Citrix Secure Access for Android

Contents

Citrix Secure Access for Android デバイス

March 15, 2024

Citrix Secure Access クライアント for Android（旧称 Citrix SSO app for Android）では、NetScaler Gateway が提供する業界屈指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利用できます。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。

> メモ：
>
> - リリース 23.12.1 以降、Citrix SSO for Android は Citrix Secure Access に名前が変更されました。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。
> - Citrix Secure Access for Android に関する管理者固有の手順については、「Citrix Secure Access for Android デバイス」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

March 15, 2024

> メモ：
>
> - リリース 23.12.1 以降、Citrix SSO for Android は Citrix Secure Access に名前が変更されました。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。
> - Citrix Secure Access for Android の使用方法に関する管理者固有の手順については、「Citrix Secure Access for Android デバイス」を参照してください。

Play ストアから Citrix Secure Access をインストールします。初めて使用する場合、MDM 以外の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。以降の使用では、MDM 展開で管理者が許可する場合、既存の接続を使用したり、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。

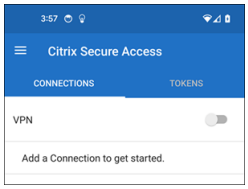
> メモ：
>
> - MDM を介して展開された接続は編集できません。
> - Citrix SSO for Android 23.8.1 以降、Citrix SSO アプリに関してすべてのパッケージに関するクエリの同意を求められる場合があります。同意すると、Citrix SSO アプリでは次の手順が発生します：
>   - Receives the package install notification from the operating system.
>   - Restarts the Always On VPN.

> 初めて VPN プロファイルに接続すると、インストールされているパッケージの情報を収集することに同意するよう求められます（Google ポリシーで要求されている）。同意すると、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。同意した後は、同意画面は再表示されません。

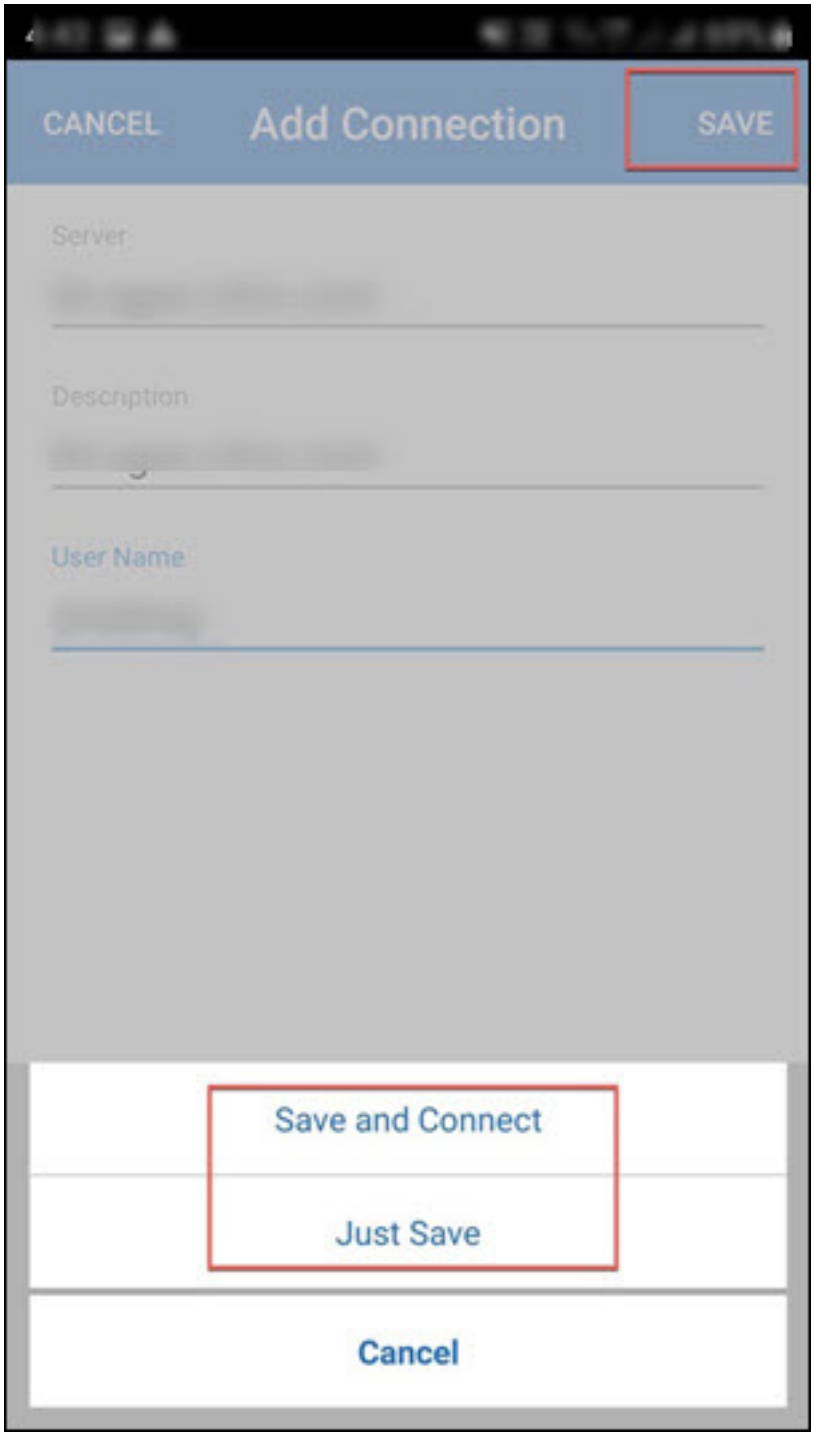
接続の追加

注：この手順は MDM 以外の場合で必要です。

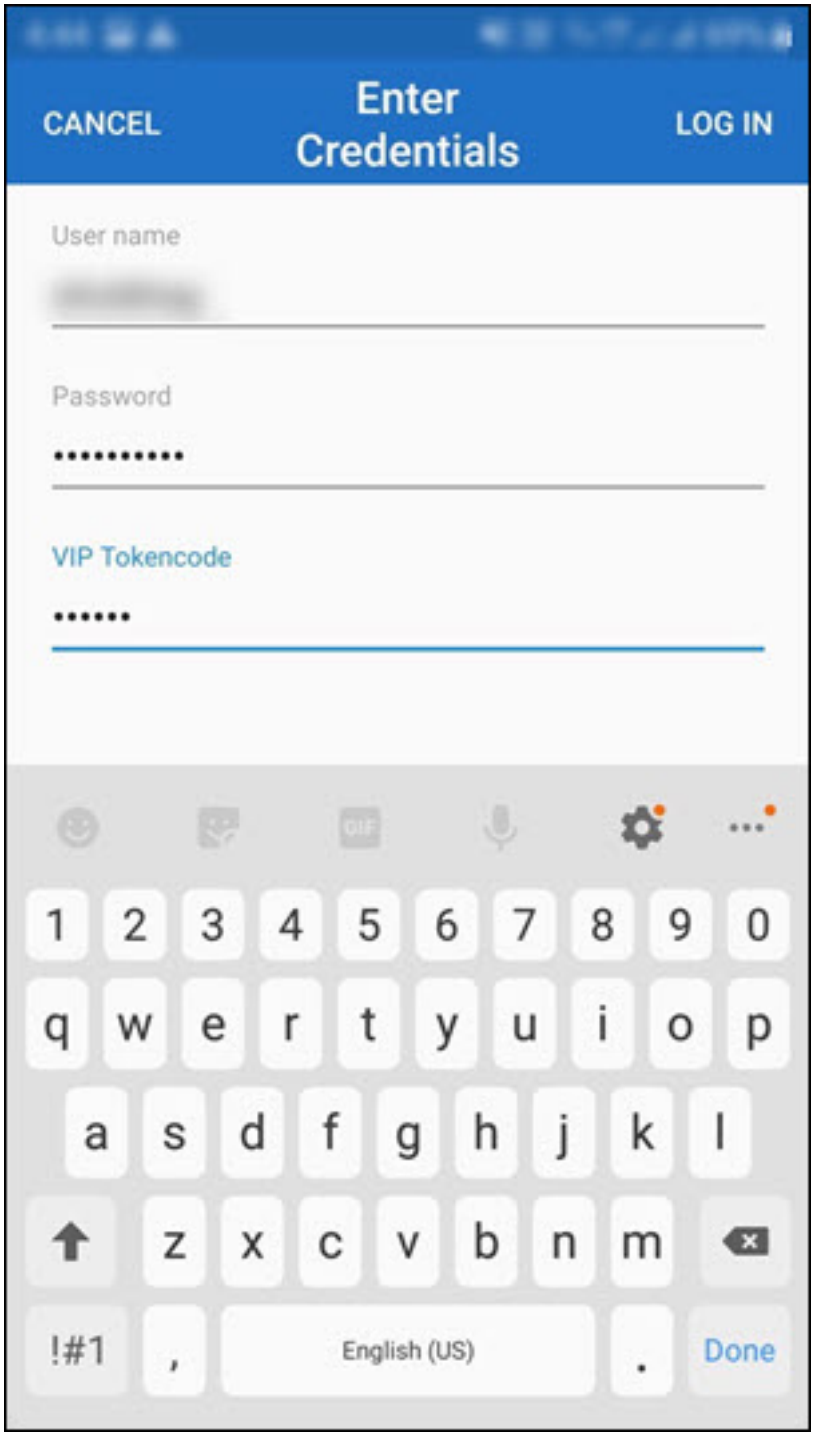
Citrix Secure Access をインストールして Android デバイスでアプリを開くと、次の画面が表示されます。



1. [+] をクリックして接続を追加します。
2. ベース URL（https://gateway.mycompany.comなど）および 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] をクリックしてから [保存して接続] か [保存のみ] のいずれかを選択します。

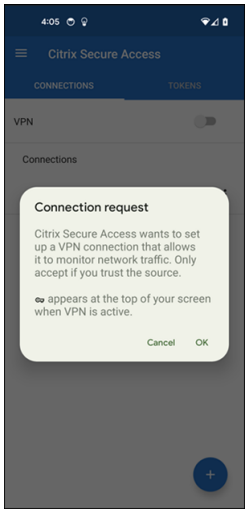


4. サーバーの認証資格情報を入力してキーパッド上で ［ログイン］または ［完了］をタップします。

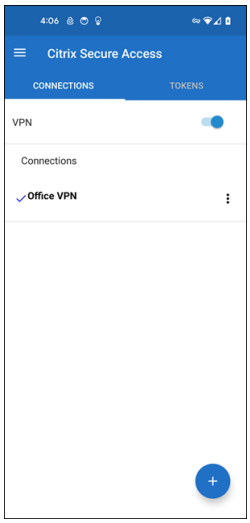


接続要求メッセージが表示されます。[**OK**] をクリックします。

注：このメッセージは、Citrix Secure Access によって初めて VPN 接続が確立されたとき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、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、このメッセージは再度表示されません。



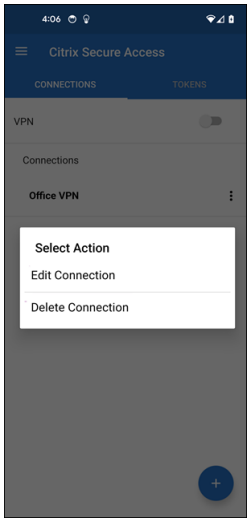
注：Citrix Secure Access からログアウトするには、**VPN** スイッチをオフにします。



既存の接続の変更または削除

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

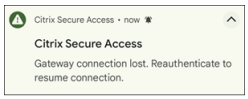
サーバー名を長押しして ［接続の編集］ または ［接続の削除］ を選択します。



VPN 接続の失敗後に **NetScaler Gateway** に再接続する（**Technical Preview**）

リリース 23.10.1 以降、Citrix SSO for Android アプリでは、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が表示されます。UI と Android デバイスの通知パネルで、NetScaler Gateway への接続が失われたため、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表示されます。

> 注:
>
> この機能はプレビュー段階です。

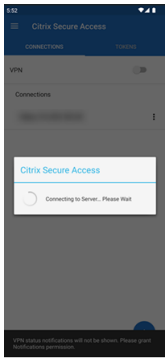


Android 13 以降のデバイスで通知を受信またはブロック

Citrix Secure Access for Android リリース 23.12.1 以降、Android 13 以降のデバイスに 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きに、Citrix Secure Access クライアントから通知を受信するための権限を提供するよう求められます。権限の提供を拒否すると、Android デバイス上の Citrix Secure Access クライアントから VPN ステータスやプッシュ通知を受信しなくなります。

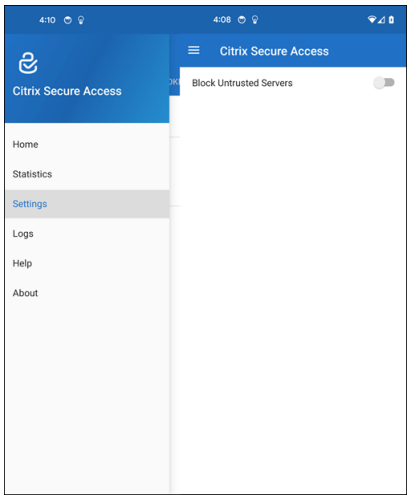
Android デバイスで ［設定］**>**［通知］に移動して、通知の権限を変更できます。

次の例では、VPN ステータス通知が無効になっています。



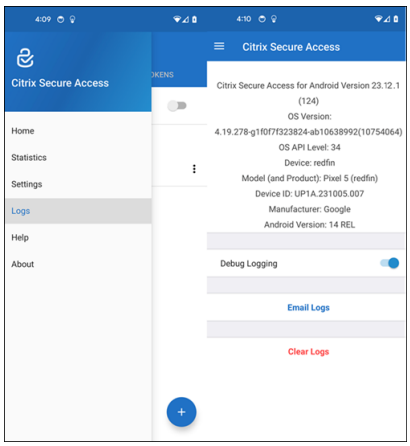
信頼されていないサーバーのブロック

デフォルトでは、Citrix Secure Access は信頼されていないサーバーに接続しません。信頼されていないサーバーとは、自己署名証明書を使用しているかまたはゲートウェイの信頼されたルート証明書がないサーバーです。これらの種類の接続を許可するには、［信頼されていないサーバーをブロックする］スイッチをオフにします。



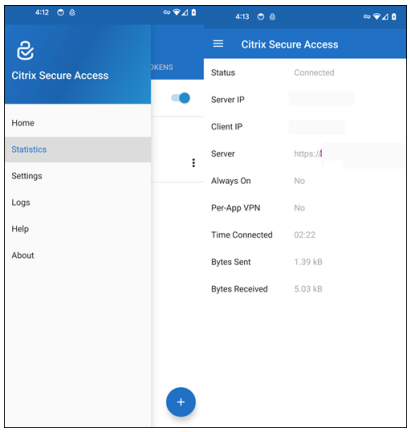
デバッグログの有効化

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で不可欠なステップです。［デバッグのログ］スイッチをオンにして、Citrix Secure Access のデバッグのログを有効にします。［ログのメール送信］リンクを使用して接続の問題をトラブルシューティングするときに、ログをメールで送信できます。



統計の表示

VPN が接続されている場合、接続の統計情報を表示できます。



パスワードトークン

第 2 要素認証として 6 桁のパスワードトークンを追加できます。このコードは時間ベースのワンタイムパスワード（OTP）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 コードをスキャンして登録できます。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第 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ノートブック上の Web ブラウザーで組織が管理するワンタイム PIN ページにログインします。
2. ［デバイスを追加］をクリックします。

3. デバイスの名前を入力し、［実行］をクリックします。

   QR コードが生成されます。

Web ブラウザーで **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. ［ホーム］ビューの ［トークン］タブに移動します。
2. [**+**]、[**QR** コードをスキャン］の順にタップします。
3. カメラのフォーカスをブラウザーの QR コードに合わせます。

Citrix Secure Access が自動的にデバイス名と秘密キーを入力します。

または、QR コードの上に表示される秘密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、プッシュ通知でゲートウェイに登録します。登録プロセスが成功すると、このトークンは［トークン］タブに正常に追加されます。

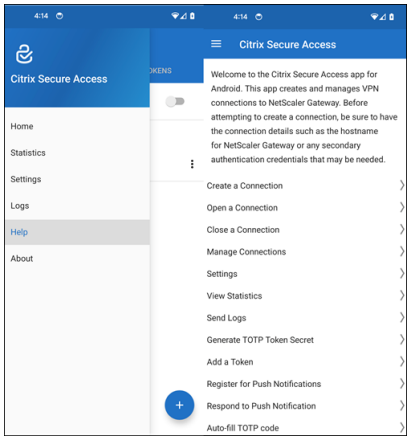
> 注:
>
> - QR コードをキャプチャするには、Citrix Secure Access にカメラへのアクセスを許可する必要があります。
> - デバイスでデバイス PIN/パスワードを有効にする必要があります。

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. [+]、［手動で入力］の順にタップします。
3. ブラウザーで生成されたパスワードトークンに表示されるデバイス名と秘密キーを入力します。

ヘルプトピック

Citrix Secure Access の使用方法について詳しくは、［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

March 15, 2024

> 注:
>
> Citrix Secure Access for Android に関する管理者固有の手順については、「Citrix Secure Access for Android デバイス」を参照してください。

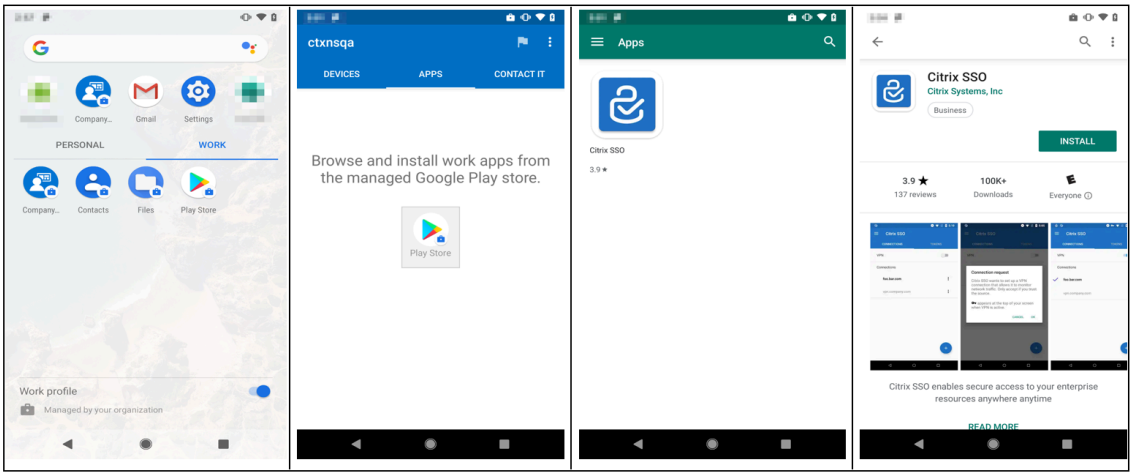
このトピックでは、Microsoft Intune の Android Enterprise 環境で構成された Citrix Secure Access クライアントを使用して企業ネットワークに接続する方法について詳しく説明します。

前提:

- Intune Company Portal アプリを使用して、デバイスを Intune に登録しました。
- デバイスで、ユーザーの仕事用プロファイルがセットアップされます。

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 ドットメニューをクリックして、アプリの設定を開き、画面の下部までスクロールします。[同期] をタップして Intune サーバーを開き、アプリのメイン画面に移動します。
3. [アプリ] タブ、[管理対象 **Google Play** ストア] リンクの順にタップします。

   ユーザーに承認済みアプリの一覧が表示されます。



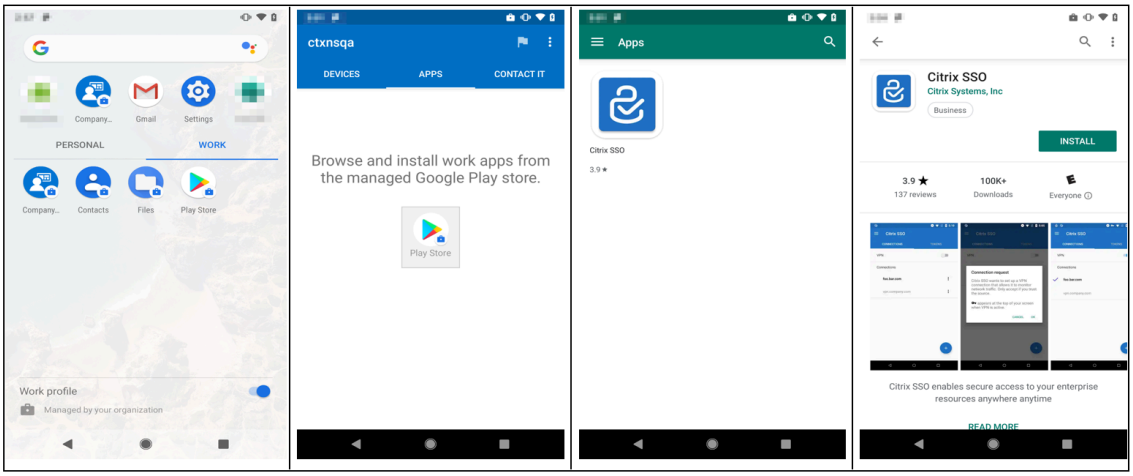
4. [**Citrix Secure Access**] をタップします。

   Citrix Secure Access クライアントが管理対象 Google Play ストアに表示されます。

5. [インストール] をタップします。

6. 仕事用プロファイルのアプリ一覧に戻ります。Citrix Secure Access がインストール済みアプリの一覧に追加されています。

7. 仕事用プロファイルのアプリ一覧で、Citrix Secure Access のアイコンをタップして開きます。



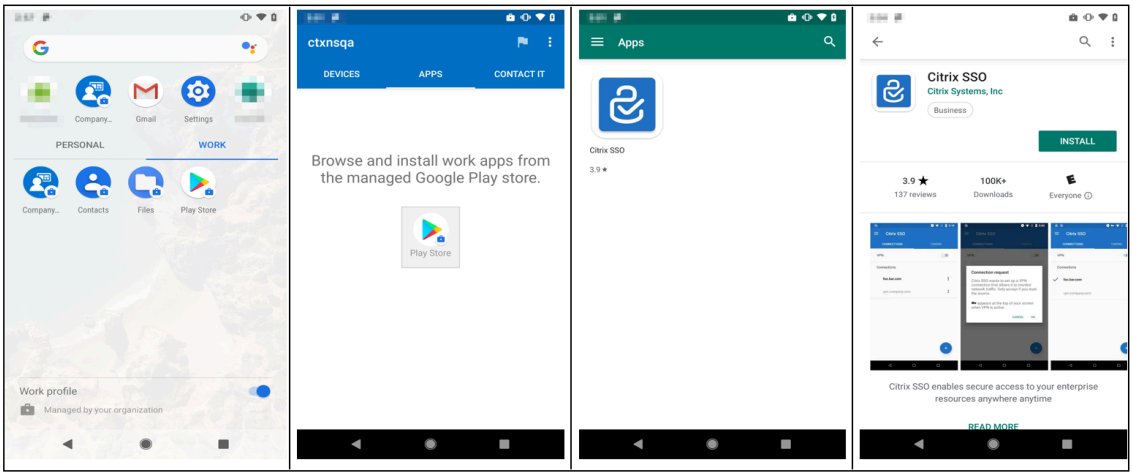
   Citrix Secure Access が開きます。企業の社内ネットワークと安全に通信する権限を許可するか拒否するかを求められます。

8. 権限を許可するには、[許可] をタップします。[許可しない] を選択すると、Citrix Secure Access が終了し、Citrix Secure Access クライアントを使用できなくなります。

   > 注:
   >
   > 管理および通話のための権限を許可または拒否するよう求められることがあります（Intune で許可されていない場合）。権限を許可するには、[許可] をタップします。この権限を拒否することはできますが、

> 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企業の社内ネットワークに接続できません。

9. **My Corporate VPN**（または Intune の Citrix Secure Access 構成で選択した名前）が［接続］タブの［管理対象の接続］セクションに表示されます。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 に認証するための資格情報を入力して ［ログイン］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、証明書を選択するよう求められることがあります。証明書へのアクセスを提供できます。

11. VPN トンネルのセットアップで Android システムから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 が企業の社内ネットワークとセキュアな接続を確立できる権限を付与します。

    注：このプロンプトは、初めて NetScaler Gateway へのセキュアな接続を確立するときにのみ表示されます。Citrix Secure Access がアンインストールされ、デバイスに再度インストールされない限り、以降の接続では表示されません。

企業の社内ネットワークに接続されます。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 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が接続済みに変わり、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。