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 4.0.x）

Revised: October 10, 2016,

AnyConnect ユーザ ガイド

AnyConnect のインストールおよび起動

AnyConnect の概要

Android 用 Cisco AnyConnect セキュア モビリティ クライアントは、企業ネットワークへのシームレスかつセキュアなリモート 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。AnyConnect は高度なネットワーキング アプリケーションであり、プリファレンスを設定したり、AnyConnect の動作を制御したり、デバイスで管理者が推奨する診断ツールや診断機能を使用したりすることも可能です。

企業で AnyConnect をモバイル デバイス管理ソフトウェアと組み合わせて使用する場合があります。その場合、デバイス管理ルールに、VPN アクセス許可を、承認された一連のアプリケーションに限定するなどの内容が含まれる場合があるため、管理者と協力してデバイス管理ルールに従うようにしてください。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ある場合があります。

Android App Store には、初期インストールとすべてのアップグレード用のアプリケーションが用意されています。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、モバイル デバイス向け AnyConnect の更新はサポートしません。

オープン ソフトウェア ライセンスに関する通知

- 本製品には、OpenSSL Toolkit（http://www.openssl.org/）で使用するために OpenSSL プロジェクトによって開発されたソフトウェアが含まれています。（This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit（http://www.openssl.org/）.）
- 本製品には、Eric Young 氏（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれています。（This product includes cryptographic software written by Eric Young（eay@cryptsoft.com）.）
- 本製品には、Tim Hudson 氏（tjh@cryptsoft.com）によって作成されたソフトウェアが含まれています。（This product includes software written by Tim Hudson（tjh@cryptsoft.com）.）

Android でサポートされるデバイス

Cisco AnyConnect on Android のフル サポートは、Android 4.0（Ice Cream Sandwich）以降を実行しているデバイスで提供されます。

Kindle Fire HD デバイスと新しい Kindle Fire 向けの Cisco AnyConnect on Kindle を Amazon から入手できます。Anyconnect for Kindle は、AnyConnect for Android パッケージと同じ機能を備えています。

Samsumg KNOX MDM を使用するように設定された場合、マネージド環境で Per App VPN がサポートされます。これには、Samsung Knox 2.0 がある Android 4.3 以降を実行している Samsung デバイスが必要です。これ以外の場合、Per App VPN は一般的な Android 方式を使用します。

インストールおよびアップグレードの手順については、Android User Guide for Cisco AnyConnect Secure Mobility Client, Release 4.0を参照してください。

Android AnyConnect アプリケーションのインストール

AnyConnect for Android は、Android デバイス用の Android Market からのみダウンロードできます。Kindle デバイス用は Amazon からダウンロードします。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。

AnyConnect for Android をインストールするには、デバイスにアプリケーションをダウンロードし、インストールまたはアップグレードするための通常の手順に従います。

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 [接続（Connection）] > [新しい VPN 接続の追加（Add New VPN Connection）] をタップして、接続エントリを設定します。詳細については、手動での接続エントリの追加, （6 ページ）を参照してください。

ステップ 4 （任意） 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を表示するには、[詳細（Details）] をタップします。「AnyConnect 統計情報の表示」を参照してください。

ステップ 5 （任意） [メニュー（Menu）] をタップして、次のいずれかを選択します。

- [設定（Settings）]：AnyConnect アプリケーション プリファレンスを指定します。「アプリケーション設定の指定」を参照してください。
- [診断（Diagnostics）]：次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：「ローカリゼーションの管理」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。
- [バージョン情報（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表示」を参照してください。

- [終了（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。

Android デバイスのアクセス許可

次のアクセス許可が AnyConnect の動作用に Android マニフェスト ファイルで宣言されます。

マニフェストのアクセス許可	説明
uses-permission: android.permission.ACCESS_NETWORK_STATE	アプリケーションがネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.ACCESS_WIFI_STATE	アプリケーションが Wi-Fi ネットワークの情報にアクセスすることを許可します。
uses-permission: android.permission.BROADCAST_STICKY	アプリケーションがスティッキ インテントをブロードキャストすることを許可します。これは、クライアントが次のブロードキャストを待たなくてもデータをすぐに取得できるよう、完了後もデータがシステムによって保持されるブロードキャストです。
uses-permission: android.permission.INTERNET	アプリケーションがネットワーク ソケットを開くことを許可します。
uses-permission: android.permission.READ_EXTERNAL_STORAGE	アプリケーションが外部ストレージから読み取ることを許可します。
uses-permission: android.permission.READ_LOGS	アプリケーションが低レベルのシステム ログ ファイルを読み取ることを許可します。
uses-permission: android.permission.READ_PHONE_STATE	デバイスの電話番号、現在の携帯電話ネットワーク情報、通話中のコールのステータス、デバイスに登録されているすべての PhoneAccounts のリストなどの電話状態への読み取り専用アクセスを許可します。
uses-permission: android.permission.RECEIVE_BOOT_COMPLETED	システムの起動完了後にアプリケーションがブロードキャストを受信することを許可します。

VPN 接続の設定

AnyConnect が VPN 接続を確立するには、次の情報が必要となります。

- 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。

  このアドレスは、接続エントリで設定されます。接続エントリは、AnyConnect のホーム画面にリストされます。アクティブな接続エントリは、AnyConnect ホーム画面または [接続（Connections）] リストに示されます。VPN 接続エントリは、デバイス上で手動で設定するか、または社内の管理者によって自動設定されます。

- 正常に接続を確立するための認証情報。

  これは、覚えておく必要のあるユーザ名とパスワードの形式となるか、またはデバイスに設定されたデジタル証明書に含められます。一部の VPN 接続では、両方の認証方式が必要になる場合があります。デジタル証明書は、デバイス上で手動で設定するか、または社内の管理者によって自動設定されます。

管理者の指示に従って AnyConnect クライアントを設定します。明確な指示がない場合は、管理者に問い合わせてください。

接続エントリの設定

接続エントリは、プライベート ネットワークへのアクセスを提供するセキュア ゲートウェイ、およびその他の接続属性を指定します。

すでにデバイスで設定されているエントリを表示するには、AnyConnect のホーム画面から [接続（Connections）] を選択します。複数の接続エントリがリストされることもあります。接続エントリは、次のステータスになっています。

- [アクティブ（Active）]：このマークまたは強調表示された接続エントリは、現在アクティブです。
- [接続済み（Connected）]：この接続エントリは、アクティブなエントリであり、現在接続され、稼動しています。
- [切断済み（Disconnected）]：この接続エントリは、アクティブなエントリですが、現在切断され、稼動していません。

手順

接続エントリは、次の方法でデバイス上で手動または自動で設定されます。

- 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、所属するグループを指定することもあります。その他の接続属性も設定できます。を参照してください手動での接続エントリの追加, （6 ページ）。

- 管理者から提供されたリンクをクリックすることで、自動的に設定されます。

  AnyConnect URI リンクは電子メールに含まれるか、または Web ページで公開されます。このことをデバイスで許可するには、アプリケーション プリファレンスの [外部制御（External Control）] を、[プロンプト（Prompt）] または [有効（Enable）] に設定する必要があります。参照先 AnyConnect の外部使用の制御, （15 ページ）

- 接続エントリを含む AnyConnect クライアント プロファイルをダウンロードするセキュア ゲートウェイに接続した後で、自動的に設定されます。AnyConnect クライアント プロファイルの管理, （19 ページ）を参照してください。
- 会社のモバイル デバイス管理ソフトウェアによる設定。デバイス管理プロファイルが、デバイスの一般設定下に見つかる場合があります。

手動での接続エントリの追加

接続する VPN セキュア ゲートウェイを特定する 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 [接続（Connection）] > [新しい VPN 接続の追加（Add New VPN Connection）] をタップし、接続エディタを開きます。
接続エディタはいつでもキャンセルできます。

ステップ 2 （任意） [説明（Description）] 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一意の名前を入力します。名前を指定しない場合、デフォルトとして [サーバ アドレス（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 [サーバ アドレス（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、グループも含まれます。

ステップ 4 （任意） [詳細プリファレンス（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。
[詳細接続エディタ（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） [証明書（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。

- [無効（Disabled）] をタップして、証明書をこの接続に使用しないことを指定します。
- [自動（Automatic）] をタップして、セキュア ゲートウェイによって要求される場合にのみ、接続の確立に証明書を使用するように指定します。
- 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） [IPSec を使って接続（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、[認証（Authentication）] パラメータがアクティブになります。

ステップ 7 （任意） [認証（Authentication）] をタップし、この IPSec 接続の認証方式を選択します。
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 [詳細接続エディタ（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 ID（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 [詳細（Advanced）] ウィンドウと [接続エディタ（Connection Editor）] ウィンドウの両方で [完了（Done）] をタップし、接続値を保存します。
AnyConnect は、新しい接続エントリを追加します。

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 ホーム ウィンドウで、[接続（Connection）] をタップします。次に、接続エントリを長押しして [アクションの選択（Select Action）] ウィンドウを表示します。

ステップ 2 [接続の編集（Edit connection）] をタップします。
[接続エディタ（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 [完了（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ます。

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。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ホーム ウィンドウで、[接続（Connection）] をタップします。次に、接続エントリを長押しして [アクションの選択（Select Action）] ウィンドウを表示します。

ステップ2 [接続を削除（Delete connection）] をタップします。

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。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、およびセキュア ゲートウェイと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。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、参考にしてもらうために提供されています。

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 [メニュー（Menu）] > [診断（Diagnostics）] > [証明書の管理（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、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。

- 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自動的にインポート。
- 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。
- 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。

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。

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。該当しない場合は、次のようになります。

- 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。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する、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。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。

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

AnyConnect 設定内で、[外部制御（External Control）] を [プロンプト（Prompt）] または [有効（Enable）] に設定します。

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。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [証明書の管理（Certificate Management）] をタップします。

ステップ 2 [ユーザ（User）] タブをタップします。

ステップ 3 [インポート（Import）] をタップして、証明書をインポートします。

ステップ 4 インポート元を選択します。

- [ファイル システム（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。
- [ネットワークの場所（URI）（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。
- [デバイス クレデンシャル ストレージ（Device Credential Storage）] をタップして、現在デバイス クレデンシャル ストレージ内に存在する証明書とリンクします。

  ソース証明書は、AnyConnect 証明書ストアに実際にコピーされません。証明書がクレデンシャル ストレージから削除されると、証明書へのリンクも削除されます。

  （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「この機能は、Android のこのバージョンではサポートされていません（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。

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 [接続を選択（Choose a connection）] 領域で、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 [証明書を取得（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。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [証明書の管理（Certificate Management）] をタップします。

ステップ 2 [ユーザ（User）] または [サーバ（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。

証明書を長押し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、[証明書の詳細の表示（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、[証明書の削除（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、[システム（System）] タブをタップします。

証明書を長押しして [証明書の詳細の表示（View certificate details）] をタップすると、証明書の内容を表示できます。

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クリアすることができます。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [証明書の管理（Certificate Management）] をタップします。
ステップ 2	[ユーザ（User）] タブまたは [サーバ（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。 [証明書オプション（Certificate Options）] が表示されます。
ステップ 4	[証明書の削除（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。

すべての証明書のクリア

手順

ステップ 1	AnyConnect のホーム ウィンドウで、[メニュー（Menu）] > [診断（Diagnostics）] > [証明書の管理（Certificate Management）] をタップします。
ステップ 2	[ユーザ（User）] タブまたは [サーバ（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	[すべてクリア（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。

VPN 接続の確立

VPN に接続するには、[AnyConnect VPN] パネルに表示されたアクティブな接続に関連付けられたチェックボックスまたはスライダをタップするか、AnyConnect ホーム画面に示されているその他の接続エントリの 1 つを選択します。

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 [接続を選択（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 ゲートウェイによって想定される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	[接続（Connection）] をタップしてから、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、この接続エントリが VPN 接続を開始したら、これ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。
- [証明書を取得（Get Certificate）] をタップし、次に管理者から提供される証明書の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。

AnyConnect 通知への応答

信頼できない VPN サーバ通知への応答

表示される [信頼されていない VPN サーバ（Untrusted VPN Server）] 通知のタイプは、[信頼できない VPN サーバのブロック（Block Untrusted VPN Server）] アプリケーション 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、ブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」が表示されます。次のいずれかを選択します。
  - [安全を確保（Keep Me Safe）]：この設定とこのブロッキング動作を保持します。
  - [設定の変更（Change Settings）]：ブロッキングをオフにします。

    [信頼できない VPN サーバのブロック（Block Untrusted VPN Server）] を変更したら、VPN 接続を再び開始します。
- 有効になっていない場合、ノンブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」が表示されます。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、[キャンセル（Cancel）] を選択します。
  - 信頼できないサーバに接続するには [続行（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、[詳細の表示（View Details）] を選択します。

別のアプリケーションへの応答

デバイスを保護するため、AnyConnect は、外部アプリケーションが AnyConnect を使用しようとすると警告します。これは、AnyConnect アプリケーション プリファレンスの [外部制御（External Control）] が [プロンプト（Prompt）] に設定されている場合に生じます。

次のプロンプトに対して [はい（Yes）] をタップするかどうか管理者に確認してください。

- `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、マルチメディア（MMS）メッセージの取得や送信はできません。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 通知をタップして、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、[次回から表示しない（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。

AnyConnect の設定と管理（オプション）

アプリケーション設定の指定

スタートアップ時の AnyConnect の起動

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、[スタートアップ時に起動（Launch at Startup）] が有効になります。

（注） 信頼ネットワーク検出を指定してプロファイルをダウンロードまたはインポートすると、[スタートアップ時に起動（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、[メニュー（Menu）] > [設定（Settings）] をタップします。

ステップ 2 [スタートアップ時に起動（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 バーのアイコンを非表示にする

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、[メニュー（Menu）] > [設定（Settings）] をタップします。

ステップ 2 [アイコンを表示しない（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設定により、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、または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、一般には管理者により電子メールまたは Web ページで提供されます。管理者は、次の値のいずれかを使用するように指示します。

- [有効（Enabled）]：AnyConnect アプリケーションは自動的にすべての URI コマンドを許可します。
- [無効（Disabled）]：AnyConnect アプリケーションは自動的にすべての URI コマンドを拒否します。
- [プロンプト（Prompt）]：AnyConnect アプリケーションは、デバイス上の AnyConnect URI にアクセスするたびプロンプトを表示します。URI 要求を許可または拒否します。詳細については、別のアプリケーションへの応答，（14 ページ）を参照してください。

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[メニュー（Menu）] > [設定（Settings）] をタップします。
ステップ 2 [外部制御（External Control）] をタップします。
ステップ 3 [有効（Enabled）]、[無効（Disabled）]、または [プロンプト（Prompt）] をタップします。

信頼されてい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 にすることは推奨されません。

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 になっている場合、ブロッキング通知「信頼できない VPN サーバ（Untrusted VPN Server!）」により、このセキュリティ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、[メニュー（Menu）] > [設定（Settings）] をタップします。
ステップ 2 [信頼されていないサーバをブロック（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、[メニュー（Menu）] > [設定（Settings）] をタップします。

ステップ 2 [FIPS モード（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。

OCSP 失効の設定

Android AnyConnect クライアントは OCSP（Online Certificate Status Protocol）をサポートします。これにより、OCSP レスポンダに要求を行い OCSP 応答を解析して証明書のステータスを取得することで、クライアントはリアルタイムで個々の証明書のステータスを照会できます。OCSP は、証明書チェーン全体を確認するために使用されます。OCSP レスポンダにアクセスする際、証明書ごとに 5 秒間のタイムアウト間隔があります。

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 [OCSP 失効（OCSP Revocation）] 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、[メニュー（Menu）] > [設定（Settings）] をタップします。

ステップ 2 [OCSP 失効（OCSP Revocation）] 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。
次に接続を試行する際、ヘッドエンドから受信した証明書の失効のステータスを確認するために、OCSP が使用されます（または使用されません）。

厳格な証明書トラスト

選択すると、リモート セキュリティ ゲートウェイを認証するときに、AnyConnect はユーザの操作なしに自動的に確認できない証明書を許可しません。これらの証明書を受け入れるようユーザにプロンプトを表示するのではなく、クライアントは接続に失敗します。この設定は、[信頼されていないサーバをブロック（Block Untrusted Servers）] よりも優先されます。

オフにすると、クライアントはユーザに証明書を受け入れるかどうかを確認するプロンプトを表示します。これはデフォルトの動作です。

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 [厳格な証明書トラスト（Strict Certificate Trust）] 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

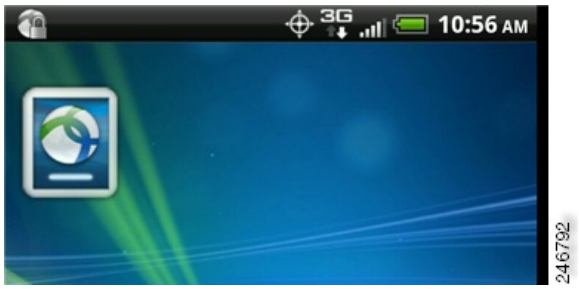
ステップ 1 AnyConnect のホーム ウィンドウで、[メニュー（Menu）] > [設定（Settings）] をタップします。

ステップ 2 [厳格な証明書トラスト（Strict Certificate Trust）] 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。
次に接続を試行する際、ヘッドエンドから受信した未確認の証明書の受け入れをユーザが選択できるかどうか決定するために、[厳格な証明書トラスト（Strict Certificate Trust）] が使用されます（または使用されません）。

AnyConnect ウィジェットの使用方法

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 アプリケーション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。VPN 接続を確立するか、または現在の VPN 接続から切断するには、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 接続を確立するか、または VPN 接続から切断するには、ウィジェットをタップします。

ウィジェットを配置する手順は、使用するデバイスおよび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	[メニュー（Menu）] > [個人設定（Personalize）] > [ウィジェット（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。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [プロファイル管理（Profile Management）] をタップします。

ステップ 2 [現在のプロファイルの詳細（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。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [プロファイル管理（Profile Management）] をタップします。

ステップ 2 [プロファイルのインポート（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。

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、[メニュー（Menu）] > [診断（Diagnostics）] > [プロファイル管理（Profile Management）] をタップします。

ステップ 2 [プロファイルの削除（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。

ローカリゼーションの管理

インストール済みローカリゼーション データの表示

AnyConnect をインストールすると、デバイスで指定されている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、モバイル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。

- カナダ フランス語（fr-ca）
- 中国語（台湾）（zh-tw）
- チェコ語（cs-cz）
- オランダ語（nl-nl）
- フランス語（fr-fr）
- ドイツ語（de-de）
- ハンガリー語（hu-hu）
- イタリア語（it-it）
- 日本語（ja-jp）
- 韓国語（ko-kr）
- 中南米スペイン語（es-co）
- ポーランド語（pl-pl）
- ポルトガル語（ブラジル）（pt-br）
- ロシア語（ru-ru）
- 簡体字中国語（zh-cn）
- スペイン語（es-es）

インストールされる言語は、[設定（Settings）]>[言語とキーボード（Language and Keyboard）]>[ロケールの選択（Select locale）] で指定されているロケールによって決定されます。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。

AnyConnect は最適なものを判断するために、言語仕様、地域仕様の順に使用します。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。

手順

ステップ 1 AnyConnect ホーム ウィンドウで、[メニュー（Menu）] > [診断（Diagnostics）] > [ローカリゼーション管理（Localization Management）] をタップします。

ステップ 2 モバイル デバイスにインストールされたローカリゼーション ファイルのリストを表示します。

示されている言語が、現在 AnyConnect で使用されています。

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） AnyConnect設定内で外部制御を[プロンプト（Prompt）]または[有効（Enable）]に設定して、この AnyConnect アクティビティ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, （15 ページ）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 ローカリゼーション管理アクティビティ（AnyConnect Localization Management Activity）] 画面の [ローカリゼーションのインポート（Import Localization）] オプションを使用して手動でインポートします。

手順

ステップ 1 AnyConnect ホーム ウィンドウで、[メニュー（Menu）] > [診断（Diagnostics）] > [ローカリゼーション管理（Localization Management）] をタップします。

ステップ 2 [ローカリゼーションのインポート（Import Localization）] をタップします。

ステップ 3 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 によって指定され、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 ホーム ウィンドウで、[メニュー（Menu）] > [診断（Diagnostics）] > [ローカリゼーション管理（Localization Management）] をタップします。

ステップ 2 [ローカリゼーションの復元（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、[設定（Settings）] > [言語とキーボード（Language and Keyboard）] > [ロケールの選択（Select locale）]で指定されているデバイスのロケールに基づいて選択されます。

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。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 接続を使用している場合があり、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、[メニュー（Menu）] > [終了（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。[強制停止（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 デバイスの [Android 設定（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 [アンインストール（Uninstall）] をタップします。

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表示

手順

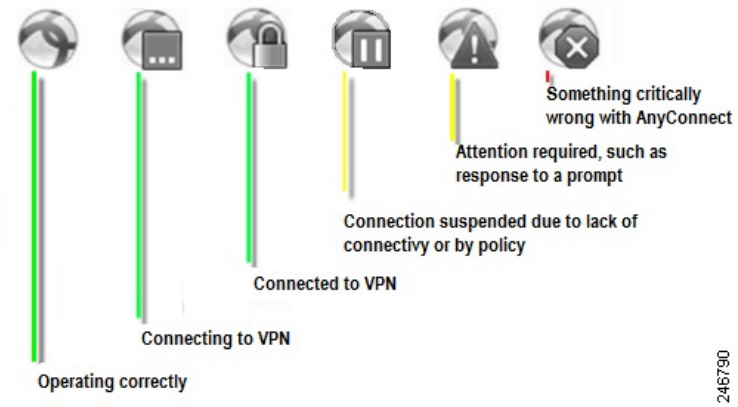
AnyConnect のホーム ウィンドウで、[メニュー（Menu）] > [バージョン情報（About）] をタップします。

次の作業

[バージョン情報（About）] ウィンドウでリンクをタップして、このガイドの最新バージョンを開きます。

接続ステータスの判別

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。



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

AnyConnect のホーム画面で、[詳細（Details）] をタップします。

詳細な統計情報には次の値が含まれます。

- [セキュア ルート（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 のエントリは、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。
- [保護されていないルート（Non-Secure Routes）]：[セキュア ルート（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 のロギング

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、[メニュー（Menu）] > [診断（Diagnostics）] > [ロギングおよびシステム情報（Logging and System Information）] をタップします。

AnyConnect はメッセージを取得し、[メッセージ（Messages）]、[システム（System）]、および [デバッグ（Debug）] ウィンドウに表示します。

ステップ 2 [メッセージ（Messages）]、[システム（System）]、または [デバッグ（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。

- [メッセージ（Messages）]：AnyConnect アクティビティに関連するログ。
- [システム（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。
- [デバッグ（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、[メニュー（Menu）] > [診断（Diagnostics）] > [ロギングおよびシステム情報（Logging and System Information）] をタップします。

ステップ 2 [メニュー（Menu）] > [ログの送信（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。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 メッセージのクリア

手順

ステップ 1 AnyConnect のホーム ウィンドウで、[メニュー（Menu）] > [診断（Diagnostics）] > [ロギングおよびシステム情報（Logging and System Information）] をタップします。

ステップ 2 [メニュー（Menu）] > [デバッグログの消去（Clear Debug Logs）] をタップします。

一般的な Android の問題

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。このモジュールがデバイスに含まれていない、またはカーネルに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用に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してみるか、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、デバイスの設定アプリケーションを使用して、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、[証明書（Certificate）] をタップします。[証明書（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、[証明書の詳細の表示（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

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管理者に問い合わせます。

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。ネットワークの接続性を確認するには、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。

「インストール エラー：不明な理由 -8（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 パッケージ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、「このアプリケーションを実行するための必要な許可を取得できませんでした。このデバイスは、AnyConnect をサポートしていません。（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 が頻繁に AnyConnect 自体に接続します

これは、信頼ネットワーク検出や自動 VPN ポリシーが原因で発生することがあります。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て、この機能をオフにします。

ワンタイム パスワードを使用した認証が動作しません

Android の問題が原因で、クリップボードからテキストを貼り付けるときに、テキストの前にスペースが挿入されます。AnyConnect では、ワンタイム パスワードなどのテキストをコピーする場合は、ユーザがこの不要な空白文字を削除する必要があります。

Android での AnyConnect の注意事項と制約事項

- AnyConnect for Android 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。
- ASA は、AnyConnect for Android のディストリビューションと更新プログラムを提供しません。Google Play からのみ入手できます。
- AnyConnect for Android では、ユーザが追加する接続エントリと、ASA によりプッシュされる AnyConnect プロファイルによって挿入される接続エントリがサポートされています。Android デバイスでは 1 つの AnyConnect プロファイル（ヘッドエンドから受信した最後のプロファイル）だけがサポートされます。ただし、プロファイルは複数の接続エントリで構成できます。
- 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、「インストールエラー：原因不明 -8（Installation Error: Unknown reason -8）」というポップアップ メッセージが表示されます。これは Android OS により生成されるメッセージです。
- ユーザがホーム スクリーンに AnyConnect ウィジェットを表示している場合、[始動時に開始（Launch at startup）] 設定に関わらず AnyConnect サービスが自動的に開始されます（ただし接続は確立されません）。
- AnyConnect for Android では、クライアント証明書からの事前入力を使用する場合に、拡張 ASCII 文字のために UTF-8 文字エンコードが必要です。事前入力機能を使用する場合は、クライアント証明書が UTF-8 でなければなりません（KB-890772 および KB-888180 の説明を参照）。
- 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。
- いくつかのよく知られているファイル圧縮ユーティリティでは、[AnyConnectログ送信（AnyConnect Send Log ）] ボタンを使用してパッケージされたログ バンドルを圧縮解除できません。回避策として、AnyConnect ログ ファイルの圧縮解除には Windows および Mac OS X のネイティブ ユーティリティを使用してください。

既知の互換性の問題

- パブリック インターフェイスとプライベート インターフェイスにおける IPv6。

  IPv6 は、AnyConnect 4.05015 以降を使用するプライベートおよびパブリック トランスポートの両方でサポートされており、Android 5 以降で対応しています。この組み合わせにより、IPv6 トンネルを介した IPv4 および IPv6 トンネルを介した IPv6 が可能になります。

以前のバージョンの AnyConnect と Android リリースで従来から使用できたトンネル設定（IPv4 トンネルを介した IPv4 および IPv4 トンネルを介した IPv6）も引き続き使用できます。

（注） Android に存在する既知の問題（Issue #65572）が原因で、IPv6 over IPv4 は Android 4.4 上で機能しません。Android 5 以降を使用する必要があります。

- バッテリ セーバーおよび AnyConnect：
  - Android 5.0 では、デバイスでのバックグラウンド ネットワーク接続をブロックするバッテリ セーバー機能が導入されました。バッテリ セーバーを有効にした場合、AnyConnect がバックグラウンドで実行されると、一時停止状態に移行します。Android 5.0 でこれを回避するには、デバイス設定でバッテリ セーバーをオフにすることができます（[設定（Settings）] -> [バッテリ（Battery）] -> [バッテリ セーバー（Battery saver）] または通知バーから）。
  - Android 6.0 以降では、AnyConnect がバッテリ セーバーの結果として一時停止状態に移行する場合、AnyConnect をバッテリ セーバー モードからホワイトリストに登録するオプションを選択できるポップアップが表示されます。AnyConnect をホワイトリストに登録すると、バックグラウンドで実行する AnyConnect の機能に影響を与えずに、バッテリ セーバーを引き続き利用できます。
  - バッテリ セーバーが原因で AnyConnect が一時停止した場合、バッテリ セーバーをオフにするにしても、AnyConnect をホワイトリストに登録するにしても、AnyConnect を一時停止状態から戻すために手動で再接続する必要があります。

- スプリット DNS は、Android 4.4 デバイスでは機能しません。また、Samsung 製の Android 5.x デバイスでも機能しません。Samsung デバイスの場合、唯一の回避策は、スプリット DNS を無効にしてグループに接続することです。その他のデバイスでは、Android 5.x にアップグレードして、この問題の修正を入手する必要があります。

  これは、Android 4.4 に存在する既知の問題（ Issue #64819）によるもので、Android 5.x で修正されましたが、Samsung 製の Android 5.x デバイスには組み込まれませんでした。

- Android 5.x のバグ（Google Issue #85758、Cisco Issue # CSCus38925）が原因で、AnyConnect アプリケーションを Recent Apps 画面から閉じると、正しく動作しない場合があります。正常な動作を復元するには、AnyConnect を [設定（Settings）] で停止してから、再起動します。

- Samsung モバイル デバイスでは、[設定（Settings）] > [Wi-Fi] > [スマート ネットワーク スイッチ（Smart network switch）] で、安定したインターネット接続を維持するために Wi-Fi から LTE に切り替えることができます（Wi-Fi 接続が最適でない場合）。この場合も、アクティブな VPN トンネルが一時停止し、再接続します。何度も繰り返し再接続することになるため、この機能を無効にすることをお勧めします。

- 複数のアクティブ ユーザをサポートする Android 5.0（Lollipop）で、VPN 接続はデバイス上のすべてのユーザではなく、単一のユーザのデータのみをトンネルします。バックグラウンド データ フローが暗号化されずに発生する可能性があります。

- Android 4.3.1 のバグ（Google Issue #62073）が原因で、AnyConnect ICS+ パッケージを使用するユーザは、非完全修飾ドメイン名を入力できません。たとえば、「internalhost」と入力できずに、「internalhost.company.com」と入力する必要があります。

- Android 4.3 への HTC One 上の AT&T ファームウェアのアップデート（ソフトウェア バージョン：3.17.502.3）は、「HTC AnyConnect」をサポートしていません。お客様は「AnyConnect HTC」をアンインストールし、「AnyConnect ICS+」をインストールする必要があります（HTC AnyConnect は、3.22.1540.1 ソフトウェア バージョンのインターナショナル エディションでは機能します）。デバイスのソフトウェア バージョンは、[設定（Settings）]>[端末情報（About）]>[ソフトウェア情報（Software information）]>[ソフトウェア番号（Software number）] で確認します。

- 管理者が Android トンネルの MTU を 1280 以下に設定した場合に VPN 接続が失敗するという Google Issue #70916 が、Android 5.0（Lollipop）で解決されたことをご報告します。次の問題情報は、参考のために提供します。

  Android 4.4.3 でのバグの再発のため（Google Issue #70916、Cisco CSCup24172）、管理者が Android トンネルの MTU を 1280 以下に設定した場合に、VPN 接続が失敗します。この問題はすでに Google に報告されています。Android 4.4.3 で再発したバグを修正するには、新しいバージョンの OS が必要になります。この問題を回避するには、ヘッドエンドの管理者はトンネル MTU を 1280 より小さい値に設定しないようにします。

  問題が発生すると、エンドユーザに「システム設定の設定値を適用できませんでした。（System configuration settings could not be applied.）VPN 接続は確立されません（A VPN connection will not be established）」というメッセージが表示され、AnyConnect デバッグ ログに以下がレポートされます。

```
E/vpnandroid( 2419): IPCInteractionThread: NCSS: General Exception occured, telling client
E/vpnandroid( 2419): java.lang.IllegalStateException: command '181 interface fwmark rule add tun0'
failed with '400 181 Failed to add fwmark rule (No such process)'
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1473)
E/vpnandroid( 2419): at android.os.Parcel.readException(Parcel.java:1419)
E/vpnandroid( 2419): at
com.cisco.android.nchs.aidl.IICSSupportService$Stub$Proxy.establish
(IICSSupportService.java:330)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.VpnBuilderWrapper.establish
(VpnBuilderWrapper.java:137)
E/vpnandroid( 2419): at com.cisco.android.nchs.support.NCSSIPCServer.callServiceMethod
(NCSSIPCServer.java:233)
E/vpnandroid( 2419): at
com.cisco.android.nchs.ipc.IPCInteractionThread.handleClientInteraction
(IPCInteractionThread.java:230)
E/vpnandroid( 2419): at com.cisco.android.nchs.ipc.IPCInteractionThread.run
(IPCInteractionThread.java:90)
E/acvpnagent( 2450): Function: ApplyVpnConfiguration
File: NcssHelper.cpp Line: 740 failed to establish VPN
E/acvpnagent( 2450): Function: PluginResult AndroidSNAKSystem::configDeviceForICS()
File: AndroidSNAKSystem.cpp Line: 665 failed to apply vpn configuration
E/acvpnagent( 2450): Function: virtual PluginResult AndroidSNAKSystem::ApplyConfiguration()
File: AndroidSNAKSystem.cpp Line: 543 Failed to Configure System for VPN.
```

- Android 4.4（KitKat）のバグ Google Issue #61948（AnyConnect ユーザが VPN 接続で大量のパケット損失を経験する/タイムアウトが発生する）が Google の Android 4.4.1 のリリース（Google がソフトウェア アップデートを介して一部のデバイスに配布を開始しました）で解決されたことをご報告します。次の問題情報は、参考のために提供します。

  Android 4.4 のバグ（Issue #61948、Cisco サポートの更新 [英語] も参照してください）が原因で、AnyConnect ユーザは VPN 接続で大量のパケット損失を経験します。これは、Android 4.4 で AnyConnect ICS+ を実行する Google Nexus 5 で確認されています。ユーザは、特定のネットワーク リソースにアクセスしようとすると、タイムアウトを経験します。また、ASA ログには、「大きいパケット 1420 バイト（しきい値 1405 バイト）を送信（Transmitting large packet 1420 (threshold 1405)）」のようなテキストの syslog メッセージが表示されます。

  Google が Android 4.4 用の修正を作成するまで、VPN 管理者は sysopt connection tcpmss <mss size> を設定することにより、ASA 上の TCP 接続のための最大セグメント サイズを一時的に小さくすることができます。このパラメータのデフォルトは 1380 バイトです。ASA ログに表示される値の差に応じてこの値を小さくします。上記の例で

は、差は 15 バイトです。値を 1365 未満にする必要があります。この値を小さくすると、大きなパケットを送信する接続済みの VPN ユーザのパフォーマンスに悪影響を及ぼします。

- AnyConnect for Android で、464xlat と呼ばれる IPv6 移行メカニズムを使用してモバイル ネットワークに接続すると、接続の問題が生じる場合があります。影響を受けることが確認されているデバイスには、T-Mobile US ネットワークに接続している Samsung Galaxy Note III LTE があります。このデバイスは、デフォルトで IPv6 モバイル ネットワーク接続のみを使用します。接続を試行すると、デバイスを再起動するまで、モバイル接続が失われることがあります。

  この問題を防止するには、AnyConnect ICS+ アプリケーションを使用し、IPv4 ネットワーク接続を取得するか、Wi-Fi ネットワークを使用して接続するようにデバイス設定を変更します。T-Mobile USA ネットワークに接続している Samsung Galaxy Note III LTE の場合、T-Mobile によって提供されている手順 [英語] に従って、デバイスのアクセス ポイント名（APN）を設定します（[APN プロトコル（APN Protocol）] が [IPv4] に設定されていることを確認します）。

- VPN 内のプライベート IP アドレスの範囲がクライアント デバイスの外部インターフェイスの範囲とオーバーラップすると、AnyConnect ICS+ パッケージに問題が発生することがあります。このルートのオーバーラップが発生すると、ユーザは VPN に正常に接続できますが、実際には何にもアクセスできません。この問題は、NAT（ネットワーク アドレス変換）を使用し、アドレスを 10.0.0.0 ～ 10.255.255.255 の範囲内に割り当てている携帯電話ネットワークで確認されています。またこの問題は、AnyConnect で Android VPN フレームワークのルート制御が制限されていると発生します。ベンダー固有の Android パッケージに完全なルーティング制御があると、このようなシナリオではより良く機能する場合があります。

- Android 4.0（ICS）を実行する Asus タブレットで、TUN ドライバが失われることがあります。これにより、AVF AnyConnect が失敗します。

- 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。

- Google Isssue 41037 が原因で、クリップボードからテキストを貼り付けるときに、テキストの前にスペースが挿入されます。AnyConnect では、ワンタイム パスワードなどのテキストをコピーする場合は、ユーザがこの不要な空白文字を削除する必要があります。

【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。

この資料の記載内容は2016年5月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

お問い合せ先

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