

Androidデバイス用Citrix Secure Accessクライアント

Android用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。これにより、いつでもどこからでも、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、および企業データに安全にアクセスできます。

注記：

- リリース23.12.1以降、Android用Citrix SSOはCitrix Secure Accessに名称変更されました。この名称変更を反映するため、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。
- Android用Citrix Secure Accessに関する管理者向けの手順については、[Androidデバイス用Citrix Secure Access](#)を参照してください。

AndroidデバイスからCitrix Secure Accessを使用する方法

PlayストアからCitrix Secure Accessをインストールします。初回ユーザーは、非MDMの場合にサーバーを追加してNetScaler Gatewayへの接続を作成する必要があります。それ以降の使用では、既存の接続に接続するか、新しい接続を追加できます。また、MDM展開で管理者が許可している場合は、既存の接続を編集することもできます。ログを表示し、それに応じて適切なアクションを実行することもできます。

注記:

- MDMを介して展開された接続は編集できません。
- Citrix Secure Accessアプリに[Query all packages](#)の同意を付与するよう求められる場合があります。同意が付与されると、Citrix Secure Accessアプリは次のようになります。

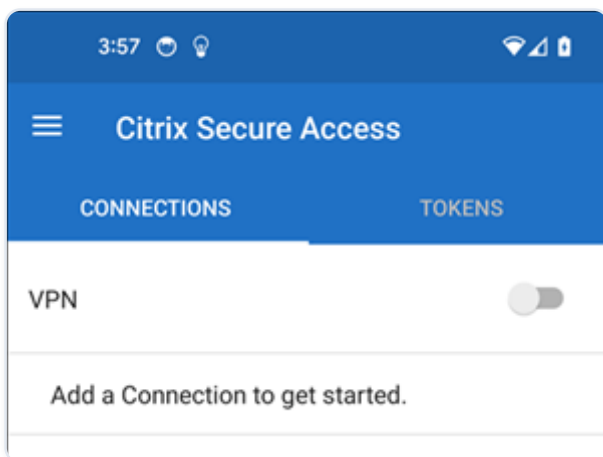
- 。オペレーティングシステムからパッケージインストール通知を受け取ります。
- 。Always On VPNを再起動します。

VPNプロファイルに初めて接続するときに、インストールされているパッケージに関する情報を収集するための同意（Googleポリシーで義務付けられています）を提供するよう求められます。同意を付与すると、VPN接続が開始されます。同意を拒否すると、VPN接続は中止されます。同意が付与されると、同意画面は再表示されません。

接続を追加

注: この手順は、非MDMの場合にのみ必要です。

Citrix Secure Accessをインストールし、Androidデバイスでアプリを開くと、次の画面が表示されます。



1. 接続を追加するには、**+**をクリックします。
2. ベースURL（例：[My company](#)）とVPN接続の名前を入力します。オプションで、ユーザー名を入力できます。
3. **保存**をクリックし、必要に応じて**保存して接続**または**保存のみ**をクリックします。

接続を保存または接続する(/en-us/citrix-sso/media/sso-andr-save-connect3.jpg)

4. サーバーの認証情報を入力し、キーパッドで**LOG IN**または**Done**をタップします。

認証情報を入力する(/en-us/citrix-sso/media/sso-andr-login4.jpg)

接続要求メッセージが表示されます。**OK**をクリックします。

注: このメッセージは、Citrix Secure AccessによってVPN接続が初めて確立された場合にのみ表示されます。ユーザーが初めて接続を許可した場合、このメッセージは、ユーザーがアプリをアンインストールして再インストールするまで再び表示されません。

接続要求確認メッセージ(/en-us/citrix-ssso/media/ssso-andr-con-req5.png)

注: Citrix Secure Accessからログアウトするには、**VPNスイッチ**をオフにします。

VPNスイッチを使用してログアウトする(/en-us/citrix-ssso/media/ssso-andr-con-req5a.png)

既存の接続を変更または削除する

Citrix Secure Accessからログアウトした後、接続を編集または削除できます。

サーバー名を長押しし、**Edit Connection**または**Delete Connection**を選択します。

接続を編集または削除する(/en-us/citrix-ssso/media/ssso-andr-del-con.png)

VPN接続の失敗後にNetScaler Gatewayに再接続する - プレビュー

VPN接続が失われた場合、Android用Citrix Secure AccessクライアントはNetScaler Gatewayでの再認証を促します。NetScaler Gatewayへの接続が失われ、接続を再開するために再認証が必要であることを示す通知が、AndroidデバイスのUIおよび通知パネルに表示されます。

注:

この機能はプレビュー版です。

NetScaler Gateway で再認証する(/en-us/citrix-ssso/media/reconnect-to-gateway-android.png)

Android 17 以降でローカルネットワークアクセス権限を許可する

Citrix Secure Access for Android リリース 26.08.1 以降、Android 17 以降でアプリケーションをインストール、再インストール、または更新するユーザーは、ローカルネットワークアクセスを許可するように求められます。アクセスが拒否された場合、VPNセッション開始時にWi-Fiプリンターなどの特定のローカルネットワークサービスが利用できなくなる可能性があります。

MDM管理者は、この権限をCitrix Secure Accessアプリケーションに事前に付与することをお勧めします。

Android 13 以降で通知を受信またはブロックする

Citrix Secure Access for Android リリース 23.12.1 以降、Android 13 以降でアプリケーションをインストール、再インストール、または更新するユーザーは、通知を許可するように求められます。

通知が拒否された場合、ユーザーはCitrix Secure AccessからのVPNステータスまたはプッシュ通知を受信しません。

Androidデバイスで**設定 > 通知**に移動して、通知権限を変更できます。

次の例では、VPNステータス通知が無効になっています。

Android 13 の通知(/en-us/citrix-sso/media/android-13-notifications.png)

信頼できないサーバーをブロックする

Citrix Secure Accessは、デフォルトでは信頼できないサーバーに接続しません。信頼できないサーバーとは、自己署名証明書を使用しているサーバー、またはゲートウェイの信頼されたルート証明書を持っていないサーバーを指します。これらの種類の接続を許可するには、**信頼できないサーバーをブロック**スイッチをオフにすることができます。

信頼できないサーバーをブロックする(/en-us/citrix-sso/media/sso-andr-block.png)

デバッグログを有効にする

デバッグログの取得は、トラブルシューティングやCitrixサポートへの問題報告において重要な部分です。Citrix Secure Accessのデバッグログを有効にするには、**デバッグログ**スイッチを**オン**にタップします。接続の問題をトラブルシューティングする際に、**ログをメールで送信**リンクを使用してログをメールで送信できます。

デバッグログを表示(/en-us/citrix-sso/media/sso-andr-logs.png)

統計を表示

VPNが接続されている場合、接続統計を表示できます。

接続統計を表示(/en-us/citrix-sso/media/sso-andr-stats.png)

パスワードトークン

6桁のパスワードトークンを2要素認証として追加できます。このコードは、時間ベースのワンタイムパスワードプロトコルを使用してOTPコードを生成します。

パスワードトークンは手動で追加するか、QRコードスキャン方式を使用して登録できます。トークンを手動で入力することを選択した場合、プッシュ通知を使用した2要素認証は有効になりません。

パスワードトークンを登録する

1. デスクトップまたはラップトップのWebブラウザで、組織のワンタイムPIN管理ページにログインします。
2. をクリックします。
3. デバイスの名前を入力し、 をクリックします。

QRコードが生成されます。

ブラウザでQRコードをスキャンしてパスワードトークンを追加する

1. ビューの タブに移動します。
2. + をタップし、 をタップします。
3. ブラウザのQRコードにカメラを向けます。

Citrix Secure Accessは、デバイス名とシークレットキーを自動入力します。

または、QRコードの上に表示されているシークレットキーを手動で入力することもできます。

Citrix Secure AccessはQRコードを検証し、プッシュ通知のためにゲートウェイに登録します。登録プロセスでエラーがなければ、トークンはトークンタブに正常に追加されます。

注:

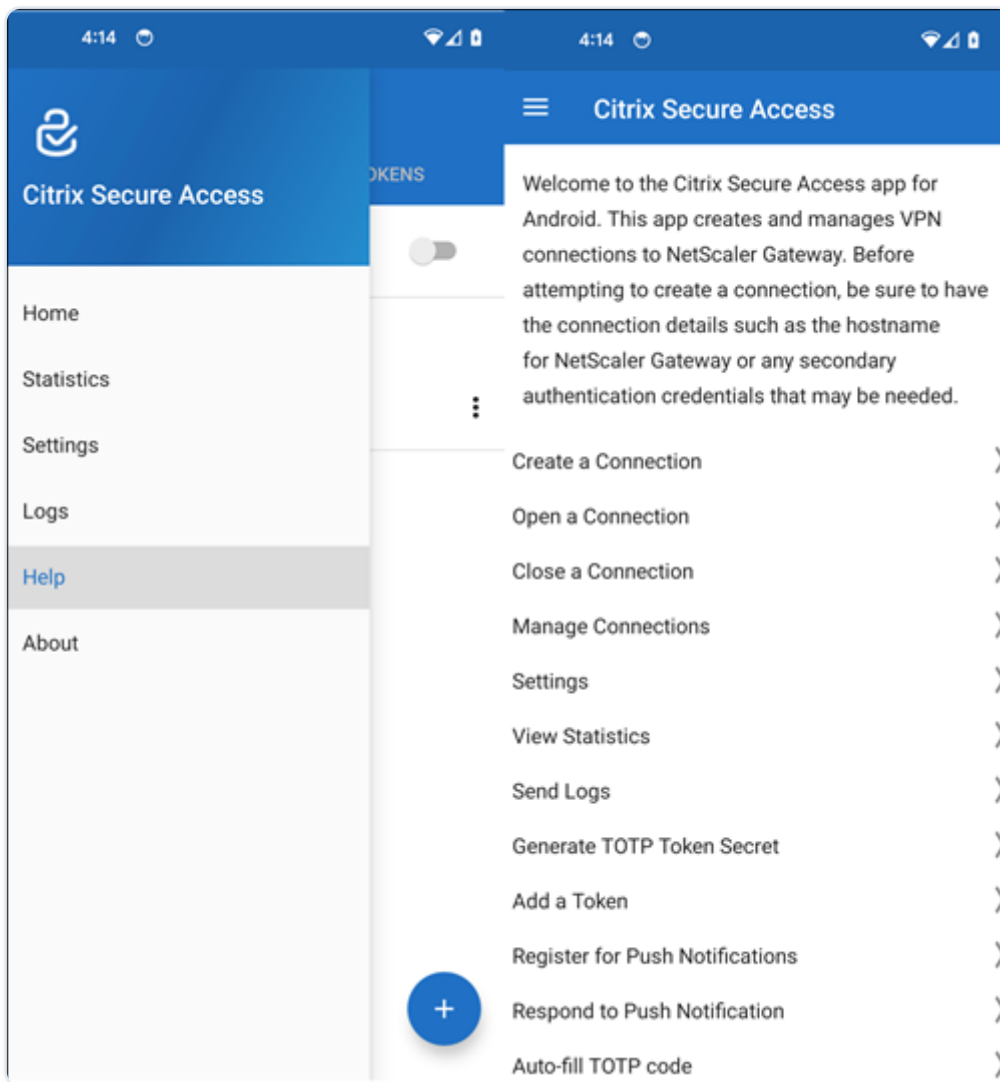
- Citrix Secure AccessがQRコードをキャプチャするには、カメラの許可を付与する必要があります。
- デバイスでデバイスのPIN/パスワードを有効にする必要があります。

パスワードトークンを手動で追加する

1. ホームビューのトークンタブに移動します。
2. + をタップし、**手動で入力**をタップします。
3. ブラウザで生成されたパスワードトークンに表示されているデバイス名とシークレットキーを入力します。

ヘルプトピック

Citrix Secure Accessの使用方法の詳細については、**ヘルプ**を参照してください。



Intune環境で構成されたCitrix Secure Accessを使用して企業ネットワークに接続する

注:

Android版Citrix Secure Accessの管理者向け手順については、「[Androidデバイス用Citrix Secure Access](#)」を参照してください。

このトピックでは、Microsoft Intune Android Enterprise環境で構成されたCitrix Secure Accessクライアントを使用して企業ネットワークに接続する方法について詳しく説明します。

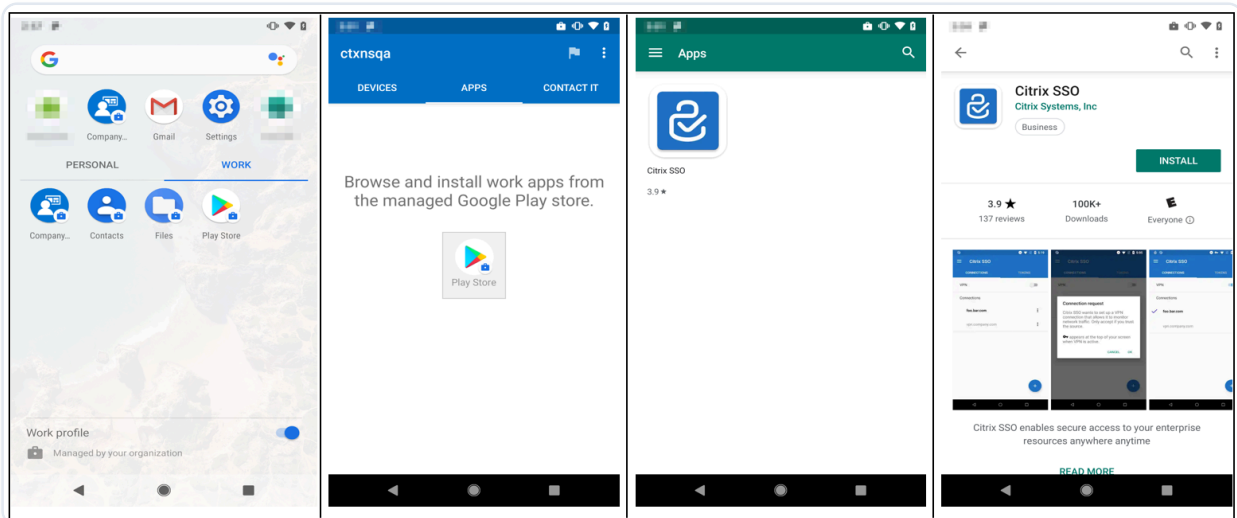
前提条件:

- Intune Company Portalアプリを使用して、デバイスをIntuneに登録していること。

- ユーザーの仕事用プロファイルがデバイスに設定されていること。

1. 仕事用プロファイルからデバイスで**Intune Company Portal**アプリを開きます。
2. 3点メニューをクリックしてアプリの設定を開き、画面の一番下までスクロールします。**SYNC**をタップしてIntuneサーバーと同期し、メインアプリ画面に移動します。
3. **APPS**タブをタップし、**Managed Google Play Store**リンクをタップします。

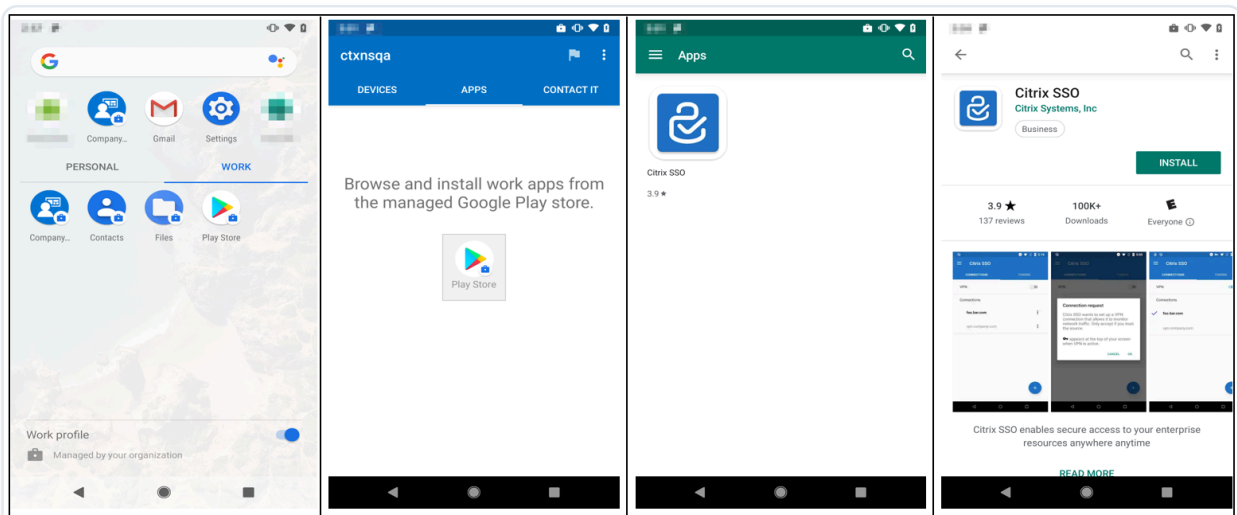
ユーザーに承認されたアプリのリストが表示されます。



4. **Citrix Secure Access**をタップします。

Managed Google PlayストアにCitrix Secure Accessクライアントが表示されます。

5. **インストール**をタップします。
6. 仕事用プロファイルアプリのリストに戻ります。Citrix Secure Access がインストール済みアプリのリストに追加されます。
7. **WORK** プロファイルアプリリストの Citrix Secure Access アイコンをタップして開きます。



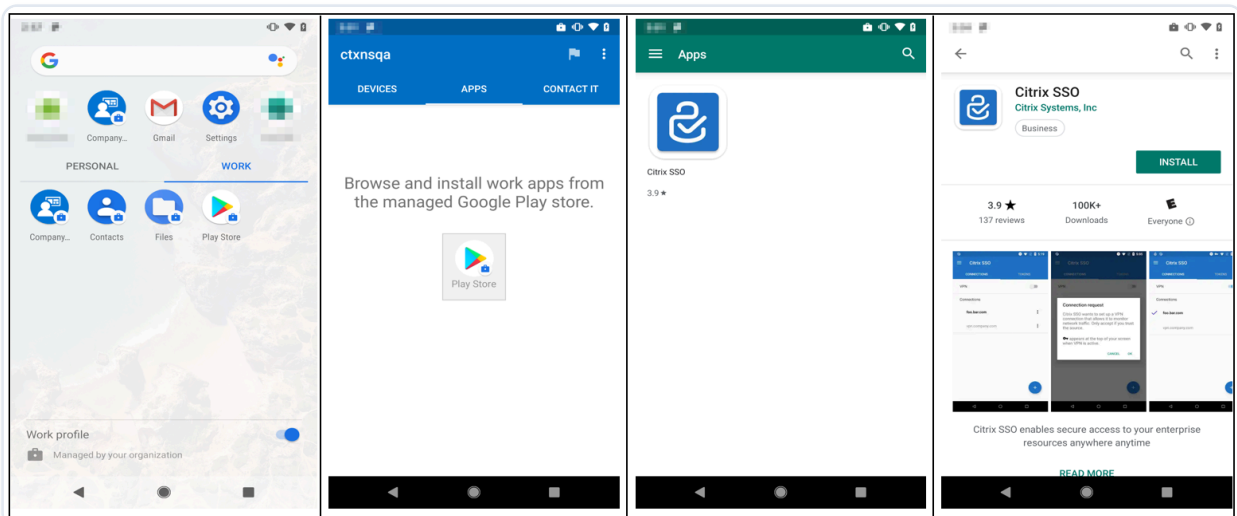
Citrix Secure Access が開きます。会社の内部ネットワークと安全に通信するための権限を許可または拒否するよう求められます。

8. **ALLOW** をタップして権限を付与します。**DON'T ALLOW** を選択した場合、Citrix Secure Access は閉じ、Citrix Secure Access クライアントを使用できません。

注:

電話の発信と管理の権限を許可または拒否するよう求められる場合があります (Intune 経由でまだ付与されていない場合)。**Allow** をタップして権限を付与します。この権限を拒否することもできますが、NetScaler Gateway でのデバイス認証に Intune NAC チェックが必要な場合、この権限を付与するまで会社の内部ネットワークに接続できません。

9. **CONNECTIONS** タブの「管理対象接続」セクションに、**My Corporate VPN** (または Intune の Citrix Secure Access 構成で選択した名前) が表示されます。この接続をタップすると、NetScaler Gateway で認証するための資格情報の入力を求められます。
10. NetScaler Gateway で認証するための資格情報を入力し、**LOG IN** をタップします。



NetScaler Gateway でクライアント証明書認証が構成されている場合、証明書の選択を求められることがあります。証明書へのアクセスを許可できます。

11. Android システムから VPN トンネル設定のための**接続要求**を許可するよう求められます。**OK** をタップして、Citrix Secure Access が会社の内部ネットワークとの安全な接続を確立する権限を付与します。

注: このプロンプトは、NetScaler Gateway への安全な接続を初めて確立するときのみ表示されます。Citrix Secure Access がアンインストールされてからデバイスに再インストールされるまで、その後の接続試行では表示されません。

会社の内部ネットワークに接続されました。デバイスのステータスバーに鍵のアイコンが表示され、VPN 接続がアクティブであることを通知します。Citrix Secure Access クライアントの VPN サービス通知アイコンもステータスバーに表示されます。接続スイッチの状態は「接続済み」に変わり、VPN プロファイル名の横にチェックマークアイコンが表示されます。

iOSデバイス用Citrix Secure Accessクライアント

iOS用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。これにより、いつでもどこからでも、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、および企業データに安全にアクセスできます。

Citrix Secure Accessアプリは、iOSで完全なモバイルデバイス管理（MDM）サポートを提供します。MDMサーバーを使用すると、管理者はデバイスレベルのVPNプロファイルとアプリごとのVPNプロファイルをリモートで構成および管理できます。

重要：

- リリース23.11.1以降、Citrix SSO for iOSはCitrix Secure Accessに名称変更されました。この名称変更を反映するため、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用Citrix Secure Accessに関する管理者向けの手順については、「[iOS用Citrix SSOおよびmacOS用Citrix Secure Access](#)」を参照してください。

Citrix Secure Accessアプリでの証明書のインポートとインストール

iOS版Citrix Secure Accessは、NetScaler Gatewayでのクライアント証明書認証をサポートしています。証明書は、以下の方法でCitrix Secure Accessに配信できます。

- **MDMサーバー** - MDMのお客様に推奨されるアプローチです。証明書はMDM管理のVPNプロファイルに直接構成されます。その後、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を参照してください。

- **メール** - MDMを使用しないお客様向けの唯一のアプローチです。管理者は、ユーザー証明書ID（証明書と秘密鍵）をPKCS#12ファイルとして添付したメールをユーザーに送信します。ユーザーは、添付ファイル付きのメールを受信するために、iOSデバイスにメールアカウントを設定する必要があります。その後、このファイルをiOS版Citrix Secure Accessにインポートできます。

注:

ファイル名拡張子 `.pfx` および `.p12` はiOSシステムによって占有されており、Citrix Secure Accessのようなサードパーティアプリでは使用できません。そのため、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、それぞれ `.citrixsso-pfx` または `.citrixsso-p12` に変更する必要があります。

1. ユーザー証明書ID（証明書と秘密鍵）がPKCS#12ファイルとして添付されているメールを開きます。

- 添付ファイルをタップして、システムの **OpenIn** メニューを表示します。
- **Citrix SSOにコピー** をタップします。

ユーザー証明書IDの添付ファイルがあるメールを開きます。(/en-us/citrix-sso/media/sso-ios-email.png)

2. Citrix Secure Accessに証明書をインストールします。

アプリが起動し、証明書のパスフレーズのプロンプトが表示されます。証明書をアプリのキーチェーンにインストールするために正しいパスフレーズを入力し、**インポート** をクリックします。

検証が成功すると、証明書がインポートされます。

検証成功後にSecure Accessにインポートされた証明書(/en-us/citrix-sso/media/sso-ios-install.png)

3. VPNで証明書ベースの認証を使用します。

- VPN認証に証明書を使用するには、まずCitrix Secure AccessでVPN構成またはプロファイルを作成する必要があります。
 - **VPN接続ビュー**に移動し、**VPN構成の追加**をタップします。

- 。VPNプロファイルの構成ビューで、**証明書**セクションでインポートされた証明書を選択できます。

VPN構成またはプロファイルの追加(/en-us/citrix-ssso/media/ssso-ios-certificate1.png)

- 証明書をインポートするには、**保存**をタップします。

証明書が正常にインポートされました(/en-us/citrix-ssso/media/ssso-ios-certificate2.png)

4. 証明書を管理します。

Citrix Secure Accessにインポートされた証明書を管理するには、**メインメニューの証明書タブ**に移動します。

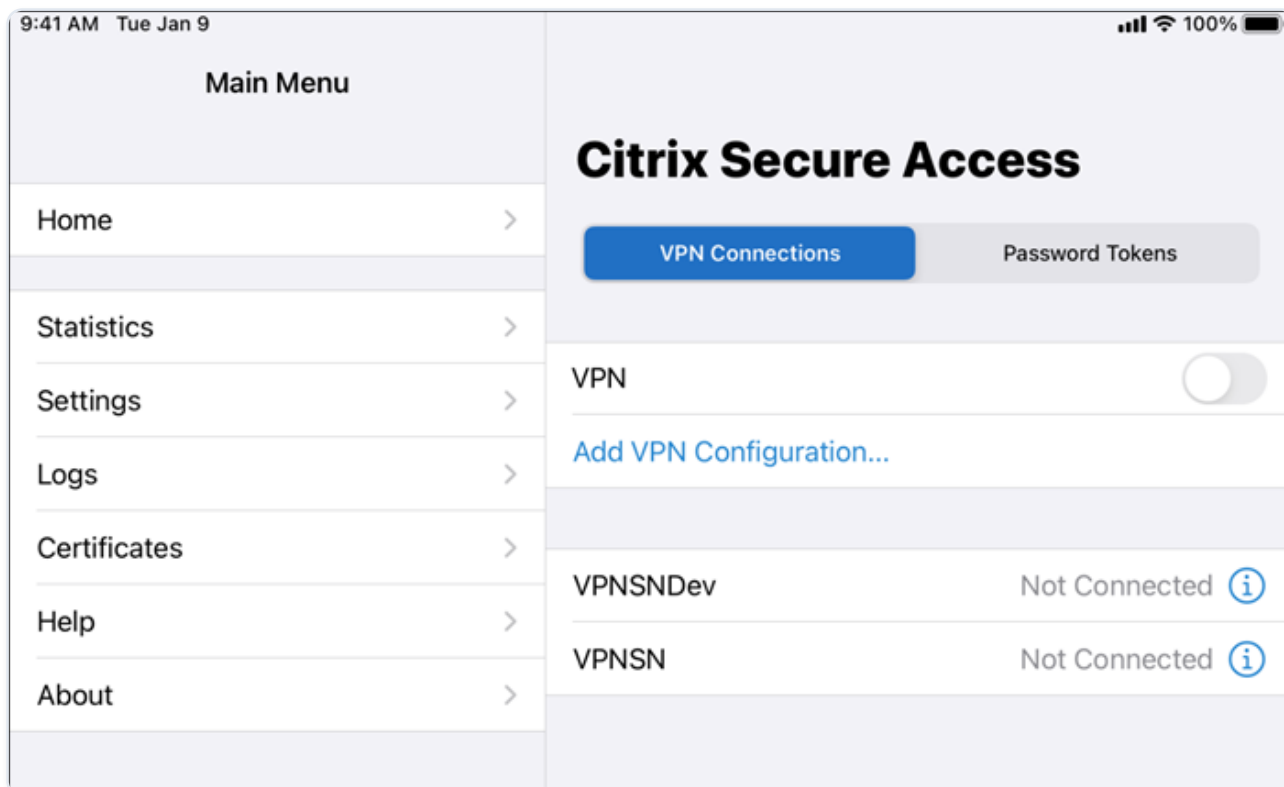
iOSデバイスからCitrix Secure Accessを使用する方法

App StoreからCitrix Secure Accessアプリをインストールします。アプリのインストール後、初回はサーバーを追加してNetScaler Gatewayへの接続を作成する必要があります。2回目以降は、既存の接続に接続したり、新しい接続を追加したり、既存の接続を編集したりできます。ログを表示して、それに応じて適切なアクションを実行することもできます。

MDMのお客様の場合、デバイスを登録すると、管理者が事前に構成したVPN接続が自動的に表示されることがあります。接続を選択し、VPNスイッチをオンにすることで、直接接続を開始できます。これらのVPN接続は、ユーザーが編集することはできません。

接続を追加する

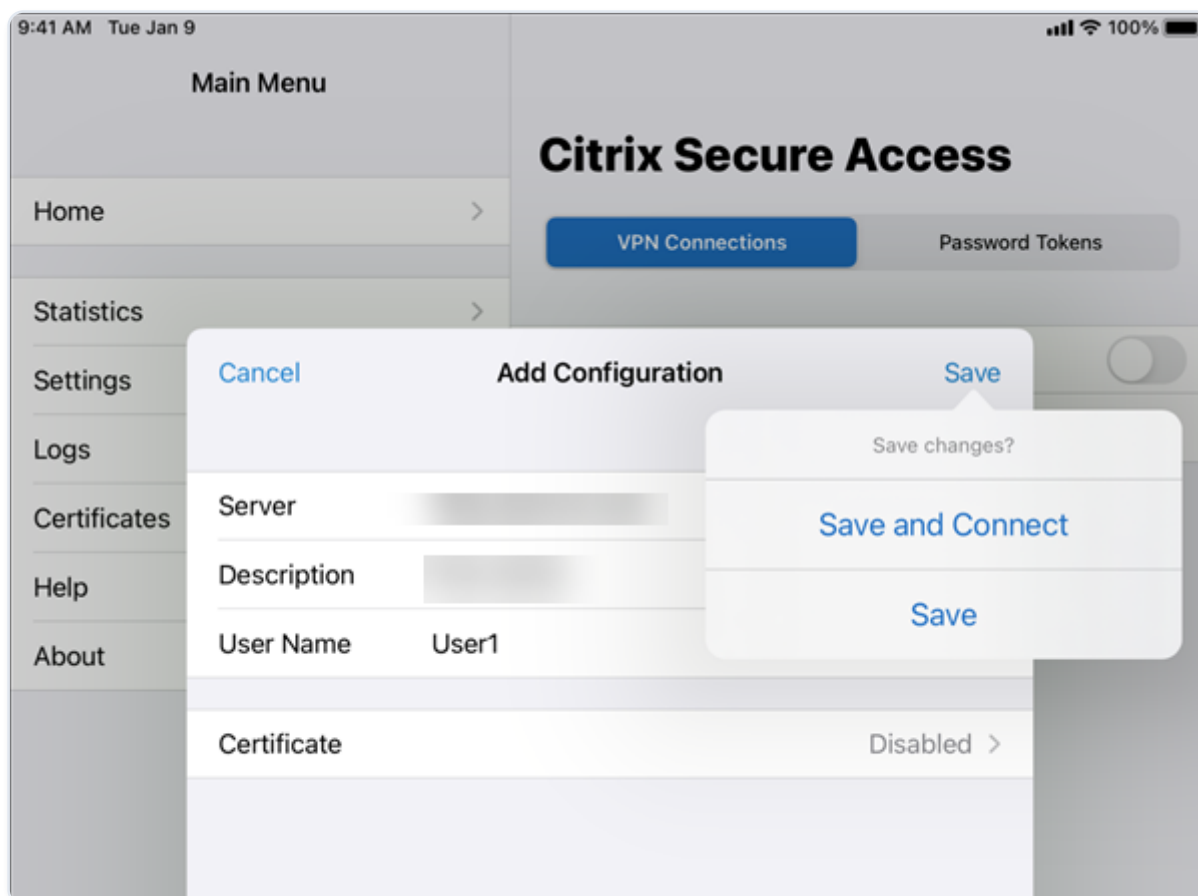
Citrix Secure Accessをインストールしてアプリを開くと、次の画面が表示されます。



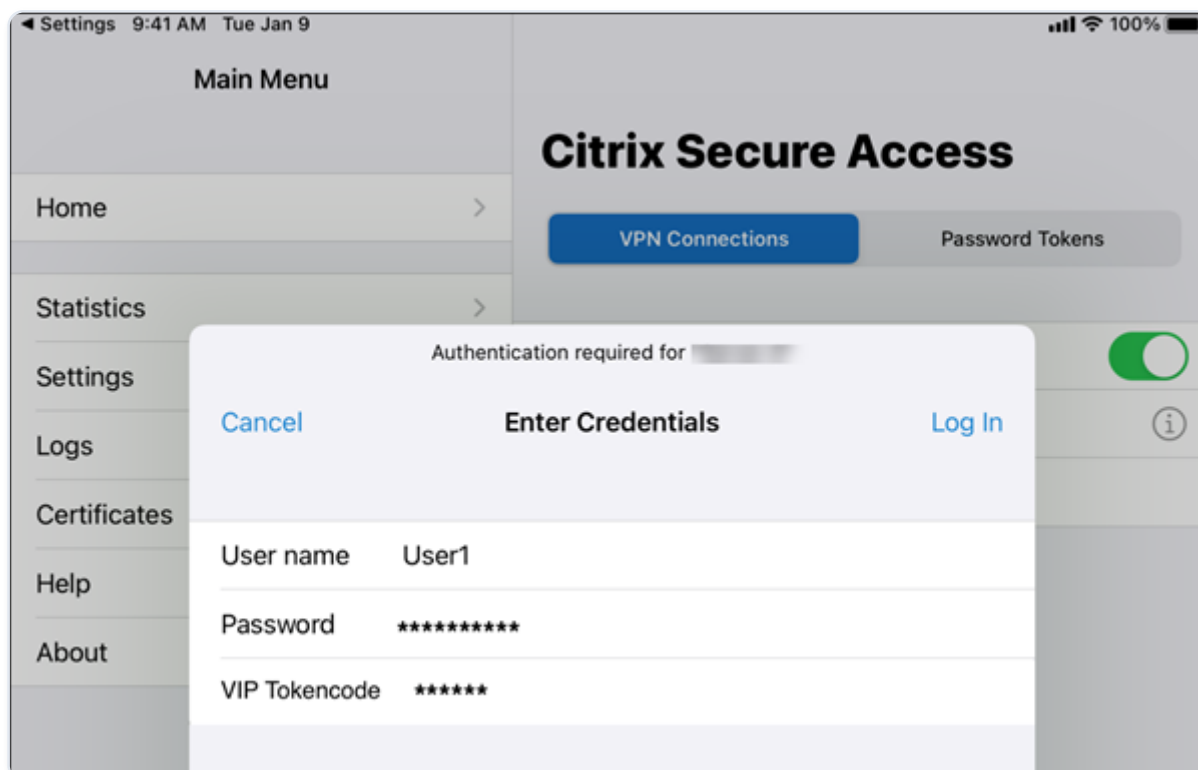
1. 新しい接続を追加するには、**VPN構成を追加**をタップします。
2. サーバーの詳細を入力します。

オプションでユーザー名を追加することもできます。

3. **保存**をタップし、必要に応じて**保存して接続**または**保存**をタップします。



4. サーバーの認証情報を入力し、ログインをタップします。



注: Citrix Secure Accessからログアウトするには、VPNをオフにします。

VPN接続の失敗後にNetScaler Gatewayに再接続する

iOS版Citrix Secure Accessアプリは、VPN接続が失われたときにNetScaler Gatewayでの再認証を促します。NetScaler Gatewayへの接続が失われたこと、および接続を再開するには再認証が必要であることがUIに通知されます。

既存の接続を削除する

接続の横にあるアイコンをタップし、 をタップします。

既存の接続を削除する(/en-us/citrix-sso/media/sso-ios-delete.png)

接続を切断する

VPNスイッチをオフに切り替えてから、 をタップします。

接続を切断する(/en-us/citrix-sso/media/sso-ios-disconnect.png)

統計を表示する

VPNが接続されているときに、接続統計を表示できます。

統計を表示する(/en-us/citrix-sso/media/sso-ios-stats.png)

信頼されていないサーバーをブロックする

Citrix SSOは、デフォルトでは信頼されていないサーバー（自己署名証明書を使用しているサーバー、またはゲートウェイの信頼されたルート証明書を持っていないサーバー）には接続しません。これらの種類の接続を許可するには、スイッチをオフにすることができます。

信頼されていないサーバーをブロックする(/en-us/citrix-sso/media/sso-ios-block.png)

ローカルLANアクセス

iOS版Citrix SSO 23.10.1は、VPN接続が確立された後、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かどうかを決定できるローカルLANアクセス機能をサポートしています。この機能は、管理者がNetScaler GatewayでローカルLANアクセス設定を構成している場合にのみ使用できます。

Citrix Secure Access UIでローカルLANアクセスを設定するには:

1. メインメニューに移動し、**設定**をクリックします。
2. **ローカルLANアクセスを許可**を有効にします。

統計ページでローカルLANアクセスのステータスを確認できます。

ログを送信

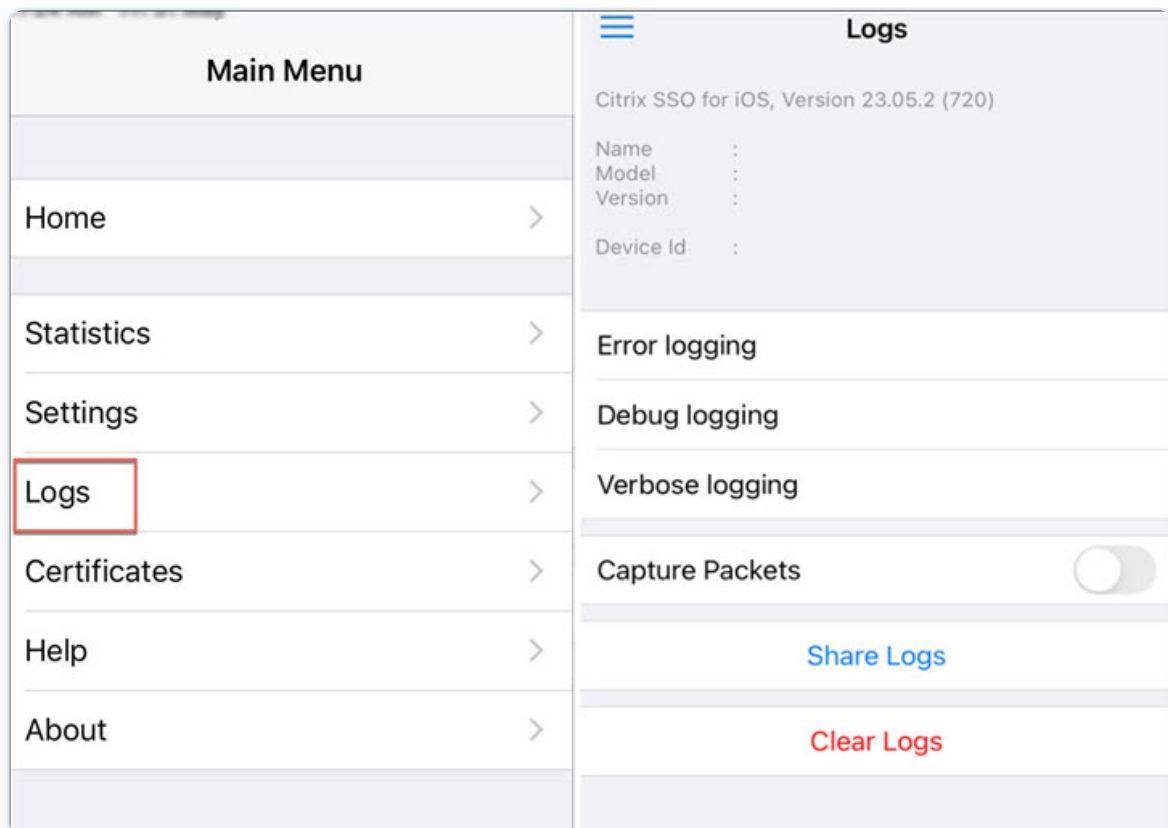
デバッグログの取得は、トラブルシューティングやCitrixサポートへの問題報告において重要な部分です。

デバッグログをキャプチャして共有する手順は次のとおりです。

1. デバッグログスイッチをオンに設定します。
2. メール、チャット、ファイルへの保存などのオプションを使用してログを共有します。

注:

- 新しいログセットを生成するには、まず**ログをクリア**を使用して古いログを削除します。
- リリース23.07.1以降、**ログをメールで送信**オプションは**ログを共有**オプションに置き換えられました。ログを共有すると、圧縮されたログファイルを共有するためのさまざまなオプションが提供されます。



クライアント証明書を表示

Citrix Secure Accessにインポートされたクライアント証明書を表示できます。インポートされた証明書は、**証明書**セクションに表示されます。次のいずれかの方法で証明書を削除できます。

- 「証明書」セルで、右から左にスライドジェスチャを実行して「**削除**」ボタンを表示します。次に、「**削除**」をタップします。
- 「**編集**」をタップして「**削除**」ボタンを表示し、次に「**削除**」をタップします。

証明書の表示または削除(/en-us/citrix-sso/media/sso-ios-certificates.png)

ヘルプトピック

さまざまな項目に関するヘルプについては、「**ヘルプ**」を参照してください。

ヘルプトピックの表示(/en-us/citrix-sso/media/sso-ios-help.png)

macOSデバイス用Citrix Secure Accessクライアント

Citrix Secure Accessアプリは、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。これにより、いつでもどこからでも、ビジネスに不可欠なアプリケーション、仮想デスクトップ、および企業データに安全にアクセスできます。Citrix Secure Accessアプリは、AppleのNetwork Extensionフレームワークを使用して構築された、NetScaler Gateway向けの次世代VPNクライアントです。App Storeの従来のCitrix VPNクライアントを置き換えるものです。

Citrix Secure Accessアプリは、macOSで完全なモバイルデバイス管理（MDM）をサポートします。MDMサーバーを使用すると、管理者はデバイスレベルのVPNプロファイルとアプリごとのVPNプロファイルをリモートで構成および管理できます。

重要:

- Citrix Secure Accessアプリは、ゼロトラストネットワークアクセスをサポートしています。NetScaler Gateway URLに加えて、Workspace URLにも接続できます。
- macOS版Citrix Secure Accessに関する管理者向けの手順については、「[iOS版Citrix SSOおよびmacOS版Citrix Secure Access](#)」を参照してください。

macOS用Citrix Secure Accessクライアントをインストールする

macOS版Citrix Secure Accessクライアントリリース25.06.1.1以降、アプリケーションは[macOS版Citrix Secure Access](#)で入手可能なパッケージ（`.pkg`）ファイルを使用するか、App Storeからダウンロードしてインストールできます。`.pkg` ファイルは、手動で、またはJamfやIntuneなどの管理ツールを使用してインストールできます。以前は、ユーザーはApp StoreからのみmacOS版Citrix Secure Accessクライアントをインストールすることに限定されていました。

.pkgファイルを使用してmacOSにCitrix Secure Accessアプリをインストールする

前提条件

Citrix Secure Accessアプリの .pkg ファイルをインストールする前に、以下の前提条件が満たされていることを確認してください。

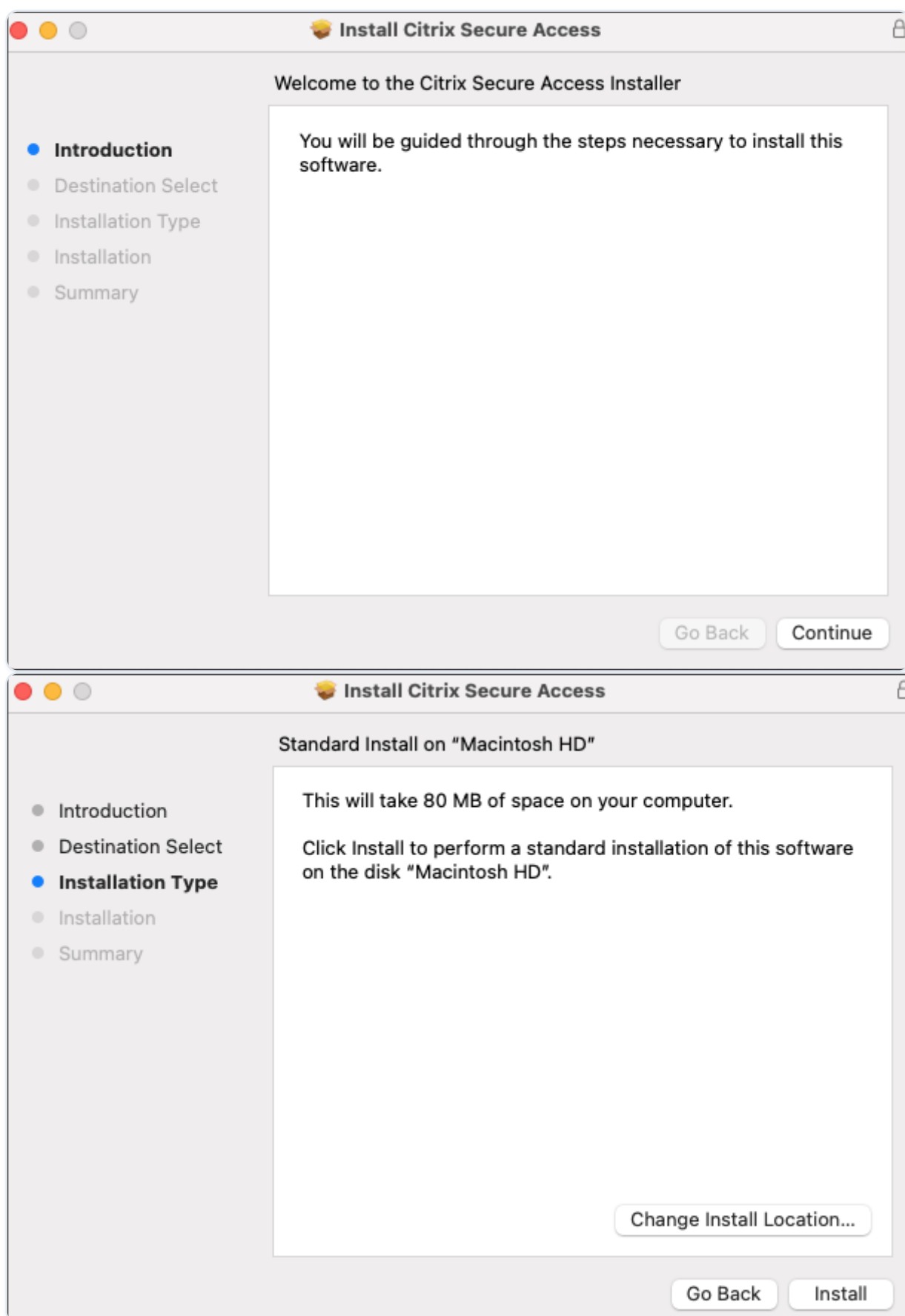
- MacコンピュータがmacOS 13.0以降で動作していること。
- ユーザーがMacコンピュータで管理者権限を持っていること。管理対象マシンでは、管理者はアプリケーションのインストール権限が有効になっており、識別子「com.citrix.NSG.macos.app.vpnplugin」を持つシステム拡張機能がアクティブ化されていることを確認する必要があります。
- Citrix Secure Accessアプリが現在実行中の場合は、ログアウトしてください。
- 以前にインストールされたApp Store版のCitrix Secure Accessアプリをすべて削除してください。

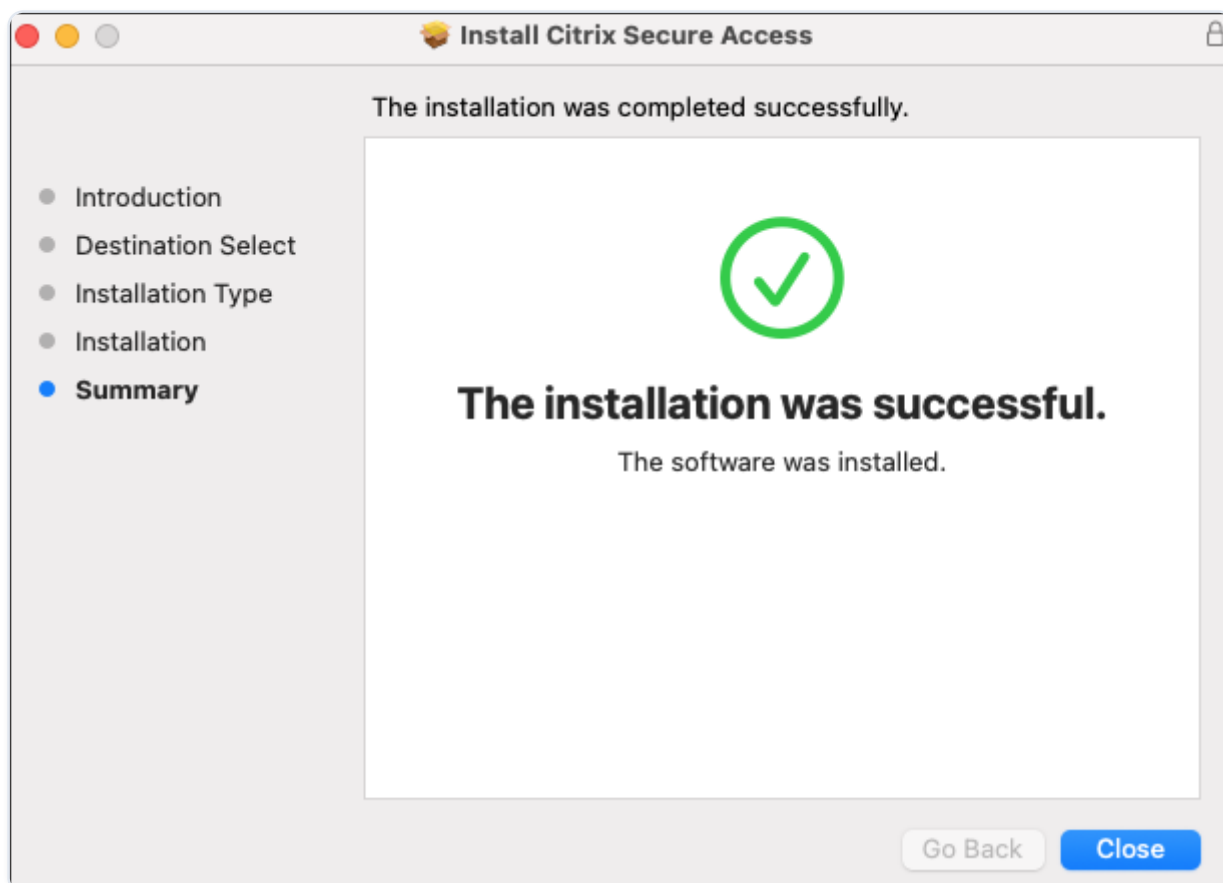
macOS に Citrix Secure Access アプリをインストールする方法

重要:

- Citrix Secure Access アプリの .pkg ファイルは、VPN 接続に識別子「com.citrix.NSG.macos.app.vpnplugin」を持つシステム拡張機能を使用します。
- クライアント証明書認証の場合、macOS システム拡張機能はログインキーチェーンから証明書にアクセスできないため、証明書はシステムキーチェーンにインストールする必要があります。
- 同じ証明書がシステムキーチェーンとログインキーチェーンの両方にインストールされている場合は、ログインキーチェーンから証明書とそのキーを削除してください。

1. Citrix Secure Access for macOS から .pkg ファイルをダウンロードします。
2. 管理ツール (Jamf または Intune) を使用するか、手動でアプリケーションをインストールします。アプリケーションを手動でインストールするには、.pkg ファイルをダブルクリックし、画面の指示に従います。

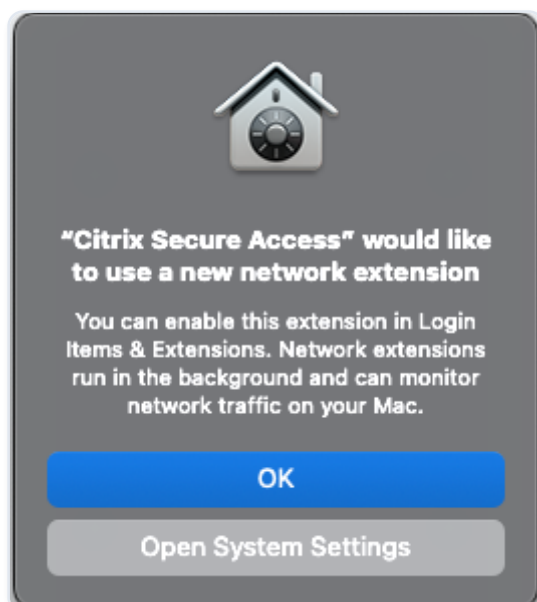




初回セットアップ

Citrix Secure Access アプリをインストールしたら、macOS デバイスから Citrix Secure Access アプリを使用するために、次の手順を実行します。

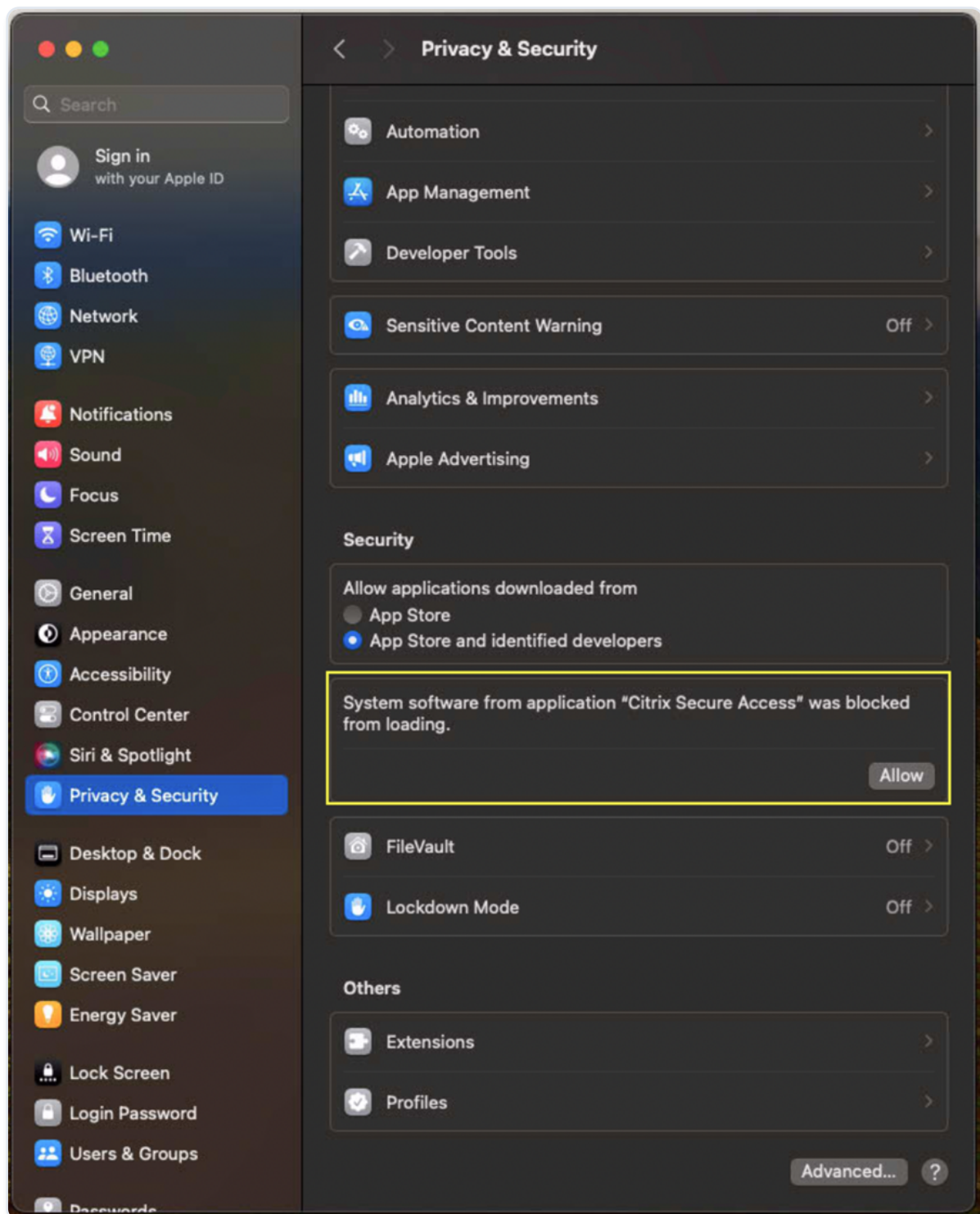
1. アプリケーションフォルダを開き、Citrix Secure Access アプリのアイコンをダブルクリックして起動します。
2. 初回起動時に、システム拡張機能をインストールするための許可を求めるプロンプトが表示されます。システムプロンプトで**OK**をクリックします。



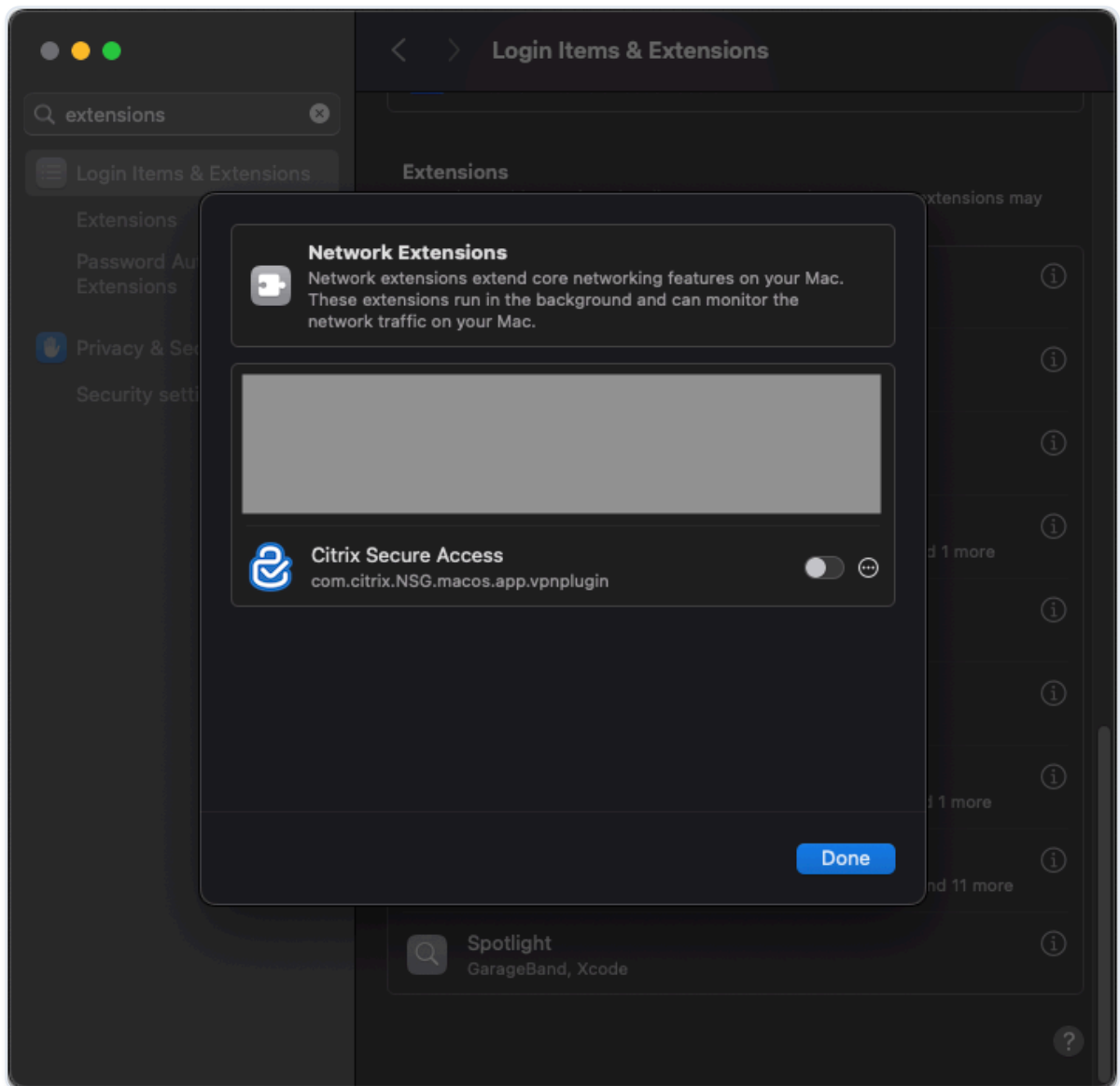
システムプロンプトが表示されない場合は、**システム設定**に移動して、識別子

「com.citrix.NSG.macos.app.vpnplugin」を持つシステム機能拡張のインストールを有効にしてください。

- macOS 14.xの場合、**システム設定**オプションは**プライバシーとセキュリティ**タブの下にあります。



- macOS 15.x以降の場合、システム設定オプションはログイン項目と機能拡張 -> ネットワーク機能拡張の下にあります。



Citrix Secure Access アプリケーションでのEndpoint Analysis™ プラグインの自動インストールをサポート

バージョン25.11.1.1以降、Citrix Secure Access アプリケーションにはEndpoint Analysis (EPA) プラグインの自動インストールが含まれています。EPAプラグインは、すべてのインストールとアップデートにデフォルトでバンドルされるようになり、個別のインストールが不要になり、セットアッププロセスが簡素化されます。この機能は、アプリケーションのApp Storeバージョンでは利用できません。

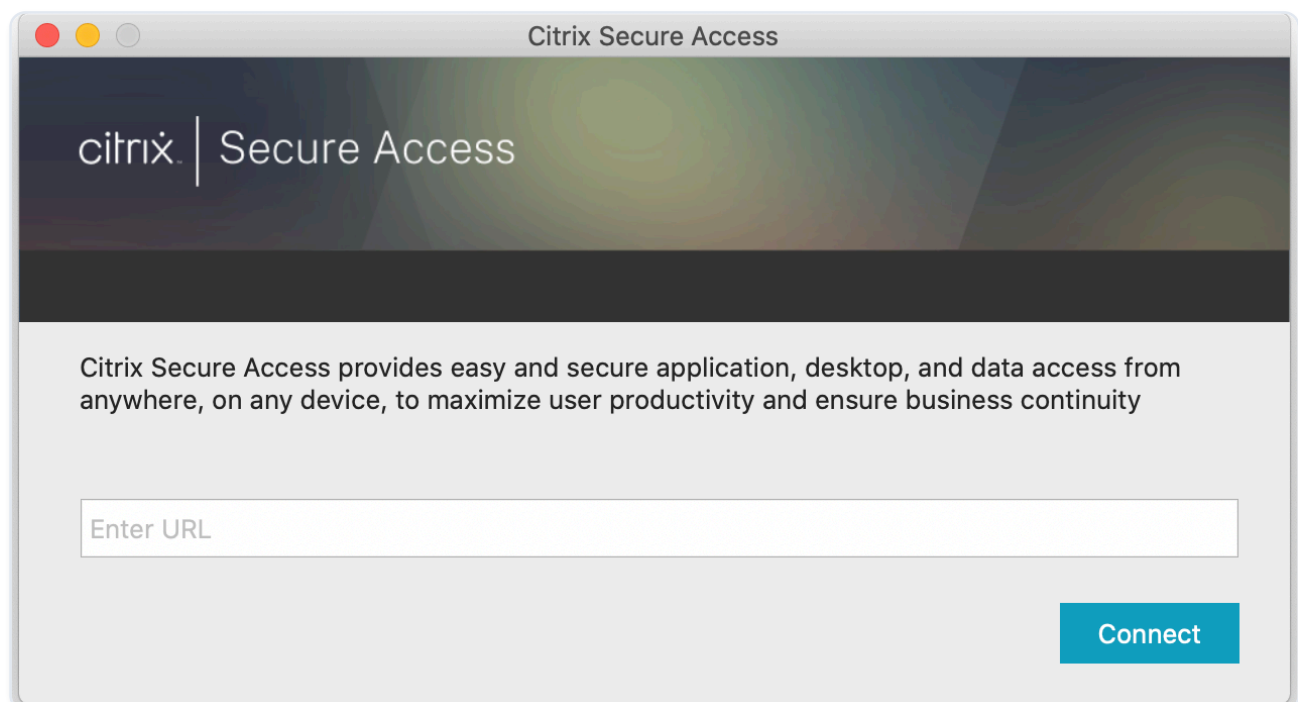
以前は、ユーザーはCitrix Secure Access アプリケーションのログイン中にEPAプラグインを手動でダウンロードしてインストールする必要がありました。

macOSデバイスからCitrix Secure Accessアプリを使用する方法

初めて利用するユーザーは、サーバーを追加してNetScaler Gatewayへの接続を作成する必要があります。既存のユーザーは、既存の接続に接続するか、新しい接続を追加するか、既存の接続を編集することができます。また、ログを表示し、それに応じて適切なアクションを実行することもできます。

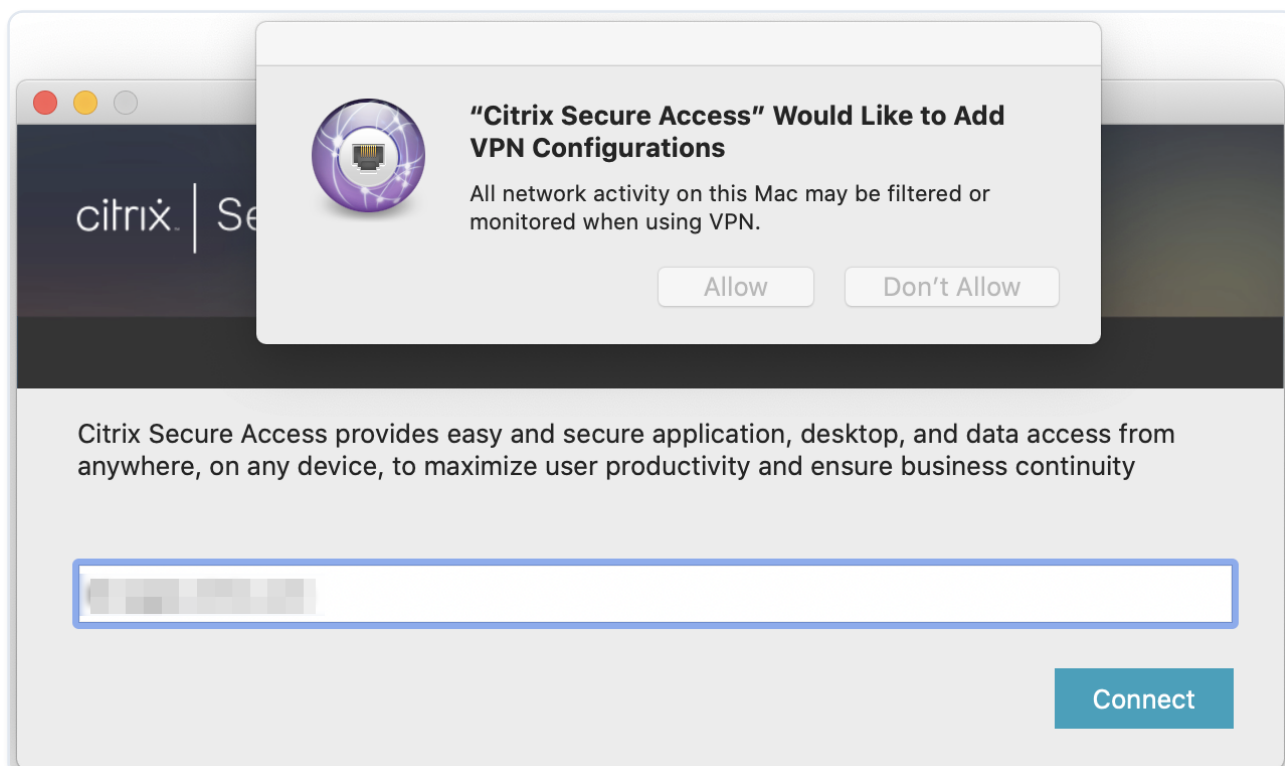
初めてのユーザーエクスペリエンス

Citrix Secure Accessアプリをインストールし、初めてアプリを開くと、次の画面が表示されます。

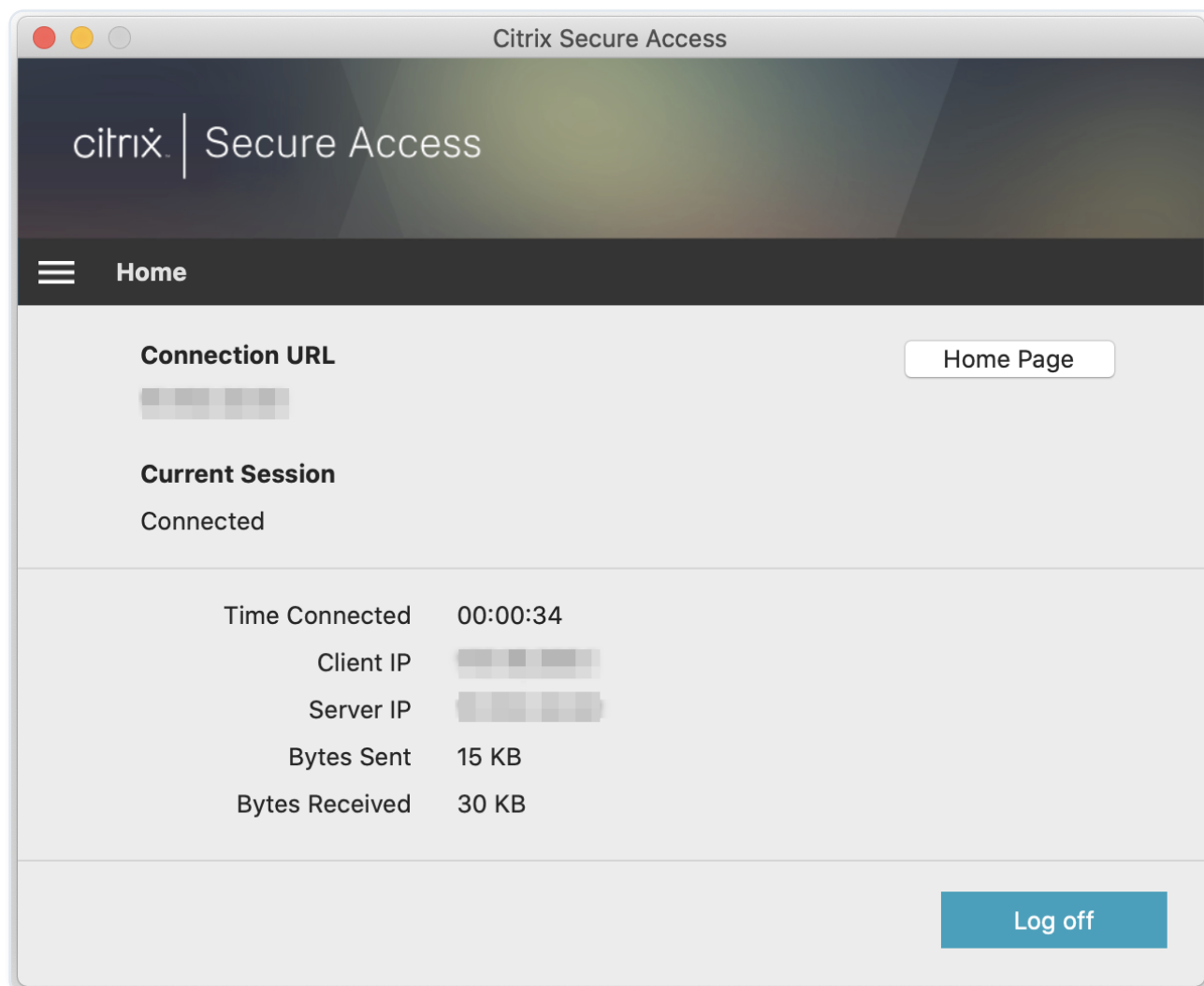


NetScaler GatewayのベースURLまたはCitrix WorkspaceのURLを入力し、**Connect**をクリックします。

ポップアップメッセージが表示されます。**Allow**をクリックして接続の追加を有効にします。このメッセージは初回のみ表示されます。それ以降の新しい接続では、このメッセージは表示されません。



注: Citrix Secure Accessからログアウトするには、まずアプリ内で**Log Off**をクリックし、その後ドックからアプリを終了することをお勧めします。ドックの**Quit**オプションは使用しないでください。

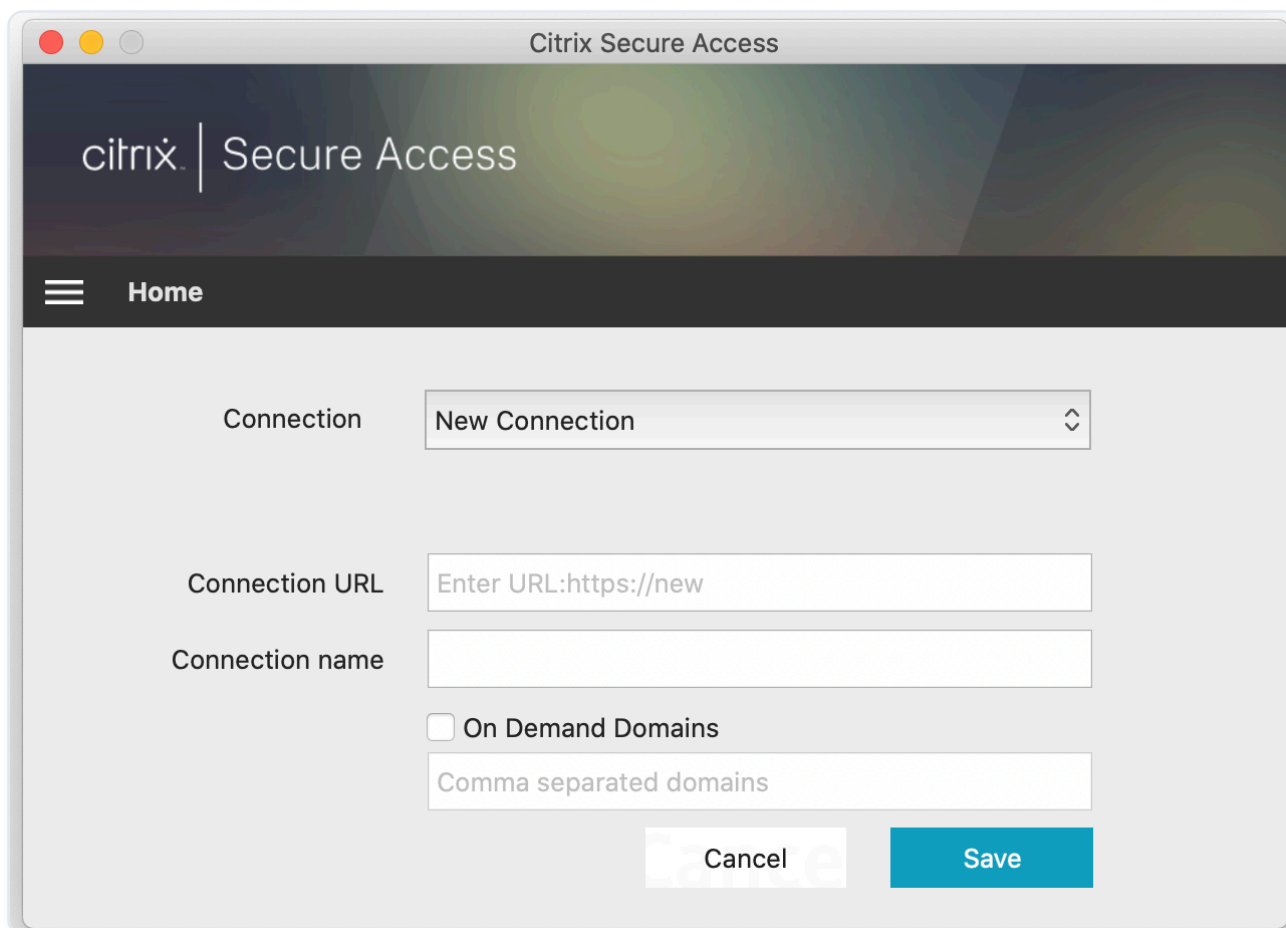


NetScaler Gatewayに接続する

最初の接続を追加した後、それ以降の接続では、既存のNetScaler GatewayまたはCitrix Workspaceに接続するか、新しい接続を追加することができます。

接続を追加する

ベースURL（例：[My company <https://gateway.mycompany.com>](https://gateway.mycompany.com)）とVPN接続の名前を入力します。

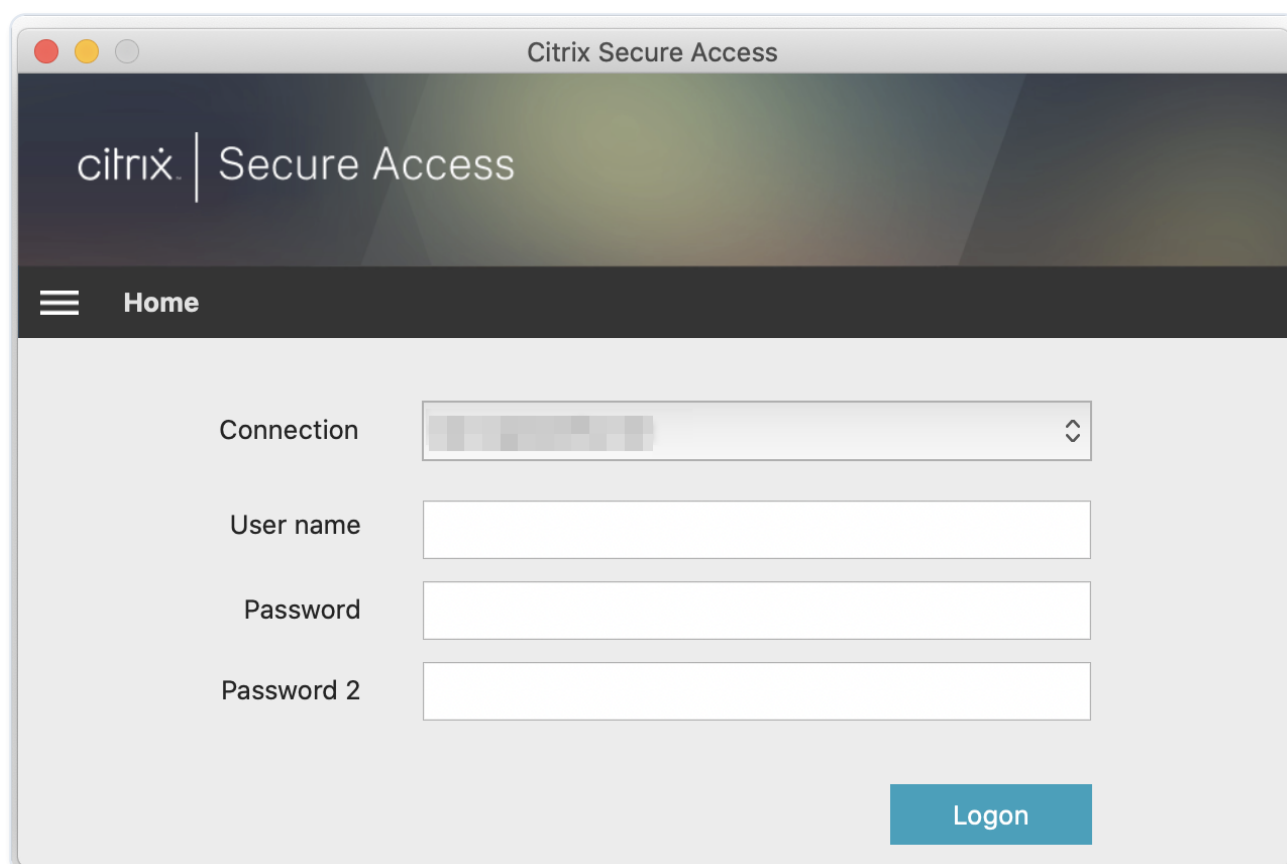


The screenshot shows the Citrix Secure Access web interface. At the top, there is a header with the Citrix logo and the text 'Secure Access'. Below the header is a navigation bar with a hamburger menu icon and the word 'Home'. The main content area contains a form for creating a new connection. The form has the following fields and controls:

- Connection:** A dropdown menu with 'New Connection' selected.
- Connection URL:** A text input field with the placeholder text 'Enter URL:https://new'.
- Connection name:** A text input field.
- On Demand Domains:** A checkbox that is currently unchecked.
- Comma separated domains:** A text input field.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

既存のNetScaler Gatewayに接続する

既存の接続を選択し、サーバーの認証情報を入力して、**ログオン**を選択します。

A screenshot of the Citrix Secure Access login window. The window has a title bar with standard macOS window controls (red, yellow, green buttons) and the text "Citrix Secure Access". The main content area has a dark header with the "citrix | Secure Access" logo. Below the header is a dark navigation bar with a hamburger menu icon and the word "Home". The main area is light gray and contains four input fields: "Connection" (a dropdown menu with a blurred selection), "User name", "Password", and "Password 2". A blue "Logon" button is located at the bottom right of the form.

VPN接続の失敗後にNetScaler Gatewayに再接続する

リリース23.09.1以降、macOS用Citrix Secure Accessクライアントは、VPN接続が失われたときにNetScaler Gatewayで再認証するよう求めます。Citrix Secure AccessクライアントのUIに、NetScaler Gatewayへの接続が失われたこと、および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。



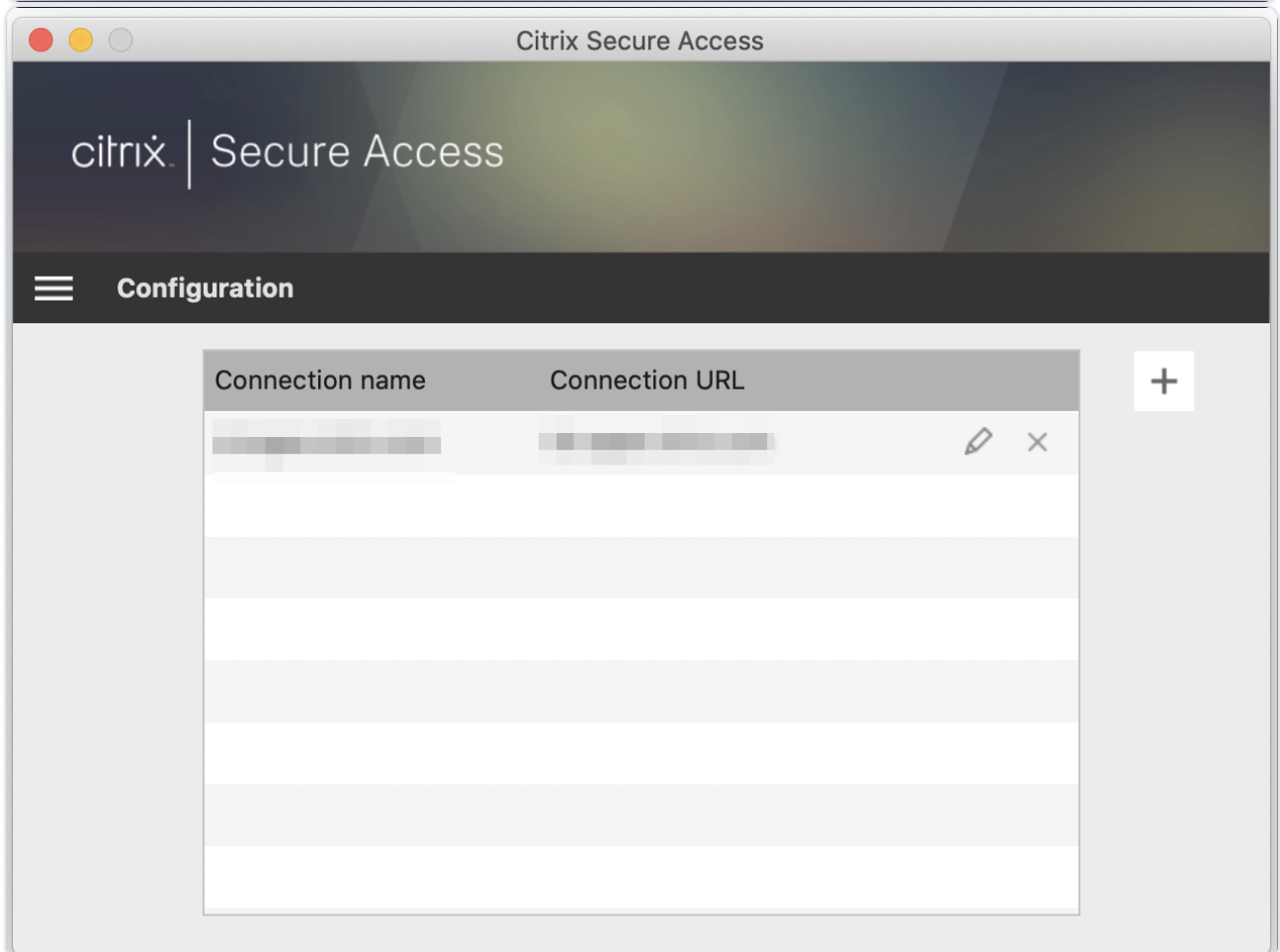
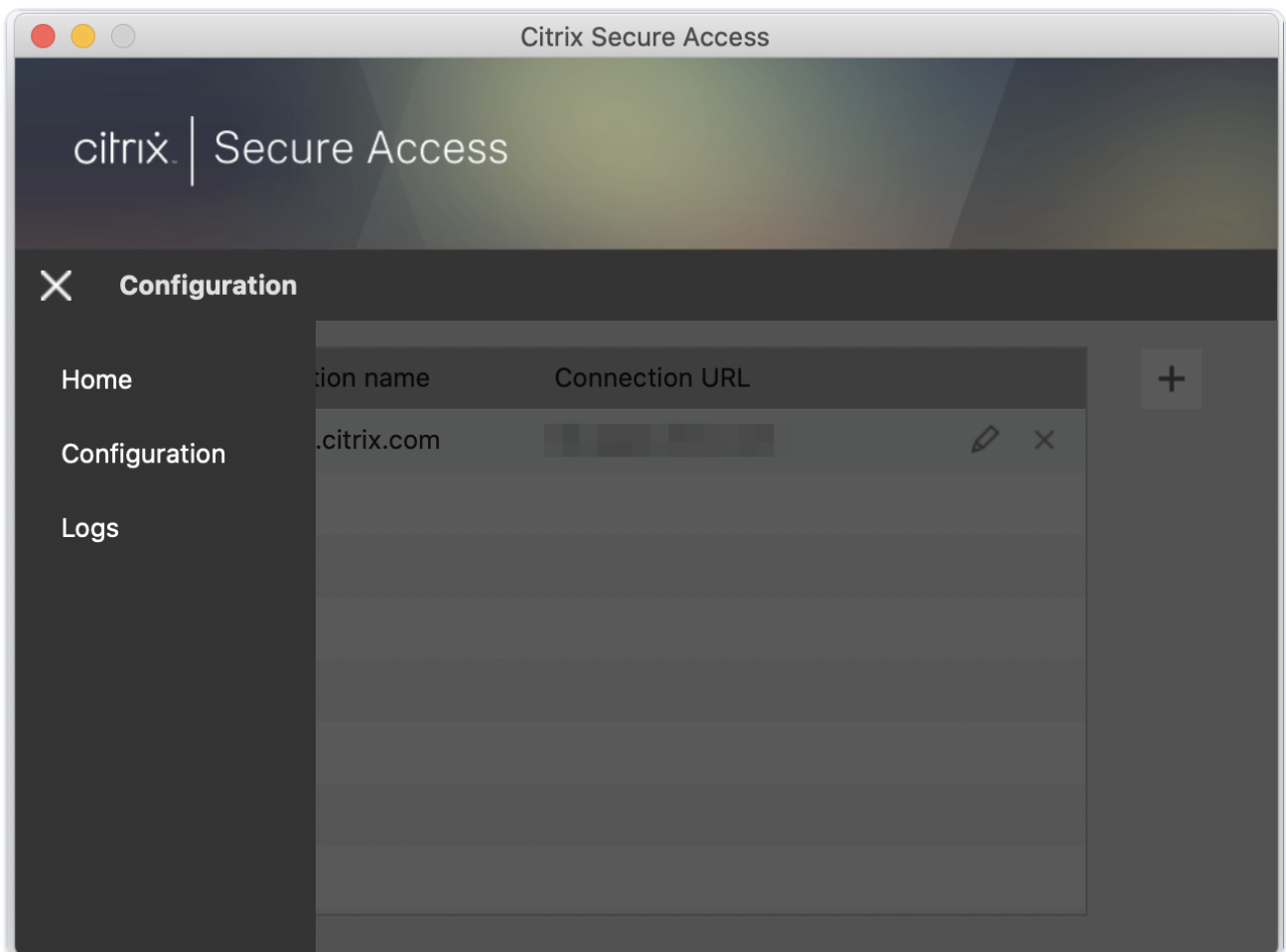
Reauthentication Needed

Gateway connection lost. Reauthenticate to resume connection.

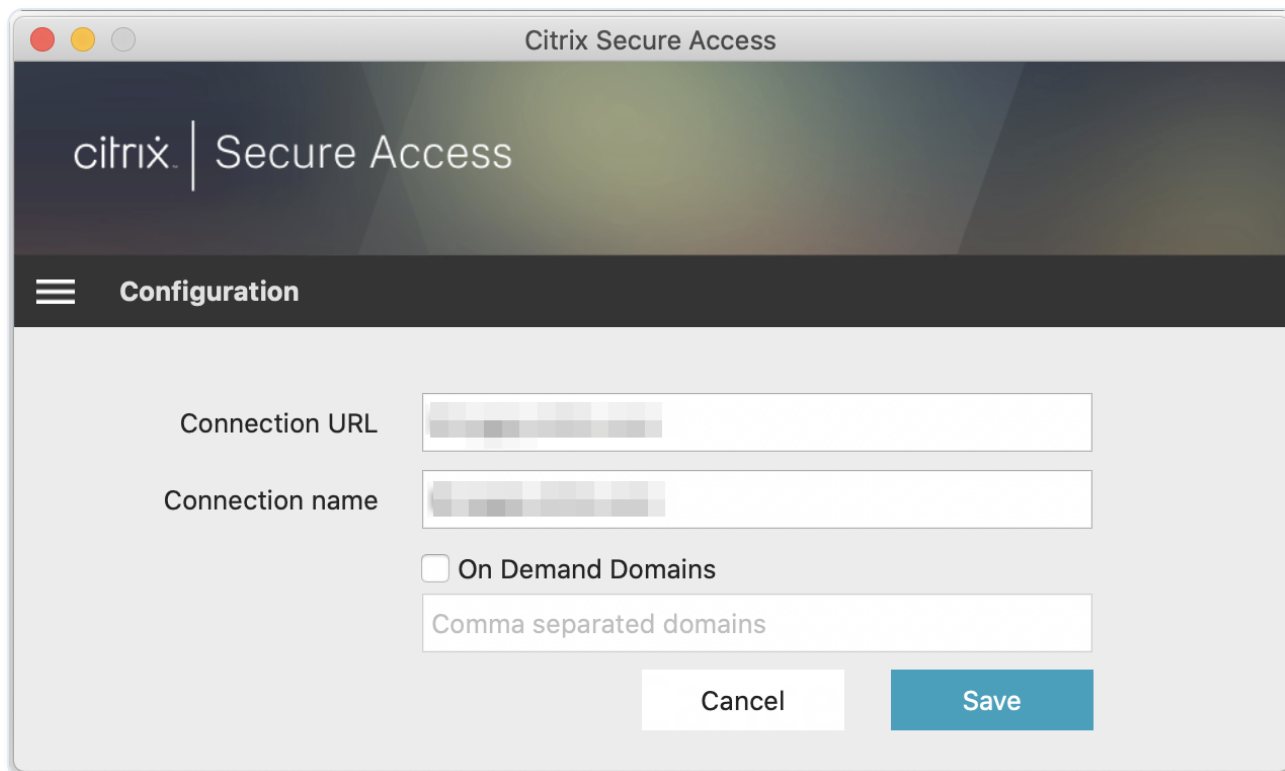
Ok

既存の接続を変更する

既存の接続を変更または削除できます。



必要に応じて接続の詳細を変更します。



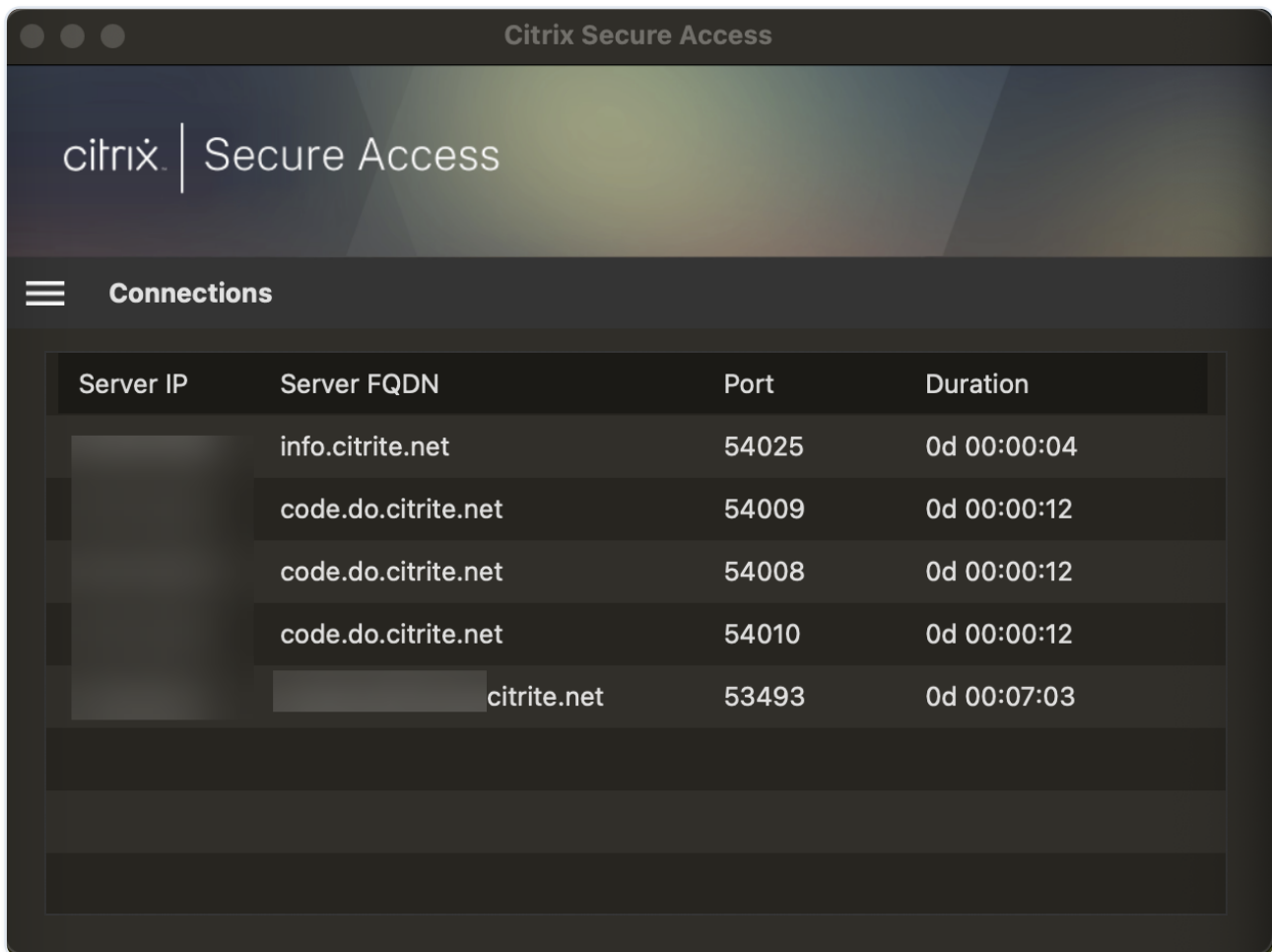
The image shows a macOS-style window titled "Citrix Secure Access". The window has a dark header bar with the Citrix logo and the text "Secure Access". Below the header is a dark bar with a hamburger menu icon and the word "Configuration". The main area is light gray and contains the following fields:

- Connection URL**: A text input field with a blurred value.
- Connection name**: A text input field with a blurred value.
- ☐ **On Demand Domains**: A checkbox that is currently unchecked.
- Comma separated domains**: A text input field with a blurred value.

At the bottom right of the dialog are two buttons: "Cancel" (white with black text) and "Save" (blue with white text).

保護された接続のインサイト

リリース23.09.1以降、IPアドレス、FQDN、宛先ポート、接続期間を含む保護された接続の詳細を表示できます。これらの詳細を表示するには、UIのハンバーガーメニューをクリックし、**接続**に移動します。



The screenshot shows the Citrix Secure Access application window. At the top, there's a header with the Citrix logo and 'Secure Access'. Below that is a 'Connections' section with a table listing active connections. The table has four columns: Server IP, Server FQDN, Port, and Duration. There are five rows of connection data visible.

Server IP	Server FQDN	Port	Duration
[REDACTED]	info.citrite.net	54025	0d 00:00:04
[REDACTED]	code.do.citrite.net	54009	0d 00:00:12
[REDACTED]	code.do.citrite.net	54008	0d 00:00:12
[REDACTED]	code.do.citrite.net	54010	0d 00:00:12
[REDACTED]	[REDACTED].citrite.net	53493	0d 00:07:03

ローカルLANアクセス

Citrix Secure Accessクライアント for macOS 23.10.1は、ローカルLANアクセス機能をサポートしており、VPN接続が確立された後、クライアントマシン上のローカルLANリソースにアクセスするかどうかを決定できます。この機能は、管理者がNetScaler GatewayでローカルLANアクセス設定を構成している場合にのみ使用できます。

Citrix Secure AccessクライアントUIでローカルLANアクセスを有効にするには、ホームページに移動し、**Allow Local LAN Access**チェックボックスを有効にします。

接続が確立された後、同じページでローカルLANアクセスのステータスを確認できます。

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

重要:

この機能はデフォルトで無効になっています。この機能を使用するには、管理者にお問い合わせください。

Citrix Secure Access for macOS 24.03.1以降、Citrix Workspaceアプリへのログインにより、エンドユーザーはCitrix Secure Accessにシングルサインオン（SSO）でき、ユーザーチャネルを確立し、TCP/UDPアプリケーションへのアクセスをシームレスに提供できます。Citrix Workspaceアプリに接続している場合、Citrix Secure Access for macOSは自動的に起動され、シングルサインオンを使用してシームレスにログインできます。

Citrix Workspaceアプリにログオンすると、Citrix Secure Accessクライアントが自動的に起動され、クライアントにシングルサインオンされます。Citrix Workspaceアプリからログアウトすると、Citrix Secure Accessは手動操作なしで自動的にアプリケーションからログアウトさせます。この機能により、エンドユーザーは1つのアプリケーションにログオンするだけで済むため、時間を節約でき、統合されたエクスペリエンスが提供されます。

注:

この機能が動作するためには、Citrix WorkspaceアプリとCitrix Secure Accessクライアントを介してアクセスされるプライマリURLが同じである必要があります。

前提条件

1. エンドユーザーは[Citrix Workspace app 2402](#)以降を使用している必要があります。Mac用Citrix Workspaceアプリのインストールについては、[Citrix Workspace app for Mac](#)を参照してください。
2. エンドユーザーは[Citrix Secure Access for macOS 24.03.1](#)以降を使用している必要があります。

注意点:

- ユーザーがこの機能を使用する前にCitrix Workspaceアプリにすでにログインしている場合、アプリがCitrix Secure Accessクライアントへのシングルサインオンをトリガーできるように、Citrix Workspaceアプリに再ログインする必要があります。
- タイムアウト、手動によるユーザーログアウトなどによりユーザーがCitrix Workspaceアプリからログアウトすると、Citrix Secure Accessもログアウトされ、

ユーザーセッションは切断されます（これは、Citrix Secure AccessがCitrix Workspaceアプリを介して自動的に起動された場合に限りです）。

- Citrix WorkspaceアプリからCitrix Secure AccessへのSSOログインは、単一のプライマリドメインでのみサポートされています。複数のドメインでのSSOはサポートされていません。
- この機能を通じてCitrix Secure Accessにシングルサインオンした後、Citrix Workspaceアプリの接続を別のURLに切り替えると、Citrix Workspaceアプリの接続URLを選択するよう求められます。

Citrix Workspaceアプリ(/en-us/citrix-sso/media/switch-cwa-connection.png)

ログを送信

デバッグログの取得は、トラブルシューティングやCitrixサポートへの問題報告において重要な部分です。ログのトラブルシューティングを行うには、**ホーム > ログ**に移動します。

ログタブをクリック(/en-us/citrix-sso/media/sso-macos-logs1.png)

次のセッションログレベルのいずれかを選択します。

- **デフォルト**: 基本的なトラブルシューティングに必要な最小限のログを出力します。
- **デバッグメッセージ**: すべてのログを出力します。
- **詳細**: トンネルメッセージや構成情報を含む詳細なログを出力します。

リリース23.07.1以降、**ログファイルの最大数**フィールドを使用して、ログ収集に追加するファイルの数を指定できます。最大50個のログファイルを追加できます。

- ログを表示するには、**ログを開く**をクリックします。
- ログをローカルディレクトリにエクスポートするには、**ログをエクスポート**をクリックします。
- **ログをメールで送信**をクリックして、ログをメールで送信します。
- **ログをクリア**をクリックして、古いログを削除します。

注：

Citrix Secure Access for macOS リリース 23.07.1 以降、**ログをメールで送信**オプションは、**ログ**ページで利用できます。

エクスポートまたはログのクリアを開く (</en-us/citrix-sso/media/sso-macos-logs2.png>)

Citrix Secure Access for macOS 23.06.1 以降、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導入されました。このメニューは、デバッグログをキャプチャして送信するための代替場所として使用できます。

ヘルプメニュー (</en-us/citrix-sso/media/help-menu.png>)

参照

Citrix SSO for iOS の管理者固有の手順については、[Citrix SSO for iOS](#) および [Citrix Secure Access for macOS](#)を参照してください。

Linux 用 Citrix Secure Access クライアント

Linux 用 Citrix Secure Access クライアントは、NetScaler Gateway によって管理される VPN クライアントソフトウェアであり、企業データやアプリケーションにリモートでアクセスできるようにします。

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。これは、NetScaler Gateway を介して企業データへのアクセスを許可する前に、エンドポイントの基準をチェックします。Citrix EPA クライアントと Citrix Secure Access クライアントは互いに独立しています。

管理者が設定している場合にのみ、Citrix EPA クライアントをインストールできます。管理者固有の手順については、[Linux 用 Citrix Secure Access クライアント](#) を参照してください。

重要な更新:

ユーザーインターフェイスと製品ドキュメントを新しい NetScaler ブランドに更新しています。この移行期間中、Citrix と NetScaler の参照が混在して使用されているのを目にするかもしれません。

Citrix Secure Access client および Citrix EPA client をインストールする

注記:

- ソフトウェアセンターから Citrix Secure Access client と Citrix EPA client をインストールする場合、最新バージョンにアップグレードする前に、既存のバージョンが最新でない場合はアンインストールする必要があります。これは、Ubuntu 18.04 とは異なり、現在のバージョンを最新バージョンに置き換えることができないためです。
- Ubuntu 20.x で、Firefox ブラウザから Citrix Secure Access client をダウンロードし、**Open With** オプションを使用して開くと、インストールが失敗する可能性があります。

これは、Firefoxがクライアントを一時的な場所にダウンロードし、その場所からはCitrix Secure Access clientのインストールが失敗するためです。

回避策として、**Save File**オプションを選択することをお勧めします。このオプションを選択すると、Citrix Secure Access clientが**Downloads**フォルダーにダウンロードされます。その後、ダウンロードしたファイルをダブルクリックしてCitrix Secure Access clientをインストールできます。

- eLuxやIGEL OSのようなシンLinuxクライアントでは、Citrix Secure Access clientとCitrix EPA clientは管理者が管理します。ユーザーはCitrix Secure Access clientとCitrix EPA clientを直接インストールすることはできません。

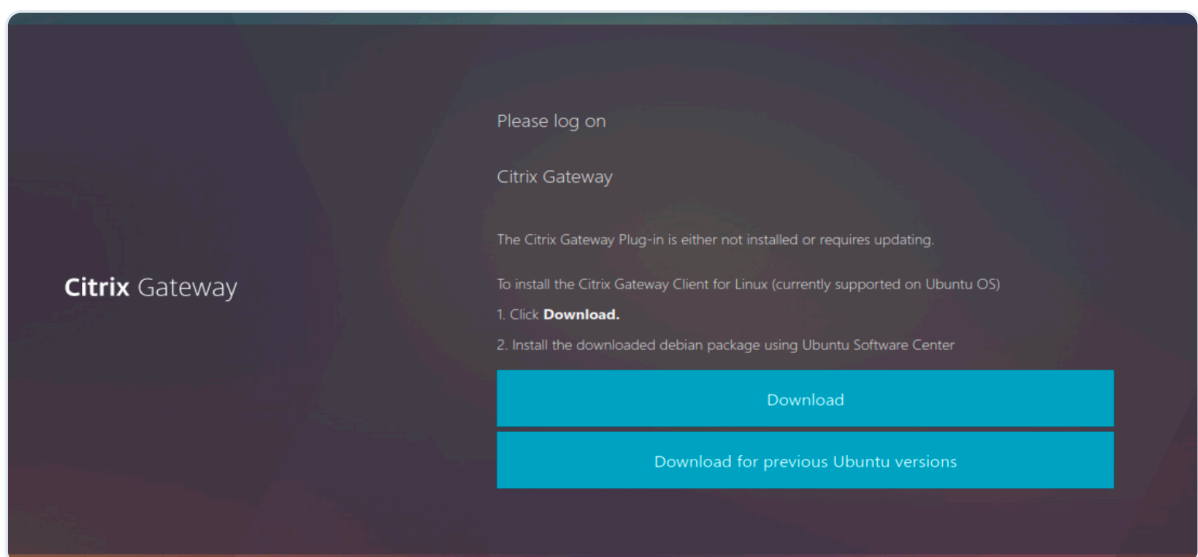
Ubuntu 20.04 用の Citrix Secure Access client および Citrix EPA client をインストールする

以下の手順でCitrix Secure Access clientとCitrix EPA clientをインストールできます。

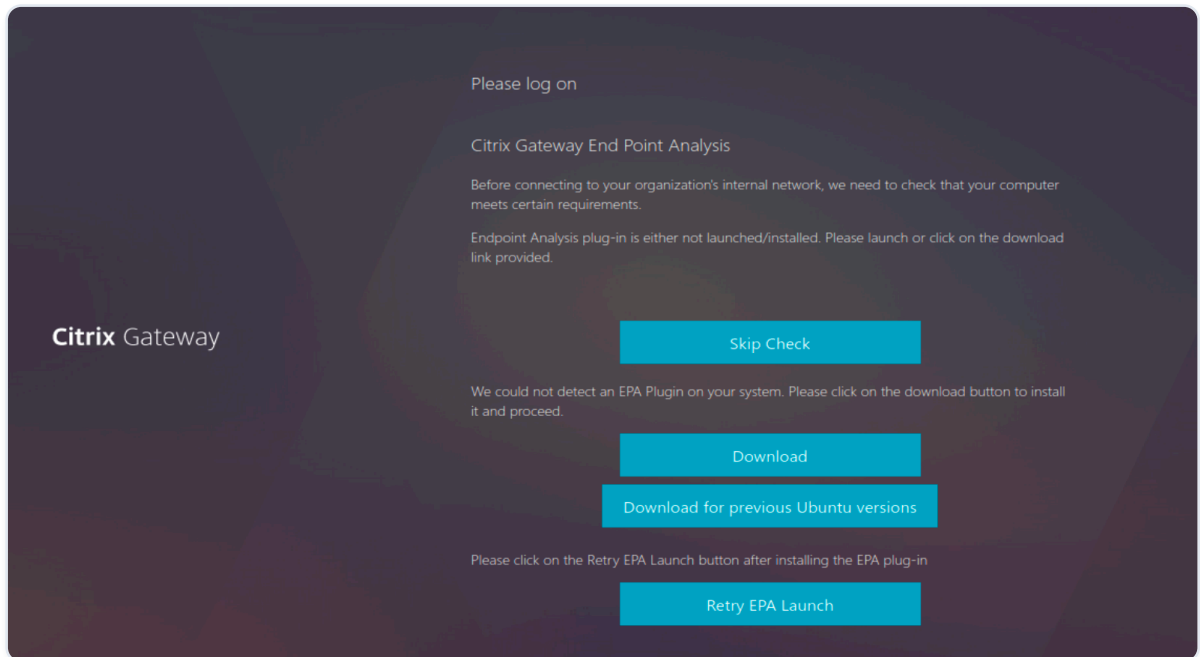
1. 以下のいずれかのオプションを使用して、Citrix Secure Access clientとCitrix EPA clientをダウンロードします。

- **オプション 1:** Webブラウザを開き、管理者から提供されたNetScaler GatewayのURLを入力します。数秒後に表示されるダウンロード画面で、**Download for previous Ubuntu versions**ボタンをクリックします。

Citrix Secure Access clientのダウンロードには、次の画面が表示されます。



Citrix EPA clientのダウンロードには、次の画面が表示されます。



- **オプション 2:** Citrix Secure Access Clients for Ubuntuにアクセスし、Ubuntu 20セクションの下にある**Download**ボタンをクリックして、Citrix Secure Access clientとCitrix EPA clientをダウンロードします。

Citrix Secure Access クライアントのダウンロード(/en-us/citrix-sso/media/csa-client-download-20.png)

2. Citrix Secure Access クライアントとCitrix EPA クライアントを、GUIまたはUbuntuターミナルを使用してインストールします。

- ダウンロードしたファイルをダブルクリックし、Citrix Secure Access クライアントとCitrix EPA クライアントをインストールします。

ダウンロードしたCitrix Secure Access クライアントをダブルクリックすると、次の画面が表示されます。

Citrix Secure Access クライアントのインストール(/en-us/citrix-sso/media/install-csa-client.png)

ダウンロードしたCitrix EPA クライアントをダブルクリックすると、次の画面が表示されます。

Citrix EPA クライアントのインストール(/en-us/citrix-sso/media/install-epa-client.png)

Citrix Secure Access クライアントがすでにインストールされているがアップグレードされていない場合、最新バージョンへのアップグレードを求められます。次の画面に示すように、**はい**をクリックして最新バージョンにアップグレードします。

このアップグレードはCitrix EPA クライアントには適用されません。

Citrix Secure Access クライアントのアップグレード(/en-us/citrix-sso/media/upgrade-secure-access-client.png)

- Ubuntuターミナルを使用して、Citrix Secure Access クライアントとCitrix EPA クライアントをインストールします。

Citrix Secure Access クライアントをインストールするには、ターミナルで次のように入力します。

```
sudo apt install ./nsgclient18_64.deb  
  
sudo apt install -f
```

Citrix EPA クライアントをインストールするには、ターミナルで次のように入力します。

```
sudo apt install ./nsepa18.deb  
  
sudo apt install -f
```

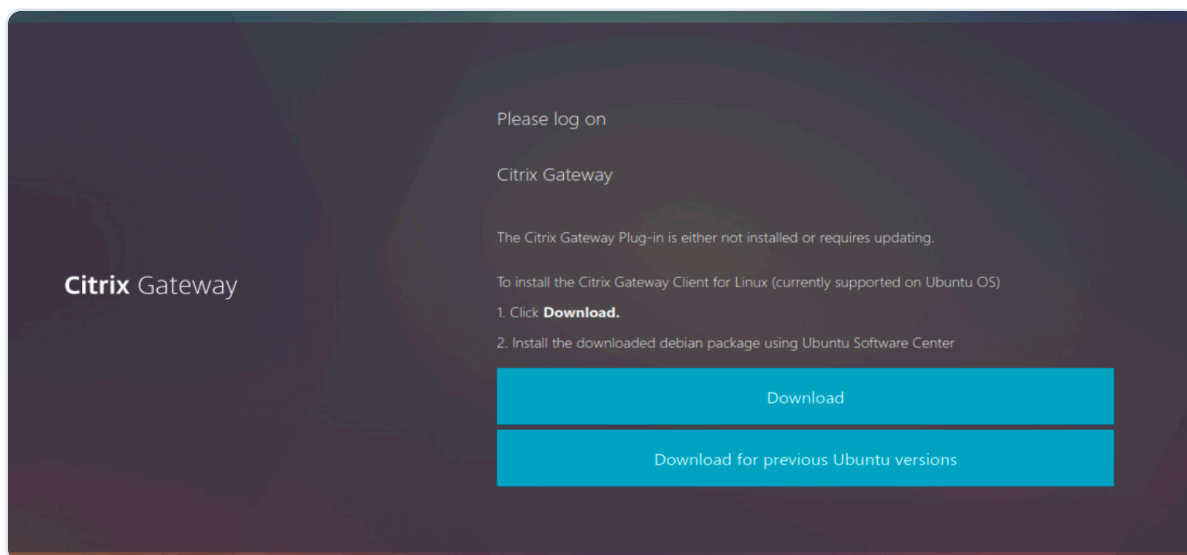
Ubuntu 22.04以降用のCitrix Secure Access クライアントとCitrix EPA クライアントをインストールする

次の手順でCitrix Secure Access クライアントとCitrix EPA クライアントをインストールできます。

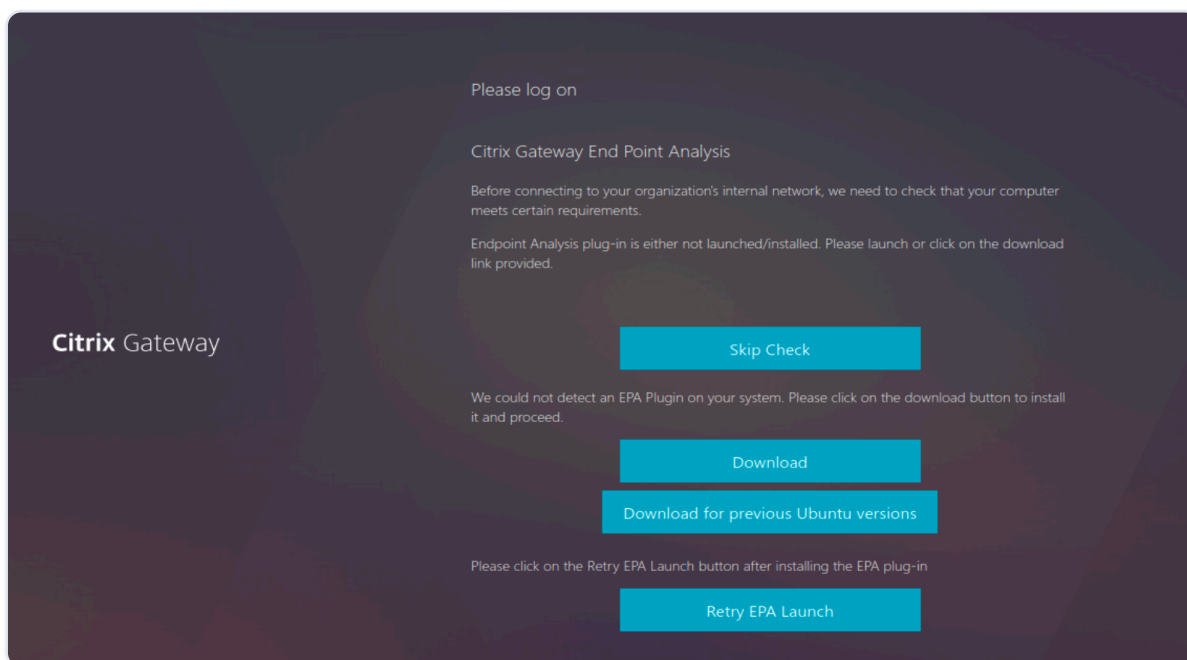
1. 以下のいずれかのオプションを使用して、Citrix Secure AccessクライアントとCitrix EPAクライアントをダウンロードします。

- **オプション1:** Webブラウザを開き、管理者から提供されたNetScaler GatewayのURLを入力します。数秒後に表示されるダウンロード画面で**ダウンロード**ボタンをクリックします

Citrix Secure Accessクライアントのダウンロードには、次の画面が表示されます。



Citrix EPAクライアントのダウンロードには、次の画面が表示されます。



- **オプション2:** Citrix Secure Access Clients for Ubuntuにアクセスし、Ubuntu 22/24セクションの下にあるダウンロードボタンをクリックして、Citrix Secure AccessクライアントとCitrix EPAクライアントをダウンロードします。

Citrix EPA client 25.5.3 for Ubuntu 20

May 19, 2025
9.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - eb4feda271c9be8e4392b5a8ec733565ae29b5ce4bf32c338352757554824138

Citrix EPA client 25.5.3 for Ubuntu 22/24

May 19, 2025
9.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - 460081aaae9d4625e27a07fcdcdb3646c8ff791d88da1a07200315954bdb7f40

Citrix Secure Access client 25.5.3 for Ubuntu 20

May 19, 2025
4.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - c802dc70e762245150a2741816a4b9b299fb8762ace8f56868ba2f66ae2b1b10

Citrix Secure Access client 25.5.3 for Ubuntu 22/24

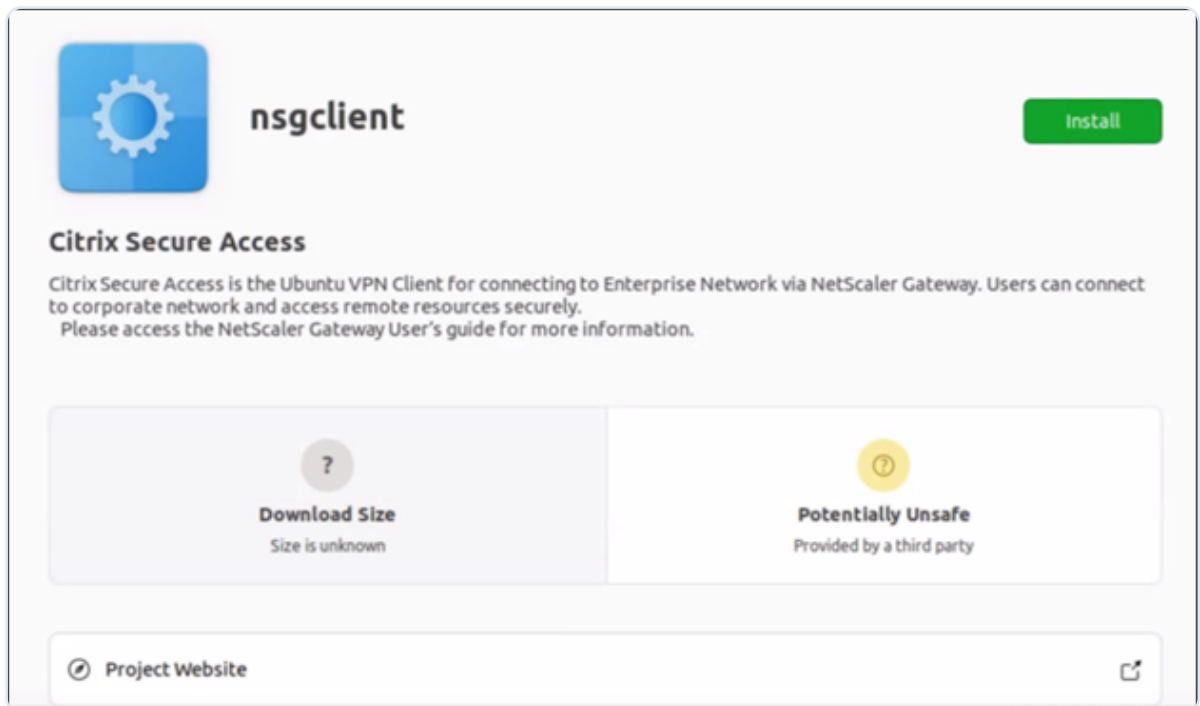
May 19, 2025
4.9 M - (.deb) [Download File](#)

Checksums
SHA-256 - 66458c71b6ff6039686939954519c57fdb745b13707473ded9c00de996318766

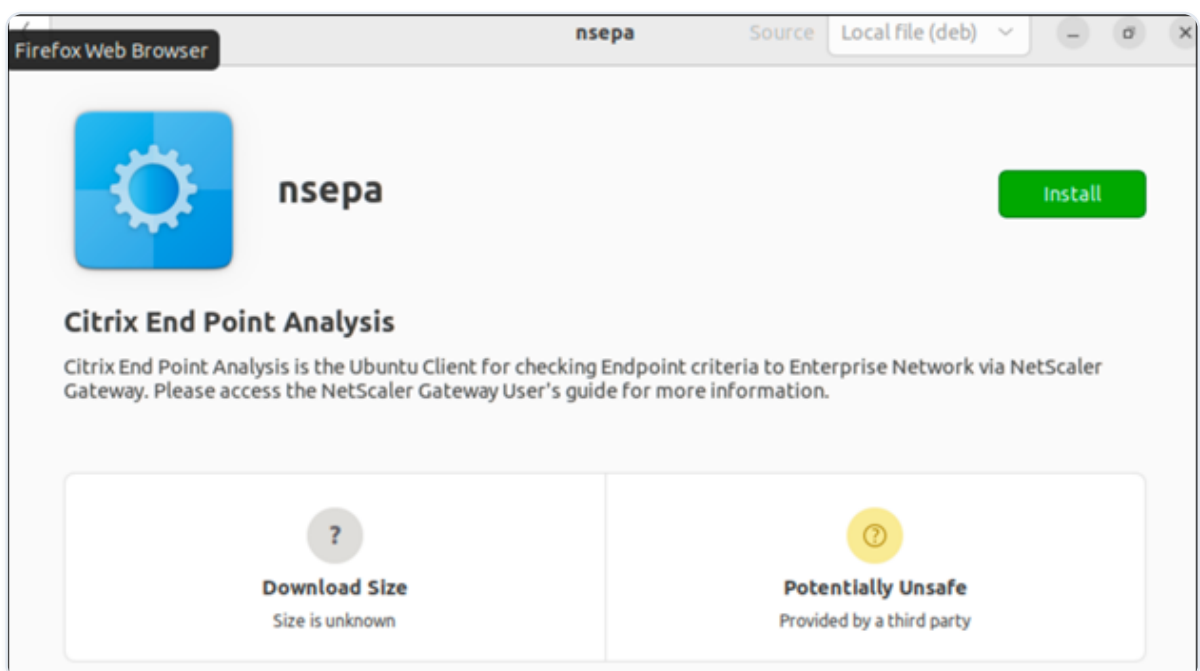
2. Citrix Secure AccessクライアントとCitrix EPAクライアントをGUIまたはUbuntuターミナルを使用してインストールします。

- ダウンロードしたファイルをダブルクリックして、Citrix Secure AccessクライアントとCitrix EPAクライアントをインストールします。

ダウンロードしたCitrix Secure Accessクライアントをダブルクリックすると、次の画面が表示されます。

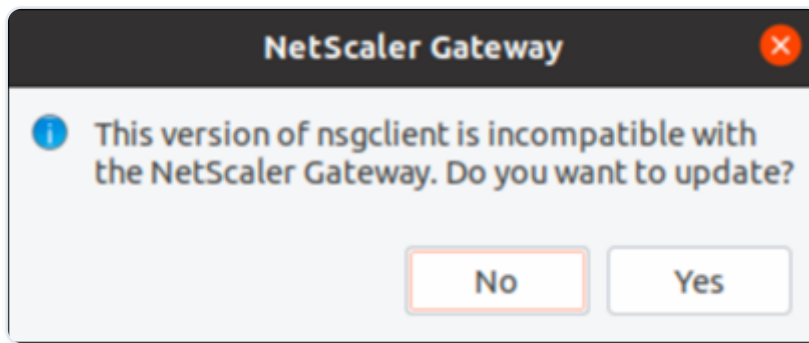


ダウンロードしたCitrix EPAクライアントをダブルクリックすると、次の画面が表示されます。



Citrix Secure Accessクライアントがすでにインストールされているがアップグレードされていない場合、最新バージョンへのアップグレードを促されます。次の画面に示すように、**はい**をクリックして最新バージョンにアップグレードします。

このアップグレードは、Citrix EPAクライアントには適用されません。



- Ubuntuターミナルを使用して、Citrix Secure AccessクライアントとCitrix EPAクライアントをインストールします。

Citrix Secure Accessクライアントをインストールするには、ターミナルで次のように入力します。

```
sudo apt install ./nsginstaller64.deb  
  
sudo apt install -f
```

Citrix EPAクライアントをインストールするには、ターミナルで次のように入力します。

```
sudo apt install ./nsepa.deb  
  
sudo apt install -f
```

Linux 用 Citrix Secure Access クライアントの使用方法

ブラウザで NetScaler Gateway の URL を入力し、Citrix Secure Access クライアントで認証します。認証が成功すると、ブラウザは Citrix Secure Access クライアントを起動するように求めます。

- タスクバーの Citrix Secure Access クライアントアイコンを選択し、をクリックします。

Citrix Secure Access クライアントの設定 (/en-us/citrix-sso/media/secure-access-client-settings.png)

- タブには、接続ステータス、ユーザー情報、トンネル接続、データ使用量などの詳細が表示されます。

Citrix Secure Access クライアントの接続設定 (/en-us/citrix-sso/media/secure-access-client-connections.png)

- タブには、NetScaler Gateway の情報、クライアント証明書をアップロードするオプション、およびログオプションが表示されます。

Citrix Secure Access クライアントの構成 (/en-us/citrix-ssso/media/secure-access-client-configuration.png)

- 証明書: クライアント証明書を構成するには、このセクションに移動します。この手順は、管理者が NetScaler Gateway で認証するためのクライアント証明書を提供した場合にのみ必要です。

Citrix Secure Access クライアント証明書 (/en-us/citrix-ssso/media/secure-access-client-certificate.png)

- ログ: デバッグログをキャプチャするには、このセクションに移動します。デバッグログのキャプチャは、トラブルシューティングや Citrix サポートへの問題報告の重要な部分です。

Citrix Secure Access クライアントのログ (/en-us/citrix-ssso/media/client-logging.png)

または、Citrix Secure Access クライアントを起動し、をクリックします。初めてのユーザーの場合、NetScaler Gateway の URL またはワークスペースの URL のいずれかを提供するように求められます。

Citrix Secure Access クライアントの起動 (/en-us/citrix-ssso/media/linux-client-logon.png)

ログを送信

管理者に送信するログファイルは、`nsgcepa.txt`、`nsepa.txt`、`nssslvpn.txt`、および `epalibv2.log` の形式です。これらのファイルは `~/.citrix/` ディレクトリにあります。以下の詳細をキャプチャします。

- **Info:** 基本ログとエラーログを出力します。
- **Debug:** すべてのログを出力します。ログを収集して管理者と共有するには、このオプションを選択することをお勧めします。
- **Verbose:** トンネルメッセージと構成情報を含む詳細ログを出力します。

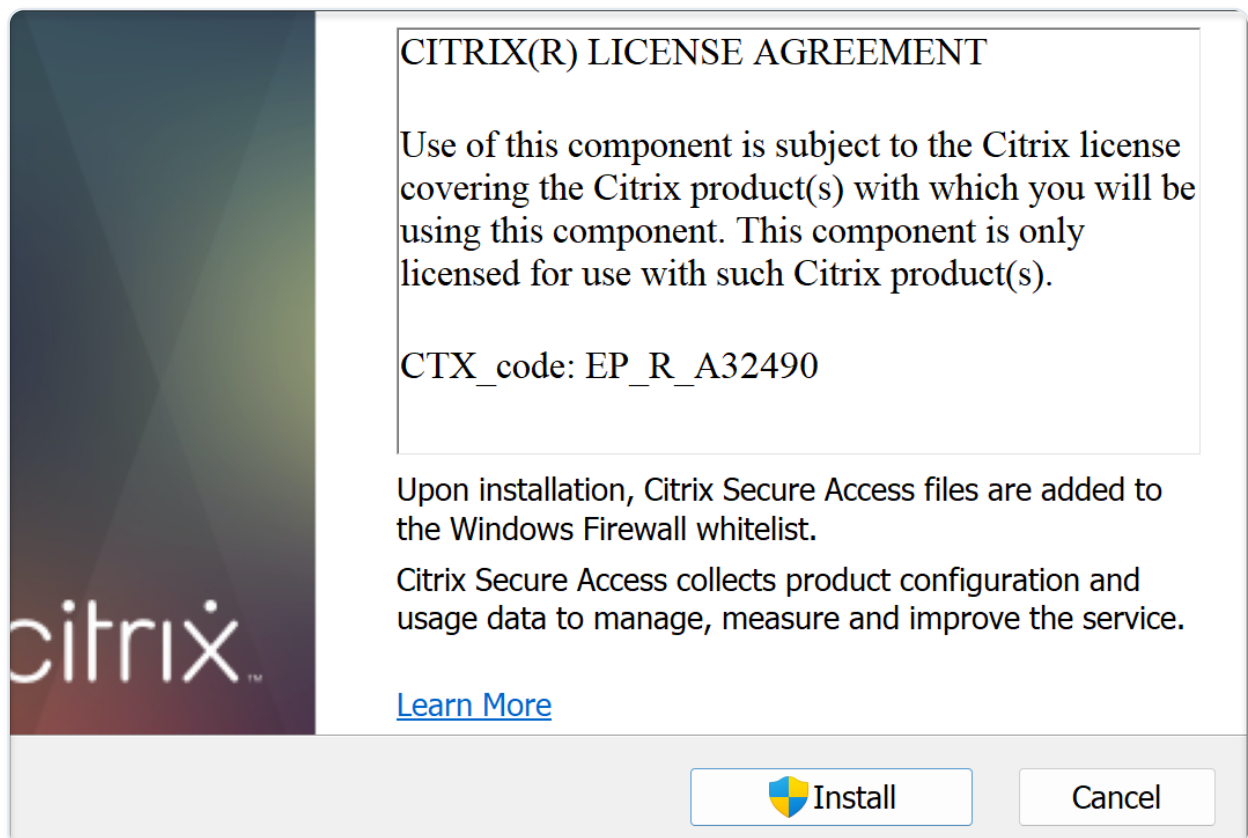
Windows 用 Citrix Secure Access クライアント

Windows 用 Citrix Secure Access クライアントは、NetScaler Gateway と Secure Private Access を使用して、企業データやアプリケーションにリモートでアクセスできる VPN クライアントソフトウェアです。

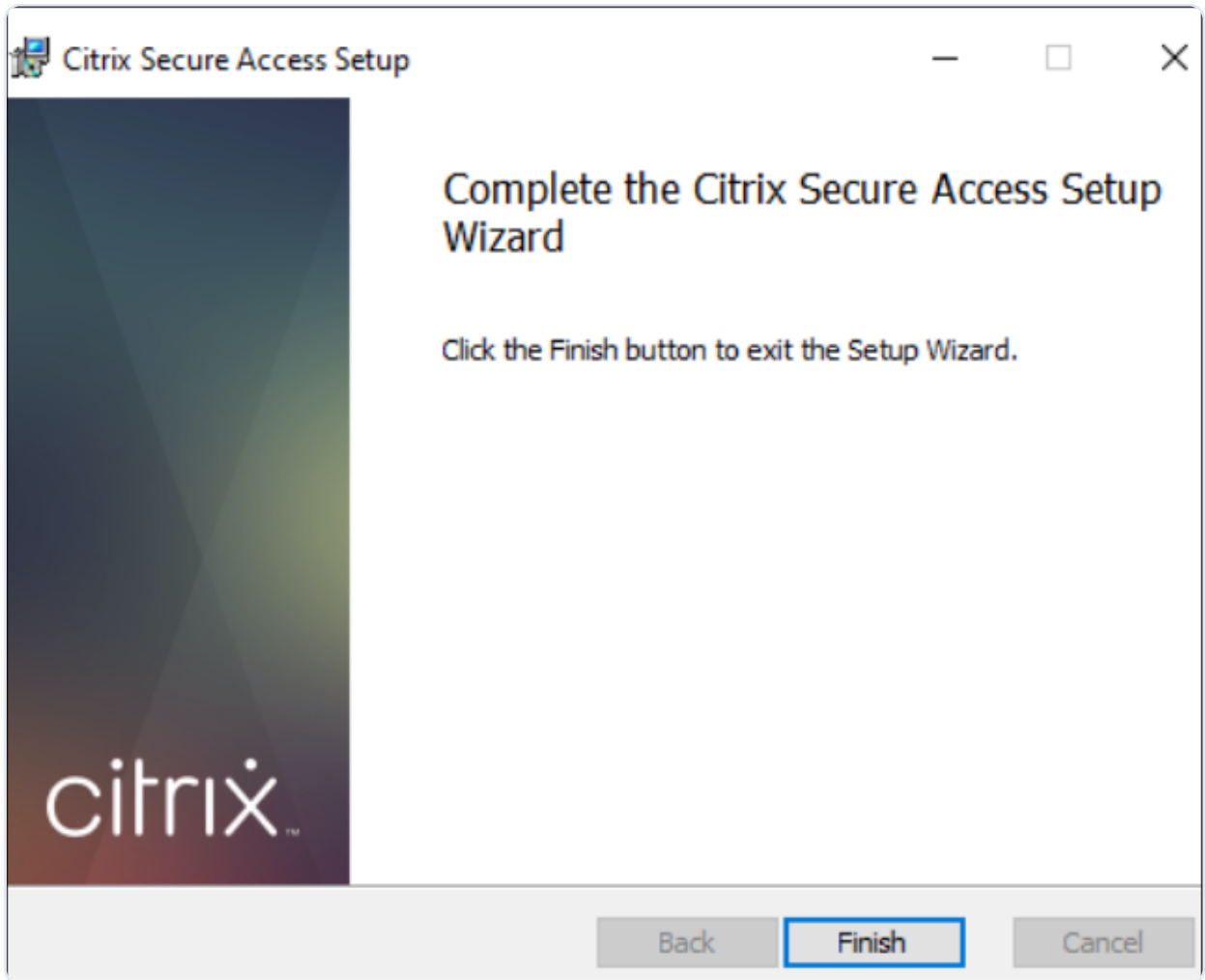
Windows 用 Citrix Secure Access クライアントのインストール

管理者権限が必要な以下の手順で、Citrix Secure Access クライアントをインストールできます。

1. [Citrix Secure Access Clients for Windows](#) から Citrix Secure Access クライアントをダウンロードします。
2. Windows マシンにクライアントをインストールするには、**インストール**をクリックします。既存の Citrix Secure Access クライアントがある場合は、それがアップグレードされます。



3. インストールを完了するには、完了をクリックします。



Windows 用 Citrix Secure Access クライアントの使用方法

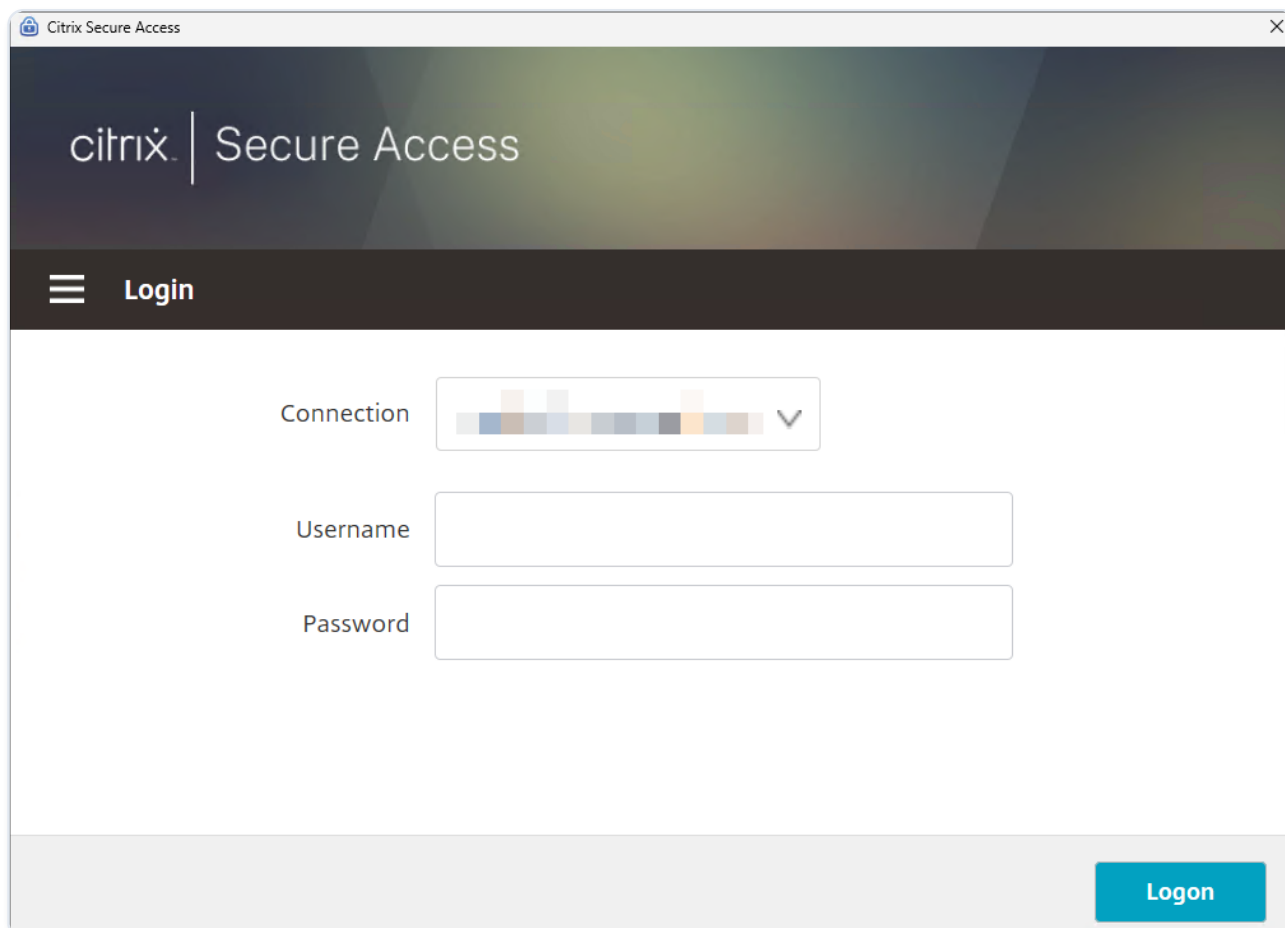
管理者がアプリケーションの接続 URL を追加していない場合、初回ユーザーは接続 URL を追加して NetScaler Gateway または Secure Private Access への接続を作成する必要があります。その後、既存の接続に接続したり、接続を追加したり、既存の接続を編集したりすることもできます。ログを表示し、それに応じて適切なアクションを実行することもできます。

接続を追加する

重要:

接続が追加されると、Citrix Secure Access クライアントは認証を要求します。プロンプトは、NetScaler Gateway または Secure Private Access で構成されている認証方法によって異なります。パスワードまたはワンタイムパスワードの入力が必要になる場合があります。あるいは、SAML 認証 URL にリダイレクトされることもあります。

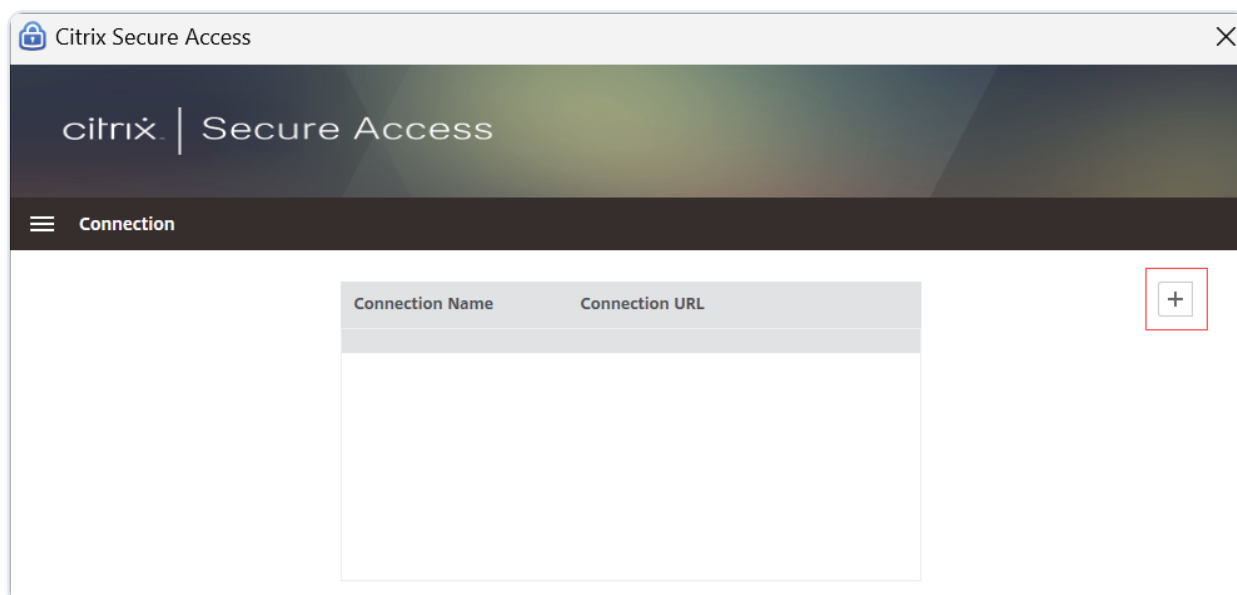
管理者がすでにアプリケーションへの接続を追加している場合は、ホームページのドロップダウンリストから接続を選択し、ユーザー名とパスワード（またはワンタイムパスワード）を入力し、**ログオン**をクリックします。



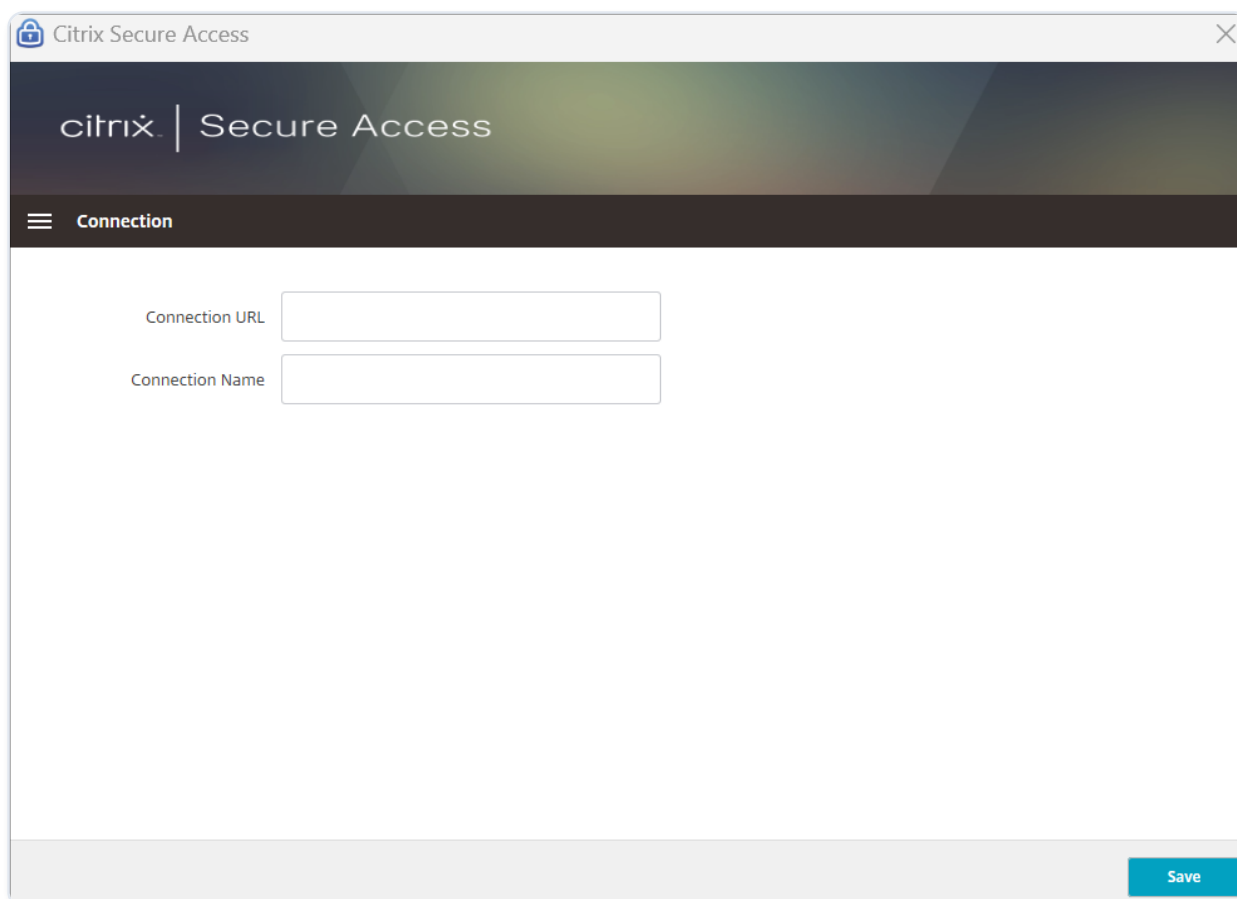
The screenshot shows the Citrix Secure Access login interface. At the top, there's a dark header with the Citrix logo and 'Secure Access' text. Below this is a dark navigation bar with a hamburger menu icon and the word 'Login'. The main content area is white and contains a 'Connection' dropdown menu with a color-coded bar, a 'Username' text input field, and a 'Password' text input field. At the bottom right, there is a blue 'Logon' button.

管理者が接続 URL を追加していない場合は、次の手順で接続を追加する必要があります。

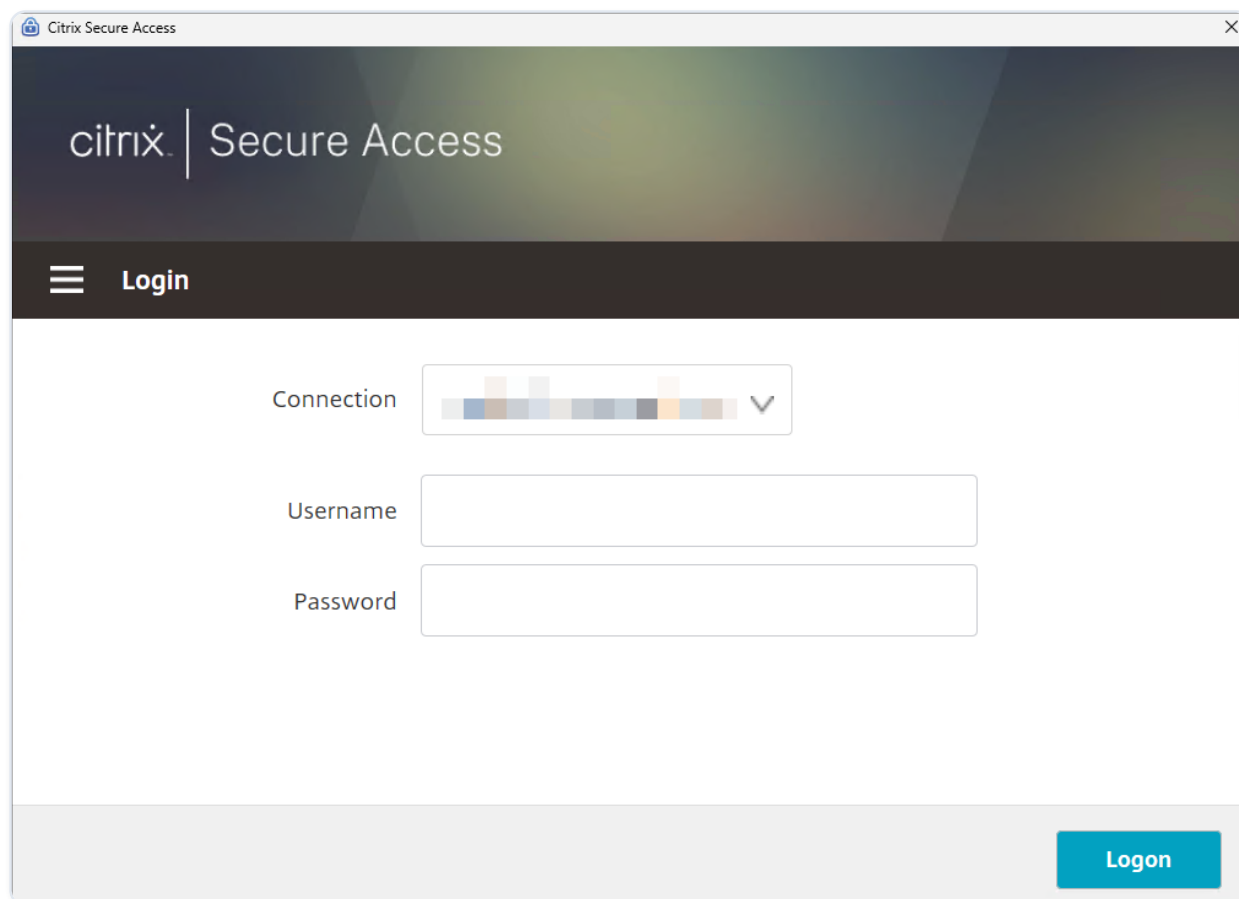
1. Windows 用 Citrix Secure Access クライアントをインストールした後、Windows マシンでアプリケーションを開きます。
2. 接続タブに移動し、**+**をクリックして接続を追加します。



3. 管理者から提供された URL を**接続 URL** テキストボックスに入力し、接続の名前を指定し、**保存**をクリックします。



4. 接続が追加されたら、**ホーム**タブに移動し、ドロップダウンリストから接続を選択し、ユーザー名とパスワード（またはワンタイムパスワード）を入力し、**ログオン**をクリックします。

A screenshot of the Citrix Secure Access login window. The window has a title bar with the Citrix logo and the text 'Citrix Secure Access'. The main header area features the 'citrix | Secure Access' logo. Below the header is a dark navigation bar with a hamburger menu icon and the word 'Login'. The main content area contains a 'Connection' dropdown menu with a color-coded bar and a downward arrow. Below this are two text input fields labeled 'Username' and 'Password'. At the bottom right, there is a blue 'Logon' button.

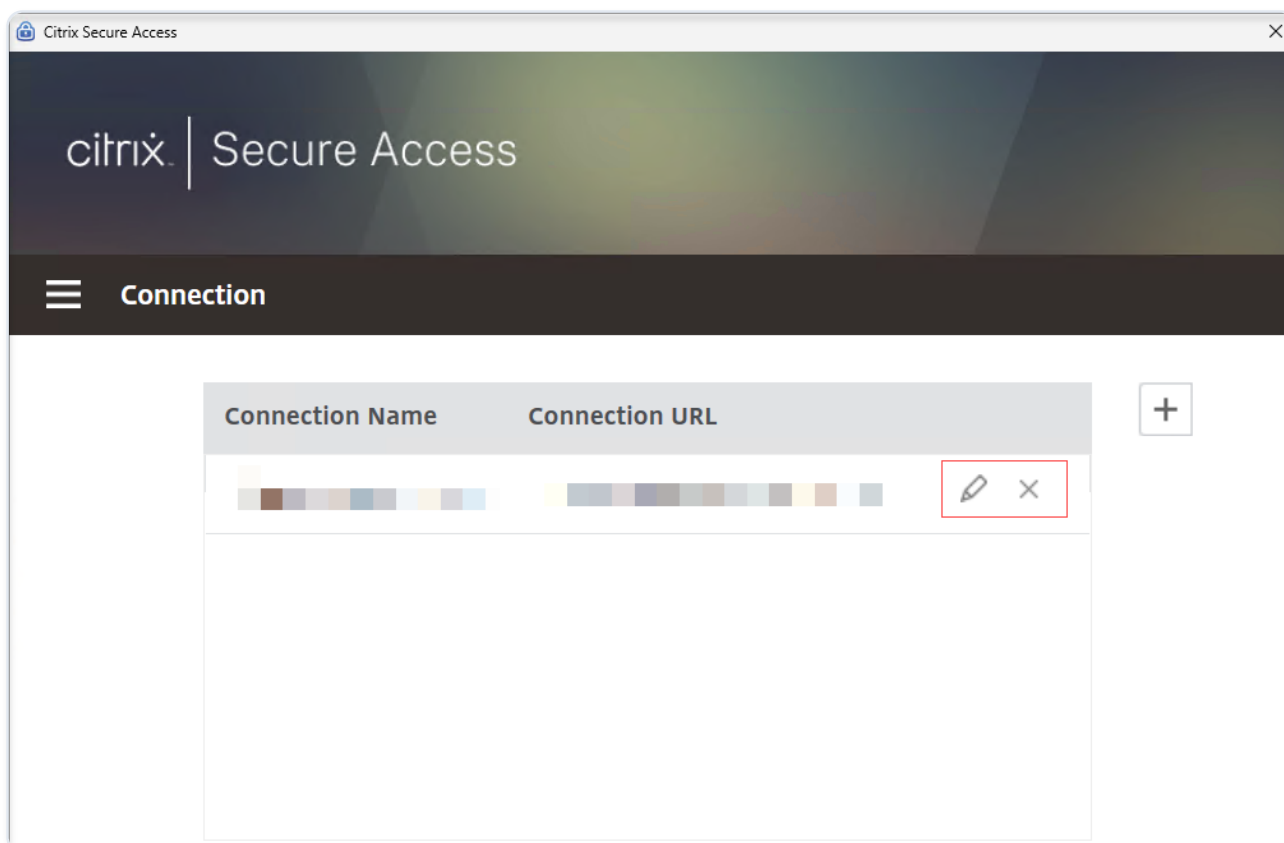
認証が成功すると、イントラネットアプリケーションにアクセスできます。

注：

初回ログイン後、管理者がNetScaler GatewayまたはSecure Private AccessでAlways OnまたはAlways On before Windows Logonプロファイルを有効にしている場合、VPNを手動で接続または切断することはできません。

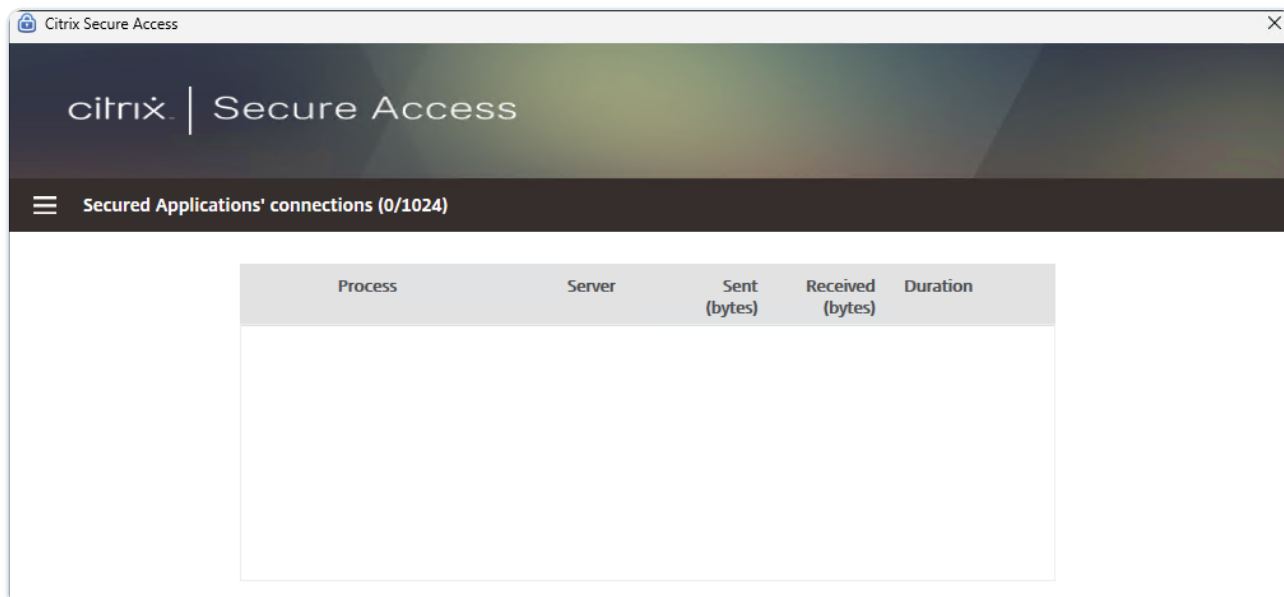
既存の接続を変更または削除する

接続タブで、編集アイコンまたはキャンセルアイコンをクリックして、既存の接続を変更または削除します。



保護されたアプリケーションを表示する

保護されたアプリケーションタブで、サーバーに接続されているアプリケーション、サーバーIP、送受信データ、および接続期間を表示できます。



ロギングを構成する

ロギングタブで、ログレベル、ファイルサイズ、およびログファイルの最大数を構成できます。

1. **ログレベルの選択**： Windows用Citrix Secure Accessクライアントには、2つのログレベルがあります。
 - **情報**： このレベルには、プログラム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。エラーと例外も含まれます。
 - **詳細**： このレベルには、**情報**レベルで報告される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。
2. **ログファイルサイズ制限**： 各ログファイルのファイルサイズを入力します。最大値は600 MBです。
3. **ログファイルの最大数**： ログ収集に追加するファイルの数を入力します。最大値は5です。
4. **保存**をクリックして、追加されたログ設定を保存します。

ログタブには、次のオプションが含まれています。

- **ログファイルをメールで送信**： ログファイルをnssslvpn.txt形式で管理者に送信します。
- **新しいログファイルを開始**： 新しいログファイルを作成します。これは通常、新しいセッションのログを新たに開始するため、またはトラブルシューティングのために特定のイベント後に使用されます。
- **ログファイルを収集**： アプリケーションのすべてのログファイルを含むzipファイルを作成します。このzipファイルはデスクトップに保存されます。
- **ログファイルを開く**： 最新のcsa_nssslvpn*.txtファイルを開きます。

The screenshot displays the Citrix Secure Access web interface. The top navigation bar includes the Citrix logo and the text 'Secure Access'. A dark sidebar on the left contains a hamburger menu icon and the word 'Logging'. The main content area is titled 'Logging' and features a configuration section. This section includes a 'Select Log Level' dropdown menu currently showing 'Info', with a list of options: 'Info', 'Verbose (Default)', and 'Debug'. Below the dropdown are two input fields: 'Log Files Size Limit (MB)' and 'Maximum Number of Log Files'. At the bottom of the page, a row of five buttons is visible: 'Email Log Files', 'Start New Log File', 'Collect Log Files', 'Open Log File', and 'Save'.

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.