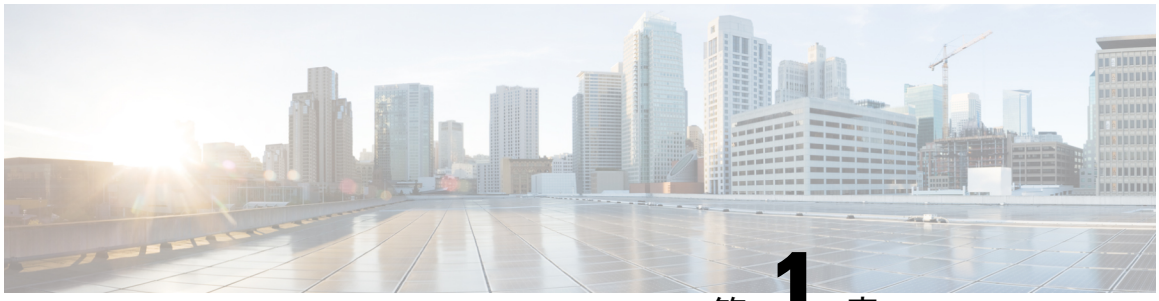
Cisco AnyConnect Secure Mobility Client リリース 4.9 管理者ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

AnyConnect の導入

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、[モジュールプロファイル（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にのみ実行され、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。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。

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。

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 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

- 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 とインストーラのカスタマイズとローカライズ （49 ページ）」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。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。

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/iseposture/
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。

```
misexec /package annyconnect-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 （275 ページ）」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タ 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*-iseposture-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。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 （379 ページ）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 （57 ページ）」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 [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、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、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。
  - 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（HostScan、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。
- 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 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 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	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。 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

手順

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) 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 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が判断されます。
  - 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 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>
<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。

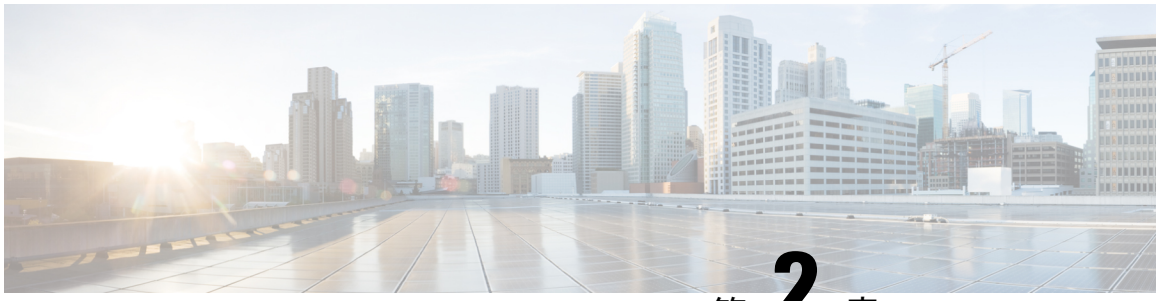
次の表に、クライアント コンピュータ上のユーザー プリファレンス ファイルのファイル名およびインストールされたパスを示します。

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



第 2 章

AnyConnect とインストーラのカスタマイズとローカライズ

AnyConnect のインストール動作の変更

ガイドライン

- Web 展開では、クライアントレス SSL ポータルの一部である AnyConnect Web 起動を使用します。クライアントレス SSL ポータルはカスタマイズできますが、このポータルの AnyConnect 部分はカスタマイズできません。たとえば、[AnyConnect の起動（Start AnyConnect）] ボタンはカスタマイズできません。

カスタマー エクスペリエンス フィードバックの無効化

カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。このモジュールは、カスタマーがどの機能およびモジュールを有効にし、使用しているかという匿名の情報をシスコに提供します。この情報によりユーザエクスペリエンスを把握できるため、シスコは品質、信頼性、パフォーマンス、ユーザエクスペリエンスを継続して改善できます。

カスタマー エクスペリエンス フィードバック モジュールを手動で無効にするには、スタンドアロン プロファイル エディタを使用して CustomerExperience_Feedback.xml ファイルを作成します。AnyConnect サービスを停止し、ファイルの名前を CustomerExperience_Feedback.xml にし、C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback\ ディレクトリにそのファイルを配置する必要があります。ファイルが無効フラグを設定して作成されると、AnyConnect に手動で展開できます。結果を確認するには、[AnyConnectについて（AnyConnect About）] メニューを開き、カスタマーエクスペリエンス フィードバック モジュールが [インストール済みモジュール（Installed Module）] セクションにリストされていないことを確認します。

カスタマー エクスペリエンス フィードバックは、次を使用して無効にできます。

- カスタマー エクスペリエンス フィードバック モジュールのクライアント プロファイル：[カスタマーエクスペリエンス フィードバック サービスの有効化（Enable Customer Experience Feedback Service）] をオフにして、プロファイルを配布します。
- MST ファイル：anyconnect-vpn-transforms-X.X.xxxxx.zip から、anyconnect-win-disable-customer-experience-feedback.mst を抽出します。

インストール動作の変更、Windows

AnyConnect のインストール動作を変更するには、以下の Windows インストーラのプロパティを使用します。ISO イメージでは、インストーラプログラム setup.hta は HTML であり、編集可能です。

- コマンド ライン パラメータ：1 つ以上のプロパティが、コマンド ライン インストーラ msiexec のパラメータとして渡されます。この方法は、事前展開に使用します。Web 展開ではサポートされません。
- インストーラ トランスフォーム：トランスフォームを使用して、インストーラのプロパティテーブルを変更できます。トランスフォームの作成には、いくつかのツールを使用できます。一般的なツールの 1 つが Microsoft Orca です。Orca ツールは、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。Windows SDK を入手するには、http://msdn.microsoft.com を参照し、使用している Windows のバージョンに対応する SDK を探します。

  トランスフォームは、事前展開のみに使用できます。（ダウンローダがインストーラを呼び出したときに、シスコによって署名されたトランスフォームのみが Web 展開を実行します。）アウトオブバンドの方法で、自分のトランスフォームを適用できますが、詳細は、このガイドの範囲外です。

制限事項

AnyConnect アンインストールプロンプトはカスタマイズできません。

クライアント インストールをカスタマイズする Windows インストーラ プロパティ

次の Windows インストーラプロパティで、AnyConnect インストールをカスタマイズします。他にも Microsoft によってサポートされる数多くの Windows インストーラ プロパティがあることに留意してください。

- システム MTU のリセット：VPN インストーラ プロパティ（RESET_ADAPTER_MTU）が 1 に設定されている場合、すべての Windows ネットワーク アダプタの MTU 設定がデフォルト値にリセットされます。変更を有効にするには、システムをリブートする必要があります。

- Windows ロックダウンの設定：デバイスの AnyConnect Secure Mobility Client に対するエンドユーザのアクセス権は制限す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、AnyConnect サービスをユーザー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、サービス パスワードを使用して、コマンド プロンプトからサービスを停止できます。

  VPN、Network Access Manager、Network Visibility Module、および Umbrella ローミング セキュリティ モジュールの MSI インストーラは、共通のプロパティ（LOCKDOWN）をサポートします。LOCKDOWN が 0 以外の値に設定されている場合、インストーラに関連付けられた Windows サービスをエンドポイント デバイスでユーザまたはローカル管理者が制御することはできません。サンプルのトランスフォームを使用して、このプロパティを設定し、ロックダウンした各 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。サンプルのトランスフォームは、AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページからダウンロードできます。

  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、LOCKDOWN 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。この操作は片方向のみであり、製品を再インストールしない限り削除できません。

  （注） AMP イネーブラ インストーラには、VPN インストーラが組み合わされています。

- ActiveX コントロールの有効化：AnyConnect 事前展開 VPN パッケージの以前のバージョンでは、VPN WebLaunch ActiveX コントロールがデフォルトでインストールされていました。設定の安全性ため、VPN ActiveX コントロールのインストールはデフォルトでオフになっています。

  AnyConnect クライアントとオプション モジュールを事前展開する際、VPN ActiveX コントロールを AnyConnect でインストールする必要がある場合には、msiexec またはトランスフォームとともに NOINSTALLACTIVEX=0 オプションを使用する必要があります。

- [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：インストールした AnyConnect モジュールをユーザーの Windows コントロールパネルの [プログラムの追加と削除（Add/Remove Program List）] リストに表示されないようにすることができます。インストーラに ARPSYSTEMCOMPONENT=1 を渡すと、そのモジュールはインストール済みプログラムのリストに表示されなくなります。

サンプルのトランスフォームを使用して、このプロパティを設定し、非表示にする各モジュールの MSI インストーラごとにトランスフォームを適用することを推奨します。サンプルのトランスフォームは、AnyConnect ソフトウェア ダウンロード ページからダウンロードできます。

AnyConnect モジュール用の Windows インストーラプロパティ

次の表に、MSI インストール コマンド ライン コールの例およびプロファイルの展開先を示します。

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 機能なしの AnyConnect （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 anyconnect-win-*version*-predeploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log
VPN 機能付きの AnyConnect	msiexec /package anyconnect-win-*version*-predeploy-k9.msi /norestart /passive /lvx* anyconnect-win-*version*-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*-predeploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-*version*-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

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
AMP	msiexec /package anyconnect-win-*version*-amp-predeploy-k9.msi /norestart/ passive /lvx* anyconnect-win-*version*-amp-predeploy-k9-install-datetimestamp.log
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 モジュール	msiexec /package anyconnect-win-*version*-umbrella-predeploy-k9.msi/norestart/ passive /lvx* anyconnect-win-*version*-predeploy-k9-install-datetimestamp.log

Cisco Secure Firewall 適応型セキュリティアプライアンスへのカスタマイズされたインストーラトランスフォームのインポート

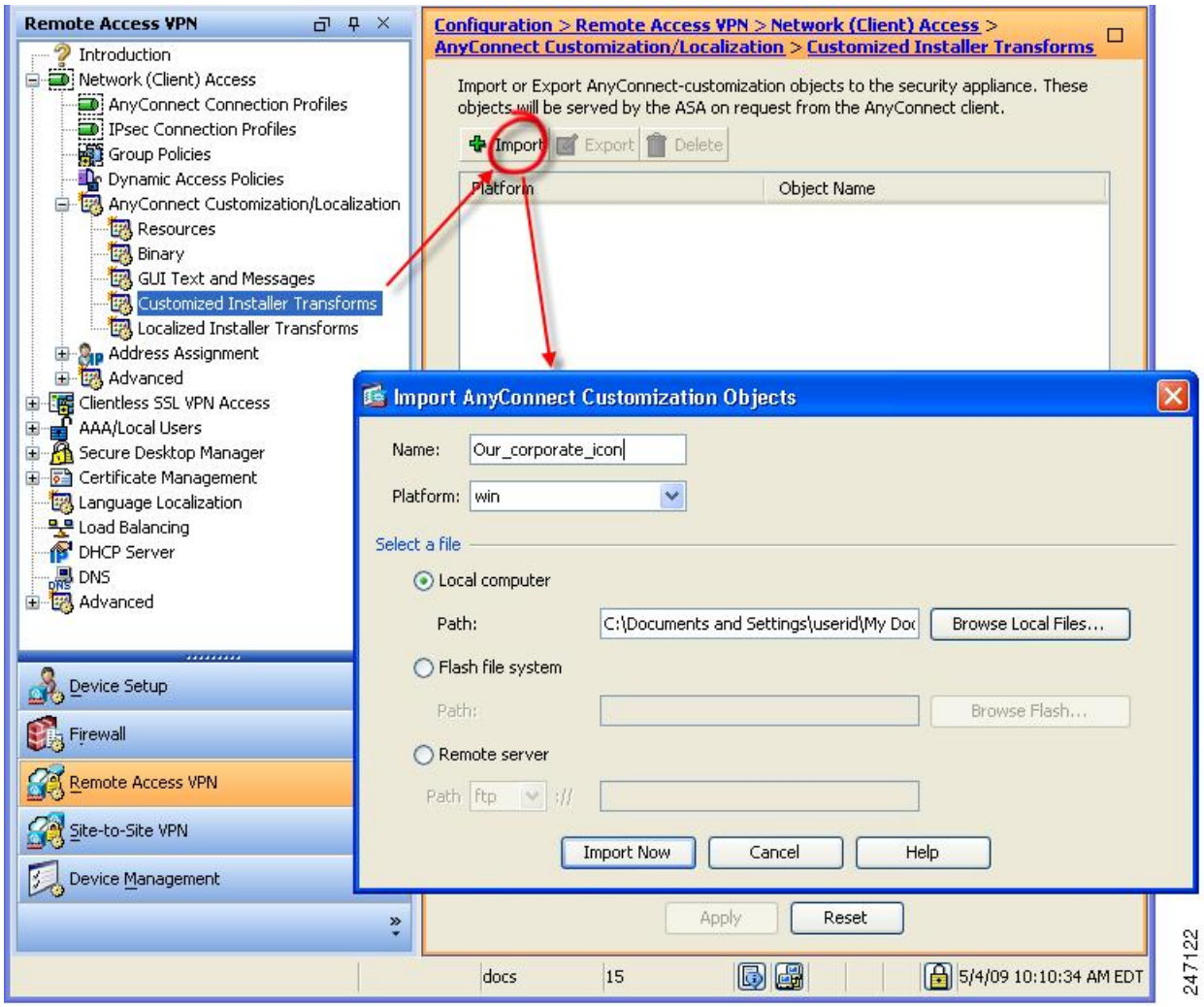
シスコが提供する Windows トランスフォームを Cisco Secure Firewall ASA にインポートすると、Web 展開に使用できます。

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）]** > **[AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）]** > **[カスタマイズされたインストーラ トランスフォーム（Customized Installer Transforms）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。

[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Objects）] ウィンドウが表示されます。



ステップ 3 インポートするファイルの名前を入力します。トランスフォームファイルの名前によって、インストーラ トランスフォーム ファイルが適用されるモジュールが決まります。次の構文を使用して、トランスフォームをグローバルに適用することも、モジュールごとに適用することもできます。

a) *_name*.mst：すべてのインストーラに適用

b) <moduleid>*_name*.mst：1 つのモジュールインストーラに適用

c) *name*.mst：VPN インストーラのみに適用

ステップ 4 プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。インストーラ トランスフォームのテーブルにファイルが表示されます。

AnyConnect インストーラ画面のローカライズ

AnyConnect インストーラに表示されるメッセージを翻訳できます。Cisco Secure Firewall ASA はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

（注） AnyConnect のすべてのリリースには、ローカライズされたトランスフォームが含まれています。このトランスフォームは、管理者が新しいソフトウェアを含む AnyConnect パッケージをアップロードすると、必ず Cisco Secure Firewall ASA にアップロードできます。ローカリゼーション トランスフォームを使用している場合は、新しい AnyConnect パッケージをアップロードする際に、必ず cisco.com の最新リリースでローカリゼーション トランスフォームをアップデートしてください。

現時点では、30 の言語に対応するトランスフォームが用意されています。これらのトランスフォームは、cisco.com の AnyConnect ソフトウェア ダウンロード ページから、次の .zip ファイルで入手できます。

```
anyconnect-win-<VERSION>-webdeploy-k9-lang.zip
```

このファイルの <VERSION> は、AnyConnect のリリースバージョンを表します。

アーカイブには使用可能な翻訳用のトランスフォーム（.mst ファイル）が含まれています。用意されている 30 以外の言語をリモートユーザーに表示する必要がある場合は、独自のトランスフォームを作成し、それを新しい言語として Cisco Secure Firewall ASA にインポートすることができます。Microsoft のデータベース エディタ Orca を使用して、既存のインストレーションおよび新規ファイルを修正できます。Orca は、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows SDK に同梱されています。

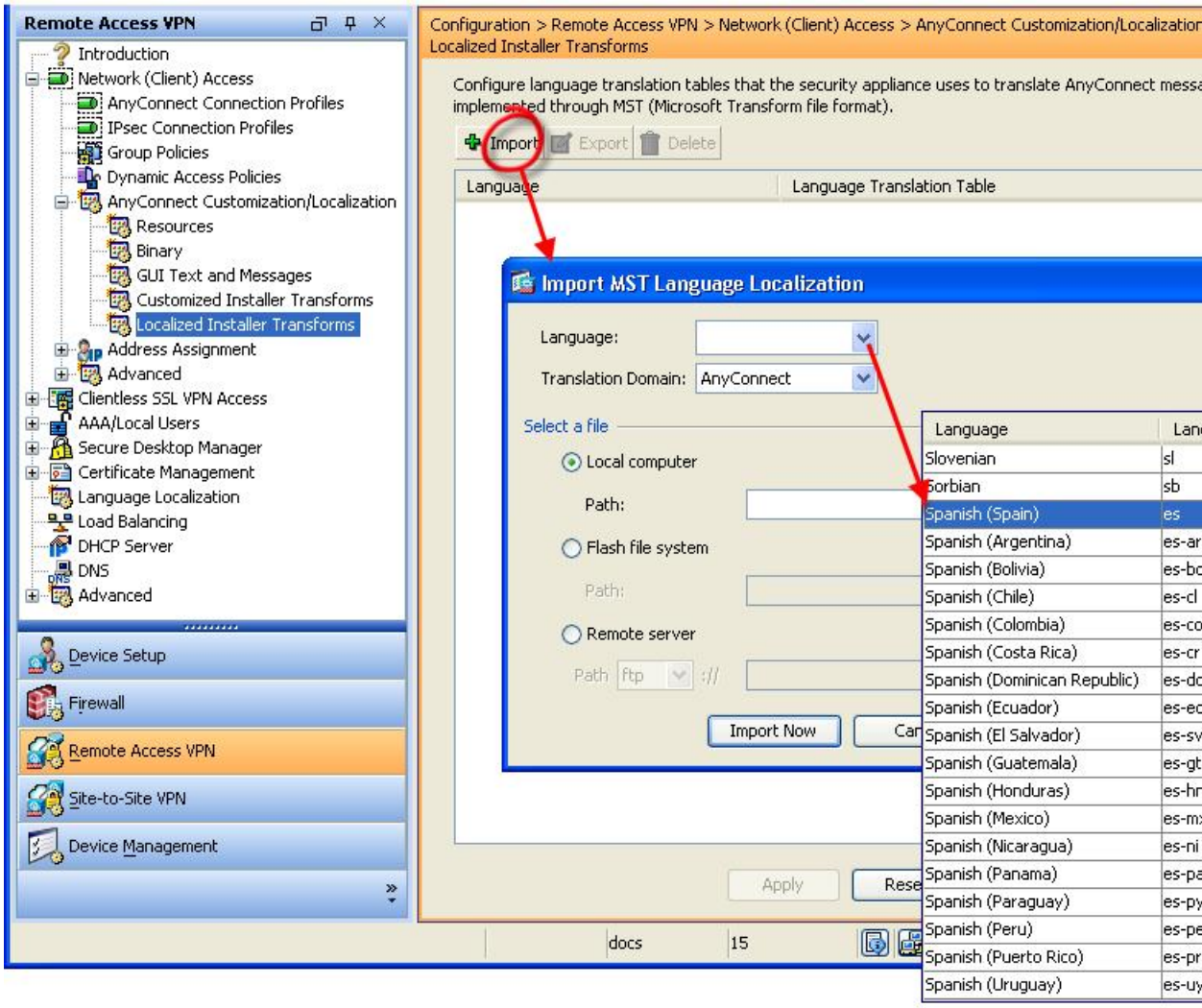
Cisco Secure Firewall ASA へのローカライズされたインストーラ トランスフォームのインポート

ここでは、ASDM を使用してトランスフォームを Cisco Secure Firewall ASA にインポートする方法について説明します。

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）]** > **[AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）]** > **[ローカライズされたインストーラ トランスフォーム（Localized Installer Transforms）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。[MST 言語ローカライズのインポート（Import MST Language Localization）] ウィンドウが表示されます。



ステップ 3 [言語（Language）] ドロップダウン リストをクリックして、このトランスフォーム用の言語（および業界で認められている略称）を選択します。手動で略称を入力する場合は、ブラウザおよびオペレーティング システムが認識できる略称を使用してください。

ステップ 4 [今すぐインポート（Import Now）] をクリックします。
テーブルが正常にインポートされたことを示すメッセージが表示されます。

ステップ 5 [適用（Apply）] をクリックして変更を保存します。

この手順では、言語にスペイン語（es）を指定しました。次の図は、AnyConnect の言語リストのスペイン語の新しいトランスフォームを示しています。

インストール動作の変更、macOS

AnyConnect インストーラーはローカライズできません。インストーラによって使用される文字列は、macOS インストーラ アプリケーションから取得され、AnyConnect インストーラからは取得されません。

（注） インストーラ UI でユーザに表示されるオプションのモジュール選択を操作することはできません。インストーラ UI でデフォルトのオプションモジュールの選択を変更するには、インストーラを編集する必要があります。これにより署名が無効になります。

ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ

macOS については .pkg の動作をカスタマイズする標準の方法が提供されていないため、ACTransforms.xml を作成しました。この XML ファイルをインストーラとともに配置すると、インストーラはインストールを実行する前にこのファイルを読み取ります。ファイルをインストーラからの特定の相対パスに配置する必要があります。インストーラは、次の場所で変更が見つかるかどうかこの順序で検索します。

1. .pkg インストーラ ファイルと同じディレクトリにある「Profile」ディレクトリ内。
2. マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内。
3. マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内。

XML ファイルの形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

たとえば、macOS ACTransforms.xml プロパティは、Network Visibility Module の「スタンドアロン」展開を作成する場合 DisableVPN です。ACTransforms.xml は、DMG ファイルの Profiles ディレクトリ内にあります。

カスタマー エクスペリエンス フィードバック モジュールの無効化

カスタマー エクスペリエンス フィードバック モジュールは、デフォルトで有効になっています。macOS でこの機能をオフにするには、次の手順を実行します。

手順

ステップ 1 ディスク ユーティリティまたは hdiutil を使用して、dmg パッケージを読み取り専用から読み取り/書き込みに変換します。次に例を示します。

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg
```

ステップ 2 まだ設定されていない場合は、ACTransforms.xml を編集し、次の値を設定または追加します。

```
<DisableCustomerExperienceFeedback>false</DisableCustomerExperienceFeedback>
```

インストール動作の変更、Linux

ACTransform.xml による Linux でのインストーラ動作のカスタマイズ

Linux については .pkg の動作をカスタマイズする標準の方法が提供されていないため、ACTransforms.xml を作成しました。この XML ファイルをインストーラとともに配置すると、インストーラはインストールを実行する前にこのファイルを読み取ります。ファイルをインストーラからの特定の相対パスに配置する必要があります。インストーラは、次の場所で変更が見つかるかどうかこの順序で検索します。

- .pkg インストーラ ファイルと同じディレクトリにある「Profile」ディレクトリ内
- マウント済みディスク イメージ ボリュームのルートにある「Profile」ディレクトリ内
- .dmg ファイルと同じディレクトリにある「Profile」ディレクトリ内

事前展開パッケージ内の Profiles ディレクトリの XML ファイルである ACTransforms.xml の形式は次のとおりです。

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

DSCP の保存の有効化

Windows または macOS X プラットフォームでは、DTLS 接続でのみ DiffServ コードポイント（DSCP）を制御するカスタム属性を設定できます。DSCP の保存により、デバイスは遅延の影響を受けやすいトラフィックを優先することができます。ルータでは、これが設定されているかどうかが反映され、アウトバウンド接続品質の向上のために優先トラフィックがマークされます。

カスタム属性タイプは DSCPPreservationAllowed であり、有効な値は True または False です。

（注） デフォルトでは、AnyConnectはDSCPの保存を実行します（True）。無効にするには、ヘッドエンドでカスタム属性値を false に設定し、接続を再初期化します。

この機能は、ASDM の **[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）] > [追加/編集（Add/Edit）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）]** で設定します。設定プロセスについては、適切なバージョンの『Cisco ASA Series VPN ASDM コンフィギュレーション ガイド』の「Enable DSCP Preservation」の項を参照してください。

パブリック DHCP サーバ ルートの設定

AnyConnect は、すべてのネットワークのトンネルが設定されているときにローカル DHCP トラフィックを暗号化せずに流せるようにするために、クライアント接続時にローカル DHCP サーバーに特殊なルートを追加します。また、このルートでのデータ漏えいを防ぐため、AnyConnectはホストデバイスのLANアダプタに暗黙的なフィルタを適用し、DHCPトラフィックを除く、そのルートのすべてのトラフィックをブロックします。外部インターフェイスに接続し、ローカルDHCPサーバを使用して接続が確立されると、そのサーバへの特殊なルートが作成され、非仮想アダプタではなくNICをポイントします。同じサーバで他のサービス（WINS、DNS など）が実行されている場合は、VPN セッションが確立されると、このルートがこれらのサービスを中断します。

Windowsでは、グループポリシーのカスタム属性を設定することで、パブリックなDHCPサーバ ルートの作成を制御できます。トンネル確立時のパブリック DHCP サーバ ルート作成を避けるために、no-dhcp-server-route カスタム属性が存在し、これを true に設定する必要があります。

この機能は、ASDM の **[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）] > [追加/編集（Add/Edit）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）]** で設定します。設定プロセスについては、適切なリリースの『Cisco ASA Series VPN ASDM コンフィギュレーション ガイド』を参照してください。

AnyConnect GUI テキストとメッセージのカスタマイズ

Cisco Secure Firewall ASA は、変換テーブルを使用して AnyConnect に表示されるユーザーメッセージを翻訳します。変換テーブルとは、翻訳されたメッセージテキストの文字列を含むテキスト ファイルです。ASDM またはトランスフォーム（Windows の場合）を使用して、既存のメッセージを編集したり、言語を追加したりできます。

ローカリゼーション用の次の Windows サンプル トランスフォームは、www.cisco.com で入手できます。

- Windows プラットフォームの事前展開パッケージ用言語ローカリゼーション トランスフォーム ファイル
- Windows プラットフォームの Web 展開パッケージ用言語ローカリゼーション トランスフォーム ファイル

Windows 用 AnyConnect パッケージファイルには、AnyConnect メッセージとして使用する、デフォルトの英語の言語テンプレートが含まれます。AnyConnect パッケージを ASA にロードすると、Cisco Secure Firewall ASA はこのファイルを自動的にインポートします。このテンプレートには、AnyConnect ソフトウェア内のメッセージ文字列の最新の変更が含まれています。これを使用すると、別の言語用の変換テーブルを新しく作成できます。または、www.cisco.com から入手可能な次の変換テーブルのいずれかをインポートすることができます（「Cisco Secure Firewall ASA への変換テーブルのインポート （63 ページ）」を参照）。

- 中国語（簡体字）
- 中国語（繁体字）
- チェコ語
- オランダ語
- フランス語
- フランス語（カナダ）
- ドイツ語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- ポーランド語
- ポルトガル語（ブラジル）
- ロシア語
- スペイン語（ラテンアメリカ）

次の項では、目的の言語が利用できない場合や、インポートした変換テーブルをさらにカスタマイズしたい場合などに、GUI テキストおよびメッセージを翻訳するための手順を説明します。

- AnyConnect のテキストとメッセージの追加または編集。メッセージ ファイルを追加または編集して、1 つ以上のメッセージ ID のメッセージテキストを次の方法で変更して、メッセージ ファイルに変更を加えることができます。
  - 開いたダイアログのテキストに変更内容を入力します。

- 開いたダイアログのテキストをテキストエディタにコピーし、変更を行い、そのテキストを元のダイアログに貼り付けます。

- Cisco Secure Firewall ASA への変換テーブルのインポート （63 ページ）。[ファイルに保存（Save to File）] をクリックして、そのファイルを編集し、ファイルを ASDM にもう一度インポートすることで、メッセージ ファイルをエクスポートできます。

Cisco Secure Firewall ASA の変換テーブルを更新した後、クライアントをリスタートして別の接続に成功するまでは、更新したメッセージは適用されません。

（注） クライアントを Cisco Secure Firewall ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのカタログユーティリティを使用して、手動で AnyConnect 変換テーブル（anyconnect.po）を .mo ファイルに変換し、その .mo ファイルをクライアントコンピュータの適切なフォルダにインストールします。詳細については、「エンタープライズ展開用のメッセージ カタログの作成」（3-22 ページ）を参照してください。

注意事項と制約事項

AnyConnect は、すべての国際化の要件に完全には準拠していません。次の例外があります。

- 日付/時刻の形式は、ロケールの要件に従わない場合があります。
- 右から左への言語はサポートされません。
- 一部の文字列はハードコードされたフィールド長により UI で切り捨てられます。
- 次のようないくつかのハードコードされた英語文字列は、そのまま維持されます。
  - 更新時のステータス メッセージ。
  - 信頼できないサーバ メッセージ。
  - 遅延アップデート メッセージ。

AnyConnect のテキストとメッセージの追加または編集

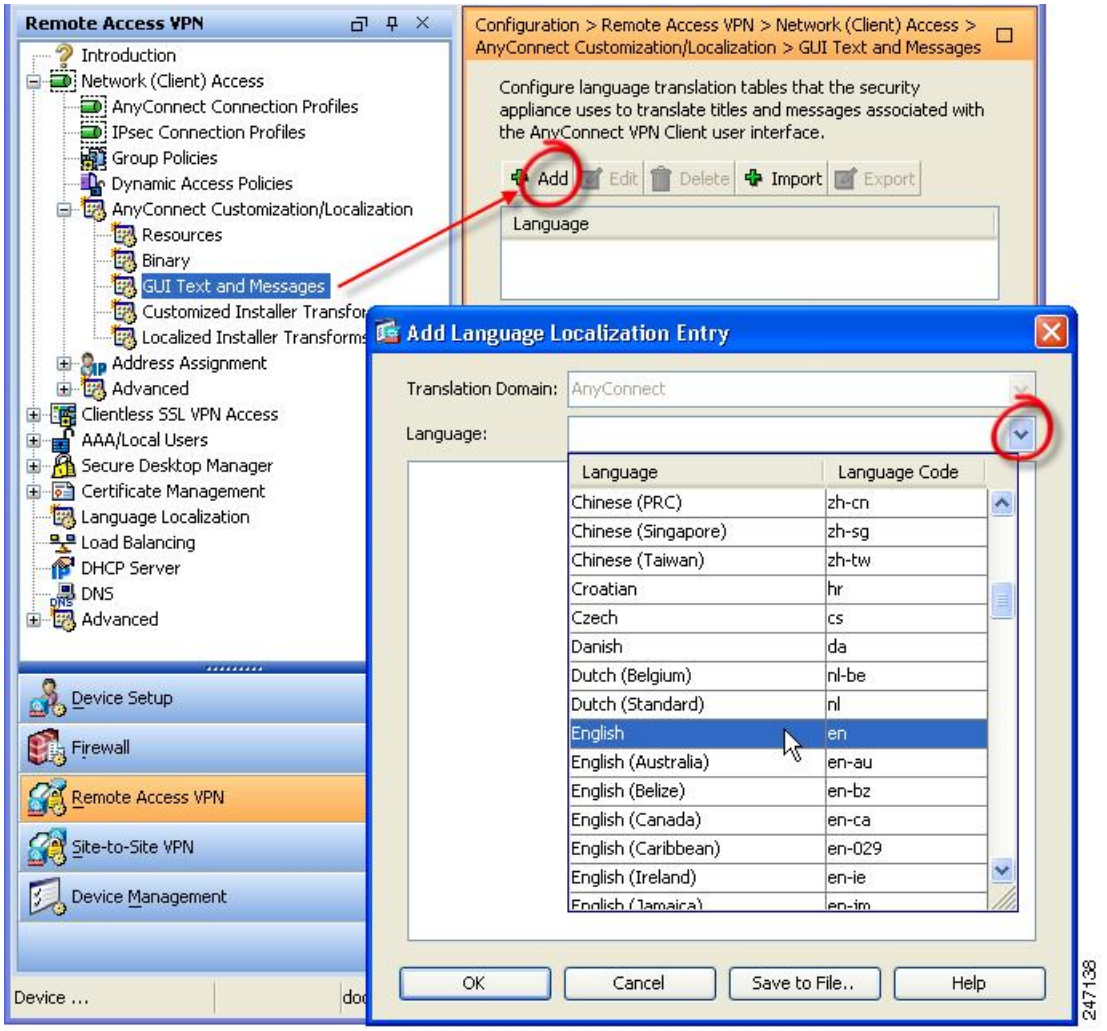
英語変換テーブルを追加または編集し、1 つ以上のメッセージ ID のメッセージ テキストを変更することによって、AnyConnect GUI に表示される英語のメッセージを変更できます。メッセージ ファイルを開いたら、次の操作でそれを編集できます。

- 開いたダイアログのテキストに変更内容を入力します。
- 開いたダイアログのテキストをテキストエディタにコピーし、変更を行い、そのテキストを元のダイアログに貼り付けます。
- [ファイルに保存（Save to File）] をクリックしてメッセージ ファイルをエクスポートし、そのファイルを編集し、ファイルを ASDM にインポートします。

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）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 2 [追加（Add）] をクリックします。[言語ローカリゼーション エントリの追加（Add Language Localization Entry）] ウィンドウが表示されます。



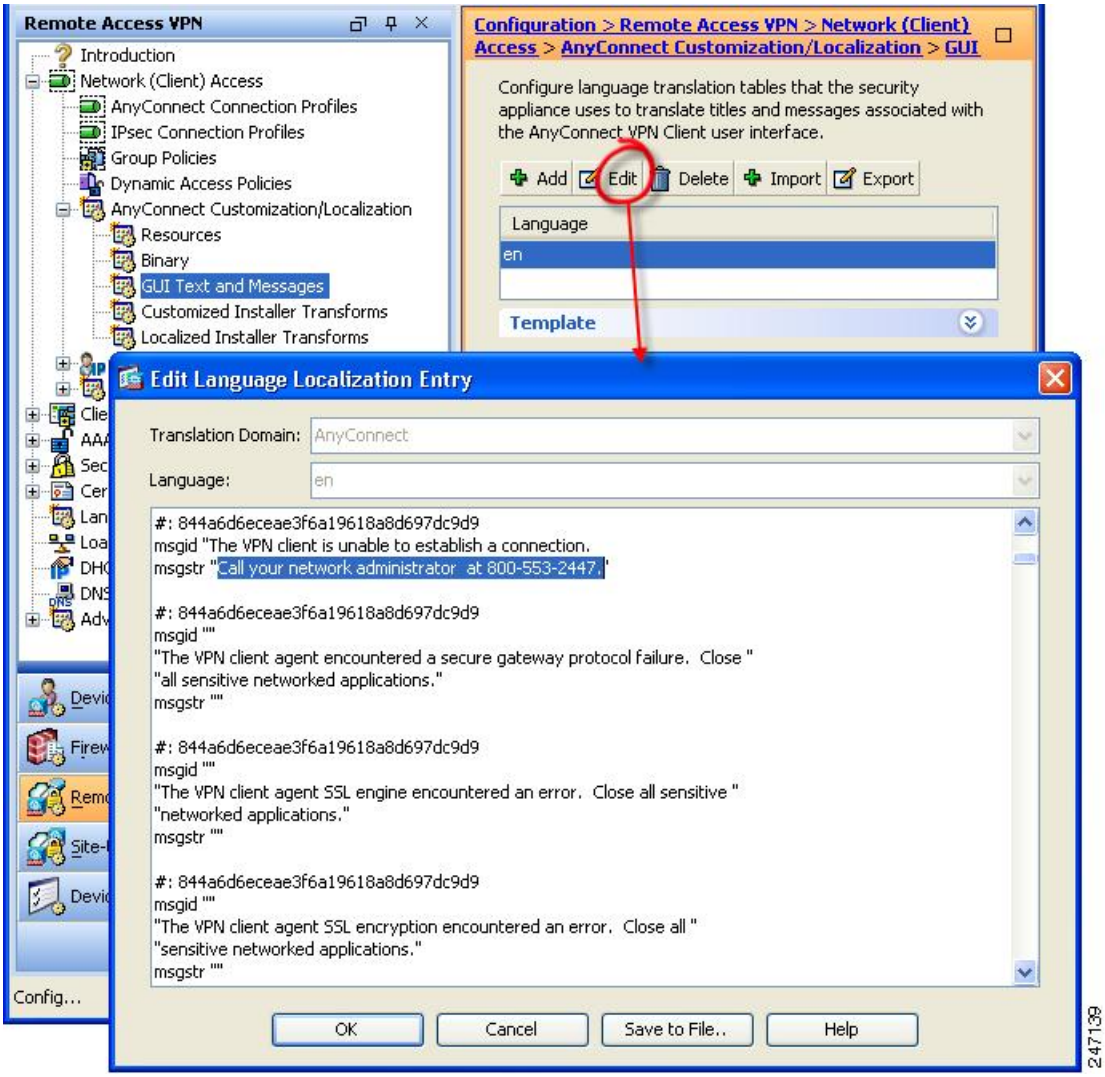
ステップ 3 [言語（Language）] ドロップ リストをクリックし、言語として [英語（en）（English (en)）] を指定します。英語の変換テーブルが、ペインの言語リストに表示されます。

ステップ 4 [編集（Edit）] をクリックして、メッセージの編集を開始します。

[言語のローカライズ エントリの編集（Edit Language Localization Entry）] ウィンドウが表示されます。msgid の引用符で囲まれたテキストは、クライアントに表示されるデフォルトの英語テキストです。変更してはいけません。msgstr の文字列には、msgid のデフォルト テキストを

置き換えるために、クライアントで使用されるテキストが含まれます。msgstr の引用符の間に、使用するテキストを挿入します。

次の例では、「Call your network administrator at 800-553-2447」が挿入されています。



ステップ 5 [OK]、[適用（Apply）] の順にクリックし、変更内容を保存します。

Cisco Secure Firewall ASA への変換テーブルのインポート

手順

ステップ 1 www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2 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）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 3 [インポート（Import）] をクリックします。[言語ローカリゼーション エントリのインポート（Import Language Localization Entry）] ウィンドウが表示されます。

ステップ 4 ドロップダウン リストから適切な言語を選択します。

ステップ 5 変換テーブルのインポート元を指定します。

ステップ 6 [今すぐインポート（Import Now）] をクリックします。この変換テーブルが、この優先言語で AnyConnect クライアントに展開されます。ローカリゼーションは、AnyConnect がリスタートし、再接続した後に適用されます。

エンタープライズ展開用のメッセージ カタログの作成

クライアントを Cisco Secure Firewall ASA から展開せずに、Altiris Agent などの社内のソフトウェア展開システムを使用する場合は、Gettext などのユーティリティを使用して、手動で AnyConnect 変換テーブルをメッセージカタログに変換できます。テーブルを .po ファイルから .mo ファイルに変換後、そのファイルをクライアント コンピュータ上の該当するフォルダに配置します。

（注） GetText と PoeEdit は、サードパーティ製ソフトウェア アプリケーションです。AnyConnect GUI をカスタマイズする推奨方法は、Cisco Secure Firewall ASA からデフォルトの .mo ファイルを取得し、クライアントへの展開での必要に応じてそのファイルを編集する方法です。デフォルトの .mo ファイルを使用することによって、GetText や PoeEdit などのサードパーティ製アプリケーションに起因する潜在的な変換に関する問題を回避することができます。

Gettext は GNU プロジェクトのユーティリティであり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。Gettext を使用してメッセージ カタログを作成する手順は、次のとおりです。

AnyConnect AnyConnect メッセージテンプレートのディレクトリ

AnyConnect メッセージテンプレートは、各オペレーティングシステムで、次に示すフォルダにあります。

（注） \l10n ディレクトリは、次に示す各ディレクトリ パスの一部です。このディレクトリ名のスペルは、小文字の l（「エル」）、1、0、小文字の n です。

- Windows の場合：<DriveLetter>:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES
- macOS および Linux の場合：/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES

手順

ステップ 1 Gettext ユーティリティを http://www.gnu.org/software/gettext/ からダウンロードし、管理用のコンピュータ（リモート ユーザーのコンピュータ以外）にインストールします。

ステップ 2 AnyConnect がインストールされたコンピュータにある、AnyConnect メッセージテンプレート AnyConnect.po のコピーを取得します。

ステップ 3 この AnyConnect.po ファイルを編集し（notepad.exe または任意のプレーン テキスト エディタを使用）、必要に応じて文字列を変更します。

ステップ 4 Gettext のメッセージ ファイル コンパイラを実行して、次のように .po ファイルから .mo ファイルを作成します。

msgfmt -o AnyConnect.mo AnyConnect.po

ステップ 5 ユーザーのコンピュータ上の正しいメッセージ テンプレート ディレクトリに .mo ファイルのコピーを格納します。

Cisco Secure Firewall ASA のカスタマイズした変換テーブルへの新しいメッセージの統合

新しいユーザーメッセージが、AnyConnect の一部のリリースに追加されています。これらの新しいメッセージの翻訳を有効にするために、新しいメッセージ文字列は、最新のクライアントイメージとともにパッケージ化された翻訳テンプレートに追加されています。以前のクライアントに含まれていたテンプレートに基づいて変換テーブルを作成した場合、リモートユーザーには新しいメッセージが自動的には表示されません。最新のテンプレートを既存の変換テーブルに統合し、変換テーブルに新しいメッセージを含める必要があります。

統合を実行するための無料のサードパーティ製ツールがあります。GNU プロジェクトの Gettext ユーティリティには Windows 版があり、コマンド ウィンドウで実行できます。詳しくは、GNU の Web サイト（gnu.org）を参照してください。また、Poedit などの、Gettext を使用する GUI ベースのユーティリティを使用することもできます。このソフトウェアは poedit.net から入手できます。両方の手順を次に示します。

（注） この手順は、すでに最新の AnyConnect イメージ パッケージを Cisco Secure Firewall ASA にロードしてあることが前提になっています。まだロードしていない場合は、テンプレートをエクスポートできません。

手順

ステップ 1 **[リモートアクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）] > [テンプレート（Templates）]** を選択し、最新の AnyConnect 翻訳テンプレートをエクスポートします。AnyConnect.pot というファイル名で、テンプレートをエクスポートします。このファイル名にすると、msgmerge.exe プログラムからこのファイルがメッセージ カタログ テンプレートとして認識されます。

ステップ 2 AnyConnect テンプレートおよび変換テーブルを統合します。

Windows 版の Gettext ユーティリティを使用している場合は、コマンド プロンプト ウィンドウを開き、次のコマンドを実行します。このコマンドでは、次のように、AnyConnect 変換テーブル（.po）とテンプレート（.pot）が統合され、AnyConnect_merged.po ファイルが新しく作成されます。

```
msgmerge -o AnyConnect_merged.po AnyConnect.po AnyConnect.pot
```

このコマンドの実行結果の例を次に示します。

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po
AnyConnect.pot

..................................... done.
```

Poedit を使用している場合は、初めに AnyConnect.po ファイルを開きます。それには、[ファイル（File）] > [オープン（Open）] > <AnyConnect.po> の順に選択します。次に、POT ファイル <AnyConnect.pot> から、[カタログ（Catalog）]>[更新（Update）] の順に選択して、テンプレートと統合します。新しい文字列と使用されなくなった文字列の両方を示す、[更新概要（Update Summary）] ウィンドウが表示されます。ファイルを保存します。このファイルを次の手順でインポートします。

ステップ 3 統合した変換テーブルを、**[リモート アクセス VPN（Remote Access VPN）] > [言語のローカライズ（Language Localization）]** にインポートします。[インポート（Import）] をクリックし、言語を指定して、変換ドメインとして [AnyConnect] を選択します。インポートするファイルとして AnyConnect_merged.po を指定します。

クライアントでの Windows のデフォルト言語の選択

リモートユーザーが Cisco Secure Firewall ASA に接続してクライアントをダウンロードすると、AnyConnect がコンピュータの優先言語を検出し、指定されたシステムロケールを検出して適切な変換テーブルを適用します。

Windows で指定されているシステム ロケールを表示または変更するには、次の手順に従います。

手順

ステップ 1 **[コントロール パネル（Control Panel）]** > **[地域と言語（Region and Languages）]** ダイアログボックスに移動します。コントロール パネルをカテゴリ別に表示している場合は、[時計、言語、および地域（Clock, Language, and Region）] > [表示言語の変更（Change display language）] > を選択します。

ステップ 2 言語/ロケール設定を指定し、これらの設定がすべてのユーザ アカウントのデフォルト設定として使用されることを指定します。

（注） 場所が指定されていない場合、AnyConnect はデフォルトで言語のみが設定されます。たとえば、「fr-ca」ディレクトリが見つからないと、AnyConnect は「fr」ディレクトリを調べます。翻訳内容を表示するのに、表示言語、場所、またはキーボードを変更する必要はありません。

AnyConnect GUI のカスタムアイコンおよびロゴの作成

この項の表は、置き換えることができる AnyConnect ファイルをオペレーティングシステムごとに示しています。表に含まれるイメージは、AnyConnect のコア VPN および Network Access Manager Module により使用されます。

制約事項

- カスタムコンポーネントのファイル名は、AnyConnect GUI で使用されるファイル名と一致している必要があります。これはオペレーティングシステムによって異なり、macOS および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを company_logo.png としてインポートする必要があります。別のファイル名でインポートすると、AnyConnect インストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、その実行ファイルから任意のファイル名のリソースファイルを呼び出すことができます。
- イメージをソースファイルとして（たとえば、company_logo.bmp）インポートする場合、インポートしたイメージは、同じファイル名を使用して別のイメージを再インポートするまで、AnyConnect をカスタマイズします。たとえば、company_logo.bmp をカスタムイメージに置き換えて、このイメージを削除する場合、同じファイル名を使用して新しいイメージ（または元のシスコロゴイメージ）をインポートするまで、クライアントはこのイメージの表示を継続します。

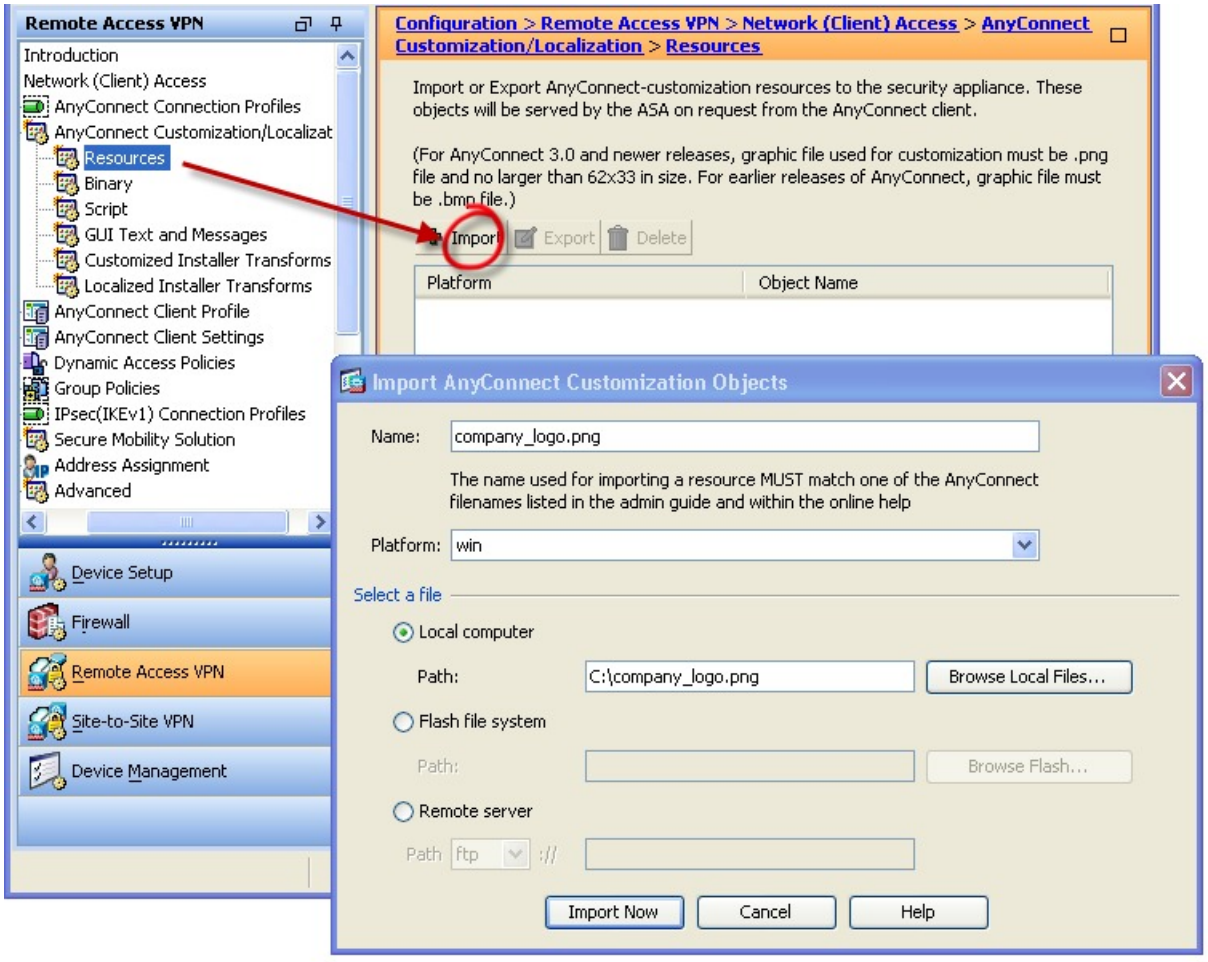
AnyConnect GUI コンポーネントの置き換え

独自のカスタム ファイルをセキュリティ アプライアンスにインポートし、その新しいファイルをクライアントに展開することによって、AnyConnectをカスタマイズすることができます。

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）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）] > [リソース（Resources）]** に移動します。

ステップ 2 [インポート（Import）] をクリックします。[AnyConnect カスタマイゼーション オブジェクトのインポート（Import AnyConnect Customization Objects）] ウィンドウが表示されます。



ステップ 3 インポートするファイルの名前を入力します。

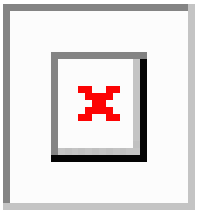
ステップ 4 プラットフォームを選択し、インポートするファイルを指定します。[今すぐインポート（Import Now）] をクリックします。オブジェクトのリストにファイルが表示されます。

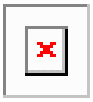
Windows 用 AnyConnect アイコンとロゴ

Windows 用のファイルはすべて次の場所に格納されています。

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

（注） %PROGRAMFILES% は、同じ名前の環境変数を指します。ほとんどの Windows インストレーションでは、`C:\Program Files` です。

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
about.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
about_hover.png [詳細（Advanced）] ダイアログの右上にある [バージョン情報（About）] ボタン。 サイズは調整できません。 	24 x 24 PNG
app_logo.png 最大サイズは 128 x 128 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 128 x 128 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	128 x 128 PNG

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
attention.ico 注意または操作が必要な状態をユーザーに通知するシステム トレイ アイコン。たとえば、ユーザー クレデンシャルについてのダイアログです。 サイズは調整できません。 	16 x 16 ICO
company_logo.png トレイ フライアウトおよび[詳細（Advanced）]ダイアログの左上に表示される企業ロゴ。 最大サイズは 97 x 58 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 97 x 58 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	97 x 58（最大） PNG
company_logo_alt.png [バージョン情報（About）]ダイアログ右下に表示される企業ロゴ。 最大サイズは 97 x 58 です。ご使用のカスタム ファイルがこのサイズ以外の場合は、アプリケーションで 97 x 58 にサイズ変更されます。比率が異なる場合は、引き伸ばされます。 	97 x 58 PNG

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
cues_bg.jpg トレイ フライアウト、[詳細（Advanced）] ウィンドウ、および[バージョン情報（About）] ダイアログの背景イメージ。 イメージが引き伸ばされることはないため、過度に小さい置換イメージを使用すると、領域が黒くなります。 	1260 x 1024 JPEG
error.ico 1 つ以上のコンポーネントで致命的な問題が発生していることをユーザーに通知するシステム トレイ アイコン。 サイズは調整できません。	16 x 16 ICO

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
neutral.ico クライアントのコンポーネントが正常に動作していることを示すシステム トレイ アイコン。 サイズは調整できません。 	16 x 16 ICO
transition_1.ico transition_2.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、Network Access Managerに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO
transition_2.ico transition_1.ico および transition_3.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、Network Access Managerに接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO

Windows インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
transition_3.ico transition_1.ico および transition_2.ico と一緒に使用されるシステム トレイ アイコンで、1 つ以上のクライアント コンポーネントが状態遷移中であることを示します（たとえば、VPN に接続中、Network Access Manager に接続中など）。3 つのアイコン ファイルが次々に表示されます。これは、左から右に移動する 1 つのアイコンのように見えます。 サイズは調整できません。 	16 x 16 ICO
vpn_connected.ico VPN が接続中であることを示すシステム トレイアイコン。 サイズは調整できません。 	16 x 16 ICO

Linux 用 AnyConnect アイコンとロゴ

Linux 用のファイルはすべて次の場所に格納されています。

`/opt/cisco/anyconnect/resources/`

次の表に、置換できるファイルと影響を受けるクライアント GUI エリアを示します。

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
company-logo.png ユーザ インターフェイスの各タブに表示される企業ロゴ。 62 x 33 ピクセル以下の PNG イメージを使用してください。 	142 x 92 PNG

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
cvc-about.png [バージョン情報（About）] タブに表示されるアイコン。 	16 X 16 PNG
cvc-connect.png [接続（Connect）] ボタンの隣、および [接続（Connection）] タブに表示されるアイコン。 	16 X 16 PNG
cvc-disconnect.png [接続解除（Disconnect）] ボタンの隣に表示されるアイコン。 	16 X 16 PNG
cvc-info.png [統計情報（Statistics）] タブに表示されるアイコン。 	16 X 16 PNG
systray_connected.png クライアントが接続中のときに表示されるトレイ アイコン。 	16 X 16 PNG
systray_notconnected.png クライアントが接続中でないときに表示されるトレイ アイコン。 	16 X 16 PNG
systray_disconnecting.png クライアントが接続解除の処理中のときに表示されるトレイ アイコン。 	16 X 16 PNG

Linux インストレーションでのファイル名および説明	イメージ サイズ（ピクセル、長さ X 高さ）およびタイプ
systray_quarantined.png クライアントが隔離中のときに表示されるトレイ アイコン。 	16 x 16 PNG
systray_reconnecting.png クライアントが再接続中のときに表示されるトレイ アイコン。 	16 X 16 PNG
vpnui48.png メイン プログラム アイコン。 	48 x 48 PNG

macOS 用 AnyConnect アイコンとロゴ

macOS の AnyConnect アイコンおよびロゴ。macOS での GUI リソースのカスタマイズは現在サポートされていません。

AnyConnect のヘルプファイルを作成してアップロードする

AnyConnect のユーザーにヘルプを提供するために、サイトに関する手順を含むヘルプファイルを作成し、Cisco Secure Firewall ASA にロードします。ユーザーが AnyConnect に接続すると、ヘルプファイルがダウンロードされ、AnyConnect ユーザーインターフェイス上にヘルプアイコンを表示します。ユーザがヘルプ アイコンをクリックすると、ブラウザにヘルプ ファイルが開きます。PDF および HTML ファイルがサポートされています。

手順

ステップ 1 `help_AnyConnect.html` という名前の HTML ファイルを作成します。

ステップ 2 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）]** > **[AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/LocalizationScript）]** > **[バイナリ（Binary）]** に移動します。

ステップ 3 **help_AnyConnect.xxx** ファイルをインポートします。サポートされる形式は、PDF、HTML、HTM、および MHT です。

ステップ 4 デバイスで、AnyConnect を起動して Secure Firewall ASA 接続します。ヘルプファイルがクライアントデバイスにダウンロードされます。
ヘルプ アイコンが自動的に UI に追加されたことがわかるはずです。

ステップ 5 ヘルプ アイコンをクリックすると、ヘルプ ファイルがブラウザに表示されます。

ヘルプアイコンが表示されない場合は、ヘルプのディレクトリを確認し、AnyConnect のダウンローダーがヘルプファイルを取得できたかどうかを確認します。

ファイル名の「help_」の部分はダウンローダにより削除されるので、ご使用のオペレーティング システムに応じて、次のいずれかのディレクトリの中に AnyConnect.html が保存されているはずです。

- Windows：`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help`
- macOS：`/opt/cisco/anyconnect/help`

スクリプトの作成および展開

AnyConnect では、次のイベントが発生したときに、スクリプトをダウンロードして実行できます。

- セキュリティ アプライアンスで新しいクライアント VPN セッションが確立された。このイベントによって起動するスクリプトを OnConnect スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。
- セキュリティ アプライアンスでクライアント VPN セッションが切断された。このイベントによって起動するスクリプトを OnDisconnect スクリプトと呼びます。スクリプトには、このファイル名プレフィックスが必要です。

Trusted Network Detection によって開始された新しいクライアント VPN セッションが確立すると、OnConnect スクリプトがトリガーされます（スクリプトを実行するための要件が満たされている場合）が、ネットワーク中断後に永続 VPN セッションを再接続しても、OnConnect スクリプトはトリガーされません。

この機能には次のような使用例があります。

- VPN 接続時にグループ ポリシーを更新する。
- VPN 接続時にネットワーク ドライブをマッピングし、接続解除後にマッピングを解除する。
- VPN 接続時にサービスにログインし、接続解除後にログオフする。

AnyConnect は、WebLaunch の起動中およびスタンドアロン起動中でのスクリプトの起動をサポートしています。

ここでの説明は、スクリプトの作成方法と、ターゲット エンドポイントのコマンド ラインからスクリプトを実行し、テストする方法についての知識があることを前提としています。

（注） AnyConnect のソフトウェア ダウンロード サイトでは、サンプルスクリプトがいくつか提供されています。これらを確認する場合は、単なるサンプルであることに留意してください。これらのサンプル スクリプトは、スクリプトを実行するために必要なローカル コンピュータの要件を満たしていない場合があります。また、ご使用のネットワークおよびユーザーのニーズに応じてカスタマイズしてからでないと使用できません。シスコでは、サンプル スクリプトまたはユーザー作成スクリプトはサポートしていません。

スクリプトの要件と制限

次のスクリプトの要件と制限事項に留意してください。

- サポートされるスクリプトの数：AnyConnect は、1 つの OnConnect スクリプトおよび 1 つの OnDisconnect スクリプトのみを実行します。ただし、これらのスクリプトが別のスクリプトを起動する場合があります。
- ファイル形式：AnyConnect は、ファイル名で OnConnect スクリプトおよび onDisconnect スクリプトを識別します。また、ファイル拡張子に関係なく、OnConnect または OnDisconnect で始まるファイルを検索します。照合プレフィックスに関連する最初のスクリプトが実行されます。解釈されたスクリプト（VBS、Perl、Bash など）または実行可能ファイルを認識します。
- スクリプト言語：クライアントでは、スクリプトを特定の言語で作成する必要はありません。ただし、スクリプトを実行可能なアプリケーションが、クライアント コンピュータにインストールされている必要があります。クライアントでスクリプトを起動するためには、このスクリプトがコマンド ラインから実行可能であることが必要です。
- Windows セキュリティ環境によるスクリプトの制限：Microsoft Windows では、AnyConnect はユーザーが Windows にログインし、VPN セッションを確立した後でのみスクリプトを起動できます。したがって、ユーザーのセキュリティ環境によって課される制限がこれらのスクリプトに適用されます。スクリプトは、ユーザーが呼び出す権限を持つ関数のみを実行できます。 AnyConnect は、Windows でのスクリプトの実行中に cmd ウィンドウを非表示にするため、スクリプトを実行してテスト目的で .bat ファイルにメッセージを表示することはできません。
- スクリプトの有効化：デフォルトでは、クライアントはスクリプトを起動しません。AnyConnect プロファイルの EnableScripting パラメータを使用して、スクリプトを有効にしてください。これにより、クライアントではスクリプトが存在する必要がなくなります。
- クライアント GUI 終了：クライアント GUI を終了しても、必ずしも VPN セッションは終了しません。OnDisconnect スクリプトは、セッションが終了した後で実行されます。

- 64 ビット Windows でのスクリプトの実行：AnyConnect は、32 ビットアプリケーションです。64 ビット Windows バージョンで実行すると、cmd.exe の 32 ビット バージョンが使用されます。

  32 ビットの cmd.exe では、64 ビットの cmd.exe でサポートされているコマンドの一部が欠けているため、一部のスクリプトについては、サポートされていないコマンドの実行を試行したときにスクリプトの実行が停止したり、一部実行されてから停止したりする場合があります。たとえば、64 ビットの cmd.exe でサポートされている msg コマンドは、32 ビット バージョンの Windows 7（%WINDIR%\SysWOW64 に含まれる）では理解されない場合があります。

  そのため、スクリプトを作成する場合は、32 ビットの cmd.exe でサポートされているコマンドを使用してください。

スクリプトの作成、テスト、および展開

対象のオペレーティング システムでスクリプトを作成およびテストします。ネイティブ オペレーティング システムのコマンドラインからスクリプトを正しく実行できない場合は、AnyConnect でも正しく実行できません。

手順

ステップ 1 スクリプトを作成およびテストします。

ステップ 2 スクリプトの展開方法を選択します。

- ASDM を使用して、スクリプトをバイナリ ファイルとして Cisco Secure Firewall ASA にインポートします。

  [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [スクリプト（Script）] に進みます。

  ASDM バージョン 6.3 以降を使用している場合、Cisco Secure Firewall ASA では、ファイルをスクリプトとして識別できるように、プレフィックス scripts_ とプレフィックス OnConnect または OnDisconnect がユーザーのファイル名に追加されます。クライアントが接続すると、セキュリティ アプライアンスは、リモート コンピュータ上の適切なターゲット ディレクトリにスクリプトをダウンロードし、scripts_ プレフィックスを削除し、OnConnect プレフィックスまたは OnDisconnect プレフィックスを残します。たとえば、myscript.bat スクリプトをインポートする場合、スクリプトは、セキュリティ アプライアンス上では scripts_OnConnect_myscript.bat となります。リモート コンピュータ上では、スクリプトは OnConnect_myscript.bat となります。

  6.3 よりも前の ASDM バージョンを使用している場合には、次のプレフィックスでスクリプトをインポートする必要があります。

  - scripts_OnConnect
  - scripts_OnDisconnect

スクリプトの実行の信頼性を確保するために、すべての Cisco Secure Firewall ASA で同じスクリプトを展開するように設定します。スクリプトを修正または置換する場合は、旧バージョンと同じ名前を使用し、ユーザーが接続する可能性のあるすべての Cisco Secure Firewall ASA に置換スクリプトを割り当てます。ユーザーが接続すると、新しいスクリプトにより同じ名前のスクリプトが上書きされます。

- 社内のソフトウェア展開システムを使用して、VPNエンドポイントにスクリプトを手動で展開します。

  この方式を使用する場合は、次のスクリプト ファイル名プレフィックスを使用します。

  - OnConnect
  - OnDisconnect

  次のディレクトリにスクリプトをインストールします。

表 *5:* スクリプトの所定の場所

OS	ディレクトリ
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Linux （Linux では、User、Group、Other にファイルの実行権限を割り当てます）	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect/script

スクリプトに関する AnyConnect プロファイルの設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [スクリプトの有効化（Enable Scripting）] をオンにします。クライアントでは、VPN 接続の接続時または接続解除時にスクリプトが起動します。

ステップ 3 [ユーザ制御可（User Controllable）] をオンにして、OnConnect スクリプトおよび OnDisconnect スクリプトの実行をユーザが有効または無効にすることができるようにします。

ステップ 4 [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）] をオンにして、スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプトプロセスをクライアントが終了できるようにします。たとえば、VPNセッションが終了すると、クライア

ントでは実行中の On Connect スクリプトが終了し、AnyConnect で新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。

ステップ 5 [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）] をオンにして（デフォルトでオン）、SBL で VPN セッションが確立された場合にクライアントにより OnConnect スクリプトが（存在すれば）起動するようにします。

（注） 必ずクライアントプロファイルを Cisco Secure Firewall ASA のグループポリシーに追加し、それを VPN エンドポイントにダウンロードしてください。

スクリプトのトラブルシューティング

スクリプトの実行に失敗した場合は、次のようにして問題を解決してください。

手順

ステップ 1 スクリプトに、`OnConnect` または `OnDisconnect` のプレフィックス名が付いていることを確認します。各オペレーティング システムで必要なスクリプト ディレクトリについては、「スクリプトの作成、テスト、および展開」を参照してください。

ステップ 2 スクリプトをコマンド ラインから実行してみます。コマンド ラインから実行できないスクリプトは、クライアントでも実行できません。コマンドラインでスクリプトの実行に失敗する場合は、スクリプトを実行するアプリケーションがインストールされていることを確認し、そのオペレーティング システムでスクリプトを作成し直してください。

ステップ 3 VPN エンドポイントのスクリプト ディレクトリに、OnConnect スクリプトと OnDisconnect スクリプトがそれぞれ 1 つのみ存在していることを確認してください。クライアントが Cisco Secure Firewall ASA から OnConnect スクリプトをダウンロードして、別の Cisco Secure Firewall ASA 用の異なるファイル名サフィックスを持つ 2 番目の OnConnect スクリプトをダウンロードした場合、クライアントは意図されたスクリプトを実行しない可能性があります。スクリプトパスに複数の OnConnect スクリプトまたは OnDisconnect スクリプトが含まれており、かつスクリプトの展開に Cisco Secure Firewall ASA を使用している場合は、スクリプトディレクトリ内のファイルを削除し、VPNセッションを再確立します。スクリプトパスに複数のOnConnectスクリプトまたはOnDisconnectスクリプトが含まれており、かつ手動展開を使用している場合は、不要なスクリプトを削除し、VPN セッションを再確立します。

ステップ 4 オペレーティング システムが Linux の場合は、スクリプト ファイルに実行権限が設定されていることを確認します。

ステップ 5 クライアント プロファイルでスクリプトが有効になっていることを確認します。

AnyConnect API によるカスタムアプリケーションの作成と展開

Windows、Linux、macOS のコンピュータでは、AnyConnect API を使用して独自の実行可能なユーザーインターフェイス（UI）を開発できます。AnyConnect バイナリファイルを置き換えることで UI を展開します。

次の表に、オペレーティングシステムごとのクライアント実行可能ファイルのファイル名を示します。

クライアント OS	クライアント GUI ファイル	クライアント CLI ファイル
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
macOS	Cisco Secure Firewall ASA 展開ではサポートされていません。ただし、Altiris Agent などの他の手段によって、クライアント GUI を置き換える macOS 用の実行ファイルを展開できます。	vpn

実行可能ファイルは、Cisco Secure Firewall ASA にインポートされたリソースファイル（ロゴイメージなど）を呼び出すことができます。独自の実行可能ファイルを展開する場合、リソース ファイルに任意のファイル名を使用できます。

制約事項

- Cisco Secure Firewall ASA から更新された AnyConnect ソフトウェアを展開することはできません。Cisco Secure Firewall ASA に AnyConnect パッケージの最新バージョンを配置すると、AnyConnect クライアントはその更新をダウンロードして、カスタム UI を置き換えます。カスタムクライアントおよび関連する AnyConnect ソフトウェアの配布を管理する必要があります。ASDM でバイナリをアップロードして AnyConnect を置き換えることができる場合でも、この展開機能は、カスタムアプリケーションを使用しているときにはサポートされません。
- Network Access Managerを展開する場合は、AnyConnect Secure Mobility Client GUI を使用します。
- Start Before Login はサポートされていません。

AnyConnect の CLI コマンドを使用します。

AnyConnect Secure Mobility Client には、グラフィカル ユーザーインターフェイスを使用せずにクライアントコマンドを入力することを希望するユーザー向けに、コマンド ライン インターフェイス（CLI）があります。ここでは、CLI コマンド プロンプトの起動方法、および CLI を介して使用できるコマンドについて説明します。

- クライアント CLI プロンプトの起動 （82 ページ）
- クライアント CLI コマンドの使用 （82 ページ）
- Cisco Secure Firewall ASA によるセッション終了時に Windows ポップアップメッセージが表示されないようにする （84 ページ）

（注） Windows と macOS では、VPN UI と VPN CLI の両方の接続で同じダウンローダーがプロファイルの更新に使用されます。Linux では、VPN UI のダウンローダーで警告やポップアップが表示される場合があります。たとえば、接続時やプロファイルまたはその他のコンポーネントのダウンロード時に表示されることが多い「信頼できない証明書」の警告などです。ただし、VPN CLI の 2 つ目の Linux ダウンローダーでは、このようなポップアップや警告を表示する機能はなく、予期しない動作として接続エラーメッセージが表示されます。

クライアント CLI プロンプトの起動

CLI コマンド プロンプトを起動するには、以下の手順を実行します。

- （Windows）Windows フォルダ C:/Program Files/Cisco/Cisco AnyConnect Secure Mobility Client にある *vpncli.exe* ファイルを見つけます。vpncli.exe をダブル クリックします。
- （Linux および macOS）/opt/cisco/anyconnect/bin/ フォルダにある *vpn* ファイルを見つけます。*vpn* ファイルを実行します。

クライアント CLI コマンドの使用

インタラクティブ モードで CLI を実行する場合、独自のプロンプトが表示されます。コマンド ラインを使用することもできます。

- connect *IP address* または *alias*：クライアントは特定の Cisco Secure Firewall ASA との接続を確立します。
- disconnect：クライアントは以前に確立した接続を閉じます。
- stats：確立された接続に関する統計情報を表示します。
- quit：CLI インタラクティブ モードを終了します。

• exit：CLI インタラクティブ モードを終了します。

次の例は、ユーザーがコマンド ラインから接続を確立し、終了する例です。

Windows

```
connect 209.165.200.224
```

アドレスが 209.165.200.224 のセキュリティ アプライアンスへの接続を確立します。要求されたホストにアクセスすると、AnyConnectに、ユーザーが属するグループが表示され、ユーザー名とパスワードが要求されます。オプションのバナーを表示するよう指定されている場合、ユーザーはバナーに応答する必要があります。デフォルトの応答は、接続の試行を終了する「n」です。次に例を示します。

```
VPN > connect 209.165.200.224
>>contacting host (209.165.200.224) for login information...
>>Please enter your username and password.
Group: testgroup
Username: testuser
Password: ********
>>notice: Please respond to banner.
VPN>
STOP! Please read. Scheduled system maintenance will occur tonight from 1:00-2:00 AM for
 one hour.
The system will not be available during that time.

accept? [y/n] y
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to 209.165.200.224.
>> State: Connected
>> notice: VPN session established.
VPN>
```

stats

現在の接続の統計情報を表示します。以下に例を示します。

```
VPN > stats
[Tunnel information]

Time Connected: 01:17:33
Client Address: 192.168.23.45
Server Address: 209.165.200.224

[Tunnel Details]

Tunneling Mode: All traffic
Protocol: DTLS
Protocol Cipher: RSA_AES_256_SHA1
Protocol Compression: None

[Data Transfer]

Bytes (sent/received): 1950410/23861719
Packets (sent/received): 18346/28851
Bypassed (outbound/inbound): 0/0
Discarded (outbound/inbound): 0/0

[Secure Routes]

Network Subnet
```

```
0.0.0.0 0.0.0.0
VPN>
```

disconnect

以前に確立した接続を閉じます。以下に例を示します。

```
VPN > disconnect
>> state: Disconnecting
>> state: Disconnected
>> notice: VPN session ended.
VPN>
```

quit または exit

いずれのコマンドも CLI のインタラクティブ モードを終了します。以下に例を示します。

```
quit
goodbye
>>state: Disconnected
```

Linux または macOS

```
/opt/cisco/anyconnect/bin/vpn connect 1.2.3.4
```

アドレスが 1.2.3.4 の Secure Firewall ASA への接続を確立します。

```
/opt/cisco/anyconnect/bin/vpn connect some_asa_alias
```

プロファイルを読み込み、エイリアス *some_asa_alias* を検索してアドレスを探し、Secure Firewall ASA への接続を確立します。

```
/opt/cisco/anyconnect/bin/vpn stats
```

vpn 接続に関する統計情報を表示します。

```
/opt/cisco/anyconnect/bin/vpn disconnect
```

存在する場合、VPN セッションを切断します。

Cisco Secure Firewall ASA によるセッション終了時に Windows ポップアップメッセージが表示されないようにする

Cisco Secure Firewall ASA からセッションリセットを発行することによって AnyConnect セッションを終了すると、エンドユーザーに次の Windows ポップアップメッセージが表示されます。

```
The secure gateway has terminated the vpn connection. The following message was received
 for the gateway: Administrator Reset
```

このメッセージを表示させたくないと思う場合があるかもしれません（たとえば、CLI コマンドを使用して VPN トンネルを開始するときなど）。クライアントが接続した後に、クライアント CLI を再起動することによって、このメッセージを表示さないようにすることができます。次に、この処理を行った場合の CLI 出力例を示します。

```
C:/Program Files (x86)\Cisco\Cisco AnyConnect Secure Mobility Client>vpncli
Cisco AnyConnect Secure Mobility Client (version 4.x).
Copyright (c) 2016 Cisco Systems, Inc.
All Rights Reserved.
>> state: Connected
>> state: Connected
```

```
>> notice: Connected to asa.cisco.com.
>> notice: Connected to asa.cisco.com.
>> registered with local VPN subsystem.
>> state: Connected
>> notice: Connected to asa.cisco.com.
>> state: Disconnecting
>> notice: Disconnect in progress, please wait...
>> state: Disconnected
>> notice: On a trusted network.
>> error: The secure gateway has terminated the VPN connection.
The following message was received from the secure gateway: Administrator Reset
VPN>
```

または、次の場所にあるエンドポイント デバイスでは、Windows レジストリに SuppressModalDialogs という名前の 32 ビットの倍精度値を作成できます。クライアントは名前の有無を検査しますが、値は無視します。

- 64 ビット Windows：

  HKEY_LOCAL_MACHINE/SOFTWARE\Wow6432Node\Cisco\ Cisco AnyConnect Secure Mobility Client

- 32 ビット Windows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client

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

AnyConnect ローカリゼーションバンドルの準備

AnyConnect ローカリゼーションバンドルは、AnyConnect をローカライズするために使用される変換テーブルファイルとインストーラ トランスフォーム ファイルを含む zip ファイルです。この zip ファイルは、ISE からユーザーに AnyConnect を展開するために使用される ISE AnyConnect リソースの一部です。この zip ファイルの内容は、次の手順に従って AnyConnect 展開でサポートする言語によって定義されます。

始める前に

ISE は、AnyConnect ローカリゼーションバンドル内のコンパイル済みのバイナリ変換テーブルを必要とします。gettext には、編集で使用されるテキスト .po とランタイムに使用されるコンパイル済みのバイナリ .mo の 2 つのファイル形式があります。コンパイルは、gettext ツールの msgfmt を使用して行われます。gettext ユーティリティを http://www.gnu.org/software/gettext/ からダウンロードし、管理に使用するローカル コンピュータ（リモートのユーザ コンピュータ以外）にインストールします。

手順

ステップ 1 AnyConnect 展開で使用する変換テーブルファイルを取得して準備します。

a) www.cisco.com の AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページから `AnyConnect-translations-(date).zip` ファイルをダウンロードしてこれを開きます。

この zip ファイルには、シスコによって提供されるすべての言語変換用 *.po ファイルが含まれます。

b) （任意） 現在の環境用にカスタマイズまたは作成した変換テーブル ファイル（*.po ファイル）があれば、それを特定します。

c) gettext メッセージ ファイル コンパイラを実行して、使用している各 *.po ファイルから *.mo ファイルを作成します。

msgfmt -o AnyConnect.mo AnyConnect.po

ステップ 2 AnyConnect 展開で使用する変換テーブルを収集します。

a) ローカル コンピュータの作業領域に `l10n` という名前のディレクトリを作成します。

b) `l10n` ディレクトリの下に、含める各言語のディレクトリを作成します。ディレクトリの名前は各言語コードです。

たとえば、フランス語（カナダ）の場合は `fr-ch` です。

c) 含めるコンパイル済み変換テーブル ファイルを、適切な名前のディレクトリに配置します。

コンパイル済み変換テーブルに *.po ファイルを含めないでください。*.mo ファイルのみをこのファイルに含める必要があります。

ディレクトリ構造は、フランス語（カナダ）、ヘブライ語、および日本語の変換テーブルを含む次のディレクトリ構造と同様になります。

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
```

ステップ 3 （Windows の場合のみ）AnyConnect 展開で使用する言語ローカリゼーション変換ファイルを取得して準備します。

a) www.cisco.com の AnyConnect Secure Mobility Client ソフトウェア ダウンロード ページから、言語ローカリゼーション変換ファイルを含む zip ファイルをダウンロードして開きます。このファイルによりインストーラ画面に翻訳が適用されます。

zip ファイル名は、 `anyconnect-win-(version)-webdeploy-k9-lang.zip` です。

（注） 言語ローカリゼーション ファイルのバージョンは、現在の環境で使用する AnyConnect のバージョンに一致する必要があります。AnyConnect を新しいバージョンにアップグレードする場合は、ローカリゼーションバンドルで使用される言語ローカリゼーションファイルも同じバージョンにアップグレードする必要があります。

zip ファイル名は、 `secureclient-win-(version)-webdeploy-k9-lang.zip` です。

（注） 言語ローカリゼーションファイルのバージョンは、現在の環境で使用する AnyConnect のバージョンに一致する必要があります。AnyConnect を新しいバージョンにアップグレードする場合は、ローカリゼーションバンドルで使用される言語ローカリゼーションファイルも同じバージョンにアップグレードする必要があります。

b) 現在の環境用にカスタマイズまたは作成した言語ローカリゼーション変換ファイルがあれば、それを特定します。

ステップ 4 （Windows の場合のみ）AnyConnect 展開で使用する言語ローカリゼーションファイルを収集します。

a) ローカル コンピュータの同じ作業領域に `mst` いう名前のディレクトリを作成します。

b) `mst`ディレクトリの下に、含める各言語のディレクトリを作成します。ディレクトリの名前は各言語コードです。

たとえば、フランス語（カナダ）の場合は `fr-ch` です。

c) 含める言語ローカリゼーション ファイルを、適切な名前のディレクトリに配置します。

ディレクトリ構造は、次のようになります。

```
l10n\fr-ch\AnyConnect.mo
    \he\AnyConnect.mo
    \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
   \he\AnyConnect_he.mst
   \ja\AnyConnect_ja.mst
```

ステップ 5 標準圧縮ユーティリティを使用して、このディレクトリ構造を 、`AnyConnect-Localization-Bundle-(release).zip` などの適切な名前のファイルに ZIP 圧縮して、AnyConnect ローカリゼーションバンドルを作成します。

次のタスク

AnyConnect ローカリゼーションバンドルを ISE にアップロードします。この ISE リソースは、ユーザーへの AnyConnect の展開に使用されます。

AnyConnect カスタマイゼーション バンドルの準備

AnyConnect カスタマイゼーション バンドルは、カスタム AnyConnect GUI リソース、カスタム ヘルプ ファイル、VPN スクリプト、およびインストーラ トランスフォームを含む zip ファイルです。この zip ファイルは、ISE からユーザーに AnyConnect を展開するために使用される ISE AnyConnect リソースの一部です。このファイルのディレクトリ構造は次のとおりです。

```
win\resource\
   \binary
   \transform
mac-intel\resource
```

```
\binary
\transform
```

カスタマイズされた AnyConnect コンポーネントは、次のように Windows および macOS プラットフォームの resource、binary、および transform サブディレクトリに含まれています。

- 各 resource サブディレクトリには、そのプラットフォーム用のすべてのカスタム AnyConnect GUI コンポーネントが含まれます。

  これらのリソースを作成する方法については、「AnyConnect GUI のカスタムアイコンおよびロゴの作成 （67 ページ）」を参照してください。

- 各 binary サブディレクトリには、そのプラットフォーム用のカスタム ヘルプ ファイルおよび VPN スクリプトが含まれます。
  - AnyConnect のヘルプファイルを作成するには、「AnyConnect のヘルプファイルを作成してアップロードする （75 ページ）」を参照してください。
  - VPN スクリプトを作成する方法については、「スクリプトの作成および展開 （76 ページ）」を参照してください。

- 各 transform サブディレクトリには、そのプラットフォーム用のインストーラ トランスフォームが含まれます。
  - Windows のカスタム インストーラ トランスフォームの作成方法については、「インストール動作の変更、Windows （50 ページ）」を参照してください。
  - macOS のインストーラトランスフォームの作成方法については、「ACTransforms.xml による macOS でのインストーラ動作のカスタマイズ （57 ページ）」を参照してください。

始める前に

AnyConnect カスタマイゼーション バンドルを準備する前に、必要なすべてのカスタムコンポーネントを作成します。

手順

ステップ 1 説明されているディレクトリ構造を、ローカル コンピュータの作業領域に作成します。

ステップ 2 resources ディレクトリに、各プラットフォーム用のカスタム AnyConnect GUI ファイルを含めます。ファイルにはすべて適切に名前が付けられ、アイコン、およびロゴのサイズが適切に調整されていることを確認します。

ステップ 3 binary ディレクトリに、カスタム help_AnyConnect.html ファイルを含めます。

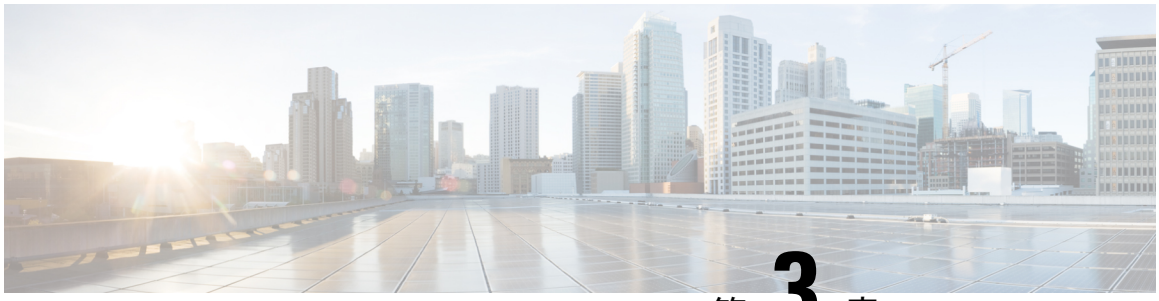
ステップ 4 binary ディレクトリに、VPN の OnConnect および OnDisconnect スクリプト、およびこれらが呼び出すその他のスクリプトを含めます。

ステップ 5 transform ディレクトリに、プラットフォーム固有のインストーラ トランスフォームを含めます。

ステップ 6 標準圧縮ユーティリティを使用して、このディレクトリ構造を AnyConnect-Customization-Bundle.zip などの適切な名前のファイルに ZIP 圧縮して、AnyConnect カスタマイゼーション バンドルを作成します。

次のタスク

AnyConnect カスタマイズバンドルを ISE にアップロードします。この ISE リソースは、ユーザーへの AnyConnect の展開に使用されます。



第 3 章

AnyConnect プロファイルエディタ

プロファイル エディタについて

AnyConnect Secure Mobility Client ソフトウェア パッケージには、すべてのオペレーティング システム用のプロファイル エディタが含まれています。AnyConnect イメージを Cisco Secure Firewall ASA にロードすると、ASDM はプロファイルエディタをアクティブにします。ローカルまたはフラッシュからクライアント プロファイルをアップロードできます。

複数の AnyConnect パッケージをロードした場合は、最新の AnyConnect パッケージからクライアントプロファイルエディタがアクティブにされます。これによりエディタには、旧バージョンのクライアントで使用される機能に加え、ロードされた最新の AnyConnect で使用される機能が表示されます。

Windows で動作するスタンドアロン プロファイル エディタもあります。

ASDM からの新しいプロファイルの追加

（注） クライアント プロファイルを作成する前に、まずクライアント イメージをアップロードする必要があります。

プロファイルが AnyConnect の一部としてエンドポイント上の管理者定義のエンドユーザー要件および認証ポリシーに展開され、これにより、エンドユーザーが事前設定済みのネットワークプロファイルを使用できるようになります。プロファイルエディターを使用して、1 つ以上のプロファイルを作成および構成します。AnyConnect には、ASDM の一部として、およびスタンドアロンの Windows プログラムとしてプロファイルエディタが含まれています。

新しいクライアント プロファイルを ASDM から Cisco Secure Firewall ASA に追加するには、次の手順を実行します。

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）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 プロファイル名を入力します。

ステップ 4 [プロファイルの使用（Profile Usage）] ドロップダウン リストから、プロファイルを作成するモジュールを選択します。

ステップ 5 （任意）[プロファイルの場所（Profile Location）] フィールドで [フラッシュの参照（Browse Flash）] をクリックし、Cisco Secure Firewall ASA の XML ファイルのデバイスファイルパスを選択します。

ステップ 6 （任意）スタンドアロン エディタを使用してプロファイルを作成した場合、[アップロード（Upload）] をクリックして、そのプロファイル定義を使用します。

ステップ 7 （任意）ドロップダウンリストから AnyConnect グループポリシーを選択します。

ステップ 8 [OK] をクリックします。

[AnyConnectVPNプロファイル（VPN Profile）]

AnyConnect Secure Mobility Client機能は、AnyConnect プロファイルで有効になっています。これらのプロファイルには、コアクライアント VPN 機能とオプション クライアント モジュール（Network Access Manager、ISE ポスチャ、Umbrella、Network Visibility Module、AMP、カスタマーエクスペリエンス フィードバックなど）の構成設定が含まれています。Cisco Secure Firewall ASA は AnyConnect のインストールおよび更新中にプロファイルを展開します。ユーザがプロファイルの管理や修正を行うことはできません。

Cisco Secure Firewall ASA または ISE は、すべての AnyConnect ユーザーにグローバルにプロファイルを展開するか、ユーザーのグループポリシーに基づいて展開するように設定できます。通常、ユーザーは、インストールされている AnyConnect モジュールごとに 1 つのプロファイルを持ちます。場合によっては、1 人のユーザーに複数の VPN プロファイルを提供することが必要になります。たとえば、複数の場所で働くユーザーなどの場合です。

一部のプロファイル設定は、ユーザのコンピュータ上のユーザ プリファレンス ファイルまたはグローバル プリファレンス ファイルにローカルに保存されます。ユーザーファイルには、クライアント GUI の [設定（Preferences）] タブにユーザー制御可能設定を AnyConnect で表示するうえで必要となる情報、およびユーザー、グループ、ホストなど、直近の接続に関する情報が保存されます。

グローバルファイルには、ユーザ制御可能設定に関する情報が保存されます。これにより、ログイン前でも（ユーザがいなくても）それらの設定を適用できます。たとえば、クライアントでは Start Before Login や起動時自動接続が有効になっているかどうかをログイン前に認識する必要があります。

AnyConnect プロファイルエディタ、プリファレンス（Part 1）

- [Start Before Loginを使用（Use Start Before Login）]：（Windows のみ）クライアントで使用するために Start Before Login を有効にします。[Start Before Loginを使用（Use Start Before Login）]が有効になっていると、Windows ログインダイアログボックスが表示される前に AnyConnect が起動します。ユーザは、Windows にログインする前に、VPN 接続を介してエンタープライズインフラストラクチャに接続します。認証後、ログインダイアログボックスが表示され、ユーザは通常どおりログインします。

- [事前接続メッセージの表示（Show Pre-connect Message）]：管理者は、ユーザーが初めて接続を試行する前にワンタイムメッセージを表示させることができます。たとえば、メッセージを表示して、ユーザにスマート カードをリーダに挿入するよう促すことができます。このメッセージは、AnyConnect メッセージカタログに表示され、ローカライズされています。

- [証明書ストア（Certificate Store）]：AnyConnect がどの証明書ストアで証明書を保存し、読み取るかを制御します。セキュア ゲートウェイは、適切に設定し、複数の証明書認証の組み合わせのうちどれが特定の VPN 接続で許容されるかをクライアントに指定する必要があります。

  VPN プロファイルの CertificateStore 設定の値は、セキュア ゲートウェイに許容される証明書のタイプによって異なります。証明書のタイプは、2 ユーザ証明書か、1 マシンおよび 1 ユーザ証明書のどちらかです。

  macOS 上で AnyConnect がアクセスできる証明書ストアをさらに絞りこめるようにするには、Windows 用または macOS 用のドロップダウンから証明書ストアを設定できます。macOS のための新しいプロファイル プリファレンスは CertificateStoreMac といい、次の追加された値をサポートします。

  - [すべて（All）]（Windows 用）：1 マシンおよび 1 ユーザ証明書が ASA 設定によって許容されます。
  - [ユーザ（User）]（Windows 用）：2 ユーザ証明書が ASA 設定によって許容されます。
  - [すべて（All）]（macOS 用）：利用可能なすべての macOS キーチェーンおよびファイル ストアからの証明書を使用します。
  - [システム（System）]（macOS 用）：macOS システム キーチェーンおよびシステム ファイル/PEM ストアからの証明書のみを使用します。
  - [ログイン（Log in）]（macOS 用）：ユーザ ファイル/PEM ストアに加え、macOS ログイン キーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。

- [証明書ストアの上書き（Certificate Store Override）]：管理者は、Windows マシン（ローカルシステム）証明書ストア内の証明書をクライアント証明書認証に使用するように AnyConnect に指示できます。証明書ストアの上書きは、デフォルトでは UI プロセスに

よって接続が開始される SSL にのみ適用されます。IPSec/IKEv2 を使用している場合、AnyConnect プロファイルのこの機能は適用されません。

（注） マシン証明書を使用して Windows に接続するには、このオプションが有効にされている事前展開されたプロファイルが必要です。接続する前に Windows デバイスにこのプロファイルが存在しない場合、証明書はマシン ストアにアクセスできず、接続は失敗します。

- True：AnyConnect は、Windows マシン証明書ストア内の証明書を検索します。CertificateStore を [すべて（all）] に設定する場合、CertificateStoreOverride は true に設定する必要があります。
- False：AnyConnect は、Windows マシン証明書ストア内の証明書を検索しません。

- AutomaticCertSelection：セキュア ゲートウェイで複数証明書の認証を設定するときは、この値を true に設定する必要があります。
- [起動時に自動接続（Auto Connect on Start）]：AnyConnect の起動時に、AnyConnect プロファイルで指定されたセキュア ゲートウェイまたはクライアントが最後に接続していたゲートウェイとの VPN 接続が自動的に確立されます。
- [接続時に最小化（Minimize On Connect）]：VPN 接続の確立後、AnyConnect GUI が最小化されます。
- [ローカル LAN アドレス（Local LAN Access）]：Cisco Secure Firewall ASA への VPN セッション中にリモートコンピュータへ接続したローカル LAN に対してユーザーが無制限にアクセスできるようになります。

（注） ローカル LAN アクセスを有効にすると、パブリック ネットワークからユーザ コンピュータを経由して、社内ネットワークにセキュリティの脆弱性が生じる可能性があります。代替手段として、セキュリティアプライアンス（バージョン 8.4(1) 以降）で、デフォルト グループ ポリシーに含まれている AnyConnect ローカル印刷ファイアウォールルールを使用した SSL クライアント ファイアウォールを展開するように設定することもできます。このファイアウォール ルールを有効にするには、このエディタ [プリファレンス（Part 2）（Preferences (Part 2)）] で、[自動 VPN ポリシー（Automatic VPN Policy）]、[常にオン（Always on）]、および [VPN の接続解除を許可（Allow VPN Disconnect）] も有効にする必要があります。

- [キャプティブポータル検出を無効にする（Disable Captive Portal Detection）]：AnyConnect が受信する証明書の共通名が、Cisco Secure Firewall ASA 名と一致しない場合、キャプティ

ブポータルが検出されます。この動作により、ユーザによる認証が促されます。自己署名証明書を使用する一部のユーザは、HTTP キャプティブ ポータルで保護されている企業リソースへの接続を有効にすることを望むことがあるため、[キャプティブポータル検出を無効にする（Disable Captive Portal Detection）] チェックボックスをオンにする必要があります。管理者は、このオプションをユーザが設定できるようにするかどうかを判断し、判断に基づいてチェックボックスをオンにすることもできます。ユーザーが設定できるようにした場合は、AnyConnect Secure Mobility Client UI の [プリファレンス（Preferences）] タブにチェックボックスが表示されます。

- [自動再接続（Auto Reconnect）]：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。[自動再接続（Auto Reconnect）] を無効にすると、接続解除の原因にかかわらず、再接続は試行されません。

（注） 自動再接続は、ユーザがクライアントの動作を制御するシナリオで使用します。この機能は、AlwaysOn ではサポートされません。

  - **自動再接続の動作**
    - Disconnect On Suspend：AnyConnect では、システムが一時停止すると VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
    - ReconnectAfterResume（デフォルト）：接続が解除された場合、AnyConnect により VPN 接続の再確立が試行されます。

- [自動更新（Auto Update）]：オンにすると、クライアントの自動アップデートが有効になります。[ユーザ制御可（User Controllable）] チェックボックスをオンにすると、クライアントのこの設定を無効にできます。
- [RSA セキュア ID 連携（RSA Secure ID Integration）]（Windows のみ）：ユーザが RSA とどのように対話するかを制御します。デフォルトでは、AnyConnect が RSA の適切な対話方法を決定します（自動設定：ソフトウェアトークンとハードウェアトークンの両方を受け入れます）。
- [Windows ログインの強制（Windows Logon Enforcement）]：Remote Desktop Protocol（RDP）セッションから VPN セッションを確立することを許可します。スプリットトンネリングはグループポリシーで設定する必要があります。VPN 接続を確立したユーザーがログオフすると、AnyConnect は VPN 確立を接続解除します。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。
  - [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）]：クライアント PC にリモート ログインしたユーザーが VPN 接続を確立した場合の AnyConnect の動作を決定します。設定可能な値は次のとおりです。
  - [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。

- [Linux ログインの適用（Linux Logon Enforcement）]：SSH セッションから VPN セッションを確立できます。グループポリシーにスプリットトンネリングを設定する必要があります。VPN 接続を確立したユーザーがログオフすると、AnyConnect は VPN 確立を接続解除します。接続がリモート ユーザによって確立されていた場合、そのリモート ユーザがログオフすると、VPN 接続は終了します。

- [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。

- [Linux VPN 確立（Linux VPN Establishment）]：SSH を使用してクライアント PC にログインしたユーザーが VPN 接続を確立した場合の AnyConnect の動作を決定します。設定可能な値は次のとおりです。
  - [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。
  - [リモート ユーザを許可（Allow Remote Users）]：リモート ユーザは VPN 接続を確立できます。

- **[スマートカードのピンのクリア（Clear SmartCard PIN）]**

- [サポートされているIPプロトコル（IP Protocol Supported）]：IPv4 アドレスおよび IPv6 アドレスの両方で AnyConnect を使用して Cisco Secure Firewall ASA に接続しようとしているクライアントの場合、AnyConnect は接続の開始に際してどの IP プロトコルを使用するか

決定する必要があります。デフォルトで、AnyConnect は最初に IPv4 を使用して接続しようとします。接続が成功しない場合、AnyConnect は IPv6 を使用して接続を開始しようとします。

このフィールドでは、最初の IP プロトコルとフォールバックの順序を設定します。

- [IPv4]：Cisco Secure Firewall ASA に対して IPv4 接続のみ可能です。
- [IPv6]：Cisco Secure Firewall ASA に対して IPv6 接続のみを確立できます。
- [IPv4、IPv6]：最初に Cisco Secure Firewall ASA に IPv4 接続しようとします。クライアントが IPv4 を使用して接続できない場合、IPv6 接続をしようとします。
- [IPv6、IPv4]：最初に Cisco Secure Firewall ASA に IPv6 接続しようとします。クライアントが IPv6 を使用して接続できない場合、IPv4 接続をしようとします。

（注） IP プロトコルのフェールオーバーも VPN セッション中に行うことができます。フェールオーバーは、VPN セッションの前に実行された場合でも VPN セッション中に実行された場合でも、現在使用されているセキュアゲートウェイの IP アドレスに到達できなくなるまで維持されます。クライアントは、現在使用されている IP アドレスに到達できない場合、代替 IP プロトコル（利用可能な場合）に一致する IP アドレスにフェールオーバーします。

AnyConnect プロファイルエディタ、プリファレンス（Part 2）

- [自動証明書選択の無効化（Disable Automatic Certificate Selection）]（Windows のみ）：クライアントによる自動証明書選択を無効にし、ユーザに対して認証証明書を選択するためのプロンプトを表示します。

  関連項目：証明書選択の設定

- [プロキシ設定（Proxy Settings）]：プロキシサーバーへのクライアントアクセスを制御するために AnyConnect プロファイルにポリシーを指定します。これは、プロキシ設定によってユーザが社内ネットワークの外からトンネルを確立できない場合に使用します。
  - [ネイティブ（Native）]：クライアントは、AnyConnect によって以前に設定されたプロキシ設定とブラウザに設定されたプロキシ設定の両方を使用します。グローバルユーザプリファレンスに設定されたプロキシ設定は、ブラウザのプロキシ設定に追加されます。
  - [プロキシを無視（IgnoreProxy）]：ユーザのコンピュータのブラウザのプロキシ設定を無視します。
  - [上書き（Override）]：パブリック プロキシサーバーのアドレスを手動で設定します。パブリック プロキシは、Linux でサポートされている唯一のプロキシです。Windows

も、パブリック プロキシをサポートしています。[ユーザ制御可（User Controllable）] になるようにパブリック プロキシ アドレスを設定できます。

- [ローカルプロキシ接続を許可（Allow Local Proxy Connections）]：デフォルトでは、Windows ユーザーは AnyConnect でローカル PC 上のトランスペアレントまたは非トランスペアレントのプロキシサービスを介して VPN セッションを確立するようになっています。ローカルプロキシ接続のサポートを無効にする場合は、このパラメータをオフにします。トランスペアレントプロキシサービスを提供する要素の例として、一部のワイヤレスデータカードによって提供されるアクセラレーション ソフトウェアや、一部のウイルス対策ソフトウェアに備えられたネットワークコンポーネントなどがあります。

- [最適なゲートウェイの選択を有効化（Enable Optimal Gateway Selection）]（OGS）、（IPv4 クライアントのみ）：AnyConnect では、ラウンドトリップ時間（RTT）に基づいて接続または再接続に最適なセキュアゲートウェイが特定され、それが選択されます。これにより、ユーザーが介入することなくインターネットトラフィックの遅延を最小限に抑えることができます。OGS はセキュリティ機能ではなく、セキュア ゲートウェイ クラスタ間またはクラスタ内部でのロード バランシングは実行されません。OGS のアクティブ化/非アクティブ化を制御し、エンドユーザがこの機能そのものを制御できるようにするかどうかを指定します。クライアント GUI の [接続（Connection）] タブにある [接続先（Connect To）] ドロップダウン リストには [自動選択（Automatic Selection）] が表示されます。

  - [一時停止時間しきい値（時間）（Suspension Time Threshold (hours)）]：新しいゲートウェイ選択の計算を呼び出す前に VPN を一時停止しておく必要がある最小時間を（時間単位で）入力します。次の設定可能パラメータ（パフォーマンス向上しきい値（Performance Improvement Threshold））と組み合わせてこの値を最適化することで、最適なゲートウェイの選択と、クレデンシャルの再入力を強制する回数の削減の間の適切なバランスを見つけることができます。

  - [パフォーマンス向上しきい値（%）（Performance Improvement Threshold (%)）]：システムの再開後にクライアントが別のセキュア ゲートウェイに再接続する際の基準となるパフォーマンス向上率。特定のネットワークに対してこれらの値を調整すれば、最適なゲートウェイを選択することと、クレデンシャルを強制的に入力させる回数を減らすこととの間で適切なバランスを取ることができます。デフォルトは 20% です。

  OGS が有効な場合は、この機能の設定をユーザが行えるようにすることも推奨します。

  OGS には次の制約事項があります。

  - Always-On を設定した状態では動作できません
  - 自動プロキシ検出を設定した状態では動作できません。
  - プロキシ自動設定（PAC）ファイルを設定した状態では動作できません。
  - AAA が使用されている場合は、別のセキュア ゲートウェイへの遷移時にユーザがそれぞれのクレデンシャルを再入力しなければならないことがあります。この問題は、証明書を使用すると解消されます。

- [自動 VPN ポリシー（Automatic VPN Policy）]（Windows および macOS のみ）：信頼ネットワーク検出を有効にして、AnyConnectが信頼ネットワークポリシーと非信頼ネットワークポリシーに従って VPN 接続をいつ開始または停止するかを自動的に管理できるようにします。無効の場合、VPN 接続の開始および停止は手動でのみ行うことができます。[自動 VPN ポリシー（Automatic VPN Policy）] を設定しても、ユーザは VPN 接続を手動で制御できます。
  - [信頼されたネットワークポリシー（Trusted Network Policy）]：ユーザーが社内ネットワーク（信頼ネットワーク）に存在する場合に AnyConnect が VPN 接続で自動的に実行するアクション。
    - [接続解除（Disconnect）]（デフォルト）：信頼ネットワークが検出されると VPN 接続が解除されます。
    - [接続（Connect）]：信頼ネットワークが検出されると VPN 接続が開始されます。
    - [何もしない（Do Nothing）]：非信頼ネットワークでは動作はありません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。
    - [一時停止（Pause）]：ユーザーが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は VPN セッションを接続解除するのではなく、一時停止します。ユーザーが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。
  - **[信頼されていないネットワークポリシー（Untrusted Network Policy）]**：ユーザーが企業ネットワークの外（非信頼ネットワーク）に存在する場合、AnyConnect により VPN接続が自動的に開始されます。この機能を使用すると、ユーザが信頼ネットワークの外にいるときに VPN 接続を開始することによって、セキュリティ意識を高めることができます。
    - [接続（Connect）]（デフォルト）：非信頼ネットワークが検出されると、VPN接続が開始されます。
    - [何もしない（Do Nothing）]：信頼ネットワークでは動作はありません。このオプションを指定すると、 Always-OnVPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。
  - [信頼された DNS ドメイン（Trusted DNS Domains）]：クライアントが信頼ネットワーク内に存在する場合にネットワークインターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）。*.cisco.com などがこれに該当します。DNS サフィックスでは、ワイルドカード（*）がサポートされます。

（注） Network Visibility Module を使用している場合、信頼できる DNS ドメインとサーバーはサポートされません。これは、Network Visibility Module が管理者定義の信頼できるサーバーと証明書ハッシュを使用して、ユーザーが信頼できるネットワーク上にあるかどうかを判断するためです。

- [信頼された DNS サーバー（Trusted DNS Servers）]：クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サーバーアドレス（カンマ区切りの IP アドレス）。たとえば、192.168.1.2, 2001:DB8::1 です。IPv4 または IPv6 DNS サーバーアドレスでは、ワイルドカード（*）がサポートされています。

- **Trusted Servers @ https://<server>[:<port>]**：信頼できる URL として追加するホスト URL。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

  信頼できる証明書を使用してアクセス可能なセキュア Web サーバーが、信頼できるサーバーとして見なされる必要があります。Secure TND は、リスト内の最初に設定されたサーバーへの接続を試行します。サーバーに接続できない場合、セキュア TND は設定済みリスト内の次のサーバーへの接続を試行します。サーバーに接続できても、証明書のハッシュが一致しない場合、ネットワークは「信頼できない」と識別されます。他のサーバーは評価されません。ハッシュが信頼できる場合、「信頼できる」基準が満たされます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバーを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバーが定義されていない場合、このフィールドは無効になります。

- [常時接続（Always On）]：対応している Windows または macOS オペレーティングシステムのいずれかを実行しているコンピュータにユーザーがログインした場合、AnyConnect が VPN へ自動的に接続するかどうかを判断します。コンピュータが信頼ネットワーク内に存在しない場合にはインターネット リソースへのアクセスを制限することによってセキュリティ上の脅威からコンピュータを保護するという企業ポリシーを適用できます。グループ ポリシーおよびダイナミック アクセス ポリシーに Always-On VPN パラメータを設定し、ポリシーの割り当てに使用される一致基準に基づいて例外を指定することにより、この設定を上書きすることもできます。AnyConnect ポリシーでは Always-On が有効になっているが、ダイナミック アクセス ポリシーまたはグループポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループポリシーが基準と一致すれば、クラ

イアントでは現在以降の VPN セッションに対して無効の設定が保持されます。有効にした後に、追加のパラメータを設定できます。

（注） AlwaysOn は、ユーザによる設定なしで接続が確立し冗長性が動作するシナリオで使用します。そのため、この機能を使用しているときは、[プリファレンス,パート 1（Preferences, part 1）] で自動再接続を有効に設定する必要はありません。

関連項目：Always-Onを使用した VPN 接続の必要性

- [VPNの接続解除を許可（Allow VPN Disconnect）]：AnyConnect で Always-On VPN セッション用の [接続解除（Disconnect）] ボタンが表示されるようにするかどうかを指定します。VPN セッションの中断後に現在の VPN セッションまたは再接続で問題が発生し、パフォーマンスが低下したなどの理由により、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

  [接続解除（Disconnect）]ボタンを使用すると、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。上述した理由により、[接続解除（Disconnect）] ボタンを無効にすると、VPN アクセスが妨害または阻止されることがあります。

- [VPNの切断時に次のホストへのアクセスを許可（Allow Access to the Following Hosts with VPN Disconnected）]：[常にオン（Always On）] の間に VPN が切断されたときに、設定されたホストにエンドポイントがアクセスできるようにします。値は、IP アドレス、IP アドレス範囲（CIDR 形式）、または FQDN を指定できるホストのカンマ区切りリストです。最大 500 のホストを指定できます。ワイルドカードは使用できません。

  警告：指定された FQDN へのアクセスは、信頼できないネットワークで実行される名前解決に依存します。

- [接続エラーポリシー（Connect Failure Policy）]：AnyConnect が VPN セッションを確立できない場合（到達不能の場合など）に、コンピュータがインターネットにアクセスできるようにするかどうかを指定します。このパラメータは、[Always-On] および [VPN の接続解除を許可（Allow VPN Disconnect）] が有効の場合にだけ適用されます。[Always-On] を選択した場合、フェールオープン ポリシーはネットワーク接続を許可し、フェールクローズポリシーはネットワーク接続を無効にします。

  - [クローズド（Closed）]：VPN が到達不能の場合にネットワーク アクセスを制限します。この設定の目的は、エンドポイントを保護するプライベートネットワーク内のリソースが使用できない場合に、企業の資産をネットワークに対する脅威から保護することにあります。

- [オープン（Open）]：VPN が到達不能の場合でもネットワーク アクセスを許可します。

注意 AnyConnect が VPN セッションの確立に失敗した場合は、接続障害クローズドポリシーによりネットワークアクセスは制限されます。このポリシーは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する非常にセキュリティの高い組織向きです。このポリシーでは、スプリットトンネリングによって許可され、ACL によって制限されたすべてのプリンタやテザードデバイスなどのローカル リソース以外のネットワーク アクセスを防止します。ユーザーが VPN を越えてインターネットにアクセスする必要がある場合に、セキュアゲートウェイを利用できないときには、このポリシーを適用すると生産性が低下する可能性があります。AnyConnect はほとんどのキャプティブポータルを検出します。キャプティブポータルを検出できない場合、接続障害クローズド ポリシーによりすべてのネットワーク接続が制限されます。

クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープンポリシーを使用して Always-On VPN を展開し、ユーザーを通じて AnyConnect がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズドポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

関連項目：キャプティブ ポータルについて

[接続エラー ポリシー（Connect Failure Policy）] が [クローズド（Closed）] である場合、次の設定を行うことができます。

- [キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]：クライアントによりキャプティブポータル（ホットスポット）が検出された場合、クローズ接続障害ポリシーにより適用されるネットワークアクセスの制限が AnyConnect により解除されます。ホテルや空港では、ユーザがブラウザを開いてインターネットアクセスの許可に必要な条件を満たすことができるようにするため、キャプティブ ポータルを使用するのが一般的です。デフォルトの場合、このパラメータはオフになっており、セキュリティは最高度に設定されます。ただし、クライアントから VPN へ接続する必要があるにもかかわらず、キャプティブ ポータルによりそれが制限されている場合は、このパラメータをオンにする必要があります。

- [修復タイムアウト（Remediation Timeout）]： AnyConnect によりネットワークアクセスの制限が解除されるまでの時間（分）。このパラメータは、[キャプティブポータルの修復を許可（Allow Captive Portal Remediation）]パラメータがオンになっており、かつクライアントによりキャプティブポータルが検出された場合に適用されます。キャプティブポータルの通常の要求を満たすことができるだけの十分な時間を指定します（5 分など）。
- [最新のVPNローカルリソースルールを適用（Apply Last VPN Local Resource Rules）]：VPN が到達不能の場合、クライアントでは Cisco Secure Firewall ASA から受信した最後のクライアント ファイアウォールが適用されます。この中には、ローカル LAN 上のリソースへのアクセスを許可する ACL が含まれている場合もあります。

関連項目：接続障害ポリシーの設定

- [キャプティブポータルの修復ブラウザのフェールオーバー（Captive Portal Remediation Browser Failover）]：エンドユーザーが（AnyConnect ブラウザを閉じた後）キャプティブポータルの修復に外部ブラウザを使用できるようにします。

  追加情報については、「キャプティブ ポータル ホットスポットの検出と修復の使用 （149 ページ）」を参照してください。

- [手動でのホスト入力を許可する（Allow Manual Host Input）]：ユーザーが、AnyConnect UI のドロップダウン ボックスにリストされていない VPN アドレスを入力できるようにします。このチェックボックスをオフにすると、VPN 接続の選択項目は、ドロップダウン ボックスに表示されているものに限定され、ユーザによる新しい VPN アドレスの入力が制限されます。

- [PPP 除外（PPP Exclusion）]：PPP 接続上の VPN トンネルの場合、除外ルートを決定するかどうかとその方法を指定します。クライアントでは、セキュア ゲートウェイより先を宛先としてトンネリングされたトラフィックから、このセキュア ゲートウェイを宛先とするトラフィックを除外できます。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。この機能をユーザ設定可能にした場合、ユーザは PPP 除外設定の読み取りや変更を行うことができます。

  - [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバーの IP アドレスを自動的に決定します。
  - [オーバーライド（Override）]：[PPP除外サーバーIP（PPP Exclusion Server IP）]フィールドで指定された定義済みのサーバー IP アドレスを使用して PPP 除外を有効にします。[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドは、このオーバーライド方式にのみ適用され、[自動（Automatic）] オプションで PPP サーバーの IP アドレスを検出できない場合にのみ使用する必要があります。

    [PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで [ユーザ制御可（User Controllable）] をオンにすると、エンドユーザーは preferences.xml ファイルを使用して IP アドレスを手動で更新できます。「ユーザに対する PPP 除外上書きの指示 （153 ページ）」セクションを参照してください。

- [無効（Disabled）]：PPP 除外は適用されません。

- [スクリプトの有効化（Enable Scripting）]：OnConnect スクリプトおよび OnDisconnect スクリプトがセキュリティ アプライアンスのフラッシュ メモリに存在する場合はそれらを起動します。
  - [次のイベント時にスクリプトを終了する（Terminate Script On Next Event）]：スクリプト処理可能な別のイベントへの遷移が発生した場合に、実行中のスクリプトプロセスを終了します。たとえば、VPN セッションが終了すると、AnyConnect では実行中の OnConnect スクリプトが終了し、クライアントで新しい VPN セッションが開始すると、実行中の OnDisconnect スクリプトが終了します。Microsoft Windows 上のクライアントでは OnConnect スクリプトまたは OnDisconnect スクリプトによって起動した任意のスクリプト、およびその従属スクリプトもすべて終了します。macOS および Linux 上のクライアントでは、OnConnect スクリプトまたは OnDisconnect スクリプトのみ終了し、子スクリプトは終了しません。
  - [Post SBL OnConnect スクリプトを有効にする（Enable Post SBL On Connect Script）]：SBL で VPN セッションが確立された場合に OnConnect スクリプトが（存在すれば）起動されるようにします（VPN エンドポイントで Microsoft Windows を実行している場合にのみサポート）。

- [ログオフ時にVPNを保持（Retain VPN On Logoff）]：ユーザが Windows または macOS からログオフした場合に、VPN セッションを維持するかどうかを指定します。
  - [ユーザの強制設定（User Enforcement）]：別のユーザがログインした場合に VPN セッションを終了するかどうかを指定します。このパラメータが適用されるのは、[ログオフ時にVPNを保持（Retain VPN On Logoff）] がオンになっており、かつ VPN セッションが確立されている間に元のユーザが Windows または macOS からログオフした場合のみです。

- [認証タイムアウト値（Authentication Timeout Values）]：デフォルトでは、AnyConnect は接続試行を終了するまでに、セキュアゲートウェイからの認証を最大 30 秒間待ちます。その時間が経過すると、認証がタイムアウトになったことを示すメッセージが AnyConnect に表示されます。10 ～ 120 の範囲で秒数を入力します。

AnyConnect プロファイルエディタのバックアップサーバー

ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップサーバのリストを設定できます。ユーザが選択したサーバで障害が発生した場合、クライアントはリストの先頭にある最適なサーバのバックアップに接続しようとします。それが失敗した場合、クライアントは選択結果の順序に従って [最適なゲートウェイの選択（Optimal Gateway Selection）] リストの残りの各サーバを試します。

（注） ここで設定するバックアップ サーバは、「AnyConnect プロファイルエディタのサーバーリストの追加/編集 （113 ページ）」でバックアップ サーバが定義されていないときに**のみ**、試行されます。サーバのリストで設定されるサーバが優先され、ここにリストされているバックアップ サーバは上書きされます。

[ホスト アドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたは完全修飾ドメイン名（FQDN）を指定します。

- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

AnyConnect プロファイルエディタの証明書照合

このペインでは、クライアント証明書の自動選択の詳細設定に使用できるさまざまな属性の定義を有効にします。

証明書一致基準を指定しない場合、AnyConnect は、次の証明書照合ルールを適用します。

- キーの使用状況：Digital_Signature
- 拡張キーの使用状況：Client Auth

仕様に一致する任意の条件がプロファイルで作成される場合、プロファイルに明記されない限り、上記一致ルールのいずれも適用されません。

- [キーの使用状況（Key Usage）]：受け入れ可能なクライアント証明書を選択する場合は、次のような証明書キー属性を使用できます。
  - Decipher_Only：データを復号化します。他のビットは設定されません（Key_Agreement は除く）。
  - Encipher_Only：データを暗号化します。他のビットは設定されません（Key_Agreement は除く）。
  - CRL_Sign：CRL の CA 署名を確認します。
  - Key_Cert_Sign：証明書の CA 署名を確認します。
  - Key_Agreement：キー共有。

- Data_Encipherment：Key_Encipherment 以外のデータを暗号化します。
- Key_Encipherment：キーを暗号化します。
- Non_Repudiation：一部のアクションを誤って拒否しないように、Key_Cert_sign および CRL_Sign 以外のデジタル署名を確認します。
- Digital_Signature：Non_Repudiation、Key_Cert_Sign、および CRL_Sign 以外のデジタル署名を確認します。

- [拡張キーの使用状況（Extended Key Usage）]：次の拡張キーの使用状況設定を使用します。OID は丸カッコ内に記載してあります。
  - ServerAuth（1.3.6.1.5.5.7.3.1）
  - ClientAuth（1.3.6.1.5.5.7.3.2）
  - CodeSign（1.3.6.1.5.5.7.3.3）
  - EmailProtect（1.3.6.1.5.5.7.3.4）
  - IPSecEndSystem（1.3.6.1.5.5.7.3.5）
  - IPSecTunnel（1.3.6.1.5.5.7.3.6）
  - IPSecUser（1.3.6.1.5.5.7.3.7）
  - TimeStamp（1.3.6.1.5.5.7.3.8）
  - OCSPSign（1.3.6.1.5.5.7.3.9）
  - DVCS（1.3.6.1.5.5.7.3.10）
  - IKE Intermediate

- [カスタム拡張照合キー（最大 10）（Custom Extended Match Key (Max 10)）]：カスタム拡張照合キー（もしあれば）を指定します（最大 10 個）。証明書は入力したすべての指定キーに一致する必要があります。OID 形式でキーを入力します（1.3.6.1.5.5.7.3.11 など）。

（注） カスタム拡張照合キーを 30 文字を超える OID サイズで作成すると、[OK] ボタンのクリック時に拒否されます。OID の最大文字数は、30 文字です。

- [拡張キーの使用状況が設定されている証明書のみを適合（Match only certificates with Extended key usage）]：以前の動作では、証明書識別名（DN）の照合ルールが設定されると、クライアントは特定の EKU OID が設定されている証明書と、EKU が設定されていないすべての証明書とを適合させていました。一貫性を保ちながら、より明確にするため、EKU が設定されていない証明書との適合を拒否できます。デフォルトでは、お客様が予想してい

る従来の動作が保持されます。新しい動作を有効にし、適合を拒否するには、チェックボックスをオンにする必要があります。

- [識別名（最大 10）（Distinguished Name (Max 10)）]：受け入れ可能なクライアント証明書を選択する際に完全一致基準として使用する識別名（DN）を指定します。
  - [名前（Name）]：照合に使用する識別名（DN）。
    - CN：サブジェクトの一般名
    - C：サブジェクトの国
    - DC：ドメイン コンポーネント
    - DNQ：サブジェクトの DN 修飾子
    - EA：サブジェクトの電子メール アドレス
    - GENQ：サブジェクトの GEN 修飾子
    - GN：サブジェクトの名
    - I：サブジェクトのイニシャル
    - L：サブジェクトの都市
    - N：サブジェクトの非構造体名
    - O：サブジェクトの会社
    - OU：サブジェクトの部署
    - SN：サブジェクトの姓
    - SP：サブジェクトの州
    - ST：サブジェクトの州
    - T：サブジェクトの敬称
    - ISSUER-CN：発行元の一般名
    - ISSUER-DC：発行元のコンポーネント
    - ISSUER-SN：発行元の姓
    - ISSUER-GN：発行元の名
    - ISSUER-N：発行元の非構造体名
    - ISSUER-I：発行元のイニシャル
    - ISSUER-GENQ：発行元の GEN 修飾子
    - ISSUER-DNQ：発行元の DN 修飾子
    - ISSUER-C：発行元の国

- ISSUER-L：発行元の都市
- ISSUER-SP：発行元の州
- ISSUER-ST：発行元の州
- ISSUER-O：発行元の会社
- ISSUER-OU：発行元の部署
- ISSUER-T：発行元の敬称
- ISSUER-EA：発行元の電子メール アドレス

- [パターン（Pattern）]：照合する文字列を指定します。 照合するパターンには、目的の文字列部分のみ含まれている必要があります。パターン照合構文や正規表現構文を入力する必要はありません。入力した場合、その構文は検索対象の文字列の一部と見なされます。

  abc.cisco.com という文字列を例とした場合、cisco.com で照合するためには、入力するパターンを cisco.com とする必要があります。

- [演算子（Operator）]：この DN で照合する場合に使用する演算子です。
  - [等しい（Equal）]：== と同等
  - [等しくない（Not Equal）]：!= と同等

- [ワイルドカード（Wildcard）]：[有効（Enabled）] を指定するとワイルドカード パターン照合が含まれます。ワイルドカードが有効であれば、パターンは文字列内のどの場所でも使用できます。
- [大文字と小文字を区別（Match Case）]：大文字と小文字を区別したパターン照合を有効にする場合はオンにします。

関連トピック

証明書照合の設定 （195 ページ）

AnyConnect プロファイルエディタの [証明書の登録（Certificate Enrollment）]

[証明書の登録（Certificate Enrollment）]によって、AnyConnect がクライアント認証に使用する証明書のプロビジョニングおよび更新を行う場合に、Simple Certificate Enrollment Protocol（SCEP）を使用できるようにします。

- [証明書失効しきい値（Certificate Expiration Threshold）]：AnyConnect が、証明書の有効期限の何日前にユーザーに対して証明書の失効が近づいていることを警告する日数（RADIUS パスワード管理ではサポートされません）。デフォルトは 0（警告は表示しない）です。値の範囲は 0 ～ 180 日です。

- **macOS**
- ユーザログインキーチェーンのみに登録証明書をインポートできます。
- **モバイルプラットフォーム**
- アプリケーション サンドボックスのみに登録証明書をインポートできます。
- [証明書インポート ストア（Certificate Import Store）]：どの Windows 証明書ストアに登録証明書を保存するかを選択します。
- [証明書の内容（Certificate Contents）]：SCEP 登録要求に含める証明書の内容を指定します。
  - Name (CN)：証明書での一般名。
  - Department (OU)：証明書に指定されている部署名。
  - Company (O)：証明書に指定されている会社名。
  - State (ST)：証明書に指定されている州 ID。
  - State (SP)：別の州 ID。
  - Country (C)：証明書に指定されている国 ID。
  - Email (EA)：電子メール アドレス。次の例では、Email (EA) は %USER%@cisco.com です。%USER% は、ユーザの ASA ユーザ名ログイン クレデンシャルに対応します。
  - Domain (DC)：ドメイン コンポーネント。次の例では、Domain (DC) は cisco.com に設定されています。
  - SurName (SN)：姓または名。
  - GivenName (GN)：通常は名。
  - UnstructName (N)：定義されていない名前。
  - Initials (I)：ユーザのイニシャル。
  - Qualifier (GEN)：ユーザの世代修飾子。たとえば、「Jr.」や「III」です。
  - Qualifier (DN)：完全 DN の修飾子。
  - City (L)：都市 ID。
  - Title (T)：個人の敬称。たとえば、Ms.、Mrs.、Mr. など。
  - CA Domain：SCEP 登録に使用されます。通常は CA ドメイン。
  - Key size：登録する証明書用に生成された RSA キーのサイズ。
- [証明書取得ボタンを表示（Display Get Certificate Button）]：次の条件下で AnyConnect GUI が [証明書を取得（Get Certificate）] ボタンを表示できるようにします。

- 証明書は [証明書失効しきい値（Certificate Expiration Threshold）] で定義された期間内に期限が切れるよう設定されている（RADIUS ではサポートされません）。
- 証明書の期限が切れています。
- 証明書が存在しません。
- 証明書を照合できません。

関連トピック

証明書登録の設定 （184 ページ）

AnyConnect プロファイルエディタの証明書ピン

前提条件

証明書のピン留めを開始する前のベストプラクティスについては、「証明書のピン留めについて （206 ページ）」を参照してください。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定には、VPN プロファイルエディタを使用します。[グローバルピン（Global Pins）] セクション内のプリファレンスが有効になっている場合は、サーバーリスト内のホストごとの証明書のみピン留めできます。プリファレンスを有効にすると、クライアントが証明書ピン検証に使用するグローバルピンのリストを設定できます。[サーバーリスト（Server List）] セクションでのホストごとのピンの追加は、グローバルピンの追加と同様です。証明書チェーン内の任意の証明書をピン留めでき、証明書は、ピン留めのために必要な情報を計算するため、プロファイルエディタにインポートされます。

[ピンを追加（Add Pin）]：証明書のプロファイルエディタへのインポートおよびピン留めを手引きする証明書ピン留めウィザードが開始します。

ウィンドウの [証明書の詳細（Certificate Details）] 部分では、[件名（Subject）] 列および [発行元（Issuer）] 列を視覚的に確認することができます。

証明書ピン留めウィザード

ピン留めに必要な情報を指定するため、サーバ証明書チェーンからの任意の証明書をプロファイル エディタにインポートすることができます。プロファイル エディタは、次の 3 つの証明書インポート オプションをサポートしています。

- ローカルのファイルを参照：お使いのコンピュータにローカルに存在している証明書を選択します。
- URL からファイルをダウンロード：任意のファイル ホスティング サーバから証明書をダウンロードします。
- PEM 形式の情報をペースト：証明書の開始および終了ヘッダーを含む PEM 形式の情報を挿入します。

（注） インポートできるのは、データ形式が DER、PEM、および PKCS7 の証明書のみです。

AnyConnect プロファイル エディタのモバイル ポリシー

AnyConnect のバージョン 3.0 以降では、Windows Mobile デバイスをサポートしません。Windows Mobile デバイスに関する情報は、『Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 2.5』を参照してください。

AnyConnect プロファイルエディタのサーバーリスト

クライアント GUI に表示されるサーバ リストの設定を行うことができます。ユーザは、VPN 接続を確立する際、このリストでサーバを選択することができます。

[サーバ リスト（Server List）] テーブルの列は次のとおりです。

- [ホスト名（Hostname）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアス。
- [ホスト アドレス（Host Address）]：サーバの IP アドレスまたは FQDN。
- [ユーザ グループ（User Group）]：[ホスト アドレス（Host Address）] と組み合わせて使用することによりグループ ベースの URL が構成されます。
- [自動 SCEP ホスト（Automatic SCEP Host）]：クライアント認証に使用する証明書のプロビジョニング用および更新用として指定された Simple Certificate Enrollment Protocol。
- [CA URL]：このサーバが認証局（CA）へ接続する際に使用する URL。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「AnyConnect プロファイルエディタの証明書ピン （111 ページ）」を参照してください。

（注） クライアントは、ピン検証の際に、グローバル ピンおよび対応するホストごとのピンを使用します。ホストごとのピンの設定は、証明書ピン留めウィザードの使用によるグローバル ピンの設定と同様に行います。

[追加/編集（Add/Edit）]：上記のサーバのパラメータを指定できる [サーバ リスト エントリ（Server List Entry）] ダイアログを起動します。

[削除（Delete）]：サーバ リストからサーバを削除します。

[詳細（Details）]：サーバのバックアップ サーバまたは CA URL に関する詳細情報を表示します。

関連トピック

VPN 接続サーバーの設定 （131 ページ）

AnyConnect プロファイルエディタのサーバーリストの追加/編集

- [ホスト表示名（Host Display Name）]：ホスト、IP アドレス、または完全修飾ドメイン名（FQDN）を参照する際に使用するエイリアスを入力します。
- [FQDN または IP アドレス（FQDN or IP Address）]：サーバの IP アドレスまたは FQDN を指定します。
  - [ホストアドレス（Host Address）] フィールドに IP アドレスまたは FQDN を指定すると、[ホスト名（Host Name）] フィールドのエントリが AnyConnect トレイフライアウト内の接続ドロップダウンリストに表示されるサーバーのラベルになります。
  - [ホスト名（Hostname）] フィールドで FQDN のみを指定し、[ホスト アドレス（Host Address）] フィールドでは IP アドレスを指定しない場合、[ホスト名（Hostname）] フィールドの FQDN が DNS サーバによって解決されます。
  - IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。
- [ユーザ グループ（User Group）]：ユーザ グループを指定します。

  このユーザ グループとホストアドレスを組み合わせてグループ ベースの URL が構成されます。プライマリ プロトコルを IPsec として指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url。

（注） IKEv2/IPsec 接続では、プライマリサーバに到達できない場合、プライマリサーバに入力された**ユーザグループ**情報がバックアップサーバに転送されます。SSL で同じ動作をさせるには、FQDN だけでなく、ユーザグループ情報を URL（https://example.com/usergroup など）としてバックアップサーバに提供する必要もあります。

- [モバイル専用追加設定（Additional mobile-only settings）]：Apple iOS および Android モバイル デバイスを設定する場合に選択します。
- **バックアップ サーバ リスト**

  ユーザが選択したサーバで障害が発生した場合にクライアントが使用するバックアップ サーバのリストを設定することをお勧めします。サーバで障害が発生した場合、クライアントではまずリストの先頭にあるサーバに対して接続が試行され、必要に応じてリストの下方向に移動します。

（注） 逆の面から述べれば、「AnyConnectプロファイルエディタのバックアップサーバー（105ページ）」で設定されるバックアップサーバは、すべての接続エントリのグローバル項目です。プロファイルエディタのバックアップサーバに入力したエントリは、ここで、個々のサーバリストエントリとしてバックアップサーバリストに入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

- [ホストアドレス（Host Address）]：バックアップ サーバ リストに表示する IP アドレスまたはFQDNを指定します。クライアントでは、ホストに接続できない場合には、バックアップ サーバへの接続が試行されます。
- [追加（Add）]：バックアップ サーバ リストにホスト アドレスを追加します。
- [上に移動（Move Up）]：選択したバックアップ サーバをリストの上方向に移動します。ユーザが選択したサーバで障害が発生した場合、クライアントではまずリストの先頭にあるバックアップ サーバに対して接続が試行され、必要に応じてリストの下方向に移動します。
- [下に移動（Move Down）]：選択したバックアップ サーバをリストの下方向に移動します。
- [削除（Delete）]：サーバ リストからバックアップ サーバを削除します。

- **ロード バランシング サーバ リスト**

  このサーバ リスト エントリのホストがセキュリティ アプライアンスのロード バランシング クラスタであり、かつAlways-On機能が有効になっている場合は、このリストでクラスタのバックアップ デバイスを指定します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスはAlways-On機能によりブロックされます。

  - [ホスト アドレス（Host Address）]：ロードバランシング クラスタにあるバックアップ デバイスの IP アドレスまたは FQDN を指定します。
  - [追加（Add）]：ロード バランシング バックアップ サーバ リストにアドレスを追加します。
  - [削除（Delete）]：ロード バランシング バックアップ サーバをリストから削除します。

- [プライマリ プロトコル（Primary Protocol）]：このサーバも接続するプロトコル（SSL または IKEv2 を使用した IPsec）を指定します。デフォルトは SSL です。
  - [標準認証のみ（IOS ゲートウェイ）（Standard Authentication Only (IOS Gateways)）]：プロトコルとして IPsec を選択した場合、このオプションを選択して、IOS サーバへの接続の認証方式を制限できます。

（注） このサーバーが Cisco Secure Firewall ASA である場合、認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、Cisco Secure Firewall ASA でセッションタイムアウト、アイドルタイムアウト、接続解除タイムアウト、スプリットトンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

- [IKE ネゴシエーション中の認証方式（Auth Method During IKE Negotiation）]：標準ベースの認証方式の 1 つを選択します。
  - [IKE ID（IKE Identity）]：標準ベースの EAP 認証方式を選択した場合、このフィールドにグループまたはドメインをクライアントアイデンティティとして入力できます。クライアントは、文字列を ID_GROUP タイプ IDi ペイロードとして送信します。デフォルトでは、文字列は *$AnyConnectClient$* です。

- [CA URL]：SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。
- [証明書ピン（Certificate Pins）]：ピン検証の際にクライアントによって使用されるホストごとのピン。「AnyConnect プロファイルエディタの証明書ピン （111 ページ）」を参照してください。
- [チャレンジ PW のプロンプト（Prompt For Challenge PW）]：有効にすると、証明書をユーザが手動で要求できるようになります。 ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。
- [CA サムプリント（CA Thumbprint）]：CA の証明書サムプリント。SHA1 ハッシュまたは MD5 ハッシュを使用します。

（注） CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行元の証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

関連トピック

VPN 接続サーバーの設定 （131 ページ）

AnyConnect プロファイルエディタのモバイル設定

Apple iOS/Android の設定

- [証明書認証（Certificate Authentication）]：接続エントリに関連付けられた証明書認証ポリシー属性は、証明書がこの接続にどのように処理されるかを指定します。有効な値は次のとおりです。
  - [自動（Automatic）]：AnyConnectは、接続がいつなされるかを認証するクライアント証明書を自動で選択します。この場合、AnyConnectでインストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、デバイス ユーザが VPN 接続の確立を試行するたびに実行されます。
  - [手動（Manual）]：AnyConnectは、プロファイルがダウンロードされ、次のいずれかを行うときに、Androidデバイスの AnyConnect証明書ストアで証明書を検索します。
    - AnyConnect は、VPN クライアントプロファイルで定められる基準に一致している証明書に基づく証明書を見つけた場合、証明書を接続エントリに割り当て、接続が確立されたときにその証明書を使用します。
    - 一致する証明書が見つからない場合、証明書認証ポリシーが [自動（Automatic）] に設定されます。
    - 割り当てられた証明書が、何らかの理由で AnyConnect 証明書ストアから削除された場合、AnyConnect は [自動（Automatic）] に証明書認証ポリシーをリセットします。
  - [無効（Disabled）]：クライアント証明書は認証に使用されません。
- [プロファイルがインポートされたときにサーバ リスト エントリをアクティブ化（Make this Server List Entry active when profile is imported）]：VPN 接続がデバイスにダウンロードされたら、サーバ リスト エントリをデフォルトとして定義します。この宛先を設定できるのは、1つのサーバリストエントリのみです。デフォルトでは、無効に設定されています。

Apple iOS のみの設定

- [3G/WiFi ネットワーク間のローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]：有効（デフォルト）の場合、AnyConnect は、接続が解除された後やデバイスが起動した後、もしくは接続種別（EDGE（2G）、1xRTT（2G）、3G または Wi-Fi など）が変更になった後で、再接続にかかる時間を制限しません。この機能は、ネットワーク全体とのセキュアな接続を維持することで、シームレスなモビリティを提供します。企業への接続が必要で、かつバッテリ寿命の消費が多いアプリケーションには有用です。

  [ネットワークローミング（Network Roaming）] が無効で、AnyConnect の接続が切断された場合、必要に応じて最大 20 秒まで再接続を試みます。接続できない場合は、デバイス

ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

（注） ネットワーク ローミングは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響しません。

- [Connect on Demand（証明書の認証が必要）（Connect on Demand (requires certificate authorization)）]：このフィールドでは、Apple iOS で提供される Connect on Demand 機能を設定できます。その他のアプリケーションが、ドメイン ネーム システム（DNS）を使用して解決されるネットワーク接続を開始したときに、毎回チェックされるルールのリストを作成できます。

  [Connect on Demand] は、[証明書認証（Certificate Authentication）] フィールドが [手動（Manual）] または [自動（Automatic）] に設定されている場合にのみ使用できるオプションです。[証明書認証（Certificate Authentication）] フィールドが [無効（Disabled）] に設定されている場合は、このチェックボックスはグレー表示されます。[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

- [ドメインまたはホストと一致（Match Domain or Host）]：ユーザが Connect on Demand ルールを作成するホスト名（host.example.com）、ドメイン名（.example.com）、またはドメインの一部（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。

- [オンデマンドアクション（On Demand Action）]：デバイスユーザーが前の手順で定義されたドメインまたはホストに接続しようとしたときに実行するアクションを次の中から 1 つ指定します。

  - [接続しない（Never Connect）]：このリストのルールに一致しても、iOS は絶対に VPN 接続を開始しません。このリストのルールは他のどのリストよりも優先されます

（注） Connect On Demand が有効の場合、アプリケーションは自動的にこのリストにサーバアドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。

  - [必要に応じて接続（Connect if Needed）]：このリストのルールに一致したときに、システムが DNS を使用してアドレスを解決できなかった場合に限り、iOS は VPN 接続を開始します。

  - [常に接続（Always Connect）]：常時接続動作は、リリースに依存します。

- Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
- iOS 7.x では、[常に接続する（Always Connect）] はサポートされていません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
- 以降のリリースでは、[常に接続する（Always Connect）] は使用されません。設定済みのルールは [必要に応じて接続（Connect if needed）] リストに移動され、それに応じて動作します。

- [追加または削除（Add or Delete）] : [ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンドアクション（On Demand Action）] フィールドに指定されたルールをルール テーブルに追加するか、または選択したルールをルール テーブルから削除します。

Network Visibility Module のプロファイルエディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、またはデュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。収集データを Stealthwatch 7.3.1 以前のリリース（または Splunk や同様の SIEM ツール以外のもの）に送信する場合、キャッシュデータは信頼ネットワークに送信はされますが、処理されません。Stealthwatch アプリケーションについては、『Stealthwatch Enterprise Endpoint License and NVM Configuration Guide』を参照してください。

TND が Network Visibility Module プロファイルに設定されている場合、信頼ネットワーク検出は Network Visibility Module によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステムログに信頼ネットワーク検出の使用状況が表示されます。

Network Visibility Module プロファイルで TND を直接設定する場合、管理者が定義した信頼できるサーバーと証明書ハッシュによって、ユーザーが信頼できるネットワーク上にいるか、信頼できないネットワーク上にいるかが判別されます。コア VPN プロファイルの信頼ネットワーク検出を設定する管理者は、代わりに、コア VPN プロファイルで信頼された DNS ドメインと信頼された DNS サーバーを設定します。AnyConnect プロファイルエディタ、プリファレンス（Part 2） （98 ページ）

- [デスクトップ（Desktop）] または [モバイル（Mobile）] ：Network Visibility Module をデスクトップとモバイルデバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）] ：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [ポート（Port）] ：コレクタがリッスンするポート番号を指定します。
  - [セキュア（Secure）] ：Network Visibility Module が DTLS 経由でコレクタにデータを安全に送信するかどうかを決定します。このチェックボックスをオンにすると、Network Visibility Module はトランスポートに DTLS を使用します。DTLS 接続では、DTLS サーバ（コレクタ）証明書がエンドポイントによって信頼されている必要があります。信頼できない証明書はサイレントに拒否されます。

    DTLS サポートには CESA Splunk App v3.1.0 の一部としてのコレクタが必要であり、DTLS 1.2 が最小サポートバージョンです。
- **キャッシュの設定**
  - [最大サイズ（Max Size）] ：データベースが到達できる最大サイズを指定します。以前はキャッシュ サイズに事前設定の制限がありましたが、プロファイル内で設定でき

るようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

- [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

  日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- **[定期テンプレート（Periodi Template）]**：テンプレートがエンドポイントから送信される間隔を指定します。デフォルト値は 1440 分です。

- [定期的なフローレポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フローレポートが定期送信されます。デフォルトで、Network Visibility Module は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、*n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- **[集約間隔（Aggregation interval）]**：データフローをエンドポイントからエクスポートする間隔を指定します。デフォルト値の 5 秒を使用すると、単一のパケットで複数のデータフローがキャプチャされます。間隔の値が 0 秒の場合は、パケットごとに単一のデータフローが含まれます。有効な範囲は 0 ~ 600 秒です。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンド ユーザーへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイムデータとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

  キャッシュ データはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または [すべてのネットワーク（all networks）] を選択します。

- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。

  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにか

かる時間が削減されるよう、ブロードキャストパケットおよびマルチキャストパケットの収集はオフになっています。ブロードキャストパケットとマルチキャストパケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。

- [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。

- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時にアクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

  [追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。

  - ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
  - それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
  - より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
  - 選択したコレクションモードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。
  - 以前の AnyConnect リリースのプロファイルがそれより後の AnyConnect リリースのプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。

  - [名前（Name）]：作成するポリシーの名前を指定します。
  - [ネットワーク タイプ（Network Type）]：収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。
  - [フロー フィルタ ルール（Flow Filter Rule）]：一連の条件と、すべての条件が満たされたときに実行するアクションを、フローの収集または無視として定義します。最大

25 のルールを設定でき、各ルールに最大 25 の条件を定義できます。[フロー フィルタ ルール（Flow Filter Rule）] リストの右側にある上下ボタンを使用してルールの優先順位を調整し、後続のルールよりも優先的に考慮されるように設定します。[追加（Add）] をクリックし、フロー フィルタ ルールのコンポーネントを設定します。

- [名前（Name）]：フロー フィルタ ルールの一意の名前。
- [タイプ（Type）]：各フィルタ ルールには[収集（Collect）]または[無視（Ignore）]が指定されます。フィルタ ルールが満たされた場合に適用するアクション（[収集（Collect）] または [無視（Ignore）]）を決定します。[収集（Collect）] する場合、条件が満たされるとフローが許可されます。[無視（Ignore）] する場合、フローはドロップされます。
- [条件（Conditions）]：照合する各フィールドのエントリと、合致と見なすのはそのフィールド値が等しいときか等しくないときか、判断する操作を追加します。各操作にはフィールド識別子とそのフィールドに対応する値が含まれます。フィールドの一致では、フィルタ エンジン ルールの設定でルール セットに大文字と小文字を区別しない操作（EqualsIgnoreCase）を適用しない限り、大文字と小文字が区別されます。有効にした後、ルール下で設定された値フィールドへの入力は、大文字と小文字が区別されません。

- **[包含（Include）]/[除外（Exclude）]**
  - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドはすべて収集されます。どのフィールドもオンになっていない場合は、フィールドはすべて収集されます。
  - [フィールド（Fields）]：エンドポイントから受信する情報と、ポリシー要件を満たすためにデータ収集に含めるフィールドを決定します。ネットワークタイプ、およびどのフィールドを含めるか、または除外するかに基づいて、Network Visibility Module はエンドポイント上で適切なデータを収集します。

（注） 次のシナリオのいずれかが存在する場合、アップグレード中に、ProcessPath、ParentProcessPath、ProcessArgs、および ParentProcessArgs はデフォルトで、フロー情報でレポートされないように除外されます。

- 古いバージョンの Network Visibility Module のプロファイルにデータ収集ポリシーがない場合、またはデータ収集ポリシーが含まれていない場合。
- 古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあり、新しいバージョンのプロファイルエディタでプロファイルが開かれて保存された場合。古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあったが、新しい 4.9 以降のバージョンのプロファイルエディタでプロファイルが開かれて保存されていない場合は、次の 4 つのフィールドが含まれます。

Network Visibility Module が親プロセス ID を計算できない場合、値はデフォルトで 4294967295 になります。

FlowStartMsec と FlowStopMsec は、フローのエポックタイムスタンプをミリ秒単位で決定します。

インターフェイスの状態と SSID を選択して、インターフェイスのネットワーク状態が信頼できるかどうかを指定できます。

- [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードを、プライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。次に、実際の値ではなく、値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

  包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- [Knoxのデータ収集ポリシー（モバイルのみ）（Data Collection Policy for Knox (Mobile Specific)]：モバイルプロファイルを選択した場合にデータ収集ポリシーを指定するオプションです。Knox コンテナのデータ収集ポリシーを作成するには、[範囲（Scope）] の下の [Knox のみ（Knox-Only）] チェックボックスをオンにします。[デバイスの範囲（Device Scope）] で適用されるデータ収集ポリシーは、別の Knox コンテナデータ収集ポリシーが指定されていない限り、Knox コンテナトラフィックの場合も適用されます。データ収集ポリシーを追加または削除するには、前述の [データ収集ポリシー（Data Collection Policy）] の説明を参照してください。モバイルプロファイルでは最大 6 つの異なるデータ収集ポリシー（デバイス用に 3 つ、Knox 用に 3 つ）を設定できます。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、Network Visibility Module が設定されると、ユーザーに対して表示されるようになります。リモートユーザーは、Network Visibility Module アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して Network Visibility Module を制御します。

- [モバイルネットワークでのエクスポート（Export on Mobile Network）]（オプションおよびモバイルのみ）：デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローのエクスポートを許可するかどうかを指定します。有効な場合（デフォルト値）、エンドユーザーは、[利用許可ポリシー（Acceptable User Policy）] ウィンドウが表示されているとき、または後で AnyConnect Android アプリケーションで **[設定（Settings）]** > **[NVM 設定（NVM-Settings）]** > > **[NVM にモバイルデータを使用する（Use mobile data for NVM）]** チェックボックスをオンにして、管理者を上書きできます。[モバイルネットワークでのエクスポート（Export on Mobile Network）] チェックボックスをオフにすると、デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローがエクスポートされず、エンドユーザーはそれを変更できません。

- [信頼ネットワーク検出（Trusted Network Detection）]：この機能は、エンドポイントが物理的に社内ネットワーク上にあるかどうかを検出します。ネットワークの状態は、いつデータをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために Network Visibility Module によって使用されます。[設定（Configure）] をクリックして、信頼ネットワーク検出の設定を行います。SSL プローブが設定済みの信頼できるヘッドエンドに送信され、到達可能であれば、証明書で応答します。次に、サムプリント（SHA-256 ハッシュ）が抽出され、プロファイル エディタのハッシュ セットと照合されます。一致が見つかった場合はエンドポイントが信頼ネットワーク内にあることを意味します。ただし、ヘッドエンドが到達不能である場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼されていないネットワーク内にあると見なされます。

  （注） 内部ネットワーク外から操作している場合、信頼ネットワーク検出は DNS 要求を行い、設定されたサーバーへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

  TND が NVM プロファイルに設定されておらず、VPN モジュールがインストールされている場合、NVM は Trusted Network Detection の設定を使用して、エンドポイントが信頼ネットワーク内にあるかどうかを判断します。NVM プロファイル エディタの TND 設定には次が含まれます。

  1. **https://**：信頼されている各サーバの URL（IP アドレス、FQDN、またはポート アドレス）を入力し、[追加（Add）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

2. [証明書ハッシュ（SHA-256）（Certificate Hash (SHA-256)）]：信頼されているサーバへのSSL接続が成功した場合、このフィールドは自動的に入力されます。それ以外の場合は、サーバ証明書の SHA-256 ハッシュを入力して [設定（Set）] をクリックすることにより手動で設定できます。

3. [信頼されているサーバのリスト（List of Trusted Servers）]：このプロセスで複数の信頼されているサーバを定義できます（最大値は 10 です）。サーバは、設定されている順序で信頼ネットワーク検出に対して試行されるため、[上に移動（Move Up）] ボタンと [下に移動（Move |Down）] ボタンを使用して順序を調整できます。エンドポイントが最初のサーバに接続できなかった場合は、2 番目のサーバという順序で試行されます。リスト内のすべてのサーバをした後、エンドポイントは 10 秒待機してからもう一度途最終試行を行います。サーバが認証されると、エンドポイントは信頼ネットワーク内で考慮されます。

プロファイルを `NVM_ServiceProfile.xml` として保存します。この名前でプロファイルを保存する必要があります。そうしないと、Network Visibility Module はデータの収集と送信に失敗します。

AnyConnect ローカルポリシー

AnyConnectLocalPolicy.xml は、セキュリティ設定を含む、クライアント上の XML ファイルです。このファイルは、Cisco Secure Firewall ASA によって展開されません。手動でインストールするか、社内のソフトウェア展開システムを使用してユーザー コンピュータに展開する必要があります。ユーザーのシステムで既存のローカルポリシーファイルに変更を加えた場合は、そのシステムをリブートする必要があります。

ローカルポリシー設定

VPN ローカルポリシーエディタで、`AnyConnectLocalPolicy.xml` ファイルに含める次の設定を指定できます。

ローカル ポリシー パラメータの手動変更

手順

ステップ 1 クライアント インストールから、AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）のコピーを取得します。

表 *6:* オペレーティング システムと *AnyConnect* ローカル ポリシー ファイルのインストール パス

オペレーティング システム	インストール パス
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client
Linux	/opt/cisco/anyconnect
macOS	/opt/cisco/anyconnect

ステップ 2 パラメータ設定を編集します。AnyConnectLocalPolicy ファイルを手動で編集するか、AnyConnect プロファイル エディタのインストーラとともに配布される VPN ローカル ポリシー エディタを使用できます。

ステップ 3 ファイルを `AnyConnectLocalPolicy.xml` として保存し、社内のソフトウェア展開システムを使用してこのファイルをリモート コンピュータに展開します。

ステップ 4 ローカル ポリシー ファイルへの変更が反映されるように、リモート コンピュータをリブートします。

MST ファイルでのローカル ポリシー パラメータの有効化

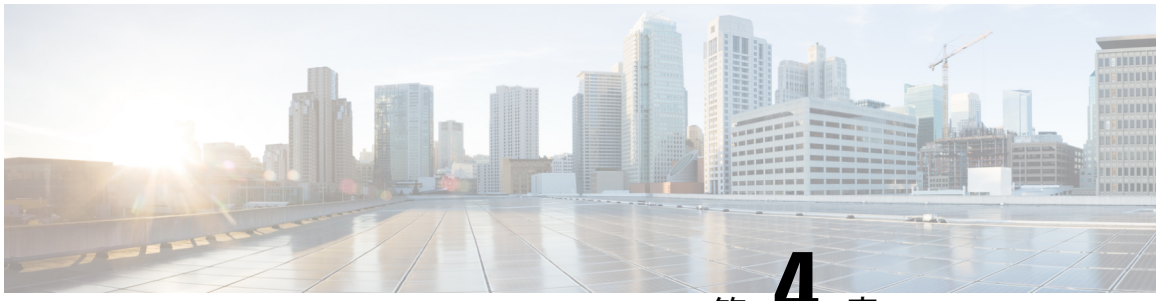
設定できる説明および値については、「ローカルポリシー設定」を参照してください。

ローカル ポリシー パラメータを変更するには、MST ファイルを作成します。MST パラメータ名は、AnyConnect ローカルポリシーファイル（AnyConnectLocalPolicy.xml）の次のパラメータに対応しています。

- LOCAL_POLICY_BYPASS_DOWNLOADER
- LOCAL_POLICY_FIPS_MODE
- LOCAL_POLICY_RESTRICT_PREFERENCE_CACHING
- LOCAL_POLICY_RESTRICT_TUNNEL_PROTOCOLS
- LOCAL_POLICY_RESTRICT_WEB_LAUNCH
- LOCAL_POLICY_STRICT_CERTIFICATE_TRUST

（注） AnyConnect インストールは、ユーザ コンピュータ上にある既存のローカル ポリシー ファイルを自動的には上書きしません。クライアント インストーラが新しいポリシー ファイルを作成できるようにするには、その前にユーザ コンピュータ上の既存のポリシー ファイルを削除しておく必要があります。

（注） ローカル ポリシー ファイルへのすべての変更には、システムのリブートが必要になります。



第 4 章

VPN アクセスの設定

VPN への接続と接続解除

AnyConnect VPN 接続オプション

AnyConnect には、自動的に VPN セッションを接続、再接続、または切断するための多数のオプションが用意されています。これらのオプションは、ユーザが VPN に接続するために便利な方法を提供し、同時にネットワーク セキュリティの要件をサポートします。

AnyConnect 接続の開始とリスタート

VPN 接続サーバーの設定を行い、ユーザが手動で接続するセキュア ゲートウェイの名前とアドレスを提供します。

便利な自動 VPN 接続を提供するための AnyConnect 機能を次から選択します。

- ログイン前の Windows VPN 接続の自動開始
- AnyConnect 起動時の VPN 接続の自動開始
- VPN 接続の自動リスタート

また、強力なネットワーク セキュリティを適用したり、ネットワーク アクセスを VPN のみに制限したりするために、次の自動 VPN ポリシー オプションの使用を検討してください。

- Trusted Network Detection について
- Always-Onを使用した VPN 接続の必要性
- キャプティブ ポータル ホットスポットの検出と修復の使用

AnyConnect 接続の再ネゴシエートと維持

アクティビティが発生していない場合でも、Cisco Secure Firewall ASA がユーザーに対して AnyConnect VPN 接続を維持する長さを制限できます。VPN セッションがアイドルになった場合、接続を終了するか、または接続を再ネゴシエートできます。

- キープアライブ：Cisco Secure Firewall ASA はキープアライブメッセージを定期的に送信します。これらのメッセージは、Cisco Secure Firewall ASA によって無視されますが、クライアントと Cisco Secure Firewall ASA の間の、デバイスを使用した接続の維持に役立ちます。

  ASDM または CLI でキープアライブを設定する手順については、『Cisco ASA Series VPN Configuration Guide』の「Enable Keepalive」の項を参照してください。

- デッド ピア検出：Cisco Secure Firewall ASA および AnyConnect クライアントは、「R-U-There」メッセージを送信します。これらのメッセージは、IPsec のキープアライブメッセージよりも少ない頻度で送信されます。Cisco Secure Firewall ASA（ゲートウェイ）および AnyConnect の両方で、DPD メッセージの送信を有効にして、タイムアウト間隔を設定できます。
  - クライアントが Cisco Secure Firewall ASA の DPD メッセージに応答しない場合、ASA はもう 1 回試行してから、セッションを「再開待機」モードに移行します。このモードでは、ユーザはネットワークをローミングしたり、スリープモードに移行してから後で接続を回復したりできます。アイドルタイムアウトが発生する前にユーザーが再接続しなかった場合、Cisco Secure Firewall ASA はトンネルを終了します。推奨されるゲートウェイ DPD 間隔は 300 秒です。
  - Cisco Secure Firewall ASA がクライアントの DPD メッセージに応答しない場合、クライアントはもう 1 回試行してから、トンネルを終了します。推奨されるクライアント DPD 間隔は 30 秒です。

    ASDM 内で DPD を設定する手順については、適切なリリースの『Cisco ASA Series VPN ASDM Configuration Guide』の「Configure Dead Peer Detection」の項を参照してください。

- ベスト プラクティス：
  - クライアント DPD を 30 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

- サーバ DPD を 300 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。
- SSL および IPsec の両方のキー再生成を 1 時間に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [キー再作成（Key Regeneration）]）。

AnyConnect VPN 接続の終了

AnyConnect VPN 接続を終了するには、ユーザーはセキュアゲートウェイに対してエンドポイントを再認証し、新しい VPN 接続を作成する必要があります。

次の接続パラメータは、タイムアウトに基づいて、VPN セッションを終了します。

- 最大接続時間：ユーザの最大接続時間を分単位で設定します。ここで指定した時間が経過すると、システムは接続を終了します。また、無制限の接続時間（デフォルト）を許可することもできます。
- VPN アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。VPN アイドル タイムアウトを設定しない場合は、デフォルトのアイドル タイムアウトが使用されます。
- デフォルト アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。デフォルト値は 30 分（1800 秒）です。

これらのパラメータを設定するには、適切なリリースの『Cisco ASA Series VPN ASDM コンフィギュレーション ガイド』の「Specify a VPN Session Idle Timeout for a Group Policy」の項を参照してください。

VPN 接続サーバーの設定

AnyConnect VPN サーバーリストは、VPN ユーザーが接続するセキュアゲートウェイを識別するホスト名とホストアドレスのペアで構成されます。ホスト名は、エイリアス、FQDN、または IP アドレスで指定できます。

サーバーリストに追加されたホストは、AnyConnect GUI の [接続先（Connect to）] ドロップダウンリストに表示されます。その後、ユーザはドロップダウン リストから選択して VPN 接続を開始できます。リストの最上位にあるホストはデフォルト サーバで、GUI のドロップダウン リストの先頭に表示されます。ユーザがリストから代替サーバを選択した場合、その選択されたサーバが新しいデフォルト サーバになります。

サーバ リストにサーバを追加すると、その詳細を表示し、サーバ エントリを編集または削除するようになります。サーバ リストにサーバを追加するには、次の手順を実行します。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 サーバのホスト名およびアドレスを設定します。

a) [ホスト表示名（Host Display Name）]、ホストの参照に使用されるエイリアス、FQDN、または IP アドレスを入力します。名前に「&」または「<」文字を使用しないでください。FQDN または IP アドレスを入力した場合、次の手順で [FQDN] または [IP アドレス（IP Address）] を入力する必要はありません。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカル セキュア ゲートウェイ アドレスの使用はサポートしていません。

b) （任意）[ホスト表示名（Host Display Name）] に入力していない場合、ホストの [FQDN] または [IP アドレス（IP Address）] を入力します。

c) （任意）[ユーザ グループ（User Group）] を指定します。

AnyConnect は、ユーザーグループとともに FQDN または IP アドレスを使用してグループ URL を形成します。

ステップ 4 [バックアップ サーバ リスト（Backup Server List）] に、バックアップ サーバとしてフォールバックするサーバを入力します。名前に「&」または「<」文字を使用しないでください。

（注） 逆の面から述べれば、[サーバ（Server）] メニューの [バックアップ サーバ（Backup Server）] タブは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

ステップ 5 （任意）[ロード バランシング サーバ リスト（Load Balancing Server List）] に、ロード バランシング サーバ を追加します。名前に「&」または「<」文字を使用しないでください。

このサーバ リスト エントリのホストにセキュリティ アプライアンスのロード バランシング クラスタを指定し、かつ Always-On 機能が有効になっている場合は、このリストにクラスタのロード バランシング デバイスを追加します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは Always-On 機能によりブロックされます。

ステップ 6 クライアントがこの Cisco Secure Firewall ASA に使用する [プライマリ プロトコル（Primary Protocol）] を指定します。

a) SSL（デフォルト）または IPSec を選択します。

IPsec を指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

b) IPSec を指定した場合は、[標準認証のみ（Standard Authentication Only）] を選択してデフォルトの認証方式（独自の AnyConnect EAP）を無効にし、ドロップダウン リストからいずれかの方式を選択します。

（注） 認証方式を独自の AnyConnect EAP から標準ベースの方式に変更すると、Cisco Secure Firewall ASA でセッションタイムアウト、アイドルタイムアウト、接続解除タイムアウト、スプリットトンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

ステップ 7 （任意）このサーバ用の SCEP を設定します。

a) SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。

b) [チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにして、ユーザが証明書を手動で要求できるようにします。ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。

c) CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します。CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

ステップ 8 [OK] をクリックします。

関連トピック

AnyConnect プロファイルエディタのサーバーリスト （112 ページ）
AnyConnect プロファイルエディタのサーバーリストの追加/編集 （113 ページ）

ログイン前の Windows VPN 接続の自動開始

Start Before Login について

Start Before Login（SBL）と呼ばれるこの機能により、ユーザーは Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。

（注） Start Before Login（SBL）および HostScan を使用する場合、SBL は事前ログインであるため、完全な HostScan 機能を実現するには、VPN ポスチャ 事前展開モジュールをエンドポイントにインストールする必要があります。

SBL がインストールされ、有効になると、[ネットワーク接続（Network Connect）] ボタンは AnyConnect コア VPN および Network Access Manager UI を起動します。

SBL には、Network Access Manager タイルも含まれており、ユーザが設定したホーム ネットワーク プロファイルを使用した接続を可能にします。SBL モードで許可されるネットワーク

プロファイルには、非802.1X認証モードを採用するすべてのメディアタイプ（オープンWEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。

SBL は Windows システムのみで利用でき、Windows のバージョンによって異なるメカニズムを使用して実装されます。

- Windows では、Pre-Login Access Provider（PLAP）が AnyConnect SBL を実装するために使用されます。

  PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [ネットワーク接続（Network Connect）] ボタンでネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

  PLAP は Windows の 32 ビット版と 64 ビット版をサポートします。

SBL を有効にする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループポリシーでキャッシュのクレデンシャル使用が許可されない場合）。このシナリオでは、コンピュータへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。SBL を有効にすると、ユーザは、ローカル インフラストラクチャおよび通常はオフィスにいるときに実行されるログイン スクリプトにアクセスできます。これには、ドメイン ログイン スクリプト、グループポリシー オブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。
- インフラストラクチャとの接続が必要な場合があるネットワーキング コンポーネント（MS NAP/CS NAC など）が存在する。

Start Before Login に関する制限事項

- AnyConnect は、高速ユーザー切り替えとの互換性がありません。
- AnyConnect は、サードパーティの Start Before Login アプリケーションでは起動できません。
- SBL は事前ログインされており、ユーザストアにアクセスできないため、複数の証明書認証（MCA）を実行できません。MCA には、マシン証明書とユーザ証明書、または 2 つのユーザ証明書が必要です。

Start Before Login の設定

手順

ステップ 1 AnyConnect Start Before Login モジュールのインストール。

ステップ 2 AnyConnect VPN プロファイルでの SBL の有効化。

AnyConnect Start Before Login モジュールのインストール

AnyConnect インストーラは、基盤となるオペレーティングシステムを検出し、システムディレクトリに AnyConnect SBL モジュールから適切な AnyConnect DLL を配置します。Windows デバイスでは、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネント（vpnplap.dll または vpnplap64.dll）をインストールします。

（注） SBL モジュールがインストールされたまま AnyConnect をアンインストールすると、SBL モジュールは無効となり、リモートユーザーの画面に表示されなくなります。

SBL モジュールを事前展開するか、SBL モジュールをダウンロードするように ASA を設定することができます。AnyConnect を事前展開する場合は、Start Before Login モジュールよりも先にコア クライアント ソフトウェアをインストールする必要があります。MSI ファイルを使用して AnyConnect VPN および Start Before Login コンポーネントを事前展開する場合は、正しい順序で実行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 左側のナビゲーションペインで **[詳細（Advanced）]** > **[AnyConnectクライアント（AnyConnect Client）]** を選択します。

ステップ 4 [ダウンロードするオプションのクライアント モジュール（Optional Client Module for Download）] 設定の [継承（Inherit）] をオフにします。

ステップ 5 ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

AnyConnect VPN プロファイルでの SBL の有効化

始める前に

- SBLは、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、その他のワイヤレス認証を設定する必要があります。
- Network Access Managerがインストールされている場合、デバイス接続を展開して、適切な接続を確実に使用できるようにする必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [Start Before Loginの使用（Use Start Before Login）] を選択します。

ステップ 3 （任意）リモート ユーザが SBL を制御できるようにする場合は、[ユーザ制御可（User Controllable）] をオンにします。

（注） SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

Start Before Login のトラブルシューティング

手順

ステップ 1 AnyConnect VPN プロファイルが Cisco Secure Firewall ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2 以前のプロファイルを削除します（*.xml と指定してハード ドライブ上の格納場所を検索します）。

ステップ 3 Windows の [プログラムの追加と削除（Add/Remove Programs）] を使用して SBL コンポーネントをアンインストールします。コンピュータをリブートして、再テストします。

ステップ 4 イベントビューアでユーザーの AnyConnect ログをクリアし、再テストします。

ステップ 5 セキュリティアプライアンスを再度参照して、AnyConnect を再インストールします。

ステップ 6 いったんリブートします。次回リブート時には、Start Before Login プロンプトが表示されます。

ステップ 7 DART バンドルを収集し、AnyConnect 管理者に送付します。

ステップ 8 次のエラーが表示された場合は、ユーザーの AnyConnect VPN プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application
 Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
 available.
```

ステップ 9 .tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

AnyConnect 起動時の VPN 接続の自動開始

[起動時に自動接続（Auto Connect on Start）] とも呼ばれるこの機能は、AnyConnect が開始されると、VPN クライアントプロファイルで指定されたセキュアゲートウェイへの VPN 接続を自動的に確立します。

[起動時に自動接続（Auto Connect on Start）] はデフォルトでは無効であり、ユーザはセキュアゲートウェイを指定または選択する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [起動時に自動接続（Auto Connect on Start）] を選択します。

ステップ 3 （任意）[起動時に自動接続（Auto Connect on Start）] をユーザが制御できるようにするには、[ユーザ制御可（User Controllable）] を選択します。

Windows システムにおける Start Before Login（PLAP）の設定

Start Before Login（SBL）機能によって、ユーザーが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。Windows にインストールできるのは、一度に 1 つの PLAP のみです。

SBL AnyConnect 機能は、Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、プログラマチック ネットワークの管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログオン前に実行することができます。PLAP では、サポートされている Windows オペレーティング システムすべてに対して SBL 機能を提供します。PLAP は、vpnplap.dll を使用する 32 ビッ

ト版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

VPN 接続の自動リスタート

[自動再接続（Auto Reconnect）] が有効（デフォルト）になっている場合、AnyConnect は初期接続に使用したメディアに関係なく、VPNセッションの中断から回復し、セッションを再確立します。たとえば、有線、ワイヤレス、または3G/4G/5Gのセッションを再確立できます。[自動再接続（Auto Reconnect）]が有効になっている場合は、システムの一時停止またはシステムの再開が発生した場合の再接続動作も指定します。システムの一時停止とは、Windowsの「休止状態」や macOS または Linux の「スリープ」など、低電力スタンバイのことです。システムの再開とは、システムの一時停止からの回復のことです。

[自動再接続（Auto Reconnect）] を無効にすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。この機能のデフォルト設定（有効）を使用することを強く推奨します。この設定を無効にすると、不安定な接続では VPN 接続の中断が発生することがあります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [自動再接続（Auto Reconnect）] を選択します。

ステップ 3 自動再接続の動作を選択します。

- [Disconnect On Suspend]（デフォルト）：AnyConnect では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
- [再開後に再接続（Reconnect After Resume）]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムの再開後は再接続が試行されます。

Trusted Network Detection を使用した接続または接続解除

Trusted Network Detection について

信頼ネットワーク検出（TND）を使用すると、ユーザーが企業ネットワークの中（信頼ネットワーク）にいる場合はAnyConnectにより自動的にVPN接続が解除され、企業ネットワークの外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。

TND を使用している場合でも、ユーザーが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザーが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザーが信頼ネットワークに移動した場合だけです。たとえば、ユーザーが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

（注） Network Visibility Module の TND 機能を設定するには、「Network Visibility Module」の章の Network Visibility Module のプロファイルエディタ （118 ページ）を参照してください。

TND は AnyConnect VPN プロファイルに設定します。Cisco Secure Firewall ASA の設定を変更する必要はありません。AnyConnect が信頼ネットワークと非信頼ネットワークの間の遷移を認識したときに実施するアクションまたはポリシーを指定する必要があります。また、信頼ネットワークおよび信頼サーバーを特定する必要があります。

Trusted Network Detection のガイドライン

- TND 機能は AnyConnect GUI を制御し、接続を自動的に開始するため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。
- さらに AnyConnect VPN で Start Before Login（SBL）が実行されている場合は、ユーザーが信頼ネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。
- Always-Onが設定されているかどうかにかかわらず、信頼ネットワーク検出は、IPv4 ネットワークおよび IPv6 ネットワーク経由での Cisco Secure Firewall ASA への IPv6 および IPv4 VPN 接続でサポートされています。
- ユーザ コンピュータ上に複数のプロファイルがあると、TND 設定が異なっている場合には問題になることがあります。

  ユーザーが過去に TND 対応のプロファイルを受け取っていた場合、システムをリスタートすると、AnyConnect は最後に接続されたセキュリティアプライアンスへの接続を試みますが、これが目的の動作ではないことがあります。別のセキュリティアプライアンスに接続するには、そのヘッドエンドを手動で接続解除してから、再接続する必要があります。この問題を回避する手段としては、次のような対策が考えられます。

  - 社内ネットワーク上にあるすべての Cisco Secure Firewall ASA にロードされるクライアントプロファイルで、TND を有効にする。
  - すべての Cisco Secure Firewall ASA がリストされた 1 つのプロファイルをホストエントリセクションに作成し、このプロファイルをすべての Cisco Secure Firewall ASA にロードする。
  - 複数の異なるプロファイルが必要ない場合は、すべての Cisco Secure Firewall ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 Cisco Secure Firewall ASA により上書きされます。

- Linux 上で TND を使用するには、ネットワーク マネージャがインストールされてターゲット（RHEL/Ubuntu）デバイス上で正しく実行されていることと、ネットワーク インターフェイスがネットワーク マネージャによって管理されていることが必要です。

Trusted Network Detection の設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。

ステップ 3 [信頼されたネットワークポリシー（Trusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク（信頼ネットワーク）内に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続解除（Disconnect）]：（デフォルト）クライアントは、信頼ネットワークで VPN 接続を終了します。
- [接続（Connect）]：クライアントは、信頼ネットワークで VPN 接続を開始します。
- [何もしない（Do Nothing）]：クライアントは、信頼ネットワークでアクションを実行しません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection（TND）は無効となります。
- [一時停止（Pause）]：ユーザーが信頼ネットワークの外で VPN セッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、AnyConnect は AnyConnect VPN セッションを接続解除するのではなく、一時停止します。ユーザーが再び信頼ネットワークの外に出ると、そのセッションは AnyConnect により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しい VPN セッションを確立する必要がなくなるため、ユーザにとっては有用です。

ステップ 4 [信頼されていないネットワークポリシー（Untrusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク外に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続（Connect）]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。
- [何もしない（Do Nothing）]：クライアントは、非信頼ネットワークの検出時にアクションを実行しません。このオプションを指定すると、Always-On VPN が無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

ステップ 5 [信頼された DNS ドメイン（Trusted DNS Domains）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができる DNS サフィックス（カンマ区切りの文字列）を指定します。split-dns リストに複数の DNS サフィックスを追加し、Cisco Secure Firewall ASA でデフォルトドメインを指定した場合、複数の DNS サフィックスを割り当てることができます。

AnyConnect は、次の順序で DNS サフィックスのリストを構築します。

- ヘッド エンドから渡されたドメイン。
- ヘッド エンドから渡されたスプリット DNS リスト。
- パブリック インターフェイスの DNS サフィックス（設定されている場合）。設定されていない場合は、プライマリ DNS サフィックスの親サフィックスを伴うプライマリおよび接続固有のサフィックス（対応するボックスが拡張 TCP/IP 設定でオンの場合）。

照合する DNS サフィックス	TrustedDNSDomains に使用する値
example.com（のみ）	*example.com
example.com および vpn.example.com	*.example.com または example.com、vpn.example.com
asa.example.com および vpn.example.com	*.example.com または asa.example.com、vpn.example.com

ステップ 6 [信頼されたDNSサーバー（Trusted DNS Servers）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるすべての DNS サーバーアドレス（カンマ区切りの文字列）。たとえば、203.0.113.1,2001:DB8::1 です。IPv4 および IPv6 DNS サーバーアドレスでは、ワイルドカード（*）がサポートされています。

DNS で解決できるヘッドエンドサーバーの DNS エントリが必要です。IP アドレスによる接続の場合、mus.cisco.com を解決できる DNS サーバーが必要です。mus.cisco.com が DNS で解決できない場合、キャプティブ ポータルの検出が期待どおりに動作しません。

（注） TrustedDNSDomains、TrustedDNSServers、またはその両方を設定できます。TrustedDNSServers を設定する場合は、DNS サーバーをすべて入力してください。その結果、サイトはすべて信頼ネットワークの一部になります。

アクティブ インターフェイスは、VPN プロファイルのすべてのルールが一致した場合に、信頼ネットワークに含まれると見なされます。

ステップ 7 信頼できる URL として追加するホスト URL を指定します。信頼できる証明書を使用してアクセス可能なセキュア Web サーバーが、信頼できるサーバーとして見なされる必要があります。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバーを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバーが定義されていない場合、このフィールドは無効になります。

Always-Onを使用した VPN 接続の必要性

Always-On VPN について

Always-On操作により、VPNセッションがアクティブでない限り、コンピュータが信頼ネットワーク上にない場合にはインターネット リソースにアクセスできなくなります。この状況で VPN を常に適用すると、コンピュータがセキュリティに対する脅威から保護されます。

Always-Onが有効になっている場合、ユーザがログインした後、および非信頼ネットワークが検出されたときに、VPN セッションが自動的に確立されます。VPN セッションは、ユーザーがコンピュータからログアウトするか、セッション タイマーまたはアイドル セッション タイマー (Secure Firewall ASA グループポリシーで指定) が期限切れになるまで開いたままになります。セッションがまだ開いている場合は、AnyConnect は、セッションを再アクティブ化するために、 接続の再確立を継続的に試行します。それ以外の場合は、新しい VPN セッションの確立を継続的に試みます。

VPN プロファイルで Always-On が有効になっている場合、AnyConnect は他のダウンロードされたすべての AnyConnect プロファイルを削除してエンドポイントを保護し、Cisco Secure Firewall ASA に接続するように設定されているパブリックプロキシを無視します。

Always-On を有効にする場合は、次の AnyConnect オプションも考慮する必要があります。

- [ユーザーに Always-On VPN セッションの接続解除を許可（Allowing the user to Disconnect the VPN session）]：AnyConnect では、ユーザーが Always-On VPN セッションの接続を解除できます。**Allow VPN Disconnect** を有効にすると、AnyConnect では VPN セッションが確立された時点で [接続解除（Disconnect）] ボタンが表示されます。Always-On VPN を有効にすると、プロファイル エディタでは、[接続解除（Disconnect）] ボタンがデフォルトで有効になります。

  [接続解除（Disconnect）]ボタンを押すと、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。現在の VPN セッションでパフォーマンスが低下したり、VPNセッションの中断後に再接続で問題が発生したりした場合、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

- [接続障害ポリシーの設定（Setting a Connect Failure Policy）]：接続障害ポリシーにより、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかが決まります。「常時接続の接続障害ポリシーの設定」を参照してください。

- [キャプティブポータルホットスポットの処理（Handling Captive Portal Hotspots）]：「キャプティブ ポータル ホットスポットの検出と修復の使用」を参照してください。
- VPN が切断されている間の特定のホストへのアクセスの許可：[VPNが切断された状態で次のホストへのアクセスを許可する（Allow access with VPN connected）]（特定の HostScan の導入に必要な場合があります）で使用可能なオプションの設定。[常にオン（Always On）] の間に AnyConnect VPN が切断されたときに、設定されたホストにエンドポイントがアクセスできるようにします。値は、IP アドレス、IP アドレス範囲（CIDR 形式）、または FQDN を指定できるホストのカンマ区切りリストです。最大 500 のホストを指定できます。

Always-On VPN の制限事項

- [常時オン（Always On）] は Windows および macOS でのみ使用可能です。
- Always-Onがオンであっても、ユーザーがログインしていない場合は、AnyConnect は AnyConnect VPN 接続を確立しません。AnyConnect はログイン後にのみ AnyConnect VPN 接続を開始します。
- Always-On VPN では、プロキシを介した接続はサポートされていません。

Always-On VPN のガイドライン

脅威に対する保護を強化するためにも、Always-On VPN の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- 認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。ASDM では、[アイデンティティ証明書（Identity Certificates）] パネル（[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] > [アイデンティティ証明書（Identity Certificates）]）に、公開証明書を容易に登録するための [ASA SSL VPN を Entrust で登録（Enroll ASA SSL VPN with Entrust）] ボタンが用意されています。
- 常時接続の VPN を使用している場合、外部 SAML IdP はサポートされません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- Always-On が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された Cisco Secure Firewall ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより、Always-Onポリシーを無視することができます。Always-Onの安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。

- Windows コンピュータ上の Cisco サブフォルダ（通常は `C:\ProgramData`）へのアクセスを制限します。
- 限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、AnyConnect プロファイルを削除できるため、Always-On 機能を無効にすることができます。
- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。macOS ユーザに対してもこれに相当するものを事前に展開します。

Always-On VPN の設定

手順

ステップ 1 Always-On を AnyConnect VPN プロファイルに設定する （144 ページ）。
ステップ 2 （任意）サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加。
ステップ 3 （任意）常時接続 VPN からのユーザの除外。

Always-On を AnyConnect VPN プロファイルに設定する

始める前に

Always-On VPN を使用するには、Cisco Secure Firewall ASA 上に有効な信頼できるサーバー証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。また、サーバー証明書が厳格な証明書トラスト モードを通過できるようにすると、Always-On VPN プロファイルのダウンロードを防止して不正なサーバーへの VPN 接続をロックできます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。
ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。
ステップ 3 Trusted Network Detection の設定 （140 ページ）。
ステップ 4 [常時接続（Always On）] を選択します。
ステップ 5 （任意）[VPN の接続解除を許可（Allow VPN Disconnect）] を選択または選択解除します。
ステップ 6 （任意）VPN が [常にオン（Always On）] の場合、切断されるときにエンドポイントがアクセスできるホストを定義します。

ステップ 7 （任意）接続障害ポリシーの設定。

ステップ 8 （任意）キャプティブ ポータル修復の設定。

サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加

Always-On VPN は、AnyConnect VPN セッションのロード バランシングに影響を与えます。Always-On VPN を無効にした状態では、クライアントからロード バランシング クラスタ内のプライマリ デバイスに接続すると、クライアントはプライマリ デバイスから任意のバックアップ クラスタ メンバーにリダイレクションされます。Always-On を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがプライマリ デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロードバランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 ロードバランシング クラスタのプライマリ デバイスであるサーバを選択し、[編集（Edit）] をクリックします。

ステップ 3 いずれかのロードバランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

常時接続 VPN からのユーザの除外

Always-Onポリシーに優先して適用される除外規定を設定できます。たとえば、特定のユーザに対して他社とのVPNセッションを確立できるようにしつつ、企業外資産に対してはAlways-On VPN ポリシーを除外するという場合があります。

Cisco Secure Firewall ASA のグループポリシーおよびダイナミック アクセス ポリシーで設定された除外規定はAlways-Onポリシーを上書きします。ポリシーの割り当てに使用される一致基準に従って例外を指定します。AnyConnect VPN ポリシーでは Always-On が有効になっているが、ダイナミック アクセス ポリシーまたはグループポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

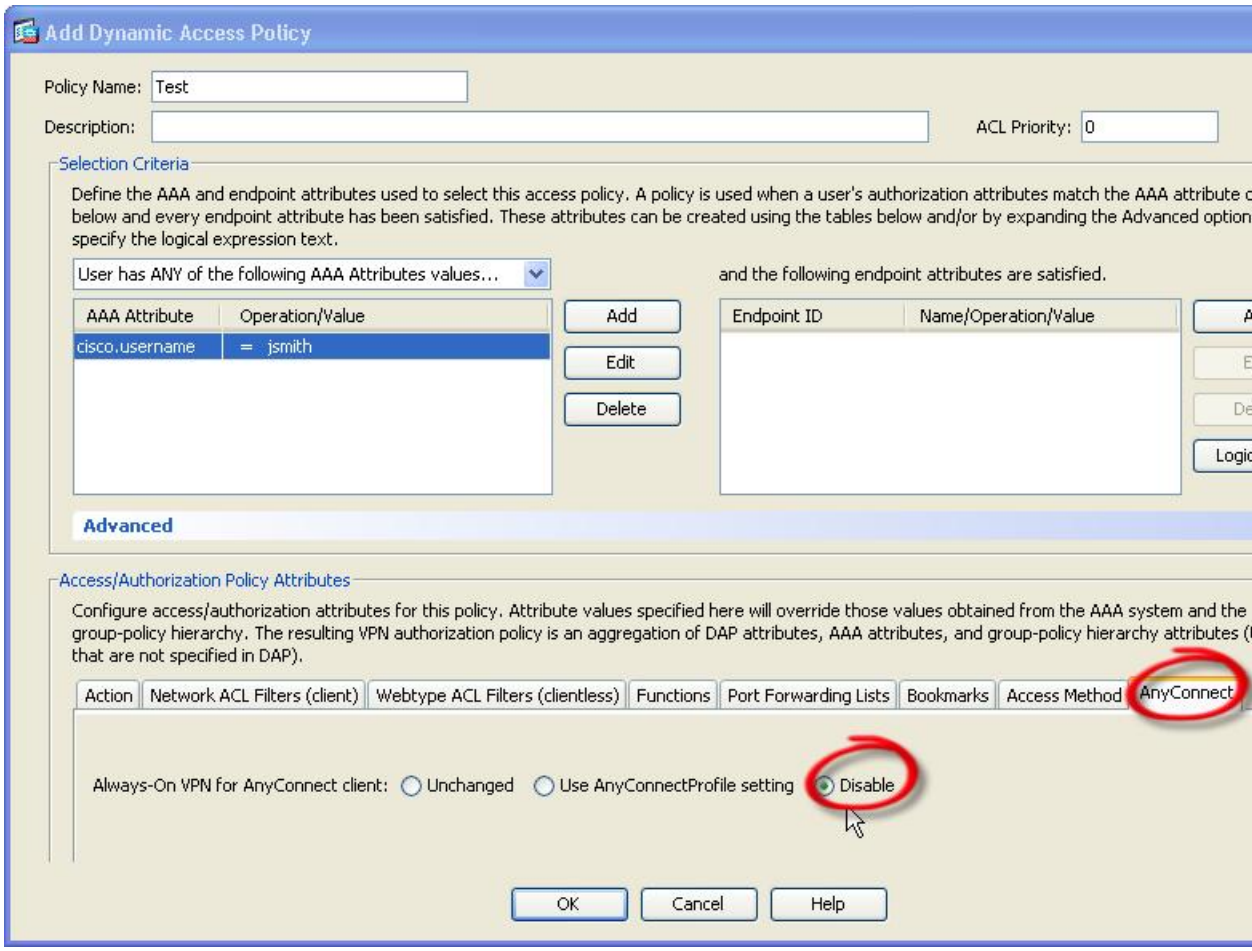
この手順では、AAA エンドポイント条件を使用して企業外資産にセッションを照合するダイナミック アクセス ポリシーを設定します。

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）]>[ダイナミック アクセス ポリシー（Dynamic Access Policies）]>[追加（Add）] または [編集（Edit）] を選択します。

ステップ 2 ユーザをAlways-On VPN から除外する条件を設定します。たとえば、[選択基準（Selection Criteria）] 領域を使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3 [ダイナミック アクセス ポリシーの追加（Add Dynamic Access Policy）] ウィンドウまたは [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] ウィンドウの下半分にある [AnyConnect] タブをクリックします。



ステップ 4 [AnyConnect クライアントのAlways-On VPN（Always-On VPN for AnyConnect client）] の横にある [無効（Disable）] をクリックします。

常時接続の接続障害ポリシーの設定

接続障害ポリシーについて

接続障害ポリシーは、Always-On VPN が有効で、AnyConnect が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかを決定します。これは、セキュアゲートウェイに到達不能な場合、または AnyConnect がキャプティブポータル ホットスポットの存在を検出できない場合に発生する可能性があります。

オープン ポリシーは、最大限のネットワーク アクセスを許可します。これにより、インターネットリソースやその他のローカルネットワークリソースへのアクセスが必要なタスクをユーザが継続して実行できるようにします。

クローズドポリシーは、VPNセッションが確立されるまで、すべてのネットワーク接続を無効にします。AnyConnect では、エンドポイントから、コンピュータが接続を許可されているセキュアゲートウェイ宛以外のトラフィックをすべてブロックするパケットフィルタを有効にすることで、この制限が実現されています。

AnyConnect では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。

接続障害ポリシーを設定するためのガイドライン

最大限のネットワーク アクセス権を許可するオープン ポリシーを使用する場合は、次の点を考慮してください。

- VPNセッションが確立されるまでセキュリティと保護は提供されません。したがって、エンドポイント デバイスが Web ベースのマルウェアに感染したり、センシティブ データが漏えいしたりする可能性があります。
- [接続解除（Disconnect）] ボタンが有効で、かつユーザが [接続解除（Disconnect）] をクリックした場合は、オープン接続障害ポリシーは適用されません。

VPNセッションが確立されるまですべてのネットワーク接続を無効にする終了ポリシーを使用する場合は、次の点を考慮してください。

- ユーザが VPN の外部へのインターネット アクセスを必要とする場合に、クローズド ポリシーを適用すると、生産性が低下する可能性があります。
- クローズドの目的は、エンドポイントを保護するプライベート ネットワークのリソースが使用できない場合に、ネットワークの脅威から企業資産を保護することです。スプリット トンネリングによって許可されたプリンタやテザー デバイスなどのローカル リソースを除き、すべてのネットワーク アクセスが禁止されるため、エンドポイントは Web ベースのマルウェアとセンシティブ データ漏えいから常に保護されます。
- このオプションは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する組織向きです。
- クローズドポリシーは、特に有効にしない限り、キャプティブ ポータルを修復しません。

- クライアントプロファイルで[最新のVPNローカルリソースを適用（Apply Last VPN Local Resources）]が有効になっている場合は、直近のVPNセッションにより適用されたローカル リソース ルールを適用できます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。
- AnyConnectソフトウェアのアップグレード中、Always-Onが有効であると、ネットワークはクローズドポリシーに関係なくブロックが解除され、開かれます。
- クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープンポリシーを使用してAlways-Onを展開し、ユーザーを通じてAnyConnectがシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPNユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワークアクセスの制限についても周知してください。

注意 AnyConnectがVPNセッションの確立に失敗した場合は、接続障害クローズドポリシーによりネットワークアクセスは制限されます。接続障害クローズドポリシーは、細心の注意を払って実装してください。

接続障害ポリシーの設定

Always-On機能を有効にする場合にのみ、接続障害ポリシーを設定します。デフォルトでは、接続障害ポリシーはクローズされており、VPNが到達不能な場合にはインターネットにアクセスできません。この状況でインターネットへのアクセスを許可するには、オープンするように接続障害ポリシーを設定する必要があります。

手順

ステップ1 VPNプロファイル エディタを開き、ナビゲーション ペインから[プリファレンス（Part 2）（Preferences (Part 2)）]を選択します。

ステップ2 [接続エラーポリシー（Connect Failure Policy）]パラメータを次のいずれかに設定します。

- [クローズド（Closed）]：（デフォルト）セキュア ゲートウェイに接続できない場合、ネットワーク アクセスが制限されます。
- [オープン（Open）]：クライアントがセキュア ゲートウェイに接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。

ステップ3 クローズド ポリシーを指定した場合は、次の手順を実行します。

a) キャプティブ ポータル修復の設定。

b) ネットワーク アクセスが無効になっている間、最後の VPN セッションのローカル デバイス ルールを保持する場合は、[最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] を選択します。

キャプティブポータルホットスポットの検出と修復の使用

キャプティブ ポータルについて

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、キャプティブ ポータルと呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。キャプティブポータルの検出はこの制限を認識することであり、キャプティブ ポータル修復はネットワーク アクセスを取得するためにキャプティブ ポータルのホットスポット要件を満たすプロセスです。

キャプティブポータルは、VPN 接続が開始されると AnyConnect によって自動的に検出され、追加設定は必要ありません。また、AnyConnect は、キャプティブポータルの検出中にブラウザの設定を変更せず、キャプティブポータルを自動的に修復しません。修復は、エンドユーザーが実行します。AnyConnect は、現在の設定に応じてキャプティブポータルの検出に対応します。

- Always-On が無効の場合、または Always-On が有効で接続障害ポリシーが開いている場合、各接続試行時に次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
 You need to log on with the service provider before you can establish a VPN session.
 You can try this by visiting any website with your browser.
```

エンドユーザは、ホットスポットプロバイダーの要件を満たすことで、キャプティブ ポータル修復を実行する必要があります。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

- Always-On が有効で、接続障害ポリシーが閉じている場合、キャプティブ ポータル修復を明示的に有効にする必要があります。有効の場合、エンドユーザは修復を前述のように実行できます。無効の場合、各接続試行時に次のメッセージが表示され、VPN に接続できません。

```
The service provider in your current location is restricting access to the Internet.
 The AnyConnect protection settings must be lowered for you to log on with the service
 provider. Your current enterprise security policy does not allow this.
```

キャプティブ ポータル修復の設定

Always-On 機能を有効にし、接続障害ポリシーをクローズドに設定する場合にのみ、キャプティブ ポータル修復を設定します。この場合、キャプティブポータルのために VPN に接続できないときは、キャプティブポータル修復を設定すると、AnyConnect は VPN に接続できます。

（注） このプラットフォームでは常時接続がサポートされていないため、キャプティブ ポータルの修復の設定は Linux に適用されません。したがって、プロファイル エディタでの [キャプティブ ポータルの修復を常に許可（Allow Captive Portal Remediation Aloways On）] の設定に関係なく、Linux ユーザはキャプティブ ポータルを修復できます。

接続障害ポリシーがオープンに設定されているか、またはAlways-Onが有効でない場合、ユーザーはネットワークアクセスが制限されないため、AnyConnect VPN プロファイルに特定の設定がなくてもキャプティブポータルを修復できます。

デフォルトでは、セキュリティを最大化するために、常時接続をサポートしているプラットフォーム（Windows と macOS）上ではキャプティブポータルの修復は無効になっています。AnyConnectは、キャプティブポータル修復フェーズ中のデータ漏洩保護機能を提供しません。データ損失保護が必要な場合は、関連するエンドポイントセキュリティ製品を使用する必要があります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [キャプティブ ポータルの修復を許可（Allow Captive Portal Remediation）] **.**を選択します。

この設定は、クローズ接続障害ポリシーによるネットワーク アクセス制限を解除します。

ステップ 3 修復タイムアウトを指定します。

AnyConnect がネットワークアクセス制限を解除する時間（分単位）を入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

キャプティブ ポータルの修復の強化（Windows のみ）

キャプティブポータルの修復が強化され、AnyConnect によって制限されているネットワークアクセス（常時接続などによる）を伴うキャプティブポータルが検出されるたびに、AnyConnect の組み込みブラウザを使用して修復が実行されます。その他のアプリケーションは、AnyConnect ブラウザでのキャプティブ ポータルの修復が保留中の間、ネットワーク アクセスがブロックされたままになります。ユーザはAnyConnectブラウザを閉じて、外部ブラウザにフェールオー

バーできます（プロファイルで有効になっている場合）。これにより、AnyConnect は通常のキャプティブ ポータルの修復動作に戻ります。その場合に、次のメッセージが表示されます。

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

キャプティブ ポータルが検出されたものの、ネットワーク アクセスが AnyConnect によって制限されている場合、AnyConnect ブラウザが自動的に起動し、ユーザに修復を求める次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the internet. You
 need to log on with the service provider before you establish a VPN session, using the
 AnyConnect browser.
```

キャプティブ ポータルの修復の設定ブラウザのフェールオーバー

キャプティブポータルの修復のために AnyConnect ブラウザが起動するたびに適用されるようにブラウザのフェールオーバーを設定することができます。ブラウザのフェールオーバーを設定することで、ユーザーは AnyConnect ブラウザを閉じた後に外部ブラウザを介してキャプティブポータルを修復できます。

キャプティブポータルの修復のために起動した AnyConnect ブラウザには、サーバーセキュリティ証明書に関して厳密なセキュリティ設定が備わっています。キャプティブ ポータルの修復中は、信頼されていないサーバ証明書は受け入れられません。信頼できないサーバー証明書が検出されると、対応する HTTPS URL が AnyConnect ブラウザによってロードされず、修復プロセスがブロックされる可能性があります。キャプティブ ポータルの修復中に信頼できないサーバ証明書が受け入れられる場合は、キャプティブ ポータルの修復ブラウザのフェールオーバーを有効にしてユーザがキャプティブ ポータルを修復できるようにする必要があります。有効にすると、ユーザーは AnyConnect ブラウザを閉じ、（AnyConnect は通常のキャプティブ ポータルの修復動作に戻るため）外部ブラウザを使用して修復を継続することができます。

始める前に

Windows および macOS でサポートされています。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 エンドユーザーが（AnyConnect ブラウザを閉じた後）キャプティブポータルの修復に外部ブラウザを使用させる場合は、[キャプティブポータルの修復ブラウザのフェールオーバー（Captive Portal Remediation Browser Failover）] をオンにします。デフォルトでは、エンドユーザーは AnyConnect ブラウザを使用してキャプティブポータルの修復のみを行えます。つまり、ユーザーは強化されたキャプティブポータルの修復を無効にすることはできません。

キャプティブ ポータルの検出と修復のトラブルシューティング

次のような状況では、AnyConnect は誤ってキャプティブポータルと見なされる場合があります。

- サーバー名が正しくない証明書（CN）を持った Cisco Secure Firewall ASA に接続しようとしている場合、AnyConnect は、その環境を「キャプティブポータル」環境と見なします。

  これを回避するには、Cisco Secure Firewall ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアントプロファイルの Cisco Secure Firewall ASA サーバーの名前と一致する必要があります。

- Cisco Secure Firewall ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる Cisco Secure Firewall ASA への接続に応答すると、AnyConnect は、その環境を「キャプティブポータル」環境と見なします。これは、ユーザーが内部ネットワークに存在し、ファイアウォールを介して Cisco Secure Firewall ASA に接続している場合に発生する可能性があります。

  企業内から Cisco Secure Firewall ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。Cisco Secure Firewall ASA への HTTP/HTTPS アクセスは許可するか、完全にブロックし、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、次のことを試すようにユーザに指示してください。

- 修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP フォン クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。

  キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、DoS 攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

- ネットワーク インターフェイスを無効にした後、再度有効にします。このアクションにより、キャプティブ ポータルの検出が再試行されます。

- コンピュータを再起動します。

L2TP または PPTP を介した AnyConnect の設定

一部の国の ISP では、Layer 2 Tunneling Protocol（L2TP）や Point-to-Point Tunneling Protocol（PPTP）のサポートが必要です。

セキュアゲートウェイを宛先としたトラフィックを Point-to-Point Tunneling Protocol（PPP）接続上で送信するため、AnyConnect は外部トンネルが生成したポイントツーポイント アダプタを使用します。PPP 接続上で VPN トンネルを確立する場合、クライアントでは Cisco Secure

Firewall ASA より先を宛先としてトンネリングされたトラフィックから、この Cisco Secure Firewall ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、除外ルートを特定する方法を指定する場合は、AnyConnect プロファイルの [PPP 除外（PPP Exclusion）] 設定を使用します。除外ルートは、セキュアでないルートとして AnyConnect GUI の [ルートの詳細（Route Details）] 画面に表示されます。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [PPP 除外（PPP Exclusion）] でその方式を選択します。また、このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザがこの設定を表示および変更できるようにします。

- [自動（Automatic）]：PPP 除外を有効にします。AnyConnect は、PPP サーバーの IP アドレスを自動的に決定します。
- [オーバーライド（Override）]：[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで指定された定義済みのサーバー IP アドレスを使用して PPP 除外を有効にします。[PPP 除外サーバーIP（PPP Exclusion Server IP）] フィールドは、このオーバーライド方式にのみ適用され、[自動（Automatic）] オプションで PPP サーバーの IP アドレスを検出できない場合にのみ使用する必要があります。

  [PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで [ユーザ制御可（User Controllable）] をオンにすると、エンドユーザーは preferences.xml ファイルを使用して IP アドレスを手動で更新できます。「ユーザに対する PPP 除外上書きの指示（153 ページ）」セクションを参照してください。
- [無効（Disabled）]：PPP 除外は適用されません。

ユーザに対する PPP 除外上書きの指示

自動検出が機能しない場合に、PPP 除外フィールドをユーザー設定可能に設定すると、ユーザーはローカルコンピュータ上で AnyConnect プリファレンスファイルを編集することにより、これらの設定を上書きすることができます。

手順

ステップ 1 メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows：%LOCAL_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。次に例を示します。

- macOS：/Users/username/VPN/.anyconnect
- Linux：/home/username/VPN/.anyconnect

ステップ 2 PPPExclusion の詳細を <ControllablePreferences> の下に挿入して、Override 値と PPP サーバーの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3 ファイルを保存します。

ステップ 4 AnyConnect を終了し、リスタートします。

管理 VPN トンネルの使用

管理 VPN トンネルについて

管理 VPN トンネルにより、エンドユーザによって VPN 接続が確立されるときだけでなく、クライアント システムの電源が入るたびに社内ネットワークの接続が確保されます。オフィス ネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内ネットワークの接続を必要とするエンドポイント OS ログイン スクリプトに対するメリットもあります。

管理 VPN トンネルはエンドユーザに対し透過的であるため、ユーザ アプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

管理トンネル機能が有効として検出されると、制限付きのユーザアカウント（ciscoacvpnuser）が作成され、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。

ログインが低速であるとユーザから報告された場合、管理トンネルが適切に設定されていない可能性があります。「管理 VPN トンネルの設定（157 ページ）」で、この機能を有効にするのに必要な設定手順について説明します。この設定を行ったにもかかわらず、社内ネットワークへの接続ができない症状が出ている場合は、「管理 VPN トンネル接続問題のトラブルシューティング」を参照してください。

管理 VPN トンネルの互換性と要件

- ASDM 9.0.1（またはそれ以降）および ASDM 7.10.1（またはそれ以降）が必要です。

- ユーザ ログインの前後にユーザによって開始された VPN トンネルが切断されるたびに接続します。

（注） 信頼ネットワーク検出（TND）機能によって信頼ネットワークが検出されるか、AnyConnect ソフトウェアアップデートが進行中の場合、管理 VPN トンネルは確立されません。

- ユーザ ログインの前後にユーザが VPN トンネルを開始するたびに切断します。
- マシン ストア証明書認証のみを使用します。
- ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンドユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作をオーバーライドする場合は、「Tunnel-All 設定をサポートするカスタム属性の設定 （159 ページ）」を参照してください。
- サーバ証明書に対して厳密な証明書のチェックを実行します。サーバー証明書のルート CA 証明書は、マシン証明書ストア（Windows の場合はコンピュータ証明書ストア、macOS の場合はシステム キーチェーンまたはシステム ファイル証明書ストア）に存在する必要があります。
- バックアップ サーバ リストで作業します。
- 現在 Windows および macOS でのみ入手可能です。以降のリリースでは、Linux のサポートが追加されます。

管理 VPN トンネルの非互換性と制限

- 管理 VPN プロファイルはプロキシ設定の値 [ネイティブ（Native）] をサポートしていません。この制限は、管理 VPN トンネルはユーザがログインしていなくても開始できるため、 Windows クライアントにのみ適用されます。 そのため、ユーザ固有のブラウザ プロキシ設定に依存することはできません。
- 管理 VPN プロファイルは、VPN サーバからプッシュされるプライベート プロキシ設定をサポートしません。管理 VPN トンネルはエンド ユーザに対して透過的であることを目的としているため、ユーザ固有の設定またはシステム プロキシ設定は変更されません。
- ユーザの VPN トンネルが非アクティブになるたびに管理 VPN トンネルが確立されるため、Always On 機能と互換性はありません。ただし、すべてのトラフィックをトンネリングするように管理トンネル接続のグループ ポリシーを設定して、ユーザの VPN トンネルが非アクティブの間にトラフィックが物理インターフェイスによってリークされないようにすることができます。「Tunnel-All 設定をサポートするカスタム属性の設定 （159 ページ）」を参照してください。
- キャプティブポータルの修復は、AnyConnect UI が実行中でユーザーがログインしている間、管理 VPN トンネル機能が有効になっていなかったかのようであるときにのみ実行されます。

- 管理VPNプロファイルの設定は、管理VPNトンネルがアクティブのときにのみAnyConnectで適用されます。管理VPNトンネルが切断されると、ユーザのVPNトンネルプロファイル設定のみが適用されます。このため、管理VPNトンネルはユーザのVPNトンネルプロファイルの信頼ネットワーク検出（TND）設定（つまり、設定済みの信頼できないネットワーク ポリシーに関係なくTNDが無効化されるか、「信頼できないネットワーク」が検出された場合）に従って開始されます。また、管理VPNプロファイルにおけるTND接続アクションは（管理VPNトンネルがアクティブである場合にのみに適用）、管理VPNトンネルがエンドユーザに対して透過的であるように常にユーザのVPNトンネルに適用されます。ユーザエクスペリエンスに一貫性をもたせるために、ユーザと管理の両方のVPNトンネルプロファイルで同じTND設定を使用する必要があります。

管理 VPN プロファイルによって適用される必須設定

特定のプロファイル設定は管理VPNトンネルがアクティブである間は必須です。有効なプロファイルの設定をサポートするために、対応するUI制御を無効にすることで、AnyConnect管理VPNプロファイルエディタにより必須設定が適用されます。主に、ユーザのインタラクションを排除してトンネルの中断を最小限に抑えるために、管理トンネルの接続中に次の設定値が上書きされます。

- *AllowManualHostInput: false*：管理トンネル (ヘッドレス クライアント) に関連しません。
- *AlwaysOn: false*：管理トンネルが切断されるたびにユーザのトンネル プロファイル設定が適用されるため、関連しません。
- *AutoConnectOnStart: false*：以前に接続されたホストに対する起動時の自動接続用UIクライアントにのみ関連します。
- *AutomaticCertSelection: true*：証明書の選択ポップアップを回避します。
- *AutoReconnect: true*：ネットワークの変更時に管理トンネルが終了するのを回避します。
- *AutoReconnectBehavior: ReconnectAfterResume*：ネットワークの変更時に管理トンネルの終了を回避します。
- *AutoUpdate: false*：管理トンネル接続中にソフトウェア アップデートは実行されません。
- *BlockUntrustedServers: true*： 信頼できないサーバ証明書のプロンプトを回避します。
- *CertificateStore: MachineStore*：管理トンネル認証はログイン ユーザなしでも成功する必要があります。
- *CertificateStoreOverride: true*：Windowsでのマシン証明書認証に必要です。
- *EnableAutomaticServerSelection: false*：管理VPNプロファイルではホスト エントリは1つのみです。
- EnableScripting: false：AnyConnectカスタマイゼーション スクリプト（接続時または切断時に呼び出される）は管理トンネル接続中は実行されません。
- *MinimizeOnConnect:false*：管理トンネル（ヘッドレス クライアント）に関連しません。

- *RetainVPNOnLogoff:true*: 管理トンネルはユーザがログオフしてもアクティブなままである必要があります。
- *ShowPreConnect Message*：管理トンネル（ヘッドレス クライアント）に関連しません。
- *UserEnforcement: AnyUser*：特定のユーザがログインしたときに管理トンネルが切断されないようにします。
- *UseStartBeforeLogon:False*：ユーザ トンネルにのみ適用されます。
- *WindowsVPNEstablishment: AllowRemote* ユーザ：どのユーザ タイプ（ローカルまたはリモート）がログインしても管理トンネルが影響されないようにします。
- [LinuxVPNEstablishment：リモート ユーザを許可（LinuxVPNEstablishment: Allow Remote Users）]：管理トンネルがどのタイプ（ローカル/リモート）のユーザによっても影響されないようにします。

また、AnyConnect では、管理トンネルの接続中は、WindowsLogonEnforcement および SCEP 関連の設定はプロファイル設定として適用されません。

管理 VPN トンネルの設定

ユーザがログインしていなくても管理トンネル接続が発生する場合があるため、マシン ストア証明書認証のみがサポートされます。したがって、少なくとも 1 つの関連するクライアント証明書がクライアント ホストのマシン証明書ストアで使用できる必要があります。

管理 VPN トンネルのトンネル グループの設定

トンネルグループの認証方法は、ASDM で**[設定（Configuration）]>[リモートアクセス（Remote Access）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）]>[AnyConnect 接続プロファイル（AnyConnect Connection Profiles）]>[追加/編集（Add/Edit）]** に移動し、[証明書のみ（certificate only）] として設定する必要があります。次に、[詳細設定（Advanced）]>[グループ エイリアス/グループ URL（Group Alias/Group URL）] でグループ URL を設定してから、次に 「管理 VPN トンネルのプロファイルの作成 （158 ページ）」の説明に従って管理 VPN プロファイルで指定します。

このトンネル グループのグループ ポリシーには、トンネル グループで設定されたクライアント アドレスの割り当てを使用するすべての IP プロトコルに対して split include トンネリングが設定されている必要があります（ASDM から [下記のネットワーク リストをトンネル（Tunnel Network List Below）] には**[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）]>[編集（Edit）]>[詳細設定（Advanced）>[スプリット トンネリング（Split Tunneling）]を選択）**。「Tunnel-All 設定をサポートするカスタム属性の設定 （159 ページ）」では、その他のスプリット トンネリング設定のサポートを有効にする方法について説明します。両方の IP プロトコルに対するトンネル グループでクライアント アドレスの割り当てが設定されていない場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] を有効にし、クライアント アドレスの割り当てのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。

管理 VPN トンネルのプロファイルの作成

特定のクライアント デバイスには、1 つの管理 VPN プロファイルのみを展開できます。管理 VPN プロファイルは固定名（VpnMgmtTunProfile.xml）で専用ディレクトリ（Windows では %ProgramData%\Cisco\Cisco AnyConnect Secure MobilityClient\Profile\MgmtTun、macOS では /opt/cisco/anyconnect/profile/mgmttun）に格納されます。管理 VPN プロファイルには、「管理 VPN トンネルのトンネル グループの設定（157 ページ）」セクションに従って設定されたトンネル グループを指しているゼロまたは 1 つのホスト エントリを使用できます。（トンネル確立中のプロファイルの更新時に）この機能を自動的に無効にするには、管理 VPN プロファイルでゼロのホスト エントリを設定する必要があります。

始める前に

管理 VPN トンネルのトンネル グループの設定（157 ページ）を完了します。

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 [追加（Add）] をクリックします。[AnyConnect クライアントプロファイルの追加（Add AnyConnect Client Profiles）] ウィンドウが表示されます。

ステップ 3 プロファイルの使用方法として、[AnyConnect 管理 VPN プロファイル（AnyConnect Management VPN Profile）] を選択します。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profiles）] 画面でフィールドを読み込む方法の詳細については、『Cisco ASA Series VPN ASDM Configuration Guide』の「Configure AnyConnect Client Profiles」セクションを参照してください。

ステップ 4 「管理 VPN トンネルのトンネル グループの設定（157 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックして管理 VPN プロファイルを作成してから、[編集（Edit）] をクリックして設定します。以降の更新に対しても同様に行います。

（オプション）すでに設定済みの管理 VPN プロファイルをアップロードする

すでに設定済みの管理 VPN プロファイル（スタンドアロン AnyConnect 管理 VPN プロファイル エディタを使用して編集または作成された、AnyConnect からコピーされた、または別の Cisco Secure Firewall ASA からエクスポートされた）を Cisco Secure Firewall ASA にアップロードする必要がある場合があります。

手順

ステップ 1 ASDM で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ウィンドウから [追加（Add）]、[アップロード（Upload）] をクリックします。.

ファイルのアップロードの接続先の場所を選択するには、 *vpnm* 拡張子付きのプロファイルを選択することを確認します。

ステップ 2 プロファイル名を提供し、プロファイルの使用率のドロップダウン メニューから **AnyConnect 管理 VPN プロファイル**を選択します。

ステップ 3 「管理 VPN トンネルのトンネル グループの設定 （157 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックし、管理 VPN プロファイルを作成します。

グループ ポリシーへの管理 VPN プロファイルの関連付け

管理トンネル接続に使用するトンネル グループに関連付けられているグループ ポリシーに管理 VPN プロファイルを追加する必要があります。

（注） 同様に、ユーザ トンネル接続に使用する正規のトンネル グループにマッピングされたグループ ポリシーに管理 VPN プロファイルを追加することもできます。ユーザが接続すると、グループ ポリシーにすでにマッピングされているユーザ VPN トンネルとともに管理 VPN プロファイルがダウンロードされ、管理 VPN トンネル機能が有効になります。

また、アウトオブバンドで管理 VPN プロファイルを展開することができます。その場合、VpnMgmtTunProfile.xml という名前が付いていることを確認し、上記の管理 VPN プロファイル ディレクトリにコピーして、AnyConnect Secure Mobility Client エージェント サービスを再起動（またはリブート）します。

始める前に

「管理 VPN トンネルのトンネル グループの設定 （157 ページ）」と「管理 VPN トンネルのプロファイルの作成 （158 ページ）」を完了します。

手順

ステップ 1 ASDM で **[グループポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）]** に移動します。

ステップ 2 ダウンロードするクライアント プロファイルで、[追加（Add）] をクリックし、「管理 VPN トンネルのプロファイルの作成 （158 ページ）」セクションで作成または更新された管理 VPN プロファイルを選択します。

Tunnel-All 設定をサポートするカスタム属性の設定

管理 VPN トンネルでは、ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンド ユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作は管理トンネル接続で使用されているグループポリシーで次のカスタム属性を設定することによりオーバーライドできます（[CreateCustom 属性 ASDM

（CreateCustom Attribute ASDM）] ウィンドウ：**[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）] > [編集（Edit）] > [詳細設定（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）] > [追加（Add）]**）。

新しいカスタム属性タイプを **ManagementTunnelAllAllowed** に設定し、対応するカスタム属性を *true* に設定すると、その構成が両方の IP プロトコルに対して tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、AnyConnect は管理トンネル接続を続行します。

管理 VPN プロファイルの更新の制限

管理 VPN プロファイルの更新を新しい AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）設定を使用した特定の信頼できるサーバリストに制限しても、ユーザが任意のサーバから VPN プロファイルを更新するのを許可することができます。この設定は、[ローカルポリシー設定（AnyConnect VPN Local Policy Editor）] を使用して [任意のサーバからの管理 VPN プロファイル更新を許可（Allow Management VPN Profile Updates From AnyServer）] チェック ボックスをオンにすることで編集できます。

たとえば、管理 VPN プロファイルの更新が VPN サーバー TrustedServer からのみ許可される場合、このチェックボックスはオフになっており、TrustedServer は信頼できるサーバーリストに追加されます。（TrustedServer を該当する VPN プロファイルのサーバ エントリに存在する FQDN または IP アドレスと置き換えてください）。

管理 VPN トンネル接続問題のトラブルシューティング

クライアント ホストがリモートから到達できない場合、さまざまなシナリオが発生して管理 VPN トンネルの切断や確立できない状況の原因となっている可能性があります。次のシナリオでは、AnyConnect GUI と CLI に管理接続状態が統計情報のエントリとして反映されます。

- [切断（無効）（Disconnected (disabled)）]：機能は無効です。
- [切断（信頼ネットワーク）（Disconnected (trusted network)）]：TND が信頼ネットワークを検出したため、管理トンネルは確立されません。
- [切断（アクティブ ユーザ トンネル）（Disconnected (user tunnel active)）]：ユーザ トンネルは現在保留中 です（つまり、管理トンネルを切断しています）。
- [切断（プロセスの起動に失敗）（Disconnected (process launch failed)）]：管理トンネル接続の試行時にプロセスの起動エラーが発生しました。
- [切断（接続に失敗）（Disconnected (connect failed)）]：管理トンネルの確立時に接続障害が発生しました。
- [切断された（無効な VPN 設定）（Disconnected (invalid VPN configuration)）]：管理トンネルの確立時に無効なスプリットトンネリング設定が発生しました。追加情報については、「Tunnel-All 設定をサポートするカスタム属性の設定 （159 ページ）」を参照してください。

- [切断（ソフトウェアアップデートが保留中）（Diconnected (software update pending)）]：AnyConnect ソフトウェアアップデートは現在保留中です（つまり、管理トンネルを切断しています）。
- [切断（Disconnected）]：管理トンネルを確立しようとしているか、その他の理由により確立できませんでした。

管理 VPN トンネル経由の接続の欠落をトラブルシューティングする場合は（クライアント ホストで確立されることを想定）、次を確認します。

- 管理 VPN 接続の状態を AnyConnect UI の [統計出力のエクスポート（Export Stats output）] の [統計（Statistics）] タブをで確認するか、CLI で [接続情報/管理接続状態（Connection Information/Management Connection State）] を確認します。管理接続状態が予期せずに [切断（disconnected）] と表示され、提供された説明が不十分な場合、詳細なトラブルシューティングについて DART ツールを使用した AnyConnect ログをキャプチャします。
- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、証明書認証で設定されたトンネル グループを指す、1 つのホスト エントリで管理 VPN プロファイルが設定されていることを確認します。関連付けられているグループ ポリシーに 1 つのプロファイル（管理 VPN プロファイル）が設定されている必要があります。

（注） 関連付けられているグループ ポリシーでバナーを有効にすることはできません。管理のトンネル接続中にユーザのインタラクションはサポートされていません。

- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、正規のユーザ トンネル接続で使用されるトンネル グループに関連付けられているグループ ポリシー内で管理 VPN プロファイルが設定されていることを確認します。ユーザがそのトンネル グループに接続すると、管理 VPN プロファイルがダウンロードされ、この機能が有効になります。

（注） また、管理 VPN プロファイルをアウト オブ バンドで展開できます。

- UI の統計行に [管理接続状態：切断（接続に失敗）（Management Connection State: Disconnected (connect failed)）] と表示される場合、次に示すように、管理トンネル接続はユーザのインタラクションが必要な場合に常に失敗することに注意してください。
  - サーバー証明書が信頼されない場合。サーバー証明書のルート CA 証明書は、マシン証明書ストア内に存在する必要があります。
  - （マシン ストア証明書に関連する）秘密キーがパスワードで保護されている場合、対応するクライアント証明書は管理トンネル接続で使用できません。秘密キーのパス

ワードを入力するようユーザにプロンプトを表示できないため、クライアント証明書は使用できません。

- macOS システム キーチェーン プライベート キーが、AnyConnect エージェント実行可能ファイル（vpnagentd）にプロンプトを表示せずにアクセスを許可するように設定されていない場合、秘密鍵にアクセスするためのクレデンシャルをユーザーに要求することができないため、対応するクライアント証明書は管理トンネル接続では使用できません。
- グループ ポリシーがバナーを使用して設定されている場合。

AnyConnect プロキシ接続の設定

AnyConnect プロキシ接続について

AnyConnect は、ローカルプロキシ、パブリックプロキシ、プライベートプロキシで VPN セッションをサポートしています。

- ローカル プロキシ接続：

  ローカルプロキシは、AnyConnect と同じ PC 上で動作し、トランスペアレントプロキシとして使用されることもあります。トランスペアレント プロキシ サービスの例として、一部のワイヤレス データ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェア（Kaspersky など）に搭載のネットワーク コンポーネントなどがあります。

  ローカルプロキシの使用は、AnyConnectプロファイルで有効または無効にします。「ローカル プロキシ接続の許可」を参照してください。

- パブリック プロキシ接続：

  通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。Windows がパブリック プロキシを使用するように設定されている場合、AnyConnect はその接続を使用します。パブリック プロキシは macOS と Linux でネイティブと上書きの両方をサポートしています。

  パブリックプロキシの設定についてパブリック プロキシ （164 ページ）は、を参照してください。

- プライベート プロキシ接続：

  プライベート プロキシ サーバーは、企業の使用ポリシーに基づいて企業ユーザーが特定の Web サイト（たとえば、アダルト、ギャンブル、ゲームなどのサイト）にアクセスできないようにするために社内ネットワークで使用されます。

  トンネルの確立後にブラウザにプライベート プロキシ設定をダウンロードするようにグループ ポリシーを設定します。VPN セッションが終了すると、設定は元の状態に復元されます。プライベート プロキシ接続の設定 （165 ページ）を参照してください。

（注） プロキシサーバーを経由する AnyConnect SBL 接続は、Windows オペレーティングシステムのバージョン、システム（マシン）の設定、またはその他のサードパーティ プロキシ ソフトウェア機能に依存します。このため、Microsoft または使用するすべてのサードパーティプロキシアプリケーションによって提供される、システム全体のプロキシ設定を参照してください。

VPN クライアント プロファイルによるクライアント プロキシの制御

VPN クライアント プロファイルでは、クライアント システムのプロキシ接続をブロックしたり、リダイレクトしたりできます。Windows および Linux の場合、パブリック プロキシ サーバのアドレスを自分で設定したり、ユーザーに設定を許可したりできます。

VPNクライアントプロファイルにプロキシ設定を設定する方法の詳細については、AnyConnect プロファイルエディタ、プリファレンス（Part 2） （98 ページ）を参照してください。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

Cisco Secure Firewall ASA の一部のバージョンでは、AnyConnect セッションの確立後にプロキシサーバーを介したクライアントレス ポータル アクセスをサポートするため、AnyConnect 設定を作成する必要があります。AnyConnect は、プロキシ自動構成（PAC）ファイルを使用して、クライアント側のプロキシ設定を変更して、これを実行できるようにします。AnyConnect は、Secure Firewall ASA がプライベート側のプロキシ設定を指定しない場合にのみ、このファイルを生成します。

AnyConnect プロキシ接続の要件

プロキシ接続の OS サポートは次のようになります。

プロキシ接続タイプ	Windows	macOS	Linux
ローカル プロキシ	○	○（上書きおよびネイティブ）	○
プライベートプロキシ	○（Internet Explorer）	○（システム プロキシ設定として設定）	×
パブリック プロキシ	○（IE および上書き）	○（上書きおよびネイティブ	○（上書きおよびネイティブ）

プロキシ接続の制限

- プロキシ経由の接続は、Always-On機能が有効になっている場合にはサポートされません。

- ローカル プロキシへのアクセスを許可するには、VPN クライアント プロファイルが必要です。

ローカル プロキシ接続の許可

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [ローカル プロキシ接続を許可（Allow Local Proxy Connections）] を選択（デフォルト）または選択解除します。ローカル プロキシはデフォルトで無効になっています。

パブリック プロキシ

パブリック プロキシは Windows および Linux の各プラットフォームでサポートされています。プロキシ サーバは、クライアント プロファイルで設定されるプリファレンスに基づいて選択されます。プロキシオーバーライドの場合、AnyConnect はプロファイルからプロキシサーバーを取得します。リリース 4.1 以降では、Linux および macOS でのネイティブプロキシ構成とともに macOS でのプロキシサポートが追加されました。

Linux では、AnyConnect の実行前にネイティブプロキシ設定がエクスポートされます。設定を変更した場合は、再起動が必要です。

プロキシサーバーの認証には、ユーザー名とパスワードが必要です。AnyConnect は、プロキシサーバーが認証を要求するように構成されている場合、基本認証と NTLM 認証をサポートします。AnyConnectダイアログは認証プロセスを管理します。プロキシサーバーに対する認証に成功すると、AnyConnect は Cisco Secure Firewall ASA ユーザー名およびパスワードの入力を求めます。

パブリック プロキシ接続の設定（Windows）

Windows でパブリック プロキシ接続を設定するには、次の手順を実行します。

手順

ステップ 1 Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。

ステップ 2 [接続（Connections）] タブを選択し、[LAN 設定（LAN Settings）] ボタンをクリックします。

ステップ 3 プロキシ サーバを使用するように LAN を設定し、プロキシ サーバの IP アドレスを入力します。

パブリック プロキシ接続の設定（macOS）

手順

ステップ 1 システム設定に移動し、接続している適切なインターフェイスを選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 新しいウィンドウで [プロキシ（Proxies）] タブを選択します。

ステップ 4 HTTPS プロキシを有効にします。

ステップ 5 右側のパネルの [セキュアプロキシサーバ（Secure Proxy Server）] フィールドに、プロキシ サーバのアドレスを入力します。

パブリック プロキシ接続の設定（Linux）

Linux でパブリック プロキシ接続を設定するには、環境変数を設定します。

プライベート プロキシ接続の設定

手順

ステップ 1 Cisco Secure Firewall ASA グループポリシーにプライベートプロキシ情報を設定します。『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「Configuring a Browser Proxy for an Internal Group Policy」の項を参照してください。

（注） macOS 環境では、（VPN 接続時に）Cisco Secure Firewall ASA からプッシュダウンされたプロキシ情報は、端末を開いて **`scutil --proxy`** を発行するまで、ブラウザに表示されません。

ステップ 2 （任意）ブラウザのプロキシ設定を無視するためのクライアントの設定。

ステップ 3 （任意）Internet Explorer の [接続（Connections）] タブのロックダウン。

ブラウザのプロキシ設定を無視するためのクライアントの設定

AnyConnect プロファイルでは、ユーザーの PC 上で Microsoft Internet Explorer または Safari のプロキシ設定が無視されるようにポリシーを指定できます。これにより、ユーザーは社内ネットワークの外部からトンネルを確立できなくなり、AnyConnect は望ましくないまたは違法なプロキシサーバー経由で接続できなくなります。

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [プロキシ設定（Proxy Settings）] ドロップダウン リストで、[プロキシを無視（Ignore Proxy）] を選択します。[プロキシを無視（Ignore Proxy）] を選択すると、クライアントはすべてのプロキシ設定を無視します。Cisco Secure Firewall ASA からダウンロードされるプロキシに対してアクションが実行されません。

Internet Explorer の [接続（Connections）] タブのロックダウン

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。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は接続解除すると反転され、このタブに適用される管理者定義のポリシーの方が優先されます。このロックダウンは、次のいずれかの条件で行われます。

- 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）。

グループポリシーで、プロキシのロックダウンを許可する、または許可しないように Cisco Secure Firewall ASA を設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

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 プロキシのロックダウンを有効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections）] タブを非表示にするには、[継承（Inherit）] をオフにして [はい（Yes）] を選

択します。または、プロキシのロックダウンを無効にして、AnyConnect のセッション中は Internet Explorer の [接続（Connections）] タブを表示するには、[いいえ（No）] を選択します。

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。

プロキシ設定の確認

- Windows の場合：次の場所でレジストリのユーザーおよびシステムのプロキシ設定を検索します。

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections
```

- macOS の場合：ターミナル ウィンドウを開き、次を入力します。

```
scutil --proxy
```

VPN トラフィックの選択および除外

VPN をバイパスするための IPv4 または IPv6 トラフィックの設定

ASA が IPv6 トラフィックのみを待機している場合は AnyConnect が IPv4 トラフィックをどのように管理するかを設定し、Cisco Secure Firewall ASA がClient Bypass Protocol 設定を使用して IPv4 トラフィックのみを待機している場合は AnyConnect クライアントが IPv6 トラフィックをどのように管理するかを設定できます。

AnyConnectで Cisco Secure Firewall ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

Client Bypass Protocol が IP プロトコルに対して有効であり、かつ、あるアドレスプールがそのプロトコルに対して設定されていない（つまり、そのプロトコルの IP アドレスが Cisco Secure Firewall ASA によってクライアントに割り当てられていない）場合、そのプロトコルを使用する IP トラフィックは VPN トンネルを介して送信されません。これは、トンネル外で送信されます。

クライアント バイパス プロトコルが無効であり、かつ、あるアドレス プールがそのプロトコル用に設定されていない場合、VPN トンネルが確立された後、クライアントではその IP プロトコルのすべてのトラフィックをドロップします。

たとえば、Cisco Secure Firewall ASA が AnyConnect 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされていると想定します。エンドポイントが IPv6 アドレスへの到達を試みた場合、クライアント バイパス プロトコルが無効になっていると、IPv6 トラ

フィックはドロップされます。クライアントバイパスプロトコルが有効になっていると、IPv6 トラフィックはクライアントからクリア テキストで送信されます。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうかが Cisco Secure Firewall ASA に通知されないため、Cisco Secure Firewall ASA は常に Client Bypass Protocol 設定をプッシュダウンします。

Client Bypass Protocol を Cisco Secure Firewall ASA でグループポリシーに設定します。

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 **[詳細（Advanced）] > [AnyConnect]** を選択します。

ステップ 4 デフォルト グループ ポリシー以外のグループ ポリシーの場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] の隣にある [継承（Inherit）] チェックボックスをオフにします。

ステップ 5 次のオプションのいずれかを選択します。

- Cisco Secure Firewall ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[無効（Disable）] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[有効（Enable）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [適用（Apply）] をクリックします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定

『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「Client Firewall with Local Printer and Tethered Device Support」の項を参照してください。

スプリット トンネリングの設定

スプリット トンネリングは、[ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定します。『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「Configure Split Tunneling for AnyConnect Traffic」の項を参照してください。

ASDM でグループ ポリシーに変更を加えたら、**[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 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）]** で、グループ ポリシーを接続プロファイルに関連付けてください。

Linux でのネットワークトラフィックのルーティング

Linuxユーザーが VMインスタンス/Dockerコンテナでネットワークトラフィックをルーティングできるようにするには、新しいカスタム属性を作成して有効にする必要があります。**tunnel-from-any-source** カスタム属性を作成し、*true* に設定すると、AnyConnect は、split-include または split-exclude トンネルモードの任意の送信元アドレスを持つパケットを許可し、VM インスタンスまたは Docker コンテナ内のネットワークアクセスを許可します。

（注） VM インスタンスまたは Docker コンテナで使用されるネットワークは、最初にトンネルから除外する必要があります。

ダイナミック スプリット トンネリングについて

ダイナミック スプリット トンネリングは、ASDM グループ ポリシー設定で [次のネットワークリストを除外（Exclude Network List Below）] または [次のネットワークリストをトンネリング（Tunnel Network List Below）] オプションを使用して設定される現在のスプリット トンネリング オプションを強化するために設計されました。スプリット トンネリングを定義するために通常使用される静的な包含または除外と違い、ダイナミック スプリット トンネリングでの包含または除外は、特定のサービスに関するトラフィックを VPN トンネリングから除外するまたは VPN トンネリングに包含する必要があるシナリオに対応しています。IP プロトコルごとに個別のスプリットトンネリング設定を構成できません。たとえば、IPv4にダイナミックスプリット包含トンネリング（IPv4 スプリット包含ドメインやダイナミックスプリット包含ドメインなど）を有効にすると、IPv6にダイナミックスプリット除外トンネリング（IPv6 Tunnel-allやダイナミックスプリット除外ドメインなど）を有効にできません。さらに、拡張ダイナミック スプリットトンネリングを提供します。ダイナミックスプリット除外ドメインとダイナミックスプリット包含ドメインの両方が拡張ドメイン名の一致に指定されています。

制限は、スタティック スプリット トンネリングからダイナミック スプリット トンネリングまでさまざまです。スタティック スプリット トンネリングの場合、IP プロトコルあたり 2500 ネットワーク/ACEに制限されます。ダイナミック スプリット トンネリングでは、制限は5000文字（約 400 ドメイン名）になり、クライアントでは切り捨てによってのみ適用されます。

ダイナミック スプリット除外トンネリング：複数のクラウド ベースのサービスが同じ IP プールにホストされており、ユーザの場所またはクラウド上のコンピュータ資源の負荷に応じて異なる IP アドレスへと解決される場合があります。そのようなサービスのうち 1 つだけを VPN トンネルから除外したい場合、管理者が静的な除外を使用してそのためのポリシーを定義するのは、特に ISP NAT、6to4、4to6 などのネットワーク変換スキームも考慮される場合は困難です。ダイナミック スプリット除外トンネリングでは、トンネルの確立後に、ホストの DNS ド

メイン名に基づいて動的にスプリット除外トンネリングをプロビジョニングできます。たとえば、VPN管理者は、実行時にexample.comをVPNトンネルから除外するように設定できます。VPNトンネルがアップしているときにアプリケーションがmail.example.comに接続しようとすると、VPNクライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、トンネル外部への接続を許可します。

拡張ダイナミックスプリット除外トンネリング：ダイナミックスプリット除外トンネリングがダイナミックスプリット除外ドメインとダイナミックスプリット包含ドメインの両方で設定されている場合、VPN トンネルから動的に除外されたトラフィックは少なくとも 1 つのダイナミックスプリット除外ドメインに一致する必要がありますが、ダイナミックスプリット包含ドメインに一致する必要はありません。たとえば、VPN 管理者がダイナミック スプリット除外ドメイン example.com とダイナミック スプリット包含ドメイン mail.example.com を設定した場合、mail.example.com 以外のすべての example.com トラフィックはトンネリングから除外されます。

ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。たとえば、VPN管理者は、実行時にdomain.comをVPNトンネルに含めるように設定できます。VPNトンネルがアップしているときにアプリケーションがwww.domain.comに接続しようとすると、VPNクライアントは、自動的にシステムルーティング テーブルとフィルタを変更し、VPN トンネル内部での接続を許可します。

拡張ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、VPNトンネルに動的に包含されたトラフィックは少なくとも1つのダイナミック スプリット包含ドメインに一致する必要がありますが、ダイナミック スプリット除外ドメインに一致する必要はありません。たとえば、VPN 管理者が domain.com をスプリット包含ドメインとして、www.domain.com をスプリット除外ドメインとして設定した場合、www.domain.com 以外のすべての domain.com トラフィックがトンネリングされます。

（注） ダイナミック スプリット トンネリングは、Linux またはモバイルプラットフォームではサポートされていません。

スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性

静的な除外と動的な除外は共存可能です。スタティック スプリット トンネリングはトンネルの確立時に適用され、ダイナミック スプリット トンネリングは、トンネルが接続済みとなっているときにドメインへのトラフィックが発生すると適用されます。

ダイナミック スプリット除外トンネリング

ダイナミック スプリット除外トンネリングは、「tunnel all」、「split include」、および「split exclude」トンネリングに適用されます。

- すべてのネットワークをトンネリングする：VPN トンネルからの除外は、すべて動的です。
- 特定のネットワークを除外する：事前設定された静的な除外に動的な除外が追加されます。
- 特定のネットワークを包含する：除外されるホスト名の IP アドレスのうち、スプリットを含むネットワークと重複する場合のみ、動的な除外が適用されます。それ以外の場合、トラフィックは VPN トンネルからすでに除外されているため、動的な除外は行われません。

拡張ダイナミック スプリット除外トンネリングは、「tunnel all」および「split exclude」トンネリングに適用されます。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方、およびスプリット包含トンネリングが設定されている場合、その結果の設定は拡張ダイナミック スプリット包含トンネリングになります。

ダイナミック スプリット包含トンネリング

ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

拡張ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

（注） Umbrella ローミング セキュリティによる保護は、スタティックまたはダイナミック スプリット トンネリングのいずれかが有効になっていると、アクティブになります。Umbrella クラウド リゾルバは、到達可能であり、かつ、VPN トンネルによるプローブが可能である場合を除き、VPN トンネルから静的に包含または除外することが必要となる場合があります。

スプリット トンネリング設定をともなう重複シナリオの結果

動的な包含または除外の対象は、まだ包含または除外されていない IP アドレスのみです。静的トンネリングおよび何らかの形式の動的トンネリングの両方が適用されており、新たな包含または除外を強制する必要がある場合、すでに適用された包含または除外との衝突が発生する可能性があります。動的な除外（除外されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、除外において考慮されるのは、まだ除外されていないアドレスのみです。同様に、動的な包含（包含されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、包含において考慮されるのは、まだ包含されていないアドレスのみです。

静的なパブリック ルート（セキュア ゲートウェイ ルートなどのスプリット除外ルートやクリティカル ルートなど）は、ダイナミック スプリット包含ルートよりも優先されます。そのため、動的な包含の少なくとも 1 つの IP アドレスが静的なパブリック ルートと一致する場合、動的な包含は強制されません。

同様に、静的スプリット包含ルートはダイナミック スプリット除外ルートよりも優先されます。そのため、動的な除外の少なくとも 1 つの IP アドレスが静的スプリット包含ルートと一致する場合、動的な除外は強制されません。

ダイナミック スプリット トンネリングの使用状況の通知

VPN トンネルの接続中は、ダイナミック スプリット トンネリングに何が設定されているかをいくつかの方法で確認できます。

- [統計（Statistics）] タブ：Cisco Secure Firewall ASA グループポリシーで設定されている VPN トンネルから除外された、または VPN トンネルに包含されたドメイン名を含むダイナミック トンネル除外およびダイナミック トンネル包含が表示されます。
- [エクスポート統計（Export Stats）]：VPN トンネリングから除外された、または VPN トンネリングに包含されたドメイン名と、IPv4 と IPv6 の両方のトンネル モードを含むファイルが生成されます。ダイナミック ルートもエクスポートされた統計に含まれます。
- [ルートの詳細（Route Details）] タブ：除外または包含された各 IP アドレスに対応するホスト名を持つ IPv4 および IPv6 ダイナミック スプリット除外および包含ルートが表示されます。

（注） AnyConnect UI には、AnyConnect VPN が実現する保護されたルートまたは保護されていないルートが、IP プロトコルにつき最大 200 個表示されます。ルートの数が 200 を超えると、切り捨てが発生します。すべてのルートを表示するには、Windows では **route print** を実行し、Linux または macOS では **netstat -rn** を実行します。

- VPN の設定ログ メッセージ：VPN トンネルから除外された、または VPN トンネルに包含されたドメインの数が示されます。

ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （169 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、Cisco Secure Firewall ASA 上でカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』の「*Configure Dynamic Split Tunneling*」を参照してください。

手順

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

ステップ 2 VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。この属性値には、VPN トンネルから除外するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com,
 example2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value example_service_domains
```

拡張ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （169 ページ） を参照してください。

ダイナミック スプリット除外トンネリングがダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミックスプリット除外トンネリングを設定するには、Cisco Secure Firewall ASA 上で 2 つのカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』の「*Configure Dynamic Split Tunneling*」を参照してください。

手順

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude
domains
```

ステップ 2 VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、example.com がダイナミック スプリット除外ドメインで、www.example.com がダイナミック スプリット包含ドメインである場合、examples.com へのすべてのトラフィックは www.example.com を除いて除外されます。この属性値には、VPN トンネルから除外する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com,
 example2.com
```

```
anyconnect-custom-data dynamic-split-include-domains example_service_domains_tunneled
www.example1.com, www.example2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value
```

```
example_service_domains
anyconnect-custom dynamic-split-include-domains value
example_service_domains_tunneled
```

ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （169 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。ダイナミック スプリット トンネリングを設定するには、Cisco Secure Firewall ASA 上でカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』の「*Configure Dynamic Split Tunneling*」を参照してください。

手順

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-include-domains description dynamic split include
domains
```

ステップ 2 VPN トンネルによるクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。この属性値には、VPN トンネルに包含するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com,
 domain2.com
```

（注） カスタム属性は421 文字以内である必要があります。制限を超えると、動的に包含されたドメインのリスト（CSV 形式）を 小さな値に分割する必要がある場合があります。

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
```

拡張ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （169 ページ） を参照してください。

ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミックスプリット包含トンネリングを設定するには、Cisco Secure Firewall ASA 上で 2 つのカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』の「*Configure Dynamic Split Tunneling*」を参照してください。

手順

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude
domains
```

ステップ 2 VPN トンネルからのクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。たとえば、domain.com がダイナミック スプリット包含ドメインであり、www.domain.com がダイナミック スプリット除外ドメインである場合、domain.com へのすべてのトラフィックは www.domain.com を除いて包含されます。属性値には、VPN トンネルに包含する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com,
 domain2.com

anyconnect-custom-data dynamic-split-include-domains corporate_service_domains_excluded
 www.domain1.com, www.domain2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value

corporate_service_domains

anyconnect-custom dynamic-split-exclude-domains value

corporate_service_domains_excluded
```

スプリット DNS

スプリット DNS が [ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定されている場合、AnyConnect は、特定の DNS クエリーをプライベート DNS サーバ（同様にグループ ポリシーに設定）にトンネルします。他の DNS クエリーはすべて DNS 解決のためのクライアント オペレーティング システムの DNS リゾルバにクリア テキストで送信されます。スプリット DNS が設定されていない場合、AnyConnect はすべての DNS クエリーをトンネルします。

スプリット DNS が設定されていない場合、AnyConnect はすべての DNS クエリーをトンネルします。

スプリット DNS の要件

スプリット DNS は、標準クエリーおよび更新クエリー（A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR、CNAME など）をサポートしています。トンネリングされたネットワークのいずれかに一致する PTR クエリーは、トンネル経由で許可されます。

スプリット DNS は、Windows と macOS プラットフォームでサポートされています。

- Linux では限定的なサポートが提供されます。具体的には、トンネル DNS 要求のみがスプリット DNS ポリシーの対象となります。そのため、トンネルの外部に送信される一部の DNS 要求は、スプリット DNS ポリシーに準拠しない可能性があります。

macOS の場合、AnyConnect は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルースプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

スプリット包含トンネリングのスプリット DNS の設定

グループポリシーにスプリット包含トンネリングのスプリット DNS を設定するには、次の手順を実行します。

手順

ステップ 1 少なくとも 1 つの DNS サーバを設定します。

『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「*Configure Server Attributes for an Internal Group Policy*」の項を参照してください。

指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバとオーバーラップしていないことを確認します。重複していると、名前解決が正しく動作しない可能性があります。

ステップ 2 Split-Include トンネリングを設定します。

[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）]>[詳細（Advanced）]>[スプリット トンネリング（Split Tunneling）] ペインで、[次のトンネル ネットワーク リスト（Tunnel Network List Below）] を選択し、[ネットワーク リスト（Network List）] にトンネルするアドレスを指定します。

スプリット DNS は、[次のネットワーク リストを除外（Exclude Network List Below）] スプリット トンネリング ポリシーをサポートしません。[次のトンネル ネットワーク リスト（Tunnel Network List Below）] スプリット トンネリング ポリシーを使用して、スプリット DNS を設定します。

ステップ 3 **[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）] > [詳細（Advanced）] > [スプリットトンネリング（Split Tunneling）]** ペインで、[トンネルですべてのDNSルックアップを送信する（Send All DNS lookups through tunnel）] をオフにし、クエリがトンネルされるドメインの名前を [DNS名（DNS Names）] に指定します。

次のタスク

ASDM でグループ ポリシーに変更を加えたら、**[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 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）]** で、グループ ポリシーを接続プロファイルに関連付けてください。

AnyConnect ログを使用したスプリット DNS の確認

スプリット DNS を使用しているドメインの確認

ドメイン名解決には、オペレーティング システムの DNS リゾルバに依存するあらゆるツールまたはアプリケーションを使用できます。たとえば、ping または Web ブラウザを使用してスプリット DNS ソリューションをテストできます。nslookup または dig などのその他のツールは、OS DNS リゾルバを回避します。

クライアントを使用して、どのドメインがスプリット DNS に使用されているかを確認する手順は次のとおりです。

手順

ステップ 1 **ipconfig/all** を実行して、DNS サフィックス検索リストの横にリストされたドメインを記録します。

ステップ 2 VPN 接続を確立し、DNS サフィックス検索リストの横にリストされたドメインを再度確認します。

トンネルを確立した後に追加されたドメインは、スプリットDNSで使用されるドメインです。

（注） このプロセスは、ASA からプッシュされたドメインと、クライアント ホストで設定済みのドメインがオーバーラップしていないことを前提としています。

VPN 認証の管理

重要なセキュリティ上の考慮事項

セキュアゲートウェイ上での自己署名証明書の使用はお勧めしません。

- 理由は、ユーザーが誤って不正なサーバー上の証明書を信頼するようにブラウザを設定する可能性があるため、また、
- ユーザがセキュアゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

AnyConnect クライアントに対する厳格な証明書トラストを有効にすることを強くお勧めします。[厳格な証明書トラスト（Strict Certificate Trust）] を設定するには、ローカルポリシー設定（125 ページ）の「ローカルポリシーパラメータと値」セクションを参照してください。

サポートされるセキュリティタイプ

AnyConnect は、サーバー証明書の検証とクライアント証明書の認証の両方で RSA 証明書と ECDSA 証明書をサポートしています。

- **RSA 証明書**

  AnyConnect は、次のプロパティを持つ RSA 証明書をサポートします。

  - 2048、4096、または 8192 ビットのキー長
  - ハッシュアルゴリズム MD5 *、SHA1、SHA256、SHA384、または SHA512

    * AnyConnect が FIPS モードで動作している場合、MD5 ハッシュを使用する RSA 証明書はサポートされません。

- **ECDSA 証明書**

  AnyConnect は、次のプロパティを持つ ECDSA 証明書をサポートします。

  - 256、384、または 521 ビットのキー長。これらは、それぞれ NIST P-256、P-384、および P-521 楕円曲線に対応します。

- **EdDSA 証明書**

  AnyConnect は、Windows および macOS オペレーティングシステムに基づいて、デジタル証明書により、信頼を確立して署名操作を実行します。これらのオペレーティングシステムでは EdDSA 証明書がまだサポートされていないため、AnyConnect でもサポートできません。

サーバ証明書処理の設定

サーバ証明書の確認

- 証明書は上記の最小キーサイズを満たし、サポートタイプ（RSA または ECDSA）のいずれかである必要があります。
- （Windows のみ）SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。プロファイルエディタで有効にすると、AnyConnect はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認します。認証局によって失効された証明書であることが判明すると、AnyConnect は接続しません。詳細は、ローカルポリシー設定 （125 ページ）を参照してください。
- サーバー証明書が設定された Cisco Secure Firewall ASA にユーザーが接続する場合、信頼チェーン（ルートや中間など）に問題があっても、その証明書を信頼し、インポートするためのチェックボックスは表示されます。証明書にそれ以外の問題がある場合、そのチェックボックスは表示されません。
- FQDN によって実行される SSL 接続では、FQDN を使用した初期検証に失敗した場合、名前検証のために FQDN が IP アドレスに解決されず、セカンダリ サーバの証明書検証が行われません。
- 検証が実行される日時（オペレーティングシステムによって報告される日時）は、証明書の有効開始日より後、かつ有効終了日より前でなければなりません。
- 推奨されませんが、サーバ証明書は、キー使用法（KU）または拡張キー使用法（EKU）を受け入れる必要はありません。ただし、フィールドが存在する場合（最も一般的）、次の条件が適用されます。

  SSL と IPsec（RSA 証明書と ECDSA 証明書の両方）の場合、KU フィールドには DigitalSignature を含める必要があります。RSA 証明書の場合、KU には KeyEncipherment または KeyAgreement も含まれている必要があります。

  IPsec VPN の場合、すべての EKU フィールドに ServerAuth または IkeIntermediate が含まれている必要があります。
- IPsec および SSL 接続は、サーバ証明書で名前の検証を実行します。IPsec および SSL 名前検証のために次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name に対してのみ実行されます。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あっても関連する属性が含まれていない場合、名前検証は、証明書の Subject で見つかった Common Name 属性に対して実行されます。

- 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。このルールに準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

- macOS の場合、期限切れの証明書は、キーチェーンアクセスで [有効期限の切れた証明書を表示（Show Expired Certificates）] が設定されている場合にのみ表示されます。期限切れの証明書は、ユーザーの混乱を招く可能性があるため、デフォルトでは表示されません。

無効なサーバ証明書の処理

非信頼ネットワーク上のモバイル ユーザを狙った攻撃の増加に対応して、シスコは重大なセキュリティ違反を防ぐため、クライアントのセキュリティ保護を強化しました。デフォルトのクライアントの動作は、中間者攻撃に対する追加の防御レイヤを提供するように変更されました。

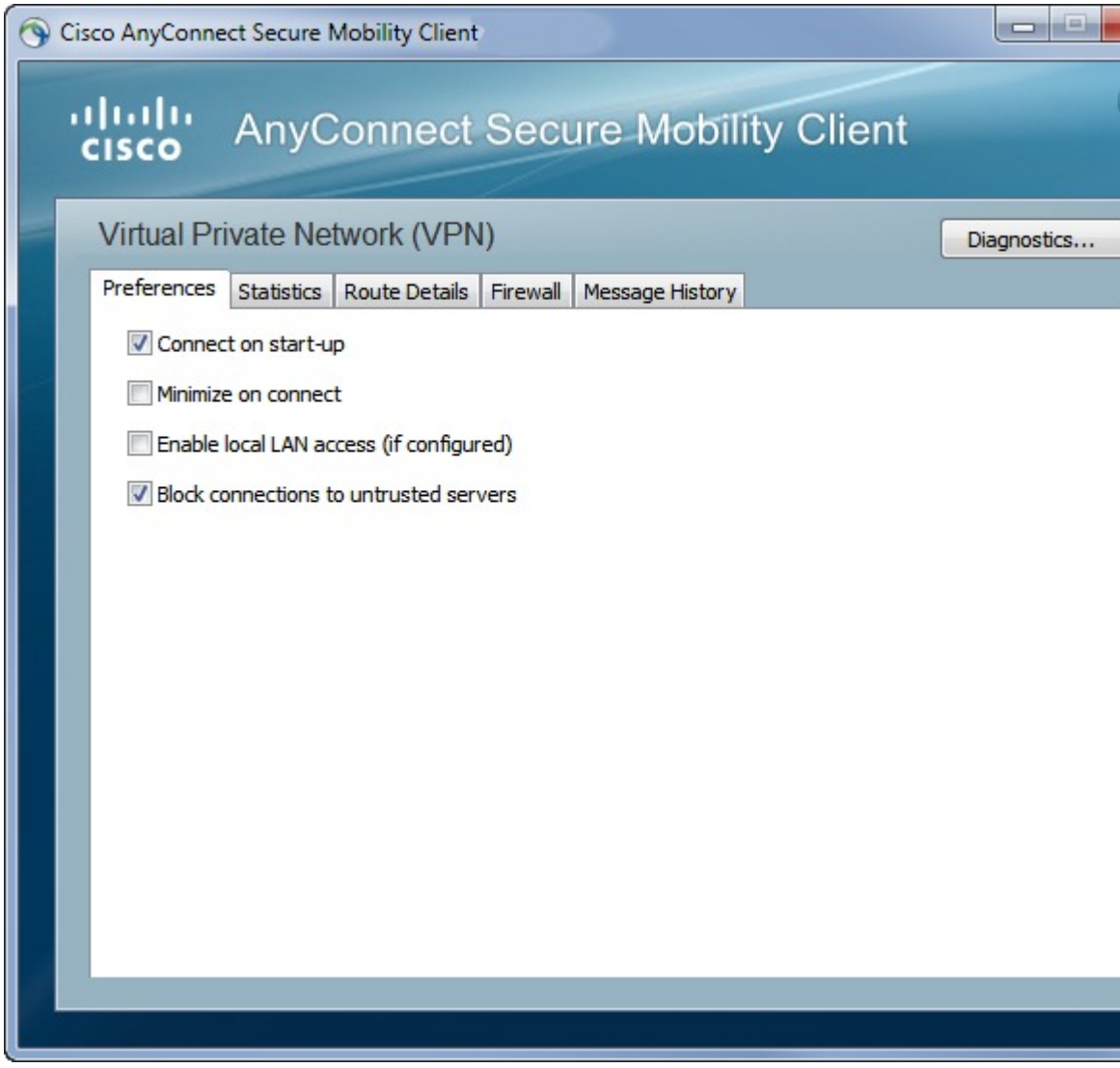
ユーザ対話

ユーザがセキュア ゲートウェイに接続しようとしたときに証明書エラーがある場合（期限切れ、無効な日付、キーの誤用、またはCNの不一致による）、[設定の変更（Change Settings）] および [安全を確保（Keep Me Safe）] ボタンを含む赤色のダイアログがユーザに表示されます。

（注） Linux のダイアログは、このマニュアルに示すものと異なる場合があります。

- [安全を確保（Keep Me Safe）] をクリックすると、接続が解除されます。

- [設定の変更（Change Settings）] をクリックすると、AnyConnect の [詳細（Advanced）] > [VPN]>[設定（Preferences）] ダイアログが開きます。ここで、ユーザーは非信頼サーバーへの接続を有効にできます。現在の接続の試行がキャンセルされます。



ユーザが [常にこの VPN サーバを信頼し、証明書をインポートする（Always trust this VPN server and import the certificate）] をオンにしている場合、このセキュア ゲートウェイへの今後の接続時に、ユーザの続行を確認するプロンプトは表示されません。

（注） ユーザーが、AnyConnect の [詳細（Advanced）] > [VPN] > [設定（Preferences）] で [信頼されていないサーバーへの接続をブロック（Block connections to untrusted servers）] をオンにしている場合、または、ユーザーの設定が注意事項と制約事項の項で説明されているモードのリストのいずれかの条件と一致する場合、AnyConnect は、プロファイルエディタの [厳格な証明書トラスト（Strict Certificate Trust）] オプションが有効になっているかどうかに関係なく、無効なサーバー証明書と信頼できないサーバーへの接続を拒否します。

改善されたセキュリティ動作

クライアントが無効なサーバ証明書を受け入れると、その証明書はクライアントの証明書ストアに保存されます。以前は、証明書のサムプリントだけが保存されました。ユーザが無効なサーバ証明書を常に信頼してインポートすることを選択した場合のみ、無効な証明書が保存されることに注意してください。

エンドユーザの安全性が自動的に損なわれる管理上の優先操作はありません。先行するセキュリティ上の判断をエンド ユーザから完全に排除するには、ユーザのローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] を有効にします。[厳格な証明書トラスト（Strict Certificate Trust）] が有効である場合、ユーザにはエラー メッセージが表示され、接続が失敗します。ユーザ プロンプトは表示されません。

ローカルポリシーファイルでの厳格な証明書トラストの有効化については、ローカルポリシー設定 （125 ページ） を参照してください。

注意事項と制約事項

無効なサーバ証明書は、次の場合に拒否されます。

- AnyConnect プロファイルで [常時接続（Always On）] が有効になっており、適用されたグループポリシーまたは DAP によりオフにされていない。
- クライアントに、厳格な証明書トラストが有効なローカル ポリシーがある。
- AnyConnect でログイン前の起動が設定されている。
- マシン証明書ストアからのクライアント証明書が認証に使用されている。

Certificate-Only 認証の設定

ユーザー名とパスワードを使用して Cisco Secure Firewall ASA でユーザーを認証するか、デジタル証明書で認証するか（または、その両方を使用するか）を指定する必要があります。証明書のみの認証を設定すると、ユーザはデジタル証明書で接続でき、ユーザ ID とパスワードを入力する必要がなくなります。

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、Cisco Secure Firewall ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が Cisco Secure Firewall ASA に提供されたときに、このグループにユーザーを配置するようにできます。

（注） セキュア ゲートウェイに対してクライアントを認証するために使用される証明書は有効であり、（CA によって署名された）信頼できるものである必要があります。自己署名されたクライアント証明書は受け入れられません。

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接続プロファイル（AnyConnect Connection Profiles）]** を選択します。接続プロファイルを選択し、[編集（Edit）] をクリックします。[AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウが開きます。

ステップ 2 選択されていない場合は、ウィンドウの左ペインにあるナビゲーションツリーの [基本（Basic）] ノードをクリックします。ウィンドウの右ペインにある [認証（Authentication）] 領域で、[証明書（Certificate）] 方式を有効にします。

ステップ 3 [OK] をクリックし、変更を適用します。

証明書登録の設定

AnyConnect Secure Mobility Clientは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一部として証明書をプロビジョニングおよび更新します。SCEP を使用した証明書の登録は、Cisco Secure Firewall ASA への AnyConnect IPsec および SSL VPN 接続で次のようにサポートされます。

- SCEP プロキシ：Cisco Secure Firewall ASA はクライアントと認証局（CA）間の SCEP 要求と応答のプロキシとして機能します。
  - クライアントが CA に直接アクセスしないため、CA は、AnyConnect ではなく Cisco Secure Firewall ASA にアクセスできる必要があります。
  - 登録は、クライアントにより常に自動的に開始されます。ユーザーの介入は必要ありません。

関連トピック

AnyConnect プロファイルエディタの [証明書の登録（Certificate Enrollment）]（109 ページ）

SCEP プロキシの登録と動作

次の手順では、AnyConnect および Cisco Secure Firewall ASA が SCEP プロキシ用に設定されている場合に、証明書が取得され、証明書ベースの接続が確立された方法について説明します。

1. ユーザーは、証明書と AAA 認証の両方用に設定された接続プロファイルを使用して、Cisco Secure Firewall ASA ヘッドエンドに接続します。Cisco Secure Firewall ASA は、クライアントからの認証用に証明書と AAA クレデンシャルを要求します。
2. ユーザーが AAA クレデンシャルを入力しますが、有効な証明書は使用可能ではありません。この状況は、入力された AAA クレデンシャルを使用してトンネルが確立された後で、クライアントが自動 SCEP 登録要求を送信するトリガーになります。
3. Cisco Secure Firewall ASA が CA に対して登録要求を転送し、CA の応答をクライアントに返します。
4. SCEP 登録が成功すると、クライアントにユーザーに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザーは、証明書認証を使用して、Cisco Secure Firewall ASA トンネルグループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザーに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザーは自分の管理者に連絡する必要があります。

他の SCEP プロキシの動作上の考慮事項：

- そうするように設定されている場合、ユーザーが介入することなく、期限切れになる前に証明書がクライアントにより自動的に更新されます。
- SCEP プロキシ登録は、SSL と IPSec トンネルの両方の証明書認証に SSL を使用します。

認証局の要件

- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- 一部の CA について、セキュリティを強化するために、電子メールで登録パスワードをユーザに送信するように設定できます。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。このパスワードはその後、AnyConnect プロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

証明書登録のガイドライン

- ASA へのクライアントレス（ブラウザ ベース）VPN アクセスは、SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 AnyConnect）がサポートされます。
- Cisco Secure Firewall ASA ロードバランシングは、SCEP 登録でサポートされます。
- Cisco Secure Firewall ASA は、クライアントから受信した要求を記録しますが、登録が失敗した理由は表示しません。接続の問題は、CA またはクライアントでデバッグされる必要があります。
- 証明書のみの認証および Cisco Secure Firewall ASA での証明書マッピング：

  複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、Cisco Secure Firewall ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が Cisco Secure Firewall ASA に提供されたときに、このトンネルグループにユーザーを配置するようにできます。
- ポリシーを適用するための登録接続の特定：

  Cisco Secure Firewall ASA で、登録接続を捕捉し、選択された DAP レコードの適切なポリシーを適用するために、aaa.cisco.sceprequired 属性が使用されます。
- Windows 証明書の警告：

  Windows クライアントが最初に認証局から証明書を取得しようとした際に、警告される可能性があります。プロンプトが表示されたら、[はい（Yes）] をクリックしてください。これにより、ルート証明書をインポートできます。クライアント証明書との接続に影響しません。

SCEP プロキシ証明書登録の設定

SCEP プロキシ登録用 VPN クライアント プロファイルの設定

手順

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイルエディタの [証明書の登録（Certificate Enrollment）]」を参照してください。

（注）
- %machineid% を使用した場合は、デスクトップクライアントに VPN ポスチャ がロードされます。
- モバイル クライアントの場合、証明書フィールドのうち少なくとも 1 つを指定する必要があります。

SCEP プロキシ登録をサポートするための Cisco Secure Firewall ASA の設定

SCEP プロキシのため、1 つの Cisco Secure Firewall ASA 接続プロファイルは、証明書登録および認証された VPN 接続をサポートします。

手順

ステップ 1 グループ ポリシー（例：cert_group）を作成します。次のフィールドを設定します。

- [一般（General）] で、[SCEP フォワーディング URL（SCEP Forwarding URL）] に CA への URL を入力します。
- [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアントプロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、SCEP プロキシ用に設定されたクライアントプロファイルを指定します。たとえば、ac_vpn_scep_proxy クライアント プロファイルを指定します。

ステップ 2 証明書の登録および接続を認証した証明書（例：cert_tunnel）用の接続プロファイルを作成します。

- [認証（Authentication）]：Both（AAA および Certificate）。
- デフォルトのグループ ポリシー：cert_group。

- [詳細（Advanced）] > [一般（General）] で、[この接続プロファイルへの SCEP 登録を有効にする（Enable SCEP Enrollment for this Connction Profile）] をオンにします。
- [詳細（Advanced）] > [グループエイリアス/グループ URL（GroupAlias/Group URL）] で、この接続プロファイルのグループ（cert_group）が含まれるグループ URL を作成します。

SCEP 用の Windows 2012 Server の認証局の設定

認証局ソフトウェアが Windows 2012 サーバーで実行されている場合、AnyConnect で SCEP がサポートされるように次のいずれかの設定変更を行う必要があります。

認証局での SCEP パスワードの無効化

次の手順は、クライアントが SCEP 登録の前にアウトオブバンドパスワードを提供せずに済むように、SCEP チャレンジ パスワードを無効にする方法について説明します。

手順

ステップ 1 認証局サーバで、レジストリ エディタを起動します。これを行うには、**[スタート（Start）]** > **[ファイル名を指定して実行（Run）]** を選択し、**regedit** と入力して [OK] をクリックします。

ステップ 2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword に移動します。

EnforcePassword キーが存在しない場合は、新しいキーとして作成します。

ステップ 3 EnforcePassword を編集し、「0」に設定します。存在しない場合は、REG-DWORD として作成します。

ステップ 4 regedit を終了し、認証局サーバをリブートします。

認証局での SCEP テンプレートの設定

以下の手順では、証明書のテンプレートを作成する方法、およびこれをデフォルト SCEP テンプレートとして割り当てる方法について説明します。

手順

ステップ 1 サーバ マネージャを起動します。これは、[スタート（Start）] > [管理ツール（Admin Tools）] > [サーバ マネージャー（Server Manager）] を選択することで実行できます。

ステップ 2 [役割（Roles）] > [証明書サービス（Certificate Services）]（または [Active Directory 証明書サービス（AD Certificate Services）]）を展開します。

ステップ 3 CA の名前 > [証明書テンプレート（Certificate Templates）] に移動します。

ステップ 4 [証明書テンプレート（Certificate Templates）] > [管理（Manage）] を右クリックします。

ステップ 5 [証明書テンプレート コンソール（Cert Templates Console）] から、ユーザ テンプレートを右クリックして [複製（Duplicate）] を選択します。

ステップ 6 新しいテンプレートの [Windows Server 2012] バージョンを選択して、[OK] をクリックします。

ステップ 7 テンプレートの表示名を、NDES IPsec SSL など、具体的な説明に変更します。

ステップ 8 サイトの有効期間を調整します。ほとんどのサイトでは、証明書の期限切れを避けるために 3 年以上を選択します。

ステップ 9 [暗号化（Cryptography）] タブで、展開の最小キー サイズを設定します。

ステップ 10 [サブジェクト名（Subject Name）] タブで、[要求に含まれる（Supply in Request）] を選択します。

ステップ 11 [拡張機能（Extensions）] タブで、[アプリケーションのポリシー（Application Policies ）] に少なくとも次が含まれるように設定します。

- クライアント認証
- IP セキュリティ末端システム
- IP セキュリティ IKE 中間
- IP セキュリティ トンネル終端
- IP セキュリティ ユーザ

これらの値は、SSL または IPSec に有効です。

ステップ 12 [適用（Apply）] をクリックして、次に [OK] をクリックして新しいテンプレートを保存します。

ステップ 13 サーバ マネージャから [証明書サービス（Certificate Services）] に移動して CA の名前を選択し、[証明書テンプレート（Certificate Templates）] を右クリックします。[新規（New ）] > [発行する証明書テンプレート（Certificate Template to Issue）] を選択し、作成した新しいテンプレートを選択します（この例では NDES-IPSec-SSL）。次に、[OK] をクリックします。

ステップ 14 レジストリを編集します。これは、[スタート（Start）]>[ファイル名を指定して実行（Run）] で regedit と入力し、[OK] をクリックすることで実行できます。

ステップ 15 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP に移動します。

ステップ 16 次の 3 つのキーの値を、NDES-IPSec-SSL に設定します。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

ステップ 17 [保存（Save）] をクリックして、認証局サーバをリブートします。

証明書失効通知の設定

認証証明書が間もなく期限切れになることをユーザーに警告するよう AnyConnect を設定します。[証明書の有効期限のしきい値（Certificate Expiration Threshold）] 設定では、証明書の有効期限までの日数を指定します。AnyConnect は、しきい値を使用して、証明書の有効期限が切れることをユーザーに警告するタイミングを決定します。証明書が実際に期限切れになるか、新しい証明書が取得されるまで、AnyConnect は接続するたびにユーザーに警告します。

（注） RADIUS 登録では、[証明書失効しきい値（Certificate Expiration Threshold）] 機能は使用できません。

手順

ステップ 1 Cisco AnyConnect Secure Mobility Client プロファイル エディタを開き、ナビゲーションウィンドウから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 [証明書失効しきい値（Certificate Expiration Threshold）] を指定します。

このしきい値は、証明書の有効期限までの日数です。AnyConnect が証明書の失効が近づいていることをユーザーに対して何日前に警告するかを決定します。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 4 [OK] をクリックします。

証明書選択の設定

次の手順では、クライアントシステムで証明書を検索する方法および証明書を選択する方法を設定する、AnyConnect プロファイル内のすべての場所を示します。いずれの手順も必須ではなく、条件を指定しなかった場合、AnyConnect はデフォルトのキー照合を使用します。

Windows では、AnyConnect はブラウザの証明書ストアを読み取ります。Linux の場合、プライバシー強化メール（PEM）形式のファイルストアを作成する必要があります。macOS の場合、プライバシー強化メール（PEM）形式のファイルストアまたはキーチェーンを使用できます。

手順

ステップ 1 Windows および macOS の場合：使用する証明書ストアの設定 （190 ページ）

VPN クライアント プロファイルに AnyConnect で使用される証明書ストアを指定します。

ステップ 2 Windows のみ：Windows ユーザに認証証明書の選択を求めるプロンプトの表示 （193 ページ）

ユーザーに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザーが選択できるように AnyConnect を設定します。

ステップ 3 macOS および Linux 環境の場合：macOS および Linux での PEM 証明書ストアの作成 （194 ページ）

ステップ 4 macOS および Linux 環境の場合：VPN ローカル ポリシー プロファイルで除外する証明書ストアを選択します。

ステップ 5 証明書照合の設定 （195 ページ）

ストアの証明書を検索する場合に、AnyConnect が照合を試みるキーを設定します。キー（拡張キー）を指定し、カスタム拡張キーを追加できます。また、AnyConnect が照合する識別名に演算子の値のパターンを指定できます。

使用する証明書ストアの設定

Windows および macOS では、AnyConnect が VPN クライアント プロファイルで使用するための別の証明書ストアが提供されます。1 つまたは複数の証明書認証の組み合わせが可能で、複数の証明書認証の選択肢のうち特定の VPN 接続において許容されるものをクライアントに指定するようにセキュア ゲートウェイを設定できます。たとえば、ローカル ポリシー ファイルで ExcludeMacNativeCertStore を true に設定（AnyConnect がユーザ ファイル証明書ストアやシステム ファイル証明書ストアなどのファイル証明書ストアのみを使用するよう強制）し、プロファイル ベースの証明書ストアを [ログイン（Login）] に設定（AnyConnect が、ユーザ ファイル ストアに加え、ログイン キーチェーンおよびダイナミック スマートカード キーチェーンなどの証明書ストアのみを使用するよう強制）すると、その組み合わせによるフィルタリングにより、AnyConnect は、厳格にユーザ ファイル証明書ストアを使用するようになります。

コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。通常、Windows ユーザには管理者権限がありません。[証明書ストアの上書き（Certificate Store Override）] を選択すると、ユーザに管理者権限がない場合でも、AnyConnect はマシン ストアにアクセスできます。

（注） マシン ストアのアクセス制御は、Windows のバージョンとセキュリティ設定によって異なる場合があります。このため、ユーザは管理者権限を持つ場合にも、マシン ストアの証明書を使用できない可能性があります。この場合、[証明書ストアの上書き（Certificate Store Override）] を選択してマシン ストアへのアクセスを許可します。

次の表に、検索対象の [証明書ストア（Certificate Store）] および [証明書ストアの上書き（Certificate Store Override）] のオン/オフに基づいて AnyConnect がクライアントで証明書を検索する方法について説明します。

証明書ストアの設定	証明書ストアの上書きの設定	AnyConnect 検索戦略
[すべて（All）]（Windows 用）	オフ	AnyConnect は、すべての証明書ストアを検索します。ユーザーに管理者権限がない場合、AnyConnect は、マシンストアにアクセスできません。 この設定は、デフォルトです。この設定は、ほとんどの状況に適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
[すべて（All）]（Windows 用）	オン	AnyConnect は、すべての証明書ストアを検索します。ユーザーに管理者権限がない場合、AnyConnect は、マシンストアにアクセスできます。
[マシン（Machine）]（Windows 用）	true	AnyConnect は、マシン証明書ストアのみを検索します。ユーザーに管理者権限がない場合、AnyConnect は、マシンストアにアクセスできます。
[すべて（All）]（macOS 用）	オン	AnyConnect は、利用可能なすべての macOS キーチェーンおよびファイルストアからの証明書を使用します。
[ユーザー（User）]（Windows 用）	適用なし	AnyConnect は、ユーザー証明書ストア内のみ検索します。管理者権限のないユーザがこの証明書ストアにアクセスできるため、証明書ストアの上書きは適用されません。
[システム（System）]（macOS 用）	オン	AnyConnect は、macOS システムキーチェーンおよびシステムファイル/PEM ストアからの証明書のみを使用します。

証明書ストアの設定	証明書ストアの上書きの設定	AnyConnect 検索戦略
[ログイン（Log in）]（macOS 用）	オン	AnyConnect は、ユーザーファイル/PEM ストアに加え、macOS ログインキーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。
[すべて（All）]（Linux 用）	適用なし	AnyConnect は、システムとユーザーの両方の PEM ファイルストア、およびユーザー Firefox NSS ストアのクライアント証明書を使用します。
[マシン（Machine）]（Linux 用）	適用なし	AnyConnect は、システム PEM ファイルストアのクライアント証明書のみを使用します。
[ユーザ（User）]（Linux 用）	適用なし	AnyConnect は、ユーザー PEM ファイルストア、およびユーザー Firefox NSS ストアのクライアント証明書のみを使用します。

複数証明書認証の使用

始める前に

- デスクトッププラットフォーム（Windows、macOS、Linux）でのみサポートされます。
- VPN プロファイルで AutomaticCertSelection を有効にしている必要があります。
- VPNプロファイルで設定した証明書照合設定によって、複数証明書認証で使用できる証明書が制限されます。

（注） SCEP はサポートされていません。

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- 1 マシンおよび 1 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] に設定し、ステップ 2 の説明に従って CertficateStoreOverride を有効にします。

- 2 ユーザ証明書の場合は、VPN プロファイルで CertificateStore を [すべて（All）] または [ユーザ（User）] に設定しますが、ステップ 2 の説明に従って CertificateStoreOverrideはそのままにします。

ステップ 2 ユーザーに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、を選択します。

基本的な証明書認証の使用

手順

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- [すべて（All）]：（デフォルト）すべての証明書ストアを使用して証明書を検索するよう AnyConnect に指示します。
- [マシン（Machine）]：証明書ルックアップを Windows ローカルマシン証明書ストアに制限するように AnyConnect に指示します。
- [ユーザー（User）]：証明書ルックアップをローカルユーザー証明書ストアに制限するように AnyConnect に指示します。

ステップ 2 ユーザーに管理者権限がない場合に AnyConnect にマシン証明書ストアの検索を許可するには、を選択します。

Windows ユーザに認証証明書の選択を求めるプロンプトの表示

ユーザーに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザーが選択できるように AnyConnect を設定できます。期限切れの証明書は必ずしも無効として見なされるわけではありません。たとえば SCEP を使用している場合、サーバが新しい証明書をクライアントに発行することがあります。期限切れの証明書を削除すると、クライアントがまったく接続できなくなることがあります。この場合、手動による介入とアウトオブバンド証明書配布が必要になります。AnyConnect では、設定されている証明書一致ルールに基づき、セキュリティ関連プロパティ（キーの使用状況、キーのタイプと強度など）に基づいて、クライアント証明書が制限されるだけです。この設定は Windows でのみ使用できます。デフォルトでは、ユーザによる証明書の選択は無効です。

手順

ステップ 1 Cisco AnyConnect セキュア モビリティ クライアント プロファイルエディタを開き、ナビゲーションウィンドウから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 証明書の選択を有効にするには、[証明書選択を無効にする（Disable Certificate Selection）] チェックボックスをオフにします。

ステップ 3 **[詳細（Advanced）] > [VPN] > [プリファレンス（Preferences）]** ペインでユーザが自動証明書の選択のオン/オフを切り替えられるようにする場合を除き、[ユーザ制御可（User Controllable）] チェックボックスをオフにします。

macOS および Linux での PEM 証明書ストアの作成

AnyConnect は、プライバシー強化メール（PEM）形式のファイルストアからの証明書の取得をサポートします。AnyConnect はリモートコンピューターのファイルシステムから PEM 形式の証明書ファイルを読み取り、検証して署名します。

始める前に

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子が .pem または .crt で終わっていること。
- すべての秘密キー ファイルは、拡張子 .key で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること（client.pem と client.key など）。

ヒント PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

PEM ファイル証明書ストアを作成する場合は、次に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca （注） .cisco/ はホーム ディレクトリにあります。	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

マシン証明書は、ルート ディレクトリ以外は PEM ファイル証明書と同じです。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外の場合は、リストされているパス、フォルダ、および証明書の種類が適用されます。また、AnyConnect はシステム CA 証明書の場所（/etc/ssl/certs）を使用してサーバー証明書を検証します。

証明書照合の設定

AnyConnect では、特定のキーのセットに一致するこれらの証明書に証明書の検索を限定できます。証明書照合は、**[証明書照合（Certificate Matching）]** ペインの AnyConnect VPN プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- [キーの使用状況（Key Usage）]
- [拡張キーの使用状況（Extended Key Usage）]
- [識別名（Distinguished Name）]

関連トピック

AnyConnect プロファイルエディタの証明書照合 （106 ページ）

キーの使用状況の設定

[キーの使用状況（Key Usage）] キーを選択すると、AnyConnect で使用できる証明書が、選択したキーの少なくとも 1 つを持つ証明書に制限されます。サポート対象のセットは、VPN クライアント プロファイルの [キーの使用状況（Key Usage）] リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

拡張キーの使用状況の設定

[拡張キーの使用状況（Extended Key Usage）] キーを選択すると、AnyConnect で使用できる証明書がこれらのキーを持つ証明書に限定されます。次の表は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

制約	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2

制約	OID
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キーの設定

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。

証明書識別名の設定

[識別名（Distinguished Name）] の表には、クライアントが使用できる証明書を指定の条件に一致する証明書に限定する証明書 ID、および一致条件が含まれています。条件をリストに追加したり、追加した条件の内容と照合するための値またはワイルドカードを設定したりするには、[追加（Add）] ボタンをクリックします。

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState

ID	説明
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

[識別名（Distinguished Name）] には、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。[識別名（Distinguished Name）] の一致では、証明書に指定の文字列が含まれている必要があるかどうか、および文字列にワイルドカードを許可するかどうかを指定します。

SAML を使用した VPN 認証

最初のセッション認証に Cisco Secure Firewall ASA リリース 9.7.1 以降と統合された SAML 2.0 を使用できます。組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わりました。SAML 認証用に設定されたトンネルグループに接続するときに、AnyConnect は組み込みブラウザウィンドウを開いて認証プロセスを完了します。SAML 試行のたびに新しいブラウザセッションが使用され、ブラウザセッションは AnyConnect に固有のものとなります（セッション状態は、他のどのブラウザとも共有されません）。各 SAML 認証試行はセッション状態なしで始まりますが、試行間で永続クッキーが保持されます。

Cisco Secure Firewall ASA リリース 9.17.1（以降）/ASDM リリース 7.17.1（以降）では、AnyConnect を使用した VPN SAML 外部ブラウザのサポートが追加されました。AnyConnect VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、Web 認証の実行時に AnyConnect が組み込みブラウザではなくローカルブラウザを使用することを選択できます。この機能により、AnyConnect は WebAuthN およびその他の SAML ベースの Web 認証オプション（シングルサインオン、生体認証、または組み込みブラウザでは利用できないその他の拡張方法など）をサポートします。SAML 外部ブラウザを使用するには、『Cisco ASA Series VPN CLI Configuration Guide, 9.17』の「Configure Default OS Browser for SAML Authentication」セクションで説明されている設定を実行する必要があります。

プラットフォーム固有の要件

組み込みブラウザで SAML を使用するためには、次のシステム要件を満たす必要があります。

- Windows：Windows 7（またはそれ以降）、Internet Explorer 11（またはそれ以降）
- macOS：macOS 10.10（またはそれ以降）（AnyConnect は、macOS 10.11 以降を公式にサポートしています）
- Linux：WebKitGTK+ 2.1x（それ以降）、Red Hat 7.4（それ以降）および Ubuntu 16.04（それ以降）の公式パッケージ

アップグレード プロセス

ネイティブ（外部）ブラウザ搭載の AnyConnect SAML 2.0 は、ASA リリース 9.7.x、9.8.x、および 9.9.1 で使用できます。組み込みブラウザを搭載した拡張バージョンを使用するには、AnyConnect 4.6（またはそれ以降）および ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）へのアップグレードが必要です。

組み込みブラウザ SAML 統合を備えたヘッドエンドまたはクライアント デバイスをアップグレードまたは展開するときには、次のシナリオに注意してください。

- AnyConnect 4.6 以降 を最初に展開した場合は、他に何も操作しなくても、ネイティブ（外部）ブラウザと組み込みブラウザの両方の SAML 統合が想定どおりに機能します。AnyConnect を最初に展開するときでも、AnyConnect 4.6 以降は既存の ASA バージョンも更新された ASA バージョンもサポートします。
- 更新された ASA バージョン（組み込みブラウザ SAML 統合を含む）を最初に展開する場合は、AnyConnect を順にアップグレードする必要があります。デフォルトでは、更新さ

れた ASA リリースは、AnyConnect 4.6 以前のリリースのネイティブ（外部）ブラウザ SAML 統合との下位互換性がありません。認証後に既存の AnyConnect 4.4 または 4.5 クライアントのアップグレードが発生し、このアップグレードを行うためには、トンネル グループ設定で **saml external-browser** コマンドを有効にする必要があります。

SAML を使用する場合は、次の注意事項に従ってください。

- フェールオーバーモードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、Secure Firewall ASA の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、AnyConnect プロファイルエディタ、プリファレンス（Part 1） （93 ページ）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の AnyConnect は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッションクッキーを使用してログオン状態を追跡している場合には、毎回ユーザーの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] [シングルサインオンサーバー（Single Sign On Servers）]** の [強制再認証（Force Re-Authentication）] は、AnyConnect が開始した SAML 認証には影響しません。

SAML の設定の詳細については、最新のリリース（9.7 以降）の『Cisco ASA Series VPN CLI or ASDM Configuration Guide』を参照してください。

SDI トークン（SoftID）統合を使用した VPN 認証

AnyConnect は、Windows x86（32 ビット）および x64（64 ビット）で動作する RSA SecurID クライアント ソフトウェア バージョン 1.1 以降のサポートを統合します。

RSA SecurID ソフトウェア オーセンティケータは、企業の資産へのセキュアなアクセスのために必要となる管理項目数を減らします。リモート デバイスに常駐する RSA SecurID Software Token は、1 回限定で使用可能なパスコードを 60 秒ごとにランダムに生成します。SDI は Security Dynamics 社製テクノロジーの略称で、ハードウェアとソフトウェアの両方のトークンを使用する、この 1 回限定利用のパスワード生成テクノロジーを意味します。

通常、ユーザーはツールトレイの [AnyConnect] アイコンをクリックし、接続する接続プロファイルを選択してから、認証ダイアログボックスに適切なクレデンシャルを入力することで AnyConnect に接続します。ログイン（チャレンジ）ダイアログボックスは、ユーザが属するトンネル グループに設定されている認証タイプと一致しています。ログイン ダイアログボックスの入力フィールドには、どのような種類の入力が認証に必要か明確に示されます。

SDI 認証では、リモート ユーザは AnyConnect ソフトウェア インターフェイスに個人識別番号（PIN）を入力して RSA SecurID パスコードを受け取ります。セキュアなアプリケーションにパスコードを入力すると、RSA Authentication Manager がこのパスコードを確認してユーザにアクセスを許可します。

RSA SecurID ハードウェアまたはソフトウェアのトークンを使用するユーザには、パスコードまたは PIN、PIN、パスコードのいずれかを入力する入力フィールドが表示されます。ダイアログボックス下部のステータス行には、さらにこの点に関連する情報が表示されます。ユーザーは、ソフトウェアトークンの PIN またはパスコードを AnyConnect ユーザーインターフェイスに直接入力します。

最初に表示されるログイン ダイアログボックスの外観は、セキュア ゲートウェイの設定によって異なります。セキュア ゲートウェイには、メインのログイン ページ、メインのインデックス URL、トンネル グループのログイン ページ、またはトンネル グループの URL（URL/トンネル グループ）からアクセスできます。メインのログインページからセキュアゲートウェイにアクセスするには、[ネットワーク（クライアント）アクセス（Network (Client) Access）] の [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] ページで [ユーザーに接続の選択を許可する（Allow user to select connection）] チェックボックスをオンにする必要があります。いずれの方法でも、セキュア ゲートウェイはクライアントにログイン ページを送信します。メインのログイン ページにはドロップダウン リストがあり、ここからトンネル グループを選択します。トンネルグループログインページにはこの表示はありません。トンネルグループは URL で指定されるためです。

メインのログイン ページ（接続プロファイルまたはトンネル グループのドロップダウン リストを表示）の場合、デフォルト トンネル グループの認証タイプによって、パスワードの入力フィールド ラベルの初期設定が決まります。たとえば、デフォルト トンネル グループが SDI 認証を使用する場合、フィールドラベルは [パスコード（Passcode）] になります。一方で、デフォルト トンネル グループが NTLM 認証を使用する場合、フィールド ラベルは [パスワード（Password）] になります。リリース 2.1 以降では、異なるトンネル グループをユーザが選択しても、フィールドラベルが動的に更新されることはありません。トンネルグループのログイン ページでは、フィールド ラベルはトンネルグループの要件に一致します。

クライアントは、パスワード入力フィールドへの RSA SecurID Software Token の PIN の入力をサポートします。RSA SecurID Software Token ソフトウェアがインストールされており、トンネルグループ認証タイプが SDI の場合、フィールド ラベルは [パスコード（Passcode）] となり、ステータス バーには、「ユーザ名およびパスコードまたはソフトウェア トークンPINを入力してください（Enter a username and passcode or software token PIN）」と表示されます。PIN を使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、フィールド ラベルが [PIN] になります。クライアントは、入力された PIN を使用して RSA SecurID Software Token DLL からパスコードを取得します。認証が成功するたびにクライアントはトンネル グループ、ユーザ名、認証タイプを保存し、保存されたトンネル グループが新たにデフォルトのトンネル グループとなります。

AnyConnect では、すべての SDI 認証でパスコードを使用できます。パスワード入力ラベルが [PIN] の場合でも、ユーザはステータス バーの指示どおりにパスコードを入力することができます。クライアントは、セキュア ゲートウェイにパスコードをそのまま送信します。パスコードを使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [パスコード（Passcode）] のフィールドが表示されます。

RSASecureIDIntegration プロファイル設定は、次の 3 つの値のいずれかになります。

- Automatic：クライアントはまず 1 つの方式を試行し、それが失敗したら別の方式を試行します。デフォルトでは、ユーザ入力がトークン パスコード（HardwareToken）として処理され、これが失敗したら、ユーザ入力がソフトウェア トークン PIN（SoftwareToken）として処理されます。認証が成功すると、成功した方式が新しい SDI トークン タイプとして設定され、ユーザ プリファレンス ファイルにキャッシュされます。SDI トークン タイプは、次回の認証試行でいずれの方式が最初に試行されるかを定義します。通常、現行の認証試行には、最後に成功した認証試行で使用されたトークンと同じものが使用されます。ただし、ユーザ名またはグループの選択を変更した場合は、入力フィールドラベルに示されている、デフォルトの方式が最初に試行される状態に戻ります。

（注） SDI トークン タイプは、設定が自動の場合のみ、意味を持ちます。認証モードが自動以外の場合は、SKI トークン タイプのログを無視できます。HardwareToken がデフォルトの場合、次のトークン モードはトリガーされません。

- SoftwareToken：クライアントは、ユーザー入力を常にソフトウェア トークン PIN として解釈し、入力フィールドラベルは [PIN:] になります。
- HardwareToken：クライアントは、ユーザー入力を常にトークンパスコードとして解釈し、入力フィールドラベルは [Passcode:] になります。

（注） AnyConnect では、RSA Software Token クライアント ソフトウェアにインポートした複数のトークンからの、トークンの選択はサポートされていません。その代わりに、クライアントは RSA SecurID Software Token GUI を介してデフォルト選択のトークンを使用します。

SDI 認証交換のカテゴリ

すべての SDI 認証交換は次のいずれかのカテゴリに分類されます。

- 通常の SDI 認証ログイン
- 新規ユーザー モード
- 新規 PIN モード
- PIN クリア モード
- 次のトークン コード モード

通常の SDI 認証ログイン

通常ログインチャレンジは、常に最初のチャレンジです。SDI認証ユーザーは、ユーザー名およびトークン パスコード（ソフトウェア トークンの場合は PIN）を、ユーザー名とパスコードまたはPINフィールドにそれぞれ指定する必要があります。クライアントはユーザーの入力に応じてセキュア ゲートウェイ（中央サイトのデバイス）に情報を返し、セキュア ゲートウェイはこの認証を認証サーバ（SDI または RADIUS プロキシ経由の SDI）で確認します。

認証サーバーが認証要求を受け入れた場合、セキュア ゲートウェイは認証が成功したページをクライアントに送信します。これで認証交換が完了します。

パスコードが拒否された場合は認証は失敗し、セキュア ゲートウェイは、エラー メッセージとともに新しいログイン チャレンジ ページを送信します。SDI サーバーでパスコード失敗しきい値に達した場合、SDI サーバーはトークンを次のトークンコードモードに配置します。

新規ユーザー モード、PIN クリア モード、および新規 PIN モード

PIN のクリアは、ネットワーク管理者だけの権限で、SDI サーバーでのみ実行できます。

新規ユーザーモード、PIN クリア モード、新規 PIN モードでは、AnyConnect は、後の「next passcode」ログインチャレンジで使用するために、ユーザー作成 PIN またはシステムが割り当てた PIN をキャッシュに入れます。

PINクリアモードと新規ユーザーモードは、リモートユーザーから見ると違いがなく、また、セキュア ゲートウェイでの処理も同じです。いずれの場合も、リモートユーザーは新しいPINを入力するか、SDIサーバーから割り当てられる新しいPINを受け入れる必要があります。唯一の相違点は、最初のチャレンジでのユーザーの応答です。

新規PINモードでは、通常のチャレンジと同様に、既存のPINを使用してパスコードが生成されます。PINクリアモードでは、ユーザーがトークンコードだけを入力するハードウェア トークンとして PIN が使用されることはありません。RSA ソフトウェア トークンのパスコードを生成するために0が8つ並ぶPIN（00000000）が使用されます。いずれの場合も、SDIサーバー管理者は、使用すべき PIN 値（ある場合）をユーザーに通知する必要があります。

新規ユーザーをSDIサーバーに追加すると、既存ユーザーのPINをクリアする場合と同じ結果になります。いずれの場合も、ユーザーは新しいPINを指定するか、SDIサーバーから割り当てられる新しい PIN を受け入れる必要があります。これらのモードでは、ユーザーはハードウェア トークンとして、RSA デバイスのトークン コードのみ入力します。いずれの場合も、

SDI サーバー管理者は、使用すべき PIN 値（ある場合）をユーザーに通知する必要があります。

新規 PIN の作成

現行の PIN がない場合、システム設定に応じて、次の条件のいずれかを満たすことが、SDI サーバーによって要求されます。

- システムがユーザーに新規 PIN を割り当てる必要がある（デフォルト）。
- ユーザーは新規 PIN を作成する必要がある。
- ユーザーは、PIN を作成するか、システムの割り当てを受け入れるかを選択できる。

PINをリモートユーザー自身で作成する方法とシステムで割り当てる方法を選択できるようにSDIサーバーを設定している場合、ログイン画面にはオプションを示すドロップダウンリストが表示されます。ステータス行にプロンプト メッセージが表示されます。

システムが割り当てる PIN の場合、ユーザーがログインページで入力したパスコードを SDI サーバーが受け入れると、セキュアゲートウェイはシステムが割り当てたPINをクライアントに送信します。クライアントは、ユーザーが新規 PIN を確認したことを示す応答をセキュアゲートウェイに返し、システムは「next passcode」チャレンジに進みます。

ユーザーが新しく PIN を作成するように選択した場合、AnyConnect にこの PIN を入力するためのダイアログボックスが表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。PINは一種のパスワードであるため、ユーザーがこの入力フィールドに入力する内容はアスタリスクで表示されます。

RADIUS プロキシを使用する場合、PIN の確認は、最初のダイアログボックスの次に表示される、別のチャレンジで行われます。クライアントは新しいPINをセキュアゲートウェイに送信し、セキュアゲートウェイは「next passcode」チャレンジに進みます。

「next passcode」チャレンジと「next Token Code」チャレンジ

「next passcode」チャレンジでは、クライアントが新規 PIN の作成または割り当て時にキャッシュに入れられた PIN 値を使用して RSA SecurID Software Token DLL から次のパスコードを取得し、ユーザーにプロンプト表示せずにこれをセキュア ゲートウェイに返します。同様に、ソフトウェア トークン用の「next Token Code」チャレンジでは、クライアントは RSA SecurID Software Token DLL から次のトークン コードを取得します。

ネイティブ SDI と RADIUS SDI の比較

ネットワーク管理者は、SDI認証を可能にするセキュア ゲートウェイを次のいずれかのモードで設定することができます。

- ネイティブ SDI：SDI サーバと直接通信して SDI 認証を処理できるセキュア ゲートウェイのネイティブ機能です。
- RADIUS SDI：RADIUS SDI プロキシを使用して SDI サーバと通信することで SDI 認証を行うセキュア ゲートウェイのプロセスです。

リモート ユーザからは、ネイティブ SDI と RADIUS SDI は同一です。SDI メッセージは SDI サーバー上で設定が可能なため、これには、Cisco Secure Firewall ASA 上のメッセージ テキストは、SDI サーバー上のメッセージテキストに一致する必要があります。一致しない場合、リモート クライアント ユーザーに表示されるプロンプトが、認証中に必要なアクションに対して適切でない場合があり、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS SDI チャレンジは、少数の例外はありますが、基本的にはミラー ネイティブの SDI 交換です。両者とも最終的には SDI サーバと通信するため、クライアントからの必要な情報と要求される情報の順序は同じです。

認証の間に、RADIUS サーバーは Cisco Secure Firewall ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージテキストは、Cisco Secure Firewall ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、AnyConnect にネイティブ SDI サーバとして認識させるために、Cisco Secure Firewall ASA は RADIUS サーバーからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバーで設定可能であるため、Cisco Secure Firewall ASA のメッセージテキストの全体または一部が、SDI サーバーのメッセージテキストと一致する必要があります。一致しない場合、リモート クライアント ユーザーに表示されるプロンプトが、認証中に必要なアクションに対して適切でない場合があり、AnyConnect が応答できずに認証に失敗することがあります。

RADIUS/SDI メッセージをサポートするための Cisco Secure Firewall ASA の設定

SDI 固有の RADIUS 応答メッセージを解釈し、適切なアクションを AnyConnect ユーザーに求めるように Cisco Secure Firewall ASA を設定するには、SDI サーバーとの直接通信をシミュレートする方法で RADIUS 応答メッセージを転送するように接続プロファイル（トンネルグループ）を設定する必要があります。SDI サーバーに認証されるユーザーは、この接続プロファイルを介して接続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接続プロファイル（AnyConnect Connection Profiles）]** を選択します。

ステップ 2 SDI 固有の RADIUS 応答メッセージを解釈するために設定する接続プロファイルを選択して、[編集（Edit）] をクリックします。

ステップ 3 [AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウで、左側のナビゲーション ペインにある [詳細（Advanced）] ノードを展開して、[グループ エイリアス/グループ URL（Group Alias / Group URL）] を選択します。

ステップ 4 [ログイン画面への SecurID メッセージの表示を有効にする（Enable the display of SecurID messages on the login screen）] をオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [AAA/ローカルユーザ（AAA/Local Users）] > [AAAサーバグループ（AAA Server Groups）]** を選択します。

ステップ 7 [追加（Add）] をクリックして、AAA サーバ グループを追加します。

ステップ 8 [AAA サーバ グループの編集（Edit AAA Server Group）] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9 [AAA サーバ グループ（AAA Server Groups）] 領域で作成した AAA サーバ グループを選択し、[選択したグループ内のサーバ（Servers in the Selected Group）] 領域で [追加（Add）] をクリックします。

ステップ 10 [SDI メッセージ（SDI Messages）] 領域で [メッセージ テーブル（Message Table）] 領域を展開します。メッセージテキスト フィールドをダブルクリックするとメッセージを編集できます。RADIUS サーバーから送信されたメッセージとテキストの一部または全体が一致するように、RADIUS 応答メッセージテキストを Cisco Secure Firewall ASA で設定します。

次の表に、メッセージコード、デフォルトの RADIUS 応答メッセージテキスト、および各メッセージの機能を示します。

（注） Cisco Secure Firewall ASA が使用するデフォルトのメッセージテキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージテキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージテキストを使用している場合、Cisco Secure Firewall ASA でメッセージテキストを設定する必要はありません。

セキュリティ アプライアンスは、テーブルでの出現順に文字列を検索するため、メッセージテキスト用に使用する文字列が別の文字列のサブセットでないことを確認する必要があります。たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージテキストのサブセットであるとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを照合します。

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。

メッセージ コード	デフォルトの RADIUS 応答メッセージ テキスト	機能
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザーが提供した PIN の確認のために Cisco Secure Firewall ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	ユーザーがシステム生成のPINに対する準備ができていることを示すために Cisco Secure Firewall ASA が内部的に使用します。

ステップ 11 [OK]、[適用（Apply）]、[保存（Save）] の順にクリックします。

証明書のピン留めについて

AnyConnect の証明書のピン留めは、サーバー証明書チェーンが実際に接続しているサーバーから来たものであるか検出するのに役立ちます。この機能は VPN プロファイル設定に基づくもので、AnyConnect サーバー証明書検証ポリシーへの追加機能です。AnyConnect のローカルポリシーファイルでの厳格な証明書トラストの設定は、証明書のピン留めチェックに影響しません。ピンは、VPNプロファイルで、グローバルにまたはホストごとに設定できます。プライマリ ホストについて設定されたピンは、サーバ リスト内のバックアップ ホストに対しても有効です。証明書のピン留めチェックを実行するプリファレンスをユーザが制御することはできません。ピン検証が失敗すると、VPN 接続が終了します。

（注） AnyConnect は、プリファレンスが有効になっており、接続サーバーの VPN プロファイルにピンがあるときのみ、ピン検証を実行します。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定は、VPNプロファイルエディタ（AnyConnectプロファイルエディタの証明書ピン（111ページ））で行うことができます。

証明書のピン留めを設定および維持するにあたっては、注意が必要です。プリファレンスを設定するときは、次の推奨事項を考慮してください。

- ルート証明書および/または中間証明書をピン留めする。理由は、これらはオペレーティング システムにおいて CA ベンダーによって十分に管理されているためです。
- CA が侵害された場合のバックアップとなるよう、別の CA からの複数のルート証明書および/または中間証明書をピン留めする。
- CA の移行が容易になるよう、複数のルート証明書および/または中間証明書をピン留めする。
- リーフ証明書がピン留めされている場合は、証明書の更新時に公開キーを保持するため、同一の証明書署名要求を使用する。
- サーバ リスト内のすべての接続ホストをピン留めする。

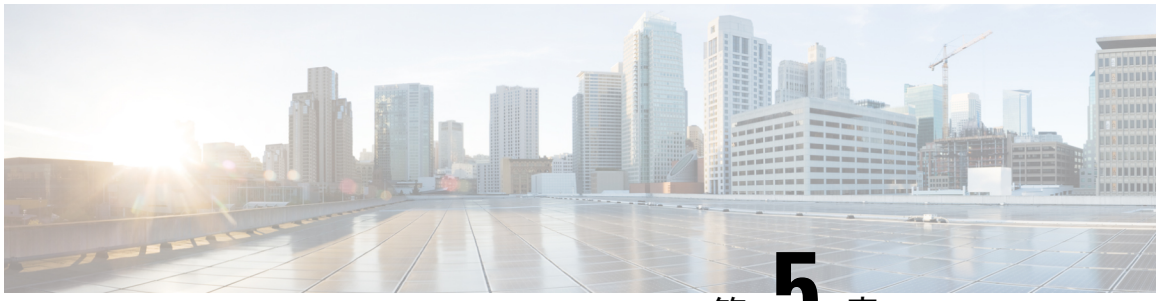
グローバル ピンとホストごとのピン

証明書ピンは、グローバルまたはホストごとに設定できます。大部分の接続ホストに対して有効なピンは、グローバル ピンとして設定されます。ルート証明書、中間証明機関の証明書、およびワイルドカード リーフ証明書は、VPN プロファイルのグローバル ピンの下に設定することを推奨します。1 つの接続ホストに対してのみ有効なピンは、ホストごとのピンと見なされます。リーフ証明書、自己署名の証明書は、VPNプロファイルのホストごとのピンの下に設定することを推奨します。

（注） AnyConnect は、ピン検証において、対応する接続サーバーのグローバルピンおよびホストごとのピンをチェックします。

（注） 複数の VPN プロファイルにまたがるグローバル ピンは、マージされません。ピンは、VPN 接続のためのファイル接続サーバから厳格に考慮されます。

（注） ホストごとの証明書のピン留めができるのは、[グローバル ピン（Global Pins）] セクションで証明書ピン留めのプリファレンスが有効になっている場合のみです。



第 5 章

Network Access Manager の設定

この章では、Network Access Manager の設定の概要について、ならびにユーザ ポリシーおよびネットワーク プロファイルの追加と設定の手順について説明します。

Network Access Manager について

Network Access Managerは、ポリシーに従ってセキュアなレイヤ 2 ネットワークを提供するクライアント ソフトウェアです。最適なレイヤ 2 アクセス ネットワークを検出して選択し、有線ネットワークとワイヤレス ネットワークの両方へのアクセスに対してデバイス認証を実行します。Network Access Managerは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。管理者定義のポリシーに違反する接続をエンド ユーザが確立しないように、インテリジェントに動作します。

Network Access Managerは、単一ホーム（一度に 1 つのネットワーク接続を許可する）になるよう設計されています。また、有線接続がワイヤレス接続によりも優先されます。そのため、有線接続を使用してネットワークに接続した場合、ワイヤレス アダプタは IP アドレスを失い無効になります。

有線またはワイヤレスネットワーク設定や特定の SSID がグループポリシーからプッシュされた場合、それらはNetwork Access Managerの適切な動作と競合する可能性があります。Network Access Managerがインストールされている場合、ワイヤレス設定のグループポリシーはサポートされません。

（注） Network Access Manager は macOS または Linux には対応していません。

（注） Windows OS で ISE ポスチャを使用する場合は、AnyConnect ISE ポスチャを開始する前に Network Access Manager をインストールする必要があります。

AnyConnect Secure Mobility Client のNetwork Access Manager コンポーネントは、次の主要な機能に対応しています。

- Transport Layer Security（TLS）プロトコルバージョン 1.2
- 有線（IEEE 802.3）およびワイヤレス（IEEE 802.11）ネットワーク アダプタ。
- Windows 7 以降でのモバイル ブロードバンド（3G）ネットワーク アダプタ（Microsoft モバイル ブロードバンド API をサポートする WAN アダプタが必要です）。
- Windows マシン クレデンシャルを使用した事前ログイン認証。
- Windows ログイン クレデンシャルを使用するシングル サインオン ユーザ認証。
- 簡素化された IEEE 802.1X 設定。
- IEEE MACsec 有線暗号化および企業ポリシー制御。
- EAP 方式：
  - EAP-FAST、PEAP、EAP-TTLS、EAP-TLS、および LEAP（IEEE 802.3 有線のみ EAP-MD5、EAP-GTC、および EAP-MSCHAPv2）。
- 内部 EAP 方式：
  - PEAP：EAP-GTC、EAP-MSCHAPv2、および EAP-TLS。
  - EAP-TTLS：EAP-MD5 および EAP-MSCHAPv2 およびレガシー方式（PAP、CHAP、MSCHAP、および MSCHAPv2）。
  - EAP-FAST：GTC、EAP-MSCHAPv2、および EAP-TLS。
- 暗号化モード：スタティック WEP（オープンまたは共有）、ダイナミック WEP、TKIP、および AES。
- キー確立プロトコル：WPA、WPA2/802.11i。
- AnyConnect は、次の環境でスマートカードにより提供されるログイン情報に対応します。
  - Windows の Microsoft CAPI 1.0 および CAPI 2.0（CNG）。
  - Windows ログインは ECDSA 証明書に対応していないため、Network Access Manager のシングル サインオン（SSO）は ECDSA クライアント証明書に対応していません。

（注） 現時点で WPA3 はサポートされていません。

Suite B および FIPS

次の機能は、Windows 7 以降で FIPS 認定されています。例外を次に示します。

- ACS および ISE は Suite B には対応していませんが、OpenSSL 1.x 搭載の FreeRADIUS 2.x は対応しています。Microsoft NPS 2008 は Suite B に一部対応しています（NPS の証明書は RSA でなければなりません）。
- 802.1X/EAP は、Suite B の遷移プロファイルのみをサポートします（RFC 5430 の定義どおり）。
- MACsec は FIPS 準拠です。
- 楕円曲線 Diffie-Hellman（ECDH）キー交換はサポートされています。
- ECDSA クライアント証明書はサポートされています。
- OS ストアの ECDSA CA 証明書はサポートされています。
- ネットワーク プロファイルの（PEM エンコードされた）ECDSA CA 証明書はサポートされています。
- サーバの ECDSA 証明書チェーン検証はサポートされています。

シングルサインオンの「シングルユーザ」の適用

Microsoft Windows では複数のユーザーが同時にログインできますが、AnyConnect Network Access Managerではシングルユーザーにネットワーク認証を制限します。AnyConnect Network Access Managerは、ログインしているユーザーの数に関係なく、デスクトップまたはサーバー当たり 1 人のユーザーをアクティブにできます。シングル ユーザ ログインの適用は、いつでもシステムにログインできるユーザは 1 人のみで、管理者は現在ログインしているユーザを強制的にログオフできないことを示しています。

Network Access Manager クライアント モジュールが Windows デスクトップにインストールされている場合、デフォルト動作はシングル ユーザ ログインを適用することです。サーバにインストールされている場合、デフォルト動作はシングル ユーザ ログインの適用を緩和することです。いずれの場合も、デフォルトの動作を変更するようにレジストリを変更または追加できます。

制約事項

- Windows 管理者は、現在ログインしているユーザの強制ログオフが制限されています。
- 接続されたワークステーションへの RDP は同一ユーザにサポートされています。
- 同一ユーザと見なされるためには、クレデンシャルを同じフォーマットにする必要があります。たとえば、user/example は user@example.com と同じではありません。
- また、スマートカードユーザが同じ PIN を持っている場合、同一ユーザと見なされます。

シングル サインオンのシングル ユーザーの適用の設定

Windows ワークステーションまたはサーバで複数のユーザーを処理する方法を変更するには、レジストリの EnforceSingleLogon の値を変更します。

Windows では、レジストリ キーは **EnforceSingleLogon** で、OverlayIcon レジストリ キーと同じ場所にあります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential
Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

1 つまたは複数のユーザー ログインを設定するには、EnforceSingleLogon という名前の DWORD を追加し、1 または 0 の値を指定します。

Windows の場合：

- 1 は、シングル ユーザーにログインを制限します。
- 0 は、複数のユーザーにログインを許可します。

Network Access Manager の展開

Network Access Managerは AnyConnect の一部として展開されます。AnyConnect をNetwork Access Managerやその他のモジュールとともにインストールする方法については、「AnyConnect 展開の概要」を参照してください。

ガイドライン

- Windows のネットワーク ステータス タスク トレイ アイコンの混同：Network Access Manager は、Windows のネットワーク管理より優先します。したがって、Network Access Manager のインストール後、ネットワークに接続するためにネットワーク ステータスのアイコンを使用できません。

  推奨アクション：Windows グループポリシーの [ネットワークアイコンを削除する（Remove the networking icon）] を設定することで、タスクトレイから Windows ネットワークアイコンを削除します。この設定は、トレイ アイコンだけに影響します。ユーザは、コントロール パネルを使用してネイティブのワイヤレス ネットワークを確立できます。

- Windows 7 以降の非表示のネットワークおよびネットワークの選択：Network Access Manager は、Network Access Managerのネットワーク スキャン リストで設定されたネットワークだけに接続を試みます。

  Windows 7 以降では、Network Access Managerは非表示 SSID をプローブします。最初の非表示 SSID が見つかると、検索を中止します。複数の非表示ネットワークが設定されている場合、Network Access Managerは次のように SSID を選択します。

  - 管理者が定義した最初の非表示社内ネットワーク
  - 管理者が定義した非表示ネットワーク

- ユーザが定義した最初の非表示ネットワークNetwork Access Managerは一度に 1 つの非ブロードキャスト SSID しかプローブできないため、サイトの非表示社内ネットワークは 1 つのみにすることをお勧めします。

- ネットワークの接続性または長い接続時間の瞬時的な喪失：Network Access Managerをインストールする前に Windows でネットワークが定義済みである場合、Windows の接続マネージャがそのネットワークに接続を試みる場合があります。

  推奨アクション：ネットワークが圏内にある場合、すべての Windows 定義ネットワークに対して [自動的に接続する（Connect Automatically）] をオフにするか、Windows 定義ネットワークをすべて削除します。

- Network Access Manager モジュールは、このモジュールがクライアント システムに初めてインストールされたときに、一部の既存の Windows 7 またはそれ以降のワイヤレス プロファイルをNetwork Access Manager プロファイル形式に変換するように設定できます。次の条件を満たすインフラストラクチャ ネットワークは変換が可能です。

  - オープン
  - 静的 WEP
  - WPA/WPA2 Personal
  - 非 GPO ネイティブ Wi-Fi ユーザ ネットワーク プロファイルだけが変換されます。
  - プロファイルの変換中は、WLAN サービスがシステムで実行している必要があります。
  - 変換は、Network Access Manager XML コンフィギュレーション ファイルがすでに存在する場合（userConfiguration.xml）は実行されません。

  ネットワーク プロファイルの変換を有効にするには、PROFILE_CONVERSION プロパティの値を 1 に設定する MSI トランスフォームを作成し、それを MSI パッケージに適用します。またはコマンド ラインで PROFILE_CONVERSION プロパティを 1 に変更して、MSI パッケージをインストールします。たとえば、**msiexec /i anyconnect-nam-<version>-k9.msi PROFILE_CONVERSION=1**。

- ISE ポスチャが開始する前にNetwork Access Managerをインストールする必要があります。ISE ポスチャは、Network Access Manager プラグインを使用して、ネットワーク変更ベントおよび 802.1x WiFi を検出します。

DHCP 接続テストの無効化

ネットワークがダイナミック IP アドレスを使用するように設定されている場合は、Windows OS サービスは DHCP を使用して接続を確立しようとします。ただし、オペレーティング システム プロセスがNetwork Access Managerに DHCP トランザクションが完了したことを通知するまでに最大で 2 分かかる場合があります。OS の DHCP トランザクションに加えて、Network

Access Managerが DHCP トランザクションをトリガーすることによって、OS 経由の接続が確立するまでの時間を短縮し、ネットワーク接続を確認します。

接続テストで NAM による DHCP トランザクションの使用を無効にする場合は、次のレジストリ キーを DWORD として追加し、指定された値を設定します。

- 64 ビット Windows：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP を 1 に設定
- 32 ビット Windows：HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Network Access Manager\DisableDHCP を 1 に設定

（注） Network Access Managerの DHCP 接続テストを無効にすると、多くの場合、接続時間が長くなるためお勧めできません。

Network Access Manager プロファイル

Network Access Manager プロファイルは、Network Access Manager プロファイル エディタで設定されます。このエディタは ASDM でスタンドアロン Windows アプリケーションとして使用できます。

クライアント ポリシー ウィンドウ

[クライアントポリシー（Client Policy）] ウィンドウでは、クライアント ポリシー オプションを設定できます。この項では次のトピックについて説明します。

接続の設定

ユーザ ログインの前または後にネットワーク接続しようとするかどうかを定義できます。

- [デフォルト接続タイムアウト（Default Connection Timeout）]：ユーザ作成ネットワークの接続タイムアウトとして使用する秒数。デフォルト値は 40 秒です。
- [ユーザ ログインの前（Before User Logon）]：ユーザがログインする前にネットワークに接続します。サポートされているユーザ ログインの種類として、ユーザ アカウント（Kerberos）認証、ユーザ GPO のロード、GPO ベースのログイン スクリプト実行があります。[ユーザ ログインの前（Before User Logon）] を選択した場合、[ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）] も設定できます。
- [ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）]：Network Access Managerが完全にネットワーク接続するのに待機する最大（最悪のケース）秒数を指定します。この時間内にネットワーク接続が確立できない場合、Windows ログイン プロセスはユーザ ログインにより継続されます。デフォルトは 5 秒です。

（注） ワイヤレス接続を管理するようNetwork Access Managerが設定されている場合、[ユーザがログインできるまでに待機する時間（Time to Wait Before Allowing a User to Logon）] を 30 秒以上に設定する必要があります。ワイヤレス接続の確立にさらに時間が必要になる可能性があるためです。DHCP 経由で IP アドレスを取得するために必要な時間も考慮する必要があります。2 つ以上のネットワーク プロファイルが設定されている場合、2 回以上の接続試行に対応するように値を大きくする必要があります。

- [ユーザ ログイン後（After User Logon）]：Windows へのユーザ ログイン後にネットワークに接続します。

メディア

Network Access Manager クライアントにより制御されるメディアの種類を指定します。

- [Wi-Fi（ワイヤレス）メディアの管理（Manage Wi-Fi (wireless) Media）]：Wi-Fi メディアの管理、また任意で WPA/WPA2 ハンドシェイクの検証ができるようになります。

  IEEE 802.11i ワイヤレス ネットワーキング標準では、サプリカント（この場合はNetwork Access Manager）がアクセス ポイントの RSN IE（堅牢でセキュアなネットワーク情報交換）を検証する必要があることを規定しています。IE は、キー導出時に IEEE 801.X プロトコル パケットの EAPOL キー データに送信され、ビーコン/プローブ応答フレームにあるアクセス ポイントの RSN IE に一致する必要があります。

- [WPA/WPA2 ハンドシェイクの検証の有効化（Enable validation of WPA/WPA2 handshake）]：WPA/WPA2 ハンドシェイクを検証します。オフの場合、この任意の検証手順はスキップされます。

（注） 一部のアダプタでは、アクセス ポイントの RSN IE を常に提供するわけではないため、認証試行に失敗し、クライアントが接続されません。

- [デフォルトのアソシエーション タイムアウト（秒）（Default Association Timeout (sec)）]：WPA/WPA2 ハンドシェイクを有効にした場合は、デフォルトのアソシエーション タイムアウトを指定する必要があります。

- [有線（IEEE 802.3）メディアの管理（Manage Wired (IEEE 802.3) Media）]：有線接続の管理を有効にします。

- [モバイルブロードバンドメディアの管理（Manage Mobile Broadband Media）]：Windows モバイル ブロードバンド アダプタの管理を有効にします。この機能は、デフォルトでは無効になっています。

（注） この機能はベータ版に入っています。Cisco TAC は、ベータ版には対応していません。

- [データ ローミングの有効化（Enable Data Roaming）]：データ ローミングを許可するかどうかを指定します。

エンド ユーザ制御

ユーザに対して次の制御を設定できます。

- [クライアントの無効化（Disable Client）]：ユーザーは、AnyConnect UI を使用して、Network Access Managerによる有線メディアおよびワイヤレスメディアの管理を無効および有効にできます。
- [ユーザ グループの表示（Display User Groups）]：管理者定義のグループに対応しない場合でも、ユーザが作成したグループ（CSSC 5.x から作成）を表示して、接続できるようにします。
- [接続時に実行するスクリプトまたはアプリケーションの指定（Specify a script or application to run when connected）]：ユーザは、ネットワーク接続時に実行するスクリプトまたはアプリケーションを指定できます。

（注） スクリプト設定は 1 つのユーザ設定ネットワークに固有であり、ユーザはローカル ファイル（.exe、.bat、または .cmd）を指定して、そのネットワークが接続状態になったときに実行できます。競合を避けるために、スクリプト機能では、ユーザはユーザ定義のネットワークについてのみスクリプトまたはアプリケーションを設定でき、管理者定義のネットワークについては設定できません。スクリプト機能では、スクリプトの実行に関して管理者ネットワークをユーザが変更できません。このため、ユーザは管理者ネットワークのインターフェイスを使用できません。また、ユーザが実行中のスクリプトを設定できないようにする場合、この機能はNetwork Access Manager GUI に表示されません。

- [自動接続（Auto-connect）]：ユーザが選択しなくても自動的にネットワークに接続します。 デフォルトは自動接続です。
- マシン接続タイプの選択：ユーザー定義ネットワークを追加するときに、エンドユーザーに対して [ログオン前に接続を許可（Allow Connection Before Logon）] の選択を有効にします。エンドユーザーの選択によって、ユーザーがログインする前にネットワークが接続できるかどうかが決まります。次に、個人、共有 WEP、またはオープンセキュリティを選択できます。

[デフォルトで有効にする（Enable by Default）]：ユーザー定義ネットワークを追加するときに、エンドユーザーに対して[ログオン前の接続を許可（Allow Connection Before Logon）]を自動的に許可します。

（注） AnyConnectを以前のバージョンから4.9.01095以降にアップグレードする場合、新しい機能で更新されたxmlを取得するために、適切なプロファイルエディタでconfiguration.xmlファイルを開き、ファイルを保存する必要があります。

管理ステータス

- [サービス オペレーション（Service Operation）]：このサービスをオフにすると、このプロファイルを使用しているクライアントはレイヤ2接続を確立するために接続できません。
- [FIPSモード（FIPS Mode）]：FIPSモードを有効にすると、Network Access Managerは政府の要件を満たす方法で暗号化操作を行います。

  連邦情報処理標準（FIPS 140-2 Level 1）は、暗号化モジュールのセキュリティ要件を指定する米国政府標準規格です。FIPSは、ソフトウェアとハードウェアのタイプに応じて、MACsecまたはWi-Fi用のNetwork Access Managerでサポートされています。

表 *7: Network Access Manager*による *FIPS* サポート

メディア/オペレーティング システム	**Windows 7** 以降
MACsecで有線	Intel HW MACsec対応NICの場合、またはハードウェア以外のMACsecを使用している場合にFIPSに準拠しています。
Wi-Fi	FIPSに準拠していません。

認証ポリシーウィンドウ

[認証ポリシー（Authentication Policy）]ウィンドウでは、すべてのネットワーク接続に適用される、アソシエーションおよび認証ネットワークフィルタを作成できます。アソシエーションモードまたは認証モードのいずれもオンにしない場合、認証Wi-Fiネットワークに接続できません。モードのサブセットを選択すると、それらのタイプのネットワークにのみ接続できます。目的のアソシエーション モードまたは認証モードをそれぞれ選択するか、[すべて選択（Select All）]を選択します。

内部方式も特定の認証プロトコルのみに制限される可能性があります。内部方式は、[許可された認証モード（Allowed Authentication Modes）]ペインの外部方式（トンネリング）下にインデントされて表示されます。

認証プロトコル選択のメカニズムは、現在のクライアント認証データベースと統合されています。セキュアなワイヤレス LAN 展開では、ユーザが新しい認証システムを作成する必要はありません。

内部トンネリングに使用できる EAP 方式は、内部方式のクレデンシャル タイプと外部トンネリング方式に基づいています。次のリストで、外部トンネル方式はそれぞれ、各クレデンシャル タイプに対応した内部方式の種類を一覧表示しています。

- PEAP
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-FAST
  - パスワード クレデンシャル：EAP-MSCHAPv2 または EAP-GTC
  - トークン クレデンシャル：EAP-GTC
  - 証明書クレデンシャル：EAP-TLS
- EAP-TTLS
  - パスワードクレデンシャル：EAP-MSCHAPv2、EAP-MD5、PAP（L）、CHAP（L）、MSCHAP（L）、MSCHAP-v2（レガシー）。
  - トークン クレデンシャル：PAP（レガシー）。チャレンジ/レスポンス方式はトークン ベースの認証には適していないため、Network Access Managerでサポートされるデフォルト トークン オプションは PAP です。
  - 証明書クレデンシャル：該当なし。

[ネットワーク（Networks）] ウィンドウ

[ネットワーク（Networks）] ウィンドウでは、企業ユーザの事前定義ネットワークを設定できます。すべてのグループで使用できるネットワークを設定するか、または特定のネットワークで使用するグループを作成できます。[ネットワーク（Networks）] ウィンドウには、既存のウィンドウにペインを追加できるウィザードが表示され、[次へ（Next）] をクリックしてより多くの設定オプションに進むことができます。

グループとは、基本的に、設定された接続（ネットワーク）の集合です。設定された各接続は、グループに属するか、すべてのグループのメンバーである必要があります。

（注） 下位互換性を確保するため、Cisco Secure Services Client で展開された管理者作成のネットワークは、SSID をブロードキャストしない非表示ネットワークとして扱われます。ユーザ ネットワークは、SSID をブロードキャストするネットワークとして扱われます。

新しいグループを作成できるのは管理者だけです。設定にグループが定義されていない場合、プロファイルエディタによって自動生成グループが作成されます。自動生成グループには、管理者定義のグループに割り当てられていないネットワークが含まれます。クライアントは、アクティブ グループに定義されている接続を使用してネットワーク接続の確立を試みます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create Networks）] オプションの設定に応じて、エンド ユーザは、ユーザ ネットワークをアクティブ グループに追加するか、アクティブ グループからユーザ ネットワークを削除できます。

定義されているネットワークは、リストの先頭にあるすべてのグループで使用できます。グローバル ネットワーク内にどのネットワークがあるかを制御できるため、ユーザ定義のネットワークが存在する場合も、エンドユーザが接続できる企業ネットワークを指定できます。エンド ユーザは管理者が設定したネットワークを変更したり、削除したりできません。

（注） エンドユーザは、globalNetworks セクションのネットワークを除き、グループにネットワークを追加できます。これらのネットワークはすべてのグループ内に存在し、プロファイルエディタを使用してしか作成できないためです。

企業ネットワークの一般的なエンドユーザは、このクライアントを使用するためにグループの知識は必要ありません。アクティブ グループは設定内の最初のグループですが、グループが 1 つしか使用できない場合、アクティブ グループは認識されず、表示されません。一方で、複数のグループが存在する場合、UI にはアクティブ グループが選択されたことを示すグループのリストが表示されます。ユーザはアクティブ グループから選択でき、設定はリブート後も保持されます。[ネットワーク グループ（Network Groups）] ウィンドウの [ネットワークの作成（Create Networks）] オプションの設定に応じて、エンド ユーザは、グループを使用せずに自分のネットワークを追加または削除できます。

（注） グループ選択はリブート後も持続して、ネットワークは修復されます（そのためには、トレイアイコンを右クリックしながら [ネットワーク修復（Network Repair）] を選択します）。Network Access Managerが修復されるか、またはリスタートされると、以前のアクティブなグループが使用されます。

ネットワーク、メディアタイプページ

[ネットワーク（Networks）] ウィンドウの [メディア タイプ（Media Type）] ページにより、有線ネットワークまたはワイヤレス ネットワークを作成または編集できます。設定は、選択内容によって異なります。

最初のダイアログには、次のセクションが含まれています。

- [名前（Name）]：このネットワーク用に表示される名前を入力します。
- [グループ メンバーシップ（Group Membership）]：このプロファイルが使用できるようにするネットワーク グループ（複数の場合もあり）を選択します。

- [ネットワーク メディア（Network Media）]：[有線（Wired）] または [Wi-Fi（ワイヤレス）（Wi-Fi (wireless)）] を選択します。[Wi-Fi] を選択すると、次のパラメータも設定できます。
  - [SSID]：ワイヤレス ネットワークの SSID（サービス セット識別子）を入力します。
  - [非表示ネットワーク（Hidden Network）]：SSID をブロードキャストしない場合でも、ネットワークへの接続を許可します。
  - [社内ネットワーク（Corporate Network）]：[社内（Corporate）] として設定されたネットワークが近接にある場合、まずそのネットワークに強制的に接続します。社内ネットワークが非ブロードキャスト（非表示）SSID を使用し、非表示として設定されている場合、Network Access Managerは非表示 SSID をアクティブにプローブし、企業 SSID が範囲内にあれば接続を確立します。
  - [アソシエーション タイムアウト（Association Timeout）]：Network Access Managerが、使用できるネットワークを再評価するまでに特定のワイヤレス ネットワークとのアソシエーションを待機する時間を入力します。デフォルトのアソシエーション タイムアウトは 5 秒です。
- 共通設定
  - [スクリプトまたはアプリケーション（Script or application）]：ローカル システムで実行するファイルのパスとファイル名を入力するか、フォルダを参照してファイルを選択します。次のルールは、スクリプトおよびアプリケーションに適用されます。
    - .exe、.bat、または .cmd 拡張子のファイルが受け入れられます。
    - ユーザは、管理者が作成したネットワークで定義されたスクリプトまたはアプリケーションは変更できません。
    - プロファイルエディタを使用してパスおよびスクリプトまたはアプリケーションのファイル名のみを指定できます。スクリプトまたはアプリケーションがユーザのマシンに存在しない場合、エラー メッセージが表示されます。ユーザは、スクリプトまたはアプリケーションがマシンにないこと、およびシステム管理者に問い合わせる必要があると通知されます。
    - アプリケーションがユーザのパスに存在する場合を除いて、実行するアプリケーションのフル パスを指定する必要があります。アプリケーションがユーザのパスに存在する場合は、アプリケーション名またはスクリプト名だけを指定できます。
    - [接続タイムアウト（Connection Timeout）]：Network Access Managerが、（接続モードが自動の場合）別のネットワークに接続しようとするか、または別のアダプタを使用するまでにネットワーク接続の確立を待機する秒数を入力します。

（注） 認証を完了するまでに 60 秒近くかかるスマートカード認証システムもあります。スマートカードを使用している場合、特に、スマートカードが接続に成功するまでにいくつかネットワークに接続しなければならない場合に、[接続タイムアウト（Connection Timeout）] 値を増やす必要があります。

（注） 特定のスマートカードミドルウェアで見つかった問題を軽減するために、AnyConnect Network Access Manager はテストデータに対して署名操作を実行し、その署名を検証することで、スマートカード PIN を検証します。このテスト署名はスマートカードにある証明書ごとに行われ、証明書の数によってはスマートカード認証が大幅に遅延する場合があります。テスト署名操作を無効にする場合は、 HKEY_LOCAL_MACHINE/SOFTWARE/Cisco/AnyConnect Network Access Manager でレジストリエントリに **DisableSmartcardPinVerifyBySigning** を追加して DWORD を 1 に設定できます。このキーを有効にする変更を加える場合は、正しく動作するように、すべてのスマートカードおよび関連するハードウェアでその変更を完全にテストしてください。

ネットワーク、セキュリティ レベルページ

[ネットワーク（Networks）] ウィザードの [セキュリティ レベル（Security Level）] ページで、[オープン ネットワーク（Open Network）]、[認証ネットワーク（Authentication Network）]、または（ワイヤレス ネットワーク メディアにのみ表示される）[共有キー ネットワーク（Shared Key Network）] を選択します。これらのネットワーク タイプの設定フローはそれぞれ異なっており、次の項で説明します。

- 認証ネットワークの設定：企業を安全に保つために推奨されます。
- オープン ネットワークの設定：推奨されません。ただし、キャプティブ ポータル環境を介したゲスト アクセスの提供に使用できます。Network Access Managerは、キャプティブ ポータルの状態にあるときはブラウザの自動起動をサポートしません。
- 共有キー ネットワークの設定：小規模オフィスまたはホーム オフィスなどの無線ネットワークに推奨されます。

認証ネットワークの設定

[セキュリティ レベル（Security Level）] セクションで [認証ネットワーク（Authenticating Network）] を選択した場合、次に説明するペインが追加で表示されます。これらのペインの設

定を完了したら、[次へ（Next）] ボタンをクリックするか、[接続タイプ（Connection Type）] タブを選択して [ネットワーク接続タイプ（Network Connection Type）] ダイアログを開きます。

802.1X 設定ペイン

ネットワーク設定に応じて IEEE 802.1X 設定を調整します。

（注） AnyConnect ISE ポスチャがNetwork Access Managerとともにインストールされた場合、ISE ポスチャはNetwork Access Manager プラグインを使用してネットワーク変更イベントと 802.1X WiFi を検出します。

- [authPeriod (sec)]：認証が開始された場合、認証メッセージの間隔がこの設定を超えるとサプリカントはタイムアウトします。認証を再度開始するには、サプリカントでオーセンティケータが必要です。
- [heldPeriod (sec)]：認証が失敗した場合、サプリカントはこの設定で定義された時間だけ待機し、この時間を超えると別の認証が試行されます。
- [startPeriod (sec)]：EAPOL-Start メッセージに対する応答をオーセンティケータから受信しない場合に、EAPOL-Start メッセージを再送信する間隔（秒）です。
- [maxStart]：サプリカントが、オーセンティケータが存在しないと見なす前に、IEEE 801.X プロトコル パケット、EAPOL Key データ、または EAPoL-Start を送信することで、サプリカントがオーセンティケータの認証を開始する回数です。これが発生した場合は、サプリカントはデータ トラフィックを許可します。

ヒント 単一の認証有線接続がオープンおよび認証ネットワークの両方と動作するように設定できます。これは、[startPeriod] および [maxStart] を注意深く設定して、認証開始試行に費やす合計時間がネットワーク接続タイマーよりも小さくなるようにします（[startPeriod] x [maxStart] < ネットワーク接続タイマー）。

このシナリオでは、ネットワーク接続タイマーを（[startPeriod] x [maxStart]）秒だけ大きくして、DHCPアドレスを取得してネットワーク接続を完了するために十分な時間をクライアントに与えることに注意してください。

逆に、認証が成功した後にのみデータ トラフィックを許可するには、認証の開始に費やした総時間がネットワーク接続タイマーより長くなるような [startPeriod] および [maxStart] になるようにします（[startPeriod] x [maxStart] > ネットワーク接続タイマー）。

セキュリティペイン

有線ネットワークの場合にのみ表示されます。

[セキュリティ（Security）] ペインで、次のパラメータの値を選択します。

- [キー管理（Key Management）]：MACsec 対応有線ネットワークで使用するキー管理プロトコルを決定します。
  - [なし（None）]：キー管理プロトコルを使用しません。また、有線暗号化を実行しません。
  - [MKA]：サプリカントは、MACsec キー承諾プロトコル ポリシーと暗号キーをネゴシエートしようとします。MACsec は MAC レイヤ セキュリティで、有線ネットワークで MAC レイヤ暗号化を行います。MACsec プロトコルは、暗号化を使用して MAC レベル フレームを保護する手段であり、MACsec Key Agreement（MKA）エンティティに依存して暗号キーをネゴシエートおよび配布します。
- [暗号化（Encryption）]
  - [なし（None）]：データ トラフィックの整合性チェックは行われますが、暗号化はされません。
  - [MACsec: AES-GCM-128]：このオプションは、キー管理に MKA を選択した場合のみ使用できます。AES-GCM-128 を使用して、データ トラフィックが暗号化されます。
  - [MACsec: AES GCM 256]： このオプションは、エンタープライズ エッジ（eEdge）統合を備えた特定の IOS バージョンでサポートされており、キー管理に MKA を選択した場合にのみ使用できます。スイッチ側の設定が一致する必要があります。MACsec 256 暗号化規格を有効にすることによって、MACsec Key Agreement（MKA）を使用した802.1AE 暗号化は、MACsec 対応デバイスとホスト デバイス間の暗号化用にダウンリンク ポートでサポートされています。

詳細については、「Identity-Based Networking Services: MAC Security」を参照してください。

ポート認証例外ポリシーペイン

このペインは、有線ネットワークでのみ表示されます。

[ポート認証例外ポリシー（Port Authentication Exception Policy）] ペインでは、認証プロセス中の IEEE 802.1X サプリカントの動作を変更できます。ポート例外が有効でない場合、サプリカントはその既存の動作を続け、設定が完全に成功した場合のみ（または、この項で前述したように、オーセンティケータからの応答がない状態で maxStarts 数の認証が開始された後に）ポートを開きます。次のいずれかのオプションを選択します。

- [認証前にデータ トラフィックを許可（Allow data traffic before authentication）]：認証試行の前にデータ トラフィックが許可されます。
- [次の場合でも認証後にデータ トラフィックを許可（Allow data traffic after authentication even if）]：次の場合でもデータ トラフィックが許可されます。
  - [EAP 失敗（EAP Fails）]：選択すると、EAP が失敗した場合でも、サプリカントは認証を試行します。認証に失敗した場合、サプリカントは認証に失敗したにもかかわらず、データ トラフィックを許可します。

- [EAP は成功したがキー管理に失敗（EAP succeeds but key management fails）]：選択すると、EAP は成功してキー管理が失敗した場合、サプリカントはキー サーバとのキーのネゴシエートを試行しますが、何らかの理由によりキー ネゴシエーションに失敗した場合でもデータ トラフィックを許可します。この設定は、キー管理が設定されている場合のみ有効です。キー管理がなしに設定されている場合、このチェックボックスは淡色表示されます。

制約事項 MACsec には、ACS バージョン 5.1 以降および MACsec 対応スイッチが必要です。ACS またはスイッチの設定については、『*Catalyst 3750-X and 3560-X Switch Software Configuration Guide*』を参照してください。

アソシエーション モード

このペインは、ワイヤレス ネットワークの場合にのみ表示されます。

アソシエーション モードを選択します。

- WEP
- WAP Enterprise（TKIP）
- WPA Enterprise（AES）
- WPA 2 Enterprise（TKIP）
- WPA 2 Enterprise（AES）
- CCKM（TKIP）：（Cisco CB21AG ワイヤレス NIC が必要）
- CCKM（AES）：（Cisco CB21AG ワイヤレス NIC が必要）

オープン ネットワークの設定

オープン ネットワークは、認証や暗号化を使用しません。オープン（非セキュア）ネットワークを作成するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ レベル（Security Level）] ページで [オープン ネットワーク（Open Network）] を選択します。この選択肢では、最もセキュリティ レベルの低いネットワークが提供されます。これは、ゲスト アクセス ワイヤレス ネットワークに推奨されています。

ステップ 2 [次へ（Next）] をクリックします。

ステップ 3 接続タイプを決定します。

共有キー ネットワークの設定

Wi-Fi ネットワークは、エンドポイントとネットワーク アクセス ポイント間のデータを暗号化する際に使用される暗号キーを導出するために、共有キーを使用することがあります。WPA または WPA2 Personal を備えた共有キーを使用すると、小規模オフィスや自宅オフィスに適した Medium レベルのセキュリティ クラスが実現します。

（注） 共有キーによるセキュリティは、企業ワイヤレス ネットワークには推奨しません。

セキュリティ レベルを共有キー ネットワークにする場合は、次の手順を実行します。

手順

ステップ 1 [共有キー ネットワーク（Shared Key Network）] を選択します。

ステップ 2 [セキュリティ レベル（Security Level）] ウィンドウで [次へ（Next）] をクリックします。

ステップ 3 [ユーザ接続（User Connection）] または [マシン接続（Machine Connection）] を指定します。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [共有キー タイプ（Shared Key Type）]：共有キーのタイプを決定する共有キー アソシエーション モードを指定します。次の選択肢があります。

- [WEP]：スタティック WEP 暗号化とのレガシー IEEE 802.11 オープン システム アソシエーション。
- [Shared]：スタティック WEP 暗号化とのレガシー IEEE 802.11 共有キー アソシエーション。
- [WPA/WPA2-Personal]：パスフレーズ事前共有キー（PSK）から暗号キーを導出する Wi-Fi セキュリティ プロトコル。

ステップ 6 レガシー IEEE 802.11 WEP または共有キーを選択した場合は、40 ビット、64 ビット、104 ビット、または 128 ビットを選択します。40 または 64 ビットの WEP キーは、5 個の ASCII 文字または 10 桁の 16 進数である必要があります。104 または 128 ビットの WEP キーは、13 個の ASCII 文字または 26 桁の 16 進数である必要があります。

ステップ 7 WPA または WPA2 Personal を選択した場合は、（TKIP/AES）を使用する暗号化のタイプを選択し、共有キーを入力します。入力するキーは、8 ～ 63 個の ASCII 文字またはちょうど 64 桁の 16 進数である必要があります。共有キーが ASCII 文字で構成されている場合は、[ASCII] を選択します。共有キーに 64 桁の 16 進数が含まれている場合は、[16進数（Hexadecimal）] を選択します。

ステップ 8 [完了（Done）] をクリックします。[OK] をクリックします。

ネットワーク、ネットワーク接続タイプペイン

ここでは、Network Access Manager プロファイル エディタの [セキュリティ レベル（Security Level）] に続く、[ネットワーク（Networks）] ウィンドウの [ネットワーク接続タイプ（network connection type）] ペインについて説明します。次のいずれかの接続タイプを選択します。

- [マシン接続（Machine Connection）]：Windows Active Directory に保存されているデバイス名が認証に使用されます。マシン接続は通常、接続時にユーザ クレデンシャルが必要ない場合に使用します。ユーザがログオフし、ユーザ クレデンシャルが使用できない場合でも、エンドステーションがネットワークにログインする必要がある場合にこのオプションを選択します。このオプションは通常、ユーザがアクセスする前に、ドメインに接続し、ネットワークから GPO および他のアップデートを取得する場合に使用します。

  （注） 既知のネットワークが使用できない場合、VPN Start Before Login（SBL）は失敗します。SBL モードで許可されるネットワーク プロファイルには、非 802-1X 認証モードを採用するすべてのメディア タイプ（オープン WEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。Network Access Managerを [ユーザがログインする前（Before User Logon）] に、およびマシン接続認証用に設定している場合、Network Access Manager はユーザにネットワーク情報を要求し、VPN SBL は正常に行われます。

- [ユーザ接続（User Connection）]：ユーザ クレデンシャルを認証に使用します。

  [クライアント ポリシー（Client Policy）] ペインで [ユーザがログインする前（Before User Logon）] が選択されている場合、Windows スタート画面でユーザがログイン クレデンシャルを入力した後、Network Access Managerはユーザのクレデンシャルを収集します。Windows がユーザの Windows セッションを開始している間に、ネットワーク接続が確立されます。

  [クライアント ポリシー（Client Policy）] ペインで [ユーザがログインした後（After User Logon）] が選択されている場合、ユーザが Windows にログインしてから、接続が開始されます。

  ユーザがログオフすると、現在のユーザのネットワーク接続は終了します。マシン ネットワーク プロファイルが使用可能な場合、NAM はマシン ネットワークに再接続します。

- [マシンおよびユーザ接続（Machine and User Connection）]：[セキュリティ レベル（Security Level）] ペインで選択したように、[認証ネットワーク（Authenticating Network）] を設定している場合にのみ指定できます。マシン ID とユーザ クレデンシャルの両方を使用しますが、マシン部分はユーザがデバイスにログインしていない場合のみ有効です。2 つの部分の設定は同じですが、マシン接続の認証タイプとクレデンシャルは、ユーザ接続の認証タイプとクレデンシャルと異なる場合があります。

  マシン接続を使用していてユーザがログインしていないとき、およびユーザ接続を使用していてユーザがログインしているときにネットワークに PC を常時接続するには、このオプションを選択します。

EAP-FAST が（次のペインで）EAP 方式として設定されている場合、EAP チェーンがサポートされています。つまり、Network Access Managerによって、マシンおよびユーザが既知のエンティティであり、企業によって管理されていることが検証されます。

このネットワーク接続タイプを選択すると、[ネットワーク（Networks）] ダイアログに追加のタブが表示されます。これらのタブでは、選択されたネットワーク接続タイプの EAP 方式とクレデンシャルを設定できます。

ネットワーク、ユーザまたはマシンの認証ページ

ネットワーク接続タイプを選択した後、それらの接続タイプの認証方式を選択します。認証方式を選択した後、選択した方式に対応するように表示が更新され、追加情報を提供するように要求されます。

（注） MACsec を有効にした場合は、PEAP、EAP-TLS、または EAP-FAST などの MSK キー派生をサポートする EAP 方式を必ず選択します。また、MACsec が有効でない場合にも、Network Access Managerを使用すると、MACsec を考慮して MTU が 1500 から 1468 に削減されます。

EAP の概要

EAP は、認証プロトコルを伝送するトランスポート プロトコルから認証プロトコルをデカップリングするための要件を示した IETF RFC です。このデカップリングによって、トランスポート プロトコル（IEEE 802.1X、UDP、または RADIUS など）は、認証プロトコルを変更せずに EAP プロトコルを伝送できます。

基本的な EAP プロトコルは、次の 4 つのパケット タイプから構成されます。

- EAP要求：オーセンティケータは、要求パケットをサプリカントに送信します。各要求にはtypeフィールドがあり、要求されている内容を示します。これには、使用するサプリカント アイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。
- EAP応答：サプリカントは応答パケットをオーセンティケータに送信し、シーケンス番号を使用して元の EAP 要求と照合します。EAP 応答のタイプは、通常 EAP 要求と一致しますが、応答が負（NAK）の場合は除きます。
- EAP成功：オーセンティケータは認証に成功した場合にサプリカントに成功パケットを送信します。
- EAP失敗：オーセンティケータは、認証が失敗した場合、サプリカントに失敗パケットを送信します。

EAP が IEEE 802.11X システムで使用中の場合、アクセス ポイントは EAP パススルー モードで動作します。このモードでは、アクセスポイントはコード、識別子、および長さのフィールドを確認して、サプリカントから受信したEAPパケットをAAAサーバーに転送します。AAAサーバーオーセンティケータから受信したパケットは、サプリカントに転送されます。

EAP-GTC

EAP-GTCは、単純なユーザ名とパスワード認証に基づくEAP認証方式です。チャレンジ/レスポンス方式を使用せずに、ユーザ名とパスワードの両方がクリアテキストで渡されます。この方式は、トンネリング EAP 方式の内部で使用（次のトンネリング EAP 方式を参照）、またはワンタイム パスワード（OTP）を使用する場合に推奨されます。

EAP-GTCは、相互認証を提供しません。クライアントのみ認証するため、不正なサーバがユーザのクレデンシャルを取得するおそれがあります。相互認証が必要な場合、EAP-GTC はトンネリング EAP 方式の内部で使用され、サーバ認証を提供します。

EAP-GTCによりキー関連情報は提供されないため、MACsecではこの方式は使用できません。さらなるトラフィック暗号化のためにキー関連情報が必要な場合、EAP-GTC はトンネリング EAP 方式の内部で使用され、キー関連情報（および必要に応じて内部および外部の EAP 方式の暗号化バインド）を提供します。

パスワード ソース オプションには、次の 2 つがあります。

- [パスワードを使った認証（Authenticate using a Password）]：十分に保護された有線環境にのみ適しています。
- [トークンを使った認証（Authenticate using a Token）]：トークン コードまたは OTP のライフタイムが短い（通常約 10 秒）ため、より高いセキュリティを備えています。

（注） Network Access Manager、オーセンティケータ、またはEAP-GTCプロトコルのいずれもパスワードとトークン コード間を区別できません。これらのオプションは、Network Access Manager内のクレデンシャルのライフタイムにのみ影響を与えます。パスワードは、ログアウトまでかそれ以降も記憶できますが、トークン コードは記憶できません（認証ごとにユーザがトークン コードの入力を求められるため）。

パスワードが認証に使用される場合、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。これは、パスワードがオーセンティケータにクリアテキストで渡されるためです。この方式は、データベースがリークしている可能性がある場合に推奨されます。

EAP-TLS

EAP-Transport Layer Security（EAP-TLS）は、TLSプロトコル（RFC 2246）に基づくIEEE 802.1X EAP 認証アルゴリズムです。TLS は、X.509デジタル証明書に基づく相互認証を使用します。EAP-TLS メッセージ交換は、相互認証、暗号スイート ネゴシエーション、キー交換、クライアントと認証サーバ間の検証、およびトラフィック暗号化に使用できるキー関連情報を提供します。

次のリストに、EAP-TLSクライアント証明書が有線およびワイヤレス接続に強固な認証を提供できる主な理由を示します。

- 通常、ユーザが介入することなく認証が自動で実行される。
- ユーザ パスワードへの依存がない。
- デジタル証明書が強固な認証保護を提供する。
- メッセージ交換が公開キー暗号化により保護される。
- 証明書がディクショナリ攻撃の被害を受けにくい。
- 認証プロセスにより、データ暗号化および署名のための相互決定されたキーが生成される。

EAP-TLS には、次の 2 つのオプションが含まれています。

- [サーバ証明書の確認（Validate Server Certificate）]：サーバ証明書の検証を有効にします。
- [高速再接続を有効にする（Enable Fast Reconnect）]：TLS セッション再開を有効にします。これにより、TLS セッション データがクライアントとサーバの両方で保持されている限り、短縮化した TLS ハンドシェイクを使用することによってはるかに高速な再認証ができます。

（注） [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）] オプションは、マシン接続認証では使用できません。

EAP-TTLS

EAP-Tunneled Transport Layer Security（EAP-TTLS）は、EAP-TLS 機能を拡張する 2 フェーズのプロトコルです。フェーズ 1 では、完全な TLS セッションを実行して、フェーズ 2 で使用するセッション キーを導出し、サーバとクライアント間で属性を安全にトンネリングします。フェーズ2 中では、トンネリングされた属性を使用して、多数のさまざまなメカニズムを使用する追加認証を実行できます。

Network Access Managerは、EAP-TTLS 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

フェーズ 2 で使用できる認証メカニズムには、次のプロトコルが含まれます。

- PAP（パスワード認証プロトコル）：ピアが 2 ウェイ ハンドシェイクを使用してそのアイデンティティを証明する単純な方式を提供します。ID/パスワード ペアは、認証が認められるか失敗するまで、ピアからオーセンティケータに繰り返し送信されます。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。

パスワードがオーセンティケータに渡されるため、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。データベースがリークしている可能性がある場合は、この方式をお勧めします。

（注） EAP-TTLS PAP は、トークンおよびOTP ベースの認証で使用できます。

- CHAP（チャレンジ ハンドシェイク認証プロトコル）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
- MS-CHAP（Microsoft CHAP）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します。相互認証が必要な場合は、EAP-TTLS を設定して、フェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用する場合は、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hash のいずれかを保存しておく必要があります。
- MS-CHAPv2：応答パケット内にピア チャレンジおよび成功パケット内にオーセンティケータ応答を含めることによって、ピア間の相互認証を提供します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃を防ぐために）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。

EAP-TTLS の設定

- EAP：次の EAP 方法の使用を許可します。
  - EAP-MD5（EAP Message Digest 5）：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを検証します（CHAP と類似）。このチャレンジ/レスポンス方式を使用する場合、オーセンティケータのデータベースにクリア テキスト パスワードを保存する必要があります。
  - EAP-MSCHAPv2：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、EAP-TTLS を設定してフェーズ 1 でサーバの証明書を検証する必要があります。パスワードのNT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードのNT-hash のいずれかを保存しておく必要があります。
- EAP-TTLS 設定

- [サーバーIDの検証（Validate Server Identity）]：サーバー証明書の検証を有効にします。

（注） これを有効にする場合は、RADIUS サーバーにインストールされたサーバー証明書にサーバー認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバーでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワーク アクセスおよび認証のためにこのサーバ認証設定が必要です。

- [高速再接続を有効にする（Enable Fast Reconnect）]：内部認証が省略されるかどうか、またはオーセンティケータによって制御されているかどうかに関係なく、外部 TLS セッション再開のみを有効にします。

（注） [スマートカードを使用するときは無効にする（Disable When Using a Smart Card）] は、マシン接続認証では使用できません。

- [内部方式（Inner Methods）]：TLS トンネルが作成された後で内部方式の使用を指定します。Wi-Fi メディア タイプにのみ使用できます。

PEAP オプション

Protected EAP（PEAP）は、トンネリング TLS ベースの EAP 方式です。PEAP は、内部認証方式の暗号化に対するクライアント認証の前に、サーバ認証にTLSを使用します。内部認証は、信頼される暗号保護されたトンネル内部で実行され、証明書、トークン、およびパスワードを含む、さまざまな内部認証方式をサポートします。Network Access Managerは、PEAP 認証中に使用する内部および外部方式の暗号化バインドをサポートしません。暗号化バインドが必要な場合は、EAP-FAST を使用する必要があります。暗号化バインドは、クレデンシャルを知らなくても攻撃者がユーザの接続をハイジャックできる中間者攻撃の特殊クラスからの保護を提供します。

PEAP は、次のサービスを提供することによって EAP 方式を保護します。

- EAP パケットに対する TLS トンネル作成
- メッセージ認証
- メッセージの暗号化
- クライアントに対するサーバの認証

次の認証方式を使用できます。

- パスワードを使った認証

- EAP-MSCHAPv2：3 ウェイ ハンドシェイクを使用してピアのアイデンティティを確認します。サーバの前に、クライアントが認証されます。（ディクショナリ攻撃の防止のためなどで）サーバをクライアントの前に認証する必要がある場合、PEAP を設定してサーバの証明書を検証する必要があります。パスワードの NT-hash に基づいてチャレンジ/レスポンス方式を使用して、オーセンティケータのデータベースにクリアテキストパスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。
- EAP-GTC（EAP Generic Token Card）：ユーザ名とパスワードを伝送するために EAP エンベロープを定義します。相互認証が必要な場合は、PEAP を設定してサーバの証明書を検証する必要があります。パスワードがクリアテキストでオーセンティケータに渡されるため、ハッシュ化パスワードを使用するデータベースに対しての認証でこのプロトコルを使用できます。この方式は、データベースがリークしている可能性がある場合に推奨されます。

- 証明書を使った EAP-TLS
  - EAP-TLS：ユーザ証明書を伝送するために EAP エンベロープを定義します。中間者攻撃（有効なユーザの接続のハイジャック）を避けるため、同じオーセンティケータに対する認証用に PEAP（EAP-TLS）および EAP-TLS プロファイルを混在させないことをお勧めします。その設定に応じて、オーセンティケータを設定する必要があります（プレーンおよびトンネリングされた EAP-TLS の両方を有効にしない）。

PEAP の設定

- PEAP-EAP 設定
  - [サーバーIDの検証（Validate Server Identity）]：サーバー証明書の検証を有効にします。

（注） これを有効にする場合は、RADIUS サーバーにインストールされたサーバー証明書にサーバー認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバーでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワーク アクセスおよび認証のためにこのサーバ認証設定が必要です。

  - [高速再接続を有効にする（Enable Fast Reconnect）]：外部 TLS セッション再開のみを有効にします。オーセンティケータは、内部認証を省略するかどうかを制御します。
  - [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）]：スマート カードを使用して認証する場合に高速再接続を使用しません。スマート カードは、ユーザ接続にのみ適用されます。
  - [トークンおよび EAP-GTC を使用して認証する（Authenticate using a token and EAP-GTC）]：マシン認証には使用できません。

- クレデンシャル ソースに基づく内部方式
  - [パスワードを使用した認証（Authenticate using a password）]：[EAP-MSCHAPv2] または [EAP-GTC]。
  - [証明書を使用した認証（Authenticate using a certificate）]：EAP-TLS に対応。
  - [トークンおよび EAP-GTC を使用して認証する（Authenticate using a token and EAP-GTC）]：マシン認証には使用できません。

（注） ユーザ ログインの前に、スマート カードのサポートは Windows では使用できません。

EAP-FAST 設定

EAP-FAST は、IEEE 802.1X 認証タイプで、柔軟性があり、展開や管理も容易です。EAP-FAST は、さまざまなユーザーおよびパスワード データベース タイプ、サーバ主導のパスワードの失効と変更、およびデジタル証明書（任意）をサポートします。

EAP-FAST は、証明書を使用せず、ディクショナリ攻撃からの保護を提供する IEEE 802.1X EAP タイプを展開するお客様向けに開発されました。

マシン接続とユーザー接続の両方が設定されている場合、EAP チェーンがサポートされています。これは、Network Access Managerが、マシンおよびユーザーが既知のエンティティであり、企業によって管理されていること検証することを意味し、社内ネットワークに接続しているユーザー所有資産を制御するのに便利です。EAP チェーンの詳細については、RFC 3748 を参照してください。

EAP-FAST は、TLS メッセージを EAP 内にカプセル化します。また、次の 3 つのプロトコル フェーズから構成されます。

1. Authenticated Diffie-Hellman Protocol（ADHP）を使用して Protected Access Credential（PAC）と呼ばれる共有秘密クレデンシャルを持つクライアントをプロビジョニングするプロビジョニング フェーズ。
2. トンネルの確立に PAC を使用するトンネル確立フェーズ。
3. 認証サーバでユーザーのクレデンシャル（トークン、ユーザー名/パスワード、またはデジタル証明書）を認証する認証フェーズ。

他のトンネリング EAP 方式とは異なり、EAP-FAST は内部および外部方式間に暗号化バインドを提供して、攻撃者が有効なユーザーの接続をハイジャックする特殊な中間者攻撃を防止します。

EAP-FAST の設定

- EAP-FAST 設定

- [サーバーIDの検証（Validate Server Identity）]：サーバー証明書の検証を有効にします。これを有効にすると、管理ユーティリティに2つの追加のダイアログが導入されて、Network Access Manager プロファイル エディタのタスク リストに [証明書（Certificate）] ペインがさらに追加されます。

（注） これを有効にする場合は、RADIUS サーバーにインストールされたサーバー証明書にサーバー認証の拡張キーの使用状況（EKU）が含まれていることを確認します。RADIUS サーバーでは、認証時にクライアントにその設定済みの証明書を送信するとき、ネットワーク アクセスおよび認証のためにこのサーバ認証設定が必要です。

- [高速再接続を有効にする（Enable Fast Reconnect）]：セッション再開を有効にします。EAP-FAST で認証セッションを再開する 2 つのメカニズムには、内部認証を再開するユーザ認可 PAC と、短縮化した外部 TLS ハンドシェイクができる TLS セッション再開があります。この [高速再接続を有効にする（Enable Fast Reconnect）] パラメータは、両方のメカニズムを有効または無効にします。オーセンティケータがいずれを使用するかを決定します。

（注） マシン PAC は、短縮化した TLS ハンドシェイクを提供し、内部認証を省きます。この制御は、PACパラメータを有効/無効にすることによって処理します。

（注） [スマート カードを使用するときは無効にする（Disable When Using a Smart Card）] オプションは、ユーザ接続認証にのみ使用できます。

- [クレデンシャル ソースに基づく内部方式（Inner methods based on Credentials Source）]：パスワードまたは証明書を使用する認証ができます。
  - [パスワードを使用した認証（Authenticate using a password）]：[EAP-MSCHAPv2] または [EAP-GTC]。EAP-MSCHAPv2 は、相互認証を提供しますが、サーバーを認証する前にクライアントを認証します。サーバーを最初に認証する相互認証を使用する場合は、EAP-FAST を認証付きプロビジョニングのみに設定して、サーバーの証明書を検証します。パスワードの NT-hash に基づいてこのチャレンジ/レスポンス方式を使用して、EAP-MSCHAPv2 を使用する場合は、オーセンティケータのデータベースにクリア テキスト パスワード、または最低でもパスワードの NT-hash のいずれかを保存しておく必要があります。パスワードは EAP-GTC 内でクリア テキストでオーセンティケータに渡されるため、データベースに対する認証でこのプロトコルを使用できます。

- [証明書を使用した認証（Authenticate using a certificate）]：証明書を使用する認証に対しての基準を、要求された場合にクライアント証明書を暗号化しないで送信、トンネル内でのみクライアント証明書を送信、またはトンネル内で EAP-TLS を使用してクライアント証明書を送信から決定します。
- トークンおよび EAP-GTC を使用して認証します。

- [PAC を使用する（Use PACs）]：EAP-FAST 認証での PAC の使用を指定できます。PAC は、ネットワーク認証を最適化するためにクライアントに配布されるクレデンシャルです。

（注） EAP-FAST では大半の認証サーバーが PAC を使用するため、通常は PAC オプションを使用します。このオプションを削除する前に、認証サーバーが EAP-FAST で PAC を使用しないことを確認します。使用する場合は、クライアントの認証試行が失敗します。

LEAP 設定

LEAP（Lightweight EAP）はワイヤレス ネットワークに対応しています。拡張認証プロトコル（EAP）フレームワークに基づき、WEP よりセキュアなプロトコルを作成するためシスコにより開発されました。

（注） 強力なパスワードおよび定期的に失効するパスワードを使用しない限り、LEAP はディクショナリ攻撃を受ける場合があります。認証方式がディクショナリ攻撃の被害を受けにくい EAP-FAST、PEAP、または EAP-TLS を使用することをお勧めします。

ユーザ認証にのみ使用できる LEAP 設定：

- ログオフを越えたユーザ接続の延長：ユーザがログオフしても接続は開いたままです。同じユーザが再度ネットワークにログインしても、接続はアクティブのままです。

詳細については、「Dictionary Attack on Cisco LEAP Vulnerability」を参照してください。

ネットワーク クレデンシャルの定義

[ネットワーク（Networks）] > [クレデンシャル（Credentials）] ペインで、ユーザー クレデンシャルまたはマシン クレデンシャルのいずれを使用するか指定し、信頼サーバ検証ルールを設定します。

ユーザ クレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえ

ば、ピアでは最初に nouser@cisco.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@cisco.com のアイデンティティを要求する場合があります。そのため、ユーザーのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

ユーザ接続で、プレースホルダ [username] および [domain] を使用する場合、次の条件が当てはまります。

- 認証にクライアント証明書を使用する場合：さまざまな X509 証明書プロパティから [ユーザー名（username）] および [ドメイン（domain）] のプレースホルダ値を取得します。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@example.com（ユーザ名 =userA、ドメイン =example.com）、マシン認証のアイデンティティが hostA.example.com（ユーザ名 =hostA、ドメイン =example.com）の場合、次のプロパティが解析されます。
- ユーザー証明書ベースの認証の場合：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@eample.com
  - Subject = .../CN=userA/DC=example/DC=com/...
  - Subject = userA (no domain)
- マシン証明書ベースの認証の場合：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- クレデンシャルのソースがエンドユーザの場合：ユーザが入力する情報からプレースホルダ値を取得します。
- クレデンシャルがオペレーティング システムから取得される場合：ログイン情報からプレースホルダ値を取得します。
- クレデンシャルが静的である場合：プレースホルダを使用しません。

[クレデンシャル（Credentials）] ペインでは、目的のクレデンシャルを関連付けられたネットワークの認証で使用するために指定できます。

手順

ステップ 1 [保護されたアイデンティティ パターン（Protected Identity Pattern）] でユーザ アイデンティティを定義します。Network Access Managerでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [username]：ユーザー名を指定します。ユーザが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [raw]：ユーザーの入力のとおりにユーザー名を指定します。
- [domain]：ユーザ デバイスのドメインを指定します。

ステップ 2 一般的な、保護されていないアイデンティティ パターンを指定します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。

- anonymous@[domain]：値がクリア テキストで送信されるときに、ユーザ アイデンティティを隠すために、トンネリングされた方式内でよく使用されます。実際のユーザ アイデンティティは、保護されたアイデンティティとして、内部方式で提供されます。
- [username]@[domain]：トンネリングされていない方式の場合。

（注） 保護されていないアイデンティティ情報はクリア テキストで送信されます。最初のクリア テキスト アイデンティティ要求または応答が改ざんされた場合は、TLS セッションが確立されるとサーバがアイデンティティを検証できないことを検出することがあります。たとえば、ユーザ ID が無効であるか、または EAP サーバが処理する領域内にない場合があります。

ステップ 3 保護されるアイデンティティ パターンを指定します。

ユーザー ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。

- [username]@[domain]
- ユーザのアイデンティティとして使用する実際の文字列（プレースホルダなし）

ステップ 4 次のユーザ クレデンシャル情報をさらに提供します。

- [シングル サインオン クレデンシャルを使用（Use Single Sign On Credentials）]：クレデンシャルをオペレーティング システムのログイン情報から取得します。ログイン クレデンシャルが失敗すると、Network Access Managerは一時的に（次のログインまで）切り替わり、ユーザに GUI でクレデンシャルの入力を求めます。

（注） Network Access Manager および SSO で、Windows ログイン クレデンシャルを自動的に使用することはできません。Network Access Managerで SSO を使用するには、ログオン クレデンシャルを代行受信する必要があります。したがって、インストールまたはログオフの後に再起動を求められます。

- [スタティック クレデンシャルを使用（Use Static Credentials）]：ユーザ クレデンシャルをこのプロファイル エディタが提供するネットワーク プロファイルから取得します。スタティック クレデンシャルが失敗すると、Network Access Managerは、新しい設定がロードされるまでクレデンシャルを再度使用しません。

  （注） アンパサンドはこのフィールドで無効な文字です。

- [クレデンシャルのプロンプト（Prompt for Credentials）]：クレデンシャルを次に指定されたとおりに AnyConnect GUI を使用してエンドユーザーから取得します。
  - [永久に記憶（Remember Forever）]：クレデンシャルは永久に記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。クレデンシャルはファイルに保存され、ローカル マシン パスワードを使用して暗号化されます。
  - [ユーザのログイン中記憶（Remember while User is Logged On）]：クレデンシャルはユーザがログオフするまで記憶されます。記憶されたクレデンシャルが失敗すると、ユーザはクレデンシャルの入力を再度求められます。
  - [記憶しない（Never Remember）]：クレデンシャルは一切記憶されません。Network Access Managerは、認証のためにクレデンシャル情報が必要なたびに、ユーザに入力を求めます。

ステップ 5 証明書が要求されたときに、認証のためにいずれの証明書ソースを使用するかを決定します。

- [スマート カードまたは OS 証明書（Smart Card or OS certificates）]：Network Access Managerは、OS の証明書ストアまたはスマート カードで検出される証明書を使用します。
- [スマート カード証明書のみ（Smart Card certificates only）]：Network Access Managerは、スマート カードで検出される証明書のみを使用します。

ステップ 6 [スマート カード PIN を記憶（Remember Smart Card Pin）] パラメータでは、Network Access Managerがスマート カードから証明書を取得するために使用した PIN を記憶する期間を決定します。使用できるオプションについては、ステップ 2 を参照してください。

（注） PIN は、証明書自体よりも長く保存されることは決してありません。

別名 Cryptographic Service Provider（CSP）および Key Storage Provider（KSP）というスマートカードのチップとドライバによっては、他より接続に時間がかかるスマートカードもあります。接続タイムアウトを長くすると、ネットワークにスマートカードベースの認証を実行するのに十分な時間を与えることができます。

マシン クレデンシャルの設定

EAP カンバセーションには、複数の EAP 認証方式が含まれ、その各認証で要求されるアイデンティティが異なる場合があります（マシン認証の次にユーザ認証が行われるなど）。たとえば、ピアでは最初に nouser@example.com のアイデンティティを要求して認証要求を cisco.com EAP サーバにルーティングする場合があります。しかし、いったん TLS セッションがネゴシエートされると、そのピアは johndoe@example.com のアイデンティティを要求する場合があります。そのため、ユーザーのアイデンティティにより保護が提供される場合でも、カンバセーションがローカル認証サーバで終端しない限り、宛先領域は必ずしも一致しません。

マシン接続の場合に、[ユーザー名（username）] および [ドメイン（domain）] プレースホルダが使用されたときは、常に次の条件が適用されます。

- 認証にクライアント証明書を使用する場合：さまざまな X509 証明書プロパティから [ユーザー名（username）] および [ドメイン（domain）] のプレースホルダ値を取得します。プロパティは最初の一致に応じて次の順序で解析されます。たとえば、ユーザ認証のアイデンティティが userA@cisco.com（ユーザー名 =userA、ドメイン =cisco.com）、マシン認証のアイデンティティが hostA.cisco.com（ユーザー名 =hostA、ドメイン =cisco.com）の場合、次のプロパティが解析されます。
- ユーザー証明書ベースの認証の場合：
  - SubjectAlternativeName: UPN = userA@example.com
  - Subject = .../CN=userA@example.com/...
  - Subject = userA@example.com
  - Subject = .../CN=userA/DC=example.com/...
  - Subject = userA (no domain)
- マシン証明書ベースの認証の場合：
  - SubjectAlternativeName: DNS = hostA.example.com
  - Subject = .../DC=hostA.example.com/...
  - Subject = .../CN=hostA.example.com/...
  - Subject = hostA.example.com
- クライアント証明書が認証に使用されない場合：クレデンシャルをオペレーティング システムから取得し、[ユーザー名（username）] プレースホルダは割り当てられたマシン名を表します。

[クレデンシャル（Credentials）] パネルでは、目的のマシン クレデンシャルを指定できます。

手順

ステップ 1 [保護されているアイデンティティ パターン（Protected Identity Pattern）] でマシン アイデンティティを定義します。Network Access Managerでは、次のアイデンティティ プレースホルダのパターンがサポートされます。

- [username]：ユーザー名を指定します。ユーザーが username@domain または domain\username を入力した場合、ドメインの部分は削除されます。
- [raw]：ユーザーの入力のとおりにユーザー名を指定します。
- [domain]：ユーザーの PC のドメインを指定します。

ステップ 2 典型的な保護されていないマシン アイデンティティのパターンを定義します。

まだネゴシエートされていないセッションでは、整合性保護または認証なしで、暗号化されていないアイデンティティ要求および応答が発生します。これらのセッションは、スヌーピングおよびパケット変更の対象になります。

- host/anonymous@[domain]
- マシンのアイデンティティとして送信する実際の文字列（プレースホルダなし）

ステップ 3 保護されているマシン アイデンティティのパターンを定義します。

ユーザー ID をスヌーピングから保護するために、クリア テキスト アイデンティティは、認証要求の正しい領域へのルーティングを有効にするために必要な情報のみを指定する場合があります。典型的な保護されているマシン アイデンティティのパターンは次のとおりです。

- host/[username]@[domain]
- マシンのアイデンティティとして使用する実際の文字列（プレースホルダなし）

ステップ 4 次のマシン クレデンシャル情報をさらに提供します。

- [マシン クレデンシャルを使用（Use Machine Credentials）]：クレデンシャルをオペレーティング システムから取得します。
- [スタティック クレデンシャルを使用（Use Static Credentials）]：展開ファイルに送信する実際のスタティック パスワードを指定します。スタティック クレデンシャルは、証明書ベースの認証には適用されません。

適切な証明書を選択するための *Network Access Manager* の設定

クライアント認証時に 2 つの証明書が存在する場合、Network Access Managerは証明書の属性に基づいて最適な証明書を自動的に選択します。優先する証明書の条件は顧客によって異なるため、次に示す証明書の選択を定義するフィールドを設定し、また証明書選択をオーバーライドするルールを指定する必要があります。

複数の証明書が同一ルールに一致するか、ルールに一致する証明書がない場合は、ACEエンジンが、証明書の優先順位を指定するアルゴリズムを実行し、特定の基準（秘密キーがあるかどうか、マシン ストアからの証明書であるかどうかなど）に基づいて証明書を選択します。複数の証明書の優先順位が同一の場合、ACEエンジンはその優先順位で最初に検出した証明書を選択します。

手順

ステップ 1 AnyConnect プロファイルエディタから [ネットワーク（Networks）] タブを選択します。

ステップ 2 編集するネットワークを選択します。

ステップ 3 [マシンクレデンシャル（Machine Credentials）] タブを選択します。

ステップ 4 ページ下部で [証明書一致ルールを使用する（Use Certificate Matching Rule）] を選択します。

ステップ 5 [証明書フィールド（Certificate Field）] ドロップダウン メニューから、検索条件として使用するフィールドを選択します。

ステップ 6 [一致（Match）] ドロップダウン メニューから、検索にフィールドの完全一致（[等しい（Equals）]）または部分一致（[含む（Includes）]）を含めるかどうかを指定します。

ステップ 7 [値（Value）] フィールドに、証明書の検索条件を入力します。

信頼サーバ検証ルールの設定

[サーバ ID の検証（Validate Server Identity）] オプションが [EAP] 方式に設定されている場合、[証明書（Certificate）] パネルが有効になって証明書サーバまたは認証局に対する検証ルールを設定できます。検証の結果によって、証明書サーバまたは認証局が信頼されるかどうかが決定されます。

証明書サーバの検証ルールを定義するには、次の手順を実行します。

手順

ステップ 1 オプション設定が [証明書フィールド（Certificate Field）] および [一致（Match）] カラムに表示されたときに、ドロップダウン矢印をクリックし、目的の設定を選択します。

ステップ 2 [値（Value）] フィールドに、値を入力します。

ステップ 3 ルールの下で [追加（Add）] をクリックします。

ステップ 4 [証明書信頼済み認証局（Certificate Trusted Authority）] ペインで、次のいずれかのオプションを選択します。

- [OS にインストールされたすべてのルート認証局（CA）を信頼（Trust any Root Certificate Authority (CA) Installed on the OS）]：選択すると、ローカル マシンまたは証明書ストアのみがサーバの証明書チェーン検証の対象になります。
- [ルート認証局（CA）証明書を含める（Include Root Certificate Authority (CA) Certificates）]。

（注） [ルート認証局（CA）証明書を含める（Include Root Certificate Authority (CA) Certificates）] を選択した場合は、[追加（Add）] をクリックして CA 証明書を設定にインポートする必要があります。使用している証明書が Windows 証明書ストアからエクスポートされる場合は、[Base 64 encoded X.509 (.cer)] オプションを使用します。

ネットワーク グループ ウィンドウ

[ネットワーク グループ（Network Groups）] ウィンドウで、ネットワーク接続を特定のグループに割り当てます。接続をグループに分類することにより、次の複数の利点がもたらされます。

- 接続の確立試行時のユーザエクスペリエンスの向上。複数の非表示ネットワークが設定された場合、接続が正常に確立するまで、クライアントは非表示ネットワークのリストを定義された順序で順を追って調べます。このような場合に、接続を確立するために必要な時間を大幅に短縮するためにグループが使用されます。
- 設定された接続の管理の簡略化。企業内で複数の役割を持つ（または同じ領域に頻繁にアクセスする）ユーザがグループ内のネットワークを調整して選択可能なネットワークのリストを管理しやすくする場合に、管理者ネットワークをユーザ ネットワークから分離できます。

配布パッケージの一部として定義されたネットワークはロックされています。これは、ユーザが設定を編集することや、ネットワーク プロファイルを削除することを防止するためです。

ネットワークをグローバルとして定義できます。グローバルとして定義すると、ネットワークは [グローバル ネットワーク（Global Networks）] セクションに表示されます。このセクションは、有線とワイヤレス ネットワーク タイプの間で分割されます。このタイプのネットワークに対しては、ソート順序の編集のみを実行できます。

すべての非グローバル ネットワークは、グループ内に存在する必要があります。1 つのグループがデフォルトで作成されています。すべてのネットワークがグローバルの場合にそのグループを削除できます。

手順

ステップ 1 ドロップダウン リストからグループを選択します。

ステップ 2 [ネットワークの作成（Create networks）] を選択して、エンド ユーザがこのグループ内にネットワークを作成できるようにします。これをオフにした場合、展開されたときにNetwork Access Managerはこのグループからユーザ作成ネットワークをすべて削除します。これにより、ユーザがネットワーク設定を別のグループに再入力する必要が生じることがあります。

ステップ 3 [スキャンリストの表示（See scan list）] を選択して、AnyConnect GUI を使用してグループがアクティブグループとして選択されたときに、エンドユーザーがスキャンリストを表示できるよ

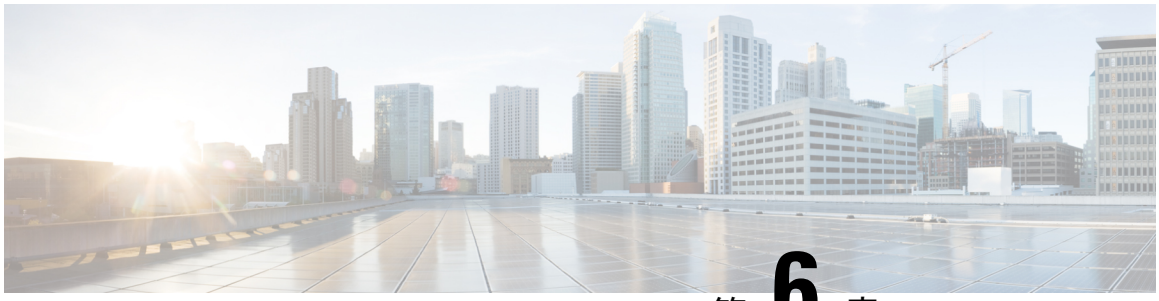
うにします。または、このチェックボックスをオフにして、ユーザによるスキャン リストの表示を制限します。たとえば、ユーザが近くのデバイスに誤って接続することを防ぐ必要がある場合に、スキャン リストへのアクセスを制限します。

（注） これらの設定は、グループごとに適用されます。

ステップ 4 右矢印および左矢印を使用して、[グループ（Group）] ドロップダウン リストから選択したグループに対してネットワークを挿入または削除します。ネットワークが現在のグループから移動された場合は、デフォルト グループに配置されます。デフォルト グループを編集する場合、デフォルト グループからネットワークを移動できません（[>] ボタンを使用）。

（注） 指定のネットワーク内で、各ネットワークの表示名は一意である必要があります。このため、1 つのグループには同じ表示名を持つ 2 つ以上のネットワークを含められません。

ステップ 5 上矢印および下矢印を使用してグループ内のネットワークの優先順位を変更します。



第 6 章

ポスチャの設定

AnyConnect セキュア モビリティ クライアント は VPN ポスチャ/HostScan モジュールおよび ISE ポスチャモジュールを提供します。両方のモジュールにより、AnyConnect で、ホストにインストールされたウイルス対策、スパイウェア対策、ファイアウォール ソフトウェアなどについてエンドポイントのコンプライアンスを評価できます。その後、エンドポイントがコンプライアンスに対応するまでネットワーク アクセスを制限したり、修復方法を確立できるようにローカル ユーザの権限を強化したりできます。

VPN ポスチャ は、hostscan_version.pkg にバインドされています。これは、どのようなオペレーティングシステム、ウイルス対策、スパイウェア対策、およびソフトウェアがホストにインストールされているかを収集するアプリケーションです。ISE ポスチャは、ISE 制御ネットワークにアクセスするときに、AnyConnect と NAC Agent の両方を展開するのではなく、1 つのクライアントを展開します。ISE ポスチャは、AnyConnect 製品に追加のセキュリティコンポーネントとしてインストールできるモジュールです。

ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。エンドポイントがコンプライアンス対応かどうかを実際には ISE が判断する場合でも、ISE はエンドポイント独自のポリシー評価を利用します。

一方、HostScan はサーバ側評価を実行します。Cisco Secure Firewall ASA がエンドポイント属性（オペレーティング システム、IP アドレス、レジストリエントリ、ローカル証明書、ファイル名など）のリストのみを要求し、これらが HostScan によって返されます。ポリシーの評価結果に基づいて、どのホストがセキュリティ アプライアンスへのリモート アクセス接続を確立できるかを制御できます。

（注） HostScan と ISE のポスチャエージェントの併用はサポートされていません。2 つの異なるポスチャエージェントを実行すると、予期しない結果が発生します。

次のポスチャチェックは、HostScan ではサポートされていますが、ISE ポスチャではサポートされていません。ホスト名、IP アドレス、MAC アドレス、ポート番号、OPSWAT バージョン、BIOS シリアル番号、および証明書フィールド属性です。

• ISE ポスチャ モジュールの提供内容 （246 ページ）

ISE ポスチャ モジュールの提供内容

ポスチャ チェック

ISE ポスチャ モジュールはポスチャ チェックの実行に OPSWAT v3 または v4 ライブラリを使用します。初回のポスチャ チェックでは、すべての必須要件への一致に失敗したエンドポイントがすべて非準拠と見なされます。その他のエンドポイントの許可ステータスは、ポスチャ不明または準拠（必須要件に合致）です。

（注） macOS 64 ビットの移行では、AnyConnect ISE ポスチャモジュールは古い OPSWAT v3 準拠モジュールと互換性がありません。

ポスチャチェックフェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザーに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャ チェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワーク アクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザーはポスチャ プロセスをリスタートできます。

必要な修復

修復ウィンドウはバックグラウンドで実行されるため、ネットワーク アクティビティのアップデートはポップアップ表示されず、干渉や中断は発生しません。AnyConnect UI の ISE ポスチャ タイル部分で [詳細（Details）] をクリックして、検出された内容およびネットワークに参加する前に必要なアップデート内容を確認できます。必須の手動修復が存在する場合、修復ウィンドウが開き、対処が必要な項目が表示されます。このシステムスキャンのウィンドウに、アップデートの進捗状況、割り当てられたアップデート時間の残り時間、すべての要件のステータス、およびシステムの準拠状態が表示されます。

（注） 昇格された権限を必要とするアプリケーションは、管理者以外のユーザアカウントでのみ自動修復を使用します。管理者アカウントでは、修復を手動で実行する必要があります。

（注） 昇格権限を必要とするポスチャ チェックおよび修復は、サーバが信頼されている場合にのみ実行されます。

オプションのアップデートのみが残っている場合、[スキップ（Skip）] を選択して次の更新に進むことも、[すべてスキップ（Skip All）] を選択して残りの修復をすべて無視することも可能です。時間を節約するためにオプションの修復をスキップしても、ネットワーク アクセスは維持されます。

修復後（または修復が必要でない場合は要件チェック後）、アクセプタブル ユース ポリシーの通知を受け取る場合があります。この場合、ネットワーク アクセスのポリシーに同意する必要があり、同意しなかった場合はアクセスが制限されます。修復のこの部分では、AnyConnect UI のポスチャ タイル部分に、「システムスキャン：ネットワークのアクセプタブル ユース ポリシー（System Scan: Network Acceptable Use Policy）」と表示されます。

修復が完了すると、必須アップデートとしてリストされたチェック項目がすべて[完了（Done）] ステータスとなり、緑色のチェックボックスが表示されます。修復後、エージェントはISE にポスチャ結果を送信します。

パッチ管理チェックと修復

AnyConnect および Microsoft System Center Configuration Manager（SCCM）の統合により、パッチ管理チェックとパッチ管理修復が導入されました。エンドポイントで欠落している重要なパッチのステータスをチェックし、ソフトウェア パッチをトリガーするべきかどうか確認します。重要なパッチが Windows エンドポイントで欠落していない場合は、パッチ管理チェックは合格です。パッチ管理修復は、管理者レベルのユーザのみに対して、1 つ以上の重要なパッチが Windows エンドポイントで欠落しているときにのみトリガーされます。

SCCM クライアントで、再起動前にインストールが行われるパッチをインストールすると、マシンが再起動するとすぐに、パッチのインストール ステータス（インストール完了または未インストール）がレポートされます。ただし、SCCM クライアントで、再起動後にインストールが開始されるパッチをインストールすると、パッチのステータスはすぐにはレポートされません。

AnyConnect コンプライアンスモジュールは、この時点で SCCM クライアントにステータスの提供を強制できません。ポスチャ モジュール クライアントがネイティブ API 要求を完了するためにかかる時間は、さまざまな動的 OS パラメータ（CPU 負荷、保留中のパッチの量、パッチ インストール後の再起動なしなど）と、ネットワークの要因（ポスチャ モジュール クライアントとサーバ間の接続と遅延）に依存します。SCCM クライアントが応答するまで待機する必要があるかもしれませんが、既知のパッチによる一部のテスト結果は約 10 分でした。

同様の動作は、Windows Server Update Services（WSUS）の検索 API でも見られ、応答時間は長めで、20 ～ 30 分かかることもあります。Windows アップデートは、Windows OS だけでなく、すべてのマイクロソフト製品（Microsoft Office など）についてパッチの不足がないかチェックします。

ISE のポリシー状態の設定方法については「Policy Conditions」を参照してください。またパッチ管理修復の詳細については「Patch Management Remediation」を参照してください。

エンドポイント コンプライアンスの再評価

エンドポイントがコンプライアンス対応と見なされ、ネットワーク アクセスが許可されると、管理者が設定した制御に基づいてエンドポイントを任意で定期的に再評価できます。パッシブ再評価ポスチャ チェックは、初期のポスチャ チェックとは異なります。失敗した場合、ユーザには修復するオプションが与えられます（管理者がそのように設定していた場合）。この構成設定では、1 つ以上の必須要件が満たされていない場合でも、ユーザが信頼ネットワーク アクセスを維持するかどうかを制御します。初期のポスチャ評価では、すべての必須要件が満たされていないと、エンドポイントはコンプライアンス非対応と見なされます。この機能はデフォルトでは無効であり、ユーザ ロールに対して有効になっている場合、ポスチャは 1 ～ 24 時間ごとに再評価されます。

管理者は、結果を [続行（Continue）]、[ログオフ（Logoff）]、または [修復（Remediate）] に設定し、適用や猶予時間など他のオプションを設定できます。

ISE の UI を使用すると、VPN ポスチャ プロファイルに表示される情報メッセージを作成できます。ボタンのテキストとリンクは、カスタマイズも可能です。

非準拠デバイスの猶予期間

Cisco ISE の UI で猶予期間を設定することができます。これを設定すると、以前のポスチャ ステータスでは準拠していたが準拠しなくなったエンドポイントに、ネットワークへのアクセスを許可できるようになります。Cisco ISE は、以前に認識された良好な状態をキャッシュ内で探し、デバイスに猶予時間を提供します。猶予期間が終了すると、AnyConnect は再度ポスチャ チェックを行いますが、今回は修復を行いません。チェックの結果に基づいてエンドポイントの状態を準拠または非準拠と判断します。

（注） デバイスが猶予期間にあるがポスチャ ポリシーで更新されると、次のようになります。

- （猶予期間が延長された場合）、以前の猶予期間が経過するか、またはデバイスが Cisco ISE から削除されたときに、新しい猶予期間が適用されます。
- （猶予期間が短縮された場合）、デバイスが再びポスチャ フロー プロセスを通過した場合にのみ、新しい猶予期間がデバイスに適用されます。

猶予期間は、一時的なエージェント、ハードウェアのインベントリ、アプリケーションのモニタリングには適用されません。

ユーザが猶予期間にいる場合は、定期的な再評価（PRA）は適用されません。

（それぞれ異なる猶予期間を設定した）複数のポスチャ ポリシーにデバイスが一致する場合、それらの異なるポリシーで設定された最大の猶予期間がデバイスに与えられます。

デバイスが猶予期間に移行すると、アクセプタブル ユース ポリシー（AUP）は表示されません。

猶予期間は、ISE UI で **[ポリシー（Policy）] > [ポスチャ（Posture）] または [ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャポリシー（Posture Policy）]** の順に移動して、VPN ポスチャ プロファイルに設定します。有効な値は、日、時間、または分単位で指定します。デフォルトでは、この設定は無効です。

柔軟な通知

猶予期間の特定の割合が経過するまでカスタム通知ウィンドウの表示を遅らせるには、遅延通知のオプションを使用します。たとえば、ISE UI の [遅延の通知（Delay Notification）] フィールドが 50 % に設定され、設定されている猶予期間が 10 分の場合、ISE ポスチャは 5 分後にエンドポイントを再スキャンし、エンドポイントに違反があると検出した場合は通知ウィンドウを表示します。エンドポイントのステータスが準拠している場合、通知ウィンドウは表示されません。通知遅延期間が 0 % に設定されている場合は、猶予期間の開始時に直ちに問題の解決を促すメッセージが表示されます。エンドポイントは、猶予期間の有効期限が切れるまで、アクセスが許可されます。

カスタム通知が ISE UI で設定されている場合にのみ、エンドポイントが準拠していないと AnyConnect UI に警告が表示されます。通知は、猶予期間の開始および猶予期間の開始後に準拠していないエンドポイントに対しても示されます。AnyConnect システムスキャン タイルにはすべてのポスチャ障害が強調表示され、**[再度スキャン（Scan Again）]** ボタンを押すと、ポスチャポリシーの再実行を強制して完全なネットワークアクセスを維持できます。

（注） [再度スキャン（Scan Again）] オプションが表示されるようにするには、[再スキャンボタンを有効にする（Enable Rescan Button）] オプションを [有効（Enabled）] に設定する必要があります。

修復フローでは、問題を解決するまで基本的にアクセスがブロックされます。一時的なアクセスは、使用可能ではありません。猶予期間フローでは、遅延アクセスの取得により、問題を解決するための猶予期間が提供されます。柔軟な通知フローの[**ブラウザを起動**（Launch Browser）]オプションをクリックすると、サーバーが信頼できる場合は、ブラウザを起動することができます。ブラウザ オプションでは、ポスチャ ポリシーへの準拠に関する詳細を取得できます。

シスコ テンポラル エージェント

シスコ テンポラル エージェントは、ユーザーが信頼ネットワークにアクセスしているときにコンプライアンス ステータスを共有できるように、Windows または macOS 環境向けに設計されています。シスコ テンポラル エージェントの設定は、ISE UI で行います。シスコ テンポラル エージェントの実行ファイル .exe（Windows 用）または dmg（macOS 用）は、エンドポイントがインターネットへのアクセスを試行するたび、エンドポイントにダウンロードされます。ユーザは、ダウンロードした実行ファイルまたはdmgを実行し、コンプライアンス チェックを行う必要があります。これには、管理者権限は不要です。

UI が自動的に起動し、エンドポイントのコンプライアンスに問題がないか判断するチェックを開始します。コンプライアンス チェックが完了すると、ISE は、ISE UI でのポリシーの設定方法に基づいて必要なアクションを取れるようになります。

Windows では、実行ファイルは自己解凍されます。この解凍により、コンプライアンス チェックに必要なすべての dll およびその他のファイルが一時フォルダに保存されます。解凍されたファイルおよび実行ファイルは、コンプライアンス チェックの完了後、削除されます。ファイルおよび実行ファイルを完全に削除するには、ユーザーが UI を終了する必要があります。

ISE UI での詳細な設定手順については、『Cisco Identity Services Engine Administrator Guide』の「Cisco Temporal Agent Workflows」を参照してください。

シスコ テンポラル エージェントの制限事項

- macOS では、VLAN 制御のポスチャ環境は、ルート権限がないと更新アダプタ（DHCP 更新）プロセスが実行されないため、テンポラルエージェントについてはサポートされていません。テンポラル エージェントはユーザー プロセスとしてのみ実行できます。ACL 制御のポスチャ環境は、エンドポイントの IP を更新する必要がないため、サポートされています。
- 修復中にネットワーク インターフェイスが発生した場合、ユーザーは、現在の UI を終了して手順全体をやり直す必要があります。
- macOS では、dmg ファイルは削除されません。
- テンポラル エージェント インストーラは、起動後、エンドポイントでの実行中にブラウザの背後に隠れてしまうことがあります。テンポラル エージェント アプリケーションでのヘルス情報の収集を続行するには、エンドユーザーは、ブラウザを最小化する必要があります。この問題は、主に Windows 10 ユーザーで発生します。理由は、これらのクライアントでは、高いセキュリティ条件で実行されるサードパーティ アプリケーションを許容するため、UAC モードが「高」に設定されていることです。

- エンドポイントでステルス モードが有効になっている場合は、テンポラル エージェントを使用できません。
- 次の状態は、シスコ テンポラル エージェントではサポートされていません。
  - サービス状態（macOS）：システム デーモンのチェック
  - サービス状態（macOS）：デーモンまたはユーザー エージェントのチェック
  - PM：最新バージョンのチェック
  - PM：有効化チェック
  - DE：暗号化の場所に基づくチェック

オプション モードのポスチャ ポリシー拡張機能

必須の要件チェックの成否に関係なく、オプションモードで失敗した要件チェックの修復を実行できます。修復に関するメッセージは、AnyConnect ISE ポスチャ UI に表示され、失敗の内容と必要な修復アクションを確認することが可能です。

- オプションモードの手動修復：[システムスキャンのサマリー（System Scan Summary）] 画面には、条件が満たされない場合に修復が必要な可能性がある、オプションモードのステータスが表示されます。[開始（Start）] を手動でクリックして修復するか、[スキップ（Skip）] をクリックします。これらはオプションの要件にすぎないため、修復が失敗しても、エンドポイントはコンプライアンス対応です。[システムスキャンのサマリー（System Scan Summary）] に、スキップされたのか、失敗したのか、成功したのかが表示されます。
- オプション モードの自動修復：オプションのアップデートの適用時、[システムスキャン（System Scan）] タイルの表示内容を監視できます。修復は自動的に実行されるため、修復を開始するか確認されません。いずれかの自動修復が失敗すると、修復を試行できなかったというメッセージが表示されます。さらに、必要に応じて、修復アクションをスキップできます。

ハードウェア インベントリの可視性

ISE UI の [コンテキストの可視性（Context Visibility）] の下に、[エンドポイント（Endpoints）] > [ハードウェア（Hardware）] タブが追加されました。これは、エンドポイント ハードウェアの情報を短時間で収集、分析、および報告するのに役立ちます。メモリ容量が小さいエンドポイントの検出や、エンドポイントのBIOSモデル/バージョンの検出など、情報を収集することができます。検出結果に基づいて、メモリ容量を増やしたり、BIOS のバージョンをアップグレードしたり、資産の購入を計画する前に要件を評価したりすることができます。[メーカー使用状況（Manufacturers Utilization）] ダッシュレットには、Windows または macOS のエンドポイントのハードウェア インベントリの詳細が表示されます。[エンドポイント使用状況（Endpoint Utilizations）] ダッシュレットには、エンドポイントの CPU、メモリ、およびディスクの使用状況が表示されます。詳細については、『Cisco Identity Services Engine Administrator Guide』の「The Hardware Tab」を参照してください。

ステルス モード

管理者は、AnyConnect UI タイルをエンドユーザークライアントに対して非表示にしている間に、ISE ポスチャを設定できます。ポップアップは表示されないので、ユーザーによる設定を必要とするどのシナリオでも、デフォルトのアクションが実行されます。この機能は、Windows および macOS オペレーティングシステムで使用できます。

『Cisco Identity Services Engine Administrator Guide』の「*Configure Posture Policies*」の項を参照してください。ここでは、クライアントレス状態を無効または有効にしてステルス モードを設定します。

ISE UI では、エンド ユーザーにエラー通知が表示されるようにステルス モードで通知を有効にするよう設定できます。

ISE ポスチャ プロファイル エディタ（260 ページ）でプロファイルをマッピングし、AnyConnect 設定を ISE の [クライアント プロビジョニング（Client Provisioning）] ページにマッピングすると、AnyConnect は、ポスチャプロファイルを読み込んで目的のモードに設定し、最初のポスチャ要求中に選択されたモードに関する情報を ISE に送信できます。モードと、ID グループ、OS、コンプライアンス モジュールなどのその他の要因に基づいて、Cisco ISE は適切なポリシーをマッチングします。

『Cisco Identity Services Engine Administrator Guide』でステルス モードの展開とその影響について参照してください。

ISE ポスチャでは、ステルス モードで次の機能を設定することはできません。

- すべての手動修復
- リンク修復
- ファイル修復
- WSUS 表示 UI 修復
- アクティブ化 GUI 修復
- AUP ポリシー

ポスチャ ポリシーの適用

エンドポイントにインストールされているソフトウェアの全体的な可視性を改善するために、シスコは次のポスチャ拡張機能を提供しました。

- エンドポイントのファイアウォール製品の状態をチェックして、その製品が実行されているかどうか確認できます。必要に応じて、ファイアウォールを有効にし、最初のポスチャ中や定期的な再評価（PRA）中にポリシーを適用できます。設定するには、『Cisco Identity Services Engine Configuration Guide』の「*Firewall Condition Settings*」の項を参照してください。
- 同様に、エンドポイントにインストールされているアプリケーションのクエリを実行できます。不要なアプリケーションが実行中またはインストールされている場合は、アプリ

ケーションを停止するか、不要なアプリケーションをアンインストールできます。設定するには、ISE UI で、『Cisco Identity Services Engine Configuration Guide』の「*Application Remediation*」の項を参照してください。

UDID 統合

AnyConnect は、デバイスにインストールされていると、AnyConnect のすべてのモジュール間で共有される独自の一意の ID（UDID）を持ちます。この UDID は、エンドポイントの ID であり、エンドポイント属性として保存されるため、MAC アドレスではなく特定のエンドポイントでのポスチャ制御が保証されます。その後は、UDID に基づいてエンドポイントをクエリすることができます。UDID は定数で、エンドポイントの状況（接続、アップグレード、アンインストールなど）に関係なく変化しません。ISE UI の [コンテキスト表示（Context Visibility）] ページ（**[コンテキスト表示（Context Visibility）] > [エンドポイント（Endpoints）] > [コンプライアンス（Compliance）]**）は、複数の NIC を持つエンドポイントについて、複数のエントリではなく 1 つのエントリを表示できます。

アプリケーション監視

ポスチャ クライアントは、動的な変化を監視し、ポリシー サーバに報告できるように、さまざまなエンドポイント属性を継続的に監視できます。ポスチャポリシーの設定に応じて、インストールされるアプリケーションや、アプリケーションが実行するスパイウェア対策、ウイルス対策、アンチマルウェア、ファイアウォールなどのさまざまな属性を監視できます。アプリケーションの条件設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「*Continuous Endpoint Attribute Monitoring*」の項を参照してください。

USB ストレージ デバイス検出

USB 大容量ストレージ デバイスを Windows エンド ポイントに接続すると、ポスチャ クライアントはそのデバイスを検出し、ポスチャ ポリシー ブロックに応じて、デバイスをブロックしたり許可したりすることができます。エージェントは USB 検出を使用して、同じ ISE 制御ネットワークにある限り、継続的にエンドポイントをモニタします。この期間内に、条件に一致する USB デバイスを接続した場合、指定した修復アクションが実行されます。インシデントは、ポリシー サーバにも報告されます。

USB ストレージ検出は、OPSWAT v4 コンプライアンス モジュールに依存しています。[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポリシー要素（Policy Elements）] > [USB] で、ISE UI の定期再評価ポリシー（PRA）の USB チェックを設定する必要があります。

（注） チェックと修復は順番に実行されるため、その他のチェックの PRA 猶予時間を最小限の値に設定することによって、USB チェックの処理での遅延を防止できます。猶予時間は、[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [再評価設定（Reassessment Config）] の ISE UI で設定されます。

ISE UI で USB ストレージの検出を設定する手順については、「USB Mass Storage Check Workflow」を参照してください。

自動コンプライアンス

ポスチャ リースにより、ISE サーバは、ポスチャを完全にスキップし、簡単にシステムを準拠状態にすることができます。この機能により、ユーザは、自分のシステムが最近ポスチャされている場合に、ネットワーク間の切り替えによる遅延を感じることがありません。ISE ポスチャ エージェントは、単に、ISE サーバが検出されたすぐ後に、システムが準拠しているかどうかを示すステータス メッセージを UI に送信します。ISE の UI（[設定（Settings）] > [ポスチャ（Posture）] > [一般設定（General Settings）]）で、最初のコンプライアンス チェックの後にエンドポイントがポスチャ準拠と見なされる時間を指定できます。ユーザがある通信インターフェイスから別の通信インターフェイスに切り替えた場合でも、コンプライアンス ステータスは維持されることが予期されています。

（注） ポスチャ リースでは、ISE でセッションが有効な場合に、エンドポイントがポスチャ不明状態から準拠状態に移行することが予期されます。

VLAN のモニタリングと遷移

サイトによっては、異なる VLAN またはサブネットを使用して、企業グループおよびアクセス レベル用にネットワークを分割しています。ISE からの認可変更（CoA）では、VLAN の変更を指定します。変更は、セッション終了など管理者のアクションによって発生することもあります。有線接続中の VLAN 変更をサポートするには、ISE ポスチャ プロファイルに次の設定を行います。

- [VLAN 検出間隔（VLAN Detection Interval）]：エージェントが VLAN の遷移を検出する頻度およびモニタリングを無効にするかどうかを決定します。VLAN モニタリングは、この間隔が 0 以外の値に設定されている場合に有効になります。macOS の場合は、この値を 5 以上に設定します。

  VLAN モニタリングは Windows と macOS の両方に実装されていますが、macOS では予期しない VLAN 変更を検出するためにのみ必要です。VPN が接続される場合、または acise（メインの AnyConnect ISE プロセス）が実行されていない場合は、自動的に無効になります。有効な値の範囲は 0 ～ 900 秒です。

- [エージェント IP 更新の有効化（Enable Agent IP Refresh）]：オフにすると、ISE はエージェントに [ネットワーク遷移遅延（Network Transition Delay）] 値を送信します。オンにすると、ISE はエージェントに DHCP リリースおよび更新の値を送信し、エージェントは IP 更新を行って最新の IP アドレスを取得します。

- [DHCP リリース遅延（DHCP release delay）] と [DHCP 更新遅延（DHCP renew delay）]：IP 更新および [エージェント IP 更新の有効化（Enable Agent IP Refresh）] 設定との相関で使用されます。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボック

スをオンにし、この値が 0 でない場合、エージェントはリリース遅延秒数を待機し、IP アドレスを更新し、更新遅延秒数を待機します。VPN が接続されている場合、IP 更新は自動的に無効になります。4 連続でプローブがドロップされると、DHCP 更新がトリガーされます。

- [ネットワーク遷移遅延（Network Transition Delay）]：（[エージェント IP 更新の有効化（Enable Agent IP Refresh）] チェックボックスで）VLAN モニタリングがエージェントによって無効または有効にされた場合に使用されます。この遅延により、VLAN が使用されていない場合にはバッファが追加され、サーバからの正確なステータスを待機する十分な時間がエージェントに与えられます。ISE はエージェントにこの値を送信します。また、ISE UI のグローバル設定に [ネットワーク遷移遅延（Network Transition Delay）] 値を設定した場合、ISE ポスチャ プロファイル エディタの値でその値が上書きされます。

（注） Cisco Secure Firewall ASA は VLAN 変更をサポートしないため、クライアントが Cisco Secure Firewall ASA を介して ISE に接続されているときには、これらの設定は適用されません。

トラブルシューティング

ポスチャの完了後にエンドポイントデバイスがネットワークにアクセスできない場合は、次の点を確認してください。

- VLAN 変更は ISE UI で設定されていますか。
  - 設定されている場合、DHCP リリース遅延および更新遅延がプロファイルに設定されていますか。
  - どちらの設定も 0 の場合、[ネットワーク遷移遅延（Network Transition Delay）] がプロファイルに設定されていますか。

AnyConnect ISE フローを中断する操作

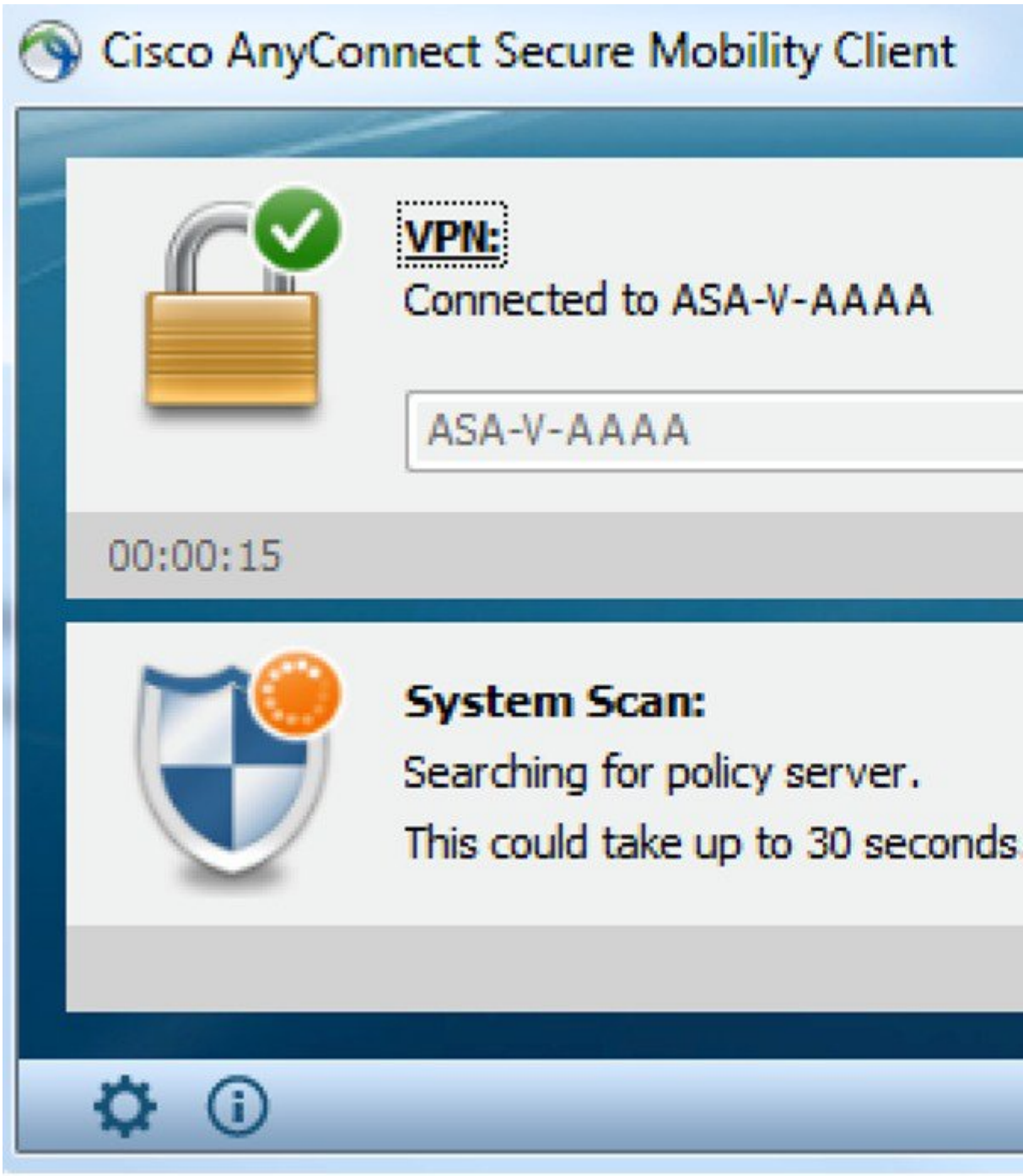
さまざまな理由から、AnyConnect ISE ポスチャフローは最初のポスチャ再アセスメントまたはパッシブ再アセスメント中に中断されることがあります。

- ユーザーが AnyConnect ISE をキャンセルする：ポスチャのチェックと修復の期間に、ユーザーは AnyConnect ISE をキャンセルできます。UI にはキャンセルが進行中であることがただちに通知されますが、これはエンドポイントを問題のある状態にすることを回避するときにだけ発生します。サードパーティ ソフトウェアを使用している場合、キャンセル操作によってはリブートが必要な場合があります。キャンセル後、AnyConnect UI の ISE ポスチャタイル部分には、準拠状態が示されます。
- 修復タイマーが期限切れになる：ポスチャ要件を満たすための管理者制御時間が終了しました。アセスメント レポートがヘッドエンドに送信されます。パッシブ再アセスメント時には、ユーザーはネットワーク アクセスを保持し、ポスチャ アセスメントでは、必須要件すべてが満たされた場合にネットワーク アクセスが許可されます。

- ポスチャチェック中のエラー：ポスチャチェックフェーズでエラーが発生し、AnyConnect が続行可能な場合、ユーザーに通知されますが、可能な場合はポスチャのチェックが続行されます。必須のポスチャチェック中にエラーが発生した場合、チェックは失敗とマークされます。ネットワークアクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザーはポスチャ プロセスをリスタートできます。
- 修復中のエラー：修復フェーズでエラーが発生し、AnyConnect ISE ポスチャが続行可能な場合は、ユーザーに通知されます。失敗した修復ステップが必須のポスチャ要件と関連付けられている場合、AnyConnect ISE ポスチャは修復プロセスを停止します。失敗した修正ステップがオプションのポスチャの要件に関連付けられている場合は、次のステップに進んで ISE ポスチャ操作を終了しようとします。ネットワークアクセスは、すべての必須要件が満たされている場合に許可されます。そうでない場合、ユーザーはポスチャプロセスをリスタートできます。
- デフォルトゲートウェイの変更：デフォルトゲートウェイに対する変更により、ユーザーが信頼ネットワークへのアクセスを失う場合があります。これにより、ISE ポスチャは ISE の再検出を試みます。AnyConnect UI の ISE ポスチャタイル部分では、再検出モードに入ると ISE ポスチャのステータスが表示されます。
- AnyConnect と ISE 間の接続の喪失：エンドポイントが準拠状態と見なされてネットワークアクセスが許可された後に、さまざまなネットワークシナリオが発生する可能性があります。エンドポイントがネットワーク接続を完全に失う場合があります。ISE がダウンする場合があります。ISE ポスチャが失敗する場合があります（セッションタイムアウト、手動リスタートなどによる）。Cisco Secure Firewall ASA の背後の ISE が VPN トンネルを喪失する場合があります。
- ISE ポスチャを使用している場合、1 つの macOS エンドポイントに複数のコンソールユーザーをログインさせることはできません。
- 初期化およびポスチャアセスメントフローの遅延（macOS のみ）：コンプライアンス モジュール ライブラリの署名検証で障害が発生しないように、ポスチャ前フェーズでサブネットを許可することをお勧めします。

ISE ポスチャのステータス

AnyConnect ISE ポスチャが機能し、想定どおりにネットワーク アクセスをブロックしている場合に、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに [システムスキャン：ポリシーサーバーを検索しています（System Scan: Searching for policy server）] と表示されます。Windows タスクマネージャまたは macOS システムログには、プロセスが実行中であると示される場合があります。サービスが実行されていない場合は、システムスキャン UI の [ISE ポスチャ（ISE Posture）] タイルに [システムスキャン：サービスは使用できません（System Scan: Service is unavailable）] と表示されます。



ネットワークを変更すると、検出フェーズが開始されます。AnyConnect ISE ポスチャの場合、プライマリインターフェイスのデフォルトルートが変更された場合、エージェントが検出プロセスに戻ります。たとえば、WiFi およびプライマリ LAN が接続された場合、エージェントは検出をリスタートします。同様に、WiFi およびプライマリ LAN が接続されたものの、その後、WiFi の接続が解除された場合、エージェントは検出をリスタートしません。

また、「システムスキャン」後、AnyConnect UI の [ISE ポスチャ（ISE Posture）] タイルに次のステータスメッセージが表示される場合があります。

- [限定的または接続なし（Limited or no connectivity）]：接続がないため検出は発生していません。AnyConnect ISE ポスチャエージェントは、ネットワーク上の不正なエンドポイントで検出を実行している可能性があります。
- [システムスキャンは現在の WiFi では不要（System scan not required on current WiFi）]：セキュアでない WiFi が検出されたため検出は発生していません。AnyConnect ISE ポスチャエージェントは、LAN、ワイヤレス（802.1X 認証が使用されている場合）、および VPN でのみ検出を開始します。WiFi がセキュアでないか、またはエージェントプロファイルで *OperateOnNonDot1XWireless* を 1 に設定してこの機能を無効にしています。
- [不正なポリシー サーバ（Unauthorized policy server）]：ネットワーク アクセスが制限されているか存在しないため、ホストが ISE ネットワークのサーバ名ルールに一致していません。
- [AnyConnect ダウンローダーが更新を実行しています…（The AnyConnect Downloader is performing update...）]：ダウンローダーが呼び出され、パッケージバージョンを比較し、AnyConnect 設定をダウンロードし、必要なアップグレードを行います。
- [システムをスキャンしています...（Scanning System...）]：ウイルス対策/スパイウェア対策のセキュリティ製品のスキャンが開始されました。このプロセス中にネットワークが変更された場合、エージェントはログファイルの生成プロセスをリサイクルし、ステータスは [検出されたポリシー サーバなし（No policy server detected）] に戻ります。
- [AnyConnect スキャンのバイパス（Bypassing AnyConnect scan）]：ネットワークは、Cisco NAC Agent を使用するように設定されています。
- [ユーザーによってキャンセルされた信頼できないポリシーサーバー（Untrusted Policy Server Cancelled by the user）]：AnyConnect UI の [システムスキャンプリファレンス（System Scan Preferences）] タブで信頼できないサーバーへの接続のブロックを解除すると、ポップアップウィンドウに AnyConnect ダウンローダーのセキュリティ警告が表示されます。この警告ページで [接続のキャンセル（Cancel Connection）] をクリックすると、[ISE ポスチャ（ISE Posture）] タイルがこのステータスに変わります。
- [ネットワークの利用規定（Network Acceptable Use Policy）]：ネットワークへのアクセスには、アクセプタブル ユース ポリシーを確認し、受け入れる必要があります。ポリシーを拒否すると、ネットワーク アクセスが制限される可能性があります。
- [ネットワーク設定の更新（Updating Network Settings）]：ISE UI の [設定（Settings）] > [ポスチャ（Posture）] > [全般設定（General Settings）] では、ネットワーク遷移間で発生させる遅延の秒数を指定できます。
- [コンプライアンス非対応。更新時間の期限が切れました。（Not Compliant. Update time expired.）]：修復のために設定された時間の期限が切れました。
- [コンプライアンス対応。ネットワーク アクセスが許可されています。（Compliant. Network access allowed.）]：修復が完了しました。[AnyConnect] > [スキャン概要（Scan Summary）] にも、ステータスが完了と示されます。

- [検出されたポリシー サーバなし（No policy server detected）]：ISE ネットワークが見つかりません。30秒後、エージェントによるプローブは低下します。デフォルトのネットワーク アクセスが有効になります。

ポスチャとマルチホーミング

AnyConnect ISE ポスチャモジュールは、マルチホーミングをサポートしていません。これは、そのようなシナリオの動作が定義されていないためです。たとえば、メディアが有線からワイヤレスに変更された後で有線に戻ると、エンドポイントが実際には有線接続でリダイレクトされている場合でも、ユーザーにはISEポスチャモジュールに準拠したポスチャステータスが表示されることがあります。

エンドポイントの同時ユーザー

AnyConnect ISE ポスチャは、複数のユーザーが同時にエンドポイントにログインしてネットワーク接続を共有した場合、個別のポスチャ評価をサポートしません。最初にAnyConnect ISEポスチャを実行したユーザーが正常にポスチャされ、エンドポイントに信頼ネットワークアクセスが許可されると、エンドポイントの他のすべてのユーザーがネットワークアクセスを継承します。これを防ぐため、管理者はエンドポイントに同時ユーザーを許可する機能を無効にできます。

ポスチャ モジュールのロギング

ISE ポスチャの場合、イベントはネイティブ オペレーティング システムのイベントログ（Windows イベントログビューアまたは macOS システムログ）に記録されます。

VPN ポスチャ の場合、エラーおよび警告は syslog（Windows 以外の場合）とイベントビューア（Windows の場合）に送信されます。使用可能なすべてのメッセージがログ ファイルに記録されます。

VPN ポスチャ モジュールコンポーネントは、オペレーティングシステム、特権レベル、および起動メカニズム（Web 起動または AnyConnect）に基づいて、ログに出力します。

- cstub.log：AnyConnect Web 起動が使用された場合にログを取り込みます。
- libcsd.log：VPN ポスチャ API を使用する AnyConnect スレッドによって作成されます。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。
- cscan.log：スキャニング実行可能ファイル（cscan.exe）によって作成される、VPN ポスチャ のメインのログです。ログ レベル設定に応じて、このログにデバッグのエントリが入力されます。

ポスチャ モジュールのログ ファイルと場所

ISE ポスチャの場合、イベントはインストールされた AnyConnect バージョンの独自のサブフォルダに含まれているため、AnyConnect イベントの他の部分から容易に分離できます。各ビューアでは、キーワードの検索およびフィルタリングが可能です。Web Agent イベントは、標準のアプリケーション ログに書き込まれます。

トラブルシューティングのために、ISE ポスチャ要件ポリシーとアセスメント レポートがイベント ログではなく、エンドポイントの別の難解化されたファイルに記録されます。一部のログ ファイル サイズ（aciseposture など）は、管理者がプロファイルに設定できますが、UI ログ サイズは事前に定義されています。

プロセスが異常終了したときは、他の AnyConnect モジュールと同じように、常にミニダンプ ファイルが生成されます。

VPN ポスチャ の場合、ファイルはユーザーのホームフォルダの次のディレクトリにあります。

- （Windows 以外）：.cisco/hostscan/log
- （Windows）：C:\Users\<user_name>\AppData\Local\Cisco HostScan\log\cscan.log

ISE ポスチャ プロファイル エディタ

管理者は、ポスチャ プロファイルを作成し、ISE にアップロードするために、このスタンドアロン エディタを使用することを選択できます。それ以外の場合、組み込みのポスチャ プロファイル エディタが ISE UI の [ポリシー要素（Policy Elements）] に設定されます。AnyConnect コンフィギュレーション エディタが ISE で起動すると、AnyConnect ソフトウェアおよび関連するモジュール、プロファイル、OPSWAT、およびカスタマイズを備えた AnyConnect 設定が作成されます。Cisco Secure Firewall ASA の ISE ポスチャ用のスタンドアロン プロファイル エディタには、次のパラメータが含まれています。

- **エージェントの動作**
  - [署名チェックの有効化（Enable signature check）]：オンにすると、エージェントによって実行される前に実行可能ファイルの署名チェックが有効になります。
  - [ログ ファイル サイズ（Log file size）]：エージェント ログ ファイルの最大サイズ。有効な値は 5 ～ 200 MB です。
  - [修復タイマー（Remediation timer）]：コンプライアンス非対応とタグ付けされるまでにユーザが修復に割くことができる時間。有効な値は 1 ～ 300 分です。
  - [エージェント ログ トレースの有効化（Enable agent log trace）]：エージェントでのデバッグ ログを有効にします。

- [非 802.1X ワイヤレス ネットワークでの動作（Operate on non-802.1X wireless networks）]：オンにすると、エージェントは非 802.1X ワイヤレス ネットワークで動作できます。
- [ステルスモードを有効にする（Enable Stealth Mode）]：ユーザによる設定なしにポスチャをサービスとして実行できるステルス モードを有効にするかどうかを選択します。
- [通知によるステルスを有効にする（Enable Stealth With Notification）]：ステルスモードの通知が有効に設定されている場合、エンドユーザーは、AnyConnect ステルスモードが非準拠の状態にある、ネットワークアクセスが制限されている、到達不能なサーバーなどがあるなどの場合でも通知メッセージを受け取ります。
- [再スキャンボタンを有効にする（Enable Rescan Button）]：障害発生後、手動修復後、ポスチャの動作不能時（など）に、ポスチャ（またはディスカバリ）を再起動する場合は、このボタンを有効にして、システムスキャン タイルに [再度スキャン（Scan Again）] の選択が表示されるようにします。このオプションは、ISE ポスチャ プロファイルで表示または非表示にできます。**[再度スキャン（Scan Again）]** をクリックすると、ディスカバリが起動し、ポスチャ フロー全体が開始されます。

（注） [再度スキャン（Scan Again）] がタイルに表示されるのは、ポスチャ プロファイルで EnableRescan タグを 1 に設定している場合だけです。0 に設定すると、[再度スキャン（Scan Again）] ボタンが表示されるのは、それが（このオプションよりも先に）表示されていた場合だけです。

（注） ISE 側でプロファイルの変更が発生すると、次回ディスカバリが起動されるときに、その変更が AnyConnect タイルに反映されます。

- [UACポップアップを無効にする（Disable UAC Popup）]：ポリシー検証中に Windows ユーザ アカウント制御（UAC）ポップアップが表示されるかどうかを決定します。デフォルト値（オフ）では、エンドユーザは引き続き接続時に管理者権限を求められます。有効にすると、ポリシーの検証中に Windows ユーザ アカウント制御（UAC）プロンプトが表示されません。UAC プロンプトをオフにすることによって、VPN ポスチャ は「管理者として実行（Run as administrator）」ではなく、特権昇格のシステム プロセスを使用します。UAC プロンプトを無効にする前に、ユーザにローカル管理者権限があるデバイスでポスチャ ポリシーを検証します。
- [バックオフタイマーの制限（Backoff Timer Limit）]：AnyConnect が ISE 検出のプローブを送信する最長時間を入力します。プローブによりトラフィックが増えるため、ネットワークの負荷にならない値を選択してください。

- [定期的なプローブ間隔（Periodic Probe Interval）]：バックオフタイマー制限を超えた後の検出プローブ間隔を指定します。AnyConnect は、有効な ISE サーバーが見つかるまで、指定された間隔で定期的なプローブを継続的に送信します。デフォルトでは 30 分で、プローブは、初回プローブの完了後、30 分間隔で継続的に送信されます。値を 0 に設定すると、定期的なプローブがディセーブルになります。

• IP アドレスの変更

最適なユーザ エクスペリエンスのため、次の値を推奨値に設定してください。

- [VLAN 検出間隔（VLAN detection interval）]：クライアント IP アドレスを更新する前にエージェントが VLAN 変更の検出を試みる間隔。有効な範囲は 0 ～ 900 秒で、推奨値は 5 秒です。
- [ping または ARP（Ping or ARP）]：IP アドレスの変更を検出する方法。デフォルトゲートウェイが ICMP パケットをブロックするように設定されている可能性があるため、推奨設定は ARP です。
- [ping の最大タイムアウト（Maximum timeout for ping）]：1 ～ 10 秒の ping タイムアウト。
- [エージェント IP 更新の有効化（Enable agent IP refresh）]：VLAN 変更の検出を有効にする場合にオンにします。
- [DHCP 更新遅延（DHCP renew delay）]：IP 更新後にエージェントが待機する秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [DHCP リリース遅延（DHCP release delay）]：エージェントによる IP 更新を遅延させる秒数。[エージェント IP 更新の有効化（Enable Agent IP Refresh）] を有効にしたときに、この値を設定します。この値が 0 ではない場合、エージェントはこの予期される遷移中に IP を更新します。更新中に VPN が検出された場合、更新は無効です。有効な値は 0 ～ 60 秒で、推奨値は 5 秒です。
- [ネットワーク遷移遅延（Network transition delay）]：計画された IP 変更を待機できるようにエージェントがネットワーク モニタリングを一時停止する期間（秒単位）。推奨値は 5 秒です。

• ポスチャ プロトコル

- [ホストの検索（Discovery host）]：エージェントが接続できるサーバ。スタンドアロン プロファイル エディタでは、1 つのホストのみを入力します。
- [サーバ名ルール（Server name rules）]：エージェントが接続できるサーバを定義する、ワイルドカード対応のカンマで区切られた名前のリスト（.cisco.com など）。
- [Call Home リスト（Call Home List）]：ロード バランシング、ルックアップのモニタリングとトラブルシューティングに使用する FQDN、またはそのノードでデフォルト

のポリシー サービス ノード（PSN）にマップする DNS の FQDN（複数シナリオの場合）を入力します。これを設定すると、ルックアップのモニタリングとトラブルシューティングついての最初のプローブは Call Home に送信されます。リダイレクト ネットワークから非リダイレクト ネットワークに移行するときにこれを設定する必要があります。

- [PRA 再送信時間（PRA retransmission time）]：パッシブ再評価の通信障害が発生した場合に、このエージェントが再試行する間隔を指定します。有効な値の範囲は 60 ～ 3600 秒です。
- [再送信遅延（Retransmission Delay）]：再試行するまでに待機する時間を秒単位で指定します。有効範囲は 5 ～ 300 秒です。
- [再送信制限（Retransmission Limit）]：メッセージに許可する再試行回数を指定します。有効な範囲は 0 ～ 10 です。

詳細パネル

AnyConnect Secure Mobility Client UI の [詳細（Advanced）] パネルは、コンポーネントの統計情報、ユーザープリファレンス、およびコンポーネント固有のその他の情報を表示するための各コンポーネントの領域です。AnyConnect システムトレイで、[すべてのコンポーネントの詳細ウィンドウ（Advanced Window for all components）] アイコンをクリックすると、新しい [システムスキャン（System Scan）] セクションに次のタブが含まれます。

（注） macOS では、これらの統計情報、ユーザー設定、メッセージ履歴などは、[統計情報（Statistics）] ウィンドウの下に表示されます。プリファレンスは、[プリファレンス（Preferences）] ウィンドウに表示され、Windows のようなタブの向きではありません。

- [プリファレンス（Preferences）]：信頼できないサーバーへの接続をブロックできます。ダウンローダーのプロセス中に、証明書が信頼できず ISE サーバーが未検証になると、「信頼できないサーバーをブロックしました（Untrusted Server Blocked）」というメッセージを受信します。ブロッキングを無効にすると、AnyConnect は悪意がある可能性があるネットワークデバイスへの接続をブロックしなくなります。
- [統計情報（Statistics）]：現在の ISE ポスチャステータス（準拠または非準拠）、OPSWAT のバージョン情報、アクセプタブル ユース ポリシーのステータス、ポスチャの最新の実行タイムスタンプ、不足要件、およびトラブルシューティングの目的で表示する必要があると判断されたその他の統計情報を提供します。
- [セキュリティ製品（Security Products）]：システムにインストールされているマルウェア対策製品のリストにアクセスします。
- [スキャンの概要（Scan Summary）]：管理者がユーザーに対して表示するように設定したポスチャ項目をユーザーが確認できるようにします。たとえば、設定されている場合、

ユーザーはシステム上にポスチャされたすべての項目を表示したり、ポスチャ チェックに失敗して修復が必要な項目のみを表示したりすることができます。

- [メッセージ履歴（Message History）]：コンポーネントについて、システムトレイに送信されたすべてのステータスメッセージの履歴を表示します。この履歴は、トラブルシューティングに役立ちます。

VPN ポスチャ モジュールが提供するもの

HostScan

HostScan は、ユーザーが Cisco Secure Firewall ASA に接続した後、かつログインする前に、リモートデバイス上にインストールされるパッケージです。HostScan は、基本モジュール、Endpoint Assessment モジュール、および Advanced Endpoint Assessment モジュールで構成されています。HostScan は、モバイルデバイス（Android、iOS、Chrome、または UWP）ではサポートされていません。

基本的機能

HostScan は自動的に AnyConnect VPN クライアントセッションを確立しているリモートデバイスのオペレーティングシステムとサービスパックを識別します。

特定のプロセス、ファイル、およびレジストリキーについて、エンドポイントを検査するように HostScan を設定することもできます。HostScan は、トンネルが完全に確立される前にこれらのすべての検査を実行し、この情報を Cisco Secure Firewall ASA に送信して、会社所有、個人用、および公共のコンピュータを識別します。この情報は、評価にも使用できます。

（注） ログイン前の評価および証明書情報の返送は実行できません。HostScan は認証方式ではありません。接続しようとしているデバイスの内容を検証するチェックを実行するだけです。

また、HostScan は、設定した DAP エンドポイント条件と照合して評価するために、次の追加の値を自動的に返します。

- Microsoft Windows、macOS、および Linux オペレーティングシステム
- Microsoft サポート技術情報（KB）番号
- デバイス エンドポイント属性タイプ（ホスト名、MAC アドレス、BIOS シリアル番号、ポート番号（レガシー属性）、TCP/UDP ポート番号、プライバシー保護、およびエンドポイント アセスメント（OPSWAT）のバージョンなど）。

（注） HostScan は Windows クライアントシステム上の Microsoft のソフトウェアアップデートに関するサービスリリース（GDR）の情報を収集します。サービスリリースには複数のホットフィックスが含まれます。サービス リリース エンドポイント属性は、ホット フィックスではなく、DAP ルールに使用されます。

エンドポイント アセスメント

エンドポイントアセスメントは、HostScan の拡張機能であり、多くの種類のウイルス対策とスパイウェア対策のアプリケーション、関連する定義の更新、およびファイアウォールについて、リモートコンピュータを検査します。Cisco Secure Firewall ASA によって特定のダイナミック アクセス ポリシー（DAP）がセッションに割り当てられる前に、この機能を使用して要件を満たすようにエンドポイント条件を組み合わせることができます。

詳細については、適切なバージョンの『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「Dynamic Access Policies」の項を参照してください。

Advanced Endpoint Assessment：マルウェア対策およびファイアウォールの修復

Windows、macOS、および Linux のデスクトップでは、マルウェア対策およびパーソナル ファイアウォール保護のソフトウェアで別のアプリケーションが修復を開始することを許可している場合に、Advanced Endpoint Assessment は、それらのソフトウェアに関するさまざまな修復を開始しようとします。

マルウェア対策：Advanced Endpoint Assessment は、マルウェア対策ソフトウェアの以下のコンポーネントを修復しようとします。

- ファイル システム保護の強制：マルウェア対策ソフトウェアが無効の場合に、Advanced Endpoint Assessment はこのコンポーネントを有効にします。
- ウイルス定義更新の強制：Advanced Endpoint Assessment の設定で定義された日数の間、マルウェア対策定義が更新されなかった場合に、Advanced Endpoint Assessment はウイルス定義の更新を開始しようとします。

パーソナル ファイアウォール：Advanced Endpoint Assessment モジュールでは、ファイアウォールを有効または無効にすることができます。

HostScan は、パーソナルファイアウォールを使用するアプリケーションとポートのブロックまたは許可をサポートしていません。

（注） すべてのパーソナル ファイアウォールがこの有効化の強制/無効化の強制機能をサポートしているわけではありません。

HostScan 用のマルウェア対策アプリケーションの設定

VPN ポスチャ モジュールをインストールする前に、次の各アプリケーションについてセキュリティ例外を指定するように、マルウェア対策ソフトウェアを設定します。マルウェア対策アプリケーションは、これらのアプリケーションの動作を悪意があるものと誤って認識する場合があります。

- cscan.exe
- ciscod.exe
- cstub.exe

ダイナミック アクセス ポリシーとの統合

Cisco Secure Firewall ASA では、HostScan の機能がダイナミック アクセス ポリシー（DAP）に統合されます。設定に応じて、Cisco Secure Firewall ASA では、DAP 割り当ての条件として、オプションの AAA 属性値と組み合わせたエンドポイント属性値が 1 つ以上使用されます。DAP のエンドポイント属性でサポートされる HostScan の機能には、OS 検出、ポリシー、基本結果、およびエンドポイントアセスメントがあります。

セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント条件がすべて満たされたときに、ASA によって DAP が適用されます。

『Cisco ASA Series VPN CLI Configuration Guide』または『Cisco ASA Series VPN ASDM Configuration Guide』の「*Configure Dynamic Access Policies*」の項を参照してください。

DAP の BIOS シリアル番号

VPN ポスチャ は、ホストの BIOS シリアル番号を取得できます。ダイナミック アクセス ポリシー（DAP）を使用し、その BIOS シリアル番号に基づいて Cisco Secure Firewall ASA への VPN 接続を許可または拒否できます。

DAP エンドポイント属性としての BIOS の指定

手順

ステップ 1 ASDM にログインします。

ステップ 2 **[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）]** または **[クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）]** > **[ダイナミックアクセスポリシー（Dynamic Access Policies）]** を選択します。

ステップ 3 [ダイナミック アクセス ポリシーの設定（Configure Dynamic Access Policies）] パネルで、[追加（Add）] または [編集（Edit）] をクリックして、BIOS を DAP エンドポイント属性として設定します。

ステップ 4 エンドポイント ID 表の右にある [追加（Add）] をクリックします。

ステップ 5 [エンドポイント属性タイプ（Endpoint Attribute Type）] フィールドで、[デバイス（Device）] を選択します。

ステップ 6 [BIOS シリアル番号（BIOS Serial Number）] チェックボックスをオンにし、[=]（等しい）または [!=]（等しくない）を選択して、[BIOS シリアル番号（BIOS Serial Number）] フィールドに BIOS 番号を入力します。[OK] をクリックし、[エンドポイント属性（Endpoint Attribute）] ダイアログボックスでの変更を保存します。

ステップ 7 [OK] をクリックして、[ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] への変更を保存します。

ステップ 8 [適用（Apply）] をクリックして、ダイナミック アクセス ポリシーへの変更を保存します。

ステップ 9 [保存（Save）] をクリックします。

BIOS シリアル番号の取得方法

- Windows：http://support.microsoft.com/kb/558124
- macOS：http://support.apple.com/kb/ht1529
- Linux：このコマンドを使用してください。

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key
system.hardware.serial
```

Cisco Secure Firewall ASA で有効にされた HostScan イメージの判別

ASDM を起動し、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [セキュアデスクトップマネージャ（Secure Desktop Manager）] > [HostScanイメージ（HostScan Image）] を選択します。

HostScan のアップグレード

AnyConnect および HostScan を手動で（msiexec を使用して）アップグレードする場合は、必ず、AnyConnect を最初にアップグレードして、その後に HostScan をアップグレードしてください。

OPSWAT サポート

VPN ポスチャ（以前の HostScan）および ISE ポスチャモジュールも、OPSWAT フレームワークを使用して、エンドポイントを保護します。

クライアントとヘッドエンドの両方を伴うこのフレームワークは、エンドポイント上のサードパーティ アプリケーションを評価するのに役立ちます。使用されている OPSWAT バージョンによって認識されるように、各ポスチャメソッドのサポートチャートが提供されます。チャートには、アプリケーションのリストの製品およびバージョン情報が含まれています。

ヘッドエンド（Cisco Secure Firewall ASA または ISE）とエンドポイント（VPN ポスチャ または ISE ポスチャ）との間にバージョン番号の不一致があるときは、ヘッドエンドのバージョンに合わせて、OPSWAT 準拠モジュールがアップグレードまたはダウングレードされます。これらのアップグレード/ダウングレードは必須であり、ヘッドエンドへの接続が確立されるとすぐにエンド ユーザの介入なしで自動的に実行されます。

VPN ポスチャ OPSWAT サポート

HostScan のサポートチャートは HostScan のパッケージバージョンに対応し、Cisco Secure Firewall ASA ヘッドエンドで機能するものを提供します。

HostScan は、AnyConnect メジャーリリースおよびメンテナンスリリースと連携するようにバージョン管理されます。ASDM で HostScan パッケージを設定するときに、バージョンを指定します。[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [セキュアデスクトップマネージャ（Secure Desktop Manager）] > [ホストスキャンイメージ（Host Scan Image）] の順に選択してください。

VPN ポスチャ のガイドライン

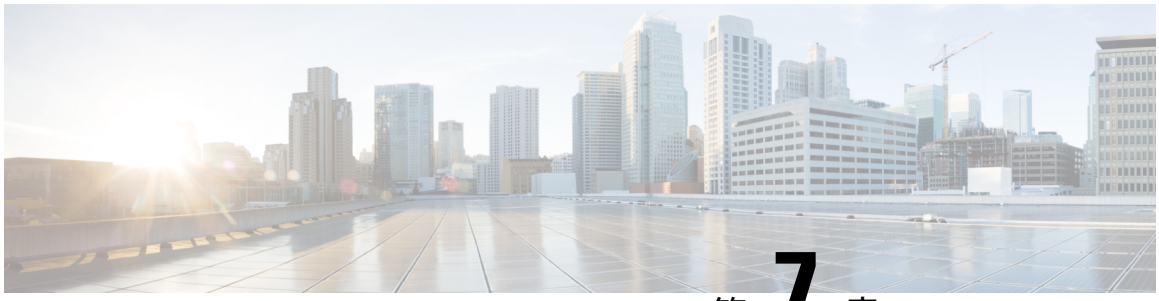
- クライアントとヘッドエンドで使用されている OPSWAT のバージョンは、一致する必要があります。
- HostScan 4.3.x までの全バージョンが OPSWAT v2 を使用します。HostScan 4.6x 以降は、OPSWAT v4 を使用します。OPSWAT v3 は、HostScan のどのバージョンでもサポートされていません。

ISE ポスチャ OPSWAT サポート

「AnyConnectエージェント準拠モジュール」は、ISE ポスチャモジュール用です。

ISE エージェント準拠モジュールのバージョンには、基盤となる OPSWAT バージョンが反映されています。ISE ポスチャでは、OPSWAT バイナリは別個のインストーラにパッケージ化されています。OPSWAT ライブラリをローカル ファイル システムから ISE ヘッドエンドに手動でロードしたり、ISE 更新フィード URL を使用して直接取得するように ISE を設定したりできます。

AnyConnect を ISE 2.1 以降とともに使用したときは、ISE 準拠モジュールに OPSWAT v3 または v4 のどちらを使用するかを選択できます。アンチマルウェアの設定は、[ワーク センター（Work Centers）] > [ポスチャ（Posture）] > [ポスチャ要素（Posture Elements）] > [条件（Conditions）] > [アンチマルウェア（Antimalware）] の ISE UI で行います。



第 7 章

AMP イネーブラの設定

AMP について

macOS 用 AMP は、エンドポイント向けの高度なマルウェア防御（AMP）を導入する手段として使用されます。社内でローカルにホストされているサーバーからエンドポイントのサブセットに AMP ソフトウェアをプッシュし、既存のユーザーベースに AMP サービスをインストールします。このアプローチでは、macOS 用 AnyConnect 管理者が、追加のセキュリティエージェントを使用できます。このエージェントは、ネットワークで発生する潜在的なマルウェア脅威を検出して排除し、企業を侵害から保護します。ダウンロードにかかる時間と帯域幅を節約し、ポータル側では変更を行う必要がなく、認証クレデンシャルをエンドポイントに送信せずに実行できます。

AMP イネーブラの導入

システム管理者権限を必要とせずに AMP イネーブラをインストールできます。ポリシーを作成して設定し、グループを作成してポリシーを割り当ててから、インストーラをダウンロードするときにそのグループを選択します。AMP イネーブラソフトウェアを適切に配布するには、https://console.amp.cisco.com/help/en/wwhelp/wwhimpl/js/html/wwhelp.htm を参照してください。

1. エンドポイント向け AMP ポータルにログインします。
2. エンドポイント向け AMP ポータルで適切なポリシーを設定します。設定したポリシーに応じて、適切なエンドポイント向け AMP ソフトウェア パッケージが作成されます。このソフトウェアパッケージは .exe ファイル（Windows 用）または .pkg ファイル（macOS 用）です。Windows では、再配布可能な .exe を選択できます。

（注） AMP コネクタのダウンロードは、ポート 443 からのみサポートされています。

3. 生成されたキット（Windows または macOS）をローカルサーバにダウンロードします。
4. AMP イネーブラ プロファイルを作成して保存するため、ASA または ISE ヘッドエンドにログインします。

（注） 特に ISE ポスチャを使用する場合は、1 つのヘッドエンド（ASA または ISE のいずれか）に
してのみプロファイルを設定することをお勧めします。

5. ASA または ISE ヘッドエンドで、オプション モジュールのリストから AMP Enable モジュールを選択し、AMP イネーブラ プロファイルを指定します。

   作成したプロファイルは、AnyConnect AMP イネーブラに使用されます。AMP イネーブラとこのプロファイルが ASA または ISE ヘッドエンドからエンドポイントにプッシュされます。

AMP イネーブラ プロファイル エディタ

管理者は、AMP プロファイルを作成して Cisco Secure Firewall ASA にアップロードするために、このスタンドアロンエディタを使用することができます。それ以外の場合は、組み込みのプロファイルエディタが [ポリシー要素（Policy Elements）] 下の ISE UI 内、または ASDM 内で設定されます。信頼されているローカル Web サーバーが AMP プロファイルエディタと連携できるようにするには、keytool コマンドを使用してルート CA 証明書を Java 証明書ストアにインポートする必要があります。

Windows：keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

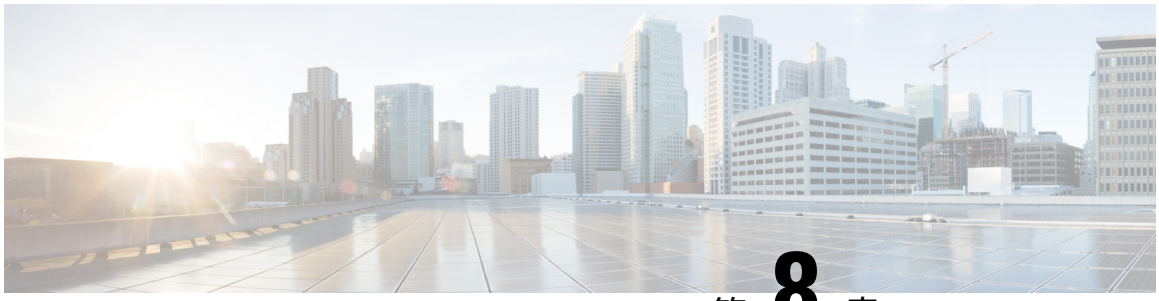
macOS：sudo keytool-import-keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer

- 名前
- 説明
- [AMPのインストール（Install AMP for Endpoints）]：AMP をインストールするためにこのプロファイルを設定する場合に選択します。
- [AMPのアンインストール（Install AMP for Endpoints）]：AMP をアンインストールするためにこのプロファイルを設定する場合に選択します。アンインストールを選択した場合、その他のフィールドに入力する必要はありません。
- [Windowsインストーラ（Windows Installer）]：.exe ファイルが存在するローカル ホスティング サーバーのアドレスまたは URL を入力します。
- [Macインストーラ（Mac Installer）]：.pkg ファイルが存在するローカル ホスティング サーバーのアドレスまたは URL を入力します。

- [チェック（Check）]：URL をチェックしてこの URL が有効であることを確認する場合にクリックします。有効な URL とは、到達可能であり信頼できる証明書が含まれている URL です。サーバーが到達可能であり、この URL で接続が確立されたら、プロファイルを保存できます。
- [スタートメニューに追加（Add to Start Menu）]：[スタート（Start）] メニューにショートカットを作成します。
- [デスクトップに追加（Add to Desktop）]：デスクトップ アイコンを作成します。
- [コンテキストメニューに追加（Add to Context Menu）]：このオプションを選択すると、ファイルやフォルダを右クリックし、[今すぐスキャン（Scan Now）] を選択してスキャンを実行できるようになります。

AMP イネーブラのステータス

AMP の実際のダウンロードとインストールに関連するメッセージはすべて、AnyConnect UI の部分的なタイルとして表示されます。マルウェア対策防御のインストール時またはアンインストール時にメッセージがユーザーに対して表示され、失敗が示されるか、または再起動が必要なことが示されます。インストール完了後、すべての AMP 関連メッセージは、AnyConnect UI ではなく AMP UI に表示されます。



第 8 章

ネットワーク可視性モジュール

ネットワーク可視性モジュールについて

ユーザーが管理対象外デバイスを使用する状況が増加しているため、企業内管理者はネットワーク内外の状況を把握しにくくなっています。Network Visibility Module（NVM）は、オンプレミスまたはオフプレミスのエンドポイントから豊富なフローコンテキストを収集するもので、Stealthwatch などのシスコソリューションまたは Splunk などのサードパーティ ソリューションと併用すると、ネットワークに接続されたデバイスおよびユーザーの動作に対する可視性を提供します。これにより、企業内管理者は、キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析を実行することができます。Network Visibility Module は、次のサービスを提供します。

- ネットワーク設計を情報に基づいてより適切に改善する（nvzFlow プロトコル仕様の IPFIX コレクタ要素の拡張：https://developer.cisco.com/site/network-visibility-module/）ために、アプリケーションの使用状況をモニタする。
- アプリケーション、ユーザー、またはエンドポイントを論理グループに分類する。
- 企業の資産を追跡し、移行アクティビティを計画するため、潜在的な異常を洗い出す。

この機能により、インフラストラクチャ導入環境全体ではなく、テレメトリを対象とするかどうかを選択できます。Network Visibility Module は、次の情報に対するより正確な可視性を得るため、エンドポイントテレメトリを収集します。

- デバイス：エンドポイント（場所に関係なく）
- ユーザー：エンドポイントにログインしているユーザー

- アプリケーション：トラフィックを生成するアプリケーション
- 場所：トラフィックが生成されるネットワークの場所
- 宛先：このトラフィックの宛先の実際の FQDN

信頼ネットワークでは、AnyConnect Network Visibility Module はフローレコードをコレクタ（Stealthwatch または Splunk などのサードパーティベンダー）にエクスポートし、このコレクタがファイル分析を実行し、UIインターフェイスおよびレポートを提供します。フロー レコードはユーザーの機能に関する情報を提供するもので、値は ID（たとえば、LoggedInUserAccountType は 12361、ProcessUserAccountType は 12362、ParentProcessUserAccountType は 12363）とともにエクスポートされます。Splunk に組み込まれた Cisco Endpoint Security Analytics（CESA）の詳細については、http://www.cisco.com/go/cesaを参照してください。ほとんどの企業内IT管理者は、データを使用して独自の可視化テンプレートを作成することを望むため、シスコは Splunk アプリケーション プラグインを介していくつかのサンプル ベース テンプレートを提供しています。

デスクトップ AnyConnect 上の NVM

従来、フロー コレクタにはスイッチまたはルータのインターフェイスに入る時点またはインターフェイスから出る時点で IP ネットワーク トラフィックを収集できる機能がありました。ネットワーク内の輻輳の原因とフローパスを特定できましたが、それ以外は特定できませんでした。エンドポイントで Network Visibility Module を使用すると、デバイスのタイプ、ユーザー、アプリケーションなどの豊富なエンドポイントコンテキストによってフローが拡張されます。これにより、収集プラットフォームの機能に応じて、フローレコードがより実用的になります。IPFIX 経由で Network Visibility Module によって提供されるエクスポートデータは、Cisco NetFlow コレクタだけでなく、Splunk、IBM Qradar、LiveAction などの他のサードパーティフロー収集プラットフォームと互換性があります。追加情報については、各プラットフォームの統合ドキュメントを参照してください。たとえば、Splunk 統合については、https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html で確認できます。

リリース 4.9 以降で Network Visibility Module コレクタを使用する場合、追加のパラメータを表示するには、Splunk アプリケーション 3.x を使用する必要があります。

この機能が有効になっている場合、Network Visibility Module の AnyConnect プロファイルは、ISE または Secure Firewall ASA ヘッドエンドからプッシュされます。ISE ヘッドエンドでは、スタンドアロン プロファイル エディタを使用し、Network Visibility Module サービスプロファイル XML を生成して ISE にアップロードし、新しい Network Visibility Module モジュールに対してマップできます。これは、Network Access Manager での操作と同様です。Cisco Secure Firewall ASA ヘッドエンドでは、スタンドアロンプロファイルエディタまたはASDMプロファイルエディタのいずれかを使用できます。

VPN の状態が接続済みに変更した時点と、エンドポイントが信頼ネットワーク内にある場合に、Network Visibility Module に通知が送信されます。

（注） Network Visibility Module を Linux で使用する場合は、必ず、Linux での Network Visibility Module の使用 （9 ページ） に記載されている準備手順を事前に完了してください。

スタンドアロン NVM

展開していない、または別の VPN ソリューションを使用している場合は、Network Visibility Module のニーズに合わせてネットワーク可視性モジュールのスタンドアロンパッケージをインストールできます。AnyConnectこのパッケージは独立して動作しますが、既存の AnyConnect Network Visibility Module ソリューションと同じレベルのフロー収集をエンドポイントから行います。スタンドアロン Network Visibility Module をインストールすると、アクティブなプロセス（macOS のアクティビティモニタなど）によってその使用が示されます。

スタンドアロンNetwork Visibility Module の設定には Network Visibility Module のプロファイルエディタ （118 ページ） を使用し、信頼ネットワーク検出（TND）の設定が必須となります。TND の設定を使用して、Network Visibility Module はエンドポイントが社内ネットワーク上にあるかどうかを判断し、適切なポリシーを適用します。

トラブルシューティングとロギングは引き続き AnyConnect DART で実行されます。AnyConnect DART は AnyConnect パッケージからインストールできます。

展開モード

Network Visibility Module は 2 つの方法のいずれかで展開できます。1) AnyConnect パッケージを使用する方法、2) スタンドアロン Network Visibility Module パッケージを使用する方法（AnyConnect デスクトップのみ）。AnyConnect パッケージの一部として展開する手順については、「*AnyConnect* の展開」の章を参照してください。そうでない場合は、次のパッケージをダウンロードすることで、完全な AnyConnect パッケージがなくても最初からスタンドアロン Network Visibility Module をインストールできます。

- anyconnect-win-[version]-nvm-standalone-k9.msi（Windows 用）
- anyconnect-macos-[version]-nvm-standalone.dmg（macOS 用）
- anyconnect-linux64-[version]-nvm-standalone.tar.gz（Linux 用）

スタンドアロン Network Visibility Module の機能は VPN には依存していません。したがって、VPN をインストールしなくてもエンドポイントに展開できます。

すでにスタンドアロン Network Visibility Module がインストールされている場合は、同じかそれ以上のバージョンの完全な AnyConnect をインストールしてシームレスに移行でき、すべての Network Visibility Module データファイルとプロファイルが保持されます。

Network Visibility Module のスタンドアロン設定にアップグレードする場合は、Network Visibility Module プロファイルでアウトオブバンドの方法（SMS など）を使用する必要があります。エンドポイントに VPN と Network Visibility Module の両方の機能が必要な場合は、VPN と Network Visibility Module の両方をインストールするために AnyConnect パッケージを展開することをお

勧めします。個別のインストールは推奨されません。次のシナリオではインストールが失敗します。

- スタンドアロンの Network Visibility Module のダウングレード
- 新しいバージョンのスタンドアロンの AnyConnect Network Visibility Module がすでに存在する場合に、古いバージョンの Network Visibility Module をインストールする。このシナリオでは、結果としてスタンドアロン Network Visibility Module がアンインストールされる。
- AnyConnect Network Visibility Module がすでに存在する場合に、スタンドアロンの Network Visibility Module の任意のバージョンをインストールする

モバイル AnyConnect での NVM

Network Visibility Module（NVM）は、Google Play Store で入手可能な Android 用の AnyConnect Secure Mobility Client の最新バージョンに含まれています。Network Visibility Module は、Samsung Knox バージョン 2.8 以降を実行している Samsung のデバイスでサポートされています。その他のモバイル デバイスは、現在サポートされていません。

Android の Network Visibility Module は、サービスプロファイル設定の一部です。Android 上で Network Visibility Module を設定するためには、AnyConnect Network Visibility Module プロファイルエディタによって AnyConnect Network Visibility Module プロファイルが生成され、モバイルデバイスマネジメント（MDM）を使用して Samsung のモバイルデバイスにプッシュされます。

ガイドライン

- Network Visibility Module は、Samsung Knox バージョン 3.0 以降を実行している Samsung のデバイスでサポートされています。その他のモバイルデバイスは、現在サポートされていません。
- モバイルデバイスでは、Network Visibility Module コレクタへの接続は、IPv4 または IPv6 でサポートされています。
- Java ベースのアプリケーションでのデータ収集トラフィックはサポートされています。

Network Visibility Module の使用方法

次のシナリオでは、Network Visibility Module を使用できます。

- セキュリティ インシデントの発生後、漏洩がなかったか確認するため、ユーザのネットワーク履歴を監査する。
- システムまたは管理者権限が、ユーザのマシンで実行されているネットワーク接続プロセスにどのように影響しているか確認する。
- レガシー OS を実行しているすべてのデバイスの一覧を取得する。

- ネットワーク内のどのアプリケーションが最も多くのネットワーク帯域幅を使用しているか確認する。
- ネットワーク内で何種類のバージョンの Firefox が使用されているか確認する。
- ネットワーク内で Chrome.exe 接続の何パーセントを IPv6 が占めているか確認する。

Network Visibility Module の収集パラメータ

3 つの syslog データソース（フロー、エンドポイント ID、インターフェイス情報）の固有識別子（UDID）フィールドが、これらのソース間でレコードを関連付ける方法として使用されます。特定のインターフェイスの詳細を収集するために、InterfaceInfoUDID フィールドを使用して、フローごとのレコードをインターフェイス情報レコードと関連付けることができます。エンドポイントで収集され、コレクタにエクスポートされるパラメータを次に示します。

表 *8 :* エンドポイントアイデンティティ

パラメータ	説明/注意事項
[仮想ステーション名（Virtual Station Name）]	エンドポイントで設定されたデバイス名（Boris-Macbook など） ドメイン参加マシンはの形式は <machinename>.<domainname>.<com>（CESA-WIN10-1.mydomain.com など）になります。 Android の場合、Samsung による提供がないため、空。
[UDID]	汎用一意識別子。各フローに対応するエンドポイントを一意に識別します。この UDID 値は、デスクトップの HostScan およびモバイルの ACIDex でも報告されます。
[OS 名（OS Name）]	エンドポイントのオペレーティングシステムの名前（WinNTなど）
[OS のバージョン（OS Version）]	エンドポイントのオペレーティングシステムのバージョン（6.1.7601など）
[OS のエディション（OS Edition）]	OS のエディション（Windows 8.1 Enterprise Edition など）
[SystemManufacturer]	エンドポイントの製造元（Lenovo、Apple など）
[システム タイプ（System Type）]	Android の場合、`arm` に設定。 それ以外のプラットフォームの場合、`x86` または `x64`。

パラメータ	説明/注意事項
[Agent バージョン（Agent Version）]	エンドポイント上で実行されている Network Visibility Module クライアントソフトウェアのバージョン。通常は major_v.minor_v.build_no の形式

表 *9:* インターフェイス情報

パラメータ	説明/注意事項
[エンドポイント UDID（Endpoint UDID）]	UDID と同じ。
[InterfaceInfoUID]	インターフェイスメタデータの一意の ID。InterfaceInfo レコードからインターフェイスメタデータを検索するために使用されます。
[インターフェイス インデックス（Interface Index）]	OS によって報告されたネットワーク インターフェイスのインデックス。
[インターフェイス タイプ（Interface Type）]	インターフェイスのタイプ（有線、ワイヤレス、セルラー、VPN など）。
[インターフェイス名（Interface Name）]	OSによって報告されたネットワーク インターフェイス/アダプタの名前。
[インターフェイス詳細リスト（Interface Details List）]	状態および SSID、InterfaceDetailsList の属性。インターフェイスのネットワークの状態（信頼または非信頼）と、当該の接続の SSID を示す。
[インターフェイス MAC アドレス（Interface MAC address）]	インターフェイスの MAC アドレス。 デスクトップのみ。Android の場合は空（サポートされていないため）

表 *10:* フロー情報

パラメータ	説明/注意事項
[送信元 IPv4 アドレス（Source IPv4 Address）]	フローがエンドポイントで生成されたインターフェイスの IPv4 アドレス。
[宛先 IPv4 アドレス（Destination IPv4 Address）]	フローがエンドポイントから生成された宛先の IPv4 アドレス。
[送信元転送ポート（Source Transport Port）]	フローがエンドポイントで生成された送信元ポート番号。

パラメータ	説明/注意事項
[宛先転送ポート（Source Transport Port）]	フローがエンドポイントから生成された宛先ポート番号。
[送信元 IPv6 アドレス（Source IPv6 Address）]	フローがエンドポイントで生成されたインターフェイスの IPv6 アドレス。 Android の場合は空（サポートされていないため）
[宛先 IPv6 アドレス（Destination IPv6 Address）]	フローがエンドポイントから生成された宛先の IPv6 アドレス。 Android の場合は空（サポートされていないため）
[開始時刻（秒）（Start Sec）] [終了時刻（秒）（End Sec）]	フローの開始または終了を示す絶対タイムスタンプ（ミリ秒単位）。
[開始ミリ秒（Start Msec）] [終了ミリ秒（End Msec）]	フローの開始または終了を示す絶対タイムスタンプ（秒単位）。
[フロー UDID（Flow UDID）]	UDID と同じ。
[ログイン ユーザ（Logged In User）]	物理デバイス上のログインユーザ名（Authority\Principal 形式） Android の場合は空（サポートされていないため）
[ログイン ユーザのアカウント タイプ（Logged In User Account Type）]	ログインユーザのアカウントタイプ。 Android の場合は空（サポートされていないため）
[プロセス ID（Process ID）]	ネットワークフローを開始したプロセスのプロセス ID。
[プロセス名（Process Name）]	エンドポイントでネットワークフローを生成する実行可能ファイルの名前。
[プロセス ハッシュ（Process Hash）]	エンドポイントでネットワークフローを生成する実行可能ファイルの一意の SHA256 ハッシュ。
[プロセス アカウント（Process Account）]	エンドポイントでネットワークフローを生成するアプリケーションが実行されたコンテキストでの Authority\Principle 形式の完全修飾アカウント。 Android の場合は空（サポートされていないため）
[プロセスアカウントタイプ（Process Account Type）]	プロセスアカウントのアカウントタイプ。 Android の場合は空（サポートされていないため）

パラメータ	説明/注意事項
[プロセスパス（Process Path）]	ネットワークフローを開始したプロセスのファイルシステムパス Android の場合は空（サポートされていないため）
[プロセス引数（Process args）]	ネットワークフローを開始したプロセスのコマンドライン引数（プロセスパスを除く）。 Android の場合は空（サポートされていないため）
[親プロセス ID（Parent Process ID）]	ネットワークフローを開始したプロセスの親プロセスの ID。
[親プロセス名（Parent Process Name）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの名前。
[親プロセスハッシュ（Parent Process Hash）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの実行可能ファイルの一意の SHA256 ハッシュ。Android の場合、0 に設定。
[親プロセスのアカウント（Parent Process Account）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスが実行されたコンテキストでの Authority \ Principle 形式の完全修飾アカウント。 Android の場合は空（サポートされていないため）
[親プロセスのアカウントタイプ（Parent Process Account Type）]	親プロセスアカウントのアカウントタイプ。 Android の場合は空（サポートされていないため）
[親プロセスパス（Parent Process Path）]	ネットワークフローを開始したプロセスの親のファイルシステムパス。 Android の場合は空（サポートされていないため）
[親プロセス引数（Parent Process Args）]	ネットワークフローを開始したプロセスの親のコマンドライン引数（親プロセスパスを除く）。 Android の場合は空（サポートされていないため）
[DNS サフィックス（DNS suffix）]	エンドポイント上のフローに関連付けられたインターフェイス上で設定。
[L4ByteCountIn]	レイヤ 4 のエンドポイントでの特定のフロー中にダウンロードされた合計バイト数（L4 ヘッダーを除く）。
[L4ByteCountOut]	レイヤ 4 のエンドポイントでの特定のフロー中にアップロードされた合計バイト数（L4 ヘッダーを除く）。

パラメータ	説明/注意事項
[宛先ホスト名（Destination Hostname）]	エンドポイントの宛先 IP に解決される実際の FQDN
[インターフェイス UID（Interface UID）]	インターフェイス情報テーブルのインターフェイス UID と同じ。UDID とともに送信されるインターフェイスレコードからこのフローのインターフェイス情報を識別するために使用されます。
[モジュール名リスト（Module Name List）]	フローを生成したプロセスによってホストされているモジュールの 0 個以上の名前のリスト。dllhost、svchost、rundll32 などの一般的なコンテナ内にメインの DLL を含めることができます。また、JVM の jar ファイルの名前など、他のホストされているコンポーネントを含めることもできます。 Android の場合は空（サポートされていないため）
[モジュールのハッシュ リスト（Module Hash List）]	モジュール名リストに関連付けられているモジュールの 0 個以上の SHA256 ハッシュのリスト。 Android の場合は空（サポートされていないため）

Network Visibility Module のプロファイルエディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、または デュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。収集データを Stealthwatch 7.3.1 以前のリリース（または Splunk や同様の SIEM ツール以外のもの）に送信する場合、キャッシュデータは信頼ネットワークに送信はされますが、処理されません。Stealthwatch アプリケーションについては、『Stealthwatch Enterprise Endpoint License and NVM Configuration Guide』を参照してください。

TND が Network Visibility Module プロファイルに設定されている場合、信頼ネットワーク検出は Network Visibility Module によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステムログに信頼ネットワーク検出の使用状況が表示されます。

Network Visibility Module プロファイルで TND を直接設定する場合、管理者が定義した信頼できるサーバーと証明書ハッシュによって、ユーザーが信頼できるネットワーク上にいるか、信頼できないネットワーク上にいるかが判別されます。コア VPN プロファイルの信頼ネットワーク検出を設定する管理者は、代わりに、コア VPN プロファイルで信頼された DNS ドメインと信頼された DNS サーバーを設定します。AnyConnect プロファイルエディタ、プリファレンス（Part 2） （98 ページ）

- [デスクトップ（Desktop）] または [モバイル（Mobile）] ：Network Visibility Module をデスクトップとモバイルデバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）] ：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [ポート（Port）] ：コレクタがリッスンするポート番号を指定します。
  - [セキュア（Secure）] ：Network Visibility Module が DTLS 経由でコレクタにデータを安全に送信するかどうかを決定します。このチェックボックスをオンにすると、Network Visibility Module はトランスポートに DTLS を使用します。DTLS 接続では、DTLS サーバ（コレクタ）証明書がエンドポイントによって信頼されている必要があります。信頼できない証明書はサイレントに拒否されます。

    DTLS サポートには CESA Splunk App v3.1.0 の一部としてのコレクタが必要であり、DTLS 1.2 が最小サポートバージョンです。
- **キャッシュの設定**
  - [最大サイズ（Max Size）] ：データベースが到達できる最大サイズを指定します。以前はキャッシュ サイズに事前設定の制限がありましたが、プロファイル内で設定でき

るようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

- [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

  日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- **[定期テンプレート（Periodi Template）]**：テンプレートがエンドポイントから送信される間隔を指定します。デフォルト値は 1440 分です。

- [定期的なフローレポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フローレポートが定期送信されます。デフォルトで、Network Visibility Module は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、 *n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- **[集約間隔（Aggregation interval）]**：データフローをエンドポイントからエクスポートする間隔を指定します。デフォルト値の 5 秒を使用すると、単一のパケットで複数のデータフローがキャプチャされます。間隔の値が 0 秒の場合は、パケットごとに単一のデータフローが含まれます。有効な範囲は 0 ~ 600 秒です。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンド ユーザーへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイムデータとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

  キャッシュデータはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または [すべてのネットワーク（all networks）] を選択します。

- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。

  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにか

かる時間が削減されるよう、ブロードキャストパケットおよびマルチキャストパケットの収集はオフになっています。ブロードキャストパケットとマルチキャストパケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。

- [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。

- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時にアクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

  [追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。

  - ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
  - それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
  - より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
  - 選択したコレクションモードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。
  - 以前の AnyConnect リリースのプロファイルがそれより後の AnyConnect リリースのプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。
  - [名前（Name）]：作成するポリシーの名前を指定します。
  - [ネットワーク タイプ（Network Type）]：収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。
  - [フロー フィルタ ルール（Flow Filter Rule）]：一連の条件と、すべての条件が満たされたときに実行するアクションを、フローの収集または無視として定義します。最大

25 のルールを設定でき、各ルールに最大 25 の条件を定義できます。[フロー フィルタ ルール（Flow Filter Rule）] リストの右側にある上下ボタンを使用してルールの優先順位を調整し、後続のルールよりも優先的に考慮されるように設定します。[追加（Add）] をクリックし、フロー フィルタ ルールのコンポーネントを設定します。

- [名前（Name）]：フロー フィルタ ルールの一意の名前。
- [タイプ（Type）]：各フィルタ ルールには [収集（Collect）] または [無視（Ignore）] が指定されます。フィルタ ルールが満たされた場合に適用するアクション（[収集（Collect）] または [無視（Ignore）]）を決定します。[収集（Collect）] する場合、条件が満たされるとフローが許可されます。[無視（Ignore）] する場合、フローはドロップされます。
- [条件（Conditions）]：照合する各フィールドのエントリと、合致と見なすのはそのフィールド値が等しいときか等しくないときか、判断する操作を追加します。各操作にはフィールド識別子とそのフィールドに対応する値が含まれます。フィールドの一致では、フィルタ エンジン ルールの設定でルール セットに大文字と小文字を区別しない操作（EqualsIgnoreCase）を適用しない限り、大文字と小文字が区別されます。有効にした後、ルール下で設定された値フィールドへの入力は、大文字と小文字が区別されません。

- **[包含（Include）]/[除外（Exclude）]**
  - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドはすべて収集されます。どのフィールドもオンになっていない場合は、フィールドはすべて収集されます。
  - [フィールド（Fields）]：エンドポイントから受信する情報と、ポリシー要件を満たすためにデータ収集に含めるフィールドを決定します。ネットワークタイプ、およびどのフィールドを含めるか、または除外するかに基づいて、Network Visibility Module はエンドポイント上で適切なデータを収集します。

（注） 次のシナリオのいずれかが存在する場合、アップグレード中に、ProcessPath、ParentProcessPath、ProcessArgs、および ParentProcessArgs はデフォルトで、フロー情報でレポートされないように除外されます。

- 古いバージョンの Network Visibility Module のプロファイルにデータ収集ポリシーがない場合、またはデータ収集ポリシーが含まれていない場合。
- 古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあり、新しいバージョンのプロファイルエディタでプロファイルが開かれて保存された場合。古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあったが、新しい 4.9 以降のバージョンのプロファイルエディタでプロファイルが開かれて保存されていない場合は、次の 4 つのフィールドが含まれます。

Network Visibility Module が親プロセス ID を計算できない場合、値はデフォルトで 4294967295 になります。

FlowStartMsec と FlowStopMsec は、フローのエポックタイムスタンプをミリ秒単位で決定します。

インターフェイスの状態と SSID を選択して、インターフェイスのネットワーク状態が信頼できるかどうかを指定できます。

- [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードを、プライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。次に、実際の値ではなく、値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

  包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- [Knoxのデータ収集ポリシー（モバイルのみ）（Data Collection Policy for Knox (Mobile Specific)]：モバイルプロファイルを選択した場合にデータ収集ポリシーを指定するオプションです。Knox コンテナのデータ収集ポリシーを作成するには、[範囲（Scope）] の下の [Knox のみ（Knox-Only）] チェックボックスをオンにします。[デバイスの範囲（Device Scope）] で適用されるデータ収集ポリシーは、別の Knox コンテナデータ収集ポリシーが指定されていない限り、Knox コンテナトラフィックの場合も適用されます。データ収集ポリシーを追加または削除するには、前述の [データ収集ポリシー（Data Collection Policy）] の説明を参照してください。モバイルプロファイルでは最大 6 つの異なるデータ収集ポリシー（デバイス用に 3 つ、Knox 用に 3 つ）を設定できます。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、Network Visibility Module が設定されると、ユーザーに対して表示されるようになります。リモートユーザーは、Network Visibility Module アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して Network Visibility Module を制御します。

- [モバイルネットワークでのエクスポート（Export on Mobile Network）]（オプションおよびモバイルのみ）：デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローのエクスポートを許可するかどうかを指定します。有効な場合（デフォルト値）、エンドユーザーは、[利用許可ポリシー（Acceptable User Policy）] ウィンドウが表示されているとき、または後で AnyConnect Android アプリケーションで **[設定（Settings）] > [NVM 設定（NVM-Settings）] > > [NVM にモバイルデータを使用する（Use mobile data for NVM）]** チェックボックスをオンにして、管理者を上書きできます。[モバイルネットワークでのエクスポート（Export on Mobile Network）] チェックボックスをオフにすると、デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローがエクスポートされず、エンドユーザーはそれを変更できません。

- [信頼ネットワーク検出（Trusted Network Detection）]：この機能は、エンドポイントが物理的に社内ネットワーク上にあるかどうかを検出します。ネットワークの状態は、いつデータをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために Network Visibility Module によって使用されます。[設定（Configure）] をクリックして、信頼ネットワーク検出の設定を行います。SSL プローブが設定済みの信頼できるヘッドエンドに送信され、到達可能であれば、証明書で応答します。次に、サムプリント（SHA-256 ハッシュ）が抽出され、プロファイル エディタのハッシュ セットと照合されます。一致が見つかった場合はエンドポイントが信頼ネットワーク内にあることを意味します。ただし、ヘッドエンドが到達不能である場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼されていないネットワーク内にあると見なされます。

（注） 内部ネットワーク外から操作している場合、信頼ネットワーク検出は DNS 要求を行い、設定されたサーバーへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

TND が NVM プロファイルに設定されておらず、VPN モジュールがインストールされている場合、NVM は Trusted Network Detection の設定を使用して、エンドポイントが信頼ネットワーク内にあるかどうかを判断します。NVM プロファイル エディタの TND 設定には次が含まれます。

1. **https://**：信頼されている各サーバの URL（IP アドレス、FQDN、またはポートアドレス）を入力し、[追加（Add）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

2. [証明書ハッシュ（SHA-256）（Certificate Hash (SHA-256)）]：信頼されているサーバへのSSL接続が成功した場合、このフィールドは自動的に入力されます。それ以外の場合は、サーバ証明書の SHA-256 ハッシュを入力して [設定（Set）] をクリックすることにより手動で設定できます。

3. [信頼されているサーバのリスト（List of Trusted Servers）]：このプロセスで複数の信頼されているサーバを定義できます（最大値は 10 です）。サーバは、設定されている順序で信頼ネットワーク検出に対して試行されるため、[上に移動（Move Up）] ボタンと [下に移動（Move |Down）] ボタンを使用して順序を調整できます。エンドポイントが最初のサーバに接続できなかった場合は、2 番目のサーバという順序で試行されます。リスト内のすべてのサーバをした後、エンドポイントは 10 秒待機してからもう一度途最終試行を行います。サーバが認証されると、エンドポイントは信頼ネットワーク内で考慮されます。

プロファイルを `NVM_ServiceProfile.xml` として保存します。この名前でプロファイルを保存する必要があります。そうしないと、Network Visibility Module はデータの収集と送信に失敗します。

フロー フィルタについて

フローフィルタの追加により、各フローで指定したフィールドに対してアクションが設定されている、単にフィールド中心であるものから現在のデータ収集ポリシーが拡張されます。フローフィルタを使用して、フロー全体（特定のフィールドのみでなく）を収集または無視するルールを作成して適用できるため、関心対象のトラフィックだけを監視し、ストレージ要件を軽減できる可能性があります。

ルール条件

- ルールとは、ルールに指定したすべての条件がフローデータに対して満たされた場合のみの一致です。
- 最初に満たされたルールがフローに適用されます。
- フィルタポリシーで許可されている場合は、残りのデータ収集ポリシー（[包含（include）] フィールド、[除外（exclude）] フィールド、[匿名化（anonymized）] フィールド）もフローに適用されます。
- 複数のルールのインスタンスを使用する場合、
  - フローデータに一致するルールがない場合、フローに対して行われるアクションはありません。デフォルトの動作（フローの収集）が行われます。

- ルールがフローデータと一致すると、そのフローのルールで指定されたアクションが適用されます。それより後のルールはチェックされません。Network Visibility Module のプロファイルエディタ （118ページ） の [フローフィルタ ルール（Flow Filter Rule）] パラメータで指定したルールの順序は、一致が複数発生した場合の優先順位を表します。

ワイルドカード、CIDR、およびエスケープ シーケンスのサポートの使用

ルールの条件を入力する際、IP アドレスの場合は、ワイルドカード文字または CIDR 表記法を使用して、より広い範囲のフィールド値を定義できます。また、フィールド値に特定のエスケープ シーケンスを使用できます。IP フィールドの場合、CIDR スラッシュ（/）表記法で、ルールに一致する必要がある IP アドレスを指定できます。たとえば、「192.30.250.00/16」は、「255.255.0.0」のサブネット マスクを適用することで派生したルーティング プレフィックス「192.30.0.0」を持つすべてのアドレスと一致します。テキスト フィールドの場合、ワイルドカード（* および ?）とエスケープ シーケンス（*、\?、および \\）を使用してより広い入力範囲を取得できます。たとえば、「Jane*」というログイン ユーザーは、「Jane」で開始するすべてのユーザー名と一致します。

フロー フィルタリング シナリオを実現するサンプル設定

特定のポート（ポート 53 など）ですべての UDP トラフィックをドロップするには、フロー フィルタ ルール タイプ [無視（Ignore）] と、次の 2 つの条件を設定します。

- 条件 1：フロー プロトコルは UDP と [等しい（Equals）] ことを指定します。
- 条件 2：ポート番号が 53 と [等しい（Equals）] ことを指定します。

1 つの特定のプロセス（Tor ブラウザなど）から発信されたトラフィックのみを収集するには、次の 1 つの条件を追加して、その他すべてのフローをドロップする [無視（Ignore）] のタイプを使用したフィルタ ルールを設定します。

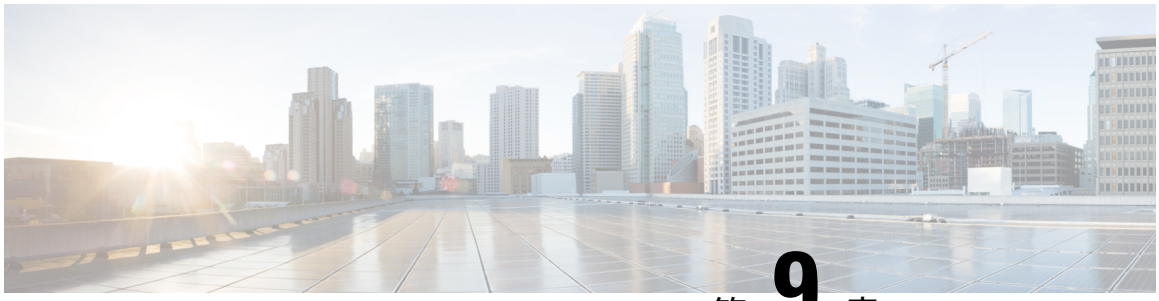
- 条件 1：プロセス名が Tor ブラウザと [等しくない（Not Equals）] ことを指定します。

サブネット内の 1 つの特定の IP から発信されたトラフィックのみを収集するには、次の 2 つのルールを設定します。

- ルール 1：IPv4 発信元アドレスが 192.168.30.14 と [等しい（Equals）] 条件で [収集（Collect）] するタイプのルールを設定します。
- ルール 2：IPv4 発信元が 192.168.30.0/24 と [等しい（Equals）] 条件で [無視（Ignore）] するタイプの 2 つ目のルールを設定します。

カスタマーフィードバックモジュールによるNVMステータスの提供

カスタマー フィードバック モジュールのコレクションの一部は、Network Visibility Module がインストールされているかどうか、1 日のフロー数、および DB サイズについてのデータを提供します。



第 9 章

Umbrella ローミング セキュリティ

Umbrella ローミング セキュリティ モジュールには、Professional、Insights、Platform、MSP のいずれかのパッケージでの Umbrella ローミング セキュリティ サービスのサブスクリプションが必要です。Umbrella ローミングセキュリティはアクティブな VPN がないときに DNS レイヤセキュリティを提供し、Cisco Umbrella サブスクリプションはインテリジェントプロキシを追加します。さらに、Cisco Umbrella サブスクリプションはコンテンツ フィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。サブスクリプションに関係なく、同じ Umbrella ローミング セキュリティ モジュールが使用されます。

Umbrella ローミング セキュリティ モジュールのプロファイル（OrgInfo.json）は、各展開を対応するサービスに関連付け、対応する保護機能は自動的に有効化されます。

Umbrella ダッシュボードは、Umbrella ローミング セキュリティ モジュールから発信されるすべてのインターネットアクティビティについてリアルタイムの可視性を提供します。ポリシーおよびレポートの精度のレベルは Umbrella サブスクリプションによって異なります。

サービス レベル サブスクリプションごとに含まれる機能の詳細な比較については、https://umbrella.cisco.com/products/packages を参照してください。

- Android 用の AnyConnect Umbrella モジュール （291 ページ）
- Android Windows または OS 用の AnyConnect Umbrella モジュール （293 ページ）

Android 用の AnyConnect Umbrella モジュール

Android OS の AnyConnect のための包括モジュールは、DNS レイヤ保護を提供する管理対象 Android デバイスのローミングクライアントです。この保護は、Android ワークプロファイルでカバーされるアプリケーションとブラウジングの両方に拡張されます。

モバイルデバイス管理システム (MDM) は、このクライアントを Android デバイスに展開し、Umbrella 設定を Android デバイスにプッシュするために必要です。サポートされている MDM およびその他の前提条件のリストについては、「Android OS で AnyConnect の Umbrella モジュールを展開するための前提条件」を参照してください。

一部の AnyConnect 機能では、Android での Umbrella 機能に制限がある場合があります。

- アプリケーションごとの VPN は、OS の制限により、Umbrella モジュールでは機能しません。リモートアクセス VPN がアクティブな場合、Umbrella による保護は、トンネルされ

たVPNによってトンネリングされたDNSトラフィックにのみ適用されます。アプリケーションごとのVPNに対してリモートアクセスが設定されている場合は、トンネル化されたアプリケーションのDNSトラフィックに対してのみ、Umbrellaによる保護が適用されます。

- ロックダウン（フェールクローズ）オプションを使用して、常時接続VPNを使用しないでください。VPNサーバに到達できない場合、インターネットアクセスを停止します。常時接続VPNがオンに設定されている場合にロックダウン設定をオフにするには、MDMガイドを参照してください。

Umbrella完全機能セットの説明については、「Umbrella Module for AnyConnect (Android OS)」を参照してください。

Android OS で AnyConnect の Umbrella モジュールを展開するための前提条件

（注） AnyConnectは、MDMで作成されたワークプロファイル内のアプリとブラウザから生成されたトラフィックをモニタし、それに応じて閲覧をブロックまたは許可します。アプリケーションやブラウザによってワークプロファイルの外部で生成されたトラフィックはモニタされません。

- ソフトウェアを展開し、Umbrella設定をモバイルデバイスにプッシュするためのモバイルデバイス管理システム（MDM）。現在テスト済みのバージョンは、Mobile Iron、Meraki、VMWare Workspace 1（AirWatch）、またはMicrosoft Intuneです。
- Android OSバージョン6.0.1以降を搭載したAndroid（Samsung/Google Pixel）モバイルデバイス。
- DNSポリシーの設定、登録済みAndroidデバイスの管理、およびレポートのためのUmbrellaライセンス。
- 機能を有効にするためのUmbrella組織ID。
- 信頼ネットワーク検出（TND）の場合：
  - Umbrellaモジュールは、HTTPSが有効な仮想アプライアンス（VA）を検出すると、それ自身を非アクティブにします。ただし、VAがHTTPSをサポートしていない場合は、Umbrellaモジュールが動作を続行します。
  - umbrella_va_fqdns内のすべてのVA FQDNを有効にする必要があります。

Android Windows または OS 用の AnyConnect Umbrella モジュール

Umbrella ローミング クライアントと Umbrella ローミング セキュリティ モジュールの非互換性

Umbrella ローミング セキュリティ モジュールと Umbrella ローミング クライアントは互換性がありません。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、ローミング セキュリティ モジュールのインストール中に Umbrella ローミングクライアント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 クライアントの既存インストールを Umbrella 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 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 ローミングクライアントをアンインストールすることもできます。

Cisco Umbrella アカウントの取得

Umbrella ダッシュボード（http://dashboard.umbrella.com/）は、展開に含める Umbrella ローミングセキュリティ モジュールのプロファイル（OrgInfo.json）を取得できるログインページです。このページでは、ローミングクライアントのアクティビティのポリシーとレポートを制御することもできます。

ダッシュボードからの OrgInfo ファイルのダウンロード

OrgInfo.json ファイルは、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 ダッシュボードインスタンスについての詳細情報です。

Umbrella ダッシュボード（https://dashboard.umbrella.com）から OrgInfo.json を取得する必要があります。

[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、[モジュールプロファイル（Module Profile）] をクリックします。特定のインストール/展開手順と特定のパッケージおよびファイルについては、AnyConnect 展開の概要 （2 ページ）を参照してください。

（注） OrgInfo.json ファイルを初めて展開すると、データ サブディレクトリ（/umbrella/data）にコピーされて、他のいくつかの登録ファイルも作成されます。したがって、OrgInfo.json 置換ファイルを展開する必要がある場合は、このデータ サブディレクトリを削除する必要があります。または、Umbrella ローミング セキュリティ モジュールをアンインストールし（データ サブディレクトリが削除されます）、新しい OrgInfo.json ファイルを再インストールすることもできます。

Umbrella ローミング セキュリティの起動と実行

AnyConnect を展開するとき、Umbrella ローミング セキュリティ モジュールは、追加機能を有効にするために含めることができるオプションモジュールの 1 つです。

Umbrella ローミング セキュリティ モジュールのステータスおよび状態に関する説明については、『The AnyConnect Plugin: Umbrella Roaming Security Client Administrator Guide』を参照してください。

Windows 7 SP1 ユーザは、インストールまたは初回使用前に、Microsoft .NET Framework 4.0 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 ローミングセキュリティ 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 ローミング セキュリティ モジュールを有効にする必要があります。

OrgInfo.json ファイルの設定

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。OrgInfo.json ファイルを展開し、CLI または GUI を使用して Cisco Secure Firewall ASA または ISE から Umbrella ローミング セキュリティ モジュールを有効にすることができます。次の手順では、最初に Cisco Secure Firewall ASA から有効にする方法、次に ISE から有効にする方法を示します。

Secure Firewall ASA CLI

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から Cisco Secure Firewall ASA ファイルシステムに取得した OrgInfo.json をアップロードします。
2. 設定に応じてグループ ポリシー名を適切に調整して、次のコマンドを実行します。

```
webvpn
 anyconnect profiles OrgInfo disk0:/OrgInfo.json

group-policy DfltGrpPolicy attribute
 webvpn
  anyconnect profiles value OrgInfo type umbrella
```

ASDM GUI

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。
2. [追加（Add）] を選択します。
3. プロファイルの名前を入力します。
4. [プロファイルの使用（Profile Usage）] ドロップダウン メニューから Umbrella セキュリティ ローミング クライアント タイプを選択します。OrgInfo.json ファイルが、[プロファイルの場所（Profile Location）] フィールドに入力されます。
5. [アップロード（Upload）] をクリックして、ダッシュボードからダウンロードした OrgInfo.json ファイルの場所を参照します。
6. [グループ ポリシー（Group Policy）] ドロップダウン メニューで DfltGrpPolicy に関連付けます。グループ ポリシーで新しいモジュール名を指定するには、追加の AnyConnect モジュールの有効化 （31 ページ）を参照してください。

ISE

ISE からイネーブルにするには、以下の手順に従います。

1. Umbrella ダッシュボード（https://dashboard.umbrella.com）から OrgInfo.json をアップロードします。
2. ファイル OrgInfo.xml の名前を変更します。
3. AnyConnect を展開するための ISE の設定 （34 ページ）の手順に従います。

クラウド最新情報

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。Umbrella ローミングセキュリティとその他の AnyConnect のクラウド更新を有効にするには、Umbrella ダッシュボードにログインします。**[ID（Identities）] > [ローミングコンピュータ（Roaming Computers）] >** 設定アイコン（歯車アイコン）の下で、[新しいバージョンがリリースされたら常に、VPNモジュールを含むAnyConnectを自動的に更新する（Automatically update AnyConnect, including VPN module, whenever new versions are released）] をオンにします。更新は VPN が有効である間は実行されません。デフォルトでは、このオプションは選択されていません。

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にのみ実行され、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）を持つデバイスを無視します。

セキュリティ ポリシーの設定とレポートの確認

保護を受信し、レポート情報を表示し、ポリシーを設定するには、Cisco Umbrellaアカウントが必要です。詳細な説明については、https://docs.umbrella.com/product/umbrella/ または https://support.umbrella.com にアクセスして追加情報を参照してください。

インストール後90分から2時間以内に、ローミング コンピュータがUmbrellaダッシュボードに表示されます。https://dashboard.umbrella.com に移動して認証し、**[ID（Identities）] > [ローミング コンピュータ（Roaming Computers）]** の順にアクセスすると、ローミング クライアントのリスト（アクティブクライアントと非アクティブクライアントの両方）とインストールされている各クライアントの詳細が表示されます。

最初は、セキュリティ フィルタリングが基本レベルのデフォルトのポリシーがローミング コンピュータに適用されています。このデフォルトのポリシーは、ダッシュボードの [ポリシー（Policies）] セクション（または [設定（Configuration）] > [Cisco Umbrella アカウントのポリシー（Policy for Cisco Umbrella accounts）]）にあります。

ローミングクライアントのレポートは、[レポート（Reports）]セクションにあります。Umbrellaローミング セキュリティ モジュールがインストールされVPNがオフにされているコンピュータからのDNSトラフィックを確認するには、アクティビティ検索レポートをチェックします。

診断の解釈

Umbrella ローミング セキュリティ モジュールの問題を診断するには、DART レポートを実行する必要があります。Umbrellaの問題とトラブルシューティングの詳細については、https://docs.umbrella.com/umbrella-user-guide/docs/appendix-c-troubleshooting を参照してください。

Umbrella ローミング セキュリティ モジュール

Umbrellaローミング セキュリティ モジュールはDNSレイヤのセキュリティを提供しますが、AnyConnect Umbrella セキュア Web ゲートウェイ（SWG）エージェントモジュールはエンドポイントでのセキュリティレベルを提供し、より多くの展開シナリオで柔軟性と潜在能力が高まります。Umbrella セキュア Web ゲートウェイでは、オフプレミスとオンプレミスの両方のシナリオにおいて、Webトラフィックを安全に認証およびリダイレクトすることができます。この実装には、Umbrellaからの SIG Essentials または SIG アドオンサブスクリプションが必要です。

セキュア Web ゲートウェイクライアントは、暗号化されたヘッダーを HTTP 要求に挿入し、ヘッドエンドはそのヘッダーを抽出して復号化し、ユーザーデータを使用してアイデンティティおよびポリシーの決定と適用を行います。同様に、HTTPS トラフィックの場合、セキュア Web ゲートウェイクライアントは SWG ヘッドエンドで HTTP 接続要求を開始し、接続要求によって暗号化されたヘッダーが伝送されます。このヘッダーは抽出、復号化され、アイデンティティ/ポリシーの決定と適用に使用されます。

デフォルトでは、セキュア Web ゲートウェイはポート 80 および 443 で HTTP または HTTPS トラフィックを代行受信します。Umbrella クラウド設定では、非標準ポート（80 および 443 以外）を追加できます。これを設定すると、セキュア Web ゲートウェイはデフォルトの標準ポートに加えて、これらの追加ポートで HTTP/HTTPS トラフィックをリッスンします。

信頼ネットワーク検出では、ユーザーは信頼ネットワーク上でセキュア Web ゲートウェイを非アクティブ化することを選択できます。この設定が Umbrella クラウドで設定されている場合に、AnyConnect VPN トンネルの状態がアクティブである場合、信頼ネットワーク上ではセキュア Web ゲートウェイ機能は無効になります。[UI統計（UI Statistics）] ウィンドウに表示される [Web保護ステータス（Web Protection Status）] には、状態の変更が反映されます。

（注） この設定を構成すると、Umbrella の DNS 保護状態によって決定される特定のエラー（Umbrella リゾルバが到達不能な場合など）の場合にもセキュア Web ゲートウェイが非アクティブになります。

プロキシされてはならないドメインまたは IP アドレスは、[展開（Deployments）] > [ドメイン管理（Domain Management）] の下にある全てのダッシュボードで定義できます。ワイルドカードはサポートされていませんが、Umbrella は親ドメインに属するすべてのサブドメインと一致します。 たとえば、example.com がドメイン管理リストに入力された場合、www.example.com も一致し、バイパスされます。Classless Inter-Domain Routing（CIDR）表記法を使用して IP アドレスを入力します。現在、IPv4 アドレスのみがサポートされています。

AnyConnect が Umbrella プロキシへの接続を設立できない場合、AnyConnect はデフォルトで設立することに失敗し、ユーザーがダイレクトアクセスできるようになってしまいます。このハードコードされた動作は設定できません。

これらのすべての Umbrella UI 設定の詳細については、『Cisco Umbrella SIG User Guide』を参照してください。

セキュア Web ゲートウェイの制限事項

- AnyConnect がインストールされているローカルホストもプロキシ自動設定（PAC）ファイルで設定されているシナリオでは、PAC ファイルが AnyConnect よりも優先されます。
- 現在、IPv4 のみがサポートされています。
- ローカルプロキシはサポートされていません。
- インストール後、Umbrella セキュア Web ゲートウェイエージェントが Umbrella クラウドと同期し、その設定を受信するまでに最大で 50 分かかることがあります。ただし、デフォルトの Web ポリシーは、同期が発生するまで適用されます。

Umbrella SWG のインストールおよびアップグレード

AnyConnect Umbrella のセキュア Web ゲートウェイモジュールは、Windows または macOS でのみ使用でき、AnyConnect VPN を必要としません。ただし、AnyConnect VPN が AnyConnect Umbrella のセキュア Web ゲートウェイエージェントとともにインストールされている場合は、VPN プロファイルで *Allowlocalproxyconnections* 設定を有効にする必要があります。

Cisco Secure Firewall ASA または ISE 経由の事前展開と Web 展開の両方がサポートされています。

クラウドのアップグレードは Umbrella クラウド経由でサポートされています。

Umbrella SWG のログファイルとメッセージ

Umbrella ローミングクライアントは、SWGConfig.json ファイルの形式で AnyConnect に設定情報を送信します。SWGConfig.json のログファイルとメッセージは次の場所に保存されます。

- Windows：C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG
- macOS：/opt/cisco/anyconnect/umbrella/swg/

Umbrella ローミングセキュリティタイルのステータス

セキュア Web ゲートウェイの状態は [詳細統計（Advanced Statistics）] ウィンドウで確認できます。このウィンドウの Umbrella ローミング セキュリティ タイルでは、Web 保護ステータスが次のいずれかによって示されます。

- 無効（Disabled）：Umbrella サービスがダウンしています
- 保護済み（Protected）：acswgagent が実行中です。
- 未保護（Unprotected）：acswgagent が実行されていません。
- 設定エラー（Config Error）：SWGConfig.json の値が正しくありません。
- クラウドサービス利用不可（Cloud Service Unavailable）：Umbrella プロキシに到達できません。

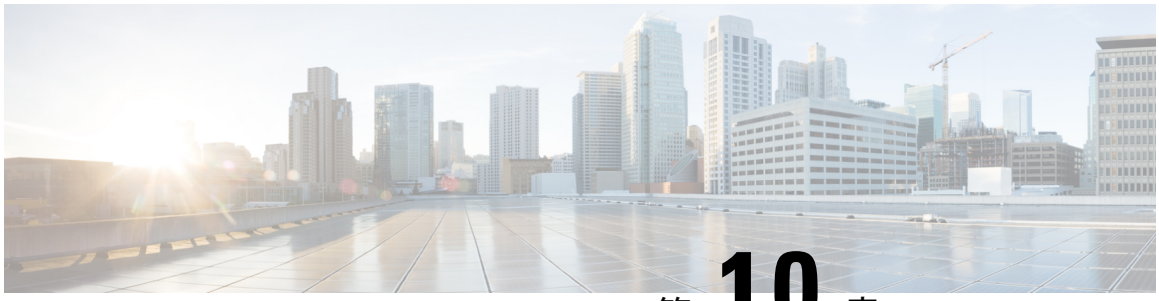
Umbrella セキュア Web ゲートウェイエージェントの詳細統計については、AnyConnect UI を開き、Umbrella ローミング セキュリティ ブランチに移動して、Umbrella プロキシにリダイレクトされた HTTP リクエストの数、Umbrella プロキシにリダイレクトされた HTTPS リクエストの数、プロキシへのリダイレクトに失敗したリクエストの数、および AnyConnect 接続先の Umbrella プロキシを表示することもできます。エラーおよび情報メッセージは、メッセージ履歴に記録されます。

Umbrella セキュア Web ゲートウェイのトラブルシューティング

DART バンドルを実行する際、[ログファイルの選択（Log File Selection）] ウィンドウで AnyConnect Umbrella ローミング セキュア モジュールをオンにしている場合は、SWGConfig.json および SWG 関連のログが追加されます。http://httpbin.org/ip に移動して、トラフィックが

Umbrellaプロキシに到達しているかどうかを確認します。接続のリセットが発生する場合は、HTTP 要求を送信して応答コードを確認してください。

- HTTP 応答コードが 452 の場合は、クライアントのクロックが同期されているかどうか、またはタイムスタンプに誤りがあるかどうかを確認します。悪意のあるユーザがヘッダーのリプレイを試みている可能性があります。
- HTTP 応答コードが 401 の場合は、キーは最新ではありません。Umbrella ダッシュボードでデバイスの最後の同期時刻を確認します。



第 10 章

ローカル ポリシーでの FIPS の有効化

FIPS、NGE、および AnyConnect について

AnyConnect には、Cisco Common Cryptographic Module（C3M）が組み込まれています。この Cisco SSL の実装には、新世代の暗号化（NGE）アルゴリズムの一部として、連邦情報処理標準（FIPS）140-2 に準拠した暗号化モジュールや国家安全保障局（NSA）Suite B 暗号化が含まれます。

Next Generation Encryption は、セキュリティおよびパフォーマンスの増大する要件に対応するために、暗号化、認証、デジタル署名、およびキー交換用の新しいアルゴリズムを導入しています。RFC 6379 では、Suite B 暗号化アルゴリズムが定義されています。これは、米国の FIPS 140-2 標準を満たす必要があります。

AnyConnect コンポーネントは、ヘッドエンド（Cisco Secure Firewall ASA または IOS ルータ）の設定に基づいて FIPS 標準暗号化をネゴシエートして使用します。次の AnyConnect クライアントモジュールは FIPS をサポートしています。

- AnyConnect VPN：VPN クライアントの FIPS 準拠は、ユーザーコンピュータ上のローカル ポリシーファイルの FIPS モードパラメータを使用して有効化されます。Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。詳細および手順については、「AnyConnect VPN のための FIPS の設定」を参照してください。

  AnyConnect ローカル ポリシー ファイル AnyConnectLocalPolicy.xml には、ローカル クライアントに適用される FIPS モードの他に追加のセキュリティ設定が含まれています。これは Cisco Secure Firewall ASA によって展開されないため、手動でインストールするか、社内のソフトウェア展開システムを使用して展開する必要があります。このプロファイルの使用方法については、「AnyConnect ローカルポリシー」を参照してください。

- AnyConnect Network Access Manager：Network Access Managerの FIPS 準拠は、AnyConnectLocalPolicy.xml ファイルの FIPS モードパラメータ、およびNetwork Access Manager プロファイルの FIPS モードパラメータを使用して有効にします。Network Access

ManagerのためのFIPSはWindowsでサポートされています。詳細および手順については、「Network Access Manager のための FIPS の設定」を参照してください。

AnyConnect の FIPS 機能

機能	コア VPN モジュール	Network Access Manager モジュール
対称暗号化や完全性のための AES-GCM サポート。	IKEv2 ペイロード暗号化と認証用の 128、192、256 ビットの各キー。 ESP パケット暗号化および認証。	ソフトウェア（Windows）で有線トラフィック暗号化を実現する 802.1AE（MACsec）用 128 ビット キー。
ハッシュ用 SHA-2 サポート、256/384/512 ビットの SHA。	IKEv2 ペイロード認証および ESP パケット認証。（Windows 7 以降および macOS 10.7 以降）。	TLS ベースの EAP 方式で SHA-2 を使用して証明書を使用できる機能。
キー交換向けの ECDH サポート。	グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS。	TLS ベースの EAP 方式で ECDH を使用できる機能（Windows）。
デジタル署名、非対称暗号化、および認証の ECDSA サポート、256、384、521 ビット楕円曲線。	IKEv2 ユーザ認証およびサーバ証明書の確認。	TLS ベースの EAP 方式で ECDSA を使用して証明書を使用できる機能。
その他のサポート。	IPsecV3 に必要なすべての暗号アルゴリズム（ヌル暗号化を除く）。 TLS/DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書。	該当なし

[1] Linux では、AnyConnect ファイルストアのみが ECDSA でサポートされます。ファイルストアに証明書を追加するには、「macOS および Linux での PEM 証明書ストアの作成」を参照してください。

[2] IPsecV3 は、ESN（Extended Sequence Numbers）がサポートされなければならないことも明記していますが、AnyConnect は ESN をサポートしません。

AnyConnect の FIPS 要件

- Suite B 暗号化は、TLS/DTLS および IKEv2/IPsec VPN 接続で使用可能です。

- FIPS または Suite B のサポートは、セキュア ゲートウェイで必要です。シスコは、Cisco Secure Firewall ASA バージョン 9.0 以降では Suite B 機能、Cisco Secure Firewall ASA バージョン 8.4.1 以降では FIPS 機能を提供します。
- ECDSA 証明書の要件は次のとおりです。
  - カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
  - Windows 7 以降、macOS 10.7 以降、Red Hat Enterprise Linux 6.x または 6.4（64 ビット）以降、Ubuntu 12.4 および 12.10（64 ビット）以降でサポートされています。ECDSA スマート カードは、Windows 7 （およびそれ以降のバージョン）でのみサポートされています。

AnyConnect FIPS の制限事項

SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。

AnyConnect FIPS のガイドライン

- AnyConnect の [統計情報（Statistics）] パネル（[トランスポート情報（Transport Information）] ヘッダーの下）には、使用中の暗号名が表示されます。
- AES-GCM は、計算集約型のアルゴリズムであるため、これらのアルゴリズムを使用するときは、全体的なデータ レートが低くなる可能性があります。一部の新しい Intel プロセッサには、AES-GCM のパフォーマンスを向上させるために導入された特別な命令が含まれています。実行中のプロセッサがこれらの新しい命令をサポートしているかどうかは、AnyConnect によって自動的に検出されます。サポートされている場合は、AnyConnect は新しい命令を使用し、特別な命令を持たないプロセッサと比較して VPN データレートを大幅に向上させます。新しい命令をサポートするプロセッサのリストについては、http://ark.intel.com/Search/FeatureFilter?productType=processors&AESTech=true を参照してください。詳細については、http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/ を参照してください。
- 暗号化と整合性の検証の両方が 1 回の操作で実行される複合モードの暗号化アルゴリズムは、ハードウェア クリプト アクセラレーションを使用する SMP ASA ゲートウェイ（5585 および 5515-X など）でのみサポートされます。AES-GCM は、シスコがサポートする複合モードの暗号化アルゴリズムです。

（注） IKEv2 ポリシーは、通常モードまたは複合モードの暗号化アルゴリズムのうちの 1 つを含めることができますが、両方は不可能です。複合モードのアルゴリズムが IKEv2 ポリシーで設定されると、通常モードのアルゴリズムすべてが無効になるので、唯一有効な整合性アルゴリズムは NULL です。

IKEv2 IPsec プロポーザルは別のモデルを使用し、同じプロポーザル内で標準モードと複合モードの両方の暗号化アルゴリズムを指定できます。この使用方法では、両方に整合性アルゴリズムを設定する必要があります。その結果、非 NULL 整合性アルゴリズムが AES-GCM 暗号化で設定されます。

- Cisco Secure Firewall ASA が SSL および IPsec 用の異なるサーバー証明書で設定されている場合は、信頼できる証明書を使用してください。異なる IPsec および SSL 証明書を持つ Suite B（ECDSA）の信用されていない証明書を使用する場合、ポスチャ評価またはダウンローダーの障害が発生する可能性があります。

AnyConnect FIPS のレジストリ変更によるエンドポイントに関する問題の回避

AnyConnect VPN の FIPS を有効にすると、エンドポイントで Windows レジストリの設定が変更されます。エンドポイントの他のコンポーネントでは、AnyConnect VPN が FIPS を有効にしたこと、および暗号化の使用を開始したことを検出できます。たとえば、Remote Desktop Protocol（RDP）では、サーバで FIPS 準拠の暗号化を使用している必要があるため、Microsoft Terminal Services クライアントの RDP は機能しません。

これらの問題を回避するために、パラメータ [Use FIPs compliant algorithms for encryption, hashing, and signing] を [Disabled] に変更することにより、[Windows Local System Cryptography] 設定で FIPS 暗号化を一時的に無効にできます。エンドポイント デバイスをリブートすると、この設定が変更されて有効に戻ることに注意してください。

AnyConnect VPN は、Windows レジストリキー HKLM\System\CurrentControlSet\ Control\Lsa の FIPSAlgorithmPolicy 値を 1 に設定します。AnyConnect ローカルポリシーファイルで FIPS モードを無効にしても、AnyConnect VPN が FIPSAlgorithmPolicy 値を変更することはありません。

AnyConnect VPN のための FIPS の設定

AnyConnect VPN のための FIPS の有効化

手順

ステップ 1 AnyConnect プロファイルエディタで、VPN ローカル ポリシープロファイルを開くか、作成します。

ステップ 2 [FIPS モード（FIPS Mode）] を選択します。

ステップ 3 VPN ローカル ポリシー プロファイルを保存します。

FIPS が有効であることを示す名前をプロファイルに付けることをお勧めします。

Windows インストール時の FIPS の有効化

Windows インストールでは、Cisco MST ファイルを標準 MSI インストール ファイルに適用して、AnyConnect ローカル ポリシーで FIPS を有効にできます。この MST のダウンロード元の詳細については、FIPS 用に受け取ったライセンシング情報を参照してください。インストール時に、FIPS が有効にされた AnyConnect ローカル ポリシー ファイルが生成されます。このユーティリティを実行した後、ユーザのシステムを更新します。

（注） この MST は FIPS だけを有効にします。その他のパラメータは変更しません。Windows インストール中に他のローカル ポリシーの設定を変更するには、「MST ファイルでのローカル ポリシー パラメータの有効化」を参照してください。

Network Access Manager のための FIPS の設定

Network Access Managerは、FIPS ネットワークと非 FIPS ネットワークの両方に同時に接続したり、FIPS ネットワークだけに接続したりするように設定できます。

手順

ステップ 1 Network Access Manager のための FIPS の有効化。

FIPS を有効にすると、Network Access Managerは FIPS ネットワークと非 FIPS ネットワークの両方に接続できます。

ステップ 2 必要に応じて、Network Access Manager に対する FIPS モードの適用。

FIPS モードを適用すると、Network Access Managerの接続が FIPS ネットワークだけに制限されます。

Network Access Manager のための FIPS の有効化

手順

AnyConnect Network Access Manager クライアント プロファイルで FIPS モードを有効にします。

a) AnyConnect プロファイルエディタで、Network Access Manager プロファイルを開くか、作成します。
b) [クライアント ポリシー（Client Policy）] 設定ウィンドウを選択します。
c) [管理ステータス（Administrative Status）] セクションで、[FIPSモード（FIPS Mode）] に [有効（Enable）] を選択します。
d) Network Access Manager プロファイルを configuration.xml として保存します。

Network Access Manager に対する FIPS モードの適用

Network Access Manager プロファイルで、許可する関連付け、暗号化モード、認証方式を制限することにより、企業の従業員に対して FIPS 準拠のネットワークのみへの接続を強制します。

まず、Network Access Manager のための FIPS の有効化を行い、FIPS モードを適用します。

手順

ステップ 1 AnyConnect プロファイルエディタでNetwork Access Manager プロファイルを開きます。

ステップ 2 Network Access Managerの FIPS 準拠では、WPA2 パーソナル（WPA2-PSK）、WPA2 エンタープライズ（802.1X）などの FIPS 認定の AES 暗号化モードをサポートしています。

ステップ 3 Network Access Managerの FIPS サポートには、EAP 方式 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST、および LEAP が含まれています。

ステップ 4 Network Access Manager プロファイルを configuration.xml として保存します。

第 11 章

モバイルデバイスの AnyConnect

モバイルデバイスの AnyConnect は、Windows、macOS、および Linux プラットフォームの AnyConnect に似ています。この章では、モバイルデバイスでの AnyConnect に固有のデバイス情報、設定情報、サポート情報、およびその他の管理タスクについて説明します。

モバイルデバイスでの AnyConnect の動作およびオプション

AnyConnect Mobile VPN 接続について

このリリースの AnyConnect Secure Mobility Client は、次のモバイルプラットフォームに対応しています。

- Android
- Apple iOS
- Chromebook
- Windows Phone

AnyConnect Secure Mobility Client は、サポートされている各プラットフォームのアプリストアに用意されています。www.cisco.com では入手できません。また、セキュリティで保護されたゲートウェイから配布されていません。

AnyConnect モバイルアプリには、コア VPN クライアントのみが含まれています。Network Access Manager、ポスチャ（VPN ポスチャ または システムスキャン）などの他の AnyConnect モジュールは含まれていません。VPN が接続中の場合は、モバイル ポスチャと呼ばれるポスチャ情報が、AnyConnect Identify Extensions（ACIDex）を使用してヘッドエンドに提供されます。

AnyConnect VPN 接続は、次のいずれかの方法で確立できます。

- ユーザが手動で確立する。
- ユーザが管理者により提供された自動接続アクションをクリックする際に手動で確立する（Android および Apple iOS のみ）。
- 自動：Connect on-Demand 機能により確立される（Apple iOS のみ）。

モバイルデバイスでの AnyConnect VPN 接続エントリ

接続エントリは、セキュア ゲートウェイのアドレスを完全修飾ドメイン名または IP アドレス（必要に応じてトンネル グループ URL を含む）で識別します。また、他の接続属性を含めることもできます。

AnyConnect では、1 台のモバイルデバイス上の複数の接続エントリをサポートすることで、異なるセキュア ゲートウェイや VPN トンネルグループに対応します。複数の接続エントリが設定されている場合は、VPN 接続を開始するためにユーザがどれを使用するかを理解することが重要です。接続エントリは次の方法のいずれかで設定されます。

- ユーザが手動で設定します。モバイル デバイスの接続エントリを設定する手順については、該当するプラットフォームのユーザ ガイドを参照してください。
- ユーザが管理者により提供されたリンクをクリックした後で追加し、接続エントリを設定します。

  ユーザにこの種の接続エントリ設定を提供するには、「VPN 接続エントリの生成 （346 ページ）」を参照してください。
- AnyConnect VPN クライアントプロファイルで定義されます。

  AnyConnect VPN クライアントプロファイルでは、クライアント動作を指定し、VPN 接続エントリを定義します。詳細については、「AnyConnect VPN プロファイルでのモバイル デバイス接続の設定 （344 ページ）」を参照してください。

トンネリング モード

AnyConnect は、マネージド BYOD またはアンマネージド BYOD 環境で動作可能です。これらの環境での VPN トンネリングは、次のいずれかのモードでのみ動作します。

- システム トンネリング モード：VPN 接続が、すべてのデータをトンネリングするために（完全トンネリング）、または特定のドメインまたはアドレスとの間で送受信されるデータのみをトンネリングするために（スプリット トンネリング）使用されます。このモードは、すべてのモバイル プラットフォームで使用できます。
- アプリケーションごとの VPN モード：VPN 接続は、モバイルデバイス（Android と Apple iOS のみ）上の特定のアプリケーションセットで使用されます。

  AnyConnect では、管理者によってヘッドエンドで定義されているアプリケーションのセットを使用できます。このリストを定義するには、Cisco Secure Firewall ASA のカスタム属性のメカニズムを使用します。このリストは AnyConnect に送信され、デバイスで適用されます。他のすべてのアプリケーションに対しては、データはトンネルを介さずに、または暗号化されずに送信されます。

  Apple iOS でこのモードで実行するには、マネージド環境が必要です。Android では、マネージドとアンマネージドの両方の環境がサポートされます。いずれのプラットフォームでも、マネージド環境では、AnyConnect でトンネリングするように設定されている一連のアプリケーションと同じアプリケーションをトンネリングするように Mobile Device Manager でデバイスを設定する必要があります。
- マルチトンネル：iOS 上の AnyConnect は、次のパターンを使用して複数のトンネルをサポートします。
  - 1 つの通常の（アプリケーションごとではない）VPN トンネルと、一度に接続された 1 つ以上のアプリケーションごとのトンネル
  - 一度に接続されたアプリケーションごとの VPN トンネルの数

  追加情報については、「iOS 向けの複数のトンネル（309 ページ）」を参照してください。

AnyConnect Cisco Secure Firewall ASA ヘッドエンドから受信した設定情報によって決定されるモードで動作します。具体的には、接続に関連付けられたグループポリシーまたはダイナミック アクセス ポリシー（DAP）内のアプリごとの VPN リストの有無です。アプリケーション単位 VPN のリストが存在する場合、AnyConnect はアプリケーション単位 VPN モードで動作し、存在しない場合は AnyConnect はシステム トンネリング モードで動作します。

iOS 向けの複数のトンネル

ユーザーは、1 つのトンネルに対して 1 つの VPN 接続しか手動で開始できません（アプリケーションごとの VPN を使用する、または使用しない、いずれの場合も）。アプリケーションごとの VPN は関連付けられたアプリケーションで自動的に開始されるため、マルチトンネルを使用するには、MDM VPN プロファイルの VendorConfig に **MultiTunnel** キーを追加し、それを **true** に設定する必要があります。

iOS AnyConnect のホーム画面には、接続されているかどうかに関係なく、選択したトンネルを示す表が表示されます。2 番目の表はダイナミックで、アプリケーションごとの VPN が接続されている場合にのみ表示されます。この 2 番目の表には、ユーザが [ステータス（Status）] をクリックして、送受信されたバイト数とともに接続の [詳細な統計情報（Detailed Statistics）] を表示するまで、アプリケーションごとのトンネルの接続ステータスのみが表示されます。

現在選択されている通常の VPN のログの [診断（Diagnostics）] を参照できます。ユーザがログを共有することを決定した場合、ログパッケージには、接続されている VPN 設定のすべての VPN デバッグログファイルが含まれます。

モバイル デバイスでのセキュア ゲートウェイ認証

信頼されていないサーバのブロック

VPN 接続を確立するときに、AnyConnect はセキュアゲートウェイから受信したデジタル証明書を使用してサーバーの身元を確認します。サーバ証明書が無効な場合（期限切れか無効な日付、キーの誤用、名前の不一致により証明書エラーがある）、または信頼できない場合（認証局が確認できない）場合、接続はブロックされます。ブロッキングメッセージが表示されるため、ユーザーは処理を選択する必要があります。

[信頼されていないサーバーをブロック（Block Untrusted Servers）] アプリケーション設定は、セキュア ゲートウェイを識別できない場合、AnyConnect がどのように反応するかを決定します。この保護はデフォルトではオンです。ユーザーはオフにできますが、これは推奨されません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオンの場合、信頼できない VPN サーバをブロックするという通知によって、ユーザーにセキュリティ上の脅威が警告されます。ユーザーは以下を選択できます。

- [安全を確保（Keep Me Safe）] を選択して、この接続を終わらせ、安全にしておきます。
- [設定の変更（Change Settings）] を選択して、[信頼されていないサーバをブロック（Block Untrusted Servers）] アプリケーション プリファレンスをオフにします。ただし、これは推奨されません。ユーザーがこのセキュリティ保護を無効にすると、VPN 接続を再起動しなくてはなりません。

[信頼されていないサーバをブロック（Block Untrusted Servers）] がオフの場合、信頼できない VPN サーバをブロックしないという通知によって、ユーザーにセキュリティ上の脅威が警告されます。ユーザーは以下を選択できます。

- [キャンセル（Cancel）] を選択して、接続をキャンセルし、安全にしておきます。
- [続行（Continue）] を選択して、接続を続行します。ただし、これは推奨されません。
- [詳細の表示（View Details）] を選択して、証明書の詳細を表示して受け入れるかどうかを判断します。

  ユーザーが確認している証明書が有効であるが信頼できない場合、ユーザーは次のことを実行できます。

  - 再使用できるようにサーバー証明書を AnyConnect 証明書ストアにインポートし、[インポートおよび継続（Import and Continue）] を選択して接続を継続します。

    AnyConnect ストアにこの証明書がインポートされると、このデジタル証明書を使用しているそのサーバーに対する後続の接続は自動的に受け入れられます。

- 前の画面に戻り、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

証明書が無効な場合、または何らかの理由で、ユーザーが前の画面にだけ戻ることができる場合、[キャンセル（Cancel）] または [続行（Continue）] を選択します。

VPN 接続の最も安全な設定では、[信頼されていないサーバーをブロック（Block Untrusted Servers）] の設定をオン（デフォルト設定）のままにし、自身のセキュアゲートウェイで設定された（有効で信頼できる）サーバー証明書を所有し、モバイルユーザーには常に [安全を確保（Keep Me Safe）] を選択させる必要があります。

（注） [厳格な証明書トラスト（Strict Certificate Trust）] はこの設定を上書きします（以下の説明を参照）。

OCSP 失効

AnyConnect は OCSP（オンライン証明書状態プロトコル）をサポートします。これにより、OCSP レスポンダに要求を行い OCSP 応答を解析して証明書のステータスを取得することで、クライアントはリアルタイムで個々の証明書のステータスを照会できます。OCSP は、証明書チェーン全体を確認するために使用されます。OCSP レスポンダにアクセスする際、証明書ごとに 5 秒のタイムアウト間隔があります。

ユーザーは AnyConnect 設定アクティビティで OCSP 検証を有効または無効にすることができます。MDM 管理者がリモートでこの機能を制御するために使用できる新しい API がフレームワークに追加されました。現在、Samsung と Google MDM がサポートされています。

厳格な証明書トラスト

ユーザーによって有効にされた場合、リモートセキュリティゲートウェイの認証時に AnyConnect は確認できない証明書を許可しません。これらの証明書を受け入れるようユーザーにプロンプトを表示するのではなく、クライアントはセキュリティゲートウェイへの接続に失敗します。

（注） この設定は、[信頼されていないサーバをブロック（Block Untrusted Servers）] よりも優先されます。

オフにすると、クライアントはユーザーに証明書を受け入れるように求めます。これはデフォルトの動作です。

以下の理由があるため、AnyConnect の厳格な証明書トラストを有効にすることを、強くお勧めします。

- 明確な悪意を持った攻撃が増えているため、ローカルポリシーで厳格な証明書トラストを有効にすると、パブリック アクセス ネットワークなどの非信頼ネットワークからユーザーが接続している場合に「中間者」攻撃を防ぐために役立ちます。

- 完全に検証可能で信頼できる証明書を使用する場合でも、AnyConnect は、デフォルトでは、未検証の証明書の受け入れをエンドユーザーに許可します。エンドユーザーが中間者攻撃の対象になった場合は、悪意のある証明書を受け入れるようエンドユーザーに求めます。エンドユーザーによるこの判断を回避するには、厳格な証明書トラストを有効にします。

モバイル デバイスでのクライアント認証

VPN接続を完了するには、ユーザはユーザ名とパスワード、もしくはデジタル証明書、またはその両方の形式でクレデンシャルを提供して認証する必要があります。管理者は、トンネルグループの認証方式を定義します。モバイルデバイスでの最適なユーザーエクスペリエンスを達成するために、認証設定に応じて複数の AnyConnect 接続プロファイルを使用することをお勧めします。ユーザエクスペリエンスとセキュリティのバランスを最適に保つ方法を決める必要があります。推奨事項は次のとおりです。

- モバイルデバイスの AAA 対応認証トンネル グループについては、クライアントを再接続状態にし、ユーザが再認証しなくても済むよう、グループ ポリシーは 24 時間など非常に長時間のアイドル タイムアウトが必要になります。
- 最もトランスペアレントなユーザエクスペリエンスを達成するには、証明書のみの認証を使用します。デジタル証明書を使用すると、VPN接続は、ユーザとの対話なしで確立されます。

証明書を使用してセキュア ゲートウェイにモバイル デバイスを認証するため、エンド ユーザは、デバイスに証明書をインポートする必要があります。インポートすると、この証明書が自動証明書選択の対象として有効になり、特定の接続エントリに手動で関連付けることもできるようになります。証明書は、次の方法を使用してインポートされます。

- ユーザが手動でインポートします。モバイルデバイスに証明書をインポートする手順については、適切なユーザ ガイドを参照してください。
- SCEP を使用します。詳細については、「証明書登録の設定 （184 ページ）」を参照してください。
- 証明書をインポートするために管理者により提供されたリンクをユーザがクリックした後に追加されます。

  ユーザにこの種の証明書展開を提供するための詳細については、「証明書のインポート（353 ページ）」を参照してください。

モバイル デバイスでのローカリゼーション

Android および Apple iOS 用 AnyConnect Secure Mobility Client は、ローカリゼーションをサポートし、AnyConnect Secure Mobility Client ユーザーインターフェイスやメッセージをユーザーのロケールに適用しています。

パッケージ済みのローカリゼーション

AnyConnect Secure Mobility Client Android および Apple iOS アプリには、次の言語訳が含まれます。

- カナダ フランス語（fr-ca）
- 中国語（台湾）（zh-tw）
- チェコ語（cs-cz）
- オランダ語（nl-nl）
- フランス語（fr-fr）
- ドイツ語（de-de）
- ハンガリー語（hu-hu）
- イタリア語（it-it）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- 中南米スペイン語（es-co）
- ポーランド語（pl-pl）
- ポルトガル語（ブラジル）（pt-br）
- ロシア語（ru-ru）
- 簡体字中国語（zh-cn）
- スペイン語（es-es）

AnyConnect Secure Mobility Client のインストール時には、これらの言語のローカリゼーションデータがモバイルデバイスにインストールされます。モバイルデバイスで指定された地域によって、表示される言語が決まります。AnyConnect は、言語仕様、次に地域仕様を使用して、最適な一致を決定します。たとえば、インストール後にロケール設定をスイス フランス語（fr-ch）にすると、カナダ フランス語（fr-ca）表示になります。AnyConnect の UI とメッセージは、AnyConnect の起動時に変換されます。

ダウンロードされたローカリゼーション

AnyConnect パッケージにはない言語に関して、管理者は、AnyConnect VPN 接続のデバイスにダウンロードされるローカライズデータを Cisco Secure Firewall ASA に追加します。

シスコは、Cisco.com の製品ダウンロードセンターで、ローカライズ可能なすべての AnyConnect の文字列を含む anyconnect.po ファイルを提供しています。 AnyConnect の管理者は anyconnect.po ファイルをダウンロードし、利用可能な文字列の翻訳を提供してから、ファイルを Secure Firewall ASA にアップロードします。Cisco Secure Firewall ASA に anyconnect.po ファイルがす

でにインストールされている場合、AnyConnect の管理者は更新バージョンをダウンロードします。

初期状態では、AnyConnect ユーザーインターフェイスおよびメッセージがインストールした言語でユーザーに表示されます。デバイスユーザーが Cisco Secure Firewall ASA への初めての接続を確立すると、AnyConnect では、デバイスの優先言語と Cisco Secure Firewall ASA 上で使用可能なローカリゼーション言語が比較されます。AnyConnect で一致するローカリゼーションファイルが検索されると、ローカライズされたファイルがダウンロードされます。ダウンロードが完了すると、AnyConnect は anyconnect.po ファイルに追加された変換文字列を使用してユーザーインターフェイスおよびユーザーメッセージを表示します。文字列が翻訳されていない場合、AnyConnect ではデフォルトの英語文字列が表示されます。

Cisco Secure Firewall ASA でのローカリゼーションの設定手順については、「Cisco Secure Firewall ASA への変換テーブルのインポート （63 ページ）」を参照してください。Cisco Secure Firewall ASA にデバイスのロケールのローカリゼーションデータが含まれていない場合、AnyConnect アプリケーションパッケージにプリインストールされたローカリゼーションデータを引き続き使用します。

モバイル デバイスにローカリゼーションを提供するその他の方法

ユーザに URI リンクを提供することにより、AnyConnect UI とメッセージのローカライズ （354 ページ）を実行します。

モバイル デバイスのユーザに、所有するデバイスでのローカリゼーション データの管理を依頼します。次のローカリゼーション アクティビティを実行する手順については、該当するユーザ ガイドを参照してください。

- 指定したサーバからのローカリゼーションデータのインポート。ユーザは、ローカリゼーション データのインポートを選択し、セキュア ゲートウェイのアドレスとロケールを指定します。ロケールは ISO 639-1 で指定されており、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。このローカリゼーション データは、インストールされたローカリゼーション データの代わりに使用されます。
- デフォルトのローカリゼーションデータのリストア。AnyConnect パッケージから事前ロードされたローカリゼーションデータの使用を復元し、インポートされたローカリゼーションデータをすべて削除します。

SAML を使用した VPN 認証

以下のリリースで、SAML 2.0 のサポートがモバイルデバイスに追加されました。SAML 認証を使用した場合、AnyConnect セッションのみに適用されます。Web サイト、ブラウザが開始した SAML ログイン、またはインストールされているアプリケーションには適用されません。中断のないシームレスな再接続を提供するために、AnyConnect は意図的に SAML 認証プロセスの繰り返しをスキップします。さらに、ユーザーがブラウザを使用して IdP からログアウトしても、AnyConnect セッションは維持されます。

- iOS：バージョン 4.6。バージョン 4.8 では SAML とクライアント証明書
- Android：バージョン 4.6。バージョン 4.8 では SAML とクライアント証明書

- Chrome：バージョン 4.0

SAML を使用する場合は、次の注意事項に従ってください。

- フェールオーバーモードで常時接続の VPN を使用している場合、外部 SAML IdP はサポートされていません（ただし、内部 SAML IdP を使用すると、Cisco Secure Firewall ASA はすべてのトラフィックを IdP にプロキシします。また、ASA はサポートされています）。
- 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
- 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は AnyConnect と共有されず、その逆も同じです。
- 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、AnyConnect では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに AnyConnect がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
- SAML 機能を使用するためには、Secure Firewall ASA の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。
- ASDM の VPN ウィザードは現在、SAML 設定をサポートしていません。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、AnyConnect プロファイルエディタ、プリファレンス（Part 1） （93 ページ）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の AnyConnect は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッションクッキーを使用してログオン状態を追跡している場合には、毎回ユーザーの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] [シングルサインオンサーバー（Single Sign On Servers）]** の [強制再認証（Force Re-Authentication）] は、AnyConnect が開始した SAML 認証には影響しません。

設定の詳細については、適切なリリース（9.7 以降）の『Cisco ASA Series VPN CLI or ASDM Configuration Guide』の「SAML 2.0」の項を参照してください。

Cisco Secure Firewall ASA への変換テーブルのインポート

手順

ステップ 1 www.cisco.com から目的の変換テーブルをダウンロードします。

ステップ 2 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）] > [AnyConnect カスタマイゼーション/ローカリゼーション（AnyConnect Customization/Localization）] > [GUI テキストおよびメッセージ（GUI Text and Messages）]** に移動します。

ステップ 3 [インポート（Import）] をクリックします。[言語ローカリゼーション エントリのインポート（Import Language Localization Entry）] ウィンドウが表示されます。

ステップ 4 ドロップダウン リストから適切な言語を選択します。

ステップ 5 変換テーブルのインポート元を指定します。

ステップ 6 [今すぐインポート（Import Now）] をクリックします。この変換テーブルが、この優先言語で AnyConnect クライアントに展開されます。ローカリゼーションは、AnyConnect がリスタートし、再接続した後に適用されます。

モバイル デバイスでの FIPS および Suite B 暗号化

モバイルデバイス向け AnyConnect には、Cisco Common Cryptographic Module（C3M）が組み込まれています。これは、新世代の暗号化（NGE）アルゴリズムの一部として FIPS 140-2 に準拠した暗号化モジュールや NSA Suite B 暗号化が含まれる Cisco SSL の実装です。Suite-B 暗号化は、IPSec VPN でのみ使用可能です。FIPS 準拠の暗号化は、IPSec VPN および SSL VPN の両方で使用可能です。

暗号化アルゴリズムを使用すると、接続の間、ヘッドエンドルータとネゴシエートされます。ネゴシエーションは、VPN 接続の両端の機能によって異なります。したがって、セキュア ゲートウェイは、FIPS に準拠する暗号化および Suite B の暗号化をサポートする必要があります。

ユーザーは、AnyConnect アプリケーション設定の **FIPS モード**を有効にすることで、ネゴシエーションにおいて NGE アルゴリズムだけを受け入れるように AnyConnect を設定します。FIPS モードが無効の場合、AnyConnect は VPN 接続の非 FIPS 暗号アルゴリズムも受け入れます。

モバイルのその他のガイドラインと制限事項

- Apple iOS 5.0 以降が Suite B の暗号化に必要です。これは Suite B で使用される ECDSA の証明書をサポートする Apple iOS の最も低いバージョンです。
- Android 4.0（Ice Cream Sandwich）以降が Suite B の暗号化に必要です。これは、SuiteB で使用される ECDSA の証明書をサポートする Android の最も低いバージョンです。

- FIPS モードで動作しているデバイスには、プロキシ方式または従来の方法でデジタル証明書をモバイルユーザに提供するための SCEP の使用との互換性がありません。状況に応じた展開計画を立ててください。

Android デバイスでの AnyConnect

リリースごとの機能および更新については、『Release Notes for AnyConnect Secure Mobility Client, for Android』[英語]を参照してください。

このリリースでサポートされている機能およびデバイスについては、『AnyConnect Secure Mobility Client Mobile Platforms and Feature Guide』[英語] を参照してください。

Android での AnyConnect の注意事項と制約事項

- Cisco Secure Firewall ASA は、Android 向け AnyConnect のディストリビューションと更新プログラムを提供しません。Google Play から入手できます。最新バージョンの APK（パッケージ）ファイルも Cisco.com に掲載されています。
- Android 向け AnyConnect は Network Visibility Module と Umbrella のみサポートし、他の AnyConnect モジュールはサポートしていません。
- Android デバイスでは 1 つの AnyConnect プロファイル（ヘッドエンドから受信した最後のプロファイル）だけがサポートされます。ただし、プロファイルは複数の接続エントリで構成できます。
- ユーザーが、サポートされていないデバイスに AnyConnect をインストールしようとすると、「インストールエラー：原因不明 -8（Installation Error: Unknown reason -8）」というポップアップメッセージが表示されます。これは Android OS により生成されるメッセージです。
- ユーザーがホームスクリーンに AnyConnect ウィジェットを表示している場合、[起動時に開く（Launch at startup）] 設定に関わらず AnyConnect サービスが自動的に開始されます（ただし接続は確立されません）。
- Android 向け AnyConnect では、クライアント証明書からの事前入力を使用する場合に、拡張 ASCII 文字のために UTF-8 文字エンコードが必要です。事前入力機能を使用する場合は、クライアント証明書が UTF-8 でなければなりません（KB-890772 および KB-888180 の説明を参照）。
- AnyConnect は、EDGE の固有の性質およびその他の早期無線テクノロジーによって EDGE 接続上の VPN トラフィックを送受信する場合、ボイスコールをブロックします。
- いくつかのよく知られているファイル圧縮ユーティリティでは、[AnyConnect 送信ログ（AnyConnect Send Log）] ボタンを使用してパッケージされたログバンドルを圧縮解除できません。回避策として、AnyConnect ログファイルの圧縮解除には Windows および macOS のネイティブユーティリティを使用してください。

- DHE の非互換性：AnyConnect で導入された DHE 暗号サポートにより、ASA 9.2 より前の Cisco Secure Firewall ASA バージョンで非互換性の問題が発生します。9.2 より前の Cisco Secure Firewall ASA リリースで DHE 暗号を使用している場合、これらの Cisco Secure Firewall ASA バージョンで DHE 暗号を無効にする必要があります。

Android 固有の考慮事項

Android モバイル ポスチャ デバイスの ID 生成

新規インストール時、またはユーザーがアプリケーションデータを消去した後、AnyConnect は Android ID に基づいて 256 バイトの一意のデバイス ID を生成します。この ID は、以前のリリースで生成された IMEI と MAC アドレスに基づく 40 バイトのレガシー デバイス ID を置き換えます。

AnyConnect の以前のバージョンがインストールされている場合、レガシー ID はすでに生成されています。AnyConnect のこのバージョンにアップグレードすると、ユーザーがアプリケーションデータを消去するか AnyConnect をアンインストールするまで、このレガシー ID は引き続きデバイスの固有 ID として報告されます。

生成されたデバイス ID は、アプリケーションの初回起動時に、AnyConnect の **[診断（Diagnostics）] > [ログインとシステム情報（Logging and System Information）] > [システム（System）] > [デバイス識別子（Device Identifiers）]** 画面、`device_identifiers.txt` ファイルの AnyConnect ログ、または [バージョン情報（About）] 画面から参照できます。

（注） セキュア ゲートウェイ上の DAP ポリシーは、新しいデバイス ID を使用するように更新する必要があります。

`Device-ID` は、次のように決定されます。

```
Device-ID = bytesToHexString(SHA256(Android-ID))
```

ここで、`Android ID` と `bytesToHexString` は次のように定義されます。

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] sha256rawbytes){
String hashHex = null;
if (sha256rawbytes != null){
  StringBuffer sb = new StringBuffer(sha256rawbytes.length * 2);
    for (int i = 0; i < sha256rawbytes.length; i++){
    String s = Integer.toHexString(0xFF & sha256rawbytes[i]).toUpperCase();
    if (s.length() < 2) {sb.append("0");}
    sb.append(s);
    }
  hashHex = sb.toString();
  }
return hashHex; }
```

Android デバイスのアクセス許可

次のアクセス許可が AnyConnect の動作用に Android マニフェスト ファイルで宣言されます。

マニフェストのアクセス許可	説明
uses-permission: android.permission.ACCESS_NETWORK_STATE	アプリケーションがネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.ACCESS_WIFI_STATE	アプリケーションが Wi-Fi ネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.BROADCAST_STICKY	アプリケーションがスティッキ インテントをブロードキャストすることを許可します。これは、クライアントが次のブロードキャストを待たなくてもデータをすぐに取得できるよう、完了後もデータがシステムによって保持されるブロードキャストです。
uses-permission: android.permission.INTERNET	アプリケーションがネットワーク ソケットを開くことを許可します。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	アプリケーションが外部ストレージから読み取ることを許可します。
uses-permission: android.permission.READ_LOGS	アプリケーションが低レベルのシステム ログ ファイルを読み取ることを許可します。
uses-permission: android.permission.READ_PHONE_STATE	デバイスの電話番号、現在の携帯電話ネットワーク情報、通話中のコールのステータス、デバイスに登録されているすべての PhoneAccounts のリストなどの電話状態への読み取り専用アクセスを許可します。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	システムの起動完了後にアプリケーションがブロードキャストを受信することを許可します。

Chromebook での Android 向け AnyConnect の設定

Google は最近、すべてのネイティブ Chromebook アプリケーションの廃止を発表しました。この手順は、ネイティブ Chromebook アプリケーションからの移行、および Chromebook での Android 向け AnyConnect の設定に役立ちます。

詳細については、この Google のマニュアルを参照してください。

手順

ステップ 1 管理者アカウントを使用して Google 管理コンソールにサインインします。

ステップ 2 Google 管理コンソールのホームページで、[Devices] > [Chrome] に移動します。

ステップ 3 [Apps & extensions] > [Users & browsers] をクリックします。

ステップ 4 設定を全員に適用する場合は、最上位の組織部門を選択したままにします。それ以外の場合は、子組織単位を適用します。

ステップ 5 [Add] > [Add from Google Play] をクリックします。

ステップ 6 管理するアプリケーションとして [AnyConnect] を選択します。

ステップ 7 管理対象の設定は JSON ファイルのみで、これを貼り付けるか、アップロードアイコンをクリックしてアップロードできます。

次のタスク

キーは、Android の .apk パッケージファイルで定義されます。唯一の必須フィールドは vpn_connection_host ですが、AnyConnect XML プロファイルをプッシュする場合、JSON キーは vpn_connection_profile です。AnyConnect は、次のセクションに示すすべての管理対象設定キーをサポートします。

AnyConnect でサポートされる管理対象設定キー

管理対象制限事項（ルート）

vpn_connection_name

- タイトル：接続名
- 型：String
- 説明：ユーザにわかりやすい名前（表示専用）。設定されていない場合は、デフォルトでホストになります。

vpn_connection_host

- タイトル：ホスト
- 型：string
- 説明：ヘッドエンドへの URL。このフィールドは必須です。

vpn_connection_profile

- タイトル：プロトコル
- 型：choice
- 設定可能な値：SSL | IPsec
- 説明：VPN トンネルプロトコル（SSL または IPsec）。デフォルトは SSL

vpn_connection_ipsec_auth_mode

- タイトル：IPsec 認証モード
- 型：choice

- 説明：（任意）トンネルプロトコルが IPsec の場合に使用する認証モード。デフォルトは EAP-AnyConnect

vpn_connection_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-Md5、または EAP-MSCHAPv2 の場合にのみ適用されます

vpn_connection_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-MD5、または EAP-MSCHAPv2 の場合にのみ適用されます。

vpn_connection_keychain_cert_alias

- タイトル：キーチェーン証明書エイリアス
- 型：string
- 説明：（任意）この VPN 設定に使用するクライアント証明書のキーチェーンエイリアス。

vpn_connection_allowed_apps

- タイトル：アプリケーションごとの VPN 許可アプリケーション
- 型：string
- 説明：（任意）トンネリングするアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされません。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_connection_disallowed_apps

- タイトル：アプリケーションごとの VPN で許可されないアプリケーション
- 型：string
- 説明：（任意）トンネリングしないアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとに VPN が有効になります。他のすべてのアプリケーションはトンネリングされます。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_connection_allow_bypass

- タイトル：VPN トンネルのバイパスをアプリケーションに許可する

- 型：bool
- 説明：（任意）この VPN 接続をバイパスすることをアプリに許可します。デフォルトでは無効になっています。

vpn_setting_replace_existing_profile

- タイトル：既存のプロファイルの置き換え
- 型：bool
- 説明：（任意）vpn_connection_profile が設定されている場合にのみ適用されます。クライアントにインストール済みのプロファイルを管理対象設定プロファイルで置き換えるかどうかを指定します。これを無効にすると、Cisco Secure Firewall ASA プッシュプロファイルとの競合を避けることができます。デフォルトでは有効になっています。

vpn_setting_apply_perapp_to_profile

- タイトル：アプリケーションごとのルールをプロファイルをインポートした構成に適用する
- 型：bool
- 説明：（任意）管理対象設定のアプリケーションごとの VPN ルール（存在する場合）を AnyConnect プロファイル XML からインポートした設定に適用するかどうかを指定します。デフォルトでは無効になっています。

vpn_connection_set_active

- タイトル：アクティブに設定
- 型：bool
- デフォルト値：True
- 説明：（任意）これが最後に選択された VPN 設定として設定されます。

vpn_setting_fips_mode

- タイトル：FIPS モード
- 型：bool
- 説明：（任意）AnyConnect の FIPS モードを有効にするかどうか。

vpn_setting_uri_external_control

- タイトル：URI 外部制御
- 型：string
- 説明：（任意）URI 処理（外部制御）を設定します。有効なオプションは、プロンプト、有効、および無効です。

vpn_setting_strict_mode

- タイトル：ストリクトモード
- 型：bool
- 説明：（任意）AnyConnect の厳格な証明書トラストモードを有効にするかどうか。

vpn_setting_certificate_revocation

- タイトル：証明書の失効
- 型：bool
- 説明：（任意）AnyConnect をチェックする OCSP サーバー証明書を有効にするかどうか。

vpn_connection_profile

- タイトル：AnyConnect プロファイル
- 型：string
- 説明：（任意）インポートのための AnyConnect プロファイル（XML 形式または XML の Base64 エンコーディング）

vpn_connection_device_id

- タイトル：デバイス ID
- 型：string
- 説明 ：（任意）ヘッドエンドへのデバイスレポートの識別子。設定されていない場合、AnyConnect はランダムな永続デバイス ID を生成します。

vpn_connection_report_hardware_id

- タイトル：VPN 認証のハードウェア ID（MAC アドレスと IMEI）の報告
- 型：bool
- 説明：（任意）AnyConnect がハードウェア ID をヘッドエンドに報告しようとするかどうかを指定します。デフォルトでは、AnyConnect はアクセス可能なハードウェア ID を報告しようとします。

vpn_setting_allowed_saved_credentials

- タイトル：ユーザによるクレデンシャルの保存を許可
- 型：bool
- デフォルト値：false
- 説明：（任意）ユーザがクレデンシャルを保存できるようにするかどうか（画面ロックが必要）。デフォルトでは、ユーザはクレデンシャルを保存できません。

vpn_configuration_list

- タイトル：VPN 接続リスト

- 型：bundle_array
- 説明：（任意）これを使用して複数の接続エントリを設定します。各エントリは vpn_configuration バンドルです。

umbrella_org_id

- タイトル：Umbrella 組織 ID
- 型：string
- 説明：顧客が属する組織 ID。Cisco Umbrella ダッシュボードからダウンロードされた設定ファイルに表示されます。

umbrella_reg_token

- タイトル：Umbrella 登録トークン
- 型：string
- 説明：組織に発行された一意の regToken。値は、Cisco Umbrella ダッシュボードからダウンロードされた設定ファイルに表示されます。

umbrella_va_fqdns

- タイトル：Umbrella VA FQDN リスト
- 型：string
- 説明：これは、接続されたネットワークに存在する VA の FQDN リストです。

admin_email

- タイトル：管理者の電子メールアドレス
- 型：string
- 説明：（任意）ログを送信するためのデフォルトの管理者電子メールアドレスを設定します。

vpn_always_on_umbrella_only

- タイトル：VPN モードを Umbrella 保護に対してのみ常にオンにする
- 型：bool
- デフォルト値：false
- 説明：（Umbrella を使用する場合にのみ適用）true に設定すると、常にオンの VPN は Umbrella 保護にのみ適用されます。false に設定すると、常にオンの VPN は Umbrella とリモートアクセスの両方に適用されます。

vpn_configuration バンドルの管理対象制限事項

vpn_name

- タイトル：表示名
- 型：string
- 説明：ユーザにわかりやすい名前（表示専用）。設定されていない場合は、デフォルトでホストになります。

vpn_host

- タイトル：ホスト
- 型：string
- 説明：ヘッドエンドへの URL。このフィールドは必須です。

vpn_protocol

- タイトル：プロトコル
- 型：choice
- 設定可能な値：SSL | IPsec
- 説明：VPN トンネルプロトコル（SSL または IPsec）。デフォルトは SSL です。

vpn_ipsec_auth_mode

- タイトル：IPsec 認証モード
- 型：choice
- 設定可能な値：EAP-AnyConnect | EAP-GTC | EAP-MD5 | EAP-MSCHAPv2 | IKE RSA
- 説明：（任意）トンネルプロトコルが IPsec の場合に使用する認証モード。デフォルトは EAP-Connect です。

vpn_ipsec_ike_identity

- タイトル：IKE ID
- 型：string
- 説明：（任意）IPsec 認証モードが EAP_GTC、EAP-MD5、または EAP-MSCHAPv2 の場合にのみ適用されます。

vpn_keychain_cert_alias

- タイトル：キーチェーン証明書エイリアス
- 型：string
- 説明：（任意）この VPN 設定に使用するクライアント証明書のキーチェーンエイリアス。

vpn_allowed_apps

- キー：vpn_allowed_apps

- タイトル：アプリケーションごとの VPN 許可アプリケーション
- 型：string
- 説明：（任意）トンネリングするアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされません。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_disallowed_apps

- タイトル：アプリケーションごとの VPN で許可されないアプリケーション
- 型：string
- 説明：（任意）トンネリングしないアプリ（Android アプリパッケージ名のカンマ区切りリスト）を指定します。これにより、アプリごとの VPN が有効になります。他のすべてのアプリケーションはトンネリングされます。この設定では、ヘッドエンドでアプリケーションごとの VPN を有効にする必要があります。

vpn_allow_bypass

- タイトル：VPN トンネルのバイパスをアプリケーションに許可する
- 型：bool
- 説明：（任意）この VPN 接続をバイパスすることをアプリに許可します。デフォルトでは無効になっています。

vpn_set_active

- タイトル：アクティブに設定：
- 型：bool
- デフォルト値：false
- 説明：（任意）これが最後に選択された VPN 設定として設定されます。

Apple iOS デバイスでの AnyConnect

このリリースでサポートされている機能およびデバイスについては、『Release Notes for AnyConnect Secure Mobility Client, for Apple iOS』を参照してください。

Apple iOS での AnyConnect の注意事項と制約事項

Apple iOS 用 AnyConnect では、リモート VPN アクセスに関連する機能では、次の機能のみがサポートされます。

- AnyConnect の設定は、ユーザー（手動で）または iPhone 設定ユーティリティ（http://www.apple.com/support/iphone/enterprise/）によって生成する AnyConnect VPN クライアントプロファイルによって行うか、エンタープライズ モバイル デバイス マネージャを使用して行うことができます。
- Apple iOS デバイスは 1 つの AnyConnect VPN クライアントプロファイルのみサポートします。生成された設定の内容は、必ず最新のプロファイルと一致します。たとえば、vpn.example1.com に接続してから vpn.example2.com に接続します。vpn.example2.com からインポートされた AnyConnect VPN クライアントプロファイルは、vpn.example1.com からインポートされたものを置き換えます。
- このリリースは、トンネル キープアライブ機能をサポートしています。ただし、デバイスのバッテリ寿命は短くなります。アップデート間隔の値を増やすことでこの問題は軽減します。

Apple iOS Connect On-Demand の注意事項：

- iOS On-Demand ロジックの結果として自動的に接続され、Disconnect on Suspend（一時停止時に接続解除）が設定されている VPN セッションは、デバイスがスリープすると切断されます。デバイスがスリープ状態から起動すると、必要に応じて On-Demand ロジックが VPN セッションを再接続します。
- AnyConnect は、UI が起動され、VPN 接続が開始されたときにデバイス情報を収集します。そのため、ユーザーが iOS の Connect on Demand 機能を使用して最初に接続を行う場合、または OS バージョンなどのデバイス情報が変更された後、AnyConnect がモバイルポスチャ情報を誤ってレポートする状況が発生します。
- これは、Apple Connect-on-Demand 機能を使用していて、4.0.05032 より前の Legacy AnyConnect リリース、または 9.3 より前の Apple iOS リリースを実行している場合にのみ、お使いの環境に適用されます。AnyConnect の更新後に Connect On-Demand VPN トンネルが適切に確立されるようにするには、ユーザーが AnyConnect アプリを手動で開始して接続を確立する必要があります。このようにしないと、次に iOS システムが VPN トンネルを確立しようとするときに、「VPN に接続するにはアプリケーションを起動する必要があります（The VPN Connection requires an application to start up）」というエラー メッセージが表示されます。

Cisco AnyConnect と Legacy AnyConnect は、異なるアプリ ID を持つ異なるアプリです。次に例を示します。

- AnyConnect 4.0.07x（およびそれ以降）で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05 x：AnyConnect の動作が次のように変更されます。AnyConnect は、スプリット包含ネットワークにない場合でも、トンネル DNS サーバのトラフィックがトンネリングされると見なします。
- AnyConnect アプリケーションを 4.0.05x 以前のバージョンから AnyConnect 4.0.07x または 4.6.x（またはそれ以降）にアップグレードすることはできません。Cisco AnyConnect 4.0.07x（または 4.6.x 以降）は別のアプリケーションであり、別の名前とアイコンを使用してインストールされています。

- AnyConnect の異なるバージョンは、モバイル デバイスに共存できますが、これはシスコではサポートされません。両方のバージョンの AnyConnect がインストールされている状況で接続しようとすると、予期せぬ動作が発生する恐れがあります。デバイスにインストールされている AnyConnect アプリは 1 つだけで、デバイスと環境に適したバージョンであることを確認してください。
- Legacy AnyConnect バージョン 4.0.05069 以前のリリースを使用してインポートされた証明書は、新しい AnyConnect アプリケーションのリリース 4.0.07072 ではアクセスおよび使用ができません。MDM で導入された証明書は、両方のアプリ バージョンでアクセスおよび使用ができます。
- 証明書やプロファイルなどの、Legacy AnyConnect アプリにインポートされたアプリ データは、新しいバージョンに更新する場合、削除する必要があります。そうしないと、システムの VPN 設定で引き続き表示されます。Legacy AnyConnect アプリをアンインストールする前にアプリ データを削除します。
- 現在の MDM プロファイルでは、新しいアプリはトリガーされません。EMM ベンダーは、VPNType（VPN）、VPNSubType（com.cisco.anyconnect）、および ProviderType（パケットトンネル）をサポートする必要があります。AnyConnect は新しいフレームワークで ISE にアクセスできなくなるため、ISE と統合させるには UniqueIdentifier を AnyConnect に渡せる必要があります。設定方法については、EMM ベンダーにお問い合わせください。カスタム VPN タイプが必要な場合もあれば、リリース時にはサポートされていない場合もあります。

AnyConnect 4.0.07x 以降で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x からの動作が次のように変更されます。

- ヘッド エンドに送信されたデバイス ID は、新しいバージョンでは UDID ではなくなり、初期設定へのリセット後には、同じデバイスで作成されたバックアップからデバイスが復元されない限り、デバイス ID が異なるものになります。
- MDM で導入された証明書だけでなく、AnyConnect で利用可能ないずれかの方法（SCEP、UI 使用 - 手動で、URI ハンドラ）を使用してインポートされた証明書も使用できます。AnyConnect の新しいバージョンでは、電子メールまたはこれらの識別されたもの以外のメカニズムを使用してインポートした証明書を使用できなくなりました。
- UI を使用して接続エントリを作成する際には、表示された iOS セキュリティ メッセージを受け入れる必要があります。
- AnyConnect VPN プロファイルからダウンロードしたホスト エントリと同じ名前のユーザーが作成したエントリは、アクティブであれば切断されるまで名前は変更されません。また、ダウンロードされたホスト接続エントリは、接続が維持されている間ではなく、接続が解除された後に UI に表示されます。
- AnyConnect では、split-include ネットワークではない場合でもトンネル DNS サーバのトラフィックがトンネル化されると見なされます。

Apple iOS 固有の注意事項

Apple iOS デバイスで AnyConnect をサポートする場合は、次の点を考慮してください。

- このマニュアルの SCEP の参照は、Apple iOS SCEP ではなく、AnyConnect SCEP にのみ適用されます。
- Apple iOS に制約があるため、プッシュ電子メール通知は VPN では動作しません。ただし、AnyConnect は、トンネルポリシーがこれらをセッションから除外する際に、外部にアクセスできる ActiveSync 接続と平行して作動します。

Apple iPhone Configuration Utility

Apple for Windows または macOS から入手できる iPhone Configuration Utility（IPCU）を使用して、Apple iOS デバイスの構成を作成および展開できます。これは、セキュアゲートウェイの AnyConnect プロファイル設定の代用にできます。

Apple で制御される既存の IPCU GUI は、AnyConnect IPsec 機能を認識しません。IPCU の既存の AnyConnect GUI 内で IPsec VPN 接続を設定します。RFC 2996 で定義されているように、次の URI 構文を [サーバ（Server）] フィールドに使用します。このサーバ フィールドの構文は SSL VPN 接続設定のドキュメント化された使用方法と下位互換性があります。

[**ipsec**://][<**AUTHENTICATION**> [」：「<**IKE-IDENTITY**>「@」]] <**HOST**> [」：「<**PORT**>] ["/"<**GROUP-URL**>]

パラメータ	説明
ipsec	IPSec 接続であることを示します。省略すると、SSL が使用されます。
AUTHENTICATION	IPSec接続の認証方式を指定します。省略すると、EAP-AnyConnect が使用されます。有効な値は次のとおりです。 • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA
IKE-IDENTITY	AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 に設定されているとき、IKE ID を指定します。このパラメータは、他の認証設定に使用されたときに無効になります。
HOST	サーバ アドレスを指定します。使用するホスト名または IP アドレス。

パラメータ	説明
PORT	現在は無視されています。HTTP URI スキームとの一貫性のために含まれています。
GROUP=URL	サーバ名に付加されるトンネル グループ名。

次に例を示します。

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

規格に準拠した Cisco IOS ルータにのみ接続するには、次を使用します。

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

Connect-on-Demand の使用上のガイドライン

Apple iOS Connect On Demand 機能を使用すると、Safari などの他のアプリケーションで VPN 接続を開始できます。Apple iOS は、デバイスのアクティブな接続エントリに設定されたルールに対して、アプリケーションから要求されたドメインを評価します。Apple iOS は、次のすべての条件が満たされた場合にのみ、アプリケーションに代わって VPN 接続を確立します。

- VPN 接続がまだ確立されていない。
- Apple iOS Connect on Demand フレームワークに対応するアプリケーションがドメインを要求している。
- 接続エントリが有効な証明書を使用するように設定されている。
- 接続エントリで Connect on Demand が有効化されている。
- Apple iOS が、[接続しない（Never Connect）] リスト内の文字列とドメイン要求の照合に失敗する。
- 次のいずれかが該当します。Apple iOS は、[常に接続する（Always Connect）] リスト内の文字列をドメイン要求に照合します（Apple iOS 6 でのみ）。または、DNS ルックアップが失敗し、Apple iOS が、[必要に応じて接続（Connect if Needed）] リスト内の文字列をドメイン要求に照合します。

Connect On Demand 機能を使用する場合は、次の点に注意してください。

- iOS の Connect on Demand を使用して VPN 接続が開始された後、iOS は、トンネルが一定の期間非アクティブである場合、そのトンネルの接続を解除します。詳細については、Apple の『VPN Connect-on-Demand』のマニュアルを参照してください。
- 規則を設定する場合は、[必要に応じて接続（Connect if Needed）] オプションを指定することをお勧めします。[必要に応じて接続（Connect if Needed）] ルールは、内部ホストへの DNS ルックアップに失敗した場合に VPN 接続を開始します。企業内のホスト名が内部 DNS サーバを使用してのみ解決されるよう、正しく DNS 設定を行う必要があります。
- 設定された Connect on Demand があるモバイル デバイス用に、証明書ベースの認証トンネル グループに短時間（60 秒）のアイドル タイムアウト（vpn-idle-timeout）が必要です。

VPNセッションがアプリケーションにとって重大な問題がなく、常時接続が必要ではない場合は、アイドル タイムアウトを短く設定します。デバイスがスリープ モードに移行するなど必要でなくなった場合、Apple デバイスは VPN 接続を閉じます。トンネル グループのデフォルト アイドル タイムアウトは 60 分です。

- 常時接続動作は、リリースに依存します。
  - Apple iOS 6 では、iOS はこのリスト ルールが一致したときに常に VPN 接続を開始します。
  - iOS 7.x では、[常に接続する（Always Connect）] はサポートされていません。このリストのルールが一致しても、[必要に応じて接続（Connect if Needed）] のルールとして動作します。
  - 以降のリリースでは、[常に接続する（Always Connect）] は使用されません。設定済みのルールは [必要に応じて接続（Connect if needed）] リストに移動され、それに応じて動作します。
- Apple は、Connect-on-Demand 機能に Trusted Network Detection（TND）の拡張機能を導入しました。この機能拡張は次のとおりです。
  - デバイス ユーザが信頼ネットワーク内にいるかどうかを判断して、Connect-on-Demand 機能を拡張します。
  - Wi-Fi 接続だけに適用されます。他のタイプのネットワーク接続を介して動作している場合、Connect on Demand は、VPN を接続するかどうかを判断するために TND を使用しません。
  - 個々の機能はなく、Connect-on-Demand 機能の外で設定または使用できません。

  iOS 6 の Connect-on-Demand 信頼ネットワーク検出に関する情報は、Apple にお問い合わせください。
- 統合された Apple iOS IPsec クライアントと AnyConnect はどちらも、同じ Apple iOS VPN Connect-on-Demand フレームワークを使用します。

スプリット トンネルによるスプリット DNS 解決の動作

Cisco Secure Firewall ASA スプリットトンネリング機能では、VPN トンネルにアクセスするトラフィックや、クリアテキストで送信されるトラフィックを指定できます。スプリット DNS と呼ばれる関連機能は、VPN トンネル上の DNS 解決のために適切な DNS トラフィックや、エンドポイント DNS リゾルバが処理する DNS トラフィックを（クリア テキストで）指定できます。スプリットトンネリングも設定した場合、スプリット DNS は Apple iOS デバイスで他のデバイスとは異なる方法で機能します。Apple iOS 向け AnyConnect は、このコマンドには次のように応答します。

- split-dns リストのドメインに対して、DNS クエリーだけを暗号化します。

  AnyConnect は、コマンドで指定されたドメインの DNS クエリのみをトンネリングします。他のすべての DNS クエリはクリア テキストでローカル DNS リゾルバに送信し、解決

を行います。たとえば、AnyConnect は次のコマンドに対して example1.com および example2.com の DNS クエリーのみトンネルします。

```
hostname(config-group-policy)# split-dns value example1.com example2.com
```

- default-domain コマンドのドメインに対して、DNS クエリーだけを暗号化します。

  split-dns none コマンドが存在し、**default-domain** コマンドがドメインを指定する場合、AnyConnect はこのドメインに DNS クエリーだけをトンネルし、他の DNS クエリーすべてをローカル DNS リゾルバにクリアテキストで送信します。たとえば、AnyConnect は次のコマンドに対して example1.com の DNS クエリーのみトンネルします。

```
hostname(config-group-policy)# split-dns none
hostname(config-group-policy)# default-domain value example1.com
```

- すべての DNS クエリーはクリア テキストで送信されます。グループ ポリシーに **split-dns none** と **default-domain none** コマンドが存在する場合、またはこれらコマンドがグループ ポリシーにはないが、デフォルトのグループポリシーに存在する場合、AnyConnect は他の DNS クエリーすべてをローカル DNS リゾルバにクリアテキストで送信します。

（注） split-dns が指定されていない場合、グループ ポリシーはデフォルトのグループ ポリシー内に存在するスプリット トンネル ドメイン リストを継承します。スプリット トンネリング ドメイン リストの継承を防ぐには、split-dns none コマンドを使用します。

iOS での AnyConnect の MDM で設定可能な設定

AnyConnect のローカルセキュア設定の定義

管理対象 Apple iOS デバイスで AnyConnect のローカルセキュア設定を定義するには、次のキーと値のペアで MDM を使用してデフォルト値を変更します。これらのキーまたは値のペアが MDM によって設定されると、エンドユーザのデバイスにプッシュされます。これらの値は MDM 設定で設定され、AnyConnect のエンドユーザーが AnyConnect UI でこれらの設定を変更できないようにします。

キー	値	タイプ
UriExternalControl	Disabled/Prompt/Enabled	文字列
BlockUntrustedServers	true/false	ブール値
EnableFipsMode	true/false	ブール値
CheckCert Revocation	true/false	ブール値
StrictCertTrust	true/false	ブール値

エンドユーザーによる VPN 接続の追加のブロック

AnyConnect エンドユーザーによる管理対象 Apple iOS デバイスへの VPN 接続の追加をブロックするには、BlockUserCreateVPNConnection キーを true の値に設定して MDM を使用します。これらの値は MDM 設定で設定され、AnyConnect エンドユーザーが VPN 接続を追加したり、プロファイルをインポートしたりできないようにします。また、VPN 接続の作成またはプロファイルのインポートのための URI の処理が無効になります。このキーまたは値のペアが MDM で設定されていない場合、エンドユーザーは VPN 接続を追加できます（デフォルト）。

Chrome OS デバイスでの AnyConnect

このリリースでサポートされている機能およびデバイスについては、『Release Notes for AnyConnect Secure Mobility Client, for Google Chrome OS』を参照してください。

Chrome OS での AnyConnect の注意事項と制約事項

- 今後の Chrome OS リリースは計画していません。現在のすべての ChromeBooks は Android アプリケーションに対応しているため、代わりに AnyConnect Android アプリを使用することをお勧めします。
- Chromebook デバイスを管理すると（Enterprise Chrome Management サービスに登録）、AnyConnect はクライアント証明書にアクセスできず、クライアント証明書認証は機能しません。
- ローエンドの Chromebook では VPN のパフォーマンスが制限されます（Chromium の問題 #514341）。
- 自動再接続（ネットワーク インターフェイスがダウンして回復したときに VPN セッションに再接続する）は、AnyConnect リリース 4.0.10113 以降を Chrome OS 51 以降で使用する場合にサポートされます。Chrome 51 より前は、Wi-Fi を失ったり、デバイスがスリープ状態になったりすると、AnyConnect は自動的に再接続できませんでした。
- Chrome OS 45 以降を使用していない限り、セキュアゲートウェイから受信されたすべてのサーバー証明書が、完全に信頼できる有効なものであっても、信頼できない証明書として表示されます。
- Chrome OS で AnyConnect をインストールまたはアップグレードした後 、初期化によって AnyConnect の設定が完了するまで待機してください。AnyConnect アプリケーションに [初期化しています。しばらくお待ちください....（Initializing, please wait...）] と表示されます。このプロセスに数分かかることがあります。

ユニバーサルWindowsプラットフォームでのAnyConnect

このリリースでサポートされている機能およびデバイスについては、『Release Notes for AnyConnect Secure Mobility Client, for Universal Windows Platform』を参照してください。

ユニバーサル Windows プラットフォームでの AnyConnect の注意事項と制約事項

- DTLS と IPsec/IKEv2 をサポートしていないため、パフォーマンスが限定されます。
- VPN ローミング（WiFi と 3G/4G/5G ネットワーク間の遷移）はサポートされていません。
- ユーザーが開始した接続の切断では、ヘッドエンドからの切断がクリーンに行われません。短いアイドルタイムアウトで Cisco Secure Firewall ASA VPN グループに接続し、Cisco Secure Firewall ASA で孤立したセッションをクリアすることを推奨します。
- 有効なモバイルライセンスがない Cisco Secure Firewall ASA にモバイルデバイスのユーザーが接続すると、クレデンシャルを入力した後に認証が再起動し、最終的に（5 回試行した後）、[VPN の接続はエラーコード 602 で失敗しました（The VPN connection has failed with error code 602）] という一般的なエラーメッセージが送信されるログインループに陥ります。管理者に問い合わせてセキュア ゲートウェイに有効なモバイル ライセンスがインストールされていることを確認してください。

Cisco Secure Firewall ASA ゲートウェイでのモバイルデバイスの VPN 接続の設定

手順

ステップ 1 デスクトップ/モバイルエンドポイントに共通の設定手順については、該当するリリースの『Cisco ASA Series VPN CLI or ASDM Configuration Guides』を参照してください。モバイル デバイスの場合は以下を考慮してください。

属性	ASDM ロケーション	例外
ホーム ページ URL	**[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）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタマイズ（Customization）]**	AnyConnect Mobile は、ホームページの URL 設定を無視します。認証の成功後に、モバイル クライアントをリダイレクトすることはできません。
AnyConnect 接続プロファイル名およびエイリアス	**[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 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add / Edit）]**	AnyConnect モバイルクライアント接続に使用するトンネルグループ（接続プロファイル）の [名前（Name）] または [エイリアス（Aliases）] フィールドに特殊文字を使用しないでください。特殊文字を使用すると、[ゲートウェイからの応答を処理できません（Unable to process response from Gateway）] とログに記録された後、[接続に失敗しました（Connect attempt has failed）] というエラーメッセージが AnyConnect クライアントに表示される場合があります。
デッド ピア検出	**[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）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]**	サーバー側のデッドピア検出機能はデバイスがスリープ状態になることを防ぐため、オフに切り替えます。ただし、ネットワークの接続性が失われたことによってトンネルが終了したとき、そのことをクライアントが判断できるように、クライアント側のデッド ピア検出はオンにしておく必要があります。

属性	ASDM ロケーション	例外
SSL キープアライブ メッセージ	**[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）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）]**	クライアント側のデッド ピア検出がすでに有効になっている場合、モバイルデバイスのバッテリ寿命を延ばすため、これらのキープアライブ メッセージを無効にすることを推奨します。
IPsec over NAT-T キープアライブ メッセージ	**[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）] > [詳細設定（Advanced）] > [IPsec] > [IKEポリシー（IKE Policies）]**	AnyConnect IPsec が機能するようにするには、[IPsec over NAT-Tの有効化（Enable IPsec over NAT-T）] を選択する必要があります。有効にすると、デフォルトでは NAT キープアライブ メッセージが 20 秒ごとに送信されるため、モバイル デバイスのバッテリーが過剰に消費されます。 これらのメッセージを無効にすることはできないため、モバイル デバイスのバッテリ消費への影響を最小限に抑えるには、NAT-T キープアライブを最大値（3600）に設定することを推奨します。 Cisco Secure Firewall ASA CLI でこれを指定するには、`crypto isakmp nat-traversal 3600` コマンドを使用します。

ステップ 2 必要に応じてモバイルの接続を受け入れるか、拒否するか、または制限するようにモバイル ポスチャ（AnyConnect Identity Extensions（ACIDex）とも呼ばれる）を設定します。

適切なリリースの『Cisco ASA Series VPN CLI or ASDM Configuration Guides』の「*Configuring Endpoint Attributes Used in DAPs*」の手順を参照してください。

例：

接続の確立時に Apple iOS で AnyConnect によりヘッドエンドに送信される属性を次に示します。

```
endpoint.anyconnect.clientversion="4.0.03004";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.devicetype="iPhone7,2";
endpoint.anyconnect.platformversion="9.0";
endpoint.anyconnect.deviceuniqueid="11025f84e99351e807f3583343bfec96351cb416";
```

ステップ 3 （任意） アプリケーション単位 VPN トンネリングモードを設定します。

「アプリごとの VPN を設定する （337 ページ）」を参照してください。

アプリケーション単位 VPN トンネリングモードが設定されていない場合、AnyConnect アプリケーションはシステムトンネリングモードで動作します。

アプリごとの VPN を設定する

始める前に

AnyConnect アプリごとの VPN トンネリングには次のものが必要です。

- ASA 9.3.1 以降（アプリケーション単位 VPN トンネリングを設定する場合）。
- AnyConnect Plus または Apex ライセンス

AnyConnect アプリケーション単位の VPN では、次のモバイルプラットフォームがサポートされています。

- Android 5.0（Lollipop）以降を実行している Android デバイス。
- モバイルデバイス管理（MDM）ソリューションでアプリケーション単位 VPN のを使用するように設定されている、Apple iOS 8.3 以降を実行している Apple iOS デバイス。

手順

ステップ 1 AnyConnect 企業アプリケーション セレクタ ツールのインストール （337 ページ）。

ステップ 2 トンネル内で許可する必要のあるアプリケーションの決定 （338 ページ）。

ステップ 3 モバイルアプリのアプリケーション ID の決定 （339 ページ）。

ステップ 4 アプリごとの VPN を設定する （337 ページ）。

ステップ 5 アプリケーション セレクタ ツールを使用して、プラットフォームに対する AnyConnect のアプリケーション単位 VPN ポリシーを指定します。

- Android デバイスでのアプリケーションごとの VPN ポリシーの定義 （340 ページ）
- Apple iOS デバイスのアプリケーション単位 VPN ポリシーの定義 （341 ページ）

ステップ 6 Secure Firewall ASA での アプリケーション単位カスタム属性の作成 （342 ページ）

ステップ 7 Cisco Secure Firewall ASA のポリシーへのカスタム属性の割り当て （343 ページ）。

AnyConnect 企業アプリケーション セレクタ ツールのインストール

アプリケーション セレクタ ツールは、Android デバイスと Apple iOS デバイスの両方のポリシー生成をサポートするスタンドアロン アプリケーションです。

始める前に

AnyConnect 企業アプリケーションセレクタには Java 7 以降が必要です。

手順

ステップ 1 Cisco.com の AnyConnect Secure Mobility Client Software Centerから AnyConnect 企業アプリケーション セレクタ ツールをダウンロードします。

ステップ 2 ポリシーで Android アプリケーションを使用している場合は、Android SDK および Android SDK Build-tools をシステムにインストールしておく必要があります。そうしない場合は、次のようにインストールします。

a) アプリケーション セレクタ ツールが実行されているプラットフォーム用の Android SDK Tools の最新バージョンをインストールします。

デフォルトのパスと設定（[全ユーザー用のインストール（Install for All Users）] が含まれるため、パッケージエンティティへのアクセスは前述のとおりになる）を使用して、プラットフォーム用の推奨された **SDK Tools Only** パッケージをインストールします。

b) Android SDK Manager を使用して、**Android SDK Build-tools** の最新バージョンをインストールします。

次のタスク

（注） アプリケーション セレクタ ツールで要求されたら、インストール場所（*Android SDK* のインストール ディレクトリ\build-tools*build-tools* バージョン番号\）を指定して、Android Asset Packaging Tool（**aapt**）へのアクセスを設定します。

トンネル内で許可する必要のあるアプリケーションの決定

Android または iOS を実行している電話などのモバイルデバイスをサポートする場合は、Mobile Device Manager（MDM）アプリケーションを使用して VPN アクセスを微調整し、サポートされているアプリケーションのみに VPN トンネルの使用を許可できます。リモートアクセス VPN を承認済みアプリケーションに制限することにより、VPN ヘッドエンドの負荷を削減し、これらのモバイルデバイスにインストールされている悪意のあるアプリケーションから企業のネットワークを保護することもできます。

アプリケーションごとのリモートアクセス VPN を使用するには、サードパーティの MDM アプリケーションをインストールして設定する必要があります。これは承認済みアプリケーションのリストを定義する MDM であり、VPN トンネル経由で使用できます。選択したサードパーティ MDM を設定および使用する方法の解説は、このドキュメントの対象範囲外です。

AnyConnect を使用してモバイルデバイスから VPN 接続を確立すると、個人アプリケーションからのトラフィックを含むすべてのトラフィックが VPN 経由でルーティングされます。代わりに企業のアプリケーションのみを VPN 経由でルーティングし、企業以外のトラフィックを VPN から除外する場合は、アプリケーションごとの VPN を使用して、VPN 経由でトンネリングするアプリケーションを選択できます。

アプリケーションごとの VPN を設定すると、次の主要なメリットがもたらされます。

- パフォーマンス：VPN 内のトラフィックを企業のネットワークに送信する必要があるトラフィックに制限します。したがって、リモートアクセス VPN のヘッドエンドでリソースを解放できます。
- 保護：承認済みのアプリケーションからのトラフィックのみが許可されるため、ユーザが意図せずモバイルデバイスにインストールした可能性がある未承認の悪意のあるアプリケーションから企業のトンネルを保護します。これらのアプリケーションはトンネルに含まれないため、これらのアプリケーションからのトラフィックはヘッドエンドに送信されません。

モバイルエンドポイントで実行されている Mobile Device Manager（MDM）は、アプリケーションごとの VPN ポリシーをアプリケーションに適用します。

モバイルアプリのアプリケーション ID の決定

ユーザーのモバイルデバイスにサービスを提供するために選択した Mobile Device Manager（MDM）にアプリケーションごとのポリシーを設定することを強く推奨します。これにより、ヘッドエンドの設定が大幅に簡素化されます。

代わりにまた、ヘッドエンドで許可されているアプリケーションのリストを設定することにした場合は、エンドポイントのタイプごとに各アプリケーションのアプリケーション ID を決定する必要があります。

iOS でバンドル ID と呼ばれるアプリケーション ID は、逆引き DNS 名です。ワイルドカードとしてアスタリスクを使用できます。たとえば、*. * はすべてのアプリケーションを示し、com.cisco. * はすべてのシスコアプリケーションを示します。

- Android：Web ブラウザで Google Play に移動し、アプリカテゴリを選択します。許可するアプリケーションをクリック（またはマウスオーバー）して、URL を確認します。アプリケーション ID は、URL 内の **id=**パラメータに示されます。たとえば、次は Facebook Messenger の URL であるため、アプリケーション ID は com.facebook.orca です。

  ```
  https://play.google.com/store/apps/details?id=com.facebook.orca
  ```

独自のアプリケーションなどの Google Play を通じて入手できないアプリケーションの場合は、パッケージ名ビューアアプリケーションをダウンロードして、アプリケーション ID を抽出します。シスコは、使用可能なアプリケーションのいずれも推奨しませんが、そのうちのいずれかはユーザが必要とするものを提供しているはずです。

- iOS：バンドル ID を検索する 1 つの方法：
  1. Chrome などのデスクトップブラウザを使用して、アプリケーション名を検索します。

2. 検索結果で、Apple App Store からアプリケーションをダウンロードするためのリンクを探します。たとえば、Facebook メッセンジャー は https://apps.apple.com/us/app/messenger/id454638411 などになります。
3. **id** 文字列の後に数値をコピーします。この例では、**454638411** です。
4. 新しいブラウザウィンドウを開き、次の URL の末尾に数値を追加します。

   ```
   https://itunes.apple.com/lookup?id=
   ```

   この例では、https://itunes.apple.com/lookup?id=454638411 です。
5. 通常は 1.txt という名前のテキストファイルをダウンロードするように求められます。ファイルをダウンロードします。
6. ワードパッドなどのテキストエディタでファイルを開き、bundleId を検索します。例："bundleId":"com.facebook.Messenger" この例では、バンドル ID は「com.facebook.Messenger」です。これをアプリケーション ID として使用します。

アプリケーション ID のリストを取得したら、ポリシーを設定できます。

Android デバイスでのアプリケーションごとの VPN ポリシーの定義

アプリケーションごとの VPN ポリシーは一連のルールで構成され、各ルールは、どのアプリケーションのデータがそのトンネルを経由するかを特定します。モバイルデバイス環境内で許容されるアプリケーションとその使用方法をより厳密に特定するには、ルールオプションを指定します。アプリケーションごとに MDM が設定されている場合でも、アプリケーションごとに機能させるために、Cisco Secure Firewall ASA でアプリケーションごとのポリシー（カスタム属性）の一部を設定する必要があります。アプリケーションセレクタ ツールは、アプリケーションパッケージファイル `*.apk` からの情報を使用して、ルールオプションを設定します。Android パッケージ マニフェスト情報については、http://developer.android.com/guide/topics/manifest/manifest-element.html を参照してください。

始める前に

AnyConnect 企業アプリケーションセレクタには Java 7 以降が必要です。

手順

ステップ 1 アプリケーション セレクタを起動し、[Android] モバイル デバイス プラットフォームを選択します。

ステップ 2 必須の [アプリケーションID（App ID）] フィールドに値を設定します。

- ローカル システムに保存されているアプリケーションからアプリケーション固有のパッケージ情報をインポートするため、[ディスクからインポート（Import from Disk）] を選択します。

[アプリケーションID（APP ID）] フィールド（逆 DNS 形式の文字列）には値が自動的に取り込まれます。例えば Apple iOS ポリシーに Chrome アプリケーションを選択した場合、[アプリケーションID（APP ID）] フィールドは **com.google.chrome.ios** に設定されます。Android の Chrome の場合、これは **com.android.chrome** に設定されます。

- あるいは、アプリケーション固有の情報を直接入力することもできます。
- ワイルドカードを使用した逆DNS形式を指定します。たとえば、ルールでアプリケーションを 1 つずつリストする代わりに、すべての Cisco アプリケーションをトンネリングするには com.cisco.* と指定します。ワイルドカードは、[アプリケーションID（APP ID）] のエントリの最後の文字である必要があります。

  管理対象環境でアプリケーションごとの VPN を設定する場合は、Cisco Secure Firewall ASA ポリシーによって、MDM ポリシーと同じアプリケーションのトンネリングが許可されていることを確認します。すべてのアプリケーションのトンネリングを許可するために、アプリケーション ID として *. * を指定し、MDM ポリシーがトンネリングされたアプリケーションの唯一のアービターとなるように確保することを推奨します。*. * 以外のポリシーはサポートされていません。

ステップ 3 （任意）リストされたアプリケーションを選択し、必要に応じてその他のパラメータを設定します。

- [最小バージョン（Minimum Version）]：パッケージのマニフェスト属性 *android:versionCode* で指定された、選択したアプリケーションの最小バージョン。
- [一致証明書 ID（Match Certificate ID）]：アプリケーション署名証明書のダイジェスト。
- [共有 UID を許可（Allow Shared UID）]：デフォルト値は true です。false に設定した場合、パッケージ マニフェストで *android: sharedUserId* 属性が指定されたアプリケーションはこのルールに一致せず、トンネルにアクセスできません。

ステップ 4 **[ファイル（File）] > [保存（Save）]** をクリックして、このアプリケーションごとの VPN ポリシーを保存します。

ステップ 5 [ポリシー（Policy）]>[ポリシーの表示（View Policy）] を選択し、定義したポリシーの表示を確認します。

この文字列をコピーします。これは、Cisco Secure Firewall ASA の *perapp* カスタム属性の値になる文字列です。

Apple iOS デバイスのアプリケーション単位 VPN ポリシーの定義

Apple iOS デバイスのアプリケーション単位 VPN のポリシーは MDM 機能で完全に制御されます。したがって、AnyConnect はすべてのアプリケーションを許可する必要があり、MDM はアプリケーション単位のポリシーを設定し、トンネリングできる特定のアプリケーションを指定する必要があります。

始める前に

Cisco AnyConnect 企業アプリケーション セレクタには Java 7 以降が必要です。

手順

ステップ 1 アプリケーション セレクタを起動し、[Apple iOS] モバイル デバイス プラットフォームを選択します。

ステップ 2 必須の [アプリケーションID（App ID）] フィールドを ***.*** に設定します。

この設定により、すべてのアプリケーションを AnyConnect 経由でトンネリングでき、MDM のアプリケーション単位のポリシーが、トンネリングされたアプリケーションの唯一のアービターとなります。

ステップ 3 [ファイル（File）] > [保存（Save）] をクリックして、アプリケーション単位 VPN ポリシーを保存します。

ステップ 4 [ポリシー（Policy）] > [ポリシーの表示（View Policy）] を選択し、定義したポリシーの表示を確認します。

この文字列をコピーします。これは、ASA の *perapp* カスタム属性の値になる文字列です。

アプリケーション単位カスタム属性の作成

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）] > [詳細（Advanced）] > [AnyConnect カスタム属性（AnyConnect Custom Attributes）]** に移動してカスタム属性タイプを設定します。

ステップ 2 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性タイプの作成/編集（Create / Edit Custom Attribute Type）] ペインで次の設定を行います。

a) タイプとして *perapp* を入力します。

タイプは *perapp* にする必要があります。これは、アプリケーション単位 VPN に関して AnyConnect が認識する唯一の属性タイプであるためです。この属性をリモートアクセス VPN グループプロファイルに追加すると、トンネルが明示的に識別されたプラットフォームに自動的に制限されます。他のすべてのアプリケーションからのトラフィックは、トンネルから自動的に除外されます。

b) 任意の説明を入力します。

ステップ 3 [OK] をクリックして、このペインを閉じます。

ステップ 4 **[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）] > [詳細（Advanced）] > [AnyConnect カスタム属性名（AnyConnect Custom Attribute Names）]** に移動してカスタム属性を設定します。

ステップ 5 [追加（Add）] または [編集（Edit）] を選択し、[カスタム属性名の作成/編集（Create / Edit Custom Attribute Name）] ペインで次の設定を行います。

a) *perapp* 属性タイプを選択します。

b) 名前を入力します。 この名前は、ポリシーにこの属性を割り当てるために使用されます。

c) ポリシー ツールから BASE64 形式をコピーしてここに貼り付けて、1 つ以上の値を追加します。

各値は 420 文字を超えることはできません。値がこの長さを超える場合は、追加の値コンテンツ用の複数の値を追加します。設定値はAnyConnectに送信される前に連結されます。

Cisco Secure Firewall ASA のポリシーへのカスタム属性の割り当て

perapp カスタム属性は、グループ ポリシーまたはダイナミック アクセス ポリシーに割り当てることができます。

手順

ステップ 1 Secure Firewall ASA でポリシーを開きます。

- グループポリシーの場合、**[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）] > [追加/編集（Add / Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）]** に移動します。
- ダイナミック アクセス ポリシーの場合、**[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）] > [ダイナミックアクセスポリシー（Dynamic Access Policies）] > [追加/編集（Add / Edit）]** に移動します。[アクセス/認証ポリシーの属性（Access/Authorization Policy Attributes）] セクションで、[AnyConnect カスタム属性（AnyConnect Custom Attributes）] タブを選択します。

ステップ 2 既存の属性の [追加（Add）] または [編集（Edit）] をクリックして、[カスタム属性の作成/編集（Create / Edit Custom Attribute）] ペインを開きます。

ステップ 3 ドロップダウン リストから定義済みの *perapp* 属性タイプを選択します。

ステップ 4 [値の選択（Select Value）] を選択し、ドロップダウン リストから定義済みの値を選択します。

ステップ 5 [OK] をクリックして、開いた設定ペインを閉じます。

AnyConnect VPN プロファイルでのモバイルデバイス接続の設定

AnyConnect VPN プロファイルは XML ファイルであり、クライアントの動作を指定し、VPN 接続エントリを識別します。各接続エントリは、このエンドポイントデバイスにアクセス可能なセキュア ゲートウェイとその他の接続属性、ポリシー、および制約を指定します。モバイルデバイスのホスト接続エントリを含む VPN クライアントプロファイルを作成するには、AnyConnect プロファイルエディタを使用します。

Cisco Secure Firewall ASA からモバイルデバイスに配信される VPN プロファイルで定義された接続エントリを、ユーザーが変更したり削除したりすることはできません。ユーザは、手動で作成する接続エントリだけを変更および削除できます。

AnyConnect は、モバイルデバイス上で一度に 1 つの現在の VPN プロファイルのみ維持します。自動または手動の VPN 接続を開始すると、現在のプロファイルが新しい VPN プロファイルによって完全に置き換えられます。ユーザが手動で現在のプロファイルを削除した場合、そのプロファイルは削除され、そのプロファイルに定義されているすべての接続エントリが削除されます。

手順

ステップ 1 基本的な VPN アクセスを設定します。

次の例外を考慮した、デスクトップ/モバイルエンドポイントに共通の手順については、「VPN アクセスの設定 （129 ページ）」を参照してください。

プロファイル属性	例外
自動再接続	Apple iOS 以外のすべてのプラットフォームでは、自動再接続の指定に関係なく、AnyConnect Mobile は常に ReconnectAfterResume を試行します。 Apple iOS の場合のみ、[中断時に接続解除（Disconnect On Suspend）] がサポートされています。[中断時に接続解除（Disconnect On Suspend）] を選択すると、AnyConnect は切断してから、VPN セッションに割り当てられたリソースを解放します。ユーザの手動接続またはオンデマンド接続（設定されている場合）に応答する形でのみ再接続されます。
ローカル LAN へのアクセス	AnyConnect Mobile はローカル LAN アクセス設定を無視し、クライアントプロファイルの設定に関係なく常にローカル LAN アクセスを許可します。

ステップ 2 モバイル固有の属性を設定します。

a) VPN プロファイルで、ナビゲーションウィンドウの [サーバーリスト（Server List）] を選択します。
b) リストに新しいサーバ エントリを追加するには、[追加（Add）] を選択するか、リストからサーバ エントリを選択し、サーバ リストの [エントリ（Entry）] ダイアログボックスを開くには、[編集（Edit）] をクリックします。
c) モバイル固有のパラメータを設定します。
d) [OK] をクリックします。

ステップ 3 次のいずれかの方法で VPN プロファイルを配布します。

- VPN接続のモバイルデバイス設定にクライアントプロファイルをアップロードするように Cisco Secure Firewall ASA を設定します。

  VPN プロファイルを Cisco Secure Firewall ASA にインポートして、グループポリシーに関連付ける方法については、「AnyConnect プロファイルエディタ （91 ページ）」の章を参照してください。

- クライアントプロファイルをインポートするために、ユーザーに AnyConnect URI リンクを提供します。（Android および Apple iOS のみ）

  ユーザにこのタイプの展開手順を提供するには、「VPNプロファイルのインポート （354 ページ）」を参照してください。

- モバイルデバイスで [プロファイル管理（Profile Management）] を使用して、AnyConnect プロファイルをユーザーがインポートするようにします。（Android および Apple iOS のみ）

URI ハンドラを使用した AnyConnect アクションの自動化

AnyConnect の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で AnyConnect にアクション要求を渡すようにします。AnyConnect ユーザー設定プロセスを簡素化するため、URI を Web ページまたは電子メールメッセージにリンクとして埋め込み、これらにアクセスする方法をユーザーに提供します。

始める前に

- AnyConnect の URI ハンドラは、他のアプリケーションが Universal Resource Identifiers（URI）形式で AnyConnect にアクション要求を渡すようにします。

  管理された環境の場合：

  外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。これらを使用する場合、URI の処理に関連付けられたプロンプトに応答する方法をユーザに知らせる必要があります。MDM で設定値を構成するキーと値は次のとおりです。

キー - *UriExternalControl*

値 - [有効（Enabled）]、[プロンプト（Prompt）]、または [無効（Disabled）]

（注） 構成設定を MDM で実行してユーザデバイスにプッシュすると、ユーザによるこの設定の変更は許可されなくなります。

管理されていない環境の場合：

AnyConnect アプリケーションで処理する URI はデフォルトで無効です。モバイル デバイスのユーザは、[外部制御（External Control）] アプリケーション設定を [有効（Enable）] または [プロンプト（Prompt）] に設定することで、この機能を許可します。外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。[プロンプト（Prompt）] に設定すると、ユーザには URI のアクティビティが通知され、要求時に許可または禁止します。

- URI ハンドラ パラメータ値を入力する場合、URL エンコーディングを使用する必要があります。このリンクで示すようなツールを使用して、アクション要求を符号化します。次の例も参照してください。
- URI では `%20` はスペース、`%3A` はコロン（:）、`%2F` はスラッシュ（/）、`%40` はアンパサンド（@）を表します。
- URI のスラッシュは任意です。

次のいずれかのアクションをユーザに指定します。

VPN 接続エントリの生成

この AnyConnect URI ハンドラを使用して、ユーザーの AnyConnect 接続エントリの生成を簡略化します。

anyconnect:[//]**create**[/]**?name**=説明**&host**=サーバ アドレス[**&Parameter1**=値**&Parameter2**=値 ...]

ガイドライン

- *host* パラメータは必須です。その他すべてのパラメータはオプションです。アクションがデバイスで実行されると、AnyConnect は、その *name* と *host* に関連付けられた接続エントリに入力するすべてのパラメータ値を保存します。
- デバイスに追加する各接続エントリの個別のリンクを使用します。単一のリンクで複数の作成接続エントリ アクションを指定することはサポートされていません。

パラメータ

- **name**：AnyConnect のホーム画面の接続リストおよび AnyConnect 接続エントリの [説明（Description）] フィールドに表示される接続エントリの一意の名前。AnyConnect は名前

が一意の場合のみ応答します。接続リストに収まるように、半角 24 文字以内にすることを推奨します。テキストをフィールドに入力する場合、デバイスに表示されたキーボード上の任意の文字、数字、または記号を使用します。文字の大文字と小文字が区別されます。

- **host**：接続する Secure Firewall ASA のドメイン名、IP アドレス、またはグループ URL を入力します。AnyConnect が、このパラメータの値を AnyConnect 接続エントリの [サーバーアドレス（Server Address）] フィールドに挿入します。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol**（任意、指定されていない場合は、デフォルトの SSL になる）：この接続に使用される VPN プロトコル。有効な値は次のとおりです。
  - SSL
  - IPsec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication**（任意、プロトコルが IPsec のみを指定している場合に適用、デフォルトは EAP-AnyConnect）：IPsec VPN 接続で使用される認証方式。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA

- **ike-identity**（authentication が EAP-GTC、EAP-MD5、EAP-MSCAPv2 に設定されている場合に必要）：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 に設定されているときの IKE ID。このパラメータは、他の認証設定に使用されたときに無効になります。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam**（任意、Apple iOS にのみ適用）：デバイスの起動後または接続タイプ（EDGE、3G、Wi-Fi など）の変更後、再接続にかかる時間を制限するかどうかを決定します。このパラメータは、データローミングまたは複数のモバイル サービス プロバイダーの使用には影響しません。有効な値は次のとおりです。
  - true：（デフォルト）このオプションは VPN アクセスを最適化します。接続エントリの Network Roaming フィールドに値 ON を挿入します。
    AnyConnectAnyConnectAnyConnect が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定により、アプリケーションは VPN への持続的な接続に依存できます。AnyConnect は再接続にかかる時間を制限しません。
  - false：このオプションでは、バッテリ寿命が最適化されます。AnyConnect はこの値を AnyConnect 接続エントリの [ネットワークローミング（Network Roaming）] フィール

ドの OFF 値と関連付けます。AnyConnect が接続を失った場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **keychainalias**（任意）：システムの証明書ストアから AnyConnect の証明書ストアに証明書をインポートします。このオプションは、Android のモバイル プラットフォーム専用です。

  名前の付いた証明書がまだシステムストアに存在しない場合、ユーザーは証明書を選択してインストールするように求められ、その後、AnyConnect ストアへのコピーを許可または拒否するかを求めるプロンプトが表示されます。モバイルデバイスで外部制御を有効にする必要があります。

  次の例では、IP アドレスが *vpn.example.com* に設定され、認証用に *client* という名前の証明書が割り当てられている *SimpleExample* という名前の新しい接続エントリを作成します。

  ```
  anyconnect://create/?name=SimpleExample&host=vpn.example.com&keychainalias=client
  ```

- **usecert**（任意）：ホストへの VPN 接続を確立するときに、デバイスにインストールされているデジタル証明書を使用するかどうかを決定します。有効な値は次のとおりです。

  - true（デフォルト設定）：ホストとの VPN 接続を確立するときに自動証明書選択を無効化します。[証明書（Certificate）] フィールドを自動にする certcommonname 値を指定することなしに usecert を true に返し、接続時に AnyConnect 証明書ストアから証明書を選択します。
  - false：自動証明書の選択を無効化します。

  ```
  anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
  ```

- **certcommonname**（任意、ただし isecert パラメータは必要）：デバイスにあらかじめインストールされた有効な証明書の共通名を照合します。AnyConnect はその値を AnyConnect 接続エントリの [証明書（Certificate）] フィールドに挿入します。

  デバイスにインストールされているこの証明書を表示するには、**[診断（Diagnostics）]** > **[証明書（Certificates）]** をタップします。host によって要求された証明書を表示するには、スクロールが必要な場合があります。証明書から読み取った共通名パラメータ、およびその他の値を表示するには、詳細表示ボタンをタップします。

- **useondemand**（任意、Apple iOS だけに適用、usercert、certcommonname パラメータ、および下記のドメイン指定が必要）：Safari などのアプリケーションが、VPN 接続を開始できるかどうか決定します。有効な値は次のとおりです。

  - false（デフォルト）：アプリケーションは VPN 接続を開始できません。このオプションは、DNS 要求を行うアプリケーションが VPN 接続をトリガーしないようにする唯一の手段です。AnyConnect は、このオプションを AnyConnect 接続エントリの [オンデマンド接続（Connect On Demand）] フィールドの OFF 値に関連付けます。
  - true：アプリケーションは Apple iOS を使用して VPN 接続を開始できます。useondemand パラメータを true に設定すると、AnyConnect は値 ON を AnyConnect 接続エントリの

[オンデマンド接続（Connect on Demand）] フィールドに挿入します。
（useondemand=true の場合、domainlistalways パラメータまたは domainlistifneeded パラメータは必須）

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever**（オプション、useondemand=true が必要）：オンデマンド接続機能の使用を不適格とするために、一致を評価するドメインをリストにまとめます。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が最初に使用するリストです。ドメインリクエストが一致する場合、AnyConnect は、ドメインリクエストを無視します。AnyConnect は、このリストを AnyConnect 接続エントリの [接続しない（Never Connect）] フィールドに挿入します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は `www.example.com` などのように指定します。

- **domainlistalways**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：オンデマンド接続機能について一致を評価するドメインをリストします。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が 2 番目に使用するリストです。アプリケーションがこのパラメータで指定されたいずれかのドメインへのアクセスを要求し、VPN 接続がまだ行われていない場合、Apple iOS は VPN 接続を確立しようとします。AnyConnect はこのリストを AnyConnect 接続エントリの [常に接続（Always Connect）] フィールドに挿入します。値リストの例は `email.example.com,pay.examplecloud.com` です。

- **domainlistifneeded**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：DNS エラーが発生した場合、AnyConnect はこのリストに対してドメイン要求が一致しているかどうか評価します。このリストの文字列がドメインに一致する場合、Apple iOS は VPN 接続の確立を試みます。AnyConnect は、このリストを AnyConnect 接続エントリの [必要に応じて接続（Connect if Needed）] フィールドに挿入します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

カンマで区切ったリストを使用して、複数のドメインを指定します。Connect-on-Demand の規則は IP アドレスではなく、ドメイン名のみサポートしています。ただし AnyConnect は、各リストエントリのドメイン名形式について次のような柔軟性があります。

一致	指示	エントリの例	一致する例	一致しない例
プレフィックスおよびドメイン名が正確に一致。	プレフィックス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org

一致	指示	エントリの例	一致する例	一致しない例
ドメイン名は正確に一致し、プレフィックスは任意。先頭にドットを付けると、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net anytext	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

VPN 接続の確立

VPN に接続してユーザーが容易に VPN 接続を確立できるようにするには、この AnyConnect URI ハンドラを使用します。また、URI に次のタスクを実行するための追加情報を埋め込むことができます。

- ユーザ名とパスワードの事前入力
- 二重認証用のユーザ名とパスワードの事前入力
- ユーザ名とパスワードの事前入力および接続プロファイル エイリアスの指定

このアクションには name または host のいずれかのパラメータが必要ですが、次の構文のいずれかを使用して両方を指定することもできます。

anyconnect:[//]**connect**[/]**?**[**name=**説明|**host=**サーバアドレス][**&Parameter1**=値**&Parameter2**=値..]

または

anyconnect:[//]**connect**[/]**?name=**説明**&host=**サーバアドレス[**&Parameter1**=値**&Parameter2**=値..]

ガイドライン

- ステートメントのすべてのパラメータ値がデバイスの AnyConnect 接続エントリに一致する場合、AnyConnect は接続を確立するために残りのパラメータを使用します。

- ステートメントのすべてのパラメータが接続エントリのパラメータと一致せず、name パラメータが一意の場合、AnyConnect は新しい接続エントリを生成し、VPN 接続を試行します。
- URI を使用して、VPN 接続を確立するためにワンタイム パスワード（OTP）インフラストラクチャとの組み合わせのみ使用する必要がある場合、パスワードを指定します。

パラメータ

- **name**：AnyConnect ホームウィンドウの接続リストに表示される、接続エントリの名前。AnyConnect はこの値を AnyConnect 接続エントリの [説明（Description）] フィールドに対して評価し、前回の手順を使用してデバイスに接続エントリを作成した場合、name とも呼ばれます。この値は大文字と小文字が区別されます。
- **host**：AnyConnect 接続エントリの [サーバーアドレス（Server Address）] フィールドと一致させるには、Cisco Secure Firewall ASA のドメイン名、IP アドレス、またはグループ URL を入力します。前回の手順を使用してデバイスに接続エントリを生成した場合、host とも呼ばれます。

  グループ URL は、[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 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループ エイリアス/グループ URL（Group Alias/Group URL）] > [グループ URL（Group-URL）] を選択して、ASDM に設定されます。
- **onsuccess**：接続が正常である場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が接続状態に遷移するとき、または anyconnect:close コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が遷移するとき、またはすでに接続状態であるときに表示する URL を指定します。複数の onsuccess アクションを指定できます。AnyConnect は、Android デバイスでの接続が成功した後で常に GUI を閉じます。
- **onerror**：接続に失敗した場合にこのアクションを実行します。プラットフォーム固有の動作は次のとおりです。
  - Apple iOS デバイスの場合、この接続が失敗したとき、または anyconnect:close コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
  - Android デバイスの場合、この接続が失敗したときに表示される URL を指定します。複数の onerror アクションを指定できます。AnyConnect は、Android デバイスでの接続が失敗した後で常に GUI を閉じます。
- **prefill_username**：connect URI にユーザ名を指定し、接続プロンプトに自動入力します。

- **prefill_password**：connect URI にパスワードを指定し、接続プロンプトに自動入力します。このフィールドは、ワンタイムパスワード用に設定した接続プロファイルでの使用のみとしてください。
- **prefill_secondary_username**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_secondary_password**：二重認証を必要とするように設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名のパスワードを指定し、接続プロンプトに自動入力します。
- **prefill_group_list**：これは、[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 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループエイリアス/グループURL（Group Alias/Group URL）] > [接続エイリアス（Connection Aliases）] を選択して、ASDM で定義されている接続エイリアスです。

例

- URI に接続名およびホスト名またはグループ URL を入力します。

```
anyconnect://connect/?name=Example

anyconnect:connect?host=hr.example.com

anyconnect:connect?name=Example&host=hr.example.com

anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 成功または失敗に対するアクションの指定

  connect アクションの結果に基づいて特定の URL ベースを開始するために、onsuccess または onerror パラメータを使用します。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com

anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

  Android では複数の onsuccess アクションを指定できます。

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

  Apple iOS デバイスでは、onsuccess パラメータまたは onerror パラメータで anyconnect://close コマンドを使用して、AnyConnect GUI を閉じることができます。

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- URI での接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
```

```
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 接続情報の指定、ユーザ名とパスワードの自動入力、および接続プロファイルエイリアスの指定：

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

VPN からの接続解除

VPN からユーザーの接続を解除するには、この AnyConnect URI ハンドラを使用します。

anyconnect:[//]**disconnect**[/]**&onsuccess=**URL

パラメータ

onsuccess パラメータは、Android デバイスだけに適用されます。この接続が解除されるとき、またはすでに接続解除状態であるときに表示される URL を指定します。

例

```
anyconnect:disconnect
```

証明書のインポート

この URI ハンドラーコマンドを使用して、PKCS12 でエンコードされた証明書バンドルをエンドポイントにインポートします。AnyConnect はエンドポイントにインストールされている PKCS12 でエンコードされた証明書を使用して、Secure Firewall ASA に対して自らを認証します。PKCS12 証明書タイプのみをサポートします。

anyconnect:[//]**import**[/]**?type=pkcs12&uri=***http%3A%2F%2Fexample.com%2Fcertificatename.p12*

パラメータ

- **type**：PKCS12 証明書タイプのみをサポートします。
- **uri**：証明書がある場所の URL エンコード ID。

例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

VPN プロファイルのインポート

AnyConnect にクライアントプロファイルを配布するため、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=profile&uri=***filename.xml*

例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

AnyConnect UI とメッセージのローカライズ

AnyConnect をローカライズするには、この URI ハンドラ方式を使用します。

anyconnect:[//]**import**[/]**?type=localization&lang=***LanguageCode***&host=**へ

パラメータ

インポート アクションには、すべてのパラメータが必要です。

- **type**：インポートのタイプ（この場合はローカリゼーション）。
- **lang**：anyconnect.po ファイルで指定されて言語を表す 2 文字または 4 文字の言語タグ。たとえば、言語タグは単純に「フランス語」なら fr、「カナダ フランス語」なら fr-ca となります。
- **host**：AnyConnect 接続エントリの [サーバーアドレス（Server Address）] フィールドと一致させるには、Cisco Secure Firewall ASA のドメイン名または IP アドレスを入力します。

例

```
anyconnect:import?type=localization&lang=fr&host=asa.example.com
```

モバイルデバイスでの AnyConnect のトラブルシューティング

始める前に

モバイルデバイスでログを有効にします。

- Cisco AnyConnect Secure Mobility Client の Android 向けユーザーガイド リリース 4.6
- Cisco AnyConnect Secure Mobility Client の Apple iOS 向けユーザーガイド リリース 4.6.x
- Cisco Anyconnect Secure Mobility Client Windows Phone 向けユーザーガイド リリース 4.1.x

これらの指示に従っても問題が解決しない場合は、次のことを試してください。

手順

ステップ 1 同じ問題がデスクトップ クライアントまたは別のモバイル OS で発生するかどうかを確認します。

ステップ 2 適切なライセンスが Cisco Secure Firewall ASA にインストールされていることを確認します。

ステップ 3 証明書認証が失敗する場合は、次のことを確認してください。

a) 適切な証明書が選択されていることを確認します。

b) デバイスのクライアント証明書に Extended Key Usage として Client Authentication があることを確認します。

c) AnyConnect プロファイルの証明書一致規則によってユーザーの選択した証明書を除外されていないことを確認します。

ユーザが証明書を選択しても、プロファイルのフィルタリング ルールに一致しなければ認証には使用されません。

d) 認証メカニズムで Cisco Secure Firewall ASA に関連するアカウンティング ポリシーが使用されている場合、ユーザーが正常に認証できることを確認します。

e) 証明書のみの認証を使用しようとしている場合に認証画面が表示されたら、グループ URL を使用するよう接続を設定し、トンネル グループのセカンダリ認証が設定されていないことを確認します。

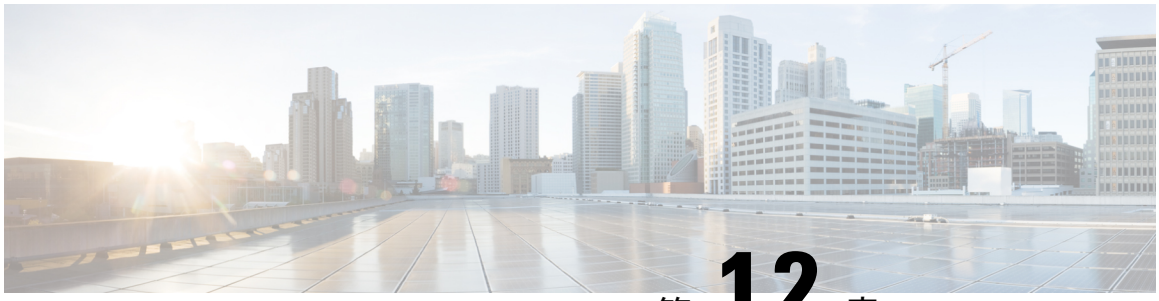
ステップ 4 Apple iOS デバイスで、次のことを確認します。

a) デバイスが起動した後で VPN 接続がリストアされていない場合は、[ネットワーク ローミング（Network Roaming）] が無効になっていることを確認します。

b) Connect On Demand を使用している場合は、証明書のみの認証およびグループ URL が設定されていることを確認します。

次のタスク

それでも問題が解決されない場合は、クライアントのロギングを有効にし、Cisco Secure Firewall ASA のデバッグ ロギングを有効にします。詳細については、適切なリリースの『Cisco ASA Series VPN CLI or ASDM Configuration Guide』を参照してください。



第 12 章

AnyConnect カスタマー エクスペリエンス フィードバック モジュールの設定

（注） デフォルトでは、プライベート データおよび企業データが収集されます。

カスタマー エクスペリエンス フィードバック（CEF）モジュールにより、カスタマーが使用し、有効にしたモジュールおよび機能の情報を取得できます。この情報によりユーザーエクスペリエンスを把握できるため、シスコは AnyConnect の品質、信頼性、パフォーマンス、ユーザーエクスペリエンスを継続して改善できます。

情報の収集および使用の詳細については、「Cisco Online Privacy Statement Highlights」ページからアクセスできる、「AnyConnect Secure Mobility Client Supplement」を参照してください。 すべてのデータは匿名で収集され、個人を特定できるデータは含まれません。また、データは安全に送信されます。

シスコは、次のタイプのデータを収集します。

- ユーザビリティ データ：詳細については、プライバシー ポリシーを参照してください。このデータは、毎月一度収集され送信されます。
- Web 脅威データ：脅威が報告されるたびに送信されます。
- クラッシュ レポート：AnyConnect が生成したクラッシュ ダンプ ファイルが 24 時間おきにチェックされ、収集され、カスタマー エクスペリエンス フィードバック サーバーに送信されます。

カスタマー エクスペリエンス フィードバック モジュールの主なコンポーネントは次のとおりです。

- フィードバックモジュール：AnyConnect のソフトウェアコンポーネントで、情報を収集し定期的にサーバーに送信します。
- Cisco フィードバック サーバ：カスタマー エクスペリエンス フィードバック データを収集し、未処理形式で一時的なストレージに保存する、シスコが所有するクラウドインフラストラクチャです。

• カスタマー エクスペリエンス フィードバックの設定 （358 ページ）

カスタマー エクスペリエンス フィードバックの設定

AnyConnect カスタマー エクスペリエンス フィードバック モジュールは AnyConnect で展開され、デフォルトで有効になっています。カスタマーエクスペリエンスフィードバック プロファイルを作成することで、エクスペリエンスフィードバックから完全に除外するなど、送信されるフィードバックの内容を変更できます。この方法は、フィードバックモジュールを無効にする場合に適した方法ですが、AnyConnect の展開中にフィードバックモジュールを完全に排除することもできます。

始める前に

カスタマー エクスペリエンス フィードバック モジュールは自動的に有効になります。

手順

ステップ 1 スタンドアロンのカスタマー エクスペリエンス フィードバック プロファイル エディタを開くか、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）] > [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 [フィードバック サービス プロファイル（Feedback Service Profile）] のプロファイルの用途で AnyConnect プロファイルを作成します。

ステップ 3 フィードバックを提供しない場合は、[カスタマーエクスペリエンス フィードバック サービスの有効化（Enable customer Experience Feedback Service）] をオフにします。

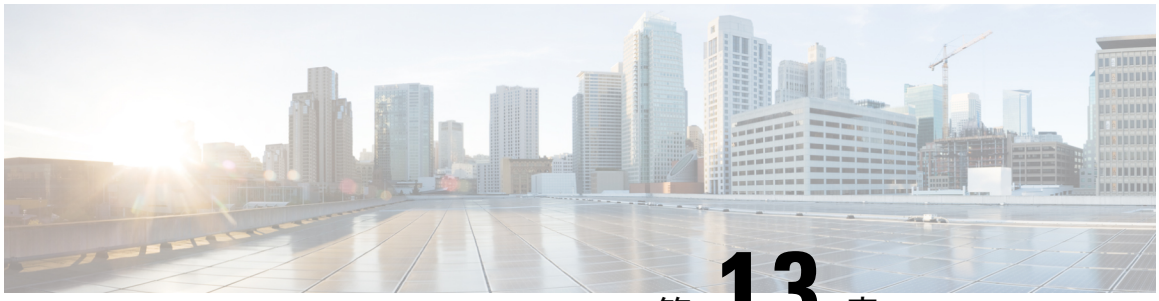
フィードバックは、インストール後にいつでも無効にできます。

ステップ 4 AnyConnect によって生成されたクラッシュレポートを送信しない場合は、[クラッシュレポートを含める（Include Crash Report）] をオフにします。

デフォルトでは、クラッシュ レポートが含まれます。

ステップ 5 任意のカスタマー キーまたはカスタマー ID を入力します。

この ID により、シスコはどの組織からの情報であるかを識別できます。



第 13 章

AnyConnect のトラブルシューティング

トラブルシューティングに必要な情報の収集

統計詳細情報の表示

管理者またはエンドユーザーは、現在の AnyConnect セッションの統計情報を表示できます。

手順

ステップ 1 Windows では、[詳細ウィンドウ（Advanced Window）] > [統計情報（Statistics）] > [VPN ドロワ（VPN drawer）] > > に移動します。Linux では、ユーザ GUI 上の [詳細（Details）] ボタンをクリックします。

ステップ 2 クライアントコンピュータにロードされたパッケージに応じて、次のオプションから選択します。

- [統計情報のエクスポート（Export Stats）]：後で分析およびデバッグできるようにテキスト ファイルに接続統計情報を保存します。
- [リセット（Reset）]：接続情報をゼロにリセットします。AnyConnect がすぐに新しいデータの収集を開始します。

- [診断（Diagnostics）]：AnyConnect Diagnostics and Reporting Tool（DART）ウィザードを起動します。ウィザードは、クライアント接続を分析およびデバッグできるように、指定されたログファイルと診断情報をバンドルします。

トラブルシューティング用にデータを収集するための DART の実行

DART は AnyConnect Diagnostics and Reporting Tool の略で、AnyConnect のインストールと接続に関する問題のトラブルシューティング用データの収集に使用できます。DART によってログ、ステータス、および診断情報が収集され、それを Cisco Technical Assistance Center（TAC）での分析に使用できます。

DART ウィザードは、AnyConnect を実行するデバイス上で実行されます。DART は AnyConnect から起動できます。または AnyConnect を使用せずにそれ自体を起動できます。

（注） DART でログを収集するには、macOS、Ubuntu 18.04、および Red Hat 7 の管理者権限が必要です。

また、ISE ポスチャの場合のみにおいて、ISE ポスチャ クラッシュの発生直後、またはエンドポイントが準拠しなくなったときに、DART が設定されている場合は自動的に DART を収集できます。自動 DART を有効にするには、DARTCount をゼロを除くすべての値として設定します。0 に設定すると、この機能は無効になります。自動 DART を有効にすると、時間によるデータ損失を防止できます。次の場所に自動収集 DARTS を収集します。

- Windows：%LocalAppData%/Cisco/Cisco AnyConnect Secure Mobility Client
- macOS：~/.cisco/iseposture/log

次のオペレーティング システムがサポートされています。

- Windows
- macOS
- Linux

手順

ステップ 1 DART を起動します。

- Windows デバイスの場合は、AnyConnect Secure Mobility Client を起動します。
- Linux デバイスの場合は、[アプリケーション（Applications）]>[インターネット（Internet）]>[Cisco DART]> > を選択します。

  または /opt/cisco/anyconnect/dart/dartui を選択します。

- macOS デバイスの場合、**[アプリケーション（Applications）]** > **[Cisco]** > **[Cisco DART]** を選択します。

ステップ 2 [統計情報（Statistics）] タブをクリックし、次に [診断（Diagnostics）] をクリックします。

ステップ 3 [デフォルト（Default）] または [カスタム（Custom）] のバンドル作成を選択します。

- [デフォルト（Default）]：AnyConnect ログファイル、コンピュータに関する一般情報、および DART ツールが実行した内容と実行しなかった内容の概要などの一般的なログファイルと診断情報を含みます。バンドルのデフォルト名は `DARTBundle.zip` であり、このバンドルはローカルデスクトップに保存されます。
- [カスタム（Custom）]：バンドルに含めるファイル（またはデフォルトファイル）、およびバンドルの保存場所を指定できます。

  Linux および macOS での成功したルートおよびフィルタリングの変更がログから除外されるようになり、重要なイベントに注意しやすくなります。そうでない場合、syslog のイベント レートの制限により、重要なイベントがドロップして見落とされる可能性があります。また、キャプチャフィルタ処理設定を使用すると、AnyConnect のフィルタ処理構成ファイルだけでなく、macOS のシステム構成ファイルも表示できるようになります。Linux の場合、これらの設定のほとんどは DART ツールが sudo を介して実行されている場合以外アクセスが制限されているにもかかわらず、iptables および ip6tables の出力が DART に表示されます。

（注） macOS のオプションは、[デフォルト（Default）] のみです。バンドルに含めるファイルは、カスタマイズできません。

（注） [カスタム（Custom）] を選択すると、バンドルに含めるファイルを指定でき、また、ファイルに対して異なる保存場所を指定できます。

ステップ 4 DART がデフォルトリストのファイル収集に時間がかかっていると思われる場合は、[キャンセル（Cancel）] をクリックし、DART を再実行して、[カスタム（Custom）] を選択して含めるファイルを減らします。

ステップ 5 [デフォルト（Default）] を選択すると、DART はバンドルの作成を開始します。[カスタム（Custom）] を選択した場合、ウィザードのプロンプトに従って、ログ、プリファレンス ファイル、診断情報、およびその他のカスタマイズを指定します。

DART で UDID を公開する

DART CLI 内では、クライアントの固有デバイス識別子（UDID) を表示できます。たとえば、Windows で、dartcli.exe（C:\Program Files\Cisco\AnyConnect Secure Mobility Client）が含まれているフォルダに移動し、 **dartcli.exe -u** または **dartclie.exe udid** を入力します。

インストールまたはアンインストールの問題についてデータを収集するためのログの収集（Windows）

AnyConnect のインストールまたはアンインストールに失敗した場合は、DART コレクションはこの状況を診断しないため、ログを収集する必要があります。

AnyConnect ファイルを解凍したのと同じディレクトリで、msiexec コマンドを実行します。

- インストールに失敗した場合は、次のように入力します。

```
C:/temp>msiexec /i anyconnect-win-version-pre-deploy-k9.msi /lvx
c:/Temp/ac-install.log?
```

ここで *c:/temp/ac-install.log?* は、任意のファイル名にすることができます。

- アンインストールに失敗した場合は、次のように入力します。

```
c:/temp/msiexec /x anyconnect-win-version-pre-deploy-k9.msi /lvx
c:/Temp/ac-install.log?
```

ここで *c:/temp/ac-uninstall.log?* は、選択したファイル名にすることができます。

（注） アンインストールに失敗した場合は、現在インストールされているバージョン固有の MSI を使用する必要があります。

上記と同じコマンドを変更して、正しくインストールまたはアンインストールされなかった Windows のすべてのモジュールに関する情報をキャプチャすることもできます。

コンピュータ システム情報の取得

Windows の場合は、**msinfo32 /nfo c:\msinfo.nfo** と入力します。

systeminfo ファイル ダンプの取得

Windows の場合は、sysinfo コマンド プロンプトで **c:\sysinfo.txt** と入力します。

レジストリ ファイルの確認

次の SetupAPI ログ ファイル内のエントリは、ファイルが見つからないことを示しています。

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot fine the file specified.
```

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce レジストリ キーが存在することを確認してください。このレジストリ キーが存在しない場合、すべての INF インストール パッケージが禁止されます。

AnyConnect ログファイルの場所

ログは、次のファイル内に保持されます。

- Windows：`\Windows\Inf\setupapi.app.log` または `\Windows\Inf\setupapi.dev.log`

（注） Windows では、隠しファイルを表示する必要があります。

これが新規の Web 展開インストールの場合、このログ ファイルは次のユーザ別の temp ディレクトリに格納されます。

`%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`。

アップグレードが最適ゲートウェイからプッシュされた場合、ログファイルは次の場所にあります。

`%WINDIR%\TEMP\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyy.log`.

インストールするクライアントのバージョンの最新ファイルを取得します。*xxx* はバージョンによって異なり、*yyyyyyyyyyyyy* はインストールの日時を示します。

- macOS（10.12 以降）：ロギングデータベース。「コンソール」アプリまたはログコマンドを使用して、VPN、DART、または Umbrella のログを照会します。
- macOS（レガシーファイルベースのログ）：`/var/log/system.log`（他のすべてのモジュール）
- Linux Ubuntu：`/var/log/syslog`
- Linux Red Hat：`/var/log/messages`

DART を実行してトラブルシューティング データをクリアする

Windows では、DART ウィザードを使用し、生成されたログをクリアできます。

手順

ステップ 1 管理者権限で DART を起動します。

ステップ 2 [**すべてのログをクリア**（Clear All Logs）] をクリックし、ログの消去を開始します。

AnyConnect 接続または接続解除の問題

AnyConnect が初期接続を確立しないか、接続解除しない

問題：AnyConnect が初期接続を確立しないか、または AnyConnect Secure Mobility Client ウィンドウで [接続解除（Disconnect）] をクリックすると予期しない結果が得られます。

解決策：次の点をチェックします。

- Citrix Advanced Gateway Client Version 2.2.1 を使用している場合は、CtxLsp.dll の問題が Citrix によって解決されるまで Citrix Advanced Gateway Client を削除してください。
- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- Cisco Secure Firewall ASA からコンフィギュレーション ファイルを取得し、次のようにして接続失敗の兆候を探します。
  - Cisco Secure Firewall ASA コンソールから **write net x.x.x.x:ASA-Config.txt** と入力します。この x.x.x.x はネットワーク上の TFTP サーバーの IP アドレスです。
  - Cisco Secure Firewall ASA コンソールから、show running-config と入力します。設定を切り取ってテキスト エディタに貼り付け、これを保存します。
- Cisco Secure Firewall ASA イベントログを表示します。
  1. Cisco Secure Firewall ASA コンソールで、次の行を追加し、ssl、webvpn、anyconnect、および auth のイベントを調べます。

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

  2. AnyConnect の接続を試行し、接続エラーが発生した場合は、そのコンソールのログ情報を切り取ってテキストエディタに貼り付け、保存します。
  3. **no logging enable** と入力し、ロギングを無効にします。

- Windows イベントビューアを使用してクライアントコンピュータから AnyConnect Secure Mobility Client ログを取得します。
  1. [スタート（Start）] > [ファイル名を指定して実行（Run）] の順に選択し、**eventvwr.msc /s** と入力します。
  2. [アプリケーションとサービスログ（Applications and Services Logs ）]（Windows 7）で、AnyConnect Secure Mobility Client を見つけ、[ログファイルの名前を付けて保存...（Save Log File As...）] を選択します。。
  3. ファイル名（たとえば、AnyConnectClientLog.evt）を割り当てます。.evt ファイル形式を使用する必要があります。
- Windows 診断デバッグ ユーティリティを変更します。
  1. WinDbg のマニュアルに記載されているとおりに vpnagent.exe プロセスを接続します。
  2. IPv6/IPv4 IP アドレス割り当てで競合が存在するかどうかを確認します。特定済みの競合がないか、イベント ログで確認します。
  3. 競合が特定されていた場合は、使用するクライアント コンピュータのレジストリにルーティングのデバッグを追加します。このような競合は、AnyConnect イベントログで次のように表示されます。

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
 Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.

Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

  4. 特定のレジストリ エントリ（Windows）またはファイル（Linux および macOS）を追加して、接続用にワンタイム単位でルートのデバッグを有効にします。
     - 32 ビット Windows の場合、DWORD レジストリ値は HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled である必要があります。
     - 64 ビット Windows の場合、DWORD レジストリ値は HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco\Cisco AnyConnect Secure Mobility Client\DebugRoutesEnabled である必要があります。
     - Linux または macOS の場合、sudo touch コマンドを使用してパス /opt/cisco/anyconnect/debugroutes にファイルを作成します。

（注） トンネル接続が開始されると、キーまたはファイルは削除されます。デバッグを有効にするには、ファイルまたはキーが存在するだけで十分であり、キーの値またはファイルの内容は重要ではありません。

VPN接続を開始します。このキーまたはファイルが見つかった場合、2つのルート デバッグ テキスト ファイルがシステムの一時ディレクトリに作成されます（通常、Windows では C:\Windows\Temp、macOS または Linux では /opt/cisco/anyconnect）。2 つのファイル（debug_routechangesv4.txt4 と debug_routechangesv6.txt）がすでに存在する場合、これらのファイルは上書きされます。

AnyConnect トラフィックを通過させない

問題：AnyConnect クライアントは、接続後、プライベートネットワークにデータを送信できません。

解決策：次の点をチェックします。

- AT&T Sierra Wireless 875 カードと AT&T Communication Manager Version 6.2 または 6.7 を使用している場合は、次の手順に従って問題を修正してください。
  1. Aircard でアクセラレーションを無効にします。
  2. [ツール（Tools）] > [設定（Settings）] > [アクセラレーション（Acceleration）] > [スタートアップ（Startup）] から AT&T Communications Manager を起動します。
  3. **manual** と入力します。
  4. [停止（Stop）] をクリックします。
- **show vpn-sessiondb detail anyconnect filter name <username>** コマンドの出力を取得します。出力にフィルタ名 XXXXX が指定されている場合は、show access-list XXXXX コマンドの出力も取得してください。ACL によってトラフィック フローがブロックされていないか確認してください。
- [AnyConnect Secure Mobility Client] > [統計情報（Statistics）] > [詳細（Details）] > [エクスポート（Export）] の順に選択し、DART のファイルまたは出力（AnyConnect-ExportedStats.txt）を取得します。統計情報、インターフェイス、およびルーティング テーブルを調べます。
- Cisco Secure Firewall ASA コンフィギュレーション ファイルの NAT 文を確認します。NAT が有効になっている場合は、クライアントに返されるデータをネットワーク アドレス変換から除外する必要があります。たとえば、AnyConnect プールから IP アドレスを NAT 除外するには、次のコードが使用されます。

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
```

```
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- トンネリングされたデフォルト ゲートウェイがその設定に対して有効になっているかどうかを確認してください。従来型のデフォルト ゲートウェイは、次のように非復号化トラフィックのラスト リゾート ゲートウェイです。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

  VPN クライアントが、VPN ゲートウェイのルーティング テーブルに存在しないリソースにアクセスする必要がある場合、パケットは標準デフォルト ゲートウェイによってルーティングされます。VPN ゲートウェイは、完全な内部ルーティング テーブルを必要としません。トンネリングされたキーワードを使用する場合、IPsec/SSL VPN 接続から受信した復号化トラフィックはルーティングによって処理されます。VPNルートから受信したトラフィックは 10.0.4.2 にルーティングされて復号化されますが、標準トラフィックは最終的に 209.165.200.225 にルーティングされます。

- AnyConnect でトンネルを確立する前後の、ipconfig /all のテキストダンプおよび route print の出力を収集します。
- クライアントでネットワーク パケット キャプチャを実行するか、Cisco Secure Firewall ASA のキャプチャを有効にします。

（注） 一部のアプリケーション（Microsoft Outlook など）がトンネルで動作しない場合、受け入れられるサイズを確認するために、一定の基準に従って大きくした ping（たとえば、ping -| 500, ping -| 1000, ping -| 1500, and ping -| 2000）を使用して、ネットワーク内の既知のデバイスに ping します。ping の結果から、ネットワークにフラグメンテーションの問題が発生しているかがわかります。その後、フラグメンテーションが発生していると思われるユーザの特別なグループを設定して、このグループの anyconnect mtu を 1200 に設定できます。また、古い IPsec クライアントから Set MTU.exe ユーティリティをコピーして、物理アダプタの MTU を強制的に 1300 に設定できます。リブート時に、違いがあるかどうか確認してください。

VPN サービスの障害

VPN サービス接続に失敗

問題：「処理を進めることができません。VPN サービスに接続できません（Unable to Proceed, Cannot Connect to the VPN Service）」というメッセージが表示されます。AnyConnect の VPN サービスが実行されていません。

解決策：別のアプリケーションがサービスと競合していないかを確認してください。11-7ページの「何がサービスと競合しているかの特定」を参照してください。

何がサービスと競合しているかの特定

次の手順では、サーバーが起動されないため、競合が起動時にサーバの初期化との間で生じたか、または他の実行中のサービスとの間で生じたかを判別します。

手順

ステップ 1 Windows 管理ツールでサービスを確認して、AnyConnect VPN エージェントが動作していないか確認します。このエージェントが動作している場合にエラーメッセージが引き続き表示される場合は、ワークステーション上の別の VPN アプリケーションを無効にするか、アンインストールすることが必要になる可能性があります。その操作を実行した後、リブートし、この手順を繰り返します。

ステップ 2 AnyConnect VPN エージェントを起動してみます。

ステップ 3 イベントビューアの AnyConnect ログに、サービスを起動できなかったことを示すメッセージがないか確認します。ステップ 2 での手動によるリスタートのタイムスタンプおよびワークステーションが起動した時間に注目します。

ステップ 4 イベントビューアのシステム ログおよびアプリケーション ログに、競合メッセージの同一の一般的なタイム スタンプがないかを確認します。

ステップ 5 サービスの起動に失敗したことをログが示している場合、同一のタイム スタンプの前後にある、次のいずれかを示すその他の情報メッセージを探します。

- 欠落したファイル：欠落したファイルを除外するには、AnyConnect をスタンドアロン MSI インストールから再インストールします。
- 別の依存するサービスでの遅延：起動アクティビティを無効にして、ワークステーションのブート時間を短縮します。
- 別のアプリケーションまたはサービスとの競合：別のサービスが、vpnagent が使用するポートと同じポート上で受信していないか、または一部の HIDS ソフトウェアによって、シスコのソフトウェアがポート上で受信できなくなっているかどうかを判別します。

ステップ 6 ログに原因が直接示されていない場合は、試行錯誤的な方法で競合を識別してください。最も可能性の高い候補を識別したら、[サービス（Services ）] パネルから該当するサービス（VPN 製品、HIDS ソフトウェア、spybot クリーナ、スニファ、ウイルス対策ソフトウェアなど）を無効にします。

ステップ 7 リブートします。VPN エージェント サービスが依然として起動に失敗する場合は、オペレーティング システムのデフォルト インストールでインストールされなかったサービスをオフにします。

VPNクライアントドライバで（MicrosoftWindowsアップデート後に）エラーが発生する

問題：最近Microsoft certclass.infファイルを更新し、その後、VPN接続を確立しようとすると、次のメッセージが表示されます。

```
The VPN client driver has encountered an error.
```

C:\WINDOWS\setupapi.log を確認すると、次のエラーが表示される場合があります。

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
 Error 0xfffffbf8: Unknown Error. Assuming all device classes are subject to driver
signing policy.
```

解決策：コマンドプロンプトで**C:\>systeminfo**と入力するか、C:\WINDOWS\WindowsUpdate.logを確認して、最近インストールされた更新プログラムを確認してください。VPNドライバを修正する手順に従ってください。

VPN クライアント ドライバ エラーの修復

上記の手順を実行すると、カタログが破損していないことが示される場合がありますが、キーファイルが無署名のもので上書きされた可能性があります。障害が解消されない場合は、ドライバ署名のデータベースの破損原因を特定するためにMicrosoftに依頼してケースをオープンしてください。

手順

ステップ1 コマンド プロンプトを管理者として開きます。

ステップ2 **net stop CryptSvc** と入力します。

ステップ3 **esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb** と入力してデータベースを分析し、そのデータベースの妥当性を検証するか、%/WINDIR%\system32\catroot2 ディレクトリの名前を catroot2_old に変更します。

ステップ4 プロンプトが表示されたら、[OK] を選択して修復を試行します。コマンド プロンプトを終了し、リブートします。

ドライバのクラッシュ

VPNVA.sys でのドライバ クラッシュの修復

問題：VPNVA.sys ドライバがクラッシュします。

解決策：AnyConnect 仮想アダプタにバインドされている中間ドライバを検索し、オフにしてください。

vpnagent.exe でのドライバ クラッシュの修復

手順

ステップ 1 c:\vpnagent という名前のディレクトリを作成します。

ステップ 2 タスク マネージャの [プロセス（process ）] タブを調べ、vpnagent.exe のプロセスの PID を判別します。

ステップ 3 コマンドプロンプトを開き、デバッグ ツールをインストールしたディレクトリに移動します。デフォルトでは、Windows のデバッグ ツールは `C:\Program Files\Debugging Tools` にあります。

ステップ 4 **cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst** と入力します。ここで、*PID* は **vpnagent.exe** の PID です。

ステップ 5 オープン ウィンドウを最小化した状態で実行します。モニタリングしている間は、システムをログオフできません。

ステップ 6 クラッシュが発生すると、c:\vpnagent の中身を zip ファイルに収集します。

ステップ 7 **!analyze -v** を使用して、crashdmp ファイルをさらに診断します。

Network Access Manager に関するリンク/ドライバの問題

Network Access Managerが有線接続のアダプタの認識に失敗した場合は、ネットワーク ケーブルのプラグを抜き、もう一度差し込んでみてください。これでうまくいかない場合は、リンクに問題がある可能性があります。Network Access Managerがアダプタの適切なリンク ステートを判別できない可能性があります。NIC ドライバの接続プロパティを確認してください。[詳細（Advanced）] パネルに [リンクを待機（Wait for Link）] オプションが表示される場合があります。この設定がオンになっている場合、有線接続の NIC ドライバの初期化コードは、自動ネゴシエーションが完了するまで待機してから、リンクが存在するかどうかを判別します。

その他のクラッシュ

AnyConnect のクラッシュ

問題：リブート後に「システムは重大なエラーから回復しました（the system has recovered from a serious error）」というメッセージを受け取りました。

解決策：%temp% ディレクトリ（C:\DOCUME~1\jsmith\LOCALS~1\Temp など）から .log および .dmp の生成済みファイルを収集します。ファイルをコピーするか、またはバックアップします。「.log ファイルまたは .dmp ファイルのバックアップ方法」を参照してください。

.log ファイルまたは .dmp ファイルのバックアップ方法

手順

ステップ 1 [スタート（Start）] > [ファイル名を指定して実行（Run）] メニューからワトソン博士（Drwtsn32.exe）という Microsoft ユーティリティを実行します。

ステップ 2 次のように設定し、[OK] をクリックします。

```
Number of Instructions     : 25
Number of Errors to Save : 25
Crash Dump Type   : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

ステップ 3 クライアントデバイス で [スタート（Start）] > [実行（Run）] メニューの順に選択し、**eventvwr.msc /s** と入力して、Windows イベントビューアから AnyConnect VPN クライアントログを取得します。

ステップ 4 [アプリケーションとサービスログ（Applications and Services Logs）]（Windows）で、AnyConnect を見つけ、[ログファイルの名前を付けて保存...（Save Log File As...）] を選択します。. .evt ファイル形式のファイル名（例：AnyConnectClientLog.evt）を割り当てます。

AnyConnectがvpndownloaderでクラッシュする（LayeredServiceProvider（LSP）モジュールおよび NOD32 AV）

問題：LSP または NOD32 AV を使用している場合、AnyConnect は、接続を確立しようとした際、認証に成功し、SSL セッションを構築するものの、その後 vpndownloader でクラッシュします。

解決策：ESET NOD32 AV のバージョン 2.7 で Internet Monitor コンポーネントを削除し、バージョン 3.0 にアップグレードしてください。

ブルー スクリーン（AT & T Dialer）

問題：AT&T Dialer を使用している場合に、クライアント オペレーティング システムでブルースクリーンが発生して、ミニ ダンプファイルが作成されることがあります。

解決策：AT&T Global Network Client を最新の 7.6.2 にアップグレードしてください。

セキュリティの警告

Microsoft Internet Explorer のセキュリティの警告

問題：Microsoft Internet Explorer で、[セキュリティアラート（security alert）] ウィンドウが表示され、次のテキストが示されます。

```
Information you exchange with this site cannot be viewed or changed by others. However,
 there is a problem with the site's security certificate. The security certificate was
issued by a company you have not chosen to trust. View the certificate to determine
whether you want to trust the certifying authority.
```

解決策：このアラートは、信頼済みサイトとして認識されていない Cisco Secure Firewall ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

「不明な機関による認証」アラート

問題：「不明な機関による Web サイト認証」アラート ウィンドウがブラウザに表示されることがあります。[セキュリティの警告（Security Alert）] ウィンドウの上半分に、次のテキストが表示されます。

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解決策：このセキュリティアラートは、信頼済みサイトとして認識されていない Cisco Secure Firewall ASA に接続すると表示されることがあります。このアラートを回避するには、クライアントに信頼できるルート証明書をインストールします。「クライアントでの信頼できるルート証明書のインストール」を参照してください。

クライアントでの信頼できるルート証明書のインストール

始める前に

信頼できるルート証明書として使用する証明書を生成または取得します。

（注） クライアントで信頼できるルート証明書として自己署名証明書をインストールすることによって、短期的にセキュリティ証明書の警告を回避できます。ただし、これはお勧めしません。理由は、ユーザが誤って不正なサーバー上の証明書を信頼するようにブラウザを設定する可能性があるため、また、ユーザがセキュア ゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

手順

ステップ 1 [セキュリティの警告（Security Alert）] ウィンドウの [証明書の表示（View Certificate）] をクリックします。

ステップ 2 [証明書のインストール（Install Certificate）] をクリックします。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] を選択します。

ステップ 5 [参照（Browse）] をクリックします。

ステップ 6 ドロップダウン リストで、[信頼されたルート証明機関（Trusted Root Certification Authorities）] を選択します。

ステップ 7 [証明書のインポート（Certificate Import）] ウィザードのプロンプトに従って続行します。

接続のドロップ

有線接続が導入された場合のワイヤレス接続のドロップ（Juniper Odyssey クライアント）

問題：Odyssey クライアントでワイヤレスサプレッションが有効である場合、有線接続が導入されると、ワイヤレス接続がドロップします。ワイヤレス サプレッションが無効である場合、ワイヤレス機能は期待どおりに動作する。

解決策：Odyssey クライアントの設定。

Odyssey クライアントの設定

手順

ステップ 1 [ネットワーク接続（Network Connections）] で、アダプタの名前を接続プロパティの表示どおりにコピーします。レジストリを編集する場合、誤って変更すると重大な問題が発生する可能性があるため、バックアップを実行してから、細心の注意を払って変更してください。

ステップ 2 レジストリを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual に移動します。

ステップ 3 virtual の下に新しい文字列値を作成します。アダプタの名前をネットワーク プロパティからレジストリ部分にコピーします。追加のレジストリ設定を保存すると、MSI が作成されて他のクライアントにプッシュされたときに、この設定が移植されます。

Cisco Secure Firewall ASA への接続に失敗（Kaspersky AV Workstation 6.x）

問題：Kaspersky 6.0.3 がインストールされると（無効であっても）、CSTP state＝CONNECTED の直後に Cisco Secure Firewall ASA への AnyConnect 接続が失敗します。次のメッセージが表示されます。

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway
(proxy authentication, handshake, bad cert, etc.).
```

解決策：Kaspersky をアンインストールし、Kaspersky のフォーラムを参照して追加のアップデートがないか確認してください。

UDP DTLS 接続なし（McAfee Firewall 5）

問題：McAfee Firewall 5 を使用しているときに、UDP DTLS 接続を確立できません。

解決策：McAfee Firewall のセンターコンソールで、[高度なタスク（Advanced Tasks）] > [高度なオプションとロギング（Advanced options and Logging）] を選択し、McAfee Firewall の [着信フラグメントを自動的にブロック（Block incoming fragments automatically）] チェックボックスをオフにします。

ホスト デバイスへの接続に失敗（Microsoft ルーティングとリモート アクセス サーバ）

問題：RRAS を使用している場合に、AnyConnect がホストデバイスへの接続を確立しようとすると、イベントログに次の終了エラーが返されます。

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service “Routing and Remote Access” is incompatible with the AnyConnect
Secure Mobility Client.
```

解決策：RRAS サービスを無効にします。

接続障害/クレデンシャル不足（ロード バランサ）

問題：ログイン情報がないために、接続が失敗します。

解決策：サードパーティ製ロードバランサでは、Cisco Secure Firewall ASA デバイスにかかる負荷を把握できません。一方、ASA のロードバランス機能は非常にインテリジェントで、VPN の負荷をデバイス全体で均等に分散できるため、Cisco Secure Firewall ASA 内蔵のロードバランシングを使用することをお勧めします。

インストールの失敗

AnyConnect がダウンロードに失敗する（Wave EMBASSY Trust Suite）

問題：AnyConnect がダウンロードに失敗し、次のエラーメッセージが表示されます。

"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."

ソリューション：dll の問題をすべて解決するために、パッチアップデートをバージョン 1.2.1.38 に更新してください。

非互換性の問題

ルーティング テーブルの更新に失敗（Bonjour Printing Service）

問題：Bonjour Print Service を使用している場合に、AnyConnect イベント ログに IP 転送テーブルの識別に失敗したことが示されます。

解決策：コマンドプロンプトで **net stop "bonjour service"** と入力し、Bonjour Print Service を無効にします。mDNSResponder の新しいバージョン（1.0.5.11）が Apple から提供されています。この問題を解決するために、Bonjour の新しいバージョンが iTunes にバンドルされ、個別のダウンロードとして Apple の Web サイトで配布されています。

TUN のバージョンに互換性がない（OpenVPN クライアント）

問題：このバージョンの TUN がこのシステムにすでにインストールされていて、AnyConnect と互換性がないことを示すエラーが表示されます。

解決策：Viscosity OpenVPN Client をアンインストールします。

Winsock カタログの競合（LSP 症状 2 競合）

問題：クライアント上に LSP モジュールが存在する場合、Winsock カタログが競合することがあります。

解決策：LSP モジュールをアンインストールしてください。

データ スループット低下（LSP 症状 3 競合）

問題：Windows で NOD32 Antivirus V4.0.468 x64 を使用すると、データスループットが低下する場合があります。

解決策：SSLプロトコルスキャンを無効にします。「SSLプロトコルスキャンの無効化」を参照してください。

SSL プロトコル スキャンの無効化

手順

ステップ 1 [詳細設定（Advanced Setup）] の **[プロトコルフィルタリング（Protocol Filtering）]** > **[SSL]** を選択し、SSL プロトコルスキャンを有効にします。

ステップ 2 **[Webアクセス保護（Web access protection）]** > **[HTTP, HTTPS]** の順に選択し、[HTTPSプロトコルチェックを使用しない（Do not use HTTPS protocol checking）] をオンにします。

ステップ 3 **[プロトコルフィルタリング（Protocol Filtering）]** > **[SSL]** に戻り、**SSL プロトコルスキャン**を無効にします。

DPD 障害（EVDO ワイヤレス カードおよび Venturi ドライバ）

問題：クライアントの接続解除中に、EVDO ワイヤレスカードおよび Venturi ドライバを使用すると、イベントログに次のことが報告されます。

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
 DPD failure.
```

ソリューション：

- アプリケーション、システム、および AnyConnect の各イベントログに関係する接続解除イベントがないか確認すると同時に、NIC カードのリセットが適用されたかどうか判別してください。
- Venturi ドライバが最新のものであるか確認してください。AT&T Communications Manager バージョン 6.7 の [ルール エンジンの使用（Use Rules Engine）] を無効にします。

DTLS トラフィック障害（DSL ルータ）

問題：DSL ルータに接続している場合、正常にネゴシエーションされても、DTLS トラフィックが失敗することがあります。

解決策：工場出荷時の設定を使用して Linksys ルータに接続してください。この設定により、DTLS セッションが安定し、ping で中断が発生しません。DTLS リターン トラフィックを許可するルールを追加してください。

NETINTERFACE_ERROR（CheckPoint と、Kaspersky などの他のサードパーティ製ソフトウェア）

問題：SSL 接続に使用されるコンピュータ ネットワークのオペレーティング システム情報を取得しようとしたときに、セキュア ゲートウェイへの接続を完全には確立できなかったことが AnyConnect ログに示されることがあります。

ソリューション：

- 整合性エージェントをアンインストールしてから AnyConnect をインストールする場合は、TCP/IP を有効にしてください。
- 整合性エージェントのインストール時に SmartDefense を無効にすると、TCP/IP がチェックされます。
- サードパーティ製のソフトウェアがネットワーク インターフェイス情報の取得中に、オペレーティング システムの API コールを代行受信またはブロックしている場合は、疑わしい AV、FW、AS などがないか確認してください。
- デバイスマネージャに AnyConnect アダプタのインスタンスが 1 つだけ表示されていることを確認してください。インスタンスが 1 つだけの場合は、AnyConnect で認証し、5 秒後にデバイスマネージャからアダプタを手動で有効にしてください。
- 疑わしいドライバが AnyConnect アダプタ内で有効にされている場合は、これらのドライバを [AnyConnect 接続（Cisco AnyConnect VPN Client Connection）] ウィンドウでオフにして無効にしてください。

パフォーマンスの問題（Virtual Machine Network Service ドライバ）

問題：一部の Virtual Machine Network Service デバイスで AnyConnect を使用しているときに、パフォーマンスの問題が発生しました。

解決策：AnyConnect 仮想アダプタ内のすべての IM デバイスに対するバインドをオフにしてください。アプリケーション dsagent.exe は、C:\Windows\System\dgagent にあります。これはプロセス リストに表示されませんが、TCPview（sysinternals）でソケットを開くと表示できます。このプロセスを終了すると、AnyConnect が正常の動作に戻ります。

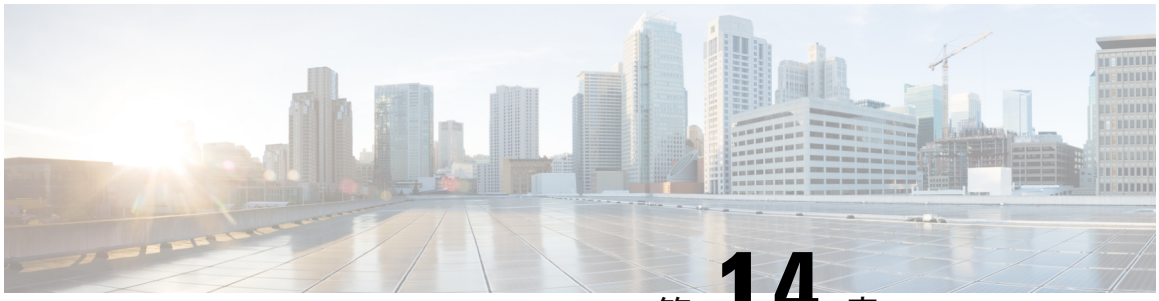
既知のサードパーティ製アプリケーション競合

次のサードパーティ アプリケーションは、AnyConnect Secure Mobility Client との間に既知の複雑な問題があります。

- Adobe および Apple：Bonjour Print Service
    - Adobe Creative Suite 3
    - BonJour Print Service

  - iTunes

- AT&T Communications Manager バージョン 6.2 および 6.7
  - AT&T Sierra Wireless 875 カード
- AT&T Global Dialer
- Citrix Advanced Gateway Client バージョン 2.2.1
- ファイアウォールとの競合
  - サードパーティ製のファイアウォールが、Cisco Secure Firewall ASA グループポリシーで設定されたファイアウォール機能と干渉する可能性があります。
- Juniper Odyssey Client
- Kaspersky AV Workstation 6.x
- McAfee Firewall 5
- Microsoft Internet Explorer 8
- Microsoft Routing and Remote Access Server
- OpenVPN クライアント
- ロード バランサ
- Wave EMBASSY Trust Suite
- Layered Service Provider（LSP）モジュールおよび NOD32 AV
- EVDO ワイヤレスカードおよび Venturi ドライバ
- DSL ルータ
- CheckPoint と、Kaspersky など他のサードパーティ製ソフトウェア
- Virtual Machine Network Service ドライバ



第 14 章

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

macOS 11 用の AnyConnect 4.9.04xxx 以降を実行している必要があります。macOS で使用可能なシステム拡張フレームワークを利用します。以前はカーネル拡張フレームワークを使用していましたが、現在は廃止されています。この変更により、管理者は AnyConnect システム拡張を承認する必要があり、これらの更新で正しい動作を確保できます。また、重大なシステム拡張（または関連する OS フレームワーク）の問題が発生した場合は、最終的な回避策として、AnyConnect カーネル拡張にフェールオーバーするための手順に従うことができます。ただし、この拡張はこの目的のためだけにインストールされ、デフォルトでは使用されなくなりました。

AnyConnect のシステム拡張について

AnyConnect は、macOS 11（およびそれ以降のバージョン）で AnyConnect ソケットフィルタという名前のアプリケーションにバンドルされたネットワークシステム拡張を使用しますこのアプリケーションは拡張のアクティブ化と非アクティブ化を制御するものであり、/Applications/Cisco にインストールされます。

AnyConnect 拡張には、macOS の [システム環境設定（System Preferences）] > [ネットワークUI（Network UI）] ウィンドウに表示される次の 3 つのコンポーネントがあります。

- DNS プロキシ
- アプリケーション/トランスペアレントプロキシ
- コンテンツフィルタ

AnyConnect が適切に動作するには、そのシステム拡張とそのすべてのコンポーネントがアクティブである必要があります。これは、前述のコンポーネントがすべて存在し、macOS ネットワークの UI の左側のペインに緑色（実行中）で表示されていることで確認できます。

AnyConnect のシステム機能拡張の許可

macOS 11 以降では、システム拡張を実行する前に、エンドユーザーによる拡張の承認、またはエンドユーザーの承認なしの MDM 承認が必要です。AnyConnect のシステム拡張には 2 つの承認が必要です。

- システム拡張のロード/アクティブ化の承認 （380 ページ）
- MDM を使用したシステム拡張の許可 （381 ページ）

システム拡張のロード/アクティブ化の承認

AnyConnect のシステム拡張とそのコンテンツ フィルタ コンポーネントは、OS プロンプトに従うか、またはより明示的に AnyConnect 通知アプリケーションの指示に従って承認します。

手順

ステップ 1 AnyConnect 通知アプリケーションの [環境設定を開く（Open Preferences）] ボタンをクリックするか、「システム拡張機能がブロックされました（System Extension Blocked）」というアプリケーションメッセージが表示された場合は、[セキュリティの環境設定を開く（Open Security Preferences）] ボタンをクリックします。システム設定アプリケーションに移動して、[セキュリティとプライバシー（Security&Privacy）] ウィンドウに移動することもできます。

ステップ 2 左下のロックをクリックし、要求されたクレデンシャルを入力してロックを解除し、変更を許可します。

ステップ 3 [セキュリティとプライバシー（Security & Privacy）] ウィンドウで [許可（Allow）] をクリックして、AnyConnect ソケットフィルタを受け入れます。

複数のシステム拡張が承認を必要とする場合、ボタンには [詳細...（Details...）] ラベルが付いています。。この場合、[詳細...（Details...）] をクリックし、[AnyConnectソケットフィルタ（Socket Filter）] チェックボックスをオンにして、[OK] をクリックし、許可を必要とする後続のプロンプトを承認します。

次のタスク

拡張のコンテンツ フィルタ コンポーネントが承認されると、通知が届きます。

MDM を使用したシステム拡張の許可

AnyConnectのシステム拡張を、エンドユーザーが操作することなく、次の設定で管理プロファイルの SystemExtensions ペイロードを使用して承認します。

プロパティ	値
チーム識別子	DE8Y96K9QP
バンドル識別子	com.cisco.anyconnect.macos.acsockext
システム拡張タイプ	NetworkExtension

次の WebContentFilter ペイロード設定を使用して、拡張のコンテンツ フィルタ コンポーネントを承認します。

プロパティ	値
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	ファイアウォール
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
PluginBundleID	com.cisco.anyconnect.macos.acsockext
VendorConfig	
UserDefinedName	Cisco AnyConnect コンテンツフィルタ

AnyConnect システム拡張のアクティブ化の確認

AnyConnect システム拡張が承認され、アクティブになっていることを確認するには、**systemextensionsctl list** コマンドを実行します。

```
% systemextensionsctl list
1 extension(s)
```

```
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsockext
(4.9.03038/4.9.03038) Cisco AnyConnect Socket Filter Extension
[activated enabled]
```

また、[システム設定（System Preferences）] ネットワーク UI を確認して、3 つの AnyConnect 拡張コンポーネントがすべてアクティブであることを確認することもできます。

AnyConnect システム拡張機能を無効にする

AnyConnect のアンインストール時に、ユーザーはシステム拡張の非アクティブ化を承認するための管理者クレデンシャルの入力を求められます。macOS 12（およびそれ以降のバージョン）では、RemovableSystemExtensions プロパティを SystemExtensions ペイロードに追加し管理プロファイルを展開した後、AnyConnect システム拡張をサイレントに削除できます。このプロパティには、AnyConnect システム拡張（com.cisco.anyconnect.macos.acsockext）のバンドル識別子が含まれている必要があります。

（注） 注：この管理プロファイル構成は、管理者が AnyConnect のアンインストールを自動化する場合にのみ使用する必要があります。これにより、root 権限を持つすべてのユーザーまたはプロセスに、ユーザーにパスワードの入力を求めずに AnyConnect システム拡張を削除する機能が付与されます。

カーネル拡張へのフェールオーバー

AnyConnect は引き続き macOS 11 にカーネル拡張をインストールします。ただし、重大なシステム拡張（または関連する OS フレームワーク）の問題が発生した場合、または Cisco Technical Assistance Center（TAC）による指示があった場合のフォールバックとしてのみ使用してください。カーネル拡張は、macOS 11 以降にロードする前に MDM による承認が必要です。エンドユーザの承認はオプションではなくなりました。

始める前に

これらの手順は、最終的な回避策としてのみ使用してください。

手順

ステップ 1 AnyConnect カーネル拡張は、次の設定で管理プロファイルの *SystemPolicyKernelExtensions* ペイロードを使用して承認します。

プロパティ	値
チーム識別子	DE8Y96K9QP

プロパティ	値
バンドル識別子	com.cisco.kext.acsock

MDM 設定プロファイルがインストールされます。

ステップ 2 次のコマンドを実行すると、AnyConnect によってシステム拡張が非アクティブ化され、代わりにカーネル拡張の使用が開始されます。管理者クレデンシャルの入力を求められます。**% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && /Applications/Cisco/Cisco\ AnyConnect\ Socket\ Filter.app/Contents/macOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt && echo kext=1 | sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist**

ステップ 3 次のコマンドを実行して、カーネル拡張がロードされたことを確認します：**% kextstat | grep com.cisco.kext.acsock**

AnyConnect がカーネル拡張のロードに失敗した場合は、リブートを実行します。

システム拡張に戻る

Cisco TAC がシステム拡張の問題の修正を確認した場合（およびカーネル拡張へのフェールオーバーの必要性がなくなった場合）、次のコマンドを実行して AnyConnect にシステム拡張に切り替えるように指示します。

```
% sudo launchctl unload /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist &&
sudo kextunload -b com.cisco.kext.acsock && sudo rm /opt/cisco/anyconnect/acsock.cfg &&
 sudo launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

修正を適用した AnyConnect または macOS バージョンをインストールします。

AnyConnect システムとカーネル拡張の承認のためのサンプル MDM 設定プロファイル

次の MDM 設定プロファイルを使用して、システム拡張のコンテンツ フィルタ コンポーネントを含む AnyConnect システム拡張とカーネル拡張の両方をロードできます。

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

      <dict>

      <key>PayloadContent</key>

      <array>

            <dict>
```

```
        <key>AllowUserOverrides</key>
        <true/>
        <key>AllowedKernelExtensions</key>
        <dict>
            <key>DE8Y96K9QP</key>
            <array>
            <string>com.cisco.kext.acsock</string>
            </array>
        </dict>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>AnyConnect Kernel Extension</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadType</key>
        <string>com.apple.syspolicy.kernel-extension-policy</string>
        <key>PayloadUUID</key>
        <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
    </dict>
    <dict>
        <key>AllowUserOverrides</key>
        <true/>
        <key>AllowedSystemExtensions</key>
        <dict>
            <key>DE8Y96K9QP</key>
```

```
                <array>
                <string>com.cisco.anyconnect.macos.acsockext</string>
                </array>
        </dict>
        <key>PayloadDescription</key>
        <string></string>
        <key>PayloadDisplayName</key>
        <string>AnyConnect System Extension</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadType</key>
        <string>com.apple.system-extension-policy</string>
        <key>PayloadUUID</key>
        <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
<dict>
        <key>Enabled</key>
        <true/>
        <key>AutoFilterEnabled</key>
        <false/>
        <key>FilterBrowsers</key>
        <false/>
        <key>FilterSockets</key>
        <true/>
        <key>FilterPackets</key>
        <false/>
```

```
                        <key>FilterType</key>

                        <string>Plugin</string>

                        <key>FilterGrade</key>

                        <string>firewall</string>

                        <key>PayloadDescription</key>

                        <string></string>

                        <key>PayloadDisplayName</key>

                        <string>Cisco AnyConnect Content Filter</string>

                        <key>PayloadIdentifier</key>


<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>

                        <key>PayloadType</key>

                        <string>com.apple.webcontent-filter</string>

                        <key>PayloadUUID</key>

                        <string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>

                        <key>PayloadVersion</key>

                        <integer>1</integer>

                        <key>FilterDataProviderBundleIdentifier</key>

                        <string>com.cisco.anyconnect.macos.acsockext</string>

                        <key>FilterDataProviderDesignatedRequirement</key>

                        <string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate
leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string>

                        <key>PluginBundleID</key>

                        <string>com.cisco.anyconnect.macos.acsock</string>

                        <key>UserDefinedName</key>

                        <string>Cisco AnyConnect Content Filter</string>

                </dict>

        </array>

        <key>PayloadDescription</key>

        <string></string>

        <key>PayloadDisplayName</key>
```

```
        <string>Approved AnyConnect System and Kernel Extensions</string>
        <key>PayloadEnabled</key>
        <true/>
        <key>PayloadIdentifier</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadOrganization</key>
        <string>Cisco Systems, Inc.</string>
        <key>PayloadRemovalDisallowed</key>
        <true/>
        <key>PayloadScope</key>
        <string>System</string>
        <key>PayloadType</key>
        <string>Configuration</string>
        <key>PayloadUUID</key>
        <string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
</dict>
</plist>
```