

Cisco AnyConnect Secure Mobility Client Apple iOS 向けリリース 4.9.x リリースノート

Apple iOS 向け AnyConnect リリースノート

Apple iOS モバイル デバイス 向け AnyConnect

AnyConnect Secure Mobility Client により、リモートユーザーは Cisco ASA 5500 シリーズへのセキュアな VPN 接続を確立できます。このクライアントは、エンタープライズ 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提供し、インストールしたアプリケーションがエンタープライズ ネットワークに直接接続されているかのように通信を行えるようにします。AnyConnect は、IPv4 または IPv6 トンネルを介した IPv4 および IPv6 リソースへの接続をサポートします。

AnyConnect セキュア モビリティ クライアントと適応型セキュリティアプライアンス (ASA) 5500 のシステム管理者向けに作成されたこのドキュメントは、Apple iOS デバイス上で動作する AnyConnect のリリースに固有の情報を提供します。

AnyConnect アプリケーションは、Apple iTunes App Store でのみ入手できます。シスコでは、AnyConnect モバイルアプリケーションを配布していません。また、ASA からモバイルアプリケーションを展開することもできません。このモバイルリリースがサポートされている間は、ASA からデスクトップ デバイス用の他の AnyConnect リリースを展開することが可能です。

AnyConnect Mobile のサポート ポリシー

シスコでは、現在 App Store で入手可能な AnyConnect バージョンをサポートしていますが、修正プログラムと拡張機能は、最新のリリース バージョンでのみ提供されます。

AnyConnect のライセンス

ASA ヘッドエンドに接続するには、AnyConnect 4.x Plus ライセンスまたは Apex ライセンスが必要です。トライアルライセンスを使用できます ([Cisco AnyConnect Ordering Guide](#))。

最新のエンドユーザーライセンス契約については、『[Cisco End User License Agreement, AnyConnect Secure Mobility Client, Release 4.x](#)』を参照してください。

オープン ソース ライセンス通知については、以下を参照してください。 [Open Source Software Used In Cisco AnyConnect Secure Mobility Client Release 4.x for Mobile](#)

TestFlight による Cisco AnyConnect のベータ テスト

TestFlight でのリリース前のテストには、AnyConnect のベータ ビルドを利用します。TestFlight でのテストに参加するには、<https://testflight.apple.com/join/N0QLSq2c> の手順に従います。

この TestFlight のリンクで後からオプトアウトすることも可能です。オプトアウトしたら、ベータ ビルドをアンインストールして最新のベータ版ではない AnyConnect を再インストールする必要があります。

ベータ テスト中に問題が見つかった場合は、シスコ (ac-mobile-feedback@cisco.com) に電子メールで速やかに報告してください。Cisco Technical Assistance Center (TAC) は、AnyConnect のベータ版で見つかった問題には対処しません。

Apple iOS で利用可能な AnyConnect のバージョン

Cisco AnyConnect for Apple iOS は、現在複数のバージョンで利用可能です。

• Cisco AnyConnect

Cisco AnyConnect 4.9 は、Apple iOS で利用可能な最新の推奨バージョンです。常に最新の Apple iOS のバグ修正を受けられるように、最新バージョンにアップグレードしてください。

このバージョンは、Apple iOS 10.3以降で使用することを推奨します。このバージョンは、iOS が提供する新しい拡張フレームワークを使用して、VPN とそのすべての機能を実装しています。アプリケーション単位 VPN トンネリングは完全にサポートされている機能であり、新しい拡張フレームワークでは TCP と UDP の両方のアプリケーションをサポートできます。今後も、新しい Cisco AnyConnect バージョンが、すべての拡張機能とバグ修正を含む唯一のバージョンとなります。

• Cisco Legacy AnyConnect

Legacy AnyConnect 4.0.05x は、11.x. を超える iOS ではサポートされていません。iOS の以降のバージョンとの互換性を確保するには、App Store で使用可能な最新の AnyConnect アプリケーションをインストールします。

Legacy AnyConnect は Apple iOS 6.0 以降をサポートするバージョンで、今後しばらくの間 App Store で利用可能です。このバージョンは時間をかけて段階的に廃止されますが、最新の推奨バージョンへの移行が容易になるように現在も利用可能です。

Legacy AnyConnect アプリの Per App VPN トンネリング機能は、TAC サポートを受けません。Per App VPN の使用を希望されるお客様は、新しいバージョンに移行する必要があります。

Legacy AnyConnect は、重要なセキュリティ上の問題に関する更新のみがなされます。このリリースには、4.0.05x という番号が使用され続けます。

Cisco AnyConnect と Legacy AnyConnect は、異なるアプリ ID を持つ異なるアプリです。次に例を示します。

- AnyConnect 4.0.07x (およびそれ以降) で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x : AnyConnect の動作が次のように変更されます。AnyConnect は、スプ

リット包含ネットワークにない場合でも、トンネル DNS サーバのトラフィックがトンネリングされると見なします。

- AnyConnect アプリケーションを 4.0.05x 以前のバージョンから AnyConnect 4.0.07x または 4.6.x (またはそれ以降) にアップグレードすることはできません。Cisco AnyConnect 4.0.07x (または 4.6.x 以降) は別のアプリケーションであり、別の名前とアイコンを使用してインストールされています。
- AnyConnect の異なるバージョンは、モバイル デバイスに共存できますが、これはシスコではサポートされません。両方のバージョンの AnyConnect がインストールされている状態で接続しようとする、予期せぬ動作が発生する恐れがあります。デバイスにインストールされている AnyConnect アプリは 1 つだけで、デバイスと環境に適したバージョンであることを確認してください。
- Legacy AnyConnect バージョン 4.0.05069 以前のリリースを使用してインポートされた証明書は、新しい AnyConnect アプリケーションのリリース 4.0.07072 ではアクセスおよび使用ができません。MDM で導入された証明書は、両方のアプリ バージョンでアクセスおよび使用ができます。
- 証明書やプロファイルなどの、Legacy AnyConnect アプリにインポートされたアプリ データは、新しいバージョンに更新する場合、削除する必要があります。そうしないと、システムの VPN 設定で引き続き表示されます。Legacy AnyConnect アプリをアンインストールする前にアプリ データを削除します。
- 現在の MDM プロファイルでは、新しいアプリはトリガーされません。EMM ベンダーは、VPNType (VPN)、VPNSubType (com.cisco.anyconnect)、および ProviderType (パケットトンネル) をサポートする必要があります。AnyConnect は新しいフレームワークで ISE にアクセスできなくなるため、ISE と統合させるには UniqueIdentifier を AnyConnect に渡せる必要があります。設定方法については、EMM ベンダーにお問い合わせください。カスタム VPN タイプが必要な場合もあれば、リリース時にはサポートされていない場合もあります。

AnyConnect 4.0.07x 以降で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x からの動作が次のように変更されます。

- ヘッドエンドに送信されたデバイス ID は、新しいバージョンでは UDID ではなく、初期設定へのリセット後には、同じデバイスで作成されたバックアップからデバイスが復元されない限り、デバイス ID が異なるものになります。
- MDM で導入された証明書だけでなく、AnyConnect で利用可能ないずれかの方法 (SCEP、UI 使用 - 手動で、URI ハンドラ) を使用してインポートされた証明書も使用できます。AnyConnect の新しいバージョンでは、電子メールまたはこれらの識別されたもの以外のメカニズムを使用してインポートした証明書を使用できなくなりました。
- UI を使用して接続エントリを作成する際には、表示された iOS セキュリティ メッセージを受け入れる必要があります。
- AnyConnect VPN プロファイルからダウンロードしたホスト エントリと同じ名前のユーザが作成したエントリは、アクティブであれば切断されるまで名前は変更されません。ま

た、ダウンロードされたホスト接続エントリは、接続が維持されている間ではなく、接続が解除された後に UI に表示されます。

- AnyConnect では、split-include ネットワークではない場合でもトンネル DNS サーバのトラフィックがトンネル化されると見なされます。

Apple iOS 対応デバイス

最新の推奨バージョンである **Cisco AnyConnect 4.9** は、Apple iOS 10.3 以降を実行するすべての iPhone、iPad、および iPod Touch デバイスで利用可能です。

デバイスが Apple iOS 10.3 以降をサポートしていない場合は、Apple iOS 6.0 以降を実行するすべての iPhone、iPad、および iPod Touch デバイスで利用可能な **Legacy AnyConnect 4.0.05x** のみを使用できます。Legacy AnyConnect の Per App トンネリングには、Apple iOS 8.3 以降が必要です。



-
- (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。
-

Apple iOS での AnyConnect のアップグレード

AnyConnect へのアップグレードは、Apple App Store を使用して管理します。Cisco AnyConnect または Legacy AnyConnect のアップグレードが利用可能であることを示す通知を Apple App Store から受けたら、次の手順に従います。



-
- (注) AnyConnect アプリケーションを 4.0.05x 以前のバージョンから AnyConnect 4.0.07x または 4.6.x 以降にアップグレードすることはできません。これらは別のアプリであり、別の名前とアイコンでインストールされます。

新しいバージョンをインストールする前に、[Apple iOS で利用可能な AnyConnect のバージョン \(2 ページ\)](#) を参照してください。Legacy AnyConnect アプリ データをすべて削除し、Legacy AnyConnect アプリを削除してから、新しいバージョンをインストールすることを推奨します。

始める前に

デバイスをアップグレードする前に、AnyConnect VPN セッションが確立されている場合はそのセッションを切断し、AnyConnect アプリケーションが開いている場合は閉じる必要があります。これに失敗した場合は、新しいバージョンの AnyConnect を使用する前に、AnyConnect はデバイスの再起動を要求します。



- (注) これは、Apple Connect-on-Demand 機能を使用していて、4.0.05032 より前の Legacy AnyConnect リリース、または 9.3 より前の Apple iOS リリースを実行している場合にのみ、お使いの環境に適用されます。AnyConnect の更新後に Connect On-Demand VPN トンネルが適切に確立されるようにするには、ユーザが AnyConnect アプリを手動で開始して接続を確立する必要があります。このようにしないと、次に iOS システムが VPN トンネルを確立しようとするときに、「VPN に接続するにはアプリケーションを起動する必要があります (The VPN Connection requires an application to start up)」というエラー メッセージが表示されます。

手順

- ステップ 1 iOS のホームページで、[App Store] アイコンをタップします。
- ステップ 2 [AnyConnect アップグレード通知 (AnyConnect upgrade notice)] をタップします。
- ステップ 3 新機能を確認します。
- ステップ 4 [更新 (Update)] をクリックします。
- ステップ 5 [Apple ID パスワード (Apple ID Password)] を入力します。
- ステップ 6 [OK] をタップします。

AnyConnect の更新が実行されます。

新機能

Apple iOS モバイル端末向け AnyConnect 4.9.05043 の新機能

この AnyConnect のリリースでは、[Apple iOS 向け AnyConnect 4.9.05043 の解決済みの問題 \(14 ページ\)](#) に記載されている不具合が解決されます。

Apple iOS モバイル端末向け AnyConnect 4.9.05041 の新機能

この AnyConnect のリリースは、次の拡張機能を含み、[Apple iOS 向け AnyConnect 4.9.05041 の解決済みの問題 \(14 ページ\)](#) に記載されている不具合が修正されています。

- VPN 接続用のサーバ名識別 (SNI) のサポートが追加されています。
- エンドユーザによる VPN 接続の追加をブロックし、AnyConnect ローカルセキュア設定を定義するための MDM の構成可能な設定が追加されました。

Apple iOS モバイル端末向け AnyConnect 4.9.00562 の新機能

この AnyConnect のリリースでは、[Apple iOS 向け AnyConnect 4.9.00562 の解決済みの問題 \(14 ページ\)](#) に記載されている不具合が解決されます。

Apple iOS モバイル端末向け AnyConnect 4.9.00542 の新機能

この AnyConnect のリリースでは、[Apple iOS 向け AnyConnect 4.9.00542 の解決済みの問題 \(14 ページ\)](#) に記載されている不具合が解決されます。

Apple iOS モバイル端末向け AnyConnect 4.9.00518 の新機能

このリリースの AnyConnect では、次の機能およびサポートが更新されています。

- 複数のトンネルのサポート：MDM VPN プロファイルで設定を行う必要があります。詳細については、『[Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.9](#)』の「[AnyConnect on Mobile Devices](#)」の章を参照してください。
- AnyConnect リリース 4.9 では、安全性の低い特定の暗号スイートが削除されました。
 - SSL VPN の場合、AnyConnect は TLS と DTLS の両方からの暗号スイート、DHE-RSA-AES256-SHA と DES-CBC3-SHA をサポートしなくなりました。
 - IKEv2/IPsec については、AnyConnect は次のアルゴリズムをサポートしなくなりました。
 - 暗号化アルゴリズム：DES と 3DES
 - 疑似ランダム関数 (PRF) アルゴリズム：MD5
 - 整合性アルゴリズム：MD5
 - Diffie-Hellman (DH) グループ：2、5、14、24

Apple iOS AnyConnect 機能マトリックス

次の機能は、Apple iOS 端末向け AnyConnect でサポートされます。

| カテゴリ：機能 | Apple iOS |
|----------------------------------|-----------|
| 展開および設定： | |
| アプリケーションストアからのインストールまたはアップグレード | 対応 |
| Cisco VPN プロファイルのサポート（手動インポート） | 対応 |
| Cisco VPN プロファイルのサポート（接続中のインポート） | 対応 |
| MDM 設定の接続エントリ | 対応 |
| ユーザー設定の接続エントリ | 対応 |
| トンネリング： | |
| TLS | 対応 |

| カテゴリ：機能 | Apple iOS |
|---|--|
| データグラム TLS (DTLS) | 対応 |
| IPsec IKEv2 NAT-T | 対応 |
| IKEv2 - raw ESP | 非対応 |
| Suite B (IPSec のみ) | 対応 |
| TLS 圧縮 | 対応 (32 ビットデバイスのみ) |
| デッドピア検出 | 対応 |
| トンネル キープアライブ | 対応 |
| 複数のアクティブ ネットワーク インターフェイス | 非対応 |
| アプリケーションごとのトンネリング | 対応 (Cisco AnyConnect 4.0.09xxx および iOS 10.3 以降が必要です) |
| フルトンネル (OSにより、アプリケーションストアへのトラフィックなど一部のトラフィックで例外が発生する可能性があります) | 対応 |
| スプリット トンネル (スプリットを含む) | 対応 |
| ローカル LAN (スプリットを含まない) * | 対応 |
| Split-DNS | 対応 |
| 自動再接続/ネットワーク ローミング | 対応 |
| オンデマンド VPN (宛先により起動) | 対応 (オンデマンドでApple iOS Connect と互換性があります) |
| オンデマンド VPN (アプリケーションによって起動) | 対応 (アプリケーション単位 VPN モードで動作している場合のみ) |
| キー再生成 | 対応 |
| IPv4 パブリック トランスポート | 対応 |
| IPv6 パブリック トランスポート | 対応 |
| IPv4 over IPv4 トンネル | 対応 |
| IPv6 over IPv4 トンネル | 対応 |
| IPv6 over IPv4 トンネル | 対応 |
| IPv6 over IPv6 トンネル | 対応 |
| デフォルト ドメイン | 対応 |
| DNS サーバーの設定 | 対応 |
| プライベート側プロキシサポート | 対応 |

| カテゴリ：機能 | Apple iOS |
|----------------------------|--------------------------------|
| プロキシ例外 | 対応（ただし、ワイルドカードの仕様はサポートされていません） |
| パブリック側プロキシサポート | 非対応 |
| ログイン前バナー | 対応 |
| ログイン後バナー | 対応 |
| DSCP の保存 | 非対応 |
| 接続と切断： | |
| VPN ロード バランシング | 対応 |
| バックアップ サーバー リスト | 対応 |
| 最適ゲートウェイ選択 | 非対応 |
| 認証： | |
| SAML 2.0 | 対応 |
| クライアント証明書認証 | 対応 |
| オンライン証明書ステータス プロトコル (OCSP) | 非対応 |
| 手動によるユーザー証明書の管理 | 対応 |
| 手動によるサーバー証明書の管理 | 対応 |
| レガシー SCEP の登録 | 非対応 |
| SCEP プロキシの登録 | 対応 |
| 自動証明書選択 | 対応 |
| 手動による証明書の選択 | 対応 |
| スマート カードのサポート | 非対応 |
| ユーザー名およびパスワード | 対応 |
| トークン/課題 | 対応 |
| 二重認証 | 対応 |
| グループ URL（サーバー アドレスで指定） | 対応 |
| グループの選択（ドロップダウン選択） | 対応 |
| ユーザー証明書からのクレデンシャルの事前入力 | 対応 |
| パスワードの保存 | 非対応 |
| ユーザー インターフェイス： | |

| カテゴリ：機能 | Apple iOS |
|---|--------------------------------------|
| スタンドアロン GUI | 対応 |
| ネイティブ OS GUI | 対応（機能制限があります） |
| API/URI ハンドラ（以下を参照） | 対応 |
| UI のカスタマイゼーション | 非対応 |
| UI のローカリゼーション | 対応（アプリケーションには事前にパッケージ化された言語が含まれています） |
| ユーザー設定 | 対応 |
| 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 | 非対応 |
| AnyConnect に固有のステータス アイコン | 非対応 |
| モバイル ポスチャ：（AnyConnect Identity Extension（ACIDex）） | |
| シリアル番号または固有 ID のチェック | 対応 |
| ヘッドエンドと共有される OS および AnyConnect のバージョン | 対応 |
| AnyConnect NVM のサポート | 非対応 |
| URI の処理： | |
| 接続エントリの追加 | 対応 |
| VPN への接続 | 対応 |
| 接続時のクレデンシャルの事前入力 | 対応 |
| VPN の解除 | 対応 |
| 証明書のインポート | 対応 |
| ローカリゼーションデータのインポート | 対応 |
| XML クライアント プロファイルのインポート | 対応 |
| URI コマンドの外部（ユーザー）制御 | 対応 |
| レポートおよびトラブルシューティング： | |
| 統計 | 対応 |
| ロギング/診断情報（DART） | 対応 |
| 認定： | |
| FIPS 140-2 レベル 1 | 対応 |

*オペレーティングシステムの実装による ASA の設定に関係なく、iOS デバイスに対してローカル LAN アクセスが有効になります。

適応型セキュリティ アプライアンスの要件

次の機能には、ASA の最小リリースが必要です。



(注) 現在の AnyConnect Mobile リリースでこれらの機能を使用できるかどうかを確認するには、お使いのプラットフォームの機能マトリックスを参照してください。

- SAML 認証機能を使用するには、ASA 9.7.1.24、9.8.2.28、9.9.2.1 以降にアップグレードする必要があります。クライアントとサーバー両方のバージョンが最新であることを確認してください。
- TLS 1.2 を使用するには、ASA 9.3.2 以降にアップグレードする必要があります。
- アプリケーション単位 VPN トンネリングモードを使用するには、ASA 9.3.2 以降にアップグレードする必要があります。
- 次のモバイル機能を使用するには、ASA 9.0 にアップグレードする必要があります。
 - IPsec IKEv2 VPN
 - Suite B 暗号化
 - SCEP プロキシ
 - モバイル ポスチャ
- ASA リリース 8.0(3) および Adaptive Security Device Manager (ASDM) 6.1(3) は、モバイル端末の AnyConnect をサポートする最小リリースです。

その他のシスコ ヘッドエンドのサポート

AnyConnect SSL 接続は、Cisco IOS 15.3(3)M 以降/15.2(4)M 以降でサポートされています。

AnyConnect IKEv2 接続は、Cisco ISR g2 15.2(4)M 以降でサポートされています。

AnyConnect SSL および IKEv2 は、Cisco Firepower Threat Defense リリース 6.2.1 以降でサポートされています。

Apple iOS での AnyConnect の注意事項と制約事項

- (iOS 14.0.x のみ) : トンネル DNS サーバーがスプリット DNS ドメイン名を指定せずに設定されている場合、トンネル DNS サーバーでアドレスを解決できなくても、デバイスのパブリック DNS サーバーにフォールバックしません。iOS の変更により、この異なる動作が発生しました。

- (iOS 14.0.x のみ) CSCvv50495 : ネットワークの変更後、ネットワークを移行、またはネットワークを一時停止して再開すると、トラフィックが停止します。VPN接続を無効にしてから再度有効にすると、再開できます。この問題は、iOS 14.1 では修正されています。
- CSCvs82209 : SCEP 経由でインポートされ、アクセスに生体認証を要求するクライアント証明書にアクセスしているときに、iOS 13.3.1以降で「有効な証明書が見つかりません」というエラーが発生します。iOS 13.3.1では、アクセスに生体認証 (TouchID / FaceID / パスコード) を要求するセキュリティプロパティを持つ SCEP インポート済み証明書を使用する AnyConnect ネットワーク拡張機能が削除されました。この変更に対応するようにクライアントを再設計できるようになるまでは、生体認証オプションを使用せずに SCEP を使用して証明書を展開します。
- AnyConnect の設定は、ユーザ (手動で) または iPhone 設定ユーティリティ (<http://www.apple.com/support/iphone/enterprise/>) によって生成する AnyConnect VPN クライアントプロファイルによって行うか、エンタープライズモバイルデバイスマネージャを使用して行うことができます。
- Apple iOS デバイスは 1 つの AnyConnect VPN クライアント プロファイルのみをサポートします。生成された設定の内容は、必ず最新のプロファイルと一致します。たとえば、ユーザが vpn.example1.com に接続してから vpn.example2.com に接続すると、vpn.example2.com からインポートされた AnyConnect VPN クライアントプロファイルにより、vpn.example1.com からインポートされたクライアントプロファイルが置き換えられます。
- このリリースは、トンネルキープアライブ機能をサポートしています。ただし、デバイスのバッテリー寿命は短くなります。アップデート間隔の値を増やすことでこの問題は軽減します。
- **DHE の非互換性**
AnyConnect リリース 4.6 で導入された DHE 暗号サポートにより、ASA 9.2 より前の ASA バージョンで非互換性の問題が発生します。9.2 より前の ASA リリースで DHE 暗号を使用している場合、これらの ASA バージョンで DHE 暗号を無効にする必要があります。

Apple iOS Connect On-Demand の注意事項 :

- iOS On-Demand ロジックの結果として自動的に接続され、Disconnect on Suspend (一時停止時に接続解除) が設定されている VPN セッションは、デバイスがスリープすると切断されます。デバイスがスリープ状態から起動すると、必要に応じて On-Demand ロジックが VPN セッションを再接続します。
- AnyConnect は、UI が起動され、VPN 接続が開始されたときにデバイス情報を収集します。そのため、ユーザが iOS の Connect on Demand 機能を使用して最初に接続を行う場合、または OS バージョンなどのデバイス情報が変更された後、AnyConnect がモバイルポスチャ情報を誤ってレポートする状況が発生します。
- Apple Connect-on-Demand 機能を使用していて、4.0.05032 より前の Legacy AnyConnect リリース、または 9.3 より前の Apple iOS リリースを実行している場合にのみ、お使いの環境に適用されます。AnyConnect の更新後に Connect On-Demand VPN トンネルが適切に確

立されるようにするには、ユーザーが AnyConnect アプリを手動で開始して接続を確立する必要があります。このようにしないと、次に iOS システムが VPN トンネルを確立しようとするときに、「VPNに接続するにはアプリケーションを起動する必要があります (The VPN Connection requires an application to start up)」というエラーメッセージが表示されません。

Cisco AnyConnect と Legacy AnyConnect は、異なるアプリ ID を持つ異なるアプリです。次に例を示します。

- AnyConnect アプリを 4.0.05x 以前のバージョンから新しいバージョンにアップグレードすることはできません。新しいバージョンは別のアプリであり、別の名前とアイコンでインストールされます。
- AnyConnect の異なるバージョンは、モバイルデバイスに共存できますが、これはシスコではサポートされません。両方のバージョンの AnyConnect がインストールされている状態で接続しようすると、予期せぬ動作が発生する恐れがあります。デバイスにインストールされている AnyConnect アプリは 1 つだけで、デバイスと環境に適したバージョンであることを確認してください。
- Legacy AnyConnect バージョン 4.0.05069 以前のリリースを使用してインポートされた証明書は、新しい AnyConnect アプリケーションのリリース 4.0.07072 ではアクセスおよび使用ができません。MDM で導入された証明書は、両方のアプリバージョンでアクセスおよび使用ができます。
- 証明書やプロファイルなどの、Legacy AnyConnect アプリにインポートされたアプリ データは、新しいバージョンに更新する場合、削除する必要があります。そうしないと、システムの VPN 設定で引き続き表示されます。Legacy AnyConnect アプリをアンインストールする前にアプリ データを削除します。
- 現在の MDM プロファイルでは、新しいアプリはトリガーされません。EMM ベンダーは、VPNType (VPN)、VPNSubType (com.cisco.anyconnect)、および ProviderType (パケットトンネル) をサポートする必要があります。AnyConnect は新しいフレームワークで ISE にアクセスできなくなるため、ISE と統合させるには UniqueIdentifier を AnyConnect に渡す必要があります。設定方法については、EMM ベンダーにお問い合わせください。カスタム VPN タイプが必要な場合もあれば、リリース時にはサポートされていない場合があります。

AnyConnect 4.6.x 以降で新しい拡張フレームワークを使用すると、Legacy AnyConnect 4.0.05x からの動作が次のように変更されます。

- ヘッドエンドに送信されたデバイス ID は、新しいバージョンでは UDID ではなく、初期設定へのリセット後には、同じデバイスで作成されたバックアップからデバイスが復元されない限り、デバイス ID が異なるものになります。
- MDM で導入された証明書だけでなく、AnyConnect で利用可能ないずれかの方法 (SCEP、UI 使用 - 手動で、URI ハンドラ) を使用してインポートされた証明書も使用できます。AnyConnect の新しいバージョンでは、電子メールまたはこれらの識別されたもの以外のメカニズムを使用してインポートした証明書を使用できなくなりました。

- UI を使用して接続エントリを作成する際には、表示された iOS セキュリティ メッセージを受け入れる必要があります。
- AnyConnect VPN プロファイルからダウンロードしたホスト エントリと同じ名前のユーザが作成したエントリは、アクティブであれば切断されるまで名前は変更されません。また、ダウンロードされたホスト接続エントリは、接続が維持されている間ではなく、接続が解除された後に UI に表示されます。

既知の互換性の問題

AnyConnect 4.7.xxxxx 以降の場合

- スプリット除外設定で IPv6 のみをトンネリングする場合（IPv4 アドレスが割り当てられていない場合）、ASA ヘッドエンドへのスプリット トンネリングは機能しません。

除外リストエントリを除き、すべてのトラフィックをトンネリングする必要がありますが、スプリット除外リストは適用されません。すべての IPv6 トラフィックは除外されません。詳細については、「CSCvb80768 : IPv6 Split Exclude & IPv4 DropAll がトンネルからのすべての v6 トラフィックを除外」を参照してください。（レーダー 29623849）。

- AnyConnect UI が開いたままの状態、iOS が UI と内部の AnyConnect 拡張機能の間のプロセス間通信（IPC）を誤って切断した場合、UI アクティビティはエラーまたは不正な応答により失敗します。

これを回復するには、IPC を再確立する AnyConnect UI を閉じてから再起動する必要があります。UI が閉じられたときに予期しない IPC 切断が発生した場合、次回 UI を開くときに、再確立されます。詳細については、「CSCvb95722 : 失敗して一時停止状態になります（レーダー 29313229）」を参照してください。

- オンデマンド接続の場合は、更新された VPN 接続プロファイルが ASA によってクライアントにプッシュされたときに、AnyConnect UI を開く必要があります。UI が開かれていない場合、更新されたプロファイルは同期されないため、変更は使用されません。

残念ながら、新しいプロファイルを同期するために UI を開くことをユーザーに示すことはありません（Legacy AnyConnect と同様）。したがって、更新された接続エントリが使用されない可能性があります。現時点では回避策はありません。詳細については、「CSCvc35923 : オンデマンド AC を使用すると、更新された接続プロファイル（レーダー 30173053）を同期するために AC を開く必要があることをユーザーに通知できません。」を参照してください。

- 管理対象のアプリケーションごとの設定では、アプリケーショントラフィックは、アプリケーションごとに設定され、不適切なタイミングでユーザーが作成した（管理対象外の）VPN 接続を通過します。

詳細については、「CSCvc36024 : アプリケーション別 : アプリケーションは、非 PAV フルトンネル（レーダー 29513803）を介してトラフィックを渡すことができます。」を参照してください。

未解決および解決済みの AnyConnect の問題

Cisco Bug Search Tool には、このリリースで未解決および解決済みの次の問題に関する詳細情報が含まれています。Bug Search Tool にアクセスするには、シスコアカウントが必要です。シスコアカウントをお持ちでない場合は、<https://Cisco.com> で登録を行ってください。

デスクトップリリースノート (https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect410/release/notes/release-notes-anyconnect-4-10.html) で定義されている一部のクロスプラットフォームのバグは、モバイルリリースに適用される場合があります。修正済みとして報告されたバグは、AnyConnect のリリース番号が大きいすべてのオペレーティングシステムプラットフォーム（モバイルオペレーティングシステムを含む）で使用可能になります。vpn、core、nvm、およびクロスプラットフォームに適用される同様のコンポーネントのバグは、後続のモバイルリリースでは重複しません。たとえば、iOS リリース 4.9.00512 では、デスクトップリリース 4.9.00086 で解決された vpn コンポーネントのバグは表示されません。iOS バージョンが、バグが修正されたと報告されたリリースバージョンよりも大きいからです。

Apple iOS 向け AnyConnect 4.9.05043 の解決済みの問題

| ID | 見出し |
|-----------|--|
| CSVw86231 | TLS 暗号スイートの AnyConnect iOS ATS の制限により、SAML 認証が失敗する可能性がある |

Apple iOS 向け AnyConnect 4.9.05041 の解決済みの問題

| ID | 見出し |
|------------|---|
| CSCvv68121 | AnyConnect アプリケーション設定は MDM では設定できない |
| CSCvv68142 | AnyConnect では、MDM がエンドユーザーによる VPN 接続の追加をブロックできるようにする必要がある |
| CSCvw37668 | コモンクライテリアのガイドラインに従うための ATS ポリシーの例外を削除 |

Apple iOS 向け AnyConnect 4.9.00562 の解決済みの問題

| ID | 見出し |
|------------|---|
| CSCvv82012 | アプリの切り替え後、iPhone/iOS AnyConnect のユーザログイン情報が保持されない |

Apple iOS 向け AnyConnect 4.9.00542 の解決済みの問題

| ID | 見出し |
|------------|--|
| CSCvv36705 | 著作権のページに掲載されているサードパーティの電子メールのリンクはクリックできません |

【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。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017–2021 Cisco Systems, Inc. All rights reserved.