



# Citrix SSO for iOS

## Contents

<b>Citrix Secure Access for iOS</b> デバイス	<b>2</b>
<b>Citrix Secure Access</b> アプリでの証明書のインポートとインストール	<b>2</b>
<b>iOS</b> デバイスから <b>Citrix Secure Access</b> を使用する方法	<b>5</b>

## Citrix Secure Access for iOS デバイス

March 15, 2024

Citrix Secure Access for iOS 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。

Citrix Secure Access アプリは、iOS での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。

**重要:**

- リリース 23.11.1 以降、Citrix SSO for iOS 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 SSO for iOS に関する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。

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

March 15, 2024

**重要:**

- リリース 23.11.1 以降、Citrix SSO for iOS 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 iOS に関する管理者固有の手順については、「[Citrix Secure Access for iOS および Citrix Secure Access for macOS](#)」を参照してください。

iOS 上の 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、次の方法で Citrix Secure Access に配信できます:

- **MDM サーバー** - MDM を使用のお客様の優先アプローチです。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を参照してください。
- **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。管理者は、ユーザー証明書 ID (証明書と秘密キー) を PKCS#12 ファイルとして添付したメールを送信します。ユーザーが添付ファイル付きのメールを受

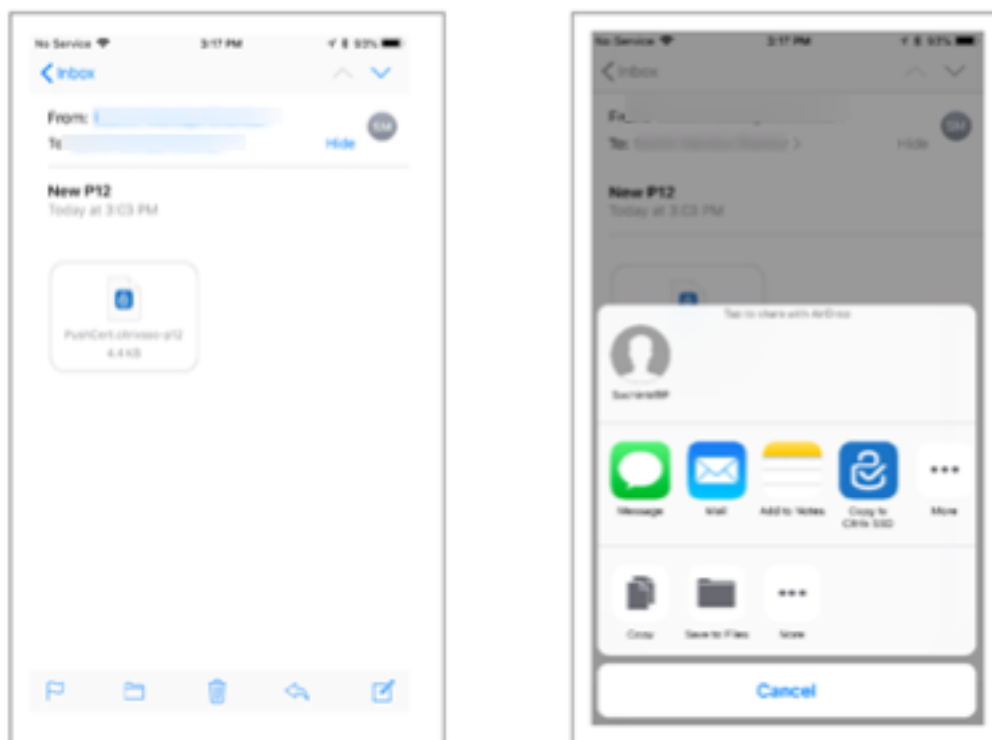
信するには、iOS デバイスでメールアカウントを設定する必要があります。その後、このファイルを iOS 上の Citrix Secure Access にインポートできます。

注:

ファイル名拡張子 **.pfx** および **.p12** は、iOS システムによって要求され、Citrix Secure Access などのサードパーティ製アプリでは要求できません。したがって、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（証明書と秘密キー）が PKCS#12 ファイルとして添付されたメールを開きます。

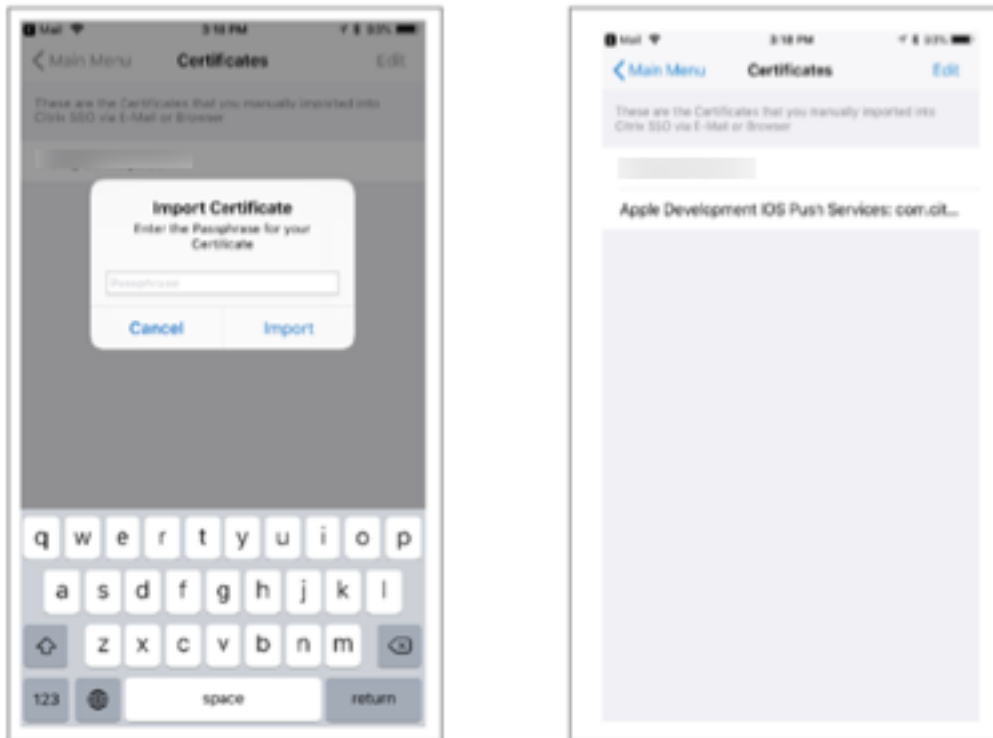
- システムの **OpenIn** メニューを表示するには添付ファイルをタップします。
- **[Copy to Citrix SSO]** をタップします。



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

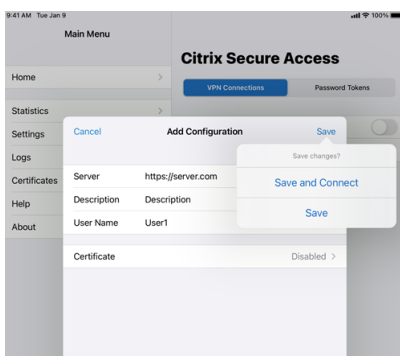
これでアプリが起動し、証明書パスフレーズのプロンプトが表示されます。証明書をアプリのキーチェーンにインストールするための正しいパスフレーズを入力して **[インポート]** をクリックします。

検証に成功すると、証明書がインポートされます。

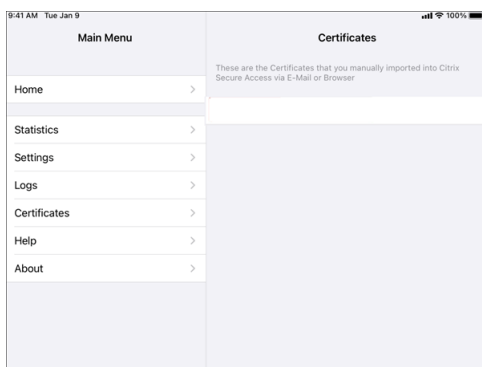


3. VPN で証明書ベースの認証を使用します。

- 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] ビューに移動して [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] セクションのインポートされた証明書を選択します。



- [保存] をタップして証明書をインポートします。



#### 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、メインメニューで [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

March 15, 2024

### 重要:

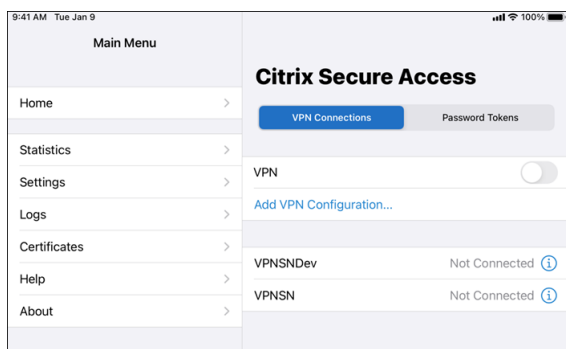
- リリース 23.11.1 以降、Citrix SSO for iOS は Citrix Secure Access に名前が変更されました。この名前の変更を反映するために、ドキュメントと UI スクリーンショットを更新中です。
- Citrix Secure Access for iOS に関する管理者固有の手順については、「[Citrix Secure Access for macOS/iOS](#)」を参照してください。

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に初めて使用する場合、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 回目以降の使用では、既存の接続を使用したり、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。

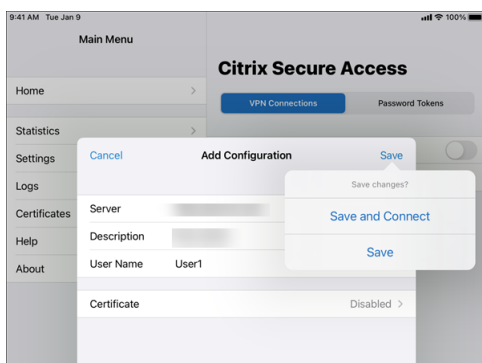
MDM のお客様の場合、デバイスを登録するときに自動的に表示される VPN 接続を管理者が事前構成していることがあります。この接続を選択し VPN スイッチをオンにすると、接続を直接開始できます。これらの VPN 接続はユーザーが編集できません。

### 接続の追加

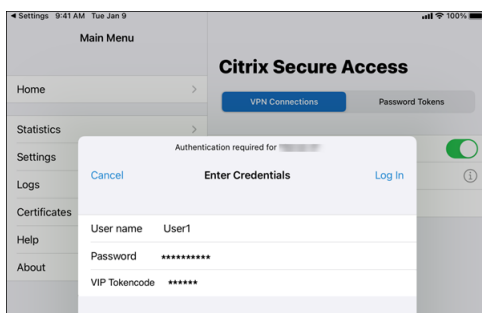
Citrix Secure Access をインストールしてアプリを開くと、次の画面が表示されます。



1. [VPN 構成を追加] をタップして新しい接続を追加します。
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、[保存して接続] または [保存] 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 [ログイン] をタップします。



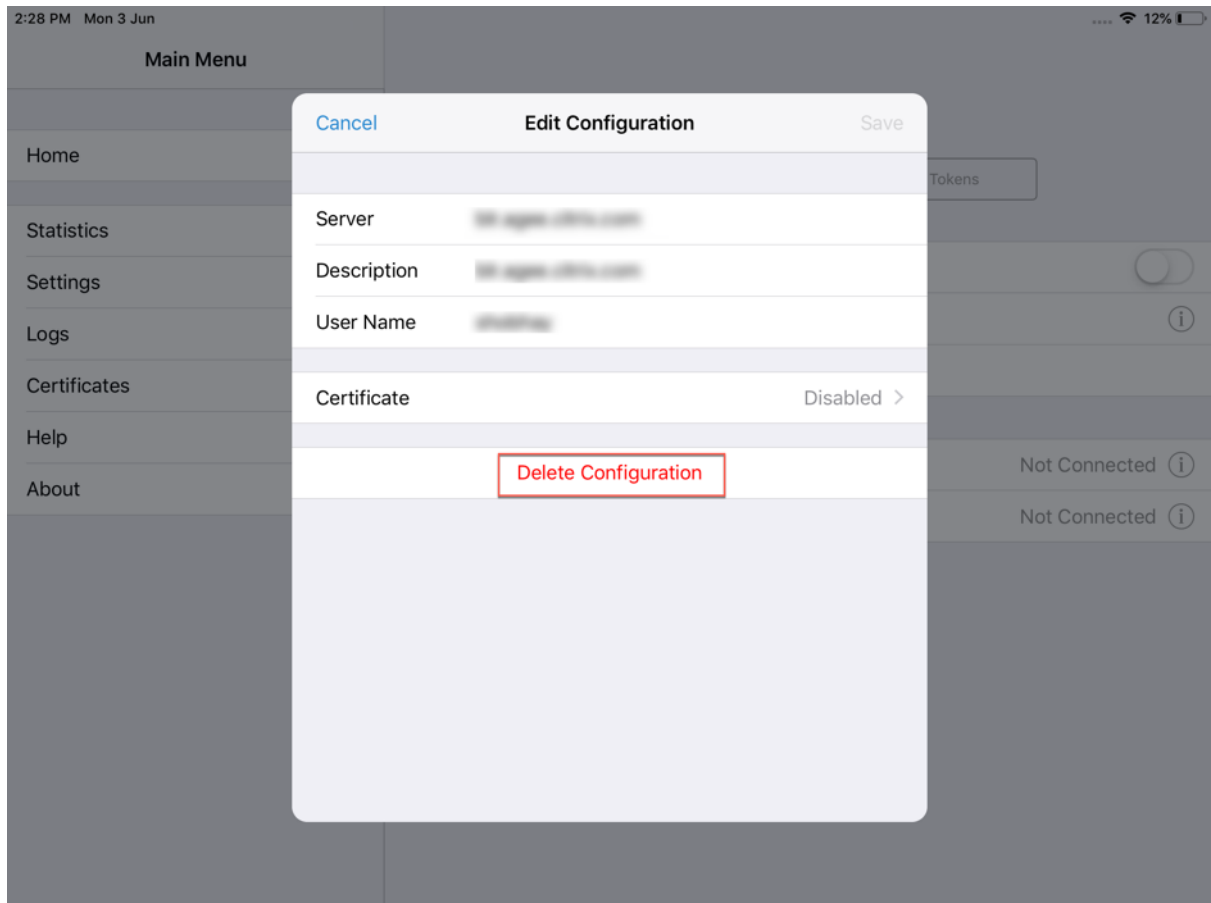
注: Citrix Secure Access からログアウトするには、VPN をオフにします。

## VPN 接続の失敗後に NetScaler Gateway に再接続する

リリース 23.09.1 以降、Citrix SSO for iOS 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。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という通知が UI に表示されます。

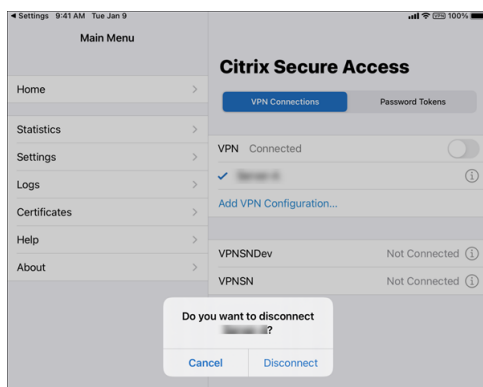
## 既存の接続の削除

接続の横にあるアイコンをタップし、[構成の削除] を選択します。



## 接続の切断

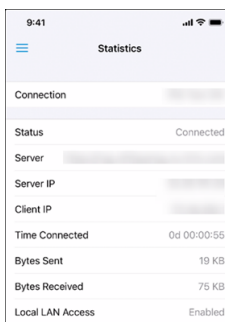
VPN スイッチをオフに切り替えてから、[切断] をタップします。





## 統計の表示

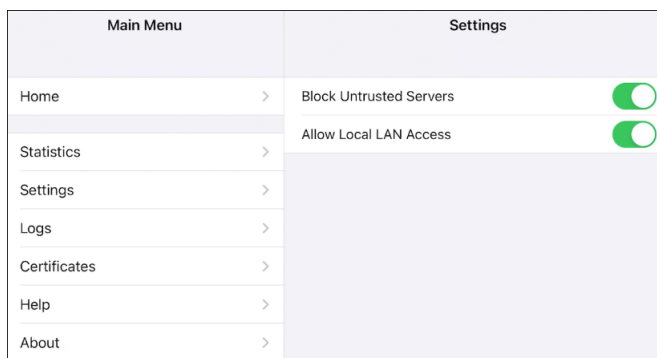
VPN が接続されている場合、接続の統計情報を表示できます。



Statistics	
Connection	
Status	Connected
Server	
Server IP	
Client IP	
Time Connected	0d 00:00:55
Bytes Sent	19 KB
Bytes Received	75 KB
Local LAN Access	Enabled

## 信頼されていないサーバーのブロック

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）に接続しません。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。



Main Menu	Settings
Home >	Block Untrusted Servers <input checked="" type="checkbox"/>
Statistics >	Allow Local LAN Access <input type="checkbox"/>
Settings >	
Logs >	
Certificates >	
Help >	
About >	

## ローカル LAN アクセス

Citrix SSO for iOS 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 接続の確立後に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 アクセスを構成するには、次の手順を実行します：

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 アクセスを許可する] 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。

## ログの送信

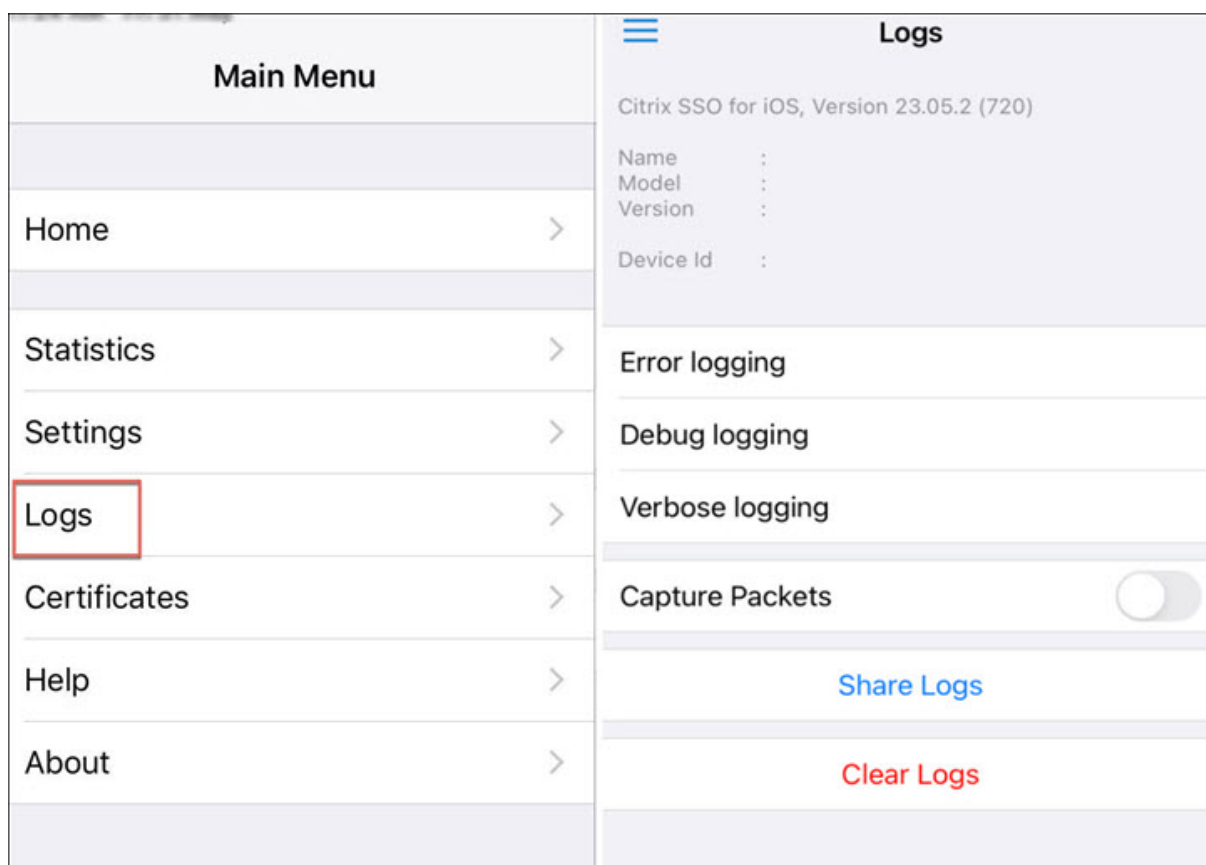
デバッグログのキャプチャは、トラブルシューティングや Citrix サポートへの問題報告で不可欠なステップです。

デバッグログを取得して共有する手順は次のとおりです：

1. [デバッグのログ] スイッチをオンにします。
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：

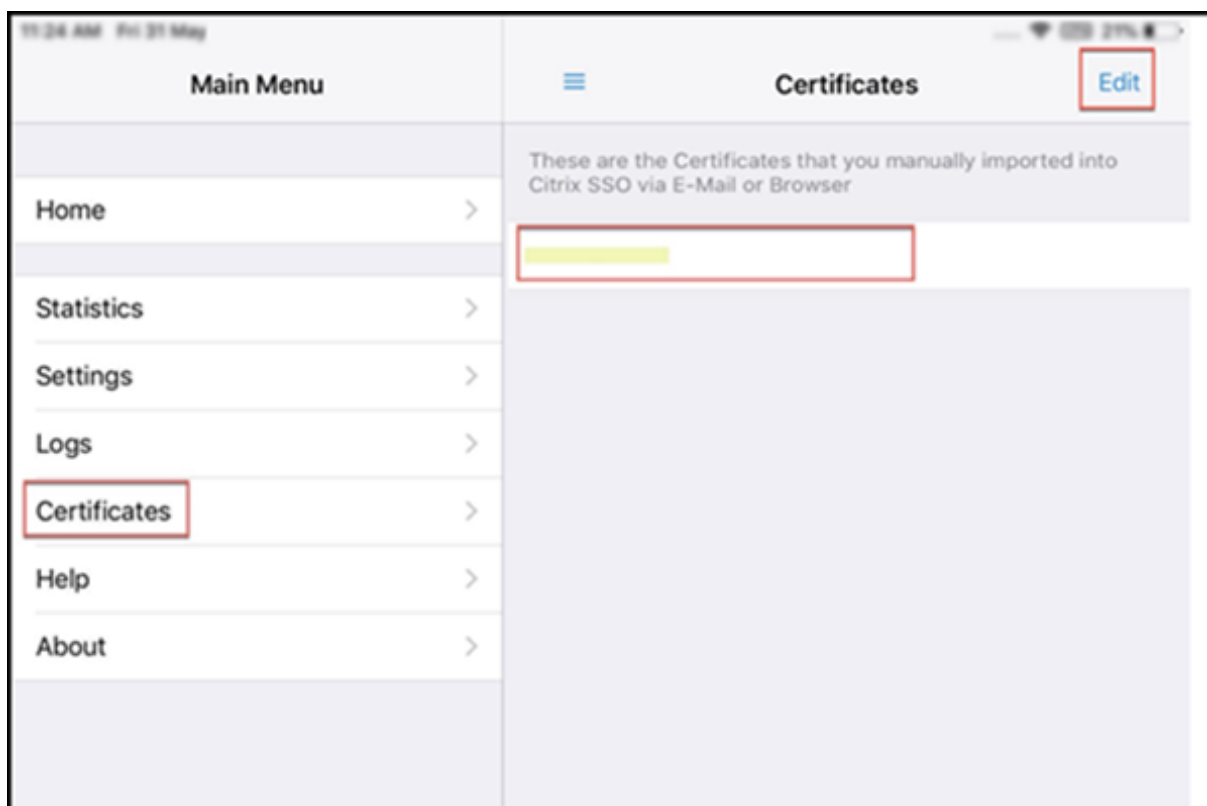
- 新しいログのセットを生成するには、まず [ログのクリア] を使用して古いログを削除します。
- リリース 23.07.1 以降、[ログのメール送信] オプションは [ログの共有] オプションに置き換えられます。[ログの共有] には、圧縮されたログファイルを共有するためのさまざまなオプションが用意されています。



## クライアント証明書の表示

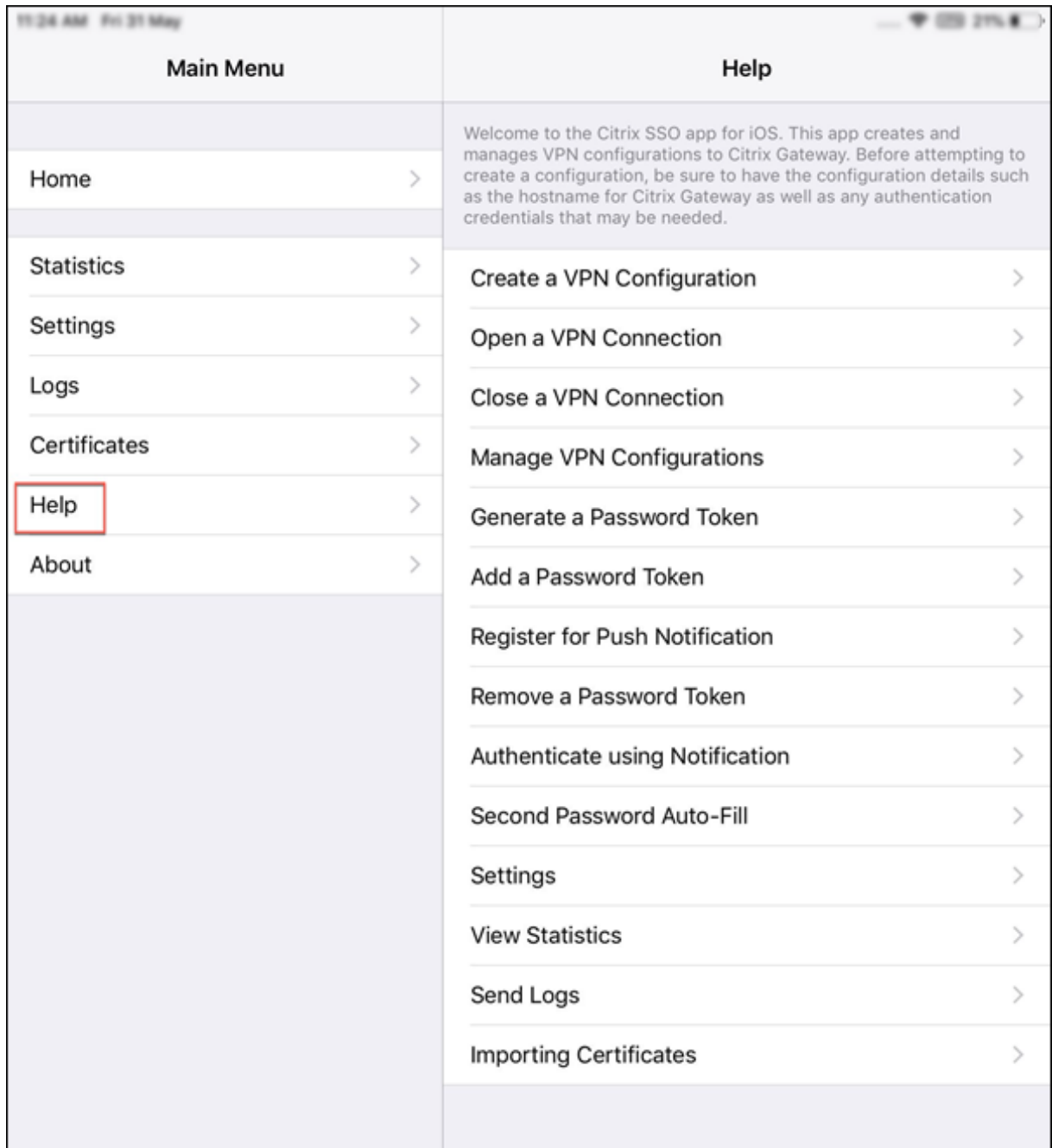
Citrix Secure Access にインポートされたクライアント証明書を表示できます。インポートされた証明書が [証明書] セクションに表示されます。次のいずれかの方法で証明書を削除できます。

- 証明書セルで右から左にスライドして [削除] ボタンを表示させます。[削除] をタップします。
- [編集] をタップして [削除] ボタンを表示させ、[削除] をタップします。



## ヘルプトピック

さまざまな項目のヘルプについては、[ヘルプ] を参照してください。





© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).