Android 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 2.5.x）

更新日：2012 年 2 月 29 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 Cisco AnyConnect Secure Mobility Client 2.5.x for Android 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。

© 2004–2012 Cisco Systems, Inc. All rights reserved.
© 2004-2012, シスコシステムズ合同会社 . All rights reserved.

概要

Cisco AnyConnect Secure Mobility Client for Android は、企業ネットワークへのシームレスかつ安全なリモート アクセスを実現します。AnyConnect 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、企業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。

組織によっては Android 向け AnyConnect の使用方法に関するその他のマニュアルが用意されていることがあります。

AnyConnect のインストールまたはアップグレード

Android Market に移動し、ご使用のデバイスに該当する AnyConnect パッケージを検索し、取得してください。

デバイスについて	インストールするもの
サポートされる Android デバイスの場合は、VPN 接続の全機能を Android OS に提供する、ブランド固有の AnyConnect パッケージがシスコから提供されます。 これらのブランド固有の AnyConnect クライアントは、デバイス ベンダーとのパートナーシップに従って提供されるものであり、サポートされるデバイスに適した AnyConnect クライアントです。	ブランド固有の AnyConnect クライアントには、次のものがあります。 • Samsung 社のデバイスについては、インストールする Samsung AnyConnect パッケージの決定を参照してください。 • HTC 社のデバイスには、HTC AnyConnect 2.5.5116 をインストールします。 • Lenovo 社のデバイスには、Lenovo AnyConnect 2.5.5116 をインストールします。 • Motorola 社のデバイスには、Motorola AnyConnect 2.5.5118 をインストールします。

デバイスについて	インストールするもの
Android 4.0（Ice Cream Sandwich）以降を実行している場合は、Android 4.0 以降の Android VPN Framework（AVF）でサポートされる VPN 接続を提供する AnyConnect クライアントが、シスコから提供されます。 AVF は、基本的な VPN 接続のみ提供します。このような基本的 VPN 機能に依存する AnyConnect AVF クライアントでは、ブランド固有のパッケージが持つフルセットの VPN 機能が提供されません。	AVF AnyConnect 2.5.5116。 **注**：Android 4.0 以降を実行する未サポートのデバイスには、AnyConnect AVF クライアントを推奨します。サポートされているデバイスでは、Android OS バージョンに関係なく、ブランドに固有の AnyConnect クライアントを使用する必要があります。
root 化された Android 2.1 以降を実行している場合は、プレビューおよびテストのみを目的として、root 化された Android モバイル デバイス用の AnyConnect パッケージが、シスコから提供されます。シスコは、このようなクライアントをサポートしていません。ただし、2.1 以降を実行する大部分の root 化されたデバイス上で動作します。 tun.ko モジュールおよび iptables の両方が必要です。不足しているものがある場合は、VPN 接続を確立しようとしたときに、それを通知するエラー メッセージが AnyConnect から表示されます。tun.ko モジュールがない場合、対応するデバイスのカーネルを入手またはビルドして、`/data/local/kernel_modules/` ディレクトリに配置します。	root 化された AnyConnect 2.5.5116。 **注意**：お使いのデバイスを root 化すると、デバイスの保証が無効になります。シスコでは、root 化されたデバイスを公式にはサポートしていません。お使いのデバイスを root 化する手順も提供していません。お使いのデバイスの root 化を選択する場合は、ユーザ自身の自己責任において行ってください。

（注） Android 向け AnyConnect は、Android Market からのみダウンロードで提供されます。Cisco Web サイトから、またはセキュア ゲートウェイに接続後にダウンロードすることはできません。

インストールする Samsung AnyConnect パッケージの決定

シスコは、Samsung 社のデバイスとの互換性を確保するため、2 つの AnyConnect パッケージを提供しています。

- Samsung AnyConnect 2.5.5116 パッケージは、2011 年 9 月以降に製造またはアップグレードされたデバイスに適用されます。
- Samsung AnyConnect Legacy 2.5.5116 パッケージは、それよりも古い（2011 年 9 月よりも前に製造された）アップグレードされていないデバイスに適用されます。

インストールしようとして、以下のいずれかのエラー メッセージが表示された場合は、別の Samsung パッケージを試してください。

- 「Installation Error: Unknown reason -8.」
- 「Incompatible with other application(s) using the same shared user ID.」

Android 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] > [Language and Keyboard] > [Select locale] 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 Menu] > [Settings] > [Localization Management] 画面で `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。

Android AnyConnect のライセンス

オープン ソース ライセンス通知については、『*Open Source Used in Cisco AnyConnect Secure Mobility Client, Release 2.5 for Android*』を参照してください。

エンド ユーザ ライセンス契約書については、『*End User License Agreement*』を参照してください。

サポートされる Android デバイス

AnyConnect は、次の製造元からのデバイスをサポートします。

- Samsung 社のデバイス向け AnyConnect
- HTC 社のデバイス向け AnyConnect
- Lenovo 社のデバイス向け AnyConnect
- Motorola 社のデバイス向け AnyConnect

シスコは、次のものも提供しています。

- Android VPN Framework デバイス向け AnyConnect
- root 化されたデバイス向け AnyConnect

Samsung 社のデバイス向け AnyConnect

Samsung AnyConnect および Samsung AnyConnect Legacy リリース 2.5.5116 は、次に示す Samsung 製品ラインをサポートします。デバイスでは、Samsung 社からの最新のソフトウェア アップデートおよび識別された Android リリースを実行している必要があります。お使いのデバイスに適用するパッケージを判断するには、Android 向け AnyConnect ユーザ ガイドにあるインストール手順を参照してください。

製品	Android リリース	モデル番号
Galaxy Note		GT-N7000 GT-I9220
Galaxy S	2.3.3 以降	GT-I9000 SC-02B SGB-N013
Galaxy S II	2.3.3 以降	GT-I9100 GT-I9100G GT-I9100M GT-I9100T GT-I9103 GT-I9108 SC-02C SGH-I727 SGH-I777 SGH-N033 SGH-T989 SHW-M250K SHW-M250L SHW-M250S SPH-D170
Galaxy Tab 7（WiFi 専用）[1]	2.3.3 以降	GT-P1000 GT-P1000M GT-P1000R GT-P1010 SC-01C SCH-I800
Galaxy Tab 7.0 Plus		GT-P6200 GT-P6210
Galaxy Tab 7.7		GT-P6800 SCH-I815
Galaxy Tab 8.9	3.0 以降	GT-P7300 GT-P7310
Galaxy Tab 10.1	Samsung Touch Wiz アップデート対応 3.1 以降	GT-P7300 GT-P7310 GT-P7500 GT-P7500D GT-P7500M GT-P7500R GT-P7510 SC-01D
Galaxy W		GT-I8150 SGH-T679
Galaxy Xcover		GT-S5690
Galaxy Y Pro		GT-B5510B GT-B5510L
Illusion		SCH-I110

製品	Android リリース	モデル番号
Infuse		SCH-I997
Stratosphere		SCH-I405

1. Samsung Galaxy Tab 7 モバイル デバイスの Sprint 配布はサポートされません。

（注） Samsung 社は、各モバイル サービス プロバイダーでこれらの製品ラインのデバイスをブランド変更します。

HTC 社のデバイス向け AnyConnect

HTC AnyConnect Release 2.5.5116 は、次の HTC 製品ラインをサポートします。ただし、デバイスが必要な最低限のソフトウェアを実行している場合に限ります。この情報は、[Settings] > [About phone] > [Software information] > [Software number] にあります。

製品	ソフトウェア番号の最小要件
Desire HD	3.04
EVO 4G+（Korea Telecom）	2.1
EVO View 4G（Sprint）	2.06
Explorer	1.05
Flyer	3.07
Incredible S	3.03
myTouch 4G Slide	1.50.531.0
Raider 4G（Korea Telecom）	2.02
Rhyme（GSM）	1.13
Beats Audio 対応 Sensation XL	1

このリストに追加される製品については、http://www.htcpro.com/enterprise/VPN を参照してください。

Lenovo 社のデバイス向け AnyConnect

Lenovo AnyConnect リリース 2.5.5116 は、Lenovo ThinkPad タブレット製品をサポートします。ただし、デバイスが Lenovo 社からの最新のソフトウェア アップデートを実行している場合に限ります。

Motorola 社のデバイス向け AnyConnect

Motorola AnyConnect リリース 2.5.5118 は、次の Motorola 製品ラインをサポートします。ただし、デバイスが Motorola 社からの最新のソフトウェア アップデートを実行している場合に限ります。

製品	ソフトウェアの最小要件
ATRIX 2	55.13.25
XYBOARD	
RAZR	6.12.173
RAZR MAXX	6.12.173
DROID 4	6.13.215

Android VPN Framework デバイス向け AnyConnect

AVF AnyConnect リリース 2.5.5116 は、Android 4.0（Ice Cream Sandwich）以降の Android VPN Framework（AVF）でサポートされる VPN 接続を提供します。

AVF は、基本的な VPN 接続のみ提供します。このような基本的 VPN 機能に依存する AnyConnect AVF クライアントでは、ブランド固有のパッケージが持つフルセットの VPN 機能が提供されません。

（注） Android 4.0 以降を実行する未サポートのデバイスには、AnyConnect AVF クライアントを推奨します。サポートされているデバイスは、Android オペレーティング システムのバージョンに関係なく、ブランドに固有の AnyConnect クライアントを使用する必要があります。

root 化されたデバイス向け AnyConnect

シスコは、プレビューおよびテストの目的でのみ、Android 2.1 以降を実行する root 化された Android モバイル デバイス向けに Rooted AnyConnect リリース 2.5.5116 を提供しています。シスコは、このクライアントをサポートしていませんが、2.1+ を実行する大部分の root 化されたデバイス上で動作します。問題が発生した場合、その問題を android-mobile-feedback@cisco.com に報告してください。解決のために、最大限の努力を払います。

tun.ko モジュールおよび iptables の両方が必要です。不足しているものがある場合は、VPN 接続を確立しようとしたときに、それを通知するエラー メッセージが AnyConnect から表示されます。tun.ko モジュールがない場合、対応するデバイスのカーネルを入手またはビルドして、`/data/local/kernel_modules/` ディレクトリに配置します。

注意 お使いのデバイスを root 化すると、デバイスの保証が無効になります。シスコでは、root 化されたデバイスをサポートしていません。お使いのデバイスを root 化する手順も提供していません。お使いのデバイスの root 化を選択する場合は、ユーザ自身の自己責任において行ってください。

AnyConnect の開始

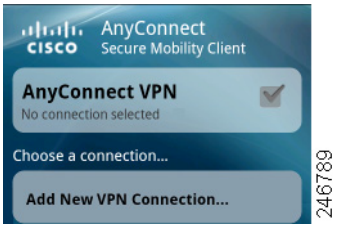
AnyConnect ホーム画面

AnyConnect アプリケーション アイコン（図 1）をタップすると、

図 1　　[AnyConnect] アイコン

AnyConnect の初期ホーム画面（図 2）が開きます。

図 2　　AnyConnect ホーム画面



- [AnyConnect VPN]：現在の VPN 接続エントリを識別します。このチェックボックスは、接続がアクティブかアイドルかを示します。この VPN に接続または切断するには、[AnyConnect VPN] 領域をタップします。
- **[Choose a connection...]**：接続エントリを追加した後、この領域に、選択可能な設定済みのすべての VPN 接続エントリが表示されます。このリストには、XML プロファイルで定義されたエントリと、ユーザが設定したエントリの両方が含まれます。接続をタップすると、その接続が現在の VPN となり、接続が始まります。
- **[Add New VPN Connection]**：接続エントリを手動で定義します。これをタップして、接続の [Description]、[Server Address]、および [Certificate] ポリシーを入力します。

接続エントリを追加すると、AnyConnect のホーム画面に入力内容が表示されます（図 3）。

図 3　AnyConnect 接続エントリ

AnyConnect メニュー

メニューをタップまたは押すと、AnyConnect のメニュー オプションが表示されます（図 4）。

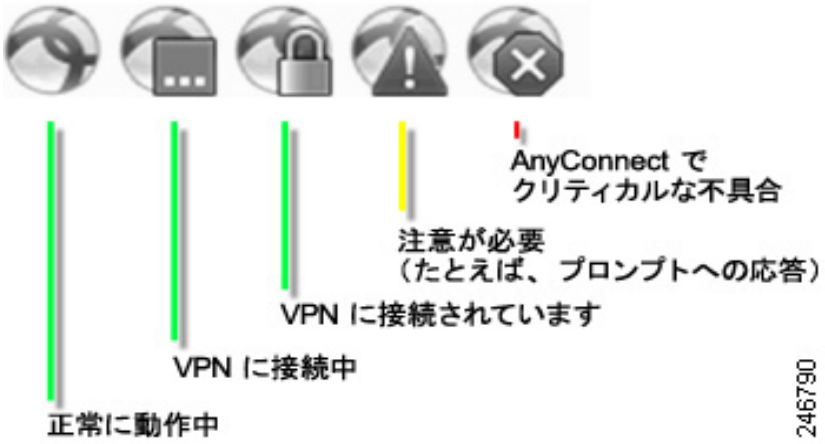
図 4　AnyConnect メニュー

- [Statistics]：現在のアクティブ VPN 接続に関する概要と詳細な統計情報が表示されます。詳細については、統計情報の表示を参照してください。
- [Diagnostics]：AnyConnect のログ メッセージを表示、送信、およびクリアします。詳細については、ログ メッセージの表示および管理を参照してください。
- [Settings]：アプリケーションのプリファレンスを指定し、AnyConnect の各種設定を管理します。詳細については、Android デバイスでの AnyConnect の管理を参照してください。
- [About]：AnyConnect のバージョンとライセンス情報を表示します。詳細については、AnyConnect のバージョンおよびライセンスの詳細の表示を参照してください。
- [Exit]：AnyConnect を終了します。

ステータス バーの AnyConnect アイコンについて

デフォルトでは、AnyConnect は、Android ウィンドウの一番上にある Android ステータス バーのアイコンを変更することによって、ステータスを表示します（図 5）。

図 5　　Android ステータス バーの AnyConnect 通知アイコン



接続前の準備

VPN 接続を開始するには、デバイスで接続エントリが定義されている必要があります。

接続エントリを手動で定義するには、ネットワーク要件に従って、管理者から以下の 1 つ以上を取得する必要があります。この情報は、VPN 接続エントリの追加で使用します。

- 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 ASA のドメイン名、IP アドレス、またはオプションのグループ 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。
- デジタル証明書。

または、管理者が社内ネットワークのリンクを提供することがあります。リンクをタップしてデバイスに必要な接続エントリを追加できます。

VPN への接続

AnyConnect のホーム画面に表示された接続エントリから 1 つを選択し、VPN に接続します。接続リストは、次のいずれかの方法で作成されたエントリで構成されます。

- 手動で設定された接続エントリ。接続エントリの追加方法については、VPN 接続エントリの追加を参照してください。
- 社内ネットワークの管理者によって提供されたリンクをクリックした後に追加された接続エントリ。
- VPN 接続時にセキュア ゲートウェイからダウンロードされた、現在の AnyConnect XML 内に定義された接続エントリ。

VPN 接続エントリの追加

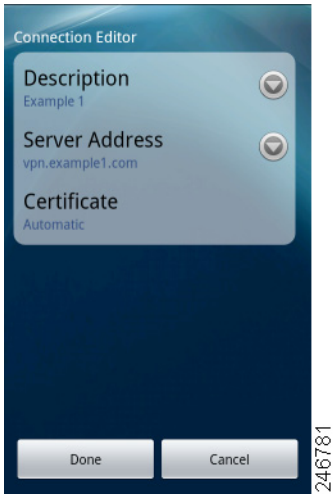
初めて VPN 接続の確立を試みる前に、次の手順で VPN 接続エントリを追加し、VPN セキュア ゲートウェイを識別できるようにします。

ステップ 1 [AnyConnect] アイコンをタップします。

ステップ 2 AnyConnect ホーム画面で、[Add New VPN Connection] をタップします。

[Add VPN Connection] ウィンドウに、VPN 接続のパラメータが表示されます（図 6）。

図 6　例の値を使用した VPN 接続の追加



ステップ 3 値を指定するには、パラメータ フィールドをタップします。

ステップ 4 次のようにフィールドに入力します。

[Description]：（任意指定、デフォルトは [Server Address]）AnyConnect ホーム画面の接続リストに表示される、接続エントリの一意の名前を入力します。キーボード表示のすべてのアルファベット、空白文字、数字、記号を使用できます。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。次に例を示します。

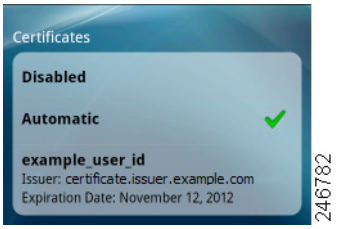
例 1

[Server Address]：接続する Cisco 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。次に例を示します。

```
vpn.example.com
```

[Certificate]：（VPN 要件に応じて任意指定）VPN セッションの確立に証明書が必要な場合、モバイル デバイスへの証明書のインストール手順が管理者から提供されます。[Certificate] をタップして、そのデバイスに登録されているすべての証明書の詳細を表示し、VPN 接続を確立するときに使用する証明書を 1 つ選択できます、[Certificates] ウィンドウには、インストールされた証明書の概要情報が表示されます（図 7）。

図 7　　証明書の例



オプションは次のとおりです。

- [Disabled]：証明書の使用がオプションではないことを示します。
- [Automatic]：セキュリティ アプライアンスに必要な場合のみ、証明書を使用します。
- 個々の証明書のリスト（たとえば、`user_user_id`）：管理者が使用するように指示している証明書をタップします。[Certificate] ウィンドウが再オープンされます。

ステップ 5　[Done] をタップして、接続の値を保存します。

AnyConnect で [Add VPN Connection] ウィンドウが閉じられ、ホーム ウィンドウ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る必要があります。証明書は、次の方法でインポートできます。

- ハイパーリンクによる証明書のインポート
- SCEP による証明書のインポート
- 手動での証明書のインポート

その他の証明書の操作については、証明書の表示と管理を参照してください。

ハイパーリンクによる証明書のインポート

管理者は、お使いのデバイスにインストールできる証明書の場所へのハイパーリンクを提供できます。

（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、AnyConnect の外部使用の制御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、提供された証明書の認証コードを入力します。

SCEP による証明書のインポート

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エントリを設定できます。AnyConnect 管理者は、この方法を使用する VPN 設定エントリの名前をユーザに通知する必要があります。

ステップ 1 AnyConnect 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 存在する場合には [Get Certificate] をタップするか、またはお使いのモバイル 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、ユーザ名とパスワードを入力します。

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ます。次に、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。

手動での証明書のインポート

管理者は、お使いのデバイスにインストールする証明書ファイルを提供できます。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Certificate Management] をタップします。

ステップ 5 [AnyConnect] タブをタップします。

ステップ 6 [Import] ボタンをタップし、ローカル ファイル システムから証明書ファイルを選択すると、証明書がファイル システムからインポートされます。

（注） この方法で証明書を手動でインポートするには、証明書ファイルが Android デバイス上に存在する必要があります。

VPN 接続の確立

ステップ 1 Wi-Fi 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。

ステップ 2 AnyConnect のホーム ウィンドウに移動します。

ステップ 3 使用する接続エントリをタップします。

AnyConnect は、現在使用中の VPN 接続をすべて切断します。

ステップ 4 必要に応じて、適切なプロンプトへの応答として次のいずれかを行います。

- クレデンシャルを入力します。管理者が二重認証を設定している場合には、セカンダリ クレデンシャルの入力を求められる場合もあります。
- [Get Certificate] をタップし、次に管理者により提供される証明書登録のクレデンシャルを入力します。AnyConnect は、証明書を保存し、VPN セキュア ゲートウェイに再接続して、認証にその証明書を使用します。

AnyConnect のホーム ウィンドウの一番上の行でチェックマークが強調表示され、VPN 接続が確立されたことを示します（図 8）。

図 8　　AnyConnect ホーム（接続）

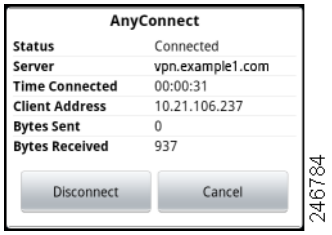
VPN セキュア ゲートウェイの設定に応じて、AnyConnect は、AnyConnect のホーム ウィンドウにあるリストに接続エントリを追加します。

（注） AnyConnect のホーム ウィンドウにある別の VPN 接続をタップすることで、現在の VPN 接続を切断し、タップした VPN 接続に関連付けられている VPN セキュア ゲートウェイに接続します。

[Connection Summary] の表示

接続された VPN セッションのサマリー ビューを表示するには、AnyConnect のホーム ウィンドウの [Choose a connection] にある現在の接続に関連する名前をタップします。図 9 に、[Connection Summary] ウィンドウの例を示します。

図 9　　Connection Summary



VPN 接続エントリの変更

設定エラーを修正したり、IT ポリシーの変更に準拠するために、VPN 接続エントリの変更が必要になることがあります。

（注） VPN セキュア ゲートウェイによってプッシュされた接続エントリの説明またはサーバ アドレスは変更できません。

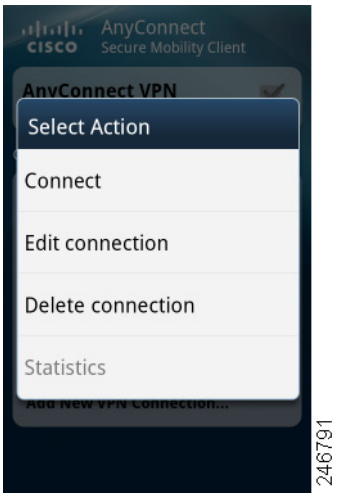
接続エントリを変更するには、次の手順を実行します。

ステップ 1　AnyConnect のホーム ウィンドウを開きます。

ステップ 2　変更する VPN 接続エントリを長押しします。

AnyConnect に、[Select Action] ウィンドウが表示されます（図 10）。

図 10　Select Action



ステップ 3　[Edit connection] をタップします。

[Connection Editor] ウィンドウに、接続エントリに割り当てられたパラメータ値が表示されます。

ステップ 4　変更する値をタップします。画面のキーボードを使用して新しい値を入力し、[OK] をタップします。

パラメータの指定については、VPN 接続エントリの追加を参照してください。

ステップ 5　[Done] をタップします。

AnyConnect はエントリを保存して、AnyConnect ウィンドウを再オープンします。

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の追加したものか、VPN セキュア ゲートウェイで追加されたものかによって 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

ユーザが手動で追加した VPN 接続エントリを完全に削除するには、次の手順に従います。

ステップ 1　AnyConnect のホーム ウィンドウを開きます。

ステップ 2　変更する VPN 接続エントリを長押しします。

AnyConnect に、[Select Action] ウィンドウが表示されます。

ステップ 3　[Delete connection] をタップします。

AnyConnect はエントリを削除して、AnyConnect ウィンドウを再オープンします。

その他の接続エントリのクリア

VPN セキュア ゲートウェイからインポートされた接続エントリを削除する唯一の方法は、現在の AnyConnect XML プロファイルを削除することにより、デバイスからすべての AnyConnect 接続エントリをクリアすることです。

ステップ 1 AnyConnect のホーム ウィンドウを開きます。

ステップ 2 [Menu] ボタンをタップします。

ステップ 3 [Settings] をタップします。

ステップ 4 [Profile Management] をタップします。

ステップ 5 [Delete Profile] をタップします。

ステップ 6 削除を [Confirm] します。

Android デバイスでの AnyConnect の管理

AnyConnect ウィジェットの使用方法

AnyConnect では、ホーム画面に追加できる 3 つのオプションのウィジェットとして large、medium、および small が提供されています。ここでは、ウィジェットを示し、Android のホーム ウィンドウにウィジェットを配置する方法について説明します。

ウィジェットの説明

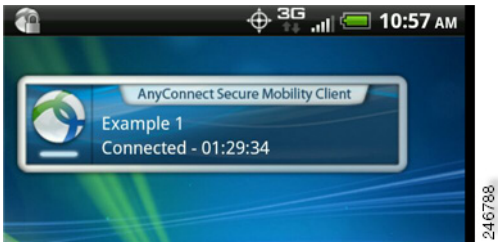
large ウィジェットにより、AnyConnect ステータス情報および制御に簡単にアクセスできます。図 11 に、large ウィジェットが Android のホーム ウィンドウでどのように表示されるかを示します。

図 11　　Large ウィジェット

large ウィジェットは、AnyConnect アイコン、App 名、デフォルト VPN セキュア ゲートウェイ、および VPN ステータスを表示します。AnyConnect が接続されている VPN セキュア ゲートウェイの名前か、存在しない場合はデフォルトの接続を表示します。アイコンの下のバーの色は、VPN ステータスを示します。アイコンをタップして、VPN セキュア ゲートウェイへの接続、または VPN セキュア ゲートウェイからの切断ができ、接続エントリをタップして、選択した VPN セキュア ゲートウェイに対し切断および接続ができます。あるいは、[Add New VPN Connection] をタップして、新しい VPN セキュア ゲートウェイの接続の詳細を指定できます。

図 12 に、medium ウィジェットが Android のホーム ウィンドウでどのように表示されるかを示します。

図 12　Medium ウィジェット



medium ウィジェットは、接続エントリのリストを除き、large ウィジェットと同じデータを提供します。ウィジェットをタップして、指定された VPN セキュア ゲートウェイへの接続、または指定された VPN セキュア ゲートウェイからの切断ができます。

図 13 に、small ウィジェットが Android のホーム ウィンドウでどのように表示されるかを示します。

図 13　Small ウィジェット

small ウィジェットは、AnyConnect App のアイコンと同じサイズです。アイコンの下のバーの色には、VPN ステータスが反映されます。ウィジェットをタップして、デフォルトの VPN セキュア ゲートウェイへの接続、またはデフォルトの VPN セキュア ゲートウェイからの切断ができます。

Android のホーム ウィンドウにウィジェットを配置する

ウィジェットを配置する手順は、お使いのデバイスおよび Android のバージョンによって異なることがあります。手順の例を次に示します。

ステップ 1　ウィジェット用に十分なスペースのある Android のホーム画面に移動します。

ステップ 2　[menu] ボタンをタップするか、押します。

ステップ 3　[Personalize] をタップします。

ステップ 4　[Widgets] をタップします。

ステップ 5　使用する AnyConnect のウィジェットをタップします。

Android により、ウィジェットがホーム画面に追加されます。

ステップ 6　ウィジェットを再配置する場合は、ウィジェットを長押しして、応答があってから移動します。

アプリケーション プリファレンスの指定

ステップ 1　AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします（図 14）。

図 14　AnyConnect アプリケーション プリファレンス

AnyConnect テーマの変更

AnyConnect は次のテーマを提供します。

- [Cisco Default Theme]（デフォルト）：コントラストのある色で、青系統が中心になっています。
- [Android]：シスコのデフォルト テーマの代わりになる Android のようなテーマです。

（注） AnyConnect への [Android] テーマの割り当ては、一部のデバイスでフィールド値が見えないなどの問題があります。[Android] テーマの使用が難しい場合は、デフォルト テーマを再度適用します。

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 のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Application Style] をタップします。

AnyConnect に、現在使用中のテーマの横にグリーンのボタンが表示されます。

ステップ 5 必要なテーマをタップします。

スタートアップ時に AnyConnect を起動

デバイスで AnyConnect を起動するタイミングを制御できます。デフォルトでは、デバイスのスタートアップ時に AnyConnect は自動的に起動しません。この設定を変更し、デバイスのスタートアップ時に AnyConnect を起動するには、次の手順に従います。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Application Preferences] をタップします。

ステップ 5 [Launch at Startup] チェックボックスをタップします。

オフのままにすると、AnyConnect はユーザが開始するまで起動しません。

（注） Trusted Network Detection を指定したプロファイルをダウンロードするか、またはインポートすると、[Launch at Startup] が自動的にイネーブルになります。

AnyConnect ステータス バー アイコンの非表示

AnyConnect がアクティブでない場合には、通知バー内の AnyConnect アイコンを非表示にできます。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Application Preferences] をタップします。

ステップ 5 [Hide Icon] チェックボックスをタップします。

オフのままにすると、アイコンが永続的に表示されます。

AnyConnect の外部使用の制御

AnyConnect が外部アプリケーションからの要求に応答する方法を指定できます。これらの外部要求により、接続エントリの作成、VPN の接続または切断、およびクライアント プロファイル、証明書、およびローカリゼーション ファイルのインポートを行うことができます。これらの外部要求は、一般には管理者が電子メールまたは Web ページで提供する URI です。

外部制御アプリケーションのプリファレンスにより、AnyConnect アプリケーションがこれらの外部 URI 要求に応答する方法が指定されます。

- [Enabled]：AnyConnect アプリケーションは、すべての URI コマンドを自動的に許可します。
- [Disabled]：AnyConnect アプリケーションは、すべての URI コマンドを自動的に拒否します。
- [Prompt]：AnyConnect アプリケーションは、デバイス上で AnyConnect URI がクリックされるたびにユーザに問い合わせます。URI 要求を許可することも、拒否することもできます。通知とプロンプトの詳細については、「Another Application has requested that AnyConnect...Do you want to

allow this?」に対処するの項を参照してください。

外部 URI 要求の制御方法を指定するには、次の手順に従います。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Application Preferences] をタップします。

ステップ 5 [External Control] をタップします。

ステップ 6 [Enabled]、[Disabled]、または [Prompt] をタップします。

証明書の表示と管理

[Menu] > [Settings] > [Certificate Management] アクティビティ画面では、システム証明書を表示したり、AnyConnect 証明書ストア内の証明書を表示または管理することができます。この画面には、Android システム証明書ストア用と、AnyConnect 証明書ストア用の 2 つのタブがあります。

- [System] タブでは、システム ストア内の証明書を参照して、各証明書の詳細を表示できます。

（注） システム証明書をインポートまたは削除することはできず、システム ストア内の証明書は表示のみ可能です。

- [AnyConnect] タブでは、インポートされた証明書を参照して各証明書の詳細を表示できます。また、個々の証明書の削除、または AnyConnect 証明書ストア内のすべての証明書の削除、および証明書を手動でインポートできます。

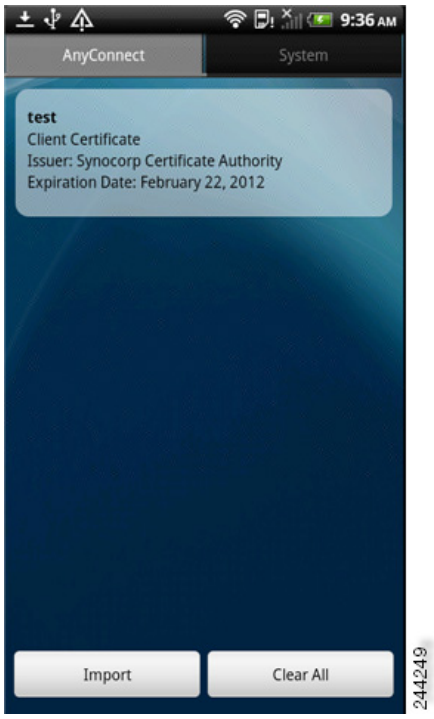
ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Certificate Management] をタップします（図 15）。

図 15　AnyConnect 証明書管理画面



ステップ 5　Android システム ストアのすべての証明書を表示するには、[System] タブをタップします。証明書を長押しして [View certificate details] を選択すると、証明書の内容を表示できます。

ステップ 6　AnyConnect 証明書ストアのすべての証明書を表示するには、[AnyConnect] タブをタップします。次の手順を実行できます。

- 証明書を長押しして [View certificate details] を選択すると、証明書の詳細が表示されます。
- 証明書を長押しして [Delete Certificate] を選択すると、証明書が削除されます。
- [Clear All] ボタンをタップすると、AnyConnect 証明書ストアからすべての証明書がクリアされます。
- [Import] ボタンをタップし、ローカル ファイル システムから証明書ファイルを選択すると、証明書がファイル システムからインポートされます。この方法で証明書を手動でインポートするには、証明書ファイルが Android デバイス上に存在する必要があります。

その他の証明書のインポート方法については、モバイル デバイスへの証明書のインストールを参照してください。

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、Android デバイス上で一度に 1 つの VPN クライアント プロファイルのみ維持します。次に、現在のプロファイルが存在する場合、それを置換または削除する主要なシナリオをいくつか示します。

- プロファイルを手動でインポートすると、現在のプロファイルがインポートしたプロファイルで置き換えられます。
- 自動または手動の VPN 接続を開始すると、現在のプロファイルが新しい接続のプロファイルによって置き換えられます。
- VPN 接続に、それに関連付けられたプロファイルが存在しない場合、その VPN の開始時に既存のプロファイルが削除されます。

現在デバイス上にある AnyConnect プロファイルを表示または削除するか、または新しいプロファイルをインポートできます。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

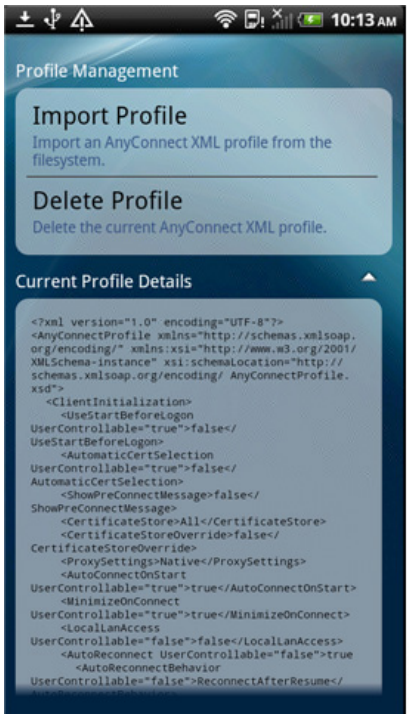
ステップ 3 [Settings] をタップします。

ステップ 4 [Profile Management] をタップします（図 16）。

図 16 AnyConnect の [Profile Management]

- [Current Profile Details] の展開アイコンをタップします。XML ファイルが表示されます。下にスクロールして、ファイル全体を表示します（図 17）。

図 17　AnyConnect プロファイルの詳細



- [Delete Profile] をタップして、この現在のプロファイルの削除を確認します。

  プロファイル内で定義された接続エントリが AnyConnect のホーム画面からクリアされ、AnyConnect クライアントの動作は、デフォルトのクライアント仕様に従います。
- [Import Profile] をタップし、デバイスのファイル システムから XML プロファイルを選択します。

  このプロファイル内で定義された接続エントリが AnyConnect のホーム画面にただちに表示され、AnyConnect クライアントの動作はこのプロファイルのクライアント仕様に従います。

ローカリゼーションの管理

AnyConnect のインストール時に、Android デバイスは、[Settings] > [Language and Keyboard] > [Select locale] で指定されたデバイスのロケールに従って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、Android デバイスのローカリゼーションを参照してください。

注意　Android デバイス上のローカリゼーションの管理は、管理者が指定する手順に基づいて実行する必要があります。

追加の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できます。

- 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 ページで提供できます。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） 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 を許可する必要があります。この設定方法については、AnyConnect の外部使用の制御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。

- [AnyConnect Localization Management Activity] 画面の [Server Localization Import] オプションを使用して、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。

ユーザ ローカリゼーション管理の操作

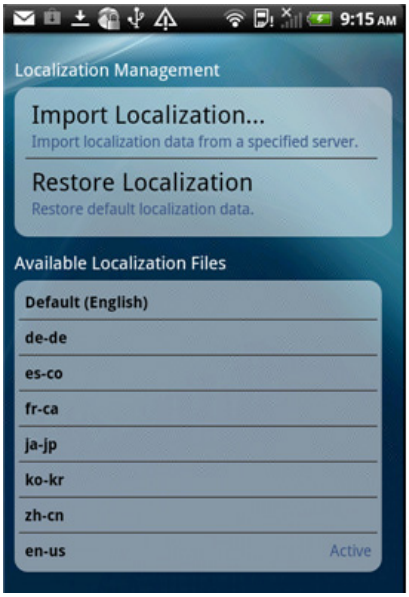
[Localization Management] 画面で、AnyConnect ローカリゼーションを管理できます。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 AnyConnect の [menu] ボタンをタップするか、押します。

ステップ 3 [Settings] をタップします。

ステップ 4 [Localization Management] をタップします。



- [Import Localization] をタップし、セキュア ゲートウェイのアドレス、およびロケールを指定します。ロケールは ISO 639-1 で指定されており、適用可能な場合には国コードが追加されます（たとえば、en-US、fr-CA、ar-IQ など）。このローカリゼーション データは、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。
- [Restore Localization] をタップします。AnyConnect パッケージから事前ロードされたローカリゼーション データの使用を復元し、インポートされたローカリゼーション データをすべて削除します。復元される言語は、[Settings] > [Language and Keyboard] > [Select locale] に指定されたデバイスのロケールに基づいて選択されます。

AnyConnect の削除

デバイスから AnyConnect を削除するには、[Settings] > [Applications] > [Manage applications] > [AnyConnect] の順に移動して、次に、[Uninstall] をタップします。

AnyConnect 情報の取得

統計情報の表示

VPN 接続が存在する場合、AnyConnect では統計情報を記録します。現在の VPN 接続の統計情報を表示するには、次の手順に従います。

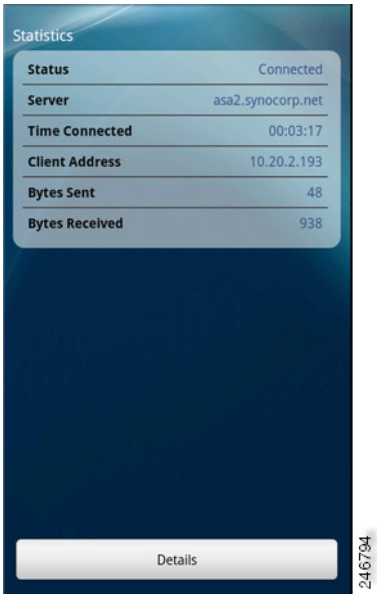
ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 [Menu] ボタンをタップするか、押します。

ステップ 3 [Statistics] をタップします。

[Statistics Overview] ウィンドウが開きます（図 18）。

図 18 Statistics Overview

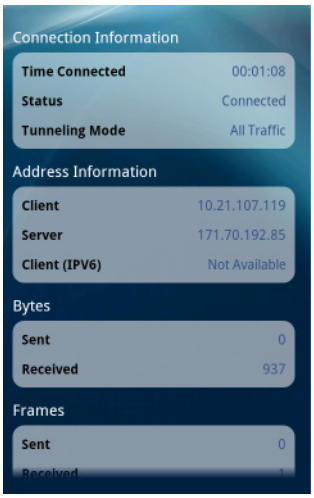


[Statistics] ウィンドウに表示される項目は、次のとおりです。

- Status（VPN 接続）
- Server（アドレス）
- Time Connected
- Client Address
- Bytes Sent
- Bytes Received

- [Details] をタップして、詳細な統計情報を表示します（図 19）。

図 19　Detailed Statistics



ステップ 4　下にスクロールして、残りの統計情報を表示します。

[Detailed Statistics] ウィンドウには、次の情報が表示されます。

- Connection Information
  - Time Connected
  - Status
  - Tunneling Mode
- Address Information
  - Client
  - Server
  - Client (IPv6)
- Bytes
  - Sent
  - Received
- Frames
  - Sent
  - Received
- Control Frames
  - Sent
  - Received
- Transport Information
  - Protocol
  - Cipher
  - Compression

- Feature Configuration：FIPS モード
- Secure Routes：VPN セキュア ゲートウェイの設定により決定したとおりに、暗号化された接続を経由するトラフィック宛先。AnyConnect に、各宛先が IP アドレス/サブネット マスクの形式で表示されます。0.0.0.0/0.0.0.0 のエントリは、特に除外しているものを除き VPN トラフィックすべてが暗号化されて、VPN 接続上を送受信されることを意味します。
- Non-Secure Routes（[Secure Routes] の下に 0.0.0.0/0.0.0.0 が存在する場合のみ表示）：VPN セキュア ゲートウェイが決定したとおりに、暗号化された接続から除外されるトラフィック宛先。

ログ メッセージの表示および管理

AnyConnect のログ メッセージを表示、送信、またはクリアするには、次の手順に従います。

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 [Menu] ボタンをタップするか、押します。

ステップ 3 [Diagnostics] をタップします。

AnyConnect は、メッセージを Android から取得し、[Messages] ウィンドウに表示します（図 20）。

図 20 Messages

このウィンドウを使用してできる操作は次のとおりです。

- [Messages]：タップすると、ログ メッセージが表示されます。
- [System]：タップすると、次の種類の AnyConnect 情報が表示されます。メモリ、インターフェイス、ルート、フィルタ、権限、プロセス、システム プロパティ、メモリ マップ、および一意のデバイス ID。

- [Debug]：タップすると、管理者および Cisco Technical Assistance Center（TAC）によって AnyConnect の問題の分析に使用されるログ メッセージが表示されます。
- [Send Logs]：タップすると、ログ メッセージおよびすべてのプロファイル データを .zip ファイルにパッケージ化して、電子メール メッセージに挿入するか、Bluetooth を使用してローカルに転送します。まず、送信デバイスと受信デバイスで Bluetooth を有効にする必要があります。AnyConnect に関する問題をレポートする場合は、電子メールのオプションを使用して、ログ ファイルを管理者に送信します。
- [Clear Debug Logs]：タップするとすべてのメッセージを削除します。

ステップ 4 他のメッセージを表示するには、ウィンドウをスクロールします。

AnyConnect のバージョンおよびライセンスの詳細の表示

ステップ 1 AnyConnect のホーム ウィンドウに移動します。

ステップ 2 [Menu] ボタンをタップするか、押します。

ステップ 3 [About] をタップします。

AnyConnect に [About] ウィンドウが表示されます。

ヒント [About] ウィンドウでリンクをタップして、このマニュアルのアップデートされた最新のバージョンをオープンします。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リンクを使用できます。

AnyConnect 通知への応答

「Another Application has requested that AnyConnect...Do you want to allow this?」に対処する

デバイスを保護するため、外部アプリケーションが接続エントリを追加する場合、VPN 接続を確立または切断する場合、またはプロファイル、証明書、またはローカリゼーション ファイルをインポートする場合には、AnyConnect がアラートを発行します。次のプロンプトへの応答で [Yes] をタップするかどうか、管理者にお問い合わせください。

- 接続エントリの作成：`Another application has requested that AnyConnect create a new connection to host.Do you want to allow this?[Yes] | [No]`
- VPN への接続：`Another application has requested that AnyConnect connect to host.Do you want to allow this?[Yes] | [No]`
- VPN の切断:`Another application has requested that AnyConnect disconnect the current connection.Do you want to allow this?[Yes] | [No]`
- インポート：

- 証明書のバンドル：`Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store.Do you want to allow this?[Yes] | [No]`
- ローカリゼーション ファイル：`Another application has requested that AnyConnect import localization files.Do you want to allow this?[Yes] | [No]`
- クライアント プロファイル:`Another application has requested that AnyConnect import profiles.Do you want to allow this?[Yes] | [No]`

MMS/HIPRI 通知への応答

AnyConnect VPN が接続されている間、マルチメディア（MMS）メッセージの取得または送信、または高プライオリティ（HPRI）サービスを使用することはできません。いずれかのアクティビティを試行してブロックされると、ステータス バーに AnyConnect 通知アイコンが表示されます。

この通知を確認するには、次の手順に従います。

ステップ 1 通知アイコンをクリックして、AnyConnect 通知を表示します。

ステップ 2 通知をクリックして、[Service Impact] を表示します。

ステップ 3 MMS/HIPRI サービスがブロックされたときに、これ以上通知を受信しない場合には、[Do not show this again] チェックボックスをオンにします。

（注） [Do not show this again] をオンにすると、選択が固定されます。このアクションを後から反転させることはできません。

ステップ 4 [OK] をクリックします。

トラブルシューティング

既知の問題およびバグ

このリリースには次の既知の問題およびバグがあります。

- AnyConnect は、EDGE の固有の性質およびその他の早期無線テクノロジーによって EDGE 接続上の VPN トラフィックを送受信する場合、ボイスコールをブロックします。
- Android セキュリティ ルールによって、VPN 接続がアップ状態の間、デバイスの *マルチメディア メッセージング サービス（MMS）メッセージ*と呼ばれる、添付ファイルを含むメッセージの送受信が阻止されます。VPN 接続がアップ状態の間に、MMS メッセージを送信しようとすると、Android にエラー メッセージが表示されますが、受信の失敗についてはユーザに通知しません。Android は、待機中の MMS メッセージが、VPN 接続終了時に送受信されることを許可します。

一般的な問題への対処

この項では、一般的な問題に対する解決策を説明します。解決策を試しても問題が続く場合は、管理者に問い合わせてください。

- **tun.ko エラー メッセージが返されました。**

  tun.ko モジュールが、まだカーネルにコンパイルされていない場合は、tun.ko モジュールが必要です。デバイスに含まれていない、またはカーネルとコンパイルされていない場合は、対応するデバイスのカーネルを入手または作成して、`/data/local/kernel_modules/` ディレクトリに配置します。

- **編集または削除できない接続エントリがあります。**

  管理者が、AnyConnect プロファイル内にこれらの接続エントリを定義しました。これらのプロファイルを削除する手順については、AnyConnect プロファイルの表示と管理を参照してください。

- **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 リソースの輻輳は、タイムアウトや未解決ホスト エラーの一般的な原因です。より強い信号のあるエリアへ移動、または WiFi を使用してみます。Wi-Fi ネットワークを利用できる場合は、デバイスの [Settings] App を使用し、最初にそのネットワーク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。

- **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。確認するには、AnyConnect ホーム ウィンドウに移動し、接続エントリを長押しします。次に、[Certificate] をタップします。[Certificates] ウィンドウにすべての証明書のリストが示されます。証明書名を長押しして、次に、[View Certificate Details] をタップします。接続に対して適切な証明書を使用しているかどうかを管理者に確認します。

- **デバイス上の使用できる証明書の表示が必要です。**

  AnyConnect によってインポートされたすべての証明書を表示するには、AnyConnect のホーム ウィンドウに移動し、[Menu] ボタンをタップまたは押して、次に [Settings] > [Certificate Management] をタップします。[Certificates] ウィンドウにすべての証明書のリストが示されます。証明書の詳細を表示するには、証明書名を長押しし、次に、[View Certificate Details] をタップします。

- **接続エラー、デバイスは正常に動作しています。**

  管理者に VPN セキュア ゲートウェイがモバイル接続を許可するように設定され、ライセンスされているかどうかを問い合わせます。

- **ASA に接続できません、解決できないホスト エラーです。**

  インターネット ブラウザを使用して、ネットワーク接続を確認します。ブラウザを使用してみて、https://*vpn.example.com* に移動します。ここで、*vpn.example.com* は、接続を確認する VPN セキュア ゲートウェイの URL です。

- **Market からの AnyConnect パッケージのインストールに失敗しました。**

  デバイスがサポートされる Android デバイスの 1 つとしてリストされていることを確認します。

- **「Installation Error: Unknown reason -8」。**

  サポートされていないデバイスにブランド固有の AnyConnect をインストールしようとすると、このメッセージが返されます。サポートされる Android デバイスのリストおよびAnyConnect のインストールまたはアップグレードの手順を確認して、お使いのデバイスに対して適切な AnyConnect パッケージをダウンロードしてください。

- **AnyConnect エラー、「Could not obtain the necessary permissions to run this application.This device does not support AnyConnect」。**

  AnyConnect は、このデバイスで動作していません。サポートされる Android デバイスのリストおよびAnyConnect のインストールまたはアップグレードの手順を確認して、お使いのデバイスに対して適切な AnyConnect パッケージをダウンロードしてください。

- **問題：現在の AnyConnect VPN プロファイルの表示が必要です。**

  AnyConnect プロファイルの表示と管理を参照してください。

- **ネットワークの接続性の問題のため、ログを電子メールで送信できません。**

  インターネットにアクセス可能な別のネットワークを試します。ネットワークの接続性がない、またはデバイスのリセットが必要な場合は、ドラフトの電子メールメッセージにログ メッセージを保存します。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Copyright © 2004-2012 Cisco Systems, Inc.
All rights reserved.

Copyright © 2004-2012, シスコシステムズ合同会社 .
All rights reserved.