NetScaler Gateway クライアント

Machine translated content

Disclaimer

Contents

NetScaler Gateway VPN クライアントとサポートされる機能

April 1, 2024

> 重要:
>
> - iOS/Android 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。
> - レガシー VPN クライアントは Apple のプライベート VPN API を使用して構築されていましたが、現在は廃止されています。macOS/iOS 向け Citrix Secure Access クライアントの VPN サポートは、Apple のパブリックネットワーク拡張フレームワークを使用して書き直されました。iOS および macOS 用の NetScaler Gateway プラグインと VPN はサポートされなくなりました。iOS/macOS 向け Citrix Secure Access は、使用することをお勧めする VPN クライアントです。
> - Android デバイス用の nFactor 認証サポートの一般提供は、今後のリリースの 1 つで利用可能になる予定です。

次の表に、各 VPN クライアントでサポートされる一般的に使用される機能の一部を示します。

機能	Windows 向け Citrix Secure Access	Linux 向け Citrix Secure Access	Citrix Secure Access for macOS	iOS 向け Citrix Secure Access	Android 向け Citrix Secure Access
常時オン (ユーザーモード)	はい (11.1 以降)	いいえ	いいえ	いいえ	はい（MDM 経由）Android 7.0+
PAC ファイル	はい (12.0 以降)	いいえ	はい	はい	いいえ
クライアントプロキシのサポート	はい	はい	いいえ	いいえ	はい。注 *1* を参照
イントラネットアプリケーションの最大制限	512	128	制限なし	制限なし	制限なし
イントラネット IP (IIP) のサポート	はい	はい	はい	はい	はい
分割トンネル ON	はい	はい	はい	はい	はい
分割トンネルのリバース	はい	はい	はい	はい	はい。注 *5* を参照

機能	Windows 向け Citrix Secure Access	Linux 向け Citrix Secure Access	Citrix Secure Access for macOS	iOS 向け Citrix Secure Access	Android 向け Citrix Secure Access
スプリット DNS リモコン	いいえ	はい	はい	はい	はい。注 *6* を参照
スプリット DNS 両方	はい	いいえ	はい	はい	はい。注 *6* を参照
FQDN ベースの分割トンネル	はいオン専用 (13.0 以降)	いいえ	はい	はい	はい。注 *5* を参照
クライアントのアイドルタイムアウト	はい	はい	はい	いいえ	いいえ
エンドポイント分析	はい	はい	はい	いいえ	いいえ
デバイス証明書 (クラシック)	はい	いいえ	はい	いいえ	いいえ
nFactor 認証	はい (12.1 以降)	いいえ	はい	はい	はい。注 *3* を参照
EPA (nFactor)	はい (12.1 以降)	いいえ	はい	いいえ	いいえ
デバイス証明書 (nFactor)	はい (12.1 以降)	いいえ	はい	いいえ	いいえ
プッシュ通知	はい (12.1 以降)	いいえ	いいえ	はい	はい
OTP トークンの自動入力のサポート。注 *2* を参照	いいえ	いいえ	いいえ	はい	はい
TLS 1.3 のサポート	はい	はい	はい	はい (デフォルトでは無効。ご要望に応じてご利用いただけます。)	はい (デフォルトでは無効。ご要望に応じてご利用いただけます。)
DTLS サポート。注 *4* を参照	はい (13.0 以降)	いいえ	はい	はい	いいえ
HTTP のみのクッキー	はい	はい	はい	はい	はい

機能	Windows 向け Citrix Secure Access	Linux 向け Citrix Secure Access	Citrix Secure Access for macOS	iOS 向け Citrix Secure Access	Android 向け Citrix Secure Access
広域サーバー負荷分散（Global Server Load Balancing: GSLB）	はい	はい	はい	はい	はい
ローカル LAN アクセス	はい	いいえ	常に有効	常に有効	いいえ

注:

1. Android 10 以降のゲートウェイ構成の VPN 仮想サーバー上のクライアント構成でのプロキシの設定がサポートされています。IP アドレスとポートを持つ基本的な HTTP プロキシ設定のみがサポートされています。
2. QR コードをスキャンしたトークンのみが自動入力の対象となります。自動入力は nFactor 認証フローではサポートされていません。
3. Android デバイスの nFactor 認証サポートはプレビュー段階にあり、この機能はデフォルトで無効になっています。この機能を有効にするには、NetScaler サポートにお問い合わせください。Android デバイス用の nFactor 認証を有効にするには、NetScaler Gateway の FQDN をサポートチームに提供する必要があります。
4. 詳細については、SSL VPN 仮想サーバーを使用した DTLS VPN 仮想サーバーの設定を参照してください。
5. Android デバイスの FQDN ベースの分割トンネルのサポートとリバース分割トンネルはプレビュー中で、この機能はデフォルトで無効になっています。この機能を有効にするには、NetScaler サポートにお問い合わせください。Android デバイスで有効にするには、NetScaler Gateway の FQDN をサポートチームに提供する必要があります。
6. Split DNS BOTH モードでは、DNS サフィックスをゲートウェイに設定する必要があり、そのサフィックスで終わる DNS A レコードクエリだけがゲートウェイに送信されます。残りのクエリはローカルで解決されます。Android 向け Citrix Secure Access は、スプリット DNS ローカルモードもサポートしています。

リファレンス

エンドユーザー向けヘルプドキュメント

macOS/iOS 向け Citrix Secure Access

April 1, 2024

レガシー VPN クライアントは Apple のプライベート VPN API を使用して構築されていましたが、現在は廃止されています。macOS および iOS 向け Citrix Secure Access の VPN サポートは、Apple のパブリックネットワーク拡張フレームワークを使用してゼロから書き直されました。

> 注
>
> - iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。
> - macOS 向け Citrix Secure Access は、10.15（カタリナ）、11.x（ビッグサー）、12.x（モントレー）でサポートされています。Intel チップと M1 チップを搭載したデバイスをサポートしています。
> - 前述のバージョン（macOS 10.15 および macOS 11.0）のいずれかにアップグレードできないハードウェアを使用しているユーザーは、App Store で最後に互換性のあるバージョンにアクセスできますが、古いバージョンへのアップデートはありません。
> - macOS ユーザーが App Store アプリと TestFlight プレビュービルドを切り替えたり、その逆に切り替えたりした場合、ユーザーは次の手順を実行して接続プロファイルを再作成する必要があります：
>
>   1. Click the hamburger menu and then click **Configuration**.
>   2. Delete the profile from the list and add the same profile again.

macOS/iOS 向け Citrix Secure Access クライアントの主な機能

- パスワードトークン：パスワードトークンは、VIP、OKTA などのセカンダリパスワードサービスの代替となる 6 桁のコードです。このコードは、時間ベースのワンタイムパスワード (T-OTP) プロトコルを使用して、Google Authenticator や Microsoft Authenticator システムなどのサービスと同様の OTP コードを生成します。ユーザーは、特定の Active Directory y ユーザーの NetScaler Gateway への認証中に 2 つのパスワードの入力を求められます。2 つ目の要因は、ユーザーが Google や Microsoft Authenticator などの登録済みのサードパーティサービスからデスクトップブラウザーにコピーする 6 桁のコードです。ユーザーは、まず NetScaler ADC アプライアンスで T-OTP に登録する必要があります。登録手順については、https://support.citrix.com/article/CTX228454を参照してください。アプリでは、NetScaler ADC で生成された QR コードをスキャンするか、TOTP シークレットを手動で入力して、OTP 機能を追加できます。一度追加された OTP トークンは、ユーザーインターフェイスのパスワードトークンセグメントに表示されます。

エクスペリエンスを向上させるために、OTP を追加すると、VPN プロファイルを自動的に作成するようにユーザーに求められます。ユーザーは、この VPN プロファイルを利用して、iOS デバイスから直接 VPN に接続できます。

macOS/iOS 向け Citrix Secure Access クライアントを使用すると、ネイティブ OTP サポートへの登録時に QR コードをスキャンできます。

NetScaler Gateway のプッシュ通知機能は、macOS/iOS 向け Citrix のセキュアアクセスユーザーのみが使用できます。

- プッシュ通知： NetScaler Gateway は、登録されたモバイルデバイスでプッシュ通知を送信し、簡素化された 2 要素認証エクスペリエンスを実現します。macOS/iOS 向け Citrix Secure Access クライアントを起動して NetScaler のログオンページに第 2 ファクタの OTP を設定する代わりに、登録されたデバイスのデバイス PIN/Touch ID /フェイス ID を入力することで本人確認を行うことができます。

デバイスをプッシュ通知用に登録すると、そのデバイスを macOS/iOS 向け Citrix Secure Access を使用してネイティブ OTP サポートに使用することもできます。プッシュ通知の登録は、ユーザーに対して透過的に行われます。ユーザーが TOTP を登録すると、NetScaler ADC がサポートしている場合、デバイスはプッシュ通知用にも登録されます。

リリースノート

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO の名前が Citrix Secure Access に変更されました。この名前の変更を反映するために、ドキュメント内の UI スクリーンショットを更新しています。また、この移行期間中に iOS ドキュメントで Citrix SSO のリファレンスが使用されていることに気付くかもしれません。

リリースノートでは、サービスリリースで利用できる新機能、既存機能の拡張、修正された問題、既知の問題について説明します。リリースノートには、次のセクションの 1 つまたは複数が含まれます:

新機能: 現在のリリースで利用できる新機能と拡張機能。

修正された問題: 現在のリリースで修正された問題。

既知の問題: 現在のリリースに存在する問題とその回避策 (該当する場合)。

> **EPA** クライアントに関する重要な注意事項**:**
>
> - EPA クライアントは macOS 10.13、10.14、10.15、11.x、12.x、13.x の各バージョンでサポートされています。
> - EPA クライアントは、NetScaler 12.1、13.0、13.1、および 14.1 のバージョンでサポートされています。

V24.03.1 (2024 年 3 月 14 日)

新機能

- EPA ライブラリが 24.03.1.0 (OPSWAT OESIS ライブラリ V 4.3.3460.0) に更新されました。

- **Citrix Workspace** アプリを介した **Citrix Secure Access** への自動シングルサインオン（**SSO**）**-**プレビュー

  macOS 向け Citrix Secure Access は、Citrix Workspace アプリにログオンしたときの Citrix Secure Access への自動シングルサインオン（SSO）をサポートするようになりました。この機能を利用するには、必ず macOS 24.03.1/Mac 2402 以降の Citrix Workspace アプリを使用してください。この機能はクラウドストアでのみサポートされ、オンプレミスストアではサポートされません。

  現在、この機能はデフォルトで無効になっています。https://podio.com/webforms/29383411/2410629を使用してプレビューにサインアップできます。

  詳しくは、Mac 向け Citrix Workspace アプリ 2402 のリリースノートを参照してください。

  [CSACLIENTS-6321]

- 全体的なパフォーマンスと安定性の向上

  Citrix Secure Access クライアントは、全体的なパフォーマンスと安定性を向上させるために、次の機能で強化されています:

  - VPN 経由でトンネリングできる同時接続数の増加。これは iOS クライアントにのみ適用されます。
  - IPv6 ゲートウェイによる VPN 接続の耐障害性が向上しました。これは macOS クライアントと iOS クライアントの両方に適用されます。

  [NSHELP-36903]

V24.02.1 (2024 年 2 月 15 日)

新機能

- **Mac** クライアントでの **EPA** スキャンオペレータのサポート

  macOS 向け Citrix Secure Access クライアントは、EPA エディターのすべての演算子<、>、>=、<=、==および!=をサポートするようになりました。また、**Mac OS** オプションは EPA エディタの個別のオプションとして使用できます (**Mac > Mac OS**)。これらのオペレータを使用して、macOS デバイスの製品バージョンスキャンを実行できます。

  詳細については、「高度なエンドポイント分析スキャン 」の「注意」セクションを参照してください。

  [CSACLIENTS-6462]

- EPA ライブラリが 24.1.2.1 (OPSWAT OESIS ライブラリ V 4.3.3405.0) に更新されました。

  [CSACLIENTS-8520]

- このリリースでは、全体的なパフォーマンスと安定性を向上させるためのいくつかの問題が修正されています。

24.1.5 MacOS 用 EPA クライアント (2024 年 2 月 12 日)

新機能

- **Apple** シリコンプロセッサを搭載した **Mac** デバイスの **EPA** サポート

  Citrix EPA クライアントは、Apple シリコンプロセッサを使用する Mac デバイスをサポートするようになりました。Mac デバイスでは、Citrix EPA クライアントを実行するために Rosetta をインストールする必要がなくなりました。

  [CSACLIENTS-8731]

- **Mac** クライアントでの **EPA** スキャンオペレータのサポート

  Mac 向け Citrix EPA クライアントは、EPA 式の演算子（<、>、>=および<=）をサポートするようになりました。管理者は EPA スキャンを設定して、さまざまな OS バージョンを許可できます。

  たとえば、12.8 を除く 12.4 から 13.0 までの OS バージョンを許可するには、管理者が式`version >= 12.4 && version <= 13.0 && version != 12.8`を設定できます。つまり、macOS のバージョンは 12.4 から 13.0 でなければなりませんが、12.8 であってはなりません。

  詳細については、高度なエンドポイント分析スキャンを参照してください。

  [CSACLIENTS-6462]

V23.12.2 (2023 年 12 月 20 日)

新機能

このリリースでは、全体的なパフォーマンスと安定性を向上させるための問題が修正されています。

V23.12.1 (2023 年 12 月 6 日)

新機能

- EPA ライブラリは 23.11.1.5 (OPSWAT OESIS ライブラリ V 4.3.3318.0) に更新されました。

  [CSACLIENTS-8516]

- このリリースでは、その他の問題も解決され、全体的なパフォーマンスと安定性が向上しています。

V23.11.2 (2023 年 11 月 1 日)

新機能

EPA ライブラリは 23.11.1.1 (OPSWAT OESIS ライブラリ V 4.3.3279.0) に更新されました。

[CSACLIENTS-8515]

V23.11.1 (2023 年 10 月 27 日)

新機能

- iOS 向け Citrix SSO の名前が Citrix Secure Access に変更されました。この名前の変更を反映するために、ドキュメント内の UI スクリーンショットを更新しています。
- EPA ライブラリは 23.10.1.1 (OPSWAT OESIS ライブラリ V 4.3.3246.0) に更新されました。
- このリリースでは、次の内容が取り上げられています:
  - Citrix Secure Private Access 環境での接続の問題。
  - 全体的なパフォーマンスと安定性を向上させるためのその他の問題。

V23.10.2 (2023 年 10 月 17 日)

このリリースでは、IPv6 ログインの問題が解決されています。

V23.10.1 (2023 年 10 月 9 日)

新機能

- EPA ライブラリは 23.9.1.2 (OPSWAT OESIS ライブラリ V4.3.3221.0) に更新されました。
- ローカル **LAN** アクセスのサポート

  Citrix Secure Access for macOS/Citrix SSO for iOS は、NetScaler Gateway のローカル LAN アクセス機能をサポートするようになりました。VPN 接続が確立されたら、エンドユーザーがクライアントデバイス上のローカル LAN リソースにアクセスすることを許可またはブロックするように、ローカル LAN アクセスを設定できます。詳しくは、以下を参照してください:
  - NetScaler Gateway 管理者設定
  - エンドユーザー設定-macOS
  - エンドユーザー設定-iOS

V23.09.1 (2023 年 9 月 7 日)

> 重要:
>
> macOS 14/iOS 17 以降などの最新の Apple OS バージョンを使用している場合は、Citrix Secure Access クライアント/Citrix SSO バージョン 23.09.1 以降にアップグレードすることをお勧めします。NetScaler

> Gateway クライアントのソフトウェア要件について詳しくは、「Citrix Secure Access クライアントのシステム要件」を参照してください。

新機能

- EPA ライブラリは 1.3.9.9 (OPSWAT OESIS v4.3.3160) にアップデートされました。

  [CSACLIENTS-6547]

- セキュリティで保護された接続に関するインサイトを **UI** で確認

  Citrix Secure Access クライアントユーザーインターフェイスの［接続］画面では、セキュリティで保護された接続の詳細を表示できます。詳細には、IP アドレス、FQDN、宛先ポート、接続時間が含まれます。詳細については、「安全な接続に関する洞察」を参照してください。

  [SPA-2364]

- **VPN** 接続障害後に **NetScaler Gateway** で再認証する

  MacOS 向け Citrix Secure Access クライアントおよび iOS 向け Citrix SSO は、VPN 接続が失われたときに NetScaler Gateway による再認証を求めるメッセージを表示するようになりました。NetScaler Gateway への接続が失われ、接続を再開するには再認証が必要であることを示す通知が UI に表示されます。詳しくは、次のトピックを参照してください:

  - VPN 接続が失敗した後に、macOS から NetScaler Gateway に再接続する
  - VPN 接続に障害が発生したら、iOS から NetScaler Gateway に再接続します。

  [CSACLIENTS-6071]

V23.08.1 (2023 年 8 月 24 日)

新機能

- このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。
- EPA ライブラリが 1.3.9.9 (OPSWAT OESIS v4.3.3122) にアップデートされました。

23.7.6 macOS 用 EPA クライアント (2023 年 8 月 10 日)

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V23.07.1 (2023 年 7 月 17 日)

新機能

- ログファイルを共有するためのさまざまなオプション

  iOS 向け Citrix SSO の「メールログ」オプションが「ログの共有」オプションに置き換えられました。圧縮されたログファイルは、電子メール、チャット、ファイルへの保存などのオプションで共有できるようになりました。

  詳しくは、「ログの送信」を参照してください。

  [CSACLIENTS-3834]

- 「ログ」ページの機能強化

  macOS 向け Citrix Secure Access の［ログ］ページが拡張され、次のオプションが追加されました。

  - ログファイルの最大数: ログ収集に追加するログファイルの最大数を指定します。
  - メールログ: ログをメールで送信します。

  詳しくは、「ログの送信」を参照してください。

  [SPA-2365]

解決された問題

VPN に接続するときに、認証用の証明書を選択するように求められた場合は、Citrix Secure Access クライアントのホームページの背後に認証ログイン画面が表示されます。

[CSACLIENTS-455]

V23.06.1 (2023 年 6 月 7 日)

新機能

- ナビゲーションバーのヘルプメニュー

  Citrix Secure Access クライアントのナビゲーションバーに [ヘルプ] メニューが追加されました。[ヘルプ] メニューのオプション ([ログを開く]、[ログをエクスポート]、[ログを電子メールで送信]、[ログをクリア]) は、ログのデバッグに使用できます。

  「ヘルプ」メニューに「メールログ」オプションが導入されました。電子メールでログを共有するために使用できます。詳しくは、「ログの送信」を参照してください。

  [SPA-2361]

解決された問題

macOS 向け Citrix Secure Access および iOS 向け Citrix SSO では、DNS の短縮名解決が失敗する場合があります。

[NSHELP-34568]

既知の問題

場合によっては、リバース分割トンネリングで除外されたルートがトンネリングされます。

[CGOP-24575]

V23.05.2 (2023 年 5 月 11 日)

解決された問題

アップグレード後、iOS 向け Citrix SSO クライアントデバイスはアプリごとの VPN 接続を確立できません。

[NSHELP-35224]

V23.05.1 (2023 年 5 月 4 日)

新機能

- EPA ライブラリは 1.3.9.3 に更新され、OPSWAT ライブラリは 4.3.2987 に更新されました。
- **Citrix Analytics** へのイベント送信のサポート

  macOS 向け Citrix Secure Access は、セッションの作成、セッションの終了、Citrix Analytics サービスへのアプリケーション接続などのイベントの送信をサポートするようになりました。その後、これらのイベントは Secure Private Access サービスのダッシュボードに記録されます。

  [SPA-2197]

解決された問題

- ユーザーが Citrix Secure Access または Citrix SSO に接続している場合、「接続時間」フィールドに地域固有の形式で時間が表示されません。

  [CGOP-23587]

V23.04.1 (2023 年 4 月 4 日)

新機能

- EPA ライブラリは 1.3.9.1 にアップデートされ、OPSWAT ライブラリは 4.3.2923 にアップデートされました。

V22.12.2 (2023 年 2 月 27 日)

新機能

- EPA ライブラリが 1.3.8.9 (OPSWAT OESIS v4.3.2892.0) にアップデートされました。

V22.12.1 (2022 年 12 月 7 日)

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V22.11.1 (2022 年 11 月 29 日)

解決された問題

- 転送ログオンは、オンプレミスゲートウェイの nFactor 以外の認証では機能しません。

  [CGOP-22729]

22.11.3 macOS 用 EPA プラグイン (2022 年 11 月 28 日)

解決された問題

- NetScaler で GSLB が有効になっていると、macOS 用 Citrix EPA プラグインがクラッシュします。

  [CGOP-22722]

V22.10.1 (2022 年 11 月 17 日)

新機能

- Citrix Endpoint Analysis プラグインは、許可される IP アドレスのリストに対してパターンセットを作成できる新しい MAC アドレス検証式をサポートするようになりました。

  [CGOP-22095]

解決された問題

- NetScaler Gateway リリース 13.0 または 13.1 のプロキシ設定が空の場合、Citrix SSO によって不適切なプロキシ設定が作成されることがあります。

  [NSHELP-31970]

- ネットワークが停止したり、デバイスがスリープモードから復帰したりすると、VPN クライアントは再接続に失敗することがあります。

  [NSHELP-32483]

- IPv6 リテラルを宛先として使用すると、ゲートウェイ接続が失敗することがあります。

  [NSHELP-32876]

22.10.1 macOS 用 EPA プラグイン (2022 年 10 月 27 日)

新機能

- Citrix Endpoint Analysis プラグインは、許可された IP アドレスのリストに対してパターンセットを作成できる新しい MAC アドレス検証式をサポートするようになりました。

  [CGOP-22098]

- Citrix Endpoint Analysis プラグインは、Google Chrome からのプライベートネットワークアクセスプリフライトリクエストを処理する際に、重複する同意アラートを送信します。

  [CGOP-21751]

V22.06.1 (2022 年 9 月 20 日)

新機能

- EPA ライブラリが 4.3.2523.0 (1.3.7.5) に更新されました

解決された問題

- EPA スキャンによる nFactor 認証は macOS クライアントでは機能しません。

  [NSHELP-32182-macOS]

- macOS 用の Secure Access Agent のホームページでは、選択したテーマ（明るいまたは暗い）に応じて、ハンバーガーメニューの左と上部に白または黒の余分なパディングが表示されます。

  [CGOP-19353-macOS]

- VPN にログインするときに、デバイス証明書が設定されていれば、WebView ウィンドウが最初の試行で最小化されます。

  [CGOP-19354-macOS]

- NetScaler ADC アプライアンスで GSLB が有効になっていると、macOS クライアント上の Citrix Secure Access アプリでエンドポイント分析が機能しません。

  [CGOP-21634-macOS]

- 設定したアプリケーション名にスペースが含まれている場合にアプリケーションにアクセスしようとしても、macOS クライアントに「セキュリティ強化有効」ポップアップが表示されません。

  [ACS-2632-macOS]

- デバイスに適切なクライアント証明書がない場合、オプションのクライアント証明書による nFactor 認証は失敗します。

  [NSHELP-32127-iOS]

- Chrome を使用する Mac デバイスで、2 つの FQDN にアクセス中に VPN 拡張機能がクラッシュします。

  [NSHELP-32144]

- Citrix Secure Access は、ゲートウェイから誤ったロケーション値を受信するとクラッシュします。これは、管理者が別のホストにリダイレクトするレスポンダーポリシーを定義した場合に発生する可能性があります。

  [NSHELP-32312]

- Citrix Secure Access によって確立されたトンネルの外部にあるリソースへの直接接続は、大幅な遅延または輻輳が発生すると失敗することがあります。

  [NSHELP-31598]

V3.2.4.9-macOS 用 EPA プラグイン (2022 年 8 月 1 日)

解決された問題

- Citrix Endpoint Analysis プラグインは、Google Chrome ブラウザバージョン 104 からのプライベートネットワークアクセスのプリフライトリクエストを処理しません。

  [CGOP-20709]

- macOS 用 Citrix Endpoint Analysis プラグインは GSLB をサポートしていません。

  [CGOP-21543]

既知の問題

- macOS 用 Citrix Endpoint Analysis プラグインを Google Chrome ブラウザバージョン 104 から起動すると、重複した同意ダイアログボックスが表示されます。ユーザーは両方のプロンプトを受け入れる必要があります。

  [CGOP-21751]

V22.03.1 (14-Jun-2022)

新機能

- EPA ライブラリは 4.3.2393.0 に更新されました。

解決された問題

- 検索リストに追加の DNS ドメインが追加されます。これは、分割トンネルが「スプリット」または「両方」に設定されている場合、指定されたドメインとそのサブドメインのみがトンネリングされないためです。指定したドメインが A.B.C の場合、A.B.C と *.A.B.C に加えて B.C も一致します。

  [CGOP-21657]

- PAC ファイルを使用しない HTTP/HTTPS プロキシ設定は壊れています。

  [CGOP-21660]

V22.02.3 (24-Mar-2022)

新機能

- Citrix Secure Access for macOS は、クラウドワークスペース接続のクライアントからのすべての TCP データ接続でサービスノードの FQDN を解決します。すべての TCP データ接続でサービスノードの FQDN を解決することは、オンプレミスのゲートウェイ接続には適用されません。

  [ACS-1068]

解決された問題

- ポート 53 を使用する一部の非 DNS プロトコル（STUN など）の問題により、macOS 向け Citrix Secure Access が接続を切断することがあります。

  [NSHELP-31004]

- Citrix Secure Access アプリは、接続が確立された直後にサーバーがクライアントの前にデータを送信すると、一部のプロトコルを中断します。

  [NSHELP-29374]

- ユーザーが認証を完了せずに macOS 向け Citrix Secure Access クライアントの認証ウィンドウを閉じると、その後サーバーに接続しようとしても、アプリが再起動されるまで失敗します。

  [ACS-2415]

- macOS 向け Citrix Secure Access クライアントが OPSWAT ライブラリバージョン 4.3.2367.0 にバンドルされるようになりました

  [NSHELP-30802]

- macOS 向け Citrix Secure Access は、認証後の EPA チェックの実行に予想よりも長い時間がかかります。

  [NSHELP-29118]

既知の問題

- macOS 向け Citrix Secure Access アプリは、すでに接続されている Citrix Secure Private Access サービスリージョンにアクセスできなくなった 1 分後にログアウトします。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

  [ACS-2715]

V22.02.2 (15-Feb-2022)

解決された問題

- ユーザーが Citrix Secure Access for macOS からサブスクライブ解除された Web アプリにアクセスしようとすると、複数のポップアップが表示されます。

  [ACS-2406]

V22.01.1 (08-Feb-2022)

解決された問題

- iOS デバイス向け Citrix SSO を使用したアプリごとの VPN 接続では、443 以外のポートで NetScaler Gateway に接続できません。

  [NSHELP-30653]

V1.4.1 (28-Jan-2022)

新機能

- macOS 向け Citrix SSO アプリは、Citrix Secure Access としてブランド名が変更されました。

  [ACS-1092]

解決された問題

- 認証サーバが同じ Web ビューセッションでクライアント証明書を複数回要求すると、クライアント証明書認証は失敗します。

  [CGOP-20388]

- クライアントと ADC の間にプロキシが存在するため、サーバー証明書に共通名の IP アドレスしかない場合、Citrix SSO は VPN 接続の確立に失敗します。

  [CGOP-20390]

- macOS でアンチウイルスの最後のフルシステムスキャンを確認するための EPA スキャンが失敗します。

  [NSHELP-29571]

- サイズの大きい DNS パケットの処理中に、Citrix SSO アプリがクラッシュすることがあります。

  [NSHELP-29133]

V1.4.0 (17-Nov-2021)

解決された問題

- サーバー証明書が信頼されていると、サーバー検証コードが失敗することがあります。その結果、エンドユーザーはゲートウェイにアクセスできなくなります。

  [NSHELP-28942]

- ネットワークが中断された後、Citrix SSO が VPN 接続の再確立に失敗します。

  [CGOP-19988]

V1.3.13 (05-Nov-2021)

解決された問題

- 管理対象 VPN と非管理対象 VPN のセッションをフィルタリングすると、障害が発生することがあります。セッションを確立する最初の要求で、User-Agent ヘッダーに「ManagedVPN」情報が欠落しています。

[CGOP-19561]

V1.3.12 (21-Oct-2021)

解決された問題

- macOS キーチェーンにクライアント証明書がない場合、Citrix SSO for macOS のクライアント証明書認証が失敗します。

  [NSHELP-28551]

- 通知を受信すると、Citrix SSO アプリが断続的にクラッシュする。

  [CGOP-19363]

- 機能フラグを確認するために「isFeatureEnabled」パラメーターが呼び出されると、VPN 拡張機能がクラッシュすることがあります。

  [CGOP-19360]

- DTLS プロトコルのペイロードが空の場合、ゲートウェイ VPN 拡張機能はクラッシュします。

  [CGOP-19361]

- デバイスがスリープモードから復帰し VPN が接続されると、SSO アプリが断続的にクラッシュします。

  [CGOP-19362]

V1.3.11 (17-Sep-2021)

解決された問題

- Citrix SSO を使用する macOS デバイスのファイアウォールチェックの EPA スキャンが失敗します。

  [CGOP-19271]

- レガシー認証または Intune ネットワークアクセスコンプライアンス（NAC）が構成されていると、iOS 12 デバイスで Citrix SSO がクラッシュする。

  [CGOP-19261]

V1.3.10 (31-Aug-2021)

新機能

- macOS 用の Citrix SSO は OPSWAT ライブラリバージョン 4.3.1977.0 にバンドルされるようになった。

  [NSHELP-28467]

V1.3.9 (13-Aug-2021)

解決された問題

- HTTP プロキシソフトウェアがインストールされている一部のシステムでは、NetScaler Gateway IP アドレスが内部的に 127.0.0.1 として表示されるため、トンネルの確立が妨げられます。

  [CGOP-18538]

- ［信頼できないサーバーをブロックする］設定は、Citrix SSO for iOS の英語以外のローカライズをサポートするシステムでは機能しません。

  [CGOP-18539]

- Citrix SSO は、DNS 名がサーバー証明書の共通名と一致しないシステムに接続できません。Citrix SSO はサブジェクトの別名をチェックし、正しく接続するようになりました。

  [NSHELP-28348]

V1.3.8 (07-Jul-2021)

新機能

- macOS 向け Citrix SSO は、バージョン 10.15（Catalina）以上とのみ互換性がある。

  [CGOP-12555]

- macOS バージョン 1.3.8 用の Citrix SSO 以降、EPA ライブラリはアプリ内に埋め込まれ、NetScaler Gateway サーバーからはダウンロードされません。現在の組み込み EPA ライブラリのバージョンは 1.3.5.1 です。

  [NSHELP-26838]

iOS ユーザー向け Citrix Secure Access のセットアップ

April 1, 2024

> 重要：
>
> - iOS 向け Citrix SSO の名前が Citrix Secure Access に変更されました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。この移行期間中に、ドキュメントで Citrix SSO のリファレンスが使用されていることに気付くかもしれません。
> - VPN は iOS 12 以降では使用できません。VPN を引き続き使用するには、Citrix Secure Access を使用

> してください。

iOS 向け Citrix Secure Access でサポートされている一般的に使用される機能の一覧については、「NetScaler Gateway VPN クライアントとサポートされている機能」を参照してください。

MDM 製品との互換性

Citrix Secure Access（macOS/iOS）は、Citrix Endpoint Management（旧 XenMobile）、Microsoft Intune などのほとんどの MDM プロバイダーと互換性があります。

Citrix Secure Access（macOS/iOS）は、ネットワークアクセス制御（NAC）と呼ばれる機能もサポートしています。NAC について詳しくは、「単一要素ログイン用の NetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成」を参照してください。NAC を使用すると、MDM 管理者は NetScaler ADC アプライアンスに接続する前にエンドユーザーデバイスのコンプライアンスを強制できます。Citrix Secure Access (macOS/iOS) 上の NAC には、Citrix Endpoint Management や Intune と NetScaler などの MDM サーバーが必要です。

> 注:
>
> macOS/iOS で Citrix Secure Access クライアントを MDM なしで NetScaler Gateway VPN で使用するには、VPN 構成を追加する必要があります。iOS の VPN 構成は、Citrix Secure Access（macOS/iOS）のホームページから追加できます。

Citrix Secure Access クライアント (macOS/iOS) 用の MDM マネージド VPN プロファイルの設定

次のセクションでは、例として Citrix Endpoint Management（旧 XenMobile）を使用して、Citrix Secure Access クライアント（macOS/iOS）のデバイス全体の VPN プロファイルとアプリごとの VPN プロファイルの両方を構成する手順を段階的に説明します。他の MDM ソリューションでは、Citrix Secure Access（macOS/iOS）を使用する際の参考資料としてこのドキュメントを使用できます。

> 注:
>
> このセクションでは、基本的なデバイス全体およびアプリごとの VPN プロファイルの設定手順について説明します。また、Citrix Endpoint Management（旧 XenMobile）のマニュアルまたは Apple の MDMVPN ペイロード構成に従って、オンデマンドプロキシを構成することもできます。

デバイスレベルの VPN プロファイル

デバイスレベルの VPN プロファイルは、システム全体の VPN を設定するために使用されます。すべてのアプリとサービスからのトラフィックは、NetScaler ADC で定義された VPN ポリシー（フルトンネル、分割トンネル、リバース分割トンネルなど）に基づいて NetScaler Gateway にトンネリングされます。

Citrix Endpoint Management でデバイスレベルの **VPN** を構成するには　Citrix Endpoint Management でデバイスレベルの VPN を構成するには、次の手順を実行します。

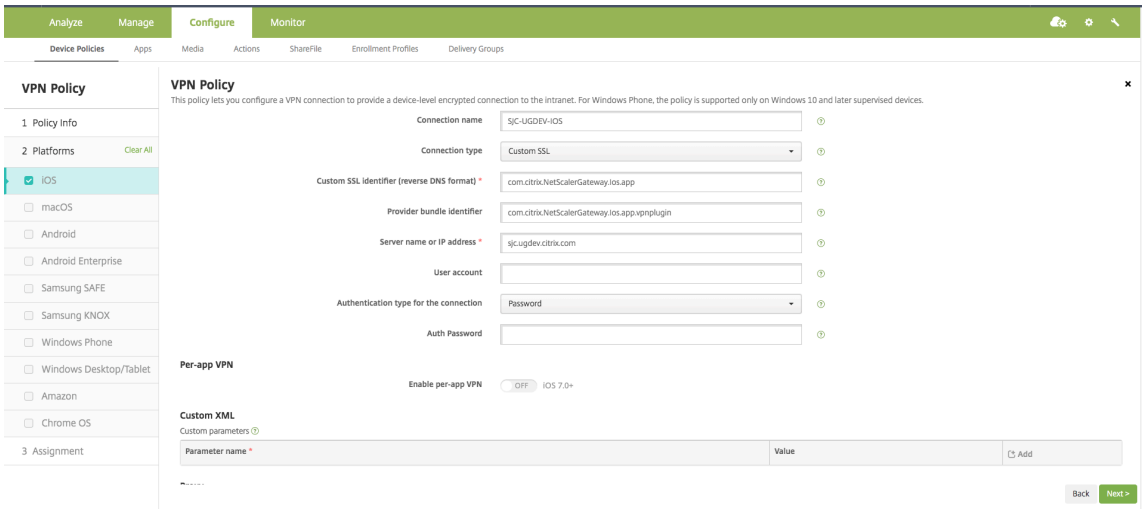
1. Citrix Endpoint Management MDM コンソールで、［構成］>［デバイスポリシー］>［新しいポリシーの追加］に移動します。
2. 左側の [ポリシープラットフォーム] ペインで [**iOS**] を選択します。右側のペインで [**VPN**] を選択します。
3. [ポリシー情報] ページで、有効なポリシー名と説明を入力し、[次へ] をクリックします。
4. **iOS** の **[**VPN** ポリシー] ページで、有効な接続名を入力し、[接続の種類] で [カスタム **SSL**] を選択します。**

   MDM VPN ペイロードでは、接続名は **UserDefinedName** キーに対応し、**VPN** タイプキーは **VPN** に設定する必要があります。
5. [カスタム **SSL** 識別子 **(**リバース **DNS** 形式**)**] に **com.citrix.NetScalerGateway.ios.app** と入力します。これは、iOS 上の Citrix Secure Access のバンドル識別子です。

   MDM VPN ペイロードでは、カスタム SSL 識別子は **VPNSubType** キーに対応します。
6. [プロバイダーバンドル識別子] に **com.citrix.NetScalerGateway.ios.app.vpnplugin** と入力します。これは、Citrix Secure Access iOS アプリバイナリに含まれるネットワーク拡張のバンドル識別子です。

   MDM VPN ペイロードでは、プロバイダーバンドル識別子は **ProviderBundleIdentifier** キーに対応します。
7. [サーバー名または **IP** アドレス] に、この Citrix Endpoint Management インスタンスに関連付けられた NetScaler ADC IP アドレスまたは FQDN（完全修飾ドメイン名）を入力します。

   設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧 XenMobile）のドキュメントを参照してください。
8. ［次へ］をクリックします。



9. ［保存］をクリックします。

アプリごとの **VPN** プロファイル

アプリごとの VPN プロファイルは、特定のアプリケーションの VPN を設定するために使用されます。特定のアプリからのトラフィックのみが、NetScaler Gateway にトンネリングされます。**Per-App VPN** ペイロードは、デバイス全体の VPN のすべてのキーに加えて、その他いくつかのキーをサポートします。

Citrix Endpoint Management でアプリごとのレベルの **VPN** を構成するには　アプリ単位 VPN を設定するには、次の手順を実行します。

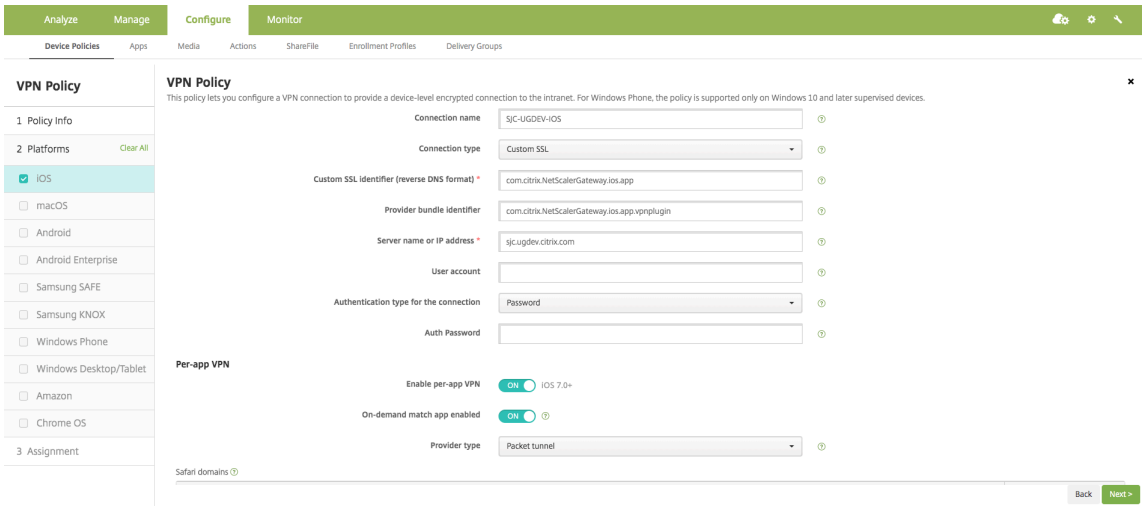
1. Citrix Endpoint Management でデバイスレベルの VPN 構成を完了します。
2. [アプリベース VPN] セクションの [アプリベース **VPN** を有効にする] スイッチをオンにします。
3. マッチアプリの起動時に Citrix Secure Access（macOS/**iOS**）を自動的に起動する必要がある場合は、「オンデマンドマッチアプリを有効にする」スイッチをオンにしてください。これは、ほとんどのアプリごとのケースで推奨されます。

   MDM VPN ペイロードでは、このフィールドは **onDemandMatchAppEnabled** キーに対応します。
4. [プロバイダーの種類] で [パケットトンネル] を選択します。

   MDM VPN ペイロードでは、このフィールドはキープロバイダータイプに対応します。
5. Safari ドメインの設定はオプションです。Safari ドメインを設定すると、ユーザーが Safari を起動し、「ドメイン」フィールドの URL と一致する URL に移動すると、Citrix Secure Access（macOS/iOS）が自動的に起動します。特定のアプリの VPN を制限する場合、これはお勧めできません。

   MDM VPN ペイロードでは、このフィールドはキー **safariDomains** に対応します。

   設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧 XenMobile）のドキュメントを参照してください。



6. [次へ] をクリックします。

7. [保存] をクリックします。

この VPN プロファイルをデバイス上の特定のアプリに関連付けるには、このガイド（）に従って、アプリインベントリポリシーと認証情報プロバイダーポリシーを作成する必要があります。https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/。

アプリ単位 **VPN** での分割トンネルの設定

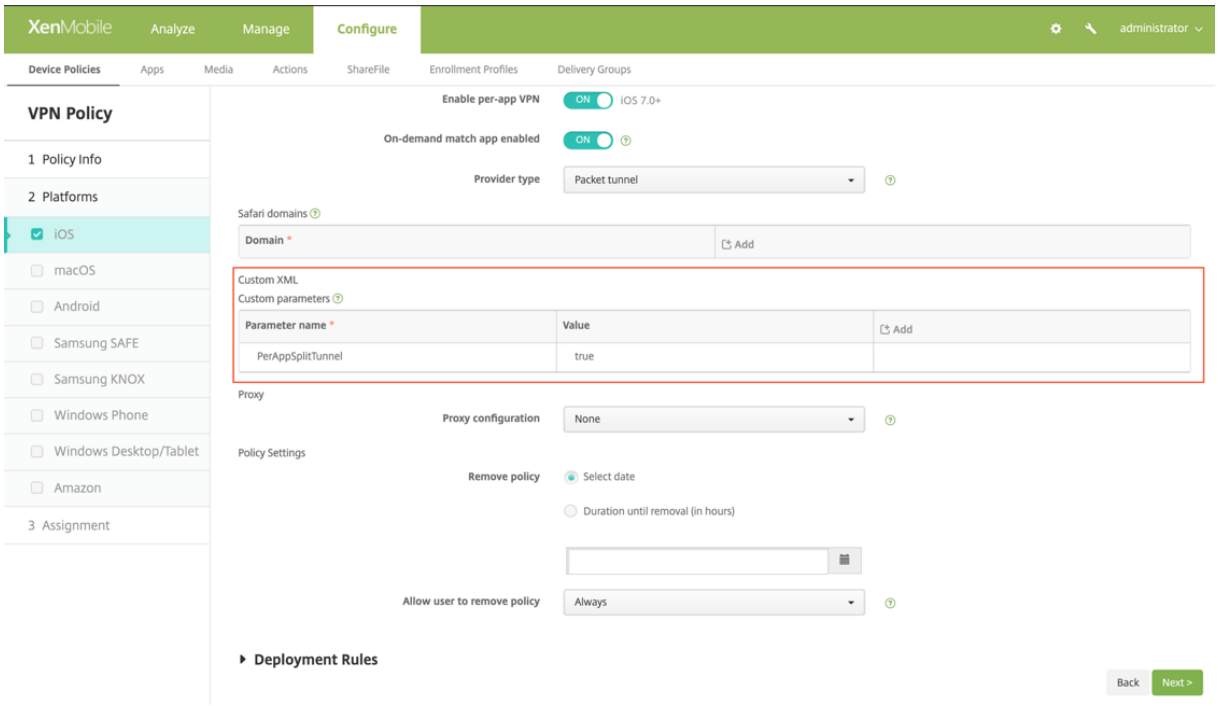
MDM のお客様は、Citrix Secure Access（macOS/iOS）用のアプリベース VPN で分割トンネルを構成できます。次のキーと値のペアは、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに追加する必要があります。

```
-  Key = "PerAppSplitTunnel"
-  Value = "true or 1 or yes"
<!--NeedCopy-->
```

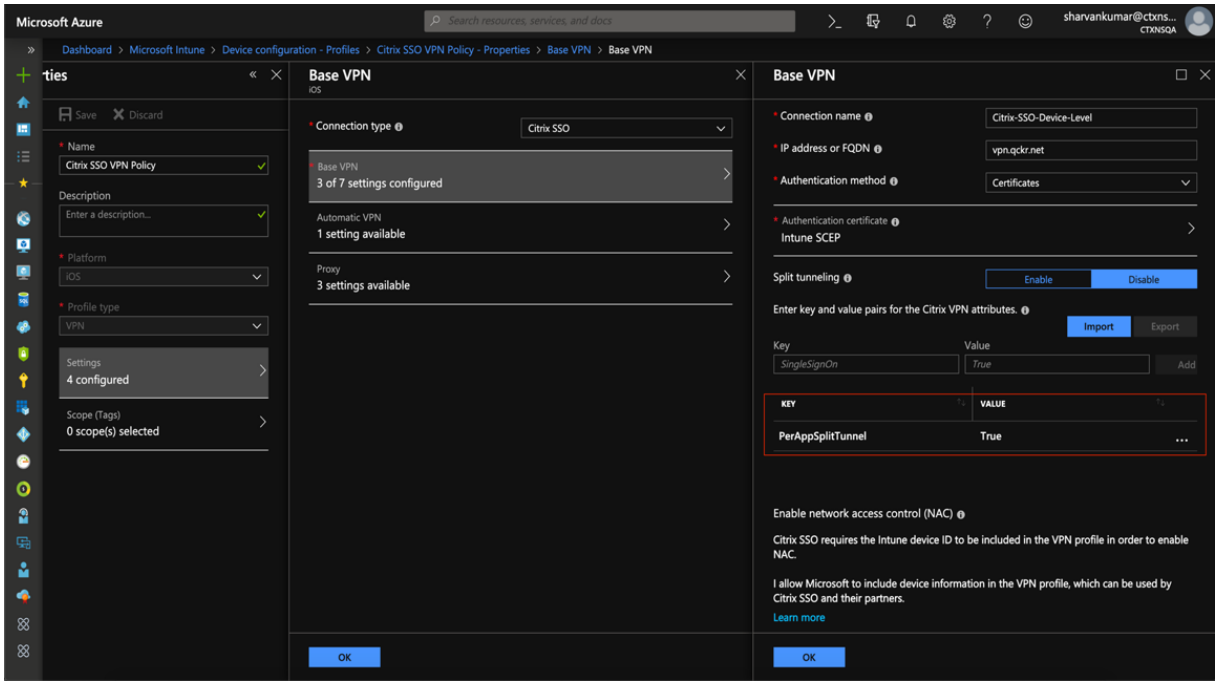
キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

> 注:
>
> ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Management の構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



ユーザー作成の **VPN** プロファイルの無効化

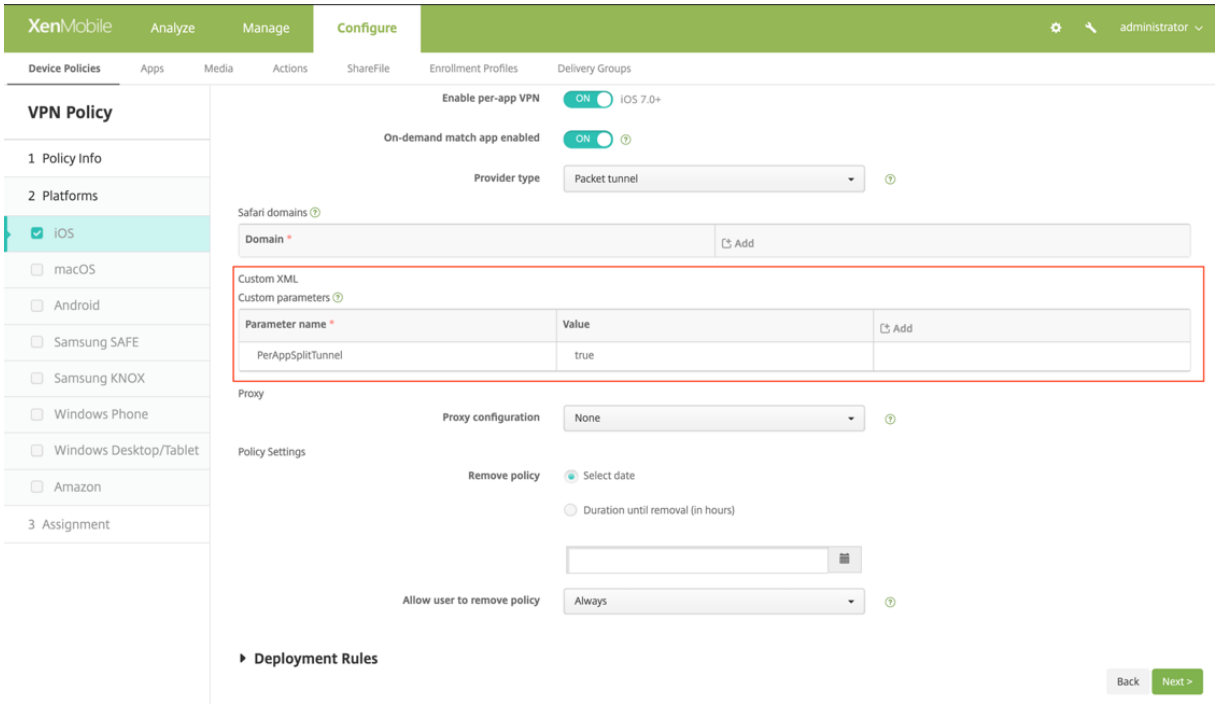
MDM のお客様は、ユーザーが Citrix Secure Access（macOS/iOS）内から手動で VPN プロファイルを作成することを防ぐことができます。これを行うには、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに、次のキーと値のペアを追加する必要があります。

```
1  -  Key = "disableUserProfiles"
2  -  Value = "true or 1 or yes"
3  <!--NeedCopy-->
```

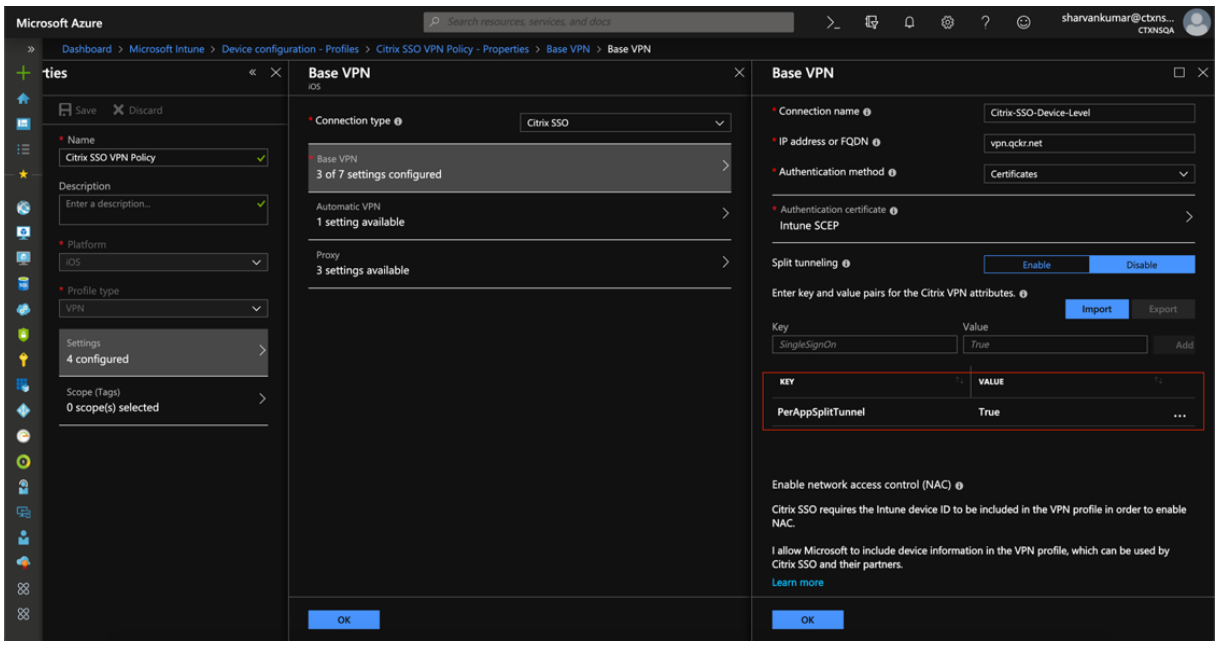
キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

> 注:
>
> ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Management の構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



DNS ハンドリング

Citrix Secure Access クライアントの推奨 DNS 設定は次のとおりです:

- 分割トンネルが **OFF** に設定されている場合は、スプリット **DNS > REMOTE**。

- 分割トンネルが **ON** に設定されている場合は、スプリット **DNS** **BOTH**。この場合、管理者はイントラネットドメインの DNS サフィックスを追加する必要があります。DNS サフィックスに属する FQDN の DNS クエリは NetScaler ADC アプライアンスにトンネリングされ、残りのクエリはローカルルーターに送信されます。

> 注:
>
> - **DNS** 切り捨て修正フラグは常に **ON** にすることをお勧めします。詳しくは、「https://support.citrix.com/article/CTX200243」を参照してください。
> - 分割トンネルが **ON** に設定され、スプリット DNS が **REMOTE** に設定されている場合、VPN の接続後に DNS クエリーを解決する際に問題が発生する可能性があります。これは、ネットワーク拡張フレームワークがすべての DNS クエリをインターセプトしない場合に関連しています。

既知の問題

問題の説明: アプリ単位 VPN またはオンデマンド VPN 構成の "`.local`" ドメインを含む FQDN アドレスのトンネリング。Apple の Network Extension フレームワークには、ドメイン部分（たとえば http://wwww.abc.local）`.local` に含まれる FQDN アドレスがシステムの TUN インターフェイスを介してトンネリングされないようにするバグがあります。代わりに、FQDN アドレスのトラフィックは、クライアントデバイスの物理インターフェイスを介して送信されます。この問題は、アプリ単位 VPN またはオンデマンド VPN の設定でのみ発生し、システム全体の VPN 設定では発生しません。Citrix は Apple にレーダーバグレポートを提出しており、Apple は、RFC-6762 によると https://tools.ietf.org/html/rfc6762、ローカルはマルチキャスト DNS（mDNS）クエリであり、したがってバグではないと述べています。しかし、Apple はまだバグをクローズしておらず、この問題が将来の iOS リリースで対処されるかどうかは明らかではありません。

回避策：回避策として、このようなアドレスに`non .local`ドメイン名を割り当てます。

制限事項

- エンドポイント分析 (EPA) は iOS ではサポートされていません。
- ポート/プロトコルに基づく分割トンネリングはサポートされていません。

ユーザー証明書の **ID** を電子メールの添付ファイルとして **iOS** ユーザーに送信する

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するた

> めに、ドキュメントと UI スクリーンショットを更新しています。

iOS 上の Citrix Secure Access は、NetScaler Gateway によるクライアント証明書認証をサポートしています。iOS では、証明書は次のいずれかの方法で Citrix Secure Access に配信できます:

- MDM サーバ-これは MDM のお客様にとって好ましいアプローチです。証明書は MDM 管理の VPN プロファイルで直接構成されます。デバイスが MDM サーバーに登録されると、VPN プロファイルと証明書の両方が登録済みデバイスにプッシュされます。このアプローチについては、MDM ベンダー固有のドキュメントに従ってください。
- メール - MDM 以外をご使用のお客様の唯一のアプローチです。この方法では、管理者は PCKS #12 ファイルとしてユーザー証明書 ID (証明書と秘密キー) を添付した電子メールをユーザーに送信します。ユーザーが添付ファイル付きのメールを受信するには、iOS デバイスでメールアカウントを設定する必要があります。その後、ファイルを iOS の Citrix Secure Access にインポートできます。次のセクションでは、このアプローチの設定手順について説明します。

前提条件

- ユーザー証明書-特定のユーザーの拡張子が.pfx または.p12 の PKCS #12 識別ファイル。このファイルには、証明書と秘密キーの両方が含まれています。
- iOS デバイスで設定された電子メールアカウント。
- iOS デバイスに Citrix Secure Access がインストールされています。

構成の手順

1. ユーザー証明書の拡張/MIME タイプの名前を変更します。

   ユーザー証明書で最も一般的に使用されるファイル拡張子は、「.pfx」、「.p12」などです。これらのファイル拡張子は、.pdf、.doc などの形式とは異なり、iOS プラットフォームでは標準ではありません。「.pfx」と「.p12」はどちらも iOS システムによって要求され、Citrix Secure Access などのサードパーティアプリでは要求できません。そのため、Citrix Secure Access は「.citrixsso-pfx」と「.citrixsso-p12」という新しい拡張機能/MIME タイプを定義しました。管理者は、ユーザー証明書の拡張子/MIME タイプを標準の「.pfx」または「.p12」から「.citrixsso-pfx」または「.citrixsso-p12」
   にそれぞれ変更する必要があります。拡張機能の名前を変更するには、管理者はコマンドプロンプトまたはターミナルで次のコマンドを実行します。

   Windows 10

   ```
   cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
   rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
      citrixsso-pfx
   <!--NeedCopy-->
   ```


macOS

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
<!--NeedCopy-->
```

2. ファイルを電子メールの添付ファイルとして送信します。

   新しい拡張子を持つユーザー証明書ファイルは、電子メールの添付ファイルとしてユーザーに送信できます。

   電子メールを受信したら、ユーザーは Citrix Secure Access に証明書をインストールする必要があります。

iOS ユーザー用の Citrix SSO アプリ用または macOS ユーザー用の Citrix Secure Access クライアント用のプロキシ PAC ファイルのセットアップ

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。

iOS 向け Citrix Secure アプリまたは macOS 向け Citrix Secure Access クライアントは、VPN トンネルの確立後に自動プロキシ構成（プロキシ PAC ファイル）をサポートします。管理者はプロキシ PAC ファイルを使用して、ホスト名の解決を含め、クライアントのすべての HTTP トラフィックがプロキシを通過することを許可できます。

プロキシ PAC ファイルを設定する方法

プロキシファイルをホストできる内部マシンがある。たとえば、マシンの IP アドレスが 172.16.111.43 で、PAC ファイルの名前が proxy.pac であるとします。

実際のプロキシサーバの IP アドレスが、ポート 8080 でリッスンしている 172.16.43.83 である場合、proxy.pac のサンプルは次のようになります。
関数 findProxyForUrl (url, host)
{「PROXY 172.16.43. 83:8080」
を返す;
}

プロキシ PAC URL はhttp://172.16.111.43/proxy.pacです。ファイルがポート HTTP ポート 80 でホストされていると仮定します。

詳細については、https://support.citrix.com/article/CTX224235または「NetScaler Gateway の送信プロキシサポートのプロキシ自動構成」を参照してください。

注:

- 分割トンネルがオンの場合は、PAC ファイルをホストするサーバの IP アドレスがイントラネットアプリケーションリストに含まれていることを確認し、VPN 経由でアクセスできるようにします。
- Citrix Secure Access（macOS/iOS）からログインすると、ブラウザはプロキシ PAC ファイルのルールを使用し始めます。前の例のようにプロキシルールを 1 つだけ指定すると、すべての HTTP または HTTPS トラフィックが内部プロキシサーバにルーティングされます。

macOS ユーザー向け **Citrix Secure Access** のセットアップ

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。

macOS 向け Citrix Secure Access クライアントは、NetScaler Gateway が提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションを提供します。ビジネスクリティカルなアプリケーション、仮想デスクトップ、企業データにいつでもどこからでも安全にアクセスできるようになりました。
Citrix Secure Access は、macOS デバイスからの VPN 接続を作成および管理するための NetScaler Gateway 用の次世代 VPN クライアントです。Citrix Secure Access は、Apple のネットワーク拡張（NE）フレームワークを使用して構築されています。Apple の NE フレームワークは、macOS のコアネットワーク機能をカスタマイズおよび拡張するために使用できる API を含む最新のライブラリです。SSL VPN をサポートするネットワーク拡張は、macOS 10.11 以降を実行しているデバイスで利用できます。

Citrix Secure Access は、macOS でモバイルデバイス管理（MDM）を完全にサポートします。管理者は、MDM サーバーを使用してデバイスレベルの VPN プロファイルやアプリごとの VPN プロファイルをリモートで構成して管理できるようになりました。
macOS 向け Citrix Secure Access は、Mac App Store からインストールできます。

macOS 向け Citrix Secure Access クライアントでサポートされる一般的に使用される機能のリストについては、「NetScaler Gateway VPN クライアントとサポートされている機能」を参照してください。

MDM 製品との互換性

macOS 向け Citrix Secure Access は、Citrix XenMobile、Microsoft Intune などのほとんどの MDM プロバイダーと互換性があります。ネットワークアクセス制御（NAC）と呼ばれる機能をサポートしています。これを使用して、MDM 管理者は NetScaler Gateway に接続する前にエンドユーザーデバイスのコンプライアンスを強制できます。Citrix Secure Access 上の NAC を使用するには、XenMobile や NetScaler Gateway などの MDM サーバー

が必要です。NAC について詳しくは、「単一要素ログイン用の NetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成」を参照してください。

> 注:
>
> MDM なしで NetScaler Gateway VPN で Citrix Secure Access を使用するには、VPN 構成を追加する必要があります。macOS の VPN 構成は、［Citrix Secure Access］構成ページから追加できます。

Citrix Secure Access の MDM 管理対象 VPN プロファイルを構成する

次のセクションでは、Citrix Endpoint Management（以前の XenMobile）を例として使用して、Citrix Secure Access のデバイス全体の VPN プロファイルとアプリごとの VPN プロファイルの両方を構成する手順を説明します。他の MDM ソリューションでは、Citrix Secure Access を使用する際の参照としてこのドキュメントを使用できます。

> 注:
>
> このセクションでは、基本的なデバイス全体およびアプリごとの VPN プロファイルの設定手順について説明します。また、Citrix Endpoint Management（旧 XenMobile）のマニュアルまたは Apple の MDMVPN ペイロード構成に従って、オンデマンドプロキシを構成することもできます。

デバイスレベルの VPN プロファイル

デバイスレベルの VPN プロファイルは、システム全体の VPN を設定するために使用されます。すべてのアプリとサービスからのトラフィックは、NetScaler ADC で定義された VPN ポリシー（フルトンネル、分割トンネル、リバース分割トンネルなど）に基づいて NetScaler Gateway にトンネリングされます。

Citrix Endpoint Management でデバイスレベルの **VPN** を構成するには　デバイスレベル VPN を設定するには、次の手順を実行します。

1. Citrix Endpoint Management MDM コンソールで、［構成］ > ［デバイスポリシー］ > ［新しいポリシーの追加］ に移動します。
2. 左側の [ポリシープラットフォーム] ペインで [**macOS**] を選択します。右側のペインで [**VPN** ポリシー] を選択します。
3. [ポリシー情報] ページで、有効なポリシー名と説明を入力し、[次へ] をクリックします。
4. **macOS** の **[**** ポリシーの詳細] ページで、有効な接続名を入力し、[接続の種類] で [カスタム **SSL**] を選択します。**

   MDM VPN ペイロードでは、接続名は **UserDefinedName** キーに対応し、**VPN** タイプキーは **VPN** に設定する必要があります。

5. [カスタム **SSL** 識別子 **(**リバース **DNS** 形式**)**] に **com.citrix.netscalergateway.macos.app** と入力します。macOS 上の Citrix Secure Access のバンドル識別子です。

   MDM VPN ペイロードでは、カスタム SSL 識別子は **VPNSubType** キーに対応します。

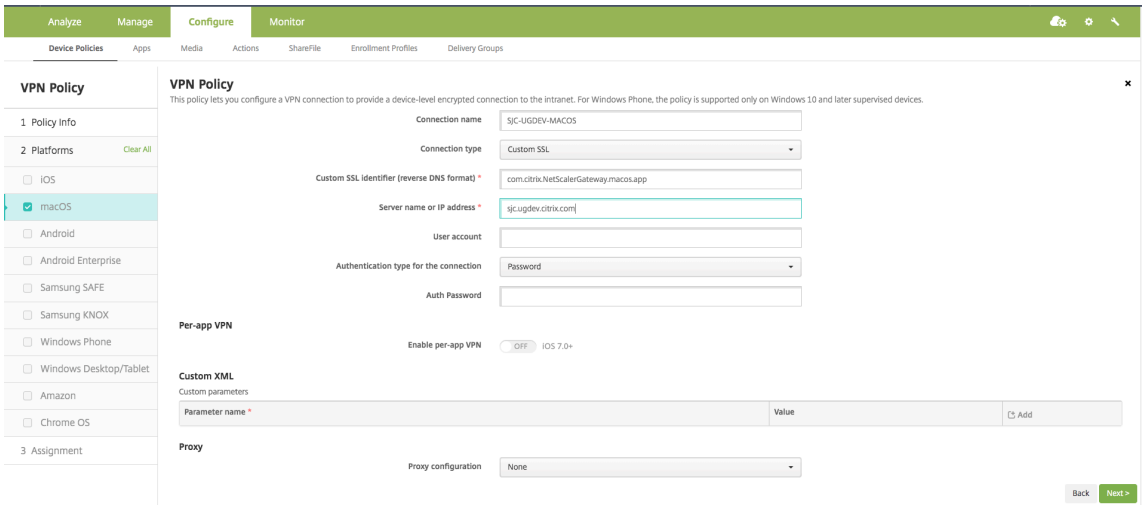
6. [プロバイダーバンドル識別子] に **com.citrix.NetScalerGateway.macos.app.VPnPlugin** と入力します。これは、Citrix Secure Access クライアントバイナリに含まれるネットワーク拡張のバンドル識別子です。

   MDM VPN ペイロードでは、プロバイダーバンドル識別子は **ProviderBundleIdentifier** キーに対応します。

7. [サーバー名または **IP** アドレス] に、この Citrix Endpoint Management インスタンスに関連付けられている NetScaler ADC IP アドレスまたは完全修飾ドメイン名を入力します。

   設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management のドキュメントを参照してください。

8. [次へ] をクリックします。



9. [保存] をクリックします。

アプリごとの **VPN** プロファイル

アプリごとの VPN プロファイルは、特定のアプリケーションの VPN を設定するために使用されます。特定のアプリからのトラフィックのみが、NetScaler Gateway にトンネリングされます。**Per-App VPN** ペイロードは、デバイス全体の **VPN** のすべてのキーに加えて、その他いくつかのキーをサポートします。

Citrix Endpoint Management でアプリごとのレベルの **VPN** を構成するには　次の手順を実行して、Citrix Endpoint Management でアプリ単位 VPN を構成します。

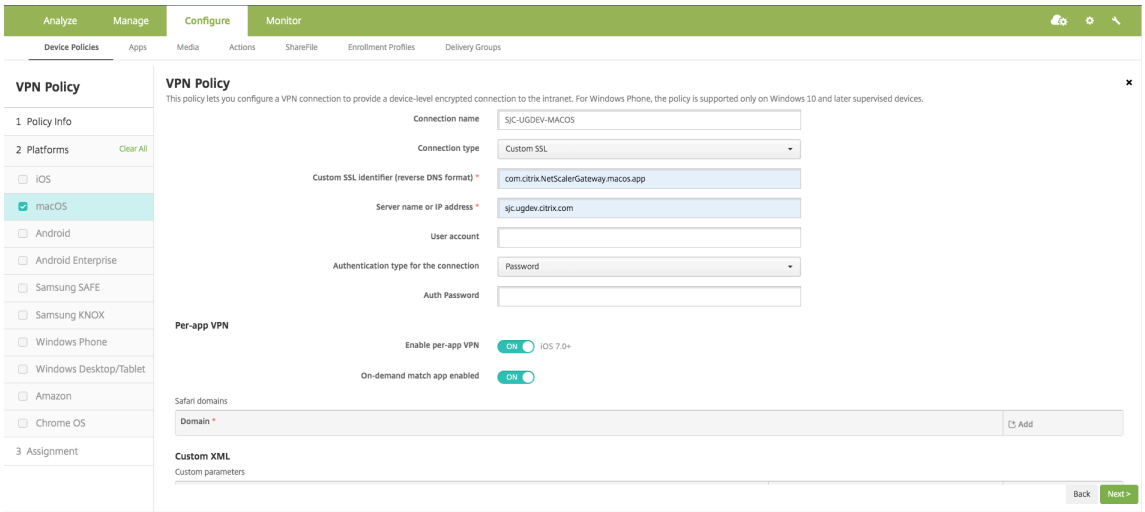
1. Citrix Endpoint Management でデバイスレベルの VPN 構成を完了します。

2. [アプリベース VPN] セクションの [アプリベース **VPN** を有効にする] スイッチをオンにします。
3. マッチアプリの起動時に **Citrix Secure Access** を自動的に起動する必要がある場合は、[オンデマンドマッチアプリ有効] スイッチをオンにします。これは、ほとんどのアプリごとのケースで推奨されます。

   MDM VPN ペイロードでは、このフィールドは **onDemandMatchAppEnabled** キーに対応します。
4. Safari ドメインの設定はオプションです。Safari ドメインが構成されている場合、ユーザーが Safari を起動し、「ドメイン」フィールドの URL と一致する URL に移動すると、Citrix Secure Access が自動的に起動します。特定のアプリの VPN を制限する場合、これはお勧めできません。

   MDM VPN ペイロードでは、このフィールドはキー **safariDomains** に対応します。

   設定ページの残りのフィールドはオプションです。これらのフィールドの構成については、Citrix Endpoint Management（旧 XenMobile）のドキュメントを参照してください。



5. [次へ] をクリックします。
6. [保存] をクリックします。

   VPN プロファイルをデバイス上の特定のアプリに関連付けるには、このガイドに従って、アプリインベントリポリシーと認証情報プロバイダーポリシーを作成する必要があります。https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

アプリ単位 **VPN** での分割トンネルの設定

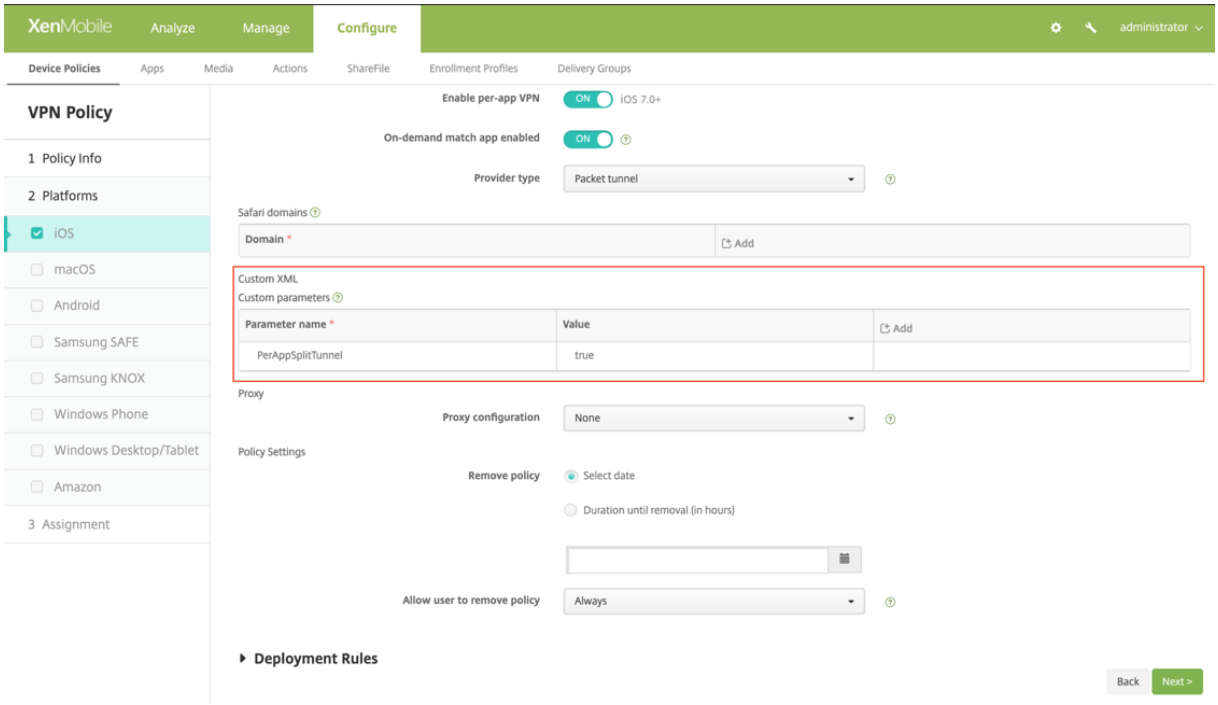
MDM のお客様は、Citrix Secure Access のアプリ単位 VPN で分割トンネルを構成できます次のキーと値のペアは、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに追加する必要があります。

```
- Key = "PerAppSplitTunnel"
- Value = "true or 1 or yes"
```

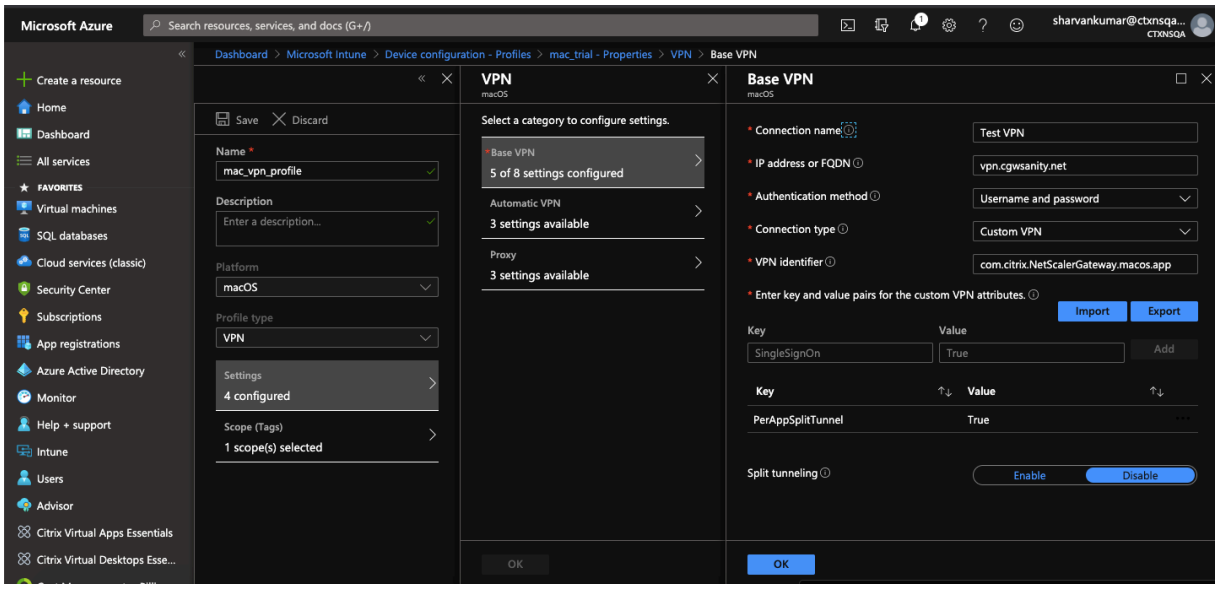
キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

> 注:
>
> ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー全体で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Management の構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



ユーザー作成の **VPN** プロファイルの無効化

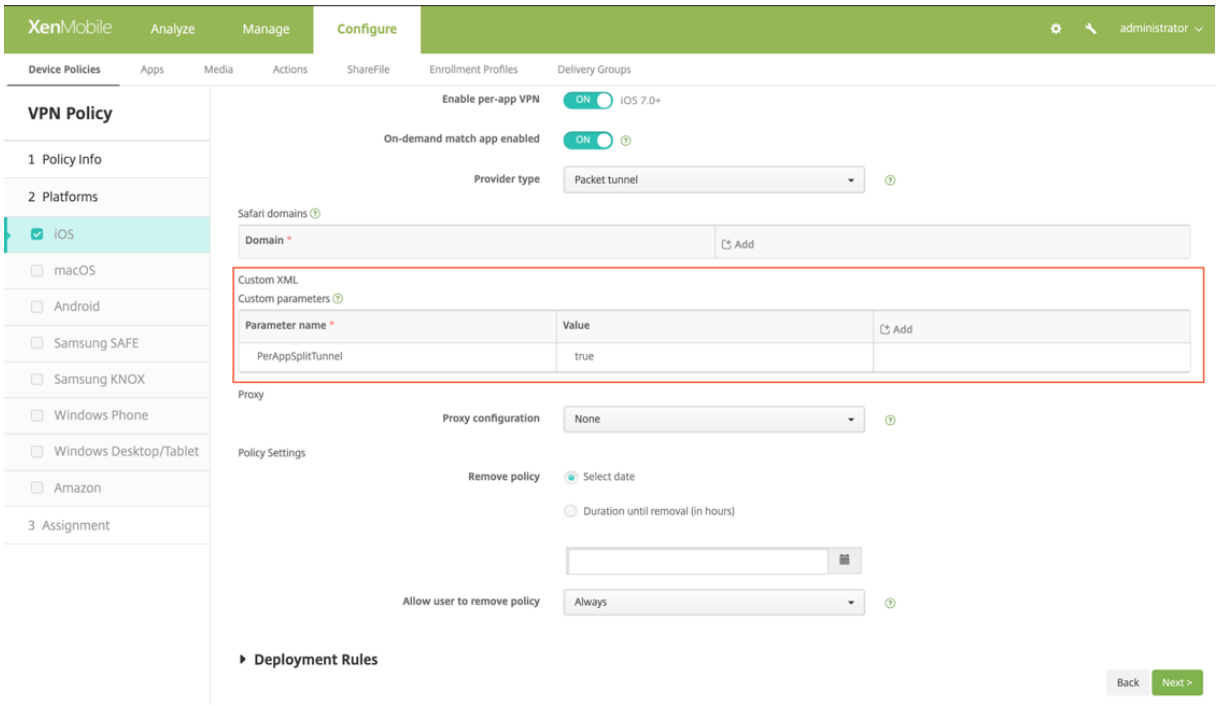
MDM のお客様は、ユーザーが Citrix Secure Access 内から VPN プロファイルを手動で作成できないようにすることができます。これを行うには、MDM サーバで作成された VPN プロファイルのベンダー設定セクションに、次のキーと値のペアを追加する必要があります。

```
1  -  Key = "disableUserProfiles"
2  -  Value = "true or 1 or yes"
```

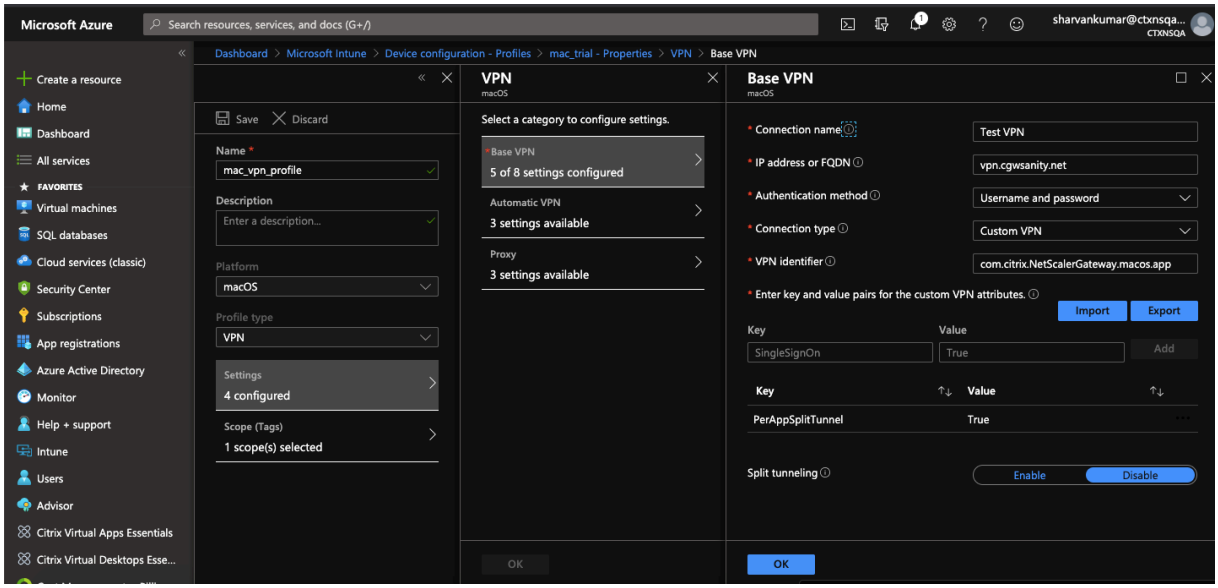
キーは大文字と小文字が区別され、完全に一致する必要がありますが、値の大文字と小文字は区別されません。

> 注:
>
> ベンダー構成を設定するためのユーザーインターフェイスは、MDM ベンダー間で標準ではありません。MDM ユーザーコンソールのベンダー設定セクションを見つけるには、MDM ベンダーに問い合わせてください。

以下は、Citrix Endpoint Management の構成（ベンダー固有の設定）のサンプルスクリーンショットです。



以下は、Microsoft Intune での構成 (ベンダー固有の設定) のサンプルスクリーンショットです。



DNS ハンドリング

Citrix Secure Access で推奨される DNS 設定は次のとおりです。

- 分割トンネルが **OFF** に設定されている場合は、スプリット **DNS > REMOTE**。
- 分割トンネルが **ON** に設定されている場合は、スプリット **DNS ****BOTH**。この場合、管理者はイントラネットドメインの DNS サフィックスを追加する必要があります。DNS サフィックスに属する FQDN の DNS クエリは NetScaler ADC アプライアンスにトンネリングされ、残りのクエリはローカルルーターに送信されます。

> 注:
>
> - **DNS** 切り捨て修正フラグは常に **ON** にすることをお勧めします。詳しくは、「https://support.citrix.com/article/CTX200243」を参照してください。
> - 分割トンネルが **ON** に設定され、スプリット DNS が **REMOTE** に設定されている場合、VPN の接続後に DNS クエリーを解決する際に問題が発生する可能性があります。これは、ネットワーク拡張フレームワークがすべての DNS クエリをインターセプトしない場合に関連しています。

サポートされている **EPA** スキャン

サポートされているスキャンの完全なリストについては、最新の EPA ライブラリを参照してください。

1. [**OPSWAT v4** でサポートされているスキャンマトリックス] セクションで、[**MAC OS** 固有] 列の [サポートされるアプリケーションリスト] をクリックします。
2. Excel ファイルで、[クラシック **EPA** スキャン] タブをクリックして詳細を表示します。

既知の問題

以下は、現在の既知の問題です。

- ユーザーが検疫グループに配置されている場合、EPA ログインは失敗します。
- 強制タイムアウト警告メッセージは表示されません。
- Citrix Secure Access では、分割トンネルがオンで、イントラネットアプリが構成されていない場合にログインできます。

制限事項

以下は、現在の制限事項です。

- 次の EPA スキャンは、サンドボックス化によりセキュアアクセスへのアクセスが制限されているために失敗する可能性があります。
  - ハードディスク暗号化 'type' と 'path'
  - Web ブラウザの「デフォルト」と「実行中」
  - パッチ管理「見つからないパッチ」
  - EPA 中にプロセスの強制終了操作
- ポート/プロトコルに基づく分割トンネリングはサポートされていません。
- キーチェーンに同じ名前と有効期限を持つ証明書が 2 つ存在しないようにしてください。この場合、クライアントには両方の証明書ではなく 1 つの証明書のみが表示されます。

トラブルシューティング

Citrix Secure Access の認証ウィンドウにエンドユーザーに［**EPA** プラグインのダウンロード］ボタンが表示される場合は、NetScaler アプライアンスのコンテンツセキュリティポリシーが URL`com.citrix.agmacepa://`の呼び出しをブロックしていることを意味します。管理者は、`com.citrix.agmacepa://`が許可されるようにコンテンツセキュリティポリシーを変更する必要があります。

macOS/iOS 上の Citrix Secure Access クライアントの nFactor サポート

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。

多要素 (nFactor) 認証は、アクセスするために複数の身元証明を提供することをユーザーに要求することにより、アプリケーションのセキュリティを強化します。管理者は、クライアント証明書、LDAP、RADIUS、OAuth、SAML など、さまざまな認証要素を設定できます。これらの認証要素は、組織のニーズに応じて任意の順序で構成できます。

macOS/iOS 上の Citrix Secure Access クライアントは、以下の認証プロトコルをサポートしています:

- **nFactor** —nFactor プロトコルは、認証仮想サーバーがゲートウェイ上の VPN 仮想サーバーにバインドされている場合に使用されます。認証要素の順序は動的であるため、クライアントはアプリケーションのコンテキスト内でレンダリングされるブラウザインスタンスを使用して認証 GUI を表示します。
- Classic: クラシックプロトコルは、ゲートウェイ上の VPN 仮想サーバでクラシック認証ポリシーが設定されている場合に使用されるデフォルトのフォールバックプロトコルです。クラシックプロトコルは、NAC などの特定の認証方式で nFactor が失敗した場合のフォールバックプロトコルです。
- **Citrix ID** プラットフォーム—Citrix ID プラットフォームプロトコルは、CloudGateway または NetScaler Gateway サービスへの認証に使用され、Citrix Cloud への MDM 登録が必要です。

次の表は、各プロトコルでサポートされているさまざまな認証方法をまとめたものです。

認証方法	nFactor	クラシック	Citrix IdP
クライアント証明書	サポート対象	サポート対象	未サポート
LDAP	サポート対象	サポート対象	未サポート
ローカル	サポート対象	サポート対象	未サポート
RADIUS	サポート対象	未サポート	未サポート
SAML	サポート対象	未サポート	未サポート
OAuth	サポート対象	未サポート	未サポート
TACACS	サポート対象	未サポート	未サポート
WebAuth	サポート対象	未サポート	未サポート
交渉する	サポート対象	未サポート	未サポート
EPA	サポート対象	サポート対象	未サポート
NAC	未サポート	サポート対象	未サポート
StoreFront	未サポート	未サポート	未サポート
ADAL	未サポート	未サポート	未サポート
DS-AUTH	未サポート	未サポート	サポート対象

nFactor 構成

nFactor の設定の詳細については、nFactor 認証の設定を参照してください。

> 重要:
>
> macOS/iOS 上の Citrix Secure Access クライアントで nFactor プロトコルを使用するには、NetScaler Gateway のオンプレミスバージョンは 12.1.50.xx 以降が推奨されます。

制限事項

- NAC（ネットワークアクセス制御）などのモバイル固有の認証ポリシーでは、クライアントは NetScaler Gateway での認証の一部として署名付きデバイス識別子を送信する必要があります。署名付きデバイス識別子は、MDM 環境に登録されているモバイルデバイスを一意に識別する回転可能な秘密キーです。このキーは、MDM サーバーによって管理される VPN プロファイルに埋め込まれます。このキーを WebView コンテキストに挿入できない場合があります。MDM VPN プロファイルで NAC が有効になっている場合、macOS/iOS 上の Citrix Secure Access クライアントは自動的に従来の認証プロトコルにフォールバックします。
- macOS 用の Intune では NAC チェックを設定できません。iOS の場合とは異なり、Intune には macOS 用の NAC を有効にするオプションが用意されていないためです。

macOS/iOS 向け **Citrix Secure Access** に関する一般的な問題のトラブルシューティング

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。

DNS 解決の問題

- デバイスがスリープ状態になったり、長時間非アクティブになった場合、VPN が再開するまで約 30 ～60 秒かかることがあります。この間、ユーザーには一部の DNS 要求が失敗することがあります。DNS 要求は、短期間で自動的に解決されます。
  DNS クエリが解決されない場合、高度な認可ポリシーが DNS トラフィックをブロックしている可能性があります。この問題を解決するには、https://support.citrix.com/article/CTX232237を参照してください。
- ブラウザから DNS 解決を常にチェックしてください。端末からの`nslookup`コマンドを使用した DNS クエリは、正確ではない場合があります。`nslookup`コマンドを使用する必要がある場合は、クライアントの IP アドレスをコマンドに含める必要があります。例: `nslookup website_name 172.16.255.1.`

EPA の問題

- ゲートキーパーはアンチウィルスとみなされます。「任意のウイルス対策」（MAC-ANTIVIR_0_0）をチェックするスキャンがある場合、ユーザーが他のベンダーのウイルス対策ソフトウェアをインストールしていなくても、スキャンは常に成功します。

注:

- クライアントセキュリティログを有効にして、EPA のデバッグログを取得します。VPN パラメータ`clientsecurityLog`を ON に設定すると、クライアントセキュリティログを有効にできます。
- アップルの内蔵パッチ管理ソフトウェアは「ソフトウェアアップデート」です。端末の「App Store」アプリに相当します。「ソフトウェアアップデート」のバージョンは次のようになっている必要があります。`"MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"`
- NetScaler ADC 上の EPA ライブラリを常に最新の状態に保ちます。最新のライブラリは https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.htmlにあります

nFactor の問題

- Citrix Secure Access は、nFactor 認証の **Citrix SSO** 認証ウィンドウを開きます。これはブラウザに似ています。このページにエラーがある場合は、Web ブラウザで認証を試すことでクロス検証できます。
- nFactor が有効になっているときに転送ログオンが失敗した場合は、ポータルのテーマを「RfWebUI」に変更します。
- 「証明書チェーンに必要な証明書が含まれていないため、NetScaler Gateway への安全な接続を確立できません。管理者に連絡してください」または「ゲートウェイに到達できません」。その後、ゲートウェイサーバー証明書の有効期限が切れているか、サーバー証明書が SNI 対応でバインドされています。Citrix Secure Access は SNI をまだサポートしていません。SNI を有効にせずにサーバー証明書をバインドします。このエラーは、MDM VPN プロファイルで構成された証明書ピン留めと、NetScaler Gateway によって提示された証明書がピン留めされた証明書と一致しないことが原因である可能性もあります。
- ゲートウェイに接続しようとしたときに、**Citrix SSO** 認証ウィンドウが開くが空白の場合は、ECC 曲線（ALL）がデフォルトの暗号グループにバインドされているかどうかを確認します。ECC 曲線 (ALL) は、デフォルトの暗号グループにバインドする必要があります。

ネットワークアクセスコントロール **(NAC)** チェック

NAC 認証ポリシーは、クラシック認証でのみサポートされます。nFactor 認証の一部としてはサポートされていません。

よくある質問

April 1, 2024

> 重要:
>
> iOS 向け Citrix SSO は、Citrix Secure Access と呼ばれるようになりました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新しています。

このセクションでは、macOS/iOS 向け Citrix Secure Access に関するよくある質問について説明します。

macOS/iOS 向け **Citrix Secure Access** クライアントは **VPN** アプリとどう違うのですか**?**
macOS 向け Citrix Secure Access クライアントおよび iOS 向け Citrix Secure Access クライアント（以前は iOS 向け Citrix SSO と呼ばれていました）は、NetScaler 向けの次世代 SSL VPN クライアントです。このアプリは Apple のネットワーク拡張フレームワークを使用して、iOS および macOS デバイスで VPN 接続を作成および管理します。Citrix VPN は、現在廃止されている Apple のプライベート VPN API を使用する従来の VPN クライアントです。Citrix VPN のサポートはアプリストアではご利用いただけなくなりました。

NE って何ですか
Apple のネットワーク拡張 (NE) フレームワークは、iOS と macOS のコアネットワーク機能をカスタマイズおよび拡張するために使用できる API を含む最新のライブラリです。SSL VPN
をサポートするネットワーク拡張は、iOS 9 以降と macOS 10.11 以降を実行しているデバイスで利用できます。

macOS/iOS 向け **Citrix Secure Access** クライアントはどのバージョンの **NetScaler** と互換性がありますか**?**
macOS/iOS 向け Citrix Secure Access クライアントの VPN 機能は、NetScaler バージョン 10.5 以降でサポートされています。TOTP は、NetScaler ADC バージョン 12.0 以降で使用できます。NetScaler プッシュ通知はまだ公開されていません。このアプリには iOS 9 以降のバージョンと macOS 10.11 以降のバージョンが必要です。

MDM 以外のお客様の証明書ベースの認証はどのように機能しますか。
以前に VPN でクライアント証明書認証を実行するために電子メールまたはブラウザ経由で証明書を配布したことがあるお客様は、macOS/iOS 向け Citrix Secure Access クライアントを使用する際に、この変更に注意する必要があります。これは主に、MDM サーバーを使用してユーザー証明書を配布しない非 MDM 顧客に当てはまります。

ネットワークアクセスコントロール **(NAC)** とは何ですか。**iOS** 向け **Citrix Secure Access** と **NetScaler Gateway** を使用して **NAC** を構成する方法を教えてください。
Microsoft Intune および Citrix Endpoint Management（旧 XenMobile）MDM のお客様は、iOS 向け Citrix Secure Access のネットワークアクセス制御（NAC）機能を利用できます。NAC を使用すると、管理者は MDM サーバーで管理されるモバイルデバイスの認証レイヤーを追加することで、企業の内部ネットワークを保護できます。管理者は、iOS 向け Citrix Secure Access の認証時にデバイスのコンプライアンスチェックを実施できます。

iOS 向け Citrix Secure Access で NAC を使用するには、NetScaler Gateway と MDM サーバーの両方で NAC を有効にする必要があります。

- NetScaler ADC で NAC を有効にするには、「単一要素ログイン用の NetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックの構成」を参照してください。

- MDM ベンダーが Intune の場合は、「ネットワークアクセス制御 (NAC) と Intune の統合」を参照してください。
- MDM ベンダーが Citrix Endpoint Management（旧 XenMobile）の場合は、「ネットワークアクセス制御」を参照してください。

> 注:
>
> サポートされている macOS/iOS 向け Citrix Secure Access クライアントの最小バージョンは 1.1.6 以上です。

Android 向け Citrix Secure Access

April 1, 2024

Android 向け Citrix Secure Access（旧 Citrix SSO）は、NetScaler Gateway が提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションを提供します。ビジネスクリティカルなアプリケーション、仮想デスクトップ、企業データにいつでもどこからでも安全にアクセスできるようになりました。

> 重要:
>
> - Android 向け Citrix SSO は、現在 Citrix Secure Access と呼ばれています。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。
> - Android 向け Citrix セキュアアクセスクライアントは、ChromeOS 上に構築された Android サブシステム内で動作します。Play ストアから Android アプリとしてインストールすれば ChromeOS で動作し、Android サブシステム内の任意のアプリケーションをトンネリングできます。

リリースノート

April 1, 2024

> 重要:
>
> - Android 向け Citrix SSO の名前が Citrix Secure Access に変更されました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。この移行期間中に、ドキュメントで Citrix SSO のリファレンスが使用されていることに気付くかもしれません。
> - FQDN ベースの分割トンネリングと nFactor 認証のサポートは、現在プレビュー中です。
> - Citrix Secure Access は、2020 年 6 月以降の Android 6.x 以前のバージョンではサポートされません。

Citrix Secure Access リリースノートには、サービスリリースに含まれる新機能、既存機能の強化、修正された問題、既知の問題が記載されています。リリースノートには、次のセクションの 1 つまたは複数が含まれます:

新機能: 現在のリリースで利用できる新機能と拡張機能。

修正された問題: 現在のリリースで修正された問題。

既知の問題: 現在のリリースに存在する問題とその回避策 (該当する場合)。

V23.12.2 (2023 年 12 月 15 日)

> 注:
>
> Citrix Secure Access for Android バージョン 23.12.2 には CSACLIENTS-8799 の修正が含まれており、バージョン 23.12.1 に置き換えられています。

[CSACLIENTS-8799]

新機能

- **Android** 向け **Citrix SSO** が **Citrix Secure Access** に名称変更されました

  Android 向け Citrix SSO は、現在 Citrix Secure Access と呼ばれています。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。

  [CSACLIENTS-6337]

- **Android 13** 以降のデバイスで通知を受信またはブロックする

  Android 13 デバイスに Citrix Secure Access クライアントをインストールまたは再インストールすると、エンドユーザーは Citrix Secure Access クライアントからの通知を受信する権限を与えるように求められるようになりました。エンドユーザーが許可を拒否した場合、そのエンドユーザーは Android デバイス上の Citrix Secure Access クライアントから VPN ステータスまたはプッシュ通知を受信しなくなります。MDM 管理者は、ソリューション内の Citrix Secure Access（パッケージ ID: `com.citrix.CitrixVPN`）に通知権限を付与することをお勧めします。

  エンドユーザーは、Android デバイスで［設定］**>**［通知］に移動して、Citrix Secure Access クライアントの通知権限を
  変更できます。詳しくは、「Android デバイスから Citrix Secure Access を使用する方法」を参照してください。

  [CSACLIENTS-8252]

- 常時接続 **VPN** モードでの転送ログオンのサポート

  Android 向け Citrix Secure Access は、常時接続 VPN モードでのログオン転送機能をサポートするようになりました。転送ログオンの構成方法の詳細については、「転送ログオンの構成」ページを参照してください。

  [CSACLIENTS-8305]

解決された問題

ユーザーが Android 13 以降のデバイスで時間ベースの OTP（TOTP）トークンをコピーすると、Citrix Secure Access がクラッシュします。

[CSACLIENTS-8799]

V23.10.2 (2023 年 12 月 19 日)

新機能

> メモ:
>
> - Android 用 Citrix SSO バージョン 23.10.2 には CSACLIENTS-8314 の修正が含まれており、バージョン 23.10.1 に置き換えられています。
> - Android 用 Citrix SSO 23.10.1 は Android 14 で動作します。

- **VPN** 接続障害後の **NetScaler Gateway** による再認証-プレビュー

  Android 向け Citrix SSO は、VPN 接続が失われたときに NetScaler Gateway による再認証を求めるメッセージを表示するようになりました。Citrix SSO UI と Android デバイスの通知パネルに、NetScaler Gateway への接続が失われたこと、接続を再開するには再認証が必要であることが通知されます。この機能はプレビュー段階です。

  詳しくは、「VPN 接続障害後の NetScaler Gateway への再接続」を参照してください。

解決された問題

特定の常時接続 VPN シナリオで VPN サービスを再起動すると、Citrix SSO が断続的にクラッシュします。

[CSACLIENTS-8314]

V23.8.1 (2023 年 8 月 31 日)

新機能

- 常時接続 **VPN** の自動再起動

  Citrix SSO アプリは、許可リストまたは禁止リストに含まれるアプリが仕事用プロファイルまたはデバイスプロファイルにインストールされている場合、Always On VPN を自動的に再起動します。このアプリからのトラフィックは、仕事用プロファイルを再起動したりデバイスを再起動したりすることなく、VPN 接続を介して自動的にトンネリングされます。Always On VPN の自動再起動を有効にするには、エンドユーザーが Citrix SSO アプリに「すべてのパッケージを照会 」の許可を与える必要があります。詳細については、「Always On VPN の自動再起動」を参照してください。

[CSACLIENTS-6158]

- マネージド **VPN** プロファイルでデバッグログを有効にする

  MDM 管理者は、EndEndpoint Management コンソールのマネージド VPN プロファイルでカスタムパラメータとしてデバッグログを有効にできるようになりました。デバッグログを有効にするには、`EnableDebugLogging`の値を True に設定する必要があります。マネージド VPN 設定のいずれかでデバッグロギングが有効になっている場合、デバッグロギング機能は設定の解析時に有効になります。詳細については、「Intune 設定のカスタムパラメータ」を参照してください。

  [CSACLIENTS-3746]

解決された問題

- Citrix SSO アプリがトラフィックを一部のリソースにトンネリングできない場合があります。この問題は、分割トンネリングがオフに設定されていて、一部の到達不能なドメインまたは IP アドレスがブラックホールされている場合に発生します。

  [NSHELP-35555]

V22.11.1 (2022 年 11 月 30 日)

新機能

- **Citrix Secure Access** が **Android 12.1**（**API** レベル **32**）を対象とするように更新されました

  Citrix Secure Access は、Android 12.1（API レベル 32）を対象とするように更新されました。Per-App VPN の場合、VPN トンネルのセットアップ後に Per-App VPN パッケージリスト内のパッケージの 1 つがインストールされると、VPN サービスが自動的に再起動しないことがあります。これは Android 11 で導入されたアプリの可視性制限によるものです。詳しくは、https://developer.android.com/training/package-visibilityを参照してください。

  [CGOP-21409]

V22.10.1 (2022 年 10 月 21 日)

新機能

- アプリのバージョン番号の表示が yy.mm.point-release という形式に更新されます。YY は 2 桁の年、MM は 2 桁の月、ポイントリリースは 1 か月以内のリリース番号にもよりますが、ポイントリリースは 1+ になります。
- EU 地域からの Google Analytics/Crashlytics データ収集は Android クライアントでは無効になっています。

解決された問題

- [接続の追加] 画面と [接続の編集] 画面で無効な入力に対して表示されるエラーメッセージはローカライズされません。

  [CGOP-22060]

V2.5.3 (2022 年 5 月 5 日)

新機能

- Citrix SSO が Android 11 ターゲット SDK（API 30）に更新されました

  Citrix SSO アプリは、Android 11 ターゲット SDK（API 30）にアップデートされました。この変更には、Microsoft Intune NAC v2 API が NetScaler Gateway によってデバイスのコンプライアンスチェックに使用される必要があります。詳細については、ナレッジベースの記事を参照してください https://support.citrix.com/article/CTX331615。

  [CGOP-19774]

解決された問題

- Citrix SSO は、ネットワーク変更後のホスト名解決に代替 DNS サーバーを使用しない場合があります。

  [NSHELP-29378]

V2.5.2 (2021 年 10 月 21 日)

解決された問題

- NAC チェックで非準拠エラーを処理すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-19198]

V2.5.1 (2021 年 8 月 12 日)

解決された問題

- CNAME チェーンが 6 ホップを超えると、Citrix SSO アプリがホストの解決に失敗します。

  [CGOP-18475]

- Citrix SSO は、NetScaler Gateway で NAC チェックのみの認証が必要な場合に認証プロンプトを表示します。

  [CGOP-18348]

- 異常に大きい ICMP パケットの処理中に Citrix SSO がクラッシュすることがあります。

  [CGOP-18286]

- 一部の Android 8.0 デバイスで VPN プロファイルを追加すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-17607]

- Always On 用に構成された VPN を再起動すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-17580]

- nFactor 認証フローで SSL エラーを処理すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-17577]

V2.5.0 (2021 年 6 月 8 日)

新機能

- **FQDN** ベースの分割トンネリングのサポート

  Android 向け Citrix SSO は、FQDN ベースの分割トンネリングをサポートするようになりました。

  [CGOP-12079]

解決された問題

- Citrix SSO プレビュービルド 2.5.0 は、NetScaler Gateway バージョン 12.1 以前への接続に失敗します(110)。

  [CGOP-17735]

- SSO アプリの再起動後は、「DisableUserProfiles」設定は適用されません。

  [CGOP-17454]

V2.4.16 (31-Mar-2021)

解決された問題

- 一部のデバイスでセーフブラウジングが有効になっていないと、nFactor 認証が中止されます。

  [CGOP-17514]

V2.4.15 (17-Mar-2021)

解決された問題

- NetScaler Gateway アプライアンスでセッションタイムアウトが発生すると、Citrix SSO が Always On VPN を再接続しないことがあります。

  [CGOP-16800]

V2.4.14 (23-Feb-2021)

解決された問題

- 証明書のみの認証を使用した常時接続 VPN を nFactor 認証とともに使用する場合、Citrix SSO はユーザーの操作を必要とします。

  [CGOP-16805]

- VPN サービスの再起動または移行中に Citrix SSO がクラッシュすることがあります。

  [CGOP-16766]

V2.4.13 (04-Feb-2021)

解決された問題

- 場合によっては、Citrix SSO ログイン要求が NetScaler Gateway が応答する前にタイムアウトすることがあります。

  [CGOP-16759]

V2.4.12 (2021 年 1 月 15 日)

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.4.11 (08-Jan-2021)

- Citrix SSO が nFactor 認証でのみ使用される HTTP ヘッダー (X-Citrix-Gateway) を NetScaler Gateway に送信するため、クラシック認証は失敗します。

  [CGOP-16449]

V2.4.10 (09-Dec-2020)

解決された問題

- Android デバイスでは、クラシック認証が失敗することがあります。

  [CGOP-16219]

- クラシック認証を実行すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-16012]

- Citrix SSO アプリの向きは、デバイスを回転しても変わりません。

  [CGOP-639]

V2.4.9 (20-Nov-2020)

解決された問題

- ユーザーがデバイスで TOTP トークンの値をタップすると、Citrix SSO アプリがクラッシュします。

  [CGOP-15886]

V2.4.8 (04-Nov-2020)

解決された問題

- ゲートウェイのセッションタイムアウト後に VPN を切断すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-15592]

V2.4.7 (12-Oct-2020)

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.4.6 (28-Sep-2020)

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.4.5 (16-Sep-2020)

新機能

- 新しい NetScaler ロゴが導入されました。

  [CGOP-15327]

V2.4.4 (10-Sep-2020)

解決された問題

- VPN セッションを再接続すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-15215]

V2.4.3

既知の問題

- Android デバイスがリソースに制約されている場合、Citrix SSO は NetScaler Gateway への VPN セッションを確立できません。

  [NSHELP-24647]

V2.4.2

解決された問題

- 以前に保存した破損したトークンデータを読み込むと、Citrix SSO アプリがクラッシュします。今回の修正により、トークンリスト内の破損したトークンについて、トークンの値が「トークンデータが破損しました」と表示されます。破損したトークンを削除し、もう一度追加します。

  [CGOP-14546]

V2.4.1

解決された問題

- Citrix SSO アプリは、2020 年 6 月以降の Android 6.x 以前のバージョンではサポートされません。

  [CGOP-13853]

V2.3.19

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.3.18

新機能

- Android 10 デバイス用の Android Citrix SSO アプリでプロキシ構成がサポートされるようになりました。

  [CGOP-12007]

V2.3.17

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.3.16

このリリースではさまざまな問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

V2.3.15

新機能

- Citrix SSO アプリは、管理対象 VPN プロファイルの NetScaler Gateway 証明書ピンニングをサポートするようになりました。

  [CGOP-12538]
- Android 10 用 Citrix SSO アプリは、システム設定から常時接続 VPN を検出するようになりました。

  [CGOP-12656]

解決された問題

- MDM VPN プロファイルのみが定義されている場合、VPN から切断すると Citrix SSO アプリがクラッシュします。

  [CGOP-13825]

V2.3.14

新機能

- Citrix SSO アプリは、ネイティブアプリのシングルサインオンのために、Citrix Workspace アプリの代わりにユーザー認証を実行できるようになりました。

  [CGOP-12083]

- VPN トンネルのセットアップ後にアプリごとの VPN パッケージリストにあるパッケージの 1 つがインストールされると、VPN サービスが再起動します。

  [CGOP-11262]

解決された問題

- Citrix SSO が最終 VPN セッション確立メッセージを正しく処理するようになりました。

  [CGOP-12488]

- NetScaler Gateway IP アドレスは一度だけ解決されるようになりました。以前は、NetScaler Gateway IP アドレスが複数回解決され、接続が失敗することがありました。

  [CGOP-12101]

既知の問題

- Always-On VPN のステータスは、アプリのユーザーインターフェイスで常に正しく更新されるとは限りません。

  [NSHELP-21709]

V2.3.13

解決された問題

- NetScaler Gateway IP アドレスは一度だけ解決されるようになりました。

  以前は、NetScaler Gateway IP アドレスが複数回解決され、接続が失敗することがありました。

  [CGOP-12101]

既知の問題

- Always-On VPN のステータスは、アプリのユーザーインターフェイスで常に正しく更新されるとは限りません。

  [NSHELP-21709]

V2.3.12

解決された問題

- VPN プロファイルを保存すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-12137]

V2.3.11

解決された問題

- VPN プロファイルを保存すると、Citrix SSO がクラッシュすることがあります。

  [CGOP-12137]

- 新しい VPN プロファイルまたは既存のプロファイルへの更新によって DisableUserProfile の値が変更された場合、disableUserProfile 設定はユーザーインターフェイスに正しく反映されません。

  [CGOP-11899]

- Android 向け Citrix SSO は、デバイス所有者（DO）モードで VPN プロファイルを処理しません。

  [CGOP-11981]

- IPv6 のみのローカル DNS サーバーがある場合、VPN 接続は確立されません。

  [CGOP-12053]

V2.3.10

解決された問題

- デバイスのアイドル時間が経過すると、VPN 接続が失われました。

  [CGOP-11381]

V2.3.8

新機能

- **Intune Android Enterprise** 環境で **Citrix SSO** アプリをセットアップする

  これで、Intune Android Enterprise 環境で Citrix SSO アプリをセットアップできるようになりました。詳しくは、「Intune Android Enterprise 環境で Citrix SSO アプリをセットアップする」を参照してください。

  [CGOP-635]

- **Android Enterprise** 経由の **VPN** プロファイルプロビジョニングのサポート

  Android Enterprise 経由の VPN プロファイルのプロビジョニングがサポートされるようになりました。

  [CGOP-631]

解決された問題

- すでに保存されているトークンを保存してから開こうとすると、トークン名に文字化けした文字が表示されます。

  [CGOP-11696]

- NetScaler Gateway で DNS 検索ドメインが構成されていない場合、Citrix SSO アプリは VPN セッションを確立できません。

  [CGOP-11259]

V2.3.6

新機能

- **Citrix SSO** の常時オンのサポート

  Citrix SSO の Always On 機能により、ユーザーは常にエンタープライズネットワークに接続できます。この永続的な VPN 接続は、VPN トンネルの自動確立によって実現されます。

  [CGOP-10015]

- **Athena** トークンの有効期限が切れてログアウトが発生すると、再ログインの通知が表示されます。

  次の条件が満たされると、ユーザーに Citrix Workspace への再ログインを求める通知が表示されます。

  - 常時接続機能は、Citrix Workspace のプロビジョニングされた VPN プロファイルで有効になっています
  - アテナ認証は SSO に使用されます。

  - Athena トークンの有効期限が切れたため、ユーザーは Citrix Workspace アプリからログアウトしています

[CGOP-10016]

- プッシュ通知サービスの登録は、**NetScaler Gateway** を使用して行われます。

  NetScaler Gateway アプライアンスを使用してプッシュ通知サービスに登録できるようになりました。以前は、クライアントデバイスで登録が行われていました。

  [CGOP-10542]

解決された問題

新しいトークンがスキャンされると、Citrix SSO がクラッシュすることがあります。たとえば、既存のトークンが削除され、別のトークンが同じトークン名でスキャンされると、Citrix SSO がクラッシュします。

[CGOP-10818]

V2.3.1

新機能

- 管理対象構成が更新され、ユーザー設定が増えます。

  マネージド構成が更新され、Android Enterprise 環境の「UntrustedServers をブロックする」、「default-ProfileName」、「DisableUserProfiles」の各設定が含まれるようになりました。

  [CGOP-10033]

- プッシュ通知サポートの強化

  「OTP」タイプのプッシュ通知用に NetScaler Gateway を構成すると、認証の続行を許可するためのユーザーの同意を要求するプッシュ通知に応答して、ユーザーが「許可」を選択した後、PIN/Fingerprint が要求されません。

  [CGOP-9843]

- **Firebase** アナリティクスのサポート

  基本的な Firebase Analytics のサポートが追加され、Citrix SSO アプリの使用状況に関する情報が提供されます。この拡張は、粗いジオロケーション、画面の使用状況、使用中の Android の異なるバージョンなどに適用されます。

  [CGOP-7523]

- **Android** 管理対象設定ベースの **VPN** プロファイル設定のサポート

  Citrix SSO アプリは、Citrix Endpoint Management などの EMM/UEM ベンダーを使用して、Android Enterprise 環境で構成できます。CEM の Android Enterprise 管理構成ウィザードを使用して、管理対象 VPN 構成を Citrix SSO アプリに展開できます。管理対象構成を使用して Citrix SSO アプリを構成する方法については、「VPN デバイスポリシー」を参照してください。

V2.2.9

新機能

- プッシュ通知のサポート

  NetScaler Gateway は、登録されたモバイルデバイスにプッシュ通知を送信し、簡素化された 2 要素認証エクスペリエンスを実現します。

  [CGOP-9592]

解決された問題

- URL 以外の文字は、[接続の追加] 画面の [サーバー] フィールドで許可されます。

  [CGOP-588]

MDM 環境での Citrix Secure Access のセットアップ

April 1, 2024

> 重要:
>
> Android 向け Citrix SSO は、現在 Citrix Secure Access と呼ばれています。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。

MDM 環境で Citrix Secure Access をセットアップするには、「Android 向け Citrix Secure Access プロトコルの構成」を参照してください。

> メモ:
>
> - MDM 以外の環境では、ユーザーは VPN プロファイルを手動で作成します。
> - Citrix Secure Access 用の Android Enterprise 管理構成を作成することもできます。詳しくは、Android Enterprise 用の VPN プロファイルの設定を参照してください。
> - Citrix Secure Access 23.12.1 以降を使用している Android 13 以降のユーザーの場合、MDM 管理者

> はソリューション内の Citrix Secure Access（パッケージ ID: `com.citrix.CitrixVPN`）に通知権限を付与することをお勧めします。

Intune Android Enterprise 環境で Citrix Secure Access をセットアップする

April 1, 2024

> 重要:
>
> Android 向け Citrix SSO は、現在 Citrix Secure Access と呼ばれています。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。

このトピックでは、Microsoft Intune による Citrix Secure Access の展開と構成について詳しく説明します。このドキュメントでは、Intune がすでに Android Enterprise サポート用に設定されており、デバイスの登録がすでに行われていることを前提としています。

前提条件

- Intune は Android Enterprise サポート用に設定されています
- デバイス登録が完了しました

Intune Android Enterprise 環境で Citrix Secure Access をセットアップするには

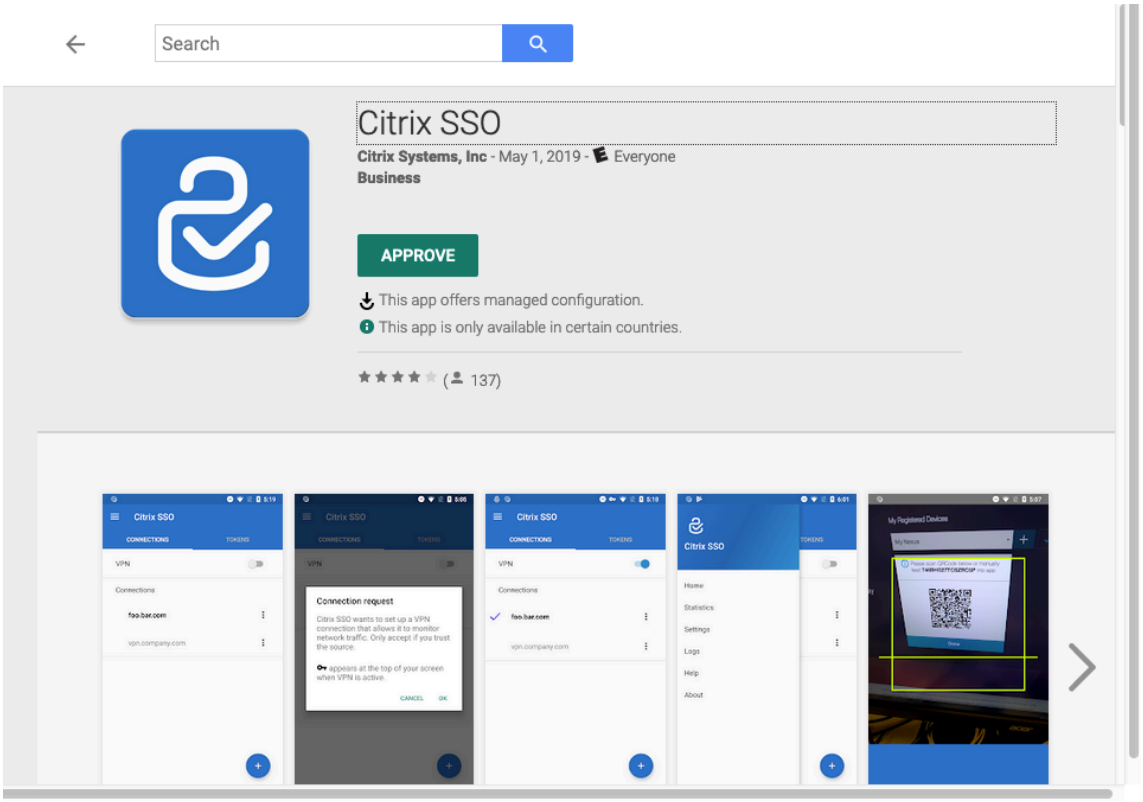
- Citrix Secure Access を管理対象アプリとして追加
- Citrix Secure Access の管理対象アプリケーションポリシーの設定

Citrix Secure Access を管理対象アプリとして追加

1. Azure Portal にログインします。
2. 左側のナビゲーションブレードの **Intune** をクリックします。
3. Microsoft Intune ブレードで [クライアントアプリ] をクリックし、[クライアントアプリ] ブレードの [アプリ] をクリックします。
4. 右上のメニューオプションで [**+** リンクを追加] をクリックします。[アプリ構成の追加] ブレードが表示されます。
5. アプリの種類として [管理対象 **Google Play**] を選択します。

   これにより、Android Enterprise を設定している場合、Google Play の検索を管理してブレードを承認するが追加されます。

6.「Citrix Secure Access」を検索し、アプリのリストから選択します。



注：Citrix Secure Access がリストに表示されない場合は、そのアプリがお住まいの国では利用できないことを意味します。

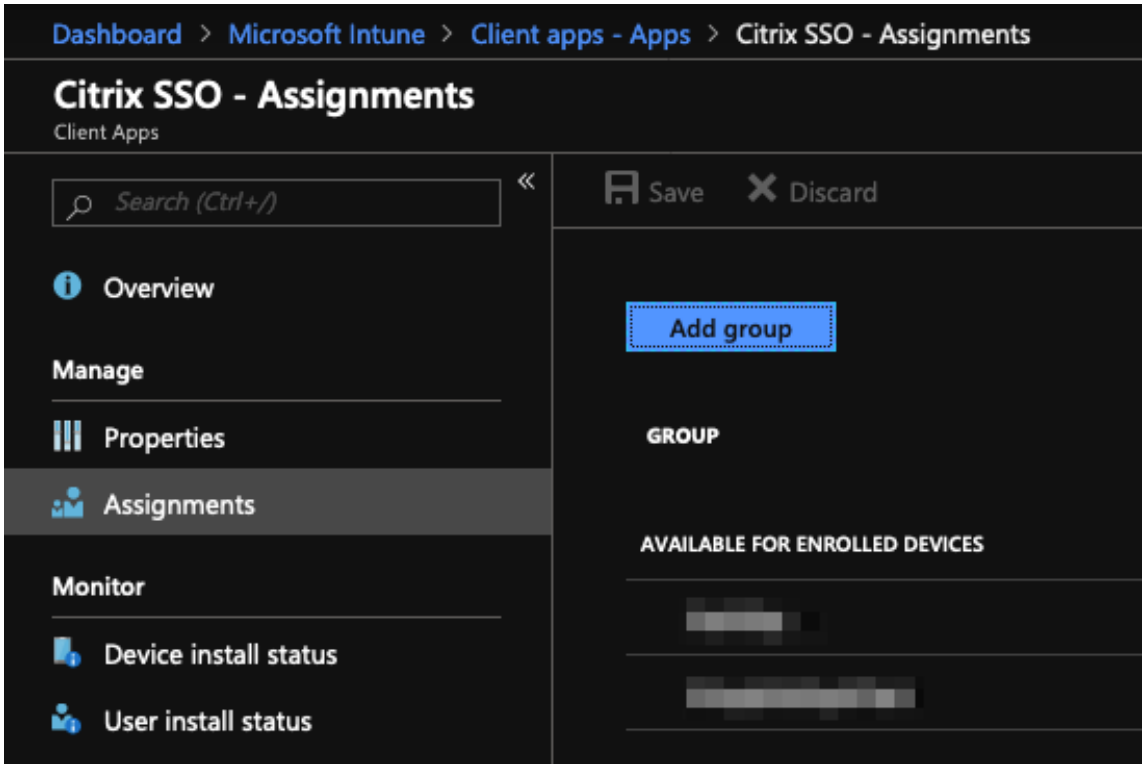
7.「承認」をクリックして、管理対象 Google Play ストアを通じて Citrix Secure Access を導入することを承認します。

Citrix Secure Access に必要な権限が一覧表示されます。

8. [**APPROVE**] をクリックして、アプリの展開を承認します。
9. [同期] をクリックして、この選択を Intune と同期します。

Citrix Secure Access がクライアントアプリリストに追加されました。多くのアプリが追加されている場合は、Citrix Secure Access を検索しなければならない場合があります。

10. **Citrix Secure Access** アプリをクリックして、アプリの詳細ブレードを開きます。
11. 詳細ブレードの [割り当て] をクリックします。**Citrix Secure Access-**アサインメントブレードが表示されます。



12. ［グループの追加］をクリックして、Citrix Secure Access のインストール権限を付与するユーザーグループを割り当てて、［保存］をクリックします。
13. Citrix Secure Access の詳細ブレードを閉じます。

Citrix Secure Access が追加され、ユーザーへの展開が可能になりました。

Citrix Secure Access の管理対象アプリケーションポリシーの設定

Citrix Secure Access を追加したら、VPN プロファイルをデバイス上の Citrix Secure Access に展開できるように、Citrix Secure Access の管理対象構成ポリシーを作成する必要があります。

1. Azure Portal で **Intune** ブレードを開きます。
2. Intune ブレードから [クライアントアプリケーション] ブレードを開きます。
3. [クライアントアプリケーション] ブレードから [アプリ構成ポリシー] 項目を選択し、[追加] をクリックして [構成ポリシーの追加] ブレードを開きます。
4. ポリシーの名前を入力し、その説明を追加します。
5. [デバイス登録の種類] で、[管理対象デバイス] を選択します。
6. [プラットフォーム] で、[**Android**] を選択します。

   これにより、関連付けられたアプリに別の構成オプションが追加されます。

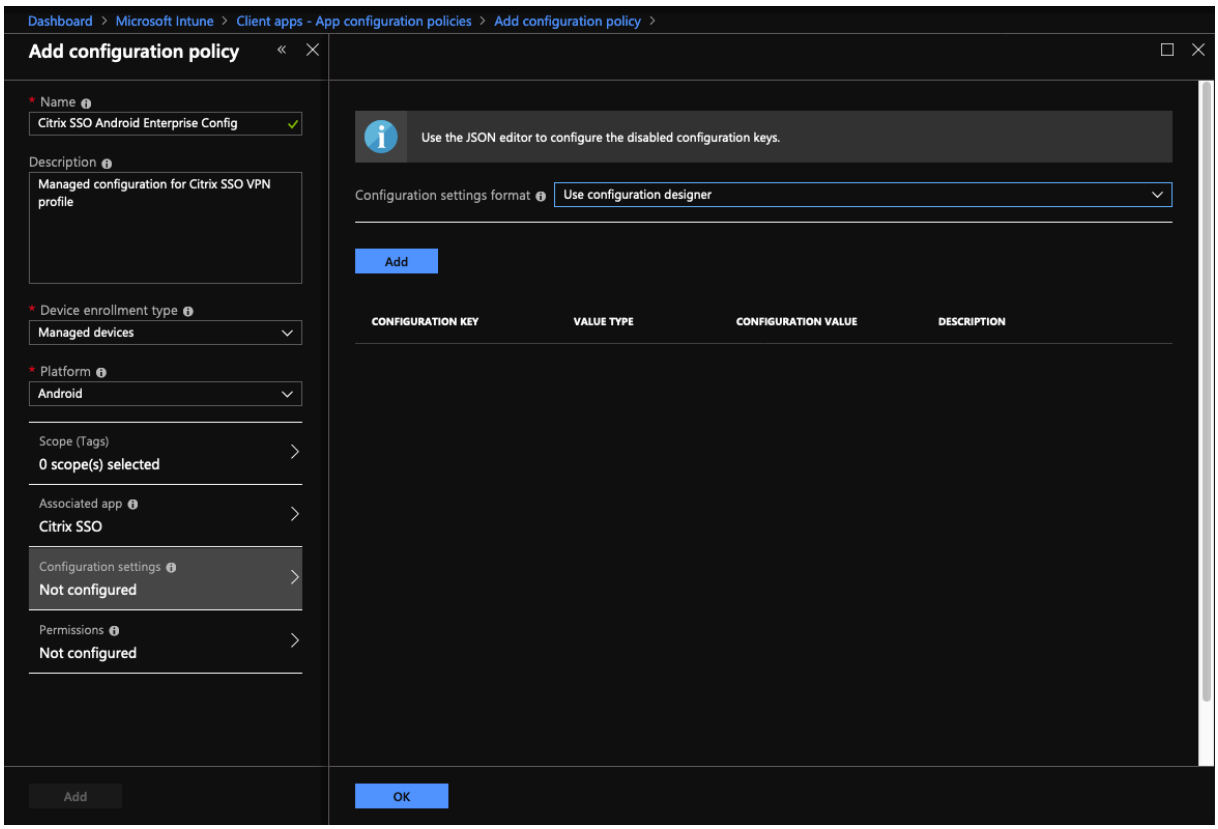
7. 「関連アプリ」をクリックし、「**Citrix Secure Access** アプリ」を選択します。

   アプリが多いなら検索しなきゃいけないかも。

8. [**OK**] をクリックします。構成設定オプションが [構成ポリシーの追加] ブレードに追加されます。
9. [構成設定] をクリックします。

   Citrix Secure Access を構成するためのブレードが表示されます。

10. [構成設定] で、[構成デザイナーを使用する] または [**JSON** データを入力する] を選択して、Citrix Secure Access を構成します。



> 注:
>
> 単純な VPN 構成の場合は、構成デザイナーを使用することをお勧めします。

構成デザイナーを使用した **VPN** 構成

1. [構成設定] で、[構成デザイナーを使用する] を選択し、[追加] をクリックします。

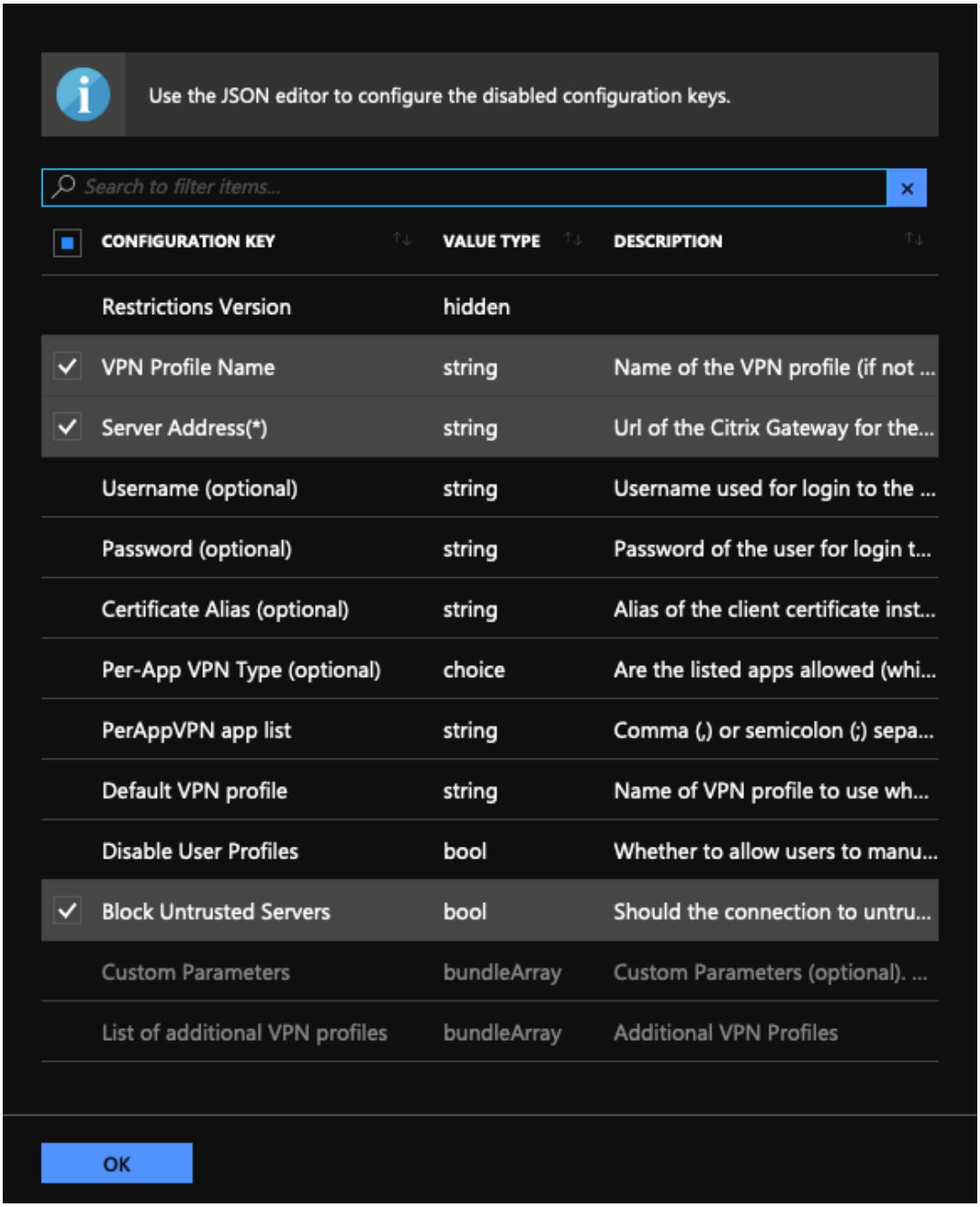
   Citrix Secure Access でサポートされているさまざまなプロパティを構成するためのキー値入力画面が表示されます。少なくとも、サーバーアドレスと **VPN** プロファイル名のプロパティを設定する必要があります。[**DESCRIPTION**] セクションにマウスポインターを合わせると、各プロパティの詳細が表示されます。

2. たとえば、[**VPN** プロファイル名] および [サーバーアドレス（*****）] プロパティを選択し、[**OK**] をクリックします。

これにより、プロパティが構成デザイナーに追加されます。次のプロパティを設定できます。

- **VPN** プロファイル名。VPN プロファイルの名前を入力します。複数の VPN プロファイルを作成している場合は、それぞれに一意の名前を使用します。名前を指定しない場合、[Server Address] フィールドに入力したアドレスが VPN プロファイル名として使用されます。
- サーバーアドレス **(*)**。NetScaler Gateway のベース完全修飾ドメイン名を入力します。NetScaler Gateway のポートが 443 ではない場合は、ポートも入力します。URL 形式を使用します。例: `https://vpn.mycompany.com:8443`。
- ユーザー名（オプション）。エンドユーザーが NetScaler Gateway への認証に使用するユーザー名を入力します。ゲートウェイがそれを使用するように設定されている場合は、このフィールドに Intune 設定値トークンを使用できます（設定値トークンを参照）。ユーザー名を指定しない場合、ユーザーは NetScaler Gateway に接続するときにユーザー名の入力を求められます。
- パスワード（オプション）。エンドユーザーが NetScaler Gateway への認証に使用するパスワードを入力します。パスワードを指定しない場合、ユーザーは NetScaler Gateway に接続するときにパスワードの入力を求められます。
- 証明書エイリアス（オプション）。クライアント証明書認証に使用する証明書エイリアスを Android KeyStore に提供します。証明書ベースの認証を使用している場合、この証明書はユーザーに対して事前に選択されています。
- ゲートウェイ証明書ピン **(**オプション**)**。NetScaler Gateway で使用される証明書ピンを記述する JSON オブジェクト。値の例: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`。詳しくは、「Android Citrix Secure Access による NetScaler Gateway 証明書ピン留め」を参照してください。
- **Per-App VPN** の種類（オプション）。アプリごとの VPN を使用してこの VPN を使用するアプリを制限している場合は、この設定を構成できます。
  - [許可] を選択すると、PerAppVPN アプリ一覧に表示されるアプリパッケージ名のネットワークトラフィックが VPN 経由でルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN 外でルーティングされます。
  - [許可しない] を選択した場合、[Per-App VPN アプリ一覧] に含まれるアプリパッケージ名のネットワークトラフィックが VPN 外でルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN を介してルーティングされます。デフォルトは [許可] です。
- **perAppVPN** アプリリスト。[Per-App VPN の種類] の値に応じ、トラフィックが VPN で許可されるか、または許可されないアプリの一覧。アプリパッケージ名がカンマまたはセミコロンで区切って一覧にされます。アプリパッケージ名は大文字と小文字が区別され、この一覧でも Google Play ストアに表示されているのと同じように表示される必要があります。この一覧はオプションです。デバイス全体の VPN をプロビジョニングする場合は、この一覧を空のままにします。

- デフォルトの **VPN** プロファイル。常時接続 VPN が Citrix Secure Access 用に構成されている場合に使用される VPN プロファイル名。このフィールドが空の場合、接続にはメインプロファイルが使用されます。プロファイルが 1 つだけ設定されている場合、そのプロファイルはデフォルトの VPN プロファイルとしてマークされます。



注:

- Citrix Secure Access を Intune で常時稼働 VPN アプリとして作成するには、VPN プロバイダーをカスタムおよび`com.citrix.CitrixVPN`をアプリパッケージ名として使用します。

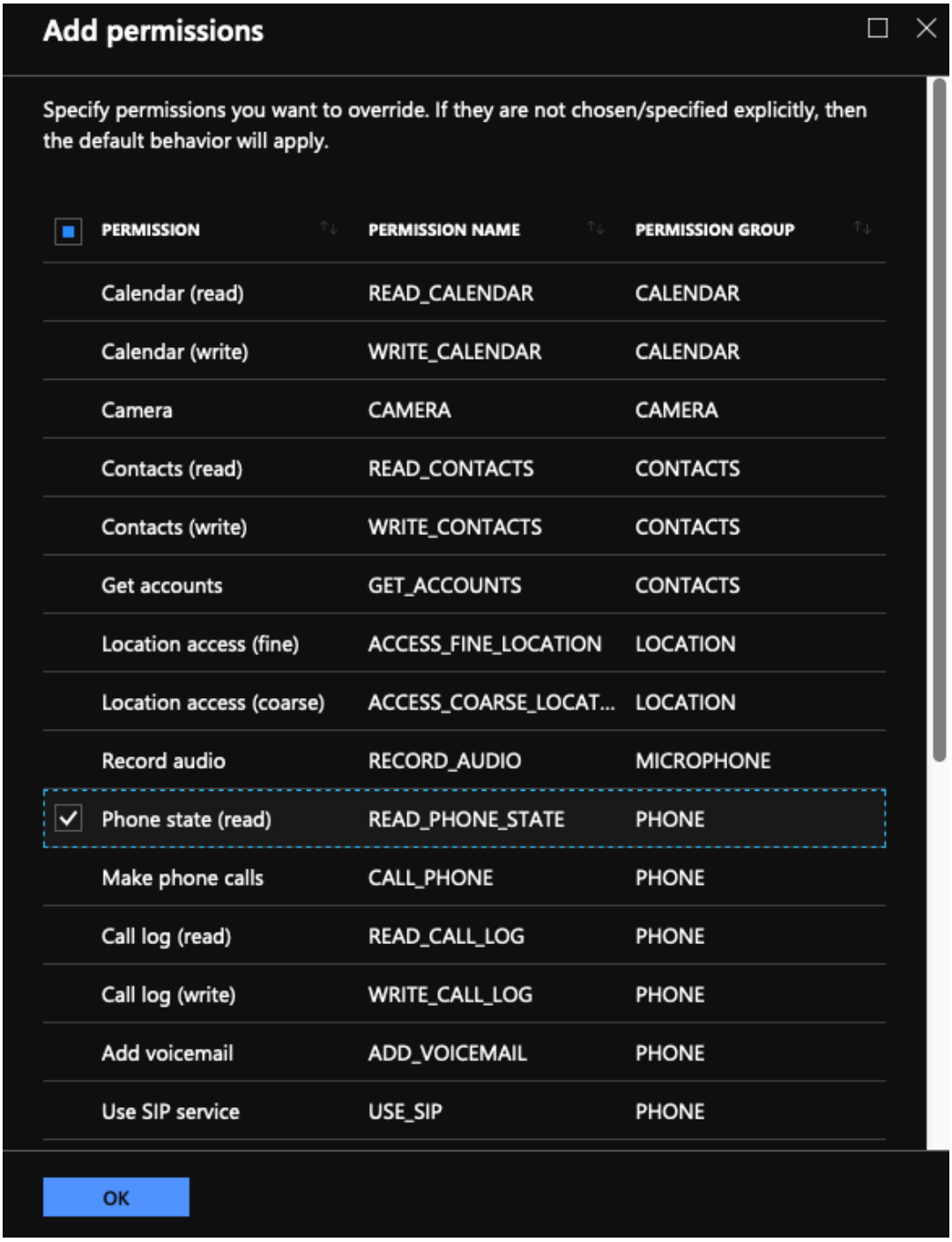
> - Citrix Secure Access による Always On VPN では、証明書ベースのクライアント認証のみがサポートされています。
> - Citrix Secure Access が意図したとおりに動作するには、管理者が NetScaler Gateway の SSL プロファイルまたは **SSL** プロパティで［クライアント認証］を選択し、［クライアント証明書］を［必須］に設定する必要があります。

- ユーザープロファイルの無効化
  - この値を true に設定すると、ユーザーはデバイスに新しい VPN プロファイルを追加できません。
  - この値を false に設定すると、ユーザーは自分のデバイスに独自の VPN を追加できます。

  デフォルト値は false です。
- 信頼できないサーバーをブロックする
  - NetScaler Gateway で自己署名証明書を使用する場合、または NetScaler Gateway 証明書を発行する CA のルート証明書がシステム CA リストにない場合は、この値を false に設定します。
  - Android オペレーティングシステムが NetScaler Gateway 証明書を検証できるようにするには、この値を true に設定します。検証に失敗した場合、接続は許可されません。

  デフォルト値は、true です。

3. [サーバーアドレス **(*)**] プロパティに、VPN ゲートウェイのベース URL（`https://vpn.mycompany.com`など）を入力します。
4.「**VPN** プロファイル名」には、Citrix Secure Access クライアントのメイン画面でエンドユーザーに表示される名前（「マイコーポレート VPN」など）を入力します。
5. NetScaler Gateway 展開環境には、必要に応じて他のプロパティを追加および構成できます。設定が完了したら、「**OK**」をクリックします。
6.「権限」セクションをクリックします。Citrix Secure Access に必要な次の権限を付与できます：
   - Intune NAC チェックを使用している場合、Citrix Secure Access では、電話状態（読み取り）権限を付与する必要があります。[追加] ボタンをクリックして、[権限] ブレードを開きます。現在、Intune には、すべてのアプリで使用できるアクセス許可の重要なリストが表示されます。
   - Intune NAC チェックを使用している場合は、電話の状態（読み取り）権限を選択し、**OK** をクリックします。これにより、アプリの権限のリストに追加されます。Intune NAC チェックが機能するように [プロンプト] または [自動許可] のいずれかを選択し、[**OK**] をクリックします。



- Citrix Secure Access に通知権限を自動付与することをお勧めします。

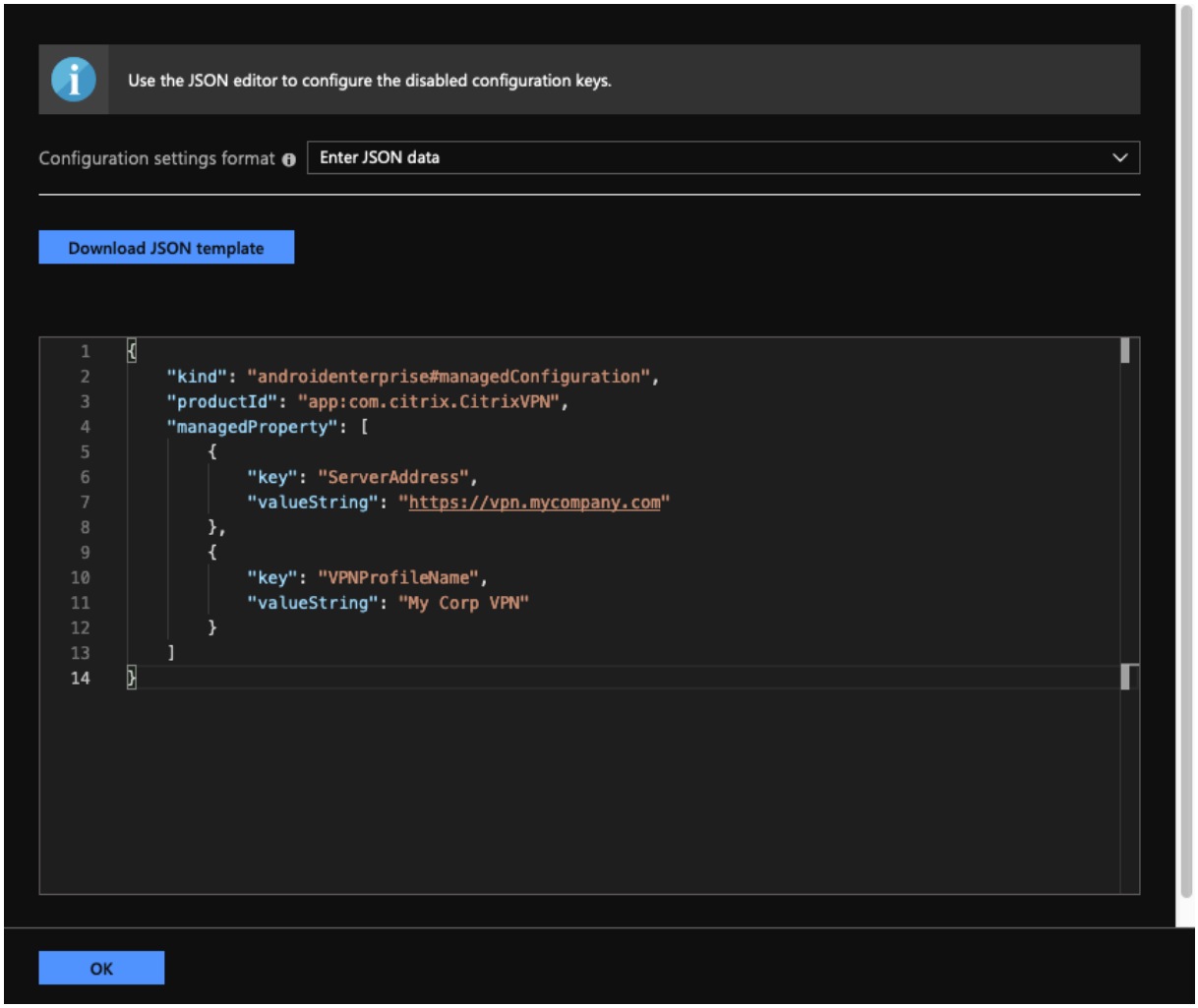
> 注:
>
> Citrix Secure Access 23.12.1 以降を使用している Android 13 以降のユーザーの場合、MDM 管理者はソリューション内の Citrix Secure Access（パッケージ ID: `com.citrix.CitrixVPN`）に通知権限を付与することをお勧めします。

7. アプリ構成ポリシーブレードの下部にある「追加」をクリックして、Citrix Secure Access の管理対象構成を保存します。
8. [アプリケーション構成ポリシー] ブレードの [割り当て] をクリックして、[割り当て] ブレードを開きます。
9. この Citrix Secure Access 構成を配信して適用したいユーザーグループを選択します。

JSON データを入力することによる **VPN** の設定

1. ［構成設定］で、［**JSON** データを入力して Citrix Secure Access を構成する］を選択します。
2. ［JSON テンプレートのダウンロード］ボタンを使用して、Citrix Secure Access のより詳細で複雑な構成を提供できるテンプレートをダウンロードします。このテンプレートは、Citrix Secure Access が認識できるすべてのプロパティを構成するための JSON キーと値のペアのセットです。

   構成可能なすべてのプロパティの一覧については、「Citrix Secure Access アプリで VPN プロファイルを構成するために使用できるプロパティ」を参照してください。
3. JSON 設定ファイルを作成したら、その内容をコピーして編集領域に貼り付けます。たとえば、構成デザイナーオプションを使用して以前に作成された基本設定の JSON テンプレートを次に示します。



これで、Microsoft Intune Android Enterprise 環境で Citrix Secure Access の VPN プロファイルを構成および展開する手順は完了です。

> 重要:
>
> クライアント証明書ベースの認証に使用される証明書は、Intune SCEP プロファイルを使用して展開されます。この証明書のエイリアスは、Citrix Secure Access の管理対象構成の「証明書エイリアス」プロパティで構成する必要があります。

Citrix Secure Access で **VPN** プロファイルを構成するために使用できるプロパティ

構成キー	JSON フィールド名	値のタイプ	説明
VPN プロファイル名	VPN プロファイル名	テキスト	VPN プロファイルの名前（デフォルトはサーバアドレスに設定されていない場合）。

構成キー	JSON フィールド名	値のタイプ	説明
サーバーアドレス (*)	サーバーアドレス	URL	接続の NetScaler Gateway のベース URL (`https://host[:port]`)。これは必須フィールドです。
`Username`（オプション）	ユーザー名	テキスト	NetScaler Gateway での認証に使用されるユーザー名（オプション）。
パスワード（オプション）	パスワード	テキスト	NetScaler Gateway での認証に使用されるユーザーのパスワード（オプション）。
証明書エイリアス（オプション）	ClientCertAlias	テキスト	証明書ベースのクライアント認証に使用するために Android 資格情報ストアにインストールされているクライアント証明書のエイリアス（オプション）。NetScaler Gateway で証明書ベースの認証を使用する場合、証明書エイリアスは必須フィールドです。
ゲートウェイ証明書ピン (オプション)	ServerCertificatePins	JSON テキスト	NetScaler Gateway に使用される証明書 PIN を記述する埋め込み JSON オブジェクト。値の例: `{ "hash-alg": "sha256", "pinset": ["AAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBB="] }`。JSON コンフィギュレーターを使用するときは、この埋め込まれた JSON データを必ずエスケープしてください。

構成キー	JSON フィールド名	値のタイプ	説明
Per-App VPN の種類（オプション）	PerAppVPN_Allow_Disallow_Setting	列挙型（許可、不許可）	リストにあるアプリで VPN トンネルを使用することを許可（許可リスト）または拒否（禁止リスト）していますか。［許可］に設定すると、リストされているアプリ（perAppVPN アプリリストプロパティ内）のみが VPN 経由のトンネリングを許可されます。［許可しない］に設定すると、一覧表示されているアプリを除くすべてのアプリが VPN 経由のトンネリングを許可されます。アプリがリストに表示されない場合、すべてのアプリが VPN 経由でトンネリングできます。
perAppVPN アプリリスト	PERAppName_appNames	テキスト	Per-App VPN のアプリパッケージ名をカンマ (,) またはセミコロン (;) で区切ったリスト。パッケージ名は、Google Play ストアのアプリ一覧ページの URL に表示されているものと同じである必要があります。パッケージ名では大文字と小文字が区別されます。
デフォルトの VPN プロファイル	DefaultProfileName	テキスト	システムが VPN サービスを開始するときに使用する VPN プロファイルの名前。この設定は、デバイスで VPN 常時接続が構成されている場合に使用する VPN プロファイルを識別するために使用されます。

構成キー	JSON フィールド名	値のタイプ	説明
ユーザープロファイルの無効化	DisableUserProfiles	ブーリアン型	エンドユーザーが手動で VPN プロファイルを作成することを許可または禁止するプロパティ。ユーザが VPN プロファイルを作成できないようにするには、この値を **true** に設定します。デフォルト値は **false** です。
信頼できないサーバーをブロックする	BlockUntrustedServers	ブーリアン型	信頼できないゲートウェイへの接続をブロックするかどうかを決定するプロパティ（たとえば、自己署名証明書を使用する場合や、発行した CA が Android オペレーティングシステムによって信頼されていない場合など）。デフォルト値は true（信頼できないゲートウェイへの接続をブロック）です。
カスタムパラメーター（オプション）	CustomParameters	一覧	Citrix Secure Access でサポートされているカスタムパラメータ（オプション）のリスト。詳細については、「カスタムパラメータ」を参照 してください。使用可能なオプションについては、**NetScaler Gateway** 製品ドキュメントを確認してください。

構成キー	JSON フィールド名	値のタイプ	説明
その他の VPN プロファイルのリスト	bundle_profiles	一覧	その他の VPN プロファイルのリスト。各プロファイルの前述の値のほとんどがサポートされています。詳しくは、「VPN プロファイルリストの各 VPN でサポートされるプロパティ」を参照してください。

カスタムパラメータ　各カスタムパラメータは、次のキーと値の名前を使用して定義する必要があります。

キー	値のタイプ	Value
ParameterName	テキスト	カスタムパラメータの名前。
ParameterValue	テキスト	カスタムパラメータの値。

Intune 設定のカスタムパラメータ

パラメーター名	説明	Value
UserAgent	Citrix Secure Access は、NetScaler Gateway と通信するときに、このパラメーター値をユーザーエージェントの HTTP ヘッダーに追加して、NetScaler Gateway で追加のチェックを実行します。	ユーザーエージェント HTTP ヘッダーに追加する必要があるテキストを指定します。テキストは、HTTP ユーザーエージェント仕様に準拠している必要があります。
EnableDebugLogging	Citrix Secure Access のデバッグログを有効にすると、常時接続 VPN の場合に VPN 接続の問題のトラブルシューティングに役立ちます。このオプションは、管理対象の VPN 構成のいずれかで有効にすることができます。デバッグのログは、管理対象の構成を処理するときに有効になります。	**True**: デバッグのログを有効にします。デフォルト値: **False**。

カスタムパラメータについて詳しくは、「Citrix Secure Access 用の Android Enterprise 管理構成の作成」を参照してください。

VPN プロファイルリストの各 **VPN** でサポートされるプロパティ　JSON テンプレートを使用して複数の VPN プロファイルを設定する場合、各 VPN プロファイルで次のプロパティがサポートされます。

構成キー	JSON フィールド名	値のタイプ
VPN プロファイル名	bundle_vpnProfileName	テキスト
サーバーアドレス (*)	bundle_serverAddress	URL
ユーザー名	bundle_username	テキスト
パスワード	bundle_password	テキスト
クライアント証明書エイリアス	bundle_clientCertalias	テキスト
ゲートウェイ証明書ピン	bundle_serverCertificatePins	テキスト
Per-App VPN の種類	bundle_perappVPN_allow_disallow	列挙型(許可、不許可)
perAppVPN アプリリスト	bundle_perappVPN_appnames	テキスト
カスタムパラメータ	bundle_customParameters	一覧

Intune で **Citrix Secure Access** を常時接続の **VPN** プロバイダーとして設定する

Android VPN サブシステムにオンデマンド VPN サポートがない場合は、Always On VPN を代替手段として使用して、Citrix Secure Access によるクライアント証明書認証とともにシームレスな VPN 接続オプションを提供できます。VPN は、起動時または仕事用プロファイルが有効になったときに、オペレーティングシステムによって起動されます。

Citrix Secure Access を Intune で常時稼働の VPN アプリにするには、次の設定を使用する必要があります。

- 使用する適切な管理対象設定の種類（仕事用プロファイルで個人所有または完全管理型、専用型、および企業所有の仕事用プロファイル）を選択します。
- デバイス構成プロファイルを作成し、[デバイスの制限] を選択し、[接続] セクションに移動します。VPN 常時接続設定で [有効] を選択します。
- VPN クライアントとして **Citrix Secure Access** を選択します。Citrix Secure Access がオプションとして利用できない場合は、「VPN クライアントとしてカスタム」を選択し、「パッケージ ID」フィールドに「**com.citrix.CitrixVPN** 」と入力します（パッケージ ID フィールドは大文字と小文字が区別されます）
- 他のオプションはそのままにしておきます。ロックダウンモードを有効にしないことをお勧めします。有効にすると、VPN が利用できない場合、デバイスは完全なネットワーク接続を失う可能性があります。

- これらの設定に加えて、前のセクションで説明したように、[****** アプリ構成ポリシー] ページで Per-App VPN の種類と ****PerAppVPN** アプリリストを設定して、Android の Per-App VPN を有効にすることもできます。

> 注:
>
> 常時接続 VPN は、Citrix Secure Access のクライアント証明書認証でのみサポートされます。

参照ドキュメント

Intune での接続オプションの設定の詳細については、次のトピックを参照してください。

- 完全に管理された企業所有の専用デバイス
- 個人所有のデバイス

常時接続 **VPN** の自動再起動

Citrix SSO for Android 23.8.1 以降、許可リストまたは禁止リストに含まれるアプリが仕事用プロファイルまたはデバイスプロファイルにインストールされている場合、Citrix Secure Access は Always On VPN を自動的に再起動します。新しくインストールされたアプリからのトラフィックは、仕事用プロファイルを再起動したりデバイスを再起動したりすることなく、VPN 接続を介して自動的にトンネリングされます。

Always On VPN の自動再起動を有効にするには、エンドユーザーが Citrix Secure Access に「すべてのパッケージを照会 」の許可を与える必要があります。同意が得られたら、Citrix Secure Access:

- オペレーティングシステムからパッケージインストール通知を受け取ります。
- 常時接続 VPN を再起動します。

エンドユーザーがアプリごとの VPN プロファイルに初めて接続すると、インストールされたパッケージの情報を収集するための同意を求めるメッセージが表示されます（Google のポリシーで義務付けられています）。エンドユーザーが同意すると、VPN 接続が開始されます。ユーザーが同意を拒否した場合、VPN 接続は中止されます。同意した後は、同意画面は再表示されません。エンドユーザーの手順について詳しくは、「Android デバイスから Citrix Secure Access を使用する方法」を参照してください。

制限事項

Android 11 で導入されたパッケージの公開設定の制限により、Android 11 以降のデバイス上の Android Enterprise 環境における Per-App VPN には、次の制限が適用されます。

- 許可/拒否リストに含まれるアプリが VPN セッションの開始後にデバイスに展開された場合、アプリがそのトラフィックを VPN セッション経由でルーティングできるようにするには、エンドユーザーが VPN セッションを再起動する必要があります。

- Per-App VPN を VPN 常時接続セッションで使用する場合、デバイスに新しいアプリをインストールした後、エンドユーザーは仕事用プロファイルを再起動するか、デバイスを再起動して、アプリのトラフィックを VPN セッション経由でルーティングする必要があります。

> 注:
>
> これらの制限は、Android 向け Citrix SSO 23.8.1 以降のバージョンを使用している場合には適用されません。詳細については、「Always On VPN の自動再起動」を参照してください。

Android 向け Citrix Secure Access による NetScaler Gateway 証明書ピン留め

April 1, 2024

> 重要:
>
> Android 向け Citrix SSO は、現在 Citrix Secure Access と呼ばれています。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。

証明書のピン留めは、中間者攻撃の防止に役立ちます。Citrix Secure Access は、Android Enterprise モードとレガシーデバイス管理者モードの管理対象 VPN 構成でのみ証明書ピン留めをサポートします。エンドユーザによって追加された VPN プロファイルではサポートされません。

Android Citrix Secure Access による NetScaler Gateway の証明書ピン留めの設定

Citrix Secure Access の管理対象構成（旧アプリ制限）における証明書ピン留めについて詳しくは、「証明書と認証」を参照してください。

固定された NetScaler Gateway 証明書ハッシュを伝送するために、新しいキーと値のペアが次のように定義されます。

```
Key: ServerCertificatePins
Value: {

  "hash-alg": "sha256",
  "pinset": [
    "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
       (SPKI)",
    "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="
    ...
  ]
 }

<!--NeedCopy-->
```


管理対象構成で証明書ピン留めの詳細を指定するためのキーは **ServerCertificatePins** です。この値は、固定された NetScaler Gateway 証明書の base64 でエンコードされた SHA-256 ハッシュと使用されるハッシュアルゴリズムを運ぶ JSON ペイロードです。固定証明書には、オペレーティングシステムによって検証された信頼チェーン内の任意の証明書を使用できます。この場合、それは Android です。

証明書のピン留めは、オペレーティングシステムが TLS ハンドシェイク中に証明書チェーンを検証した後にのみ実行されます。証明書の PIN は、証明書のサブジェクト公開キー情報 (SPKI) をハッシュすることによって計算されます。JSON ペイロードには、両方のフィールド (「hash-alg」と「**pinset**」) を指定する必要があります。

「**hash-alg**」は、SPKI ハッシュの計算に使用されるハッシュアルゴリズムを指定します。
「ピンセット」は、NetScaler Gateway 証明書の SPKI データの base64 でエンコードされた SHA-256 ハッシュを含む JSON 配列を指定します。
証明書の PIN には少なくとも 1 つの値を指定する必要があります。証明書のローテーションまたは有効期限を許可するために、PIN 値をさらに指定できます。

次の openssl コマンドを使用して、ドメイン（たとえば、gw.yourdomain.com）の暗証番号の値を計算できます。

```
openssl s_client -servername gw.yourdomain.com -connect gw.yourdomain.com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64
<!--NeedCopy-->
```

このコマンドは、ゲートウェイによって提示されたリーフ証明書の base64 エンコードされた SHA-256 ハッシュを表示します。チェーン内の任意の証明書を証明書のピン留めに使用できます。たとえば、企業が独自の中間 CA を使用して複数のゲートウェイの証明書を生成している場合、中間署名証明書に対応する PIN を使用できます。検証済みの証明書チェーン内の証明書と一致する PIN がない場合、TLS ハンドシェイクは中止され、ゲートウェイへの接続は続行されません。

> 注:
>
> デバイス管理者モードでは、証明書のピン留めは、Citrix Endpoint Management および Microsoft Endpoint Management ソリューションでのみサポートされます。証明書のピン留めは、レガシー VPN プロファイル（管理対象設定ではない）で使用されるカスタムパラメータで、固定用の同じ JSON ペイロードを持つカスタムパラメータ serverCertificatePins で設定する必要があります。

Citrix Secure Access for Windows リリースノート

April 1, 2024

Windows 向け Citrix Secure Access クライアントは現在スタンドアロンベースでリリースされており、すべての NetScaler ADC バージョンと互換性があります。Citrix Secure Access クライアントバージョンは、YY.MM リリース. ビルドの形式に従います。

リリースノートでは、新機能、既存機能の拡張、修正された問題について説明しています。

新機能: 現在のリリースで利用可能な新機能と機能強化。

修正された問題: 現在のリリースで修正された問題。

サポートされる機能について詳しくは、NetScaler Gateway 製品ドキュメントを参照してください。

> 注:
>
> - Windows 用 Citrix Secure Access クライアントビルド 23.7.1.1 以降には、https://support.citrix.com/article/CTX564833の修正が含まれています。
> - Citrix Secure Access クライアント（以前は Windows 用 NetScaler Gateway プラグインとして知られていました）ビルド 21.9.1.2 以降には、https://support.citrix.com/article/CTX341455の修正が含まれています。

24.2.1.15 (2024 年 3 月 4 日)

新機能

- **SNI** のサポート

  Citrix Secure Private Access 環境では、Citrix Secure Access クライアントはすべての事前認証要求でサーバー名表示（SNI）拡張をサポートするようになりました。

  [SPAHELP-236]

- **TLS 1.3** のサポート

  Citrix Secure Access クライアントは TLS 1.3 プロトコルをサポートするようになりました。TLS 1.3 は次のプラットフォームでサポートされています:

  - Windows 11 以降
  - Windows Server 2022 以降

  NetScaler で TLS 1.3 を構成する方法について詳しくは、「TLS 1.3 プロトコルのサポート」を参照してください。

  [CSACLIENTS-6106]

- **HTTP** ヘッダーの **Windows OS** 詳細のサポート

  Citrix Secure Access クライアントには、Windows OS の詳細が HTTP ヘッダー（ユーザーエージェント）文字列の一部として含まれるようになりました。

  [NSHELP-36732]

解決された問題

クライアントネットワークアダプタで IPv6 が有効になっていると、DNS 解決が断続的に失敗します。

[NSHELP-35708]

自動ログオンを使用して同時にログインしようとすると、ユーザーは Citrix Secure Access クライアントにログオンできないことがあります。

[NSHELP-35768]

英語以外のクライアントマシンでスマートアプリコントロールが有効になっていると、Citrix Secure Access のインストールが失敗します。

[NSHELP-36126]、[NSHELP-36907]

Citrix Secure Access クライアントが WFP ドライバーで構成されている場合、ユーザーは VPN 経由で一部のアプリケーションにアクセスできません。この問題は、ファイアウォールポリシーの変更が原因で発生します。

[NSHELP-36254]、[NSHELP-36312]

EPA スキャン中にポップアップダイアログが表示されます。ただし、ユーザーが「OK」をクリックすると、EPA スキャンは通常どおり機能します。この問題は、Citrix Secure Access クライアント UI でスウェーデン語を選択した場合（[構成] **>** [言語]）に発生します。

[NSHELP-36408]

Always On VPN モードでは、NetScaler Gateway でユーザー証明書認証が構成されていると、マシンレベルのトンネルがセッションを転送できません。

[NSHELP-36492]

Citrix Secure Access クライアントで Windows フィルタリングプラットフォーム（WFP）ドライバーが有効になっていると、イントラネットリソースへのアクセスが断続的に失敗します。

[NSHELP-36568]

ユーザーが［ホーム］ボタンをクリックすると、Citrix Secure Access クライアントの UI ページが断続的にフリーズします。

[NSHELP-37046]

管理者以外のユーザーは、次の条件が満たされている場合、完全な VPN トンネルに接続できません:

- EPA は nFactor フローのファクターとして設定されます。
- Edge WebView は有効になっています。
- Citrix EPA クライアントのコントロールアップグレード設定が［NetScaler **Gateway** の常時オン］に設定されており、クライアントデバイスと NetScaler の間で Citrix EPA クライアントのバージョンが一致していません。

[NSHELP-37340]

クライアントマシンのシステム証明書ストアにデバイス証明書が 1 つしか含まれていない場合、EPA デバイス証明書スキャンは失敗します。

[NSHELP-37371]

Citrix Secure Private Access サービスに接続すると、Citrix Secure Access クライアントのログインページが断続的に空白になります。

[SPAHELP-202]

Windows Server 2019 以降のバージョンを使用している場合、エンドユーザーは VPN 経由でクライアントマシンをドメインに接続できないことがあります。

[SPAHELP-219]

Citrix Device Posture サービスが有効になっていると、Citrix Secure **Access** クライアント **UI** の接続ドロップダウンリストに不要なエントリが表示されます。

[SPAHELP-271]

Citrix Secure Access クライアントでシングルサインオン機能が有効になっている場合、エンドユーザーはイントラネットリソースにアクセスできません。

[CSACLIENTS-9940]

23.10.1.7 (2023 年 11 月 29 日)

新機能

- サーバーが開始する接続のプライベートポート範囲の設定

  サーバーが開始する接続用に、49152 ～64535 の範囲のプライベートポートを設定できるようになりました。プライベートポートを構成することで、ポートを使用して Citrix Secure Access クライアントとクライアントマシン上のサードパーティアプリとの間でソケットを作成するときに発生する可能性のある競合を回避できます。プライベートポートは、「SicBeginPort」の Windows VPN レジストリを使用して設定できます。または、NetScaler の VPN プラグインカスタマイズ JSON ファイルを使用してプライベートポート範囲を構成することもできます。

  詳しくは、「サーバー起動接続の構成」および「NetScaler Gateway WindowsVPN クライアントのレジストリキー」を参照してください。

  [NSHELP-36627]

- シームレスな自動ログオンを実現する **Kerberos** 認証サポート

  Citrix Secure Access クライアントは、自動ログオンに Kerberos 認証方法を使用するようになりました。このサポートの一環として、VPN クライアントのレジストリキー「EnableKerberosAuth」が導入されまし

た。前提条件として、管理者は NetScaler とクライアントマシンで Kerberos 認証を構成する必要があります。エンドユーザーは、自分のマシンに Microsoft Edge WebView をインストールして、Kerberos 認証方法を有効にする必要があります。詳しくは、「Kerberos 認証による自動ログオン」を参照してください。

[CSACLIENTS-3128]

- スプーフィング **IP** アドレス範囲の自動割り当て

  Citrix Secure Access Client は、管理者が構成したスプーフィング IP アドレス範囲と IP ベースのアプリケーションまたはエンドユーザーのネットワークとの間に競合がある場合に、新しいスプーフィング IP アドレス範囲を検出して適用できるようになりました。

  [CSACLIENTS-6132]

- **Microsoft** 通知

  Citrix Secure Access クライアントの通知が、Windows マシンの通知パネルに Microsoft の通知として表示されるようになりました。

  [CSACLIENTS-6136]

- ログ収集の改善

  ログ収集とトラブルシューティングを強化するため、Verbose ログレベルがデフォルトのデバッグログレベルとして使用されるようになりました。ログについて詳しくは、「クライアントユーザーインターフェイスを使用してログを構成する」を参照してください。

  [CSACLIENTS-8151]

解決された問題

Always On サービスのマシントンネルがクライアントデバイスの場所を検出できない場合、Citrix Secure Access クライアントは「接続中」状態のままになります。

[CSACLIENTS-1174]

Citrix Secure Access クライアントで Microsoft Edge WebView が有効になっていると、ログオン転送機能が動作しません。

[CSACLIENTS-6655]

Always On サービスモードでは、デバイス証明書ベースの従来の認証ポリシーが VPN 仮想サーバーにバインドされている場合、Citrix Secure Access クライアントは NetScaler Gateway とのマシンレベルのトンネルを確立できません。

[NSHELP-33766]

ユーザが VPN に接続すると、着信および発信の Webex コールが失敗します。この問題は、Citrix Secure Access クライアントで確定的ネットワークエンハンサー（DNE）ドライバーではなく Windows フィルタープラットフォーム（WFP）ドライバーが有効になっている場合に発生します。

[NSHELP-34651]

次の条件が満たされると、Citrix Secure Access クライアントがクラッシュします:

- SAML ポリシーが VPN 仮想サーバーにバインドされると、接続が切り替わります。
- Internet Explorer WebView サポートが有効になっています。

[NSHELP-35366]

Citrix Secure Access クライアントのユーザーインターフェイスには、自動ログオン中に「接続」ボタンが表示されます。この問題は、UserCert 認証方法を使用して VPN に接続する場合に発生します。

[NSHELP-36134]

マシンレベルのトンネルが構成されている場合、ローカル LAN アクセス機能は Citrix Secure Access クライアントでは機能しません。

今回のリリースでは、ローカル LAN アクセス機能をマシンレベルのトンネル構成で設定できます。これを実現するには、マシントンネルモードを使用するときにローカル LAN アクセスパラメータを FORCESD に設定する必要があります。詳細については、「ADC 構成に基づいてエンドユーザーにローカル LAN アクセスを強制する」を参照してください。

[NSHELP-36214]

クライアントマシンがスリープモードから複数回起動すると、Citrix Secure Access クライアントはイントラネットアプリケーションとの VPN 接続を確立できません。

[NSHELP-36221]

23.8.1.11 (2023 年 10 月 19 日)

解決された問題

NetScaler Gateway でフォワードプロキシサポートが構成されている場合、epaPackage.exe ファイルのダウンロードに失敗することがあります。

[CSACLIENTS-6917]

C ドライブへのアクセスが制限されている管理者以外のユーザーでは、Citrix EPA クライアントのインストールが失敗します。

[NSHELP-36590]

23.8.1.5 (2023 年 8 月 9 日)

解決された問題

Citrix Secure Private Access・サービスを介してアプリケーションに接続すると、Kerberos SSO が失敗します。

[CSACLIENTS-912]

Citrix Secure Private Access サービスによるアプリケーションアクセスが断続的に失敗します。この問題は、Citrix Secure Access クライアントが TCP または UDP トラフィックの誤った宛先 IP アドレスを共有している場合に発生します。

[CSACLIENTS-1151, CSACLIENTS-6326]

DNS キャッシュの問題により、Citrix Secure Access クライアントが断続的にアプリケーションを起動できなくなります。

[CSACLIENTS-1170]

Citrix Secure Access クライアントが Citrix 仮想アダプタに DNS サフィックスを適用できません。この問題は、Citrix 仮想アダプターが Active Directory による認証に失敗した場合に発生します。

[NSHELP-33817]

次の条件が満たされると、Citrix Secure Access クライアントがクラッシュします:

- NetScaler Gateway 仮想サーバーには、nFactor 認証の要素としてクライアント証明書が含まれています。
- Microsoft Edge WebView サポートが有効になっています。

[CSACLIENTS-6171]

VPN に接続していると、Microsoft KB5028166 を適用した後にバックエンドリソースにアクセスできなくなる場合があります。

[NSHELP-35909]

ポータルのカスタマイズが許可されている制限を超えると、Citrix Secure Access クライアントは NetScaler Gateway からの構成のダウンロードに断続的に失敗します。

[NSHELP-35971]

既知の問題

転送ログオン機能は Citrix Secure Access クライアントでは動作しません。この問題は、Microsoft Edge WebView が有効になっている場合に発生します。

回避策:Web ブラウザを使用してログオンし、セッションを転送します。

23.7.1.1 (2023 年 7 月 14 日)

解決された問題

リリースバージョン 23.x.x.x にアップグレードした後、NetScaler でイントラネット IP 範囲が構成されていると、トラフィックが VPN トンネルを通過できず、VPN アクセスがブロックされることがあります。これは、クロスプロファイルファイアウォールルールが VPN アプリケーションに適用されていない場合に発生します。

[NSHELP-35766]

23.5.1.3 (2023 年 6 月 2 日)

解決された問題

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`下の「useNewLogger」レジストリを使用して改善されたログ収集を有効にすると、Always On サービスがクラッシュします。

[CGOP-24462]

23.4.1.5 (2023 年 4 月 14 日)

新機能

- **Microsoft Edge WebView** サポート

  Windows 向け Citrix Secure Access クライアントでの Microsoft Edge WebView サポートにより、エンドユーザーエクスペリエンスが強化されました。この機能はデフォルトでは無効になっています。詳細については、「Windows Citrix Secure Access の Microsoft Edge WebView サポート」を参照してください。

  [CGOP-22245]

- **IP** アドレスに **FQDN** を解決するための **DNS** サフィックスの追加

  管理者は、オペレーティングシステムレベルでアプリケーションにサフィックスを追加できるようになりました。これにより、Citrix Secure Access クライアントは、名前解決時に完全修飾されていないドメイン名を解決できます。

  管理者は、エンドユーザーが対応する FQDN を使用してアプリケーションにアクセスできるように、IP アドレス（IP CIDR/IP 範囲）を使用してアプリケーションを設定することもできます。詳細については、「FQDN を IP アドレスに変換するための DNS サフィックス」を参照してください。

  [ACS-2490]

- ログ収集の改善

  Windows Secure Access クライアントのログ機能が改善され、ログの収集とデバッグが可能になりました。ロギング機能に次の変更が加えられました。

- ユーザーがログファイルの最大サイズを 600 MB 未満の値に変更できるようにします。
- ユーザーがログファイルの数を 5 個未満に更新できるようにします。
- 新しいロギング機能のログレベルを 3 に増やしてください。

これらの変更により、管理者とエンドユーザーは現在のセッションと過去のセッションからログを収集できます。以前は、ログの収集は現在のセッションのみに制限されていました。詳細については、「Windows クライアントのログ収集の改善」を参照してください。

> 注:
>
> デバッグログを有効にするには、「ログレベルの選択」ドロップダウンリストから「Logging」>「Verbose」を選択します。Citrix Secure Access クライアントの Windows 23.4.1.5 リリースより前のリリースでは、［構成］**>**［デバッグログを有効にする］チェックボックスを使用してデバッグログを有効にできました。

[CGOP-23537]

- **Citrix Analytics** サービスへのイベント送信のサポート

  Windows 向け Citrix Secure Access クライアントは、セッションの作成、セッションの終了、Citrix Analytics サービスへのアプリケーション接続などのイベントの送信をサポートするようになりました。その後、これらのイベントは Citrix Secure Private Access ダッシュボードに記録されます。

  [SPA-2197]

解決された問題

- Citrix Workspace アプリによるクラウドエンドポイントへの Citrix Secure Access クライアントのシングルサインオン認証は、Unicode ユーザーでは失敗します。

  [CGOP-22334]

- Citrix Secure Private Access でホスト名ベースのアプリケーションを DNS サフィックスと一緒に構成すると、リソースへのアクセスが失敗します。

  [SPA-4430]

- ゲートウェイの仮想サーバーへの到達性の問題により、Always-On VPN 接続が起動時に断続的に失敗します。

  [NSHELP-33500]

- Citrix Secure Access クライアントで分割トンネルがオフに設定されていると、なりすまし IP アドレス範囲と重複するイントラネットリソースにアクセスできません。

  [NSHELP-34334]

- Citrix Secure Access クライアントが認証スキーマの読み込みに失敗し、Citrix Secure Private Access サービスへのログインが失敗します。

  [SPAHELP-98]

23.1.11 (2023 年 2 月 20 日)

このリリースでは、Citrix Secure Private Access サービスの全体的なパフォーマンスと安定性の向上に役立つ問題が修正されています。

23.1.1.8 (2023 年 2 月 8 日)

解決された問題

- DNS 解決の失敗は、Citrix Secure Access が IPv4 パケットを IPv6 パケットよりも優先しない場合に発生します。

  [NSHELP-33617]

- OS のフィルタリングルールは、Citrix Secure Access クライアントが Windows フィルタリングプラットフォーム（WFP）モードで実行されているときにキャプチャされます。

  [NSHELP-33715]

- Citrix Secure Access クライアントが Citrix Deministic Network Enhancer（DNE）モードで実行されている場合、スプーフィングされた IP アドレスが IP ベースのイントラネットアプリケーションに使用されます。

  [NSHELP-33722]

- Windows フィルタリングプラットフォーム (WFP) ドライバーを使用する場合、VPN を再接続した後にイントラネットアクセスが機能しないことがあります。

  [NSHELP-32978]

- Windows 10 および Windows 11 Enterprise のマルチセッションデスクトップで、OS バージョンチェック用のエンドポイント分析 (EPA) スキャンが失敗します。

  [NSHELP-33534]

- Windows クライアントは、デフォルトで 64 KB の構成ファイルサイズをサポートしているため、ユーザーは構成ファイルにさらにエントリを追加することが制限されます。このサイズは、HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client のレジストリ値`ConfigSize`を設定することで増やすことができます。`ConfigSize`レジストリキータイプは`REG_DWORD`で、キーデータは<`Bytes size`>です。構成ファイルのサイズがデフォルト値 (64 KB) より大きい場合は、64 KB を追加するたびに ConfigSize レジストリ値を (バイトに変換後) 5 x 64 KB に設定する必要があります。たとえば、64 KB を追加する場合

は、レジストリ値を 64 x 1024 x 5 = 327680 に設定する必要があります。同様に、128 KB を追加する場合は、レジストリ値を 64 x 1024 x (5+5) = 655360 に設定する必要があります。

[SPA-2865]

- VPN ログオフ時に、SearchList レジストリの DNS サフィックスリストのエントリは、1 つ以上のカンマで区切られた逆の順序で書き換えられます。

  [NSHELP-33671]

- NetScaler ADC アプライアンスがウイルス対策の EPA スキャンを完了すると、プロキシ認証は失敗します。

  [NSHELP-30876]

- Citrix Secure Access 関連のレジストリ値が 1500 文字を超える場合、ログコレクターはエラーログを収集できません。

  [NSHELP-33457]

22.10.1.9 (2022 年 11 月 8 日)

新機能

- **GSLB** での接続プロキシタイプのサイトパーシステンスに対する **EPA** サポート

  Windows EPA スキャンは、スキャンをブラウザーから開始するときの GSLB での接続プロキシタイプのサイトパーシステンスをサポートするようになりました。以前は、Windows 用 EPA スキャンは、ブラウザが開始する EPA スキャンの接続プロキシパーシステンスタイプをサポートしていませんでした。

  [CGOP-21545]

- ワークスペース **URL** のシームレスなシングルサインオン **(**クラウドのみ**)**

  Citrix Secure Access クライアントは、ユーザーが Citrix Workspace アプリですでにログオンしている場合、ワークスペース URL のシングルサインオン（クラウドのみ）をサポートするようになりました。詳しくは、「Citrix Workspace アプリを使用してログインしたユーザーのワークスペース URL のシングルサインオンサポート」を参照してください。

  [ACS-2427]

- **Citrix Workspace** アプリ（クラウドのみ）を使用して **Citrix Secure Access** クライアントおよび**/**または **EPA** プラグインバージョンを管理

  Citrix Workspace アプリでは、グローバルアプリ構成サービスを介して最新バージョンの Citrix Secure Access または EPA プラグインをダウンロードしてインストールできるようになりました。詳細については、「グローバルアプリ構成サービス」を参照してください。

  [ACS-2426]

- デバッグロギング制御の強化

  Citrix Secure Access クライアントのデバッグログ制御は、NetScaler Gateway に依存せず、マシントンネルとユーザートンネルの両方のプラグイン UI から有効または無効にできるようになりました。

  [NSHELP-31968]

- プライベートネットワークアクセスのプリフライトリクエストのサポート

  Citrix Secure Access Client for Windows は、公開 Web サイトからプライベートネットワークリソースにアクセスするときに Chrome ブラウザによって発行されるプライベートネットワークアクセスのプリフライトリクエストをサポートするようになりました。

  [CGOP-20544]

解決された問題

- Citrix Secure Access クライアントのバージョン 21.7.1.1 以降では、管理者権限のないユーザーが新しいバージョンにアップグレードできません。

  これは、Citrix Secure Access クライアントのアップグレードが NetScaler ADC アプライアンスから行われた場合にのみ適用されます。詳しくは、「Citrix Secure Access クライアントのアップグレード/ダウングレードの問題」を参照してください。

  [NSHELP-32793]

- EPA の障害が断続的に発生するため、ユーザーは VPN にログオンできません。

  [NSHELP-32138]

- マシントンネルのみモードの Citrix Secure Access クライアントは、マシンがスリープモードから復帰した後に、自動的にマシントンネルを確立しないことがあります。

  [NSHELP-30110]

- Always on service モードでは、マシントンネルのみが構成されていても、ユーザートンネルは起動を試みます。

  [NSHELP-31467]

- Microsoft Edge がデフォルトのブラウザの場合、Citrix Secure Access UI のホームページリンクは機能しません。

  [NSHELP-31894]

- カスタマイズされた EPA 障害ログメッセージは NetScaler Gateway ポータルには表示されず、代わりに「内部エラー」というメッセージが表示されます。

  [NSHELP-31434]

- ユーザーが Windows 向け Citrix Secure Access 画面の［ホームページ］タブをクリックすると、ページに接続拒否エラーが表示されます。

  [NSHELP-32510]

- 一部のクライアントマシンでは、Citrix Secure Access クライアントがプロキシ設定を検出できず、ログオンが失敗します。

  [SPAHELP-73]

既知の問題

- Windows Update チェックベースの EPA スキャンは、Windows 11 22H2 バージョンでは機能しません。詳細については、「Windows11 22H2 の EPA チェックが失敗する」を参照してください。

  [NSHELP-33068]

22.6.1.5 (2022 年 6 月 17 日)

新機能

- ログインとログアウトのスクリプト設定

  Citrix Secure Access クライアントは、Citrix Secure Access クライアントが Citrix Secure Private Access クラウドサービスに接続するときに、次のレジストリからログインおよびログアウトスクリプト構成にアクセスします。

  レジストリパス：**HKEY_LOCAL_MACHINE>** ソフトウェア **>Citrix>Secure Access Client**

  レジストリ値:

  - SecureAccessLoginScript タイプ REG_SZ-ログインスクリプトへのパス
  - SecureAccessLogoutScript タイプ REG_SZ-ログアウトスクリプトへのパス

  [ACS-2776]

- **Windows** フィルタリングプラットフォーム **(WFP)** を使用する **Windows Citrix Secure Access** クライアント

  WFP は、ネットワークフィルタリングアプリケーションを作成するためのプラットフォームを提供する一連の API およびシステムサービスです。WFP は、DNE ドライバーで使用されていたネットワークドライバーインターフェイス仕様 (NDIS) フィルターという、以前のパケットフィルター技術を置き換えるように設計されています。詳しくは、「Windows フィルタリングプラットフォームを使用する Windows Citrix Secure Access クライアント」を参照してください。

  [CGOP-19787]

- **FQDN** ベースの逆分割トンネルのサポート

  WFP ドライバーが FQDN ベースの REVERSE 分割トンネリングのサポートを有効にするようになりました。DNE ドライバーではサポートされていません。リバース分割トンネルの詳細については、分割トンネリングオプションを参照してください。

  [CGOP-16849]

解決された問題

- ユーザーが Always On サービスモードで Windows マシンにログインすると、Windows 自動ログオンが機能しない場合があります。マシントンネルはユーザートンネルに移行せず、VPN プラグインの UI に「接続中」というメッセージが表示されます。

  [NSHELP-31357]

- VPN ログオフ時に、SearchList (コンピューター\ HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client) レジストリ内の DNS サフィックスリストのエントリは、1 つ以上のカンマで区切られた逆の順序で書き換え

  [NSHELP-31346]

- なりすまし IP アドレスは、NetScaler ADC イントラネットアプリケーションの構成が FQDN ベースから IP ベースのアプリケーションに変更された後でも使用されます。

  [NSHELP-31236]

- ゲートウェイのホームページは、ゲートウェイプラグインが VPN トンネルを正常に確立した直後には表示されません。

  今回の修正により、次のレジストリ値が導入されました。

  \HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds

  種類：DWORD

  デフォルトでは、このレジストリ値は設定も追加もされません。「SecureChannelResetTimeoutSeconds」の値が 0 または追加されていない場合、遅延を処理するための修正が機能しません。これはデフォルトの動作です。管理者は、このレジストリをクライアントに設定して修正を有効にする必要があります (つまり、ゲートウェイプラグインが VPN トンネルを正常に確立した直後にホームページを表示する)。

  [NSHELP-30189]

- レジストリ値が 2000 バイトを超えると、AlwaysOnAllow リストレジストリが期待どおりに動作しません。

  [NSHELP-31836]

- Windows 向け Citrix Secure Access クライアントは、すでに接続されている Citrix Secure Private Access サービスリージョンにアクセスできなくなった場合でも、新しい TCP 接続をバックエンド TCP サーバーにトンネリングしません。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

[ACS-2714]

22.3.1.5 (2022 年 3 月 24 日)

解決された問題

- Windows EPA プラグイン名は、NetScaler Gateway EPA プラグインに戻されます。

  [CGOP-21061]

既知の問題

- Windows 向け Citrix Secure Access クライアントは、すでに接続されている Citrix Secure Private Access サービスリージョンにアクセスできなくなった場合でも、新しい TCP 接続をバックエンド TCP サーバーにトンネリングしません。ただし、これはオンプレミスのゲートウェイ接続には影響しません。

  [ACS-2714]

22.3.1.4 (2022 年 3 月 10 日)

新機能

- **ADC** 構成に基づいてエンドユーザーにローカル **LAN** アクセスを強制する

  管理者は、エンドユーザーがクライアントマシンのローカル LAN アクセスオプションを無効にすることを制限できます。既存のローカル LAN アクセスパラメータ値に、FORCED という新しいオプションが追加されました。ローカル LAN アクセス値が FORCED に設定されている場合、クライアントマシンのエンドユーザーはローカル LAN アクセスが常に有効になります。エンドユーザーは、Citrix Secure Access クライアント UI を使用してローカル LAN 設定を無効にすることはできません。管理者がエンドユーザーにローカル LAN アクセスを有効または無効にするオプションを提供したい場合は、ローカル LAN アクセスパラメーターを ON に再構成する必要があります。

  GUI を使用して **FORCED** オプションを有効にするには、次の手順を実行します:

  1. ［**NetScaler Gateway**］**>**［グローバル設定］**>**［グローバル設定の変更］に移動します。
  2. [クライアントエクスペリエンス] タブをクリックし、[詳細設定] をクリックします。
  3. [ローカル **LAN** アクセス] で [強制] を選択します

  CLI を使用して **FORCED** オプションを有効にするには、次のコマンドを実行します。

  ```
  set vpn parameter -localLanAccess FORCED
  <!--NeedCopy-->
  ```

  [CGOP-19935]

- **EPA OS** スキャンでの **Windows** サーバー **2019** および **2022** のサポート

  EPA OS スキャンで、Windows サーバー 2019 および 2022 がサポートされるようになりました。

  GUI を使用して新しいサーバを選択できます。

  1. **NetScaler Gateway >** ポリシー **>** 事前認証に移動します。
  2. 新しい事前認証ポリシーを作成するか、既存のポリシーを編集します。
  3. [**OPSWAT EPA** エディタ**]** リンクをクリックします。
  4. 式エディタで、[ウィンドウ**] > [Windows Update**] を選択し、[**+**] アイコンをクリックします。
  5. [**OS Name**] で、要件に従ってサーバを選択します。

  EPA OS スキャンで Windows サーバー 2019 および 2022 を使用するには、OPSWAT バージョン 4.3.2744.0 にアップグレードできます。

  [CGOP-20061]

- 不足しているセキュリティパッチに対する新しい **EPA** スキャン分類タイプ

  不足しているセキュリティパッチの EPA スキャンに、次の新しい分類タイプが追加されました。クライアントに次の不足しているセキュリティパッチのいずれかがある場合、EPA スキャンは失敗します。

  - アプリケーション
  - コネクタ
  - クリティカルなアップデート
  - 定義更新
  - developerKits
  - FeaturePack
  - ガイダンス
  - セキュリティアップデート
  - ServicePack
  - ツール
  - UpdateRollUps
  - アップデート

  GUI を使用して分類タイプを設定できます。

  1. **NetScaler Gateway >** ポリシー **>** 事前認証に移動します。
  2. 新しい事前認証ポリシーを作成するか、既存のポリシーを編集します。
  3. ((OPSWAT EPA エディタ)) リンクをクリックします。
  4. 式エディタで [ウィンドウ**] > [Windows Update**] を選択します。
  5. [次の **Windows Update** 分類タイプの未適用パッチがあってはならない] で、未適用のセキュリティパッチの分類タイプを選択します。
  6. [**OK**] をクリックします。

  OPSWAT バージョン 4.3.2744.0 にアップグレードして、これらのオプションを使用できます。

  - Windows サーバ更新サービス分類 GUID の詳細については、https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)を参照してください。
  - Microsoft のソフトウェア更新プログラムの用語については、「https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates」を参照してください。

以前は、欠落しているセキュリティパッチの EPA スキャンは、Windows クライアントの重大度 (重大、重要、中、低) で行われていました。

[CGOP-19465]

- **EPA** スキャン用の複数デバイス証明書のサポート

  Always on VPN 設定では、複数のデバイス証明書が設定されている場合、有効期限が最も長い証明書が VPN 接続で試行されます。この証明書で EPA スキャンが正常に許可されると、VPN 接続が確立されます。この証明書がスキャンプロセスで失敗すると、次の証明書が使用されます。このプロセスは、すべての証明書が試行されるまで続きます。

  以前は、複数の有効な証明書が構成されていて、1 つの証明書の EPA スキャンが失敗すると、他の証明書に対してスキャンは試行されませんでした。

  [CGOP-19782]

解決された問題

- VPN 仮想サーバーを構成するときに SSL プロファイルで ClientCert パラメーターが「オプション」に設定されている場合、スマートカードを選択するように求めるメッセージが複数回表示されます。

  [NSHELP-30070]

- ［NetworkAccessonVPNFailure］プロファイルパラメーターを［フルアクセス］から［OnlyToGateway］に変更すると、ユーザーは NetScaler Gateway アプライアンスに接続できなくなります。

  [NSHELP-30236]

- Always on が設定されている場合、aoservice.exe ファイルのバージョン番号（1.1.1.1）が正しくないため、ユーザトンネルが失敗します。

  [NSHELP-30662]

- 内部リソースと外部リソースに対する DNS 解決は、長期間の VPN セッションでは機能しなくなります。

  [NSHELP-30458]

- Windows VPN クライアントは、サーバからの「SSL close notify」アラートを尊重せず、同じ接続で転送ログイン要求を送信します。

  [NSHELP-29675]

- レジストリ EPA は「==」と「!=」演算子は一部のレジストリエントリで失敗します。

  [NSHELP-29582]

22.1.103 (2022 年 2 月 17 日)

解決された問題

- Chrome 98 または Edge 98 ブラウザバージョンにアップグレードすると、ユーザーは EPA プラグインまたは VPN プラグインを起動できません。この問題を解決するには、次の手順に従います。

  1. VPN プラグインをアップグレードする場合、エンドユーザーは最初に VPN クライアントを使用して接続し、各自のマシンで修正プログラムを取得する必要があります。それ以降のログイン試行では、接続するブラウザまたはプラグインを選択できます。
  2. EPA のみのユースケースでは、エンドユーザにはゲートウェイに接続するための VPN クライアントがありません。この場合は、次の操作を行います。

     a) ブラウザを使用してゲートウェイに接続します。
     b) ダウンロードページが表示されるのを待ち、nsepa_setup.exe をダウンロードします。
     c) ダウンロード後、ブラウザを閉じて nsepa_setup.exe ファイルをインストールします。
     d) クライアントを再起動します。

  [NSHELP-30641]

21.12.1.4 (17-Dec-2021)

新機能

- リブランディングの変更

  Windows 用 NetScaler Gateway プラグインは、Citrix Secure Access クライアントにリブランドされました。

  [ACS-2044]

- **TCP/HTTP (S)** プライベートアプリケーションのサポート

  Citrix Secure Access クライアントは、Citrix Workspace Secure Access サービスを通じてリモートユーザー向けの TCP/HTTP (S) プライベートアプリケーションをサポートするようになりました。

  [ACS-870]

- 追加言語のサポート

  NetScaler Gateway 用の Windows VPN および EPA プラグインで、次の言語がサポートされるようになりました。

- 韓国語
- ロシア語
- 繁体字中国語

[CGOP-17721]

- **Windows 11** での **Citrix Secure Access** のサポート

  Citrix Secure Access クライアントが Windows 11 でサポートされるようになりました。

  [CGOP-18923]

- ユーザーが同じマシンからログインしていて、**Always on** が構成されている場合の自動転送ログオン

  Always on が構成され、ユーザーが同じマシンからログインしている場合に、ユーザーの介入なしに自動ログイン転送が行われるようになりました。以前は、システムの再起動やネットワーク接続の問題などのシナリオでクライアント (ユーザ) が再ログインすると、ポップアップメッセージが表示されていました。ユーザーは移管ログインを確認する必要がありました。この機能強化により、ポップアップウィンドウは無効になりました。

  [CGOP-14616]

- **NetScaler ADC** が提供するネットマスクから **Citrix** 仮想アダプタのデフォルトゲートウェイ **IP** アドレスを導出する

  Citrix 仮想アダプタのデフォルトゲートウェイ IP アドレスは、NetScaler ADC が提供するネットマスクから導出されるようになりました。

  [CGOP-18487]

解決された問題

- 分割トンネル ON モードで VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。Citrix Virtual アダプターのデフォルトルートに誤りがあると、このネットワークの問題が発生します。

  [NSHELP-26779]

- 分割トンネルが「リバース」に設定されている場合、イントラネットドメインの DNS 解決は失敗します。

  [NSHELP-29371]

21.9.100.1 (2021 年 12 月 30 日)

新機能

- **Windows 11** での **Citrix Secure Access** のサポート

  Citrix Secure Access クライアントが Windows 11 でサポートされるようになりました。

  [CGOP-18923]

解決された問題

- 分割トンネル ON モードで VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。Citrix Virtual アダプターのデフォルトルートに誤りがあると、このネットワークの問題が発生します。

  [NSHELP-26779]

- 分割トンネルが「リバース」に設定されている場合、イントラネットドメインの DNS 解決は失敗します。

  [NSHELP-29371]

21.9.1.2（04-Oct-2021）

解決された問題

- VPN の切断後、DNS リゾルバがホスト名の解決に失敗することがあります。これは、VPN の切断中に DNS サフィックスが削除されるためです。

  [NSHELP-28848]

- クライアントのアイドルタイムアウトが設定されていると、ユーザーが数秒以内に NetScaler Gateway からログアウトすることがあります。

  [NSHELP-28404]

- Windows プラグインは、認証中にクラッシュすることがあります。

  [NSHELP-28394]

- Always On サービスモードでは、Windows 用 VPN プラグインは、ユーザーが Windows マシンにログオンした後、ユーザートンネルを自動的に確立できません。

  [NSHELP-27944]

- トンネルの確立後、以前のゲートウェイ IP アドレスで DNS サーブルートを追加する代わりに、Windows プラグインはデフォルトゲートウェイアドレスを持つルートを追加します。

  [NSHELP-27850]

V21.7.1.1 (27-Aug-2021)

新機能

- 新しい **MAC** アドレススキャン

  新しい MAC アドレススキャンのサポートが追加されました。

  [CGOP-16842]

- **EPA** スキャンで **Windows OS** とそのビルドバージョンを確認する

  Windows OS とそのビルドバージョンを確認するための EPA スキャンを追加しました。

  [CGOP-15770]

- **EPA** スキャンで特定の値の存在をチェックする

  レジストリ EPA スキャンの新しいメソッドは、特定の値の存在をチェックするようになりました。

  [CGOP-10123]

解決された問題

- ネットワークエラーが原因でログイン中に JavaScript エラーが発生した場合、後続のログイン試行は同じ JavaScript エラーで失敗します。

  [NSHELP-27912]

- McAfee アンチウイルスの最終更新時刻のチェックで EPA スキャンが失敗する。

  [NSHELP-26973]

- VPN トンネルが確立されると、ユーザがインターネットにアクセスできなくなることがあります。

  [NSHELP-26779]

- VPN プラグインのスクリプトエラーが nFactor 認証中に表示されることがあります。

  [NSHELP-26775]

- ネットワークの中断が発生した場合、ネットワークが中断する前に開始された UDP トラフィックフローは、最大 5 分間はドロップされません。

  [NSHELP-26577]

- DNS 登録に予想よりも長い時間がかかる場合、VPN トンネルの開始に遅延が生じることがあります。

  [NSHELP-26066]

V21.3.1.2 (31-Mar-2021)

新機能

- アップグレードされた **EPA** ライブラリ

  EPA ライブラリは、EPA スキャンで使用されるソフトウェアアプリケーションの最新バージョンをサポートするようにアップグレードされます。

  [NSHELP-26274]

- **NetScaler Gateway** 仮想アダプタの互換性

  NetScaler Gateway 仮想アダプターは、Hyper-V および Microsoft Wi-Fi Direct 仮想アダプター（プリンターで使用）と互換性があります。

  [NSHELP-26366]

解決された問題

- Windows VPN ゲートウェイプラグインは、VPN トンネルでの「CTRL + P」と「CTRL + O」の使用をブロックします。

  [NSHELP-26602]

- Windows 向け NetScaler Gateway プラグインは、マシン名の`"nslookup"`アクションが要求されたときに、Active Directory に登録されたイントラネット IP アドレスでのみ応答します。

  [NSHELP-26563]

- スプリット DNS が「ローカル」または「両方」に設定されている場合、IIP の登録および登録解除は断続的に失敗します。

  [NSHELP-26483]

- Always On が構成されている場合、Windows VPN ゲートウェイプラグインへの自動ログオンが失敗します。

  [NSHELP-26297]

- Windows VPN ゲートウェイプラグインが IPv6 DNS パケットのドロップに失敗し、DNS 解決に問題が生じます。

  [NSHELP-25684]

- Windows VPN ゲートウェイプラグインは、Internet Explorer のプロキシ除外リストのブラウザー制限のためにプロキシ除外リストがオーバーフローした場合でも、既存のプロキシ除外リストを維持します。

  [NSHELP-25578]

- Windows VPN ゲートウェイプラグインは、VPN クライアントが Always On モードでログオフすると、プロキシ設定を復元できません。

  [NSHELP-25537]

- Windows 用 VPN プラグインは、次の条件が満たされている場合、Windows へのログオン後にトンネルを確立しません。

  - NetScaler Gateway アプライアンスは、常時オン機能用に構成されています。
  - アプライアンスは、2 要素認証が「off」の証明書ベースの認証用に設定されています。

  [NSHELP-23584]

Windows Citrix Secure Access の Microsoft Edge WebView サポート-プレビュー

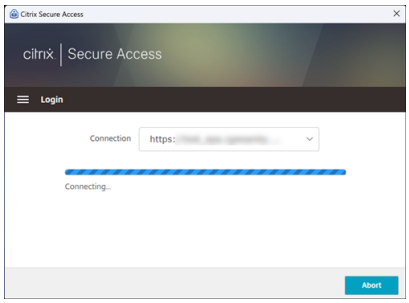
April 1, 2024

Internet Explorer WebView は廃止されたため、Microsoft Edge WebView はマイクロソフトが推奨している WebView になりました。Microsoft Edge WebView の機能を利用するには、Citrix Secure Access クライアント 23.8.1.5 以降のバージョンを使用することをお勧めします。

現在、Microsoft Edge ウェブビューはデフォルトで無効になっています。https://podio.com/webforms/28291989/2245437を使用してプレビューにサインアップできます。

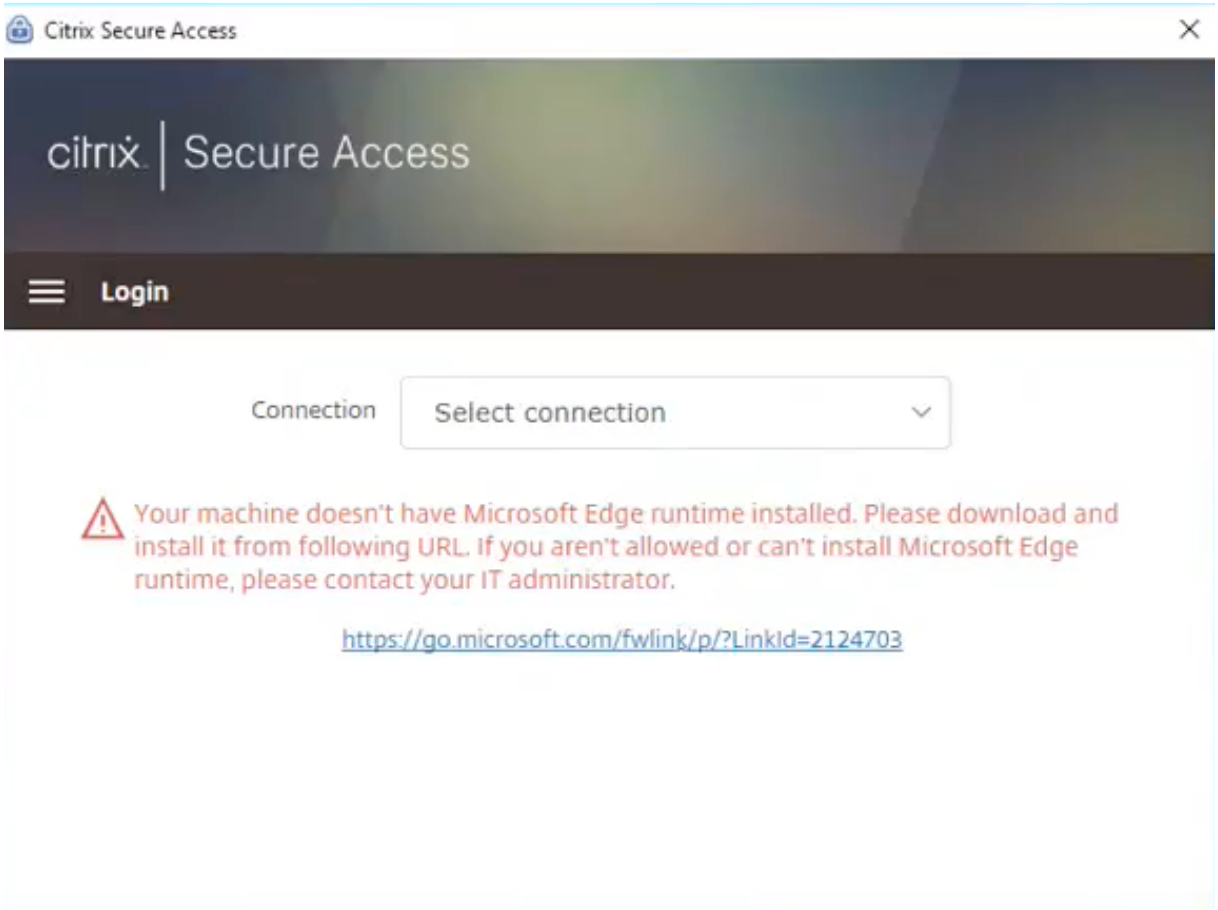
エンドユーザーへの変更

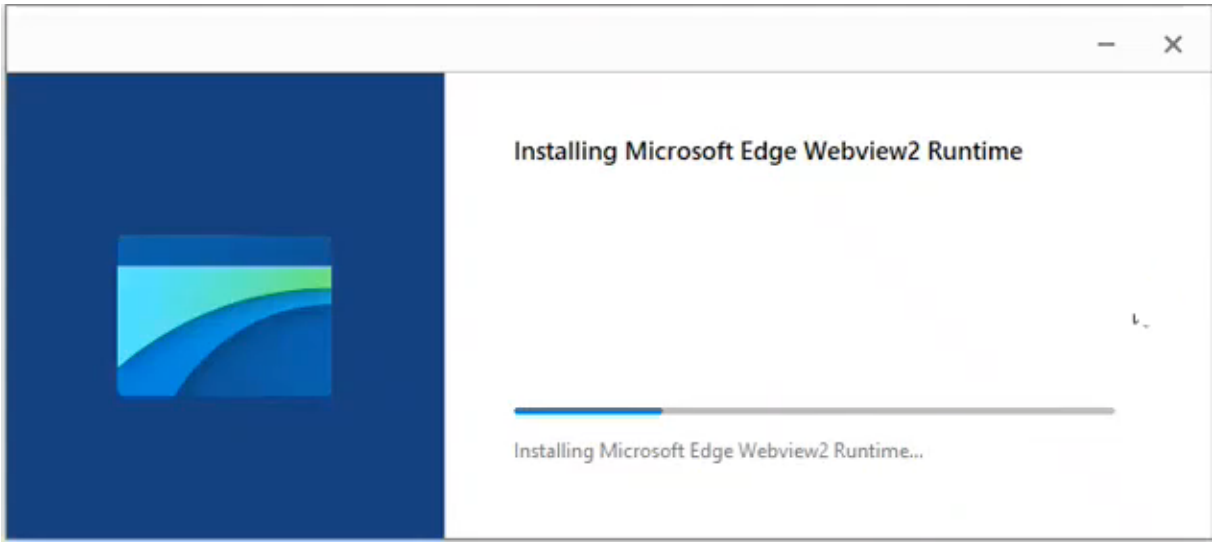
Citrix Secure Access クライアントユーザーインターフェイスの認証画面は次のように表示されます。



エンドユーザーが URL を選択すると、Citrix Secure Access クライアントは新しいウィンドウを開き、資格情報を使用して NetScaler Gateway にログオンするように求めます。

Windows クライアントマシンに Microsoft Edge WebView ランタイムがインストールされていない場合、エンドユーザーには、Microsoft Edge WebView ランタイムをダウンロードしてインストールするためのリンクが Citrix Secure Access クライアント UI に表示されます。エンドユーザーは VPN に接続すると、Edge WebView ランタイムをシームレスにダウンロードしてインストールでき、このプロセス中に認証が中断されることはありません。





メモ:

- Microsoft Edge WebView 機能は、管理者固有の構成には影響しません。
- Citrix Secure Access で Edge WebView を使用する場合は、HttpOnly Cookie 機能を有効にすることをお勧めします。これにより、EPA を nfactor フローの要素として使用する場合の NetScaler

> Gateway のログオン時間が短縮されます。

トラブルシューティング

- この機能で問題が発生した場合は、Citrix サポートにお問い合わせください。
- < citrixgatewaybetafeedback@cloud.com >Edge WebView 機能に関するフィードバックは、を通じて送信できます。

Windows クライアントのログ収集が改善されました

April 1, 2024

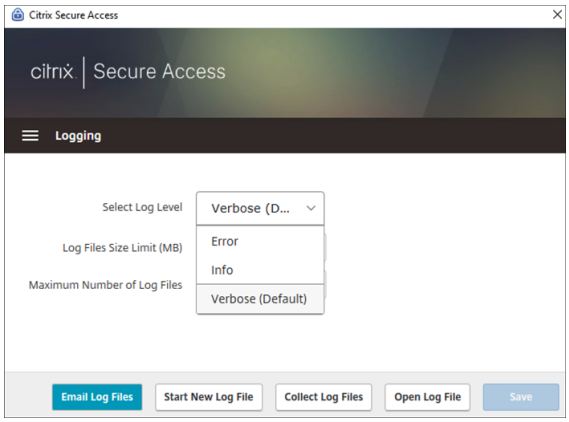
Windows Secure Access クライアントのロギング機能が強化され、ログの収集とデバッグが強化されました。新しいログファイルの先頭には「csa_」が付きます。

Windows 23.10.1.7 向け Citrix Secure Access クライアント以降、ログ収集とトラブルシューティングを強化するため、デフォルトのログレベルは Verbose に設定されています。

これらの変更により、管理者とエンドユーザーは現在のセッションと過去のセッションからログを収集できます。以前は、ログの収集は現在のセッションのみに制限されていました。

Citrix Secure Access クライアントユーザーインターフェイスを使用してログを構成する

1. Windows 用 Secure Access クライアントをインストールします。
2. メニューから [ロギング] をクリックします。ログに関するすべての設定は、ロギング画面で行うことができます。



- ログレベルの選択**:**

  新しいロギングメカニズムを有効にすると、次の 3 つのログレベルを使用できます。

  - エラー: アプリケーションによって報告された例外または障害のみがログに記録されます。
  - 情報: このレベルには、プログラムの実行に関連する情報メッセージとイベントが含まれます。エラーや例外も含まれます。
  - Verbose (デフォルト): このレベルには、Error および Info ログレベルで報告されたすべてのログメッセージと、トラブルシューティングに役立つ可能性のあるその他のメッセージが含まれます。

- ログファイルのサイズ制限**:** (必須) 各ログファイルのログファイルサイズを入力します。最大値は 600 MB です。
- ログファイルの最大数**:** (必須) ログ収集用に追加するファイルの数を入力します。最大値は 5 です。
- メールログファイル—登録した電子メール ID にログファイルを電子メールで送信します。
- 新しいログファイルを開始—このオプションを選択すると、新しいログファイルが作成されます。
- ログファイルの収集—クリックすると、アプリケーションのすべてのログファイルを含む zip ファイルが作成されます。この zip ファイルはクライアントのデスクトップに保存されます。
- ログファイルを開く—このオプションを選択すると、最新の`csa_nssslvpn*.txt`ファイルが開きます。

Linux 向け Citrix Secure Access クライアント

April 1, 2024

Linux 向け Citrix Secure Access クライアントは、NetScaler Gateway が管理する VPN クライアントソフトウェアで、ユーザーは企業のデータやアプリケーションにリモートでアクセスできます。Citrix Secure Access クライアントは、不正アクセス、アプリケーションレベルの脅威、およびブラウザベースの攻撃からアプリケーションを保護します。

Citrix End Point Analysis（EPA）クライアントは、NetScaler Gateway によって管理されるクライアントソフトウェアです。NetScaler Gateway 経由での企業データへのアクセスを許可する前に、エンドポイント基準をチェックします。Citrix EPA クライアントと Citrix Secure Access クライアントは相互に独立しています。

> 注:
>
> EPA を使用しない場合でも、後で EPA 機能を使用する場合に備えて、EPA と VPN の両方のプラグインバイナリを同時に更新することをお勧めします。

サポートされている Linux バージョン

Citrix Secure Access クライアントと Citrix EPA クライアントは、Ubuntu 18.04、Ubuntu 20.04、および Ubuntu 22.04 バージョンと互換性があります。サポートされているブラウザの詳細については、「クライアントソフトウェア要件」を参照してください。

> 注:
>
> Ubuntu 22.04 を Citrix Secure Access クライアントおよび Citrix EPA クライアントと連携させるには、NetScaler CLI で SSL パラメータdenySSLRenegをNONSECUREに設定します。

サポートされる機能

Ubuntu 向け Citrix Secure Access クライアントは、以下の機能をサポートしています。

- 分割トンネリングとリバース分割トンネリング
- TCP、UDP、および ICMP アプリケーションのトンネリング
- イントラネット IP (IIP) 経由のサーバー起動接続
- スプリット DNS リモート
- クライアント側のプロキシ
- 従来の EPA スキャン
- 高度な EPA スキャンを含む高度な認証 (nFactor) (ブラウザからのみ)
- HTTP のみのクッキー
- 広域サーバー負荷分散（Global Server Load Balancing：GSLB）

> 注:
>
> スプリット DNS BOTH は Ubuntu 用 Citrix Secure Access クライアントではサポートされていません。

NetScaler Gateway での **Ubuntu** クライアントのアップグレード

Ubuntu 用の Citrix Secure Access クライアントと Citrix EPA クライアントは、ダウンロードページからダウンロードできます。

Citrix Secure Access クライアントと Citrix EPA クライアントには、それぞれ「nsgclient18_64.deb」と「nsepa18.deb」という名前が付けられています。クライアントは Ubuntu 18.04 と 20.04 の両方に対応しています。

Ubuntu 22.04 をサポートする Citrix Secure Access クライアントと Citrix EPA クライアントには、それぞれ「nsginstaller64.deb」と「nsepa.deb」という名前が付けられています。

Citrix Secure Access クライアントの最新バージョンをバージョン 1.0.0.x からバージョン 23.6.1 にアップグレードする場合は、たとえば次のようにします。

1. シェルプロンプトを使用して、場所/var/netscaler/gui/vpn/scripts/linux/にある「nsgclient18_64.deb」と「nsginstaller64.deb」ファイルを置き換えます。
2. シェルプロンプトを使用して、場所/var/netscaler/gui/epa/scripts/linux/にある「nsepa18.deb」と「nsepa.deb」ファイルを置き換えます。

3. /var/netscaler/gui/vpn/scripts/linux/clientversions.xmlファイルを開きます。

   a) Citrix EPA クライアントの場合は、次の XML タグの現在のバージョン (1.0.0.x) を最新バージョン (23.6.1) に置き換えます。XML タグが存在しない場合は、それらを XML ファイルに追加します。例:

   変更前

   ```
   <component pkgname="nsepa18"currentversion="1.0.0.x"minversion
   ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
   ="100"updatetype="compatible"action="/epa/scripts/linux/
   nsepa18.deb"/>
   ```

   変更後

   ```
   <component pkgname="nsepa18"currentversion="23.6.1"minversion
   ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
   ="100"updatetype="compatible"action="/epa/scripts/linux/
   nsepa18.deb"/>
   ```

   変更前

   ```
   <component pkgname="nsepa22"currentversion="1.0.0.x"minversion
   ="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion
   ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
   .deb"/>
   ```

   変更後

   ```
   <component pkgname="nsepa22"currentversion="23.6.1"minversion
   ="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion
   ="100"updatetype="compatible"action="/epa/scripts/linux/nsepa
   .deb"/>
   ```

   b) Citrix Secure Access クライアントの場合は、次の XML タグ内の現在のバージョン (1.0.0.x) を最新バージョン (23.6.1) に置き換えてください。XML タグが存在しない場合は、それらを XML ファイルに追加します。例:

   変更前

   ```
   <component pkgname="nsgclient18"currentversion="1.0.0.x"
   minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
   "maxkernelversion="5.16"updatetype="compatible"action="/vpn/
   scripts/linux/nsgclient18_64.deb"/>
   ```

   変更後

   ```
   <component pkgname="nsgclient18"currentversion="23.6.1"minversion
   ="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
   ```



```
="5.16"updatetype="compatible"action="/vpn/scripts/linux/
nsgclient18_64.deb"/>
```

および

```
<component pkgname="nsgclient22"currentversion="1.0.0.x"
minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0
"maxkernelversion="5.20"updatetype="compatible"action="/vpn/
scripts/linux/nsginstaller64.deb"/>
```

変更後

```
<component pkgname="nsgclient22"currentversion="23.6.1"minversion
="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion
="5.20"updatetype="compatible"action="/vpn/scripts/linux/
nsginstaller64.deb"/>
```

4. NetScaler シェルプロンプトで、次のコマンドを実行します。

```
rm -rf /netscaler/ns_gui
ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. NetScaler CLI で、以下のコマンドを実行します。

```
set vpn parameter -clientversions all
flush cache contentgroup loginstaticobjects
```

参照ドキュメント

- NetScaler Gateway VPN クライアントとサポートされる機能
- Ubuntu でサポートされるエンドポイント分析スキャン
- エンドユーザー向けヘルプドキュメント

Linux 向け Citrix Secure Access リリースノート

April 1, 2024

Linux 向け Citrix Secure Access クライアントと Citrix End Point Analysis（EPA）クライアントは現在、スタンドアロンベースでリリースされており、すべての NetScaler バージョンと互換性があります。Citrix Secure Access クライアントバージョンは、YY.MM リリース. ビルドの形式に従います。

リリースノートには、新機能、既存機能の強化、解決された問題、既知の問題が記載されています。

新機能: 現在のリリースで利用可能な新機能と機能強化。

修正された問題: 現在のリリースで修正された問題。

既知の問題: 現在のリリースに存在する問題とその回避策 (該当する場合)。

サポートされる機能について詳しくは、NetScaler Gateway 製品ドキュメントを参照してください。

23.10.3 (2023 年 10 月 16 日)

解決された問題

フランスのユーザーの場合、Citrix Secure Access for Linux ユーザーインターフェイスの［接続］ページには、データ転送速度がそれぞれ KB 単位と Mo 単位ではなく、KB 単位と MB 単位で表示されます。

[NSOSLX-177]

23.9.1 (2023 年 9 月 8 日)

新機能

このリリースでは問題に対応しているため、パフォーマンスや安定性が総合的に向上しています。

[CGOP-25231]

23.6.2 (2023 年 6 月 20 日)

新機能

- **Ubuntu 22.04** の **Citrix Secure Access** クライアントと **Citrix EPA** クライアントのサポート

  Ubuntu 22.04 は、Ubuntu の最新の長期サポートリリースです。Citrix Secure Access と Citrix EPA クライアントは Ubuntu 22.04 と互換性があります。詳しくは、「クライアントソフトウェア要件」を参照してください。

  [CGOP-24312]

- **Citrix Secure Access** および **Citrix EPA** クライアントの **GSLB** サポート

  Ubuntu 向け Citrix Secure Access クライアントと Citrix EPA クライアントは、NetScaler Gateway のグローバルサーバー負荷分散（GSLB）機能をサポートしています。NetScaler Gateway の GSLB を構成することで、管理者はエンドユーザーがどこからでもエンタープライズネットワーク（イントラネットリソース）を常に利用できるようにすることができます。GSLB は、あるデータセンターのユーザーが別のデータセンターにリダイレクトされるような災害状況やネットワーク障害にも対処します。詳しくは、「NetScaler Gateway でのアクティブ-アクティブ GSLB 展開のサポート」を参照してください。

  [CGOP-23506]

- **Citrix Secure Access** および **Citrix EPA** クライアントの **HTTP** のみのサポート

  Citrix Secure Access クライアントと Citrix EPA クライアントは、認証クッキーの HttpOnly フラグをサポートしています。NetScaler Gateway の管理者は、Web アプリケーションによって生成される認証クッキーに HTTPOnly 機能を構成します。この機能は、クロスサイトスクリプティングによる Cookie の盗難を防ぐのに役立ちます。詳細については、「認証クッキーに HttpOnly フラグを適用する」を参照してください。

  [CGOP-23517]