



AnyConnect の導入

- [展開前の作業](#) (1 ページ)
- [AnyConnect 展開の概要](#) (2 ページ)
- [AnyConnect のためのエンドポイントの準備](#) (5 ページ)
- [Linux での Network Visibility Module の使用](#) (9 ページ)
- [AnyConnect の事前展開](#) (11 ページ)
- [AnyConnect の Web 展開](#) (28 ページ)
- [AnyConnect ソフトウェアおよびプロファイルの更新](#) (37 ページ)

展開前の作業

Umbrella ローミングセキュリティ モジュールを展開している場合は、Umbrella ローミングセキュリティのすべての既存のインストールが検出され、競合を防ぐために自動的に削除されます。Umbrella ローミングセキュリティ クライアントの既存インストールを Umbrella ローミングセキュリティ サービスサブスクリプションに関連付けている場合は、OrgInfo.json ファイルを AnyConnect インストーラと同じ場所に配置して Umbrella ローミングセキュリティ モジュールのディレクトリで Web 展開または事前展開を設定していない限り、Umbrella ローミングセキュリティ モジュールに自動的に移行されます。Umbrella ローミングセキュリティ モジュールを展開する前に、手動で Umbrella ローミングセキュリティ クライアントをアンインストールすることができます。

Umbrella ローミングセキュリティ モジュールを使用している場合は、次の前提条件も満たす必要があります。

- **Umbrella ローミング アカウントを取得する。** Umbrella ダッシュボード (<http://dashboard.umbrella.com>) は、Umbrella ローミングセキュリティ モジュールの操作に必要な情報を取得するログインページです。ローミング クライアント アクティビティのレポートを制御するためにもこのサイトを使用します。
- **ダッシュボードから OrgInfo ファイルをダウンロードする。** Umbrella ローミングセキュリティ モジュールの導入準備を行うには、Umbrella ダッシュボードから OrgInfo.json ファイルを取得します。[ID (Identities)] メニュー ストラクチャで [ローミング コンピュータ (Roaming Computers)] をクリックし、続いて、ページ左上隅の [+] 記号をクリックしま

す。Umbrella ローミングセキュリティ モジュールまでスクロールし、[モジュールプロフィール (Module Profile)] をクリックします。

OrgInfo.json ファイルには、Umbrella ローミングセキュリティ モジュールにレポートの送信先と適用するポリシーを知らせる、Umbrella サービスサブスクリプションについての詳細が含まれています。

AnyConnect 展開の概要

AnyConnect の展開は、AnyConnect 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。

AnyConnect Secure Mobility 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。
- Web 展開：AnyConnect パッケージは、ヘッドエンド (Firepower 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、AnyConnect がクライアントに展開されます。
 - 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 AnyConnect 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、AnyConnect がすでにインストールされているシステムで AnyConnect 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。
- クラウド更新：Umbrella ローミングセキュリティ モジュールの展開後に、上記およびクラウド更新のいずれかの方法を使用して AnyConnect モジュールを更新できます。クラウド更新では、ソフトウェアアップグレードは Umbrella クラウド インフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。デフォルトでは、クラウド更新からの自動更新は無効です。



- (注) クラウド更新に関して以下を検討してください。
- 現在インストールされているソフトウェアモジュールのみが更新されます。
 - カスタマイズ、ローカリゼーション、およびその他の展開タイプはサポートされません。
 - 更新は、デスクトップにログインしたときのみ実行され、VPN が確立されているときは実行されません。
 - 更新を無効にすると、最新のソフトウェア機能と更新を利用できません。
 - クラウド更新を無効にしても、他の更新メカニズムや設定（Web 展開、遅延更新など）には影響しません。
 - クラウド更新は、AnyConnect のより新しいバージョンや未公開バージョン（暫定リリース、修繕公開されたバージョンなど）があっても無視します。

AnyConnect を展開する場合に、追加機能を含めるオプションのモジュール、および VPN やオプション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、[AnyConnect 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。AnyConnect 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。

AnyConnect のインストール方法の決定

AnyConnect 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。AnyConnect 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

AnyConnect をアップグレードする、または（Secure Firewall ASA/ISE/Firepower Threat Defense 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 Firepower 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 AnyConnect クライアントレスポータルに接続して、AnyConnect のダウンロードを選択します。Cisco Secure Firewall ASA は AnyConnect ダウンローダーをダウンロードします。AnyConnect 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。AnyConnect 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

AnyConnect 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。
- AnyConnect 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、『[AnyConnect Secure Mobility Client Features, License, and OS Guide](#)』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 VPN ポスチャを使用している場合は、VPN ポスチャを事前展開することを推奨します。
-

AnyConnect のインストールに必要なリソースの決定

AnyConnect 展開は、複数の種類のファイルで構成されています。

- AnyConnect パッケージに含まれている AnyConnect。
- 追加機能をサポートするモジュール。AnyConnect パッケージに含まれています。
- AnyConnect 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)。

AnyConnect のためのエンドポイントの準備

AnyConnect 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、AnyConnect 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、AnyConnect 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。AnyConnect 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、AnyConnect 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)、AnyConnect は古い切断を解除する前に新しい接続を確立します。

Windows での Internet Explorer 信頼済みサイトのリストへの ASA の追加

Active Directory 管理者が Internet Explorer の信頼済みサイトのリストに ASA を追加するには、グループ ポリシーを使用できます。この手順は、ローカルユーザーが Internet Explorer の信頼済みサイトに追加する方法とは異なります。

手順

- ステップ 1** Windows ドメイン サーバで、ドメイン管理者グループのメンバーとしてログインします。
- ステップ 2** [Active Directory ユーザーとコンピュータ (Active Directory Users and Computers)] MMC スナップインを開きます。
- ステップ 3** グループ ポリシー オブジェクトを作成するドメインまたは組織ユニットを右クリックして、[プロパティ (Properties)] をクリックします。
- ステップ 4** [グループ ポリシー (Group Policy)] タブを選択して、[新規 (New)] をクリックします。
- ステップ 5** 新しいグループ ポリシー オブジェクトの名前を入力して、Enter を押します。
- ステップ 6** 一部のユーザーまたはグループにこの新しいポリシーが適用されないようにするには、[プロパティ (Properties)] をクリックします。[セキュリティ (Security)] タブを選択します。この

ポリシーを適用しないユーザーまたはグループを追加し、[許可 (Allow)] カラムの [読み取り (Read)] チェックボックスと [グループポリシーの適用 (Apply Group Policy)] チェックボックスをオフにします。[OK] をクリック

- ステップ 7** [編集 (Edit)] をクリックし、[ユーザーの構成 (User Configuration)] > [Windows の設定 (Windows Settings)] > [Internet Explorer メンテナンス (Internet Explorer Maintenance)] > [セキュリティ (Security)] > > > を選択します。
- ステップ 8** 右側のペインで [セキュリティ ゾーンおよびコンテンツの規則 (Security Zones and Content Ratings)] を右クリックし、[プロパティ (Properties)] をクリックします。
- ステップ 9** [現行のセキュリティ ゾーンとプライバシーの設定をインポートする (Import the current security zones and privacy settings)] を選択します。プロンプトが表示されたら、[続行 (Continue)] をクリックします。
- ステップ 10** [設定の変更 (Modify Settings)] をクリックし、[信頼されたサイト (Trusted Sites)] を選択して、[サイト (Sites)] をクリックします。
- ステップ 11** 信頼済みサイトのリストに追加するセキュリティ アプライアンスの URL を入力し、[追加 (Add)] をクリックします。形式は、ホスト名 (<https://vpn.mycompany.com>) または IP アドレス (<https://192.168.1.100>) を含めることができます。完全一致 (<https://vpn.mycompany.com>) またはワイルドカード (https://*.mycompany.com) でも構いません。
- ステップ 12** [閉じる (Close)] をクリックし、すべてのダイアログボックスが閉じるまで [OK] をクリックします。
- ステップ 13** ドメインまたはフォレスト全体にポリシーが伝搬されるまで待ちます。
- ステップ 14** [インターネット オプション (Internet Options)] ウィンドウで [OK] をクリックします。

Internet Explorer でのプロキシ変更のブロック

ある条件下では、AnyConnect 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、AnyConnect 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。

手順

- 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、AnyConnect 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、AnyConnect 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。

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

AnyConnect 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、AnyConnect Secure Mobility 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がログインしている場合でも、ローカルユーザが 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 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。

その他の VPN セッションの接続オプションについては、「[AnyConnect VPN接続オプション](#)」を参照してください。

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

AnyConnect 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、AnyConnect Secure Mobility 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せん。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。

その他の VPN セッションの接続オプションについては、「[AnyConnect VPN接続オプション](#)」を参照してください。

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、AnyConnect 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。AnyConnect 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。

AnyConnect 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 AnyConnect Linux カーネルモジュールとのパッケージ化

始める前に

「[AnyConnect カーネルモジュールを構築するための前提条件 \(10 ページ\)](#)」に記載されている前提条件を満たす必要があります。

AnyConnect Network Visibility Module は、構築済みの AnyConnect 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と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 AnyConnect 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。

手順

ステップ 1 AnyConnect 事前展開パッケージ、`anyconnect-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

スクリプトを実行すると、構築済みの AnyConnect Linux カーネルモジュールを含む anyconnect-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。

次のタスク

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 AnyConnect Network Visibility Module を再展開する必要があります。

AnyConnect の事前展開

AnyConnect 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、AnyConnect 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。

AnyConnect 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、「[AnyConnect プロファイル事前展開場所 \(13 ページ\)](#)」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

- 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 AnyConnect 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 AnyConnect 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、「[AnyConnect 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。

手順

ステップ 1 AnyConnect 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 AnyConnect ファイルは cisco.com で入手できます。

OS	AnyConnect 事前展開パッケージ名
Windows	anyconnect-win-version-predeploy-k9.zip

OS	AnyConnect 事前展開パッケージ名
macOS	anyconnect-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) anyconnect-linux64-version-predeploy-k9.tar.gz

Umbrella ローミングセキュリティ 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。

AnyConnect 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
- AMP
- 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

AnyConnect 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
- VPN 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

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 上のスタンドアロン 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、「[AnyConnect とインストーラー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、「[AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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 Umbrella ローミングセキュリティモジュール、Network Access Manager、AMP イネーブラ、ISE ポスチャ、Web セキュリティ、および Network Visibility 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
Network Access Manager	anyconnect-win-version-nam-webdeploy-k9.msi	anyconnect-win-version-nam-predeploy-k9.msi
ISE ポスチャ	anyconnect-win-version-iseposture-webdeploy-k9.msi	anyconnect-win-version-iseposture-predeploy-k9.msi
AMP	anyconnect-win-version-amp-webdeploy-k9.msi	anyconnect-win-version-amp-predeploy-k9.exe
ネットワーク可視性モジュール	anyconnect-win-version-nvm-webdeploy-k9.exe	anyconnect-win-version-nvm-predeploy-k9.msi
Umbrella ローミングセキュリティモジュール	anyconnect-win-version-umbrella-webdeploy-k9.exe	anyconnect-win-version-umbrella-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。WLAN Autoconfig 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。

AnyConnect 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: AnyConnect コア ファイル

ファイル	説明
anyfilename.xml	AnyConnect 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。

ファイル	説明
AnyConnectProfile.xsd	XML スキーマ形式を定義します。AnyConnect 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 AnyConnect Secure Mobility Client\Profile
Network Access Manager	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Network AccessManager\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 AnyConnect Secure Mobility Client\CustomerExperienceFeedback
ISE ポスチャ	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
AMP イネーブラ	Cisco Advanced Malware Protection イネーブラーは、リリース 5.0 での SecureX の導入に伴い、Windows オペレーティングシステムでは削除されましたが、macOS では引き続き使用できます。 %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler
ネットワーク可視性モジュール	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NVM
Umbrella ローミング セキュリティ モジュール	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility 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	
バイナリ	/opt/cisco/anyconnect/bin

モジュール	参照先
ライブラリ	/opt/cisco/anyconnect/lib
UI リソース	/Applications/Cisco/Cisco Secure Mobility Client.app/Contents/Resources/
ISE ポスチャ	/opt/cisco/anyconnect/ise posture/
AMP イネーブラ	/opt/cisco/anyconnect/ampenabler/
ネットワーク可視性モジュール	/opt/cisco/anyconnect/NVM/
Umbrella ローミングセキュリティモジュール	/opt/cisco/anyconnect/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/anyconnect/profile
Linux	
NVM	/opt/cisco/anyconnect/NVM
AnyConnect VPN プロファイル	/opt/cisco/anyconnect/profile

その他の AnyConnect ファイルの場所

プロファイルの更新

- **Windows**
 - %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
- **macOS および Linux**
 - /opt/cisco/anyconnect/profile

Windows のカスタマイズとローカリゼーション

- L10N

- %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\l10n

- リソース

- %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

macOS および Linux のカスタマイズとローカリゼーション

- **L10N**

- /opt/cisco/anyconnect/l10n

- リソース

- /opt/cisco/anyconnect/resources

ヘルプ

- **Windows**

- %ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Help

- **macOS および Linux**

- /opt/cisco/anyconnect/help

OPSWAT ライブラリ

ISE ポスチャと HostScan で使用

- **Windows**

- %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\OPSWAT

- **macOS**

- /opt/cisco/anyconnect/lib/opswat

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

AnyConnect エンドポイントは、AnyConnect 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、AnyConnect を使用する前に次のアクションを実行します。

1. **C:\Program Files\Cisco\Cisco AnyConnect Secure Mobility Client** 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 AnyConnect モジュールの事前展開

Network Access Manager、Web セキュリティ、および Umbrella ローミングセキュリティモジュールは、スタンドアロンアプリケーションとして実行できます。コア AnyConnect クライアントがインストールされていますが、VPN および AnyConnect 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

手順

- 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 anyconnect-win-version-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 anyconnect-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。

```
msiexec /package anyconnect-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 AnyConnect 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 AnyConnect モジュールの展開

AnyConnect Network Access Manager Module または Umbrella ローミングセキュリティ モジュールは、スタンドアロンアプリケーションとしてユーザコンピュータに展開できます。これらのアプリケーションでは、DART がサポートされます。

その利点と展開方法の詳細については、「[スタンドアロン NVM](#)」を参照してください。

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 AnyConnect 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。

手順

- ステップ 1** ユーザーに AnyConnect Network Access Manager Module または Umbrella ローミングセキュリティ モジュールを確認するように指示します。
- 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 または Umbrella ローミングセキュリティ 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 AnyConnect 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 または Umbrella ローミングセキュリティ モジュール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、AnyConnect 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 または Umbrella ローミングセキュリティ インストーラを起動します。
- e) 指定に応じて、Network Access Manager Module または Umbrella ローミングセキュリティ モジュールが、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 AnyConnect 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ト メニュー プログラム、AnyConnect 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 AnyConnect 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。

AnyConnect zip ファイルの内容

ファイル	目的
GUI.ico	AnyConnect 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。
anyconnect-win-version-dart-predeploy-k9.msi	DART モジュール用 MSI インストーラ ファイル。
anyconnect-win-version-gina-predeploy-k9.msi	SBL モジュール用 MSI インストーラ ファイル。
anyconnect-win-version-ise posture-predeploy-k9.msi	ISE ポスチャ モジュール用 MSI インストーラ。

ファイル	目的
anyconnect-win-version-amp-predeploy-k9.exe	AMP イネーブラ用 MSI インストーラ ファイル。
anyconnect-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。
anyconnect-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。
anyconnect-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。
anyconnect-win-version-posture-predeploy-k9.msi	ポストチャ モジュール用 MSI インストーラ ファイル。
anyconnect-win-version-core-vpn-predeploy-k9.msi	AnyConnect VPN 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 AnyConnect 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

- AnyConnect 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、AnyConnect 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
VPN なしの AnyConnect コア クライアント機能。 スタンドアロンの Network Access Manager Module をインストールするときに使用します。	msiexec /package anyconnect-win-version-core-vpn-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-version-core-vpn-predeploy-k9-install-datetimestamp.log
VPN ありの AnyConnect コア クライアント機能。	msiexec /package anyconnect-win-version-core-vpn-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-version-core-vpn-predeploy-k9-install-datetimestamp.log
カスタマー エクスペリエンスのフィードバック	msiexec /package anyconnect-win-version-core-vpn-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-version-core-vpn-predeploy-k9-install-datetimestamp.log
Diagnostic and Reporting Tool (DART)	msiexec /package anyconnect-win-version-dart-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-version-dart-predeploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-win-version-gina-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-version-gina-predeploy-k9-install-datetimestamp.log
Network Access Manager	msiexec /package anyconnect-win-version-nam-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-version-nam-predeploy-k9-install-datetimestamp.log
VPN ポスチャ	msiexec /package anyconnect-win-version-posture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-version-posture-predeploy-k9-install-datetimestamp.log
ISE ポスチャ	msiexec /package anyconnect-win-version-iseposture-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-version-iseposture-predeploy-k9-install-datetimestamp.log
AMP イネーブラ	msiexec /package anyconnect-win-version-amp-predeploy-k9.msi / norestart/passive /lvx*

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
ネットワーク可視性モジュール	msiexec /package anyconnect-win-version-nvm-predeploy-k9.msi /norestart/passive /lvx* anyconnect-win-version-nvm-predeploy-k9-install-datetimestamp.log
Umbrella ローミングセキュリティ	msiexec /package anyconnect-win-version-umbrella-predeploy-k9.msi /norestart/passive /lvx* anyconnect-version-umbrella-predeploy-k9-install-datetimestamp.log

AnyConnect 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

AnyConnect Secure Mobility Client をホストするデバイスでは、エンドユーザーに限定的なアクセス権を与えることを推奨します。エンドユーザー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。また、ユーザーが AnyConnect をアンインストールできないように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

(anyconnect-vpn-transforms-X.X.xxxxx.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 AnyConnect 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 AnyConnect モジュールを非表示にできます。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 (anyconnect-vpn-transforms-X.X.xxxxx.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 AnyConnect 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。

手順

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

- a) AnyConnect 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、AnyConnect 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) AnyConnect 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、AnyConnect 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、AMP イネーブラ、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 AnyConnect 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、AMP イネーブラ、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) AnyConnect 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。



(注) 設計上、一部の XML ファイルは AnyConnect 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 AnyConnect のインストールおよびアンインストール

macOS 向け AnyConnect は、すべての AnyConnect モジュールを含む DMG ファイルで配布されます。ユーザが DMG ファイルを開き、AnyConnect.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。

AnyConnect 4.9.04xxx が、macOS 11 で必要な最小バージョンです。macOS 11 に関連する AnyConnect の変更の詳細については、[付録 : macOS 11 \(およびそれ以降のバージョン\) に関する AnyConnect の変更点を参照してください](#)。

いずれかの AnyConnect モジュールを配布から除外するには、Apple pkgutil ツールを使用し、変更後にパッケージに署名します。言語と外観をカスタマイズできます。その他のインストールアクションも修正できます。これについては、「[ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ](#)」のカスタマイズの章で説明されています。

macOS への AnyConnect モジュールのスタンドアロンアプリケーションとしてのインストール

VPN なしで、Network Visibility Module または Umbrella ローミングセキュリティ モジュールのみをインストールできます。VPN および AnyConnect UI は使用されません。

次の手順では、スタンドアロンプロファイルエディタをインストールして、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ことによって、モジュールをカスタマイズする方法について説明します。また、ブート時に自動的に起動するように AnyConnect 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 AnyConnect が提供できるようにします。

手順

- ステップ 1** Cisco.com から AnyConnect Secure Mobility Client DMG ファイルをダウンロードします。
- ステップ 2** 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 3** 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 4** 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または完全インストールの一部として、必要な AnyConnect モジュールを選択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 5** プロファイルエディタを起動して、プロファイルを作成します。

ステップ 6 セキュアな場所に、OrgInfo.json（ダッシュボードから取得します）としてプロファイルを適切に保存します。

- 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（AnyConnect x.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、NVM インスタンスに対して以下のような端末アプリケーションを使用します。

```
cp <path to the wso> \Volumes\ "AnyConnect <VERSION>"\Profiles\nvm\
```

- b) macOS インストーラで、AnyConnect x.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、AnyConnect DMG パッケージをユーザーに配布する準備ができました。

ステップ 7 セキュアな場所に、NVM_ServiceProfile.xml または OrgInfo.json（ダッシュボードから取得します）としてプロファイルを適切に保存します。

これらのモジュールについて、プロファイルエディタが NVM 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、NVM 用のファイル（NVM_ServiceProfile.xml など）を保存したのと同じ場所に保存します。難解化を完了するには、以下のステップに従います。

- a) 指定した .wso ファイルを Windows デバイスから NVM 用の適切なフォルダパス（AnyConnect x.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、NVM インスタンスに対して以下のような端末アプリケーションを使用します。

```
cp <path to the wso> \Volumes\ "AnyConnect <VERSION>"\Profiles\nvm\
```

- b) macOS インストーラで、AnyConnect x.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、AnyConnect 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。

最新バージョンの AnyConnect は、Apple 証明書を使用した署名付きアプリケーションです。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 AnyConnect をインストールして実行するには、[あらゆる場所 (Anywhere)] 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、<http://www.apple.com/macosx/mountain-lion/security.html> 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。

手順

-
- ステップ 1** AnyConnect 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、AnyConnect コア VPN モジュールインストールに関する、有用な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。
-

Linux 用モジュールのアンインストール

ユーザーが AnyConnect 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。

手順

-
- 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** AnyConnect 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

手順

ステップ1 AnyConnect 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/anyconnect/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

AnyConnect でサーバ証明書を使用する場合は、AnyConnect が証明書にアクセスして信頼済みとして検証できるように、証明書ストアを使用可能にする必要があります。デフォルトでは、AnyConnect は Firefox 証明書ストアを使用します。

Firefox 証明書ストアをアクティブにする方法

AnyConnect を Linux デバイスにインストールした後、AnyConnect 接続を初めて試行する前に、Firefox ブラウザを開始します。Firefox を開くと、プロファイルが作成され、そこに証明書ストアが含まれます。

Firefox 証明書ストアを使用しない場合

Firefox を使用しない場合、Firefox 証明書ストアを除外するローカル ポリシーを設定し、PEM ストアを設定する必要があります。

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。ロックダウンについては、「[Windows 事前展開 MSI の例 \(21 ページ\)](#)」で説明しています。

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 AMP 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. anyconnect-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/anyconnect/dart/dart_uninstall.sh` しか使用できません。

AnyConnect の Web 展開

Web 展開とは、クライアントシステム上の AnyConnect ダウンローダーがヘッドエンドから AnyConnect 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 AnyConnect 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、AnyConnect 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、AnyConnect 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 AnyConnect 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 AnyConnect 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 VPN 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、HostScan 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 AnyConnect 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。AnyConnect 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。
- Internet Explorer の信頼済みサイトのリストに Web 起動をサポートするセキュリティ アプライアンスの URL を追加する必要があります。これは、「[Windows での Internet Explorer 信頼済みサイトのリストへの ASA の追加](#)」の説明に従って、グループ ポリシーを使用して行うことができます。
- 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、AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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

AnyConnect 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 AnyConnect Secure Mobility 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	anyconnect-win-version-webdeploy-k9.pkg
macOS	anyconnect-macos-version-webdeploy-k9.pkg
Linux (64 ビット)	anyconnect-linux64-version-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 AnyConnect パッケージのロード

手順

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。AnyConnect パネルには、現在 Secure Firewall ASA にロードされている AnyConnect 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 AnyConnect イメージを追加するには、[追加 (Add)] をクリックします。

- Cisco Secure Firewall ASA にアップロードした AnyConnect 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 AnyConnect 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 [適用 (Apply)] をクリックします。

追加の AnyConnect 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、AnyConnect 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 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。

手順

- 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、AnyConnect Web 展開パッケージを追加する必要があります。

手順

- 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 [AnyConnect 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、AnyConnect 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 AnyConnect 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、AnyConnect をダウンロードし、VPN 接続を確立します。AnyConnect 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 AnyConnect 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 AnyConnect ポータルに接続し、ISE 上の AnyConnect 設定で定義された AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect ダウンローダーをダウンロードし、ダウンローダーが AnyConnect 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。ここでは、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、AnyConnect 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 AnyConnect 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 AnyConnect リソースを追加する
- リモートサイトから AnyConnect プロビジョニングリソースを追加する
- AnyConnect とリソースを展開する



- (注) AnyConnect 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』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 AnyConnect リソースの設定および展開が可能です。

- AnyConnect 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、AMP、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 AnyConnect 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 AnyConnect ファイルの準備

- オペレーティングシステムの AnyConnect パッケージ、およびローカル PC に展開する他の AnyConnect 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 のダウンロードャ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、AnyConnect 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ク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。
 - AnyConnect 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

AnyConnect 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 AnyConnect 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。

AnyConnect を展開するための ISE の設定

追加の AnyConnect リソースをアップロードして作成する前に、AnyConnect 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 AnyConnect 設定オブジェクトを設定する場合、[AnyConnect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、AnyConnect 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 AnyConnect 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 AnyConnect 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。

AnyConnect ISE ポスチャプロファイルは、ISE、Cisco Secure Firewall ASA、または Windows AnyConnect 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 AnyConnect 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: AnyConnect ISE のリソース

プロンプト	ISE リソース タイプと説明
AnyConnect パッケージ	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
コンプライアンス モジュール	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect プロファイル	AnyConnectプロファイル (Profile) ISE により、アップロードされた AnyConnect 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	AnyConnectCustomizationBundle
ローカリゼーションバンドル	AnyConnectLocalizationBundle

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。AnyConnect 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、AnyConnect 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。AnyConnect エージェントを設定する場合、ステップ 2 で作成した AnyConnect 設定を 1 つ選択します。

FTD での Web 展開の設定

Firepower 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。Firepower Threat Defense デバイスは AnyConnect Secure Mobility 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。FTD デバイスに接続するときには、IKEv1 はサポートされません。

Windows、macOS、および Linux の AnyConnect は Firepower 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、

Firepower 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、AnyConnect をダウンロードおよびインストールします。Firepower 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 AnyConnect 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、Firepower Threat Defense ヘッドエンドへの接続を確立します。AnyConnect 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、Firepower 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 AnyConnect VPN と、AnyConnect 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。

AnyConnect と Firepower 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 AnyConnect Secure Mobility 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、AnyConnect 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。
- AnyConnect を Firepower Threat Defense で使用するには、バージョン 4.0 以降の AnyConnect、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 AnyConnect 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 AnyConnect 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 AnyConnect モジュールと、それらのコア VPN 機能を越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。
- すべてのポストチャ派生機能（HostScan、エンドポイント ポストチャ アセスメント、および ISE）と、クライアントポスト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。
- Firepower Threat Defense デバイスは、AnyConnect 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、AnyConnect 上でカスタム属性を必要とする機能は、Firepower Threat Defense ではサポートされません。
- Firepower 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。Firepower 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

Firepower Threat Defense 上での AnyConnect 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『[Firepower Management Center コンフィギュレーションガイド](#)』の「[Firepower Threat Defense リモートアクセス VPN](#)」の章を参照してください。

AnyConnect ソフトウェアおよびプロファイルの更新

AnyConnect は、いくつかの方法で更新できます。

- **AnyConnect** : AnyConnect が Cisco Secure Firewall ASA に接続する場合、AnyConnect 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。
- **クラウド更新** : Umbrella ローミングセキュリティ モジュールは、Umbrella クラウドインフラストラクチャから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できます。クラウド更新では、ソフトウェア アップグレードは Umbrella クラウドインフラストラクチャから自動的に得られます。更新トラックは管理者のアクションではなくこれによって決まります。デフォルトでは、クラウド更新からの自動更新は無効です。
- **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 AnyConnect 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、AnyConnect 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、AnyConnect 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 AnyConnect 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。

- AnyConnect 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 AnyConnect 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 AnyConnect 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。

AnyConnect 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 AnyConnect 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. AnyConnect が AnyConnect 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 AnyConnect 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 AnyConnect ダウンローダーをダウンロードして起動します。
3. AnyConnect ダウンローダーが ISE に設定された AnyConnect アップグレード (これには、AnyConnect 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。

AnyConnect 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. ユーザー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. AnyConnect 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. AnyConnect 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。ダウンローダーが完了します。

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 AnyConnect 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. Internet Explorer では、ActiveX コントロールがダウンローダーを起動します。その他のブラウザの場合、ユーザーが Network Setup Assistant をダウンロードして実行し、これがダウンローダーをダウンロードして起動します。
3. AnyConnect 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、AnyConnect 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。
4. ISE ポスチャ エージェントがポスチャ評価を開始します。

AnyConnect 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、AnyConnect 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、AnyConnect 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。ユーザーがこの設定を切り替えられるようにすることもできます。
- 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 AnyConnect 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 AnyConnect 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 AnyConnect 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。

手順

- 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

「AnyConnect 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 AnyConnect 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、AnyConnect 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](#)』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	<p>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 AnyConnect の最小バージョン。</p> <p>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。</p> <p>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)。</p>

カスタム属性 *	有効な値	デフォルト値	注記
DeferredUpdateDismissTimeout	0 ~ 300 (秒)	150 秒	<p>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）。</p> <p>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）。</p> <p>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。</p> <ul style="list-style-type: none"> インストールされているバージョンおよび <code>DeferredUpdateMinimumVersion</code> の値。 <code>DeferredUpdateDismissResponse</code> 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

手順

ステップ 1 次のナビゲーションに従ってください。

- [ポリシー (Policy)] > [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)] を展開します。
- [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。
- AnyConnect 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 AnyConnect 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 AnyConnect パッケージを使用して [AnyConnect 設定 (AnyConnect Configuration)] を追加します。[AnyConnect 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。

遅延アップデートの GUI

次の図は、更新が可能で、遅延アップデートが設定されている場合に表示される UI を示します。図の右側は [DeferredUpdateDismissTimeout] が設定されている場合の UI を示しています。

更新ポリシーの設定

更新ポリシーの概要

AnyConnect 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 AnyConnect 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 AnyConnect 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 AnyConnect 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判断されます。
 - AnyConnect 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。
 - AnyConnect 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。
 - AnyConnect 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 AnyConnect 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 AnyConnect Secure Mobility 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、AnyConnect 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 AnyConnect 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>
<AllowVPNProfileUpdatesFromAnyServer>false</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>false</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>true</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>true</AllowComplianceModuleUpdatesFromAnyServer>
<AllowManagementVPNProfileUpdatesFromAnyServer>true</AllowManagementVPNProfileUpdatesFromAnyServer>
<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
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 AnyConnect 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 AnyConnect 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、AnyConnect 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

AnyConnect 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。AnyConnect 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。

AnyConnect 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、クライアント コンピュータ上のユーザー 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	C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
	グローバル	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml
macOS	ユーザー	/Users/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global
Linux	ユーザー	/home/username/.anyconnect
	グローバル	/opt/cisco/anyconnect/.anyconnect_global

AnyConnect で使用されるポート

次の表に、AnyConnect Secure Mobility 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	AnyConnect 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