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 2.4.x）

更新日：2011 年 9 月 15 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。

内容

このマニュアルでは Cisco AnyConnect Secure Mobility Client 2.4.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。

© 2004–2011 Cisco Systems, Inc. All rights reserved.
Copyright © 2004–2012, シスコシステムズ合同会社. All rights reserved.

概要

Cisco AnyConnect Secure Mobility Client 2.4.x 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。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、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。

Android Market では、インストール App へのアクセスが提供されます。サポートされるすべての Samsung デバイスおよび root 化された Android デバイスに App をインストールできます。

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。

機能

表 1 に Android デバイス向け AnyConnect 2.4.x の機能がリストされています。

表 1　　Android 向け AnyConnect 2.4.x の機能

機能	説明	導入された Android 向け AnyConnect のバージョン
起動時の起動制御	モバイル デバイスの起動時に Android が AnyConnect をただちに開始するかどうか、エンド ユーザが制御できます。デフォルトの動作では、起動時に AnyConnect を開始しません。	2.4.7073
アイドル時の AnyConnect アイコンの非表示	モバイル エンドポイントが AnyConnect を使用して接続されていない場合に、ユーザが AnyConnect アイコンを表示または非表示にする必要があるかどうか指定できます。 設定には [App] メニューの [Settings] ボタンからアクセスできます。 デフォルトの動作では、接続されていない場合、AnyConnect アイコンは非表示です。	2.4.7073
VPN 回復の向上	ネットワークを切り替える場合、AnyConnect は VPN 接続をより効率的に回復します。	2.4.7073
内部ネットワークに対する IPv6 サポート	IPv6 をサポートする電話機を使用している Android ユーザは、これで IPv6 アドレスを割り当てるプライベート ネットワークに接続でき、IPv6 でネットワーク リソースにアクセスできるようになります。	2.4.7073
AnyConnect の終了	新しいメニュー アイテムによって、ユーザは AnyConnect を接続解除できます。	2.4.7073
AnyConnect が「一時停止」であることを示す新しいアイコン	接続していないため接続が中断されています。 	2.4.7073
3G-WiFi ローミング	AnyConnect は、3G および WiFi ネットワーク間を移動するユーザとして VPN を維持します。	2.4.7030
ホーム画面用の AnyConnect ウィジェット	ワンクリック VPN アクセス用に、Android ウィジェットを、ホーム画面でインストールできます。	2.4.7030

表 1　Android 向け AnyConnect 2.4.x の機能 （続き）

機能	説明	導入された Android 向け AnyConnect のバージョン
アプリケーション URI 処理	Web ブラウザなどの他のアプリケーションは、VPN 接続エントリの AnyConnect 設定の追加、VPN 接続の確立、VPN からの接続解除、および証明書のインポートが可能です。システム管理者は、この機能を利用するリンクを入手できるように選択することもできます。	2.4.7030
Cisco AnyConnect VPN 接続エントリ（AnyConnect ユーザ プロファイル）のインポート	デバイスが接続された場合、AnyConnect は、ASA から保存された使用可能な VPN 接続プロファイルを自動的にインポートします。	2.4.7030
Cisco SSL トンネリング プロトコルおよび Cisco DTLS トンネリング プロトコル	AnyConnect は、Cisco SSL トンネリング プロトコルおよび Cisco DTLS トンネリング プロトコルの両方を使用する VPN 接続を確立できます。	2.4.7030
AnyConnect 管理者に対する電子メールによるログの送信	ユーザは、トラブルシューティングのために、統計情報、ログ メッセージ、およびシステム情報詳細を AnyConnect システム管理者へ電子メールで迅速に送信できます。	2.4.7030
複数の認証方法	ユーザ名とパスワード、グループ選択、証明書からのユーザ名の事前入力、および二重認証による認証です。Cisco VPN セキュア ゲートウェイの設定では、証明書が必要かどうかを指定します。必要な場合、証明書へのアクセスを提供します。	2.4.7030
Cisco デフォルト ユーザ インターフェイス テーマに代わるネイティブ Android。	ユーザは、AnyConnect インターフェイスまたはネイティブ Android VPN インターフェイスを使用して AnyConnect VPN 接続を設定できます。	2.4.7030

Lenovo デバイス向け AnyConnect の要件

Cisco AnyConnect for Lenovo, Release 2.4.x 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 からの最新のソフトウェアのアップデートを実行している場合に限ります。

root 化されたデバイス向け AnyConnect の要件

Cisco AnyConnect for Rooted, Release 2.4.x は、Android 2.1 以降を実行している root 化されたほとんどのデバイスで実行されます。デバイスが、サポートされている Samsung デバイスである場合を除いて、root 化されたデバイスは必須になります。

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。

Samsung 用の AnyConnect クライアント ダウンロードは、root 化されたデバイスで動作しません。root 化されたデバイスで AnyConnect の root 化されたバージョンを使用する必要があります。

tun.ko モジュールおよび IP テーブルの両方が必要です。AnyConnect に、VPN を確立しようとしたときに失われた内容を通知するエラー メッセージが表示されます。tun.ko モジュールが失われた場合、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。

Samsung デバイス向け AnyConnect の要件

Cisco AnyConnect for Samsung, Release 2.4.x は、次の Samsung 製品ラインをサポートします。ただし、デバイスが Samsung からの最新のソフトウェアのアップデートを実行している場合に限ります。

- Android 2.3.3 以降を実行する Galaxy S。
- Android 2.3.3 以降を実行する Galaxy S II。
- Android 2.3.3 以降を実行する Galaxy Tab 7（WiFi のみ）。

  （注） 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。

- Android 3.0 以降を実行する Galaxy Tab 8.9。
- Samsung TouchWiz アップデートを使用して Android 3.1 以降を実行する Galaxy Tab 10.1。

（注） Samsung は、各キャリア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。

インストールおよびアップグレード

Android 向け AnyConnect をインストールまたはアップグレードするには、次のデバイスに一致する APP 用の Android Market に移動します。

- サポートされる Samsung デバイス用の「Cisco AnyConnect for Samsung」。
- Android 2.1 以降を実行する root 化されたデバイス用の「Cisco AnyConnect for Rooted」。

（注） Cisco AnyConnect は、これらの 2 つの基準のいずれかを満たしていない Android デバイスでは動作しません。

接続前の準備

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、システム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 接続エントリの追加

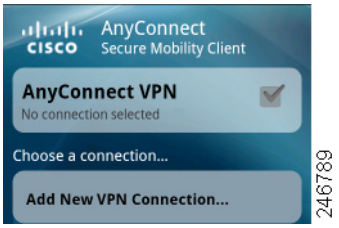
初めて VPN 接続の確立を試みる前に、次の手順で VPN 接続エントリを追加し、VPN セキュア ゲートウェイを識別できるようにします。

ステップ 1 [AnyConnect] アイコンをタップします（図 1）。

図 1 [AnyConnect] アイコン

AnyConnect のホーム ウィンドウに VPN 接続ステータスが表示されます（図 2）。

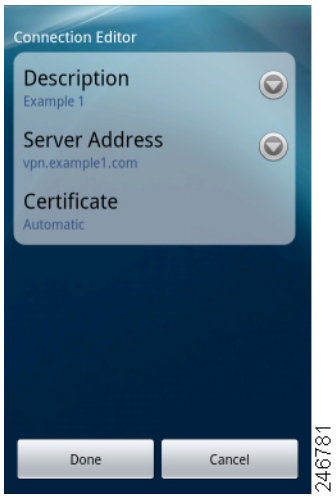
図 2 AnyConnect ホーム（新規インストール）



ステップ 2 [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 3）。

図 3　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] : AnyConnect のホーム 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。

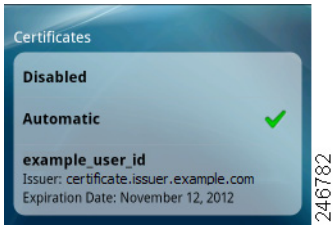
```
Example 1
```

[Server Address] : 接続する 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 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、システム管理者が証明書をインストールする手順を示します。[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概要の詳細を表示し、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 4）。

図 4　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）: システム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。

VPN への接続

VPN 接続を確立するには、次の手順に従います。

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。入力を求められたら、二重認証をサポートするセカンダリ クレデンシャルも入力します。
- [Get Certificate] をタップし、次にシステム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 5）。

図 5 AnyConnect ホーム（接続）

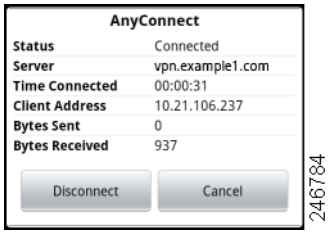
VPN セキュア ゲートウェイの設定に応じて、AnyConnect は接続エントリを取得し、AnyConnect のホーム ウィンドウにある VPN 接続リストに追加します。

注意 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] を表示する

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] の下にある接続に関連付けられている名前をタップします。図 6 に、[Connection Summary] ウィンドウの例を示します。

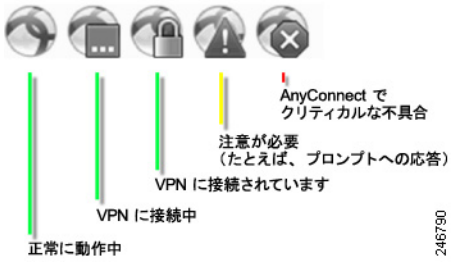
図 6　　Connection Summary



ステータス バーの AnyConnect アイコンの使用方法

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 7）。

図 7　　Android ステータス バーの AnyConnect 通知アイコン



AnyConnect のステータスのテキスト説明を表示するには、ステータス バーを下にドラッグします。次に、AnyConnect のホーム ウィンドウに移動するには、[AnyConnect] をタップします。

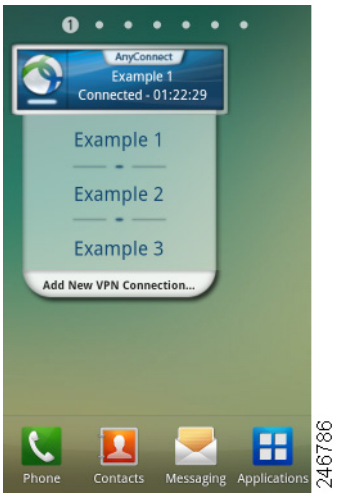
AnyConnect ウィジェットの使用方法

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 8 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。

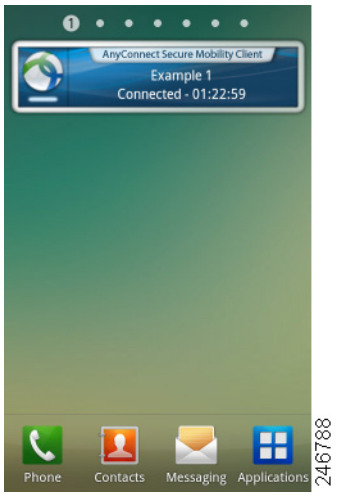
図 8　　Large ウィジェット



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 9 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。

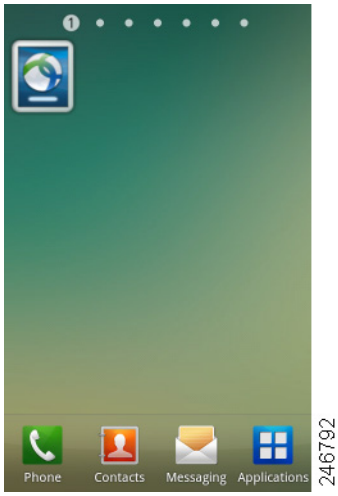
図 9　　Medium ウィジェット



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 10 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 10　　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 [Add] 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。

統計情報の概要の表示

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 接続の統計情報概要を表示するには、次の手順に従います。

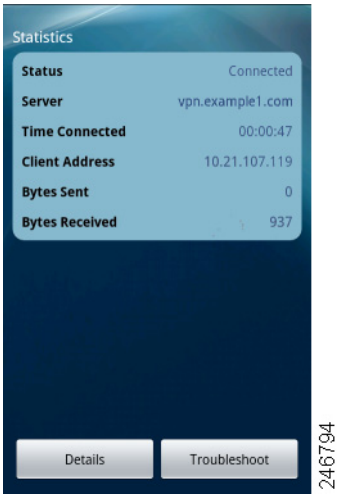
ステップ 1 AnyConnect のホーム ウィンドウに移動します。

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 11）。

図 11 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 接続の）。
- 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）。
- [Troubleshoot]：タップするとログ ファイルが表示されます。

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 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。

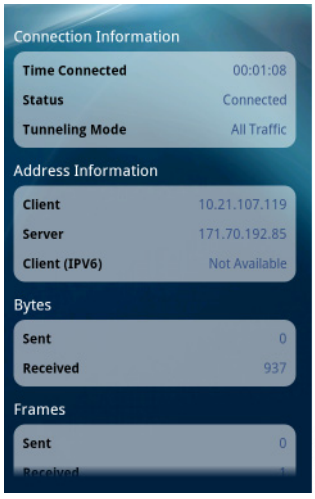
ステップ 3 [Statistics] をタップします。

ステップ 4 [Statistics] ウィンドウが開きます。

ステップ 5 [Details] をタップします。

[Detailed Statistics] ウィンドウが開きます（図 12）。

図 12 Detailed Statistics



ステップ 6 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 Mode]
- [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 [Statistics] をタップします。

ステップ 4 [Statistics] ウィンドウが開きます。

ステップ 5 [Troubleshoot] 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 13）。

図 13 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（Samsung についてのみ収集）、権限、プロセス、システム プロパティ、メモリ マップ。
- [Debug]：タップすると、システム管理者および 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 ファイルをシステム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 6 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。

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。

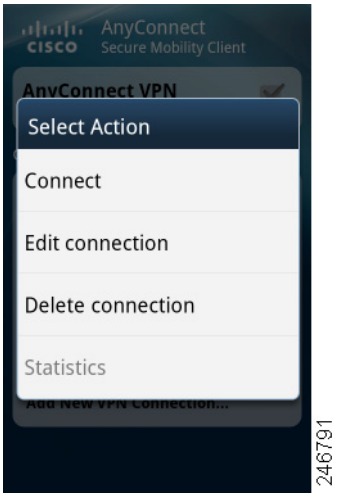
接続エントリを変更するには、次の手順を実行します。

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 14）。

図 14 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、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 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を削除する

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。

AnyConnect データをすべてクリアする

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、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。

注意 すべての AnyConnect データをクリアする場合、すべての証明書、接続エントリ、およびプロファイル データの作成、または再インポートが必要になります。

すべてのデータをクリアするには、Android のホーム ウィンドウに移動し、[Applications] > [Settings] > [Applications] > [Manage Applications] > [AnyConnect] > [Clear Data] の順にタップします。

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）：Apple iOS のインターフェイス上の AnyConnect 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。
- [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。

AnyConnect のバージョンおよびライセンスの詳細の表示

このマニュアルのオンライン バージョン、お使いのデバイスで実行している AnyConnect のバージョン、および著作権とライセンス情報へのリンクを表示するには、次の手順を実行します。

ステップ 1 AnyConnect のホーム 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。

「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、AnyConnect は、別のアプリケーションが接続エントリのセットの追加、証明書のインポート、VPN 接続の確立、または VPN からの切断を試みたときに警告します。次のプロンプトへの応答で [Yes] をタップするかどうか、システム管理者にお問い合わせください。

- 作成：「`Another application has requested that AnyConnect create a new connection to host.Do you want to allow this?[Yes or No]`」
- インポート：「`Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store.Do you want to allow this?[Yes or No]`」
- 接続:「`Another application has requested that AnyConnect connect to host.Do you want to allow this?[Yes or No]`」
- 切断：「`Another application has requested that AnyConnect disconnect the current connection.Do you want to allow this?[Yes or No]`」

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。
- デバイスの IP アドレスを更新する Wi-Fi および DHCP 上に VPN 接続が確立されている場合、LAN へのメディア接続は停止しますが、制御接続は停止しません。回復するには、WiFi をディセーブルにして再度イネーブルにします。
- Android セキュリティ フィルタリング 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。

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。解決策を試しても問題が続く場合は、システム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。**

  システム管理者が、VPN セキュア ゲートウェイからインポートされたホスト エントリの変更と削除を禁止するポリシーを設定しています。それらのホスト エントリを削除する唯一の方法は、すべての AnyConnect データをクリアすることです。

- **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システム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証明書をすべて表示するには、AnyConnect ホーム ウィンドウに移動し、[Add New VPN Connection] をタップして、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、デバイスは問題なく動作します**

  システム管理者に 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 root 化されている、またはサポートされる Samsung デバイスにリストされていることを確認します。

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

  ユーザがサポートされていないデバイスに AnyConnect をインストールしようとすると、このメッセージが返されます。デバイスが root 化されている、またはサポートされる Samsung デバイスにリストされていることを確認します。

- **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。デバイスが root 化されている、またはサポートされる Samsung デバイスにリストされている必要があります。

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

  AnyConnect では、電子メールでログを送信するときに、現在のプロファイルが含まれています。

- **デバイス IMEI（一意の ID）の表示が必要です**

  [Applications] > [Settings] > [About Phone] -> [Status] の順に移動します。

- **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。

AnyConnect を削除する

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。

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 2.4 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。

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。

© 2004-2011 Cisco Systems, Inc.
All rights reserved.

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