CITRIX

Secure Hub

Contents

Citrix Secure Hub

June 13, 2019

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 およびそのほか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。

このリリースでの新機能

Secure Hub for Android 19.5.5

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。

以前のリリースの新機能

Secure Hub 19.5.0、19.4.5、および 19.3.5

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。WiFi 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、「[WiFi デバイスポリシー。]」を参照してください。(/ja-jp/citrix-endpoint-management/policies/wifi-policy.html)
- 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。(/ja-jp/citrix-endpoint-management/policies/custom-xml-policy.html)
- 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。(/ja-jp/citrix-endpoint-management/policies/files-policy.html)

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、シトリックス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、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 18.10.0

- **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。

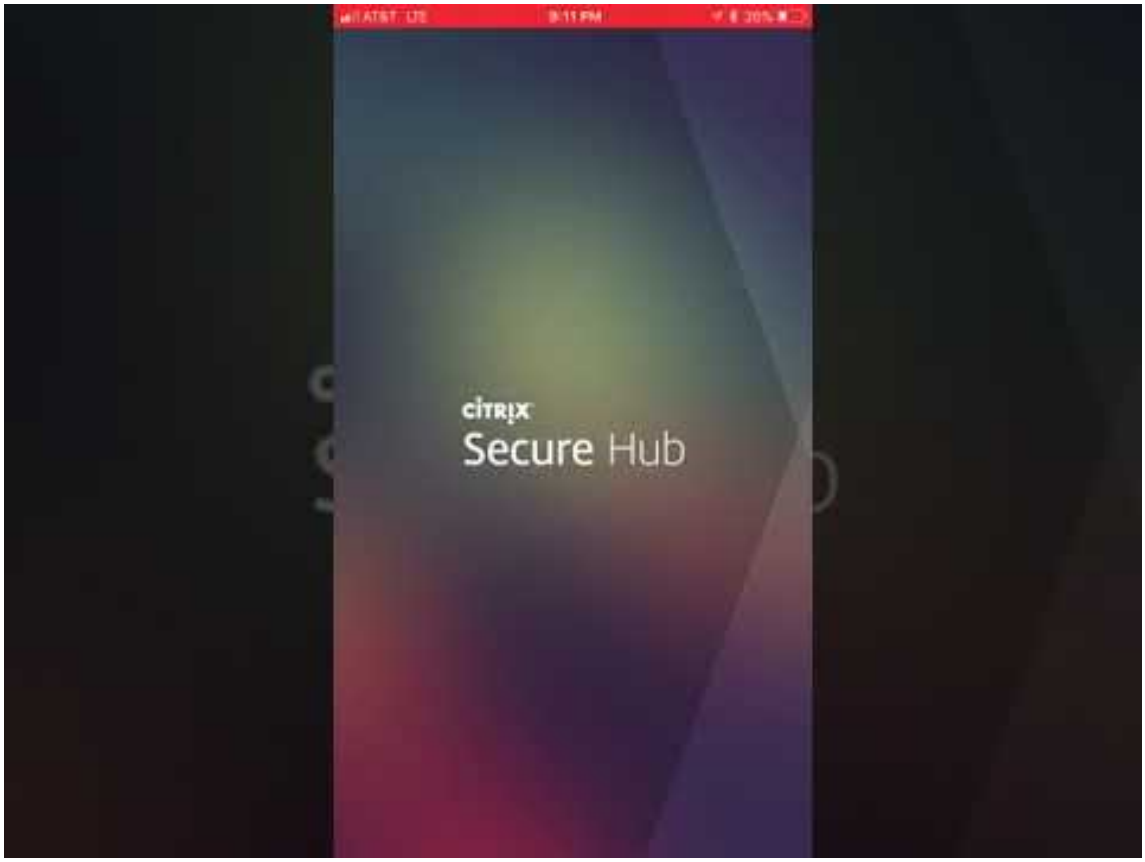
- **Android SafetyNet** のサポート： **Android SafetyNet** 機能を使用して、Secure Hub がインストールされている Android デバイスの互換性とセキュリティを評価するように Endpoint Management を設定できます。結果は、デバイス上で自動化された操作をトリガーするために使用できます。詳しくは、「Android SafetyNet」を参照してください。
- **Android Enterprise** デバイスのカメラ使用を禁止する： 制限デバイスポリシーの新しい設定である ［カメラの使用を許可］ を設定することで、ユー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

バグの修正とパフォーマンスの向上。

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詳しくは、「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詳しくは、「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詳しくは、「ワークスペース構成」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。
- 証明書のピンニングを有効にすると、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 Developer サイトのAndroid P の動作の変更点に関する記事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の指定、および PIN の強度と長さの要件の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、および無通信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。

証明書ピンニング

Secure Hub for iOS および Secure Hub for Android は、SSL 証明書ピンニング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。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、「Endpoint Management AutoDiscovery サービス」を参照してください。
- プライベート/自己署名 CA と Endpoint Management Auto Discovery 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、証明書のピンニング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。証明書のピンニングを有効にすると、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。ユーザーが証明書を承認しない場合、登録は失敗します。

証明書ピンニングを使用するには、Citrix ADS サーバーへの証明書のアップロードをシトリックスに依頼する必要があります。シトリックス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。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。
- 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 でこの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。
3. 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。

   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。

4. 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。
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。
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。
13. ［バインド］ 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。
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。

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 にアクセスできる必要があります。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、シトリックス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ニング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。

証明書ピンニング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:

完全修飾ドメイン名	IP アドレス	ポート	IP とポートの使用
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - ADS 通信
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - ADS 通信
ads.xm.cloud.com: Secure Hub バージョン 10.6.15 以降ではads.xm.cloud.com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
ads.xm.cloud.com: Secure Hub バージョン 10.6.15 以降ではads.xm.cloud.com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

証明書ピンニングが有効な場合、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ニング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。

証明書ピンニング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。証明書ピンニングは、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。

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。デバイス登録について詳しくは、「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、シトリックスからのものではありません。［許可］ をタップしても、シトリックスと、Secure Hub を管理する管理者には、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ないか、Secure Mail に登録する追加手順を実行する必要がないことを意味します。

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、電子メールアドレスを使用して自動検出します。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。

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。

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。

［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、シトリックス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 ［シトリックスサポート］ をタップして、Citrix Knowledge Centerを開くこともできます。ここでは、すべてのシトリックス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ない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。Crashyltics 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。

既知の問題と解決された問題

June 13, 2019

Secure Hub for Android 19.5.5 の既知の問題

- Secure Hub for Android で、特定業務専用コーポレート所有端末（COSU）モードのデバイスを登録すると数分後に接続が切断され、GCM が有効になっていても通知を受け取らなくなります。[CXM-62977]
- プロファイル所有者モードとデバイス所有者モードのデバイスに場所ポリシーを同時展開すると、デバイス所有者モードのユーザーアカウントが削除されます。この問題は、NFC バンプ登録中および Endpoint Management が MDM モードで設定されている場合に発生します。[CXM-63429]

Secure Hub for Android 19.5.5 で解決された問題

- このリリース以降、Secure Hub は Android 5.0 以降を実行するデバイスのみでサポートされます。[CXM-35542]
- Secure Hub for Android で、デバイス所有者モードでデバイスを登録し、新しいパスワードを設定します。この場合、最初の試行でデバイスがロックされていません。[CXM-66509]

以前のバージョンでの既知の問題と解決された問題

Secure Hub for Android バージョン **19.5.0** の既知の問題

- 登録後、OnePlus Android バージョン 7.1.1 および OnePlus 5T Android バージョン 9.0.3 の Secure Hub で Citrix PIN の入力画面を表示するには、手動で再起動する必要があります。[CXM-64120]
- Secure Hub for Android では、ポリシーまたはストアを更新しない限り、必須アプリは Android デバイスに展開されません。[CXM-65635]

Secure Hub for Android バージョン **19.5.0** で解決された問題

- このリリース以降、Secure Hub は Android 5.0 以降を実行するデバイスのみでサポートされます。[CXM-35542]
- Secure Hub for Android では、サーバー証明書に複数のサブジェクトの別名が存在する場合、Android 6.0 デバイスの登録に失敗します。[CXM-65030]
- Secure Hub for Android では、管理対象アプリがデバイスの登録解除後もアンインストールされません。[CXM-65369]
- Samsung S9 デバイスでは、ユーザーが Android P にアップデートした後に次の問題が発生します: Endpoint Management 経由でデバイスパスワードを変更したときに、デバイス上でパスワードが変更されません。代わりに表示画面が黒色になり、Endpoint Management コンソールにデバイスがロックされたステータスが表示されます。[CXM-66391]

Secure Hub バージョン **19.4.5** の既知の問題

このリリースには既知の問題はありません。

バージョン **19.4.5** で解決された問題

Secure Hub for iOS

iOS デバイスでは、デバイス登録リンクをクリックしても、Endpoint Management の FQDN、インスタンス名が Secure Hub に自動的に入力されません。デバイス登録要求は失敗します。[CXM-65423]

Secure Hub for Android

このリリースで解決された問題はありません。

バージョン **19.3.5** の既知の問題

Secure Hub for iOS

Secure Hub for iOS から通知が送信されると、Secure Hub の通知バッジの数字が更新されません。[CXM-53500]

Secure Hub for Android

このリリースには既知の問題はありません。

バージョン **19.3.5** で解決された問題

Secure Hub for iOS

このリリースで解決された問題はありません。

Secure Hub for Android

- Secure Hub for Android では、共有デバイスを登録し、**Web** クリップポリシーを展開し、Web および SaaS アプリを追加すると、展開は成功します。ただし、Citrix Endpoint Management コンソールのアプリインベントリ画面では、展開が失敗したと表示されます。[CXM-57500]
- Secure Hub for Android では、ユーザーが Secure PIN でログインすると VPN トンネルが確立されますが、Secure Web は Web サイトを読み込みません。ただし、Secure Web を閉じて再度開くと、Web サイトが正常に読み込まれます。[CXM-60751]
- Microsoft Intune ポリシーが構成された Secure Mail for Android では、認証後空白の画面が表示されます。[CXM-61457]
- Secure Hub for Android では、暗号化を無効にしたアプリが Secure Hub から暗号キーを取得しようとします。[CXM-61459]
- Intune ポータルサイトバージョン 5.0.4324.0 がインストールされている場合、Secure Mail for Android は起動時にクラッシュします。詳しくは、Support Knowledge Center の記事を参照してください。[CXM-62516]
- Secure Hub for Android は、Android 7.1.1 が動作する Android Enterprise デバイスの特定業務専用コーポレート所有端末（COSU）で、システムアプリを使用できません。[CXM-63653]
- Secure Hub for Android では、Google Play で複数のアプリを必須アプリとして構成し登録しようとすると、最初のアプリをインストールするよう求められます。このプロンプトの後にすぐ次のプロンプトが表示され、2 番目のアプリをインストールするよう促し、以降は同様にプロンプトが表示されます。[CXM-63654]

バージョン **19.3.0** の既知の問題

Secure Hub for iOS

このリリースには既知の問題はありません。

Secure Hub for Android

- Secure Hub for Android では、共有デバイスを登録し、Web クリップポリシーを展開し、Web および SaaS アプリを追加すると、展開は成功します。ただし、Citrix Endpoint Management コンソールのアプリインベントリ画面では、展開が失敗したと表示されます。[CXM-57500]
- Android Enterprise デバイスでは、ジオフェンスが侵害されたときに場所ポリシーでロック操作が設定されている場合、システムによって生成されたパスコードを使用する代わりに、新しいパスコードを設定するように求められます。[CXM-60425]

バージョン **19.3.0** で解決された問題

Secure Hub for iOS

このリリースで解決された問題はありません。

Secure Hub for Android

完全に管理されている Android Enterprise デバイスを、パスコードを使用したロックによるセキュリティ操作を使用してリモートでロックしようとすると、エラーメッセージの表示なく失敗することがあります。デバイスが確実にロックされるようにするには、パスコードを使用したロックを 2 回設定します。デバイスは、2 度目に設定したパスコードでロックされます。[CXM-61095]

バージョン **19.3.0** の既知の問題

Secure Hub for iOS

このリリースには既知の問題はありません。

Secure Hub for Android

- Secure Hub for Android では、共有デバイスを登録し、Web クリップポリシーを展開し、Web および SaaS アプリを追加すると、展開は成功します。ただし、Citrix Endpoint Management コンソールのアプリインベントリ画面では、展開が失敗したと表示されます。[CXM-57500]
- Android Enterprise デバイスでは、ジオフェンスが侵害されたときに場所ポリシーでロック操作が設定されている場合、システムによって生成されたパスコードを使用する代わりに、新しいパスコードを設定するように求められます。[CXM-60425]

バージョン **19.3.0** で解決された問題

Secure Hub for iOS

このリリースで解決された問題はありません。

Secure Hub for Android

完全に管理されている Android Enterprise デバイスを、パスコードを使用したロックによるセキュリティ操作を使用してリモートでロックしようとすると、エラーメッセージの表示なく失敗することがあります。デバイスが確実にロックされるようにするには、パスコードを使用したロックを 2 回設定します。デバイスは、2 度目に設定したパスコードでロックされます。[CXM-61095]

バージョン **19.2.0** の既知の問題

バージョン 19.2.0 には既知の問題はありません。

バージョン **19.2.0** で解決された問題

Secure Hub for iOS

Secure Hub for iOS では、ユーザーが Secure Hub ストアからログオフすると、次の SSL ハンドシェイクの失敗メッセージが繰り返し表示されます：アプリを取得するネットワーク要求がサーバからタイムアウトされます。[CXM-61339]

Secure Hub for Android

- Android Enterprise のファイルデバイスポリシーが仕事用プロファイルモードの Android デバイスに展開されません。[CXM-61196]
- Secure Hub for Android では、共有デバイスでの新しいユーザーのログイン認証に時間がかかります。登録ユーザーとしてログオフしてから新しいユーザーとしてログインしようとすると、デバイスを再起動するまで Secure Hub が読み込みを続けます。[CXM-61338]
- Secure Hub for Android では、クラウドの顧客が Android Enterprise デバイスを外部 ID プロバイダーで登録できません。[CXM-61738]
- Secure Hub for Android では、特定業務専用コーポレート所有端末（COSU）モードの場合、アプリのアイコンが重なって表示されます。[CXM-61740]
- Secure Hub for Android では、既存のセットアップで証明書ピンニングが有効な場合、証明書に複数のサブジェクトの別名があると認証が失敗し初回のユーザー画面に戻ります。[CXM-61933]

バージョン **19.1.5** の既知の問題

- Samsung Galaxy S8 デバイスの場合、パスワードポリシーの変更に伴って Secure Hub for Android でパスワードを更新すると、アプリのアイコンが表示されなくなります。[CXM-61177]
- Secure Hub for Android では、Android Enterprise がファイルデバイスポリシーを仕事用プロファイルモードのデバイスに展開しません。[CXM-61196]

バージョン **19.1.5** で解決された問題

- Secure Hub for Android では、ユーザーが Secure PIN でログインすると VPN トンネルが確立されますが、Secure Web は Web サイトを読み込みません。ただし、Secure Web を閉じて再度開くと、Web サイトが正常に読み込まれます。[CXM-58576]

- Secure Hub for Android では、ユーザーが Secure PIN でログインすると VPN トンネルが確立されますが、Secure Web は Web サイトを読み込みません。ただし、Secure Web を閉じて再度開くと、Web サイトが正常に読み込まれます。[CXM-60751]
- Secure Hub for Android では、TechXpert という社内アプリのログをキャプチャしようとすると、Secure Hub が再起動し、再認証を要求します。[CXM-61310]

バージョン **19.1.0** の既知の問題

Secure Hub for iOS

Secure Hub for iOS で MDX と Web/SaaS アプリを展開すると、［マイアプリ］ 画面に表示されます。［その他］をタップすると、［削除］ および ［キャンセル］ オプションを含む、古い UI ブランド設定によるポップアップが開きます。[CXM-60683]

バージョン **18.12.0** で解決された問題

- Android for Work で登録済みの Samsung Knox デバイス上に、1 日または 2 日で期限切れになるようにパスワードポリシーが設定されている場合に「パスワードの期限切れ」というメッセージが繰り返し表示されます。[CXM-59250]
- QR コードを使う登録方法では、Android Enterprise で OnePlus 5T デバイスを登録できません。[CXM-59288]

バージョン **18.11.0** で修正された問題

Secure Hub iOS

- 共有デバイスモードで登録されている Android デバイスでシングルサインオンを実行することはできません。次のエラーが表示されます：現在、コーポレート資格情報を取得できません。ShareFile への手動ログインは、管理ポリシーによりブロックされます。[CXM-58238]
- 企業所有の特定用途の（COSU）デバイスで Android ボリュームレベルを編集することができません。[CXM-58323]

バージョン **18.10.5** で解決された問題

- XenMobile Server で FIPS モードが有効になっている場合、ユーザーが Secure Hub for iOS をバージョン 18.10.5 に更新した後にアプリを開くと、暗号化関連のエラーメッセージが表示されます。解決策の更新状態については、Citrix Knowledge Center の記事を参照してください。[CXM-56454]

バージョン **10.8.25** ～ **18.10.6** で解決された問題

- Secure Hub バージョン 10.8.25 ～ 18.10.6（Android）に既知の問題はありません。次の問題は、Secure Hub で解決されています。Secure Hub に影響を与える MDX に関する問題も含まれています。

Version 18.10.0 で解決された問題

- EMS コンソールで MVPN ポリシーがオフになっている場合、Intune 管理対象アプリを開くときに Secure Hub に空白の画面が表示されます。[CXM-56033、CXM-56086、CXM-54393、CXM-54823]

バージョン **10.8.60** で解決された問題

- Samsung Galaxy Tab Active 2 SM-T395 デバイスで、管理者が XenMobile の「工場出荷時リセット無効化」の制限を設定すると、Secure Hub for Android でのセキュリティ操作である［完全なワイプ］が失敗します。[CXM-54452]
- VPN ポリシーが設定されていて、Citrix SSO アプリケーションがデバイスにインストールされていない場合、デバイスの登録時に Secure Hub for Android が応答しなくなります。［戻る］ ボタンをタップするかアプリを再起動すると反応するようになります。[CXM-54627]
- Android Enterprise 環境でのデバイスオーナーモードでの登録時、Secure Hub for Android がクラッシュします。[CXM-55008]
- Secure Hub for iOS の有効な PIN を入力した後、Secure Hub から PIN の入力を繰り返し求められます。[CXM-55047]
- Android Enterprise 環境でのプロファイルオーナーモードでの登録時、Secure Hub for Android がクラッシュします。[CXM-55076]
- Secure Hub for Android で Android Enterprise を使用すると、デフォルトで Google Chrome がインストールされます。[CXM-55232]
- Secure Hub for iOS をバージョン 10.8.55 にアップグレードすると、既存または新規 iOS デバイスを登録できなくなります。[CXM-55267]

バージョン **10.8.55** で解決された問題

- G Suite の資格情報が Endpoint Management の資格情報と異なる場合、Secure Hub にサインインして Android for Work アカウントに登録できません。[CXM-53956]

バージョン **10.8.55** で解決された **MDX** 関連の問題

- 優先 VPN モードが SecureBrowse に設定されていると、エンタープライズアプリで内部リソースへの接続の問題が発生することがあります。[CXM-52309]

- アプリケーションクラスに android.support.multidex.MultiDexApplication または android.app.Application を指定したアプリは、セキュアブラウズモードで内部ネットワークに接続できません。[CXM-53126]
- Android デバイスでは、複数の証明書が生成されており、有効期限前に証明書が失効しています。[CXM-53428]

バージョン **10.8.55** の既知の問題

- デバイスから Secure Hub アカウントを削除すると、MDM の再登録に失敗します。[CXM-54142]

バージョン **10.8.50** の既知の問題

- Secure Hub for Android で Web リンクのショートカットを追加できない。[XMHELP-952]

バージョン **10.8.35** で解決された問題

- Android O で、ポリシーによって作成されたショートカットがデバイスのホーム画面に表示されない。これは Android O の仕様です。[CXM-35460]
- Android では、一定期間使用しないと Secure Hub が Samsung タブレットで開かれません。[CXM-50797]
- Secure Hub for Android では、Samsung Knox デバイスにプッシュポリシーを展開できません。[CXM-50869]
- Secure Hub for iOS では、次のような問題が発生することがあります: Active Directory のパスワードを変更した後も、PIN を入力し続ける必要があります。[CXM-50224]

バージョン **10.8.25** で解決された問題

- MDX Toolkit バージョン 10.7.20 でラッピングしたサードパーティ製の iOS 用 Cordova アプリでは、画面の内容を不鮮明にするポリシーを有効にすると、PIN 画面ではなく黒い画面が表示されます。[CXM-48471]
- Android 7 を実行している Zebra T51 デバイスに、Citrix Launcher アプリをインストールできません。[CXM-50621]

バージョン **10.8.20** で解決された問題

- ユーザーが Android デバイスをバージョン 8（Oreo）に更新すると、Endpoint Management から展開したアプリストアからエンタープライズアプリまたは.apk アプリをインストールできません。サードパーティのアプリケーションのインストールを有効にしても、この問題は解決されません。この問題は、Samsung デバイスに限定されません。[CXM-50401]

バージョン **10.8.15** で解決された問題

- Android O を実行しているデバイスで位置情報の詳細を取得する時に、Secure Hub for Android がクラッシュします。[CXM-47893]

バージョン **10.8.10** で解決された問題

- Android デバイスでは、複数のアプリが自動的にインストールされない場合や、ユーザーが ［インストール］をクリックしない場合でも、アプリはダウンロードを続けます。その結果、データ使用率が高くなります。[CXM-46404]
- Android 7 以降を実行するデバイスの場合：パスワードを伴うロックセキュリティの操作を XenMobile Server からデバイスに送信すると、デバイスはロックされます。ただし、既存のロック画面のパスワードがある場合、デバイスのパスワードは変更されません。ユーザーは元のパスコードを使用してデバイスのロックを解除できます。[CXM-47908]

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。

認証を求められるシナリオ

April 18, 2019

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が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。
- 認証がオフラインで行われるか、またはオンラインでの認証が必要か（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、必要とされる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。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須です。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:
>
> この記事の管理対象アプリは、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で、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。

iOS VPN のインストール

March 8, 2019

iOS 10 以降のデバイスでは、Secure Hub と MDX アプリ間のローカルデータ共有をセキュリティで保護するために Secure Hub VPN が使用されます。Secure Hub VPN は、iOS 10 以降のデバイスで実行されます。Secure Hub VPN は、Secure Hub と MDX アプリがこの VPN を通じてシームレスに通信できることにより理想的なユーザーエクスペリエンスを実現します。

Secure Hub VPN は、Apple Enterprise のデベロッパーアカウント（「チーム ID」）証明書、Citrix 証明書、Enterprise 証明書、またはサードパーティの ISV 証明書で署名されたアプリで動作します。

Secure Hub VPN は、iOS 10 デバイスではデフォルトで使用されます。Secure Hub VPN が iOS 10 デバイスで実行されていない場合、MDX はデータ共有のセキュリテイ保護に iOS の共有キーチェーンを使用します。iOS の共有キーチェーンメカニズムでは、iOS「チーム ID」証明書の特定の共有キーチェーンにアクセスできるように、参加しているすべてのアプリに同じ証明書で署名されている必要があります。Citrix 署名済みの Secure Hub アプリと同じ証明書で署名されていないアプリは、Secure Hub に移動して必要な情報を取得する可能性があります。

Secure Hub VPN は、Citrix Endpoint Management Enterprise および MAM-only 展開でのみ利用可能です。Secure Hub VPN は Endpoint Management MDM-only 環境には適用されず、VPN は MDM-only の登録ではインストールされません。

Secure Hub VPN は Secure Hub と業務用モバイルアプリ間の通信に使用されます。Worx Home VPN はデバイス上のネットワークトラフィックをフィルターまたは監視せず、MDX マイクロ VPN メカニズムに依存していません。

> 注:
>
> Secure Hub VPN がデフォルトで有効になっている環境では、有効なままにすることをお勧めします。
>
> iOS では複数の VPN クライアントを 1 つの iOS デバイス上で同時に実行することができないため、次の状況に注意してください。Cisco AnyConnect や Citrix VPN などの別の VPN アプリを iOS デバイス上で実行する必要がある場合（デバイスレベルの VPN を確立するために）、Secure Hub VPN を使用することはできません。Secure Hub VPN が無効になっていない場合でも、iOS Per-App VPN を設定できます。iOS Per-App VPN を使用するアプリにより、アプリがフォアグラウンドにあるときに Per-App VPN 接続が確立されます。
>
> Secure Hub VPN を無効にするには、次のセクションを参照してください。Secure Hub VPN が無効な場合、管理対象アプリから Secure Hub への切り替えがより多く発生する可能性があります。

Endpoint Management での **Secure Hub VPN** の無効化と再有効化

Secure Hub VPN は、ユーザーが iOS 10 で Secure Hub 10.3.10 以降を使い始めるとデフォルトで有効になります。

Secure Hub VPN を無効化して、共有キーチェーンメカニズムを使用するように展開環境の iOS デバイスを設定するには、次の手順に従ってください。

1. Endpoint Management コンソールで、［設定］**>**［クライアント］**>**［クライアントプロパティ］ の順に選択します。
2. ［クライアントプロパティ］ ページで、**ENABLE_NETWORK_EXTENSION** という名前のカスタムクライアントプロパティを作成し、値を 0 に設定します。

   Secure Hub VPN を再有効化するには、Secure Hub VPN に移動して、**ENABLE_NETWORK_EXTENSION** の値を 1 に設定します。

クライアントデバイス上での **Secure Hub VPN** のインストール

Secure Hub VPN は、Secure Hub 10.3.10 以降が iOS 10 デバイス上にインストールされた後、または Secure Hub 10.3.10 以降を実行しているデバイスを iOS 10 にアップグレードするときの 2 つのケースでインストールされます。

ユーザーには、次の情報メッセージが表示されます。

その後、VPN 構成の追加の許可を求める iOS メッセージが表示されます。このメッセージは、VPN が初めてインストールされるときに一度だけ表示されます。Secure Hub を再び開くときには表示されません。

この画面のメッセージはカスタマイズできません。これは、すべての VPN インストールに使用される標準の iOS ダイアログボックスです。

VPN の構成の追加に関する許可を求める画面で ［許可しない］ を選択すると、Secure Hub にアクセスするには VPN をインストールする必要があると通知する別のメッセージが表示されます。

クライアントデバイス上での **Secure Hub VPN** の実行

Secure Hub VPN が仕様どおり実行されている場合は、iOS 設定アプリの ［一般］**>**［**VPN**］ 画面にテキスト 「接続中」 が表示されます。

これは想定どおりの動作であり、MDX の共有と通信メカニズムが機能していないことを意味するものではありません。このメッセージが表示されていれば、ユーザーが操作する必要はありません。

派生資格情報を使用したデバイスの登録

January 25, 2019

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ーに保管します。

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 コードのスキャ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。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States