CHAPTER 13

モバイル デバイス向け AnyConnect の管理

この章では、デバイス情報、設定情報、サポート情報、Apple iOS および Android デバイス向けの AnyConnect 3.0 に固有の他の管理タスクを提供します。

Apple iOS デバイスの AnyConnect

サポートされる Apple iOS デバイス

デバイス	必要な Apple iOS リリース
iPad 2	6.0 以降
iPad（第 3 世代）	6.0 以降
iPad（第 4 世代）	6.0 以降
iPad mini	6.0 以降
iPhone 3GS	6.0 以降
iPhone 4	6.0 以降
iPhone 4S	6.0 以降
iPhone 5	6.0 以降
iPhone 5C	7.0 以降
iPhone 5S	7.0 以降

デバイス	必要な Apple iOS リリース
iPod Touch（第 4 世代）	6.0 以降
iPod Touch（第 5 世代）	6.0 以降

（注）　AnyConnect は、iPhone 上の場合と同じように iPod Touch 上に表示され、動作します。このデバイスには、『*iPhone User Guide for Cisco AnyConnect Secure Mobility Client*』を使用してください。

Apple iOS デバイスでサポートされている AnyConnect 機能

次の AnyConnect 機能では、Apple iOS 向け AnyConnect 3.0.x でサポートされます。

- トンネル プロトコル
  - Cisco SSL Tunneling Protocol（CSTP）
  - Cisco DTLS Tunneling Protocol（CDTP）
  - IPsec IKEv2
- SSL 暗号スイート
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - RC4-SHA
  - RC4-MD5
  - DES-CBC-SHA
- DTLS の暗号スイート
  - AES256-SHA
  - AES128-SHA
  - DES-CBC3
  - DES-CBC-SHA
- Suite B（IPSec のみ）
- FIPS 140-2 レベル 1
- 認証
- クライアント証明書認証
- 自動再接続（自動再接続プロファイルの指定にかかわらず、ユーザが携帯電話と WiFi ネットワークの間を移動するときに、AnyConnect Mobile は VPN を常に維持する）
- ルーティングポリシー
  - Tunnel All
  - Split Include
  - Split Exclude
- キー再生成

- ネットワーク ローミング
- TLS 圧縮
- Cisco プロファイルのサポート
- プロファイルの更新
- IPv6 over IPv4
- ログイン後バナー
- デッド ピア検出
- トンネル キープアライブ
- バックアップ サーバ リスト
- デフォルト ドメイン
- クラスタのサポート
- DNS サーバ設定
- プライベート側プロキシ サポート
- ネットワーク変更のモニタリング
- 統計情報（Statistics）
- グラフィカル ユーザ インターフェイス
- ログイン前バナー
- Certificate Enrollment Protocol（SCEP）を保護します。
- SCEP プロキシ
- Certificate Management
  - クライアント インターフェイスまたは URI のコマンドを使用して証明書をインポートします。
  - デバイスの証明書をすべて削除します。
- オンデマンド接続（オンデマンドで Apple iOS Connect と互換性がある）
- モバイル ポスチャ
- ローカリゼーション

Apple iOS デバイスの AnyConnect のインストールおよびアップグレード

エンド ユーザは、Apple App Store にアクセスし、アプリケーションをダウンロードすることによって他の iPad、iPhone または iPod touch のアプリケーションなどの Apple iOS デバイス向け AnyConnect セキュア モビリティ クライアントをインストールまたはアップグレードします。AnyConnect クライアント アプリケーションは無料です。詳細なインストール手順については、iPhone または iPad の AnyConnect ユーザ ガイドを参照してください。

Apple iOS デバイスの AnyConnect UI

AnyConnect アプリケーション、ユーザ インターフェイスおよびアプリケーションで実行されたすべてのアクティビティの説明は、iPhone または iPad の AnyConnect ユーザ ガイドを参照してください。

Apple iOS 固有の注意事項

Apple iOS デバイスの AnyConnect をサポートする際には、次の事項に考慮します。

- このマニュアルの SCEP の参照は、Apple iOS SCEP ではなく、AnyConnect SCEP にのみ適用されます。
- Apple iOS に制約があるため、プッシュ電子メール通知は VPN では動作しません。ただし、AnyConnect は、トンネル ポリシーがこれらをセッションから除外する際に、外部にアクセスできる ActiveSync 接続と平行して作動します。

Connect On Demand 機能の使用

Apple iOS Connect On Demand 機能は、ユーザが該当するドメイン リストで指定されたホスト名で任意の宛先にアクセスしようとする場合に VPN 接続を開始します。たとえば、ユーザが internal.example.com に移動し *.example.com が Always Connect リストに存在する場合、デバイスが現在どのネットワーク接続されていても、クライアントは VPN 接続を開始します。

Apple は、iOS 6 の Connect On Demand 機能に Trusted Network Detection（TND）の拡張機能を導入しました。この機能拡張は次のとおりです。

- ユーザが信頼ネットワーク内にいるかどうかを判断して、Connect on Demand 機能を拡張します。
- Wi-Fi 接続だけに適用されます。他のタイプのネットワーク接続に動作している場合、Connect on Demand は、VPN が接続するかどうかを判断するために TND を使用しません。
- 個々の機能はなく、Connect On Demand 機能の外で設定または使用できません。

iOS 6 の Connect on Demand Trusted Network Detection に関する情報は、Apple にお問い合わせください。

（注）　iOS 6 以前のリリースは、信頼ネットワークと非信頼ネットワーク間の識別をサポートしていません。

Connect on Demand の設定に関する注意事項

- 設定された Connect on Demand があるモバイル デバイス用に、証明書ベースの認証トンネル グループに短時間（60 秒）のアイドル タイムアウト（vpn-idle-timeout）が必要です。VPN セッションがアプリケーションにとって重大な問題がなく、常時接続が必要ではない場合は、アイドル タイムアウトを短く設定します。デバイスがスリープ モードに移行するなど必要でなくなった場合、Apple デバイスは VPN 接続を閉じます。トンネル グループのデフォルト アイドル タイムアウトは 60 分です。
- 規則を設定する場合は、[必要に応じて接続（Connect if Needed）] オプションを指定することをお勧めします。Connect if Needed 規則は、内部ホストへの DNS ルックアップに失敗した場合に VPN 接続を開始します。企業内のホスト名が内部 DNS サーバを使用してのみ解決されるよう、正しく DNS を構成する必要があります。
- Apple iOS 7 は、[*常に接続（Always Connect）*] ドメインをサポートしません。Apple iOS 7 デバイスの AnyConnect を実行すると、[*常に接続（Always Connect）*] としてリストアップされているデバイスは、[*必要に応じて接続（Connect if Needed）*] ドメインとして取り扱われます。

詳細な設定手順および機能情報については、「Apple iOS Connect On Demand」を参照してください。

スプリット トンネルによるスプリット DNS 解決の動作

ASA スプリット トンネリング機能では、VPN トンネルにアクセスするトラフィックや、クリア テキストで送信されるトラフィックを指定することができます。スプリット DNS と呼ばれる関連機能は、VPN トンネル上の DNS 解決のために適切な DNS トラフィックや、エンドポイント DNS リゾルバが処理する DNS トラフィックを指定することができます。

Apple iOS 向け AnyConnect は、任意の **split-dns** コマンドをサポートし、解決のために DNS クエリーを指定します。しかし、スプリット トンネル VPN も設定する場合、コマンドは他のデバイスでの働きとは異なる働きをします。

グループ ポリシー コンフィギュレーション モードで入力する **split-dns** コマンドは、VPN セッションを介して解決されるドメインを次のようにリストにまとめます。

```
hostname(config-group-policy)# split-dns {value domain-name1 [domain-name2 ...
domain-nameN] | none}
```

split-dns コマンドがない場合、グループ ポリシーはデフォルトのグループ ポリシー内に存在するスプリット トンネル ドメイン リストを継承します。スプリット トンネリング ドメインのリストの継承を防ぐためには、**split-dns none** コマンドを使用します。

Apple iOS 向け AnyConnect は、このコマンドには次のように応答します:

- **split-dns** リストのドメインに対して、DNS クエリーだけを暗号化します AnyConnect は、コマンドで指定されたドメインの DNS クエリーだけをトンネルし、ローカル DNS リゾルバに他の DNS クエリーすべてをクリア テキストで送信します。たとえば、AnyConnect は次のコマンドに対して example1.com および example2.com の DNS クエリーのみトンネルします。

  ```
  hostname(config-group-policy)# split-dns value example1.com example2.com
  ```

- **default-domain** コマンドのドメインに対して、DNS クエリーだけを暗号化します。**split-dns none** コマンドが存在し、**default-domain** コマンドがドメインを指定する場合、AnyConnect はこのドメインに DNS クエリーだけをトンネルし、他の DNS クエリーすべてをローカル DNS リゾルバにクリア テキストで送信します。たとえば、AnyConnect は次のコマンドに対して example1.com の DNS クエリーのみトンネルします。

  ```
  hostname(config-group-policy)# split-dns none
  hostname(config-group-policy)# default-domain value example1.com
  ```

- すべての DNS クエリーはクリア テキストで送信されます。グループ ポリシーに **split-dns none** と **default-domain none** コマンドが存在する場合、またはこれらコマンドがグループ ポリシーにはないが、デフォルトのグループ ポリシーに存在する場合、AnyConnect は他の DNS クエリーすべてをローカル DNS リゾルバにクリア テキストで送信します。

Apple iPhone Configuration Utility

Apple for Windows または Mac OS X から入手できる iPhone Configuration Utility（IPCU）を使用して、Apple iOS デバイスの設定を作成および展開できます。これは、セキュア ゲートウェイの AnyConnect XML クライアント プロファイル設定の代わりになります。

Apple で制御される既存の IPCU GUI は、AnyConnect IPsec 機能を認識しません。[サーバ（Server）] フィールドで RFC 2996 で定義されている次の URI 構文を使用することで、IPCU の既存 AnyConnect GUI で IPsec VPN 接続を設定します。

```
[ipsec://][<AUTHENTICATION>[":"<IKE-IDENTITY>"@"]] <HOST>[":"<PORT>]["/"<GROUP-URL>]
```

（注） このサーバ フィールドの構文は SSL VPN 接続設定のドキュメント化された使用と下位互換性があります。

パラメータは、ここで説明されたとおりに指定されます。

- **ipsec**：IPSec 接続であることを示します。省略すると、SSL が使用されます。
- **AUTHENTICATION**：IPSec 接続の認証方式を指定します。省略すると、EAP-AnyConnect が使用されます。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **IKE-IDENTITY**：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 にセットされているとき、IKE ID を指定します。このパラメータは、他の認証設定に使用されたときに無効になります。
- **HOST**：サーバ アドレスを指定します。使用するホスト名または IP アドレス。
- **PORT**：現在は無視されています。HTTP URI スキームの一貫性のために含まれています。
- **GROUP-URL**：サーバ名に付加されるトンネル グループ名。

例

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

規格に準拠した Cisco IOS ルータにのみ接続するには、次を使用します。

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

Android デバイスの AnyConnect

サポートされる Android デバイス

シスコは次のメーカーのモバイル デバイスをサポートするため、AnyConnect ブランド固有のアプリケーションを提供します。

- Samsung デバイス
- HTC デバイス
- Kindle デバイス

シスコは、Android デバイスをサポートするために次の AnyConnect アプリケーションを提供します。

- Android 4.0 以降のデバイス（ICS+）用の AnyConnect
- root 化されたデバイス向け AnyConnect

（注）　シスコは、Lenovo および Motorola デバイスのブランド仕様 AnyConnect アプリケーションを提供せず、またサポートもしません。Android バージョン 4.0（Ice Cream Sandwich）以降を実行する Lenovo および Motorola のデバイスは AnyConnect ICS+ アプリケーションを使用できます。AnyConnect 3.0 へアップグレードする前に、古いブランド仕様の AnyConnect パッケージをアンインストールします。

Samsung デバイス

Samsung AnyConnect Release 3.0.x および Samsung AnyConnect レガシー リリース 3.0.x は、次に示す Samsung 製品ラインをサポートします。デバイスは、Samsung から最新のソフトウェア アップデートを実行する必要があります。お使いのデバイスに適用するパッケージを判断するには『*Android 向け AnyConnect ユーザ ガイド*』にあるインストール手順を参照してください。

製品	モデル番号
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

製品	モデル番号
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 S 4	GT-I9500、GT-I9505、SCH-I545、SGH-I337
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。

（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。

HTC デバイス

HTC AnyConnect Release 3.0.x は、http://www.htcpro.com/enterprise/VPN に示された HTC 製品ラインが 3.0 を介して Android リリース 2.1（Honeycomb を介した Eclair）を実行している場合、これらをサポートしています。これらのデバイスは、表に示すような必要とされる最小限のソフトウェアを実行しなくてはなりません [設定（Settings）] > [電話について（About phone）] > [ソフトウェア情報（Software information）] > [ソフトウェア番号（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。

AnyConnect ICS+ Release 3.0.x は、Android 4.0（Ice Cream Sandwich）以降で実行されている、または Android 4.0（Ice Cream Sandwich）以降にアップグレードされている場合、次の HTC デバイスで使用される必要があります。HTC AnyConnect をインストールする間に、HTC デバイスをアップグレードする場合は、HTC AnyConnect アプリケーションをアンインストールしてから、新しい AnyConnect ICS+ アプリケーションをダウンロードする前に、デバイスを再起動します。

- HTC Rhyme S510b
- HTC ADR6330VW
- HTC Vivid
- HTC EVO Design 4G
- HTC ThunderBolt ADR6400L
- HTC Sensation XE
- HTC Sensation
- HTC Amaze 4G
- Beats Audio 対応 HTC Sensation XL
- HTC EVO 3D
- HTC EVO 3D X515m
- HTC X515d
- HTC ADR6425LVW

HTC Holiday としても知られる HTC Raider は、Cisco AnyConnect では作動しません。シスコと HTC は、実行中の Android のリリースに関係なく、HTC AnyConnect アプリケーションがすべての HTC デバイスで実行できるよう、この問題を対処するために作業しています。

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 4.0 以降のデバイス（ICS+）用の AnyConnect

AnyConnect ICS+ Release 3.0.x は、Android 4.0（Ice Cream Sandwich）以降の Android VPN フレームワーク（AVF）でサポートされる VPN 接続を提供します。このパッケージは、ICS 以降を実行しているすべての Android デバイスで使用できます。

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。

（注）　Android 4.0 以降を実行する未サポートのデバイスには、AnyConnect AVF クライアントを推奨します。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 化されたデバイス向け AnyConnect

シスコは、プレビューおよびテストの目的でのみ、Android 2.1 以降を実行する root 化された Android モバイル デバイス向けに Rooted AnyConnect リリース 3.0.x を提供しています。

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。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ルート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。

Android デバイスでサポートされる AnyConnect 機能

Android ブランド固有の AnyConnect

Samsung 用に、HTC と Motorola はデバイスをサポートおよび認定し、シスコは Android オペレーティング システム間でフル機能の VPN エクスペリエンスを提供するブランド固有の AnyConnect パッケージを提供しています。これらのブランド固有の AnyConnect パッケージは、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、これらデバイスに適した AnyConnect クライアントです。

Android AnyConnect Plus

Motorola がサポートおよび認定したデバイス（2012 年 5 月以降にリリース）に関して、シスコはブランド固有のパッケージと機能面において同等であるフル機能 VPN エクスペリエンスをもたらす特定のベンダーに特化しないパッケージを提供しています。

Android VPN フレームワークの AnyConnect

ブランド仕様の AnyConnect パッケージまたは AnyConnect Plus の使用ができないその他の Android デバイスのため、シスコはを使用することなくです。他の Android デバイスにシスコは、Android 4.0（Ice Cream Sandwich）導入された Android VPN Framework（AVF）にサポートされる VPN 接続をもたらす AnyConnect クライアントを提供しています。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、デバイス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。これらの矛盾が表に示されます。Kinde デバイスもこのパッケージを使用しています。

Android をルーツとする AnyConnect

シスコは、ブランド固有パッケージの機能と同等であるルーツ化された Android デバイスに AnyConnect パッケージを提供しています。このパッケージは、Android 2.1 以降を実行するほとんどの root 化されたデバイスで動作します。ブランド仕様の AnyConnect パッケージは、ルーツ化されたデバイスで動作しません。したがって、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。

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネリング	TLS/DTLS	Yes	Yes
	IPsec IKEv2	Yes	Yes
	IKEv2 - NAT-T	Yes	Yes
	IKEv2 - raw ESP	Yes	Yes
	Suite B のサポート	Yes（IPsec のみ）	Yes（IPsec のみ）
	TLS 圧縮	Yes	Yes
	デッド ピア検出	Yes	Yes
	トンネル キープアライブ	Yes	Yes
トンネルの確立	最適ゲートウェイ選択	No	No
	VPN ロード バランシング	Yes	Yes
	バックアップ サーバ リスト	Yes	Yes
	プロファイル インポートの接続をアクティブ化	Yes	Yes
	URI 接続クレデンシャルの事前入力	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネル ポリシー	すべての、または完全なトンネル	Yes	Yes
	スプリット トンネル（スプリットを含む）	Yes	Yes
	ローカル LAN（スプリット を含まない）	Yes	No
	Split-DNS	Yes	スプリットを含んで作動
	常時接続の適用	No	No
	自動再接続	Yes。自動再接続プロファイルの指定にかかわらず、ユーザが 3G と WiFi ネットワークの間を移動するときに、AnyConnect Mobile は VPN を常に維持します。	
	オンデマンド VPN（宛先により起動）	No	No
	オンデマンド VPN（アプリケーションによって起動）	No	No
	Trusted Network Detection（TND）	Yes	No
	キー再生成	Yes	Yes
	ASA グループ プロファイル サポート	Yes、制限されている	Yes、制限されている
	IPv4 パブリック トランスポート	Yes	Yes
	IPv6 パブリック トランスポート	No	No
	IPv4 over IPv4 トンネル	Yes	Yes
	IPv6 over IPv4 トンネル	Yes	Yes
	デフォルト ドメイン	Yes	Yes
	DNS サーバの設定	Yes	Yes
	プライベート側プロキシ サポート	No	No、VPN を確立した場合、WiFi プロキシは無効です。
	ログイン前バナー	Yes	Yes
	ログイン後バナー	Yes	Yes
	スクリプティング	No	No
	VPN の再設定	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
トンネル セキュリティ	ネットワーク変更のモニタリング	Yes	Yes
	シムのインターセプト/フィルタリング	No	No
	組み込みファイアウォール ルール	No	No
	フィルタのサポート（iptables）	Yes	No
認証	手動による証明書のインポート（証明書を取得）	Yes	Yes
	SCEP 登録	Yes	Yes
	SCEP プロキシ	Yes	Yes
	自動証明書選択	Yes	Yes
	手動による証明書の選択	Yes	Yes
	エクスポート不可の証明書	該当なし	該当なし
	スマート カードのサポート	No	No
	ユーザ名およびパスワード	Yes	Yes
	トークン/課題	Yes	Yes
	二重認証	Yes	Yes
	グループ選択	Yes	Yes
	クレデンシャルの事前入力	Yes	Yes
	パスワードの保存	No	No

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
ユーザ インターフェイス	スタンドアロン GUI	Yes	Yes
	ネイティブ OS GUI	No	No
	CLI	No	No
	API	Yes。Java（C++ ではない）	Yes。Java（C++ ではない）
	UI のカスタマイゼーション	Yes（テーマ）	Yes（テーマ）
	UI のローカリゼーション	Yes	Yes
	ユーザ設定	Yes	Yes
	証明書確認の理由	Yes	Yes
	ワンクリック VPN アクセス用のホーム画面のウィジェット	Yes	Yes
	TND で接続が停止した場合の一時停止アイコン	Yes	Yes
	アイドル時の AnyConnect アイコンの非表示	Yes	Yes
	モバイル デバイスの起動	Yes	Yes
	AnyConnect の終了	Yes	Yes
	ユーザ証明書の管理	Yes	Yes
	ユーザ プロファイルの管理	Yes	Yes
	ユーザ ローカリゼーションの管理	Yes	Yes
配備	WebLaunch（ブラウザから開始）	No	No
	アプリケーション ストアへのウェブ リダイレクト	No	No
	スタンドアロン インストーラ	No	No
	OEM によるプレインストール	No	No
	ASA からのインストールまたはアップグレード	No	No
	Android Market からのインストールまたはアップグレード	Yes	Yes
	一部の言語用にパッケージ化されたローカリゼーション	Yes	Yes

表 13-1　AnyConnect Android 機能

AnyConnect 機能	副機能	Android ブランドの仕様、Anyconnect Plus、および root 化された AnyConnect パッケージ	Android VPN フレームワークと Kindle AnyConnect パッケージ
設定	接続中の XML クライアント プロファイルのインポート	Yes	Yes
	XML クライアント プロファイルをインポートするための URI ハンドラ サポート	Yes	Yes
	ユーザ設定の接続エントリ	Yes	Yes
ポスチャ評価	デバイス チェック（ピンのロックや暗号化など）	No	No
	実行中またはインストールされたアプリケーション	No	No
	シリアル番号または固有 ID のチェック	No	No
	モバイル ポスチャ	Yes	Yes
URI の処理	接続エントリの追加	Yes	Yes
	VPN への接続	Yes	Yes
	接続時のクレデンシャルの事前入力	Yes	Yes
	VPN の解除	Yes	Yes
	証明書のインポート	Yes	Yes
	ローカリゼーション データのインポート	Yes	Yes
	XML クライアント プロファイルのインポート	Yes	Yes
	URI コマンドの外部（ユーザ）制御	Yes	Yes
トラブルシューティング	統計情報（Statistics）	Yes	Yes
	ログ	Yes	Yes
	電子メールの統計情報、ログ メッセージおよびシステム情報	Yes	Yes
	シスコへの直接的なフィードバック	Yes	Yes
	DART	No	No
サーティフィケーション	FIPS 140-2 レベル 1	Yes	Yes
	共通の基準	No	No

AnyConnect の Android デバイスへのインストールおよびアップグレード

Android デバイス向け AnyConnect は、Android Market からのみ使用できます。AnyConnect は、ASA からダウンロードできません。Android デバイスの適切な AnyConnect パッケージをダウンロードする手順については、『*Cisco AnyConnect セキュア モビリティ クライアント用 Android ユーザ ガイド*』を参照してください

Android デバイスの AnyConnect UI

AnyConnect アプリケーション、ユーザ インターフェイスとすべてのアクティビティついての説明は、『*Cisco AnyConnect セキュア モビリティ クライアント用 Android ユーザ ガイド*』を参照してください。

Android 固有の考慮事項

Android モバイル ポスチャ デバイスの ID 生成

（注） Android でモバイル ポスチャ デバイス ID を生成するアルゴリズムは、AnyConnect 3.0 で変更されました。AnyConnect の旧バージョンから生成されたデバイス ID を使用する DAP 規則を定義している場合、新しく生成されたデバイス ID にバインドするように更新しなければなりません。

AnyConnect 3.0 はインストール時に一義的な 40 バイトのデバイス ID を生成します。生成されたデバイス ID は、インストール時に使用可能な場合、Android ID と次のいずれかの値、もしくは両方の値に基づいています。

- MEID/IMEI（Mobile Equipment Identifier/International Mobile Equipment Identity）
- MAC-ADDRESS（デバイスの MAC アドレス）

デバイス ID はこれらの値の可用性によって生成されます。

使用可能な値	生成アルゴリズム
両方の値がインストール時に検索可能な場合：	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI + MAC-ADDRESS))`
MEID/IMEI のみインストール時に検索可能な場合：	`device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI))`
MAC-ADDRESS のみインストール時に検索可能な場合	`device-ID = bytesToHexString(SHA1(Android-ID + MAC-ADDRESS))`

ここで、

- Android ID は次のとおり設定されます。

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

- および `bytesToHexString` 機能：

```
String bytesToHexString(byte[] sha1rawbytes)
{
     String hashHex = null;
```

```
        if (sha1rawbytes != null)
        {
            StringBuffer sb = new StringBuffer(sha1rawbytes.length * 2);
            for (int i = 0; i < sha1rawbytes.length; i++)
            {
                String s = Integer.toHexString(0xFF & sha1rawbytes[i]).toUpperCase();
                if (s.length() < 2)
                {
                    sb.append("0");
                }
                sb.append(s);
            }
            hashHex = sb.toString();
        }
        return hashHex;
    }
```

（注）　MEID/IMEI もしくは MAC-ADDRESS 値のいずれかがインストール時に取得可能でない場合、デバイス ID を生成する際に、`Android-ID` と乱数が使用されます。

生成されたデバイス ID は、AnyConnect の **[診断（Diagnostics）] > [ログインとシステム情報（Logging and System Information）] > [システム（System）] > [デバイス識別子（Device Identifiers）]** 画面から、または device_identifiers.txt ファイルの AnyConnect ログから AnyConnect アプリケーションを起動して参照できます。

AnyConnect 2.5 では、MEID/IMEI がデバイス ID として使用されます。MEID/IMEI が使用可能でない場合、AnyConnect は MAC-ADDRESS を使用しようとします。この値も使用可能でない場合、AnyConnect インストールは失敗します。

AnyConnect の動作およびオプション

VPN 接続

VPN 接続を開始するには、ユーザがセキュア ゲートウェイのサーバ アドレスを識別するモバイル デバイスの接続エントリ、または他の接続属性を選択します。サーバ アドレスは、必要に応じてトンネル グループ URL を含めるセキュア ゲートウェイの完全修飾ドメイン名または IP アドレスです。AnyConnect は、モバイル デバイス アドレスの異なるセキュア ゲートウェイまたは VPN トンネル グループの複数の接続エントリをサポートします。複数の接続エントリが設定されている場合は、VPN 接続を開始するためにユーザがどれを使用するかを理解することが重要です。接続エントリは次の方法のいずれかで設定されます。

- ユーザが手動で設定します。

  モバイル デバイスの接続エントリを設定する手順については、適切なユーザ ガイドを参照してください。

- Anyconnect VPN クライアント プロファイルで定義されます。

  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 接続エントリを識別します。各接続エントリは、このエンドポイント デバイスに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。詳細については、「AnyConnect プロファイル設定でモバイル デバイス接続の設定」セクションおよび「AnyConnect プロファイルの展開」セクションを参照してください。

- ユーザが管理者により提供されたリンクをクリックした後で追加し、接続エントリを設定します。

  ユーザに対するこの種の接続エントリの設定の提供は、「URI ハンドラを使用した VPN 接続エントリの生成」を参照してください。

VPN 接続を完了するには、ユーザはユーザ名とパスワード、もしくはデジタル証明書、またはその両方の形式でクレデンシャルを提供して認証する必要があります。管理者は、トンネル グループの認証方式を定義します。

モバイル デバイスの最高のユーザ エクスペリエンスのために、認証設定による複数の AnyConnect 接続プロファイルを使用することを推奨します。ユーザ エクスペリエンスとセキュリティのバランスを最適に保つ方法を決める必要があります。

- モバイル デバイスの AAA 対応認証トンネル グループについては、クライアントを再接続状態にし、ユーザが再認証しなくても済むよう、トンネル グループは 24 時間など非常に長時間のアイドル タイムアウトが必要になります。
- 最もトランスペアレントなユーザ エクスペリエンスを達成するには、証明書のみの認証を使用します。デジタル証明書を使用すると、VPN 接続は、ユーザとの対話なしで確立されます。

クライアント証明書

証明書を使用してセキュア ゲートウェイにモバイル デバイスを認証するため、エンド ユーザは、デバイスに証明書をインポートする必要があります。この証明書は自動証明書選択のために使用可能であり、また特定の接続エントリに手動で関連づけることができます。証明書は、次の方法を使用してインポートされます。

- ユーザが管理者により提供されたリンクをクリックした後で追加し、証明書をインポートします。ユーザにこの種の証明書を提供するため証明書をインポートするために、URI ハンドラを使用を参照します。
- SCEP の使用 管理者用の設定は、『*Cisco AnyConnect Secure Mobility Client 管理者ガイド リリース 3.0*』の「VPN アクセスの設定」の章の「SCEP を使用して証明書登録を設定する」を参照してください。
- ユーザが手動でインポートします。モバイル デバイスに証明書をインポートするために適切なユーザ ガイドを参照してください。

サーバ証明書

セキュア ゲートウェイで設定される有効で信頼できるサーバの証明書は、ユーザに簡単で安全な VPN 接続を提供します。

モバイル デバイスの AnyConnect は、セキュア ゲートウェイによって提示された証明書が無効または信頼できない、もしくはその両方の場合、VPN 接続をブロックすることでセキュア ゲートウェイにアクセスする際に、改善されたセキュリティ保護を提供します。

新しい [信頼できないサーバのブロッキング（Block Untrusted Servers）] アプリケーション設定は、セキュア ゲートウェイを識別できない場合、AnyConnect が接続をどのようにブロックするか決定します。この保護はデフォルトでは ON です。ユーザが 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デジタル証明書を使用してそのアイデンティティを確認します。証明書が無効な場合（期限切れか無効な日付、不正なキーの用途、名前の不一致により証明書エラーがある）、または信頼できない場合（認証局が確認できない）場合、接続はブロックされます。ブロッキング メッセージが表示されるため、ユーザは処理を選択する必要があります。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] が ON の場合、ブロッキング**信頼できない VPN サーバ**の通知は、ユーザにセキュリティ上の脅威を警告します。ユーザは以下を選択できます。

- [安全にしておく（Keep Me Safe）] を選択して、この接続を終らせ、安全にしておきます。
- [信頼できないサーバのブロッキング（Block Untrusted Servers）] アプリケーションを OFF に**設定変更**します。ただし、これは推奨されません。ユーザがこのセキュリティ保護を無効にすると、VPN 接続を再起動しなくてはなりません。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] が OFF の場合、ブロックされていない**信頼できない VPN サーバ**の通知は、ユーザにセキュリティ上の脅威を警告します。ユーザは以下を選択できます。

- **接続をキャンセルし、**安全にしておきます。
- **接続を続行**します。ただし、これは推奨されません。
- **証明書の詳細を表示します。**

  ユーザが確認している証明書が有効であるが信頼できない場合、ユーザは次のことを実行できます。

  - 再使用できるようにサーバ証明書を AnyConnect 証明書ストアにインポートし、[インポートおよび継続（Import and Continue）] を選択して接続を継続します。AnyConnect ストアにこの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してい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。
  - 前の画面に戻り [キャンセル（Cancel）] または [続行（Continue）] を選択します。

  証明書が無効な場合、または何らかの理由で、ユーザが前の画面にだけ戻ることができる場合 [キャンセル（Cancel）] または [続行（Continue）] を選択します。

[信頼できないサーバのブロッキング（Block Untrusted Servers）] の設定を ON のままにし、自身のセキュア ゲートウェイで設定された有効で信頼できるサーバ証明書を持ち、モバイル ユーザを常に [安全にしておく（Keep Me Safe）] を選択させておくことが、ネットワークの VPN 接続の最も安全な設定です。

AnyConnect プロファイルの展開

モバイル デバイスの接続エントリがある VPN クライアント プロファイルを作成した後、管理者は次のいずれかの方法でクライアント プロファイルを配布する方法を選択する必要があります。

- VPN 接続のモバイル デバイス設定にクライアント プロファイルをアップロードして ASA を設定します。

  クライアント プロファイルを ASA にインポートし、グループ ポリシーと関連付ける方法については、『*Cisco AnyConnect Secure Mobility Client 管理者ガイド*』の「VPN アクセスの設定」の章の「AnyConnect プロファイルの展開」を参照してください。

- クライアント プロファイルをインポートするために、ユーザに AnyConnect URI リンクを提供します。

  詳細については、「VPN クライアント プロファイルをインポートするために URI ハンドラを使用」セクションを参照してください。

- モバイル デバイスのプロファイル管理を使用して AnyConnect プロファイルをインポートします。

  デバイス固有の手順については、該当するモバイル デバイスのユーザ ガイドを参照してください。

管理者がこれらのプロファイルを作成して配布した場合、エンド ユーザは、定義された接続エントリを変更できません。エンド ユーザは、手動で作成する接続エントリだけを変更できます。

AnyConnect は、モバイル 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。

- ユーザは手動でプロファイルをインポートします。インポートされたプロファイルは、現在のプロファイルに置き換えられます。
- 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によって置き換えられます。
- ユーザは手動で現在のプロファイルを削除します。現在のプロファイルが削除されると、削除されたプロファイルに定義されているすべての接続エントリが削除されます。

AnyConnect プロファイル設定でモバイル デバイス接続の設定

ステップ 1　次の点を考慮するデスクトップおよびモバイル エンドポイントに共通の設定手順については、VPN アクセスの設定 を参照してください:

プロファイル属性	例外
自動再接続	自動再接続仕様にかかわらず、AnyConnect Mobile は常に ReconnectAfterResume を試行します。

ステップ 2　この章で説明されているモバイル仕様の属性を設定します。

AnyConnect プロファイル エディタのダウンロード

モバイル デバイスのホスト接続エントリを含む VPN クライアント プロファイルを作成するには、AnyConnect プロファイル エディタ リリース 3.0.1047 以降を使用します。プロファイル エディタはスタンドアロン ツールです。次の方法でプロファイル エディタをダウンロードします。

ステップ 1　www.cisco.com の [AnyConnect セキュア モビリティ クライアント（AnyConnect Secure Mobility Client）] ページにアクセスし、[ソフトウェアをダウンロード（Download Software）] をクリックします。

ステップ 2　[リリースすべてと 3.0（All Releases and 3.0）] ディレクトリを展開し、AnyConnect の **3.0.1047** 以降を選択します。

ステップ 3　右のカラムで、命名規則の **anyconnect-profileeditor-win-<*version*>-k9.exe** でファイルを検索します。AnyConnect 3.0.1047 でリリースされた AnyConnect プロファイル エディタをダウンロードしていた場合、**anyconnect-profileeditor-win-3.0.1047-k9.exe** が見つかります。

ステップ 4　[今すぐダウンロード（Download now）] をクリックし、サイトの手順に従ってダウンロード プロセスを完了します。

Mobile-Specific の属性

証明書認証

接続エントリと関連する**証明書の認証**ポリシー属性が、この接続に証明書をどのように処理するかを指定します。有効な値は、自動、手動、または無効化です。

- **自動**：AnyConnect は、接続がいつなされるかを認証するクライアント証明書を自動で選択します。この場合、インストールされているすべての証明書が確認されて期限切れの証明書が無視され、VPN クライアント プロファイルに定義された基準に一致する証明書が適用されます。次に、基準に一致する証明書を使用して認証されます。これは、ユーザが VPN 接続の確立を試行するたびに実行されます。
- **手動**：AnyConnect は、プロファイルがダウンロードされ、次のいずれかを行うときに、Android デバイスの AnyConnect 証明書ストアで証明書を検索します。
  - AnyConnect は、VPN クライアント プロファイルで定められる基準に一致している証明書に基づく証明書を見つけた場合、証明書を接続エントリに割り当て、接続が確立されたときにその証明書を使用します。
  - 一致する証明書が見つからない場合、証明書認証ポリシーが自動に設定されます。

  割り当てられた証明書が、何らかの理由で AnyConnect 証明書ストアから削除された場合、AnyConnect は自動に証明書認証ポリシーをリセットします。
- **無効**：クライアント証明書は認証に使用されません。

インポートでのアクティブ化

インポートでのアクティブ化、または**プロファイルがインポートされたときにサーバ リスト エントリをアクティブ化は、VPN 接続がデバイスにダウンロードされると、**サーバ リスト エントリをデフォルトとして定義します。この宛先を設定できるのは、1 つのサーバ リスト エントリのみです。デフォルトでは、無効に設定されています。

Apple iOS ネットワーク ローミング

この属性は、Apple iOS デバイスの接続にだけ適用されます。

[ネットワーク ローミング（Network Roaming）]、または[3G/Wifi ネットワーク間でのローミング時に再接続（Reconnect when roaming between 3G/Wifi networks）]は、デフォルトで有効です。無効の場合、AnyConnect は、接続が切断された後やデバイスが起動した後、もしくは接続種別（EDGE（2G）、1xRTT（2G）、3G または Wi-Fi など）が変更になった後で、再接続にかかる時間を制限しません。

この機能により、ネットワークにおいて揺ぎない安全な接続で、シームレスなモビリティを提供します。エンタープライズとの接続を必要としますが、より良いバッテリ寿命によりアプリケーションには有用です。

[ネットワーク ローミング（Network Roaming）] が無効で、AnyConnect の接続が切断された場合、必要に応じて最大 20 秒まで再接続を試みます。接続できない場合は、ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

（注） ネットワーク ローミングは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響*しません*。

Apple iOS Connect On Demand

この属性は、Apple iOS デバイスの接続にだけ適用されます。

Apple iOS Connect On Demand 機能を使用すると、Safari などのアプリケーションで VPN 接続を開始できます。Apple iOS は、アプリケーションが要求したドメインを、*アクティブ*な接続エントリ（横にチェック マークが付いているエントリ）のドメイン リスト内の文字列に対して評価します。

iOS の Connect on Demand 経由で VPN 接続が開始されると、iOS は、トンネルが一定の期間非アクティブである（トンネルを通過するトラフィックがない）場合、そのトンネルを切断します。詳細については、Apple の『VPN On Demand』のマニュアルを参照してください。

Apple iOS を評価するドメイン リストを定義します。

- [接続しない（Never Connect）] : Apple iOS は最初に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS はドメイン要求を無視します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は `www.example.com` などのように指定します。

（注）　Connect On Demand を有効化すると、AnyConnect によって VPN 設定内のサーバ アドレスが Never Connect リストに追加され、ブラウザを使用してセキュア ゲートウェイに接続したときに VPN 接続が開始されなくなります。この規則をそのままにしておいても、Connect on Demand に悪影響はありません。

- [常に接続（Always Connect）] : Apple iOS は次に、ドメイン要求をこのリストの内容に対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。このリストの最も一般的な用途は、内部リソースへの短時間のアクセス権を取得することです。値は `email.example.com` などのように指定します。

（注）　Apple iOS 7 は、[*常に接続（Always Connect）*] ドメインをサポートしません。Apple iOS 7 デバイスの AnyConnect を実行すると、[*常に接続（Always Connect）*] としてリストアップされているデバイスは、[*必要に応じて接続（Connect if Needed）*] ドメインとして取り扱われます。

- [必要に応じて接続（Connect if Needed）] : Apple iOS は、DNS エラーが発生した場合に、ドメイン要求をこのリストに対して評価し、一致するものを探します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

Apple iOS は、次のすべての条件が満たされた場合にのみ、アプリケーションに代わって VPN 接続を確立します。

- VPN 接続がまだ確立されていない。
- Apple iOS Connect on Demand フレームワークに対応するアプリケーションがドメインを要求している。
- 接続エントリが有効な証明書を使用するように設定されている。
- 接続エントリで Connect on Demand が有効化されている。
- Apple iOS が、[接続しない（Never Connect）] リスト内の文字列とドメイン要求の照合に失敗する。
- 次のどちらかの条件を満たしている。

- Apple iOS で、[常に接続（Always Connect）] リスト内にドメイン要求と一致する文字列を見つけている。
- DNS ルックアップが失敗し、Apple iOS で、Connect if Needed リスト内にドメイン要求と一致する文字列を見つけている。

Connect On Demand のルールは、ドメイン名だけをサポートし、IP アドレスをサポートしません。しかし、ルール内で指定されたドメイン名は部分的または全体のドメイン文字列である場合があります。

（注） 統合された Apple iOS IPsec クライアントと AnyConnect は、Demand フレームワークで同じ Apple iOS VPN を使用します。

詳細については、iPad または iPhone ユーザ ガイドの「Connect-On-Demand ルールの設定」または、このマニュアルで後ほど説明する「URI ハンドラを使用した VPN 接続エントリの生成」を参照ください。

モバイル固有属性の設定

ステップ 1　VPN クライアント プロファイルで、[サーバ リスト（Server List）] を選択します。

ステップ 2　リストに新しいサーバ エントリを追加するには、[追加（Add）] を選択するか、リストからサーバ エントリを選択し、サーバ リストの [エントリ（Entry）] ダイアログボックスを開くには、[編集（Edit）] をクリックします。

ステップ 3　[サーバ リスト エントリ（Server List Entry）] ダイアログボックスで、[追加のモバイル専用設定（Additional mobile-only settings）] をオンにして [編集（Edit）] をクリックします。

ステップ 4　[Apple iOS / Android の設定（Apple iOS / Android Settings）] エリアでは、Apple iOS または Android オペレーティング システムを実行するデバイスに、次の属性を設定します。

a.　**証明書認証**タイプの選択：**自動**、**手動**または**無効化**。

b.　必要に応じて、[プロファイルがインポートされた場合、このサーバ リスト エントリをアクティブにする（Make this Server List Entry active when profile is imported）] チェックボックスをオンまたはオフにします。

ステップ 5　[Apple iOS のみの設定（Apple iOS Only Settings）] エリアでは、Apple iOS オペレーティング システムのみを実行するデバイスに、次の属性を設定します。

a.　必要に応じて、[3G/Wifi ネットワーク間でローミングされた場合は再接続（Reconnect when roaming between 3G/Wifi networks）] チェックボックスをオンまたはオフにします。

b.　必要に応じて、[要求に応じて接続（Connect on Demand）] チェックボックスをオンまたはオフにします。

[要求に応じて接続（Connect on Demand）] は、[証明書認証（Certificate Authentication）] フィールドが**手動**または**自動**に設定されている場合に有効です。[証明書の認証（Certificate Authentication）] フィールドが [無効（Disabled）] に設定されている場合は、このチェックボックスはグレー表示されます。[ドメインまたはホストと一致（Match Domain or Host）] フィールドおよび [オンデマンド アクション（On Demand Action）] フィールドで定義される Connect on Demand ルールは、チェックボックスがグレー表示されている場合でも、設定および保存できます。

Connect On Demand がイネーブルの場合、アプリケーションは自動的にこのリストにサーバ アドレスを追加します。これにより、Web ブラウザを使用してサーバのクライアントレス ポータルへのアクセスを試行する場合は、VPN 接続が自動的に確立されなくなります。この動作が望ましくない場合にはこのルールを削除します。

c. [ドメインまたはホストと一致（Match Domain or Host）] フィールドに、Connect on Demand ルールを作成する対象のホスト名（host.example.com）、ドメイン名（.example.com）、または部分ドメイン（.internal.example.com）を入力します。このフィールドには、IP アドレス（10.125.84.1）を入力しないでください。

d. [オンデマンド アクション（On Demand Action）] フィールドで、ユーザが前述の手順で定義されたドメインまたはホストに接続しようと試みる場合、次のアクションから 1 つ指定します：[常に接続（Always connect）]、[必要に応じて接続（Connect if needed）]、または [接続しない（Never connect）]。

e. [追加（Add）] をクリックします。

このルールが、下部のルール リストに表示されます。

ステップ 6　[**OK**] をクリックします。

推奨する ASA 設定

ステップ 1　次の例外を考慮するデスクトップおよびモバイル エンドポイントに共通する設定手順については、『*Cisco ASA Series VPN ASDM Configuration Guide*』の「General VPN Setup」を参照してください。

属性	ASDM ロケーション	例外
ホーム ページ URL	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network（Client）Access）] > [グループ ポリシー（Group Policies）] > [追加または編集（Add or Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタマイゼーション（Customization）]。	AnyConnect Mobile は、ホーム ページ URL 設定を無視します。認証の成功後に、モバイル クライアントをリダイレクトすることはできません。
AnyConnect 接続プロファイル名およびエイリアス	[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加（Add）]	AnyConnect モバイル クライアント接続に使用するトンネル グループ（接続プロファイル）の [名前（Name）] または [エイリアス（Aliases）] フィールドに特殊文字を使用しないでください。特殊文字の使用により、ゲートウェイからの応答処理ができないことにより、「接続に失敗しました（Connect attempt）」というエラー メッセージがログイン後に表示される原因になります。

ステップ 2　この章で説明したとおり、次の属性を設定します。

デッド ピア検出の設定

サーバ側のデッド ピア検出機能デバイスは、スリープ状態になることを防ぐため、オフになります。ただし、ネットワーク接続性の欠如によりトンネルが終了するときに、または、VPN 接続でトラフィックを送信し続けるには送信品質が非常に低下しているか、不可能かをクライアントが判断するため、クライアント側のデッド ピア検出は、オンになっている必要があります。

キープアライブ メッセージの無効化

クライアント側のデッド ピア検出がすでにイネーブルになっている場合、モバイル デバイスのバッテリ寿命を延ばすため、キープアライブ メッセージをディセーブルにすることをお勧めします。Keepalive Messages パラメータにアクセスするには、ASDM を使用して [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [追加（Add）] または [編集（Edit）] > [詳細（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] に移動します。

モバイル ポスチャの設定

Release 8.2（5+）および 8.4（2）を実行する ASA は、モバイル デバイスを検出する AnyConnect モバイル ポスチャを特徴としています。モバイル ポスチャにより、モバイル接続の受け入れ、拒否、または制限をできます。AnyConnect Premium と AnyConnect モバイル ライセンスが必要です。

モバイル デバイスの次の属性に基づいて、ダイナミック アクセス ポリシー（DAP）を設定します。

- クライアントのバージョン：AnyConnect クライアントのバージョン。
- プラットフォーム：Android および Apple iOS を含むオペレーティング システム。
- Platform Version：オペレーティング システム バージョン番号
- Device Type：iPad または Samsung GT-I9000 などのモバイル デバイス タイプ。
- Device Unique ID：モバイル デバイスの一意の ID Android プラットフォームのデバイス ID に関する重要な情報については、「Android モバイル ポスチャ デバイスの ID 生成」を参照してください。

詳細な手順については、「Cisco 5500 Series Configuration Guide using ASDM, 6.4」の「Adding Mobile Posture Attributes to a DAP」セクション、もしくは「Cisco Security Appliance Configuration Guide using ASDM, 6.2」の「Add/Edit Endpoint Attributes」セクションを参照ください。

VPN 接続の確立からモバイル デバイスの制限

AnyConnect Mobile ライセンスが ASA で動作しない場合は、自動的にモバイル デバイスからの接続要求を拒否します。

AnyConnect Mobile ライセンスでアクティブ化される ASA は、モバイル デバイス VPN 接続をサポートします。デフォルトでは、認証したユーザは AnyConnect が作動するモバイル デバイスからログインできます。

これらの接続を防ぐため、ASA を設定します。設定は ASA リリースによって異なります。

- Release 8.2（5+）および 8.4（2）を実行する ASA は、モバイル デバイスを検出する AnyConnect モバイル ポスチャを特徴としています。
- 以前のリリース、ASA リリース 8.0（4）から 8.2（4）、そして 8.4（1）では、異なる DAP の仕様、Cisco Secure Desktop、AnyConnect Premium ライセンスが必要です。

VPN モバイル デバイス接続を防ぐために ASA を設定するため、次のようにダイナミック アクセス ポリシーを追加します。

モバイル ポスチャを使用するための手順

ステップ 1　ASA で ASDM セッションを確立します。

ステップ 2　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

ステップ 3　エンドポイント属性テーブルの右側にある [追加（Add）] を選択します。

ステップ 4　エンドポイント属性タイプを **AnyConnect** に変更します。

ステップ 5　プラットフォームを **Android** または **Apple iOS** に変更します。

ステップ 6　[デバイス種別（Device Type）] フィールドにモデル名を入力します。

ASDM がデバイス種別の横にあるドロップダウン リストに表示されます。しかし、ドロップダウン オプションはサポートされていません。

ステップ 7　各デバイス用にエンドポイント属性 1 つを DAP 追加し、ポリシーをこれに割り当てます。

ステップ 8　[追加（Add）]、[編集（Edit）]、[ダイナミック アクセス ポリシー（Dynamic Access Policies）] ウィンドウのアクセス/認証ポリシー属性セクションのタブを使用して、Android 接続の制限の継続、終了、再接続をします。

以前の ASA リリースの手順

ステップ 1　ASA で ASDM セッションを確立します。

ステップ 2　[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] を選択します。

ステップ 3　ポリシーに名前をつけます（例：`Apple iOS の拒否 や Android の拒否など`）。

ステップ 4　[詳細（Advanced）] をクリックします。

ステップ 5　[論理式（Expressions）] テキスト ボックスに次のいずれかを入力します。

```
EVAL(endpoint.os.version, "EQ", "Apple Plugin", "string")
```

または

```
EVAL(endpoint.os.version, "EQ", "Android", "string")
```

ステップ 6　[追加（Add）]、[編集（Edit）]、[ダイナミック アクセス ポリシー（Dynamic Access Policies）] ウィンドウのアクセス/認証ポリシー属性セクションのタブを使用して、Android 接続の制限の継続、終了、再接続をします。

ステップ 7　[OK] および [適用（Apply）] をクリックします。

FIPS および Suite B の暗号化

モバイル デバイス向け AnyConnect 3.0 は、Cisco Common Cryptographic Module（C3M）が組み込まれています。これは、新世代の暗号化（NGE）アルゴリズムの一部として FIPS 140-2 に準拠した暗号化モジュールや NSA Suite B 暗号化が含まる Cisco SSL の実装です。

モバイル デバイス向け AnyConnect 3.0 では、Suite B の暗号化は、IPSec VPN でだけ使用可能です。FIPS 準拠の暗号化は、IPSec および SSL VPN で利用可能です。

暗号化アルゴリズムを使用すると、接続の間、ヘッドエンド ルータとネゴシエートされます。ネゴシエーションは、VPN 接続の両端の機能によって異なります。したがって、セキュア ゲートウェイは、FIPS に準拠する暗号化および Suite B の暗号化をサポートする必要があります。

ユーザは、AnyConnect 設定の **FIPS モード**を無効にすることで、ネゴシエーションにおいて NGE アルゴリズムだけを受け入れるように AnyConnect を設定します。FIPS モードが無効の場合、AnyConnect は VPN 接続の非 FIPS 暗号アルゴリズムも受け入れます。

モバイル デバイス向け AnyConnect 3.0 には、次の Suite B のアルゴリズムが含まれます。

- 対称暗号化と整合性のための AES-GCM サポート（128、192、256 ビット キー）
  - IKEv2 ペイロード暗号化および認証（AES-GCM のみ）
  - ESP パケット暗号化および認証
- ハッシュ用の SHA-2（256/384/512 ビットの SHA）サポート
  - IKEv2 認証ペイロード
  - ESP パケット認証
- キー交換向けの ECDH サポート
  - グループ 19、20、および 21 の IKEv2 キー交換および IKEv2 PFS
- デジタル署名、非対称暗号化、および認証用の ECDSA サポート（256、384、512 ビット楕円曲線）
  - IKEv2 ユーザ認証およびサーバ証明書の確認
- アルゴリズム間の他の暗号スイートの依存関係は、次のサポートを促進します。
  - IKEv2 用の Diffie-Hellman Groups 14 および 24
  - DTLS および IKEv2 用の 4096 ビット キーを使用する RSA 証明書

要件

- FIPS または Suite B のサポートは、セキュア ゲートウェイで必要です。シスコは、ASA バージョン 9.0 以降での Suite B 機能、および ASA バージョン 8.4.1 以降の FIPS 機能を提供します。
- ASA への FIPS または Suite B リモート アクセス接続には、AnyConnect Premium のライセンスが必要です。

（注）
- モバイル向け AnyConnect 3.0 のリリース時に、Apple iOS は ECDSA の証明書をサポートしていません。この問題は、Apple によって対処されます。固定されると、次の要件が適用されます。

  Apple iOS 5.0 以降は Suite B の暗号化に必要です。これは Suite B で使用される ECDSA の証明書をサポートする Apple iOS の最も低いバージョンです。

- Android 4.0（Ice Cream Sandwich）以降は、Suite B の暗号化に必要です。これは、SuiteB で使用される ECDSA の証明書をサポートする Android の最も低いバージョンです。
- VPN 接続には、デジタル署名の Key Usage 属性とキー暗号化、さらにはサーバ認証の Enhanced Key Usage 属性または IPsec の IKE 中間を含むサーバ証明書が必要です。キーの用途を含まないサーバ証明書では、すべてのキーの用途が無効と見なされます。同様に、キーの拡張用途を含まないサーバ証明書は、すべてのキーの拡張用途が無効と見なされます。

注意事項と制約事項

- Suite B は IKEv2/IPsec でのみ利用できます。
- FIPS モードで動作しているデバイスは、デジタル証明書、プロキシ方式または従来の方法をモバイル ユーザに提供するために、SCEP 使用との互換性はありません。したがって適切に計画を立てましょう。
- SHA-2 を使用して署名された証明書を検証する際、EAP 方式は、TLS ベースの EAP を除き SHA-2 をサポートしません。
- ECDSA 証明書には、カーブ強度以上のダイジェスト強度がなければなりません。たとえば、EC-384 キーは SHA2-384 以上を使用しなければなりません。
- VPN 接続は、サーバ証明書で名前の検証を実行します。名前検証では、次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name のみを使用します。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あるけれども関連する属性を含んでいない場合、名前検証は、証明書の Subject で見つかった　Common Name 属性を使用します。
  - 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、サブドメインの最後（右端）の文字でなければなりません。この規則に準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

AnyConnect インターフェイスおよびメッセージのローカライズ

リリース 2.5 から、Android および Apple iOS 用 AnyConnect セキュア モビリティ クライアントは、ローカリゼーションをサポートし、AnyConnect ユーザ インターフェイスやメッセージをユーザのロケールに適用しています。

パッケージ化されたローカリゼーション

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）

AnyConnect のインストール時には、これらの言語のローカリゼーション データがモバイル デバイスにインストールされます。モバイル デバイスで指定されたロケールにより、表示される言語が決定します。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。

ダウンロードされたローカリゼーション

AnyConnect パッケージではない言語に関して、管理者は、AnyConnect VPN 接続のデバイスにダウンロードされる ASA にローカライズ データを追加します。ASA のローカリゼーション設定については、Localizing the AnyConnect GUI を参照ください。ASA がデバイスのロケールにローカリゼーション データを含めない場合、AnyConnect アプリケーション パッケージにプリインストールされたローカリゼーション データを引き続き使用します。

シスコでは、ローカライズ可能な AnyConnect 文字列をすべて含む anyconnect.po ファイルを Cisco.com の製品ダウンロード センターで提供しています。AnyConnect 管理者は、anyconnect.po ファイルをダウンロードし、使用可能な文字列を翻訳してから、ASA にファイルをアップロードします。AnyConnect 管理者は、anyconnect.po ファイルを ASA にインストールしたあと、この更新バージョンをダウンロードしてください。

最初に AnyConnect ユーザ インターフェイスおよびメッセージがインストールした言語でユーザに表示されます。エンド ユーザが ASA への初めての接続を確立すると、AnyConnect では、デバイスの優先言語が比較され、ASA でのローカリゼーション言語が使用可能になります。一致するローカリゼーション ファイルが検索されると、ローカライズされたファイルがダウンロードされます。ダウンロードが完了すると、AnyConnect は anyconnect.po ファイルに追加された変換文字列を使用してユーザ インターフェイスおよびユーザ メッセージを表示します。文字列が翻訳されていない場合、AnyConnect ではデフォルトの英語文字列が表示されます。

ASA がデバイスのロケールにローカリゼーション データを含めない場合、使用している AnyConnect アプリケーション パッケージからインストール済みのローカリゼーション データを含めます。

手順

ステップ 1　[製品を選択（Select a Product）] ページから開始します。

ステップ 2　[製品（Products）] > [セキュリティ（Security）] > [仮想プライベート ネットワーク（VPN）（Virtual Private Networks (VPN)）] > [シスコ VPN クライアント（Cisco VPN Clients）] > [シスコ AnyConnect セキュア モビリティ クライアント（Cisco AnyConnect Secure Mobility Client）] を選択します。

ステップ 3　リリースのフォルダ ツリーの**すべてのリリース** フォルダを展開し、**3.0** を展開します。そして、最新の AnyConnect 3.0 リリースを開きます。

ステップ 4　ダウンロード可能なファイルのリストから、**anyconnect.po** を探し、[今すぐダウンロード（Download Now）] をクリックします。

ステップ 5　ファイルをダウンロードするプロンプトに従います。

追加のローカリゼーション

管理者にとって、ユーザのデバイスにローカリゼーション データを取得する追加の方法は、ローカリゼーション データをインポートするために、AnyConnect URI をユーザに提供することです。次に例を示します。

```
anyconnect://import?type=localization&host=asa.example.com&lang=ja-jp
```

詳細については、URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズを参照してください。

ユーザ ローカリゼーションの管理

モバイル デバイスのユーザは、自身のデバイスでローカリゼーションのデータを管理します。次のローカリゼーション アクティビティを実行する手順については、適切なユーザ ガイドを参照してください。

- 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。ユーザは、ローカリゼーション データのインポートを選択し、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、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。
- デフォルトのローカリゼーション データのリストア。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。

URI ハンドラを使用した AnyConnect アクションの自動化

AnyConnect の URI ハンドラは、他のアプリケーションに Universal Resource Identifiers（URI）形式で AnyConnect に対してアクション要求を割り当てさせます。AnyConnect ユーザ設定プロセスを簡素化するため、URI を Web ページまたは電子メール メッセージにリンクとして埋め込み、これらにアクセスする方法をユーザに提供します。URI では、次を実行できます

- VPN 接続エントリを生成します。
- VPN への接続を確立し、VPN の接続を解除します。
- ローカリゼーション ファイル、証明書および AnyConnect プロファイルをインポートします。

AnyConnect アプリケーションで処理する URI はデフォルトで無効です。モバイル デバイスのユーザは、AnyConnect Application Preference External Control を有効もしくはプロンプトに設定することで、この機能を使用できます。外部制御を有効にすると、ユーザとの対話なしですべての URI コマンドを割り当てることができます。

ユーザは、URI のアクティビティの通知がされ、[プロンプト（Prompt）] を選択することによって、要求時に許可または不許可されます。これらを使用する場合、URI の処理に関連付けられたプロンプトに応答する方法をユーザに通知する必要があります。

URI ハンドラ パラメータ値を入力する場合、URL エンコードを使用する必要があります。アクション要求を符号化するために、リンクでこのようなツールを使用します。

（注） Android ユーザは、Web ブラウザのアドレス バーにこれらの URI を入力できません。リモート Web サーバからこれらの URI にアクセスする必要がある場合、もしくは電子メールのクライアントにより、電子メールのリンクをクリックできる場合があります。

URI ハンドラを使用した VPN 接続エントリの生成

AnyConnect URI ハンドラの **create** アクションを使用して、ユーザの AnyConnect 接続エントリの生成を簡略化します。

デバイスに追加する各接続エントリの個別のリンクを挿入します。単一のリンクで複数の作成接続エントリ アクションを指定することはサポートされていません。

エンドポイント設定に AnyConnect 接続エントリを追加するため、次の URI 構文を使用します。

anyconnect:[**//**]**create**[**/**]**?name=***Description*&**host=***ServerAddress*[**&***Parameter1*=*Value*&*Parameter2*=*Value ...*]

例：

anyconnect://create/?name=SimpleExample**&host=**vpn.example.com

anyconnect:create?name=SimpleExample**&host=**vpn.example.com

スペースに一致させるには、**%20** と入力します。たとえば、`Example Connection 1` という接続エントリに一致させるには、**Example%20Connection%201** と入力します。

作成処理には、`host` パラメータが必要となり、他のすべてのパラメータはオプションとなります。アクションがデバイスで実行すると、AnyConnect は、その `name` と `host` に関連付けられた接続エントリに入力するすべてのパラメータ値を保存します。

パラメータ オプションを作成します。

- **name**：AnyConnect のホーム ウィンドウの接続リストおよび AnyConnect 接続エントリの [説明（Description）] フィールドに表示される接続エントリの一意の名前。AnyConnect は名前が一意の場合のみ応答します。接続リストに収まるように、半角 24 文字以内にすることを推奨します。テキストをフィールドに入力する場合、デバイスに表示されたキーボード上の任意の文字、数字、または記号を使用します。文字の大文字と小文字が区別されます。
- **host**：接続に使用する ASA 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。AnyConnect はこのパラメータの値を AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドに挿入します。
- **protocol**（任意、指定されていない場合は、SSL にデフォルト）：この接続に使用される VPN プロトコル。有効な値は次のとおりです。
  - SSL
  - IPsec

  anyconnect:create?name=ExampleIPsec&**host**=vpn.company.com&**protocol**=IPsec
- **authentication**（任意、**プロトコル**が IPsec のみを指定している場合に適用、デフォルトは EAP-AnyConnect）：IPsec VPN 接続で使用される認証手法方法。有効な値は次のとおりです。
  - EAP-AnyConnect
  - EAP-GTC
  - EAP-MD5
  - EAP-MSCHAPv2
  - IKE-RSA
- **ike-identity**（**authentication** が EAP-GTC、EAP-MD5、EAP-MSCAPv2 に設定されている場合に必要）：AUTHENTICATION が EAP-GTC、EAP-MD5 または EAP-MSCHAPv2 にセットされているときの IKE ID。このパラメータは、他の認証設定に使用されたときに無効になります。

  anyconnect:create?**name**=Description&**host**=vpn.company.com&**protocol**=IPsec&**authentication**=eap-md5&**ike-identity**=012A4F8B29A9BCD
- **netroam**（任意、Apple iOS にのみ適用）：デバイス起動後、または接続タイプ（EDGE、3G、Wi-Fi など）の変更後、再接続にかかる時間を制限するかどうかを決定します。

  anyconnect:create?name=Example%201**&host=**vpn.example.com**&netroam=**true

  （注） このパラメータは、データ ローミングや複数のモバイル サービス プロバイダーの使用には影響*しません*。

  有効な値は次のとおりです。
  - **true :**（デフォルト）このオプションでは、VPN アクセスが最適化されます。AnyConnect は値 ON を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドに挿入します。AnyConnect が接続を失った場合、成功するまで新しい接続の確立が試行されます。この設定では、アプリケーションは VPN への持続的な接続に依存します。AnyConnect は、再接続にかかる時間を制限しません。
  - **false**：このオプションでは、バッテリ寿命が最適化されます。AnyConnect はこの値を AnyConnect 接続エントリの [ネットワーク ローミング（Network Roaming）] フィールドの OFF 値と関連付けます。AnyConnect が接続を失った場合、新しい接続の確立が 20 秒間試行され、その後試行が停止されます。ユーザまたはアプリケーションは、必要な場合は新しい VPN 接続を開始する必要があります。

- **usecert**（任意）：ホストへの VPN 接続を確立するときに、デバイスにインストールされているデジタル証明書を使用するかどうかを決定します。

  anyconnect:create?name=Example%201**&host=**vpn.example.com**&usecert=**true

  有効な値は次のとおりです。

  - **true**（デフォルト設定）：ホストとの VPN 接続を確立するときに自動証明書選択を無効化します [証明書（Certificate）] フィールドを自動にする **certcommonname** 値を指定することなしで **usecert** を true に返し、接続時に AnyConnect 証明書ストアから証明書を選択します。
  - **false**：自動証明書の選択を無効化します。

- **certcommonname**（任意、ただし usecert パラメータは必要）：デバイスにあらかじめインストールされた有効な証明書の Common Name（CN; 通常名）を一致させます。AnyConnect はその値を AnyConnect 接続エントリの [証明（Certificate）] フィールドに挿入します。

  デバイスにインストールされているこの証明書を表示するには、[診断（Diagnostics）] > [証明書（Certificates）] をタップします。

  host で必要な証明書を表示するため、スクロールしなければならない場合があります。その他の値と同様に、証明書から読み取った共通名パラメータを表示するために、詳細表示ボタンをタップします。

- **useondemand**（任意、Apple iOS だけに適用、usecert および certcommonname パラメータが必要）：Safari などのアプリケーションが、VPN 接続を開始できるかどうか決定します。
  - **true**：アプリケーションは Apple iOS を使用して VPN 接続を開始できます useondemand パラメータを true に設定すると、AnyConnect は値 ON を AnyConnect 接続エントリの [オンデマンド接続（Connect on Demand）] フィールドに挿入します。
  - **false**（デフォルト）：アプリケーションは VPN 接続を開始できません。このオプションは、DNS 要求を行うアプリケーションが VPN 接続をトリガーしないようにする唯一の手段です。AnyConnect は、AnyConnect 接続エントリの Connect on Demand フィールドで OFF 値でこのオプションを関連付けます。

  anyconnect:create?name=Example%20with%20certificate**&host=**vpn.example.com**&netroam=**true**&usecert=**true**&certcommonname=**example-ID**&useondemand=**true**&domainlistalways=**email.example.com,pay.examplecloud.com**&domainlistnever=**www.example.com**&domainlistifneeded=**intranet.example.com

- **domainlistnever**（オプション、useondemand=true が必要）：Connect on Demand 機能の使用を不適格とするために、一致を評価するドメインをリストにまとめます。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が最初に使用するリストです。ドメイン要求が一致すると、ドメイン要求は無視されます。AnyConnect はこのリストを AnyConnect 接続エントリの [接続しない（Never Connect）] フィールドに挿入します。このリストを使用して、特定のリソースを除外できます。たとえば、公開されている Web サーバ経由では自動 VPN 接続を許可しない場合などが考えられます。値は www.example.com などのように指定します。

- **domainlistalways**（useondemand=true）の場合、domainlistalways または domainlistifneeded パラメータが必要）：Connect on Demand 機能について一致を評価するドメインをリストします。このリストは、ドメイン要求の一致を評価する場合に AnyConnect が 2 番目に使用するリストです。アプリケーションがこのパラメータで指定されたいずれかのドメインへのアクセスを要求し、VPN 接続がまだ行われていない場合、Apple iOS は VPN 接続を確立しようとします。AnyConnect はこのリストを AnyConnect 接続エントリの [常に接続（Always Connect）] フィールドに挿入します。値リストの例は email.example.com,pay.examplecloud.com です。

- **domainlistifneeded**（useondemand=true の場合、domainlistalways または domainlistifneeded パラメータが必要）：DNS エラーが発生した場合、AnyConnect はこのリストに対してドメイン要求が一致しているかどうか評価します。このリスト内の文字列がドメインに一致した場合、Apple iOS は VPN 接続の確立を試行します。AnyConnect はこのリストを AnyConnect 接続エントリの [

必要に応じて接続（Connect if Needed）] フィールドに挿入します。このリストの最も一般的な用途は、社内ネットワーク内の LAN ではアクセスできない内部リソースへの短時間のアクセス権を取得することです。値は `intranet.example.com` などのように指定します。

カンマで区切ったリストを使用して、複数のドメインを指定します。Connect-on-Demand の規則は IP アドレスではなく、ドメイン名のみサポートしています。ただし AnyConnect は、各リスト エントリのドメイン名形式について次のような柔軟性があります。

一致	指示	エントリの例	一致する例	一致しない例
プレフィックスおよびドメイン名が正確に一致。	プレフィックス、ドット、ドメイン名を入力します。	email.example.com	email.example.com	www.example.com email.1example.com email.example1.com email.example.org
ドメイン名は正確に一致し、プレフィックスは任意。先頭にドットを付けると、*example.com で終わるホスト（notexample.com など）への接続を防止できます。	ドットに続けて、照合するドメイン名を入力します。	.example.org	anytext.example.org	anytext.example.com anytext.1example.org anytext.example1.org
指定したテキストで終わる任意のドメイン名。	照合するドメイン名の最後の部分を入力します。	example.net	anytext.anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

URI ハンドラを使用した VPN 接続の確立

接続情報を URI に組み込み、ユーザが簡単に VPN 接続を確立できるよう、これら URI を提供します。次の作業を行う URI 文字列を作成します。

- URI での接続名およびホスト名の指定
- URI での接続情報の指定およびユーザ名とパスワードの自動入力
- 二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力
- 接続情報の指定、ユーザ名およびパスワードの自動入力、および接続プロファイル エイリアスの指定

Connect パラメータおよび構文の説明も参照してください。

（注）　URI を使用して、VPN 接続を確立するためにワンタイム パスワード（OTP）インフラストラクチャとの組み合わせのみ使用する必要がある場合、パスワードを指定します。

URI での接続名およびホスト名の指定

connect アクションに **name** および **host** パラメータを挿入するには、次のいずれかの構文式を使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]
anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress*

完成した URI の例

anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example**&host=**hr.example.com

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

成功または失敗に対するアクションの指定

connect アクションの結果に基づいて特定の URL ベースを開始するために、**onsuccess** または **onerror** パラメータを使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=***Description*|**host=***ServerAddress*]
[**&onsuccess**=URL**&onerror**=URL]

anyconnect:[**//**]**connect**[**/**]**?name=***Description***&host=***ServerAddress*[**&onsuccess**=URL**&onerror**=URL]

例

anyconnect://connect?host=vpn.company.com**&onsuccess**=http%3A%2F%2Fwww.cisco.com
anyconnect://connect?host=vpn.company.com**&onerror**=http%3A%2F%2Fwww.cisco.com%2Ffailure.html**&onsuccess**=http%3A%2F%2Fwww.cisco.com

加えて、onsuccess もしくは onerror パラメータで **anyconnect://close** コマンドを使用して、AnyConnect GUI を閉じます。

anyconnect://connect?host=vpn.company.com**&onsuccess**=anyconnect%3A%2F%2Fclose

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

URI での接続情報の指定およびユーザ名とパスワードの自動入力

connect アクションの名前およびホスト パラメータに加えて、事前入力されたユーザ名とパスワード パラメータを指定するには、いずれかの構文を使用します。

anyconnect:[**//**]**connect**[**/**]**?**[**name=**Description|**host=**ServerAddress]**&prefill_username**=username**&prefill_password**=password

anyconnect:[**//**]**connect**[**/**]**?name=**Description**&host=**ServerAddress**&prefill_username**=username**&prefill_password**=password

完成した URI の例

anyconnect://connect/?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password=**password1

anyconnect:connect?name=Example**&host=**hr.example.com**&prefill_username=**user1**&prefill_password**=password1

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

二重認証のための接続情報の指定およびユーザ名とパスワードの自動入力

事前入力されたプライマリおよびセカンダリ ユーザ名および事前入力されたパスワードを connect アクションでの name と host パラメータに加えて指定するには、次のどちらかの構文を使用します。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]&prefill_username=username&prefill_password=password&prefill_secondary_username=username2&prefill_secondary_password=password2
```

```
anyconnect:[//]connect[/]?name=Description&host=ServerAddress&prefill_username=username&prefill_password=password&prefill_secondary_username=username2&prefill_secondary_password=password2
```

完成した URI の例

```
anyconnect://connect/?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_secondary_username=user2&prefill_secondary_password=password2
```

```
anyconnect:connect?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_secondary_username=user2&prefill_secondary_password=password2
```

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

接続情報の指定、ユーザ名およびパスワードの自動入力、および接続プロファイル エイリアスの指定

この例では、接続プロファイル エイリアスを connect アクションで name および host パラメータに加えて、自動入力のユーザ名と自動入力のパスワードを指定する URI に追加しています。

```
anyconnect:[//]connect[/]?[name=Description|host=ServerAddress]&prefill_username=username&prefill_password=password&prefill_group_list=10.%20Single%20Authentication
```

```
anyconnect:[//]connect[/]?name=Description&host=ServerAddress&prefill_username=username&prefill_password=password&prefill_group_list=10.%20Single%20Authentication
```

完成した URI の例

```
anyconnect://connect/?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_group_list=10.%20Single%20Authentication
```

```
anyconnect:connect?name=Example&host=hr.example.com&prefill_username=user1&prefill_password=password1&prefill_group_list=10.%20Single%20Authentication
```

パラメータおよびその他の構文上の要件の補足説明については、Connect パラメータおよび構文の説明を参照してください。

Connect パラメータおよび構文の説明

connect アクションでは name パラメータもしくは host パラメータのいずれかが必要ですが、両方指定できます。ステートメントのすべてのパラメータ値がデバイスの AnyConnect 接続エントリに一致する場合、AnyConnect は接続を確立するために残りのパラメータを使用します。ステートメントのすべてのパラメータが接続エントリのパラメータと一致せず、name パラメータが一意の場合、新しい接続エントリが生成され、VPN 接続が試行されます。

connect パラメータ オプションの説明を次に示します。

- **name**：AnyConnect ホーム ウィンドウの接続リストに表示される、接続エントリの名前。AnyConnect はこの値を AnyConnect 接続エントリの [説明（Description）] フィールドに対して評価し、前回の手順を使用して Apple iOS デバイスに接続エントリを作成した場合、`name` とも呼ばれます。値は大文字と小文字を区別します。ステートメントの文字と接続エントリの文字の大文字または小文字が一致しない場合は、AnyConnect はこのフィールドを一致させません。
- **host**：AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドと一致させるには、ASA 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。前回の手順を使用してデバイスに接続エントリを生成した場合 host とも呼ばれます。
- **onsuccess**：接続が接続状態に変わるとき、または **anyconnect:close** コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
- **onerror**：接続が接続解除状態に変わるとき、または **anyconnect:close** コマンドを使用して AnyConnect GUI を閉じるときに表示される URL を指定します。
- **prefill_username**：connect URI にユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_password**：connect URI にパスワードを指定し、接続プロンプトに自動入力します。

（注）　prefill_password のフィールドでは、ワンタイム パスワードに設定されている接続プロファイルでのみ使用する必要があります。

- **prefill_secondary_username**：必要な二重認証に設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名を指定し、接続プロンプトに自動入力します。
- **prefill_secondary_password**：必要な二重認証に設定されている環境では、このパラメータは connect URI でセカンダリ ユーザ名のパスワードを指定し、接続プロンプトに自動入力します。
- **prefill_group_list**：これは、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [詳細（Advanced）] > [グループ エイリアス / グループ URL（Group Alias/Group URL）] > [接続エイリアス（Connection Aliases）] を選択して、ASDM で定義されている接続エイリアスです。

URI ハンドラを使用した VPN からの切断

disconnect アクションを挿入するには、次の構文を使用します。

```
anyconnect:[//]disconnect[/]
```

例：

```
anyconnect:disconnect
```

スラッシュは省略可能です。disconnect アクションにはパラメータは必要ありません。

URI ハンドラを使用した AnyConnect UI およびメッセージのローカライズ

（注）　AnyConnect UI やメッセージのローカライズのために URI ハンドラを使用するため、Apple iOS デバイスにインストールされた Apple iOS 5 以降を持っている必要があります。

URI で **import** コマンドを使用するには、次の構文を使用してください。

anyconnect:[**//**]**import**[**/**]**?type=localization&lang=***LanguageCode***&host=***ServerAddress***

例：

anyconnect:import?type=localization&lang=fr**&host=**asa.example.com

スラッシュは省略可能です。インポート アクションは、すべてのパラメータが必要です。**type**、**lang**、および **host** の各パラメータを下に定義します。

- **type**：インポートのタイプ（この場合**はローカリゼーション**）。
- **lang** : anyconnect.po ファイルで指定されて言語を表す 2 文字または 4 文字の言語タグ。たとえば、言語タグは単純に「French」なら fr、「Canadian French」なら fr-ca となります。
- **host** : AnyConnect 接続エントリの [サーバ アドレス（Server Address）] フィールドと一致させるには、ASA のドメイン名または IP アドレスを入力します。

証明書をインポートするために、URI ハンドラを使用

AnyConnect クライアントは、エンドポイントにインストールされた PKCS12 符号化証明書を使用して自ら ASA に認証します。URI ハンドラ **import** コマンドを使用して、PKCS12 符号化証明書バンドルをエンドポイントにインポートします。

PKCS12 証明書を URL からインポートするには、次の構文を使用します。

anyconnect://import/?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com**%2F**CertName.p12

URI の先頭のスラッシュは省略可能です。

スペースに一致させるには、**%20** と入力します。たとえば、Example Connection 1 という文字列に一致させるには、Example**%20**Connection**%20**1 と入力します。

URI のコロンと一致させるには、**%3A** を使用します。URI のスラッシュと一致させるには、**%2F** を使用します。たとえば、http://example.cisco.com/CertName.p12 と一致させるには、http**%3A%2F%2F**example.cisco.com**%2F**CertName.p12 と入力します。

次は、インポート パラメータ オプションの説明です。

- **type**：PKCS12 証明書タイプのみをサポートします。
- **ur**：URL は、証明書がある ID を符号化します。「http」、「https」および「ftp」をサポートします。URI では **%3A** はコロン（:）、**%2F** はスラッシュ（/）、**%40** はアンパサンド（@）を表します。

HTML ハイパーリンクの例

URI を HTML ページに追加するには、URI をハイパーリンクに組み込む必要があります。[HTML] ハイパーリンクで URI を使用する方法を示す例です。例中で太字の部分が URI です。

HTTP の例

```
<p>
<a href="anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12>
click here to import certificate using http</a>
</p>
```

FTP の例

```
<p><ahref="anyconnect://import?type=pkcs12
&uri=ftp%3A%2F%2FAdministrator%3Apassword%40192.168.10.20%2Fcerts%2FCertName.pfx">ここをクリックして、ftp を使用して証明書をインポートします</a>
</p>
```

Secure Digital（SD）カードの例

```
<p><a href="anyconnect://import?type=pkcs12
&uri=file%3A%2F%2F%2Fsdcard%2CertName.pfx">ここをクリックして、モバイル デバイスの SD カードから証明書をインポートします</a>
</p>
```

VPN クライアント プロファイルをインポートするために URI ハンドラを使用

AnyConnect クライアントにクライアント プロファイルを配信するため、この URI ハンドラのメソッドを使用します。

URI で **import** コマンドを使用するには、次の構文を使用してください。

anyconnect:[**//**]**import**[**/**]**?type=profile&uri=***Filename.xml*

例：

anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml

スラッシュは省略可能です。インポート アクションは、uri パラメータが必要です。

トラブルシューティング

モバイル デバイスでログインを有効にし、適切なユーザ ガイドのトラブルシューティングの指示に従ってください。

- *iPhone 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）*
- *iPad 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）*
- *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）*

次の手順で問題が解決しない場合、次の提案を試してください。

- 同じ問題がデスクトップ クライアントで発生しているかどうか判断します。
- AnyConnect Mobile ライセンスが ASA にインストールされていることを確認します。
- 証明書認証が失敗する場合、正しい証明書が選択されていることを確認します。デバイスのクライアント証明書に Extended Key Usage として Client Authentication があることを確認します。AnyConnect プロファイルの証明書一致規則がユーザの選択した証明書を除外していないことを確認します。ユーザが証明書を選択しても、プロファイルのフィルタリング ルールに一致しなければ認証には使用されません。認証メカニズムで ASA に関連するアカウンティング ポリシーが使用されている場合、ユーザが正常に認証できることを確認します。それでも問題が解決されない場合は、クライアントのロギングをイネーブルにし、ASA のデバッグ ロギングをイネーブルにします。
- 証明書のみの認証を使用しようとしている場合に認証画面が表示されたら、グループ URL を使用するよう接続を設定し、トンネル グループのセカンダリ認証が設定されていないことを確認します。詳細については、適切な『ASA 管理者ガイド』を参照してください。

Apple iOS 固有のトラブルシューティング

- デバイスが起動したあとで VPN 接続がリストアされていない場合は、[ネットワーク ローミング（Network Roaming）] が無効になっていることを確認します。
- 証明書認証および Apple iOS Connect On Demand 機能が接続するよう設定されている場合に AnyConnect アプリケーションを使用して Apple iOS が接続開始するよう要求している場合、グループ URL を使用するよう接続を設定します。グループ URL および証明書のみの認証の両方とも Connect on Demand の要件です。