



# Secure Hub

## Contents

<b>Citrix Secure Hub</b>	<b>2</b>
既知の問題と解決された問題	<b>37</b>
認証を求められるシナリオ	<b>40</b>
派生資格情報を使用したデバイスの登録	<b>45</b>
<b>Citrix Endpoint Management</b> コンソールを使用したヒントの構成	<b>53</b>

## Citrix Secure Hub

June 6, 2024

Citrix Secure Hub は、業務用モバイルアプリへの入り口です。ユーザーは Secure Hub にデバイスを登録して、アプリストアにアクセスします。アプリストアから、Citrix の業務用モバイルアプリとサードパーティ製アプリを追加できます。

Secure Hub およびその他のコンポーネントは、[Citrix Endpoint Management のダウンロードページ](#)からダウンロードできます。

Secure Hub および業務用モバイルアプリの他のシステム要件については、「[システム要件](#)」を参照してください。

業務用モバイルアプリの最新情報については、「[最新の情報](#)」を参照してください。

次のセクションでは、Secure Hub の最新リリースおよび以前のリリースの新機能について説明します。

注:

Secure Hub の Android 6.x および iOS 11.x バージョンのサポートは、2023 年 10 月に終了しました。

最新バージョンの新機能

### Secure Hub for iOS 24.5.0

#### iOS 17 の Return to Service (サービスに戻す) をサポート

Secure Hub は iOS 17 の Return to Service (サービスに戻す) 機能をサポートしており、より効率的で安全なモバイルデバイス管理 (MDM) エクスペリエンスを提供します。以前は、デバイスをワイプした後、新しいユーザー用に設定するには手動で構成する必要がありました。現在、Return to Service 機能により、会社のデバイスを再利用する場合でも、個人のデバイス (BYOD) を適切なセキュリティポリシーと統合する場合でも、このプロセスが自動化されます。

Return to Service 機能を使用すると、MDM サーバーは Wi-Fi の詳細とデフォルトの MDM 登録プロファイルを含む消去コマンドをユーザーデバイスに送信できます。その後、デバイスはすべてのユーザーデータを自動的に消去し、指定された Wi-Fi ネットワークに接続し、提供された登録プロファイルを使用して MDM サーバーに再登録します。

以前のバージョンの新機能

### Secure Hub for Android 24.3.0

**Samsung Knox Enhanced Attestation v3** のサポート Secure Hub は、Samsung Enhanced Attestation v3 をサポートするようになりました。これにより、Knox 構成証明を活用して、Citrix Endpoint Management を

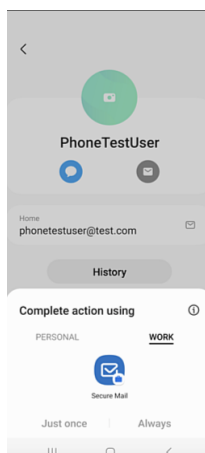
通じて管理される Samsung デバイスのセキュリティ対策が強化されます。この高度な構成証明プロトコルは、デバイスの整合性とセキュリティのステータスを検証し、デバイスがルータ化されていないこと、および承認されたファームウェアが実行されていることを確認します。この機能は、セキュリティの脅威に対して重要な保護機能を提供し、企業のセキュリティポリシーへの遵守を保証します。

### Secure Hub for Android 23.12.0

**Samsung Knox** によるセキュリティ強化 Citrix Endpoint Management に Knox Platform for Enterprise Key デバイスポリシーを追加すると、Samsung デバイス上の Secure Hub のセキュリティ機能が大幅に強化されます。このポリシーにより、必要な Samsung Knox Platform for Enterprise (KPE) ライセンス情報を提供し、KPE ライセンスを使用して Samsung デバイスのセキュリティを強化できます。Samsung Knox は、企業データの保護を維持しながら、管理を容易にしてスムーズなユーザーエクスペリエンスを実現します。

詳しくは、「[Knox Platform for Enterprise Key デバイスポリシー](#)」を参照してください。

ユーザーの個人プロフィールから **Secure Mail** にアクセスする ユーザーは、個人プロフィールから仕事用プロフィールの Secure Mail にアクセスして使用できるようになりました。ユーザーが個人プロフィールのアドレス帳でメールアドレスをクリックすると、仕事用プロフィールで Secure Mail を使用するオプションが表示されます。これによって、ユーザーは個人プロフィールからメールを送信できます。この機能は、BYOD または WPCOD デバイスで利用できます。



### Secure Hub for iOS 24.1.0

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。

### Secure Hub for Android 23.12.0

サインインページに認証 PIN に関するヒントを追加する 23.12.0 リリース以降、サインインページに認証 PIN に関するヒントを追加できるようになりました。この機能はオプションであり、2 要素認証に登録されたデバイスに適

用されます。ヒントにより、PIN にアクセスする方法がわかります。

ヒントはテキストまたはリンクとして構成できます。ヒントのテキストでは PIN に関する簡単な情報が提供され、リンクでは PIN へのアクセス方法に関する詳細情報が提供されます。ヒントの構成方法について詳しくは、「[Citrix Endpoint Management コンソールを使用したヒントの構成](#)」を参照してください。

**nFactor** 認証によるシングルサインオン機能のサポート Secure Hub for Android バージョン 23.12.0 以降、nFactor のモバイルアプリケーション管理 (MAM: Mobile Application Management) 登録またはログインはシングルサインオン (SSO) 機能をサポートします。この機能により、以前に入力したサインイン資格情報が MAM 登録またはログインプロセスを通過できるため、ユーザーが再度手動でサインイン資格情報を入力する必要がなくなります。nFactor SSO プロパティについて詳しくは、Citrix Endpoint Management ドキュメントの「[クライアントプロパティリファレンス](#)」を参照してください。

直接起動モードでの完全なワイプのサポート 以前は、再起動したデバイスで完全なワイプコマンドを実行するには、デバイスのロックを解除する必要がありました。今回、デバイスがロックされている場合でも、直接起動モードで完全なワイプコマンドを実行できるようになりました。この機能は、特にデバイスが権限のない個人によって所有されている場合に、セキュリティの観点から役立ちます。完全なワイプコマンドについて詳しくは、Citrix Endpoint Management のドキュメントの「[セキュリティ操作](#)」を参照してください。

**Secure Hub** の **App Store** の読み込み速度を最適化 Secure Hub の App Store の読み込みが以前より速くなり、ユーザーはより迅速にアクセスできるようになりました。

### Secure Hub for iOS 23.11.0

サインインページに認証 **PIN** に関するヒントを追加する 23.11.0 リリース以降、サインインページに認証 PIN に関するヒントを追加できるようになりました。この機能はオプションであり、2 要素認証に登録されたデバイスに適用されます。ヒントにより、PIN にアクセスする方法がわかります。

ヒントはテキストまたはリンクとして構成できます。ヒントのテキストでは PIN に関する簡単な情報が提供され、リンクでは PIN へのアクセス方法に関する詳細情報が提供されます。ヒントの構成方法について詳しくは、「[Citrix Endpoint Management コンソールを使用したヒントの構成](#)」の記事を参照してください。

**nFactor** 認証によるシングルサインオン機能のサポート Secure Hub for iOS バージョン 23.11.0 以降、nFactor のモバイルアプリケーション管理 (MAM: Mobile Application Management) 登録またはサインインはシングルサインオン (SSO) 機能をサポートします。この機能により、以前に入力したサインイン資格情報が MAM 登録またはサインインプロセスを通過できるため、ユーザーが再度手動でサインイン資格情報を入力する必要がなくなります。

nFactor SSO プロパティについて詳しくは、Citrix Endpoint Management ドキュメントの「[クライアントプロパティリファレンス](#)」を参照してください。

## Secure Hub 23.10.0

### Secure Hub for Android

Secure Hub for Android 23.10.0 は Android 14 をサポートしています。Secure Hub バージョン 23.10.0 にアップグレードすると、Android 14 に更新されたデバイスが引き続きサポートされます。

## Secure Hub 23.9.0

### Secure Hub for Android

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

## Secure Hub 23.8.1

**Secure Hub for iOS** 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。

## Secure Hub 23.8.0

**Secure Hub for iOS** 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。

## Secure Hub 23.7.0

### Secure Hub for Android

**Play Integrity API** SafetyNet Attestation API は、廃止予定のタイムラインに従って Google によって間もなく廃止され、推奨されている Play Integrity API に移行します。

詳しくは、Citrix Endpoint Management のドキュメントの「[Play Integrity API](#)」を参照してください。

廃止予定のタイムラインについて詳しくは、Citrix Endpoint Management のドキュメントの「[廃止と削除](#)」を参照してください。

Android の SafetyNet 機能については、「[SafetyNet](#)」を参照してください。

## Secure Hub 23.4.0

### Secure Hub for iOS

ユーザーエクスペリエンスの向上 バージョン 23.4.0 以降、Secure Hub for iOS では次のユーザーエクスペリエンスが向上しています：

- ストアエクスペリエンス

☒ 以前は、[マイアプリ] ページが最初に表示されていました。バージョン 23.4.0 では、[ストア] ページが最初に表示されます。

☒ 以前は、ユーザーが [ストア] オプションをクリックするたびに、Secure Hub ストアは再読み込み操作を実行していました。

バージョン 23.4.0 では、ユーザーエクスペリエンスが向上しています。今後は、ユーザーが初めてアプリを起動したとき、アプリを再起動したとき、または画面を下にスワイプしたときに、アプリが再読み込みされるようになりました。

- ユーザーインターフェイス：以前は、[サインオフ] オプションは画面の左下に配置されていました。23.4.0 バージョンでは、[サインオフ] オプションはメインメニューの一部で、[バージョン] オプションの上にあります。

- ハイパーリンク：以前は、アプリの詳細ページのハイパーリンクはプレーンテキストとして表示されていました。バージョン 23.4.0 では、ハイパーリンクをクリックできるようになり、リンクを示す下線の書式が設定されています。

**MDX から MAM SDK への移行エクスペリエンス** バージョン 23.4.0 以降、レガシ MDX から MAM SDK への移行エクスペリエンスが iOS デュアルモードアプリ向けに強化されています。この機能は、通知メッセージの数を減らし、Secure Hub に切り替えることで、業務用モバイルアプリを使用するときのユーザーエクスペリエンスを向上させます。

**Citrix PIN** を使用したアプリのロックの解除 以前は、エンドユーザーはデバイスのパスコードを入力して、モバイルアプリ管理 (MAM) に基づいてアプリのロックを解除していました。

バージョン 23.4.0 以降、エンドユーザーはパスコードとして Citrix PIN を入力して、MAM ベースのアプリのロックを解除できるようになります。管理者は、CEM サーバー上のクライアントプロパティを使用してパスコードの複雑さを設定できます。

アプリが許可された時間を超えて非アクティブな場合、エンドユーザーは管理者が設定した構成に応じて Citrix PIN を入力し、アプリのロックを解除できます。

Android 向け Secure Hub の場合、MAM アプリケーションで非アクティブタイマーに対応する方法を構成するための別のクライアントプロパティがあります。詳しくは、「[Android 向けの個別の非アクティブタイマー](#)」を参照してください。

### Secure Hub 23.4.1

**Secure Hub for Android** 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。

### Secure Hub 23.4.0

**Secure Hub for Android** 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。

### Secure Hub 23.2.0

#### Secure Hub for Android

注:

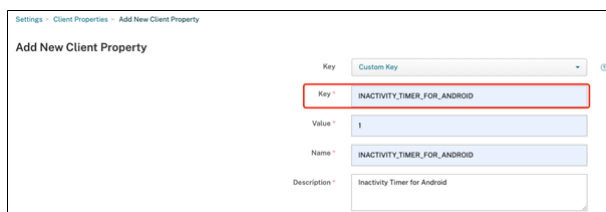
- 欧州連合 (EU)、欧州経済領域 (EEA)、スイス、および英国 (UK) のユーザーの分析データは収集されません。

**MDX 完全トンネルモード VPN** MDX マイクロ VPN (完全トンネルモード) は廃止されました。

詳しくは、Citrix Endpoint Management のドキュメントの「[廃止](#)」を参照してください。

**Android** 用の個別の非アクティブタイマー 以前は、非アクティブタイマーのクライアントプロパティは Android および iOS の Secure Hub で共通でした。

バージョン 23.2.0 以降、IT 管理者は新しいクライアントプロパティ **Inactivity\_Timer\_For\_Android** を使用して、非アクティブタイマーを iOS から分離できます。IT 管理者は、**Inactivity\_Timer\_For\_Android** の値を 0 に設定して、Android の非アクティブタイマーを個別に無効にできます。この場合、Secure Hub を含む仕事用プロフィール内のすべてのアプリは、PIN のみで機能します。



The screenshot shows a form titled "Add New Client Property" with the following fields:

Key	Custom Key
Key	INACTIVITY_TIMER_FOR_ANDROID
Value	1
Name	INACTIVITY_TIMER_FOR_ANDROID
Description	Inactivity Timer for Android

クライアントプロパティの追加および変更について詳しくは、XenMobile のドキュメントの「[クライアントプロパティ](#)」を参照してください。

### Secure Hub 22.11.0

**Secure Hub for Android** このリリースには、バグの修正が含まれています。



## Secure Hub 22.9.0

**Secure Hub for Android** このリリースには、次の内容が含まれています：

- デバイスのパスコードにおけるパスコードの複雑さ（Android 12 以降）
- SDK 31 のサポート
- バグ修正

デバイスのパスコードにおけるパスコードの複雑さ（**Android 12** 以降） パスコードの複雑さは、カスタムのパスワード要件よりも優先されます。パスコードの複雑さのレベルは、事前定義されたレベルの 1 つです。したがって、エンドユーザーは複雑さのレベルが低いパスワードを設定できません。

Android 12 以降のデバイスのパスコードの複雑さは次のとおりです：

- パスコードの複雑さを適用する：カスタムのパスワード要件ではなく、プラットフォームによって定義された複雑さのレベルのパスワードが必要です。Android 12 以降で Secure Hub 22.9 以降を使用しているデバイスのみ対象。
- 複雑さのレベル：事前定義されたパスワードの複雑さのレベル。
  - なし：パスワードは必要ありません。
  - 低：パスワードは次の場合があります：
    - \* パターン
    - \* PIN（4 つ以上の数字）
  - 中：パスワードは次の場合があります：
    - \* 繰り返しの文字（4444）または順番どおりの文字（1234）ではない PIN と、最低 4 つの数字
    - \* 4 文字以上のアルファベット
    - \* 4 文字以上の英数字
  - 高：パスワードは次の場合があります：
    - \* 繰り返しの文字（4444）または順番どおりの文字（1234）ではない PIN と、最低 8 つの数字
    - \* 6 文字以上のアルファベット
    - \* 6 文字以上の英数字

### メモ：

- BYOD デバイスの場合、最小文字数、必須文字、生体認証、詳細規則などのパスワード設定は、Android 12 以降では適用できません。代わりにパスワードの複雑さを使用してください。
- 仕事用プロファイルのパスワードの複雑さが有効になっている場合は、デバイス側のパスワードの複雑さも有効にする必要があります。

詳しくは、Citrix Endpoint Management のドキュメントの「[Android Enterprise の設定](#)」を参照してください。

### **Secure Hub 22.7.0**

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 22.6.0**

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 22.5.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

### **Secure Hub 22.4.0**

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 22.2.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.11.0**

#### **Secure Hub for Android**

会社所有のデバイスでの仕事用プロファイルのサポート Android Enterprise デバイスで、会社所有のデバイスモードでの仕事用プロファイルに Secure Hub を登録できるようになりました。この機能は、Android 11 以降を実行しているデバイスで使用できます。以前に個人使用可能なコーポレート所有 (COPE) モードで登録されていたデバイスは、デバイスが Android 10 から Android 11 以降にアップグレードされると、会社所有のデバイスモードでの仕事用プロファイルに自動的に移行します。

### **Secure Hub 21.10.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android Android 12** のサポート。このリリース以降、Secure Hub は Android 12 を実行するデバイスでサポートされます。

### **Secure Hub 21.8.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.7.1**

**Secure Hub for Android** 既に登録されているデバイスで **Android 12** を使用できます。Android 12 へのアップグレードを検討している場合は、最初に Secure Hub をバージョン 21.7.1 に更新してください。Secure Hub 21.7.1 は、Android 12 にアップグレードするために必要な最小バージョンです。このリリースでは、既に登録されているユーザーが Android 11 から Android 12 にシームレスにアップグレードできるようになっています。

注:

Android 12 にアップグレードする前に Secure Hub がバージョン 21.7.1 に更新されていない場合、以前の機能を回復するために、デバイスの再登録または工場出荷時状態へのリセットが必要になる場合があります。

Citrix は、Android 12 について Day 1 サポートの提供を約束しており、Secure Hub の後続のバージョンにさらに更新を追加していき、Android 12 を完全にサポートします。

### **Secure Hub 21.7.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.6.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.5.1**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.5.0**

**Secure Hub for iOS** このリリースでは、MDX Toolkit バージョン 19.8.0 以前でラッピングされたアプリは機能しなくなります。機能を適切に再開するには、アプリを最新の MDX Toolkit でラッピングしてください。

### **Secure Hub 21.4.0**

Secure Hub の色の刷新。Secure Hub は、Citrix の最新のブランドカラーに準拠しています。

### **Secure Hub 21.3.2**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.3.0**

このリリースには、バグの修正が含まれています。

### **Secure Hub 21.2.0**

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 21.1.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### **Secure Hub 20.12.0**

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android** Secure Hub for Android は、直接起動モードをサポートしています。直接起動モードについて詳しくは、[Developer.android.com](https://developer.android.com) で、Android ドキュメントを参照してください。

### **Secure Hub 20.11.0**

**Secure Hub for Android** Secure Hub は、Android 10 に関する Google Play の最新のターゲット API 要件をサポートしています。

## Secure Hub 20.10.5

このリリースには、バグの修正が含まれています。

## Secure Hub 20.9.0

**Secure Hub for iOS** Secure Hub for iOS は iOS 14 をサポートしています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

## Secure Hub 20.7.5

### Secure Hub for Android

- Secure Hub for Android は Android 11 をサポートしています。
- **Secure Hub** のアプリが **32** ビットから **64** ビット版へ移行。Secure Hub バージョン 20.7.5 では、32 ビットアーキテクチャのサポートが終了し、64 ビット版に更新されました。Citrix ではバージョン 20.6.5 から 20.7.5 にアップグレードすることをお勧めします。ユーザーが Secure Hub バージョン 20.6.5 へのアップグレードをスキップし、代わりに 20.1.5 から直接 20.7.5 に更新する場合、再認証が必要です。再認証には、資格情報の入力と Secure Hub の PIN のリセットが含まれます。Secure Hub バージョン 20.6.5 は、Google Play ストアで入手できます。
- **App Store** から更新をインストールします。Secure Hub for Android では、利用可能な更新があるアプリが強調表示され、[更新可能] 機能が App Store 画面に表示されます。

[更新可能] をタップすると、保留中の更新があるアプリの一覧を表示するストアに移動します。アプリの [詳細] をタップして、更新をインストールします。アプリが更新されると、[詳細] の下向き矢印がチェックマークに変わります。

## Secure Hub 20.6.5

**Secure Hub for Android** アプリが **32** ビット版から **64** ビット版へ移行。Secure Hub 20.6.5 リリースは、Android モバイルアプリの 32 ビットアーキテクチャをサポートする最後のリリースです。以降のリリースでは、Secure Hub は 64 ビットアーキテクチャをサポートします。再認証なしで以降のバージョンにアップグレードできるように、ユーザーが Secure Hub バージョン 20.6.5 にアップグレードすることを Citrix ではお勧めします。ユーザーが Secure Hub バージョン 20.6.5 へのアップグレードをスキップし、代わりに直接 20.7.5 に更新する場合、再認証が必要です。再認証には、資格情報の入力と Secure Hub の PIN のリセットが含まれます。

注:

20.6.5 リリースは、デバイス管理者モードで Android 10 を実行しているデバイスの登録をブロックしません。

**Secure Hub for iOS** iOS デバイスで構成されたプロキシを有効にします。Secure Hub for iOS では、ユーザーが [設定] > [W-Fi] で構成するプロキシサーバーを使用できるようにする場合、新しいクライアントプロパティ `ALLOW_CLIENTSIDE_PROXY` を有効にする必要があります。詳しくは、「[クライアントプロパティリファレンス](#)」の「`ALLOW_CLIENTSIDE_PROXY`」を参照してください。

### Secure Hub 20.3.0

注:

Android 6.x および iOS 11.x バージョンの Secure Hub、Secure Mail、Secure Web、Citrix Workspace アプリのサポートは、2020 年 6 月に廃止されます。

### Secure Hub for iOS

- ネットワーク拡張が無効になりました。最近の App Store レビューガイドラインの変更により、Secure Hub リリース 20.3.0 以降では、iOS を実行しているデバイスでネットワーク拡張 (NE) をサポートしていません。NE は、Citrix の業務用モバイルアプリには影響を与えません。ただし NE の削除は、展開済みの、MDX でラップされたエンタープライズアプリに多少の影響を与えます。認証トークン、タイマー、PIN の再試行などによるコンポーネントの同期で、Secure Hub への必要のない切り替えが発生することがあります。詳しくは、<https://support.citrix.com/article/CTX270296> を参照してください。

注:

新規ユーザーには、VPN のインストールを求めるメッセージは表示されません。

- 登録プロファイルの拡張機能のサポート。Secure Hub は、「[登録プロファイルサポート](#)」で説明している Citrix Endpoint Management の登録プロファイルの拡張機能をサポートしています。

### Secure Hub 20.2.0

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

### Secure Hub 20.1.5

このリリースには、次の内容が含まれています:

- ユーザープライバシーポリシーの形式と表示の更新。この機能の更新により、Secure Hub の登録フローが変更されます。
- バグ修正。

### Secure Hub 19.12.5

このリリースには、バグの修正が含まれています。

### Secure Hub 19.11.5

このリリースには、バグの修正が含まれています。

### Secure Hub 19.10.5

**Secure Hub for Android COPE** モードで **Secure Hub** を登録する。Android Enterprise デバイスでは、個人使用可能なコーポレート所有端末 (COPE) 登録プロファイルで Citrix Endpoint Management が構成されている場合、COPE モードで Secure Hub を登録します。

### Secure Hub 19.10.0

このリリースには、バグの修正が含まれています。

### Secure Hub 19.9.5

**Secure Hub for iOS** このリリースには、バグの修正が含まれています。

**Secure Hub for Android Android Enterprise** の仕事用プロファイルおよび完全に管理されているデバイスの **Keyguard** 管理機能のサポート。Android の Keyguard は、デバイスのロック画面および仕事用チャレンジのロック画面を管理します。Citrix Endpoint Management の Keyguard 管理デバイスポリシーを使用して、仕事用プロファイルデバイスの keyguard 管理と、完全に管理された専用デバイスの keyguard 管理を制御します。keyguard 管理を使用すると、Keyguard 画面のロックを解除する前に、ユーザーが使用できる機能 (信頼できるエージェントやセキュアカメラなど) を指定できます。または、すべての Keyguard 機能を無効にできます。

機能の設定とデバイスポリシーの構成方法について詳しくは、「[Keyguard 管理デバイスポリシー](#)」を参照してください。

### Secure Hub 19.9.0

**Secure Hub for iOS** Secure Hub for iOS は iOS 13 をサポートしています。

**Secure Hub for Android** このリリースには、バグの修正が含まれています。

### Secure Hub for Android 19.8.5

このリリースには、バグの修正が含まれています。

## Secure Hub 19.8.0

**Secure Hub for iOS** このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

**Secure Hub for Android Android Q** のサポート。このリリースには、Android Q のサポートが含まれます。Android Q プラットフォームにアップグレードする前に、Google Device Administration API の廃止が Android Q を実行するデバイスに与える影響について、「[Device Administration から Android Enterprise への移行](#)」を参照してください。また、ブログ（[Citrix Endpoint Management および Android Enterprise - 変革](#)）も参照してください。

## Secure Hub 19.7.5

**Secure Hub for iOS** このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

**Secure Hub for Android Samsung Knox SDK 3.x** のサポート。Secure Hub for Android は Samsung Knox SDK 3.x をサポートしています。Samsung Knox 3.x の移行について詳しくは、Samsung Knox の開発者向けドキュメントを参照してください。このリリースでは、新しい Samsung Knox 名前空間もサポートしています。以前の Samsung Knox 名前空間からの変更について詳しくは、「[古い Samsung Knox 名前空間の変更](#)」を参照してください。

注：

Secure Hub for Android は、Android 5 を実行しているデバイスで Samsung Knox 3.x をサポートしていません。

## Secure Hub 19.3.5 ~ 19.6.6

これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

## Secure Hub 19.3.0

**Samsung Knox Platform for Enterprise** のサポート。Secure Hub for Android は、Android Enterprise デバイスで Knox Platform for Enterprise (KPE) をサポートします。

## Secure Hub 19.2.0

このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。



## Secure Hub 19.1.5

Secure Hub for Android Enterprise は、次のポリシーをサポートするようになりました：

- **WiFi** デバイスポリシー Wi-Fi デバイスポリシーは、Android Enterprise をサポートするようになりました。このポリシーについて詳しくは、「[Wi-Fi デバイスポリシー](#)」を参照してください。
- カスタム **XML** デバイスポリシー カスタム XML デバイスポリシーは、Android Enterprise をサポートするようになりました。このポリシーについて詳しくは、「[カスタム XML デバイスポリシー](#)」を参照してください。
- ファイルデバイスポリシー Citrix Endpoint Management にスクリプトファイルを追加して、Android Enterprise デバイスで機能を実行できます。このポリシーについて詳しくは、「[ファイルデバイスポリシー](#)」を参照してください。

## Secure Hub 19.1.0

**Secure Hub** のフォント、色、そのほかの **UI** の要素が刷新されました。この変更は、Citrix の業務用モバイルアプリ全体により統一感を与え、ユーザーの操作性も向上しています。

## Secure Hub 18.12.0

このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

## Secure Hub 18.11.5

- **Android Enterprise** の制限デバイスポリシー設定。制限デバイスポリシーの新しい設定により、ユーザーは Android Enterprise デバイスでステータスバー、ロック画面の Keyguard、アカウント管理、位置情報の共有、デバイス画面の表示を維持する機能にアクセスできます。詳しくは、「[制限デバイスポリシー](#)」を参照してください。

Secure Hub 18.10.5~18.11.0 には、パフォーマンスの強化機能とバグの修正が含まれています。

## Secure Hub 18.10.0

- **Samsung DeX** モードのサポート： Samsung DeX を使用すると、ユーザーは KNOX 対応デバイスを外部ディスプレイに接続して、PC のようなインターフェイスでアプリを使用したり、ドキュメントを確認したり、ビデオを見ることができます。Samsung DeX のデバイス要件と Samsung DeX の設定については、「[Samsung DeX の機能](#)」を参照してください。

Citrix Endpoint Management で Samsung DeX モードの機能を設定するには、Samsung Knox の制限デバイスポリシーを更新します。詳しくは、「[制限デバイスポリシー](#)」の「**Samsung KNOX** の設定」を参照してください。

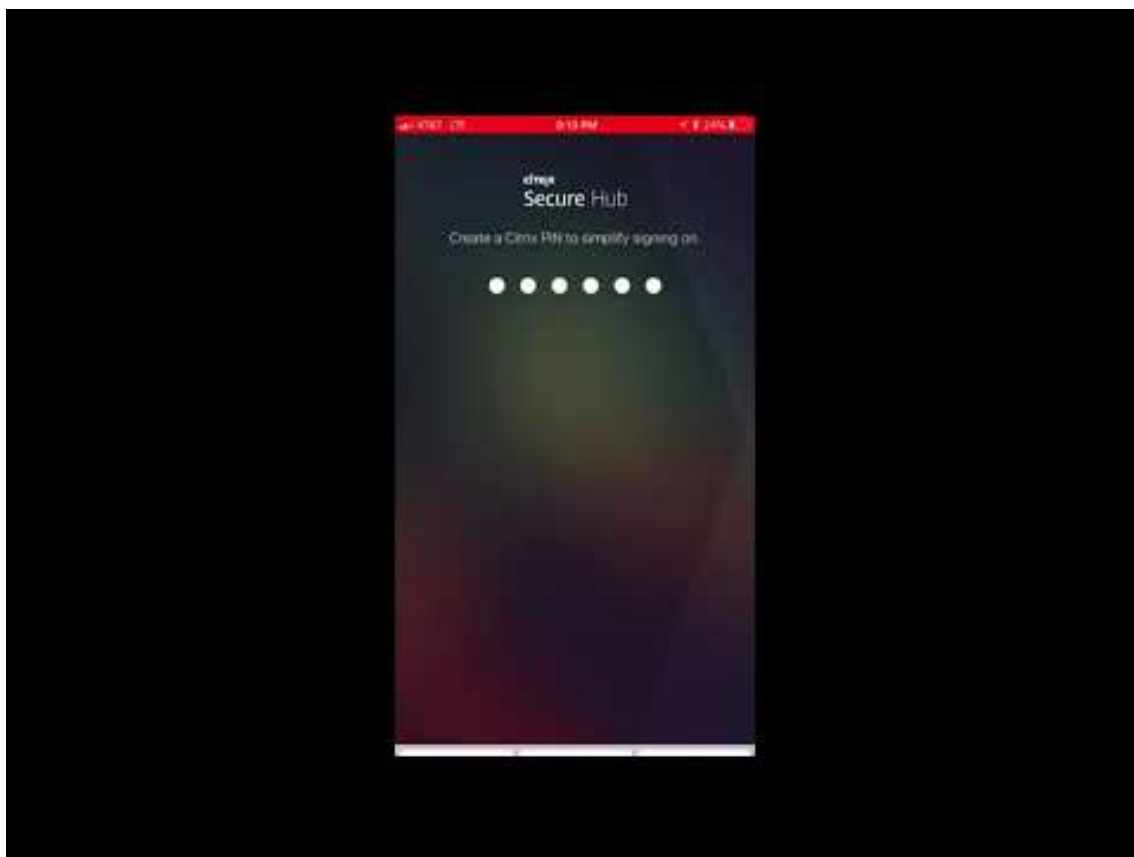
- **Android SafetyNet** のサポート: **Android SafetyNet** 機能を使用して、Secure Hub がインストールされている Android デバイスの互換性とセキュリティを評価するように Endpoint Management を設定できます。結果は、デバイス上で自動化された操作をトリガーするために使用できます。詳しくは、「[Android SafetyNet](#)」を参照してください。
- **Android Enterprise** デバイスのカメラ使用を禁止する: 制限デバイスポリシーの新しい設定である [カメラの使用を許可] を設定することで、ユーザーが Android Enterprise デバイスでカメラを使用できないようにすることができます。詳しくは、「[制限デバイスポリシー](#)」を参照してください。

### Secure Hub 10.8.60~18.9.0

これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

#### Secure Hub 10.8.60

- ポーランド語のサポート。
- Android P のサポート。
- ワークスペースアプリストアの使用のサポート。  
Secure Hub を開いても、Secure Hub ストアは表示されません。[アプリを追加] ボタンを押すと、ワークスペースアプリストアに移動します。次のビデオでは、iOS デバイスで Citrix Workspace アプリを使用して、Citrix Endpoint Management への登録を行う様子を示します。



**重要:**

この機能は新規顧客にのみ提供されます。現在のところ、既存の顧客の移行はサポートされていません。

この機能を使用するには、以下を設定します:

- パスワードのキャッシュポリシーおよびパスワード認証ポリシーを有効にします。これらのポリシーの構成については、「[業務用モバイルアプリの MDX ポリシーの概要](#)」を参照してください。
- Active Directory 認証を AD または AD+Cert として構成します。これら 2 つのモードをサポートしています。認証の構成については、「[ドメインまたはドメイン+セキュリティトークン認証](#)」を参照してください。
- Endpoint Management のワークスペース統合を有効にします。ワークスペース統合については詳しくは、「[ワークスペースの構成](#)」を参照してください。

**重要:**

この機能を有効にすると、Citrix Files SSO は Endpoint Management (旧 XenMobile) ではなく、ワークスペースを通して実行されます。ワークスペースの統合を有効にする前に、Endpoint Management コンソールで Citrix Files の統合を無効にすることをお勧めします。

### Secure Hub 10.8.55

- JSON 構成を使用して、Google のゼロタッチ登録と Samsung Knox Mobile Environment (KME) ポータルにユーザー名とパスワードを渡す機能です。詳しくは、「[Samsung Knox の一括登録](#)」を参照してください。
- 証明書のピン留めを有効にすると、ユーザーは自己署名証明書を使用して Endpoint Management に登録することはできません。ユーザーが自己署名証明書を使用して Endpoint Management に登録しようとすると、証明書が信頼されていないという警告が表示されます。

**Secure Hub 10.8.25:** Secure Hub for Android では Android P デバイスがサポートされています。

注:

Android P プラットフォームにアップグレードする前に:サーバーインフラストラクチャが、subjectAltName (SAN) 拡張で一致するホスト名を持つセキュリティ証明書に準拠していることを確認します。ホスト名を検証するには、サーバーは一致する SAN を含む証明書を提示する必要があります。ホスト名に一致する SAN を含まない証明書は信頼されません。詳しくは、Android 開発者ドキュメントを参照してください。

**Secure Hub for iOS の更新 (2018 年 3 月 19 日):** Secure Hub for iOS バージョン 10.8.6 では、VPP アプリポリシーの問題を修正できます。詳しくは、[Citrix Knowledge Center の記事](#)を参照してください。

**Secure Hub 10.8.5:** Android Work (Android for Work) の COSU モード対応 Secure Hub for Android でサポート。詳しくは、[Citrix Endpoint Management のドキュメント](#)を参照してください。

### Secure Hub の管理

Secure Hub に関連する大部分の管理タスクは、Endpoint Management の初期構成時に実行します。ユーザーが iOS や Android で Secure Hub を利用できるようにするために、Secure Hub を iOS App Store、または Google Play ストアにアップロードします。

Secure Hub は、Citrix Gateway を使用した認証後にユーザーの Citrix Gateway セッションが更新されたときに、インストールされているアプリの、Endpoint Management に格納されている MDX ポリシーのほとんどを更新します。

重要:

これらのポリシーのうちのいずれかを変更する場合は、ユーザーはアプリを削除してから再インストールし、更新されたポリシーを適用する必要があります: セキュリティグループ、暗号化を有効化、Secure Mail の Exchange Server

### Citrix PIN

Citrix PIN を使用するように、Secure Hub を構成できます。このセキュリティ機能は、Endpoint Management コンソールで [設定] > [クライアントプロパティ] を選択して有効にします。この設定では、登録されているモバ

イルデバイスユーザーが Secure Hub にサインオンし、ラップされた MDX アプリを暗証番号 (PIN) の使用によりアクティブ化する必要があります。

Citrix PIN 機能で、セキュリティで保護されたラップアプリにログオンするときのユーザー認証が簡単になります。Active Directory のユーザー名やパスワードなど、別の資格情報を繰り返し入力する必要はありません。

Secure Hub に初めてサインオンするユーザーは、Active Directory ユーザー名とパスワードを入力する必要があります。サインオン時に、Secure Hub は Active Directory 資格情報またはクライアント証明書をユーザーデバイスに保存し、ユーザーに対して PIN を入力するよう要求します。ユーザーは再度のサインオン時に PIN を入力することにより、アクティブなユーザーセッションの次回アイドルタイムアウトが終了するまで、Citrix アプリおよび Store にセキュアにアクセスできます。関連するクライアントのプロパティでは、PIN を使用したシークレットの暗号化、PIN のパスコードの種類指定、および PIN の強度と長さの要件指定を実行できます。詳しくは、「[クライアントプロパティ](#)」を参照してください。

指紋認証 (Touch ID) が有効なときに、アプリが無効なためにオフライン認証が求められた場合、ユーザーは指紋を使用してサインインできます。ただし、初めて Secure Hub にサインインしたり、デバイスを再起動したりする場合、および非アクティブタイマーの有効期限が切れた後には、PIN を入力する必要があります。指紋認証の有効化について詳しくは、「[指紋認証または Touch ID 認証](#)」を参照してください。

### 証明書ピン留め

Secure Hub for iOS および Secure Hub for Android は、SSL 証明書のピン留めをサポートしています。これにより、Citrix クライアントが Endpoint Management と通信する際に、企業が署名した証明書が使用されます。したがって、デバイス上のルート証明書のインストールにより SSL セッションに危害が及ぶ場合に、クライアントから Endpoint Management への接続が阻止されます。Secure Hub がサーバー公開キーに対する何らかの変更を検出すると、接続が拒否されます。

Android N 以降、ユーザーが追加した認証機関 (CA) はオペレーティングシステムで許可されなくなります。Citrix ではユーザーが追加した CA の代わりに、パブリックルート CA を使用することをお勧めします。

Android N にアップグレードするユーザーは、プライベートまたは自己署名 CA を使用すると問題が発生する可能性があります。次の状況では、Android N デバイス上の接続が切断されます：

- Endpoint Management オプションのプライベート/自己署名 CA と必須の信頼済み CA が [オン] に設定されている。詳しくは、「[デバイス管理](#)」を参照してください。
- プライベート/自己署名 CA と Endpoint Management AutoDiscovery サービス (ADS) は到達可能ではありません。セキュリティ上の問題により ADS に到達できない場合、必須の信頼済み CA は、最初は [オフ] に設定されていた場合でも [オン] になります。

デバイスの登録または Secure Hub のアップグレード前に、証明書のピン留めを有効にすることを検討してください。デフォルトで、このオプションは [オフ] になっており、ADS によって管理されます。証明書のピン留めを有効にすると、ユーザーは自己署名証明書を使用して Endpoint Management に登録することはできません。ユーザーが自己署名証明書を使用して登録しようとする、証明書が信頼されていないという警告が表示されます。ユーザーが証明書を承認しない場合、登録は失敗します。

証明書ピン留めを使用するには、Citrix ADS サーバーに Citrix が証明書をアップロードするように依頼する必要があります。[Citrix サポートポータル](#)でテクニカルサポートケースを開きます。秘密キーを Citrix に送信しないでください。次に、以下の情報を入力します：

- ユーザーが登録時に使用するアカウントを含むドメイン。
- Endpoint Management の完全修飾ドメイン名 (FQDN)。
- Endpoint Management のインスタンス名。デフォルトでは、インスタンス名は zdm であり、大文字と小文字が区別されます。
- ユーザー ID のタイプ。UPN またはメールのいずれかにできます。デフォルトでは、タイプは UPN です。
- デフォルトポート 8443 からポート番号を変更した場合は、iOS 登録に使用されるポート。
- デフォルトポート 443 からポート番号を変更した場合は、Endpoint Management が接続を受け入れるポート。
- Citrix Gateway の完全な URL。
- 管理者のメールアドレス (オプション)。
- ドメインに追加する PEM 形式の証明書。これは、秘密キーではなく公開証明書である必要があります。
- 既存のサーバー証明書の制御方法。古いサーバー証明書を (危険にさらされているため) 直ちに削除するか、失効するまでサポートを継続するか。

詳細情報および証明書が Citrix サーバーに追加されると、テクニカルサポートケースが更新されます。

### 証明書 + ワンタイムパスワード認証

Citrix ADC を構成して、証明書とセキュリティトークンを使用して Secure Hub で認証を行うようにすることができます。セキュリティトークンはワンタイムパスワードとして機能します。この構成により、Active Directory のフットプリントをデバイスに残さない強力なセキュリティオプションが提供されます。

Secure Hub で証明書 + ワンタイムパスワードタイプの認証を使用できるようにするには：Citrix ADC の書き換えアクションと書き換えポリシーを追加する必要があります。これにより、Citrix Gateway ログオンタイプを示す「**X-Citrix-AM-GatewayAuthType: CertAndRSA**」形式のカスタム応答ヘッダーが挿入されます。

通常 Secure Hub では、Endpoint Management コンソールで構成された Citrix Gateway ログオンタイプが使用されます。ただしこの情報は、Secure Hub が初回のログオンを完了するまで、Secure Hub では使用できません。そのため、カスタムヘッダーが必要となります。

注：

Endpoint Management と Citrix ADC で異なるログオンタイプが設定されている場合は、Citrix ADC の構成で上書きされます。詳しくは、「[Citrix Gateway と Endpoint Management](#)」を参照してください。

1. Citrix ADC で、[構成] > [AppExpert] > [書き換え] > [アクション] の順に選択します。
2. [追加] をクリックします。  
[書き換えアクションの作成] 画面が開きます。

- 以下のとおりに各フィールドを入力して、[作成] をクリックします。

### Create Rewrite Action

Name\*

Type\*

Use this action type to insert a header.

Header Name\*

Expression Expression Editor

Operators  Saved Policy Expressions  Frequently Used Expressions  Clear

Evaluate

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string constants are enclosed in double quotes.

Comments

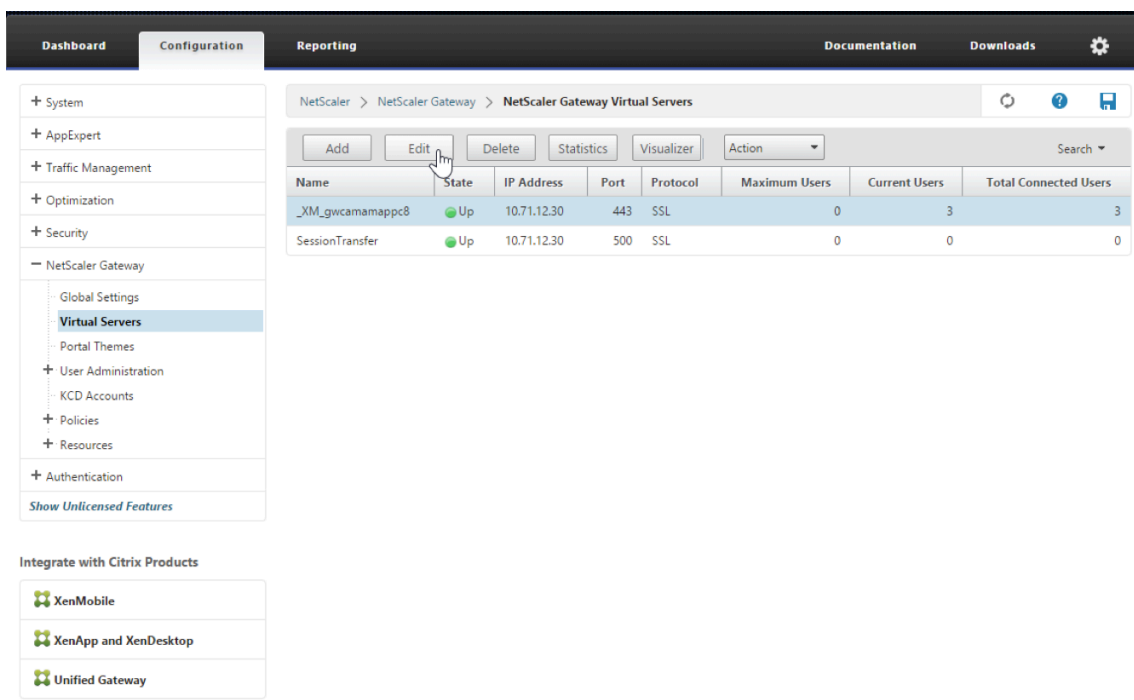
メインの [書き換えアクション] 画面に次の結果が表示されます。

NetScaler > AppExpert > Rewrite > Rewrite Actions Refresh Help Save

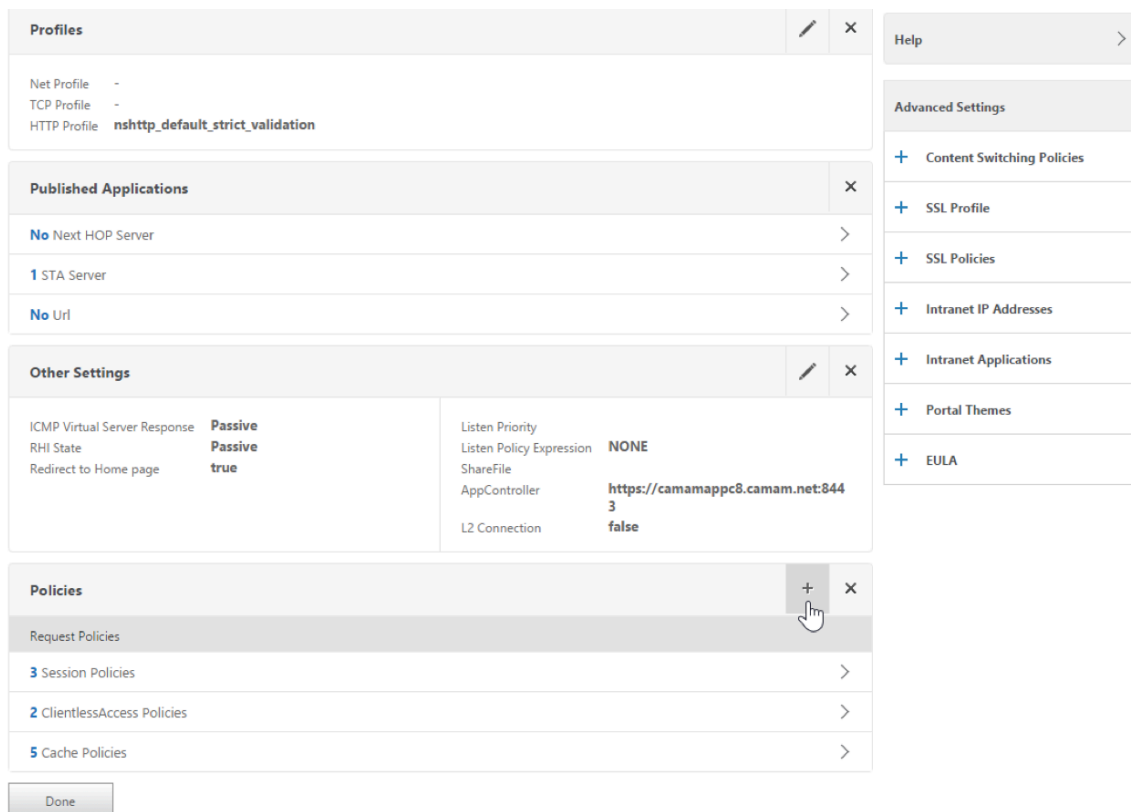
Show built-in Rewrite Actions Search

Name	Type	Target Expression	Expression	Pattern
ns_cvpn_sp_js_checkout_rw_act	insert_after_all	TEXT	"\\\\"+window.location.pathname.split("\\\\")[1]+\\"+wi...	re~a.substr(0,3),toLowerCase(\\)=\\="%2f\\"a=
InsertGatewayAuthTypeHeader	insert_http_header	X-Citrix-AM-GatewayAuthType	"CertAndRSA"	

- 書き換えアクションを書き換えポリシーとして仮想サーバーにバインドします。[構成] > [NetScaler Gateway] > [仮想サーバー] の順に選択して、仮想サーバーを選択します。

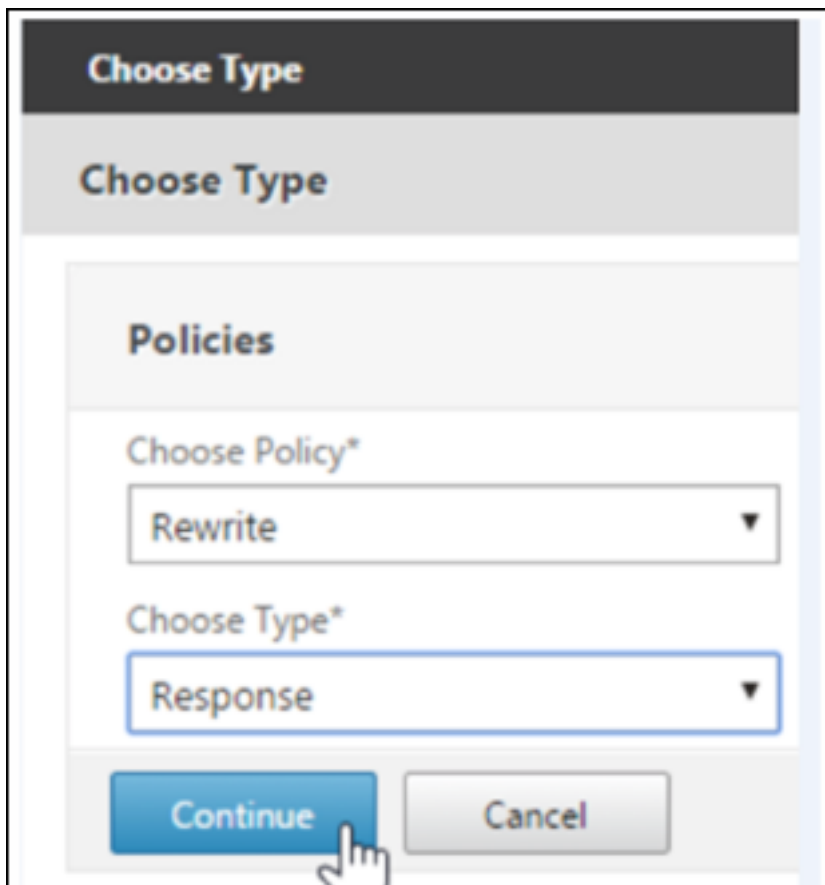


5. [編集] をクリックします。
6. [仮想サーバーの構成] 画面で、[ポリシー] までスクロールします。
7. + をクリックして、ポリシーを追加します。





8. [ポリシーの選択] フィールドで [書き換え] を選択します。
9. [種類の選択] フィールドで [応答] を選択します。



10. [続行] をクリックします。  
[ポリシーバインディング] セクションが展開されます。

**Choose Type**

Choose Type

**Policies**

Choose Policy  
**Rewrite**

Choose Type  
**Response**

**Policy Binding**

Select Policy\*

Click to select

+

?

**Binding Details**

Priority\*

100

Goto Expression\*

END

Bind Close

11. [ポリシーの選択] をクリックします。

使用可能なポリシーの画面が表示されます。

**Choose Type > Rewrite Policies**

**Rewrite Policies**

Select Add Edit Delete Show Bindings Policy Manager Statistics Action

Show built-in Rewrite Policies Search

Name	Expression	Action	Undefined-Result Action	Hits	Undefined Hits	Active
InsertGatewayAuthTypePolicy	true	InsertGatewayAuthTypeHeader	Use Global	0	0	✕

12. 作成したポリシーの行をクリックして、[選択] をクリックします。選択したポリシーが入力された [ポリシーバインディング] 画面に戻ります。

**Choose Type**

Choose Policy: Rewrite

Choose Type: Response

**Policy Binding**

Select Policy\*: InsertGatewayAuthTypePolicy

**Binding Details**

Priority\*: 100

Goto Expression\*: END

Buttons: Bind, Close

13. **[Bind]** をクリックします。

正常にバインドされると、メインの構成画面に戻り、完成した書き換えポリシーが表示されます。

Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED
Refresh Count	0	Client Authentication	ENABLED	SSLv3	ENABLED
Enable Session Reuse	ENABLED	Client Certificate	Mandatory	TLSv1	ENABLED
Time-out	120	Send Close-Notify	YES	TLSv1.1	ENABLED
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLSv1.2	ENABLED
		SNI Enable	DISABLED		

**Published Applications**

No Next HOP Server	>
1 STA Server	>
No Url	>

**Other Settings**

ICMP Virtual Server Response	Passive	Listen Priority	
RHI State	Passive	Listen Policy Expression	None
Redirect to Home page	true	ShareFile	
		AppController	https://xms3.dm.com:8443
		L2 Connection	false

**Policies**

Request Policies	>
3 Session Policies	>
2 ClientlessAccess Policies	>
4 Cache Policies	>
Response Policies	>
1 Rewrite Policy	>

14. ポリシーの詳細を表示するには、**[書き換えポリシー]** をクリックします。

VPN Virtual Server Rewrite Policy Binding				
VPN Virtual Server Rewrite Policy Binding				
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/> <input type="button" value="Edit"/>				
Priority	Policy Name	Expression	Action	Goto Expression
100	InsertGatewayAuthTypeHeaderPolicy	true	InsertGatewayAuthTypeHeader	END
<input type="button" value="Close"/>				

**Android** デバイスの **ADS** 接続のためのポート要件 ポート構成により、Secure Hub から接続する Android デバイスで社内ネットワークから Citrix ADS にアクセスできることを保証します。ADS を介して利用可能なセキュリティ更新プログラムをダウンロードする時、ADS にアクセスする能力は重要です。ADS 接続はプロキシサーバーと互換性がない可能性があります。このシナリオでは、ADS 接続がプロキシサーバーをバイパスすることを可能にします。

**重要:**

Secure Hub for Android および iOS では、Android デバイスから ADS にアクセスする必要があります。詳しくは、Citrix Endpoint Management のドキュメントの「[ポート要件](#)」を参照してください。この通信は送信ポート 443 で実行されます。大半の場合で、既存の環境ではこれを許可するよう設計されています。この通信を保証できない場合は、Secure Hub 10.2 にアップグレードしないでください。不明の点があれば、Citrix サポートに問い合わせてください。

**前提条件:**

- Endpoint Management と Citrix ADC の証明書を収集します。証明書は PEM 形式で、秘密キーではなく公開証明書である必要があります。
- Citrix サポートに証明書ピン留めの有効化を依頼します。このプロセスで、証明書の提出を求められます。

証明書ピン留めに追加された機能向上のため、デバイスは登録前に ADS に接続する必要があります。この前提条件により、デバイスを登録する環境の最新のセキュリティ情報が Secure Hub で利用できることが保証されます。デバイスが ADS に接続できない場合は、Secure Hub はデバイスの登録を許可しません。したがって、内部ネットワーク内で ADS アクセスを可能にすることは、デバイスの登録を有効にするために重要です。

Secure Hub for Android に ADS へのアクセスを許可するには、以下の IP アドレスおよび FQDN のポート 443 を開放します:

FQDN	IP アドレス	ポート	IP とポートの使用
<a href="#">discovery.mdm.zenprise.com</a>	52.5.138.94	443	Secure Hub - ADS 通信

FQDN	IP アドレス	ポート	IP とポートの使用
<a href="#">discovery.mdm.zenprise.com</a>	52.1.30.122	443	Secure Hub - ADS 通信
<a href="#">ads.xm.cloud.com</a> : Secure Hub バージョン 10.6.15 以降では <a href="#">ads.xm.cloud.com</a> が使用されることに注意してください。	34.194.83.188	443	Secure Hub - ADS 通信
<a href="#">ads.xm.cloud.com</a> : Secure Hub バージョン 10.6.15 以降では <a href="#">ads.xm.cloud.com</a> が使用されることに注意してください。	34.193.202.23	443	Secure Hub - ADS 通信

証明書ピン留めが有効な場合、次の処理が実行されます：

- Secure Hub は、デバイス登録時に企業の証明書を固定します。
- Secure Hub は、アップグレード時に現在固定されている証明書を破棄し、登録済みユーザーに対して最初の接続でサーバー証明書を固定します。

注：

アップグレード後に証明書ピン留めを有効にする場合は、再登録する必要があります。

- 証明書公開キーを変更しなかった場合、証明書の更新時に再登録する必要はありません。

証明書ピン留めではリーフ証明書がサポートされますが、中間証明書および発行者証明書はサポートされません。証明書ピン留めは、Endpoint Management、Citrix Gateway などの Citrix サーバーには適用されますが、サードパーティ製のサーバーには適用されません。

#### [アカウントの削除] の無効化

Auto Discovery Services (ADS) が有効になっている環境では、Secure Hub で [アカウントの削除] を無効にできます。

[アカウントの削除] を無効にするには、次の手順を実行します：

1. ドメインの ADS を構成します。

2. Citrix Endpoint Management で [**AutoDiscovery** サービス情報]を開き、`displayReenrollLink` の値を **False** に設定します。  
デフォルトでは、この値は **True** です。
3. デバイスが MDM+MAM (ENT) モードで登録されている場合、ログオフしてから再度ログインすると、変更が有効になります。  
デバイスが他のモードで登録されている場合は、デバイスを再登録する必要があります。

### Secure Hub の使用

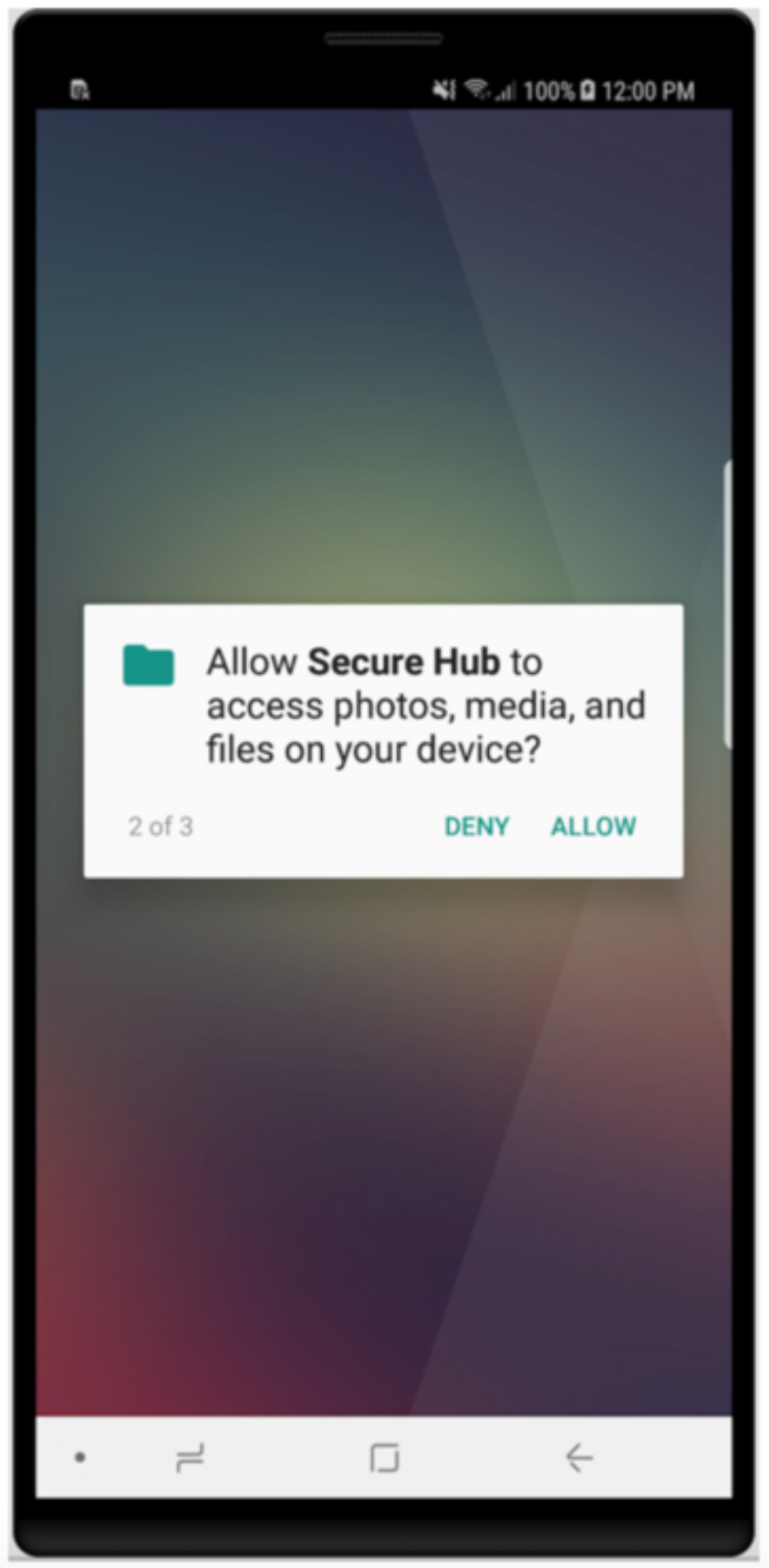
ユーザーは、最初に Apple または Android のストアから自分のデバイス上に Secure Hub をダウンロードします。

Secure Hub を起動すると、勤務先や組織から提供された資格情報を入力してデバイスを登録するための画面が開きます。デバイス登録の詳細については、「[ユーザーアカウント](#)、[役割](#)、[および登録](#)」を参照してください。

Secure Hub for Android では、初期インストールおよび登録時に、次のメッセージが表示されます。「Secure Hub がデバイス上の写真、メディア、ファイルにアクセスできるようにしますか?」

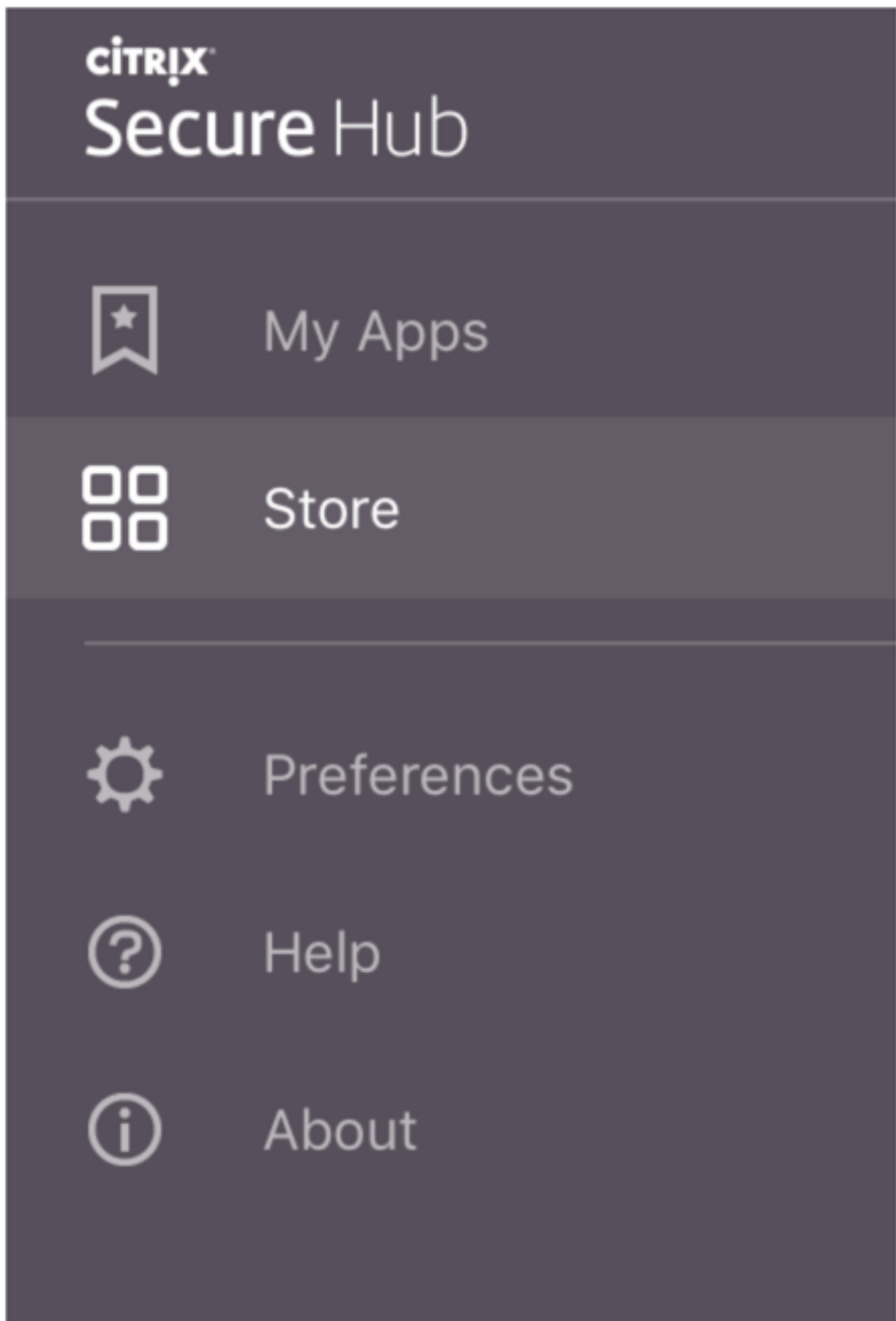
このメッセージは、Android オペレーティングシステムによるものであり、Citrix からのものではありません。[許可] をタップしても、Secure Hub を管理する管理者および Citrix には、個人データは表示されません。ただし、管理者とのリモートサポートセッションを行っている場合、管理者はセッション内で個人ファイルを表示できます。

登録が完了すると、ユーザーの [マイアプリ] タブに指定したアプリとデスクトップが表示されます。ユーザーは Store からアプリを追加できます。スマートフォン上の左上隅のハンバーガーアイコンの [設定] の下に Store へのリンクがあります。



タブレットでは、Store は別のタブとなります。





iOS 9 以降の iPhone を使用するユーザーがストアから業務用モバイルアプリをインストールすると、メッセージが表示されます。そのメッセージでは、エンタープライズデベロッパーである Citrix がその iPhone で信頼されていないことが示されます。このメッセージは、デベロッパーが信頼できる状態になるまで、アプリを使用できないことを説明しています。このメッセージが表示された場合、Secure Hub はユーザーに、iPhone で Citrix エンタープライズアプリが信頼されるようにする手順を示すガイドを表示するよう求めます。

### Secure Mail での自動登録

MAM-only 展開の場合、Endpoint Management を、Android または iOS デバイスを持ち、メール資格情報で Secure Hub に登録したユーザーが Secure Mail に自動的に登録されるように構成できます。これは、ユーザーが追加情報を入力する必要があるか、Secure Mail に登録する追加手順を実行する必要があることを意味します。

Secure Mail を初めて使用する場合、Secure Mail は Secure Hub からユーザーの電子メールアドレス、ドメインおよびユーザー ID を取得します。Secure Mail は、Autodiscovery に電子メールアドレスを使用します。ドメインとユーザー ID を使用して Exchange Server が識別されます。Exchange Server によって、Secure Mail のユーザー自動認証が行われます。パスワードをパススルーしないようにポリシーが設定されている場合、ユーザーはパスワードの入力を求められます。ただし、ユーザーはさらに情報を入力する必要はありません。

この機能を有効にするには、3 つのプロパティを作成する必要があります：

- サーバープロパティ MAM\_MACRO\_SUPPORT。手順については、「[サーバープロパティ](#)」を参照してください。
- クライアントプロパティ ENABLE\_CREDENTIAL\_STORE および SEND\_LDAP\_ATTRIBUTES。手順については、「[クライアントプロパティ](#)」を参照してください。

### カスタマイズされたストア

ストアをカスタマイズする場合は、[設定] > [クライアントのブランド設定] の順に選択して、名前を変更し、ロゴを追加して、アプリの外観を指定します。

XenMobile Analyze Manage Configure administrator

Settings > Client Branding

### Client Branding

You can set the way apps appear in the store and add a logo to brand Worx Home on mobile devices.

Store name\*

Default store view

Category

A-Z

Device

Phone

Tablet

Branding file

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

Endpoint Management コンソールでアプリの説明を編集できます。[構成] をクリックして、[アプリ] を選択します。表からアプリを選択して [編集] をクリックします。編集する説明があるアプリのプラットフォームを選択し、[説明] ボックスに文字列を入力します。

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Delivery Groups

### MDX

1 App Information

2 Platform

iOS

Android

Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

### App Information

Name\*

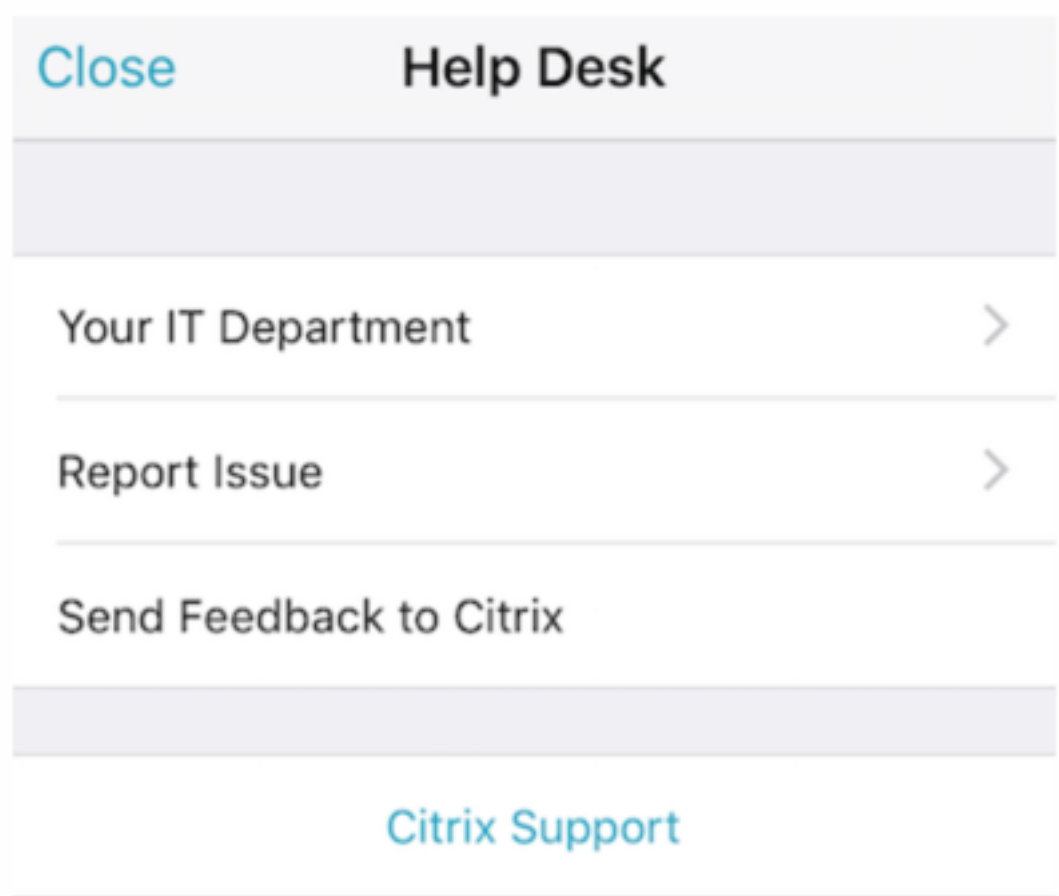
Description

App category

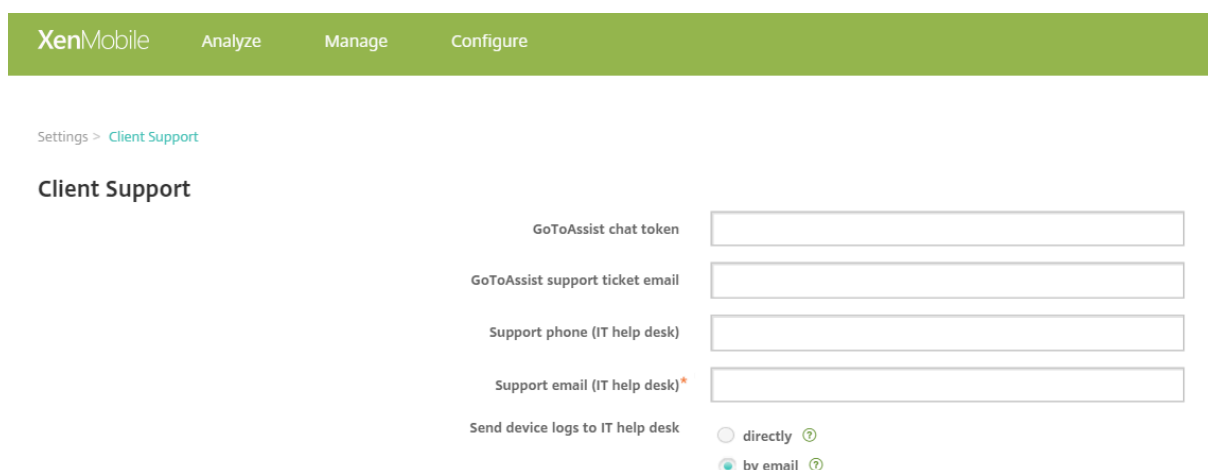
Store では、ユーザーは Endpoint Management で構成および保護されたアプリおよびデスクトップのみを参照できます。アプリを追加するには、[詳細] をタップしてから、[追加] をタップします。

#### 構成済みのヘルプオプション

また、Secure Hub では、ユーザーがヘルプを得られるさまざまな方法も提供しています。タブレットでは、右上隅にあるクエスチョンマークをタップするとヘルプオプションが表示されます。スマートフォンで、左上隅にあるハンバーガーメニューアイコンをタップしてから、[ヘルプ] をタップします。



[IT 部門] には会社のヘルプデスクの電話番号とメールアドレスが表示され、ユーザーがアプリから直接アクセスできます。Endpoint Management コンソールで電話番号とメールアドレスを入力します。右上隅にある歯車のアイコンをクリックします。[設定] ページが開きます。[詳細] をクリックして [クライアントサポート] をクリックします。情報を入力する画面が表示されます。



XenMobile Analyze Manage Configure

Settings > Client Support

### Client Support

GoToAssist chat token

GoToAssist support ticket email

Support phone (IT help desk)

Support email (IT help desk)\*

Send device logs to IT help desk  directly  by email

[問題の報告] にユーザーのアプリの一覧が表示されます。ユーザーは、問題のあるアプリを選択します。Secure

Hub で自動的にログが生成され、Secure Mail に、zip ファイルとしてログが添付されたメッセージが開かれます。ユーザーは、件名の行と問題の説明を追加します。スクリーンショットを添付することもできます。

[[Citrix へのフィードバックの送信](#)] をクリックすると、Citrix サポートのアドレスが入力された Secure Mail のメッセージが開きます。メッセージの本文で、Secure Mail の改善点についてのメッセージを入力することができます。デバイスに Secure Mail がインストールされていない場合は、ネイティブのメールプログラムが開きます。

またユーザーは [[Citrix サポート](#)] をタップして、[Citrix Knowledge Center](#)を開くこともできます。ここでは、すべての Citrix 製品のサポート文書を検索できます。

[[環境設定](#)] で、ユーザーのアカウントとデバイスに関する情報を確認できます。

### 位置情報ポリシー

また、Secure Hub は位置情報ポリシーや地理追跡ポリシーを提供します。これにより、たとえば、会社所有のデバイスが特定の地理的境界の外側に出ているかどうかを確認できます。詳しくは、「[位置情報デバイスポリシー](#)」を参照してください。

### クラッシュ発生時の情報収集と分析

Secure Hub では障害の原因を確認できるように、障害の情報を自動的に収集し分析します。Crashlytics ソフトウェアがこの機能をサポートします。

iOS および Android で利用できる機能については、「[Citrix Secure Hub](#)」のプラットフォームごとの機能を参照してください。

## Secure Hub のデバイスログの生成

このセクションでは、Secure Hub のデバイスログを生成するとともに、ログに正しいデバッグレベルを設定する方法について説明します。

Secure Mail のログを取得するには、以下を実行します。

1. [[Secure Hub](#)] > [[ヘルプ](#)] > [[問題の報告](#)] の順に選択します。アプリの一覧から [Secure Mail] を選択します。  
組織のヘルプデスク宛の電子メールが開きます。
2. ログの設定は、サポートチームからそうするように指示があった場合にのみ、変更します。設定が正しく行われていることを常に確認してください。
3. Secure Mail に戻り、問題を再現します。問題の再現を開始した時刻と、問題が発生した時刻またはエラーメッセージが表示された時刻に注目してください。

4. [**Secure Hub**] > [ヘルプ] > [問題の報告] の順に戻ります。アプリの一覧から [Secure Mail] を選択します。

組織のヘルプデスク宛の電子メールが開きます。

5. 件名行と、問題を簡単に説明する本文を入力します。手順 3 で収集したタイムスタンプも追加して、[送信] をクリックします。

完成したメッセージが開きます。圧縮されたログファイルが添付されています。

6. [送信] をもう一度クリックします。

送信される圧縮ファイルには、次のログが含まれています：

- CtxLog\_AppInfo.txt (iOS)、Device\_And\_AppInfo.txt (Android)、logx.txt and WH\_logx.txt (Windows Phone)

アプリケーション情報ログには、デバイスとアプリケーションに関する情報が含まれています。

## 既知の問題と解決された問題

June 6, 2024

Citrix では、業務用モバイルアプリの直近 2 つのバージョンからのアップグレードをサポートしています。

### Secure Hub for iOS 24.5.0

#### 解決された問題

このリリースで解決された問題はありません。

#### 既知の問題

このリリースには既知の問題はありません。

### Secure Hub for Android 24.3.0

#### 解決された問題

工場出荷時リセットの制限ポリシーが「いいえ」に設定されている場合でも、ユーザーは会社所有の Android Enterprise デバイスで工場出荷時リセットを実行できます。この問題は、ユーザーが Secure Hub を再起動したときに発生します。[XMHELP-4479]

### 既知の問題

このリリースには既知の問題はありません。

## Secure Hub for iOS 24.1.0

### 解決された問題

- Palera1n アプリを使用して iOS デバイスをジェイルブレイクすると、Citrix Endpoint Management サーバーはこのデバイスをジェイルブレイク済みとして検出しません。その結果、Endpoint Management サーバーはジェイルブレイクされたデバイスを工場出荷時の状態に設定にリセットできません。さらに、Endpoint Management サーバーは、ジェイルブレイクされたデバイスのエントリをサーバーコンソールから削除できません。[XMHELP-4397]
- MAM SDK を使用して iOS アプリを管理すると、Secure Hub ストアで次のいずれかの問題が発生します：
  - アプリの更新が利用可能になった場合に通知しません。
  - アプリが更新された後も継続的に更新を通知します。

[XMHELP-4427]

- MAM SDK を使用して iOS アプリを管理すると、次のコンプライアンス通知が表示される場合があります：

「このアプリはアカウントから削除されました。お使いのデバイスから削除できます。」

この問題は、MAM SDK と MDX Toolkit の両方を同じ iOS デバイスにインストールすると発生します。[XMHELP-4463]

## Secure Hub for Android 23.12.0

### 解決された問題

Citrix Gateway 資格情報の有効期限が切れると、Secure Hub は Citrix Gateway サーバーに接続するための新しい証明書を生成しないことがあります。その結果、Secure Hub は起動に失敗し、次のエラーメッセージが表示されます。

「接続エラーが発生しました。再接続してください」

[XMHELP-4446]

## Secure Hub for iOS 23.11.0

### 解決された問題

- Citrix Gateway クライアント証明書の有効期限が切れても自動更新されないため、iOS デバイスで Secure Hub の認証が失敗します。この問題は、Citrix Gateway が TLSv1.3 プロトコルを使用している場合に発生します。[XMHELP-4396]
- Citrix Gateway 経由で Secure Hub にサインインすると、次のエラーメッセージが表示される場合があります:

「サインオンできませんでした。資格情報が正しくありません。セッションを終了します (Could not sign on. Incorrect credentials. Ending the session)」

この問題は、nFactor を使用して iOS デバイスを Citrix Endpoint Management (CEM) に登録するときに発生します。[XMHELP-4423]

## Secure Hub for Android 23.10.0

### 解決された問題

Android バージョン 11 以降では、Android Enterprise デバイスで Wi-Fi ポリシーが展開されない可能性があります。この問題は、Wi-Fi ポリシーの匿名フィールドにドメイン値が指定されていない場合に発生します。[XMHELP-4379]

### 既知の問題

このリリースには既知の問題はありません。

## Secure Hub for Android 23.9.0

### 解決された問題

このリリースでは、パフォーマンスや安定性が総合的に向上する分野に対処しています。

### 既知の問題

このリリースには既知の問題はありません。



## Secure Hub for iOS 23.8.1

### 解決された問題

- ユーザーが Secure Hub 23.8.0 を使用してデバイスを登録しようとする場合に、ユーザー名の形式がSAMAccountだと、プロセスが失敗し、次のエラーメッセージが表示されます。

「登録に失敗しました。MAM のログイン済みユーザーが登録ユーザーと一致しません。もう一度登録してください。」 [XMHELP-4410]

### 既知の問題

このリリースには既知の問題はありません。

## Secure Hub for iOS 23.8.0

### 解決された問題

- nFactor を使用して iOS デバイスを Citrix Endpoint Management (CEM) に登録すると、マイクロ VPN トンネルを確立する際に問題が発生する可能性があります。 [XMHELP-4390]

### 既知の問題

このリリースには既知の問題はありません。

### 古いバージョンでの既知の問題と修正された問題

Secure Hub の以前のバージョンでの既知の問題と解決された問題については、「[Secure Hub の既知の問題および解決された問題の履歴](#)」を参照してください。

### 認証を求められるシナリオ

October 31, 2022

Secure Hub では、ユーザーの認証が必要になり、デバイスで資格情報の入力求められるさまざまなシナリオがあります。

シナリオは次の要因によって異なります：

- Endpoint Management コンソール設定での MDX アプリポリシーおよびクライアントプロパティの設定。
- 認証が行われるのがオフラインかオンラインか（デバイスは Endpoint Management へのネットワーク接続が必要）。

また、ユーザーが入力する資格情報の種類（Active Directory パスワード、Citrix PIN やパスコード、ワンタイムパスワード、指紋認証（iOS では Touch ID）も、認証の種類や頻度によって異なります。

最初に、認証を求められる結果となるシナリオについて説明します。

- デバイスの再起動：ユーザーは、デバイスを再起動する場合、Secure Hub で再認証する必要があります。
- 非アクティブなオフライン（タイムアウト）：デフォルトでアプリパスコードの MDX ポリシーが有効になっていると、Endpoint Management のクライアントプロパティ「Inactivity Timer」が機能します。Inactivity Timer は、セキュアコンテナを使用するすべてのアプリにおいて、ユーザーアクティビティのない状態で経過する最大時間を制限します。

指定された時間内にユーザーアクティビティがないと、ユーザーはデバイスのセキュアコンテナに資格情報を再入力しなければなりません。たとえば、Inactivity Timer の有効期限が切れている場合は、ユーザーがデバイスを置いてその場を離れても、ほかのユーザーがそのデバイスを使ってコンテナ内の機密情報にアクセスすることはできません。**Inactivity Timer** の設定は Endpoint Management コンソールで行います。デフォルトは 15 分です。[オン] に設定されたアプリパスコードと Inactivity Timer の組み合わせは、認証を求められるシナリオの多くに影響します。

- **Secure Hub** からのサインオフ：Secure Hub からサインオフすると、Secure Hub や MDX アプリの次回アクセス時に、アプリパスコードの MDX ポリシーと Inactivity Timer の状態で定められた通りに、パスコード入力を求めるメッセージが表示されるため、ユーザーは再入力の必要があります。
- 最大オフライン期間：このシナリオはアプリ単位の MDX ポリシーによって引き起こされるので、個別のアプリにのみ当てはまります。MDX ポリシーの最大オフライン期間は、デフォルトで 3 日です。Secure Hub でアプリをオフラインで実行できる最大期間が経過すると、アプリ使用権の確認とポリシー更新のために、Endpoint Management からのチェックインが必要になります。チェックインが行われると、Secure Hub でアプリのオンライン認証が求められます。MDX アプリを使用する前に、パスコードを再入力する必要があります。

最大オフライン期間とアクティブなポーリング周期の関係に注意してください。

- アクティブなポーリング周期とは、アプリが Endpoint Management からチェックインして、アプリのロックやワイプなどのセキュリティ操作を実行する周期のことです。またアプリは、アプリのポリシー更新もチェックします。
- アクティブなポーリング周期のポリシー経由で、ポリシーのチェックが正常に行われると、最大オフライン期間のタイマーがリセットされ、再びカウントダウンが始まります。

アクティブなポーリング周期、および最大オフライン期間の経過後のいずれについても、Endpoint Management からのチェックインには、デバイスに有効な Citrix Gateway トークンがあることが必要です。デバイスに有効な Citrix Gateway トークンがある場合、アプリは一切の中断なく、Endpoint Management から新しいポリシーを

取得します。アプリで Citrix Gateway トークンが必要な場合は、Secure Hub に切り替わり、認証を求めるメッセージが表示されます。

Android デバイスでは、Secure Hub のアクティビティ画面が、現在使用中のアプリ画面の上部に直接表示されます。iOS デバイスでは、Secure Hub が最前面に表示されて、現在使用中のアプリが一時的に隠れます。

ユーザーが資格情報を入力すると、Secure Hub が元のアプリに戻ります。この場合に、キャッシュされた Active Directory 資格情報を許可するか、設定済みのクライアント資格情報があれば、ユーザーは PIN、パスワード、または指紋認証を入力できます。そうでない場合は、Active Directory の資格情報をすべて入力する必要があります。

次の Citrix Gateway ポリシーで説明するように、非アクティブな Citrix Gateway セッション、または強制的なセッションタイムアウトポリシーにより、Citrix ADC トークンが無効になることがあります。Secure Hub に再度サインインすると、アプリの実行を続けることができます。

- **Citrix Gateway** セッションポリシー： Citrix Gateway の 2 つのポリシーも、ユーザーが認証を求められるシナリオに影響します。このような場合、Citrix Gateway ポリシーが、Endpoint Management に接続するための、Citrix ADC とのオンラインセッションを確立する認証を行います。
  - セッションのタイムアウト： 設定された期間内にネットワークアクティビティが発生しない場合、Endpoint Management の Citrix ADC セッションが切断されます。デフォルトは 30 分です。ただし、Citrix Gateway ウィザードを使用してポリシーを設定すると、デフォルトは 1440 分になります。社内ネットワークへの再接続に、資格情報の入力を求めるメッセージが表示されます。
  - 強制的なタイムアウト： この設定が [オン] の場合は、強制的なタイムアウト期間の経過後に、Endpoint Management の Citrix ADC セッションが切断されます。強制的なタイムアウトでは、設定された期間後に、資格情報の再入力が必要で、次の使用時に、社内ネットワークへの再接続に、資格情報の入力を求めるメッセージが表示されます。デフォルトは [オフ] です。ただし、Citrix Gateway ウィザードを使用してポリシーを設定すると、デフォルトは 1440 分になります。

### 資格情報の種類

前のセクションでは、どのような場合にユーザーが認証を求められるかについて説明しました。このセクションでは、ユーザーの入力が必要な資格情報の種類について説明します。デバイス上の暗号化されたデータにアクセスするには、さまざまな認証方法での認証が必要です。最初にデバイスのロックを解除するには、プライマリコンテナのロックを解除します。これが発生してコンテナが再び保護されると、再度アクセスするために、セカンダリコンテナのロックを解除します。

#### 注：

管理対象アプリという用語は、MDX Toolkit でラップしたアプリを指します。この場合の MDX Toolkit は、アプリパスコードの MDX ポリシーがデフォルトで有効のまま、Inactivity Timer が活用されています。

資格情報の種類を決定する状況は次の通りです：

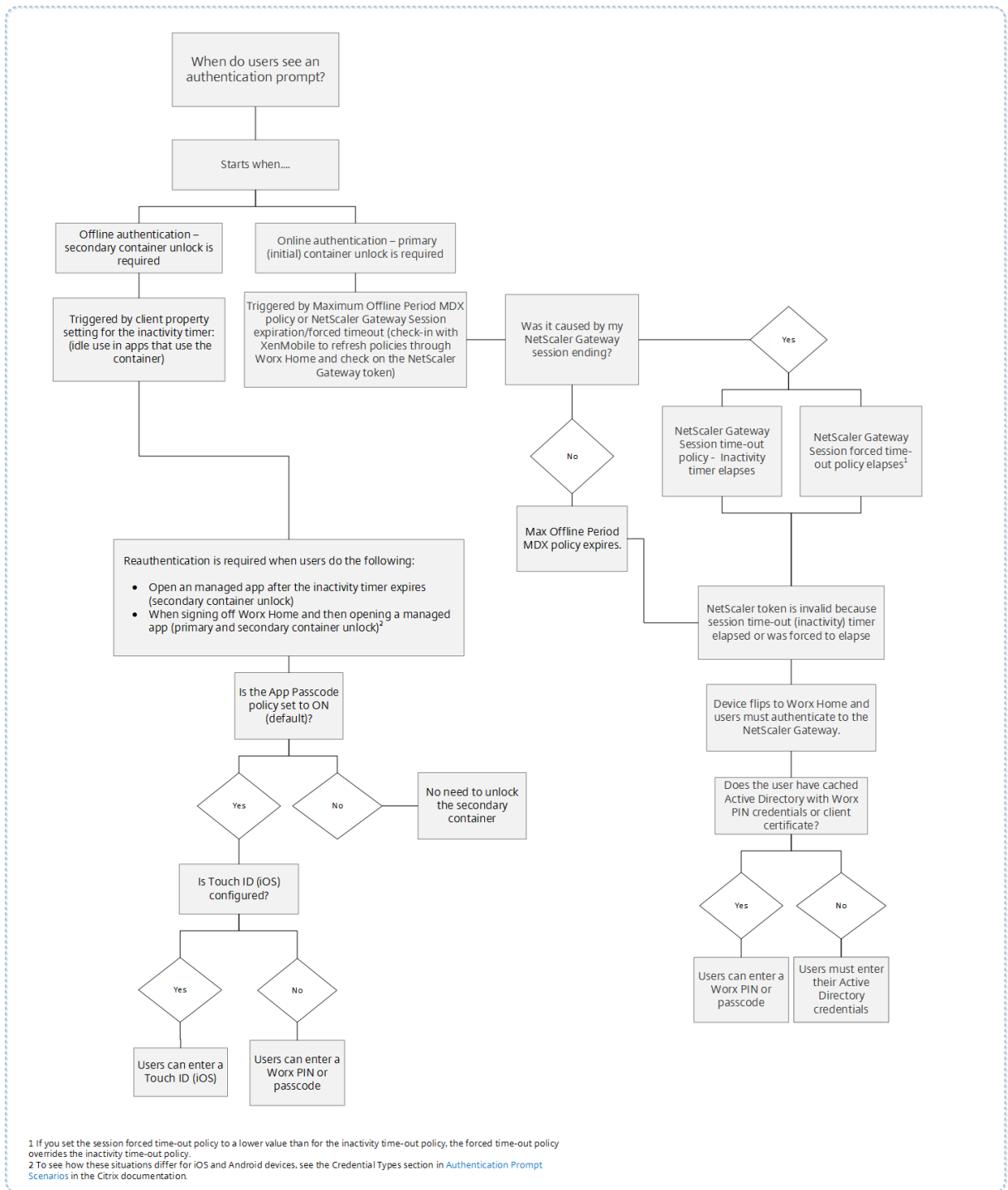
- プライマリコンテナのロック解除: Active Directory パスワード、Citrix PIN またはパスコード、ワンタイムパスワード、Touch ID またはフィンガープリント ID は、プライマリコンテナをロック解除するために必要です。
  - iOS で、デバイスに管理対象アプリをインストールした後に、Secure Hub または管理対象アプリを最初に開く場合。
  - iOS で、デバイスを再起動してから Secure Hub を開く場合。
  - Android で、Secure Hub が実行されていないときに管理対象アプリを開く場合。
  - Android で、デバイスの再起動を含む何らかの理由で、Secure Hub を再起動する場合。
- セカンダリコンテナのロック解除: セカンダリコンテナのロック解除には、指紋認証（設定されている場合）、Citrix PIN またはパスコード、Active Directory 資格情報のいずれかが必要です。
  - Inactivity Timer の有効期限が切れた後に、管理対象アプリを開く場合。
  - Secure Hub のサインオフ後に管理対象アプリを開く場合。

次の状況が当てはまる場合は、いずれのコンテナのロック解除にも Active Directory 資格情報が必要です:

- ユーザーがコーポレートアカウントと関連付けられたパスコードを変更する場合。
- Citrix PIN: 「ENABLE\_PASSCODE\_AUTH」および「ENABLE\_PASSWORD\_CACHING」を有効化するためのクライアントプロパティを Endpoint Management コンソールで設定していない場合。
- 次の状況で NetScaler Gateway セッションが終了した場合: セッションタイムアウトまたは強制的なタイムアウトポリシーのタイマーが有効期限切れとなり、デバイスで資格情報がキャッシュされていないか、デバイスにクライアント証明書がない。

指紋認証が有効な時に、アプリが無効なためにオフライン認証が求められた場合、ユーザーは指紋を使用してサインインできます。ただし、初めて Secure Hub にサインインしたり、デバイスを再起動したりする場合には、PIN を入力する必要があります。指紋認証の有効化について詳しくは、「[指紋認証または Touch ID 認証](#)」を参照してください。

次のフローチャートは、認証情報の入力を求められたとき、どの資格情報を入力するか判断するためのフローです。



### Secure Hub の画面切り替えについて

このほかに注意すべき状況としては、アプリから Secure Hub への切り替えと、元のアプリへの切り替えが必要な場合が挙げられます。画面が切り替わると、ユーザーの確認が必要な通知が表示されます。このとき、認証は必要ありません。この状況が生じるのは、最大オフライン期間とアクティブなポーリング周期で指定された Endpoint

Management からのチェックイン後に、Endpoint Management が、Secure Hub によるデバイスへのプッシュ通知が必要な、ポリシーの更新を検出した場合です。

### デバイスのパスコードにおけるパスコードの複雑さ (**Android 12** 以降)

パスコードの複雑さは、カスタムのパスワード要件よりも優先されます。パスコードの複雑さのレベルは、事前定義されたレベルの 1 つです。したがって、エンドユーザーは複雑さのレベルが低いパスワードを設定できません。

Android 12 以降のデバイスのパスコードの複雑さは次のとおりです：

- パスコードの複雑さを適用する：カスタムのパスワード要件ではなく、プラットフォームによって定義された複雑さのレベルのパスワードが必要です。Android 12 以降で Secure Hub 22.9 以降を使用しているデバイスのみ対象。
- 複雑さのレベル：事前定義されたパスワードの複雑さのレベル。
  - なし：パスワードは必要ありません。
  - 低：パスワードは次の場合があります：
    - \* パターン
    - \* PIN (4 つ以上の数字)
  - 中：パスワードは次の場合があります：
    - \* 繰り返しの文字 (4444) または順番どおりの文字 (1234) ではない PIN と、最低 4 つの数字
    - \* 4 文字以上のアルファベット
    - \* 4 文字以上の英数字
  - 高：パスワードは次の場合があります：
    - \* 繰り返しの文字 (4444) または順番どおりの文字 (1234) ではない PIN と、最低 8 つの数字
    - \* 6 文字以上のアルファベット
    - \* 6 文字以上の英数字

#### 注：

- BYOD デバイスの場合、最小文字数、必須文字、生体認証、詳細規則などのパスコード設定は、Android 12 以降では適用できません。代わりにパスコードの複雑さを使用してください。
- 仕事用プロファイルのパスコードの複雑さが有効になっている場合は、デバイス側のパスコードの複雑さも有効にする必要があります。

詳しくは、Citrix Endpoint Management のドキュメントの「[Android Enterprise の設定](#)」を参照してください。

### 派生資格情報を使用したデバイスの登録

November 21, 2020

派生資格情報によって、モバイルデバイスに強力なユーザー認証が得られます。資格情報は、スマートカードから派生したもので、カードの代わりにモバイルデバイスの中に存在します。スマートカードは、Personal Identity Verification (PIV) カードまたは Common Access Card (CAC) です。

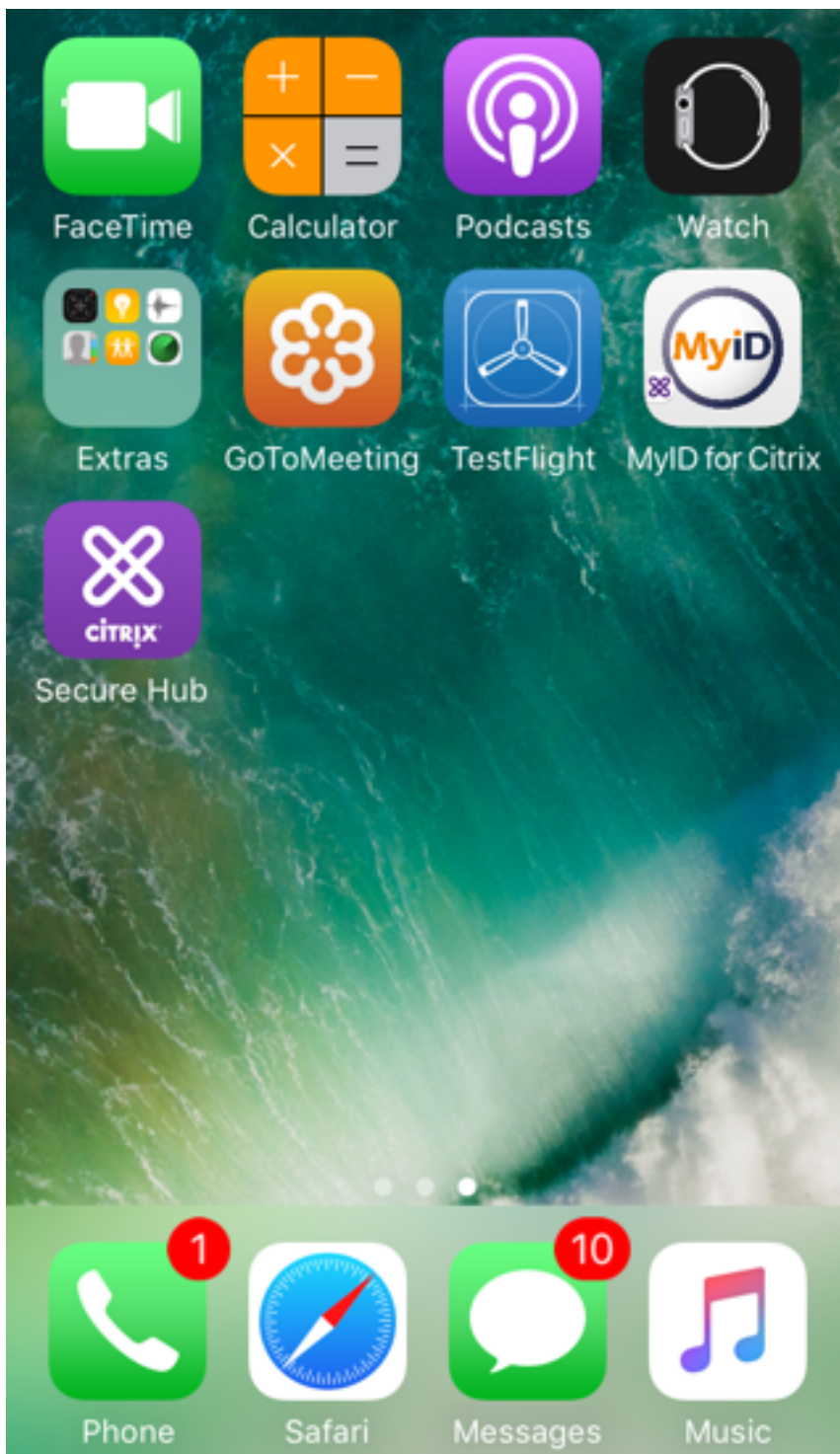
派生資格情報は、UPN などのユーザー識別子を含む登録証明書です。Endpoint Management は、資格情報プロバイダーから取得した資格情報をデバイスの安全なコンテナに保管します。

Endpoint Management では、iOS デバイスの登録に派生資格情報を使用できます。Endpoint Management を派生資格情報用に構成した場合、iOS デバイスの登録招待状や他の登録モードはサポートされません。ただし同じ Endpoint Management サーバーを使用して、登録招待状や他の登録モードで Android デバイスを登録することはできます。

### 派生資格情報を使用する場合のデバイス登録手順

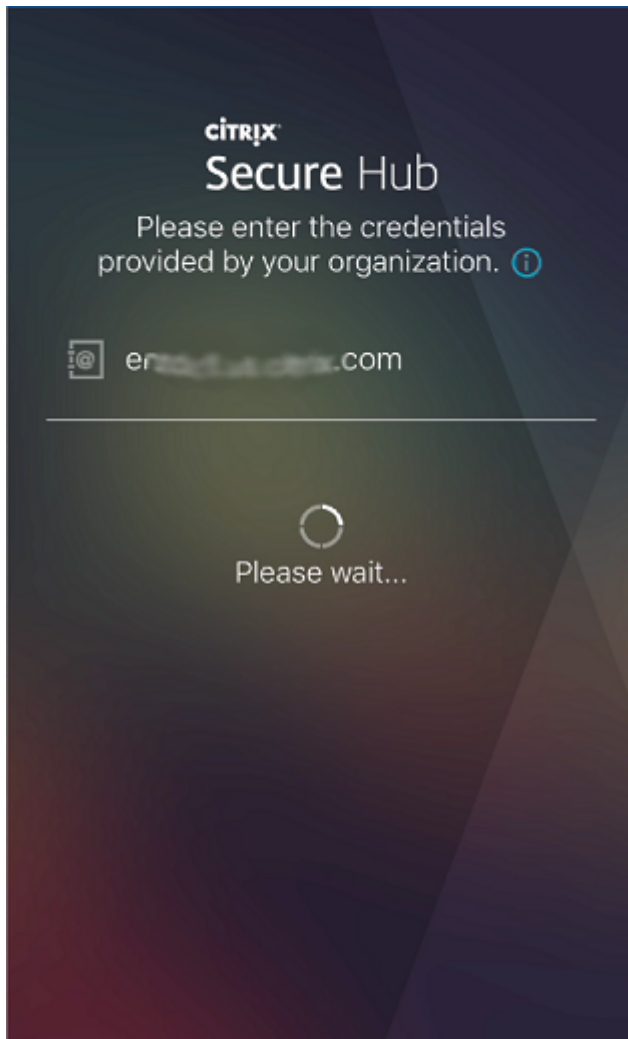
登録するには、デスクトップに取り付けられたスマートカードリーダーにユーザーが各自のカードを挿入する必要があります。

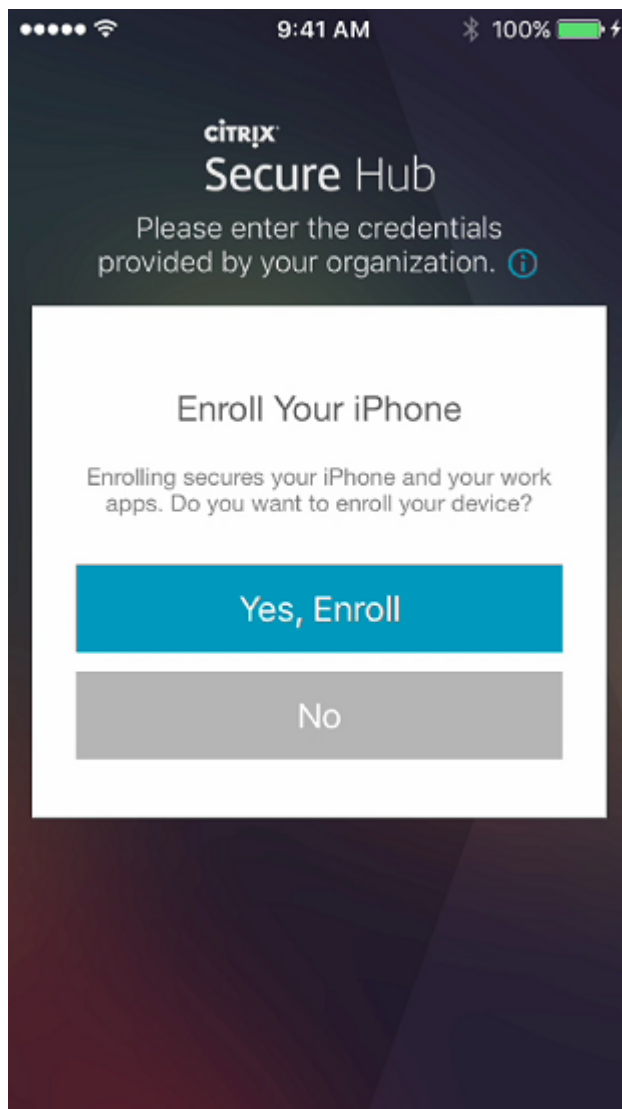
1. 派生資格情報プロバイダーから Secure Hub とアプリをインストールします。この例では、ID プロバイダーアプリは、Intercede MyID Identity Agent です。

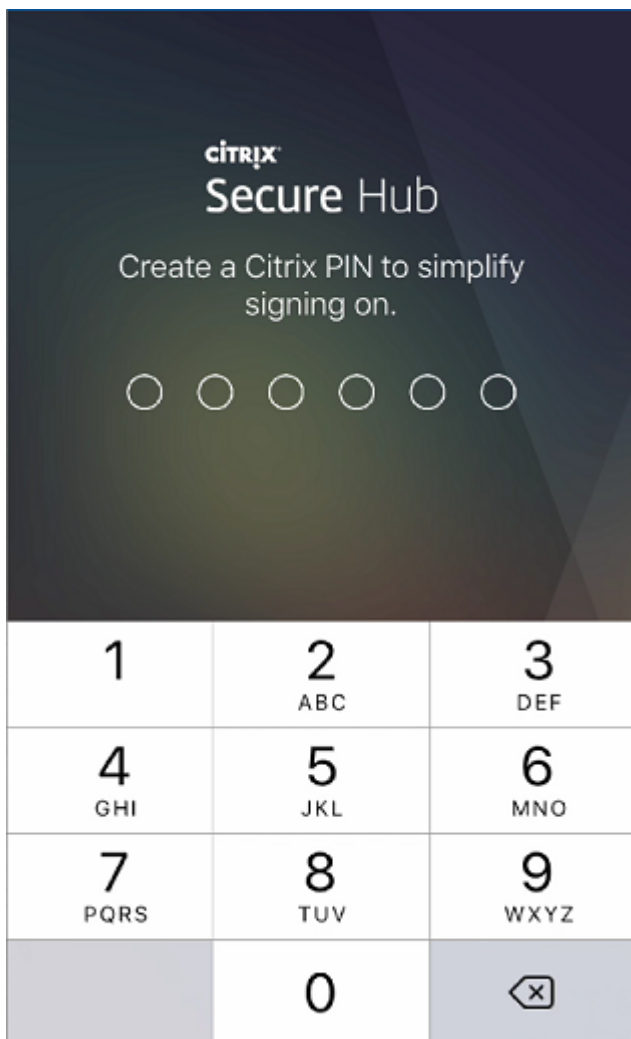


2. Secure Hub を起動します。プロンプトが表示されたら、Endpoint Management の完全修飾ドメイン名 (FQDN) を入力して [次へ] をクリックします。Secure Hub への登録が開始されます。Endpoint Management で派生資格情報がサポートされる場合、Secure Hub から Citrix PIN を作成するように求められます。

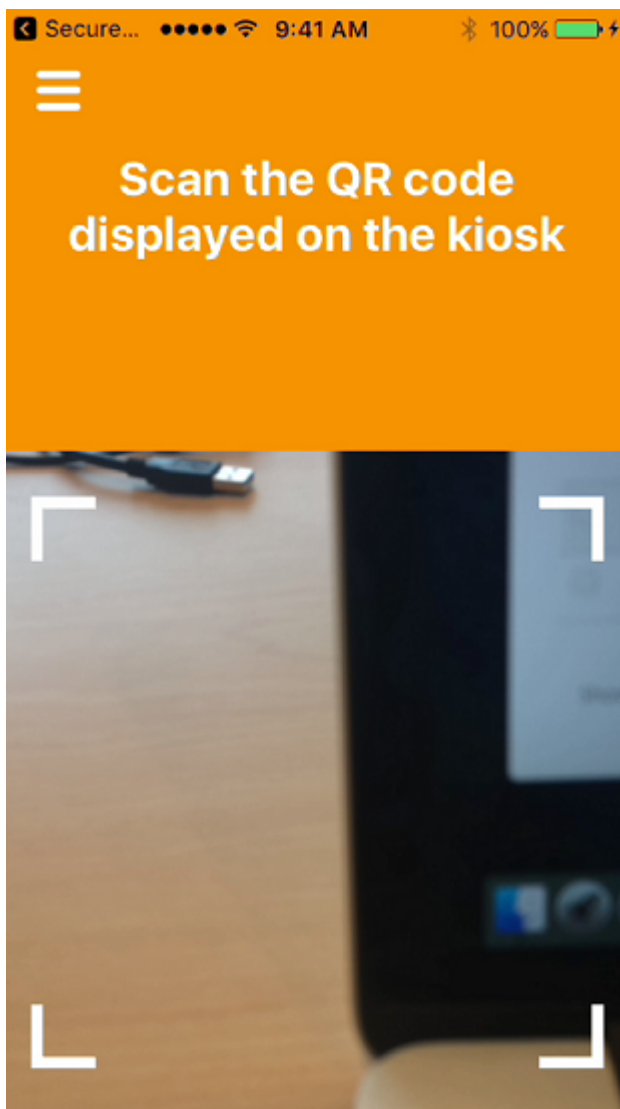




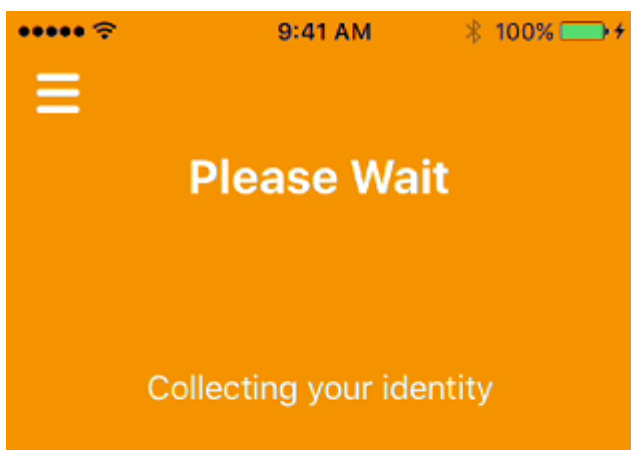




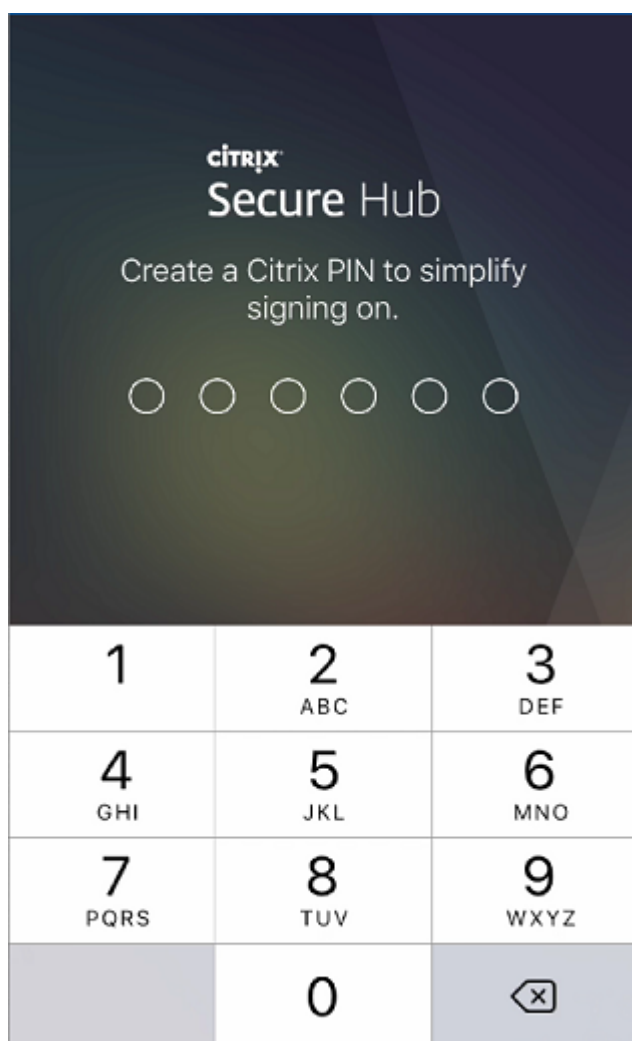
3. 指示に従ってスマート資格情報をアクティブ化します。スプラッシュ画面に続いて、QRコードのスクリーンを求めるプロンプトが表示されます。



4. デスクトップに取り付けられたスマートカードリーダーに、カードを挿入します。デスクトップのアプリによって QR コードが表示され、モバイルデバイスを使用してコードをスキャンするよう求められます。



プロンプトが表示されたら、Secure Hub の PIN を入力します。



PINの認証後に、Secure Hubによって証明書がダウンロードされます。後はプロンプトに従って登録を完了させます。

Endpoint Management コンソールでデバイス情報を表示するには、次のいずれかを実行します：

- [管理] > [デバイス] の順に移動し、コマンドボックスを表示するデバイスを選択します。[詳細表示] をクリックします。
- [分析] > [ダッシュボード] の順に移動します。

## Citrix Endpoint Management コンソールを使用したヒントの構成

February 27, 2024

管理者は、登録モードが 2 要素に設定されているデバイスの Secure Hub サインインページでヒントを構成できます。次のいずれかの方法でヒントを構成できます：

- ヒントをテキストとして構成する
- Web ページのリンクを記載したヒントのテキストを構成する

### ヒントをテキストとして構成する

ヒントのテキストを構成するには、次の手順を実行します：

1. Citrix Endpoint Management コンソールに管理者資格情報を使用してサインインします。
2. [設定] > [クライアントプロパティ] に移動して、[Add New Client Property] をクリックします。
3. [キー] ドロップダウンリストから、[カスタムキー] を選択します。
4. [キー] フィールドに、**enrollment.twofactor.token.hint** と入力します。
5. [値] フィールドには、サインインページにヒントとして表示されるテキストを入力できます。ヒントは、ユーザーが 2 要素認証用の PIN を見つけることができるようガイドします。
6. [名前] フィールドに、**enrollment.twofactor.token.hint** と入力します。
7. [説明] フィールドに、構成したヒントに関して今後の参考になるようなコメントを入力できます。

Settings > Client Properties > Add New Client Property

#### Add New Client Property

Key	Custom Key
Key *	enrollment.twofactor.token.hint
Value *	Please check your mail for security token/PIN
Name *	enrollment.twofactor.token.hint
Description *	Please check your mail for security token/PIN. This is where to get your security token/PIN.

8. [保存] をクリックします。

構成を完了すると、ヒントのテキストがサインインページに表示されます。

citrix | Secure Hub

Please enter the credentials provided by your organization.

Username

Password

Pin

Please check your mail for security token/PIN

Back Next

Privacy Policy

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

## Web ページのリンクを記載したヒントのテキストを構成する

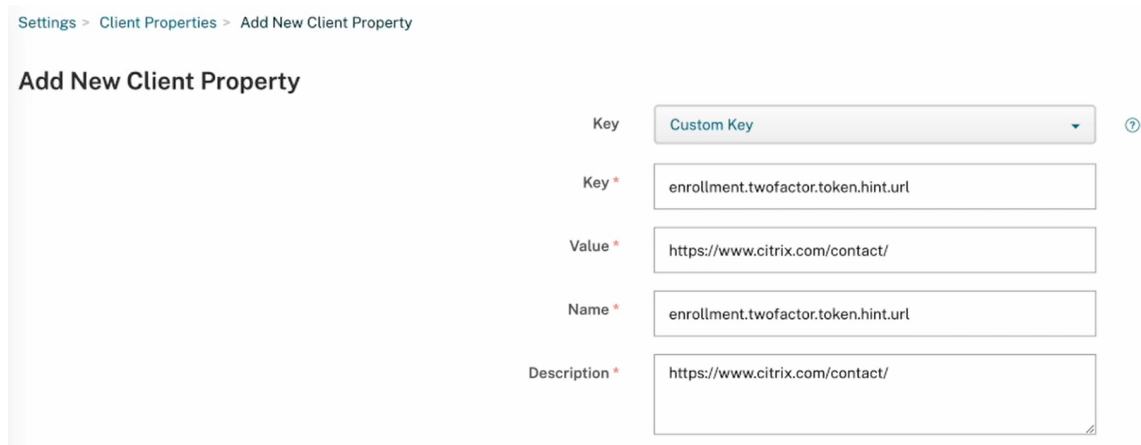
PIN へのアクセスに関する詳細情報を含む Web ページを構成できます。後から、ヒントのテキストで Web ページのリンクをハイパーリンクとして指定します。ユーザーがサインインページのヒントをクリックすると、Secure Hub は埋め込みブラウザを開き、既に構成されている Web ページに移動します。

Web ページのリンクを使用してヒントのテキストを構成するには、まず、「[ヒントをテキストとして構成](#)」の記事で説明されているように、ヒントのテキストを構成する必要があります。完了したら、次の手順に進みます：

1. Citrix Endpoint Management コンソールに管理者資格情報を使用してサインインします。
2. [設定] > [クライアントプロパティ] に移動して、[**Add New Client Property**] をクリックします。
3. [キー] ドロップダウンリストから、[カスタムキー] を選択します。
4. [キー] フィールドに、**enrollment.twofactor.token.hint.url** と入力します。
5. [値] フィールドに、構成した Web ページの URL を入力します。
6. [名前] フィールドに、**enter enrollment.twofactor.token.hint.url** と入力します。
7. [説明] フィールドに、構成したヒントに関して今後の参考になるようなコメントを入力できます。

注：

ユーザーがヒントのリンクをクリックすると、埋め込みブラウザに Web ページが表示されます。



Settings > Client Properties > Add New Client Property

### Add New Client Property

Key	Custom Key
Key *	enrollment.twofactor.token.hint.url
Value *	https://www.citrix.com/contact/
Name *	enrollment.twofactor.token.hint.url
Description *	https://www.citrix.com/contact/

8. [保存] をクリックします。

構成を完了すると、ヒントのテキストが Web ページのリンクとともにサインインページに表示されます。



citrix | Secure Hub

Please enter the credentials provided by your organization.

 Username

 Password

 Pin

Where to get your enrollment token?

[Back](#) [Next](#)

[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.



© 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).