

# AnyConnect for Androidのマネージド設定

## 内容

AnyConnect for Androidは、MDM/EMMアプリでプロビジョン可能な管理構成をサポートしています。このスキーマはAnyConnectのAPK(res/restrictions.xml)に組み込まれており、Googleの[EMM APIを介して取得できます](#)。スキーマには各フィールドの詳細なドキュメントが含まれ、EMM管理ポータルでレンダリングできるフォームを定義します。

単一のVPN構成エントリのみをプロビジョニングするには、管理者がvpn\_connection\_\*フィールドを使用します。複数のVPN構成をプロビジョニングするために、管理者はvpn\_configuration\_listフィールドを使用できます。このフィールドは、1つ以上のvpn\_configurationエントリを含むBundleArrayです。

一部の管理構成キーは、EMMソフトウェアで入力する必要がある動的トークン化された値に関連付けられています。

### クライアント証明書のプロビジョニング

AnyConnectは、クライアント証明書のEMMプロビジョニングの標準プロセスをサポートします。vpn\_keychain\_cert\_aliasには、証明書のAndroid KeyChainエイリアスを含める必要があります。この値が存在する場合、AnyConnectは[KeyChain.choosePrivateKeyAliasを呼び出](#)して、インポートを開始します（エイリアスがまだインポートされていない場合）。通常、これはユーザーが要求を承認するためのOSプロンプトになります。よりシームレスなユーザーエクスペリエンスを実現するために、EMMアプリは[onChoosePrivateKeyAliasを実装](#)し、ユーザーに対するプロンプトを回避できます。

ほとんどのEMMポータルでは、管理者がvpn\_keychain\_cert\_aliasフィールドに特別なトークン化値を入力できます。EMMアプリが証明書をAndroid KeyChainにインポートすると、特別なトークンの代わりに実際の証明書エイリアスが使用されます。

注：vpn\_keychain\_cert\_aliasの値は、証明書の実際のKeyChainエイリアスと一致している必要があります。それ以外の場合は、証明書がインポートされていないとAnyConnectが認識するため、ユーザーに繰り返しプロンプトが表示されることがあります。

クライアント証明書のEMMプロビジョニングのプロセスを要約するには、次の手順を実行します。

1. EMMアプリは証明書を取得し（SCEP経由など）、Android KeyChainにインポートします。
2. （推奨）EMMアプリケーションはDeviceAdminReceiver.onChoosePrivateKeyAlias()を実装しているため、AnyConnectは証明書を使用するための自動承認を受けます
3. EMMアプリケーションは、インポートされた証明書のキーチェーンエイリアスをAnyConnectの管理構成のvpn\_keychain\_cert\_aliasフィールドに設定します。

### プロビジョニングデバイスID

AnyConnectは、ネットワークアクセス制御または特別なトークン化値フィールドvpn\_connection\_device\_idを使用したレポートに使用できるデバイスIDのEMMプロビジョニングをサポートします。デバイスIDの詳細については、このテクニカルゾーンノート[を参照してください](#)。