Cisco Secure Client とインストーラのカスタマイズとローカライズ

Cisco Secure Client のインストール動作の変更

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。Cisco Secure Client 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 Secure 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、Cisco Secure Client に手動で展開できます。結果を確認するには、[Cisco Secure Client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：secureclient-vpn-transforms-X.X.xxxxx.zip から、secureclient-win-disable-customer-experience-feedback.mst を抽出します。

インストール動作の変更、Windows

Cisco Secure Client 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。

（注） Cisco Secure Client は、Windows インストーラの ADVERTISE モードをサポートしていません。

- 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

Cisco Secure Client 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、Cisco Secure Client 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 Cisco Secure 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、Cisco Secure Client 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、Cisco Secure 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。

- [プログラムの追加と削除（Add/Remove Program List）] リストでの Cisco Secure Client の非表示：インストールした Cisco Secure Client 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、Cisco Secure 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。

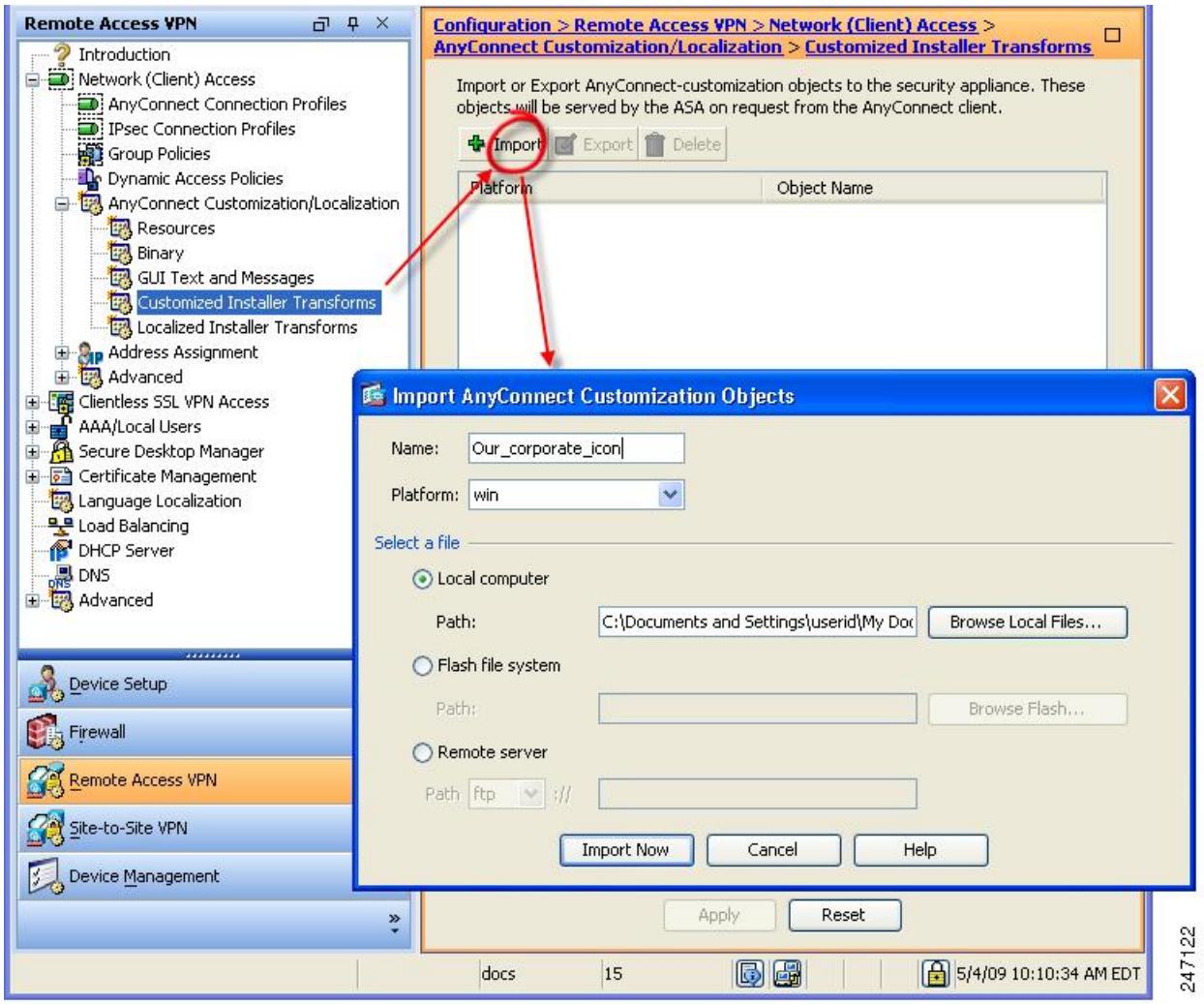
Cisco Secure Firewall 適応型セキュリティアプライアンスへのカスタマイズされたインストーラトランスフォームのインポート

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。

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。

Cisco Secure Client インストーラ画面のローカライズ

Cisco Secure Client 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） Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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。

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

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

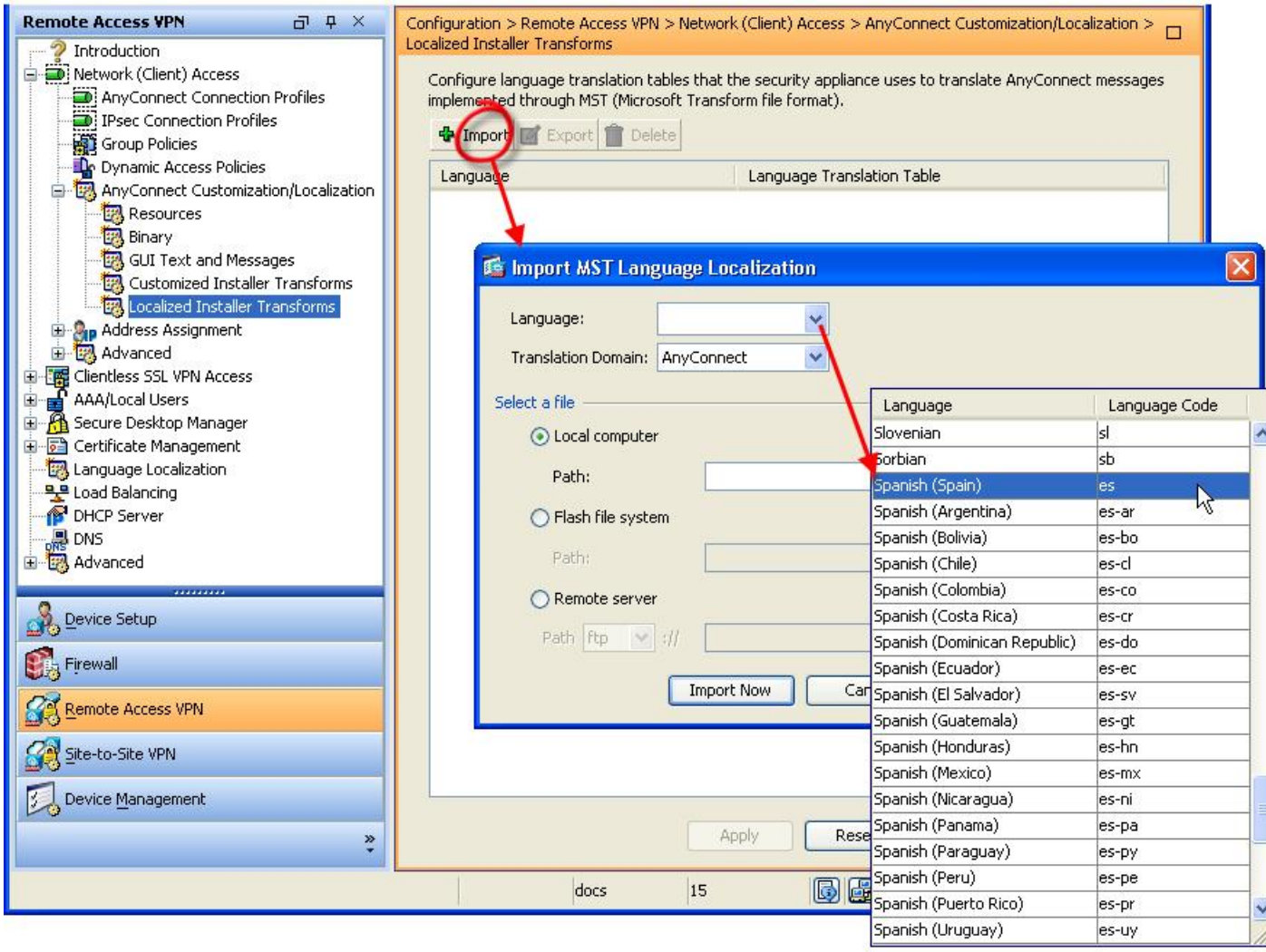
アーカイブには使用可能な翻訳用のトランスフォーム（.mst ファイル）が含まれています。用意されている 30 以外の言語をリモートユーザーに表示する必要がある場合は、独自のトランスフォームを作成し、それを新しい言語として Cisco Secure Firewall ASA にインポートすることができます。Microsoft のデータベース エディタ Orca を使用して、既存のインストレーションおよび新規ファイルを修正できます。Orca は、Microsoft Windows Installer Software Development Kit（SDK）の一部で、Microsoft Windows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

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、Cisco Secure Client 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

Cisco Secure Client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、Cisco Secure Client 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。

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 cisco-secure-client-macosx-version-predeploy-k9.dmg -format UDRW -o
cisco-secure-client-macosx-version-predeploy-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、Cisco Secure Client 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 Configuration Guide』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

Cisco Secure Client 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、Cisco Secure Client 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 Configuration Guide』[英語] を参照してください。

Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client パッケージファイルには、Cisco Secure Client 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。Cisco Secure Client 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、Cisco Secure Client 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 （15 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）

Cisco Secure Client リリース 5.0 では、さまざまな言語のデフォルトのローカリゼーションファイルがインストールに含まれています。デスクトップデバイスでのローカリゼーション （12 ページ） を参照してください。

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。

- Cisco Secure Client 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 （15 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 Cisco Secure Client 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

Cisco Secure Client 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。

デスクトップデバイスでのローカリゼーション

Cisco Secure Client のインストールには、さまざまな言語のデフォルトのローカリゼーション ファイルが含まれています。デバイスで指定されたロケールによって、表示される言語が決まります。Cisco Secure Client 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。

ASA/ASDM で他の言語を設定する必要があります。Cisco Secure Client は ASA から翻訳を取得すると、デフォルトの翻訳を使用して翻訳ギャップを埋めようとします。たとえば、管理者側に翻訳で提供されなかった文字列があり、その文字列がデフォルトの翻訳の一部である場合、Cisco Secure Client は引き続き翻訳します。デフォルトでは、これらの言語のローカリゼーションデータが提供されます。

- カナダフランス語（カナダ）：（fr-CA）
- 中国語（中国）：（zh-CN）
- 中国語（簡体字）：（zh-HANS）
- 中国語（台湾）：（zh-TW）
- 中国語（繁体字）：（zh-HANT）
- チェコ語（チェコ共和国）：（cs_CZ）
- オランダ語（オランダ）：（nl-nNL）
- フランス語（フランス）：（fr_FR）
- ドイツ語（ドイツ）：（de_DE）
- ハンガリー語（ハンガリー）：（hu_HU）
- イタリア語（イタリア）：（it_IT）
- 日本語（日本）：（ja-JP）
- 韓国語（韓国）：（ko-KR）
- ポーランド語（ポーランド）：（pl-PL）
- ポルトガル語（ブラジル）：（pt-BR）
- ロシア語（ロシア）：（ru-RU）
- スペイン語（スペイン）：（es_ES）

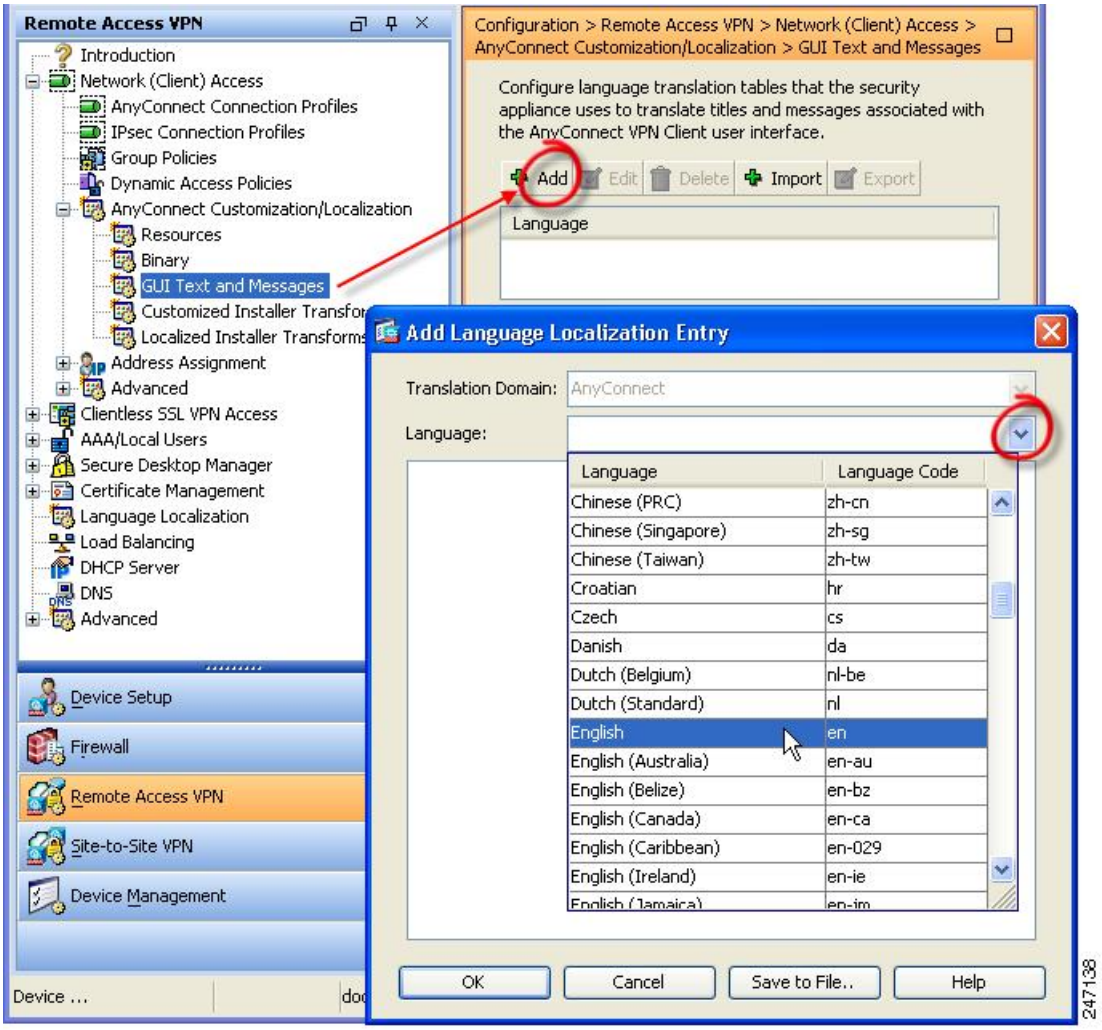
Cisco Secure Client のテキストとメッセージの追加または編集

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、Cisco Secure Client 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。

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。

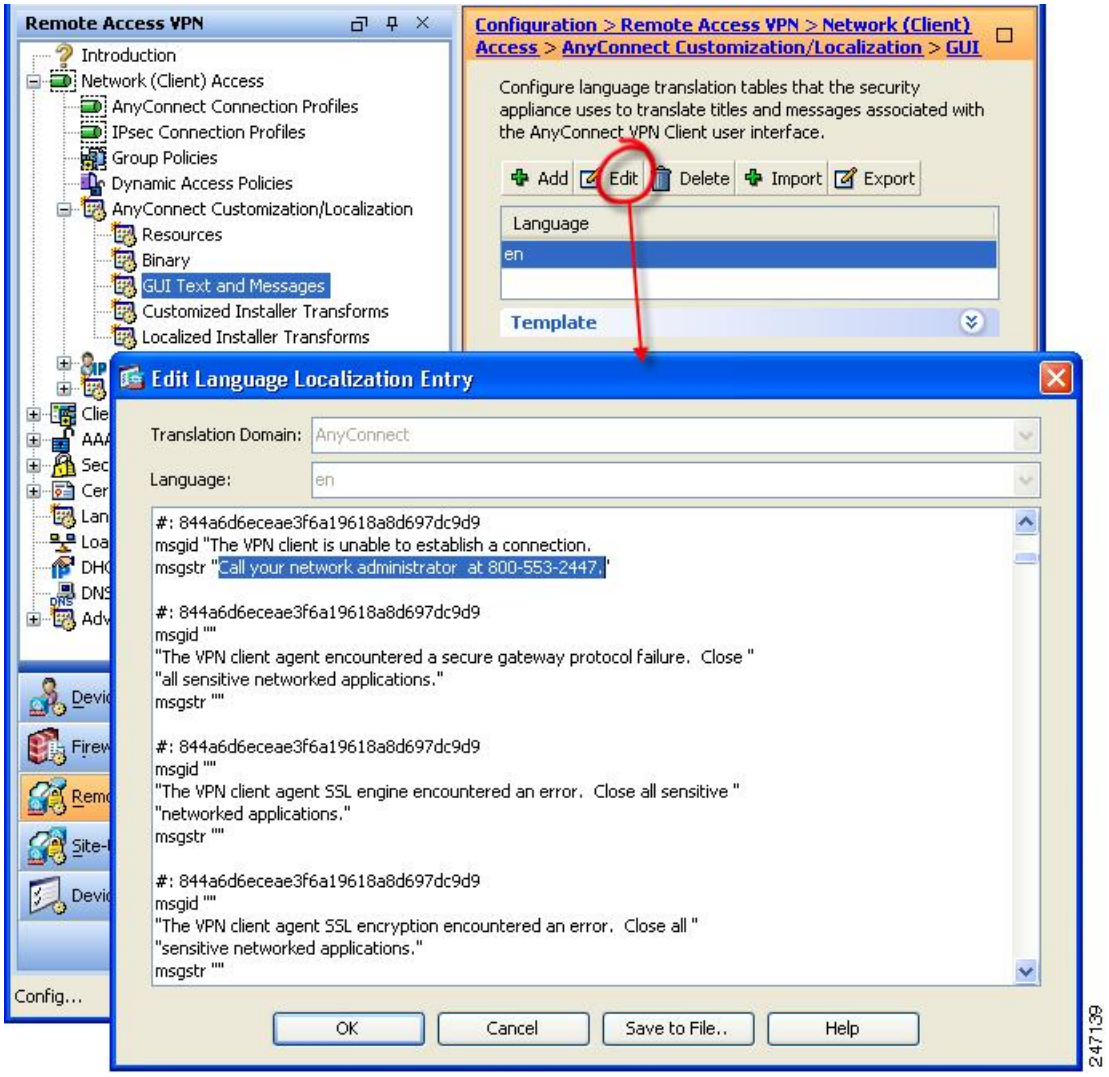


ステップ 3 [言語（Language）] ドロップ リストをクリックし、言語として [英語（en）（English (en)）] を指定します。英語の変換テーブルが、ペインの言語リストに表示されます。

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

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 Cisco Secure Client クライアントに展開されます。ローカリゼーションは、Cisco Secure Client 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 Cisco Secure Client 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。Cisco Secure Client 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。

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

Cisco Secure Client 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 Secure Client\l10n\<LANGUAGE-CODE>\LC_MESSAGES`
- macOS および Linux の場合：`/opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES`

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 Cisco Secure Client がインストールされたコンピュータにある、Cisco Secure Client 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、Cisco Secure Client 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 Cisco Secure Client 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。

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 Cisco Secure Client 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 Cisco Secure Client 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、Cisco Secure Client 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、テンプレートとマージします。 Poedit には、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、Cisco Secure Client 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。

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、Cisco Secure Client 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、Cisco Secure Client 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。

Cisco Secure Client 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 Cisco Secure Client 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、Cisco Secure Client のコア VPN および Network Access Manager Module により使用されます。

制約事項

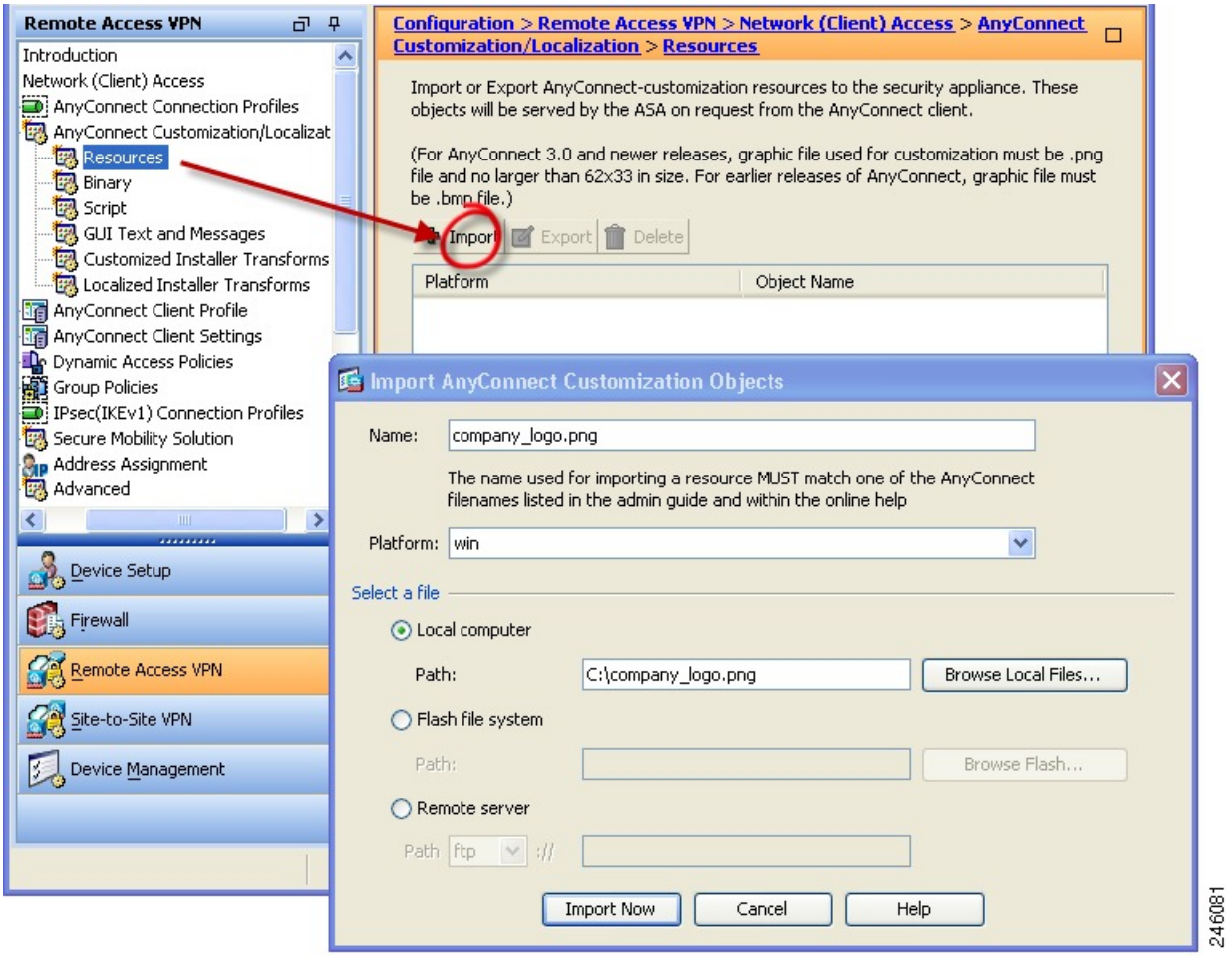
- カスタムコンポーネントのファイル名は、Cisco Secure Client GUI で使用されるファイル名と一致している必要があります。これはオペレーティングシステムによって異なり、macOS および Linux では大文字と小文字が区別されます。たとえば、Windows クライアント用の企業ロゴを置き換えるには、独自の企業ロゴを company_logo.png としてインポートする必要があります。別のファイル名でインポートすると、Cisco Secure Client インストーラはそのコンポーネントを変更しません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合は、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、Cisco Secure Client 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。

Cisco Secure Client 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、Cisco Secure Client をカスタマイズすることができます。

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [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 Cisco Secure Client アイコンとロゴ

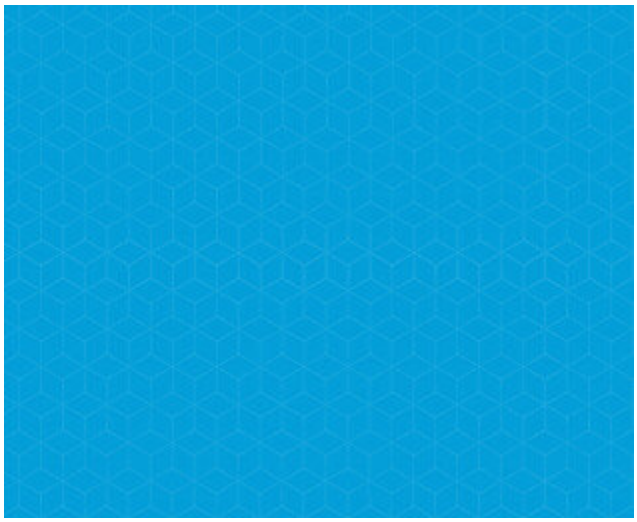
Windows 用のファイルはすべて次の場所に格納されています。

```
%PROGRAMFILES%\Cisco\Cisco Secure 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
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

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_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
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

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
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 Cisco Secure Client 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/secure client/pixmaps
```

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
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

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-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
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

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
vpnui48.png メイン プログラム アイコン。 	48 x 48 PNG

macOS 用 Cisco Secure Client アイコンとロゴ

macOS の Cisco Secure Client アイコンおよび macOS GUI リソースカスタマイズのロゴは現在サポートされていません。

Cisco Secure Client のヘルプファイルを作成してアップロードする

Cisco Secure Client 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 Cisco Secure Client に接続すると、ヘルプファイルがダウンロードされ、Cisco Secure Client 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。

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、Cisco Secure Client 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、Cisco Secure Client 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 Secure Client\Help`
- macOS：`/opt/cisco/secureclient/help`

スクリプトの作成および展開

Cisco Secure Client 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。

Cisco Secure Client 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） Cisco Secure Client 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：Cisco Secure Client 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：Cisco Secure Client 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、Cisco Secure Client 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。 Cisco Secure Client 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。Cisco Secure Client 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：Cisco Secure Client 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、Cisco Secure Client でも正しく実行できません。

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 *1*: スクリプトの所定の場所

OS	ディレクトリ
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco Secure Client\VPN\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/secureclient/vpn/script
macOS	/opt/cisco/secureclient/vpn/script

スクリプトに関する Cisco Secure Client プロファイルの設定

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、Cisco Secure Client 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。

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。

Cisco Secure Client 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、Cisco Secure Client 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。Cisco Secure Client 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 Cisco Secure Client ソフトウェアを展開することはできません。Cisco Secure Firewall ASA に Cisco Secure Client パッケージの最新バージョンを配置すると、Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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、Cisco Secure Client GUI を使用します。
- Start Before Login はサポートされていません。

Cisco Secure Client の CLI コマンドを使用します。

Cisco Secure 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 （33 ページ）
- クライアント CLI コマンドの使用 （33 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 （35 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 (x86)\Cisco\Cisco Secure Clientt 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/secureclient/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、Cisco Secure Client 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/secureclient/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/secureclient/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/secureclient/bin/vpn stats
```

vpn 接続に関する統計情報を表示します。

```
/opt/cisco/secureclient/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 Cisco Secure Client 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 Secure Client>vpncli
Cisco Secure Client (version 5.x).
Copyright (c) 2022 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 Secure Client

- 32 ビット Windows：

  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client

ISE 展開のための Cisco Secure Client カスタマイズおよびローカリゼーションの準備

Cisco Secure Client ローカリゼーションバンドルの準備

Cisco Secure Client ローカリゼーションバンドルは、Cisco Secure Client 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 Cisco Secure Client を展開するために使用される ISE Cisco Secure Client 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 Cisco Secure Client 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、Cisco Secure Client 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。

ステップ 1 Cisco Secure Client 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 Cisco Secure 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 Cisco Secure Client 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）Cisco Secure Client 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 Cisco Secure 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、 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 Cisco Secure Client のバージョンに一致する必要があります。Cisco Secure Client 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）Cisco Secure Client 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 と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 SecureClient-Localization-Bundle-*(release)*.zip、などの適切な名前のファイルに ZIP 圧縮して、Cisco Secure Client ローカリゼーションバンドルを作成します。

次のタスク

Cisco Secure Client 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 Cisco Secure Client の展開に使用されます。

Cisco Secure Client カスタマイゼーション バンドルの準備

Cisco Secure Client カスタマイゼーション バンドルは、カスタム Cisco Secure Client 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 Cisco Secure Client を展開するために使用される ISE Cisco Secure Client 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 Cisco Secure Client 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 Cisco Secure Client 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、「Cisco Secure Client GUI のカスタムアイコンおよびロゴの作成 （18 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。

  - Cisco Secure Client のヘルプファイルを作成するには、「Cisco Secure Client のヘルプファイルを作成してアップロードする （26 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 （27 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 （2 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 （7 ページ）」を参照してください。

始める前に

Cisco Secure Client 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。

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 Cisco Secure Client 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 cisco-secure-client-*version*-core-vpn-lang-webdeploy-k9.zip などの適切な名前のファイルに ZIP 圧縮して、Cisco Secure Client 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

Cisco Secure Client 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 Cisco Secure Client の展開に使用されます。

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