CHAPTER 9

AnyConnect for Apple iOS デバイスの管理

この章では、サポート情報、システム要件、イストール情報だけでなく、AnyConnect 2.5 for Apple iOS デバイス固有のその他管理作業について説明します。

サポートされているモバイル デバイス

AnyConnect 2.5 が動作できる Apple iOS モバイル デバイスのリストについては、『Release Notes for Cisco AnyConnect VPN Client, Release 2.5.x for Apple iOS』の「Apple iOS Devices Supported」を参照してください。

システム要件

サポートされているセキュリティ アプライアンスおよび ASA ソフトウェアのリストについては、『Release Notes for Cisco AnyConnect VPN Client, Release 2.5.x for Apple iOS』の「Security Appliances and Software Supported」を参照してください。

Apple iOS デバイスでサポートされている AnyConnect 機能

このリリースでサポートされている AnyConnect 機能のリストについては、『Release Notes for Cisco AnyConnect VPN Client, Release 2.5.x for Apple iOS』の「New Features in AnyConnect 2.5.4038」および「Other Supported Features」を参照してください。

コネクション パーシステンス機能固有の事項

AnyConnect for Apple iOS は、AnyConnect for Windows、Mac OS X、および Linux に似た認証機能の完全なスイートをサポートしています。

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。デジタル証明書が発行されている場合、AnyConnect はユーザが操作しなくても VPN 接続を確立できる Apple iOS Connect On Demand 機能をサポートしています。ユーザは手動で接続を確立することもできます。

Apple iOS Connect On Demand

Apple iOS Connect On Demand 機能を使用すると、Safari などのアプリケーションで VPN 接続を開始できます。Apple iOS は、アプリケーションが要求したドメインを、*アクティブ*な接続エントリ（横にチェック マークが付いているエントリ）のドメイン リスト内の文字列に対して評価します。

AnyConnect を使用して Apple iOS が評価するドメイン リストを定義します。

- **Never Connect**：Apple iOS は最初に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS はドメイン要求を無視します。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。

（注）　Connect On Demand を有効化すると、AnyConnect によって VPN 設定内のサーバ アドレスが Never Connect リストに追加され、ブラウザを使用してセキュア ゲートウェイに接続したときに VPN 接続が開始されなくなります。この規則をそのままにしておいても、Connect on Demand に悪影響はありません。

- **Always Connect**：Apple iOS は次に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。このリストの最も一般的な用途は、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「`email.example.com`」などのように指定します。
- **Connect if Needed**：Apple iOS は、DNS エラーが発生した場合に、ドメイン要求をこのリストに対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。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。

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 で、*Never Connect* リスト内にドメイン要求と一致する文字列を見つけられない。
- *次のどちらか*の条件を満たしている。
  - Apple iOS で、*Always Connect* リスト内にドメイン要求と一致する文字列を見つけている。
  - DNS ルックアップが失敗し、Apple iOS で、*Connect if Needed* リスト内にドメイン要求と一致する文字列を見つけている。

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が、この規則には、ドメイン文字列の一部または全部をドメイン名として指定できます。

（注）　統合 Apple iOS IPsec クライアントと AnyConnect の両方で同じ Apple iOS VPN on Demand フレームワークが使用されています。

iPad または iPhone のユーザ ガイドの「Configuring Connect-On-Demand Rules」またはこのマニュアル後半にある手順URI ハンドラを使用した VPN 接続エントリの生成を参照してください。

ネットワーク ローミング

パーシステント リコネクトとも呼ばれるネットワーク ローミングは、デバイスが再起動した後、または接続タイプ（EDGE、3G、Wi-Fi など）が変わった後に再接続に必要な時間の制限を確認するかどうかを決定します。シームレスなモビリティにネットワーク全体で続くセキュア接続を実現することは、企業に接続する必要があるアプリケーションに役立ちます。

ネットワーク ローミングがイネーブル化されている状態で AnyConnect の接続が切れた場合、再接続に必要な時間に制限はないため、この機能でバッテリの消耗が早くなる可能性があります。

（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。

VPN トラフィックを制限するポリシーにより、デバイスは企業以外のインターネット リソースにアクセスできません。ネットワーク ローミングがイネーブルになっている場合、パーシステント コネクションをサポートする ASA に対してポリシーが必要です。

ネットワーク ローミングがディセーブルになっている状態で AnyConnect の接続が切れた場合、20 秒間接続を再確立しようとします。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。

デフォルトでは、AnyConnect は VPN 接続ですべてのネットワーク トラフィックを送信します。スプリット トンネリング ポリシーをイネーブルにして、トラフィック フローを制御し、トンネルに該当するトラフィックおよびデータ ネットワークに該当するトラフィックを誘導できます。詳細は、『ASA Configuration Guide』を参照してください。

AnyConnect on iOS デバイスのインストールおよびアップグレード

AnyConnect クライアントのインストール

エンド ユーザは、Apple App Store を開いてアプリをダウンロードすることで AnyConnect Secure Mobility Client for iOS デバイスを他の iPad または iPhone アプリのようにインストールします。AnyConnect クライアント アプリは無償で、次の URL にあります。
http://itunes.apple.com/us/app/cisco-anyconnect/id392790924?mt=8

インストール手順の詳細は、iPhone または iPad のユーザ ガイドの「Installation」を参照してください。

AnyConnect 2.4 から AnyConnect 2.5 へのアップグレード

エンド ユーザは、新しい AnyConnect クライアントを Apple App store からダウンロードすることで AnyConnect 2.4.4 から AnyConnect 2.5.4038 へアップグレードします。

アップグレードの前に次の作業を行う必要があります。

- AnyConnect VPN セッションが確立されている場合は切断する。
- AnyConnect アプリが開いている場合は閉じる。

一連のアップグレード手順については、iPhone または iPad のユーザ ガイドの「Upgrading AnyConnect 2.4 to AnyConnect 2.5 for Apple iOS Devices」を参照してください。

Apple iOS デバイスの AnyConnect クライアント インターフェイス

iPad ユーザ インターフェイスの説明については、『iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5』の「Client User Interface」を参照してください。

iPhone ユーザ インターフェイスの説明については、『iPhone User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5』の「Client User Interface」を参照してください。

AnyConnect App の設定および導入の概要

AnyConnect では、最低でも次の情報を必要とする接続エントリを作成する必要があります。

- 説明：1 つの VPN 接続を別の接続と一意に識別します。
- サーバ アドレス：ASA VPN 設定でグループ URL が指定されている場合の URL パスなど、宛先の完全修飾ドメイン名または IP アドレス。

AnyConnect VPN クライアント プロファイルへのモバイル固有の追加機能

AnyConnect for Apple iOS の以前のリリースでは、ユーザは次の VPN 機能を組み込んだ VPN 接続プロファイルを作成できました。

- ネットワーク ローミング プリファレンス
- 証明書認証方法
- Connect on Demand プリファレンス

現在は AnyConnect 管理者もこれらの機能を AnyConnect VPN クライアント プロファイルで設定し、セキュア ゲートウェイ（ASA）に接続する際にプロファイル ファイルをモバイル デバイスに配信できます。管理者がこれらのプロファイルを作成および配信する場合、エンド ユーザがそれらを変更することはできません。エンド ユーザは、自分が作成した接続プロファイルは変更できます。

AnyConnect VPN クライアント ユーザ プロファイルは、エンドポイントにアクセスできるようにしたいセキュア ゲートウェイ（ASA）のリストを識別できる XML ファイルです。また、AnyConnect VPN クライアント プロファイルは、接続属性および制約をユーザに追加します。

AnyConnect プロファイル エディタを使用して VPN クライアント プロファイル内にクライアント機能を設定し、AnyConnect がセキュア ゲートウェイに VPN 接続を作成する際にこのファイルをアップロードするよう ASA を設定できます。

（注）　AnyConnect は Apple iOS デバイスに一度に 1 つのプロファイルしか保持しません。しかし、プロファイルは複数の接続エントリで構成できます。

VPN クライアント プロファイルのモバイル デバイスの接続設定

Apple iOS デバイスの接続プロファイルを含む VPN クライアント プロファイルを作成するには、プロファイル エディタ 3.0.1047 以降を使用する必要があります。プロファイル エディタはスタンドアロン ツールとして使用でき、Cisco.com からダウンロードできます。

プロファイル エディタをダウンロードしたら、Apple iOS デバイスの接続の設定方法について、『*AnyConnect Secure Mobility Client Administrator Guide, release 3.0*』の「Configuring Connections for Mobile Devices」を参照してください。

Apple iOS 接続エントリを使用して VPN クライアント プロファイルを作成したら、VPN クライアントを ASA にインポートし、グループ ポリシーと関連付ける方法について、「Deploying the AnyConnect Profile」を参照してください。

プロファイル エディタをダウンロードするには、次の手順を実行します。

1. Cisco.com の [AnyConnect Secure Mobility Client] ページに接続し、[Download Software] をクリックします。
2. [All Releases] および **3.0** ディレクトリを展開し、AnyConnect の **3.0.1047** 以降のバージョンを選択します。
3. 右のカラムで **anyconnect-profileeditor-win-<*version*>-k9.exe** という命名規則のファイルを探します。AnyConnect 3.0.1047 でリリースされた AnyConnect プロファイル エディタをダウンロードしていた場合、**anyconnect-profileeditor-win-3.0.1047-k9.exe** が見つかります。
4. [Download now] をクリックし、サイトの手順に従ってダウンロード プロセスを完了します。

推奨する ASA 設定

最高のユーザ エクスペリエンスを体験するため、認証設定に応じてモバイル デバイスに複数のトンネル グループ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。

Connect on Demand が設定されているモバイル デバイスの証明書対応認証トンネル グループについては、トンネル グループには非常に短い（60 秒など）アイドル タイムアウト（vpn-idle-timeout）を指定しておく必要があります。VPN セッションがアプリケーションにとり重要でなく、常に接続している必要がない場合、アイドル タイムアウトを設定する場合があります。これにより Apple デバイスは、デバイスがスリープ モードになった場合など、必要なくなった時点で VPN 接続を閉じることができます。トンネル グループのアイドル タイムアウトのデフォルト値は 60 分です。

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、トンネル グループは 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。

スプリット DNS による DNS 解決動作

ASA スプリット トンネリング機能により、どのトラフィックが VPN トンネルを通り、どのトラフィックを暗号化されずに送信するか指定できます。スプリット DNS と呼ばれる関連機能により、どの DNS トラフィックが VPN トンネルでの DNS 解決に適しているか、またどの DNS トラフィックをエンドポイント DNS リゾルバが処理するか指定できます。

AnyConnect for Apple iOS は、解決する DNS クエリーを指定するオプションの **split-dns** コマンドをサポートしていますが、スプリット トンネル VPN も設定すると、他のデバイスではコマンド動作が異なります。

group-policy コンフィギュレーション モードに入力された **split-dns** コマンドは、次のように VPN セッション経由で解決するドメインをリストしています。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2...
domain-nameN] | none}
```

split-dns コマンドが存在しない場合、グループ ポリシーはデフォルト グループ ポリシーにあるドメインを継承します。スプリット トンネリング ドメイン リストを継承しないようにするには、**split-dns none** コマンドを使用します。

AnyConnect for Apple iOS は、このコマンドに次のように応答します。

- **split-dns** リストのドメインの DNS クエリーのみ暗号化する：AnyConnect はコマンドで指定されたドメインの DNS クエリーのみトンネルし、他のすべての DNS は暗号化せずにローカル DNS リゾルバに送信して、解決します。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 example1.com example2.com
  ```

- **default-domain** コマンドのドメインの DNS クエリーのみ暗号化する：**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している場合、AnyConnect はそのドメインの DNS クエリーのみトンネルし、他のすべての DNS は暗号化せずにローカル DNS リゾルバに送信して、解決します。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 クエリーを暗号化せずに送信する：**split-dns none** コマンドおよび **default-domain none** コマンドがグループ ポリシーに存在する場合、あるいはこれらのコマンドがグループ ポリシーに存在しないが、デフォルト グループ ポリシーに存在する場合、AnyConnect はすべての DNS を暗号化せずにローカル DNS リゾルバに送信して、解決します。

AnyConnect インターフェイスおよびメッセージのローカライズ

リリース 2.5.4038 から、ローカリゼーション サポートが Apple iOS 5 以降を実行するデバイスに追加されます。

Cisco.com の製品ダウンロード センターに、ローカライズ可能なすべての AnyConnect 文字列を含む **anyconnect.po** ファイルが提供されています。AnyConnect 管理者は anyconnect.po ファイルをダウンロードし、使用できる文字列を変換して、ファイルを ASA にアップロードできます。

最初に AnyConnect ユーザ インターフェイスおよびメッセージが米国語でユーザに表示されます。エンド ユーザが初めて ASA への接続を確立すると、AnyConnect は [Settings] > [General] > [International] > [Language] の Apple iOS デバイスで設定された、デバイスが選択した言語と ASA で使用できるローカリゼーション言語を比較します。一致するローカリゼーション ファイルが見つかると、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 インターフェイスおよびユーザ メッセージを表示します。文字列が変換されなかった場合、最初に提供されたデフォルト文字列が表示されます。

手順の詳細

ステップ 1　[Select a Product] ページから開始します。

ステップ 2　[Products] > [Security] > [Virtual Private Networks (VPN)] > [Cisco VPN Clients] > [Cisco AnyConnect Secure Mobility Client] を選択します。

ステップ 3　リリース フォルダ ツリーの **All Releases** フォルダを展開し、**3.0** を展開し、最新の AnyConnect 3.0 リリースのフォルダを開きます。

ステップ 4　ダウンロード可能なファイルのリストで、**anyconnect.po** を見つけ、[Download Now] をクリックします。

ステップ 5　プロンプトに従ってファイルをダウンロードします。

ステップ 6　「AnyConnect クライアントの GUI とインストーラのローカライズ」（P.7-15）に進みます。

URI ハンドラによるローカリゼーション ファイルのインポート

この URI ハンドラ方法を使用して、ローカリゼーション ファイルを AnyConnect クライアントに配布できます。Apple iOS デバイスは Apple iOS 5 以降を実行している必要があります。詳細については、「URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズ」（P.9-16）を参照してください。

ローカリゼーションのクリア

AnyConnect アプリをそのデフォルト テキスト文字列に戻すには、次の手順に従います。

ステップ 1　[AnyConnect icon] をホーム画面でタップします。

ステップ 2　[Diagnostics] をタップします。

ステップ 3　[Clear Localization Data] をタップします。

すべてのローカリゼーション データおよびすべての UI が削除され、メッセージ テキストはデフォルト設定に戻ります。

Apple iOS デバイスへの証明書のインストール

証明書を使用してモバイル デバイスをセキュア ゲートウェイに認証するには、エンド ユーザは証明書をデバイスにインポートし、その証明書を接続エントリと関連付ける必要があります。Apple iOS デバイスに証明書をインポートする場合に使用できる 3 種類の方法を次に紹介します。

- 電子メールに添付された証明書のインポートとインストール
- ハイパーリンクからの証明書のインポートとインストール
- SCEP 設定接続エイリアスによる証明書のインポートとインストール

iPhone または iPad のユーザ ガイドの「Installing a Certificate on Your Mobile Device」を参照してください。

セキュア ゲートウェイでのモバイル ポスチャの設定

モバイル デバイスの次の属性に基づき Dynamic Access Policies（DAP; ダイナミック アクセス ポリシー）を設定できます。

- Client Version：AnyConnect クライアント バージョン
- Platform：Android および Apple iOS などのオペレーティング システム

- Platform Version：オペレーティング システム バージョン番号
- Device Type：iPad または Samsung GT-I9000 などのモバイル デバイス タイプ
- Device Unique ID：モバイル デバイスの一意の ID

手順の詳細については、『*Cisco 5500 Series Configuration Guide using ASDM, 6.4*』の「Adding Mobile Posture Attributes to a DAP」または『*Cisco Security Appliance Configuration Guide using ASDM, 6.2*』の「Add/Edit Endpoint Attributes」を参照してください。

Apple iOS デバイスでの SSL VPN 接続の禁止

Apple iOS SSL VPN 接続をサポートするよう AnyConnect Mobile ライセンスで ASA をアクティブにしておく必要があります。ASA が AnyConnect Mobile ライセンスでアクティブになっていない場合、接続は自動的に拒否されます。

デフォルトでは、AnyConnect Mobile ライセンスでアクティブになった ASA により、認証できるユーザは AnyConnect を実行している Apple iOS デバイスからログインできます。これらの接続を行わないよう ASA を設定できます。

これらの接続を行わないよう ASA を設定できますが、設定するには、この時点で次の両方が必要になります。

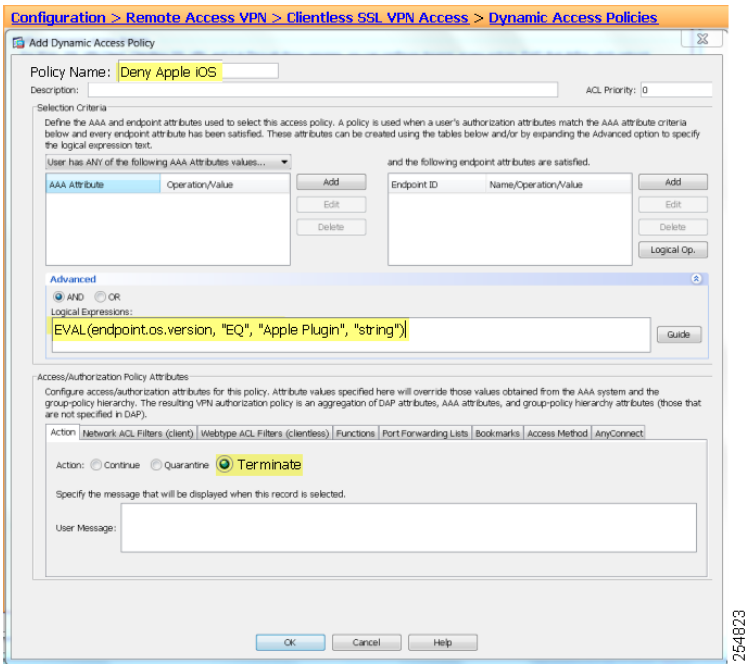
- AnyConnect Premium ライセンスで ASA をアクティブにしておく必要があります。これは技術上の要件です。
- CSD がイネーブルである必要があります。

Apple iOS が SSL VPN 接続しないよう ASA を設定するには、DAP を次のように追加します。

ステップ 1　ASA で ASDM セッションを確立します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] > [Add] を選択します。

図 9-1　Apple iOS デバイスが SSL VPN 接続しないようにする DAP



ステップ 3　ポリシーの名前を付けます（`Deny Apple iOS` など）。

ステップ 4　[Advanced] をクリックします。

ステップ 5　[Logical Expressions] テキスト ボックスに次を入力します。

```
EVAL(endpoint.os.version, "EQ", "Apple Plugin", "string")
```

ステップ 6　[Action] タブの [Terminate] をクリックします。

ステップ 7　[OK] および [Apply] をクリックします。

URI ハンドラを使用した AnyConnect アクションの自動化

Apple でサポートされている URI ハンドラによりアプリケーションは、Universal Resource Indicator（URI; ユニバーサル リソース インジケータ）の形でアクション要求を渡すことができます。URI を使用して VPN 接続エントリの生成、VPN の接続または切断、AnyConnect ユーザ インターフェイスおよびメッセージのローカライズされた文字列のインポートができます。

URI を Web ページまたはアプリケーションに挿入できます。次にこの機能の使用例を示します。

- 証明書のインポート
- Apple iOS ユーザの Web ページを作成し、クライアントにアクセスして設定する。この方法で AnyConnect ユーザ セットアップ プロセスを簡略化します。
- AnyConnect 以外のアプリケーションに VPN 接続を開始させ、必要に応じて内部リソースにアクセスし、切断する。

（注）　エンド ユーザはこの機能を [External Control] として認識します。エンド ユーザは、[Settings] > [AnyConnect] > [External Control] を選択し [Enable] を選択することでモバイル デバイスでこの機能をイネーブルにできます。

次の項で、サポートされているアクションの構文、例、およびパラメータを説明します。

URI ハンドラを使用した VPN 接続エントリの生成

AnyConnect URI ハンドラの create アクションを使用して、ユーザの AnyConnect 接続エントリの生成を簡略化できます。

デバイスに追加する接続エントリごとに個別のリンクを挿入します。1 つのリンクで複数の create アクションはサポートされていません。

create アクションを挿入し、AnyConnect 接続エントリをエンドポイント設定に追加するには、次の構文を使用します。

anyconnect:[**//**]**create**[**/**]**?name=***Description***&host=***ServerAddress*[**&***Parameter1***=***Value***&***Parameter2***=***Value...*]

次に、例を示します。

anyconnect://create/?name=SimpleExample**&host=**vpn.example.com

anyconnect:create?name=SimpleExample**&host=**vpn.example.com

anyconnect:create?name=Example%201**&host=**vpn.example.com**&netroam=**true**&usecert=**false

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

create アクションでは `name` パラメータまたは `host` パラメータのいずれかが必要ですが、両方指定できます。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` および `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。

URI の先頭のスラッシュは省略可能です。

スペースに一致させるには、**%20** と入力します。たとえば、`Example Connection 1` という接続エントリに一致させるには、**Example%20Connection%201** と入力します。

create パラメータ オプションの説明を次に示します。

- **name**：AnyConnect のホーム ウィンドウの接続リストおよび AnyConnect 接続エントリの [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、または記号を使用できます。文字は大文字と小文字を区別します。
- **host**：接続に使用する 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 はこのパラメータの値を AnyConnect 接続エントリの [Server Address] フィールドに挿入します。次に例を示します。

  `vpn.example.com`

- **netroam**（任意）：デバイスが再起動してから、または接続タイプ（EDGE、3G、Wi-Fi など）を変更してからの再接続にかかる時間を制限するかどうかを決定します。

（注）　このパラメータは、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。

有効な値は次のとおりです。

- true：（デフォルト）このオプションでは、VPN アクセスが最適化されます。AnyConnect は値 ON を AnyConnect 接続エントリの [Network Roaming] フィールドに挿入します。AnyConnect 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。この設定では、アプリケーションは VPN への持続的な接続に依存します。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 [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、20 秒間新しい接続を確立しようとし、その後試行は停止します。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。

- **usecert**（任意）：VPN 接続を `host` に確立する場合、デバイスにあらかじめインストールされた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：このオプションを使用すると、ネットワークのセキュリティ アクセスが強化されます。また、Connect on Demand では必須です。AnyConnect は値 ON を AnyConnect 接続エントリの [Use Certificates] フィールドに挿入します。AnyConnect は `host` に VPN 接続を確立しながらデジタル証明書を使用します。`host` 設定で VPN アクセスにデジタル証明書が必要な場合、このオプションを入力する必要があります。usecert が true に設定されているものの certcommonname が指定されていない場合、Automatic Certificate Selection が使用されます。
  - false：（デフォルト）VPN アクセスにデジタル証明書が必要ない場合は、このオプションを使用します。AnyConnect はこの値を AnyConnect 接続エントリの [Certificate] フィールドの Disabled 値と関連付けます。
- **certcommonname**（任意、ただし `usecert` 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 Common Name（CN; 通常名）を一致させます。AnyConnect はその値を AnyConnect 接続エントリの [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た証明書のこの値を表示するには、ボタン バーの [Diagnostics] をタップし、[Manage Certificates] をタップします。デバイスにインストールされた証明書のリストが確認できるようになりました。次の例の通常名は `example-id` です。

図 9-2　[Select Certificate] ウィンドウ

`host` で必要な証明書を表示するため、スクロールしなければならない場合があります。証明書の要約の右側にある [detail disclosure] ボタンをタップして、証明書から読み取られた Common Name パラメータおよびその他の値を表示することもできます。

- **useondemand**（任意、ただし `usecert` および `certcommonname` パラメータは必要）：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を決定します。

  - 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 [Connect on Demand] フィールドに挿入します。
  - 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 接続をトリガしないようにする唯一の手段です。AnyConnect はこの値を AnyConnect 接続エントリの [Connect on Demand] フィールドの OFF 値と関連付けます。

- **domainlistnever**（任意）：Connect on Demand 機能を使用できなくするため、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 が最初に使用するリストです。ドメイン要求が一致すると、ドメイン要求は無視されます。AnyConnect はこのリストを AnyConnect 接続エントリの [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**（domainlistalways または domainlistifneeded パラメータは必要）：Connect on Demand 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 [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**（domainlistalways または domainlistifneeded パラメータは必要）：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。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。AnyConnect はこのリストを AnyConnect 接続エントリの [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。

表 9-1　AnyConnect ドメイン一致

一致	指示	エントリの例	一致する例	一致しない例
プレフィクスおよびドメイン名が正確に一致。	プレフィクス、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

表 9-1　AnyConnect ドメイン一致 （続き）

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

URI ハンドラを使用した VPN 接続の確立

ユーザが簡単に VPN 接続を確立できるよう、URI に接続情報を埋め込み、これらの URI をユーザに提供できます。

次の作業を行う URI 文字列を作成できます。

- URI での接続名およびホスト名の指定
- 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
- 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
- 接続情報の指定、ユーザ名およびパスワードの自動入力、および接続エイリアスの指定

Connect パラメータおよび構文の説明も参照してください。

URI での接続名およびホスト名の指定

connect アクションに **name** および **host** パラメータを挿入するには、次のいずれかの構文式を使用します。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]
anyconnect:[//]connect[/]?name=Description&host=ServerAddress
```

完成した URI の例

```
anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
```

パラメータおよびその他の構文上の要件の補足説明については、「Connect パラメータおよび構文の説明」を参照してください。

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

connect アクションで name および host パラメータに加えて、prefilled username パラメータと prefilled password パラメータを指定するには、次のいずれかの構文を使用します。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]&prefill_username=username&
prefill_password=password
```

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username=**username**&prefill_password=**password

完成した URI の例

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1

anyconnect:connect?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

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

connect アクションで name および host パラメータに加えて、prefilled primary username および secondary username パラメータおよび prefilled password パラメータを指定するには、次のいずれかの構文を使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=**Description|**host=**ServerAddress]**&prefill_username=**username**&prefill_password=**password**&prefill_secondary_username=**username2**&prefill_secondary_password=**password2

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username=**username**&prefill_password=**password**&prefill_secondary_username=**username2**&prefill_secondary_password=**password2

完成した URI の例

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1**&prefill_secondary_username=**user2**&prefill_secondary_password=**password2

anyconnect:connect?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1**&prefill_secondary_username=**user2**&prefill_secondary_password=**password2

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

接続情報の指定、ユーザ名およびパスワードの自動入力、および接続エイリアスの指定

この例では、接続エイリアスを connect アクションで name および host パラメータに加えて、自動入力のユーザ名と自動入力のパスワードを指定する URI に追加しています。

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]**&prefill_username=***username***&prefill_password=***password***&prefill_group_list=**10.%20Single%20Authentication

anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress***&prefill_username=***username***&prefill_password=***password***&prefill_group_list=**10.%20Single%20Authentication

完成した URI の例

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1**&prefill_group_list=**10.%20Single%20Authentication

```
anyconnect:connect?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_group_list=10.%20Single%20Authentication
```

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

Connect パラメータおよび構文の説明

connect アクションでは name パラメータまたは host パラメータのいずれかが必要ですが、両方指定できます。あるいは、ステートメントのすべてのパラメータ値がデバイス上の AnyConnect 接続エントリの値と一致する場合、Apple iOS は残りのパラメータを使用して接続を確立します。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、新しい接続エントリが生成されます。Apple iOS は VPN 接続を試行します。

URI の先頭のスラッシュは省略可能です。

スペースに一致させるには、**%20** と入力します。たとえば、Example Connection 1 という接続エントリに一致させるには、**Example%20Connection%201** と入力します。a ～ z、A ～ Z、および 0 ～ 9 以外のすべての文字は URI に符号化する必要があります。

connect パラメータ オプションの説明を次に示します。

- **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 [Description] フィールドに対して評価し、前回の手順を使用して Apple iOS 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。値は大文字と小文字を区別します。ステートメントの文字と接続エントリの文字の大文字または小文字が一致しない場合は、AnyConnect はこのフィールドを一致させません。
- **host** : AnyConnect 接続エントリの [Server Address] フィールドと一致させるには、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 Apple iOS 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。
- **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。

注意　[Prefill] パスワード フィールドは、1 回限定のパスワードに設定された接続プロファイルでのみ使用します。

- **prefill_secondary_username** : 必要な二重認証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** : 必要な二重認証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、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] > [Advanced] > [Group Alias/Group URL] > [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。

URI ハンドラを使用した VPN からの切断

disconnect アクションを挿入するには、次の構文を使用します。

```
anyconnect:[//]disconnect[/]
```

次に、例を示します。

```
anyconnect://disconnect/
anyconnect:disconnect
```

スラッシュは省略可能です。disconnect アクションにはパラメータは必要ありません。

URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズ

この URI ハンドラ方法を使用して、ローカリゼーション ファイルを AnyConnect クライアントに配布できます。

前提条件

URI ハンドラを使用して AnyConnect UI およびメッセージをローカライズするには、Apple iOS 5 以降をモバイル デバイスにインストールしておく必要があります。

詳細

URI で import コマンドを使用するには、次の構文を使用します。

anyconnect:[**//**]**import**[**/**]**?type=localization&lang=***LanguageCode***&host=***ServerAddress***

例：

anyconnect:import?type=localization&lang=fr**&host=**asa.example.com

スラッシュは省略可能です。import アクションでは `host` パラメータが必要です。**type**、**lang**、および **host** の各パラメータを下に定義します。

- **type**：インポートのタイプで、この場合は常に **localization** になります。
- **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「French」なら fr、「Canadian French」なら fr-ca となります。
- **host**：AnyConnect 接続エントリの [Server Address] フィールドと一致させるには、ASA のドメイン名または IP アドレスを入力します。

URI ハンドラを使用した PKCS12 符号化証明書バンドルのインポート

AnyConnect クライアントは、エンドポイントにインストールされた PKCS12 符号化証明書を使用して自ら ASA に認証させることができます。URI ハンドラ **import** コマンドを使用して、PKCS12 符号化証明書バンドルをエンドポイントにインポートできます。

PKCS12 証明書を URL からインポートするには、次の構文を使用します。

anyconnect://import/?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

URI の先頭のスラッシュは省略可能です。

スペースに一致させるには、**%20** と入力します。たとえば、`Example Connection 1` という文字列に一致させるには、Example**%20**Connection**%20**1 と入力します。

URI のコロンと一致させるには、**%3A** を使用します。URI のスラッシュと一致させるには、**%2F** を使用します。たとえば、http://example.cisco.com/CertName.p12 と一致させるには、`http`**`%3A%2F%2F`**`example.cisco.com`**`%2F`**`CertName.p12` と入力します。

import パラメータ オプションの説明を次に示します。

- **type**：pkcs12 証明書タイプのみサポートされています。
- **uri**：証明書が見つかる URL 符号化 ID。「http」、「https」、および「ftp」がサポートされています。URI では **%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。

HTML ハイパーリンクの例

URI を HTML ページに追加するには、URI をハイパーリンクに組み込む必要があります。次に HTML ハイパーリンクで URI を使用する方法を示す例を示します。例中で太字の部分が URI です。

HTTP の例

```
<p>
<a href="anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12>
click here to import certificate using http</a>
</p>
```

FTP の例

```
<p>
<a
href="anyconnect://import?type=pkcs12&uri=ftp%3A%2F%2FAdministrator%3Apassword%40192.168.10.20%2Fcerts%2FCertName.pfx">click here to import certificate using ftp </a>
</p>
```

Secure Digital（SD）カードの例

```
<p>
<a
href="anyconnect://import?type=pkcs12&uri=file%3A%2F%2Fsdcard%2CertName.pfx">click
here to import certificate from sdcard on mobile device</a>
</p>
```

その他 Apple iOS 固有の考慮事項

Apple iOS デバイスで AnyConnect をサポートする場合は、次の事項を考慮する必要があります。

- Apple for Windows または Mac OS X から入手できる iPhone Configuration Utility を使用して構成し Apple iOS デバイスに展開できます。
- Apple iOS は信頼ネットワークと非信頼ネットワーク間の識別はサポートしていません。Apple iOS Connect On Demand 機能は、ユーザが該当するドメイン リストで指定されたホスト名で任意の宛先にアクセスしようとする場合に VPN 接続を開始します。たとえば、ユーザが internal.example.com に移動し「.example.com」が Always Connect リストに存在する場合、デバイスが現在どのネットワーク接続されていても、クライアントは VPN 接続を開始します。
- 規則を設定する場合は、[Connect if Needed] オプションを指定することをお勧めします。Connect if Needed 規則は、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 を構成する必要があります。

- クライアント側のデッド ピア検出がすでにイネーブルになっている場合、モバイル デバイスのバッテリ寿命を延ばすため、キープアライブ メッセージをディセーブルにすることをお勧めします。Keepalive Messages パラメータにアクセスするには、ASDM を使用して [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add] または [Edit] > [Advanced] > [AnyConnect Client] に移動します。
- デバイスがスリープしなくなるため、サーバ側の DPD はオフにする必要があります。しかし、ネットワークの接続性がないという理由でいつトンネルが終了するかクライアントが判断できるため、クライアント側の DPD はオンにしておく必要があります。

（注）　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。しかし、トンネル ポリシーをセッションから除外できる外部アクセス可能な ActiveSync 接続と並行して AnyConnect を使用できます。

トラブルシューティング

デバイスのロギングをイネーブルにし、次のいずれかのガイドのユーザ トラブルシューティング手順に従ってください。

- 『*iPhone User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5*』
- 『*iPad User Guide for Cisco AnyConnect Secure Mobility Client, Release 2.5*』

ユーザ トラブルシューティング手順は、ユーザ インターフェイスは異なりますが、iPhone および iPad で同じです。次の手順で問題が解決しない場合、次の提案を試してください。

- 同じ問題がデスクトップ クライアントで発生しているかどうか判断します。
- AnyConnect Mobile ライセンスが ASA にインストールされていることを確認します。
- デバイスが再起動した後 VPN 接続が復元されない場合、プロファイルでネットワーク ローミングがイネーブルになっており、Auto-Reconnect がイネーブルになっていることを確認します。
- 証明書認証が失敗する場合、正しい証明書が選択されていることを確認します。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。AnyConnect プロファイルの証明書一致規則がユーザの選択した証明書を除外し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。認証メカニズムで 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、ユーザが正常に認証できることを確認します。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イネーブルにし、ASA のデバッグ ロギングをイネーブルにします。
- 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。詳細については、『ASA Administrator Guide』を参照してください。
- 証明書認証および Apple iOS Connect On Demand 機能が接続するよう設定されている場合に AnyConnect アプリケーションを使用して Apple iOS が接続開始するよう要求している場合、グループ URL を使用するよう接続を設定します。グループ URL および証明書のみの認証の両方とも Connect on Demand の要件です。