

Release Notes for Cisco Secure Client (AnyConnect を含む) 、ユニバーサル Windows プラットフォームのリリース 5

ユニバーサル Windows プラットフォーム向け Cisco Secure Client

ユニバーサル Windows プラットフォーム向け Cisco Secure Client (AnyConnect を含む) は、リモートの Windows ユーザーに、Cisco Secure Firewall ASA およびその他のシスコがサポートするヘッドエンドデバイスへのセキュアな VPN 接続を提供します。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は、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できます。Cisco Secure Client 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。

Cisco Secure Client および Cisco Secure Firewall ASA のシステム管理者向けに作成されたこのドキュメントには、上で動作する Secure Client のリリースに固有の情報が記載されています。ユニバーサル Windows プラットフォーム

Cisco Secure Client アプリケーションは、入手できます。Windows Store のみ。Cisco Secure Firewall ASA からモバイルアプリを展開することはできません。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 Cisco Secure Client リリースを展開できます。

Cisco Secure Client のモバイルサポートポリシー

シスコでは、現在 App Store で入手可能な Cisco Secure Client 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。

Cisco Secure Client のライセンス

Cisco Secure Firewall ASA ヘッドエンドに接続するには、Advantage または Premier 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 Secure Client 発注ガイド](#)。

最新のエンドユーザーライセンス契約書については、[シスコエンドユーザーライセンス契約](#)、[Cisco Secure Client \[英語\]](#) 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、[モバイル向け Cisco Secure Client で使用されるオープンソースソフトウェア \[英語\]](#) を参照してください。

Cisco Secure Client Mobile の関連ドキュメント

詳細については、次のドキュメントを参照してください。

- [Cisco Secure Client Release Notes](#)
- [Cisco Secure Client 管理者ガイド](#)
- [Cisco Secure Firewall ASA ドキュメントのランディングページ](#)

ユニバーサル Windows プラットフォームのサポート対象デバイス

Windows のサポート

ユニバーサル Windows プラットフォーム向け Cisco Secure Client は、Microsoft Windows 10 RS4 (1803) 以降を実行するデバイスでサポートされます。

ユニバーサル Windows プラットフォームの Cisco Secure Client 機能マトリックス

次のリモートアクセス機能は、ユニバーサル Windows プラットフォーム上の Cisco Secure Client でサポートされています。

カテゴリ：機能	ユニバーサル Windows プラットフォーム
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）	×
Cisco VPN プロファイルのサポート（接続中のインポート）	非対応
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
データグラム TLS (DTLS)	対応
IPsec IKEv2 NAT-T	×
IKEv2 - raw ESP	×
Suite B (IPSec のみ)	×
TLS 圧縮	×
デッド ピア検出	×

カテゴリ：機能	ユニバーサル Windows プラットフォーム
トンネル キープアライブ	×
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 (Advantage または Premier ライセンスと ASA 9.4.2 以降が必要)	非対応
フルトンネル (OS は、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に対して例外を発生させる可能性がある)	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 (スプリット除外)	×
Split-DNS	対応
自動再接続/ネットワーク ローミング	対応。ユーザが同じネットワーク上にとどまっており、ネットワーク接続が終了していない場合。
オンデマンド VPN (宛先により起動)	対応
オンデマンド VPN (アプリケーションによって起動)	非対応
キー再生成	×
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
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
プロキシ例外	非対応
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	×
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	×
最適ゲートウェイ選択	非対応

カテゴリ：機能	ユニバーサル Windows プラットフォーム
認証：	
SAML 2.0	非対応
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)	×
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
SCEP レガシー登録 (お使いのプラットフォームを確認してください)	×
SCEP プロキシ登録 (お使いのプラットフォームを確認してください)	×
自動証明書選択	対応
手動による証明書の選択	×
スマートカードのサポート	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：	
スタンドアロン GUI	対応 (機能制限があります)
ネイティブ OS GUI	対応
API/URI ハンドラ (以下を参照)	×
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	×
ユーザー設定	部分的に対応
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	×

カテゴリ：機能	ユニバーサル Windows プラットフォーム
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	×
ヘッドエンドと共有される OS および Cisco Secure Client のバージョン	対応
URI の処理：	
接続エントリの追加	×
VPN への接続	×
接続時のクレデンシャルの事前入力	×
VPN の解除	×
証明書のインポート	×
ローカリゼーションデータのインポート	×
XML クライアントプロファイルのインポート	×
URI コマンドの外部（ユーザー）制御	×
レポートおよびトラブルシューティング：	
統計	×
ロギング/診断情報（DART）	対応。Windows10 のディレクトリ 「C:\ProgramData\Cisco\SecureClient\Logs」からログを取得
認定：	
FIPS 140-2 レベル 1	非対応

ユニバーサル Windows プラットフォーム用 Cisco Secure Client 5.0.00907 の新機能

この 5.0.00907 バージョンでは、ユニバーサル Windows プラットフォーム用の新しい Cisco Secure Client（AnyConnect を含む）が導入され、次の新機能と既知の制限が含まれています。

— DTLS のサポート。この新機能には、次の注意事項があります。

- トンネルのキー再生成はサポートされていません。
- DTLS がブロックされている場合、3 秒の遅延が発生します。
- DTLS トンネルには TLS MTU が使用されます。
- フレームワークの制限により、トンネルはスリープ時とネットワーク移行時に切断されません。

- DTLS トンネル圧縮はサポートされていません。
- デッドピア検出 (DPD) はサポートされていません。

ARM64 デバイスでの UWP の既知の制限：証明書のしきい値警告がトリガーされると、常に残り 0 日が報告されます (CSCwd60132)。

Cisco Secure Firewall ASA の要件

Cisco Secure Firewall ASA リリース 8.0(3) および Adaptive Security Device Manager (ASDM) 6.1(3) は、モバイルデバイスの Cisco Secure Client をサポートする最小リリースです。次の機能を使用するには、Cisco Secure Firewall ASA の最小リリースが必要です。



(注) 現在の Cisco Secure Client モバイルリリースにおけるこれらの機能の可用性については、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：Cisco Secure Firewall ASA 9.7.1.24、9.8.2.28、9.9.2.1 以降。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：Cisco Secure Firewall ASA 9.3.2 以降。
- IPsec IKEv2 VPN、Suite B 暗号化、SCEP プロキシ、またはモバイルポスチャ：Cisco Secure Firewall ASA 9.0。

翻訳について

このドキュメントは、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。