Cisco Secure Client（AnyConnect を含む）リリース 5.1 リリースノート

初版：2023 年 7 月 27 日

最終更新：2023 年 12 月 13 日

Cisco Secure Client リリース 5.1.x.x リリースノート

このリリースノートには、Windows、macOS、および Linux 上の Cisco Secure Client に関する情報が記載されています。Secure Client デバイスは、常時接続のインテリジェント VPN を通じて最適なネットワーク アクセス ポイントを自動的に選択し、そのトンネリングプロトコルを最も効率的な方法に適応させます。

（注） Cisco Secure Client 5.1.x.x は、5.x.x.x のバグのメンテナンスパスになります。Cisco Secure Client 5.0.x.x のお客様は、今後の不具合修正を利用するために Cisco Secure Client 5.1.x.x にアップグレードする必要があります。Cisco Secure Client 5.0.x.x で見つかった不具合は、Cisco Secure Client 5.1.x.x メンテナンスリリースでのみ修正されます。

最新バージョンの Cisco Secure Client のダウンロード

始める前に

最新バージョンの Cisco Secure Client をダウンロードするには、Cisco.com に登録されたユーザーである必要があります。

手順

ステップ 1 Cisco Secure Client 製品のサポートページを参照します。

http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

ステップ 2 Cisco.com にログインします。

ステップ 3 [ソフトウェアのダウンロード（Download Software）] をクリックします。

ステップ 4 [最新リリース（Latest Releases）] フォルダを展開し、最新リリースをクリックします（まだ選択されていない場合）。

ステップ 5 次のいずれかの方法で Secure Client パッケージをダウンロードします。

- 1 つのパッケージをダウンロードする場合は、ダウンロードするパッケージを見つけて[ダウンロード（Download）] をクリックします。
- 複数のパッケージをダウンロードする場合は、目的のパッケージの横にある [カートに追加（Add to cart）] をクリックし、[ソフトウェアのダウンロード（Download Software）] ページの上部にある [カートのダウンロード（Download cart）] をクリックします。

ステップ 6 メッセージが表示されたら、シスコのライセンス契約書を読んで承認します。

ステップ 7 ダウンロードを保存するローカルディレクトリを選択し、[保存（Save）] をクリックします。

ステップ 8 Cisco Secure Client 管理者ガイド、リリース 5.x を参照してください。

Web 展開用の Cisco Secure Client パッケージファイル名

OS	Cisco Secure Client Web 展開パッケージ名
Windows	cisco-secure-client-win-バージョン-webdeploy-k9.pkg
macOS	cisco-secure-client-macos-バージョン-webdeploy-k9.pkg
Linux（64 ビット）*	cisco-secure-client-linux64-バージョン-webdeploy-k9.pkg

* RPM および DEB インストールの Web 展開は、現時のところサポートされていません。

事前展開用の Cisco Secure Client パッケージファイル名

OS	Cisco Secure Client 事前展開パッケージ名
Windows	cisco-secure-client-win-version-predeploy-k9.zip
macOS	cisco-secure-client-macos-version-predeploy-k9.dmg
Linux（64 ビット）	（スクリプトインストーラーの場合） cisco-secure-client-linux64-version-predeploy-k9.tar.gz （RPM インストーラ*の場合） cisco-secure-client-linux64-*version*-predeploy-rpm-k9.tar.gz （DEB インストーラ*の場合）cisco-secure-client-linux64-*version*-predeploy-deb-k9.tar.gz

*RPM および DEB インストーラで提供されるモジュール：VPN、DART

Cisco Secure Client への機能の追加に役立つその他のファイルもダウンロードできます。

Cisco Secure Client 5.1.2.42 の新機能

このリリースには次の機能とサポートの更新が含まれており、Cisco Secure Client 5.1.2.42 （40 ページ） に記載されている不具合を修正します。

- （CSCwh29292）ダイナミック スプリット トンネリングは、必要に応じて、トンネルからのダイナミック除外と、特定の設定に対応するトンネルへのダイナミック包含の両方を実行できるようになりました。たとえば、拡張ダイナミックスプリット除外トンネリングを使用すると、スタティックスプリット除外ネットワークをオーバーライドする必要がある場合、ダイナミック包含ドメインに一致するトラフィックをトンネルに動的に含めることができます。詳細については、『*Cisco Secure Client (including AnyConnect) Administrator Guide, Release 5*』の「About Dynamic Split Tunneling」を参照してください。
- プロファイルエディタで、[ロードバランシングサーバーリスト（Load Balancing Server List）]のホストアドレスの先頭または末尾にワイルドカードを追加できるようになりました。
- Windows の修正プログラムが利用可能になるまで PMF IGTK の設定を無効にするために、ネットワーク アクセス マネージャの追加機能を実装しました。Microsoft は、Windows 10 22H2 および Windows 11 21H2（およびそれ以降）の修正プログラムが 2024 年の前半に利用可能になると見積もっています。これにより、ネットワーク アクセス マネージャから IGTK を設定できるようになります。それまでは、PMF IGTK の設定を無効にしておけば、管理フレーム保護（PMF）を提供するように設定されたネットワークへ接続できます。Windows の修正プログラムがまだ利用できず、PMF が有効になっているネットワークへの接続を回避できない場合は、次のレジストリキーを DWORD として追加し、説明に従って設定することで Windows レジストリエディタを変更し、ネットワーク アクセス マネージャによる IGTK の使用を無効にする必要があります。

  ```
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\Cisco Secure Client Network Access
  Manager\DisableIGTK set to 1
  ```

（注） この IGTK の修正は、WPA2/WPA3 Enterprise ネットワークにのみ適用されます。WPA3 Personal（SAE）または WPA3 Open（OWE）には適用されません。ワイヤレス管理フレームを保護するため、必要な場合以外は PMF IGTK を無効にしないことを強くお勧めします。

- Zero Trust Access モジュール（5.1.2.5191）と相互運用するには、適切な AnyConnect VPN バージョン（5.1.1.42）が必要です。
- Windows 10 ARM64 のサポートは終了しました。

Cisco Secure Client 5.1.1.42 の新機能

このリリースには次の機能とサポートの更新が含まれており、Cisco Secure Client 5.1.1.42 （41 ページ） に記載されている不具合を修正します。

- Web 展開のアップグレードでの致命的なエラー（CSCwi37384）：Windows 11 ARM64 でのみ ASA または ISE を Web 展開すると、Cisco Secure Client 5.1.0.x から 5.1.1.x にアップグレードするときに致命的なエラーが発生します。Windows 11 ARM64 デバイスで Web 展開を機能させるには、回避策として Secure Client 5.1.0.x をアンインストールして 5.1.1.x を新規インストールする必要があります。または、事前展開を使用して、Windows 11 ARM64 デバイスで Secure Client 5.1.0.x から 5.1.1.x にアップグレードできます。
- Zero Trust Access モジュール（5.1.1.4867）と相互運用するには、適切な AnyConnect VPN バージョン（5.1.1.42）が必要です。
- macOS での Web 展開のアップグレードに管理者権限が必要（CSCwi69393）：新しい Apple API の変更により、webdeploy を使用して Cisco Secure Client 5.0.x（またはそれ以前）から 5.1.x（またはそれ以降）にアップグレードする場合は、管理者権限が必要です。または、MDM を介して macOS デバイスを管理して、アプリケーション拡張を事前承認します。
- Network Visibility Module への更新
  - Network Visibility Module を実行している Windows クライアントからの HTTP 1.1 フローの追加の収集パラメータとして HTTP ホストが追加されました。
  - 収集パラメータモジュール名リストを拡張し、Windows および macOS クライアントからの Chrome、Firefox、および MS Edge ブラウザフローのブラウザプラグイン情報（名前とバージョン）を含めるようにしました。
  - **既知の問題**：CSCwi48979：macOS の [HTTP ホスト（HTTP Host）] フィールドが、HTTP トラフィックの適切な宛先ホスト名を提示せずに空として報告される。
  - **既知の問題**：CSCwi49003：Network Visibility Module が macOS の Safari ブラウザプラグインを報告していない。
- **既知の問題**：CSCwi49850：macOS 12：キャプティブポータルの修復中に AnyConnect 組み込みブラウザでハイパーリンクが機能しない

Cisco Secure Client 5.1.0.136 の新機能

このリリースには次の機能とサポートの更新が含まれており、Cisco Secure Client 5.1.0.136 （42 ページ） に記載されている不具合を修正します。

- Zero Trust Access モジュール：アプリケーションを非表示にすることで攻撃対象領域を縮小し、ネットワーク上の誰と何を把握、理解、および制御するレベルを向上させます。Zero Trust Access モジュール（5.1.0.4464）と相互運用するには、適切な AnyConnect VPN バージョン（5.1.0.136）が必要です。現在、Zero Trust Access モジュールは Cisco Secure

Access サービスのみをサポートしています。詳細については、Secure Access のマニュアルを参照してください。

Cisco Secure Client から分離されているスタンドアロンのアプリケーションである Duo Desktop も、Zero Trust Access モジュールインストーラ（Windows および macOS 用）にパッケージ化されており自動的にインストールされます。ただし macOS では、Duo Desktop で証明書の展開のための追加のセットアップを行う必要があります。詳細については、「Getting Zero Trust Access Up and Running on Desktop」を参照してください。

（注） Duo Health Application（DHA）は、Duo Desktop にブランド変更されています。

DART は、Duo Desktop ログを収集するように拡張されました。Windows では、Duo トラブルシューティング スクリプトの実行が許可されている場合にのみ、DART は Duo Desktop ログを収集できます。Duo は PowerShell スクリプトを使用してログを収集します。

現在の制限事項または制約事項

- 複数のユーザーがエンドポイントに同時にログインしている場合、Zero Trust Access 機能は無効になります。
- サーバーが最初にトラフィックを送信するトンネリング アプリケーション（例：MySQL）はサポートされません。
- DART は macOS 5.1 の Duo Desktop ログを収集しません。
- macOS の Web 展開では、DART はアップグレードされません。エラーが表示され、DART 収集用に手動でインストールできます。
- ASDM では、Zero Trust Access はグループポリシー（[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）]>[Secure Client接続プロファイル編集グループポリシー、ダウンロードする高度なSecure Clientオプションモジュール（Secure Client Connection Profiles Edit Group-Policy, Advanced-Secure Client-Optional Modules to Download）]）ドロップダウンメニューにモジュールとして表示されません。不具合は、対処する ASDM チームに割り当てられています。

詳細、制限事項、および前提条件については、『*Cisco Secure Client（AnyConnect を含む）管理者ガイド、リリース 5.1*』の「Zero Trust Access モジュール」セクションを参照してください。

- ネットワーク アクセス マネージャに、WPA3 802.11 CCMP128 暗号化および保護された管理フレーム（PMF）のサポートが追加されました。ただし WPA3 は、Microsoft が完全性 Group Temporal Key（GTK）の生成に関連する修正をリリースするまで機能しません。この修正は実稼働環境では使用できませんが、今後の Windows 11 リリースおよび Windows 10 22H2 更新で修正されると予想されます。PMF は WPA2 で使用できますが、WPA3 Enterprise では必須です。PMF が必須またはオプションの WPA2 ネットワークがある場合、Microsoft が修正するまで Secure Client 5.1.0.136 への接続は失敗します。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.2.42 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.2.42 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.1.42 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.1.42 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれ、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.1.42 （44 ページ） に記載されている不具合が修正されています。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.0.136 の新機能

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.0.136 リリースには、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれ、Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.0.136 （44 ページ） に記載されている不具合が修正されています。

システム要件

ここでは、このリリースの管理要件とエンドポイント要件について説明します。各機能のエンドポイント OS のサポートとライセンス要件については、『Cisco Secure Client Features, Licenses, and OSs』[英語] を参照してください。

シスコは、他の VPN サードパーティクライアントとの互換性を保証できません。

Cisco Secure Client プロファイルエディタの変更

プロファイルエディタを起動する前に、Java（バージョン 8 以降）をインストールする必要があります。Cisco Secure Client プロファイルエディタは、OpenJDKだけでなく Oracle Java もサポートしています。特定の OpenJDK ビルドでは、JRE のパスを特定できなければ、プロファイルエディタの起動に失敗することがあります。インストール済みの JRE のパスに移動すると、プロファイルエディタを正しく起動するように求められます。

Cisco Secure Client の ISE 要件

- 警告：

  非互換性警告：2.0 以降を実行している Identity Services Engine（ISE）のお客様は、次に進む前にこちらをお読みください。

  ISE RADIUS はリリース 2.0 以降 TLS 1.2 をサポートしてきましたが、CSCvm03681 により追跡される TLS 1.2 を使用した EAP-FAST の ISE 導入に不具合が見つかりました。この不

具合は、ISE の 2.4p5 リリースで修正されました。この修正は、ISE のサポートされているリリース用の今後のホット パッチで提供されます。

上記のリリースより前の TLS 1.2 をサポートする ISE リリースの EAP-FAST を使用して、ネットワーク アクセス マネージャ 4.7（以降）が認証に使用される場合、認証は失敗し、エンドポイントはネットワークにアクセスできません。

- ISE 2.6（以降）と Cisco Secure Client 4.7MR1（以降）では、有線および VPN フローで IPv6 非リダイレクトフロー（ステージ 2 検出を使用）がサポートされます。
- Cisco Secure Client のテンポラル エージェント フローは、ネットワークトポロジに基づいて IPv6 ネットワークで機能します。ISE は、ネットワークインターフェイス（eth0/eth1 など）で IPv6 を設定する複数の方法をサポートしています。
- ISE ポスチャフローに関する IPv6 ネットワークには、（IPv6）ISE ポスチャ検出が特定のタイプのネットワークアダプタ（Microsoft Teredo 仮想アダプタなど）のために無限ループに陥る（CSCvo36890）という制限があります。
- ISE 2.0 は、Cisco Secure Client ソフトウェアをエンドポイントに展開し、Cisco Secure Client 4.0 以降の新しい ISE ポスチャモジュールを使用してそのエンドポイントをポスチャできる最小リリースです。
- ISE 2.0 は Cisco Secure Client リリース 4.0 以降だけを展開できます。Cisco Secure Client の旧リリースは、ASA から Web 展開するか、SMS で事前展開するか、手動で展開する必要があります。
- Cisco Secure Client ISE ポスチャモジュールをインストールまたは更新する場合、ASA で設定されたパッケージとモジュールは、ISE で設定されたものと同じである必要があります。VPN は、他のモジュールのアップグレード時に常にアップグレードされますが、トンネルがアクティブな場合、ISE からの VPN モジュールのアップグレードは許可されません。

ISE ライセンス要件

ISE ヘッドエンドから Cisco Secure Client を展開し、ISE ポスチャモジュールを使用するには、ISE 管理ノードに Cisco ISE Premier ライセンスが必要です。ISE ライセンスの詳細については、『Cisco Identity Services Engine Admin Guide』[英語] の「*Cisco ISE Licenses*」の章を参照してください。

Cisco Secure Client 用の Cisco Secure Firewall ASA の要件

特定の機能に関する最小 ASA/ASDM リリース要件

- Cisco Secure Client VPN SAML 外部ブラウザを使用するには、Cisco Secure Firewall ASA 9.17.x（またはそれ以降）と ASDM 7.17.x（またはそれ以降）にアップグレードする必要があります。そのバージョンと Cisco Secure Client バージョン 5 を使用すると、VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthN、FIDO2、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、認証の選択肢をさらに加えることができます。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML

を使用する場合は、Secure Client がSecure Client の組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。

- DTLSv1.2 を使用するには、Cisco Secure Firewall ASA 9.10.1 以降と ASDM 7.10.1 以降にアップグレードする必要があります。

（注） DTLSv1.2 は、5506-X、5508-X、および 5516-X を除くすべての Cisco Secure Firewall ASA モデルでサポートされており、ASA がクライアントとしてではなくサーバーとしてのみ機能している場合に適用されます。DTLS 1.2 は、現在のすべての TLS/DTLS 暗号方式と大きなCookieサイズに加えて、追加の暗号方式をサポートしています。

- 管理VPN トンネルを使用するには、ASDM 7.10.1 にアップグレードする必要があります。
- Network Visibility Module を使用するには、ASDM 7.5.1 にアップグレードする必要があります。
- AMP イネーブラを使用するには、ASDM 7.4.2 にアップグレードする必要があります。

（注） Cisco Secure Client リリース 5.0 には、AMP イネーブラは含まれていません。

- TLS 1.2 を使用するには、Cisco Secure Firewall ASA 9.3(2) にアップグレードする必要があります。
- 次の機能を使用する場合は、Cisco Secure Firewall ASA 9.2(1) にアップグレードする必要があります。
  - VPN を介した ISE ポスチャ
  - Cisco Secure Client の ISE 展開
  - ASA での認可変更（CoA）は、このバージョン以降でサポートされています。
- 次の機能を使用する場合は、Cisco Secure Firewall ASA 9.0 にアップグレードする必要があります。
  - IPv6 のサポート
  - シスコの次世代暗号化「Suite-B」セキュリティ
  - ダイナミック スプリット トンネリング（カスタム属性）

- Cisco Secure Client 遅延アップグレード
- 管理 VPN トンネル（カスタム属性）

- 次を実行する場合は、Cisco Secure Firewall ASA 8.4(1) 以降を使用する必要があります。
  - IKEv2 の使用。
  - ASDM による非 VPN クライアントプロファイル（ネットワーク アクセス マネージャなど）の編集。
  - ファイアウォールルールの展開。常時接続 VPN を展開するときは、スプリットトンネリングを有効にして、ローカル印刷デバイスとテザーモバイルデバイスへのネットワークアクセスを制限するファイアウォールルールを設定する必要がある場合があります。
  - 認定された VPN ユーザーを常時接続 VPN 展開から除外するダイナミック アクセス ポリシーまたはグループポリシーの設定。
  - Cisco Secure Client セッションが隔離されているときに Cisco Secure Client GUI にメッセージを表示するダイナミック アクセス ポリシーの設定。

- 4.3x から 4.6.x への Secure Firewall ポスチャ 移行を実行するには、ASDM 7.9.2 以降が必要です。

Cisco Secure Firewall ASA のメモリ要件

⚠

注意 Cisco Secure Client を使用するすべての Cisco Secure Firewall ASA モデルに推奨される最小フラッシュメモリは 512 MB です。これにより、ASA で複数のエンドポイント オペレーティング システムをホストし、ロギングとデバッグを有効にすることができます。

Cisco Secure Firewall ASA のフラッシュサイズの制限（最大 128 MB）により、Cisco Secure Client パッケージの一部の置換は、このモデルにロードできません。Cisco Secure Client を正常にロードするには、使用可能なフラッシュに収まるまでパッケージのサイズを小さくする必要があります（OS を減らす、Secure Firewall ポスチャ をなくすなど）。

Cisco Secure Client のインストールまたはアップグレードを続行する前に、使用可能なスペースを確認してください。これを行うには、次のいずれかの方法を使用できます。

- CLI：**show memory** コマンドを入力します。

```
asa3# show memory
Free memory:       304701712 bytes (57%)
Used memory:       232169200 bytes (43%)
-------------     ----------------
Total memory:      536870912 bytes (100%)
```

- ASDM：[Tools] > [File Management] を選択します。[ファイル管理（File Management）] ウィンドウにフラッシュスペースが表示されます。

Cisco Secure Firewall ASA にデフォルトの内部フラッシュメモリサイズかデフォルトの DRAM サイズ（キャッシュメモリ用）だけがある場合、ASA 上で複数の Cisco Secure Client パッケージを保存およびロードすると、問題が発生することがあります。フラッシュメモリにパッケージファイルを保持するために十分な容量がある場合でも、クライアントイメージの unzip とロードのときに Cisco Secure Firewall ASA のキャッシュメモリが不足する場合があります。ASA のメモリ要件と ASA のメモリアップグレードの詳細については、Cisco ASA の最新のリリースノートを参照してください。

Secure Firewall ポスチャ

Cisco Secure Client 5.0.x は、Secure Firewall Posture 5.0.x（またはそれ以降）を**使用する必要があります**。

（注） Cisco Secure Client 5.0.x は、互換性のないバージョンの HostScan と使用すると、VPN 接続を確立しません。したがって、Cisco Secure Client 5.0.x エンドポイントでの HostScan 4.x の使用はサポートされていません。

現在 **HostScan 4.3.x 以前**を使用している場合は、HostScan の新しいバージョンにアップグレードする前に、1 回限りの HostScan の移行を**実行する必要があります**。この移行の詳細については、『AnyConnect HostScan Migration 4.3.x to 4.6.x and Later』を参照してください。

また、Secure Firewall ポスチャ と ISE ポスチャの併用は推奨されません。2 つの異なるポスチャエージェントを実行する場合、予期しない結果が発生します。

Cisco Secure Firewall ポスチャモジュール（旧 HostScan）により、Cisco Secure Client は、Cisco Secure Firewall ASA のホストにインストールされているオペレーティングシステム、マルウェア対策、およびファイアウォールの各ソフトウェアを識別できます。

Start Before Login（SBL）および Secure Firewall ポスチャ を使用する場合、SBL は事前ログインであるため、完全な Secure Firewall ポスチャ 機能を実現するには、Cisco Secure Client 事前展開モジュールをエンドポイントにインストールする必要があります。

Secure Firewall Posture（独自のソフトウェアパッケージとして入手可能）は、新しいオペレーティングシステム、マルウェア対策、およびファイアウォール ソフトウェアの情報で定期的に更新されます。最新バージョンの Secure Firewall Posture（Cisco Secure Client のバージョンと同じ）を実行することをお勧めします。

Secure Firewall ポスチャ マルウェア対策およびファイアウォール サポート チャートは、Cisco.com で入手できます。

ISE ポスチャ準拠モジュール

（CSCwa91572）互換性と展開の容易さを実現するには、Cisco Secure Client バージョン 5.0.01242 以降で次のコンプライアンスモジュールを使用する必要があります（Windows バージョン 4.3.2755、macOS バージョン 4.3.2379、および Linux バージョン 4.3.2063）。また、すでにリリースされているコンプライアンスモジュールは、Cisco Secure Client バージョン 5.0.01242（およびそれ以降）のビルドではサポートされていません。

（CSCvy53730-Windows のみ）AnyConnect 4.9.06037 の時点では、ISE からコンプライアンスモジュールを更新できません。この変更により、AnyConnect 4.9.06037（およびそれ以降）と Cisco Secure Client 5（5.0.01242 まで）にはバージョン 4.3.1634.6145 以降のコンプライアンスモジュールが必要です。

ISE ポスチャ準拠モジュールには、ISE ポスチャでサポートされているマルウェア対策とファイアウォールのリストが含まれています。Secure Firewall ポスチャ のリストはベンダー別に編成されていますが、ISE ポスチャのリストは製品タイプ別に編成されています。ヘッドエンド（ISE または Cisco Secure Firewall ASA）のバージョン番号がエンドポイントのバージョンよりも大きい場合は、OPSWAT が更新されます。これらのアップグレードは必須であり、エンドユーザーの介入なしで自動的に実行されます。

ライブラリ（zip ファイル）内の個別のファイルは、OPSWAT, Inc. によってデジタル署名され、ライブラリ自体はシスコの証明書によって署名されたコードである単一の自己解凍実行可能ファイルとしてパッケージ化されています。詳細については、ISE コンプライアンスモジュールを参照してください。

Cisco Secure Client における iOS のサポート

シスコでは、セキュアゲートウェイとして機能する iOS リリース 15.1(2)T への AnyConnect VPN アクセスをサポートしています。 ただし、iOS リリース 15.1(2)T は現在、次の Cisco Secure Client 機能をサポートしていません。

- ログイン後の VPN 常時接続
- 接続障害ポリシー
- ローカル プリンタおよびテザーデバイスへのアクセスを提供するクライアント ファイアウォール
- 最適ゲートウェイ選択
- 検疫
- Cisco Secure Client プロファイルエディタ
- DTLSv1.2

AnyConnect VPN に関する IOS サポートのその他の制限については、「Features Not Supported on the Cisco IOS SSL VPN」[英語] を参照してください。

その他の IOS 機能のサポート情報については、http://www.cisco.com/go/fn [英語] を参照してください。

Cisco Secure Client がサポートするオペレーティングシステム

次の表に、サポートされている最小バージョンを示します。*8.x* などとは対照的に、特定のバージョンが示されているのは、特定のバージョンのみがサポートされているためです。たとえば、ISE ポスチャは Red Hat 8.0 ではサポートされていませんが、Red Hat 8.1 以降ではサポートされており、そのように記載しています。

表 *1 : Windows*

Windows のバージョン	VPN	Network Access Manager	Secure Firewall ポスチャ	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック	ネットワーク可視性モジュール	AMP イネーブラ	Umbrella ローミングセキュリティ	Tetra Endpoint Agent
Windows 11（64 ビット）と現在 Microsoft がサポートしているバージョンの Windows 10 x86（32 ビット）および x64（64 ビット）	対応	対応	対応	対応	対応	対応	対応	×	対応	対応
ARM64 ベースの PC 用に Microsoft がサポートしているバージョンの Windows 11	対応	×	対応	対応	対応	対応	対応	×	対応	×

表 *2 : macOS*

macOS のバージョン	VPN	Network Access Manager	Secure Firewall ポスチャ	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック	ネットワーク可視性モジュール	AMP イネーブラ	Umbrella ローミングセキュリティ	Tetra Endpoint Agent
macOS 14 Sonoma、macOS 13 Ventura、macOS 12 Monterey、および macOS 11 Big Sur	対応	×	対応	対応	対応	対応	対応	対応	対応	macOS 10.10 以降

表 *3 : Linux*

Linux のバージョン	VPN	Secure Firewall ポスチャ	ネットワーク可視性モジュール	ISE ポスチャ	DART	カスタマーエクスペリエンスのフィードバック
Red Hat	9.x および 8.x	9.x および 8.x	9.x および 8.x	9.x および 8.1（およびそれ以降）	対応	対応
Ubuntu	22.04 および 20.04	22.04 および 20.04	22.04 および 20.04	22.04 および 20.04	対応	対応
SUSE（SLES）	制限付きのサポート。ISE ポスチャのインストールにのみ使用	未サポート	未サポート	12.3（以降のバージョン）および 15.0（以降のバージョン）	対応	対応

Cisco Secure Client における Microsoft Windows のサポート

Windows の要件

- Pentium クラス以上のプロセッサ。
- 100 MB のハードディスク容量。
- Microsoft インストーラバージョン 3.1。
- 以前の Windows リリースから Windows 8.1 にアップグレードするには、Cisco Secure Client をアンインストールし、Windows のアップグレードが完了した後に再インストールする必要があります。
- Windows XP からそれ以降の Windows リリースにアップグレードする場合は、アップグレード時に Cisco Secure Client 仮想アダプタが保存されないため、クリーンインストールが必要です。Cisco Secure Client を手動でアンインストールし、Windows をアップグレードしてから手動で（または WebLaunch を介して）Cisco Secure Client を再インストールしてください。

- WebLaunch で Cisco Secure Client を起動するには、32 ビットバージョンの Firefox 3.0 以降を使用し、ActiveX を有効にするか Sun JRE 1.4 以降をインストールする必要があります。
- Windows 8 または 8.1 を使用する場合は ASDM バージョン 7.02 以降が必要です。

Windows の制約事項

- リリース 4.10.03104 より前の AnyConnect では、Windows ADVERTISE インストーラアクションはサポートされていませんでした（CSCvw79615）。リリース 4.10.03104 以降では、下位バージョンの AnyConnect を使用している場合に Windows ADVERTISE とともに正常にアップグレードするための修正が提供されています。ただし、AnyConnect バージョン 4.10.02086 以前（4.10.03104 以降ではなく）がアドバタイズされている場合は、今後のアップグレードが失敗する可能性があることに留意してください。
- Cisco Secure Client は、Windows RT ではサポートされません。このオペレーティングシステムでは、この機能を実装するための API が提供されません。シスコでは、この問題に関して Microsoft にオープンな要求を行っています。この機能をご希望の場合は、Microsoft に連絡して関心があることを表明してください。
- 他のサードパーティ製品と Windows 8 には互換性がないため、Cisco Secure Client はワイヤレスネットワーク経由で VPN 接続を確立できません。以下に、この問題の 2 つの例を示します。
  - Wireshark と共に配布されている WinPcap サービス「Remote Packet Capture Protocol v.0 (experimental)」は、Windows 8 をサポートしていません。

    この問題を回避するには、Wireshark をアンインストールするか WinPcap サービスを無効にして Windows 8 コンピュータを再起動し、Cisco Secure Client の接続を再試行します。
  - Windows 8 をサポートしない古いワイヤレスカードまたはワイヤレスカードドライバは、Cisco Secure Client による VPN 接続の確立を妨げます。

    この問題を回避するには、Windows 8 コンピュータが Windows 8 をサポートする最新のワイヤレス ネットワーク カードまたはドライバを備えていることを確認してください。
- Cisco Secure Client は、Windows 8 に導入されている Metro デザイン言語と呼ばれる新しい UI フレームワークと統合されません。ただし、Cisco Secure Client は Windows 8 においてデスクトップモードで動作します。
- HP Protect Tools は、Windows 8.x 上の Cisco Secure Client と連動しません。
- スタンバイをサポートするシステムでネットワーク アクセス マネージャを使用する場合は、デフォルトの Windows 8.x アソシエーションタイマー値（5 秒）を使用することをお勧めします。Windows でのスキャンリストの表示が予想より短い場合は、ドライバがネットワークスキャンを完了してスキャンリストに入力できるように、アソシエーションタイマーの値を増やしてください。

Windows での注意事項

- クライアントシステム上のドライバが、お使いの Windows のバージョンでサポートされていることを確認してください。サポートされていないドライバは、断続的な接続上の問題を発生させる可能性があります。
- ネットワーク アクセス マネージャについては、Microsoft KB 2743127 に記載されているレジストリ修正がクライアントデスクトップに適用されていないかぎり、マシンパスワードを使用するマシン認証が Windows 8 または 10/Server 2012 では機能しません。この修正には、DWORD 値 LsaAllowReturningUnencryptedSecrets を HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa レジストリキーに追加し、この値を 1 に設定することが含まれます。

  （マシンパスワードではなく）マシン証明書を使用したマシン認証では変更は不要であり、より安全なオプションです。マシンパスワードは暗号化されていない形式でアクセスできるため、Microsoft は特別なキーが必要になるように OS を変更しました。ネットワーク アクセス マネージャはオペレーティングシステムと Active Directory サーバー間で確立されたパスワードを認識できず、上記のキーを設定することによってのみパスワードを取得できます。この変更により、Local Security Authority（LSA）が Cisco Network Access Manager などのクライアントにマシンパスワードを提供できるようになります。

（注） マシン認証では、ユーザーがログインする前にクライアントデスクトップをネットワークに対して認証できます。その間、管理者は、このクライアントマシンに対してスケジュールされた管理タスクを実行できます。RADIUS サーバーが特定のクライアントに関してユーザーとマシンの両方を認証できる EAP チェーン機能にもマシン認証が必要です。これにより、企業資産が特定され、適切なアクセスポリシーが適用されます。たとえば、それが個人資産（PC/ラップトップ/タブレット）である場合、企業のログイン情報が使用されると、エンドポイントはマシン認証に失敗しますが、ユーザー認証は成功し、ユーザーのネットワーク接続に適切なネットワークアクセス制限が適用されます。

- Windows 8 では、[環境設定（Preferences）] > [VPN] > [統計（Statistics）] タブの [統計のエクスポート（Export Stats）] ボタンをクリックすると、ファイルがデスクトップに保存されます。他のバージョンの Windows では、ユーザーは、ファイルを保存する場所を尋ねられます。
- AnyConnect VPN は、WWAN アダプタを介して Windows と連動する 3G/4G/5G データカードと互換性があります。

Cisco Secure Client における Linux のサポート

Linux の要件

- GUI セッション（SSH など）を使用しない VPN CLI の使用はサポートされていません。
- インストールするには管理者権限が必要です。
- x86 命令セット
- 64 ビットプロセッサ
- 100 MB のハードディスク容量
- Linux カーネルでの TUN のサポート
- libnss3 (NSS 証明書ストアを使用している場合のみ)
- libstdc++ 6.0.19（GLIBCXX_3.4.19）以降
- iptables 1.4.21 以降
- NetworkManager 1.0.6 以降
- zlib（SSL deflate 圧縮をサポートするため）
- glib 2.36 以降
- polkit 0.105 以降
- gtk 3.8 以降
- systemd
- webkitgtk+ 2.10 以降（Cisco Secure Client 組み込みブラウザアプリケーションを使用する場合にのみ必要）
- libnm（libnm.so または libnm-glib.so）：Network Visibility Module を使用する場合にのみ必要

Cisco Secure Client における macOS のサポート

macOS の要件

- Cisco Secure Client には、50 MB のハードディスク容量が必要です。
- macOS で正しく動作させるには、Cisco Secure Client の最小ディスプレイ解像度を 1,024 X 640 ピクセルに設定する必要があります。

macOS での注意事項

- macOS 用の Cisco Secure Client 4.8（以降）が認証され、インストーラ ディスク イメージ（dmg）がステープルされました。

- macOS 10.15 でのアクセス制御の導入により、Cisco Secure Firewall Posture（旧 HostScan）または ISE ポスチャがエンドポイントでスキャンを実行しているときに、追加のポップアップが表示される場合があります。アクセスしてスキャンできるファイルとフォルダを承認する必要があります。

Cisco Secure Client のライセンス

最新のエンドユーザーライセンス契約書については、『End User License Agreement, 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、『Open Source Software Used in Cisco Secure Client』[英語] を参照してください

ISE ヘッドエンドから Cisco Secure Client を展開し、ISE ポスチャモジュールを使用するには、ISE 管理ノードに Cisco ISE Premier ライセンスが必要です。ISE ライセンスの詳細については、『Cisco Identity Services Engine 』[英語] の「*Cisco ISE Licenses*」の章を参照してください。

Cisco Secure Firewall ASA ヘッドエンドから Cisco Secure Client を展開して VPN と Secure Firewall ポスチャ モジュールを使用するには、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も使用できます。『Cisco Secure Client Ordering Guide』[英語] を参照してください。

Advantage および Premier ライセンスの概要と各機能で使用されるライセンスの説明については、『Cisco Secure Client Features, Licenses, and OSs』[英語] を参照してください。

Cisco Secure Client のインストールの概要

Cisco Secure Client の展開は、Cisco Secure Client と関連ファイルのインストール、設定、アップグレードを意味します。Cisco Secure Client は、次の方法によってリモート ユーザに展開できます。

- 事前展開：新規インストールとアップグレードは、エンドユーザによって、または社内のソフトウェア管理システム（SMS）を使用して実行されます。
- Web 展開：Cisco Secure Client パッケージは、ヘッドエンド（Cisco Secure Firewall ASA または ISE サーバー）にロードされます。ユーザが Cisco Secure Firewall ASA または ISE に接続すると、Cisco Secure Client がクライアントに展開されます。
  - 新規インストールの場合、ユーザーはヘッドエンドに接続して Cisco Secure Client をダウンロードします。クライアントは、手動でインストールするか、または自動（Web 起動）でインストールされます。
  - アップデートは、Secure Client がすでにインストールされているシステムで Cisco Secure Client を実行すること、またはユーザーを Cisco Secure Firewall ASA クライアントレスポータルに誘導することによって行われます。

- SecureX クラウド管理：SecureX UI の [展開の管理（Deployment Management）] ページにある [ネットワークインストーラ（Network Installer）] ボタンをクリックします。これにより、インストーラの実行可能ファイルがダウンロードされます。有効にする Secure Client オプション（Start Before Login、診断およびレポートツール、Cisco Secure Firewall ポスチャ、Network Visibility Module、Secure Umbrella、ISE ポスチャ、ネットワーク アクセス マネージャなど）も選択できます。

Cisco Secure Client を展開するときに、追加機能を有効にするオプションモジュールや VPN などの機能を設定するクライアントプロファイルを含めることができます。次の点を考慮してください。

- Cisco Secure Client モジュールおよびプロファイルはすべて事前展開できます。事前展開時には、モジュールのインストール手順やその他の詳細に特に注意する必要があります。
- VPN ポスチャモジュールによって使用されるカスタマー エクスペリエンス フィードバック モジュールと Secure Firewall ポスチャ パッケージは、ISE から Web 展開できません。
- ISE ポスチャモジュールによって使用されるコンプライアンスモジュールは、Cisco Secure Firewall ASA から Web 展開できません。

（注） 新しい Cisco Secure Client パッケージにアップグレードする場合は、必ずローカリゼーション MST ファイルを CCO の最新リリースで更新してください。

64 ビット Windows で Web ベースのインストールに失敗する場合がある

この問題は、Windows 8 上の Internet Explorer バージョン 10 および 11 に該当します。

Windows レジストリエントリ HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\TabProcGrowth が 0 に設定されている場合、Cisco Secure Client の Web 展開時に Active X で問題が発生します。

詳細については、http://support.microsoft.com/kb/2716529 を参照してください。

解決策は次のとおりです。

- 32 ビットバージョンの Internet Explorer を実行します。
- レジストリエントリを 0 以外の値に編集するか、レジストリからその値を削除します。

（注） Windows 8 では、Windows のスタート画面から Internet Explorer を起動すると 64 ビットバージョンが実行されます。デスクトップから起動すると 32 ビットバージョンが実行されます。

Cisco Secure Client サポートポリシー

シスコでは、最新の バージョン 5 リリースに基づいてのみ 5.x の修正と拡張機能を提供しています。TAC サポートは、Cisco Secure Client バージョン 5 のリリースバージョンを実行するアクティブな Cisco Secure Client バージョン 5 の契約期間を持つすべてのユーザーが利用できます。古いソフトウェアバージョンで問題が発生した場合は、現在のメンテナンスリリースで問題を解決できるかどうかの確認を求められることがあります。

Software Center へのアクセスは、最新の修正が適用された Cisco Secure Client バージョン 5 バージョンに制限されます。展開する予定のバージョンが将来もダウンロードできることを保証できないため、展開用にすべてのイメージをダウンロードすることをお勧めします。

注意事項と制約事項

macOS 13 以降での Web 展開のアップグレードに必要な管理者権限

新しい OS の要件により、5.0.x 以前から 5.1.x 以降へ Web 展開をアップグレードする場合は、1 回限りの管理者権限が必要です。以降の更新では必要ありません。この制限は、MDM を介して macOS デバイスを管理し、アプリケーションを事前承認することで回避できます。

IE11 の廃止後に発生する組み込みブラウザの変更

IE11 の廃止により、Cisco Secure Client の組み込みブラウザはデフォルトで WebView2 になります（ランタイムがインストールされている場合）。従来の組み込みブラウザによる制御に戻す必要がある場合は、1 に設定された DWORD レジストリ値 *UseLegacyEmbeddedBrowser* を次の Windows レジストリキーに追加します。

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Cisco\Cisco Secure Client
```

暗号化された DNS の影響とその影響の軽減

暗号化されたドメインネームシステム（DNS）の解決は、Secure Client の機能に影響します。具体的に言うと、暗号化された DNS を介して解決される FQDN をターゲットとするネットワークフローは、Secure Client の次の機能により、回避されるか、適切に処理されません：Cisco Umbrella DNS の保護、Cisco Umbrella Web の保護（名前ベースのリダイレクトルールが使用されている場合）、AnyConnect VPN（ダイナミック スプリット トンネリングと名前ベースの例外のある常時接続）、Network Visibility（ピア FQDN のレポート）、および Zero Trust Access（名前ベースのルールが適用されている場合）。このような影響を軽減するには、Secure Client ユーザーに関するブラウザ設定で暗号化された DNS を無効にする必要があります。

追加の軽減策として、Cisco Secure Client は、ローカルポリシー設定を介した Windows DNS クライアントの DNS over HTTPS（DoH）名前解決（**DNS over HTTP（DoH）名前解決の設定**（[コンピュータの設定（Computer Configuration）] > [管理テンプレート（Administrative Templates）] > [ネットワーク（Network）] > [DNSクライアント（DNS Client）]））を禁止します。この変更は、Windows 11 以降のバージョンに該当するものであり、VPN、Cisco Umbrella

ローミングセキュリティ、またはNetwork Visibilityのいずれかのモジュールがアクティブなときに適用されます。（ドメインGPO設定などの）優先順位の高い競合設定が検出された場合、Cisco Secure Clientはこのポリシー設定を変更しません。

Windows ARM64 の既知の問題

Windows ARM64 の既知の問題は次のとおりです。

- CSCwh12493：ASDMがエラーをスローし、ARM64のISEポスチャプロファイルでセキュア クライアント プロファイル エディタをロードできない
- CSCwd81735：Cisco Secure Firewall ASA で Cisco Secure Firewall ポスチャ（以前の HostScan）が有効になっていて、Secure Client と同じ 5.0 バージョンを実行している場合、障害が発生する可能性がある。ただし、Secure Client UI にはステータスメッセージもエラーも表示されない。クライアントは引き続き正常に機能しており、[接続（Connect）] をクリックすると応答するが、ステータスメッセージには何も表示されない。
- CSCwd71408：ASA は、スクリプトを機能させるために、Cisco Secure Client バイナリファイルのカスタマイズのサポートを追加する必要がある。
- CSCwh63153：Windows ARM CP が設定されていないが、エージェントがすでにインストールされている場合、ダウンローダーの起動に失敗するエラー
- ISE ポスチャサービスを使用できない。csc_ise_agent を手動で再起動すると、サービスを復元できる。
- Java の ARM64 バージョンがサポートされていない。X86 または X64 バージョンのみサポートされる。
- ARM64 プラットフォームの Network Visibility Module の場合、モジュール名とモジュールハッシュが、SVCHost プロセス用に生成されたフローで報告されない。
- XDR ポータルからの Cisco Secure Client 5.1.0.136 以降のインストールは、ARM64 ではサポートされていない。

有線接続による RDP が機能しない

リモートデバイスからの Windows リモート デスクトップ プロトコルの試行中にネットワークアクセスマネージャがマシンまたはユーザー認証用に設定されている場合、接続が失敗する可能性があります。この障害の原因は、Microsoftファイアウォールがネットワークの検疫を確立する方法におけるインターフェイスの変更です。Microsoft と解決策を調整できるまでは、CSCvo47467 に記載されている回避策を試すことができます。

同時 VPN セッションはサポートされない

AnyConnect VPN は、他のクライアント VPN（ユニバーサル Windows プラットフォーム用の Cisco Secure Client のようなシスコソフトウェア、またはサードパーティの VPN のいずれか）と同時にアクティブにできません。

macOS 13 の既知の問題

現時点では、macOS 13 の Continuity Camera はアクティブな VPN 接続中は機能していません。

macOS 12.x での DNS（名前解決）が失敗することがある

macOS 12.x で Cisco Secure Client を実行している場合、DNS（名前解決）が失われ、復元のために再起動が必要になる場合があります。この問題の原因は macOS のバグとして特定されており、macOS 12.3（FB9803355）で解決されています。

Windows のローカルグループポリシーの DNS 設定は無視される

グローバル DNS 設定の Searchlist と UseDomainNameDevolution は、VPN 接続の DNS サフィックス検索リストを作成するために Cisco Secure Client で使用されます。ローカルグループポリシーを使用して設定されたオーバーライドはすべて無視されます。

ルート CA と Firefox NSS ストアの競合（Linux のみ）

ルート認証局（CA）が公的に信頼されている場合、その CA はすでにファイル証明書ストアにあります。ただし、シスコではファイル証明書ストアでの OCSP チェックのみをサポートしているため、Firefox NSS ストアが同時に有効になっていると、OCSP チェックがバイパスされる可能性があります。こうしたバイパスを防ぐには、ローカルポリシーファイルで ExcludeFirefoxNSSCertStore を *true* に設定して Firefox NSS ストアを無効にします。

TND との自動 VPI 接続の開始（CSCvz02896）

信頼ネットワーク検出を使用している場合、システムルートテーブルにデフォルトルートが含まれていなければ、TND ポリシーに従って自動 VPN 接続が開始されないことがあります。

Linux での AnyConnect 4.10 アップグレードの失敗（4.9.01095 よりも前の AnyConnect バージョンのみ）

Web 展開を使用して 4.9.01095 より前のバージョンから AnyConnect または HostScan 4.10 にアップグレードすると、エラーが発生する可能性があります。バージョン 4.9.01095 よりも前の AnyConnect にはシステム CA ストアを解析する能力がなく、ユーザーのプロファイルディレクトリで正しい NSS 証明書ストアのパスを特定できないため、アップグレードが失敗します。4.9.01095 より前のリリースから AnyConnect 4.10 にアップグレードする場合は、エンドポイントで AnyConnect をアップグレードする前に、ルート証明書（DigiCertAssuredIDRootCA.pem）を /opt/.cisco/certificates/ca にコピーします。

Ubuntu 20 で NVM のインストールが失敗する

（カーネルバージョンが 5.4 の）Ubuntu 20.04 を使用している場合は、AnyConnect 4.8 以降を使用する必要があります。そうしないと Network Visibility Module のインストールに失敗します。

ローカルおよびネットワークのプロキシの非互換性

ローカルやネットワークのプロキシ（Web HTTP/HTTPS インスペクションや復号の機能を含む、Fiddler、Charles Proxy、またはサードパーティ製マルウェア対策/セキュリティソフトウェアなどのソフトウェア/セキュリティ アプリケーション）は、Cisco Secure Client と互換性がありません。

Linux での Web 展開ワークフローの制限事項

Linux で Web 展開を行う場合は、次の 2 つの制限事項を考慮してください。

- Ubuntu NetworkManager の接続確認機能を使用すると、インターネットにアクセスできるかどうかを定期的にテストできます。接続確認には独自のプロンプトがあるため、インターネット接続のないネットワークが検出された場合は、ネットワーク ログオン ウィンドウを表示できます。ブラウザウィンドウに関連付けられておらず、ダウンロード機能がないネットワークプロンプトを回避するには、Ubuntu 17 以降で接続確認を無効にする必要があります。無効にすることで、ユーザーは ISE ベースの Cisco Secure Client Web 展開用にブラウザを使用して ISE ポータルからファイルをダウンロードできます。
- Linux エンドポイントに Web 展開を行う前に、xhost+ コマンドを使用してアクセス制御を無効にする必要があります。xhost は、デフォルトで制限されているエンドポイントで端末を実行しているリモートホストのアクセスを制御します。アクセス制御を無効にしないと、Cisco Secure Client Web 展開は失敗します。

AnyConnect 4.9.01xxx へのアップグレード後にクライアントの最初の自動再接続が失敗する（Linux のみ）

CSCvu65566 の修正とそのデバイス ID 計算の変更により、Linux の特定の展開（特に LVM を使用する展開）では、ヘッドエンドから 4.9.01xxx 以降に更新した直後に 1 回限りの接続試行エラーが発生します。AnyConnect 4.8 以降を実行し、自動更新（Web 展開）を実行するためにヘッドエンドに接続している Linux ユーザーは、次のエラーを受け取る場合があります。「セキュアゲートウェイが接続試行を拒否しました。同じまたは別のセキュアゲートウェイへの新しい接続の試行が必要であり、再認証が必要です。（The secure gateway has rejected the connection attempt. A new connection attempt to the same or another secure gateway is needed, which requires re-authentication.）」正常に接続するには、Cisco Secure Client のアップグレード後に別の VPN 接続を手動で開始します。4.9.01xxx 以降に最初にアップグレードした後は、この問題は発生しません。

AnyConnect 4.7MR4 からのアップグレード後のワイヤレスネットワークへの接続に関する潜在的な問題

ネットワーク アクセス マネージャは、メモリ内の一時プロファイルを使用するのではなく、ワイヤレス LAN プロファイルをディスクに書き込むように改訂されました。Microsoft は OS のバグに対処するためにこの変更を要求しましたが、[ワイヤレスLANデータの使用状況（Wireless LAN Data Usage）] ウィンドウがクラッシュし、最終的に断続的なワイヤレス接続の問題が発生しました。これらの問題を防ぐために、ネットワーク アクセス マネージャを、

メモリ内の元の一時的な WLAN プロファイルを使用するように戻しました。ネットワーク アクセス マネージャは、バージョン 4.8MR2 以降にアップグレードするときに、ディスク上のほとんどのワイヤレス LAN プロファイルを削除します。一部のハードプロファイルは、指示されたときに OS WLAN サービスによって削除できませんが、ネットワーク アクセス マネージャがワイヤレスネットワークに接続する機能を妨げるものがあります。4.7MR4 から 4.8MR2 へのアップグレード後にワイヤレスネットワークへの接続に問題が発生した場合は、次の手順を実行します。

1. Secure Client ネットワーク アクセス マネージャ サービスを停止します。
2. 管理者のコマンドプロンプトから、次のように入力します

```
netsh wlan delete profile name=*(AC)
```

これにより、以前のバージョン（Secure Client 4.7MR4 ー 4.8MR2）から残りのプロファイルが削除されます。または、名前に **AC** が追加されたプロファイルを検索し、ネイティブサプリカントから削除することもできます。

nslookup コマンドを予期したように機能させるには macOS の修正が必要

macOS 11 では、nslookup コマンドに関連する AnyConnect バージョン 4.8.03036 以降で発生した問題（split-include トンネリング構成で nslookup が VPN トンネルを介して DNS クエリを送信しない問題）が修正されました。この問題は、不具合 CSCvo18938 の修正がそのバージョンに含まれていた場合に AnyConnect 4.8.03036 で発生します。Apple が提案したその不具合の変更により、nslookup の問題動作を引き起こす別の OS の 問題が明らかになりました。

macOS 10.x の回避策として、VPN DNS サーバーをパラメータとして nslookup に渡すことができます（**`nslookup [name] [ip_dnsServer_vpn]`**）。

サーバー証明書の検証エラー

（CSCvu71024）Cisco Secure Firewall ASA ヘッドエンドまたは SAML プロバイダーが AddTrust ルート（またはいずれかの仲介者）によって署名された証明書を使用する場合、2020 年 5 月に期限切れになるため、Cisco Secure Client 認証が失敗する場合があります。期限切れの証明書は、オペレーティングシステムが 2020 年 5 月の有効期限に対応するのに必要な更新を行うまで、Cisco Secure Client の失敗の原因となり、サーバー証明書検証エラーとして表示されます。

Windows DNS クライアントの最適化に関する注意事項

Windows 8 以降の Windows DNS クライアント最適化では、スプリット DNS が有効になっている場合に、特定のドメイン名の解決に失敗する可能性があります。回避策は、次のレジストリキーを更新して、このような最適化を無効にすることです。

```
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters

Value:DisableParallelAandAAAA

Data: 1

Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient

Value: DisableSmartNameResolution
```

```
Data: 1
```

macOS 10.15 ユーザーの準備

macOS 10.15 オペレーティングシステムでは、32 ビットのバイナリがサポートされません。さらに、10.15 にインストールされているすべてのソフトウェアは、デジタル署名によって暗号的に認証されていることが Apple に確認されます。AnyConnect 4.8 以降、macOS 10.15 での操作は 32 ビットコードなしでサポートされます。

次の制限事項に注意してください。

- 4.7.03052 よりも前の AnyConnect バージョンでは、アップグレードにアクティブなインターネット接続が必要な場合があります。
- 4.8.x より前の HostScan バージョンは、macOS 10.15 では機能しません。
- macOS 10.15 で Secure Firewall ポスチャ と ISE ポスチャ を使用する場合、初回起動時に権限ポップアップが表示されます。

Secure Firewall ポスチャ はアップグレードなしの macOS 10.15 では機能しない（CSCvq11813）

4.8.x より前の HostScan パッケージは、macOS Catalina（10.15）では機能しません。4.8.x より前の HostScan パッケージを実行しているエンドユーザーが macOS Catalina から Cisco Secure Firewall ASA ヘッドエンドに接続しようとすると、VPN 接続を正常に完了できず、ポスチャ評価失敗メッセージを受信します。

macOS Big Sur (11.x) 上の AnyConnect 4.10.x クライアントでは、HostScan 4.9.04045 以降を使用する必要があります。

Secure Firewall ポスチャ ユーザが VPN 接続を正常に行えるようにするには、すべての DAP ポリシーと Secure Firewall ポスチャ ポリシーが HostScan 4.8.00175 （以降）に準拠していなければなりません。HostScan 4.3.x から 4.8.x へのポリシー移行に関するその他の情報については、『AnyConnect HostScan Migration 4.3.x to 4.6.x and Later』[英語] を参照してください。

VPN 接続を復元するための回避策として、Cisco Secure Firewall ASA ヘッドエンドに Secure Firewall ポスチャ パッケージを使用するシステムの管理者が Secure Firewall ポスチャ を無効にする方法があります。無効にすると、すべての Secure Firewall ポスチャ のポスチャ機能、およびエンドポイント情報に依存する DAP ポリシーは使用できなくなります。

関連する Field Notice については、https://www.cisco.com/c/en/us/support/docs/field-notices/704/fn70445.html [英語] を参照してください。

Secure Firewall ポスチャ またはISE ポスチャの初回起動時の権限ポップアップ（CSCvq64942）

macOS 10.15（およびそれ以降）では、デスクトップ、ドキュメント、ダウンロード、およびネットワークボリュームの各フォルダにアクセスするためのユーザー権限をアプリケーションが取得する必要があります。このアクセス権を付与するにあたり、Secure Firewall ポスチャ の

初回起動時にISE ポスチャ（ネットワークで ISE ポスチャが有効になっている場合）、または DART（ISE ポスチャまたは Cisco Secure Client がインストールされている場合）のポップアップが表示されることがあります。ISE ポスチャと Secure Firewall ポスチャ はエンドポイントのポスチャアセスメントに OPSWAT を使用し、設定された製品とポリシーに基づいてポスチャがこれらのフォルダのアクセス権を確認します。

このようなポップアップでは、[OK] をクリックしてこれらのフォルダへのアクセスを許可し、ポスチャ フローを続行する必要があります。[許可しない（Don't Allow）] をクリックした場合、エンドポイントが準拠しなくなり、これらのフォルダにアクセスせずにポスチャ評価および修復が失敗することがあります。

[許可しない（Don't Allow）] の選択を修復するには

これらのポップアップを再表示してフォルダにアクセス権を付与するには、キャッシュされた設定を編集します。

1. [システム設定（System Preferences）] を開きます。
2. **[セキュリティおよびプライバシー（Security & privacy）]** > **[プライバシー（Privacy）]** > **[ファイルおよびフォルダ（Files and Folders）]** に移動します。
3. Cisco Secure Client フォルダ内のフォルダアクセスに関連するキャッシュの詳細を削除します。

権限ポップアップの再表示に続いてポスチャが開始され、ユーザーが [OK] をクリックするとアクセス権を付与できます。

macOS での GUI カスタマイズはサポートされていない

macOS での GUI リソースのカスタマイズは現在サポートされていません。

SentinelOne との非互換性

Cisco Secure Client Umbrella モジュールは、SentinelOne エンドポイント セキュリティ ソフトウェアと互換性がありません。

4.8 へのアップグレード後に macOS 管理トンネルが切断される

次のいずれかのシナリオが発生した場合は、Apple 認証に準拠するためのセキュリティ改善に関連しています。

- AnyConnect 4.7 では管理トンネル接続ができていた同じ環境で、AnyConnect 4.8 バージョンが失敗する。
- VPN統計情報ウィンドウに、管理トンネルの状態として「接続解除（接続失敗）（Disconnect (Connect Failed)）」と表示される。
- コンソール ログには、「証明書の検証エラー（Certificate Validation Failure）」が示される。これは、管理トンネルの接続解除を意味します。

Cisco Secure Client アプリケーションまたは実行可能ファイルへのアクセスを（プロンプトなしで）許可するように設定されている場合、AnyConnect 4.8（以降）にアップグレードした後に、アプリケーションまたは実行可能ファイルを再度追加して ACL を再設定する必要があります。vpnagentd プロセスを含めるには、キーチェーンアクセスのシステムストアの秘密キーアクセスを変更する必要があります。

1. **[システムキーチェーン（System Keychain）] > [システム（System）] > [証明書（My Certificates）] > [秘密キー（Private key）]**の順に移動します。
2. [アクセス制御（access control）] タブから vpnagentd プロセスを削除します。
3. 現在の vpnagentd を /opt/cisco/secureclient/bin フォルダに追加します。
4. プロンプトが表示されたら、パスワードを入力します。
5. キーチェーンアクセスを終了し、VPN サービスを停止します。
6. 再起動します。

PMK ベースのローミングはネットワーク アクセス マネージャでサポートされていない

Windows では、ネットワーク アクセス マネージャで PMK ベースのローミングを使用できません。

DART には Admin 権限が必要

システムセキュリティの制約により、DART でログを収集するには、macOS、Ubuntu、および Red Hat の管理者権限が必要になりました。

FIPS モードで復元される IPsec 接続（CSCvm87884）

AnyConnect リリース 4.6.2 および 4.6.3 には、IPsec 接続の問題がありました。AnyConnect リリース 4.7 以降で IPsec 接続（CSCvm87884）を復元する場合、FIPS モードの Diffie-Hellman グループ 2 および 5 がサポートされなくなります。そのため、FIPS モードの Cisco Secure Client は、リリース 9.6 より古い Cisco Secure Firewall ASA および DH グループ 2 または 5 を指定するように設定された Cisco Secure Firewall ASA に接続できなくなっています。

Firefox 58 上の証明書ストアデータベース（NSS ライブラリ更新）にともなう変更点

（*58* より前のバージョンの *Firefox* を使用しているユーザーにのみ影響）Firefox 58 以降、NSS 証明書ストア DB 形式が変更されたため、Cisco Secure Client も新しい証明書 DB を使用するように変更されました。58 より前のバージョンの Firefox を使用している場合は、Firefox と Cisco Secure Client が同じ DB ファイルにアクセスできるように、NSS_DEFAULT_DB_TYPE="sql" 環境変数を 58 に設定してください。

ネットワーク アクセス マネージャおよびグループポリシーとの競合

有線またはワイヤレスネットワーク設定や特定の SSID が Windows グループポリシーからプッシュされた場合、それらはネットワーク アクセス マネージャの適切な動作と競合する可能性があります。ネットワーク アクセス マネージャがインストールされている場合、ワイヤレス設定のグループポリシーはサポートされません。

Windows 10 バージョン 1703 でネットワーク アクセス マネージャに非表示ネットワークスキャンリストがない（CSCvg04014）

Windows 10 バージョン 1703 では、WLAN の動作が変更されたため、ネットワーク アクセス マネージャがワイヤレスネットワーク SSID をスキャンするときに中断が発生していました。Microsoft が調査中の Windows コードのバグのために、ネットワーク アクセス マネージャの非表示ネットワークへのアクセスの試みが影響を受けます。最適なユーザーエクスペリエンスを提供するために、ネットワーク アクセス マネージャのインストール時に 2 つのレジストリキーを設定し、アンインストール時にそれらを削除することによって、Microsoft の新機能を無効化しています。

Cisco Secure Client の macOS 10.13（High Sierra）互換性

AnyConnect 4.5.02XXX 以降では、macOS の [システム環境設定（Preferences）] > [セキュリティとプライバシー（Security & Privacy）] ペインで Secure Client（旧 AnyConnect） ソフトウェア拡張機能を有効にすることにより、全機能を活用するのに必要な手順をガイドする追加機能と警告が提供されます。ソフトウェア拡張機能を手動で有効にする必要があることが、macOS 10.13（High Sierra）の新しいオペレーティングシステム要件です。さらに、ユーザーのシステムを macOS 10.13 以降にアップグレードする前に Secure Client をアップグレードすると、Secure Client ソフトウェア拡張機能は自動的に有効になります。

ユーザーのシステムが macOS 10.13（以降）である場合、4.5.02XXX より前のバージョンを使用しているときは、macOS の [システム環境設定（Preferences）] > [セキュリティとプライバシー（Security & Privacy）] ペインで Secure Client（旧 AnyConnect）ソフトウェア拡張機能を有効にする必要があります。拡張機能を有効にした後は、手動での再起動が必要になる場合があります。

macOS システム管理者は User Approved Kernel Extension Loading を無効にする追加機能を利用できる場合があります（https://support.apple.com/en-gb/HT208019 [英語] を参照）。これは現在サポートされているバージョンの Secure Client で有効です。

電源イベントまたはネットワークの中断が発生したときのポスチャへの影響

ネットワークの変更または電源イベントが発生した場合、中断されたポスチャプロセスは正常に完了しません。ネットワークまたは電力の変更により、Cisco Secure Client ダウンローダーエラーが発生します。ユーザーがこれを確認しないと、プロセスを続行できません。

ネットワーク アクセス マネージャが WWAN/3G/4G/5G に自動的にフォールバックしない

WWAN/3G/4G/5G へのすべての接続は、ユーザーによって手動でトリガーされる必要があります。有線またはワイヤレス接続を利用できない場合、ネットワーク アクセス マネージャは、これらのネットワークに自動的に接続しません。

NAM、DART、ISE ポスチャ、またはポスチャの Web 展開が署名/ファイル整合性検証エラーで失敗する

「タイムスタンプの署名及び/または証明書を検証できないか、または形式が違います（timestamp signature and/or certificate could not be verified or is malformed）」というエラーは、Windows でのみ、Cisco Secure Firewall ASA または ISE からの AnyConnect 4.4MR2（またはそれ以降）の Web 展開時に発生します。MSI ファイルとして展開されるネットワーク アクセス マネージャ、DART、ISE ポスチャ、およびポスチャモジュールだけが影響を受けます。SHA-2 タイムスタンプ証明書サービスを使用することから、タイムスタンプ証明書チェーンを正しく検証するために、最新の信頼できるルート証明書が必要です。事前展開や、ルート証明書を自動的に更新するように設定された標準の Windows システムでは、この問題は発生しません。ただし、自動ルート証明書更新設定が無効になっている（デフォルトではない）場合は、https://technet.microsoft.com/en-us/library/dn265983(v=ws.11).aspx [英語] を参照するか、シスコが使用するタイムスタンプルート証明書を手動でインストールしてください。署名ツールを使用して、Microsoft 提供の Windows SDK からコマンドを実行することにより、問題が Cisco Secure Client の

```
signtool.exe verify /v /all/debug/pa<file to verify>
```

外部にあるかどうかを確認することもできます。

認証時の macOS キーチェーンプロンプト

macOS では、VPN 接続の開始後にキーチェーン認証プロンプトが表示される場合があります。このプロンプトは、セキュアゲートウェイからのクライアント証明書要求後に、クライアント証明書の秘密キーへのアクセスが必要な場合にのみ表示されます。トンネルグループに証明書認証が設定されていなくても、Cisco Secure Firewall ASA で証明書マッピングが 設定されている可能性があります。その場合、クライアント証明書の秘密キーのアクセス制御設定が [アクセスを許可する前に確認する（Confirm Before Allowing Access）] に設定されているとキーチェーンプロンプトが表示されます。

ログインキーチェーンからクライアント証明書への Secure Client のアクセスを制限するように Cisco Secure Client プロファイルを設定します（ASDM プロファイルエディタで、[設定（パート1）（Preferences (Part 1)）] > [証明書ストア（Certificate Store）] > [macOS] の [ログイン（Login）] を選択）。キーチェーン認証プロンプトを停止するには、次のいずれかの操作を行います。

- 既知のシステムキーチェーン証明書を除外するようにクライアントプロファイルの証明書一致基準を設定します。

- Cisco Secure Client へのアクセスを許可するようにシステムキーチェーン内のクライアント証明書秘密キーのアクセス制御設定を指定します。

Umbrella ローミング セキュリティ モジュールの変更

`OrgInfo.json` ファイルを取得するためのダッシュボードは、https://dashboard.umbrella.com です。そこから [アイデンティティ（Identity）]>[ローミングコンピュータ（Roaming Computers）] の順に移動し、左上にある [+]（追加アイコン）をクリックして、[Cisco Secure Client Umbrella ローミングセキュリティモジュール（AnyConnect Umbrella Roaming Security Module）] セクションの [モジュールプロファイル（Module Profile）] をクリックします。

Cisco Secure Client の Microsoft Windows 10 との互換性

最良の結果を得るために、Windows 7/8/8.1 からのアップグレードではなく Windows 10 システムへの Cisco Secure Client のクリーンインストールをお勧めします。Cisco Secure Client がプレインストールされた Windows 7/8/8.1 からアップグレードする場合は、オペレーティングシステムをアップグレードする前に、必ず、まず Cisco Secure Client をアップグレードしてください。Windows 10 にアップグレードする前に、ネットワーク アクセス マネージャ モジュールをアンインストールする**必要があります**。システムのアップグレードが完了したら、ネットワーク アクセス マネージャをシステムに再インストールできます。また、Windows 10 へのアップグレード後に、Cisco Secure Client を完全にアンインストールし、サポートされているいずれかのバージョンを再インストールすることもできます。

新しいスプリット包含トンネルの動作（CSCum90946）

以前は、スプリット包含ネットワークがローカル サブネットのスーパーネットである場合、ローカルサブネットと完全に一致するスプリット包含ネットワークが設定されていないかぎり、ローカル サブネット トラフィックはトンネリングされませんでした。CSCum90946 の解決により、スプリット包含ネットワークがローカルサブネットのスーパーネットである場合、アクセスリスト（ACE/ACL）でスプリット除外（deny 0.0.0.0/32 or ::/128）も設定されていないかぎり、ローカル サブネット トラフィックはトンネリングされます。

スーパーネットがスプリット包含 で設定されており、かつ、 目的の動作が LocalLan アクセスの許可である場合、次の設定が必要です。

- アクセスリスト（ACE/ACL）には、スーパーネットに関する許可アクションと、0.0.0.0/32 または ::/128 に関する拒否アクションの両方を含める必要があります。
- プロファイルエディタの Cisco Secure Client プロファイル（[設定（パート1）（Preferences (Part 1)）] メニュー）で [ローカルLANアクセス（Local LAN Access）] を有効にします（ユーザー制御可能にするオプションもあります）。

認証に SHA512 証明書を使用した場合に認証に失敗する

（バージョン 4.9.03047 以前の AnyConnect を実行している Windows 7、8、および 8.1 ユーザーの場合）クライアントが認証に SHA512 証明書を使用すると、証明書が使用されていることが

クライアントログに記録されていても認証は失敗します。ASA ログには、AnyConnect によって証明書が送信されていないことが正しく示されます。これらのバージョンの Windows では、TLS 1.2 で SHA512 証明書のサポートを有効にする必要があります。これはデフォルトではサポートされていません。これらの SHA512 証明書のサポートの有効化については https://support.microsoft.com/en-us/kb/2973337 を参照してください。4.9.03049

ISE ポスチャでのログ トレースの使用

新規インストールが完了すると、予期どおりの動作として、ISE ポスチャ ログ トレース メッセージが表示されます。ただし、ISE ポスチャ プロファイル エディタを開いて [エージェントログトレースファイルの有効化（Enable Agent Log Trace file）] を 0（無効）に変更する場合は、期待どおりの結果を得るために Cisco Secure Client のサービスを再起動する必要があります。

macOS での ISE ポスチャとの相互運用性

macOS 10.9 以降を使用しており、ISE ポスチャを使用する場合は、問題を回避するために次の作業を行う必要があります。

- ポスチャアセスメント時に「ポリシーサーバーへの接続の失敗」というエラーが発生することを回避するには、証明書の検証を無効にします。
- キャプティブ ポータル アプリケーションを無効にします。無効にしない場合は、検出プローブがブロックされ、アプリケーションはポスチャ前の ACL 状態のままになります。

macOS 上の Firefox 証明書ストアはサポートされない

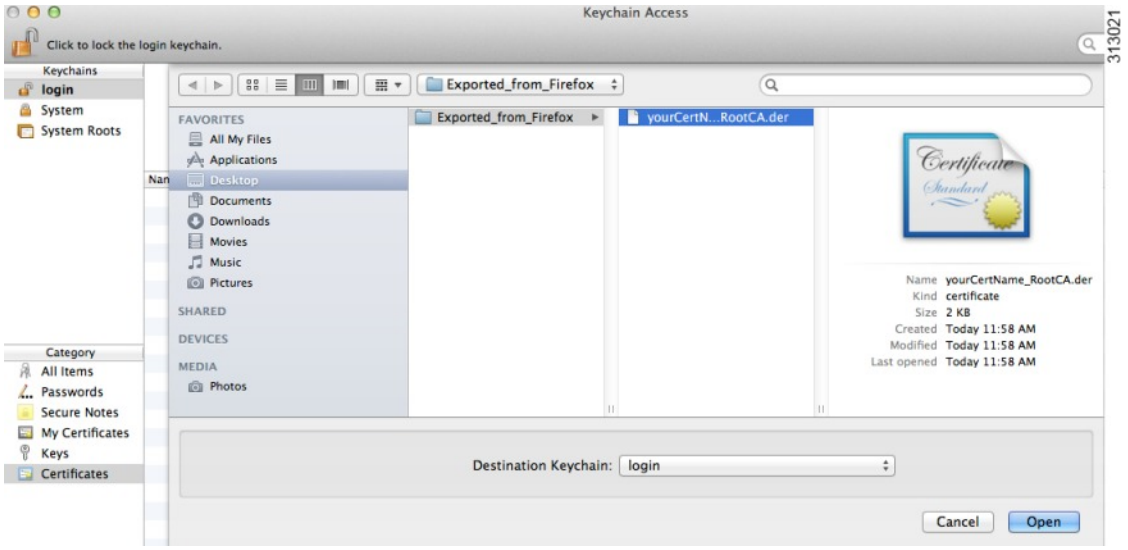
macOS 上の Firefox 証明書ストアは、任意のユーザーによるストアの内容の変更を許可するアクセス権を使用して保存されます。これにより、未認可のユーザーまたはプロセスが不正な CA を信頼されたルートストアに追加することが可能になります。Cisco Secure Client は、サーバー検証またはクライアント証明書に Firefox ストアを使用しなくなりました。

必要に応じて、Cisco Secure Client 証明書を Firefox の証明書ストアからエクスポートする方法とそれらを macOS キーチェーンにインポートする方法をユーザーに指示してください。一例として、Cisco Secure Client ユーザーに次のような手順を伝えます。

1. Firefox の [オプション（Preferences）]>[プライバシーとセキュリティ（Privacy & Security）]>[詳細設定（Advanced）] の [証明書（Certificates）] タブに移動し、[証明書を表示（View Certificates）] をクリックします。
2. Cisco Secure Client に使用する証明書を選択し、[エクスポート（Export）] をクリックします。

   多くの場合、Cisco Secure Client 証明書は [認証局証明書（Authorities）] カテゴリにあります。目的の証明書は別のカテゴリ（[あなたの証明書（Your Certificates）] または [サーバー証明書（Servers）]）に含まれている可能性があるため、証明書管理者に確認してください。
3. 証明書を保存する場所（デスクトップ上のフォルダなど）を選択します。

4. [ファイルの種類（Format）]プルダウンメニューで、[X.509 証明書（DER）（X.509 Certificate (DER)）] を選択します。必要に応じて、証明書名に .der 拡張子を追加します。

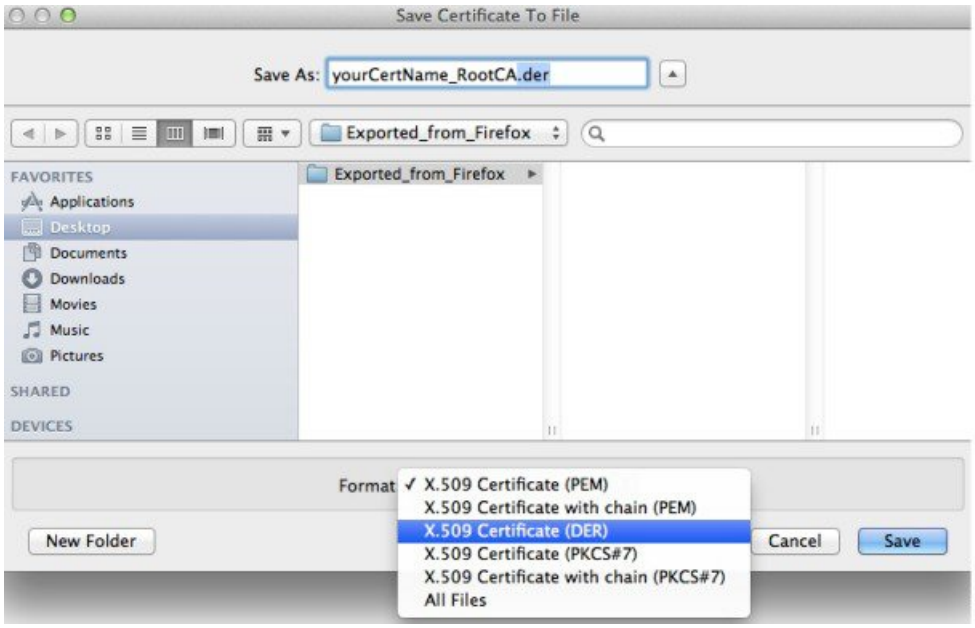


（注） 複数の Cisco Secure Client 証明書または秘密キー（あるいはその両方）が使用される場合や必要な場合は、証明書ごとに上記のプロセスを繰り返してください。

5. KeyChain を起動します。[ファイル（File）]>[アイテムのインポート...（Import Items…）] に移動し、Firefox からエクスポートした証明書を選択します。

   [宛先キーチェーン:（Destination Keychain:）] で目的のキーチェーンを選択します。この例で使用されているログインキーチェーンは、ユーザーの会社で使用されているものと異なる場合があります。証明書をインポートする必要があるキーチェーンについては、証明書管理者に問い合わせてください。

6. [宛先キーチェーン:（Destination Keychain:）] で目的のキーチェーンを選択します。この例で使用されているログインキーチェーンは、ユーザーの会社で使用されているものと異なる場合があります。証明書をインポートする必要があるキーチェーンについては、証明書管理者に問い合わせてください。



7. Cisco Secure Client に使用される（または必要な）追加の証明書について、上記の手順を繰り返します。

Active X のアップグレードで WebLaunch が無効になることがある

ActiveX コントロールに必要な変更を加えない限り、WebLaunch による Cisco Secure Client ソフトウェアの自動アップグレードは、限定的なユーザーアカウントで機能します。

場合によっては、このコントロールが、セキュリティの修正または新しい機能の追加によって変更されます。

限定的なユーザーアカウントからコントロールを起動するときにコントロールのアップグレードが必要な場合、管理者は、Cisco Secure Client プレインストーラ、SMS、GPO、またはその他の管理展開方法を使用してコントロールを展開する必要があります。

Java 7 の問題

Java 7 では、Cisco Secure Client と Secure Firewall ポスチャ で問題が発生する可能性があります。この問題と回避策については、トラブルシューティングテクニカルノートの『ava 7 Issues with AnyConnect, CSD/HostScan, and WebVPN - Troubleshooting Guide』[英語]（[セキュリティ（Security）] > [Cisco Secure Firewall ポスチャ] にあるシスコのドキュメント）を参照してください。

トンネルオールネットワークが設定されていると暗黙の DHCP フィルタが適用される

Cisco Secure Client は、すべてのネットワークのトンネルが設定されているときにローカル DHCP トラフィックを暗号化せずに流せるようにするために、Cisco Secure Client の接続時にローカル DHCP サーバーに特殊なルートを追加します。また、このルートでのデータ漏洩を防

ぐため、Cisco Secure Client はホストマシンの LAN アダプタに暗黙的なフィルタを適用し、DHCP トラフィックを除く、そのルートのすべてのトラフィックをブロックします。

テザーデバイス上の Cisco Secure Client

Bluetooth か USB でテザリングされた携帯電話またはモバイルデータデバイスが提供するネットワーク接続は、シスコによって特に認定されていないため、展開前に Cisco Secure Client で検証する必要があります。

Cisco Secure Client スマートカードのサポート

Cisco Secure Client は、次の環境でスマートカードによって提供されるログイン情報に対応します。

- Windows 7、Windows 8、Windows 10 上の Microsoft CAPI 1.0 および CAPI 2.0。
- macOS 上のキーチェーンと macOS 10.12 以降上の CryptoTokenKit。

（注） Cisco Secure Client は、Linux または PKCS #11 デバイスではスマートカードをサポートしていません。

Cisco Secure Client 仮想テスト環境

シスコは、次の仮想マシン環境を使用して Cisco Secure Client クライアントテストの一部を実行します。

- VM Fusion 7.5.x、10.x、11.5.x
- ESXi ハイパーバイザ 6.0.0、6.5.0、および 6.7.x
- VMware Workstation 15.x

仮想環境での Cisco Secure Client の実行はサポートしませんが、Cisco Secure Client はシスコがテストする VMware 環境で適切に機能すると予測されます。

仮想環境で Cisco Secure Client の問題が発生した場合は、報告してください。シスコが解決に向けて最善を尽くします。

自動更新を無効にするとバージョンの競合によって接続が妨げられる場合がある

Cisco Secure Client を実行するクライアントの自動更新が無効になっている場合、Cisco Secure Firewall ASA に同じバージョンかそれ以前のバージョンの Cisco Secure Client がインストールされていないと、クライアントは VPN に接続できません。

この問題を回避するには、Cisco Secure Firewall ASA で同じバージョンかそれ以前のバージョンの Cisco Secure Client パッケージを設定するか、自動更新を有効にしてクライアントを新しいバージョンにアップグレードします。

ネットワーク アクセス マネージャと他の接続マネージャの間の相互運用性

ネットワーク アクセス マネージャが動作している場合、ネットワーク アダプタが排他的に制御され、他のソフトウェア接続マネージャ（Windows のネイティブ接続マネージャを含む）による接続確立の試みがブロックされます。そのため、Cisco Secure Client ユーザーにエンドポイントコンピュータ上の他の接続マネージャ（iPassConnect Mobility Manager など）を使用させる場合は、ネットワーク アクセス マネージャ GUI のクライアント無効化オプションを使用するか、ネットワーク アクセス マネージャ サービスを停止することによって、ネットワーク アクセス マネージャを無効にする必要があります。

ネットワーク アクセス マネージャと互換性のないネットワーク インターフェイス カード ドライバ

Intel ワイヤレス ネットワーク インターフェイス カード ドライバ バージョン 12.4.4.5 は、ネットワーク アクセス マネージャと互換性がありません。このドライバがネットワーク アクセス マネージャと同じエンドポイントにインストールされている場合、一貫性のないネットワーク接続や Windows オペレーティングシステムの突然のシャットダウンが発生する可能性があります。

Cisco Secure Client 用のウイルス対策アプリケーションの設定

ウイルス対策、マルウェア対策、侵入防御システム（IPS）などのアプリケーションが、Cisco Secure Client アプリケーションの動作を誤って悪意のあるものと判断する場合があります。そのような誤解釈を避けるために例外を設定できます。Cisco Secure Client のモジュールかパッケージをインストールしたら、Secure Client のインストールフォルダを許可するか、Secure Client アプリケーションのセキュリティ例外を指定するようにウイルス対策ソフトウェアを設定します。

除外する一般的なディレクトリを次に示しますが、リストは完全ではない場合があります。

- C:\Users\<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files x86)\Cisco

Secure Firewall ポスチャ 用のウイルス対策アプリケーションの設定

ウイルス対策アプリケーションが、ポスチャモジュールや Secure Firewall ポスチャ パッケージに含まれる一部のアプリケーションの動作を誤って悪意のあるものと判断する場合があります。ポスチャモジュールまたは Secure Firewall ポスチャ パッケージをインストールする前に、以下の Secure Firewall ポスチャ アプリケーションに対してセキュリティ例外を許可するか指定するようにウイルス対策ソフトウェアを設定します。

- cscan.exe
- ciscod.exe
- cstub.exe

IKEv2 でサポートされないパブリックプロキシ

IKEv2 はパブリック側プロキシをサポートしていません。この機能のサポートが必要な場合は、SSL を使用してください。プライベート側プロキシは、セキュアゲートウェイから送信される設定の指示に従って、IKEv2 と SSL の両方でサポートされます。IKEv2 はゲートウェイから送信されるプロキシ設定を適用し、それ以降の HTTP トラフィックはそのプロキシ設定の影響を受けます。

IKEv2 に関してグループポリシーの MTU 調整が必要な場合がある

Cisco Secure Client は、一部のルータによるパケットフラグメントを受信およびドロップする場合があり、その結果として、一部の Web トラフィックが通過できなくなります。

この問題を回避するには MTU の値を小さくします。推奨値は 1200 です。次に、CLI を使用してこれを実行する例を示します。

```
hostname# config t
hostname(config)# group-policy DfltGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# anyconnect mtu 1200
```

ASDM を使用して MTU を設定するには、[設定（Configuration）] > [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）] の順に選択します。

DTLS 使用時に MTU が自動的に調整される

DTLS に関してデッドピア検出（DPD）が有効になっている場合、クライアントは自動的にパス MTU を決定します。以前に Cisco Secure Firewall ASA を使用して MTU を減らした場合は、設定をデフォルト値（1406）に復元する必要があります。トンネルの確立時に、クライアントは、特別な DPD パケットを使用して MTU を自動調整します。それでも問題が解決しない場合は、Cisco Secure Firewall ASA での MTU 構成を使用して以前と同様に MTU を制限します。

ネットワーク アクセス マネージャとグループポリシー

Windows Active Directory ワイヤレスグループポリシーにより、特定の Active Directory ドメイン内の PC に展開されるワイヤレス設定とワイヤレスネットワークが管理されます。ネットワーク アクセス マネージャをインストールする場合、管理者は、特定のワイヤレス グループ ポリシー オブジェクト（GPO）がネットワーク アクセス マネージャの動作に影響を与える可能性があることに注意する必要があります。完全な GPO 展開を実行する前に、必ず、ネットワーク アクセス マネージャを使用して GPO ポリシー設定をテストしてください。ワイヤレスネットワークに関連する GPO はサポートされていません。

ネットワーク アクセス マネージャを使用する場合の FreeRADIUS 設定

ネットワーク アクセス マネージャを使用するには、FreeRADIUS 設定を調整する必要があります。脆弱性を防ぐために、ECDH 関連の暗号はデフォルトで無効になっています。/etc/raddb/eap.conf で cipher_list の値を変更してください。

アクセスポイント間のローミングには完全認証が必要

Windows 7 以降を実行しているモバイルエンドポイントは、クライアントが同じネットワーク上のアクセスポイント間をローミングするときに、より迅速な PMKID 再アソシエーションを利用する代わりに、完全な EAP 認証を実行する必要があります。その結果、場合によっては、Cisco Secure Client は完全認証のたびにログイン情報を入力するようにユーザーに要求します（アクティブプロファイルによって要求される場合）。

LAN 内の他のデバイスでのホスト名の表示を防止する

Cisco Secure Client を使用してリモート LAN 上の Windows 7 以降と VPN セッションを確立すると、ユーザーの LAN 内にある他のデバイス上のネットワークブラウザに保護されたリモートネットワーク上のホストの名前が表示されます。ただし、他のデバイスはこれらのホストにアクセスできません。

Cisco Secure Client ホストが（Cisco Secure Client エンドポイントホストの名前を含む）サブネット間でのホスト名の漏洩を確実に防ぐようにするために、そのエンドポイントがプライマリまたはバックアップブラウザにならないように設定してください。

1. [プログラムとファイルの検索（Search Programs and Files）] テキストボックスに「**regedit**」と入力します。
2. **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters** に移動します。
3. [MaintainServerList] をダブルクリックします。

[文字列の編集（Edit String）] ウィンドウが開きます。

1. 「**No**」と入力します。
2. [OK] をクリックします。
3. [レジストリエディター（Registry Editor）] ウィンドウを閉じます。

失効メッセージ

配信ポイントが内部的にしかアクセスできない場合に、Secure Client が LDAP 証明書失効リスト（CRL）の配信ポイントを指定するサーバー証明書を確認しようとすると、認証後に Cisco Secure Client 証明書失効警告ポップアップウィンドウが表示されます。

このポップアップウィンドウが表示されないようにするには、次のいずれかを実行します。

- プライベート CRL 要件を持たない証明書を取得します。

- Internet Explorer でサーバー証明書失効確認を無効にします。

注意 Internet Explorer でサーバー証明書失効確認を無効にすると、他の OS の使用に関してセキュリティ上の重大な悪影響が生じる可能性があります。

ローカリゼーションファイル内のメッセージが複数行になる場合がある

ローカリゼーションファイル内のメッセージの検索を試みると、次の例のように、それらが複数行になる場合があります。

```
msgid ""
"The service provider in your current location is restricting access to the "
"Secure Gateway. "
```

特定のルータの背後にある場合の macOS 用 Cisco Secure Client のパフォーマンス

macOS 用の Cisco Secure Client が、iOS を実行するゲートウェイへの SSL 接続の確立を試みる場合、または Cisco Secure Client が特定タイプのルータ（Cisco Virtual Office（CVO）ルータなど）の背後から Cisco Secure Firewall ASA への IPsec 接続の確立を試みる場合、一部の Web トラフィックが接続を通過し、その他のトラフィックがドロップされる可能性があります。Cisco Secure Client は MTU を誤って計算する場合があります。

この問題を回避するには、macOS コマンドラインから次のコマンドを使用して、Cisco Secure Client アダプタの MTU の値を手動で減らします。

```
sudo ifconfig utun0 mtu 1200
```

Windows ユーザーによる常時接続の無効化を防止する

Windows コンピュータでは、限定的な権限または標準的な権限を持つユーザーは、それぞれのプログラムデータフォルダに対して書き込みアクセスを実行できる場合があります。これらの権限により、Cisco Secure Client プロファイルを削除することが可能なため、常時接続機能を無効にできます。これを防止するには、`C:\ProgramData` フォルダ（または少なくとも Cisco サブフォルダ）へのアクセスを制限するようにコンピュータを設定します。

Wireless Hosted Network を無効にする

Windows 7 以降の Wireless Hosted Network 機能を使用すると Cisco Secure Client が不安定になる可能性があります。Cisco Secure Client を使用する場合、この機能を有効にしたり、（Connectify または Virtual Router など）この機能を有効にするフロントエンド アプリケーションを実行したりすることはお勧めしません。

Cisco Secure Client では Cisco Secure Firewall ASA が SSLv3 トラフィックを要求しないように設定する必要があります。

Cisco Secure Client では、Cisco Secure Firewall ASA が TLSv1 または TLSv1.2 トラフィックを受け入れ、SSLv3 トラフィックを受け入れないようにする必要があります。SSLv3 キー生成アルゴリズムは、キー生成機能を低下させる可能性がある方法で MD5 と SHA-1 を使用します。SSLv3 の後継規格である TLSv1 を使用すると、SSLv3 に存在するこの問題とその他のセキュリティ上の問題が解決されます。

Cisco Secure Client は、「ssl server-version」の次の Cisco Secure Firewall ASA 設定では接続を確立できません。

ssl server-version sslv3

ssl server-version sslv3-only

Trend Micro がインストールを妨げる

デバイスに Trend Micro がインストールされている場合、ドライバが競合するために、ネットワーク アクセス マネージャをインストールできません。Trend Micro をアンインストールするか [Trend Micro共通ファイアウォールドライバ（trend micro common firewall driver）] をオフにすると、この問題を回避できます。

Secure Firewall ポスチャ がレポートする情報

サポートされているマルウェア対策製品およびファイアウォール製品はいずれも、最終スキャン時間情報をレポートしません。Secure Firewall ポスチャ がレポートする情報は、次のとおりです。

- マルウェア対策について
  - 製品の説明
  - 製品のバージョン
  - ファイルシステム保護ステータス（アクティブスキャン）
  - データファイル時間（最終更新日時とタイムスタンプ）
- ファイアウォールについて
  - 製品の説明
  - 製品のバージョン
  - ファイアウォールの有効/無効

再接続に時間がかかる（CSCtx35606）

IPv6 が有効になっており、プロキシ設定の自動検出が Internet Explorer で有効になっているか現在のネットワーク環境でサポートされていない場合、Windows で再接続に時間がかかることがあります。回避策として、プロキシの自動検出が現在のネットワーク環境でサポートされていない場合は、VPN 接続に使用されない物理ネットワークアダプタを切断するか、IE でプロキシの自動検出を無効にすることができます。

限定的な権限を持つユーザーは ActiveX をアップグレードできない

ActiveX コントロールをサポートする Windows クライアントでは、限定的な権限を持つユーザーアカウントは ActiveX コントロールをアップグレードできないため、Web 展開方式で Cisco Secure Client をアップグレードできません。最も安全な選択肢として、ユーザーが、ヘッドエンドに接続してアップグレードすることにより、アプリケーション内からクライアントをアップグレードすることをお勧めします。

（注） 以前に管理者アカウントを使用して ActiveX コントロールがクライアントにインストールされている場合、ユーザーは ActiveX コントロールをアップグレードできます。

プロアクティブ キー キャッシング（PKC）または CCKM のサポートがない

ネットワーク アクセス マネージャは PKC または CCKM キャッシングをサポートしていません。高速ローミングは、すべての Windows プラットフォームで利用できるわけではありません。

Cisco Secure Client のアプリケーション プログラミング インターフェイス

Cisco Secure Client には、独自のクライアントプログラムを構築するユーザー向けのアプリケーション プログラミング インターフェイス（API）が含まれています。

API パッケージには、Cisco Secure Client の C++ インターフェイスに対応するマニュアル、ソースファイル、およびライブラリファイルが含まれています。Windows、Linux、および Mac プラットフォームで構築する際に、ライブラリおよびプログラム例を使用できます。Windows プラットフォーム用の Makefile（またはプロジェクトファイル）も含まれています。他のプラットフォーム用には、サンプルコードのコンパイル方法を示すプラットフォーム固有スクリプトが含まれています。ネットワーク管理者は、アプリケーション（GUI、CLI、または組み込みアプリケーション）とこれらのファイルやライブラリをリンクできます。

API は Cisco.com からダウンロードできます。

Cisco Secure Client API に関するサポートの問題については、anyconnect-api-support@cisco.com に電子メールでお問い合わせください。

Cisco Secure Client 5.1.2.42

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警告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 [英語] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwf21453	core	プロキシ設定を検証しようとすると、RetainVpnOnLogoffエラーが発生する
CSCwh73937	core	ENH：CNAME DNS 応答に基づいてダイナミックスプリット除外をサポートする macOS AnyConnect
CSCwi07144	core	zlib の脆弱性：複数のバージョン
CSCwi78167	core	AO構成のロードバランシングサーバーに対するワイルドカードのサポート
CSCwi27062	nam	NAM が Eero メッシュ AP に接続できない
CSCwi27137	nam	NAM がデフォルトの PMF IGTK 暗号を認識しない
CSCwi38780	nam	PMF が有効になっている高速移行ワイヤレスネットワークの接続を NAM が完了しない
CSCwi48979	nvm	macOS クライアントに対する NVM HTTP ホストのサポート
CSCwi49003	nvm	NVM が macOS 用の Safari ブラウザプラグインを報告しない
CSCwi50185	posture-ise	ISE ポスチャ：PSN 検出の失敗

識別子	コンポーネント	タイトル
CSCwh29292	vpn	ENH：スタティックスプリット除外とともに DSI と DSE の設定を許可する
CSCwi17408	vpn	ENH：グループポリシー設定によるスプリットトンネリングのプロキシアクセス強化のバイパスを許可する
CSCwi33431	vpn	事前展開/Web 展開のアップグレード後に複数の ZTA バージョンがインストール済みとして表示される

Cisco Secure Client 5.1.1.42

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警告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 [英語] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwf67833	core	（Windows のみ）エラー：VPN クライアントがプライベート側のプロキシ設定を行えない
CSCwh57935	core	AnyConnect がコア更新の外部でクライアント ダウンローダー ポップアップを起動する
CSCwh96410	core	curl の脆弱性：複数のバージョン
CSCwi20597	core	macOS 14.2：インストール後に VPN エージェントが起動しない
CSCwi28687	core	macOS でプロキシを認証すると Vpnagentd がクラッシュする

識別子	コンポーネント	タイトル
CSCwf92159	gui	クライアントプロファイルで自動サーバー選択が有効になっている場合、アップグレード後に CSC UI がクラッシュする
CSCwh35676	nvm	ENH：AnyConnect/Secure Client と SWG がアクティブな場合、元の NVM プロセスと宛先ホストを表示する
CSCwi03257	posture-ise	Symantec WSS が接続されると macOS 上の ISE ポスチャ IPC が破損し、ポスチャ障害が発生す
CSCwe35649	vpn	macOS 13.2：1 つの IP プロトコルに対してのみ有効になっている場合、スプリット包含トンネリングが機能しない
CSCwe49687	vpn	macOS 12 および 13：CP 修復前の遅延が起こる可能性、AnyConnect ブラウザが使用されない
CSCwh51369	vpn	SBL が再接続中にプロキシ設定を復元できない
CSCwh75976	vpn	v117.x へのアップグレード後、キャプティブポータルが WebView2 ベースの組み込みブラウザにロードされない
CSCwi24180	ztna	ZTA モジュールが登録解除後もトラフィックの傍受を続行する

Cisco Secure Client 5.1.0.136

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警告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 [英語] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCvz45813	core	ENH：関連する一連のメッセージ交換をグループ化するために、AnyConnect ログにセッション ID を追加
CSCvu57988	dart	ENH：DART はサポートバンドルに Windows レジストリのコピーを含める必要がある
CSCvy66557	dart	ENH：Windows 向けの DART にはデバイス ID を含める必要がある
CSCvy66584	dart	ENH：macOS 向けの DART には MDM プロファイルを含める必要がある
CSCvq05530	nam	ENH：NAM：管理フレーム保護（PMF）のサポートを追加
CSCvz20268	opswat-ise	ENH：ISE ポスチャが Google Chrome バージョン 89 をサポートしていない
CSCvz202709	opswat-ise	ENH：ISE ポスチャが Mozilla Firefox バージョン 87 をサポートしていない
CSCwc20207	posture-ise	Apex One（MAC）セキュリティエージェント [Trend Micro] AM の最新の定義日/バージョンが反映されない
CSCwd27667	posture-ise	Linux でのローカリゼーションの変更
CSCwd49714	posture-ise	Win、Lin NSA パッケージで翻訳が行われなかった
CSCwd52815	posture-ise	MAC NSA パッケージで翻訳が行われなかった
CSCwd81612	profile-editor	SSI が PE の UNICODE 文字である場合、NAM プロファイルを保存できない

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.2.42

Cisco Secure Firewall ポスチャ 5.1.2.42 には、Windows、macOS、および Linux 用の OPSWAT エンジンバージョンの更新が含まれています。詳細については、「Release and Compatibility」の「Secure Firewall Posture Support Charts」[英語] を参照してください。

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.1.42

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警告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 [英語] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwh71692	posture-asa	HostScan：60 秒ごとのアセスメントでヘッダーを追加する定期的なポーリング

Cisco Secure Firewall ポスチャ（旧称 HostScan）5.1.0.136

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警告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 [英語] で登録を行ってください。

解決済み

識別子	コンポーネント	タイトル
CSCwd44206	opswat-asa	HostScan：HostScan バージョン 4.10.05111 へのアップグレード後にファイアウォールがシステムのログイン情報を要求する

関連資料

Cisco Secure Firewall ASA および Cisco Secure Client の互換性に関する詳細については、『Supported VPN Platforms, Cisco Secure Firewall ASA Series』または『Release Notes for Cisco ASA Series』を参照してください。

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。