iPhone 用 Cisco AnyConnect セキュア モビリティ クライアント ユーザ ガイド（リリース 3.0.x）

更新日：2012 年 10 月 25 日

【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。

このマニュアルでは、Apple iOS 向け Cisco AnyConnect セキュア モビリティ クライアント 3.0x について説明します。このマニュアルの構成は、次のとおりです。

概要

Apple iOS 向け Cisco AnyConnect セキュア モビリティ クライアントは、エンタープライズ ネットワークに対するシームレスでセキュアなリモート アクセスを実現します。このクライアントを使用すると、インストールされているすべてのアプリケーションで、エンタープライズ ネットワークに直接接続されているかのように通信できます。

App Store でインストール アプリケーションおよびすべての更新が提供されます。Cisco 適応型セキュリティ アプライアンス（ASA）は、VPN へのアクセスを許容するセキュア ゲートウェイですが、Apple iOS 向け AnyConnect の更新はサポートしません。

Apple iOS 向け AnyConnect は、Windows、Mac OS X、および Linux 向け AnyConnect と同様のものです。Apple iOS で AnyConnect を使用する際の追加資料がお客様の組織から提供されることがあります。

サポートされている Apple iOS デバイス

デバイス	必要な Apple iOS リリース
iPad 1	5.0 以降
iPad 2	5.0 以降
iPad 3	5.0 以降
iPhone 3GS	5.0 以降
iPhone 4	5.0 以降
iPhone 4S	5.0 以降
iPhone 5	5.0 以降
iPod touch（第 3 世代以降）	5.0 以降

（注） AnyConnect は、iPhone 上の場合と同じように iPod Touch 上に表示され、動作します。このデバイスには、『*iPhone User Guide for Cisco AnyConnect Secure Mobility Client*』を使用してください。

AnyConnect のインストールまたはアップグレード

AnyConnect のインストール

次の手順で Apple App Store から Apple iOS 向け Cisco AnyConnect セキュア モビリティ クライアントをインストールします。

ステップ 1 App Store を開きます。

ステップ 2 [Search] を選択します。

ステップ 3 検索ボックスに `anyconnect` と入力し、[Suggestions] リストにある [cisco anyconnect] をタップします。

ステップ 4 [AnyConnect] をタップします。

ステップ 5 [Free]、[INSTALL APP] の順にタップします。

ステップ 6 [Install] を選択します。

AnyConnect のアップグレード

AnyConnect 3.0 へのアップグレードは、Apple App Store を使用して管理します。デバイスをアップグレードする前に次の手順を実行します。

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

AnyConnect のアップグレードが利用可能であることを示す通知を Apple App Store から受けたら、次の手順に従います。

ステップ 1 iOS のホームページで、[App Store] アイコンをタップします。

ステップ 2 [AnyConnect upgrade notice] をタップします。

ステップ 3 新機能を確認します。

ステップ 4 [Update] をクリックします。

ステップ 5 **Apple ID のパスワード**を入力します。

ステップ 6 [OK] をタップします。

ステップ 7 AnyConnect のアップグレードが実行されます。

デバイスのローカリゼーション

AnyConnect パッケージには、次の言語変換が含まれます。

- チェコ語（cs-cz）
- ドイツ語（de-de）
- 中南米スペイン語（es-co）
- カナダ フランス語（fr-ca）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- ポーランド語（pl-pl）
- 簡体字中国語（zh-cn）

AnyConnect 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 Android デバイスにインストールされます。表示される言語は、[Settings] > [General] > [International] > [Language] で指定されたロケールによって決まります。AnyConnect は最適なものを判断するため、言語仕様を使用してから、リージョン仕様を使用します。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 を起動するとすぐに変換されます。選択されたローカリゼーションは、AnyConnect の [Localization Management] 画面に `Active` と表示されます。

インストール後のローカリゼーション アクティビティとオプションについては、ローカリゼーションの管理を参照してください。

オープン ソフトウェア ライセンスに関する通知

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

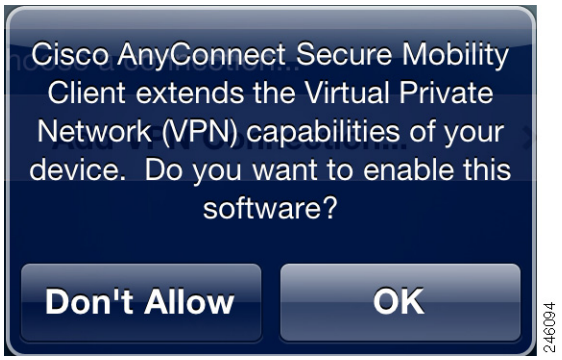
AnyConnect の開始

クライアント ユーザ インターフェイス

iPhone または iPad のホーム画面で [AnyConnect] アイコンをタップすると、AnyConnect のホーム画面が開きます。

ステップ 1 [Cisco AnyConnect Secure Mobility Client] アイコンをタップします。

デバイスで初めて AnyConnect を起動する場合は、確認ウィンドウが表示されます。



ステップ 2 [OK] をタップします。

AnyConnect のホーム画面に VPN 接続ステータスが表示されます。図 1 に iPhone 向けの AnyConnect のホーム画面を示します。図 2 に iPad 向けの AnyConnect のホーム画面を示します。

AnyConnect のホーム画面には、デバイスに保存されている VPN 接続エントリの名前のリストが表示され、新しい VPN 接続エントリを追加できます。最上部付近のスライダ スイッチでは、チェックマークが付いている接続エントリを使用して VPN 接続を確立できます。[Status] パラメータには、VPN 接続の状態が表示されます。

各 iPhone ディスプレイの下部にあるタブ バーには、[Home]、[Statistics]、[Diagnostics]、および [About] の各ウィンドウのナビゲーション アイコンが表示されます。iPad AnyConnect のホーム画面には、これらの機能が統合されています。

図 1　　iPhone AnyConnect のホーム画面

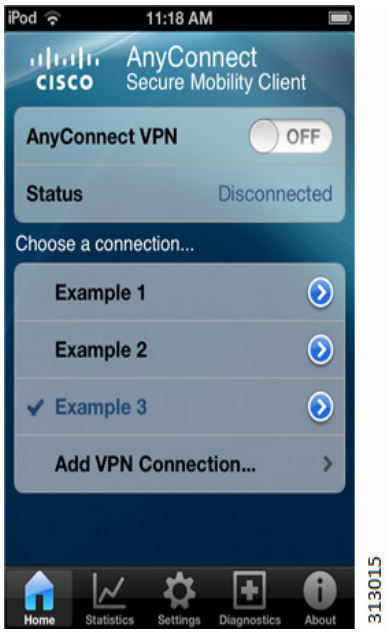


図 2　　iPad AnyConnect のホーム画面

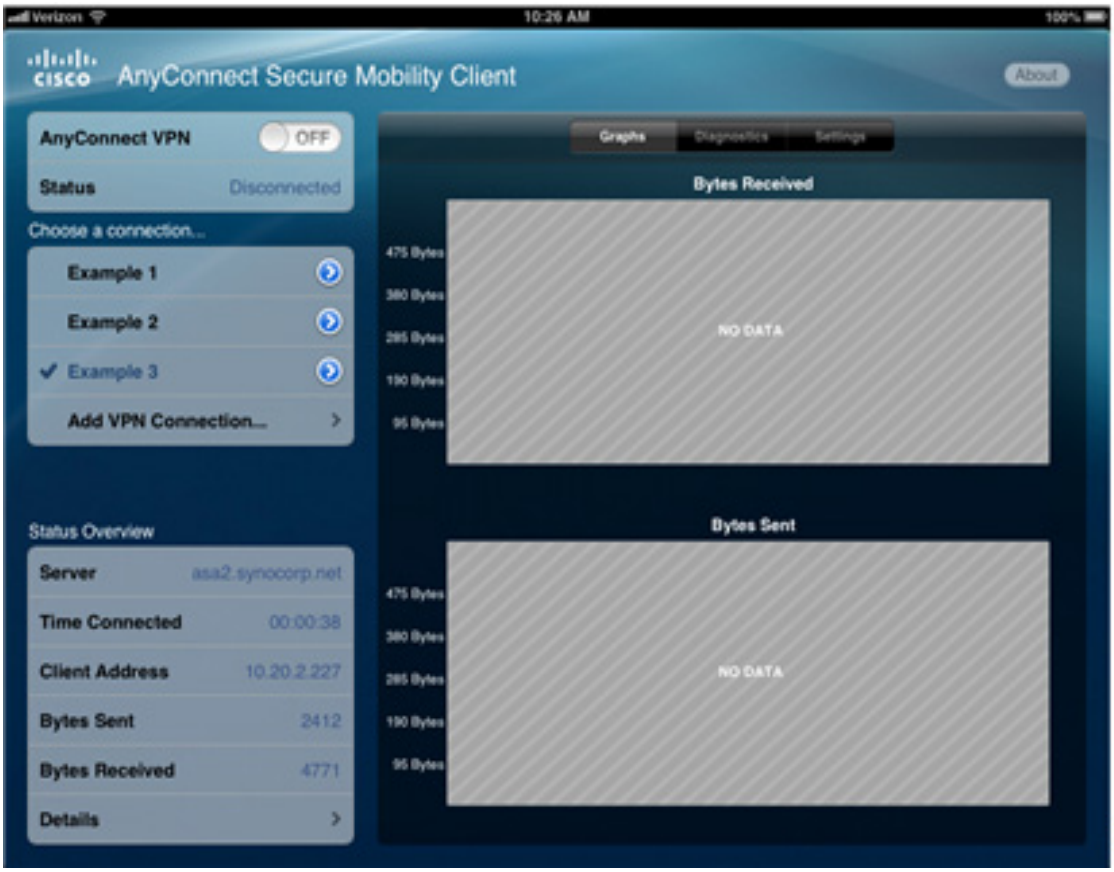


表 1 に iPhone 向け AnyConnect と iPad 向け AnyConnect の相違点を示します。

表 1　iPhone と iPad の AnyConnect UI の相違点

機能	iPhone	iPad
[Home]：AnyConnect アイコンをタップすると開きます。	VPN 接続コントロールが表示されます。 AnyConnect 画面の下部にある [Home] アイコンをタップしてもアクセスできます。	VPN 接続コントロールは、AnyConnect のホーム画面の左上にあります。 この画面は表示されたままになります。
[Statistics]：接続ステータスの概要	iPhone AnyConnect アプリ画面の下部にある [Statistics] アイコンをタップします。	AnyConnect のホーム画面の左下の [Status Overview] パネル。
[Statistics] > [Details]	[Statistics] 画面の [Details] をタップします。	AnyConnect のホーム画面の [Status Overview] パネルで [Details] をタップします。
Settings	iPhone AnyConnect アプリ画面の下部にある [Settings] アイコンをタップします。	AnyConnect のホーム画面の [Status Overview] パネルで [Settings] をタップします。
Diagnostics	タブ バーで [Diagnostics] アイコンをタップして、お使いのデバイスに保存されている証明書、プロファイル、またはローカリゼーション データの表示または削除、デバッグのロギング、AnyConnect ログの表示と管理を実行します。	AnyConnect のホームページで [Diagnostics] ボタンをタップして、デバイスに保存されている証明書、プロファイル、またはローカリゼーション データの表示または削除、デバッグのロギング、AnyConnect ログの表示と管理を実行します。
[About]：AnyConnect のバージョンとライセンスの詳細およびユーザ ガイドへのリンクが表示されます。	AnyConnect 画面の下部にある [About] アイコンをタップします。	AnyConnect のホーム画面の右上にある [About] をタップします。
帯域幅のグラフ（送受信バイト数）	[Statistics] > [Graphs] の順にタップして、送受信バイト数のグラフを表示します。	AnyConnect のホーム画面の右上部付近にある [Graphs] をタップします。

ステップ 3　最初の VPN 接続を確立する前に、選択するための VPN 接続エントリを追加する必要があります。前述の図の Example 1、Example 2 などは、設定済みの接続エントリです。管理者からの指示に従い、接続エントリを設定します。次の操作が必要になる場合があります。

a. AnyConnect の設定を行う前に必要となるものを取得する。

b. VPN 接続エントリの追加のためのいずれかの方法を行う。

c. モバイル デバイスへの証明書のインストールのためのいずれかの方法を行う。

d. 最後に、VPN 接続の確立を行う。

ヘルプの表示

AnyConnect では、ヘルプを使用できる場合に、画面の右下隅に情報アイコン（***i***）が表示されます。

このアイコンをタップし、現在のオプションに関するヘルプ情報を表示します。

または、AnyConnect のホーム画面の右下隅にある [About] をタップして、本ガイドへのリンクを表示します。

AnyConnect の設定を行う前に必要となるもの

AnyConnect を設定して VPN セッションを確立するには、ネットワーク要件に応じて、システム管理者から次の情報を 1 つまたは複数取得する必要があります。

- サーバ アドレス : VPN セキュア ゲートウェイとして使用する Cisco 適応型セキュリティ アプライアンスのドメイン名、IP アドレス、またはグループ URL。
- ユーザ名およびパスワード : VPN へのアクセスに必要なクレデンシャル。

または、システム管理者により社内ネットワークのリンクが提供されることがあります。このリンクをタップすると iPhone に必要な接続エントリを追加できます。

Apple iOS Connect On Demand 機能を使用すると、デバイス上のアプリケーションでの必要に応じた自動 VPN 接続がサポートされます。ただし、最初にデジタル証明書をデバイスにインストールする必要があります。この証明書は、セキュア ゲートウェイで受け付けられるものである必要があります。セキュア ゲートウェイが各グループ URL についてどの証明書を受け付けるかは、システム管理者が決定します。

次の方法を使用して、1 つまたは複数の証明書をインストールします。

- Apple iOS デバイスの構成プロファイル（iPhone 構成ユーティリティ経由でインストールしたもの）を使用します。
- システム管理者からの指示に従い、AnyConnect を使用して証明書をインポートします。
- 証明書のインストール方法については、「モバイル デバイスへの証明書のインストール」（P.11）を参照してください。

他の形態の認証をまったく使用しない場合は、システム管理者が提供するグループ URL を使用するのが最善です。

VPN への接続

VPN 接続エントリの追加

AnyConnect 設定に接続エントリを追加するための Web ページのリンクがシステム管理者から提供されている場合、次の手順は不要なことがあります。

VPN 接続の確立を試みる前に、次の手順で VPN 接続エントリを追加し、Cisco セキュア ゲートウェイを識別できるようにします。

ステップ 1 AnyConnect のホーム画面で [Add VPN Connection] をタップします。[Add VPN Connection] 画面に、最初の VPN 接続のパラメータが表示されます。設定プロセスは、[Cancel] をタップしていつでもキャンセルできます。接続エントリを保存するには、[Save] をタップします。

ステップ 2 （オプション）[Description] をタップして、接続エントリの一意な名前を入力します。

この名前は、AnyConnect のホーム画面の接続リストに表示されます。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。キーボードのアルファベット、空白文字、数字、記号を使用します。AnyConnect では、ユーザが指定した大文字と小文字が維持されます。次の例を参考にしてください。

```
Example 1
```

ステップ 3 [Server Address] をタップして、接続する Cisco Adaptive Security Appliance 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。次の例を参考にしてください。

```
vpn.example.com
```

ステップ 4 [Advanced] をタップして、高度な VPN 接続パラメータを開きます。

このウィンドウで、[Add VPN Connection] をタップすると、いつでも接続エントリをキャンセルまたは保存するための初期設定ウィンドウに戻ります。

ステップ 5 （オプション）この接続の [Network Roaming] を設定します。

[Network Roaming] で、デバイスが起動してから、または接続タイプ（EDGE（2G）、1xRTT（2G）、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*。

このスイッチは、次のようにタップします。

- [ON]：（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 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。
- [OFF]：このオプションでは、バッテリ寿命が最適化されます。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。接続が必要な場合、新しい VPN 接続を開始する必要があります。

ステップ 6 （オプション）この接続に使用する証明書を設定します。

a. [Certificate] をタップして、[Select Certificate] 画面を表示します。

b. 次のいずれかの選択肢をタップします。

- [Disabled]：（デフォルト）クライアント証明書は認証に使用されません。

- [Automatic] : AnyConnect では、認証で使用されるクライアント証明書が自動的に選択されます。この場合、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、ユーザが VPN 接続の確立を試行するたびに実行されます。
- [Certificate Name] : デバイスに証明書をインストール済みの場合、この VPN 接続に関連付ける証明書を選択します。

c. [Advanced] をタップして、高度な設定ウィンドウに戻ります。

（注） 認証に証明書を**使用しない**場合、証明書のフィールドでは**操作を行わずに** [Save] をタップします。接続設定では、[Disabled] 証明書設定が維持されます。

認証に証明書を**使用する**場合、証明書のフィールドでは**操作を行わずに** [Save] をタップします。次に、モバイル デバイスへの証明書のインストールの手順を使用して、接続プロファイルの証明書認証をインポートし、設定します。

ステップ 7 （オプション）この接続の Connect on Demand を設定します。

VPN 接続の認証に証明書を使用する場合、[Connect on Demand] スイッチが表示されます。この機能の設定については、Connect-On-Demand 規則の設定を参照してください。

ステップ 8 この接続を設定して、SSL の代わりに IPsec VPN プロトコルを使用します。

a. （オプション）[Connect with IPsec] をタップして、この VPN 接続に SSL の代わりに IPsec を使用します。

VPN 接続プロトコルに IPsec を選択した場合、[Authentication] パラメータが表示されます。

b. （オプション）[Authentication] をタップして、この IPsec 接続の認証方法を選択します。

- EAP-AnyConnect（デフォルト）
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

[Advanced] をタップして、高度な設定ウィンドウに戻ります。[Advanced Connection Editor] ウィンドウに認証オプションが表示されます。

EAP-GTC、EAP-MD5、または EAP-MSCHAPv3 を認証に使用するように指定している場合、[IKE Identity] パラメータが表示されます。

c. （オプション）[IKE Identity] をタップして、必要なクライアント ID を入力します。これは管理者から提供されます。

ステップ 9 接続エントリ名をタップして、[Add VPN Connection] ウィンドウに戻ります。

ステップ 10 （任意）接続の値を保持するには、[Save] をタップします。

[Add VPN Connection] 画面が閉じ、AnyConnect のホーム画面にエントリが追加されます。

モバイル デバイスへの証明書のインストール

証明書を使用して、お使いのデバイスをセキュア ゲートウェイに対して認証するためには、デバイスに証明書をインポートし、その証明書と接続エントリを関連付けます。次の方法のいずれかを使用して、Apple iOS デバイスに証明書をインポートします。

- 電子メール添付の証明書のインポートとインストール
- ハイパーリンクによる証明書のインポートとインストール
- SCEP で設定された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

各手順の最後に、接続エントリへの証明書の関連付けへのリンクが含まれています。

その他の証明書関連の操作については、証明書の管理を参照してください。

電子メール添付の証明書のインポートとインストール

管理者から、認証に使用する証明書が電子メールで送信されます。証明書を受信したら、次の手順に従います。

ステップ 1 添付された証明書のアイコンをタップします。

証明書を開いたことが Apple iOS で認識され、インストール ウィザードが開きます。

ステップ 2 [Install] をタップします。

ステップ 3 インストール ウィザードの指示に従います。

ステップ 4 プロンプトが表示されたら、証明書の認証コードを入力します。

ステップ 5 [Next] をタップします。

Apple iOS で証明書がインストールされます。

ステップ 6 接続エントリへの証明書の関連付けに進みます。

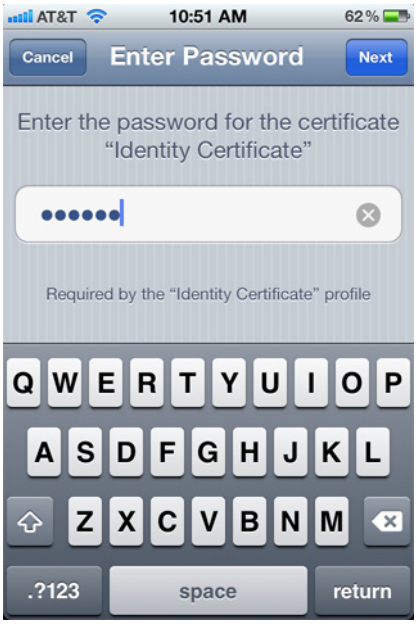
ハイパーリンクによる証明書のインポートとインストール

管理者から、お使いの iOS デバイスにインストールする証明書の場所へのハイパーリンクが提供されます。

（注） この操作を実行するには、外部制御を設定してプロンプトを表示するか、AnyConnect 設定内で有効にする必要があります。詳細については、外部制御の設定を参照してください。

ステップ 1 管理者から受け取ったハイパーリンクをタップします。リンクは、電子メールに含まれているか、イントラネットの Web ページに公開されています。

ステップ 2 プロンプトが表示されたら、証明書の認証コードを入力します。



ステップ 3 [Next] をタップします。

Apple iOS で、証明書がハイパーリンクで指定された場所からインポートされます。iOS で証明書が正常にインポートされると、証明書の登録メッセージを受信します。

ステップ 4 [OK] をタップします。

ステップ 5 接続エントリへの証明書の関連付けに進みます。

SCEP で設定された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

管理者は、SCEP プロトコルを使用して、証明書を配布する接続プロファイルを設定することがあります。AnyConnect 管理者は、VPN 設定の名前またはその設定を使用する接続プロファイルの名前をユーザに通知する必要があります。

SCEP で設定された接続エイリアスを使用して証明書をインポートし、インストールする方法は、次の 2 つです。

- 手動による証明書のインポートとインストール
- 証明書の自動的なインポートとインストール

手動による証明書のインポートとインストール

ステップ 1 AnyConnect セキュア モビリティ クライアント アプリケーションを開きます。

ステップ 2 [Choose a connection...] 領域で、お使いのモバイル デバイスに証明書をダウンロードできる接続の名前をタップします。

ステップ 3 AnyConnect の [On] ボタンをタップします。

ステップ 4 [Get Certificate] をタップします。

セキュア ゲートウェイによって、証明書がお使いのデバイスにダウンロードされます。

VPN セッションが切断され、認証が正常に登録されたことを伝えるメッセージを受信します。ユーザは、証明書をグループに手動で割り当てる必要があります。

ステップ 5 プロンプトが表示されたら、ユーザ名およびパスワードを入力します。

ステップ 6 [OK] をタップします。

ステップ 7 接続エントリへの証明書の関連付けに進みます。

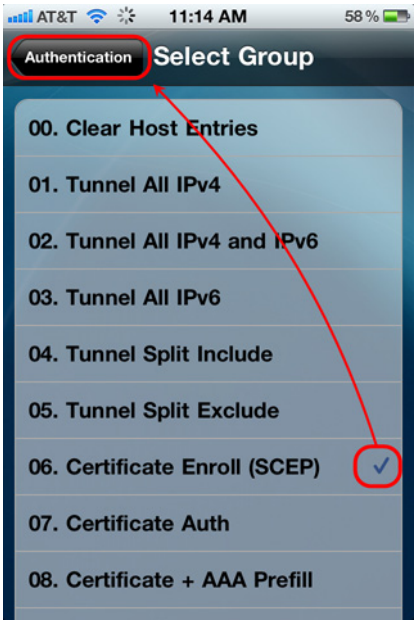
証明書の自動的なインポートとインストール

ステップ 1 AnyConnect セキュア モビリティ クライアント アプリケーションを開きます。

ステップ 2 [Choose a connection...] 領域で、お使いのモバイル デバイスに証明書をダウンロードできる接続の名前をタップします。

ステップ 3 AnyConnect の [On] ボタンをタップします。

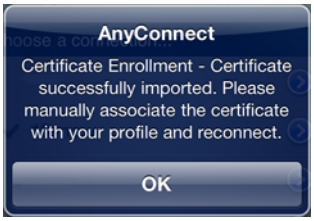
ステップ 4 [Authentication] 画面で、お使いのモバイル デバイスに証明書をダウンロードするように設定されたグループを選択してから、[Authentication] 画面に戻ります。



ステップ 5 接続プロファイルのユーザ名およびパスワードを入力し、[Connect] をタップします。

セキュア ゲートウェイによって、証明書がお使いのデバイスにダウンロードされます。

VPN セッションが切断され、認証が正常に登録されたことを伝えるメッセージを受信します。ユーザは、証明書をグループに手動で割り当てる必要があります。



ステップ 6 [OK] をタップします。

ステップ 7 接続エントリへの証明書の関連付けに進みます。

接続エントリへの証明書の関連付け

VPN 接続エントリの追加を使用して VPN を作成済みであるか、VPN 接続エントリの変更を使用して変更できる接続エントリがお使いのデバイスに存在します。

ステップ 1 [Choose a connection...] パネルで、接続の詳細表示ボタンを選択します。

ステップ 2 [Advanced] > [Certificate] の順にタップします。

ステップ 3 今インポートした証明書の名前をタップします。

証明書には、選択した証明書であることを示すチェックマークが付けられます。

ヒント [Select Certificate] 画面では、自動証明書選択の [Automatic] をオンにします。お使いのデバイスに複数の証明書がインストールされている場合、認証に使用する適切な証明書が選択されます。

ステップ 4 接続の詳細に戻ります。

ステップ 5 （任意）Connect-On-Demand 規則の設定を使用して、Connect on Demand を設定します。

ステップ 6 [Save] をタップします。

ホーム画面で AnyConnect を [ON] にして、VPN 接続を開始します。

Connect-On-Demand 規則の設定

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。AnyConnect では、アプリケーションで要求されたドメインが、選択した接続エントリ（横にチェック マークが付いているエントリ）内のドメイン リストの文字列に対して評価されます。

iOS の Connect on Demand 経由で VPN 接続が開始されると、iOS は、トンネルが一定の期間非アクティブである（トンネルを通過するトラフィックがない）場合、そのトンネルを切断します。詳細については、Apple の『VPN オンデマンド』のマニュアルを参照してください。

- [Never Connect] : AnyConnect 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 を有効にすると、AnyConnect で VPN 設定内のセキュア ゲートウェイ アドレスが [Never Connect] リストに追加され、Web 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] : AnyConnect 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] : AnyConnect 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 からはアクセスできない内部リソースに一時的にアクセスできるようにすることです。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。
- アプリケーションでは、IP アドレスではなく、完全修飾ドメイン名が使用されて、宛先が指定されている。
- 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。
- AnyConnect 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。
  - AnyConnect 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、AnyConnect 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。

ドメインリストは Connect-on-Demand 規則を指定します。規則では、ドメイン名のみがサポートされ、IP アドレスはサポートされません。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。リスト エントリはカンマで区切ります。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
完全なドメイン名の一致。	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
最上位ドメインまでの一連の個別サブドメインの完全一致。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

AnyConnect では、リストに含めるドメインの数に制限はありません。

前提条件

接続エントリが、有効な証明書を使用して認証するように設定されています。

接続エントリは、ユーザが作成したエントリです。ユーザは、ASA からダウンロードした接続プロファイルで Connect on Demand を設定できません。

手順の詳細

Connect on Demand を設定するには、次の手順に従います。

ステップ 1 AnyConnect のホーム画面を開きます。

ステップ 2 [Choose a connection...] 領域で、Connect on Demand を設定する接続の接続詳細アイコンをタップします。

ステップ 3 [Advanced] をタップして、高度な設定ウィンドウを開きます。

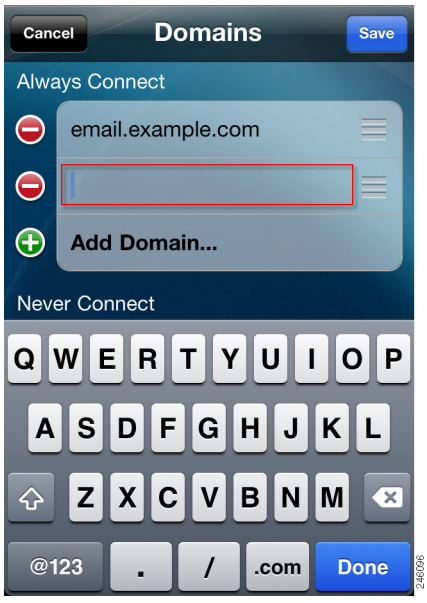
ステップ 4 [Connect On Demand] の横にある [ON] をタップします。

ステップ 5 [Domain List] をタップします。

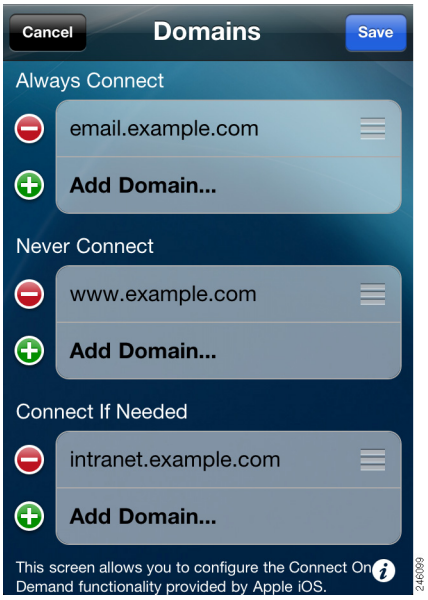
[Domains] 画面に、ドメイン リストが表示されます。

ステップ 6 次のいずれかを実行します。

- 表示されたリストに、[Add Domain] をタップしてドメイン文字列を追加します。[Domains] 画面のリストに行が追加され、ドメイン文字列を入力するためのオンスクリーン キーボードが表示されます。



- 画面の上部にある [Edit] をタップし、ドメイン文字列を追加、編集、または削除します。



この画面では、次の操作が可能です。

- リストにドメイン名を追加する。ドメイン名を追加するには、[Add Domain] をタップします。リストに空の行が追加され、リスト エントリを追加するためのオンスクリーン キーボードが表示されます。
- ドメイン名をリスト間で移動する。移動するには、ドメイン エントリの右にある 3 本バーにタッチし、移動先のリストのタイトル下にある領域にドラッグします。
- ドメイン名を削除する。ドメイン名の左にある赤い円で囲んだ部分をタップしてから、ドメイン名の右にある [Delete] をタップします。

ステップ 7 [Save] をタップします。

VPN 接続の確立

前提条件

LAN 接続またはサービス プロバイダーに接続されていることを確認します。

手順の詳細

ステップ 1 AnyConnect のホーム画面に移動します。

ステップ 2 使用する接続エントリをタップします。

AnyConnect で、その接続エントリの横にチェック マークが移動され、実行中のすべての VPN 接続が解除されます。

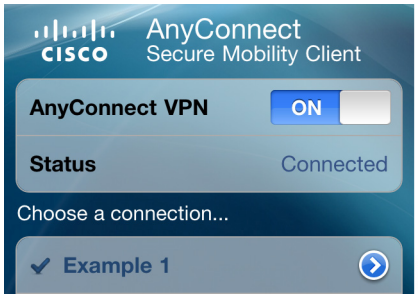
ステップ 3 [AnyConnect VPN] の横にある [ON] をタップします。

ステップ 4 必要に応じて、システム管理者から提供された資格情報を使用してログインします。

ステップ 5 システム管理者から指示があった場合は、[Get Certificate] をタップします。

ステップ 6 必要に応じて、[Connect] をタップします。

[Status] パラメータには、新しい接続の状態が表示されます。



ステータス バーには、[VPN] アイコンが表示されます。

セキュア ゲートウェイの設定に応じて、AnyConnect は接続エントリを取得し、AnyConnect のホーム画面にある VPN 接続リストに追加します。

注意 AnyConnect のホーム画面で別の VPN 接続をタップすると、現在の VPN 接続は切断されます。

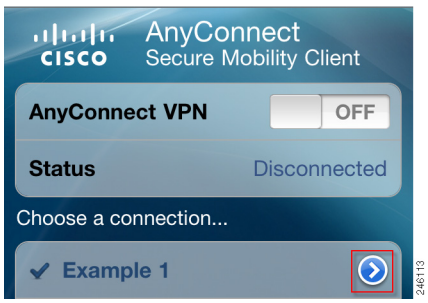
VPN 接続エントリの変更

作成した接続エントリのすべての側面を変更できます。

Apple iOS モバイル デバイスが ASA に接続すると、AnyConnect によってこの VPN クライアント プロファイルがインポートされ、デバイスにインストールされます。ユーザは、AnyConnect 管理者によって定義された VPN クライアント プロファイルのほとんどのフィールドを変更できません。

ステップ 1 AnyConnect のホーム画面を開きます。

ステップ 2 VPN 接続エントリの右にある詳細表示ボタンをタップします。



AnyConnect に、VPN 接続パラメータが表示されます。

ステップ 3 [Advanced] をタップして追加のパラメータにアクセスし、[Add VPN Connection] を選択して基本設定画面に戻ります。

ステップ 4 値を変更するには、いずれかの画面で任意のパラメータをタップします。

ステップ 5 オンスクリーン キーボードを使用して、新しい値を入力します。

（注） AnyConnect VPN プロファイルまたは iPhone 構成ユーティリティの mobileconfig からインポートした接続については、全体の編集はできません。

パラメータの指定については、オンライン ヘルプを使用するか、VPN 接続エントリの追加を参照してください。

ステップ 6 [Add VPN Connection] 画面で [Save] をタップします。

接続パラメータの画面が閉じます。

接続エントリの削除

AnyConnect では、接続エントリの削除の際に、そのエントリがユーザが追加したものかセキュア ゲートウェイで追加されたものかに応じて 2 つの手順を使用できます。

ユーザが追加した接続エントリの削除

ステップ 1 AnyConnect のホーム画面を開きます。

ステップ 2 削除する接続エントリの右にある、詳細表示ボタンをタップします。

ステップ 3 [Delete VPN Connection] をタップします。

ステップ 4 確認プロンプトが表示されたら [OK] をタップします。

接続パラメータの画面が閉じ、AnyConnect のホーム画面からエントリが削除されます。

自動的に追加された接続エントリの削除

セキュア ゲートウェイによって追加されたすべての VPN 接続エントリを完全に削除し、その AnyConnect プロファイルを削除するには、次の手順に従います。

ステップ 1 AnyConnect のホーム画面で、[Diagnostics] > [Profile] > [Delete Profile] の順にタップします。

（注） 同じ ASA のドメイン、IP アドレス、またはグループ URL に再接続すると、プロファイルがリロードされ、セキュリティ ポリシーが再度適用されます。

AnyConnect の管理

アプリケーション設定の指定

テーマの変更

AnyConnect では、2 つのテーマを使用できます。

- [Cisco Default Theme] : Apple iOS のインターフェイスに似た、カラー コントラストがあり、青系統の影の色を強調したテーマです。
- [High Contrast] : シスコのデフォルト テーマに代わるテーマです。このテーマでは、色がいくつか使用されていますが、白と黒が強調されています。視覚障がいを持つユーザ、または明るい場所で表示するときに適しています。

AnyConnect のユーザ インターフェイスのテーマを変更するには、次の手順に従います。

ステップ 1 AnyConnect アプリ内で、[Settings] > [Theme] の順にタップします。

ステップ 2 目的のテーマ（[Cisco Default Theme] または [High Contrast]）をタップします。

選択したテーマの横に、Apple iOS によってチェック マークが挿入され、アプリケーション テーマがただちに変更されます。

ステップ 3 [Settings] をタップして、[Settings] 画面に戻ります。

外部制御の設定

外部制御を有効にすると、管理者から送信されたリンクをクリックして、接続の作成または証明書のインポートなどの作業を実行できます。AnyConnect 管理者以外から送信された URI のコマンドに従って Apple iOS を動作させることもできます。

ステップ 1 AnyConnect アプリ内で、[Settings] > [Theme] の順にタップします。

ステップ 2 次のオプションのいずれかを選択します。

- [Disable] : 外部制御は許可されません。電子メール内または Web ページ上の URI をクリックすると、次のエラー メッセージが表示されます。

  「The External Control feature is disabled. Enable it from the AnyConnect settings.」

- [Prompt] : モバイル デバイス ユーザが電子メール内または Web ページ上の URI をクリックすると、リモート サーバへの接続を受け入れるか、拒否するかを尋ねる次のメッセージが表示されます。

  「Another application has requested that AnyConnect connect to <asa.example.com>.Do you want to allow this?」

- [Enable] : モバイル デバイス ユーザが電子メール内または Web ページ上の URI をクリックすると、ユーザの動作を中断することなく URI に指定されたコマンドが実行されます。

ステップ 3 [Settings] をタップして、[Settings] 画面に戻ります。

信頼できないサーバのブロッキング

このアプリケーションの設定により、セキュア ゲートウェイを特定できない場合に AnyConnect がその接続を自動的にブロックするかどうかが決まります。この保護はデフォルトで ON になっています。OFF にできますが、推奨しません。

AnyConnect は、期限切れや無効な日付、誤ったキーの用途、名前の不一致が原因の証明書エラーがあり、接続がブロックされている場合、サーバから受信した証明書を使用してその ID を検証します。

この設定が ON になっている場合、信頼できない VPN サーバのブロッキングの通知により、このセキュリティの脅威が警告されます。

ステップ 1 AnyConnect アプリ内で、[Settings] > [Theme] の順にタップします。

ステップ 2 [Block Untrusted Servers] スイッチをタップして、自動ブロッキングを有効または無効にします。

FIPS モードの設定

FIPS モードでは、すべての IPsec VPN 接続で連邦情報処理標準（FIPS）暗号化アルゴリズムが使用されます。ネットワークに IPsec VPN 接続するためにモバイル デバイス上で FIPS モードを有効にする必要がある場合、管理者から通知されます。

ステップ 1 AnyConnect アプリ内で、[Settings] をタップします。

ステップ 2 [FIPS Mode] スイッチをタップして、FIPS モードを有効または無効にします。

証明書の管理

証明書は VPN 接続の各端（セキュア ゲートウェイまたはサーバ、および AnyConnect クライアントまたはユーザ）をデジタル識別するために使用されます。サーバ証明書は AnyConnect 向けのセキュア ゲートウェイを識別し、ユーザ証明書はセキュア ゲートウェイ向けの AnyConnect ユーザを識別します。証明書は認証局（CA）から取得されます。また、認証局によって検証されます。

接続を確立する際、AnyConnect は常にセキュア ゲートウェイからのサーバ証明書を待ちます。セキュア ゲートウェイは、AnyConnect からの証明書のみを待ちます（そのように設定されている場合）。VPN 接続を認証するもう 1 つの方法は、AnyConnect ユーザが証明書を手動で入力するのを待つことです。実際、セキュア ゲートウェイは、AnyConnect ユーザをデジタル証明書、手動による証明書の入力、またはその両方で認証するように設定できます。証明書のみの認証では、ユーザ介入なしで VPN を接続できます。

セキュア ゲートウェイおよびデバイスに対する証明書の配布および使用については、管理者から指示されます。管理者からの指示に従い、AnyConnect VPN のサーバ証明書とユーザ証明書のインポート、使用、および管理を行います。このマニュアルの証明書および証明書の管理に関連した情報および手順は、ユーザに理解し、参照してもらうために提供されています。

AnyConnect は、独自の証明書ストアに認証用のユーザ証明書とサーバ証明書を保存します。AnyConnect 証明書ストアは、[Diagnostics] > [Certificates] 画面から管理します。

ユーザ証明書の管理

AnyConnect ユーザがデジタル証明書を使用してセキュア ゲートウェイへの認証を行うためには、お使いのデバイスの AnyConnect 証明書ストアにユーザ証明書を保存しておく必要があります。ユーザ証明書は、管理者から指示される次のいずれかの方法を使用してインポートされます。

- デバイスのファイル システム、デバイスのクレデンシャル ストレージ、またはネットワーク サーバから手動でインポート。
- 管理者から提供される電子メール内、または Web ページ上のハイパーリンクをクリックしてインポート。
- ユーザに証明書を提供するために管理者が設定したセキュア ゲートウェイに接続してインポート。

インポートされた証明書は、特定の接続エントリに関連付けられるか、または接続の確立中に自動認証のために自動的に選択されます。

AnyConnect ストア内のユーザ証明書は、認証に必要なくなった場合は削除できます。

サーバ証明書の管理

接続の確立中にセキュア ゲートウェイから受信したサーバ証明書は（証明書が有効で信頼できる場合のみ）、そのサーバを AnyConnect に対して自動的に認証します。その他の場合：

- 有効だが信頼できないサーバ証明書は、確認、認可後に、AnyConnect 証明書ストアにインポートされます。AnyConnect ストアにサーバ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に対する後続の接続は自動的に受け入れられます。
- 無効な証明書は AnyConnect ストアにインポートできませんが、現在の接続を完了するために受け入れられます。推奨しません。

AnyConnect ストア内のサーバ証明書は、認証に必要なくなった場合は削除できます。

証明書の表示

AnyConnect 証明書ストアにインポートされているユーザ証明書とサーバ証明書を表示するには、次の手順を実行します。

ステップ 1 [AnyConnect] メニューで、[Diagnostics] > [Certificates] の順にタップします。

ステップ 2 [User] または [Server] タブをタップして、AnyConnect 証明書ストア内の証明書を表示します。

ステップ 3 この画面を使用して、次の処理のいずれかを実行します。

- 証明書の詳細表示ボタンをタップして、証明書のプロパティを表示します。
- [Edit] ボタンをタップして、証明書を削除します。
- [Import Certificate...] をタップして、証明書を手動でインポートします。
- [Delete All Certificates] をタップして、デバイスからすべての証明書を削除します。

AnyConnect プロファイルの表示と管理

AnyConnect VPN クライアント プロファイルは XML ファイルで、クライアントの動作を指定し、VPN 接続を識別します。VPN クライアント プロファイル内の各接続エントリは、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、およびその他の接続属性、ポリシー、および制約を指定します。デバイスに対してユーザがローカルに設定した VPN 接続に加えて、これらの接続エントリが、VPN 接続を開始するときに選択する対象として AnyConnect のホーム画面に表示されます。

（注） AnyConnect は、デバイス上で一度に 1 つの VPN クライアント プロファイルのみを維持します。

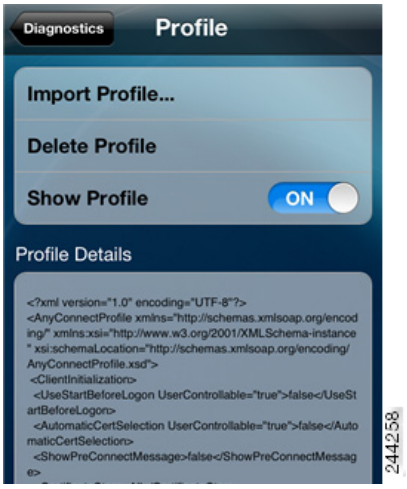
ユーザはそれぞれのデバイスの AnyConnect VPN クライアント プロファイルを管理できるようになりました。ユーザは次の操作を実行します。

ステップ 1 AnyConnect タブ バーで、[Diagnostics] をタップします。

[Diagnostics] 画面が開きます。

ステップ 2 [Profile] をタップします。

この画面を使用して、次の処理のいずれかを実行します。



- **[Import Profile...]**：インポートするプロファイルの URL を指定します。
- **[Delete Profile]**：この操作を確定し、デバイスから現在のプロファイルを削除します。
- **[Show Profile]**：[ON] をタップして、デバイスの現在のプロファイルを表示します。

ローカリゼーションの管理

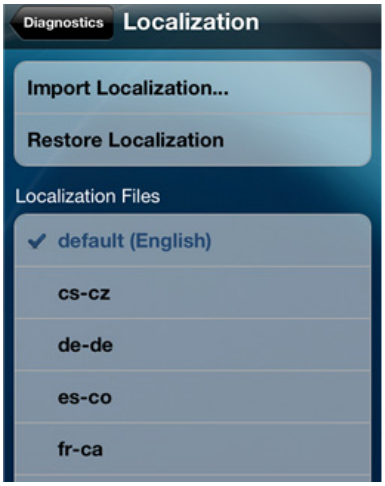
AnyConnect インストール時に、設定されている言語に従いデバイスがローカライズされます。インストール時にサポートされる言語のリストについては、デバイスのローカリゼーションを参照してください。デバイス上のローカリゼーションのさらなる管理は、管理者が指定する手順に基づいて実行します。

ステップ 1 AnyConnect タブ バーで、[Diagnostics] をタップします。

[Diagnostics] 画面が開きます。

ステップ 2 [Localization] をタップします。

この画面を使用して、次の処理のいずれかを実行します。



- [Import Localization...] : インポートするサーバ アドレスと言語を入力します。このローカリゼーション データは、事前にパッケージ化されて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。デバイスにローカリゼーション データをインポートするその他の方法については、ローカリゼーション データのインポートを参照してください。
- [Restore Localization] : インポートされているすべてのローカリゼーション ファイルを削除し、インストール済みのローカリゼーション ファイルを復元します。

ローカリゼーション データのインポート

インストール後に、AnyConnect パッケージでサポートされていない言語のローカリゼーション データを、次のようにしてインポートします。

- 管理者によって提供され、ローカリゼーション データをインポートするように定義されたハイパーリンクをクリックします。

  管理者は、クリックするとローカリゼーション データがインポートされるハイパーリンクを、電子メールまたは Web ページで提供します。この方法では、ユーザ用の AnyConnect の設定および管理を簡素化するため、管理者に提供されている機能である AnyConnect URI ハンドラを使用します。

  （注） ユーザは、外部制御を設定してプロンプトを表示するか、AnyConnect 設定内で有効にすることにより、この AnyConnect 操作を許可する必要があります。この設定方法については、外部制御の設定を参照してください。

- VPN 接続時にダウンロード可能なローカリゼーション データを提供するように管理者が設定したセキュア ゲートウェイに接続します。

  この方法を使用する場合には、管理者が適切な VPN 接続情報を提供するか、または XML プロファイル内に事前定義された接続エントリを提供します。VPN 接続時に、ローカリゼーション データがデバイスにダウンロードされ、ただちに有効になります。

- [Localization Management] 画面を使用して、指定されたサーバから手動でローカリゼーション データをインポートします。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。インポート手順については、ローカリゼーションの管理を参照してください。

AnyConnect の削除

デバイスから AnyConnect を削除するには、次の手順に従います。

ステップ 1 [AnyConnect] メニューで、[Diagnostics] をタップします。

ステップ 2 [Profile] をタップします。

ステップ 3 [Delete Profile] をタップします。

ステップ 4 メニュー ボタンを押して AnyConnect のホーム画面に移動します。

ステップ 5 AnyConnect をフォルダに入れた場合は、そのフォルダを開きます。

ステップ 6 （**X**）アイコンが AnyConnect アイコンの上に表示されるまで、AnyConnect アイコンをタップしたままにします。

ステップ 7 削除アイコンをタップします。

AnyConnect 情報の取得

AnyConnect のバージョンおよびライセンスの詳細の表示

AnyConnect のバージョンおよびライセンスの詳細を表示するには、タブ バーの [About] アイコンをタップします。

ヒント リンクをタップすると、本ガイドの最新の更新バージョンが Safari で開かれます。これらの手順が後で必要になった場合のリソースとして使用できます。

システム情報の表示

AnyConnect の操作に関連したシステム情報は、[System Information] 画面に表示されます。この情報を表示するには、次の手順を実行します。

ステップ 1 AnyConnect のホーム画面に移動します。

ステップ 2 AnyConnect タブ バーで、[Diagnostics] をタップします。

ステップ 3 [System Information] をタップします。

次の情報が表示されます。

- [Wi-Fi] : IPv4 アドレス、IPv4 サブネット マスク、IPv6 アドレス、IPv6 サブネット マスク、MAC アドレス
- [Cellular Data] : ネットワーク IP、サブネット マスク
- DNS サーバ
- [Device] : プラットフォーム バージョン、デバイス タイプ、UDID
- ルーティング テーブル

VPN 接続統計の概要の表示

VPN 接続があり、[Statistics] 画面を開いている場合、AnyConnect は統計情報を記録します。

現在の VPN 接続についての統計情報を表示するには、AnyConnect のホーム画面に移動し、下部にある [Statistics] タブをタップします。[Statistics] 画面が開きます。

[Statistics] 画面に表示される項目は、次のとおりです。

- [Status]（接続状態）
- [Server]（アドレス）
- Time Connected
- Client Address
- Bytes Sent

- Bytes Received
- [Details]：タップすると詳細な統計情報を表示できます（これについては次の項で説明します）。
- [Graphs]：タップすると、送受信バイト数のグラフが表示されます。

詳細な統計情報の表示

現在の VPN 接続についての詳細な統計情報を表示するには、次の手順に従います。

ステップ 1 AnyConnect のホーム画面で、[Statistics] > [Details] の順にタップします。

[Detailed Statistics] 画面が開きます。

ステップ 2 スクロールして、すべての統計情報を確認します。

[Detailed Statistics] 画面には、次の情報が表示されます。

- Connection Information
  - State
  - Mode
  - Time Connected
- Address Information
  - Client
  - Server
  - Client (IPv6)
- Bytes
  - Sent
  - Received
- Frames
  - Sent
  - Received
- Control Frames
  - Sent
  - Received
- Transport Information
  - Protocol
  - Cipher
  - Compression
- [Feature Configuration] : [FIPS Mode]
- [Secure Routes] : 通信相手が 0.0.0.0 かつサブネット マスクが 0.0.0.0 の場合、すべての VPN トラフィックが暗号化され、VPN 接続を通して送受信されることを意味します。

送受信バイト数のグラフを表示する

ステップ 1 AnyConnect のホームページに移動します。

ステップ 2 [Statistics] > [Graphs] の順にタップします。

送受信バイト数を示すグラフが表示されます。

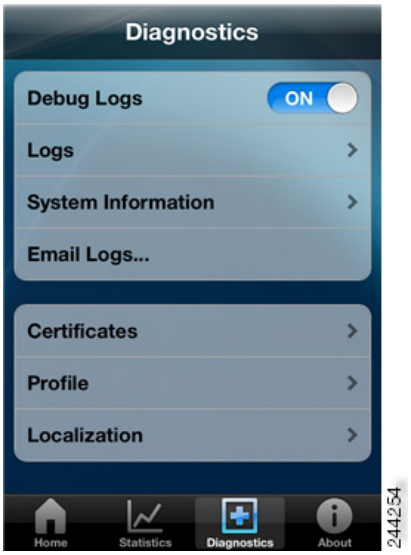
ログ メッセージの表示および管理

デバイス リソースに対する不要な負荷を避けるために、AnyConnect のデフォルトではメッセージをログ記録しません。トラブルシューティングの場合のみログを有効化してください。

ログ メッセージを有効化、表示、管理するには、次の手順に従います。

ステップ 1 AnyConnect タブ バーに移動し、[Diagnostics] をタップします。

[Diagnostics] 画面が開きます。

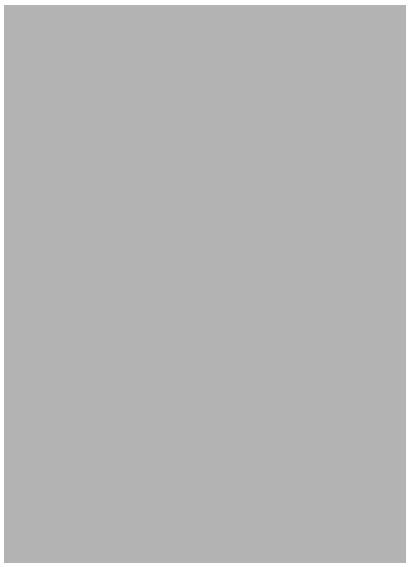


ステップ 2 [Debug Logs] を [ON] にして、ロギングを有効にします。

この [Diagnostics] 画面で、次の項目を選択します。

- [System Information] : 詳細については、システム情報の表示を参照してください。
- [Email Logs] : タップすると、電子メール アドレスにログ メッセージが送信されます。電子メール アプリケーションによって、現在のログおよびデバイス情報を含む電子メール メッセージが作成されます。
- [Certificates] の管理。詳細については、証明書の管理を参照してください。
- [Profiles] の管理。詳細については、AnyConnect プロファイルの表示と管理を参照してください。
- [Localization] の管理。詳細については、ローカリゼーションの管理を参照してください。

ステップ 3 [Logs] をタップすると、[Logs] 画面が開きます。



[Logs] 画面を使用して、次のいずれかの操作を行います。

- [Messages]：タップするとログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [Service]：タップするとサービス デバッグ ログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [App]：タップするとアプリケーション デバッグ ログ メッセージが表示されます。さらなるメッセージを確認するには、スクロールします。
- [Clear Logs]：ログ メッセージを削除する場合は、[Clear Logs] をタップします。

[Diagnostics] をタップして、[Diagnostics] 画面に戻ります。

AnyConnect 通知への応答

信頼できない VPN サーバの通知への応答

表示される信頼できない VPN サーバ通知のタイプは、Block Untrusted VPN Server アプリケーションのプリファレンスによって異なります。

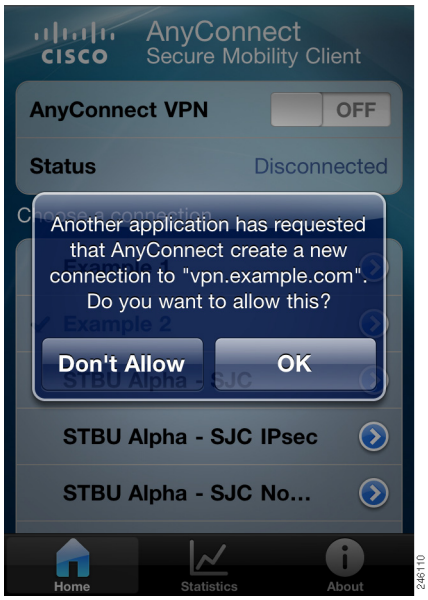
- 有効になっている場合、信頼できない VPN サーバのブロッキングの通知が表示されます。次のいずれかを選択します。
  - [Keep Me Safe]：この設定とこのブロッキング動作を保持します。
  - [Change Settings]：ブロッキングをオフにします。

  Block Untrusted VPN Server を変更したら、VPN 接続を再開します。
- 有効になっていない場合、信頼できない VPN サーバの非ブロッキングの通知が表示されます。次のいずれかを選択します。

- [Cancel]：信頼できないサーバへの VPN 接続を中断します。
- [Continue]：信頼できないサーバへの接続を行います。これは推奨しません。
- [View Details]：証明書の詳細を表示し、今後の承認のためにサーバ証明書を AnyConnect 証明書ストアにインポートし、接続を継続するかどうかを決めます。

「Another Application has requested that AnyConnect...Do you want to allow this?」への対処

AnyConnect はデバイスを保護するために、別のアプリケーションによって、接続プロファイルの作成、VPN 接続の確立、または VPN からの接続解除が試行されたときなどにユーザに通知します。



デバイスおよびデータを保護するために、次のようなプロンプトのタイプで [OK] をタップして承認してよいかどうかをシステム管理者に確認してください。

- 作成：「Another application has requested that AnyConnect create a new connection to '*host*'. Do you want to allow this?」
- 接続:「Another application has requested that AnyConnect connect to '*host*'. Do you want to allow this?」
- 接続：「Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this?」

（注） これらのメッセージが表示されるのは、外部制御が [Prompt] に設定されている場合だけです。お使いのモバイル デバイスのホームページを開いて [Settings] > [AnyConnect] > [External Control] にナビゲートして、デバイスの外部制御を設定します。

トラブルシューティング

この項では、一般的な問題に対する解決策を説明します。これらの解決策を試みても問題が解決しない場合は、所属する組織の IT サポート部門に問い合わせてください。

- **一部の接続プロファイルで編集と削除ができません。**

  AnyConnect 接続プロファイルにインポートしたホスト エントリに影響するポリシーが、システム管理者によって設定されています。これらのプロファイルを削除するには、[Diagnostics] > [Profile] > [Clear Profile Data] の順にタップします。

- **設定を保存または編集しようとするとエラーが発生します。**

  オペレーティング システムの既知の問題が原因です。Apple は、この問題の解決に取り組んでいます。回避策として、アプリケーションの再起動を試してください。

- **接続タイムアウトおよび未解決ホスト。**

  インターネット接続の問題、携帯電話の信号レベルが低い、およびネットワークの輻輳などが原因で、タイムアウトや未解決ホスト エラーを引き起こすことがよくあります。LAN を利用できる場合は、デバイスの Settings アプリケーションを使用し、最初に LAN との接続の確立を試してください。タイムアウトになったときに、何度か再試行することで、成功することがよくあります。

- **デバイスがスリープから復帰したときに VPN 接続が再確立されません。**

  VPN 接続エントリで [Network Roaming] を有効化します。ネットワーク ローミングを有効化しても問題が解決されない場合は、EDGE（2G）、1xRTT（2G）、3G、または Wi-Fi 接続を確認します。

  （注） この問題は、ユーザが所属する組織での VPN の設定に基づく動作である場合があります。

- **証明書ベースの認証が機能しません。**

  該当する証明書を以前は使用できた場合、証明書の有効性と期限を確認します。接続に対して適切な証明書を使用しているかどうかをシステム管理者に確認します。

- **Apple iOS Connect On Demand 機能が動作しない、または接続できません。**

  その接続で、[Never Connect] リスト内に競合する規則がないかどうかを確認します。その接続に [Connect If Needed] 規則が存在する場合は、[Always Connect] 規則に置き換えます。

- **AnyConnect は接続を確立できませんでしたが、エラー メッセージが表示されません。**

  メッセージは、AnyConnect アプリケーションが開かれている場合にのみ表示されます。

- **Cisco AnyConnect というプロファイルがありますが削除できません。**

  アプリケーションの再起動を試してください。

- **AnyConnect アプリケーションを削除しても、Apple iOS の VPN 設定に VPN 設定が表示されます。**

  これらのプロファイルを削除し、AnyConnect を再インストールするには、[Diagnostics] > [Profile] > [Clear Profile Data] の順にタップします。

VPN に影響を及ぼす Apple iOS の既知の問題

次の iOS の問題を Apple に報告しています。これらの問題は、今後の iOS リリースで解決される可能性があります。

- デバイスが休止中の場合、DTLS パケットを受信してもデバイスが起動しない。ただし、通知または Facetime が有効になっている場合、TLS パケットによりデバイスが起動します。AnyConnect は、デバイスが休止状態になると DTLS トンネルを自動的に接続解除して、TLS 接続経由で受信したパケットでデバイスを起動できるようにします。DTLS トンネルは、デバイス再開時に復元されます。
- iPod Touch のバックグラウンドで実行中の音声アプリケーションが、VPN 経由でパケットを受信できない。この機能は、iPhone デバイスでは想定どおりに動作します。
- VPN 設定に多数のルートまたはスプリット DNS ルールが含まれている場合、Apple デバイスが VPN 接続を確立できない。このバグは、たとえば、接続時に ASA 設定によって、トラフィックを個々のサブネットに導く 70 以上のルールがある VPN Split-Include リストがプッシュされる場合に発生します。このバグがユーザに影響を及ぼすのを防ぐには、tunnel-all 設定を適用するか、ルールの数を減らします。
- モバイル デバイスに多数の VPN 接続が設定されている場合に、AnyConnect が遅くなったり、クラッシュしたりすることがある。
- IPv6 トラフィックのトンネリングを希望するお客様は、iPhone および iPad を iOS 5.0 以降にアップグレードする必要がある。iOS 4.3 には、デフォルトの IPv6 ルートを設定できないことが原因で、AnyConnect が IPv6 トラフィックを正しく処理できない既知の問題があります。

Apple iOS は Tunnel-all のすべてのローカル LAN トラフィックを許可

Apple iOS は、tunnel-all ポリシーが有効であるかどうかに関係なく、デバイスのコア操作に欠かせないトラフィックを許可します。トンネル ポリシーに関係なく、Apple iOS がクリア テキストで送信するトラフィックの例には、次のものがあります。

- すべてのローカル LAN トラフィック
- 既存接続用のスコープ指定ルート（VPN 起動前にストリーミングされているビデオなど）
- コア Apple サービス（Visual Voice Mail トラフィックなど）

AnyConnect for Apple iOS の制限

このリリースの AnyConnect for Apple iOS は、リモート アクセスに関連している機能のみサポートしています。

- AnyConnect は、次のタイプの VPN 設定をサポートしています。
  - 手動で生成された設定。
  - AnyConnect VPN クライアント プロファイルがインポートした設定。
  - iPhone Configuration Utility が生成した設定。iPhone Configuration Utility の詳細については、http://www.apple.com/support/iphone/enterprise/ を参照してください。
- iPhone Configuration Utility によって作成された VPN 設定は、Network Roaming をサポートしません。ユーザが Network Roaming を必要とする場合は、AnyConnect プロファイルを使用します。
- 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、ユーザが vpn.example1.com にアクセスしてから vpn.example2.com にアクセスした場合、vpn.example2.com からインポートされた AnyConnect VPN クライアント プロファイルによって vpn.example1.com からインポートされたクライアント プロファイルが置き換えられます。
- 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。

- 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。

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/