM Configuration Guide』（英語）の「Configure Secure Client Custom Attributes in an Internal Group Policy」を参照してください。

- 手動で VPN プロファイルを展開している場合、ヘッドエンドにもプロファイルをアップロードする必要があります。クライアントシステムが接続する場合、クライアントのプロファイルがヘッドエンドのプロファイルに一致することを Cisco Secure Client が確認します。プロファイルのアップデートを無効にしており、ヘッドエンド上のプロファイルがクライアントと異なる場合、手動で展開したプロファイルは動作しません。
- 手動で Cisco Secure Client ISE ポスチャプロファイルを展開する場合、ISE にもそのファイルをアップロードする必要があります。
- クローンされた VM を使用している場合は、「Cisco Secure Client を使用した VM のクローンに関するガイドライン（Windows のみ） （16 ページ）」を参照してください。

ステップ 1 Cisco Secure Client 事前展開パッケージをダウンロードします。

事前展開用の Cisco Secure Client ファイルは cisco.com で入手できます。

OS	Cisco Secure Client 事前展開パッケージ名
Windows	cisco-secure-client-win-version-predeploy-k9.zip
macOS	cisco-secure-client-macos-version-predeploy-k9.dmg
Linux（64 ビット）	（スクリプトインストーラーの場合） cisco-secure-client-linux64-version-predeploy-k9.tar.gz （RPM インストーラーの場合） cisco-secure-client-linux64- version -predeploy-rpm-k9.tar.gz （DEB インストーラーの場合） cisco-secure-client-linux64-*version*-predeploy-deb-k9.tar.gz

Secure Umbrella モジュールは、Linux オペレーティングシステムでは使用できません。

ステップ 2 クライアントプロファイルを作成します。一部のモジュールおよび機能にはクライアントプロファイルが必要です。

Cisco Secure Client プロファイルを必要とするモジュールは次のとおりです。

- AnyConnect VPN
- Network Access Manager
- ISE ポスチャ
- Cisco Secure Endpoint
- ネットワーク可視性モジュール
- Umbrella ローミング セキュア モジュール

Cisco Secure Client プロファイルを必要としないモジュールは次のとおりです。

- Start Before Login
- Diagnostic and Reporting Tool
- Secure Firewall 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
- ThousandEyes Endpoint Agent モジュール

ASDM でクライアント プロファイルを作成して、PC にこれらのファイルをコピーできます。または、Windows PC でスタンドアロンのプロファイルエディタを使用できます。

ステップ 3 任意で、「Cisco Secure Client とインストーラのカスタマイズとローカライズ」を行います。

ステップ 4 配布用ファイルを準備します。ファイルのディレクトリ構造は、「Cisco Secure Client プロファイルを事前展開する場所」で説明されています。

ステップ 5 Cisco Secure Client のインストール用ファイルをすべて作成したら、これらをアーカイブファイルで配布するか、クライアントにファイルをコピーできます。同じ Cisco Secure Client ファイルが、接続する予定のヘッドエンド、Cisco Secure Firewall ASA、および ISE などにも存在することを確認します。

事前展開と Web 展開向けの Cisco Secure Client モジュール実行可能ファイル

次の表に、Windows コンピュータに Zero Trust Access モジュール、Cisco Umbrella ローミング セキュリティ モジュール、Network Access Manager、ISE ポスチャ、Network Visibility Module、および Thousand Eyes Module の各クライアントを事前展開または Web 展開する際のエンドポイントコンピュータ上のファイル名を示します。

表 *1 : Web* 展開または事前展開のモジュールのファイル名

モジュール	Web 展開インストーラ（ダウンロード）	事前展開インストーラ
Zero Trust Access	cisco-secure-client-win-<*version*>-zta-webdeploy-k9.msi	cisco-secure-client-win-<*version*>-zta-predeploy-k9.msi
Network Access Manager	cisco-secure-client-win-バージョン -nam-webdeploy-k9.msi	cisco-secure-client-win-*version*-nam-predeploy-k9.msi
ISE ポスチャ	cisco-secure-client-win-バージョン -iseposture-webdeploy-k9.msi	cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi
ネットワーク可視性モジュール	cisco-secure-client-win-バージョン -nvm-webdeploy-k9.msi	cisco-secure-client-win-*version*-nvm-predeploy-k9.msi
Umbrella ローミングセキュリティ モジュール	cisco-secure-client-win-バージョン -umbrella-webdeploy-k9.msi	cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi

モジュール	Web 展開インストーラ（ダウンロード）	事前展開インストーラ
ThousandEyes Endpoint Agent モジュール	適用対象外	cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi

（注） Windows サーバー OS が存在する場合、Network Access Managerをインストールするときに、インストールエラーが発生することがあります。WLANサービスはサーバーのオペレーティングシステムにデフォルトではインストールされないため、このソフトウェアをインストールし、PC をリブートする必要があります。WLANAutoconfig サービスは、Network Access Managerがすべての Windows オペレーティング システムで機能するための要件です。

Cisco Secure Client プロファイルを事前展開する場所

クライアント システムにファイルをコピーする場合は、次の表に示す場所にファイルを配置する必要があります。

表 *2 : Cisco Secure Client* コア ファイル

ファイル	説明
anyfilename.xml	Cisco Secure Client プロファイル。このファイルは、特定のユーザ タイプに対して設定される機能および属性値を指定します。
AnyConnectProfile.xsd	XML スキーマ形式を定義します。Cisco Secure Client は、このファイルを使用してプロファイルを検証します。

表 *3 :* すべてのオペレーティング システムに対するプロファイルの場所

モジュール	参照先
Windows	
AnyConnect VPN プロファイル	%ProgramData%\Cisco\Cisco Secure Client\VPN\Profile
Zero Trust Access	（バイナリ）C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA （設定およびその他のファイル）C:\ProgramData\Cisco\Cisco Secure Client\ZTA
Network Access Manager	%ProgramData%\Cisco\ Cisco Secure Client\Network Access Manager\newConfigFiles
カスタマー エクスペリエンスのフィードバック	%ProgramData%\Cisco\ Cisco Secure Client\CustomerExperienceFeedback

モジュール	参照先
ISE ポスチャ	%ProgramData%\Cisco\Cisco Secure Client\ISE Posture
Cisco Secure Endpoint	%ProgramData%\Cisco\AMP
ネットワーク可視性モジュール	%ProgramData%\Cisco\Cisco Secure Client\NVM
Umbrella ローミング セキュリティ モジュール	%ProgramData%\Cisco\Cisco Secure Client\Umbrella （注） Umbrella ローミング セキュリティ モジュールを有効にするためには、Umbrella ダッシュボードから OrgInfo.json ファイルをコピーして、名前を変更しないでこの対象ディレクトリに配置する必要があります。または、インストールする前にファイルを \Profiles\umbrella に配置して、OrgInfo.json ファイルと Umbrella ローミング セキュリティ モジュール インストーラを同じ場所に置くこともできます。
macOS	
ISE ポスチャ	/opt/cisco/secureclient/iseposture/
AMP イネーブラ	/opt/cisco/secureclient/AMPEnabler/
ネットワーク可視性モジュール	/opt/cisco/secureclient/NVM/
Umbrella ローミング セキュリティ モジュール	/opt/cisco/secureclient/umbrella （注） Umbrella ローミング セキュリティ モジュールを有効にするためには、Umbrella ダッシュボードから OrgInfo.json ファイルをコピーして、名前を変更しないでこの対象ディレクトリに配置する必要があります。または、インストールする前にファイルを \Profiles\umbrella に配置して、OrgInfo.json ファイルと Umbrella ローミング セキュリティ モジュール インストーラを同じ場所に置くこともできます。
AnyConnect VPN プロファイル	/opt/cisco/secureclient/vpn/profile
Linux	
NVM	/opt/cisco/secureclient/NVM
AnyConnect VPN プロファイル	/opt/cisco/secureclient/vpn/profile

その他の Cisco Secure Client ファイルの場所

カスタマイズとローカリゼーション：**Windows**

- **L10N**
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\l10n
- リソース
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\UI\res

カスタマイズとローカリゼーション：**macOS** および **Linux**

- **L10N**
  - /opt/cisco/secureclient/l10n
- リソース
  - /opt/cisco/secureclient/resources

macOS バイナリ、ライブラリ、および **UI** リソース

- **UI** リソース
  - /Applications/Cisco/Cisco Secure Client.app/Contents/Resources/
- バイナリ
  - /opt/cisco/secureclient/bin
- ライブラリ
  - /opt/cisco/secureclient/lib

ヘルプ

- **Windows**
  - %ALLUSERSPROFILE%\Cisco\Cisco Secure Client\Help
- **macOS** および **Linux**
  - /opt/cisco/secureclient/help

OPSWAT ライブラリ

ISE ポスチャと Secure Firewall ポスチャ で使用

- **Windows**
  - %PROGRAMFILES%\Cisco\Cisco Secure Client\OPSWAT
- **macOS**

  /opt/cisco/secureclient/lib/opswat

Cisco Secure Client を使用した VM のクローンに関するガイドライン（Windows のみ）

Cisco Secure Client エンドポイントは、Cisco Secure Client のすべてのモジュールが使用するユニバーサルデバイス識別子（UDID）によって一意に識別されます。Windows VM が複製されると、UDID は送信元からのすべてのクローンで同じままになります。複製された VM で発生する可能性のある問題を回避するには、Cisco Secure Client を使用する前に次のアクションを実行します。

1. **%ProgramFiles(x86)%\Cisco\Cisco Secure Client\DART** に移動し、管理者権限で次のように dartcli.exe を実行します。

   ```
   dartcli.exe -nu
   ```

   または

   ```
   dartcli.exe -newudid
   ```

2. このコマンドで UDID が変更されたことを確認するため、このコマンドの前と後で UDID を出力します。

   ```
   dartcli.exe -u
   ```

   または

   ```
   dartcli.exe -udid
   ```

スタンドアロンアプリケーションとしての Cisco Secure Client モジュールの事前展開

Network Access Manager、Umbrella ローミング セキュリティ モジュール、 ThousandEyes Endpoint Agent モジュールなどのモジュールは、スタンドアロン アプリケーションとして実行できます。Cisco Secure Client はインストールされていますが、VPN および Cisco Secure Client UI は使用されません。

Windows での SMS によるスタンドアロンモジュールの展開

ステップ 1 ソフトウェア管理システム（SMS）を設定して MSI プロパティ PRE_DEPLOY_DISABLE_VPN=1 を設定し、VPN 機能を無効にします。次に例を示します。

```
msiexec /package cisco-secure-client-win-version-core-vpn-predeploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

MSI は、MSI に埋め込まれた VPNDisable_ServiceProfile.xml ファイルを VPN 機能のプロファイルに指定されたディレクトリにコピーします。

ステップ 2 モジュールをインストールします。たとえば、次の CLI コマンドは、Cisco Umbrella をインストールします。

```
msiexec /package cisco-secure-client-win-version-umbrella-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

ステップ 3 （任意）DART をインストールします。

```
misexec /package cisco-secure-client-win-version-dart-predeploy-k9.msi /norestart /passive /lvx*
c:\test.log
```

ステップ 4 難解化 クライアント プロファイルのコピーを、正しい Windows フォルダに保存します。

ステップ 5 Cisco Cisco Secure Client サービスを再起動します。

スタンドアロン アプリケーションとしての Cisco Secure Client モジュールの展開

要件

VPNDisable_ServiceProfile.xml ファイルは、VPN クライアント プロファイル ディレクトリにある唯一の Cisco Secure Client プロファイルである必要もあります。

スタンドアロンモジュールのユーザインストール

個別のインストーラを取得して、手動で配布できます。

zipイメージをユーザが使用できるようにし、それをインストールするように要求する場合は、スタンドアロンモジュールだけをインストールするように指示してください。

（注） コンピュータ上にNetwork Access Managerが事前にインストールされていなかった場合、ユーザは、Network Access Managerのインストールを完了するためにコンピュータをリブートする必要があります。一部のシステム ファイルのアップグレードを必要とする、アップグレードインストールの場合も、ユーザはリブートを必要とします。

ステップ 1 Cisco Secure Client Network Access Manager、Secure Umbrella モジュール、または ThousandEyes Endpoint Agent モジュールを確認するようにユーザーに指示します。

ステップ 2 [Cisco AnyConnect VPN モジュール（Cisco AnyConnect VPN Module）] チェックボックスをオフにするようユーザに指示します。

このようにすると、コアクライアントの VPN 機能が無効になり、Network Access Manager Module、Secure Umbrella モジュール、または ThousandEyes Endpoint Agent モジュールが、インストールユーティリティによって、VPN 機能なしのスタンドアロン アプリケーションとしてインストールされます。

ステップ 3 （任意）[ロックダウン コンポーネント サービス（Lock Down Component Services）] チェックボックスをオンにします。ロックダウンコンポーネントサービスによって、ユーザは、Windows サービスを無効または停止できなくなります。

ステップ 4 オプションモジュール用のインストーラを実行するようにユーザーに指示します。このインストーラでは、VPN サービスなしで Cisco Secure Client GUI を使用できます。ユーザが [選択済みをインストール（Install Selected）] ボタンをクリックすると、次の処理が行われます。

a) スタンドアロン Network Access Manager Module、Umbrella ローミング セキュリティ モジュール、または ThousandEyes Endpoint Agent Module の選択を確認するポップアップ ダイアログボックスが表示されます。

b) ユーザーが [OK] をクリックすると、設定値 PRE_DEPLOY_DISABLE_VPN=1 を使用して、インストールユーティリティにより、Cisco Secure Client インストーラが起動されます。

c) インストール ユーティリティは、既存のすべての VPN プロファイルを削除してから VPNDisable_ServiceProfile.xml をインストールします。

d) インストールユーティリティは、指定に応じて、Network Access Manager、Secure Umbrella、または ThousandEyes Endpoint Agent モジュールインストーラを起動します。

e) 指定に応じて、Network Access Manager Module、Secure Umbrella モジュール、または ThousandEyes Endpoint Agent が、コンピュータ上で VPN サービスなしで有効になります。

Windows への事前展開

zip ファイルを使用した Cisco Secure Client の配布

この zip パッケージファイルは、インストールユーティリティ、個々のコンポーネントインストーラを起動するセレクタ メニュー プログラム、Cisco Secure Client のコアモジュールとオプションモジュール用の MSI を含みます。zip パッケージ ファイルをユーザに対して使用可能にすると、ユーザはセットアップ プログラム（setup.exe）を実行します。このプログラムでは、インストール ユーティリティ メニューが表示されます。このメニューから、ユーザーはインストールする Cisco Secure Client モジュールを選択します。多くの場合、ロードするモジュールをユーザが選択しないようにする必要があります。したがって、zip ファイルを使用して配布する場合は、zip を編集し、使用されないようにするモジュールを除外して、HTA ファイルを編集します。

ISO を配布する 1 つの方法は、SlySoft や PowerIS などの仮想 CD マウント ソフトウェアを使用することです。

事前展開 zip の変更

- ファイルをバンドルしたときに作成したすべてのプロファイルを使用して zip ファイルを更新し、配布しないモジュールのインストーラをすべて削除します。

- HTA ファイルを編集して、インストール メニューをカスタマイズし、配布しないモジュールのインストーラへのリンクをすべて削除します。

Cisco Secure Client zip ファイルの内容

ファイル	目的
GUI.ico	Cisco Secure Client のアイコン画像。
Setup.exe	インストール ユーティリティを起動します。
cisco-secure-client-win-*version*-dart-predeploy-k9.msi	DART モジュール用 MSI インストーラファイル。
cisco-secure-client-win-<*version*>-zta-predeploy-k9.msi	Zero Trust Access 用の MSI インストーラファイル
cisco-secure-client-win-*version*-SBL-predeploy-k9.msi	SBL モジュール用 MSI インストーラファイル。
cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi	ISE ポスチャモジュール用 MSI インストーラ。
cisco-secure-client-win-*version*-nvm-predeploy-k9.msi	ネットワーク可視性モジュール用 MSI インストーラ ファイル。
cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi	Umbrella ローミング セキュリティ モジュール用 MSI インストーラ ファイル。
cisco-secure-client-win-*version*-nam-predeploy-k9.msi	Network Access Manager モジュール用 MSI インストーラ ファイル。
cisco-secure-client-win-*version*-posture-predeploy-k9.msi	ポスチャモジュール用 MSI インストーラファイル。
cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi	ThousandEyes Endpoint Agent モジュールの MSI インストーラファイル。
cisco-secure-client-win-*version*-core-predeploy-k9.msi	AnyConnect VPN モジュール用 MSI インストーラファイル。
autorun.inf	setup.exe の情報ファイル。
eula.html	Acceptable Use Policy（アクセプタブル ユース ポリシー）の略。
setup.hta	サイトに合わせてカスタマイズできる、インストールユーティリティ HTML アプリケーション（HTA）。

SMS を使用した Cisco Secure Client の配布

展開するモジュールのインストーラ（*.msi）を zip イメージから抽出した後で、これらを手動で配布できます。

要件

- Cisco Secure Client を Windows にインストールする場合、AlwaysInstallElevated または Windows User Account Control（UAC）グループポリシー設定のいずれかを無効にする必要があります。無効にしないと、Cisco Secure Client インストーラはインストールに必要な一部のディレクトリにアクセスできない場合があります。

- Microsoft Internet Explorer（MSIE）ユーザーは、信頼済みサイト リストにヘッドエンドを追加するか、Java をインストールする必要があります。信頼済みサイトのリストへの追加により、最低限のユーザー操作で ActiveX コントロールによるインストールが可能になります。

プロファイルの展開プロセス

- MSI インストーラを使用する場合、MSI が Profiles\vpn フォルダに配置されている任意のプロファイルを選択し、インストール中に適切なフォルダに配置します。適切なフォルダパスは、CCO で使用可能な事前展開 MSI ファイルに含まれています。
- インストール後にプロファイルを手動で事前展開する場合は、手動か、Altiris などの SMS を使用してプロファイルをコピーすることにより、適切なフォルダにプロファイルを展開します。
- クライアントに事前展開したプロファイルと同じクライアントプロファイルを、必ずヘッドエンドにも配置してください。このプロファイルは、Cisco Secure Firewall ASA で使用されるグループポリシーに結合する必要もあります。クライアントプロファイルがヘッドエンドのものと一致しないか、グループポリシーに結合されていない場合は、アクセスの拒否など、一貫性のない動作を招く可能性があります。
- 次の表は、ログファイル名の推奨事項を示しています。推奨事項に従うことで、予測可能な場所が得られ、DART コレクション内で目的のログを見つけやすくなります。同様に、提供されているコマンドの例は、ユーザーが望まない機能を提供する場合があります。たとえば、カスタマー エクスペリエンス フィードバック コマンドは、デフォルトで有効になっているフィードバックを無効にします。

Windows 事前展開 MSI の例

インストールされるモジュール	コマンドおよびログ ファイル
Cisco Secure コアクライアント：VPN 機能なし。 （スタンドアロンモジュールのインストール時に使用。）	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Cisco Secure コアクライアント（VPN 機能あり） （スタンドアロンモジュールのインストール時を除くすべての場合に使用。）	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Zero Trust Access	msiexec /package cisco-secure-client-win-*version*-zta-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-<*version*>-zta-predeploy-k9-install-datetimestamp.log

インストールされるモジュール	コマンドおよびログ ファイル
カスタマー エクスペリエンスのフィードバック	msiexec /package cisco-secure-client-win-*version*-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* cisco-secure-client-win-*version*-core-vpn-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool（DART）	msiexec /package cisco-secure-client-win-*version*-dart-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package cisco-secure-client-win-*version*-SBL-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-SBL-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package cisco-secure-client-win-*version*-nam-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-nam-predeploy-k9-install-datetimestamp.log
Secure Firewall ポスチャ	msiexec /package cisco-secure-client-win-*version*-posture-predeploy-k9.msi /norestart/passive /lvx* cisco-secure-client-win-*version*-posture-predeploy-k9-install-datetimestamp.log
ISE ポスチャ	msiexec /package cisco-secure-client-win-*version*-iseposture-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-iseposture-predeploy-k9-install-datetimestamp.log
ネットワーク可視性モジュール	msiexec /package cisco-secure-client-win-*version*-nvm-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-win-*version*-nvm-predeploy-k9-install-datetimestamp.log
Umbrella ローミング セキュリティ	msiexec /package cisco-secure-client-win-*version*-umbrella-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-*version*-umbrella-predeploy-k9-install-datetimestamp.log
ThousandEyes Endpoint Agent モジュール	msiexec /package cisco-secure-client-win-*version*-thousandeyes-predeploy-k9.msi /norestart /passive /lvx* cisco-secure-client-*version*-thousandeyes-predeploy-k9-install-datetimestamp.log

Cisco Secure Client の Windows トランスフォームの例

サンプルの Windows トランスフォームが、その使用方法を説明したドキュメントとともに用意されています。下線文字（_）で始まるトランスフォームは、一般的な Windows トランスフォームで、特定のモジュールインストーラに特定のトランスフォームのみを適用できます。英文字で始まるトランスフォームは VPN トランスフォームです。各トランスフォームには、その使用方法を説明したマニュアルがあります。トランスフォーム ダウンロードは sampleTransforms-*x.x.x*.zip です。

Windows 事前展開セキュリティ オプション

Cisco Secure Client をホストするデバイスでは、エンド ユーザに限定的なアクセス権を与えることを推奨します。エンドユーザに追加の権限を与える場合、インストーラでは、エンドポイントでロックダウン済みとして設定されている Windows サービスをユーザとローカル管理者がオフにしたり停止したりできないようにするロックダウン機能を提供できます。ロックダウンサービスオプションを有効にすると、管理者権限がある場合は、すべての Cisco Secure Client モジュールをアンインストールすることもできます。

Windows ロックダウン プロパティ

各 MSI インストーラでは、共通のプロパティ（LOCKDOWN）がサポートされます。これは、ゼロ以外の値に設定されている場合に、そのインストーラに関連付けられた Windows サービスがエンドポイントデバイスでユーザまたはローカル管理者によって制御されないようにします。インストール時に提供されるサンプルのトランスフォーム（tools-cisco-secure-client-win-X.X.xxxx-transforms.zip）を使用して、このプロパティを設定し、ロックダウンする各 MSI インストーラにトランスフォームを適用することを推奨します。ロックダウン オプションも ISO インストール ユーティリティ内のチェックボックスです。

[プログラムの追加と削除（Add/Remove Program List）] リストでの Cisco Secure Client の非表示

Windows のプログラムの追加と削除リストを表示するユーザに対して、インストールされている Cisco Secure Client モジュールを非表示にできます。Cisco Secure Client サービスを開始または停止することはできません。ARPSYSTEMCOMPONENT=1 を使用して任意のインストーラを起動した場合、そのモジュールは、Windows の [プログラムの追加と削除（Add/Remove Program List）] リストに表示されません。

サンプルのトランスフォーム（tools-cisco-secure-client-win-X.X.xxxxx-transforms.zip）を使用して、このプロパティを設定することを推奨します。非表示にするモジュールごとに、各 MSI インストーラにトランスフォームを適用します。

Windows での Cisco Secure Client モジュールのインストールおよび削除の順序

モジュールのインストーラは、インストールを開始する前に、インストーラがコア クライアントと同じバージョンであることを確認します。バージョンが一致しない場合は、モジュールはインストールされず、不一致がユーザに通知されます。インストールユーティリティを使用する場合は、パッケージ内のモジュールが、まとめてビルドおよびパッケージ化されるため、バージョンは常に一致します。

ステップ 1 Cisco Secure Client モジュールは次の順番でインストールします。

a) Cisco Secure Client コアクライアントモジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

Windows および macOS では、制限付きユーザ アカウント（ciscoacvpnuser）が作成され、管理トンネル機能が有効として検出された場合にのみ、最小権限の原則が適用されます。このアカウントは、Cisco Secure Client のアンインストール中、またはインストールのアップグレード中に削除されます。

b) Cisco Secure Client Diagnostic and Reporting Tool（DART）モジュールをインストールします。このモジュールは、Cisco Secure Client クライアントインストールに関する有用な診断情報を提供します。
c) Umbrella ローミングセキュリティ、Network Visibility Module、、SBL、Network Access Manager、ポスチャモジュール、ISE 準拠モジュールを任意の順序でインストールします。

ステップ 2 Cisco Secure Client モジュールは次の順番でアンインストールします。

a) Umbrella ローミング セキュリティ、Network Visibility Module、、Network Access Manager、ポスチャ、ISE 準拠モジュール、または SBL を任意の順序でアンインストールします。
b) Cisco Secure Client コアクライアントモジュールをアンインストールします。
c) 最後に DART をアンインストールします。

DART 情報は、万一アンインストール プロセスが失敗した場合に役立ちます。Secure Clientをアンインストールしても、ThousandEyes Endpoint Agent モジュールはアンインストールされません。個別のアンインストールが必要です。

AnyConnect VPN をアンインストールすると、Duo Desktop と ThousandEyes を除き、Zero Trust Access を含むすべてのモジュールがアンインストールされます。Zero Trust Access を個別にアンインストールすることもできます。

（注） 設計上、一部の XML ファイルは Cisco Secure Client のアンインストール後もそのままの状態です。

macOS への事前展開

macOS での Cisco Secure Client のインストールおよびアンインストール

macOS 向け Cisco Secure Client は、すべての Cisco Secure Client モジュールを含む DMG ファイルで配布されます。ユーザーが DMG ファイルを開き、cisco-secure-client.pkg ファイルを実行すると、インストールダイアログが開始され、インストール方法が手順を追って説明されます。[インストール タイプ（Installation Type）] 画面で、ユーザはインストールするパッケージ（モジュール）を選択できます。

Zero Trust Access モジュールは、macOS の Web 展開パッケージには含まれていません。

Cisco Secure Client 5 は、Apple がサポートするすべてのバージョンの macOS 11 をサポートします。

ディストリビューションから Cisco Secure Client モジュールを削除するには、Finder で Cisco Secure Client アンインストーラを実行し、[アプリケーション（Applications）] > [Cisco] に移動して、[アンインストール（Uninstall）] をダブルクリックします。または、/opt/cisco/secure client/bin で VPN vpn_uninstall.sh スクリプトを実行します。

AnyConnect VPN をアンインストールすると、Zero Trust Access が削除されます。また、sudo を使用して次のシェルスクリプトを実行し、Zero Trust Access のみを削除できます：/opt/cisco/secureclient/bin/zta_uninstall.sh

macOS 事前展開用にプロファイルを配置するための書き込みアクセス許可を取得する

次の手順では、モジュールをカスタマイズし、プロファイルを作成し、そのプロファイルを DMG パッケージに追加する方法について説明します。ファイルを埋め込みプロファイルフォルダにコピーする前に、インストーライメージの書き込み権限を確立する必要があります。また、ブート時に自動的に起動するように Cisco Secure Client ユーザーインターフェイスを設定し、モジュールに必要なユーザーおよびグループ情報を Cisco Secure Client が提供できるようにします。

ステップ 1 Cisco Secure Client DMG パッケージ（Network Visibility Module の cisco-secure-client-macos-<version>-nvm-standalone.dmg など）を Cisco.com でダウンロードします。

ステップ 2 インストールプロセス中に、表示されるシステム拡張ポップアップを承認します。
インストールが完了すると、スタンドアロンアプリケーションがエンドポイントにインストールされ、サポートファイルが適切なモジュールの /opt/cisco/secureclient ディレクトリに配置されます。たとえば、Network Visibility Module の場合、ファイルは /opt/cisco/secureclient/nvm に配置されます。

ステップ 3 ファイルを開いて、インストーラにアクセスします。ダウンロードしたイメージは読み取り専用ファイルです。

ステップ 4 ディスクユーティリティを実行するか、次のようにターミナルアプリケーションを使用して、インストーライメージを書き込み可能にします。`hdiutil convert <source dmg> -format UDRW -o <output dmg>`

ステップ 5 Windows オペレーティング システムが実行されているコンピュータにスタンドアロンのプロファイルエディタをインストールします。カスタムインストールの一部として Cisco Secure Client モジュールを選択するか、完全インストールを実行する必要があります。デフォルトではインストールされていません。

ステップ 6 プロファイルエディタを起動し、必要な構成でプロファイルを作成します。

ステップ 7 例として Network Visibility Module を使用して、以下の手順でプロファイルを適切に保存する方法を説明します。次の手順に従い、プロファイルエディタで Network Visibility Module 用に難解化バージョンのプロファイル（NVM_ServiceProfile.wso など）を作成し、ファイル（NVM_ServiceProfile.xml など）を保存したのと同じ場所に保存します。

a) 指定した .wso ファイルを Windows デバイスから適切なフォルダパス（Cisco Secure Clientx.x.x/Profiles/NVM など）の macOS インストーラパッケージにコピーします。または、Network Visibility Module インスタンスに対して、次のようにターミナルアプリケーションを使用します。`cp <path to the wso> \Volumes\"Cisco Secure Client <VERSION>"\Profiles\nvm\`

b) macOS インストーラで、Cisco Secure Clientx.x.x/Profiles ディレクトリに移動し、編集用に TextEdit で ACTransforms.xml ファイルを開きます。VPN 機能がインストールされないように、<DisableVPN> 要素を **true** に設定します。`<ACTransforms><DisableVPN>true</DisableVPN></ACTransforms>`

c) これで、Cisco Secure Client DMG パッケージをユーザーに配布する準備ができました。

macOS 上のアプリケーションの制限

ゲートキーパーは、システムでの実行を許可するアプリケーションを制限します。次からダウンロードされたアプリケーションを許可するか選択できます。

- Mac App Store
- Mac App Store and identified developers
- あらゆる場所

デフォルト設定は Mac App Store and identified developers（署名付きアプリケーション）です。

Cisco Secure Client の現在のバージョンは、Apple が発行した証明書を使用して署名されており、Apple によって公証されています。ゲートキーパーが Mac App Store（のみ）に設定されている場合、事前展開されたインストールから Cisco Secure Client をインストールして実行するには、[App Store および特定されたデベロッパー（App Store and identified developers）] 設定を選択するか、または Ctrl キーを押しながらクリックして選択した設定をバイパスする必要があります。詳細については、「Safely open apps on your Mac」[英語] を参照してください。

macOS 11 以降での Duo Desktop の追加要件

Zero Trust Access モジュールには Duo Desktop のインストールが含まれており、macOS 11 以降で MDM を介して Zero Trust Access を展開する場合に必要な独自の追加セットアップ要件があります。

これらの追加の Duo セットアップ要件については、「Guide to Duo Device Health App certificate deployment for macOS 11+ users」を参照してください。

Linux への事前展開

Linux 用モジュールのインストール

Linux 用の個々のインストーラを取り出して、手動で配布できます。事前展開パッケージ内の各インストーラは、個別に実行できます。tar.gz ファイル内のファイルの表示および解凍には、圧縮ファイル ユーティリティを使用します。

ステップ 1 Cisco Secure Client コア VPN モジュールをインストールします。このモジュールは、GUI および VPN 機能（SSL、IPsec の両方）をインストールします。

ステップ 2 DART モジュールをインストールします。このモジュールは、Cisco Secure Client コア VPN およびその他のインストールされたモジュールに関する診断情報を提供します。

ステップ 3 ポスチャ モジュールまたは ISE 準拠モジュールをインストールします。

ステップ 4 Network Visibility Module をインストールします。

アップグレードに RPM または DEB インストーラを使用

RPM/DEB インストーラを使用して、スクリプトによってインストールされたバージョンからアップグレードする場合、次の制限があります。

- ヘッドエンドからの自動クライアント更新はサポートされていません。システムパッケージ マネージャを使用して、アウトオブバンドで更新を行う必要があります。
- RPM および DEB インストーラでサポートされる Cisco Secure Client モジュールは、VPN と DART のみです。
- RPM または DEB インストーラの使用に切り替える前に、現在の既存の Cisco Secure Client（すべてのモジュールを含む）をアンインストールする必要があります。
- スクリプトインストーラを使用して、既存の RPM または DEB のインストールを更新することはできません。

Linux 用モジュールのアンインストール

ユーザーが Cisco Secure Client をアンインストールする順序は重要です。

DART 情報は、アンインストール プロセスが失敗した場合に役立ちます。

ステップ 1 Network Visibility Module をアンインストールします。
ステップ 2 ポスチャ モジュールまたは ISE 準拠モジュールをアンインストールします。
ステップ 3 Cisco Secure Client コア VPN モジュールをアンインストールします。
ステップ 4 DART をアンインストールします。

Linux デバイスへの NVM の手動インストール/アンインストール

ステップ 1 Cisco Secure Client 事前展開パッケージを解凍します。
ステップ 2 nvm ディレクトリに移動します。
ステップ 3 次のスクリプトを呼び出します。**$sudo ./nvm_install.sh**

/opt/cisco/secureclient/bin/nvm_uninstall.sh. を使用して、Network Visibility Module をアンインストールできます。

サーバ証明書の検証用の証明書ストア

デフォルトでは、Cisco Secure Client は、システム CA 証明書の場所 （/etc/ssl/certs）を含む、PEM ファイル証明書ストアを使用してサーバー証明書を検証します。NSS 証明書ストアも、Cisco Secure Client でサーバー証明書を検証するために使用できます。

NSS 証明書ストアをアクティブにする方法

次のいずれかのオプションに従います。

- フォルダ ~/.cisco/certificates/nssdb を作成します。Cisco Secure Client は、このパスを使用して NSS 証明書データベースを保存します。このフォルダは OnConnect スクリプトで作成できます。
- Cisco Secure Client が現在のユーザの Firefox のデフォルトプロファイル内の NSS 証明書データベースを検索して使用するように指定します。Snap または Flatpak を介してインストールされた Firefox はサポートされていません。

インストールされている Firefox ブラウザを起動したことがない場合は、Firefox にデフォルトのプロファイルを生成させるために、最初に起動する必要があります。

NSS 証明書ストアを使用しない場合

Firefox NSS 証明書ストアを除外するようにローカルポリシーを設定し、PEM ファイル証明書ストアを有効にしておく必要があります。

複数モジュールの要件

1 つ以上のオプション モジュールに加えてコア クライアントを展開する場合、ロックダウン プロパティを各インストーラに適用する必要があります。

このアクションは、VPN インストーラ、Network Access Manager、Network Visibility Module、および Umbrella ローミング セキュリティ モジュールに使用できます。

（注） VPN インストーラのロックダウンをアクティブにすると、その結果として Cisco Secure Endpoint もロックダウンされます。

Linux デバイスへの DART の手動インストール

1. ciscosecureclient-dart-linux-(ver)-k9.tar.gz をローカルに保存します。
2. 端末から、**tar -zxvf <***path to tar.gz file including the file name* コマンドを使用して tar.gz ファイルを抽出します。
3. 端末から、抽出したフォルダに移動し、**sudo ./dart_install.sh** コマンドを使用して dart_install.sh を実行します。
4. ライセンス契約書に同意し、インストールが完了するまで待機します。

（注） DART のアンインストールには、**/opt/cisco/ciscosecureclient/dart/dart_uninstall.sh** しか使用できません。

Cisco Secure Client の Web 展開

Web 展開とは、クライアントシステム上の Cisco Secure Client ダウンローダーがヘッドエンドから Cisco Secure Client ソフトウェアを取得するか、またはヘッドエンドのポータルを使用して Cisco Secure Client をインストールまたは更新することです。ブラウザのサポート（および Java と ActiveX の要件）にあまりにも大きく依存していた従来の Web 起動に代わり、自動 Web 展開のフローを改善しました。このフローは、クライアントレスページからの初期ダウンロードおよび開始時に提示されます。自動プロビジョニング（Weblaunch）は、Internet Explorer ブラウザを備えた Windows オペレーティングシステムでのみ動作します。

Cisco Secure Firewall ASA を使用した Web 展開

Cisco Secure Firewall ASA のクライアントレスポータルは、Cisco Secure Client を Web 展開します。

ユーザーがブラウザを開き、Cisco Secure Firewall ASA のクライアントレスポータルに接続します。ポータルで、ユーザが **[AnyConnectクライアントの起動（Start AnyConnect Client）]** ボタンをクリックします。これで、Cisco Secure Client パッケージを手動でダウンロードできます。

別の方法を使用してソフトウェアアップデートを行っている場合、またはプロファイルエディタを ASDM と統合する必要がない場合は、Secure Firewall ASA で Cisco Secure Client Web 展開パッケージを設定する必要はありません。

Cisco Secure Firewall ASA における Web 展開の制限

- 同じオペレーティングシステム用の複数の Cisco Secure Client パッケージを Cisco Secure Firewall ASA にロードすることはサポートされていません。
- OPSWAT 定義は、Web 展開時には Secure Firewall ポスチャ モジュールに含まれません。OPSWAT 定義をクライアントに配信するには、Secure Firewall ポスチャ モジュールを手動で展開するか、または ASA にロードする必要があります。
- Cisco Secure Firewall ASA にデフォルトの内部フラッシュメモリサイズしかない場合、ASA に複数の Cisco Secure Client パッケージを保存およびロードすると問題が生じる可能性があります。フラッシュメモリにパッケージファイルを保持するために十分な容量がある場合でも、クライアントイメージの unzip とロードのときに Cisco Secure Firewall ASA のキャッシュメモリが不足する場合があります。Cisco Secure Client 展開時および ASA メモリのアップグレード時の Cisco Secure Firewall ASA メモリ要件の詳細については、VPN アプライアンスの最新のリリースノートを参照してください。
- ユーザーは IP アドレスまたは DNS を使用して Cisco Secure Firewall ASA に接続できますが、リンクローカル セキュア ゲートウェイ アドレスはサポートされていません。
- Windows ユーザーは、インストールまたは初回使用前に、Microsoft .NET Framework 4.6.2 以降をインストールすることを推奨します。起動時に、Umbrella サービスは .NET Framework 4.0（または以上）がインストールされているかどうかを確認します。検出されない場合は、Umbrella モジュールはアクティブにならず、メッセージが表示されます。.NET

Framework にアクセスし、これをインストールするには、再起動して Umbrella モジュールを有効にする必要があります。

ISE による Web 展開

ISE のポリシーでは、Cisco Secure Client をいつ展開するかを指定します。ユーザーがブラウザを開き、ISE によって制御されるリソースに接続すると、ユーザーは Cisco Secure Client ポータルにリダイレクトされます。その ISE ポータルでは、ユーザーが Cisco Secure Client をダウンロードし、インストールできます。ポータルによって Network Setup Assistant がダウンロードされ、ユーザーがそれを使用して Cisco Secure Client をインストールします。

ISE 展開の制限

- ISE と Cisco Secure Firewall ASA の両方が Cisco Secure Client を Web 展開する場合は、設定が両方のヘッドエンドで一致する必要があります。
- ISE サーバーが Cisco Secure Client ISE ポスチャエージェントによって検出されるのは、そのエージェントが ISE クライアント プロビジョニング ポリシーに設定されている場合だけです。ISE 管理者は、[エージェント設定（Agent Configuration）] > [ポリシー（Policy）] > [クライアントプロビジョニング（Client Provisioning）] で NAC Agent または Cisco Secure Client ISE ポスチャ モジュールを設定します。

ASA での Web 展開の設定

Cisco Secure Client パッケージをダウンロードします。

Cisco Software Download の Web ページから最新の Cisco Secure Client パッケージをダウンロードします。

OS	AnyConnect Web 展開パッケージ名
Windows	cisco-secure-client-win-バージョン-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-バージョン-webdeploy-k9.pkg
Linux（64 ビット）	cisco-secure-client-linux64-バージョン-webdeploy-k9.pkg

（注） Cisco Secure Firewall ASA で同じオペレーティングシステムの異なるバージョンを使用してはなりません。

Cisco Secure Firewall ASA での Cisco Secure Client パッケージのロード

ステップ 1 **[設定（Configuration）] > [リモートアクセス（Remote Access）] > [VPN] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnectクライアントソフトウェア（AnyConnect Client**

Software）] に移動します。Cisco Secure Client パネルには、現在 Secure Firewall ASA にロードされている Cisco Secure Client イメージが表示されます。イメージが表示される順序は、Cisco Secure Firewall ASA がリモートコンピュータにイメージをダウンロードした順序です。

ステップ 2 Cisco Secure Client のイメージを追加するには、[追加（Add）] をクリックして、次のいずれかを選択します。

- Cisco Secure Firewall ASA にアップロードした Cisco Secure Client イメージを選択するには、[フラッシュの参照（Browse Flash）] をクリックします。
- コンピュータ上にローカルに保存した Cisco Secure Client イメージを参照して選択するには、[アップロード（Upload）] をクリックします。

ステップ 3 [OK] または [アップロード（Upload）] をクリックします。

ステップ 4 [Apply] をクリックします。

追加の Cisco Secure Client モジュールの有効化

追加機能を有効にするには、グループ ポリシーまたはローカル ユーザ設定で新しいモジュール名を指定します。追加モジュールの有効化は、ダウンロード時間に影響することに注意してください。機能を有効にすると、Cisco Secure Client は VPN エンドポイントにそれらのモジュールをダウンロードする必要があります。

（注） [ログイン前の起動（Start Before Logon）] を選択した場合は、AnyConnect VPN プロファイルでもこの機能を有効にする必要があります。

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 ナビゲーションウィンドウで、**[VPNポリシー（VPN Policy）] > [AnyConnectクライアント（AnyConnect Client）]** の順に選択します。[ダウンロードするクライアント モジュール（Client Modules to Download）] で [追加（Add）] をクリックし、このグループ ポリシーに追加する各モジュールを選択します。使用可能なモジュールは、Cisco Secure Firewall ASA に追加またはアップロードしたモジュールです。

ステップ 4 [適用（Apply）] をクリックし、変更をグループ ポリシーに保存します。

ASDM でのクライアント プロファイルの作成

Cisco Secure Firewall ASA でクライアントプロファイルを作成する前に、Cisco Secure Client Web 展開パッケージを追加する必要があります。

ステップ 1 **[設定（Configuration）]** > **[リモートアクセスVPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** に移動します。

ステップ 2 グループと関連付けるクライアント プロファイルを選択し、[グループ ポリシーの変更（Change Group Policy）] をクリックします。

ステップ 3 [プロファイル ポリシー名のポリシーの変更（Change Policy for Profile policy name）] ウィンドウで、[使用可能なグループ ポリシー（Available Group Policies）] フィールドからグループ ポリシーを選択し、右矢印をクリックして [ポリシー（Policies）] フィールドに移動します。

ステップ 4 [OK] をクリックします。

ステップ 5 [Cisco Secure Client クライアントプロファイル（AnyConnect Client Profile）] ページで、[適用（Apply）] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 設定が終了したら、[OK] をクリックします。

ISE での Web 展開の設定

ISE は、ISE のポスチャをサポートするために、Cisco Secure Client コア VPN モジュール、ISE ポスチャモジュール、および OPSWAT（コンプライアンスモジュール）を設定して展開できます。また、ISE は、Cisco Secure Firewall ASA に接続する場合に使用可能なすべての Cisco Secure Client モジュールおよびリソースを展開できます。ユーザーが ISE によって制御されるリソースを参照すると次のようになります。

- ISE が Cisco Secure Firewall ASA の背後にある場合、ユーザーは ASA に接続し、Cisco Secure Client をダウンロードし、VPN 接続を確立します。Cisco Secure Client ISE ポスチャが Cisco Secure Firewall ASA によってインストールされていない場合、ISE ポスチャをインストールするために、ユーザーは Cisco Secure Client ポータルにリダイレクトされます。
- ISE が Cisco Secure Firewall ASA の背後にない場合、ユーザーは Cisco Secure Client ポータルに接続し、ISE 上の Cisco Secure Client 設定で定義された Cisco Secure Client リソースをインストールするように誘導されます。一般的な設定では、ISE ポスチャステータスが不明な場合、ブラウザが Cisco Secure Client プロビジョニングポータルにリダイレクトされます。
- ユーザーが ISE 内の Cisco Secure Client プロビジョニングポータルに誘導されると次のようになります。
  - ブラウザが Internet Explorer の場合、ISE は Cisco Secure Client ダウンローダーをダウンロードし、ダウンローダーが Cisco Secure Client をロードします。
  - 他のすべてのブラウザの場合、ISEはクライアントプロビジョニング リダイレクション ポータルを開きます。ここには、Network Setup Assistant（NSA）ツールをダウンロードするためのリンクが表示されます。ユーザーは NSA を実行します。これによ

り、ISE サーバーが検出され、Cisco Secure Client ダウンローダーがダウンロードされます。

NSA が Windows での実行を終了した場合、自動的に削除されます。macOS での実行を終了した場合は、手動で削除する必要があります。

ISE のマニュアルでは、次の方法について説明しています。

- ISE で Cisco Secure Client 設定プロファイルを作成する
- ローカルデバイスから ISE に Cisco Secure Client リソースを追加する
- リモートサイトから Cisco Secure Client プロビジョニングリソースを追加する
- Cisco Secure Client とリソースを展開する

（注） Cisco Secure Client ISE ポスチャモジュールでは、検出時に Web プロキシベースのリダイレクションはサポートされていないため、非リダイレクションベースの検出を使用することをお勧めします。詳細については、『Cisco Identity Services Engine Administrator Guide』[英語] の「Client Provisioning Without URL Redirection for Different Networks」セクションを参照してください。

ISE では、次の Cisco Secure Client リソースの設定および展開が可能です。

- Cisco Secure Client コア VPN およびその他のモジュール（ISE ポスチャモジュールを含む）
- プロファイル：Network Visibility Module、Cisco Secure Endpoint、VPN、Network Access Manager、カスタマーフィードバック、および ISE ポスチャ
- カスタマイズ用ファイル
  - UI リソース
  - バイナリ、接続スクリプト、およびヘルプ ファイル
- ローカリゼーション ファイル
  - メッセージのローカリゼーション用 Cisco Secure Client gettext 変換
  - Windows インストーラ トランスフォーム

ISE アップロードのための Cisco Secure Client ファイルの準備

- オペレーティングシステムの Cisco Secure Client パッケージ、およびローカル PC に展開する他の Cisco Secure Client リソースをダウンロードします。

（注） Cisco Secure Firewall ASA を使用すると、インストールは VPN のダウンローダーによって行われます。ダウンロードでは、ISE ポスチャプロファイルは Cisco Secure Firewall ASA によってプッシュされ、後続のプロファイルのプロビジョニングに必要なホスト検出が利用可能になってから、ISE ポスチャモジュールが ISE に接続します。その一方、ISE では、ISE ポスチャ モジュールは ISE が検出された後にのみプロファイルを取得し、これがエラーの原因になることがあります。したがって、VPN に接続するとき Cisco Secure Firewall ASA を ISE ポスチャモジュールにプッシュすることを推奨します。

- 展開するモジュールのプロファイルを作成します。最低でも、Cisco Secure Client ISE ポスチャプロファイル（ISEPostureCFG.xml）を作成します。

（注） 非リダイレクションベースのディスカバリを使用する場合、ISE ポスチャモジュールを事前展開するには、Call Home リストを持つ ISE ポスチャプロファイルが必須です。

- ISE バンドルと呼ばれる ZIP アーカイブにカスタマイズおよびローカリゼーション リソースを統合します。バンドルには次を含めることができます。
  - Cisco Secure Client の UI リソース
  - VPN 接続スクリプト
  - ヘルプ ファイル
  - インストーラ トランスフォーム

  Cisco Secure Client ローカリゼーションバンドルには、次を含めることができます。
  - バイナリ形式の Cisco Secure Client gettext 変換
  - インストーラ トランスフォーム

ISE バンドルの作成については、「ISE 展開のための AnyConnect カスタマイズおよびローカリゼーションの準備」で説明します。

Cisco Secure Client を展開するための ISE の設定

追加の Cisco Secure Client リソースをアップロードして作成する前に、Cisco Secure Client パッケージを ISE にアップロードする必要があります。

（注） ISE で Cisco Secure Client 設定オブジェクトを設定する場合、[Cisco Secure Clientモジュールの選択（Module Selection）] の下にある VPN モジュールの選択を解除しても、展開された、またはプロビジョニングされたクライアントの VPN は無効になりません。

1. ISE で、**[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（results）] > を選択します。**[クライアント プロビジョニング（Client Provisioning）] を展開して [リソース（Resources）] を表示して、[リソース（Resources）] を選択します。
2. **[追加（Add）] > [ローカルディスクからのエージェントリソース（Agent resources from local disk）]** を選択して、Cisco Secure Client パッケージファイルをアップロードします。展開を計画しているその他の Cisco Secure Client リソースについて、ローカルディスクからのエージェントリソースの追加を繰り返して行ってください。
3. **[追加（Add）] > [AnyConnect設定（AnyConnect Configuration）] > を選択します。**この Cisco Secure Client 設定は、次の表に示すように、モジュール、プロファイル、カスタマイズ/言語パッケージ、および OPSWAT パッケージを設定します。

   Cisco Secure Client ISE ポスチャプロファイルは、ISE、Cisco Secure Firewall ASA、または Windows Cisco Secure Client プロファイルエディタで作成および編集できます。次の表では、ISE の各 Cisco Secure Client リソースの名前およびリソースの種類の名前について説明します。

   表 4 : Cisco Secure Client ISE のリソース

プロンプト	ISE リソース タイプと説明
Cisco Secure Client パッケージ	CiscoSecureClientDesktopWindows CiscoSecureClientDesktopOSX CiscoSecureClientDesktopLinux CiscoTemporalAgentWindows CiscoTemporalAgentOSX
コンプライアンス モジュール	CiscoSecureClientComplianceModuleWindows CiscoSecureClientComplianceModuleOSX CiscoSecureClientComplianceModuleLinux
Cisco Secure Client プロファイル	エージェントプロファイル（Profile） ISE により、アップロードされた Cisco Secure Client パッケージで提供される各プロファイルのチェックボックスが表示されます。
カスタマイゼーション バンドル	エージェントCustomizationBundle

プロンプト	ISE リソース タイプと説明
ローカリゼーション バンドル	エージェントLocalizationBundle

4. ロールまたは OS ベースのクライアント プロビジョニング ポリシーを作成します。Cisco Secure Client および ISE レガシー NAC/MAC エージェントを、クライアント プロビジョニングのポスチャエージェントに選択できます。各 CP ポリシーは、Cisco Secure Client エージェントまたはレガシー NAC/MAC エージェントのいずれか 1 つのエージェントのみをプロビジョニングできます。Cisco Secure Client エージェントを設定する場合、ステップ 2 で作成した Cisco Secure Client 設定を 1 つ選択します。

Cisco Secure Firewall Threat Defense での Web 展開の設定

Secure Firewall Threat Defense デバイスは、Cisco Secure Firewall ASA と同様のセキュアゲートウェイ機能を提供する次世代ファイアウォール（NGFW）です。Secure Firewall Threat Defense デバイスは Cisco Secure Client を使用するリモートアクセス VPN（RA VPN）のみをサポートしており、その他のクライアントまたはクライアントレス VPN アクセスはサポートしていません。トンネルの確立と接続は、IPsec IKEv2 または SSL で行われます。Cisco Secure Firewall Threat Defense デバイスに接続する場合、IKEv1 はサポートされません。

Windows、macOS、および Linux の Cisco Secure Client は Secure Firewall Threat Defense ヘッドエンド上で設定され、接続時に展開されます。これにより、リモートユーザーは、クライアントソフトウェアのインストールおよび構成なしに、SSL または IKEv2 IPsec VPN クライアントの利点を活用できます。以前からインストールされているクライアントの場合は、ユーザーの認証時に、Secure Firewall Threat Defense ヘッドエンドによってクライアントのリビジョンが点検され、必要に応じてアップグレードされます。

以前にインストールされたクライアントがない場合、リモートユーザーは、設定されているインターフェイスの IP アドレスを入力し、Cisco Secure Client をダウンロードおよびインストールします。Secure Firewall Threat Defense ヘッドエンドは、リモートコンピュータのオペレーティングシステムに適合するクライアントをダウンロードおよびインストールして、セキュリティで保護された接続を確立します。

Apple iOS デバイスおよび Android デバイス用の Cisco Secure Client アプリは、当該プラットフォームのアプリ ストアからインストールされます。これらは、必要最小限の設定で、Secure Firewall Threat Defense ヘッドエンドへの接続を確立します。Cisco Secure Client ソフトウェアの配布には、他のヘッドエンドデバイスおよび環境と同様、この章で説明する代替的な展開方法が使用できます。

現在、Secure Firewall Threat Defense での設定およびエンドポイントへの配布が可能なのは、中核的な Cisco Secure Client VPN と、Cisco Secure Client VPN プロファイルのみです。Cisco Secure Firewall Management Center のリモートアクセス VPN ポリシーウィザードを使用すると、これらの基本的 VPN 機能を迅速かつ簡単にセットアップできます。

Cisco Secure Client と Secure Firewall Threat Defense に関する注意事項と制限事項

- サポートされている唯一の VPN クライアントは Cisco Secure Client です。それ以外のクライアントまたはネイティブ VPN はサポートされていません。クライアントレス VPN は、Cisco Secure Client の展開に使用されるだけで、エンティティ自体としてはサポートされていません。
- Cisco Secure Client を Secure Firewall Threat Defense で使用するには、バージョン 4.0 以降の Cisco Secure Client、およびバージョン 6.2.1 以降の Secure Firewall Management Center が必要です。
- Cisco Secure Firewall Management Center 自体は Cisco Secure Client プロファイルエディタをサポートしていません。VPN プロファイルを別途で設定する必要があります。VPN プロファイルおよび Cisco Secure Client VPN パッケージは Cisco Secure Firewall Management Center にファイルオブジェクトとして追加され、RA VPN 設定の一部となります。
- セキュアモビリティ、ネットワーク アクセス マネジメント、およびその他すべての Cisco Secure Client モジュールと、それらのコア VPN 機能を超えたプロファイルは、現在サポートされていません。
- VPN ロード バランシングはサポートされません。
- ブラウザ プロキシはサポートされません。
- すべてのポスチャ派生機能（Secure Firewall ポスチャ、エンドポイント ポスチャ アセスメント、および ISE）と、クライアントポスチャに基づくダイナミック アクセス ポリシーは、サポートされていません。
- Secure Firewall Threat Defense デバイスは、Cisco Secure Client のカスタマイズまたはローカライズに必要なファイルの設定または展開を行いません。
- デスクトップクライアントでの遅延アップグレードやモバイルクライアントでのアプリごとの VPN など、Cisco Secure Client上でカスタム属性を必要とする機能は、Secure Firewall Threat Defense ではサポートされません。
- Secure Firewall Threat Defense ヘッドエンドでローカルに認証を行うことはできません。したがって、設定されているユーザーは、リモート接続に使用できません。Secure Firewall Threat Defense が認証局の役割を果たすことはできません。また、次の認証機能はサポートされていません。
  - セカンダリ認証または二重認証
  - SAML 2.0 を使用するシングル サインオン
  - TACACS、Kerberos（KCD 認証）および RSA SDI
  - LDAP 認証（LDAP 属性マップ）
  - RADIUS CoA

Secure Firewall Threat Defense 上での Cisco Secure Client の設定および展開の詳細については、適切なリリース（リリース 6.2.1 以降）の『irepower Management Center Configuration Guide』[英語] の「*Firepower Threat Defense Remote Access VPN*」の章を参照してください。

Cisco Secure Client ソフトウェアおよびプロファイルの更新

Cisco Secure Client は、いくつかの方法で更新できます。

- Cisco Secure Client：Cisco Secure Client が Cisco Secure Firewall ASA に接続する場合、Cisco Secure Client ダウンローダーは新しいソフトウェアまたはプロファイルが Cisco Secure Firewall ASA にロードされたかどうかを確認します。それらの更新はクライアントにダウンロードされ、VPN トンネルが確立されます。
- ASA または FTD ポータル：Cisco Secure Firewall ASA のクライアントレスポータルに接続して更新を取得するように、ユーザーに指示します。FTD は、コア VPN モジュールのみをダウンロードします。
- ISE：ユーザーが ISE に接続すると、ISE は Cisco Secure Client 設定を使用して、更新されたコンポーネントまたは新しいポスチャ要件があるかどうかを確認します。認証時、ユーザーはネットワーク アクセス デバイス（NAD）によって ISE ポータルにリダイレクトされ、パッケージの抽出とインストールを管理するために、Cisco Secure Client のダウンローダーがクライアントにインストールされます。展開パッケージを Cisco Secure Firewall ASA ヘッドエンドにアップロードし、Cisco Secure Client のバージョンが Cisco Secure Firewall ASA と ISE の展開パッケージのバージョンと一致することを確認する必要があります。

  「ソフトウェアの自動アップデートが必要ですが、VPN トンネルが確立されている間は実行できません」という意味のメッセージが表示された場合は、設定済みの ISE ポリシーで更新が必要であることを示します。ローカルデバイスの Cisco Secure Client バージョンが ISE で設定されているバージョンよりも古い場合、VPN がアクティブな間はクライアントの更新が許可されないため、次のオプションを選択できます。

  - Cisco Secure Client の更新をアウトオブバンドで展開する
  - Cisco Secure Firewall ASA と ISE で同じバージョンの Cisco Secure Client を設定する

エンドユーザに遅延更新を許可することができ、ヘッドエンドに更新をロードしてもクライアントの更新を回避することもできます。

アップグレード例のフロー

前提条件

ここでの例の前提は次のとおりです。

- クライアントのポスチャステータスを使用してどのタイミングでクライアントを ISE の Cisco Secure Client クライアント プロビジョニング ポータルにリダイレクトするかを決定

する Dynamic Authorization Control List（DACL）を ISE に作成し、Cisco Secure Firewall ASA にプッシュしておきます。

- ISE が Cisco Secure Firewall ASA の背後にあります。

Cisco Secure Client がクライアントにインストールされている

1. ユーザーが Cisco Secure Client を起動し、ログイン情報を入力し、[接続（Connect）] をクリックします。
2. Cisco Secure Firewall ASA がクライアントとの SSL 接続を開いて認証ログイン情報を ISE に渡し、ISE がログイン情報を検証します。
3. Cisco Secure Client が Cisco Secure Client ダウンローダーを起動し、ダウンローダーがアップグレードを実行し、VPN トンネルを開始します。

ISE ポスチャが Cisco Secure Firewall ASA によってインストールされなかった場合は、次のようになります。

1. ユーザーが任意のサイトを参照し、DACL によって ISE の Cisco Secure Client プロビジョニングポータルにリダイレクトされます。
2. ブラウザで、ユーザーが Network Setup Assistant（NSA）をダウンロードして実行し、NSA が Cisco Secure Client ダウンローダーをダウンロードして起動します。
3. Cisco Secure Client ダウンローダーが ISE に設定された Cisco Secure Client アップグレード（これには、Cisco Secure Client ISE ポスチャモジュールが含まれています）を実行します。
4. クライアントの ISE ポスチャ エージェントがポスチャを起動します。

Cisco Secure Client がインストールされていない

1. ユーザーがサイトを参照して、Cisco Secure Firewall ASA ポータルへの接続を開始します。
2. ユーザが認証クレデンシャルを入力し、これが ISE に渡されて検証されます。
3. Cisco Secure Client ダウンローダーが、Internet Explorer では ActiveX コントロールによって起動され、他のブラウザでは Java アプレットによって起動されます。
4. Cisco Secure Client ダウンローダーが Cisco Secure Firewall ASA に設定されたアップグレードを実行し、VPN トンネルを開始します。ダウンロードが完了します。

ISE ポスチャが Cisco Secure Firewall ASA によってインストールされなかった場合は、次のようになります。

1. ユーザーがサイトを再度参照し、ISE の Cisco Secure Client クライアント プロビジョニング ポータルにリダイレクトされます。
2. Cisco Secure Client ダウンローダーが、既存の VPN トンネルによって ISE に設定されたアップグレード（これには、Cisco Secure Client ISE ポスチャモジュールの追加が含まれています）を実行します。
3. ISE ポスチャ エージェントがポスチャ評価を開始します。

Cisco Secure Client 自動更新の無効化

クライアントプロファイルを設定し、配布することによって、Cisco Secure Client 自動更新を無効にしたり、制限したりできます。

- VPN クライアント プロファイル：
  - 自動更新では、自動更新を無効にします。このプロファイルは、Cisco Secure Client の Web 展開インストールに含めるか、既存のクライアントインストールに追加できます。ユーザがこの設定を切り替えられるようにすることもきます。
- VPN ローカル ポリシー プロファイル：
  - ダウンローダーのバイパスにより、Cisco Secure Firewall ASA の更新されたコンテンツがクライアントにダウンロードされないようにします。
  - 更新ポリシーにより、さまざまなヘッドエンドへの接続時のソフトウェアおよびプロファイルの更新をきめ細かく制御できます。

ユーザーに WebLaunch 中に Cisco Secure Client のダウンロードを求めるプロンプトの表示

リモートユーザーに対して Web 展開の開始を求めるプロンプトを表示するように Cisco Secure Firewall ASA を設定し、ユーザーが Cisco Secure Client をダウンロードするか、クライアントレス ポータル ページを表示するかを選択できる期間を設定できます。

ユーザーに Cisco Secure Client のダウンロードを求めるプロンプトの表示は、グループポリシーまたはユーザーアカウントで設定されます。次の手順は、グループ ポリシーでこの機能を有効にする方法を示しています。

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 ナビゲーションペインで、**[詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] > [ログイン設定（Login Settings）]** を選択します。必要に応じて [継承（Inherit）] チェックボックスをオフにし、[ログイン後の設定（Post Login setting）] を選択します。

ユーザにプロンプトを表示する場合は、タイムアウト時間を指定し、その時間経過後のデフォルト動作を [デフォルトのログイン後選択（Default Post Login Selection）] 領域で選択します。

ステップ 4 [OK] をクリックし、変更をグループ ポリシーに適用して、[保存（Save）] をクリックします。

ユーザーに対するアップグレード遅延の許可

「Cisco Secure Client 自動更新の無効化」の説明に従って AutoUpdate を無効にし、ユーザーに Cisco Secure Client の更新の受け入れを強制できます。AutoUpdate はデフォルトでオンになっています。

遅延アップデートを設定して、ユーザーがクライアントのアップデートを後で行うことを許可できます。遅延アップデートが設定されている場合に、クライアントのアップデートが利用可能になると、Cisco Secure Client は更新を実行するか延期するかをユーザーに尋ねるダイアログを開きます。遅延アップグレードは、すべての Windows、Linux、および macOS でサポートされます。

Cisco Secure Firewall ASA での遅延アップデートの設定

Cisco Secure Firewall ASA では、遅延アップデートはカスタム属性を追加し、グループポリシーでその属性を参照および設定することで有効になります。遅延アップデートを使用するには、**すべての**カスタム属性を作成し、設定する必要があります。

Cisco Secure Firewall ASA 設定にカスタム属性を追加するための手順は、実行中の ASA/ASDM のリリースによって異なります。カスタム属性の設定手順については、ASA/ASDM の展開リリースに対応した『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] を参照してください。

次の属性と値により、ASDM に遅延アップデートを設定します。

カスタム属性 *	有効な値	デフォルト値	注記
DeferredUpdateAllowed	true false	false	true は遅延アップデートを有効にします。遅延アップデートが無効（false）の場合、次の設定は無視されます。
DeferredUpdateMinimumVersion	*x.x.x*	0.0.0	アップデートを遅延できるようにインストールする必要がある Cisco Secure Client の最小バージョン。 最小バージョンのチェックは、ヘッドエンドで有効になっているすべてのモジュールに適用されます。有効になっているモジュール（VPN を含む）がインストールされていないか、最小バージョンを満たしていない場合、接続は遅延アップデートの対象になりません。 この属性が指定されていない場合、エンドポイントにインストールされているバージョンに関係なく、遅延プロンプトが表示されます（または自動消去されます）。

カスタム属性 *	有効な値	デフォルト値	注記
DeferredUpdateDismissTimeout	0 ～ 300（秒）	150 秒	遅延アップデートプロンプトが表示され、自動的に消去されるまでの秒数。この属性は、遅延アップデート プロンプトが表示される場合に限り適用されます（最小バージョン属性が最初に評価されます）。 この属性がない場合、自動消去機能が無効になり、ユーザが応答するまでダイアログが表示されます（必要な場合）。 この属性を0に設定すると、次に基づいて強制的に自動遅延またはアップグレードが実施されます。 • インストールされているバージョンおよびDeferredUpdateMinimumVersionの値。 • DeferredUpdateDismissResponse の値。
DeferredUpdateDismissResponse	defer update	update	DeferredUpdateDismissTimeout が発生した場合に実行するアクション。

* カスタム属性値は大文字と小文字を区別します。

ISE での遅延アップデートの設定

ステップ 1 次のナビゲーションに従ってください。

a) **[ポリシー（Policy）]** > **[結果（Results）]** を選択します。
b) [クライアント プロビジョニング（Client Provisioning）] を展開します。
c) [リソース（Resources）] を選択し、**[追加（Add）]** > **[ローカル ディスクからのエージェント リソース（Agent Resources from Local Disk）]** をクリックします。
d) Cisco Secure Client pkg ファイルをアップロードして、[送信（Submit）] を選択します。

ステップ 2 作成したその他の Cisco Secure Client リソースもアップロードします。

ステップ 3 [リソース（Resources）] で、アップロードした Cisco Secure Client パッケージを使用して [AnyConnect設定（AnyConnect Configuration）] を追加します。[Cisco Secure Client設定（AnyConnect Configuration）] には遅延アップデートを設定するフィールドがあります。

更新ポリシーの設定

更新ポリシーの概要

Cisco Secure Client ソフトウェアおよびプロファイルの更新は、ヘッドエンドへの接続時に使用可能で、かつクライアントによって許可されている場合に発生します。ヘッドエンドに対して Cisco Secure Client 更新の設定を行うと、更新を使用できるようになります。VPN ローカル ポリシー ファイルの更新ポリシー設定によって、更新が許可されるかどうかが決まります。

更新ポリシーは、ソフトウェア ロックと呼ばれることもあります。複数のヘッドエンドが設定されている場合、更新ポリシーはマルチ ドメイン ポリシーとも呼ばれます。

デフォルトでは、更新ポリシー設定ではすべてのヘッドエンドからのソフトウェアおよびプロファイルの更新を許可します。これを制限するには、次のように更新ポリシー パラメータを設定します。

- **Server Name** リストにヘッドエンドを指定することで、特定のヘッドエンドにすべての Cisco Secure Client ソフトウェアおよびプロファイルの更新を許可（認証）します。

  ヘッドエンドのサーバ名はFQDNまたはIPアドレスで指定できます。また、*.example.com のようにワイルドカードにすることもできます。

  更新がどのように発生するかの詳細については、下記の「許可されたサーバ更新ポリシーの動作」を参照してください。

- 他のすべての無指定または認証されていないヘッドエンドの場合：
  - 任意のサーバからソフトウェア更新を許可（**Allow Software Updates From Any Server**）オプションを使用して、VPN コア モジュールおよびその他のオプション モジュールのソフトウェア更新を許可または拒否します。
  - 任意のサーバからVPNプロファイル更新を許可（**Allow VPN Profile Updates From Any Server**）オプションを使用して、VPNプロファイルの更新を許可または拒否します。
  - 任意のサーバからサービスプロファイル更新を許可（**Allow Service Profile Updates From Any Server**）オプションを使用して、その他のサービス モジュールのプロファイルの更新を許可または拒否します。
  - [任意のサーバからの ISE ポスチャ プロファイル更新を許可（Allow ISE Posture Profile Updates From Any Server）] オプションを使用して ISE ポスチャ プロファイルの更新を許可または拒否します。
  - [任意のサーバからのコンプライアンス モジュール更新を許可（Allow Compliance Module Updates From Any Server）] オプションを使用して、コンプライアンス モジュールの更新を許可または拒否します。

    更新がどのように発生するかの詳細については、下記の「不正なサーバー更新ポリシーの動作」を参照してください。

許可されたサーバ更新ポリシーの動作

Server Name リストで識別されている、許可されたヘッドエンドに接続する場合は、他の更新ポリシー パラメータは適用されず、次のようになります。

- ヘッドエンド上の Cisco Secure Client パッケージのバージョンがクライアント上のバージョンと比較され、ソフトウェアの更新が必要かどうかが判断されます。
  - Cisco Secure Client パッケージのバージョンがクライアント上のバージョンより古い場合、ソフトウェアは更新されません。

- Cisco Secure Client パッケージのバージョンがクライアント上のバージョンと同じである場合、ヘッドエンドでダウンロード対象として設定され、クライアントに存在しないソフトウェア モジュールのみがダウンロードされてインストールされます。
- Cisco Secure Client パッケージのバージョンがクライアント上のバージョンより新しい場合、ヘッドエンドでダウンロード対象として設定されたソフトウェアモジュール、およびすでにクライアントにインストールされているソフトウェアモジュールがダウンロードされてインストールされます。

- ヘッドエンド上の VPN プロファイル、ISE ポスチャ プロファイル、および各サービス プロファイルが、クライアント上の該当プロファイルと比較され、更新が必要かどうかが判断されます。
  - ヘッドエンド上のプロファイルがクライアント上のプロファイルと同じ場合は、プロファイルは更新されません。
  - ヘッドエンド上のプロファイルがクライアント上のプロファイルと異なる場合、プロファイルがダウンロードされます。

不正なサーバー更新ポリシーの動作

非正規のヘッドエンドに接続すると、次のような、**Allow ... Updates From Any Server** オプションを使用して Cisco Secure Client の更新方法が決定されます。

- **Allow Software Updates From Any Server:**
  - このオプションがオンの場合、この認証されていない Cisco Secure Firewall ASA に対してソフトウェア更新が許可されます。更新は、認証されたヘッドエンドに対する、上記のようなバージョン比較に基づきます。
  - このオプションがオフの場合、ソフトウェア更新は行われません。また、バージョン比較に基づく更新を行う必要があった場合、VPN 接続の試行は終了します。

- **Allow VPN Profile Updates From Any Server:**
  - このオプションがオンの場合、VPN プロファイルは、ヘッドエンドの VPN プロファイルがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、VPNプロファイルは更新されません。また、差異に基づくVPNプロファイル更新を行う必要があった場合、VPN接続の試行は終了します。

- **Allow Service Profile Updates From Any Server:**
  - このオプションがオンの場合、各サービスプロファイルは、ヘッドエンドのプロファイルがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、サービス プロファイルは更新されません。

- **Allow ISE Posture Profile Updates From Any Server:**

- このオプションがオンの場合、ISE ポスチャ プロファイルは、ヘッドエンドの ISE ポスチャ プロファイルがクライアントのものと異なる場合に更新されます。
- このオプションがオフの場合、ISE ポスチャ プロファイルは更新されません。ISE ポスチャ プロファイルは、ISE ポスチャ エージェントを機能させるために必要です。

- **Allow Compliance Module Updates From Any Server:**
  - このオプションがオンの場合、コンプライアンスモジュールは、ヘッドエンドのコンプライアンス モジュールがクライアントのものと異なる場合に更新されます。
  - このオプションがオフの場合、コンプライアンスモジュールは更新されません。コンプライアンス モジュールは、ISE ポスチャ エージェントを機能させるために必要です。

更新ポリシーのガイドライン

- 認証された **Server Name** リストにサーバの IP アドレスを表示することで、リモート ユーザはヘッドエンドにその対応する IP アドレスを使用して接続できます。ユーザが IP アドレスを使用して接続しようとしたときに、ヘッドエンドが FQDN でリストされている場合、この試行は、認証されていないドメインへの接続として扱われます。
- ソフトウェア更新には、カスタマイズ、ローカリゼーション、スクリプト、およびトランスフォームのダウンロードが含まれます。ソフトウェア更新が許可されていない場合、これらの項目はダウンロードされません。一部のクライアントがスクリプトの更新を許可しない場合、ポリシーの適用にスクリプトを使用しないでください。
- Always-Onを有効にした状態でVPNプロファイルをダウンロードすると、クライアントの他のすべての VPN プロファイルが削除されます。認証されていない、または社外のヘッドエンドからの VPN プロファイルの更新を許可するかどうかを決定する場合は、このことを考慮してください。
- インストールおよび更新ポリシーのためにVPNプロファイルがクライアントにダウンロードされない場合、次の機能は使用できません。

サービス無効化	信頼されていないネットワーク ポリシー
証明書ストアの上書き	信頼できる DNS ドメイン
事前接続メッセージの表示	信頼できる DNS サーバ
ローカル LAN へのアクセス	Always-On
Start Before Login	キャプティブ ポータル修復
ローカル プロキシ接続	スクリプティング
PPP 除外	ログオフ時の VPN の保持
自動 VPN ポリシー	必要なデバイス ロック

信頼されたネットワーク ポリシー	自動サーバ選択

- Windows では、ダウンローダーは、ダウンロード履歴を記録する個別のテキストログ（UpdateHistory.log）を作成します。このログは、更新時刻、クライアントを更新した Cisco Secure Firewall ASA、更新されたモジュール、インストールされているバージョン（アップグレードの前および後）を含みます。このログファイルは、次の場所に保存されます。

  `%ALLUSERESPROFILE%\Cisco\Cisco Secure Client\Logs` ディレクトリ。

- ローカルポリシーファイルの変更を反映するには、Cisco Secure Client サービスを再起動する必要があります。

更新ポリシーの例

この例では、クライアントの Cisco Secure Client バージョンがさまざまな Cisco Secure Firewall ASA ヘッドエンドと異なる場合のクライアントの更新動作を示します。

VPN ローカル ポリシー XML ファイルでの更新ポリシーが次のようになっているとします。

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>false</FipsMode>
<BypassDownloader>false</BypassDownloader><RestrictWebLaunch>false</RestrictWebLaunch>
<StrictCertificateTrust>false</StrictCertificateTrust>
<RestrictPreferenceCaching>false</RestrictPreferenceCaching>
<RestrictTunnelProtocols>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>false</AllowSoftwareUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowScriptUpdatesFromAnyServer>true</AllowScriptUpdatesFromAnyServer>
<AllowHelpUpdatesFromAnyServer>true</AllowHelpUpdatesFromAnyServer>
<AllowResourceUpdatesFromAnyServer>true</AllowResourceUpdatesFromAnyServer>
<AllowLocalizationUpdatesFromAnyServer>true</AllowLocalizationUpdatesFromAnyServer>
<AuthorizedServerList>
<ServerName>seattle.example.com</ServerName>
<ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>
```

Cisco Secure Firewall ASA ヘッドエンド設定は次のようになっています。

ASA ヘッドエンド	ロードされている **AnyConnect** パッケージ	ダウンロードするモジュール
seattle.example.com	バージョン 4.7.01076	VPN、Network Access Manager
newyork.example.com	バージョン 4.7.03052	VPN、Network Access Manager

ASA ヘッドエンド	ロードされている AnyConnect パッケージ	ダウンロードするモジュール
raleigh.example.com	バージョン 4.7.04056	VPN、ポスチャ

次の更新シーケンスは、クライアントが現在Cisco Secure Client VPN コアおよびNetwork Access Manager Module を実行している場合に実行可能です。

- クライアントは、同じバージョンのCisco Secure Clientが設定された、認証されたサーバーである seattle.example.com に接続します。VPN およびNetwork Access Manager プロファイルがダウンロード可能で、かつクライアントのものとは異なる場合、それらのプロファイルもダウンロードされます。
- 次に、クライアントは、Cisco Secure Clientの新しいバージョンが設定された、認証されたCisco Secure Firewall ASA である newyork.example.com に接続します。VPN とNetwork Access Managerのモジュールがアップグレードされます。ダウンロード可能で、かつクライアントのものとは異なるプロファイルもダウンロードされます。
- 次に、クライアントは、認証されていない Cisco Secure Firewall ASA である raleigh.example.com に接続します。必要なソフトウェアアップデートが利用可能である場合でも、ポリシーによりバージョンのアップグレードを許可しないと判断されるため、アップデートは許可されません。接続が終了します。

ローカル コンピュータ上のユーザ プリファレンス ファイルの場所

Cisco Secure Clientは、一部のプロファイル設定をユーザーコンピュータ上のユーザープリファレンス ファイルおよびグローバル プリファレンス ファイルに保存します。 Cisco Secure Clientは、ローカルファイルを使用して、クライアントGUIの[プリファレンス（Preferences）]タブでユーザー制御可能設定を行い、ユーザー、グループ、ホストなど直近の接続に関する情報を表示します。

Cisco Secure Client は、Start Before Login や起動時自動接続など、ログイン前に実行するアクションにグローバルファイルを使用します。

次の表に、Cisco Secure Client の VPN サブディレクトリにあるプリファレンスファイルのファイル名およびインストールされたパスを示します。

オペレーティングシステム	タイプ	ファイルおよびパス
Windows	ユーザー	%USERPROFILE%\AppData\Local\Cisco\ Cisco Secure Client\VPN\preferences.xml
	グローバル	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\preferences_global.xml
macOS	ユーザー	$HOME/.vpn/.anyconnect
	グローバル	/opt/cisco/secureclient/vpn/.anyconnect_global

オペレーティングシステム	タイプ	ファイルおよびパス
Linux	ユーザー	$HOME/.vpn/.anyconnect
	グローバル	/opt/cisco/secureclient/.vpn/.anyconnect_global

Cisco Secure Client で使用されるポート

次の表に、Cisco Secure Client で使用されるポートをプロトコルごとに示します。

プロトコル	Cisco Secure Client ポート
TLS（SSL）	TCP 443
SSL リダイレクション	TCP 80（任意）
DTLS	UDP 443（任意、ただし強く推奨）
IPsec/IKEv2	UDP 500、UDP 4500

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。