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

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

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
手動での証明書のインポート
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
証明書の表示，（4 ページ）
証明書の削除，（5 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
証明書の表示，（4 ページ）
証明書の削除，（5 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
サーバ証明書について，（4 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
サーバ証明書について，（4 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。

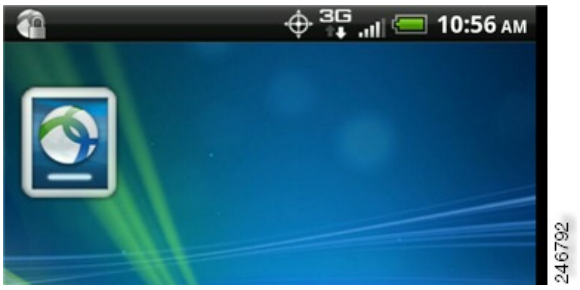
ステップ 2 [Trusted Network Detection] チェックボックスをタップし、このプリファレンスを有効または無効にします。

AnyConnect ウィジェットの使用

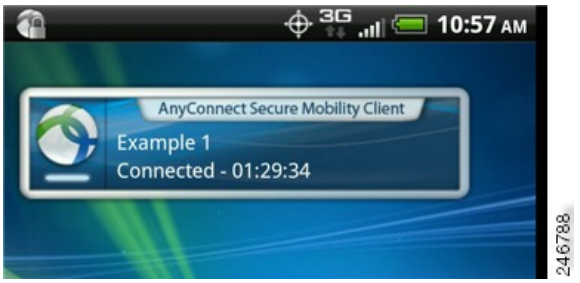
AnyConnect ウィジェットについて

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, （12 ページ）
AnyConnect プロファイルのインポート, （12 ページ）
AnyConnect プロファイルの削除, （13 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，（11 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，（11 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，（11 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。