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 3.0.x）

初版：2012 年 10 月 22 日

最終更新：2012 年 11 月 06 日

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/

【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。

目 次

第 1 章

AnyConnect のインストールと起動

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 アプリケーションのインストール

（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。

手順

ステップ 1 お使いのデバイスがサポートされているかどうかを確認し、該当するブランド固有の AnyConnect パッケージをインストールします。

シスコは、サポートされているデバイス向けのフル機能の VPN 接続を提供するブランド固有の AnyConnect パッケージを提供します。 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。

a) Samsung デバイス：

- お使いのデバイスが 2011 年 9 月以降に製造またはアップグレードされたものである場合は、Samsung AnyConnect をインストールします。
- お使いのデバイスが 2011 年 9 月以前に製造されたものであり、アップグレードを受け取っていない場合は、Samsung AnyConnect Legacy をインストールします。

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.”

b) HTC デバイス では、HTC AnyConnect をインストールします。

c) Motorola デバイス：

- お使いのデバイスが 2012 年 5 月以降にリリースされたものである場合は、AnyConnect Plus をインストールします。
- お使いのデバイスが 2012 年 5 月以前にリリースされたものである場合は、Motorola AnyConnect をインストールします。

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

d) Kindle デバイスの場合、Cisco AnyConnect（Kindle Tablet Edition）をインストールします。

ステップ 2 それ以外の場合は、AnyConnect ICS+ をインストールするため、お使いのデバイスで Android 4.0（Ice Cream Sandwich）以降が実行されているかどうかを確認してください。

AnyConnect クライアントは、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。

ステップ 3 それ以外の場合は、お使いのデバイスが root 化されており Android 2.1 以降が実行されているかどうかを確認し、Rooted AnyConnect をインストールします。

（注） シスコは、この AnyConnect パッケージをプレビューおよびテストの目的でのみ提供しています。 シスコは、このクライアントをサポートしていませんが、このクライアントは 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。

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。

サポートされる Android デバイス

Samsung デバイス

Samsung AnyConnect および Samsung AnyConnect Legacy では、以下に示す Samsung 製品ラインがサポートされています。 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。 Android のインストール手順を参照し、お使いのデバイスに該当するパッケージを確認してください。

（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。

製品名	製品モデル
ACE+	GT-S7500、GT-S7500、GT-S7500W
ACE II	GT-I8160
Conquer 4G	SPH-D600
Galaxy Appeal	SGH-I827
Galaxy Beam	GT-I8530
Galaxy Exhilarate	SGH-I577
Galaxy Mini	GT-S5570、GT-S5570B、GT-S5570BD1、GT-S5570L、GT-S5578、SCH-I559、SGH-T499、SGH-T499V、SGH-T499Y、
Galaxy Note	GT-I9220、GT-N7000、GT-N7000B、SHV-E160K、SHV-E160S、SHV-E160L、SCH-I889、SCH-I717M、SCH-I717R、SCH-I717D、SGH-NO54、SCH-I717
Galaxy Note 10.1	GT-N8000、GT-N8005、SHW-M480S、SHW-M480K、GT-N8010、GT-N8013、SHW-M480W
Galaxy Rush	SPH-M830

Galaxy S	GT-I9000、GT-I9000B、GT-I9000L、GT-I9000LD1、GT-I9000M、GT-I9000T、GT-I9001、GT-I9003、GT-I9003B、GT-I9003L、GT-I9008、GT-I9008L、GT-I9018、GT-I9070、GT-I9070P、GT-I9088、SC-02B、SCH-I400、SCH-I405、SCH-I500、SCH-I809、SCH-I909、SGH-I896、SGH-I897、SGH-I927、SGH-I997R、SGH-N013、SGH-T699、SGH-T759、SGH-T769、SGH-T959、SGH-T959D、SGH-T959P、SGH-T959V、SGH-T959W、SHW-M100S、SHW-M110S、SHW-M130L、SHW-M190S、SHW-M220L、SHW-M340K、SHW-M340L、SHW-M340S、SPH-D720
Galaxy S II	GT-I9100、GT-I9100G、GT-I9100M、GT-I9100T、GT-I9100P、GT-I9103、GT-I9108、GT-I9210、GT-I9210T、SC-O2C、SC-O3D、SCH-I510、SCH-I919、SCH-I919U、SCH-I929、SCH-J001、SCH-W999、SGH-I727、SGH-I727R、SGH-I757M、SGH-N033、SGH-N034、SGH-T989、SCH-T989D、SHV-E110S、SHV-E120K、SHV-E120L、SHV-E120S、SHW-M250K、SHW-M250L、SHW-M250S、SPH-D170
Galaxy S III	GT-I9300、SCH-I535、SGH-I747、SGH-T999、SHV-E210K、SHV-E210L、SHV-E210S、SPH-L710
Galaxy Stellar	SCH-I200
Galaxy Tab 7（WiFi 専用）[1]	GT-P1000、GT-P1000L、GT-P1000M、GT-P1000N、GT-P1000R、GT-P1000T、GT-P1010、SC-01C、SCH-I800、SGH-I849、SGH-I987、SHW-M180L、SHW-M180S
Galaxy Tab 7.0 Plus & 7.7	GT-P6200、GT-P6201、GT-P6210、GT-P6211、GT-P6800、GT-P6801、GT-P6810、GT-P6811、SCH-I815、SGH-N024、SGH-T869、SHV-E150S、SHW-M430W
Galaxy Tab 8.9	GT-P7300、GT-P7300B、GT-P7310、GT-P7320、GT-P7320T、SCH-P739、SGH-I957、SGH-I957M、SGH-I957R、SHV-E140K、SHV-E140L、SHV-E140S、SHW-M300S、SHW-M300W、SHW-M305W

Galaxy Tab 10.1	GT-P7500、GT-P7500D、GT-P7500M、GT-P7500R、GT-P7500V、GT-P7501、GT-P7503、GT-P7510、GT-P7511、SC-01D、SCH-I905、SGH-T859、SHW-M380K、SHW-M380S、SHW-M380W
Galaxy Tab 2 7.0	GT-P3100、GT-P3110、GT-P3113、SCH-I705
Galaxy Tab 2 10.1	GT-P5100、GT-P5110、GT-P5113
Galaxy W	GT-I8150、SGH-T679
Galaxy Xcover	GT-S5690
Galaxy Y Pro	GT-B5510B、GT-B5510L
Illusion	SCH-I110
Infuse	SCH-I997
Rugby	SGH-I847
Stratosphere	SCH-I405
Stratosphere II	SCH-I415
Transform Ultra	SPH-M930

[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。

HTC デバイス

HTC AnyConnect は、http://www.htcpro.com/enterprise/VPN でリストされている HTC 製品ラインをサポートしています。

デバイスでは必要最小限のソフトウェアが実行されている必要があります。 [Settings] > [About phone] > [Software information] > [Software number] に進み、デバイスで実行中のソフトウェア番号を確認します。

Motorola デバイス

Motorola AnyConnect 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。

- ATRIX 2
- Atrix HD (MB886)
- DROID 4
- Qinara
- RAZR

- RAZR i
- RAZR MAXX
- XYBOARD

Kindle デバイス

Kindle Fire HD デバイスと新しい Kindle Fire 向けの Cisco AnyConnect（Kindle Tablet Edition）Release 3.0.x を Amazon から入手できます。 Anyconnect for Kindle は Android VPN Framework によってサポートされており、AnyConnect ICS+ パッケージと同じ機能を備えています。

Android VPN Framework デバイス

AnyConnect ICS 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 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 以降を実行するサポート対象外のデバイスには、AVF AnyConnect クライアントが推奨されます。 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

Cisco は、Android 2.1 以降を実行する root 化された Android モバイル デバイス向けの Rooted AnyConnect を提供しています。 このクライアントは、プレビューおよびテストの目的でのみ提供されています。 シスコはこのクライアントをサポートしていませんが、このクライアントは Android 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。 問題が発生した場合は、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） 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 の起動

手順

ステップ 1 AnyConnect アイコンをタップして AnyConnect アプリケーションを起動します。

ステップ 2 AnyConnect のインストール後またはアップグレード後に初めて AnyConnect を起動する場合は、表示されるエンド ユーザ ライセンス契約書に同意します。

ステップ 3 [Add New VPN Connection]、または [Menu] をタップして以下のいずれかを選択します。

- [Statistics]：現在アクティブな VPN 接続に関する概要と詳細な統計情報が表示されます。「AnyConnect 統計情報の表示」を参照してください。
- [Settings]：AnyConnect アプリケーション プリファレンスを指定します。 「アプリケーション プリファレンスの指定」を参照してください。
- [Diagnostics]：以下の診断アクティビティを実行します。
  - 証明書の管理：「Android デバイス上の証明書について」を参照してください。
  - AnyConnect プロファイルの管理：「AnyConnect クライアント プロファイルについて」を参照してください。
  - AnyConnect ローカリゼーションの管理：「Android デバイスのローカリゼーションについて」を参照してください。
  - ロギング情報とシステム情報の表示：「ログ メッセージの表示」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。 「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。 「AnyConnect の終了」を参照してください。

次の作業

管理者から提供される手順に従い、ネットワークへの VPN 接続を設定、確立します。

第 2 章

VPN 接続の設定

AnyConnect 設定の概要

AnyConnect で VPN 接続を設定するには、以下の情報が必要です。

- ネットワークにアクセスするためのセキュア ゲートウェイのアドレス。
- 適切に接続するための認証情報。ユーザ名とパスワード、デジタル証明書、またはこの両方を指定します。

管理者の指示に従って AnyConnect クライアントを設定します。明確な手順がない場合は、管理者に連絡してください。 管理者から次のいずれかが提供されます。

- アドレス指定と認証に関する情報。また、デバイスを手動で設定する場合は必要に応じてその他の接続属性。
- この情報を使用して設定を自動化する手順。

AnyConnect を使用するには、以下の内容を理解しておく必要があります。

- 接続エントリ：お使いのデバイスで設定されている VPN 接続。 これらのエントリは手動または自動で設定され、AnyConnect ホーム画面にリストされます。 現在アクティブな接続エントリは、アプリケーションのホーム画面の [AnyConnect VPN] パネルに表示されます。
- VPN 接続の確立手順：VPN 接続を手動で確立できます。このためには、接続リストで接続エントリをタップするか、または [AnyConnect VPN] パネルでチェックボックスまたはスライダをタップします。 VPN 接続は、管理者から提供される手順を使用して自動的に確立することもできます。
- 接続の確立に使用される認証方法：ユーザ名とパスワードを記憶するか、またはユーザ証明書をインポートして接続エントリに割り当てます。

AnyConnect は複雑かつ高度なネットワーキング アプリケーションであり、次の操作が可能です。

- アプリケーションのプリファレンスを設定し、AnyConnect の外観と動作を制御します。
- 管理者の推奨に従い、デバイスに対して診断ツールと管理機能を使用します。

AnyConnect 接続エントリについて

接続エントリは、このデバイスから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を指定します。 接続エントリは次の方法で設定されます。

- 自動追加：管理者から提供される接続エントリを設定するためのリンクをクリックした後で自動的に追加されます。
- 手動での設定：ネットワークへのセキュア ゲートウェイのアドレスを把握しておく必要があります。 このアドレスはセキュア ゲートウェイのドメイン名または IP アドレスであり、接続先のグループも指定することがあります。

接続エントリは、接続時に Cisco ASA セキュア ゲートウェイからダウンロードされる AnyConnect クライアント プロファイルでも定義されています。

関連トピック

ハイパーリンクによる接続エントリの追加, （10 ページ）
手動での接続エントリの追加, （11 ページ）
接続エントリの変更, （23 ページ）
接続エントリの削除, （24 ページ）

ハイパーリンクによる接続エントリの追加

管理者から、接続エントリを追加するためのハイパーリンクが提供されます。

はじめる前に

外部制御を設定してプロンプトを表示するか、AnyConnect 設定内で有効にします。

手順

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。

AnyConnect ホーム ウィンドウの接続リストに接続エントリが追加されます。

関連トピック

AnyConnect 接続エントリについて，（10 ページ）

手動での接続エントリの追加

接続する VPN セキュア ゲートウェイを示す VPN 接続エントリを追加します。

手順

ステップ 1 AnyConnect のホーム ウィンドウで [Add new VPN Connection] をタップし、[Connection Editor] を開きます。

[Connection Editor] ウィンドウはいつでもキャンセルできます。

ステップ 2 （任意） [Destination] を選択し、接続エントリを説明する名前を入力します。

この接続エントリの固有名を入力します。名前を指定しない場合、デフォルトとして Server Address が使用されます。 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。 このフィールドでは大文字と小文字が区別されます。

ステップ 3 [Server Address] を選択し、セキュア ゲートウェイのアドレスを入力します。

セキュア ゲートウェイのドメイン名または IP アドレスを入力します。管理者がグループを指定している場合は、グループも含めます。

ステップ 4 （任意） [Advanced Preferences] をタップし、証明書とプロトコルの詳細設定を変更します。

[Advanced Connection Editor] ウィンドウはいつでもキャンセルできます。

ステップ 5 （任意） [Certificate] をタップし、この接続でユーザ証明書をどのように使用するかを指定します。

- [Disabled] をタップし、証明書をこの接続に使用しないことを指定します。
- セキュア ゲートウェイで必要な場合にのみ、[Automatic] をタップし、接続の確立時に証明書を使用することを指定します。
- 管理者から使用するように指示された証明書をタップします。

VPNセッションの確立にユーザ証明書が必要な場合、モバイルデバイスにユーザ証明書をインストールする手順が管理者から提供されます。 リストで証明書をタップすると、その詳細が表示されます。

ステップ 6 （任意） [Connect with IPsec] をタップし、この VPN 接続に SSL ではなく IPsec を使用します。

この接続属性は管理者から提供されます。

VPN 接続プロトコルとして IPSec を選択すると、[Authentication] パラメータがアクティブになります。

ステップ 7 （任意） [Authentication] をタップし、この IPSec 接続の認証方法を選択します。

この接続属性は管理者から提供されます。

- EAP-AnyConnect（デフォルトの認証オプション）
- IKE-RSA
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2

認証オプションは [Advanced Connection Editor] ウィンドウに表示されます。

ステップ 8 （任意） 認証に使用するプロトコルとして EAP-GTC、EAP-MD5、または EAP-MSCHAPv2 を指定した場合は、[IKE Identity] をタップし、管理者から受け取ったアイデンティティ情報を入力します。

ステップ 9 [Advanced Connection Editor] ウィンドウと [Connection Editor] ウィンドウの両方で [Done] をクリックし、接続値を保存します。

AnyConnectにより、ホーム ウィンドウのリストに新規に作成した接続エントリが追加されます。

関連トピック

AnyConnect 接続エントリについて，（10 ページ）

ユーザ証明書について

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が含まれている必要があります。 ユーザ証明書は、管理者からの指示に従い次のいずれかの方法でインポートされます。

- 電子メールまたはWebページに含まれている管理者から提供されたハイパーリンクをクリックすると、自動的に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します。

- 証明書を提供するように管理者によって設定されたセキュア ゲートウェイへ接続するとインポートされます。

証明書のインポート後、この証明書を特定の接続エントリに関連付けるか、または接続確立中に認証のためにこの証明書を自動的に選択させることができます。

AnyConnect ストアに格納されているユーザ証明書は、認証に必要ではなくなった場合には削除できます。

関連トピック

ハイパーリンクによる証明書のインポート，（13 ページ）
手動での証明書のインポート，（13 ページ）
セキュア ゲートウェイから提供される証明書のインポート，（14 ページ）
証明書の表示，（26 ページ）
証明書の削除，（27 ページ）

ハイパーリンクによる証明書のインポート

管理者から、証明書をデバイスにインストールするためのハイパーリンクが提供されます。

はじめる前に

外部制御を設定してプロンプトを表示するか、AnyConnect 設定内で有効にします。

手順

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。

証明書が Android デバイスの AnyConnect 証明書ストアにインストールされます。この証明書の表示、接続エントリへの割り当て、または削除を行うことができます。

関連トピック

ユーザ証明書について，（12 ページ）

手動での証明書のインポート

以下の説明では、VPN 認証の目的でユーザ証明書を AnyConnect ストアに手動でインポートする場合のすべてのオプションを説明します。

はじめる前に

管理者から証明書インポート手順を入手します。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Certificate Management] をタップします。

ステップ 2 [User] タブをタップします。

ステップ 3 [Import] をタップし、次のいずれかの方法で証明書をインポートします。

- [File System] 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インポートします。
- [Network Location (URI)] をタップし、ネットワーク上のサーバから証明書をインポートします。
- [Device Credential Storage] をタップし、Android Credential Storage から証明書をインポートします。

（注）
- このオプションは、Android 4.0（Ice Cream Sandwich）以降を実行しているデバイスでのみ使用できます。
- Android 4.1（Jelly Bean）の Device Credential Storage から証明書をインポートしようとすると、クライアントではエラー メッセージ「This feature is not supported on this version of Android」が表示されます。 Android のネイティブ ストアを使用する代わりに、証明書を AnyConnect ストアに直接インポートします。

関連トピック

ユーザ証明書について，（12 ページ）

セキュアゲートウェイから提供される証明書のインポート

はじめる前に

管理者は、証明書の配布を有効にするようにセキュア ゲートウェイを設定し、セキュア ゲートウェイへの接続情報をユーザに提供します。

手順

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 [Get Certificate] が表示される場合はこれをタップします。それ以外の場合は、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ているグループを選択します。

ステップ 4 管理者から受け取った認証情報を入力します。

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、証明書の登録が正常に完了したことを示すメッセージを受け取ります。

関連トピック

ユーザ証明書について，（12 ページ）

第 3 章

VPN 接続の確立

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。

はじめる前に

- VPN に接続するには、アクティブな Wi-Fi 接続があるか、またはサービス プロバイダーに接続している必要があります。
- VPN 接続を開始するには、AnyConnect のホーム ウィンドウで [Choose a Connection] に接続エントリが 1 つ以上リストされている必要があります。
- VPN に接続するには、セキュア ゲートウェイに必要な認証情報が必要です。

手順

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 使用する接続エントリをタップします。

AnyConnect は、VPN 接続の開始時に、現在使用されているすべての VPN 接続を切断し、この接続エントリを現行接続にします。

ステップ 3 必要に応じて、認証プロンプトに対して次のいずれかの方法で応答します。

- ユーザ名とパスワードからなる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、次に管理者から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。

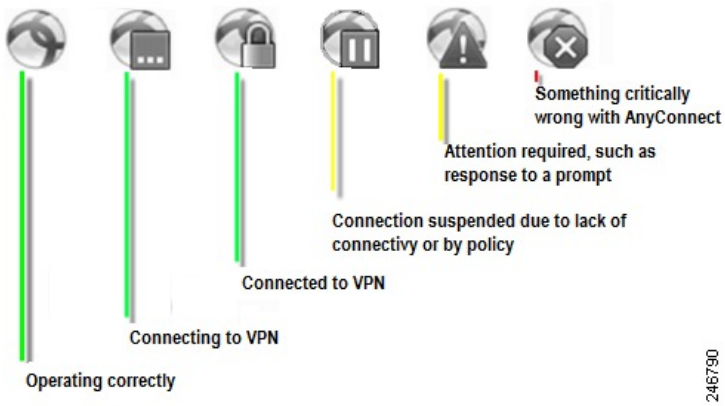
VPN セキュア ゲートウェイの設定に応じて、AnyConnect は、AnyConnect のホーム ウィンドウにあるリストに接続エントリを追加します。

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。

（注） AnyConnect のホーム ウィンドウにある別の VPN 接続をタップすると、現在の VPN 接続が切断され、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。

接続ステータスの確認

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。 アイコンは、AnyConnect接続の現在のステータスを示します。



[Connection Summary] の表示

手順

AnyConnect のホーム ウィンドウで、[Choose a connection] に表示される現在の接続の名前をタップします。

第 4 章

AnyConnect 通知への応答

信頼できない VPN サーバの通知への対応

表示される [Untrusted VPN Server] 通知のタイプは、[Block Untrusted VPN Server] アプリケーション プリファレンスに基づいています。

- このプリファレンスが有効であり、ブロックする **Untrusted VPN Server!** に関する通知が表示される場合は、次のいずれかを選択します。
  - この設定とこのブロック動作を維持する場合は、[Keep Me Safe] を選択します。
  - ブロックをオフにする場合は、[Change Settings] を選択します。

    [Block Untrusted VPN Server] を変更したら、VPN 接続を再び開始します。
- このプリファレンスが無効であり、ブロックしない **Untrusted VPN Server!** に関する通知が表示される場合は、次のいずれかを選択します。
  - 信頼できないサーバへの VPN 接続を中止するには、[Cancel] を選択します。
  - 信頼できないサーバに接続するには [Continue] を選択します。このオプションは推奨されません。
  - 証明書の詳細を表示し、今後接続を受け入れて続行するためにサーバ証明書を AnyConnect 証明書ストアにインポートするかどうかを決定するには、[View Details] を選択します。

関連トピック

サーバ証明書について，（26 ページ）

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

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。

- `Another application has requested that AnyConnect create a new connection to host. Do you want to allow this? [Yes] | [No]`
- `Another application has requested that AnyConnect connect to host. Do you want to allow this? [Yes] | [No]`
- `Another application has requested that AnyConnect disconnect the current connection. Do you want to allow this? [Yes] | [No]`
- `Another application has requested that AnyConnect import a certificate bundle to the AnyConnect certificate store. Do you want to allow this? [Yes] | [No]`
- `Another application has requested that AnyConnect import localization files. Do you want to allow this? [Yes] | [No]`
- `Another application has requested that AnyConnect import profiles. Do you want to allow this? [Yes] | [No]`

MMS 通知への応答

AnyConnect VPN に接続している間は、Multimedia（MMS）メッセージを取得または送信できません。 取得または送信しようとしてブロックされた場合、ステータス バーに MMS 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。

手順

ステップ 1 通知アイコンをタップして、通知を表示します。

ステップ 2 通知をクリックして、サービスの影響を表示します。

ステップ 3 今後 MMS 通知を受信しない場合は、[Do not show this again] チェックボックスをオンにします。

注目 これは永続的な選択操作です。 このアクションを後から取り消すことはできません。

ステップ 4 [OK] をタップします。

第 5 章

AnyConnect の設定と管理（オプション）

接続エントリの変更と削除

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したりする場合に、VPN 接続エントリを変更します。

（注） セキュア ゲートウェイからダウンロードし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。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、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 2 [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 3 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。

ステップ 4 [Done] をタップします。

AnyConnect は変更された接続エントリを保存して、AnyConnect ホーム ウィンドウを再オープンします。

関連トピック

AnyConnect 接続エントリについて，（10 ページ）

接続エントリの削除

この手順では、手動で設定した VPN 接続エントリを削除します。

（注） VPN セキュア ゲートウェイからインポートした接続エントリを削除する唯一の方法は、接続エントリが含まれているダウンロードした AnyConnect プロファイルを削除する方法です。

手順

ステップ 1 AnyConnect のホーム ウィンドウを開き、削除する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 2 [Delete connection] をタップします。

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

関連トピック

AnyConnect 接続エントリについて，（10 ページ）

証明書の設定

Android デバイス上の証明書について

証明書は、VPN 接続の両端（セキュア ゲートウェイまたはサーバと AnyConnect クライアントまたはユーザ）を電子的に識別するために使用されます。 サーバ証明書は AnyConnect に対してセキュア ゲートウェイを識別し、ユーザ証明書はセキュア ゲートウェイに対して AnyConnect ユーザを識別します。 証明書は認証局（CA）から取得し、CA によって検証されます。

接続の確立時に、AnyConnect は常にセキュア ゲートウェイからのサーバ証明書を要求します。 セキュア ゲートウェイでは、そのように設定されている場合にのみ AnyConnect からの証明書を要求します。 AnyConnect ユーザがクレデンシャルを手動で入力するように要求することでも、VPN接続を認証できます。 実際に、デジタル証明書、手動入力したクレデンシャル、またはこの両方を使用して AnyConnect ユーザを認証するようにセキュア ゲートウェイを設定できます。 証明書のみによる認証では、ユーザの操作を必要とせずに VPN が接続できます。

セキュア ゲートウェイとデバイスへの証明書の配布と、これらのデバイスによる証明書の使用は、管理者によって指示されます。 AnyConnect VPN のサーバ証明書とユーザ証明書をインポート、使用、管理する場合は、管理者の指示に従ってください。 このマニュアルに記載されている証明書と証明書管理に関連する情報と手順は、ユーザが理解し、参照できるようにする目的で提供されています。

AnyConnectは認証に使用するユーザ証明書とサーバ証明書の両方をAndroidデバイスのAnyConnect用の証明書ストアに格納します。 AnyConnect 証明書ストアは [Menu] > [Diagnostics] > [Certificate Management] 画面で管理します。また、この画面では Android System の証明書も確認できます。

ユーザ証明書について

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が含まれている必要があります。 ユーザ証明書は、管理者からの指示に従い次のいずれかの方法でインポートされます。

- 電子メールまたはWebページに含まれている管理者から提供されたハイパーリンクをクリックすると、自動的に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します。
- 証明書を提供するように管理者によって設定されたセキュア ゲートウェイへ接続するとインポートされます。

証明書のインポート後、この証明書を特定の接続エントリに関連付けるか、または接続確立中に認証のためにこの証明書を自動的に選択させることができます。

AnyConnectストアに格納されているユーザ証明書は、認証に必要ではなくなった場合には削除できます。

関連トピック

ハイパーリンクによる証明書のインポート，（13 ページ）
手動での証明書のインポート，（13 ページ）
セキュア ゲートウェイから提供される証明書のインポート，（14 ページ）
証明書の表示，（26 ページ）
証明書の削除，（27 ページ）

サーバ証明書について

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が有効かつ信頼できるものである場合にのみ、AnyConnect に対してそのサーバが自動的に認証されます。 その他の場合：

- 有効だが信頼できないサーバ証明書を調べて許可し、AnyConnect証明書ストアにインポートできます。 サーバ証明書が AnyConnect ストアにインポートされたら、これ以降このデジタル証明書を使用して行われるサーバ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。 証明書を受け入れて現行接続を確立することができますが、この方法は推奨されません。

AnyConnect ストアに格納されているサーバ証明書は、認証に必要ではなくなった時点で削除できます。

関連トピック

信頼できない VPN サーバの通知への対応，（21 ページ）
証明書の表示，（26 ページ）
証明書の削除，（27 ページ）

証明書の表示

AnyConnect 証明書ストアにインポートされたユーザ証明書とサーバ証明書、Android システム証明書を表示します。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Certificate Management] をタップします。

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

証明書を長押して次の項目をタップします。

- 証明書の内容を表示するには、[View certificate details] をタップします。
- AnyConnect ストアからこの証明書を削除するには、[Delete certificate] をタップします。

ステップ 3 Android Credential Storage 内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] をタップすると、証明書の内容を表示できます。

関連トピック

ユーザ証明書について，（12 ページ）
サーバ証明書について，（26 ページ）

証明書の削除

AnyConnect 証明書ストアの証明書のみを削除します。システム証明書ストアの証明書は削除できません。

証明書は個々に削除するか、または AnyConnect 証明書ストアから一括で削除することができます。

関連トピック

ユーザ証明書について，（12 ページ）
サーバ証明書について，（26 ページ）

1 つの証明書の削除

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Certificate Management] をタップします。

ステップ 2 [User] タブまたは [Server] タブをタップし、AnyConnect 証明書ストアのユーザ証明書またはサーバ証明書を表示します。

ステップ 3 証明書を長押しします。

[Certificate Options] が表示されます。

ステップ 4 [Delete certificate] を選択し、この特定の証明書を削除することを確認します。

すべての証明書の削除

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Certificate Management] をタップします。

ステップ 2 [User] タブまたは [Server] タブをタップし、AnyConnect 証明書ストアのユーザ証明書またはサーバ証明書を表示します。

ステップ 3 [Clear All] をタップし、AnyConnect 証明書ストアからすべての証明書を削除します。

アプリケーション プリファレンスの指定

手順

AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

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。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

ステップ 2 [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 3 表示する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。 オンにすると、[Launch at Startup] が有効になります。

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

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

ステップ 2 [Launch at Startup] チェックボックスをタップし、このプリファレンスを有効または無効にします。

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。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

ステップ 2 [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

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外部 URI 要求に応答する方法が指定されます。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が行われます。

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。 管理者から、このプリファレンスを次のいずれかの値に設定するよう指示されます。

- [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 にアクセスするたびにユーザに問い合わせます。 URI 要求を許可または拒否します。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。
ステップ 2 [External Control] をタップします。
ステップ 3 [Enabled]、[Disabled]、または [Prompt] をタップします。

信頼できないサーバのブロック

このアプリケーション設定は、AnyConnect がセキュア ゲートウェイを識別できない場合に接続をブロックするかどうかを決定します。 この保護はデフォルトでは ON です。OFF にできますが、OFF にする操作は推奨されません。

AnyConnect はサーバから受信した証明書を使用してそのアイデンティティを確認します。 期限切れまたは無効な日付、キーの不正な使用、または名前の不一致が原因で証明書エラーが発生すると、接続がブロックされます。

この設定が ON の場合は、ブロックに関する「**Untrusted VPN Server!**」通知によってこのセキュリティ上の脅威が警告されます。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。
ステップ 2 [Block Untrusted Servers] チェックボックスをタップし、このプリファレンス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 VPN 接続に連邦情報処理標準（FIPS）暗号化アルゴリズムが使用されます。

はじめる前に

ネットワークに接続するためにお使いのモバイル デバイスで FIPS モードを有効にする必要がある場合は、管理者からそのことが通知されます。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

ステップ 2 [FIPS Mode] チェックボックスをタップし、このプリファレンスを有効または無効にします。

FIPS モードの変更の確認後に、AnyConnect が終了します。AnyConnect を手動で再起動する必要があります。 再起動後に FIPS モード設定が有効になります。

Trusted Network Detection の設定

Trusted Network Detection（TND）により、デバイスが信頼ネットワーク外部にある場合に VPN 接続が自動的に開始され、デバイスが信頼ネットワークに戻ると VPN 接続が自動的に中断します。

管理者はこの機能を有効にし、信頼ネットワークと非信頼ネットワークを定義し、ネットワーク移行を検出した場合の AnyConnect の動作を決定します。 たとえば、管理者はホーム ネットワークに接続している間は自動的に接続し、企業ネットワークに移動すると切断するように TND を設定できます。

管理者がこの機能を有効にしている場合は、ユーザ自身のデバイスでこの機能を無効にできます。この機能は利便性のために提供されており、VPN を自動で接続、切断するため、ユーザが手動でこの操作を行う必要がないことに注意してください。 この機能を使用できるようにするには、TND を有効にします。

TND を有効にしても、信頼ネットワークに接続している間に VPN 接続を手動で確立したり、開始された VPN 接続を切断したりできます。 TND が VPN セッションを切断するのは、デバイスが最初に（自動または手動で）非信頼ネットワークに接続してから、信頼ネットワークに移行する場合だけです。

はじめる前に

Trusted Network Detection を使用するには、AnyConnect アプリケーションが実行されている必要があります。 [Menu] > [Exit] を使用してアプリケーションを終了した場合、または Android 設定を使用してアプリケーションを強制的に終了した場合は、AnyConnect は信頼ネットワークを検出できません。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Settings] > [Application Preferences] をタップします。

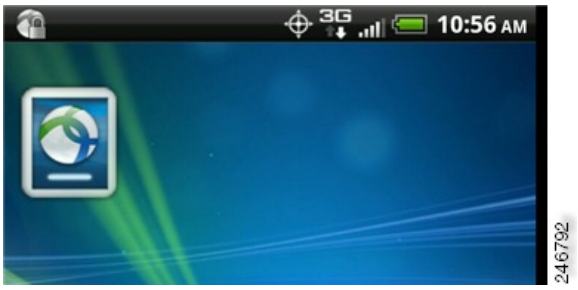
ステップ 2 [Trusted Network Detection] チェックボックスをタップし、このプリファレンスを有効または無効にします。

AnyConnect ウィジェットの使用

AnyConnect ウィジェットについて

AnyConnect には、ホーム画面に追加できるウィジェットがあります。

- 最も小さいウィジェットは、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。 現在の VPN セキュア ゲートウェイへ接続するか、または現在の VPN セキュア ゲートウェイから切断するには、ウィジェットをタップします。



- 大きなウィジェットは、AnyConnect アイコンと名前、現在の VPN 接続、VPN ステータスを示します。 VPN セキュア ゲートウェイへ接続するか、または VPN セキュア ゲートウェイから切断するには、ウィジェットをタップします。

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。 手順の例を示します。

手順

ステップ 1　使用するウィジェットを配置できる十分なスペースがある Android ホーム画面に移動します。

ステップ 2　[Menu] > [Personalize] > [Widgets] をタップします。

ステップ 3　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 4　ウィジェットを配置し直すには、ウィジェットを長押しします。 ウィジェットが応答したら、移動します。

AnyConnect クライアント プロファイルの管理

AnyConnect クライアント プロファイルについて

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、このデバイスから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。デバイスで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。

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で置き換えられます。
- VPN 接続にプロファイルが関連付けられていない場合、その VPN の起動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します。

関連トピック

AnyConnect プロファイルの表示, （34 ページ）
AnyConnect プロファイルのインポート, （34 ページ）
AnyConnect プロファイルの削除, （35 ページ）

AnyConnect プロファイルの表示

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Profile Management] をタップします。

ステップ 2 [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。

関連トピック

AnyConnect クライアント プロファイルについて，（33 ページ）

AnyConnect プロファイルのインポート

はじめる前に

プロファイル ファイルをこの方法でインポートするには、Android デバイスにプロファイル ファイルが存在している必要があります。 管理者から、デバイスにインストールするプロファイル ファイルの名前が提供されます。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Profile Management] をタップします。

ステップ 2 [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。

このプロファイルで定義されている接続エントリが 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仕様に従います。

関連トピック

AnyConnect クライアント プロファイルについて，（33 ページ）

AnyConnect プロファイルの削除

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Profile Management] をタップします。

ステップ 2 [Delete Profile] をタップして、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。

関連トピック

AnyConnect クライアント プロファイルについて，（33 ページ）

ローカリゼーションの管理

Android デバイスのローカリゼーションについて

インストールされているローカリゼーション

AnyConnect をインストールすると、Android デバイスのロケールがパッケージに含まれている言語変換に一致する場合には Android デバイスがローカライズされます。 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）

表示言語は [Settings] > [Language and Keyboard] > [Select locale] で指定されているロケールによって決定します。 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。 選択されているローカリゼーションは、AnyConnect の [Menu] > [Diagnostics] > [Localization Management] 画面で [Active] として示されます。

ローカリゼーションのインポート

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 ページで提供できます。 この方法では、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 [Import Localization] オプションを使用して手動でインポートされます。

ローカリゼーションの復元

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すると、インポートされたローカリゼーションデータがすべて削除されます。復元する言語は、指定されたデバイス ロケールをインストールされているローカリゼーションデータと照合することで選択されます。

ローカリゼーション データの管理

手順

AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Localization Management] をタップします。

次の作業

- [Import Localization]：指定したサーバからローカリゼーション データをインポートします。
- [Restore Localization]：デフォルト ローカリゼーション データを復元します。
- [Localization Files]：ローカリゼーション ファイルのリストを表示します。

サーバからのローカリゼーション データのインポート

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Localization Management] をタップします。

ステップ 2 [Import Localization] をタップします。

セキュア ゲートウェイのアドレスと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。

ローカリゼーション データの復元

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Localization Management] をタップします。

ステップ 2 [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。

復元する言語は、[Settings] > [Language and Keyboard] > [Select locale] で指定されているデバイスのロケールによって決定します。

AnyConnect の終了

AnyConnect を終了すると、現在の VPN 接続が終了し、すべての AnyConnect プロセスが停止されます。 このアクションは慎重に使用してください。お使いのデバイス上の他のアプリケーションやプロセスが現在の VPN 接続を使用しており、AnyConnect を終了するとこれらのアプリケーションやプロセスの動作に悪影響を及ぼす可能性があります。

手順

AnyConnect のホーム ウィンドウで、[Menu] > [Exit] をタップします。

AnyConnect がすべてのプロセスを正常に終了できない場合は、Android アプリケーション管理画面が表示されます。[Force Stop] をタップして AnyConnect を手動で終了します。

AnyConnect の削除

手順

ステップ 1 お使いのデバイスの [Android Settings] に移動し、アプリケーション管理領域に進みます。

ステップ 2 [Uninstall] をタップします。

第 6 章

AnyConnectのモニタリングとトラブルシューティング

AnyConnectのバージョンおよびライセンスの詳細の表示

手順

AnyConnect のホーム ウィンドウで、[Menu] > [About] をタップします。

次の作業

[About] ウィンドウでリンクをタップして、このマニュアルの最新のバージョンをオープンします。

AnyConnect 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。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Statistics] をタップします。

ステップ 2 [Details] をタップして、詳細な統計情報を表示します。

統計	説明
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されます。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です。

AnyConnect ロギング

ログ メッセージの表示

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Logging and System Information] をタップします。

AnyConnect はメッセージを取得し、[Messages]、[System]、および [Debug] ウィンドウに表示します。

ステップ 2 [Messages] 、[System] 、または [Debug] タブをタップし、ログ メッセージまたはシステム情報を表示します。

- [Messages]：AnyConnect アクティビティに関連するログ。
- [System]：メモリ、インターフェイス、ルート、フィルタ、許可、プロセス、システム プロパティ、メモリ マップ、および固有のデバイス ID に関する情報。
- [Debug]：管理者と Cisco Technical Assistance Center（TAC）が AnyConnect の問題を分析するときに使用するログ。

ステップ 3 すべて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。

ログ メッセージの送信

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Logging and System Information] をタップします。

ステップ 2 [Send Logs] をタップします。

ログ メッセージとすべてのプロファイル データが .zip ファイルにパッケージ化され、電子メール メッセージに挿入されます。 AnyConnect に関する問題を報告する場合は、電子メール 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。 ログ メッセージを送信する前に、問題記述と問題再現手順を指定する必要があります。

ローカルに送信する場合はBluetooth を使用します。 最初に送信デバイスと受信デバイスの両方で Bluetooth を有効にしておく必要があります。

デバッグ ログ メッセージの消去

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[Menu] > [Diagnostics] > [Logging and System Information] をタップします。

ステップ 2 [Clear Debug Logs] をタップします。

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）メッセージの送受信が阻止されます。 ほとんどのデバイスとサービス プロバイダーでは、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通知が表示されます。 Android では VPN に接続していないときにメッセージの送受信が許可されます。

一般的な問題

tun.ko エラー メッセージが返されます

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の削除手順については、AnyConnectプロファイルの表示および管理に関する項を参照してください。

接続タイムアウトと未解決のホスト

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 のホーム 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。

接続エラー、デバイスは問題なく動作します

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。 ネットワーク接続を確認するには、https://vpn.example.com（vpn.example.com はVPNセキュア ゲートウェイのURL）に移動します。

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 デバイスのリストと、AnyConnect のインストールまたはアップグレードの手順を参照して、デバイスに適切な AnyConnect パッケージをダウンロードします。

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。 サポートされる Android デバイスのリストと、AnyConnect のインストールまたはアップグレードの手順を参照して、デバイスに適切な AnyConnect パッケージをダウンロードします。

ネットワーク接続の問題のため、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。 ネットワーク接続がない場合、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 が頻繁に AnyConnect 自体に接続します

これは、Trusted Network Detection / Automatic VPN Policy が原因で発生することがあります。 この機能をオフにするには、AnyConnect 設定の TND アプリケーション プリファレンスを無効にします。