CITRIX

XenMobile Server：最新リリース

Contents

XenMobile Server 10.11 の新機能

January 10, 2020

Apple Volume Purchase Program から Apple Business Manager（ABM）および Apple School Manager（ASM）への移行

Apple Volume Purchase Program（VPP）を使用している組織および教育機関は、2019 年 12 月 1 日より前に Apple Business Manager または Apple School Manager のアプリとブックに移行する必要があります。

XenMobile で VPP アカウントを移行する前に、「Apple サポートの記事」を参照してください。

所属する組織または教育機関が Volume Purchase Program（VPP）のみを使用している場合、ABM/ASM に登録してから既存の VPP 購入者を新しい ABM/ASM アカウントに招待することができます。ASM の場合は、https://school.apple.comにアクセスします。ABM の場合は、https://business.apple.comにアクセスします。

XenMobile で一括購入（以前の VPP）アカウントを更新するには：

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［一括購入］ をクリックします。［一括購入］ 構成ページが開きます。
3. ABM アカウントまたは ASM アカウントのアプリ構成が、以前の VPP アカウントと同じであることを確認します。
4. ABM ポータルまたは ASM ポータルで、更新されたトークンをダウンロードします。
5. XenMobile コンソールで、以下を実行します：
    a) その場所の更新されたトークン情報を使用して、既存の一括購入アカウントを編集します。
    b) ABM 資格情報または ASM 資格情報を編集します。サフィックスを変更しないでください。
    c) ［保存］ を 2 回クリックします。

iOS 13 のサポート

> 重要：
>
> iOS 12 以上へのデバイスアップグレードの準備：iOS 用の VPN デバイスポリシーの Citrix VPN 接続タイプは、iOS 12 以降をサポートしていません。VPN デバイスポリシーを削除し、Citrix SSO 接続タイプで新しい VPN デバイスポリシーを作成します。
>
> VPN デバイスポリシーを削除すると、以前に展開されたデバイスで Citrix VPN 接続が引き続き動作します。新しい VPN デバイスポリシーの設定は、XenMobile Server 10.11 ではユーザー登録時に有効になります。

XenMobile Server は、iOS 13 にアップグレードされたデバイスをサポートしています。アップグレードは、ユーザーに以下のように影響します：

- 登録時に、新しい iOS セットアップアシスタントのオプション画面がいくつか表示されます。Apple は、iOS 13 に新しい iOS セットアップアシスタントのオプション画面を追加しました。新しいオプションは、このリリースの［設定］**>** ［**Apple** デバイス登録プログラム（**DEP**）］ページには含まれていません。そのため、これらの画面をスキップするように XenMobile Server を構成することはできません。これらのページは、iOS 13 デバイスでユーザーに表示されます。
- 旧バージョンの iOS では監視対象デバイスと監視対象外デバイスで使用できた制限デバイスポリシー設定の一部が、iOS 13 以上では監視対象デバイスでのみ使用できます。現在の XenMobile Server コンソールのツールチップでは、これらの設定が iOS 13 以上では監視対象デバイス専用であることが通知されません。
  - ハードウェアの制御を許可:
    * FaceTime
    * アプリのインストール
  - アプリを許可:
    * iTunes ストア
    * Safari
    * Safari> 自動入力
  - ネットワーク - 実行できる iCloud の操作:
    * iCloud ドキュメントおよびデータ
  - 監視対象のみの設定 - 許可:
    * Game Center> 友達を追加
    * Game Center> マルチプレイゲーム
  - メディアコンテンツ - 許可:
    * 不適切な音楽、Podcast、iTunes U コンテンツ

これらの制限は、次のように適用されます:

- iOS 12（以前）のデバイスが既に XenMobile Server に登録されていて、iOS 13 にアップグレードする場合、上記の制限は監視対象外のデバイスおよび監視対象デバイスに適用されます。
- iOS 13 以降の監視対象外のデバイスを XenMobile Server に登録する場合、上記の制限は監視対象デバイスにのみ適用されます。
- iOS 13 以降の監視対象デバイスを XenMobile Server に登録する場合、上記の制限は監視対象デバイスにのみ適用されます。

iOS 13 および **macOS 15** での信頼された証明書の要件

Apple では、TLS サーバー証明書の新しい要件を設定しています。すべての証明書が新しい Apple の要件に準拠していることを確認します。詳しくは、Apple のドキュメントhttps://support.apple.com/en-us/HT210176を参照してください。証明書の管理については、「XenMobile での証明書のアップロード」を参照してください。

GCM から FCM へのアップグレード

2018 年 4 月 10 日、Google は Google Cloud Messaging（GCM）の廃止を発表しました。2019 年 5 月 29 日をもって、GCM サーバーとクライアント API は削除されました。

> 重要な要件：
>
> - XenMobile Server の最新バージョンにアップグレードします。
> - Secure Hub の最新バージョンにアップグレードします。

Google は、Firebase Cloud Messaging（FCM）にアップグレードして新機能を活用することを推奨しています。Google が提供する情報については、https://developers.google.com/cloud-messaging/faqおよびhttps://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.htmlを参照してください。

Android デバイスへのプッシュ通知の利用を継続するには：XenMobile Server で GCM を使用している場合は、FCM に移行してください。次に、Firebase Cloud Messaging コンソールで入手した新しい FCM キーを使用して、XenMobile Server を更新します。

次の手順は、信頼された機関からの証明書を使用する場合の登録ワークフローを反映しています。

アップグレード手順：

1. Google から提供された情報に従って、GCM から FCM にアップグレードしてください。
2. Firebase Cloud Messaging コンソールで、新しい FCM キーをコピーします。このキーは、次の手順で必要です。
3. XenMobile Server コンソールの ［設定］ > ［**Firebase Cloud Messaging**］ で設定を構成します。

次回 XenMobile Server にチェックインしてポリシーを更新したときに、デバイスは FCM に切り替わります。Secure Hub にポリシーの更新を適用するには：Secure Hub で、［設定］ > ［デバイス情報］ に移動して、［ポリシーの更新］ をタップします。
FCM の構成について詳しくは、「Firebase Cloud Messaging」を参照してください。

XenMobile Migration Service

XenMobile Server をオンプレミスで使用している場合、XenMobile Migration Service によって Endpoint Management の使用を開始することができます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。

詳しくは、地域のシトリックス営業担当者、システムエンジニア、またはシトリックスパートナーにお問い合わせください。以下のブログで、XenMobile Migration Service について解説しています：

New XenMobile Migration Service（英語）

Making the Case for XenMobile in the Cloud（英語）

XenMobile 10.11（オンプレミス）にアップグレードする前に

システム要件がいくつか変更されました。詳しくは、「システム要件と互換性」および「XenMobile の互換性」を参照してください。

1. XenMobile Server 10.11 の最新バージョンにアップデートする前に、Citrix ライセンスサーバーを 11.15 以降にアップデートしてください。

   最新バージョンの XenMobile では、Citrix ライセンスサーバー 11.15 以降が必要です。

   > 注:
   >
   > プレビュー用に独自のライセンスを使用する場合は、XenMobile 10.11 のカスタマーサクセスサービスの日付（以前の Subscription Advantage の日付）は 2019 年 4 月 9 日であることをご確認ください。Citrix ライセンスのカスタマーサクセスサービスの日付は、この日付より後である必要があります。
   >
   > 日付は、ライセンスサーバーのライセンスの隣に表示されています。XenMobile の最新バージョンを古いライセンスサーバー環境に接続すると、接続チェックが失敗し、ライセンスサーバーを構成できません。

   ライセンスの日付を更新するには、Citrix ポータルから最新のライセンスファイルをダウンロードし、ライセンスサーバーにファイルをアップロードします。詳しくは、「カスタマーサクセスサービス」を参照してください。

2. クラスタ化された環境の場合: iOS 11 以降を実行するデバイスへの iOS ポリシーおよびアプリの展開には、次の要件があります。NetScaler Gateway が SSL 永続性に設定されている場合、すべての XenMobile Server ノードでポート 80 を開く必要があります。

3. アップグレードする XenMobile Server を実行する仮想マシンの RAM が 4GB 未満の場合、最低 4GB に RAM を増設してください。実稼働環境では、推奨される最小 RAM 容量は 8GB であることに留意願います。

4. 推奨事項: XenMobile の更新をインストールする前に、仮想マシンの機能を使用して、システムのスナップショットを取得してください。また、システム構成データベースもバックアップしてください。アップグレードで問題が発生した場合でも、完全なバックアップがあれば復元を行うことができます。

アップグレードするには

XenMobile 10.10.x または 10.9.x からは XenMobile 10.11 に直接アップグレードできます。アップグレードを実行するには、Citrix のダウンロードページで取得できる最新の 10.11 バイナリを使用します。アップグレードをアップロードするには、XenMobile コンソールで ［リリース管理］ ページを使用します。詳しくは、「リリース管理ページを使用してアップグレードする」を参照してください。

アップグレードした後

XenMobile 10.11（オンプレミス）にアップグレードした後に:

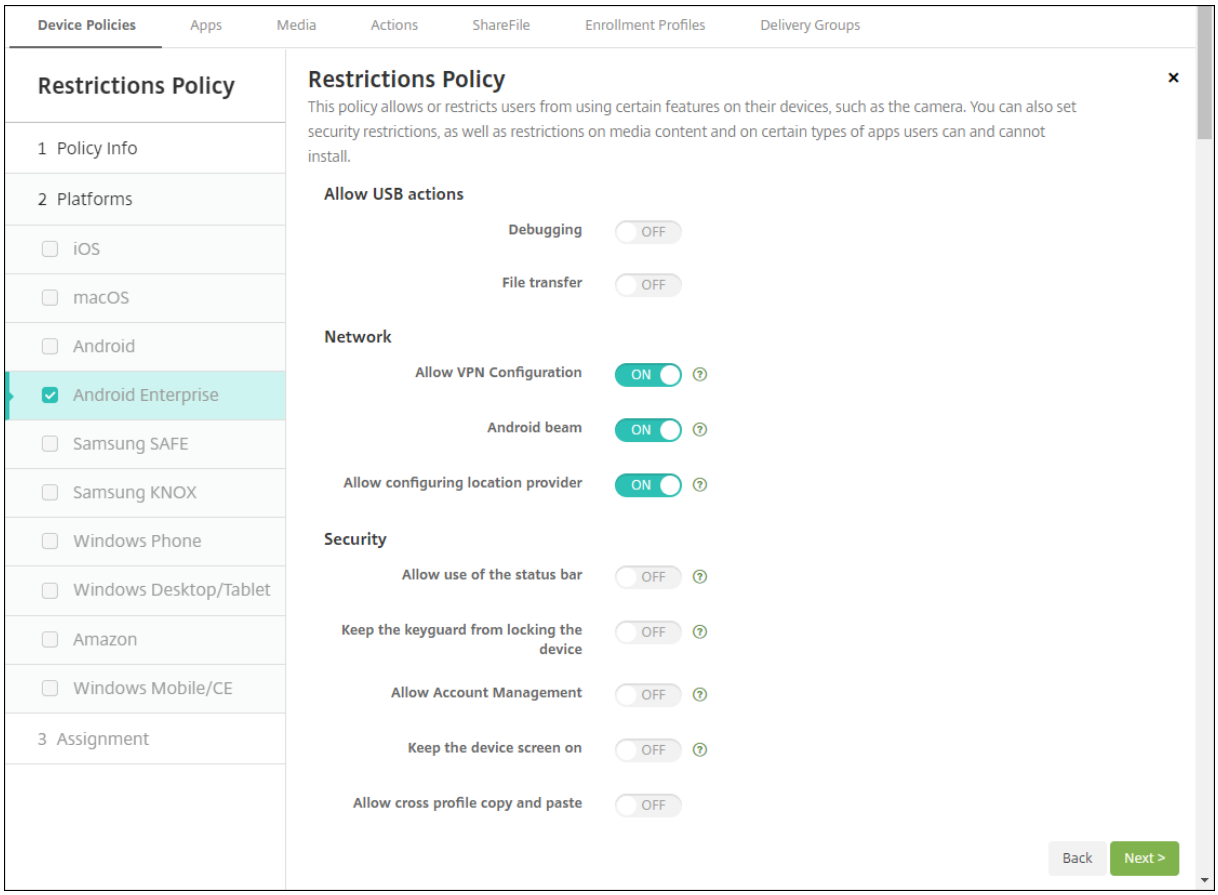
接続の構成を変更していないのに送信接続に関連した機能が動作しなくなった場合は、XenMobile Server のログを調べて、「VPP サーバーに接続できません: ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」のような内容のエラーが含まれていないかを確認します。

証明書の検証エラーは、XenMobile Server でホスト名の認証を無効にする必要があることを示しています。デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証によって展開が損なわれる場合は、サーバープロパティ`disable.hostname.verification`を**`true`**に変更します。このプロパティのデフォルト値は**`false`**です。

Android Enterprise デバイスの新規および更新されたデバイスポリシー設定

Samsung Knox と **Android Enterprise** のポリシー統一。Samsung Knox 3.0 以降および Android 8.0 以降を実行している Android Enterprise デバイスの場合: Knox と Android Enterprise は、デバイスおよびプロファイルの一元的な管理ソリューションに統合されます。
[Android Enterprise] ページで Knox の設定に関する以下のデバイスポリシーを設定します:

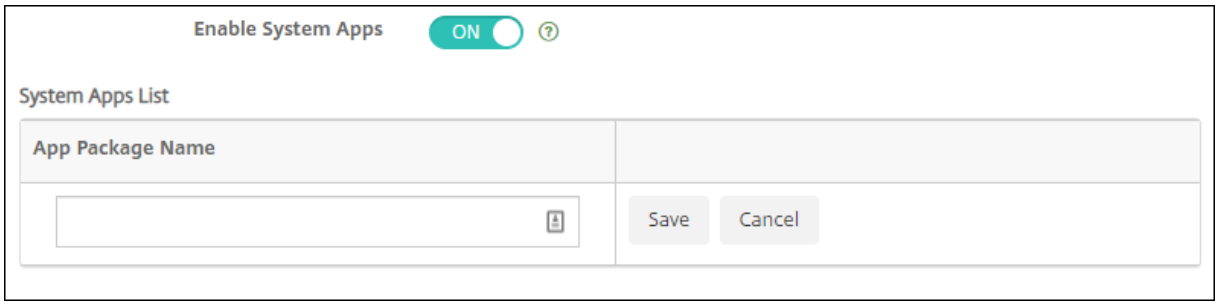
- **OS** 更新デバイスポリシー。Samsung Enterprise FOTA の更新のための設定が含まれています。
- パスコードデバイスポリシー。
- **Samsung MDM** ライセンスキーデバイスポリシー。Knox ライセンスキーを設定します。
- 制限デバイスポリシー設定。



Android Enterprise 向けアプリインベントリデバイスポリシー。管理対象デバイスで Android Enterprise アプリのインベントリを収集できるようになりました。アプリインベントリデバイスポリシーを参照してください。

管理対象 **Google Play** ストアにあるすべての **Google Play** アプリにアクセスします。**Access all apps in the managed Google** サーバープロパティによって、パブリック Google Play ストアのすべてのアプリに管理対象 Google Play ストアからアクセスできるようになります。このプロパティを **true** に設定すると、すべての Android Enterprise ユーザー向けのパブリック Google Play ストアアプリがホワイトリストに登録されます。管理者は、制限デバイスポリシーを使用してこれらのアプリへのアクセスを制御できます。

Android Enterprise デバイスでシステムアプリを有効にします。Android Enterprise 仕事用プロファイルモードまたは完全管理モードで、事前インストールされたシステムアプリを実行できるようにするには、制限デバイスポリシーを構成します。この構成により、ユーザーはカメラ、ギャラリーなどのデフォルトのデバイスアプリにアクセスできます。特定のアプリへのアクセスを制限するには、Android Enterprise の権限デバイスポリシーを使用してアプリの権限を設定します。



Android Enterprise 専用デバイスのサポート。XenMobile は、以前は特定業務専用コーポレート所有（COSU）デバイスと呼ばれていた専用デバイスの管理をサポートするようになりました。

Android Enterprise 専用デバイスは、単一のユースケース専用の完全に管理されたデバイスです。これらのデバイスは、このユースケースに必要なタスクを実行する 1 つのアプリまたはアプリの小セットのみに制限されます。また、ユーザーがこれらのデバイスで他のアプリを有効にしたり、他の操作を実行したりすることを禁止することもできます。

Android Enterprise デバイスのプロビジョニングについて詳しくは、「Android Enterprise 専用デバイスのプロビジョニング」を参照してください。

名前が変更されたポリシー。Google の用語に合わせて、Android Enterprise アプリ制限デバイスポリシーを Android Enterprise 管理対象構成と呼ぶようになりました。Android Enterprise 管理対象の構成デバイスポリシーを参照してください。

Android Enterprise のパスワードのロックおよびリセット

XenMobile では、Android Enterprise デバイスのパスワードのロックとリセットのセキュリティ操作がサポートされるようになりました。これらのデバイスは、Android 8.0 以上を実行している仕事用プロファイルモードで登録する必要があります。

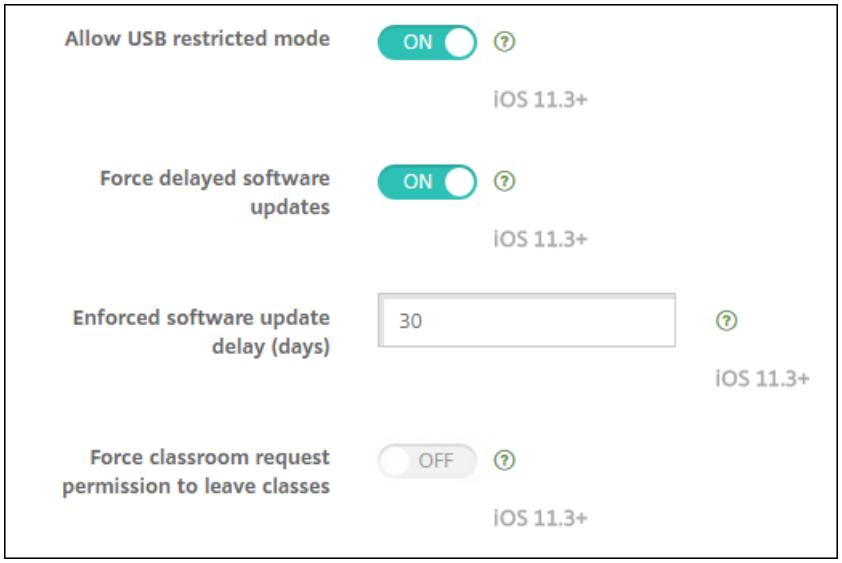
- 送信されたパスコードによって仕事用プロファイルはロックされます。デバイスはロックされません。

- パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていない場合:
  - 仕事用プロファイルにパスコードが設定されていないため、デバイスはロックされています。
  - 仕事用プロファイルにパスコードが既に設定されている場合、仕事用プロファイルはロックされますが、デバイスはロックされません。

パスワードのロックとリセットのセキュリティ操作について詳しくは、「セキュリティ操作」を参照してください。

iOS または **macOS** 向けの新しい［制限］デバイスポリシー設定

- 非管理対象アプリによる管理対象アカウント連絡先の読み取り: オプション。［管理対象アプリから非管理対象アプリへのドキュメントの移動］ が無効になっている場合にのみ利用できます。このポリシーを有効にすると、非管理対象アプリが管理対象アカウントの連絡先からデータを読み取ることができるようになります。デフォルトは ［オフ］ です。iOS 12 以降で利用できます。
- 管理対象アプリによる非管理対象アカウント連絡先への書き込み: オプション。有効にすると、管理対象アプリによる非管理対象アカウントの連絡先への書き込みを許可します。［管理対象アプリから非管理対象アプリへのドキュメントの移動］ を有効にすると、この制限は有効になりません。デフォルトは ［オフ］ です。iOS 12 以降で利用できます。
- パスワードの自動入力: オプション。無効にすると、ユーザーはパスワードの自動入力または自動強力パスワード機能を使用できません。デフォルトは ［オン］ です。iOS 12 および macOS 10.14 以降で利用できます。
- パスワード近接要求: オプション。無効にすると、ユーザーのデバイスは近くのデバイスにパスワードを要求しません。デフォルトは ［オン］ です。iOS 12 および macOS 10.14 以降で利用できます。
- パスワード共有: オプション。無効にすると、ユーザーは AirDrop パスワード機能を使用してパスワードを共有できません。デフォルトは ［オン］ です。iOS 12 および macOS 10.14 以降で利用できます。
- 自動的な日付と時刻を強制: 監視対象。有効にすると、ユーザーは ［全般］ **>** ［日付と時刻］ **>** ［自動的に設定］ オプションを無効にできません。デフォルトは ［オフ］ です。iOS 12 以降で利用できます。
- **USB** 制限モードを許可: 監視対象デバイスでのみ使用できます。［オフ］ に設定すると、デバイスはロックされた状態でも常に USB アクセサリーに接続できます。デフォルトは ［オン］ です。iOS 11.3 以降で利用できます。
- ソフトウェア更新の延期を強制する: 監視対象デバイスでのみ使用できます。［オン］ に設定すると、ソフトウェア更新のユーザー表示が延期されます。この制限が設定されている場合、ソフトウェアの更新がリリースされてから指定された日数が経過するまで、ソフトウェアの更新は表示されません。デフォルトは ［オフ］ です。iOS 11.3 および macOS 10.13.4 以降で利用できます。
- ソフトウェア更新の強制延期（日） 監視対象デバイスでのみ使用できます。この制限により、管理者は、デバイスのソフトウェア更新の延期期間を設定できます。最大値は 90 日で、デフォルト値は **30** です。iOS 11.3 および macOS 10.13.4 以降で利用できます。
- クラスを離れるときの許可の要求を強制する: 監視対象デバイスでのみ使用できます。［オン］ に設定すると、クラスルームの管理対象外コースに登録した生徒は、コースを離れるときに教師の許可を求める必要があります。デフォルトは ［オフ］ です。iOS 11.3 以降で利用できます。



制限デバイスポリシーを参照してください。

iOS または macOS 用の Exchange デバイスポリシーの更新

iOS 12 以降、**S/MIME Exchange** の署名と暗号化の設定が増えています。Exchange デバイスポリシーに、S/MIME 署名と暗号化を構成するための設定が含まれるようになりました。

S/MIME 署名の場合:

- 署名 **ID** 資格情報: 使用する署名資格情報を選択します。
- **S/MIME** 署名（ユーザー上書き可能）: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。
- **S/MIME** 署名証明書 **UUID**（ユーザー上書き可能）: ［オン］ に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］ です。

S/MIME 暗号化の場合:

- 暗号化 **ID** 資格情報: 使用する暗号化資格情報を選択します。
- メッセージごとの **S/MIME** 切り替えの有効化: ［オン］ に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］ です。
- デフォルトの **S/MIME** 暗号化（ユーザー上書き可能）: ［オン］ に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］ です。
- **S/MIME** 暗号化証明書 **UUID**（ユーザー上書き可能）: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。

iOS 12 以降の **Exchange OAuth** の設定。Exchange との接続の認証に OAuth を使用するように設定できるようになりました。

mac OS 10.14 以降の **Exchange OAuth** の設定。Exchange との接続の認証に OAuth を使用するように設定できるようになりました。OAuth を使用した認証では、自動検出を使用しないセットアップのサインイン URL を指定

できます。

Exchange デバイスポリシーを参照してください。

iOS 用のメールデバイスポリシーの更新

iOS 12 以降、**S/MIME Exchange** の署名と暗号化の設定が増えています。メールデバイスポリシーには、S/MIME 署名と暗号化を構成するためのその他の設定が含まれています。

S/MIME 署名の場合:

- **S/MIME** 署名の有効化: アカウントで S/MIME 署名をサポートするかどうかを指定します。デフォルトは［オン］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - **S/MIME** 署名（ユーザー上書き可能）: ［オン］に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - **S/MIME** 署名証明書 **UUID**（ユーザー上書き可能）: ［オン］ に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。

S/MIME 暗号化の場合:

- **S/MIME** 暗号化の有効化: このアカウントで S/MIME 暗号化をサポートするかどうかを選択します。デフォルトは ［オフ］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - メッセージごとの **S/MIME** 切り替えの有効化: ［オン］ に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］ です。
  - デフォルトの **S/MIME** 暗号化（ユーザー上書き可能）: ［オン］ に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - **S/MIME** 暗号化証明書 **UUID**（ユーザー上書き可能）: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。

メールデバイスポリシーを参照してください。

iOS 向けのアプリ通知デバイスポリシーの更新

iOS12 以降では、以下のアプリ通知設定を利用できます。

- **CarPlay** で表示: ［オン］ にすると、Apple CarPlay に通知が表示されます。デフォルトは ［オン］ です。
- 重大アラートを有効にする: ［オン］ にすると、アプリは通知を重大な通知としてマークできます。これによって［応答不可］および警告設定を無視します。デフォルトは ［オフ］ です。

詳細については、「アプリ通知デバイスポリシー」を参照してください。

Apple Education で使用される共有 iPad のサポート

Apple の教育向け機能との XenMobile の統合により、共有 iPad がサポートされるようになりました。クラスルーム内の複数の生徒は、1 人または複数の講師が教えているさまざまな科目について、iPad を共有できます。

管理者か講師が共有 iPad を登録し、デバイスポリシー、アプリ、メディアをデバイスに展開します。その後、生徒が管理対象 Apple ID の資格情報を入力して共有 iPad にサインインします。以前生徒に［教育の構成］ポリシーを展開したことがある場合、生徒はデバイスを共有するために「その他のユーザー」としてサインインする必要はありません。

共有 iPad の前提条件:

- iPad Pro、iPad 第 5 世代、iPad Air 2 以降、iPad mini 4 以降
- 32GB 以上のストレージ容量
- 監視

詳しくは、「共有 iPad の構成」を参照してください。

役割ベースのアクセス制御（RBAC）権限の変更

RBAC 権限［ローカルユーザーの追加/削除］が、［ローカルユーザーの追加］と［ローカルユーザーの削除］の 2 つの権限に分割されました。

詳しくは、「RBAC を使用した役割の構成」を参照してください。

XenMobile Server 10.10 の新機能

October 25, 2019

XenMobile Server 10.10（PDF のダウンロード）

> 重要:
>
> iOS 12 へのデバイスアップグレードの準備: iOS 用の VPN デバイスポリシーの Citrix VPN 接続タイプは、iOS 12 をサポートしていません。VPN デバイスポリシーを削除し、Citrix SSO 接続タイプで新しい VPN デバイスポリシーを作成します。
>
> VPN デバイスポリシーを削除すると、以前に展開されたデバイスで Citrix VPN 接続が引き続き動作します。新しい VPN デバイスポリシーの設定は、XenMobile Server 10.10 ではユーザー登録時に有効になります。

GCM から FCM へのアップグレード

2018 年 4 月 10 日、Google は Google Cloud Messaging（GCM）の廃止を発表しました。2019 年 5 月 29 日をもって、GCM サーバーとクライアント API は削除されます。

> 重要な要件：
>
> - 中断を避けるため、5 月 29 日までに XenMobile Server 10.10 にアップグレードしてください。
> - Secure Hub 19.3.5 以降にアップグレードします。

Google は、Firebase Cloud Messaging（FCM）にアップグレードして新機能を活用することを推奨しています。Google が提供する情報については、https://developers.google.com/cloud-messaging/faqおよびhttps://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.htmlを参照してください。

Android デバイスへのプッシュ通知の利用を継続するには：XenMobile Server で GCM を使用している場合は、FCM に移行してください。次に、Firebase Cloud Messaging コンソールで入手した新しい FCM キーを使用して、XenMobile Server を更新します。

次の手順は、信頼された機関からの証明書を使用する場合の登録ワークフローを反映しています。

アップグレード手順：

1. Google から提供された情報に従って、GCM から FCM にアップグレードしてください。
2. Firebase Cloud Messaging コンソールで、新しい FCM キーをコピーします。このキーは、次の手順で必要です。
3. XenMobile Server コンソールの ［設定］ > ［**Firebase Cloud Messaging**］ で設定を構成します。

次回 XenMobile Server にチェックインしてポリシーを更新したときに、デバイスは FCM に切り替わります。Secure Hub にポリシーの更新を適用するには：Secure Hub で、［設定］ > ［デバイス情報］ に移動して、［ポリシーの更新］ をタップします。
FCM の構成について詳しくは、「Firebase Cloud Messaging」を参照してください。

XenMobile Migration Service

XenMobile Server をオンプレミスで使用している場合、XenMobile Migration Service によって Endpoint Management の使用を開始することができます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。

詳しくは、地域のシトリックス営業担当者、システムエンジニア、またはシトリックスパートナーにお問い合わせください。以下のブログで、XenMobile Migration Service について解説しています：

New XenMobile Migration Service（英語）

Making the Case for XenMobile in the Cloud（英語）

iOS MDM 登録ワークフローの変更

不備のあるプロファイルをインストールしないようにしてプラットフォームのセキュリティを向上させるため、Apple は MDM にデバイスを手動で登録するための新しいワークフローをリリースしました。この新しいワークフローは、XenMobile Server を含むすべての MDM ソリューションに影響を与えます。

Apple Business Manager または Apple School Manager で割り当てられたサーバーへの MDM 登録に変更はありません。ワークフローの変更は、MDM での手動登録のみが対象です。

信頼された機関からの証明書を使用している場合は、さらに登録が簡単です。これまで、iOS デバイスユーザーには、登録時にルート CA と MDM デバイス証明書の 2 つのプロンプトが表示されていましたが、iOS デバイスユーザーには、MDM デバイス証明書のプロンプトのみが表示されるようになりました。この変更を利用するには、以下の設定が必要です:

- 信頼された機関からの証明書を使用する場合、［設定］**>**［サーバープロパティ］でプロパティの値を`ios.mdm.enrollment.installRootCaIfRequired`から**`false`**に変更します。その結果、MDM 登録中に Safari ウィンドウが開き、ユーザーのプロファイルのインストールが簡素化されます。iOS デバイスユーザーには、MDM デバイス証明書のプロンプトのみが表示されます。そのプロンプトには「XenMobile Profile Service」というラベルが付いています。

Display name	Key	Value	Default value	Description
iOS Device Management Enrollment Install Root CA if Required	ios.mdm.enrollment.installRootCaIfRequired	true	true	Bypass installation of the root CA. Third-party public certificate required trusted by iOS.

詳しくは、「iOS デバイスの登録」および次の YouTube ビデオを参照してください:

XenMobile 10.10（オンプレミス）にアップグレードする前に

システム要件がいくつか変更されました。詳しくは、「システム要件と互換性」および「XenMobile の互換性」を参照してください。

1. XenMobile Server 10.10 の最新バージョンにアップデートする前に、Citrix ライセンスサーバーを 11.15 以降にアップデートしてください。

   最新バージョンの XenMobile では、Citrix ライセンスサーバー 11.15 以降が必要です。

   > 注
   >
   > XenMobile 10.10 の Subscription Advantage（SA）の日付は 2019 年 4 月 9 日です。Citrix ライセンスの Subscription Advantage（SA）日付がこの日以降である必要があります。SA 日付は、ライセンスサーバーのライセンスの隣に表示されています。XenMobile の最新バージョンを古いライセンスサーバー環境に接続すると、接続チェックが失敗し、ライセンスサーバーを構成できません。

   ライセンスの SA 日付を更新するには、Citrix ポータルから最新のライセンスファイルをダウンロードし、ライセンスサーバーにファイルをアップロードします。詳しくは、「https://support.citrix.com/article/CTX134629」を参照してください。

2. クラスタ化された環境の場合：iOS 11 以降を実行するデバイスへの iOS ポリシーおよびアプリの展開には、次の要件があります。NetScaler Gateway が SSL 永続性に設定されている場合、すべての XenMobile Server ノードでポート 80 を開く必要があります。

3. アップグレードする XenMobile Server を実行する仮想マシンの RAM が 4GB 未満の場合、最低 4GB に RAM を増設してください。実稼働環境では、推奨される最小 RAM 容量は 8GB であることに留意願います。

4. 推奨事項：XenMobile の更新をインストールする前に、仮想マシンの機能を使用して、システムのスナップショットを取得してください。また、システム構成データベースもバックアップしてください。アップグレードで問題が発生した場合でも、完全なバックアップがあれば復元を行うことができます。

アップグレードするには

Citrix が、アップグレードファイルへの ShareFile リンクを提供します。

XenMobile 10.9 または 10.8 からは XenMobile Server 10.10 に直接アップグレードできます。XenMobile コンソールで ［リリース管理］ ページを使用します。詳しくは、「リリース管理ページを使用してアップグレードする」を参照してください。

アップグレードした後

XenMobile 10.10（オンプレミス）にアップグレードした後に：

接続の構成を変更していないのに送信接続に関連した機能が動作しなくなった場合は、XenMobile Server のログを調べて、「VPP サーバーに接続できません: ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」のような内容のエラーが含まれていないかを確認します。

証明書の検証エラーは、XenMobile Server でホスト名の認証を無効にする必要があることを示しています。デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証によって展開が損なわれる場合は、サーバープロパティ`disable.hostname.verification`を**`true`**に変更します。このプロパティのデフォルト値は**`false`**です。

管理者のグループ許可を制限するための **RBAC** の機能強化

［管理］**>**［ユーザー］ および ［管理］**>**［登録招待］ ページ: 表示されるユーザー情報は、RBAC 管理者のグループアクセス許可によって制限されるようになりました。これまで、XenMobile Server コンソールでは、これらのページにすべてのローカルユーザーとドメインユーザーの情報が含まれていました。

RBAC 管理者が表示および管理する権限を持つユーザーグループを指定するには、管理者ロールを編集し、ユーザーグループを指定します。詳しくは、「RBAC を使用した役割の構成」を参照してください。

Android Enterprise デバイスの新しいポリシー

XenMobile Server の最新バージョンには、Android Enterprise デバイス用に次のような新しいポリシーがあります。

- **WiFi** デバイスポリシー。Android Enterprise デバイス用の WiFi デバイスポリシーを作成できます。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。Android Enterprise デバイス用のカスタム XML デバイスポリシーを作成できます。カスタム XML デバイスポリシーを参照してください。
- 位置情報デバイスポリシー。Android Enterprise デバイス所有者モードまたはプロファイル所有者モードで登録するデバイスの位置情報設定を定義できます。位置情報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。XenMobile Server に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。ファイルデバイスポリシーを参照してください。
- 新しい［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 デバイスで次の機能にアクセスできます。制限デバイスポリシーを参照してください。
  - ファイル転送
  - テザリング
  - Android ビーム
  - コピーと貼り付けを許可
  - アプリの検証を有効化
  - ユーザーにアプリケーション設定の制御を許可
  - デバイスの連絡先で仕事用プロファイルの連絡先を許可
  - スクリーンキャプチャを許可

- カメラの使用を許可
- ホーム画面で仕事用プロファイルアプリのウィジェットを許可
- アカウント管理を許可
- 位置情報サービスを許可
- アプリケーションを無効化

> 注：
>
> 最新の Android Enterprise ポリシーにアクセスするため、Secure Hub の最新 Google Play バージョンを使用していることを確認してください。

XenMobile Server 10.9 の新機能

May 21, 2019

XenMobile Server 10.9（PDF のダウンロード）

> 重要：
>
> iOS 12 へのデバイスアップグレードの準備：iOS 用の VPN デバイスポリシーの Citrix VPN 接続タイプは、iOS 12 をサポートしていません。VPN デバイスポリシーを削除し、Citrix SSO 接続タイプで新しい VPN デバイスポリシーを作成します。
>
> VPN デバイスポリシーを削除すると、以前に展開されたデバイスで Citrix VPN 接続が引き続き動作します。新しい VPN デバイスポリシーの設定は、XenMobile Server 10.9 ではユーザー登録時に有効になります。

XenMobile Migration Service

XenMobile Server をオンプレミスで使用している場合、XenMobile Migration Service によって Endpoint Management の使用を開始することができます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。

詳しくは、地域のシトリックス営業担当者、システムエンジニア、またはシトリックスパートナーにお問い合わせください。以下のブログで、XenMobile Migration Service について解説しています：

New XenMobile Migration Service（英語）

Making the Case for XenMobile in the Cloud（英語）

コンソールから **XenMobile** ツールへのアクセス

XenMobile コンソールから XenMobile ツールにアクセスできます。

- **XenMobile Analyzer**： 展開に関する潜在的な問題を特定し、トリアージします。

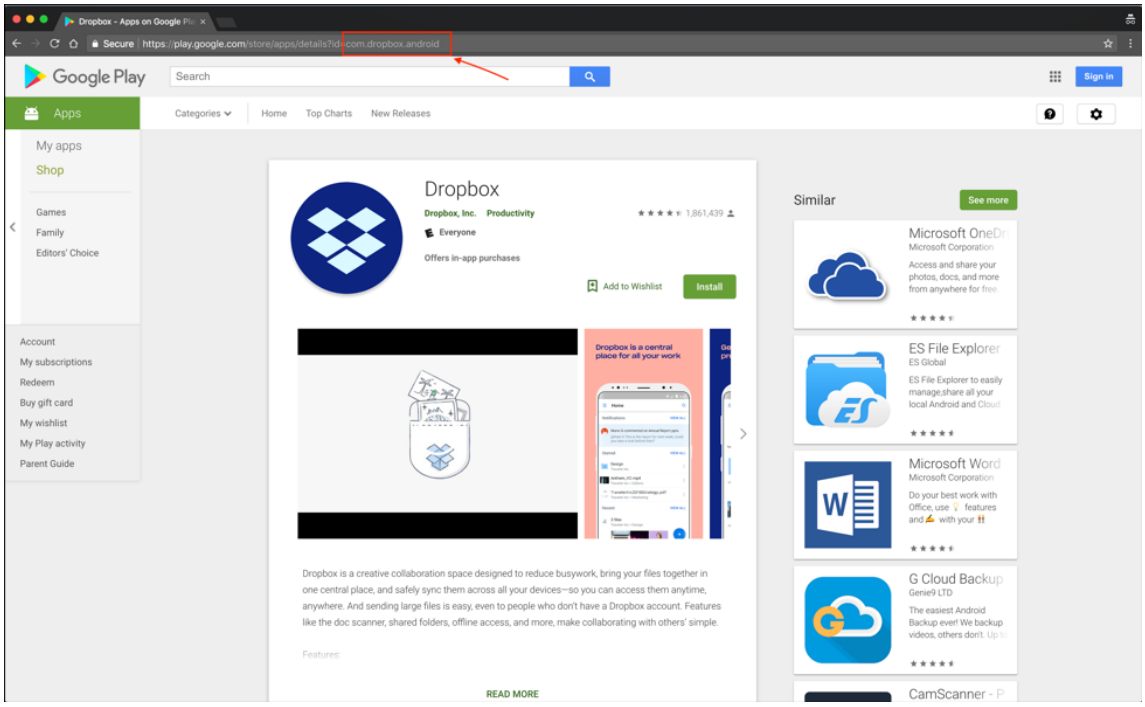
- **APNs** ポータル: シトリックスに APNs 証明書への署名を求める要求を送信します。署名された証明書は、Apple に提出します。
- 自動検出サービス: ドメインの XenMobile の自動検出を要求および構成します。
- プッシュ通知の管理: iOS および Windows の業務用モバイルアプリのプッシュ通知を管理します。
- **MDX** サービス: アプリをラップします。ラップしたアプリは、XenMobile で管理できるようになります。

これらのツールにアクセスするには、［設定］**>**［**XenMobile Tools**］に移動します。

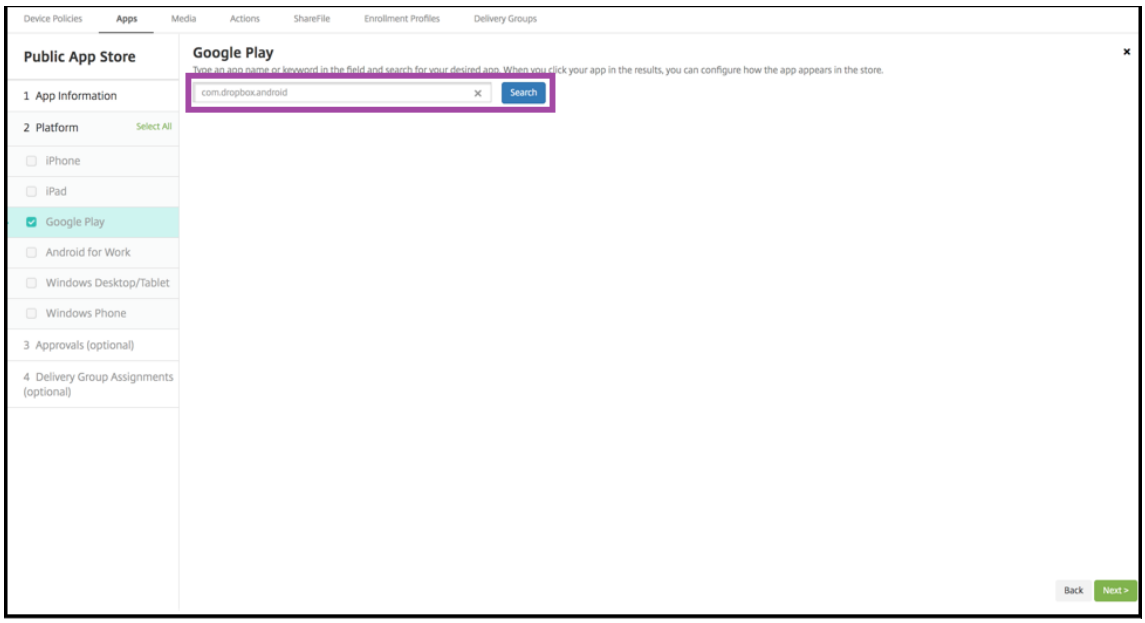
Google Play ストアからアプリを追加するための新しいワークフロー

アプリを追加する際に、Google Play の資格情報を指定する代わりに、パブリックストアの Android アプリのパッケージ ID を追加するようになりました。

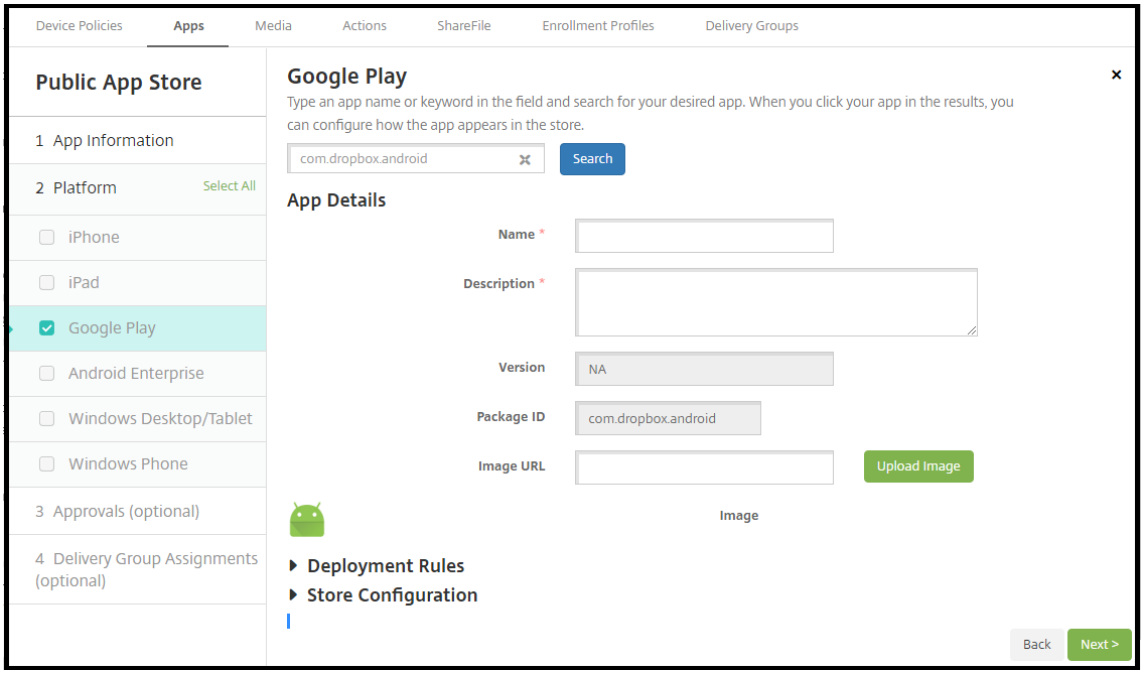
1. Google Play ストアでパッケージ ID をコピーします。ID はアプリの URL に含まれています。



2. パブリックストアのアプリを XenMobile Server コンソールに追加する際に、検索バーに含まれるパッケージ ID を貼り付けます。



3. パッケージ ID が有効な場合は、アプリの詳細を入力できる UI が表示されます。



詳しくは、「パブリックアプリストアのアプリの追加」を参照してください。

新しいパブリック **REST API**

- Get Devices by Filters API の新しいバージョンでは、デバイスに関する追加の詳細情報が提供されています。詳細は、REST サービスのための XenMobile Public API PDF の「3.16.2 フィルタでデバイスを取得する（バージョン 2）」のセクションを参照してください。

- ルート CA、デバイス CA、サーバー CA を再生成し、デバイス証明書を更新する機能

  XenMobile Server は、内部的に PKI のために次の認証機関を使用します：ルート CA、デバイス CA、およびサーバー CA。それらの CA は論理グループとして分類され、グループ名が与えられます。新しい XenMobile Server インスタンスがプロビジョニングされると、3 つの CA が生成され、グループ名が「default」になります。

  サポートされている iOS、macOS、および Android デバイスの CA を更新するには、XenMobile サーバーコンソールまたは公開 REST API を使用します。登録済み Windows デバイスの場合、ユーザーは新しいデバイス CA を受信するためにデバイスを再登録する必要があります。

  XenMobile サーバーで内部 PKI CA を更新または再生成し、これらの証明機関によって発行されたデバイス証明書を更新するには、次の API を使用します。

  - 新しいグループ証明機関（CA）を作成します。
  - 新しい CA をアクティブにし、古い CA を無効にします。
  - 設定済みのデバイスリストでデバイス証明書を更新します。既に登録済みのデバイスは、中断することなく動作し続けます。デバイスがサーバーに接続すると、デバイス証明書が発行されます。
  - 古い CA を使用しているデバイスのリストを返します。
  - すべてのデバイスに新しい CA が割り当てられたら、古い CA を削除します。

  詳しくは、「REST サービスのための XenMobile Public API」の PDF の次のセクションを参照してください：

  - 第 3.16.58 項「デバイス証明書の更新」
  - 第 3.23 項「XenMobile CA グループのリフレッシュ」

  この機能の一部として、新しいセキュリティ操作である証明書の書き換えを ［デバイスの管理］ コンソールから実行できます。この操作は、そのデバイス上の登録証明書を更新します。

  前提条件：

  - デフォルトでは、この証明書の書き換え機能は無効になっています。証明書の書き換え機能を有効にするには、サーバープロパティ **refresh.internal.ca** の値を **True** に設定します。

  > 重要：
  >
  > NetScaler で SSL オフロードが設定されている場合は、新しい証明書を生成するときに、必ず新しい cacert.perm を使ってロードバランサーを更新してください。NetScaler Gateway の設定について詳しくは、「To use SSL Offload mode for NetScaler VIPs」を参照してください。

サードパーティ製品についての通知

March 11, 2019

XenMobile のこのリリースには、次のドキュメントで定義された条件の元でライセンスが有効になったサードパーティのソフトウェアが含まれている可能性があります：

XenMobile サードパーティ製品についての通知

解決された問題

October 25, 2019

XenMobile 10.11 では、次の問題が解決されています。

- 業務用モバイルアプリに関連する解決された問題については、Secure Hub、Secure Mail、およびSecure Webを参照してください。
- バージョン 10.10.0 Rolling Patch リリースの解決された問題については、以下を参照してください：
  - XenMobile Server 10.10.0 Rolling Patch 1
  - XenMobile Server 10.10.0 Rolling Patch 2
  - XenMobile Server 10.10.0 Rolling Patch 3
- RBAC 管理者によって、新規ユーザーや既存ユーザーにデフォルトの Admin の役割が割り当てられます。デフォルトの Admin の役割の割り当ては、スーパー管理者に限定する必要があります。[CXM-37805]
- 既に登録されている Android Enterprise デバイスでは、［**AllUsers**］ デリバリーグループに対する新規必須アプリは Google Play Store に表示されません。[CXM-64910]
- デバイスの Android 登録中に、次の致命的なエラーが表示されます：値を暗号化解除できません。[CXM-65936]
- Android Enterprise のエンタープライズの名前と所有者が Google Play ストア管理者コンソールに正しく表示されない場合があります。[CXM-65996]
- XenMobile Server 上で有効な VPP トークンを構成し、Apple の VPP ポータルから新しい VPP ブックを購入します。新しく追加したメディアブックは同期されず、コンソールに表示されません。[CXM-66453]
- 新しくインポートされた CA 証明書は、公開キーインターフェイス（PKI）エントリには表示されません。[CXM-67960]
- VPP アカウントを追加するとき（［設定］**>**［**iOS** 設定］）に、トークンが 350 文字を超えると、次のメッセージが表示されます：「入力された会社トークンは有効ではありません、新しいトークンを入力してください。」[CXM-68113]
- StoreFront サーバーにアクセスできない場合、MDX アプリを一覧表示する前に iOS 用の Secure Hub がタイムアウトします。[CXM-68117]
- XenMobile Server 10.11 の Secure Hub Apple プッシュ通知サービス（APNs）証明書の有効期限は、2019 年 8 月 2 日に終了します。その結果、iOS デバイスではエージェント通知が失敗し、アプリケーションのプッシュが遅れることがあります。今回のアップデートにより、Secure Hub APNs 証明書が更新され、2020 年 7 月 12 日に期限切れになります。[CXM-68354]

- XenMobile Server コンソールでは、クライアントプロパティの値の文字数制限は 256 です。[CXM-68386]
- Android を実行しているデバイスでは、エンタープライズアプリを更新できないことがあります。[CXM-68391]
- サーバープロパティ「bulk.enrollment.fetchRosterInfoDelay」の期間終了後、Apple School Manager DEP デバイスがサーバーと同期します: Apple School Manager ユーザーアカウントはサーバーから削除され、デバイスは匿名状態に移行します。[CXM-68417]
- Citrix SSO プロトコルを使用するように iOS の VPN デバイスポリシーが構成されている場合: ［接続時に **PIN** を要求］ 設定をオンにしてポリシーを保存すると、その設定は ［オフ］ に戻ります。[CXM-68463]
- REST API 経由で更新した最新バージョンにエンタープライズアプリを更新しても、バージョン番号は更新されません。[CXM-68588]
- アプリアクセスデバイスポリシーを展開した後、非準拠のデバイスは構成済みのアクションをトリガーしません。[CXM-69480]
- XenMobile Server を使用してパブリック iOS アプリをアップデートしようとすると、構成エラーが表示されます。[CXM-69555]
- Tomcat サーバーのステータスを確認する場合、サーバーのステータスが正常であっても、**0** ではなく **1** の戻り値が取得されることがあります。[CXM-69900]
- 以前のバージョンから移行したお客様の場合、デバイスの登録プロファイルが削除されていると、コンソールの［管理］タブを開くとエラーが表示される。[CXM-70341]
- RBAC の役割「階層 2 の技術者」は、2000 を超えるユーザーのユーザーグループへの登録招待状を作成できません。招待状を作成できるのは、完全な管理者ユーザーのみです。[CXM-71224]

関連情報

- XenMobile サポートナレッジセンター

既知の問題

January 10, 2020

XenMobile 10.11 には次の既知の問題があります。

- XenMobile Server で Apple Deployment Programs（以前の DEP）との通信エラーが発生します。この問題は、XenMobile 10.11 および 10.10 で発生します。最新情報は、「https://support.citrix.com/article/CTX267079」を参照してください。

- 業務用モバイルアプリに関連する既知の問題については、Secure Hub、Secure Mail、およびSecure Webを参照してください。
- バージョン 10.10.0 Rolling Patch リリースの既知の問題については、以下を参照してください:
  - XenMobile Server 10.10.0 Rolling Patch 1
  - XenMobile Server 10.10.0 Rolling Patch 2
  - XenMobile Server 10.10.0 Rolling Patch 3

関連情報

- XenMobile サポートナレッジセンター

アーキテクチャ

September 24, 2019

展開する XenMobile リファレンスアーキテクチャの XenMobile コンポーネントは、組織のデバイスまたはアプリケーションの管理要件がベースになります。XenMobile コンポーネントはモジュール形式で、相互に依存しています。たとえば、組織のユーザーのモバイルアプリに対してリモートアクセスを提供し、ユーザーデバイスのタイプを追跡するには、XenMobile に合わせて NetScaler Gateway を展開します。XenMobile でアプリケーションとデバイスを管理し、NetScaler Gateway によって、ユーザーがネットワークに接続できるようにします。

XenMobile コンポーネントの展開: XenMobile を展開し、ユーザーが内部ネットワーク内のリソースに接続できるようにする方法を次に示します。

- 内部ネットワークへの接続ユーザーがリモートの場合、NetScaler Gateway を介した VPN または Micro VPN 接続を使用して接続することができます。この接続により、内部ネットワークのアプリとデスクトップにアクセスできるようになります。
- デバイス登録。ユーザーは XenMobile でモバイルデバイスを登録できるので、管理者はネットワークリソースに接続するデバイスを XenMobile コンソールで管理できます。
- Web、SaaS、モバイルアプリユーザーは Secure Hub を使って、XenMobile から Web、SaaS、モバイルアプリにアクセスできます。
- Windows ベースのアプリケーションと仮想デスクトップユーザーは Citrix Receiver または Web ブラウザーを使用して接続し、StoreFront や Web Interface から、Windows ベースのアプリケーションや仮想デスクトップにアクセスすることができます。

オンプレミスの XenMobile Server の上記の機能のいずれかを実現するには、次の順番で XenMobile コンポーネントを展開することをお勧めします。

- で接続する必要があります。NetScaler Gateway で設定を構成し、Quick Configuration ウィザードを使用して、XenMobile、StoreFront、または Web Interface との通信を有効にすることができます。NetScaler

Gateway で Quick Configuration ウィザードを使用する前に、XenMobile、StoreFront、または Web Interface のいずれかをインストールし、通信を設定しておく必要があります。

- XenMobile。XenMobile をインストールした後、ユーザーによるモバイルデバイスの登録を許可するポリシーと設定を XenMobile コンソールで構成できます。モバイル、Web、および SaaS アプリケーションも構成できます。モバイルアプリには、Apple App Store や Google Play で提供されているアプリが含まれます。また、管理者が MDX Toolkit を使ってラップし、コンソールにアップロードしたモバイルアプリに接続することもできます。
- MDX Toolkit。MDX Toolkit は、組織内または社外で作成されたモバイルアプリを安全にラップできます。アプリケーションをラップした後、XenMobile コンソールを使用してアプリケーションを XenMobile に追加し、ポリシー構成を必要に応じて変更します。また、アプリカテゴリを追加したり、ワークフローを適用したり、アプリをデリバリーグループに展開したりすることができます。MDX Toolkit についてを参照してください。
- StoreFront（オプション）。Receiver との接続を介して、StoreFront から Windows ベースのアプリケーションや仮想デスクトップへのアクセスを提供できます。
- ShareFile Enterprise（オプション）。ShareFile を展開する場合は、XenMobile からエンタープライズディレクトリ統合を有効にできます。これは、Security Assertion Markup Language（SAML）ID プロバイダーとして機能します。ShareFile の ID プロバイダーの構成について詳しくは、ShareFile サポートサイトを参照してください。

XenMobile は、XenMobile コンソールを介してデバイス管理とアプリ管理を提供します。ここでは、XenMobile 展開のリファレンスアーキテクチャについて説明します。

実稼働環境では、スケーラビリティとサーバー冗長性の両方を実現するために、XenMobile ソリューションをクラスター構成で展開することをお勧めします。また、NetScaler SSL オフロード機能を使用すると、XenMobile Server の負荷をさらに軽減し、スループットを高めることができます。NetScaler で 2 つの負荷分散仮想 IP アドレスを構成することによって XenMobile のクラスタリングをセットアップする方法について詳しくは、「クラスタリング」を参照してください。

障害回復に対応する XenMobile 環境の構成について詳しくは、展開ハンドブックの障害回復の記事を参照してください。その記事にはアーキテクチャ図が含まれています。

以降のセクションでは、XenMobile 展開のさまざまなリファレンスアーキテクチャについて説明します。リファレンスアーキテクチャ図については、『XenMobile 展開ハンドブック』の、オンプレミス環境のリファレンスアーキテクチャについての記事と、アーキテクチャについての記事を参照してください。すべてのポートの一覧については、オンプレミスのポート要件の記事とクラウドのポート要件の記事を参照してください。

モバイルデバイス管理（**MDM**）モード

> 重要：
>
> MDM モードに構成し、後で ENT モードに変更する場合は、必ず同じ（Active Directory）認証を使用してください。XenMobile では、ユーザー登録後の認証モードの変更をサポートしていません。詳しくは、「XenMobile

> MDM Edition から Enterprise Edition へのアップグレード」を参照してください。

XenMobile MDM Edition では、モバイルデバイス管理を使用できます。プラットフォームのサポートについては、「サポートされるデバイスオペレーティングシステム」を参照してください。XenMobile の MDM 機能のみを使用する場合は、XenMobile を MDM モードで展開します。たとえば、次を実行する場合、

- デバイスポリシーやアプリを展開する
- アセットインベントリを取得する
- デバイスのワイプなどのアクションをデバイスで実行する

推奨モデルでは、XenMobile サーバーを DMZ に配置し、オプションで NetScaler をその前に配置して、XenMobile の追加保護を提供します。

モバイルアプリケーション管理（**MAM**）モード

MAM（別名 MAM-only モード）によってモバイルアプリケーション管理を実現します。プラットフォームのサポートについては、「サポートされるデバイスオペレーティングシステム」を参照してください。デバイスを MDM に登録せずに、XenMobile の MAM 機能のみを使用する場合は、XenMobile を MAM モードで展開します。たとえば、次を実行する場合、

- BYO モバイルデバイスのアプリとデータのセキュリティを保護する
- エンタープライズモバイルアプリを配信する
- アプリのロックおよびデータのワイプを実行する

デバイスを MDM に登録することはできません。

この展開モデルでは、XenMobile Server を配置し、NetScaler Gateway をその前に配置して、XenMobile をさらに保護します。

MDM+MAM モード

MDM モードと MAM モードを併用すると、モバイルアプリとデータの管理に加えてモバイルデバイス管理を行うことができます。プラットフォームのサポートについては、「サポートされるデバイスオペレーティングシステム」を参照してください。XenMobile の MDM+MAM 機能を使用する場合は、XenMobile を ENT（エンタープライズ）モードで展開します。たとえば、次のようにしたいとします。

- MDM を使用してコーポレート発行のデバイスを管理する
- デバイスポリシーやアプリを展開する
- アセットインベントリを取得する
- デバイスのワイプ
- エンタープライズモバイルアプリを配信する
- アプリをロックしてデバイス上のデータをワイプする

推奨展開モデルでは、XenMobile サーバーを DMZ に配置し、NetScaler Gateway をその前に配置して、XenMobile の追加保護を提供します。

内部ネットワークの **XenMobile**： もう一つの展開オプションは、DMZ ではなく内部ネットワークにオンプレミスの XenMobile Server を配置します。この展開は、ネットワークアプライアンスのみを DMZ に配置できるようセキュリティポリシーが求める場合に使用されます。この展開では、XenMobile サーバーは、DMZ にありません。そのため、DMZ から SQL Server と PKI サーバーにアクセスできるようにするため内部ファイヤフォール上でポートを開く必要がありません。

システム要件と互換性

January 24, 2020

> 注：
>
> この記事では、XenMobile Server 10.11 のシステム要件と互換性について説明します。Endpoint Management のシステム要件について詳しくは、「システム要件」を参照してください。

要件と互換性情報について詳しくは、次の記事を参照してください。

- XenMobile の互換性
- サポートされるデバイスオペレーティングシステム
- ポート要件
- スケーラビリティ
- ライセンス
- FIPS 140-2 への準拠
- 言語サポート

XenMobile 10.11 を実行するための最小システム要件は以下のとおりです：

- 以下のいずれかのサーバーオペレーティングシステム
  - Citrix Hypervisor 8.0 または Citrix XenServer（サポートされるバージョン：6.5.x、7.0、7.1、7.2、7.3、7.4、7.5、7.6）。詳しくは「XenServer」を参照してください。
  - VMware（サポートされるバージョン：ESXi 5.5 Update 3、ESXi 6.0、ESXi 6.5.0 Update 3、または ESXi 6.7 Update 2 patch 10）。詳しくは「VMware」を参照してください。
  - Hyper-V（サポートされるバージョン：Windows Server 2012 R2、Windows Server2016、Windows Server 2019）。詳しくは「Hyper-V」を参照してください。
  - Endpoint Management コネクタ：Exchange ActiveSync 用 10.1.9.24
  - Citrix Gateway コネクタ：Exchange ActiveSync 用 8.5.3.19
- デュアルコアプロセッサ
- 4 つの仮想 CPU
- 実稼働環境で RAM は 8GB、概念実証およびテスト環境で RAM は 4GB

- 50GB のディスクスペース
- Citrix ライセンスサーバー 11.15.x 以降
  XenMobile Server をアップグレードする前に、ライセンスサーバーを更新します。

> 重要：
>
> ESXi 6.7 を実行するには、次の回避策を実行する必要があります。
>
> 1. VMware が提供する OVF ツールを使用して、citrix.com からダウンロードした OVA ファイルを展開します。VMware のページから OVF ツールを入手します（https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491）。
> 2. 抽出された 3 つのファイルのうち、.vmdk ファイルをデータストアにアップロードします。
> 3. 仮想マシンを作成します。
>   a) 仮想マシンに名前を付け、互換性オプションとして ［**ESX / ESXi 4.x** 仮想マシン］ を選択します。
>   b) ゲスト OS ファミリは、［**Linux** ］ を選択します。
>   c) ゲスト OS のバージョンは、［その他の **2.6.x Linux**（**64** ビット）］ を選択します。
>   d) データストアは、［デフォルト］ を選択します。
>   e) カスタマイズ中に、デフォルトのハードディスク、USB コントローラ、および CD / DVD ドライブを取り外します。
>   f) ［ネットワーク］ で、アダプタの種類に ［**VMXNET3**］ を選択します。
>   g) ESXi 上では、ディスクがローカルの場合は、［**SCSI** コントローラー］ と ［**LSI** ロジックパラレル］ を選択します。共有ディスクを使用している場合は、［**VMware Paravirtual**］ を選択します。
>   h) ［次へ］ をクリックして VM の作成を終了します。
> 4. データストアに移動し、先にアップロードした.vmdk ファイルをコピーします。それを XenMobile 用に作成した VM ディレクトリにコピーします。
> 5. ESXi Web インターフェイスから、VM を選択して設定を編集します。
> 6. ［ハードディスクの追加］ をクリックします。
> 7. 先ほどコピーした.vmdk ファイルを選択し、VM に接続します。
> 8. ［保存］ をクリックします。
> 9. VM の電源を入れます。

NetScaler Gateway のシステム要件

XenMobile 10.11 で NetScaler Gateway を実行するための最小システム要件は以下のとおりです。

- NetScaler Gateway（オンプレミス）。サポートされるバージョン：11.1（最新ビルド）、12.0、12.1（最新ビルド）、13（最新ビルド）
- また、Active Directory と通信できる必要があり、これにはサービスアカウントが必要です。クエリおよび読み取りアクセス権限のみが必要です。

XenMobile 10.11 のデータベース要件

XenMobile では、次のいずれかのデータベースが必要です。

- Microsoft SQL Server

  XenMobile リポジトリでは、以下のサポート対象バージョンのいずれかで稼動している Microsoft SQL Server データベースをサポートします。Microsoft SQL Server データベースの詳細については、「Microsoft SQL Server」を参照してください。

  - Microsoft SQL Server 2012 SP4
  - Microsoft SQL Server 2014 SP3
  - Microsoft SQL Server 2016 SP2
  - Microsoft SQL Server 2017 CU 13
  - Microsoft SQL Server 2019 CTP 3.2

  XenMobile はデータベース高可用性用に、SQL の基本的な可用性グループ（AlwaysOn 可用性グループ）および SQL クラスタリングをサポートします。

  Citrix では、Microsoft SQL をリモートで使用することをお勧めします。

  Microsoft SQL のアップグレードについて詳しくは、Microsoft 社の記事SQL Server をアップグレードするを参照してください。

- PostgreSQL（テスト環境のみ）。PostgreSQL は XenMobile に含まれます。テスト環境で、ローカルまたはリモートで使用できます。データベースの移行はサポートされていません。テスト環境で作成したデータベースを実稼働環境に移行することはできません。

  XenMobile の全エディションが Remote PostgreSQL 9.5.1 と 9.5.11 for Windows をサポートしますが次の制限事項があります：実稼働環境での使用はお勧めしません。サポートするのは最大 300 デバイスです。300 台を超える場合は、オンプレミスの SQL Server を使用します。クラスタリングはサポートされていません。

SQL Server サービスアカウントの要件

XenMobile で使用される SQL Server のサービスアカウントに、DBcreator 役割の権限があることを確認します。XenMobile サーバーのインストール時に指定した SQL サーバーアカウントのパスワードを記録します。このパスワードは、XenMobile サーバーの回復中に XenMobile データベースのクローンを作成する必要がある場合に必要です。

SQL Server のサービスアカウントについて詳しくは、Microsoft Developer Network のサイトで以下のページを参照してください。以下のリンクから SQL Server 2014 の情報にアクセスできます。これらのリンクは SQL Server 2014 の情報を示します。別のバージョンを使用している場合は、［その他のバージョン］ の一覧で該当するサーバーのバージョンを選択してください：

- サーバー構成 - サービスアカウント

- Windows のサービスアカウントと権限の構成
- Server-Level の役割

Virtual Apps and Desktops の互換性

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906

StoreFront の互換性

- StoreFront 3.12.2
- StoreFront 7 1811
- StoreFront 7 1906

その他の互換性

- Endpoint Management コネクタ：Exchange ActiveSync 用 10.1.9.24
  - 古いバージョンはテストされていません。
- Citrix Gateway コネクタ：Exchange ActiveSync 用 8.5.3.19
  - 古いバージョンはテストされていません。

XenMobile の互換性

October 25, 2019

> 注：
>
> この記事では、XenMobile Server の互換性について説明します。エンドポイント管理でテストされたコンポーネントについては、「Endpoint Management の互換性」を参照してください。

新しい機能や修正された機能、およびポリシーの更新を利用するには、最新バージョンの MDX Toolkit、Secure Hub、および業務用モバイルアプリをインストールすることをお勧めします。MDX Toolkit の代わりに MDX Service を使用できます。詳しくは、「XenMobile MDX Service」を参照してください。

> 重要：
>
> XenMobile 業務アプリに関するエンタープライズ配信のサポートは、2017 年 12 月 31 日に終了しました。詳しくは、シトリックスの製品マトリクスを参照してください。現在は、パブリックアプリストア配信のみがサポ

> ートされています。

このトピックでは、連係可能な XenMobile コンポーネントのサポートされているバージョンを示しています。

サポートされているバージョンとアップグレードパス

最新バージョンの Secure Hub、MDX Toolkit、業務用モバイルアプリは、最新バージョンと 2 つ前までのバージョンの XenMobile Server と互換性があります。

最新バージョンの業務用モバイルアプリには、最新バージョンの Secure Hub が必要です。2 つ前までのバージョンのアプリは、最新の Secure Hub と互換性があります。

XenMobile Server（オンプレミス）

- Citrix は、直近 2 つのバージョンの XenMobile Server からのアップグレードをサポートしています。
- XenMobile Server の最新バージョン：
  - XenMobile Server 10.11
- アップグレード元：
  - XenMobile Server 10.10.x
  - XenMobile Server 10.9.x

業務用モバイルアプリ

最新バージョンの業務用モバイルアプリには、最新バージョンの Secure Hub が必要です。2 つ前までのバージョンのアプリは、最新の Secure Hub と互換性があります。

業務用モバイルアプリの 2 週間ごとのリリースの流れと Secure Mail および Secure Web の段階的リリースプロセスについて詳しくは、「リリーススケジュール」を参照してください。サポートについて詳しくは、「業務用モバイルアプリのサポート」を参照してください。

MDX Toolkit

- Citrix は、最新の 3 つのリリース（n.n.n）の MDX Toolkit をサポートしています。また、XenMobile MDX Service をアプリのラッピングに使用することもできます。詳しくは、「XenMobile MDX Service」を参照してください。
- サードパーティ製アプリをラップする場合、最新のオンプレミスツールキットのバージョンは MDX Toolkit 19.9.5（iOS と Android 用）です。MDX Toolkit 19.9.0 および 19.8.0 から MDX Toolkit 19.9.5 にアップグレードできます。

MDX Toolkit 10.7.10 は、業務用モバイルアプリ（旧称 XenMobile Apps）のラッピングをサポートする最終リリースです。業務用モバイルアプリには、パブリックアプリストアからアクセスします。

ブラウザーサポート

XenMobile Server は、次のブラウザーをサポートしています：

- Internet Explorer（ただし、バージョン 9 以前は対象外）
- Chrome
- Firefox
- Self Help Portal で使用するためのモバイルデバイス上の Safari

XenMobile Server は、ほとんどの最新バージョンおよび 1 つ前のバージョンのブラウザーと互換性があります。

サポートされるデバイスオペレーティングシステム

January 10, 2020

> 注：
>
> この記事では、XenMobile Server 10.11 でサポートされているデバイスオペレーティングシステムについて説明します。Endpoint Management でサポートされているオペレーティングシステムについては、「サポートされるデバイスオペレーティングシステム」を参照してください。

XenMobile は次のプラットフォームとオペレーティングシステムを実行中のデバイスをサポートし、アプリおよびデバイスの管理を含むエンタープライズモビリティを管理します。プラットフォーム固有の制限事項やセキュリティ機能によって、XenMobile ではすべてのプラットフォームですべての機能がサポートされるわけではありません。

ここに記載したサポートされるデバイスプラットフォーム情報は、XenMobile コネクタ：Exchange ActiveSync 用および Citrix Gateway コネクタ：Exchange ActiveSync 用にも適用されます。

> 注：
>
> 最低限、主要オペレーティングシステムプラットフォームの最新バージョンおよび 1 つ前のバージョンをサポートします。XenMobile の新しいバージョンには、以前のプラットフォームリリースで使用できない機能もあります。

オペレーティングシステムのサポートリスト

Citrix XenMobile は、以下のオペレーティングシステムをサポートします：

- **Android**： 6.x、7.x、8.x、9.x、Android Q

  > 注：
  >
  > Android Q については、「Android に関する注意事項」を参照してください。

- **iOS**： 11.x、12.x、13.x

- **macOS**：10.11 El Capitan、10.12 Sierra、10.13 High Sierra
- **Windows 10** デスクトップおよびタブレット： Windows 10 RS4 および RS5（MDM のみ）
- **Windows Phone**：Windows Phone 8.1、Windows Phone 10、Windows 10 RS4 および RS5（MDM のみ）
- **Windows Mobile/CE**： （MDM のみ）。2018 年第 2 四半期以降、新しいお客様は Windows Mobile/CE デバイスのサポートをご利用できなくなります。
- **Symbian** デバイス： 2018 年第 2 四半期以降、新規ユーザーは Symbian デバイスのサポートを利用できなくなります。以下のリストには、Symbian デバイスを以前構成したユーザーに対して XenMobile がサポートするデバイスの一部が含まれています。
  - Symbian 3
  - Symbian S60 5th Edition
  - Symbian S60 3rd Edition、Feature Pack 2
  - Symbian S60 3rd Edition、Feature Pack 1
  - Symbian S60 3rd Edition
  - Symbian S60 3rd Edition、Feature Pack 2
  - Symbian S60 2nd Edition、Feature Pack 2
- **Samsung SAFE** および **KNOX**： 互換性のある Samsung デバイスでは、XenMobile は Samsung for Enterprise (SAFE) ポリシーと Samsung Knox ポリシーの両方をサポートし、拡張しています。XenMobile では、SAFE ポリシーと制限を展開する前に SAFE API を有効にする必要があります。これを行うには、組み込みの Samsung Enterprise License Management（ELM）キーをデバイスに展開します。Samsung Knox API を有効にするには：
  1. Samsung Knox License Management System（KLMS）を使用して Samsung Knox ライセンスを購入します。
  2. Samsung ELM キーを展開します。
- **HTC**： HTC 固有のポリシーの場合、HTC API バージョン 0.5.0
- **Sony**： Sony 固有のポリシーの場合、Sony Enterprise SDK 2.0

Android に関する注意事項

AndroidQ 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。

- 従来のデバイス管理モードで Android Q デバイスを登録しないようにすることをお勧めします。Google はデバイス管理 API を廃止しますが、これは Android Q を実行しているデバイスに影響があります。API が廃止された後、従来のデバイス管理モードで Android Q デバイスを登録すると失敗します。

- Android Q デバイスでは Android Enterprise を使用することをお勧めします。詳しくは、「Device Administration から Android Enterprise への移行」を参照してください。
- Google API の変更は、MAM-only モードで登録されているデバイスには影響しません。

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。Citrix では、ホスト名に一致する SAN が含まれている場合にのみ証明書を信頼します。
- 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。

Android O（バージョン 8）のリリースに伴う変更:

- SSLv3 は Android O ではサポートされていません。Google では SSLv3 接続がサポートされなくなりました。つまり、Android O デバイス上で稼働する業務用モバイルアプリは、SSLv3 接続を使用する内部サーバーに接続できません。SSLv3 を使って接続するサーバーを使用する場合は、ユーザーの接続障害を回避するために、Android O を展開する前にこの制限に対処することが重要です。
- パブリックアプリストアでの Citrix 業務用モバイルアプリバージョン 10.6.20 のリリースをもって、Android 4.4x のサポートは終了しました。
- Citrix 業務用モバイルアプリと MDX ラップしたアプリは、ARM ベースのプロセッサを搭載した Android デバイスで使用できます。Intel x86 または x64 ベースの Android デバイスではサポートされていません。

BlackBerry

BlackBerry デバイスの管理は、XenMobile コネクタ: Exchange ActiveSync 用によって提供されます。詳しくは、「XenMobile コネクタ: Exchange ActiveSync 用」を参照してください。

ポート要件

September 24, 2019

デバイスとアプリが XenMobile と通信できるようにするには、ファイアウォールの特定のポートを開きます。次の表に、開く必要があるポートを一覧で示します。

アプリ管理のために **NetScaler Gateway** および **XenMobile** 用のポートを開く

Citrix Secure Hub、Citrix Receiver、および NetScaler Gateway Plug-in から NetScaler Gateway 経由でユーザーが以下のコンポーネントに接続できるように、次のポートを開きます:

- XenMobile

- StoreFront
- Citrix Virtual Apps and Desktops
- Citrix Gateway コネクタ：Exchange ActiveSync 用
- イントラネット Web サイトなどのその他の内部ネットワークリソース

NetScaler から Launch Darkly へのトラフィックを有効化するには、こちらのCitrix Knowledge Center の記事に示されている IP アドレスを使用します。

NetScaler Gateway について詳しくは、NetScaler Gateway ドキュメントを参照してください。NetScaler IP（NSIP）、仮想サーバー IP（VIP）、サブネット IP（SNIP）のアドレスの情報は参照先のドキュメントに記載されています。

TCP ポート	説明	接続元	接続先
21 または 22	FTP または SCP サーバーへのサポートバンドルの送信に使用されます。	XenMobile	FTP または SCP サーバー
53 (TCP と UDP)	DNS 接続に使用されます。	NetScaler Gateway、XenMobile	DNS サーバー
80	NetScaler Gateway は、2 番目のファイアウォールを介して VPN 接続を内部ネットワークリソースに渡します。こうした状況は、通常、ユーザーが NetScaler Gateway Plug-in でログオンした場合に起こります。	NetScaler Gateway	イントラネット Web サイト
80 または 8080; 443	列挙、チケット機能、および認証に使用される XML および Secure Ticket Authority（STA）ポート。ポート 443 の使用を推奨します。	StoreFront および Web Interface XML のネットワークトラフィック、NetScaler Gateway STA	Virtual Apps または Desktops
123 (TCP と UDP)	ネットワークタイムプロトコル（Network Time Protocol：NTP）サービスに使用されます。	NetScaler Gateway、XenMobile	NTP サーバー

TCP ポート	説明	接続元	接続先
389	セキュリティで保護されない LDAP 接続に使用	NetScaler Gateway、XenMobile	LDAP 認証サーバーまたは Microsoft Active Directory
443	Citrix Receiver から StoreFront への接続または Receiver for Web から Virtual Apps and Desktops への接続に使用されます。	インターネット	NetScaler Gateway
443	Web、モバイル、および SaaS アプリの配信のための XenMobile への接続に使用されます。	インターネット	NetScaler Gateway
443	XenMobile Server との一般的なデバイス通信に使用されます。	XenMobile	XenMobile
443	登録のためにモバイルデバイスから XenMobile への接続に使用されます。	インターネット	XenMobile
443	XenMobile から Citrix Gateway コネクタ: Exchange ActiveSync 用への接続に使用されます。	XenMobile	Citrix Gateway コネクタ：Exchange ActiveSync 用
443	Citrix Gateway コネクタ：Exchange ActiveSync 用から XenMobile への接続に使用されます。	Citrix Gateway コネクタ：Exchange ActiveSync 用	XenMobile
443	証明書認証のない展開でのコールバック URL に使用されます。	XenMobile	NetScaler Gateway
514	XenMobile と syslog サーバー間の接続に使用されます。	XenMobile	Syslog サーバー

TCP ポート	説明	接続元	接続先
636	セキュリティで保護される LDAP 接続に使用されます。	NetScaler Gateway、XenMobile	LDAP 認証サーバーまたは Active Directory
1494	内部ネットワーク内の Windows ベースのアプリケーションへの ICA コネクションに使用されます。このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway	Virtual Apps または Desktops
1812	RADIUS 接続に使用されます。	NetScaler Gateway	RADIUS 認証サーバー
2598	セッション画面の保持を使用した内部ネットワーク内の Windows ベースのアプリケーションへの接続に使用されます。このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway	Virtual Apps または Desktops
3268	Microsoft Global Catalog のセキュリティで保護されない LDAP 接続に使用されます。	NetScaler Gateway、XenMobile	LDAP 認証サーバーまたは Active Directory
3269	Microsoft Global Catalog のセキュリティで保護される LDAP 接続に使用されます。	NetScaler Gateway、XenMobile	LDAP 認証サーバーまたは Active Directory
9080	NetScaler と Citrix Gateway コネクタ: Exchange ActiveSync 用間の HTTP トラフィックに使用されます。	NetScaler	Citrix Gateway コネクタ：Exchange ActiveSync 用
30001	HTTPS サービスの初期ステージング用の管理 API	内部 LAN	XenMobile Server

TCP ポート	説明	接続元	接続先
9443	NetScaler と Citrix Gateway コネクタ: Exchange ActiveSync 用間の HTTPS トラフィックに使用されます。	NetScaler	Citrix Gateway コネクタ：Exchange ActiveSync 用
45000; 80	2 つの XenMobile VM がクラスターで展開されている場合にそれらの VM 間の通信に使用されます。ポート 80 は、ノード間通信と SSL オフロード用です。	XenMobile	XenMobile
8443	登録、XenMobile Store、モバイルアプリ管理（MAM）に使用されます。	XenMobile; NetScaler Gateway; デバイス; インターネット	XenMobile
4443	管理者がブラウザーを使用して XenMobile コンソールにアクセスする場合に使用されます。また、すべての XenMobile クラスターノードのログとサポートバンドルを 1 つのノードからダウンロードするために使用されます。	アクセスポイント（ブラウザー）; XenMobile	XenMobile
27000	外部の Citrix ライセンスサーバーへのアクセスに使用されるデフォルトポート。	XenMobile	Citrix ライセンスサーバー
7279	Citrix ライセンスのチェックインおよびチェックアウトに使用されるデフォルトポート。	XenMobile	Citrix ベンダーデーモン

TCP ポート	説明	接続元	接続先
161	UDP プロトコルを使用する SNMP トラフィックに使用されます。	SNMP マネージャー	XenMobile
162	XenMobile から SNMP マネージャーに SNMP トラップ通知を送信するために使用されます。接続元は XenMobile で、接続先は SNMP マネージャーです。	XenMobile	SNMP マネージャー

デバイス管理のために **XenMobile** ポートを開く

XenMobile がネットワーク内で通信できるように、次のポートを開きます。

TCP ポート	説明	接続元	接続先
25	XenMobile 通知サービスのデフォルトの SMTP ポート。SMTP サーバーで別のポートを使用する場合は、そのポートがファイアウォールによってブロックされないことを確認してください。	XenMobile	SMTP サーバー

TCP ポート	説明	接続元	接続先
80、443	Apple iTunes App Store、Google Play (80 を使用する必要があります)、または Windows Phone Store への Enterprise App Store 接続。Apple ボリューム購入プログラムに使用されます。iOS 上の Citrix Mobile Self-Serve、Secure Hub for Android、または Secure Hub for Windows Phone を介してアプリストアからアプリを公開するために使用されます。	XenMobile	ax.apps.apple.comおよび*.mzstatic.com; vpp.itunes.apple.com; login.live.com; *.notify.windows.com; play.google.com, android.clients.google.com, android.l.google.com
80 または 443	XenMobile と Nexmo SMS Notification Relay 間の送信接続に使用されます。	XenMobile	Nexmo SMS Relay Server
389	セキュリティで保護されない LDAP 接続に使用されます。	XenMobile	LDAP 認証サーバーまたは Active Directory
443	Android および Windows Mobile の登録およびエージェント設定に使用されます。	インターネット	XenMobile
443	Android および Windows デバイス、XenMobile Web コンソール、および MDM Remote Support Client の登録およびエージェント設定に使用されます。	インターネット LAN および Wi-Fi	XenMobile

TCP ポート	説明	接続元	接続先
1433	デフォルトでリモートデータベースサーバーへの接続に使用されます（オプション）。	XenMobile	SQL Server
2195	iOS デバイスの通知およびデバイスポリシーのプッシュのための`gateway.push.apple.com`への Apple Push Notification サービス（APNs）送信接続に使用されます。	XenMobile	インターネット（パブリック IP アドレス 17.0.0.0/8 を使用している APNs ホスト）
2196	iOS デバイスの通知およびデバイスポリシーのプッシュのための`feedback.push.apple.com`への APNs 送信接続に使用されます。		
5223	Wi-Fi ネットワーク上の iOS デバイスから`*.push.apple.com`への APNs 送信接続に使用されます。	Wi-Fi ネットワーク上の iOS デバイス	インターネット（パブリック IP アドレス 17.0.0.0/8 を使用している APNs ホスト）
8081	オプションの MDM Remote Support Client からアプリトンネルに使用されます。デフォルトは 8081 です。	リモートサポート	XenMobile
8443	iOS および Windows Phone デバイスの登録に使用されます。	インターネット LAN および Wi-Fi	XenMobile

自動検出サービスの接続のポート要件

このポート構成では、Secure Hub for Android から接続する Android デバイスで内部ネットワークから Citrix ADS（Autodiscovery Service：自動検出サービス）にアクセスできるようにします。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とき、ADS にアクセスする能力は重要です。

> 注：
>
> ADS 接続ではプロキシサーバーがサポートされ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。

証明書ピン留めを有効にする場合は、次の前提条件を実行します。

- **XenMobile** サーバーと **NetScaler** 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。
- シトリックス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。

証明書ピン留めでは、デバイスを登録前に ADS に接続する必要があります。この要件により、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。Secure Hub でデバイスを登録する場合、デバイスが ADS にアクセスできる必要があります。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 FQDN および IP アドレスのポート 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
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS 通信
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS 通信

> 注：
>
> 10.6.15 より前の Secure Hub バージョンでは、FQDN は discovery.mdm.zenprise.com。IP アドレス 52.5.138.94 および 52.1.30.122 用にポート 443 を開きます。

Android Enterprise のネットワーク要件

いくつかの発信接続は、Android Enterprise のネットワーク環境の設定時に注意が必要です。

デバイスのポート要件

接続先ホスト	ポート	説明
*.googleapis.com	TCP/443	Google Mobile Management、Google API、Google Play ストア API に使用
play.google.com、android.com google-analytics.com、android.clients.google.com	TCP/443	Google Play および android.clients.google.com 経由の更新に使用アプリ、更新、Google Play ストア API をダウンロード
cm.googleapis.com	TCP/443	Firebase Cloud Messaging に使用
android.apis.google.com、cm.googleapis.com	TCP/5228、5229、5230	Firebase Cloud Messaging の送信、デバイスの Wi-Fi でのインターネット通信に使用
connectivitycheck.android.com www.google.com	TCP/443	CloudDPC v470 より前の接続性チェックに使用 N MR1 以降の Android 接続性チェックでは、`https://www.google.com/generate_204`にアクセスできるか、指定された Wi-Fi ネットワークでアクセス可能な PAC ファイルが指定されている必要があります。

XenMobile のポート要件

EMM コンソールがオンプレミスにある場合、Managed Google Play Enterprise を作成して Managed Google Play iFrameにアクセスするには、次の接続先ホストにネットワークからアクセスできる必要があります。Google では、アプリの検索と承認を簡素化するため、Managed Play iFrame を EMM 開発者が利用できるようにしました。

接続先ホスト	ポート	説明
play.google.com	TCP/443	Google Play ストア、Play Enterprise サインアップに使用
accounts.youtube.com、accounts.google.com	TCP/443	アカウント認証に使用

接続先ホスト	ポート	説明
apis.google.com	TCP/443	GCM とその他 Google Web サービスに使用
ogs.google.com	TCP/443	iFrame UI 要素に使用
notifications.google.com	TCP/443	デスクトップ通知とモバイル通知に使用
fonts.googleapis.com、*.gstatic.com、*.googleusercontent.com	TCP/443	Google Fonts ユーザー生成コンテンツに使用。たとえば、ストア内のアプリのアイコン
cri.pki.goog、ocsp.pki.goog	TCP/443	証明書の検証に使用

スケーラビリティとパフォーマンス

January 10, 2020

XenMobile インフラストラクチャの規模を理解することは XenMobile を展開し構成する方法を決定するうえで重要な役割を果たします。このトピックは、小規模から大規模なオンプレミス XenMobile エンタープライズ展開でパフォーマンスおよびスケーラビリティのインフラストラクチャ要件を判断するための、スケーラビリティテストのデータおよび手順で構成されています。

ここでスケーラビリティは、展開環境に既に登録されているデバイスが同時に展開に再接続する能力によって定義されています。

- スケーラビリティは展開に登録されたデバイスの最大数として定義されます。
- ログインレートは既存のデバイスが環境に再接続できる最大レートです。

このトピックのデータは、10,000 ～ 75,000 デバイスの規模の展開でテストされた結果です。テストは、既知のワークロードを使用したモバイルデバイスで構成されています。

すべてのテストは、XenMobile Enterprise Edition で実行されました。

テストは NetScaler Gateway 8200 を使用して実行されました。同様の、またはそれ以上の容量を持つ NetScaler アプライアンスの場合は、同様のまたはそれ以上のスケーラビリティおよびパフォーマンスを提供することが予想されます。

スケーラビリティテスト結果の要約は以下のとおりです。

最大 **75,000** 台のデバイスを展開する場合のスケーラビリティテストの結果の概要

ログインレート（既存ユーザーの再接続レート）- 1 時間に最大 9,375 個のデバイス

使用される構成:

- NetScaler Gateway
- MPX 8200
- XenMobile Enterprise Edition のみです。
- 7 ノードで構成される XenMobile Server クラスター
- データベース: Microsoft SQL Server 外部データベース

デバイスおよびハードウェア構成ごとのテスト結果

デバイス数	12,500	30,000	60,000	75,000
1 時間あたりの既存デバイスの再接続レート	1,250	3,750	7,500	9,375
XenMobile Server – モード	スタンドアロン	クラスター	クラスター	クラスター
XenMobile Server – クラスター	-	3	5	7
XenMobile Server - 仮想アプライアンス	メモリー = 8 GB RAM、vCPUs = 4	メモリー = 16 GB RAM、vCPUs = 6	メモリー = 24 GB RAM、vCPUs = 8	メモリー = 24 GB RAM、vCPUs = 8
Active Directory	メモリー = 4 GB RAM、vCPUs = 2	メモリー = 8 GB RAM、vCPUs = 4	メモリー = 16 GB RAM、vCPUs = 4	メモリー = 16 GB RAM、vCPUs = 4
Microsoft SQL Server 外部データベース	メモリー = 8 GB RAM、vCPUs = 4	メモリー = 16 GB RAM、vCPUs = 8	メモリー = 24 GB RAM、vCPUs = 16	メモリー = 24 GB RAM、vCPUs = 16

スケーラビリティプロファイル

Active Directory 構成	使用したプロファイル
ユーザー	100,000
グループ	200,000
入れ子構造のレベル	5

XenMobile Server の構成	合計	ユーザーごと
ポリシー	20	20
アプリ	270	50
パブリックアプリ	200	0
MDX	50	30
Web および SaaS	20	20
アクション	50	
デリバリーグループ	20	
デリバリーグループあたりの Active Directory グループ	10	
SQL		
データベースの数	1	

デバイス接続およびアプリアクティビティ

これらのスケーラビリティテストでは、展開で登録されたデバイスが 8 時間の期間を通して再接続する能力のデータを収集しています。

テストは、デバイスがすべての関連セキュリティポリシーを取得できる再接続間隔をシミュレーションします。XenMobile Server ノードは、通常よりも高い負荷条件下に置かれます。以降の再接続では、変更されたポリシー、または新しいポリシーのみが iOS デバイスにプッシュされるため、XenMobile Server ノードの負荷は軽減されます。

テストに使用されるのは、50% が iOS デバイスで、残りの 50% が Android デバイスです。

これらのテストでは、再接続する Android デバイスが、事前に GCM 通知を受信しているものとします。

8 時間のテスト間隔中、以下のアプリ関連のアクティビティが発生します。

- Secure Hub が一度起動し、対象アプリ一覧を表示します
- 2 つの SAML Web アプリが起動します

- 4 つの MAM アプリがダウンロードされます
- Secure Mail で使用する 1 つの STA が生成されます
- 240 の STA チケットの検証は、マイクロ VPN 経由の Secure Mail の再接続イベントごとに、1 つずつ実行されます。

リファレンスアーキテクチャ

スケーラビリティテストで使用される展開のリファレンスアーキテクチャについては、「オンプレミス環境のリファレンスアーキテクチャ」の「コア MAM+MDM リファレンスアーキテクチャ」を参照してください。

制限事項

このトピックのスケーラビリティテストの結果を検討するときに、以下に注意してください。

- Windows プラットフォームはテストしていません。
- ポリシーのプッシュは、iOS および Android デバイスでテストされました。
- 各 XenMobile Server ノードは最大 12,000 デバイスを同時にサポートします。

ライセンス

January 10, 2020

XenMobile では、Citrix ライセンスサーバーを使ってライセンスを管理します。XenMobile Server および NetScaler Gateway にはライセンスが必要です。

NetScaler Gateway ライセンスについて詳しくは、NetScaler Gateway ドキュメントを参照してください。Citrix ライセンスサーバーについて詳しくは、「The Citrix Licensing System」を参照してください。

XenMobile Server を購入すると、ライセンスのアクティブ化手順について書かれた注文確認メールメッセージが送信されます。新規顧客は、ライセンスプログラムを登録してから注文を行う必要があります。XenMobile ライセンスモデルおよびプログラムについては、XenMobile ライセンスを参照してください。

要件

- XenMobile Server の最新バージョンにアップデートする前に、Citrix ライセンスサーバーを 11.145.x 以降にアップデートしてください。それより前のバージョンのライセンスサーバーは、最新バージョンの XenMobile はサポートしません。

- XenMobile のライセンスをダウンロードする前に、Citrix ライセンスサーバーをインストールする必要があります。ライセンスファイルを生成するには、Citrix ライセンスサーバーをインストールしたサーバー名が必要となります。XenMobile をインストールする場合、そのサーバーにはデフォルトで Citrix ライセンスサーバーがインストールされます。または、既存の Citrix ライセンスサーバー展開を使って XenMobile のライセンスを管理できます。Citrix ライセンスサーバーのインストール、展開、および管理について詳しくは、「製品ライセンスの有効化」を参照してください。
- XenMobile のノード（インスタンス）をクラスター化する場合は、リモートサーバー上で Citrix ライセンスサーバーを使用する必要があります。
- 受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、すべてのライセンスファイルもバックアップに含まれます。ただし、最初に構成ファイルをバックアップせずに XenMobile を再インストールする場合は、元のライセンスファイルが必要になります。

XenMobile ライセンスについての考慮事項

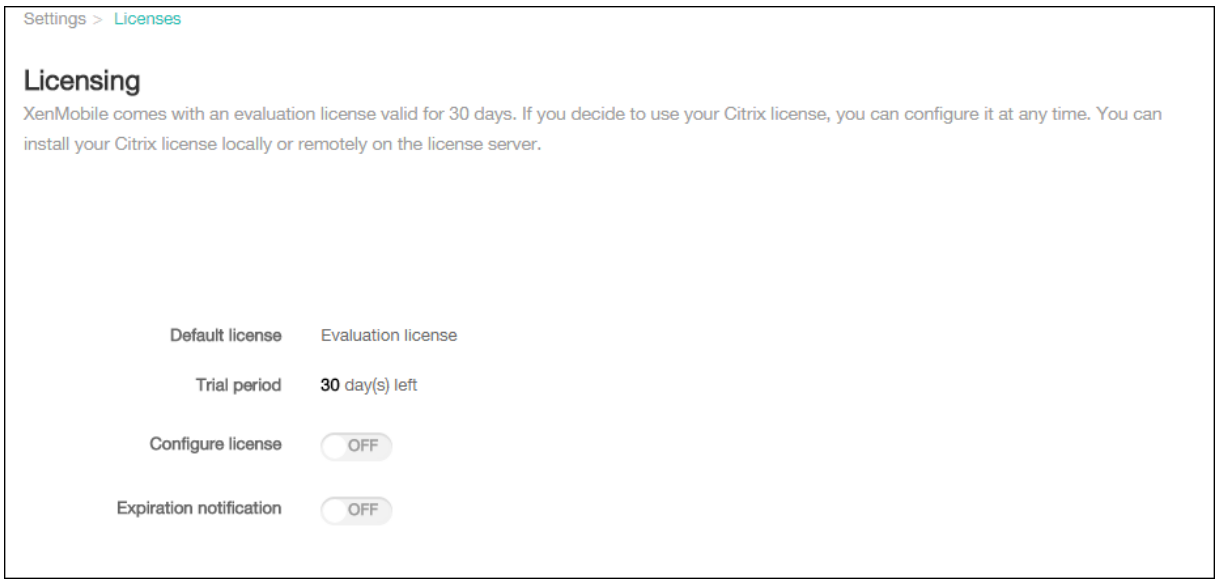
ライセンスがない場合、30 日間は試用モードで XenMobile のすべての機能を操作することができます。この試用モードを使用できるのは、XenMobile のインストール時から 30 日間の 1 回限りです。有効な XenMobile ライセンスを使用できるかどうかに関係なく、XenMobile Web コンソールへのアクセスはブロックされません。XenMobile コンソールで、試用期間の残り日数を参照できます。

XenMobile では複数のライセンスをアップロードできますが、アクティブ化できるライセンスは一度に 1 つだけです。

XenMobile ライセンスの有効期限が切れると、すべてのデバイス管理機能を実行できなくなります。たとえば、新しいユーザーまたはデバイスを登録することができず、また登録済みデバイスに展開されたアプリケーションや構成を更新できません。XenMobile ライセンスモデルおよびプログラムについては、XenMobile ライセンスを参照してください。

XenMobile コンソールで［ライセンス］ページを開くには

XenMobile をインストールすると最初に［ライセンス］ページが開き、デフォルトの 30 日間試用モードでライセンスが設定されますが、まだライセンスは構成されていません。このページでライセンスを追加して構成できます。



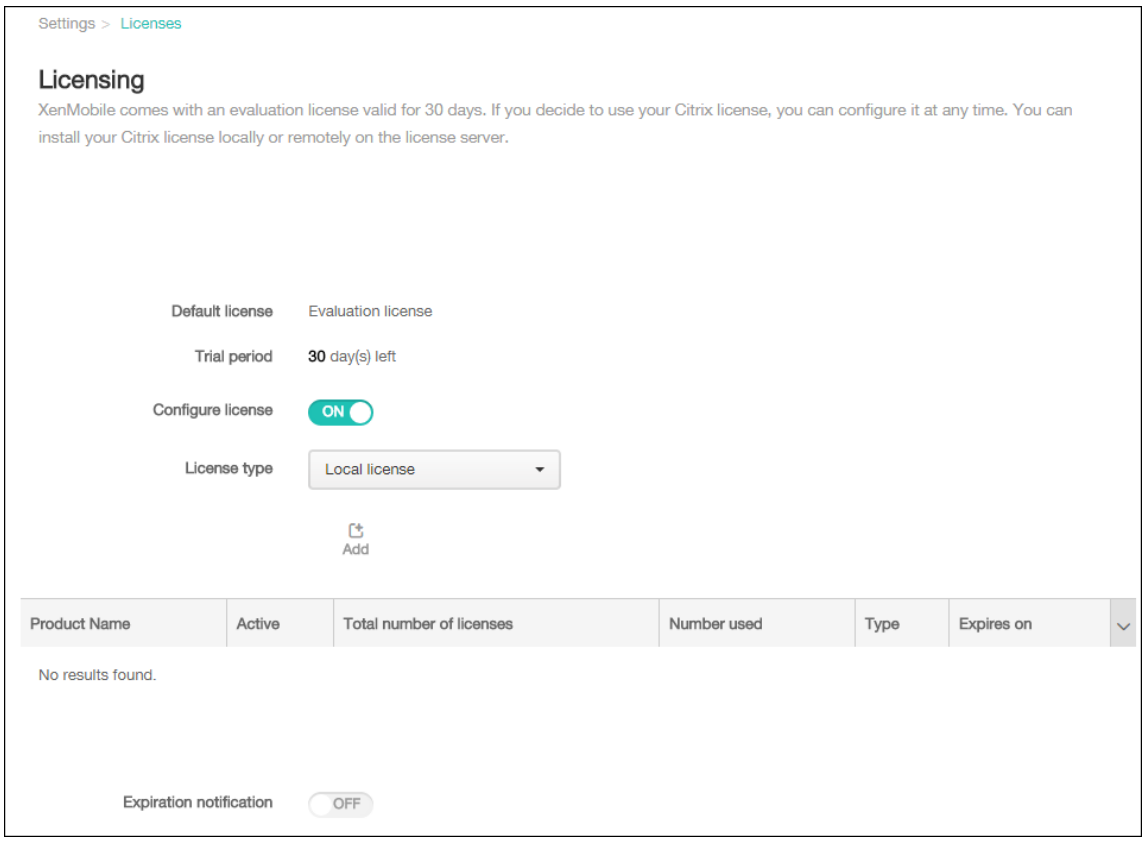
1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［ライセンス］ をクリックします。［ライセンス］ ページが開きます。

ローカルライセンスを追加するには

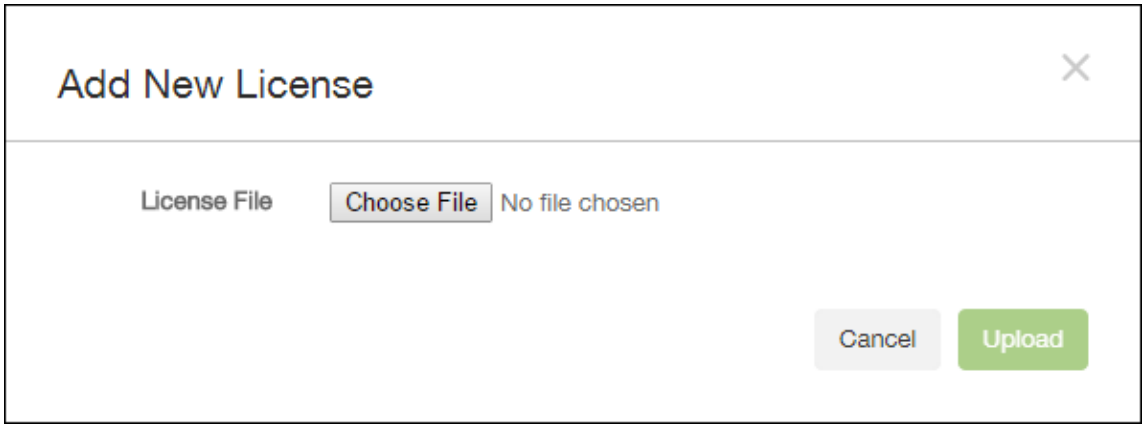
新しいライセンスを追加すると、そのライセンスは表に表示されます。最初に追加したライセンスは自動的にアクティブ化されます。カテゴリ（Enterprise など）および種類が同じライセンスを複数追加した場合、表ではこれらのライセンスが 1 つの行として表示されます。この場合、［ライセンス数合計］ と ［使用数］ に、共通するライセンスの合計数が表示されます。［有効期限］ の日付は、共通するライセンスのうち最も後の有効期限を示します。

ローカルライセンスの管理は、すべて XenMobile コンソールで行います。

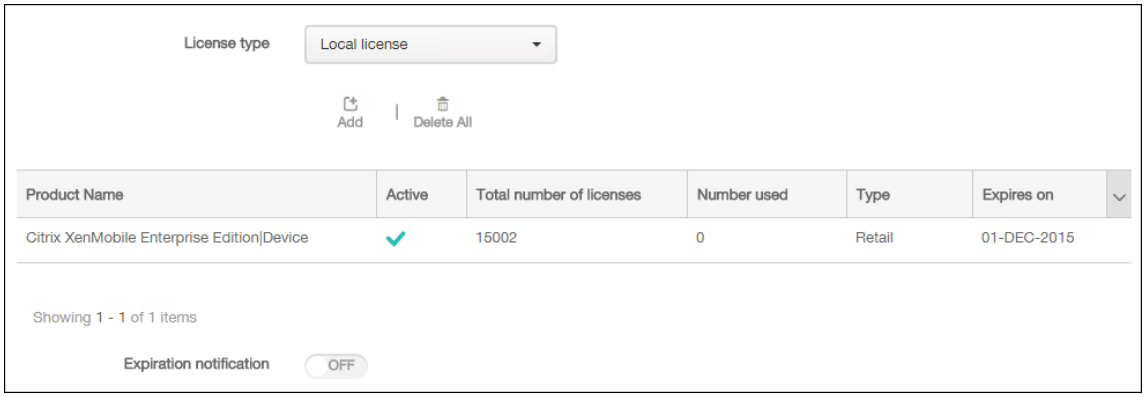
1. ライセンス管理コンソールを介して Simple License Service から、または Citrix.com のアカウントから直接、ライセンスファイルを入手します。詳しくは、Citrix ライセンスのドキュメントを参照してください。
2. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
3. ［ライセンス］ をクリックします。［ライセンス］ ページが開きます。
4. ［ライセンスを構成］ を ［オン］ に設定します。［ライセンスの種類］ ボックス、［追加］ ボタン、［ライセンス］ の表が表示されます。［ライセンス］ 表には、XenMobile で使用したライセンスが含まれています。Citrix ライセンスをまだ追加していない場合、この表は空白です。



5. ［ライセンスの種類］ が ［ローカルライセンス］ に設定されていることを確認して、［追加］ をクリックします。［新しいライセンスの追加］ ダイアログボックスが開きます。



6. ［新しいライセンスの追加］ ダイアログボックスで、［ファイルの選択］ をクリックし、ライセンスファイルの場所を参照します。
7. ［アップロード］ をクリックします。ライセンスがローカルにアップロードされ、表に表示されます。



8. ライセンスが ［ライセンス］ ページの表に表示されたら、ライセンスをアクティブ化します。ライセンスが表の最初にある場合、ライセンスは自動的にアクティブ化されます。

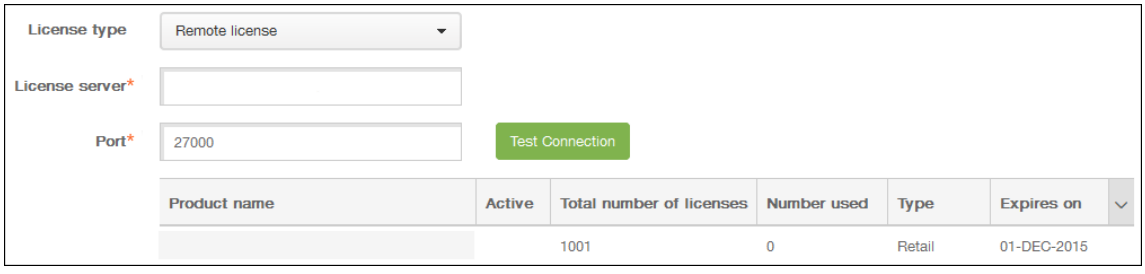
リモートライセンスを追加するには

リモートの Citrix ライセンスサーバーを使用する場合は、Citrix ライセンスサーバーを使用してすべてのライセンス使用状況を管理します。詳しくは、「製品ライセンスの有効化」を参照してください。

1. ライセンスサーバーの証明書を XenMobile Server にインポートします（［設定］ **>** ［証明書］）。
2. デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証によって展開が損なわれる場合は、サーバープロパティ **disable.hostname.verification** を **true** に変更します。このプロパティのデフォルト値は **false** です。

   ホスト名の認証に失敗すると、サーバーログに「VPP サーバーに接続できません：ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」のようなエラーが記録されます。

3. ［ライセンス］ ページで、［ライセンスを構成］ を ［オン］ に設定します。［ライセンスの種類］ ボックス、［追加］ ボタン、［ライセンス］ の表が表示されます。［ライセンス］ 表には、XenMobile で使用したライセンスが含まれています。Citrix ライセンスをまだ追加していない場合、この表は空白です。
4. ［ライセンスの種類］ を ［リモートライセンス］ に設定します。［追加］ ボタンが、［ライセンスサーバー］ フィールドおよび ［ポート］ フィールドと、［接続のテスト］ ボタンに置き換わります。



5. 次の設定を構成します。

   - ライセンスサーバー： リモートライセンスサーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

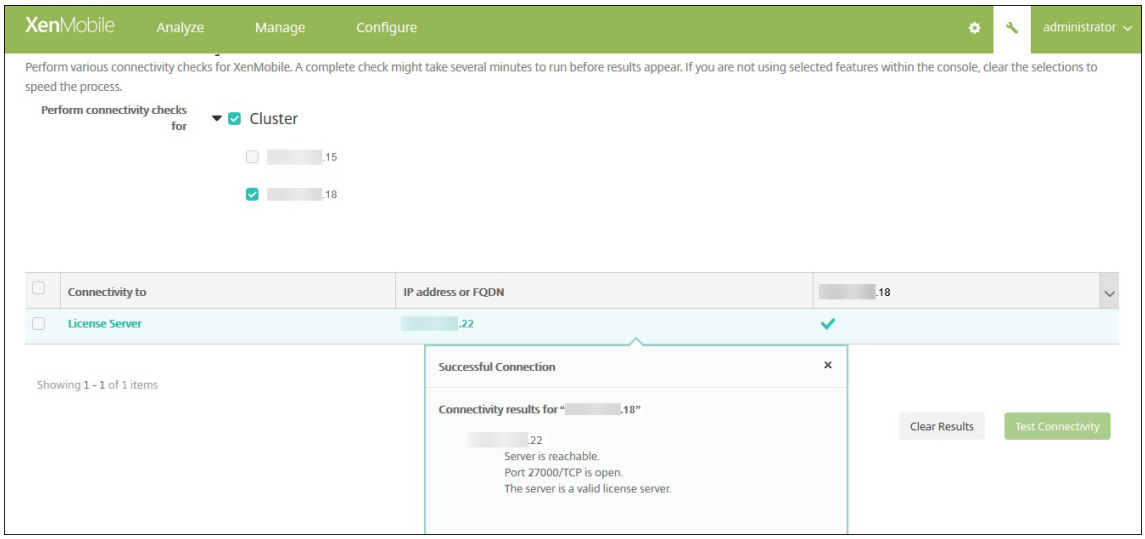
- ポート: デフォルトポートをそのまま使用するか、ライセンスサーバーとの通信に使用するポート番号を入力します。

6. [接続のテスト] をクリックします。接続が成功した場合、XenMobile はライセンスサーバーに接続し、使用可能なライセンスがライセンスの表に表示されます。ライセンスが 1 つのみの場合は、自動的にアクティブ化されます。

   [接続のテスト] をクリックすると、XenMobile で以下のことが確認されます。

   - XenMobile がライセンスサーバーと通信できるか。
   - ライセンスサーバーのライセンスは有効であるか。
   - ライセンスサーバーは XenMobile と互換性があるか。

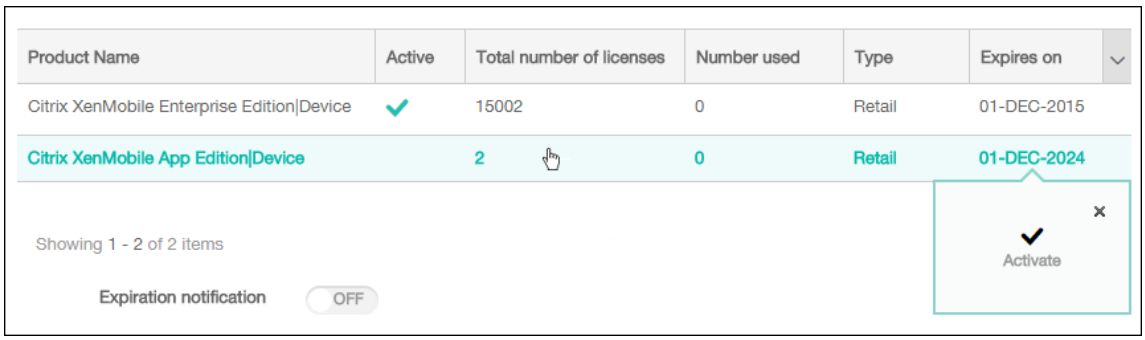
   接続に失敗した場合は、表示されたエラーメッセージを確認し、必要な修正を加えてから、 [接続のテスト] をクリックします。



別のライセンスをアクティブ化するには

複数のライセンスがある場合、アクティブ化するライセンスを選択できます。ただし、アクティブ化できるライセンスは一度に 1 つだけです。

1. [ライセンス] ページのライセンスの表で、アクティブ化するライセンスの行をクリックします。行の横にアクティブ化確認ダイアログが表示されます。



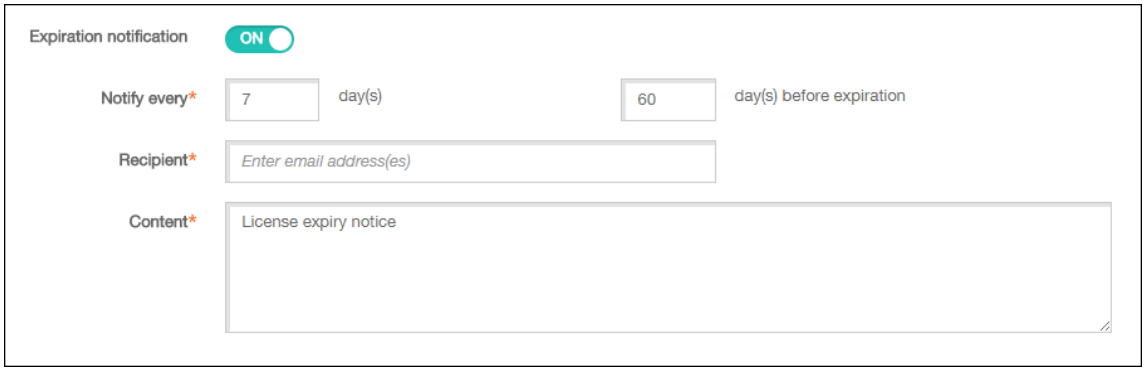
2. [アクティブ化] をクリックします。[アクティブ化] ダイアログボックスが開きます。
3. [アクティブ化] をクリックします。選択したライセンスがアクティブ化されます。

> 重要:
>
> 選択したライセンスをアクティブ化すると、現在アクティブなライセンスは非アクティブになります。

有効期限通知を自動化するには

リモートライセンスまたはローカルライセンスをアクティブ化した後、ライセンスの有効期限が近づいたときに自分または指定先に通知されるように、XenMobile を構成することができます。

1. [ライセンス] ページで、[有効期限についての通知] を [オン] に設定します。通知に関連するフィールドが新たに表示されます。



2. 次の設定を構成します。
   - 通知間隔: 次を入力します:
   - 通知が送信される頻度(**7** 日ごとなど)。
   - 通知の送信を開始する時期(ライセンス有効期限の 60 日前など)。
   - 受信者: 自分またはライセンス担当者のメールアドレスを入力します。
   - コンテンツ: 受信者への有効期限通知メッセージの内容を入力します。
3. [保存] をクリックします。設定に基づいて、[受信者] に入力した受信者への、[コンテンツ] に入力したテキストを含むメールメッセージの送信が開始されます。設定した頻度で通知が送信されます。

FIPS 140-2 への準拠

May 21, 2019

米国立標準技術研究所（National Institute of Standards and Technologies：NIST）が発行している FIPS（Federal Information Processing Standard：米国の情報処理標準）は、セキュリティシステムで使用される暗号化モジュールのセキュリティ要件を規定しています。FIPS 140-2 はこの標準の 2 つ目のバージョンです。NIST 検証済み FIPS 140 モジュールについて詳しくは、NIST Computer Security Resource Centerを参照してください。

> 重要：
>
> - XenMobile FIPS モードは、初回インストール時にのみ有効化できます。
> - HDX アプリが使用されない限り、XenMobile モバイルデバイス管理のみ、XenMobile モバイルアプリ管理のみ、および XenMobile MDM+MAM はすべて FIPS に準拠しています。

iOS では、すべての保存データおよび転送中データの暗号化操作で、OpenSSL および Apple により提供された FIPS 認定済み暗号化モジュールが使用されます。Android では、すべての保存データの暗号化操作およびモバイルデバイスから NetScaler Gateway へのすべての転送中データの暗号化操作で、OpenSSL により提供された FIPS 認定済み暗号化モジュールが使用されます。

サポートされる Windows デバイスでは、モバイルデバイス管理（MDM）のためのすべての保存データおよび転送中データの暗号化操作で、Microsoft によって提供された FIPS 認定済み暗号モジュールが使用されます。

XenMobile MDM のすべての保存データおよび転送中データの暗号化操作で、OpenSSL により提供された FIPS 認定済み暗号化モジュールが使用されます。MDM フローのすべての保存データおよび転送中データは、FIPS 準拠の暗号化モジュールをエンドツーエンドで使用します。そのセキュリティには、モバイルデバイス用の上記の暗号化操作と、モバイルデバイスと NetScaler Gateway 間の暗号化操作が含まれます。

iOS、Android、および Windows モバイルデバイスと NetScaler Gateway 間のすべての転送中データの暗号化操作では、FIPS 認定済み暗号化モジュールが使用されます。XenMobile は、認定済み FIPS モジュール装備の DMZ がホストする NetScaler FIPS Edition アプライアンスを使用し、これらのデータを保護します。詳しくは、NetScaler のドキュメントの「FIPS」を参照してください。

MDX Vault は、OpenSSL によって提供された FIPS 認定済み暗号化モジュールを使って、iOS デバイスおよび Android デバイス上の、MDX でラップされたアプリおよび割り当てられた保存データを暗号化します。

各ケースで使用される特定のモジュールを含む XenMobile FIPS 140-2 の完全なコンプライアンスステートメントについては、Citrix 担当者に問い合わせてください。

言語サポート

August 22, 2019

業務用モバイルアプリおよび XenMobile コンソールは英語以外の言語での使用にも適応しています。サポートには、アプリがユーザーの優先言語にローカライズされていない場合でも、英語以外の文字およびキーボード入力が含まれます。全シトリックス製品のグローバル化サポートについて詳しくは、https://support.citrix.com/article/CTX119253を参照してください。

ここでは、最新リリースの XenMobile でサポートされる言語を示します。

XenMobile コンソールおよび Self Help Portal

- フランス語
- ドイツ語
- スペイン語
- 日本語
- 韓国語
- ポルトガル語
- 簡体字中国語

業務用モバイルアプリ

☒ は、その個別言語でアプリケーションを使用できることを示しています。

iOS または Android

言語	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
日本語	☒	☒	☒	☒	☒	☒
簡体字中国語	☒	☒	☒	☒	☒	☒
繁体字中国語	☒	☒	☒	☒	☒	☒
フランス語	☒	☒	☒	☒	☒	☒
ドイツ語	☒	☒	☒	☒	☒	☒
スペイン語	☒	☒	☒	☒	☒	☒
韓国語	☒	☒	☒	☒	☒	☒
ポルトガル語	☒	☒	☒	☒	☒	☒
オランダ語	☒	☒	☒	☒	☒	☒
イタリア語	☒	☒	☒	☒	☒	☒
デンマーク語	☒	☒	☒	☒	☒	☒

言語	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
スウェーデン語	☒	☒	☒	☒	☒	☒
ヘブライ語	☒	☒	☒	☒	☒	iOS 9 のみ
アラビア語	☒	☒	☒	☒	☒	☒
ロシア語	☒	☒	☒	☒	☒	☒
トルコ語	☒	☒	Android のみ	-	-	-

Windows

言語	Secure Hub	Secure Mail	Secure Web
フランス語	☒	☒	☒
ドイツ語	☒	☒	☒
スペイン語	☒	☒	☒
イタリア語	☒	☒	☒
デンマーク語	☒	☒	☒
スウェーデン語	☒	☒	☒

右書きの言語のサポート

次の表は、XenMobile アプリの機能の概要です。☒ は、プラットフォームごとに利用可能な機能です。Windows デバイスでは、右から左へと記述する言語のサポートは使用できません。

アプリ	iOS	Android
Secure Hub	☒	☒
Secure Mail	☒	☒
Secure Web	☒	☒
Secure Tasks	☒	☒
Secure Notes	☒	☒
QuickEdit	☒	☒

インストールと構成

January 10, 2020

はじめに

次のチェックリストを使用して、XenMobile をオンプレミスでインストールするための前提条件と設定を記録できます。各タスクまたは注には、要件が適用されるコンポーネントまたは機能を示す列があります。

XenMobile 展開を計画する場合は、多くの検討事項があります。完全な XenMobile 環境の推奨事項、よくある質問、およびユースケースについては、『XenMobile 展開ハンドブック』を参照してください。

インストール手順については、この記事で後述している「XenMobile のインストール」を参照してください。

インストール前チェックリスト

基本的なネットワーク接続

以下は XenMobile ソリューションに必要なネットワーク設定です。

前提条件または設定	コンポーネントまたは機能	設定の記録
リモートユーザーが接続する完全修飾ドメイン名 (Fully Qualified Domain Name: FQDN) を記録します。	XenMobile と NetScaler Gateway	
パブリックおよびローカルの IP アドレスを書き留めます。		

前提条件または設定	コンポーネントまたは機能	設定の記録	
ファイアウォールを設定してネットワークアドレス変換（NAT）を設定するには、これらの IP アドレスが必要です。	XenMobile および NetScaler Gateway		
サブネットマスクを書き留めてください。	XenMobile および NetScaler Gateway		
DNS の IP アドレスに注意してください。	XenMobile と NetScaler Gateway		
WINS サーバーの IP アドレスを書き留めます（該当する場合）。	NetScaler Gateway		
NetScaler Gateway ホスト名を特定して書き留めます。	NetScaler Gateway	この項目は FQDN ではありません。FQDN は、仮想サーバーにバインドされ、ユーザーが接続する署名されたサーバー証明書に含まれます。NetScaler Gateway のセットアップウィザードを使用してホスト名を設定できます。	NetScaler Gateway

前提条件または設定	コンポーネントまたは機能	設定の記録	
XenMobile の IP アドレスを書き留めます。 XenMobile のインスタンスを 1 つインストールする場合は、IP アドレスを 1 つ予約します。クラスタを構成する場合は、必要なすべての IP アドレスを書き留めます。	XenMobile		
NetScaler Gateway で設定された 1 つのパブリック IP アドレス	NetScaler Gateway		
NetScaler Gateway 用の 1 つの外部 DNS エントリ	NetScaler Gateway		
Web プロキシサーバーの IP アドレス、ポート、プロキシホストリスト、および管理者のユーザー名とパスワードを書き留めます。ネットワークにプロキシサーバーを展開する場合は、これらの設定はオプションです（該当する場合）。	NetScaler Gateway	Web プロキシのユーザー名を設定するときは、sAMAccountName または UPN（User Principal Name）のいずれかを使用できます。	XenMobile と NetScaler Gateway
既定のゲートウェイ IP アドレスを書き留めます。	XenMobile と NetScaler Gateway		

前提条件または設定	コンポーネントまたは機能	設定の記録
システム IP（NSIP）アドレスとサブネットマスクを書き留めます。	NetScaler Gateway	
サブネット IP（SNIP）アドレスとサブネットマスクを書き留めます。	NetScaler Gateway	
証明書の NetScaler Gateway 仮想サーバーの IP アドレスと FQDN を書き留めます。複数の仮想サーバーを構成するには、証明書のすべての仮想 IP アドレスと FQDN を書き留めます。	NetScaler Gateway	

前提条件または設定	コンポーネントまたは機能	設定の記録
ユーザーが NetScaler Gateway を介してアクセスできる内部ネットワークに注意してください。例：10.10.0.0/24 次のような場合にユーザーがアクセスする必要があるすべての内部ネットワークとネットワークセグメントを入力します：分割トンネリングがオンに設定されていて、ユーザーが Secure Hub または NetScaler Gateway Plug-in を使用して接続する場合。	NetScaler Gateway	
XenMobile Server、NetScaler Gateway、外部 Microsoft SQL Server、および DNS サーバー間のネットワーク接続が可能であることを確認してください。	XenMobile と NetScaler Gateway	

ライセンス

XenMobile では、NetScaler Gateway および XenMobile のライセンスオプションを購入する必要があります。Citrix ライセンスサーバーについて詳しくは、「The Citrix Licensing System」を参照してください。

前提要件	コンポーネント	場所を記録します。
ユニバーサルライセンスを Citrix Web サイトから入手します。詳しくは、NetScaler Gateway のドキュメントの「Licensing」を参照してください。	NetScaler Gateway、XenMobile、および Citrix ライセンスサーバー	

証明書

XenMobile および NetScaler Gateway は、ほかのシトリックス製品およびユーザーデバイスのアプリと接続するために、証明書が必要です。詳しくは、XenMobile のドキュメントの「証明書および認証」を参照してください。

前提要件	コンポーネント	注
必要な証明書を入手してインストールします。	XenMobile と NetScalerGateway	

ポート

XenMobile コンポーネントと通信できるように、ポートを開きます。

前提要件	コンポーネント	注
XenMobile 用にポートを開きます。	XenMobile と NetScaler Gateway	

データベース

XenMobile では、データベース接続を構成する必要があります。XenMobile リポジトリでは、「システム要件と互換性」に記載された以下のサポート対象バージョンのいずれかで稼動している Microsoft SQL Server データベースが必要です。Citrix では、Microsoft SQL をリモートで使用することをお勧めします。PostgreSQL は XenMobile に含まれます。PostgreSQL はテスト環境でのみローカルまたはリモートで使用する使用します。

デフォルトでは、XenMobile は jTDS データベースドライバーを使用します。XenMobile Server のオンプレミスインストールに Microsoft JDBC ドライバーを使用するには、「SQL Server のドライバー」を参照してください。

前提要件	コンポーネント	注
Microsoft SQL Server の IP アドレスとポート。XenMobile で使用される SQL Server のサービスアカウントに、DBcreator 役割の権限があることを確認します。	XenMobile	

Active Directory の設定

前提要件	コンポーネント	注
Active Directory のプライマリサーバーおよびセカンダリサーバーの IP アドレスおよびポートを記録します。ポート 636 を使用する場合は、CA から取得したルート証明書を XenMobile にインストールし、[セキュア接続を使用] オプションを [はい] に変更します。	XenMobile と NetScaler Gateway	
Active Directory ドメイン名を記録します。	XenMobile と NetScaler Gateway	
Active Directory サービスアカウントには、ユーザー ID、パスワード、およびドメインエイリアスが必要です。		
Active Directory サービスアカウントは、XenMobile が Active Directory に照会するために使用するアカウントです。	XenMobile と NetScaler Gateway	

前提要件	コンポーネント	注
ユーザーが存在するディレクトリレベルであるユーザーベース DN に注意してください。例: `cn=users,dc=ace,dc=com`。NetScaler Gateway および XenMobile は、User Base DN を使用して Active Directory にクエリします。	XenMobile と NetScaler Gateway	
グループが存在するディレクトリレベルであるグループベース DN に注意してください。NetScaler Gateway および XenMobile はこの DN を使用して Active Directory にクエリを行います。	XenMobile と NetScaler Gateway	

XenMobile と **NetScaler Gateway** の間の接続

前提要件	コンポーネント	設定の記録
XenMobile のホスト名を記録します。	XenMobile	
XenMobile の FQDN または IP アドレスを記録します。	XenMobile	
ユーザーがアクセスできるアプリを確認します。	NetScaler Gateway	
コールバック URL を記録します。	XenMobile	

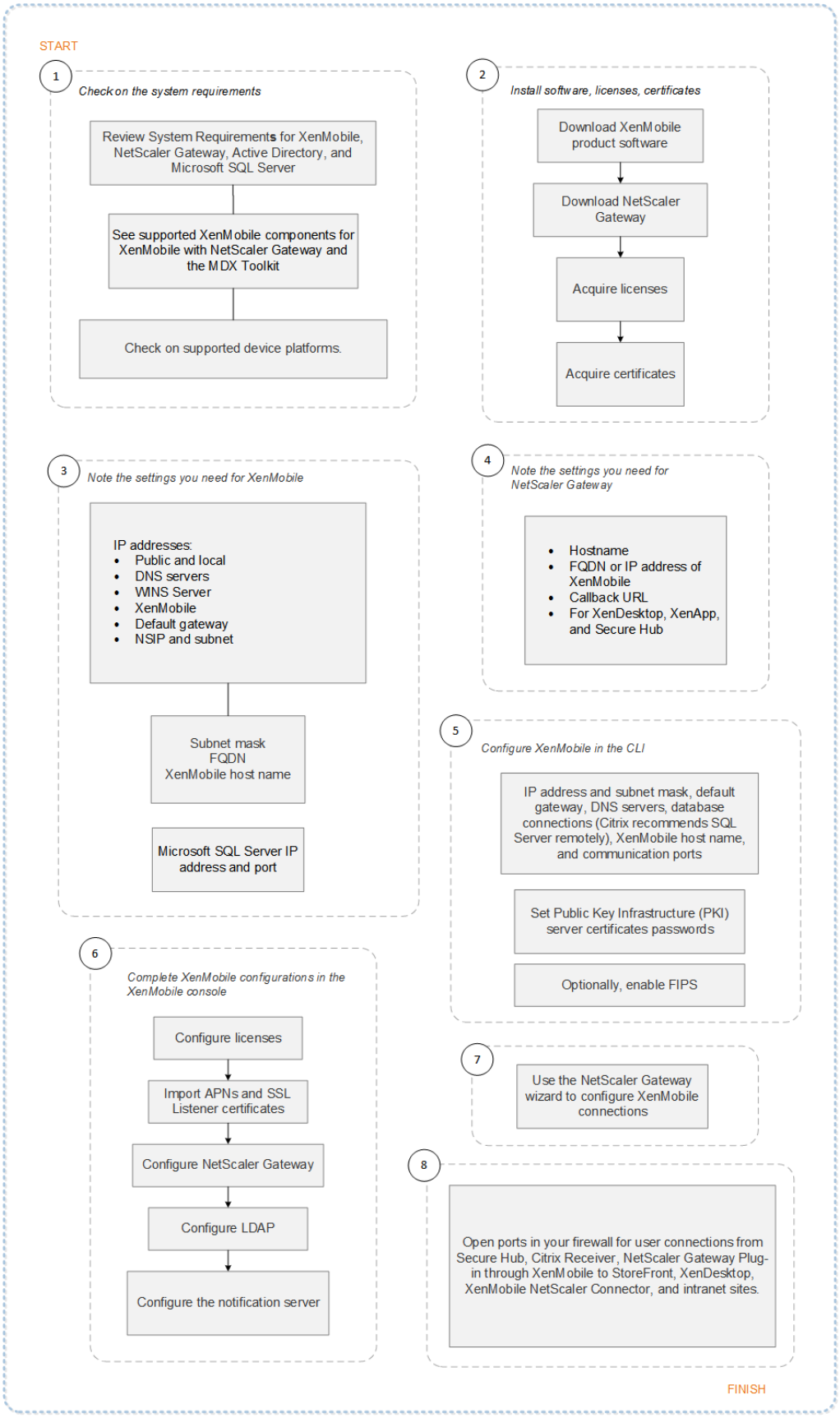
ユーザー接続: **Citrix Virtual Apps and Desktops** および **Citrix Secure Hub** へのアクセス

NetScaler の Quick Configuration ウィザードを使用して、XenMobile と NetScaler Gateway の間、XenMobile と Secure Hub の間の接続設定を構成することをお勧めします。第 2 の仮想サーバーを作成して、Citrix Receiver および Web ブラウザーからのユーザー接続を有効にします。これらは、Virtual Apps and Desktops の Windows ベースのアプリケーションおよび仮想デスクトップへの接続です。また、NetScaler の Quick Configuration ウィザードを使用して、これらの設定を構成することをお勧めします。

前提要件	コンポーネント	設定の記録
NetScaler Gateway のホスト名および外部 URL を記録します。外部 URL は、ユーザーが接続する Web アドレスです。	XenMobile	
NetScaler Gateway コールバック URL を記録します。	XenMobile	
仮想サーバーの IP アドレスおよびサブネットマスクを記録します。	NetScaler Gateway	
Program Neighborhood エージェントまたは Virtual Apps and Desktops サイトのパスを記録します。	NetScaler Gateway と XenMobile	
Secure Ticket Authority（STA）を実行している Citrix Virtual Apps and Desktops サーバーの FQDN または IP アドレスを記録します（ICA コネクションの場合のみ）。	NetScaler Gateway	
XenMobile のパブリック FQDN を記録します。	NetScaler Gateway	
Secure Hub のパブリック FQDN を記録します。	NetScaler Gateway	

XenMobile 展開のフローチャート

このフローチャートは、XenMobile を展開する場合の主な手順を示しています。各手順のトピックのリンクは図に従っています。



1: システム要件と互換性

2: インストールと構成

3、4: インストール前のチェックリスト（この記事）

5: コマンドプロンプトウィンドウでの XenMobile の構成（この記事）

6: Web ブラウザーでの XenMobile の構成（この記事）

7: XenMobile 環境の設定の構成

8: ポート要件

XenMobile のインストール

XenMobile 仮想マシン（Virtual Machine: VM）は、Citrix XenServer、VMware ESXi、または Microsoft Hyper-V で動作します。XenCenter または vSphere の管理コンソールを使用して、XenMobile をインストールできます。

> 注:
>
> XenMobile はハイパーバイザーの時刻を使用するので、NTP サーバーまたは手動による構成を使用して、ハイパーバイザーの時刻が正しく構成されていることを確認してください。XenMobile の時間とハイパーバイザーの同期でタイムゾーンの問題が発生する場合、XenMobile が NTP サーバーを参照するようにして、これを回避できます。このためには、「コマンドラインインターフェイスオプション」に説明されているように、XenMobile CLI を使用します。

XenServer または **VMware ESXi** の前提条件。XenMobile を XenServer または VMware ESXi にインストールする前に、以下を実行する必要があります。詳しくは、XenServerまたはVMwareのドキュメントを参照してください。

- 十分なハードウェアリソースを持つコンピューターに XenServer または VMware ESXi をインストールします。
- 別のコンピューターに XenCenter または vSphere をインストールします。XenCenter または vSphere をインストールしたコンピューターから、XenServer または VMware ESXi ホストにネットワーク経由で接続します。

Hyper-V の前提条件。XenMobile を Hyper-V にインストールする前に、以下を実行する必要があります。詳しくは、Hyper-Vのドキュメントを参照してください。

- 十分なシステムリソースのあるコンピューターに、Hyper-V と役割を有効にした Windows Server 2008 R2、Windows Server 2012、または Windows Server 2012 R2 をインストールします。Hyper-V の役割をインストールするときは、仮想ネットワークを作成するために Hyper-V で使用されるサーバー上の NIC を必ず指定してください。一部の NIC は、ホスト用に確保できます。
- Virtual Machines/<*build-specific UUID*>.xml ファイルを削除します。
- Legacy/<*build-specific UUID*>.exp ファイルを Virtual Machines に移動します。

Windows Server 2008 R2 または Windows Server 2012 をインストールする場合は、以下の操作を行います:

VM 構成を表す Hyper-V マニフェストファイルには 2 つの異なるバージョン（.exp と.xml）があるため、これらの手順は必須です。Windows Server 2008 R2 と Windows Server 2012 のリリースは.exp のみをサポートします。これらのリリースでは、インストール前に.exp マニフェストファイルのみが配置されている必要があります。

Windows Server 2012 R2 では、これらの追加手順は必要ありません。

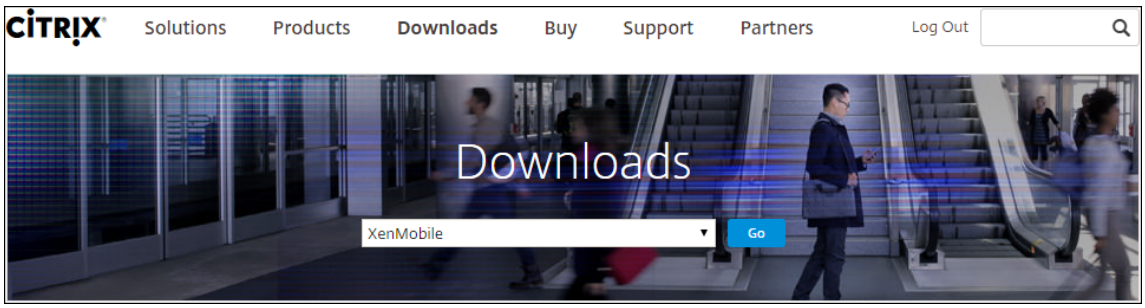
FIPS 140-2 モード。XenMobile Server を FIPS モードでインストールしようとする場合は、「XenMobile での FIPS の構成」で説明されている一連の前提条件グループを完了させます。

XenMobile 製品ソフトウェアのダウンロード

製品ソフトウェアは、シトリックス Web サイトからダウンロードできます。サイトにログオンし、次に [Downloads] リンクを使用してダウンロードするソフトウェアを含むページに移動します。

XenMobile のソフトウェアをダウンロードするには

1. シトリックス Web サイトにアクセスします。
2. [Search] ボックスの横の ［**Log On**］ をクリックしてアカウントにログオンします。
3. ［**Downloads**］ タブをクリックします。
4. [Downloads] ページの製品一覧で、 ［**XenMobile**］ を選択します。



5. ［**Go**］ をクリックします。[XenMobile] ページが開きます。
6. ［**XenMobile Server**］ を展開します。
7. ［**Product Software**］ を展開します。
8. ［**XenMobile Server 10**］ をクリックします。
9. ［**Jump to Download**］ メニューをクリックし、XenMobile をインストールするために使用する適切な仮想イメージを選択します。または、ページを下方向にスクロールして、インストールするイメージの ［**Download File**］ ボタンを見つけます。
10. 画面の指示に従ってソフトウェアをダウンロードしてください。

NetScaler Gateway のソフトウェアをダウンロードするには

NetScaler Gateway 仮想アプライアンスや、既存の NetScaler Gateway アプライアンスのソフトウェアアップグレードをダウンロードするには、以下の手順に従います。

1. シトリックス Web サイトにアクセスします。
2. Citrix の Web サイトにまだログオンしていない場合は、［Search］ボックスの横の ［**Log On**］ をクリックしてアカウントにログオンします。
3. ［**Downloads**］ タブをクリックします。
4. ［Downloads］ページの製品一覧で、 ［**NetScaler Gateway**］ を選択します。
5. ［**Go**］ をクリックします。［NetScaler Gateway］ページが開きます。
6. ［NetScaler Gateway］ページで、実行する NetScaler Gateway のバージョンを展開します。
7. ［**Firmware**］ の下で、ダウンロードするアプライアンスソフトウェアのバージョンをクリックします。

   > 注:
   >
   > ここで ［**Virtual Appliances**］ をクリックして NetScaler VPX をダウンロードすることもできます。この場合、対象のハイパーバイザーを選択するためのページが開きます。

8. ダウンロードするアプライアンスソフトウェアのバージョンをクリックします。
9. ダウンロードするバージョンのアプライアンスソフトウェアページで、適切な仮想アプライアンスの ［ダウンロード］ をクリックします。
10. 画面の指示に従ってソフトウェアをダウンロードしてください。

初回使用時の **XenMobile** の構成

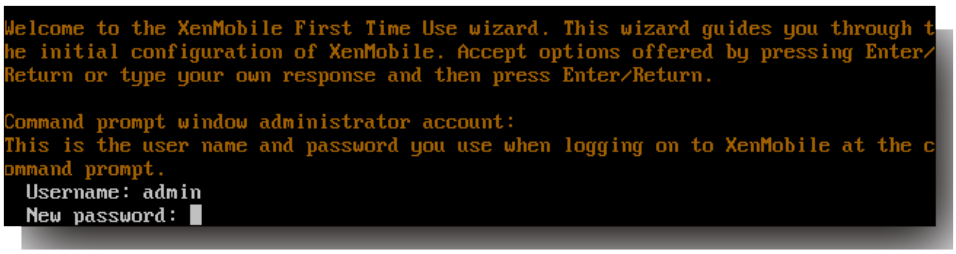
1. XenMobile の IP アドレスやサブネットマスク、デフォルトゲートウェイ、DNS サーバーなどの設定を構成するには：XenCenter または vSphere のコマンドラインコンソールを使用します。

   > 注:
   >
   > vSphere Web クライアントを使用する場合、［**Customize**］テンプレートページで OVF テンプレートを展開しながらネットワークプロパティを構成しないことをお勧めします。それにより、高可用性構成で、2 番目の XenMobile 仮想マシンを複製してから再起動する場合に発生する IP アドレスの問題を回避できます。

2. XenMobile 管理コンソールに、XenMobile Server の完全修飾ドメイン名またはノードの IP アドレスのみを使用してアクセスします。
3. ログオンし、初回ログオン画面の手順に従います。

コマンドプロンプトウィンドウでの **XenMobile** の構成

1. XenMobile 仮想マシンを Citrix XenServer、Microsoft Hyper-V、または VMware ESXi にインポートします。詳しくは、XenServer、Hyper-V、またはVMwareのドキュメントを参照してください。
2. ハイパーバイザーで、インポートした XenMobile 仮想マシンを選択してコマンドプロンプトビューを起動します。詳しくは、ハイパーバイザーのドキュメントを参照してください。
3. ハイパーバイザーのコンソールページから、コマンドプロンプトウィンドウで XenMobile の管理者のユーザー名とパスワードを入力して管理者アカウントを作成します。

   > 重要：
   >
   > コマンドプロンプトで作成する管理者アカウント、公開キー基盤（PKI）サーバー証明書、および FIPS のパスワードを作成または変更すると、XenMobile では以下の規則を Active Directory ユーザーを除くすべてのユーザーに適用します。Active Directory ユーザーのパスワードは XenMobile の外部で管理されます。
   >
   > - パスワードは 8 文字以上でなければなりません。
   > - パスワードは、以下の複雑度の条件のうち 3 つ以上を満たす必要があります。
   >   - 大文字（A ～ Z）
   >   - 小文字（a ～ z）
   >   - 数字（0 ～ 9）
   >   - 特殊文字（! ## $ %など）
   >
   > 
   >
   >
   > 新しいパスワードを入力するとき、アスタリスクなどの文字は表示されません。

4. 次のネットワーク情報を入力してから、「**y**」を入力して設定をコミットします：

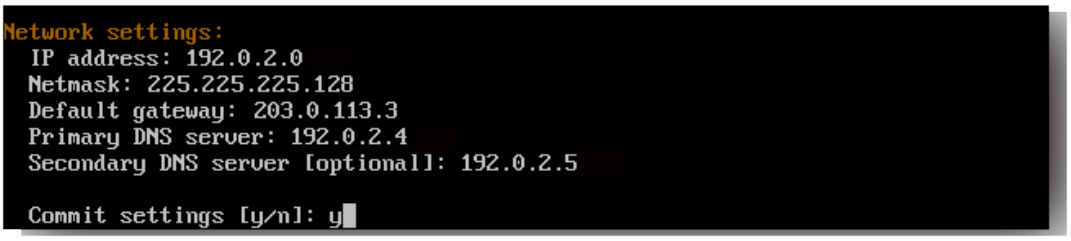
   a) XenMobile サーバーの IP アドレス

   b) ネットマスク

   c) デフォルトゲートウェイ（DMZ 内のデフォルトゲートウェイの IP アドレス）

   d) プライマリ DNS サーバー（DNS サーバーの IP アドレス）

   e) セカンダリ DNS サーバー（オプション）



> 注:
>
> この画像および次の画像に示されているアドレスは機能しておらず、例として提供されています。

5. 「**y**」を入力して、セキュリティを高めるためにランダムな暗号化パスフレーズを生成するか、「**n**」を入力して独自のパスフレーズを入力します。「**y**」を入力してランダムなパスフレーズを生成することをお勧めします。

   このパスフレーズは、機密データを保護するために使用される暗号化キーの保護手段の 1 つとして使用されます。サーバーのファイルシステムに保存されたパスフレーズのハッシュが、データの暗号化と復号化でキーを取得するときに使用されます。このパスフレーズを表示することはできません。

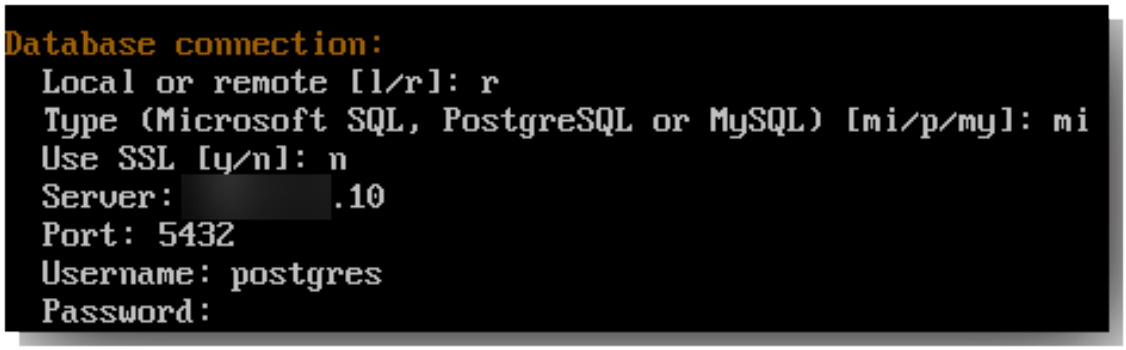
   > 注:
   >
   > 環境を拡張して追加のサーバーを構成する場合は、独自のパスフレーズを指定します。ランダムなパスフレーズを選択した場合、そのパスフレーズは表示されません。

6. オプションで、連邦情報処理標準（FIPS）を有効にします。FIPS について詳しくは、「FIPS」を参照してください。また、「XenMobile での FIPS の構成」で説明されている一連の前提条件を完了させる必要があります。

7. 以下の情報を入力してデータベース接続を構成します。

   - ご使用のデータベースは、ローカルでもリモートでもかまいません。ローカルの場合は「**l**」、リモートの場合は「**r**」を入力します。

- データベースの種類を選択します。Microsoft SQL の場合は「**ml**」と入力し、PostgreSQL の場合は「**p**」を入力します。

  > 重要：
  >
  > – Citrix では、Microsoft SQL をリモートで使用することをお勧めします。PostgreSQL は XenMobile に含まれます。PostgreSQL はテスト環境でのみローカルまたはリモートで使用する使用します。
  > – データベースの移行はサポートされていません。テスト環境で作成したデータベースを実稼働環境に移行することはできません。

- 通常、「**y**」を使用してデータベースで SSL 認証を使用します。
- XenMobile のあるサーバーのデータベースサーバーの完全修飾ドメイン名（FQDN）を入力します。この 1 つのホストサーバーは、デバイス管理サービスとアプリ管理サービスの両方を提供します。
- データベースのポート番号がデフォルトのポート番号と異なる場合は入力します。Microsoft SQL のデフォルトポートは 1433 で、PostgreSQL のデフォルトポートは 5432 です。
- データベース管理者のユーザー名を入力します。
- データベース管理者のパスワードを入力します。
- データベース名を入力します。
- **Enter** キーを押してデータベース設定を確定します。

8. 必要に応じて、「**y**」を入力して XenMobile ノードまたはインスタンスのクラスタ化を有効にします。

   > 重要：
   >
   > XenMobile クラスタを有効にする場合は、クラスタメンバー間のリアルタイム通信を有効にするために、システム構成を完了した後でポート 80 を必ず開放してください。すべてのクラスタノードでこの設定を完了します。

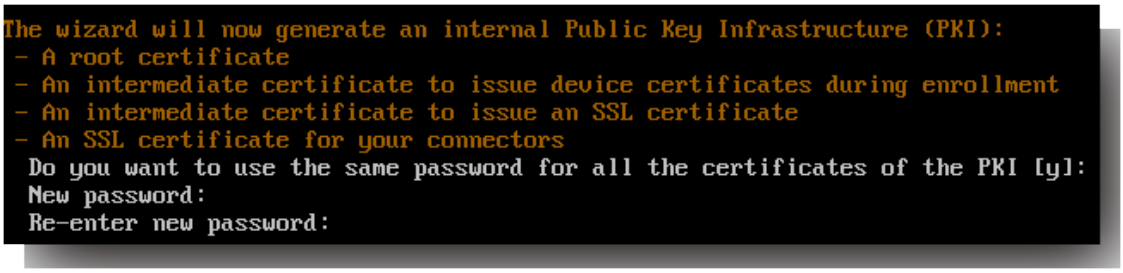
9. XenMobile サーバーの完全修飾ドメイン名（FQDN）を入力します。

10. **Enter** キーを押して設定を確定します。
11. 通信ポートを指定します。ポートおよびその使用方法について詳しくは、「ポート要件」を参照してください。

    > 注：
    >
    > **Enter** キー（Mac の場合は Return キー）を押して、デフォルトポートをそのまま使用します。

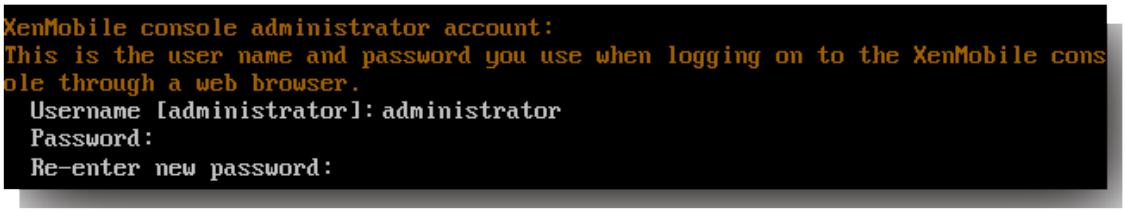
12. 初めて XenMobile をインストールしているので、以前の XenMobile リリースからのアップグレードに関する次の質問をスキップします。
13. 公開キー基盤（PKI）証明書それぞれに同じパスワードを使用する場合は「**y**」を入力します。XenMobile PKI 機能について詳しくは、「証明書のアップロード」を参照してください。



> 重要:
>
> XenMobile のノード（インスタンス）をまとめてクラスター化する場合は、後続ノードで同じパスワードを入力する必要があります。

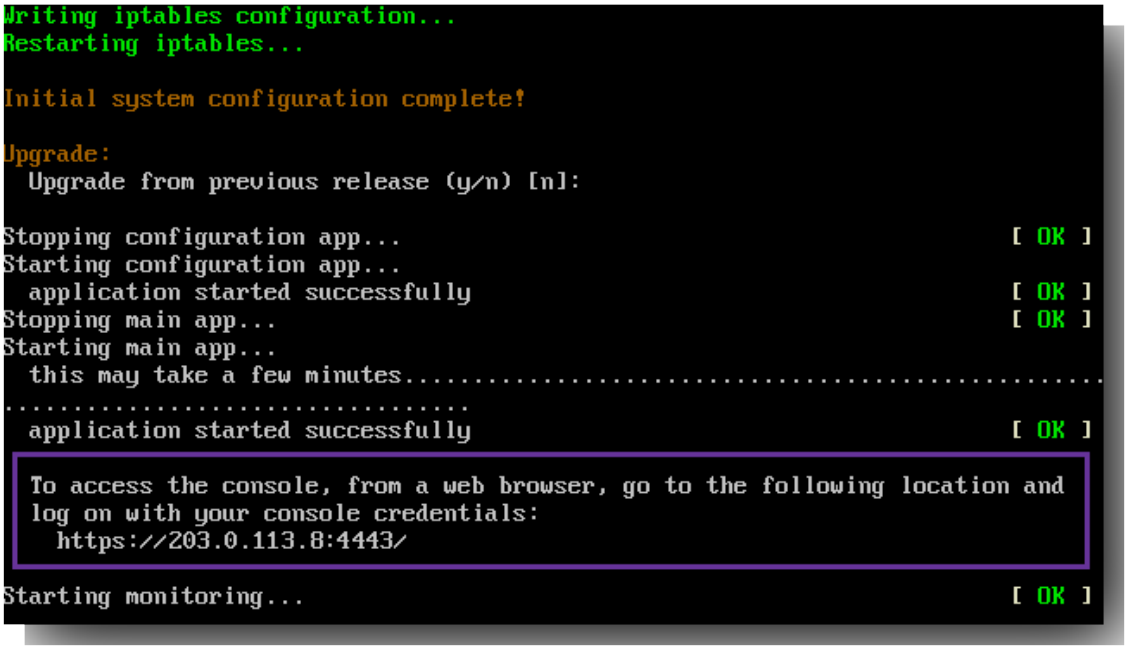
14. 新しいパスワードを入力し、確認のために新しいパスワードを再入力します。

    新しいパスワードを入力するとき、アスタリスクなどの文字は表示されません。
15. **Enter** キーを押して設定を確定します。
16. Web ブラウザーを使用して XenMobile コンソールにログオンするための管理者アカウントを作成します。後で使用するために、これらの資格情報を必ず記録してください。



> 注:
>
> 新しいパスワードを入力するとき、アスタリスクなどの文字は表示されません。

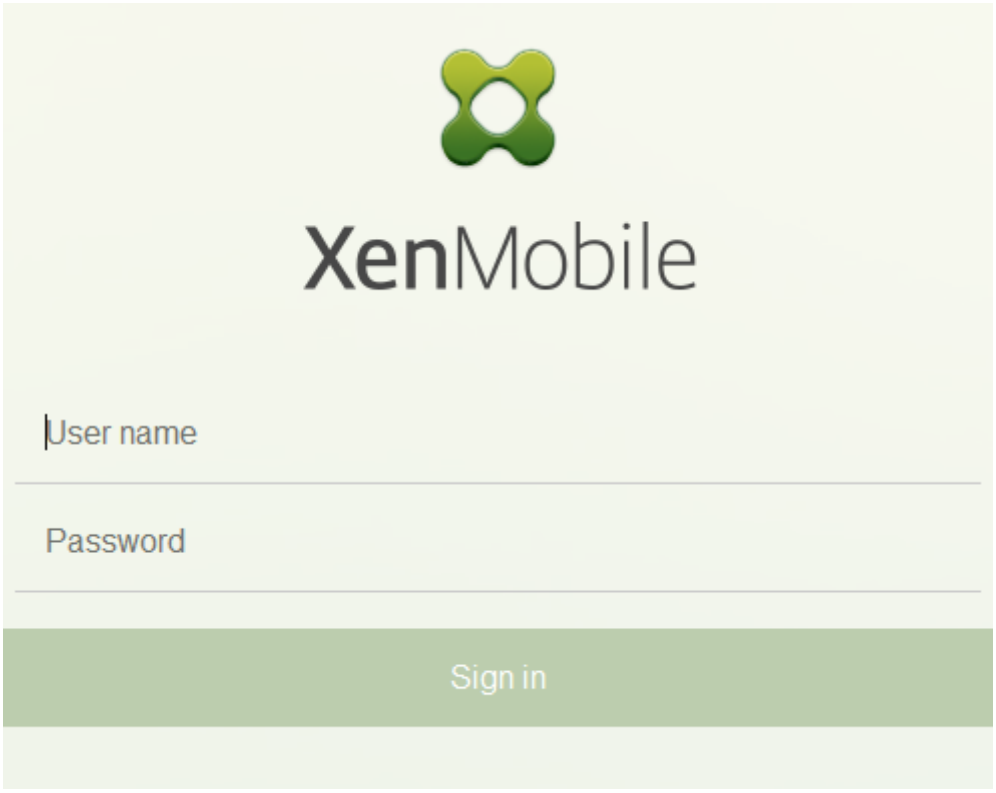
17. **Enter** キーを押して設定を確定します。最初のシステム構成が保存されます。
18. アップグレードかどうかを確認するメッセージが表示されたら、新規インストールであるため、「**n**」を入力します。
19. 画面に表示された URL 全体をコピーして、この XenMobile 初期構成を Web ブラウザーで続行します。



Web ブラウザーでの XenMobile の構成

ハイパーバイザーのコマンドプロンプトウィンドウで XenMobile 構成の最初の部分が完了した後、Web ブラウザーでその処理を完了します。

1. Web ブラウザーで、コマンドプロンプトウィンドウでの構成の最後に示された場所へ移動します。
2. コマンドプロンプトウィンドウで作成した、XenMobile コンソール管理者アカウントのユーザー名とパスワードを入力します。



3. ［はじめに］ページで ［開始］ をクリックします。［ライセンス］ ページが開きます。
4. ライセンスを構成します。ライセンスをアップロードしない場合、30 日間有効な評価版ライセンスを使用します。ライセンスの追加と構成、および有効期限切れ通知の構成について詳しくは、「ライセンス」を参照してください。

   > 重要：
   >
   > XenMobile のクラスターノード（インスタンス）を追加して XenMobile クラスタリングを使用する場合は、リモートサーバー上で Citrix ライセンスサーバーを使用する必要があります。

5. ［証明書］ ページで ［インポート］ をクリックします。［インポート］ダイアログボックスが開きます。
6. APN と SSL リスナー証明書をインポートします。iOS のデバイス管理には APN 証明書が必要です。証明書の取り扱いについて詳しくは、「証明書」を参照してください。

   > 注：
   >
   > この手順にはサーバーの再起動が伴います。

7. 環境が該当する場合は、NetScaler Gateway を構成します。NetScaler Gateway の構成について詳しくは、「NetScaler Gateway と XenMobile」および「XenMobile 環境の設定の構成」を参照してください。

   > 注：
   >
   > - NetScaler Gateway は、内部ネットワーク（またはイントラネット）の境界で展開できます。展開後、内部ネットワークに存在するサーバー、アプリ、その他のネットワークリソースに安全にア

> クセスできる単一のポイントが提供されます。この展開では、すべてのリモートユーザーが、内部ネットワークの任意のリソースにアクセスする前に、NetScaler Gateway に接続する必要があります。
> - NetScaler Gateway はオプションの設定ですが、ページでのデータ入力後にそのページから移動するには、必須フィールドを消去するか入力する必要があります。

8. Active Directory からのユーザーとグループにアクセスするため、LDAP 構成を完了します。LDAP 接続の設定について詳しくは、「LDAP 構成」を参照してください。
9. 通知サーバーを構成して、ユーザーにメッセージを送信できるようにします。通知サーバー構成について詳しくは、「通知」を参照してください。

Post-requisite。XenMobile Server を再起動して、証明書を有効にします。

XenMobile での FIPS の構成

October 25, 2019

XenMobile の米国の情報処理標準（FIPS：Federal Information Processing Standards）モードは、すべての暗号化操作に対して FIPS 140-2 証明済みライブラリのみを使用して、米国政府のカスタマーをサポートします。XenMobile サーバーを FIPS モードでインストールすると、すべての XenMobile クライアントとサーバーのデータを FIPS 140-2 に完全に準拠させることができます。このコンプライアンスは、静止データとやり取りされるデータに適用されます。

XenMobile サーバーを FIPS モードでインストールする前に、次の前提条件を完了させます。

- XenMobile データベースには外部の SQL Server 2012 または SQL Server 2014 を使用します。また SQL Server をセキュア SSL 通信用に構成する必要があります。SQL Server への安全な SSL 通信の構成については、「SQL Server Books Online」を参照してください。
- セキュア SSL 通信を実行するには、SQL Server に既知の CA（証明機関）からの信頼される SSL 証明書をインストールする必要があります。SQL Server 2014 はワイルドカード証明書を受け付けることはできません。そのため、SQL Server の FQDN 付き SSL 証明書を要求することをお勧めします。

FIPS モードの構成

FIPS モードは、XenMobile サーバーの初回セットアップ時にのみ有効にできます。インストールが完了したら、FIPS を有効にはできません。そのため、FIPS モードの使用を予定している場合は、XenMobile サーバーを最初から FIPS モードでインストールする必要があります。また、XenMobile クラスタの場合、すべてのクラスタノードで FIPS が有効になっている必要があります。同一クラスタ内に FIPS と非 FIPS XenMobile サーバーを混在させることはできません。

本番用でない XenMobile コマンドラインインターフェイスには ［**Toggle FIPS mode**］ オプションがあります。このオプションは診断目的のための非実稼働環境用のもので、実稼働環境での XenMobile サーバーではサポートされません。

1. 初期セットアップ時に **FIPS** モードを有効にします。
2. SQL Server 用のルート CA 証明書をアップロードします。
3. SQL Server のサーバー名とポート、SQL Server にログインするための資格情報、および XenMobile に対して作成するデータベース名を指定します。

   > 注:
   >
   > SQL Server にアクセスするには、SQL ログオンまたは Active Directory アカウントのいずれかを使用できますが、使用するログオン資格情報には DBcreator 役割が必要です。

4. Active Directory アカウントを使用するには、「ドメイン\ユーザー名」形式で資格情報を入力します。
5. これらの手順が完了したら、XenMobile の初期セットアップを実行します。

FIPS モードの構成が成功したことを確認するには、XenMobile コマンドラインインターフェイスにログオンします。ログオンバナーに ［**In FIPS Compliant Mode**］ と表示されます。

証明書のインポート中

以下で、VMware ハイパーバイザーを使用する場合に必要となる証明書をインポートして XenMobile 上で FIPS を構成する方法について説明します。

SQL の前提条件

1. XenMobile から SQL インスタンスの接続をセキュリティで保護し、SQL Server のバージョンは 2012 または 2014 が必要です。接続を保護するには、「Microsoft 管理コンソールを使用して SQL Server のインスタンスの SSL 暗号化を有効にする方法」を参照してください。
2. サービスが適切に再起動しない場合は、**Services.msc** を開いて次のようにチェックします。
   a) SQL Server サービスで使用されたログオンアカウント情報をコピーします。
   b) SQL Server で MMC.exe を開きます。
   c) ［ファイル］ **>** ［スナップインの追加と削除］ の順に選択し、証明書アイテムをダブルクリックして証明書スナップインを追加します。ウィザードの 2 つのページでコンピューターアカウントとローカルコンピューターを選択します。
   d) ［**OK**］ をクリックします。
   e) ［証明書（ローカルコンピューター）］ **>** ［個人］ **>** ［証明書］ の順に選択し、インポートされた SSL 証明書を探します。

f) インポートされた証明書を右クリックして ［すべてのタスク］**>**［秘密キーの管理］ の順に選択します。

g)［グループ名またはユーザー名］ の下にある ［追加］ をクリックします。

h) 前の手順でコピーした SQL サービスアカウント名を入力します。

i)［フルコントロールを許可］ オプションをクリアします。デフォルトでは、サービスアカウントにはフルコントロールと読み取り権限のどちらもが付与されますが、秘密キーの読み取りだけが必要です。

j) **MMC** を閉じて SQL サービスを開始します。

3. SQL サービスが正常に開始されたか確認します。

インターネットインフォメーションサービス（**IIS**）の前提条件

1. ルート証明書（base 64）をダウンロードします。
2. ルート証明書を IIS サーバー上のデフォルトサイト（C:\inetpub\wwwroot）にコピーします。
3. デフォルサイトに対して ［**Authentication**］ チェックボックスをオンにします。
4.［**Anonymous**］ を ［**enabled**］ に設定します。
5.［**Failed Request Tracking**］ 規則チェックボックスをオンにします。
6. .cer がブロックされていないか確認します。
7. ローカルサーバーの Internt Explorer ブラウザーで.cer の場所を参照します（`https://localhost/certname.cer`）。ルート証明書テキストがブラウザーに表示されます。
8. ルート証明書が Internet Explorer ブラウザーに表示されない場合、ASP が IIS サーバーで有効化されていることを、次のようにして確認します。

   a) サーバーマネージャーを開きます。

   b)［**Manage**］**>**［**Add Roles and Features**］ の順に移動します。

   c) サーバーの役割で、［**Web Server (IIS)**］、［**Web Server**］、［**Application Development**］ の順に展開して ［**ASP**］ を選択します。

   d)［**Next**］ をクリックしてインストールを完了させます。

9. Internet Explorer を開いて`https://localhost/cert.cer`を参照します。

   詳しくは、「Web Server (IIS)」を参照してください。

   > 注:
   >
   > これを実行するには、CA の IIS インスタンスを使用できます。

初期 **FIPS** 構成中のルート証明書のインポート

コマンドラインコンソールで初めて XenMobile を構成するための手順を実行する場合、これらの設定を完了させてルート証明書をインポートする必要があります。インストール手順について詳しくは、「XenMobile のインストール」を参照してください。

- FIPS の有効化：はい
- ルート証明書のアップロード：はい
- コピー（c）またはインポート（i）：i
- インポートする HTTP URL を入力：`https://<FQDN of IIS server>/cert.cer`
- サーバー：*SQL Server の FQDN *
- Port：1433
- ユーザー名：データベースを作成できるサービスアカウント（`domain\username`）。
- パスワード：サービスアカウントのパスワード。
- データベース名：選択した名前。

モバイルデバイスで **FIPS** モードを有効にする

デフォルトでは、モバイルデバイスで FIPS モードは無効になっています。FIPS モードを有効にするには、［設定］**>**［クライアントプロパティ］ の順に選択し、［**FIPS** モードの有効化］ プロパティを編集して、値を **true** に設定します。詳しくは、「クライアントプロパティ」を参照してください。

クラスタリングの構成

January 10, 2020

クラスタリングを構成するには、以下の 2 つの負荷分散仮想 IP アドレスを NetScaler で構成します。

- モバイルデバイス管理（**MDM**）負荷分散仮想 **IP** アドレス： クラスター内に構成された XenMobile ノードと通信するには、MDM 負荷分散仮想 IP アドレスが必要です。この負荷分散は SSL ブリッジモードで行われます。
- モバイルアプリケーション管理（**MAM**）負荷分散仮想 **IP** アドレス： クラスター内に構成された XenMobile ノードと NetScaler Gateway が通信するには、MAM 負荷分散仮想 IP アドレスが必要です。XenMobile ではデフォルトで、NetScaler Gateway からのすべてのトラフィックはポート 8443 で負荷分散仮想 IP アドレスにルーティングされます。

この項目の手順では、新しい XenMobile 仮想マシン（VM）を作成し、新しい VM を既存の VM に参加させる方法について説明します。これらの手順でクラスタ設定が作成されます。

前提条件

- 必要な XenMobile ノードが完全に構成されていること
- すべてのクラスタノードと XenMobile データベースで NTP を構成すること。これらのすべてのサーバーで時刻がそろっていないと、クラスタリングは正しく機能しません
- MDM ロードバランサー用の 1 つのパブリック IP アドレスと MAM 用の 1 つのプライベート IP アドレス
- サーバー証明書
- NetScaler Gateway 仮想 IP アドレス用の 1 つの空き IP アドレス
- XenMobile を MDM-only モードまたはエンタープライズモード（MDM + MAM）のクラスターセットアップで展開する場合：NetScaler のすべての MDM ロードバランサー、つまりポート 8443 とポート 443 用に設定された仮想サーバーに送信元 **IP** のパーシステンスを使用するように、NetScaler 負荷分散装置の構成を変更します。ユーザーデバイスを iOS 11 にアップグレードする前に、この構成を完了してください。詳しくは、Citrix Knowledge Center の記事（https://support.citrix.com/article/CTX227406）を参照してください。
- iOS 11 デバイス上の XenMobile Store からアプリをインストールするには、XenMobile Server でポート 80 を有効にする必要があります。

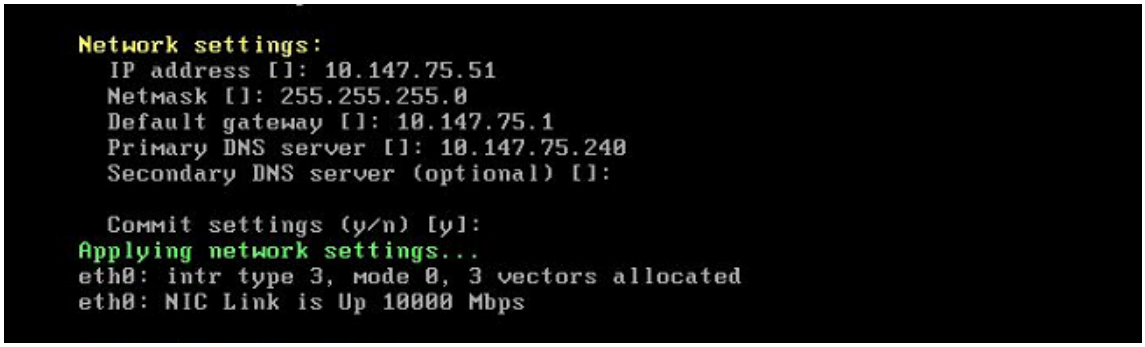
クラスター構成における XenMobile 10.x のリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。

XenMobile クラスターノードのインストール

必要なノードの数に基づいて、XenMobile VM を作成します。新しい VM が同じデータベースを指すようにし、同じ PKI 証明書のパスワードを指定します。

1. 新しい VM のコマンドラインコンソールを開き、管理者アカウントの新しいパスワードを入力します。

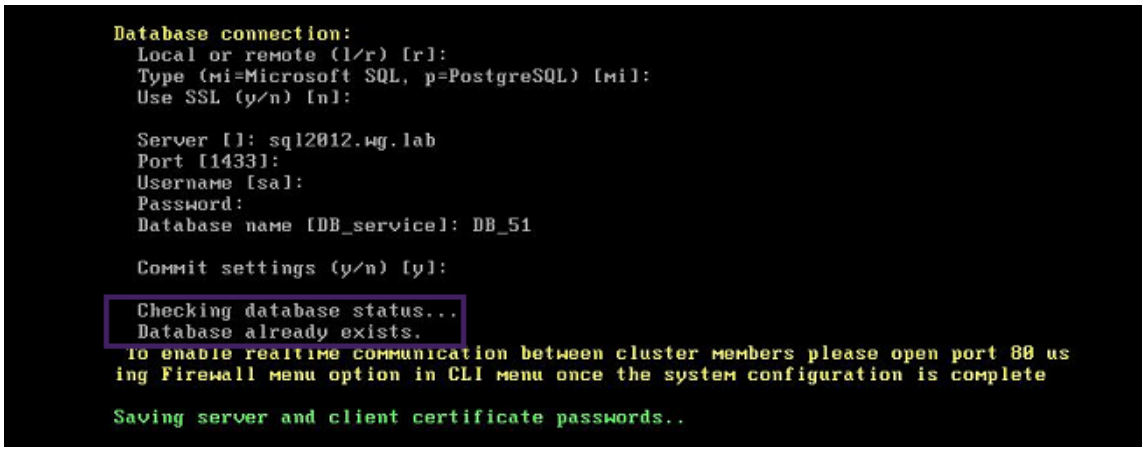
2. 次の図に示すように、ネットワーク構成の詳細を入力します。



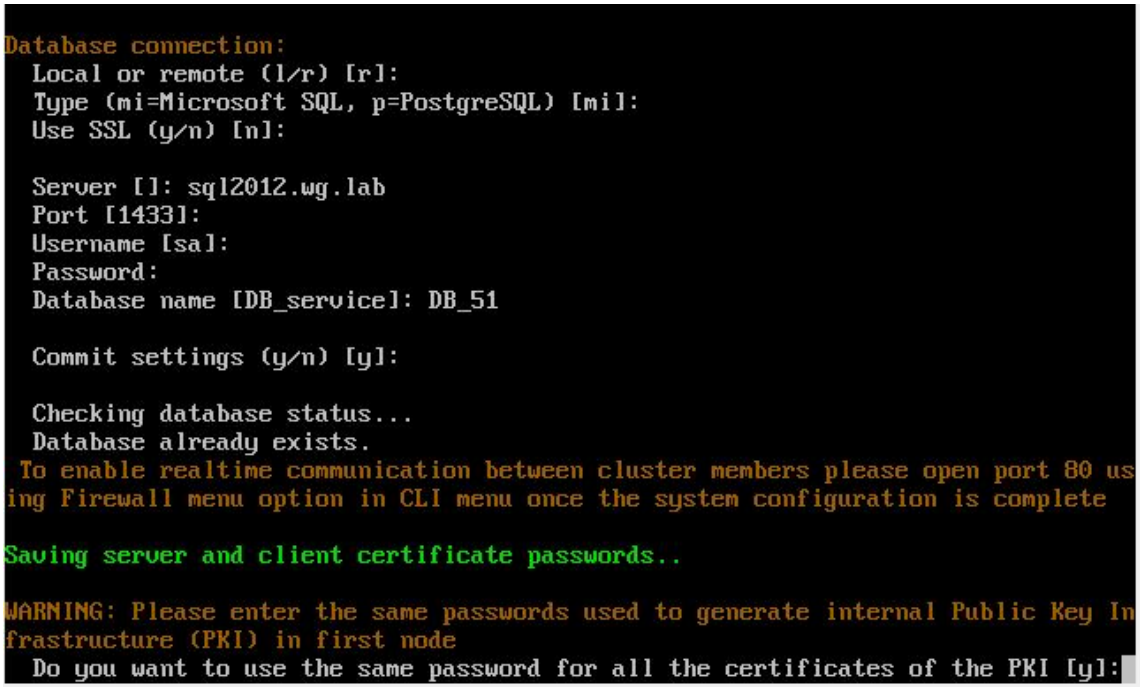
3. データ保護のためにデフォルトのパスワードを使用する場合、「**y**」と入力します。そうでない場合は「**n**」と入力して新しいパスワードを入力します。

4. FIPS を使用する場合は、「**y**」または「**n**」と入力します。

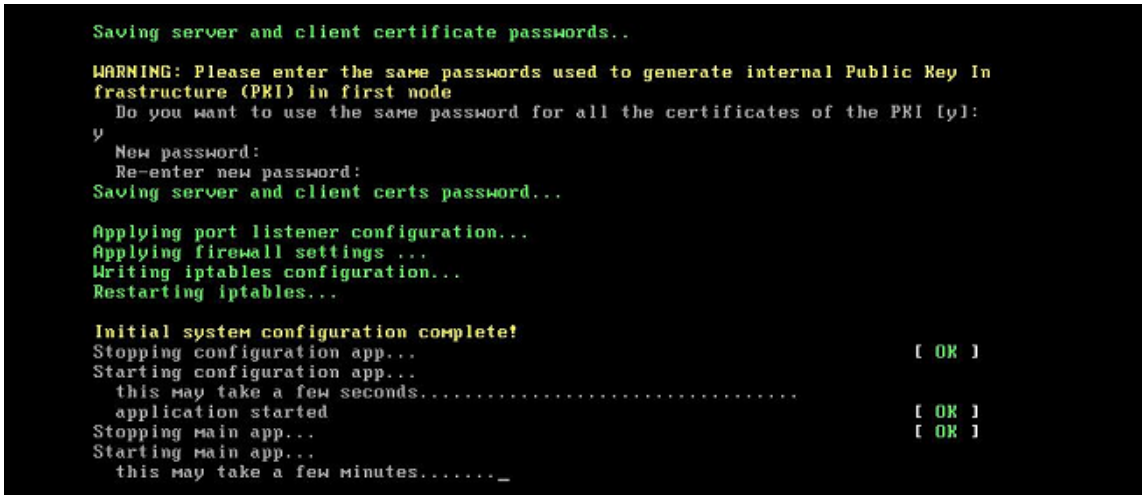
5. 以前に完全に構成された VM が参照するのと同じデータベースを参照するようにデータベースを構成します。次のメッセージが表示されます:「データベースが既に存在します」。



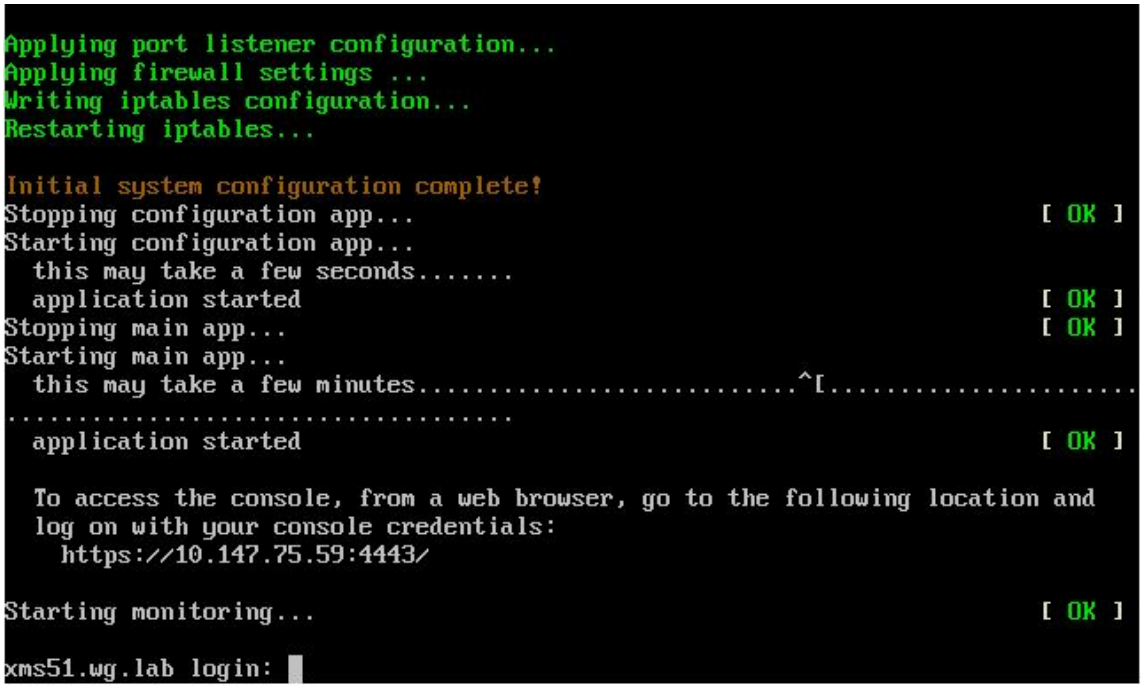
6. 最初の VM に指定した証明書に対して同じパスワードを入力します。



パスワードを入力すると、2 番目のノードの初期設定が完了します。



7. 構成が完了するとサーバーが再起動され、ログオンダイアログボックスが表示されます。

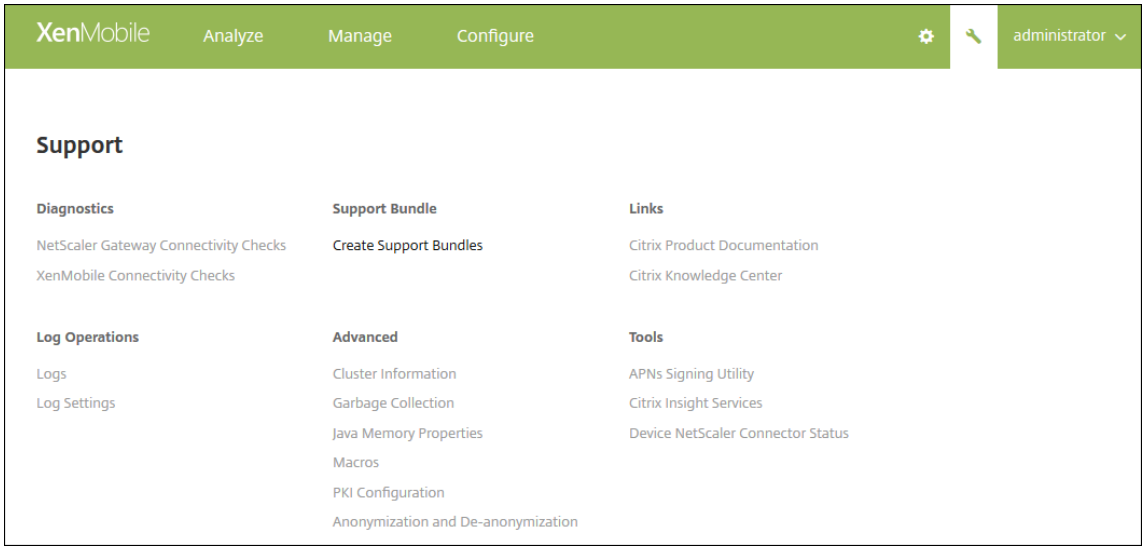


> 注:
>
> ログオンダイアログボックスは最初の VM のログオンダイアログボックスと同じです。同じであるため、両方の VM で同じデータベースサーバーを使用していることが確認できます。

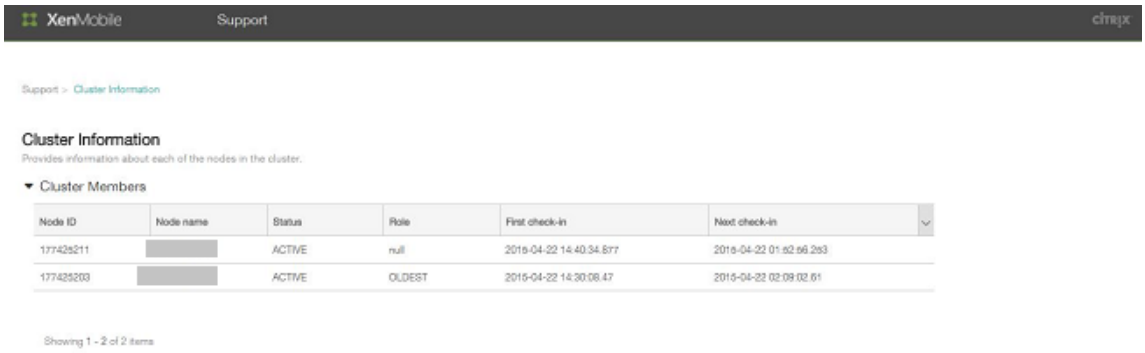
8. XenMobile の完全修飾ドメイン名（FQDN）を使用して、Web ブラウザで XenMobile コンソールを開きます。
9. XenMobile コンソールで、右上のレンチアイコンをクリックします。

［サポート］ ページが開きます。

10. ［上級］ の ［クラスター情報］ をクリックします。



クラスターのメンバー、デバイス接続情報、タスクなど、クラスターに関するすべての情報が表示されます。新しいノードがクラスターのメンバーになります。

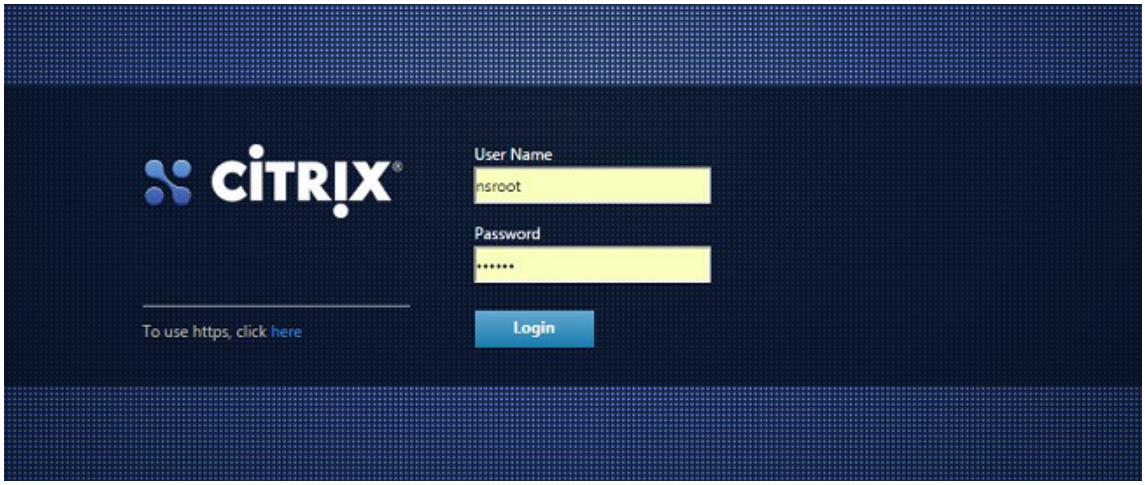


別のノードを追加する場合も、手順は同じです。クラスターに追加された最初のノードの役割は **OLDEST** です。その後追加されたノードの役割は、**NONE** または **null** と表示されます。

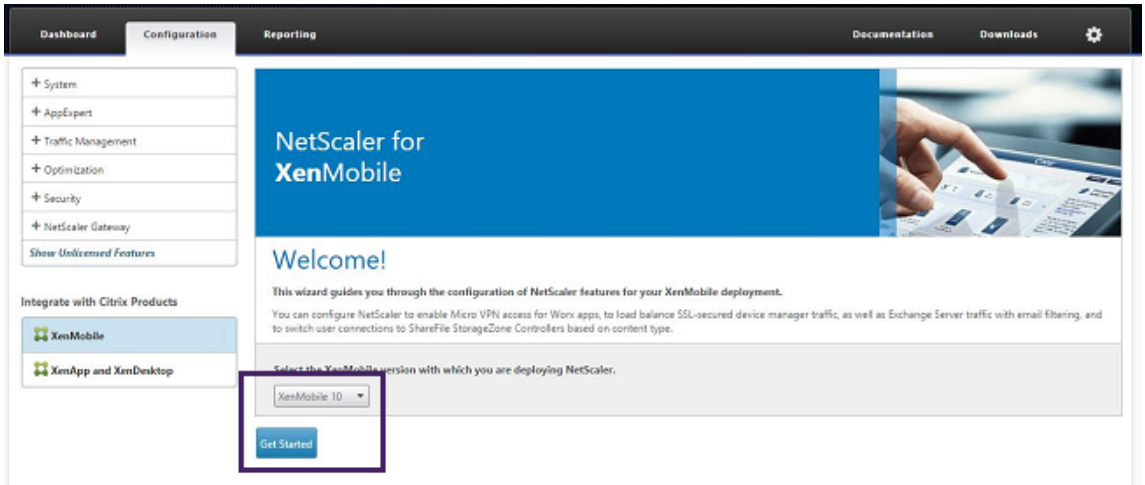
NetScaler で XenMobile クラスターの負荷分散を構成するには

必要なノードを XenMobile クラスターのメンバーとして追加した後、クラスターにアクセスできるようにノードの負荷分散を行います。負荷分散を行うには、NetScaler で利用可能な XenMobile ウィザードを実行します。次の手順では、ウィザードを実行して XenMobile の負荷を分散する方法について説明します。

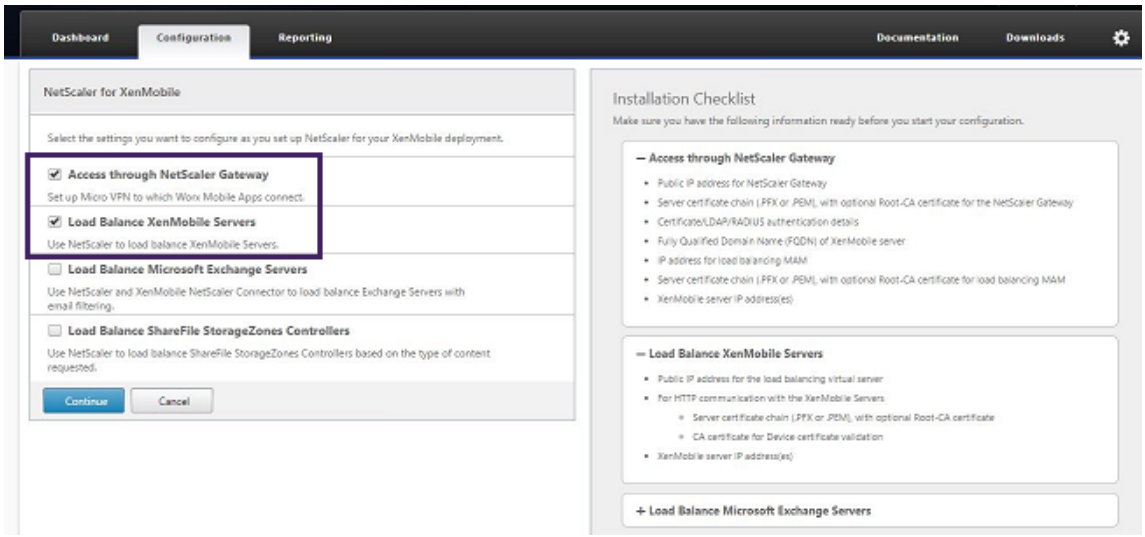
1. NetScaler にログオンします。



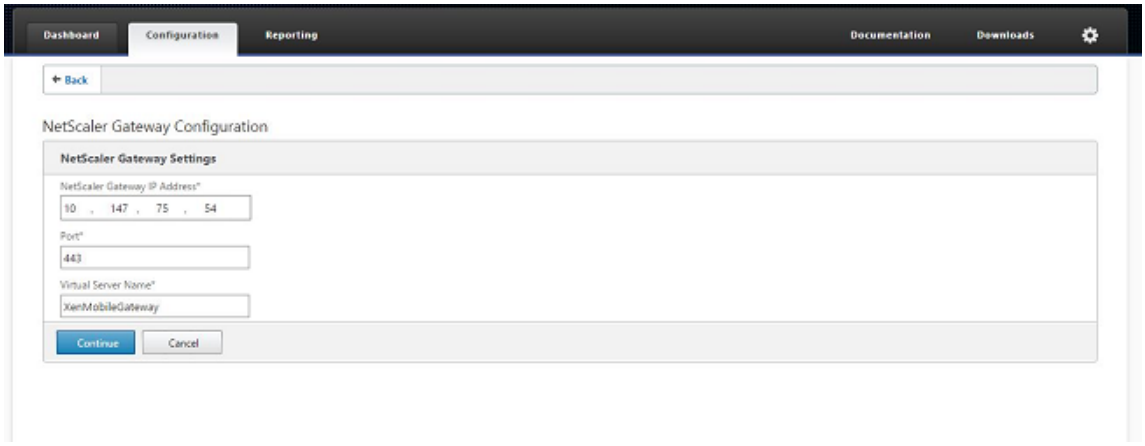
2. [Configuration] タブで [**XenMobile**] をクリックし、[**Get Started**] をクリックします。



3. [**Access through NetScaler Gateway**] チェックボックスと [**Load Balance XenMobile Servers**] チェックボックスを選択してから、[**Continue**] をクリックします。

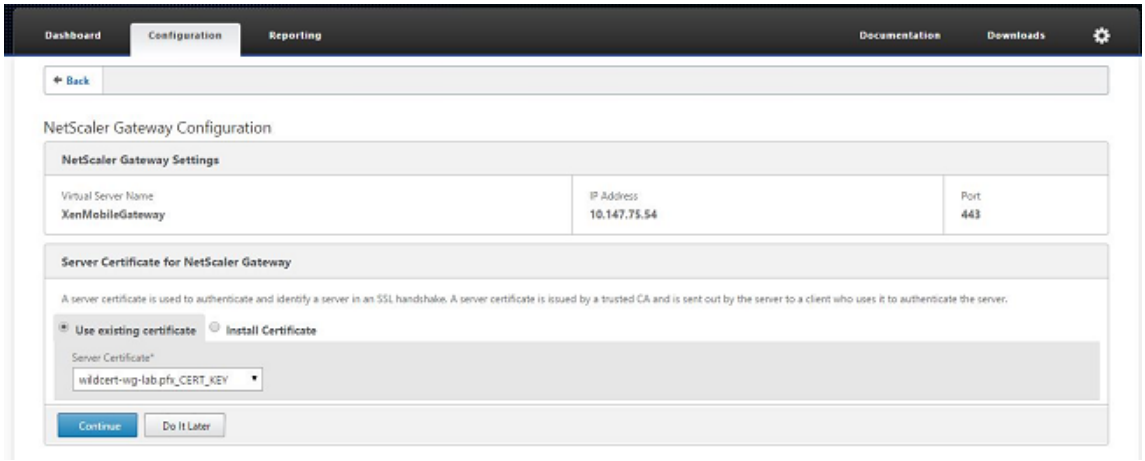


4. NetScaler Gateway の IP アドレスを入力してから ［**Continue**］ をクリックします。

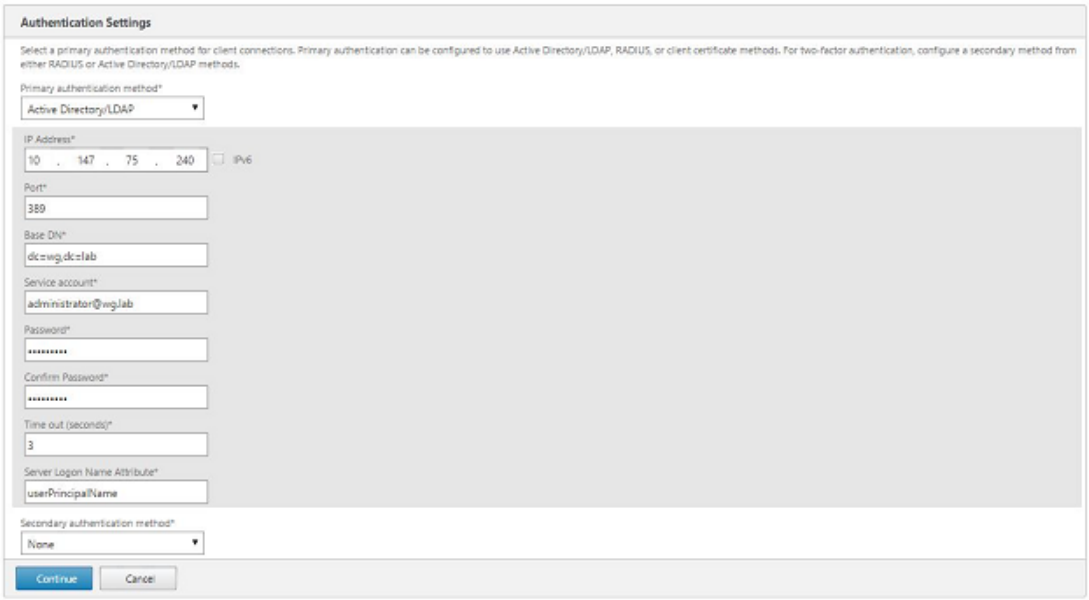


5. 次のいずれかを実行して、サーバー証明書を NetScaler Gateway の仮想 IP アドレスにバインドし、［**Continue**］をクリックします。

   - ［**Use existing certificate**］ で、リストからサーバー証明書を選択します。
   - ［**Install Certificate**］ をクリックして、新しいサーバー証明書をアップロードします。

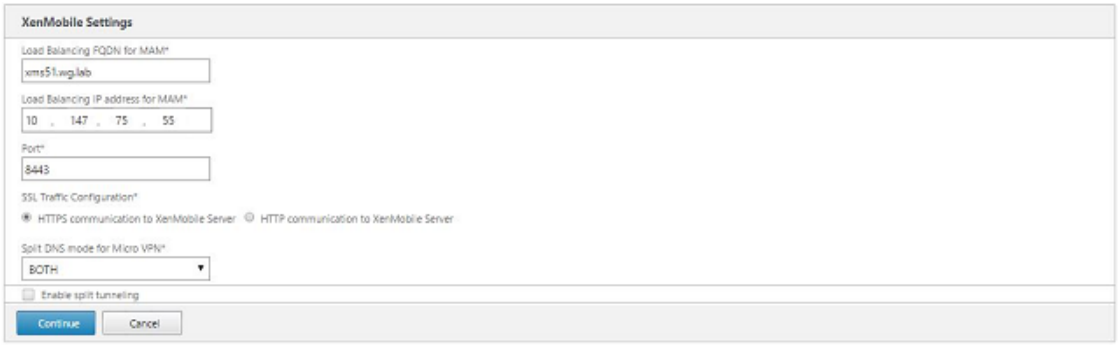


6. 認証サーバーの詳細を入力し、［**Continue**］ をクリックします。



> 注：
>
> ［Server Logon Name Attribute］が XenMobile LDAP 構成で指定したものと同じであることを確認してください。

7. ［XenMobile settings］の下で［Load Balancing FQDN for MAM］を入力し、［**Continue**］をクリックします。

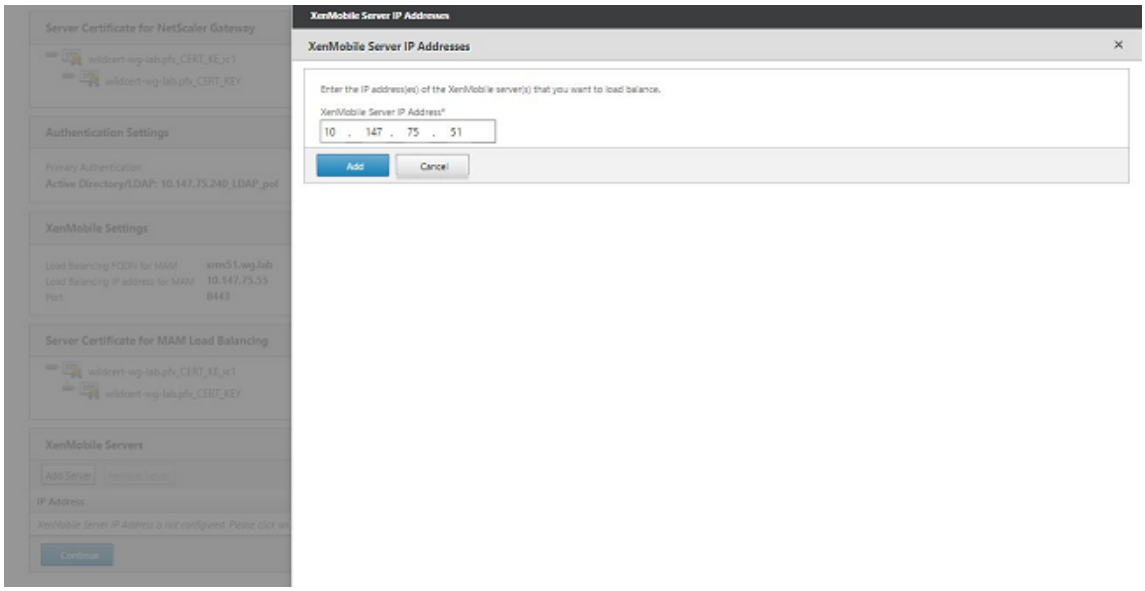


> 注：
>
> MAM 負荷分散仮想 IP アドレスの FQDN と XenMobile の FQDN が同じであることを確認してください。

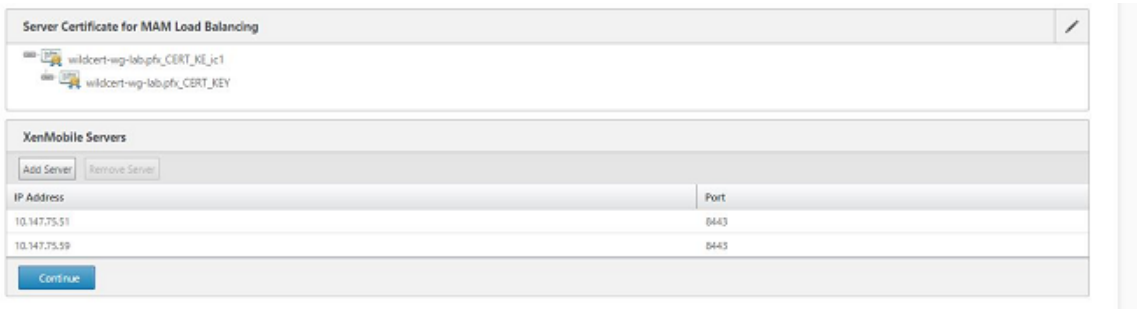
8. SSL ブリッジモード（HTTPS）を使用する場合は、［**HTTPS communication to XenMobile Server**］を選択します。ただし、SSL オフロードを使用する場合は、上の図に示したように［**HTTP communication to XenMobile Server**］を選択します。このトピック用には、SSL ブリッジモード（HTTPS）が選択されます。
9. サーバー証明書を MAM 負荷分散仮想 IP アドレスにバインドし、［Continue］をクリックします。

10. ［XenMobile Servers］の下で ［**Add Server**］ をクリックして XenMobile ノードを追加します。

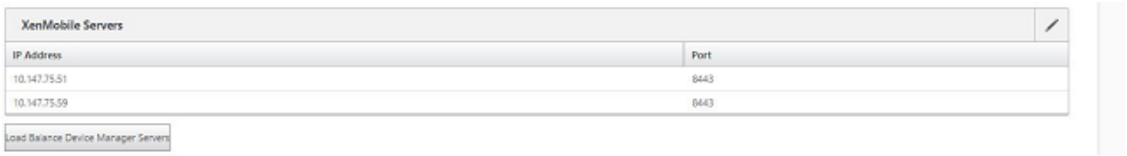
11. XenMobile ノードの IP アドレスを入力し、［Add］をクリックします。



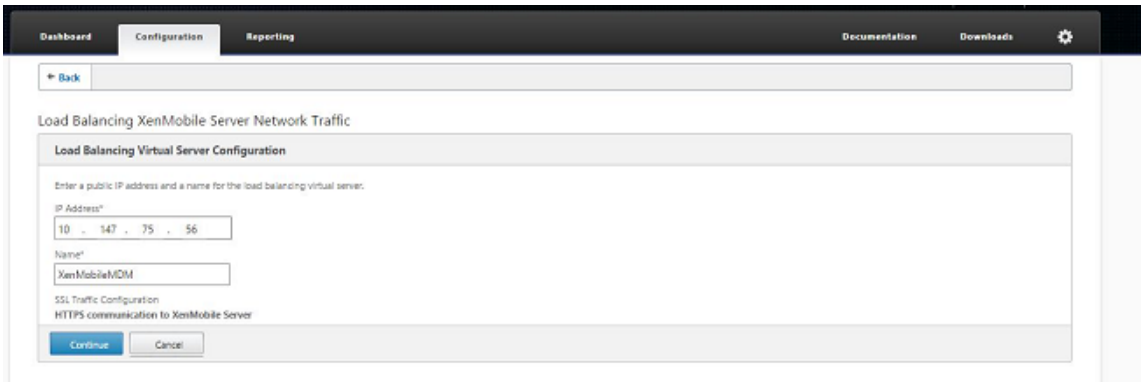
12. 手順 10 および 11 を繰り返して、XenMobile クラスターに含まれる XenMobile ノードを追加します。追加したすべての XenMobile ノードが表示されます。［続行］をクリックします。



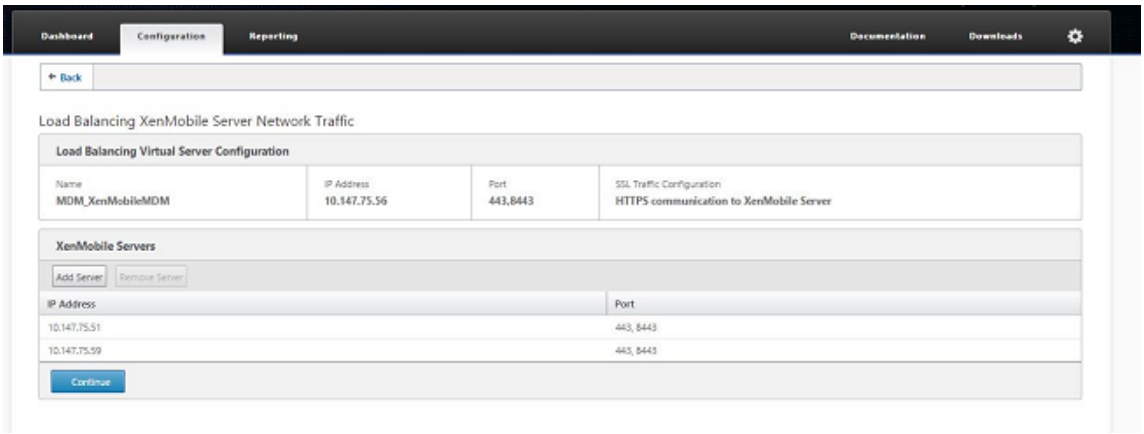
13. [**Load Balance Device Manager Servers**] をクリックして MDM 負荷分散の設定を続行します。



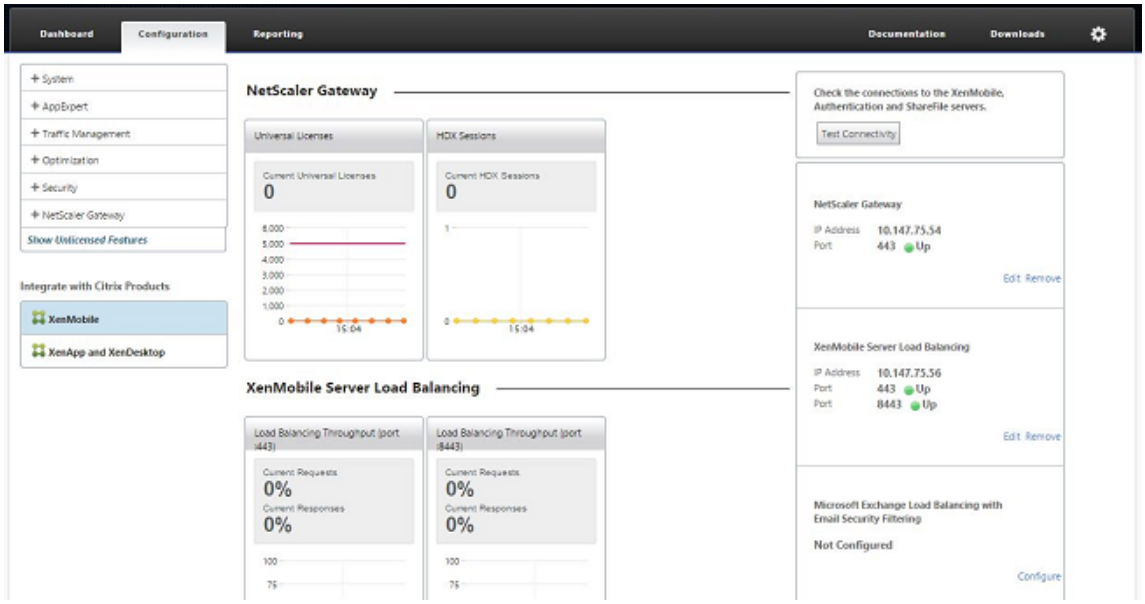
14. MDM 負荷分散 IP アドレスに使用する IP アドレスを入力し、 [**Continue**] をクリックします。



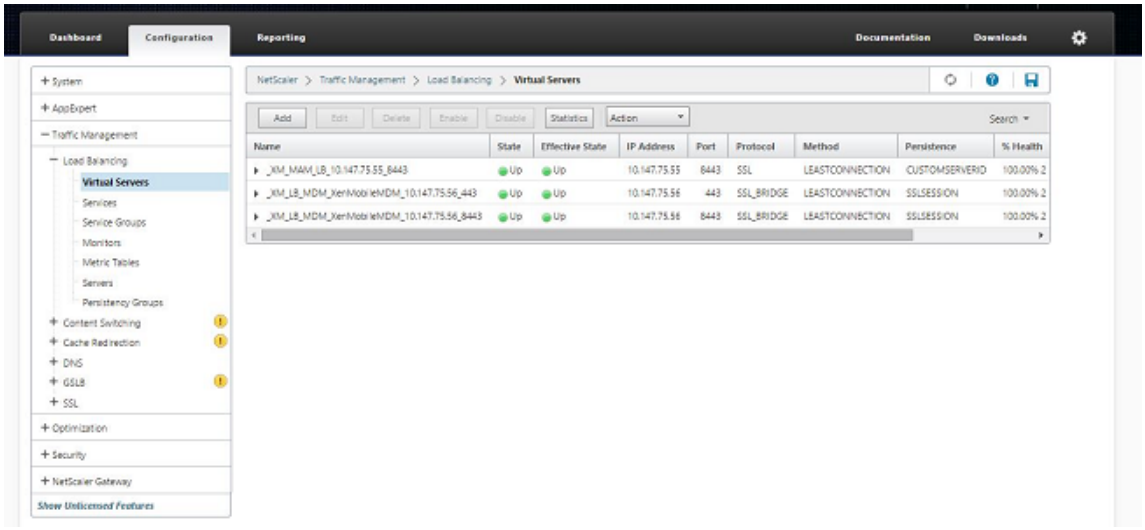
15. 一覧に XenMobile ノードが表示されたら、 [**Continue**] をクリックしてから [Done] をクリックして処理を完了します。



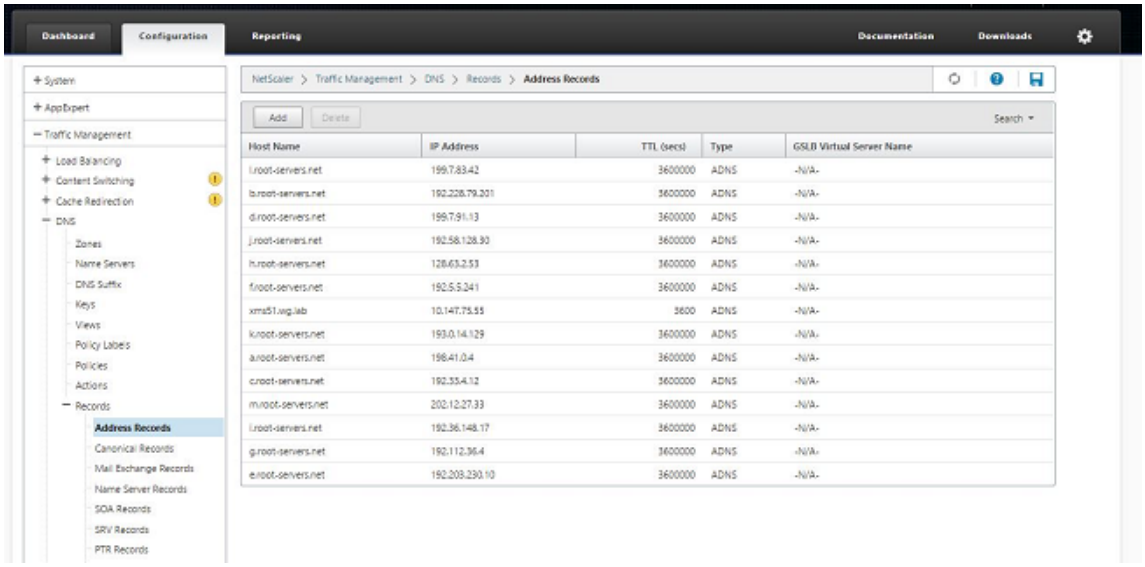
[XenMobile] ページに仮想 IP アドレスのステータスが表示されます。



16. 仮想 IP アドレスが使用可能で動作状態になっているかどうかを確認するには、[Configuration] タブをクリックし、 [**Traffic Management**]、[**Load Balancing**]、[**Virtual Servers**] の順にクリックします。



NetScaler の DNS エントリが MAM 負荷分散仮想 IP アドレスを参照していることも示されます。



障害回復ガイド

May 21, 2019

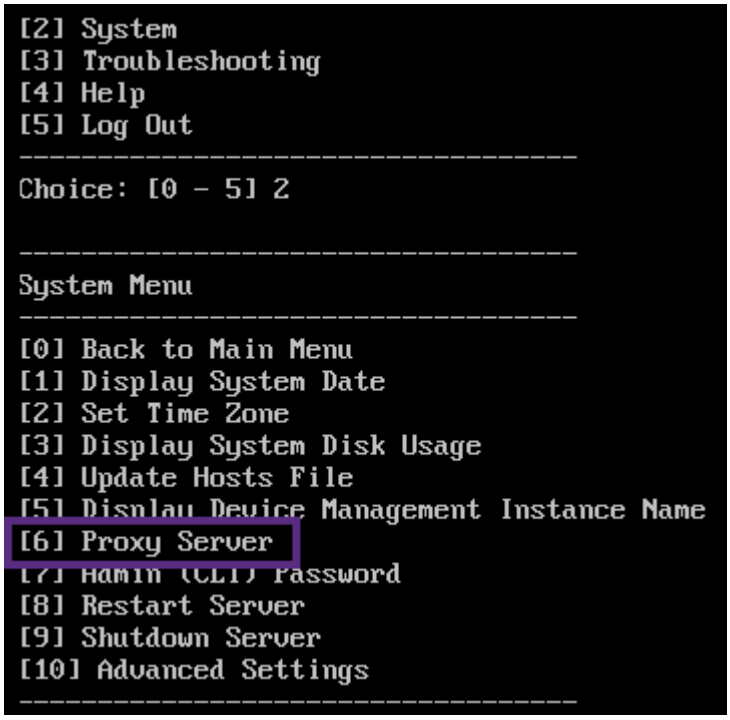
アクティブ/パッシブフェイルオーバー戦略を使用して複数サイトの障害回復を含めた XenMobile 展開環境を構築し、構成できます。詳しくは、XenMobile 展開ハンドブックの障害回復のトピックを参照してください。

プロキシサーバーの有効化

January 10, 2020

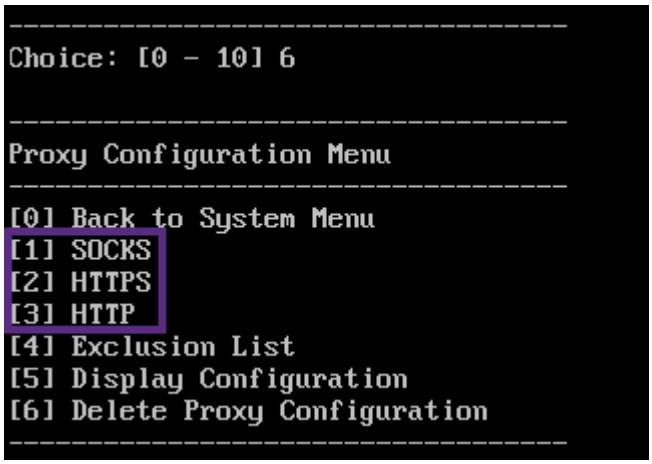
発信インターネットトラフィックを制御するために、そのトラフィックを発信するプロキシサーバーを XenMobile にセットアップできます。コマンド行インターフェース（CLI）を使用してプロキシー・サーバーをセットアップします。プロキシサーバーのセットアップにはシステムの再起動が必要です。

1. XenMobile CLI メインメニューで、「**2**」と入力して［System］メニューを開きます。
2. ［System］メニューで、「**6**」と入力して［Proxy Server］メニューを選択します。



3. ［プロキシの構成］メニューで、「**1**」と入力して［SOCKS］を選択します。

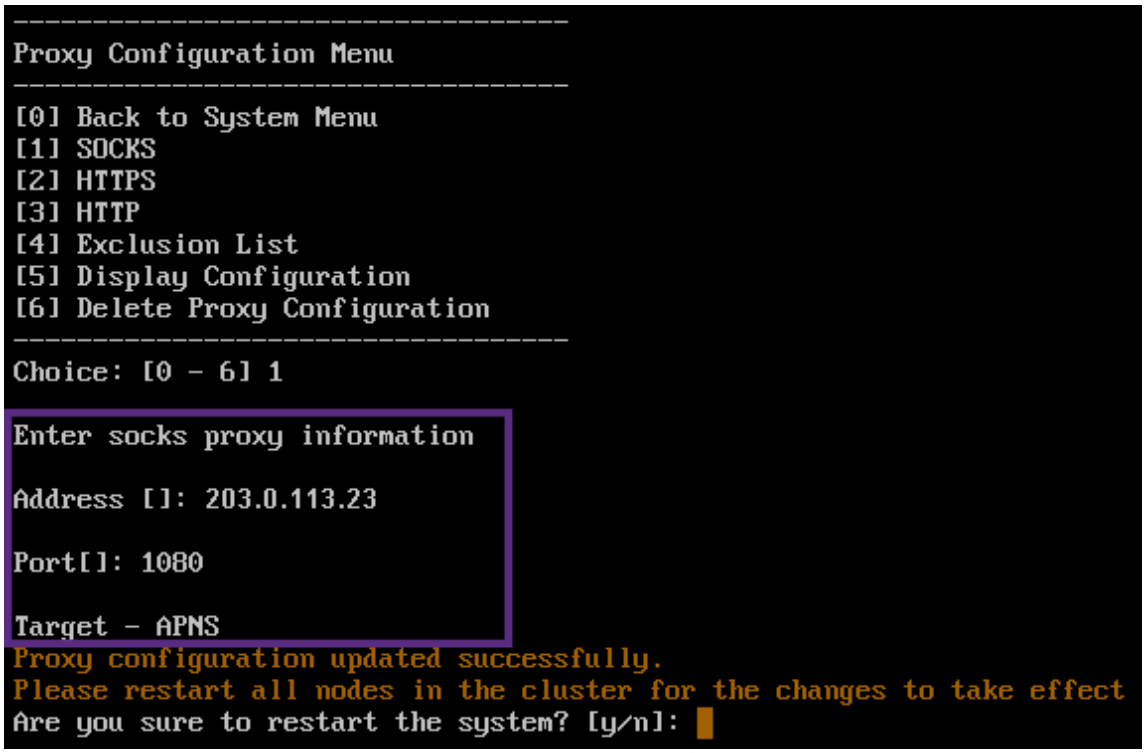
   この設定を保存する前に、HTTPS も構成する必要があります。SOCKS と HTTPS の設定を同じ構成で保存しない限り、プロキシは機能しません。



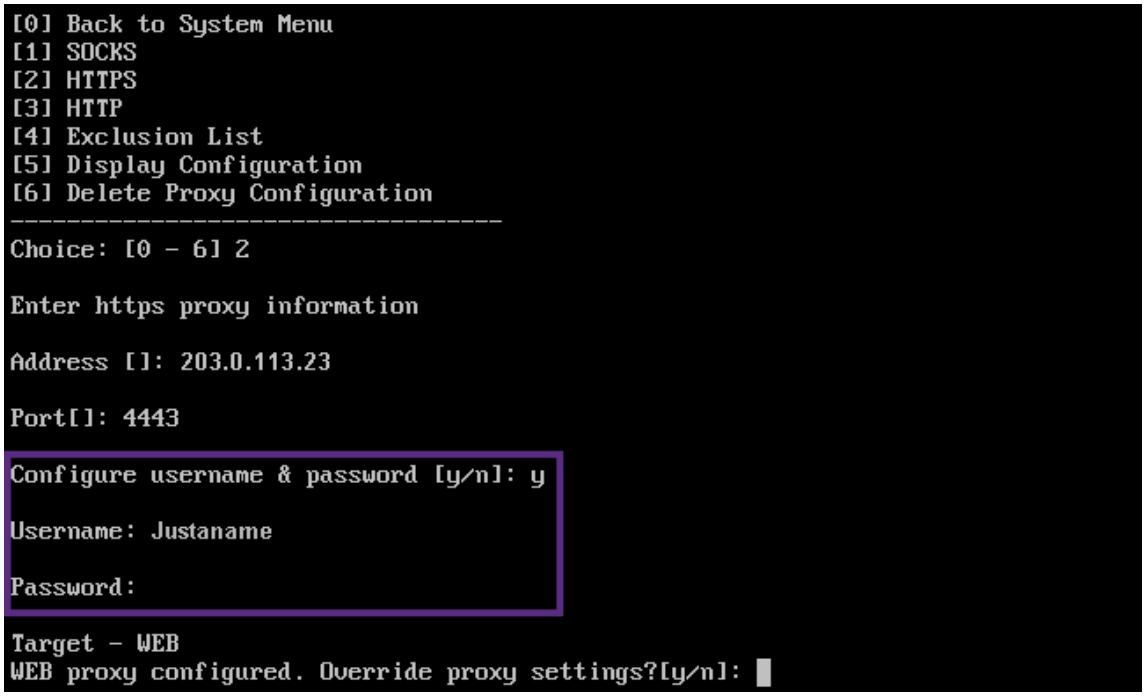
4. プロキシサーバーの IP アドレス、ポート番号、およびターゲットを入力します。プロキシサーバーの種類別の、サポートされるターゲットの種類については以下の表を参照してください。

プロキシの種類	サポートされるターゲット
SOCKS	APNS
HTTP	APNS、Web、PKI

HTTPS	Web、PKI
認証付き HTTP	Web、PKI
認証付き HTTPS	Web、PKI



5. 「**n**」、「**2**」と入力して［HTTPS］を選択し、プロキシサーバーの IP アドレス、ポート番号、およびターゲットを入力します。
6. プロキシサーバーに認証用のユーザー名およびパスワードを構成する場合は「**y**」と入力し、ユーザー名とパスワードを入力します。



7.「**y**」と入力して設定を保存します。

SQL Server の構成

August 22, 2019

オンプレミスの XenMobile Server から SQL Server に接続する場合は、デフォルトのドライバーである jTDS、または Microsoft Java Database Connectivity（JDBC）ドライバーを使用できます。jTDS ドライバは、次の場合のデフォルトのドライバです:

- オンプレミスの XenMobile Server をインストールします。
- jTDS ドライバを使用するように設定された XenMobile サーバーからアップグレードします。

どちらのドライバーでも、XenMobile では SQL Server 認証または Windows 認証がサポートされます。認証とドライバーのこれらの組み合わせでは、SSL をオンまたはオフにすることができます。

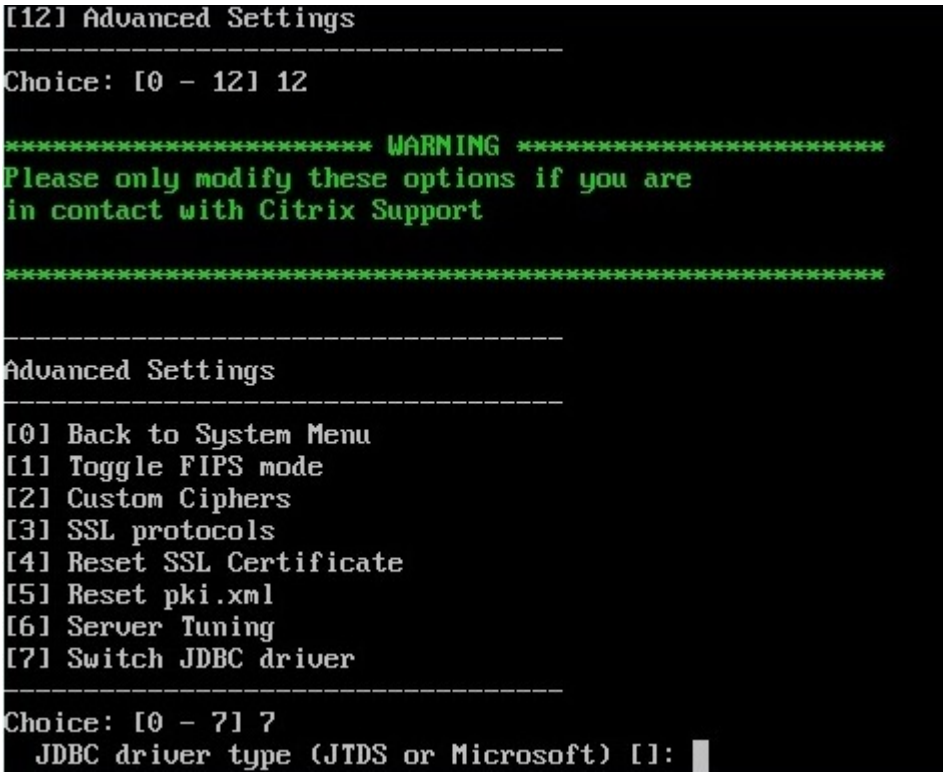
Microsoft JDBC ドライバーで Windows 認証を使用する場合、ドライバーは Kerberos との統合認証を使用します。XenMobile は Kerberos とやり取りをして、Kerberos キー配布センター（KDC）の詳細情報を取得します。必要な詳細が取得できない場合は、XenMobile CLI で Active Directory サーバーの IP アドレスを入力するように求められます。

jTDS ドライバーから JDBC ドライバーに切り替えるには、すべての XenMobile Server ノードに SSH を適用し、XenMobile CLI を使用して構成します。次のように、現在の jTDS ドライバーの構成によって手順が異なります。

Microsoft JDBC への切り替え（**SQL Server** 認証）

次の手順を完了するには、SQL Server のユーザー名とパスワードが必要です。

1. すべての XenMobile Server ノードに SSH を適用します。
2. XenMobile CLI メインメニューで、「**2**」と入力して［System］メニューを開きます。
3. 「**12**」を入力して［Advanced Settings］を選択します。
4. 「**7**」を入力して［Switch JDBC driver］を選択し、Microsoft の場合は「**m**」を入力します。



5. プロンプトが表示されたら、「**y**」を入力して SQL 認証を選択し、SQL Server のユーザー名とパスワードを入力します。
6. 各 XenMobile Server ノードに対して手順を繰り返します。
7. 各 XenMobile Server ノードを再起動します。

Microsoft JDBC への切り替え（**SSL** はオフ、**Windows** 認証）

次の手順を完了するには、Active Directory のユーザー名とパスワード、Kerberos KDC 領域、および KDC のユーザー名が必要です。

1. すべての XenMobile Server ノードに SSH を適用します。
2. XenMobile CLI メインメニューで、「**2**」と入力して［System］メニューを開きます。

3.「**12**」を入力して［Advanced Settings］を選択します。
4.「**7**」を入力して［Switch JDBC driver］を選択し、「**m**」を入力します。
5. SQL Server 認証を使用するかどうかを確認するメッセージが表示されたら、「**n**」と入力します。
6. プロンプトが表示されたら、SQL Server 用に構成された Active Directory のユーザー名とパスワードを入力します。
7. XenMobile で Kerberos KDC 領域が自動検出されない場合は、SQL Server の FQDN を含む KDC の詳細を入力するように求められます。
8. SSL を使用するかどうかを確認するメッセージが表示されたら、「**n**」と入力します。XenMobile によって構成が保存されます。エラーのため XenMobile が構成を保存できない場合は、エラーメッセージと入力した詳細が表示されます。
9. 各 XenMobile Server ノードに対して手順を繰り返します。
10. 各 XenMobile Server ノードを再起動します。

XenMobile データベースのパスワードを変更するには

XenMobile のデータベースパスワードを変更するには、このガイドラインに従ってください（Citrix サポートからパスワードの変更を指示された場合など）。

> 重要：
>
> - データベースパスワードを変更するための予定されたメンテナンスウィンドウを計画します。システムのダウンタイム中にパスワードを変更する必要があります。
> - パスワードを変更するときは、すべての XenMobile ノードがネットワークに接続されていることを確認してください。パスワードを変更したら、XenMobile を再起動します。
>
>   パスワード変更後に XenMobile を再起動しないと、XenMobile はリカバリモードになります。その場合は、SQL Server で古いパスワードに戻し、XenMobile を再起動して、パスワードを再度変更する必要があります。
> - SQL Server が Windows 認証を使用している場合は、Windows Active Directory でデータベースのパスワードを変更します。

1. すべての XenMobile サーバーノードが実行されていることを確認します。クラスタ環境では、すべてのノードを起動します。
2. vServers を無効にすることによって、Netscaler ロードバランサーで XenMobile に着信するデバイストラフィックをブロックします。
3. SQL Server でデータベースのパスワードを変更するには、次の手順を実行します：XenMobile CLI にログインし、［**Configuration**］**>**［**Database**］に移動し、プロンプトが表示されたら、変更後のパスワードを入力します：


```
Server []: <ipAddress>
Port [1433]: 1433
Username [sa]: <userName>
Password: <****>
```

4. **Y** を選択してサーバーを再起動します。
5. クラスタ内の他のすべてのノードについて、手順 3 と 4 を繰り返します。
6. NetScaler ロードバランサーで vServers を有効にして、着信デバイストラフィックのブロックを解除します。

サーバープロパティ

January 10, 2020

XenMobile には、サーバー全体の操作に適用される多くのプロパティがあります。この記事ではさまざまなサーバープロパティと、サーバープロパティを追加、編集、削除する方法について説明します。

一部のプロパティはカスタムキーです。カスタムキーを追加するには、［追加］ をクリックし、［キー］ から ［カスタムキー］ を選択します。

使用されることが多いプロパティについて詳しくは、XenMobile 仮想ハンドブックの「サーバープロパティ」を参照してください。

サーバープロパティ定義

常にデバイスを追加

- **true** の場合、XenMobile はデバイスを XenMobile コンソールに追加します。そのため、登録に失敗しても、登録しようとしたデバイスを確認できます。デフォルトは **false** です。

AG クライアント証明書の発行調整間隔

- 証明書の作成の猶予期間です。この間隔により、XenMobile で短時間にデバイスの証明書が複数作成されることを防ぎます。この値は変更しないでください。デフォルトは **30** 分です。

監査ログのクリーンアップ実行日時

- 監査ログクリーンアップを開始する時刻（「HH:MM AM/PM」の形式）。例: 04:00 AM。デフォルトは **02:00 AM** です。

監査ログのクリーンアップ間隔 **(**日**)**

- XenMobile に監査ログが保持される日数です。デフォルトは **1** です。

Audit Logger

- **False** の場合、ユーザーインターフェイス（UI）イベントはログに記録されません。デフォルト値は **False** です。

監査ログの保持期間 **(**日**)**

- XenMobile に監査ログが保持される日数です。デフォルトは **7** です。

auth.ldap.connect.timeout および **auth.ldap.read.timeout**

- LDAP の反応が遅い場合に対処するには、次のカスタムキーのサーバープロパティを追加することをお勧めします。
  - キー：カスタムキー
  - キー：**auth.ldap.connect.timeout**
  - 値：**60000**
  - 表示名：**auth.ldap.connect.timeout**
  - 説明：**LDAP** 接続のタイムアウト
  - キー：カスタムキー
  - キー：**auth.ldap.read.timeout**
  - 値：**60000**
  - 表示名：**auth.ldap.read.timeout**
  - 説明：**LDAP** 読み取りのタイムアウト

証明書の書き換え（秒数）

- 証明書の有効期限が切れる前に、XenMobile が証明書の更新を開始する秒数です。たとえば、証明書が 12 月 30 日に期限切れになる予定でこのプロパティが 30 日に設定されている場合、デバイスが 12 月 1 日から 12 月 30 日の間に接続すると XenMobile は証明書の更新を試みます。デフォルトは **2592000** 秒（30 日間）です。

接続タイムアウト

- 無操作状態でセッションがタイムアウトになるまでの期間（分単位）です。この期間を過ぎると、XenMobile はデバイスへの TCP 接続を閉じます。セッションは開いたままになります。Android デバイス、Windows CE デバイス、Remote Support に適用されます。デフォルトは **5** 分です。

Microsoft 証明書サーバーへの接続タイムアウト

- XenMobile が証明書サーバーからの応答を待機する秒数です。証明書サーバーの接続速度が遅く、トラフィックが多い場合、この値を 60 秒以上にします。証明書サーバーが 120 秒経っても応答しない場合は、保守が必要です。デフォルトは **15000** ミリ秒（15 秒）です。

デフォルトの展開チャネル

- XenMobile でのデバイスへのリソースの展開：ユーザーレベル（**DEFAULT_TO_USER** ）とデバイスレベルのどちらで行うかを指定します。デフォルトは **DEFAULT_TO_DEVICE** です。

展開ログのクリーンアップ **(**日**)**

- XenMobile に展開ログが保持される日数です。デフォルトは **7** です。

ホスト名の検証を無効化

- デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証に失敗すると、サーバーログに「VPP サーバーに接続できません：ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」のようなエラーが記録されます。ホスト名の認証によって展開が損なわれる場合は、このプロパティを **true** に変更します。デフォルトは **false** です。

SSL サーバーの検証を無効化

- **True** の場合、以下の条件がすべて満たされると SSL サーバー証明書の検証が無効になります。
  - XenMobile Server で証明書ベースの認証を有効にしている
  - 証明書発行者に Microsoft CA サーバーを指定している
  - ルート XenMobile Server に信頼されていない内部 CA により証明書に署名している

デフォルトは **True** です。

コンソールの有効化

- **true** の場合、Self Help Portal コンソールへのユーザーアクセスが可能になります。デフォルトは **true** です。

Enable Crash Reporting

- **true** の場合、Secure Hub for iOS および Android での問題のトラブルシューティングを目的として、Citrix によりクラッシュレポートと診断情報が収集されます。**false** の場合、データは収集されません。デフォルト値は **true** です。

診断のための **Hibernate** 統計ログの有効化/無効化

- **True** にすると、アプリケーションパフォーマンスの問題のトラブルシューティングを支援する、Hibernate による診断統計ログが有効になります。Hibernate は、Microsoft SQL Server への XenMobile の接続のために使用されるコンポーネントです。ログはアプリケーションのパフォーマンスに影響を及ぼすため、デフォルトでは無効になっています。膨大なログファイルが作成されるのを避けるため、ログを有効にするのは短期間だけにしてください。XenMobile は、/opt/sas/logs/hibernate_stats.log にログを書き込みます。デフォルト値は **False** です。

Enable macOS OTAE

- **false** の場合、macOS デバイス用の登録リンクの使用が禁止され、macOS ユーザーの登録方法が登録招待状のみに制限されます。デフォルトは **true** です。

通知トリガーの有効化

- Secure Hub クライアントの通知を有効または無効にします。値 **true** を指定すると、通知が有効になります。デフォルトは **true** です。

force.server.push.required.apps

- 次のような場合に、Android および iOS デバイスで必要なアプリの強制展開を有効にします。
  - アップロードした新しいアプリを必要なアプリとしてマーク付けした場合。
  - 既存のアプリを必要なアプリとしてマーク付けした場合。
  - 必要なアプリをユーザーが削除した場合。
  - Secure Hub の更新が利用可能な場合。

必須アプリの強制展開は、デフォルトでは **false** です。強制展開を有効にするには、カスタムキーを作成して値を **true** に設定します。強制展開中には、エンタープライズアプリやパブリック App Store アプリなどの MDX 対応の必要なアプリは、即時アップグレードされます。アップグレードは、アプリの更新猶予期間の MDX ポリシーを構成し、ユーザーが後でアプリをアップグレードすることを選択した場合でも発生します。

- キー：カスタムキー
- キー：**force.server.push.required.apps**
- 値：**false**
- 表示名：**force.server.push.required.apps**
- 説明：必須アプリを強制的に展開する

許可および禁止された **ActiveSync** ユーザーの完全な抽出

- XenMobile が許可および禁止された ActiveSync ユーザーの完全な一覧（ベースライン）を抽出する間隔（秒単位）です。デフォルトは **28800** 秒です。

hibernate.c3p0.idle_test_period

- この［カスタムキー］という XenMobile Server プロパティでは、接続が自動的に検証されるまでのアイドル時間を秒単位で指定します。このキーは次のように構成します。デフォルトは **30** です。
- キー：カスタムキー
- キー：**hibernate.c3p0. idle_test_period**
- 値：**30**
- 表示名：**hibernate.c3p0. idle_test_period =*nnn***
- 説明：**Hibernate idle test period**

hibernate.c3p0.max_size

- このカスタムキーでは、XenMobile で SQL Server データベースに対して開くことのできる最大接続数を指定します。XenMobile では、このカスタムキーに指定した値が上限として使用されます。接続は必要な場合のみ開かれます。値は、データベースサーバーの処理能力に合わせて設定します。詳しくは、「XenMobile の動作の調整」を参照してください。このキーは次のように構成します。デフォルト値は **1000** です。
- キー：**hibernate.c3p0.max_size**
- 値：**1000**
- 表示名：**hibernate.c3p0.max_size**
- 説明：**DB connections to SQL**

hibernate.c3p0.min_size

- このカスタムキーでは、XenMobile が SQL Server データベースに対して開く最小接続数を指定します。このキーは次のように構成します。デフォルトは **100** です。
- キー：**hibernate.c3p0.min_size**
- 値：**100**
- 表示名：**hibernate.c3p0.min_size**
- 説明：**DB connections to SQL**

hibernate.c3p0.timeout

- このカスタムキーでは、アイドル状態のタイムアウトを秒単位で指定します。デフォルトは **120** です。
- キー：カスタムキー
- キー：**hibernate.c3p0.timeout**
- 値：**120**
- 表示名：**hibernate.c3p0.timeout**
- 説明：データベースアイドルタイムアウト

テレメトリが有効かを特定します

- 利用統計情報（カスタマーエクスペリエンス向上プログラム、すなわち CEIP）が有効かどうかを指定します。XenMobile のインストールまたはアップグレード時に CEIP にオプトインすることができます。XenMobile が連続して 15 回アップロードを失敗した場合、利用統計情報は無効になります。デフォルトは **false** です。

無操作状態によるタイムアウト（分）

- サーバープロパティ **WebServices timeout type** が **INACTIVITY_TIMEOUT** に設定されている場合：このプロパティで、次の条件を満たす非アクティブな管理者が XenMobile からログアウトされるまでの分数を指定します：
  - REST サービス用の XenMobile パブリック API を使用して XenMobile コンソールにアクセスした
  - REST サービス用の XenMobile パブリック API を使用してサードパーティアプリにアクセスした。タイムアウト値が **0** の場合、非アクティブなユーザーはログインしたままになります。

デフォルトは **5** です。

iOS デバイス管理登録：自動インストールを有効にする

- true の場合、このプロパティはデバイスの登録中に必要なユーザー操作の量を削減します。ユーザーは ［ルート **CA** のインストール］（必要に応じて）および ［**MDM** プロファイルのインストール］ をクリックする必要があります。

iOS デバイス管理登録：最初の手順の遅延

- この値では、ユーザーがデバイス登録で資格情報を入力した後にルート CA を要求するメッセージが表示されるまでの待機時間を指定します。このプロパティは、ネットワーク遅延またはスピードの問題がある場合のみ編集することをお勧めします。編集する場合は、5000 ミリ秒（5 秒）を超える値を設定しないでください。デフォルトは **1000** ミリ秒（1 秒）です。

iOS デバイス管理登録：最後の手順の遅延

- デバイスの登録中、このプロパティの値は MDM プロファイルのインストールからデバイスでエージェントを開始するまでの待機時間を指定します。このプロパティは、ネットワーク遅延またはスピードの問題がある場合のみ編集することをお勧めします。編集する場合は、5000 ミリ秒（5 秒）を超える値を設定しないでください。デフォルトは **1000** ミリ秒（1 秒）です。

iOS デバイス管理：**ID** デリバリーモード

- XenMobile は、**SCEP**（セキュリティ上推奨される）または **PKCS12** を使用して MDM 証明書をデバイスに配布するかを指定します。PKCS12 モードの場合、サーバーでキーペアが生成され、ネゴシエーションは実行されません。デフォルトは **SCEP** です。

iOS デバイス管理：**ID** キーサイズ

- MDM ID、iOS プロファイルサービス、XeMobile iOS エージェント ID の秘密キーのサイズを定義します。デフォルトは **1024** です。

iOS デバイス管理：**ID** 更新日数

- 証明書の有効期限が切れる前に、XenMobile が証明書の更新を開始する秒数を指定します。たとえば、証明書が 10 日後に期限切れになり、このプロパティが **10** 日間に設定されている場合、デバイスが期限切れの 9 日前に接続すると XenMobile は新しい証明書を発行します。デフォルトは **30** 日間です。

iOS MDM APNS 秘密キーのパスワード

- このプロパティには、XenMobile が Apple サーバーに通知をプッシュするために必要な APNs パスワードが含まれます。

デバイスが切断されるまでの非アクティブ期間

- デバイスが XenMobile から切断されるまで非アクティブ状態（最後の認証を含む）でいられる期間を指定します。デフォルトは **7** 日間です。

MAM のみのデバイスの最大値

- このカスタムキーでは、各ユーザーが登録可能な MAM-only デバイスの数を制限します。このキーは次のように構成します。値を **0** にすると、デバイスを無制限に登録できます。
- キー = **number.of.mam.devices.per.user**
- 値 = **5**
- 表示名 = **MAM** のみのデバイスの最大値
- 説明 = 各ユーザーが登録できる **MAM** デバイスの数を制限します。

MaxNumberOfWorker

- 多数の VPP ライセンスをインポートする時に使用するスレッド数です。デフォルトは **3** です。さらに最適化が必要な場合は、スレッド数を増やすことができます。ただし、スレッド数を大きくする（6 など）と、VPP ライセンスのインポートにより CPU 使用率が非常に高くなります。

NetScaler シングルサインオン

- **False** の場合、NetScaler から XenMobile へのシングルサインオン時に XenMobile コールバック機能が無効にされます。コールバック機能は、NetScaler Gateway の構成でコールバック URL が設定されている場合に NetScaler Gateway のセッション ID の検証に使用されます。デフォルト値は **False** です。

連続して失敗したアップロードの数

- カスタマーエクスペリエンス向上プログラム（CEIP）アップロード中の連続失敗回数を表示します。アップロードが失敗した場合、XenMobile がこの値を増やします。アップロードが 15 回失敗すると、XenMobile によって CEIP（利用統計情報）が無効化されます。詳しくは、サーバープロパティの「テレメトリが有効かを特定する」を参照してください。アップロードが成功した場合、XenMobile によってこの値は **0** にリセットされます。

デバイスごとのユーザーの数

- モバイルデバイス管理（MDM：Mobile Device Management）に同じデバイスを登録できるユーザーの最大数。値 **0** は、無制限の数のユーザーが同じデバイスを登録できることを意味します。デフォルトは **0** です。

許可および禁止されたユーザーの増分変更の抽出

- ActiveSync デバイスの差分を取得する PowerShell コマンドを実行するときに、XenMobile がドメインからの応答を待機する秒数です。デフォルトは **60** 秒です。

Microsoft 証明書サーバーへの読み取りタイムアウト

- 読み取りを実行する場合、XenMobile が証明書サーバーからの応答を待つ秒数です。証明書サーバーの接続速度が遅く、トラフィックが多い場合、この値を 60 秒以上にすることができます。証明書サーバーが 120 秒経っても応答しない場合は、保守が必要です。デフォルトは **15000** ミリ秒（15 秒）です。

REST Web サービス

- RESTWeb サービスを有効化します。デフォルトは **true** です。

指定されたサイズのチャンクでデバイス情報を取得する

- この値は、デバイスのエクスポート中のマルチスレッド処理で内部的に使用されます。この値を大きくすると、単一のスレッドで解析できるデバイス数が増加します。この値を小さくすると、デバイスをフェッチするスレッド数が増加します。この値を小さくすると、エクスポートおよびデバイスリストのフェッチのパフォーマンスが向上する可能性がありますが、利用可能なメモリが減少する可能性もあります。デフォルトは **1000** です。

セッションログのクリーンアップ（日）

- XenMobile にセッションログが保持される日数です。デフォルトは **7** です。

サーバーモード

- アプリ管理、デバイス管理、またはアプリおよびデバイス管理に対応して、XenMobile を MAM、MDM、または ENT（エンタープライズ）のいずれのモードで実行するかを指定します。次の表に示すように、デバイスの登録方法に応じて、サーバーモードプロパティを設定します。サーバーモードの既定値は、ライセンスの種類にかかわらず **ENT** です。

XenMobile MDM Edition のライセンスがある場合は、サーバープロパティに設定するサーバーモードにかかわらず、有効なサーバーモードは常に MDM です。これは、MDM エディションの場合、サーバーモードを MAM または ENT に設定しても、アプリ管理を有効にできないことを意味します。

現在のライセンスのエディション	デバイスを登録するモード	必要なサーバーモードプロパティの設定
エンタープライズ/上級	MDM モード	MDM
エンタープライズ/上級	MDM+MAM モード	ENT
MDM	MDM モード	MDM

有効なサーバーモードとは、サーバーモードとインストールされているライセンスの種類の組み合わせです。MDM ライセンスの場合は、サーバーモードにかかわらず、有効なサーバーモードは常に MDM です。エンタープライズおよび上級ライセンスの場合、有効なサーバーモードはサーバーモードに一致します（サーバーモードが **ENT** または **MDM** の場合）。サーバーモードが **MAM** の場合、有効なサーバーモードは ENT です。

ライセンスのアクティブ化、ライセンスの削除、およびサーバープロパティでのサーバーモードの変更が行われるたびに、サーバーログにサーバーモードが追加されます。ログファイルの作成と表示の詳細については、「ログ」および「XenMobile でのログファイルの表示および分析」を参照してください。

ShareFile の構成の種類

- ShareFile のストレージの種類を指定します。［エンタープライズ］ では、ShareFile Enterprise モードが有効になります。［コネクタ］ では、アクセス先が XenMobile コンソールで作成した StorageZone コネクタのみに制限されます。デフォルトは ［なし］ で、［構成］ **>** ［**ShareFile**］ 画面の初期表示が表示されます。この画面では、ShareFile Enterprise とコネクタの選択を行います。デフォルトは ［なし］ です。

静的タイムアウト（分）

- **WebServices timeout type** サーバープロパティが **STATIC_TIMEOUT** に設定されている場合：このプロパティで、管理者が次のいずれかの操作を行った後に XenMobile からログアウトされるまでの分数を指定します。
  - REST サービス用の XenMobile パブリック API を使用して XenMobile コンソールにアクセスする
  - REST サービス用の XenMobile パブリック API を使用してサードパーティアプリにアクセスする

デフォルトは **60** です。

エージェントメッセージの無効化をトリガーする

- Secure Hub クライアントのメッセージを有効または無効にします。値を **false** に設定すると、メッセージが有効になります。デフォルトは **true** です。

エージェントのサウンドの無効化をトリガーする

- Secure Hub クライアントのサウンドを有効または無効にします。値を **false** に設定すると、サウンドが有効になります。デフォルトは **true** です。

認証されていない **Android** デバイス用アプリのダウンロード

- **True** の場合、セルフホストされたアプリを、Android Enterprise を実行している Android デバイスにダウンロードできます。このプロパティは、Google Play Store で静的にダウンロード URL を提供する Android Enterprise オプションが有効になっている場合に必要となります。この場合、ダウンロード URL に認証トークンを含む（**XAM One-Time Ticket** サーバープロパティによって定義された）ワンタイムチケットを含めることはできません。デフォルト値は **False** です。

認証されていない **Windows** デバイス用アプリのダウンロード

- ワンタイムチケットが検証されない古い Secure Hub バージョンでのみ使用されます。**False** の場合、XenMobile から Windows デバイスに、未認証のアプリをダウンロードできます。デフォルト値は **False** です。

ActiveSync ID を使用して **ActiveSync** デバイスをワイプする

- **true** の場合、Endpoint Management コネクタ: Exchange ActiveSync 用は、ActiveSync 識別子を asWipeDevice メソッドの引数として使用します。デフォルトは **false** です。

ユーザー定義のデバイスプロパティ **N**

- Windows CE デバイスにのみ使用します。このカスタムキーを使用すると、Windows CE デバイスのレジストリで作成したプロパティを取得できます。XenMobile データベースにこれらのプロパティを格納したら、プロパティの値に基づいて展開規則を作成できます。
- キー：カスタムキー
- キー：**device.properties.userDefinedN**
- 値：管理者定義

- 表示名：管理者定義
- 説明：管理者定義

Exchange のみのユーザー

- **true** の場合、Exchange ActiveSync ユーザーに対するユーザー認証を無効化します。デフォルトは **false** です。

VPP 基準間隔

- XenMobile が VPP ライセンスを Apple から再インポートする最小間隔です。ライセンス情報を更新することにより、XenMobile にすべての変更が反映されます（インポートされたアプリを VPP から手動で削除した場合など）。デフォルトで、XenMobile は VPP ライセンスベースラインを最低 **720** 分ごとに更新します。

多数の VPP ライセンスをインストールしている場合（たとえば、50,000 個以上）、ベースライン間隔を広げてライセンスをインポートする頻度とオーバーヘッドを減らすことをお勧めします。Apple からの頻繁な VPP ライセンス変更が予想される場合は、変更に対して XenMobile が最新状態を維持できるよう、この値を下げることをお勧めします。2 つのベースライン間の最小間隔は 60 分です。また、XenMobile は 60 分ごとに差分インポートを実行して前回のインポートからの変更を取得します。このため、VPP のベースライン間隔が 60 分の場合、ベースライン間の間隔は最大 119 分開く可能性があります。

WebServices Timeout Type

- パブリック API から取得する認証トークンが期限切れになる方法を指定します。**STATIC_TIMEOUT** の場合、サーバープロパティ **Static Timeout in Minutes** に値が指定されると、XenMobile は認証トークンを期限切れと見なします。

INACTIVITY_TIMEOUT の場合、サーバープロパティ **Inactivity Timeout in Minutes** に指定された間非アクティブであれば、XenMobile は認証トークンを期限切れと見なします。デフォルトは **STATIC_TIMEOUT** です。

Windows Phone MDM 証明書の延長検証（**5** 年）

- Windows Phone およびタブレットで MDM から発行されたデバイス証明書の有効期限です。デバイスは、デバイス管理中はデバイス証明書を使用して MDM サーバーへの認証を行います。**true** の場合、有効期限は 5 年間になります。**false** の場合、有効期限は 2 年間になります。デフォルトは **true** です。

Windows WNS Channel - Number of Days Before Renewal

- ChannelURI の更新間隔。デフォルトは **10** 日間です。

Windows WNS Heartbeat Interval

- XenMobile で 3 分ごとのデバイスへの接続を 5 回行った後に再びデバイスへ接続するまでの待機時間です。デフォルトは **6** 時間です。

XAM ワンタイムチケット

- アプリをダウンロードするときのワンタイム認証トークン（OTT：One-Time Authentication Token）の有効時間（ミリ秒）です。このプロパティは、認証されていない **Android** デバイス用アプリのダウンロードプロパティおよび認証されていない **Windows** デバイス用アプリのダウンロードプロパティとともに使用されます。これらのプロパティにより、未認証アプリのダウンロードを許可するかどうかを指定します。デフォルトは **3600000** です。

XenMobile MDM Self Help Portal コンソールの最大非アクティブ間隔 **(**分**)**

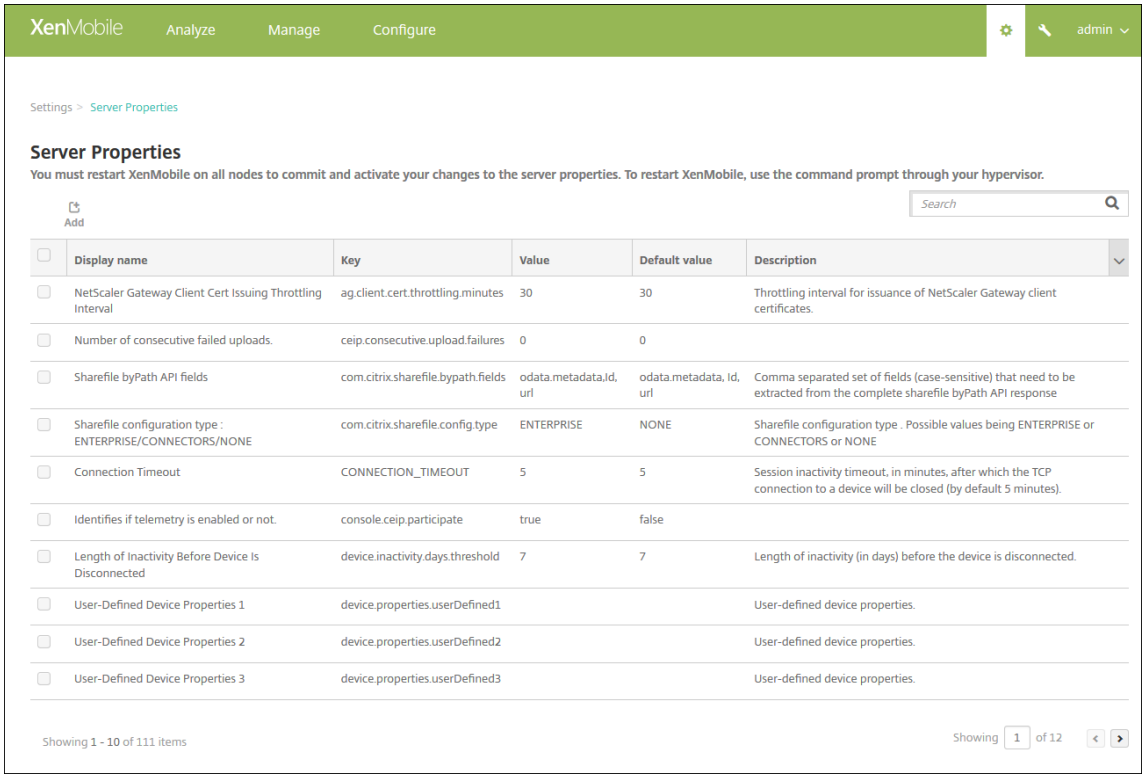
- 非アクティブなユーザーが XenMobile Self-Help Portal からログアウトされるまでの分数です。タイムアウトが **0** の場合、 非アクティブなユーザーはログインしたままになります。デフォルトは **30** です。

サーバープロパティを追加、編集、または削除するには

XenMobile で、サーバーにプロパティを適用できます。変更後は、すべてのノードで XenMobile を再起動し、変更を確定して有効化してください。

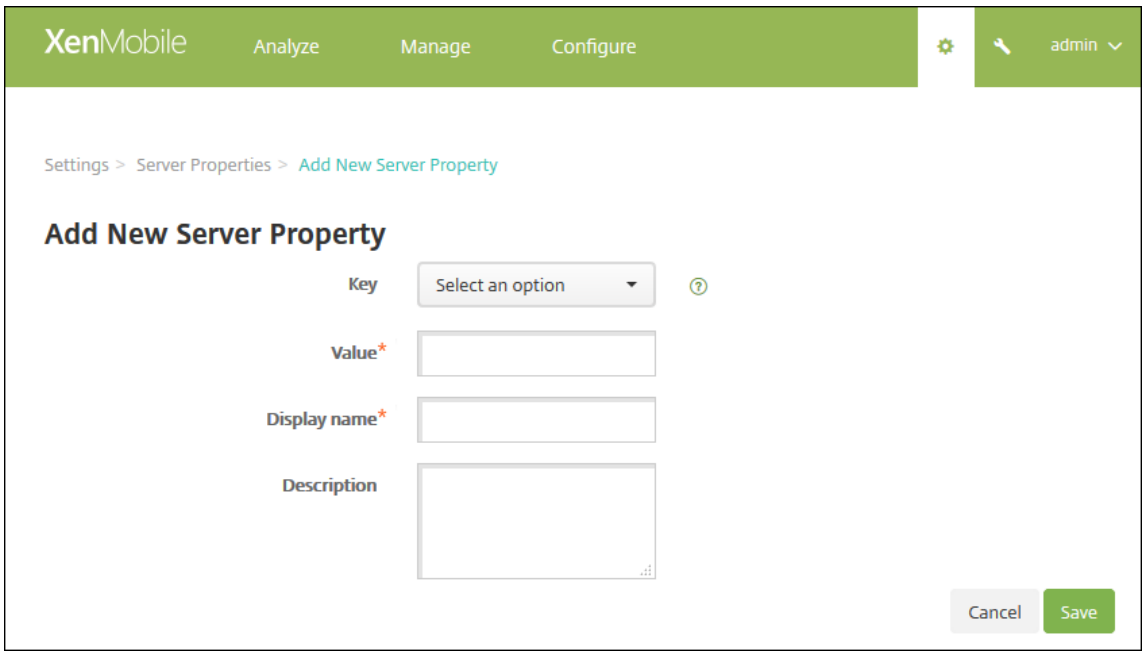
> 注:
>
> XenMobile を再起動するには、ハイパーバイザーからコマンドプロンプトを使用します。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［サーバープロパティ］ をクリックします。［サーバープロパティ］ ページが開きます。このページでは、サーバープロパティを追加、編集、または削除できます。



サーバープロパティを追加するには

1. [追加] をクリックします。[新しいサーバープロパティの追加] ページが開きます。



2. 次の設定を構成します。

- キー: 一覧から、適切なキーを選択します。キーでは大文字と小文字が区別されます。プロパティの値を編集する前にシトリックスサポートに問い合わせるか、特殊キーをリクエストしてください。
- 値: 選択したキーに応じて値を入力します。
- 表示名: ［サーバープロパティ］ の表に表示される、新しいプロパティ値の名前を入力します。
- 説明: 任意で、新しいサーバープロパティの説明を入力します。

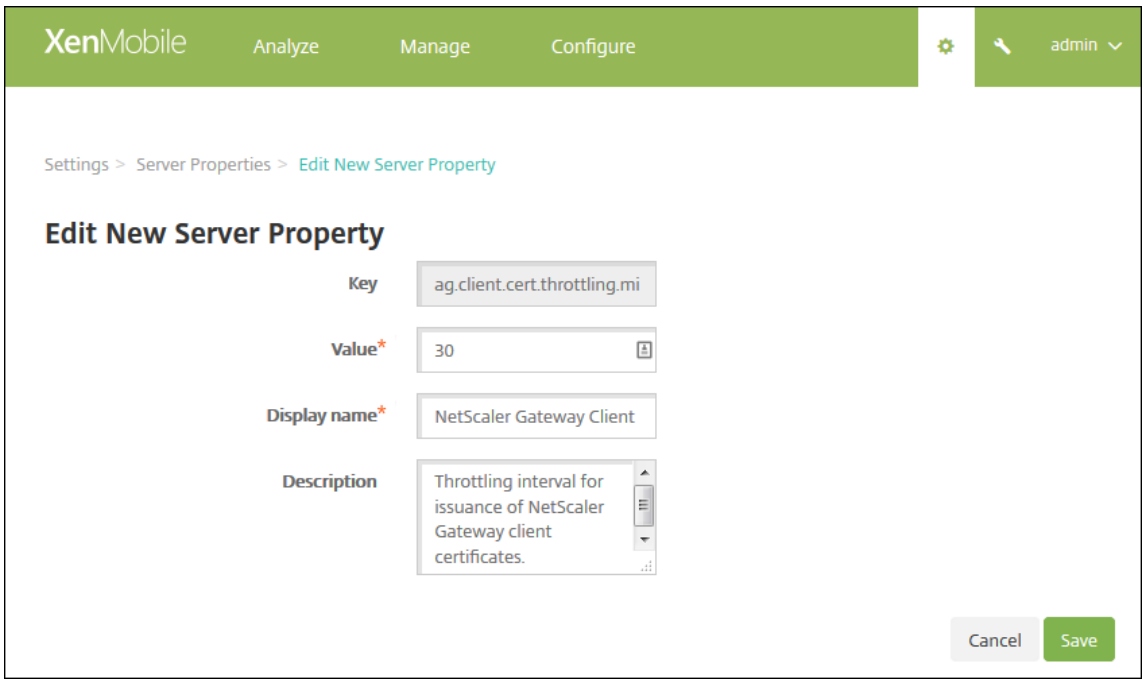
3. ［保存］ をクリックします。

サーバープロパティを編集するには

1. ［サーバープロパティ］ の表で、編集するサーバープロパティを選択します。

   サーバープロパティの横にあるチェックボックスをオンにすると、サーバープロパティ一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを開きます。

2. ［編集］ をクリックします。［新しいサーバープロパティの編集］ ページが開きます。



3. 必要に応じて以下の情報を変更します。

   - キー: このフィールドは変更できません。
   - 値: プロパティの値です。
   - 表示名: プロパティの名前です。
   - 説明: プロパティの説明です。

4. ［保存］ をクリックして変更を保存するか、［キャンセル］ をクリックしてプロパティを変更せずそのままにします。

サーバープロパティを削除するには

1. ［サーバープロパティ］ の表で、削除するサーバープロパティを選択します。

   各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。

2. ［削除］ をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］ をクリックします。

コマンドラインインターフェイスオプション

January 10, 2020

XenMobile Server のオンプレミスインストールについては、以下のように CLI オプションが利用できます:

- **XenMobile** をインストールしたハイパーバイザーから: ハイパーバイザーで、インポートした XenMobile 仮想マシンを選択してコマンドプロンプトビューを起動し、XenMobile の管理者アカウントにログオンします。詳しくは、ハイパーバイザーのドキュメントを参照してください。
- ファイアウォールで **SSH** が有効な場合、**SSH** を使用します: XenMobile の管理者アカウントにログオンします。

CLI を使用して、さまざまな構成タスクやトラブルシューティングを実行できます。以下の図は、CLI のトップレベルメニューです。

```
-----------------------------------
Main Menu
-----------------------------------
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----------------------------------
```

構成オプション

以下は、［**Configuration**］メニューと、各オプションに表示される設定です。

```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```


[1] Network

```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  IP address [10.207.87.75]:10.200.87.75
  Netmask [255.255.254.0]:255.255.254.0
  Default gateway [10.207.86.1]:10.200.86.1
  Primary DNS server [10.207.86.50]:10.200.86.50
  Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]:
```

[2] Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
 - comma separated list of hosts or networks
 - e.g. 10.20.5.3, 10.20.6.0/24
 - an empty value means no access restriction
 - enter c as value to clear list

  HTTP service
    Port: 80
    Enable access (y/n) [y]: y
    Access white list []:

  Management HTTPS service
    Port: 4443
    Enable access (y/n) [y]:
    Access white list []:

  SSH service
    Port [22]:
    Enable access (y/n) [y]:
    Access white list []:

  Management API (for initial staging) HTTPS service
    Port [30001]:
    Enable access (y/n) [n]:

  Remote support tunnel
    Port [8081]:
    Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```


[3] Database

```
  Type: [mi]
  Use SSL (y/n) [n]:
  Server [10.207.86.64]:
  Port [1433]:
  Username [sa]:
  Password:
  Database name [RC]:

 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]:
```

[4] Listener Ports

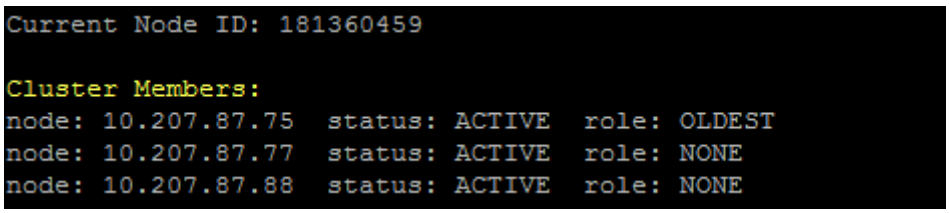
```
 Reboot is required to save the changes.
 Do you want to proceed? (y/n) [y]: y
  HTTP [80]:
  HTTPS with certificate authentication [443]:
  HTTPS with no certificate authentication [8443]:
  HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]:
```

［**Clustering**］オプション

以下は、［**Clustering**］メニューと、各オプションに表示される設定です。

```
-----------------------------------
Clustering Menu
-----------------------------------
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----------------------------------
```

[1] Show Cluster Status



[2] Enable/disable cluster

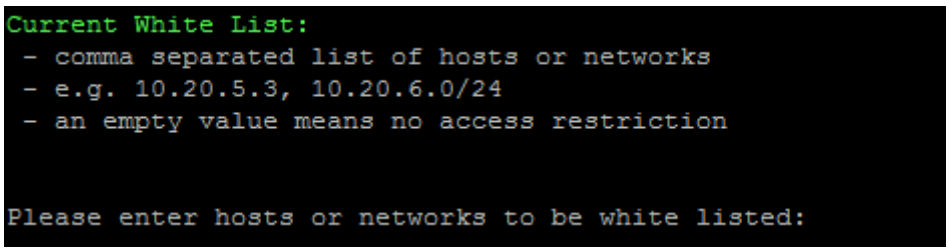
クラスタリングの有効化を選択すると、次のメッセージが表示されます。

```
To enable real-time communication between cluster members, please open port
 80 using the Firewall menu option in CLI menu. Also configure Access white
 list under Firewall settings for restricted access.
```

クラスタリングの無効化を選択すると、次のメッセージが表示されます。

```
You have chosen to disable clustering. Access to port 80 is not needed.
Please disable it.
```

[3] Cluster member white list



[4] Enable or disable SSL offload

SSL オフロードの有効化または無効化を選択すると、次のメッセージが表示されます。

```
Enabling SSL offload opens port 80 for everyone. Please configure Access
white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster

Hazelcast クラスターの表示を選択した場合は、次のオプションが表示されます。

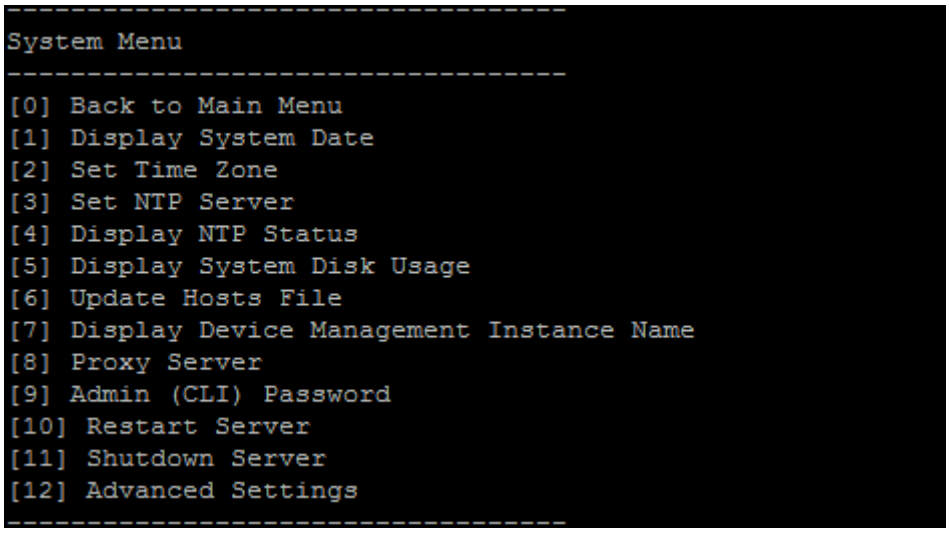
Hazelcast Cluster Members:

[IP addresses listed]

> 注：
>
> 構成されたノードがクラスターの一部ではない場合、そのノードを再起動してください。

［**System**］オプション

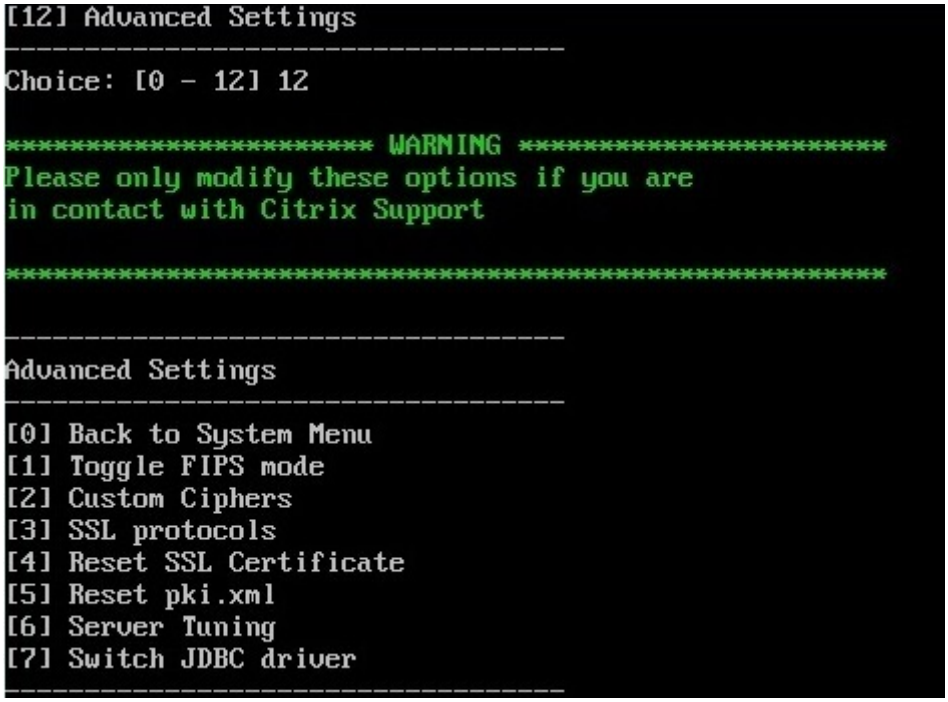
［**System Menu**］から、システムレベルの情報の表示や設定、サーバーの再起動またはシャットダウン、［**Advanced Settings**］ へのアクセスを実行できます。



NTP サーバーを設定して、NTP サーバー情報を指定できます。XenMobile の時間とハイパーバイザーの同期でタイムゾーンの問題が発生する場合、XenMobile が NTP サーバーを参照するようにして、これを回避できます。このオプションを変更した後は、すべてのクラスタサーバーを再起動します。

[5] Display System Disk Usage メニューアイテムを表示して、ディスクスペースを確認することもできます。

[12] Advanced Settings



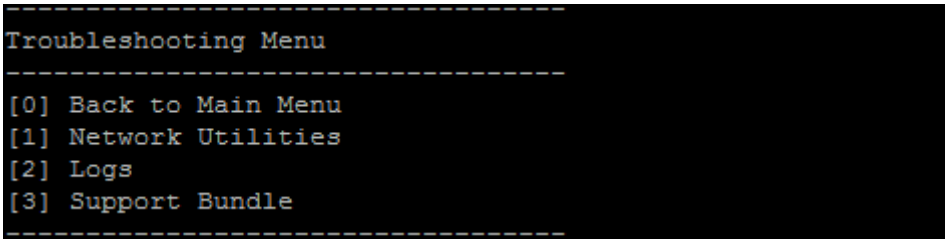
［**SSL protocols**］オプションが、すべての許可されたプロトコルのデフォルトになります。［**New SSL protocols to enable**］ プロンプトの後に、有効にするプロトコルを入力します。XenMobile はそのときに入力しなかったプロトコルを無効にします。たとえば、TLSv1 を無効にするには、「**TLSv1.2,TLSv1.1**」と入力し、「**y**」と入力して XenMobile Server を再起動します。

［**Server Tuning**］ オプションには、サーバー接続のタイムアウト、最大接続数（ポートごと）、最大スレッド数（ポートごと）が含まれます。

［**Switch JDBC driver**］オプションには、**jTDS** と **Microsoft** JDBC があります。デフォルトのドライバーは jTDS です。Microsoft JDBC ドライバーへの切り替えについては、「SQL Server のドライバー」を参照してください。

［**Troubleshooting**］オプション

以下は、［**Troubleshooting**］ メニューと、各オプションに表示される設定です。



[1] Network Utilities

```
-----------------------------------
Network Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Network Information
[2] Show Routing Table
[3] Show Address Resolution Protocol (ARP) Table
[4] PING
[5] Traceroute
[6] DNS Lookup
[7] Network Trace
-----------------------------------
```

[2] ログ

```
-----------------------------------
Logs Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display Log File
-----------------------------------
```

[3] Support Bundle

```
-----------------------------------
Support Bundle Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----------------------------------
```

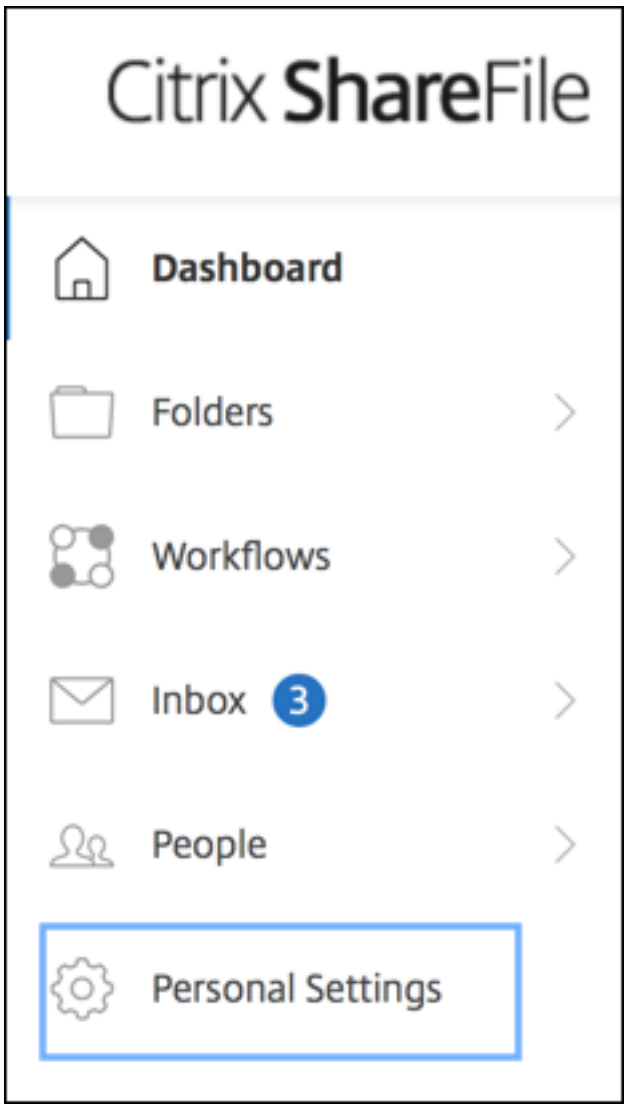
ShareFile を **FTP** サイトとして使用してサポートバンドルをアップロードするには

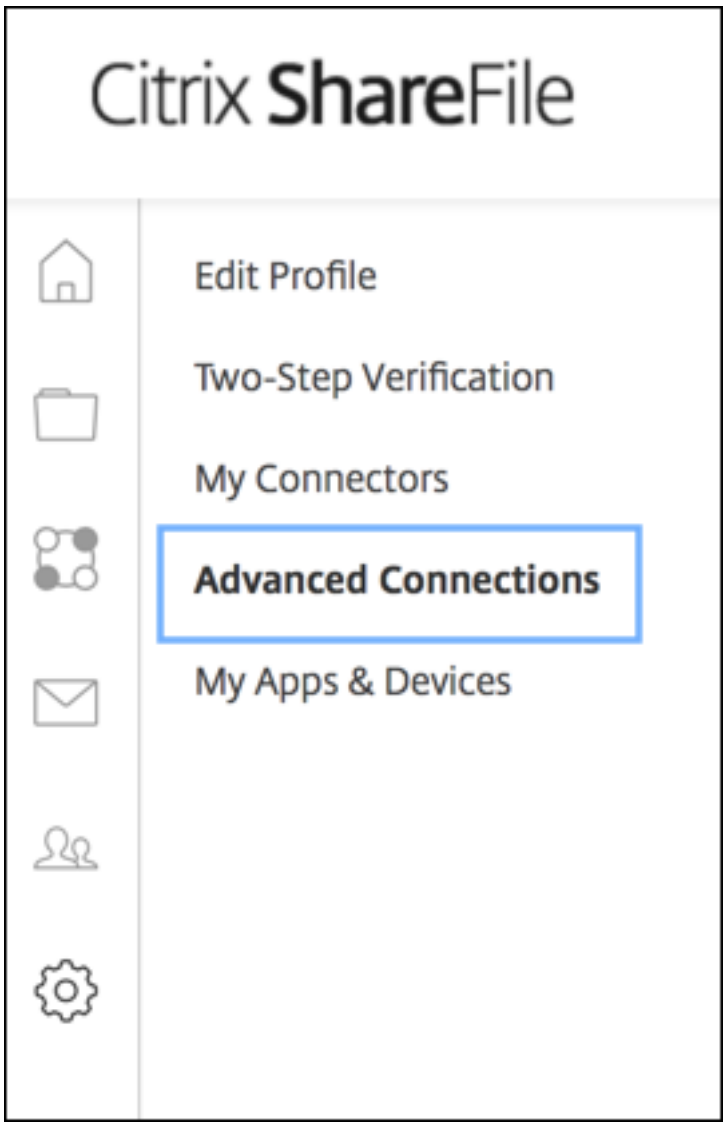
サポートバンドルのアップロードを開始する前に、ShareFile で次の前提条件を構成します:

1. FTP ログオンの詳細を確認します。

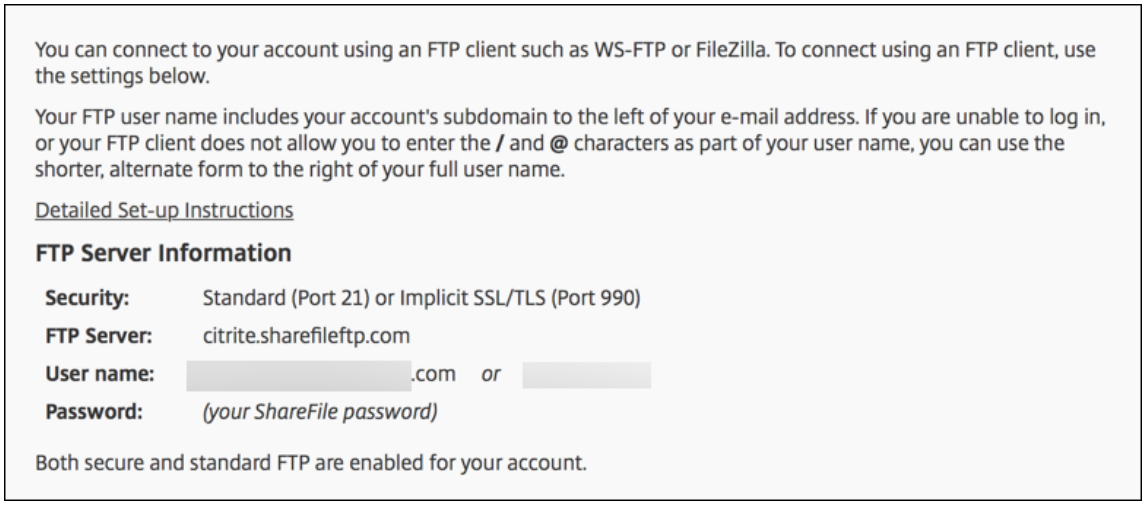
   a. Web ブラウザーで、https://citrix.sharefile.comを開きます。

   b. ［個人設定］ 、［高度な接続］ の順にクリックします。





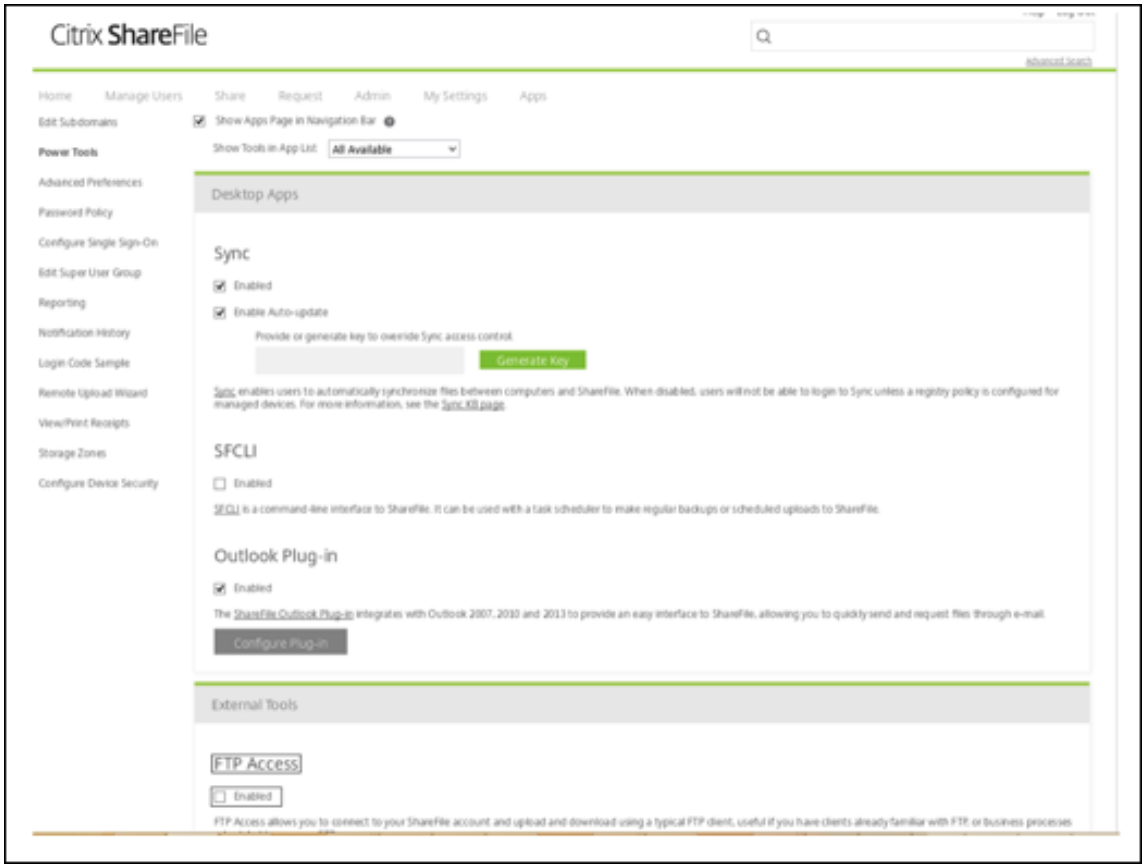
c. ［FTP Server Information］で、［User name」に英数字のユーザー ID とデフォルトのサブドメイン/ユーザー名の詳細が表示されていることを確認します。



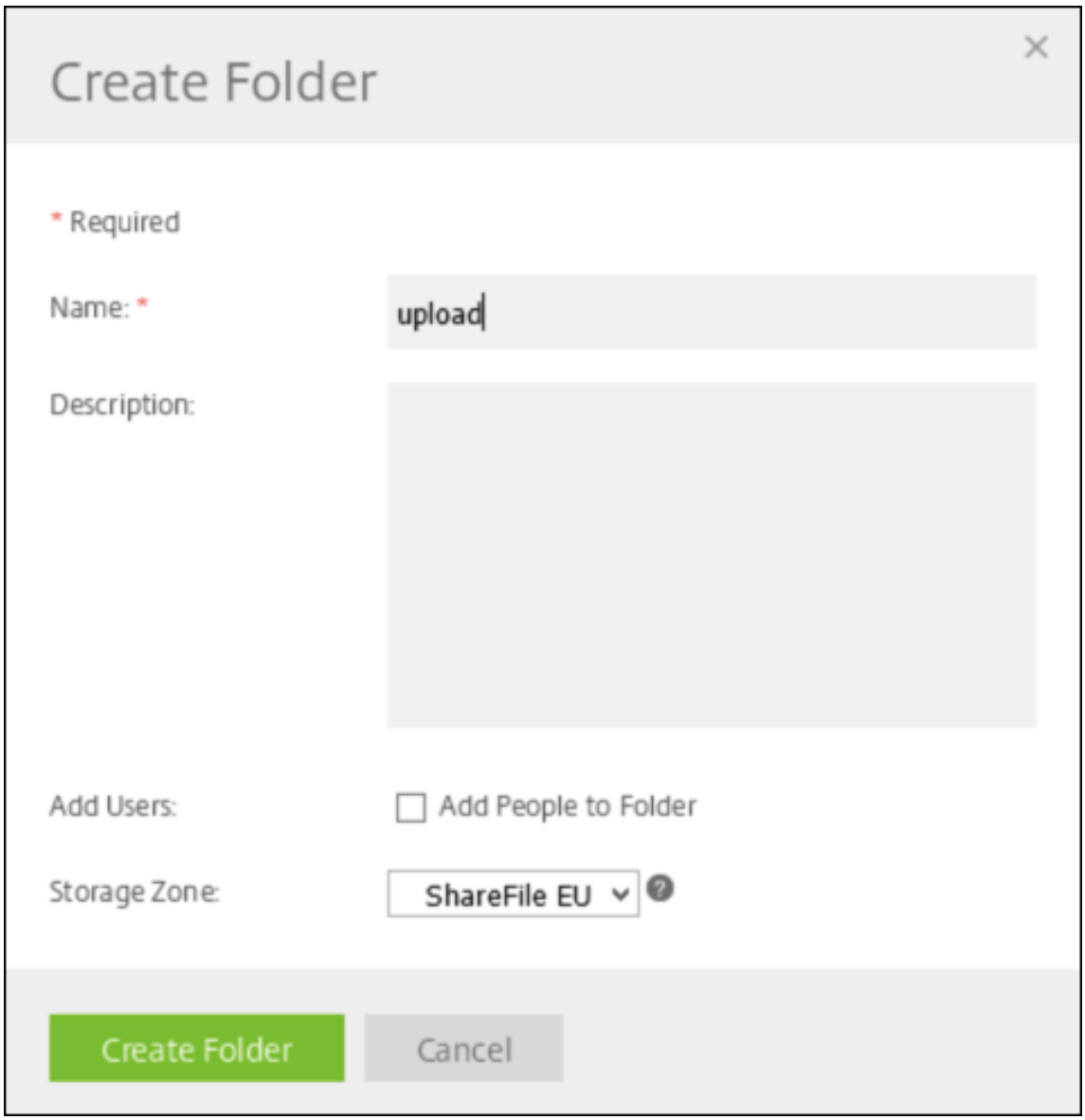
> 注:
>
> - ユーザー名にバックスラッシュ（/）とアットマーク（@）文字を含めることはできません。これは、Linux CLI ベースの FTP クライアントである XenMobile からファイルをアップロードするためです。
> - 英数字のユーザー ID が表示されていない場合は、ShareFile 管理者または ShareFile サポートに問い合わせてください。

2. ShareFile サーバーで FTPS と FTP 通信が有効になっていることを確認します。可能であれば、ShareFile 管理者は FTP 通信が許可されたユーザーアカウントを開くことができます。ただし、場合によっては FTPS 通信のみが許可されます。

   管理者権限を持つユーザーは、［設定］、［管理設定］、［高度な設定］、［**ShareFile** ツールを有効にする］の順にクリックして、この設定を確認して有効化することができます。［外部アプリ］の［**FTP Access**］で、［有効］ チェックボックスをオンにします。



3. FTP クライアントがファイルアップロード用のディレクトリとして使用する共有フォルダーを作成します。［ホーム］、［フォルダー］、［個人用フォルダー］ の順にクリックします。
4. 右端のプラス記号（+）をクリックし、［フォルダーの作成］ をクリックしてフォルダーに付ける名前を入力します。



5. XenMobile Server CLI で、［**Main Menu**］ から ［**Troubleshooting**］**>**［**Support Bundle**］ の順に選択します。次に、［**Support Bundle Menu**］ で ［**Generate Support Bundle**］ を選択します。

> 注:
>
> 既存のサポートバンドルがある場合、プロンプトの後に「**y**」を入力してバンドルを上書きします。

6. サポートバンドルを FTP サーバーにアップロードします:

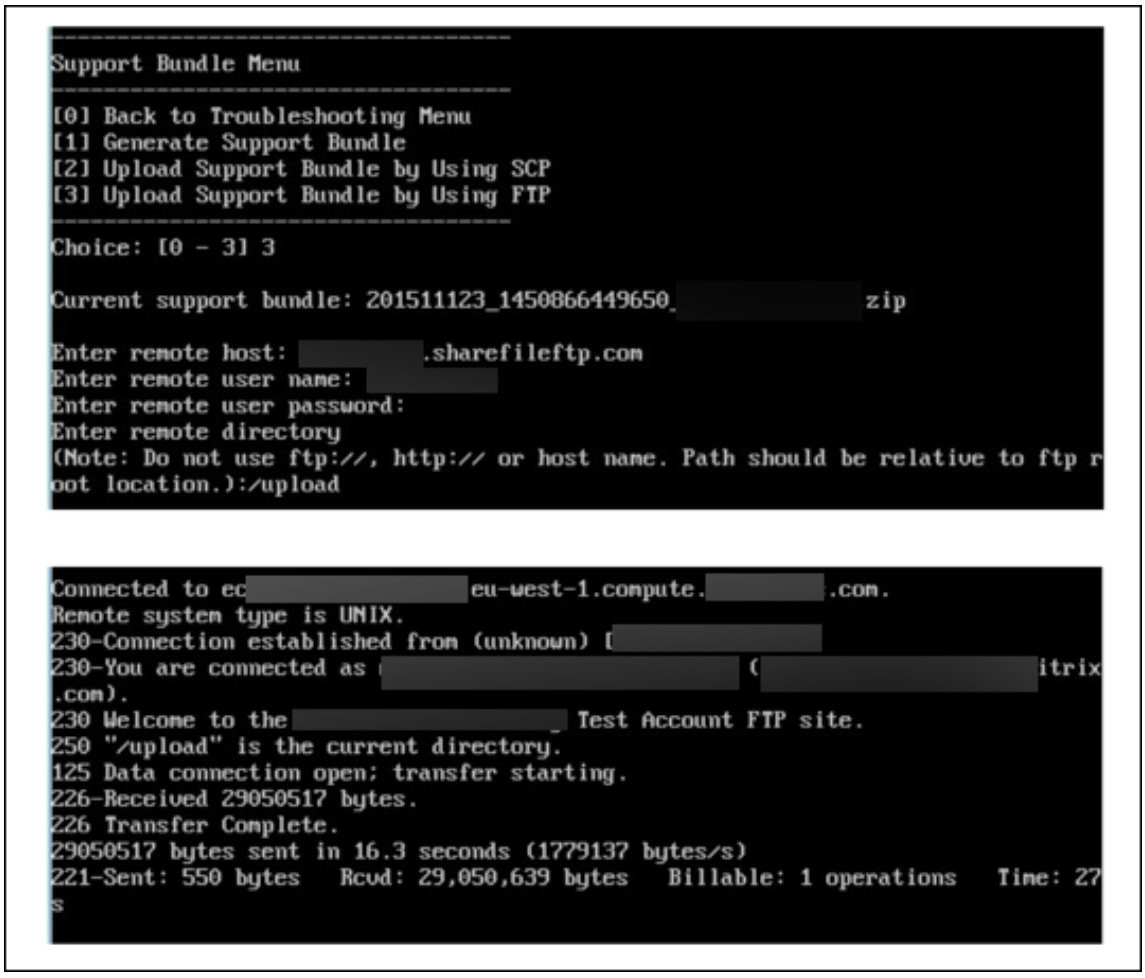
   a.［**Upload Support Bundle by using FTP**］ を選択します。

   b.［**Enter remote host**］のプロンプトの後に、FTP サーバー名を入力します。ShareFile を FTP サーバーとして使用する場合は、会社名の後に Sharefile FTP サイト名を入力します。例: citrix.sharefileftp.com。

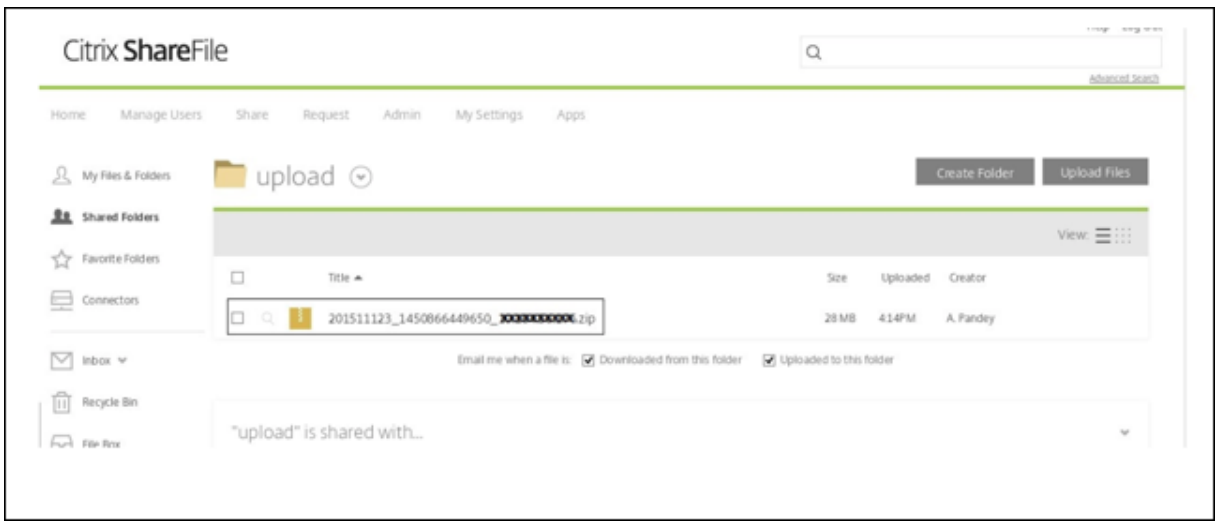
   c.［**Enter remote user name**］ のプロンプトの後に、英数字のユーザー ID を入力します。

d. [**Enter remote user password**] のプロンプトの後に、パスワードを入力します。

e. [**Enter remote directory**] のプロンプトの後に、ShareFile で作成した共有フォルダー名を入力して **Enter** キーを押します。



アップロードされたサポートバンドルが ShareFile で作成した共有フォルダーに表示されます。



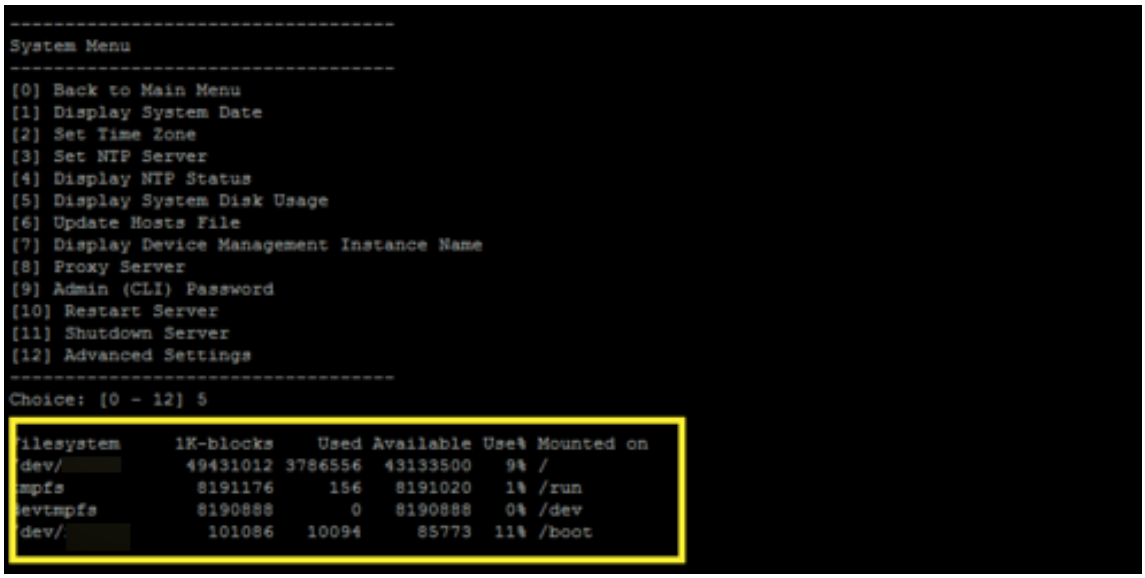
ShareFile FTP について詳しくは、このCitrix Support Knowledge Center の記事を参照してください。

ディスクスペースを確認するには

CLI でシステムディスクのディスクスペースを確認するには、以下の手順を実行します:

1. メインメニューの **System** Menu を選択します。
2. **System** Menu で **Display System Disk Usage** オプションを選択します。

   ファイルのシステム情報が表示されます。



XenMobile コンソールの導入ワークフロー

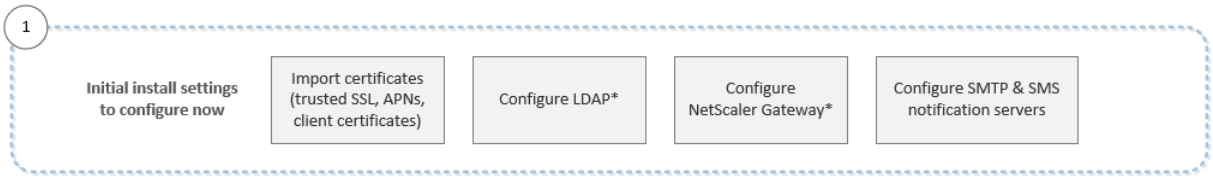
October 25, 2019

XenMobile コンソールは、XenMobile の統合管理ツールです。ここでの説明は、XenMobile がインストール済みで、コンソールで作業できる状態になっていることが前提となっています。XenMobile をまだインストールしていない場合は、「XenMobile のインストール」を参照してください。XenMobile コンソールのブラウザーサポートについて詳しくは、「XenMobile の互換性」を参照してください。

初期設定のワークフロー

最初にコマンドラインコンソールで XenMobile の構成を完了したら、次に XenMobile コンソールのダッシュボードが開きます。初期構成画面に戻ることはできません。インストール構成を一部スキップした場合、次の設定をコンソールで構成できます。ユーザー、アプリケーション、デバイスの追加を開始する前に、これらのインストール設定を完了することを考慮してください。設定を開始するには、コンソールの右上にある歯車アイコンをクリックします。

> 注:
>
> アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下の Citrix 製品ドキュメントの記事やセクションを参照してください。

- 認証
- NetScaler Gateway と XenMobile
- 通知

Android、iOS、Windows プラットフォームをサポートするには、以下のアカウント関連のセットアップが必要です。

Android

- Google Play 資格情報を作成します。詳しくは、Google Play のリリースを参照してください。
- Android Enterprise 管理者アカウントを作成します。詳しくは、「Android Enterprise」を参照してください。
- Google でのドメイン名を検証します。詳しくは、「G Suite のドメイン所有権の確認」を参照してください。
- API を有効にして Android Enterprise のサービスアカウントを作成します。詳しくは、「Android Enterprise ヘルプ」を参照してください。

iOS

- Apple ID および開発者アカウントを作成します。詳しくは、Apple Developer Programの Web サイトを参照してください。
- Apple プッシュ通知サービス（APNs）証明書を作成します。XenMobile Server 展開で iOS デバイスを管理することを計画している場合は、Apple APN 証明書が必要です。Secure Mail の展開でプッシュ通知を使用する場合も、Apple APNs 証明書が必要です。Apple APNs 証明書の取得方法について詳しくは、Apple Push Certificates Portalを参照してください。XenMobile と APN について詳しくは、「APN 証明書」および「Secure Mail for iOS のプッシュ通知」を参照してください。
- Volume Purchase Program (VPP) の企業トークンを作成します。詳しくは、「Apple Volume Purchasing Program」を参照してください。

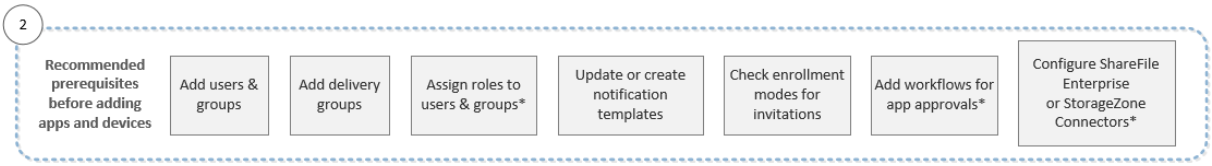
Windows

- Microsoft Windows ストア開発者アカウントを作成します。詳しくは、「アカウントの種類、場所、料金」を参照してください。
- Microsoft Windows ストア発行元 ID を入手します。詳しくは、「Manage account settings and profile info」を参照してください。
- DigiCert からエンタープライズ証明書を入手します。詳しくは、「Windows Phone 用の自社アプリの配布」を参照してください。
- Windows Phone の登録のために XenMobile 自動検出を活用したい場合は、パブリックな SSL 証明書を利用できるようにします。詳しくは、「XenMobile AutoDiscovery サービス」を参照してください。
- アプリケーション登録トークン（AET）を作成します。詳しくは、「Windows Phone 用のアプリケーション登録トークンを生成する方法」を参照してください。

コンソールの前提条件のワークフロー

このワークフローは、アプリケーションとデバイスを追加する前に構成する必要がある前提条件を示しています。

> 注:
>
> アスタリスクが付いている項目はオプションです。



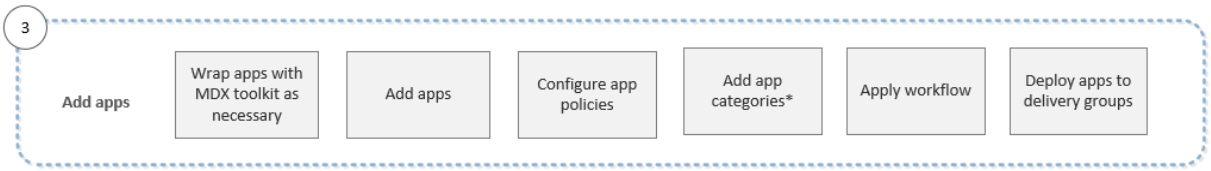
各設定の詳細と具体的な手順については、以下の Citrix 製品ドキュメントの記事やセクションを参照してください。

- ユーザーアカウント、役割、および登録
- リソースの展開
- RBAC を使用した役割の構成
- 通知
- ワークフローの作成および管理
- ShareFile を XenMobile と使用する

アプリケーションの追加のワークフロー

このワークフローは、XenMobile にアプリケーションを追加するときに従うことが推奨される順序を示しています。

> 注:
>
> アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下の Citrix 製品ドキュメントの記事やセクションを参照してください。

- MDX Toolkit について
- アプリの追加
- MDX ポリシーの概要
- ワークフローの作成および管理
- リソースの展開

デバイスの追加のワークフロー

このワークフローは、XenMobile にデバイスを追加して登録するときに従うことが推奨される順序を示しています。

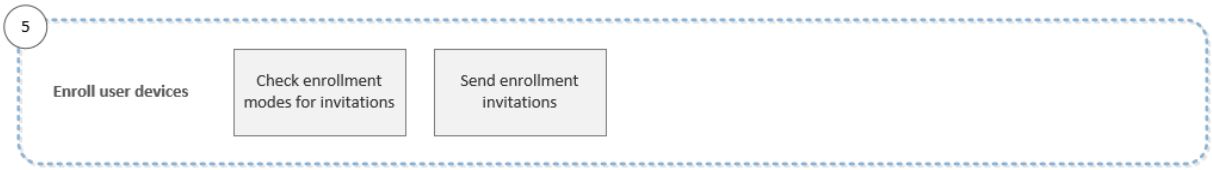
> 注:
>
> アスタリスクが付いている項目はオプションです。

各設定の詳細と具体的な手順については、以下の Citrix 製品ドキュメントの記事やセクションを参照してください。

- デバイス
- サポートされるデバイスオペレーティングシステム
- リソースの展開
- モニターとサポート
- 自動化された操作

ユーザーデバイスの登録のワークフロー

このワークフローは、XenMobile にユーザーデバイスを登録するときに従うことが推奨される順序を示しています。



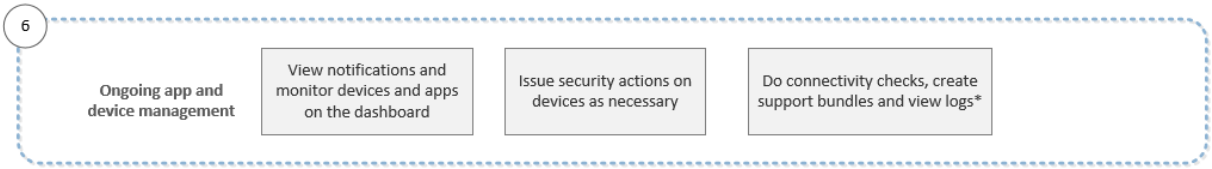
各設定の詳細と具体的な手順については、以下の Citrix 製品ドキュメントを参照してください。

- ユーザーアカウント、役割、および登録
- 通知

アプリケーションおよびデバイスの継続的な管理のワークフロー

このワークフローでは、コンソールで実行可能な、アプリケーションおよびデバイスの管理作業を示します。

> 注:
>
> アスタリスクが付いている項目はオプションです。



コンソールの右上のレンチアイコンをクリックすると表示されるサポートオプションについて詳しくは、「モニターとサポート」を参照してください。

証明書と認証

January 24, 2020

XenMobile の動作では、複数のコンポーネントが認証に関与します。

- **XenMobile Server**: XenMobile Server では、登録に関するセキュリティと登録の動作を定義します。導入するユーザーの選択肢には次が含まれます:
  - 登録を全員にオープンにするか、または招待のみにするか。
  - 2 要素認証または 3 要素認証を必須にするかどうか。XenMobile のクライアントプロパティを介して、Citrix PIN 認証を有効化して、PIN の複雑度や有効期限を構成できます。
- **NetScaler**: NetScaler はマイクロ VPN SSL セッションを終了させます。NetScaler はネットワーク転送中セキュリティも提供し、ユーザーがアプリにアクセスするたびに使用される認証エクスペリエンスを定義できるようにします。
- **Secure Hub**: Secure Hub と XenMobile Server は、登録操作で連携します。Secure Hub は NetScaler と通信するデバイス上のエンティティです。セッションが期限切れになると、Secure Hub は NetScaler から認証チケットを取得して、MDX アプリにチケットを渡します。中間者攻撃を防げる証明書ピン留めの使用をお勧めします。詳しくは、「Secure Hub」にある次のセクションを参照してください:「証明書ピンニング」

  Secure Hub では MDX セキュリティコンテナも容易になります。Secure Hub は、ポリシーをプッシュし、アプリがタイムアウトすると NetScaler でセッションを作成し、MDX タイムアウトおよび認証エクスペリエ

ンスを定義します。Secure Hub は、ジェイルブレイク検出、地理位置情報チェック、および適用するすべてのポリシーを担当します。

- **MDX** ポリシー： MDX ポリシーは、デバイス上にデータ格納場所を作成します。MDX ポリシーは、マイクロ VPN 接続に NetScaler を参照させ、オフラインモード制限を強制し、タイムアウトなどのクライアントポリシーを強制します。

1 要素または 2 要素による認証方法の概要など、認証の構成について詳しくは、『Deployment Handbook』の認証に関するトピックを参照してください。

XenMobile では証明書を使用し、セキュリティで保護された接続を作成してユーザーを認証します。この記事の残りの部分では、証明書について説明します。そのほかの構成について詳しくは、以下の記事を参照してください。

- ドメインまたはドメイン + セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- PKI エンティティ
- 資格情報プロバイダー
- APN 証明書
- ShareFile での SAML によるシングルサインオン
- Microsoft Azure Active Directory サーバー設定
- 証明書をデバイスに送信して Wi-Fi サーバーを認証するには：Wi-Fi デバイスポリシー
- 認証や特定のポリシーのために使用されていない一意の証明書をプッシュするには：資格情報デバイスポリシー

証明書

XenMobile では、サーバーへの通信フローを保護するため、インストール中に自己署名 SSL（Secure Sockets Layer）証明書が生成されます。この SSL 証明書を、既知の CA（Certificate Authority：証明機関）からの信頼される SSL 証明書に置き換える必要があります。

XenMobile はまた、独自の PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）サービスを使用するか、CA からクライアント証明書を取得します。すべての Citrix 製品でワイルドカード証明書と SAN（Subject Alternative Name：サブジェクトの別名）証明書がサポートされます。ほとんどの展開では、2 つのワイルドカード認証または SAN 認証のみが必要です。

クライアント証明書認証を使用するとモバイルアプリのセキュリティが強化され、ユーザーはシームレスに HDX アプリにアクセスできます。クライアント証明書認証が構成されている場合、ユーザーは XenMobile 準拠アプリへのシングルサインオン（SSO）アクセスには Citrix PIN を入力します。また Citrix PIN により、ユーザー認証工程が簡素化されます。Citrix PIN は、クライアント証明書をセキュリティで保護するため、または Active Directory 資格情報をデバイス上にローカルに保存するために使用されます。

XenMobile で iOS デバイスを登録して管理するには、Apple の Apple Push Notification Service（APNs）証明書を設定および作成します。手順については、「APN 証明書」を参照してください。

次の表は、各 XenMobile コンポーネントの証明書の形式と種類を示しています。

XenMobile コンポーネント	証明書の形式	必要な証明書の種類
NetScaler Gateway	PEM（BASE64）、PFX（PKCS # 12）	SSL、ルート（NetScaler Gateway によって自動的に PFX が PEM に変換されます）
XenMobile Server	.p12（Windows ベースのコンピューターの.pfx）	SSL、SAML、APN（XenMobile はインストール処理中に完全な PKI も生成します）重要：XenMobile Server では、拡張子「.pem」の証明書はサポートされません。.pem 証明書を使用するには、.pem ファイルを証明書とキーに分割し、それぞれを XenMobile Server にインポートします。
StoreFront	PFX（PKCS#12）	SSL、ルート

XenMobile は SSL リスナー証明書およびクライアント証明書をサポートします。ビット長は 4096、2048 および 1024 です。1024 ビットの証明書は簡単に改ざんされることに注意してください。

NetScaler Gateway および XenMobile Server の場合は、Verisign、DigiCert、Thawte などの商用 CA からサーバー証明書を取得することをお勧めします。NetScaler Gateway または XenMobile 構成ユーティリティから証明書署名要求（Certificate Signing Request：CSR）を作成できます。CSR の作成後、CA へ署名のために送信します。CA から署名入り証明書を受け取ったら、NetScaler Gateway または XenMobile に証明書をインストールできます。

> 重要：**iOS 13** および **macOS 15** での信頼された証明書の要件
>
> Apple は、TLS サーバー証明書の新しい要件を設定しています。すべての証明書が新しい Apple の要件に準拠していることを確認します。詳しくは、Apple のドキュメントhttps://support.apple.com/en-us/HT210176を参照してください。

XenMobile での証明書のアップロード

アップロードする各証明書は、［証明書］の表で 1 つのエントリを持ち、その内容がまとめられています。証明書が必要な PKI 統合コンポーネントを構成するときは、コンテキスト依存の条件を満たすサーバー証明書を選択します。たとえば、XenMobile を Microsoft CA と統合するように構成する場合があります。Microsoft CA への接続はクライアント証明書を使用して認証されます。

このセクションでは、証明書をアップロードする一般的な手順について説明します。クライアント証明書の作成、アップロード、構成について詳しくは、「クライアント証明書、または証明書とドメイン認証の組み合わせ」を参照して

ください。

秘密キーの要件

XenMobile は、特定の証明書に対して秘密キーを所有する場合と所有しない場合があります。同様に、XenMobile は、アップロードする証明書に対して秘密キーを要求する場合と要求しない場合があります。

コンソールへの証明書のアップロード

コンソールに証明書をアップロードする場合、主に 2 つのオプションがあります:

- クリックしてキーストアをインポートすることができます。次にインストールするキーストアリポジトリのエントリを識別します（PKCS#12 形式をアップロードする場合を除く）。
- クリックして証明書をインポートできます。

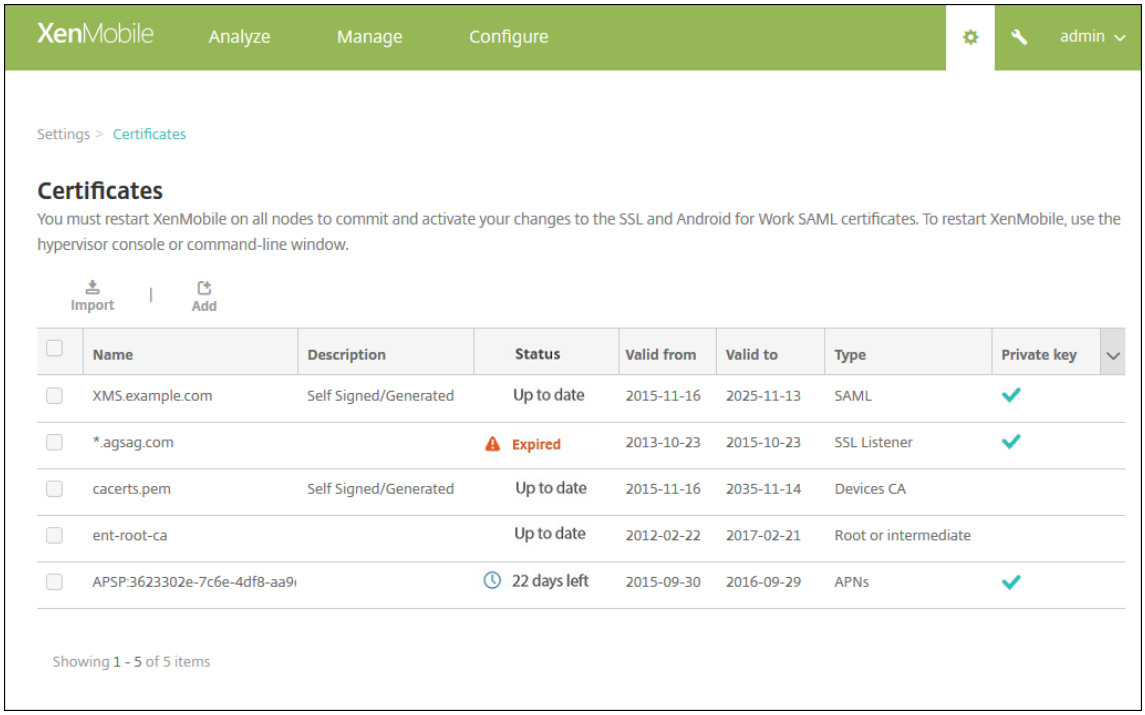
CA がリクエストに署名するときに使用する（秘密キーなしの）CA 証明書をアップロードすることができます。クライアント認証用の（秘密キー付きの）SSL クライアント証明書をアップロードすることもできます。

Microsoft CA エンティティを構成する場合は、CA 証明書を指定します。CA 証明書であるすべてのサーバー証明書の一覧から CA 証明書を選択します。同様に、クライアント認証を構成する場合は、XenMobile が秘密キーを持っているすべてのサーバー証明書の一覧から選択できます。

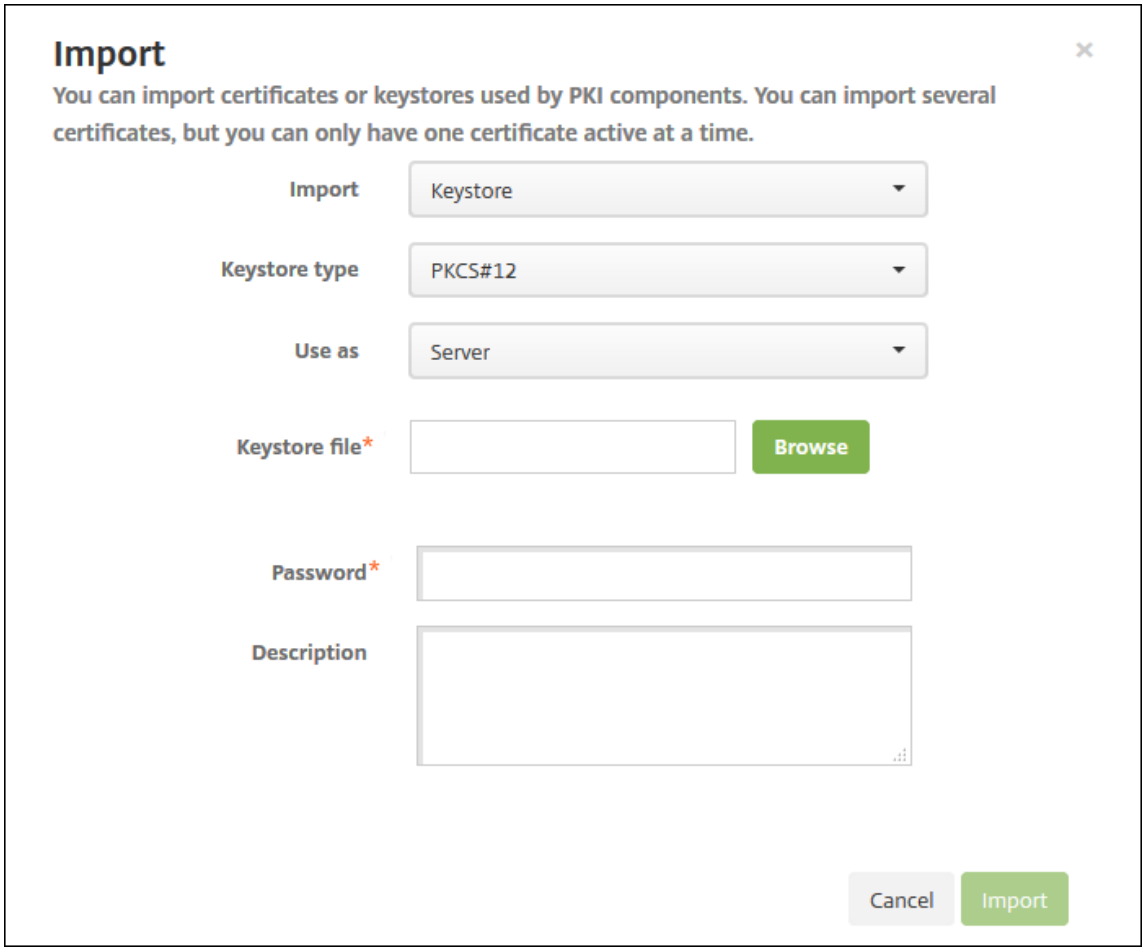
キーストアをインポートするには

設計上、セキュリティ証明書のリポジトリであるキーストアには、複数のエントリが含まれていることがあります。このため、キーストアから読み込むときに、読み込むエントリを識別するエントリエイリアスの指定を求めるメッセージが表示されます。エイリアスを指定しない場合、ストアの最初のエントリが読み込まれます。PKCS#12 ファイルに含まれるエントリは通常 1 つだけであるため、キーストアの種類として PKCS#12 を選択した場合、エイリアスフィールドは表示されません。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［証明書］ をクリックします。［証明書］ ページが開きます。



3. ［インポート］ をクリックします。［インポート］ ダイアログボックスが開きます。
4. 次の設定を構成します。
   - インポート： ボックスの一覧から、［キーストア］ を選択します。［インポート］ ダイアログボックスが、使用可能なキーストアオプションを反映した表示に変わります。



- キーストアの種類： ボックスの一覧から、［**PKCS#12**］ を選択します。
- 使用目的： 一覧から、証明書の使用方法を選択します。以下の種類から選択できます。
  - サーバー。サーバー証明書は XenMobile Server で機能上使用される証明書で、XenMobile Web コンソールにアップロードされます。サーバー証明書には、CA 証明書、RA 証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。これは特に、デバイスで信頼性を確立するために使用される CA に適用されます。
  - **SAML**。Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Web サイト、およびアプリへの SSO アクセスを提供できます。
  - **APNs**。Apple の APNs 証明書を使用すると、Apple Push Network を使用してモバイルデバイスを管理できます。
  - **SSL** リスナー。SSL（Secure Sockets Layer）リスナーは、XenMobile に SSL 暗号化アクティビティを通知します。
- キーストアファイル： インポートするファイル形式.p12（または、Windows ベースのコンピューターで.pfx）のキーストアを参照して指定します。
- パスワード： 証明書に割り当てられたパスワードを入力します。
- 説明： 任意で、キーストアの説明を入力します。この説明は、ほかのキーストアと区別するときに役立

ちます。

5.［インポート］ をクリックします。キーストアが［証明書］の表に追加されます。

証明書をインポートするには

ファイルまたはキーストアエントリから証明書をインポートするときに、XenMobile は入力から証明書チェーンの作成を試行します。XenMobile はそのチェーンのすべての証明書をインポートして、各証明書のサーバー証明書エントリを作成します。この操作は、ファイルまたはキーストアエントリの証明書がチェーンを形成する場合にのみ機能します。たとえば、チェーン内の連続する各証明書が前の証明書発行者である場合などです。

インポートされた証明書にオプションで説明を追加できます。説明はチェーンの 1 つ目の証明書にのみ追加されます。ほかの証明書の説明は後から更新できます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックした後、［証明書］ をクリックします。
2.［証明書］ ページで ［インポート］ をクリックします。［インポート］ ダイアログボックスが開きます。
3.［インポート］ ダイアログボックスの ［インポート］ の一覧から、まだ選択していない場合は ［証明書］ を選択します。
4.［インポート］ ダイアログボックスが、使用可能な証明書オプションを反映した表示に変わります。［使用目的］ で、キーストアの使用方法を選択します。以下の種類から選択できます。
   - サーバー。サーバー証明書は XenMobile Server で機能上使用される証明書で、XenMobile Web コンソールにアップロードされます。サーバー証明書には、CA 証明書、RA 証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。このオプションは特に、デバイスで信頼性を確立するために使用される CA に適用されます。
   - **SAML**。Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Web サイト、およびアプリへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
   - **SSL** リスナー。SSL（Secure Sockets Layer）リスナーは、XenMobile に SSL 暗号化アクティビティを通知します。
5. インポートするファイル形式.p12（または、Windows ベースのコンピューターで.pfx）のキーストアを参照して指定します。
6. 任意で、証明書の秘密キーファイルを参照して指定します。秘密キーは、証明書と共に暗号化と復号化で使用されます。
7. 任意で、証明書の説明を入力します。この説明は、ほかの証明書と区別するときに役立ちます。
8.［インポート］ をクリックします。証明書が［証明書］の表に追加されます。

証明書の更新

XenMobile で同時に存在できるのは 1 つの公開キーにつき 1 つの証明書のみです。既にインポートされている証明書と同じキーペアの証明書をインポートしようとする場合: 既存のエントリを置き換えるか、または削除することができます。

XenMobile コンソールで、証明書を最も効率的に更新するには、以下の手順に従います。コンソールの右上にある歯車アイコンをクリックして［設定］ページを開き、［証明書］をクリックします。［インポート］ダイアログボックスで、新しい証明書をインポートします。

サーバー証明書を更新すると、以前の証明書を使用していたコンポーネントが新しい証明書を使用するように自動的に切り替わります。同様に、デバイスにサーバー証明書を展開している場合、証明書は次回展開するときに自動的に更新されます。

証明書のリフレッシュ

XenMobile Server は、内部的に PKI のために次の認証機関を使用します: ルート CA、デバイス CA、およびサーバー CA。それらの CA は論理グループとして分類され、グループ名が与えられます。新しい XenMobile Server インスタンスがプロビジョニングされると、3 つの CA が生成され、グループ名が「default」になります。

サポートされている iOS、macOS、および Android デバイスの CA を更新するには、XenMobile サーバーコンソールまたは公開 REST API を使用します。登録済み Windows デバイスの場合、ユーザーは新しいデバイス CA を受信するためにデバイスを再登録する必要があります。

XenMobile サーバーで内部 PKI CA を更新または再生成し、これらの証明機関によって発行されたデバイス証明書を更新するには、次の API を使用します。

- 新しいグループ証明機関（CA）を作成します。
- 新しい CA をアクティブにし、古い CA を無効にします。
- 設定済みのデバイスリストでデバイス証明書を更新します。既に登録済みのデバイスは、中断することなく動作し続けます。デバイスがサーバーに接続すると、デバイス証明書が発行されます。
- 古い CA を使用しているデバイスのリストを返します。
- すべてのデバイスに新しい CA が割り当てられたら、古い CA を削除します。

詳しくは、「REST サービスのための XenMobile Public API」の PDF の次のセクションを参照してください:

```
1 - 第 3.16.58 項 「デバイス証明書の更新」
2 - 第 3.23 項 「XenMobile CA グループのリフレッシュ」
```

この機能の一部として、新しいセキュリティ操作である 証明書の書き換えを ［デバイスの管理］ コンソールから実行できます。この操作は、そのデバイス上の登録証明書を更新します。

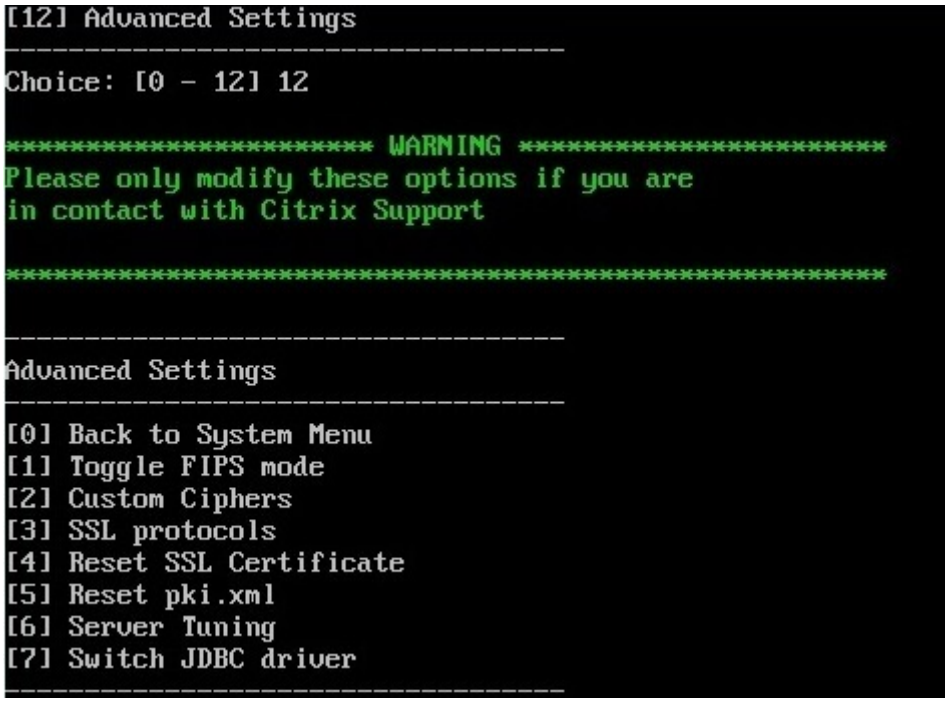
前提条件

- デフォルトでは、この証明書の書き換え機能は無効になっています。証明書の書き換え機能を有効にするには、サーバープロパティ **refresh.internal.ca** の値を **True** に設定します。

> 重要：
>
> NetScaler で SSL オフロードが設定されている場合は、新しい証明書を生成するときに、必ず新しい cacert.perm を使ってロードバランサーを更新してください。NetScaler Gateway の設定について詳しくは、「To use SSL Offload mode for NetScaler VIPs」を参照してください。

クラスタノードのサーバー **CA** 証明書パスワードをリセットする **CLI** オプション

1 つの XenMobile サーバーノードでサーバー CA 証明書を生成したら、XenMobile CLI を使用して他のクラスタノードの証明書パスワードをリセットします。CLI のメインメニューから、［システム］**>**［詳細設定］**>**［**CA** 証明書パスワードをリセットする］ を選択します。新しい CA 証明書がないときにパスワードをリセットしても、XenMobile はパスワードをリセットしません。



XenMobile 証明書の管理

XenMobile 展開で使用する証明書の情報、特に有効期限と関連パスワードを記録することをお勧めします。このセクションは、XenMobile で証明書をより簡単に管理する方法について説明します。

ご使用の環境には以下の一部、またはすべての証明書が含まれている可能性があります：

- XenMobile Server
  - MDM FQDN の SSL 証明書
  - SAML 証明書（ShareFile 用）
  - 上記証明書およびその他の内部リソース（StoreFront やプロキシなど）用のルート CA 証明書と中間 CA 証明書

  - iOS デバイス管理用の APN 証明書
  - XenMobile サーバー Secure Hub 通知用の内部 APN 証明書
  - PKI に接続するための PKI ユーザー証明書
- MDX Toolkit
  - Apple Developer 証明書
  - Apple プロビジョニングプロファイル（アプリケーションごと）
  - Apple APNS 証明書（Citrix Secure Mail で使用）
  - Android キーストアファイル
  - Windows Phone – DigiCert 証明書
- NetScaler
  - MDM FQDN の SSL 証明書
  - Gateway FQDN の SSL 証明書
  - ShareFile SZC FQDN の SSL 証明書
  - Exchange 負荷分散用の SSL 証明書（オフロード構成）
  - StoreFront 負荷分散用の SSL 証明書
  - 上記証明書のルート証明書および中間 CA 証明書

XenMobile 証明書の有効期限ポリシー

証明書の有効期限が切れると、証明書が無効になります。環境で安全なトランザクションを実行することや、XenMobile リソースにアクセスすることができなくなります。

> 注:
>
> 有効期限前に、証明機関（CA）から SSL 証明書を更新するよう求められます。

Citrix Secure Mail の **APN** 証明書

Apple プッシュ通知サービス（APNs）証明書は毎年有効期限が切れます。証明書の有効期限が切れる前に、APNs SSL 証明書を作成し、Citrix ポータルで証明書を更新してください。証明書の期限が切れた場合、Secure Mail プッシュ通知に一貫性がなくなります。また、アプリのプッシュ通知を送信することもできなくなります。

iOS デバイス管理用の **APN** 証明書

XenMobile で iOS デバイスを登録して管理するには、Apple の APNs 証明書を設定および作成します。証明書の期限が切れた場合、XenMobile に登録したり、iOS デバイスを管理したりできなくなります。詳しくは、「APN 証明書」を参照してください。

Apple Push Certificates Portal にログオンして、APNs 証明書のステータスと有効期限を表示できます。証明書を作成した時と同じユーザー名でログオンするようにしてください。

また、有効期限の 30 日前と 10 日前に、Apple からメール通知を受信します。この通知には、次の情報が含まれます:


```
The following Apple Push Notification Service certificate, created for
    Apple ID CustomerID will expire on Date. Revoking or allowing this
    certificate to expire will require existing devices to be re-
    enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR),
    then visit https://identity.apple.com/pushcert to renew your Apple
    Push Notification Service certificate.

Thank You,

Apple Push Notification Service
```

MDX Toolkit（iOS 配布証明書）

物理的な iOS デバイス（Apple App Store のアプリ以外）上で実行するアプリの署名要件は次のとおりです:

- プロビジョニングプロファイルでアプリに署名します。
- 対応する配布用証明書でアプリに署名します。

有効な iOS 配布証明書があるかを確認するには、以下の操作を行います:

1. Apple Enterprise Developer ポータルから、MDX Toolkit でラップする各アプリで新しいプロビジョニングプロファイルと一意で明示的な App ID を作成します。有効な App ID の例: `com.CompanyName.ProductName`
2. Apple Enterprise Developer ポータルから、［**Provisioning Profiles**］**>**［**Distribution**］に移動して、社内プロビジョニングプロファイルを作成します。前述の手順で作成された App ID ごとに、この手順を繰り返します。
3. すべてのプロビジョニングプロファイルをダウンロードします。詳しくは、「iOS モバイルアプリのラッピング」を参照してください。

すべての XenMobile Server 証明書が有効であることを確認するには、以下の操作を行います。

1. XenMobile コンソールで、［設定］**>**［証明書］の順にクリックします。
2. APNs 証明書、SSL 証明書、リスナー証明書、ルート証明書、中間証明書を含むすべての証明書が有効であることを確認してください。

Android キーストア

キーストアは Android アプリに署名するために使用する証明書を含むファイルです。キーの有効期間が切れると、アプリの新しいバージョンにシームレスにアップグレードできなくなります。

DigiCert の Windows Phone 用エンタープライズ証明書

DigiCert は、Microsoft App Hub サービスのコード署名証明書を提供する唯一のプロバイダーです。開発者およびソフトウェアの発行元は Microsoft App Hub に参加して、Windows Marketplace からダウンロードされる Windows Phone および Xbox 360 アプリケーションを配布します。DigiCert ドキュメントについて詳しくは、Windows Phone 用の DigiCert コード署名証明書を参照してください。

証明書の有効期限が切れた場合、Windows phone ユーザーは登録できません。ユーザーは同社が公開し署名したアプリのインストール、Windows phone にインストールされた会社のアプリの起動ができなくなります。

NetScaler

NetScaler の証明書の有効期限について詳しくは、Citrix Support Knowledge Center で「How to handle certificate expiry on NetScaler」を参照してください。

NetScaler 証明書の有効期限が切れると、ユーザーはストアに登録したり、アクセスすることができなくなります。Citrix Gateway 証明書の有効期限が切れると、ユーザは Secure Mail を使用するときに Exchange Server に接続することもできなくなります。また、ユーザーは（証明書の有効期限切れによって）HDX アプリを一覧にしたり起動することもできなくなります。

Expiry Monitor および Command Center によって、NetScaler 証明書の記録を確認できます。証明書の有効期限が切れると Command Center から通知が送信されます。これらのツールは、以下の NetScaler 証明書の監視に役立ちます:

- MDM FQDN の SSL 証明書
- Gateway FQDN の SSL 証明書
- ShareFile SZC FQDN の SSL 証明書
- Exchange 負荷分散用の SSL 証明書（オフロード構成）
- StoreFront 負荷分散用の SSL 証明書
- 上記証明書のルート証明書および中間 CA 証明書

NetScaler Gateway と XenMobile

January 10, 2020

XenMobile を使用して NetScaler Gateway を構成すると、リモートデバイスで内部ネットワークにアクセスするための認証メカニズムが確立されます。この機能を利用すると、モバイルデバイス上のアプリでイントラネット内にある社内サーバーにアクセスすることができます。XenMobile により、デバイス上のアプリから NetScaler Gateway への Micro VPN が作成されます。

XenMobile で使用する NetScaler Gateway を構成するには、NetScaler Gateway で実行するスクリプトを XenMobile からエクスポートします。

NetScaler Gateway 構成スクリプトを使用するための前提条件

NetScaler の要件

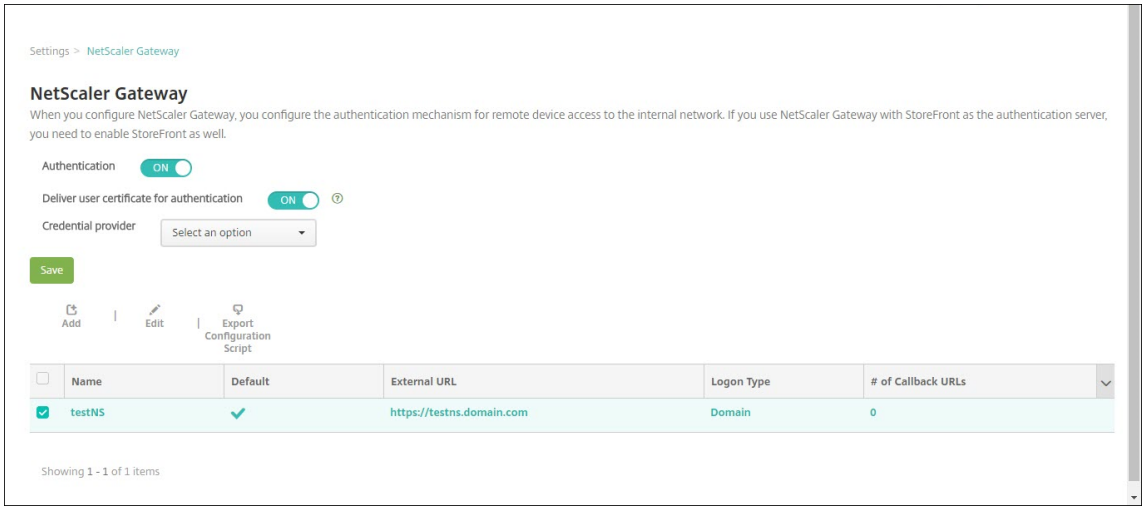
- NetScaler（最小バージョン 11.0、ビルド 70.12）
- NetScaler の IP アドレスが構成済みであり、LDAP サーバーに接続できる（LDAP が負荷分散されていない場合）
- NetScaler のサブネット IP（SNIP：Subnet IP）アドレスが構成済みであり、必要なバックエンドサーバーに接続でき、ポート 8443/TCP 経由でパブリックネットワークにアクセスできる
- DNS でパブリックドメインを解決できる
- NetScaler にプラットフォーム/ユニバーサルライセンスまたはトライアルライセンスが付与されている。詳しくは、「https://support.citrix.com/article/CTX126049」を参照してください。
- NetScaler Gateway の SSL 証明書を NetScaler でアップロードしインストールしている。詳しくは、https://support.citrix.com/article/CTX136023を参照してください。

XenMobile の要件

- XenMobile サーバー（最小バージョン 10.6）
- LDAP サーバーが構成済みである

内部ネットワークへのリモートデバイスアクセスに対する認証の構成

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**NetScaler Gateway**］ をクリックします。［**NetScaler Gateway**］ページが開きます。次の例では、NetScaler Gateway インスタンスが 1 つ存在しています。



3. 次の設定を構成します。

    - 認証： 認証を有効にするかどうかを選択します。デフォルトは ［オン］ です。

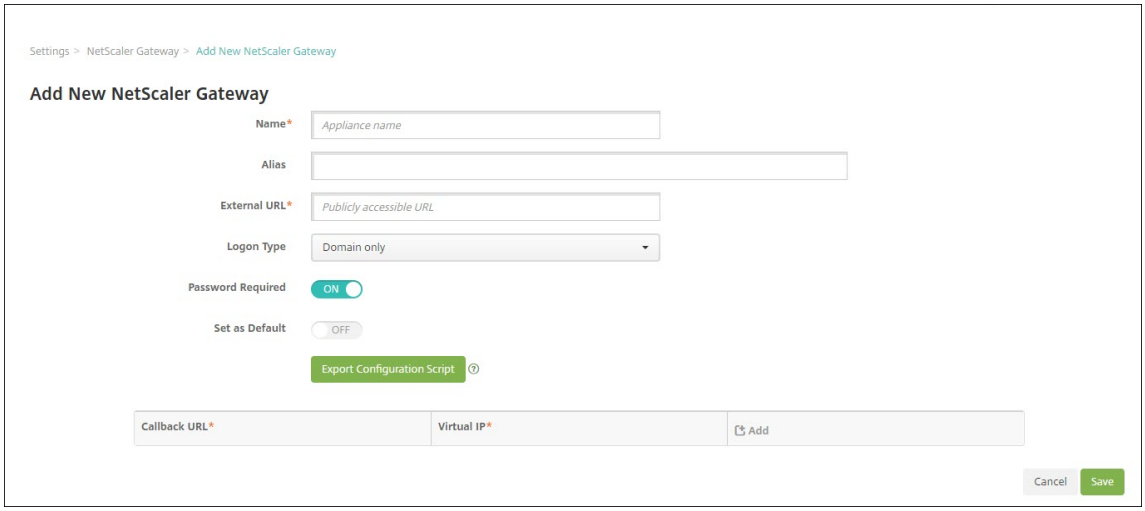
- 認証用のユーザー証明書を配信: XenMobile で Secure Hub と認証証明書を共有し、NetScaler Gateway でクライアント証明書認証を処理できるようにするかどうかを選択します。デフォルトは［オフ］ です。
- 資格情報プロバイダー: ボックスの一覧で、使用する資格情報プロバイダーを選択します。詳しくは、「資格情報プロバイダー」を参照してください。

4. ［保存］ をクリックします。

NetScaler Gateway インスタンスの追加

認証設定の保存後、NetScaler Gateway インスタンスを XenMobile に追加します。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**NetScaler Gateway**］ をクリックします。［**NetScaler Gateway**］ページが開きます。
3. ［追加］ をクリックします。［新しい **NetScaler Gateway** の追加］ ページが開きます。



4. 次の設定を構成します。

- 名前: NetScaler Gateway インスタンスの名前を入力します。
- エイリアス: オプションで、NetScaler Gateway のエイリアス名を入力します。
- 外部 **URL**: NetScaler Gateway の、パブリックにアクセスできる URL を入力します。たとえば、`https://receiver.com`のようになります。
- ログオンの種類: ログオンの種類を選択します。種類には、［ドメインのみ］、［セキュリティトークンのみ］、［ドメインおよびセキュリティトークン］、［証明書］、［証明書およびドメイン］、［証明書およびセキュリティトークン］ があります。［パスワードが必要］ フィールドのデフォルト設定は、選択した ［ログオンの種類］ に基づいて変化します。デフォルトは ［ドメインのみ］ です。

ドメインが複数ある場合は、［証明書およびドメイン］ を使用します。XenMobile と NetScaler Gateway で複数ドメイン認証を構成する方法については、「複数ドメイン認証の構成」を参照してください。

［**Certificate and security token**］を使用する場合、NetScaler Gateway で Secure Hub がサポートされるようにするには、追加の設定が必要となります。詳しくは、「証明書認証およびセキュリティトークン認証のための XenMobile の構成」を参照してください。

詳しくは、展開ハンドブックの「認証」を参照してください。

- パスワードが必要: パスワード認証を必須にするかどうかを選択します。デフォルト値は、選択した［ログオンの種類］ に応じて変化します。
- デフォルトとして設定: この NetScaler Gateway をデフォルトとして使用するかどうかを選択します。デフォルトは ［オフ］ です。
- 構成スクリプトのエクスポート: 構成バンドルをエクスポートする場合はこのボタンをクリックします。エクスポートした構成バンドルは NetScaler Gateway にアップロードし、XenMobile の設定を使用して構成します。詳しくは、これらの手順の後で「XenMobile サーバーで使用するオンプレミスの NetScaler Gateway の構成」を参照してください。
- ［コールバック **URL**］ と ［仮想 **IP**］: これらのフィールドを追加する前に設定を保存してください。詳しくは、この記事の「コールバック URL および NetScaler Gateway VPN の仮想 IP の追加」を参照してください。

5. ［保存］ をクリックします。

   新しい NetScaler Gateway が追加され、表に表示されます。インスタンスを編集または削除するには、表で名前をクリックします。

XenMobile サーバーで使用する NetScaler Gateway の構成

XenMobile サーバーで使用するオンプレミスの NetScaler Gateway を構成するには以下の一般的な手順を実行します。これらの手順の詳細は下記で説明します。

1. XenMobile サーバーからスクリプトと関連ファイルをダウンロードします。最新の手順について詳しくは、スクリプトに付属する readme ファイルを参照してください。
2. 環境が前提条件を満たしていることを確認します。
3. 環境に合わせてスクリプトを更新します。
4. NetScaler でスクリプトを実行します。
5. 構成をテストします。

スクリプトにより、XenMobile に必要なこれらの NetScaler Gateway の設定が構成されます。

- MDM と MAM に必要な NetScaler Gateway 仮想サーバー
- NetScaler Gateway 仮想サーバー用セッションポリシー
- XenMobile Server の詳細
- NSG 仮想サーバーの認証ポリシーとアクション。
  スクリプトによって LDAP の構成設定が説明されます。

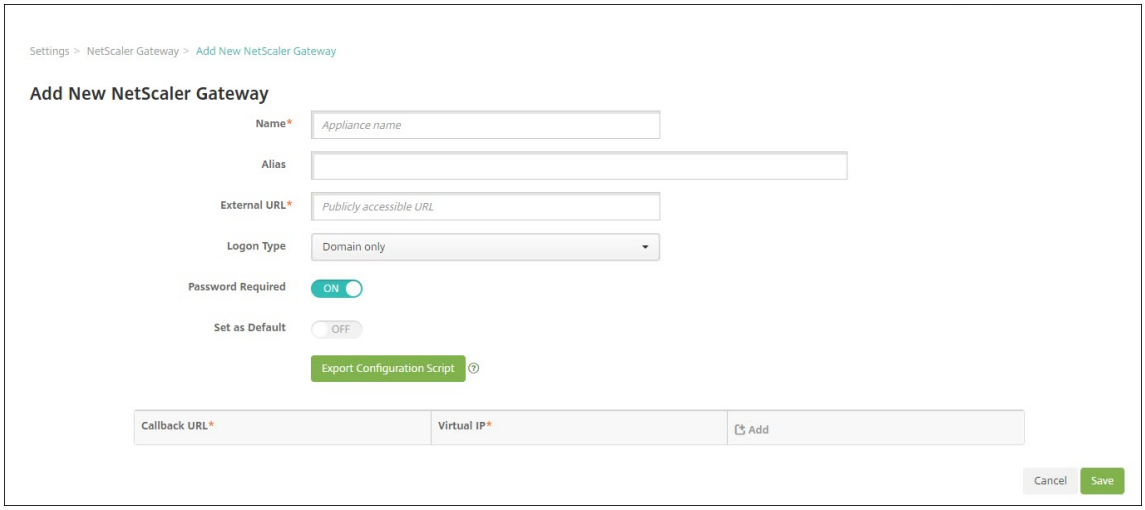
- プロキシサーバーのトラフィックアクションとポリシー
- クライアントレスアクセスプロファイル
- NetScaler の静的ローカル DNS レコード
- 他のバインディング：サービスポリシー、CA 証明書

このスクリプトは以下の構成には対応していません。

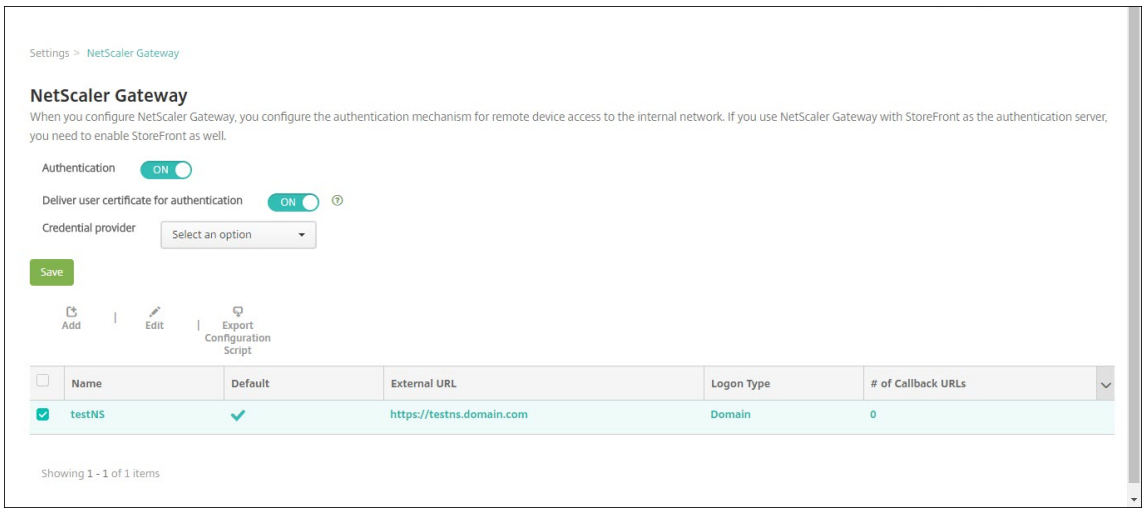
- Exchange 負荷分散
- ShareFile 負荷分散
- ICA プロキシ構成
- SSL オフロード

スクリプトをダウンロード、更新、実行するには

1. NetScaler Gateway を追加中の場合は、［新しい **NetScaler Gateway** の追加］ページで ［構成スクリプトのエクスポート］ をクリックします。



   NetScaler Gateway インスタンスを追加しスクリプトのエクスポート前に ［保存］ をクリックしている場合は、［設定］ **>** ［**NetScaler Gateway**］ に戻り、目的の NetScaler を選択して ［構成スクリプトのエクスポート］ をクリックし、［ダウンロード］ をクリックします。



[構成スクリプトのエクスポート] をクリックすると、XenMobile により.tar.gz 形式のスクリプトバンドルが作成されます。このスクリプトバンドルの内容は次のとおりです。

- 詳細説明付きの readme ファイル
- NetScaler の必須コンポーネントの構成に使用する NetScaler CLI コマンドを含むスクリプト
- XenMobile サーバーのパブリックルート CA（認証機関：Certificate Authority）証明書および中間 CA 証明書（現在のリリースでは、SSL オフロードの場合これらの証明書は不要です）
- NetScaler の構成の削除に使用する NetScaler CLI コマンドを含むスクリプト

2. スクリプト（NSGConfigBundle_CREATESCRIPT.txt）を編集し、すべてのプレースホルダーを環境の情報で置き換えます。

```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.
```

3. スクリプトバンドルに含まれる readme ファイルの説明に従って、編集済みのスクリプトを NetScaler の bash シェルで実行します。次に例を示します:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management
 Password> batch -f ”/var/NSGConfigBundle_CREATESCRIPT.txt”
```



```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

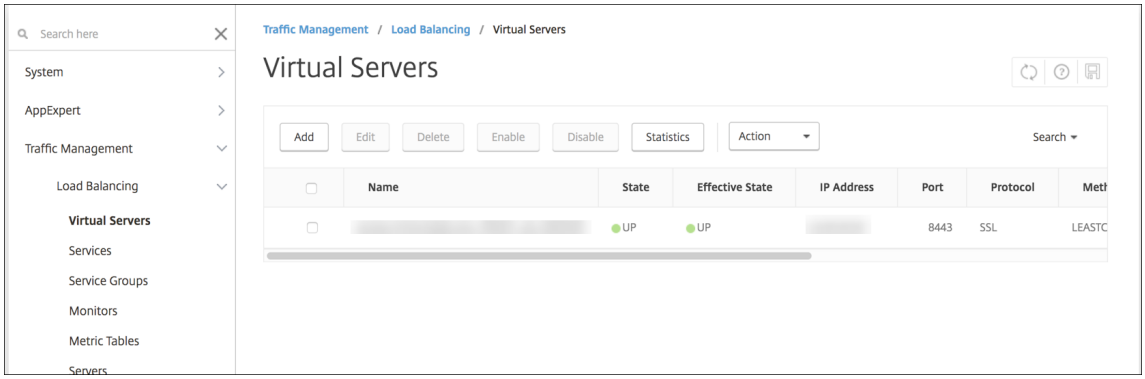
スクリプトが完了すると、次の行が表示されます。

```
exec: save ns config
 Done
 Done
root@ns#
```

構成のテスト

1. NetScaler Gateway 仮想サーバーの状態表示が ［**UP**］ であることを確認します。

2. Proxy 負荷分散仮想サーバーの状態表示が ［**UP**］ であることを確認します。



3. Web ブラウザーを開いて NetScaler Gateway の URL に接続し、認証を試みます。認証が失敗した場合、「HTTP Status 404 - Not Found」というメッセージが表示されます。
4. デバイスを登録して、MDM と MAM の両方に登録されたことを確認します。

コールバック **URL** および **NetScaler Gateway VPN** の仮想 **IP** の追加

NetScaler Gateway インスタンスを追加した後で、コールバック URL を追加し NetScaler Gateway 仮想 IP アドレスを指定できます。この設定はオプションですが、特に XenMobile Server が DMZ に配置されている場合、構成することでセキュリティを強化できます。

1. [設定] > [**NetScaler Gateway**] で、目的の NetScaler Gateway を選択して [編集] をクリックします。
2. 表で [追加] をクリックします。
3. [コールバック **URL**] に完全修飾ドメイン名（FQDN）を入力します。このコールバック URL により、要求元が NetScaler Gateway であることが証明されます。

   入力したコールバック URL が、XenMobile サーバーからアクセス可能な IP アドレスに解決されることを確認します。コールバック URL には、外部の NetScaler Gateway の URL や他の URL も指定できます。
4. NetScaler Gateway の 仮想 **IP** アドレスを入力してから [保存] をクリックします。

複数ドメイン認証の構成

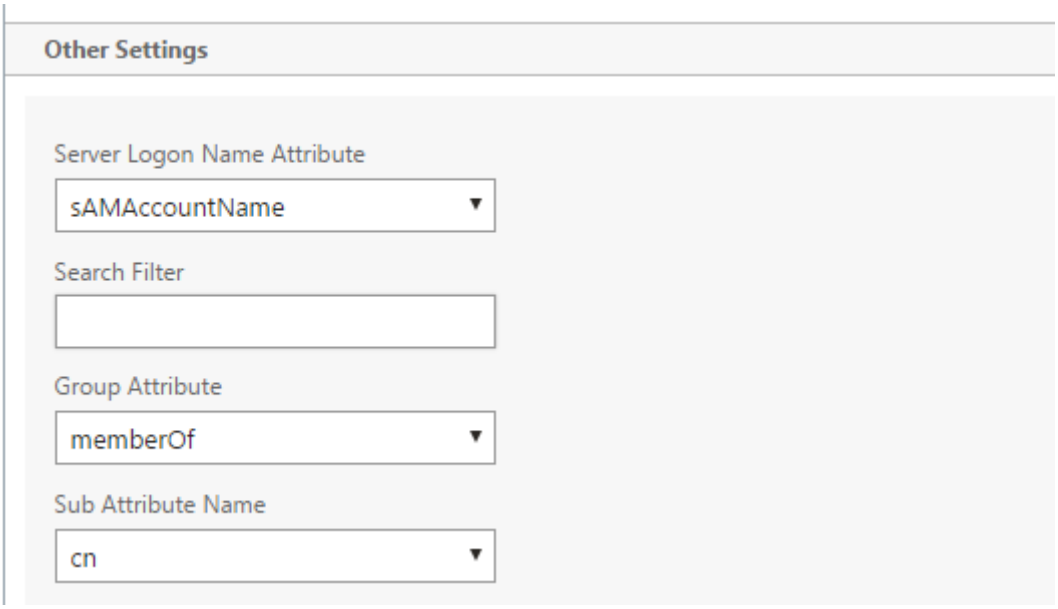
テスト環境、開発環境、および実稼働環境などの複数の XenMobile Server インスタンスがある場合は、追加の環境用に手動で NetScaler Gateway を構成します。(NetScaler for XenMobile ウィザードは 1 回のみ使用できます)。

NetScaler Gateway 構成

複数ドメイン環境で NetScaler Gateway 認証ポリシーとセッションポリシーを構成するには:

1. NetScaler Gateway 構成ユーティリティの [構成] タブで [**NetScaler Gateway**] > [ポリシー] > [認証] を展開します。

2. ナビゲーションペインで ［**LADP**］ をクリックします。
3. クリックして LDAP プロファイルを編集します。［サーバーログオン名の属性］ を **userPrincipalName**、または検索に使用する属性に変更します。指定した属性を記録します。この属性は、XenMobile コンソールで LDAP 設定を構成するときに使用する必要があります。

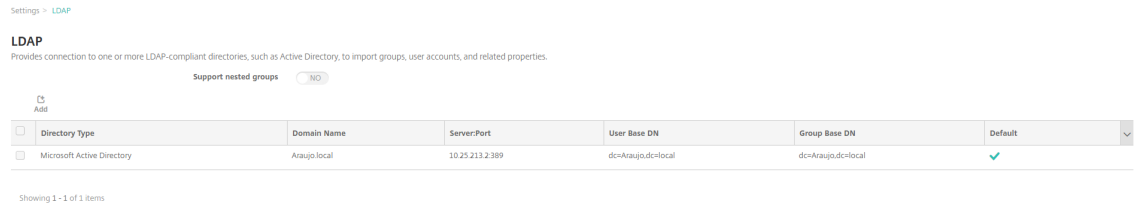


4. 各 LDAP ポリシーに対してこれらの手順を繰り返します。ドメインごとに個別の LDAP ポリシーが必要です。
5. NetScaler Gateway 仮想サーバーにバインドされたセッションポリシーで、［**Edit session profile**］ **>** ［**Published Applications**］ に移動します。［**Single Sign-On Domain**］ は空白にしてください。

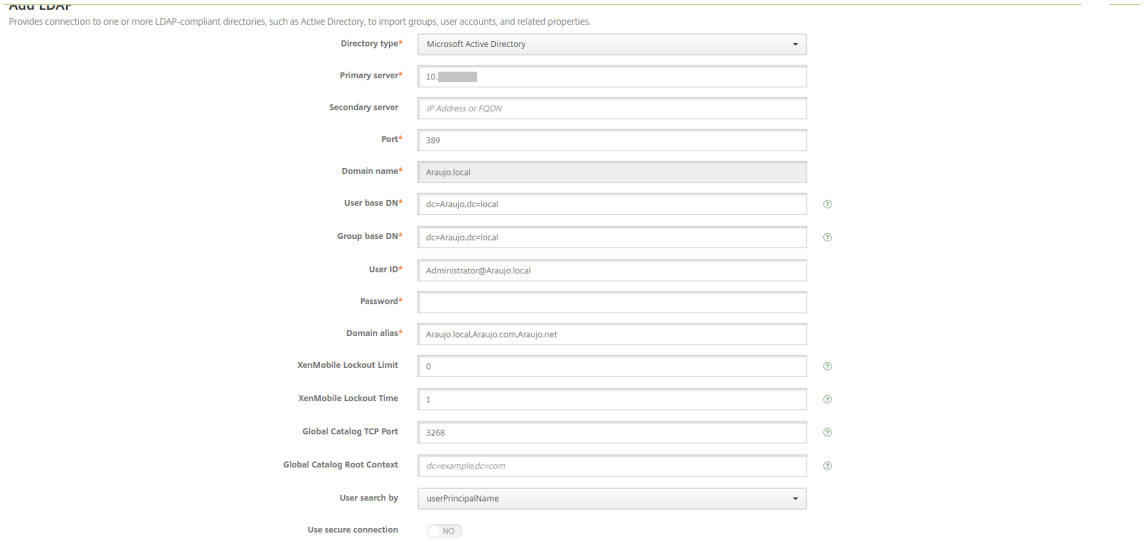
XenMobile Server の構成

LDAP を複数ドメインの XenMobile 環境に構成するには：

1. XenMobile コンソールで、［設定］ **>** ［**LDAP**］ に移動し、ディレクトリを追加または編集します。



2. 情報を指定します。
   - ［ドメインエイリアス］ でユーザー認証に使用する各ドメインを指定します。ドメインはコンマで区切り、ドメイン間にはスペースを入れないでください。例：domain1.com,domain2.com,domain3.com
   - ［ユーザー検索基準］ フィールドが NetScaler Gateway LDAP ポリシーで指定された ［サーバーログオン名の属性］ と一致するようにしてください。



特定の **URL** への受信接続要求を破棄

ご使用の環境の Citrix Gateway が SSL オフロード用に構成されている場合は、ゲートウェイで特定の URL への受信接続要求が破棄されるようにすることができます。

この方法でセキュリティを強化する必要がある場合は、Citrix Gateway で 2 台の MDM ロードバランサー vServer（ポート 443 用とポート 8443 用）を構成します。以下の情報を設定のテンプレートとして使用してください。

> 重要：
>
> 以下の更新は、SSL オフロード用に設定された Citrix Gateway 専用です。

1. 名前XMS_DropURLsのパターンセットを作成します。

```
add policy patset XMS_DropURLs
```

2. 新しいパターンセットに次の URL を追加します。必要に応じてこの一覧をカスタマイズしてください。

```
bind policy patset XMS_DropURLs /zdm/shp/console -index 6

bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5

bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4

bind policy patset XMS_DropURLs /zdm/log.jsp -index 3

bind policy patset XMS_DropURLs /zdm/login.jsp -index 2

bind policy patset XMS_DropURLs /zdm/console -index 1
```

3. 接続要求が指定されたサブネットから発信されていない限り、これらの URL へのすべてのトラフィックを破棄するためのポリシーを作成します。

```
1 add responder policy XMS_DROP_pol  “CLIENT.IP.SRC.IN_SUBNET
      (192.168.0.0/24).NOT &&
2 HTTP.REQ.URL.CONTAINS_ANY(” XMS_DropURLs” )”  DROP -comment ”Allow
      only subnet 192.168.0.0/24 to access these URLs. All other
      connections are DROPed”
```

4. 新しいポリシーを両方の MDM ロードバランサー vServer にバインドします（ポート 443 と 8443）。

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
      XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
      REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
      XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
      REQUEST
```

ドメインまたはドメイン + セキュリティトークン認証

August 22, 2019

XenMobile は、LDAP（Lightweight Directory Access Protocol）に準拠している 1 つまたは複数のディレクトリに対するドメインベースの認証をサポートしています。XenMobile では、1 つまたは複数のディレクトリへの接続を構成し、LDAP 構成を使用して、グループ、ユーザーアカウント、関連するプロパティをインポートすることができます。

LDAP は、オープンソースで特定のベンダーに依存しないアプリケーションプロトコルであり、インターネットプロトコル（IP）ネットワーク経由で分散ディレクトリ情報サービスへのアクセスや管理を行うためのものです。ディレクトリ情報サービスは、ネットワークで使用可能な、ユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。

LDAP は一般的に、シングルサインオン（SSO）をユーザーに提供するために利用されます。SSO では（ユーザーごとに）1 つのパスワードを複数のサービス間で共有します。シングルサインオンにより、ユーザーは会社の Web サイトに一度ログオンすると、社内イントラネットへのアクセスが認証されます。

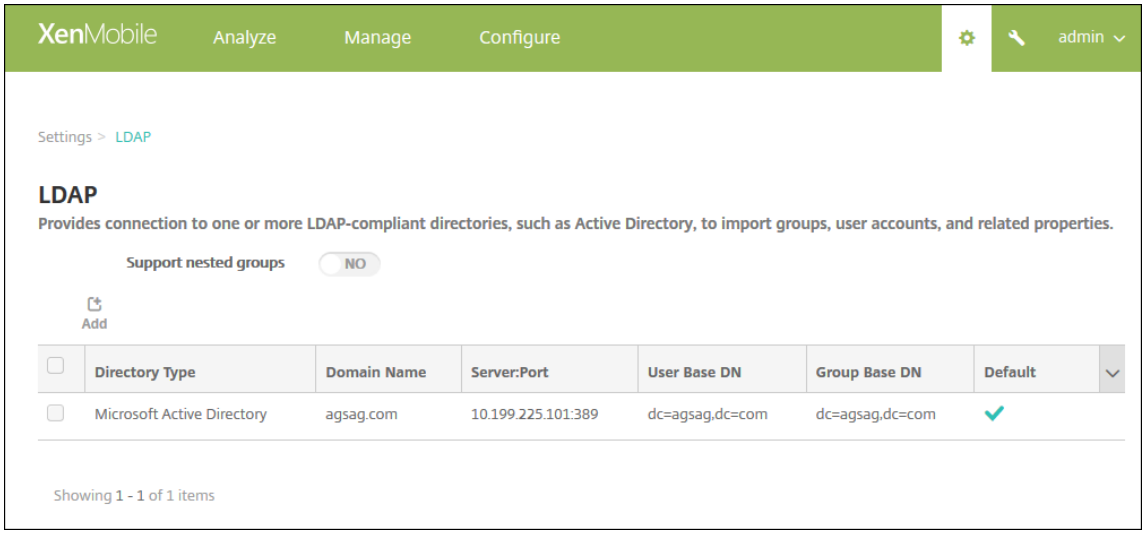
クライアントが、ディレクトリシステムエージェント（DSA）と呼ばれる LDAP サーバーに接続して、LDAP セッションを開始します。次に、クライアントは操作要求をサーバーに送信し、サーバーは適切な認証で応答します。

> 重要:
>
> XenMobile では、ユーザーが XenMobile にデバイスを登録した後に、認証モードをドメイン認証から他の認

> 証モードに変更することはサポートされていません。

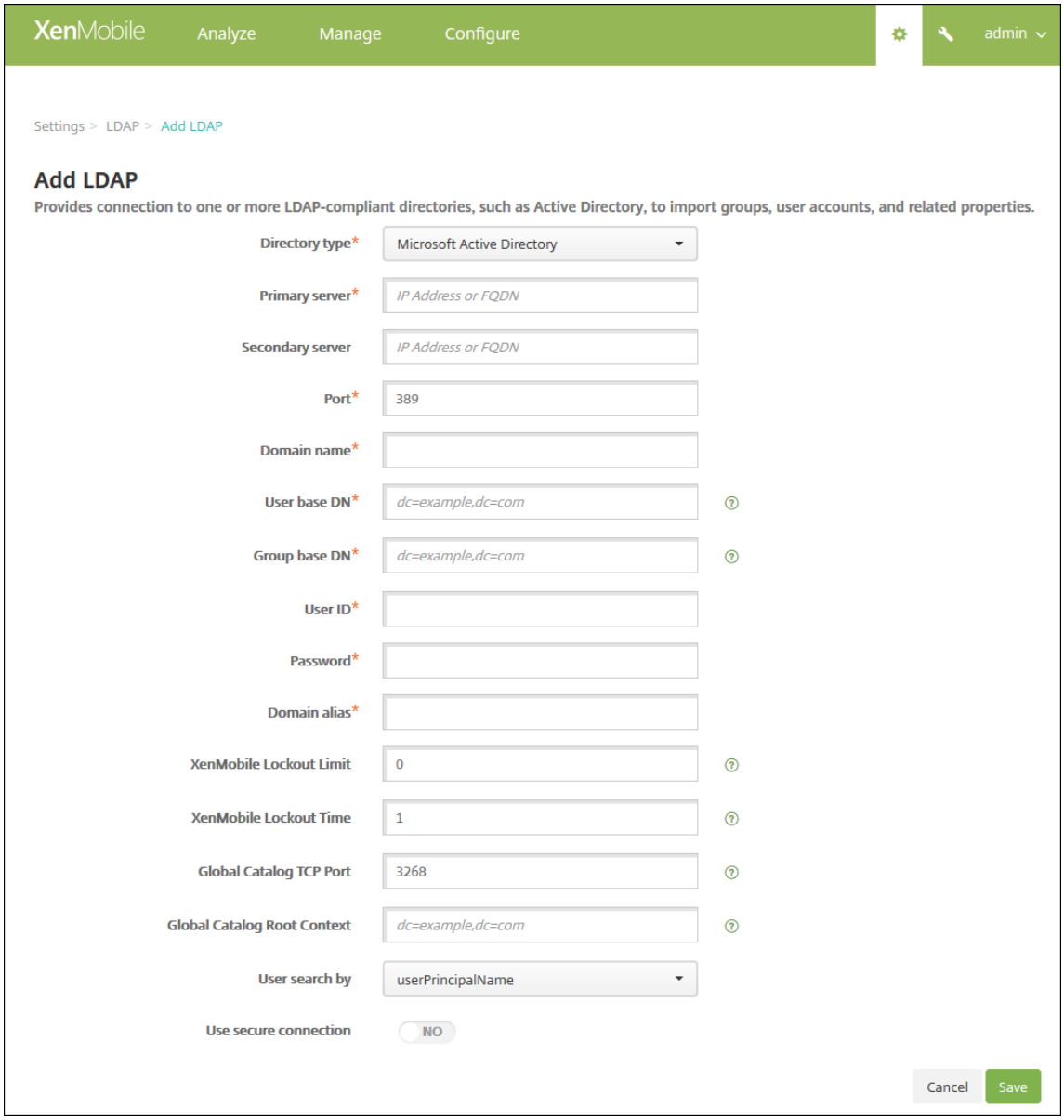
XenMobile で LDAP 接続を追加するには

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**LDAP**］ をクリックします。［**LDAP**］ ページが開きます。この記事で説明するように、LDAP 準拠のディレクトリを［追加］、［編集］、［削除］することができます。



LDAP 準拠のディレクトリを追加するには

1. ［**LDAP**］ ページで、 ［追加］ をクリックします。［**LDAP** の追加］ ページが開きます。



2. 次の設定を構成します。

   - ディレクトリの種類： 一覧から、適切なディレクトリの種類を選択します。デフォルトは ［**Microsoft Active Directory**］ です。
   - プライマリサーバー： LDAP で使用するプライマリサーバーを入力します。IP アドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
   - セカンダリサーバー： セカンダリサーバーが構成されている場合、任意でセカンダリサーバーの IP アドレスまたは FQDN を入力します。このサーバーは、プライマリサーバーが使用できない場合に使用するフェイルオーバーサーバーです。
   - ポート： LDAP サーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていない LDAP 接続用のポート番号 **389** に設定されています。セキュリティ保護された LDAP 接続ではポート番号 **636**、Microsoft のセキュリティ保護されていない LDAP 接続では **3268**、Microsoft の

セキュリティ保護された LDAP 接続では **3269** を使用します。

- ドメイン名: ドメイン名を入力します。
- ユーザーベース **DN**: Active Directory 内でのユーザーの位置を一意の識別子で入力します。構文例には次が含まれます: `ou=users`、`dc=example`、`dc=com`
- グループベース **DN**: Active Directory のグループの場所を入力します。たとえば、`cn=users, dc=domain, dc=net`の場合、`cn=users`はグループのコンテナ名で`dc`は Active Directory のドメインコンポーネントです。
- ユーザー **ID**: Active Directory アカウントに関連付けられたユーザー ID を入力します。
- パスワード: ユーザーに関連付けられたパスワードを入力します。
- ドメインエイリアス: ドメイン名のエイリアスを入力します。
- **XenMobile** ロックアウト制限: ログオンの試行失敗回数として、**0** ～ **999** の数値を入力します。「**0**」の値に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
- **XenMobile** ロックアウト時間: ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、**0** ～ **99999** の数値を入力します。「**0**」の値に設定すると、ユーザーがロックアウト後に強制的に待機させられることはなくなります。
- グローバルカタログ **TCP** ポート: グローバルカタログサーバーの TCP ポート番号を入力します。デフォルトでは、TCP ポート番号は **3268** に設定されています。SSL 接続では、ポート番号 **3269** を使用します。
- グローバルカタログルートコンテキスト: 任意で、Active Directory でのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準の LDAP 検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- ユーザー検索基準: 一覧から、［**userPrincipalName**］ または ［**sAMAccountName**］ を選択します。デフォルトは ［**userPrincipalName**］ です。
- セキュア接続を使用: セキュリティ保護された接続を使用するかどうかを選択します。デフォルトは ［**NO**］ です。

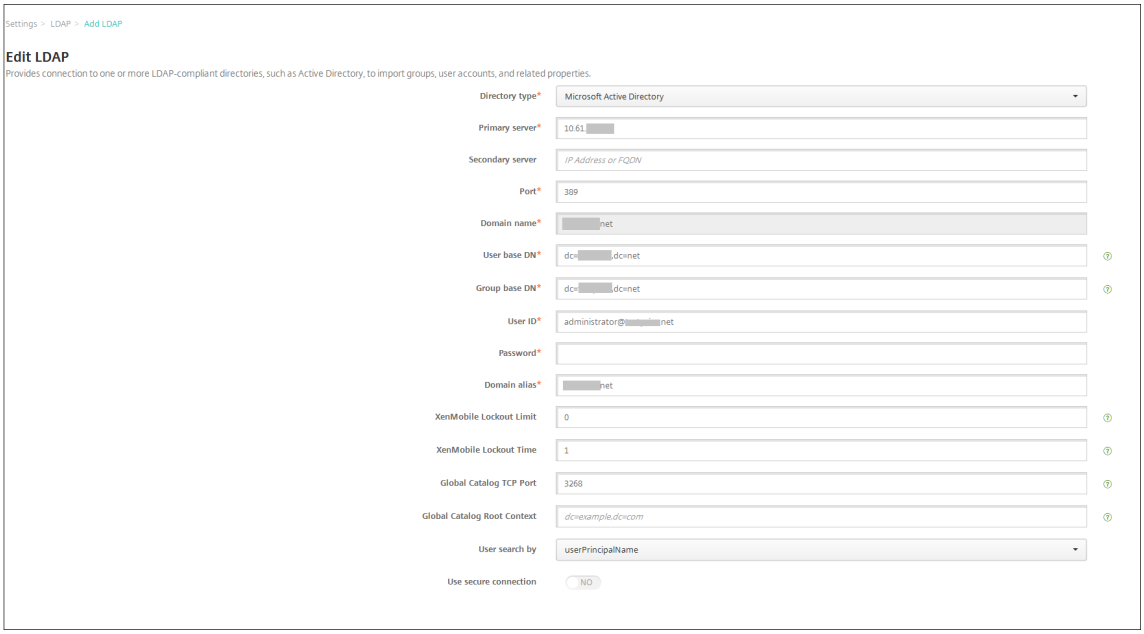
3. ［保存］ をクリックします。

LDAP 準拠のディレクトリを編集するには

1. ［**LDAP**］ の表で、編集するディレクトリを選択します。

   ディレクトリの横にあるチェックボックスをオンにすると、LDAP 一覧の上にオプションメニューが表示されます。一覧の項目をクリックすると、その項目の右側にオプションメニューが表示されます。

2. ［編集］ をクリックします。［**LDAP** の編集］ ページが開きます。



3. 必要に応じて以下の情報を変更します。

   - ディレクトリの種類： 一覧から、適切なディレクトリの種類を選択します。
   - プライマリサーバー： LDAP で使用するプライマリサーバーを入力します。IP アドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
   - セカンダリサーバー： 任意で、セカンダリサーバーの IP アドレスまたは FQDN を入力します（構成されている場合）。
   - ポート： LDAP サーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていない LDAP 接続用のポート番号 **389** に設定されています。セキュリティ保護された LDAP 接続ではポート番号 **636**、Microsoft のセキュリティ保護されていない LDAP 接続では **3268**、Microsoft のセキュリティ保護された LDAP 接続では **3269** を使用します。
   - ドメイン名： このフィールドは変更できません。
   - ユーザーベース **DN**： Active Directory 内でのユーザーの位置を一意の識別子で入力します。構文例には次が含まれます：`ou=users`、`dc=example`、`dc=com`
   - グループベース **DN**： 「`cn=groupname`」のように指定される、グループのベース DN グループ名を入力します。たとえば、「`cn=users, dc=servername, dc=net`」で、「`cn=users`」はグループ名です。DN および servername は、Active Directory を実行しているサーバーの名前を表します。
   - ユーザー **ID**： Active Directory アカウントに関連付けられたユーザー ID を入力します。
   - パスワード： ユーザーに関連付けられたパスワードを入力します。
   - ドメインエイリアス： ドメイン名のエイリアスを入力します。
   - **XenMobile** ロックアウト制限： ログオンの試行失敗回数として、**0** ～ **999** の数値を入力します。「**0**」の値に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
   - **XenMobile** ロックアウト時間： ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、**0** ～ **99999** の数値を入力します。「**0**」の値に設定すると、ユーザーがロックアウト後に強制的に待機させられることはなくなります。

- グローバルカタログ **TCP** ポート: グローバルカタログサーバーの TCP ポート番号を入力します。デフォルトでは、TCP ポート番号は **3268** に設定されています。SSL 接続では、ポート番号 **3269** を使用します。
- グローバルカタログルートコンテキスト: 任意で、Active Directory でのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準の LDAP 検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- ユーザー検索基準: 一覧から、［**userPrincipalName**］ または ［**sAMAccountName**］ を選択します。
- セキュリティで保護された接続を使用: セキュリティ保護された接続を使用するかどうかを選択します。

4. ［保存］ をクリックして変更を保存するか、［キャンセル］ をクリックしてプロパティを変更せずそのままにします。

LDAP 準拠のディレクトリを削除するには

1. ［**LDAP**］ の表で、削除するディレクトリを選択します。

   各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。

2. ［削除］ をクリックします。確認ダイアログボックスが開きます。もう一度 ［削除］ をクリックします。

複数ドメイン認証の構成

XenMobile Server を構成して LDAP の構成で複数のドメインサフィックスを使用するには、Citrix Endpoint Management ドキュメントの「複数ドメイン認証の構成」で手順を参照してください。この手順は、オンプレミス版の XenMobile Server および Endpoint Management のクラウド版と同様です。

ドメイン + セキュリティトークン認証の構成

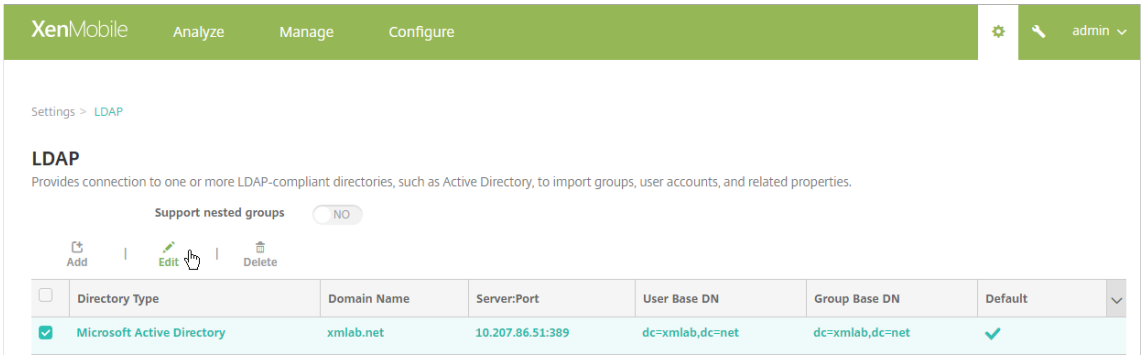
RADIUS プロトコルを使用して、LDAP 資格情報とワンタイムパスワードによる認証をユーザーに要求するように XenMobile を構成できます。

ユーザービリティを最適にするために、この構成を Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。この構成により、ユーザーは LDAP ユーザー名とパスワードを繰り返し入力する必要がなくなります。ただし、登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力します。

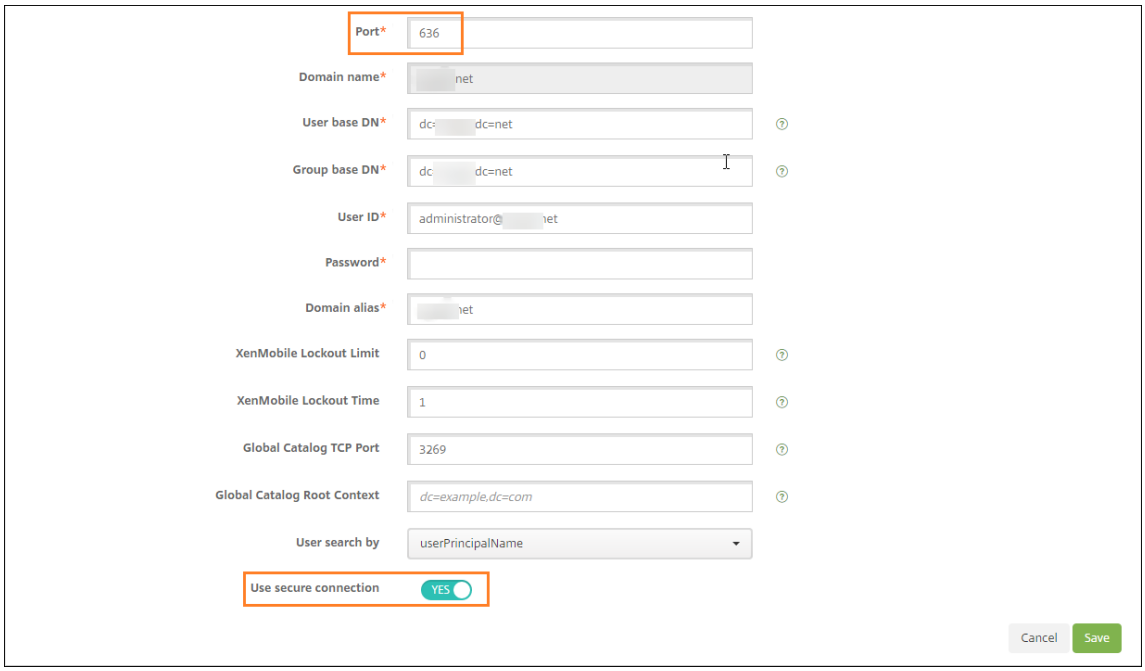
LDAP 設定の構成

認証に LDAP を使用する場合、証明機関から XenMobile に SSL 証明書をインストールする必要があります。詳しくは、「XenMobile での証明書のアップロード」を参照してください。

1. [設定] で [**LDAP**] をクリックします。
2. [**Microsoft Active Directory**] を選択して [編集] をクリックします。



3. [ポート] が **636** であることを確認します（セキュリティで保護された LDAP 接続の場合）。セキュリティで保護された Microsoft LDAP 接続の場合は **3269** です。
4. [セキュリティで保護された接続を使用] を [はい] に変更します。

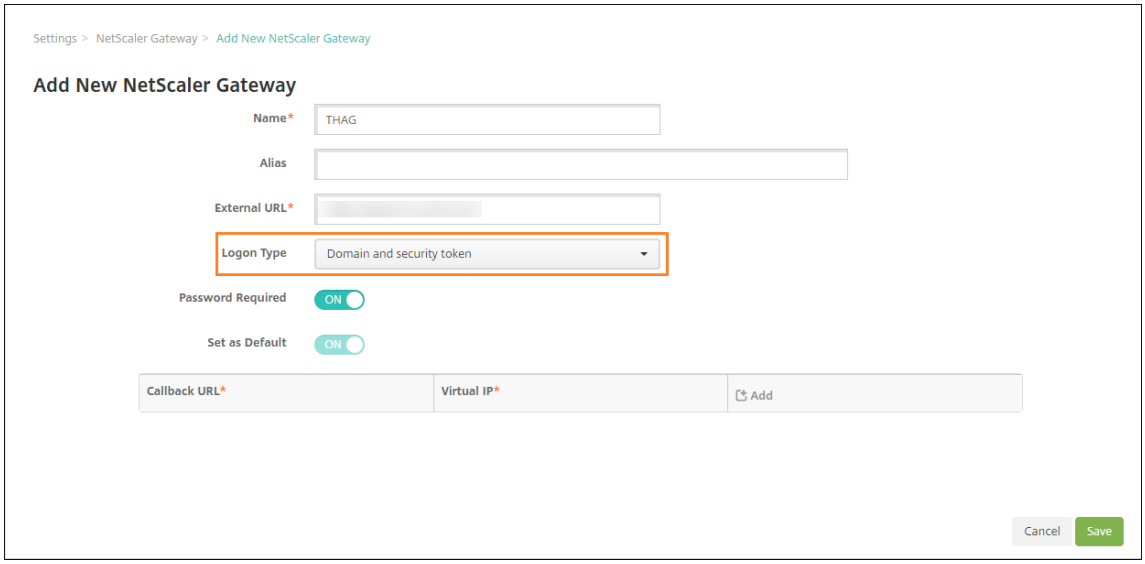


NetScaler Gateway 設定の構成

次の手順では、NetScaler Gateway インスタンスをすでに XenMobile に追加してあると想定しています。NetScaler Gateway インスタンスを追加するには、「NetScaler Gateway インスタンスの追加」を参照してください。

1. [設定] で [**NetScaler Gateway**] をクリックします。
2. **NetScaler Gateway** を選択して [編集] をクリックします。

3. ［ログオンの種類］ で ［ドメインおよびセキュリティトークン］ を選択します。



Citrix PIN とユーザーパスワードキャッシュの有効化

Citrix PIN とユーザーパスワードキャッシュを有効化するには、［設定］ **>** ［クライアントプロパティ］ に移動し、チェックボックス ［**Citrix PIN** 認証の有効化］ および ［ユーザーパスワードキャッシュの有効化］ をオンにします。詳しくは、「クライアントプロパティ」を参照してください。

ドメインおよびセキュリティトークン認証のための **NetScaler Gateway** の構成

NetScaler Gateway セッションのプロファイルおよびポリシーを、XenMobile で使用される仮想サーバー用に構成します。詳しくは、Citrix NetScaler Gateway のドキュメントを参照してください。

クライアント証明書、または証明書とドメイン認証の組み合わせ

January 10, 2020

XenMobile のデフォルト構成は、ユーザー名とパスワードによる認証です。登録および XenMobile 環境へのアクセスのセキュリティを強化するには、証明書ベースの認証の使用を考慮してください。XenMobile 環境では、この構成はセキュリティとユーザーエクスペリエンスの最適な組み合わせです。証明書とドメイン認証を利用すれば、NetScaler の 2 要素認証で提供されるセキュリティとと共に SSO の最高の可能性を引き出します。

ユーザービリティを最適にするために、この証明書とドメイン認証を Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。その結果、ユーザーは LDAP ユーザー名とパスワードを繰り返し入力する必要がなくなります。ただし、登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力します。

> 重要：
>
> XenMobile では、ユーザーが XenMobile にデバイスを登録した後に、認証モードをドメイン認証から他の認証モードに変更することはサポートされていません。

LDAP やスマートカードの使用または同様の方法を許可しない場合、証明書を構成すると XenMobile にスマートカードを提示できます。ユーザーはそれにより、XenMobile が生成する一意の PIN を使用して登録できます。ユーザーがアクセス権を獲得すると、XenMobile は、XenMobile 環境を認証するために使用される証明書を作成して展開します。

NetScaler for XenMobile ウィザードを使用すると、NetScaler 証明書のみの認証または証明書とドメイン認証の組み合わせを使用する場合、XenMobile に必要な構成を実行できます。NetScaler for XenMobile ウィザードは 1 回のみ実行できます。

高セキュリティの環境では、パブリックネットワークまたは保護されていないネットワークで組織外の LDAP 資格情報を使用することは、組織に対する最大のセキュリティ脅威とみなされます。高セキュリティの環境では、クライアント証明書とセキュリティトークンを使用する 2 要素認証がオプションとなります。詳しくは、「証明書認証およびセキュリティトークン認証のための XenMobile の構成」を参照してください。

クライアント証明書認証は、XenMobile の MAM モード（MAM-only）および ENT モードで使用できます（ユーザーが MDM に登録している場合）。ユーザーが従来の MAM モードに登録している場合、クライアント証明書認証は、XenMobile の ENT モードで使用できません。XenMobile ENT および MAM モードでクライアント証明書認証を使用するには、Microsoft サーバー、XenMobile Server を構成してから、NetScaler Gateway を構成する必要があります。この記事に説明されているとおり、次の手順に従ってください。

Microsoft サーバーの場合：

1. 証明書のスナップインを Microsoft 管理コンソールに追加します。
2. テンプレートを証明機関（CA）に追加します。
3. CA サーバーから PFX 証明書を作成します。

XenMobile Server の場合：

1. 証明書を XenMobile にアップロードします。
2. 証明書に基づいた認証のために PKI エンティティを作成します。
3. 資格情報プロバイダーを構成します。
4. NetScaler Gateway を構成して、認証用のユーザー証明書を配信します。

   NetScaler Gateway の構成について詳しくは、次の Citrix ADC ドキュメントを参照してください：クライアント認証、SSL プロファイルインフラストラクチャ、クライアント証明書認証ポリシーの構成およびバインド。

前提条件

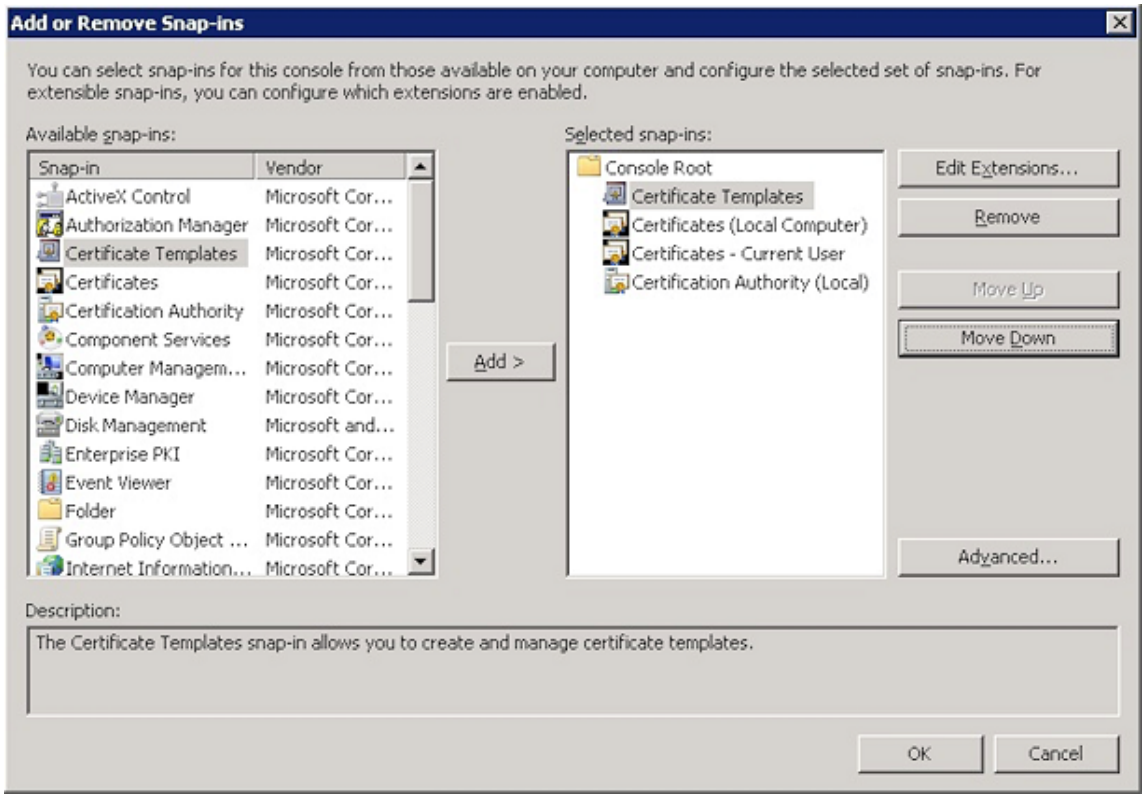
- Microsoft 証明書サービスのエンティティテンプレートを作成する場合は、登録済みデバイスの認証に関する問題を避けるため、特殊文字を使用しないでください。たとえば、テンプレート名には以下の文字を使用しないでください: : ! $ ()## % + * ~ ? | { } []
- 証明書認証および SSL オフロードを使用する Windows Phone 8.1 デバイスの場合、NetScaler 内の両方の負荷分散仮想サーバー上のポート 443 に対する SSL セッション再利用を無効にしてください。そうするには、vserver 上でポート 443 に対して次のコマンドを実行します:

  ```
  set ssl vserver <ssl lb vserver> sessReuse DISABLE
  ```

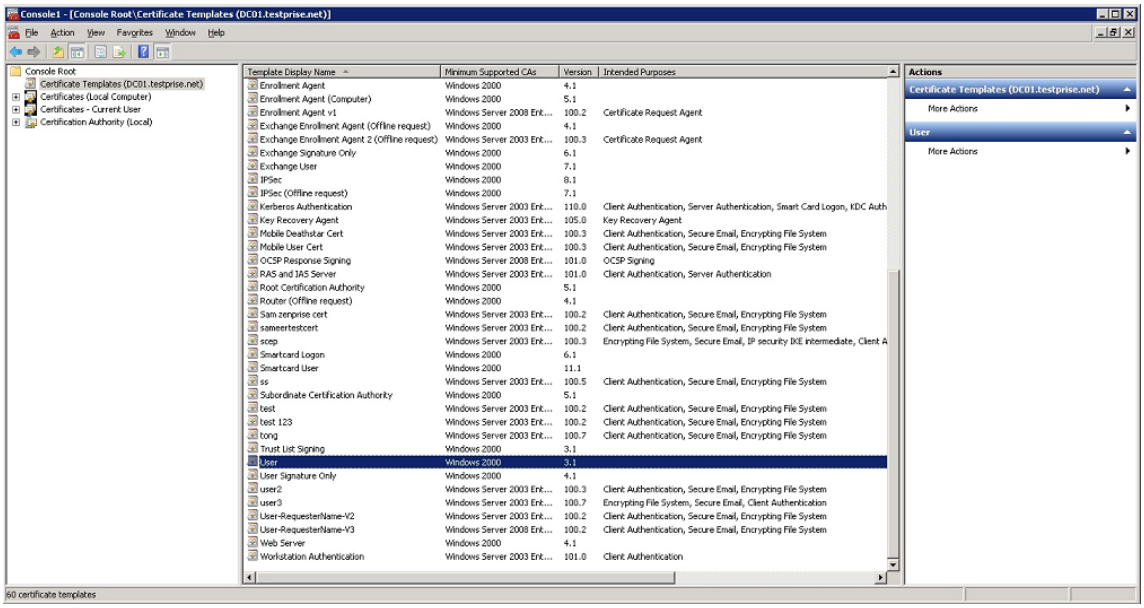
  SSL セッション再利用を無効にすると、NetScaler で提供される最適化の一部が無効になり、NetScaler 上のパフォーマンスが低下することがあります。
- Exchange ActiveSync に対して証明書ベースの認証を構成するには、このMicrosoft ブログを参照してください。
- プライベートサーバー証明書を使用して Exchange Server への ActiveSync トラフィックを保護する場合は、モバイルデバイスにすべてのルート証明書および中間証明書があることを確認してください。これらの証明書がない場合、Secure Mail でのメールボックス設定時に、証明書ベースの認証が失敗します。Exchange IIS コンソールでは、次のことが必要です:
  - XenMobile を Exchange と使用するための Web サイトを追加し、Web サーバー証明書をバインドします。
  - ポート 9443 を使用します。
  - その Web サイトに対して、Microsoft-Server-ActiveSync 用と EWS 用に、2 つのアプリケーションを追加する必要があります。それらの両方のアプリケーションに対して、［**SSL Settings**］で［**Require SSL**］を選択します。
- 展開方法で必要な場合は、Secure Mail が最新の MDX Toolkit でラップされていることを確認してください。

証明書のスナップインを **Microsoft** 管理コンソールに追加する

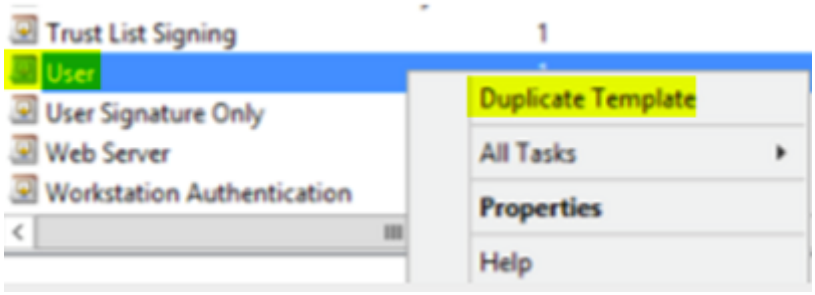
1. コンソールを開いて、［スナップインの追加と削除］をクリックします。
2. 次のスナップインを追加します:
   - 証明書テンプレート
   - 証明書（ローカルコンピューター）
   - 証明書 - 現在のユーザー
   - 証明機関（CA）（ローカル）



3. [証明書テンプレート] を展開します。



4. [ユーザー] テンプレートと [テンプレートの複製] を選択します。

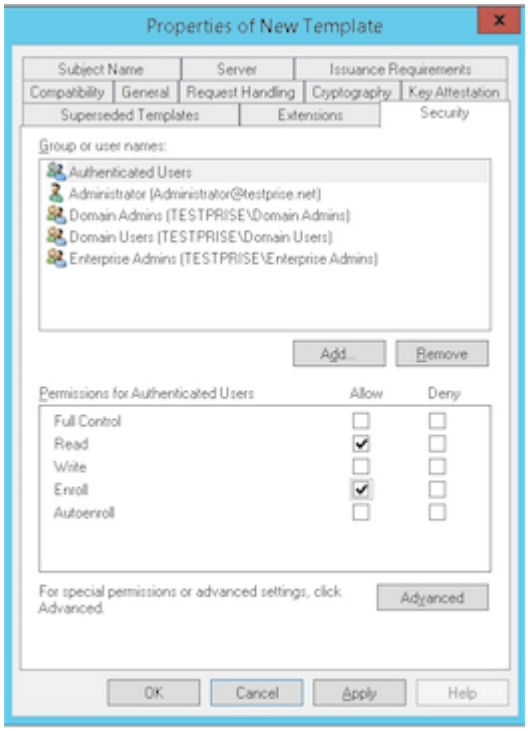


5. ［テンプレート］の表示名を入力します。

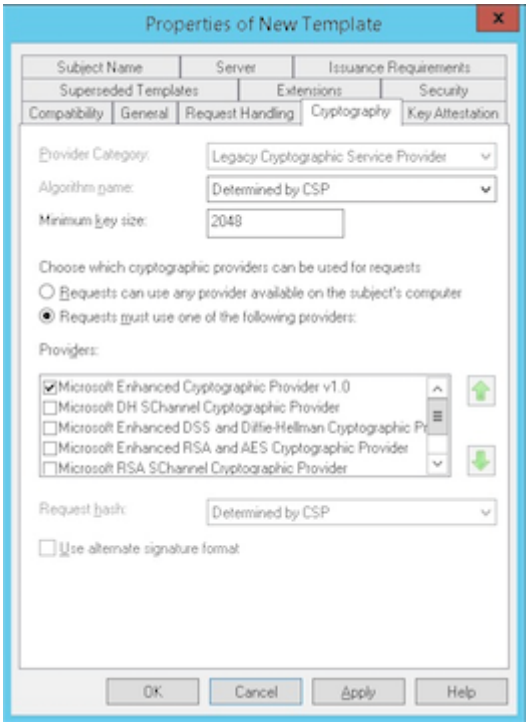
> 重要:
>
> 必要な場合のみ、［**Active Directory** の証明書を発行する］チェックボックスをオンにします。このオプションがオンの場合、すべてのユーザークライアント証明書が Active Directory で作成され、Active Directory データベースを圧迫する可能性があります。

6. テンプレートの種類として［**Windows 2003 Server**］を選択します。Windows 2012 R2 サーバーの［互換性］で、［証明機関］ を選択して **Windows 2003** を受信者として設定します。

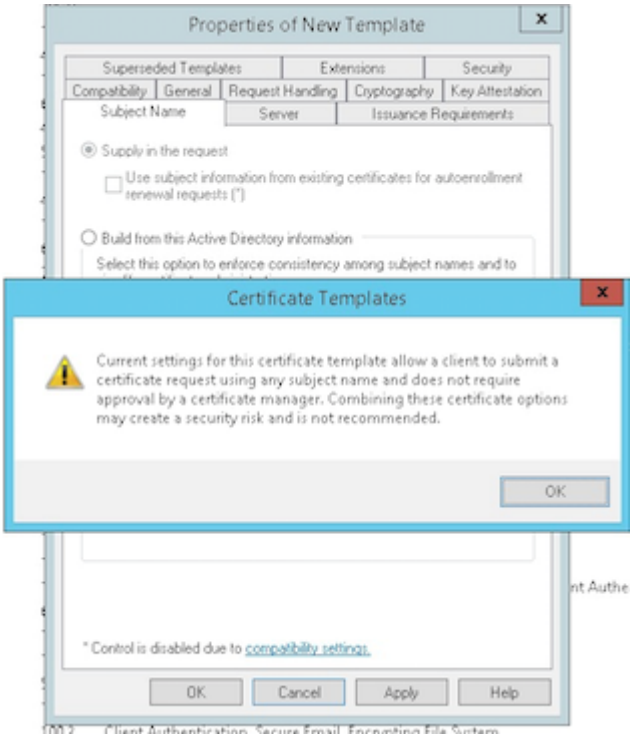
7. ［セキュリティ］ で、認証ユーザーの ［許可］ 列の ［登録］ オプションを選択します。



8. ［暗号化］ に、必ずキーのサイズを指定してください。あとで、XenMobile の構成中にキーのサイズを入力します。



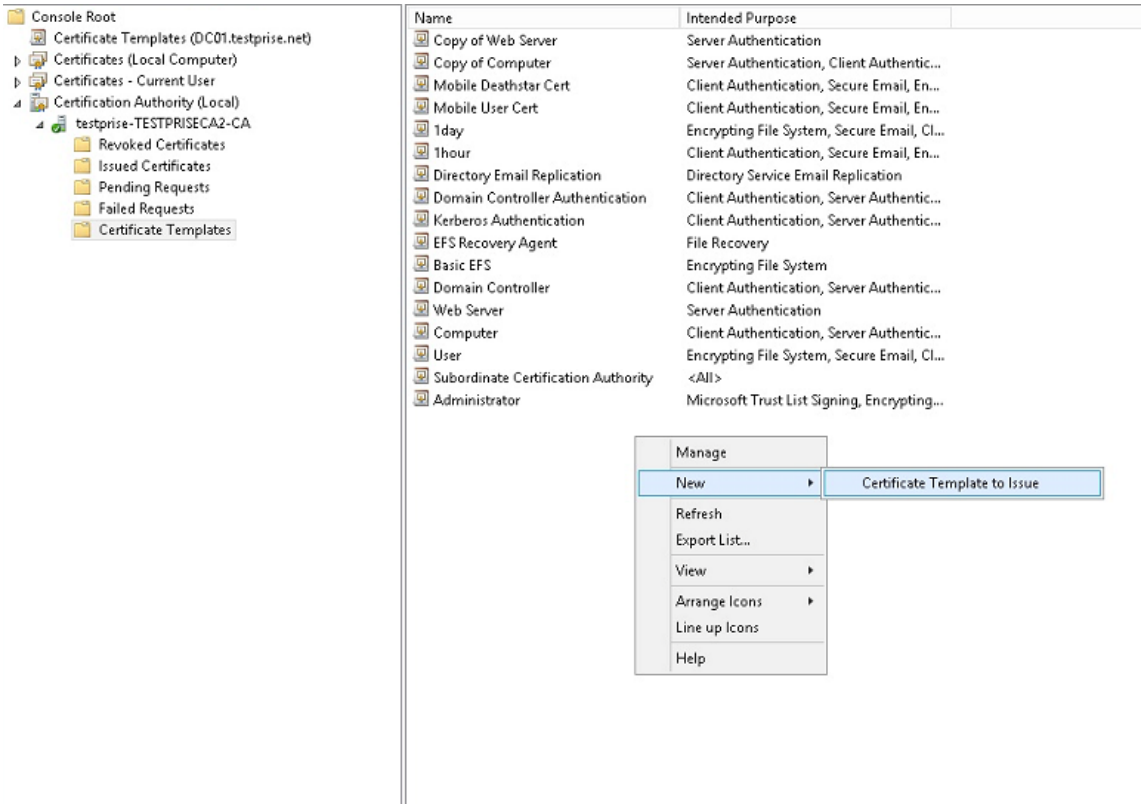
9. ［サブジェクト名］ で、［要求に含まれる］ を選択します。変更を適用して、保存します。



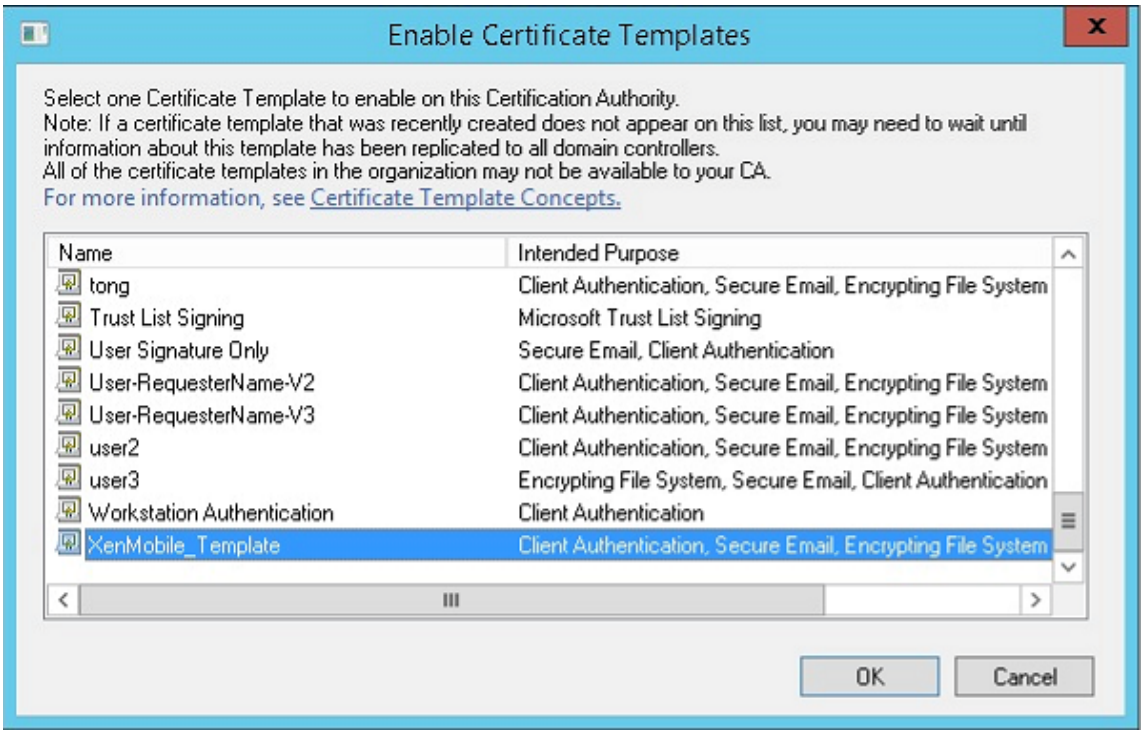
テンプレートを証明機関（**CA**）に追加する

1. ［証明機関］ に移動して、［証明書テンプレート］ を選択します。

2. 右ペインを右クリックして、［新規］、［発行する証明書テンプレート］ の順に選択します。

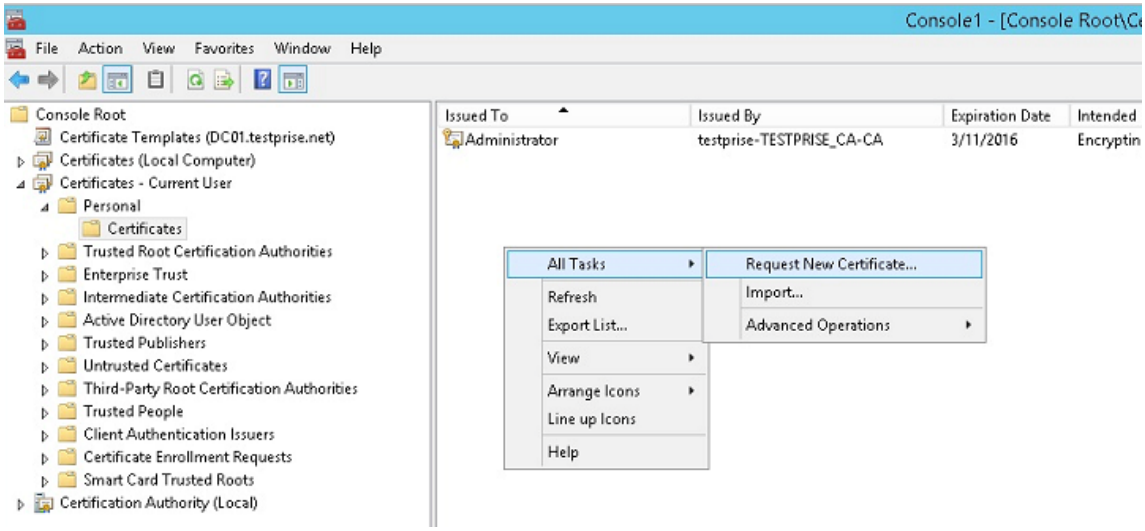


3. 前の手順で作成したテンプレートを選択し、［**OK**］ をクリックして ［証明機関］ に追加します。

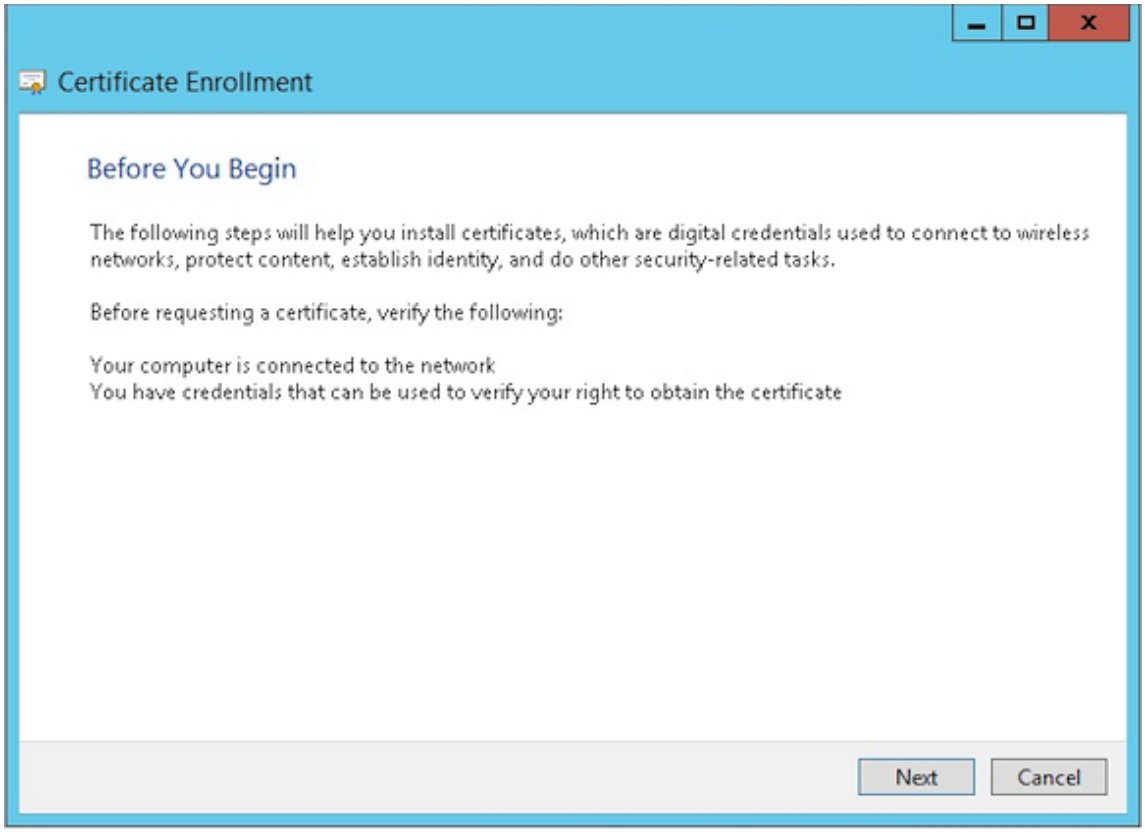


CA サーバーから PFX 証明書を作成する

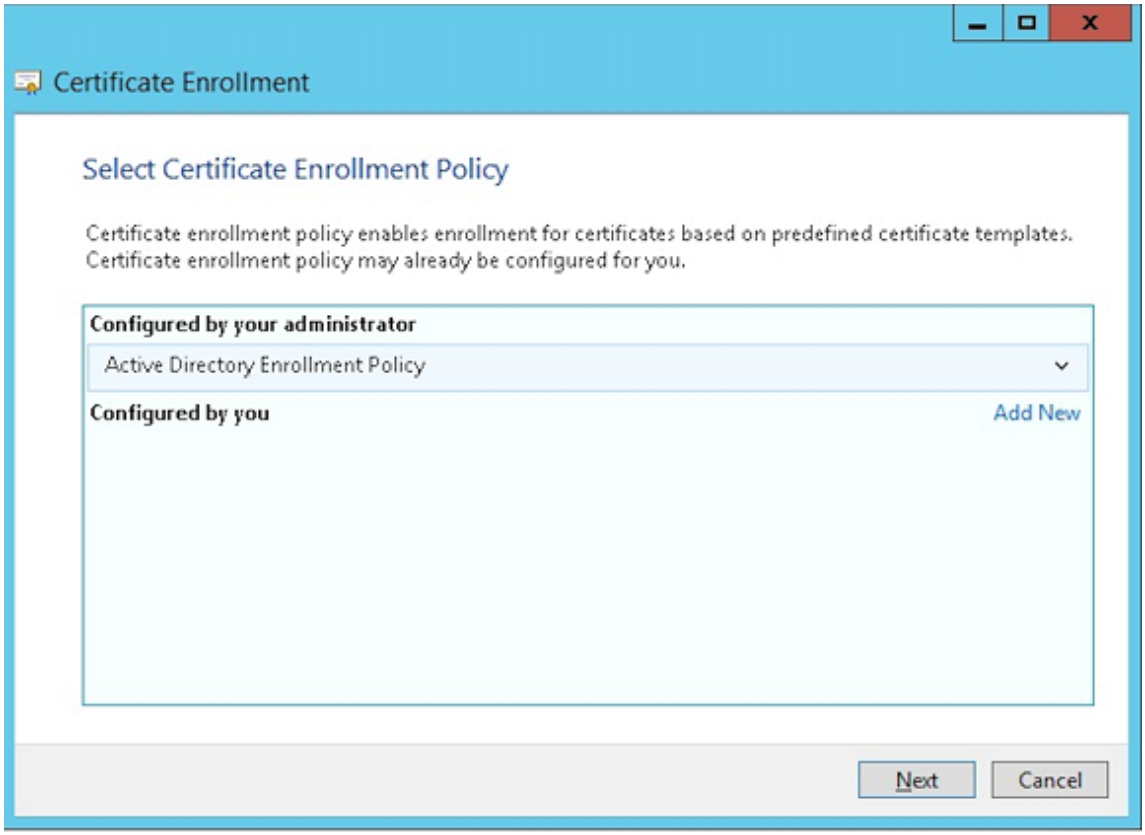
1. ログインしたサービスアカウントで、ユーザー.pfx cert を作成します。この.pfx ファイルは XenMobile にアップロードされ、デバイスを登録するユーザーのためにユーザー証明書を要求します。
2. [現在のユーザー] で、[証明書] を展開します。
3. 右ペインで右クリックし、[新しい証明書の要求] をクリックします。



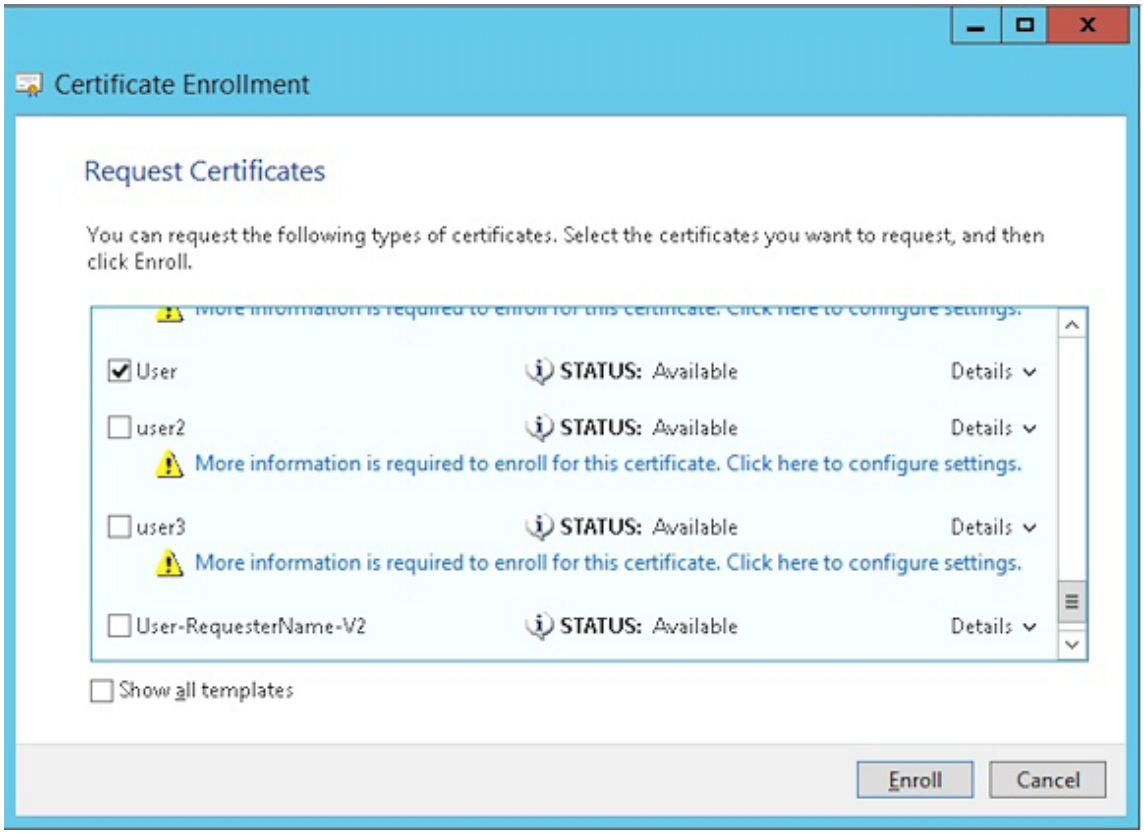
4. [証明書の登録] 画面が開きます。[次へ] をクリックします。



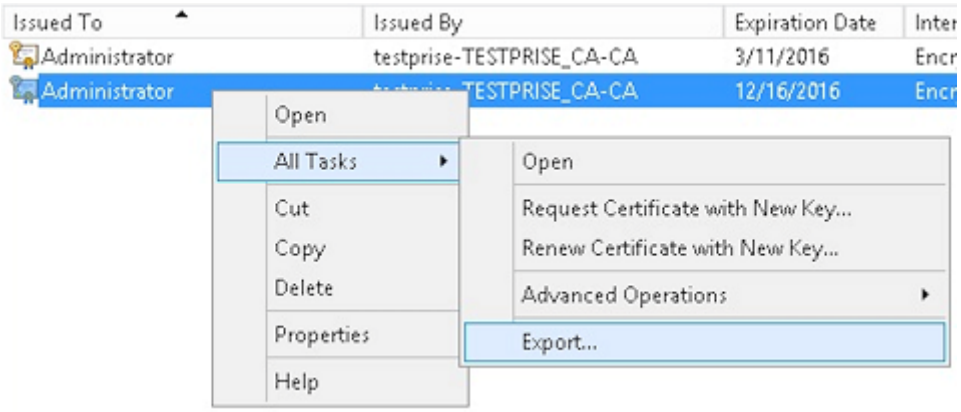
5. [**Active Directory** 登録ポリシー] を選択して [次へ] をクリックします。



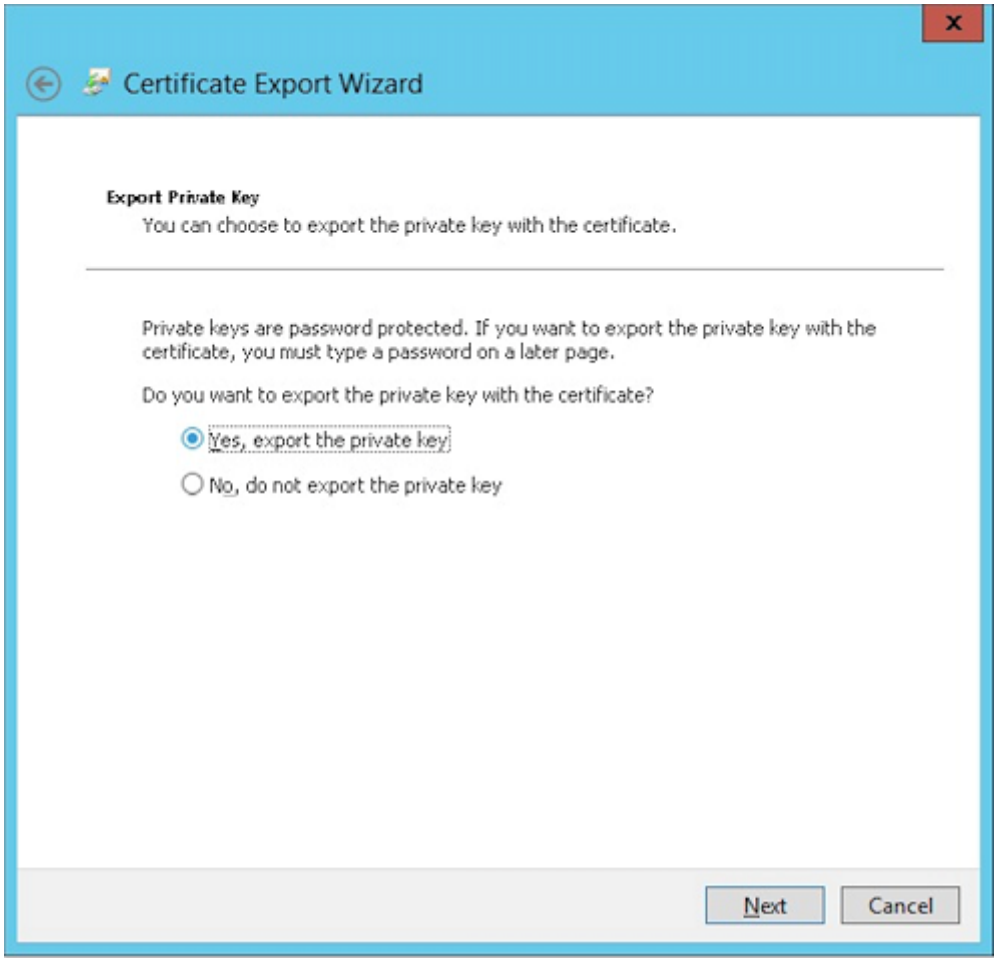
6. [ユーザー] テンプレートを選択し、[登録] をクリックします。



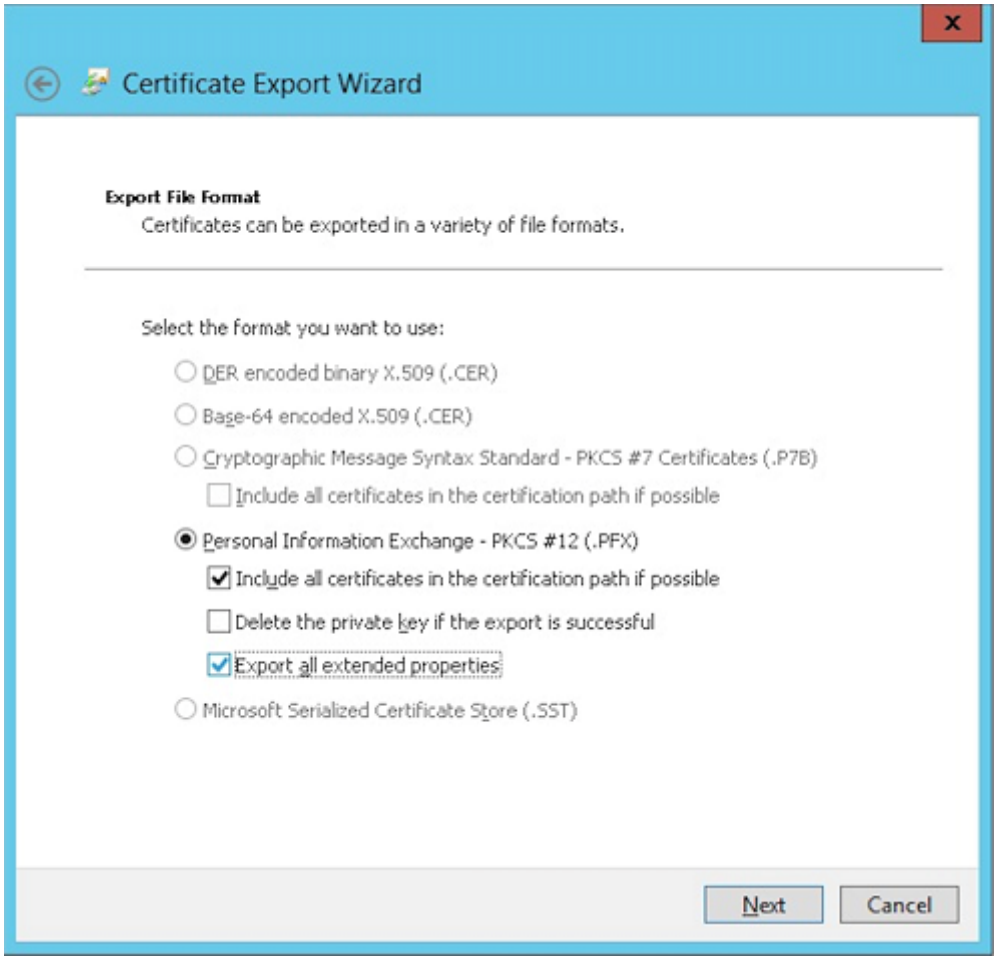
7. 前の手順で作成した.pfx ファイルをエクスポートします。



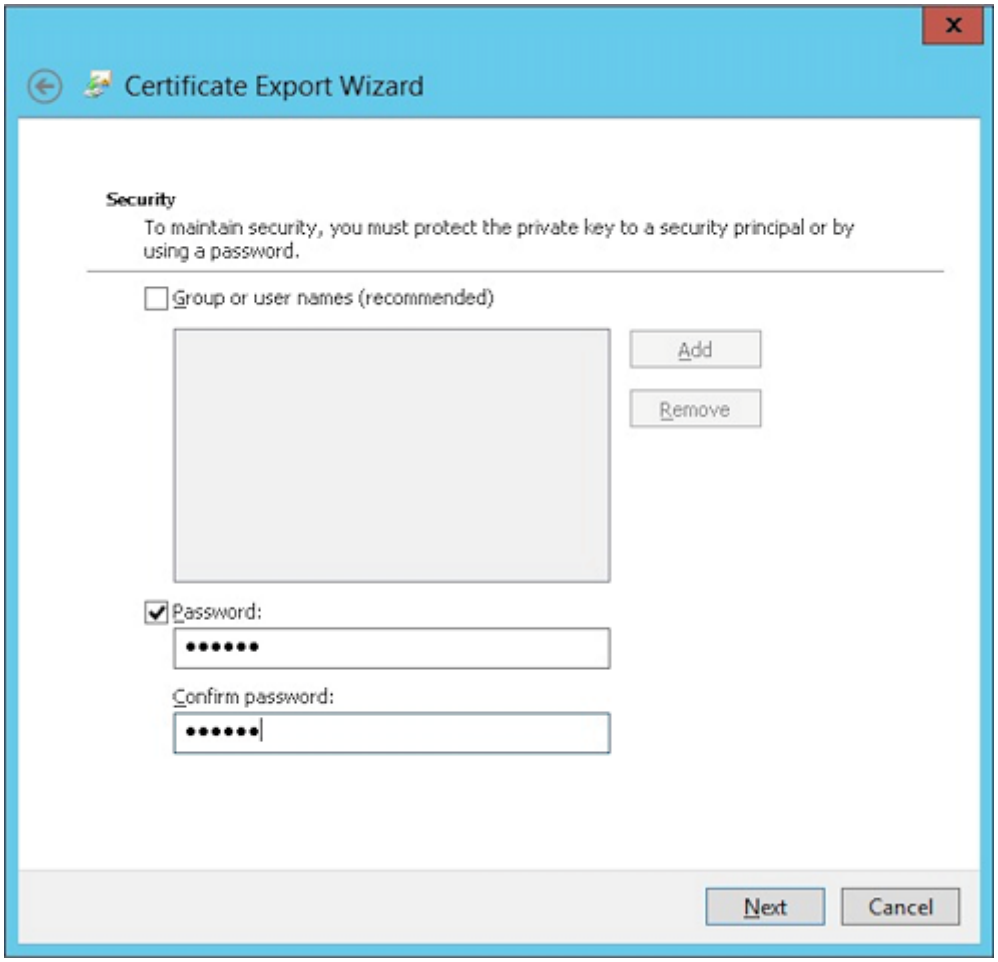
8. [はい、秘密キーをエクスポートします] をクリックします。



9. [証明のパスにある証明書を可能であればすべて含む] を選択し、[すべての拡張プロパティをエクスポートする] チェックボックスをオンにします。



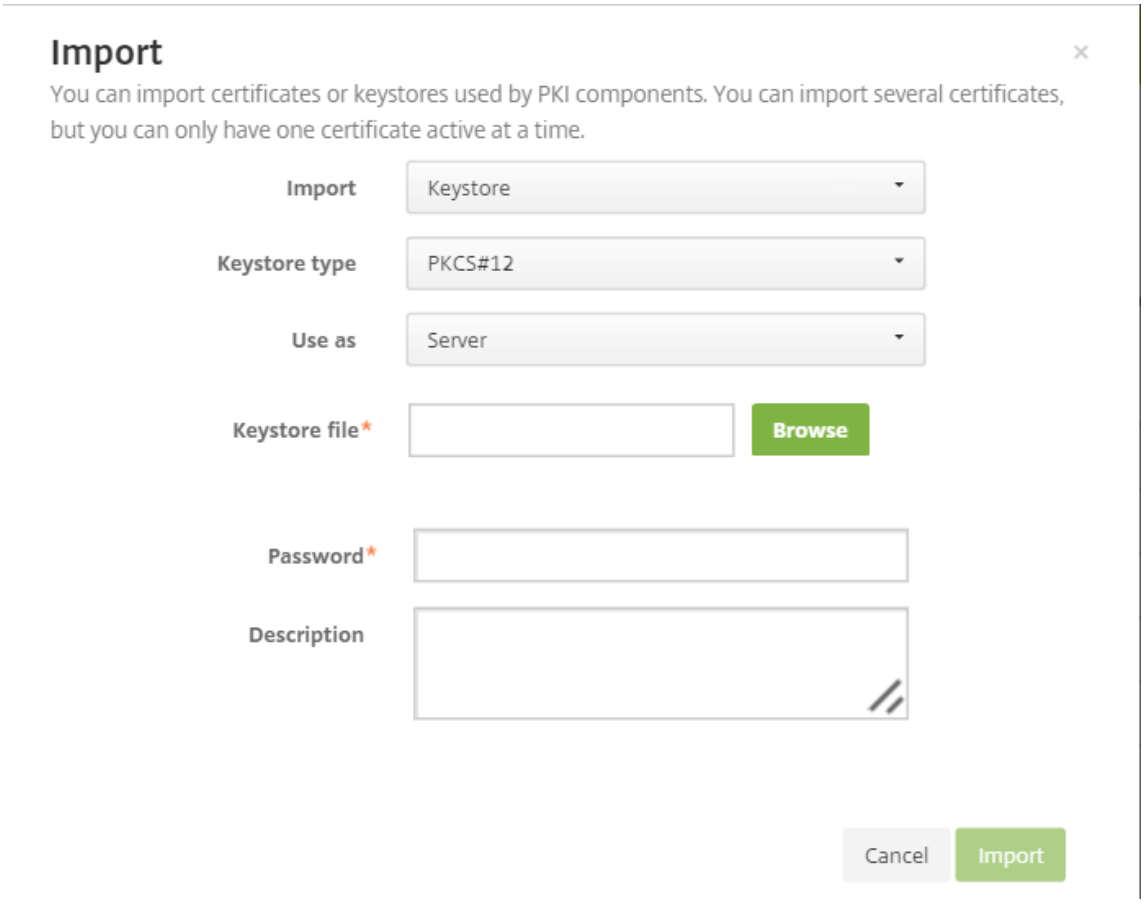
10. XenMobile にこの証明書をアップロードするときに使用するパスワードを設定します。



11. 証明書をローカルのハードドライブに保存します。

XenMobile への証明書のアップロード

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ 画面が表示されます。
2. ［証明書］ をクリックしてから、［インポート］ をクリックします。
3. 以下のパラメーターを入力します。
   - インポート： キーストア
   - キーストアの種類： PKCS#12
   - 使用目的： サーバー
   - キーストアファイル： ［参照］をクリックして、前の手順で作成した.pfx 証明書を選択します。
   - パスワード： この証明書用に作成したパスワードを入力します。

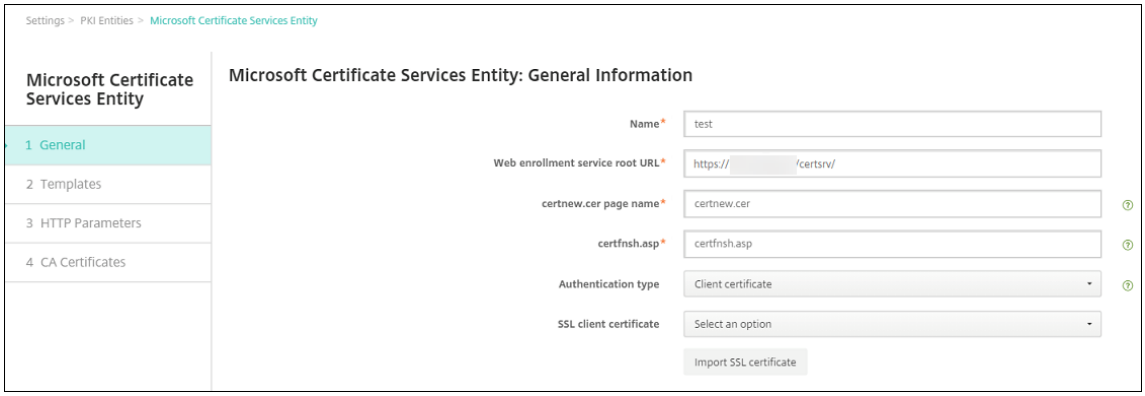


4. ［インポート］ をクリックします。
5. 証明書が正常にインストールされているか確認します。正常にインストールされた証明書がユーザー証明書として表示されます。

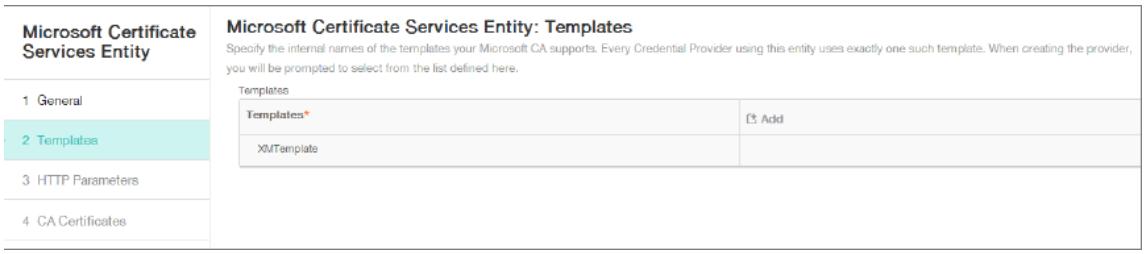
証明書に基づいた認証のための **PKI** エンティティの作成

1. ［設定］ で、 ［詳細］ **>** ［証明書管理］ **>** ［**PKI** エンティティ］ の順に移動します。
2. ［追加］ をクリックしてから、 ［**Microsoft** 証明書サービスエンティティ］ をクリックします。 ［**Microsoft** 証明書サービスエンティティ：一般的な情報］ 画面が開きます。
3. 以下のパラメーターを入力します。
   - 名前： 任意の名前を入力します。
   - **Web** 登録サービスルート **URL**： `https://RootCA-URL/certsrv/`（URL パスの最後にスラッシュ（/）があることを確認してください。）
   - **certnew.cer** ページ名： certnew.cer（デフォルト値）
   - **certfnsh.asp**： certfnsh.asp（デフォルト値）
   - 認証の種類： クライアント証明書

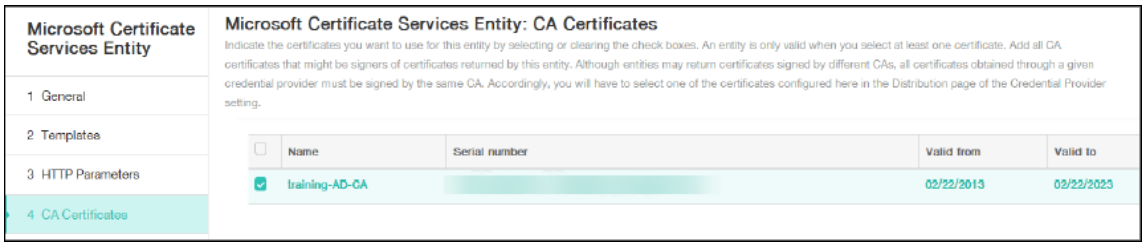
- **SSL** クライアント証明書: XenMobile クライアント証明書を発行するために使用するユーザー証明書を選択します。



4. [テンプレート] で、Microsoft 証明書を構成したときに作成したテンプレートを追加します。スペースを追加しないでください。



5. HTTP パラメーターをスキップし、 [**CA** 証明書] をクリックします。
6. 環境内で関連するルート CA 証明書の名前を選択します。このルート CA 証明書は、XenMobile クライアント証明書からインポートされたチェーンの一部です。



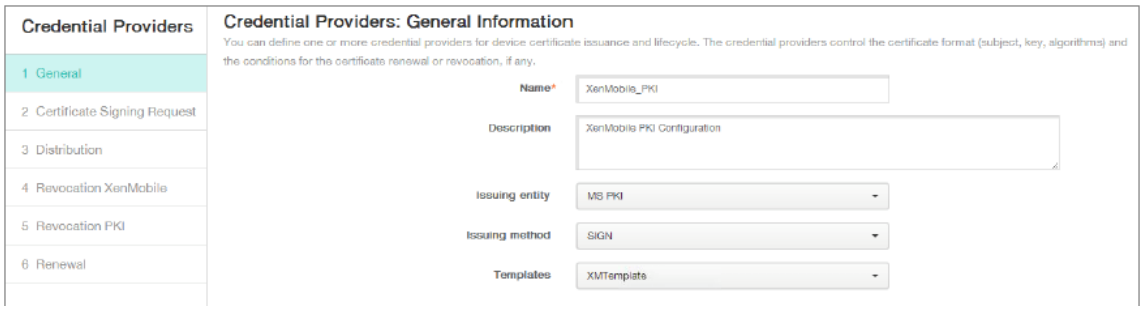
7. [保存] をクリックします。

資格情報プロバイダーの構成

1. [設定] で、 [詳細] > [証明書管理] > [資格情報プロバイダー] の順に移動します。
2. [追加] をクリックします。
3. [全般] で、次のパラメーターを入力します:

   - 名前: 任意の名前を入力します。

- 説明: 任意の説明を入力します。
- 発行エンティティ: 前に作成した PKI エンティティを選択します。
- 発行方式: SIGN
- テンプレート: PKI エンティティに追加されたテンプレートを選択します。



4. [証明書署名要求] をクリックしてから、次のパラメーターを入力します:

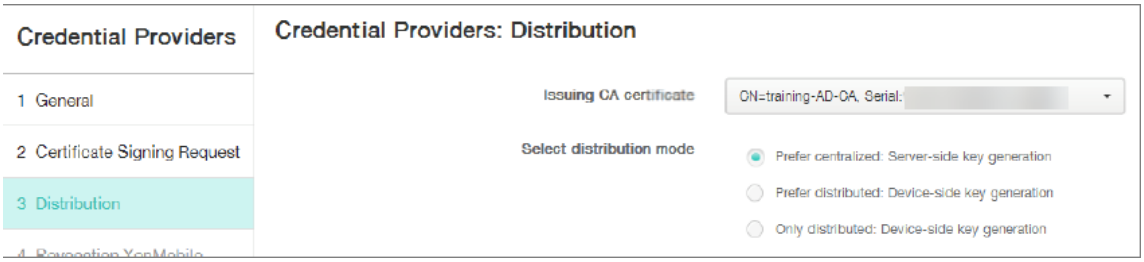
   - キーアルゴリズム: RSA
   - キーサイズ: 2048
   - 署名アルゴリズム: SHA1withRSA
   - サブジェクト名: `cn=$user.username`

   [サブジェクトの別名] の [追加] をクリックしてから、次のパラメーターを入力します:

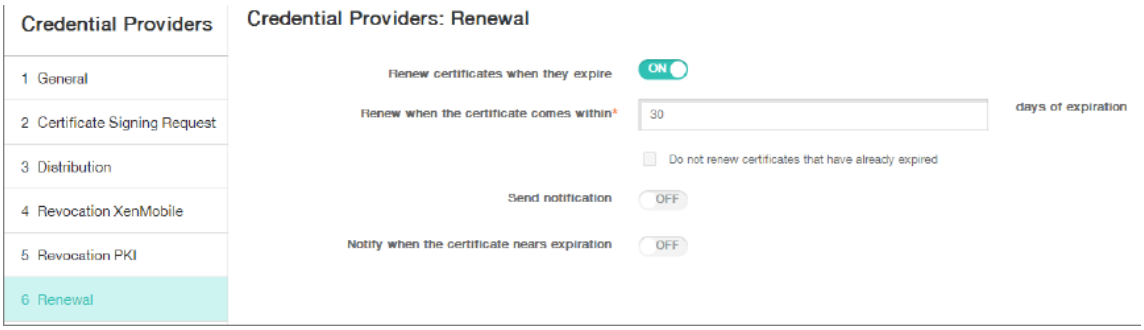
   - 種類: ユーザープリンシパル名
   - 値のデータ: `$user.userprincipalname`

5. [説明] をクリックし、次のパラメーターを入力します:

   - 発行 **CA** 証明書: 署名済みの XenMobile クライアント証明書の発行 CA を選択します。
   - ディストリビューションモードの選択: [集中を優先: サーバー側のキー生成] を選択します。



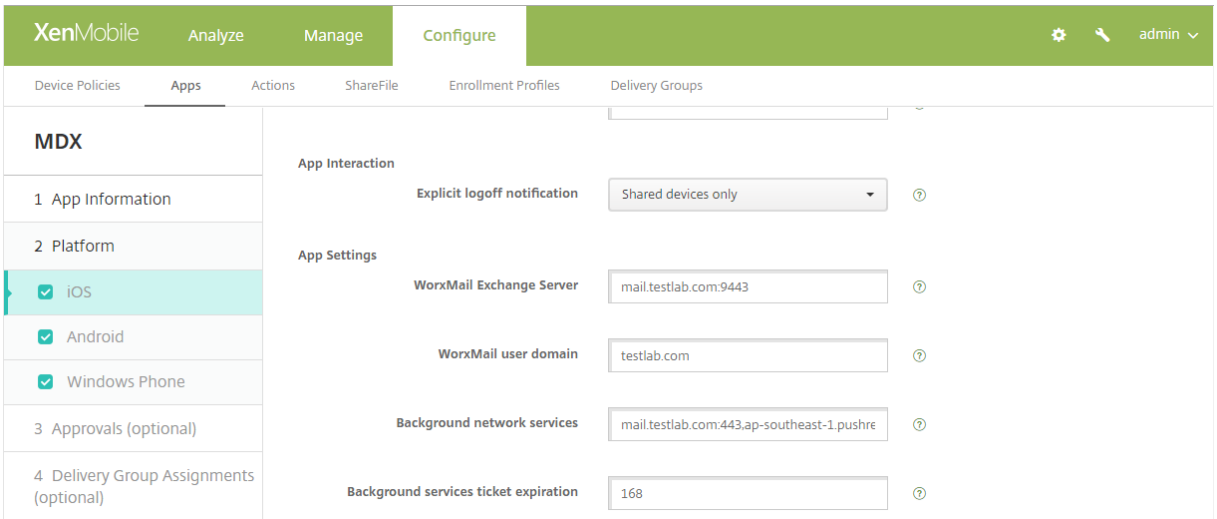
6. 次の 2 つのセクション、失効 **XenMobile** と失効 **PKI** で必要なパラメーターを設定します。この例では、どちらのオプションもスキップします。
7. [更新] をクリックします。
8. [有効期限が切れたら証明書を更新] で [オン] を選択します。
9. そのほかの設定はすべてそのままにするか、必要な変更を加えます。



10. [保存] をクリックします。

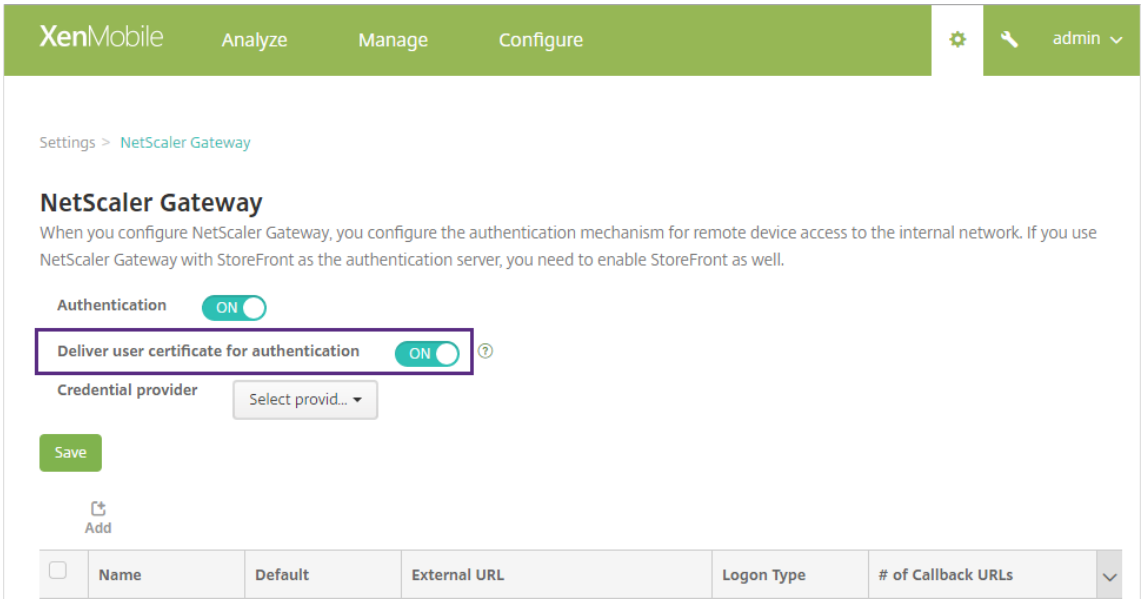
証明書ベースの認証を使用するように **Secure Mail** を構成する

XenMobile に Secure Mail を追加する場合、必ず [**App Settings**] で Exchange の設定を構成してください。

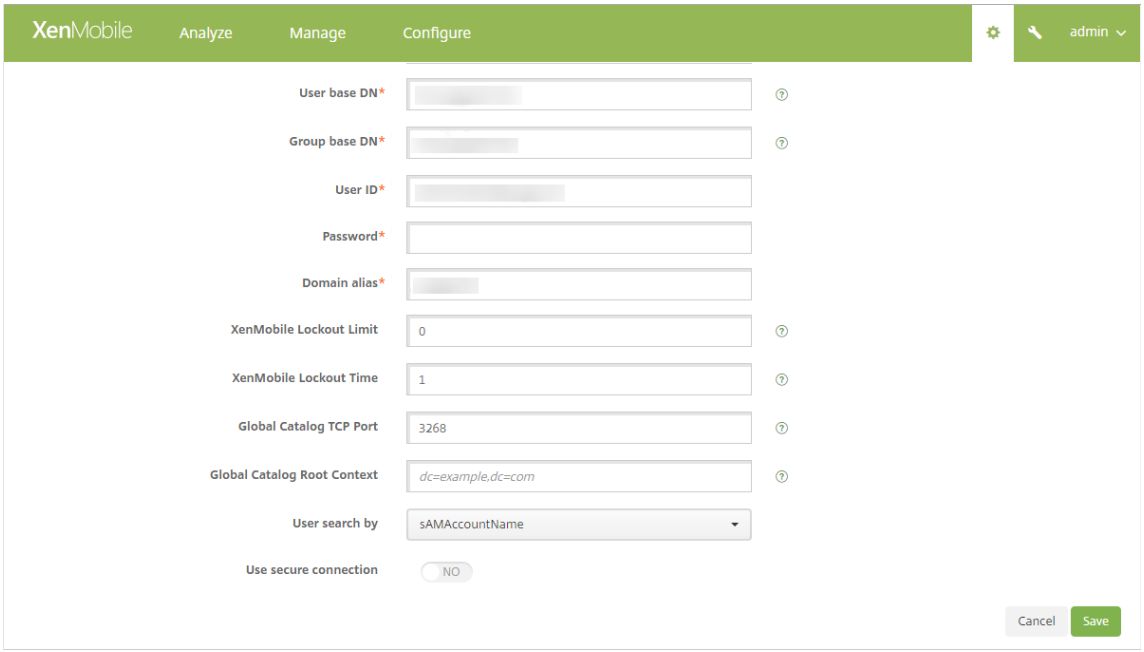


XenMobile での **NetScaler** 証明書の配信の構成

1. XenMobile コンソールにログオンして、右上の歯車アイコンをクリックします。［設定］ 画面が表示されます。
2. ［サーバー］ の下の ［**NetScaler Gateway**］ をクリックします。
3. NetScaler Gateway がまだ追加されていない場合、［追加］ をクリックして、次のように設定を指定します。
   - 外部 **URL**： `https://YourNetScalerGatewayURL`
   - ログオンの種類： 証明書およびドメイン
   - パスワードが必要： オフ
   - デフォルトとして設定： オン
4. ［認証用のユーザー証明書を配信］ で ［オン］ を選択します。



5. ［資格情報プロバイダー］ でプロバイダーを選択し、 ［保存］ をクリックします。
6. ユーザープリンシパル名（UPN）の代替としてユーザー証明書の sAMAccount 属性を使用するには、XenMobile の LDAP コネクタを次のように構成します： ［設定］ **>** ［**LDAP**］ に移動し、ディレクトリを選択して ［編集］ をクリックし、 ［ユーザー検索基準］ で ［**sAMAccountName**］ を選択します。



Citrix PIN とユーザーパスワードキャッシュの有効化

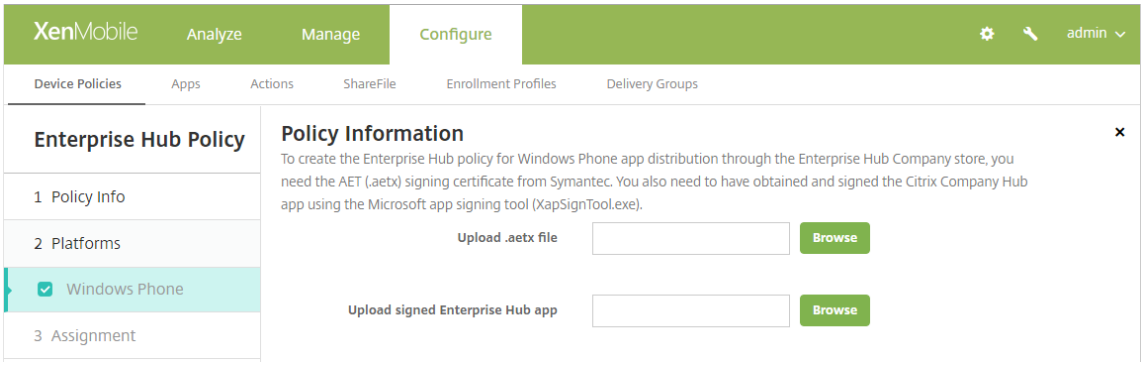
Citrix PIN とユーザーパスワードキャッシュを有効化するには、［設定］**>**［クライアントプロパティ］ に移動し、チェックボックス ［**Citrix PIN** 認証の有効化］ および ［ユーザーパスワードキャッシュの有効化］ をオンにします。詳しくは、「クライアントプロパティ」を参照してください。

Windows Phone 用のエンタープライズハブポリシーの作成

Windows Phone デバイスの場合、エンタープライズハブデバイスポリシーを作成して、AETX ファイルおよび Secure Hub クライアントを配信する必要があります。

> 注:
>
> AETX ファイルと Secure Hub ファイルの両方が次のものを使用していることを確認してください:
>
> - 証明書プロバイダーの同じエンタープライズ証明書。
> - Windows ストア開発者アカウントの同じ発行者 ID。

1. XenMobile コンソールで、［構成］**>**［デバイスポリシー］ をクリックします。
2. ［追加］ をクリックした後、［詳細］**>**［**XenMobile** エージェント］ の下の ［エンタープライズハブ］ をクリックします。
3. ポリシーに名前を付けた後で、エンタープライズハブに対して適切な.AETX ファイルと署名された Secure Hub アプリを選択します。



4. ポリシーをデリバリーグループに割り当て、保存します。

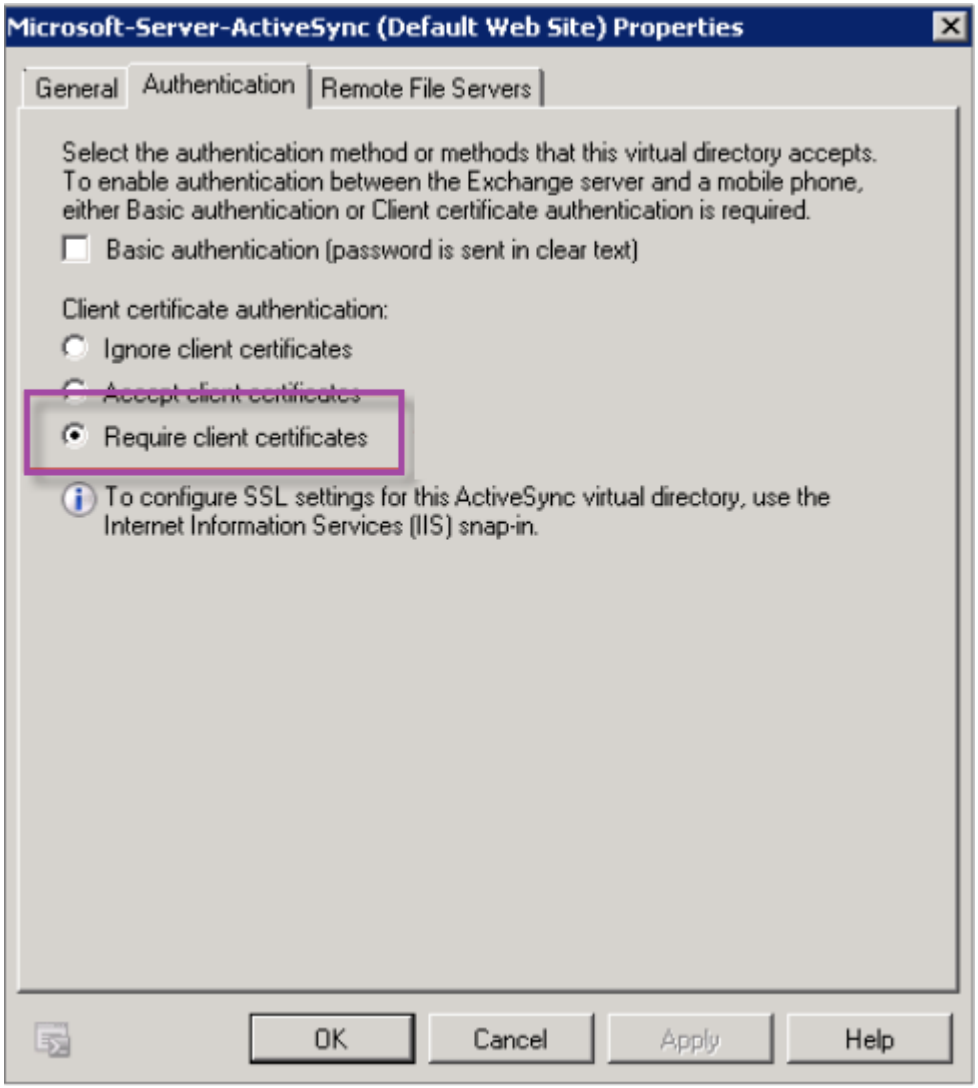
クライアント証明書構成のトラブルシューティング

先行する構成と NetScaler Gateway の構成が成功すると、ユーザーワークフローは次のようになります。

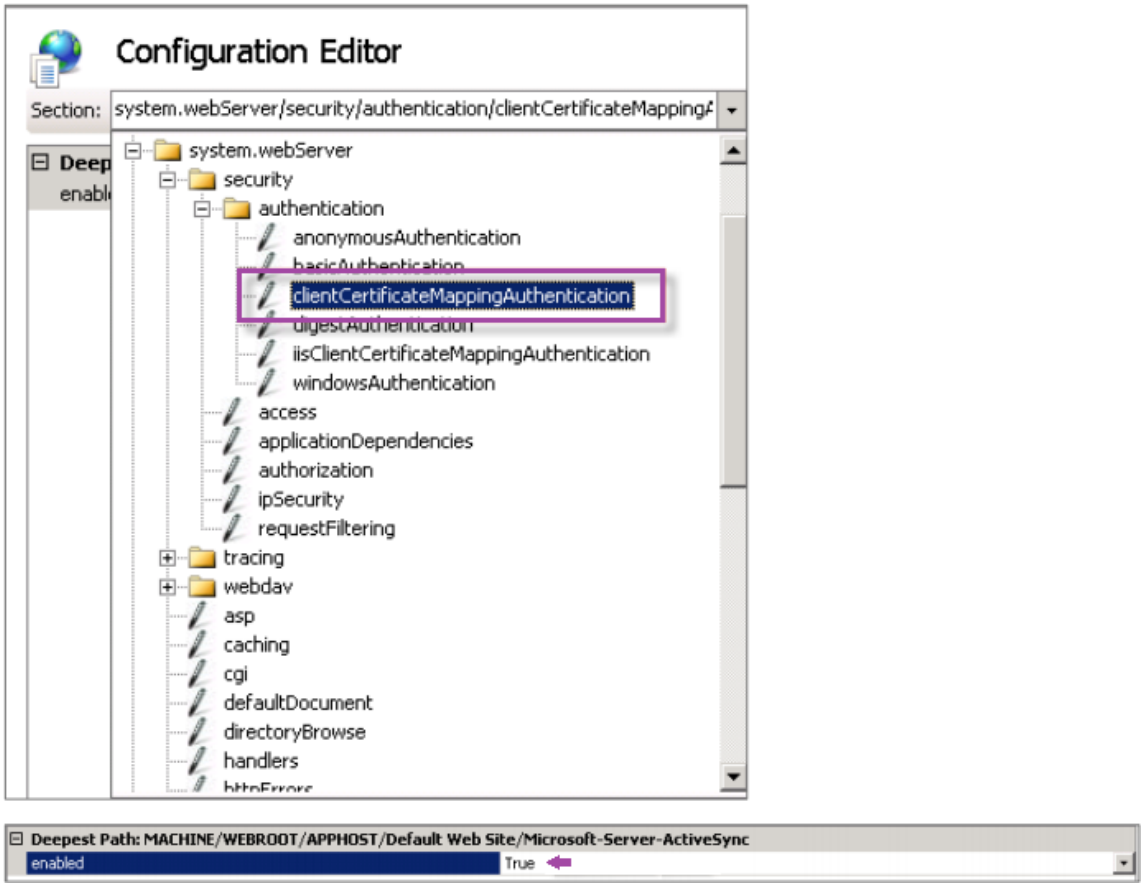
1. ユーザーがモバイルデバイスを登録します。
2. XenMobile がユーザーに Citrix PIN を作成するよう求めます。
3. ユーザーが XenMobile Store にリダイレクトされます。
4. Secure Mail の起動時、XenMobile はメールボックスの構成でユーザー資格情報を要求しません。その代わりに、Secure Mail は Secure Hub からのクライアント証明書を要求し、認証のために Microsoft Exchange Server に送信します。ユーザーが Secure Mail を起動したときに XenMobile で資格情報を求められた場合は、構成を確認してください。

ユーザーは Secure Mail をダウンロードしてインストールできるが、Secure Mail でメールボックス構成時に構成を完了できない場合:

1. Microsoft Exchange Server ActiveSync がプライベート SSL サーバー証明書を使用してトラフィックを保護している場合、ルート証明書または中間証明書がモバイルデバイスにインストールされていることを確認してください。
2. ActiveSync に対して選択された認証の種類が ［クライアント証明書を要求する］ であることを確認します。



3. Microsoft Exchange Server で、**Microsoft-Server-ActiveSync** サイトのクライアント証明書マッピング認証が有効になっていることを確認します。デフォルトでは、クライアント証明書マッピング認証は無効になっています。オプションは、［**Configuration Editor**］**>**［**Security**］**>**［**Authentication**］にあります。



［**True**］ を選択したら、必ず ［適用］ をクリックして変更を反映してください。

4. XenMobile コンソールで NetScaler Gateway 設定を確認します: ［認証用のユーザー証明書を配信］ が［オン］ で、［資格情報プロバイダー］ で適切なプロファイルが選択されていることを確認してください。

クライアント証明書がモバイルデバイスに配信されたかどうかを判定するには

1. XenMobile コンソールで、［管理］ **>** ［デバイス］ と移動して、デバイスを選択します。
2. ［編集］ または ［詳細表示］ をクリックします。
3. ［デリバリーグループ］ セクションに移動し、以下のエントリを検索します:

   NetScaler Gateway 資格情報: 必要な資格情報、**CertId=**

クライアント証明書ネゴシエーションが有効かどうか確認するには

1. このnetshコマンドを実行して、IIS Web サイトにバインドされた SSL 証明書構成を表示します。

   ```
   netsh http show sslcert
   ```


2. ［クライアント証明書のネゴシエート］ の値が ［無効］ の場合、次のコマンドを実行して有効化します：

```
netsh http delete sslcert ipport=0.0.0.0:443

netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={
 app_id } certstorename=store_name verifyclientcertrevocation=Enable
 VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable
clientcertnegotiation=Enable
```

次に例を示します：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c54
 appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreNam
 verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

XenMobile を介して Windows Phone 8.1 デバイスにルート証明書または中間証明書を配信できない場合：

- 電子メールを介して Windows Phone 8.1 デバイスにルート証明書または中間証明書（.cer）ファイルを送信し、直接インストールします。

Secure Mail が Windows Phone 8.1 に正常にインストールされない場合は、以下を確認してください：

- Enterprise ハブデバイスポリシーを使用して、XenMobile 経由でアプリケーション登録トークン（.AETX ファイル）が配信されている。
- アプリケーション登録トークンが、Secure Mail のラップおよび Secure Hub アプリの署名に使用された証明書プロバイダーからのエンタープライズ証明書と同じものを使用して作成されている。
- Secure Hub、Secure Mail、アプリケーション登録トークンのラップと署名に同一の発行者 ID が使用されている。

PKI エンティティ

January 24, 2020

XenMobile の PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）エンティティ構成は、実際の PKI 処理（発行、失効、状態情報）を実行するコンポーネントを表します。これらのコンポーネントは、XenMobile に対して内部または外部のどちらかです。内部コンポーネントは、任意として参照されます。外部コンポーネントは企業インフラストラクチャの一部です。

XenMobile は次の種類の PKI エンティティをサポートします。

- 汎用 PKIs（GPKIs）

  XenMobile Server の汎用 PKI サポートには、DigiCert マネージド PKI が含まれます。

- Microsoft 証明書サービス

- 任意 CA（Certificate Authority：証明機関）

XenMobile では、次の CA サーバーがサポートされます。

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

共通の **PKI** 概念

種類に関係なく、すべての PKI エンティティには以下の機能のサブセットがあります。

- 署名： 証明書署名要求（CSR）に基づく新しい証明書の発行
- フェッチ： 既存の証明書とキーペアの回収
- 失効： クライアント証明書の失効

CA 証明書

PKI エンティティを構成するときに、そのエンティティにより発行される（またはそのエンティティから回収される）証明書の署名者である CA 証明書を XenMobile に示します。その PKI エンティティから、複数の異なる CA が署名した、（フェッチされたか、または新たに署名された）証明書が返されることがあります。

これらの CA それぞれの証明書を、PKI エンティティ構成の一部として提供します。これを行うために、証明書を XenMobile にアップロードして、PKI エンティティでそれらを参照します。任意 CA の場合、証明書は暗黙的に署名 CA 証明書です。外部エンティティの場合は、証明書を手動で指定する必要があります。

> 重要：
>
> Microsoft 証明書サービスのエンティティテンプレートを作成する場合は、登録済みデバイスの認証に関する問題を避けるため、テンプレート名に特殊文字を使用しないでください。たとえば、以下は使用しないでください：`! : $ ( )## % + * ~ ? | { } [ ]`

汎用 **PKI**

汎用 PKI（Generic PKI：GPKI）プロトコルは、さまざまな PKI ソリューションとの統一された連携を目的として SOAP Web サービスレイヤーで実行される独自の XenMobile プロトコルです。GPKI プロトコルは、以下の 3 つの基本 PKI 処理を定義します。

- 署名： アダプターは CSR を取得し、それらの要求を PKI に送信して、新しい署名入り証明書を返すことができます。
- フェッチ： アダプターは既存の証明書とキーペア（入力パラメーターによる）を PKI から取得できます。
- 失効： アダプターは PKI で特定の証明書を失効させることができます。

GPKI プロトコルの受信側は GPKI アダプターです。GPKI アダプターによって、基本処理がそのアダプターが作成された特定の種類の PKI に変換されます。たとえば、RSA や Entrust 用の GPKI アダプターがあります。

GPKI アダプターは、SOAP Web サービスのエンドポイントとして、自己記述型の Web Services Description Language（WSDL）定義を公開します。GPKI PKI エンティティの作成は、URL を通じてまたはファイルそのものをアップロードして、XenMobile にその WSDL 定義を提供することを意味します。

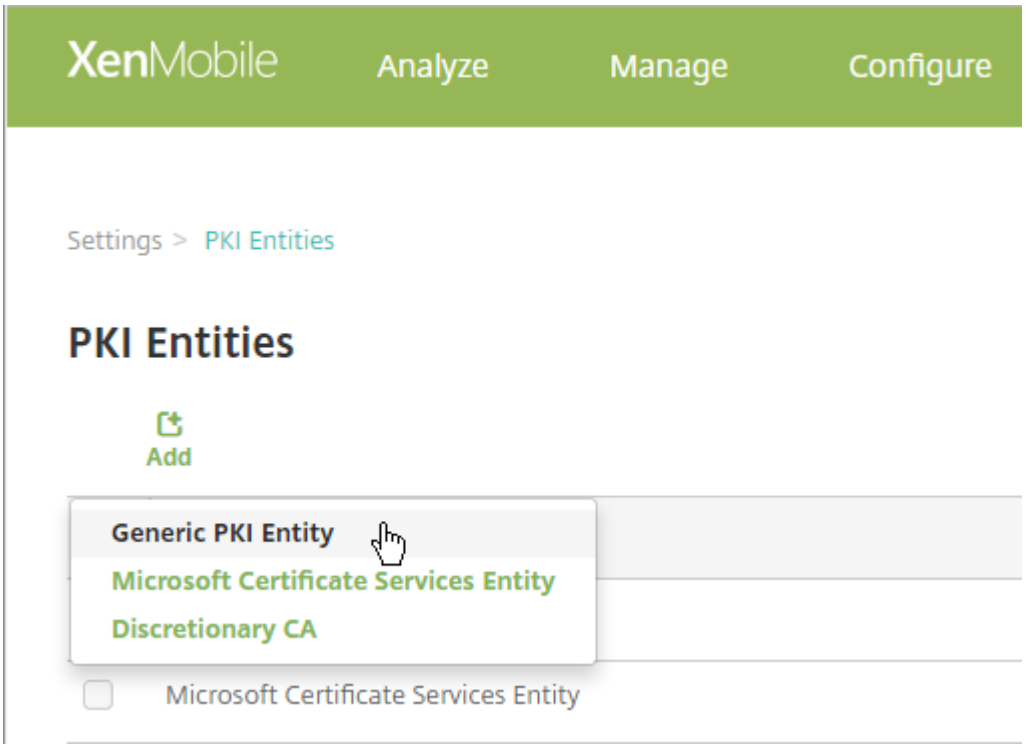
アダプターでの各 PKI 操作のサポートはオプションです。アダプターが特定の処理をサポートする場合、アダプターには対応する機能（署名、フェッチ、失効）があると見なされます。これらの各機能は一連のユーザーパラメーターに関連付けられている場合があります。

ユーザーパラメーターは、特定の処理について GPKI アダプターで定義されるパラメーターで、XenMobile に値を提供する必要があります。アダプターが実行する処理と各処理に必要なパラメーターは、XenMobile により WSDL ファイルを解析して決定されます。選択した場合、SSL クライアント認証によって XenMobile と GPKI アダプターの間の接続が保護されます。

汎用 **PKI** を追加するには

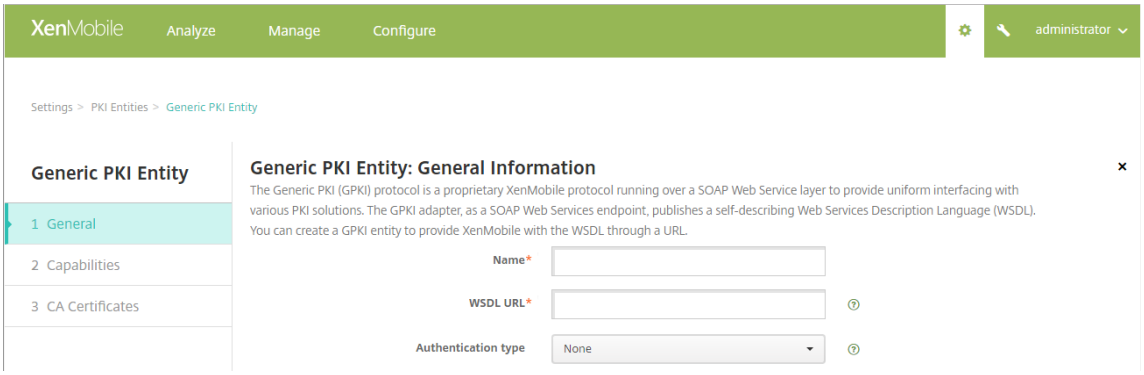
1. XenMobile コンソールで、［設定］、［**PKI** エンティティ］ の順にクリックします。
2. ［**PKI** エンティティ］ ページで、［追加］ をクリックします。

   PKI エンティティタイプのメニューが表示されます。



3. ［汎用 **PIK** エンティティ］ をクリックします。

   ［汎用 PKI エンティティ: 一般情報］ページが開きます。



4. [汎用 **PKI** エンティティ**:** 一般情報] ページで、以下を行います。

   - 名前: PKI エンティティの説明的な名前を入力します。
   - **WSDL URL**: アダプターについて記述している WSDL の場所を入力します。
   - 認証の種類: 使用する認証方法を選択します。
   - なし
   - **HTTP** 基本: アダプターへの接続に必要なユーザー名とパスワードを指定します。
   - クライアント証明書: 適切な SSL クライアント証明書を選択します。

5. [次へ] をクリックします。

   [汎用 PKI エンティティ: アダプターの機能] ページが開きます。

6. [汎用 **PKI** エンティティ: アダプターの機能] ページで、アダプターに関連付けられた機能とパラメーターを確認して、[次へ] をクリックします。

   [汎用 **PKI** エンティティ: **CA** 証明書の発行] ページが表示されます。

7. [汎用 PKI エンティティ: CA 証明書の発行] ページで、エンティティで使用する証明書を選択します。

   エンティティからは、異なる CA によって署名された証明書が返される場合がありますが、特定の証明書プロバイダーから取得される証明書の署名は、すべて同じ CA によって行われる必要があります。したがって、資格情報プロバイダー設定を構成するときに、[ディストリビューション] ページで、ここで構成したいずれかの証明書を選択してください。

8. [保存] をクリックします。

   [PKI エンティティ] の表にエンティティが表示されます。

DigiCert マネージド **PKI**

XenMobile Server の汎用 PKI サポートには、DigiCert マネージド PKI（MPKI とも呼ばれる）が含まれます。このセクションでは、DigiCert マネージド PKI 用に Windows Server と XenMobile Server をセットアップする方法について説明します。

前提条件

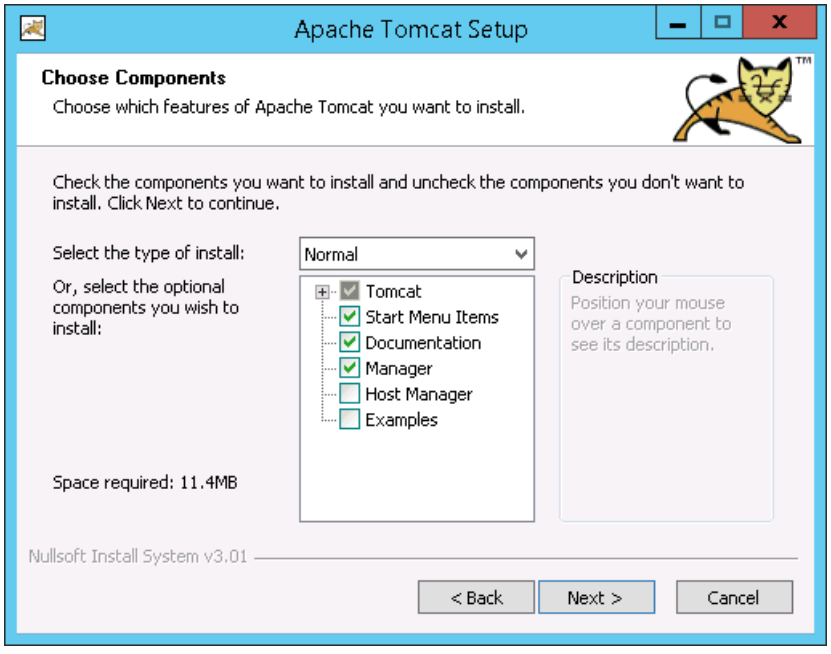
- DigiCert マネージド PKI インフラへのアクセス
- この記事で説明した、次のコンポーネントがインストールされた Windows Server 2012 R2 サーバー:
  - Java
  - Apache Tomcat
  - DigiCert PKI クライアント
  - Portecle
- XenMobile ダウンロードサイトへのアクセス

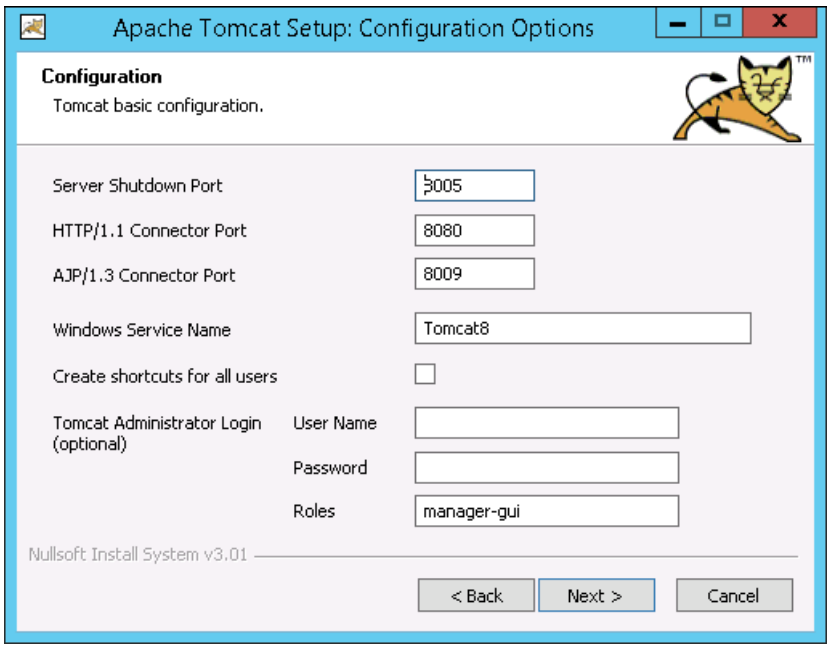
Windows Server への **Java** のインストール

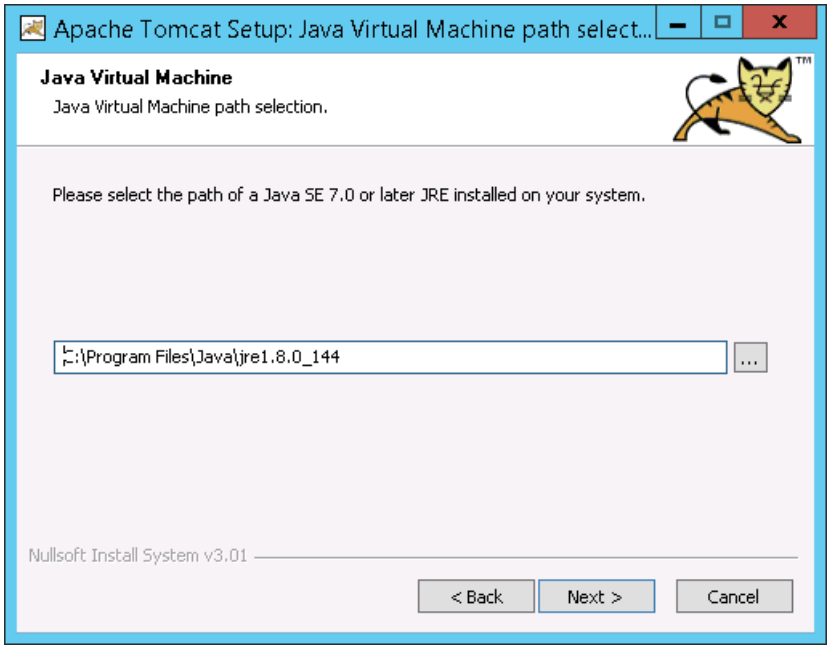
Java をhttps://java.com/en/download/faq/java_win64bit.xmlからダウンロードして、インストールします。[セキュリティの警告] ダイアログボックスで、 [実行] をクリックします。

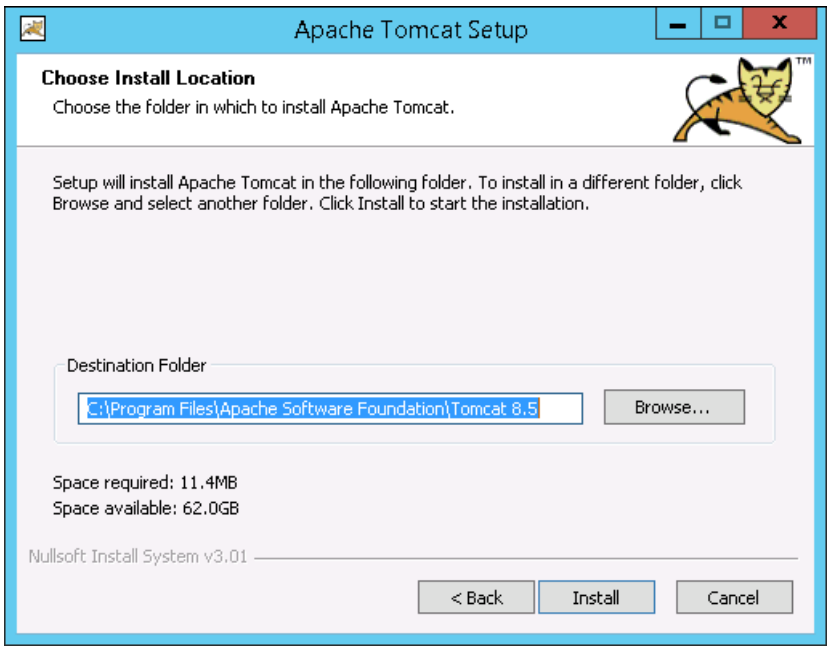
Windows Server に **Apache Tomcat** をインストールする

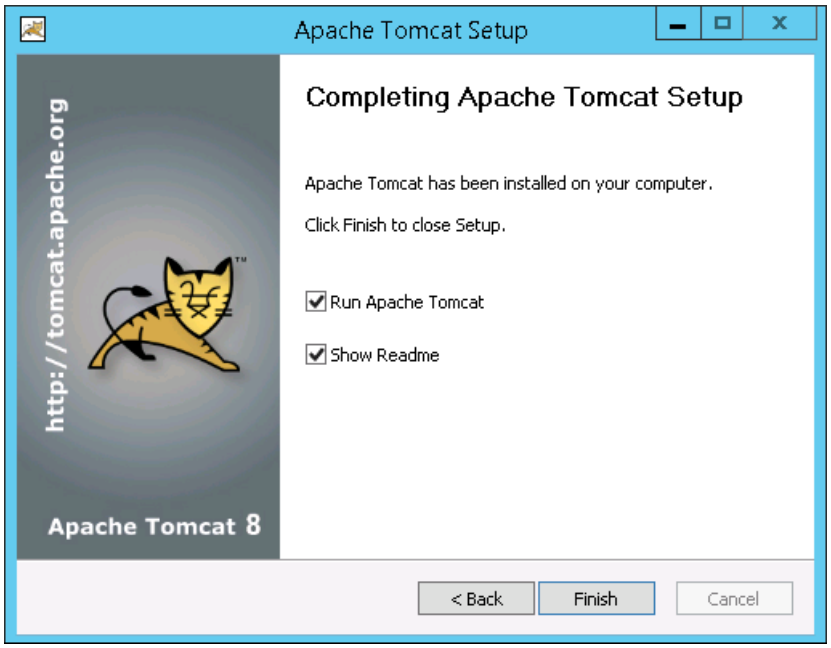
Apache Tomcat（32 ビットまたは 64 ビットバージョン）の Windows サービスインストーラーをhttps://tomcat.apache.org/download-80.cgiからダウンロードして、インストールします。[セキュリティの警告] ダイアログボックスで、 [実行] をクリックします。次の例を参考にして、Apache Tomcat のセットアップを完了します。



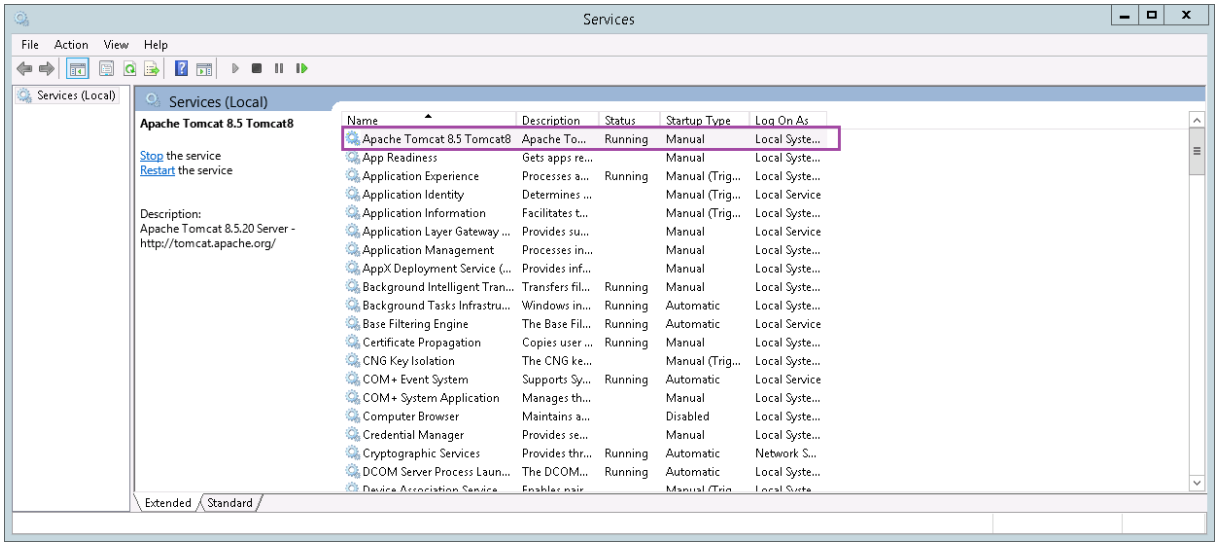


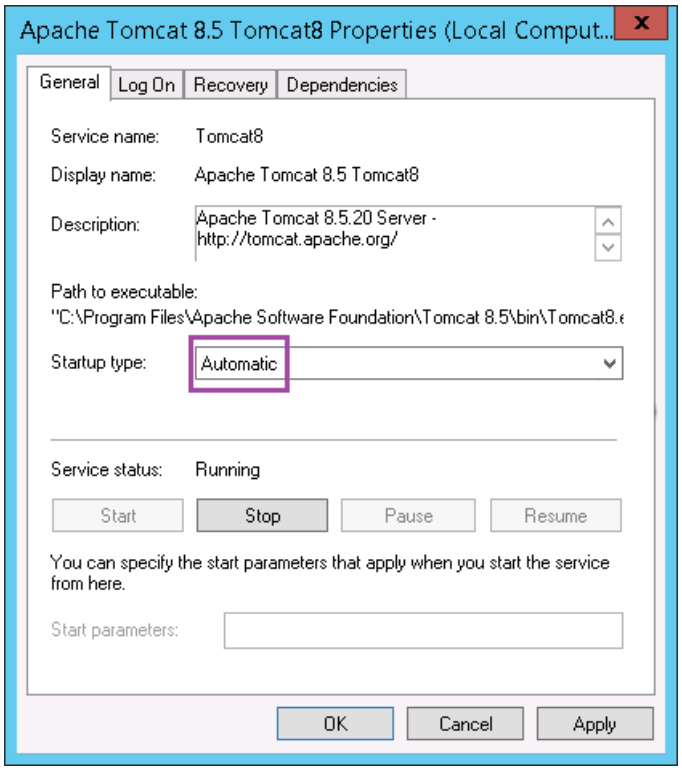






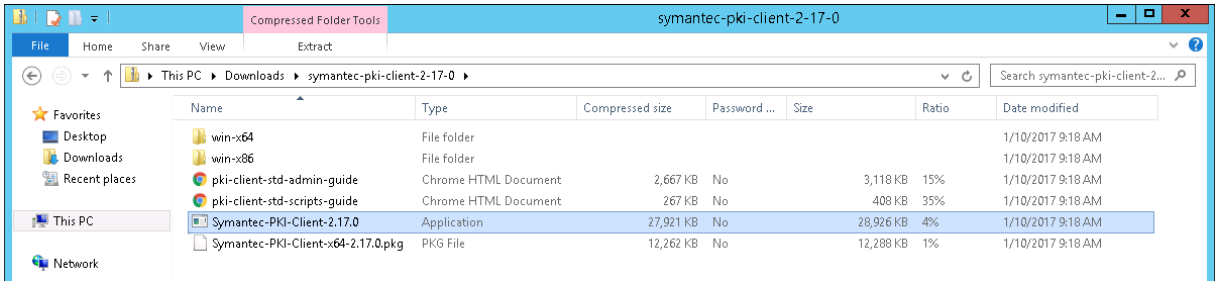
次に［Windows サービス］に移動して、［スタートアップの種類］ を ［手動］ から ［自動］ に変更します。

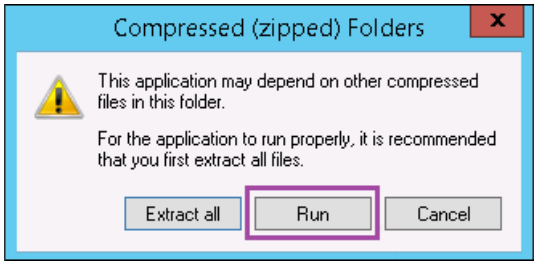




Windows Server に **DigiCert PKI Client** をインストールする

PKI Manager コンソールからインストーラーをダウンロードします。このコンソールにアクセスできない場合は、DigiCert のサポートページ（DigiCert PKI クライアントのダウンロード方法）からインストーラーをダウンロードします。圧縮解除してインストーラーを実行します。





[セキュリティの警告] ダイアログボックスで、 [実行] をクリックします。インストーラーに従ってセットアップを完了します。インストーラーが完了すると、再起動するように求められます。

Windows Server に **Portecle** をインストールする

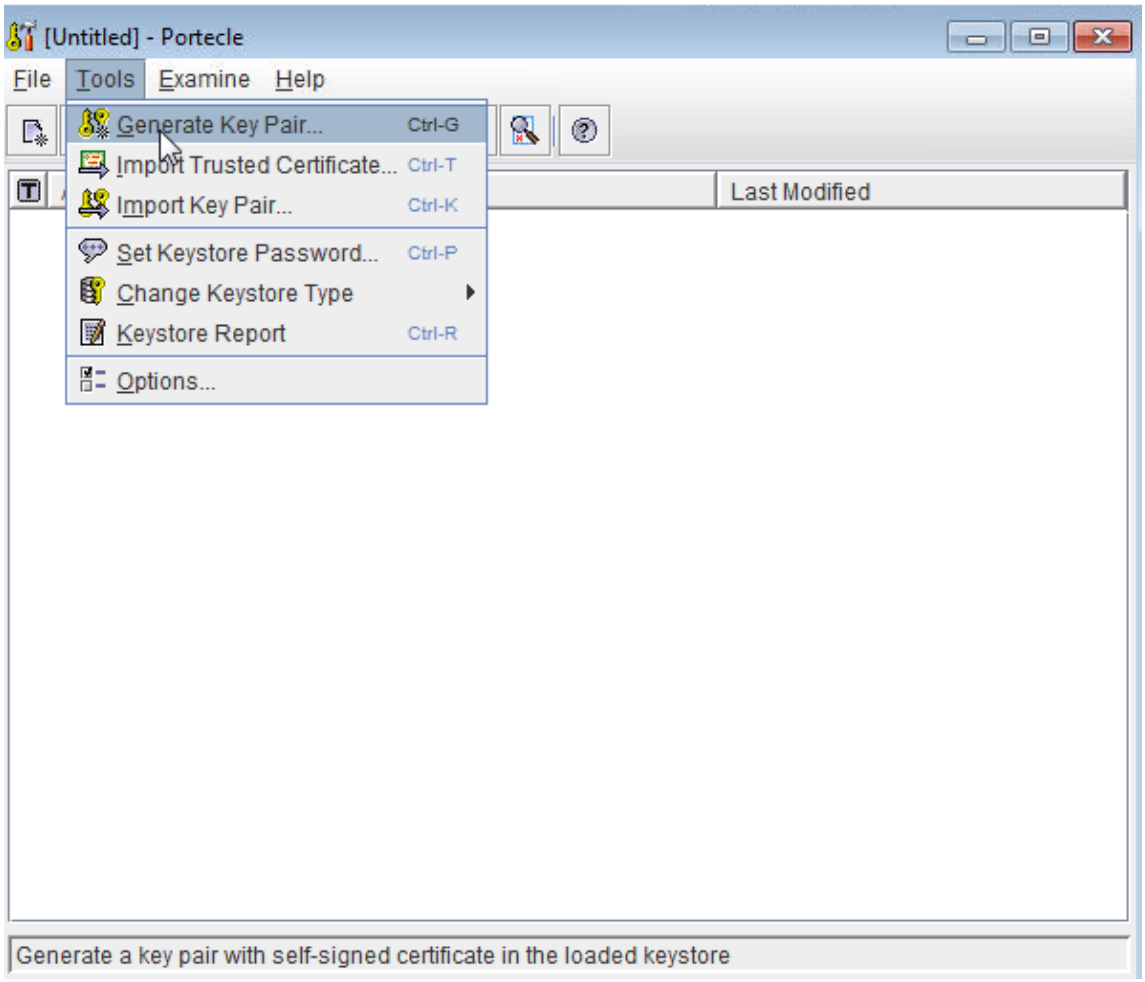
https://sourceforge.net/projects/portecleinstall/files/からインストーラーをダウンロードし、解凍してインストーラーを実行します。

DigiCert マネージド **PKI** の登録機関（**RA**）証明書を生成する

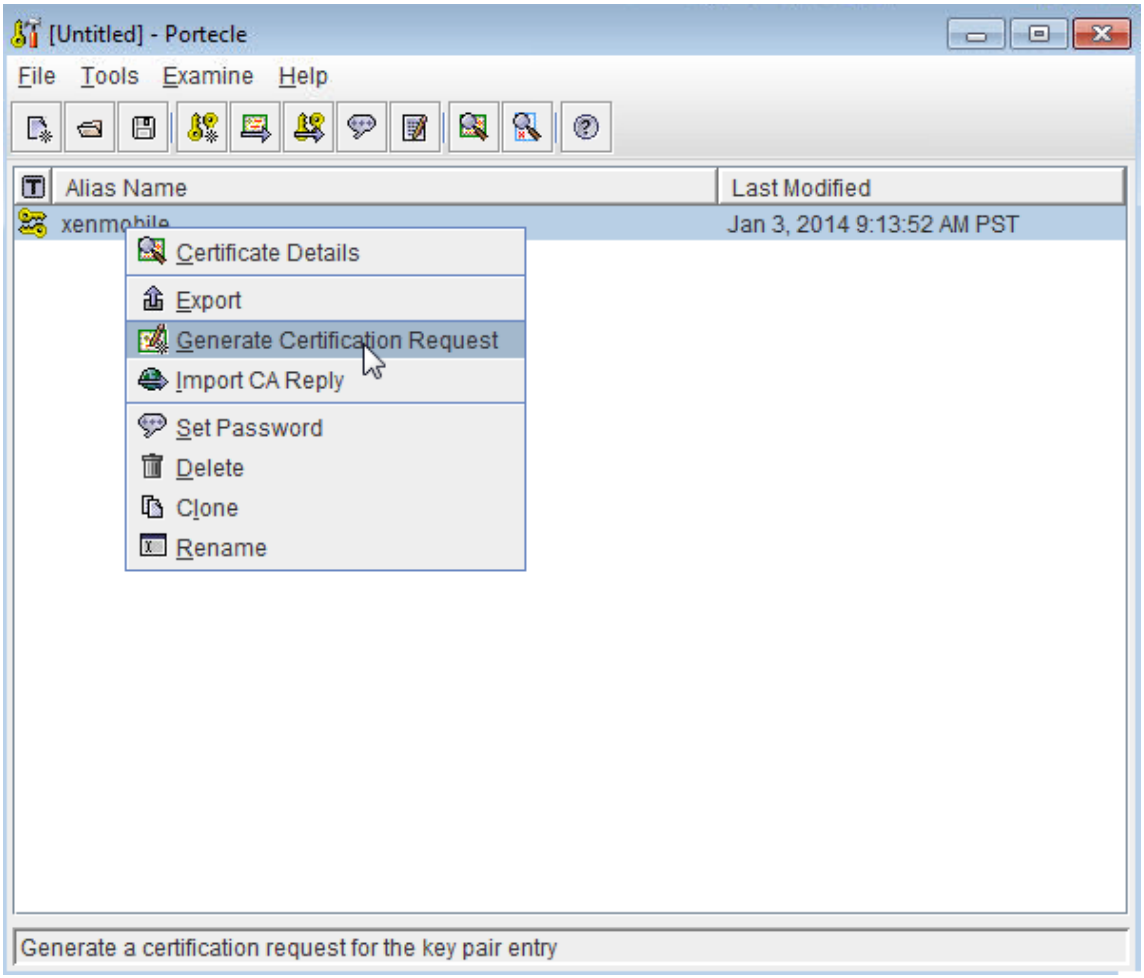
クライアント証明書認証用のキーストアは、RA.jks という名前の登録機関（RA）証明書に含まれています。次の手順では、Portecle を使用してその証明書を生成する方法について説明します。Java CLI を使用して RA 証明書を生成することもできます。

また、RA とパブリック証明書をアップロードする方法についても説明します。

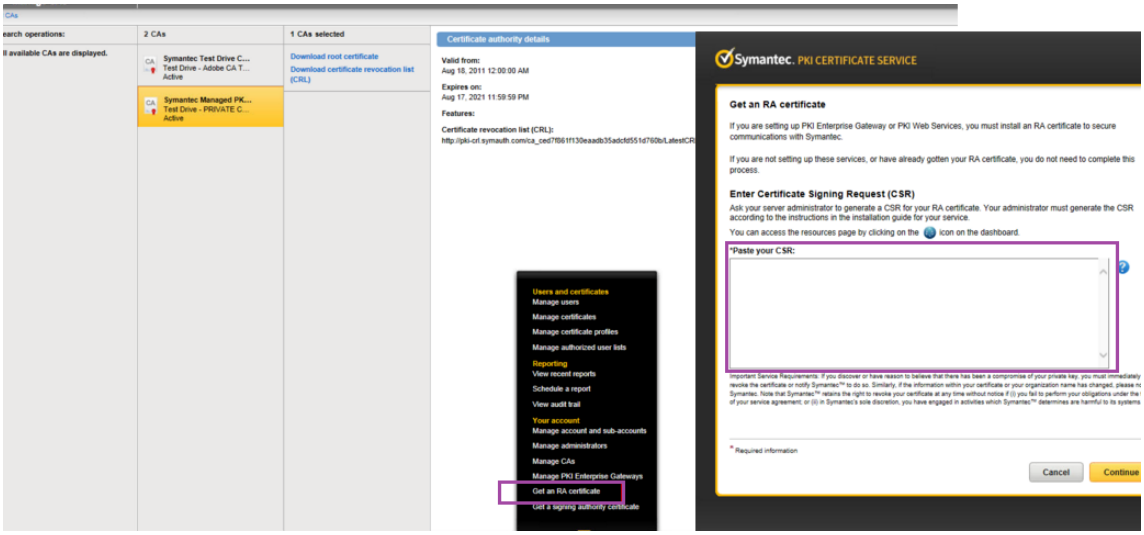
1. Portecle で [**Tools**] の [**Generate Key Pair**] に移動し、必要な情報を入力してキーペアを生成します。



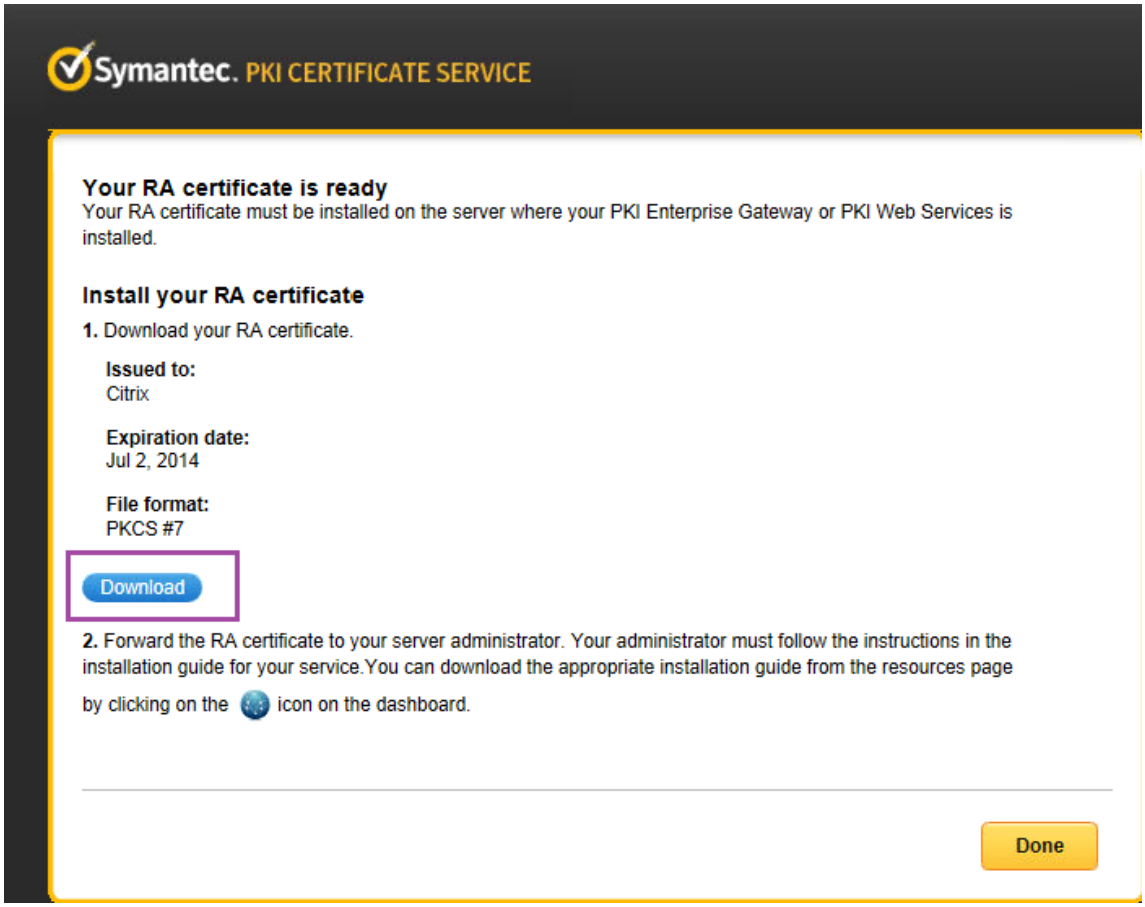
2. キーペアを右クリックし、［**Generate Certification Request**］ を選択します。



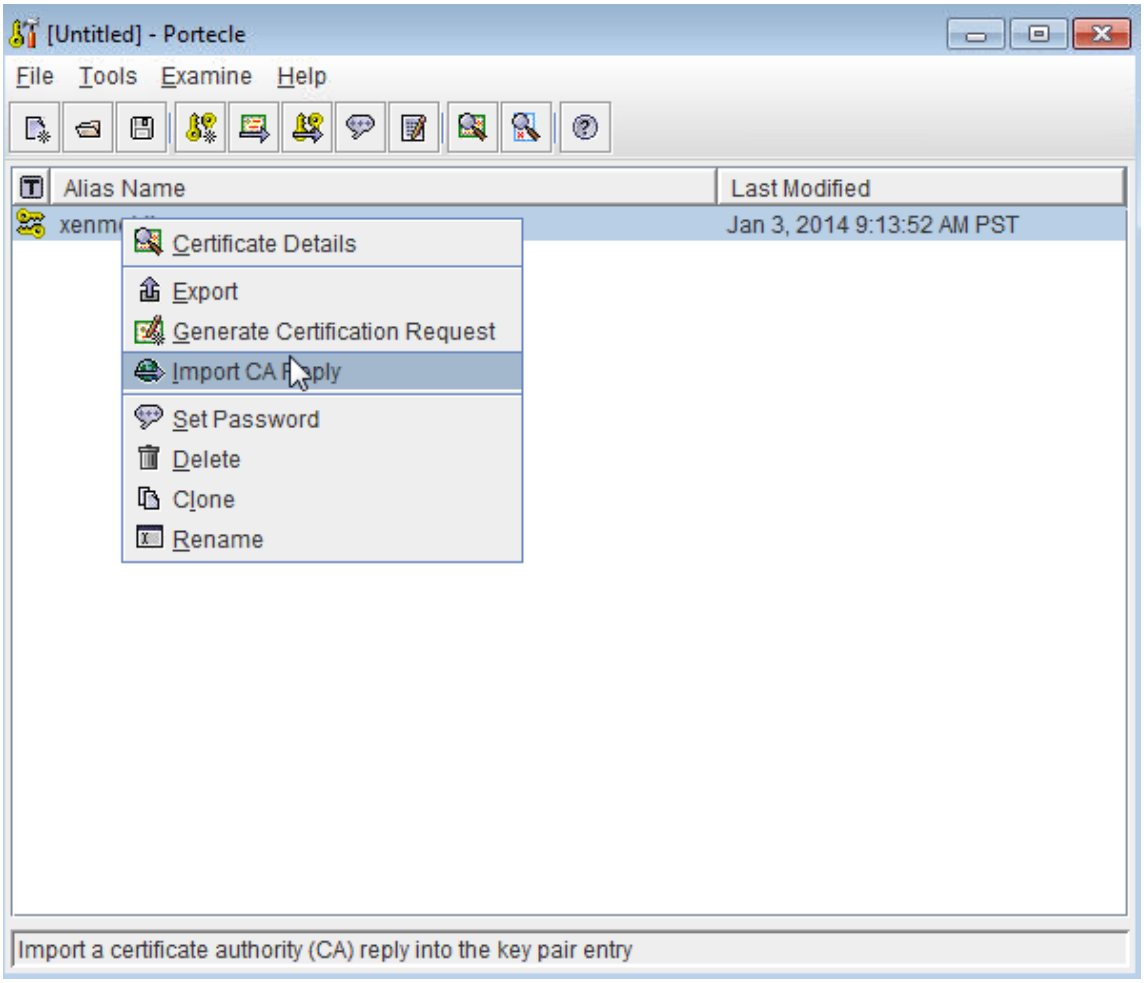
3. CSR をコピーします。
4. DigiCert PKI Manager で RA 証明書を生成する: ［**Settings**］、［**Get a RA Certificate**］ の順にクリックし、CSR を貼り付け、［**Continue**］ をクリックします。



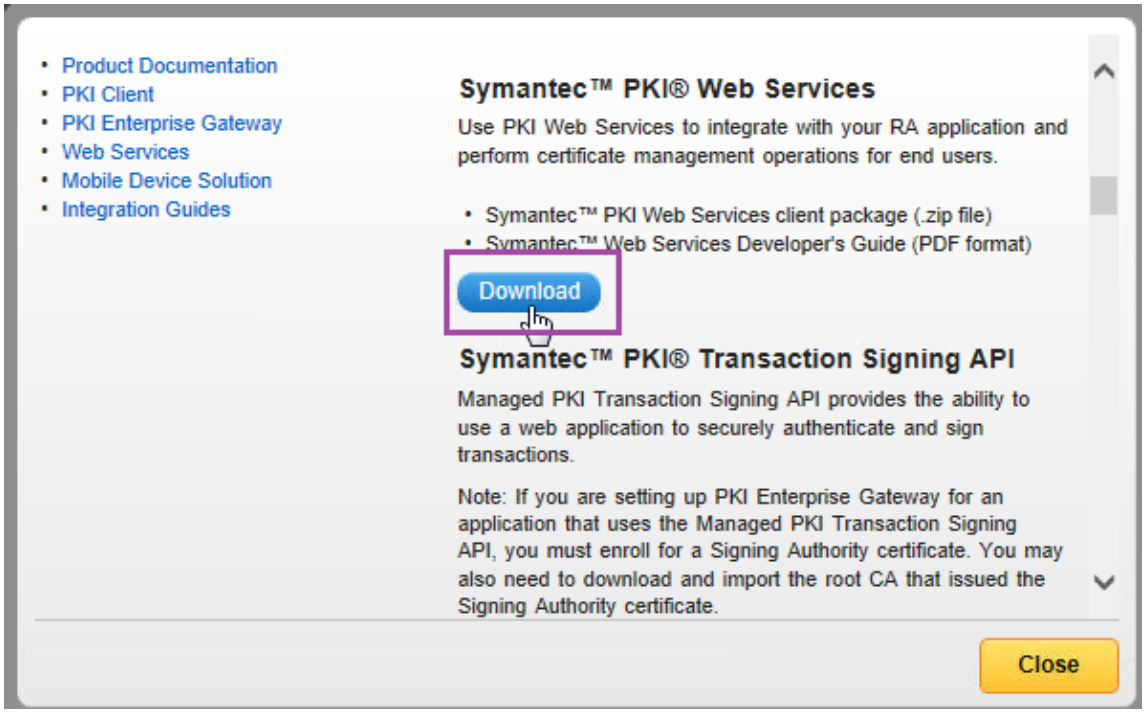
5.［**Download**］ をクリックして、生成された RA 証明書をダウンロードします。



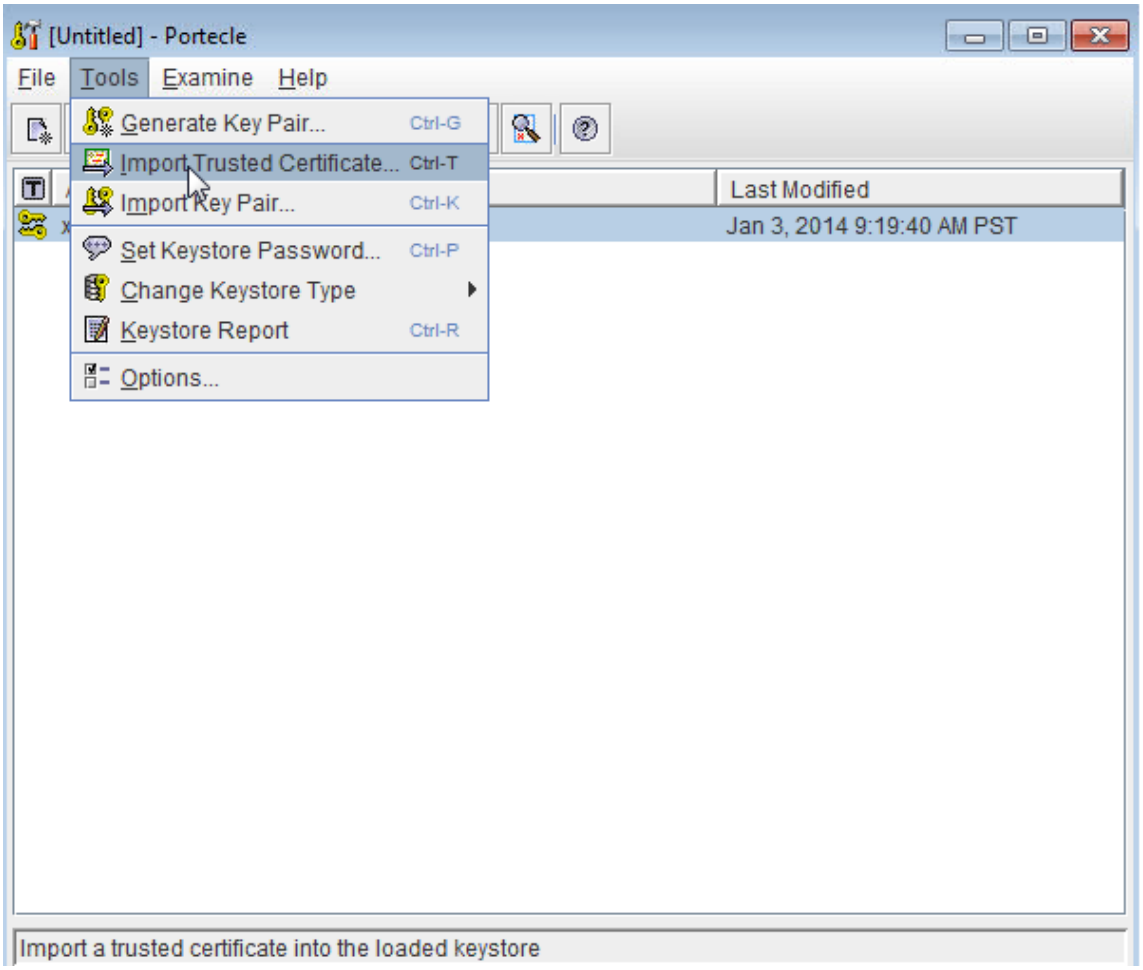
6. Portecle で RA 証明書をインポートする：キーペアを右クリックし、［**Import CA Reply**］ を選択します。



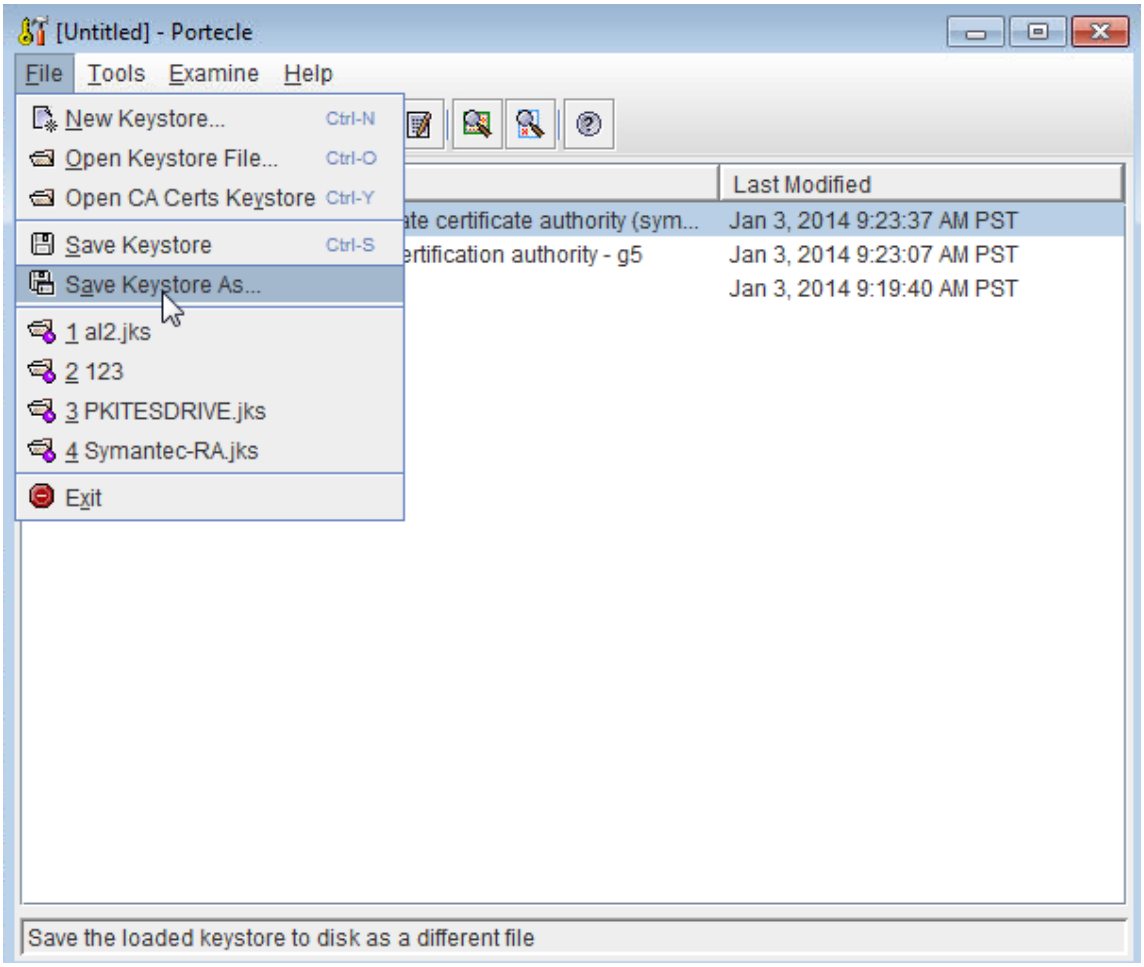
7. DigiCert PKI Manager の場合: ［**Resources**］、［**Web Services**］ の順に移動し、CA 証明書をダウンロードします。



8. Portecle で RA 中間証明書およびルート証明書をキーストアにインポートする: [**Tools**]、[**Import Trusted Certificates**] の順に移動します。



9. CA のインポート後、キーストアを RA.jks という名前で Windows サーバーの C:\DigiCert フォルダーに保存します。



Windows Server で **DigiCert PKI** アダプターを構成する

1. Windows Server に管理者としてログオンします。
2. 前のセクションで生成した RA.jks ファイルをアップロードします。また、Symantec MPKI サーバーのパブリック証明書（cacerts.jks）もアップロードします。
3. XenMobile Server 10 のダウンロードページで、［ツール］ を展開して Symantec PKI Adapter ファイルをダウンロードします。ファイル名は、XenMobile_Symantec_PKI_Adapter.zip です。ファイルを解凍し、これらのファイルを Windows Server の C ドライブにコピーします。
   - custom_gpki_adapter.properties
   - Symantec.war
4. custom_gpki_adapter.properties をメモ帳で開き、次の値を編集します。

```
Gpki.CaSvc.Url=https://<managed PKI URL>

# keystore for client-cert auth
```

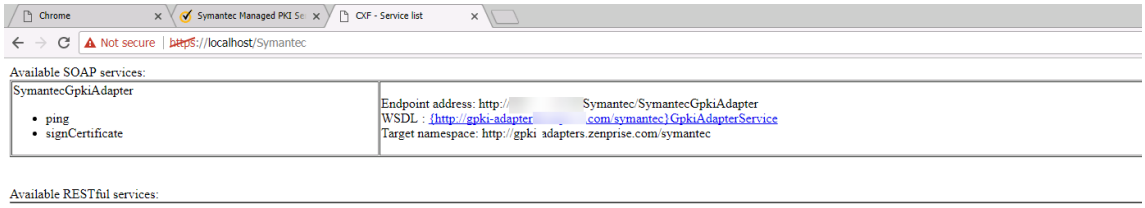


```
4
5 keyStore=C:\Symantec\RA.jks
6
7 # truststore for server with self-signed root CA
8
9 trustStore=C:\Symantec\cacerts.jks
```

5. Symantec.war を<tomcat dir>\webappsフォルダーにコピーし、Tomcat を起動します。
6. アプリケーションが展開されたことを確認する: Web ブラウザーを開き、https://localhost/Symantecに移動します。
7. <tomcat dir>\webapps\Symantec\WEB-INF\classesフォルダーに移動し、gpki_adapter.properties を編集します。次に示すように、**CustomProperties** プロパティが C:\Symantec フォルダーの custom_gpki_adapter ファイルを指すように変更します:

   ```
   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties
   ```

8. Tomcat を再起動し、https://localhost/Symantecに移動して、エンドポイントのアドレスをコピーします。次のセクションで、PKI アダプターを構成するときにこのアドレスを貼り付けます。

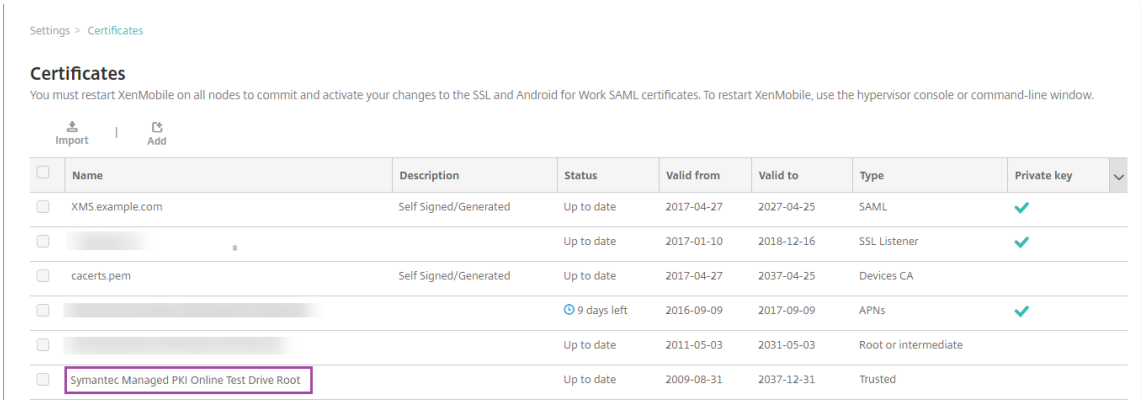


XenMobile Server を DigiCert マネージド PKI 用に構成する

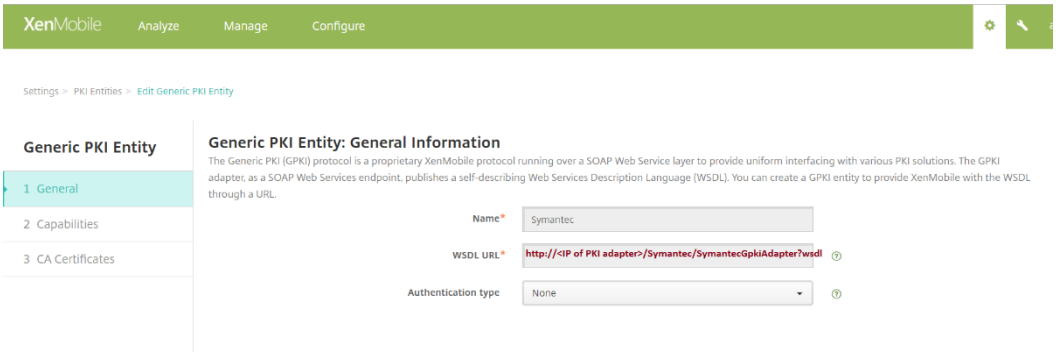
次の XenMobile Server の構成を実行する前に、Windows Server のセットアップを完了してください。

DigiCert CA 証明書をインポートして PKI エンティティを構成するには

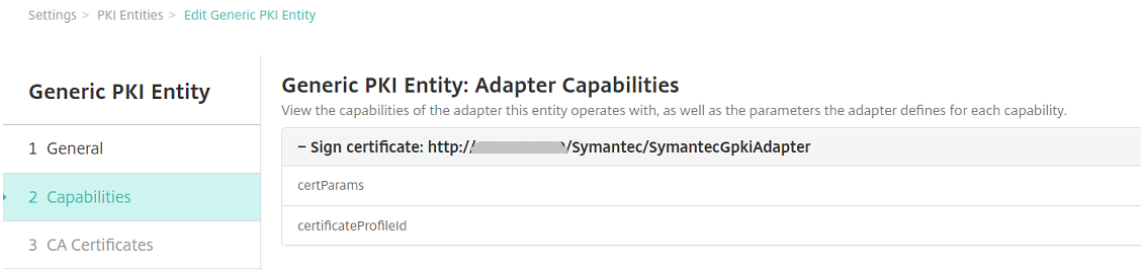
1. 次の手順を実行して、エンドユーザー証明書を発行する DigiCert CA 証明書をインポートします: XenMobile Server コンソールで、［設定］**>**［証明書］ の順に選択し、［インポート］ をクリックします。



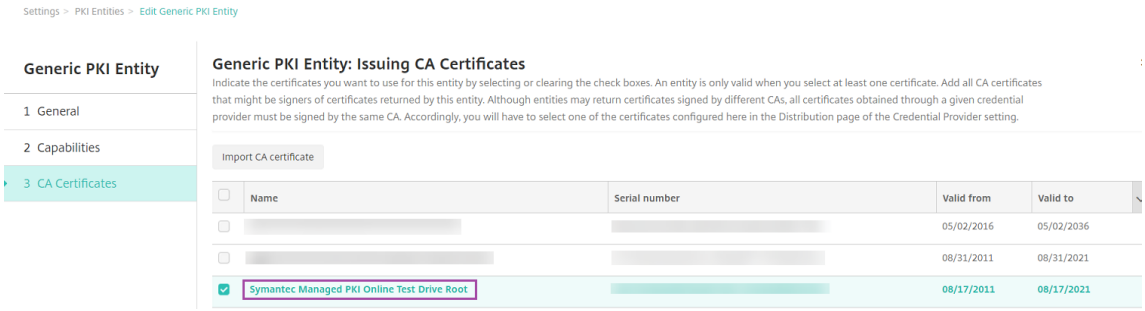
2. 次の手順を実行して、PKI エンティティを追加および構成します: ［設定］ **>** ［**PKI** エンティティ］ の順に選択し、［追加］ をクリックして、［汎用 **PKI** エンティティ］ を選択します。［**WSDL URL**］ に、前のセクションで PKI アダプターを構成するときにコピーしたエンドポイントアドレスを貼り付けてから、以下に示すように`?wsdl`を追加します。



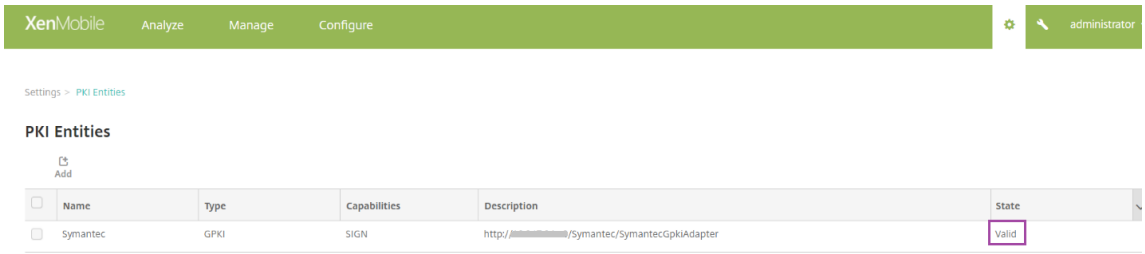
3. ［次へ］ をクリックします。XenMobile に、WSDL からパラメーター名が入力されます。



4. ［次へ］ をクリックし、適切な CA 証明書を選択して、［保存］ をクリックします。

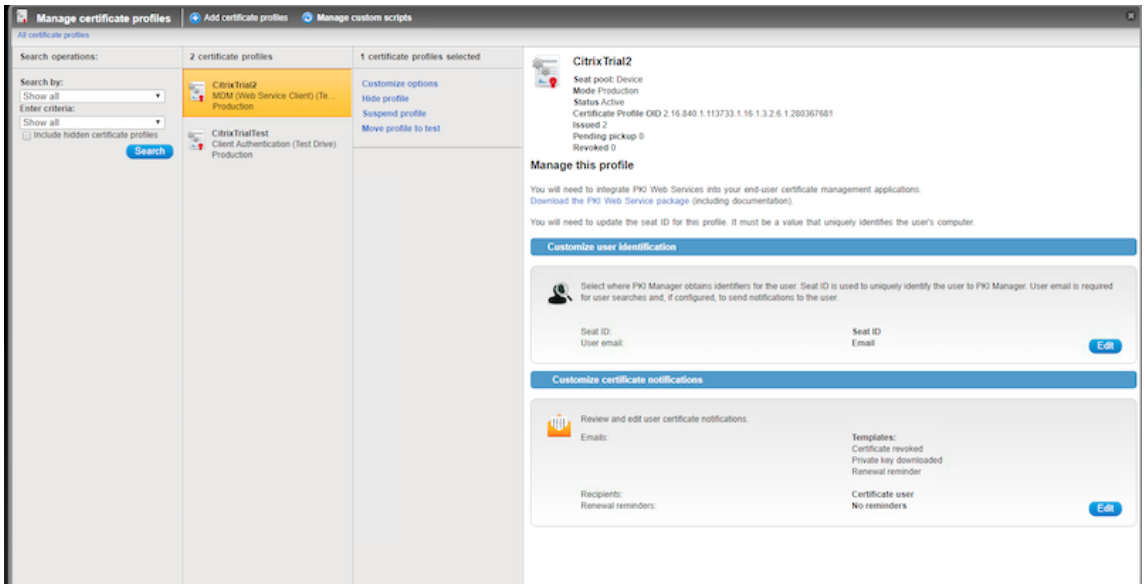


5. ［設定］**>**［**PKI** エンティティ］ページで、追加した PKI エンティティの ［状態］ が ［有効］ であることを確認します。



DigiCert マネージド **PKI** の資格情報プロバイダーを作成するには

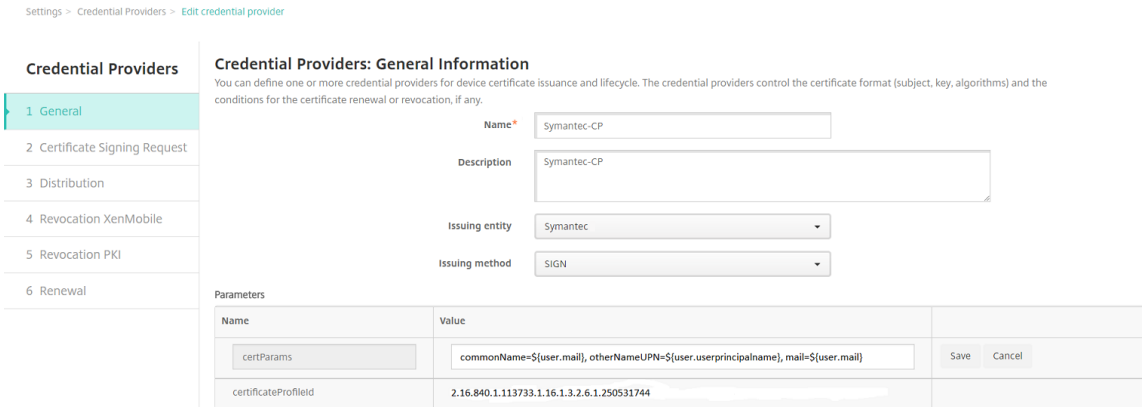
1. DigiCert PKI Manager コンソールで、証明書テンプレートから証明書プロファイルの **OID** をコピーします。



2. XenMobile Server コンソールで、［設定］**>**［資格情報プロバイダー］ の順に選択し、［追加］ をクリックして、次のように設定を構成します。

   - 名前：新しいプロバイダー構成の一意の名前を入力します。この名前は XenMobile コンソールのほかの部分で構成を参照するために使用されます。

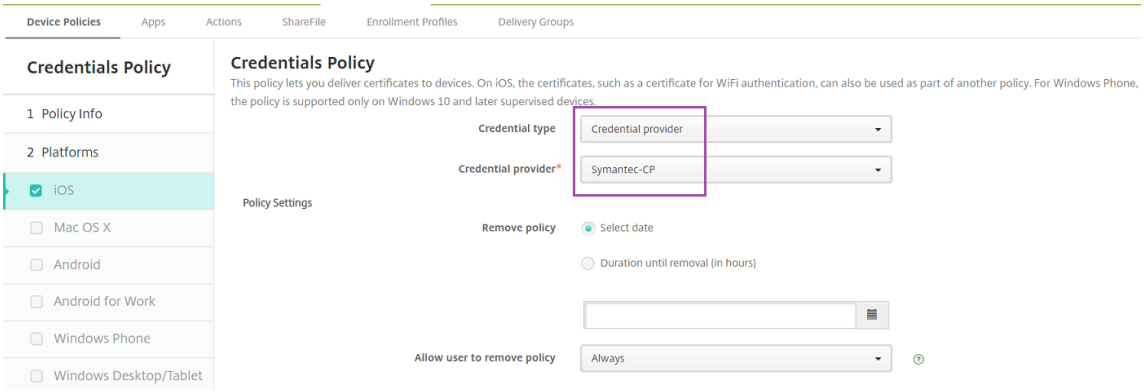
- 説明： 資格情報プロバイダーの説明です。このフィールドはオプションですが、この資格情報プロバイダーの詳細が必要なときに説明が役立ちます。
- 発行エンティティ： 証明書発行エンティティを選択します。
- 発行方式： 構成されたエンティティから証明書を取得するために使用する方法として ［署名］ を選択します。
- **certParams**: 以下の値を追加します:**commonName=${user.mail},otherNameUPN=${user.userprincipa**
- **certificateProfileid**： 手順 1 でコピーした証明書プロファイルの OID を貼り付けます。



3. ［次へ］ をクリックします。残りの各ページ（書き換えによる証明書の署名要求）では、デフォルトの設定を適用します。完了したら、［保存］をクリックします。

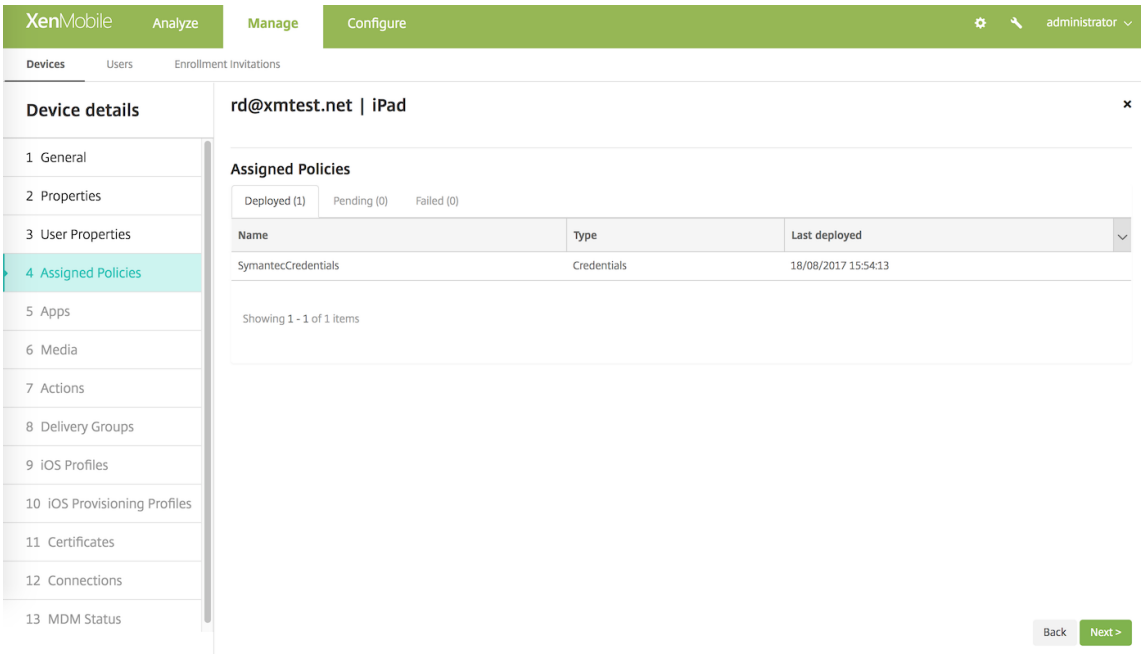
構成をテストおよびトラブルシューティングするには

1. 次の手順を実行し、資格情報デバイスポリシーを作成します： ［構成］ **>** ［デバイスポリシー］ の順に選択し、［追加］ をクリックして、「資格情報」 と入力してから ［資格情報］ をクリックします。
2. ポリシー名を指定します。
3. プラットフォームの設定を、次のように構成します。
   - 資格情報の種類： ［資格情報プロバイダー］ を選択します。
   - 資格情報プロバイダー： DigiCert プロバイダーを選択します。

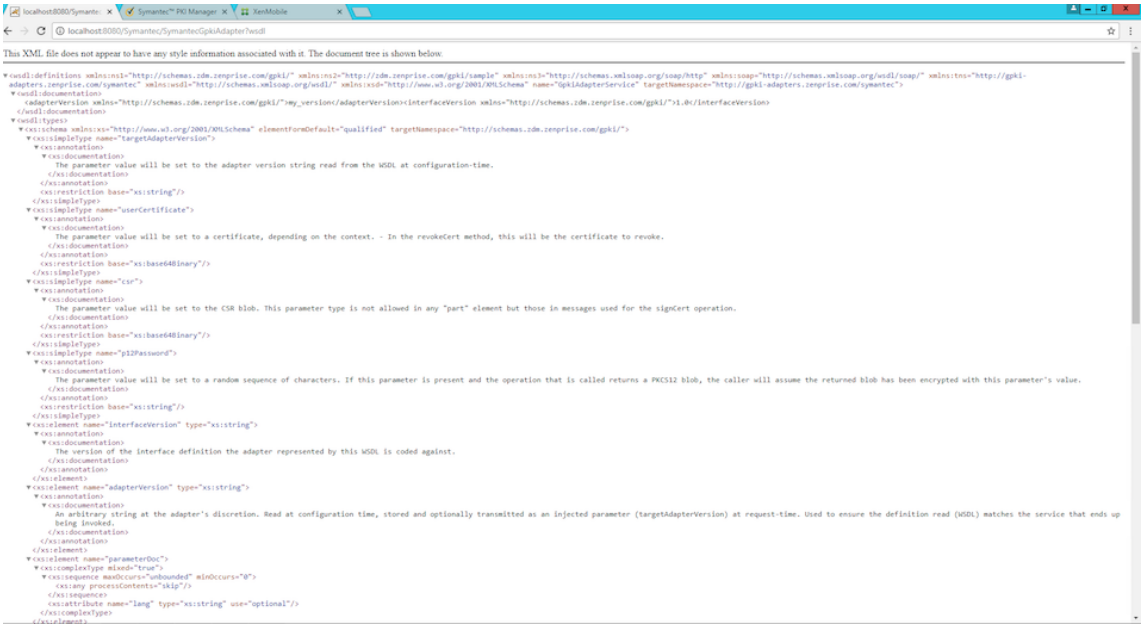


4. プラットフォームの設定が完了したら、引き続き ［割り当て］ ページに移動し、デリバリーグループにポリシーを割り当てて、［保存］ をクリックします。

5. ポリシーがデバイスに展開されたことを確認するには、［管理］ > ［デバイス］ の順に選択し、該当するデバイスを選択して、［編集］、［割り当て済みポリシー］ の順にクリックします。次の例は、ポリシーの展開が正常に行われたことを示しています。



ポリシーが展開されていない場合は、Windows Server にログオンして、WSDL が適切にロードされているかどうかを確認します。



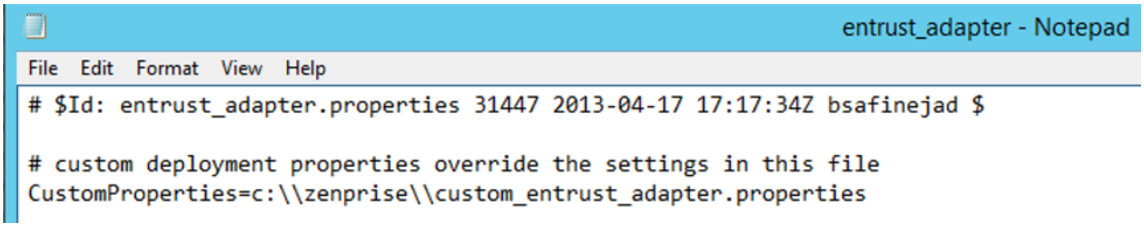
トラブルシューティングの詳細については、<tomcat dir>\logs\catalina.<current date>で Tomcat のログを確認してください。

Entrust PKI アダプター

DigiCert マネージド PKI の代わりに、Entrust PKI アダプターをインストールできます。アダプターをインストールする前に、この記事の「DigiCert マネージド PKI」セクションで Windows Server に Java と Apache Tomcat をインストールする手順を参照してください。

Entrust PKI アダプターのインストール

1. https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-10-server.htmlの「**Entrust** アダプター」セクションから、Entrust PKI アダプターをダウンロードします。
2. ダウンロードした.zip ファイルから entrust.war ファイルを抽出して、ProgramFiles (x86)\Apache Software Foundation\Tomcat 8.5\webapps ディレクトリに置きます。
3. C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes で、entrust_adapter.properties を編集し、CustomProperties をc:\\zenprise\\custom_entrust_adapter.propertiesに設定します。



4. C: ドライブで、zenprise ディレクトリを作成し、custom_entrust_adapter.properties という名前の新しいファイルを作成します。
5. 以下の内容でファイルを編集します。Entrust.MdmSvc.URL、AdminUserId、および AdminPassword は適切に置き換えてください。

   ~

   # set the following to the proper URL for AS/IG

   Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8

```
# set to 1 or true to force user creation from passed user and
    group parameters if using IG and user does not exist
CreateUser =

# set the credentials for the endpoint
AdminUserId=‘[User ID]‘
AdminPassword=‘[password]‘
```

   # クライアント証明書認証のキーストア

   #keyStore=

   #keyStorePassword=

   #keyStoreType: JKS、JCEKS、および PKCS12 – .p12 および.jks ファイルには不要

   # 自己署名のルート CA を持つサーバーのトラストストア

   #trustStore=

   #trustStorePassword=

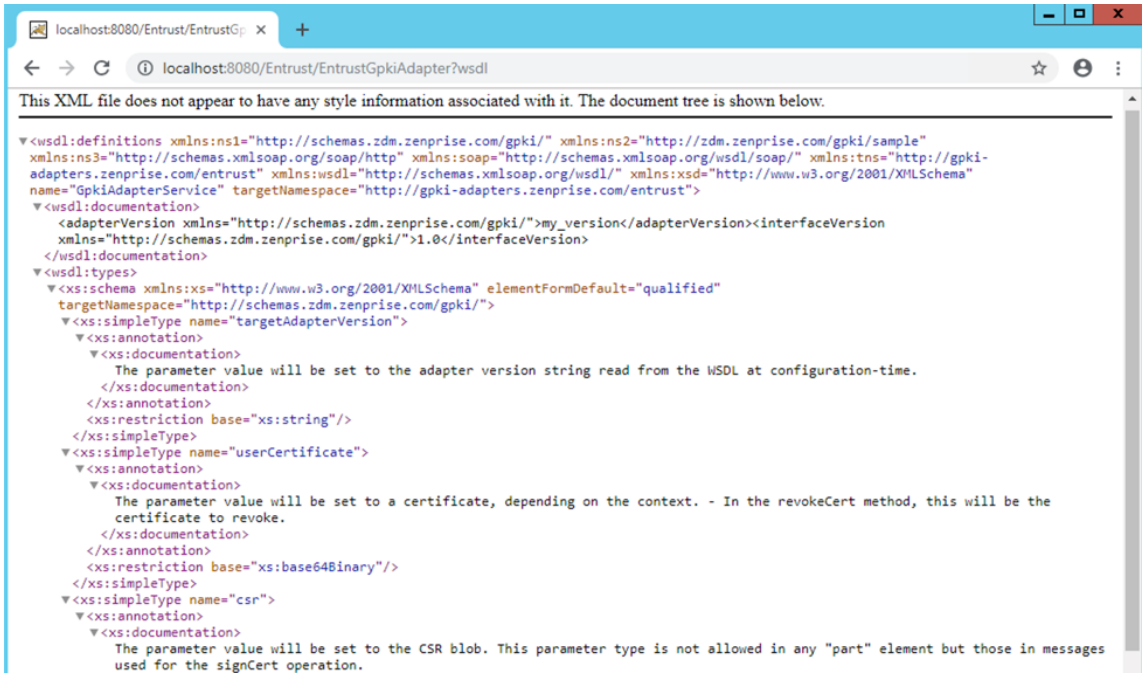
   #trustStoreType: JKS, JCEKS and PKCS12 – not needed for .p12 and .jks files

   ~

6. Tomcat サービスを再起動します。C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs に移動し、Catalina_201x-MM-DD.log を開きます。エラーがなく、次の行が表示されていることを確認します:

   13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf.endpoint.ServerImpl.initDestination Setting the server’s publish address to be /EntrustGpkiAdapter

7. http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdlまたはサーバーのパブリック URL に移動し、正しい XML が表示されていることを確認します。



XenMobile で **Entrust PKI** アダプターを構成する

1. XenMobile コンソールにログインし、［設定］**>**［**PKI** エンティティ］ に移動します。［追加］**>**［汎用 **PIK** エンティティ］ の順にクリックします。
2. 次の情報を入力します:
   - 名前: PKI エンティティの名前を入力します。
   - **WSDL URL**: サーバーのパブリック URL を入力します。
   - 認証の種類: 使用する認証方法を選択します。
     - なし
     - **HTTP** 基本: 接続に必要なユーザー名とパスワードを指定します。
     - クライアント証明書: 適切な SSL クライアント証明書を選択します。
   - リソースの場所: ［マイリソースの場所］ を選択します。
   - 許可する相対パス: `/Entrust/*`を入力します。
3. PKI エンティティの構成が終了したら、［設定］ ページに戻り、［資格情報プロバイダー］ を追加します。
4. ［全般］ タブで、［発行エンティティ］ として Entrust エンティティ、［発行方式］ として ［**SIGN**］ を選択します。
5. ［証明書署名要求］ タブで、次のように設定を構成します:
   - キーアルゴリズム: **RSA**
   - キーサイズ: 2048
   - 署名アルゴリズム: **SHA1withRSA**
   - サブジェクト名: cd=$user.username
   - サブジェクトの別名: オプションです。以下をお勧めします:
     - 種類: ユーザープリンシパル名

- 値： $user.userprincipalname

> 注：
> アダプターの設定を変更した場合は、この手順に従って資格情報プロバイダーを再構成します。

6. 資格情報プロバイダーの構成が完了したら、［構成］**>**［デバイスポリシー］ に移動し、資格情報ポリシーを追加します。
7. 使用予定の OS のポリシーを構成します。各 OS 構成ページで、［資格情報の種類］に対して ［資格情報プロバイダー**]** を選択します。［資格情報プロバイダー］ メニューで、事前に構成した資格情報プロバイダーを選択します。

Microsoft 証明書サービス

XenMobile は、Web 登録インターフェイスを通じて Microsoft Certificate Services と連携します。XenMobile はこのインターフェイス（GPKI 署名機能と同等の機能）を使用した新しい証明書の発行のみをサポートします。Microsoft CA が NetScaler Gateway ユーザー証明書を生成する場合、NetScaler Gateway はこれらの証明書の更新と失効をサポートします。

XenMobile で Microsoft CA PKI エンティティを作成するには、Certificate Services の Web インターフェイスのベース URL を指定する必要があります。選択した場合、SSL クライアント認証によって、XenMobile と Certificate Services の Web インターフェイスとの間の接続が保護されます。

Microsoft Certificate Services エンティティを追加する

1. XenMobile コンソールで、右上の歯車アイコンをクリックした後、［**PKI** エンティティ］ をクリックします。
2. ［**PKI** エンティティ］ ページで、［追加］ をクリックします。

   PKI エンティティタイプのメニューが表示されます。
3. ［**Microsoft** 証明書サービスエンティティ］ をクリックします。

   ［**Microsoft** 証明書サービスエンティティ**:** 一般的な情報］ ページが開きます。
4. ［**Microsoft** 証明書サービスエンティティ**:** 一般的な情報］ ページで次の設定を構成します。
   - 名前： 新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意の名前にする必要があります。
   - **Web** 登録サービスルート **URL**： Microsoft CA Web 登録サービスのベース URL（`https://192.0.2.13/certsrv/`など）を入力します。URL には、HTTP または HTTP-over-SSL を使用します。
   - **certnew.cer** ページ名： certnew.cer ページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
   - **certfnsh.asp**： certfnsh.asp ページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。

- 認証の種類： 使用する認証方法を選択します。
  - なし
  - **HTTP** 基本： 接続に必要なユーザー名とパスワードを指定します。
  - クライアント証明書： 適切な SSL クライアント証明書を選択します。

5. ［接続のテスト］ をクリックして、サーバーにアクセスできることを確認します。アクセスできない場合は、接続が失敗したことを示すメッセージが表示されます。構成設定を確認してください。
6. ［次へ］ をクリックします。

   ［**Microsoft** 証明書サービスエンティティ： テンプレート］ ページが開きます。このページで、Microsoft CA がサポートするテンプレートの内部名を指定します。資格情報プロバイダーを作成するとき、ここで定義したテンプレートを一覧で選択します。このエンティティを使用するすべての資格情報プロバイダーが、このようなテンプレートを 1 つだけ使用します。

   Microsoft Certificate Services テンプレートの要件については、お使いの Microsoft Server バージョンの Microsoft ドキュメントを参照してください。XenMobile には、「証明書」で説明している証明書の形式以外、配布する証明書の要件はありません。
7. ［**Microsoft** 証明書サービスエンティティ： テンプレート］ ページで ［追加］ をクリックし、テンプレートの名前を入力して、［保存］ をクリックします。追加する各テンプレートについて、この手順を繰り返します。
8. ［次へ］ をクリックします。

   ［**Microsoft** 証明書サービスエンティティ：**HTTP** パラメーター］ ページが開きます。このページで、Microsoft Web 登録インターフェイスに対する HTTP 要求に XenMobile が追加するカスタムパラメーターを指定します。カスタムパラメーターは、CA で実行されているカスタマイズされたスクリプトでのみ有効です。
9. ［**Microsoft** 証明書サービスエンティティ： **HTTP** パラメーター］ ページで ［追加］ をクリックし、追加する HTTP パラメーターの名前と値を入力して、［次へ］ をクリックします。

   ［**Microsoft** 証明書サービスエンティティ： **CA** 証明書］ ページが開きます。このページでは、このエンティティを通じてシステムが取得する証明書の署名者を XenMobile に通知する必要があります。CA 証明書が更新されたら、XenMobile で更新します。XenMobile は変更をエンティティに透過的に適用します。
10. ［**Microsoft** 証明書サービスエンティティ： **CA** 証明書］ ページで、このエンティティで使用する証明書を選択します。
11. ［保存］ をクリックします。

    ［PKI エンティティ］ の表にエンティティが表示されます。

NetScaler 証明書失効一覧（**CRL**）

XenMobile は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートします。Microsoft CA が構成されている場合、XenMobile は NetScaler を使用して失効を管理します。

クライアント証明書ベースの認証を構成する場合、NetScaler 証明書失効一覧（CRL）設定 ［**CRL** 自動更新を有効化］ を構成するかどうか検討します。この手順を使用すると、MAM-only モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できなくなります。

ユーザー証明書が失効してもユーザーによる生成が制限されるわけではないため、XenMobile は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

任意 **CA**

任意 CA は、CA 証明書と関連の秘密キーを XenMobile に提供したときに作成されます。XenMobile は、管理者が指定したパラメーターに従って、証明書の発行、失効、および状態情報を内部で処理します。

随意 CA を構成するときに、その CA に対して OCSP（Online Certificate Status Protocol）サポートをアクティブにできます。OCSP サポートを有効にした場合に限り、CA は発行する証明書に`id-pe-authorityInfoAccess`拡張を追加します。この拡張は、次の場所にある XenMobile の内部 OCSP レスポンダーを参照します:

```
https://<server>/<instance>/ocsp
```

OCSP サービスを構成するときに、該当の任意エンティティの OCSP 署名証明書を指定する必要があります。CA 証明書そのものを署名者として使用できます。CA 秘密キーの不必要な漏えいを防ぐには（推奨）: CA 証明書で署名された、委任 OCSP 署名証明書を作成し、`id-kp-OCSPSigning extendedKeyUsage`拡張を含めます。

XenMobile OCSP レスポンダーサービスは、基本の OCSP 応答と要求の以下のハッシュアルゴリズムをサポートします。

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

応答は SHA-256 および署名証明書キーアルゴリズム（DSA、RSA または ECDSA）で署名されます。

任意 **CA** を追加する

1. XenMobile コンソールで、右上の歯車アイコンをクリックした後、［詳細］の［**PKI** エンティティ］ をクリックします。
2. ［**PKI** エンティティ］ ページで、［追加］ をクリックします。

   PKI エンティティタイプのメニューが表示されます。
3. ［随意 **CA**］ をクリックします。

   ［随意 **CA**: 一般情報］ ページが開きます。

4. [随意 **CA**: 一般情報] ページで以下を行います。
   - 名前: 随意 CA の説明的な名前を入力します。
   - 証明書要求に署名するための **CA** 証明書: 一覧から、証明書要求に署名するために使用する随意 CA の証明書を選択します。

     この証明書の一覧は、[構成] **>** [設定] **>** [証明書] から XenMobile にアップロードした、秘密キー付きの CA 証明書から生成されます。
5. [次へ] をクリックします。

   [随意 **CA**: パラメーター] ページが開きます。
6. [随意 **CA**: パラメーター] ページで、以下を行います:
   - シリアル番号ジェネレーター: 随意 CA は発行する証明書のシリアル番号を生成します。一覧で [シーケンシャル] または [非シーケンシャル] を選択して、番号の生成方法を指定します。
   - 次のシリアル番号: 値を入力して、次に発行される番号を指定します。
   - 証明書の有効期限: 証明書の有効期間(日数)を入力します。
   - キー使用法: 適切なキーを [オン] に設定して、随意 CA が発行する証明書の目的を指定します。設定すると、CA による証明書の発行がそれらの目的に限定されます。
   - 拡張キー使用法: さらにパラメーターを追加するには、[追加] をクリックし、キー名を入力して [保存] をクリックします。
7. [次へ] をクリックします。

   [随意 **CA**: ディストリビューション] ページが開きます。
8. [随意 **CA**: ディストリビューション] ページで、配布モードを選択します:
   - 集中: サーバー側のキー生成。この集中管理オプションをお勧めします。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
   - 分散: デバイス側のキー生成。ユーザーデバイス上で秘密キーが生成されます。この分散モードは SCEP を使用し、**keyUsage keyEncryption**拡張による RA 暗号化証明書と**keyUsage digitalSignature**拡張による RA 署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。
9. [次へ] をクリックします。

   [随意 **CA**: **Online Certificate Status Protocol**(**OCSP**)] ページが開きます。

   [随意 **CA**: **Online Certificate Status Protocol (OCSP)**] ページで、以下を行います:
   - この CA が署名する証明書に`AuthorityInfoAccess`(RFC2459)拡張を追加する場合は、[この **CA** の **OCSP** サポートを有効にする] を [オン] に設定します。この拡張は、CA の OCSP レスポンダー(`https://<server>/<instance>/ocsp`)を参照します。
   - OCSP サポートを有効にした場合は、OSCP 署名 CA 証明書を選択します。この証明書一覧は、XenMobile にアップロードした CA 証明書から生成されます。

10.［保存］ をクリックします。

［PKI エンティティ］の表に任意 CA が表示されます。

資格情報プロバイダー

January 10, 2020

資格情報プロバイダーは、XenMobile システムのさまざまな部分で使用する実際の証明書の構成です。資格情報プロバイダーは、証明書のソース、パラメーター、およびライフサイクルを定義します。これらの操作は、証明書がデバイス構成の一部であるかスタンドアロン（つまり、デバイスにそのままプッシュされる）であるかに関わらず発生します。

デバイス登録によって証明書のライフサイクルは制約されます。つまり、登録前に証明書は発行されませんが、登録の一部として一部の証明書が発行される場合があります。また、1 回の登録のコンテキスト内で内部 PKI から発行された証明書は、登録が失効すると失効します。管理関係が終了すると、証明書の有効性は維持されません。

1 つの資格情報プロバイダーの構成を複数の場所で使用し、1 つの構成によって任意の数の証明書を同時に管理することができます。この場合、この全体は展開リソースおよび展開上にあります。たとえば、資格情報プロバイダー P が構成 C の一部としてデバイス D に展開された場合、D に展開される証明書は P の発行設定によって決まります。同様に、C が更新された場合は D の更新設定が適用されます。また、C が削除された、または D が失効した場合には、D の失効設定も適用されます。

この規則に従って、XenMobile の資格情報プロバイダー構成により以下が決まります。

- 証明書のソース。
- 証明書の取得方法：新しい証明書に署名するか、既存の証明書とキーペアをフェッチ（回復）します。
- 発行または回復のパラメーター。キーサイズ、キーアルゴリズム、証明書拡張などの証明書署名要求（Certificate Signing Request：CSR）パラメーターがあります。
- 証明書をデバイスに配信する方法。
- 失効条件。管理関係が失われると XenMobile のすべての証明書が失効しますが、構成によっては、早期の失効を指定する場合もあります。たとえば、関連するデバイス構成が削除されたときに証明書が失効するように指定できます。また、条件によっては、XenMobile で関連付けられた証明書の失効がバックエンドの PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）に送信されることがあります。つまり、XenMobile の証明書失効により、PKI で証明書失効が発生する場合があります。
- リニューアル設定。特定の資格プロバイダーを通して取得された証明書は、有効期限が近づくと自動的に更新されます。または、そのような状況とは別に、有効期限が近づくと通知を出すこともできます。

構成オプションの可用性は主に、資格情報プロバイダーに対して選択した PKI エンティティの種類と発行方法によって異なります。

証明書の発行方法

証明書は 2 つの方法で取得でき、これを発行方法と呼びます。

- 署名：この方法では、新しい秘密キーを作成し、CSR を作成して CA（Certificate Authority：証明機関）に送信し、署名してもらいます。XenMobile では 3 つの PKI エンティティ（MS 証明書サービスエンティティ、汎用 PKI、随意 CA）の署名方法がサポートされています。
- フェッチ： この方法では、発行は XenMobile のためのもので、既存のキーペアの回復を意味します。XenMobile は汎用 PKI でのみフェッチの方法をサポートします。

資格情報プロバイダーは署名またはフェッチの発行方法を使用します。選択した方法は使用可能な構成オプションに影響します。特に、CSR 構成と分散配信は、発行方法が署名の場合にのみ使用できます。フェッチされた証明書は常に PKCS #12 としてデバイスに送信されます（署名方法の集中配信モードと同じ）。

証明書の配信

XenMobile での証明書の配信には、集中と分散の 2 つのモードがあります。分散モードは SCEP（Simple Certificate Enrollment Protocol）を使い、クライアントがこのプロトコルをサポートする状況でのみ使用できます（iOS のみ）。場合によっては分散モードが必須となります。

資格情報プロバイダーで分散（SCEP を使用した）配信をサポートするには、特別な構成手順として、RA（Registration Authority：登録機関）証明書の設定が必要です。RA 証明書が必要なのは、SCEP プロトコルを使用する場合、XenMobile が実際の証明機関に対する代理（登録機関）と同様に機能するためです。XenMobile は、そのように行動する権限を持っていることをクライアントに証明する必要があります。その権限は、XenMobile に前述の証明書をアップロードすることにより確立されます。

RA 署名と RA 暗号化の 2 つの異なる証明書の役割が必要です（1 つの証明書で両方の要件を満たすことができます）。これらの役割には以下の制約があります。

- RA 署名証明書には、X.509 キー使用法デジタル署名が必要です。
- RA 暗号化証明書には、X.509 キー使用法キーの暗号化が必要です。

資格情報プロバイダーの RA 証明書を構成するには、それらの証明書を XenMobile にアップロードし、資格情報プロバイダーでそれらの証明書にリンクします。

資格情報プロバイダーに証明書の役割について構成されている証明書がある場合、分散配信のみをサポートするとみなされます。各資格情報プロバイダーは、集中モードを優先するか、分散モードを優先するか、または分散モードを必須とするように構成できます。実際の結果はコンテキストに応じて異なります。コンテキストが分散モードをサポートしないにもかかわらず、資格情報プロバイダーに分散モードが必要な場合、展開は失敗します。同様に、コンテキストに分散モードが必要な場合でも、資格情報プロバイダーが分散モードをサポートしていなければ、展開は失敗します。ほかのすべての場合、優先設定が適用されます。

次の表は、XenMobile 全体における SCEP 分散を示しています。

コンテキスト	SCEP のサポート	SCEP の必要
iOS プロファイルサービス	はい	はい
iOS モバイルデバイス管理登録	はい	いいえ
iOS 構成プロファイル	はい	いいえ
SHTP 登録	いいえ	いいえ
SHTP の構成	いいえ	いいえ
Windows Phone および Windows タブレットの登録	いいえ	いいえ
Windows Phone および Windows タブレットの構成	いいえ。ただし、Windows Phone 8.1 および最新の Windows 10 リリースでサポートされる Wi-Fi デバイスポリシーを除く。	いいえ

証明書の失効

失効には以下の 3 つの種類があります。

- 内部失効： XenMobile で維持されている証明書の状態に影響します。XenMobile は、提示された証明書を評価するとき、または証明書の OCSP ステータス情報を提供するときに、このステータスを考慮します。資格情報プロバイダー構成により、さまざまな条件下でこの状態がどのように影響を受けるかが決まります。たとえば、資格情報プロバイダーは、証明書がデバイスから削除されたときに失効済みのフラグを立てるよう指定する場合があります。
- 外部に伝達される失効： 失効 XenMobile とも呼ばれるこの種類の失効は、外部の PKI から取得した証明書に適用されます。資格情報プロバイダー構成で定義された条件下で、XenMobile で証明書が内部失効すると、その証明書は PKI でも失効します。失効を実行するための呼び出しを行うには、失効対応 GPKI（General PKI：汎用 PKI）エンティティが必要です。
- 外部で誘導される失効： 失効 PKI とも呼ばれるこの種類の失効も、外部の PKI から取得した証明書のみに適用されます。XenMobile で特定の証明書の状態が評価されるたびに、その状態について PKI に照会されます。PKI で証明書が失効している場合、XenMobile で証明書が内部失効します。このメカニズムでは OCSP プロトコルが使用されます。

これらの 3 つのタイプは排他的ではなく、むしろ同時に適用されます。外部失効または個別の調査により、内部失効が発生する場合もあります。内部失効は、外部失効に影響する可能性があります。

証明書の書き換え

証明書の書き換えとは、既存の証明書の失効と別の証明書の発行を両方行うことです。

XenMobile では、発行が失敗した場合にサービスが中断されないように、以前の証明書が失効する前にまず新しい証明書の取得を試行します。分散型（SCEP 対応）配信の場合、証明書がデバイスに正常にインストールされた後にのみ失効が行われます。それ以外の場合は、新しい証明書がデバイスに送信される前に失効が発生します。そのような失効は、証明書のインストールの成功や失敗とは無関係です。

失効の構成では、特定の期間を日単位で指定する必要があります。デバイスが接続されると、証明書の`NotAfter`の日付からこの指定した期間を引いて、現在の日付より後になっているかどうかがサーバーによって検証されます。証明書がこの条件を満たしている場合、XenMobile は証明書の更新を試行します。

資格情報プロバイダーの作成

資格情報プロバイダーの構成は、主に、資格情報プロバイダーに対して選択した発行エンティティや発行方法により異なります。内部エンティティを使用する資格情報プロバイダーと外部エンティティを使用する資格情報プロバイダーを区別できます。

- XenMobile に対して内部である随意エンティティは、内部エンティティです。随意エンティティの発行方法は常に署名です。署名とは、各発行操作で、XenMobile がエンティティに対して選択された CA 証明書で新しいキーペアに署名する方法です。キーペアがデバイスまたはサーバーのどちらで生成されるかは、選択した分散方法によって異なります。
- 企業インフラストラクチャの一部である外部エンティティには、Microsoft CA や汎用 PKI が含まれます。

資格情報プロバイダーの作成などの DigiCert マネージド PKI の設定について詳しくは、「PKI エンティティ」の「DigiCert マネージド PKI」を参照してください。

1. XenMobile コンソールで、右上の歯車アイコンをクリックした後、［設定］の［資格情報プロバイダー］ をクリックします。
2. ［資格情報プロバイダー］ ページで、［追加］ をクリックします。

   ［資格情報プロバイダー：一般情報］ ページが開きます。
3. ［資格情報プロバイダー：一般情報］ ページで、以下を指定します：
   - 名前：新しいプロバイダー構成の一意の名前を入力します。この名前は XenMobile コンソールのほかの部分で構成を特定するために後で使用されます。
   - 説明： 資格情報プロバイダーの説明です。このフィールドはオプションですが、この資格情報プロバイダーの詳細が必要なときに説明が役立ちます。
   - 発行エンティティ： 証明書発行エンティティを選択します。
   - 発行方式： ［署名］ または ［取得］ をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。クライアント証明書認証の場合は、［署名］ を使用します。

- テンプレート一覧が使用できる場合は、資格情報プロバイダーの PKI エンティティで追加したテンプレートを選択します。

  これらのテンプレートは、[設定]、[**PKI** エンティティ] の順にクリックすると開くページで、Microsoft 証明書サービスエンティティが追加されている場合に使用可能になります。

4. [次へ] をクリックします。

   [資格情報プロバイダー: 証明書署名要求] ページが表示されます。

5. [資格情報プロバイダー: 証明書署名要求] ページで、証明書の構成に応じて以下を構成します:

   - キーアルゴリズム: 新しいキーペアのキーアルゴリズムを選択します。使用可能な値は [**RSA**]、[**DSA**]、および [**ECDSA**] です。
   - キーサイズ: キーペアのサイズ (ビット単位) を入力します。このフィールドは必須です。

     許容値はキータイプによって異なります。たとえば、DSA キーの最大サイズは 1024 ビットです。基になるハードウェアおよびソフトウェアに依存する偽陰性を回避するため、XenMobile ではキーサイズが強制されません。資格情報プロバイダーの構成を実稼働環境でアクティブにする前に、必ずテスト環境でテストしてください。
   - 署名アルゴリズム: 新しい証明書の値を選択します。値はキーアルゴリズムによって異なります。
   - サブジェクト名: 必須です。新しい証明書のサブジェクトの識別名 (Distinguished Name: DN) を入力します。次に例を示します:
     `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } ,C=${ user.c } \endquotation`

     たとえば、クライアント証明書認証には次の設定を使用します。

     - キーアルゴリズム: RSA
     - キーサイズ: 2048
     - 署名アルゴリズム: SHA1withRSA
     - サブジェクト名: `cn=$user.username`
   - [サブジェクトの別名] の表に新しいエントリを追加するには、[追加] をクリックします。別名の種類を選択して、2 つ目の列に値を入力します。

     クライアント証明書認証では、次のように指定します:

     - 種類: ユーザープリンシパル名
     - 値のデータ: `$user.userprincipalname`

       サブジェクト名と同様に、値フィールドで XenMobile マクロを使用できます。

6. [次へ] をクリックします。

   [資格情報プロバイダー: ディストリビューション] ページが開きます。

7. [資格情報プロバイダー: ディストリビューション] ページで、以下を行います:

- ［発行 **CA** 証明書］ の一覧から、提供された CA 証明書を選択します。資格情報プロバイダーは随意 CA エンティティを使用するため、資格情報プロバイダーの CA 証明書は常にエンティティそのものに構成されている CA 証明書になります。ここでは、外部エンティティを使用する構成との整合性のために CA 証明書を示します。
- ［ディストリビューションモードの選択］ で、キーを生成し、配布する方法として以下のいずれかの方法をクリックします:
  - 集中を優先: サーバー側のキー生成: シトリックスではこの集中オプションを推奨しています。このオプションは XenMobile でサポートされるすべてのプラットフォームをサポートし、NetScaler Gateway 認証を使用する場合は必須です。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
  - 分散を優先: デバイス側のキー生成: 秘密キーはユーザーデバイス上で生成され、保存されます。この分散モードは SCEP を使用し、keyUsage keyEncryption による RA 暗号化証明書と KeyUsage digitalSignature による RA 署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。
  - 分散のみ: デバイス側のキー生成: このオプションは［分散を優先: デバイス側のキー生成］と同じように動作しますが、「優先」ではなく「のみ」であるため、デバイス側でのキー生成が失敗した場合、または使用できない場合にはオプションを使用できない点が異なります。

［優先分散**:** デバイス側のキー生成］ または ［分散のみ**:** デバイス側のキー生成］ を選択した場合は、［RA 署名証明］の一覧から RA 署名証明書を選択し、［RA 暗号化証明書］の一覧から RA 暗号化証明書を選択します。両方に同じ証明書を使用できます。これらの証明書のための新しいフィールドが表示されます。

8. ［次へ］ をクリックします。

［資格情報プロバイダー: 失効 **XenMobile**］ ページが開きます。このページで、XenMobile がこのプロバイダー構成により発行された証明書に内部で失効のフラグを設定する条件を構成します。

9. ［資格情報プロバイダー: 失効 **XenMobile**］ ページで、以下を行います。

   - ［発行された証明書の失効］ で、証明書がいつ失効するかを示すいずれかのオプションを選択します。
   - 証明書が失効したときに XenMobile から通知を送信する場合は、［通知の送信］ の値を ［オン］ に設定して、通知テンプレートを選択します。
   - XenMobile で証明書が失効したときに、PKI でも証明書を失効させる場合: ［**PKI** 上の証明書の失効］を ［オン］ に設定し、［エンティティ一覧］ からテンプレートを選択します。エンティティ一覧には、失効機能で使用できるすべての GPKI エンティティが表示されます。XenMobile で証明書が失効すると、エンティティ一覧から選択した PKI に、失効呼び出しが送信されます。

10. ［次へ］ をクリックします。

［資格情報プロバイダー: 失効 **PKI**］ ページが開きます。このページで、証明書が失効したときに PKI で行うアクションを特定します。また、通知メッセージを作成するオプションもあります。

11. PKI で証明書を失効させる場合、［資格情報プロバイダー: 失効 **PKI**］ ページで以下を行います。

- ［外部失効チェックの有効化］ の設定を ［オン］ に変更します。失効 PKI に関連する詳細フィールドが表示されます。
- ［**OCSP** レスポンダー **CA** 証明書］の一覧から、証明書のサブジェクトの識別名（Distinguished Name: DN）を選択します。

  DN フィールドの値には、XenMobile マクロを使用できます。次に例を示します：`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`
- ［証明書が失効した場合］ の一覧から、証明書が失効したときに PKI エンティティで行う次のいずれかのアクションを選択します。
  - 何もしない。
  - 証明書の書き換え。
  - デバイスの失効とワイプ。
- 証明書が失効したときに XenMobile から通知を送信する場合：［通知の送信］ の値を ［オン］ に設定します。

  2 つの通知オプションから選択できます。
- ［通知テンプレートを選択］ を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［通知テンプレート］の一覧にあります。
- ［通知の詳細を入力］ を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

12. ［次へ］ をクリックします。

    ［資格情報プロバイダー：更新］ ページが開きます。このページで、XenMobile を構成して次のことを実行できます。

    - 証明書の書き換え。必要に応じて、更新時に通知を送信したり、期限切れの証明書を操作から除外することもできます。
    - 期限が近い証明書に関する通知の発行（更新前の通知）。

13. 証明書が失効したら更新する場合は、［資格情報プロバイダー：更新］ ページで以下を行います：

    ［有効期限が切れたら証明書を更新］ で ［オン］ を選択します。詳細フィールドが表示されます。

    - ［更新が必要な有効期限までの日数］ フィールドに、期限の何日前に証明書を更新するかを入力します。
    - 必要に応じて、［既に有効期限が切れている証明書は更新しない］ チェックボックスをオンにします。この場合の「既に有効期限が切れている」とは、`NotAfter`が過去の日付であることを意味し、証明書が失効しているという意味ではありません。XenMobile では、内部失効した証明書は更新しません。

    証明書が更新されたときに XenMobile から通知を送信する場合：［通知の送信］ を ［オン］ に設定します。
    証明書の期限が近いときに XenMobile から通知を送信する場合：［証明書の有効期限が近づいたら通知］ を ［オン］ に設定します。
    どちらの選択肢についても、以下の 2 つの通知オプションからいずれかを選択できます：

- 通知テンプレートを選択： カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［通知テンプレート］の一覧にあります。
- 通知の詳細を入力： 独自の通知メッセージを作成できます。受信者の電子メールアドレス、メッセージ、および通知の送信頻度を指定します。

［通知が必要な証明書の有効期限までの日数］ フィールドで、証明書の期限の何日前に通知を送信するかを入力します。

14. ［保存］ をクリックします。

［資格情報プロバイダー］の表に資格情報プロバイダーが追加されます。

APN 証明書

October 25, 2019

XenMobile で iOS デバイスを登録して管理するには、Apple の Apple プッシュ通知サービス（APNs）証明書を設定します。

> 注：
>
> - Apple の APN 証明書を使用すると、Apple Push Network を使用してモバイルデバイスを管理できます。証明書を失効させると、過失であっても故意であっても、デバイスを管理できなくなります。
> - Secure Mail for iOS でプッシュ通知を使用する場合も、XenMobile で APNs 証明書が必要です。
> - iOS Developer Enterprise Program を使用して Mobile Device Manager プッシュ証明書を作成した場合：既存の証明書を Apple Push Certificates Portal に移行するためのアクションが必要になることがあります。

手順の概要を説明するトピックを示します。この順番で実行してください。プロセスの概要を以下に示します。

手順 **1**： Windows の場合は、Windows Server 2012 R2 または Windows 2008 R2 Server と Microsoft IIS を使用して CSR を生成します。Mac の場合は、Mac コンピューターで CSR を生成します。この方法を使用することをお勧めします。

手順 **2**： シトリックスに CSR を送信します。モバイルデバイス管理の署名証明書を使用して署名された.plist 形式のファイルが返送されます。

手順 **3**： 署名済みの CSR を Apple に送信し、Apple の APNs 証明書をダウンロードします。

手順 **4**： （IIS、Mac、または SSL で）APNs 証明書を PCKS #12（.pfx）証明書としてエクスポートします。

手順 **5**： APNs 証明書を XenMobile にインポートします。

> 重要：

> 証明書の作成に使用された Apple ID の記録をとる必要があります。また、Apple ID は個人 ID ではなく会社 ID でなければなりません。

Microsoft IIS を使用して CSR を作成するには

iOS デバイスの APNs 証明書要求を生成するには、まず CSR（Certificate Signing Request：証明書署名要求）を作成します。Windows 2012 R2 または Windows 2008 R2 Server では、Microsoft IIS を使用して CSR を生成できます。

1. Microsoft IIS を開きます。
2. IIS のサーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ウィンドウで、［証明書の要求の作成］ をクリックします。
4. 適切な識別名（Distinguished Name：DN）を入力して ［次へ］ をクリックします。
5. ［暗号化サービスプロバイダー］で ［**Microsoft RSA SChannel Cryptographic Provider**］ を選択して、ビット長として ［**2048**］ を選択し、［次へ］ をクリックします。
6. ファイル名を入力して CSR を保存する場所を指定し、［完了］ をクリックします。

Mac コンピューターで CSR を作成するには

1. macOS を実行する Mac コンピューターの ［アプリケーション］**>**［ユーティリティ］ で、キーチェーンアクセスアプリケーションを起動します。
2. ［キーチェーンアクセス］ メニューを開いて ［環境設定］ を選択します。
3. ［証明書］ タブをクリックして、［**OCSP**］ および ［**CRL**］ のオプションを ［切］ に変更し、［環境設定］ウィンドウを閉じます。
4. ［キーチェーンアクセス］ メニューで、［証明書アシスタント］**>**［認証局に証明書を要求］ の順に選択します。
5. 証明書アシスタントにより、次の情報の入力を求められます：
   - メールアドレス： 証明書の管理を担当する個人または役割アカウントのメールアドレス。
   - 共通名： ホスト名およびドメイン名として共通名を構成します。これは、通常、「www.website.com」または「website.com」のように見えます。共通名は、サイトに接続するときにアクセスする Web アドレスと同じである必要があります。
   - **CA** のメールアドレス： 認証局のメールアドレス。
6. ［ディスクに保存］ をクリックし、［鍵ペア情報を指定］ チェックボックスをオンにして、［続ける］ をクリックします。
7. CSR ファイルの名前を入力してコンピューターにファイルを保存し、［保存］ を選択します。
8. 鍵ペア情報を指定：［鍵のサイズ］ で［2048 ビット］を選択し、アルゴリズムに ［**RSA**］ を選択してから［続ける］ をクリックします。APN 証明書プロセスの一環として CSR ファイルをアップロードする準備ができました。
9. 証明書アシスタンスによる CSR プロセスが完了してから ［完了］ をクリックします。

OpenSSL を使用して CSR を作成するには

Mac コンピューターまたはサポートされている Windows Server と Microsoft IIS を使用して CSR を生成できない場合: 代わりに OpenSSL を使用できます。

OpenSSL を使用して CSR を作成するには、まず、OpenSSL の Web サイトから OpenSSL をダウンロードしてインストールします。

1. OpenSSL をインストールしたコンピューターで、コマンドプロンプトまたはシェルから次のコマンドを実行します。

   ```
   openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.
   csr -newkey rsa:2048
   ```

2. 証明書の名前に関する次のメッセージが表示されます。要求された情報を入力します。

   ```
   1  You are about to be asked to enter information that will be
          incorporated into your certificate request.
   2  What you are about to enter is what is called a Distinguished Name
           or a DN.
   3  There are quite a few fields but you can leave some blank
   4  For some fields there will be a default value,
   5  If you enter '.', the field will be left blank.
   6  -----
   7  Country Name (2 letter code) [AU]:US
   8  State or Province Name (full name) [Some-State]:CA
   9  Locality Name (eg, city) []:RWC
   10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
          Customer
   11 Organizational Unit Name (eg, section) [:Marketing
   12 Common Name (eg, YOUR name) []:John Doe
   13 Email Address []:john.doe@customer.com
   ```

3. 次のメッセージが表示されたら、CSR の秘密キーのパスワードを入力します。

   ```
   1  Please enter the following 'extra' attributes
   2  to be sent with your certificate request
   3  A challenge password []:
   4  An optional company name []:
   ```

CSR に署名するには

証明書を、Apple に送信する前に Citrix に送信し、署名を受けて XenMobile で使用できるようにします。

1. ブラウザーで、XenMobile APNs CSR 署名Web サイトに移動します。

2. ［**Upload the CSR**］をクリックします。
3. 証明書に移動して選択します。

   証明書は「.pem/txt」形式である必要があります。
4. **XenMobile APNs CSR** 署名ページで、［署名］ をクリックします。CSR が署名されて、構成されているダウンロードフォルダーに自動的に保存されます。

署名入り **CSR** を **Apple** に送信して **APN** 証明書を取得するには

署名入り CSR（Certificate Signing Request：証明書署名要求）をシトリックスから受け取ったら、それを Apple に送信して APNs 証明書を取得します。

> 注：
>
> 一部のユーザーから、Apple Push Portal へのログイン時の問題が報告されています。代わりの手段として、手順 1 で identity.apple.com リンクにアクセスする前に、Apple Developer Portalにログオンしても構いません。

1. ブラウザーで、https://identity.apple.com/pushcertに移動します。
2. ［証明書識別情報を作成］ をクリックします。
3. Apple で初めて証明書を作成する場合：［利用規約を読みました。内容に同意します。］ チェックボックスをオンにして、［同意します］ をクリックします。
4. ［ファイルの選択］ をクリックし、コンピューター上の署名入り CSR を指定して ［アップロード］ をクリックします。アップロードが成功したことを示す確認メッセージが表示されます。
5. ［ダウンロード］ をクリックして、.pem 証明書を取得します。

   Internet Explorer を使用していて、ファイル拡張子がない場合は、［キャンセル］ を 2 回クリックして、次のウィンドウからダウンロードします。

Microsoft IIS を使用して**.pfx APN** 証明書を作成するには

XenMobile で Apple の APNs 証明書を使用するには：Microsoft IIS で証明書要求を完成させて、証明書を PCKS #12（.pfx）ファイルとしてエクスポートし、この APN 証明書を XenMobile にインポートします。

> 重要：
>
> このタスクには、CSR を生成するために使用したサーバーと同じ IIS サーバーを使用します。

1. Microsoft IIS を開きます。
2. サーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ ウィンドウで、［証明書の要求の完了］ をクリックします。

4. Apple の Certificate.pem ファイルを指定します。フレンドリ名または証明書名を入力して［**OK**］をクリックします。名前に空白や特殊文字は含めないでください。
5. 手順 4 で指定した証明書を選択して［エクスポート］をクリックします。
6. .pfx 証明書の場所とファイル名およびパスワードを指定して［**OK**］をクリックします。

   XenMobile のインストール中にこの証明書のパスワードが必要になります。
7. .pfx 証明書を XenMobile をインストールするサーバーにコピーします。
8. XenMobile コンソールに管理者としてサインオンします。
9. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
10. ［証明書］をクリックします。［証明書］ページが開きます。
11. ［インポート］をクリックします。［インポート］ダイアログボックスが開きます。
12. ［インポート］メニューから、［キーストア］を選択します。
13. ［使用目的］から、［**APNs**］を選択します。
14. ［キーストア］ファイルで、［参照］をクリックしてインポートするキーストアファイルの場所に移動し、そのファイルを選択します。
15. ［パスワード］ボックスに、証明書に割り当てられたパスワードを入力します。
16. ［インポート］をクリックします。

Mac コンピューターで**.pfx APN** 証明書を作成するには

.p12 ファイルと.pfx ファイルは同じものであり、置き換え可能です。

1. macOS を実行する、CSR の生成に使用したものと同じ Mac コンピューターで、Apple から受け取った Production identity（.pem）証明書を見つけます。
2. 証明書ファイルをダブルクリックして、ファイルをキーチェーンにインポートします。
3. 特定のキーチェーンへの証明書の追加を確認するメッセージが表示された場合は、デフォルトの選択されたログインキーチェーンを維持して［**OK**］をクリックします。新たに追加された証明書が証明書の一覧に表示されます。
4. 証明書をクリックして、［ファイル］メニューで［エクスポート］を選択し、証明書の PCKS #12（.pfx）証明書へのエクスポートを開始します。
5. XenMobile Server で使用するには、証明書ファイルに一意の名前を付けるようにします。名前に空白や特殊文字は含めないでください。次に、保存する証明書のフォルダーの場所を選び、.pfx ファイル形式を選択して［保存］をクリックします。
6. パスワードを入力して証明書をエクスポートします。一意で強力なパスワードを使用することをお勧めします。また、後で使用および参照するために証明書とパスワードを安全に保管するようにします。

7. キーチェーンアクセスアプリケーションによって、ログインパスワードまたは選択したキーチェーンを確認するメッセージが表示されます。パスワードを入力して、［**OK**］ をクリックします。XenMobile Server で保存された証明書を使用する準備ができました。

   > 注:
   >
   > CSR を生成して証明書のエクスポートプロセスを完了した元のコンピューターとユーザーアカウントを保持しない場合：ローカルシステムの個人キーと公開キーを保存するかエクスポートすることをお勧めします。そうしなければ、再利用のための APNs 証明書へのアクセスは無効になり、CSR および APNs プロセス全体を繰り返す必要があります。

OpenSSL を使用して**.pfx APNs** 証明書を作成するには

OpenSSL を使用して CSR（Certificate Signing Request：証明書署名要求）を作成した後、OpenSSL を使用して.pfx APNs 証明書を作成することもできます。

1. コマンドプロンプトまたはシェルで、次のコマンドを実行します。`Customer.privatekey.pem`は CSR からの秘密キー、`APNs_Certificate.pem`は Apple から受け取った証明書です。

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey
   .pem -out apns_identity.pfx
   ```

2. .pfx 証明書ファイルのパスワードを入力します。このパスワードは、証明書を XenMobile にアップロードするときに再び使用するので覚えておいてください。
3. .pfx 証明書ファイルの場所を確認します。次に、XenMobile コンソールを使用してアップロードできるように XenMobile Server にコピーします。

APN 証明書を **XenMobile** にインポートするには

新しい APNs 証明書を要求して受け取ったら：その APN 証明書を XenMobile にインポートして、最初の証明書として追加するか、既存の証明書を置き換えます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［証明書］ をクリックします。［証明書］ ページが開きます。
3. ［インポート］ をクリックします。［インポート］ ダイアログボックスが開きます。
4. ［インポート］ メニューから、［キーストア］ を選択します。
5. ［使用目的］ から、［**APNs**］ を選択します。
6. コンピューターの.pfx ファイルまたは.p12 ファイルを指定します。
7. パスワードを入力して、［インポート］をクリックします。

XenMobile の証明書について詳しくは、「証明書」を参照してください。

APN 証明書を更新するには

APNs 証明書を更新するには、証明書を作成する場合と同じ手順を実行します。その後、Apple Push Certificates Portalにアクセスして、新しい証明書をアップロードします。ログオンすると、既存の証明書（または、前の Apple Developers アカウントからインポートされた証明書）が表示されます。

証明書を更新する場合は、証明書を作成する場合との唯一の違いとして、Certificates Portal で ［更新］ をクリックします。Certificates Portal にアクセスするには、このサイトの開発者アカウントが必要です。証明書を更新するときは、同じ組織名と Apple ID を使用していることを確認してください。

APNs 証明書の有効期限を調べるには、XenMobile コンソールで ［構成］ **>** ［設定］ **>** ［証明書］ の順にクリックします。ただし、証明書の有効期限が切れていても証明書を失効させないでください。

1. IIS（Microsoft）、OpenSSL、またはキーチェーンアクセス（macOS）を使用して CSR を生成します。
2. XenMobile APNs CSR 署名Web サイトで、［プッシュ通知証明書の署名要求］ を選択します。
3. ［**+ Upload the CSR**］ をクリックします。次に、ダイアログボックスで CSR に移動し、［開く］、［署名］ の順にクリックします。
4. .plist ファイルを受信したら保存します。
5. **Apple Push Certificates Portal** をクリックしてサインオンします。
6. 更新する証明書を選択して ［更新］ をクリックします。
7. .plist ファイルをアップロードします。出力として.pem ファイルを受信します。.pem ファイルを保存します。
8. この.pem ファイルを使用し、（手順 1 で CSR を作成するために使用した方法に従って）CSR を完了します。
9. 証明書を.pfx ファイルとしてエクスポートします。

XenMobile コンソールで.pfx ファイルをインポートし、以下の手順を実行して構成を完了します:

1. ［設定］ **>** ［証明書管理］ に移動します。
2. ［証明書］ ページで ［インポート］ をクリックします。
3. ［インポート］ メニューから、［キーストア］ を選択します。
4. ［キーストアの種類］ から、［**PKCS # 12**］ を選択します。
5. ［使用目的］ から、［**APNs**］ を選択します。
6. ［キーストアファイル］ では、［ブラウザー］ をクリックしてファイルに移動します。
7. ［パスワード］ ボックスに、証明書のパスワードを入力します。
8. 必要に応じて ［説明］ に入力します。
9. ［インポート］ をクリックします。

XenMobile で ［証明書］ ページにリダイレクトされます。［名前］、［状態］、［有効期限開始］、および ［有効期限終了］ フィールドが更新されます。

ShareFile での SAML によるシングルサインオン

January 24, 2020

XenMobile と ShareFile を構成して、SAML（Security Assertion Markup Language：セキュリティアサーションマークアップランゲージ）を使用した ShareFile Mobile アプリへのシングルサインオン（SSO：Single Sign-On）アクセスを提供することができます。MDX Toolkit を使用してラップされた ShareFile アプリと、Web サイト、Outlook プラグイン、Sync クライアントなどのラップされてない ShareFile クライアントがこの機能の対象となります。

- ラップされている **ShareFile** アプリの場合。ShareFile Mobile アプリを介して ShareFile にログオンするユーザーは、ユーザー認証のために Secure Hub にリダイレクトされ、SAML トークンを取得します。認証が成功した後で、ShareFile Mobile アプリから ShareFile に SAML トークンが送信されます。最初のログオンの後、ユーザーは SSO を介して ShareFile モバイルアプリにアクセスできます。また、毎回ログオンしなくても、Secure Mail のメールに ShareFile からドキュメントを添付できます。
- ラップされていない **ShareFile** クライアントの場合。Web ブラウザーまたはほかの ShareFile クライアントを介して ShareFile にログオンするユーザーは、XenMobile にリダイレクトされます。XenMobile で認証されると、ユーザーは ShareFile に送信された SAML トークンを取得します。最初のログオンの後は、毎回ログオンしなくてもユーザーは SSO を介して ShareFile クライアントにアクセスできます。

XenMobile を ShareFile の SAML ID プロバイダー（IdP）として使用するには、この記事で説明するように、XenMobile を ShareFile Enterprise を使用するように構成する必要があります。または、StorageZone コネクタでのみ動作するように XenMobile を構成することもできます。詳しくは、「ShareFile を XenMobile と使用する」を参照してください。

詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。

前提条件

XenMobile および ShareFile アプリに SSO を構成する前に、以下の前提条件を満たす必要があります：

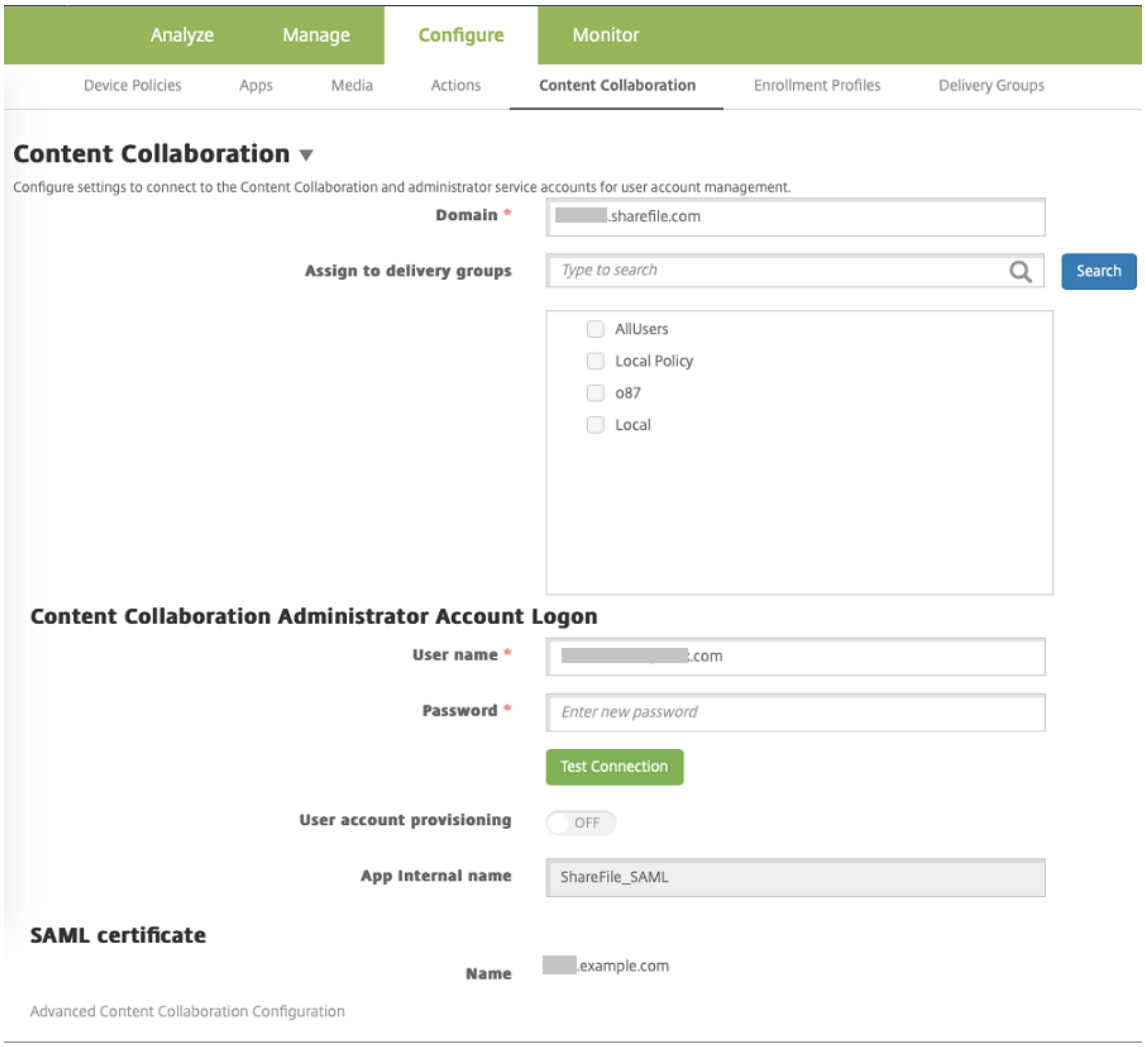
- MDX Service または互換性があるバージョンの MDX Toolkit（ShareFile Mobile アプリ用）

  詳しくは、「XenMobile の互換性」を参照してください。
- 互換性があるバージョンの ShareFile Mobile アプリと Secure Hub
- ShareFile 管理者アカウント
- XenMobile と ShareFile 間の確認された接続

ShareFile アクセスを構成する

ShareFile のために SAML を設定する前に、以下のように ShareFile アクセス情報を入力します。

1. XenMobile Web コンソールで、［構成］の［**ShareFile**］ をクリックします。［**ShareFile**］ 構成ページが開きます。コンソールには、ShareFile ではなく Content Collaboration という用語が表示される場合があります。



2. 次の設定を構成します。

   - ドメイン： ShareFile サブドメイン名を入力します。例：`example.sharefile.com`。
   - デリバリーグループに割り当て： ShareFile と共に SSO を使用するデリバリーグループを選択または検索します。
   - **ShareFile** 管理者アカウントログオン
   - ユーザー名： ShareFile 管理者のユーザー名を入力します。このユーザーには管理特権が必要です。
   - パスワード： ShareFile 管理者のパスワードを入力します。
   - ユーザーアカウントのプロビジョニング： XenMobile でユーザープロビジョニングを有効にするには、この設定を有効にします。ユーザープロビジョニングに ShareFile User Management Tool を使用するには、この設定を無効のままにします。

> 注：
>
> 選択した役割に ShareFile アカウントを持たないユーザーが含まれ、［ユーザーアカウントのプロビジョニング］が有効な場合：そのユーザーに自動的に ShareFile アカウントがプロビジョニングされます。構成をテストするために、メンバーが少ない役割を使用することをお勧めします。これにより、多くのユーザーが ShareFile アカウントを持たない可能性を避けることができます。

3. ［接続のテスト］をクリックして、ShareFile 管理者アカウントのユーザー名とパスワードが特定の ShareFile アカウントに対して認証されることを検証します。
4. ［保存］ をクリックします。
   - XenMobile が ShareFile と同期して、ShareFile の **ShareFile** 発行者**/**エンティティ **ID** と ログイン **URL** の設定が更新されます。
   - ［構成］ **>** ［**ShareFile**］ ページにアプリの内部名が表示されます。アプリの内部名は、後述の「ShareFile.com の SSO 設定を変更する」で説明する手順を完了するために必要になります。

ラップされた **ShareFile MDX** アプリ用の **SAML** の設定

以下の手順が iOS および Android のアプリおよびデバイスに当てはまります。

1. MDX Toolkit で ShareFile Mobile アプリをラップします。MDX Toolkit によるアプリのラップについて詳しくは、「MDX Toolkit によるアプリのラップ」を参照してください。
2. XenMobile コンソールで、ラップされた ShareFile Mobile アプリをアップロードします。MDX アプリをアップロードする方法について詳しくは、「XenMobile に MDX アプリを追加するには」を参照してください。
3. SAML 設定の検証：上記の手順で構成した管理者のユーザー名とパスワードで ShareFile にログオンします。
4. ShareFile および XenMobile が同じタイムゾーンで構成されていることを確認します。構成したタイムゾーンに関して、XenMobile に正しい時刻が表示されていることを確認します。そうでない場合、SSO が失敗する可能性があります。

ShareFile Mobile アプリを検証する

1. ユーザーデバイスに Secure Hub をインストールして構成します。
2. XenMobile Store から ShareFile Mobile アプリをダウンロードしてインストールします。
3. ユーザー名やパスワードの入力を求められずに ShareFile が開始されます。

Secure Mail による検証

1. まだ行っていない場合は、ユーザーデバイスに Secure Hub をインストールして構成します。

2. XenMobile Store から Secure Mail をダウンロード、インストール、および設定します。
3. 新規メールを開いて ［**ShareFile** から添付］ をタップします。メールに添付できるファイルがユーザー名とパスワードを入力しなくても表示されます。

ほかの **ShareFile** クライアントのために **NetScaler Gateway** を構成する

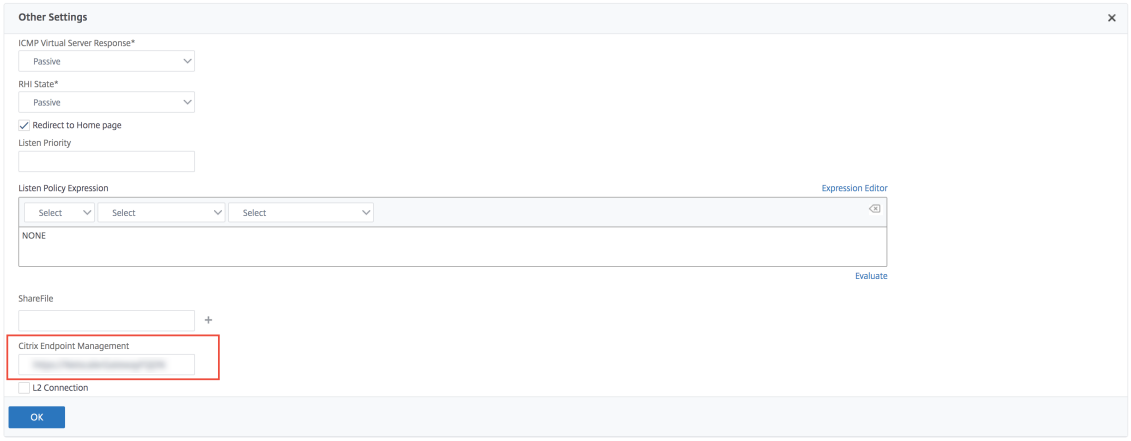
Web サイト、Outlook Plug-in、Sync クライアントなどのラップされていない ShareFile クライアントへのアクセスを構成するには、以下のように NetScaler Gateway を構成して、SAML ID プロバイダーとしての XenMobile の使用をサポートする必要があります。

- ホームページのリダイレクトを無効にする。
- ShareFile のセッションポリシーとプロファイルを作成する。
- NetScaler Gateway 仮想サーバーにポリシーを構成する。

ホームページのリダイレクトを無効にする

/cginfra パスから送られる要求に対するデフォルトの動作を無効にします。この操作により、ユーザーは、構成されたホームページの代わりに本来要求された内部 URL を見ることができるようになります。

1. XenMobile のログオンに使用される NetScaler Gateway 仮想サーバーの設定を編集します。NetScaler で、 ［**Other Settings**］ に移動して ［**Redirect to Home Page**］ チェックボックスをオフにします。



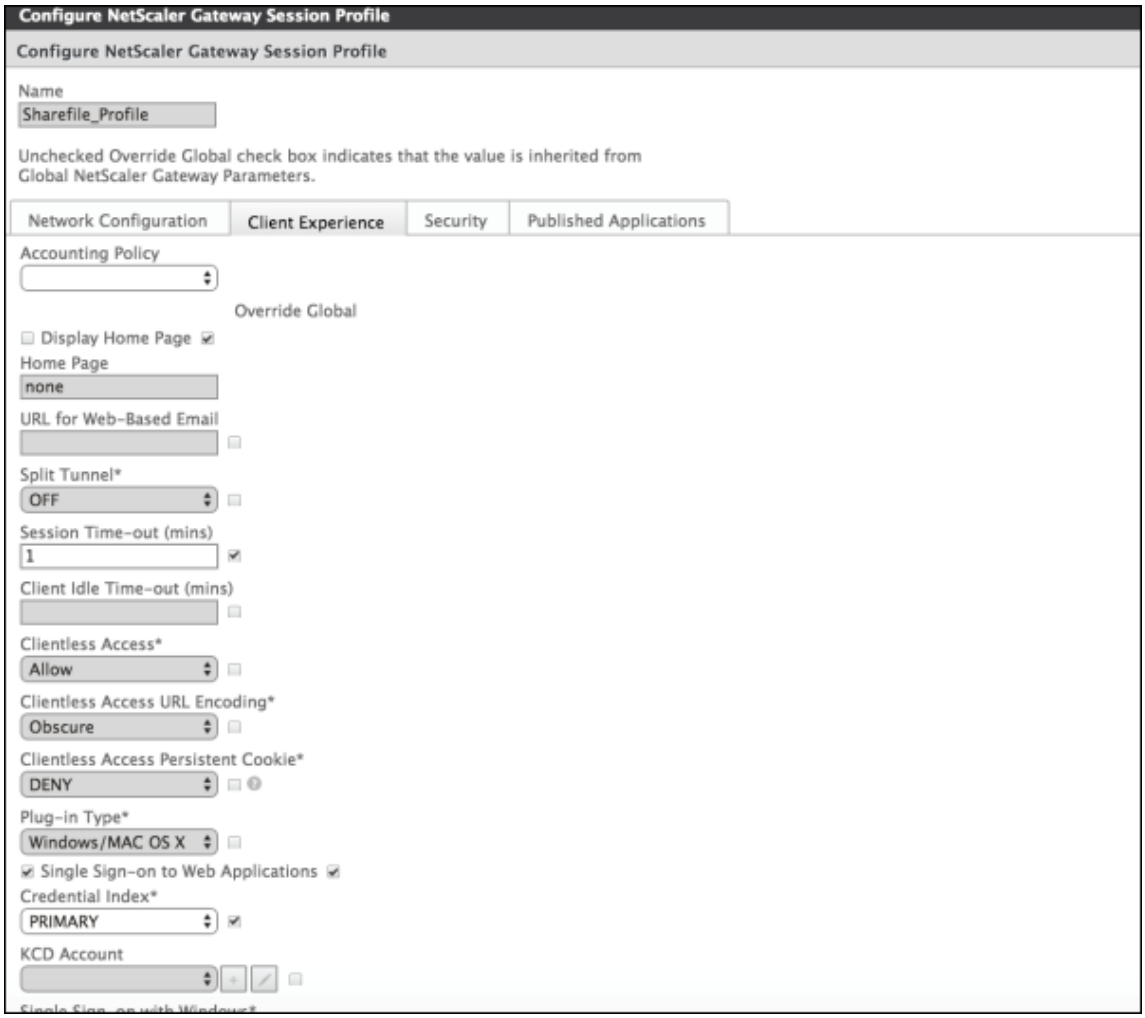
2. ［**ShareFile**］ の下に XenMobile の内部サーバー名およびポート番号を入力します。
3. **Citrix Endpoint Management** で、XenMobile の URL を入力します。使用するバージョンの Citrix Gateway が、古い製品名 **AppController** を参照している場合があります。

   この構成により、/cginfra パスを介して入力した URL に対する要求が承認されます。

ShareFile のセッションポリシーと要求プロファイルを作成する

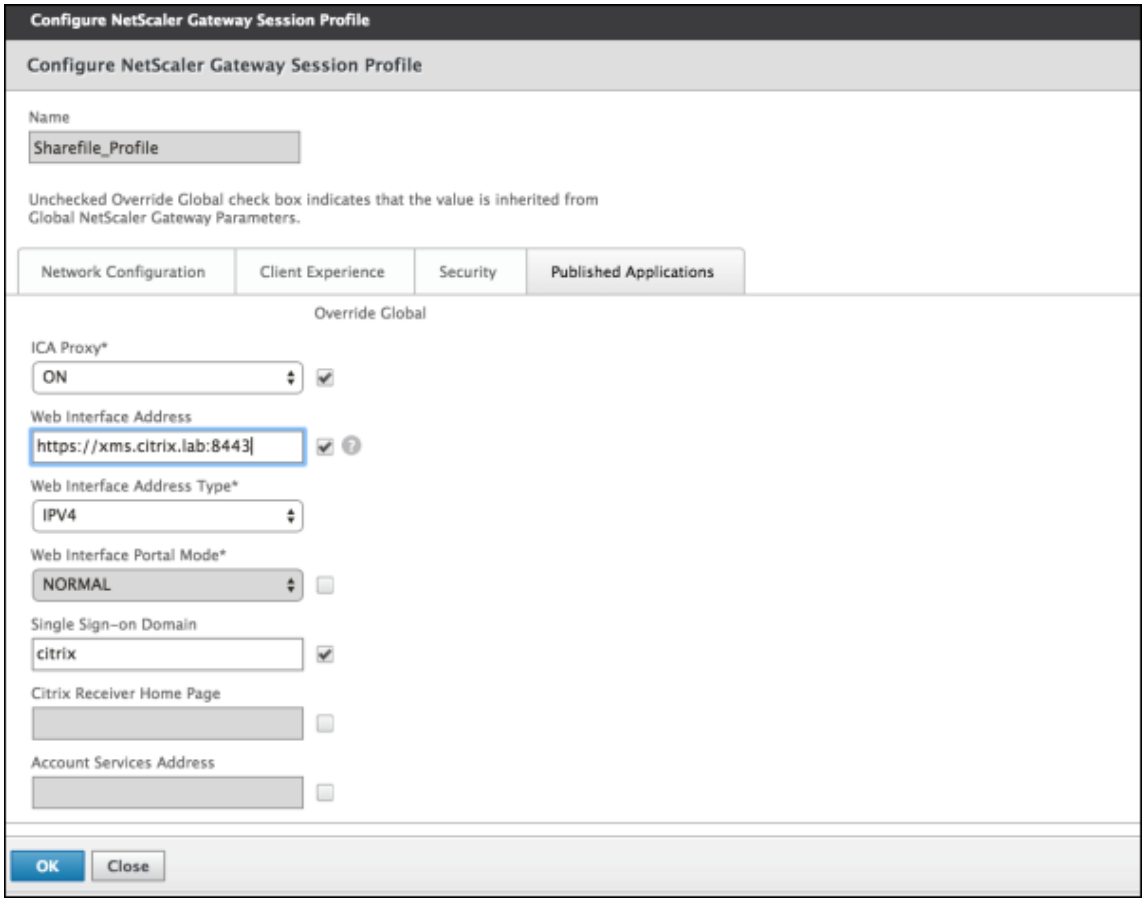
以下の設定を構成して ShareFile セッションポリシーと要求プロファイルを作成します。

1. NetScaler Gateway 構成ユーティリティの左側のナビゲーションペインで、[**NetScaler Gateway**]、[**Policies**]、[**Session**] の順にクリックします。
2. セッションポリシーを作成します。[**Policies**] タブで [**Add**] をクリックします。
3. [**Name**] ボックスに「**ShareFile_Policy**」と入力します。
4. [**+**] をクリックして操作を作成します。[**Create NetScaler Gateway Session Profile**] ページが開きます。



次の設定を構成します。

- **Name**:「**ShareFile_Profile**」と入力します。
- [**Client Experience**] タブをクリックし、以下の設定を構成します:
  - **Home Page**:「**none**」と入力します。
  - **Session Time-out (mins)**:「**1**」と入力します。
  - **Single Sign-on to Web Applications**: この設定をクリックします。
  - **Credential Index**:[**PRIMARY**] をクリックします。
- [**Published Applications**] タブをクリックします。

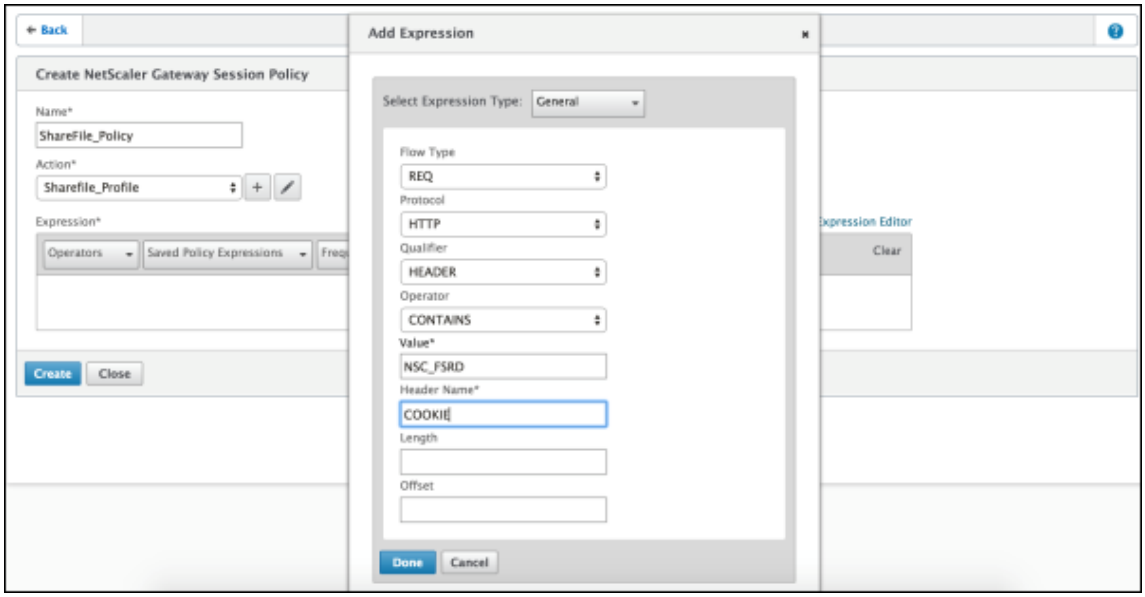


次の設定を構成します。

- **ICA Proxy**：［**ON**］ を選択します。
- **Web Interface Address**： XenMobile サーバーの URL を入力します。
- **Single Sign-on Domain**： Active Directory ドメイン名を入力します。

  WNetScaler Gateway セッションプロファイルを構成するとき、［**Single Sign-on Domain**］ に入力するドメインサフィックスを LDAP に定義する XenMobile ドメインエイリアスと一致させる必要があります。

5. ［**Create**］ をクリックしてセッションプロファイルを定義します。
6. ［**Expression Editor**］ をクリックします。



次の設定を構成します。

- **Value**: 「**NSC_FSRD**」と入力します。
- **Header Name**: 「**COOKIE**」と入力します。

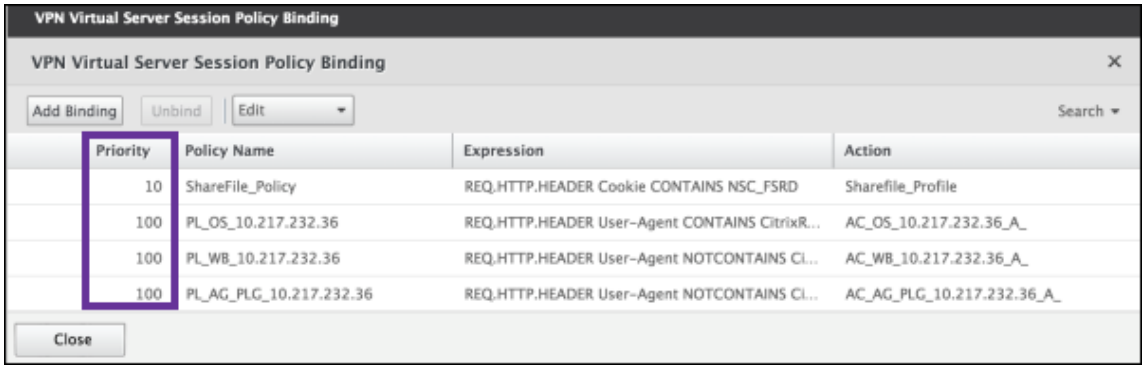
7. [**Create**] をクリックしてから、 [**Close**] をクリックします。

NetScaler Gateway 仮想サーバーにポリシーを構成する

以下の設定を NetScaler Gateway 仮想サーバーに構成します。

1. NetScaler Gateway 構成ユーティリティの左側のナビゲーションペインで、 [**NetScaler Gateway**] の [**Virtual Servers**] をクリックします。
2. [**Details**] ペインで NetScaler Gateway 仮想サーバーをクリックします。
3. [編集] をクリックします。
4. [**Configured policies**] の [**Session policies**] をクリックし、 [**Add binding**] をクリックします。

5. [**ShareFile_Policy**] を選択します。
6. このポリシーの優先順位が一覧表示されるほかのポリシーよりも高くなるように、選択したポリシーに対して自動生成される [**Priority**] の番号を最も小さい数に変更します。次に例を示します:



7. [**Done**] をクリックして、NetScaler 構成を保存します。

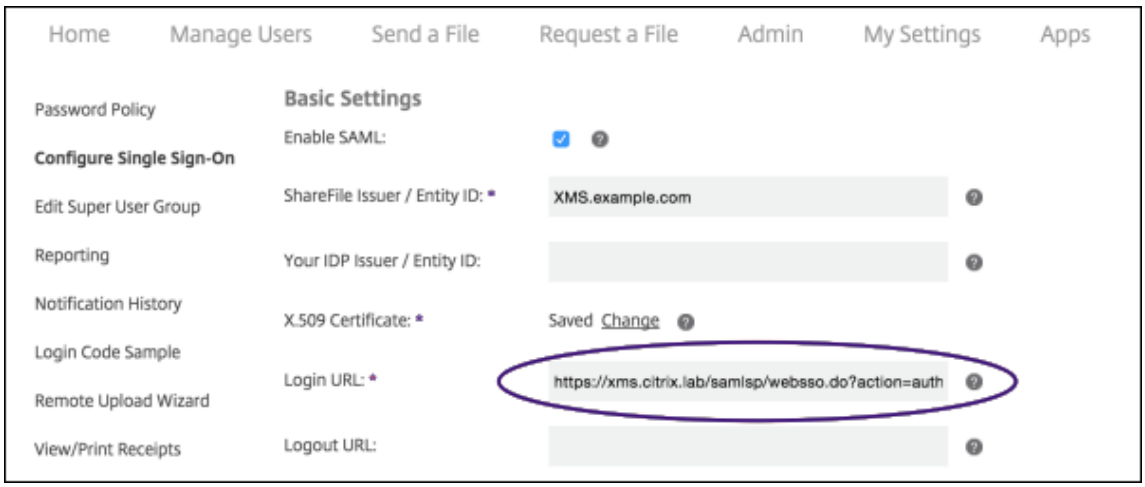
ShareFile.com の SSO 設定を変更する

MDX および非 MDX ShareFile アプリの両方に対して以下の変更を行います。

> 重要:
>
> XenMobile で ShareFile アプリを編集または再作成したり ShareFile の設定を変更したりするたびに、内部アプリ名に新しい番号が付加されます。このため、ShareFile Web サイトでログイン URL も更新して、更新されたアプリ名を反映する必要があります。
>
> Chrome または FireFox で、ShareFile から参照元ヘッダーが送信されなくなりました。詳しくは、「リリースノート、ShareFile Web アプリケーション v19.17」を参照してください。

1. ShareFile アカウント（`https://<subdomain>.sharefile.com`）に ShareFile 管理者としてログオンします。
2. ShareFile Web インターフェイスで [管理] をクリックし、[シングルサインオンの構成] を選択します。
3. [ログイン **URL**] を以下のように編集します:

   編集前の [ログイン **URL**] の例は次のとおりです: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`



- NetScaler Gateway 仮想サーバーの外部 FQDN および「**/cginfra/https/**」を XenMobile サーバーの FQDN の前に挿入し、XenMobile の FQDN の後に「**8443**」を追加します。

  編集した URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

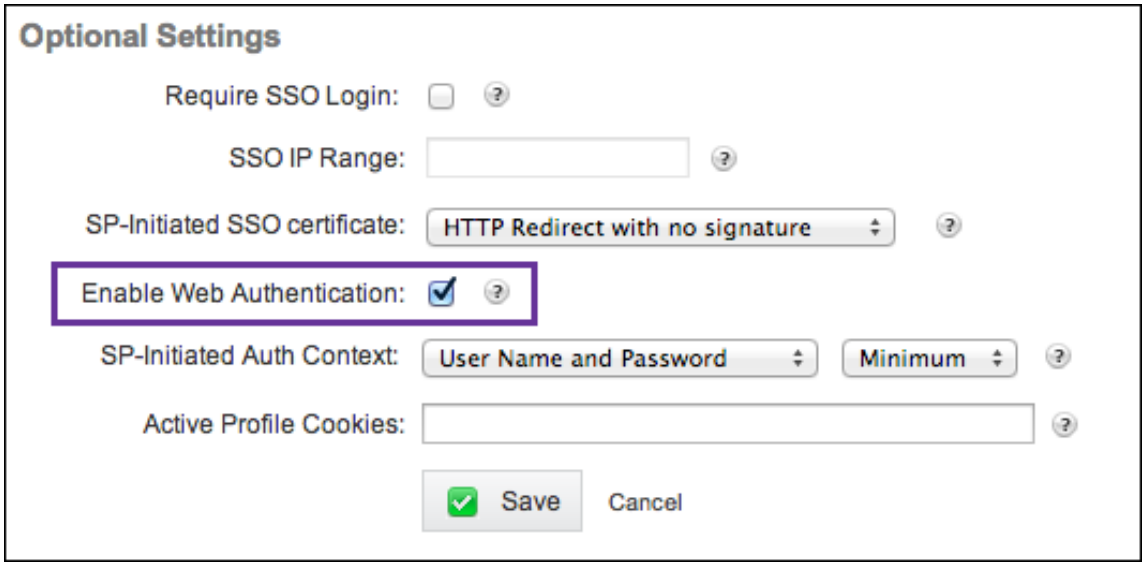
- パラメーター&app=ShareFile_SAML_SPを、ShareFile 内部アプリ名に変更します。内部名はデフォルトで「ShareFile_SAML」です。ただし、構成を変更するたびに、内部名に数字が付加されます (例: ShareFile_SAML_2、ShareFile_SAML_3)。アプリの内部名は、［構成］**>** ［**ShareFile**］ページで調べることができます。

  編集した URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- 「&nssso=**true**」を URL の最後に追加します。

  最終的な URL の例は次のとおりです: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`

4. ［オプション設定］ の下の ［**Web** 認証の有効化］ チェックボックスをオンにします。



構成を検証する

以下の操作を実行して構成を検証します。

1. ブラウザーで`https://<subdomain>sharefile.com/saml/login`にアクセスします。

   NetScaler Gateway のログオンフォームにリダイレクトされます。リダイレクトされない場合は前の構成設定を検証します。

2. NetScaler Gateway および構成した XenMobile 環境のユーザー名とパスワードを入力します。

   `<subdomain>.sharefile.com`の ShareFile フォルダーが表示されます。ShareFile フォルダーが表示されない場合は、正しいログオン資格情報を入力したかどうか確認します。

IDP としての Azure Active Directory

August 22, 2019

Azure Active Directory（AD）を ID プロバイダー（IDP）として構成すると、ユーザーは各自の Azure 資格情報を使って XenMobile に登録できます。

iOS、Android、および Windows 10 のデバイスがサポートされています。iOS および Android デバイスは Secure Hub を通じて登録します。

Azure を IDP として構成するには、［設定］**>**［認証］**>**［**IDP**］の順に選択します。［**IDP**］ページは、このバージョンの XenMobile で新しく追加されています。XenMobile の以前のバージョンでは、Azure の構成は ［設定］**>**［**Microsoft Azure**］ で行いました。

要件

- バージョンおよびライセンス
  - iOS デバイスまたは Android デバイスを登録するには、Secure Hub 10.5.5 が必要となります。
  - Windows 10 デバイスを登録するには、Microsoft Azure プレミアムライセンスが必要となります。
- ディレクトリサービスと認証
  - XenMobile サーバーは、証明書ベースの認証用に構成する必要があります。
  - 認証に NetScaler を使用している場合は、NetScaler は証明書ベースの認証用に構成する必要があります。
  - Secure Hub 認証は Azure AD を使用し、Azure AD で定義された認証モードを履行します。
  - XenMobile サーバーは、LDAP を使用して Windows Active Directory（AD）に接続する必要があります。ローカル LDAP サーバーを Azure AD と同期するように構成します。

認証フロー

デバイスが Secure Hub を使用して登録され、Azure を IDP として使用するように XenMobile が構成される場合

1. ユーザーは自分のデバイスの Secure Hub に表示された Azure AD ログイン画面で、ユーザー名とパスワードを入力します。
2. Azure AD はそのユーザーを認証し、ID トークンを送信します。
3. Secure Hub は ID トークンを XenMobile サーバーと共有します。
4. XenMobile は、ID トークンと、ID トークンの中のユーザー情報を確認します。XenMobile はセッション ID を返送します。

Azure アカウント設定

Azure AD を IDP として使用するには、まず Azure アカウントにログインして以下の変更をします。

1. カスタムドメインを登録して、ドメインを検証します。詳しくは、「Azure Active Directory に独自のドメイン名を追加する」を参照してください。
2. ディレクトリ統合ツールを使用して、オンプレミスのディレクトリを Azure Active Directory に拡張します。詳しくは、「ディレクトリ統合」を参照してください。

Azure AD を使用して Windows 10 デバイスを登録するには、Azure アカウントに以下の変更をします。

1. MDM を Azure AD の信頼できるパーティーにします。そのためには、［**Azure Active Directory**］**>**［アプリケーション］ をクリックして、［追加］ をクリックします。
2. ギャラリーの ［アプリケーションを追加する］ を選択します。［モバイルデバイス管理］ に移動して、オンプレミスの **MDM** アプリケーションを選択します。設定を保存します。

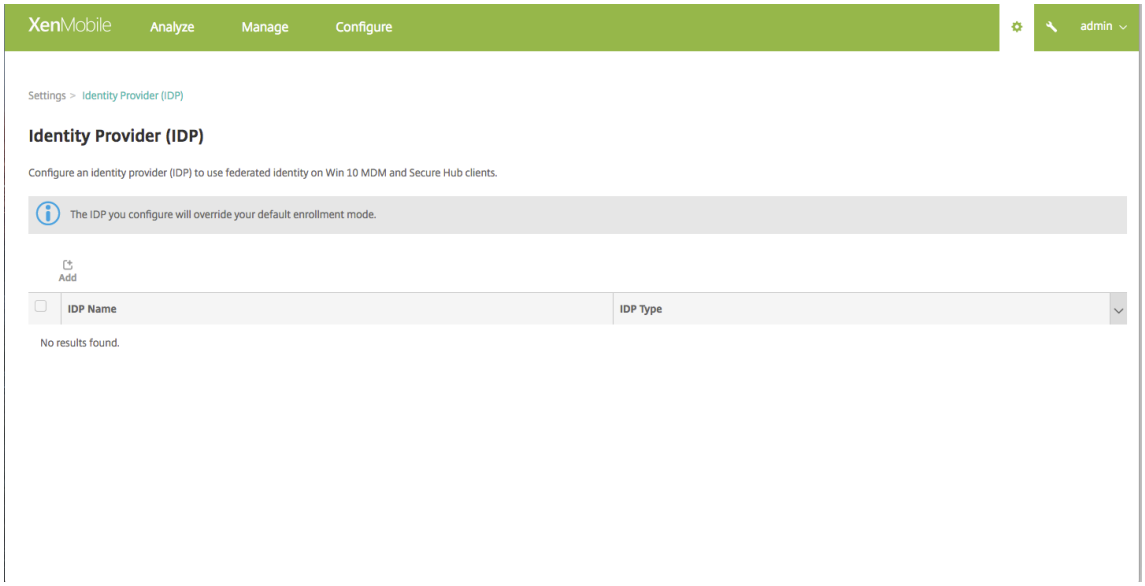
Citrix XenMobile クラウドの契約をした場合でも、オンプレミスアプリケーションを選択します。Microsoft の用語では非マルチテナントアプリケーションは、オンプレミス MDM アプリケーションです。

3. アプリケーションで、XenMobile サーバー検出、使用条件エンドポイント、および APP ID URI を構成します。
   - **MDM** 検出 **URL**： `https://<FQDN>:8443/<instanceName>/wpe`
   - **MDM** 利用規約 **URL**： `https://<FQDN>:8443/<instanceName>/wpe/tou`
   - アプリ **ID URI**： `https://<FQDN>:8443/`
4. 手順 2 で作成したオンプレミス MDM アプリケーションを選択します。［**Manage devices for these users**］ オプションを有効にして、すべてのユーザーまたは特定のユーザーグループに対して MDM 管理を有効にします。

   Windows 10 デバイスに Azure AD を使用することについて詳しくは、Microsoft の記事「Azure Active Directory と MDM の統合」を参照してください。

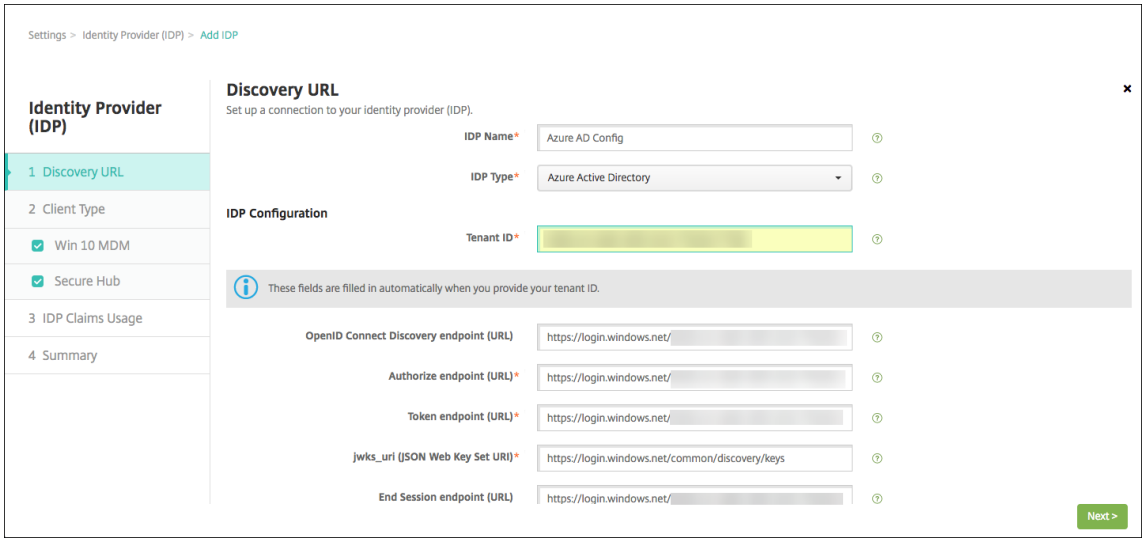
Azure AD を IDP として構成

1. Azure アカウントから以下のように必要な情報を探して記録します。
   - テナント ID - Azure アプリケーション設定ページに記載
   - Azure AD を使用して Windows 10 デバイスを登録する場合は、以下についても必要です。
     - アプリ **ID URI**： XenMobile を実行しているサーバーの URL
     - クライアント **ID**： Azure の構成ページのアプリの一意の識別子
     - キー： Azure アプリケーション設定ページに記載
2. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
3. ［認証］ の下の ［**ID** プロバイダー（**IDP**）］ をクリックします。［**ID** プロバイダー］ ページが開きます。

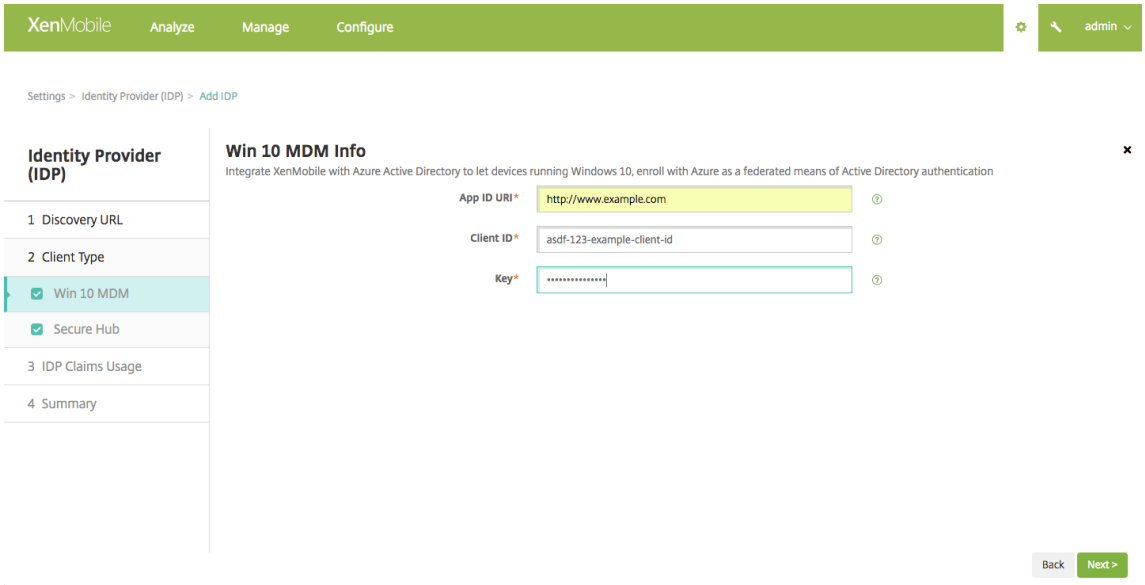


4. ［追加］ をクリックします。［**IDP** 構成］ ページが開きます。
5. IDP の以下の情報を構成します。
   - **IDP** 名： 作成している IDP 接続の名前を入力します。
   - **IDP** の種類： IDP の種類として Azure Active Directory を選択します。
   - テナント **ID**： Azure アプリケーション設定のページから値をコピーします。ブラウザーのアドレスバーに表示されている、数字と文字から成る部分をコピーします。

   たとえば、`https://manage.windowszaure.com/acmew.onmicrosoft.com##workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...` ではテナント ID は次のとおりです：`abc123-abc123-abc123`



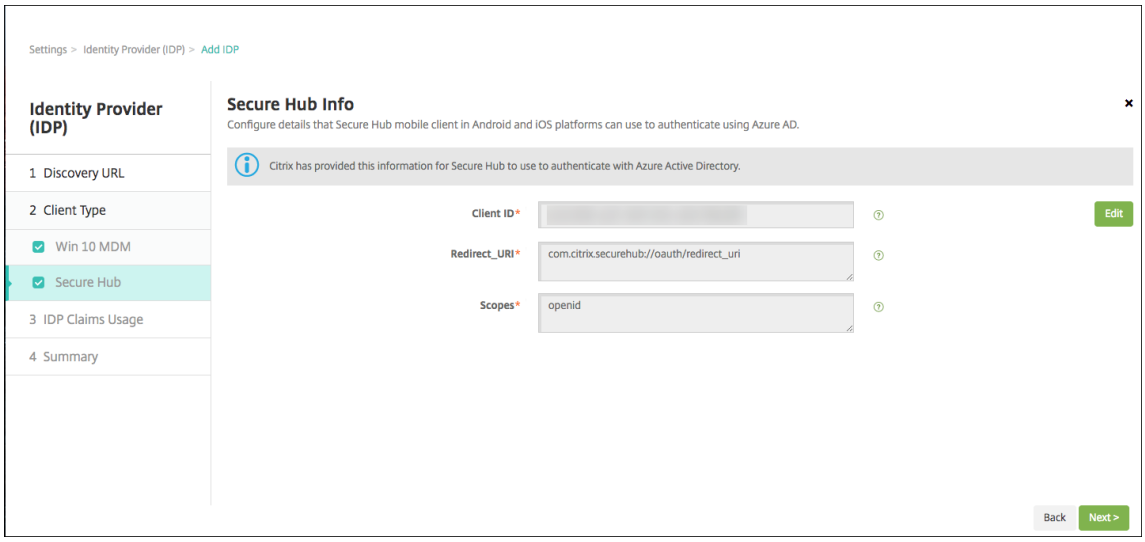
6. 残りのフィールドは自動的に入力されます。入力後、［次へ］ をクリックします。
7. Azure AD を使用して Windows 10 デバイスを MDM 登録するために XenMobile を構成するには、以下の設定を構成します。この任意の手順をスキップするには、［**Win 10 MDM**］ をオフにします。
   - アプリ **ID URI**： Azure 設定の構成時に入力した、XenMobile サーバーの URL を入力します。
   - クライアント **ID**： Azure 構成のページから値をコピーして貼り付けます。クライアント ID はアプリの一意の識別子です。
   - キー： Azure アプリケーション設定のページから値をコピーします。［キー］ の下で、一覧から期間を選択し、設定を保存します。キーは、コピーしてこのフィールドに貼り付けることができます。キーは、Microsoft Azure AD でアプリがデータを読み取ったり書き込んだりする場合に必要です。



8. [次へ] をクリックします。

   Citrix は Secure Hub を Microsoft Azure と共に登録し、その情報をメンテナンスしています。この画面は、Secure Hub が Azure Active Directory と通信するのに使用する詳細情報を表示します。このページは将来この情報を変更することが必要になった場合に使用されます。このページは Citrix が変更の通知をしたときにのみ編集します。

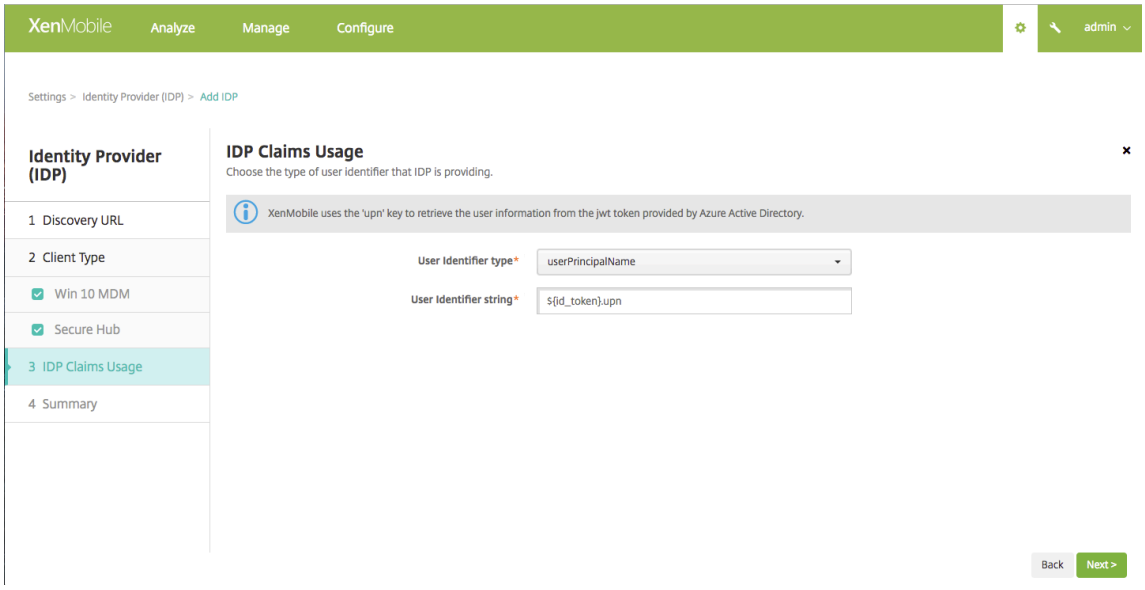
9. [次へ] をクリックします。



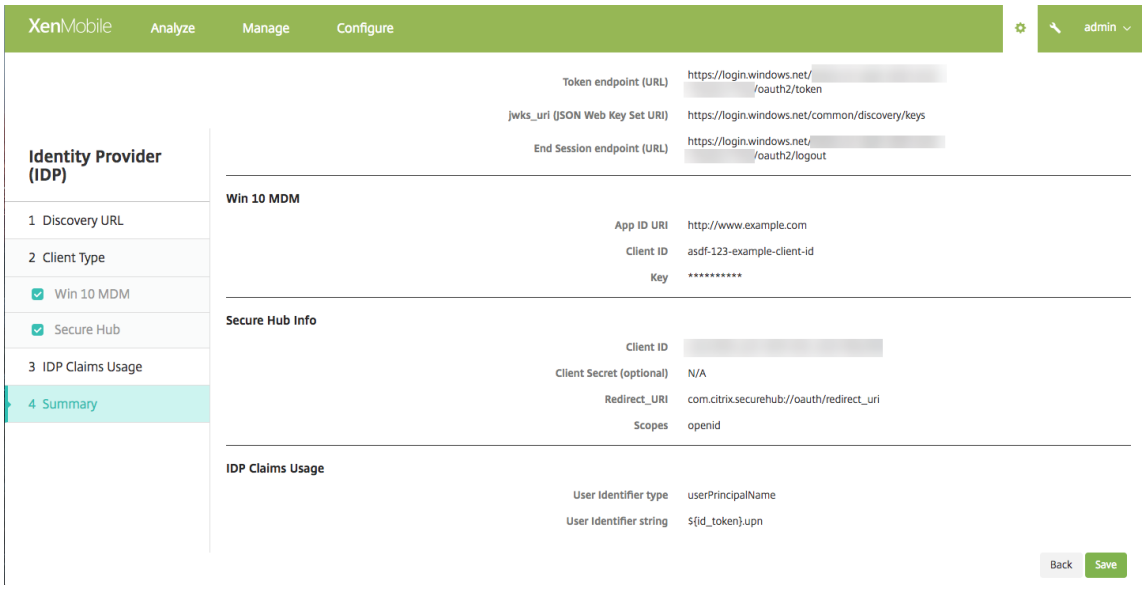
10. IDP が指定するユーザー識別子の種類を選択します。

    - ユーザー識別子の種類: リストから [**userPrincipalName**] を選択します。
    - ユーザー識別子の文字列: このフィールドは自動入力されます。

11. [次へ] をクリックします。

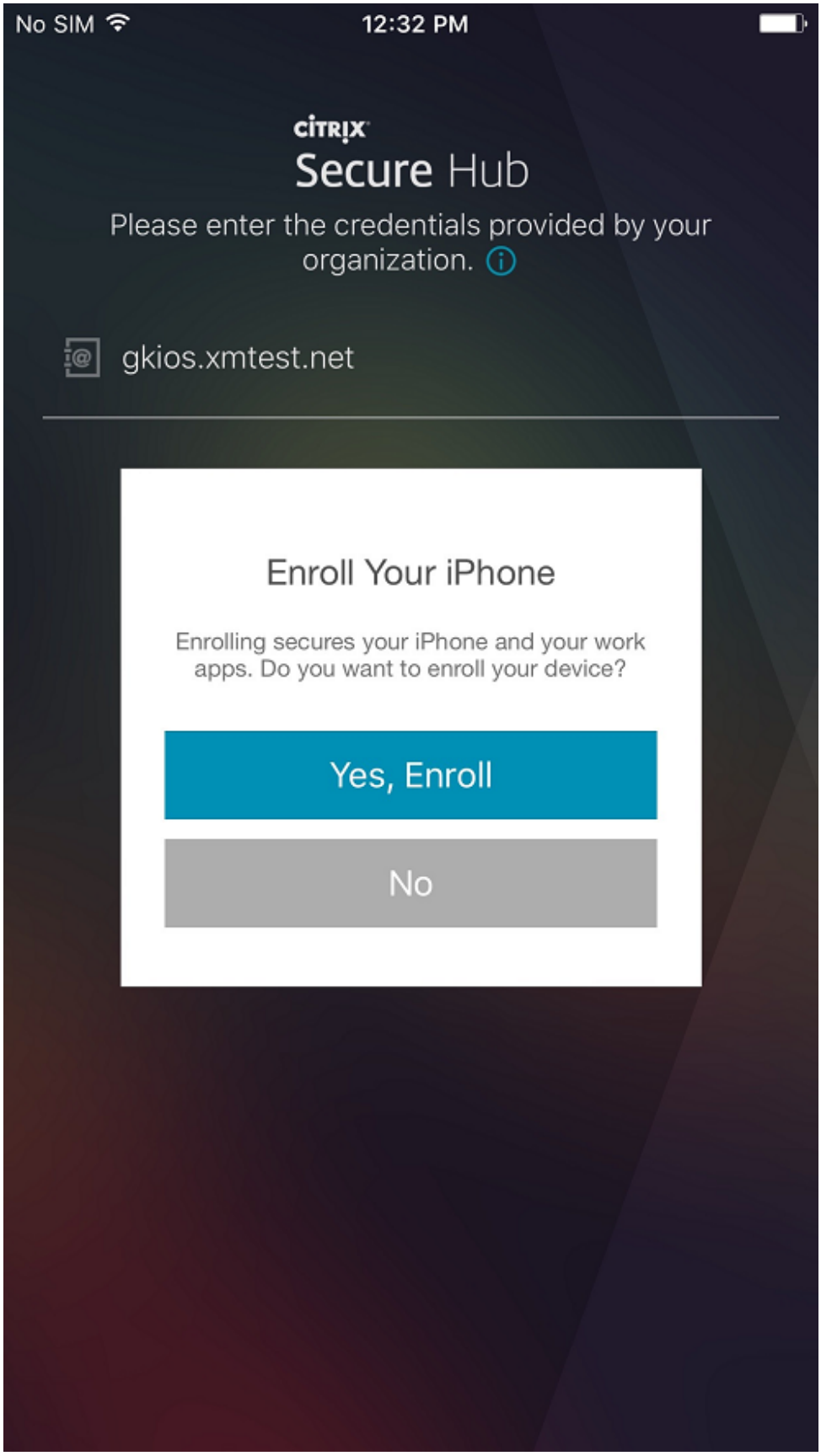


12. [設定の適用] ページで内容を確認し、 [保存] をクリックします。

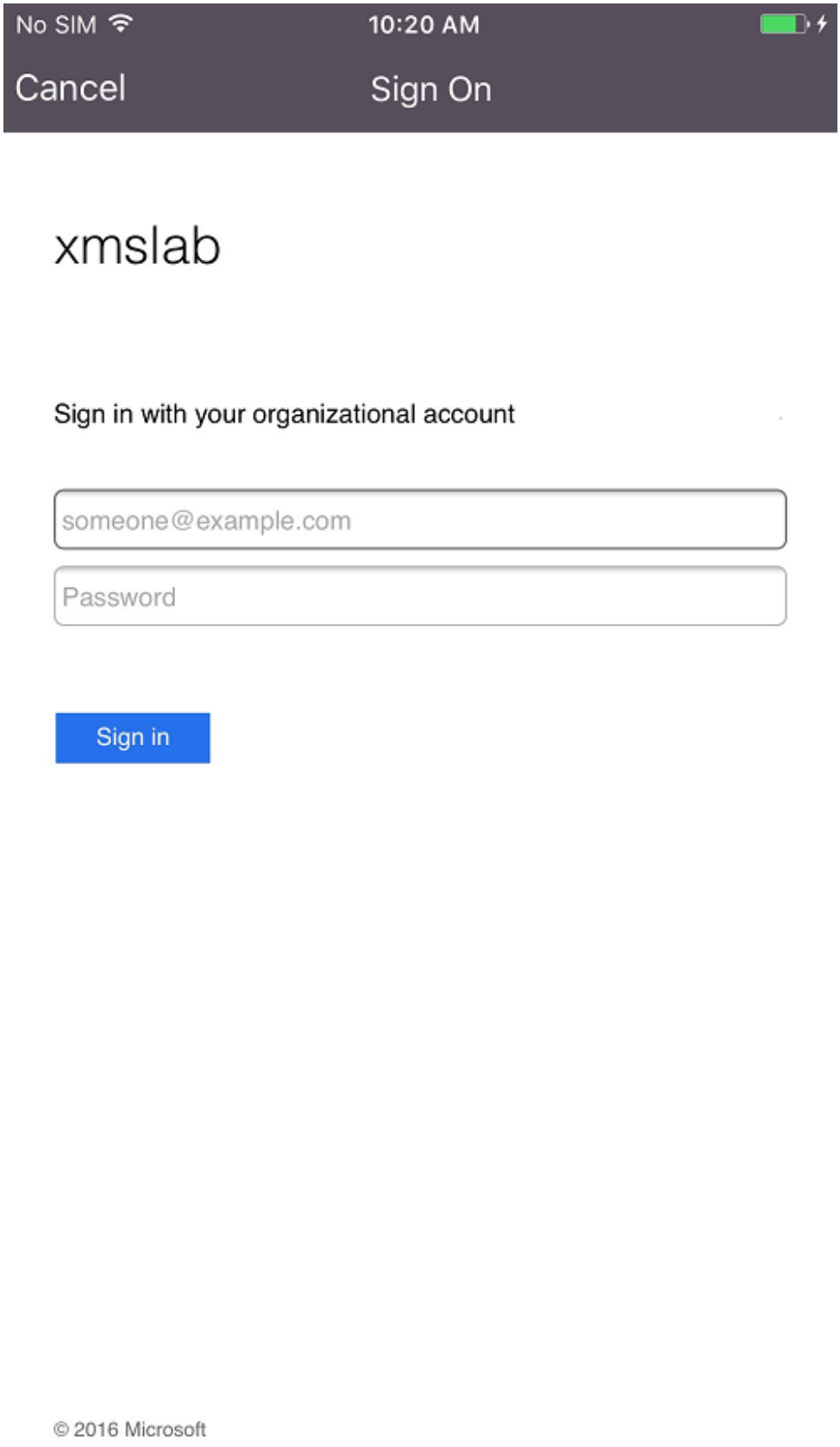


ユーザーエクスペリエンスとは

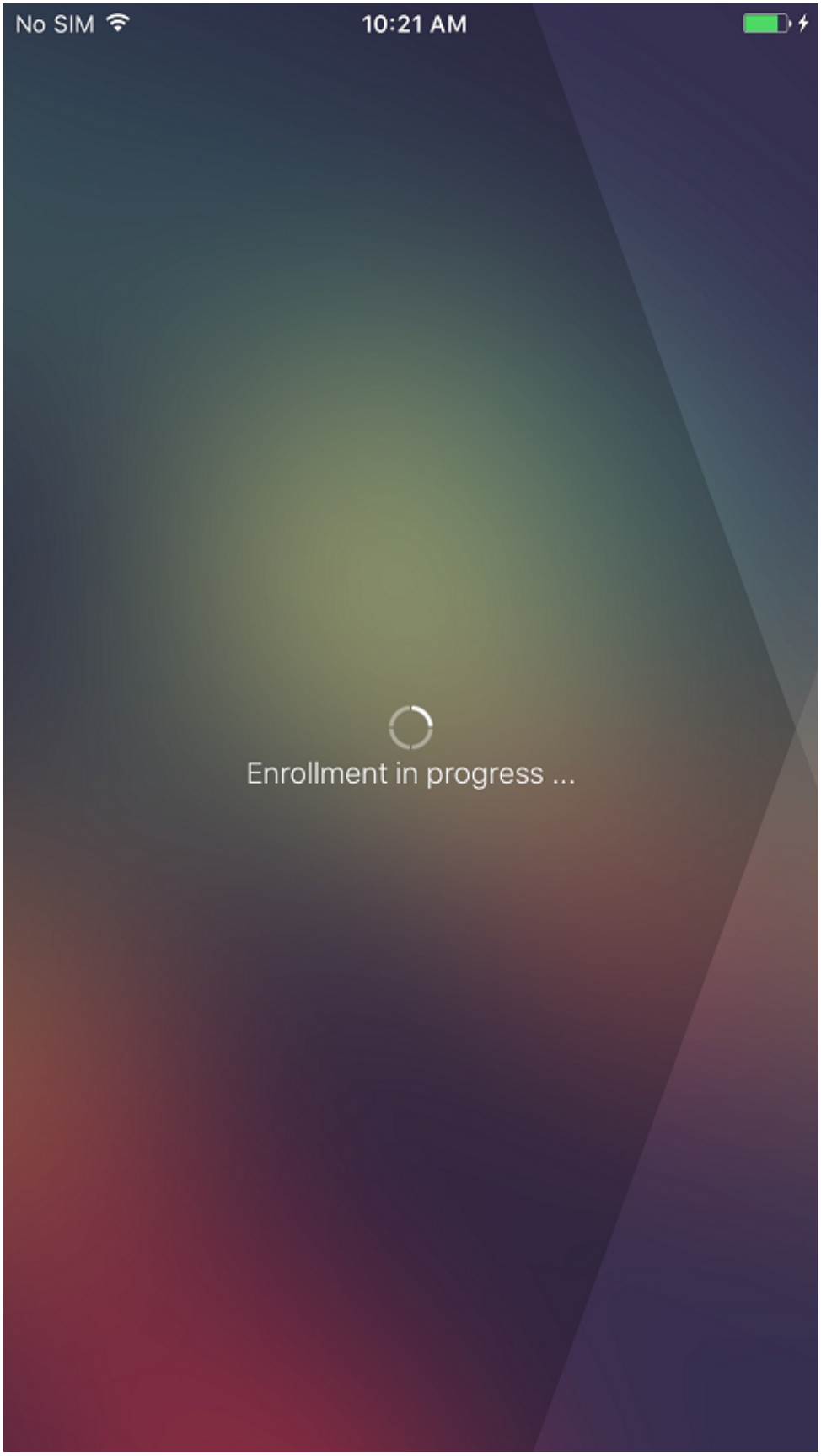
1. Secure Hub を起動します。次に、XenMobile サーバーの完全修飾ドメイン名（FQDN）、ユーザープリンシパル名（UPN）、またはメールアドレスを入力します。

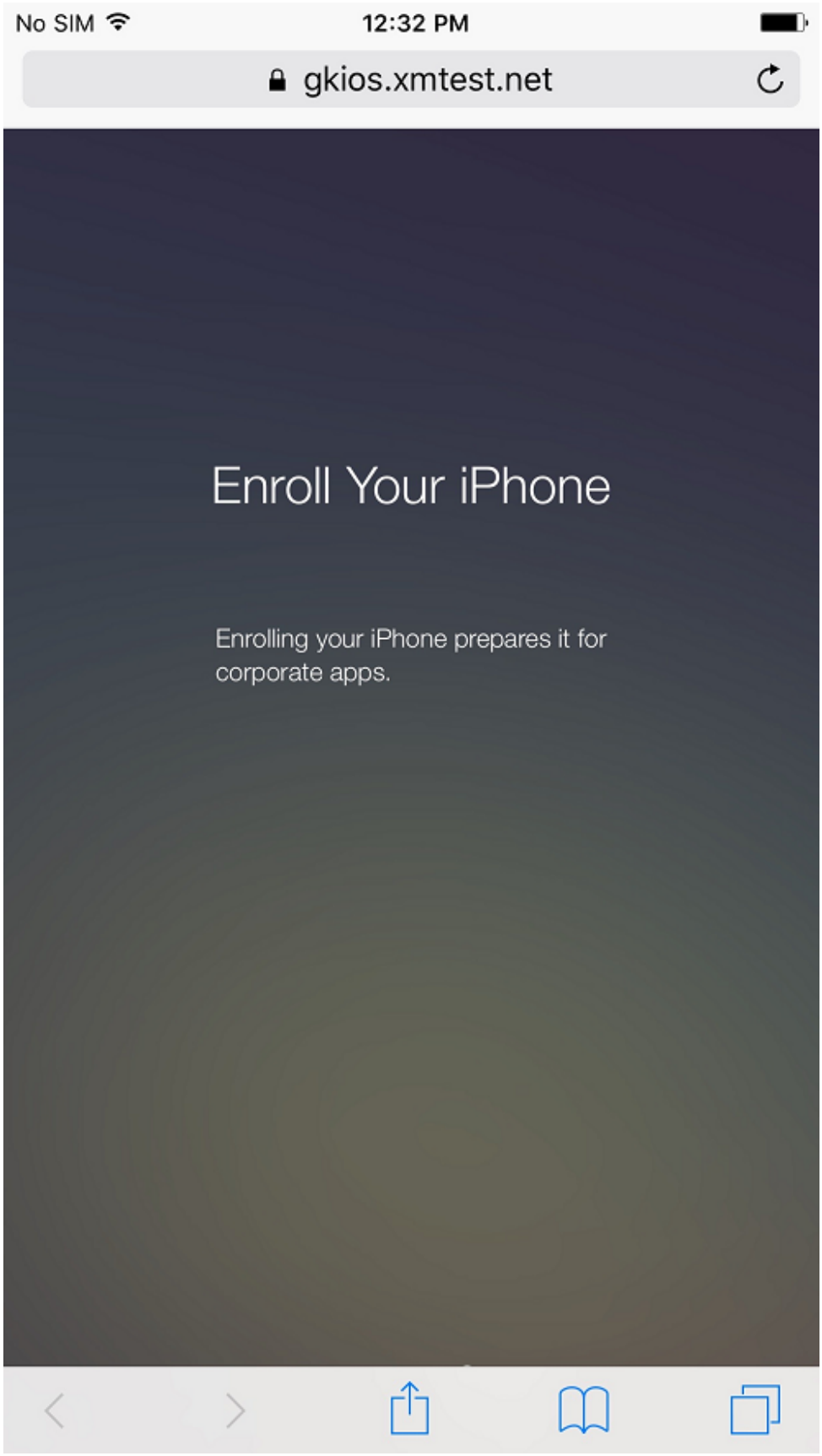


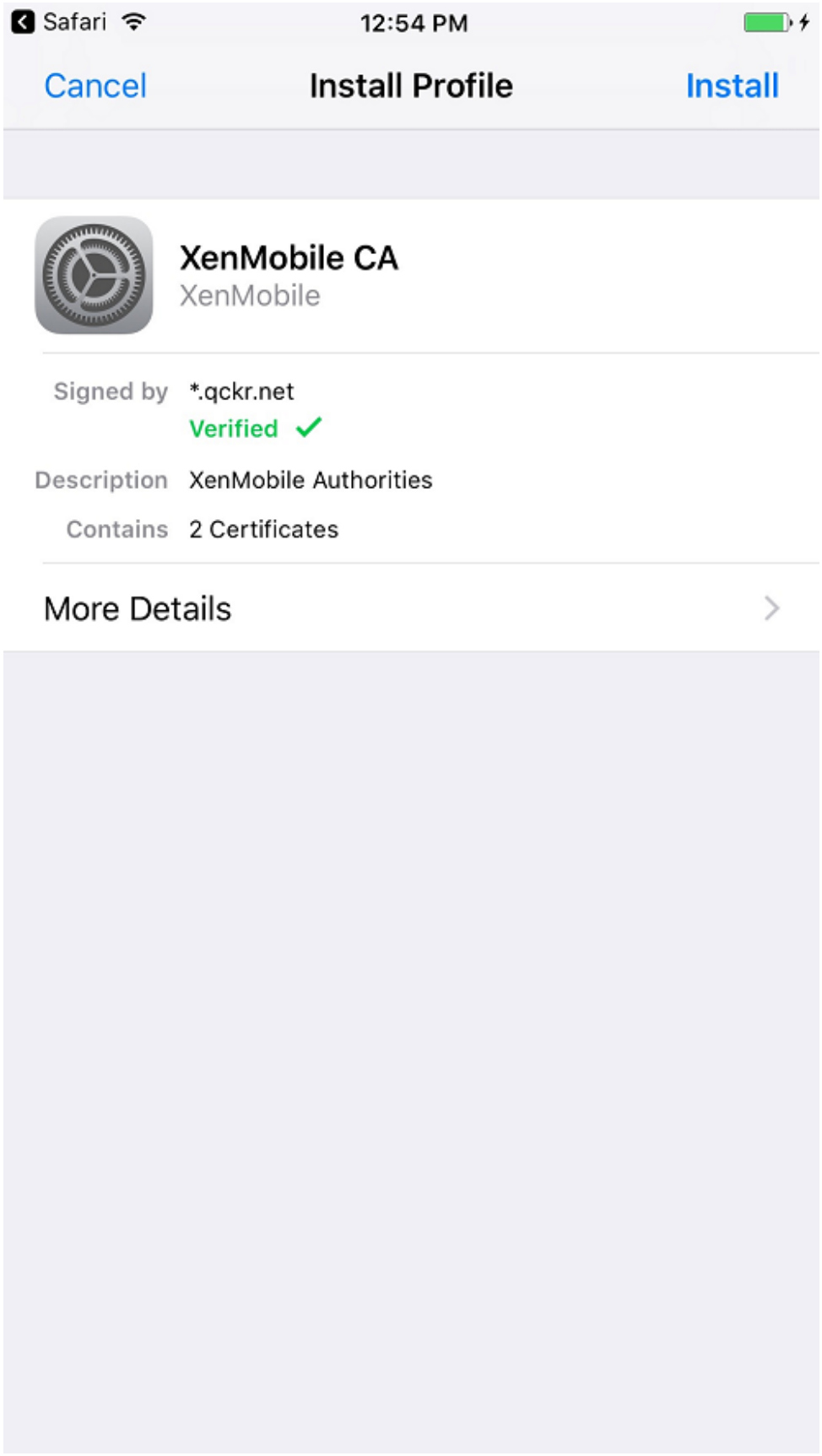
2. 次に、［はい、登録します］ をクリックします。



3. Azure AD 資格情報を使用してログオンします。







4. Secure Hub によるその他の登録と同じ方法で登録手順を完了します。

> 注:
>
> XenMobile は登録招待状の Azure AD による認証をサポートしていません。登録 URL を含む登録招待状をユーザーに送信する場合は、ユーザーは Azure AD の代わりに LDAP を使用して認証します。

派生資格情報

January 10, 2020

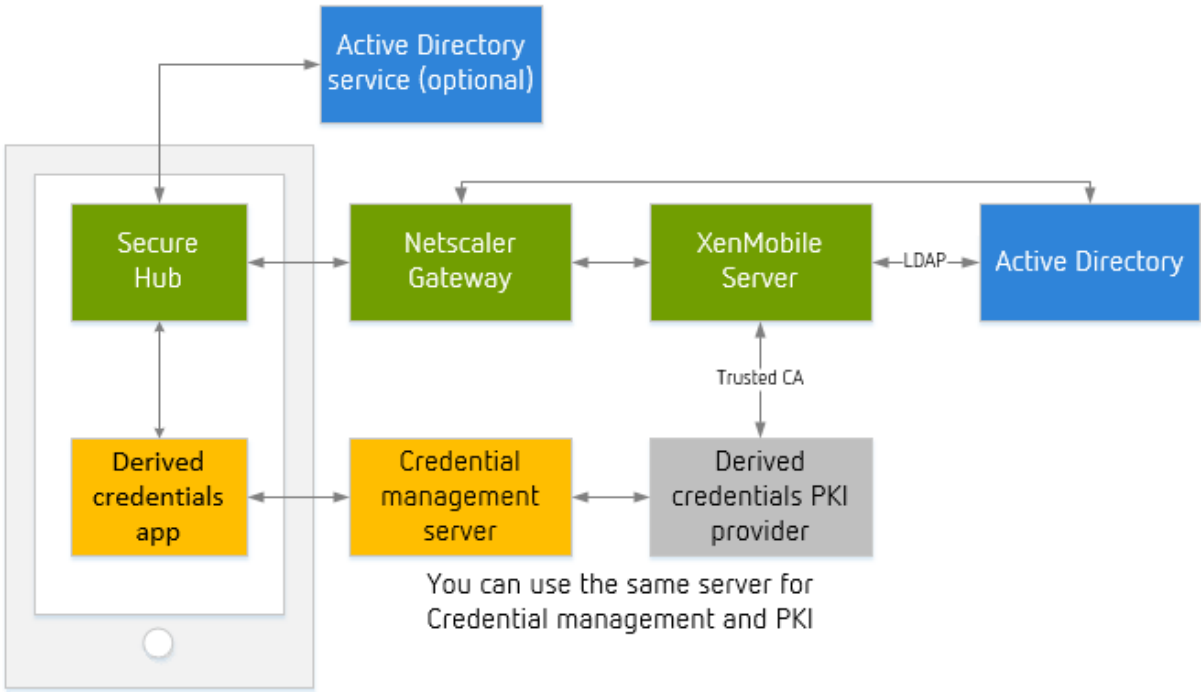
派生資格情報によって、モバイルデバイスに強力なユーザー認証が得られます。資格情報は、スマートカードから派生したもので、カードの代わりにモバイルデバイスの中に存在します。スマートカードは、Personal Identity Verification（PIV）カードです。

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。XenMobile は、資格情報プロバイダーから取得した資格情報を、デバイスのセキュアなボールトに保存します。

XenMobile では、デバイスの登録と認証に派生資格情報を使用できます。派生資格情報用に構成された場合、XenMobile では登録招待状や他の登録モードはサポートされません。iOS の登録で派生資格情報を使用できます。

アーキテクチャ

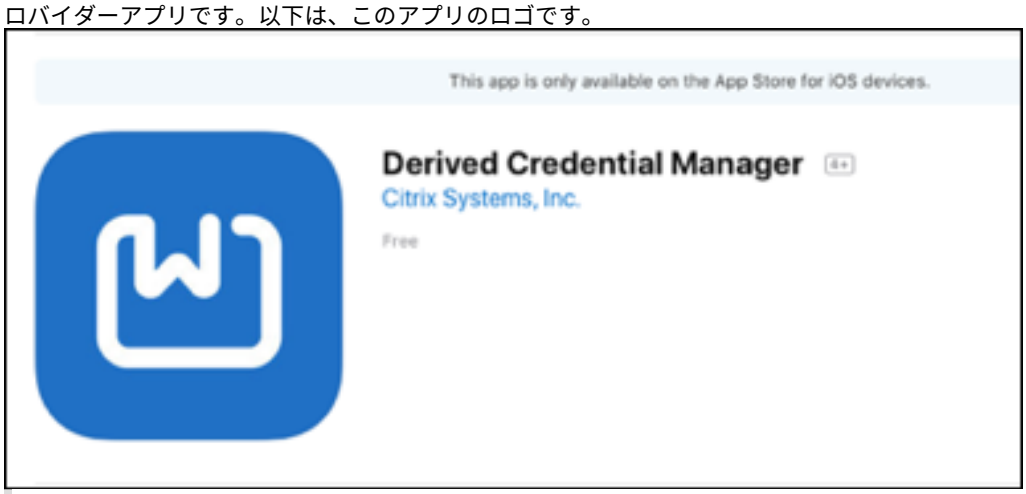
登録の場合は、XenMobile Server は、以下の図に示す通り、コンポーネントに接続します。



- デバイス登録中に、Secure Hub は派生資格情報アプリから証明書を取得します。
- 派生資格情報アプリは、登録中に資格情報管理サーバーと通信します。
- 資格情報管理サーバーとサードパーティ PKI プロバイダーについては、同一のサーバーを使用することも、別のサーバーを使用することもできます。
- XenMobile Server はサードパーティ PKI サーバーに接続して、証明書を取得します。

要件

- Citrix Secure Hub をダウンロードしてインストールします。
- 派生資格情報を使用して、アプリをダウンロードして構成します:
  - **Entrust Datacard** の場合:
    * XenMobile の登録前に、デバイスで Citrix Derived Credentials Manager アプリをダウンロードしてインストールします。Derived Credentials Manager アプリは、シトリックスの ID プロバイダーアプリです。以下は、このアプリのロゴです。



> 注:
> Citrix Derived Credentials Manager アプリは、新しい登録のみをサポートします。デバイスユーザーは再登録する必要があります。

    * XenMobile Server バージョン 10.8 以降。
    * XenMobile Server は Enterprise モードで構成されていることが必要。
  - その他の派生情報資格プロバイダー: その他の資格情報ソリューションのほとんどは、おそらく XenMobile と互換性がありますが、実稼働させる前に統合テストをしてください。
- 資格情報プロバイダーサーバーに証明書を発行する証明機関のルート証明書を持つ必要があります。その設定によって、XenMobile は登録中にデジタル署名済みの証明書を受信することができます。証明書の追加について詳しくは、「証明書と認証」を参照してください。
  - ユーザーのメールドメインが LDAP ドメインと異なる場合は、メールドメインを、[設定] **>** [**LDAP**] のドメインエイリアス設定に含めます。たとえば、メールアドレスのドメインが`citrix.com`で、LDAP ドメイン名が`sample.com`の場合は、ドメインエイリアスを**`sample.com, citrix.com`**に設定

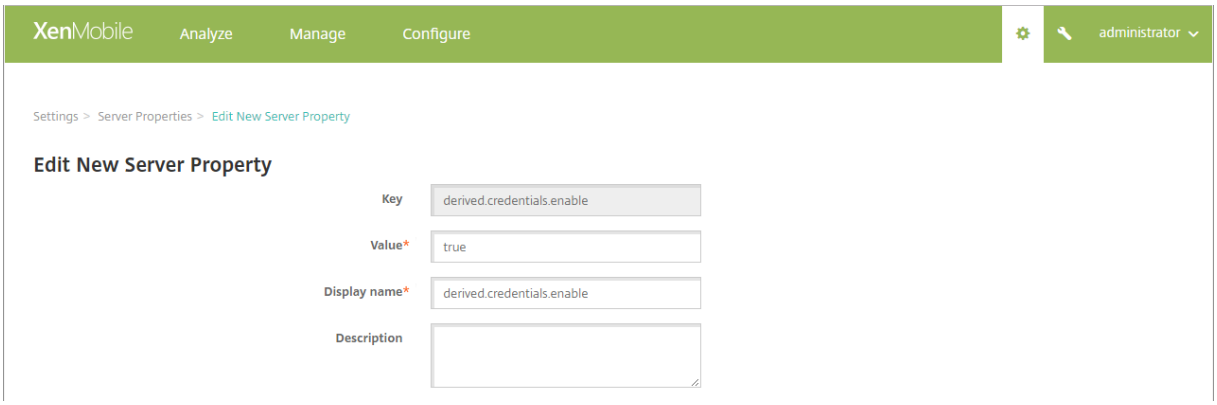
します。
  - XenMobile は共有デバイスで派生資格情報の使用をサポートしていません。
- ユーザー ID 証明書
  - サブジェクトの別名フィールドのユーザー名は、SujectAltName 拡張の otherName フィールド、rfc822Name フィールド、または dNSName フィールドの形式である必要があります。その他のフィールドはサポートされていません。サブジェクトの別名について詳しくは、RFC、https://www.ietf.org/rfc/rfc5280.txtを参照してください。
  - メールまたは CN のサブジェクトフィールド内のユーザ ID はサポートされていません。
- 証明書認証または証明書 + セキュリティトークン認証用に構成された Citrix Gateway

派生資格情報の有効化

デフォルト設定では、XenMobile コンソールには、［設定］**>**［派生資格情報］ のページがありません。

派生資格情報のインターフェイスを有効にするには:

- ［設定］**>**［サーバープロパティ］ の順に移動し、サーバー属性 **derived.credentials.enable** を追加してプロパティを **true** に設定します。

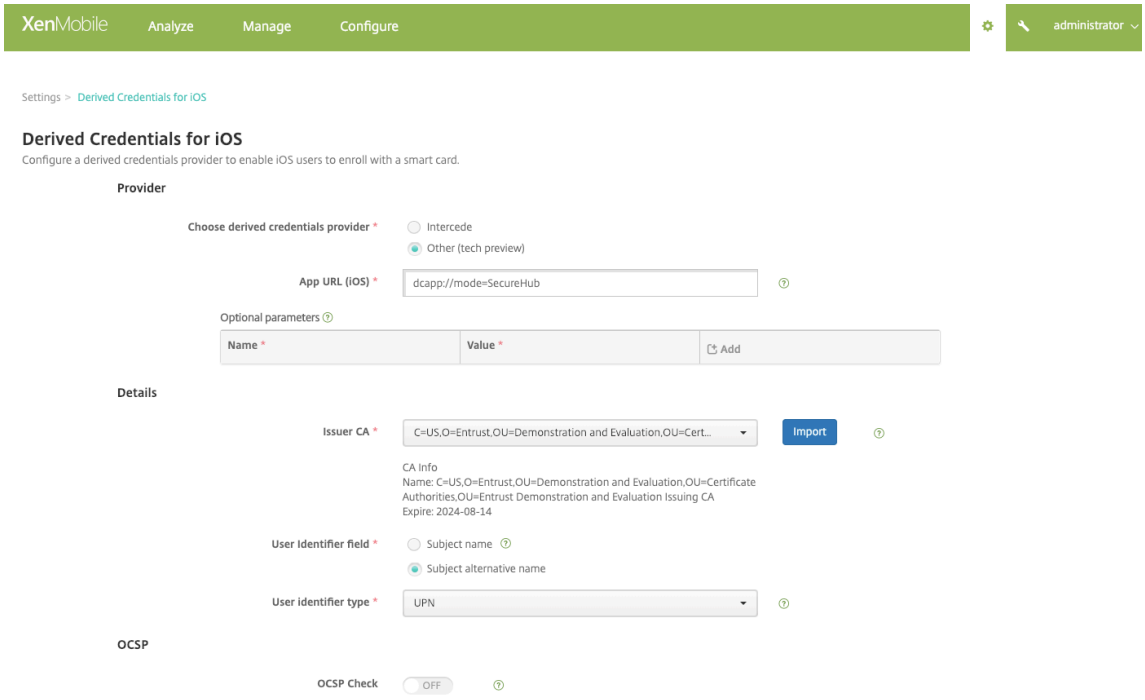


派生資格情報の構成

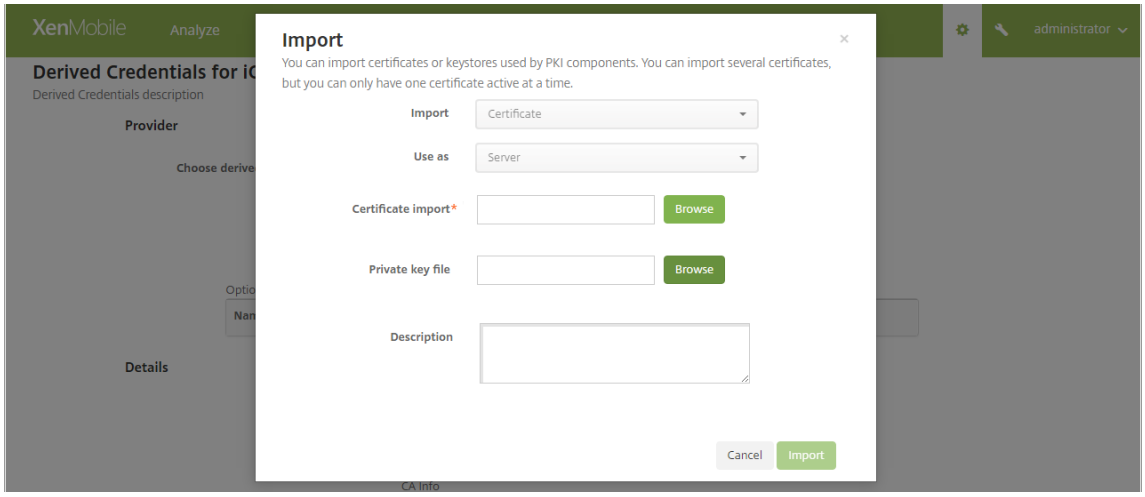
XenMobile との統合を計画している派生資格情報プロバイダー向けの実用的な構成があることを前提としています。XenMobile を構成すると、サーバーとの通信が可能になります。また、XenMobile に追加済みの派生資格情報の CA 証明書を選択するか、CA 証明書をインポートできます。

その CA 証明書のオンライン証明書状態プロトコル（OCSP）サポートをアクティブにすることができます。OCSP について詳しくは、「PKI エンティティ」の「任意 CA」を参照してください。

1. XenMobile コンソールで、［設定］**>**［**iOS** の派生資格情報］ の順に選択します。
2. ［派生資格情報のプロバイダーを選択］ の場合、Entrust Datacard で ［その他］ を選択します。［アプリケーション **URL**（**iOS**）］ にdcapp://mode=SecureHubを入力します。



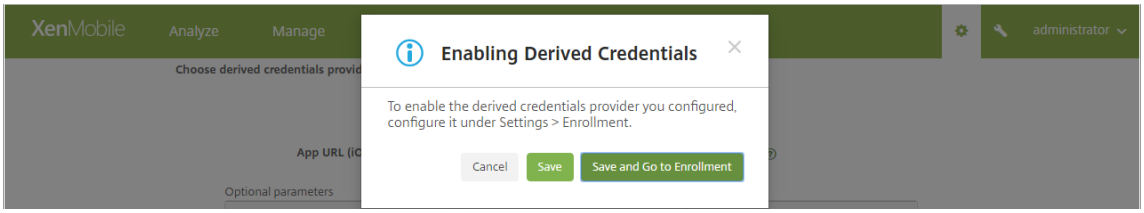
3. オプションのパラメーター: 派生資格情報プロバイダーの中には、接続のパラメーターを指定する必要があるものもあります。たとえば、ベンダーがバックエンドサーバーの URL を指定することを要求する場合もあります。［追加］ をクリックしてパラメーターを設定します。
4. 派生資格情報の証明書の指定: 証明書が既に XenMobile にアップロードされている場合は、［発行者 **CA**］からこの証明書を選択します。それ以外の場合は、［インポート］ をクリックして証明書を追加します。［証明書のインポート］ ダイアログボックスが開きます。
5. ［証明書のインポート］ ダイアログボックスで、［参照］ をクリックし、証明書を選択します。次に、［参照］ をクリックし、秘密キーファイルを選択します。



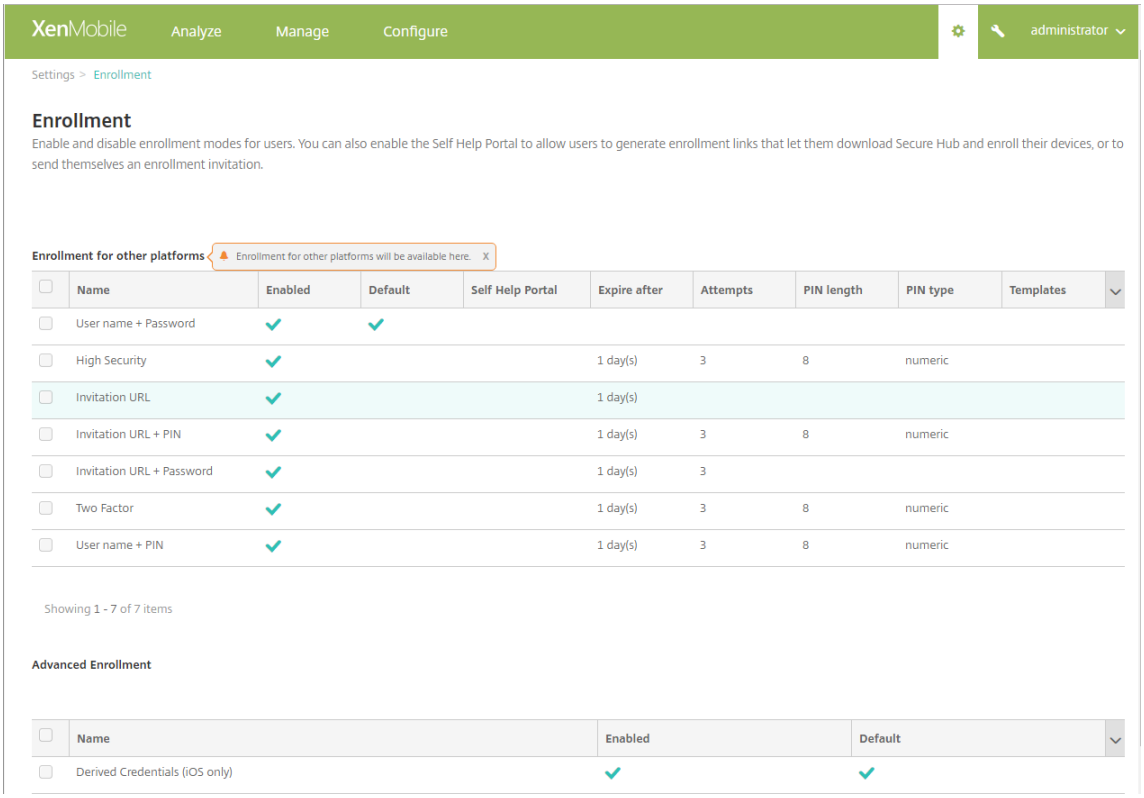
6. 次の設定を構成します。

- Citrix Derived Credentials Manager アプリの場合: ［ユーザー識別子のフィールド］ はサブジェクトの別名で、［ユーザー識別子の種類］ は **userPrincipalName** です。
- その他の派生資格情報プロバイダーの情報については、当該プロバイダーに連絡してください。

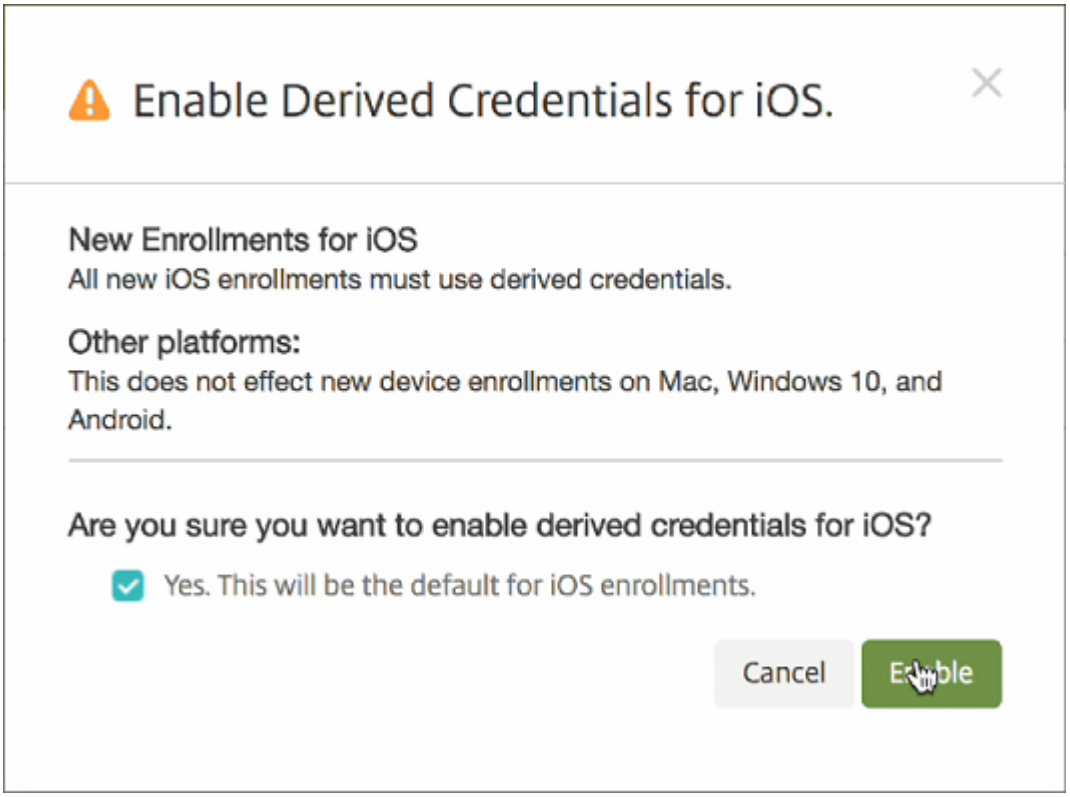
7. 証明書失効のチェックに OCSP レスポンダーを使用することもできます。セキュリティ上の理由から、OCSP レスポンダーを使用することをお勧めします。デフォルトでは、OCSP チェックはオフになっています。
   - CA 証明書の OCSP サポートをアクティブにする場合、［**OCSP** のカスタム **URL** を使用］のオプションを選択します。デフォルトでは、XenMobile は OCSP URL を証明書（［失効の証明書定義を使用］オプション）から抽出します。レスポンダー URL を指定するには、［カスタムを使用］ をクリックして URL を入力します。
   - レスポンダー **CA**: ［レスポンダー **CA**］ から証明書を選択します。または、［インポート］ をクリックし、次に ［証明書のインポート］ ダイアログボックスを使用して証明書を検索します。
8. ［保存］ をクリックします。［派生資格情報を有効にする］ ダイアログボックスが表示されます。



   - 派生資格情報構成を有効にするには、［保存］ をクリックします。派生資格情報を使用するには、登録設定も構成する必要があります。
   - 派生資格情報構成を有効にして、そのまま ［設定］ **>** ［登録］ に進むには、［保存して登録に移動］ をクリックします。
9. 派生資格情報を登録のために有効にするには、［設定］ **>** ［登録］ ページの ［詳細な登録］ の下にある 派生資格情報（**iOS** のみ)］ を選択して ［有効化］ をクリックします。



10. 確認ダイアログボックスが開きます。派生資格情報を有効にするには、チェックボックスを選択し、［有効化］をクリックします。



11. 派生資格情報登録のためにオプションを編集するには、［設定］**>**［登録］ の順に選択し、［派生資格情報 (**iOS** のみ)］ を選択して、［編集］ をクリックします。

派生資格情報を有効にした後: デバイス登録レポートで、［登録モード］ 列に **derived_credentials** が表示されます。

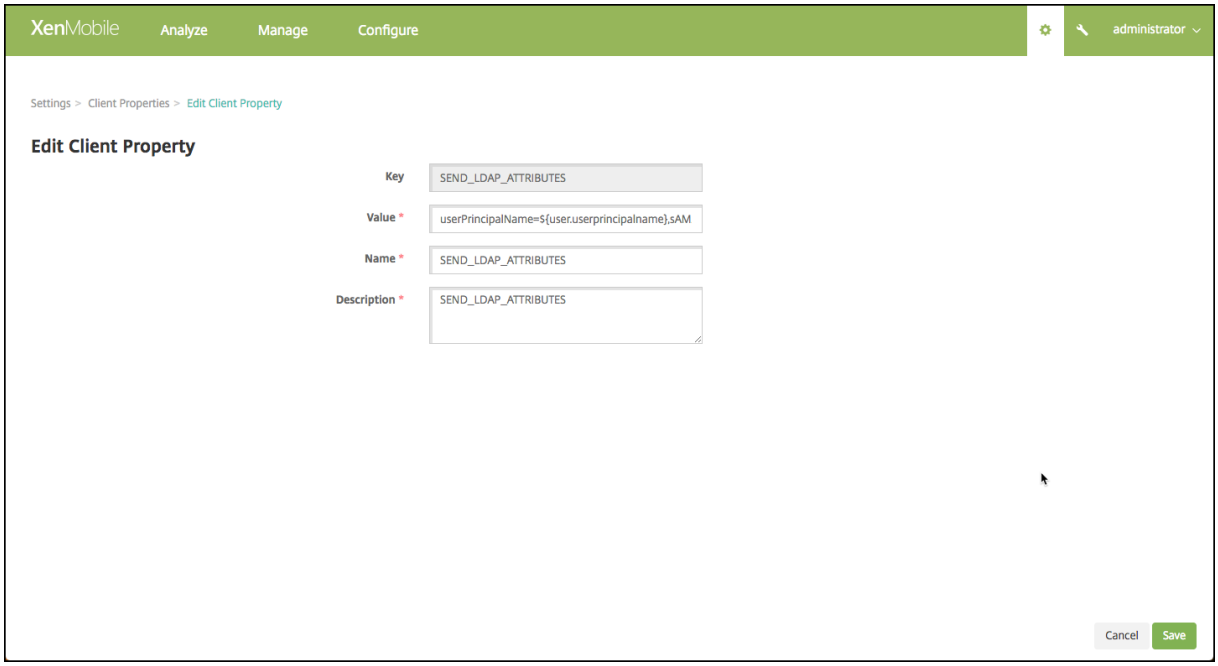
> 重要:
>
> 派生資格情報プロバイダーの追加後、XenMobile Server を再起動します。

Secure Mail 用に **XenMobile Server** を構成する

Secure Mail が派生資格情報で正しく動作するようにするには、LDAP 属性のクライアントプロパティを追加します。クライアントプロパティの追加について詳しくは、「クライアントプロパティ」を参照してください。

クライアントプロパティには、次の情報を使用します:

- キー: `SEND_LDAP_ATTRIBUTES`
- 値のデータ: `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

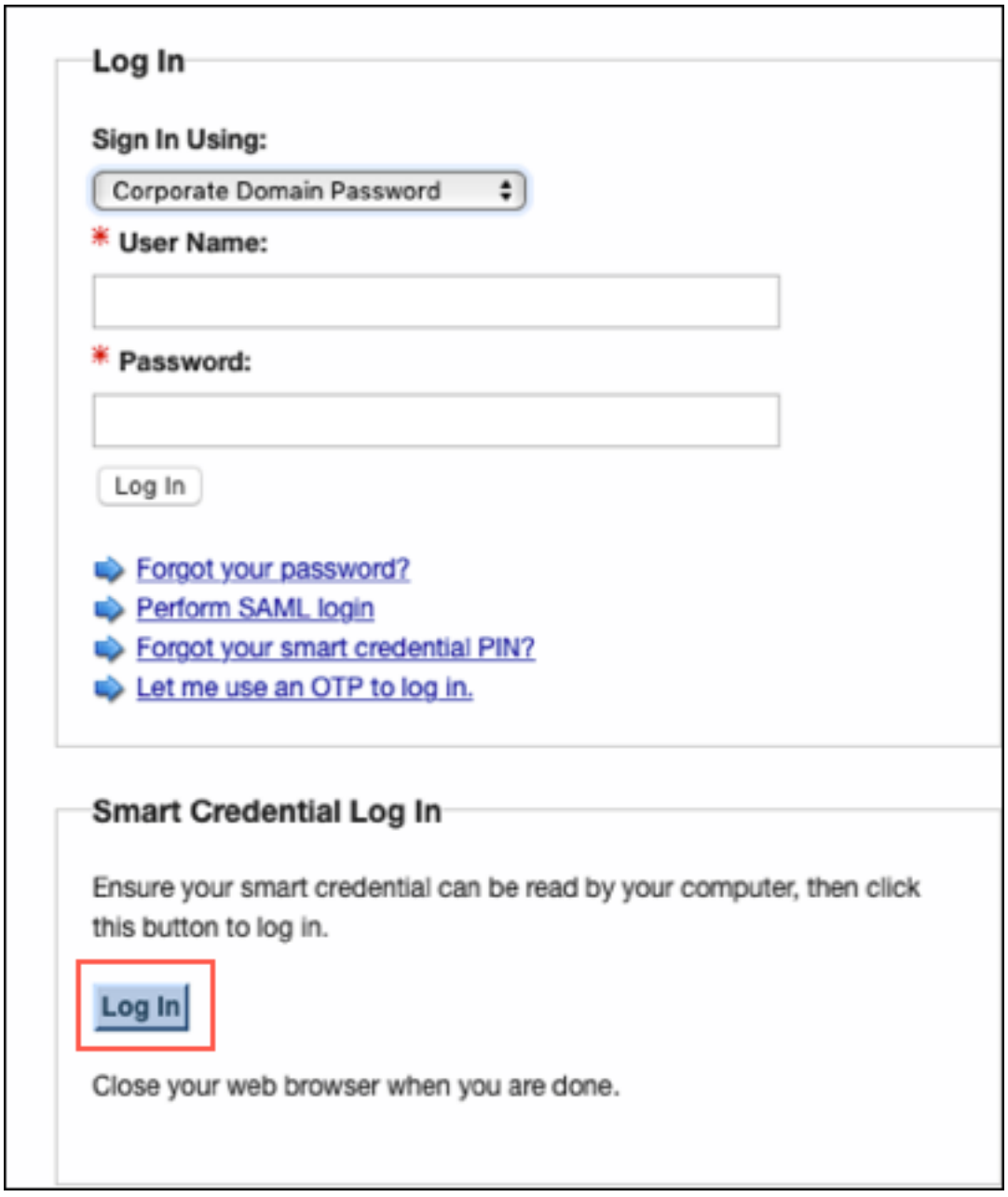


iOS デバイスで **Entrust Datacard** 資格情報をアクティブ化する

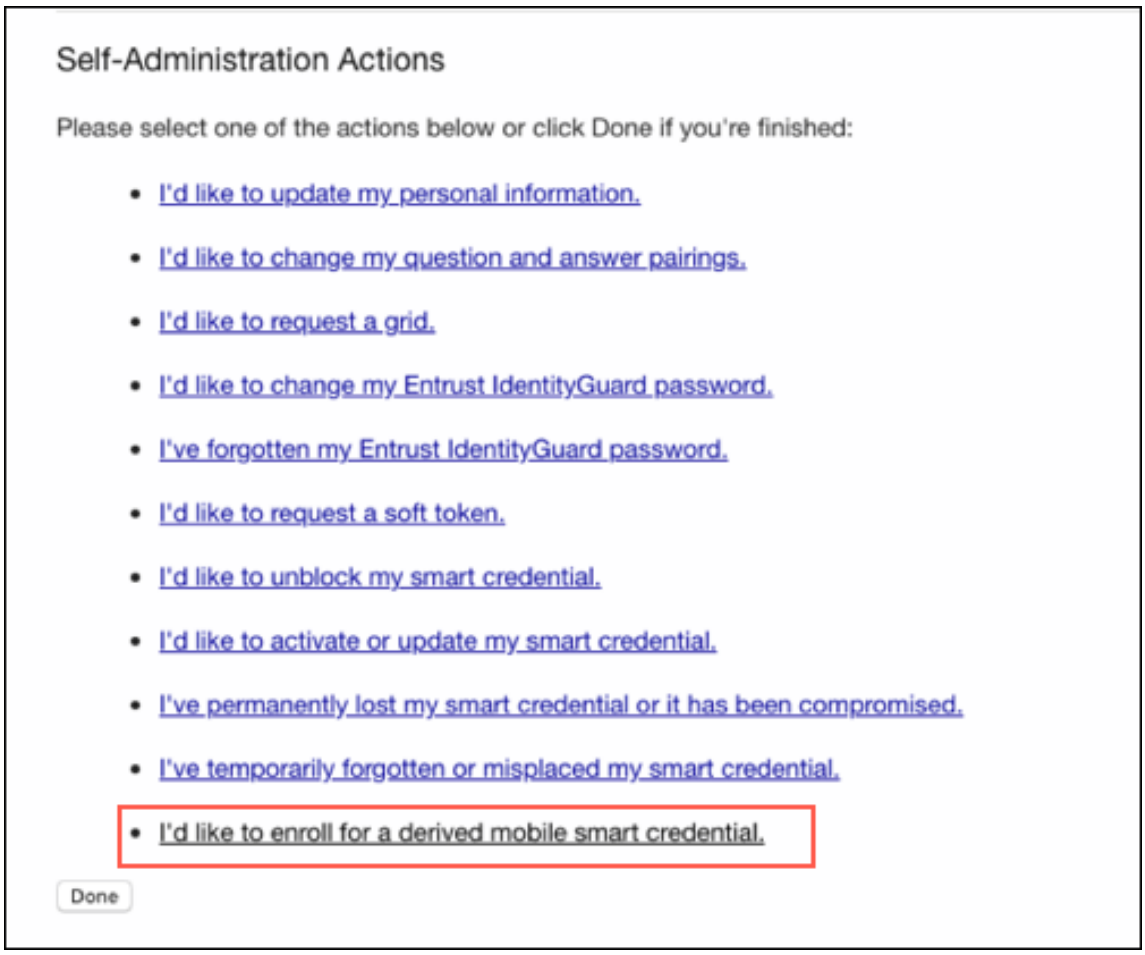
> 注:
>
> Entrust Web サイトを使用する場合:

- PIV カードをプログラミングするときに、Internet Explorer ブラウザーで Java を有効にしてください。
- PIV カードを変更するときには、ブラウザーキャッシュを消去してください。

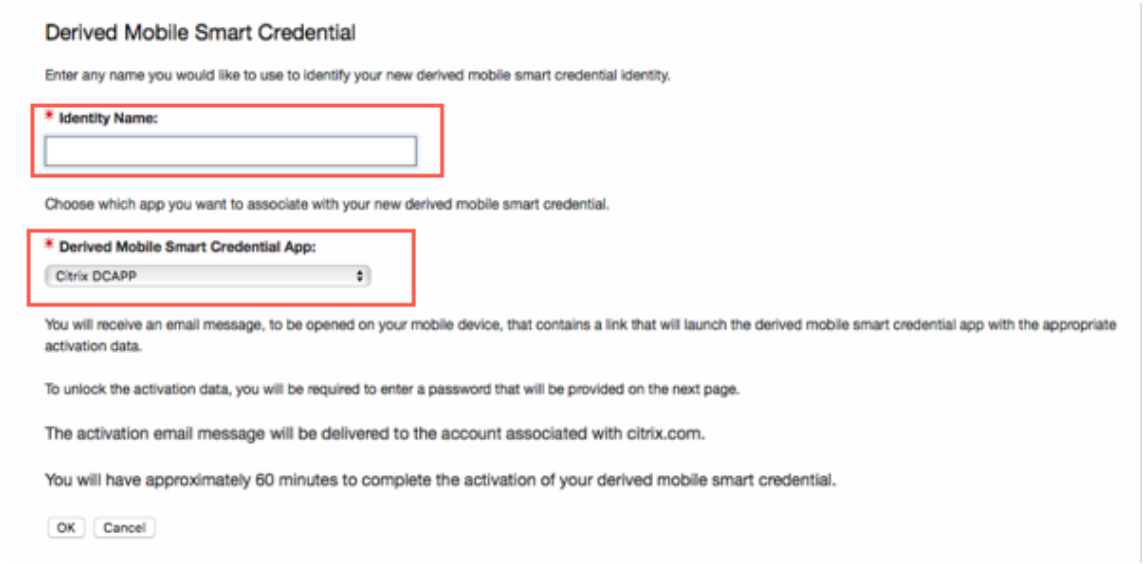
1. 新しいスマート資格情報を要求するには、デスクトップまたはデバイスを使用して Entrust サイトにログインします。ページ下部の **“Smart Credential Log In”** のボタンを使用してログインします。デスクトップに取り付けられたスマートカードリーダーにユーザーが各自のカードを挿入します。



2. **“Self-Administration Actions”** で **“I’d like to enroll for a derived mobile smart credential”** を選択し、**”Done”** をクリックします。



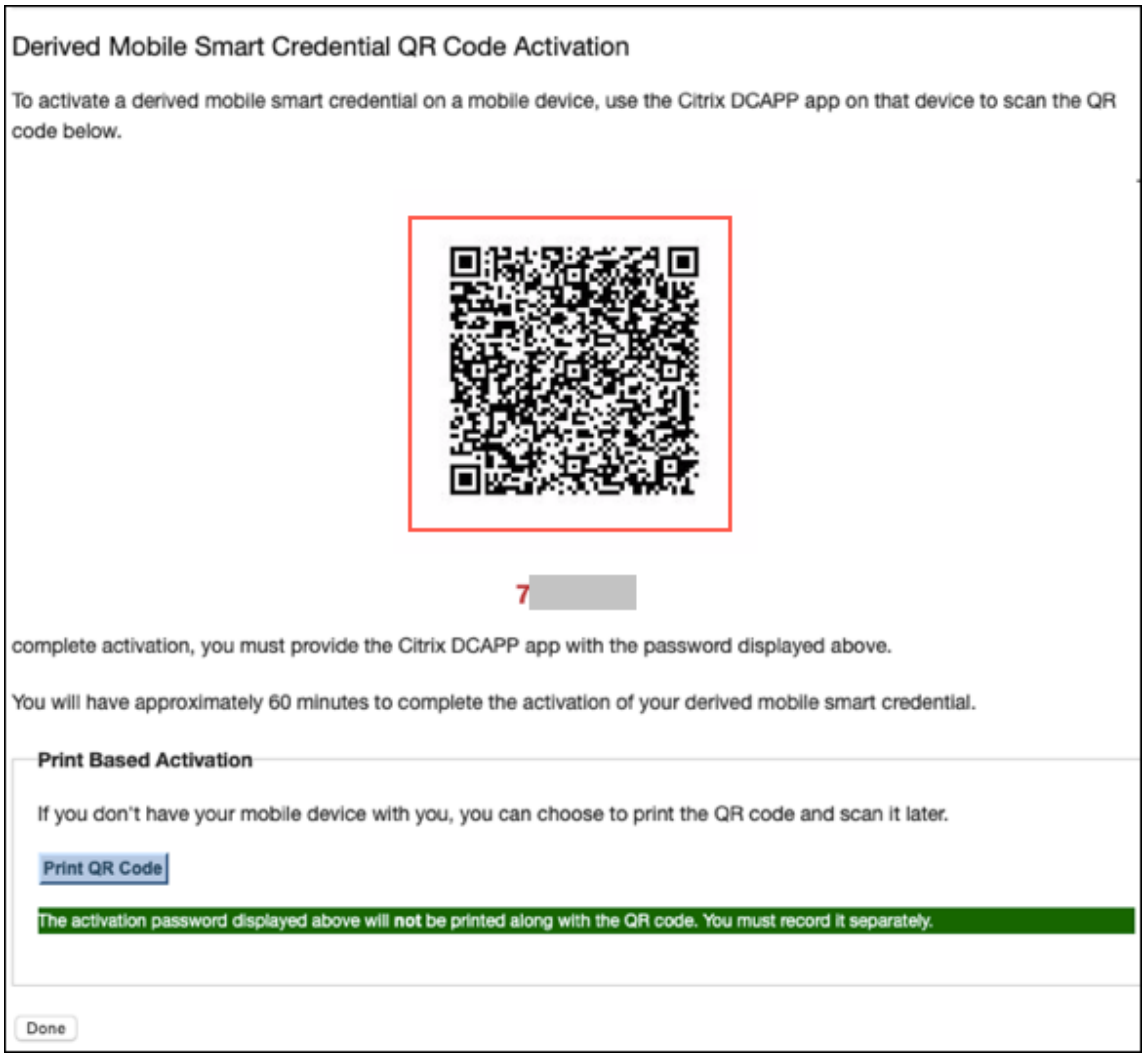
3. **“Derived Mobile Smart Credential”** 画面で、**“Identity Name”** を入力します。ユーザー名や ID 番号のような一意の名前を選択できます。
4. 派生資格情報アプリメニューで **Citrix DCAPP** を選択し、**“OK”** をクリックします。



QR コードのアクティブ化画面が開き、モバイルデバイスでコードをスキャンするよう求められます。

> 注:
>
> デフォルトで、派生資格情報の QR コードの有効期限は 3 分です。

5. デバイスの **Derived Credential Manager** アプリを使用して QR コードをスキャンし、アクティブ化を完了します。



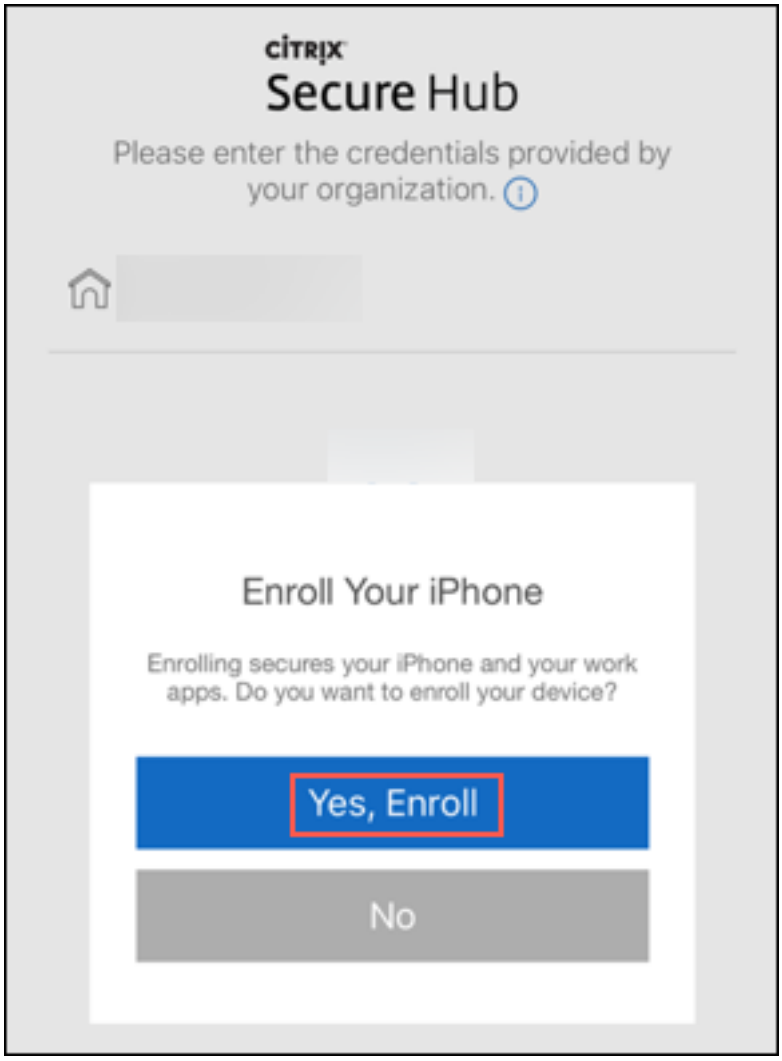
デバイス登録

前述のセットアップの完了後、ユーザーは派生資格情報でデバイスを登録できます。

> 注:
>
> このセクションのスクリーンショットでは、例として Entrust Datacard を使用しています。

1. タップして **Secure Hub** を開きます。プロンプトが表示されたら、XenMobile Server の完全修飾ドメイン名を入力して ［次へ］ をクリックします。

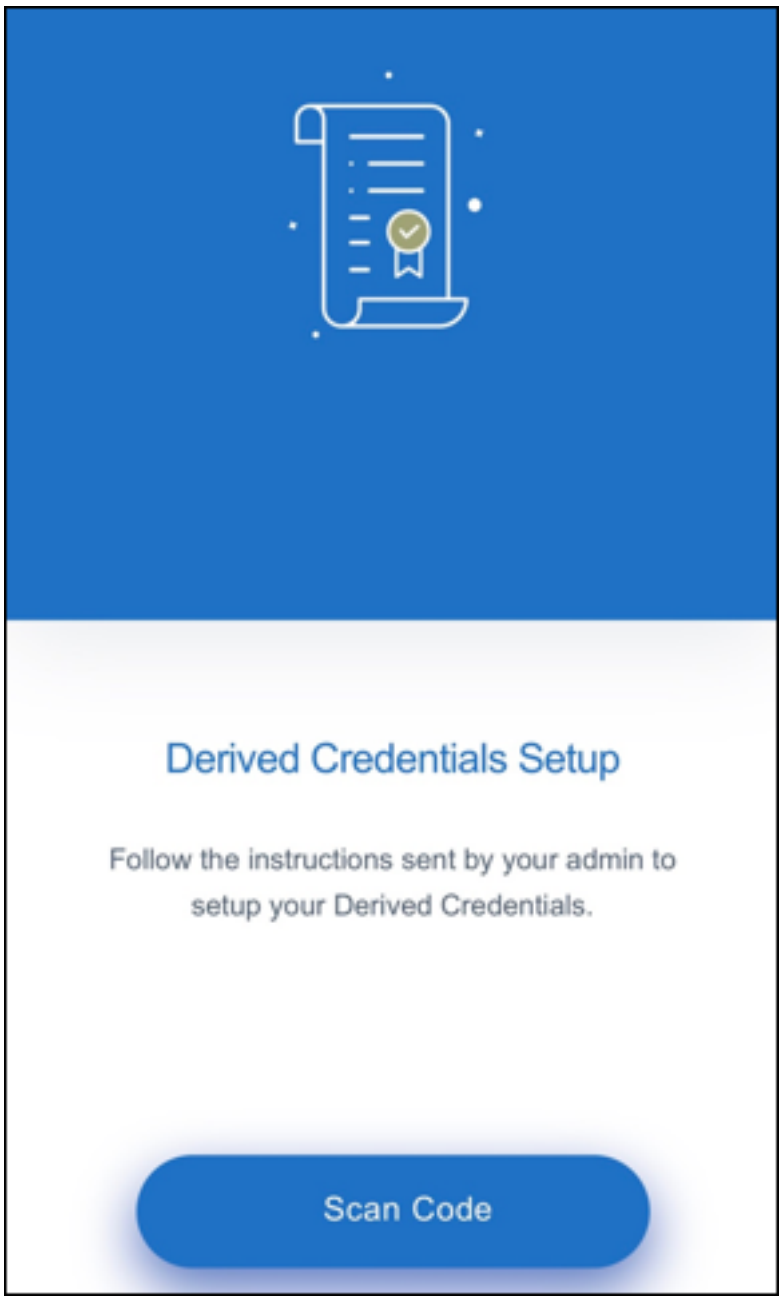
2. [はい、登録します] をクリックします。Secure Hub でデバイスの登録が開始されます。



XenMobile Server で派生資格情報がサポートされる場合、Secure Hub はユーザーに Citrix PIN の作成と確認を求めます。

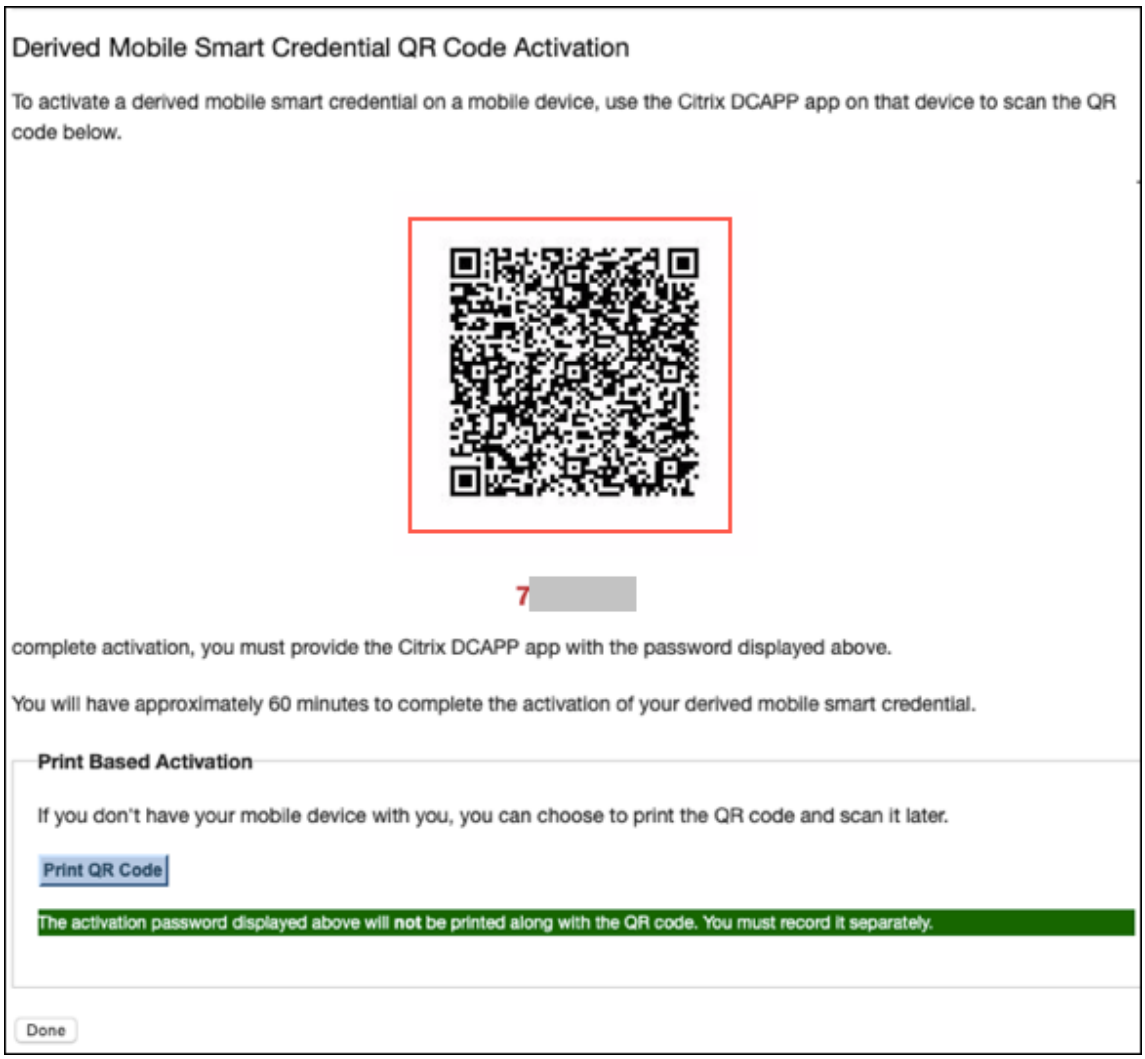
Citrix PIN の確認後、派生資格情報セットアップのスプラッシュ画面が開きます。指示に従ってスマート資格情報をアクティブ化します。

3. **“Scan code”** をタップします。携帯電話のカメラが起動します。

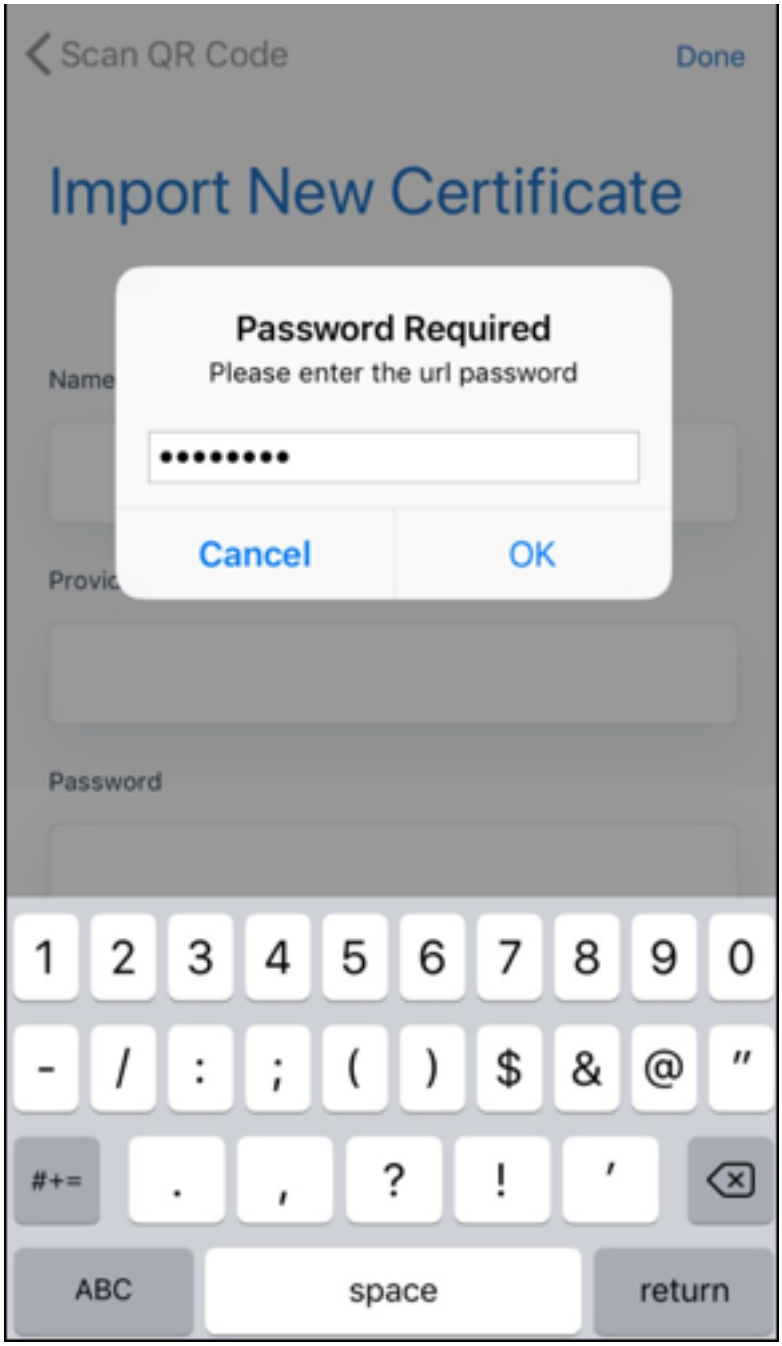


> 注:
>
> QR コードをスキャンするには、カメラとマイクが有効で、これらの機能を使用するために必要なアクセス権限があることを確認してください。

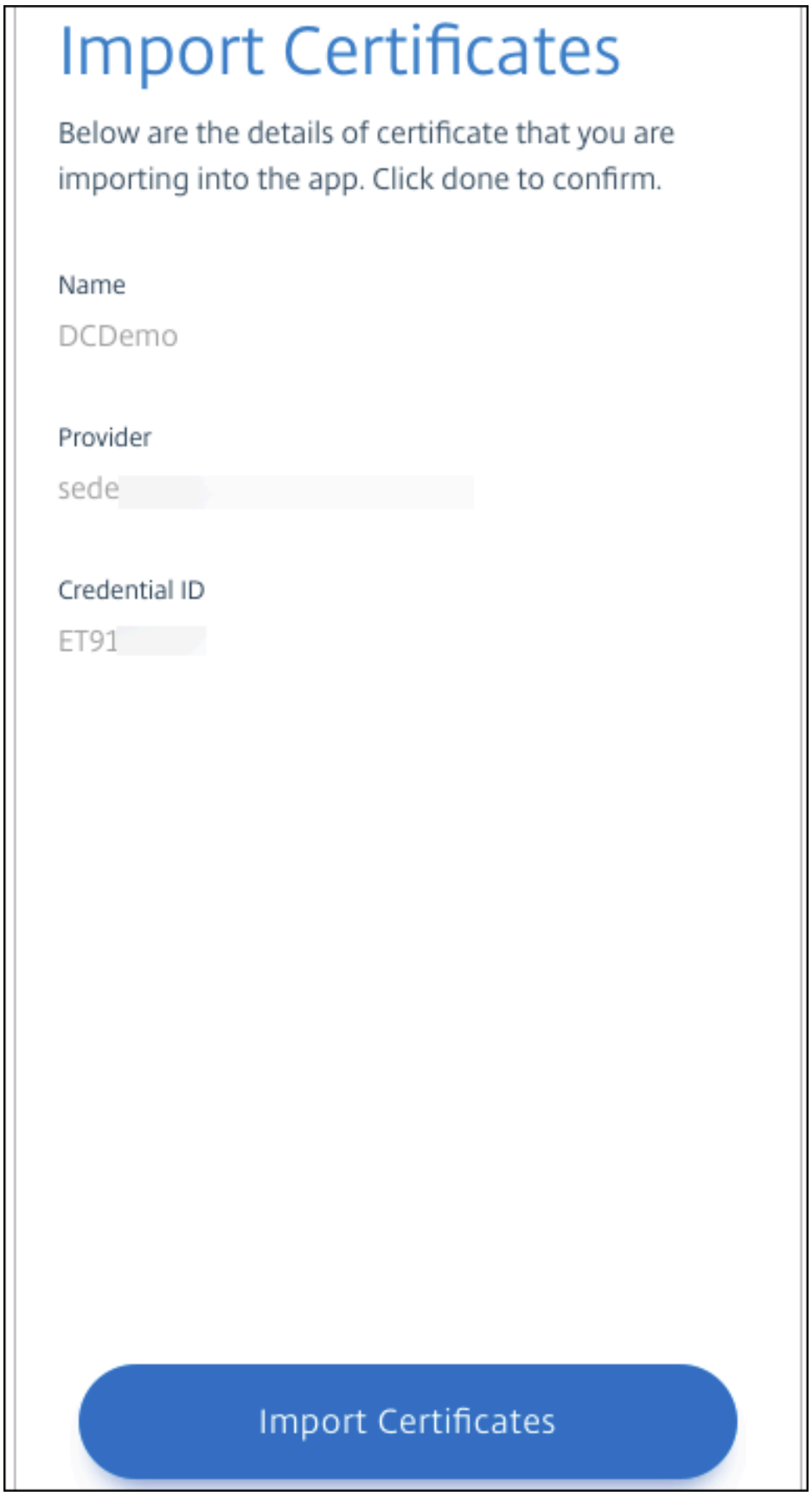
4. 派生資格情報アプリで、前述の手順で作成された QR コードをスキャンします。



5. QR コードのスキャン後、**“Import New Certificate”** 画面のパスワードダイアログボックスにパスワードを入力して **“OK”** をクリックします。



“Import New Certificate” 画面のフィールドが自動入力されます。



6. 証明書が追加された後、**“Derived Credentials”** 画面で **“Continue to Secure Hub”** をクリックします。

7. Secure Hub で、プロンプトが表示されたら新しい 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。

XenMobile コンソールでデバイス情報を表示するには

- ［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。

アップグレード

September 24, 2019

> ヒント: XenMobile Migration Service
>
> XenMobile Server をオンプレミスで使用している場合、XenMobile Migration Service によって Endpoint Management の使用を開始することができます。XenMobile Server から Citrix Endpoint Management への移行では、デバイスを再登録する必要はありません。
>
> 詳しくは、地域のシトリックス営業担当者、システムエンジニア、またはシトリックスパートナーにお問い合わせください。以下のブログで、XenMobile Migration Service について解説しています:
>
> New XenMobile Migration Service（英語）
>
> Making the Case for XenMobile in the Cloud（英語）

XenMobile 10.11 にアップグレードする前に

1. XenMobile Server 10.11 の最新バージョンにアップデートする前に、Citrix ライセンスサーバーを 11.15 以降にアップデートしてください。

   最新バージョンの XenMobile では、Citrix ライセンスサーバー 11.15 以降が必要です。

   XenMobile 10.11 のカスタマーサクセスサービスの日付（以前の Subscription Advantage の日付）は、2019 年 4 月 9 日です。Citrix ライセンスのカスタマーサクセスサービスの日付は、この日付より後である必要があります。日付は、ライセンスサーバーのライセンスの隣に表示されています。XenMobile の最新バージョンを古いライセンスサーバー環境に接続すると、接続チェックが失敗し、ライセンスサーバーを構成できません。

   ライセンスの日付を更新するには、Citrix ポータルから最新のライセンスファイルをダウンロードし、ライセンスサーバーにファイルをアップロードします。詳しくは、「カスタマーサクセスサービス」を参照してください。

2. クラスタ化された環境の場合：iOS 11 以降を実行するデバイスへの iOS ポリシーおよびアプリの展開には、次の要件があります。NetScaler Gateway が SSL 永続性に設定されている場合、すべての XenMobile Server ノードでポート 80 を開く必要があります。
3. アップグレードする XenMobile Server を実行する仮想マシンの RAM が 4GB 未満の場合、最低 4GB に RAM を増設してください。実稼働環境では、推奨される最小 RAM 容量は 8GB であることに留意願います。
4. 推奨事項：XenMobile の更新をインストールする前に、仮想マシンの機能を使用して、システムのスナップショットを取得してください。また、システム構成データベースもバックアップしてください。アップグレードで問題が発生した場合でも、完全なバックアップがあれば復元を行うことができます。

アップグレードするには

XenMobile 10.10.x または 10.9.x からは XenMobile 10.11 に直接アップグレードできます。アップグレードを実行するには、Citrix のダウンロードページで取得できる最新の 10.11 バイナリを使用します。アップグレードをアップロードするには、XenMobile コンソールで ［リリース管理］ ページを使用します。

リリース管理ページを使用してアップグレードする

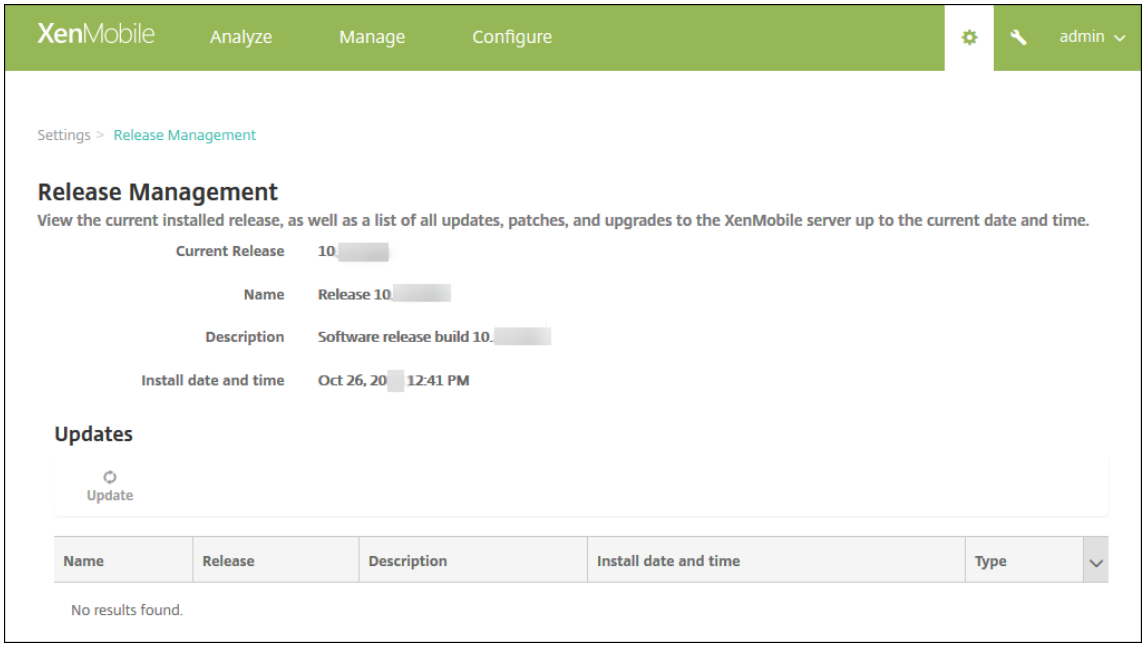
［**Release Management**］ ページを使用して、最新バージョンの XenMobile Server にアップグレードします。

前提条件：

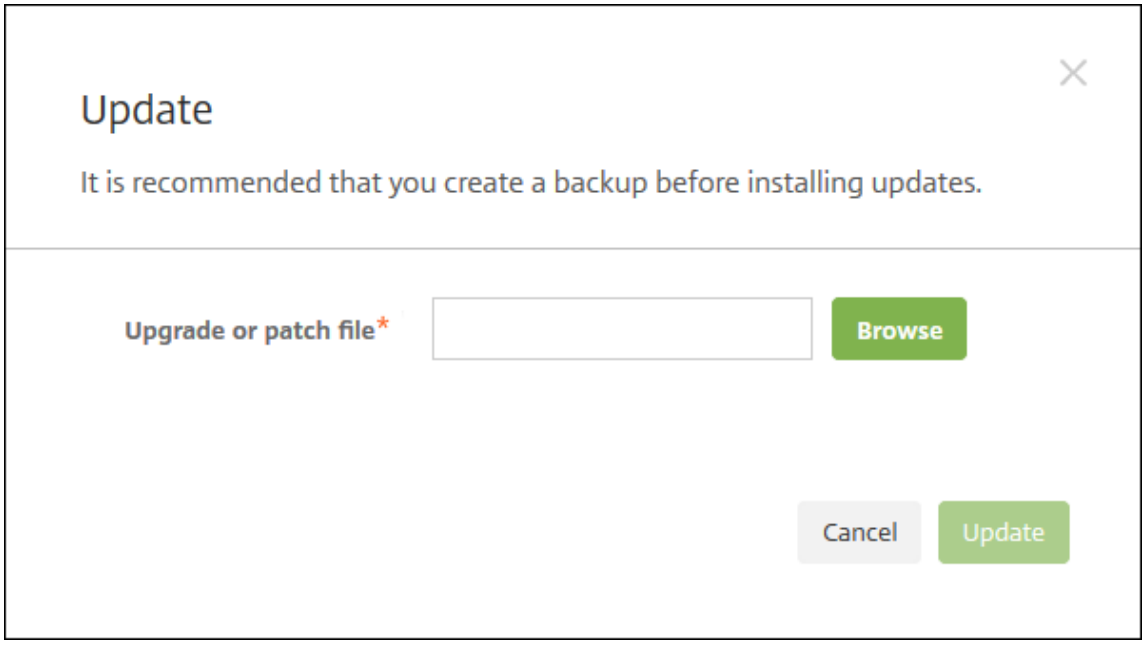
- 「システム要件」を確認してください。

クラスター展開の場合、このトピックの最後にある手順を参照してください。

1. Citrix Web サイトのアカウントにログオンし、ダウンロードページに移動します。XenMobile Upgrade（.bin）ファイルを適切な場所にダウンロードします。
2. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
3. ［リリース管理］ をクリックします。［リリース管理］ ページが表示されます。



4. [**Updates**] の下の [**Update**] をクリックします。[**Update**] ダイアログボックスが開きます。



5. [参照] をクリックして Citrix.com からダウンロードした XenMobile アップグレードファイルの場所に移動し、ファイルを選択します。

6. [**Update**] をクリックし、メッセージが表示されたら XenMobile を再起動します。

   何らかの理由で更新が正常に完了しなかった場合は、問題を示すエラーメッセージが表示されます。システムは更新を試行する前の状態に戻ります。

アップグレードした後

アップグレード後、XenMobile を再起動する必要があります。XenMobile CLI を使用して XenMobile Server を再起動してください。システムの再起動後にブラウザーのキャッシュを消去することが重要です。

接続の構成を変更していないのに送信接続に関連した機能が動作しなくなった場合は、XenMobile Server のログを調べて、「VPP サーバーに接続できません：ホスト名 192.0.2.0 はピアによって提供された証明書のサブジェクトと一致しません」のような内容のエラーが含まれていないかを確認します

証明書の検証エラーは、XenMobile Server でホスト名の認証を無効にする必要があることを示しています。デフォルトでは、Microsoft PKI サーバーを除く送信接続でホスト名の認証が有効です。ホスト名の認証によって展開が損なわれる場合は、サーバープロパティ **disable.hostname.verification** を **true** に変更します。このプロパティのデフォルト値は **false** です。

Citrix は、XenMobile の新しいバージョンまたは重要な更新を Citrix.com に公開しています。同時に、顧客ごとに記録された連絡先に通知が送信されます。

クラスター化された **XenMobile** 展開にアップグレードするには

> 重要：
>
> XenMobile の更新をインストールする前に、仮想マシン（VM）の機能を使用して、システムのスナップショットを取得してください。また、システム構成データベースもバックアップしてください。アップグレードで問題が発生した場合でも、完全なバックアップがあれば復元を行うことができます。

システムがクラスターモードで構成されている場合、以下の手順に従って XenMobile 10 リリースから各ノードを更新します。

1. ［**Settings**］＞［**Release Management**］ から、すべてのノードで.bin ファイルをアップロードします。
2. CLI で、［**System**］メニューのすべてのノードをシャットダウンします。
3. CLI で ［**System**］ メニューから 1 つのノードを起動し、サービスが実行されているか確認します。
4. 他のノードを 1 つずつ起動します。

   XenMobile が更新を完了できなかった場合は、問題を示すエラーメッセージが表示されます。XenMobile によってシステムは更新を試行する前の状態に戻ります。

XenMobile MDM Edition から **Enterprise Edition** へのアップグレード

iOS および Android デバイス用に、XenMobile MDM Edition を XenMobile Enterprise Edition にアップグレードすることができます。

前提条件

- 適切な Enterprise ライセンス
- NetScaler Gateway が構成済みであること

アップグレードするには

1. ［設定］**>**［ライセンス］ に移動し、Enterprise Edition の適切なライセンスの種類がアップロードされていることを確認します。
2. ［設定］**>**［サーバープロパティ］ に移動し、［**Server Mode**］ プロパティを ［**MDM**］ から ［**ENT**］ に変更します。
3. ［設定］**>**［**Netscaler Gateway**］ に移動し、NetScaler Gateway の詳細を構成します。認証モードを、MDM Edition のときと同じドメイン（Active Directory）認証に設定します。XenMobile では、ユーザー登録後の認証モードの変更をサポートしていません。
4. オプション：［設定］**>**［クライアントプロパティ］ に移動し、Citrix PIN 認証を有効にします。

上記の手順の完了後に、ユーザーがデバイスを Enterprise モードに切り替えるには、次の手順を実行する必要があります。

iOS ユーザー

1. Secure Hub を閉じる：デバイスのホームボタンを 2 回（すばやく）タップし、Secure Hub アプリケーションを表示します。
2. Secure Hub を開きます。

Android ユーザー

1. Secure Hub を開きます。
2. ［基本設定］**>**［デバイス情報］ に移動します。
3. ［ポリシーの更新］ をクリックします。

Citrix PIN 認証を有効にした場合、Secure Hub ではユーザーに PIN の作成を求めるメッセージが表示されます。ユーザーが PIN を作成すると、XenMobile はそのデバイスをエンタープライズモードで構成します。XenMobile コンソールの ［管理］**>**［デバイス］ ページに、MDM と MAM の両方がデバイスでアクティブになっていることが表示されます。

ユーザーアカウント、役割、および登録

January 10, 2020

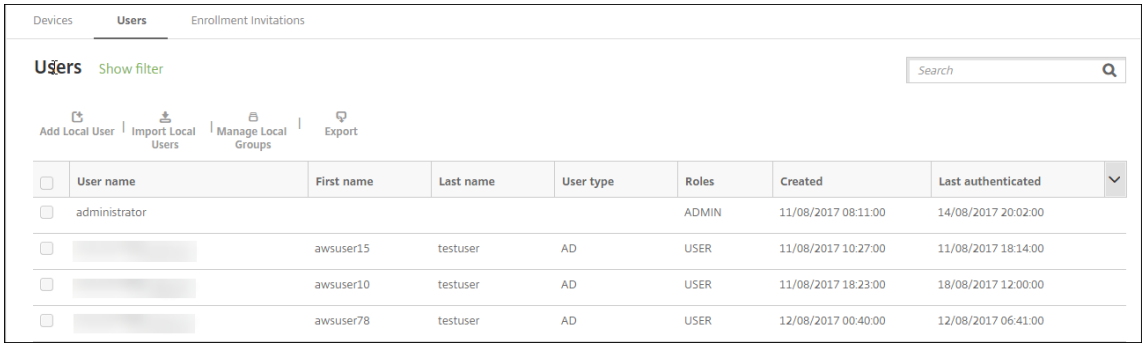
XenMobile コンソールの ［管理］ タブおよび ［設定］ ページで、ユーザーアカウント、役割、登録を構成します。別途記載されていない限り、ここでは以下のタスクの手順を説明します。

- ユーザーアカウントおよびグループ:
  - ［管理］ > ［ユーザー］ で、ユーザーアカウントを手動で追加するか、.csv プロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理します。
  - ［設定］ > ［ワークフロー］ で、ワークフローを使用して、ユーザーアカウントの作成および削除を管理します。
- ユーザーアカウントおよびグループの役割
  - ［設定］ > ［役割ベースのアクセス制御］ で、権限の定義済みセットである役割をユーザーとグループに割り当てます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。詳しくは、「RBAC を使用した役割の構成」を参照してください。
  - ［設定］ > ［通知テンプレート］ で通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Secure Hub、SMTP、SMS の 3 つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。詳しくは、「通知テンプレートの作成および更新」を参照してください。
- 登録モードおよび招待状
  - ［設定］ > ［登録］ で、最大 7 つの登録モードの構成と登録招待の送信を行います。各登録モードに独自のセキュリティレベルと、ユーザーがデバイス登録時に実行する必要のある手順を設定します。
  - XenMobile でのユーザー登録の自動検出を有効にする

ローカルユーザーアカウントを追加、編集、または削除するには

ローカルユーザーアカウントを XenMobile に手動で追加したり、プロビジョニングファイルを使用してアカウントをインポートしたりすることができます。プロビジョニングファイルからユーザーをインポートする手順については、「ユーザーアカウントのインポート」を参照してください。

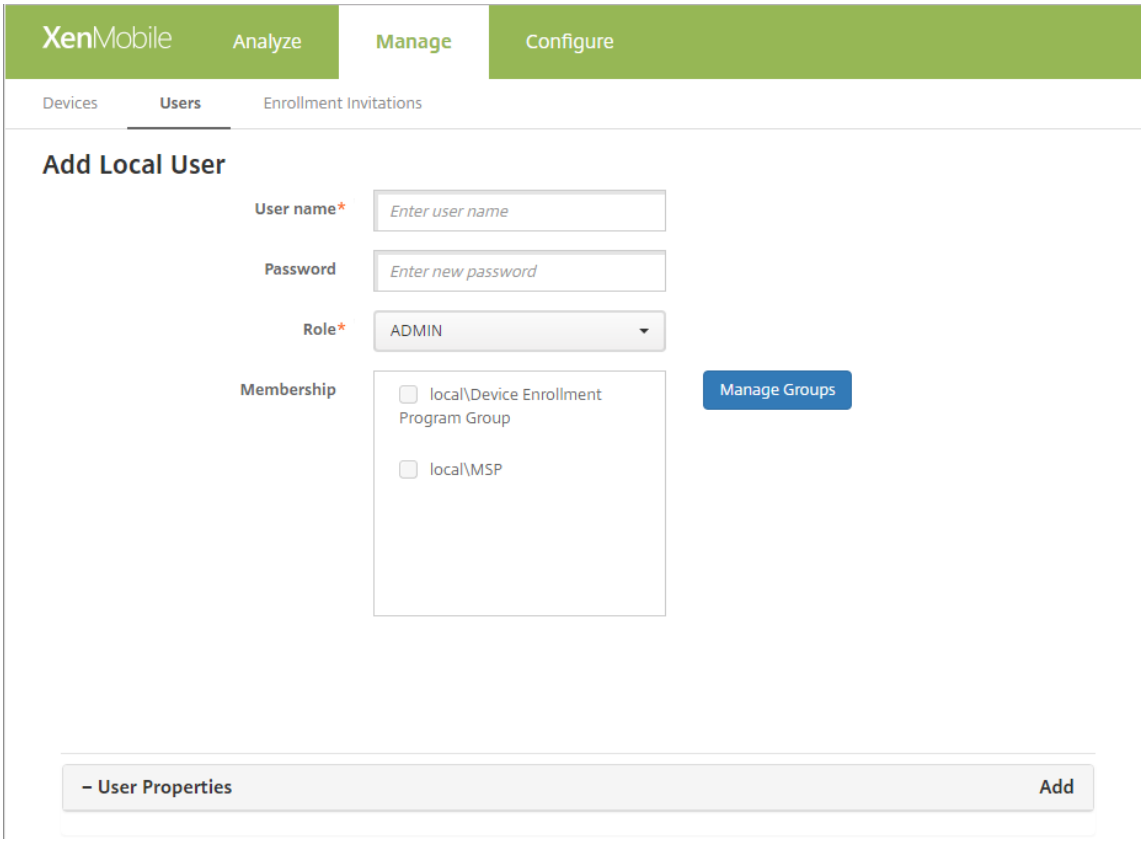
1. XenMobile コンソールで、 ［管理］ > ［ユーザー］ の順にクリックします。 ［ユーザー］ ページが開きます。



2. ［フィルターを表示］ をクリックして一覧をフィルターします。

ローカルユーザーアカウントを追加するには

1. ［ユーザー］ ページで、［ローカルユーザーの追加］ をクリックします。［ローカルユーザーの追加］ ページが開きます。



2. 次の設定を構成します。

   - ユーザー名： 名前を入力します。このフィールドは必須です。名前にはスペースや大文字、小文字を含めることができます。
   - パスワード： 任意で、ユーザーのパスワードを入力します。
   - 役割： 一覧から、ユーザーの役割を選択します。役割について詳しくは、「RBAC を使用した役割の構成」を参照してください。選択できるオプションは以下のとおりです：
     - ADMIN
     - DEVICE_PROVISIONING
     - SUPPORT
     - USER
   - メンバーシップ： 一覧から、ユーザーを追加するグループを選択します。
   - ユーザープロパティ： 任意でユーザープロパティを追加します。追加するユーザープロパティごとに、［追加］ をクリックして以下の操作を行います。
     - ユーザープロパティ： 一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。

– ［完了］ をクリックしてユーザープロパティを保存するか、［キャンセル］ をクリックします。

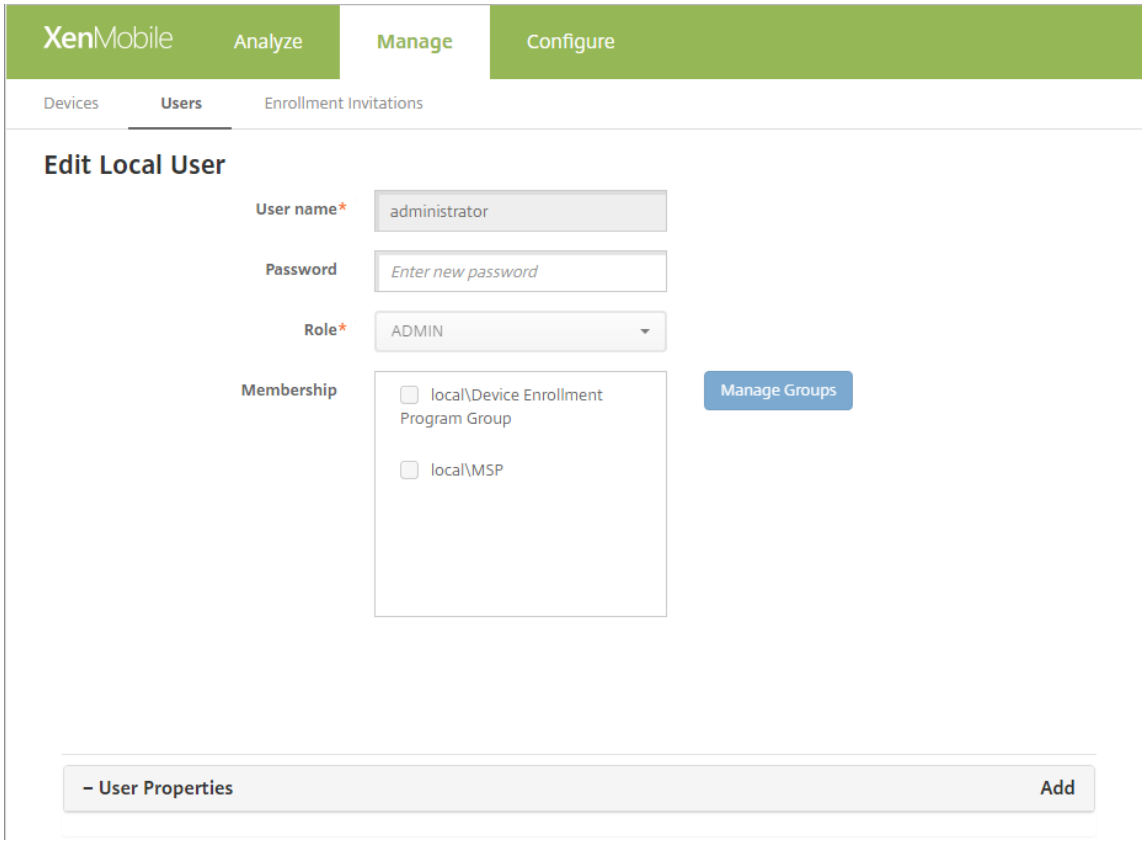
既存のユーザープロパティを削除するには、プロパティが含まれる行の上にマウスポインターを置き、右側の［X］をクリックします。プロパティがすぐに削除されます。

既存のユーザープロパティを編集するには、プロパティを選択して変更を加えます。［完了］ をクリックして変更した項目を保存するか、［キャンセル］ をクリックして項目を変更せずそのままにします。

3. ［保存］ をクリックします。

ローカルユーザーアカウントを編集するには

1. ［ユーザー］ ページのユーザー一覧で、ユーザーをクリックして選択してから ［編集］ をクリックします。［ローカルユーザーの編集］ ページが開きます。



2. 必要に応じて以下の情報を変更します。

- ユーザー名： ユーザー名は変更できません。
- パスワード： ユーザーパスワードを変更または追加します。
- 役割： 一覧から、ユーザーの役割を選択します。
- メンバーシップ： 一覧から、ユーザーアカウントを追加または編集するグループを選択します。ユーザーアカウントをグループから削除するには、グループ名の横にあるチェックボックスをオフにします。
- ユーザープロパティ： 次のいずれかを行います：

- 変更するユーザープロパティごとに、プロパティを選択して変更を加えます。［完了］ をクリックして変更した項目を保存するか、［キャンセル］ をクリックして項目を変更せずそのままにします。
- 追加するユーザープロパティごとに、［追加］ をクリックして以下の操作を行います:
  * ユーザープロパティ: 一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
  * ［完了］ をクリックしてユーザープロパティを保存するか、［キャンセル］ をクリックします。
- 削除する既存のユーザープロパティごとに、プロパティが含まれる行の上にマウスポインターを置き、右側の ［**X**］ をクリックします。プロパティがすぐに削除されます。

3. ［保存］ をクリックして変更を保存するか、［キャンセル］ をクリックしてユーザーを変更せずそのままにします。

ローカルユーザーアカウントを削除するには

1. ［ユーザー］ ページのユーザーアカウント一覧で、ユーザーアカウントをクリックして選択します。

各ユーザーアカウントの横のチェックボックスをオンにして、削除するユーザーアカウントを複数選択できます。

1. ［削除］ をクリックします。確認ダイアログボックスが開きます。
2. ［削除］ をクリックしてユーザーアカウントを削除するか、［キャンセル］ をクリックします。

Active Directory ユーザーを削除するには

一度に 1 人または複数の Active Directory ユーザーを削除するには、該当するユーザーを選択して ［削除］ をクリックします。

削除したユーザーがデバイスを登録していて、これらのデバイスを再登録する必要がある場合、再登録前に対象のデバイスを削除してください。デバイスを削除するには、［管理］ **>** ［デバイス］ の順に選択し、対象のデバイスを選択して ［削除］ をクリックします。

ユーザーアカウントのインポート

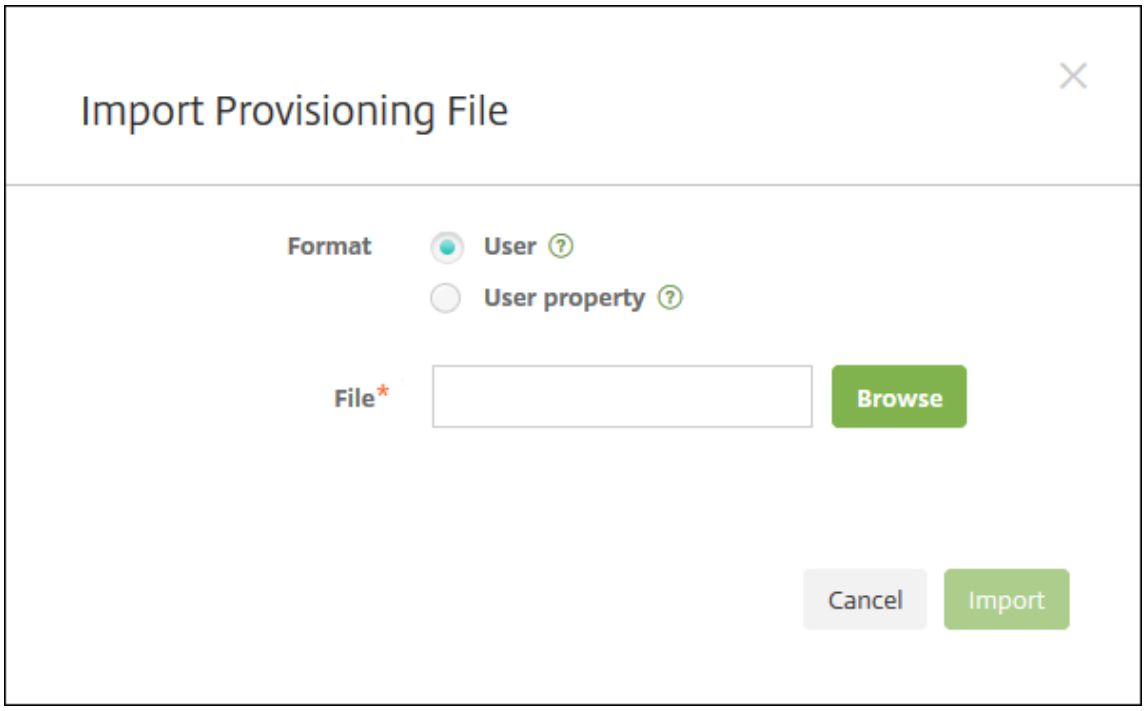
ローカルユーザーアカウントやプロパティを、プロビジョニングファイルと呼ばれる.csv ファイルからインポートできます。このファイルは手動で作成できます。プロビジョニングファイルの形式について詳しくは、「プロビジョニングファイル形式」を参照してください。

> 注:
>
> - ローカルユーザーの場合は、インポートファイル内のユーザー名とともにドメイン名を使用します。たとえば、username@domain のように指定します。作成またはインポートしたローカルユーザーが XenMobile の管理対象ドメイン用である場合、このユーザーは対応する LDAP 資格情報を使って登録することはできません。

> - XenMobile の内部ユーザーディレクトリにユーザーアカウントをインポートする場合は、インポートプロセスの速度を上げるため、デフォルトのドメインを無効にします。ドメインの無効化によって登録が影響を受けることがあります。そのため、内部ユーザーのインポートを完了した後、デフォルトのドメインを再度有効にする必要があります。
> - ローカルユーザーはユーザープリンシパル名（UPN：User Principal Name）形式で指定できます。ただし、管理対象ドメインは使用しないことをお勧めします。たとえば、example.com が管理対象である場合、「user@example.com」という UPN 形式のローカルユーザーは作成しないでください。

プロビジョニングファイルを準備した後、以下の手順に従ってファイルを XenMobile にインポートします。

1. XenMobile コンソールで、［管理］**>**［ユーザー］ の順にクリックします。［ユーザー］ ページが開きます。
2. ［ローカルユーザーのインポート］ をクリックします。［プロビジョニングファイルのインポート］ ダイアログボックスが開きます。



3. インポートするプロビジョニングファイルの形式として、［ユーザー］ または ［プロパティ］ を選択します。
4. ［参照］ をクリックして使用するプロビジョニングファイルの場所へ移動し、そのファイルを選択します。
5. ［インポート］ をクリックします。

プロビジョニングファイル形式

手動で作成し、XenMobile へのユーザーアカウントとプロパティのインポートに使用するプロビジョニングファイルは、次のいずれかの形式である必要があります。

- ユーザープロビジョニングファイルのフィールド： user;password;role;group1;group2

- ユーザー属性プロビジョニングファイルのフィールド: user;propertyName1;propertyValue1;propertyName2;prope

> 注:
>
> - プロビジョニングファイル内のフィールドはセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。たとえば、プロパティ **propertyV;test;1;2** は、プロビジョニングファイルでは「**propertyV\;test\;1\;2**」と入力します。
> - 役割として有効な値は、定義済みの役割である USER、ADMIN、SUPPORT、DEVICE_PROVISIONING のほか、ユーザーが定義した役割です。
> - グループの階層構造を作成するための区切り文字としてピリオド（.）を使用します。グループ名にピリオドは使用しないでください。
> - 属性プロビジョニングファイル内のプロパティ属性には小文字を使用してください。データベースの大文字と小文字は区別されます。

ユーザープロビジョニングファイルの内容例

エントリ「`user01;pwd\\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01`」の意味:

- ユーザー: user01
- パスワード: pwd;01
- 役割: USER
- **Groups**:
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

別の例「`AUser0;1.password;USER;ActiveDirectory.test.net`」の意味:

- ユーザー: AUser0
- パスワード: 1.password
- 役割: USER
- グループ: ActiveDirectory.test.net

ユーザー属性プロビジョニングファイルの内容例

エントリ「`user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value`」の意味:

- ユーザー: user01
- プロパティ **1**:
  - 名前: propertyN
  - 値: propertyV;test;1;2
- プロパティ **2**:

- 名前： prop 2
- 値： prop2 value

登録モードを構成するには

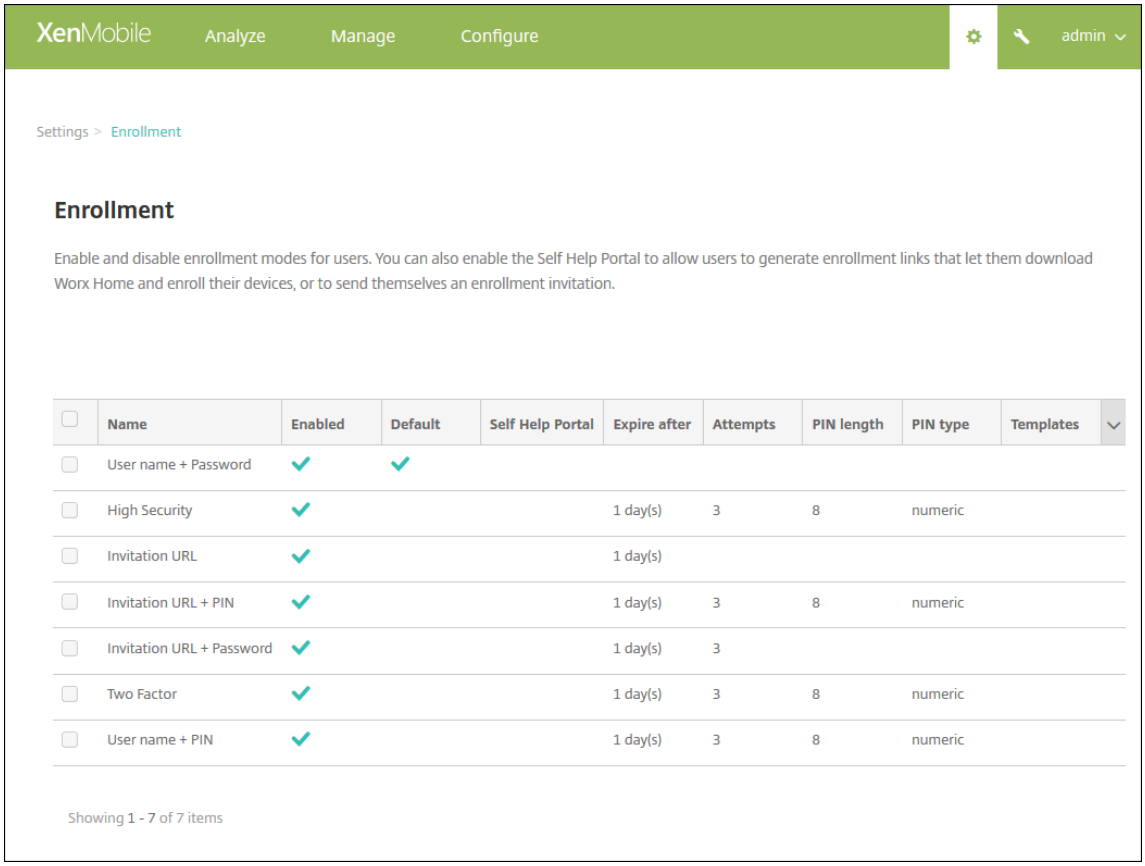
デバイス登録モードを構成して、ユーザーがデバイスを XenMobile に登録できるようにします。XenMobile には 7 つのモードがあり、それぞれに独自のセキュリティレベルと、ユーザーがデバイスを登録するときに行う必要がある手順があります。一部のモードは Self Help Portal で使用可能にすることができます。ユーザーはこのポータルにログオンして、デバイスを登録できる登録リンクを生成したり、登録招待状を自分に送信したりすることができます。登録モードの構成は、XenMobile コンソールの ［設定］**>**［登録］ ページから行います。

登録招待の送信は、［管理］**>**［登録招待］ ページから行います。詳しくは、「登録招待の送信」を参照してください。

> 注:
>
> カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［登録］ をクリックします。［登録］ ページが開き、すべての使用可能な登録モードの表が表示されます。デフォルトでは、すべての登録モードが有効です。
3. 一覧から登録モードを選択して編集します。編集が完了したら、編集後のモードをデフォルトとして設定するか、無効にするか、またはユーザーが Self Help Portal からアクセスできるようにします。

   > 注:
   >
   > 登録モードの横のチェックボックスを選択すると、登録モード一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。



次の登録モードから選択します。

- ユーザー名およびパスワード
- 高セキュリティ
- 招待 URL
- 招待 URL および PIN
- 招待 URL およびパスワード
- 2 要素
- ユーザー名および PIN

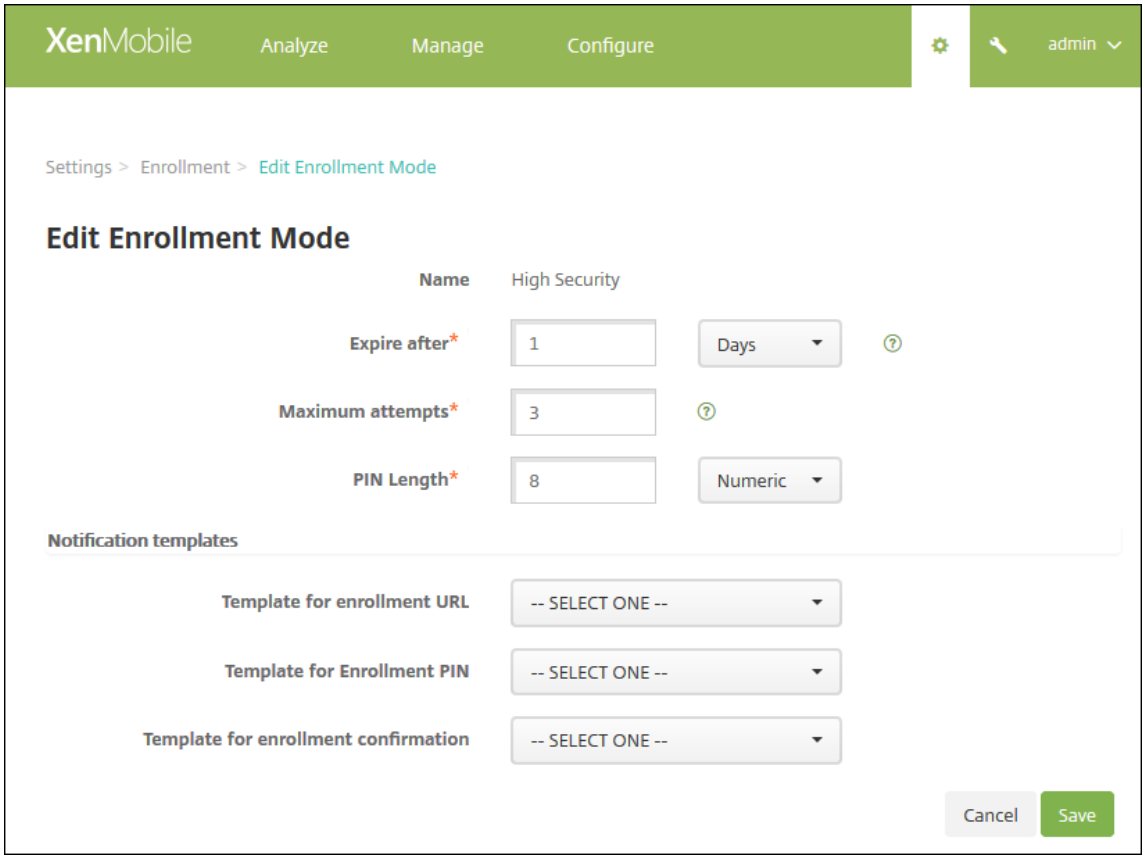
登録招待状を使用すると、招待状を持つユーザーだけが登録できるように制限できます。

ワンタイム PIN（OTP：One-Time PIN）登録招待状は、2 段階認証として使用できます。OTP 登録招待状では、ユーザーが登録可能なデバイスの数を制限できます。

環境のセキュリティ要件が非常に厳しい場合は、SN、UD、または EMEI を使用して登録招待状とデバイスを関連付けることができます。Active Directory のパスワードと OTP を求める 2 段階オプションも用意されています。

登録モードを編集するには

1. ［登録］ の一覧で登録モードを選択し、 ［編集］ をクリックします。 ［登録モードの編集］ ページが開きます。選択したモードによって、異なるオプションが表示される場合があります。



2. 必要に応じて以下の情報を変更します。

   - 有効期限： ユーザーがデバイスを登録できなくなる、有効期限を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。

     招待の有効期限が切れないようにするには **0** を入力します。

   - 日：一覧から、［有効期限］ボックスに入力した有効期限に応じて、［日］ または ［時間］ を選択します。
   - 最大試行数： 登録処理からロックアウトされるまでにユーザーが実行できる登録の試行回数を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。

     無制限に試行できるようにするには **0** を入力します。

   - **PIN** 長： 生成される PIN の長さを設定する数字を入力します。
   - 数字： 一覧から、PIN の種類として、 ［数字］ または ［英数字］ を選択します。
   - 通知テンプレート：

     – 登録 **URL** 用テンプレート： 一覧から、登録 URL に使用するテンプレートを選択します。たとえば、登録招待テンプレートでは、ユーザーにメールまたは SMS が送信されます。通知方法は、

XenMobile へのデバイスの登録に使用するテンプレートの構成内容によって決まります。通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

- 登録 **PIN** 用テンプレート: 一覧から、登録 PIN に使用するテンプレートを選択します。
- 登録確認用テンプレート: 一覧から、登録が成功したことをユーザーに通知するときに使用するテンプレートを選択します。

3. [保存] をクリックします。

登録モードをデフォルトとして設定するには

登録モードをデフォルトとして設定すると、別の登録モードを選択しない限り、そのモードがすべてのデバイス登録要求に対して使用されます。デフォルトとして設定されている登録モードがない場合は、デバイス登録ごとに登録の要求を作成する必要があります。

> 注:
>
> デフォルトの登録モードとして使用できるのは、[ユーザー名およびパスワード]、[**2** 要素]、[ユーザー名および **PIN**] のいずれかのみです。

1. [ユーザー名およびパスワード]、[**2** 要素]、[ユーザー名および **PIN**] のいずれかをデフォルトの登録モードとして設定します。

   モードをデフォルトとして使用するには、まずそのモードを有効化する必要があります。

2. [デフォルト] をクリックします。これにより、選択したモードがデフォルトになります。ほかの登録モードがデフォルトとして設定されていた場合、そのモードはデフォルトでなくなります。

登録モードを無効化するには

登録モードを無効化すると、その登録モードは、グループ登録招待状でも Self Help Portal でも使用できなくなります。ある登録モードを無効化して別の登録モードを有効化することで、ユーザーがデバイスを登録できる方法を変更できます。

1. 登録モードを選択します。

   デフォルトの登録モードは無効化できません。デフォルトの登録モードを無効化するには、登録モードのデフォルト状態をまず解除する必要があります。

2. [無効化] をクリックします。登録モードが有効でなくなります。

Self Help Portal で登録モードを有効化するには

Self Help Portal で登録モードを有効化すると、ユーザーが個別にデバイスを XenMobile に登録できます。

> 注：
>
> - Self Help Portal で登録モードを使用できるようにするには、登録が有効化され、通知テンプレートにバインドされている必要があります。
> - Self Help Portal では、登録モードを一度に 1 つのみ有効化できます。

1. 登録モードを選択します。
2. [**Self Help Portal**] をクリックします。選択した登録モードを Self Help Portal でユーザーが使用できるようになります。Self Help Portal で既に有効化されていたモードがあった場合、ユーザーはそれを使用できなくなります。

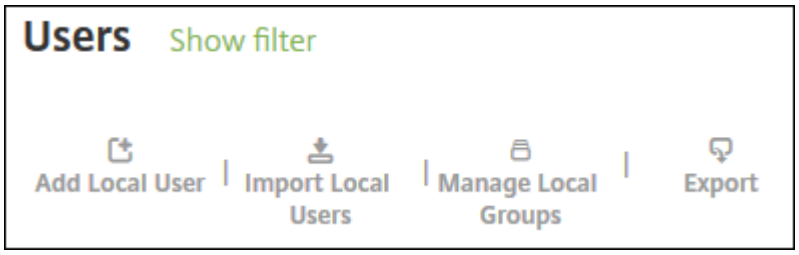
グループの追加または削除

グループの管理は、XenMobile コンソールの ［グループ管理］ ダイアログボックスで行います。このダイアログボックスは、［ユーザー］ ページ、［ローカルユーザーの追加］ ページ、または ［ローカルユーザーの編集］ ページからアクセスできます。グループ編集コマンドはありません。

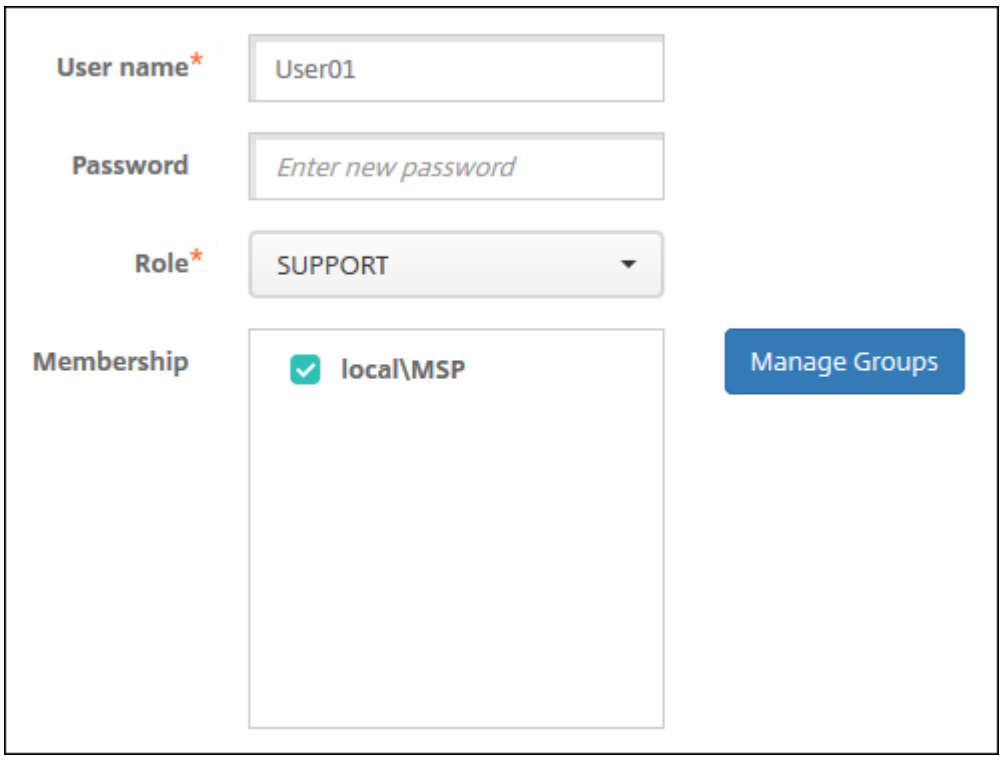
グループを削除する場合、グループを削除してもユーザーアカウントには影響しない点に注意してください。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

ローカルグループを追加するには

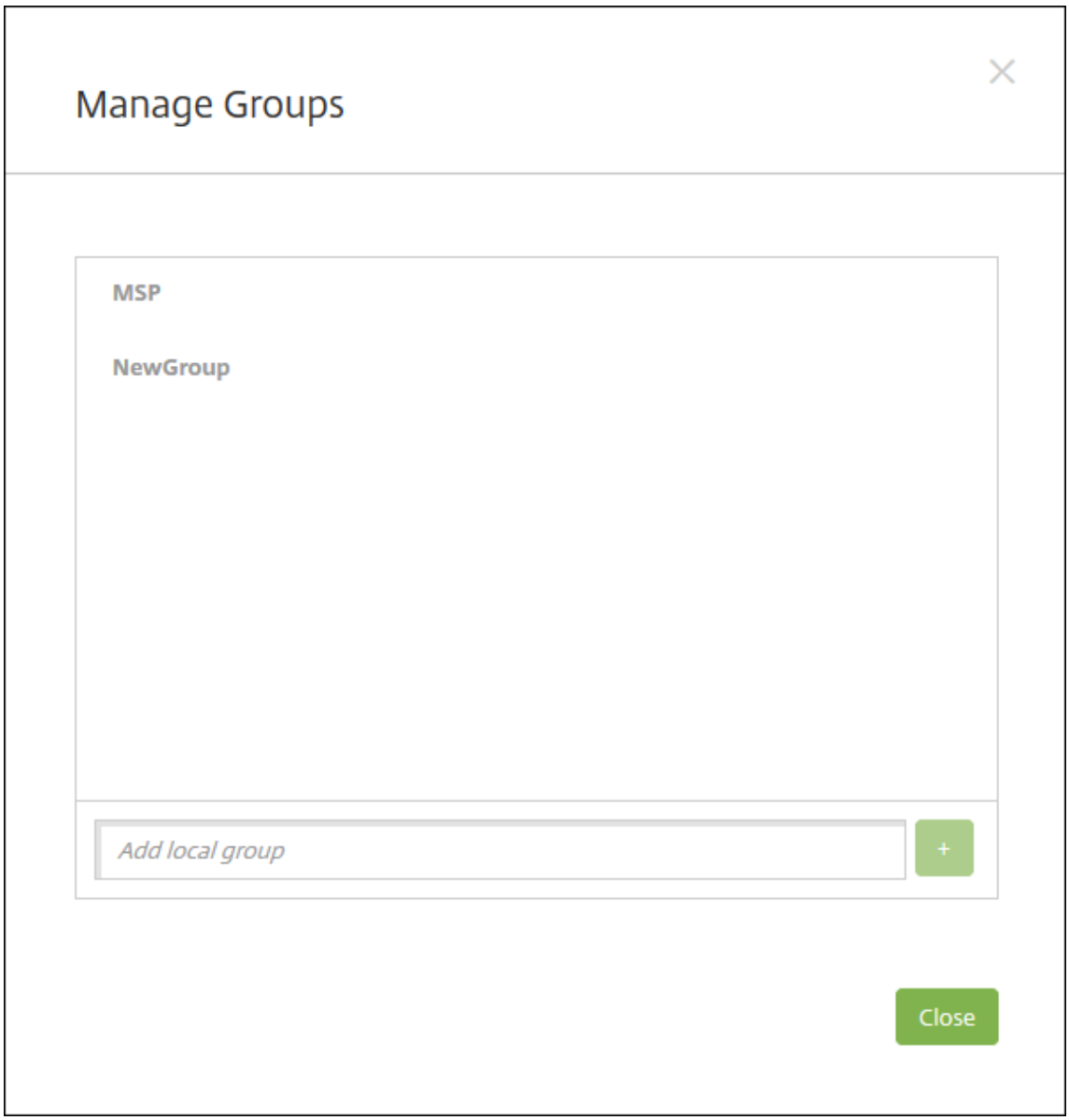
1. 次のいずれかを行います：
   - ［ユーザー］ ページで、［ローカルグループの管理］ をクリックします。



   - ［ローカルユーザーの追加］ ページまたは ［ローカルユーザーの編集］ ページで、［グループの管理］ をクリックします。



［グループ管理］ ダイアログボックスが開きます。



2. グループの一覧の下で、新しいグループ名を入力してプラス記号（**+**）をクリックします。ユーザーグループが一覧に追加されます。
3. [閉じる] をクリックします。

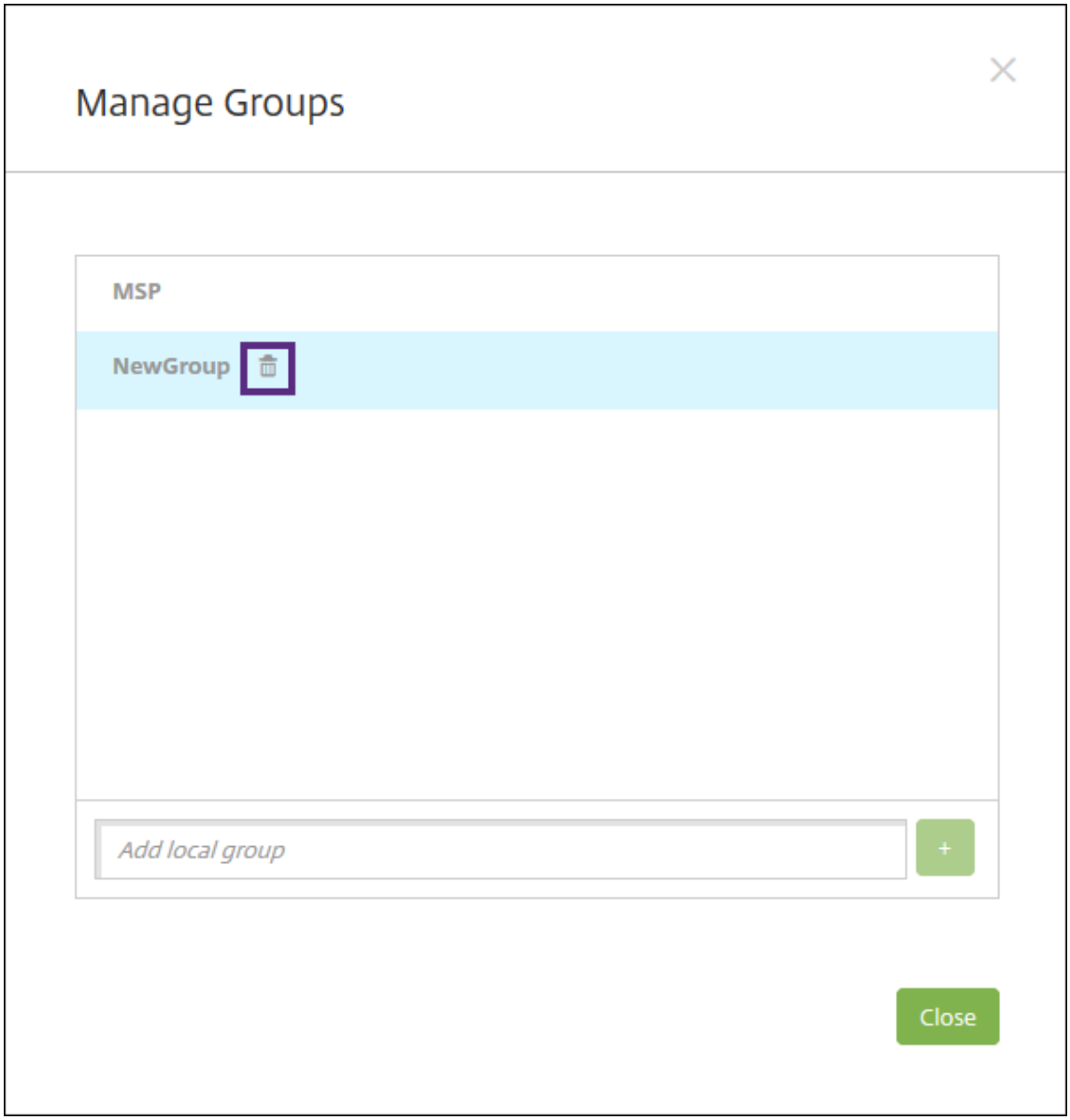
グループを削除するには

グループを削除してもユーザーアカウントには影響ありません。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

1. 次のいずれかを行います:

- ［ユーザー］ ページで、［ローカルグループの管理］ をクリックします。
- ［ローカルユーザーの追加］ ページまたは［ローカルユーザーの編集］ ページで、［グループの管理］ をクリックします。

［グループ管理］ ダイアログボックスが開きます。



2. ［グループ管理］ ダイアログボックスで、削除するグループを選択します。
3. グループ名の右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。
4. ［削除］ をクリックして操作を確認し、グループを削除します。

> 重要:
>
> この操作を元に戻すことはできません。

5. ［グループ管理］ ダイアログボックスで、［閉じる］ をクリックします。

ワークフローの作成および管理

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

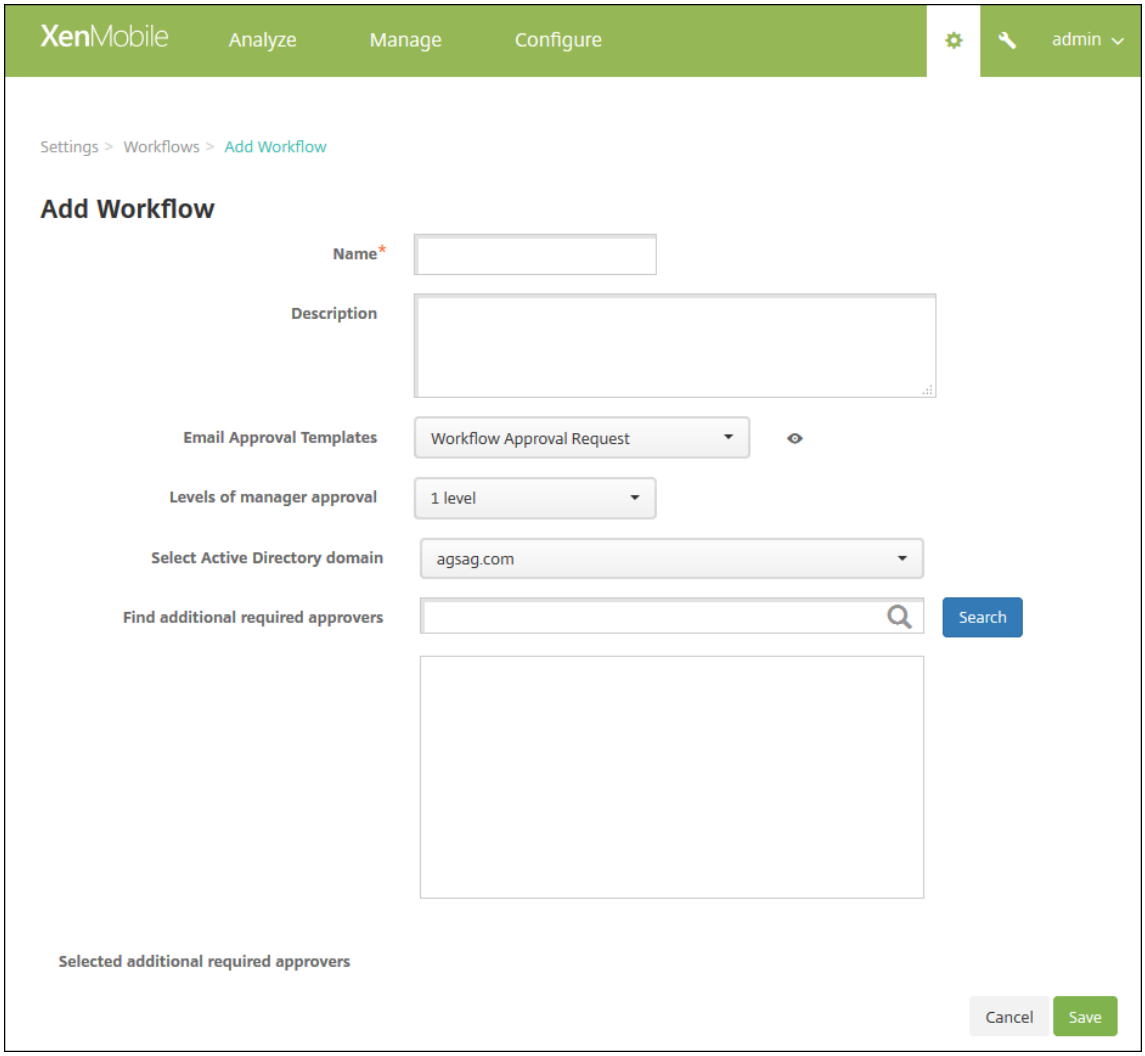
XenMobile を初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

XenMobile の次の 2 つの方法でワークフローを構成できます:

- XenMobile コンソールの ［ワークフロー］ ページ。［ワークフロー］ ページでは、アプリの構成で使用する複数のワークフローを構成できます。［ワークフロー］ページでワークフローを構成するとき、アプリを構成するときのワークフローを選択できます。
- アプリケーションコネクタを構成するとき、アプリで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。XenMobile へのアプリの追加を参照してください。

ユーザーアカウントの管理者承認を最大 3 レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、名前またはメールアドレスでユーザーを検索して選択します。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［ワークフロー］ をクリックします。［ワークフロー］ ページが開きます。
3. ［追加］ をクリックします。［ワークフローの追加］ ページが開きます。



4. 次の設定を構成します。

   - 名前: ワークフローの固有の名前を入力します。
   - 説明: 任意で、ワークフローの説明を入力します。
   - メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。電子メールテンプレートの作成は、XenMobile コンソールの［設定］の［通知テンプレート］セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、構成中のテンプレートのプレビューが表示されます。
   - マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［**1** つのレベル］です。選択できるオプションは以下のとおりです:
     - 不必要
     - 1 つのレベル
     - 2 つのレベル
     - 3 つのレベル
   - **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ド

メインを選択します。

- 追加の必須承認者を検索： 検索フィールドにユーザー名を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
  - 一覧からユーザー名を削除するには、次のいずれかの操作を行います：
    * ［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    * 名前の全体または一部を検索ボックスに入力して ［検索］ をクリックし、検索結果を絞り込みます。
    * ［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

5. ［保存］ をクリックします。作成したワークフローが ［ワークフロー］ ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリを表示したり、ワークフローを削除したりできます。ワークフローを作成した後でワークフローを編集することはできません。承認レベルまたは承認者が異なるワークフローが必要な場合は、別のワークフローを作成します。

ワークフローの詳細の表示および削除を行うには

1. ［ワークフロー］ ページの既存のワークフロー一覧で特定のワークフローを選択します。この選択を行うには、表の列をクリックするか、ワークフローの横にあるチェックボックスをオンにします。
2. ワークフローを削除するには、［削除］ をクリックします。確認ダイアログボックスが開きます。もう一度［削除］ をクリックします。

> 重要：
>
> この操作を元に戻すことはできません。

RBAC を使用した役割の構成

January 10, 2020

定義済みの役割ベースのアクセス制御（Role-Based Access Control：RBAC）の各役割には、一定のアクセス権と機能権限が関連付けられています。このトピックでは、これらの権限で実行できる内容について説明します。組み込みの役割ごとのデフォルト権限に関する完全な一覧は、『Role-Based Access Control Defaults』（英文）をダウンロードしてください。

権限を適用することで、RBAC の役割が管理する権限があるユーザーグループを定義します。デフォルトの管理者は、適用された権限設定を変更できないことに注意してください。デフォルトでは、適用された権限はすべてのユーザー

グループに適用されます。

割り当てを実行して、RBAC の役割をグループに割り当てて、そのユーザーグループが RBAC の管理者権限を持つようにできます。

この記事は、次のセクションで構成されています。

- Admin の役割
- Device Provisioning の役割
- Support の役割
- User の役割
- RBAC を使用した役割の構成

Admin の役割

定義済みの Admin の役割を持つユーザーがアクセスできる、またはアクセスできない XenMobile の機能を以下に示します。デフォルトでは、［承認済みアクセス］（Self Help Portal を除く）、［コンソールの機能］、および ［適用権限］ が有効になります。

承認済みアクセス

管理コンソールへのアクセス	管理者は XenMobile コンソールのすべての機能にアクセスできます。
Self-Help Portal へのアクセス	管理者は Self-Help Portal にアクセスできません。
共有デバイスの登録機能	管理者は共有デバイスの登録機能にアクセスできません。これは、ユーザーが共有デバイスを登録するための機能です。
リモートサポートアクセス	管理者はリモートサポートにアクセスできます。*
パブリック API へのアクセス	管理者はパブリック API にアクセスして、XenMobile コンソールで利用可能な処理をプログラム的に実行できます。これらの処理には証明書、アプリ、デバイス、デリバリーグループ、ローカルユーザーの管理が含まれます。

* リモートサポートを使用すると、ヘルプデスクの担当者は管理対象の Windows CE および Android モバイルデバイスをリモートで制御できます。画面のキャストは Samsung KNOX でのみサポートされています。XenMobile サービスのお客様はリモートサポートを利用できません。またリモートサポートはクラスター化されたオンプレミスの

XenMobile Server 展開ではサポートされていません。2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。

コンソールの機能

管理者は XenMobile コンソールに無制限にアクセスできます。

ダッシュボード	ダッシュボードは、管理者が XenMobile コンソールにログオンした後に表示される最初のページです。ダッシュボードには通知とデバイスに関する基本情報が表示されます。
レポート	[分析] > [レポート] ページでは事前定義されたレポートが提供され、アプリおよびデバイスの展開を分析できます。
デバイス	[管理] > [デバイス] ページは、管理者がユーザーデバイスを管理するためのページです。ページに個々のデバイスを追加したり、デバイスプロビジョニングファイルをインポートして一度に複数のデバイスを追加したりすることができます。
ローカルユーザーおよびグループ	[管理] > [ユーザー] ページでは、ローカルユーザーおよびローカルユーザーグループの追加、編集、または削除を行うことができます。
登録	[管理] > [登録招待] ページは、管理者がユーザーを招待してデバイスを XenMobile に登録する方法を管理するためのページです。
ポリシー	[構成] > [デバイスポリシー] ページでは、管理者が VPN や Wi-Fi のようなデバイスポリシーを管理します。
アプリ	[構成] > [アプリ] ページは、管理者が、ユーザーがデバイスにインストールできる各種アプリを管理するためのページです。
メディア	[構成] > [メディア] ページは、管理者が、ユーザーがデバイスにインストールできる各種メディアを管理するためのページです。

スマートアクション	［構成］**>**［アクション］ ページは、管理者が、イベントをトリガーする応答を管理するためのページです。
登録プロファイル	［構成］**>**［登録プロファイル］ ページは、管理者が登録プロファイル（モード）を構成して、ユーザーがデバイスを登録できるようにするためのページです。
デリバリーグループ	［構成］**>**［デリバリーグループ］ ページは、管理者がデリバリーグループ、およびデリバリーグループに関連付けられているリソースを管理するためのページです。
設定	［設定］ ページは、管理者がシステムの設定（クライアントおよびサーバープロパティ、証明書、資格情報プロバイダーなど）を管理するためのページです。
サポート	［トラブルシューティングとサポート］ ページは、管理者がトラブルシューティングアクティビティ（診断の実行やログの生成など）を実行するためのページです。

デバイス

管理者はコンソール全体のデバイス機能にアクセスするため、デバイスの制限を設定したり、デバイスへの通知を設定して送信したり、デバイス上のアプリを管理したりします。

デバイスの完全なワイプ	デバイスからすべてのデータやアプリを消去します。デバイスに設置されている場合、メモリカードもその対象となります。
制限の削除	1 つまたは複数のデバイスの制限を削除します。
デバイスの選択的なワイプ	個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。
場所の表示	デバイスの場所を表示し、デバイスの地理的制約を設定します。含まれるもの：デバイスの検索、デバイスの場所の表示、デバイスの追跡、時間の経過によるデバイスの位置の追跡。
デバイスのロック	ユーザーがデバイスを使用できないように、リモートでデバイスをロックします。

デバイスのロック解除	ユーザーがデバイスを使用できるように、リモートでデバイスのロックを解除します。
コンテナのロック	リモートでデバイス上の企業のコンテナをロックします。
コンテナのロック解除	リモートでデバイス上の企業のコンテナのロックを解除します。
コンテナのパスワードのリセット	企業のコンテナのパスワードをリセットします。
ASM DEP/バイパスアクティベーションロックを有効化	アクティベーションロックが有効な場合、監視対象の iOS デバイスにバイパスコードを格納します。デバイスの消去が必要な場合は、このコードを使用するとアクティベーションロックが自動的に解除されます。
デバイスを呼び出します	リモートで、Windows のデバイスの警報をフルボリュームで 5 分間鳴らします。
デバイスを再起動	XenMobile コンソールから Windows デバイスを再起動します。
デバイスに展開	デバイスにアプリ、通知、制限などを送信します。
デバイスの編集	デバイスの設定を変更します。
デバイスへの通知	デバイスに通知を送信します。
デバイスの追加/削除	XenMobile でのデバイスの追加または削除を行います。
デバイスのインポート	ファイルから XenMobile にデバイスのグループをインポートします。
デバイステーブルのエクスポート	[デバイス] ページからデバイス情報を収集し、.csv ファイルにエクスポートします。
デバイスの取り消し	デバイスから XenMobile への接続を禁止します。
アプリのロック	デバイスのすべてのアプリへのアクセスを拒否します。Android では、ユーザーはまったく XenMobile にログインできなくなります。iOS では、ユーザーはまだログインできますが、アプリにアクセスできません。
アプリのワイプ	Android では、これによりユーザーの XenMobile アカウントが削除されます。iOS では、これにより、ユーザーが XenMobile 機能にアクセスするために必要な暗号キーが削除されます。

ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを表示します。
AirPlay ミラーリングの要求	AirPlay ストリーミング開始の要求
AirPlay ミラーリングの停止	AirPlay ストリーミングの停止
紛失モードを有効化	デバイスを紛失した、または盗難にあった場合、［Devices］の［Manage］ページで、監視対象デバイスを紛失モードにして、ロック画面で監視対象デバイスへのアクセスをブロックし、デバイスの位置を特定できます。
紛失モードを無効化	［デバイス］の［管理］ページで、紛失モードが設定されたデバイスの紛失モードを無効化できます。
OS 更新デバイス	OS 更新の制御デバイスポリシーをデバイスに展開できます。
デバイスのシャットダウン	XenMobile コンソールから iOS デバイスをシャットダウンします。
デバイスの再起動	XenMobile コンソールから iOS デバイスを再起動します。

ローカルユーザーおよびグループ

管理者は、XenMobile の ［管理］**>** ［ユーザー］ ページで、ローカルユーザーおよびローカルユーザーグループを管理します。

ローカルユーザーの追加
ローカルユーザーの削除
ローカルユーザーの編集
ローカルユーザーのインポート
ローカルユーザーのエクスポート
ローカルユーザーグループ

登録

管理者は登録招待の追加および削除、ユーザーへの通知の送信、.csv ファイルへの登録テーブルのエクスポートを行うことができます。

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待状を追加または削除します。
ユーザーに通知	ユーザーまたはユーザーグループに登録招待状を送信します。
登録招待状テーブルのエクスポート	［登録］ページから登録情報を収集し、.csv ファイルにエクスポートします。

ポリシー

ポリシーの追加/削除	デバイスまたはアプリポリシーを追加または削除します。
ポリシーの編集	デバイスまたはアプリポリシーを変更します。
ポリシーのアップロード	デバイスまたはアプリポリシーをアップロードします。
ポリシーの複製	デバイスまたはアプリポリシーをコピーします。
ポリシーを無効にする	既存のアプリポリシーを無効にします。
ポリシーのエクスポート	［デバイスポリシー］ページからデバイスポリシーの情報を収集し、.csv ファイルにエクスポートします。
ポリシーの割り当て	デバイスポリシーを 1 つまたは複数のグループに割り当てます。

アプリ

管理者は XenMobile の ［構成］**>**［アプリ］ ページでアプリを管理します。

アプリストアまたはエンタープライズアプリの追加/削除	パブリックアプリストアのアプリ、または MDX Toolkit でラップされていないアプリを追加または削除します。

アプリストアまたはエンタープライズアプリの編集	パブリックアプリストアのアプリ、または MDX Toolkit でラップされていないアプリに対する変更を行います。
MDX、Web、SaaS アプリの追加/削除	MDX Toolkit でラップされたアプリ（MDX アプリ）、内部ネットワークからのアプリ（Web アプリ）、またはパブリックネットワークから XenMobile へのアプリ（SaaS）を追加または削除します。
MDX、Web、SaaS アプリの編集	MDX Toolkit でラップされたアプリ（MDX アプリ）、内部ネットワークからのアプリ（Web アプリ）、またはパブリックネットワークから XenMobile へのアプリ（SaaS）に対する変更を行います。
カテゴリの追加/削除	XenMobile Store でのアプリの表示に使用できるカテゴリを追加または削除します。
パブリック/エンタープライズアプリのデリバリーグループへの割り当て	パブリックアプリストアのアプリ、または MDX Toolkit でラップされていないアプリを、展開のためにデリバリーグループに割り当てます。
デリバリーグループへの MDX/WebLink/Saas アプリの割り当て	MDX Toolkit でラップされたアプリ（MDX アプリ）、シングルサインオンの不要なアプリ（WebLink）、またはパブリックネットワークからのアプリ（SaaS）を、ユーザーデバイスで展開するためにデリバリーグループに割り当てます。
アプリテーブルのエクスポート	［アプリ］ページからアプリ情報を収集し、.csv ファイルにエクスポートします。

メディア

パブリックアプリストアから、または VPP ライセンスを介して取得したメディアを管理します。

アプリストアまたはエンタープライズブックの追加/削除
パブリック/エンタープライズブックのデリバリーグループへの割り当て
アプリストアまたはエンタープライズブックの編集

スマートアクション

スマートアクションの追加/削除	トリガー（イベント/デバイス/ユーザープロパティ、またはインストールされたアプリの名前）とそれに関連する応答によって定義される操作を追加または削除します。
スマートアクションの編集	トリガー（イベント/デバイス/ユーザープロパティ、またはインストールされたアプリの名前）とそれに関連する応答によって定義される操作を変更します。
スマートアクションのデリバリーグループへの割り当て	ユーザーデバイスへの展開のために、デリバリーグループに操作を割り当てます。
スマートアクションのエクスポート	［アクション］ページから操作の情報を収集し、.csv ファイルにエクスポートします。

デリバリーグループ

管理者は ［構成］**>**［デリバリーグループ］ ページからデリバリーグループを管理します。

デリバリーグループの追加/削除	デリバリーグループを作成または削除します。このグループには、指定のユーザーおよびオプションのポリシー、アプリ、操作が追加されています。
デリバリーグループの編集	既存のデリバリーグループを変更します。このグループでは、ユーザーおよびオプションのポリシー、アプリ、操作の変更が行われます。
デリバリーグループの展開	デリバリーグループが使用できる状態にします。
デリバリーグループのエクスポート	［デリバリーグループ］ページからデリバリーグループの情報を収集し、.csv ファイルにエクスポートします。

登録プロファイル

登録プロファイルを管理します。

登録プロファイルの追加/削除

登録プロファイルの編集
登録プロファイルのデリバリーグループへの割り当て

設定

管理者は ［設定］ ページで各種設定を構成します。

RBAC	RBAC の割り当て、役割の割り当て
LDAP	グループ、ユーザーアカウント、および関連のプロパティをインポートする Active Directory のような 1 つまたは複数の LDAP 準拠のディレクトリを管理します。
ライセンス	オンプレミスの XenMobile Server 用です。Citrix ライセンスを管理します。
登録	Self-Help Portal とユーザーの登録モードを有効にします。
リリース管理	現在インストールされてるリリースの情報を表示します。含まれるもの：リリース管理の更新
証明書	APNs 証明書の編集、証明書 SSL リスナー
通知テンプレート	自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを作成します。
ワークフロー	アプリの構成で使用するユーザーアカウントの作成、承認、削除を管理します。
資格情報プロバイダー	デバイスの証明書の発行を許可されている 1 つまたは複数の資格情報プロバイダーを追加します。資格情報プロバイダーは、証明書の形式および証明書の更新または失効の条件を管理します。
PKI エンティティ	公開キーのインフラストラクチャエンティティ（通常は Microsoft Certificate Services、または随意 CA）を管理します。

PKI 接続のテスト	［設定］**>**［**PKI** エンティティ］ ページの［接続のテスト］ボタンを使用して、サーバーがアクセス可能であることを確認します。
クライアントプロパティ	パスコードのタイプ、強度、満了日など、ユーザーデバイスの各種プロパティを管理します。
クライアントサポート	ユーザーがサポートサービスに連絡する方法を設定します（メール、電話、またはサポートチケットメール）。
クライアントのブランド設定	XenMobile Store のカスタムストア名とデフォルトストア表示を作成します。XenMobile Store や Secure Hub に表示されるカスタムロゴを追加します。
キャリア SMS ゲートウェイ	キャリア SMS ゲートウェイを設定して、電話会社の SMS ゲートウェイ経由で XenMobile が送信する通知を構成します。
通知サーバー	メールをユーザーに送信するための SMTP ゲートウェイサーバーを設定します。
ActiveSync ゲートウェイ	規則およびプロパティを通してユーザーおよびデバイスへのユーザーアクセスを管理します。
Apple デバイス登録プログラム（DEP）	Apple DEP アカウントを XenMobile に追加します。
Apple Configurator デバイス登録	XenMobile で Apple Configurator 設定を構成します。
iOS/VPP の設定	Apple 社の Volume Purchase Program のアカウントを追加します。
モバイルサービスプロバイダー	Mobile Service Provider インターフェイスを使用して、BlackBerry やそのほかの Exchange ActiveSync デバイスに対してクエリを実行したり、操作を発行したりします。
NetScaler Gateway	オンプレミスの XenMobile Server 用です。NetScaler Gateway を追加します。認証を有効にするか、および認証用にユーザーの証明書をプッシュするかを選択します。資格情報プロバイダーを選択します。
ネットワークアクセス制御	デバイスが準拠していないため、ネットワークへのアクセスを拒否されたと判断するための条件を設定します。

Samsung KNOX	XenMobile による Samsung KNOX 認証サーバー REST API に対するクエリの実行を有効または無効にします。
サーバープロパティ	サーバープロパティを追加または変更します。すべてのノードで XenMobile を再起動する必要があります。
Syslog	オンプレミスの XenMobile Server 用です。サーバーのホスト名または IP アドレスを使用して、システムログ（syslog）サーバーにログファイルを送信します。
XenApp/XenDesktop	Secure Hub を介してユーザーは Virtual Apps and Desktops を追加できます。
ShareFile	ShareFile Enterprise で XenMobile を使用する場合：ShareFile アカウントと、ユーザーアカウント管理用の管理者サービスアカウントに接続するための設定を構成します。既存の ShareFile ドメインと管理者の資格情報が必要です。StorageZone コネクタで XenMobile を使用する場合：ShareFile StorageZone コネクタで定義されたネットワーク共有と SharePoint の場所を指すように XenMobile を構成します。
エクスペリエンス向上プログラム	オンプレミスの XenMobile Server 用です。匿名の統計および使用情報の Citrix への送信を選択するか、見合わせます。
Microsoft Azure	オンプレミスの XenMobile Server 用です。XenMobile を Microsoft Azure に統合します。
Android Enterprise	Android Enterprise サーバー設定を構成します。
ID プロバイダー（IDP）	ID プロバイダーを構成します。
派生資格情報	iOS デバイス登録のための派生資格情報を構成します。
XenMobile ツール	[XenMobile Tools] ページにアクセスします。
SNMP 構成	XenMobile Server ノードの SNMP を有効にします。監視ユーザーを編集または追加し、トラップ通知が表示される SNMP マネージャーをセットアップし、トラップ間隔としきい値を構成します。

サポート

管理者は各種サポートタスクを実行できます。

NetScaler Gateway 接続性チェック	IP アドレスによる NetScaler Gateway の各種接続確認を実行します。ユーザー名とパスワードが必要です。
XenMobile 接続性チェック	選択した XenMobile の機能、たとえば、データベース、DNS、Google Plan などの接続確認を実行します。
サポートバンドルの作成	オンプレミスの XenMobile Server 用です。トラブルシューティングのためにシトリックスサポートに送信するファイルを作成します。XenMobile または NetScaler Gateway のシステム情報、ログ、データベース情報、コア情報、トレースファイル、最新の構成情報が含まれます。
シトリックス製品ドキュメント	Citrix XenMobile ドキュメントの公開サイトにアクセスします。
Citrix Knowledge Center	ナレッジベースの文書を検索するために Citrix Support サイトにアクセスします。
ログ	デバッグ、管理監査、ユーザー監査のログファイルの詳細情報にアクセスし、分析します。
クラスター情報	オンプレミスの XenMobile Server 用です。クラスター環境内の各ノードに関する情報にアクセスします。
ガベージコレクション	オンプレミスの XenMobile Server 用です。使用されなくなったメモリオブジェクトに関する情報にアクセスします。
Java メモリのプロパティ	オンプレミスの XenMobile Server 用です。Java のメモリ使用のスナップショット、メモリの詳細、メモリプールの詳細にアクセスします。
マクロ	プロファイル、ポリシー、通知、または登録テンプレートのテキストフィールド内にユーザーまたはデバイスのプロパティデータを設定します。単一のポリシーを構成して大きなユーザーベースに展開し、各対象ユーザーに固有の値を表示させることができます。
PKI 構成	PKI 構成情報をインポートおよびエクスポートします。

APNs 署名ユーティリティ	Apple 社の Push Network signing（APNs）証明書の要求を提出するか、iOS 用の Secure Mail APN 証明書をアップロードします。
Citrix Insight Services	さまざまな問題に対する支援が得られるように、Citrix Insight Services（CIS）にログをアップロードします。
Citrix Gateway コネクタ：Exchange ActiveSync 用のデバイスの状態	Citrix Gateway コネクタ：Exchange ActiveSync 用に送信された時点のデバイスの状態について、デバイスの ActiveSync ID に基づいて XenMobile に対するクエリを実行します。
匿名化および匿名化解除	オンプレミスの XenMobile Server 用です。XenMobile でサポートバンドルを作成する場合、デフォルトでは、機密性の高いユーザー、サーバー、ネットワークのデータは匿名化されます。この動作は、［詳細］、［サポート］の［匿名化および匿名化解除］ページで変更できます。
ログ設定	ログレベルをカスタマイズしたりカスタムロガーを追加したりします。

グループアクセスの制限

Admin ユーザーはすべてのユーザーグループに権限を適用することができます。

Device Provisioning の役割

> 重要：
>
> Device Provisioning の役割は、Windows CE デバイスにのみ適用されます。

事前定義されたデバイスプロビジョニングの役割のユーザーは、コンソール機能へのアクセスが限定されています。デフォルトで、すべてのユーザーグループにこのユーザーの権限が設定され、ユーザーが設定を変更することはできません。

コンソールの機能

XenMobile コンソールに対して、Device Provisioning ユーザーは以下の制限付きアクセスが行えます。デフォルトでは、以下の機能がそれぞれ有効になっています。

デバイス

デバイスの編集	デバイスの設定を変更します。
デバイスの追加/削除	XenMobile でのデバイスの追加または削除を行います。

設定

デバイスプロビジョニングのユーザーは ［設定］ ページにアクセスできますが、機能を構成する権限はありません。

Support の役割

Support の役割があるユーザーは、リモートサポートにアクセスできます。このユーザー権限は、デフォルトですべてのユーザーに適用され、ユーザーが設定を編集することはできません。

User の役割

User の役割を持つユーザーは、XenMobile に対して以下の制限付きアクセスが行えます。

承認済みアクセス

Self-Help Portal	ユーザーは XenMobile の Self-Help Portal にのみアクセスできます。

コンソールの機能

XenMobile コンソールに対して、ユーザーは以下の制限付きアクセスが行えます。

デバイス

デバイスの完全なワイプ	デバイスからすべてのデータやアプリを消去します。デバイスに設置されている場合、メモリカードもその対象となります。
デバイスの選択的なワイプ	個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。
場所の表示	デバイスの場所を表示し、デバイスの地理的制約を設定します。含まれるもの：デバイスの検索、デバイスの場所の表示、デバイスの追跡、時間の経過によるデバイスの位置の追跡。
デバイスのロック	デバイスが使用できないように、リモートでロックします。
デバイスのロック解除	デバイスが使用できるように、リモートでロックを解除します。
コンテナのロック	リモートでデバイス上の企業のコンテナをロックします。
コンテナのロック解除	リモートでデバイス上の企業のコンテナのロックを解除します。
コンテナのパスワードのリセット	企業のコンテナのパスワードをリセットします。
ASM DEP/バイパスアクティベーションロックを有効化	アクティベーションロックが有効な場合、監視対象の iOS デバイスにバイパスコードを格納します。デバイスの消去が必要な場合は、このコードを使用するとアクティベーションロックが自動的に解除されます。
デバイスを呼び出します	リモートで、Windows のデバイスの警報をフルボリュームで 5 分間鳴らします。
デバイスを再起動	Windows デバイスを再起動します。
ソフトウェアインベントリの表示	デバイスにインストールされているソフトウェアを表示します。

登録

登録の追加/削除	ユーザーまたはユーザーグループへの登録招待状を追加または削除します。

ユーザーに通知	ユーザーまたはユーザーグループに登録招待状を送信します。

グループアクセスの制限

4 つデフォルトの役割のすべてで、この権限がデフォルトで設定され、すべてのユーザーグループに適用できます。役割を編集することはできません。

RBAC を使用した役割の構成

XenMobile の役割ベースのアクセス制御（Role-Based Access Control：RBAC）機能では、権限の定義済みセットである役割をユーザーとグループに割り当てることができます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。

XenMobile には、システムの機能へのアクセスを論理的に区分するために、4 つのデフォルトのユーザー役割が実装されています。

- 管理者： システムへのフルアクセスが許可されます。
- デバイスプロビジョニング： Windows CE デバイスで基本的なデバイス管理へのアクセスが許可されます。
- サポート： リモートサポートへのアクセスが許可されます。
- ユーザー： デバイスを登録でき、Self Help Portal にアクセスできるユーザーが使用します。

デフォルトの役割をテンプレートとして使用することもできます。テンプレートをカスタマイズして、デフォルトの役割によって定義されている機能には含まれない特定のシステム機能にアクセスするための権限を持つ、新しいユーザーの役割を作成できます。

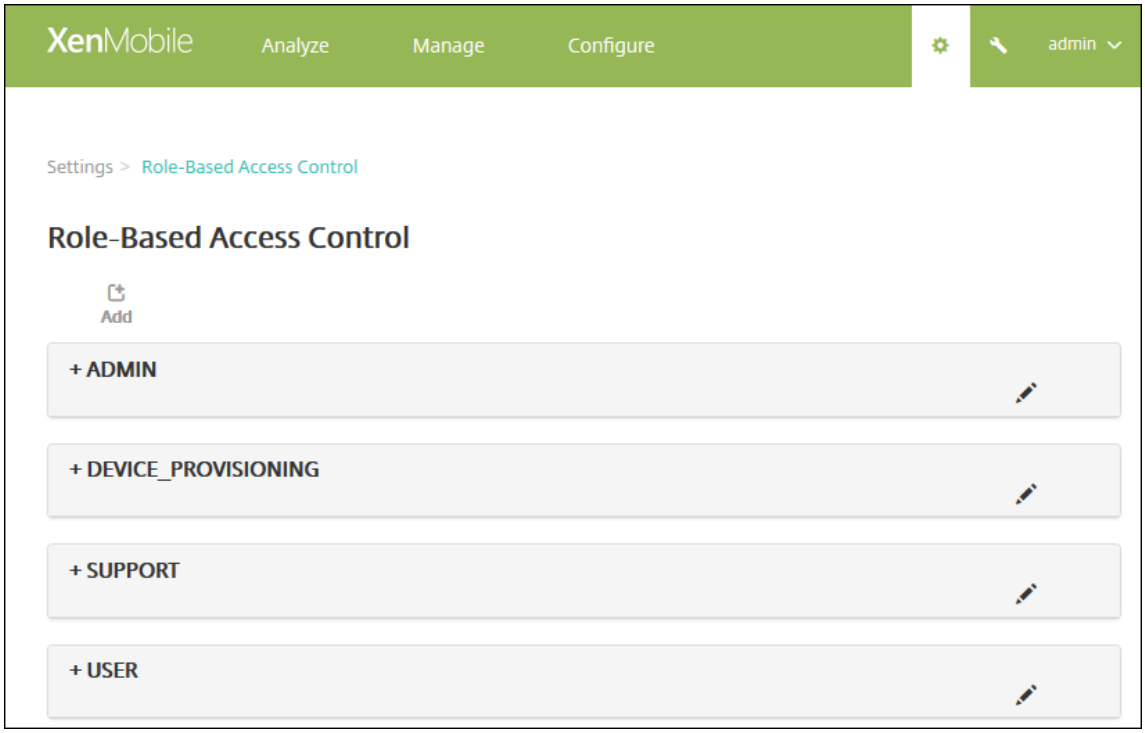
役割をローカルユーザーに（ユーザーレベルで）割り当てることや、Active Directory グループに割り当てることができます（そのグループ内のすべてのユーザーが同じ権限を持ちます）。ユーザーが複数の Active Directory グループに属している場合は、すべての権限が統合されてそのユーザーの権限が定義されます。たとえば、ADGroupA のユーザーがマネージャーのデバイスを検索でき、ADGroupB のユーザーが従業員のデバイスをワイプできる場合、両方のグループに属するユーザーは、マネージャーおよび従業員のデバイスを検索し、ワイプすることができます。

> 注：
>
> ローカルユーザーに割り当てることができる役割は 1 つだけです。

XenMobile の RBAC 機能を使用すると、次のことを実行できます。

- 新しい役割を作成する。
- 役割にグループを追加する。
- ローカルユーザーを役割に関連付ける。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［役割ベースのアクセス制御］ をクリックします。［役割ベースのアクセス制御］ ページが開き、4 つのデフォルトのユーザー役割と、以前に追加した役割が表示されます。

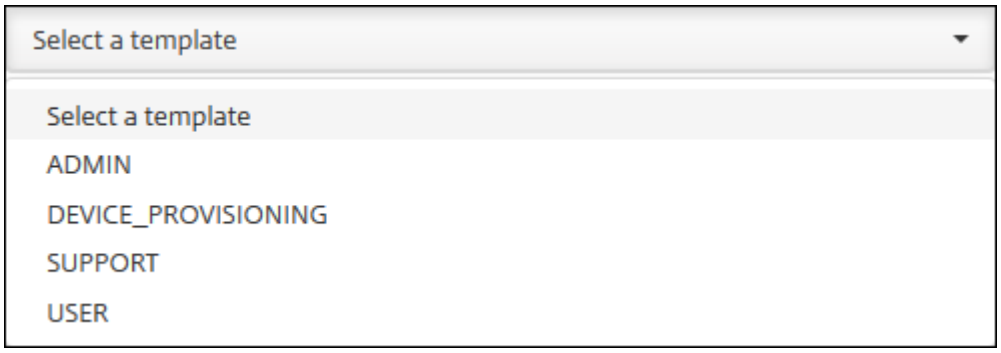


役割の横のプラス記号（+）をクリックすると、次の図のように役割が展開され、その役割のすべての権限が表示されます。

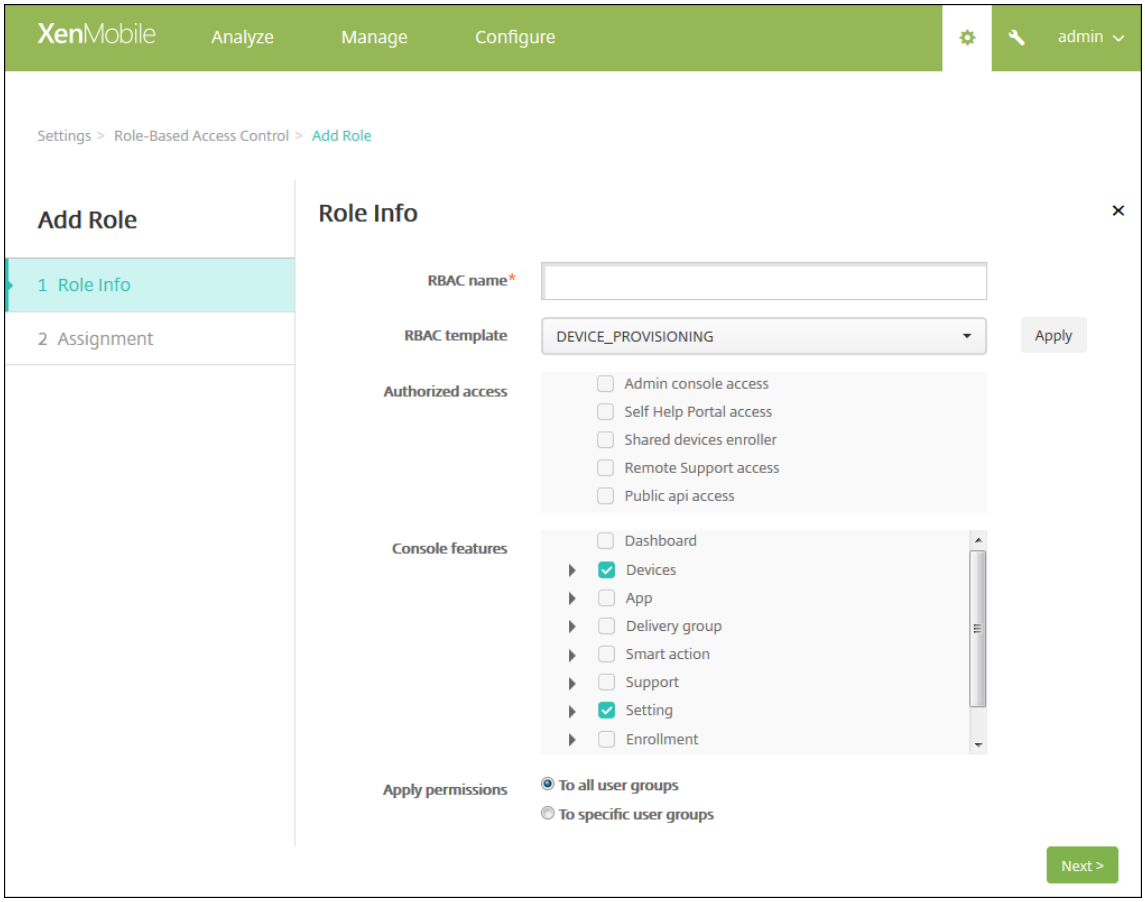
3. ［追加］ をクリックして新しいユーザー役割を追加したり、既存の役割の右にあるペンアイコンをクリックして役割を編集したり、以前定義した役割の右にあるごみ箱アイコンをクリックして役割を削除したりします。デフォルトのユーザー役割を削除することはできません。
   - ［追加］ またはペンアイコンをクリックすると、［役割の追加］ ページまたは ［役割の編集］ ページが開きます。
   - ごみ箱アイコンをクリックすると、確認ダイアログボックスが開きます。［削除］ をクリックすると、選択した役割が削除されます。
4. 新しいユーザー役割を作成するか、または既存のユーザー役割を編集するには、次の情報を入力します。

- **RBAC** 名: 新しいユーザー役割の説明的な名前を入力します。既存の役割の名前は変更できません。
- **RBAC** テンプレート: 任意で、新しい役割の開始点とするテンプレートを選択します。既存の役割を編集する場合、テンプレートは選択できません。

RBAC テンプレートは、デフォルトのユーザー役割です。RBAC テンプレートによって、その役割に関連付けられているユーザーがシステムの機能に対して持つアクセス権を定義します。RBAC テンプレートを選択すると、［承認済みアクセス］ および ［コンソールの機能］ フィールドで、その役割に関連付けられているすべての権限を参照できます。テンプレートの使用はオプションです。［承認済みアクセス］ および ［コンソールの機能］ フィールドで、役割に割り当てるオプションを直接選択することができます。

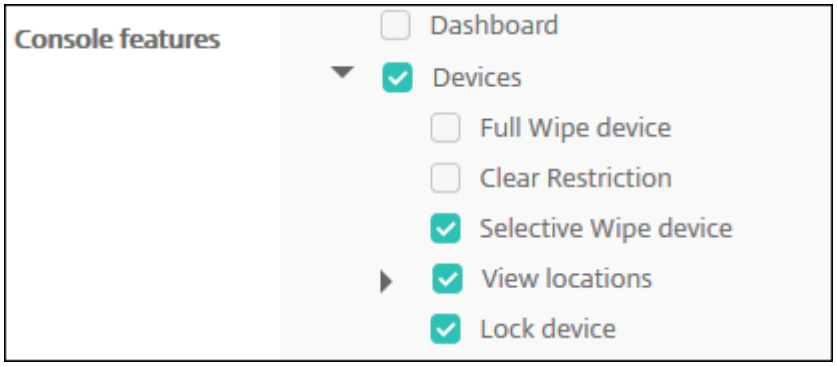


5. ［**RBAC** テンプレート］ フィールドの右にある ［適用］ をクリックして、選択したテンプレートで定義されているアクセス権と機能権限を、［承認済みアクセス］ および ［コンソールの機能］ にあるチェックボックスに反映させます。



6. ［承認済みアクセス］ および ［コンソールの機能］ のチェックボックスをオンまたはオフにして、役割をカスタマイズします。

   ［コンソールの機能］の横にある三角をクリックすると、その機能に固有の権限が表示され、オンまたはオフを選択できます。最上位のチェックボックスをオンにすると、そのコンソール部分に対するアクセスを禁止できます。最上位レベルより下のオプションを有効にするには、それらのオプションを個別にオンにする必要があります。たとえば、次の図の場合、役割に割り当てられているユーザーのコンソールに ［デバイスの完全なワイプ］ オプションおよび ［デバイスの制限の削除］ オプションは表示されません。一方で、チェックボックスがオンになっているオプションは表示されます。

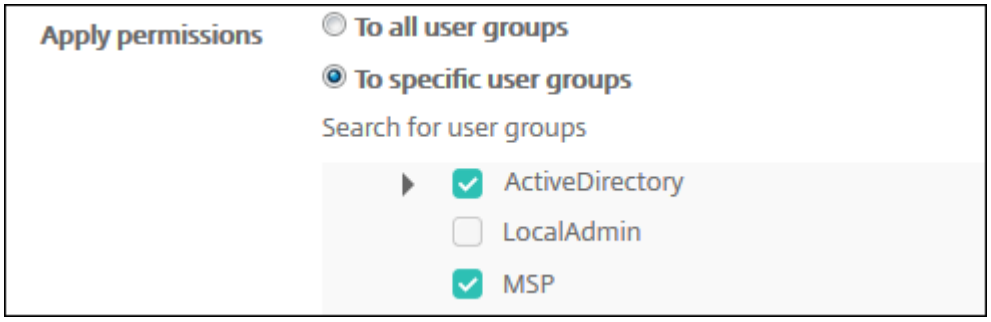


7. 権限の適用： 管理者が管理できるグループを制限するには、1 つ以上のユーザーグループを選択します。［特

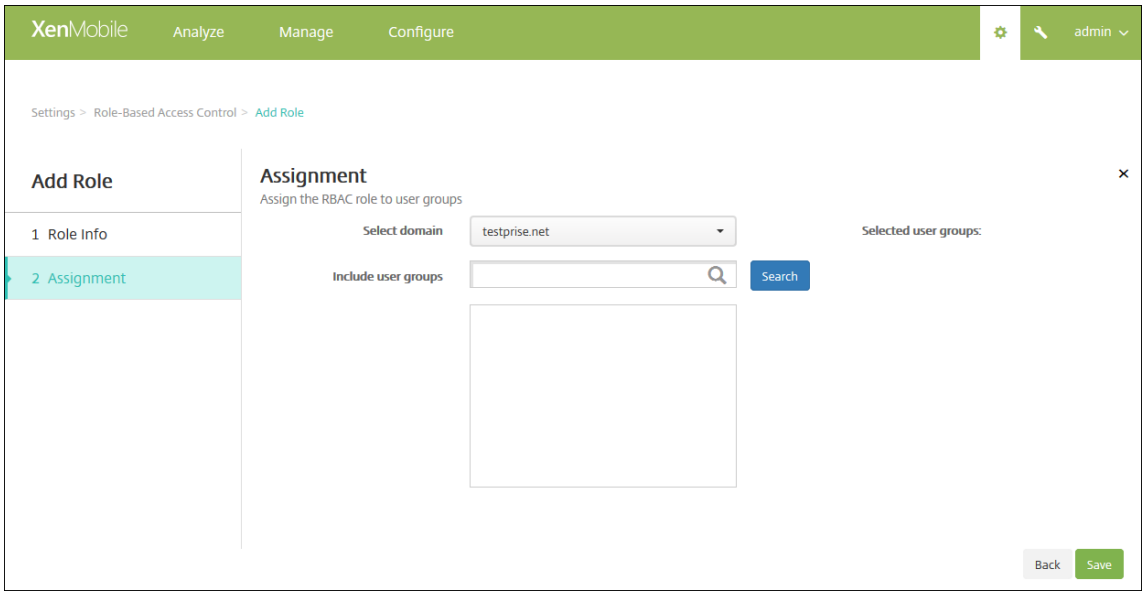
定のユーザーグループ] をクリックするとグループの一覧が開き、1 つまたは複数のグループを選択できます。

たとえば、RBAC 管理者が ActiveDirectory および MSP ユーザーグループに対するアクセス権限を持っている場合:

- 管理者は、ActiveDirectory グループ、MSP グループ、またはその両方のグループに属するユーザーの情報にのみアクセスできます。
- 管理者は、他のローカルユーザーまたは AD ユーザーを表示することはできません。管理者が表示できるのは、いずれかのグループの子グループのメンバーであるユーザーです。
- 管理者は次のグループに招待状を送ることができます:
  - 権限グループとその子グループ
  - 権限グループのメンバーであるユーザーとその子グループ



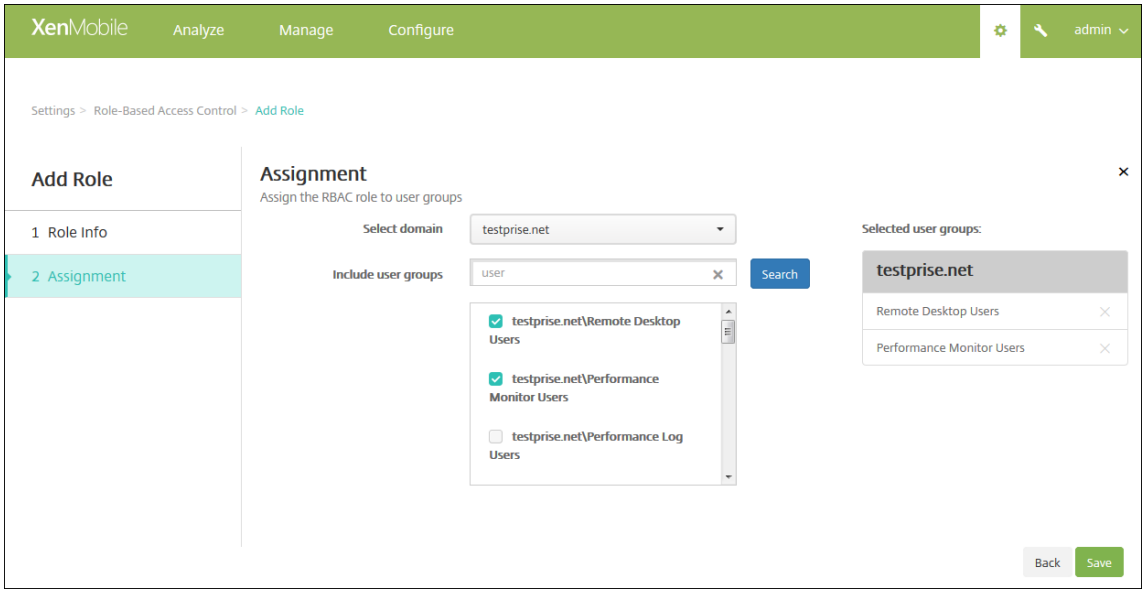
8. [次へ] をクリックします。[割り当て] ページが開きます。



9. ユーザーグループに役割を割り当てるための次の情報を入力します。

- ドメインを選択: 一覧から、ドメインを選択します。
- ユーザーグループを含める: [検索] をクリックして使用可能なすべてのグループの一覧を表示するか、グループ名の全体または一部を入力してその名前を持つグループのみに一覧を絞り込みます。
- 表示された一覧で、役割を割り当てるユーザーグループを選択します。ユーザーグループを選択すると、

［選択したユーザーグループ］ の一覧にグループが表示されます。



> 注:
>
> ［選択したユーザーグループ］ の一覧からユーザーグループを削除するには、ユーザーグループ名の横にある［X］をクリックします。

10. ［保存］ をクリックします。

通知

August 22, 2019

XenMobile での通知は以下の目的で利用できます。

- 多くのシステム関連機能に関して、選択したグループのユーザーに連絡します。また、これらの通知の対象を特定のユーザーにすることもできます。たとえば、iOS デバイスを持つすべてのユーザー、コンプライアンスを満たしていないデバイスのユーザー、個人所有のデバイスを持つユーザーなどです。
- ユーザーとデバイスを登録します。
- 特定の条件が満たされたときに（自動化された操作を使用して）ユーザーに自動的に通知します。次に例を示します:
  - コンプライアンスの問題により、ユーザーデバイスが企業ドメインからブロックされようとしているとき。
  - デバイスが改造されたりルートされたりした場合。

自動化された操作について詳しくは、「自動化された操作」を参照してください。

XenMobile で通知を送信するには、ゲートウェイおよび通知サーバーを構成する必要があります。XenMobile で通知サーバーを設定して、SMTP（簡易メール転送プロトコル: Simple Mail Transfer Protocol）サーバーやショー

トメッセージサービス（SMS）のゲートウェイサーバーを構成し、電子メールやテキスト（SMS）通知をユーザーに送信することができます。通知では、SMTP または SMS の 2 種類のチャネル経由でメッセージを送信できます。

- SMTP はコネクション型のテキストベースプロトコルで、通常は TCP（Transmission Control Protocol）経由で、メール送信者がコマンド文字列を発行して必要なデータを供給し、メール受信者と通信します。SMTP セッションは、SMTP クライアント（メッセージの送信者）から送信されたコマンドと、コマンドに対応する、SMTP サーバーからの応答によって構成されます。
- SMS は、電話、Web、またはモバイル通信システムのテキストメッセージサービスコンポーネントです。標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

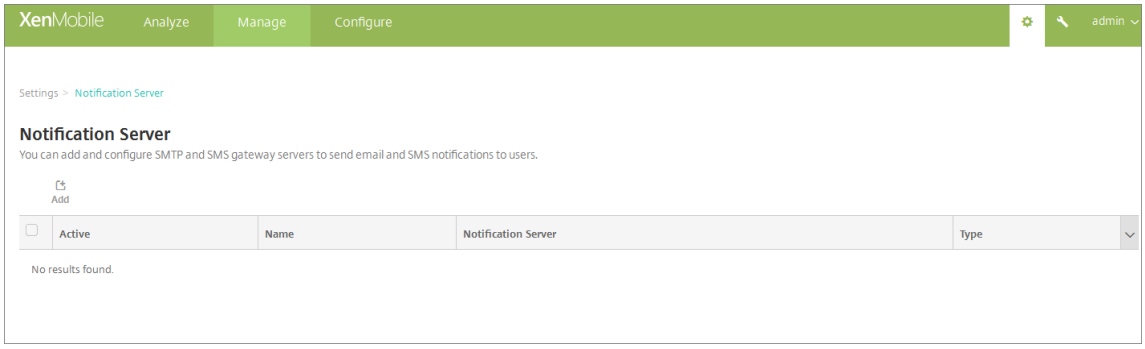
また、XenMobile でキャリア SMS ゲートウェイを設定して、電話会社の SMS ゲートウェイ経由で送信される通知を構成することもできます。電話会社は SMS ゲートウェイを使用して、通信ネットワークと相互に SMS メッセージを送受信します。これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

前提条件

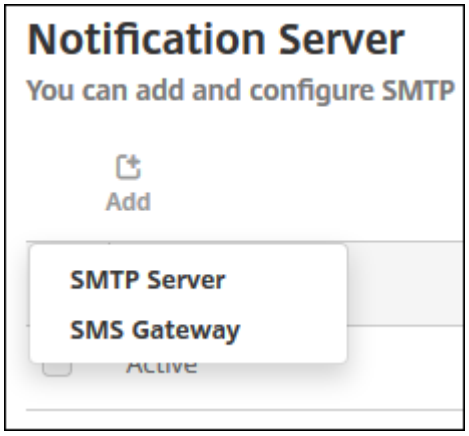
- SMS ゲートウェイを構成する前に、システム管理者に問い合わせてサーバー情報を確認してください。SMS サーバーが社内サーバーでホストされているか、ホストされている電子メールサービスに含まれているかを確認することが重要です。後者の場合は、サービスプロバイダーの Web サイトからの情報が必要です。
- メッセージをユーザーに送信するための SMTP 通知サーバーを構成してください。サーバーが社内サーバーでホストされている場合は、システム管理者に構成情報を問い合わせてください。サーバーが、ホストされている電子メールサービスの場合は、サービスプロバイダーの Web サイトで適切な構成情報を確認してください。
- SMTP サーバーと SMS サーバーは、それぞれ一度に 1 つのみがアクティブになるようにしてください。
- ネットワークの DMZ 内の XenMobile からポート 25 を開き、内部ネットワークの SMTP サーバーにポイントバックしてください。これにより、XenMobile は通知を正常に送信できます。

SMTP サーバーおよび **SMS** ゲートウェイの構成

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［通知］ の下の ［通知サーバー］ をクリックします。［通知サーバー］ ページが開きます。

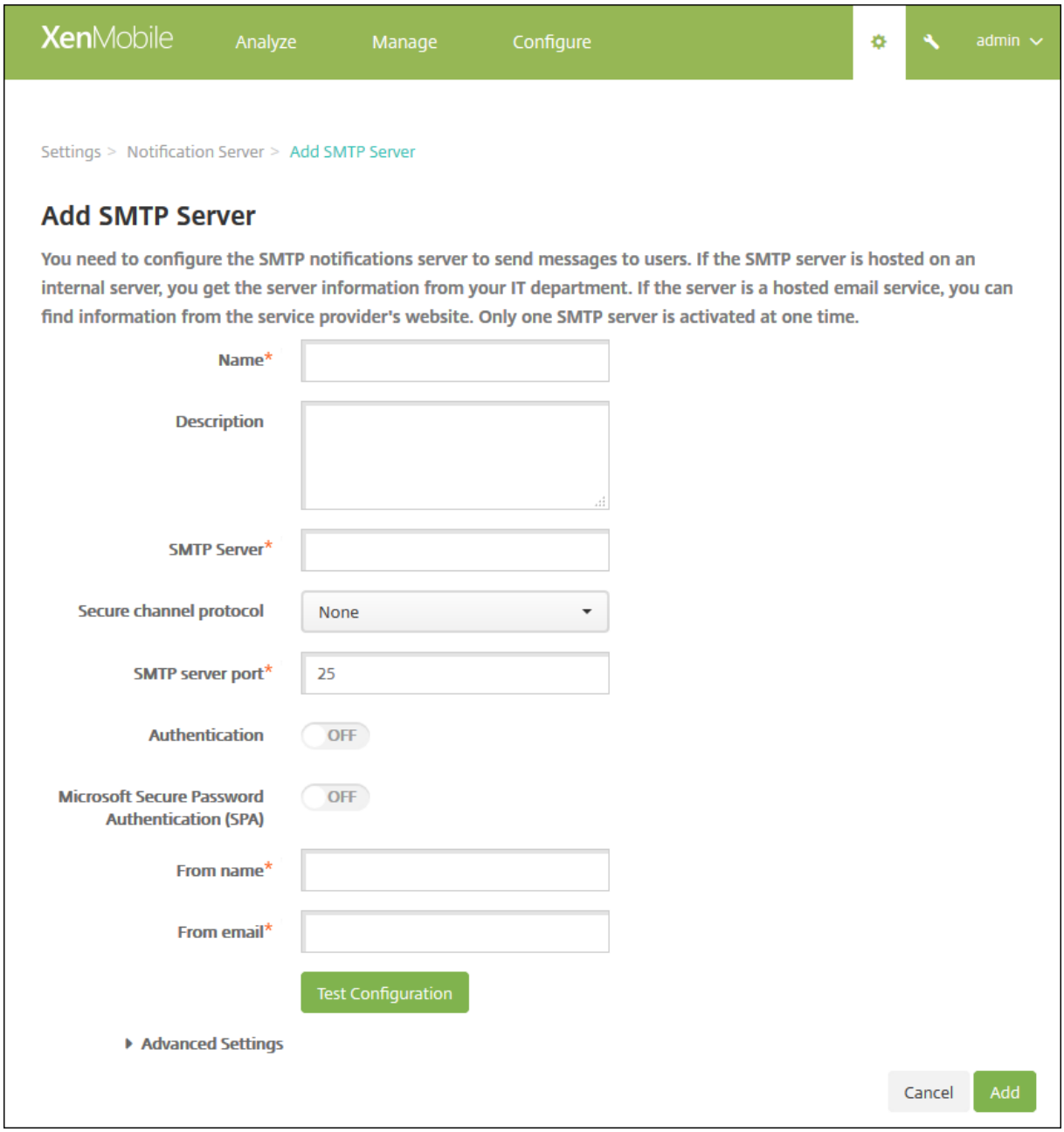


3. ［追加］ をクリックします。SMTP サーバーおよび SMS ゲートウェイを構成するためのオプションが含まれたメニューが開きます。



- SMTP サーバーを追加するには、［**SMTP** サーバー］ を選択します。この設定を構成する手順については、「SMTP サーバーを追加するには」を参照してください。
- SMS ゲートウェイを追加するには、［**SMS** ゲートウェイ］ を選択します。この設定を構成する手順については、「SMS ゲートウェイを追加するには」を参照してください。

SMTP サーバーの追加



1. 次の設定を構成します。

   - 名前: この SMTP サーバーアカウントに関連付ける名前を入力します。
   - 説明: 任意で、サーバーの説明を入力します。
   - **SMTP** サーバー: サーバーのホスト名を入力します。ホスト名には、完全修飾ドメイン名（FQDN）または IP を指定できます。
   - セキュアチャネルプロトコル: （サーバーが安全な認証を使用するよう構成されている場合）一覧から、サーバーが使用する適切なセキュアチャネルプロトコルとして［**SSL**］、［**TLS**］、または［なし］を

選択します。デフォルトは ［なし］ です。

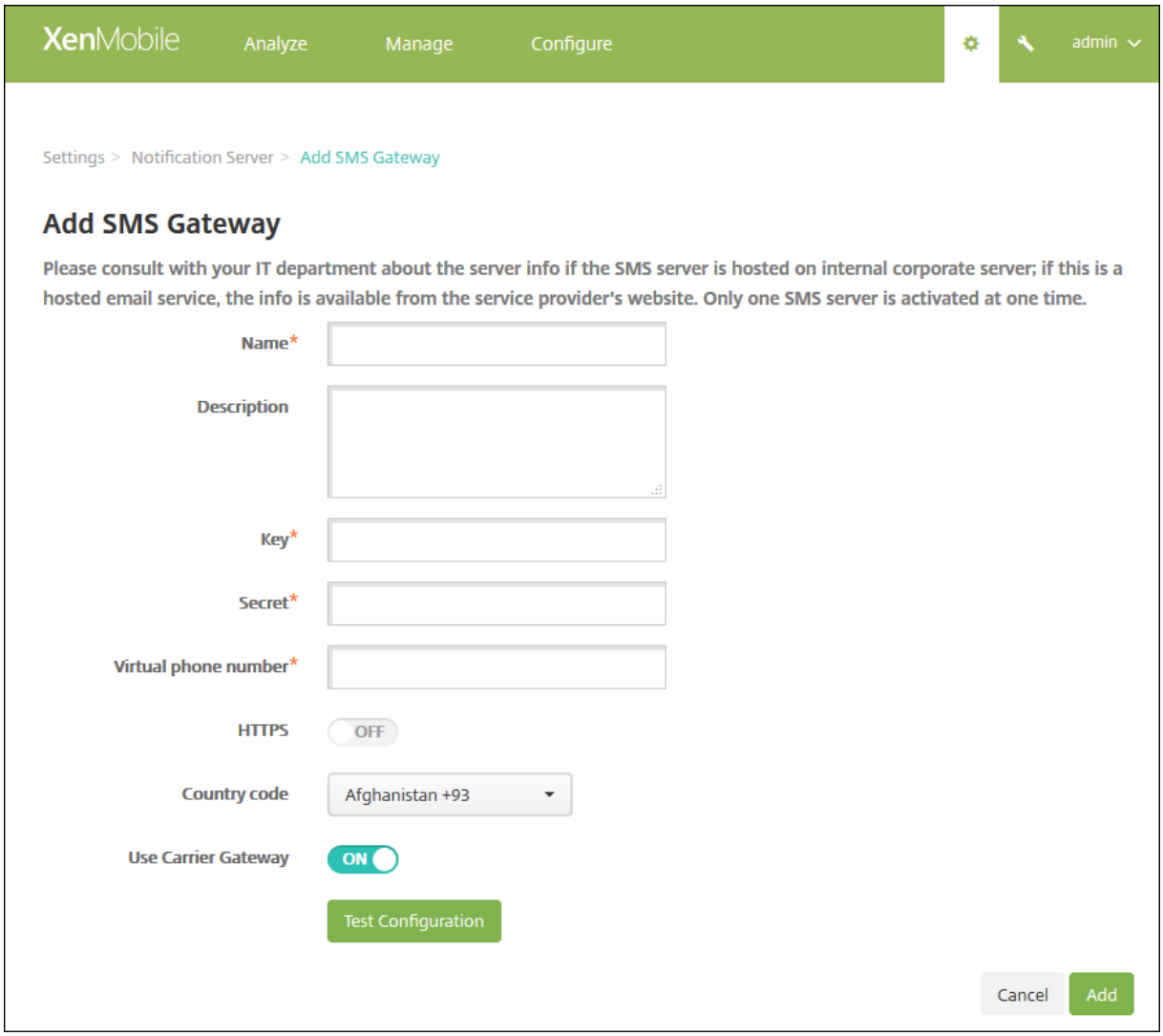
- **SMTP** サーバーポート: SMTP サーバーが使用するポートを入力します。デフォルトでは、ポートは 25 に設定されています。SMTP 接続で SSL セキュアチャネルプロトコルを使用する場合、ポートは 465 に設定されます。
- 認証: ［オン］ または ［オフ］ を選択します。デフォルトは ［オフ］ です。
- ［認証］ を有効にした場合は、次の設定を構成します。
  - ユーザー名: 認証に使用するユーザー名を入力します。
  - パスワード: 認証に使用するユーザーのパスワードを入力します。
- **Microsoft** セキュリティで保護されたパスワード認証（**SPA**）: SMTP サーバーが SPA を使用している場合は、［オン］ をクリックします。デフォルトは ［オフ］ です。
- 送信名: クライアントがこのサーバーから通知メールを受信したとき、メールの送信者として表示される名前を入力します。たとえば、「Corporate IT」です。
- 送信メールアドレス: SMTP サーバーによって送信された通知に、メール受信者が返信する場合に使用されるメールアドレスを入力します。

2. ［構成のテスト］ をクリックして、テストのメール通知を送信します。
3. ［詳細設定］ を展開して以下の設定を構成します。

- **SMTP** 再試行数: SMTP サーバーからのメッセージの送信が失敗した場合に再試行する回数を入力します。デフォルトは 5 です。
- **SMTP** タイムアウト: SMTP 要求送信時に待機する時間（秒）を入力します。送信しているメッセージが、タイムアウトに起因して失敗し続ける場合には、この値を大きくします。この値を小さくするとタイムアウト回数が多くなり、配信されないメッセージが増える場合があるため、注意してください。デフォルトは 30 秒です。
- 最大 **SMTP** 受信者数: SMTP サーバーによって送信される各電子メールメッセージの最大受信者数を入力します。デフォルトは 100 です。

4. ［追加］ をクリックします。

SMS ゲートウェイの追加



> 注：
>
> XenMobile は Nexmo SMS メッセージのみをサポートします。Nexmo メッセージを使用するためのアカウントがまだない場合は、Web サイトにアクセスしてアカウントを作成してください。

1. 次の設定を構成します：

   - 名前： SMS ゲートウェイ構成の名前を入力します。このフィールドは必須です。
   - 説明： 任意で、構成の説明を入力します。
   - キー： アカウントをアクティブ化するときにシステム管理者から提供された、数値形式の識別子を入力します。このフィールドは必須です。
   - シークレット： パスワードを紛失した場合や盗まれた場合にアカウントへのアクセスに使用する、システム管理者から提供されたシークレットを入力します。このフィールドは必須です。
   - 仮想電話番号： このフィールドは、北米の電話番号（プレフィックスが +1）への送信時に使用されます。Nexmo 仮想電話番号を入力する必要があります。このフィールドで使用できるのは、数字のみで

す。仮想電話番号は Nexmo の Web サイトで購入できます。

- **HTTPS**: Nexmo への SMS 要求の伝送に HTTPS を使用するかどうかを選択します。デフォルトは［オフ］です。

> 重要:
>
> HTTPS は、［オン］に設定してください（Citrix サポートから［オフ］に設定するよう指示があった場合を除く）。

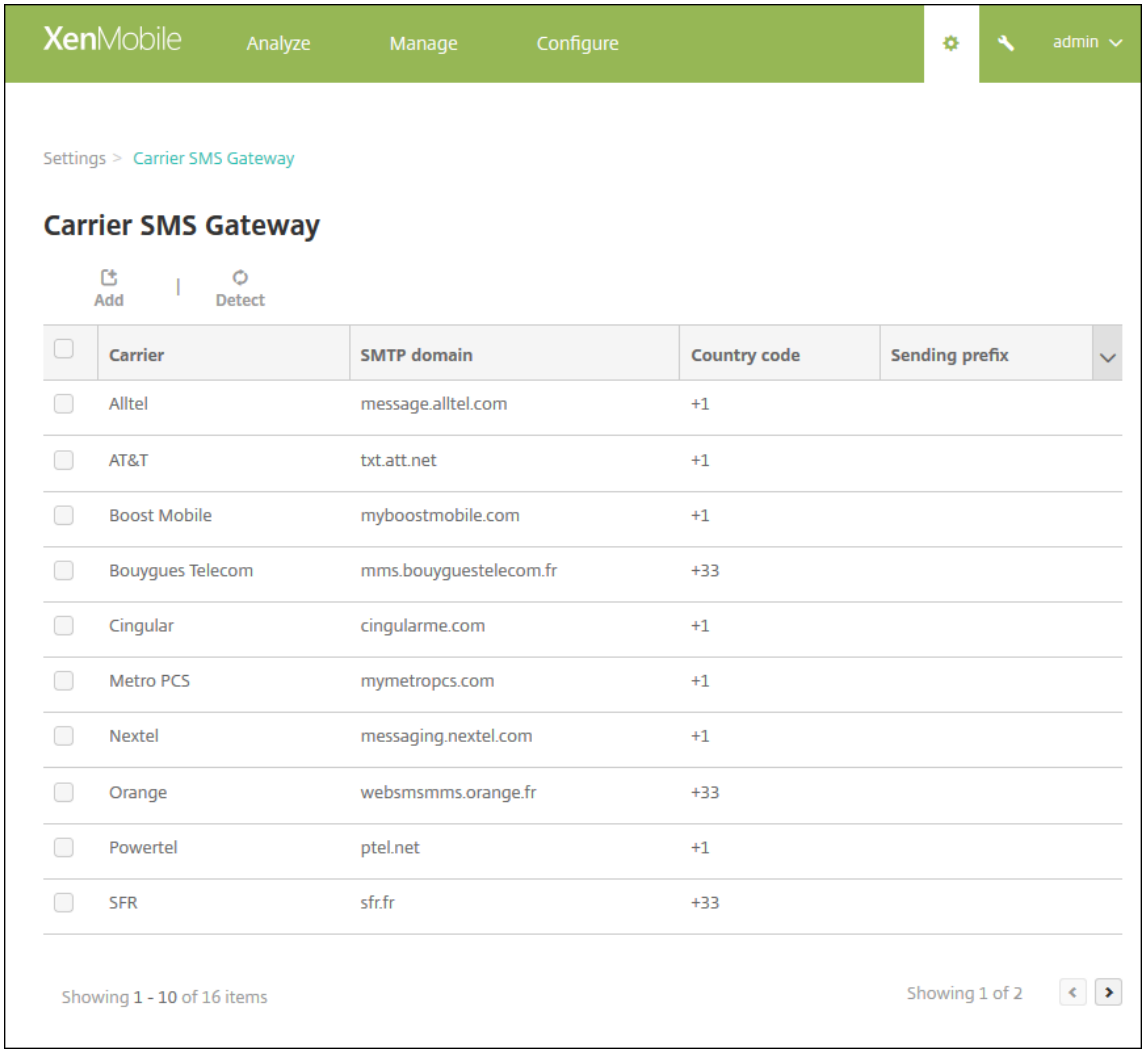
- 国コード: 一覧から、組織内受信者のデフォルトの SMS 国コードプレフィックスを選択します。このフィールドは常に + 記号で始まります。デフォルトは［アフガニスタン **+93**］です。

2. ［構成のテスト］をクリックし、現在の構成を使用してテストメッセージを送信します。認証エラーや仮想電話番号エラーなど、接続エラーが即時に検出され、表示されます。メッセージは、携帯電話間で送信された場合と同様の所要時間で受信されます。
3. ［追加］をクリックします。

キャリア **SMS** ゲートウェイの追加

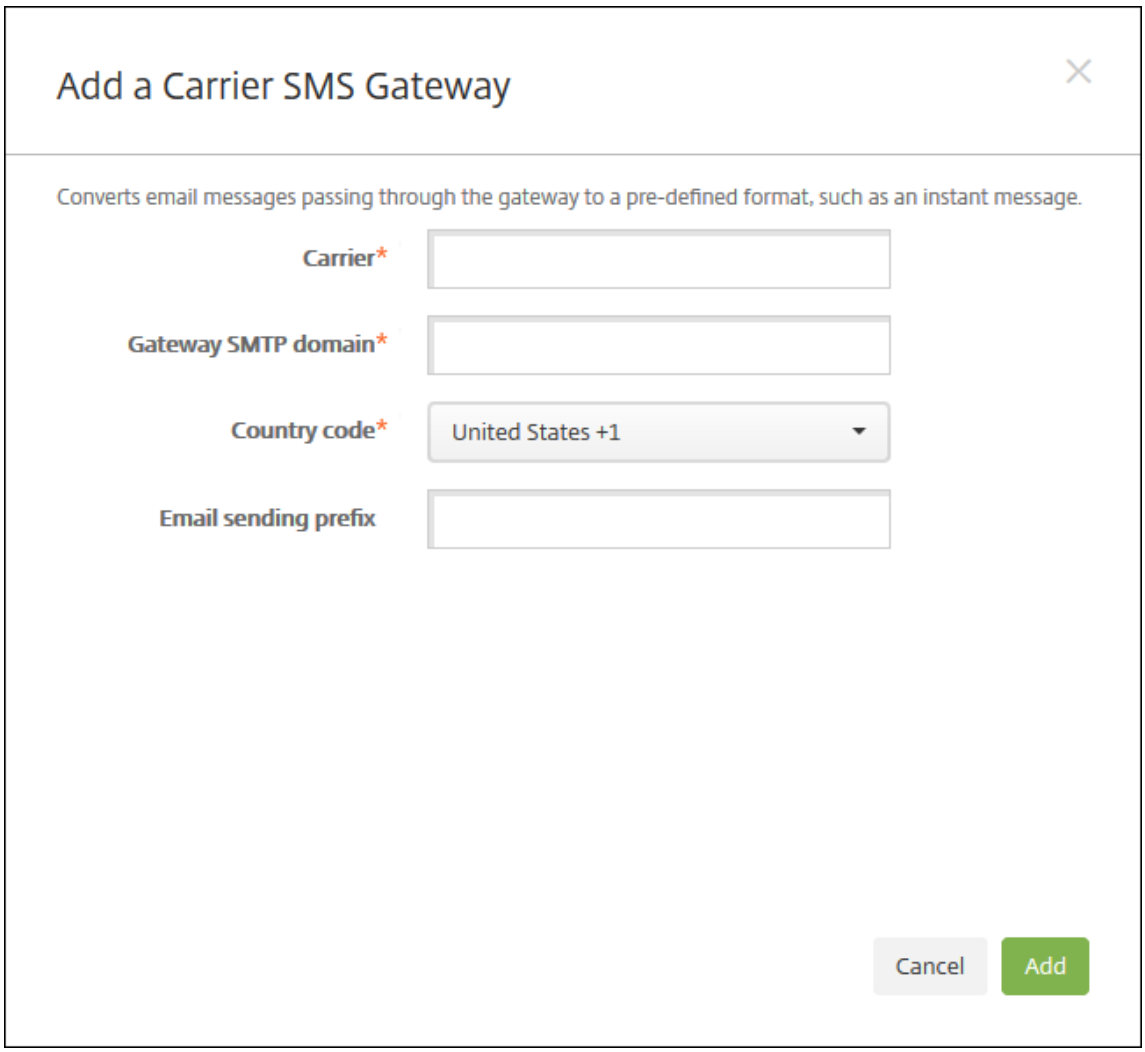
XenMobile でキャリア SMS ゲートウェイを設定して、電話会社の SMS ゲートウェイ経由で送信される通知を構成できます。電話会社はショートメッセージサービス（SMS）ゲートウェイを使用して、通信ネットワークと相互に SMS メッセージを送受信します。これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［通知］の下の［キャリア **SMS** ゲートウェイ］をクリックします。［キャリア **SMS** ゲートウェイ］ページが開きます。



3. 次のいずれかを行います:

   - ゲートウェイを自動的に検出するには ［検出］ をクリックします。新しいキャリアが検出されなかったことを示すダイアログボックス、または登録済みのデバイス間で検出された新しいキャリアを一覧表示したダイアログボックスが開きます。
   - ［追加］ をクリックします。［キャリア **SMS** ゲートウェイの追加］ ダイアログボックスが開きます。



> 注:
>
> XenMobile は Nexmo SMS メッセージのみをサポートします。Nexmo メッセージを使用するためのアカウントがまだない場合は、Web サイトにアクセスしてアカウントを作成してください。

4. 次の設定を構成します。
   - キャリア: 電話会社の名前を入力します。
   - ゲートウェイ **SMTP** ドメイン: SMTP ゲートウェイに関連付けられたドメインを入力します。
   - 国コード: 一覧から、電話会社の国コードを選択します。
   - メール送信プレフィックス: 任意で、メール送信プレフィックスを指定します。
5. [追加] をクリックして新しいキャリアを追加するか、[キャンセル] をクリックして操作を取り消します。

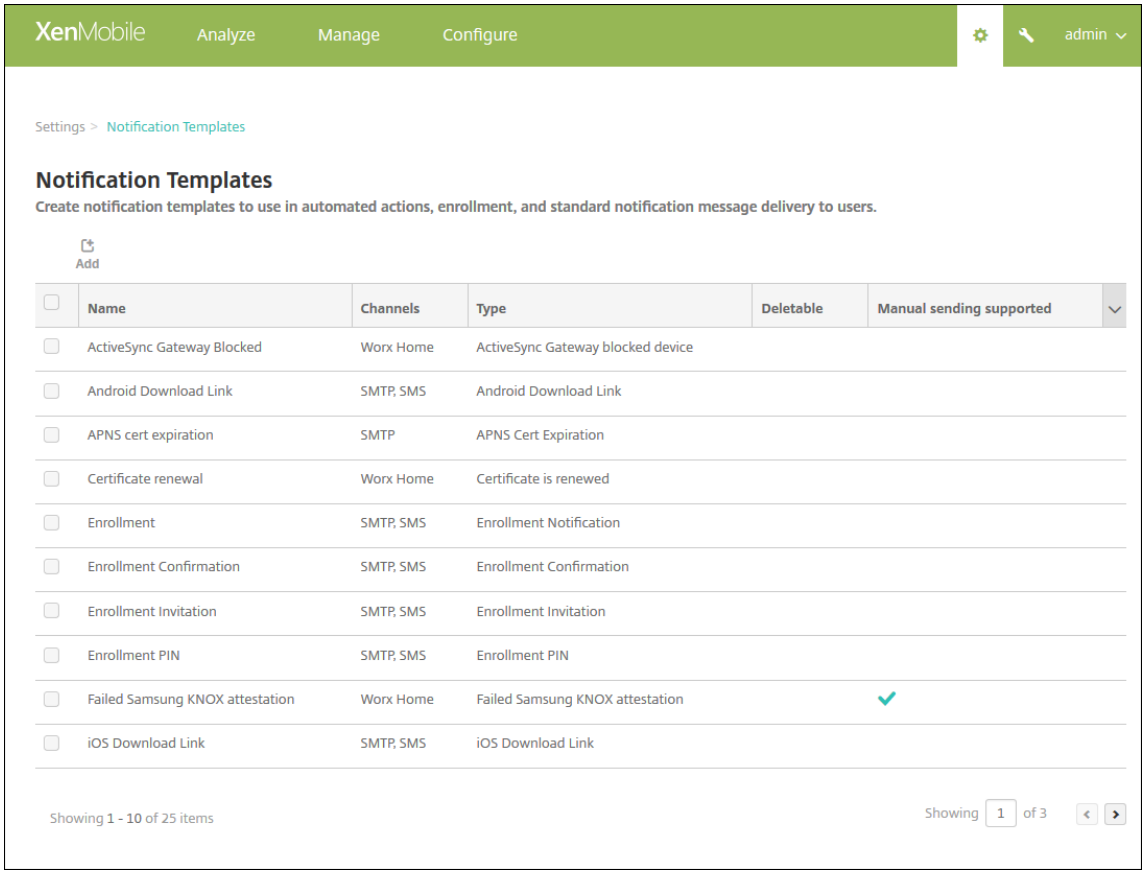
通知テンプレートの作成および更新

XenMobile で通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Secure Hub、SMTP、SMS の 3 つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。

XenMobile には、システム内のすべてのデバイスに対して XenMobile が自動的に応答する個別の種類のイベントを反映した、定義済みの通知テンプレートが多数用意されています。

> 注:
>
> SMTP または SMS チャネルを使用してユーザーに通知を送信する場合は、アクティブ化する前にチャネルを設定する必要があります。通知テンプレートを追加するときにチャネルがまだ設定されていないと、チャネルを設定するよう求めるメッセージが表示されます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［通知テンプレート］ をクリックします。［通知テンプレート］ ページが開きます。



通知テンプレートの追加

1. ［追加］ をクリックします。SMS ゲートウェイまたは SMTP サーバーが設定されていない場合、SMS および SMTP 通知に関するメッセージが表示されます。SMTP サーバーまたは SMS ゲートウェイを今すぐ設定する

か後で設定するかを選択できます。

SMS または SMTP サーバーを今すぐ設定することを選択した場合は、［設定］ページの ［通知サーバー］ページにリダイレクトされます。使用するチャネルを設定した後、［通知テンプレート］ ページに戻って、通知テンプレートの追加または変更を続けることができます。

> 重要：
>
> SMS または SMTP サーバーの設定を後で行うことを選択した場合、通知テンプレートの追加または編集のときにこれらのチャネルをアクティブ化することはできません。つまり、ユーザー通知の送信にこれらのチャネルを使用することができません。

2. 次の設定を構成します。

   - 名前： テンプレートの説明的な名前を入力します。
   - 説明： テンプレートの説明を入力します。
   - 種類： 一覧から、通知の種類を選択します。選択した種類でサポートされるチャネルのみが表示されます。定義済みテンプレートである［APNs 証明書の有効期限］テンプレートは 1 つだけ使用できます。つまり、この種類の新しいテンプレートは追加できません。

   > 注：
   >
   > テンプレートの種類の一部では、種類の下に［マニュアル送信がサポートされています］が表示されます。これは、このテンプレートが ［ダッシュボード］ および ［デバイス］ ページの ［通知］ 一覧に表示され、手動でユーザーに通知を送信できることを意味します。いずれのチャネルの場合も、［件名］フィールドまたは［メッセージ］フィールドに以下のマクロが使われているテンプレートでは、手動送信は使用できません。

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

3. ［チャネル］ で、この通知で使用される各チャネルの情報を構成します。一部またはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。

   - ［**Secure Hub**］ を選択した場合、iOS デバイスおよび Android デバイスのみが通知を受信し、通知はデバイスの通知トレイに表示されます。
   - ［**SMTP**］ を選択した場合、ほとんどのユーザーはメールアドレスを使って登録するため、ほとんどのユーザーがメッセージを受信します。
   - ［**SMS**］ を選択した場合、SIM カードが搭載されたデバイスのユーザーのみが通知を受信します。

   Secure Hub:

   - アクティブ化： クリックして通知チャネルを有効にします。
   - メッセージ： ユーザーに送信されるメッセージを入力します。Secure Hub を使用する場合、このフィールドは必須です。メッセージでのマクロの使用について詳しくは、「マクロ」を参照してください。
   - 音声ファイル： 一覧から、ユーザーが通知を受信したときに再生される通知音を選択します。

   SMTP:

- アクティブ化: クリックして通知チャネルを有効にします。

  SMTP サーバーをセットアップした後でのみ、SMTP 通知をアクティブ化できます。

- 差出人: 任意で、通知の送信者（名前、メールアドレス、またはその両方）を入力します。
- 受信者: このフィールドには、アドホック通知を除くすべての通知で、通知が正しい SMTP 受信者アドレスに送信されるようにするためのマクロが事前設定されています。テンプレートのマクロは変更しないでください。アドレスをセミコロン（;）で区切って追加することにより、ユーザー以外の受信者（社内の管理者など）を追加することもできます。アドホック通知を送信するには、このページで個別に受信者を入力するか、［管理］**>**［デバイス］ ページでデバイスを選択して、そこから通知を送信します。詳しくは、「デバイス」を参照してください。
- 件名: 通知の説明的な件名を入力します。このフィールドは必須です。
- メッセージ: ユーザーに送信されるメッセージを入力します。メッセージでのマクロの使用について詳しくは、「マクロ」を参照してください。

SMS:

- アクティブ化: クリックして通知チャネルを有効にします。

  SMTP サーバーをセットアップした後でのみ、SMTP 通知をアクティブ化できます。

- 受信者: このフィールドには、アドホック通知を除くすべての通知で、通知が正しい SMS 受信者アドレスに送信されるようにするためのマクロが事前設定されています。テンプレートのマクロは変更しないでください。アドホック通知を送信するには、個別に受信者を入力するか、［管理］**>**［デバイス］ ページでデバイスを選択します。
- メッセージ: ユーザーに送信されるメッセージを入力します。このフィールドは必須です。メッセージでのマクロの使用について詳しくは、「マクロ」を参照してください。

4. ［追加］ をクリックします。すべてのチャネルが正しく構成されている場合、［通知テンプレート］ ページに、SMTP、SMS、Secure Hub の順に表示されます。正しく構成されていないチャネルがあれば、正しく構成されているチャネルの後に表示されます。

通知テンプレートの編集

1. 通知テンプレートを選択します。選択したテンプレートに固有の編集ページが開き、［種類］ フィールド以外のすべてを変更することができます。チャネルをアクティブ化または非アクティブ化することもできます。
2. ［保存］ をクリックします。

通知テンプレートの削除

追加した通知テンプレートのみを削除できます。事前定義済みの通知テンプレートは削除できません。

1. 既存の通知テンプレートを選択します。
2. ［削除］ をクリックします。確認ダイアログボックスが開きます。
3. ［削除］ をクリックして通知テンプレートを削除するか、［キャンセル］ をクリックして通知テンプレートの削除を取り消します。

デバイス

August 22, 2019

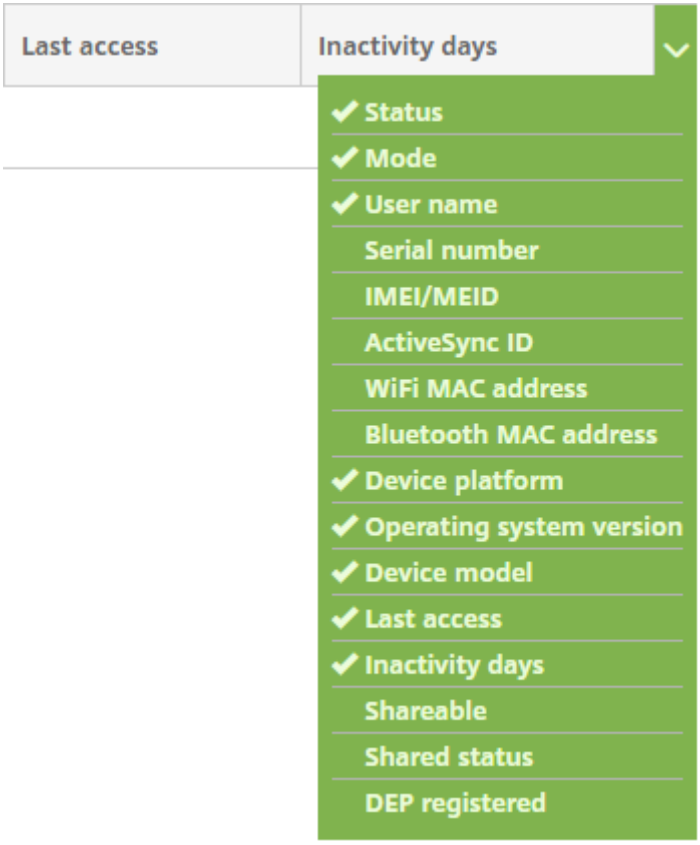
Citrix XenMobile では、単一の管理コンソール内で、幅広いタイプのデバイスの管理、セキュリティ保護、インベントリを行うことができます。

XenMobile サーバーのデータベースには、モバイルデバイスの一覧が保存されます。各モバイルデバイスは、一意のシリアル番号または IMEI（International Mobile Station Equipment Identity）/MEID（Mobile Equipment Identifier）識別番号によって定義されます。XenMobile コンソールにデバイスを追加するには、手動でデバイスを追加するか、ファイルからデバイスの一覧をインポートします。デバイスプロビジョニングファイル形式について詳しくは、後述の「デバイスプロビジョニングファイル形式」を参照してください。

XenMobile コンソールの ［デバイス］ ページは、各デバイスおよび以下の情報を表示します。

- 状態：デバイスがジェイルブレイクされているか、管理されているか、Active Sync Gateway が使用可能か、およびデバイスの展開環境の状態などを示すアイコンです。
- モード： デバイスのモードが MDM、MAM、またはその両方かを示します。
- ほかに、次のようなデバイスの情報を表示できます：ユーザー名、デバイスプラットフォーム、オペレーティングシステムバージョン、デバイスモデル、最終アクセス日時、非アクティブ日数。これらの見出しは、デフォルトで表示されます。

［デバイス］ の表をカスタマイズするには、見出しの右端の下向き矢印をクリックします。次に、その表に表示する追加の見出しをオンにするか、または削除する見出しをオフにします。

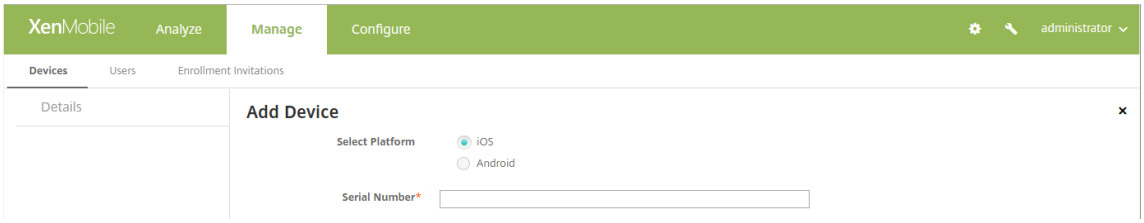


手動によるデバイスの追加、デバイスプロビジョニングファイルからのデバイスのインポート、デバイスの詳細の編集、セキュリティの操作の実行、デバイスへの通知の送信を行うことができます。デバイス表のデータ全体を.csv ファイルにエクスポートして、このファイルからカスタムレポートを作成することもできます。サーバーはすべてのデバイス属性をエクスポートします。フィルターを適用している場合、XenMobile は.csv ファイルの作成時にそのフィルターを使用します。

手動によるデバイスの追加

1. XenMobile コンソールで、［管理］**>**［デバイス］ の順にクリックします。［デバイス］ ページが開きます。

2. ［追加］ をクリックします。［デバイスの追加］ ページが開きます。



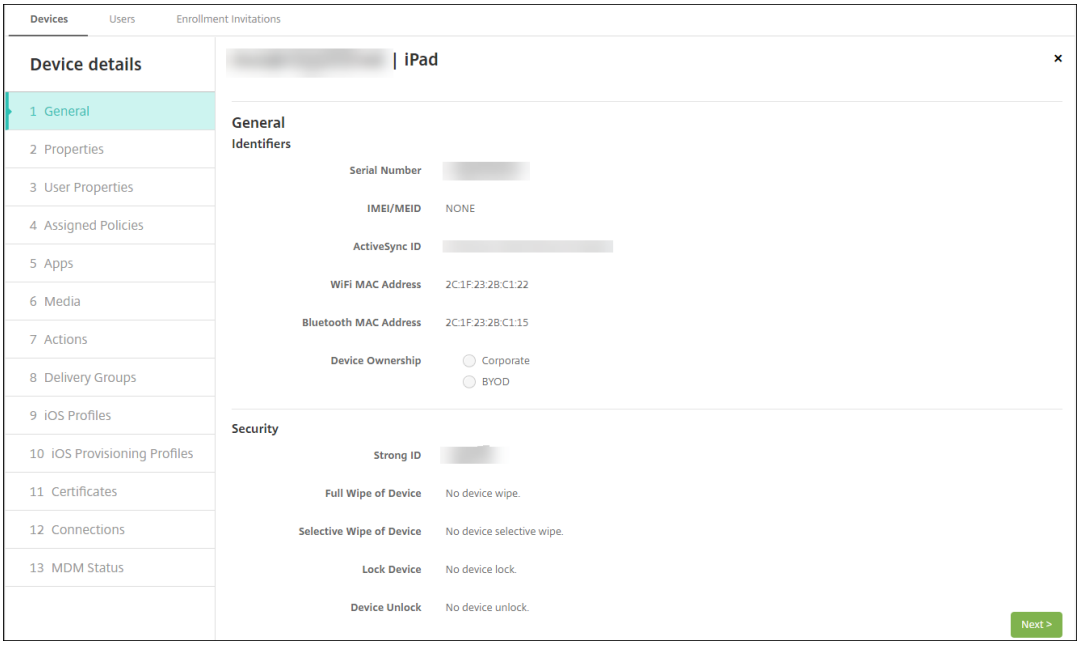
3. 次の設定を構成します。

   - プラットフォーム選択： ［**iOS**］ または ［**Android**］ を選択します。
   - シリアル番号： デバイスのシリアル番号を入力します。
   - **IMEI/MEID**： Android デバイスに限り、任意で、デバイスの IMEi/MEID 情報を入力します。

4. ［追加］ をクリックします。［デバイス］ の表に示される一覧の一番下に、追加したデバイスが表示されます。追加したデバイスを選択して表示されるメニューで ［編集］ をクリックし、デバイスの詳細を表示して確認します。

   > 注：
   >
   > デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

   - Enterprise（XME）モードまたは MDM モードで構成された XenMobile Server
   - 構成された LDAP
   - ローカルグループおよびローカルユーザーを使用する場合：
     - 1 つまたは複数のローカルグループ。
     - ローカルグループに割り当てられたローカルユーザー。
     - デリバリーグループはローカルグループと関連付けられます。
   - Active Directory を使用する場合：
     - デリバリーグループは Active Directory グループと関連付けられます。



5. ［一般］ ページには、シリアル番号、ActiveSync ID、プラットフォームの種類に関するその他の情報など、デバイスの識別子が表示されます。［デバイス所有権］ で、［コーポレート］ または ［**BYOD**］ を選択します。

   ［一般］ ページには、デバイスの ［セキュリティ］ プロパティ（[Strong ID]、［デバイスのロック］、［アクティベーションロックバイパス］、プラットフォームの種類に関するその他の情報など）も表示されます。［デバイスの完全なワイプ］ フィールドには、ユーザーの PIN コードが含まれます。デバイスがワイプされた後、ユーザーはこのコードを入力する必要があります。ユーザーがコードを忘れた場合は、こちらで確認できます。

6. ［プロパティ］ ページには、XenMobile がプロビジョニングするデバイスのプロパティが表示されます。この一覧は、デバイスの追加に使用されるプロビジョニングファイルに含まれるデバイスのプロパティを表示します。プロパティを追加するには、［追加］ をクリックして一覧からプロパティを選択します。各プロパティの有効な値に関しては、デバイスのプロパティ名と値に関する PDF を参照してください。

   プロパティを追加すると、最初に追加したカテゴリに表示されます。［次へ］ をクリックして ［プロパティ］ ページに戻ると、プロパティは適切な一覧に表示されます。

   プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の［**X**］をクリックします。XenMobile デバイスがその項目を検出します。

7. 残りの ［デバイス詳細］ セクションには、デバイスの概要が表示されます。

   - ユーザープロパティ： ユーザーの RBAC の役割、グループメンバーシップ、VPP アカウント、およびプロパティを表示します。このページでインベントリから VPP アカウントを削除できます。
   - 割り当て済みポリシー： 展開済み、保留中、失敗したポリシーの数を含む、割り当て済みポリシーの数が表示されます。各ポリシーの名前、種類、最新展開の情報が表示されます。
   - アプリ： インストール済み、保留中、失敗のアプリ展開数を含む、最新のインベントリ時点のアプリ数が表示されます。アプリ名、ID、種類、その他の情報が表示されます。
   - メディア： 展開済み、保留中、失敗のメディア展開数を含む、最新のインベントリ時点のメディア数が

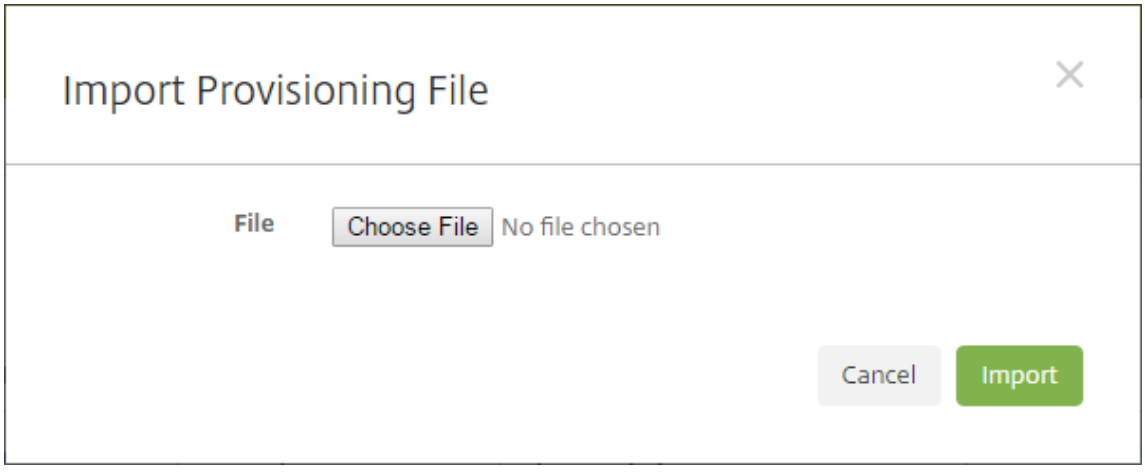
表示されます。

- 操作: 展開済み、保留中、失敗のアクション数を含む、アクション数が表示されます。最新展開のアクション名と時間が表示されます。
- デリバリーグループ: 成功、保留中、失敗したデリバリーグループの数が表示されます。各展開のデリバリーグループ名と展開時間が表示されます。デリバリーグループを選択すると、状態、アクション、チャネル、またはユーザーなどの詳細な情報を表示できます。
- **iOS** プロファイル: 名前、種類、組織、説明など、最新の iOS プロファイルインベントリが表示されます。
- **iOS** プロビジョニングプロファイル: UUID、有効期限、管理対象かどうかなど、エンタープライズ配布プロビジョニングプロファイルの情報を表示します。
- 証明書: 有効な証明書と期限切れまたは失効した証明書が表示され、種類、プロバイダー、発行者、シリアル番号、期限切れまでの残日数などの情報も表示されます。
- 接続: 最初の接続状態と最後の接続状態が表示されます。各接続のユーザー名、最後から 2 番目の認証時間、最後の認証時間が表示されます。
- **MDM** ステータス: MDM ステータス、最後のプッシュ時間、最後のデバイス応答時間などの情報が表示されます。
- **TouchDown**: (Android デバイスのみ) 最後のデバイス認証と最後のユーザー認証の情報が表示されます。それぞれ該当するポリシー名とポリシー値が表示されます。

デバイスプロビジョニングファイルからのデバイスのインポート

モバイル事業者やデバイス製造元が提供するファイルをインポートしたり、独自のデバイスプロビジョニングファイルを作成したりすることができます。詳しくは、後述の「デバイスプロビジョニングファイル形式」を参照してください。

1. [管理] > [デバイス] に移動して、[インポート] を選択します。[プロビジョニングファイルのインポート] ダイアログボックスが開きます。



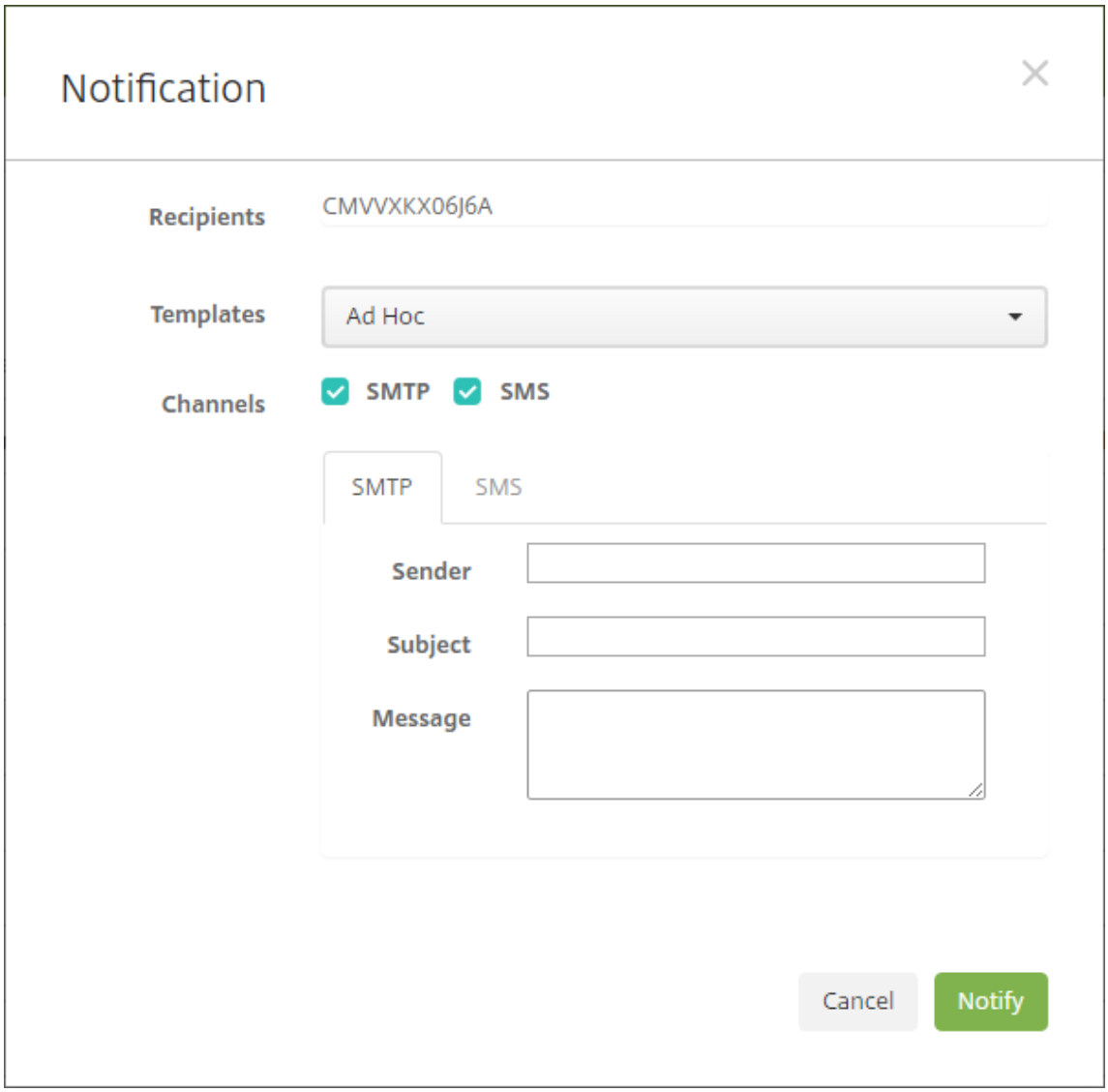
2. [ファイルの選択] を選択して、インポートするファイルまで移動します。

3. ［インポート］ をクリックします。インポートされたファイルが ［デバイス］ の表に追加されます。
4. デバイスの情報を編集するには、［デバイス詳細］を選択して ［編集］ をクリックします。［デバイス詳細］ページについて詳しくは、「手動によるデバイスの追加」を参照してください。

デバイスに通知を送信する

［デバイス］ページで、デバイスに通知を送信できます。通知について詳しくは、「通知」を参照してください。

1. ［管理］ > ［デバイス］ ページで、通知を送信するデバイスを選択します。
2. ［通知］ をクリックします。［通知］ ダイアログボックスが開きます。［受信者］ フィールドに、通知を受信するすべてのデバイスの一覧が表示されます。



3. 次の設定を構成します。

- テンプレート: 一覧から、送信する通知の種類を選択します。［アドホック］ を選択した場合を除き、［件名］ フィールドおよび ［メッセージ］ フィールドには、選択したテンプレートで構成済みのテキストが入力されます。
- チャネル: メッセージの送信方法を選択します。デフォルトは ［**SMTP**］ および ［**SMS**］ です。各チャネルのメッセージの形式を表示するには、タブをクリックします。
- 差出人: オプションで送信者を入力します。
- 件名: ［アドホック］ メッセージの場合、件名を入力します。
- メッセージ: ［アドホック］ メッセージの場合、メッセージを入力します。

4. ［通知］ をクリックします。

［デバイス］の表のエクスポート

1. エクスポートファイルで表示する内容によって、［デバイス］ の表にフィルターを適用します。
2. ［デバイス］ の表の上にある ［エクスポート］ をクリックします。XenMobile によって ［デバイス］ の表の情報が抽出され、.csv ファイルに変換されます。
3. .csv ファイルを開くか、保存します。

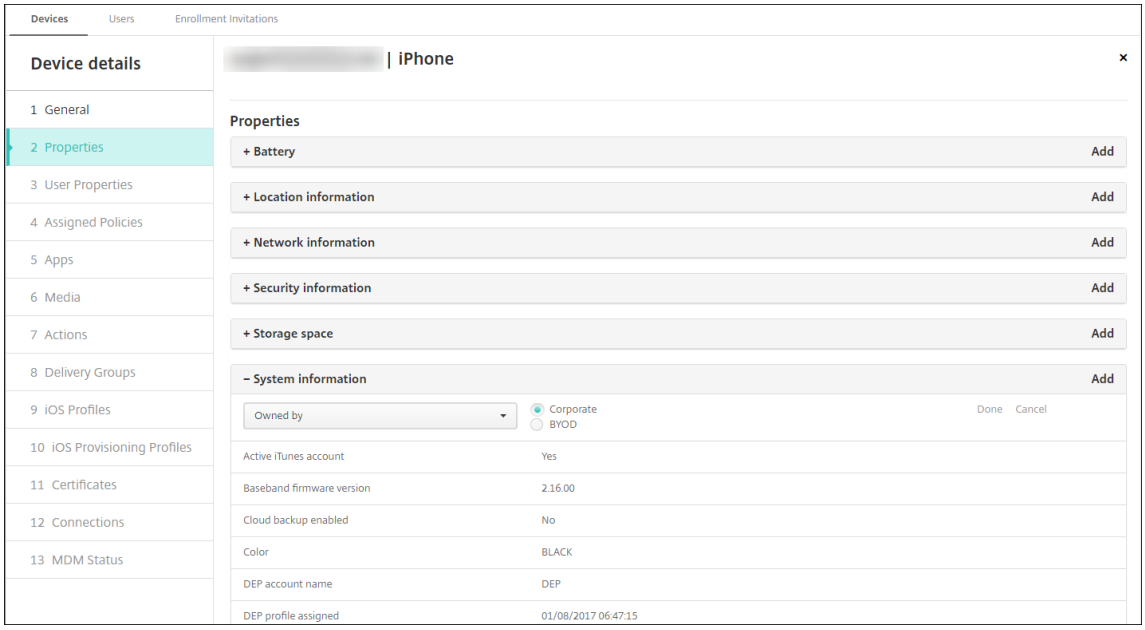
ユーザーデバイスの手動タグ付け

次のいずれかの方法で、XenMobile のデバイスに手動でタグ付けすることができます。

- 招待状に基づく登録処理中
- Self Help Portal 登録処理中
- デバイスの所有権をデバイスプロパティとして追加する

組織または個人所有のいずれかとして、デバイスにタグ付けするオプションが用意されています。Self Help Portal を使ってデバイスを自動登録するときに、組織または個人所有のいずれかとして、デバイスにタグを付けることができます。以下のように手動でデバイスにタグを付けることもできます。

1. XenMobile コンソールの ［デバイス］ タブから、プロパティをデバイスに追加します。
2. ［所有者］ という名前のプロパティを追加し、［コーポレート］ か ［**BYOD**］（個人所有）のいずれかを選択します。



デバイスプロビジョニングファイル形式

携帯電話会社またはデバイス製造業者の多くが公認のモバイルデバイスの一覧を提供しています。この一覧を使用することで、モバイルデバイスの長い一覧を手動で入力することを避けることができます。XenMobile は、Android、iOS、Windows の 3 種類のサポート対象デバイスすべてに共通のインポートファイル形式をサポートしています。

手動で作成し、XenMobile へのデバイスのインポートに使用するプロビジョニングファイルは次の形式である必要があります。

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2;… propertyNameN;propertyValueN

次のことに注意してください:

- 各プロパティの有効な値に関しては、デバイスのプロパティ名と値に関する PDF を参照してください。
- UTF-8 形式の文字セットを使用します。
- プロビジョニングファイル内では、フィールドをセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。

  例えば、このプロパティの場合は次のようになります:

  ```
  propertyV;test;1;2
  ```

  以下のようにエスケープします:

  ```
  propertyV\;test\;1\;2
  ```

- シリアル番号は iOS デバイスの識別子であるため、iOS デバイスにはシリアル番号が必須です。
- その他のデバイスプラットフォームの場合、シリアル番号または IMEI が必要です。

- **OperatingSystemFamily** の有効な値は、**WINDOWS**、**ANDROID**、**iOS** のいずれかです。

デバイスプロビジョニングファイルの例:

```
‘1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;
   propertyV$*&&éééétest
3050BF3F51730108161006551059039l;35244201625379903;iOS;test;
4050BF3F51730108161006551059039l;;iOS;test;
;55244201625379903;ANDROID;test.testé;value;‘
```

ファイルの各行にデバイスの説明が含まれています。上のサンプルの最初のエントリは以下を意味しています:

- シリアル番号: 1050BF3F51730108161006551059039l
- IMEI: 15244201625379901
- オペレーティングシステムファミリ: WINDOWS
- プロパティ名: propertyN
- プロパティ値: propertyV\;test\;1\;2;prop 2

ActiveSync ゲートウェイ

August 22, 2019

ActiveSync は、Microsoft が開発したモバイルデータ同期プロトコルです。ActiveSync は、ハンドヘルドデバイスやデスクトップ（またはラップトップ）コンピューターとデータを同期します。

XenMobile で ActiveSync ゲートウェイの規則を構成できます。これらの規則に基づいて、デバイスの ActiveSync データへのアクセスを許可または拒否することができます。たとえば、［不足必須アプリ］の規則をアクティブ化した場合、XenMobile は必須アプリのアプリアクセスポリシーをチェックし、必須アプリが不足している場合は ActiveSync データへのアクセスを拒否します。規則ごとに、［許可］ または ［禁止］ を選択できます。デフォルト設定は、［許可］です。

アプリアクセスポリシーについて詳しくは、「アプリアクセスデバイスポリシー」を参照してください。

XenMobile では、次の規則がサポートされます。

匿名デバイス： デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときに XenMobile がユーザーを再認証できない場合に使用できます。

Samsung KNOX 構成証明に失敗しました： デバイスが、Samsung KNOX 構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ： デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。

暗示的許可および拒否: このアクションは、ActiveSync ゲートウェイのデフォルトです。その他のフィルター規則条件に合致しないすべてのデバイスの一覧が作成され、この一覧に基づいて接続が許可または拒否されます。いずれの規則にも合致しない場合、デフォルトは黙示的な許可です。

非アクティブデバイス: ［サーバープロパティ］でデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。

不足必須アプリ: デバイスにアプリアクセスポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ: デバイスにアプリアクセスポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード: ユーザーパスワードが正しいかを確認します。iOS デバイスおよび Android デバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかを XenMobile が確認できます。例えば、iOS では、XenMobile がデバイスにパスコードポリシーを送信する場合、ユーザーは 60 分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

コンプライアンス外デバイス: ［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス違反かどうかを確認します。通常、このプロパティは自動化された操作により変更されるか、XenMobile API を利用するサードパーティにより変更されます。

失効状態: デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

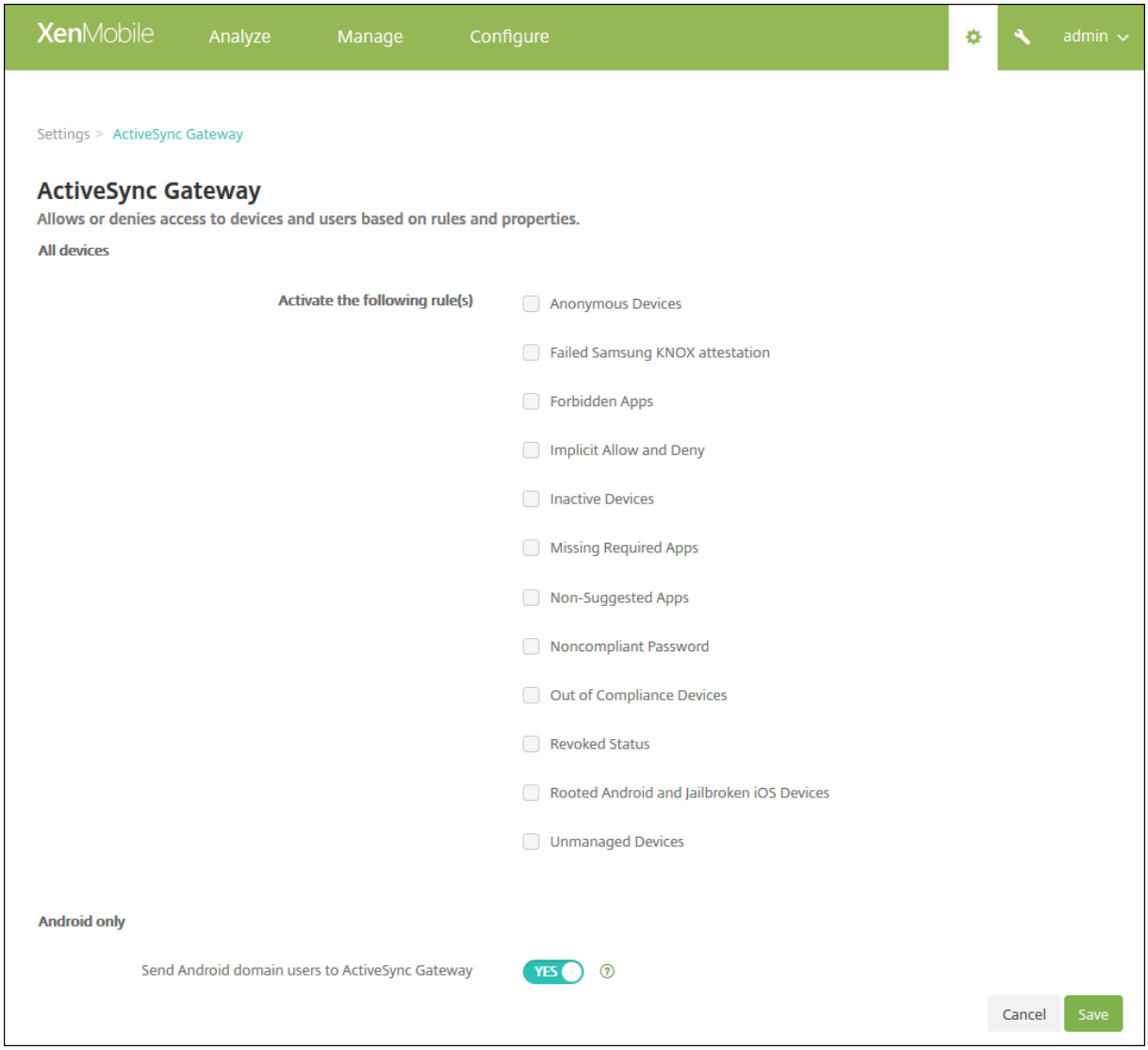
ルート化された **Android** およびジェイルブレイクした **iOS** デバイス: Android または iOS デバイスがジェイルブレイクされていないかを確認します。

非管理デバイス: デバイスがまだ XenMobile の管理下にあるかを確認します。例えば、MAM モードで実行されているデバイスや未登録のデバイスは管理されていません。

Android ドメインユーザーを **ActiveSync Gateway** に送信: XenMobile によって Android デバイスの情報が ActiveSync ゲートウェイに送信されるようにするには、［はい］ をクリックします。

ActiveSync ゲートウェイ設定を構成するには

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**ActiveSync** ゲートウェイ］ をクリックします。［**ActiveSync** ゲートウェイ］ ページが開きます。



1. ［次の規則をアクティブ化］ で、有効にするルールを 1 つまたは複数オンにします。
2. ［**Android** のみ］の［**Android** ドメインユーザーを **ActiveSync Gateway** に送信］で［はい］をクリックし、XenMobile によって Android デバイスの情報が Secure Mobile Gateway に送信されるようにします。
3. ［保存］ をクリックします。

Device Administration から **Android Enterprise** への移行

January 10, 2020

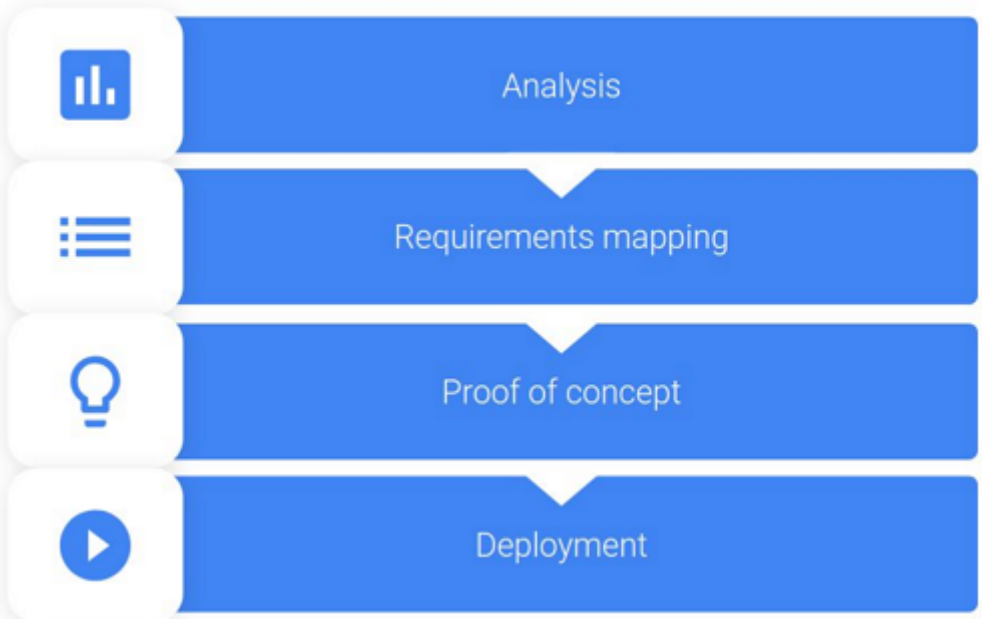
この記事では、従来の Android デバイス管理から Android Enterprise への移行に関する考慮事項と推奨事項について説明します。Google は Android Device Administration API を廃止します。この API は、Android デバイ

ス上のエンタープライズアプリをサポートしていました。Android Enterprise は、Google と Citrix が推奨する最新の管理ソリューションです。

XenMobile は Android Enterprise に変更され、これが Android デバイスのデフォルトの登録方法となります。Google がこの API を廃止した後は、Android Q デバイスはデバイス管理モードで登録できなくなります。

Android Enterprise では、完全管理デバイスモードと仕事用プロファイルデバイスモードがサポートされます。Google のドキュメント『Android Enterprise Migration Bluebook』で、従来のデバイス管理と Android Enterprise の違いについて詳しく説明しています。Google が提供する移行に関する情報を参照していただくことをお勧めします。

このドキュメントでは、デバイス管理の移行の 4 つのフェーズについても説明しており、次の図が含まれています。この記事には、移行フェーズの XenMobile に固有の推奨事項が含まれています。



『Android Enterprise Migration Bluebook』に掲載の図
Google の許可を得て再発行。

デバイス管理の廃止の影響

Google は、次のデバイス管理 API を廃止します。Secure Hub を Android Q API レベルを対象にしてアップグレードすると、以下の API は Android Q が稼働するデバイスでは機能しなくなります：

- カメラの無効化：デバイスのカメラへのアクセスを制御します。
- Keyguard 機能：生体認証やパターンなど、デバイスのロックに関連する機能を制御します。
- パスワードの有効期限切れ：設定可能な期間が過ぎると、ユーザーはパスワードの変更を強制されます。
- パスワードの制限：パスワードの制限要件を設定します。

この API の廃止は、Citrix MAM-only モードで登録されたデバイスには影響ありません。

推奨事項

次の推奨事項は、Android の従来のデバイス管理モードで既に登録されているデバイス、未登録のデバイス、および Citrix MAM-only モードで登録されているデバイス向けです。

デバイス登録ステータス	推奨される操作
既存のデバイスがデバイス管理モードで登録されており、Android Q にアップグレード可能。	デバイスを Android Q にアップグレードする前に、デバイス管理モードから Android Enterprise に移行します。
既存のデバイスがデバイス管理モードで登録されている。デバイスは Android Q にアップグレードできない。	デバイスはデバイス管理モードのままにできます。ただし、デバイスの更新時にデバイスの Android Enterprise への移行を計画してください。
既存のデバイスがデバイス管理モードで登録されており、Android Q にアップグレードされる。	Google が API を廃止する前に、デバイス管理モードから Android Enterprise に移行します。これらのデバイスの警告メッセージが XenMobile コンソールに表示されます。
Android Q が搭載された、デバイス管理モードで登録された新しいデバイス。	Google が API を廃止する前に、デバイス管理モードから Android Enterprise に移行します。これらのデバイスの警告メッセージが XenMobile コンソールに表示されます。
Android Q が搭載された、または Android Q にアップグレード可能な新しいデバイス。デバイスは未登録。	新しいデバイスには Android Enterprise を使用します。
Google が API を廃止した後には、Android Q が搭載された新規または既存のデバイスはデバイス管理モードで登録されます。	Google API の廃止の影響を回避するために、Google が API を廃止する前に Android Enterprise に移行することをお勧めします。廃止日以降には、これらのデバイスの登録は失敗します。
Citrix MAM-only モードで登録された新規または既存のデバイス。	対応は不要です。この Google API の廃止は、MAM-only モードのデバイスには影響ありません。

分析

移行の分析フェーズでは以下を行います:

- 従来の Android 設定を把握する
- 従来の機能と Android Enterprise の機能をマッピングできるように、従来の設定を文書化する

推奨される分析

1. XenMobile 上で Android Enterprise を評価します：完全管理、仕事用プロファイルでの完全管理、専用デバイス、仕事用プロファイル（BYOD）。
2. 現在のデバイス管理機能を Android Enterprise と比較して分析します。
3. デバイス管理のユースケースを文書化します。

デバイス管理のユースケースを文書化するには：

1. スプレッドシートを作成し、XenMobile コンソールに現在のポリシーグループを表示します。
2. 既存のポリシーグループに基づいて個別のユースケースを作成します。
3. ユースケースごとに、以下を文書化します：
    - 名前
    - ビジネス責任者
    - ユーザー ID モデル
    - デバイスの要件
        - セキュリティ
        - 管理
        - 使いやすさ
    - デバイスインベントリ
        - 製造元とモデル
        - OS のバージョン
    - アプリ
4. アプリごとに、以下を示します：
    - アプリ名
    - パッケージ名
    - ホスティング方法
    - アプリがパブリックかプライベートか
    - アプリが必須かどうか（真/偽）

要件マッピング

分析結果に基づいて、Android Enterprise の機能要件を決定します。

推奨される要件マッピング

1. 管理モードと登録方法を決定します：
    - 仕事用プロファイル（BYOD）：再登録が必要です。工場出荷時リセットは不要です。

- 完全管理：工場出荷時リセットが必要です。QR コード、近距離無線通信（NFC）バンプ、デバイスポリシーコントローラー（DPC）ID、ゼロタッチを使用してデバイスを登録します。

2. アプリの移行戦略を作成します。
3. ユースケース要件を Android Enterprise 機能にマッピングします。要件とそれに対応する Android バージョンに最も一致するデバイス要件ごとに機能を文書化します。
4. 機能要件に基づいて Android の最小 OS を決定します（7.0、8.0、9.0）。
5. ID モデルを選択します：
   - 推奨：managed Google Play アカウント
   - Google Cloud Identity のお客様の場合のみ、Google G-Suite アカウントを使用します。
6. デバイス戦略を作成します：
   - アクションなし：デバイスが最小 OS レベル要件を満たしている場合
   - アップグレード：デバイスがサポート対象 OS をサポートしており、それに更新できる場合
   - 置換：デバイスをサポート対象 OS レベルに更新できない場合

推奨されるアプリ移行戦略

要件のマッピングが完了したら、アプリを Android プラットフォームから Android Enterprise プラットフォームに移行します。アプリの公開の詳細については、「アプリの追加」を参照してください。

- パブリックストアアプリ

  1. 移行するアプリを選択し、アプリを編集して Google Play 設定をクリアし、プラットフォームとして［**Android Enterprise**］ を選択します。
  2. デリバリーグループを選択します。アプリが必須の場合、デリバリーグループの ［必須アプリ］ リストにアプリを移行します。

  アプリを保存すると、Google Play ストアに表示されます。仕事用プロファイルがある場合、アプリは仕事用プロファイルの Google Play ストアに表示されます。

- プライベート（エンタープライズ）アプリ

  プライベートアプリは、社内で開発されるか、サードパーティの開発者によって開発されます。Google Play を使用してプライベートアプリを公開することをお勧めします。

  1. 移行するアプリを選択し、アプリを編集して、プラットフォームとして ［**Android Enterprise**］ を選択します。
  2. APK ファイルをアップロードし、アプリの設定を構成します。
  3. 必要なデリバリーグループにアプリを公開します。

- MDX アプリ

  1. 移行するアプリを選択し、アプリを編集して、プラットフォームとして ［**Android Enterprise**］ を選択します。
  2. MDX ファイルをアップロードします。アプリの承認プロセスを実行します。
  3. MDX ポリシーを選択します。

  エンタープライズ MDX アプリの場合、MDX に変更することをお勧めします。SDK モードのラップされたアプリ:

  - オプション 1: 組織に非公開で割り当てられた開発者アカウントを使用して、Google Play で APK をホストする。MDX ファイルを XenMobile で公開します。
  - オプション 2: XenMobile からエンタープライズアプリとしてアプリを公開する。XenMobile で APK を公開し、MDX ファイルのプラットフォームに ［**Android Enterprise**］ を選択します。

Citrix デバイスポリシーの移行

Android プラットフォームと Android Enterprise プラットフォームの両方で使用可能なポリシーの場合: ポリシーを編集してプラットフォーム ［**Android Enterprise**］ を選択します。

Android Enterprise の場合、登録モードを検討してください。一部のポリシーオプションは、仕事用プロファイルモードまたは完全管理モードのデバイスでのみ使用できます。

概念実証

アプリを Android Enterprise に移行したら、意図したとおりに機能することを確認するための移行テストを設定できます。

推奨の概念実証設定

1. 展開インフラストラクチャを設定します:
   - Android Enterprise テスト用のデリバリーグループを作成します。
   - XenMobile で Android Enterprise を構成します。
2. ユーザーアプリを設定します。
3. Android Enterprise 機能を構成します。
4. ポリシーを Android Enterprise デリバリーグループに割り当てます。
5. 機能をテストして確認します。
6. ユースケースごとにデバイスセットアップウォークスルーを実行します。

7. ユーザーのセットアップ手順を文書化します。

展開

これで、Android Enterprise セットアップを展開し、ユーザーの移行準備ができました。

推奨される展開戦略

Citrix は展開戦略として、Android Enterprise の本番システムをすべてテストした後で、デバイスを移行することを推奨します。

- このシナリオでは、ユーザーは従来のデバイスを最新の構成で使い続けることができます。Android Enterprise 管理用に新しいデバイスをセットアップします。
- アップグレードまたは交換が必要な場合にのみ、既存のデバイスを移行します。
- 通常のライフサイクルの最後に、既存のデバイスを Android Enterprise 管理に移行します。または、紛失や破損のために交換が必要な場合にデバイスを移行します。

Android Enterprise

January 24, 2020

Android Enterprise は、Google が Android デバイス用のエンタープライズ管理ソリューションとして提供するツールとサービスのセットです。Android Enterprise では、XenMobile を使用して、企業所有の Android デバイスとユーザー所有の（BYOD）Android デバイスを管理します。デバイス全体を管理することも、デバイス上の個別のプロファイルを管理することもできます。この個別のプロファイルでは、ビジネス用のアカウント、アプリ、データが個人のアカウント、アプリ、データと分離されています。在庫管理など、1 度のみの使用専用のデバイスを管理することもできます。

XenMobile でサポートされている Android オペレーティングシステムについては、「サポートされるデバイスオペレーティングシステム」を参照してください。

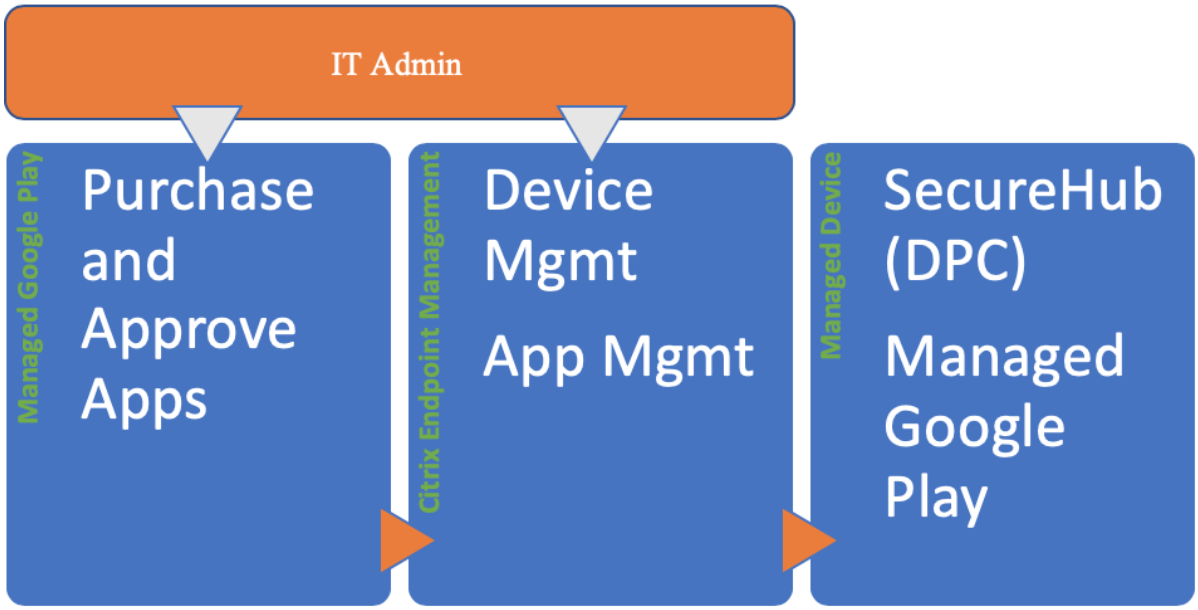
Android Enterprise に関連する用語と定義の一覧については、「Google Android Enterprise 開発者ガイド」の「Android Enterprise の用語」を参照してください。Google はこれらの用語を頻繁に更新します。

XenMobile を managed Google Play と統合して Android Enterprise を使用する場合、エンタープライズを作成します。Google はエンタープライズを、組織とエンタープライズモバイル管理（EMM）ソリューションとの間のバインディングと定義しています。組織がソリューションを通して管理するすべてのユーザーとデバイスは、そのエンタープライズに属します。

Android Enterprise のエンタープライズには、EMM ソリューション、デバイスポリシーコントローラー（DPC）アプリ、および Google エンタープライズアプリプラットフォームの 3 つのコンポーネントがあります。XenMobile を Android Enterprise と統合すると、完成されたソリューションには次のコンポーネントが含まれます:

- **XenMobile**: Citrix EMM。XenMobile は、安全なデジタルワークスペースのための統合されたエンドポイント管理ソリューションです。XenMobile は、IT 管理者が組織のデバイスとアプリを管理する手段を提供します。
- **Citrix Secure Hub**: Citrix DPC アプリ。Secure Hub は、XenMobile のスタートパッドです。Secure Hub はデバイスにポリシーを適用します。
- **managed Google Play**: XenMobile と統合する Google エンタープライズアプリプラットフォーム。Google Play EMM API がアプリポリシーを設定し、アプリを配布します。

次の図に、管理者がこれらのコンポーネントとやり取りする方法と、コンポーネントが互いにやり取りする方法を示します:



XenMobile での managed Google Play の使用

> 注:
>
> 管理対象 Google Play または G Suite を使用して、Citrix を EMM プロバイダーとして Google Play に登録できます。この記事では、管理対象 Google Play で Android Enterprise を使用する方法について説明します。組織が G Suite を使用してアプリへのアクセスを提供している場合、Android Enterprise で使用できます。G Suite ユーザー向けの従来の Android Enterpriseを参照してください。

管理対象 Google Play を使用する場合、デバイスおよびエンドユーザーに管理対象 Google Play アカウントをプロビジョニングします。管理対象 Google Play アカウントは、管理対象 Google Play へのアクセスを提供し、管理者が利用可能にしたアプリをユーザーがインストールし、使用できるようにします。組織がサードパーティの ID サービ

スを使用する場合、ビジネス向け Google Play アカウントと既存の ID アカウントを関連付けることができます。

この種類のエンタープライズはドメインに関連付けられていないため、1 つの組織用に 1 つまたは複数のエンタープライズを作成できます。たとえば、組織の各部門または各地域は異なるエンタープライズとして登録し、デバイスおよびアプリの個別セットとして管理できます。

XenMobile の管理者のために、managed Google Play では、Google Play のユーザーエクスペリエンスとアプリストアの機能が、エンタープライズ向けに設計された管理機能セットと組み合わされています。ビジネス向け Google Play を使用して、アプリを追加、購入、および承認し、デバイスの Android Enterprise ワークスペースに展開します。Google Play を使用してパブリックアプリ、プライベートアプリ、およびサードパーティアプリを展開できます。

管理対象デバイスのユーザーの場合、管理対象 Google Play がエンタープライズアプリストアです。ユーザーは、アプリの閲覧、アプリの詳細の表示、アプリのインストールを実行できます。Google Play のパブリックバージョンとは異なり、ユーザーは管理者が利用可能にしたアプリのみをビジネス向け Google Play からインストールできます。

デバイス展開シナリオと操作モード

デバイス展開シナリオは、展開するデバイスの所有者とデバイスの管理方法を示します。操作モードは、DPC がデバイスのポリシーを管理および実施する方法を指します。操作モードは、デバイス展開シナリオをサポートします。

仕事用プロファイル：**BYOD** デバイスの展開、プロファイル所有者モード

BYOD 展開シナリオでは、従業員が個人所有のデバイスを持ち込み、それらのデバイスを使用して会社の情報やアプリケーションにアクセスできます。

プロファイル所有者操作モードは、BYOD 展開をサポートします。企業は DPC を介して、デバイス上のプライマリユーザーアカウントに仕事用プロファイルを追加することにより、個人用デバイスを仕事で使用できるようにします。この仕事用プロファイルでは、ビジネス用のアカウント、アプリ、データが個人のアカウント、アプリ、データと分離されています。仕事用プロファイルはプライマリユーザーに個別のプロファイルとして関連付けられます。DPC はプロファイル所有者としてデバイス上の仕事用プロファイルのみを管理し、仕事用プロファイル以外の制御は制限されています。仕事用プロファイルの詳細については、Google Android Enterprise のヘルプトピック（仕事用プロファイルとは）を参照してください。

デバイスが XenMobile に登録されると、プロファイル所有者モードが有効になります。DPC はデバイス全体ではなく仕事用プロファイルのみを管理するため、プロファイル所有者モードで登録されたデバイスは、新規または工場出荷時リセットである必要はありません。

プロファイル所有者モードのデバイスは、仕事用プロファイルデバイスとも呼ばれます。プロファイル所有者モードは、仕事用プロファイルモードまたは管理対象プロファイルモードとも呼ばれます。

> 注：
>
> XenMobile では、プロファイル所有者モードの Zebra デバイスはサポートされません。XenMobile では、

> Zebra デバイスは完全に管理されたデバイスとして、およびデバイス従来モード（デバイス管理者モードともいう）でサポートされます。

完全に管理された：企業所有デバイスの展開、デバイス所有者モード

企業所有の展開シナリオでは、エンタープライズが使用するデバイスを所有し、完全に制御します。通常、デバイス全体を厳密に監視および管理する必要がある場合に、組織は企業所有デバイスを展開します。

デバイス所有者操作モードは、企業所有の展開をサポートします。デバイス所有者モードでは、DPC はデバイス全体を管理します。DPC はデバイス所有者として、デバイス全体のアクションを実行できます。デバイス全体の接続の構成、グローバル設定の構成、工場出荷時設定へのリセットなどです。

デバイス所有者モードのデバイスは、完全に管理されたデバイスです。

デバイス所有者モードは、デバイスの初期セットアップ中に有効になります。デバイス所有者モードで XenMobile に登録できるのは、新しいデバイスまたは工場出荷時の状態にリセットされたデバイスのみです。

専用デバイス：企業所有デバイスの展開、デバイス所有者モード

専用デバイスは、完全に管理されたデバイスです。デバイス所有者モードで実行されている企業所有デバイスです。専用デバイスは、デジタルサイネージ、チケットの印刷、在庫管理などの専用の制限されたアプリセットを提供します。専用デバイスをプロビジョニングする場合、必要なアプリのみを提供し、ユーザーが他のアプリを追加できないようにします。

専用デバイスは、企業所有の単一使用（COSU）デバイスとも呼ばれます。

従来のデバイスの展開、従来モード

従来展開シナリオは、5.0 より前の Android バージョンが実行されているデバイス向けのシナリオです。5.0 より前の Android バージョンでは、デバイス所有者モードとプロファイル所有者モードはサポートされていません。Android バージョン 5.1 では、デバイス所有者モードはサポートされていますが、プロファイル所有者モードはサポートされていません。

従来操作モードはデバイス管理者モードとも呼ばれ、レガシーデバイスの展開をサポートします。従来モードでは、DPC はデバイスの制御が制限されます。DPC は、デバイスのワイプ、パスコードの要求、またはポリシーの実施を行うことができます。従来のデバイスでアプリ管理を提供するには、Google Play を使用して、ユーザーが Google アカウントを追加できるようにします。DPC が管理対象 Google Play アカウントを従来のデバイスに追加するように設定することもできます。

従来モードは、デバイス所有者モードまたはプロファイル所有者モードを実装できる展開には推奨されません。Google では、大規模なフリートで低レベルのソリューションを使用するのではなく、可能な限り最高レベルのデバイス管理を使用することをお勧めします。従来モードからデバイス所有者モードまたはプロファイル所有者モードへの移行の詳細については、「Device Administration から Android Enterprise への移行」を参照してください。

> 注:
>
> シトリックスでも、managed Google play ではなく XenMobile や G Suite を使用するお客様について、または管理対象の Android Enterprise デバイスについて言う場合に従来という用語を使用します。

認証方法

XenMobile は、Android デバイスを MDM+MAM モードまたは MDM モードに登録します。ユーザーは、任意で MAM-only モードで登録することもできます。XenMobile は、MDM+MAM モードの Android デバイスに対して、次の認証方法をサポートします。詳しくは、「証明書と認証」を参照してください。

- ドメイン
- ドメイン + セキュリティトークン
- クライアント証明書
- クライアント証明書およびドメイン
- ID プロバイダー:
  - Azure Active Directory
  - Citrix ID プロバイダー

使用頻度が少ない別の認証方法には、クライアント証明書とセキュリティトークンの組み合わせがあります。詳しくは、「https://support.citrix.com/article/CTX215200」を参照してください。

要件

Android Enterprise の使用を開始するには、以下が必要となります:

- アカウントと資格情報:
  - 管理対象 Google Play で Android Enterprise をセットアップする場合、企業 Google アカウント
  - 最新の MDX ファイルをダウンロードする場合、Citrix カスタマーアカウント
  - プライベートアプリを展開する場合（オプション）、Google 開発者アカウント
- Samsung Knox Mobile Enrollment の場合（オプション）、Knox プレミアムライセンス

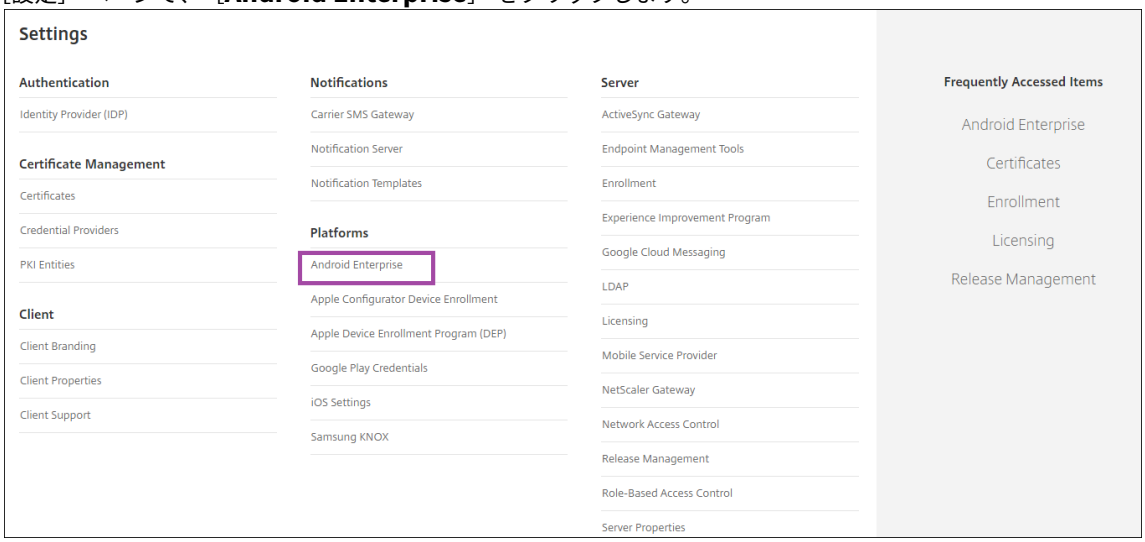
XenMobile の **Google Play** への接続

組織の Android Enterprise をセットアップするには、管理対象 Google Play から Citrix を EMM プロバイダーとして登録します。これにより、managed Google Play と XenMobile が接続され、XenMobile で Android Enterprise のエンタープライズが作成されます。

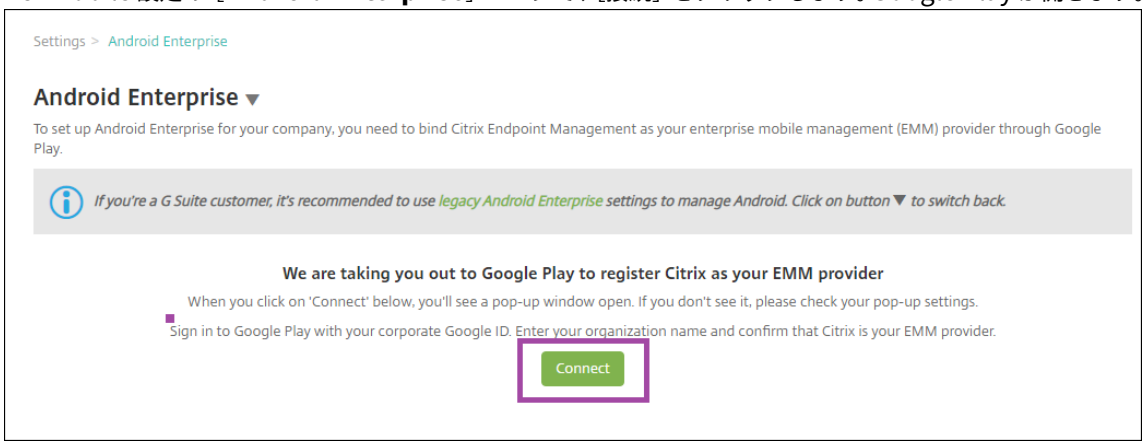
Google Play にサインインするための企業 Google アカウントが必要です。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。

2. [設定] ページで、[**Android Enterprise**] をクリックします。

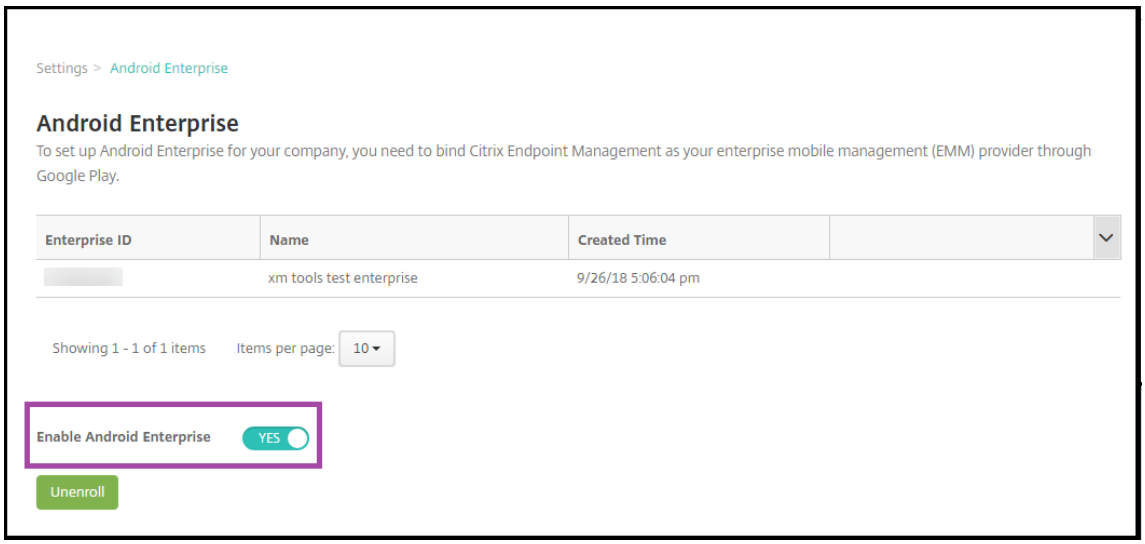


3. XenMobile 設定の [**Android Enterprise**] ページで、[接続] をクリックします。Google Play が開きます。

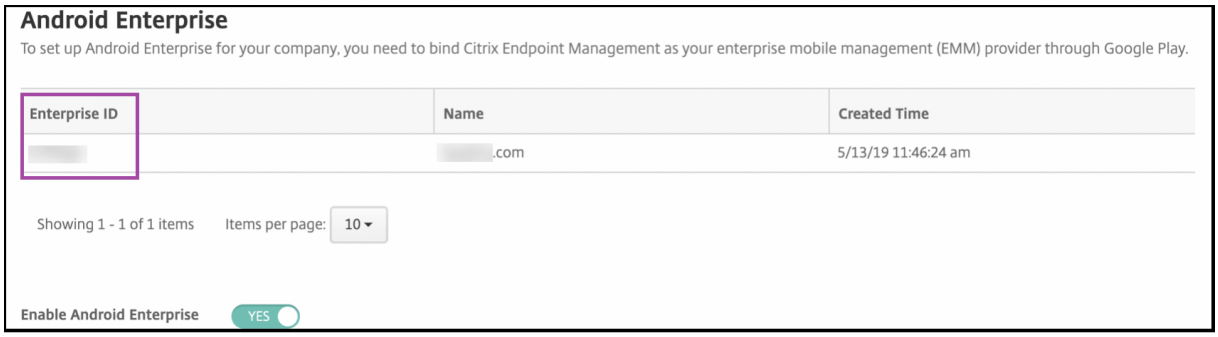


4. 企業 Google アカウントの資格情報で Google Play にサインインします。組織名を入力し、Citrix が EMM プロバイダであることを確認します。

5. Android Enterprise にエンタープライズ ID が追加されます。Android Enterprise を有効にするには、[**Android Enterprise** の有効化] を [はい] に切り替えます。



XenMobile コンソールにエンタープライズ ID が表示されます。



使用する環境が Google に接続され、デバイスを管理する準備ができます。これで、ユーザーにアプリを提供できるようになりました。

XenMobile を使用して、ユーザーに Citrix 業務用モバイルアプリ、MDX アプリ、パブリックアプリストアアプリ、Web および SaaS アプリ、エンタープライズアプリ、Web リンクを提供できます。これらの種類のアプリとこれらのアプリのユーザーへの提供の詳細については、「アプリの追加」を参照してください。

次のセクションでは、業務用モバイルアプリを提供する方法を示します。

Android Enterprise ユーザーに Citrix 業務用モバイルアプリを提供する

Android Enterprise ユーザーに Citrix 業務用モバイルアプリを提供するには、以下の手順を実行する必要があります。

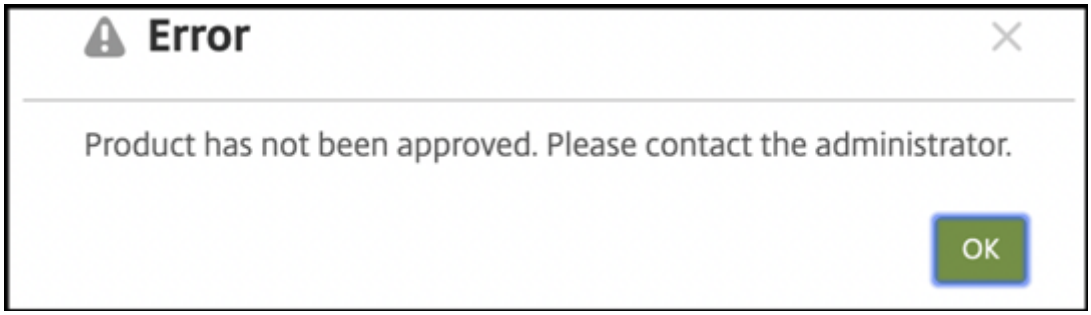
1. 管理対象 Google Play ストアで、ユーザーに必要なアプリを承認します。管理対象 Google Play でアプリを承認するを参照してください。
2. XenMobile コンソールで、アプリをパブリックアプリストアアプリとして公開します。「アプリをパブリックアプリストアアプリとして構成する」を参照してください。

3. XenMobile コンソールで、同じアプリを MDX アプリとして再度公開し、アプリが MDX ポリシーを受信できるようにします。アプリを MDX アプリとして構成するを参照してください。
4. XenMobile コンソールで、ユーザーがデバイス上の仕事用プロファイルにアクセスするために使用するセキュリティ確認のルールを構成します。セキュリティ確認ポリシーを構成するを参照してください。

公開するアプリは、Android Enterprise エンタープライズに登録されているデバイスで利用できます。

管理対象 **Google Play** でアプリを承認する

アプリを XenMobile に追加するには、まず managed Google Play ストアでアプリを承認します。managed Google Play ストアでアプリを承認していない場合、アプリを追加しようとすると、XenMobile コンソールで次のエラーが表示されます:

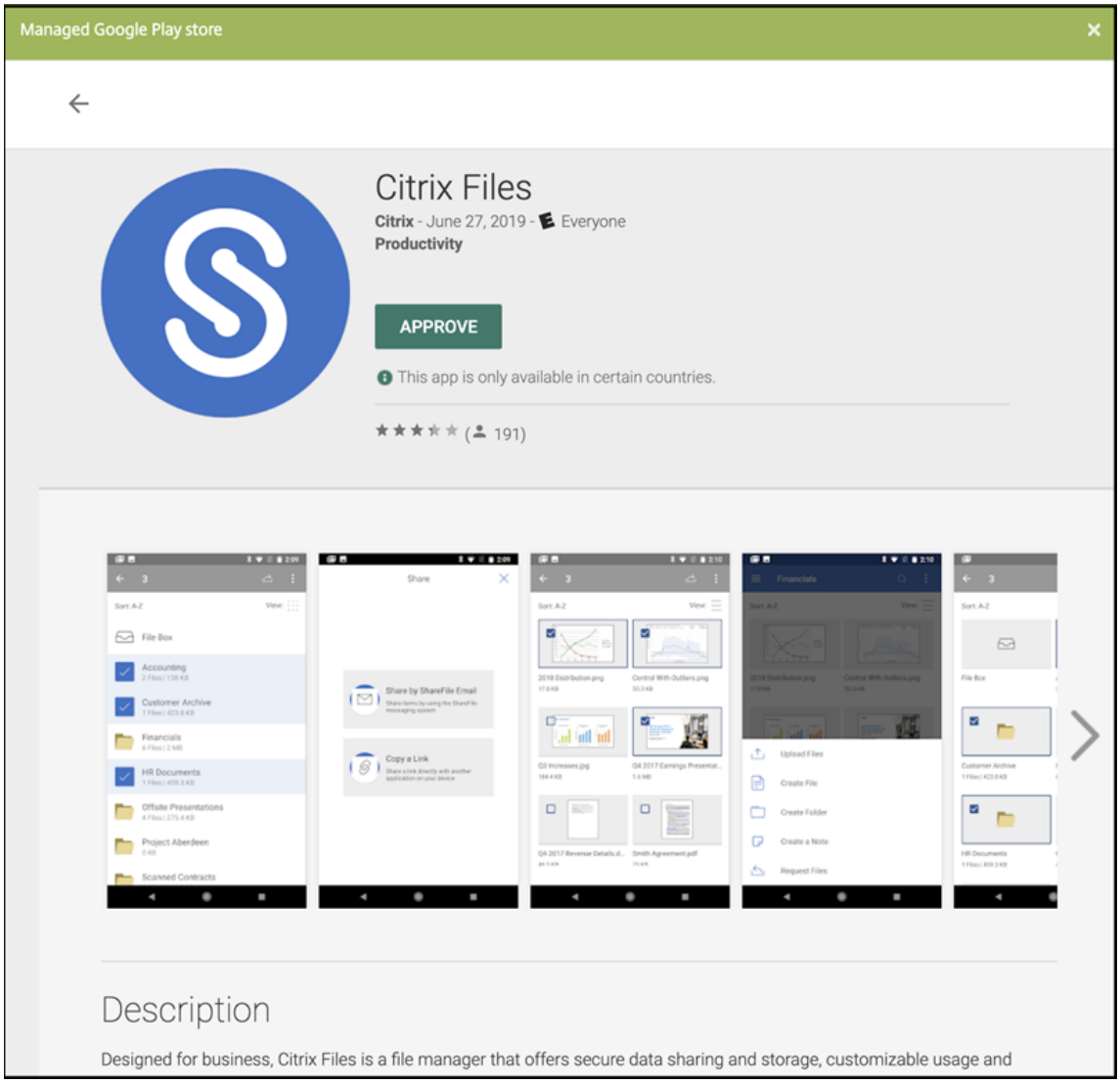


管理対象 Google Play ストアにアクセスして、エンタープライズで既に承認されていて利用可能なアプリを確認します。

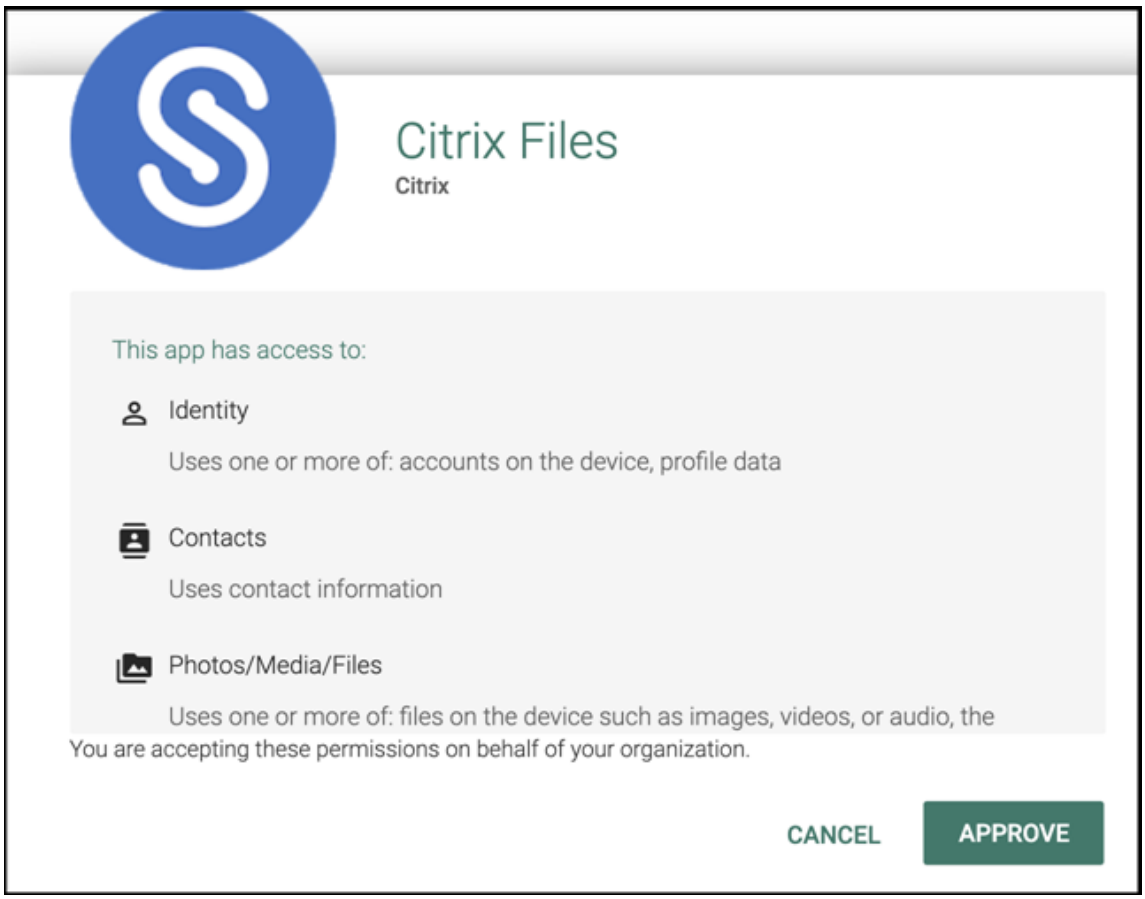
1. Google アカウントの資格情報を使用してhttps://play.google.com/workにログインします。
2. [マイ管理対象アプリ] をクリックして、ユーザーに対して承認されているすべてのアプリを表示します。

管理対象 Google Play ストアでアプリを承認するには:

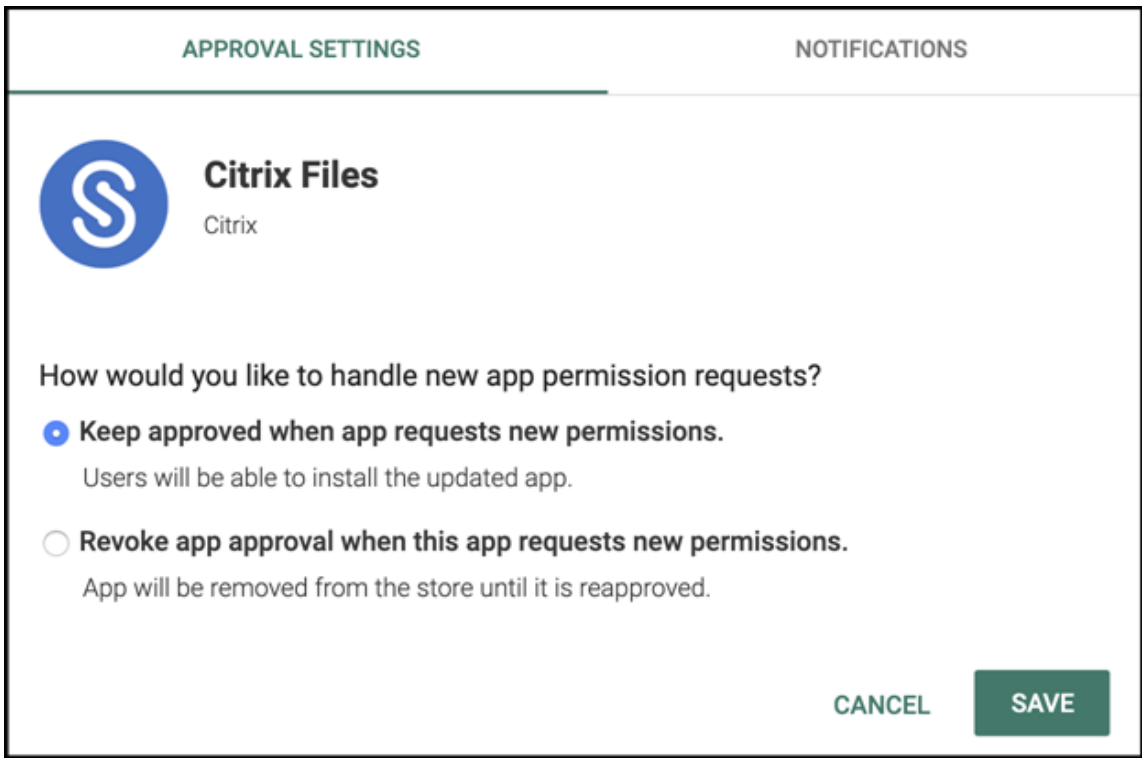
1. 管理対象 Google Play にログインした状態で、承認するアプリを選択します。対象アプリのページに [承認] ボタンが表示されます。



2. ［承認］ をクリックします。



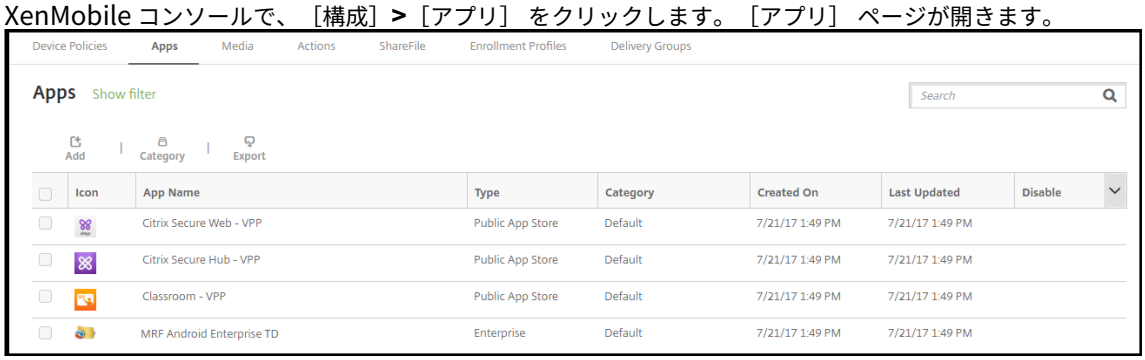
3. ［承認］ を再度クリックします。
4. ［アプリが新しい権限を要求したときには承認を維持する］ を選択します。［保存］ をクリックします。



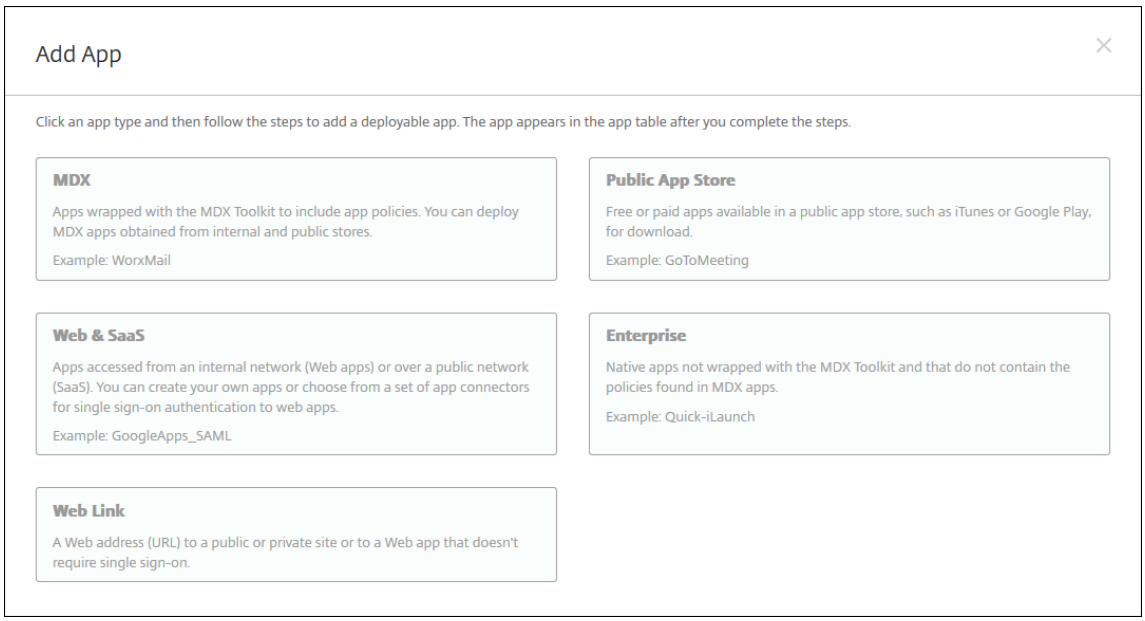
アプリをパブリックアプリストアアプリとして構成する

Citrix ShareFile を Android Enterprise パブリックアプリストアアプリとして構成するには:

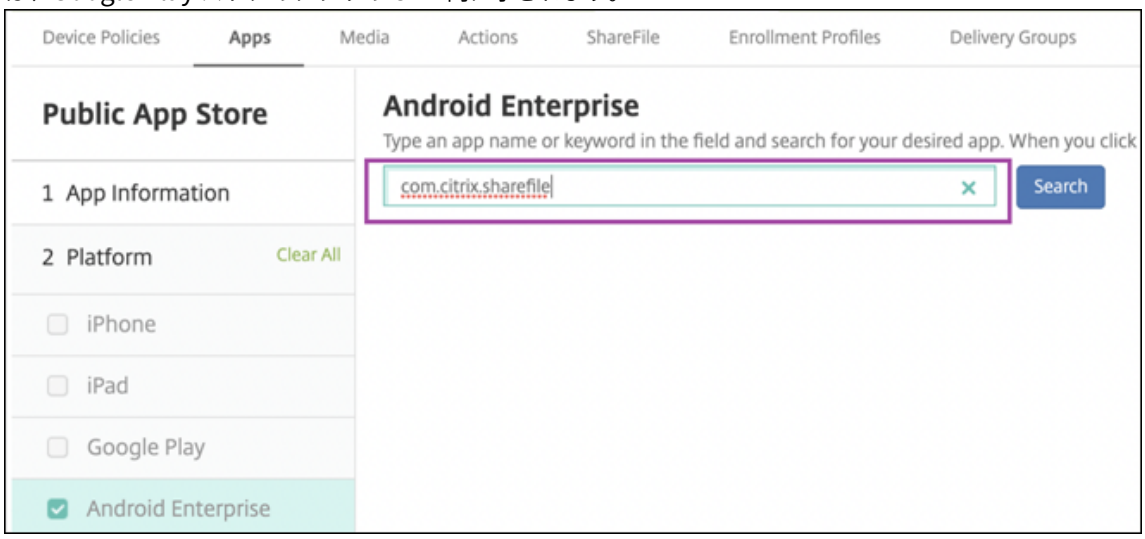
1. XenMobile コンソールで、［構成］**>**［アプリ］ をクリックします。［アプリ］ ページが開きます。



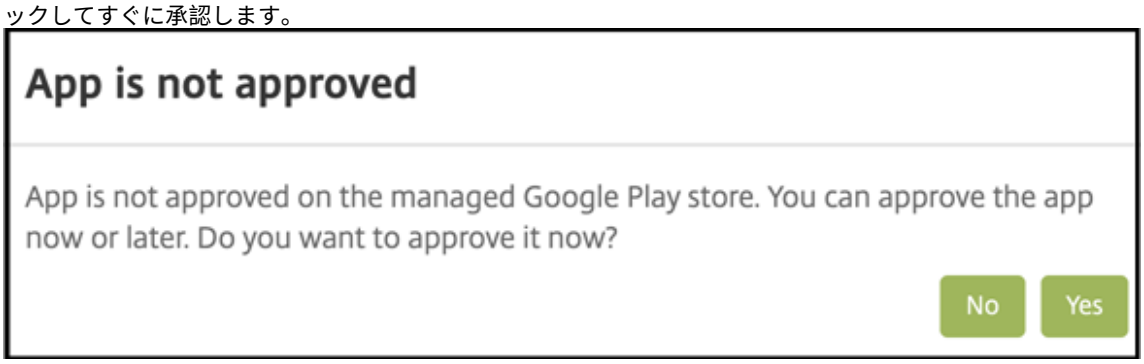
2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



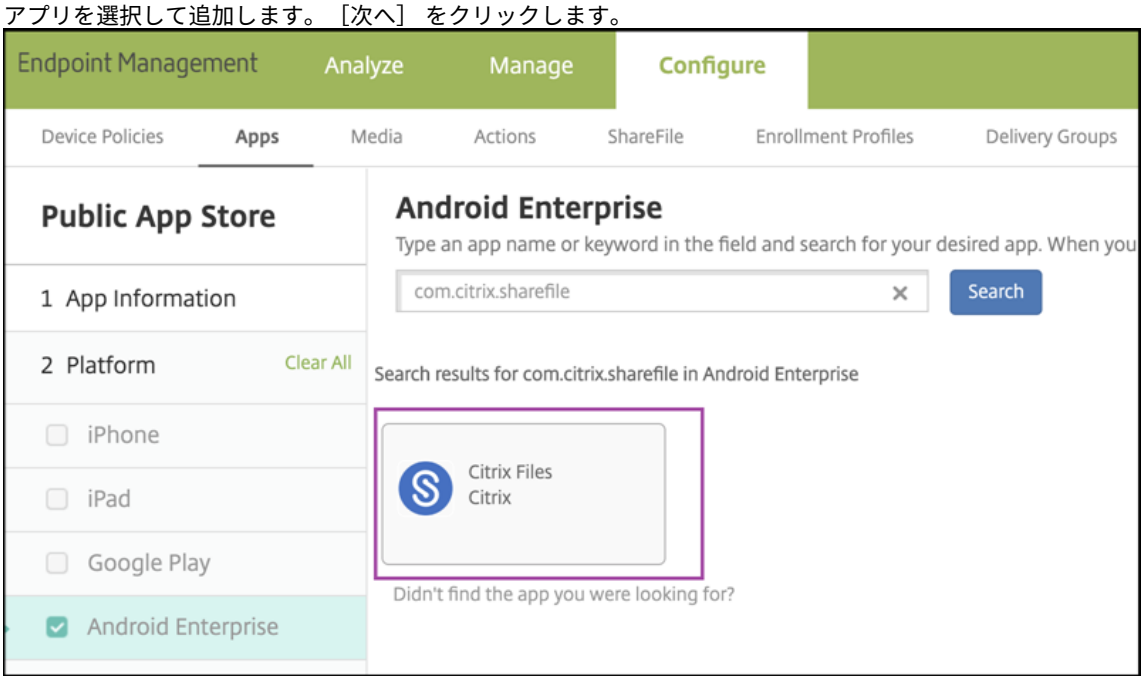
3. [パブリックアプリストア] をクリックします。[アプリ情報] ページが開きます。
4. [アプリケーション情報] ページで、以下の情報を入力します:
   - 名前: アプリの説明的な名前を入力します。この名前は、[アプリ] の表の [アプリ名] の下に表示されます。
   - 説明: 任意で、アプリの説明を入力します。
   - アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリカテゴリの作成」を参照してください。
5. [次へ] をクリックします。アプリのプラットフォームページが開きます。
6. [プラットフォーム] で [**Android Enterprise**] を選択します。他のプラットフォームをクリアします。
7. [**Android Enterprise**] の下で、アプリのバンドル ID を入力して [検索] をクリックします。アプリ ID は、Google Play ストアのアプリの URL 内に示されます。



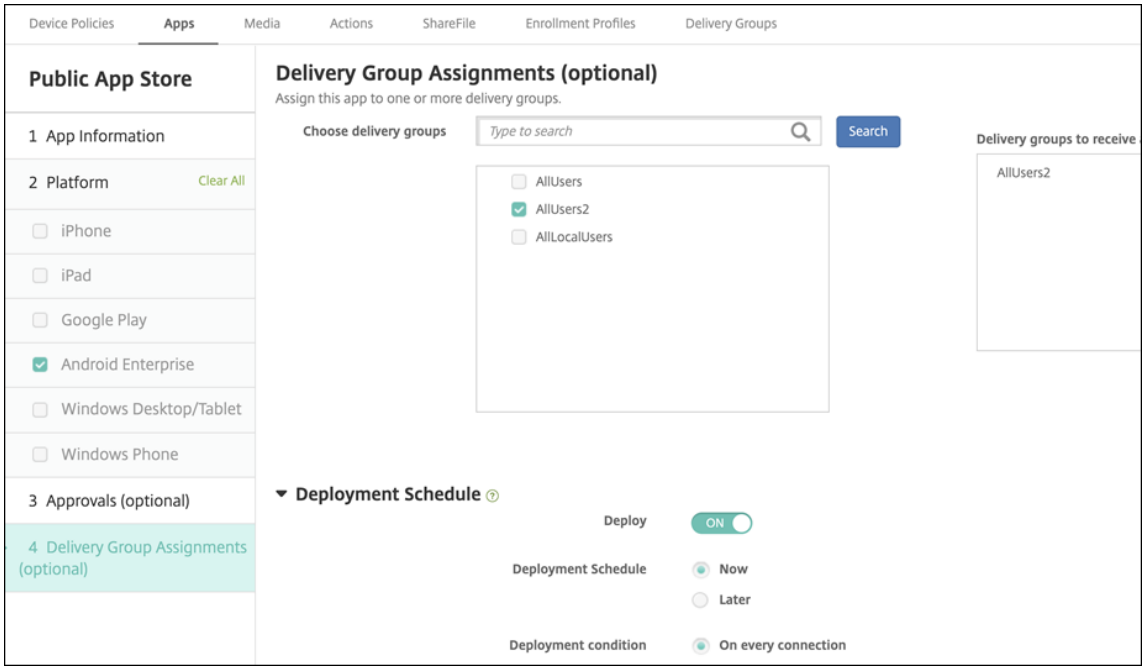
8. アプリが Google Play ストアで承認されていないことがコンソールに表示されている場合、［はい］ をクリックしてすぐに承認します。



9. アプリを選択して追加します。［次へ］ をクリックします。



10. このアプリを 1 つ以上のデリバリーグループに割り当てます。



11. [保存] をクリックします。

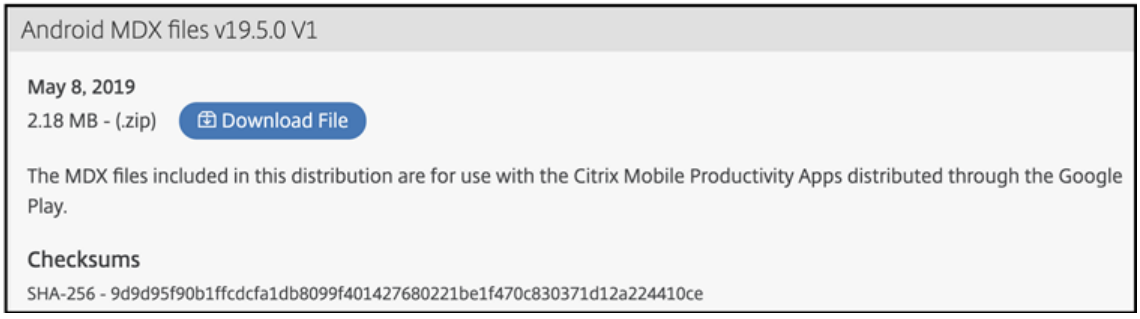
Citrix Secure Mail と Citrix Secure Web でこれらの手順を繰り返します。

アプリを **MDX** アプリとして構成する

業務用モバイルアプリでは、ネイティブの Android マニフェストは使用されません。アプリをユーザーに展開する前に、これらのアプリを MDX アプリとして追加し、MDX ポリシーを構成する必要があります。

MDX アプリを追加する前に、最新の Android MDX ファイルをダウンロードします:

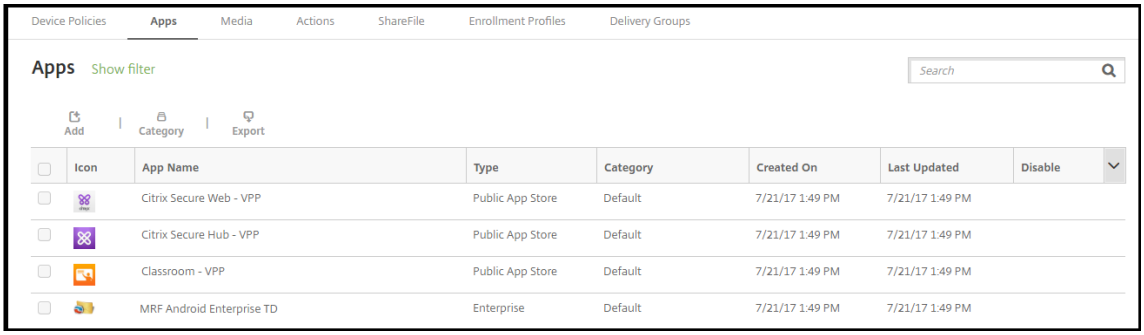
1. 以下の XenMobile ダウンロードページにアクセスして、Citrix の顧客資格情報でログインします: https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html



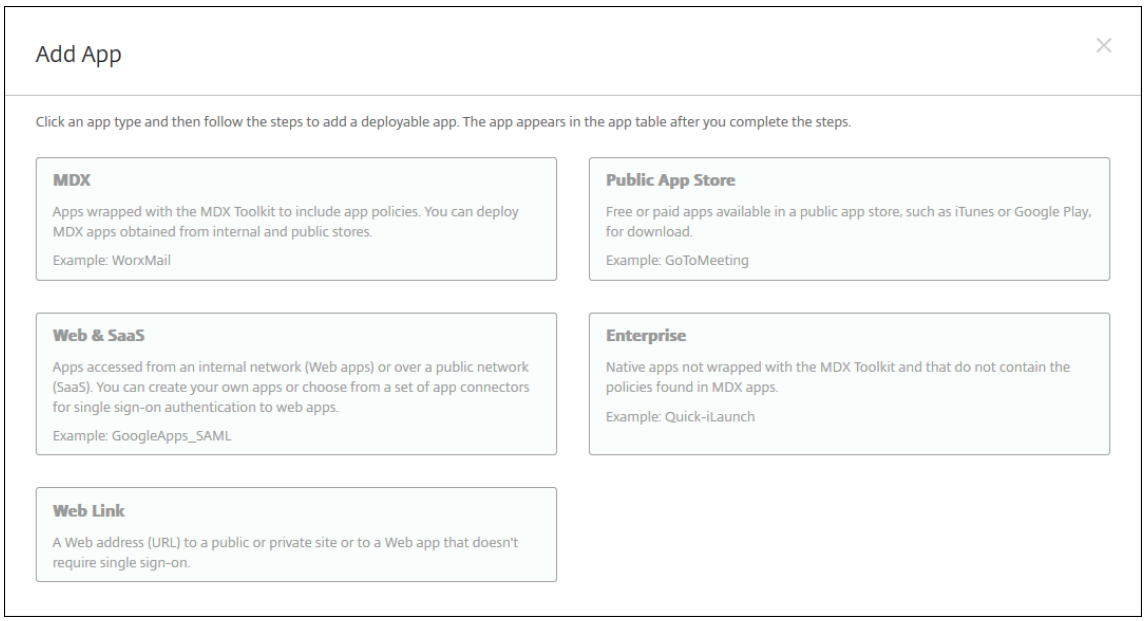
2. ダウンロードしたファイルを解凍し、その内容を抽出します。

MDX アプリを追加して構成するには:

1. XenMobile コンソールで、［構成］**>**［アプリ］ をクリックします。［アプリ］ ページが開きます。

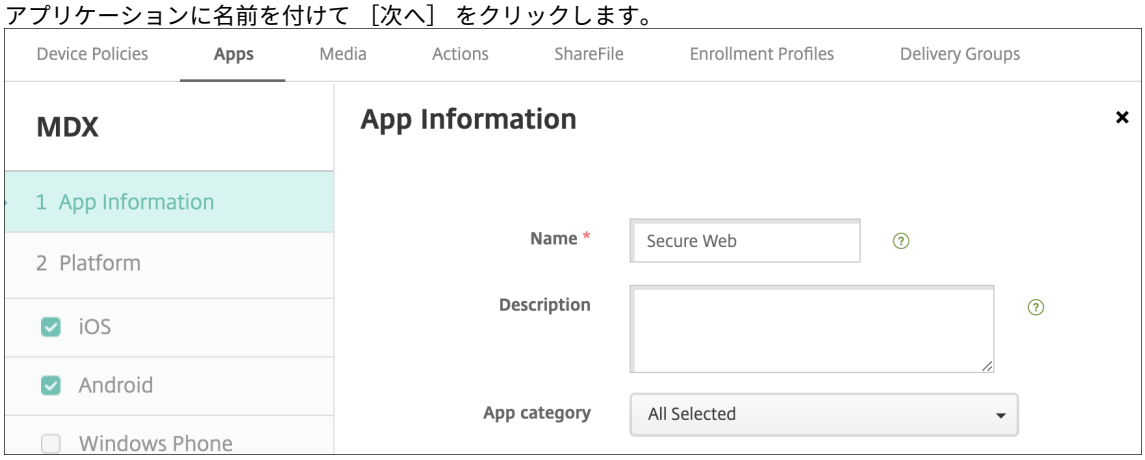


2.［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3.［**MDX**］ をクリックします。［アプリ情報］ ページが開きます。

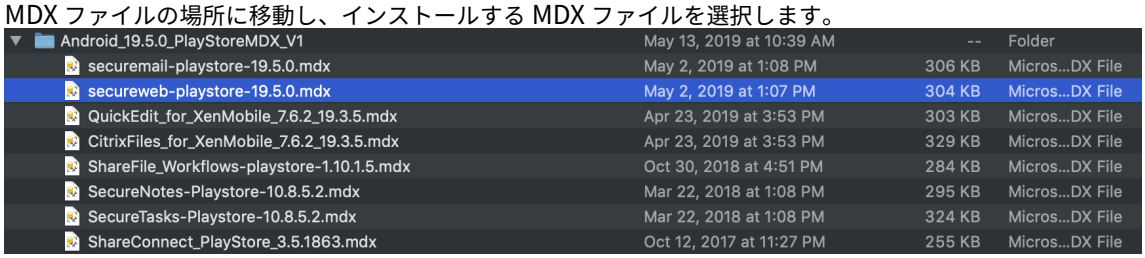
4. アプリケーションに名前を付けて ［次へ］ をクリックします。



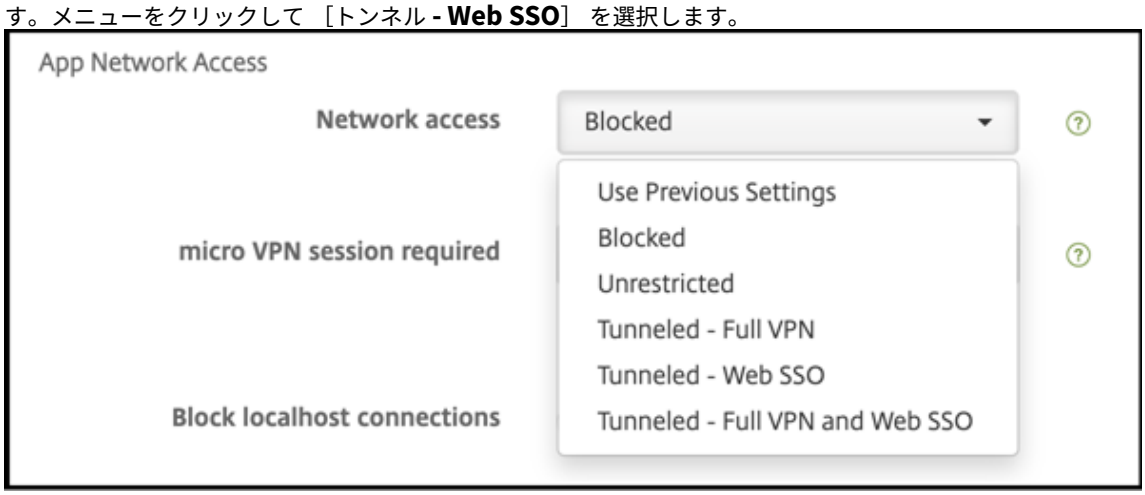
5.［次へ］ をクリックして Android プラットフォームの構成を取得します。

6. ［アップロード］をクリックします。

7. MDX ファイルの場所に移動し、インストールする MDX ファイルを選択します。



8. 一部のアプリのネットワークアクセスはデフォルトでブロックされます。ネットワークアクセスを有効にします。メニューをクリックして ［トンネル **- Web SSO**］ を選択します。



9. ［次へ］ をクリックして、デフォルト以外のページを通過し、［デリバリーグループの割り当て］ページに到達するまで続けます。
10. パブリックアプリストアアプリとして公開したときに割り当てたのと同じデリバリーグループにアプリを割り当てます。
11. ［保存］ をクリックします。

この手順を繰り返して、業務用モバイルアプリごとに MDX アプリを構成します。

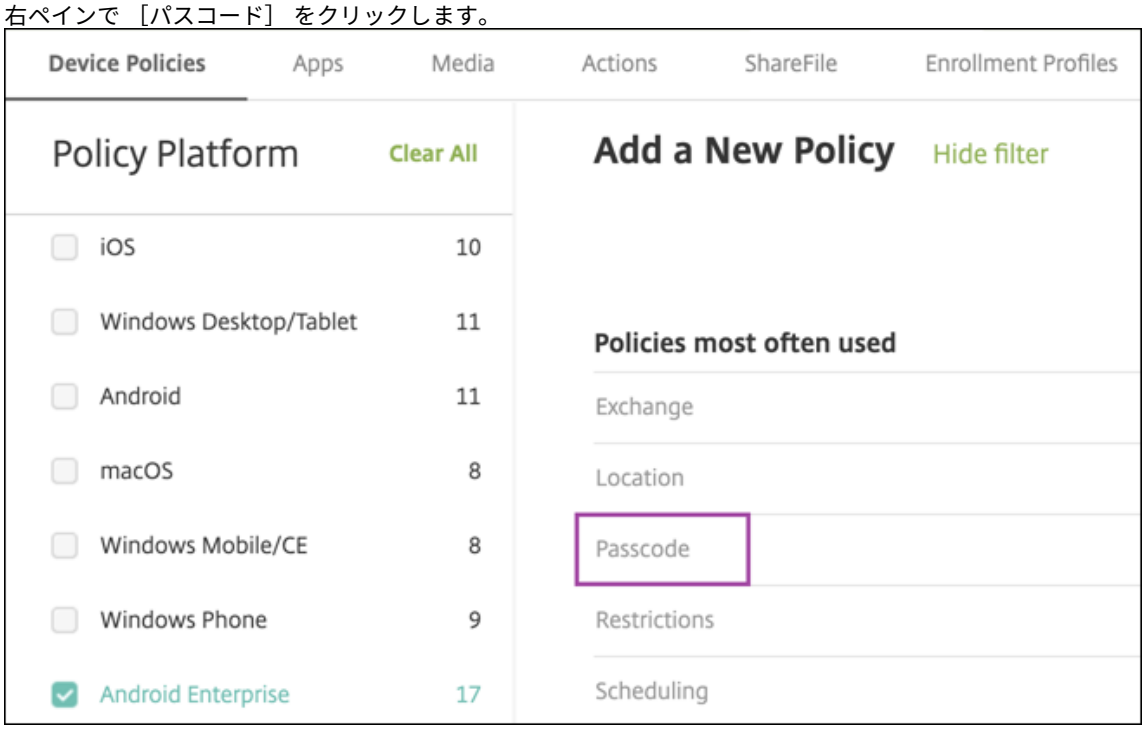
セキュリティ確認ポリシーを構成する

XenMobile パスコードデバイスポリシーでは、ユーザーがデバイスまたはデバイス上の Android Enterprise の仕事用プロファイルにアクセスするためのセキュリティ確認のルールセットを構成します。セキュリティ確認はパスコードか生体認証です。パスコードポリシーの詳細については、「パスコードデバイスポリシー」を参照してください。

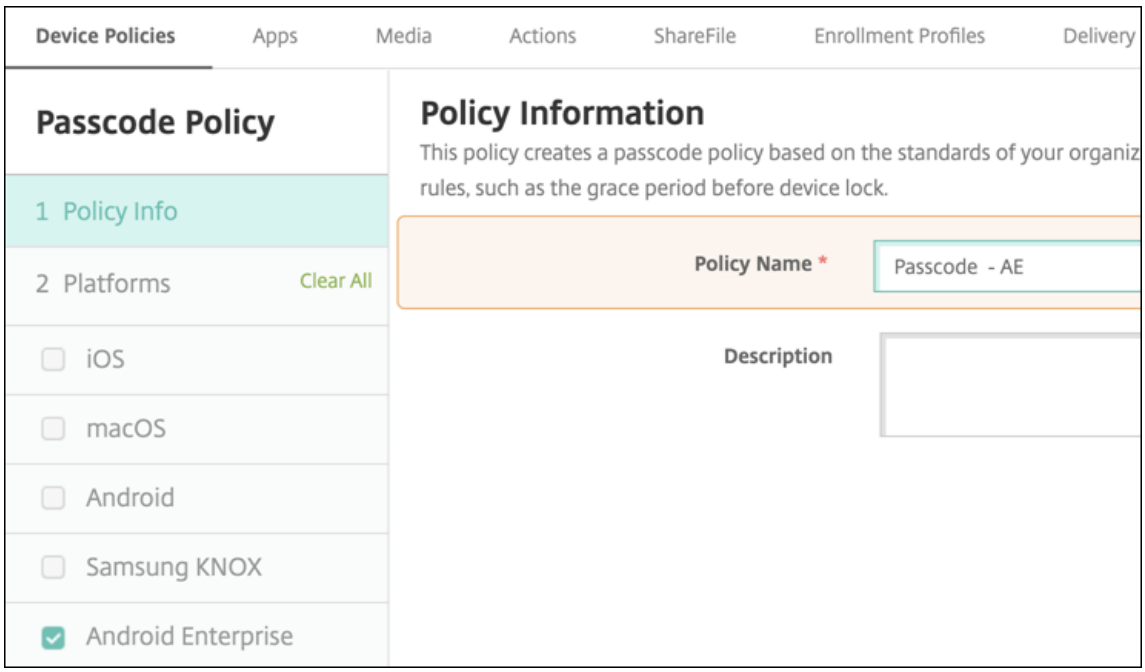
Android Enterprise の展開に BYOD デバイスが含まれる場合、仕事用プロファイルのパスコードポリシーを構成します。展開に企業所有の完全管理デバイスが含まれる場合、デバイス自体のパスコードポリシーを構成します。展開に両方のタイプのデバイスが含まれる場合、両方のタイプのパスコードポリシーを構成します。

パスコードポリシーを構成するには:

1. XenMobile コンソールで、［構成］**>**［デバイスポリシー］ に移動します。
2. ［追加］ をクリックします。
3. ［フィルターを表示］ をクリックして、［ポリシープラットフォーム］ ペインを開きます。［ポリシープラットフォーム］ ペインで、［**Android Enterprise**］ を選択します。
4. 右ペインで ［パスコード］ をクリックします。



5. ［ポリシー名］ を入力します。［次へ］ をクリックします。



6. パスコードポリシー設定を構成します。
   - デバイス自体のセキュリティ確認に使用できる設定を確認するには、［デバイスのパスコードを要求］を ［オン］ に設定します。
   - 仕事用プロファイルのセキュリティ確認に使用できる設定を確認するには、［仕事用プロファイルのセキュリティ確認］ を ［オン］ に設定します。
7. ［次へ］ をクリックします。
8. このポリシーを 1 つ以上のデリバリーグループに割り当てます。
9. ［保存］ をクリックします。

Android Enterprise での仕事用プロファイルデバイスのプロビジョニング

Android Enterprise 仕事用プロファイルデバイスは、プロファイル所有者モードで登録されます。これらのデバイスは、新しいデバイスまたは工場出荷時の状態にリセットされたデバイスである必要はありません。BYOD デバイスは、仕事用プロファイルデバイスとして登録されます。登録手順は、XenMobile で Android を登録する場合と同様です。ユーザーは Google Play から Secure Hub をダウンロードし、デバイスを登録します。

デバイスが Android Enterprise で仕事用プロファイルデバイスとして登録されている場合、デフォルトでは USB デバッグおよび不明なソース設定は無効になっています。

Android Enterprise のデバイスを仕事用プロファイルデバイスとして登録する場合は、必ず Google Play にアクセスしてください。そこから、ユーザーの個人プロファイルでの Secure Hub の表示を有効にします。

Android Enterprise の完全に管理されたデバイスのプロビジョニング

前のセクションで設定した展開に、完全に管理されたデバイスを登録できます。完全に管理されたデバイスは企業所有デバイスで、デバイス所有者モードで登録されます。デバイス所有者モードで登録できるのは、新しいデバイスまたは工場出荷時の状態にリセットされたデバイスのみです。

デバイス所有者モードでデバイスを登録するには、次の登録方法のいずれかを使用します:

- **DPC ID** トークン: この登録方法では、ユーザーがデバイスの設定時に「afw##xenmobile」という文字を入力します。afw##xenmobileは Citrix DPC ID トークンです。このトークンにより、デバイスが XenMobile の管理対象であると識別され、Google Play ストアから Secure Hub がダウンロードされます。Citrix DPC 識別子トークンを使用したデバイスの登録を参照してください。
- 近距離無線通信（**NFC**）バンプ: NFC バンプの登録方法では、近距離無線通信を使用して 2 つのデバイス間でデータを転送します。新しいデバイスまたは工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびそのほかの通信モードは無効になっています。この状態のデバイスが使用する通信プロトコルは NFC のみです。NFC バンプを使用してデバイスを登録するを参照してください。
- **QR** コード: QR コード登録は、NFC をサポートしていないタブレットなどの分散型端末を登録するのに使用できます。QR コードによる登録方法では、セットアップウィザードから QR コードをスキャンすることによって、デバイスプロファイルモードを設定および構成します。QR コードを使用してデバイスを登録するを参照してください。
- ゼロタッチ: ゼロタッチ登録では、最初に電源をオンにしたときに自動で登録されるようにデバイスを構成できます。ゼロタッチ登録は、Android 8.0 以降が動作する一部の Android デバイスでサポートされています。ゼロタッチ登録を参照してください。
- **Google** アカウント: ユーザーは、Google アカウントの資格情報を入力して、プロビジョニングプロセスを開始します。このオプションは、G Suite を使用しているエンタープライズ向けです。

Citrix DPC 識別子トークンを使用したデバイスの登録

初期セットアップで新しいデバイスまたは工場出荷時の状態にリセットされたデバイスの電源を入れた後、Google アカウントの入力を求められたら「afw#xenmobile」と入力します。この操作により、Secure Hub がダウンロードされインストールされます。インストール後、Secure Hub の設定プロンプトに従って登録を完了します。

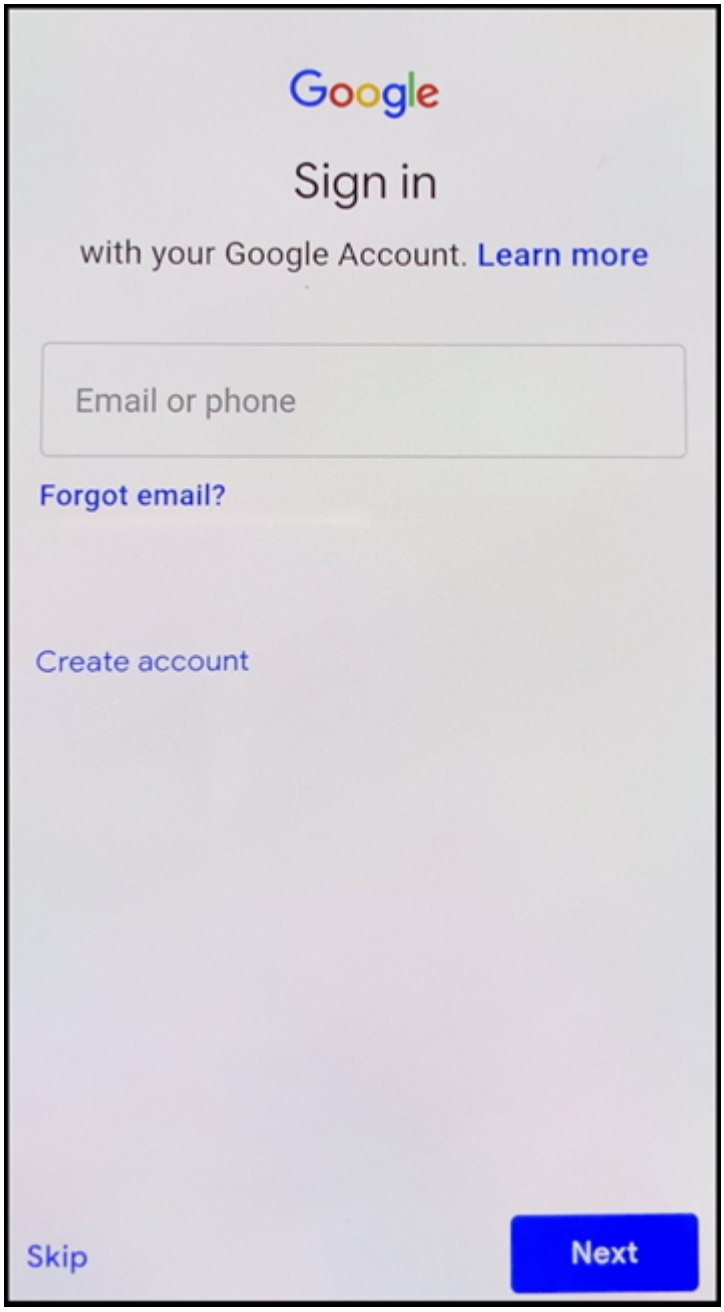
この登録方法では Secure Hub の最新バージョンが Google Play ストアからダウンロードされるため、ほとんどのお客様に推奨されます。他の登録方法とは異なり、XenMobile サーバーでダウンロード用に Secure Hub を提供することはありません。

システム要件

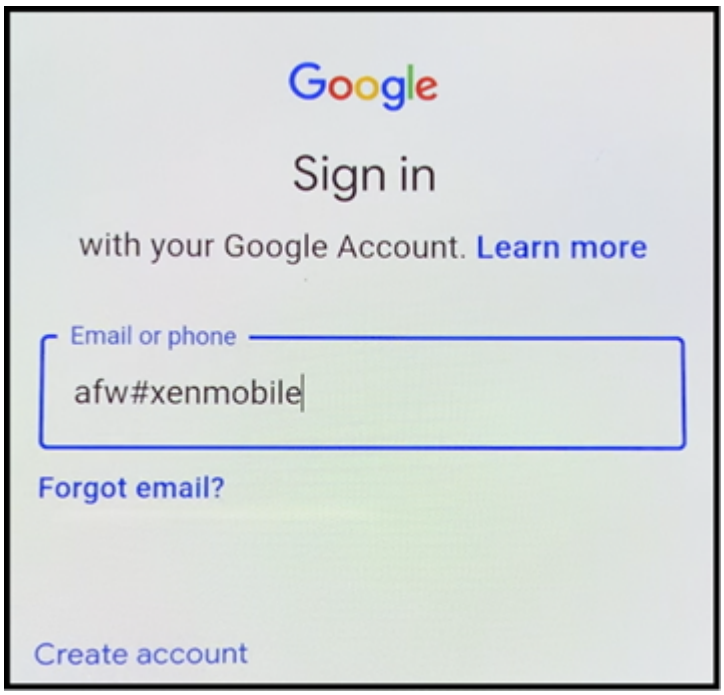
- Android OS を実行するすべての Android デバイスでサポートされます。

デバイスを登録するには

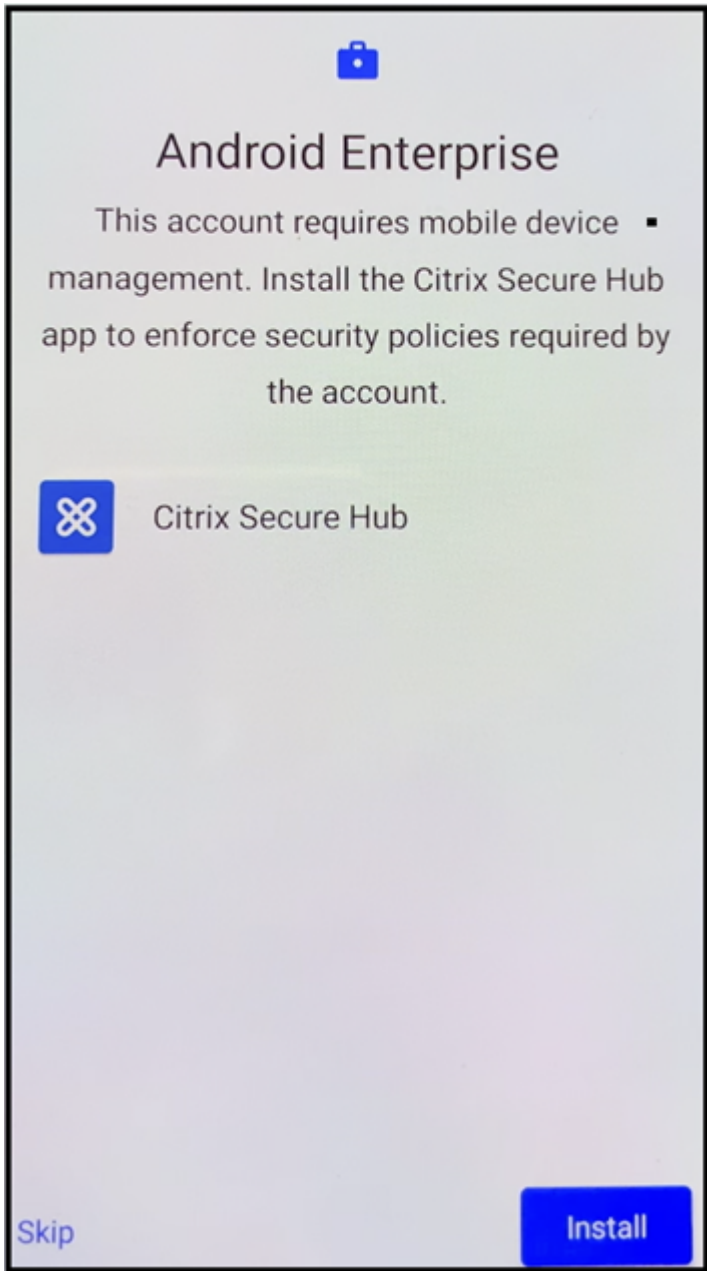
1. 新しいデバイスまたは工場出荷時の設定にリセットされたデバイスの電源を入れます。
2. デバイスの初期セットアップが読み込まれ、Google アカウントの入力が求められます。デバイスのホーム画面が読み込まれたら、通知バーのセットアップ完了通知を確認します。



3. メールまたは電話フィールドに「`afw##xenmobile`」と入力します。

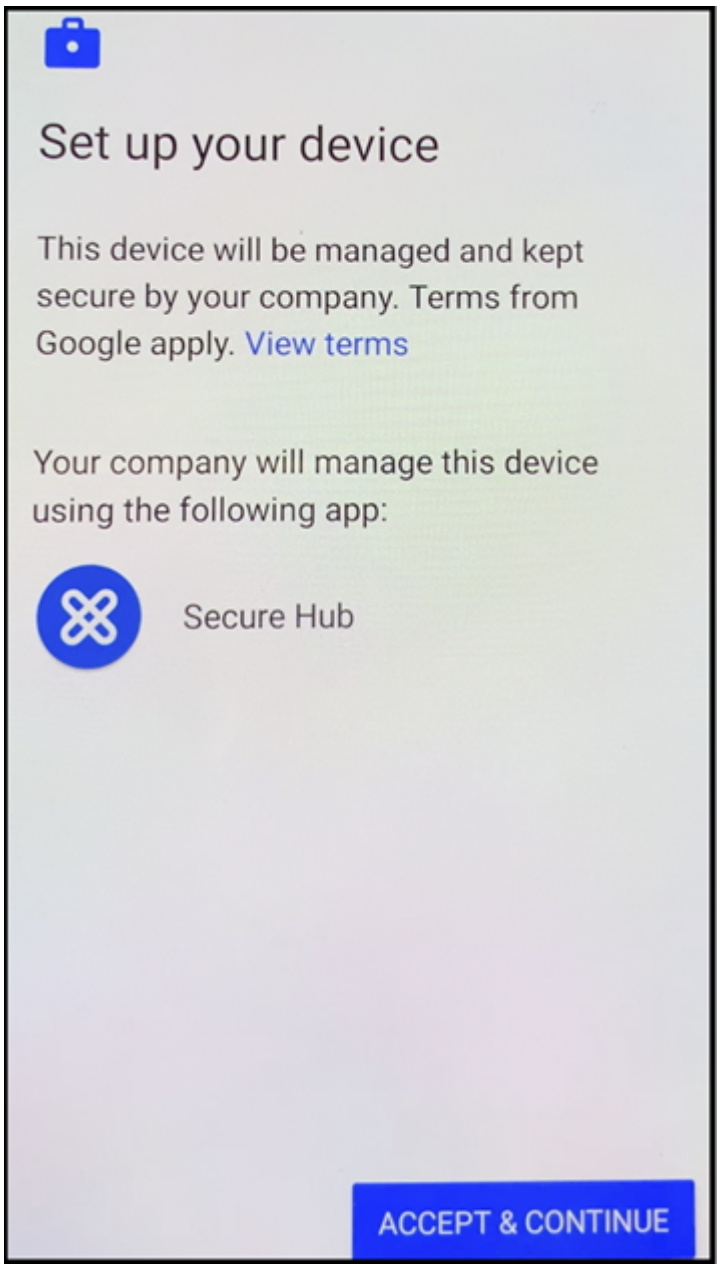


4. Secure Hub のインストールを求める Android Enterprise 画面で ［インストール］ をタップします。

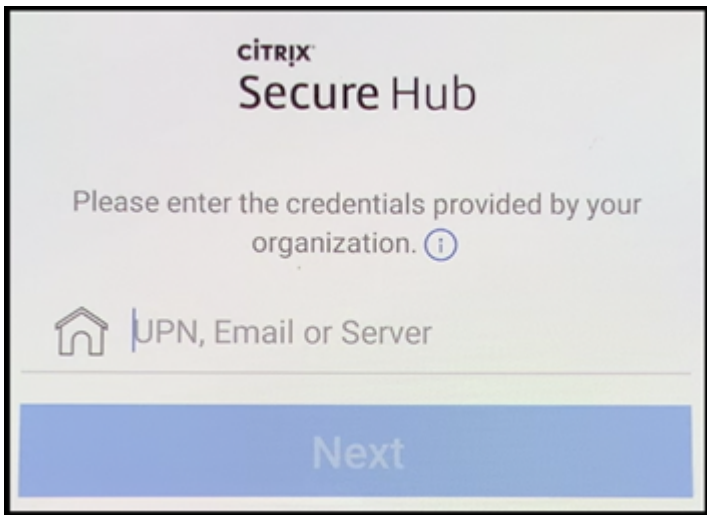


5. Secure Hub インストーラー画面で ［インストール］ をタップします。

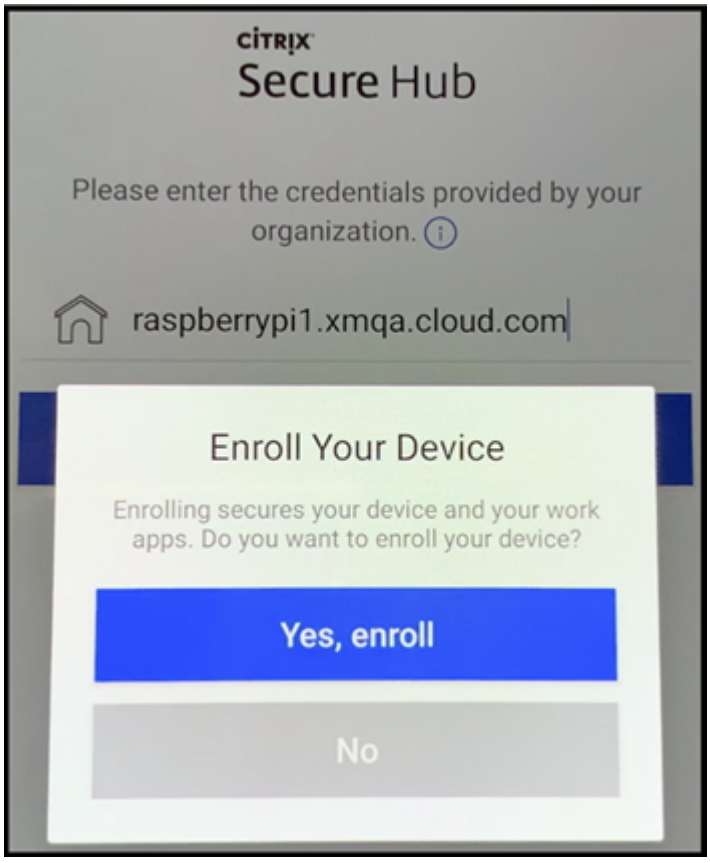
6. すべてのアプリの許可リクエストに対して ［許可する］ をタップします。
7. ［同意して続行］ をタップして Secure Hub をインストールし、デバイスを管理できるようにします。



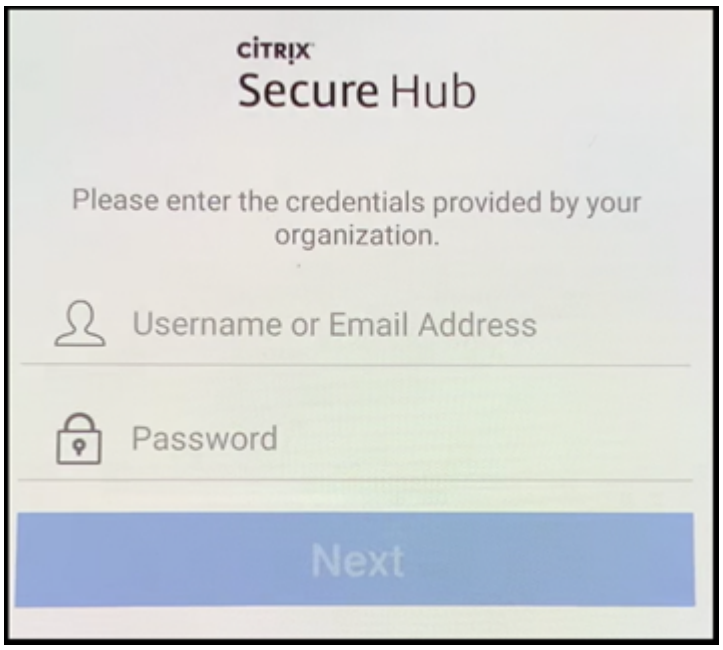
8. これで、Secure Hub がインストールされ、デフォルトの登録画面に表示されます。この例では、自動検出は設定されていません。自動検出が設定されている場合、ユーザーはユーザー名/メールアドレスを入力可能で、それに対応するサーバーが検出されます。自動検出が設定されていない場合、環境の登録 URL を入力して ［次へ］ をタップします。



9. XenMobile のデフォルト設定では、MAM を使用するか、MDM+MAM を使用するかを選択できます。このようにプロンプトが表示されたら、［はい、登録します］ をタップして MDM+MAM を選択します。

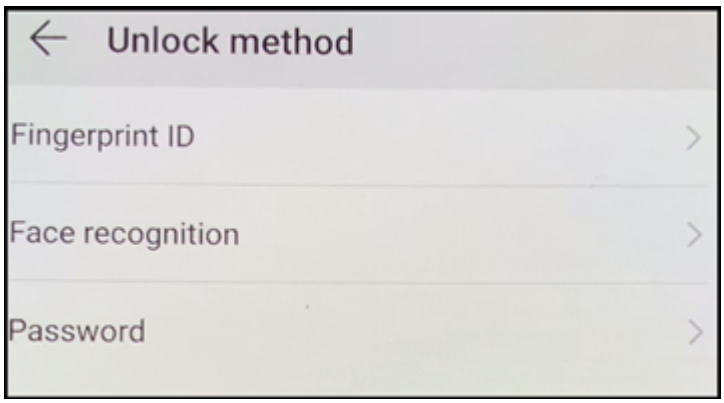


10. ユーザー名とパスワードを入力し、［次へ］ をタップします。

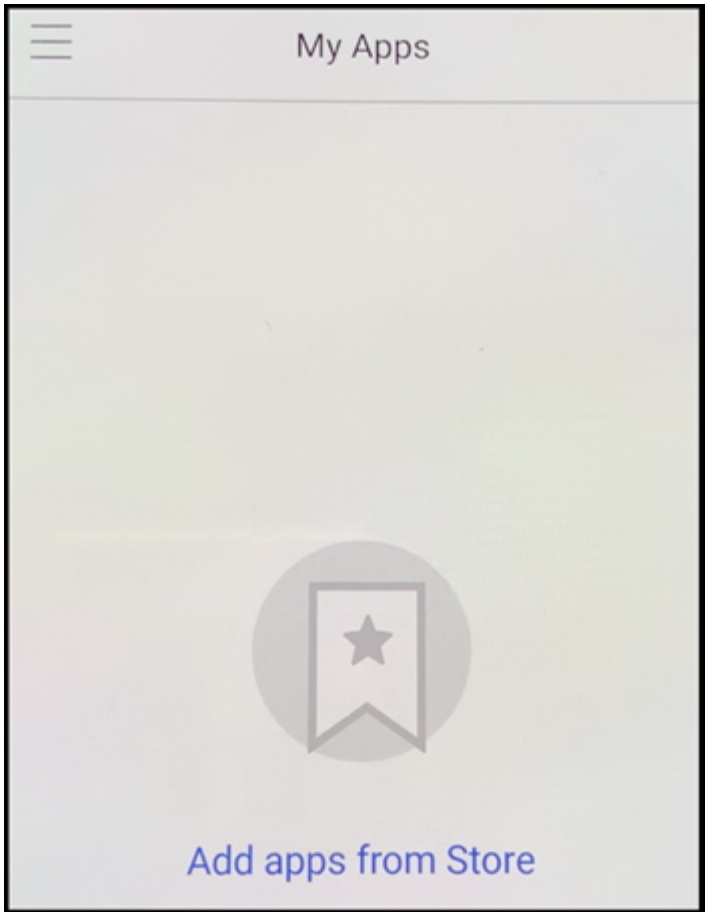


11. デバイスのパスコードを設定するように求められます。［設定］ をタップしてパスコードを入力します。

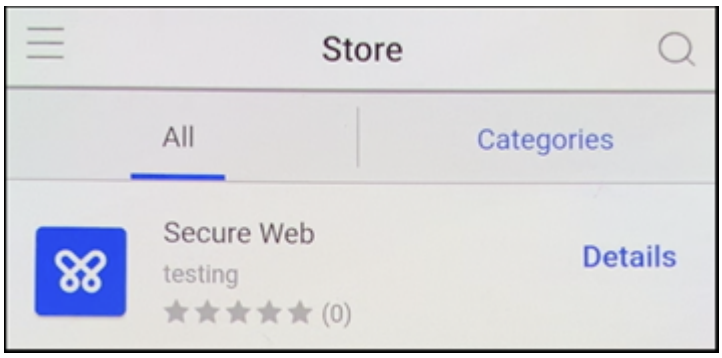
12. 仕事用プロファイルのロック解除方法を設定するよう求められます。この例では ［パスワード］、［**PIN**］ をタップして PIN を入力します。



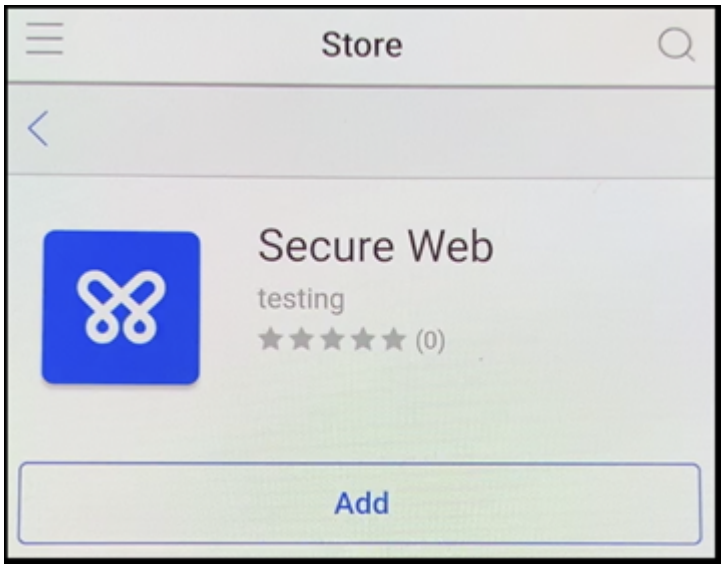
13. デバイスに Secure Hub の ［マイアプリ］ ランディング画面が表示されます。［ストアからアプリを追加］をタップします。



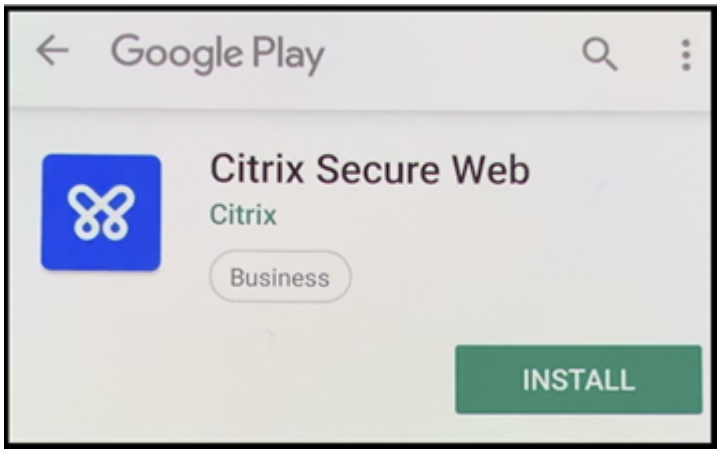
14. Secure Web を追加するには、［**Secure Web**］ をタップします。



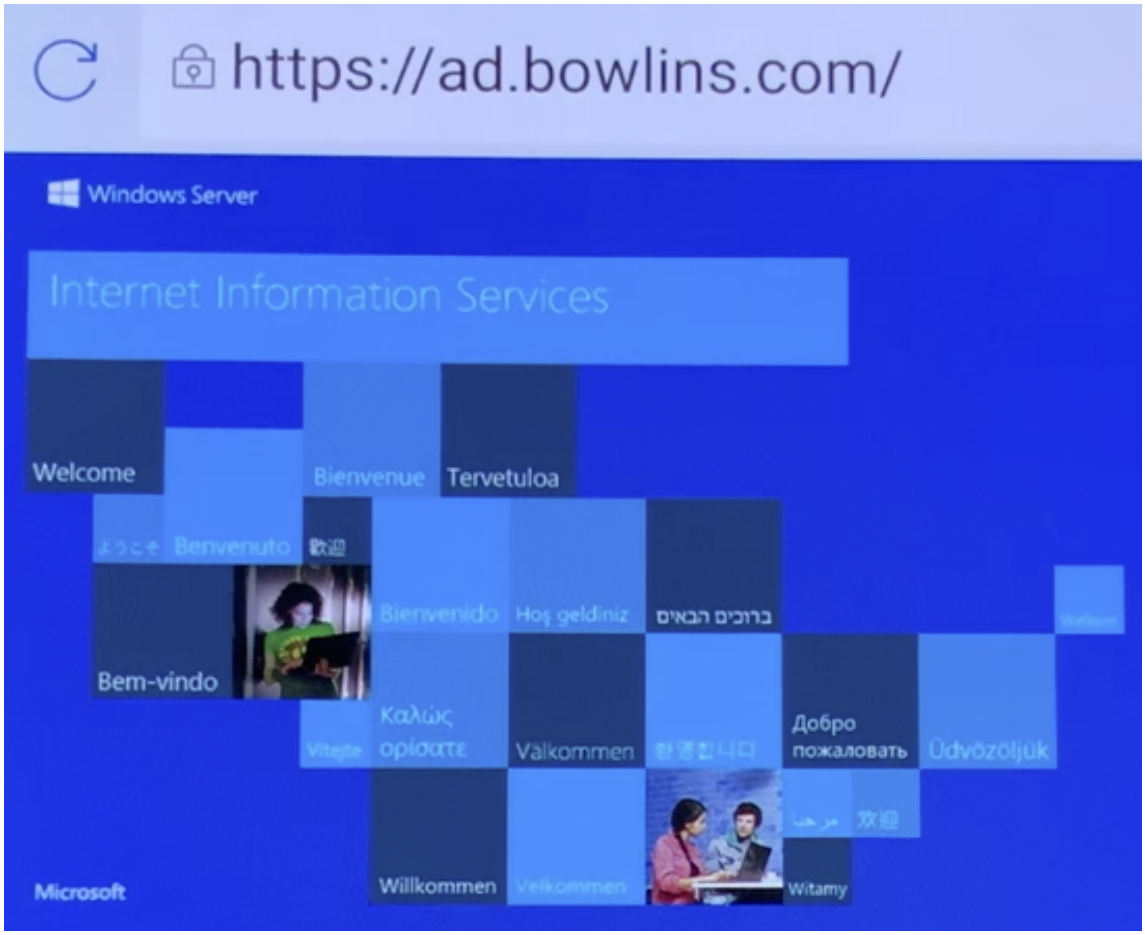
15. ［追加］ をタップします。



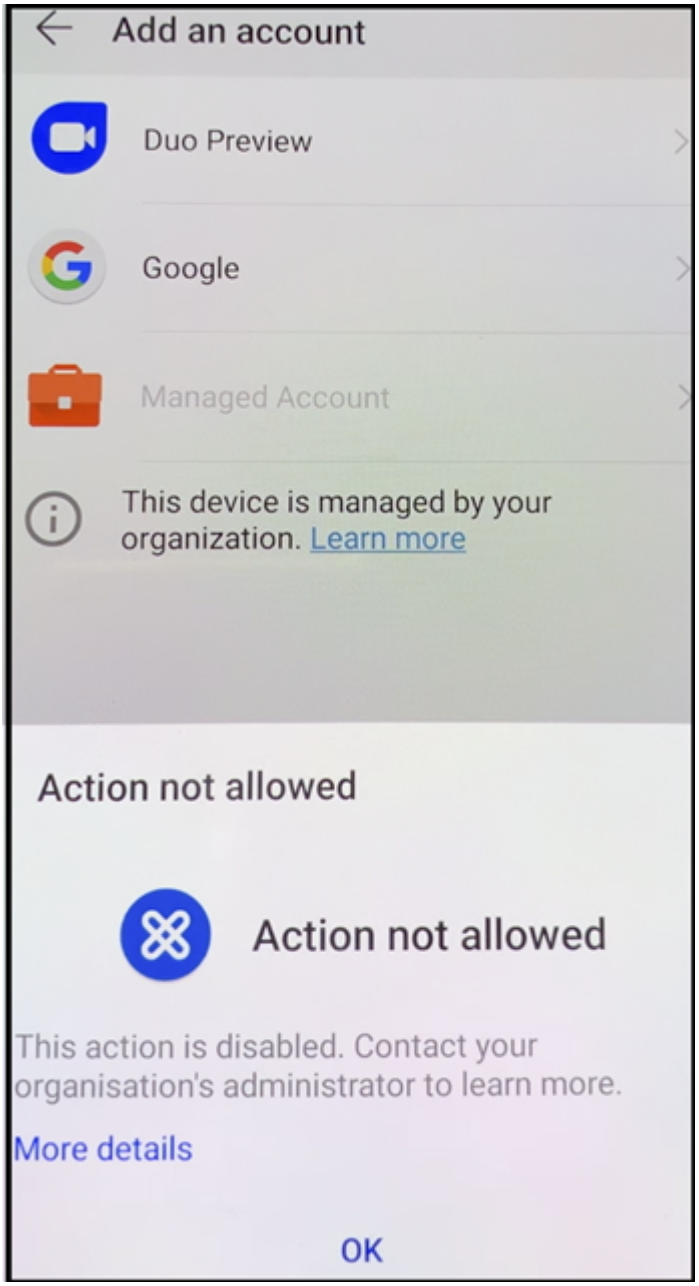
16. Secure Hub で、Secure Web をインストールするために Google Play ストアに移動します。［インストール］ をタップします。



17. Secure Web がインストールされたら、［開く］ をタップします。アドレスバーに内部サイトの URL を入力し、ページが読み込まれることを確認します。



18. デバイスで ［設定］ **>** ［アカウント］ に移動します。管理対象アカウントが変更できないことを確認します。画面の共有またはリモートデバッグのための開発者オプションもブロックされます。



NFC バンプを使用してデバイスを登録する

NFC バンプを使用して完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットされたデバイスと、XenMobile Provisioning Tool を実行するデバイスの 2 台のデバイスが必要です。

システム要件および前提条件

- サポートされる Android デバイス

- 完全に管理されたデバイスとして Android Enterprise 向けにプロビジョニングされた、新規または工場出荷時設定にリセットされたデバイス。この前提条件を完了する手順については、後述します。
- 構成済みの Provisioning Tool を実行している、NFC 機能が備わった別のデバイス。Provisioning Tool は、Secure Hub またはシトリックスのダウンロードページから入手できます。

各デバイスでは、管理対象 Secure Hub という Android Enterprise プロファイルを 1 つのみ保有できます。各デバイスで許可されるプロファイルは 1 つのみです。2 つ目の DPC アプリを追加しようとすると、インストール済みの Secure Hub が削除されます。

NFC バンプを介して転送されるデータ

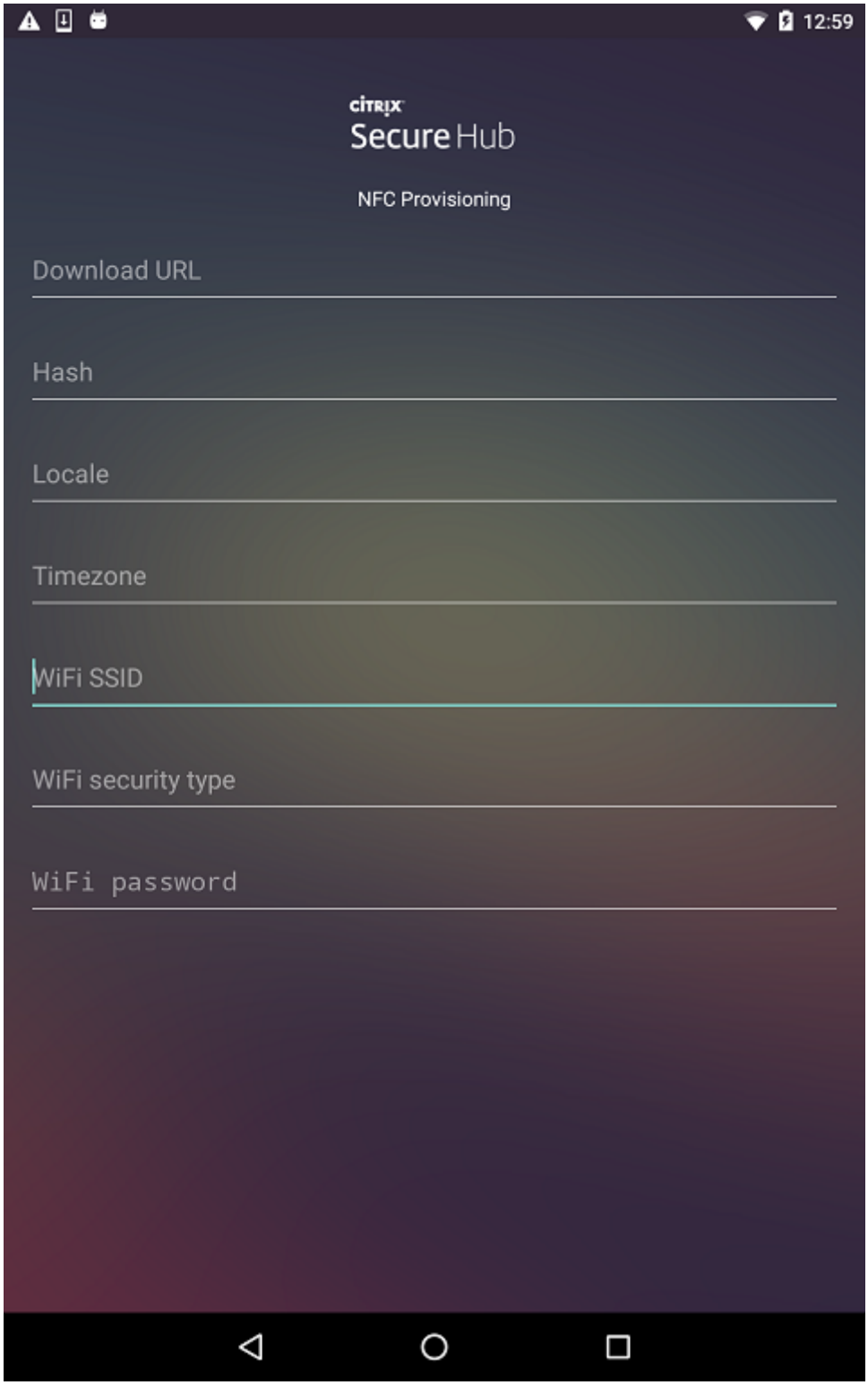
工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータを NFC バンプ経由で送信して Android Enterprise を初期化する必要があります：

- デバイス所有者として機能する DPC アプリ（この場合は Secure Hub）のパッケージ名。
- デバイスが DPC アプリをダウンロードできるイントラネット/インターネット上の場所。
- ダウンロードが正常に完了したかどうかを確認する DPC アプリの SHA1 ハッシュ。
- 工場出荷時の設定にリセットされたデバイスが DPC アプリに接続してダウンロードできるようにする Wi-Fi 接続の詳細。注：現時点では、Android はこの手順での 802.1x Wi-Fi をサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、Provisioning Tool のデータが工場出荷時の設定にリセットされたデバイスに送信されます。このデータはその後、管理者設定での Secure Hub のダウンロードに使用されます。タイムゾーンと場所の値を入力しない場合、新しいデバイスでは Android によって自動的にこれらの値が構成されます。

XenMobile Provisioning Tool の構成

NFC バンプを行う前に、Provisioning Tool を構成する必要があります。この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFC バンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルから入力することもできます。次の手順では、テキストファイルを構成する方法と各フィールドに説明を含める方法について説明します。入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

テキストファイルを使用して **Provisioning Tool** を構成するには

ファイルの名前を nfcprovisioning.txt にして、/sdcard/フォルダーにあるデバイスの SD カードに格納します。アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには、次のデータを含める必要があります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

この行は、EMM プロバイダーアプリのイントラネット/インターネットの場所です。工場出荷時設定のデバイスが NFC バンプの後に Wi-Fi に接続した場合、デバイスはダウンロードのためにこの場所にアクセスする必要があります。URL は通常の URL で、特別な形式にする必要はありません。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>

この行は、EMM プロバイダーアプリのチェックサムです。このチェックサムはダウンロードが成功したかを検証するために使用されます。チェックサムを取得する手順については、後述します。

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

この行は、Provisioning Tool を実行しているデバイスが接続されている Wi-Fi の SSID です。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

サポートされる値は WEP および WPA2 です。Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_LOCALE=<locale>

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

デバイスが実行されるタイムゾーンです。フォームの地域/場所の Olson 名を入力します。たとえば、米国太平洋標準時の場合は「America/Los_Angeles」です。名前を入力しない場合、タイムゾーンは自動的に入力されます。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

このデータは Secure Hub としてアプリにハードコードされるため、必須ではありません。ここでは、情報の完全性を守るためだけに記載しています。

WPA2 を使用して保護された Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk


```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

保護されていない Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Secure Hub チェックサムを取得するには

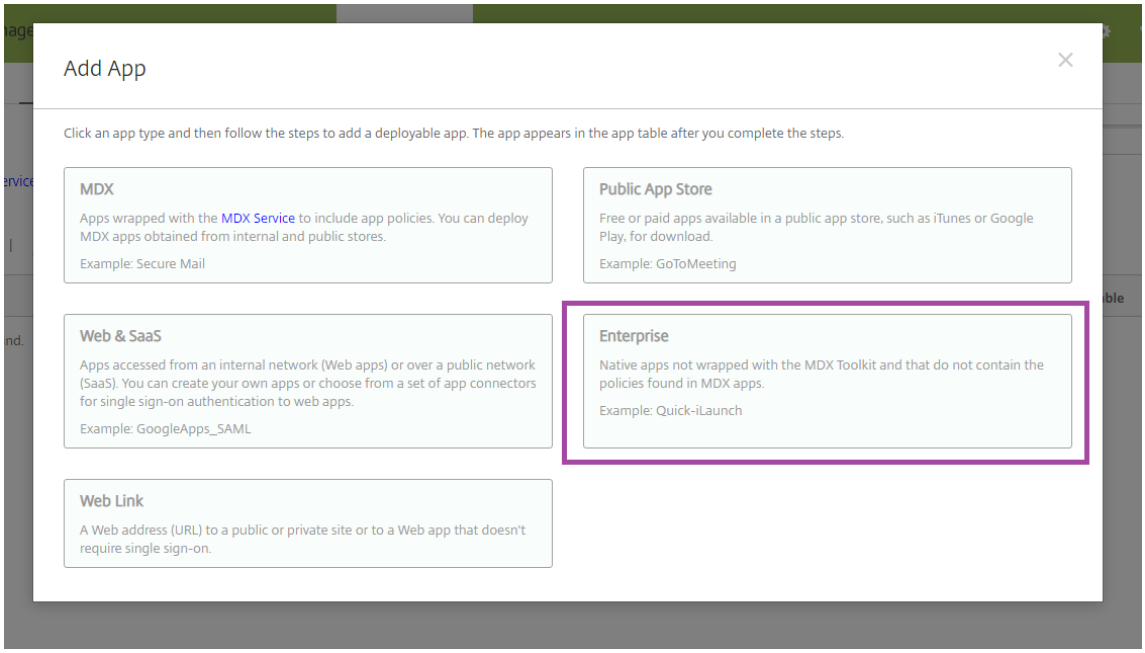
アプリのチェックサムを取得するには、そのアプリをエンタープライズアプリとして追加します。

1. XenMobile コンソールで、［構成］**>**［アプリ］ を選択してから、［追加］ をクリックします。

   ［アプリの追加］ ウィンドウが開きます。

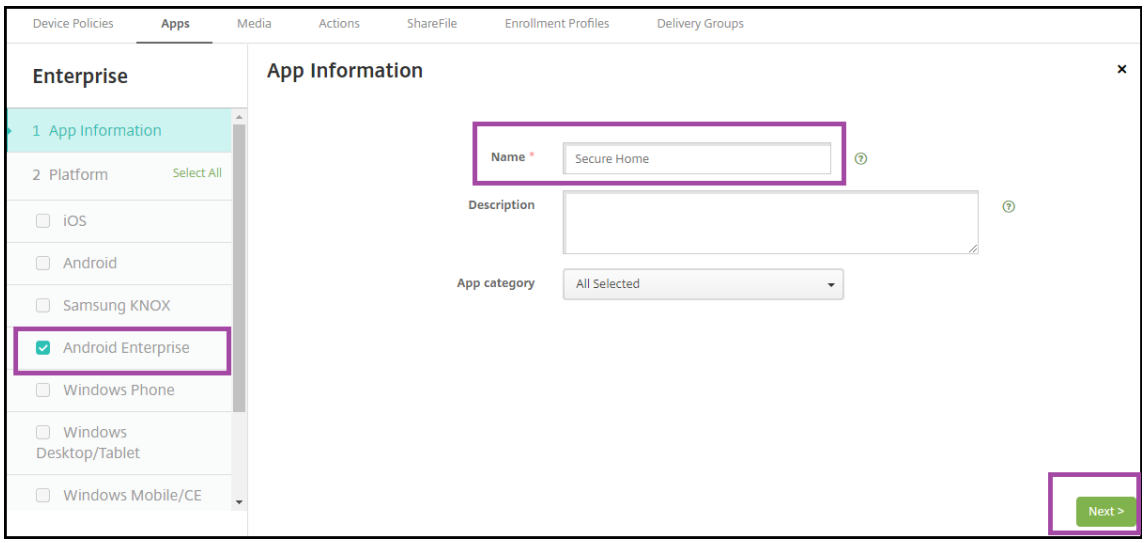
2. ［エンタープライズ］ をクリックします。

   ［アプリ情報］ ページが開きます。



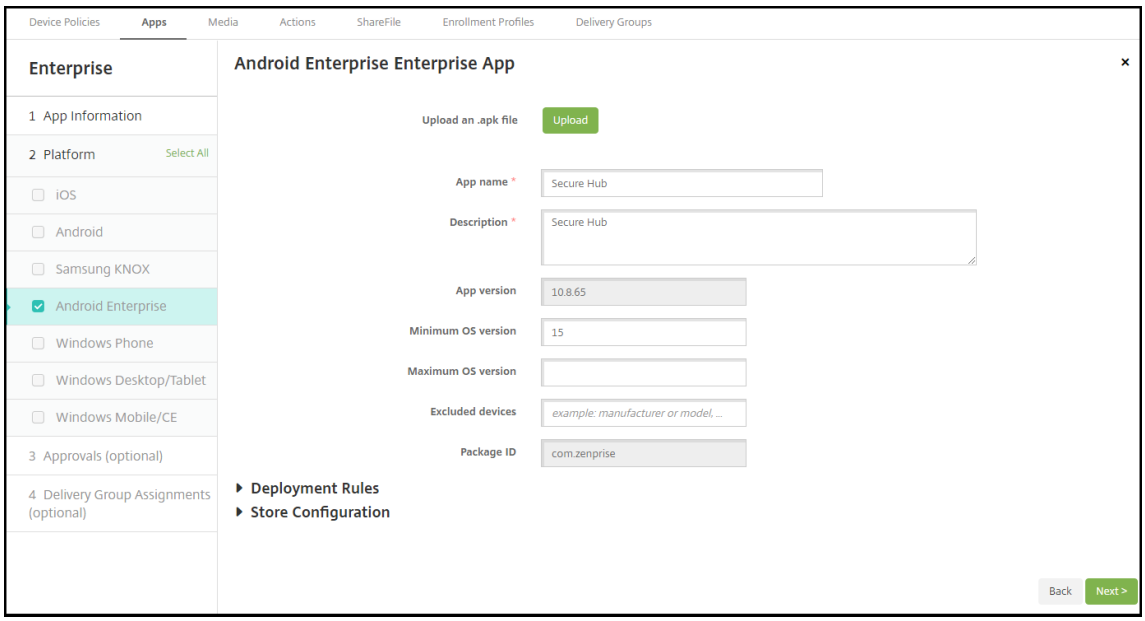
3. 次の構成を選択して ［次へ］ をクリックします。

   ［**Android Enterprise** エンタープライズアプリ］ ページが開きます。

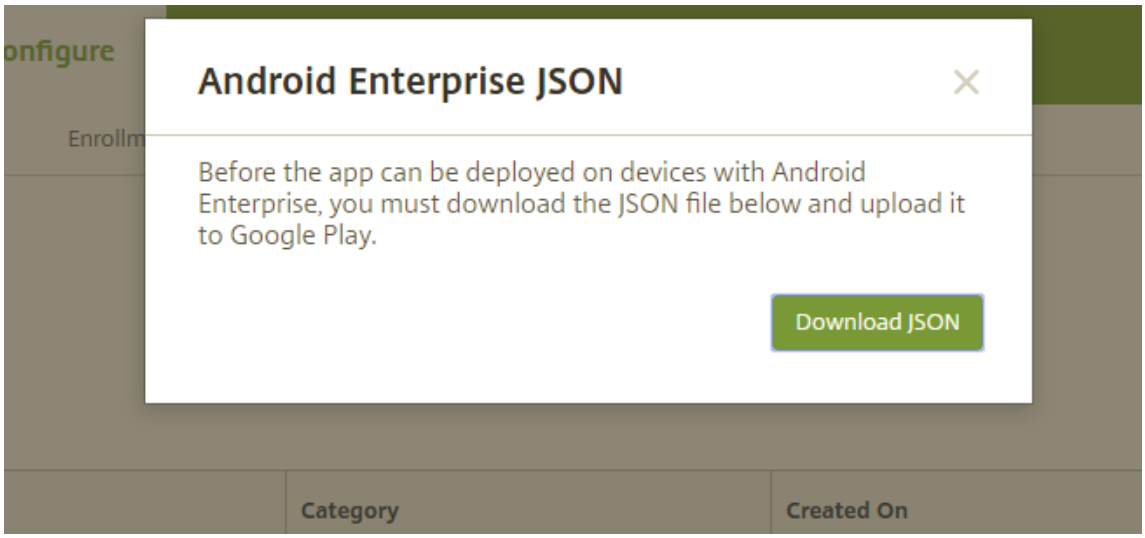


4. .apk へのパスを入力し、 ［次へ］ をクリックしてファイルをアップロードします。

   アップロードが完了すると、アップロードされたパッケージの詳細が表示されます。



5. [次へ] をクリックします。[**JSON** のダウンロード] をクリックして JSON ファイルをダウンロードします。このファイルは、この後 Google Play へのアップロードに使用します。Secure Hub の場合、Google Play にアップロードする必要はありませんが、SHA1 を読み込む元になる JSON ファイルが必要です。



以下の図に、典型的な JSON ファイルの例を示します:

6. **file_sha1_base64** の値をコピーして、この値を Provisioning Tool の [ハッシュ] フィールドで使用します。

> 注：ハッシュは URL セーフのものにする必要があります。

- **+** 記号はすべて**-**に変換します。
- **/**記号はすべて **_** に変換します。
- 末尾の**\u003d** は **=** に置き換えます。

ハッシュをデバイスの SD カードの nfcprovisioning.txt ファイルに格納すると、安全のための変換が行われます。ただし、ハッシュを手動で入力すると、URL の安全性は入力者の責任になります。

使用するライブラリ

Provisioning Tool では、以下のライブラリがソースコードに使用されています。

- v7 appcompat library、Design support library、および v7 Palette library by Google（Apache license 2.0）

  詳しくは、「Support Library の機能」を参照してください。

- Butter Knife by Jake Wharton（Apache license 2.0）

QR コードを使用してデバイスを登録する

QR コードを使用して完全に管理されたデバイスを登録するには、JSON を作成して QR コードに変換し、QR コードを生成します。この QR コードをデバイスカメラでスキャンし、デバイスを登録します。

システム要件

- Android 8.0 以降を実行するすべての Android デバイスでサポートされます。

JSON から **QR** コードを作成する

次のフィールドがある JSON を作成します。

これらのフィールドは必須です。

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

値：com.zenprise / com.zenprise.configuration.AdminFunction

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

値：qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

キー：android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

値：`https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

これらのフィールドはオプションです。

- **android.app.extra.PROVISIONING_LOCALE**: 言語コードおよび国コードを入力します。

  言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。

- **android.app.extra.PROVISIONING_TIME_ZONE**: これはデバイスが実行されているタイムゾーンです。

  フォームの地域/場所の Olson 名を入力します。たとえば、米国太平洋標準時の場合は「America/Los_Angeles」です。入力しない場合、タイムゾーンは自動的に入力されます。

- **android.app.extra.PROVISIONING_LOCAL_TIME:** エポックからのミリ秒単位の時間。

  Unix エポック（または Unix 時間または POSIX 時間または Unix タイムスタンプ）は、1970 年 1 月 1 日（UTC/GMT 午前 0 時）から経過した秒数で、うるう秒数は含まれません（ISO 8601: 1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**: プロファイル作成時に暗号化をスキップするには、**true** に設定します。プロファイルの作成時に暗号化を強制するには、**false** に設定します。

以下の図に、典型的な JSON の例を示します。

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "[redacted]",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

https://jsonlint.comなどの JSON 検証ツールを使用して作成された JSON を検証します。https://goqr.meなどのオンライン QR コードジェネレータを使用して、JSON 文字列を QR コードに変換します。

この QR コードは工場出荷時の設定にリセットされたデバイスによってスキャンされ、これによってデバイスを完全に管理されたデバイスとして登録できます。

デバイスを登録するには

新しいデバイスまたは工場出荷時の設定にリセットされたデバイスの電源を入れた後、以下を行います:

1. ようこそ画面で画面を 6 回タップすると、QR コードの登録フローが開始されます。
2. プロンプトが表示されたら、Wi-Fi に接続します。（JSON でエンコードされた）QR コードにある Secure Hub のダウンロード場所には、この Wi-Fi ネットワーク経由でアクセスできます。

   端末が Wi-Fi に接続されると、Google から QR コードリーダーをダウンロードしてカメラを起動します。
3. カメラを QR コードに合わせて、コードをスキャンします。

   Android は、QR コードのダウンロード場所から Secure Hub をダウンロードし、署名証明書の署名を検証し、Secure Hub をインストールし、デバイス所有者として設定します。

詳しくは、Android EMM デベロッパー向け Google ガイド（https://developers.google.com/android/work/prov-devices#qr_code_method）を参照してください。

ゼロタッチ登録

ゼロタッチ登録を使用すると、初めてデバイスの電源をオンにしたときに完全に管理されているデバイスとしてプロビジョニングするようにセットアップできます。

デバイスのリセラーは、Android のゼロタッチポータルにアカウントを作成します。このポータルは、デバイスに構成を適用できるオンラインツールです。Android のゼロタッチポータルを使用して、1 つまたは複数のゼロタッチ登録構成を作成し、アカウントに割り当てられたデバイスにこの構成を適用します。ユーザーがこれらのデバイスの電源をオンにすると、デバイスは自動的に XenMobile に登録されます。デバイスに割り当てられた構成によって、自動登録プロセスが定義されます。

システム要件

- ゼロタッチ登録は、Android 8.0 以降でサポートされます。

リセラーからのデバイスとアカウントの情報

- ゼロタッチ登録の対象となるデバイスは、エンタープライズリセラーまたは Google パートナーから購入します。Android Enterprise のセロタッチパートナー一覧については、Android の Web サイトを参照してください。
- リセラーによって作成された Android Enterprise のゼロタッチポータルアカウント。
- リセラーから提供された Android Enterprise のゼロタッチポータルアカウントのログイン情報。

ゼロタッチ構成の作成

ゼロタッチ構成を作成する場合は、カスタム JSON を含めて構成の詳細を指定します。

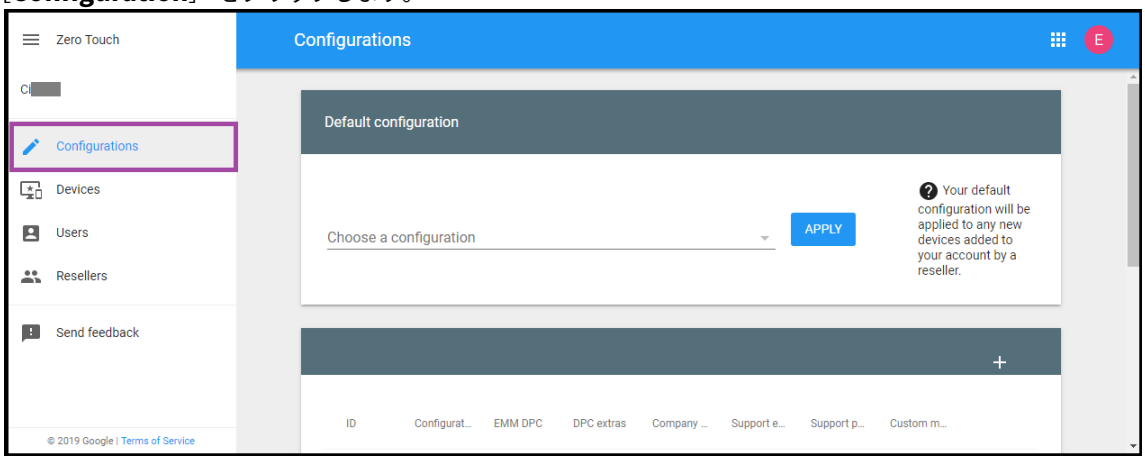
この JSON を使用して、指定した XenMobile Server に登録するようにデバイスを構成します。この例では、サーバーの URL を「URL」に置き換えます。

```
{

    ”android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE”:
  {

        ”serverURL”:”URL”,
    }

 }
```

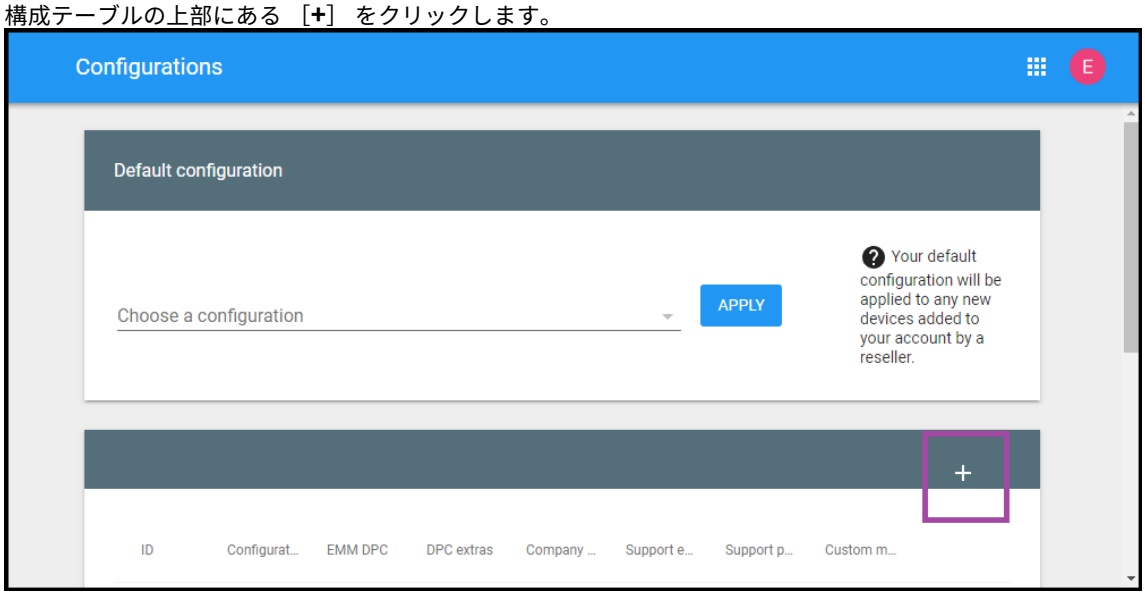
オプションでより多くのパラメーターを持つ JSON を使用して、構成をさらにカスタマイズできます。この例では、XenMobile Server と、この構成を使用するデバイスがそのサーバーにログオンするために使用するユーザー名とパスワードを指定します。


```
{

   ”android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE”:
     {

         ”serverURL”:”URL”,
         ”xm_username”:”username”,
         ”xm_password”:”password”
      }

        }
```

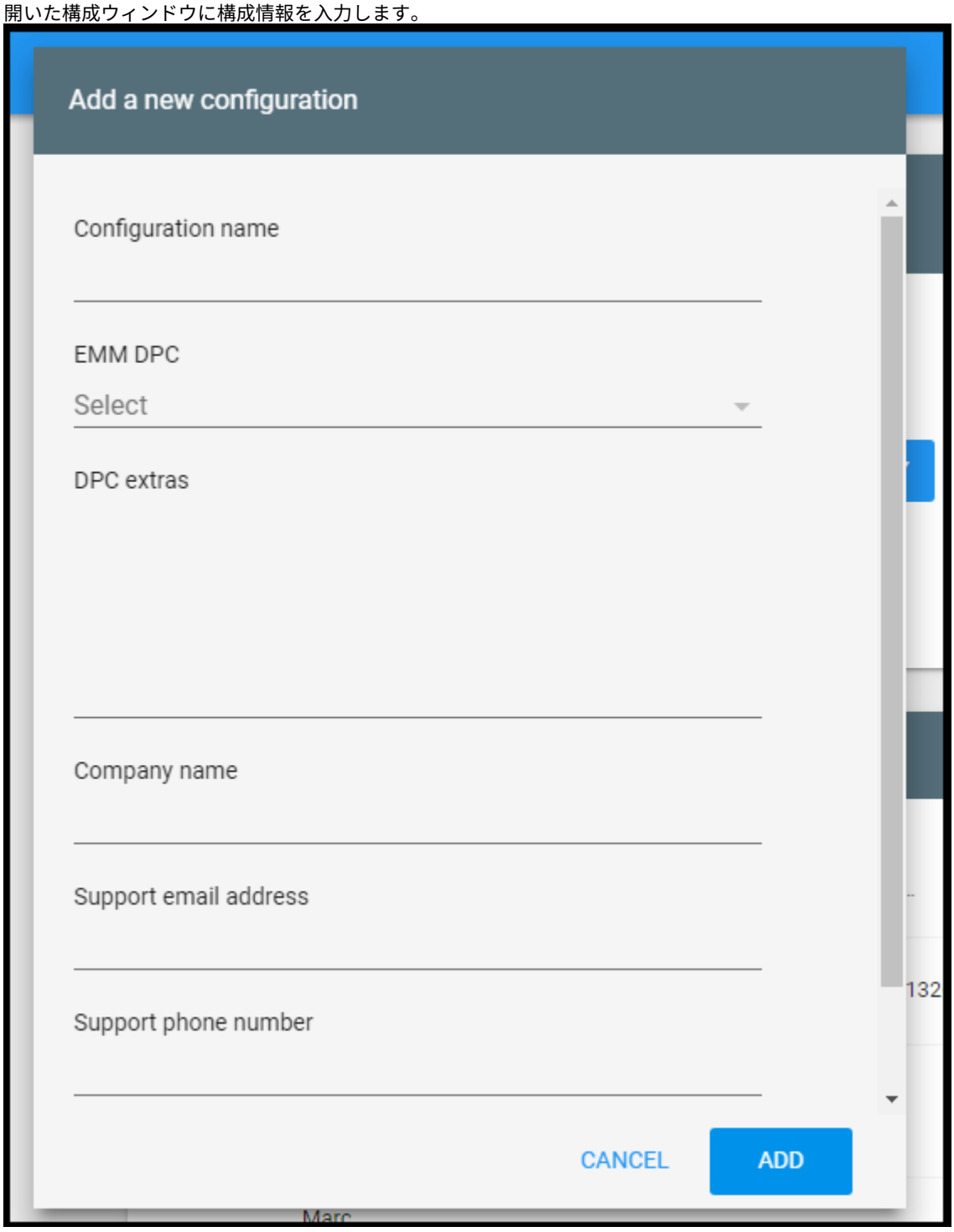
1. Android のゼロタッチポータル（https://partner.android.com/zerotouch）に移動します。ゼロタッチデバイスのリセラーのアカウント情報を使用してログインします。
2. [**Configuration**] をクリックします。



3. 構成テーブルの上部にある [**+**] をクリックします。



4. 開いた構成ウィンドウに構成情報を入力します。



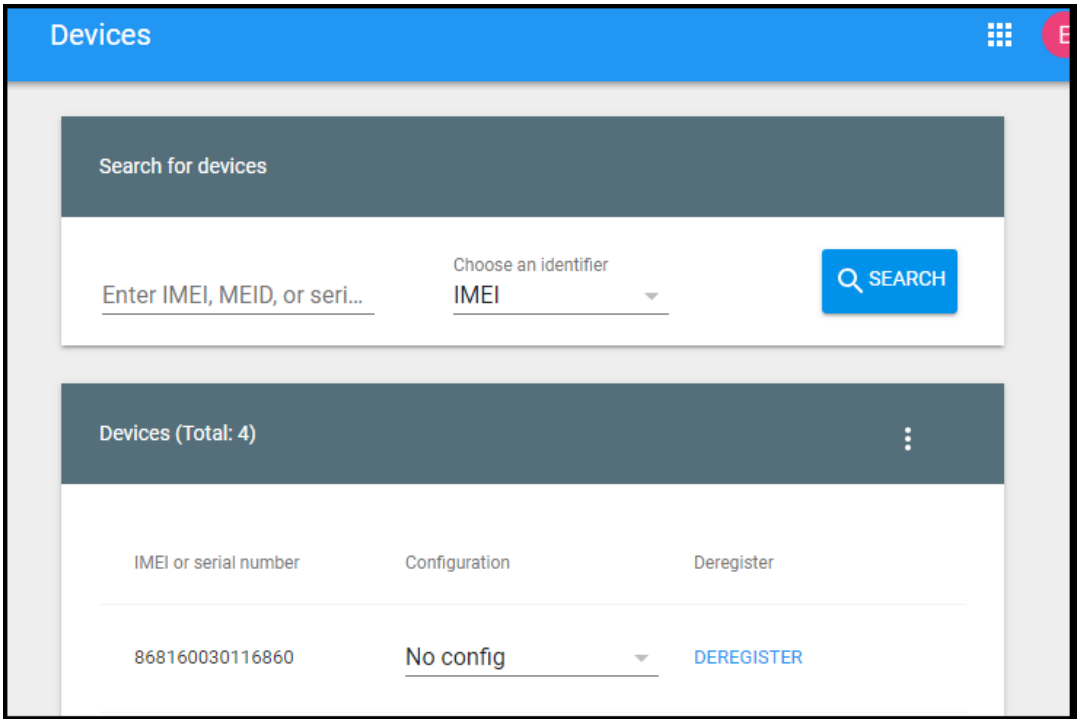
- **Configuration name**： この構成の名前を入力します。
- **EMM DPC**： ［**Citrix Secure Hub**］ を選択します。
- **DPC extras**： カスタム JSON テキストをフィールドに貼り付けます。
- **Company name**： デバイスのプロビジョニング中、Android Enterprise のゼロタッチデバイスに表示させる名前を入力します。

- **Support email address**: サポートが必要なときにユーザーが連絡するメールアドレスを入力します。このアドレスは、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。
- **Support phone number**: ユーザーがサポートが必要なときに連絡する電話番号を入力します。この電話番号は、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。
- **Custom Message**: オプション。ユーザーが管理者にサポートを求めるように促す、またはデバイスで発生している状況をユーザーに説明するための、1、2 行程度の文章を追加します。このカスタムメッセージは、デバイスのプロビジョニング前に Android Enterprise のゼロタッチデバイスに表示されます。

5. [追加] をクリックします。
6. さらに構成を作成するには、手順 2 ～ 4 を繰り返します。
7. デバイスに構成を適用するには、以下の手順を実行します:

   a) Android のゼロタッチポータルで [**Devices**] をクリックします。

   b) デバイスの一覧でデバイスを探し、割り当てる構成を選択します。



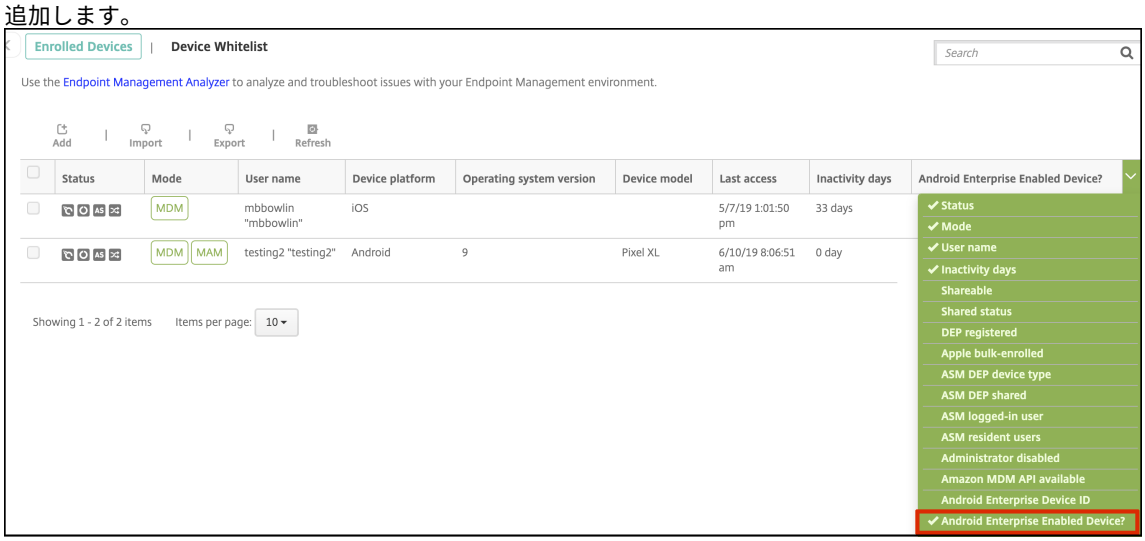
   c) [更新] をクリックします。

CSV ファイルを使用して、多数のデバイスに構成を適用できます。

多数のデバイスに構成を適用する方法については、Android Enterprise のヘルプトピック（ゼロタッチ登録: IT 管理者向け）を参照してください。この Android Enterprise のヘルプトピックには、構成を管理してデバイスに適用する方法の詳細が記載されています。

XenMobile コンソールで完全に管理されたデバイスを表示する

1. XenMobile コンソールで、［管理］**>**［デバイス］ の順に移動します。
2. このページの表の右側にあるメニューをクリックして、［**Android Enterprise** 対応デバイスですか**?**］ 列を追加します。



3. 利用可能なセキュリティアクションを表示するには、完全に管理されたデバイスを選択して ［セキュリティ］ をクリックします。デバイスが完全に管理されている場合、完全なワイプ操作は使用できますが、選択的なワイプ操作は使用できません。これは、デバイスが管理対象 Google Play ストアのアプリのみを許可するためです。ユーザーがパブリックストアからアプリケーションをインストールするオプションはありません。組織はデバイス上のすべてのコンテンツを管理しています。

Android Enterprise 専用デバイスのプロビジョニング

Android Enterprise 専用デバイスは、単一のユースケース専用の完全に管理されたデバイスです。これらのデバイスは、このユースケースに必要なタスクを実行する 1 つのアプリまたはアプリの小セットのみに制限されます。また、ユーザーがこれらのデバイスで他のアプリを有効にしたり、他の操作を実行したりすることを禁止することもできます。

専用デバイスは、「Android Enterprise の完全に管理されたデバイスのプロビジョニング」の説明のとおり、他の完全に管理されたデバイスで使用されている登録方法のいずれかを使用して登録されます。専用デバイスをプロビジョニングするには、登録前に追加のセットアップが必要です。

専用デバイスは、企業所有の単一使用（COSU）デバイスとも呼ばれます。

> 注：
>
> 他の完全に管理されたデバイスとは異なり、専用デバイスは Active Directory アカウントを持つユーザーのみが登録できます。ローカルユーザーは専用デバイスを登録できません。

専用デバイスをプロビジョニングするには：

- XenMobile 管理者が専用デバイスを XenMobile 展開に登録できるように、役割ベースのアクセス制御（RBAC）の役割を追加します。専用デバイスを登録するユーザーにこの役割を割り当てます。
- XenMobile 管理者が専用デバイスを XenMobile 展開に登録できるように、XenMobile 管理者の登録プロファイルを追加します。
- 専用デバイスがアクセスするアプリをホワイトリストに登録します。
- 必要に応じて、ホワイトリストのアプリがロックタスクモードを許可するように設定します。アプリがロックタスクモードになると、ユーザーがアプリを開いた時にデバイス画面にアプリが固定されます。［ホーム］ボタンは表示されず、［戻る］ボタンは無効になります。ユーザーは、サインアウトなど、アプリでプログラムされた操作を使用してアプリを終了します。
- 各デバイスを完全に管理されたデバイスとして登録します。

システム要件

- 専用デバイスの登録は、Android 6.0 以降でサポートされます。

専用デバイス用の **RBAC** 役割を追加する

専用デバイスを登録するための RBAC の役割により、XenMobile はデバイスに管理対象 Google Play アカウントをサイレントプロビジョニングし、アクティブにすることができます。管理された Google Play のユーザーアカウントとは異なり、これらのデバイスアカウントは、ユーザーに関連付けられていないデバイスを識別します。

この RBAC 役割を XenMobile 管理者に割り当てて、専用デバイスを登録できるようにします。

専用デバイスを登録するための RBAC 役割を追加するには：

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［役割ベースのアクセス制御］ をクリックします。［役割ベースのアクセス制御］ページが開き、4 つのデフォルトのユーザー役割と、以前に追加した役割が表示されます。
3. ［追加］ をクリックします。［役割の追加］ ページが開きます。
4. 次の情報を入力します。
   - **RBAC** 名: 「COSU」と入力するか、役割を説明する名前を入力します。役割の名前は変更できません。
   - **RBAC** テンプレート: ［ADMIN］テンプレートを選択します。
   - 承認済みアクセス: ［管理コンソールへのアクセス］ および ［**COSU** デバイスの登録機能］ を選択します。
   - コンソールの機能: ［デバイス］ を選択します。
   - 適用権限: COSU の役割を適用するグループを選択します。［特定のユーザーグループ］ をクリックするとグループの一覧が開き、1 つまたは複数のグループを選択できます。
5. ［次へ］ をクリックします。［割り当て］ ページが開きます。
6. Active Director グループに役割を割り当てるために、次の情報を入力します。
   - ドメインを選択: 一覧から、ドメインを選択します。
   - ユーザーグループを含める: 使用可能なすべてのグループ一覧を表示するには、［検索］ をクリックします。または、グループ名の一部または全部を入力して、その名前のグループのみに表示を限定できます。
   - 表示された一覧で、役割を割り当てるユーザーグループを選択します。ユーザーグループを選択すると、［選択したユーザーグループ］ の一覧にグループが表示されます。

7. ［保存］ をクリックします。

専用（**COSU**）登録プロファイルの追加

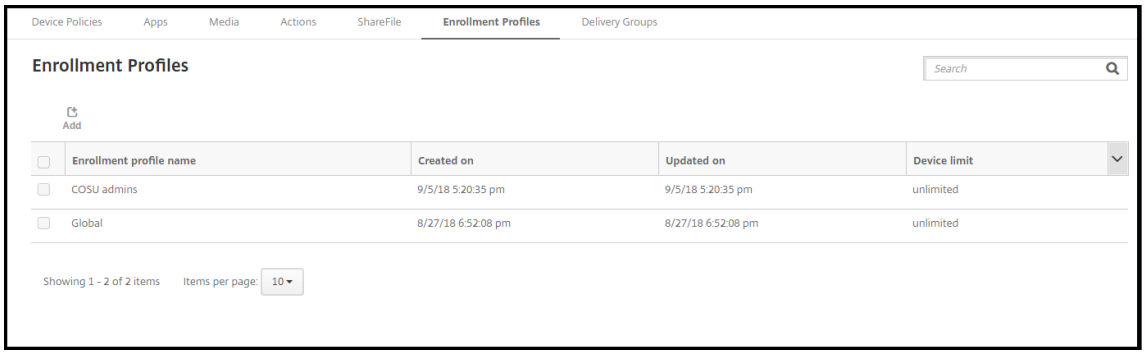
XenMobile 展開に専用デバイスが含まれている場合、1 人の XenMobile 管理者、または数人の管理者グループが多数の専用デバイスを登録します。こうした管理者が必要なすべてのデバイスを登録できるようにするには、ユーザーごとに無制限のデバイスを許可した状態で登録プロファイルを作成します。このプロファイルを、専用デバイスを登録する管理者を含むデリバリーグループに割り当てます。これによって、デフォルトのグローバルプロファイルにユ

ーザーあたりのデバイス数が制限されている場合でも、管理者はデバイスを無制限に登録できます。これらの管理者は、専用（COSU）登録プロファイルに含める必要があります。

1. XenMobile コンソールで、［構成］**>**［登録プロファイル］ の順に移動します。デフォルトの Global プロファイルが表示されます。
2. 登録プロファイルを追加するには、［追加］ をクリックします。［登録情報］ページで、登録プロファイルの名前を入力します。このプロファイルのメンバーが登録できるデバイスの数が無制限に設定されていることを確認します。

3. ［次へ］ をクリックします。［デリバリーグループ割り当て］ページが開きます。
4. 専用デバイスを登録した管理者を含む、1 つまたは複数のデリバリーグループを選択します。次に、［保存］ をクリックします。

［登録プロファイル］ページに、追加したプロファイルが表示されます。



アプリをホワイトに登録しロックタスクモードを設定

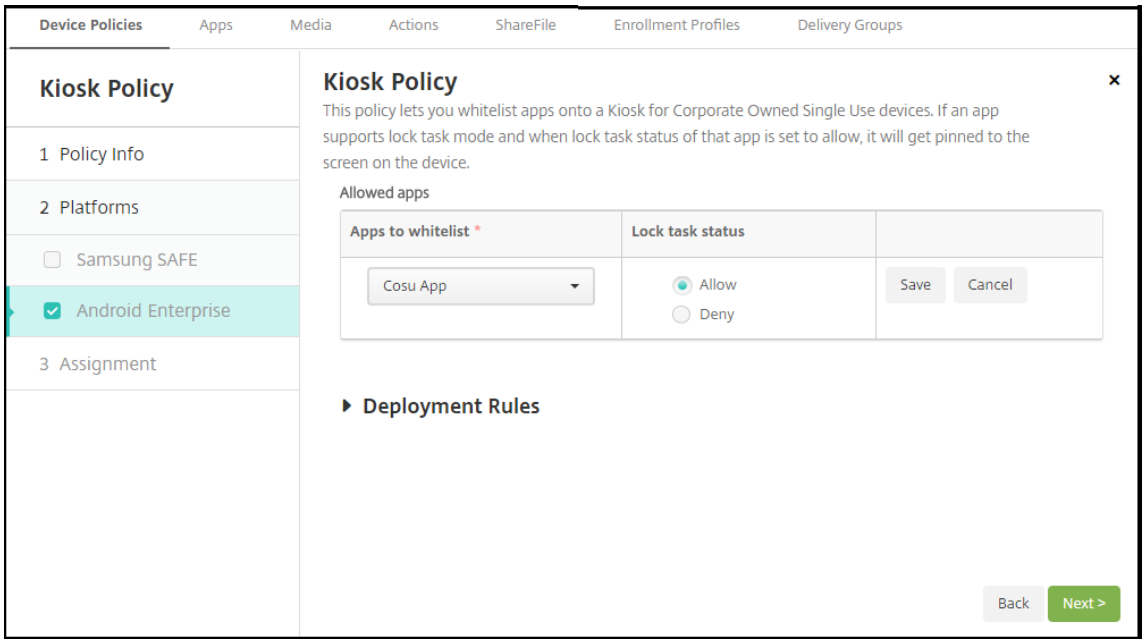
キオスクデバイスポリシーを使用すると、アプリがホワイトリストに登録され、ロックタスクモードを設定できます。デフォルトでは、Secure Hub と Google Play サービスはホワイトリストに登録されています。

キオスクポリシーを追加するには:

1. XenMobile コンソールで、［構成］**>**［デバイスポリシー］ をクリックします。［デバイスポリシー］ ページが開きます。
2. ［追加］ をクリックします。［新しいポリシーの追加］ ダイアログボックスが開きます。
3. ［詳細］ を展開した後、［セキュリティ］の下の ［キオスク］ をクリックします。［キオスクポリシー］ページが開きます。
4. ［プラットフォーム］で ［**Android Enterprise**］ を選択します。他のプラットフォームをクリアします。
5. ［ポリシー情報］ペインで、［ポリシー名］ および任意で ［説明］ を入力します。
6. ［次へ］ をクリックし、［追加］ をクリックします。
7. アプリをホワイトリストに登録し、ロックタスクモードを許可または拒否するには:

   ホワイトリストに登録するアプリを一覧から選択します。

   ユーザーがアプリを起動した時にアプリをデバイス画面に固定するには、［許可］ を選択します。アプリをデバイス画面に固定しない場合は、［禁止］ を選択します。デフォルトは ［許可］ です。



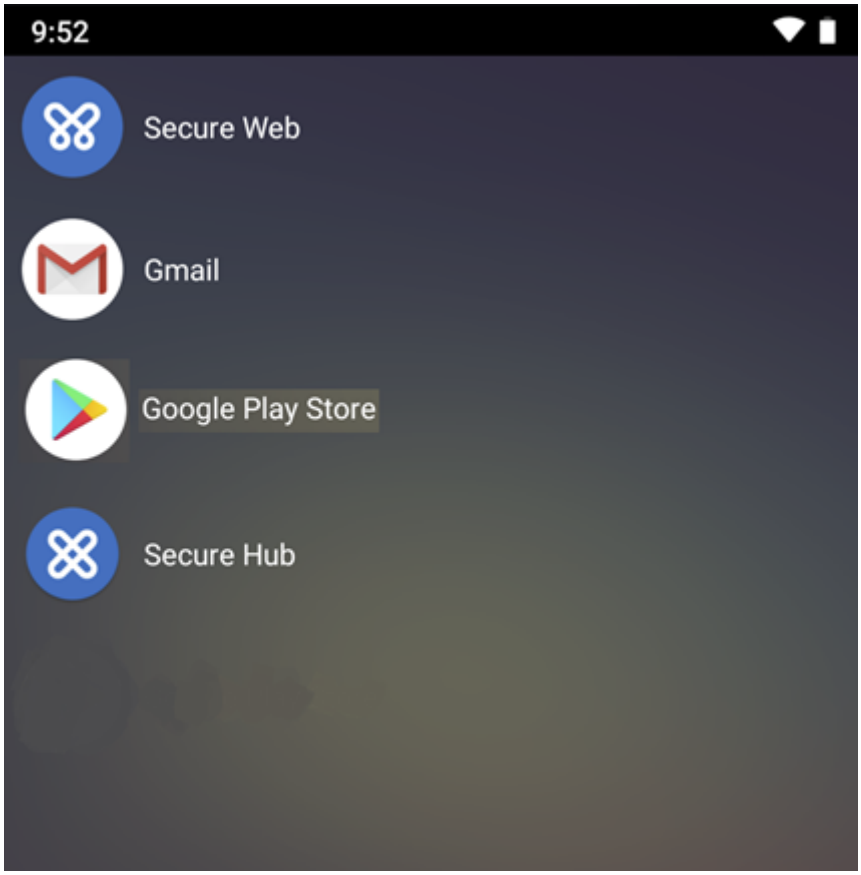
8. ［保存］ をクリックします。
9. さらにアプリをホワイトリストに登録し、ロックタスクモードを許可または禁止する場合は、［追加］ をクリックします。
10. 展開規則を構成し、デリバリーグループを選択します。詳しくは、「デバイスポリシー」を参照してください。

デバイスを登録するには

1. 新しいデバイスまたは工場出荷時の設定にリセットされたデバイスの電源を入れます。

2. デバイスを完全に管理されたデバイスとして登録し、専用のデバイス RBAC 役割を持つユーザーに割り当てます。

デバイスが登録されると、ユーザーが実行できるアプリのリストが表示され、この画面にロックされます。



この例は、Gmail がデバイス上にある間は実行できないことを示しています。

Android Enterprise デバイスポリシーの構成

デバイスポリシーを使用して、XenMobile と Android Enterprise を実行するデバイスとの通信に関する構成を行います。次の表は、Android Enterprise デバイスで使用可能なデバイスポリシーの一覧です。

> 重要:
>
> Android Enterprise に登録して MDX アプリを使用するデバイスの場合: MDX および Android Enterprise を介して一部の設定を制御できます。MDX に対して最も制限の少ないポリシー設定を使用し、Android Enterprise を介してポリシーを制御します。

Android Enterprise 管理対象の構成　アプリインベントリ　アプリアンインストール

OS 更新の制御	資格情報	カスタム XML
Exchange	ファイルデバイスポリシー	キオスク
場所	パスコード	制限
Samsung MDM ライセンスキー	スケジュール設定	Wi-Fi

セキュリティ操作

Android Enterprise は、以下のセキュリティ操作をサポートしています。各セキュリティ操作の説明については、「セキュリティ操作」を参照してください。

セキュリティ操作	Android Enterprise（BYOD）	Android Enterprise（会社所有）
証明書の書き換え	はい	はい
完全なワイプ	いいえ	はい
検索	はい	はい
ロック	はい	はい
パスワードのロックとリセット	いいえ	はい
通知（通知音）	はい	はい
取り消し	はい	はい
選択的なワイプ	はい	いいえ

> 注：
>
> 位置情報デバイスポリシーでデバイスの位置情報モードが ［高精度］ モードまたは ［バッテリー節約］ モードに設定されていない限り、検索セキュリティアクションは失敗します。
>
> ロックおよびパスワードのリセットコマンドは、Android 8.0 より前のバージョンの Android を実行する、仕事用プロファイルデバイスではサポートされていません。Android 8.0 以降を実行する仕事用プロファイルデバイスの場合：送信されたパスコードによって仕事用プロファイルはロックされますが、デバイスはロックされません。パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たさず、仕事用プロファイルに設定済みのパスコードがない場合：デバイスはロックされます。パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていないが、仕事用プロファイルにパスコードが設定済みの場合：仕事用プロファイルはロックされますが、デバイスはロックされません。

Android Enterprise エンタープライズの登録を解除する

Android Enterprise エンタープライズを使用しない場合は、エンタープライズの登録を解除できます。

> 警告:
>
> エンタープライズの登録を解除すると、エンタープライズ経由で登録されていたデバイスの Android Enterprise アプリはデフォルトの状態にリセットされます。これらのデバイスは Google の管理対象外になります。それらのデバイスを Android Enterprise エンタープライズで再登録しても、以前の機能を復元することはできません。追加で構成を行う必要があります。

Android Enterprise エンタープライズの登録を解除した後:

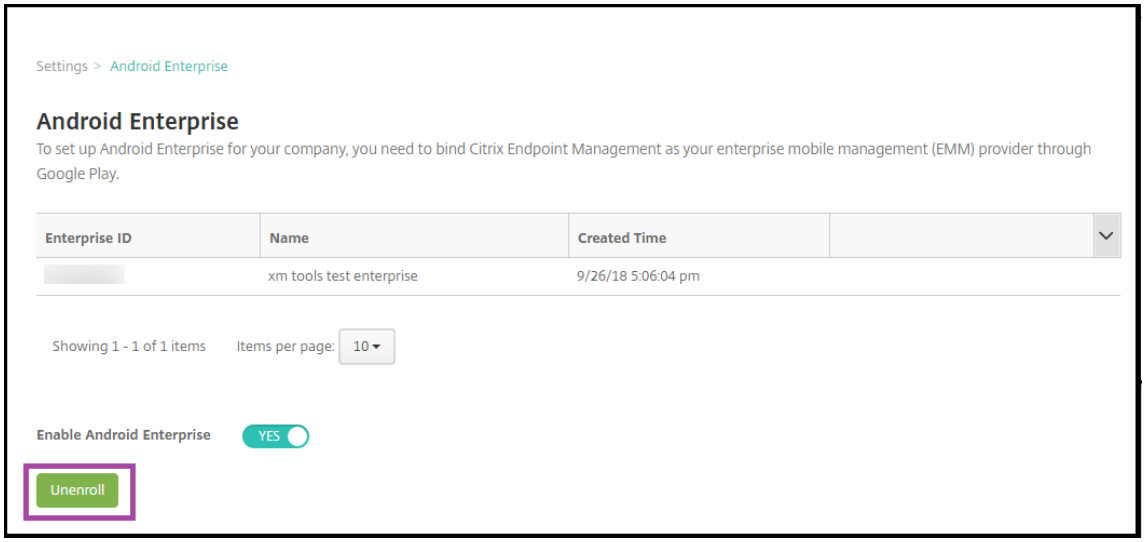
- エンタープライズ経由で登録されていたデバイスとユーザーの Android Enterprise アプリは、デフォルト状態にリセットされます。以前に適用されていた［Android Enterprise 管理対象の構成］ポリシーは無効になります。
- XenMobile はエンタープライズ経由で登録されたデバイスを管理します。Google からは、これらのデバイスは管理されてないと見なされるため、新しい Android Enterprise アプリを追加することはできません。［Android Enterprise 管理対象の構成］ポリシーは適用できません。［スケジュール設定］、［パスワード］、［制限］などのその他のポリシーは、これらのデバイスに適用できます。
- Android Enterprise にデバイスを登録しようとすると、Android Enterprise デバイスではなく Android デバイスとして登録されます。

XenMobile Server コンソールと XenMobile Tools を使用して、Android Enterprise エンタープライズを登録解除します。

このタスクを実行すると、XenMobile サーバーに XenMobile ツールのポップアップウィンドウが開きます。始める前に、XenMobile サーバーに、使用する Web ブラウザーでポップアップウィンドウを開く権限があることを確認してください。Google Chrome などの一部のブラウザーでは、ポップアップブロックを無効にし、XenMobile サイトのアドレスをポップアップブロックのホワイトリストに追加する必要があります。

Android Enterprise エンタープライズの登録を解除するには:

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで、［**Android Enterprise**］ をクリックします。
3. ［登録解除］ をクリックします。



G Suite ユーザー向けの従来の Android Enterprise

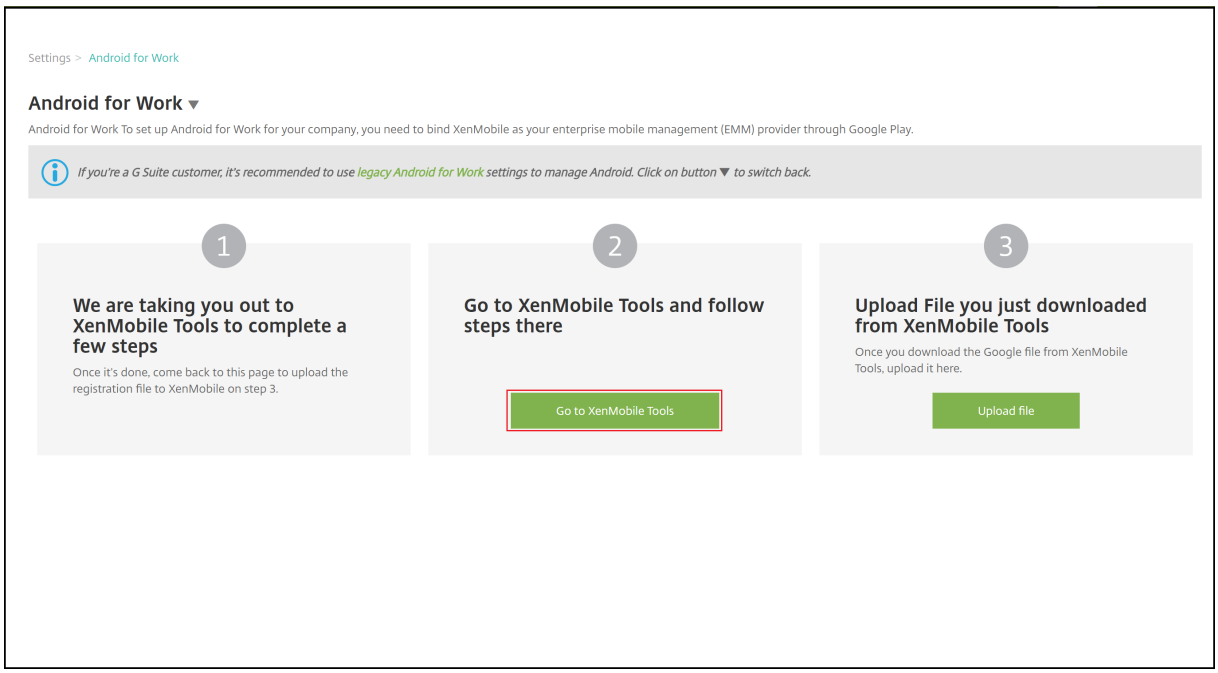
January 10, 2020

G Suite ユーザーが従来の Android Enterprise を構成するには、従来の Android Enterprise の設定を使用する必要があります。

従来の Android Enterprise の要件:

- パブリックにアクセスできるドメイン
- Google 管理者アカウント
- 管理されたプロファイルサポートがあり、Android 5.0 以降の Lollipop を実行しているデバイス
- Google Play がインストールされている Google アカウント
- デバイスで設定されたワークプロファイル

従来の Android Enterprise の構成を始めるには、XenMobile 設定の ［**Android Enterprise**］ ページで ［従来の **Android Enterprise**］ をクリックします。



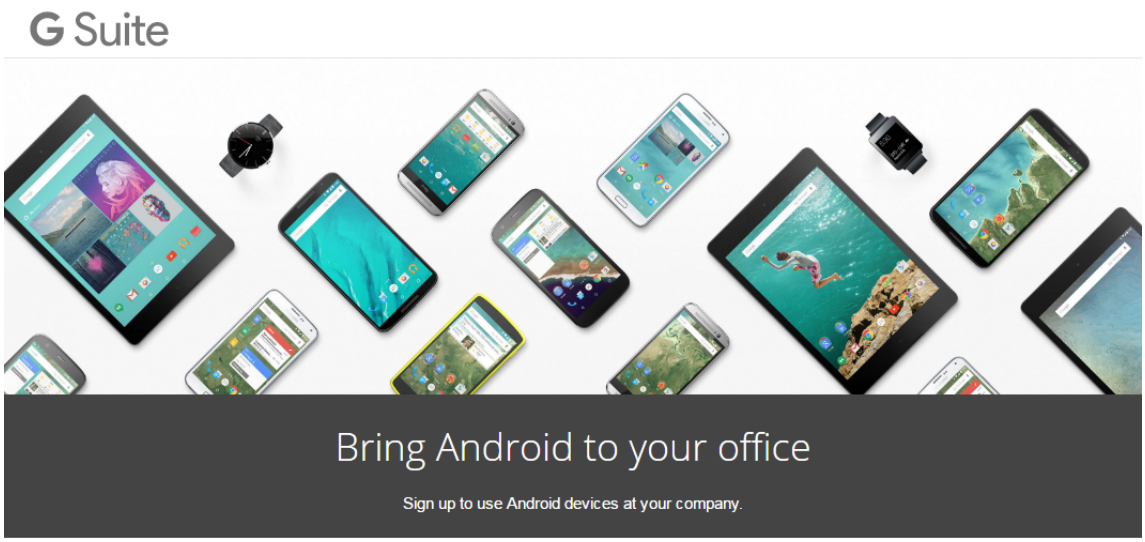
Android Enterprise アカウントの作成

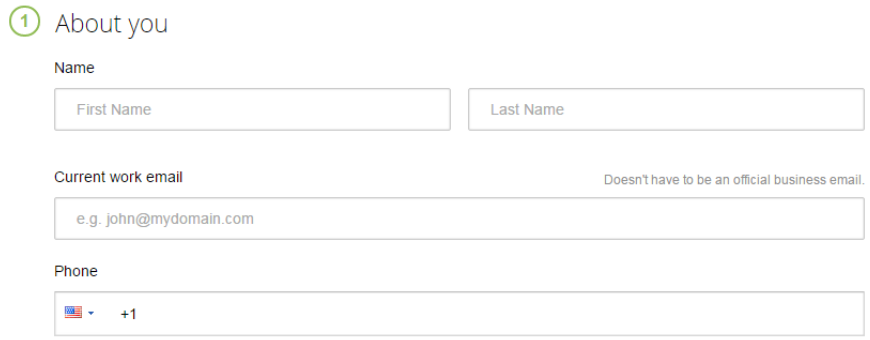
Android Enterprise アカウントをセットアップするには、Google でドメイン名を検証する必要があります。

ドメイン名が既に Google で検証済みの場合は、以下の手順を省略して「Android Enterprise サービスアカウントの設定と Android Enterprise 証明書のダウンロード」に進むことができます。

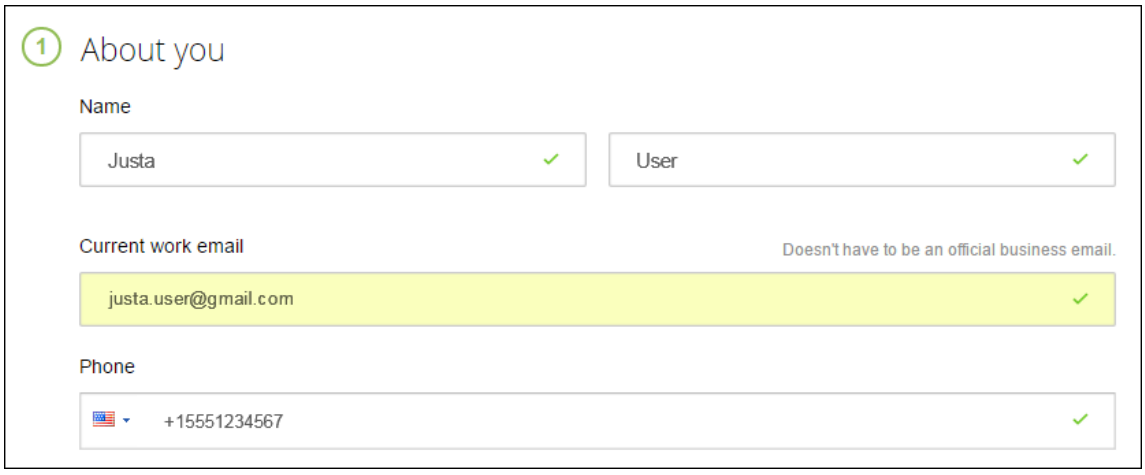
1. https://www.google.com/a/signup/?enterprise_product=ANDROID_WORKにアクセスします。

   管理者情報と会社情報を入力する次のページが開きます。

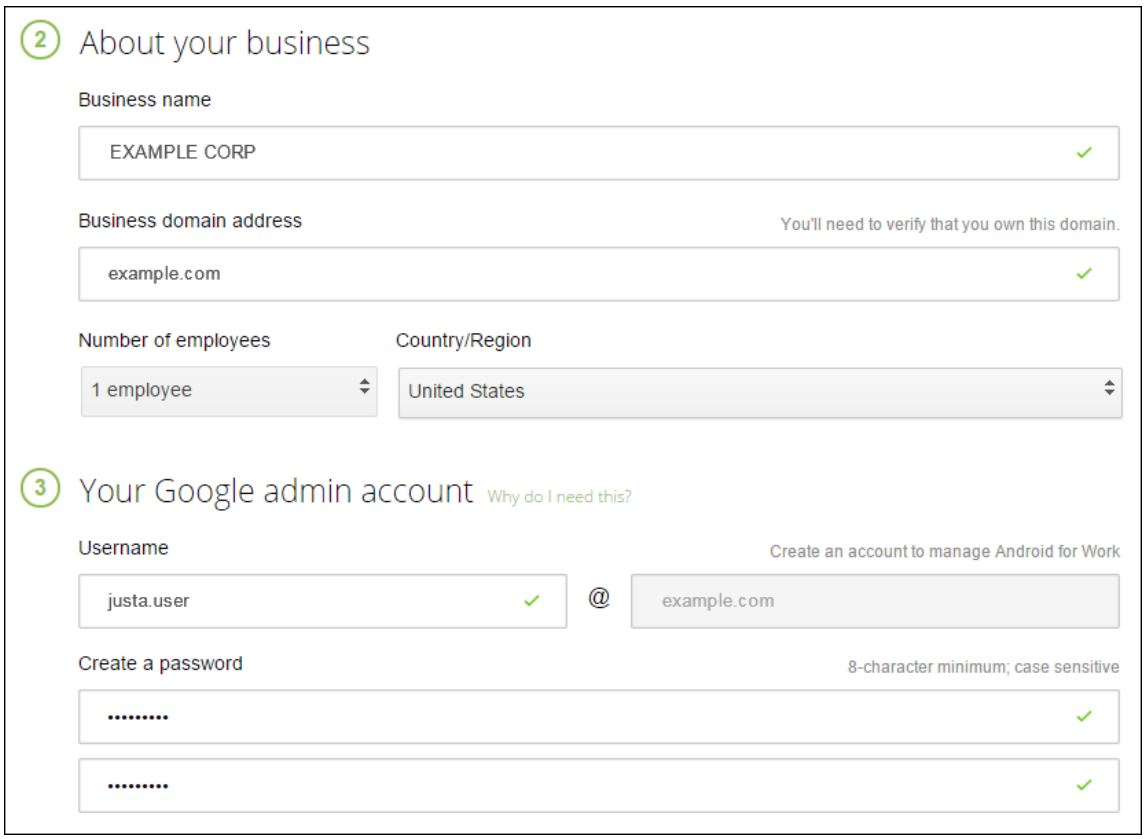




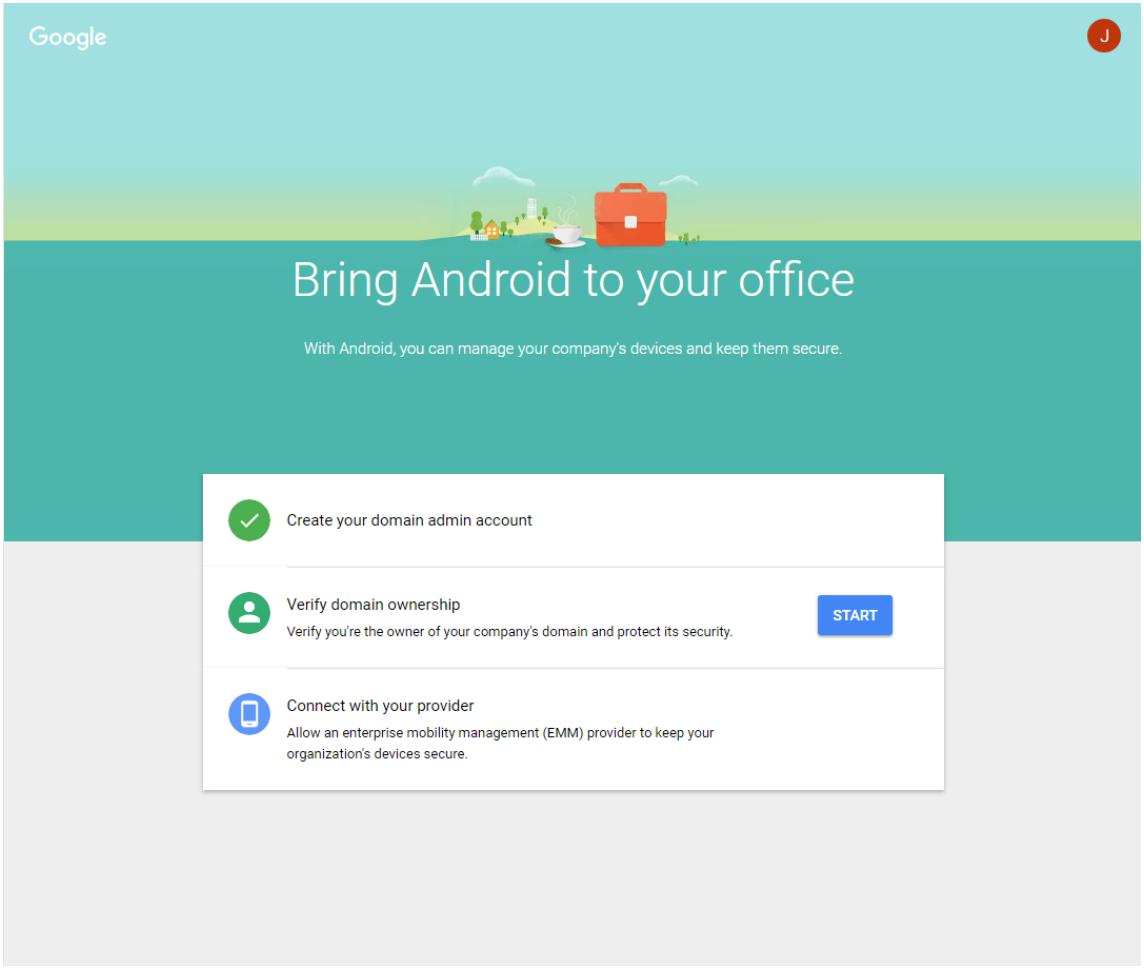
2. 管理者のユーザー情報を入力します。



3. 管理者のアカウント情報だけでなく、会社情報も入力してください。



プロセスの最初の手順が完了します。以下のページが開きます。



ドメイン所有権の検証

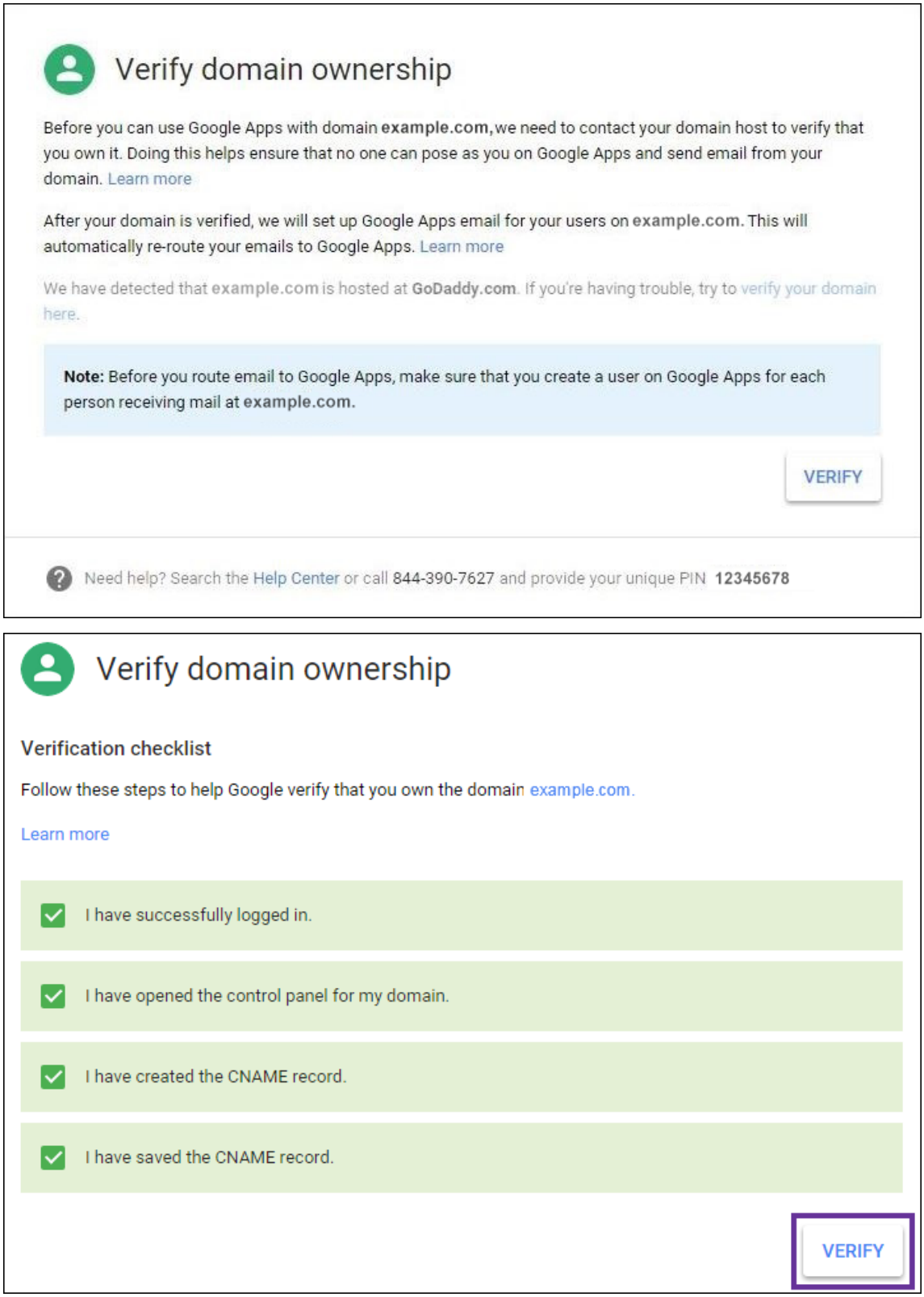
以下のいずれかの方法で、Google がドメインを検証できるようにします。

- ドメインホストの Web サイトに TXT または CNAME レコードを追加します。
- HTML ファイルをドメインの Web サーバーにアップロードします。
- ホームページに<meta>タグを追加します。Google では最初の方法を推奨しています。ドメインの所有権を検証する手順についてはこの記事では扱いませんが、必要な情報はhttps://support.google.com/a/answer/6248925に記載されています。

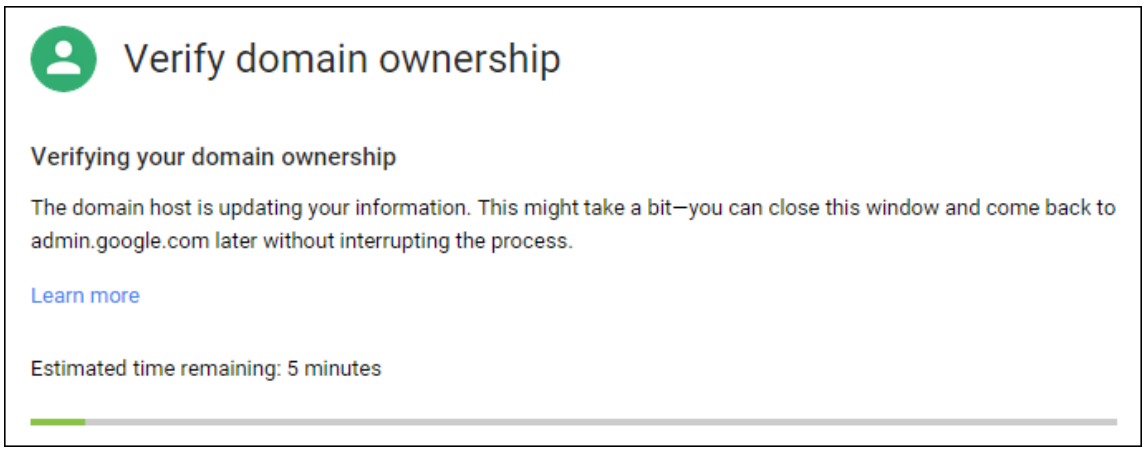
1. [**Start**] をクリックして、ドメインの検証を開始します。

   [**Verify domain ownership**] ページが開きます。画面の指示に従ってドメインを検証します。

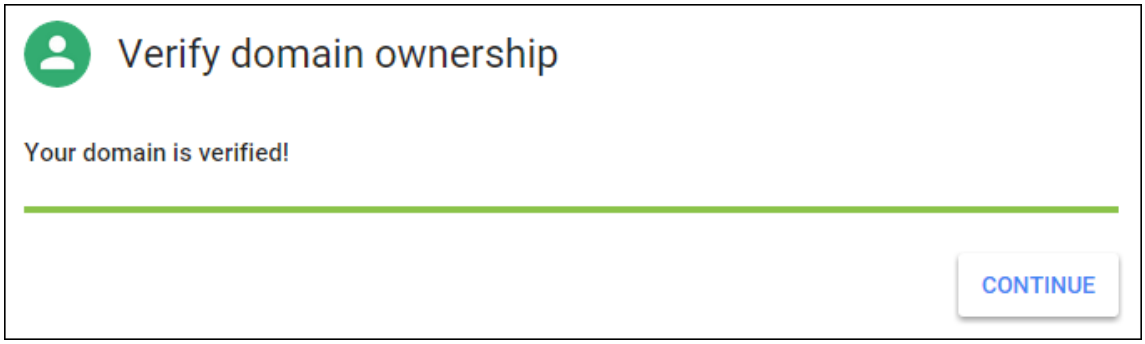
2. [**Verify**] をクリックします。



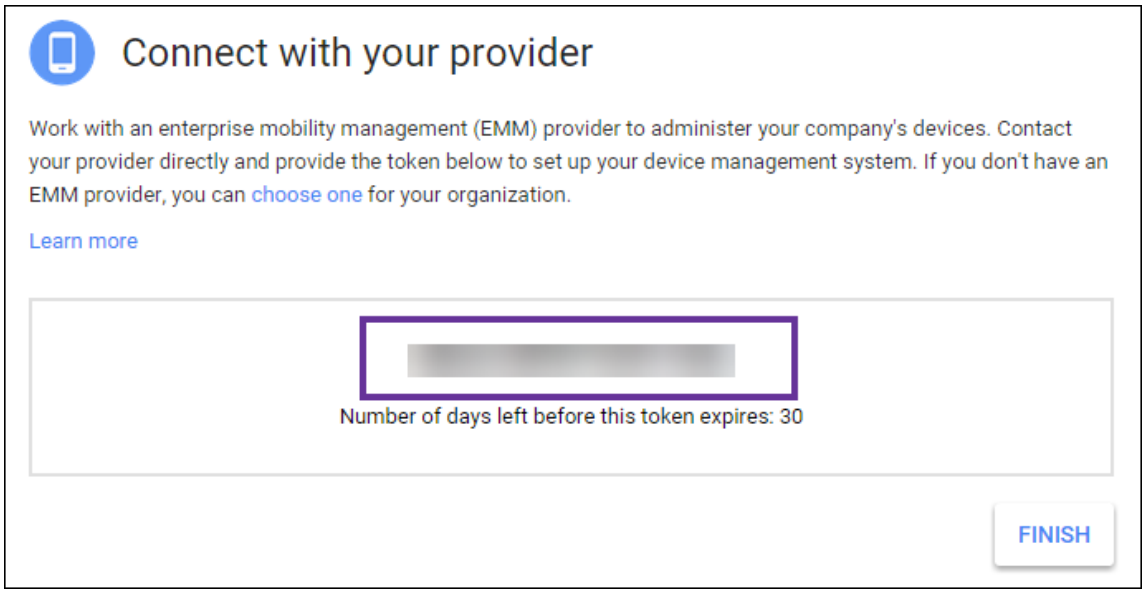
3. Google によってドメイン所有権が検証されます。



4. 検証が成功すると、次のページが開きます。［続行］ をクリックします。



5. シトリックスに提供し Android Enterprise 設定を構成するときに使用する EMM バインドトークンが、Google によって作成されます。トークンをコピーして保存します。後でセットアップ中に必要になります。



6. ［**Finish**］ をクリックして Android Enterprise の設定を完了します。ドメインの検証に成功したことを示すページが表示されます。

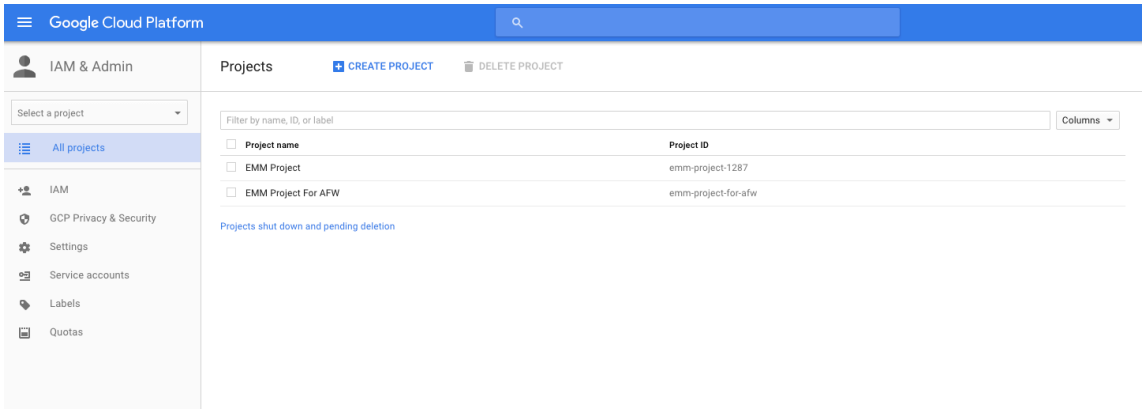
Android Enterprise サービスアカウントを作成したら、Google Admin コンソールにサインインしてモビリティ

管理設定を管理できます。

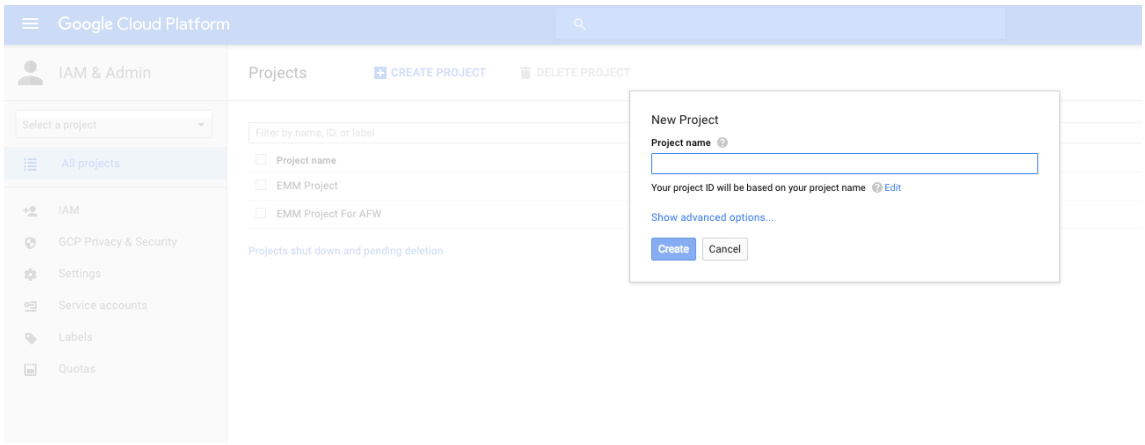
Android Enterprise サービスアカウントの設定と **Android Enterprise** 証明書のダウンロード

XenMobile から Google Play サービスおよび Directory サービスにアクセスできるようにするには、Google のデベロッパー用プロジェクトポータルを使用してサービスアカウントを作成する必要があります。このサービスアカウントは、XenMobile と Android at Work 用の Google の各種サービスのサーバー間通信で使用します。使用されている認証プロトコルについて詳しくは、https://developers.google.com/identity/protocols/OAuth2ServiceAccountを参照してください。

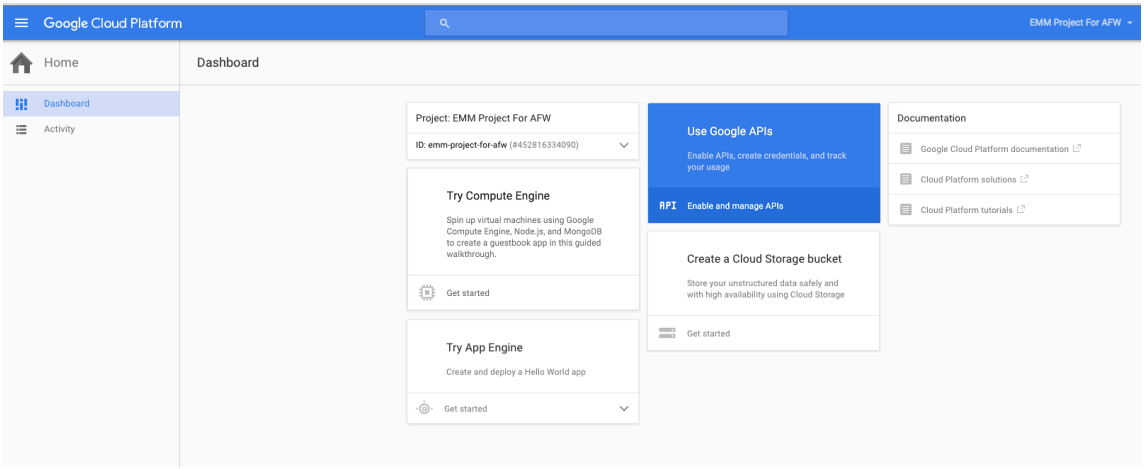
1. Web ブラウザーでhttps://console.cloud.google.com/projectを開いて、Google 管理者の資格情報でサインインします。
2. [**Projects**] の一覧で、 [**Create Project**] をクリックします。



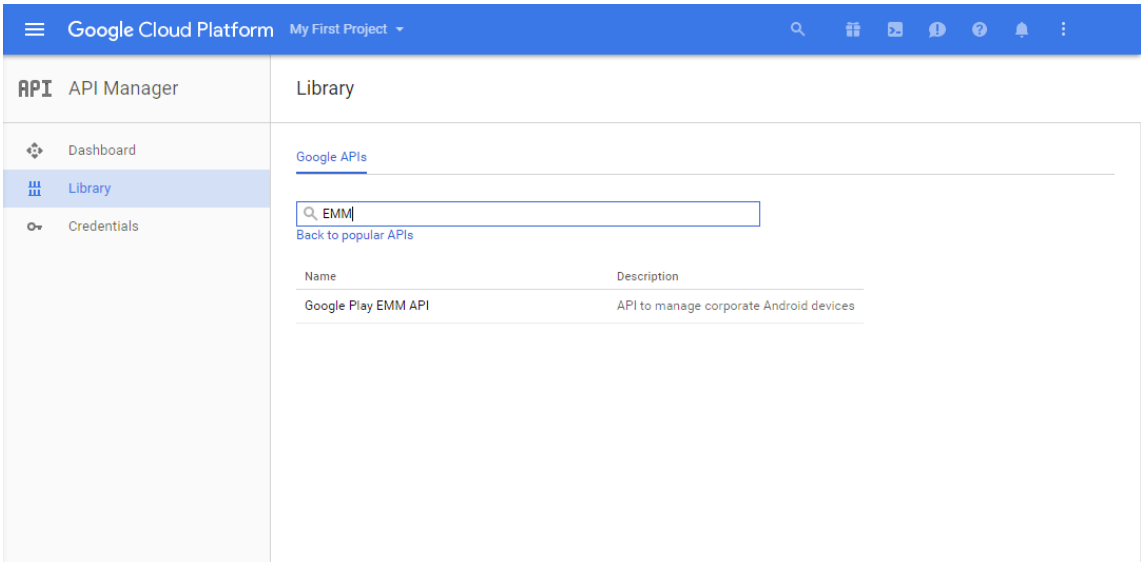
3. [**Project name**] ボックスに、プロジェクトの名前を入力します。



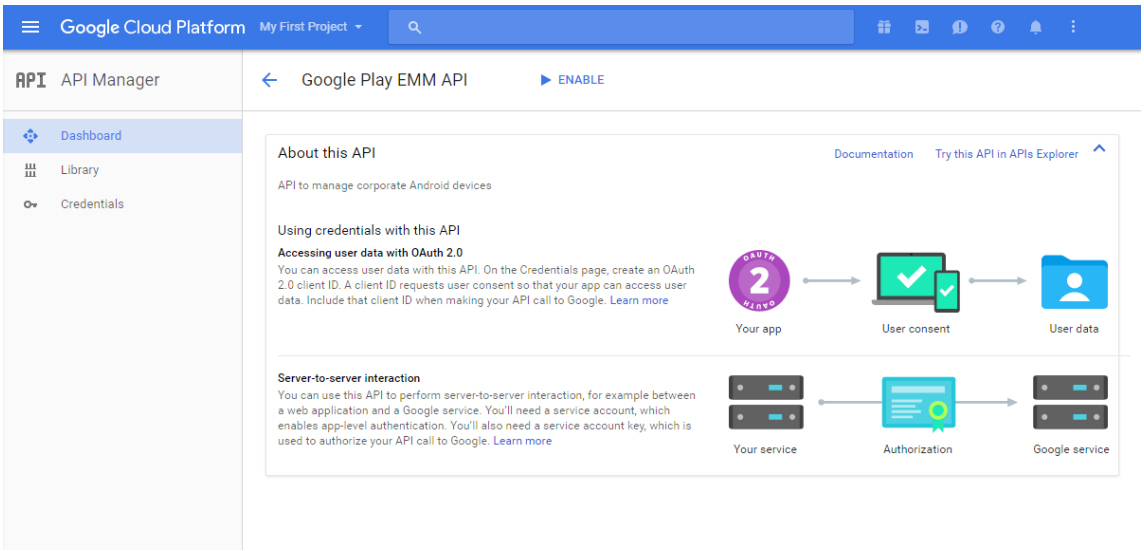
4. [Dashboard] ページで、 [**Use Google APIs**] をクリックします。



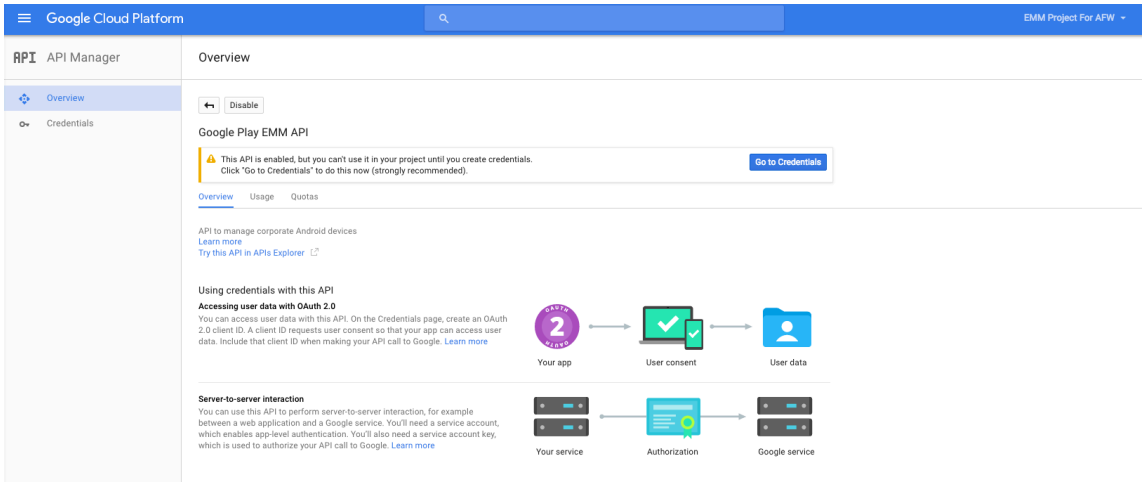
5. [**Library**] をクリックして、 [**Search**] に **EMM** と入力して、検索結果をクリックします。



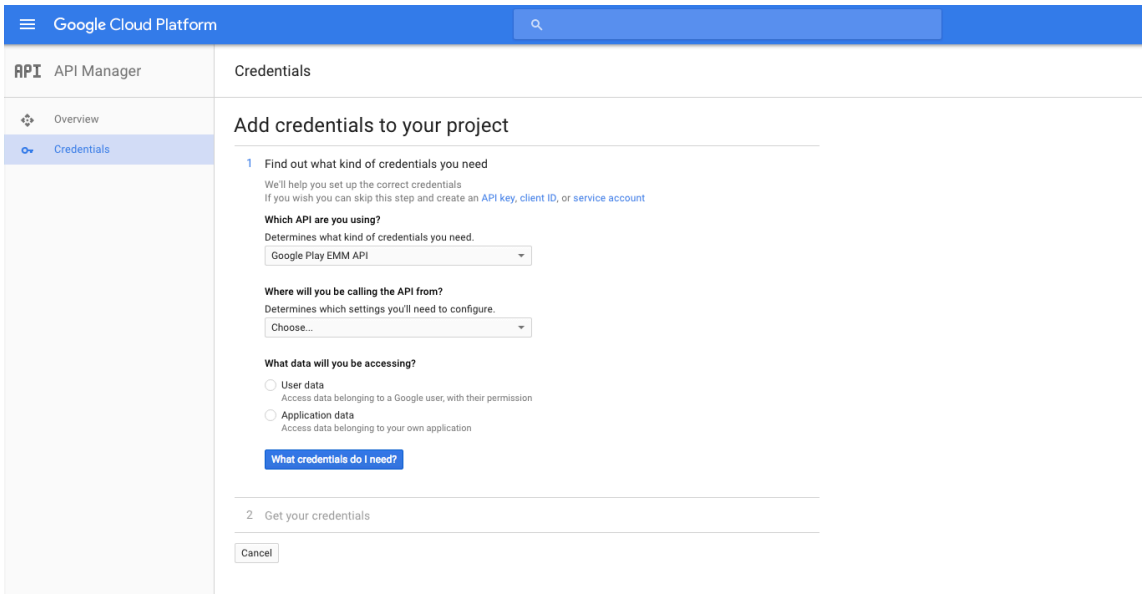
6. [**Overview**] ページで、 [**Enable**] をクリックします。



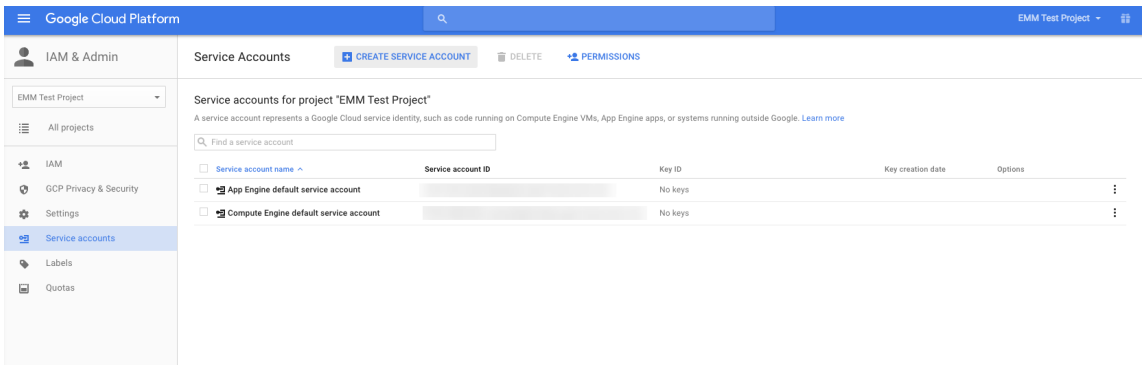
7. ［**Google Play EMM API**］ の横にある ［**Go to Credentials**］ をクリックします。



8. ［**Add credentials to our project**］ の一覧の手順 1 で、 ［**service account**］ をクリックします。

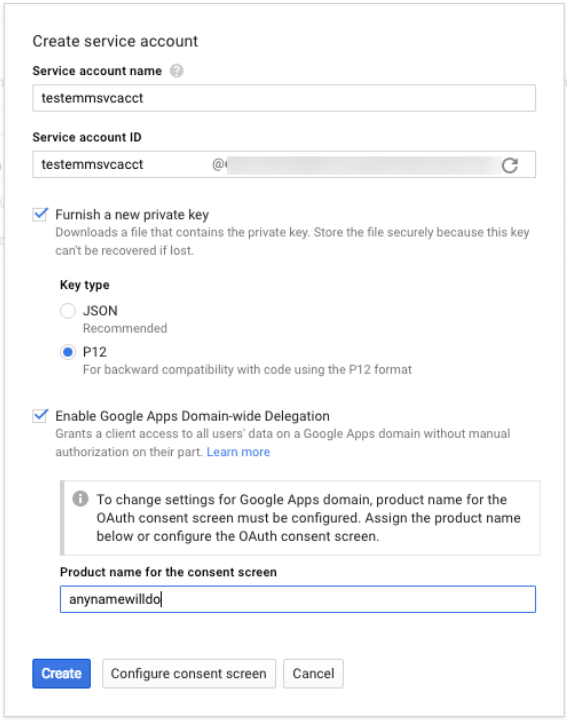


9. ［**Service Accounts**］ページで、 ［**Create Service Account**］ をクリックします。



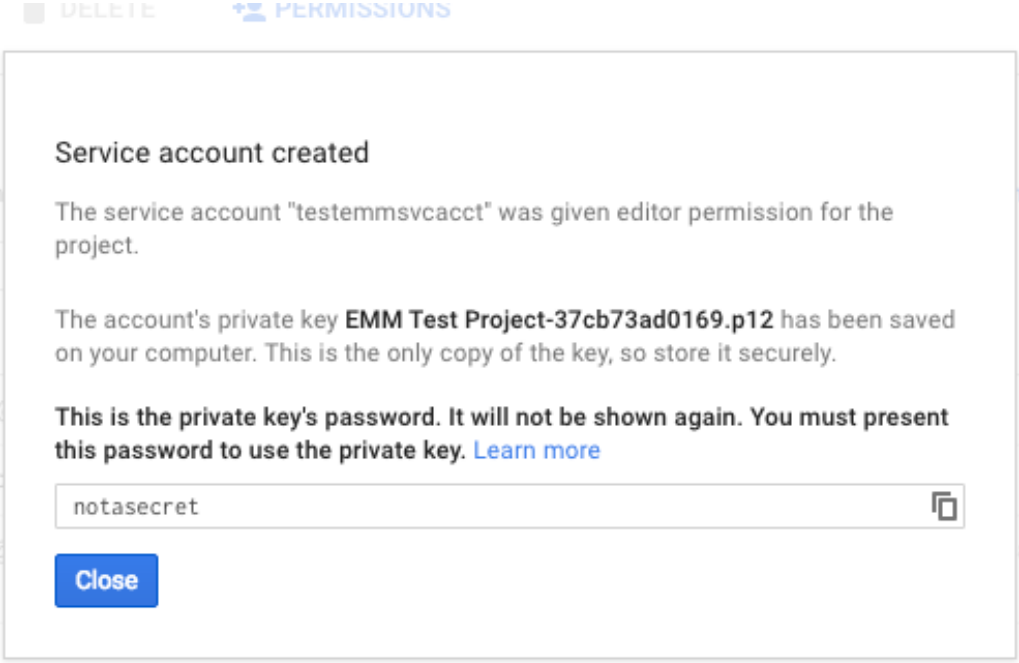
10. ［**Create service account**］ で、アカウントに名前を付けて、［**Furnish a new private key**］ をオンにし

ます。［**P12**］を選択して、［**Enable Google Apps Domain-wide Delegation**］をオンにし、［**Create**］をクリックします。

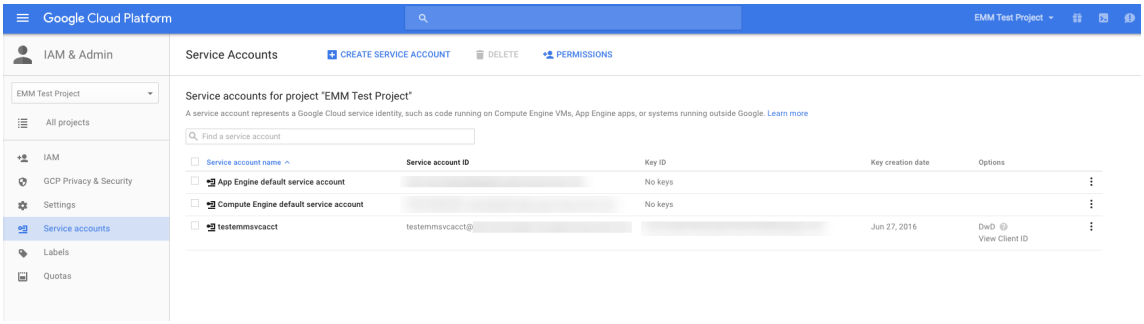


証明書（P12 ファイル）がコンピューターにダウンロードされます。証明書を安全な場所に保存してください。

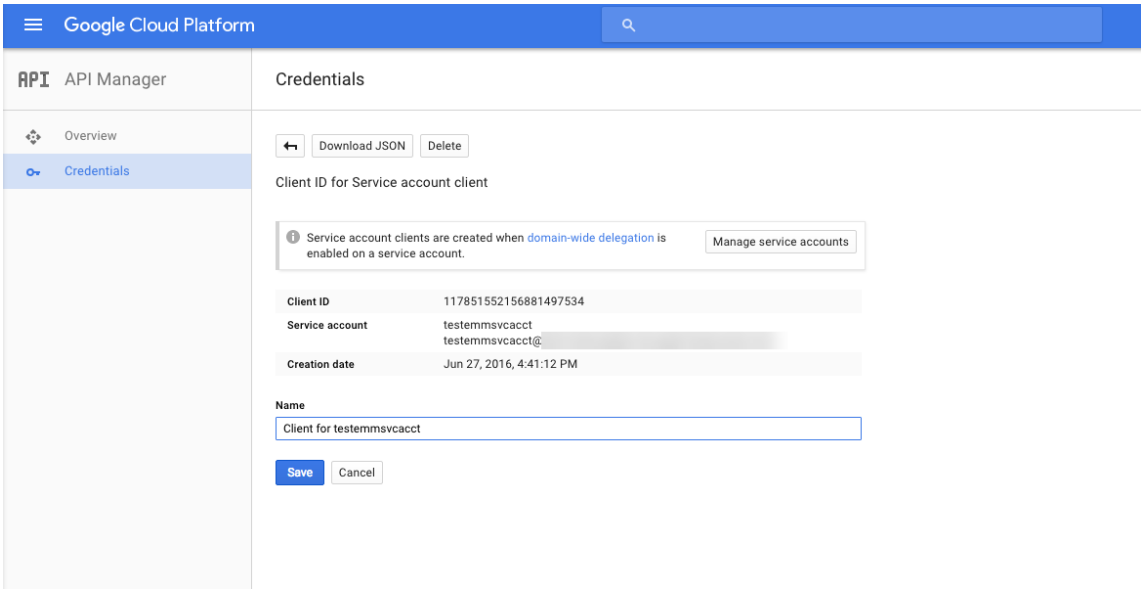
11. ［**Service account created**］ 確認画面で、 ［**Close**］ をクリックします。



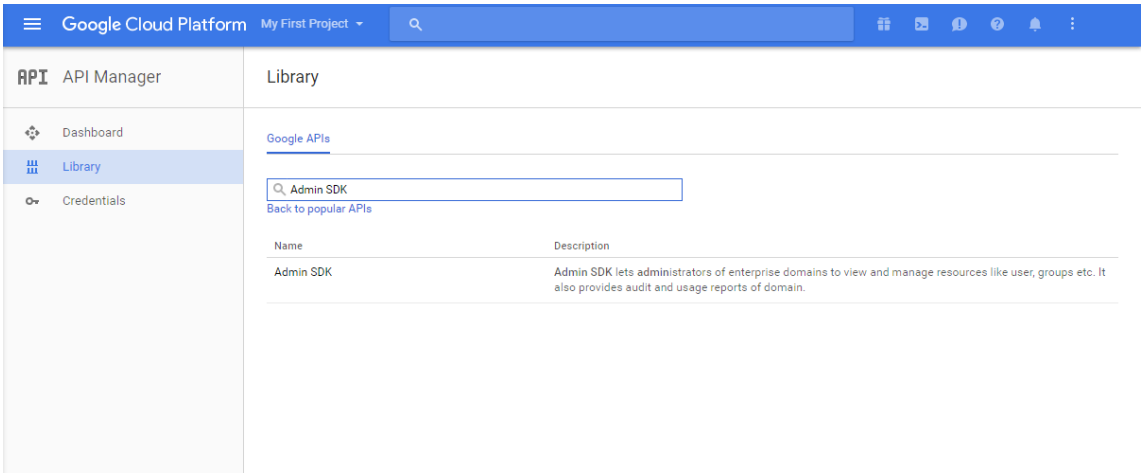
12. ［**Permissions**］ページで ［**Service accounts**］ をクリックし、サービスアカウントの ［**Options**］ の下で、 ［**View Client ID**］ をクリックします。



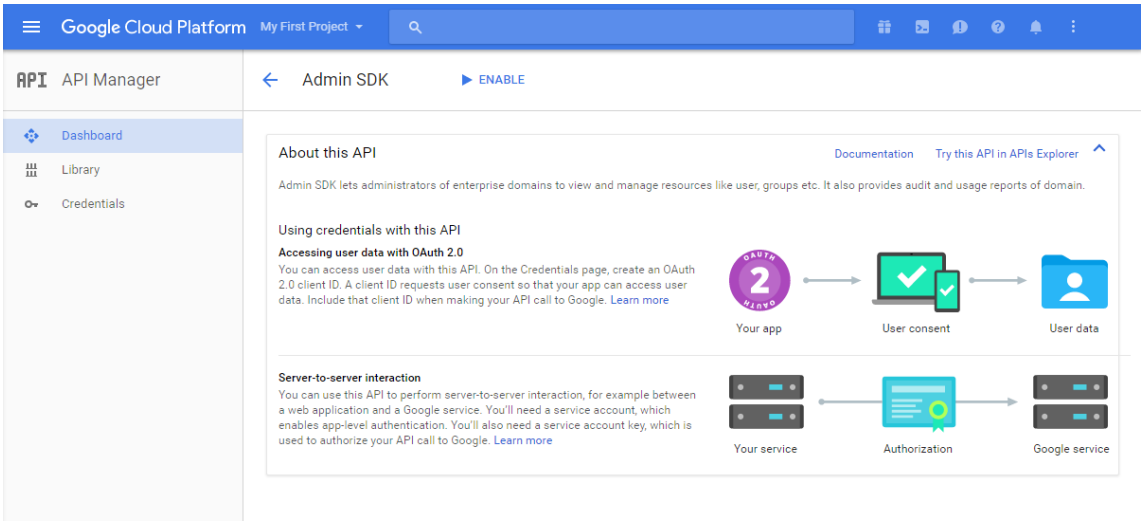
13. Google 管理コンソールでアカウントの承認に必要になる詳細情報が表示されます。［**Client ID**］と［**Service account ID**］を、後でこの情報を引き出せる場所にコピーします。この情報は、ドメイン名と共に、ホワイトリスト作成の目的でシトリックスサポートに送信するときに必要になります。



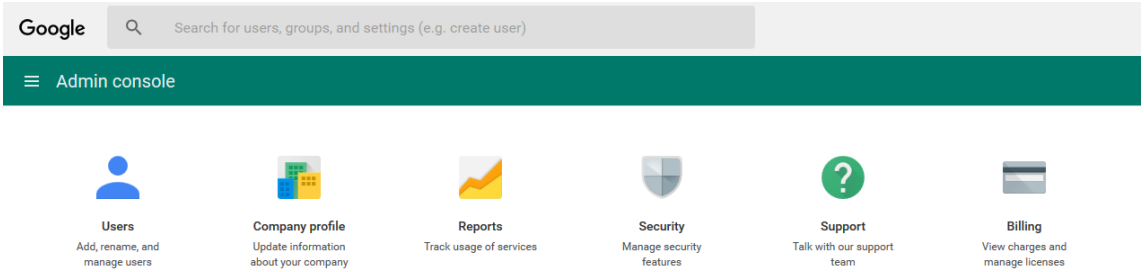
14. ［**Library**］ ページで **Admin SDK** を検索して、検索結果をクリックします。



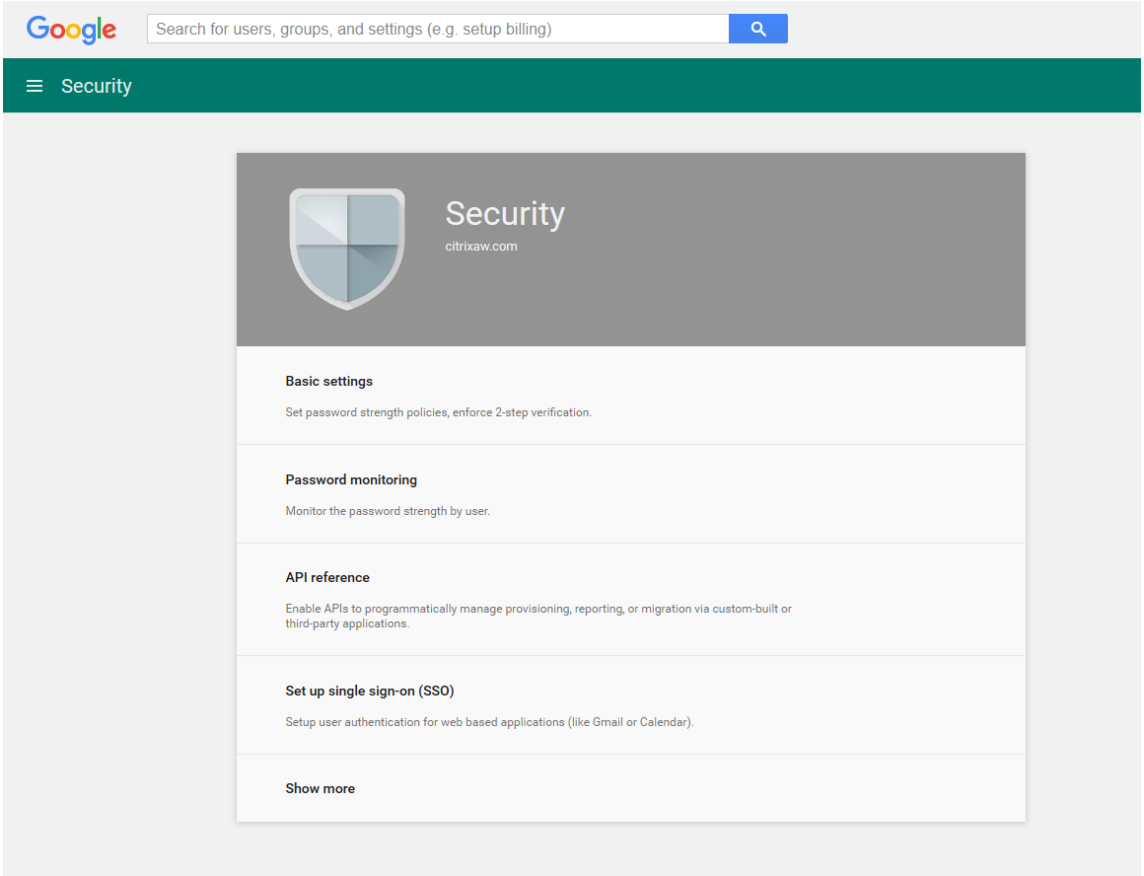
15. [**Overview**] ページで、 [**Enable**] をクリックします。

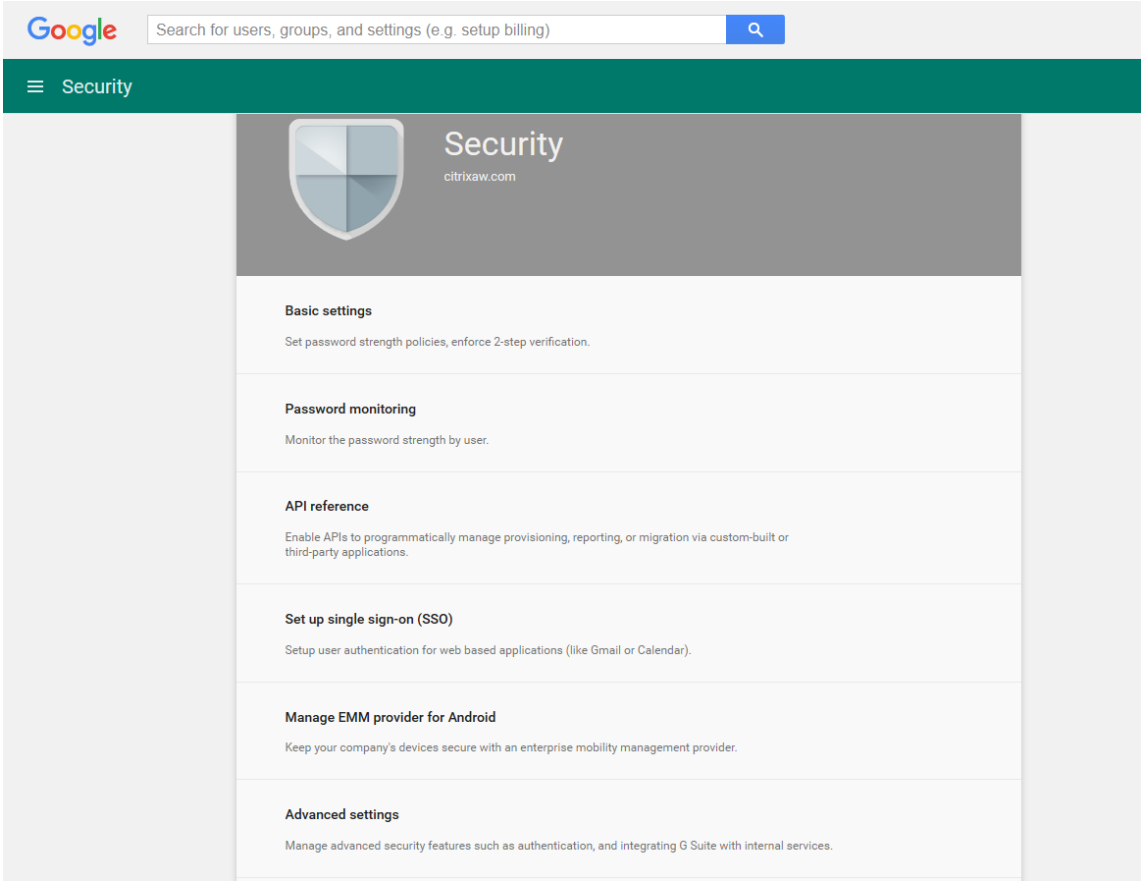


16. ユーザーのドメインの Google 管理コンソールを開き、 [**Security**] をクリックします。

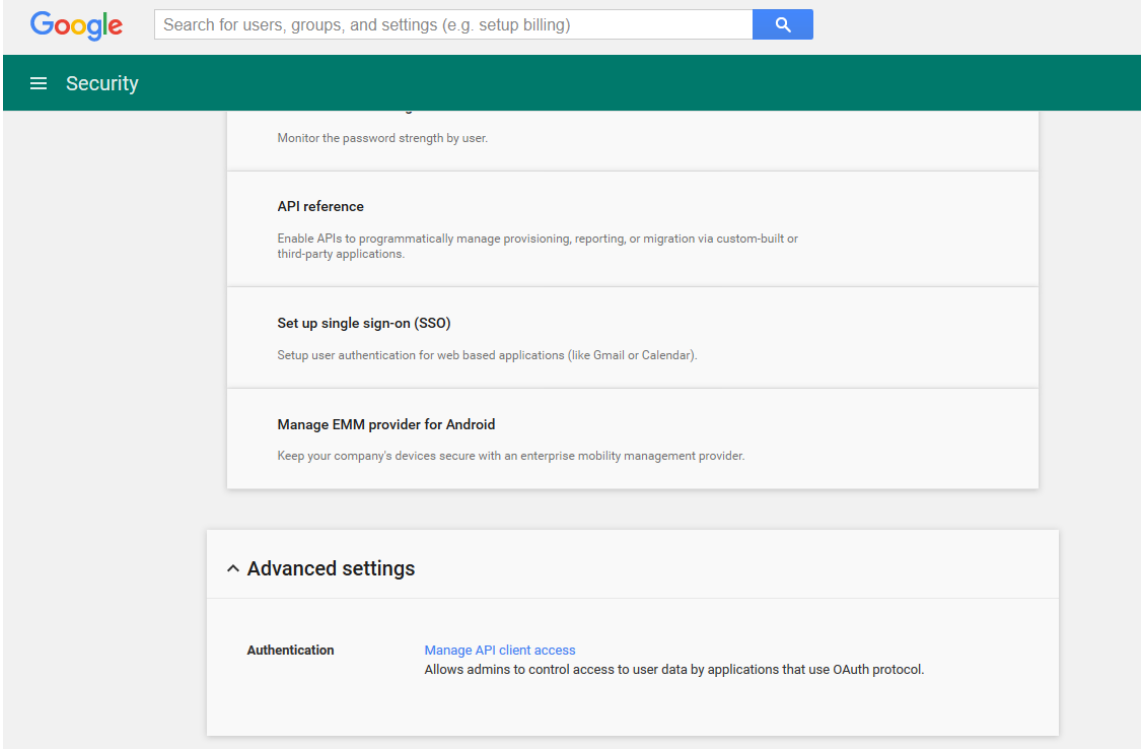


17. [**Settings**] ページで [**Show more**] をクリックして、 [**Advanced settings**] を選択します。

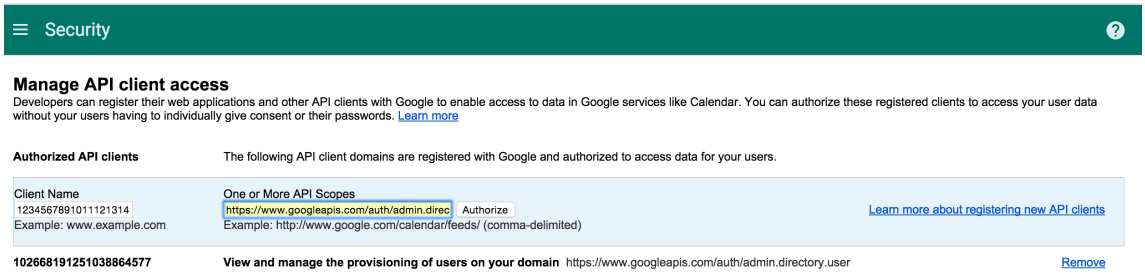




18. [**Manage API client access**] をクリックします。



19. ［**Client Name**］ ボックスに前の手順で保存したクライアント ID を入力し、 ［**One or More API Scopes**］ ボックスに「https://www.googleapis.com/auth/admin.directory.user」と入力して、［**Authorize**］ をクリックします。



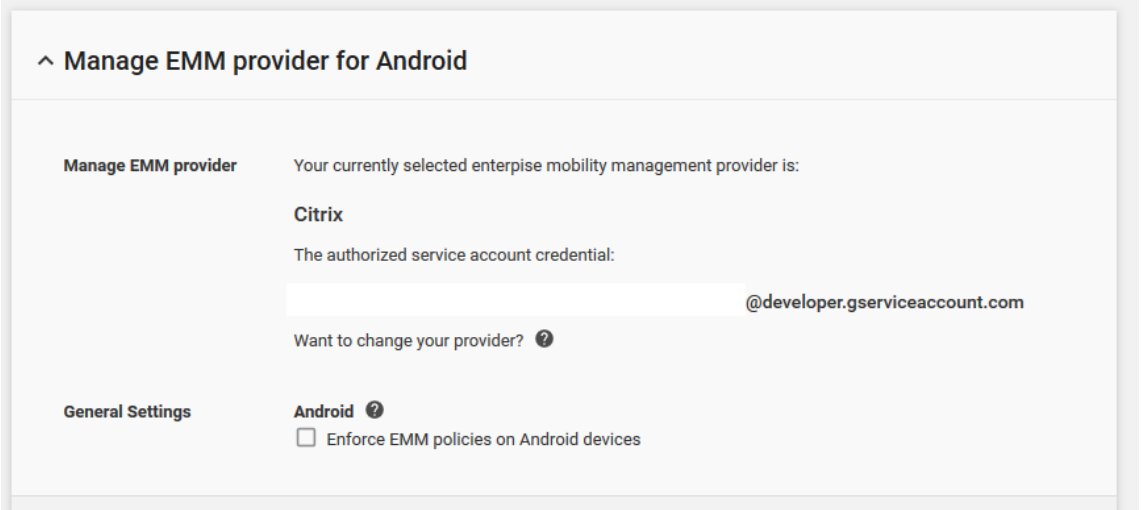
EMM へのバインド

XenMobile を使用して Android デバイスを管理するには、Citrix テクニカルサポートにドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。Citrix はトークンを EMM（エンタープライズモビリティ管理）プロバイダーとしての XenMobile にバインドします。シトリックステクニカルサポートへのお問い合わせは、シトリックステクニカルサポートを参照してください。

1. バインドを確認するには、Google Admin ポータルにサインインして ［**Security**］ をクリックします。
2. ［**Manage EMM provider for Android**］ をクリックします。

   Google Android Enterprise アカウントが EMM プロバイダーであるシトリックスにバインドされていることが表示されます。

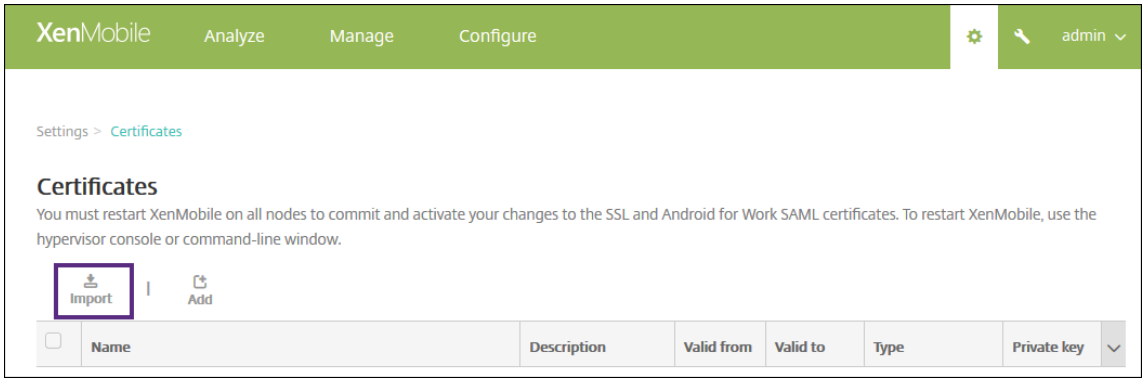
   トークンのバインドを確認した後で、XenMobile コンソールを使用して Android デバイスの管理を開始できます。手順 14 で生成した P12 証明書をインポートします。Android Enterprise サーバー設定をセットアップし、SAML ベースのシングルサインオン（Single Sign-On：SSO）を有効化し、少なくとも Android Enterprise デバイスポリシーを 1 つ定義する必要があります。



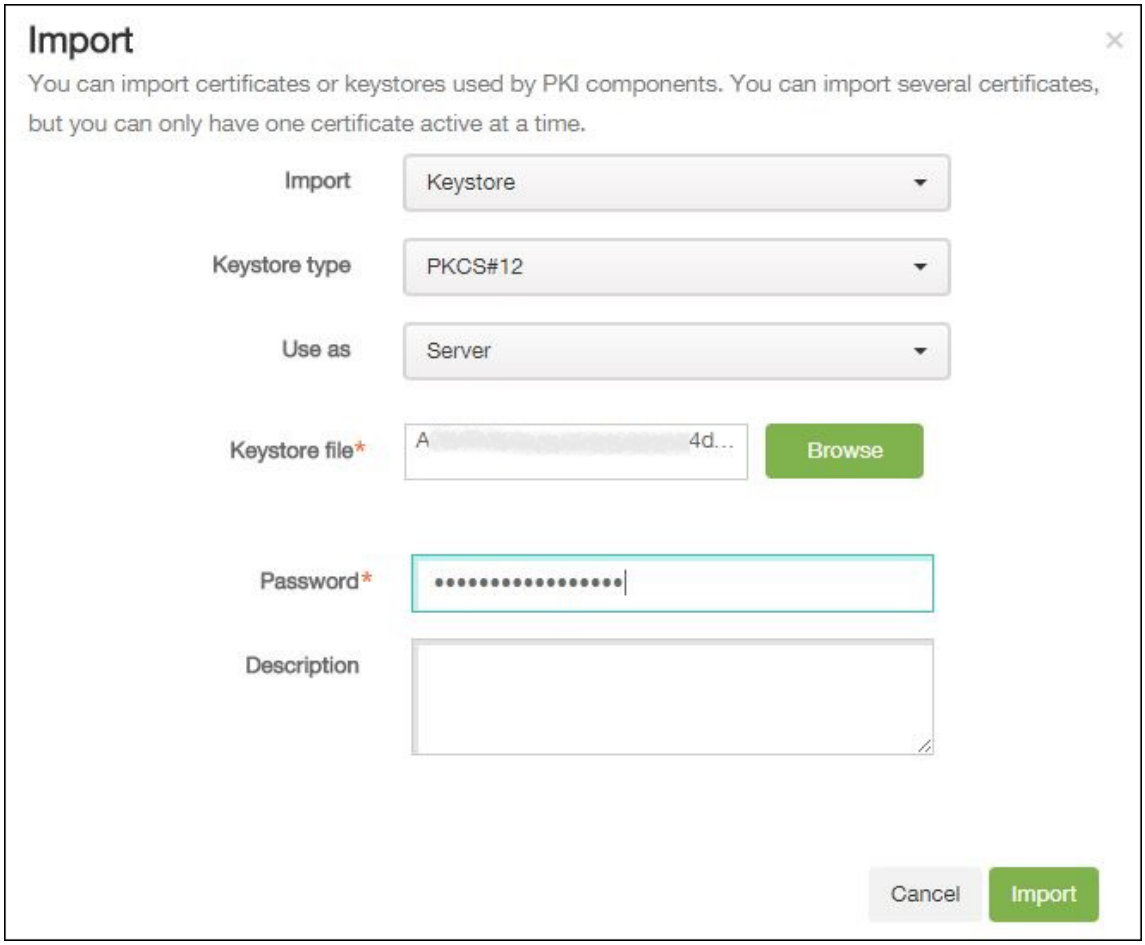
P12 証明書のインポート

以下の手順に従って Android Enterprise の P12 証明書をインポートします:

1. XenMobile コンソールにサインインします。
2. コンソールの右上にある歯車アイコンをクリックして ［設定］ ページを開き、［証明書］ をクリックします。［証明書］ ページが開きます。



3. ［インポート］ をクリックします。［インポート］ ダイアログボックスが開きます。



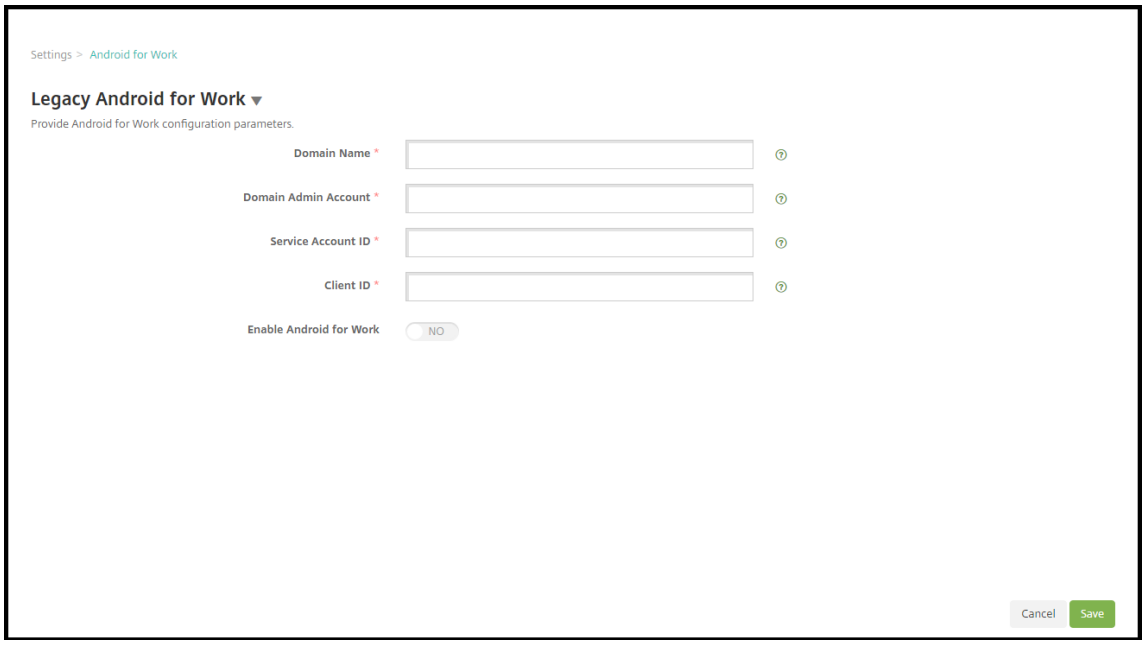
次の設定を構成します:

- インポート: ボックスの一覧から、［キーストア］ を選択します。
- キーストアの種類: ボックスの一覧から、［**PKCS#12**］ を選択します。
- 使用目的: ボックスの一覧から、［サーバー］ を選択します。
- キーストアファイル: ［ブラウザー］ をクリックして、P12 証明書を選択します。
- パスワード: キーストアのパスワードを入力します。
- 説明: 任意で、証明書の説明を入力します。

4. ［インポート］ をクリックします。

Android Enterprise サーバー設定のセットアップ

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**Android Enterprise**］ をクリックします。［**Android Enterprise**］ ページが開きます。



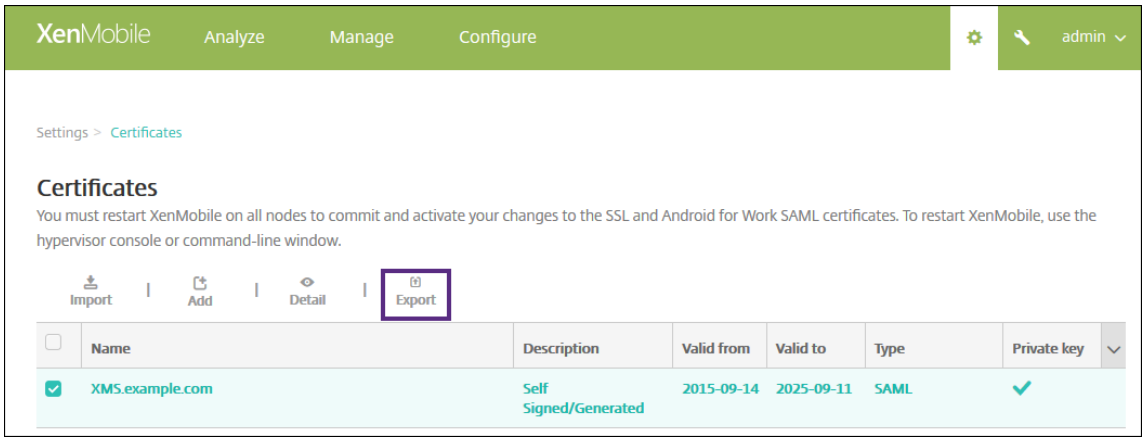
これらの設定を構成し、［保存］ をクリックします。

- ドメイン名: Android Enterprise のドメイン名を入力します（例: domain.com）。
- ドメイン管理アカウント: ドメイン管理者のユーザー名を入力します（例: Google Developer Portal で使用しているメールアカウント）。
- サービスアカウント **ID**: サービスアカウント ID を入力します（例: Google Service Account（serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com）に関連付けられたメールアドレス）。
- クライアント **ID**: Google サービスアカウントの数値形式のクライアント ID を入力します。

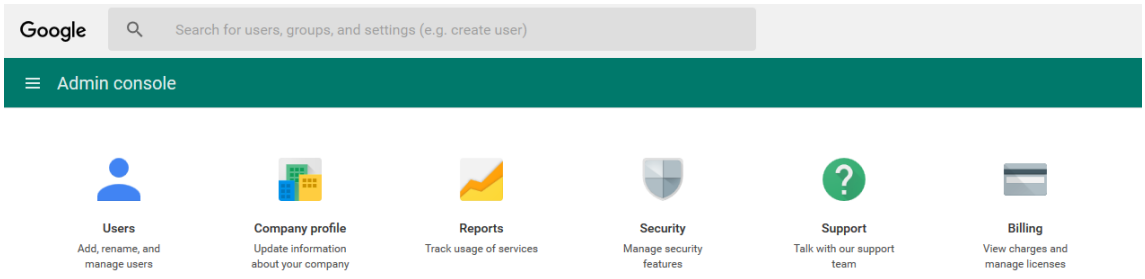
- **Android Enterprise** の有効化： Android Enterprise を有効にするのか、無効にするのかを選択します。

SAML ベースのシングルサインオンの有効化

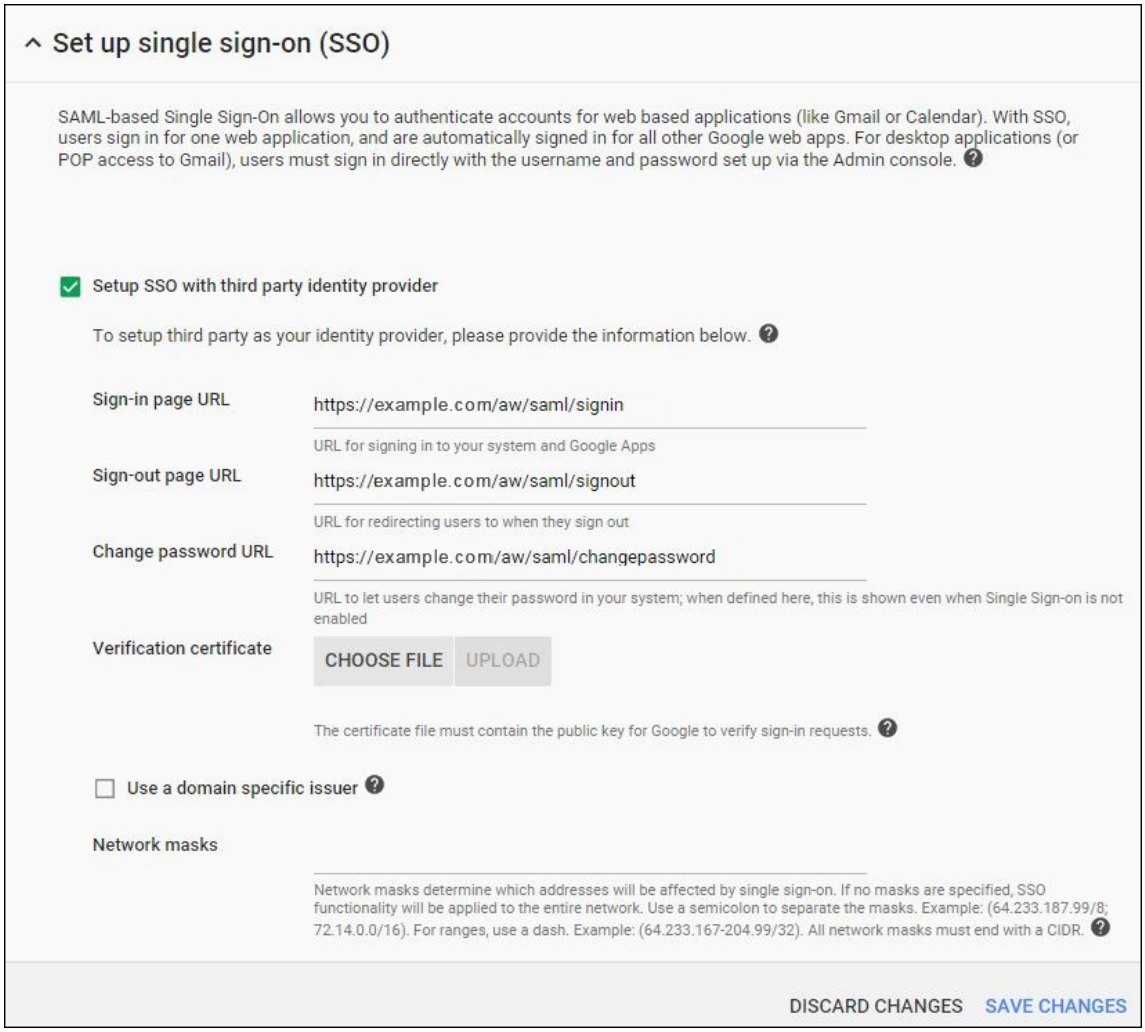
1. XenMobile コンソールにサインインします。
2. コンソールの右上にある歯車アイコンをクリックします。［設定］ ページが開きます。
3. ［証明書］ をクリックします。［証明書］ ページが開きます。



4. 証明書の一覧から、SAML 証明書を選択します。
5. ［エクスポート］ をクリックして証明書をコンピューターに保存します。
6. Android Enterprise の管理者資格情報で Google Admin ポータルにサインインします。ポータルへのアクセスについて詳しくは、Google Admin portalを参照してください。
7. ［**Security**］ をクリックします。



8. ［**Security**］ の下の ［**Set up single sign-on**（**SSO**）］ をクリックして以下の設定を構成します。

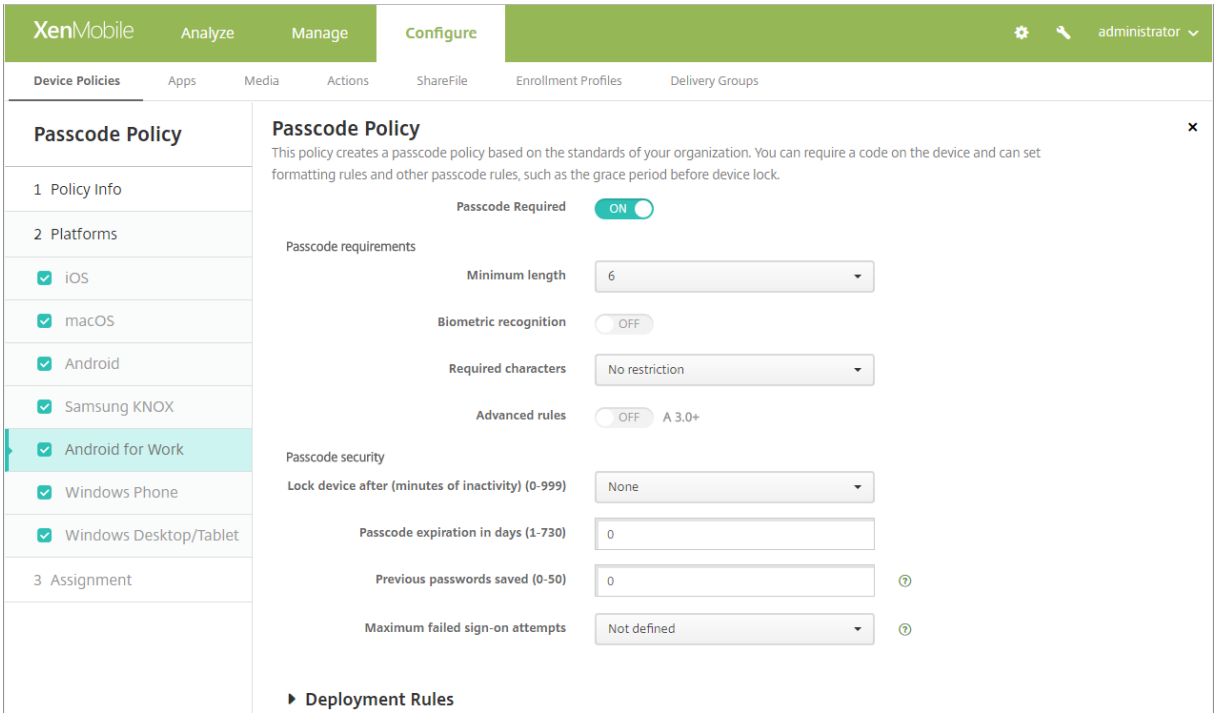


- **Sign-in page URL**： お使いのシステムおよび Google Apps にサインインするページの URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/signin`。
- **Sign-out page URL**： ユーザーがサインアウト時にリダイレクトされる URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/signout`。
- **Change password URL**： ユーザーがシステム内でパスワードを変更するときにアクセスする URL を入力します。例：`https://<Xenmobile-FQDN>/aw/saml/changepassword`。このフィールドが定義されると、SSO が使用できない場合でもこのメッセージが表示されます。
- **Verification certificate**： ［**CHOOSE FILE**］ をクリックして、XenMobile からエクスポートされた SAML 証明書を選択します。

9. ［**SAVE CHANGES**］ をクリックします。

Android Enterprise デバイスポリシーのセットアップ

パスコードポリシーをセットアップして、ユーザーが初めて登録するときにデバイスでのパスコード設定を必須にします。



デバイスポリシーの基本的なセットアップ手順は以下のとおりです。

1. XenMobile コンソールにサインオンします。
2. [構成] > [デバイスポリシー] をクリックします。
3. [追加] をクリックして、[新しいポリシーの追加] ダイアログボックスから追加するポリシーを選択します。この例では [パスコード] をクリックします。
4. [ポリシー情報] ページに入力します。
5. [**Android Enterprise**] をクリックしてポリシーの設定を構成します。
6. ポリシーをデリバリーグループに割り当てます。

サポートされているデバイスポリシーと **MDX** ポリシー

次の表に、Android Enterprise コンテナでサポートされているデバイスポリシーと MDX ポリシーを示します。デバイスポリシーと MDX ポリシーについて詳しくは、「デバイスポリシー」および「MDX ポリシーの概要」をそれぞれ参照してください。

認証ポリシー	サポート対象	サポートされている値	注
アプリのパスコード	☒	すべて	
オンラインセッションを必須とする		[オフ] のみ	

認証ポリシー	サポート対象	サポートされている値	注
最大オフライン期間	☒	すべて	
代替 NetScaler Gateway		空白のみ	

アプリのネットワークアクセスポリシー	サポート対象	サポートされている値	注
ネットワークアクセス	☒	すべて	
証明書ラベル		空白のみ	
優先 VPN モード	☒	すべて	
VPN モードの切り替えを許可	☒	すべて	
PAC ファイルの URL、またはプロキシサーバー	☒	すべて	
デフォルトのログ出力	☒	すべて	
デフォルトのログレベル	☒	すべて	
最大ログファイル数	☒	すべて	
最大ログファイルサイズ	☒	すべて	
アプリログのリダイレクト	☒	すべて	
ログの暗号化	☒	すべて	
WiFi ネットワークのホワイトリストへの追加		空白のみ	

デバイスセキュリティポリシー	サポート対象	サポートされている値	注
ジェイルブレイクまたは Root 化を禁止	☒	すべて	
デバイスの暗号化を要求	☒	すべて	
デバイスのロックを必須とする	☒	すべて	

ネットワーク要件ポリシー	サポート対象	サポートされている値	注
Wi-Fi を必須とする	☒	無効	

その他のアクセスポリシー	サポート対象	サポートされている値	注
アプリ更新猶予期間（時間）	☒	すべて	
ロック時にアプリデータを消去	☒	すべて	
アクティブなポーリング周期 (分)	☒	すべて	

暗号化ポリシー	サポート対象	サポートされている値	注
暗号キー	☒	オフラインアクセスを許可	Android エンタープライズポリシーでサポート
プライベートファイルの暗号化	☒	［無効］のみ	Android エンタープライズポリシーでサポート
プライベートファイルの暗号化から除外する対象	☒	該当なし（空）	Android エンタープライズポリシーでサポート
パブリックファイルへのアクセス制限	☒	該当なし（空）	Android エンタープライズポリシーでサポート
パブリックファイルの暗号化	☒	［無効］のみ	Android エンタープライズポリシーでサポート
パブリックファイルの暗号化から除外する対象	☒	該当なし（空）	Android エンタープライズポリシーでサポート
パブリックファイルの移行	☒	［無効］のみ	Android エンタープライズポリシーでサポート

アプリ相互作用ポリシー	サポート対象	サポートされている値	注
セキュリティグループ	☒	空	Android エンタープライズポリシーでサポート

アプリ相互作用ポリシー	サポート対象	サポートされている値	注
切り取りおよびコピー	☒	[制限なし] のみ	Android エンタープライズポリシーでサポート
貼り付け	☒	[制限なし] のみ	Android エンタープライズポリシーでサポート
ドキュメント交換（このアプリケーションで開く）	☒	[制限なし] のみ	Android エンタープライズポリシーでサポート
受信ドキュメント交換 (このアプリケーションで開く)	☒	すべて	Android エンタープライズポリシーでサポート
受信ドキュメント交換のホワイトリスト	☒	空	Android エンタープライズポリシーでサポート
Restricted Open-In exception list	☒	空	Android エンタープライズポリシーでサポート

アプリ制限ポリシー	サポート対象	サポートされている値	注
カメラを禁止	☒	[オン] のみ	Android エンタープライズポリシーでサポート
ギャラリーを禁止	☒	[オン] のみ	Android エンタープライズポリシーでサポート
localhost 接続をブロック	☒	すべて	
マイク録音を禁止	☒	[オフ] のみ	Android エンタープライズポリシーでサポート
位置情報サービスを禁止	☒	[オフ] のみ	Android エンタープライズポリシーでサポート
SMS 作成を禁止	☒	[オフ] のみ	Android エンタープライズポリシーでサポート
スクリーンショットを禁止	☒	[オフ] のみ	Android エンタープライズポリシーでサポート
デバイスのセンサーを禁止	☒	すべて	

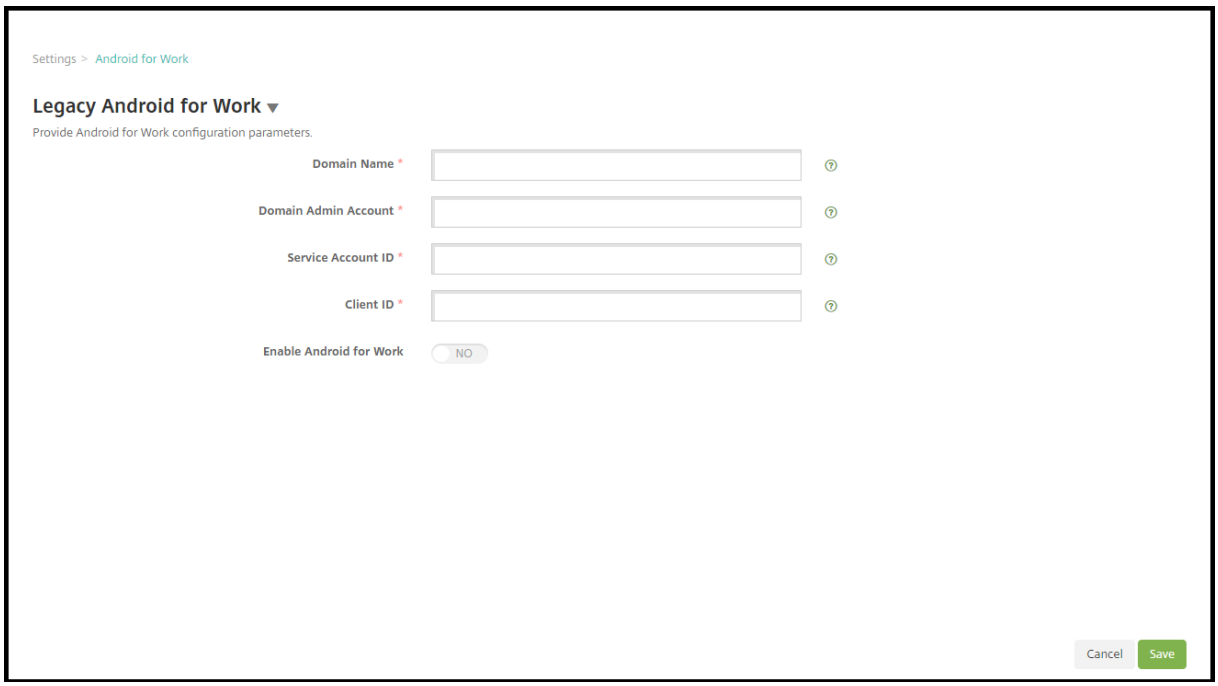
アプリ制限ポリシー	サポート対象	サポートされている値	注
NFC を禁止	☒	［オフ］のみ	Android エンタープライズポリシーでサポート
印刷を禁止	☒	すべて	
アプリログを禁止	☒	すべて	

アプリのジオフェンスポリシー	サポート対象	サポートされている値	注
中心点の経度	☒	すべて	
中心点の緯度	☒	すべて	
半径	☒	すべて	

Android Enterprise アカウント設定の構成

ユーザーのデバイスで Android のアプリとポリシーを管理できるようにするには、XenMobile で Android Enterprise のドメインおよびアカウント情報を設定する必要があります。まず、Google で Android Enterprise の設定タスクを完了してドメイン管理者を設定し、サービスアカウント ID とバインドトークンを取得する必要があります。

1. XenMobile Web コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**Android Enterprise**］ をクリックします。［**Android Enterprise**］ 構成ページが開きます。



1. [**Android Enterprise**] ページで以下の設定を構成します:
   - ドメイン名: ドメイン名を入力します。
   - ドメイン管理アカウント: ドメイン管理者のユーザー名を入力します。
   - サービスアカウント **ID**: Google のサービスアカウント ID を入力します。
   - クライアント **ID**: Google サービスアカウントのクライアント ID を入力します。
   - **Android Enterprise** の有効化: Android Enterprise を有効にするかどうかを選択します。
2. [保存] をクリックします。

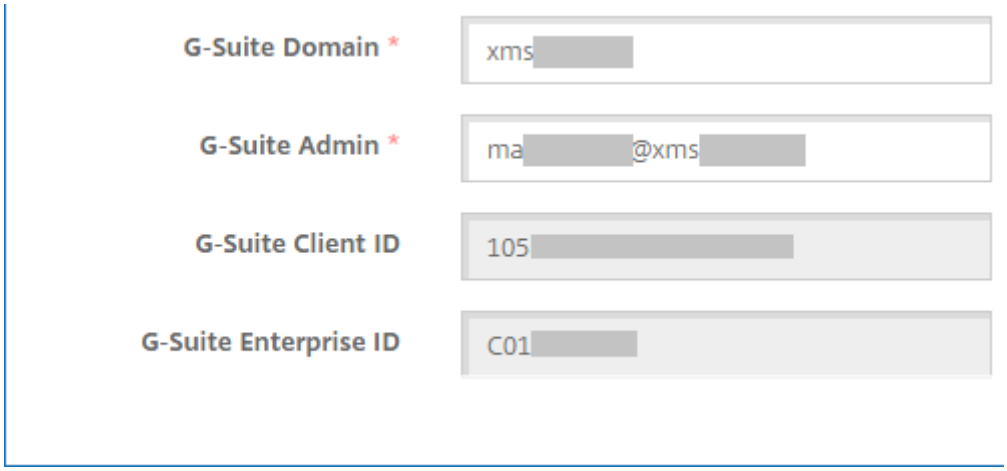
XenMobile の **G Suite** パートナーアクセスをセットアップ

Chrome の一部のエンドポイント管理機能では、Google パートナー API を使用して XenMobile と G Suite ドメイン間で通信します。たとえば、XenMobile では、シークレットモードやゲストモードなどの Chrome 機能を管理するデバイスポリシーに API が必要です。

パートナー API を有効にするには、XenMobile コンソールで G Suite ドメインをセットアップしてから、G Suite アカウントを構成します。

XenMobile で **G Suite** ドメインをセットアップする

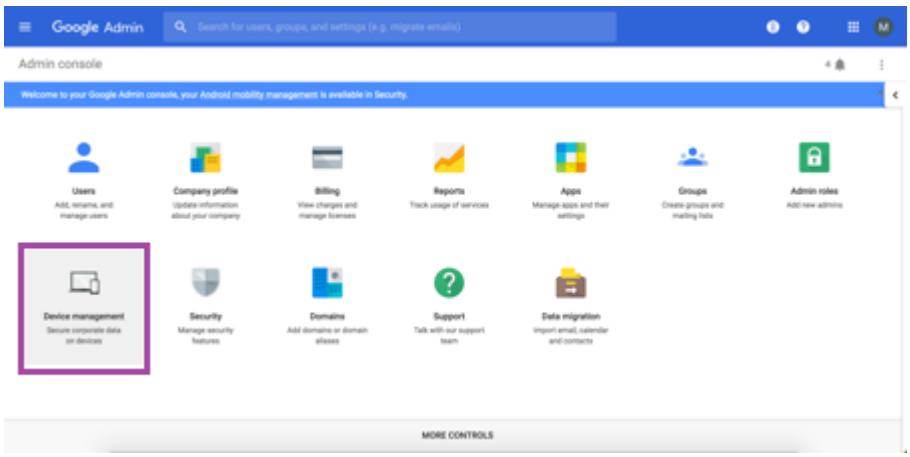
XenMobile で G Suite ドメインの API と通信できるようにするには、[設定] **>** [**Google Chrome** の構成] で設定を構成します。



- **G Suite** ドメイン： XenMobile に必要な API をホストする G Suite ドメイン。
- **G Suite** 管理者アカウント： G Suite ドメインの管理者アカウント。
- **G Suite** クライアント **ID**： シトリックスのクライアント ID。G Suite ドメインのパートナーアクセスを構成する場合は、この値を使用します。
- **G Suite** エンタープライズ **ID**： アカウントのエンタープライズ ID。お客様の Google エンタープライズアカウントから入力されます。

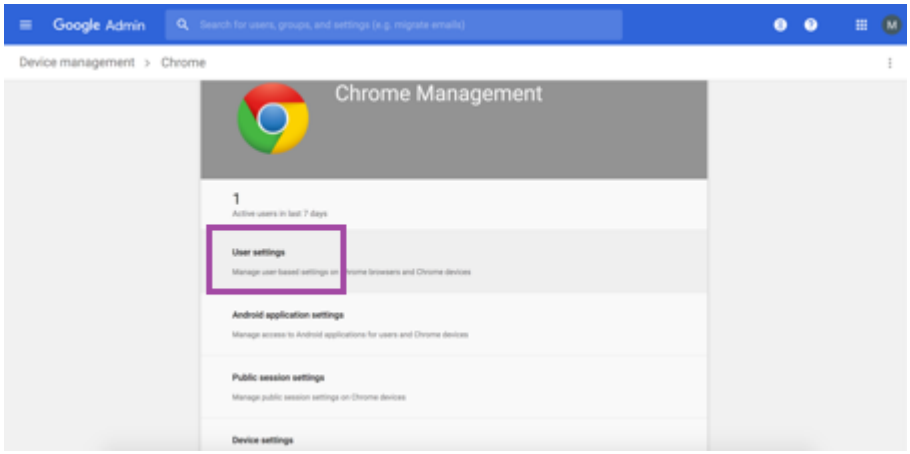
G Suite ドメイン内のデバイスとユーザーのパートナーアクセスを有効にする

1. Google 管理コンソールにログインします。https://admin.google.com
2. [端末管理] をクリックします。



3. [**Chrome** 管理] をクリックします。

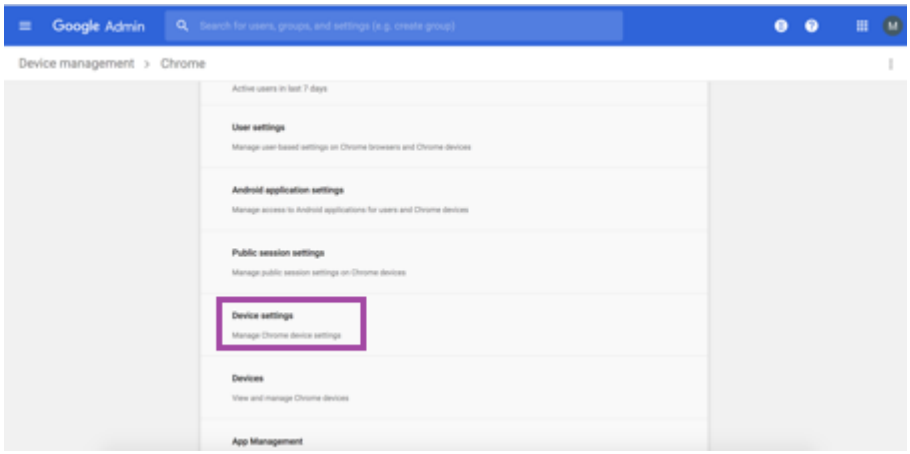
4. [ユーザー設定] をクリックします。



5. [**Chrome** 管理-パートナーアクセス] を見つけます。

6. [**Chrome** 管理-パートナーアクセスを有効にします] チェックボックスをオンにします。
7. パートナーアクセスについて了承し、有効にする必要があることに同意します。[保存] をクリックします。

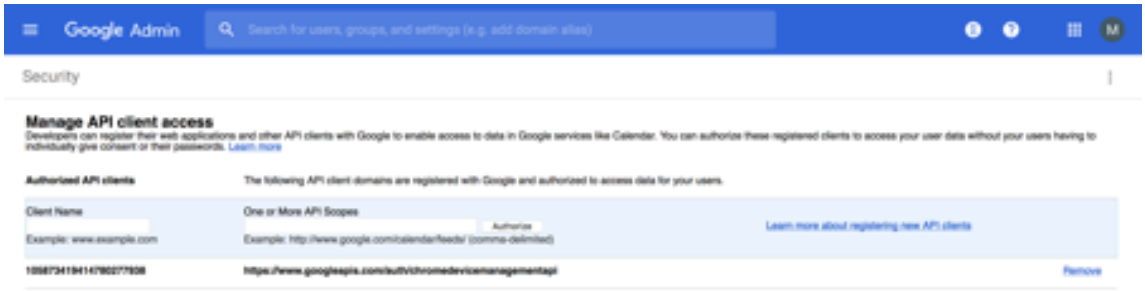
8. [Chrome 管理] ページで ［端末設定］ をクリックします。



9. [**Chrome** 管理-パートナーアクセス] を見つけます。

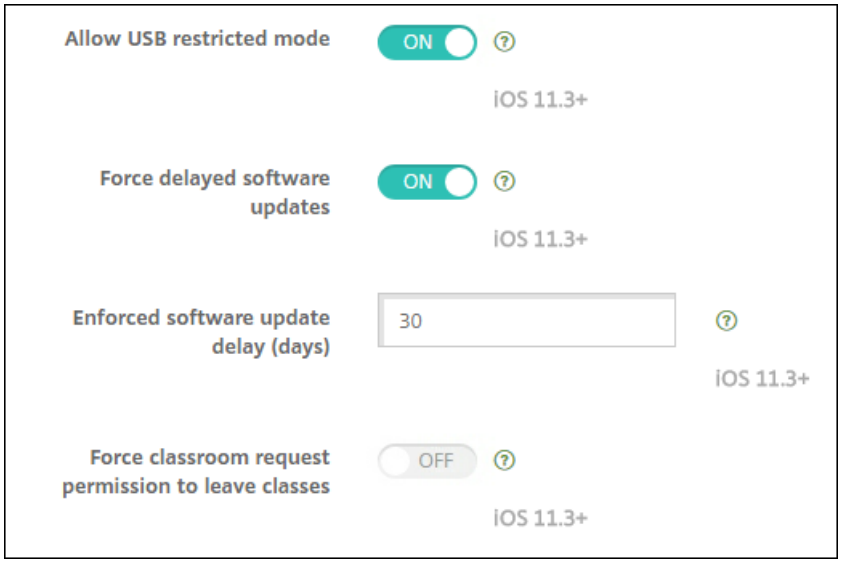
10. [**Chrome** 管理-パートナーアクセスを有効にします] チェックボックスをオンにします。
11. パートナーアクセスについて了承し、有効にする必要があることに同意します。［保存］ をクリックします。
12. ［セキュリティ］ ページに移動し、［詳細設定］ をクリックします。

13. [**API** クライアントアクセスを管理する] をクリックします。
14. XenMobile コンソールで、[設定] **>** [**Google Chrome** の構成] に移動し、[G Suite クライアント ID] の値をコピーします。次に、[**API** クライアントアクセスを管理する] ページに戻り、コピーした値を [クライアント名] フィールドに貼り付けます。
15. [**1** つ以上の **API** の範囲] に次の URL を追加します: **https://www.googleapis.com/auth/chromedevicemanagementapi**



16. [承認] をクリックします。

「設定が保存されました」というメッセージが表示されます。



Android Enterprise デバイスの登録

デバイス登録処理でユーザーがユーザー名またはユーザー ID を入力する必要がある場合、受け入れる形式は、XenMobile サーバーがユーザープリンシパル名（UPN）または SAM アカウント名でユーザーを検索するように構成されているかどうかによって異なります。

XenMobile サーバーが UPN でユーザーを検索するように構成されている場合、ユーザーは以下の形式で UPN を入力する必要があります:

- ユーザー名 @ ドメイン

XenMobile サーバーが SAM によってユーザーを検索するように構成されている場合、ユーザーは以下のどちらかの形式で SAM を入力する必要があります。

- ユーザー名 @ ドメイン
- ドメイン\ユーザー名

XenMobile サーバーが構成されているユーザー名の種類を確認するには:

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［**LDAP**］ をクリックして、LDAP 接続の設定を表示します。
3. ページの下部にある ［ユーザー検索基準］ フィールドを表示します。
    - **userPrincipalName** に設定すると、XenMobile サーバーは UPN に設定されます。
    - **sAMAccountName** に設定すると、XenMobile サーバーは SAM に設定されます。

Android Enterprise エンタープライズの登録解除

XenMobile Server コンソールと XenMobile Tools を使用して、Android Enterprise エンタープライズを登録解除できます。

このタスクを実行すると、XenMobile Server によって XenMobileTools のポップアップウィンドウが開かれます。始める前に、XenMobile Server に、使用している Web ブラウザーでポップアップウィンドウを開く権限があることを確認してください。Google Chrome などの一部のブラウザーでは、ポップアップブロックを無効にし、XenMobile サイトのアドレスをポップアップブロックのホワイトリストに追加する必要があります。

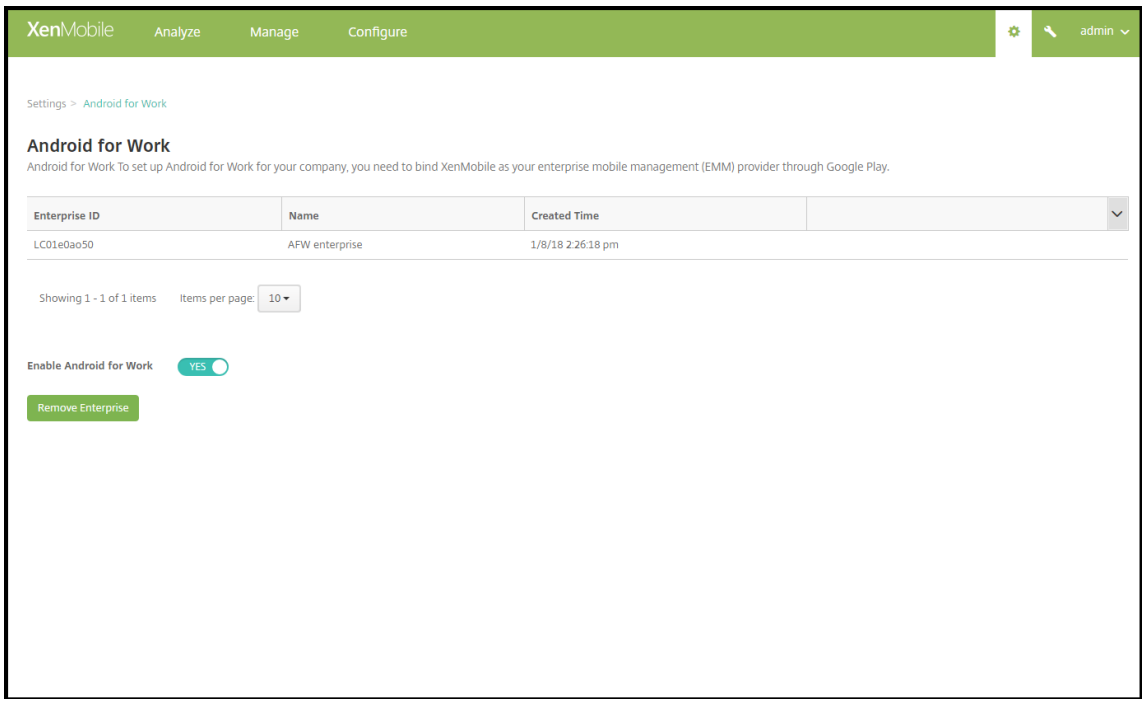
> 警告:
>
> エンタープライズの登録を解除すると、エンタープライズ経由で登録されていたデバイスの Android Enterprise アプリはデフォルトの状態にリセットされます。デバイスは Google によって管理されなくなります。それらのデバイスを Android Enterprise エンタープライズで再登録しても、以前の機能を復元することはできません。追加で構成を行う必要があります。

Android Enterprise エンタープライズの登録を解除した後:

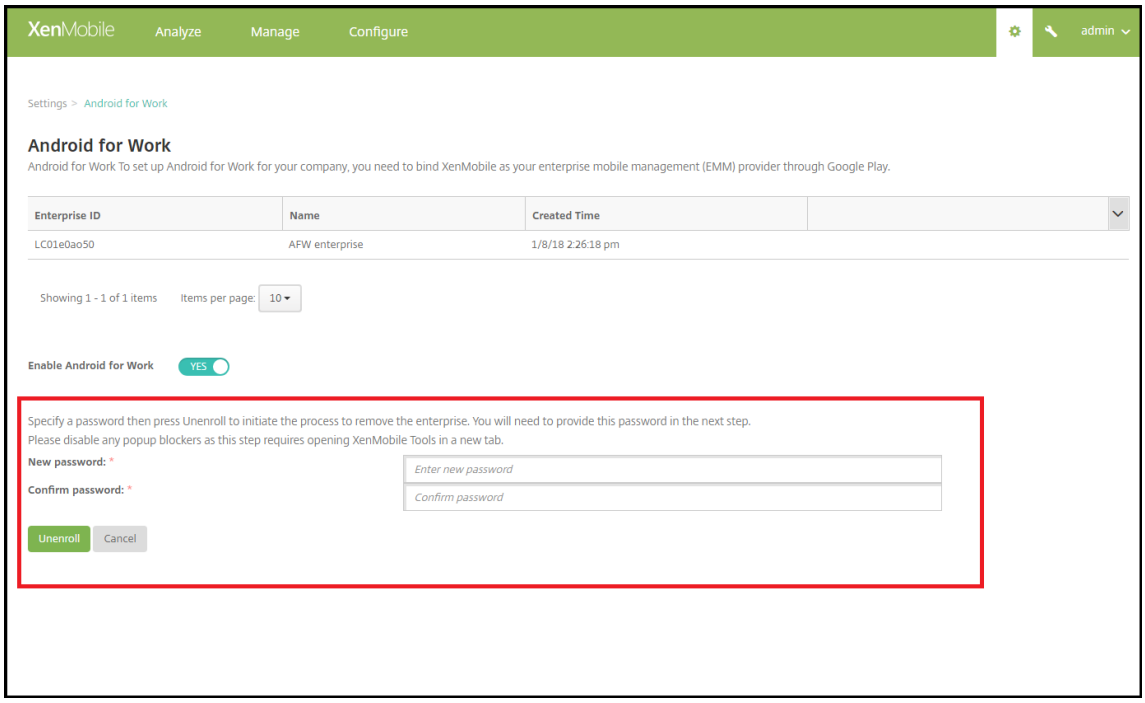
- エンタープライズ経由で登録されていたデバイスとユーザーの Android Enterprise アプリは、デフォルト状態にリセットされます。以前に適用されていた［Android Enterprise アプリの権限］ポリシーと［Android Enterprise アプリの制限］ポリシーは無効になります。
- エンタープライズ経由で登録されていたデバイスは XenMobile によって管理されますが、Google の観点からは管理されません。新しい Android Enterprise アプリを追加することはできません。［Android Enterprise アプリの権限］ポリシーと［Android Enterprise アプリの制限］ポリシーは適用できません。ただし、これらのデバイスには引き続き、スケジュール設定、パスワード、制限などのポリシーは適用できます。
- Android Enterprise にデバイスを登録しようとすると、Android Enterprise デバイスではなく Android デバイスとして登録されます。

Android Enterprise エンタープライズの登録を解除するには:

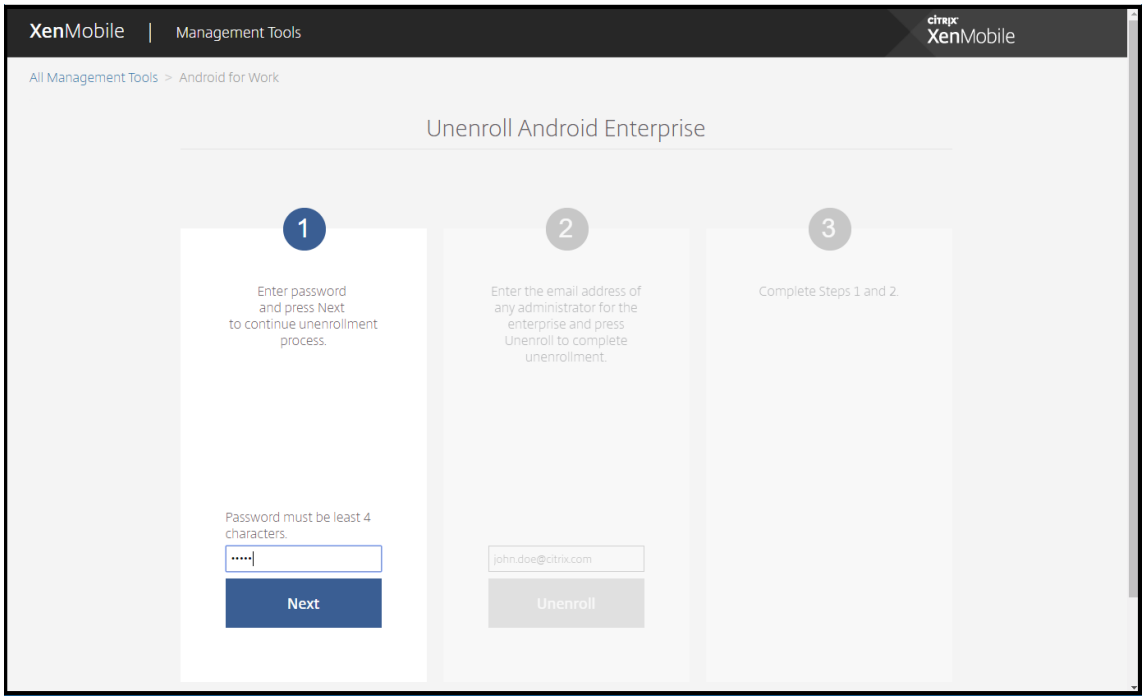
1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。
2. ［設定］ページで、［**Android Enterprise**］ をクリックします。
3. ［エンタープライズの削除］ をクリックします。



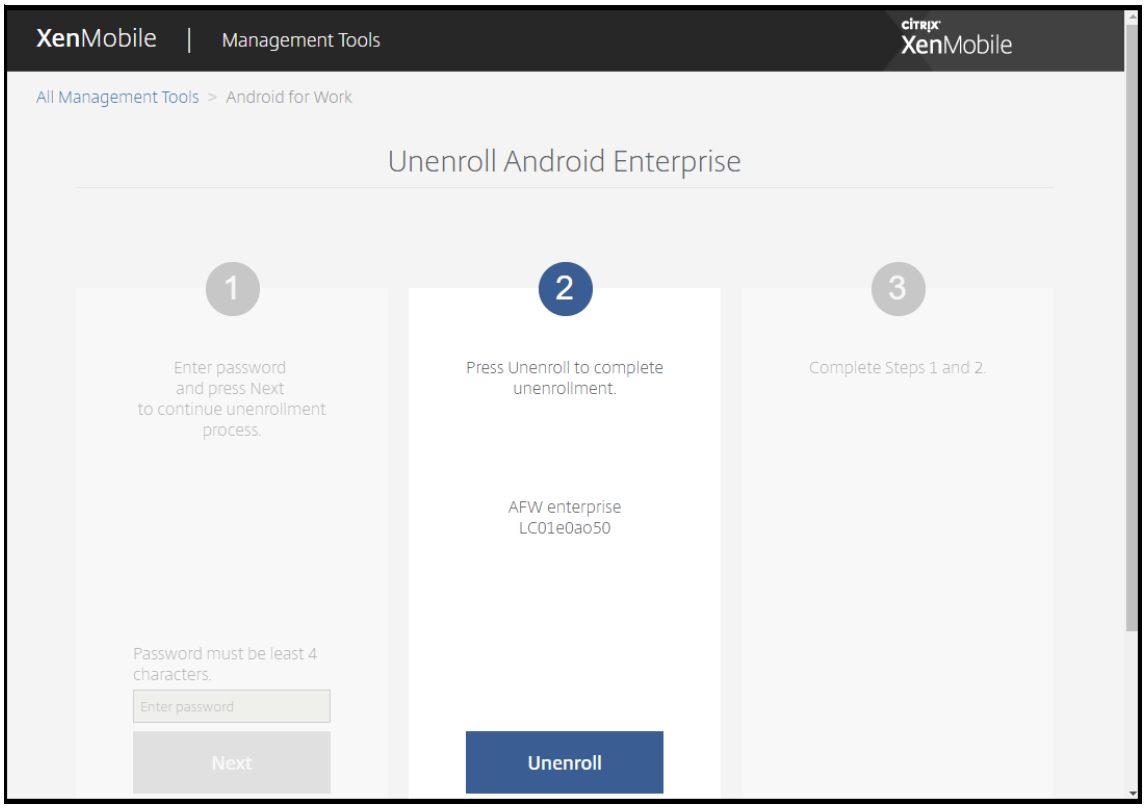
4. パスワードを指定します。登録解除を完了するには、次のステップでこのパスワードが必要になります。［登録解除］ をクリックします。



5. ［XenMobile Tools］ページが開いたら、前の手順で作成したパスワードを入力します。



6. [登録解除] をクリックします。



Android Enterprise での完全に管理されたデバイスのプロビジョニング

Android Enterprise で完全に管理されたデバイスとして使用できるのは、会社所有のデバイスのみです。完全に管理されたデバイスでは、仕事用プロファイルだけでなく、デバイス全体が会社または組織によって管理されます。完全に管理されたデバイスは、仕事用管理対象デバイスとも呼ばれます。

XenMobile は、完全に管理されたデバイスで以下の登録方法をサポートしています：

- **afw#xenmobile**： この登録方法では、ユーザーがデバイスの設定時に「afw#xenmobile」という文字を入力します。このトークンにより、デバイスが XenMobile の管理対象であると識別され、Secure Hub がダウンロードされます。
- **QR** コード： QR コードプロビジョニングは、NFC をサポートしていない、タブレットなどの分散型端末を簡単にプロビジョニングする方法です。QR コード登録方法は、出荷時の設定にリセットされたフリートデバイスで使用できます。QR コードによる登録方法では、セットアップウィザードから QR コードをスキャンすることによって、完全に管理されたデバイスを設定および構成します。
- **NFC**（近距離無線通信）バンプ： NFC バンプ登録方法は、出荷時の設定にリセットされたフリートデバイスで使用できます。NFC バンプは、近距離無線通信を使用して 2 つのデバイス間でデータを転送します。工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびそのほかの通信モードは無効になっています。この状態のデバイスが使用する通信プロトコルは NFC のみです。

afw#xenmobile

この登録方法は、新規デバイスまたは工場出荷時設定にリセットされたデバイスの電源を入れ、初期セットアップを行った後に使用します。ユーザーは、Google アカウントの入力を求められたら「afw#xenmobile」と入力します。この操作により、Secure Hub がダウンロードされインストールされます。インストール後、Secure Hub の設定プロンプトに従って登録を完了します。

この登録方法では Secure Hub の最新バージョンが Google Play ストアからダウンロードされるため、ほとんどのお客様に推奨されます。他の登録方法とは異なり、XenMobile サーバーでダウンロード用に Secure Hub を提供することはありません。

前提条件：

- Android 5.0 以降を実行するすべての Android デバイスでサポートされます。

QR コード

QR コードを使用してデバイスモードでデバイスを登録するには、JSON を作成してから QR コードに変換して、QR コードを生成します。この QR コードをデバイスカメラでスキャンし、デバイスを登録します。

前提条件：

- Android 7.0 以降を実行するすべての Android デバイスでサポートされます。

JSON から **QR** コードを作成する

次のフィールドがある JSON を作成します。

これらのフィールドは必須です。

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

値: com.zenprise / com.zenprise.configuration.AdminFunction

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

値: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

の値: `https://path/to/securehub.apk`

> 注:
>
> Secure Hub が Citrix XenMobile サーバーにエンタープライズアプリとしてアップロードされている場合は、`https://<fqdn>:4443/*instanceName*/worxhome.apk`からダウンロードできます。上記の値として使用される Secure Hub APK へのパスは、プロビジョニング中にデバイスが接続される Wi-Fi 接続を介してアクセスできる必要があります。

これらのフィールドはオプションです。

- **android.app.extra.PROVISIONING_LOCALE**: 言語コードおよび国コードを入力します。

  言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。

- **android.app.extra.PROVISIONING_TIME_ZONE**: これはデバイスが実行されているタイムゾーンです。

  フォームの地域/場所の Olson 名を入力します。たとえば、米国太平洋標準時の場合は「America/-Los_Angeles」です。入力しない場合、タイムゾーンは自動的に入力されます。

- **android.app.extra.PROVISIONING_LOCAL_TIME:** エポックからのミリ秒単位の時間。

  Unix エポック（または Unix 時間または POSIX 時間または Unix タイムスタンプ）は、1970 年 1 月 1 日（UTC/GMT 午前 0 時）から経過した秒数で、うるう秒数は含まれません（ISO 8601: 1970-01-01T00:00:00Z）。

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION**: プロファイル作成時に暗号化をスキップするには、**true** に設定します。プロファイルの作成時に暗号化を強制するには、**false** に設定します。

以下の図に、典型的な JSON の例を示します。

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "                                                  ",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```


https://jsonlint.comなどの JSON 検証ツールを使用して作成された JSON を検証します。https://goqr.meなどのオンライン QR コードジェネレータを使用して、JSON 文字列を QR コードに変換します。

この QR コードは工場出荷時の設定にリセットされたデバイスによってスキャンされ、これによってデバイスを仕事用管理対象デバイスモードで登録できます。

デバイスを登録するには

完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットする必要があります。

1. ようこそ画面で画面を 6 回タップすると、QR コードの登録フローが開始されます。
2. プロンプトが表示されたら、Wi-Fi に接続します。（JSON でエンコードされた）QR コードにある Secure Hub のダウンロード場所には、この Wi-Fi ネットワーク経由でアクセスできます。

   端末が Wi-Fi に接続されると、Google から QR コードリーダーをダウンロードしてカメラを起動します。
3. カメラを QR コードに合わせて、コードをスキャンします。

   Android は、QR コードのダウンロード場所から Secure Hub をダウンロードし、署名証明書の署名を検証し、Secure Hub をインストールし、デバイス所有者として設定します。

詳しくは、Android EMM デベロッパー向け Google ガイド（https://developers.google.com/android/work/prov-devices#qr_code_method）を参照してください。

NFC バンプ

NFC バンプを使用して完全に管理されたデバイスとしてデバイスを登録するには、工場出荷時の設定にリセットされたデバイスと、XenMobile Provisioning Tool を実行するデバイスの 2 台のデバイスが必要です。

前提条件:

- Android 5.0、Android 5.1、Android 6.0 以降を実行するすべての Android デバイスでサポートされます。
- Android Enterprise を有効にした XenMobile Server バージョン 10.4。
- 完全に管理されたデバイスとして Android Enterprise 向けにプロビジョニングされた、新規または工場出荷時設定にリセットされたデバイス。この前提条件を完了する手順については、後述します。
- 構成済みの Provisioning Tool を実行している、NFC 機能が備わった別のデバイス。Provisioning Tool は、Secure Hub 10.4 またはシトリックスのダウンロードページから入手できます。

各デバイスにはエンタープライズモビリティ管理（EMM）アプリで管理された Android Enterprise プロファイルが 1 つのみ存在します。XenMobile で、Secure Hub は EMM アプリです。各デバイスには、1 つのプロファイルしか許可されません。2 つ目の EMM アプリを追加すると、1 つ目の EMM アプリが削除されます。

NFC バンプを介して転送されるデータ

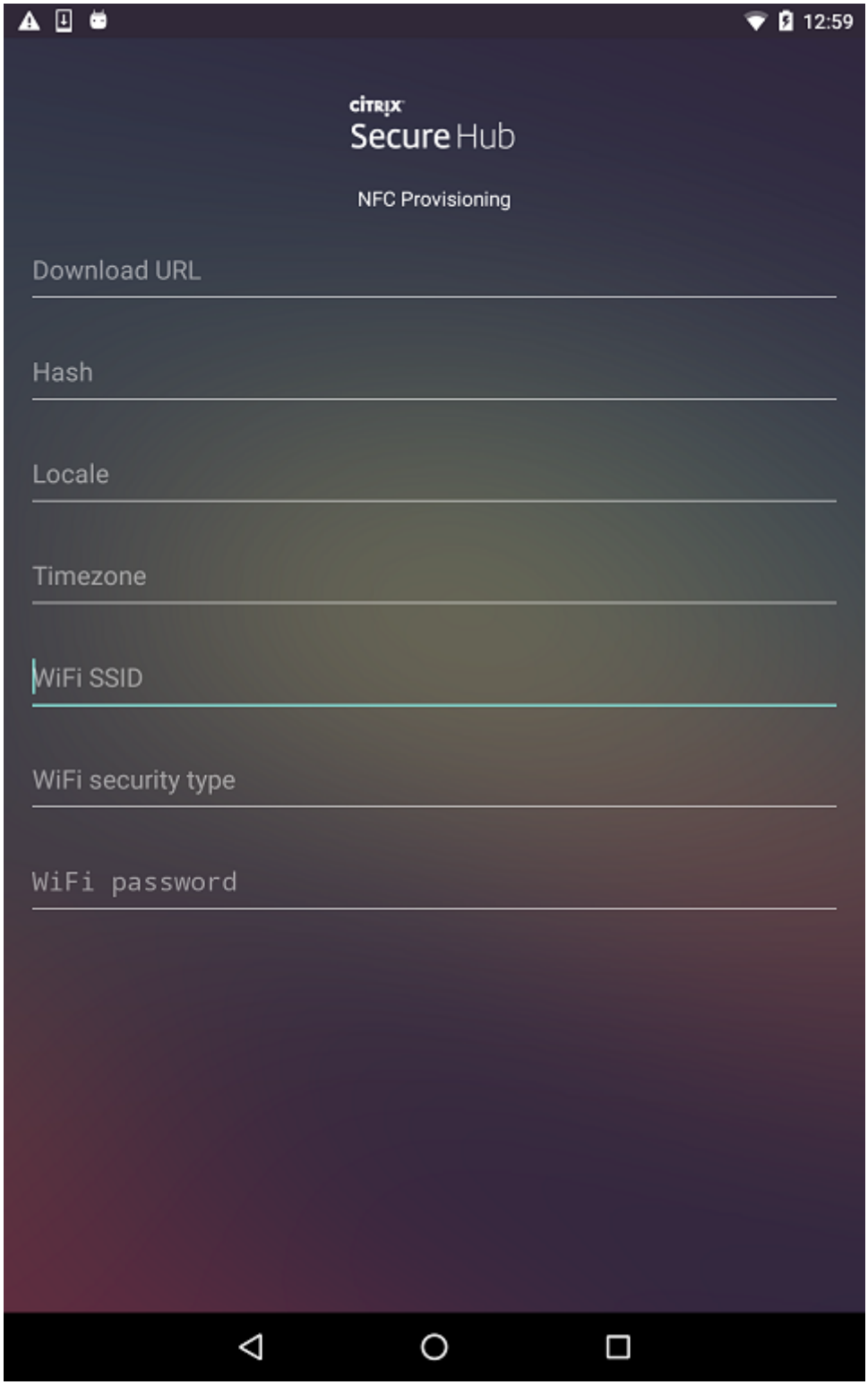
工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータを NFC バンプ経由で送信して Android Enterprise を初期化する必要があります:

- デバイス所有者として機能する EMM プロバイダーアプリ（この場合は、Secure Hub）のパッケージ名。
- デバイスが EMM プロバイダーアプリをダウンロードできるイントラネット/インターネット上の場所。
- ダウンロードが正常に完了したかどうかを確認する EMM プロバイダーアプリの SHA1 ハッシュ。
- 工場出荷時の設定にリセットされたデバイスが EMM プロバイダーアプリに接続してダウンロードできるようにする Wi-Fi 接続の詳細。注: 現時点では、Android はこの手順での 802.1x Wi-Fi をサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、Provisioning Tool のデータが工場出荷時の設定にリセットされたデバイスに送信されます。このデータはその後、管理者設定での Secure Hub のダウンロードに使用されます。タイムゾーンと場所の値を入力しない場合、新しいデバイスでは Android によって自動的にこれらの値が構成されます。

XenMobile Provisioning Tool の構成

NFC バンプを行う前に、Provisioning Tool を構成する必要があります。この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFC バンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルから入力することもできます。次の手順では、テキストファイルを構成する方法と各フィールドに説明を含める方法について説明します。入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

テキストファイルを使用して **Provisioning Tool** を構成するには

ファイルの名前を nfcprovisioning.txt にして、/sdcard/フォルダーにあるデバイスの SD カードに格納します。アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには、次のデータを含める必要があります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>

この行は、EMM プロバイダーアプリのイントラネット/インターネットの場所です。工場出荷時設定のデバイスが NFC バンプの後に Wi-Fi に接続した場合、デバイスはダウンロードのためにこの場所にアクセスする必要があります。URL は通常の URL で、特別な形式にする必要はありません。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>

この行は、EMM プロバイダーアプリのチェックサムです。このチェックサムはダウンロードが成功したかを検証するために使用されます。チェックサムを取得する手順については、後述します。

android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>

この行は、Provisioning Tool を実行しているデバイスが接続されている Wi-Fi の SSID です。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>

サポートされる値は WEP および WPA2 です。Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>

Wi-Fi が保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_LOCALE=<locale>

言語コードと国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で 2 文字の ISO 言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で 2 文字の ISO 国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

android.app.extra.PROVISIONING_TIME_ZONE=<timezone>

デバイスが実行されるタイムゾーンです。フォームの地域/場所の Olson 名を入力します。たとえば、米国太平洋標準時の場合は「America/Los_Angeles」です。名前を入力しない場合、タイムゾーンは自動的に入力されます。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<**package** name>

このデータは Secure Hub としてアプリにハードコードされるため、必須ではありません。ここでは、情報の完全性を守るためだけに記載しています。

WPA2 を使用して保護された Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk


```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

保護されていない Wi-Fi の場合、完了した nfcprovisioning.txt ファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https
://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crb
\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Secure Hub チェックサムを取得するには

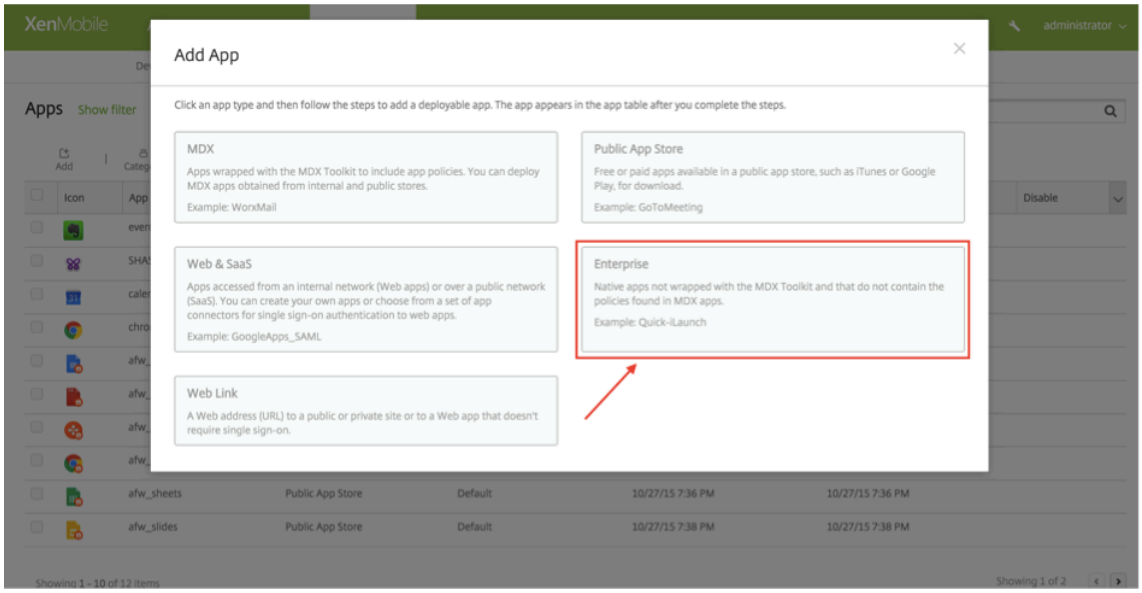
アプリのチェックサムを取得するには、そのアプリをエンタープライズアプリとして追加します。

1. XenMobile コンソールで、［構成］**>**［アプリ］ を選択してから、［追加］ をクリックします。

   ［アプリの追加］ ウィンドウが開きます。

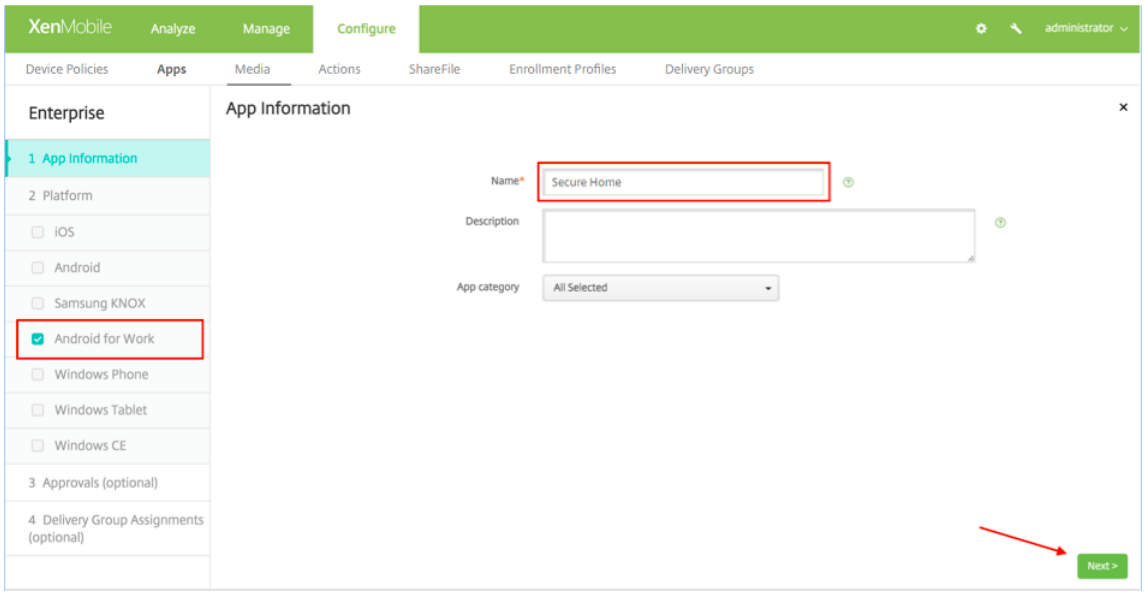
2. ［エンタープライズ］ をクリックします。

   ［アプリ情報］ ページが開きます。



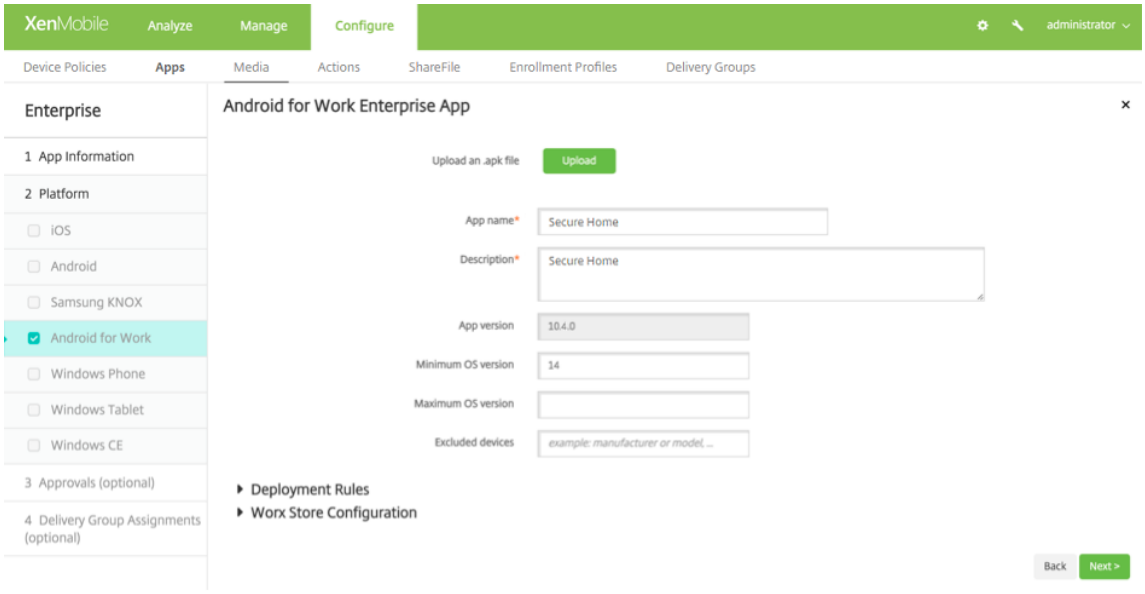
3. 次の構成を選択して ［次へ］ をクリックします。

   ［**Android Enterprise** エンタープライズアプリ］ ページが開きます。

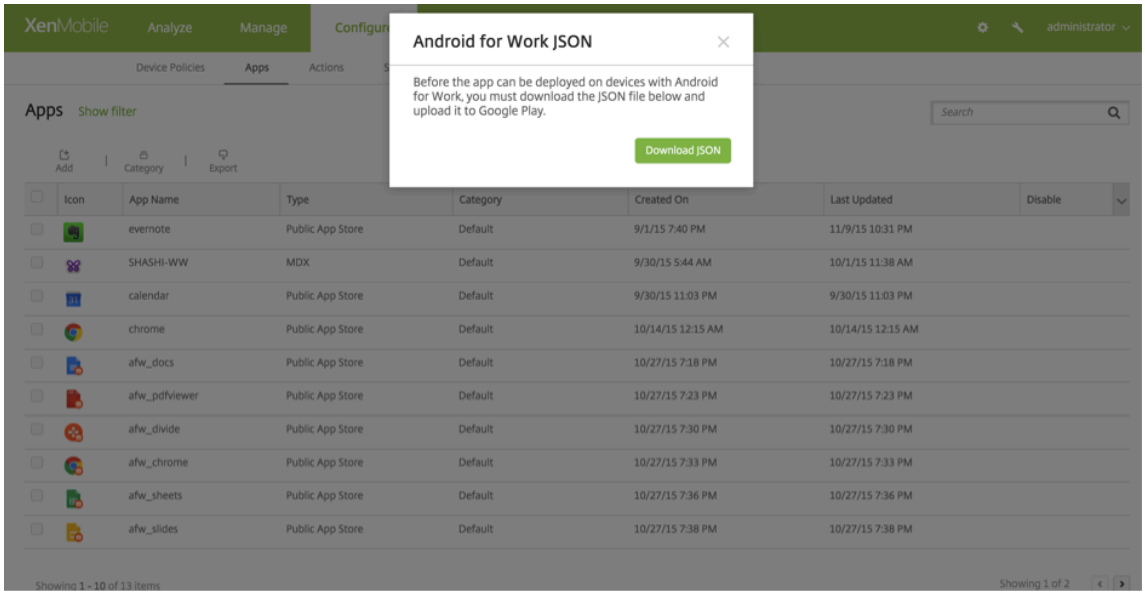


4. .apk へのパスを入力し、 ［次へ］ をクリックしてファイルをアップロードします。

   アップロードが完了すると、アップロードされたパッケージの詳細が表示されます。



5. [次へ] をクリックして JSON ファイルをダウンロードするページを表示します。このファイルは、この後 Google Play へのアップロードに使用します。Secure Hub の場合、Google Play にアップロードする必要はありませんが、SHA1 を読み込む元になる JSON ファイルが必要です。



以下の図に、典型的な JSON ファイルの例を示します:

6. **file_sha1_base64** の値をコピーして、この値を Provisioning Tool の [ハッシュ] フィールドで使用します。

> 注：
>
> ハッシュは URL セーフのものにする必要があります。

- **+** 記号はすべて**-**に変換します。
- **/**記号はすべて **_** に変換します。
- 末尾の**\u003d** は **=** に置き換えます。

ハッシュをデバイスの SD カードの nfcprovisioning.txt ファイルに格納すると、安全のための変換が行われます。ただし、ハッシュを手動で入力すると、URL の安全性は入力者の責任になります。

使用するライブラリ

Provisioning Tool では、以下のライブラリがソースコードに使用されています。

- v7 appcompat library、Design support library、および v7 Palette library by Google（Apache license 2.0）

  詳しくは、「Support Library の機能」を参照してください。

- Butter Knife by Jake Wharton（Apache license 2.0）

Android Enterprise での仕事用プロファイルデバイスのプロビジョニング

Android Enterprise の仕事用プロファイルデバイスでは、デバイス上の会社領域と個人領域を安全に分離できます。たとえば、BYOD デバイスを仕事用プロファイルデバイスにすることができます。仕事用プロファイルデバイスの登録は、XenMobile の Android 登録と同様の操作です。ユーザーは Google Play から Secure Hub をダウンロードし、デバイスを登録します。

デバイスが Android Enterprise で仕事用プロファイルデバイスとして登録されている場合、デフォルトでは USB デバッグおよび不明なソース設定は無効になっています。

> ヒント：
>
> Android Enterprise のデバイスを仕事用プロファイルデバイスとして登録する場合は、必ず Google Play にアクセスしてください。そこから、ユーザーの個人プロファイルでの Secure Hub の表示を有効にします。

iOS および **macOS** デバイスの一括登録

January 24, 2020

次の 2 つの方法で多数の iOS デバイスと macOS デバイスを XenMobile に追加できます。

- Apple、加入式の Apple 認定リセラー、またはキャリアから直接購入した iOS および macOS デバイスの登録は、Apple デバイス登録プログラム（DEP）を使用して登録できます。XenMobile は、ビジネス向けデバイス登録プログラムと、教育向け Apple School Manager をサポートします。ここでは、ビジネス用 DEP アカウントとの統合について説明します。Apple School Manager の DEP アカウントについて詳しくは、「Apple Education 機能との統合」を参照してください。

  XenMobile で macOS デバイスを DEP により登録する場合、そのデバイスでは macOS 10.10 以降を実行している必要があります。

- また、iOS デバイスは、Apple から直接購入したかどうかにかかわらず Apple Configurator を使用してを登録できます。

企業向け DEP の場合:

- 実物のデバイスを直に設定つまり準備する必要はありません。代わりに、デバイスのシリアル番号または発注番号を DEP 経由で送信して、デバイスの構成と登録を行います。
- XenMobile にデバイスが登録されると、ユーザーは、登録されたデバイスをすぐに使い始めることができます。さらに、DEP でデバイスをセットアップすると、ユーザーが初めてデバイスを起動したときに入力する必要のある設定アシスタントの手順の一部を省略できます。
- DEP のセットアップについて詳しくは、Apple のビジネスサポートページを参照してください。

Apple Configurator の場合:

- macOS 10.7.2 以降および Apple Configurator 2 アプリが動作する Apple コンピューターに iOS デバイスを接続します。Apple Configurator 2 を介して iOS デバイスを準備しポリシーを構成します。
- デバイスを必要なポリシーでプロビジョニングした後に初めて XenMobile に接続すると、そのデバイスに XenMobile からポリシーが送信されます。その後、デバイスの管理を開始できます。
- Apple Configurator の使用について詳しくは、Apple Configurator サポートページを参照してください。

前提条件

- Apple、加入式の Apple 認定リセラー、またはキャリアから直接購入した iOS および macOS デバイスの登録は、Apple デバイス登録プログラム（DEP）を使用して登録できます。XenMobile は、ビジネス向けデバイス登録プログラムと、教育向け Apple School Manager をサポートします。ここでは、ビジネス用 DEP アカウントとの統合について説明します。Apple School Manager の DEP アカウントについて詳しくは、「Apple Education 機能との統合」を参照してください。

XenMobile と Apple を接続するには、必要なポートを開く必要があります。詳しくは、「ポート要件」を参照してください。

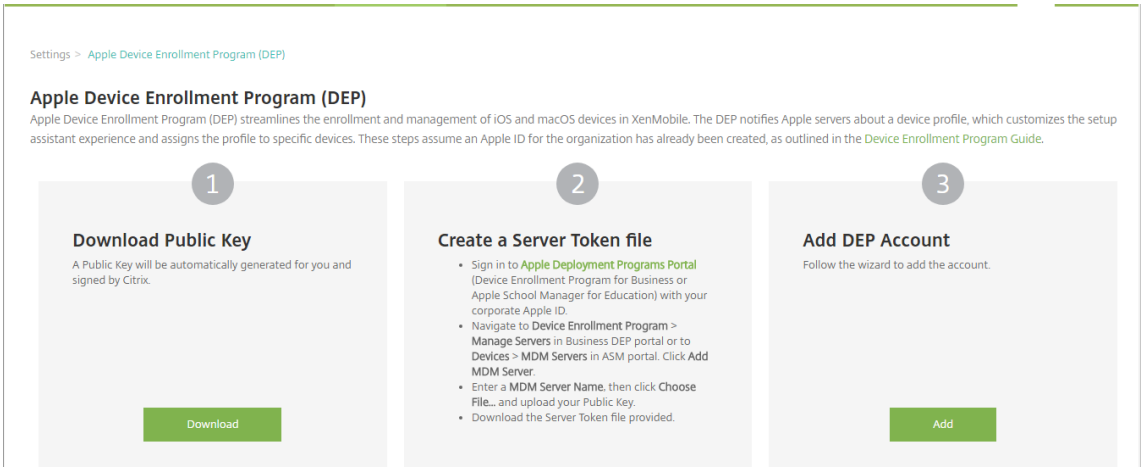
ビジネス用 **Apple DEP** アカウントと **XenMobile** の統合

企業向け Apple DEP アカウントを持っていない場合は「Apple DEP を介した iOS と macOS デバイスの展開」を参照して下さい。

ビジネス用 Apple DEP アカウントを XenMobile サーバー環境に接続するには、以下の手順に従って XenMobile コンソールと Apple DEP ポータルで情報を入力します。

手順 **1**: **XenMobile** サーバーから公開キーをダウンロードします

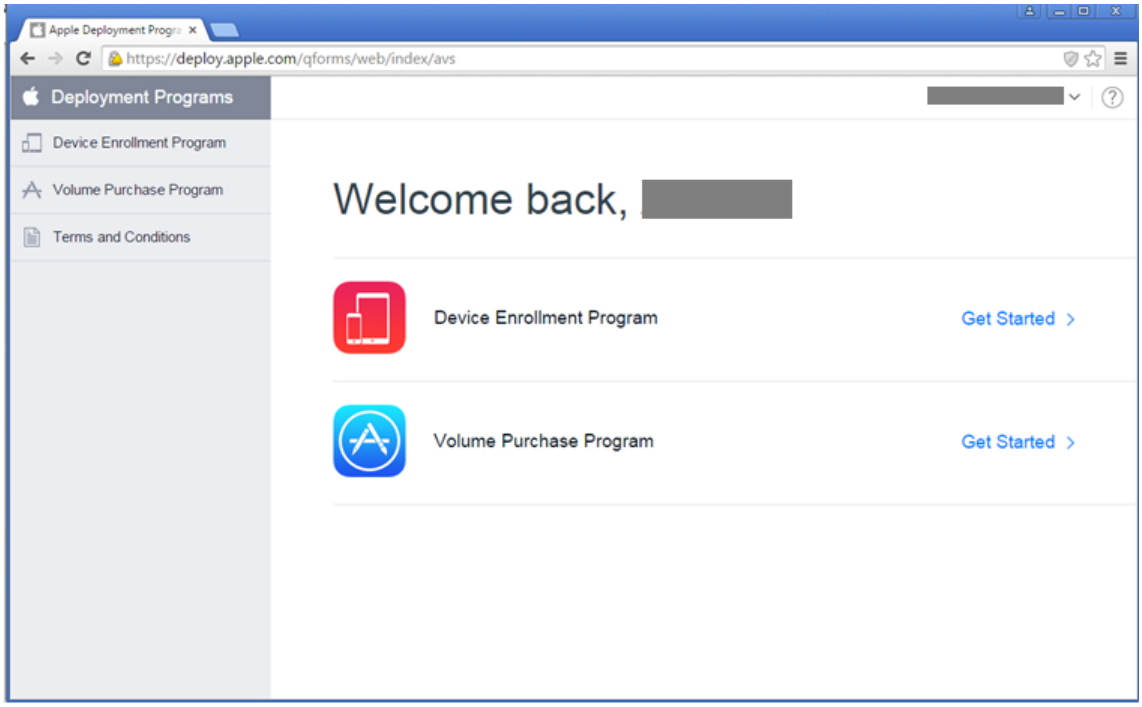
1. XenMobile コンソールにログオンし、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ の順に移動します。



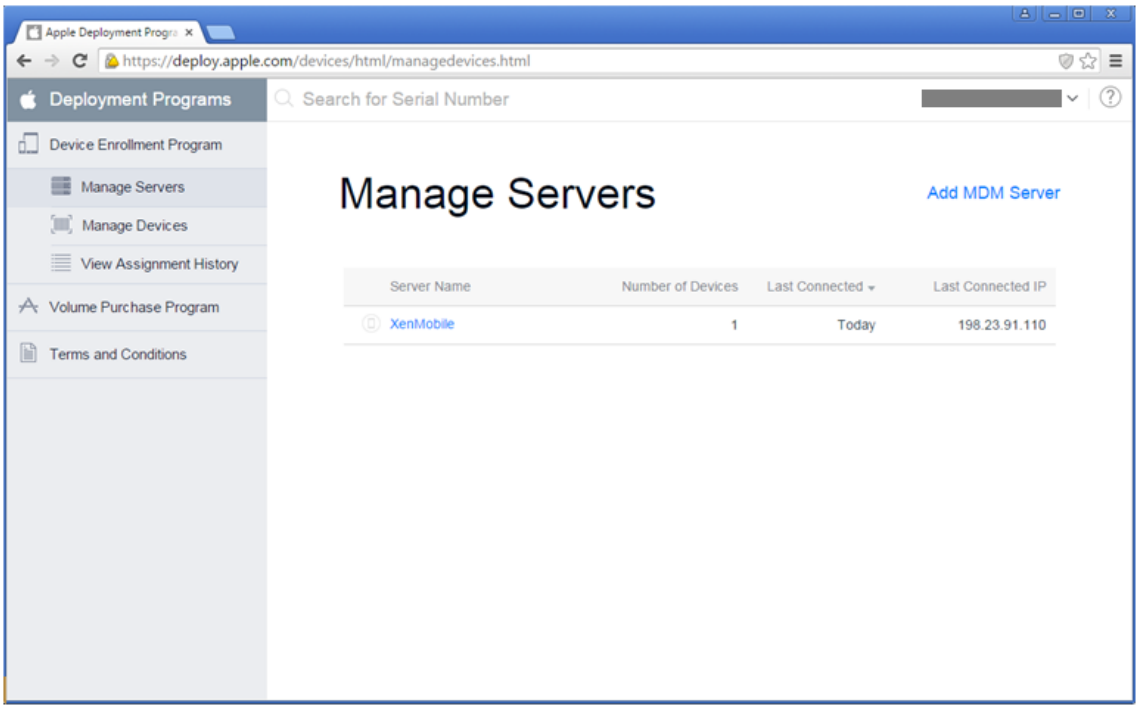
2. ［公開キーのダウンロード］ の下にある ［ダウンロード］ をクリックします。

手順 **2**: **Apple** アカウントからサーバートークンファイルを作成してダウンロードします

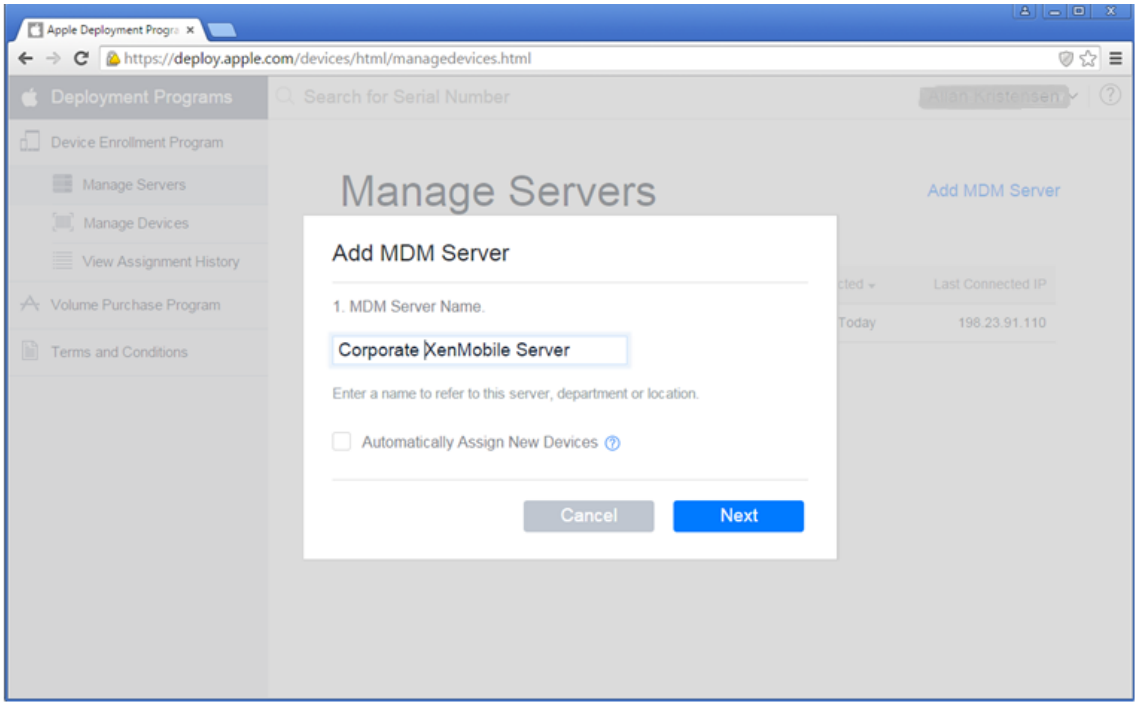
1. 企業の Apple ID を使用して、Apple Deployment Program Portalにログオンします。
2. Apple DEP Portal で、［**Device Enrollment Program**］ をクリックします。



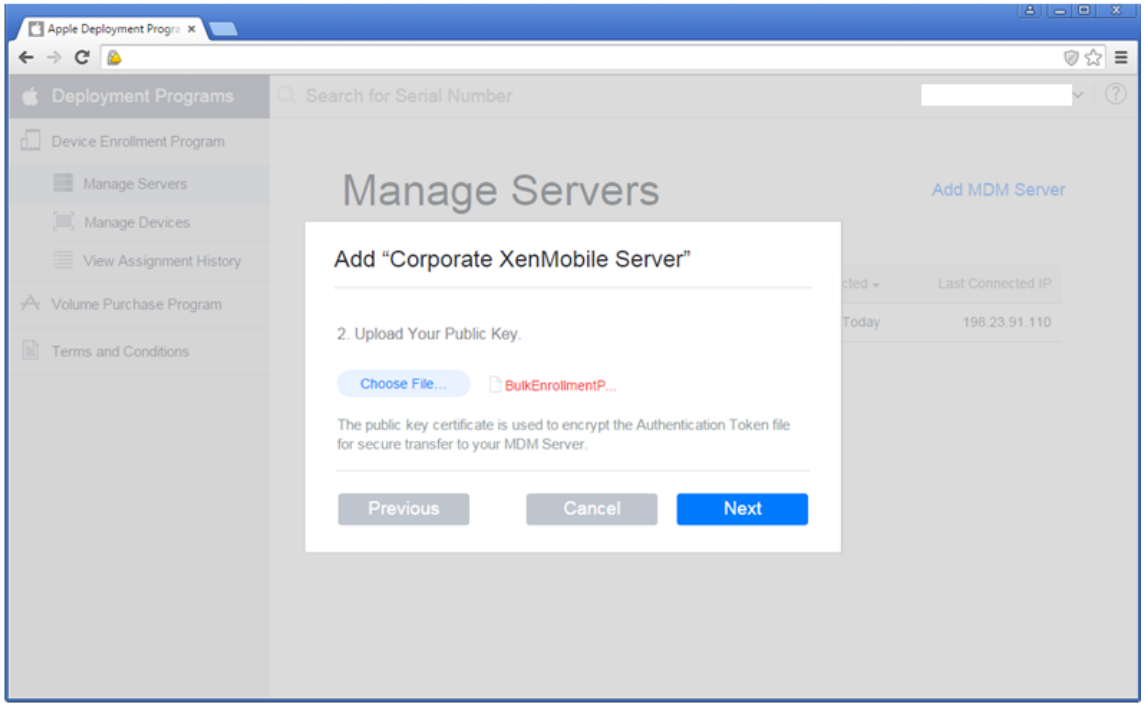
3. [**Manage Servers**] をクリックし、右側にある [**Add MDM Server**] をクリックします。



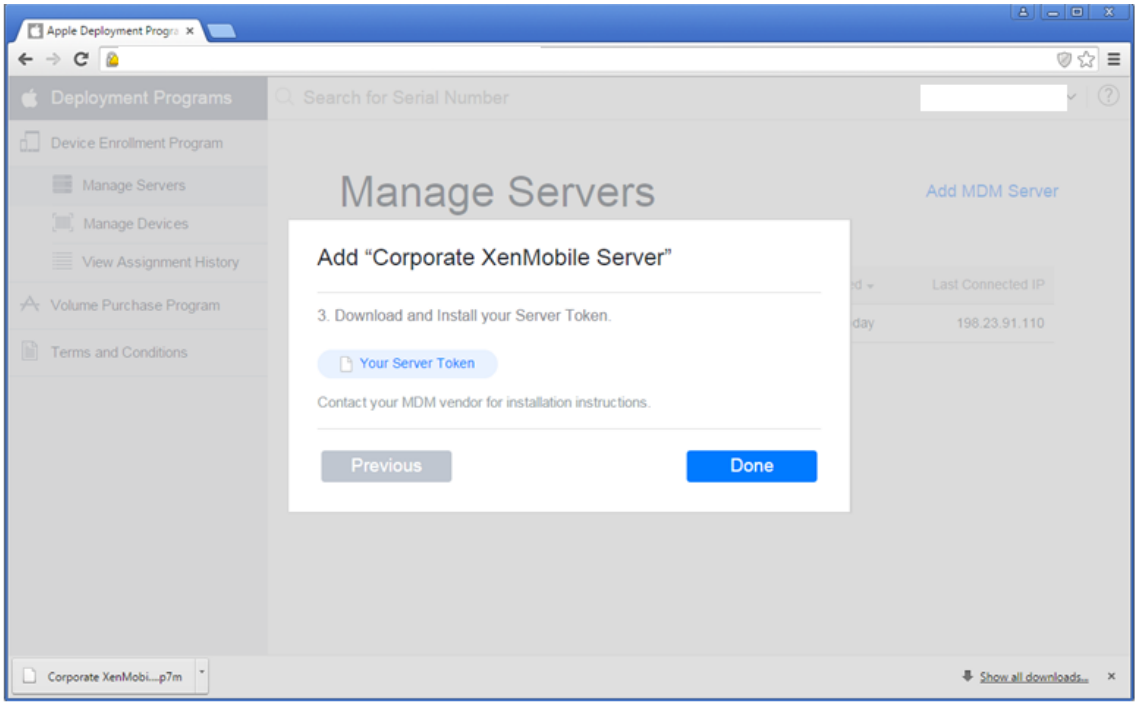
4. [**Add MDM Server**] に XenMobile サーバーの名前を入力し、[**Next**] をクリックします。



5. Apple DEP Portal で、［**Choose file**］ をクリックして、XenMobile からダウンロードした公開キーを選択し、［**Next**］ をクリックします。



6. ［**Your Server Token**］ をクリックして、ブラウザーからダウンロードするサーバートークンを生成し、［**Done**］ をクリックします。



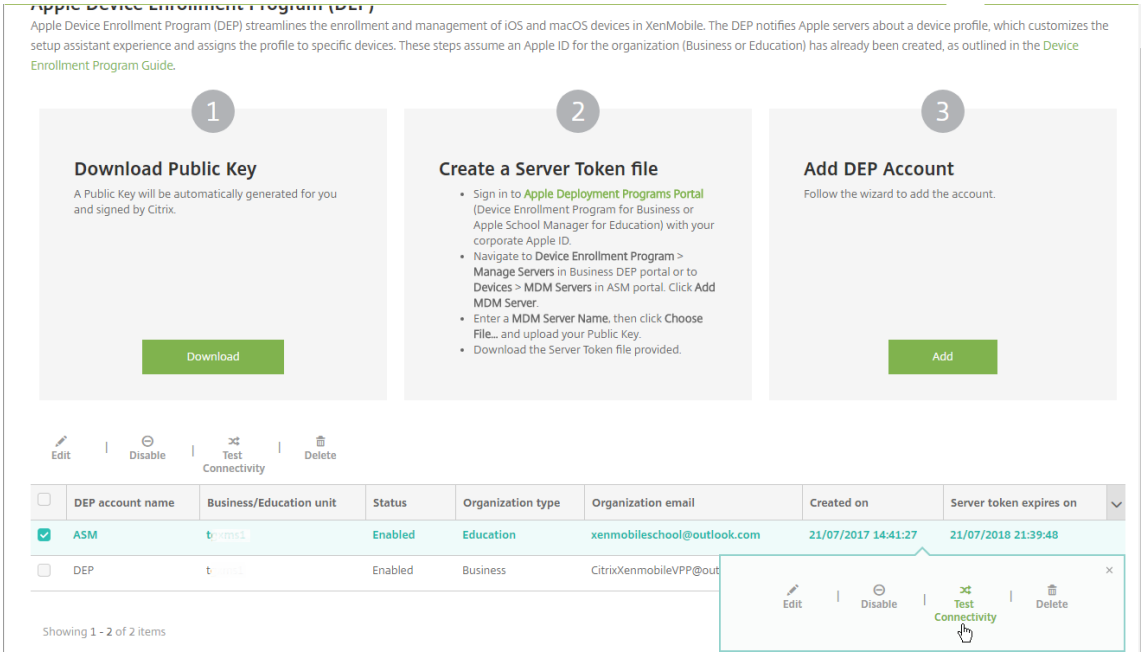
トークンファイルをインポートした後、Apple DEP トークン情報が XenMobile コンソールに表示されます。XenMobile に DEP アカウントを追加するときに、このサーバートークンファイルをアップロードします。

手順 **3**: **XenMobile** に **DEP** アカウントを追加します

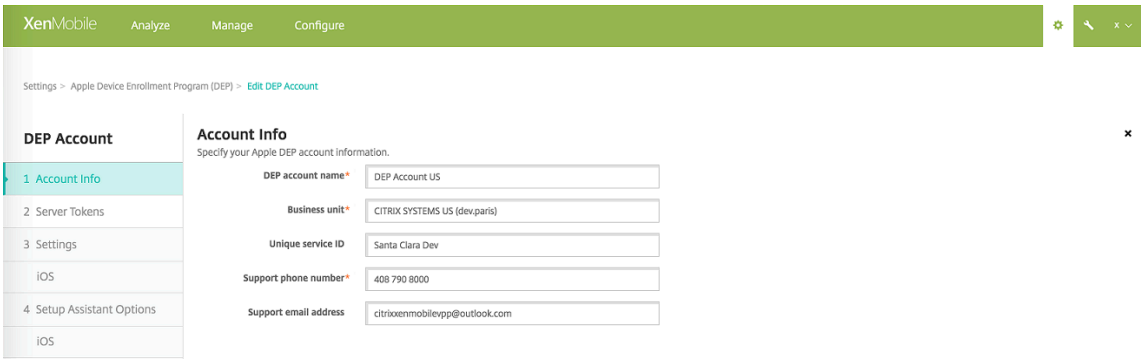
XenMobile には複数の DEP アカウントを追加できます。この機能によって、国や部門などごとに異なる登録設定や設定補助オプションを利用できるようになります。追加後、各 DEP アカウントをさまざまなデバイスポリシーに関連付けることができます。

たとえば、同じ XenMobile サーバーにさまざまな国の DEP アカウントをすべて集約して、すべての DEP デバイスをインポートして管理することもできます。登録設定と設定補助オプションを部門、組織上の階層、または他の構造ごとにカスタマイズすることで、ポリシーが組織全体で適切に機能し、デバイスユーザーが適切な設定補助を受けられるようになります。

1. XenMobile コンソールで、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ に移動し、［**DEP** アカウントの追加］ の ［追加］ をクリックします。

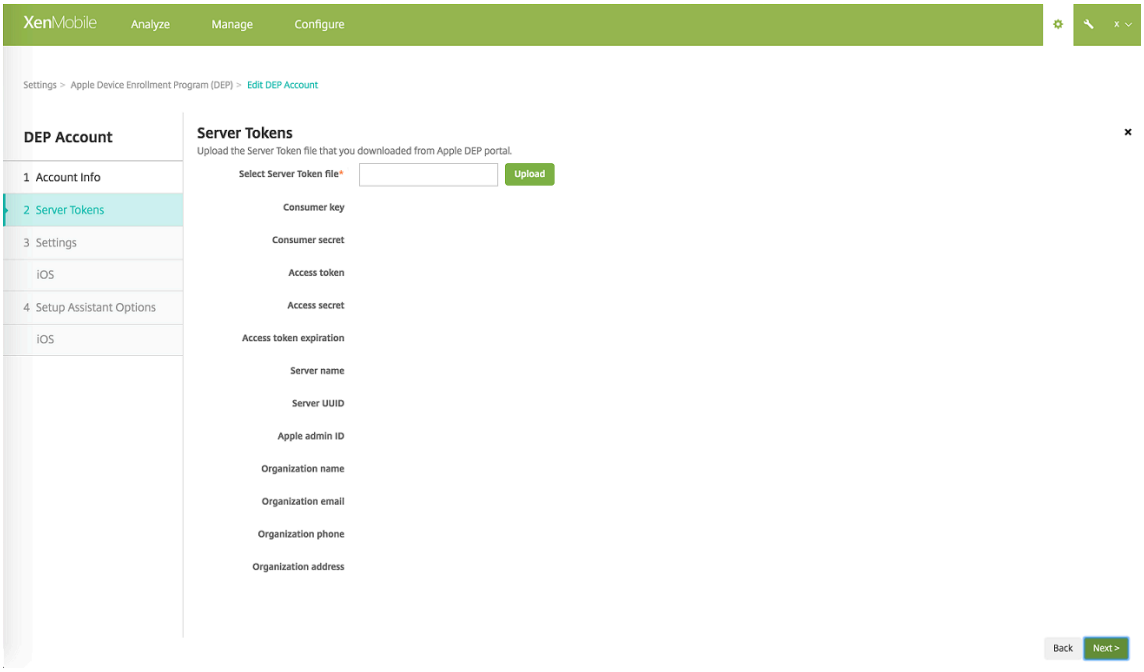


2. [アカウント情報] ページで次の設定を入力します。



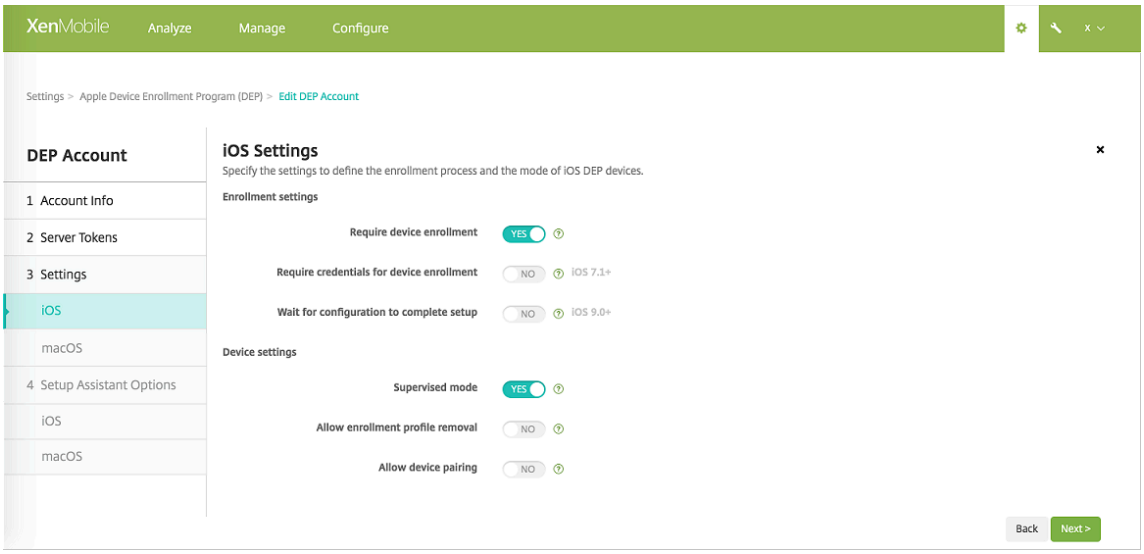
- **DEP** アカウント名： この DEP アカウントの一意の名前。国や組織構造など、DEP アカウントの分類を示す名前を付けます。
- 事業/教育単位： デバイスを割り当てる事業単位または部門。このフィールドは必須です。
- 一意のサービス **ID**： アカウントの識別に役立つオプションの一意の ID です。
- サポート用電話番号： ユーザーがセットアップ時にサポートが必要となった場合に連絡するサポートの電話番号。このフィールドは必須です。
- サポート用メールアドレス： エンドユーザーが使用できるサポート用のメールアドレス（オプション）。

3. [サーバートークン] ページでサーバートークンファイルを指定し、 [アップロード] をクリックします。



サーバートークンの情報が表示されます。

4. [**iOS** 設定] で次の設定を入力します。



登録設定：

- デバイス登録を必須にする：ユーザーにデバイス登録を要求するかどうか。デフォルトは［はい］です。
- デバイス登録のための資格情報を求める： DEP のセットアップ時にユーザーに資格情報の入力を要求するかどうか。デバイスの登録ですべてのユーザーに資格情報を入力を要求し、承認済みのユーザーだけがデバイスを登録できるようにしてください。デフォルトは ［はい］ です。

  初回のセットアップで DEP を有効にしており、このオプションをオンにしない場合、DEP ユーザー、Secure Hub、ソフトウェアインベントリ、DEP 展開グループなどの DEP コンポーネントが作成され

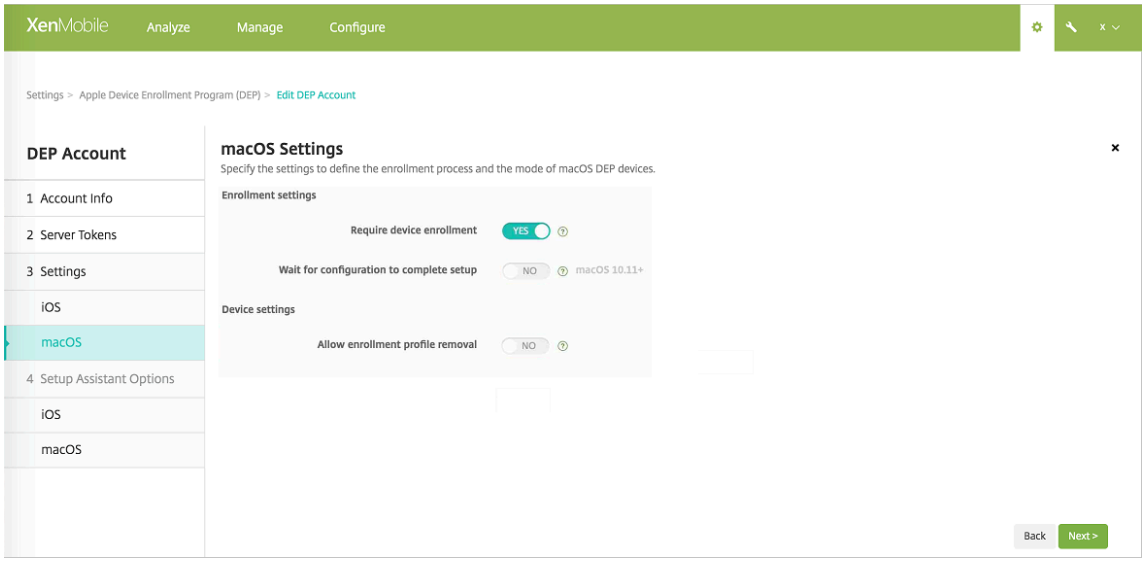
ます。このオプションを選択すると、XenMobile によってコンポーネントは作成されません。そのため、後でこのオプションをオフにしても、これらの DEP コンポーネントは存在しないため、資格情報を入力していないユーザーは DEP 登録を実行できません。その場合、DEP コンポーネントを追加するには、DEP アカウントを無効化してもう一度有効化する必要があります。

- セットアップを完了するため構成を待機する: すべての MDM リソースがユーザーのデバイスに展開されるまで、デバイスをセットアップアシスタントモードのままにしておく必要があるかどうか。これは iOS 9.0 以降の Supervised モードのデバイスでのみ使用できます。デフォルトは ［いいえ］ です。
- Apple のドキュメントによると、デバイスがセットアップアシスタントモードの間は以下のコマンドが機能しない場合があります。
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

デバイス設定:

- 監視モード: DEP で登録したデバイスを Apple Configurator で管理する場合、または ［セットアップを完了するため構成を待機する］ が有効な場合は、［はい］ に設定する必要があります。デフォルトは ［はい］ です。iOS デバイスを Supervised モードにする方法について詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。
- 登録プロファイルの削除を許可: リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。デフォルトは ［いいえ］ です。
- デバイスのペアリングを許可: DEP で登録したデバイスを iTunes および Apple Configurator で管理できるかどうか。デフォルトは ［いいえ］ です。

5. ［**macOS** 設定］ で設定を入力します。



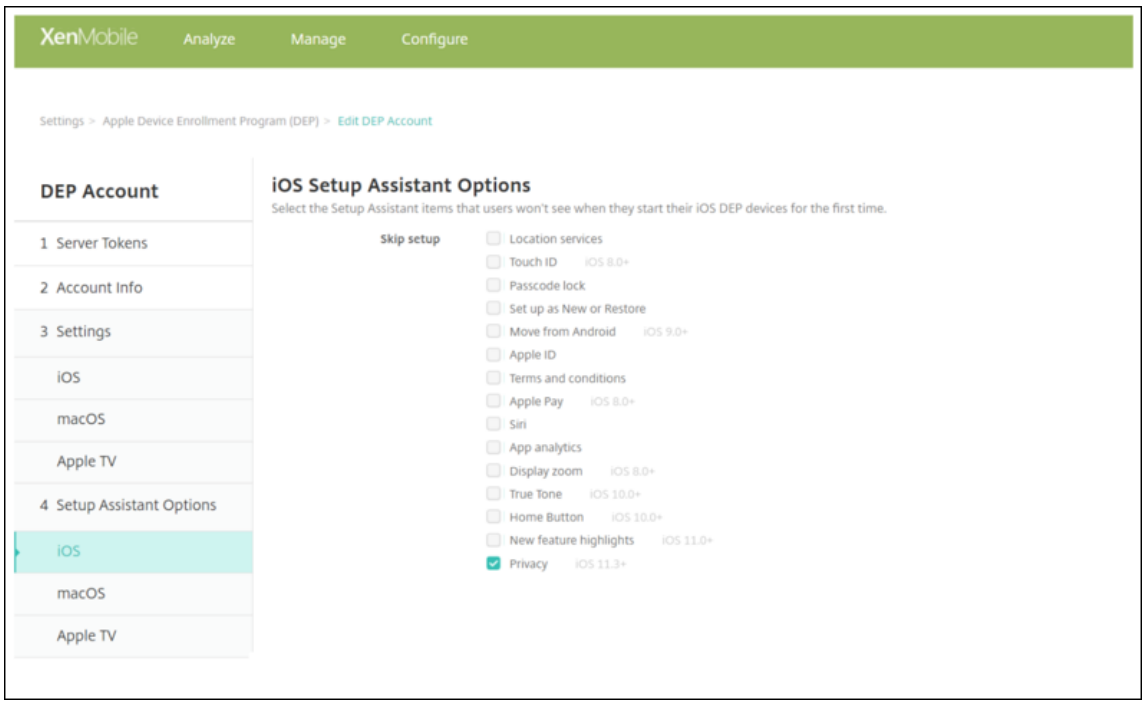
登録設定：

- デバイス登録を必須にする：ユーザーにデバイス登録を要求するかどうか。デフォルトは［はい］です。
- セットアップを完了するため構成を待機する：［はい］の場合、MDM リソースパスコードがデバイスに展開されるまで、macOS デバイスはセットアップアシスタントを続行しません。その展開が行われるのは、ローカルアカウントの作成前になります。この設定は macOS 10.11 以降のデバイスで使用できます。デフォルトは［いいえ］です。

デバイス設定：

- 登録プロファイルの削除を許可：リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。デフォルトは［いいえ］です。

6. ［**iOS** セットアップアシスタントオプション］で、ユーザーが初めてデバイスを起動するときにスキップする iOS セットアップアシスタントの手順を選択します。すべての項目は、デフォルトで選択が解除されています。



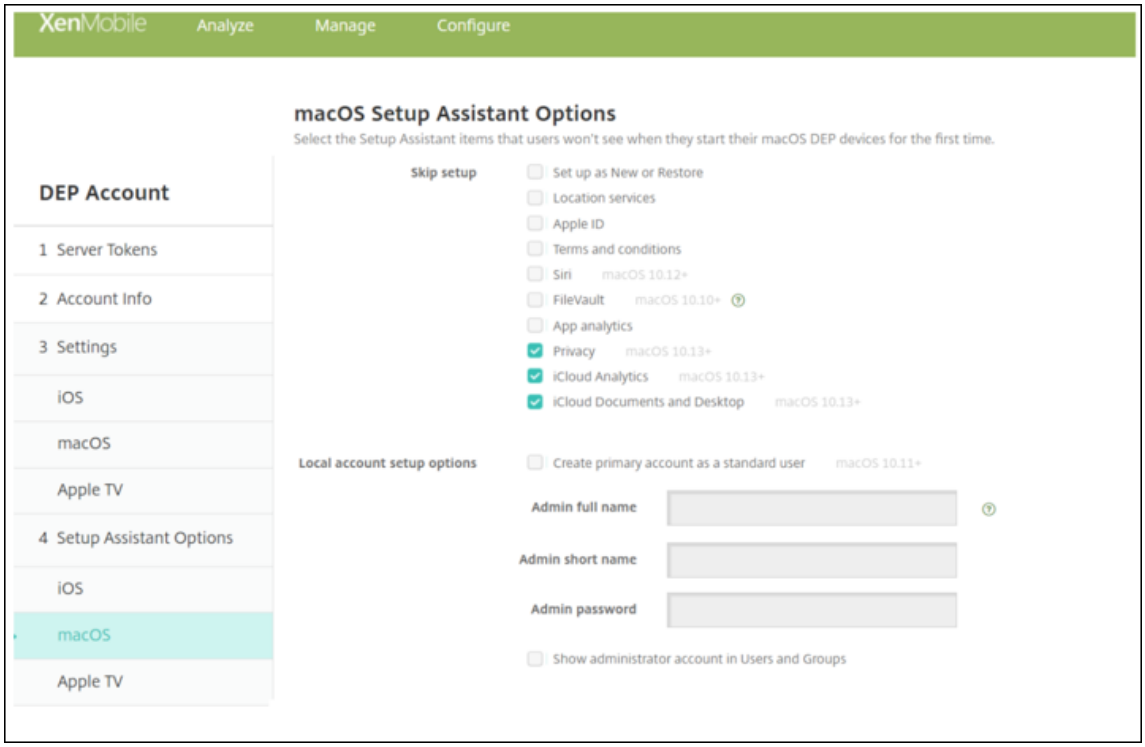
- 位置情報サービス： デバイスに位置情報サービスを設定します。
- **Touch ID**： iOS 8.0 以降のデバイスに Touch ID を設定します。
- パスコードロック： デバイスのパスコードを作成します。
- 新規としてセットアップまたは復元： 新規に、または iCloud か iTunes のバックアップからデバイスを設定します。
- **Android** から移動： Android デバイスから iOS 9 以降のデバイスへのデータ転送を有効にします。このオプションは、［新規としてセットアップまたは復元］ がオンの場合（すなわち、手順をスキップする場合）にのみ使用できます。
- **Apple ID**： デバイスの Apple ID アカウントを設定します。
- 使用条件： デバイスの使用契約条件に対する同意をユーザーに要求します。
- **Apple Pay**： iOS 8.0 以降のデバイスに Apple Pay を設定します。
- **Siri**： デバイスで Siri を使用するかどうかを選択します。
- **App Analytics**： クラッシュデータおよび使用状況の統計情報を Apple と共有するかどうかを設定します。
- ディスプレイズーム： iOS 8.0 以降のデバイスにディスプレイ解像度（標準またはズーム）を設定します。
- **True Tone**： iOS 10.0 デバイス（最小バージョン）に True Tone ディスプレイを設定します。
- ホームボタン： iOS 10.0 デバイス（最小バージョン）に、ホームボタンの画面の感度を設定します。
- 新機能のハイライト： iOS 11.0 デバイス（最小バージョン）で、配布準備情報画面、[Access the Dock from Anywhere］および［Switch Between Recent Apps］を設定します。
- プライバシー： DEP デバイスの設定中に、［データおよびプライバシー］ペインがユーザーにを表示されないようにします。iOS 11.3 以降の場合。
- 外観： DEP デバイスの設定中にユーザーが［Choose Your Look］画面を表示できないようにします。

iOS 12.0 以降の場合。

- ソフトウェアの更新： DEP デバイスのセットアップ中に必須ソフトウェアの更新画面が表示されないようにします。iOS 12.0 以降の場合。
- スクリーンタイム： DEP デバイスのセットアップ中にスクリーンタイム画面が表示されないようにします。iOS 12.0 以降の場合。
- **SIM Setup**： DEP デバイスのセットアップ中に［Add Cellular Plan］画面が表示されないようにします。iOS 12.0 以降の場合。
- **iMessage & FaceTime**： DEP デバイスのセットアップ中に iMessage と FaceTime の画面が表示されないようにします。iOS 12.0 以降の場合。

DEP アカウントを表示するには、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ に移動します。

1. ［**macOS** セットアップアシスタントオプション］ で、ユーザーが初めてデバイスを起動するときにスキップする macOS セットアップアシスタントの手順を選択します。すべての項目は、デフォルトで選択が解除されています。



- 新規としてセットアップまたは復元： 新規に、または iCloud か iTunes のバックアップからデバイスを設定します。
- 位置情報サービス： デバイスに位置情報サービスを設定します。
- **Apple ID**： デバイスの Apple ID アカウントを設定します。
- 使用条件： デバイスの使用契約条件に対する同意をユーザーに要求します。
- **Siri**： デバイスで Siri を使用するかどうかを選択します。

- **FileVault**：FileVault を使用して起動ディスクを暗号化します。XenMobile が FileVault の設定を適用するのは、ローカルユーザーアカウントがシステムに 1 つで、そのアカウントが iCloud にサインインしている場合のみです。

  macOS の FileVault ディスク暗号化機能を使ってコンテンツを暗号化し、システムボリュームを保護します（https://support.apple.com/en-us/HT204837）。FileVault がオンになっていない旧モデルのポータブル Mac でセットアップアシスタントを実行すると、この機能を有効にするように求められることがあります。このプロンプトは、新しいシステムと OS X 10.10 または 10.11 にアップグレードされたシステムの両方に表示されますが、システムのローカル管理者アカウントが 1 つで、そのアカウントが iCloud にサインインしている場合にのみ表示されます。

- **App Analytics**： クラッシュデータおよび使用状況の統計情報を Apple と共有するかどうかを設定します。

- 登録： ユーザーにデバイスの登録を要求します。

  登録情報の設定は、OS X 10.9 で利用可能でした。登録プロセスを使用して、システムの登録情報を Apple に送信することができました。この情報によってユーザーの連絡先情報と Mac のハードウェアが関連付けられたのです。Apple では主に、この情報を AppleCare のサポートに役立てるために使用していました。以前に Apple ID を入力した場合は、セットアップアシスタントによって、必要に応じて、Apple ID アカウントに基づいて登録が送信されています。Apple ID を入力しなかった場合は、連絡先情報を手動で入力することができました。

  ［ローカルアカウントのセットアップオプション］ で、macOS に必要な管理者アカウントを作成するための設定を指定します。XenMobile は、指定された情報を使用してアカウントを作成します。

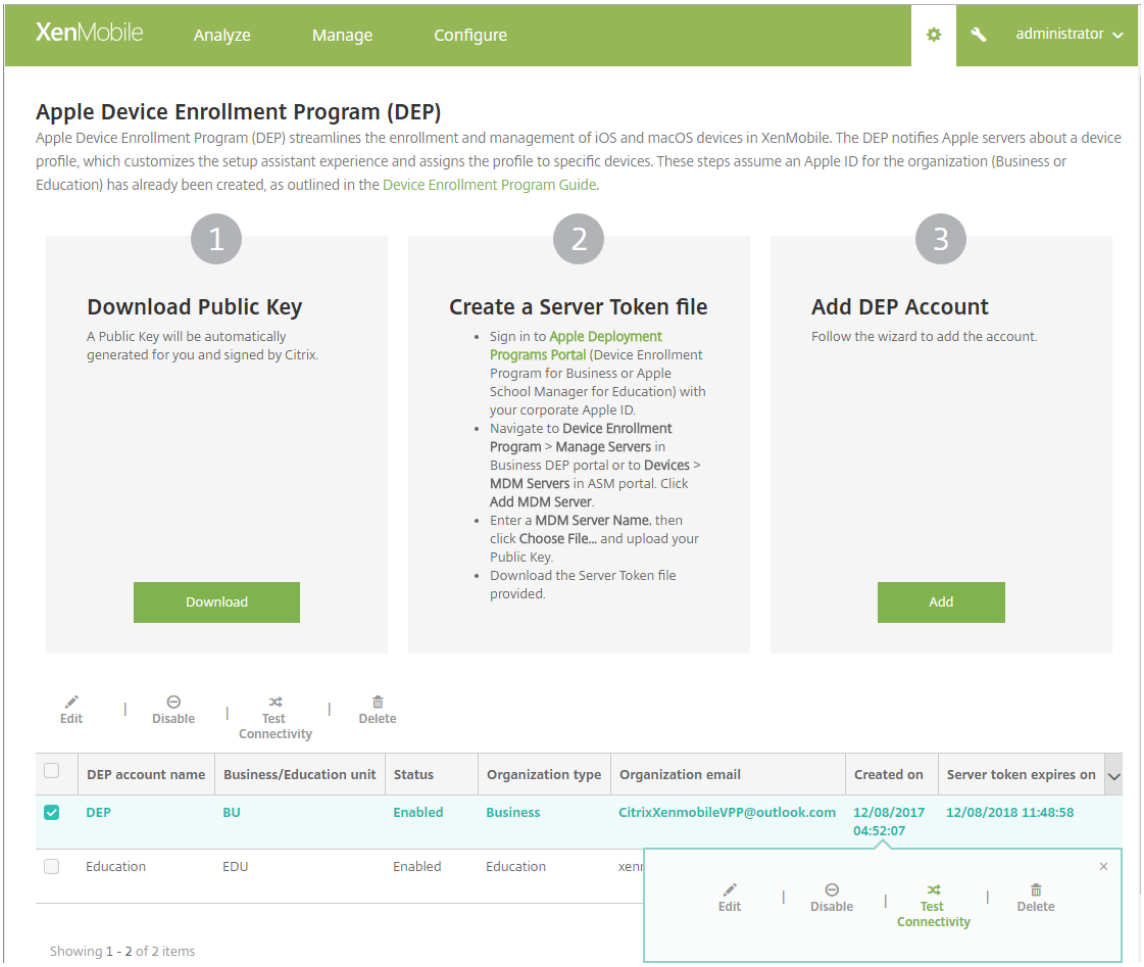
- プライバシー： DEP デバイスの設定中に、［データおよびプライバシー］ペインがユーザーに表示されないようにします。macOS 10.13 以降の場合。

- **iCloud Analytics**： DEP デバイスの設定中に、iCloud Analytics 画面がユーザーに表示されないようにします。macOS 10.13 以降の場合。

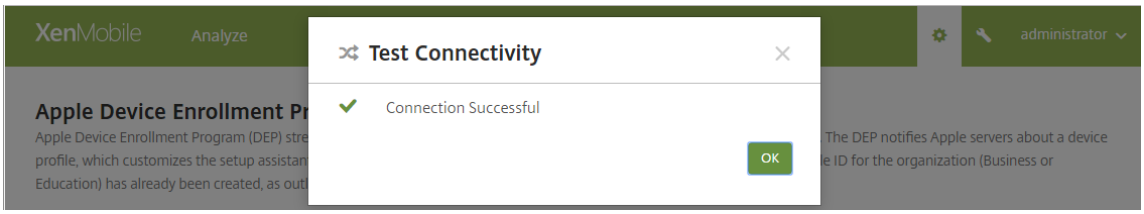
- **iCloud** の書類とデスクトップ： DEP デバイスの設定中に、iCloud の書類とデスクトップ画面がユーザーに表示されないようにします。macOS 10.13 以降の場合。

- 外観： DEP デバイスの設定中にユーザーが［Choose Your Look］画面を表示できないようにします。macOS 10.14 以降の場合。

2. XenMobile Server と Apple 間の接続をテストするには、アカウントを選択して ［接続性をテスト］ をクリックします。



状態を示すメッセージが表示されます。



DEP アカウント用のデバイスポリシーの展開規則およびアプリの構成

[設定] > [デバイスポリシー] および [設定] > [アプリ] の [展開規則] セクションから、DEP アカウントをさまざまなデバイスポリシーとアプリに関連付けることができます。ポリシーまたはアプリを次のいずれかの方法で指定できます。

- 特定の Apple DEP アカウントに対してのみ展開する。
- 選択したものを除くすべての Apple DEP アカウントに展開する。

DEP アカウントの一覧には、ステータスが有効または無効のアカウントのみが含まれます。DEP アカウントが無効の場合、DEP デバイスはこのアカウントに属しません。このため、XenMobile ではこれらのデバイスにアプリまた

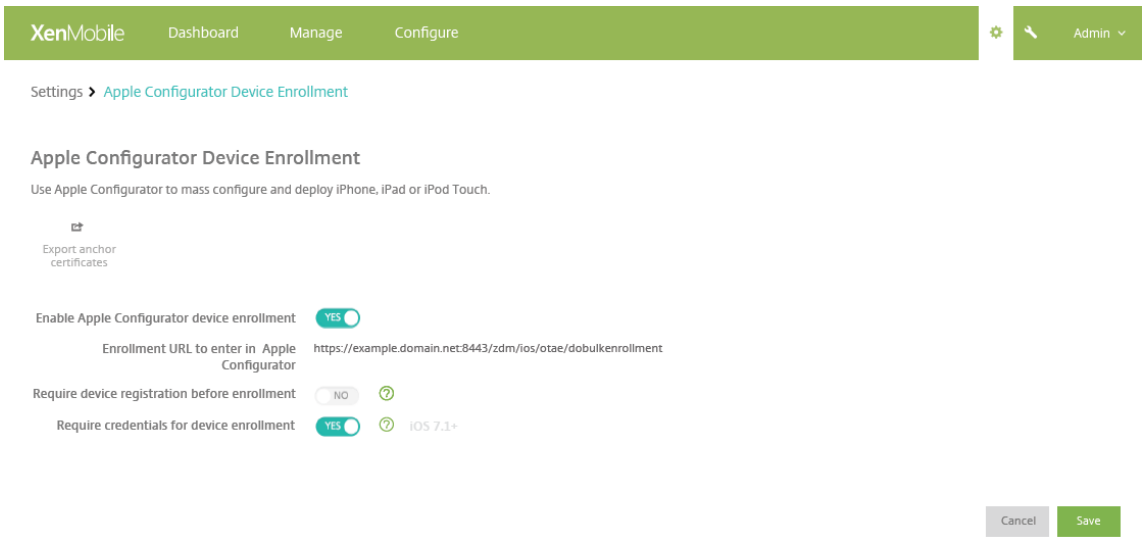
はポリシーが展開されません。

以下の例では、デバイスポリシーを、Apple DEP アカウント名が「DEP Account NR」に設定されているデバイスのみに展開するように構成しています。

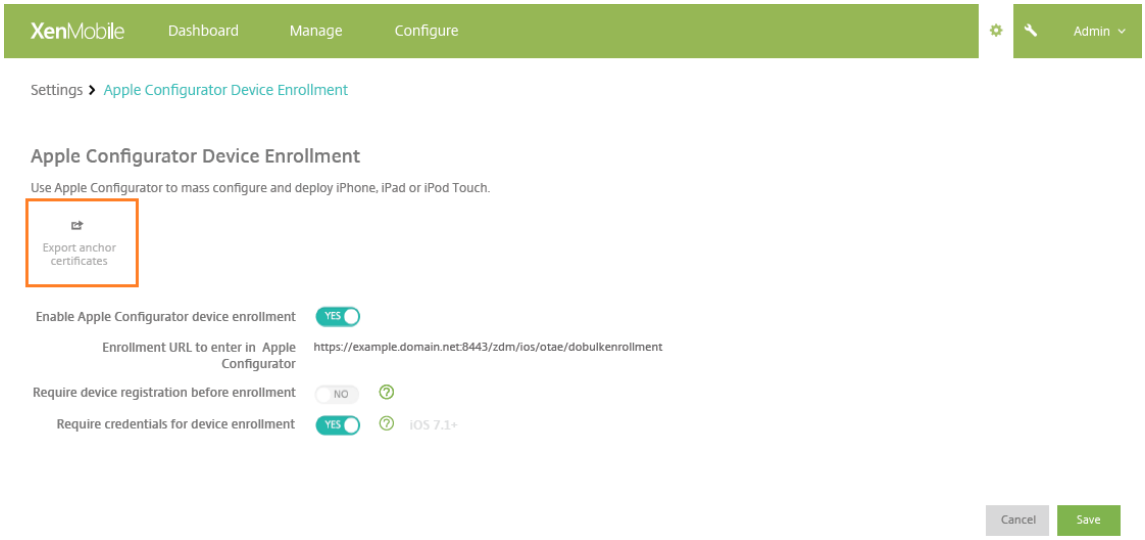
```
1 ![Apple DEP設定画面の画像](/ja-jp/xenmobile/server/media/apple-dep-deployment-rule-policy-example.png)
```

Apple Configurator 設定の構成

1. XenMobile コンソールで、［設定］>［**Apple Configurator** デバイス登録］ の順に選択します。



2. ［**Apple Configurator** デバイス登録を有効にする］ を ［はい］ に設定します。
3. ［**Apple Configurator** で入力する登録 **URL**］ は、読み取り専用のフィールドです。これは XenMobile サーバーが Apple との通信に使用する URL です。手順の後半で、この URL をコピーして Apple Configurator に貼り付けます。Apple Configurator 2 の場合、登録用 URL は、XenMobile サーバーの完全修飾ドメイン名（FQDN。`mdm.server.url.com`など）または IP アドレスです。
4. 認識のないデバイスが登録されないようにするには、［登録前にデバイスの登録が必要です］ を ［はい］ に設定します。注: この設定が ［はい］ の場合、登録前に XenMobile の ［管理］>［デバイス］ から手動で行うか、CSV ファイルを使用して、設定済みのデバイスを追加する必要があります。
5. iOS デバイスのユーザーに対して、登録時に資格情報の入力を要求するには、［デバイス登録のための資格情報を求める］ を ［はい］ に設定します。デフォルトでは資格情報は不要です。
6. 注: XenMobile サーバーで信頼済みの SSL 証明書を使用する場合は、この手順はスキップしてください。［アンカー証明書のエクスポート］ をクリックして、certchain.pem ファイルを macOS キーチェーン（ログインまたはシステム）に保存します。



7. Apple Configurator を開始して ［**Prepare**］ **>** ［**Setu**］ **>** ［**Configure Settings**］ の順に選択します。
8. Configurator の ［**Device Enrollment**］ 設定の ［**MDM server URL**］ ボックスに、手順 4 の MDM サーバー URL を貼り付けます。
9. XenMobile で信頼済みの SSL 証明書を使用しない場合は、［**Device Enrollment**］設定の［**Anchor**］証明書にルート証明機関および SSL サーバー証明機関をコピーします。
10. Dock コネクタ USB ケーブルを使用して、最大で 30 台のデバイスを同時に Apple Configurator が動作する Mac に接続して構成します。Dock コネクタがない場合は、1 台または複数の Powered USB 2.0 高速ハブを使用してデバイスを接続します。
11. ［**Prepare**］ をクリックします。Apple Configurator を使用したデバイスの準備について詳しくは、Apple Configurator のヘルプページ「デバイスを準備する」を参照してください。
12. Apple Configurator で、必要なデバイスポリシーを構成します。
13. 準備ができたデバイスから電源を入れて iOS 設定アシスタントを開始し、初回使用のためにデバイスを準備します。

Apple DEP を使用しているときに証明書を更新するには

XenMobile Secure Sockets Layer（SSL）証明書が更新されたら、XenMobile コンソールで ［設定］ **>** ［証明書］ の順に選択し、新しい証明書をアップロードします。［インポート］ ダイアログボックスの ［使用目的］ で、［**SSL** リスナー］ をクリックして証明書が SSL に使用されるようにします。サーバーを再起動すると、新しい SSL 証明書が使用されるようになります。XenMobile の証明書について詳しくは、「XenMobile での証明書のアップロード」を参照してください。

SSL 証明書を更新するときに、Apple DEP と XenMobile の間の信頼関係を再構築する必要はありません。ただし、この記事の上記の手順に従って、いつでも DEP 設定を再構成できます。

Apple DEP について詳しくは、Apple のドキュメントを参照してください。

Apple Configurator を使用して **iOS** デバイスを **Supervised** モードにするには

> 重要:
>
> デバイスを Supervised モードにすると、特定のバージョンの iOS がデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリケーションがデバイスから完全に消去されます。

1. iTunesから Apple Configurator をインストールします。
2. iOS デバイスを Apple コンピューターに接続します。
3. Apple Configurator を起動します。監視の準備が整っているデバイスがあることが Configurator に表示されます。
4. デバイスの監視の準備を行うには:
   - [**Supervision control**] を [**On**] に設定します。構成を定期的に再適用することによってデバイスを管理する場合は、この設定を選択することをお勧めします。
   - 必要に応じてデバイスの名前を指定します。
   - 最新バージョンの iOS をインストールする場合、[iOS] ボックスの一覧で [**Latest**] を選択します。
5. デバイスの監視の準備が整ったら、[準備] をクリックします。

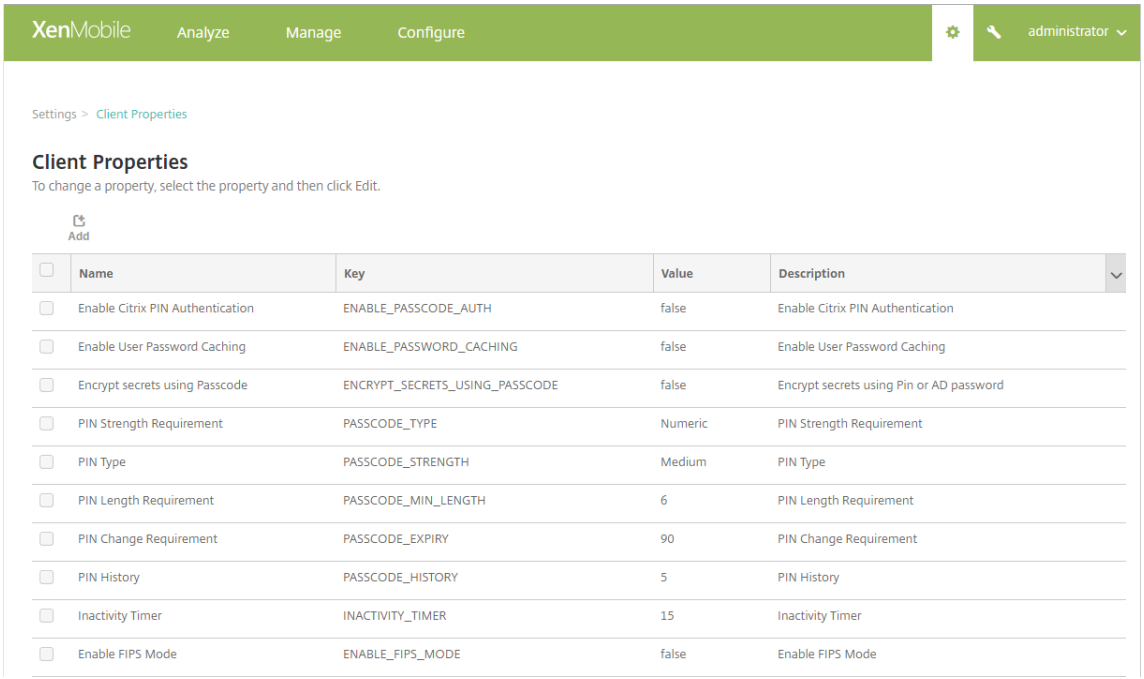
クライアントプロパティ

January 10, 2020

クライアントプロパティには、ユーザーのデバイスの Secure Hub に直接提供される情報が含まれています。これらのプロパティを使用して、Citrix PIN などの詳細設定を構成することができます。クライアントプロパティは Citrix サポートから取得します。

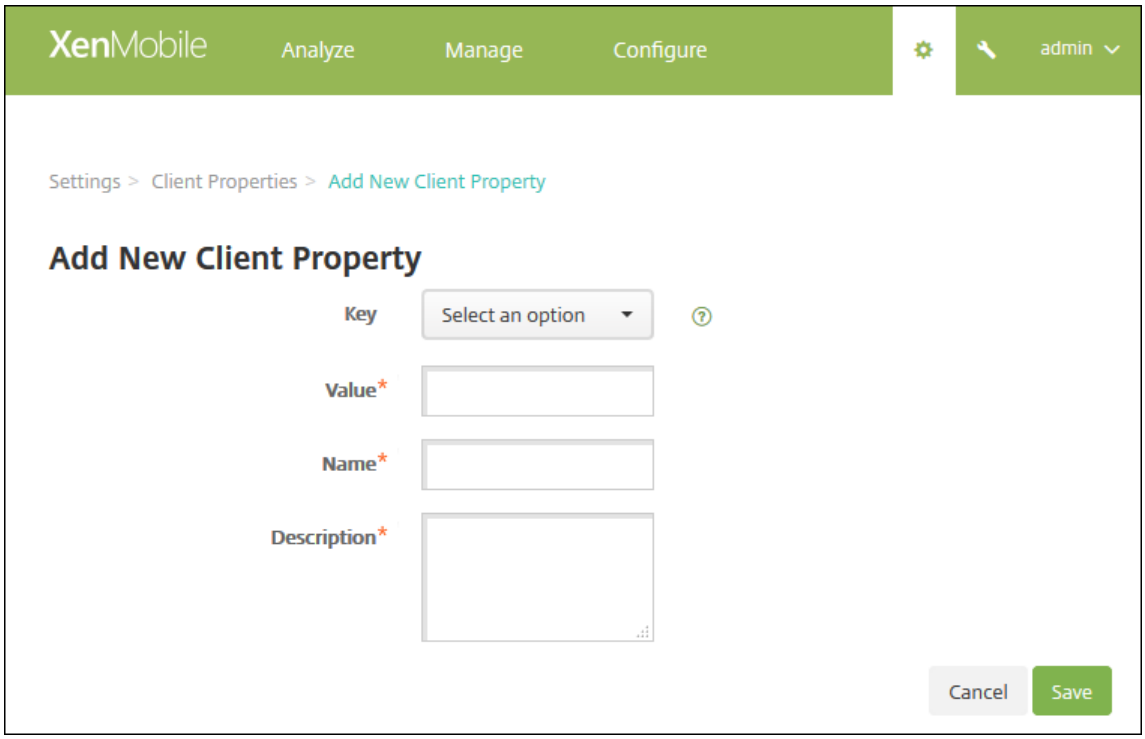
クライアントプロパティは、Secure Hub のリリースごとに変更されるほか、クライアントアプリのリリースで変更されることもあります。一般的に構成されたクライアントプロパティについて詳しくは、「クライアントプロパティリファレンス」を参照してください。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [クライアント] の下の [クライアントプロパティ] をクリックします。[クライアントプロパティ] ページが開きます。このページでは、クライアントプロパティを追加、編集、または削除できます。



クライアントプロパティを追加するには

1. [追加] をクリックします。 [新しいクライアントプロパティの追加] ページが開きます。



2. 次の設定を構成します。

- キー: 一覧から、追加するプロパティキーを選択します。重要: 設定を更新する前に、シトリックスサポートにご連絡ください。特殊キーを要求できます。
- 値: 選択したプロパティの値です。
- 名前: プロパティの名前です。
- 説明: プロパティの説明です。

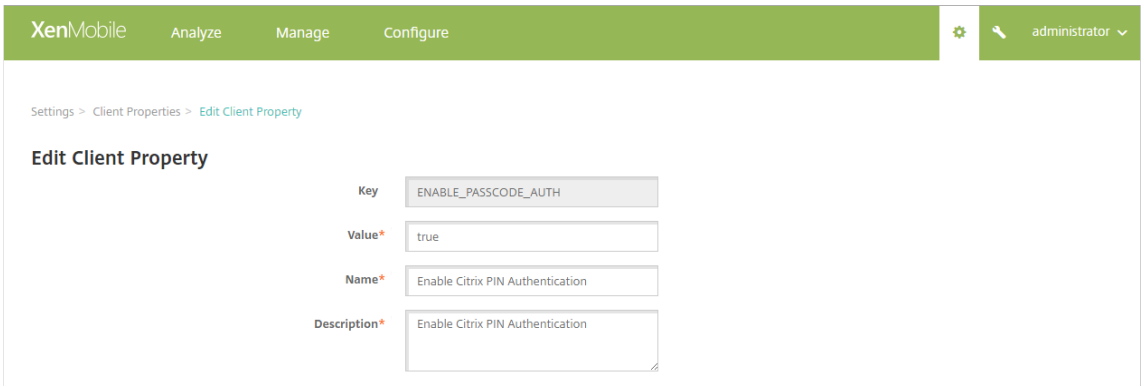
3. [保存] をクリックします。

クライアントプロパティを編集するには

1. [クライアントプロパティ] の表で、編集するクライアントプロパティを選択します。

   クライアントプロパティの横にあるチェックボックスをオンにすると、クライアントプロパティ一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

2. [編集] をクリックします。[クライアントプロパティの編集] ページが開きます。



3. 必要に応じて以下の情報を変更します。

   - キー: このフィールドは変更できません。
   - 値: プロパティの値です。
   - 名前: プロパティの名前です。
   - 説明: プロパティの説明です。

4. [保存] をクリックして変更を保存するか、[キャンセル] をクリックしてプロパティを変更せずそのままにします。

クライアントプロパティを削除するには

1. [**Client Properties**] の表で、削除するクライアントプロパティを選択します。

   各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。

2. [削除] をクリックします。確認ダイアログボックスが開きます。もう一度 [削除] をクリックします。

クライアントプロパティリファレンス

次に、XenMobile の定義済みクライアントプロパティとそのデフォルトの設定を示します。

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 表示名：MDX Container Self Destruct Period
  - 非アクティブな状態で指定の日数を経過すると、自動削除機能により、Secure Hub および管理対象アプリにアクセスできなくなります。指定の期間を過ぎると、アプリを使用できなくなります。データのワイプでは、各インストール済みアプリのアプリデータ（アプリキャッシュ、ユーザーデータなど）が消去されます。

    非アクティブ状態とは、サーバーが一定期間、ユーザーの検証をするための認証要求を受け取っていない状態です。たとえば、このプロパティを 30 日に設定した場合、ユーザーがアプリを 30 日を超えて使用しない状況が続くと、このポリシーが適用されます。

    このグローバルセキュリティポリシーは、既存のアプリのロックポリシーおよびワイプポリシーの機能拡張であり、iOS および Android のプラットフォームに適用されます。
  - このグローバルポリシーを構成するには、［設定］**>**［クライアントプロパティ］ の順に選択し、カスタムキー **CONTAINER_SELF_DESTRUCT_PERIOD** を追加します。
  - 値：日数
- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - 表示名：Send device logs to IT help desk
  - このプロパティで、IT ヘルプデスクへのログ送信機能を有効または無効にします。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**
- **DISABLE_LOGGING**
  - 表示名：Disable Logging
  - このプロパティを使用して、ユーザーが各自のデバイスからログを収集してアップロードすることを防ぎます。このプロパティで、Secure Hub およびすべてのインストール済み MDX アプリのログを無効にします。ユーザーが［サポート］ページから任意のアプリのログを送信することはできません。メール作成ダイアログボックスは開きますが、ログは添付されません。ログが無効になっているというメッセージが表示されます。またこの設定は、XenMobile コンソールで Secure Hub と MDX アプリのログ設定が更新されるのを防ぎます。

    このプロパティを **true** に設定すると、Secure Hub によって ［アプリケーションログのブロック］ が **true** に設定されます。これによって、新しいポリシーが適用されたときに MDX アプリのログが停止します。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**（ロギングは有効です）

- **ENABLE_CRASH_REPORTING**
  - 表示名: Enable Crash Reporting
  - **true** の場合、Secure Hub for iOS および Android での問題のトラブルシューティングを目的として、シトリックスによりクラッシュレポートと診断情報が収集されます。**false** の場合、データは収集されません。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **true**
- **ENABLE_CREDENTIAL_STORE**
  - 表示名: Enable Credential Store
  - 資格情報ストアを有効にすると、Android および iOS のユーザーは、業務用モバイルアプリにアクセスする場合にパスワードを１度入力するだけで済むようになります。Citrix PIN を有効にするかどうかに関係なく、資格情報ストアを使用できます。Citrix PIN を有効にしないと、ユーザーは Active Directory のパスワードを入力します。XenMobile が認証情報ストアで Active Directory のパスワードの使用をサポートしているのは、Secure Hub とパブリックストアアプリに対してのみです。資格情報ストアで Active Directory のパスワードを使用する場合、XenMobile では PKI 認証はサポートされていません。
  - Secure Mail での自動登録では、このプロパティを **true** に設定する必要があります。
  - このカスタムクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］ の順に選択し、カスタムキー **ENABLE_CREDENTIAL_STORE** を追加して、［値］ を **true** に設定します。
- **ENABLE_FIPS_MODE**
  - 表示名: Enable FIPS Mode
  - このプロパティでは、モバイルデバイスで FIPS モードを有効または無効にします。値を変更すると、Secure Hub は、次のオンライン認証のときに新しい値をデバイスに送信します。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false**
- **ENABLE_NETWORK_EXTENSION**
  - 表示名: ENABLE_NETWORK_EXTENSION
  - Secure Hub がインストールされると、XenMobile はデフォルトで Apple Network Extension フレームワークを有効にします。Network Extension を無効にするには、［設定］**>**［クライアントプロパティ］でカスタムキー **ENABLE_NETWORK_EXTENSION** を追加し、［値］を **false** に設定します。
  - デフォルト値: **true**
- **ENABLE_PASSCODE_AUTH**
  - 表示名: Enable Citrix PIN Authentication
  - このプロパティを使用すると、Citrix PIN 機能を有効にできます。ユーザーは、Citrix PIN またはパスコードにより、Active Directory パスワードの代わりに使用する PIN を定義するように求められます。

ENABLE_PASSWORD_CACHING が有効になっているとき、または XenMobile で証明書認証を使用しているときは、この設定が自動的に有効になります。

オフライン認証では、Citrix PIN がローカルで検証されて、要求したアプリやコンテンツへのアクセスがユーザーに許可されます。オンライン認証では、Citrix PIN またはパスコードによって Active Directory パスワードまたは証明書がロック解除されて、XenMobile との認証を実行するために送信されます。

ENABLE_PASSCODE_AUTH が true で ENABLE_PASSWORD_CACHING が false の場合、Secure Hub でパスワードが保存されないため、オンライン認証では常にパスワードの入力が求められます。

- 設定可能な値: **true** または **false**
- デフォルト値: **false**

- **ENABLE_PASSWORD_CACHING**
  - 表示名: Enable User Password Caching
  - このプロパティによって、Active Directory パスワードをモバイルデバイス上にローカルにキャッシュできます。このプロパティを **true** に設定する場合、**ENABLE_PASSCODE_AUTH** プロパティを **true** に設定する必要があります。ユーザーパスワードのキャッシュを有効にすると、ユーザーは Citrix PIN またはパスコードを設定するよう求められます。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - 表示名: Enable Touch ID Authentication
  - Touch ID 認証をサポートするデバイスの場合、このプロパティでデバイスの Touch ID 認証を有効または無効にします。要件

    ユーザーデバイスでは、Citrix PIN または LDAP を有効にする必要があります。LDAP 認証がオフの場合（証明書による認証が使用されている場合など）、ユーザーは Citrix PIN を設定する必要があります。この場合、クライアントプロパティの **ENABLE_PASSCODE_AUTH** が **false** であっても、XenMobile に Citrix PIN が必要になります。

    ENABLE_PASSCODE_AUTH を **false** に設定します。これによって、ユーザーがアプリを起動したとき、Touch ID の使用を促すメッセージが表示されます。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false**
- **ENABLE_WORXHOME_CEIP**
  - 表示名: Enable Worx Home CEIP
  - このプロパティにより、カスタマーエクスペリエンス向上プログラムがオンになります。この機能により、構成および使用データが定期的に、匿名で Citrix に送信されます。このデータは、XenMobile の品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。

- 値：**true** または **false**
- デフォルト値：**false**

- **ENABLE_WORXHOME_GA**
  - 表示名：Enable Google Analytics in Worx Home
  - このプロパティでは、Secure Hub の Google Analytics を使用したデータ収集機能を有効または無効にします。この設定を変更した場合、ユーザーが次回 Secure Hub（以前の名称は Worx Home）にログオンすると初めて新しい値が設定されます。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**true**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 表示名：Encrypt secrets using Passcode
  - このプロパティでは、機密データをプラットフォームベースのネイティブな格納場所（iOS キーチェーンなど）ではなく、デバイスの Secret Vault に格納します。このプロパティにより、重要なデータの強力な暗号化が可能になるとともにユーザーエントロピーが追加されます。ユーザーエントロピーは、ユーザーが生成した、ユーザーしか知らないランダムな PIN コードです。

    ユーザーデバイスのセキュリティを強化するために、このプロパティを有効にすることをお勧めします。これによって、Citrix PIN の認証メッセージが増えます。
  - 設定可能な値：**true** または **false**
  - デフォルト値：**false**

- **INACTIVITY_TIMER**
  - 表示名：Inactivity Timer
  - このプロパティで、ユーザーがデバイスを非アクティブにした後で、Citrix PIN またはパスコードの入力を求められずにアプリにアクセスできる時間を定義します。MDX アプリでこの設定を有効にするには、［アプリのパスコード］設定を［オン］に設定します。［アプリのパスコード］設定を［オフ］に設定すると、ユーザーは完全認証を実行するよう Secure Hub にリダイレクトされます。この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。

    iOS では、Inactivity Timer は MDX アプリと MDX 以外のアプリの Secure Hub へのアクセスにも対応します。
  - 設定可能な値：正の整数
  - デフォルト値：**15**（分）

- **ON_FAILURE_USE_EMAIL**
  - 表示名：On failure Use Email to Send device logs to IT help desk
  - このプロパティで、メールを使用して IT にデバイスログを送信する機能を有効または無効にします。
  - 設定可能な値：**true** または **false**

  - デフォルト値: **true**

- **PASSCODE_EXPIRY**
  - 表示名: PIN Change Requirement
  - このプロパティで、Citrix PIN またはパスコードが有効な期間を定義します。この期間を過ぎると、ユーザーは Citrix PIN またはパスコードを変更する必要があります。この設定を変更すると、現在の Citrix PIN またはパスコードの有効期限が切れた場合のみ、新しい値が設定されます。
  - 設定可能な値: **1** から **99** までの間を推奨。PIN をリセットする必要がないようにするためには、大きな値に設定してください（例: 100,000,000,000）。有効期限を 1 から 99 日の間で設定し、その期間中に大きな値に変更した場合、PIN は最初に設定した期間の最終日に満期になり、満期がその後に設定されることはありません。
  - デフォルト値: **90**（日）

- **PASSCODE_HISTORY**
  - 表示名: PIN History
  - このプロパティでは、使用済みであり、Citrix PIN またはパスコードの変更時にユーザーが再使用できない Citrix PIN またはパスコードの個数を定義します。この設定を変更すると、ユーザーが Citrix PIN またはパスコードを次回再設定したときに新しい値が設定されます。
  - 設定可能な値: **1** から **99** までの間
  - デフォルト値: **5**

- **PASSCODE_MAX_ATTEMPTS**
  - 表示名: PIN Attempts
  - このプロパティで、完全認証が必要になる前に、ユーザーが誤った Citrix PIN またはパスコードを入力できる回数を定義します。完全認証に成功した後で、ユーザーは Citrix PIN またはパスコードを作成するように求められます。
  - 設定可能な値: 正の整数
  - デフォルト値: **15**

- **PASSCODE_MIN_LENGTH**
  - 表示名: PIN Length Requirement
  - このプロパティは、Citrix PIN の最小文字数を定義します。
  - 設定可能な値: **4** ～ **10**
  - デフォルト値: **6**

- **PASSCODE_STRENGTH**
  - 表示名: PIN Strength Requirement
  - このプロパティで、Citrix PIN またはパスコードの強度を定義します。この設定を変更すると、ユーザーは、次回認証を求められたときに、Citrix PIN またはパスコードを作成するように求められます。
  - 設定可能な値: **Low**、**Medium**、または **Strong**
  - デフォルト値: **Medium**

- PASSCODE_TYPE 設定に基づいた、各強度設定のパスワード規則は次のとおりです。

数字パスコードの規則は以下のとおりです。

パスコードの強度	数字パスコードの規則	許可	許可しない
低	すべての数字を任意の順序で使用できます。	444444、123456、654321	
Medium（デフォルト設定）	すべての番号を同じにしたり連番にしたりすることはできません。	444333、124567、136790、555556、788888	444444、123456、654321
高	パスコード強度「Medium」と同じです。		
強	パスコード強度「Medium」と同じです。		

英数字パスコードの規則は以下のとおりです。

パスコードの強度	英数字パスコードの規則	許可	許可しない
低	1 つ以上の数字と 1 つ以上の文字が含まれている必要があります。	aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa	AAAaaa、aaaaaa、abcdef
Medium（デフォルト設定）	パスコード強度「低」の規則に加えて、文字およびすべての数字を同じにすることはできません。連続した文字および連続した数字は使用できません。	aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1 #、Ab123~	aaaa11、aa11aa、または aaa111; abcd12、bcd123、123abc、xy1234、xyz345、または cba123
高	1 つ以上の大文字、および 1 つ以上の小文字を含めます。	Abcd12、jkrtA2、23Bc#、AbCd	abcd12、DFGH2
強	1 つ以上の数字、1 つ以上の特殊記号、1 つ以上の大文字、および 1 つ以上の小文字を含めます。	Abcd1 #、Ab123~、xY12 # 3、Car12 #、AAbc1 #	abcd12、Abcd12、dfgh12、jkrtA2

- **PASSCODE_TYPE**

- 表示名：PIN Type
- このプロパティで、数字の Citrix PIN または英数字パスコードのいずれをユーザーが定義できるようにするのかを定義します。［**Numeric**］を選択した場合、ユーザーは数字のみを使用できます（Citrix PIN）。［**Alphanumeric**］ を選択した場合、ユーザーは文字と数字の組み合わせを使用できます（パスコード）。

  この設定を変更すると、ユーザーは、次回認証を求められたときに、新しい Citrix PIN またはパスコードを設定する必要があります。
- 設定可能な値：**Numeric** または **Alphanumeric**
- デフォルト値：**Numeric**

• **REFRESHINTERVAL**

- 表示名：REFRESHINTERVAL
- デフォルトで、XenMobile は Auto Discovery Server（ADS）のピンニングされた証明書に対して 3 日ごとに ping を実行します。更新時間を変更するには、［設定］**>**［クライアントプロパティ］でカスタムキー **REFRESHINTERVAL** を追加して、［値］ を時間数に設定します。
- デフォルト値：**72** 時間（3 日）

• **SEND_LDAP_ATTRIBUTES**

- Android、iOS、または macOS デバイスの MAM-only 展開の場合、XenMobile を、電子メール資格情報で Secure Hub に登録するユーザーが Secure Mail に自動的に登録されるように構成します。これにより、ユーザーが追加の情報を入力したり、Secure Mail に登録するための追加の手順を実行する手間が省かれます。
- このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］ の順に選択し、カスタムキー **SEND_LDAP_ATTRIBUTES** を追加して、［値］ を以下のように設定します。
- の値: `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`
- MDM ポリシーと同様、属性値はマクロとして指定されます。
- このプロパティのアカウントサービスレスポンスのサンプルを以下に示します。

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com" name="SEND_LDAP_ATTRIBUTES"/>
  ```
- このプロパティでは、XenMobile はコンマ文字を文字列の終わりとして扱います。そのため、属性値にコンマが含まれる場合は、コンマの前にバックスラッシュを置きます。バックスラッシュは、含まれているコンマがクライアントによって属性値の末尾と解釈されるのを防ぎます。バックスラッシュ文字は「`"\\"`」と表します。

- **HIDE_THREE_FINGER_TAP_MENU**
  - このプロパティが設定されていないか、または **false** に設定されている場合、ユーザーはデバイスで 3 本指タップすることで隠し機能メニューにアクセスできます。隠し機能メニューによって、アプリケーションデータをリセットできます。このプロパティを **true** に設定すると、ユーザーは隠し機能メニューにアクセスできなくなります。
  - このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］ の順に選択し、カスタムキー **HIDE_THREE_FINGER_TAP_MENU** を追加して、［値］ を設定します。
- **TUNNEL_EXCLUDE_DOMAINS**
  - 表示名：Tunnel Exclude Domains
  - デフォルトで、MDX は、XenMobile SDK およびアプリが各種機能で使用する一部のサービスエンドポイントを、Micro VPN トンネルから除外します。たとえば、このようなエンドポイントには、社内ネットワークを経由する必要がない、Google Analytics、Citrix Cloud サービス、Active Directory サービスなどのサービスが含まれます。このクライアントプロパティを使用して、除外対象ドメインのデフォルトの一覧を上書きします。
  - このグローバルクライアントポリシーを構成するには、［設定］**>**［クライアントプロパティ］ の順に選択し、カスタムキー **TUNNEL_EXCLUDE_DOMAINS** を追加して、［値］を設定します。
  - 値：デフォルトの一覧をトンネルから除外するドメインで置き換えるには、ドメインサフィックスのコンマ区切りの一覧を入力します。すべてのドメインをトンネルに含めるには、「**none**」と入力します。デフォルトは次のとおりです。

    ```
    app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test
    .citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.
    launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net
    ,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf
    -staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,
    stream.launchdarkly.com
    ```

Apple DEP を介した iOS と macOS デバイスの展開

January 10, 2020

Apple では、ビジネスおよび教育機関アカウント向けのデバイス登録プログラムが提供されています。ビジネス用アカウントの場合、デバイスを XenMobile で登録して管理するには、Apple Deployment Program に登録して、Apple の DEP（Device Enrollment Program：デバイス登録プログラム）を利用する必要があります。これは、iOS および macOS デバイス向けのプログラムです。ビジネス向け Apple Deployment Program への申し込みの詳細は、Apple のこのPDFを参照してください。

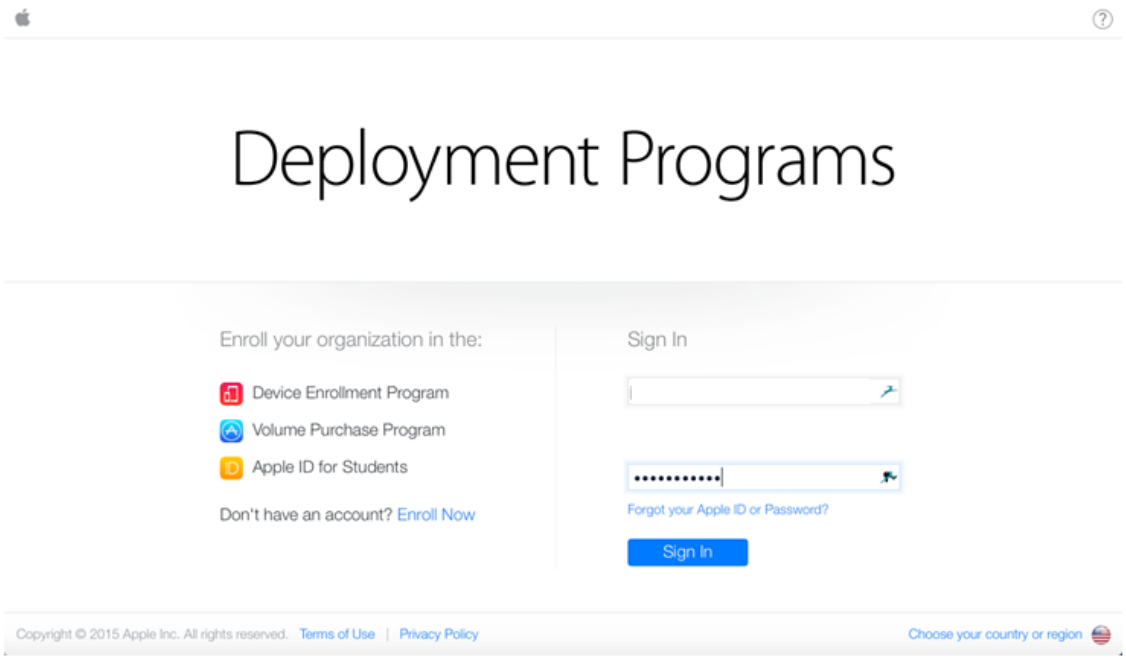
Apple Deployment Program は、団体の利用は可能ですが、個人では利用できないことにご注意ください。Apple Deployment Program アカウントを作成するには、相当量の企業の詳細と情報を提供する必要があります。そのため、アカウントの要求と承認の取得には時間がかかる場合があります。

教育機関アカウントの場合は、Apple School Manager アカウントを作成します。Apple School Manager では、デバイス登録プログラム(DEP)と Volume Purchase Program(VPP)が統合されています。Apple School Manager は、教育向け DEP の一種です。Apple School Manager アカウントを作成するには、https://school.apple.com/にアクセスします。

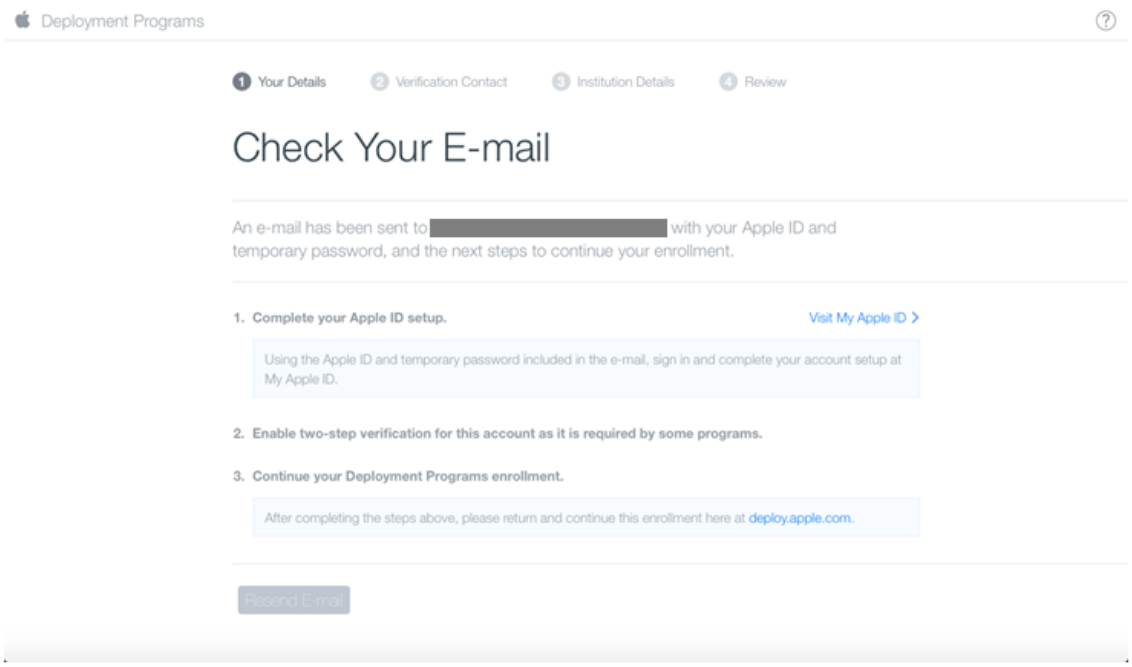
Apple Deployment Program への登録

1. deploy.apple.comにアクセスして、Apple Deployment Program アカウントを申し込みます。DEP アカウントを申し込む場合、ベストプラクティスは dep@company.com などの、組織のメールアドレスを使うことです。

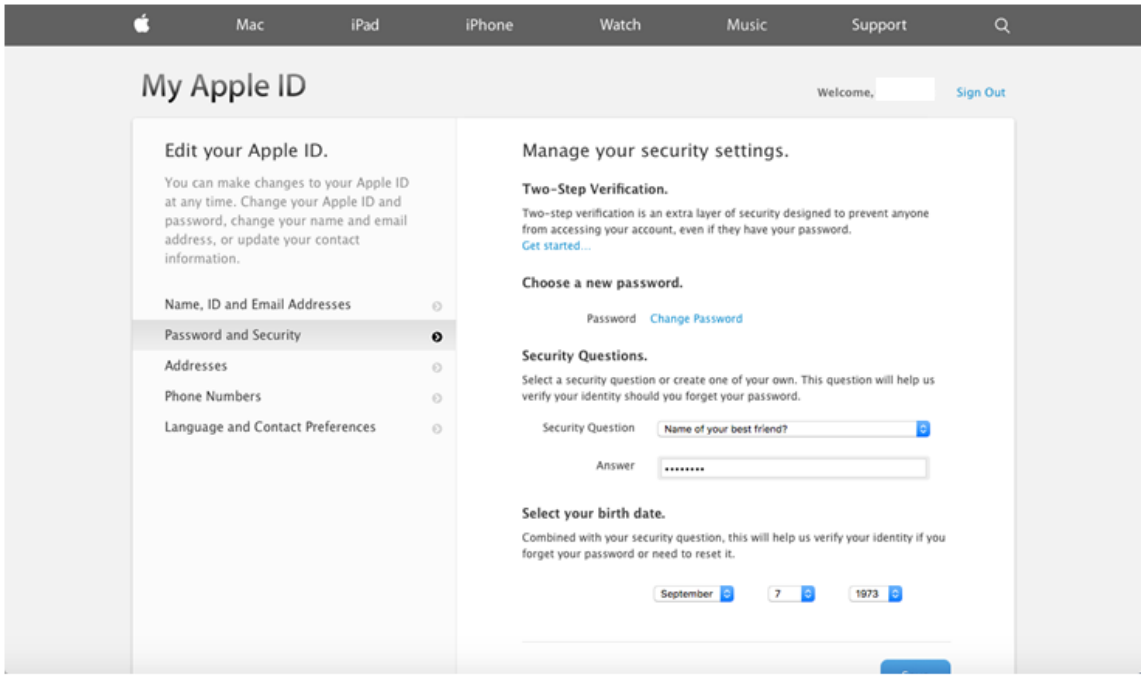
   > 注:
   >
   > 教育機関アカウントについては、https://school.apple.com/を参照してください。



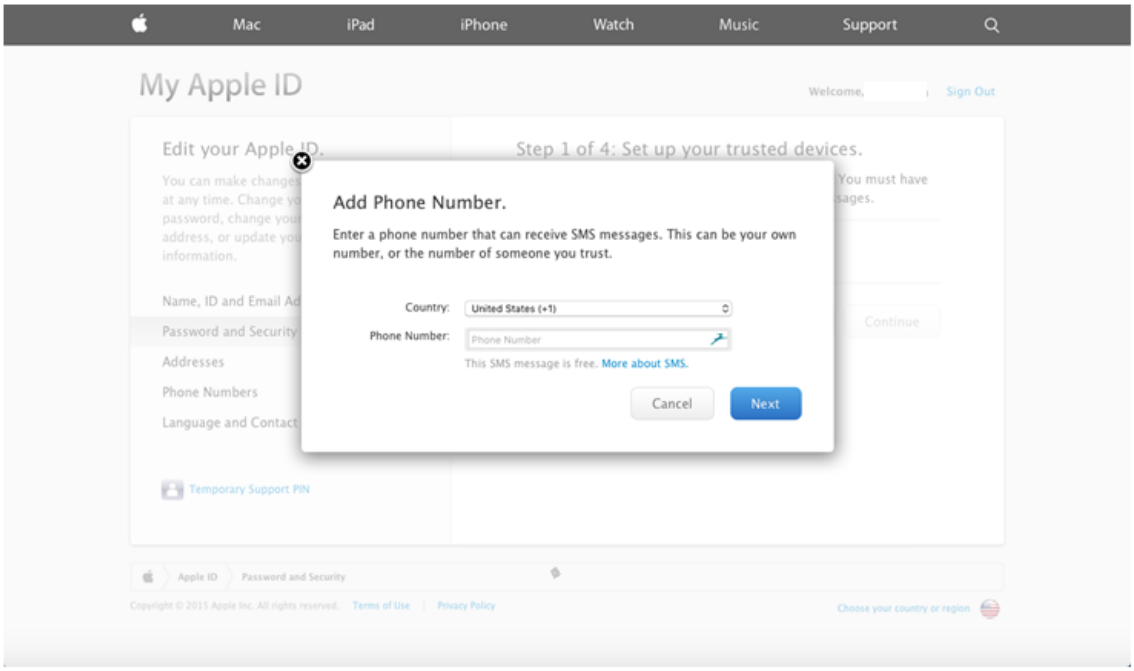
2. 組織に関する情報を入力した後、メールで新しい Apple ID の一時パスワードを受け取ります。



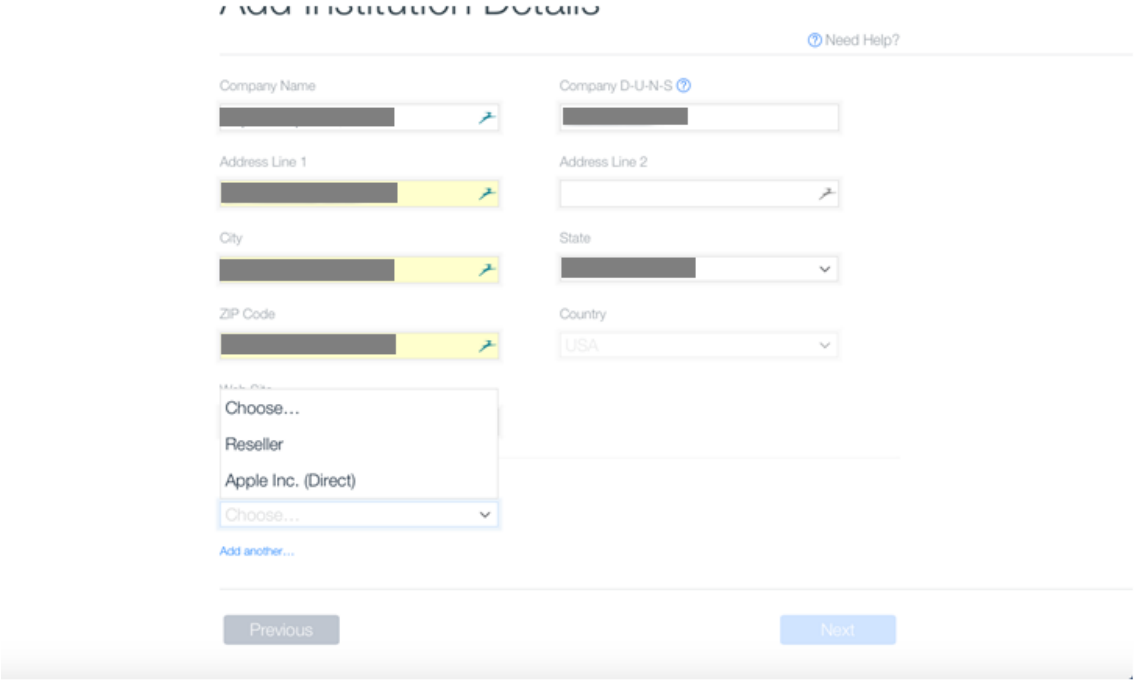
3. 次に、Apple ID でサインインしてアカウントのセキュリティ設定を完了させます。



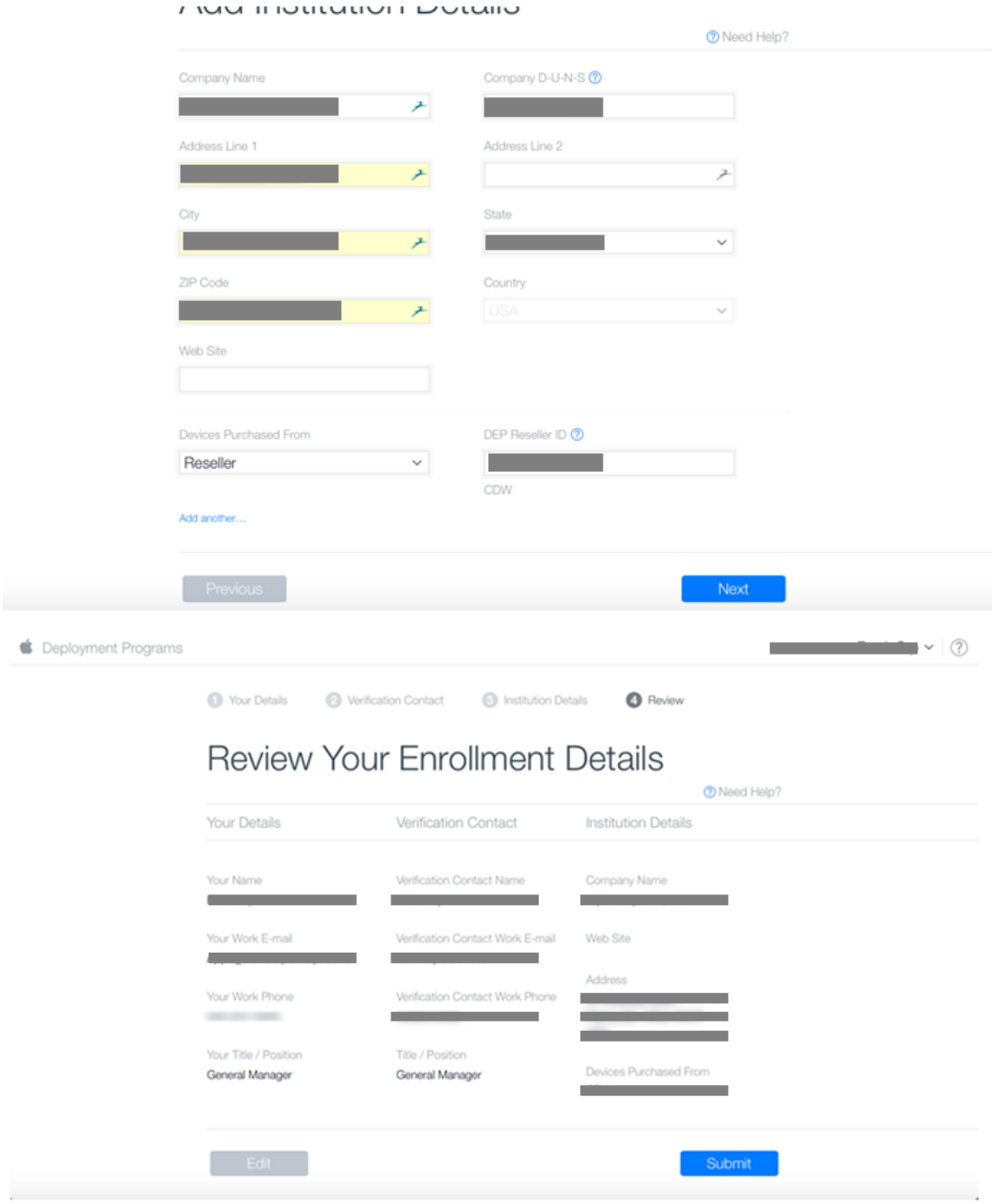
4. 2 段階認証を構成して有効にします。これは、DEP Portal で使用するために必要です。この手順では、電話番号を追加すると、2 段階認証用の 4 桁の PIN を受信します。



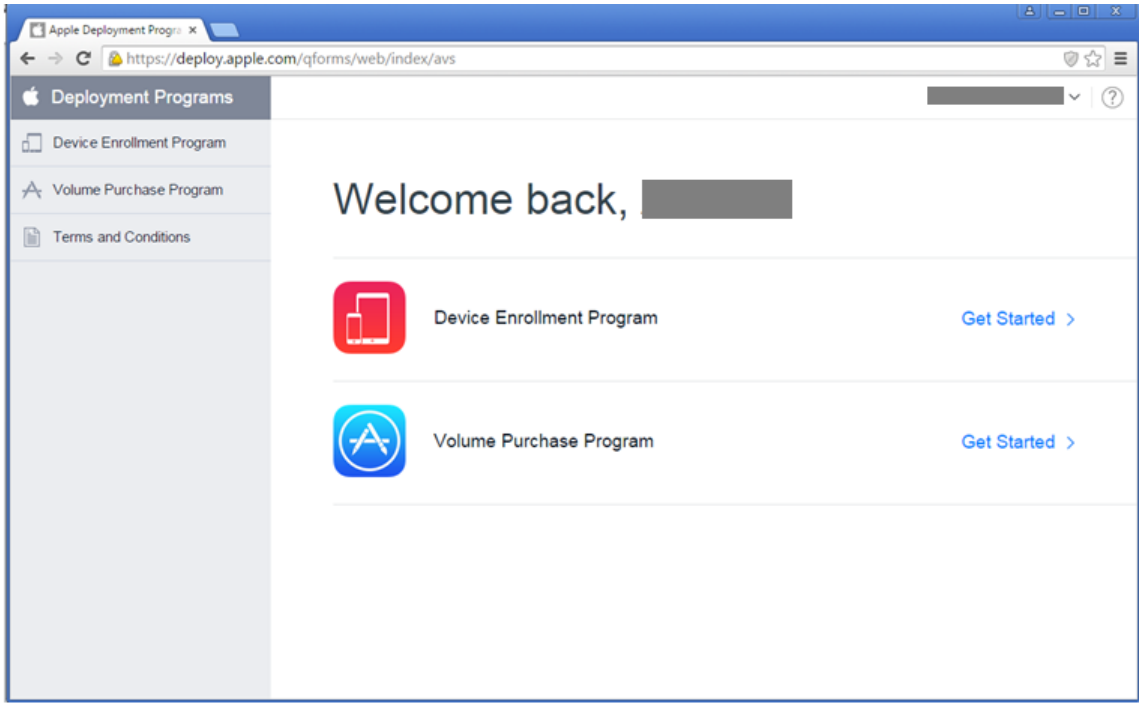
5. DEP Portal にログインし、セットアップした 2 段階認証を使用するアカウント構成を完了させます。
6. 会社の詳細を追加して、デバイスを購入する場所を選択します。購入オプションについては、次のセクションの「DEP 対応デバイスの注文」を参照してください。



7. Apple Customer Number または DEP Reseller ID を追加します。次に、登録の詳細を認証し、Apple がアカウントを承認するのを待ちます。



8. Apple からログオン資格情報を受け取ったら、Apple DEP Portal にログインします。



アカウントを XenMobile に接続する方法については、「iOS および macOS デバイスの一括登録」の「Apple DEP アカウントと XenMobile の統合」を参照してください。

DEP 対応デバイスの注文

DEP 対応デバイスを Apple から直接、または DEP 対応認証リセラーまたはキャリアから注文できます。Apple から注文するには、Apple DEP ポータルに Apple Customer ID を入力します。Customer ID により、Apple は、顧客が購入したデバイスを顧客の Apple DEP アカウントに関連付けることができます。

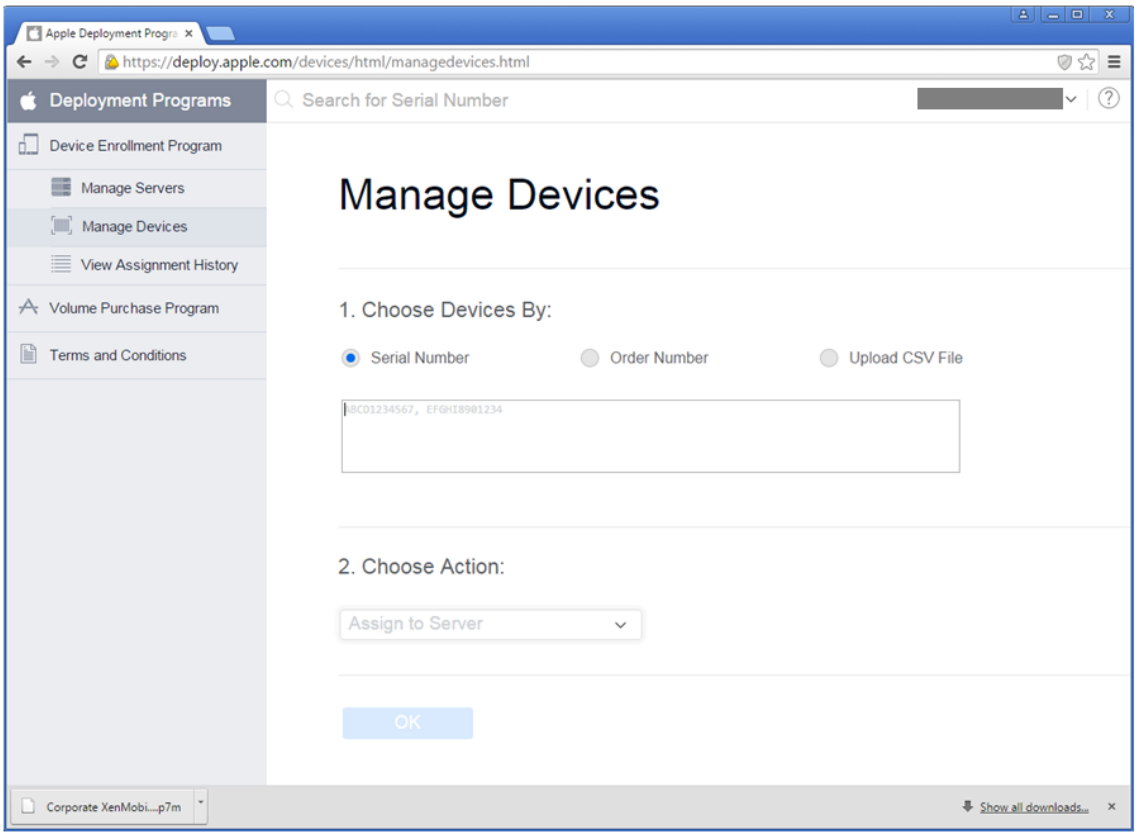
リセラーやキャリアから注文するには、Apple リセラーまたはキャリアに Apple DEP に参加しているかどうかを問い合わせます。デバイスを購入する場合、リセラーの Apple DEP ID が必要です。Apple DEP リセラーを Apple DEP アカウントに追加するにはこの情報が必要となります。再販業者の Apple DEP ID を追加すると、DEP カスタマー ID が届きます。DEP カスタマー ID をリセラーに提供します。リセラーはこの ID を使ってデバイス購入に関する情報を Apple に送信します。詳しくは、Apple の Web サイトを参照してください。

DEP 対応デバイスの管理

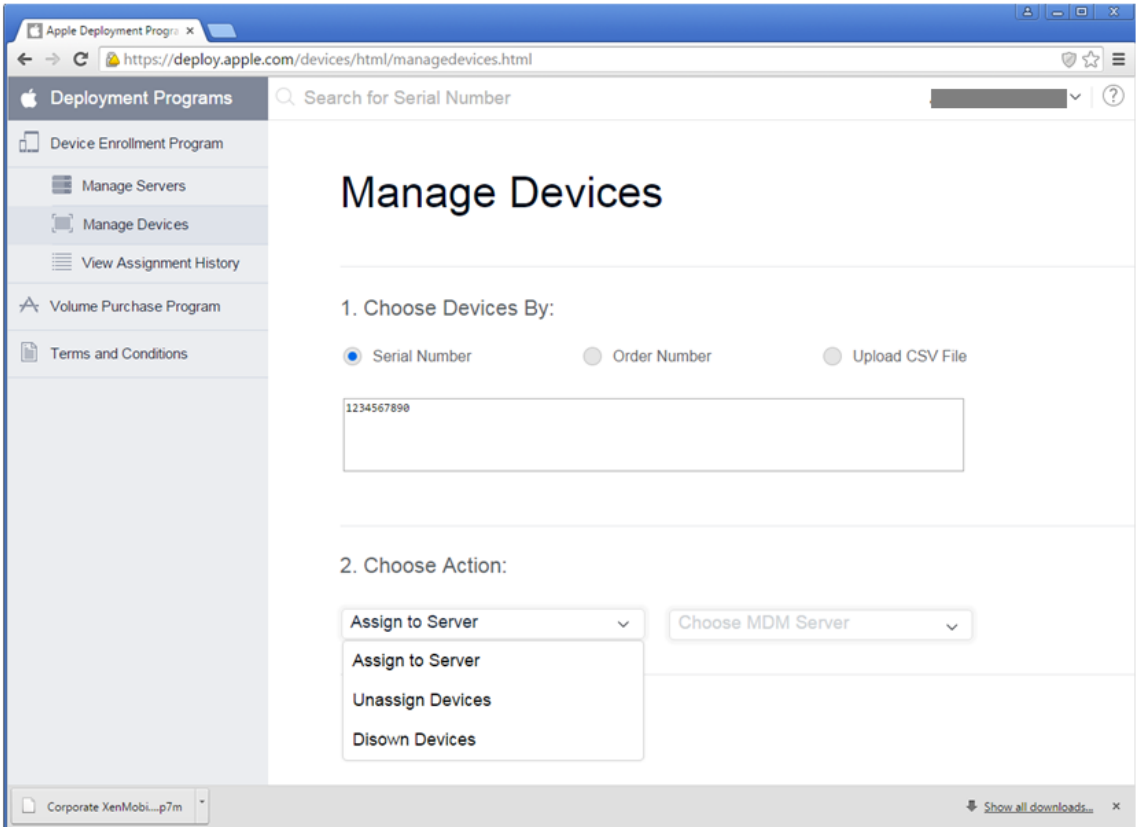
これらの手順に従って、DEP Portal を介して Apple DEP アカウントを更新することで、デバイスを XenMobile Server に割り当てます。

1. Apple DEP Portal にログオンします。
2. [**Device Enrollment Program**] をクリックし、[**Manage Devices**] をクリックします [**Choose Devices By**] で、Apple DEP 対応デバイスをアップロードして定義するためのオプションである [**Serial**

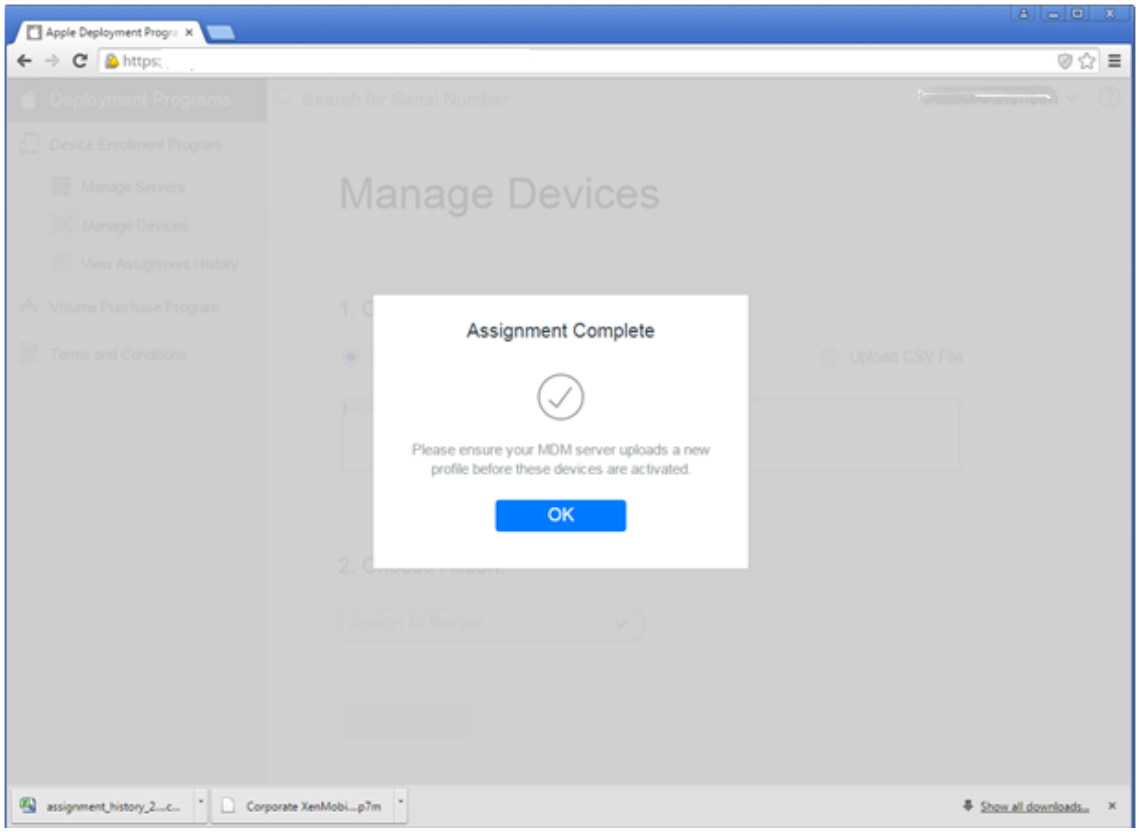
Number］、［**Order Number**］、または ［**Upload CSV File**］ を選択します。



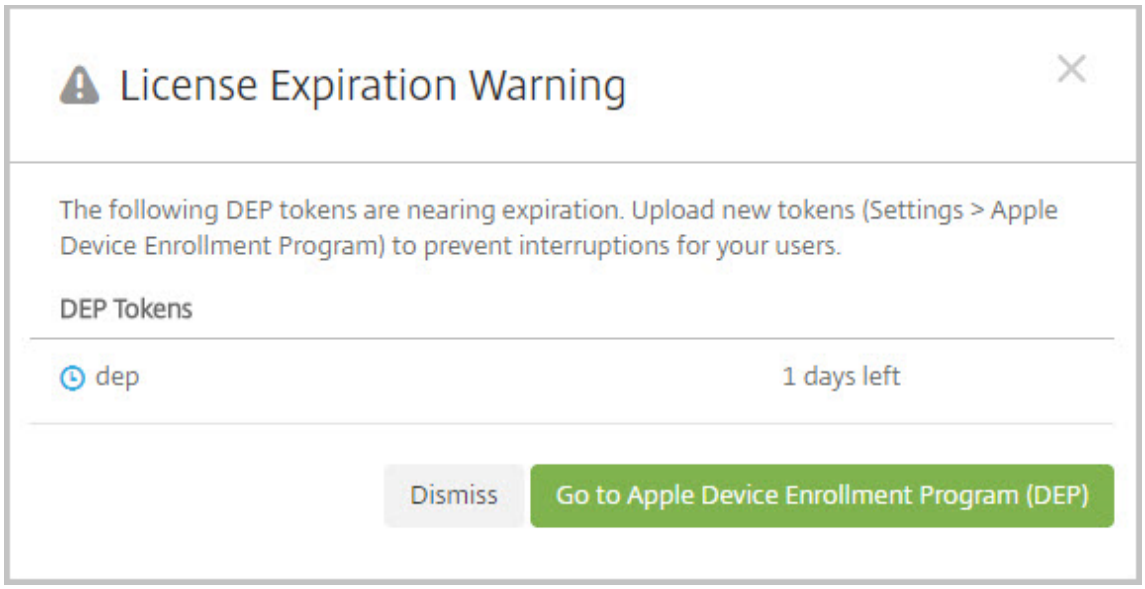
3. デバイスを XenMobile Server に割り当てるには、［**Choose Action**］ で ［**Assign to Server**］ を選択します。次に、一覧で、XenMobile Server の名前を選択します。［**OK**］ をクリックします。



Apple DEP デバイスが選択した XenMobile Server に割り当てられました。



XenMobile は、Apple DEP トークンの有効期限が近づいているか、期限が切れている場合、ライセンス有効期限切れ警告を表示します。



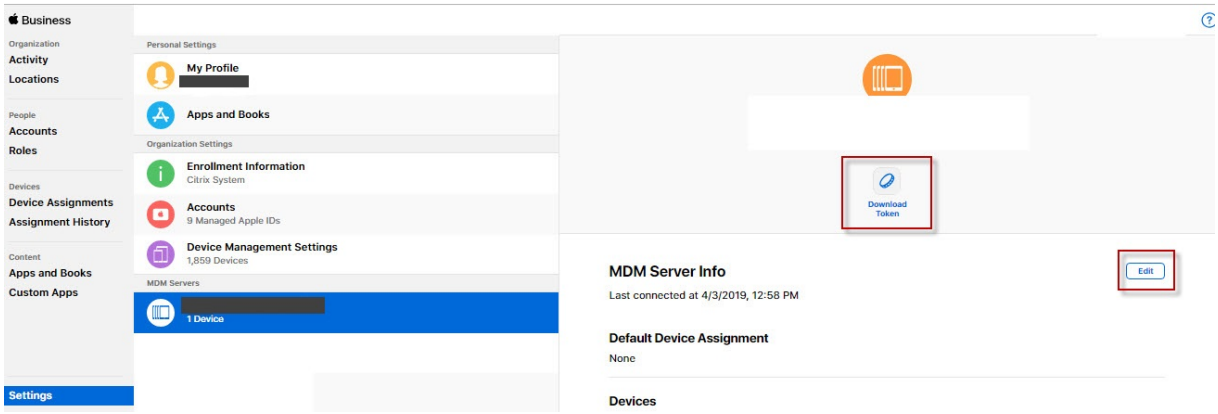
Apple Deployment Program の登録の更新

手順 **1**: **XenMobile** サーバーから公開キーをダウンロードします

1. XenMobile コンソールで、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ の順に移動します。

手順 **2**: **Apple** アカウントからサーバートークンファイルを作成してダウンロードします

1. Apple Deployment Program Portalにサインインしてトークンを更新します。
2. ［**Settings**］**>**［**MDM Server Info**］ を開いて ［**Edit**］ をクリックします。XenMobile からダウンロードした新しい公開キーをアップロードして、変更を保存します。
3. ［**Settings**］ に戻って、新しいトークンをダウンロードします。



手順 **3**: **XenMobile** にサーバートークンファイルをアップロードします

1. XenMobile で、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ の順に移動します。DEP アカウントを選択して、［編集］ をクリックし、サーバートークンファイルをアップロードします。
2. ［次へ］ をクリックして変更を保存します。

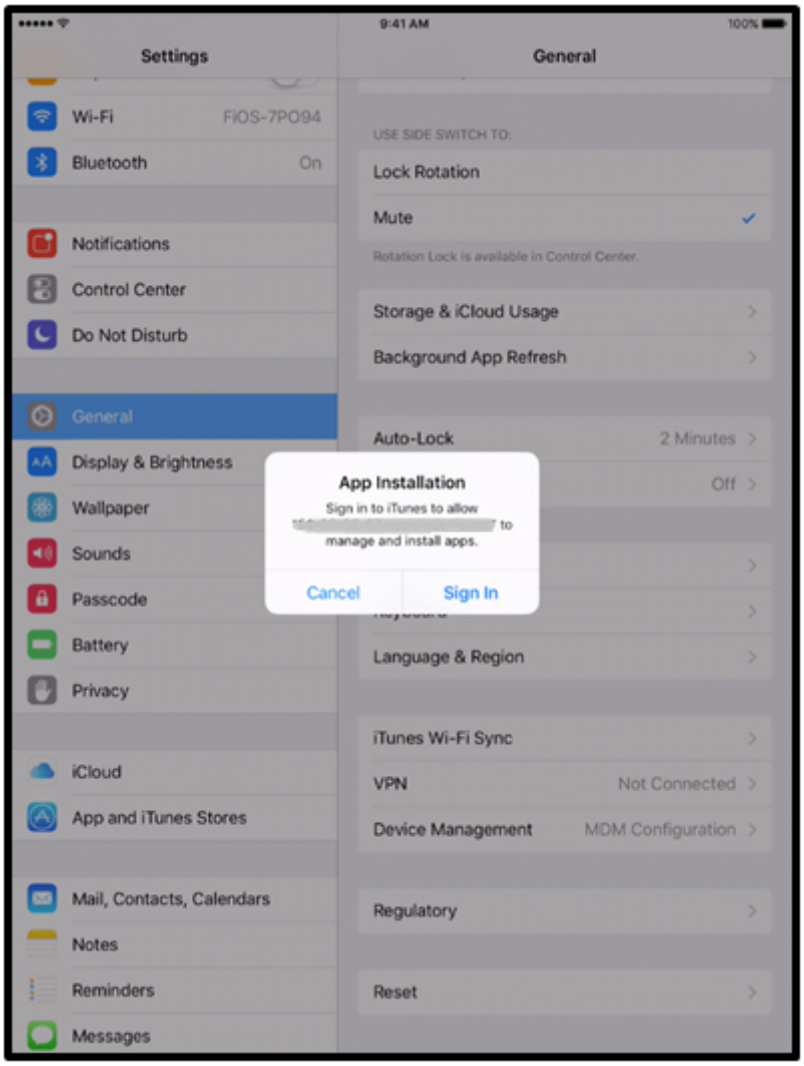
Apple DEP 対応デバイス登録時のユーザーエクスペリエンス

ユーザーが Apple DEP 対応デバイスを登録する場合の手順は次のとおりです。

1. Apple DEP 対応デバイスを開始します。
2. XenMobile から、XenMobile コンソールで構成した Apple DEP 構成が Apple DEP 対応デバイスに配信されます。
3. ユーザーのデバイスで初期設定を構成します。
4. デバイスが自動的に XenMobile デバイス登録処理を開始します。

5. ユーザーのデバイスでその他の初期設定を続行します。
6. ホーム画面では、ユーザーが Citrix Secure Hub をダウンロードできるように、iTunes へのサインインを求められることがあります。

   > 注:
   >
   > XenMobile が、デバイスベースの Volume Purchase Program（VPP）アプリの割り当てを使用して Secure Hub アプリを展開するように設定されている場合、この手順は省略可能です。この場合、iTunes アカウントを作成、または既存のアカウントを使用する必要はありません。



7. Secure Hub を開いて資格情報を入力します。ポリシーにより求められる場合、Citrix PIN を作成して検証するよう求めるメッセージが表示されることがあります。

   XenMobile が残りの必要なアプリをデバイスにすべて展開します。

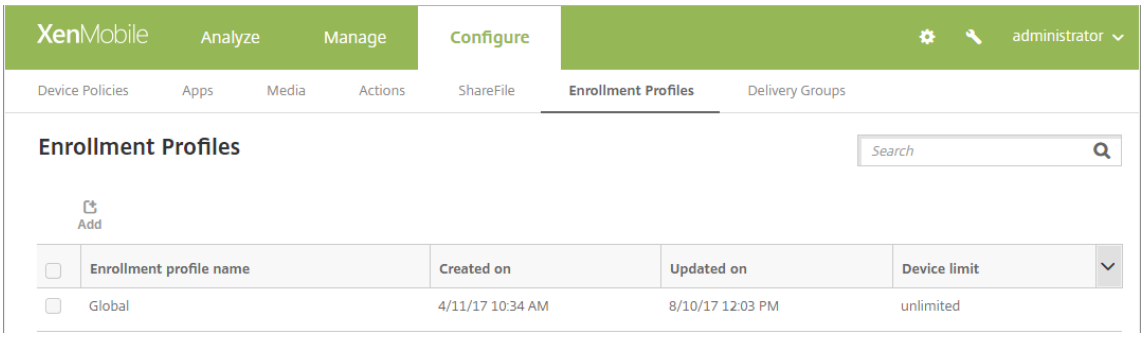
デバイス登録の制限

January 18, 2019

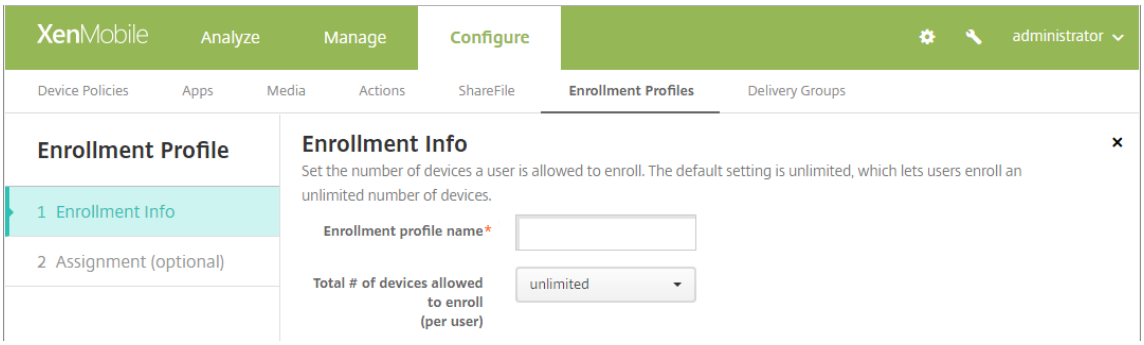
XenMobile には、ユーザーがデバイスをいくつでも登録できるデフォルトの登録プロファイルが含まれています。デフォルトのプロファイル名は Global です。ユーザーが登録できるデバイスの数を制限する場合にのみ、登録プロファイルを作成します。登録プロファイルは、デリバリーグループに関連付けます。

デバイス登録の制限は、ENT、MDM、および MAM サーバーモードに適用されます。この機能は、iOS および Android デバイスでのみ利用できます。

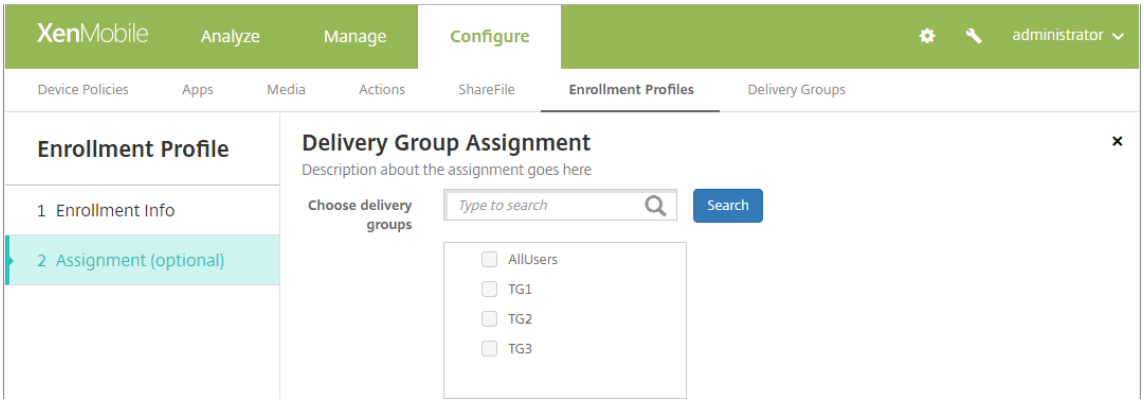
1. [構成] > [登録プロファイル] の順に移動します。デフォルトの Global プロファイルが表示されます。



2. 登録プロファイルを追加するには、[追加] をクリックします。[登録情報] ページで登録プロファイル名を入力してから、このプロファイルのメンバーが登録できるデバイスの数を選択します。

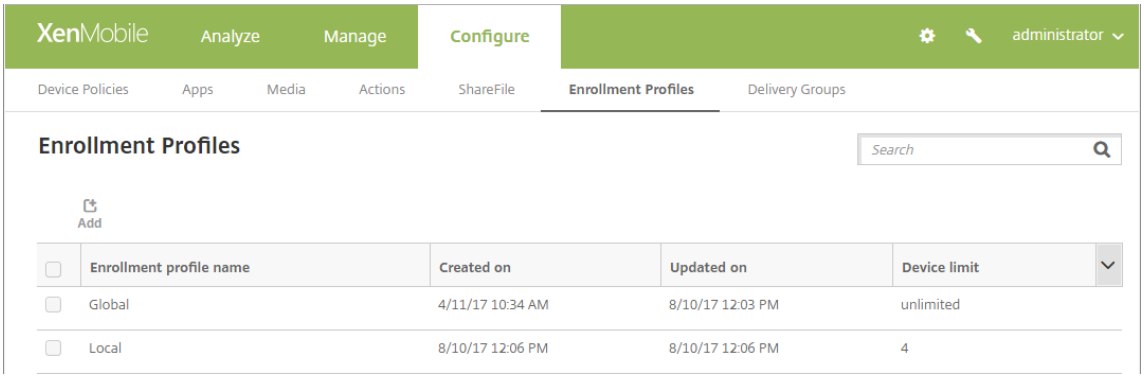


3. [次へ] をクリックします。[デリバリーグループ割り当て] ページが開きます。

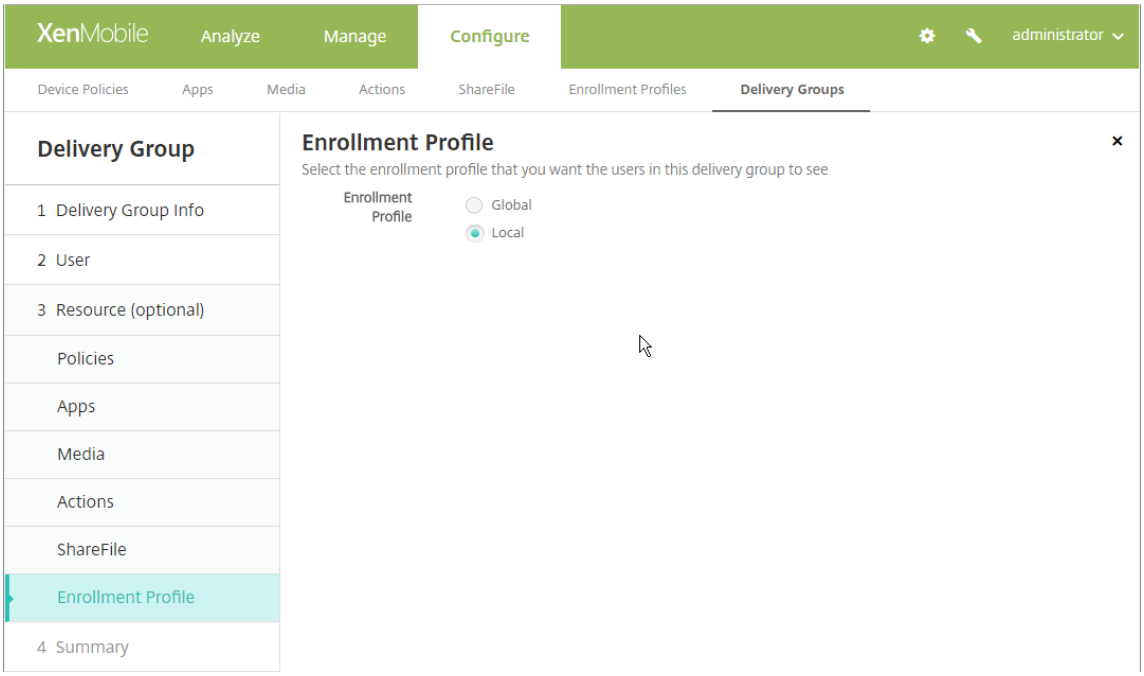


4. この登録プロファイルのデリバリーグループを選択し、［保存］ をクリックします。

［デリバリーグループ］ ページが開きます。



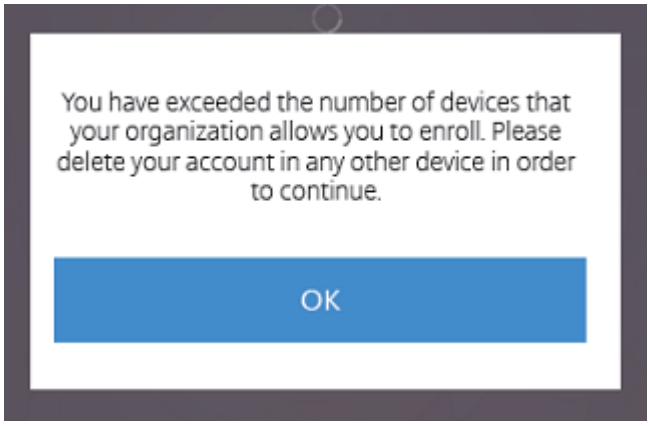
デリバリーグループに関連付けられた登録プロファイルを変更するには、［構成］ **>** ［デリバリーグループ］ の順に移動して、［登録プロファイル］ をクリックします。



デバイス登録制限のユーザーエクスペリエンス

デバイス登録制限を設定してユーザーが新しいデバイスを登録する場合、以下の手順に従います:

1. Secure Hub にサインインします。
2. 登録するサーバーアドレスを入力します。
3. 資格情報を入力します。
4. デバイスの上限に達すると、デバイス登録の上限を超えたことを知らせるエラーメッセージがユーザーに表示されます。



Secure Hub 登録画面が再度表示されます。

デバイスの登録

January 10, 2020

ユーザーデバイスをリモートで安全に管理するために、ユーザーデバイスを XenMobile に登録します。XenMobile クライアントソフトウェアがユーザーデバイスにインストールされ、ユーザーの ID が認証されます。次に、XenMobile とユーザーのプロファイルがインストールされます。すると、XenMobile コンソールでデバイス管理タスクを実行できます。ポリシーの適用、アプリの展開、データのデバイスへのプッシュ、紛失または盗難されたデバイスのロック、ワイプ、および捜索が可能です。

Azure Active Directory への登録は、iOS、Android、および Windows 10 デバイスでサポートされています。Azure を ID プロバイダー（IDP）として構成する方法について詳しくは、「IDP としての Azure Active Directory と XenMobile の統合」を参照してください。

> 注:
>
> iOS デバイスユーザーを登録する前に、APNS 証明書を要求する必要があります。詳しくは、「証明書と認証」を参照してください。

ユーザーとデバイスの構成オプションを更新するには、［管理］**>**［登録招待］ ページを使用します。詳しくは、この文書の「登録招待の送信」を参照してください。

Android デバイス

> 注：
>
> Android Enterprise デバイスの登録について詳しくは、「Android Enterprise」を参照してください。

1. Android デバイスで Google Play ストアにアクセスして、Citrix Secure Hub アプリをダウンロードしてタップします。
2. インストールを求めるメッセージが表示されたら、［次へ］ をクリックし、［インストール］ をクリックします。
3. インストールが完了したら、［開く］ をタップします。
4. 会社の資格情報（XenMobile Server 名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなど）を入力します。入力後、［次へ］ をクリックします。
5. ［デバイス管理者を有効にしますか］ 画面で、［有効にする］ をタップします。
6. 会社のパスワードを入力し、［サインオン］ をタップします。
7. XenMobile の構成方法に応じて、Citrix PIN の作成を求められる場合があります。この PIN を使用して、Secure Hub とその他の XenMobile 対応アプリ（Secure Mail および ShareFile など）にサインオンできます。Citrix PIN は 2 回入力します。［**Citrix PIN** の作成］ 画面で、PIN を入力します。
8. PIN を再入力します。Secure Hub が開きます。その後、XenMobile Store にアクセスし、Android デバイスにインストールできるアプリを確認することができます。
9. 登録の後でアプリをデバイスに自動的にプッシュするように XenMobile を構成している場合は、アプリのインストールを求めるプロンプトがユーザーに表示されます。さらに、XenMobile で構成したポリシーはデバイスに展開されます。［インストール］ をタップしてアプリをインストールします。

Android デバイスを登録解除および再登録するには

ユーザーは Secure Hub 内から登録解除できます。次の手続きを使って登録解除する場合、デバイスは XenMobile コンソールのデバイスインベントリに表示され続けます。ただし、そのデバイスで操作を実行することはできません。そのデバイスを追跡したり、デバイスのコンプライアンスを監視したりすることはできません。

1. Secure Hub アプリをタップして開きます。
2. スマートフォンかタブレットかに応じて、次の操作を行います。

   スマートフォンの場合：

   - 画面左側からスワイプして設定ペインを開きます。
   - ［設定］、［アカウント］、［アカウントの削除］ の順にタップします。

   タブレットの場合：

- 右上のメールアドレスの横の矢印をタップします。
- ［設定］、［アカウント］、［アカウントの削除］ の順にタップします。

3. ［再登録］ をタップします。デバイスの再登録を確認するメッセージが表示されます。
4. ［**OK**］ をタップします。

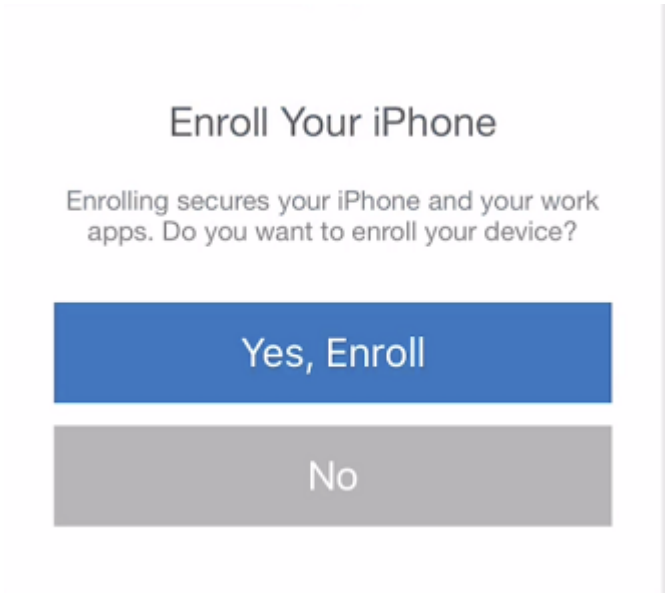
   デバイスの登録が解除されます。
5. 画面の指示に従って、デバイスを再登録します。

iOS デバイスの登録

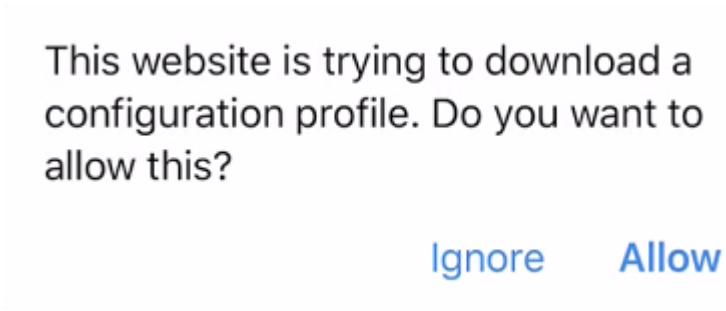
このセクションでは、ユーザーが iOS デバイス（12.2 以降）を XenMobile Server に登録する方法について説明します。iOS の登録について詳しくは、以下のビデオを確認してください:

1. iOS デバイスで Apple ストアにアクセスし、Citrix Secure Hub アプリをダウンロードしてタップします。
2. アプリをインストールするよう求められたら、［次へ］ をタップし、［インストール］ をタップします。
3. インストールが完了したら、［開く］ をタップします。

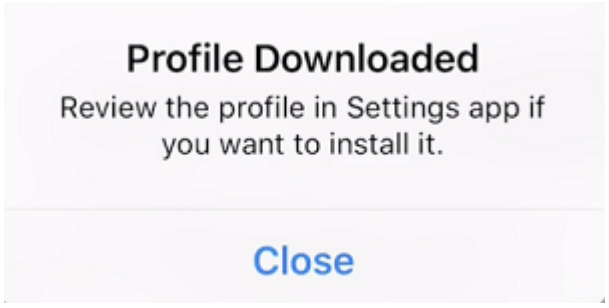
4. 会社の資格情報（XenMobile Server 名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなど）を入力します。入力後、［次へ］ をクリックします。
5. ［はい、登録します］ をタップし、iOS デバイスを登録します。



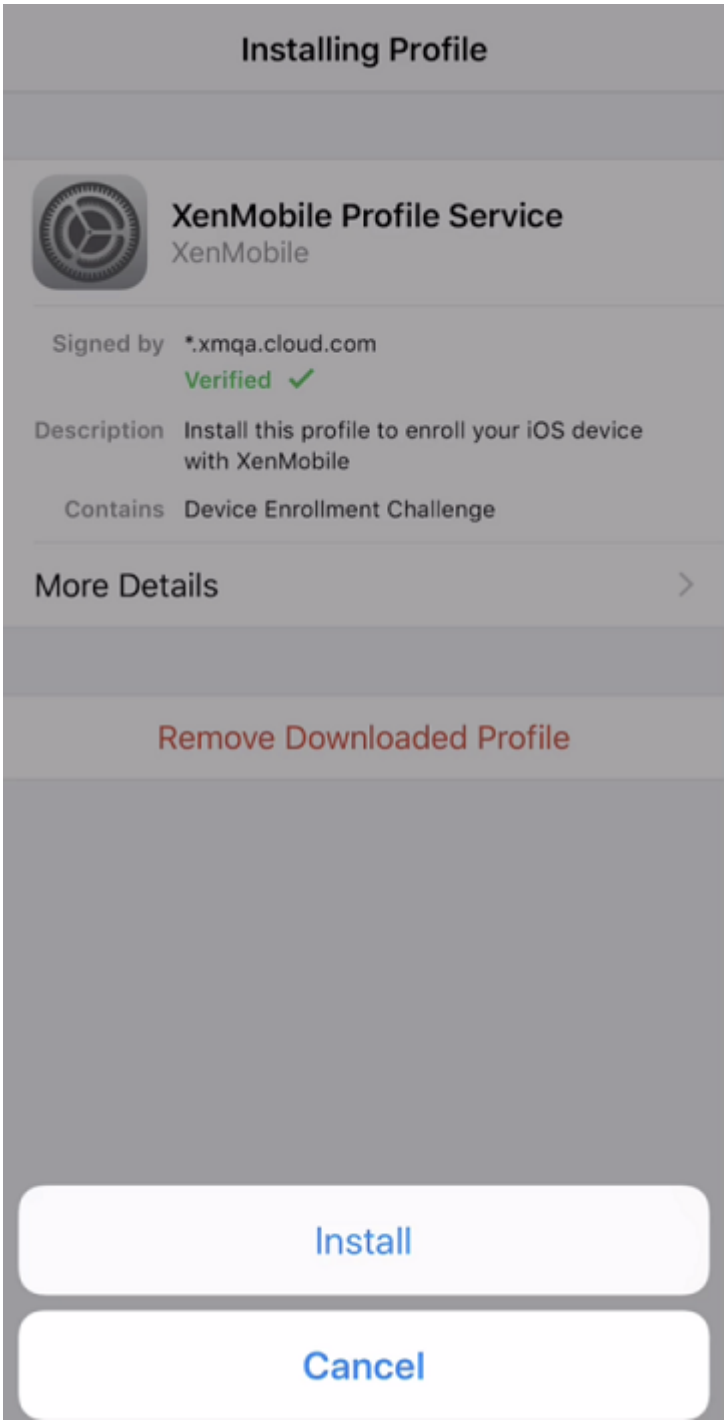
6. 資格情報を入力し、プロンプトが表示されたら［許可］をタップし、構成プロファイルをダウンロードします。



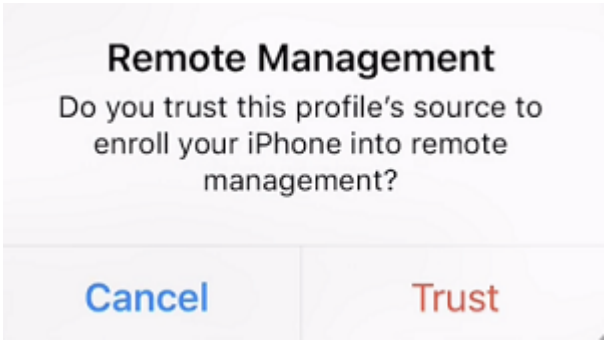
7. 構成プロファイルをダウンロードしたら、［閉じる］ をタップします。



8. デバイス設定で、iOS 証明書をインストールし、デバイスを信頼済み一覧に追加します。
   - ［設定］**>** ［全般］**>** ［プロファイル］**>** ［**XenMobile Profile Service**］ に移動し、［インストール］ をタップしてプロファイルを追加します。



- 通知ウィンドウで ［信頼］ をタップし、デバイスをリモート管理に登録します。

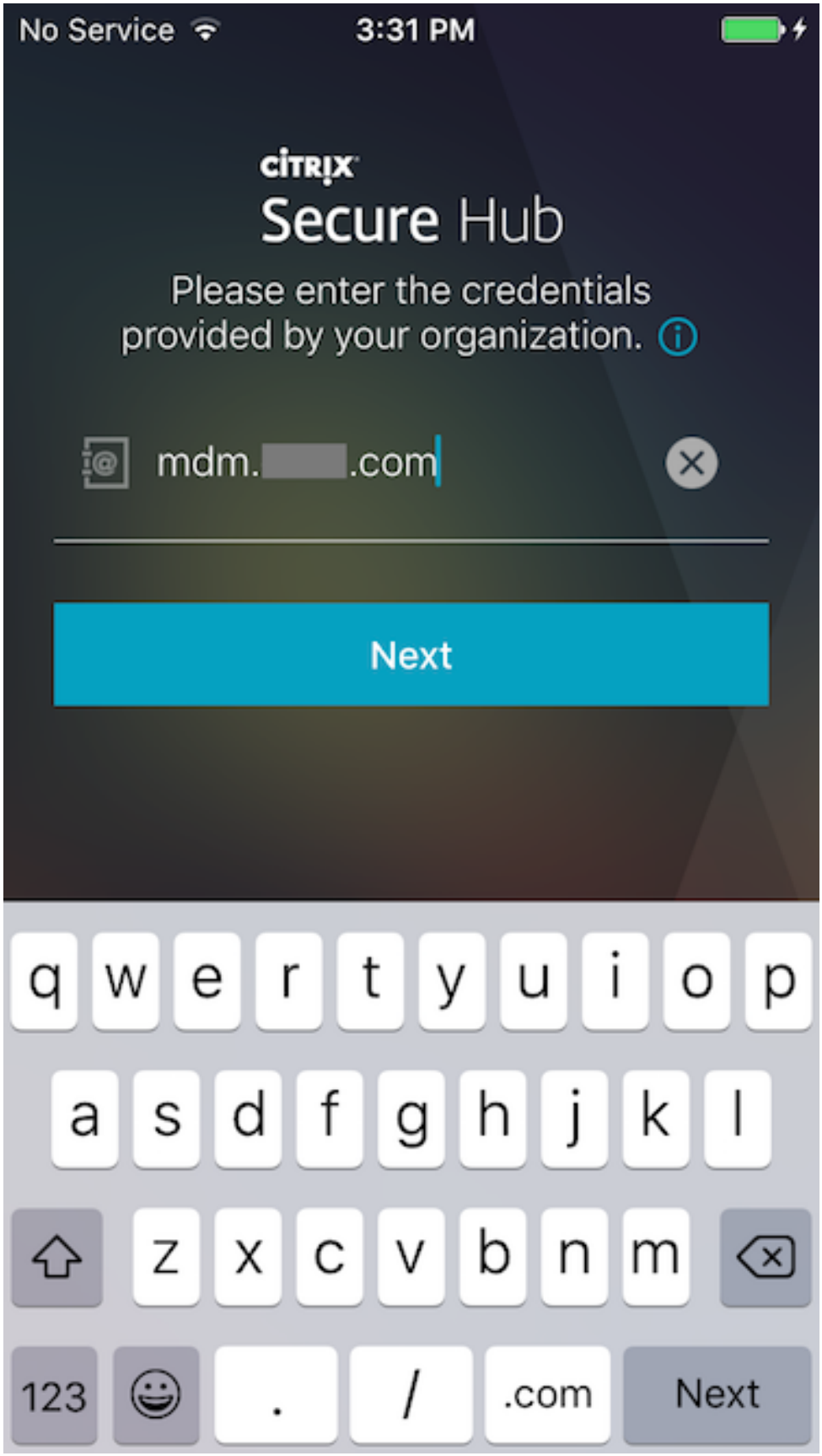


9. Secure Hub にサインインします。MDM+MAM に登録する場合：認証情報を検証した後、プロンプトが表示されたら Citrix PIN を作成および確認します。
10. ワークフローの完了後、デバイスが登録されます。その後、アプリストアにアクセスし、iOS デバイスにインストールできるアプリを確認することができます。

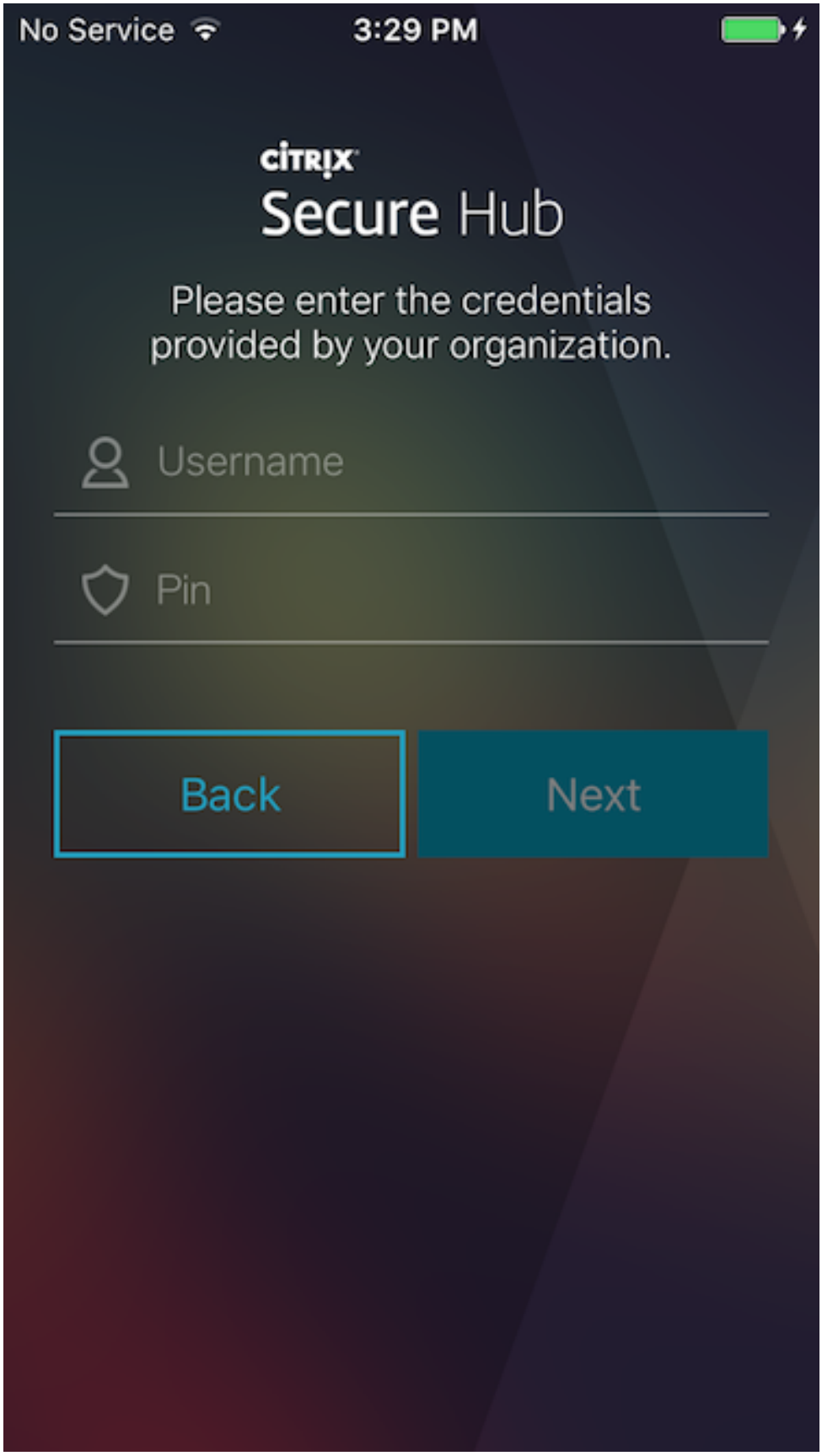
ユーザーが提供する資格情報を使用する **iOS** デバイス

1. Secure Hub アプリをデバイスの Apple 社の iTunes App Store からダウンロードした後、アプリをデバイスにインストールします。
2. iOS デバイスのホーム画面で、Secure Hub アプリをタップします。
3. Secure Hub の起動後、ヘルプデスクが指定するサーバーアドレスを入力します。

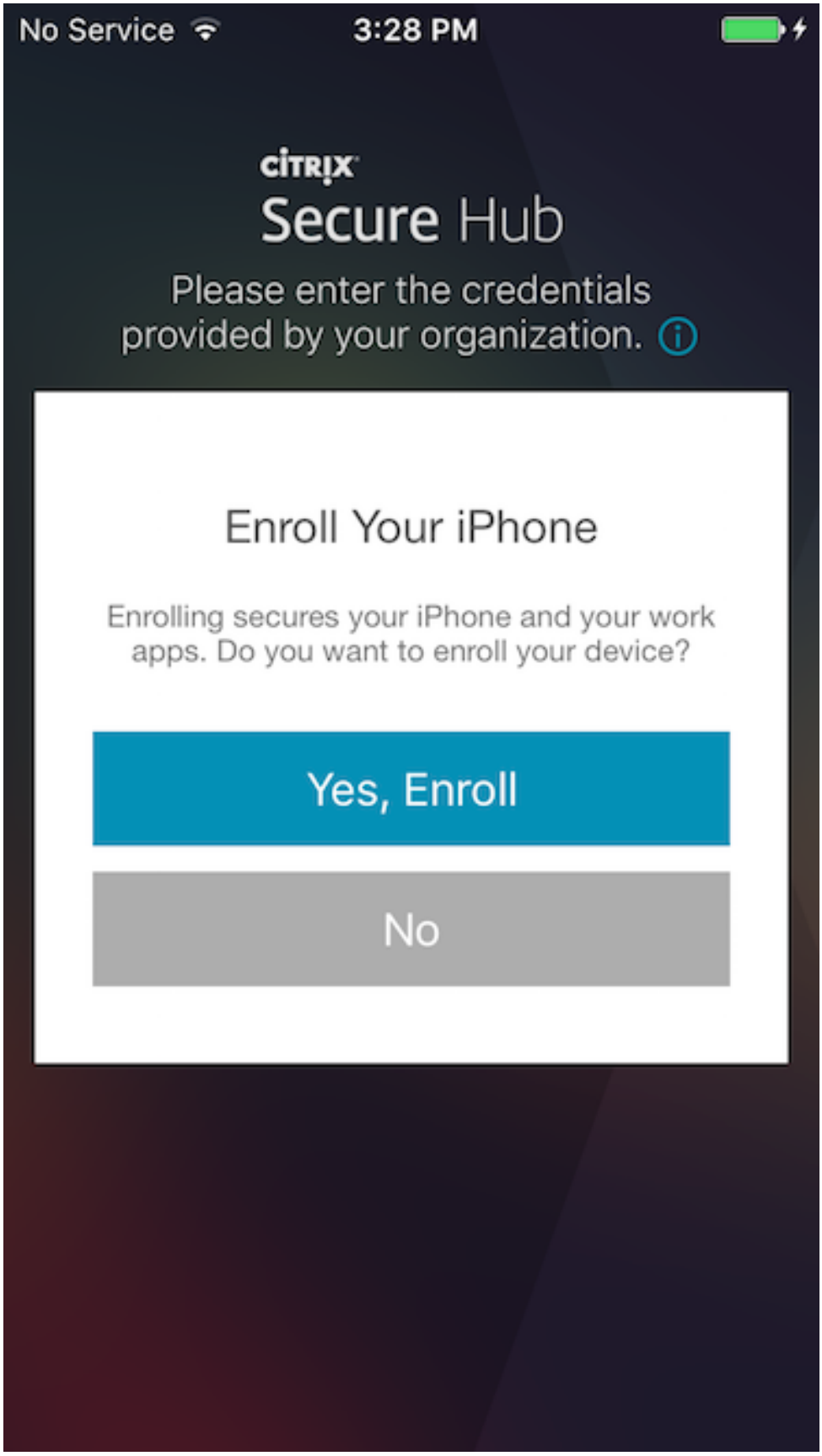
   表示される画面は、XenMobile の構成方法に応じて、次の例と異なる可能性があります。



4. 画面に指示に従って、ユーザー名とパスワード、または PIN を入力します。［次へ］ をクリックします。

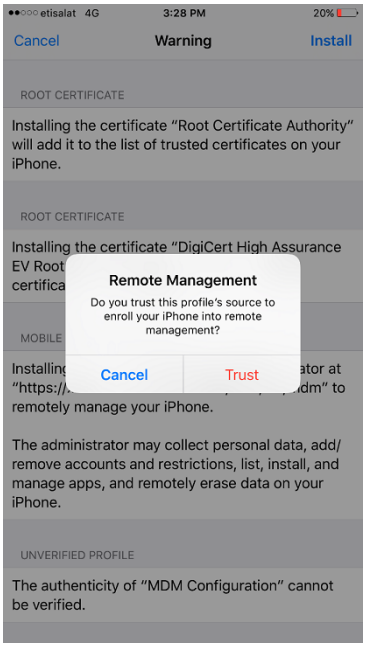


5. 登録するよう求められたら［はい、登録します］をクリックし、続いて画面の指示に従って資格情報を入力します。



6. [インストール] をタップして、Citrix Profile サービスをインストールします。

7. [信頼] をタップします。



8. [開く] をタップし、続いて資格情報を入力します。

派生資格情報を使用する iOS デバイス

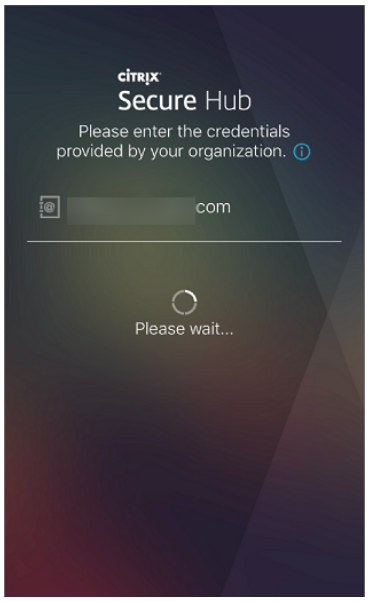
登録するには、デスクトップに取り付けられたスマートカードリーダーにユーザーが各自のカードを挿入する必要があります。

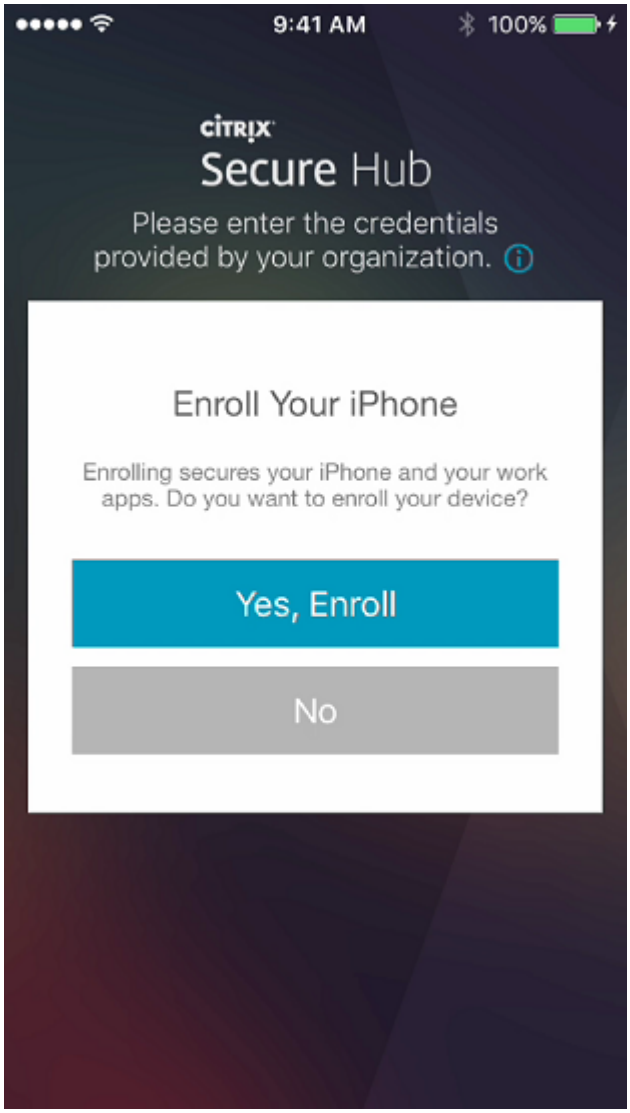
1. 派生資格情報プロバイダーから Secure Hub とアプリをインストールします。

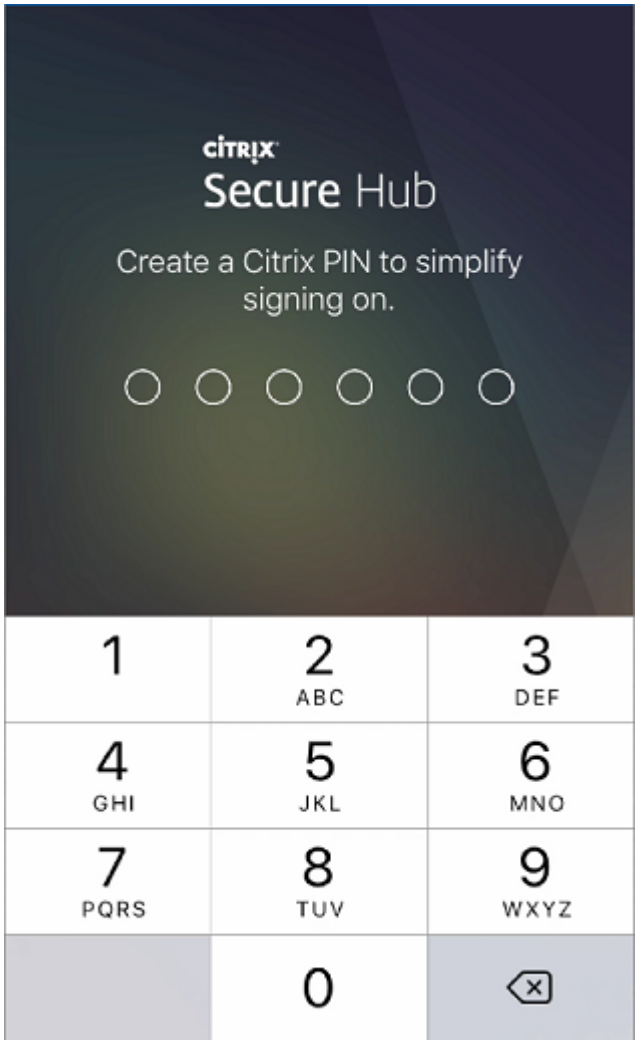
   Intercede の ID プロバイダーアプリは、MyID for Citrix です。以下は、このアプリのロゴです。

2. Secure Hub を起動します。プロンプトが表示されたら、XenMobile Server の完全修飾ドメイン名を入力して ［次へ］ をクリックします。Secure Hub への登録が開始されます。XenMobile Server で派生資格情報がサポートされる場合、Secure Hub はユーザーに Citrix PIN の作成を求めます。

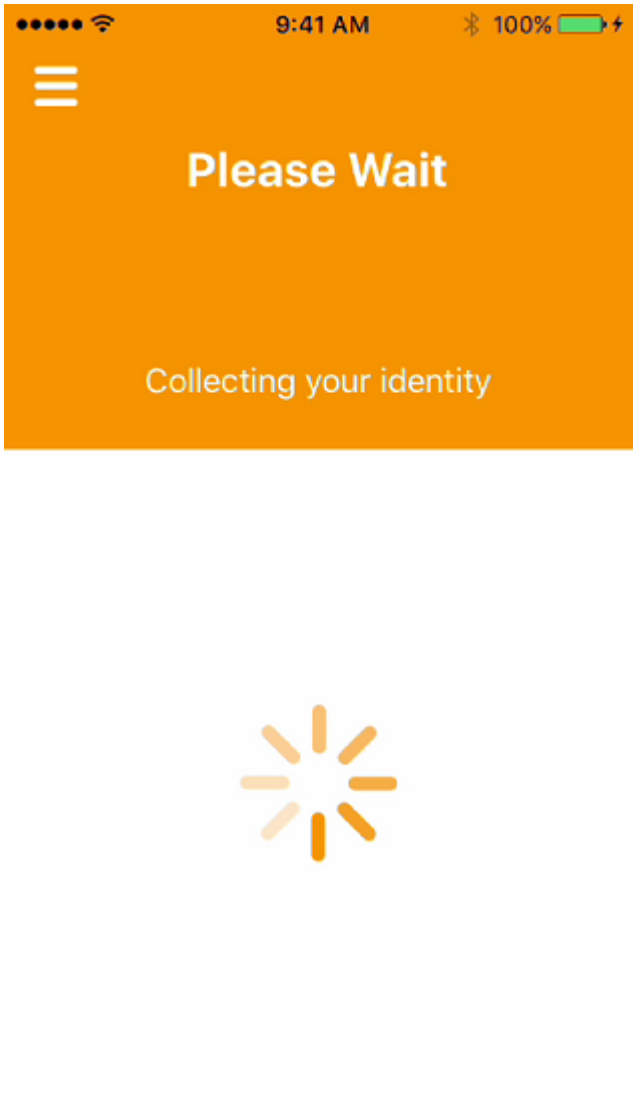
   



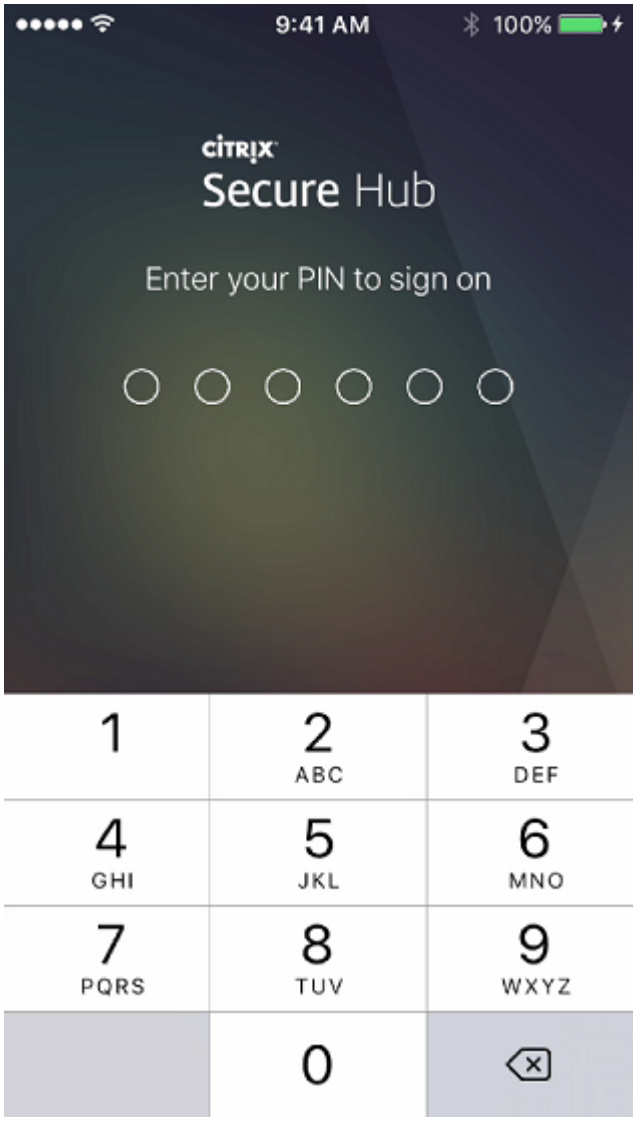


3. 指示に従ってスマート資格情報をアクティブ化します。スプラッシュ画面に続いて、QR コードのスキャンを求めるプロンプトが表示されます。

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。



5. プロンプトが表示されたら、Secure Hub の PIN を入力します。



6. 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。

XenMobile コンソールでデバイス情報を表示するには

- ［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。

macOS デバイス

XenMobile では macOS を実行するデバイスに 2 つの登録方法が提供されます。いずれの方法でも、macOS ユーザーは各自のデバイスから無線経由で直接登録できます。

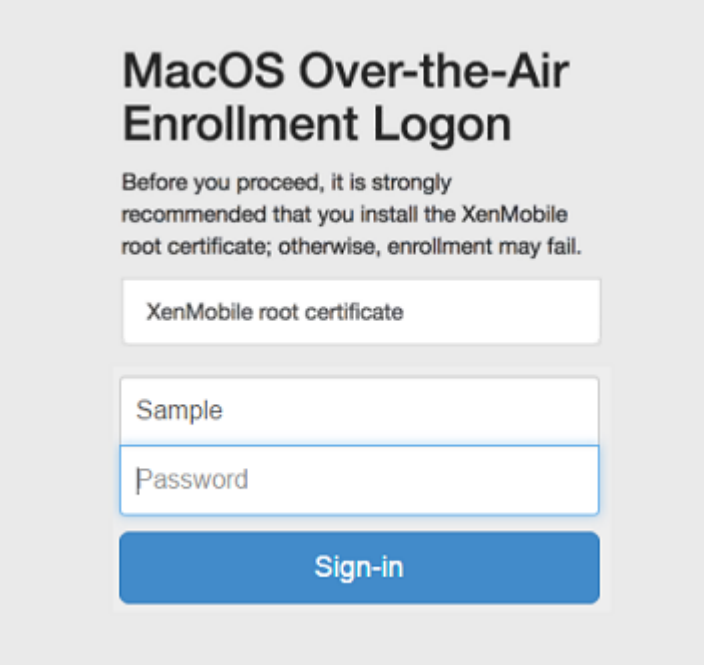
- ユーザーに登録招待を送信します。 この登録方法を使用すると、以下の macOS デバイスの登録モードをいずれも設定できます。
  - ユーザー名およびパスワード
  - ユーザー名および PIN
  - 2 要素

  ユーザーが登録招待の指示に従うと、ユーザー名が入力されたサインオン画面が表示されます。
- ユーザーにインストールリンクを送信します。 この macOS デバイスの登録方法ではユーザーに登録リンクを送信し、ユーザーは Safari ブラウザーまたは Chrome ブラウザーでこのリンクを開くことができます。ユーザーはユーザー名とパスワードを入力して登録を行います。

  macOS デバイスでの登録リンクの使用を防ぐには、サーバープロパティ ［**Enable macOS OTAE**］ を **false** に設定します。これにより、macOS ユーザーは登録招待を使用してのみ登録できるようになります。

ユーザーへの登録招待の送信

1. 任意で、XenMobile コンソールで macOS のデバイスポリシーを設定します。デバイスポリシーについて詳しくは、「デバイスポリシー」を参照してください。
2. macOS ユーザーを登録するための招待を追加します。詳しくは、この記事の「登録招待の送信」を参照してください。
3. ユーザーが招待を受信してリンクをクリックすると、Safari ブラウザーに次の画面が表示されます。ユーザー名は XenMobile によって入力されます。登録モードに ［**2** 要素］ を選択すると、別のフィールドが表示されます。



4. 必要に応じて、ユーザーが証明書をインストールします。ユーザーに証明書のインストールを求めるメッセージが表示されるかは、管理者が macOS 用の公式に信頼される SSL 証明書および公式に信頼されるデジタル署名証明書を構成したかどうかによります。証明書について詳しくは、「証明書と認証」を参照してください。
5. 要求された資格情報をユーザーが入力します。

   Mac のデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、XenMobile で Mac を管理できるようになります。

ユーザーへのインストールリンクの送信

1. 任意で、XenMobile コンソールで macOS のデバイスポリシーを設定します。デバイスポリシーについて詳しくは、「デバイスポリシー」を参照してください。
2. 登録リンク（`https://serverFQDN:8443/instanceName/macos/otae`）を送信します。ユーザーはこのリンクを Safari ブラウザーまたは Chrome ブラウザーで開くことができます。
   - **serverFQDN** は、XenMobile が動作するサーバーの完全修飾ドメイン名（FQDN）です。
   - ポート **8443** は、デフォルトのセキュアポートです。別のポートを構成している場合は、8443 ではなく、構成済みのポートを使用します。
   - 通常 zdm と表示される **instanceName** は、サーバーのインストール時に指定された名前です。

   インストールリンクの送信について詳しくは、「インストールリンクを送信するには」を参照してください。
3. 必要に応じて、ユーザーが証明書をインストールします。管理者が iOS および macOS 用の公式に信頼される SSL 証明書およびデジタル署名証明書を構成すると、ユーザーに証明書のインストールを求めるメッセージが表示されます。証明書について詳しくは、「証明書と認証」を参照してください。
4. ユーザーが Mac にサインオンします。

   Mac のデバイスポリシーがインストールされます。これで、モバイルデバイスを管理するのと同じように、XenMobile で Mac を管理できるようになります。

Windows デバイス

> 注:
>
> このセクションには、Microsoft が 2017 年 7 月 11 日にサポートを終了した Windows Phone 8.1 デバイスのリファレンスも含まれます。XenMobile では、MDM 登録でのみ Windows Phone 8.1 デバイスをサポートしています。

Windows 10 が実行されているデバイスを、Azure を Active Directory 認証の統合手段として使用して登録します。管理者は、以下のいずれかの方法を用いて Windows 10 デバイスを Microsoft Azure AD に統合できます。

- 初めてデバイスの電源を入れたときに、特別な設定をすることなく Azure AD 統合の一部として MDM に登録する。
- デバイスを構成したあとに、[Windows の設定] ページから Azure AD 統合の一部として MDM に登録する。

XenMobile には、以下の Windows オペレーティングシステムが動作するデバイスを登録できます。

- Windows 10 のスマートフォンおよびタブレット
- Windows Phone 8.1

登録は、ユーザーが各自のデバイスから直接実行できます。

> 注：
>
> Windows 10 RS2 Phone およびタブレットでは、再登録時に、サーバー URL の入力を求めるメッセージがユーザーに表示されない点に注意してください。この問題を回避するには、デバイスを再起動します。または［メールアドレス］画面で ［サービスへの接続］ の反対側の［X］をタップし、［サーバー URL］ページに移動します。これはサードパーティ製品の問題です。

ユーザー登録のため自動検出および Windows 検出サービスを構成して、サポートされる Windows デバイスの管理を有効にする必要があります。

Windows デバイスユーザーが Azure を使用して登録できるようにするには、Microsoft Azure サーバーの設定を XenMobile で構成する必要があります。詳しくは、「Microsoft Azure Active Directory サーバー設定」を参照してください。

自己検出を使用して **Windows** デバイスを登録するには

Windows デバイスの管理を有効にするには、Autodiscovery サービスおよび Windows 検出サービスを構成することをお勧めします。詳しくは、「XenMobile AutoDiscovery サービス」を参照してください。

1. デバイスで使用可能な Windows Update をすべて確認し、インストールします。
2. Windows 10 の場合：チャームメニューで ［設定］ をタップし、続けて ［アカウント］ **>** ［職場または学校へのアクセス］ **>** ［職場または学校への接続］ の順にタップします。Windows 8.1 のスマートフォンの場合：［**PC** 設定］ **>** ［ネットワーク］ **>** ［社内］ の順にタップします。
3. 会社のメールアドレスを入力してから、［続行］ （Windows 10）または ［デバイス管理を有効にする］（Windows 8.1）をタップします。ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します（例：`foo@mydomain.com`）。これによって、Windows の埋め込みデバイス管理によって登録が実行される、既知の Microsoft の制限を回避できます。［サービスに接続しています］ ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。デバイスが XenMobile Server を自動的に検出し、登録処理が開始されます。
4. パスワードを入力します。XenMobile のユーザーグループのメンバーであるアカウントに関連付けられたパスワードを使用します。
5. Windows 10 の場合：［使用条件］ ダイアログボックスで、デバイスの管理に同意して、［同意する］ をタップします。Windows 8.1 の場合：［**IT** 管理者によるアプリやサービスの管理を許可する］ ダイアログボックスで、デバイスの管理に同意して、［オンにする］ をタップします。

自己検出なしで **Windows** デバイスを登録するには

自動検出なしで Windows デバイスを登録することができます。しかし、自動検出を構成するようお勧めします。自動検出なしで登録すると、希望する URL に接続する前にポート 80 を呼び出すことになるため、実稼働環境でのベストプラクティスとはみなせません。このような処理は、テスト環境や概念実証展開でのみ使用するようにしてください。

1. デバイスで使用可能な Windows Update をすべて確認し、インストールします。
2. Windows 10 の場合: チャームメニューで ［設定］ をタップし、続けて ［アカウント］ **>** ［職場または学校へのアクセス］ **>** ［職場または学校への接続］ の順にタップします。Windows 8.1 の場合: ［**PC** 設定］ **>** ［ネットワーク］ **>** ［社内］ の順にタップします。
3. 会社のメールアドレスを入力します。
4. Windows 10 の場合: 自動検出が構成されていない場合、手順 5 で説明されているようにサーバーの詳細を入力できるオプションが表示されます。Windows 8.1 の場合: ［サーバーアドレスを自動検出する］ が ［オン］ に設定されている場合、タップしてこのオプションを ［オフ］ にします。
5. Windows 10 の場合: ［サーバーアドレスを入力してください］ フィールドに以下のアドレスを入力します。`https://serverfqdn:8443/serverInstance/wpe`

   未認証の SSL 接続に 8443 以外のポートが使用される場合、このアドレスの 8443 の箇所にそのポート番号を指定します。

   Windows 8.1 の場合: 以下の形式でサーバーアドレスを入力します。`https://serverfqdn:8443/serverInstance/Discovery.svc`

   未認証の SSL 接続に 8443 以外のポートが使用される場合、このアドレスの 8443 の箇所にそのポート番号を指定します。
6. パスワードを入力します。
7. Windows 10 の場合: ［使用条件］ ダイアログボックスで、デバイスの管理に同意して、［同意する］ をタップします。Windows 8.1 の場合: ［**IT** 管理者によるアプリやサービスの管理を許可する］ ダイアログボックスで、デバイスの管理に同意して、［オンにする］ をタップします。

Windows Phone デバイスを登録するには

XenMobile で Windows Phone デバイスを登録するには、ユーザーは Active Directory または内部ネットワークのメールアドレスおよびパスワードを入力する必要があります。自動検出がセットアップされていない場合、ユーザーは XenMobile Server のサーバー Web アドレスも必要です。以下の手順に従って、デバイスを登録します。

> 注:
>
> Windows Phone の業務用ストアを介してアプリを展開する場合は、ユーザーが登録する前に、（署名済みの Secure Hub、サポートする各プラットフォーム向け Windows Phone アプリを使って）エンタープライズ

> ハブポリシーを構成します。

1. Windows Phone のメイン画面で ［設定］ アイコンをタップします。
   - Windows 10 の場合: バージョンに応じて ［アカウント］ **>** ［職場または学校へのアクセス］ **>** ［職場または学校への接続］ の順にタップするか、［アカウント］ **>** ［職場のアクセス］ **>** ［デバイス管理に登録する］ の順にタップします。
   - Windows 8.1 の場合: ［**PC** 設定］ **>** ［ネットワーク］ **>** ［社内］ の順にタップし、次に ［アカウントの追加］ をタップします。
2. 次の画面でメールアドレスとパスワードを入力し、［サインイン］ をタップします。

   ドメインに AutoDiscovery が構成されている場合、以降のいくつかの手順で求められる情報は自動的に抽出されます。手順 8 に進みます。

   ドメインに AutoDiscovery が構成されていない場合、次の手順に進みます。ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します (例: foo@mydomain.com)。これによって既知の Microsoft の制限を回避できます。［**Connecting to a service**］ ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。
3. 次の画面で XenMobile サーバーの Web アドレスを、「https://<xenmobile_server>:<portnumber>/<instancename>/wpe」のように入力します。たとえば、https://mycompany.mdm.com:8443/zdm/wpeのようになります。

   > 注:
   >
   > ポート番号は実際の実装に合わせる必要があります。iOS の登録で使用したポートと同じである必要があります。
4. ユーザー名とドメインを介して認証が検証される場合、ユーザー名とドメインを入力し、次に ［サインイン］ をタップします。
5. Windows Phone 8.1 で、アカウントを追加すると ［業務用アプリをインストール］ というオプションが表示されます。管理者が業務用アプリストアを構成済みの場合、このオプションをオンにして、［完了］ をタップします。このオプションをオフにした場合、業務用アプリストアを受信するには再登録が必要になります。
6. Windows Phone 8.1 で、［アカウントが追加されました］ 画面で ［完了］ をタップします。
7. サーバーへの接続を強制的に実行するには、［最新の情報に更新］ アイコンをタップします。デバイスを手動でサーバーに接続できない場合、XenMobile は再接続を試行します。XenMobile は 3 分ごとに 5 回連続でデバイスに接続し、その後は 2 時間ごとに接続します。この接続頻度は、［サーバーのプロパティ］ にある［**Windows WNS** ハートビートの間隔］ で変更できます。登録の完了後、Secure Hub がバックグラウンドで登録を実行します。インストールが完了してもそれについては何も通知されません。［すべてのアプリ］ 画面から Secure Hub をタップします。

登録招待の送信

XenMobile コンソールで、iOS、macOS、および Android デバイスを使用しているユーザーに登録招待を送信できます。iOS または Android デバイスを使用しているユーザーにインストールリンクを送信することもできます。

登録招待は次のように送信されます。

- 1 人のローカルユーザーまたは Active Directory ユーザーあての登録招待の場合：指定された電話番号と通信事業者で、ユーザーあてに招待の SMS が送信されます。
- グループ宛ての登録招待の場合：ユーザーは SMS 経由で招待を受信します。Active Directory ユーザーのメールアドレスと携帯電話番号が Active Directory に登録されている場合、ユーザーは招待を受信します。ローカルユーザーは、ユーザープロパティで指定されたメールアドレスと電話番号で招待を受信します。

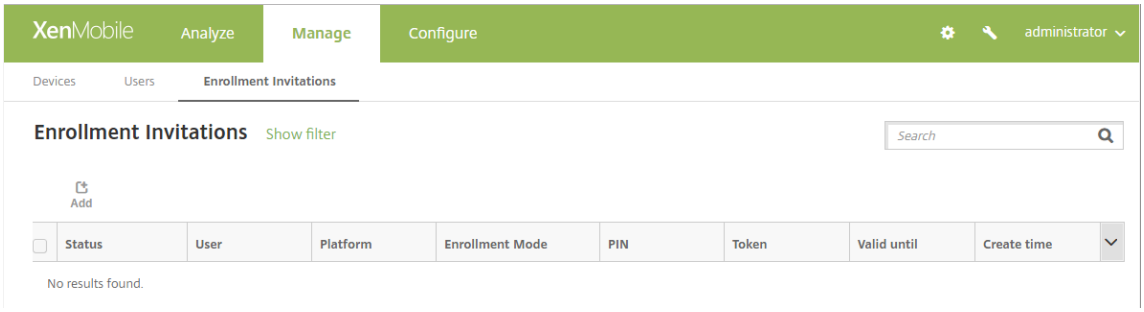
ユーザーが登録すると、そのデバイスは ［管理］ **>** ［デバイス］ で管理対象として表示されます。招待 URL の状態は ［再開］ と表示されます。

前提条件

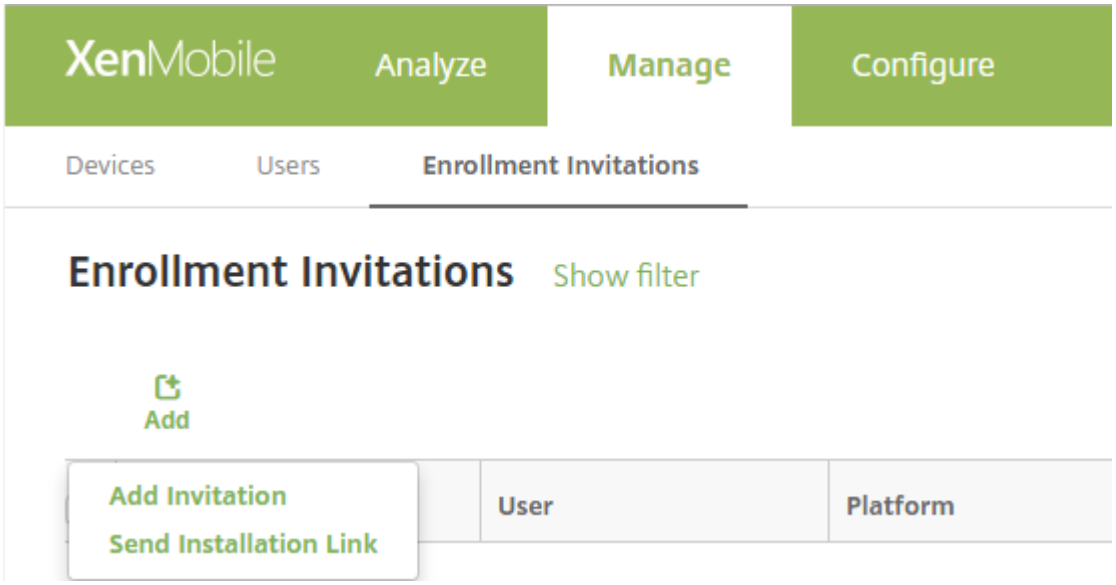
- Enterprise（XME）モードまたは MDM モードで構成された XenMobile Server
- 構成された LDAP
- ローカルグループおよびローカルユーザーを使用する場合：
  - 1 つまたは複数のローカルグループ。
  - ローカルグループに割り当てられたローカルユーザー。
  - デリバリーグループはローカルグループと関連付けられます。
- Active Directory を使用する場合：
  - デリバリーグループは Active Directory グループと関連付けられます。

登録招待の作成

1. XenMobile コンソールで、 ［管理］ **>** ［登録招待］ の順にクリックします。 ［登録招待］ ページが開きます。



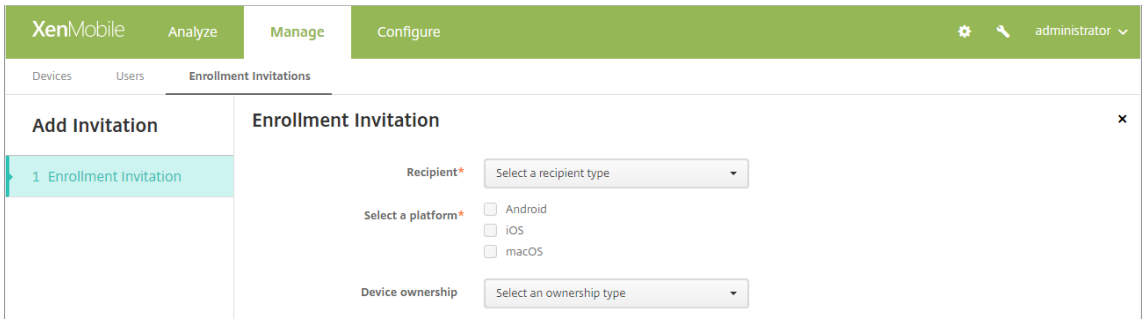
2. ［追加］ をクリックします。登録オプションのメニューが表示されます。



- 1 人のユーザーまたは 1 つのグループに登録招待を送信するには、［招待の追加］ をクリックします。
- SMTP または SMS 経由で登録インストールリンクを受信者の一覧に送信するには、［インストールリンクの送信］ を選択します。

登録招待およびインストールリンクの送信は、次の手順の後に説明します。

3. ［招待の追加］ をクリックします。［登録招待］ 画面が開きます。

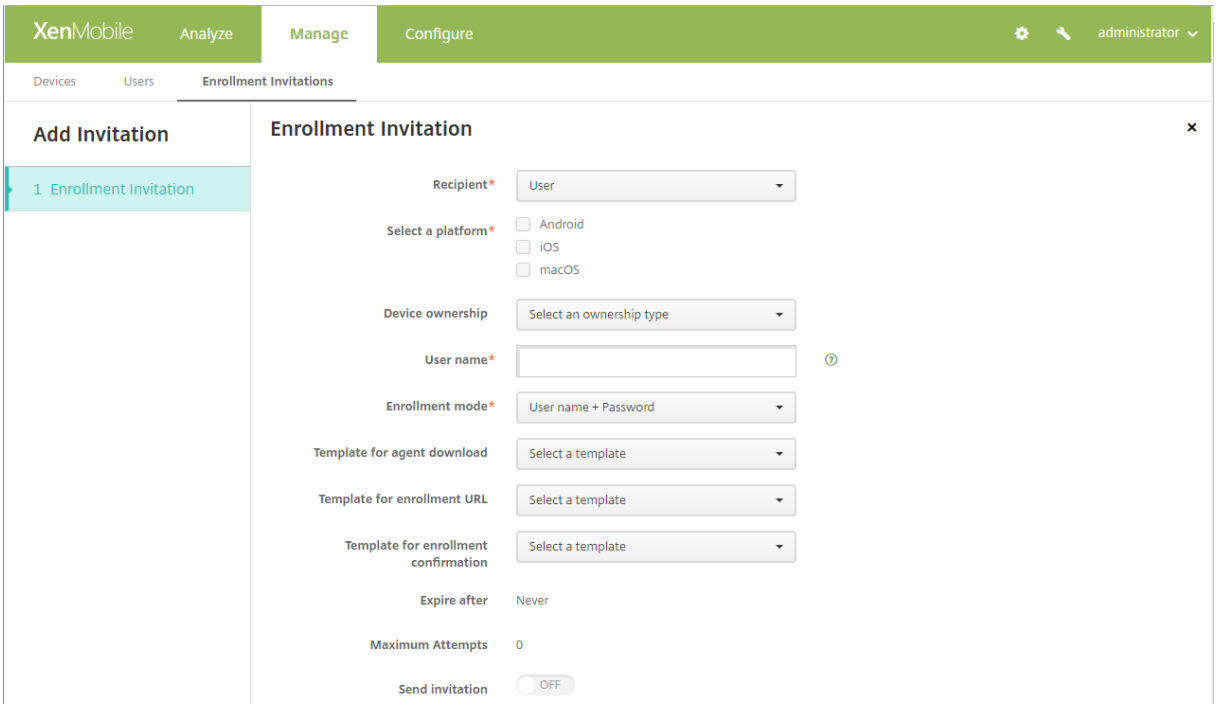


4. 次の設定を構成します。

- 宛先： ［グループ］ または ［ユーザー］ を選択します。
- プラットフォームを選択： ［宛先］ が ［グループ］ の場合はすべてのプラットフォームが選択されます。プラットフォームの選択は変更可能です。［宛先］ が ［ユーザー］ の場合はいずれのプラットフォームも選択されません。プラットフォームを選択します。
- デバイス所有権： ［コーポレート］ または ［従業員］ を選択します。

次のセクションで説明するように、ユーザーまたはグループの設定が表示されます。

登録招待をユーザーに送信するには



1. [ユーザー] について、次の設定を構成します。

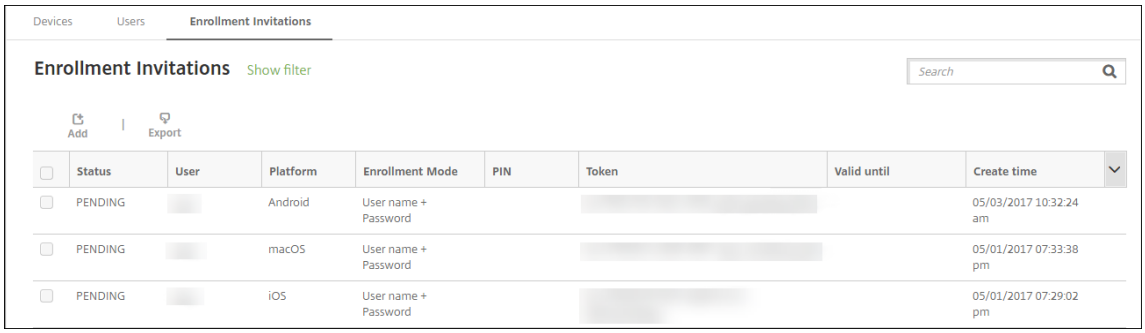
   - ユーザー名: ユーザー名を入力します。ユーザーは、XenMobile Server のローカルユーザー、または Active Directory のユーザーとして存在している必要があります。ローカルユーザーの場合、通知を送信できるようにユーザーのメールプロパティが設定されていることを確認します。Active Directory ユーザーの場合、LDAP が構成されていることを確認します。
   - デバイス情報: 複数のプラットフォームを選択した場合、または macOS のみを選択した場合は、この設定は表示されません。[シリアル番号]、[**UDID**]、または [**IMEI**] を選択します。オプションを選択すると、デバイスに応じて値を入力できるフィールドが表示されます。
   - 電話番号: 複数のプラットフォームを選択した場合、または macOS のみを選択した場合は、この設定は表示されません。任意で、ユーザーの電話番号を入力します。
   - キャリア: 複数のプラットフォームを選択した場合、または macOS のみを選択した場合は、この設定は表示されません。ユーザーの電話番号に関連付けるキャリアを選択します。
   - 登録モード: ユーザーに求める登録の方法を選択します。デフォルトは [ユーザー名およびパスワード] です。次のオプションの中には、すべてのプラットフォームでは使用できないものもあります:
     - ユーザー名およびパスワード
     - 高セキュリティ
     - 招待 URL
     - 招待 URL および PIN
     - 招待 URL およびパスワード
     - 2 要素
     - ユーザー名および PIN

選択した各プラットフォームに有効な登録モードのみが表示されます。登録用の PIN はワンタイム PIN とも呼ばれます。このような PIN は、ユーザーの登録時にのみ有効です。

> 注:
>
> PIN を含む登録モードを選択すると、［登録 **PIN** 用テンプレート］ フィールドが表示されます。このフィールドで、［登録 **PIN**］ を選択します。

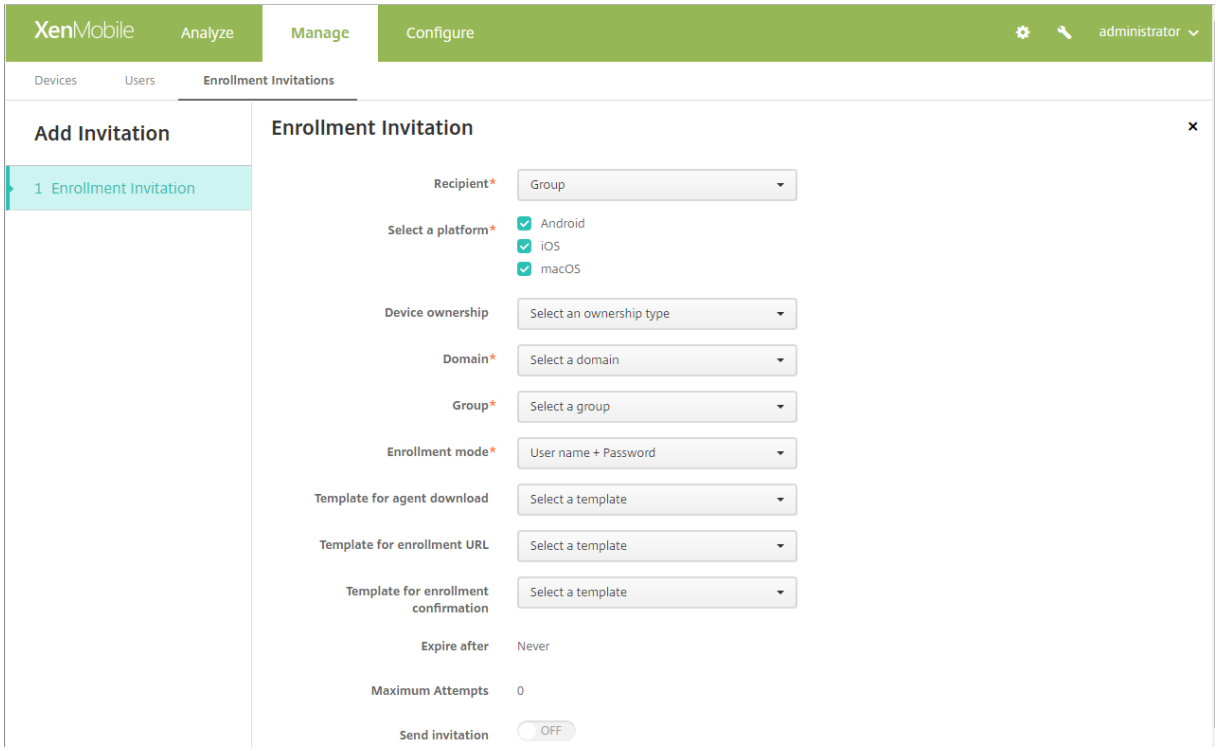
- エージェントダウンロード用テンプレート: ダウンロードリンクという名称のダウンロードリンクのテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォームで使用できます。
- 登録 **URL** 用テンプレート: ［登録招待］ を選択します。
- 登録確認用テンプレート: ［登録確認］ を選択します。
- 有効期限: このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- 最大試行数: このフィールドは登録処理を行う上限回数を示すものであり、登録モードを構成する時に設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- 招待を送信: 招待を直ちに送信するには、［オン］ を選択します。［登録招待］ ページの表に招待は追加するものの送信しない場合は、［オフ］ を選択します。

2. ［招待を送信］ を有効にした場合は ［保存］ および［送信］ をクリックします。それ以外の場合は ［保存］ をクリックします。［登録招待］ ページの表に招待が追加されます。



登録招待をグループに送信するには

以下は、グループへの登録招待を構成するための設定画面です。



1. 次の設定を構成します。

   - ドメイン： 招待の宛先グループのドメインを選択します。
   - グループ： 招待の宛先グループを選択します。
   - 登録モード： ユーザーに求める登録の方法を選択します。デフォルトは［ユーザー名およびパスワード］です。次のオプションの中には、すべてのプラットフォームでは使用できないものもあります：
     - ユーザー名およびパスワード
     - 高セキュリティ
     - 招待 URL
     - 招待 URL および PIN
     - 招待 URL およびパスワード
     - 2 要素
     - ユーザー名および PIN

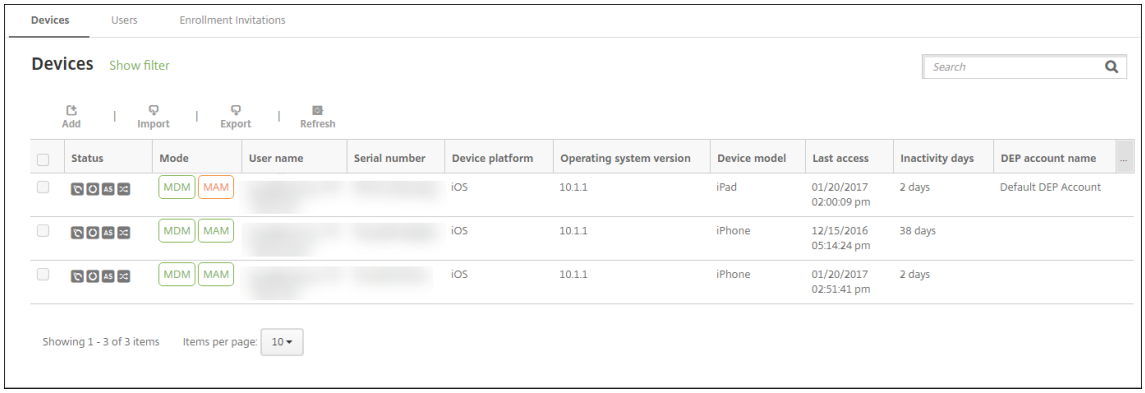
   選択した各プラットフォームに有効な登録モードのみが表示されます。

   > 注：
   >
   > PIN を含む登録モードを選択すると、［登録 **PIN** 用テンプレート］ フィールドが表示されます。このフィールドで、［登録 **PIN**］ を選択します。

   - エージェントダウンロード用テンプレート： ダウンロードリンクという名称のダウンロードリンクのテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォームで使用できます。
   - 登録 **URL** 用テンプレート： ［登録招待］ を選択します。

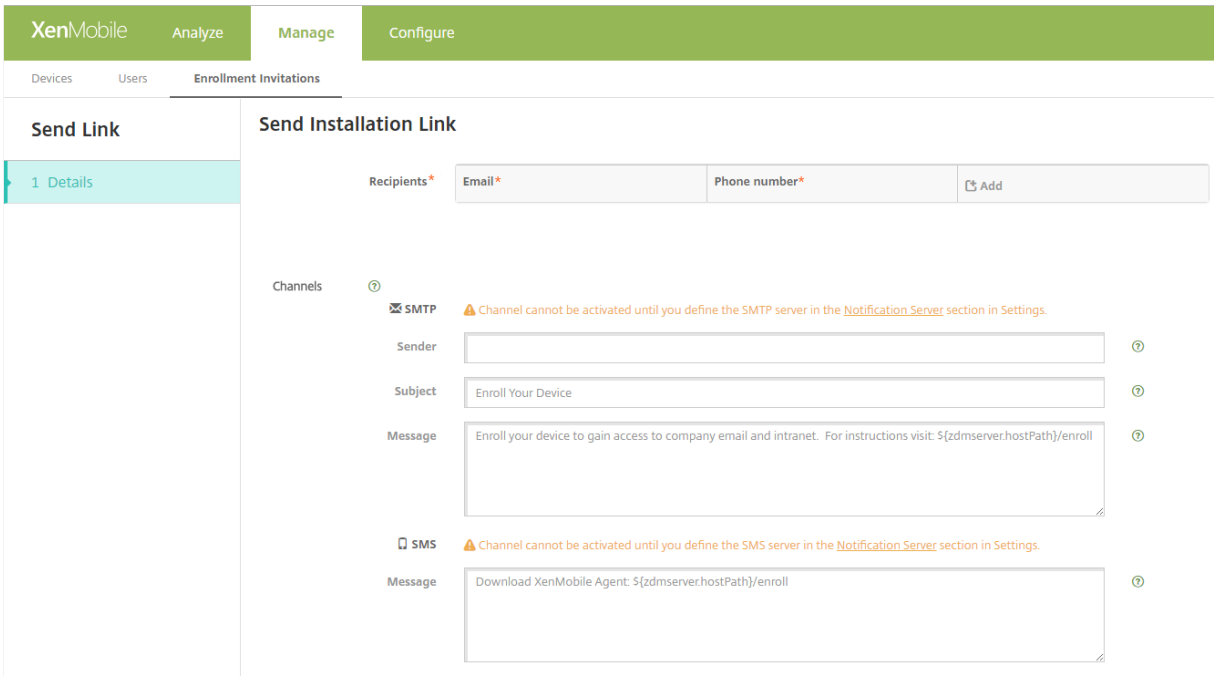
- 登録確認用テンプレート： ［登録確認］ を選択します。
- 有効期限： このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- 最大試行数： このフィールドは登録処理を行う上限回数を示すものであり、登録モードを構成する時に設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- 招待を送信： 招待を直ちに送信するには、［オン］ を選択します。［登録招待］ ページの表に招待は追加するものの送信しない場合は、［オフ］ を選択します。

2. ［招待を送信］ を有効にした場合は ［保存］ および［送信］ をクリックします。それ以外の場合は ［保存］ をクリックします。［登録招待］ ページの表に招待が表示されます。



インストールリンクを送信するには

登録インストールリンクを送信する前に、［設定］ ページでチャネル（SMTP または SMS）を構成する必要があります。詳しくは、「[通知]」（/ja/jp/xenmobile/server/users/notifications.html）を参照してください。



1. これらの設定を構成し、［保存］ をクリックします。

    - 宛先: 追加する宛先ごとに、［追加］ をクリックして以下の操作を行います:
        - メール: 送信先のメールアドレスを入力します。このフィールドは必須です。
        - 電話番号: 送信先の電話番号を入力します。このフィールドは必須です。

    > 注:
    >
    > 既存の送信先を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには ［削除］ をクリックし、項目をそのままにするには ［キャンセル］ をクリックします。

    既存の送信先を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［保存］ をクリックして変更した項目を保存するか、［キャンセル］ をクリックして項目を変更せずそのままにします。

    - チャネル: 登録インストールリンクの送信に使用するチャネルを選択します。通知は **SMTP** または **SMS** で送信することができます。［通知サーバー］ の ［設定］ ページでサーバー設定を構成するまでは、これらのチャネルをアクティブ化できません。詳しくは、「通知」を参照してください。
    - **SMTP**: 次の設定を任意で構成します。これらのフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
        - 差出人: オプションで送信者を入力します。
        - 件名: 任意でメッセージの件名を入力します。たとえば、「Enroll your device」などです。
        - メッセージ: 任意で、送信先に送信されるメッセージを入力します。たとえば、「Enroll your device to gain access to organizational apps and email.」などです。
    - **SMS**: 以下の設定を構成します。このフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
        - メッセージ: 送信先に送信されるメッセージを入力します。SMS ベースの通知の場合、このフィールドは必須です。

    > 注: 北米の場合、160 文字を超える SMS メッセージは複数のメッセージとして配信されます。

2. ［送信］ をクリックします。

    > 注:
    >
    > 環境が sAMAccountName を使用している場合、ユーザーが招待を受け取ってリンクをクリックした後、認証を完了するには、ユーザー名を編集する必要があります。ユーザー名は「sAMAccount-Name@domainname.com」の形式で表示されます。ユーザーは「@domainname.com」の部分を削除する必要があります。

Firebase Cloud Messaging

January 10, 2020

> 注:
>
> Firebase Cloud Messaging（FCM）は以前は Google Cloud Messaging（GCM）と呼ばれていました。XenMobile コンソールのラベルとメッセージの一部には、GCM 用語が使用されています。

Firebase Cloud Messaging（FCM）を使用して Android デバイスが XenMobile に接続するタイミングと方法を制御することをお勧めします。XenMobile で FCM が構成されている場合、FCM で有効な Android デバイスに接続通知を送信します。セキュリティ操作や展開コマンドによって、ユーザーに XenMobile Server への再接続を求めるプッシュ通知が送信されます。

この記事の構成手順を完了し、デバイスがチェックインすると、デバイスは XenMobile Server で FCM サービスに登録します。これにより、FCM を使用して XenMobile サービスからデバイスにほぼリアルタイムで通信することができます。FCM の登録は、新しく登録するデバイスおよび以前に登録されたデバイスで機能します。

XenMobile がデバイスへの接続を開始する必要がある場合、XenMobile は FCM サービスに接続し、FCM サービスは接続するようにデバイスに通知します。この種類の接続は、Apple プッシュ通知サービスでの接続と似ています。

前提条件

- 最新の Secure Hub クライアント
- Google デベロッパーアカウントの資格情報
- FCM 対応 Android デバイスにインストールされた Google Play サービス

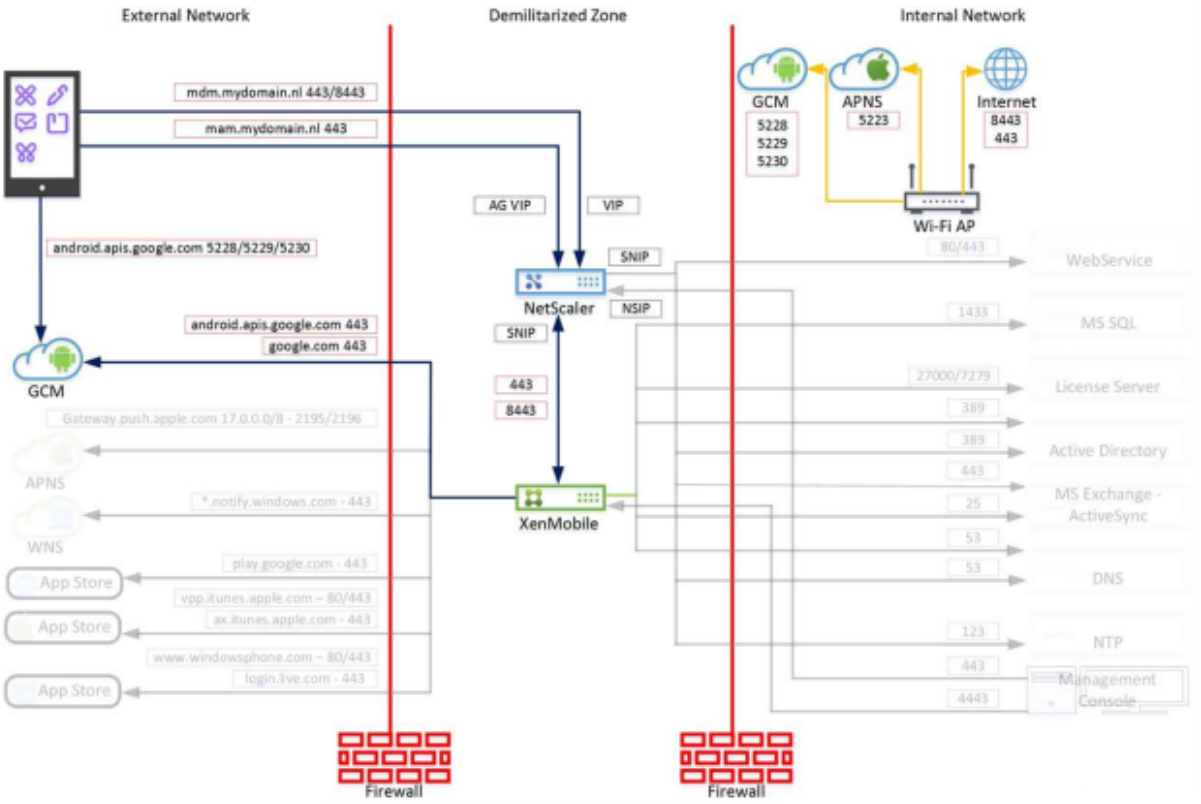
ファイアウォールポート

- `fcm.googleapis.com`および`Google.com`に対しては、XenMobile のポート 443 を開きます。
- デバイスの Wi-Fi によるインターネット送信接続用にポート 5228、5229、5230 を開きます。
- 送信接続を許可するには、IP 制限なしでポート 5228 ～ 5230 をホワイトリストに登録することをお勧めします。ただし、IP 制限が必要な場合は、IPv4 および IPv6 ブロック内のすべての IP アドレスをホワイトリストに登録しすることをお勧めします。ブロックは、Google のASN 15169に記載されています。このリストは、毎月更新してください。

詳しくは、「ポート要件」を参照してください。

アーキテクチャ

次の図は、外部および内部ネットワークにおける FCM の通信フローを示しています。

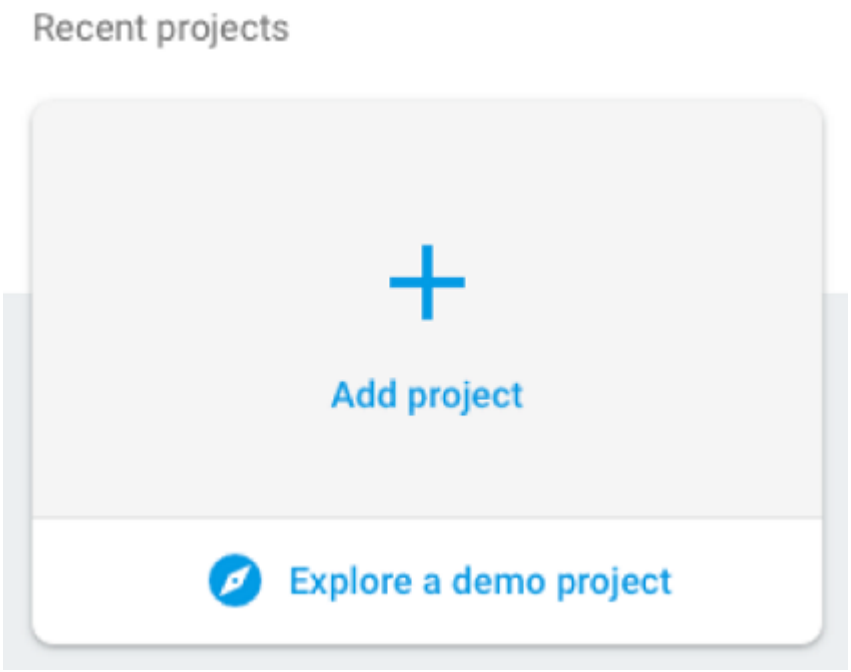


Google アカウントを **FCM** 向けに構成するには

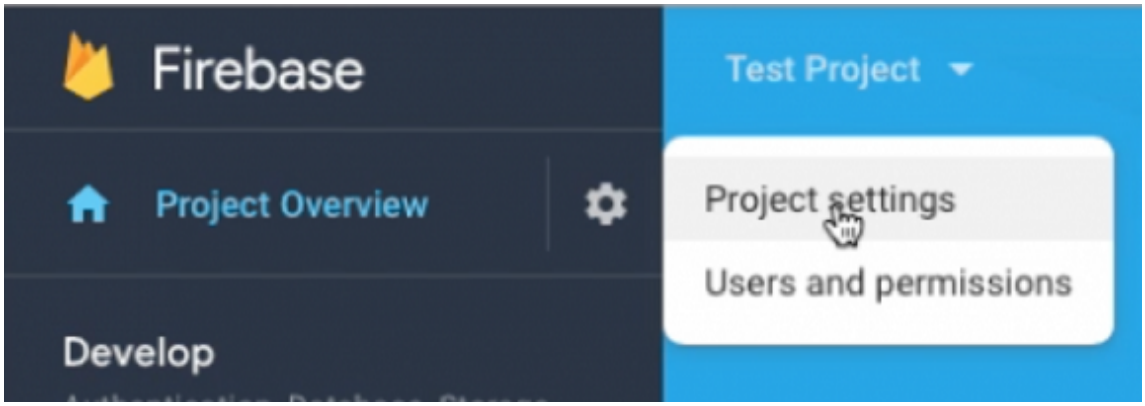
1. Google デベロッパーアカウントの資格情報を使用して次の URL にサインインします:

   https://console.firebase.google.com/

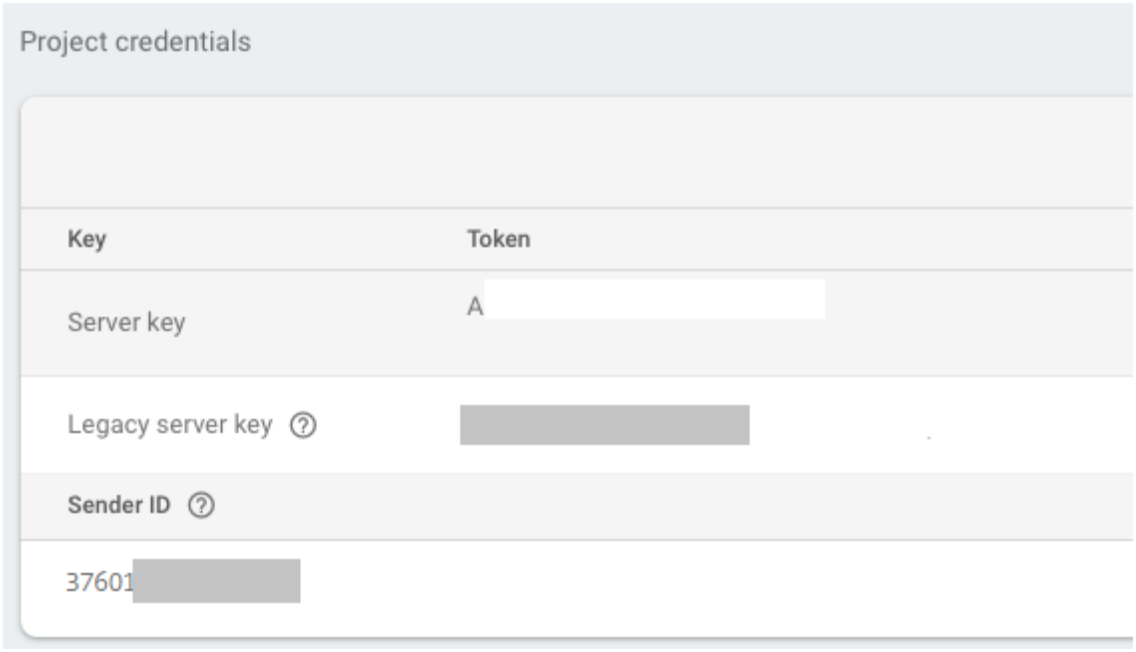
2. [**Add project**] をクリックします。



3. プロジェクトを作成したら、［**Project settings**］をクリックします。



4. ［**Cloud Messaging**］タブを選択します。［**Server key**］および［**Sender ID**］の値をコピーします。次の手順で、これらの値を XenMobile コンソールに貼り付けます。2016 年 10 月時点では、Firebase コンソールでサーバーキーを作成する必要があります。

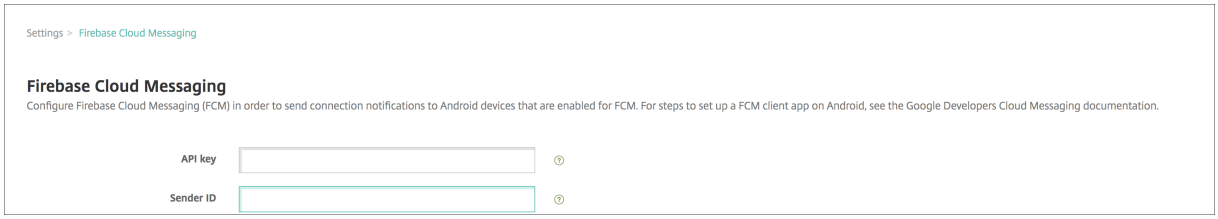


Android で FCM クライアントアプリをセットアップする手順については、Google Developers Cloud Messaging の記事https://firebase.google.com/docs/cloud-messaging/android/clientを参照してください。

XenMobile を FCM 用に構成するには

XenMobile コンソールで、［設定］**>**［**Firebase Cloud Messaging**］ の順に選択します。

- ［**API** キー］ を編集して、Firebase Cloud Messaging 構成の最後の手順でコピーした Firebase Cloud Messaging の **Server key** を入力します。
- ［送信者 **ID**］ を編集して、前の手続きでコピーした送信者 **ID** 値を入力します。

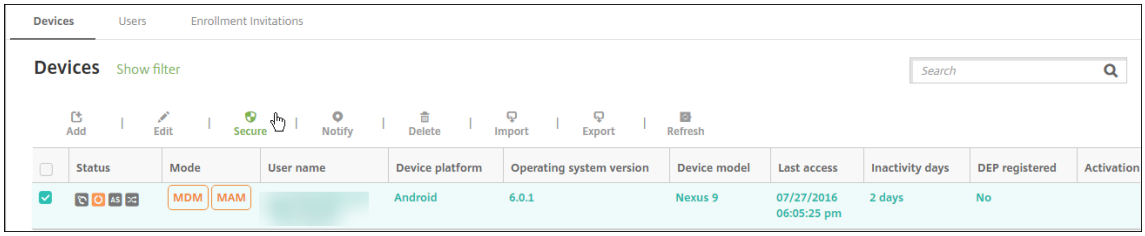


セットアップを完了後は、接続スケジュールデバイスポリシーを削除するか、接続頻度を下げるようにポリシーを変更できます。

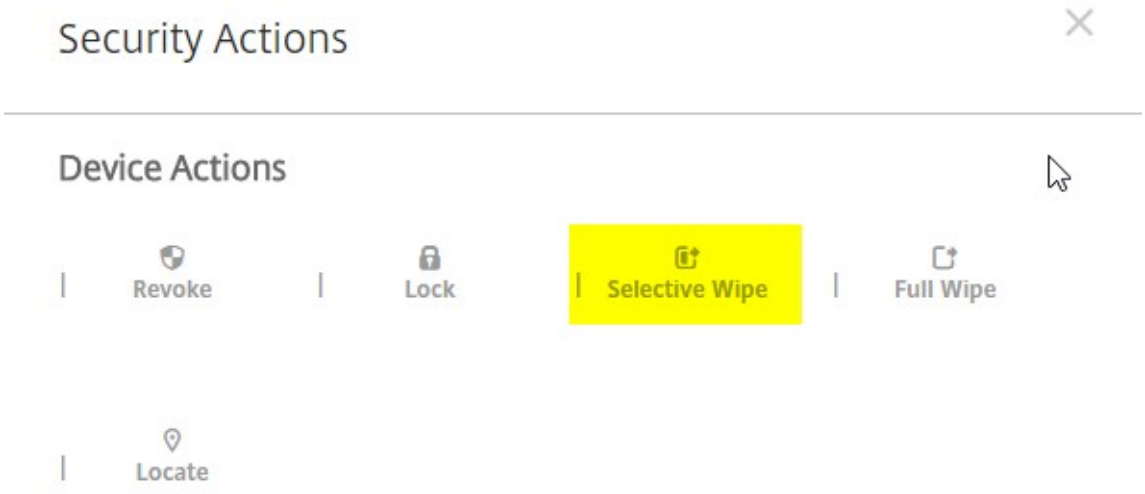
構成をテストするには

1. Android デバイスを登録します。
2. このデバイスを XenMobile から切断するため、少しの時間アイドル状態にします。

3. XenMobile コンソールにサインインして ［管理］ をクリックし、Android デバイスを選択して ［保護］ をクリックします。



4. ［デバイス操作］ で、 ［選択的なワイプ］ をクリックします。



正常に構成されている場合、XenMobile に再接続せずにデバイスで選択的なワイプが行われます。

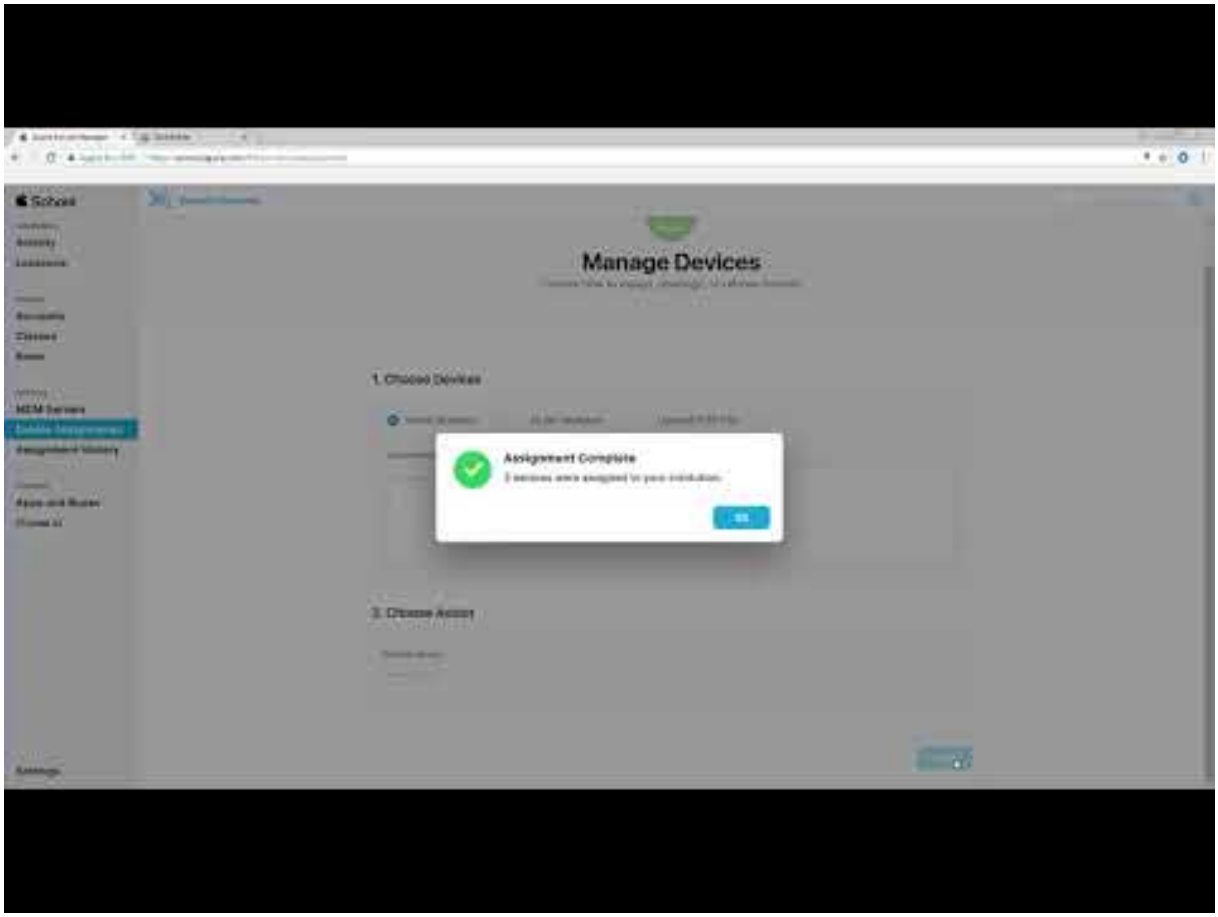
Apple Education 機能との統合

January 10, 2020

Apple Education を使用する環境で、XenMobile Server をモバイルデバイス管理（MDM）ソリューションとして使用できます。XenMobile のサポートには、Apple School Manager や iPad 用のクラスルームアプリが含まれています。XenMobile の教育の構成デバイスポリシーで、Apple の教育向け機能を使用するように講師および生徒のデバイスを構成します。

講師と生徒には事前に構成された監視対象 iPad が提供されます。この構成には、XenMobile での Apple School Manager DEP の登録、新しいパスワードで構成された管理対象 Apple ID アカウント、および必須の VPP アプリと iBooks が含まれます。

次のビデオでは、Apple School Manager と XenMobile Server に対して行う変更のクイックツアーを提供しています。



XenMobile による Apple の教育向け機能のサポートの概要をお伝えします。

Apple School Manager

Apple School Manager は、教育機関で使用する iOS デバイスと macOS ラップトップコンピューターのセットアップ、展開、管理を可能にするサービスです。Apple School Manager に含まれる Web ベースのポータルを使用することで、IT 管理者は次のことが可能になります:

- 異なる MDM サーバーへの DEP デバイスの割り当て
- アプリと iBooks の VPP ライセンスの購入
- 管理対象 **Apple ID** の一括作成。これらのカスタマイズされた Apple ID を使用することで、iCloud Drive でのドキュメントの保存、iTunes コースへの登録などの、Apple サービスを利用できます。

Apple School Manager は、教育向け DEP の一種です。XenMobile は、ビジネス向け DEP と Apple School Manager の登録の両方をサポートします。

XenMobile Server には複数の Apple School Manager DEP アカウントを追加できます。たとえば、この機能によって、教育の単位や学部ごとに異なる登録設定、設定補助オプションが利用できるようになります。追加後、各 DEP アカウントをさまざまなデバイスポリシーに関連付けることができます。

Apple School Manager DEP アカウントを XenMobile コンソールに追加すると、XenMobile はクラスおよび名簿情報を取得します。デバイスのセットアップ時に、XenMobile Server は以下を行います:

- デバイスを登録します。
- デバイスポリシー（教育の構成、ホーム画面のレイアウトなど）などの、展開用に構成されたリソースをインストールします。また、VPP を通じて購入されたアプリと iBooks もインストールします。

その後、事前に構成されたデバイスを講師と生徒に提供します。デバイスを紛失した場合や盗難に遭った場合は、MDM の紛失モード機能を使用してデバイスをロックしたり検索したりすることができます。

iPad 用クラスルームアプリ

iPad 用クラスルームアプリを使用すると、講師は生徒のデバイスに接続してデバイスを管理できます。デバイス画面を表示したり、iPad でアプリを開いたり、Web リンクを共有して開いたり、生徒の画面を Apple TV に表示したりすることができます。

クラスルームアプリは、App Store で無料で入手できます。XenMobile コンソールにアプリをアップロードします。次に教育の構成デバイスポリシーを使用して、講師のデバイスに展開するクラスルームアプリを構成します。

Apple の教育向け機能について詳しくは、Apple の「教育」サイトおよび「教育用導入ガイド」を参照してください。

前提条件

- NetScaler Gateway
- Enterprise モード（XME、MDM+MAM とも呼ばれます）または MDM モードで構成された XenMobile Server XenMobile Server が XME または MDM モードですでに構成されている場合は、Apple School Manager と使用できます。
- Apple iPad 第 3 世代（最小バージョン）、または iOS 9.3（最小バージョン）を実行する iPad Mini

注:

- XenMobile Server は、LDAP または Active Directory に対する Apple School Manager ユーザーアカウントの検証を行いません。ただし、XenMobile Server を LDAP または Active Directory に接続して、Apple School Manager の講師や生徒と関連付けられていないユーザーとデバイスを管理できます。たとえば、Active Directory を使用して、そのほかの Apple School Manager メンバー（IT 管理者やマネージャーなど）に Secure Mail と Secure Web を提供できます。
- Apple School Manager の講師と生徒はローカルユーザーであるため、彼らのデバイスに Citrix Secure Hub を展開する必要はありません。
- NetScaler Gateway の認証を含む MAM 登録では、ローカルユーザーはサポートされません（Active Directory ユーザーのみ）。このため、XenMobile は講師と生徒のデバイスに必須の VPP アプリと iBooks のみを展開します。

共有 **iPad** の前提条件

- iPad Pro、iPad 第 5 世代、iPad Air 2 以降、iPad mini 4 以降
- 32GB 以上のストレージ容量
- 監視

Apple School Manager と **XenMobile Server** の構成

Apple、Apple 正規販売店、または通信事業者から iPad を購入したら、このセクションのワークフローに従って、Apple School Manager アカウントとデバイスをセットアップします。このワークフローには、Apple School Manager ポータルと XenMobile コンソールで実行する手順が含まれています。

この手順に従って、1 対 1 モデル（学生 1 人当たり 1 つの iPad）で使用するすべての iPad、または講師の iPad（非共有）の統合を構成します。共有 iPad を構成するには、「共有 iPad の構成」を参照してください。

手順 **1**: **Apple School Manager** アカウントを作成し、セットアップアシスタントを完了する

Apple Deployment Program からアップグレードする場合は、Apple サポートの記事「Apple School Manager へのアップグレードに備える」を参照してください。Apple School Manager アカウントを作成するには、https://school.apple.com/にアクセスし、指示に従って登録します。Apple School Manager への初回ログオン時に、セットアップアシスタントが開きます。

- Apple School Manager の前提条件、セットアップアシスタント、および管理タスクについて詳しくは、「Apple School Manager ヘルプ」を参照してください。
- Apple School Manager のセットアップには、Active Directory のドメイン名とは異なるドメイン名を使用します。例えば、Apple School Manager のドメイン名には「**appleid**」のようなプレフィックスを付けます。
- Apple School Manager を名簿データに接続すると、Apple School Manager によって講師と生徒の管理対象 Apple ID が作成されます。名簿データには講師、生徒、およびクラスを含めるようにします。Apple School Manager への名簿データの追加について詳しくは、「Apple School Manager ヘルプ」の「職員、生徒、クラスの検索」の記事を参照してください。
- 「Apple School Manager ヘルプ」の「管理対象 Apple ID」で説明されているように、管理対象 Apple ID の形式を所属機関に合わせてカスタマイズできます。

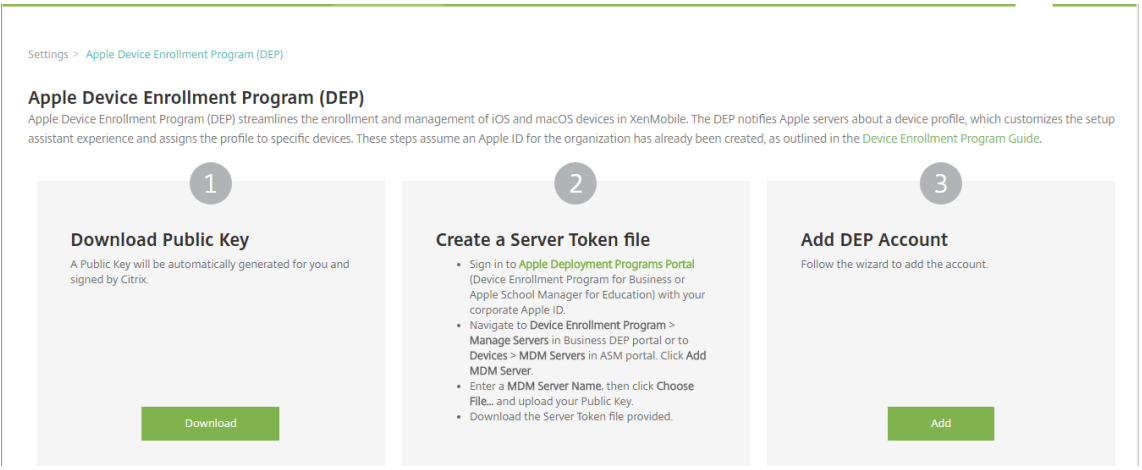
  > 重要:
  >
  > Apple School Manager 情報を XenMobile Server にインポートした後に、管理対象 Apple ID を変更しないでください。

- 正規販売店や通信事業者を通じてデバイスを購入した場合は、Apple School Manager にデバイスをリンクします。詳しくは、「Apple School Manager ヘルプ」の「デバイスの管理」の記事を参照してください。

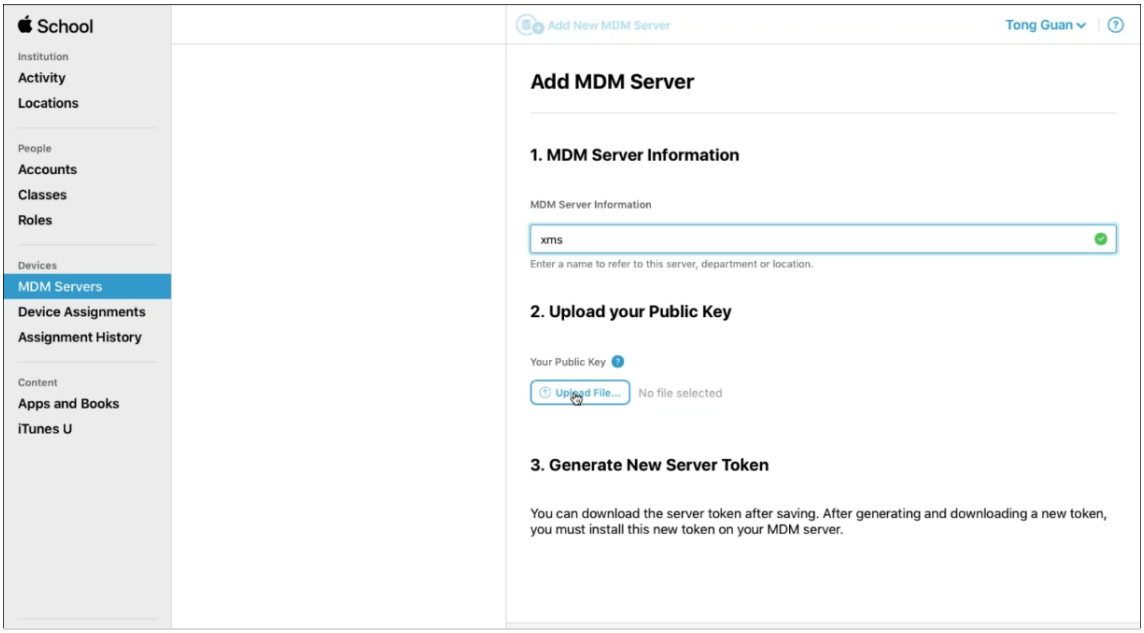
手順 **2**: **XenMobile Server** を **Apple School Manager** の **MDM Server** として構成し、デバイスの割り当てを構成する

Apple School Manager ポータルには［**MDM** サーバ］タブが含まれています。このセットアップを完了するには、XenMobile Server の公開キーファイルが必要です。

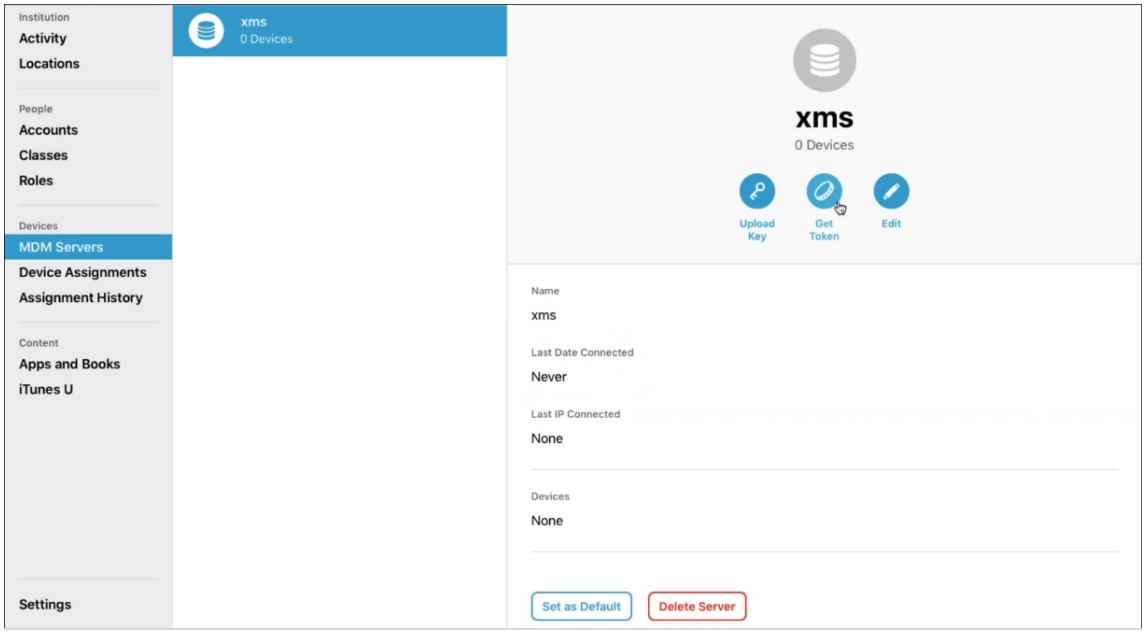
1. 次の手順を実行して、XenMobile Server の公開キーをローカルコンピューターにダウンロードします。XenMobile コンソールにログオンし、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］の順に選択します。



2. ［**Download Public Key**］の下にある［**Download**］をクリックして PEM ファイルを保存します。
3. Apple School Manager ポータルで **“MDM** サーバ**”** をクリックし、XenMobile Server の名前を入力します。入力するサーバーの名前は参考用であり、サーバー URL やサーバー名ではありません。
4. ［パブリックキーのアップロード］の下にある［ファイルのアップロード］をクリックします。



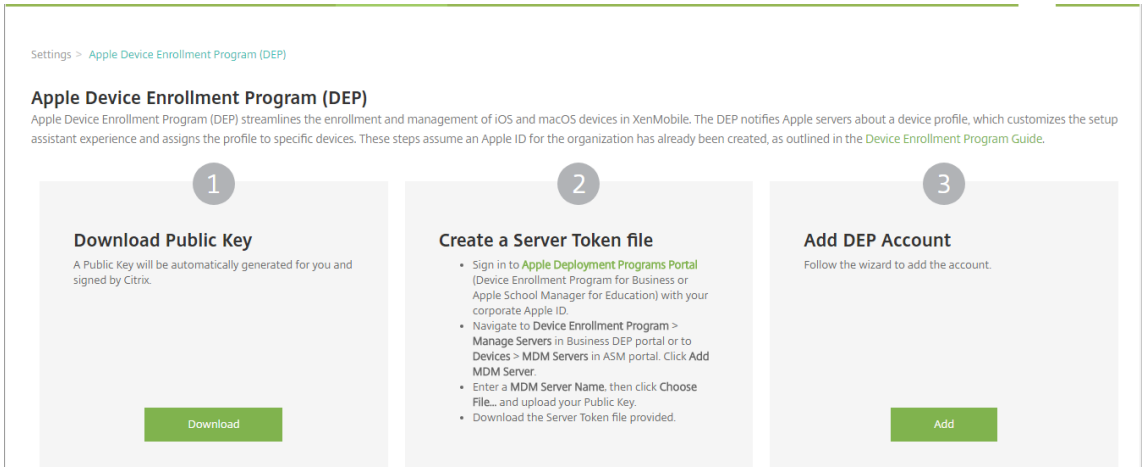
5. XenMobile Server からダウンロードしたサーバーキーをアップロードして、**“保存”** をクリックします。
6. サーバートークンを生成します。［トークンの取得］ をクリックし、コンピューターにサーバートークンファイルをダウンロードします。



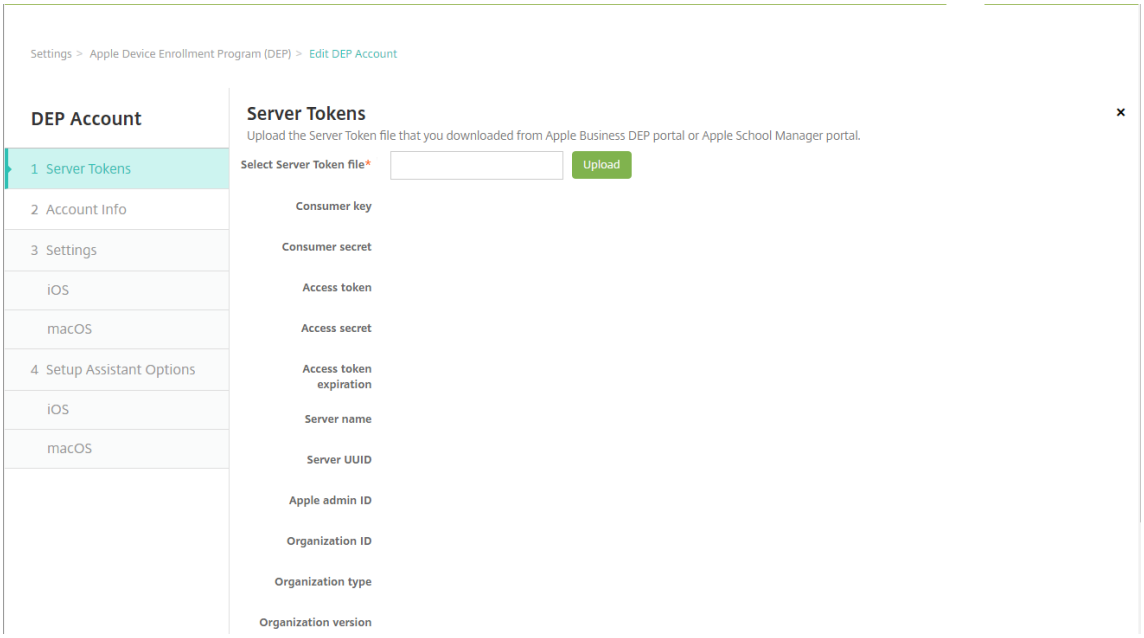
7. ［デバイスの割り当て］ をクリックし、どのようにデバイスを割り当てるかを選択して求められる情報を入力します。詳しくは、「Apple School Manager ヘルプ」の「デバイスの割り当て」を参照してください。
8. ［アクションの実行］ メニューの ［アクションの選択］ で、［サーバに割り当て］ をクリックします。次に、**“MDM** サーバ**”** メニューで、デバイスの管理に “XenMobile Server” をクリックしたあと、**“完了”** をクリックします。

手順 **3**: **Apple School Manager** アカウントを **XenMobile Server** に追加する

1. XenMobile コンソールで、［設定］ **>** ［**Apple** デバイス登録プログラム（**DEP**）］ に移動し、［**DEP** アカウントの追加］ の ［追加］ をクリックします。



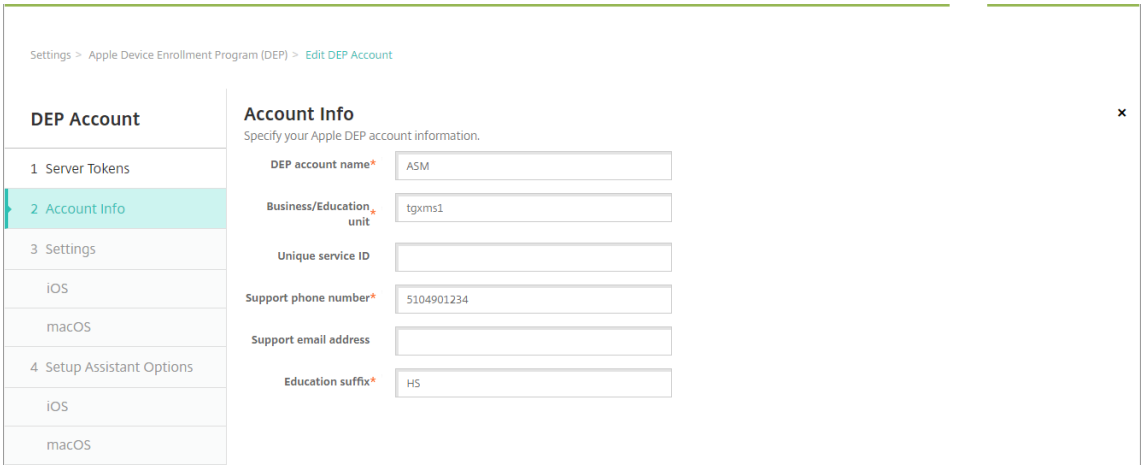
2. ［サーバートークン］ ページで、［アップロード］ をクリックし、Apple School Manager ポータルからダウンロードしたサーバートークン（.p7m）ファイルを選択します。トークンの情報が表示されます。



注：

- 組織の **ID** は、DEP の顧客 ID です。
- Apple School Manager アカウントでは、［組織の種類］ は教育、［組織のバージョン］ は **v2** です。

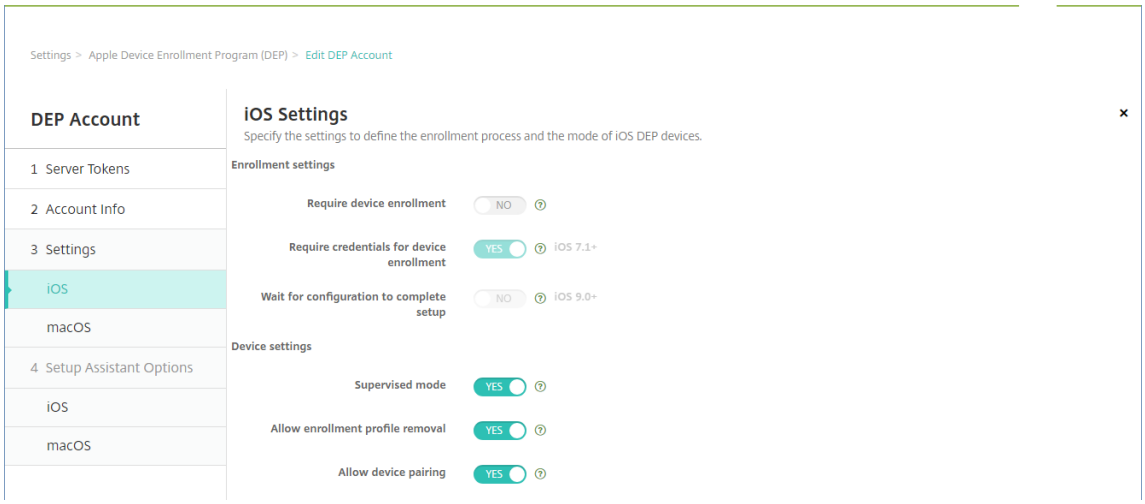
3. ［アカウント情報］ ページで次の設定を入力します。



- **DEP** アカウント名： この DEP アカウントの一意の名前。国や組織構造など、DEP アカウントの分類を示す名前を付けます。
- 事業/教育単位： デバイスを割り当てる教育の単位や学部です。このフィールドは必須です。
- 一意のサービス **ID**： アカウントの識別に役立つオプションの一意の ID です。

- サポート用電話番号: ユーザーがセットアップ時にサポートが必要となった場合に連絡するサポートの電話番号。このフィールドは必須です。
- サポート用メールアドレス: エンドユーザーが使用できるサポート用のメールアドレス（オプション）。
- 教育機関のサフィックス: 特定の Apple School Manager DEP アカウントのクラスのフラグを設定します（VPP のサフィックスは、VPP アカウントのアプリと iBooks のフラグを設定します）。Apple School Manager DEP と Apple School Manager VPP の両方のアカウントで、同じサフィックスを使用することをお勧めします。

4. ［次へ］ をクリックします。［**iOS** 設定］ で次の設定を入力します。

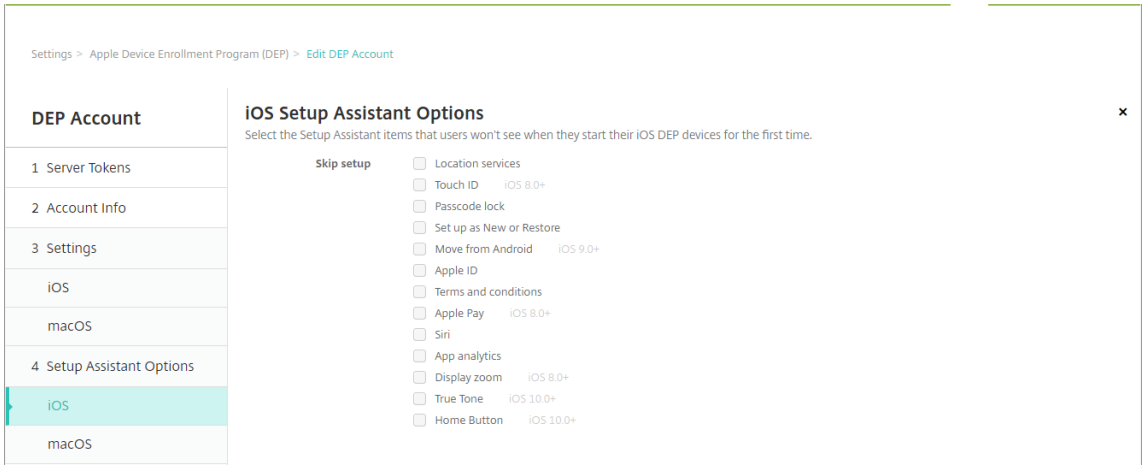


- 登録設定
  - デバイス登録を必須にする: ユーザーにデバイスの登録を要求します。この設定を ［いいえ］ に変更します。
  - デバイス登録のための資格情報を求める: DEP のセットアップ時にユーザーに資格情報の入力を要求します。Apple School Manager と XenMobile Server の統合では、この設定はデフォルトで ［はい］ になっています。
  - セットアップを完了するため構成を待機する: すべての MDM リソースがユーザーデバイスに展開されるまで、デバイスをセットアップアシスタントモードのままにしておく必要があるかどうか。Apple School Manager と XenMobile Server の統合では、この設定はデフォルトで ［いいえ］ になっています。Apple のドキュメントによると、デバイスがセットアップアシスタントモードの間は以下のコマンドが機能しない場合があります。
    * InviteToProgram
    * InstallApplication
    * InstallMedia
    * ApplyRedemptionCode
- デバイス設定

- 監視モード： iOS デバイスを監視モードにします。デフォルトの ［はい］ を変更しないでください。iOS デバイスを Supervised モードにする方法について詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。
- 登録プロファイルの削除を許可： Apple School Manager の統合で、ユーザーがデバイスから登録プロファイルを削除できるようにします。この設定を ［はい］ に変更します。
- デバイスのペアリングを許可： Apple School Manager の統合では、デバイスのペアリングを許可して iTunes と Apple Configurator を通じてデバイスを管理できるようにします。この設定を ［はい］ に変更します。

5. ［**iOS** セットアップアシスタントオプション］ で、ユーザーが初めてデバイスを起動するときにスキップする iOS セットアップアシスタントの手順を選択します。デフォルトでは、セットアップアシスタントにはすべての手順が含まれています。セットアップアシスタントから手順を削除すると、ユーザーエクスペリエンスが簡素化されます。

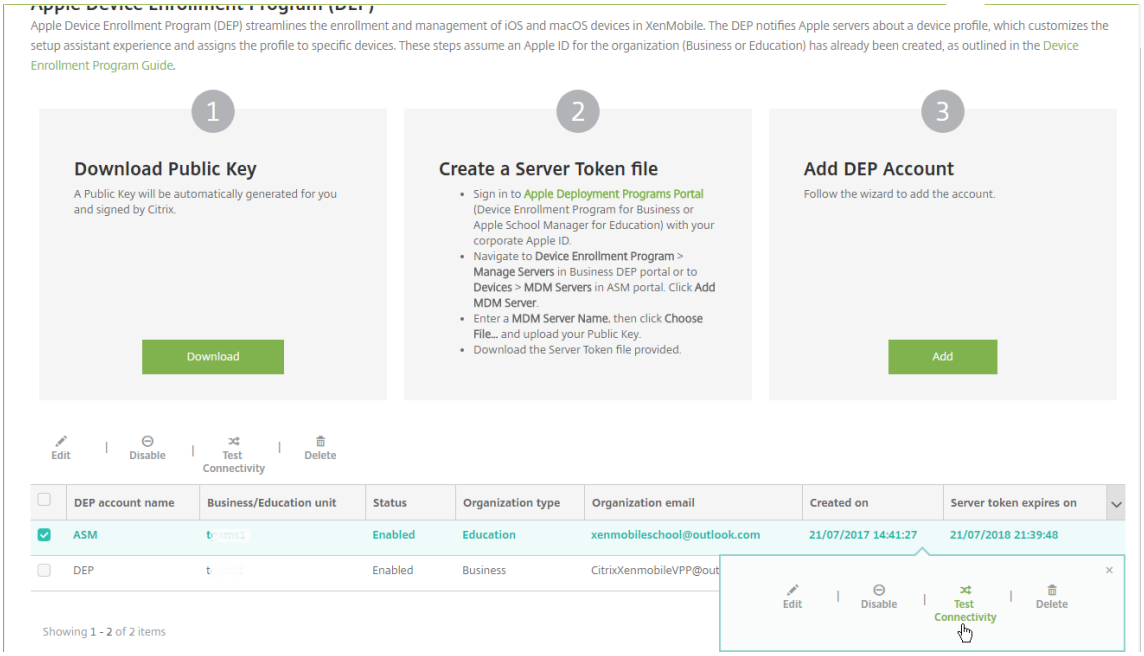
   > 重要：
   >
   > **Apple ID** と使用条件の手順は含めることを強くお勧めします。これらの手順により、講師と生徒は管理対象 Apple ID の新しいパスワードを入力して、要求される使用条件を受け入れることができます。



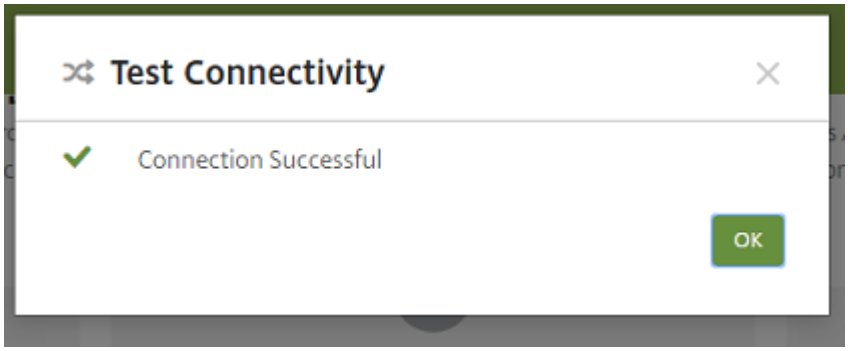
   - 位置情報サービス： デバイスに位置情報サービスを設定します。
   - **Touch ID**： iOS 8.0 以降のデバイスに Touch ID を設定します。
   - パスコードロック： デバイスのパスコードを作成します。
   - 新規としてセットアップまたは復元： 新規に、または iCloud か iTunes のバックアップからデバイスを設定します。
   - **Android** から移動： Android デバイスから iOS 9 以降のデバイスへのデータ転送を有効にします。このオプションは、 ［新規としてセットアップまたは復元］ がオンの場合（すなわち、手順をスキップする場合）にのみ使用できます。
   - **Apple ID**： デバイスの Apple ID アカウントを設定します。チェックボックスをオンにして、この手順を含めることをお勧めします。

- 使用条件： デバイスの使用契約条件に対する同意をユーザーに要求します。チェックボックスをオンにして、この手順を含めることをお勧めします。
- **Apple Pay**： iOS 8.0 以降のデバイスに Apple Pay を設定します。
- **Siri**： デバイスで Siri を使用するかどうかを選択します。
- **App Analytics**： クラッシュデータおよび使用状況の統計情報を Apple と共有するかどうかを設定します。
- ディスプレイズーム： iOS 8.0 以降のデバイスにディスプレイ解像度（標準またはズーム）を設定します。
- **True Tone**： iOS 10.0 デバイス（最小バージョン）に True Tone ディスプレイを設定します。
- ホームボタン： iOS 10.0 デバイス（最小バージョン）に、ホームボタンの画面の感度を設定します。

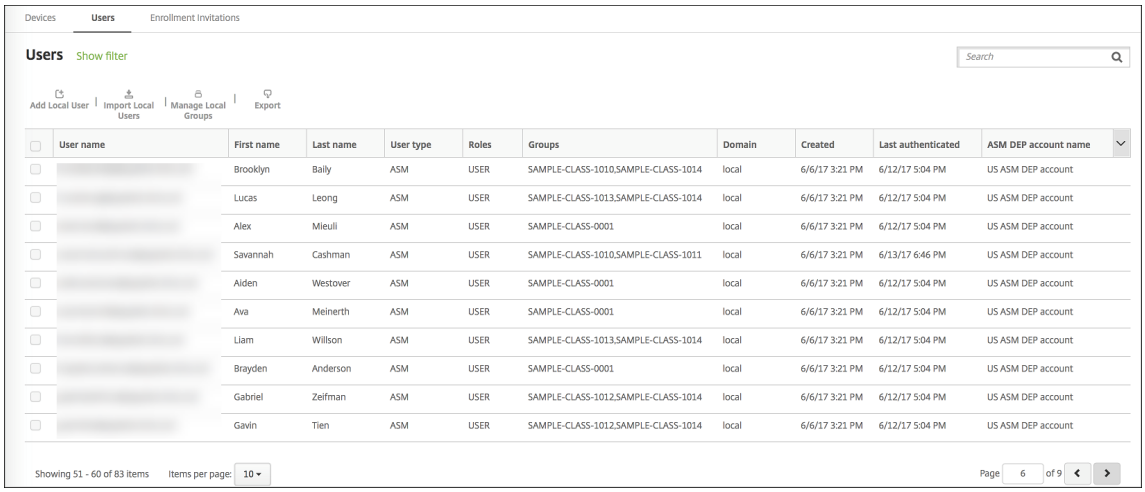
6. DEP アカウントを表示するには、［設定］**>**［**Apple** デバイス登録プログラム（**DEP**）］ に移動します。アカウントを選択して ［接続性をテスト］ をクリックし、XenMobile Server と Apple School Manager 間の接続をテストします。



状態を示すメッセージが表示されます。



数分後に、Apple School Manager のユーザーアカウントが ［管理］**>** ［ユーザー］ ページに表示されます。XenMobile Server では、インポートされた各ユーザーの管理対象 Apple ID に基づいて、ローカルユーザーアカウントが作成されます。次の例では、ユーザーアカウント用にカスタマイズされた Apple ID で、ドメイン名のプレフィックスが **appleid** になっています。

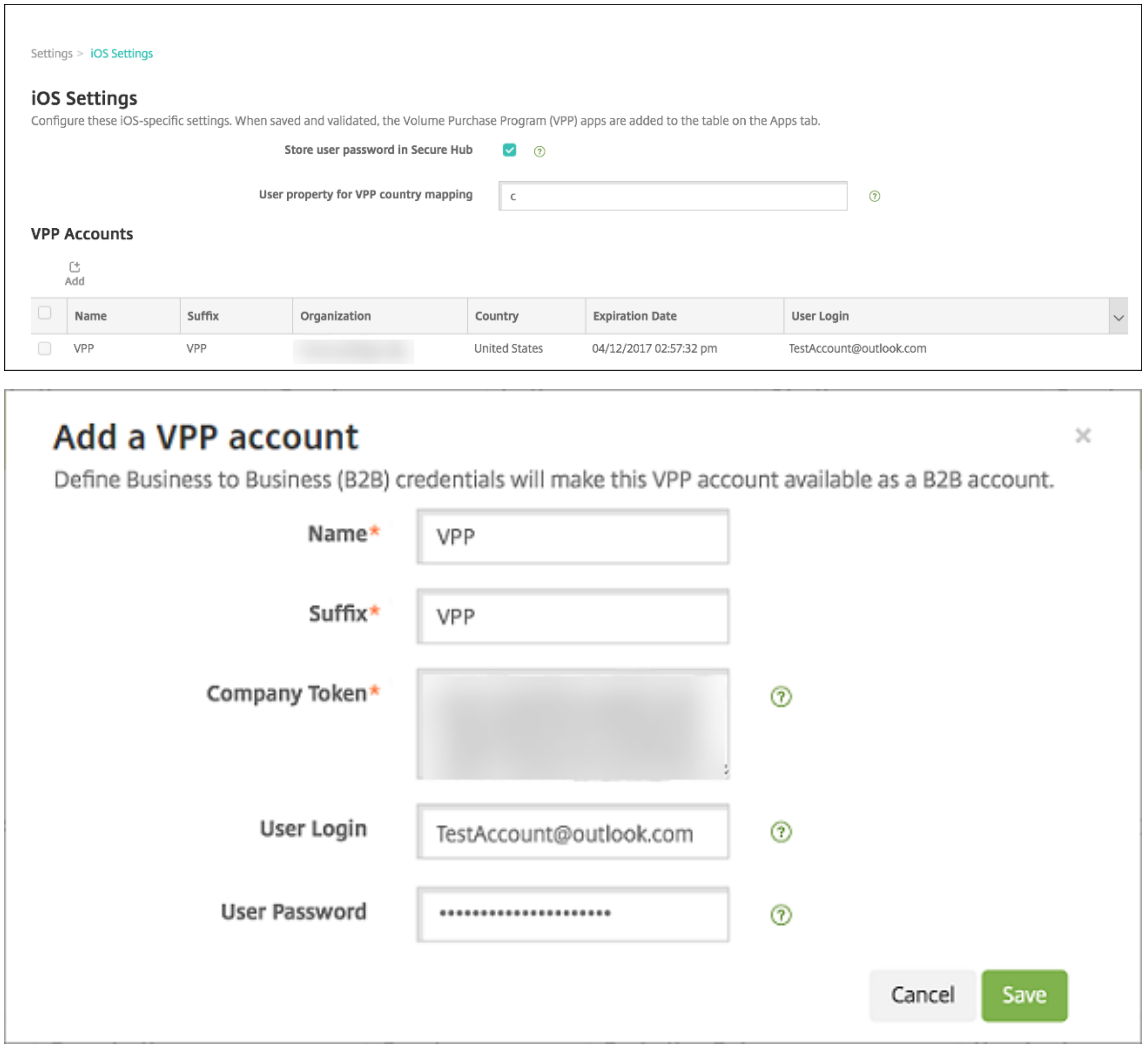


特定の Apple School Manager DEP アカウントのすべてのユーザーを検索するには、ユーザー検索のフィルターにアカウント名を入力します。

手順 **4**: **Apple School Manager** の教育用 **VPP** アカウントを構成する

このセクションでは、XenMobile が、アプリと iBooks の VPP ライセンス購入に使用される VPP アカウントを指すように構成します。

1. Apple School Manager 向けの教育用 VPP アカウントを構成するには、「iOS Volume Purchase Program」の指示に従います。[VPP アカウントの追加] 画面では、会社トークンを入力する必要があります。教育用 VPP アカウント（https://volume.apps.apple.com/us/store）から直接トークンをダウンロードして、［**VPP** アカウントの追加］ 画面に貼り付けます。



2. VPP ライセンスが XenMobile Server にインポートされるまで数分間待ちます。

手順 **5**: **Apple School Manager** ユーザーのパスワードを追加する

Apple School Manager DEP アカウントが追加されると、XenMobile Server が Apple School Manager からクラスとユーザーをインポートします。XenMobile はクラスをローカルグループとして扱い、コンソール内で「グループ」の用語が使用されます。Apple School Manager でグループ名があるクラスには、XenMobile によってグループ名が割り当てられます。それ以外の場合、XenMobile ではグループ名にソースシステム ID を使用します。Apple School Manager のコース名は一意でないため、XenMobile ではクラス名にコース名を使用しません。

XenMobile は管理対象 Apple ID を使用して、ユーザーの種類が **ASM** のローカルユーザーを作成します。Apple School Manager では、すべての外部データソースとは別に資格情報が作成されるため、ユーザーはローカルです。そのため、XenMobile ではこれらの新しいユーザーの認証にディレクトリサーバーを使用しません。

Apple School Manager は、一時的なユーザーパスワードを XenMobile Server に送信しません。CSV ファイルからインポートするか、手動で追加します。一時的なユーザーパスワードをインポートするには、次の手順を実行し

ます:

1. 管理対象 Apple ID の一時的なパスワードを作成するときに Apple School Manager によって生成された CSV ファイルを取得します。
2. CSV ファイルを編集し、一時的なパスワードを、XenMobile Server への登録でユーザーが入力した新しいパスワードに置き換えます。この目的では、パスワードの種類に対する制約はありません。

   以下の形式で CSV ファイルに入力します:`firslast@appleid.citrix.com,Firstname,Middle,Lastname,Citrix123!`

   各項目の意味は次の通りです:

   ユーザー: `firstlast@appleid.citrix.com`

   名: `Firstname`

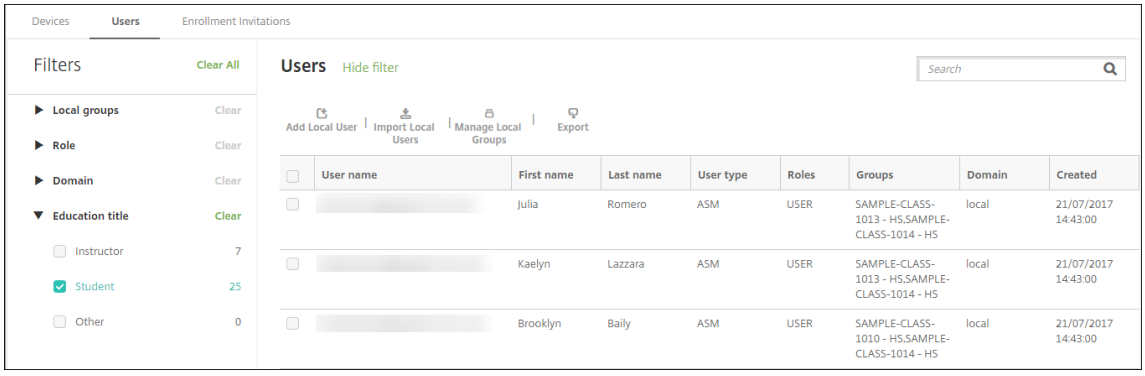
   ミドルネーム: `Middle`

   姓: `Lastname`

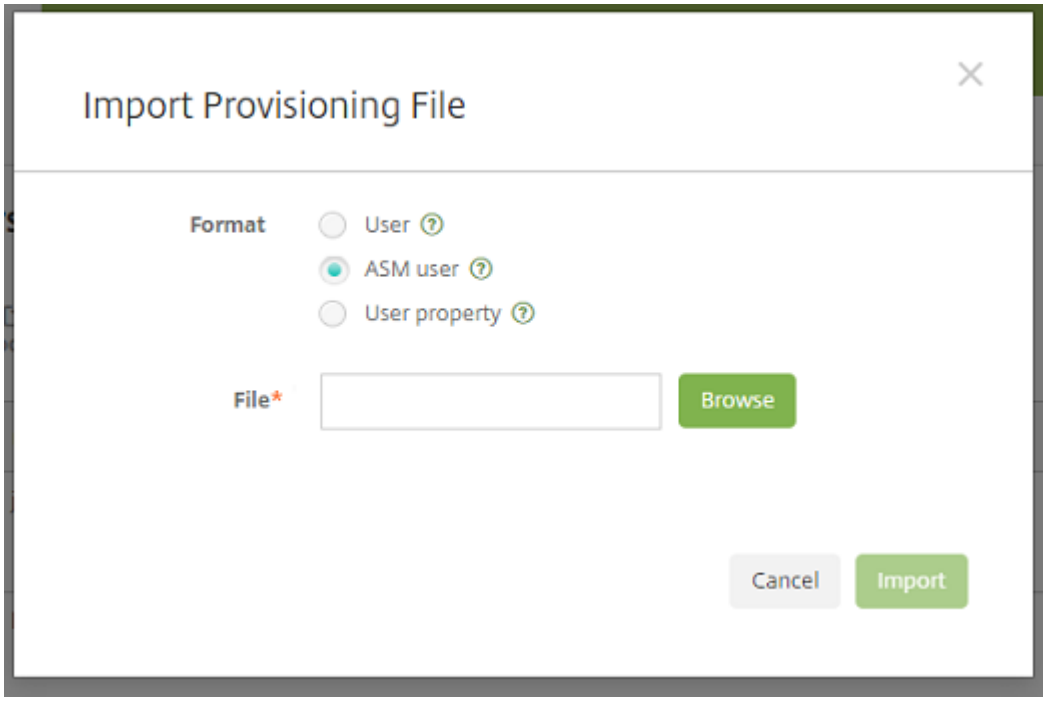
   パスワード: `Citrix123!`
3. XenMobile コンソールで、［管理］**>**［ユーザー］ の順にクリックします。［ユーザー］ ページが開きます。

   次の ［管理］**>**［ユーザー］ 画面の例では、Apple School Manager からインポートされたユーザー一覧が表示されています。［ユーザー］ 一覧には以下のように表示されます。

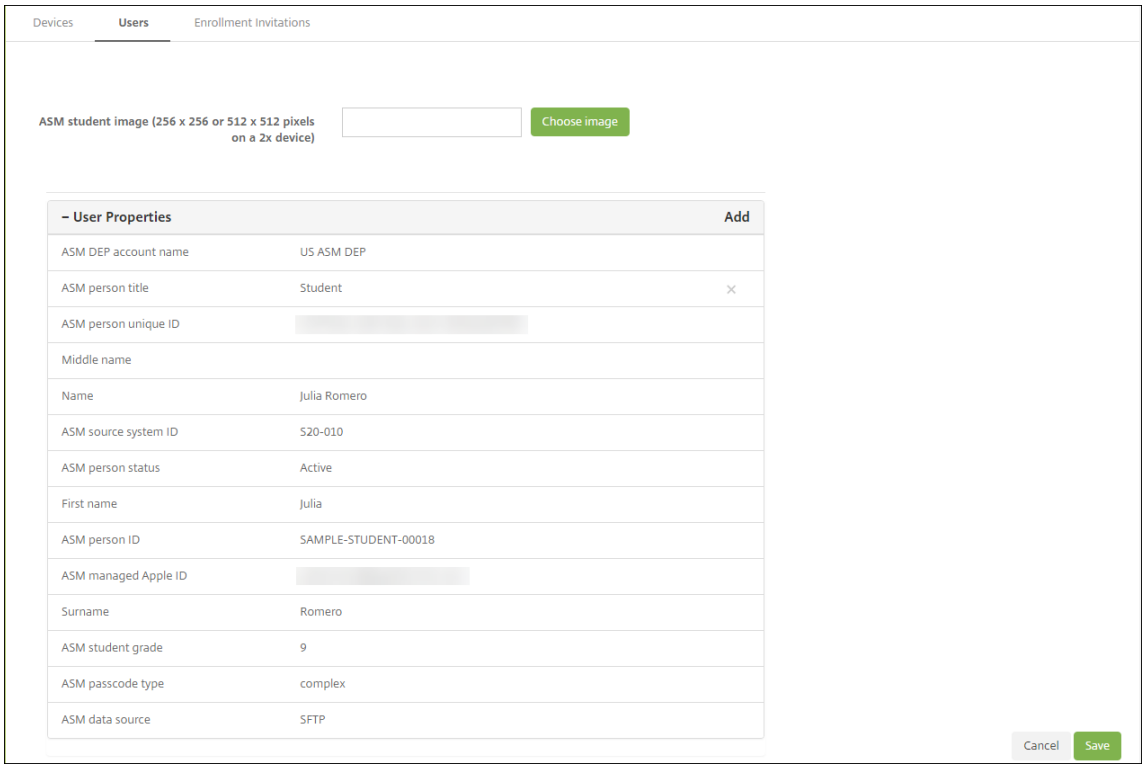
   - ［ユーザー名］ には管理対象 Apple ID が表示されます。
   - ［ユーザーの種類］の **ASM** は、Apple School Manager 由来のアカウントであることを示しています。
   - ［グループ］ にはクラスが表示されます。



4. ［ローカルユーザーのインポート］ をクリックします。［プロビジョニングファイルのインポート］ ダイアログボックスが開きます。
5. ［形式］では ［**ASM** ユーザー］ を選択し、手順 2 で準備した CSV ファイルに移動して、［インポート］ をクリックします。



6. ローカルユーザーのプロパティを表示するには、該当するユーザーを選択して ［編集］ をクリックします。



名前のプロパティのほかに、Apple School Manager の以下のプロパティが表示されます。

- **ASM DEP** アカウント： XenMobile Server でアカウントに付けた名前です。
- **ASM** の個人の役職： 講師、生徒、そのほかのいずれかです。

- **ASM** の一意の個人 **ID**： ユーザーの識別子です。
- **ASM** のソースシステム **ID**： 所属組織によってユーザーに構成された ID です。
- **ASM** の個人の状態：管理対象 Apple ID がアクティブか非アクティブかを指定します。管理対象 Apple ID アカウントにユーザーが新しいパスワードを入力すると、この状態がアクティブになります。
- **ASM** の管理対象 **Apple ID**： 管理対象 Apple ID には、所属機関名と **appleid** を含めることができます。たとえば、ID は johnappleseed@appleid.myschool.edu のようになります。XenMobile Server では、管理対象 Apple ID の認証が要求されます。
- **ASM** の生徒の学年： 生徒の学年情報です（講師は使用しません）。
- **ASM** のパスコードの種類： 複合（8 つ以上の英数字で構成された生徒以外のパスワード）、**4**（桁）、または **6**（桁）の、個人のパスワードポリシーです。
- **ASM** のデータソース： クラスのデータソース（**CSV** または **SFTP** など）です。

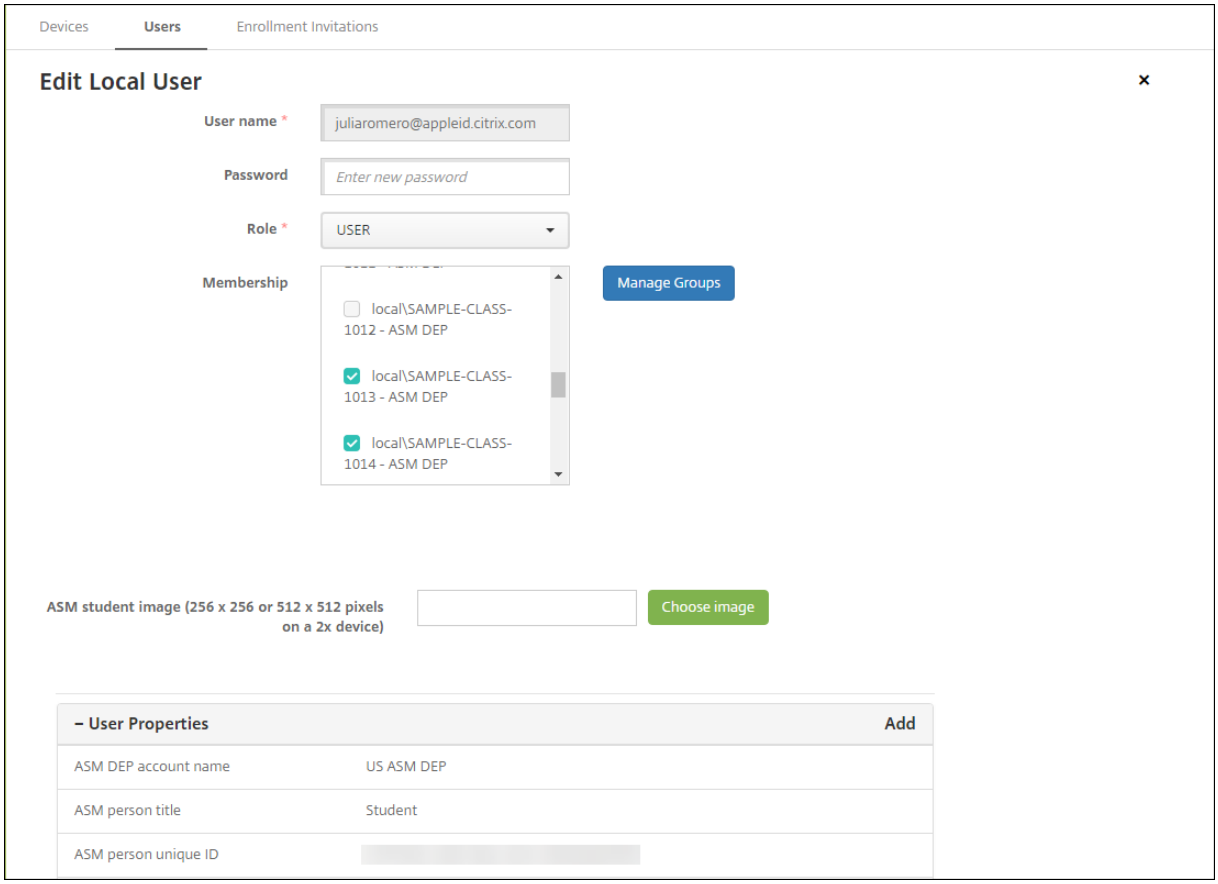
手順 **6**：必要に応じて生徒の写真を追加する

各生徒の写真を追加できます。講師が Apple のクラスルームアプリを使用すると、アプリに写真が表示されます。

写真の推奨事項は次のとおりです：

- 解像度：256 x 256 ピクセル（2x デバイスで 512 x 512 ピクセル）
- 形式：JPEG、PNG、または TIFF

写真を追加するには、［管理］**>**［ユーザー］ の順に選択し、ユーザーを選択して、［編集］、［イメージを選択］ の順にクリックします。



手順 **7**: リソースとデリバリーグループを計画して **XenMobile Server** に追加する

デリバリーグループで、ユーザーのカテゴリに展開するリソースを指定できます。たとえば、講師と生徒のデリバリーグループを 1 つ作成できます。または、複数のデリバリーグループを作成して、さまざまな講師や生徒に送信するアプリ、メディア、ポリシーをカスタマイズできます。クラスごとに 1 つまたは複数のデリバリーグループを作成できます。また、マネージャー（教育機関のそのほかの職員）のデリバリーグループを 1 つまたは複数作成することもできます。

ユーザーデバイスに展開するリソースには、デバイスポリシー、VPP アプリ、および iBooks が含まれます。

- デバイスポリシー:

  講師がクラスルームアプリを使用する場合は、教育の構成デバイスポリシーが必要です。そのほかのデバイスポリシーを確認して、講師と生徒の iPad をどのように構成および制限するかを決定します。

- VPP アプリ:

  XenMobile では、VPP アプリを必須アプリとして教育ユーザーに展開する必要があります。XenMobile Server では、このような VPP アプリをオプションとして展開することはサポートされません。

  Apple のクラスルームアプリを使用する場合は、講師のデバイスにのみ展開します。

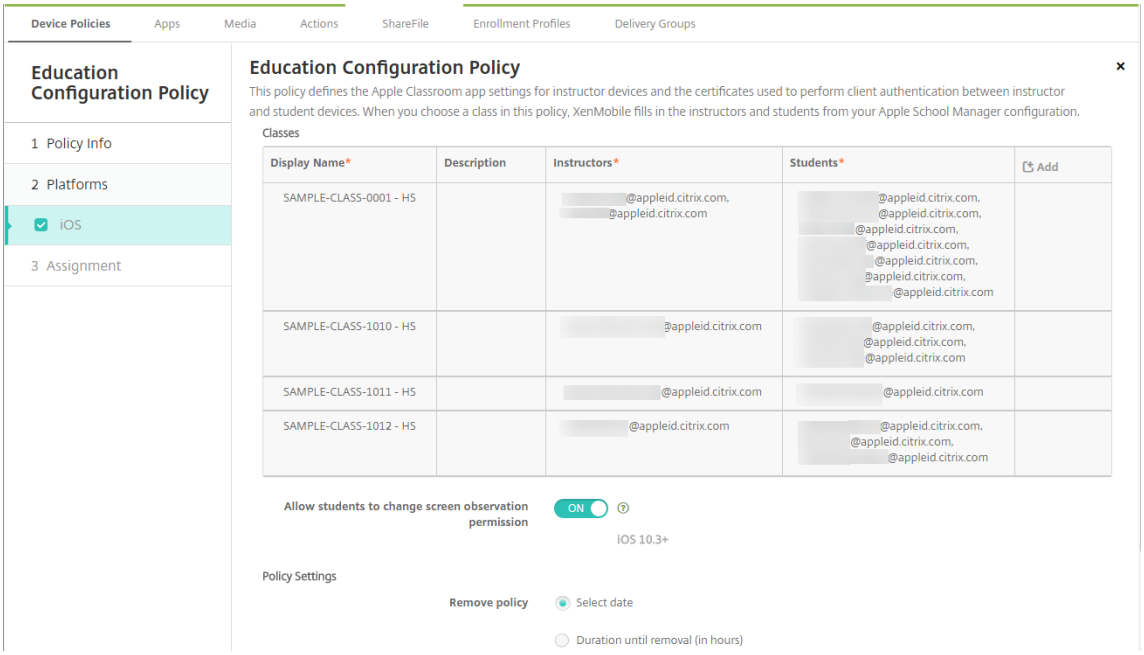
講師や生徒に提供するそのほかのアプリを展開します。このソリューションでは Citrix Secure Hub アプリを使用しないため、講師や生徒に展開する必要はありません。

- VPP iBooks:

  XenMobile Server を Apple School Manager VPP アカウントに接続すると、XenMobile コンソールの［構成］>［メディア］ に、購入した iBooks が表示されます。このページに一覧表示された iBooks を、デリバリーグループに追加できます。XenMobile Server では、iBooks を必須メディアとしてのみ追加できます。

講師および生徒のリソースとデリバリーグループを計画したら、XenMobile コンソールでこれらのアイテムを作成できます。

1. 講師または生徒のデバイスに展開するデバイスポリシーを作成します。教育の構成デバイスポリシーについて詳しくは、「Education の構成デバイスポリシー」を参照してください。

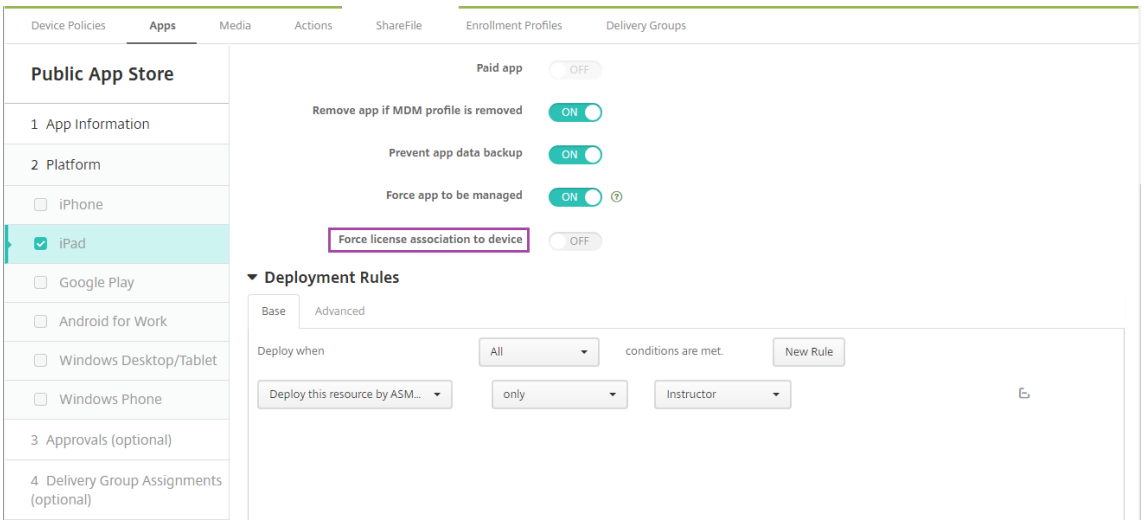


   デバイスポリシーについて詳しくは、「デバイスポリシー」および個々のポリシーに関する記事を参照してください。

2. アプリ（［構成］>［アプリ］）と iBooks（［構成］>［メディア］ ）を構成します。

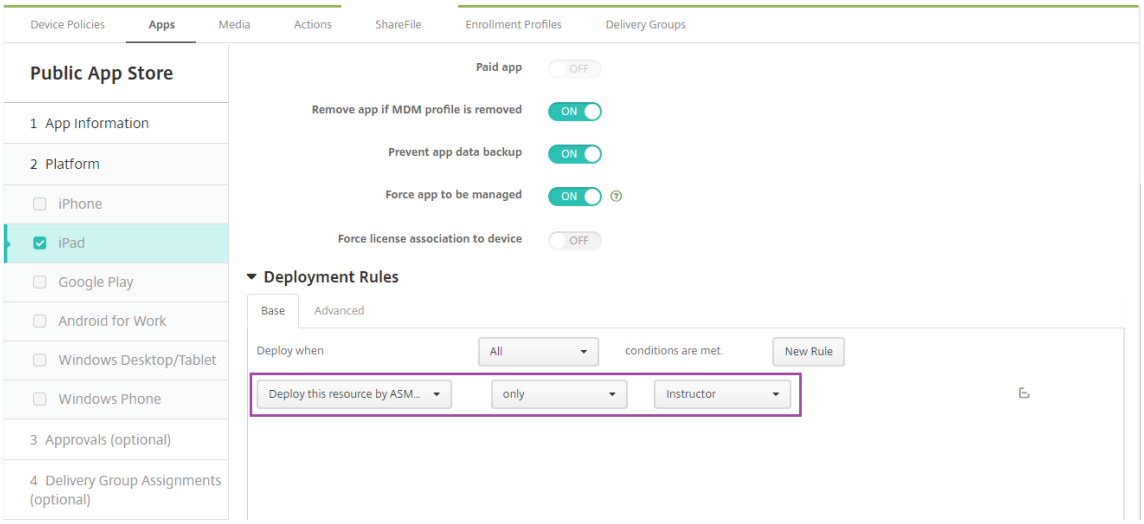
   - デフォルトで、XenMobile はアプリと iBooks をユーザーレベルで展開します。初回展開時に、VPP への登録を求めるメッセージが講師と生徒に送信されます。招待状を受け入れると、ユーザーは次回展開時（6 時間以内）に VPP アプリと iBooks を受信します。新規 VPP ユーザーに、アプリと iBooks の強制展開を適用することをお勧めします。これを実行するには、デリバリーグループを選択して ［展開］ をクリックします。

     デバイスレベルで、アプリ（iBooks は除く）の割り当てを選択できます。これを実行するには、［デバイスへの強制ライセンス割り当て］ の設定を ［オン］ に変更します。デバイスレベルでアプリを割り当てる場合、VPP プログラム参加の招待状はユーザーに送信されません。



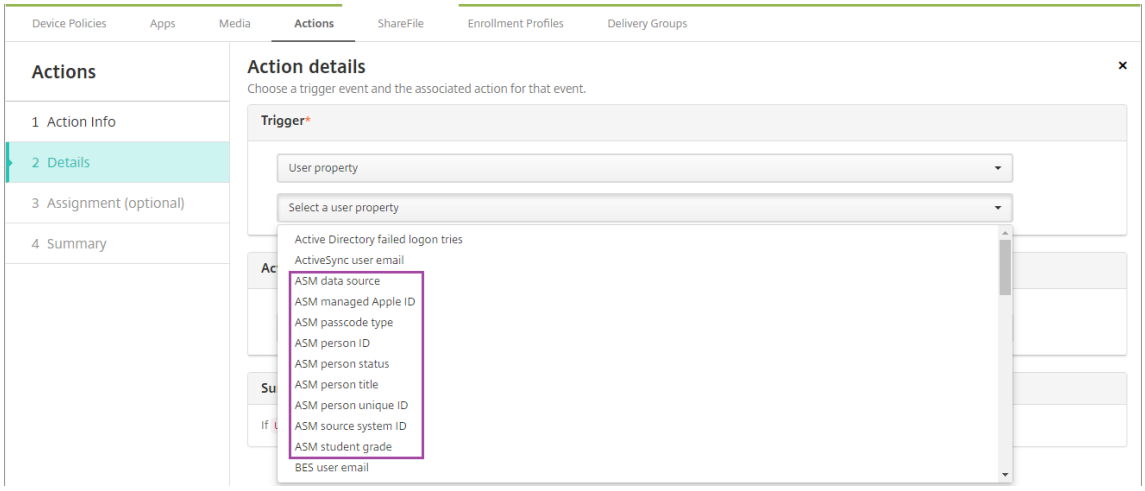
- 講師にのみアプリを展開するには、講師のみを含むデリバリーグループを選択するか、次の展開規則を使用します。

```
Deploy this resource by ASM DEP device type
only
Instructor
```



- VPP アプリの追加方法について詳しくは、「パブリックアプリストアのアプリの追加」を参照してください。

3. オプションです。Apple School Manager のユーザープロパティに基づいてアクションを作成します。たとえば、新しいアプリのインストール時に生徒のデバイスに通知を送信するアクションを作成できます。または、次の例に示すように、ユーザープロパティによってトリガーされるアクションを作成できます。

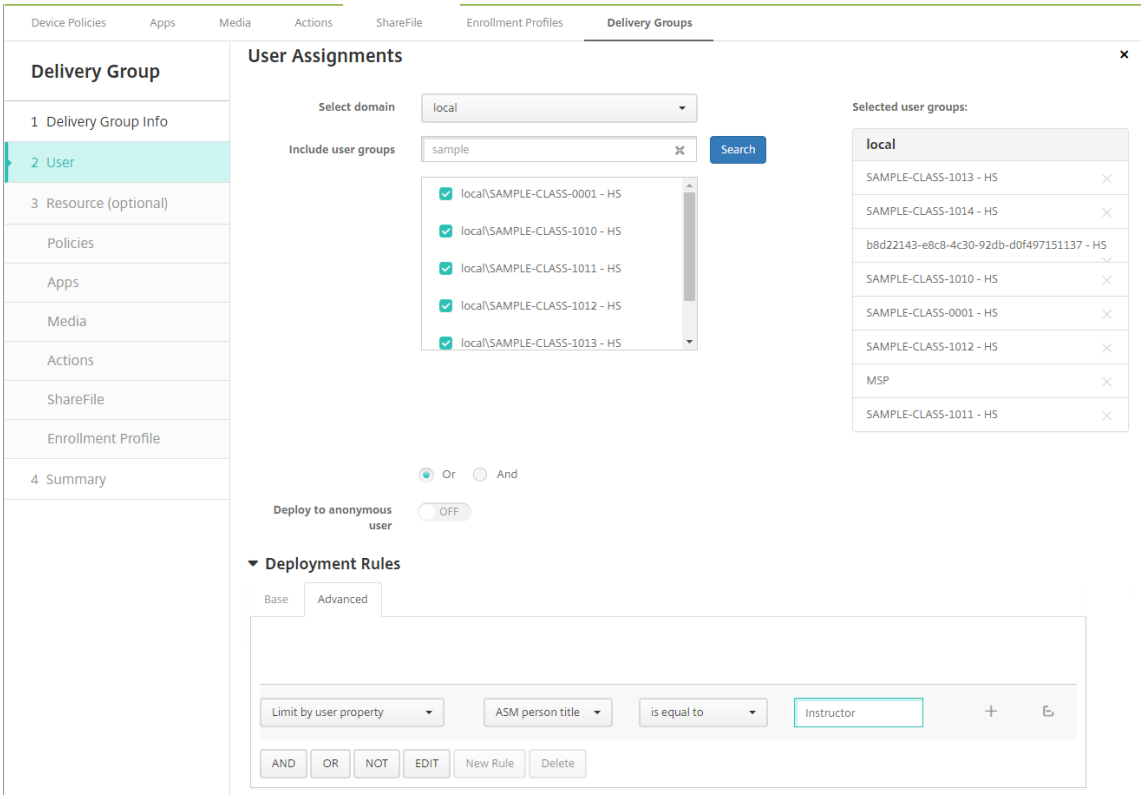


アクションを作成するには、［構成］**>**［アクション］ の順に選択します。アクションの構成について詳しくは、「自動化された操作」を参照してください。

4. ［構成］**>**［デリバリーグループ］ の順に選択し、講師と生徒のデリバリーグループを作成します。Apple School Manager からインポートしたクラスを選択します。また、講師と生徒の展開規則も作成します。

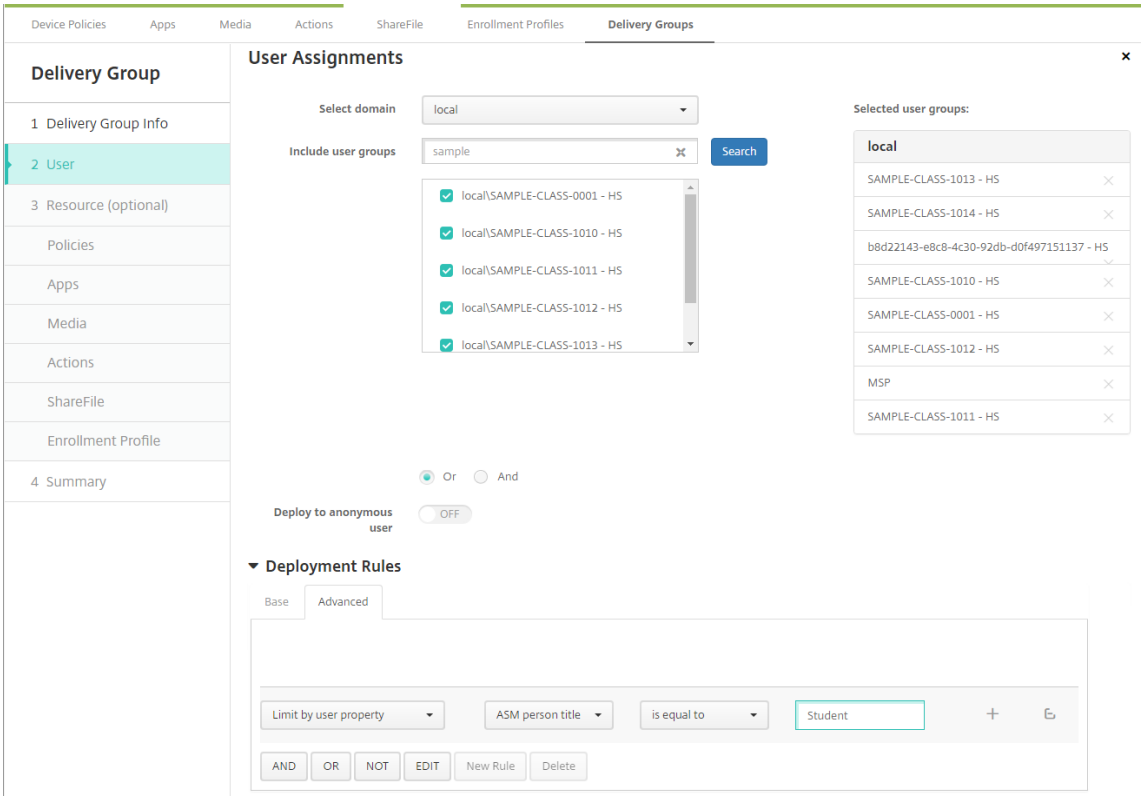
   たとえば、講師のユーザー割り当てを次に示します。展開規則は次のとおりです。

```
Limit by user property
ASM person title
is equal to
Instructor
```

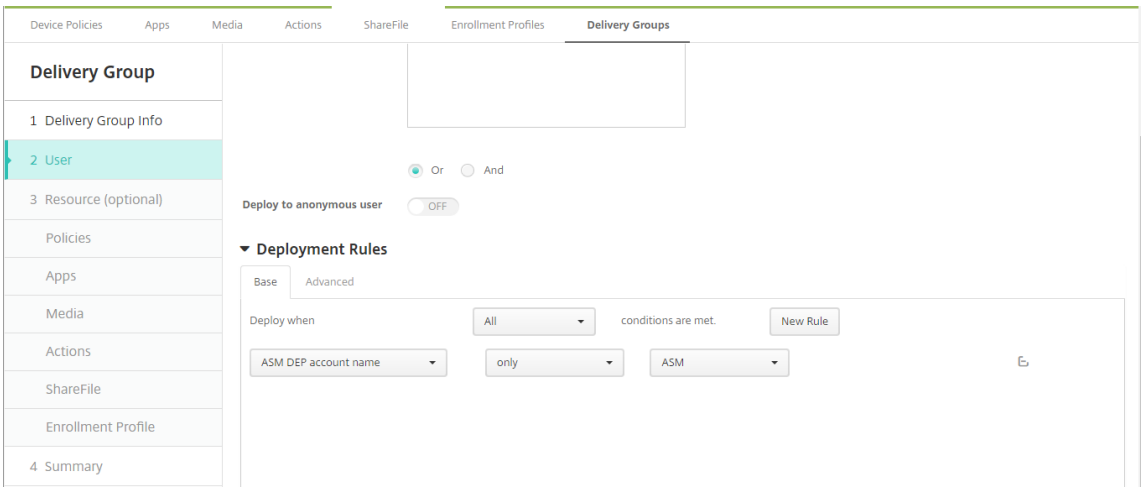



生徒のユーザー割り当てを次に示します。展開規則は次のとおりです。

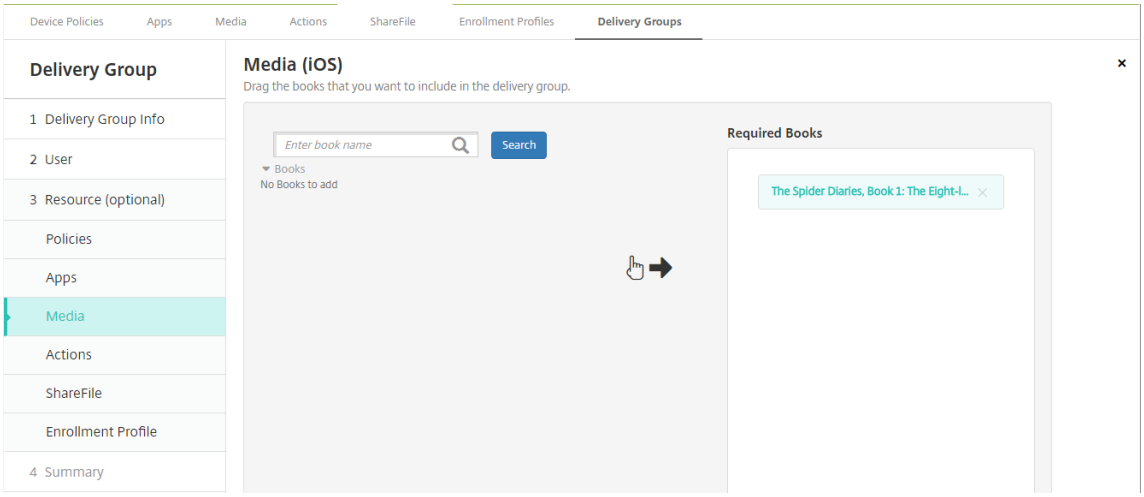
```
Limit by user property
ASM person title
is equal to
Student
```

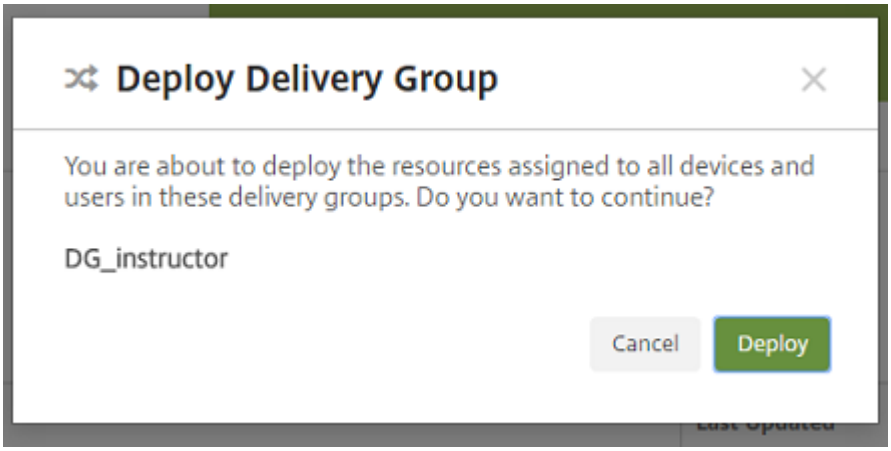
Apple School Manager DEP アカウント名に基づく展開規則を使用して、デリバリーグループをフィルター処理することもできます。



5. リソースをデリバリーグループに割り当てます。次の例は、デリバリーグループに含まれる iBook を示しています。



次の例は、デリバリーグループを選択して ［展開］ をクリックすると開く確認ダイアログボックスを示しています。



詳しくは、「リソースの展開」の「デリバリーグループを編集するには」と「デリバリーグループを展開するには」を参照してください。

手順 **8**: 講師および生徒のデバイス登録をテストする

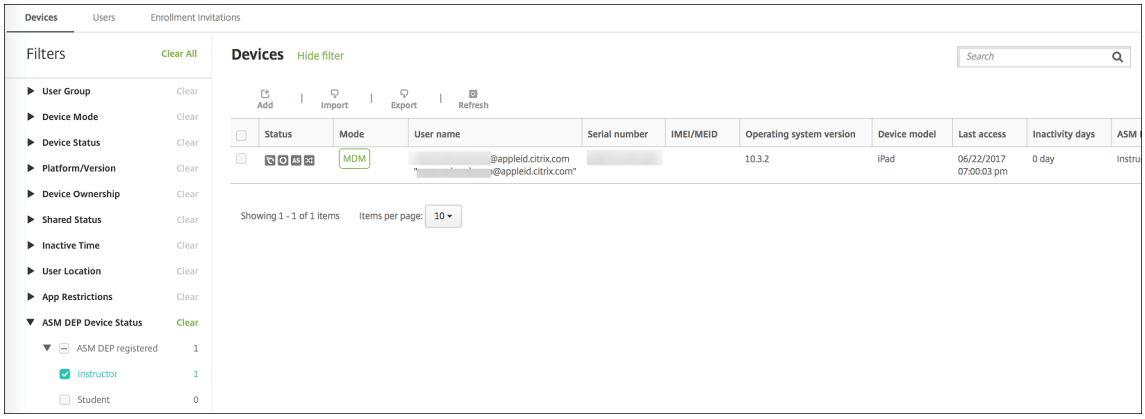
次の方法のいずれかを使用してデバイスを登録できます。

- 学校管理者は、XenMobile コンソールで設定したユーザーパスワードを使用して、講師と生徒のデバイスを登録できます。これにより、アプリとメディアが既にセットアップされたデバイスをユーザーに提供できます。
- デバイスを受け取ったユーザーは、管理者によって提供されたユーザーパスワードを使用して登録します。登録が完了すると、XenMobile Server によってデバイスポリシー、アプリ、およびメディアがデバイスに送信されます。

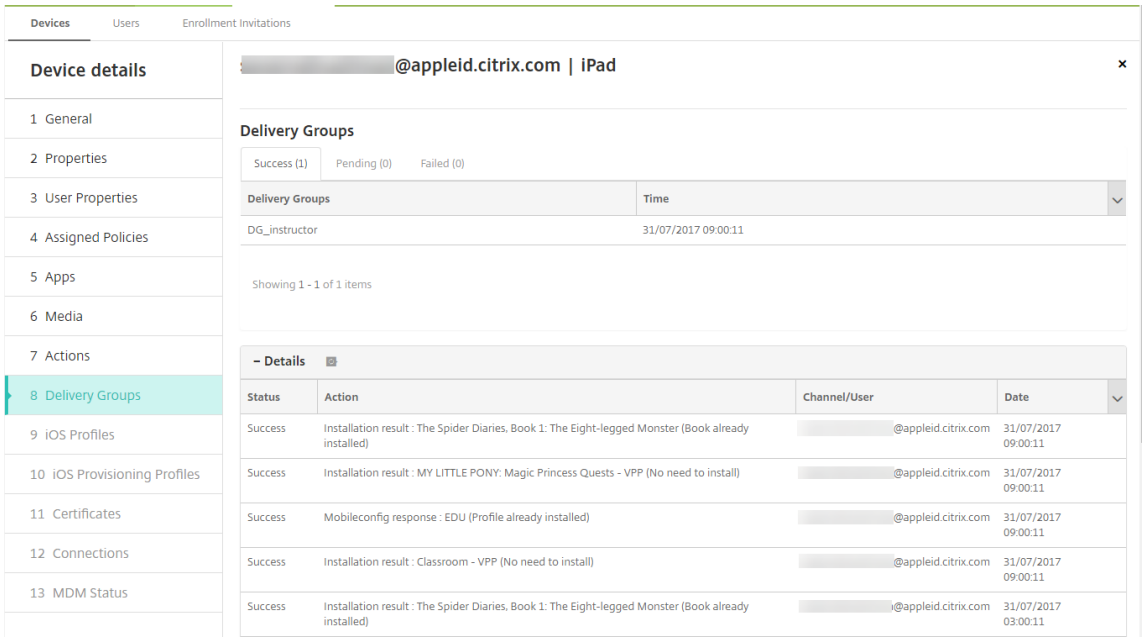
登録をテストするには、Apple School Manager にリンクした DEP デバイスを使用します。

1. デバイスが Apple School Manager にリンクしていない場合は、ハードリセットを実行してデバイスのコンテンツと設定を消去します。
2. 講師の Apple School Manager DEP デバイスを登録します。次に、生徒の Apple School Manager DEP デバイスを登録します。
3. ［管理］ **>** ［デバイス］ ページで、両方の Apple School Manager DEP デバイスが MDM のみに登録されていることを確認します。

   ［デバイス］ ページを、Apple School Manager DEP デバイスの状態（ ［**ASM DEP** が登録されました］、［講師］、 ［生徒］ ）ごとにフィルター処理できます。



4. MDM リソースが各デバイスに適切に展開されたことを確認するには、デバイスを選択し、 ［編集］ をクリックして、各種ページを確認します。



手順 **9**：デバイスの配布

Apple では、講師と生徒にデバイスを配布できるように、イベントをホストすることを推奨しています。

事前登録済みのデバイスを配布しない場合も、これらのユーザーに以下を提供します：

- DEP 登録用の XenMobile Server パスワード
- 管理対象 Apple ID 用の、Apple School Manager の一時的なパスワード。

初回時のユーザーエクスペリエンスは次のとおりです。

1. ハードリセット後にユーザーが初めてデバイスを起動すると、XenMobile により DEP 登録画面でデバイスを登録するように求められます。
2. ユーザーは管理対象 Apple ID と、XenMobile Server への認証に使用する XenMobile Server パスワードを入力します。
3. Apple ID のセットアップ手順で、管理対象 Apple ID と Apple School Manager の一時的なパスワードの入力を求めるメッセージがデバイスに表示されます。これらの項目によって、Apple サービスへのユーザー認証が行われます。
4. iCloud でのデータの保護に使用される、管理対象 Apple ID のパスワード作成を求めるメッセージがデバイスに表示されます。
5. セットアップアシスタントの終了時に、XenMobile Server によりデバイスへのポリシー、アプリ、メディアのインストールが開始されます。ユーザーレベルで割り当てられるアプリと iBooks については、講師と生徒に VPP への登録を促すメッセージがセットアップアシスタントにより表示されます。招待状を受け入れると、ユーザーは次回展開時（6 時間以内）に VPP アプリと iBooks を受信します。

共有 **iPad** の構成

クラスルーム内の複数の生徒は、1 人または複数の講師が教えているさまざまな科目について、iPad を共有できます。

管理者か講師が共有 iPad を登録し、デバイスポリシー、アプリ、メディアをデバイスに展開します。その後、生徒が管理対象 Apple ID の資格情報を入力して共有 iPad にサインインします。以前生徒に［教育の構成］ポリシーを展開したことがある場合、生徒はデバイスを共有するために「その他のユーザー」としてサインインする必要はありません。

XenMobile Server は共有 iPad：デバイス所有者（講師）用のシステムチャネルおよび現在の常駐ユーザー（生徒）用のユーザーチャネルという 2 つの通信チャネルを使用します。XenMobile Server は、これらのチャネルから Apple がサポートするリソースに対応した適切な MDM コマンドを送信します。

システムチャネル上に展開されるリソースは次のとおりです。

- 教育の構成、ロック画面のメッセージ、最大常駐ユーザー数、パスコードロックの猶予期間などのデバイスポリシー

- デバイスベースの VPP アプリ

  Apple は、共有 iPad でエンタープライズアプリやユーザベースの VPP アプリをサポートしていません。共有 iPad では、アプリはユーザーごとではなく、デバイス全体にインストールされます。

- ユーザーベースの VPP iBook

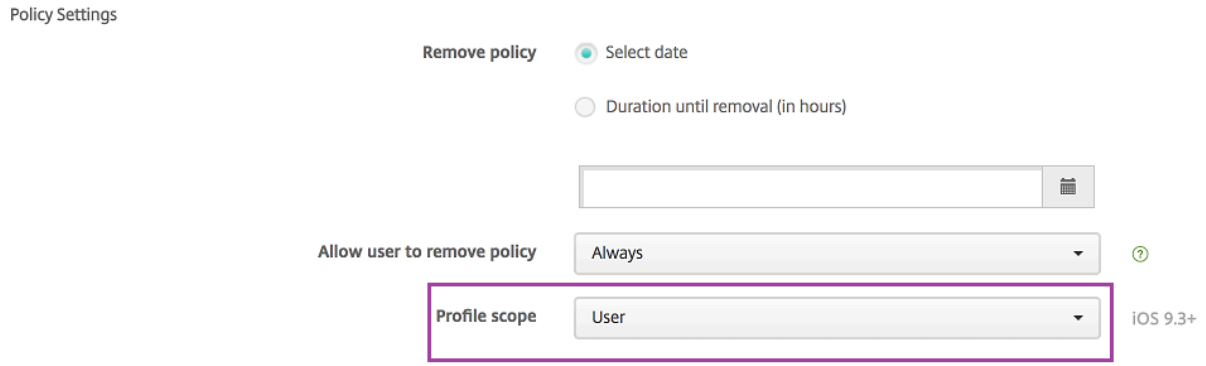
  Apple は、共有 iPad でのユーザーベースの VPP iBooks の割り当てをサポートしています。

ユーザーチャネル上に展開されるリソースは次のとおりです。

- デバイスポリシー：アプリ通知、ホーム画面レイアウト、制限

  XenMobile Server は、ユーザーチャネル上のデバイスポリシーのみをサポートしています。

デバイスポリシーを構成する場合、ポリシー設定の ［プロファイルの対象］ で展開するチャネルを指定します。



ユーザーチャネルで展開したデバイスポリシーを削除する場合、［プロファイルの削除］ポリシーの ［展開範囲］ で［ユーザー］ を選択するようにしてください。

一般的なワークフロー

通常、講師には事前に構成された監視対象共有 iPad が提供されます。講師は生徒に各デバイスを配布します。事前登録済みの共有 iPad を講師に配布しない場合：講師に XenMobile Server のパスワードを提供して、デバイスを登録できるようにしてください。

共有 iPad の構成と登録の一般的なワークフローは次のとおりです。

1. XenMobile Server コンソールで共有モードを有効にして、ASM DEP アカウントを追加します（［設定］**>** ［**Apple** デバイス登録プログラム（**DEP**）］）。詳しくは、「共有 iPad の ASM DEP アカウントを管理する」を参照してください。
2. このセクションで説明するように、必要なデバイスポリシー、アプリ、メディアを XenMobile Server に追加して、これらのリソースをデリバリーグループに割り当てます。
3. 講師に共有 iPad のハードリセットを実行するよう指示します。DEP 登録の［Remote Management］画面が開きます。

4. 講師が共有 iPad を登録します。
   XenMobile Server から、登録済みの各共有 iPad に構成済みのリソースが展開されます。自動再起動後、講師は生徒とデバイスを共有できるようになります。サインインページが iPad に表示されます。
5. 生徒がクラスを選択し、管理対象 Apple ID と一時的な Apple School Manager（ASM）のパスワードを入力します。
   共有 iPad が ASM を認証すると、生徒は ASM パスワードを作成するよう促されます。次回の共有 iPad へのサインインでは、生徒は新しい ASM パスワードを使用します。
6. iPad を共有している別の生徒は、ここまでの手順を繰り返してサインインすることができます。

共有 **iPad** の **ASM DEP** アカウントを管理する

既に Apple の教育向け機能で XenMobile Server を使用している場合：講師が使用するデバイスなど、共有されていないデバイスに対しては、XenMobile Server に既存の ASM DEP アカウントが設定されています。同一の ASM と XenMobile Server を、共有デバイスと非共有デバイスの両方に使用できます。

XenMobile は、次の展開シナリオをサポートしています。

- 1 クラスあたり 1 グループの共有 iPad

  このシナリオでは、複数の共有 iPad を 1 クラスの生徒に割り当てます。iPad はクラスルームにとどまります。そのクラスの各科目の講師達は、同じグループの iPad を使用します。

- 講師 1 人あたり 1 グループの共有 iPad

  このシナリオでは、複数の共有 iPad を 1 人の講師に割り当てます。講師は、授業を行うさまざまなクラスでこれらの iPad を使用します。

共有 **iPad** をデバイスグループにまとめる

ASM によって、複数の MDM サーバーを作成して、デバイスをグループに編成できます。共有 iPad を MDM サーバーに割り当てる時は、クラスごとまたは講師ごとに、共有 iPad のグループのデバイスグループを作成します。

- グループ 1 の共有 iPad> デバイスグループ 1 MDM サーバー
- 共有 iPad のグループ 2> デバイスグループ 2 MDM サーバー
- 共有 iPad のグループ N> デバイスグループ N MDM サーバー

各デバイスグループに **ASM DEP** アカウントを追加する

XenMobile Server コンソールで複数の ASM DEP アカウントを作成すると、クラスごとまたは講師ごとに共有 iPad のグループが 1 つずつ自動的にインポートされます：

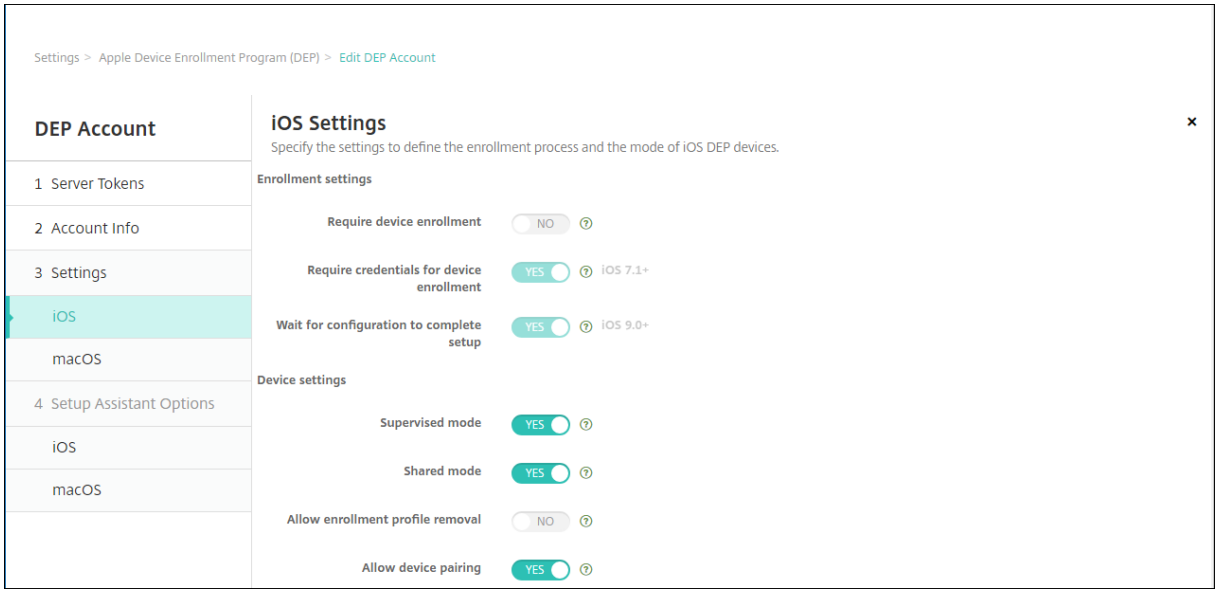
- デバイスグループ 1 MDM サーバー > デバイスグループ 1 DEP アカウント
- デバイスグループ 2 MDM サーバー > デバイスグループ 2 DEP アカウント

- デバイスグループ N MDM サーバー > デバイスグループ N DEP アカウント

共有 iPad に固有の要件は以下のとおりです。

- デバイスグループごとに 1 つの ASM DEP アカウントを用意し、以下の設定を有効にします。
  - デバイス登録を必須にする
  - 監視モード
  - 共有モード
- 同じ教育機関では、すべての ASM DEP アカウントに同じ教育機関のサフィックスを使用してください。

DEP アカウントを追加するには、[設定] > [**Apple** デバイス登録プログラム（**DEP**）] に移動します。

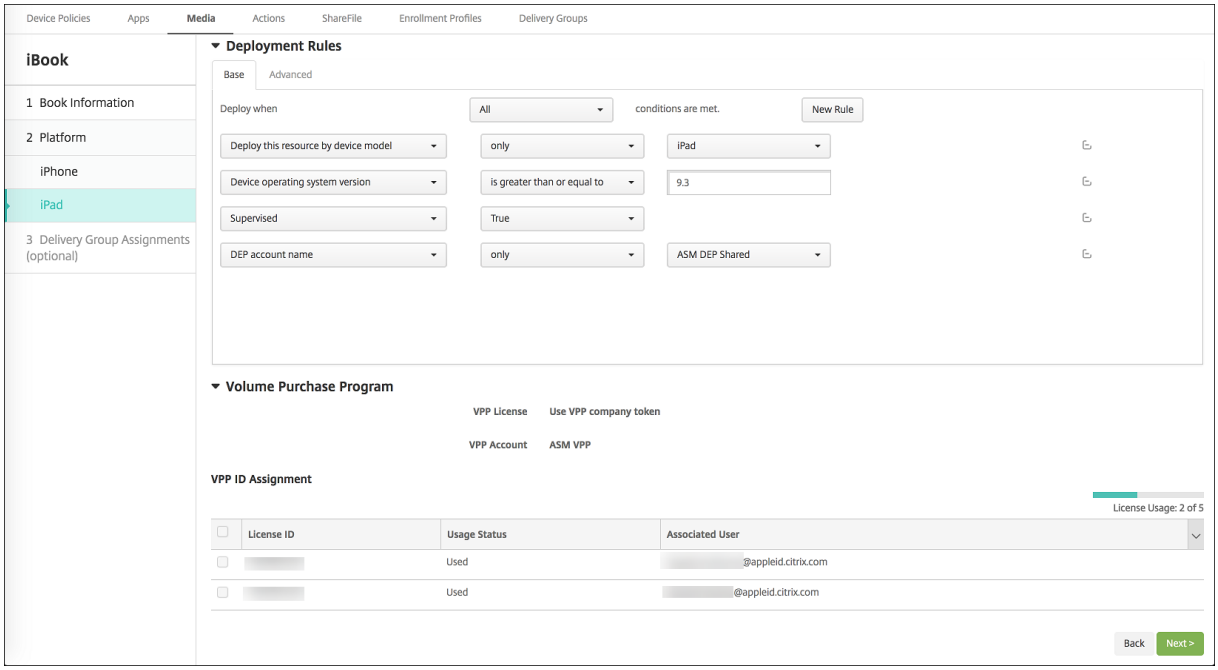


共有 **iPad** のアプリ

共有 iPad は、デバイスベースの VPP アプリの割り当てをサポートしています。XenMobile Server は共有 iPad にアプリを展開する前に、デバイスに VPP ライセンスを割り当てるように Apple VPP サーバーに要求を送信します。VPP の割り当てを確認するには、[構成] > [アプリ] > [**iPad**] に進み、[**Volume Purchase Program**（**VPP**）] を展開します。

共有 **iPad** 用のメディア

共有 iPad は、ユーザーベースの VPP iBooks の割り当てをサポートします。共有 iPad に iBooks を展開する前に、生徒に VPP ライセンスを割り当てるように XenMobile Server が Apple VPP サーバーに要求を送信します。VPP の割り当てを確認するには、[構成] > [**Media**] > [**iPad**] に移動し、「**Volume Purchase Program**」を展開します。



共有 **iPad** の展開規則

デリバリーグループレベルの規則はユーザープロパティに関するものであるため、共有 iPad を展開する場合これらの規則は適用されません。デバイスのグループごとにポリシー、アプリ、メディアを絞り込むには、DEP アカウント名に基づいて、リソースの展開規則を追加します。次に例を示します:

- デバイスグループ 1 の DEP アカウントでは、次の展開規則を設定します。

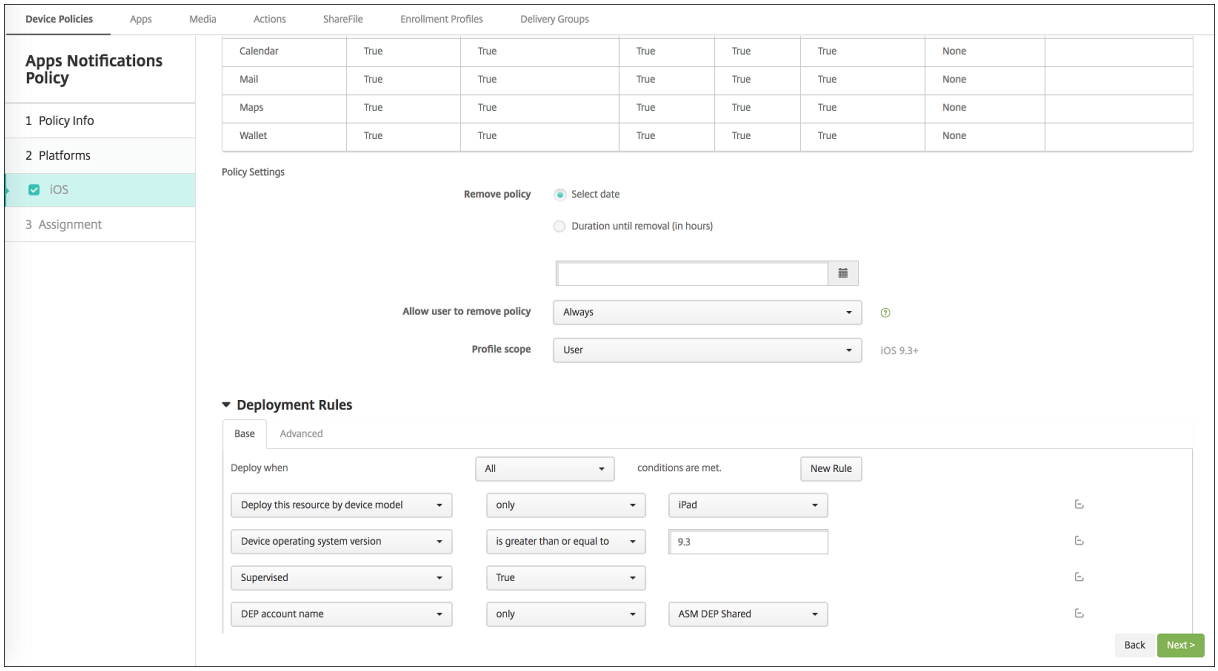
```
1  DEP account name
2  Only
3  Device Group 1 DEP account
```

- デバイスグループ 2 の DEP アカウントでは、次の展開規則を設定します。

```
1  DEP account name
2  Only
3  Device Group 2 DEP account
```

- デバイスグループ N の DEP アカウントでは、次の展開規則を設定します。

```
1  DEP account name
2  Only
3  Device Group N DEP account
```

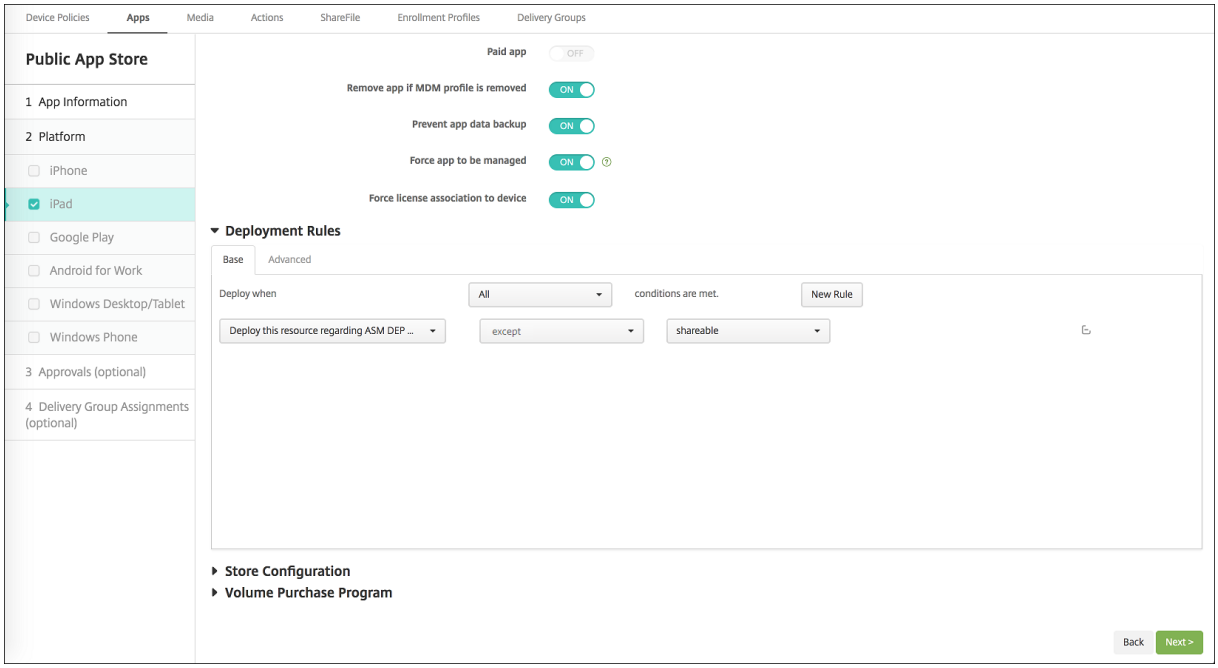



非共有の iPad を使用して講師にのみ Apple クラスルームアプリを展開する場合、ASM DEP の共有状態を次の展開規則で絞り込みます。

```
Deploy this resource regarding ASM DEP shared mode
only
unshared
```

または:

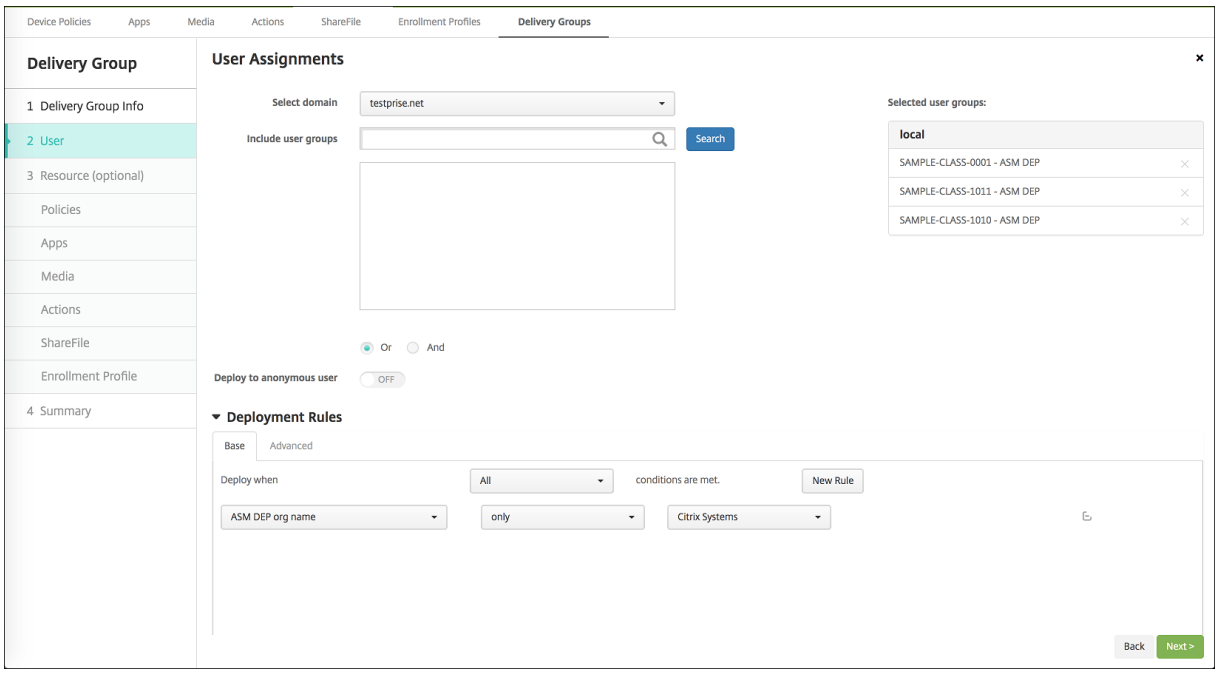
```
Deploy this resource regarding ASM DEP shared mode
except
shareable
```

共有 **iPad** のデリバリーグループ

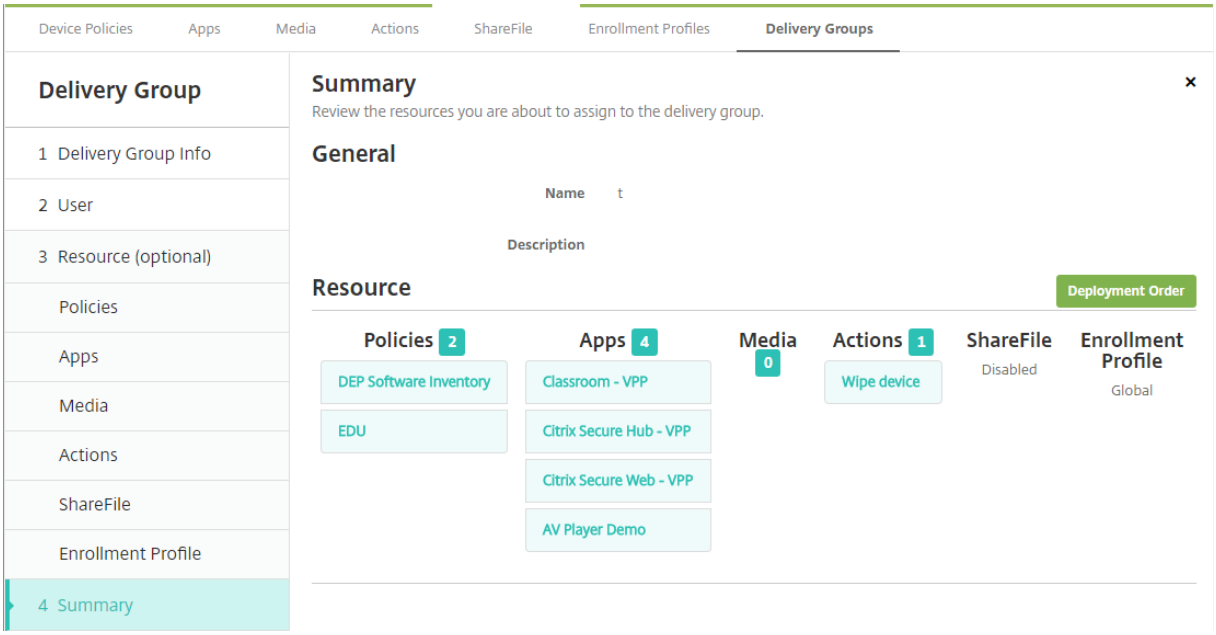
講師ごとのデバイスグループについては、次を参照してください。

- 1 つのデリバリーグループを構成する。講師には、[教育の構成] ポリシーで定義されているすべてのクラスを割り当てます。



- このデリバリーグループには、次の MDM リソースを含める必要があります。

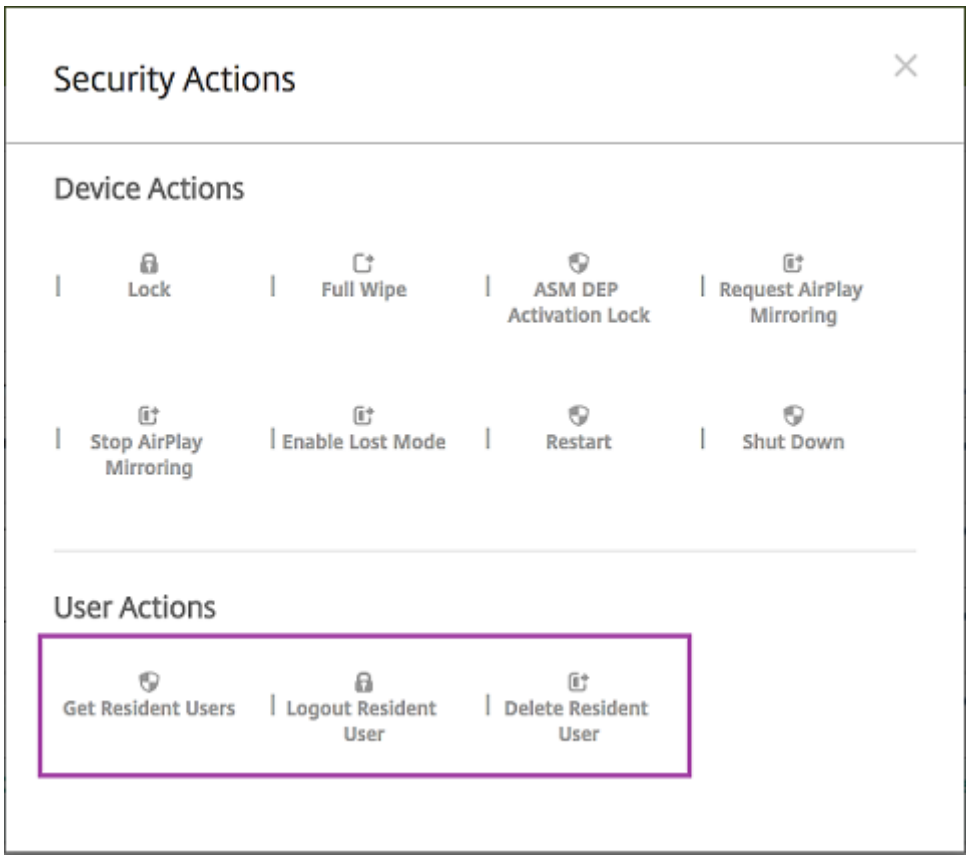
- デバイスポリシー:
  - 教育の構成
  - ロック画面のメッセージ
  - アプリ通知
  - ホーム画面のレイアウト
  - 制限
  - 最大常駐ユーザー数
  - パスコードロックの猶予期間
- 必須の VPP アプリ
- 必須の VPP iBooks



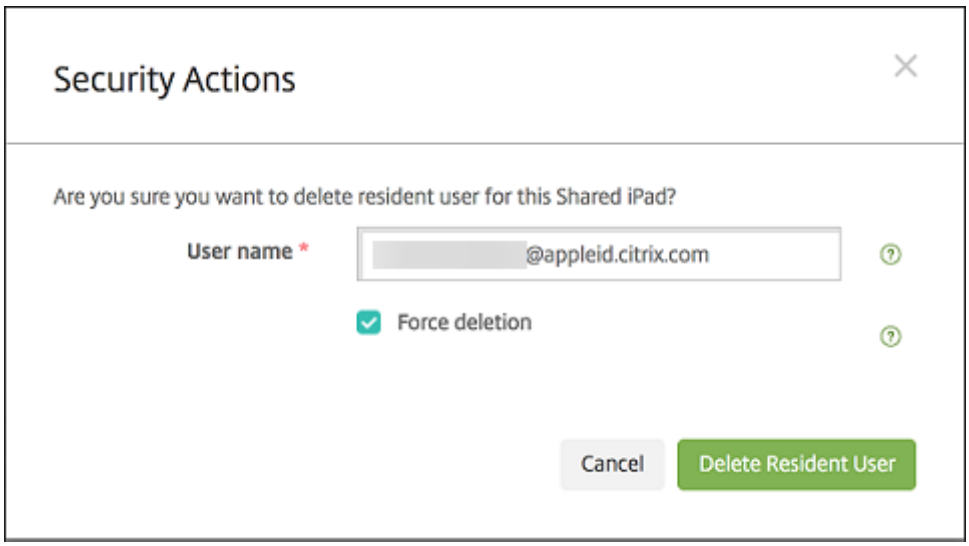
共有 **iPad** のセキュリティ操作

既存のセキュリティ操作に加えて、共有 iPad では次のセキュリティ操作を使用できます:

- 常駐ユーザーの取得: 現在のデバイスで有効なアカウントを持つユーザーの一覧を表示します。この操作により、デバイスと XenMobile Server コンソール間の同期が強制されます。
- 常駐ユーザーのログアウト: 現在のユーザーを強制的にログアウトさせます。
- 常駐ユーザーの削除: 指定したユーザーの現在のセッションを削除します。ユーザーは再びサインインできます。



［常駐ユーザーの削除］ のクリック後、ユーザー名を指定できます。

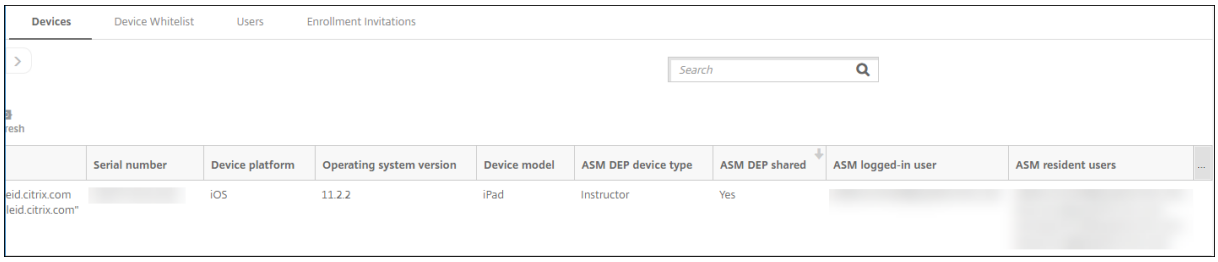


セキュリティ操作の結果は、［管理］ **>** ［デバイス］ **>** ［一般］ ページおよび ［管理］ **>** ［デバイス］ **>** ［デリバリーグループ］ ページに表示されます。

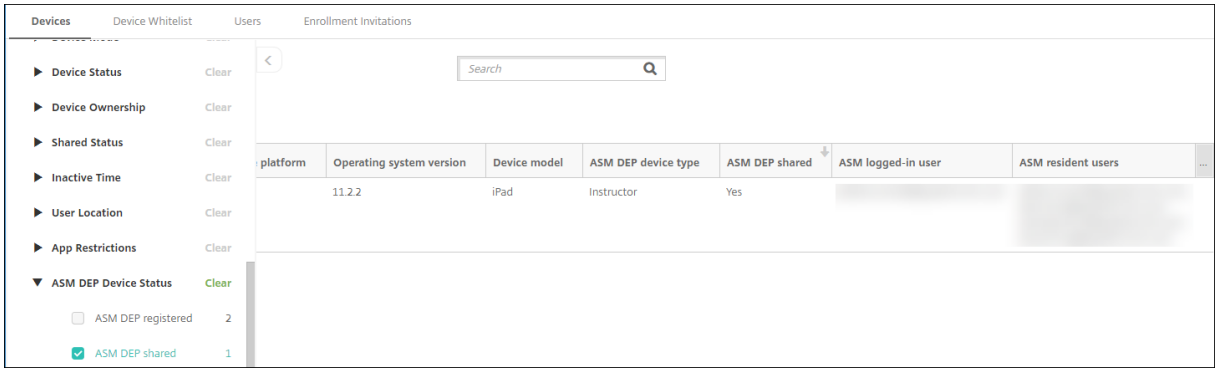
共有 **iPad** の情報を取得する

共有 iPad に関する情報は、［管理］**>**［デバイス］ ページで確認できます。

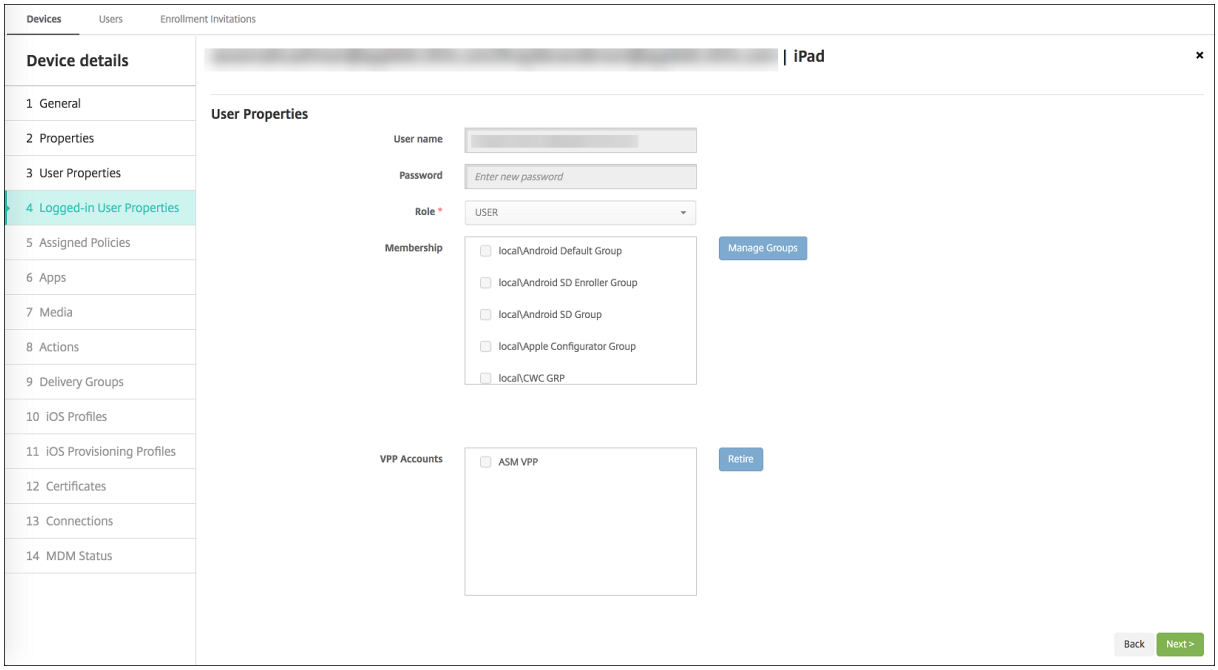
- 次を検索できます。
  - デバイスが共有されているか（［**ASM DEP** 共有］）
  - 共有デバイスにログインしているユーザー（［**ASM** ログイン済みユーザー］）
  - 共有デバイスに割り当てられているすべてのユーザー（［**ASM** 常駐ユーザー］）

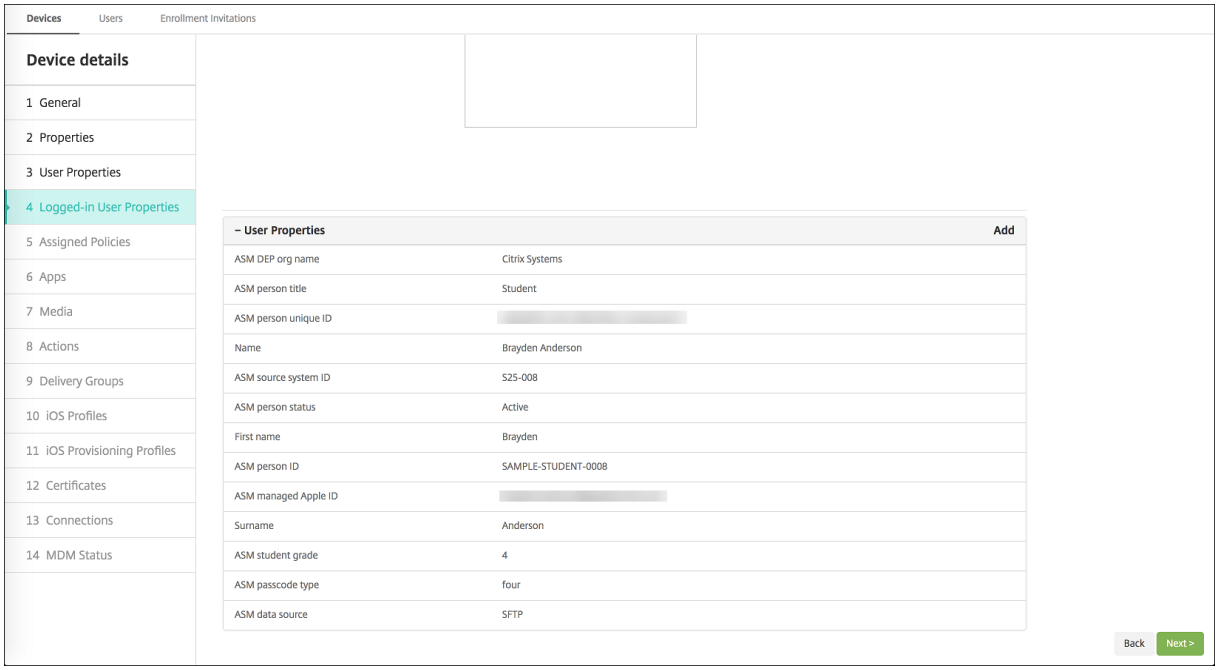


- ［**ASM DEP** デバイスの状態］ でデバイス一覧を絞り込む:

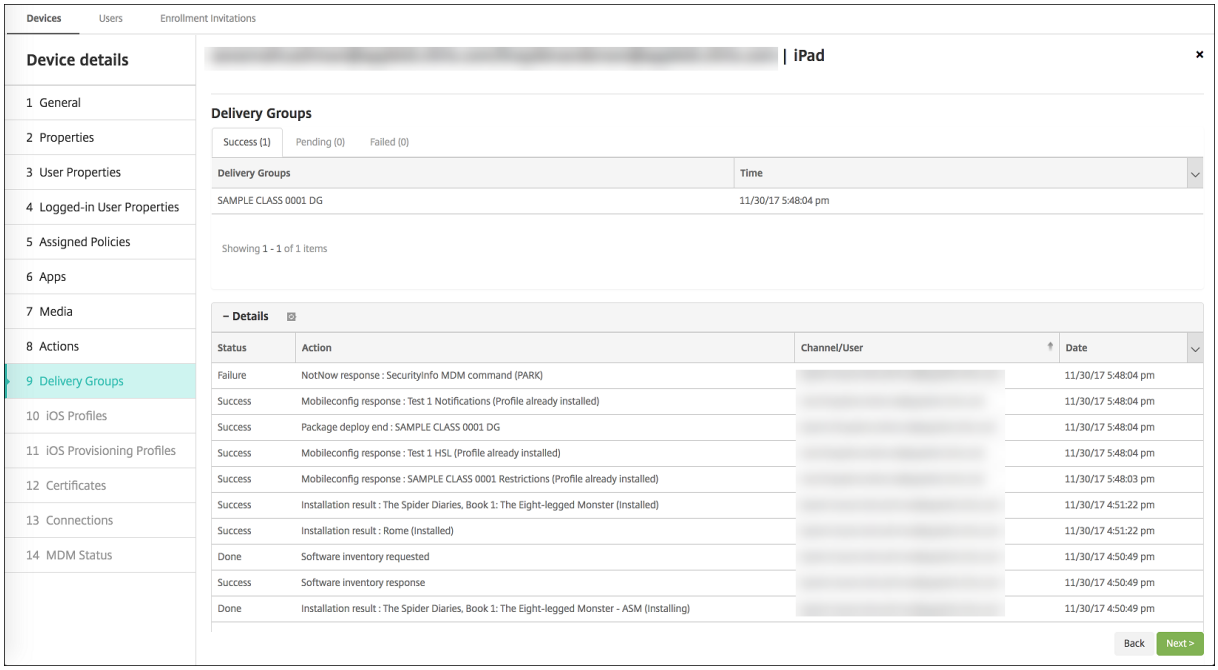


- ［管理］**>**［デバイス］**>**［ログイン済みユーザーのプロパティ］ ページで、共有 iPad にログインしているユーザーの詳細を確認できます。

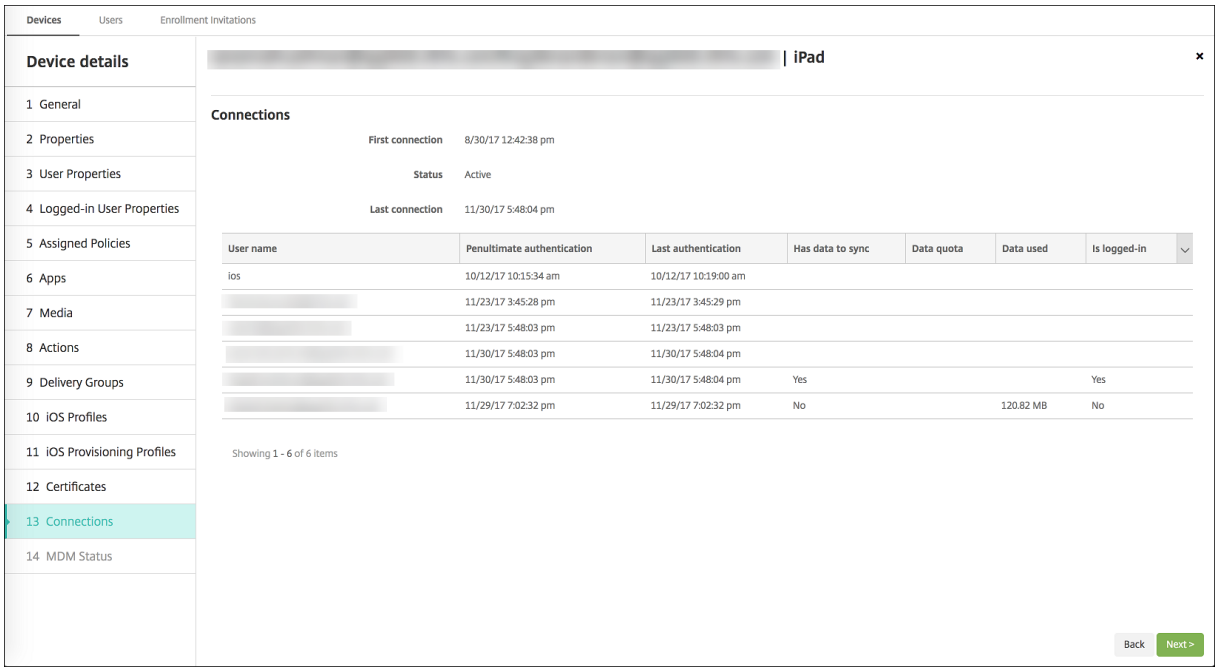




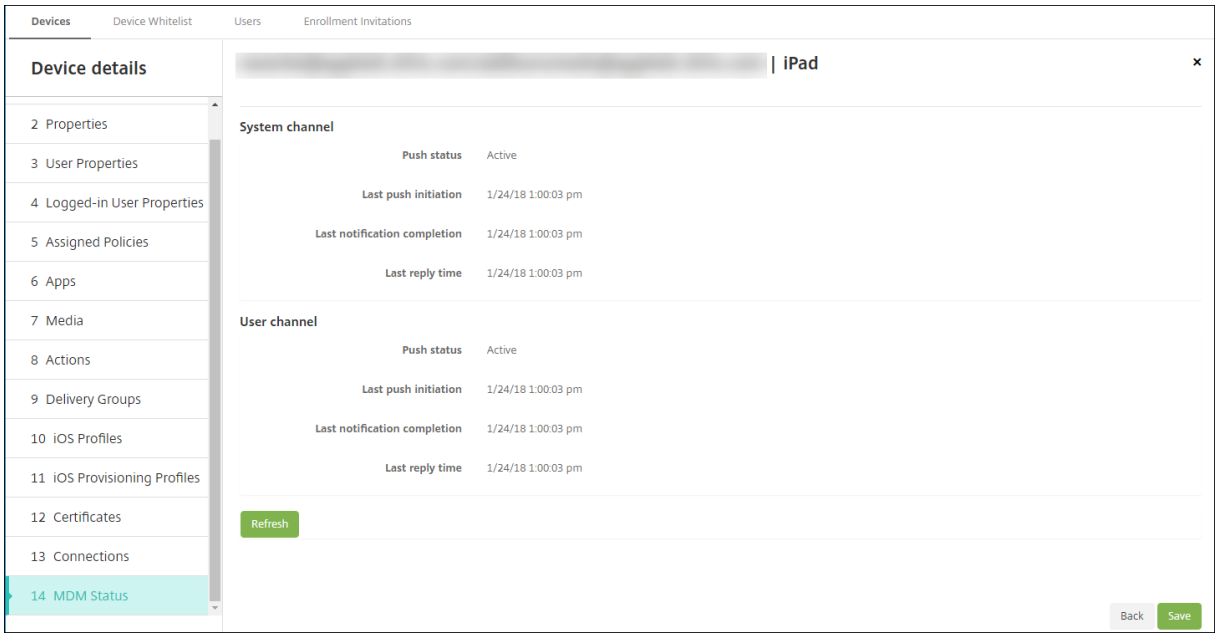
- [管理] > [デバイス] > [デリバリーグループ] ページでは、デリバリーグループの講師およびユーザーへのリソース展開に使用されているチャネルを確認できます。[チャネル/ユーザー] 列には、チャネルの種類（[システム] または [ユーザー]）と受信者（講師または生徒）が表示されます。



- 常駐ユーザーの情報を取得できます。
  - 同期するデータがある： クラウドに同期させるデータをユーザーが持っているかどうか。
  - データクォータ： ユーザーに設定されているデータクォータ（バイト単位）。ユーザークォータが一時的にオフになっているか、ユーザーに割り当てられていない場合は、クォータが表示されないことがあります。
  - 使用済みデータ： ユーザーが使用したデータ量（バイト単位）。システムの情報収集時にエラーが発生した場合、値が表示されないことがあります。
  - ログイン中： ユーザーがデバイスにログオンしているかどうか。



- 両方のチャネルのプッシュステータスを確認できます。



講師、生徒、およびクラスのデータの管理

講師、生徒、およびクラスのデータを管理する場合は、次のことに注意してください。

- Apple School Manager 情報を XenMobile Server にインポートした後に、管理対象 Apple ID を変更しないでください。XenMobile は、ユーザーの特定に Apple School Manager のユーザー識別子も使用します。
- 1 つまたは複数の教育の構成デバイスポリシーを作成した後に、Apple School Manager にクラスデータの追加や変更を行った場合は、ポリシーを編集してから再展開します。
- 教育の構成デバイスポリシーを展開した後にクラスの講師を変更する場合は、ポリシーを確認して XenMobile コンソールで確実に更新してから、ポリシーを再展開します。
- Apple School Manager ポータルでユーザープロパティを更新すると、XenMobile でもコンソールでプロパティが更新されます。ただし、XenMobile では、そのほかのプロパティと同じ方法で［ASM の個人の役職］プロパティ（講師、生徒、またはそのほか）が受信されません。このため、Apple School Manager で ASM の個人の役職を変更する場合は、次の手順を完了して XenMobile に変更が反映されるようにします。

データを管理するには:

1. Apple School Manager ポータルで、生徒の学年を更新し、講師の学年を削除します。
2. 生徒のアカウントを講師のアカウントに変更した場合は、クラスの生徒一覧からそのユーザーを削除します。次に、同じまたは別のクラスの講師一覧に、そのユーザーを追加します。

   講師のアカウントを生徒のアカウントに変更した場合は、クラスからそのユーザーを削除します。次に、同じまたは別のクラスの生徒一覧に、そのユーザーを追加します。更新内容は、次回の同期時（デフォルトで 5 分ごと）またはフェッチ時（デフォルトで 24 時間ごと）に、XenMobile コンソールに表示されます。

3. 教育の構成デバイスポリシーを編集し、変更を適用して再展開します。

    - Apple School Manager ポータルからユーザーを削除すると、XenMobile Server でもフェッチ後に XenMobile コンソールからそのユーザーが削除されます。

      サーバープロパティ値 **bulk.enrollment.fetchRosterInfoDelay** を変更することで、2 つのベースライン間の間隔を短縮できます（デフォルトは **1440** 分）。

    - リソース展開後に、生徒をクラスに参加させる場合は、その生徒だけで構成されたデリバリーグループを作成してリソースを展開します。

    - 生徒や講師が一時的なパスワードを紛失した場合は、Apple School Manager 管理者に問い合わせるようにします。管理者によって一時的なパスワードが提供されるか、または新しいパスワードが生成されます。

Apple School Manager DEP に登録済みの紛失または盗難に遭ったデバイスの管理

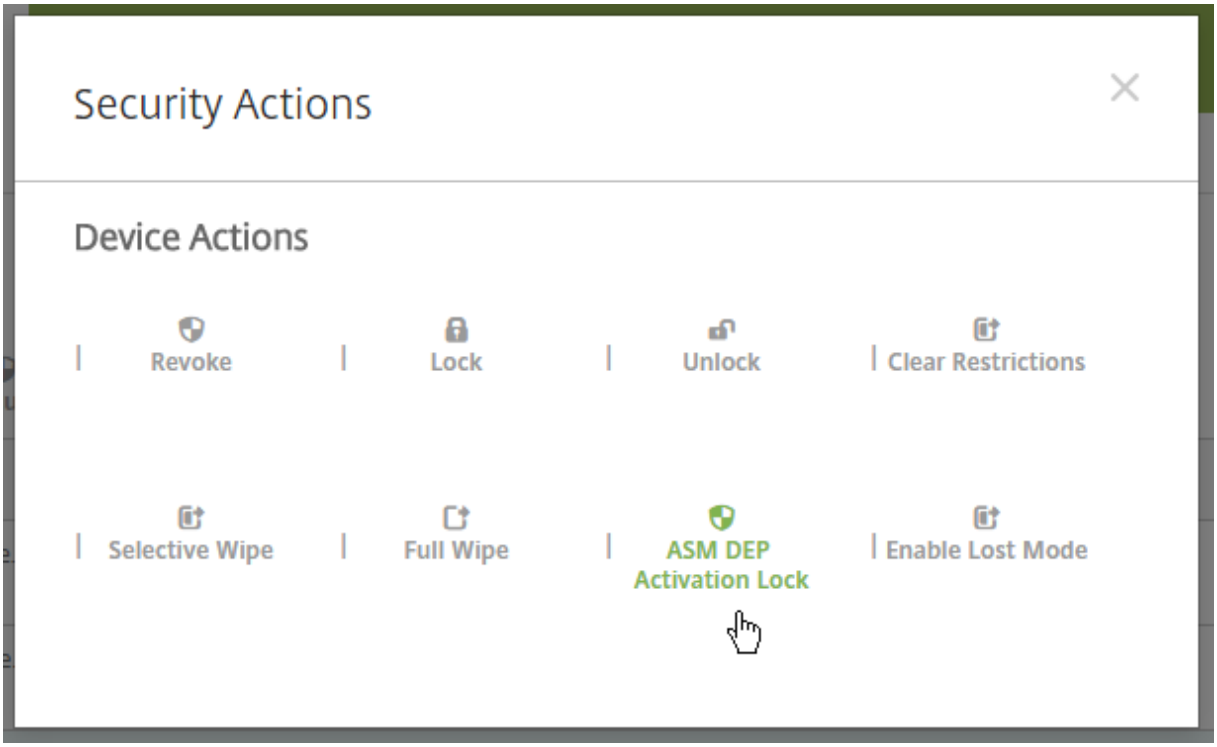
Apple の［iPhone/iPad を探す］サービスには、アクティベーションロック機能が含まれています。アクティベーションロックは、DEP に登録済みのデバイスが紛失または盗難に遭った場合に、不正ユーザーがそのデバイスを使用したり転売したりすることを防止します。

XenMobile には、Apple School Manager DEP に登録済みのデバイスにロックコードを送信できる、［**ASM DEP** アクティベーションロック］ のセキュリティ操作が含まれています。

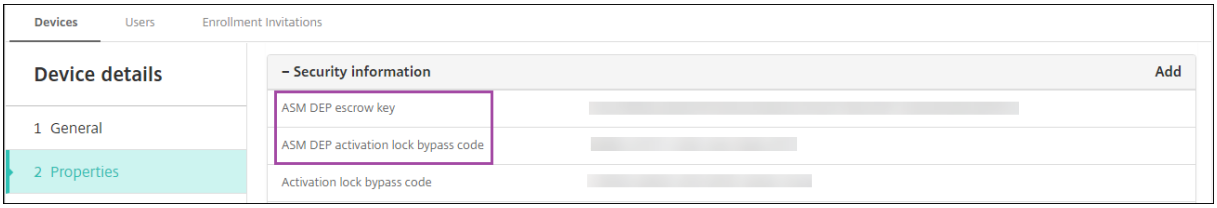
［**ASM DEP** アクティベーションロック］ のセキュリティ操作を使用すると、ユーザーに “iPhone/iPad を探す” サービスの有効化を要求せずに、XenMobile でデバイスを検索できます。Apple School Manager デバイスが強制リセットまたは完全にワイプされた場合、ユーザーは管理対象 Apple ID とパスワードを入力してデバイスのロックを解除します。

コンソールからロックを解除するには、セキュリティ操作 ［アクティベーションロックバイパス］ をクリックします。アクティベーションロックをバイパスする方法については、「セキュリティ操作」の記事の「iOS アクティベーションロックのバイパス」を参照してください。ログインパネルを空白のままにして、パスワードとして ［**ASM DEP** アクティベーションロックバイパスコード］ を入力することもできます。この情報は、［プロパティ］ タブの ［デバイス詳細］ で入手できます。

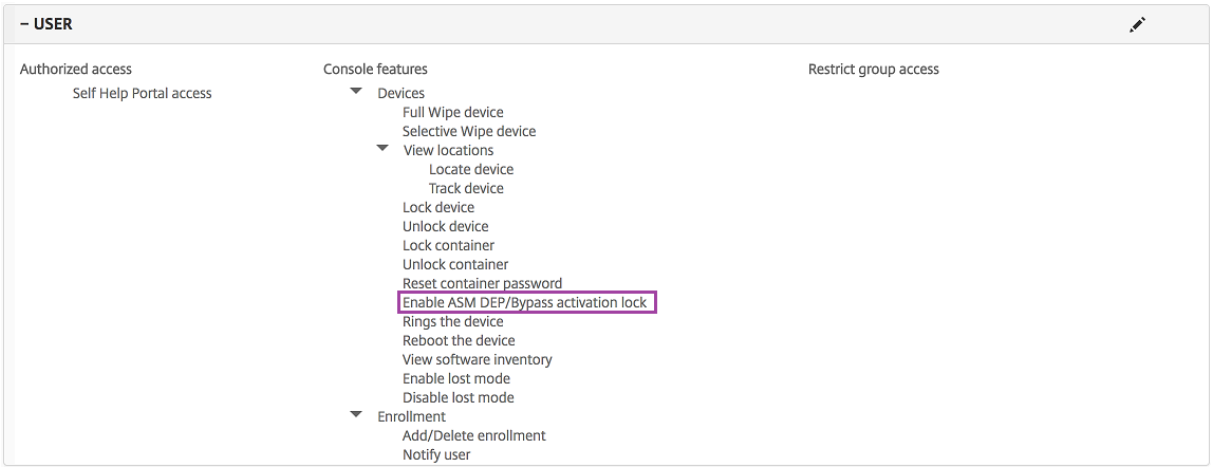
アクティベーションロックを設定するには、［管理］ **>** ［デバイス］ の順に選択し、該当するデバイスを選択して、［セキュリティ］、［**ASM DEP** アクティベーションロック］ の順にクリックします。



[**ASM DEP** エスクローキー] と [**ASM DEP** アクティベーションロックバイパスコード] のプロパティが、[デバイス詳細] に表示されます。



ASM DEP アクティベーションロックに対する RBAC の権限は、[デバイス] > [**ASM DEP**/バイパスアクティベーションロックの有効化] です。



ネットワークアクセス制御

August 22, 2019

XenMobile で、Cisco ISE などの NAC（Network Access Control：ネットワークアクセス制御）アプライアンスをネットワークで設定する場合は、フィルターで規則またはプロパティに基づいてデバイスを NAC に準拠または非準拠として設定することができます。XenMobile の管理対象デバイスが指定された条件を満たしておらず、その結果［Not Compliant］としてマークされている場合、そのデバイスは NAC アプライアンスによりネットワーク上でブロックされます。iOS デバイスの場合、VPN ポリシーを展開し、NAC フィルターを有効にして、非準拠のアプリがインストールされているデバイスの VPN 接続をブロックすることができます。詳細については、下記の「iOS NAC の設定」セクションを参照してください。

XenMobile コンソールの一覧で、デバイスを非準拠として設定する条件を 1 つまたは複数選択します。

XenMobile では、次の NAC 準拠フィルターがサポートされます。

匿名デバイス： デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときに XenMobile がユーザーを再認証できない場合に使用できます。

Samsung KNOX 構成証明に失敗しました： デバイスが、Samsung KNOX 構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ： デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。アプリアクセスポリシーについて詳しくは、「アプリケーションアクセスデバイスポリシー」を参照してください。

非アクティブデバイス： ［サーバープロパティ］でデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。詳しくは、「サーバープロパティ」を参照してください。

不足必須アプリ： デバイスにアプリアクセスポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ： デバイスにアプリアクセスポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード： ユーザーパスワードが正しいかを確認します。iOS デバイスおよび Android デバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかを XenMobile が確認できます。例えば、iOS では、XenMobile がデバイスにパスコードポリシーを送信する場合、ユーザーは 60 分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

コンプライアンス外デバイス： ［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス違反かどうかを確認します。通常、このプロパティは自動化された操作により変更されるか、XenMobile API を利用するサードパーティにより変更されます。

失効状態： デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

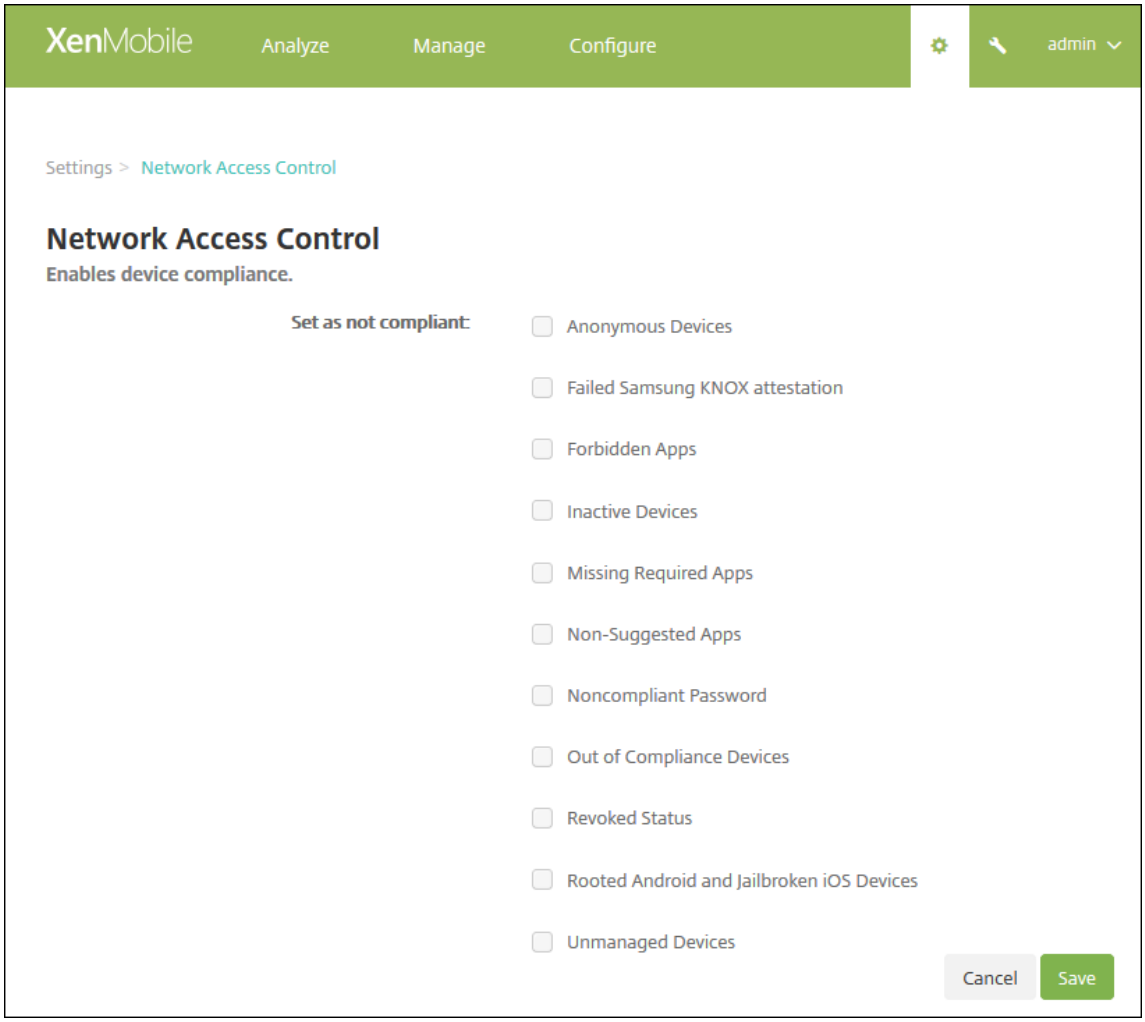
ルート化された **Android** およびジェイルブレイクした **iOS** デバイス： Android または iOS デバイスがジェイルブレイクされていないかを確認します。

非管理デバイス: デバイスがまだ XenMobile の管理下にあるかを確認します。例えば、MAM モードで実行されているデバイスや未登録のデバイスは管理されていません。

> 注:
>
> [暗黙的な準拠/非準拠] または [非準拠] フィルターは、XenMobile による管理対象デバイスでのみデフォルト値を設定します。たとえば、ブラックリストに入っているアプリケーションがインストールされているデバイスや、登録されていないデバイスは [非準拠] としてマークされ、NAC アプライアンスによりネットワークからブロックされます。

ネットワークアクセス制御の構成

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [サーバー] の下の [ネットワークアクセス制御] をクリックします。[ネットワークアクセス制御] ページが開きます。



3. 有効にする [非準拠として設定] フィルターのチェックボックスをオンにします。

4. [保存] をクリックします。

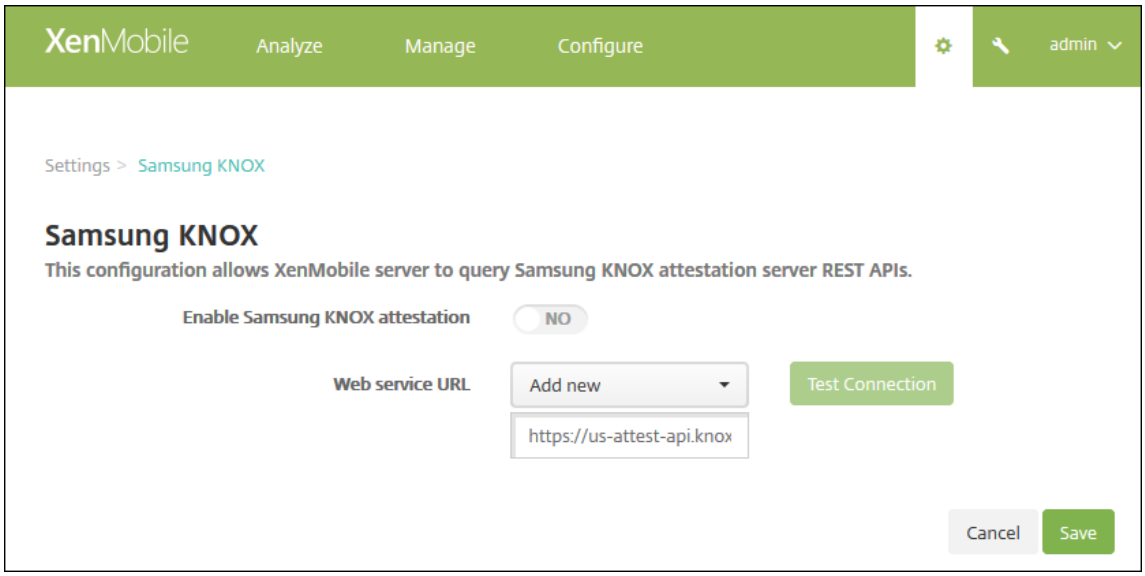
Samsung KNOX

January 10, 2020

XenMobile を構成して、Samsung KNOX 認証サーバー REST API に対するクエリを実行できます。

Samsung KNOX は、オペレーティングシステムとアプリケーションを複数レベルで保護する、ハードウェアセキュリティ機能を利用します。このセキュリティの 1 つのレベルは、認証を通じてプラットフォームに存在します。認証サーバーは、モバイルデバイスのコアシステムソフトウェア（ブートローダーやカーネルなど）の検証を提供します。検証は、信頼できる起動時に収集されるデータに基づいて、実行時に行われます。

1. XenMobile Web コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [プラットフォーム] の [**Samsung KNOX**] をクリックします。[**Samsung KNOX**] ページが開きます。



3. [**Samsung KNOX** 構成証明を有効にする] で、Samsung KNOX 認証を有効にするかどうかを選択します。デフォルトは [**NO**] です。
4. [**Samsung KNOX** 構成証明を有効にする] を [はい] に設定すると、[**Web** サービス **URL**] オプションが有効になります。一覧から、次のいずれかを選択します。
   - 適切な認証サーバーを選択します。
   - [新規追加] を選択して、Web サービス URL を入力します。
5. [接続のテスト] をクリックして、接続を検証します。成功、または失敗のメッセージが表示されます。
6. [保存] をクリックします。

> 注：
>
> Samsung KNOX Mobile Enrollment を使用すると、複数の Samsung KNOX デバイスを XenMobile（または、その他のモバイルデバイスマネージャー）に登録する場合に、各デバイスを手動で構成する必要がありません。詳しくは、「Samsung KNOX の一括登録」を参照してください。

セキュリティ操作

January 24, 2020

［管理］>［デバイス］ ページでデバイスやアプリのセキュリティの操作を実行できます。デバイスの操作には、取り消し、ロック、ロック解除、ワイプがあります。アプリのセキュリティの操作には、アプリのロック、アプリのワイプが含まれます。

- アクティベーションロックバイパス： デバイスのライセンス認証の前に、監視対象の iOS デバイスからアクティベーションロックを解除します。このコマンドでは、Apple の個人 ID やユーザーのパスワードが要求されることはありません。
- アプリのロック： デバイスのすべてのアプリへのアクセスを拒否します。Android では、アプリロック後にユーザーが XenMobile にサインインすることはできません。iOS では、ユーザーはサインインできますが、アプリにアクセスすることはできません。
- アプリのワイプ： Android では、アプリのワイプにより XenMobile からユーザーアカウントが削除されます。iOS では、Secure Hub のユーザーアカウントが削除されます。
- **ASM DEP** アクティベーションロック： Apple School Manager DEP に登録されている iOS デバイスのアクティベーションロックバイパスコードを作成します。
- 制限の解除： 監視対象の iOS デバイスでこのコマンドを使用すると、ユーザーによって構成された制限パスワードと制限設定を XenMobile Server で解除できます。
- 紛失モードを有効化/無効化： 監視対象の iOS デバイスを紛失モードにして、デバイスに表示されるメッセージ、電話番号、補足説明を送信します。2 回目にこのコマンドを送信すると、デバイスの紛失モードは無効になります。
- 追跡を有効にする： Android または iOS デバイスでは、このコマンドによって XenMobile が指定された頻度で特定のデバイスの場所をポーリングできます。デバイスの座標と位置をマップ上に表示するには、［管理］>［デバイス］ に移動し、デバイスを選択して ［編集］ をクリックします。デバイス情報は、［全般］ タブの［セキュリティ］ にあります。
- フルワイプ： デバイスからメモリカードを含むすべてのデータとアプリを直ちに消去します。
  - Android デバイスの場合、メモリカードをワイプするオプションをこの要求に含めることができます。

  - iOS デバイスと macOS デバイスの場合、デバイスがロックされていても直ちにワイプが実行されます。iOS 11 デバイス（最小バージョン）の場合：フルワイプを確認したら、携帯データネットワークプランをデバイスに保存することができます。
  - Windows Phone デバイスの場合、フルワイプを実行すると、すべての XenMobile 情報に加え、個人的なコンテンツ（アプリ、メール、連絡先、メディアなど）を含むすべてのユーザーデータが削除されます。
  - Windows Mobile 6 以前を実行している Windows Mobile デバイスの場合、ワイプ実行後、デバイスを製造元に送り返して、元のオペレーティングシステムやソフトウェア、あるいはその両方を再ロードしなければならない場合があります。
  - メモリカードの内容が削除される前にユーザーがデバイスの電源をオフにした場合、ユーザーはデバイスのデータにまだアクセスできる場合があります。
  - ワイプの要求がデバイスに送信されるまでは、要求をキャンセルできます。

- 検索： ［管理］**>**［デバイス］ ページの、［デバイス詳細］**>**［全般］ で、デバイスを検索してデバイスの場所（マップなど）を報告します。Android Enterprise デバイスの場合、位置情報デバイスポリシーでデバイスの位置情報モードが ［高精度］ または ［バッテリー節約］ に設定されていない限り、この要求は失敗します。iOS デバイスの場合、このコマンドは、デバイスが MDM の紛失モードである場合にのみ成功します。［検索］は、［追跡を有効にする］の継続的な追跡とは対照的に 1 回限りの操作です。Secure Hub は、実行中にデバイスの場所を定期的に報告します。
- ロック： デバイスをリモートでロックします。これは、デバイスを紛失し、デバイスが盗まれたかどうかわからない場合に便利です。その後 XenMobile によって PIN コードが生成されてデバイスに設定されます。デバイスにアクセスするには、PIN コードを入力します。XenMobile コンソールからロックを解除するには ［ロックのキャンセル］ を使用します。
- ロックおよびパスワードのリセット： デバイスをリモートロックしてパスコードをリセットします。
  - Android 8.0 より前のバージョンの Android を実行する、仕事用プロファイルモードで Android Enterprise に登録されているデバイスではサポートされていません。
  - Android 8.0 以降を実行する、仕事用プロファイルモードで Android Enterprise に登録されているデバイスの場合：
    * 送信されたパスコードによって仕事用プロファイルはロックされます。デバイスはロックされません。
    * パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たさず、仕事用プロファイルに設定済みのパスコードがない場合：デバイスはロックされます。
    * パスコードが送信されない場合、または送信されたパスコードがパスコードの要件を満たしていないが、仕事用プロファイルにパスコードが設定済みの場合：仕事用プロファイルはロックされますが、デバイスはロックされません。
- 通知（通知音）： Android デバイスで通知音を鳴らします。
- 再起動： Windows 10 デバイスを再起動します。Windows タブレットおよび PC では、「システムを再起動

します」という内容のメッセージが表示されて、5 分以内に再起動が実行されます。Windows Phone では、ユーザーに警告メッセージは表示されず、数分後に再起動が実行されます。

- **AirPlay** ミラーリングの要求/停止： 監視対象の iOS デバイスで、AirPlay ミラーリングを開始および停止します。
- 再起動/シャットダウン： 監視対象の iOS デバイスを直ちに再起動またはシャットダウンします。
- 取り消し： デバイスから XenMobile への接続を禁止します。
- 取り消し/認証（**iOS**、**macOS**）： 選択的なワイプと同じ操作を実行します。取り消し後に、デバイスを再承認して再登録できます。
- 警報：監視対象の iOS デバイスが紛失モードの場合に、デバイスで警告音を鳴らします。警告音は、デバイスの紛失モードが解除されるか、ユーザーがサウンドを無効にするまで鳴り続けます。
- 選択的なワイプ： 個人のデータとアプリは残して、企業のすべてのデータとアプリをデバイスから消去します。選択的なワイプ後に、ユーザーはデバイスを再登録できます。
  - Android デバイスを選択的にワイプしても、Device Manager や社内ネットワークから切断されることはありません。デバイスが Device Manager にアクセスしないようにするには、デバイス証明書を失効させる必要もあります。
  - Samsung KNOX API に対応している場合、デバイスを選択的にワイプするには、Samsung KNOX コンテナも削除する必要があります。
  - iOS デバイスおよび macOS デバイスでは、このコマンドにより、MDM を通じてインストールされたすべてのプロファイルが削除されます。
  - Windows デバイスに対して選択的ワイプを実行した場合、その時点でサインオンしているすべてのユーザーのプロファイルフォルダーの内容も削除されます。選択的なワイプでは、構成を介してユーザーに配信した Web クリップは削除されません。Web クリップを削除するには、ユーザーはデバイスを手動で登録解除します。選択的にワイプされたデバイスを再登録することはできません。
  - Windows Phone デバイスを選択的にワイプすると、XenMobile がデバイスにアプリをインストールできるエンタープライズトークンが削除されます。このワイプによって、デバイスに展開された XenMobile のすべての証明書と構成も削除されます。選択的にワイプされた Windows Phone デバイスを再登録することはできません。
  - Android デバイスでの選択的なワイプによってデバイスも取り消されます。デバイスを再度承認するかコンソールから削除した後にのみ、デバイスを再登録することができます。
- ロック解除： デバイスがロックされたときに送信されたパスコードをクリアします。このコマンドによってデバイスがロック解除されることはありません。

［管理］**>**［デバイス］ の ［デバイス詳細］ ページには、デバイスの［セキュリティ］プロパティも表示されます。これらのプロパティには、[Strong ID]、[デバイスのロック]、[アクティベーションロックバイパス]、およびプラットフォームの種類に関するその他の情報などが含まれます。［デバイスの完全なワイプ］ フィールドには、ユーザーの PIN コードが含まれます。デバイスがワイプされた後、ユーザーはこのコードを入力する必要があります。ユーザーがコードを忘れた場合は、こちらで確認できます。

Android デバイスのセキュリティ操作

セキュリティ操作	Android（Android Enterprise デバイスを除く）	Android Enterprise（BYOD）	Android Enterprise（コーポレート所有）
アプリのロック	はい	いいえ	いいえ
アプリのワイプ	はい	いいえ	いいえ
完全なワイプ	はい	いいえ	はい
検索	はい。Android 6.0 以降を実行するデバイスの場合、検索には、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しない選択をできます。登録時にユーザーによって権限が付与されないと、XenMobile は検索コマンドの送信時に再度検索の権限を要求します。	はい。Android 6.0 以降を実行するデバイスの場合、検索には、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しない選択をできます。登録時にユーザーによって権限が付与されないと、XenMobile は検索コマンドの送信時に再度検索の権限を要求します。	はい。Android 6.0 以降を実行するデバイスの場合、検索には、登録時にユーザーによって検索の権限が付与される必要があります。ユーザーは、検索の権限を付与しない選択をできます。登録時にユーザーによって権限が付与されないと、XenMobile は検索コマンドの送信時に再度検索の権限を要求します。
ロック	はい	はい	はい
パスワードのロックとリセット	はい	いいえ	はい
通知（通知音）	はい	はい	はい
取り消し	はい	はい	はい
選択的なワイプ	はい	はい	いいえ

iOS デバイスと **macOS** デバイスのセキュリティ操作

セキュリティ操作	**iOS**	**macOS**
アクティベーションロックのバイパス	はい	いいえ
アプリのロック	はい	いいえ
アプリのワイプ	はい	いいえ

セキュリティ操作	**iOS**	**macOS**
ASM DEP アクティベーションロック	はい	いいえ
制限の削除	はい	いいえ
紛失モードを有効化/無効化	はい	いいえ
追跡を有効/無効にする	はい	いいえ
完全なワイプ	はい	はい
検索	はい	いいえ
ロック	はい	はい
警報	はい	はい
AirPlay ミラーリングの要求/停止	はい	いいえ
再起動/シャットダウン	はい	いいえ
取り消し/承認	はい	はい
選択的なワイプ	はい	はい
ロック解除	はい	いいえ

Windows デバイスのセキュリティ操作

セキュリティ操作	**Windows Phone 10**	**Windows** タブレット **10**	**Windows Phone 8.1**
検索	はい	はい	いいえ
ロック	はい	はい	はい
パスワードのロックとリセット	はい	いいえ	はい
再起動	はい	はい	いいえ
取り消し	はい	はい	はい
警報	はい	いいえ	はい
選択的なワイプ	はい	はい	はい
ワイプ	はい	はい	はい

この記事の残りの部分では、各種セキュリティ操作を実行する手順について説明します。一部の操作を自動化することもできます。詳しくは、「自動化された操作」を参照してください。

iOS デバイスのロック

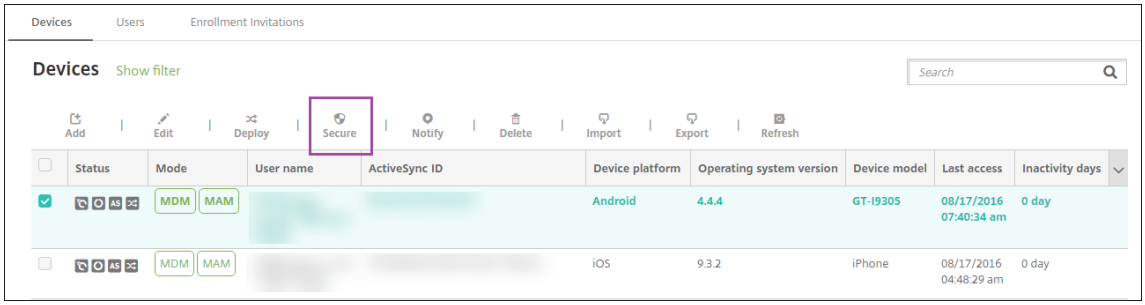
iOS デバイスをロックし、デバイスのロック画面にメッセージと電話番号を表示することができます。この機能は、iOS 7 以降を実行しているデバイスでサポートされます。

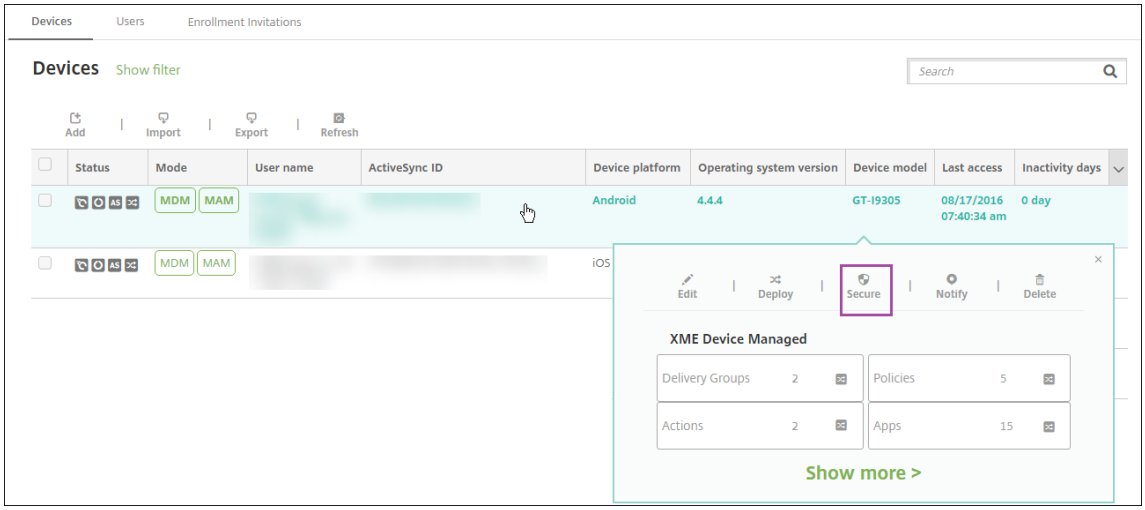
ロックされたデバイスにメッセージと電話番号を表示するには、パスコードポリシーが XenMobile コンソールで **true** に設定されている必要があります。あるいは、デバイス上でパスコードを手動で有効化できます。

1. ［管理］ **>** ［デバイス］ の順にクリックします。［デバイス］ ページが開きます。

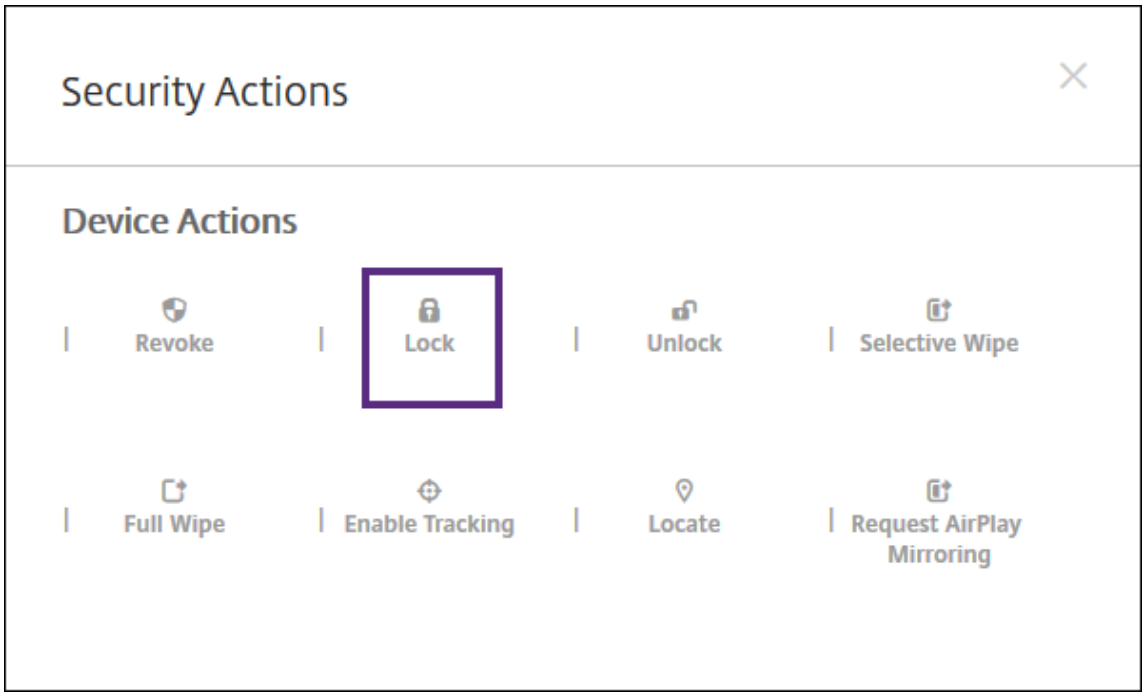
2. ロックする iOS デバイスを選択します。

   デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

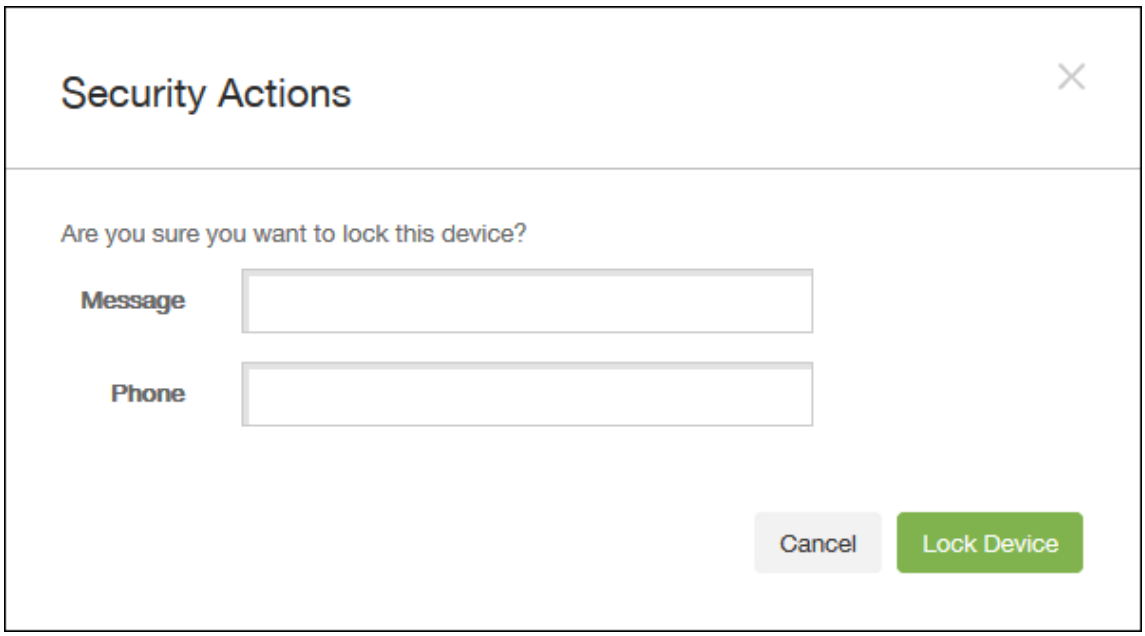




3. オプションメニューの ［保護］ を選択します。［セキュリティ操作］ ダイアログボックスが開きます。



4. ［ロック］ をクリックします。［セキュリティ操作］ 確認ダイアログボックスが開きます。



5. 必要に応じて、デバイスのロック画面に表示するメッセージと電話番号を入力します。

   iOS 7 以降を実行している iPad：iOS は「Lost iPad」という文字列をユーザーが ［メッセージ］ フィールドに入力した内容に追加します。

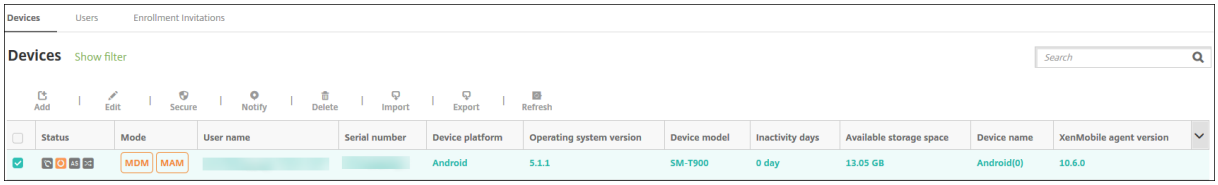
   iOS 7 以降を実行している iPhone：［メッセージ］ フィールドを空白にして電話番号を指定すると、Apple はメッセージ「Call owner」をデバイスのロック画面に表示します。

6. ［デバイスのロック］ をクリックします。

XenMobile コンソールからのデバイスの削除

> 重要：
>
> XenMobile コンソールからデバイスを削除した場合、管理対象アプリとデータはデバイスに残っています。デバイスから管理対象アプリとデータを削除するには、この記事で後述する「デバイスの削除」を参照してください。

XenMobile コンソールからデバイスを削除するには、［管理］ > ［デバイス］ の順に選択し、管理対象デバイスを選択して ［削除］ をクリックします。



デバイスの選択的なワイプ

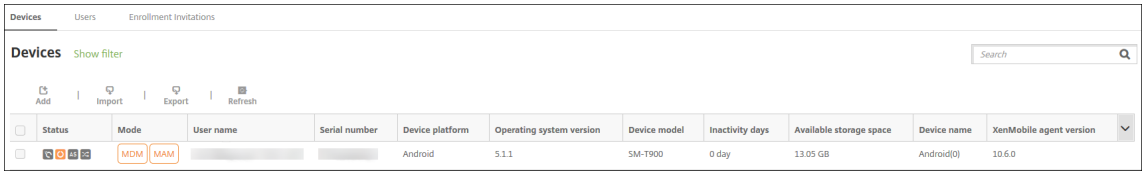
1. ［管理］ **>** ［デバイス］ の順に選択し、管理対象デバイスを選択して ［保護］ をクリックします。
2. ［セキュリティ操作］ で、 ［選択的なワイプ］ をクリックします。
3. Android デバイスのみ、デバイスをワイプした後、 ［セキュリティ操作］ で ［取り消し］ をクリックして、社内ネットワークからデバイスを切断します。

   選択的ワイプ要求が実行される前にその要求を取り消すには、 ［セキュリティ操作］ で、 ［選択的なワイプのキャンセル］ をクリックします。

デバイスの削除

この手順では、管理対象アプリとデータをデバイスから削除し、XenMobile コンソールの［デバイス］一覧からデバイスを削除します。

1. ［管理］ **>** ［デバイス］ の順に選択し、管理対象デバイスを選択して ［保護］ をクリックします。
2. ［選択的なワイプ］ をクリックします。プロンプトが表示されたら、 ［選択的なワイプの実行］ をクリックします。
3. ワイプコマンドが成功したことを確認するには、［管理］ **>** ［デバイス］ を更新します。［モード］ 列で MDM と MAM が黄色の場合は、ワイプコマンドが成功したことを示します。



4. ［管理］ **>** ［デバイス］ に移動し、デバイスを選択して ［削除］ をクリックします。プロンプトが表示されたら、再び ［削除］ をクリックします。

アプリのロック、ロック解除、ワイプ、ワイプ解除

1. ［管理］ **>** ［デバイス］ の順に選択し、管理対象デバイスを選択して ［保護］ をクリックします。
2. ［セキュリティ操作］ で、アプリの操作をクリックします。

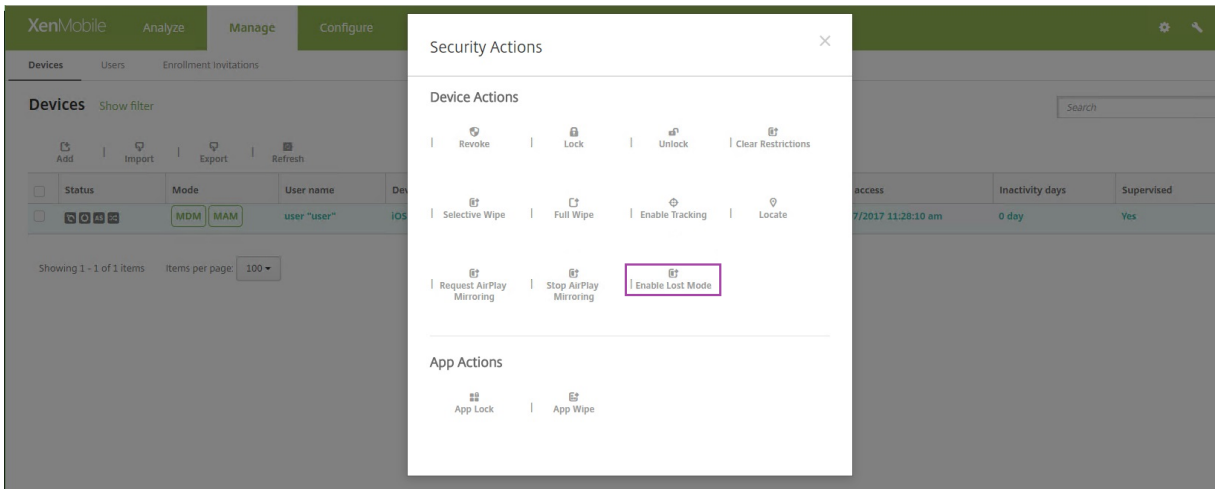
   ［セキュリティ操作］ ボックスは、アカウントが無効になっているか、Active Directory から削除されているユーザーのデバイスの状態を確認するために使用することもできます。アプリロック解除またはアプリワイプ解除アクションが存在する場合、アプリがロックまたはワイプされていることを意味します。

iOS デバイスを紛失モードにする

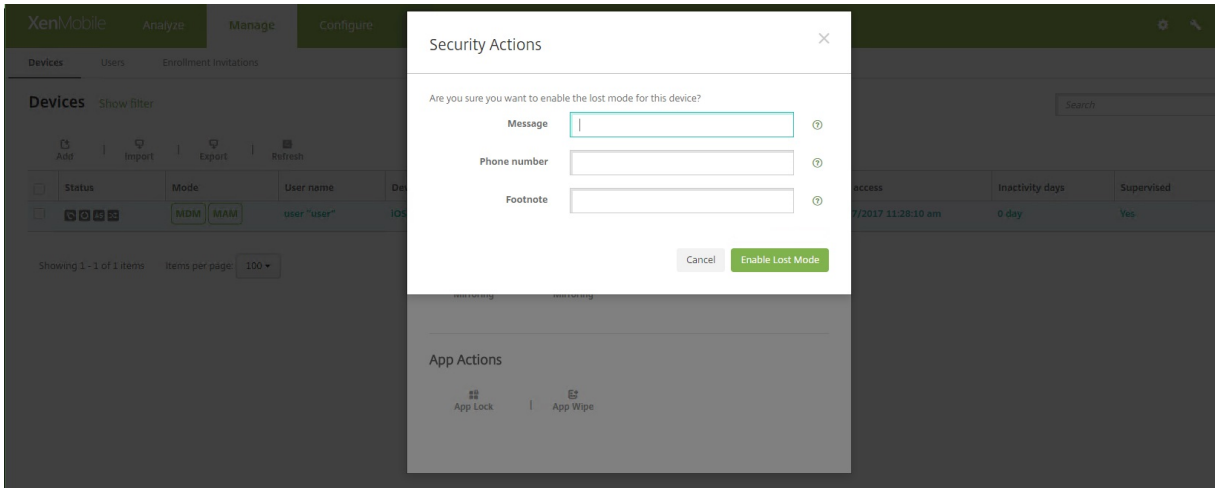
XenMobile の紛失モードデバイスプロパティで、iOS デバイスを紛失モードにします。Apple のマネージド紛失モードと異なり、XenMobile の紛失モードでは、ユーザーは自分のデバイスを探せるようにするために、次のどちらの操作も実行する必要がありません。［iPhone/iPad を探す］を構成するか Citrix Secure Hub の位置情報サービスを有効化します。

XenMobile の紛失モードでは、デバイスのロックを解除できるのは XenMobile Server だけです。一方、XenMobile のデバイスロック機能を使用すると、ユーザーは管理者によって提供された PIN コードを使用して、デバイスを直接ロック解除できます。

紛失モードを有効または無効にするには: ［管理］**>**［デバイス］ に移動し、監視対象デバイスを選択して ［保護］ をクリックします。次に、［紛失モードを有効化］ または ［紛失モードを無効化］ をクリックします。



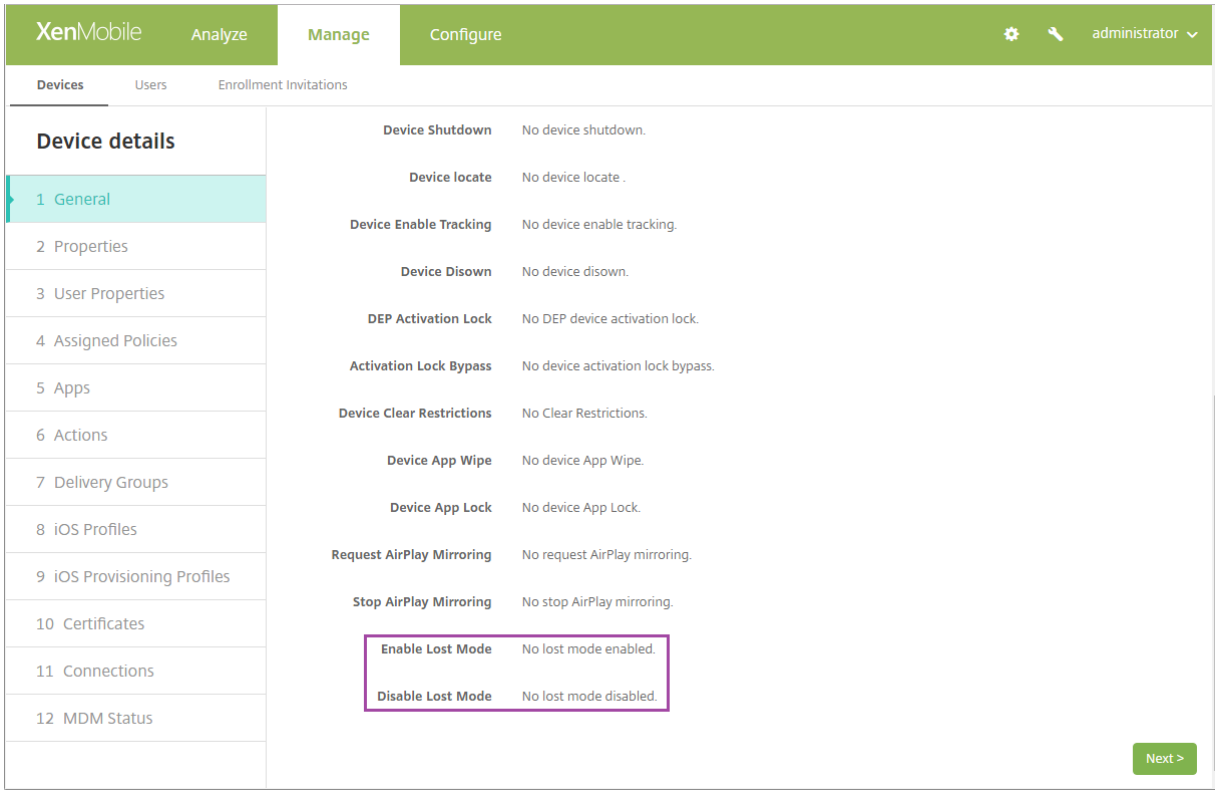
［紛失モードを有効化］ をクリックした場合は、デバイスが紛失モードになったときにデバイスに表示される情報を入力します。



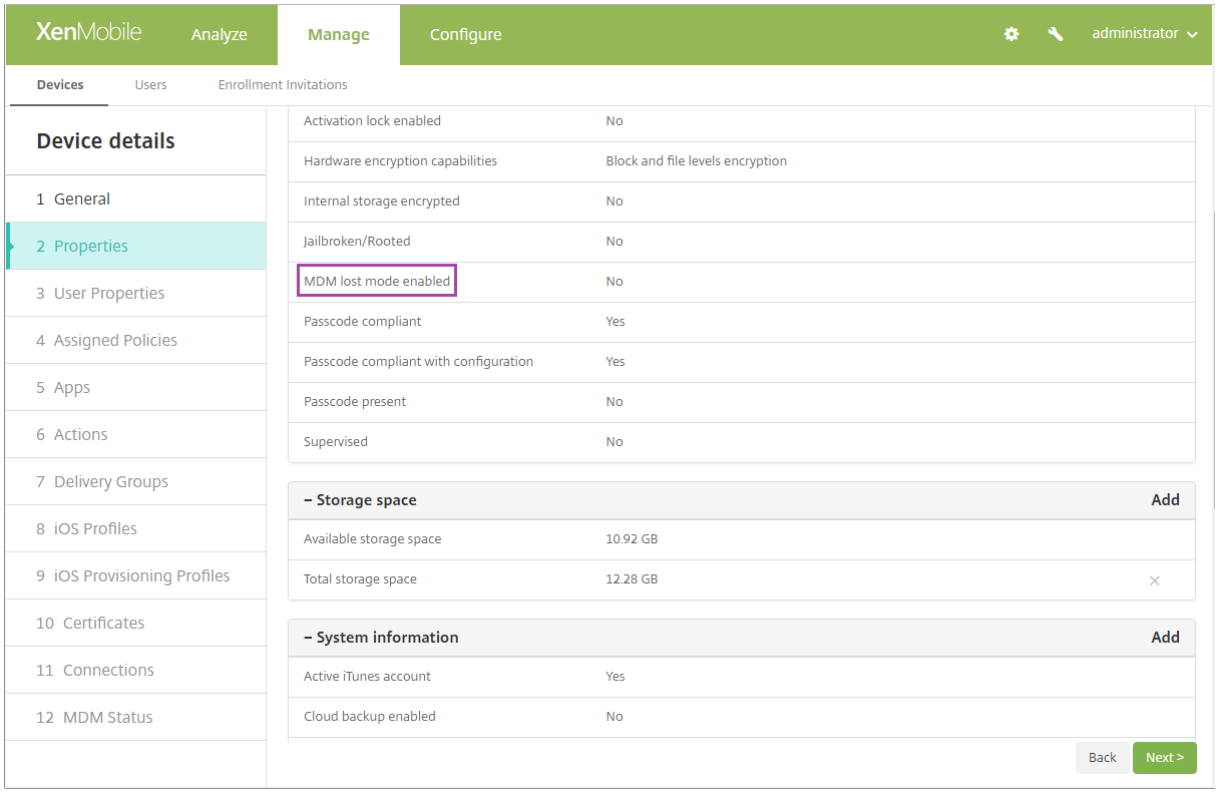
次のいずれかの方法を使って紛失モードの状態を確認する:

- ［セキュリティ操作］ ウィンドウで、ボタンが ［紛失モードを無効化］ であることを確認します。

- ［管理］**>**［デバイス］ から、［セキュリティ］ の ［一般］ タブで、［紛失モードを有効化］または［紛失モードを無効化］の最後の操作を確認します。



- ［管理］**>**［デバイス］ から ［プロパティ］ タブで、［**MDM** の紛失モードの有効化］ の設定値が正しいことを確認します。



iOS デバイスで XenMobile の紛失モードを有効化すると、XenMobile コンソールも以下のように変更されます。

- [構成] > [操作] の [操作] 一覧には、自動化された操作 [デバイスを失効]、[デバイスの選択的なワイプ]、[デバイスを完全にワイプ] は含まれません。
- [管理] > [デバイス] の [セキュリティ操作] 一覧に、[失効] および [選択的なワイプ] デバイス操作が含まれなくなりました。必要に応じて、セキュリティ操作を使ってフルワイプを実行することは引き続き可能です。

iOS 7 以降を実行している iPad: iOS は「Lost iPad」という文字列をユーザーが [セキュリティ操作] 画面の [メッセージ] に入力した内容に追加します。

iOS 7 以降を実行している iPhone: [メッセージ] を空白にして電話番号を入力すると、Apple はメッセージ「Call owner」をデバイスのロック画面に表示します。

iOS アクティベーションロックのバイパス

アクティベーションロックは、紛失したり盗まれたりした管理対象デバイスが再アクティブ化されないようにすることを目的とした [iPhone/iPad を探す] の機能です。アクティベーションロックでは、ユーザーの Apple ID とパスワードを入力してからでないと、[iPhone/iPad を探す] をオフにしたり、デバイスを消去したり、デバイスを再アクティブ化したりすることはできません。組織所有のデバイスの場合は、デバイスのリセットや再割り当てなどを行う際にアクティベーションロックをバイパスする必要があります。

アクティベーションロックを有効にするには、XenMobile MDM オプションのデバイスポリシーを設定して展開します。その後はユーザーの Apple 資格情報なしで、XenMobile コンソールからデバイスを管理することができます。

アクティベーションロックで必要な Apple 資格情報の入力をバイパスするには、XenMobile コンソールから［アクティベーションロックバイパス］のセキュリティ操作を発行します。

たとえば、紛失した iPhone がユーザーによって返却されたり、フルワイプの前または後にデバイスを設定したりする場合、iPhone で iTunes アカウントの資格情報を入力するよう求められた際に、XenMobile コンソールから［アクティベーションロックバイパス］のセキュリティ操作を発行することでこの手順をバイパスすることができます。

アクティベーションロックバイパスのデバイス要件

- iOS 7.1（最小バージョン）
- Apple Configurator または Apple DEP による監視対象である
- iCloud アカウントで構成済みである
- ［iPhone/iPad を探す］が有効になっている
- XenMobile に登録済みである
- MDM オプションデバイスポリシー（アクティベーションロックが有効になっている）がデバイスに展開されている

デバイスのフルワイプを発行する前にアクティベーションロックをバイパスするには、次の手順を実行します：

1. ［管理］**>**［デバイス］ の順に選択し、デバイスを選択して ［保護］、［アクティベーションロックバイパス］の順にクリックします。
2. デバイスをワイプします。デバイスの設定時に、アクティベーションロック画面は表示されません。

デバイスのフルワイプを発行した後にアクティベーションロックをバイパスするには、次の手順を実行します：

1. デバイスをリセットまたはワイプします。デバイスの設定時に、アクティベーションロック画面が表示されます。
2. ［管理］**>**［デバイス］ の順に選択し、デバイスを選択して ［保護］、［アクティベーションロックバイパス］の順にクリックします。
3. デバイスの［戻る］ボタンをタップします。ホーム画面が開きます。

次のことに注意してください：

- ユーザーが「iPhone/iPad を探す」をオフにしないようアドバイスしてください。デバイスからフルワイプを実行しないでください。いずれの場合も、ユーザーは iCloud アカウントのパスワードを入力するよう求められます。アカウントの検証後にすべてのコンテンツと設定が消去されると、iPhone/iPad のアクティブ化画面がユーザーに表示されなくなります。
- 作成されたアクティベーションロックバイパスコードがあり、アクティベーションロックが有効になっているデバイスの場合は、フルワイプ後に［iPhone/iPad のアクティブ化］ページをバイパスできなくても、XenMobile からデバイスを削除する必要はありません。管理者またはユーザーが Apple サポートに連絡することで、デバイスのブロックを直接解除することができます。
- ハードウェアインベントリの際に、XenMobile はデバイスでアクティベーションロックバイパスコードの照会を行います。バイパスコードが使用可能な場合は、デバイスから XenMobile にバイパスコードが送信されます。その後、バイパスコードをデバイスから削除するには、XenMobile コンソールから［アクティベーショ

ンロックバイパス］のセキュリティ操作を送信します。この時点で、XenMobile Server と Apple には、デバイスのブロック解除に必要なバイパスコードがあります。

- ［アクティベーションロックバイパス］のセキュリティ操作は、Apple のサービスの可用性に依存しています。操作がうまくいかない場合は、次の手順を実行してデバイスのブロックを解除できます。デバイスで、iCloud アカウントの資格情報を手動で入力します。または、［ユーザー名］フィールドは空のままにして、［パスワード］フィールドにバイパスコードを入力します。バイパスコードを見つけるには、［管理］**>**［デバイス］に移動し、デバイスを選択して［編集］、［プロパティ］の順にクリックします。［セキュリティ情報］の下に［アクティベーションロックバイパスコード］があります。

共有デバイス

January 10, 2020

XenMobile では、複数のユーザーが共有できるデバイスを構成できます。共有デバイス機能を使用すると、たとえば、病院の臨床医は、特定のデバイスを持ち歩くのではなく、近くにある任意のデバイスを使用して、アプリやデータにアクセスできます。場合によっては、法執行機関、リテール、製造などの現場で交代勤務労働者にデバイスを共有させ、機器費用の削減を図る必要があります。

共有デバイスに関する注意点

サポートされている iOS デバイスと Android デバイスのいずれかを共有デバイスとして使用できます。現在サポートされているデバイスの一覧については、「サポートされるデバイスオペレーティングシステム」を参照してください。

MDM モード

- iOS および Android 搭載のタブレットおよびスマートフォンで使用できます。XenMobile Enterprise の共有デバイスでは、基本的なデバイス登録プログラム（DEP）による登録はサポートされません。共有デバイスをこのモードで登録するするには、認証済みの DEP を使用する必要があります。
- クライアント証明書認証、Citrix PIN、Touch ID、ユーザーエントロピー、2 要素認証はサポートされません。

MDM+MAM モード

- iOS および Android タブレットでのみ使用できます。
- Active Directory のユーザー名およびパスワード認証のみがサポートされます。
- クライアント証明書認証、Worx PIN、Touch ID、ユーザーエントロピー、2 要素認証はサポートされません。
- MAM のみのモードはサポートされません。デバイスは MDM に登録する必要があります。
- Secure Mail、Secure Web、および ShareFile モバイルアプリのみがサポートされます。HDX アプリはサポートされません。

- Active Directory ユーザーのみがサポートされます。ローカルユーザーおよびグループはサポートされません。
- 既存の MDM-only モードの共有デバイスを MDM+MAM モードに更新するには、再登録が必要です。
- ユーザーはデバイス上でネイティブアプリを共有できません。
- 最初の登録時に業務用モバイルアプリをダウンロードすれば、新しいユーザーがデバイスにログオンするたびにこのアプリがダウンロードされることはありません。新しいユーザーは、デバイスを起動して、サインインし、使用を始めることができます。
- セキュリティのために、Android 上で各ユーザーのデータを隔離する場合は、XenMobile コンソールで［**Disallow rooted devices**］ ポリシーを ［オン］ にする必要があります。

共有デバイスの登録の前提条件

共有デバイスを登録する前に、以下の操作を行う必要があります。

- 共有デバイス登録ユーザーの役割を作成します。RBAC を使用した役割の構成を参照してください。
- 共有デバイスユーザーを作成します。ローカルユーザーアカウントを追加、編集、または削除するには を参照してください。
- 共有デバイス登録ユーザーに適用されるベースポリシー、アプリ、およびアクションを含むデリバリーグループを作成します。リソースの展開を参照してください。

MDM+MAM モードの前提条件

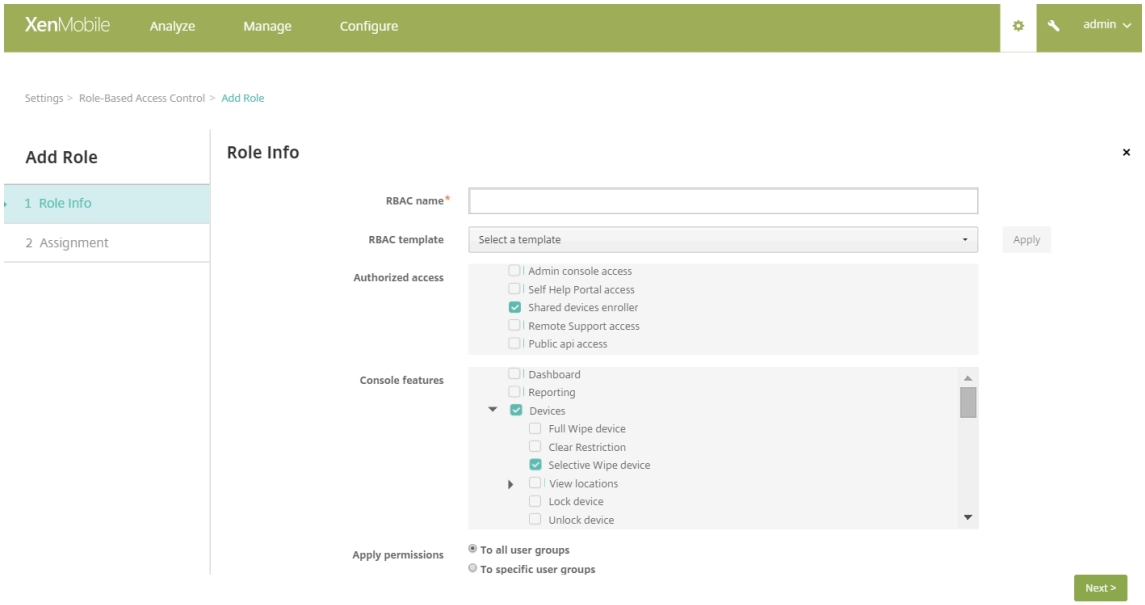
1. **Shared Device Enrollers** などの名前の Active Directory グループを作成します。
2. 共有デバイスを登録する Active Directory ユーザーをこのグループに追加します。このために新しいアカウントが必要な場合は、新しい Active Directory ユーザー（**sdenroll** など）を作成して、このユーザーを Active Directory グループに追加します。

共有デバイスを構成する

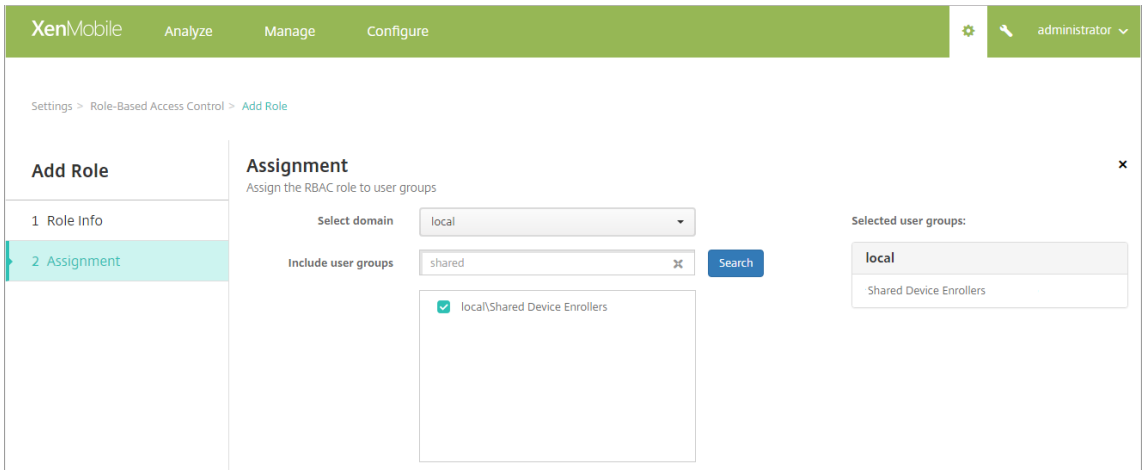
以下の手順に従って、共有デバイスを構成します。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［役割ベースのアクセス制御］、［追加］ の順にクリックします。［役割の追加］ ページが開きます。
3. ［承認済みのアクセス］ で ［共有デバイスの登録機能］ 権限を持つ **Shared Device Enrollment User** という名前の共有デバイス登録ユーザーの役割を作成します。［コンソールの機能］ の ［デバイス］ を展開し、［デバイスの選択的なワイプ］ をオンにします。この設定によって、共有デバイス登録機能アカウントにプロビジョニングされたアプリとポリシーは、デバイスの登録が解除されると Secure Hub から削除されます。

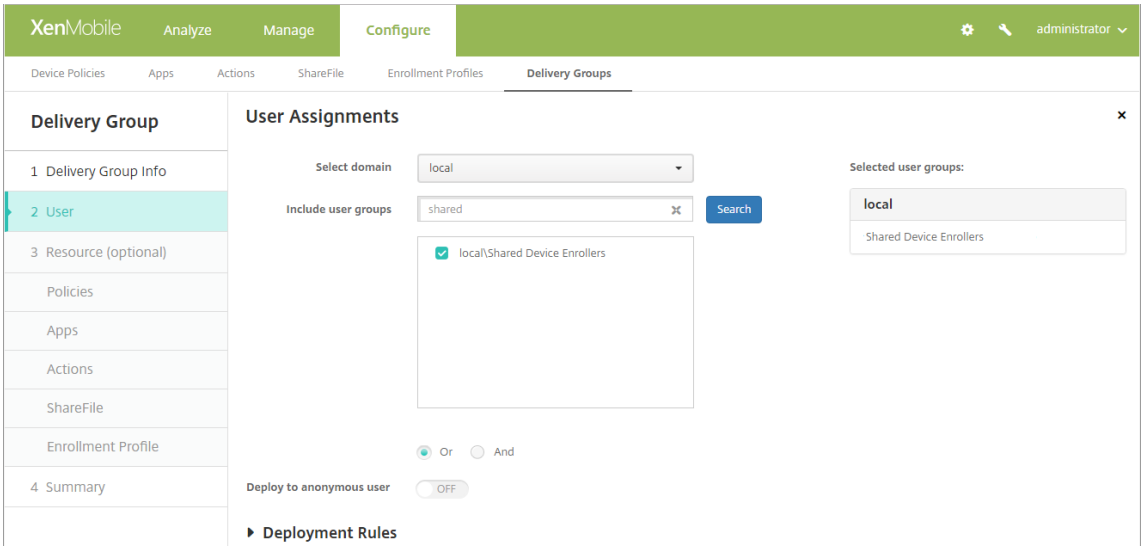
   ［適用権限］ で、デフォルト設定の ［すべてのユーザーグループ］ を保持するか、特定の Active Directory ユーザーグループに ［特定のユーザーグループ］ で権限を割り当てます。



［次へ］ をクリックして ［割り当て］ 画面に進みます。作成したばかりの共有デバイス登録の役割を、前提条件の手順 1 で共有デバイス登録ユーザーのために作成した Active Directory グループに割り当てます。下の図で **citrix.lab** は Active Directory ドメイン、**Shared Device Enrollers** は Active Directory グループです。



4. ユーザーがサインオンしていないときにデバイスに適用するベースポリシー、アプリ、アクションを含むデリバリーグループを作成し、共有デバイス登録ユーザー Active Directory グループにそのデリバリーグループを関連付けます。



5. 共有するデバイスで、Secure Hub をインストールし、共有デバイス登録ユーザーアカウントを使用して XenMobile にデバイスを登録します。XenMobile コンソールでデバイスを表示および管理できるようになります。詳しくは、「デバイスの登録」を参照してください。
6. 認証されたユーザーに異なるポリシーを適用したり、追加のアプリを提供するには、そのユーザーに関連付け、共有デバイスにのみ展開するデリバリーグループを作成する必要があります。グループを作成するときは、展開規則を構成して、パッケージが共有デバイスに展開されるようにします。詳しくは、「リソースの展開」を参照してください。
7. デバイスの共有を停止するには、選択的なワイプを実行して、共有デバイス登録ユーザーアカウントおよび展開されたアプリとポリシーをデバイスから削除します。

共有デバイスのユーザーエクスペリエンス

MDM モード

ユーザーにはそのユーザーが使用できるリソースだけが表示され、すべての共有デバイスに同じエクスペリエンスが提供されます。共有デバイス登録ポリシーとアプリは常にデバイスに残ります。共有デバイス登録ユーザー以外のユーザーが Secure Hub にサインオンすると、そのユーザーのポリシーとアプリがデバイスに展開されます。ユーザーがサインオフすると、共有デバイス登録に必要とされているものを除いて、ポリシーおよびアプリは削除されます。

MDM+MAM モード

共有デバイス登録ユーザーによって登録されると、Secure Mail と Secure Web がデバイスに展開されます。ユーザーデータはデバイスに安全に保持されます。ユーザーが Secure Mail または Secure Web にサインオンした場合、データはほかのユーザーには表示されません。

Secure Hub にサインオンできるユーザーは、一度に 1 人だけです。前のユーザーがサインオフしてからでないと、次のユーザーはサインオンできません。セキュリティ上の理由から、共有デバイスにはユーザーの資格情報が保存されないので、ユーザーはサインオンのたびに資格情報を入力する必要があります。前のユーザーのためのリソースに新しいユーザーがアクセスできないように、前のユーザーに関連付けられているポリシー、アプリ、データが削除されている間、新しいユーザーはサインオンできません。

共有デバイス登録によって、アプリのアップグレードプロセスが変更されることはありません。通常通り、共有デバイスユーザーにアップグレードをプッシュし、共有デバイスユーザーはデバイス上でアプリをアップグレードできます。

推奨される **Secure Mail** ポリシー

- Secure Mail のパフォーマンスを最適化するためには、デバイスを共有するユーザーの数に応じて ［同期の最大期間］ を設定します。無制限同期を許可することは推奨されません。

デバイスを共有するユーザーの数	推奨される［同期の最大期間］
21 ～ 25	1 週間以内
6 ～ 20	2 週間以内
5 以下	1 か月以内

- ［連絡先のエクスポートの有効化］ を禁止して、ユーザーの連絡先がデバイスを共有する他のユーザーにさらされないようにします。
- iOS では、次の設定のみをユーザーごとに設定できます。その他の設定は、デバイスを共有するユーザー間で共通になります。
  - 通知
  - 署名
  - 不在
  - メールの同期期間
  - S/MIME
  - スペルチェック

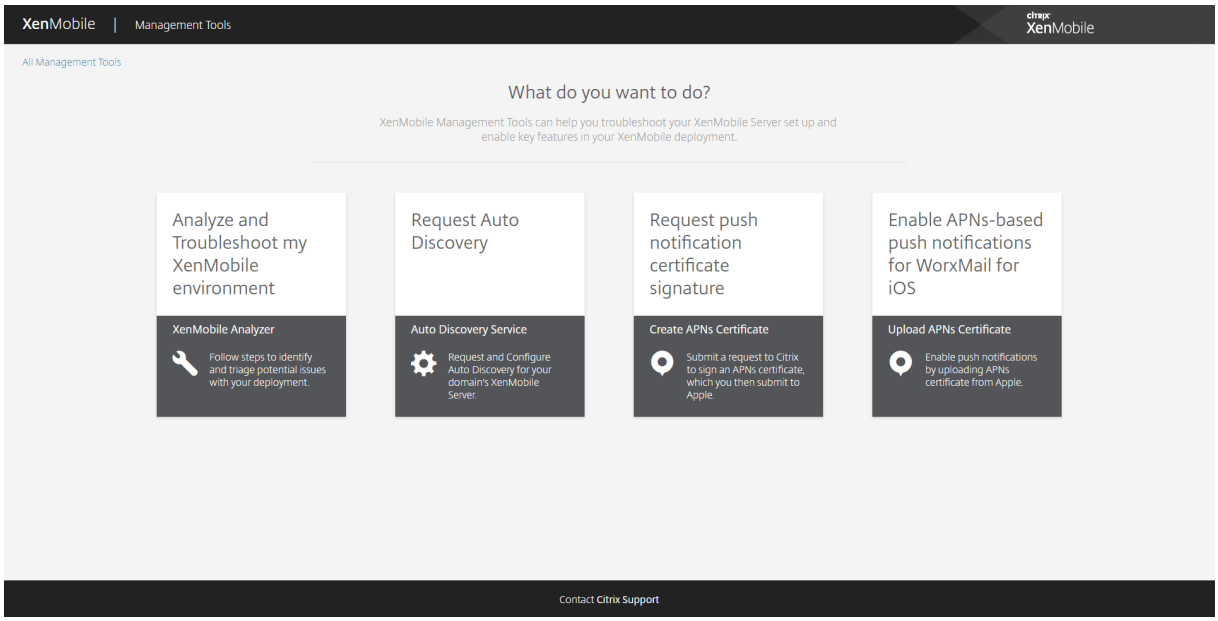
XenMobile AutoDiscovery サービス

August 22, 2019

多くの XenMobile 展開にとって、自動検出は重要な要素となります。自動検出を使用するとユーザー登録処理が簡単になります。ユーザーは、ネットワークユーザー名と Active Directory パスワードを使用してデバイスを登録

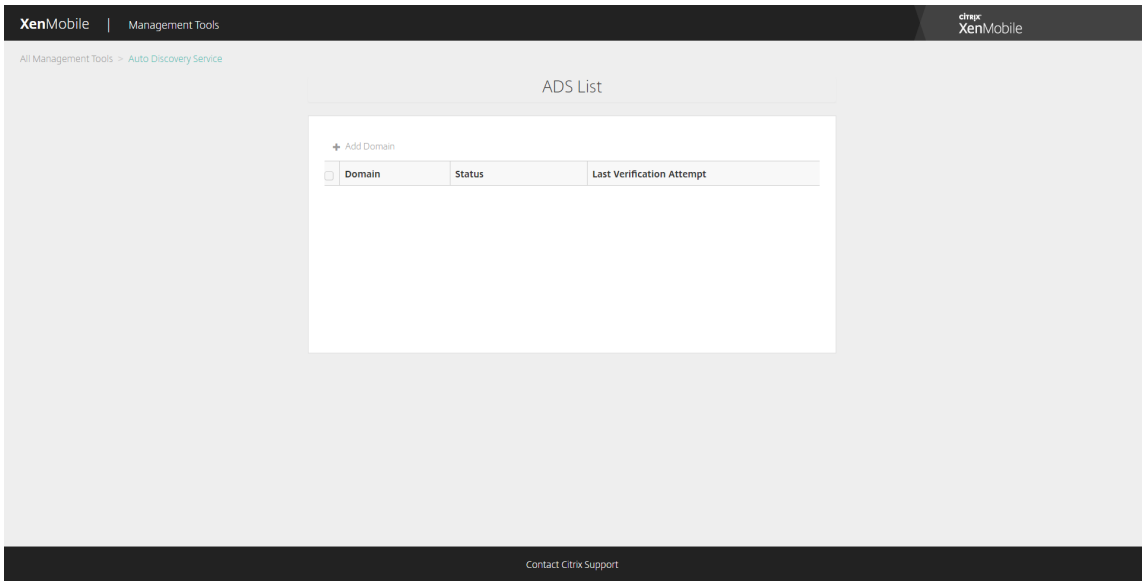
できます。XenMobile サーバーの詳細を入力する必要はありません。ユーザーは、ユーザー名をユーザープリンシパル名（User Principal Name：UPN）形式で入力します（たとえば、user@mycompany.com）。XenMobile AutoDiscovery サービスを使用すると、Citrix サポートの補助を受けずに自動検出レコードを作成または編集できます。

XenMobile AutoDiscovery サービスにアクセスするには、https://xenmobiletools.citrix.comに移動して［**Request Auto Discovery**］ をクリックします。

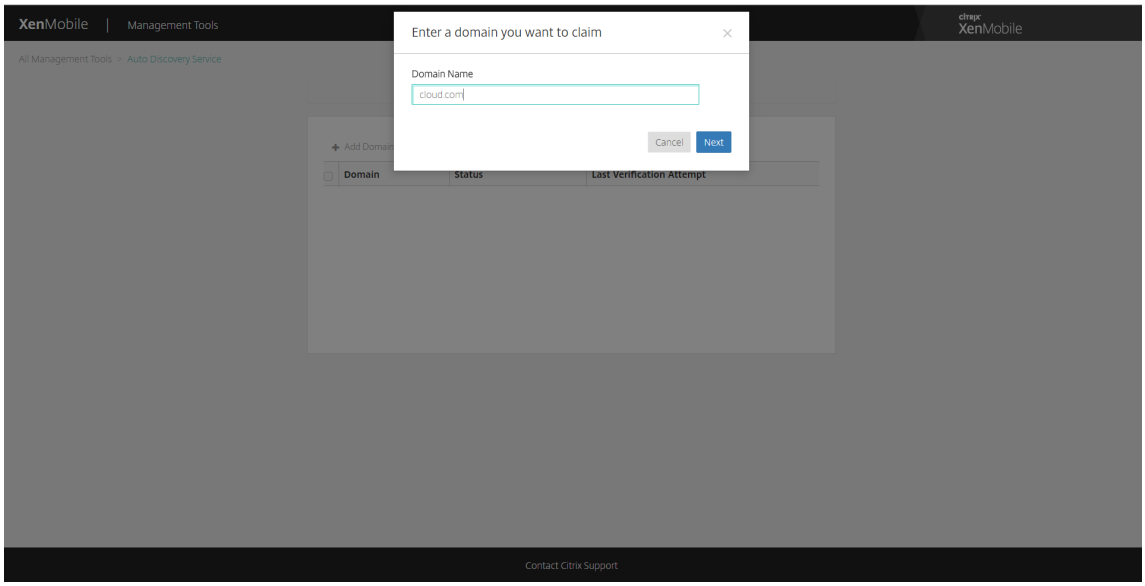


AutoDiscovery のリクエスト

1. AutoDiscovery サービスのページでは、まずドメインを指定する必要があります。［**Add Domain**］ をクリックします。



2. 表示されたダイアログボックスで、お使いの XenMobile 環境のドメイン名を入力してから ［**Next**］ をクリックします。



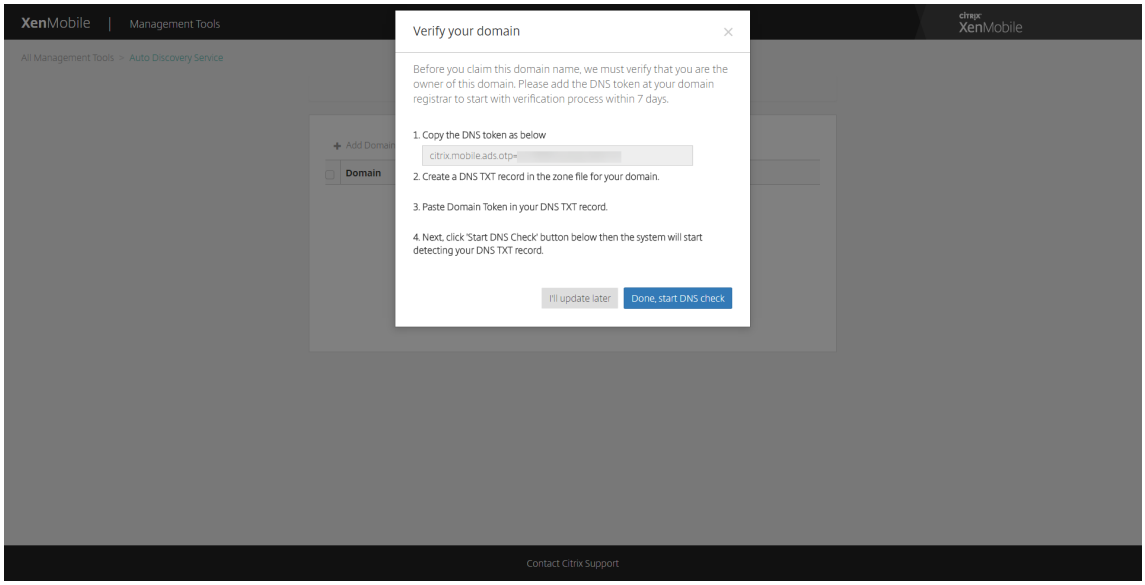
3. 次の手順では、ユーザーがドメインの所有者であることを確認するための手順が示されます。

   - XenMobile ツールポータルで提供された DNS トークンをコピーします。
   - ドメインホスティングプロバイダーポータルで、ドメインのゾーンファイルに DNS TXT レコードを作成します。

     DNS TXT レコードを作成するには、上の手順 2 で追加したドメインのドメインホスティングプロバイダーポータルにログインする必要があります。ドメインホスティングポータルでは、ドメインネームサーバーレコードを編集したり、カスタムの TXT レコードを追加したりできます。サンプルドメイン domain.com のホスティングポータルでの DNS TXT エントリの追加の例。
   - DNS TXT レコードにドメイントークンを貼り付け、ドメインネームサーバーレコードを保存します。
   - XenMobile ツールポータルに戻って ［完了］ をクリックし、DNS チェックを開始します。

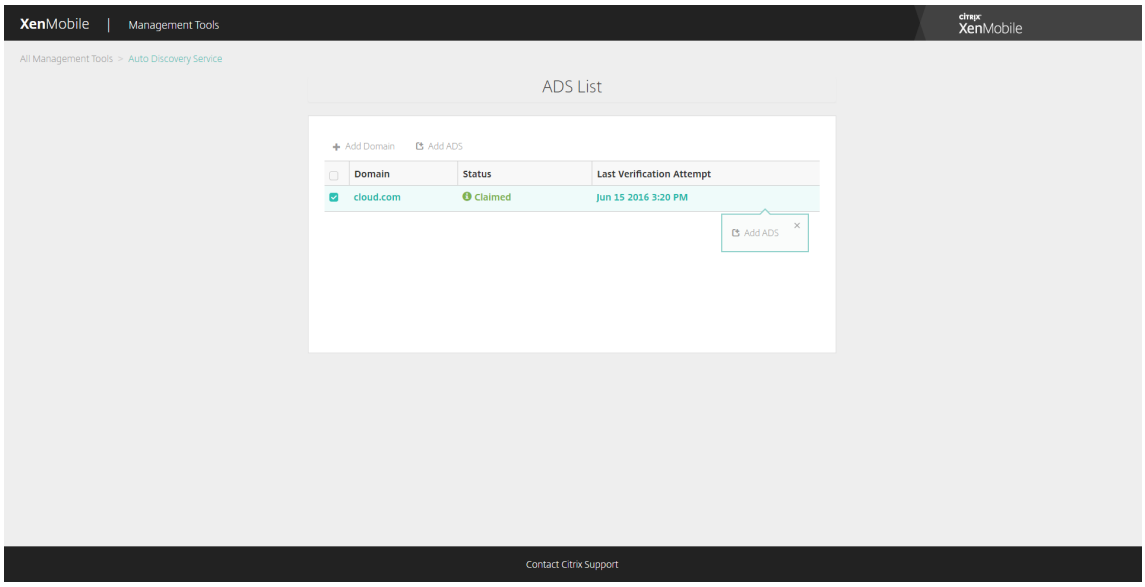
   作成した DNS TXT レコードが検出されます。または、 ［**I'll update later**］ をクリックして、レコードを保存することもできます。［Waiting］ レコードを選択して ［**DNS Check**］ をクリックするまで、DNS チェックは開始されません。

   このチェックにかかる時間は最短で約 1 時間ですが、応答が返されるまでに最大 2 日かかることがあります。さらに、ステータスの変更を確認するには、ポータルを閉じてから再びアクセスする必要がある場合もあります。

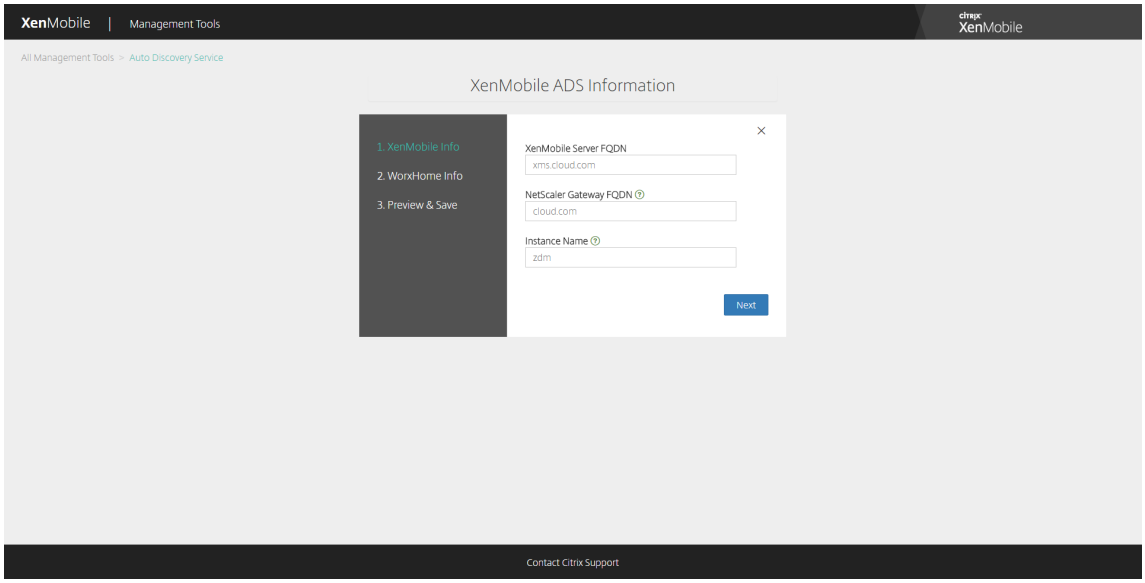


4. ドメインを指定すると、AutoDiscovery サービス情報を入力できるようになります。自動検出をリクエストするドメインレコードを右クリックしてから、［**Add ADS**］ をクリックします。

   ドメインに既に AutoDiscovery レコードがある場合、シトリックステクニカルサポートに事例を記録して、必要に応じて詳細を変更します。



5. **XenMobile Server** の完全修飾ドメイン名、**NetScaler Gateway** の完全修飾ドメイン名、およびインスタンス名を入力して、［**Next**］ をクリックします。不明な場合、デフォルトインスタンスの「zdm」を追加します。



> 注：
>
> 上のスクリーンショットの Worx Home は、現在では Secure Hub と呼ばれている点に注意してください。

6. Secure Hub に次の情報を入力して、［**Next**］ をクリックします。

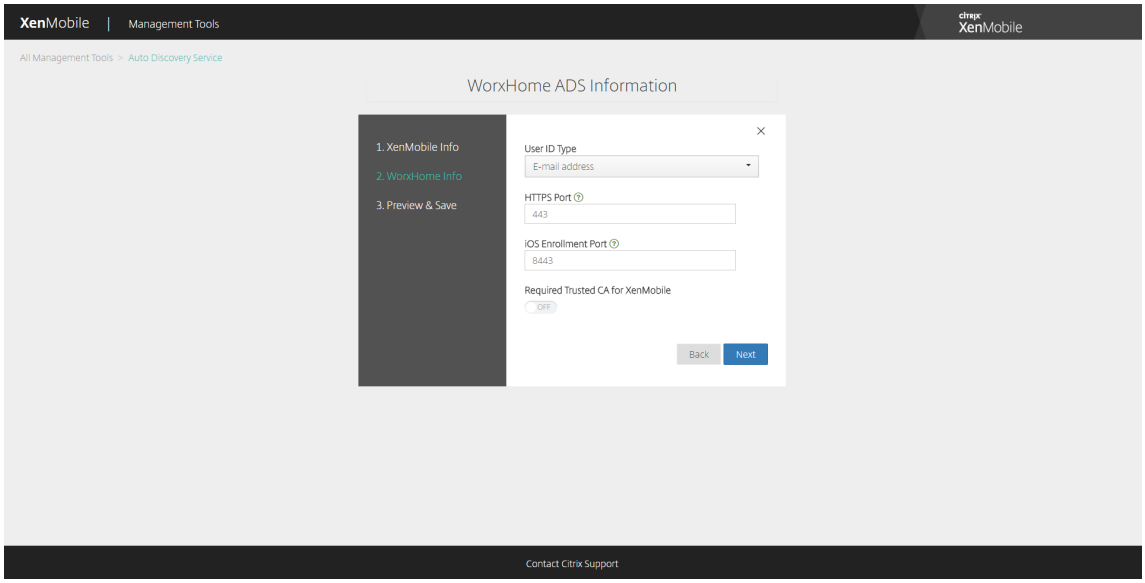
   - **User ID Type**： ユーザーがサインオンに使用する ID の種類（メールアドレスまたは **UPN**）を選択します。

     UPN は、ユーザーの UPN（ユーザープリンシパル名）がメールアドレスと同じである場合に使用されます。どちらの方法も、サーバーアドレスを検出するために入力したドメインを使用します。メールアドレスの場合、ユーザーはユーザー名とパスワードを入力するよう求められます。**UPN** の場合はパスワードを入力するよう求められます。

   - **HTTPS Port**： HTTPS で Secure Hub にアクセスする時に使用するポートを入力します。通常、これはポート 443 です。

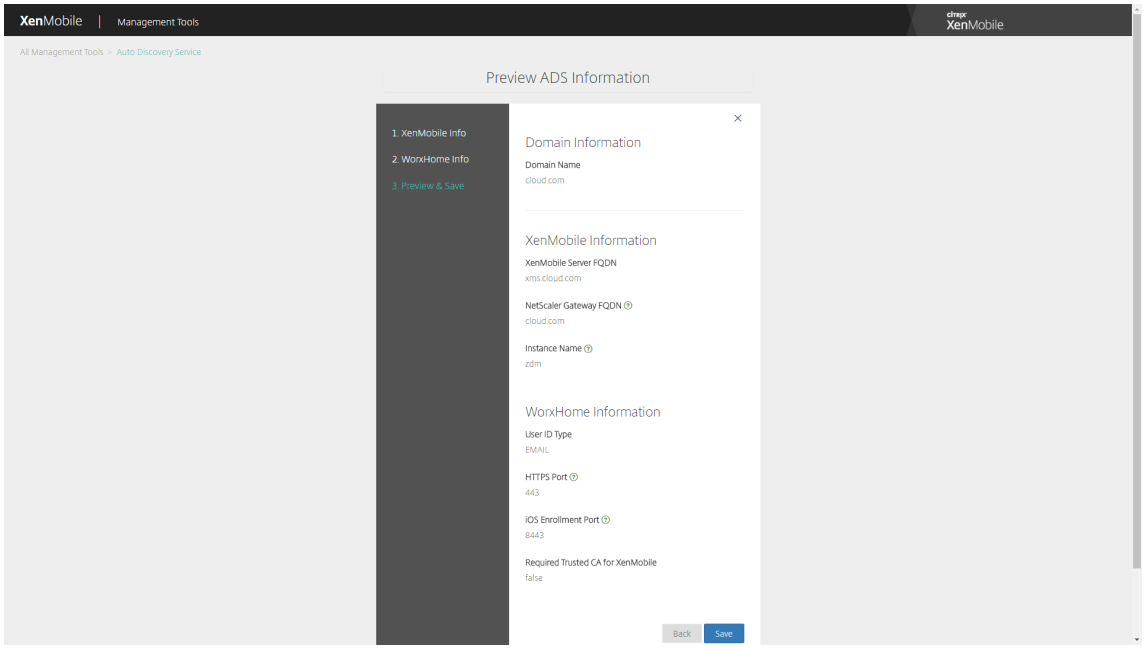
   - **iOS Enrollment Port**： iOS の登録で Secure Hub にアクセスする時に使用するポートを入力します。通常、これはポート 8443 です。

   - **Required Trusted CA for XenMobile**： XenMobile へのアクセスで信頼された機関からの証明書が必要かどうかを指定します。このオプションは、必要に応じて ［**OFF**］ または ［**ON**］ にできます。信頼された証明書を使用するには、シトリックスサポートに証明書のアップロードを依頼してください。証明書ピン留めについて詳しくは、業務用モバイルアプリのドキュメントの「Secure Hub」にある、証明書ピン留めについてのセクションを参照してください。証明書ピン留めが機能するために必要なポートについては、サポート記事XenMobile Port Requirements for ADS Connectivityを参照してください。



> 注:
>
> 上のスクリーンショットの Worx Home は、現在では Secure Hub と呼ばれている点に注意してください。

7. 概要ページに、これまでの手順で入力したすべての情報が表示されます。データが正しいことを確認し、[**Save**] をクリックします。



> 注:
>
> 上のスクリーンショットの Worx Home は、現在では Secure Hub と呼ばれている点に注意してください。

デバイスポリシー

January 10, 2020

ポリシーを作成して、XenMobile とデバイスの連携方法を構成できます。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、プラットフォーム間で異なる場合や、Android デバイスの製造元によっても違いがある場合があります。

各デバイスポリシーの概要説明については、この記事の「デバイスポリシーの概要」を参照してください。

> 注:
>
> 環境がグループポリシーオブジェクト（GPO）で構成されている場合:
>
> Windows 10 で XenMobile デバイスポリシーを構成するときは、次のルールに留意してください。登録済みの Windows 10 デバイス間でポリシーの競合が発生した場合、GPO に合っているポリシーが優先されます。

Android Enterprise コンテナがサポートするポリシーを確認するには、「Android Enterprise」を参照してください。

前提条件

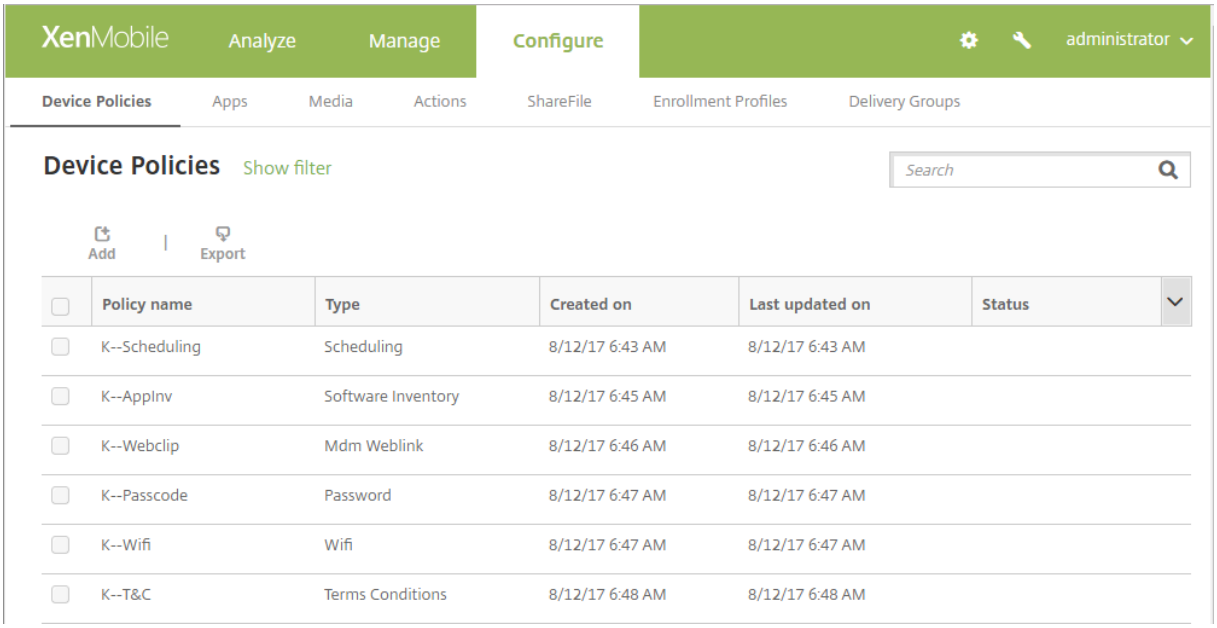
- 使用する予定のデリバリーグループを作成します。
- 必要な CA 証明書をインストールします。

デバイスポリシーの追加

デバイスポリシーの基本的な作成手順は次のとおりです:

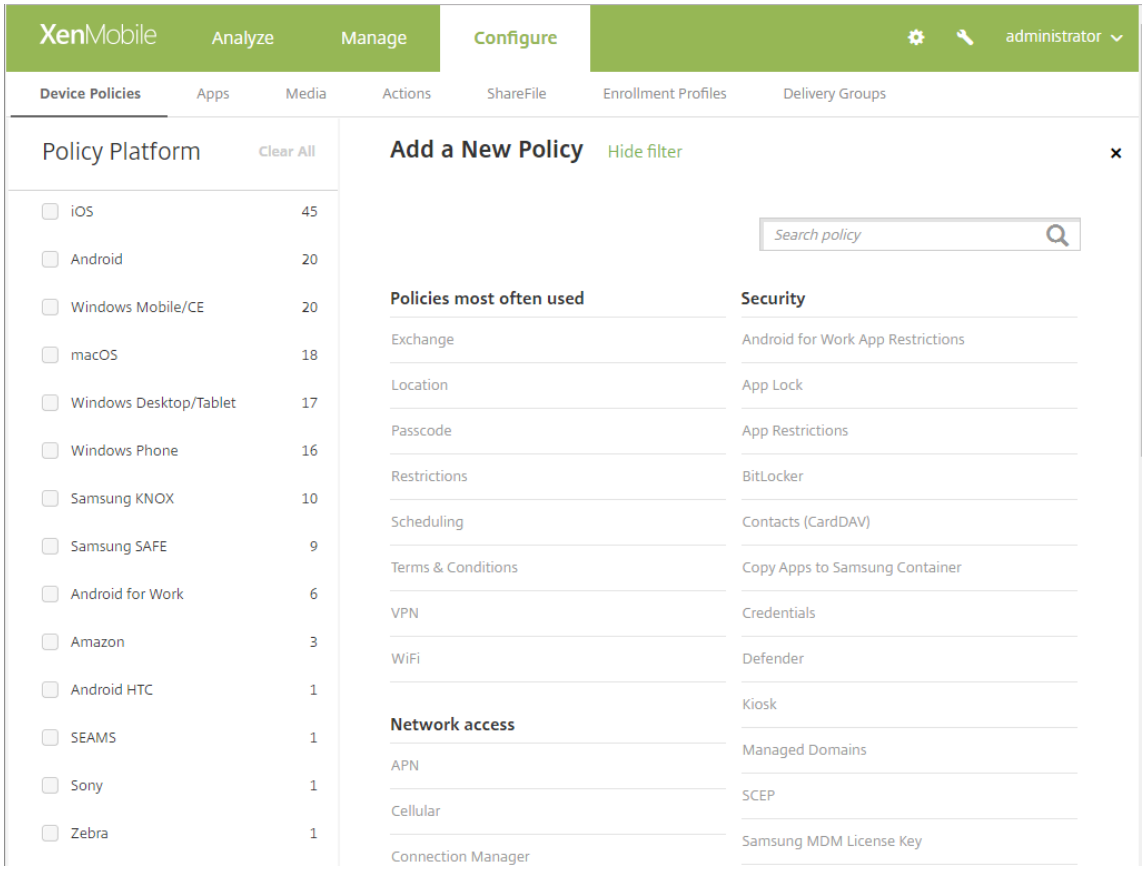
1. ポリシーの名前と説明を指定します。
2. 1 つまたは複数のプラットフォームのポリシーを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

デバイスポリシーを作成し、管理するには、［構成］**>**［デバイスポリシー］ の順に選択します。

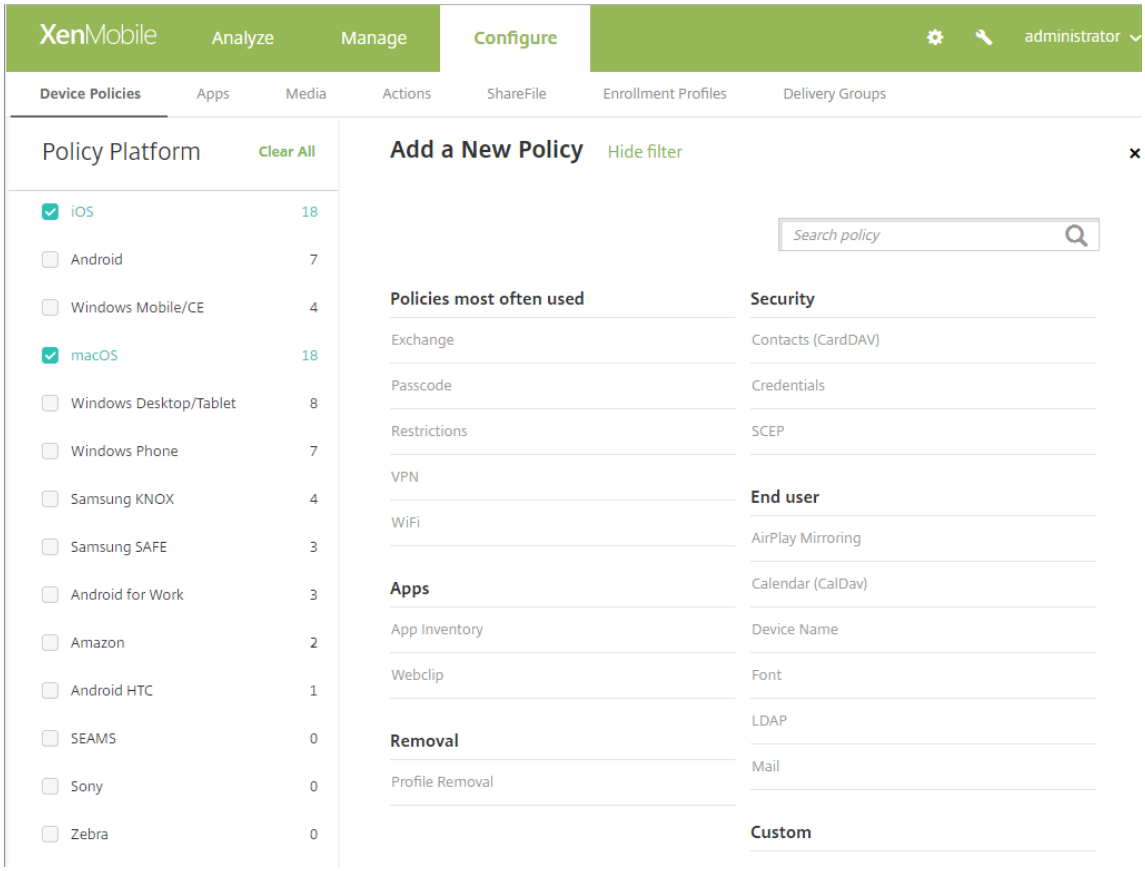


ポリシーを追加するには

1. ［デバイスポリシー］ ページで、 ［追加］ をクリックします。 ［新しいポリシーの追加］ ページが開きます。



2. 1 つまたは複数のプラットフォームをクリックし、選択したプラットフォームのデバイスポリシー一覧を表示します。ポリシーの追加を続けるにはポリシー名をクリックします。



検索ボックスにポリシーの名前を入力することもできます。入力すると一致候補が表示されます。一覧の中に目的のポリシーがあれば、それをクリックします。その結果、選択したポリシーのみが残ります。それをクリックして、そのポリシーの［ポリシー情報］ページを開きます。

3. ポリシーに含めるプラットフォームを選択します。選択したプラットフォームの構成ページが手順 5. で表示されます。
4. ［ポリシー情報］ページで必要な情報を入力して、［次へ］をクリックします。［ポリシー情報］ページにはポリシー名などの情報が集約されているため、ポリシーの識別や追跡に役立ちます。このページはすべてのポリシーで類似しています。
5. プラットフォームページの入力を完了します。手順 3 で選択した各プラットフォームのページが開きます。これらのページはポリシーごとに異なります。ポリシーはプラットフォームによって異なる可能性があります。すべてのポリシーがすべてのプラットフォームに適用される訳ではありません。

   一部のページにはアイテムの表が含まれています。既存の項目を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログで、［削除］をクリックします。

   既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。

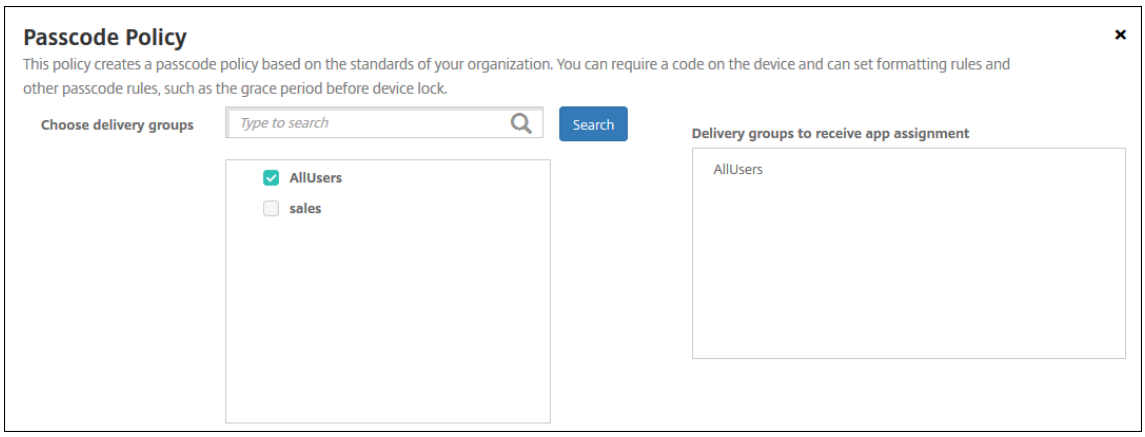
展開ルール、割り当て、およびスケジュールを構成するには

展開規則の構成について詳しくは、「リソースの展開」を参照してください。

1. プラットフォームのページで、［展開規則］ を展開して以下の設定を構成します。デフォルトでは ［基本］ タブが表示されます。
   - 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは ［すべて］ です。
   - ［新しい規則］ をクリックして条件を定義します。
   - 一覧から ［デバイス所有権］ や ［**BYOD**］ などの条件を選択します。
   - 条件をさらに追加する場合は、［新しい規則］ をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［詳細］ タブをクリックし、ブール値オプションを使用して規則を組み合わせます。［基本］ タブで選択した条件が表示されます。
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   - ［**AND**］、［**OR**］、または［**NOT**］をクリックします。
   - 一覧から、規則に追加する条件を選択します。次に右側のプラス記号（**+**）をクリックし、規則に条件を追加します。

     いつでも、条件をクリックして選択し、［編集］ をクリックして条件を変更したり、［削除］ をクリックして条件を削除したりすることができます。
   - ［新しい規則］ をクリックして別の条件を追加します。
4. ［次へ］ をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、［割り当て］ ページに移動します。
5. ［割り当て］ ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、［アプリ割り当てを受信するためのデリバリーグループ］ ボックスにそのグループが表示されます。

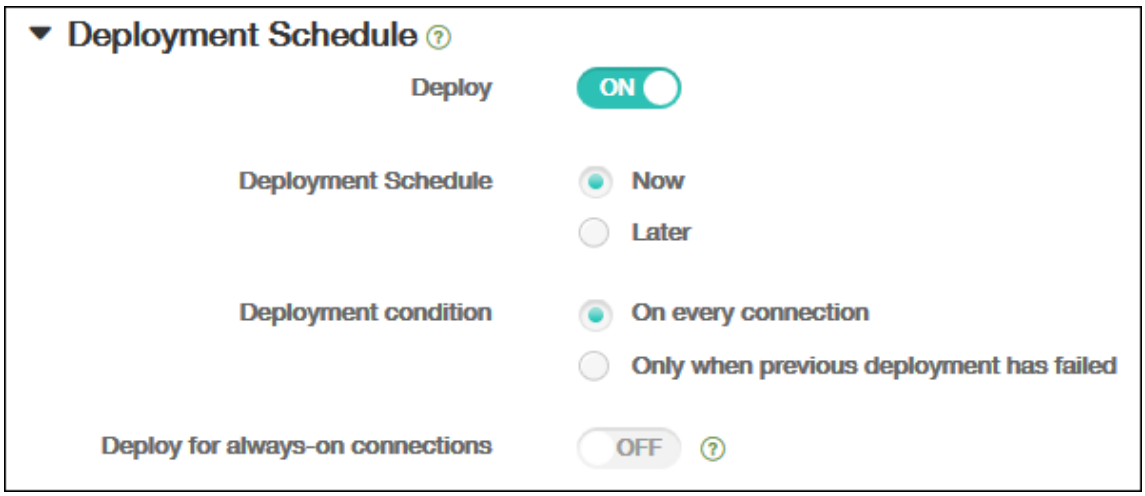
   ［アプリ割り当てを受信するためのデリバリーグループ］ ボックスは、デリバリーグループを選択するまで表示されません。



6. ［割り当て］ ページで ［展開スケジュール］ を展開して以下の設定を構成します:

   - ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。
   - ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
   - ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
   - ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリックします。デフォルトのオプションは、［接続するたび］ です。
   - ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

     > 注:
     >
     > このオプションは、［設定］ > ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
     >
     > 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。

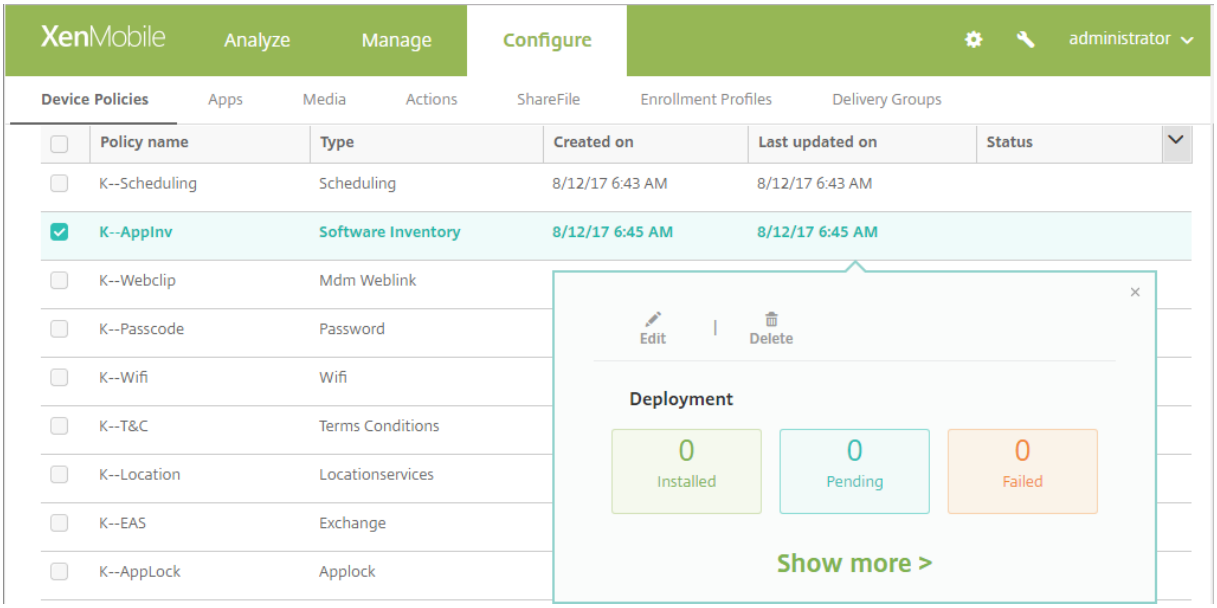


7. ［保存］ をクリックします。

   ポリシーが ［デバイスポリシー］ の表に表示されます。

デバイスポリシーの編集または削除

ポリシーを編集または削除するには、ポリシーの横にあるチェックボックスをオンにして、ポリシー一覧の上にオプションメニューを表示します。または、一覧でポリシーをクリックして、その項目の右にオプションメニューを表示します。



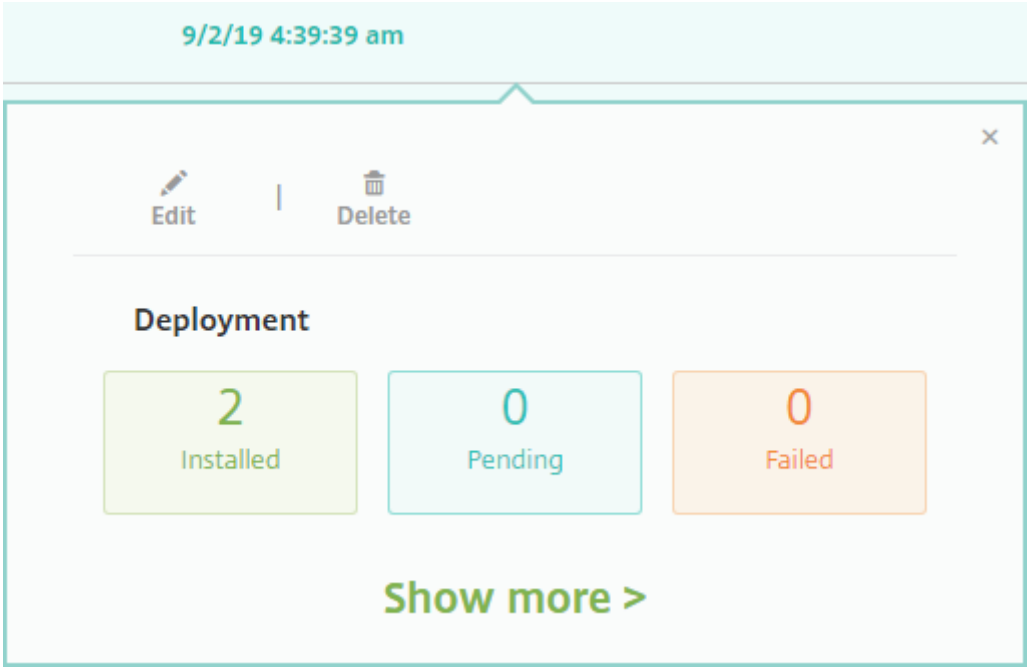
ポリシーの詳細を表示するには、 ［詳細表示］ をクリックします。

デバイスポリシーのすべての設定を編集するには、 ［編集］ をクリックします。

［削除］ をクリックすると、確認ダイアログボックスが開きます。もう一度 ［削除］ をクリックします。

ポリシー展開ステータスの確認

［構成］ > ［デバイスポリシー］ ページでポリシー行をクリックし、展開ステータスを確認します。



ポリシーの展開が保留中の場合、ユーザーは ［環境設定］ > ［デバイス情報］ > ［ポリシーの更新］ の順にタップし、Secure Hub からポリシーを更新できます。

デバイスからのデバイスポリシーの削除

デバイスからデバイスポリシーを削除する手順は、プラットフォームによって異なります。

- Android

  Android デバイスからデバイスポリシーを削除するには、XenMobile アンインストールデバイスポリシーを使用します。詳しくは、「XenMobile アンインストールデバイスポリシー」を参照してください。

- iOS と macOS

  iOS または macOS デバイスからデバイスポリシーを削除するには、プロファイル削除デバイスポリシーを使用します。iOS および macOS デバイスでは、すべてのポリシーが MDM プロファイルの一部です。したがって、削除するポリシーに限定したプロファイル削除デバイスポリシーを作成できます。その他のポリシーとプロファイルはデバイスに残ります。詳しくは、「プロファイル削除デバイスポリシー」を参照してください。

- Windows 10

  Windows 10 デスクトップまたはタブレットデバイスから直接デバイスポリシーを削除することはできません。ただし、次のいずれかの方法を使用できます:

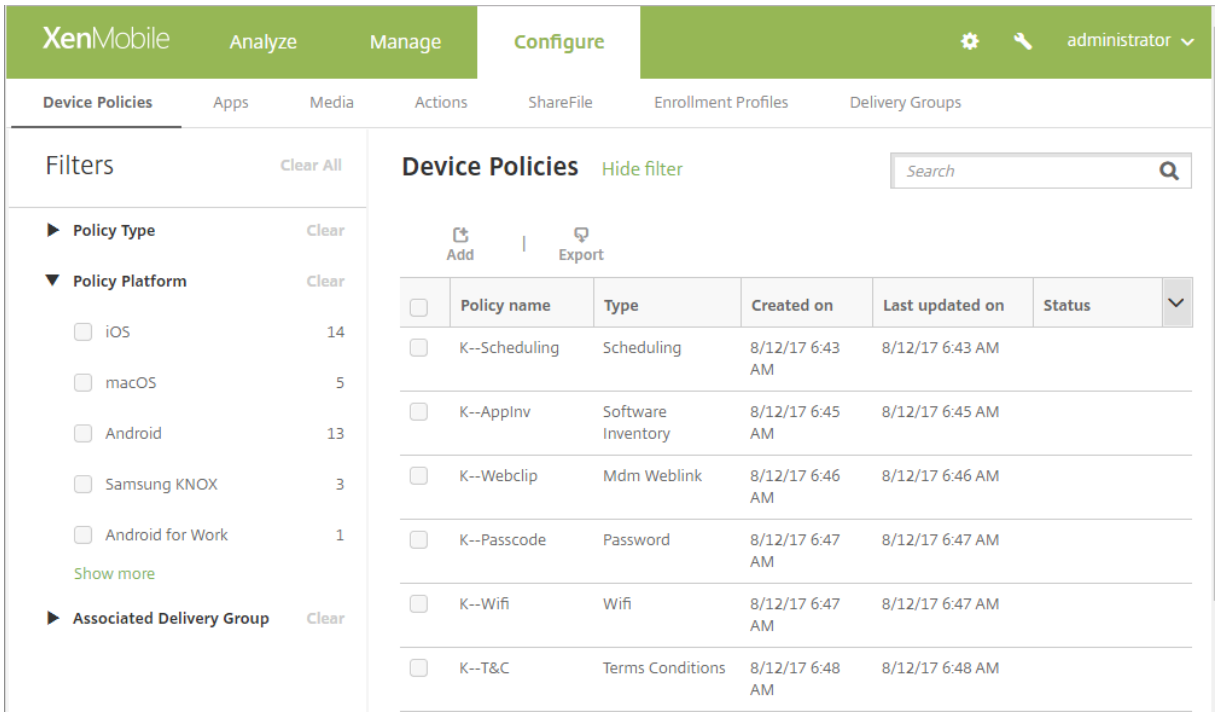
  - デバイスの登録を解除し、新しいポリシーセットをデバイスにプッシュします。その後、ユーザーが再登録します。
  - 特定のデバイスを選択的にワイプするには、セキュリティ操作をプッシュします。この操作は、企業のすべてのアプリとデータをデバイスから削除します。次に、そのデバイスだけを含むデリバリーグループからデバイスポリシーを削除し、デリバリーグループをデバイスにプッシュします。その後、ユーザーが再登録します。

- Chrome OS

  Chrome OS デバイスからデバイスポリシーを削除するには、そのデバイスだけを含むデリバリーグループからデバイスポリシーを削除します。その後、デリバリーグループをデバイスにプッシュします。

追加されたデバイスポリシーの一覧のフィルター

ポリシーの種類、プラットフォーム、および関連するデリバリーグループで追加されたポリシー一覧にフィルターすることができます。［構成］**>**［デバイスポリシー］ページで、［フィルターを表示］をクリックします。一覧で、表示する項目のチェックボックスをオンにします。



［このビューを保存］をクリックしてフィルターを保存します。フィルターの名前が、［このビューを保存］ボタンの下のボタンに表示されます。

デバイスポリシーの概要

デバイスポリシー名	デバイスポリシーの説明
AirPlay ミラーリング	特定の AirPlay デバイス（Apple TV やほかの Mac コンピューターなど）を iOS デバイスに追加します。監視対象デバイスのホワイトリストにデバイスを追加するオプションもあります。このオプションは、ホワイトリストの AirPlay デバイスのみにユーザーを制限します。
AirPrint	AirPrint プリンターを iOS デバイスの AirPrint プリンター一覧に追加します。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。
Android Enterprise のアプリ権限	仕事用プロファイル内で、Android Enterprise アプリへの要求で、Google で「危険」とされる権限をどう処理するかを構成します。
Android Enterprise アプリの制限	Android アプリに関連する制限を更新します。
APN	特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。ほとんどの新しい電話機において、この設定は既に定義されています。このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマー APN を使用しない組織で使用します。
アプリアクセス	デバイス上で必須、オプション、または禁止されるアプリの一覧を定義します。次に、そのアプリ一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。
アプリ属性	iOS デバイスのための属性（管理対象アプリのバンドル ID やアプリごとの VPN 識別子など）を指定します。
アプリ構成	管理対象の構成をサポートするアプリのさまざまな設定や動作をリモートで構成します。そのために、XML 構成ファイル（プロパティリスト、または plist と呼ばれる）を iOS デバイスに展開します。または、キー/値ペアを Windows 10 phone、デスクトップ、タブレットデバイスに展開します。

デバイスポリシー名	デバイスポリシーの説明
アプリインベントリ	管理対象デバイス上のアプリのインベントリを収集します。XenMobile は、次にインベントリをそのデバイスに展開されたアプリケーションアクセスポリシーと比較します。この方法で、アプリアクセスのブラックリストまたはホワイトリストにあるアプリを検出し、それに応じて対応できます。
アプリのロック	ユーザーが iOS または特定の Android デバイスで実行できるアプリと実行できないアプリの一覧を定義します。
アプリネットワーク使用状況	ネットワーク使用状況規則を設定して、iOS デバイスで管理対象のアプリが携帯データネットワークなどのネットワークをどのように使用するのかを指定します。規則は管理対象のアプリにのみ適用されます。管理対象のアプリケーションとは、XenMobile を使用してユーザーのデバイスに展開されるアプリケーションです。
アプリ制限	Samsung KNOX デバイスへのユーザーによるインストールを禁止するアプリのブラックリストを作成します。ユーザーによるインストールを許可するアプリのホワイトリストも作成できます。
アプリアンインストール	ユーザーのデバイスからアプリを削除します。
アプリのアンインストール制限	ユーザーがアンインストールできる、またはアンインストールできないアプリを指定します。
アプリ通知	iOS ユーザーが指定したアプリから通知を受け取る方法を制御します。
BitLocker	Windows 10 デバイスの BitLocker インターフェイスで使用できる設定を構成します。
ブラウザー	ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、デバイスで使用できるブラウザー機能を定義したりします。
カレンダー（CalDav）	カレンダー（CalDAV）アカウントを iOS または macOS デバイスに追加します。CalDAV アカウントによって、ユーザはスケジュールデータを CalDAV をサポートするサーバーと同期させることができます。
携帯ネットワーク	携帯ネットワーク設定を構成します。

デバイスポリシー名	デバイスポリシーの説明
接続マネージャー	インターネットおよびプライベートネットワークに自動的に接続するアプリの接続設定を指定します。このポリシーは Windows Pocket PC でのみ使用できます。
連絡先（CardDAV）	iOS 連絡先（CardDAV）アカウントを iOS または macOS デバイスに追加します。CardDAV アカウントによって、ユーザは連絡先データを CardDAV をサポートするサーバーと同期させることができます。
OS 更新の制御	サポートされている監視対象デバイスに最新の OS 更新を展開します。
Samsung コンテナへのアプリのコピー	デバイスに既にインストールされているアプリを、サポートされている Samsung デバイス上の SEAMS コンテナまたは KNOX コンテナにコピーします。SEAMS コンテナにコピーされたアプリは、デバイスのホーム画面で使用できます。KNOX コンテナにコピーされたアプリは、ユーザーが KNOX コンテナにサインインした場合のみ使用できます。
資格情報	XenMobile PKI 構成で統合認証を有効にします。たとえば、PKI エンティティ、キーストア、資格情報プロバイダー、サーバー証明書などを使用します。
カスタム XML	デバイスプロビジョニング、デバイス機能の有効化、デバイスの構成、および障害管理などの機能をカスタマイズします。
ディフェンダー	デスクトップおよびタブレットの Windows 10 で Windows Defender 設定を構成します。
ファイルおよびフォルダーの削除	Windows Mobile/CE デバイスから特定のファイルまたはフォルダーを削除します。
レジストリキーおよび値の削除	Windows Mobile/CE デバイスから特定のレジストリキーおよび値を削除します。

デバイスポリシー名	デバイスポリシーの説明
デバイス正常性構成証明	Windows 10 デバイスにデバイスの正常性状態を報告させます。そのため、分析目的で特定のデータおよびランタイム情報を Health Attestation Service （HAS）に送信させます。HAS は、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスから XenMobile に送信されます。XenMobile は正常性構成証明書を受信すると、その内容に基づいて、管理者が構成した自動アクションを展開します。
デバイス名	デバイスを特定できるように、iOS デバイスおよび macOS デバイスに名前を設定します。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。
教育の構成	Apple の教育向け機能を使用するように講師および生徒のデバイスを構成します。講師がクラスルームアプリを使用する場合は、教育の構成デバイスポリシーが必要です。
エンタープライズハブ	エンタープライズハブの業務用ストア経由で Windows Phone にアプリを配信します。XenMobile では、Windows Phone Secure Hub の 1 つのモードについて、1 つの Enterprise Hub ポリシーだけがサポートされています。たとえば、複数の Enterprise Hub ポリシーをさまざまなバージョンの Secure Home for XenMobile Enterprise Edition 用に作成する必要はありません。デバイスの登録中にのみ最初のエンタープライズハブポリシーを展開できます。
Exchange	デバイス上のネイティブの電子メールクライアントで ActiveSync メールを有効にします。
ファイル	ユーザーに対して特定の機能を実行するスクリプトファイルを XenMobile に追加します。または、Android デバイスユーザーがデバイスでアクセスできるドキュメントファイルを追加することができます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。

デバイスポリシー名	デバイスポリシーの説明
FileVault	このポリシーによって、macOS デバイスで登録された FileVault デバイスの暗号化を有効にできます。ログイン中にユーザーが FileVault のセットアップをスキップできる回数を制御することもできます。macOS 10.7 以降で使用できます。
ファイアウォール	ファイアウォールの設定を構成します。デバイスで許可または禁止する IP アドレス、ポート、ホスト名を入力します。プロキシおよびプロキシ再ルーティングの設定を構成することもできます。
フォント	iOS デバイスおよび macOS デバイスにフォントを追加します。フォントは TrueType（.TTF）または OpenType（.OFT）である必要があります。XenMobile はフォントコレクション（.TTC または.OTC）をサポートしていません。
ホーム画面のレイアウト	iOS 9.3 以降の監視対象デバイスのホーム画面について、アプリとフォルダーのレイアウトを指定します。
iOS および macOS プロファイルのインポート	iOS および macOS デバイス用のデバイス構成 XML ファイルを XenMobile にインポートします。XML ファイルには、Apple Configurator を使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。
キオスク	Samsung SAFE デバイスでのアプリの使用を制限します。利用可能なアプリを特定のアプリに制限できます。このポリシーは、特定の種類またはクラスのアプリのみを実行することを目的とするコーポレートデバイスで役立ちます。また、このポリシーを使用して、キオスクモードのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。
Launcher 構成	許可されたアプリや Launcher アイコン用のカスタムロゴイメージなど、Android デバイス上の Citrix Launcher の設定を指定します。
LDAP	LDAP サーバーホスト名などの必要なアカウント情報など、iOS デバイスに使用する LDAP サーバーに関する情報を指定します。また、LDAP サーバーの照会に使用する LDAP 検索ポリシーのセットが提供されます。

デバイスポリシー名	デバイスポリシーの説明
場所	そのデバイスの GPS が Secure Hub に対応している場合に、地図上で位置を検出できるデバイスを許可します。このポリシーをデバイスに展開した後、XenMobile Server から位置を確認するコマンドを送信することができます。デバイスはその後位置情報を返信します。XenMobile は、ジオフェンシングおよび追跡ポリシーもサポートします。
メール	iOS デバイスまたは macOS デバイスのメールアカウントを構成します。
管理対象ドメイン	メールおよび Safari ブラウザーに適用する管理対象ドメインを定義します。管理対象ドメインを使用すると、Safari を使用してドメインからダウンロードしたドキュメントを開くことができるアプリを制御して、会社のデータを保護することができます。iOS8 以降の管理対象デバイスでは、URL またはサブドメインを使用して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御できます。
MDM オプション	監視対象の iOS 7.0 以降のモバイルデバイスで［iPhone と iPad を探す］の［アクティベーションロック］を管理します。
組織情報	XenMobile が iOS デバイスに展開するアラートメッセージの組織情報を指定します。
パスコード	管理対象デバイスに PIN コードまたはパスワードを適用します。デバイス上でパスコードの複雑さやタイムアウトを設定できます。
パーソナルホットスポット	ユーザーが WiFi ネットワーク圏外にいてもインターネットに接続できるようにします。ユーザーは、個人用ホットスポット機能を介して iOS デバイスの携帯データネットワーク接続で接続します。
プロファイルの削除	iOS デバイスまたは macOS デバイスからアプリプロファイルが削除されます。

デバイスポリシー名	デバイスポリシーの説明
プロビジョニングプロファイル	エンタープライズ配信のプロビジョニングプロファイルを指定してデバイスに送信します。iOS エンタープライズアプリを開発し、コード署名をするときは、通常は、プロビジョニングプロファイルを含めます。Apple は、iOS デバイスで実行するアプリについてはプロファイルを要求します。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。
プロビジョニングプロファイルの削除	iOS プロビジョニングプロファイルを削除します。
プロキシ	Windows Mobile/CE および iOS を実行しているデバイスのグローバル HTTP プロキシ設定を指定します。グローバル HTTP プロキシポリシーはデバイスごとに 1 つのみ展開できます。
レジストリ	Windows Mobile/CE デバイスの管理に使用するレジストリキーおよび値を定義します。Windows Mobile/CE のレジストリには、アプリ、ドライバー、ユーザー設定、および構成設定に関するデータが格納されています。
リモートサポート	Samsung KNOX デバイスへのリモートアクセスを行うことができます。2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。
制限	管理対象デバイスをロックダウンしたり、機能を制御する数百のオプションが提供されています。制限オプションの例：カメラやマイクの無効化、ローミング規則の適用、アプリストアのようなサードパーティサービスへのアクセスの適用。
ローミング	iOS デバイスおよび Windows Mobile/CE デバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成します。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。

デバイスポリシー名	デバイスポリシーの説明
Samsung MDM ライセンスキー	SAFE のポリシーおよび制限を展開する前に、デバイスに展開する必要がある組み込みの Samsung Enterprise License Management（ELM）キーを指定します。XenMobile は、Samsung Enterprise Firmware-Over-The-Air（E-FOTA）サービスもサポートしています。XenMobile は Samsung for Enterprise（SAFE）および Samsung KNOX ポリシーの両方をサポートし、拡張しています。
スケジュール設定	Android および Windows Mobile デバイスが MDM 管理、アプリのプッシュ、ポリシーの展開のために XenMobile Server に接続する際に必要です。このポリシーをデバイスに送信せず、Google FCM を有効にしない場合、デバイスはサーバーに接続することができません。
SCEP	iOS デバイスおよび macOS デバイスを構成し、外部 SCEP サーバーから証明書を取得します。XenMobile に接続されている PKI から SCEP を使用してデバイスに証明書を配布することもできます。そのためには、PKI エンティティと PKI プロバイダーを分散モードで作成します。
SSO アカウント	ユーザーが 1 回サインオンするだけで、XenMobile および社内リソースにアクセスすることができるように、シングルサインオン（SSO）アカウントを作成します。デバイスに資格情報を保存する必要はありません。XenMobile では、SSO アカウントのエンタープライズユーザーの資格情報は、App Store からのアプリを含む複数のアプリで使用されます。このポリシーは、Kerberos 認証と互換性があります。iOS で使用できます。
ストレージ暗号化	内部ストレージおよび外部ストレージを暗号化します。一部のデバイスについては、このポリシーによって、ユーザーがデバイスでメモリーカードを使用できなくなります。

デバイスポリシー名	デバイスポリシーの説明
購読済みカレンダー	サブスクライブされたカレンダーを iOS デバイスのカレンダー一覧に追加します。ユーザーのデバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みであることを確認します。
使用条件	ユーザーが社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに要求します。ユーザーが XenMobile にデバイスを登録するときに、ユーザーは自分のデバイスを登録するために契約条件に同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。
トンネル	リモートサポートにのみ使用します。リモートサポートを使用すると、ヘルプデスクの担当者は管理対象の Windows CE および Android モバイルデバイスをリモートで制御できます。XenMobile サービスのお客様はリモートサポートを利用できません。またリモートサポートはクラスター化されたオンプレミスの XenMobile Server 展開ではサポートされていません。2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。
VPN	従来の VPN Gateway テクノロジを使用するバックエンドシステムへのアクセスを提供します。このポリシーでは、デバイスに展開できる VPN ゲートウェイ接続の詳細を提供します。XenMobile は、Cisco AnyConnect、Juniper、および Citrix VPN などの、いくつかの VPN プロバイダーをサポートしています。VPN ゲートウェイがこのオプションをサポートしている場合、このポリシーを CA にリンクして、VPN オンデマンドを有効にできます。
壁紙	.png ファイルまたは.jpg ファイルを追加して、iOS デバイスのロック画面かホーム画面、または両方の画面の壁紙に設定します。iPad および iPhone で異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開します。

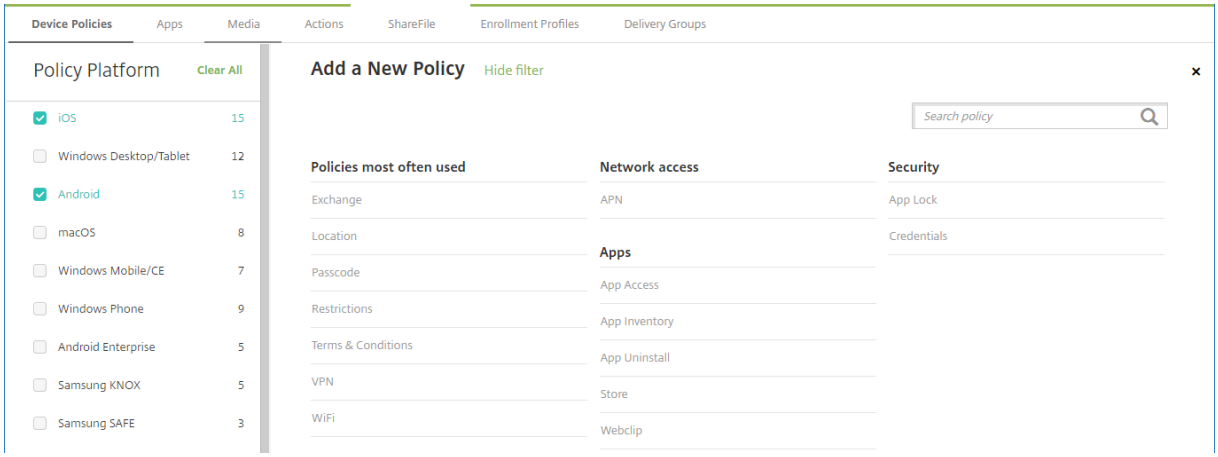
デバイスポリシー名	デバイスポリシーの説明
Web コンテンツフィルター	fiOS デバイスの Web コンテンツをフィルターします。XenMobile は、Apple のオートフィルター機能およびホワイトリストとブラックリストに追加したサイトを使用します。iOS の監視対象デバイスでのみ利用できます。
Web クリップ	ショートカットや Web クリップを Web サイトに配置してユーザーデバイスのアプリと一緒に表示します。iOS、macOS、Android デバイスの Web クリップを表す独自のアイコンを指定できます。Windows タブレットのみ、ラベルおよび URL が必要になります。
Wi-Fi	管理者が WiFi ルーターの詳細を管理対象デバイスに展開することを許可します。ルーターの詳細には、SSID、認証データ、構成データなどがあります。
Windows CE 証明書	外部の PKI を基に Windows Mobile/CE PKI 証明書を作成し、ユーザーのデバイスに配布します。
Windows Information Protection	設定した適用レベルでの Windows Information Protection を必要とするアプリを指定します。このポリシーは、Windows 10 バージョン 1607 以降の監視対象デバイスに適用されます。
XenMobile Store	XenMobile Store Web クリップが、ユーザーデバイスのホーム画面に表示されるかどうかを指定します。
XenMobile オプション	Android デバイスおよび Windows Mobile/CE デバイスから XenMobile に接続するときの Secure Hub の動作を構成します。
XenMobile のアンインストール	XenMobile を Android デバイスおよび Windows Mobile/CE デバイスからアンインストールします。このポリシーを展開すると、展開グループ内のすべてのデバイスから XenMobile が削除されます。

プラットフォームごとのデバイスポリシー

May 21, 2019

プラットフォーム別ポリシーを参照するには、次の手順を実行します:

1. XenMobile コンソールで、［構成］ > ［デバイスポリシー］ に移動します。
2. ［追加］ をクリックします。
3. デバイスプラットフォームが、［ポリシープラットフォーム］ ペインに一覧表示されます。このペインが開いていない場合は、［フィルターを表示］ をクリックします。
4. 1 つのプラットフォームで使用可能なすべてのポリシーの一覧を表示するには、このプラットフォームを選択します。複数のプラットフォームで使用可能なポリシーの一覧を表示するには、各プラットフォームを選択します。ポリシーは、選択した各プラットフォームに適用される場合にのみ一覧に表示されます。



最新リリースの XenMobile は、以下のプラットフォームのデバイスポリシーをサポートしています。

- Amazon
- Android
- Android HTC
- Android Sony
- Android TouchDown
- Android Enterprise
- Android Zebra
- Chrome OS
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Samsung SEAMS
- Windows 10 デスクトップ/タブレット
- Windows 10 Phone
- Windows Mobile/CE

XenMobile の最新リリースでサポートされるデバイスについて詳しくは、「サポート対象のデバイスプラットフォーム」を参照してください。

> 注：
>
> 環境がグループポリシーオブジェクト（GPO）で構成されている場合：
>
> Windows 10 で XenMobile デバイスポリシーを構成するときは、次のルールに留意してください。登録済みの Windows 10 デバイス間でポリシーの競合が発生した場合、GPO に合っているポリシーが優先されます。

AirPlay ミラーリングデバイスポリシー

January 10, 2020

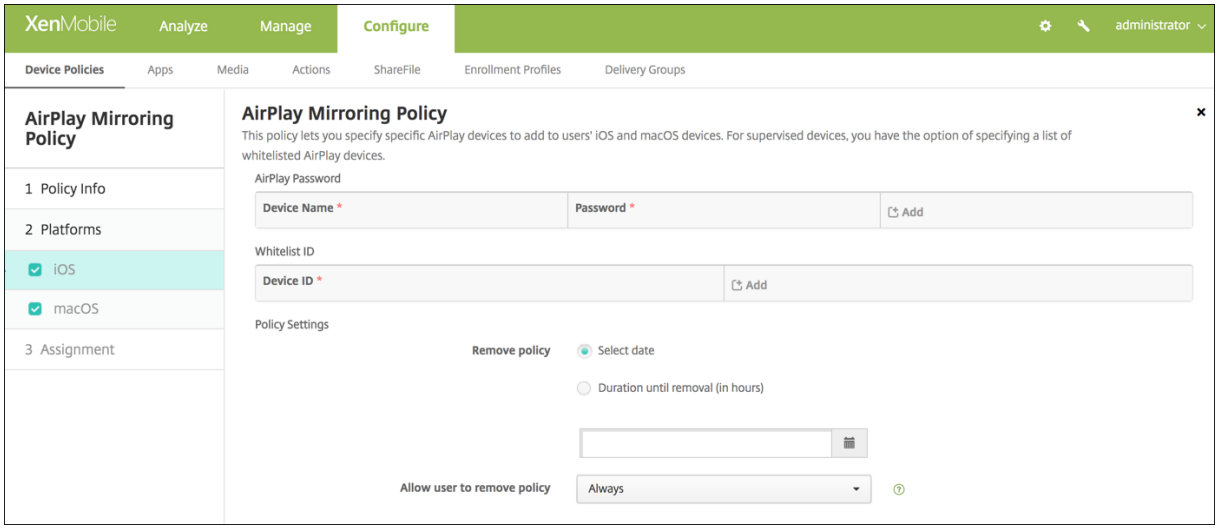
Apple AirPlay 機能を使用すると、Apple TV を介して iOS デバイスから TV 画面にコンテンツをワイヤレスでストリーム配信したり、デバイス上の表示を TV 画面またはほかの Mac コンピューターに正確にミラーリングしたりすることができます。

XenMobile でデバイスポリシーを追加して、特定の AirPlay デバイス（Apple TV やほかの Mac コンピューターなど）をユーザーの iOS デバイスに追加することができます。また、デバイスを監視対象デバイスのホワイトリストに追加して、ユーザーをホワイトリストにある AirPlay デバイスのみに限定するオプションもあります。デバイスを Supervised モードにする方法については、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

> 注：
>
> 続行する前に、追加するすべてのデバイスのデバイス ID とパスワードがあることを確認してください。

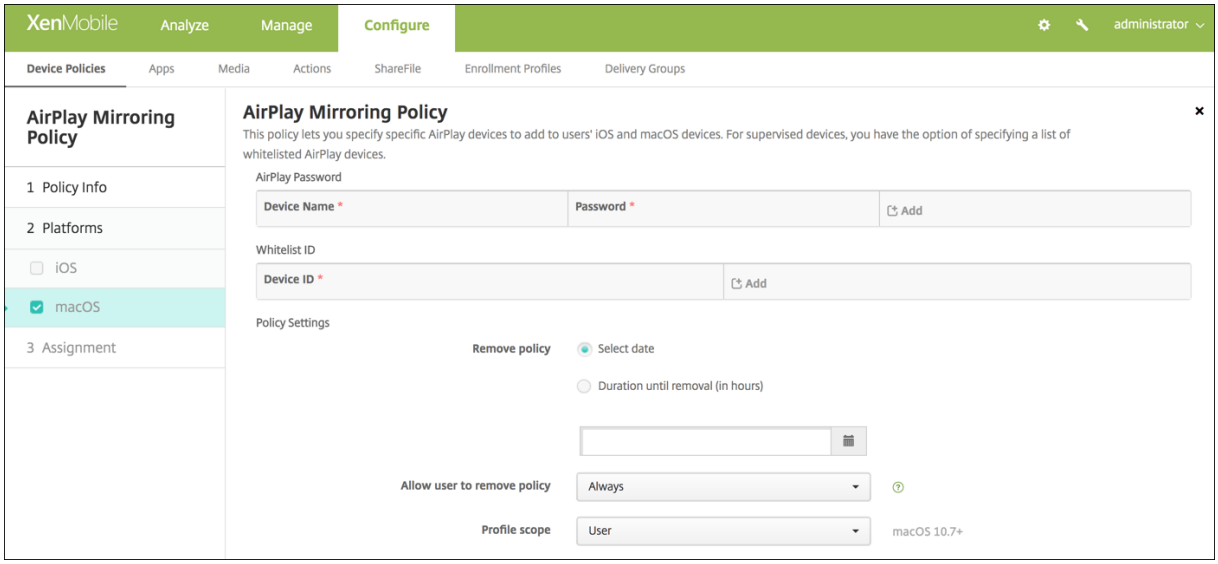
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **AirPlay** パスワード: 追加するデバイスごとに、［追加］ をクリックして以下の操作を行います。
  - デバイス **ID**: ハードウェアのアドレス（MAC アドレス）を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - パスワード: 任意で、デバイスのパスワードを入力します。
  - ［追加］ をクリックしてデバイスを追加するか、［キャンセル］ をクリックしてデバイスの追加を取り消します。
- ホワイトリスト **ID**: この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーのデバイスで使用できる AirPlay デバイスのデバイス ID のみを追加できます。一覧に追加する AirPlay デバイスごとに、［追加］ をクリックして以下の操作を行います。
  - デバイス **ID**: デバイス ID を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - ［追加］ をクリックしてデバイスを追加するか、［キャンセル］ をクリックしてデバイスの追加を取り消します。

macOS 設定



- **AirPlay** パスワード: 追加するデバイスごとに、［追加］ をクリックして以下の操作を行います。
  - デバイス **ID**: ハードウェアのアドレス（MAC アドレス）を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - パスワード: 任意で、デバイスのパスワードを入力します。
  - ［追加］ をクリックしてデバイスを追加するか、［キャンセル］ をクリックしてデバイスの追加を取り消します。
- ホワイトリスト **ID**: この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーのデバイスで使用できる AirPlay デバイスのデバイス ID のみを追加できます。一覧に追加する AirPlay デバイスごとに、［追加］ をクリックして以下の操作を行います。

- デバイス **ID**: デバイス ID を「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
- ［追加］ をクリックしてデバイスを追加するか、［キャンセル］ をクリックしてデバイスの追加を取り消します。

AirPrint デバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、AirPrint プリンターをユーザーの iOS デバイスの AirPrint プリンター一覧に追加できます。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。

このポリシーは iOS 7.0 以降に適用されます。

> 注:
>
> 各プリンターの IP アドレスとリソースパスがあることを確認してください。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- **AirPrint** 出力先: 追加する AirPrint の出力先ごとに、［追加］ をクリックして以下の操作を行います。
  - **IP** アドレス: AirPrint プリンターの IP アドレスを入力します。
  - リソースパス: プリンターに関連付けられているリソースパスを入力します。この値は、_ipps.tcp Bonjour レコードのパラメーターに対応します。たとえば、printers/Canon_MG5300_series or printers/Xerox_Phaser_7600。
  - ［保存］ をクリックしてプリンターを追加するか、［キャンセル］ をクリックしてプリンターの追加を取り消します。

Android Enterprise 管理対象の構成ポリシー

January 10, 2020

Android Enterprise 管理対象構成デバイスポリシーが、さまざまなアプリ構成オプションとアプリの制限を管理します。アプリで使用できるオプションとヒントは、アプリ開発者によって定義されます。ヒントに「テンプレートの値」を使用すると記述されている場合は、代わりに対応する XenMobile マクロを使用します。詳しくは、「Remote configuration overview」（Android 開発者サイト）および「マクロ」を参照してください。

アプリ構成の設定には、次のような項目が含まれます:

- アプリのメール設定
- Web ブラウザーのホワイトリストまたはブラックリストへの URL 登録
- 携帯ネットワーク接続経由または Wi-Fi 接続のみでアプリコンテンツの同期を制御するオプション

アプリに表示される設定について詳しくは、アプリ開発者に問い合わせてください。

前提条件

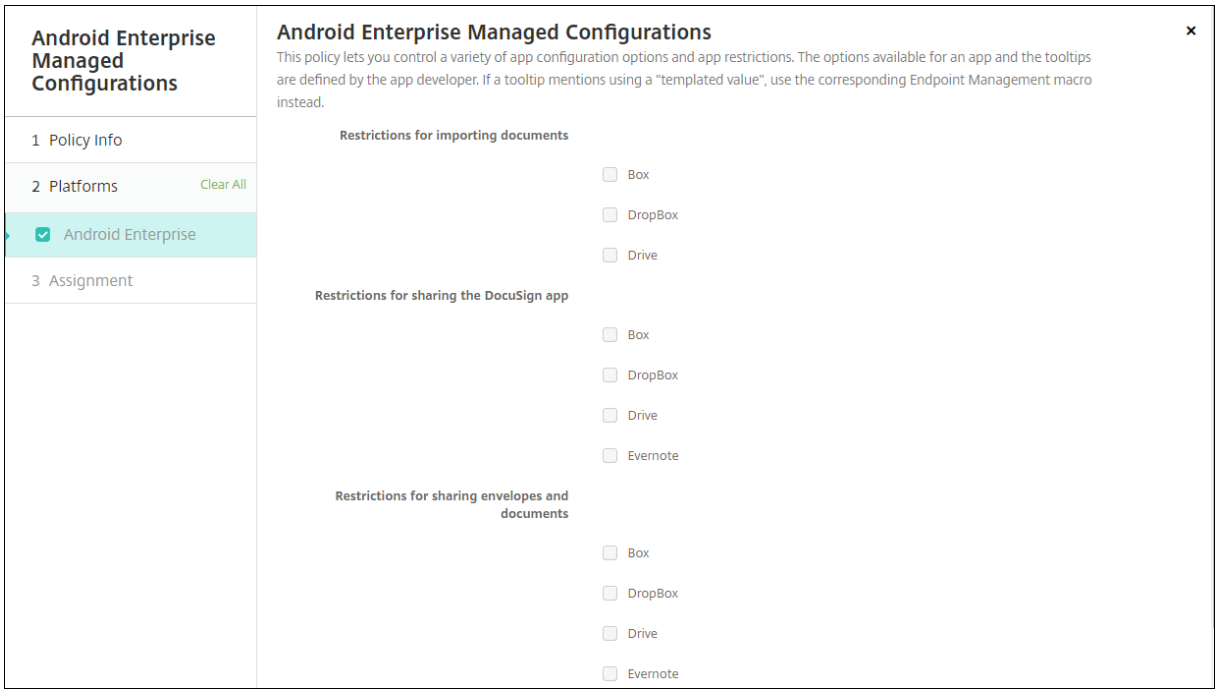
- Google で Android Enterprise セットアップタスクを完了し、Android Enterprise を managed Google Play に接続します。詳しくは、「Android Enterprise」を参照してください。
- Android Enterprise アプリを XenMobile に追加します。詳しくは、「XenMobile へのアプリケーションの追加」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise の設定

Android Enterprise 管理対象の構成デバイスポリシーを追加することを選択すると、アプリを選択するように促すメッセージが表示されます。XenMobile に追加された Android Enterprise アプリがない場合は、続行できません。

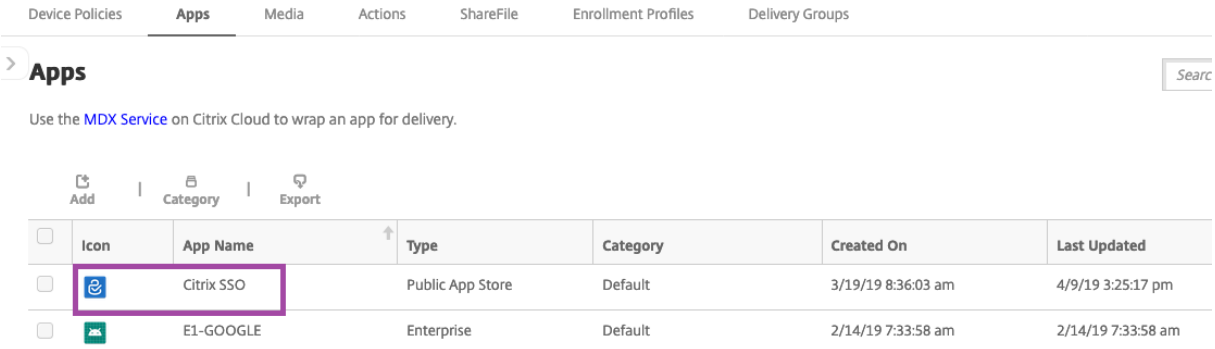
アプリを選択した後、ポリシー設定を構成します。設定は各アプリに固有です。



Android Enterprise に対する **VPN** プロファイルの構成

Android Enterprise 管理対象の構成デバイスポリシーに基づき、Citrix SSO アプリを使用して VPN プロファイルを Android Enterprise デバイスで使用できるようにします。

最初に、Google Play ストアアプリとして Citrix SSO を XenMobile コンソールに追加します。「パブリックアプリストアのアプリの追加」を参照してください。

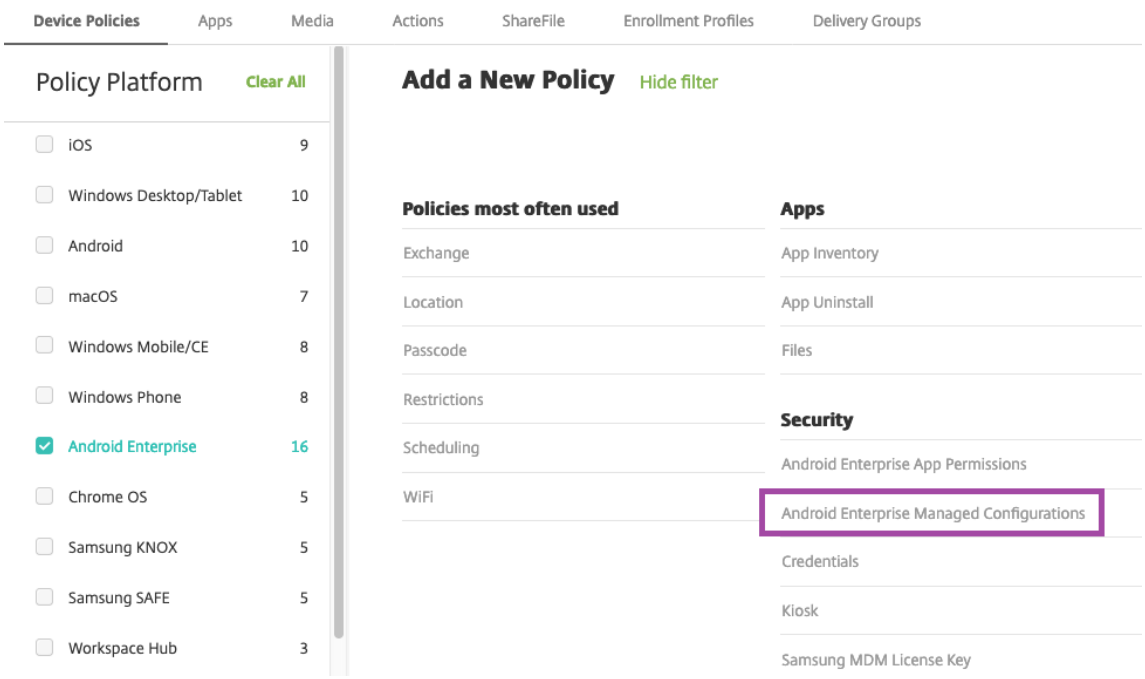


Citrix SSO に対する **Android Enterprise** 管理対象の構成の作成

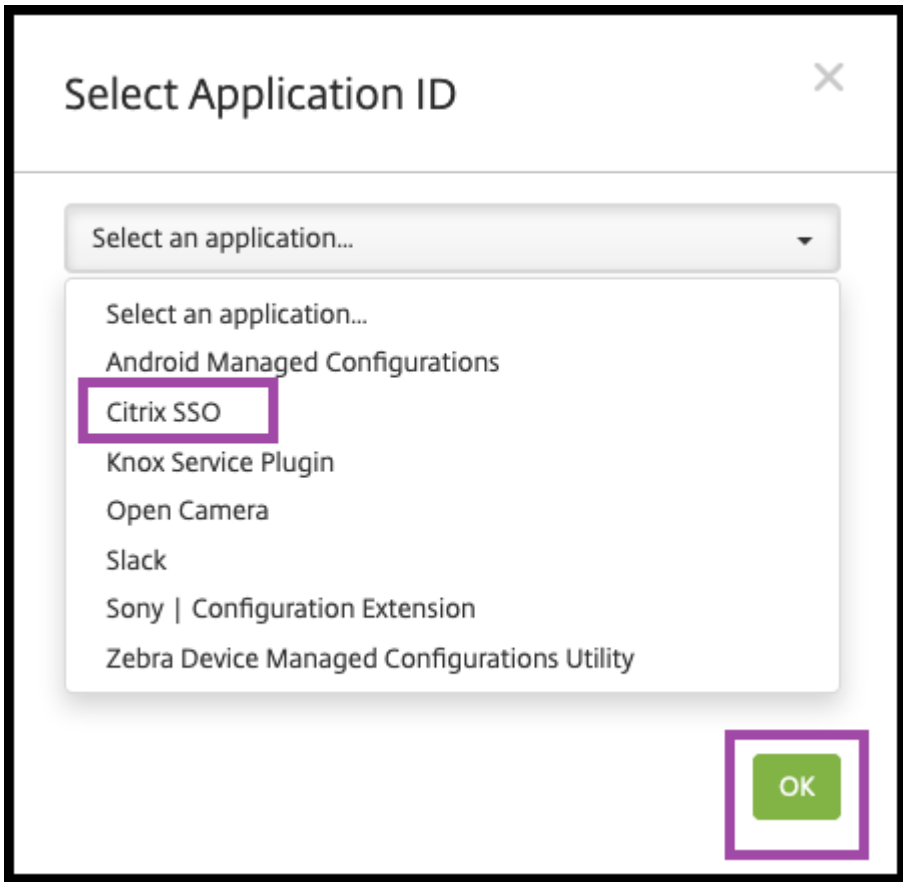
VPN プロファイルを作成するため、Citrix SSO に対する Android Enterprise 管理対象の構成デバイスポリシーを構成します。Citrix SSO アプリがインストールされており、ポリシーが展開されているデバイスは、作成した VPN プロファイルにアクセスできます。

Citrix Gateway の完全修飾ドメイン名とポートが必要です。

1. XenMobile コンソールで、［構成］**>**［デバイスポリシー］ をクリックします。［追加］ をクリックします。
2. ［**Android Enterprise**］ を選択します。［**Android Enterprise** 管理対象の構成］ をクリックします。



3. ［アプリケーション **ID** の選択］ウィンドウが表示されたら、リストから［**Citrix SSO**］をクリックし、［**OK**］をクリックします。



4. Citrix SSO VPN 構成の名前と説明を入力します。［次へ］ をクリックします。

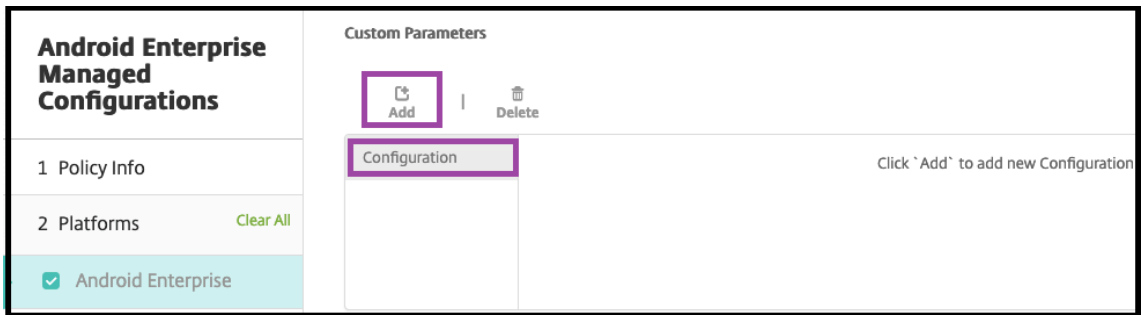
5. VPN プロファイルパラメータを構成します。

   - **VPN** プロファイル名。VPN プロファイルの名前を入力します。複数の VPN プロファイルを作成している場合は、それぞれに一意の名前を使用します。名前を入力しないと、［サーバーアドレス］ フィールドに入力したアドレスが VPN プロファイル名として使用されます。
   - サーバーアドレス（*****）。Citrix Gateway の完全修飾ドメイン名を入力します。Citrix Gateway のポートが 443 ではない場合は、ポートも入力します。URL 形式を使用します。たとえば、`https://gateway.mycompany.com:8443`のようにします。
   - ユーザー名（オプション）。エンドユーザーが Citrix Gateway の認証に使用するユーザー名を入力します。このフィールドには、XenMobile マクロ {user.username} を使用できます。（マクロを参照）ユーザー名を入力しないと、Citrix Gateway への接続時にユーザー名の入力を求められます。
   - パスワード（オプション）。エンドユーザーが Citrix Gateway の認証に使用するパスワードを入力します。パスワードを入力しないと、Citrix Gateway への接続時にユーザーがパスワードの入力を求められます。
   - 証明書エイリアス（オプション）。クライアント証明書認証に使用される Android キーストアの証明書エイリアスを入力します。この証明書は、証明書ベースの認証を使用している場合にはユーザーに対して事前選択されています。
   - **Per-App VPN** の種類（オプション）。Per-App VPN を使用してこの VPN を使用するようにアプリを制限している場合、この設定を構成できます。［許可］ を選択した場合、［**Per-App VPN** アプリ一覧］に含まれるアプリパッケージ名のネットワークトラフィックが VPN を介してルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN 外でルーティングされます。［許可しない］を選択した場合、［**Per-App VPN** アプリ一覧］ に含まれるアプリパッケージ名のネットワークトラフィックが VPN 外でルーティングされます。ほかのアプリのネットワークトラフィックは、すべて VPN

を介してルーティングされます。デフォルトは ［許可］ です。

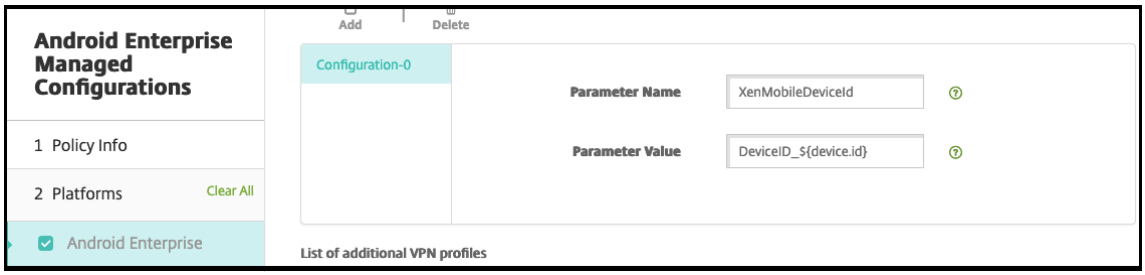
- **PerAppVPN** アプリ一覧。［**Per-App VPN** の種類］ の値に応じ、トラフィックが VPN で許可されるか、または許可されないアプリの一覧。アプリパッケージ名がカンマまたはセミコロンで区切って一覧にされます。アプリパッケージ名は大文字と小文字が区別され、この一覧でも Google Play ストアに表示されているのと同じように表示される必要があります。この一覧はオプションです。デバイス全体の VPN をプロビジョニングする場合は、この一覧を空のままにします。
- デフォルトの **VPN** プロファイル。ユーザーが特定のプロファイルをタップするのではなく、Citrix SSO アプリのユーザーインターフェイスで接続スイッチをタップした場合に使用する VPN プロファイルの名前を入力します。このフィールドを空白のままにすると、メインプロファイルが接続に使用されます。構成されているプロファイルが 1 つだけの場合は、それがデフォルトプロファイルに設定されます。常時 VPN の場合、このフィールドは常時 VPN を確立するために使用する VPN プロファイル名に設定する必要があります。
- ユーザープロファイルの無効化。この設定が［オン］の場合、ユーザーは自分のデバイスで独自の VPN を作成できません。この設定が［オフ］の場合、ユーザーは自分のデバイスで独自の VPN を作成できます。デフォルトは［オフ］です。
- 信頼されていないサーバーをブロック。Citrix Gateway で自己署名証明書を使用しているか、Citrix Gateway の証明書を発行する証明機関のルート証明書がシステムの証明機関リストに含まれていない場合、この設定は［オフ］になります。この設定が［オン］の場合、Citrix Gateway の証明書は Android オペレーティングシステムによって検証されます。検証に失敗した場合、接続は許可されません。デフォルト値は［オン］です。

6. オプションで、カスタムパラメーターを作成します。カスタムパラメーター **XenMobileDeviceId** および **UserAgent** がサポートされています。現在の VPN 設定を選択し、［追加］ をクリックします。



a) カスタムパラメーターを作成します:

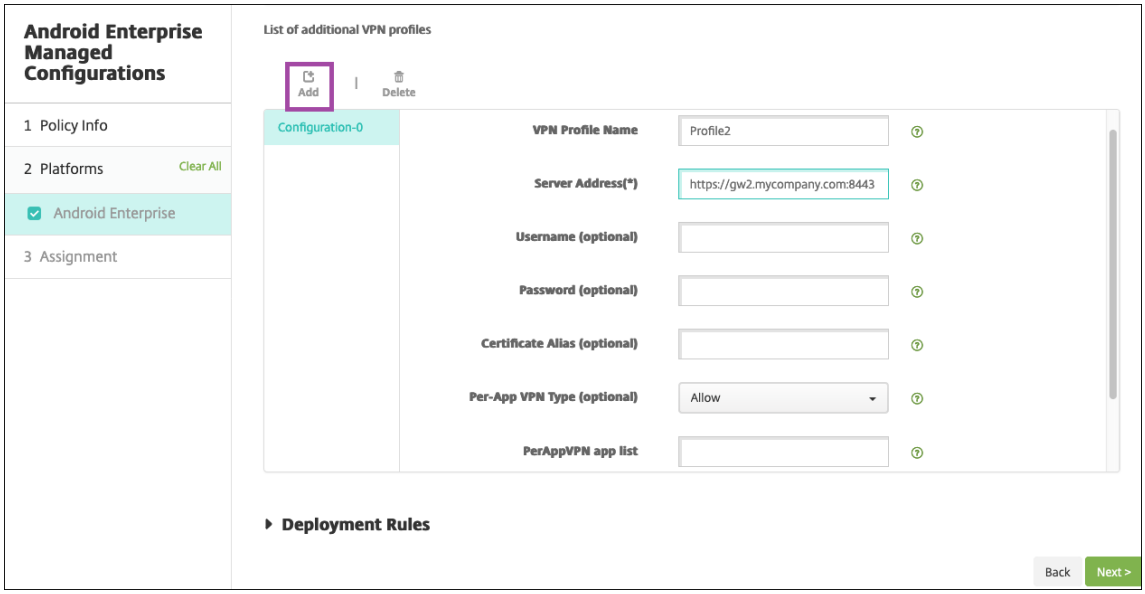
- パラメーター名。**XenMobileDeviceId** を入力します。このフィールドは、XenMobile でのデバイス登録に基づくネットワークアクセスチェックに使用するデバイス ID です。デバイスが XenMobile で登録および管理されている場合、VPN 接続は許可されます。登録および管理されていない場合、認証は VPN の確立時に拒否されます。
- パラメーター値。XenMobile でデバイスの登録および管理状態を特定できるよう、XenMobileDeviceID の値が`DeviceID_${ device.id }` に設定されます。



a) 別のカスタムパラメーターを作成するには、再び ［追加］ をクリックします。このカスタムパラメーターを作成します。

- パラメーター名。**UserAgent** を入力します。このテキストは、Citrix Gateway への追加チェックを実行するため、User-Agent HTTP ヘッダーに追加されます。このテキストの値は、Citrix Gateway との通信時に Citrix SSO アプリによって User-Agent HTTP ヘッダーに追加されます。
- パラメータ値。User-Agent HTTP ヘッダーに追加する任意のテキストを入力します。このテキストは、User-Agent HTTP の指定に準拠している必要があります。

7. オプションで、追加の VPN プロファイル構成を作成します。構成リストで ［追加］ をクリックします。新しい構成がリストに表示されます。新しい構成を選択し、手順 5 と、オプションで手順 6 を繰り返します。



8. 必要な VPN プロファイルをすべて作成したら、**[次へ]** をクリックします。
9. Citrix SSO に対するこの管理対象構成の展開規則を構成します。
10. ［保存］ をクリックします。

Citrix SSO に対するこの管理対象構成が、構成済みデバイスポリシーのリストに表示されます。

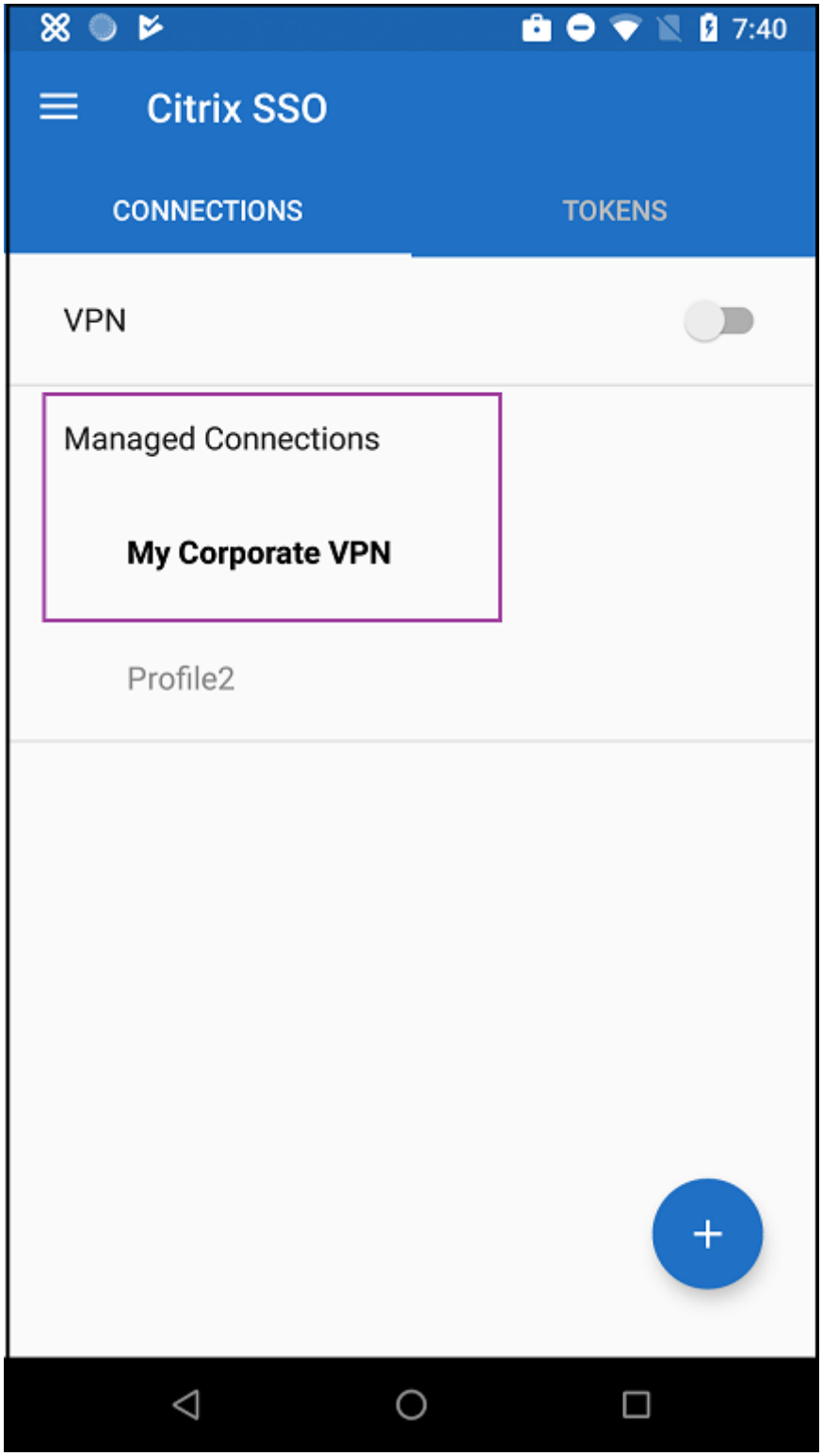
構成した VPN プロファイルの常時接続を有効にするには、XenMobile オプションデバイスポリシーを設定します。

> 注:
> Android Enterprise で VPN 常時接続にするには、Citrix Secure Hub 19.5.5 以降が必要です。

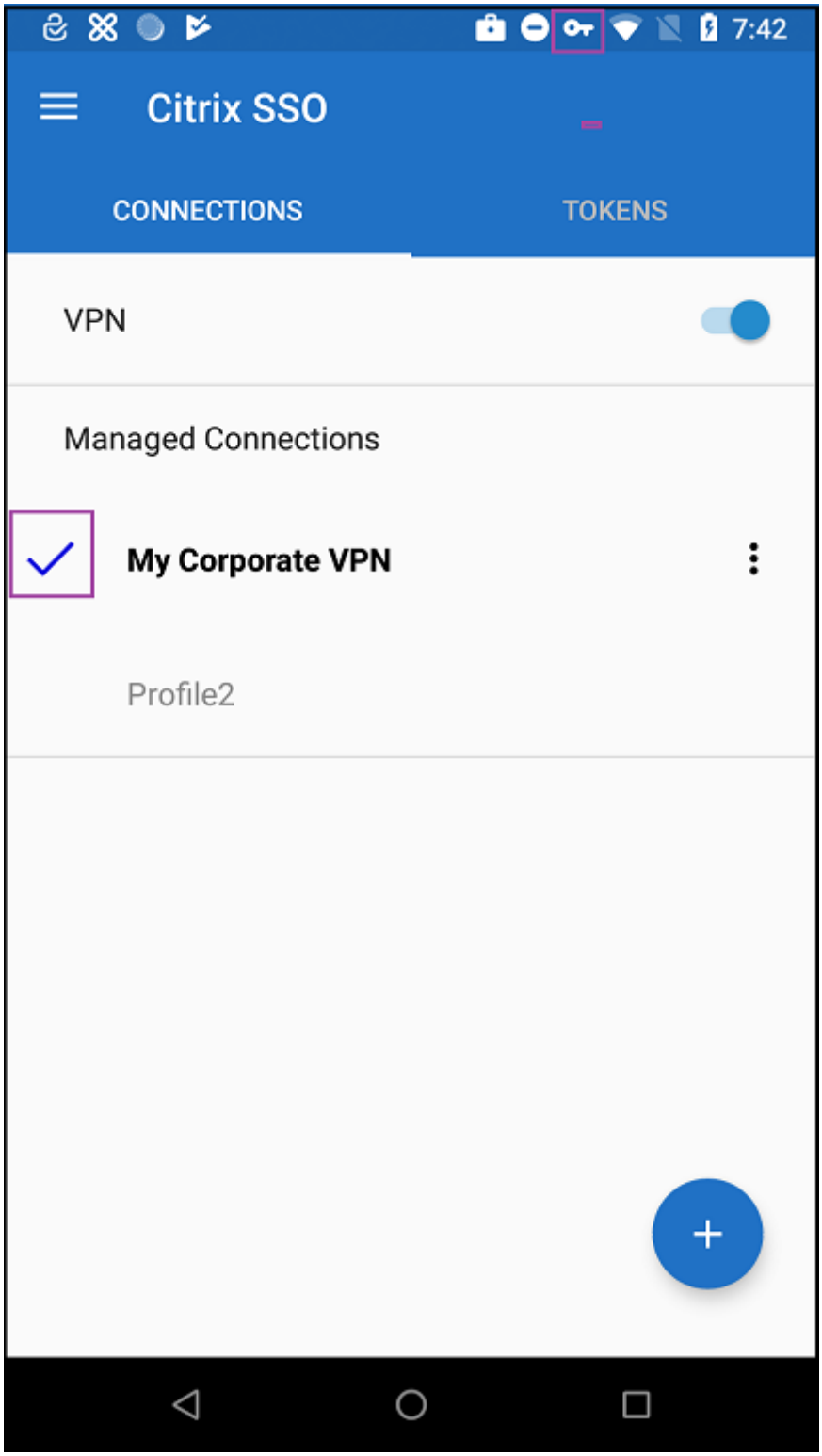
デバイスから **VPN** プロファイルへのアクセス

作成した VPN プロファイルにアクセスするには、Android Enterprise ユーザーが Google Play ストアから Citrix SSO をインストールします。

構成した 1 つまたは複数の VPN プロファイルが、アプリの ［管理接続］ 領域に表示されます。ユーザは VPN プロファイルをタップし、その VPN プロファイルを使用して接続します。



ユーザが認証され、接続されると、VPN プロファイルの横にチェックマークが表示されます。鍵のアイコンは、VPN に接続されていることを示します。



Android Enterprise の権限

January 10, 2020

仕事用プロファイル内で、Android Enterprise アプリへの要求で、Google が「危険な」権限を呼ぶ権限をどう処理するかを構成できます。アプリからの権限要求を許可または拒否するためのプロンプトをユーザーに表示するかどうかを制御します。この機能は、Android 7.0 以降を実行するデバイス向けです。

Google は、危険な権限を、アプリにユーザーの個人情報に関わるデータやリソースへのアクセス権、またはユーザーの格納されたデータや他のアプリの操作に影響を与える可能性のあるアクセス権を与える権限として定義しています。たとえば、ユーザーの連絡先を読み取る能力は危険な権限です。

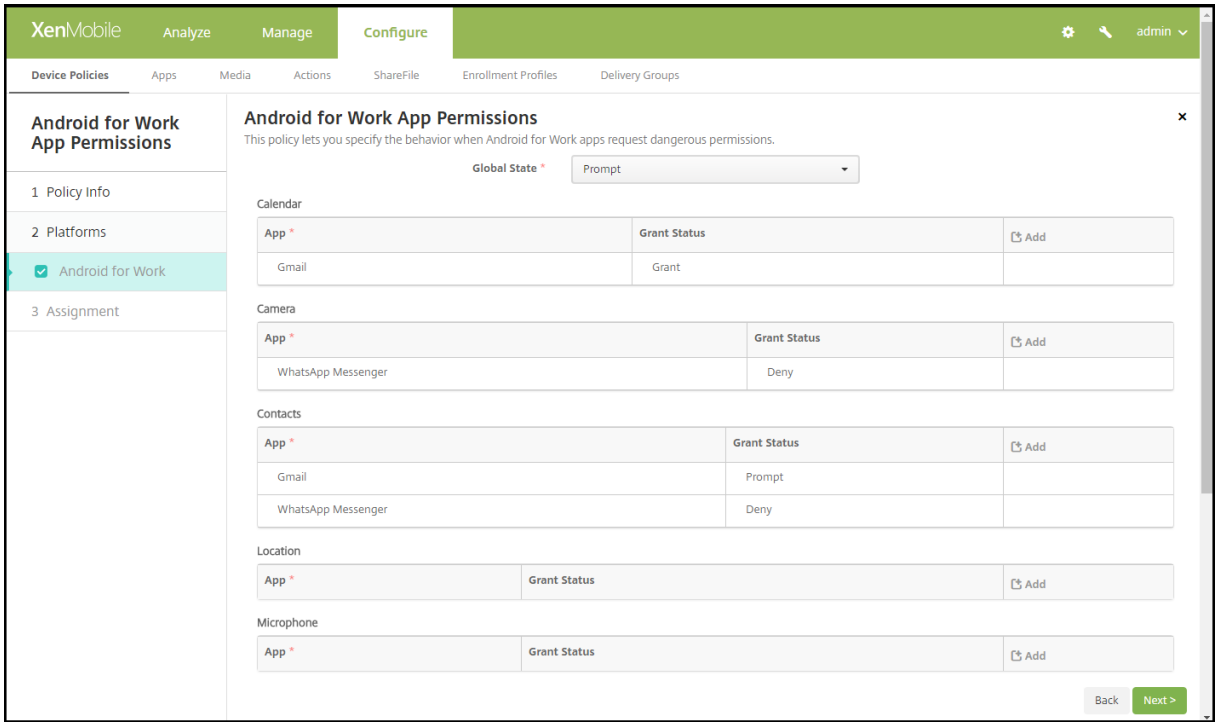
仕事用プロファイルで、Android Enterprise アプリに対するすべての危険な権限要求の動作を制御するグローバルな状態を設定できます。Google で定義されているように、アプリごとに、個々の権限グループに対して危険な権限の要求の動作を制御することもできます。これらの個々の設定は、グローバルな状態を上書きします。

Google が権限グループを定義する方法について詳しくは、この『Android 開発者ガイド』の「パーミッショングループ」を参照してください。

デフォルトでは、危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise の設定



- グローバルの状態： すべての危険な権限要求の動作を制御します。一覧で［プロンプト］、［許可］、または［拒否］ をクリックします。
  - プロンプト： 危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。
  - 許可： すべての危険な権限要求は許可されます。ユーザーにはプロンプトは表示されません。
  - 拒否： すべての危険な権限要求は拒否されます。ユーザーにはプロンプトは表示されません。

  デフォルトは ［プロンプト］ です。
- 各アプリについて各権限グループの個別の動作を設定します。権限グループの動作を構成するには、［追加］をクリックし、［アプリ］の下の一覧からアプリを選択します。Android Enterprise システムアプリを構成する場合、［新規追加］ をクリックして、制限デバイスポリシーで有効にしたアプリケーションパッケージ名を入力します。［許可の状態］で［プロンプト］、［許可］、または ［拒否］ を選択します。この許可の状態は、グローバルの状態を上書きします。
  - プロンプト： このアプリのこの権限グループからの危険な権限要求を許可または拒否するためのプロンプトがユーザーに表示されます。
  - 許可： このアプリのこの権限グループからの危険な権限要求が許可されます。ユーザーにはプロンプトは表示されません。
  - 拒否： このアプリのこの権限グループからの危険な権限要求が拒否されます。ユーザーにはプロンプトは表示されません。

  デフォルトは ［プロンプト］ です。
- アプリと［許可の状態］の横にある ［保存］ をクリックします。
- 権限グループにアプリを追加するには、もう一度 ［追加］ をクリックして、これらの手順を繰り返します。
- 必要なすべての権限グループの状態の許可の設定が完了したら、［次へ］をクリックします。

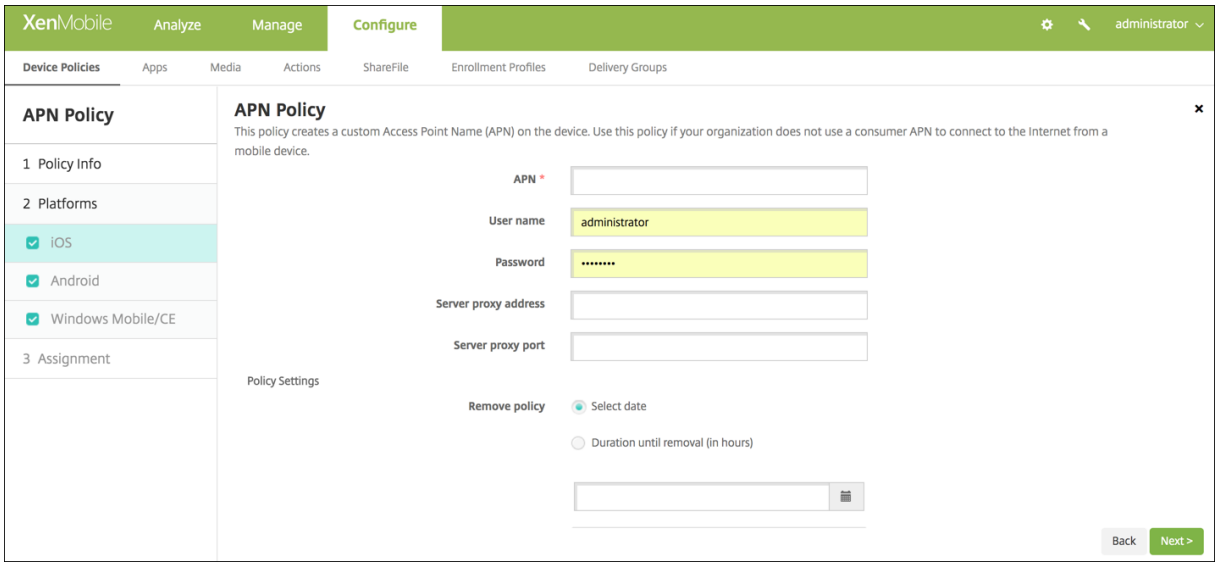
APN デバイスポリシー

January 10, 2020

iOS、Android、Windows Mobile/CE デバイスのカスタムアクセスポイント名（APN）デバイスポリシーを追加できます。このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマー APN を使用しない組織で使用します。APN ポリシーによって、特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。ほとんどの新しい電話機において、この設定は既に定義されています。

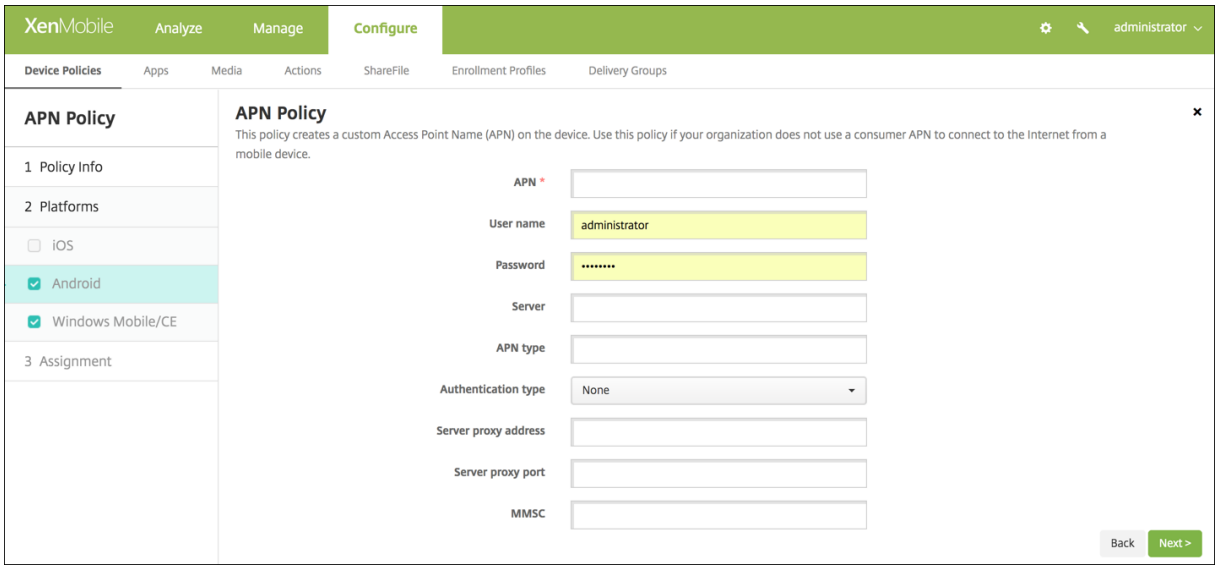
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **APN**: アクセスポイントの名前を入力します。これは承認されている iOS の APN と一致する必要があります。一致しない場合、ポリシーは機能しません。
- ユーザー名: この APN のユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- パスワード: この APN のユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- サーバープロキシアドレス: APN プロキシの IP アドレスまたは URL です。
- サーバープロキシポート: APN プロキシのポート番号です。サーバーのプロキシアドレスを入力した場合は必須です。
- [ポリシー設定] の下の [ポリシーの削除] の横にある、[日付を選択] または [削除までの期間（日）を指定] をクリックします。
  - [日付を選択] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [ユーザーにポリシーの削除を許可] の一覧で、[常に]、[パスワードが必要]、[許可しない] のいずれかを選択します。
  - [パスワードが必要] を選択した場合、[パスワードを削除] の横に必要なパスワードを入力します。

Android の設定

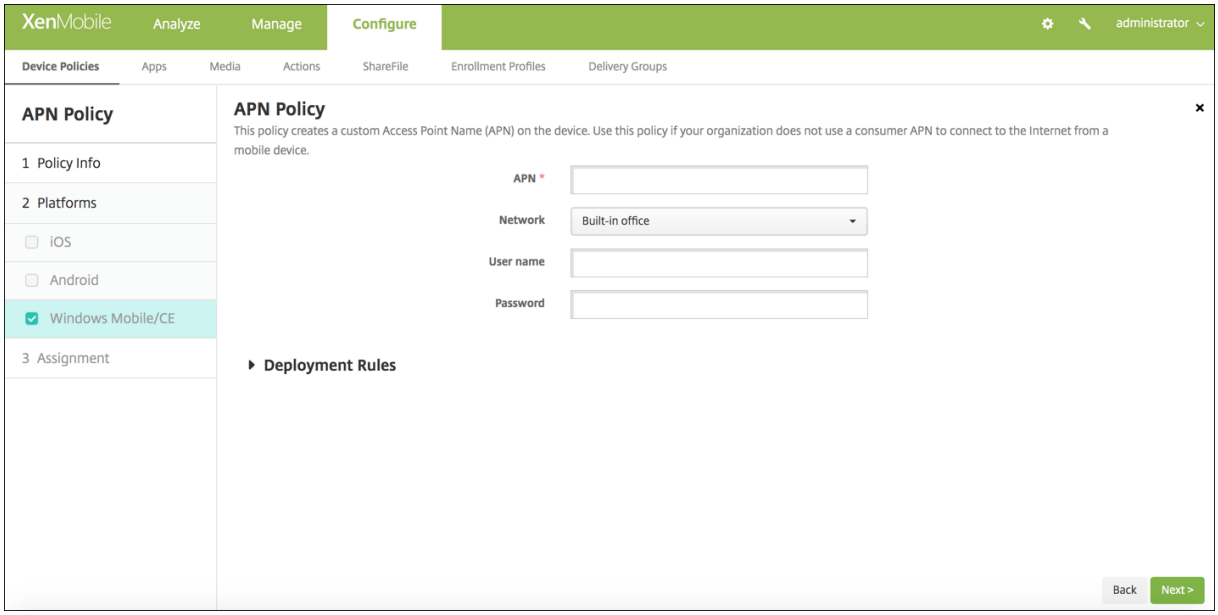


- **APN**: アクセスポイントの名前を入力します。これは承認されている Android の APN と一致する必要があります。一致しない場合、ポリシーは機能しません。
- ユーザー名: この APN のユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- パスワード: この APN のユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- サーバー: この設定はスマートフォンに先行するもので、通常は空白です。標準の Web サイトにアクセスできない、または標準の Web サイトを表示できない電話機用のワイヤレスアプリケーションプロトコル（WAP）ゲートウェイサーバーを参照します。
- **APN** の種類: この設定は、電話会社が想定しているアクセスポイントの使用方法に一致している必要があります。内容は APN サービス指定子のコンマ区切り文字列であり、携帯電話会社が公開している定義と一致している必要があります。以下に例を示します:
  - *。すべてのトラフィックがこのアクセスポイントを経由します。
  - mms。マルチメディアトラフィックがこのアクセスポイントを経由します。
  - default。マルチメディアトラフィックを含め、すべてのトラフィックがこのアクセスポイントを経由します。
  - supl。SUPL（Secure User Plane Location）は補助 GPS に関連付けられています。
  - dun。ダイヤルアップネットワークは古いため、ほとんど使用されません。
  - hipri。高優先度ネットワークです。
  - fota。FOTA（Firmware over the air）は、ファームウェア更新の受信に使用されます。
- 認証の種類: 一覧から、使用する認証の種類を選択します。デフォルトは［なし］です。
- サーバープロキシアドレス: 電話会社の APN HTTP プロキシの IP アドレスまたは URL です。
- サーバープロキシポート: APN プロキシのポート番号です。サーバーのプロキシアドレスを入力した場合は

必須です。

- **MMSC**: 電話会社が提供する MMS ゲートウェイサーバーのアドレスです。
- マルチメディアメッセージングサーバー（**MMS**）プロキシアドレス: これは、MMS トラフィック用のマルチメディアメッセージングサービスサーバーです。MMS は SMS の後継で、画像やビデオなどのマルチメディアコンテンツを含む大きいサイズのメッセージを送信できます。これらのサーバーは特定のプロトコルを必要とします（MM1、... MM11）。
- **MMS** ポート: MMS プロキシに使用されるポートです。

Windows Mobile/CE の設定



- **APN**: アクセスポイントの名前を入力します。これは承認されている Android の APN と一致する必要があります。一致しない場合、ポリシーは機能しません。
- ネットワーク: 一覧から、使用するネットワークの種類を選択します。デフォルトは ［組み込みのオフィス］です。
- ユーザー名: この APN のユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- パスワード: この APN のユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。

アプリアクセスデバイスポリシー

August 22, 2019

XenMobile のアプリケーションアクセスデバイスポリシーでは、デバイスへのインストールが必須のアプリケーション、デバイスにインストール可能なアプリケーション、デバイスへのインストールが禁止されるアプリケーションの一覧を定義できます。次に、そのアプリ一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。アプリケーションアクセスポリシーは、iOS、Android、Windows Mobile/CE デバイスに対して作成できます。

アクセスポリシーは一度に 1 種類のみ構成できます。必須アプリ、推奨アプリ、禁止アプリのいずれかの一覧のポリシーを追加できますが、同じアプリアクセスポリシー内に混在させることはできません。一覧の種類ごとにポリシーを作成する場合、XenMobile でどのポリシーがどのアプリケーション一覧に適用されるかがわかるようにするため、各ポリシーの名前付けに注意することをお勧めします。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

プラットフォーム設定

- アクセスポリシー: ［必須］、［推奨］、［禁止］ のいずれかをクリックします。デフォルトは ［必須］ です。
- 1 つまたは複数のアプリを一覧に追加するには、［追加］ をクリックして以下の操作を行います:
  - アプリ名: アプリ名を入力します。
  - アプリ識別子: 任意で、アプリ識別子を入力します。
  - ［保存］ または ［キャンセル］ をクリックします。
  - 追加するアプリごとに上記の手順を繰り返します。

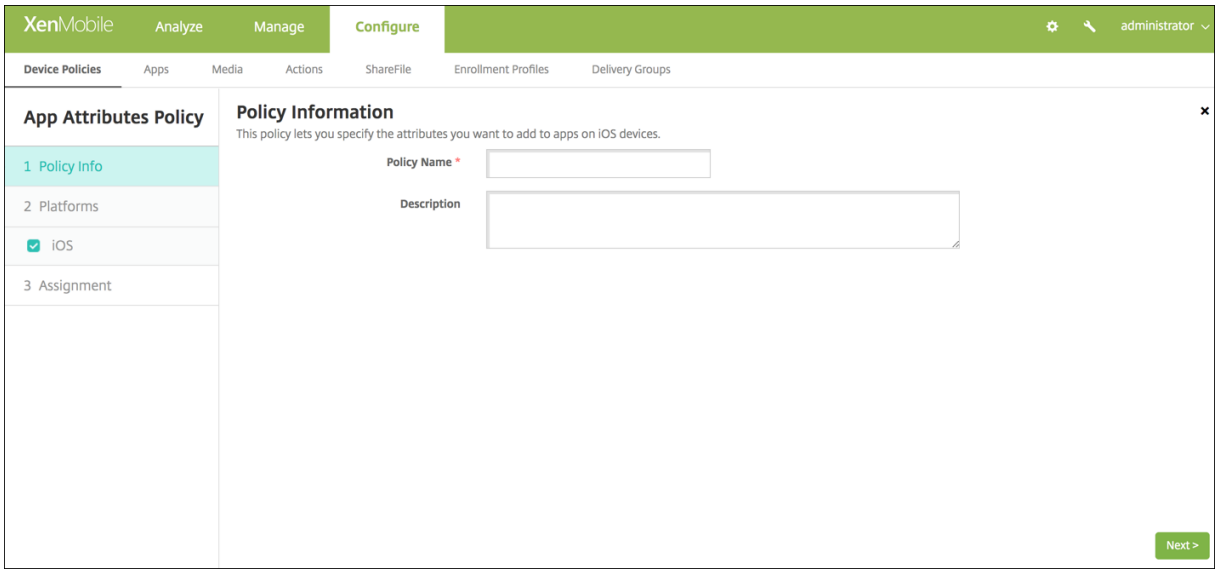
アプリ属性デバイスポリシー

January 10, 2020

アプリ属性デバイスポリシーで、iOS デバイスのための属性（管理対象アプリのバンドル ID やアプリごとの VPN 識別子など）を指定できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- 管理対象アプリのバンドル **ID**: 一覧からアプリバンドル ID を選択するか、［新規追加］ をクリックします。
  - ［新規追加］ をクリックした場合は、表示されるフィールドにアプリバンドル ID を入力します。
- アプリ単位の **VPN** 識別子: 一覧から、アプリごとの VPN ID を選択します。

アプリ構成デバイスポリシー

January 10, 2020

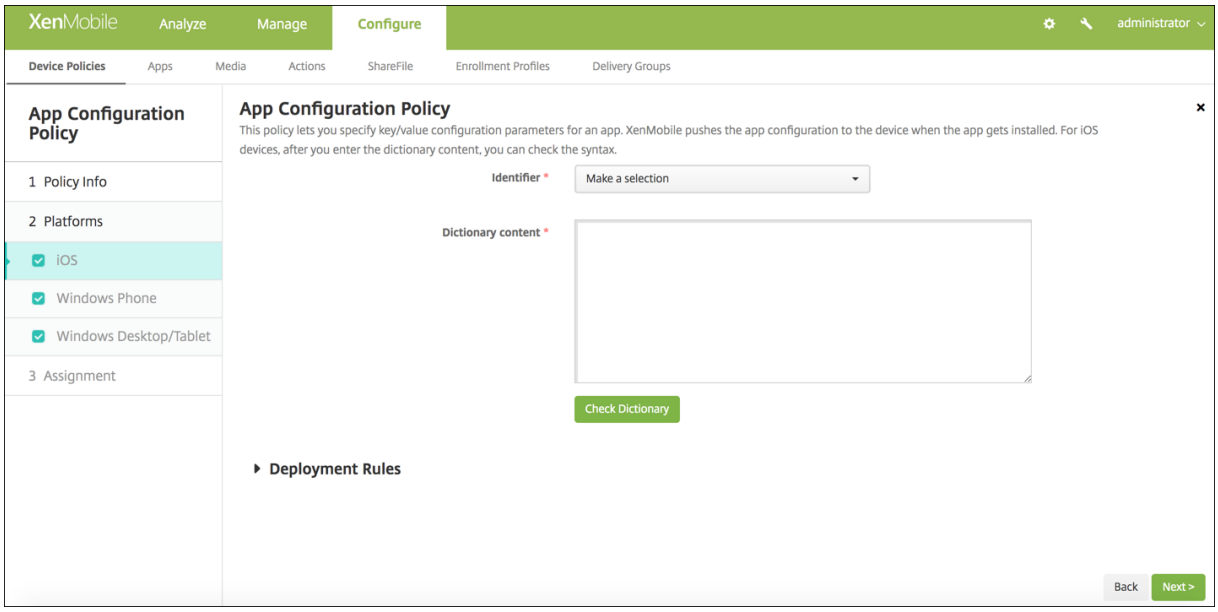
以下を展開することによって、管理対象の構成をサポートするアプリをリモートで構成できます。

- XML 構成ファイル（プロパティ一覧、または plist と呼ばれる）を iOS デバイスに展開します。
- または、キー/値ペアを Windows 10 Phone、タブレット、またはデスクトップデバイスに展開します。

この構成では、アプリ内のさまざまな設定や動作を指定します。ユーザーがアプリをインストールすると、XenMobile はこの構成をデバイスにプッシュします。設定できる実際の設定と動作は、アプリによって異なり、この記事では扱いません。

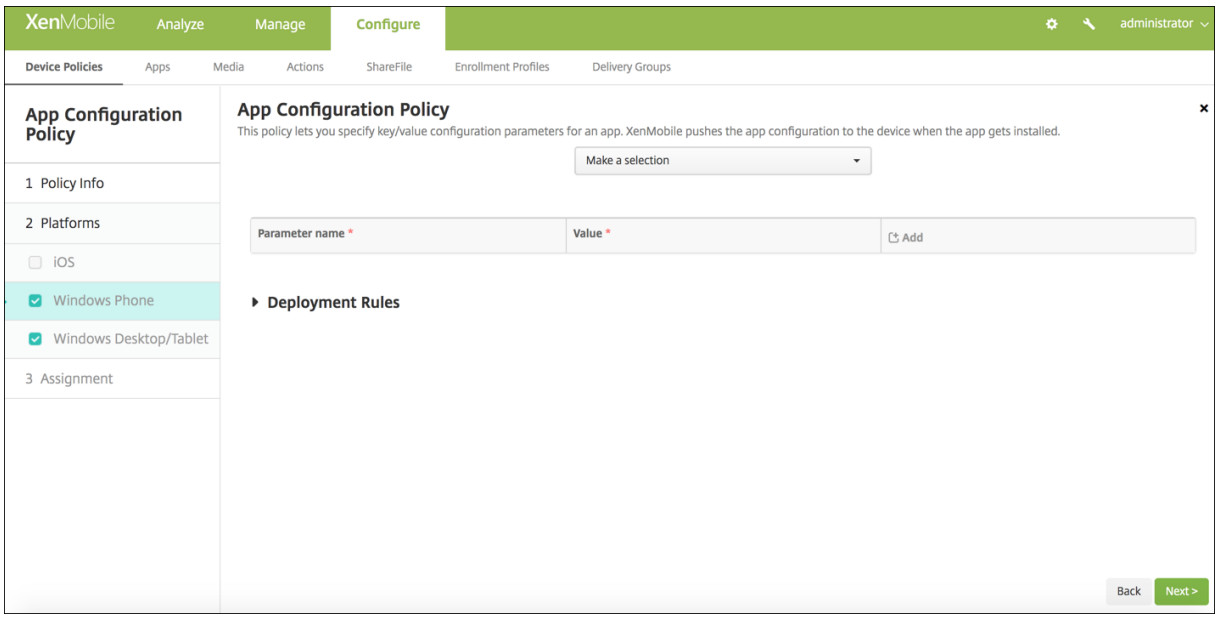
このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

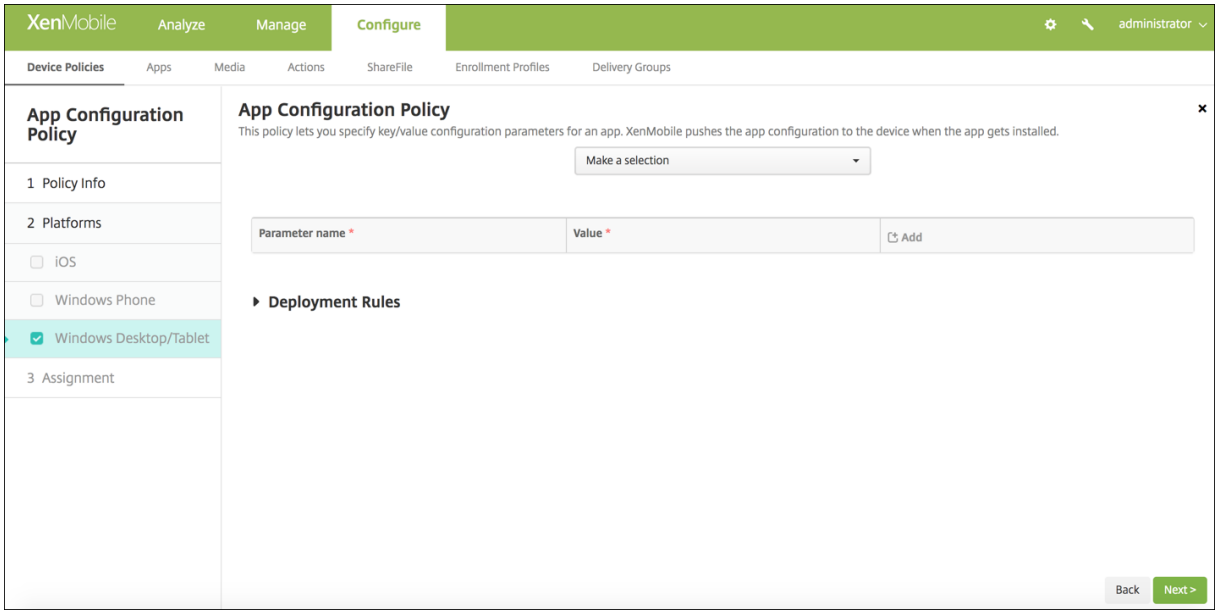
iOS の設定



- 識別子: 一覧から構成するアプリを選択するか、［新規追加］をクリックして新しいアプリを一覧に追加します。
  - ［新規追加］をクリックした場合は、表示されるフィールドにアプリ識別子を入力します。
- ディクショナリの内容: XML プロパティ一覧（plist）の構成情報を入力するか、コピーして貼り付けます。
- ［ディクショナリをチェック］をクリックします。XenMobile が XML を検証します。エラーがなければ、コンテンツボックスの下に「有効な **XML**」と表示されます。コンテンツボックスの下に何らかの構文エラーが表示された場合は、続行する前にエラーを修正する必要があります。

Windows Phone またはデスクトップ/タブレットの設定





- ［選択］ ボックスから構成するアプリを選択するか、［新規追加］ をクリックして新しいアプリを一覧に追加します。
  - ［新規追加］ をクリックした場合は、表示されるフィールドにパッケージファミリ名を入力します。
- 構成パラメーターごとに、［追加］ をクリックして以下の操作を行います:
  - パラメーター名: Windows デバイスのアプリケーション設定のキー名を入力します。Windows アプリの設定については、Microsoft 社のドキュメントを参照してください。
  - 値: 指定されたパラメーターの値を入力します。
  - ［追加］ をクリックしてパラメーターを追加するか、［キャンセル］ をクリックしてパラメーターの追加を取り消します。

アプリインベントリデバイスポリシー

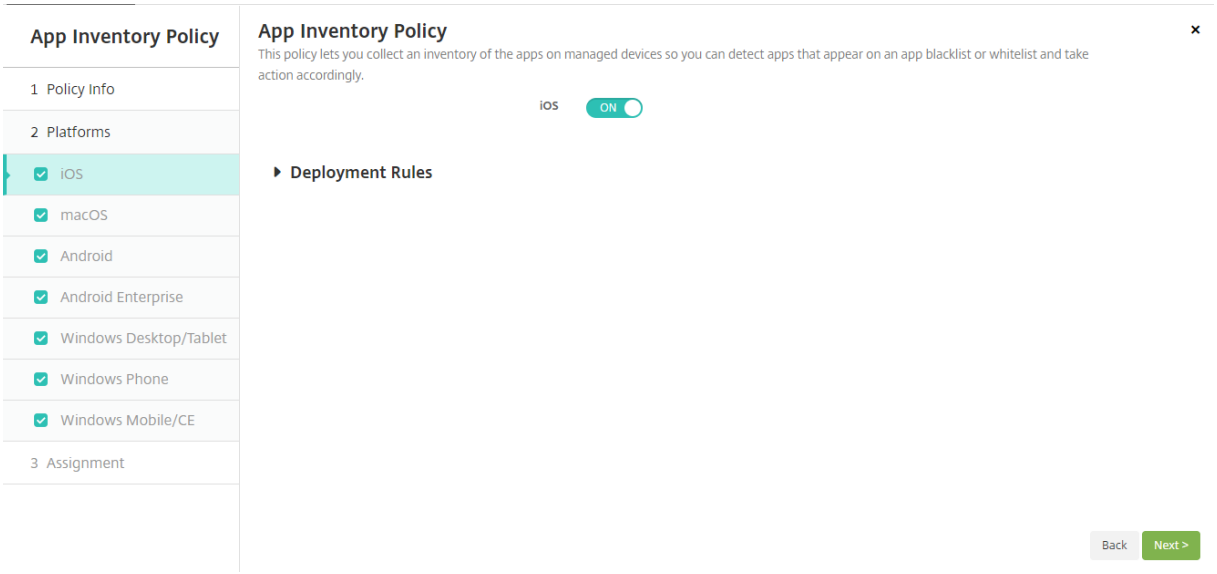
September 24, 2019

アプリインベントリポリシーでは、管理対象デバイス上のアプリのインベントリを収集できます。XenMobile はその後、インベントリをそのデバイスに展開されたアプリケーションアクセスポリシーと比較できます。この方法で、アプリのブラックリスト（アプリアクセスポリシーで禁止）またはホワイトリスト（アプリアクセスポリシーで必須）に表示されるアプリを検出し、それに応じた操作を実行することができます。

アプリアクセスポリシーは、iOS、macOS、Android、Android Enterprise、Windows デスクトップ/タブレット、Windows Phone、Windows Mobile/CE デバイスに対して作成できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

プラットフォーム設定



- 選択したプラットフォームごとに、デフォルト設定のままにしておくか、設定を ［オフ］ に変更します。デフォルトは ［オン］ です。

アプリのロックデバイスポリシー

January 10, 2020

アプリロックデバイスポリシーは、デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行をブロックするアプリの一覧を定義します。このポリシーは、iOS デバイスと Android デバイスの両方に対して構成できます

が、ポリシーが実際にどのように機能するかは各プラットフォームで異なります。たとえば、iOS デバイスで複数のアプリを禁止することはできません。

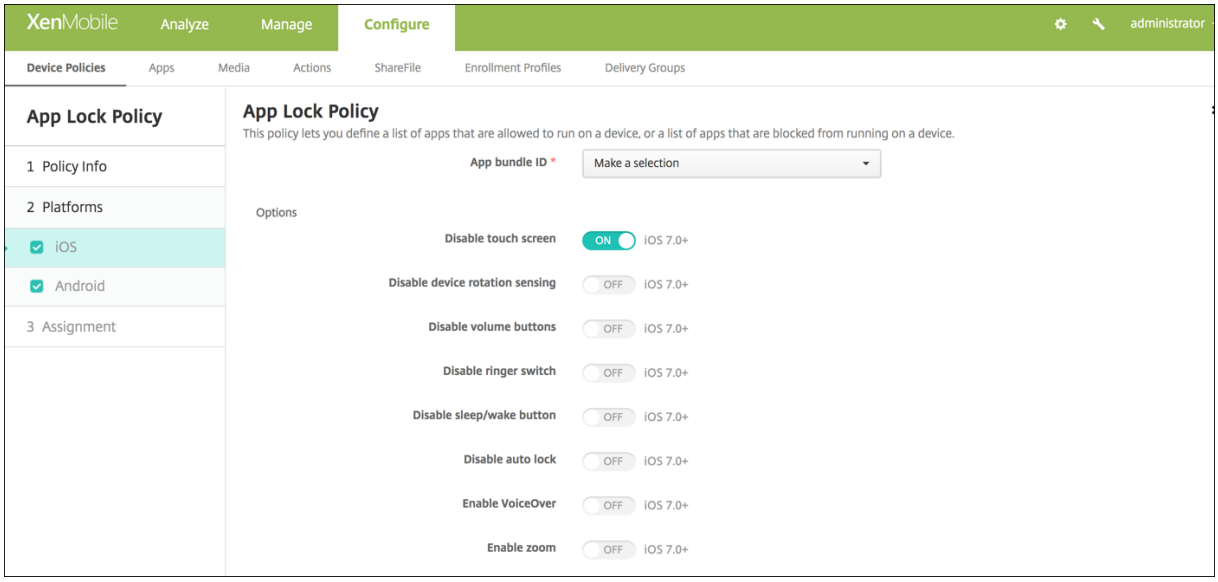
また、iOS デバイスで選択できる iOS アプリは、ポリシーあたり 1 つのみです。これによって、デバイスで実行できるのは 1 つのアプリのみになります。アプリのロックポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。

また、iOS デバイスは、アプリのロックポリシーをプッシュするように監視される必要があります。

デバイスポリシーは大部分の Android L および M デバイスで機能しますが、必要な API が Google によって廃止されたため、アプリのロックは Android N 以降のデバイスでは機能しません。

このポリシーを追加または構成するには、［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

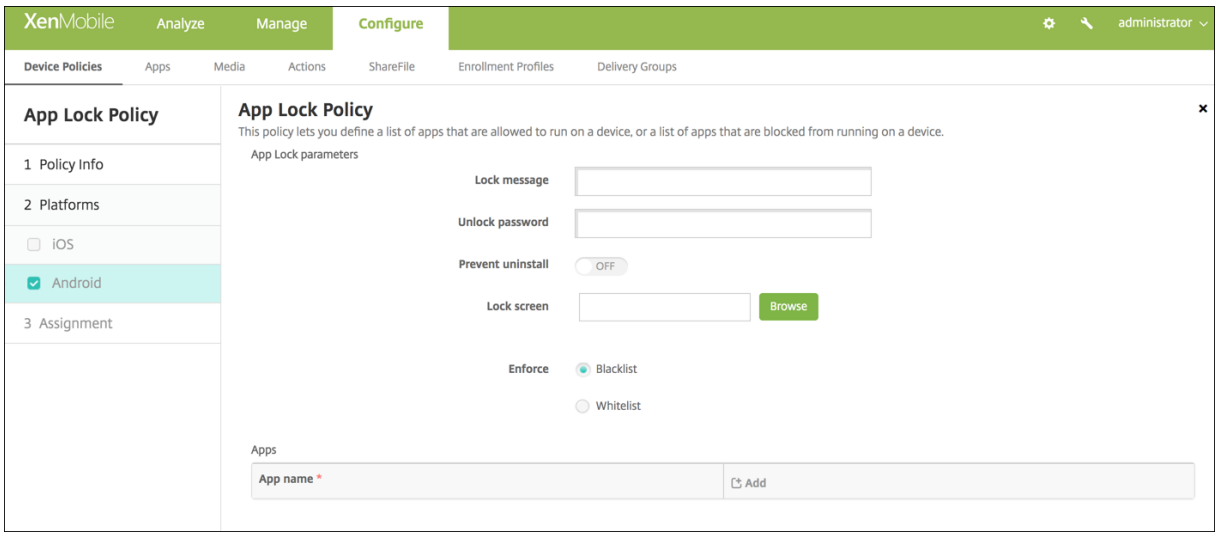


- アプリバンドル **ID**: このポリシーを適用するアプリを一覧から選択するか、［新規追加］ をクリックして、新しいアプリを一覧に追加します。［新規追加］ をクリックした場合は、表示されるフィールドにアプリ名を入力します。
- オプション: 以下の各オプションは、iOS 7.0 以降にのみ適用されます。［タッチスクリーンを無効化］を除き、各オプションのデフォルトは ［オフ］ です（［タッチスクリーンを無効化］はデフォルトで ［オン］ に設定されています）。
  - タッチスクリーンを無効化
  - デバイスの回転検出を無効化
  - 音量ボタンを無効化
  - 着信/サイレントスイッチを無効化

［着信/サイレントスイッチを無効化］が ［オン］ の場合、着信動作は、スイッチが最初に無効化されたときの場所に依存します。
  - スリープ/スリープ解除ボタンを無効化
  - 自動ロックを無効化
  - VoiceOver を無効化
  - ズームを有効化
  - 色の反転を有効化
  - AssistiveTouch を有効化
  - 選択項目の読み上げを有効化
  - モノラルオーディオを有効化
- ユーザーが有効化するオプション： 以下の各オプションは、iOS 7.0 以降にのみ適用されます。どのオプションも、デフォルトは ［オフ］ です。
  - VoiceOver の調整を許可
  - ズームの調整を許可
  - 色の反転の調整を許可
  - AssitiveTouch の調整を許可

Android の設定

> 注：
>
> Android の設定アプリは、アプリのロックデバイスポリシーを使用してブロックできません。



- アプリロックのパラメーター
  - ロックメッセージ： ユーザーがロックされているアプリを開こうとしたときに表示されるメッセージを入力します。
  - ロック解除のパスワード： アプリのロックを解除するパスワードを入力します。
  - アンインストールを禁止： ユーザーにアプリのアンインストールを許可するかどうかを選択します。デ

フォルトは ［オフ］ です。
  - ロック画面: ［参照］をクリックして、デバイスのロック画面に表示するイメージファイルの場所に移動し、ファイルを選択します。
  - 強制: ［ブラックリスト］ をクリックしてデバイスでの実行を禁止するアプリの一覧を作成するか、［ホワイトリスト］ をクリックしてデバイスでの実行を許可するアプリの一覧を作成します。
- アプリ: ［追加］ をクリックして、以下の操作を行います:
  - アプリ名: 一覧からホワイトリストまたはブラックリストに追加するアプリの名前を選択するか、［新規追加］ をクリックして、使用可能なアプリの一覧に新しいアプリを追加します。
  - ［新規追加］ をクリックした場合は、表示されるフィールドにアプリ名を入力します。
  - ［保存］ または ［キャンセル］ をクリックします。
  - ホワイトリストまたはブラックリストに追加するアプリごとに、上記の手順を繰り返します。

アプリネットワーク使用状況デバイスポリシー

January 10, 2020

ネットワーク使用状況規則を設定して、iOS デバイスで管理対象のアプリが携帯データネットワークなどのネットワークをどのように使用するのかを指定できます。規則は管理対象のアプリにのみ適用されます。管理対象のアプリケーションとは、XenMobile を使用してユーザーのデバイスに展開されるアプリケーションです。これには、ユーザーが XenMobile を使用して展開することなく直接デバイスにダウンロードしたアプリケーションや、デバイスの XenMobile への登録時に既にデバイスにインストールされていたアプリケーションは含まれません。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 携帯データのローミングを許可: 指定したアプリに、ローミング中に携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは ［オフ］ です。
- 携帯データを許可: 指定したアプリに、携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは ［オフ］ です。
- アプリ **ID** 照合: 一覧に追加するアプリごとに、［追加］ をクリックして以下の操作を行います:
  - アプリ識別子: アプリ識別子を入力します。
  - ［保存］をクリックしてアプリを一覧に追加するか、［キャンセル］をクリックして操作を取り消します。

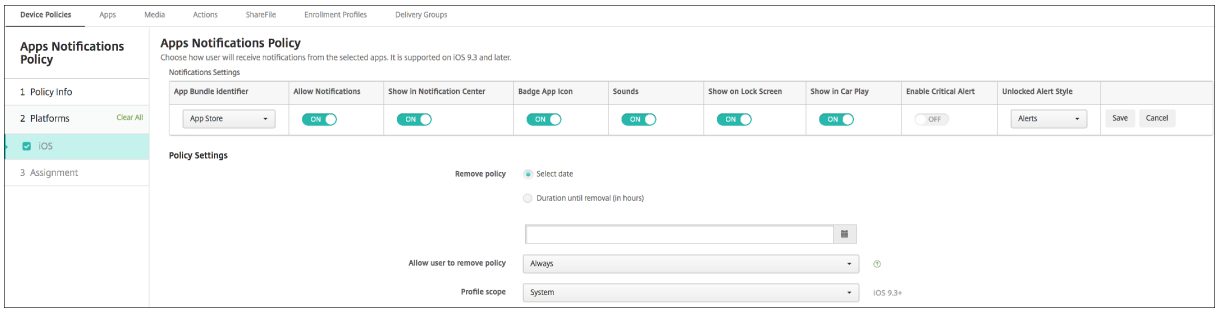
アプリ通知デバイスポリシー

January 10, 2020

アプリ通知ポリシーでは、iOS ユーザーが指定したアプリから通知を受け取る方法を制御できます。このポリシーは、iOS 9.3 以降を実行しているデバイスでサポートされています。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- アプリバンドル **ID**: このポリシーを適用するアプリを指定します。
- 通知を許可: 通知を許可するには、［オン］ を選択します。
- 通知センターに表示: ［オン］ を選択すると、ユーザーデバイスの通知センターに通知が表示されます。
- アプリアイコンをバッジ表示: ［オン］ を選択すると、通知がある場合、アプリアイコンにバッジ表示します。
- サウンド: ［オン］ を選択すると通知にサウンドが含まれます。
- セキュリティ-ロック画面に表示: ［オン］ を選択すると、ユーザーデバイスのロック画面に通知が表示されます。
- **CarPlay** で表示: ［オン］ にすると、Apple CarPlay に通知が表示されます。iOS 12 以降で利用できます。デフォルトは ［オン］ です。
- 重大アラートを有効にする: ［オン］ にすると、アプリは通知を重大な通知としてマークできます。これによって［応答不可］および警告設定を無視します。iOS 12 以降で利用できます。デフォルトは ［オフ］ です。
- ロック解除されたアラートスタイル: 一覧で、［なし］、［バナー］、または ［アラート］ を選択して、ロック解除されたアラートの外観を構成します。

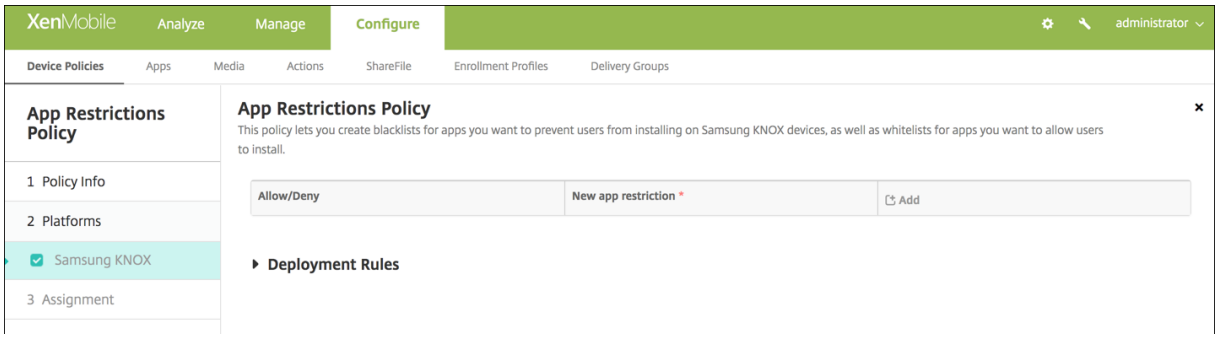
アプリ制限デバイスポリシー

August 22, 2019

ユーザーによる Samsung KNOX デバイスへのインストールを禁止するアプリケーションのブラックリストを作成したり、ユーザーによるインストールを許可するアプリケーションのホワイトリストを作成したりできます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung KNOX の設定



［許可/禁止］の一覧に追加するアプリごとに、［追加］ をクリックして以下の操作を行います:

- 許可/禁止: ユーザーにアプリのインストールを許可するかどうかを選択します。
- 新規アプリの制限: アプリパッケージ ID（例: com.kmdm.af.crackle）を入力します。
- ［許可/禁止］の一覧にアプリを保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。

アプリトンネリングデバイスポリシー

August 22, 2019

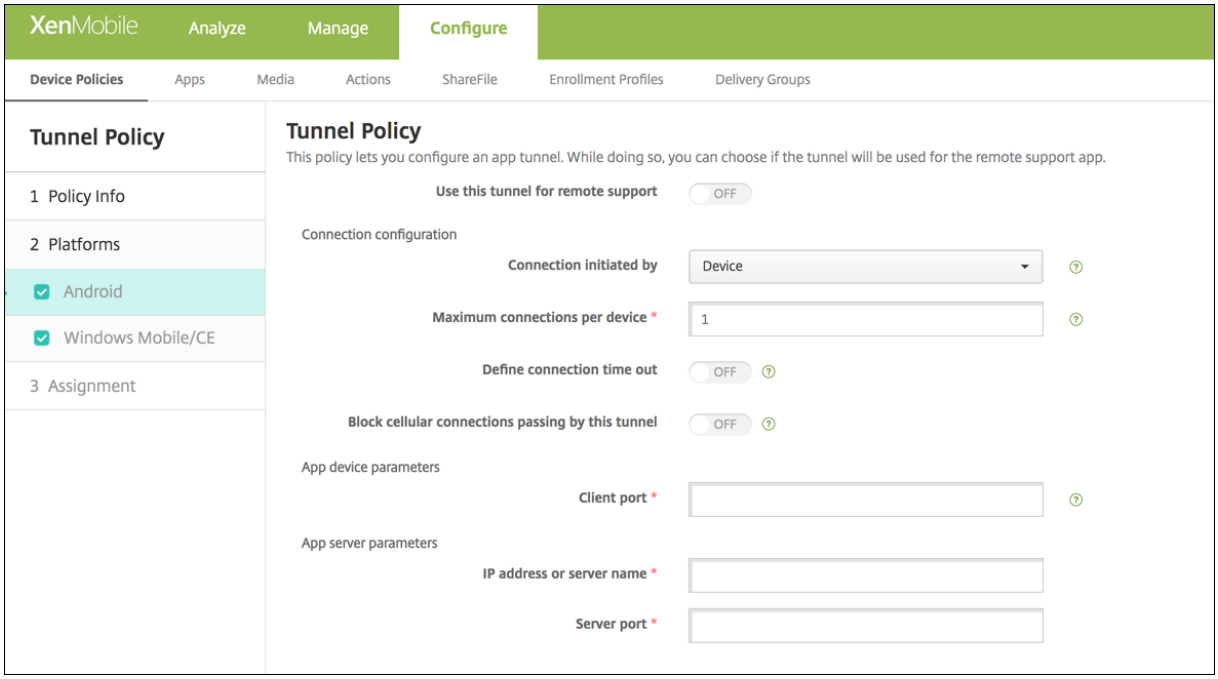
> 重要:
>
> アプリケーショントンネリングポリシーは、リモートサポートでのみ使用します。リモートサポートについては、「サポートオプションとリモートサポート」を参照してください。2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。

アプリトンネルは、モバイルアプリのサービスの継続性およびデータ転送の信頼性を向上させるように設計されています。アプリトンネルは、モバイルデバイスアプリのクライアントコンポーネントとアプリサーバーコンポーネント間のプロキシパラメーターを定義します。また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。アプリケーショントンネリングポリシーは、Android デバイスおよび Windows Mobile/CE デバイスに対して構成できます。

このポリシーで定義したトンネルを使用して送信されるアプリケーショントラフィックは、XenMobile を経由してから、アプリケーションを実行するサーバーにリダイレクトされます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android の設定



- このトンネルをリモートサポートに使用： トンネルを Remote Support に利用するかどうか選択します。

  リモートサポートを選択するかどうかによって、構成手順が異なります。

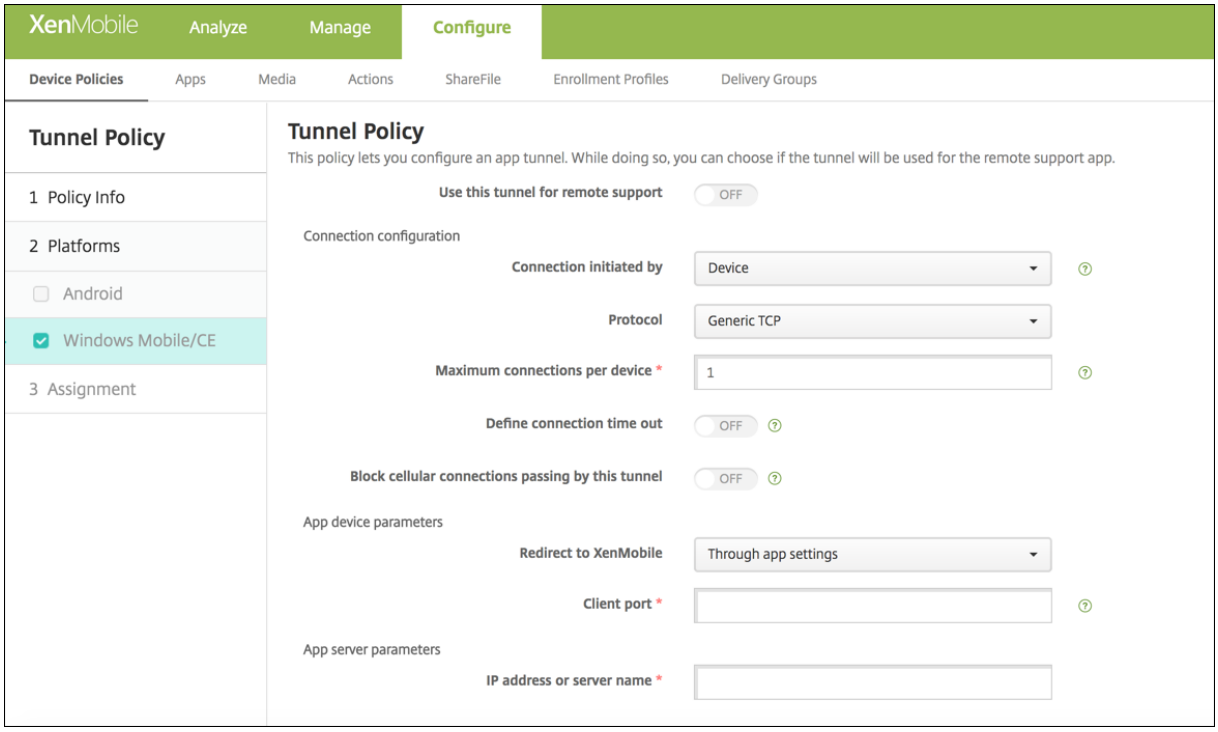
- リモートサポートを選択しない場合、以下の手順を実行します。
  - 接続を開始する側：［デバイス］ または ［サーバー］ を選択して、接続の開始元を指定します。
  - デバイスごとの最大接続数： 数値を入力して、アプリが確立できる同時 TCP 接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - 接続のタイムアウトを定義： アプリのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    * 接続タイムアウト：［接続のタイムアウトを定義］ を ［オン］ に設定した場合に、アプリのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - このトンネルを通過する携帯ネットワーク接続をブロック： ローミング中にこのトンネルをブロックするかどうか選択します。

> 注：
>
> WiFi および USB 接続はブロックされません。

- クライアントポート： クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
- **IP** アドレスまたはサーバー名： アプリサーバーの IP アドレスまたは名前を入力します。このフィールドはデバイスで開始する接続にのみ適用されます。
- サーバーポート： サーバーのポート番号を入力します。

- リモートサポートを選択する場合、以下の手順を実行します。
  - このトンネルをリモートサポートに使用：［オン］ に設定します。
  - 接続のタイムアウトを定義：アプリのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    * 接続タイムアウト：［接続のタイムアウトを定義］ を ［オン］ に設定した場合に、アプリのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **SSL** 接続を使用： このトンネルで、安全な SSL 接続を使用するかどうかを選択します。
  - このトンネルを通過する携帯ネットワーク接続をブロック： ローミング中にこのトンネルをブロックするかどうか選択します。この設定は WiFi と USB 接続をブロックしません。

Windows Mobile/CE の設定



- このトンネルをリモートサポートに使用： トンネルを Remote Support に利用するかどうか選択します。

リモートサポートを選択するかどうかによって、構成手順が異なります。

- リモートサポートを選択しない場合、以下の手順を実行します。
  - 接続を開始する側：［デバイス］ または ［サーバー］ を選択して、接続の開始元を指定します。
  - プロトコル： 一覧で使用するプロトコルを選択します。デフォルトは ［汎用 **TCP**］ です。
  - デバイスごとの最大接続数： 数値を入力して、アプリケーションが確立できる同時 TCP 接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - 接続のタイムアウトを定義： アプリのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    * 接続タイムアウト：［接続のタイムアウトを定義］ を ［オン］ に設定した場合に、アプリのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - このトンネルを通過する携帯ネットワーク接続をブロック： ローミング中にこのトンネルをブロックするかどうか選択します。

    > 注：
    > WiFi および USB 接続はブロックされません。

  - **XenMobile** にリダイレクト： 一覧から、XenMobile へのデバイスの接続方法を選択します。デフォルトは ［アプリ設定で］ です。
    * ［ローカルエイリアスで］ を選択した場合は、［ローカルエイリアス］ にエイリアスを入力します。デフォルト値は ［**localhost**］ です。
    * ［**IP** アドレスの範囲で］ を選択した場合は、［**IP** アドレスの範囲：開始アドレス］ に開始 IP アドレスを入力し、［**IP** アドレスの範囲：終了アドレス］ に終了 IP アドレスを入力します。
  - クライアントポート： クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
  - **IP** アドレスまたはサーバー名： アプリサーバーの IP アドレスまたは名前を入力します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - サーバーポート： サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - このトンネルをリモートサポートに使用：［オン］ に設定します。
  - 接続のタイムアウトを定義： アプリのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    * 接続タイムアウト：［接続のタイムアウトを定義］ を ［オン］ に設定した場合に、アプリのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **SSL** 接続を使用： このトンネルで、安全な SSL 接続を使用するかどうかを選択します。
  - このトンネルを通過する携帯ネットワーク接続をブロック： ローミング中にこのトンネルをブロックするかどうか選択します。WiFi と USB 接続はブロックされません。

アプリのアンインストールデバイスポリシー

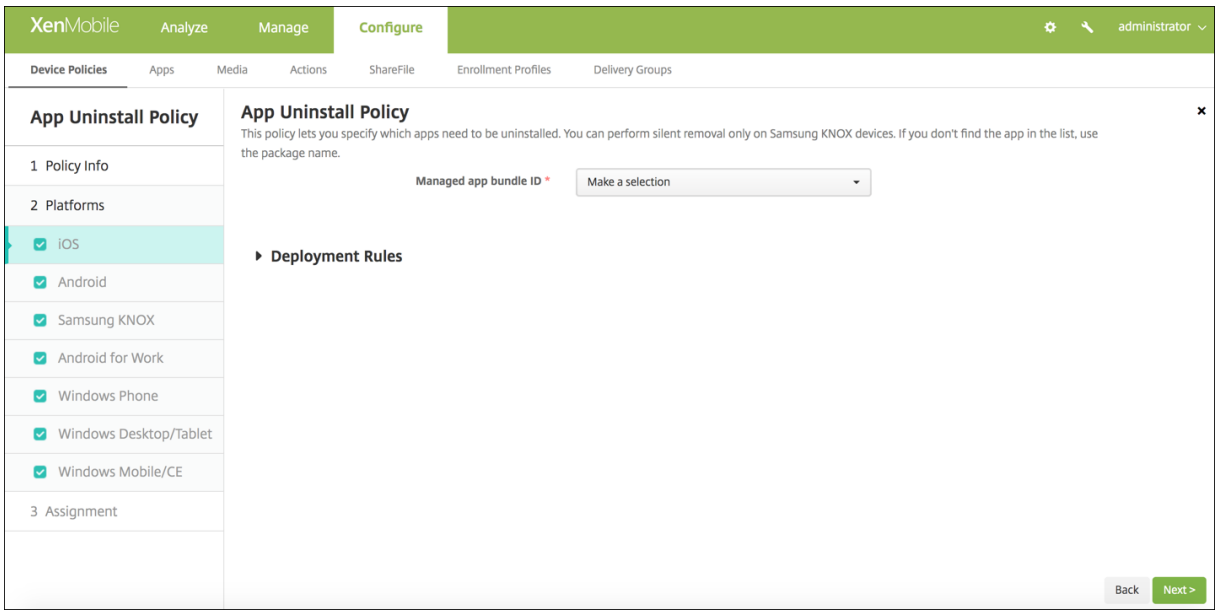
January 10, 2020

iOS、Android、Samsung KNOX、Android Enterprise、Windows デスクトップ/タブレット、および Windows Mobile/CE のプラットフォームに対するアプリケーションアンインストールポリシーを作成できます。アプリケーションアンインストールポリシーにより、さまざまな理由でユーザーのデバイスからアプリケーションを削除できます。この理由には、特定のアプリをサポートしなくなったことや、会社が既存アプリから異なるベンダーが提供する類似アプリへの置き換えを希望していることなどがあります。

このポリシーがユーザーのデバイスに展開されると、アプリが削除されます。Samsung KNOX 以外のデバイスでは、ユーザーにアプリのアンインストールを求めるメッセージが表示されます。Samsung KNOX デバイスでは、ユーザーにアプリのアンインストールを求めるメッセージは表示されません。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- 管理対象アプリのバンドル **ID**: 一覧で、既存のアプリを選択するか、［新規追加］ をクリックします。このプラットフォームに対してアプリが構成されていない場合は一覧が空になるため、新しいアプリを追加する必要があります。
  - ［追加］ をクリックすると、アプリ名を入力できるフィールドが表示されます。

ほかのすべてのプラットフォーム設定

- アンインストールするアプリ: 構成パラメーターごとに、［追加］ をクリックして以下の操作を行います:
  - アプリ名: 一覧で既存のアプリを選択するか、［新規追加］ をクリックして新しいアプリ名を入力します。このプラットフォームに対してアプリが構成されていない場合は一覧が空になるため、新しいアプリを追加する必要があります。
  - ［保存］ をクリックしてアプリを追加するか、［キャンセル］ をクリックしてアプリの追加を取り消します。

対応するパブリックアプリストアのアプリをインストールした後、エンタープライズアプリを自動的にアンインストールします

XenMobile を構成して、Citrix アプリのパブリックアプリケーションストアバージョンをインストールするときに、エンタープライズバージョンを削除することができます。この機能によって、パブリックアプリストアバージョンのインストール後に、ユーザのデバイスが 2 つの同じアプリアイコンを持つことを防ぎます。

アプリケーションアンインストールデバイスポリシーの展開条件によって、新バージョンのインストール時に、XenMobile はユーザのデバイスから旧バージョンを削除します。この機能は、XenMobile サーバーに Enterprise モード（XME）で接続した管理対象の iOS デバイスでのみ使用できます。

インストールしたアプリ名の条件で展開規則を構成するには:

- エンタープライズアプリの ［管理対象アプリのバンドル **ID**］ を指定します。
- 規則を追加します。［新しい規則］をクリックし、サンプルに示すように、［インストール済みのアプリ名］と［は、次のものと等しい］ を選択します。パブリックアプリストアのアプリのアプリバンドル ID を入力します。

この例では、指定したデリバリーグループのデバイスにパブリックアプリケーションストアのアプリ（com.citrix.mail.ios）がインストールされると、XenMobile によってエンタープライズバージョン（com.citrix.mail）が削除されます。

アプリのアンインストール制限デバイスポリシー

August 22, 2019

ユーザーに Samsung SAFE デバイスまたは Amazon デバイスでのアンインストールを許可する、または許可しないアプリを指定することができます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung SAFE または Amazon の設定

- アプリのアンインストール制限設定： 追加するアプリ規則ごとに、［追加］ をクリックして以下の操作を行います：
  - アプリ名： 一覧でアプリをクリックするか、または ［新規追加］ をクリックして新しいアプリを追加します。
  - 規則： ユーザーがアプリをアンインストールできるかどうかを選択します。デフォルトの設定ではアンインストールが許可されています。
  - ［保存］ または ［キャンセル］ をクリックします。

BitLocker デバイスポリシー

October 25, 2019

Windows 10 にはディスク暗号化機能 BitLocker が搭載されており、紛失または盗難に遭った Windows デバイスへの不正アクセスに対して、ファイルとシステムの保護が強化されています。さらに保護を強化するために、BitLocker とトラステッドプラットフォームモジュール（TPM）チップ（バージョン 1.2 以降）を組み合わせて使用できます。TPM チップは暗号化操作を処理し、暗号化キーの生成、保存、および使用の制限を行います。

Windows 10 のビルド 1703 以降では、MDM ポリシーで BitLocker を制御できるようになりました。XenMobile の BitLocker デバイスポリシーを使用して、Windows 10 デバイスの BitLocker ウィザードで使用可能な設定を構成します。たとえば、BitLocker が有効なデバイスでは、BitLocker はユーザーに、起動時にドライブをロック解除する方法、回復キーをバックアップする方法、固定ドライブをロック解除する方法を設定するよう求めます。BitLocker デバイスポリシーの設定では、以下についても構成します。

- TPM チップの内蔵されていないデバイスで BitLocker を有効にするかどうか。
- BitLocker インターフェイスに回復オプションを表示するかどうか。
- BitLocker が有効でない場合に、固定ドライブやリムーバブルドライブへの書き込みを拒否するかどうか。

> 注：
>
> BitLocker 暗号化がデバイスで開始されると、更新された BitLocker デバイスポリシーをデバイスに展開して BitLocker の設定を変更できなくなります。

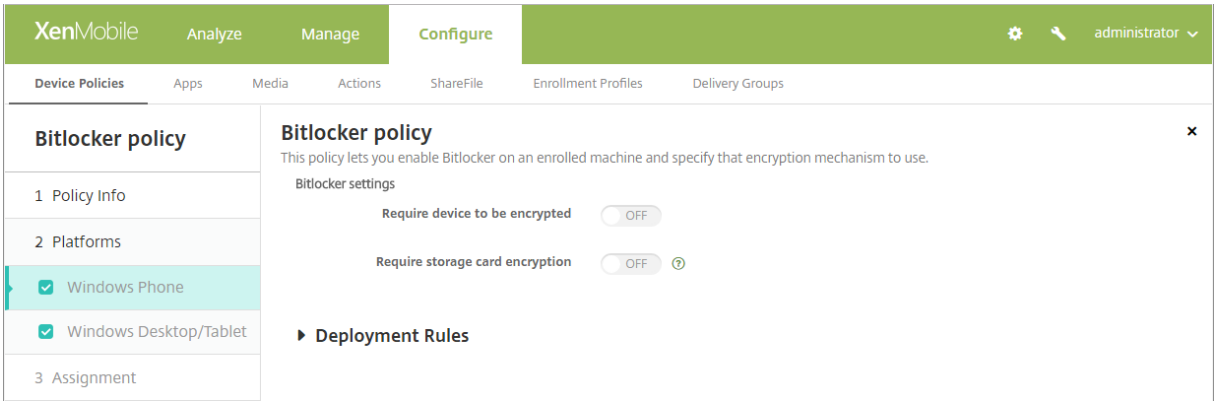
このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

要件

- BitLocker デバイスポリシーには、Windows 10 Enterprise エディションが必要です。

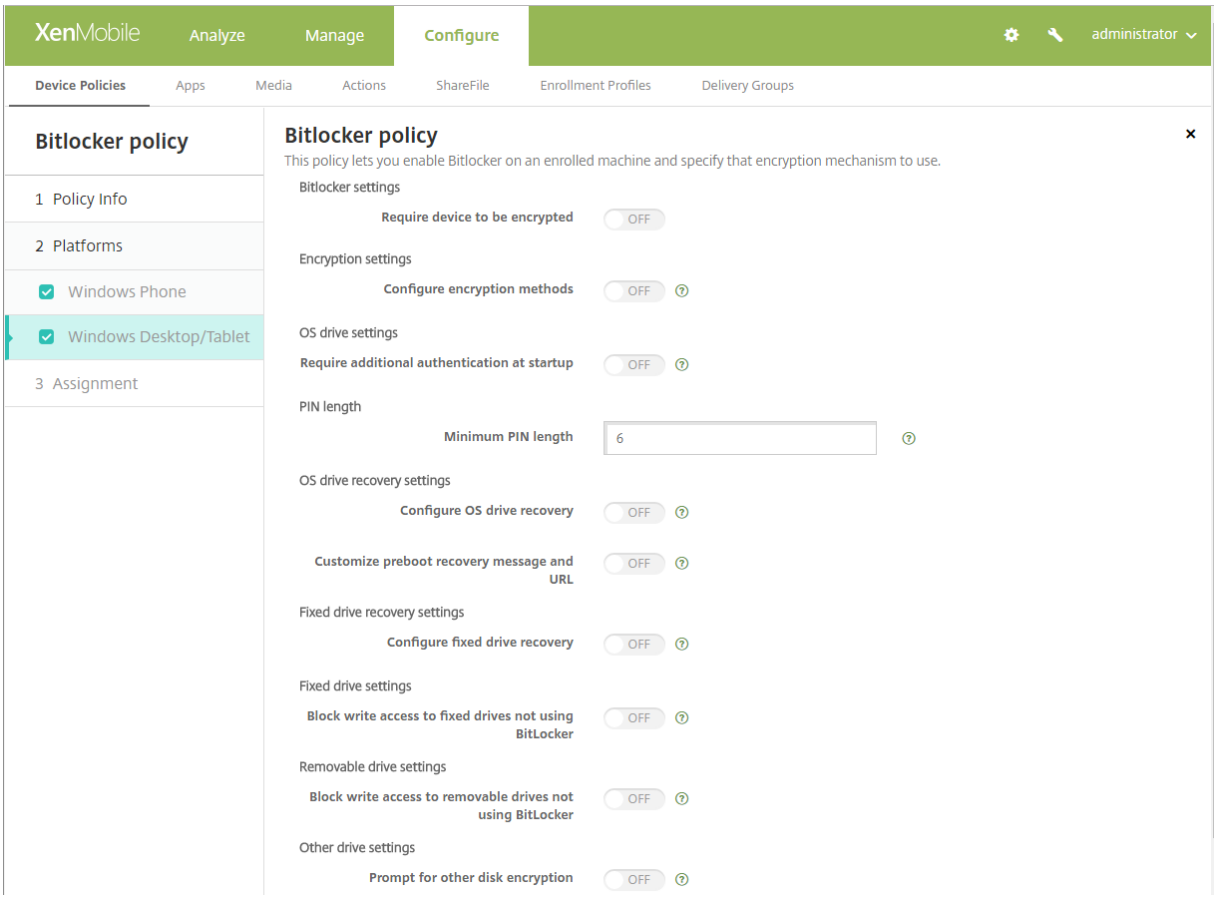
- BitLocker デバイスポリシーを展開する前に、BitLocker の使用に向けて環境を準備します。BitLocker のシステム要件とセットアップなどの Microsoft が提供する詳細情報については、「BitLocker」とそのノードの記事を参照してください。

Windows Phone の設定



- デバイスの暗号化が必須: Windows Phone のシステムカードで BitLocker の暗号化を有効にするよう求めるメッセージをユーザーに表示するかどうかを決定します。［オン］ にすると、登録完了後に、組織によってデバイスの暗号化が求められていることを示すメッセージがデバイスに表示されます。デバイスの暗号化を選択しないユーザーは、システムカードへの書き込みが許可されません。［オフ］ の場合はユーザーにメッセージは表示されず、デバイスを暗号化するかどうかは BitLocker のポリシーによって決定されます。デフォルトは、［オフ］ です。
- メモリカードの暗号化が必須: Windows Phone のメモリカードで BitLocker の暗号化を有効にするよう求めるメッセージをユーザーに表示するかどうかを決定します。［オン］ にすると、カードへの書き込み権限を取得するには、メモリカードの暗号化が必要になります。デフォルトは、［オフ］ です。

Windows デスクトップとタブレットの設定



- デバイスの暗号化が必須: Windows デスクトップまたはタブレットで BitLocker の暗号化を有効にするよう求めるメッセージをユーザーに表示するかどうかを決定します。［オン］ にすると、登録完了後に、組織によってデバイスの暗号化が求められていることを示すメッセージがデバイスに表示されます。［オフ］ の場合、ユーザーにメッセージは表示されず、BitLocker はポリシー設定を使用します。デフォルトは、［オフ］ です。
- 暗号化方式を構成する: 特定の種類のドライブに使用する暗号化方式を決定します。［オフ］ の場合、BitLocker ウィザードによって、ドライブの種類に使用する暗号化方式を尋ねるメッセージがユーザーに表示されます。デフォルトでは、すべてのドライブの暗号化方式は XTS-AES 128 ビットです。デフォルトでは、リムーバブルドライブの暗号化方式は AES-CBC 128 ビットです。［オン］ にすると、BitLocker はポリシーで指定された暗号化方式を使用します。［オン］ の場合は、オペレーティングシステムドライブ、固定ドライブ、リムーバブルドライブの追加の設定が表示されます。ドライブの種類ごとに、デフォルトの暗号化方式を選択します。デフォルトは、［オフ］ です。
- スタートアップ時に追加の認証を要求する: デバイスの起動時に必要な、追加の認証を指定します。また、TPM チップの内蔵されていないデバイスで、BitLocker を許可するかどうかも指定します。［オフ］ の場合、TPM の内蔵されていないデバイスでは、BitLocker の暗号化を使用できません。TPM について詳しくは、Microsoft 社の記事「トラステッドプラットフォームモジュール技術概要」を参照してください。［オン］ の場合は、次の追加の設定が表示されます。デフォルトは、［オフ］ です。

  - **TPM** チップの内蔵されていないデバイスで **BitLocker** をブロックする： TPM チップの内蔵されていないデバイスで、BitLocker はユーザーにロック解除のパスワードまたはスタートアップキーを作成するように要求します。スタートアップキーは USB ドライブに保存し、ユーザーは起動前にこれをデバイスに接続する必要があります。ロック解除のパスワードは、8 文字以上含める必要があります。デフォルトは、［オフ］ です。
  - **TPM** スタートアップ： TPM の内蔵されたデバイスには、TPM-only、TPM と PIN、TPM とキー、TPM と PIN とキーの、4 つのロック解除モードがあります。［TPM スタートアップ］は、暗号キーが TPM チップに保存されている、TPM-only のモードです。このモードでは、ユーザーに追加のロック解除データを入力するよう要求しません。起動時には TPM チップから暗号キーが使用されて、ユーザーデバイスは自動的にロック解除されます。デフォルトは ［**TPM** を許可する］ です。
  - **TPM** スタートアップ **PIN**： この設定は、TPM と PIN の組み合わせのロック解除モードです。PIN には、最大 20 文字の数字を含めることができます。［**PIN** の最小文字数］ の設定を使用して、PIN の最小文字数を指定します。ユーザーは、BitLocker のセットアップ時に PIN を構成し、デバイスの起動時に PIN を入力します。
  - **TPM** スタートアップキー： この設定は、TPM とキーの組み合わせのロック解除モードです。スタートアップキーは USB ドライブまたは他のリムーバブルドライブに保存し、ユーザーは起動前にこれをデバイスに接続する必要があります。
  - **TPM** スタートアップキーと **PIN**： この設定は、TPM と PIN とキーを組み合わせたロック解除モードです。

    ロック解除に成功すると、オペレーティングシステムがロードを開始します。ロック解除に失敗すると、デバイスはリカバリモードになります。

- **PIN** の最小文字数： TPM スタートアップ PIN の最小文字数です。デフォルトは **6** です。
- **OS** ドライブの回復の構成： ロック解除のステップに失敗すると、BitLocker は、構成された回復キーの入力を求めるメッセージをユーザーに表示します。この設定では、ユーザーがロック解除パスワードや USB のスタートアップキーを持っていない場合に使用できる、オペレーティングシステムドライブの回復オプションを構成します。デフォルトは ［オフ］ です。
  - 証明書に基づくデータ回復エージェントを許可する： 証明書ベースのデータ回復エージェントを許可するかどうかを指定します。グループポリシー管理コンソール（GPMC）またはローカルグループポリシーエディターで公開キーポリシーを見つけて、データ回復エージェントを追加します。データ回復エージェントについて詳しくは、BitLocker のグループポリシー設定に関する Microsoft の記事を参照してください。デフォルトは ［オフ］ です。
  - **OS** ドライブの回復用に **48** ビットの回復パスワードを作成： 回復パスワードの使用をユーザーに許可または要求するかどうかを指定します。BitLocker はパスワードを生成し、ファイルまたは Microsoft Cloud アカウントに保存します。デフォルトは ［**48** 桁のパスワードを許可する］ です。
  - **256** 桁の回復キーを作成： 回復キーの使用をユーザーに許可または要求するかどうかを指定します。回復キーは BEK ファイルであり、USB ドライブに保存されます。デフォルトは ［**256** ビットの回復キー

を許可する］ です。

- **OS** ドライブの回復オプションを非表示にする: BitLocker インターフェイスに回復オプションを表示または非表示にするかどうかを指定します。［オン］ にすると、BitLocker インターフェイスに回復オプションは表示されません。この場合はデバイスを Active Directory に登録し、回復オプションを Active Directory に保存して、［回復情報を **AD DS** に保存］を ［オン］ に設定します。デフォルトは［オフ］ です。
- 回復情報を **AD DS** に保存: 回復オプションを Active Directory ドメインサービスに保存するかどうかを指定します。デフォルトは ［オフ］ です。
- **AD DS** に保存された回復情報を構成する: BitLocker の回復パスワード、または回復パスワードとキーパッケージを、Active Directory ドメインサービスに保存するかどうかを指定します。キーパッケージを保存すると、物理的に破損したドライブからのデータの回復がサポートされます。デフォルトは、［回復パスワードをバックアップする］です。
- 回復情報を **AD DS** に保存した後に **BitLocker** を有効にする: デバイスがドメインに接続され、BitLocker 回復情報の Active Directory へのバックアップが正常に完了するまでは、ユーザーが BitLocker を有効にすることを禁止するかどうかを指定します。［オン］ にすると、BitLocker を起動する前にデバイスをドメインに参加させる必要があります。デフォルトは ［オフ］ です。

- プリブートの回復メッセージと **URL** をカスタマイズする: BitLocker が、回復の画面でカスタマイズされたメッセージと URL を表示するかどうかを指定します。［オン］ にすると、［既定の回復メッセージと **URL** を表示する］、［空の回復メッセージと **URL** を使用する］、［カスタム回復メッセージを使用する］、［カスタム回復 **URL** を使用する］の追加の設定が表示されます。［オフ］ の場合は、デフォルトの回復メッセージと URL が表示されます。デフォルトは ［オフ］ です。
- 固定ドライブの回復を構成する: BitLocker で暗号化された固定ドライブに対する、ユーザーの回復オプションを構成します。BitLocker は、固定ドライブの暗号化に関するメッセージをユーザーに表示しません。起動時にドライブのロックを解除するには、パスワードまたはスマートカードを使用します。ユーザーが固定ドライブでの BitLocker 暗号化を有効にすると、このポリシーにはない起動時のロック解除の設定が BitLocker インターフェイスに表示されます。関連設定について詳しくは、この一覧で前述した 「**OS** ドライブの回復の構成」 を参照してください。デフォルトは ［オフ］ です。
- **BitLocker** を使用しない固定ドライブへの書き込みアクセスをブロックする: ［オン］ にすると、固定ドライブが BitLocker で暗号化されている場合にのみ、ユーザーはこれらのドライブに書き込むことができます。デフォルトは ［オフ］ です。
- **BitLocker** を使用しないリムーバブルドライブへの書き込みアクセスをブロックする: ［オン］ にすると、リムーバブルドライブが BitLocker で暗号化されている場合にのみ、ユーザーはこれらのドライブに書き込むことができます。他の組織のリムーバブルドライブへの書き込みが、組織によって許可されているかどうかに従って、この設定を構成します。デフォルトは ［オフ］ です。
- 他のディスク暗号化のプロンプトを表示: デバイス上の他のディスク暗号化に対する警告プロンプトを無効にすることができます。デフォルトは、［オフ］ です。

ブラウザーデバイスポリシー

August 22, 2019

Samsung SAFE または Samsung KNOX デバイスのブラウザーデバイスポリシーを作成して、ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、ユーザーのデバイスで使用できるブラウザー機能を制限したりできます。

Samsung デバイスでは、ブラウザーを完全に無効にすることや、ポップアップ、JavaScript、Cookie、オートフィル、不正 Web サイト警告の適用の有無を有効または無効にすることができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung SAFE および **Samsung KNOX** の設定

- ブラウザーを無効化： ユーザーのデバイスで Samsung ブラウザーを完全に無効にするかどうかを選択します。デフォルトは ［オフ］ で、ユーザーはブラウザーを使用できます。ブラウザーを無効にした場合、以下のオプションは表示されなくなります。
- ポップアップを無効化： ブラウザーでポップアップメッセージを許可するかどうかを選択します。
- **Javascript** を無効化： ブラウザーで JavaScript の実行を許可するかどうかを選択します。
- **Cookie** を無効化： Cookie を許可するかどうかを選択します。
- オートフィルを無効化： ユーザーがブラウザーのオートフィル機能をオンにできるかどうかを選択します。
- 不正な **Web** サイトに対する警告を表示： ユーザーが不正な、または信頼できない Web サイトを参照したときに、警告メッセージを表示するかどうかを選択します。

カレンダー（**CalDav**）デバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、カレンダー（CalDAV）アカウントをユーザーの iOS デバイスまたは macOS デバイスに追加し、CalDAV をサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明： アカウントの説明を入力します。このフィールドは必須です。

- ホスト名: CalDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート: CalDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**: ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名: ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード: 任意で、ユーザーのパスワードを入力します。
- **SSL** を使用: CalDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］ です。

macOS 設定

- アカウントの説明: アカウントの説明を入力します。このフィールドは必須です。
- ホスト名: CalDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート: CalDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**: ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名: ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード: 任意で、ユーザーのパスワードを入力します。
- **SSL** を使用: CalDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］ です。

モバイルデバイスポリシー

January 10, 2020

このポリシーを使用すると、iOS デバイスのモバイルネットワーク設定を構成できます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- **APN** をアタッチ
  - 名前: この構成の名前です。
  - 認証の種類: 一覧から、［**CHAP**］（Challenge-Handshake Authentication Protocol: チャレンジハンドシェイク認証プロトコル）または ［**PAP**］（Password Authentication Protocol: パスワード認証プロトコル）のいずれかを選択します。デフォルトは ［**PAP**］ です。
  - ［ユーザー名］ と ［パスワード］: 認証に使用するユーザー名とパスワードです。

- **APN**
  - 名前： APN（Access Point Name：アクセスポイント名）構成の名前です。
  - 認証の種類： 一覧から、［**CHAP**］ または ［**PAP**］ を選択します。デフォルトは［**PAP**］です。
  - ［ユーザー名］ と ［パスワード］： 認証に使用するユーザー名とパスワードです。
  - プロキシサーバー： プロキシサーバーのネットワークアドレスです。
  - プロキシサーバーポート： プロキシサーバーのポート番号です。

接続マネージャーデバイスポリシー

August 22, 2019

XenMobile では、インターネットおよびプライベートネットワークに自動的に接続するアプリケーションの接続設定を指定できます。このポリシーは Windows Pocket PC でのみ使用できます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Mobile/CE の設定

> 注：
>
> 組み込みのオフィスとは、すべての接続が社内のイントラネットに接続されていることを意味します。組み込みのインターネットとは、すべての接続がインターネットに接続されていることを意味します。

- プライベートネットワークに接続するアプリで自動的に使用： 一覧から、［組み込みのオフィス］ または ［組み込みのインターネット］ を選択します。デフォルトは ［組み込みのオフィス］ です。
- プライベートネットワークに接続するアプリで自動的に使用： 一覧から、［組み込みのオフィス］ または ［組み込みのインターネット］ を選択します。デフォルトは ［組み込みのオフィス］ です。

接続スケジュールデバイスポリシー

August 22, 2019

> 重要：
>
> Firebase Cloud Messaging (FCM) を使用して Android、Android Enterprise、Chrome OS の各デバイスから XenMobile Server への接続を制御することをお勧めします。FCM の使用について詳しくは、「Firebase Cloud Messaging」を参照してください。

FCM を使用しない場合は、接続スケジュールポリシーを作成して、ユーザーデバイスを XenMobile Server に接続する方法と時間を管理します。

ユーザーが手動でデバイスを接続するか、定義した期間内にデバイスが接続されるようにするかを指定できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

プラットフォーム設定

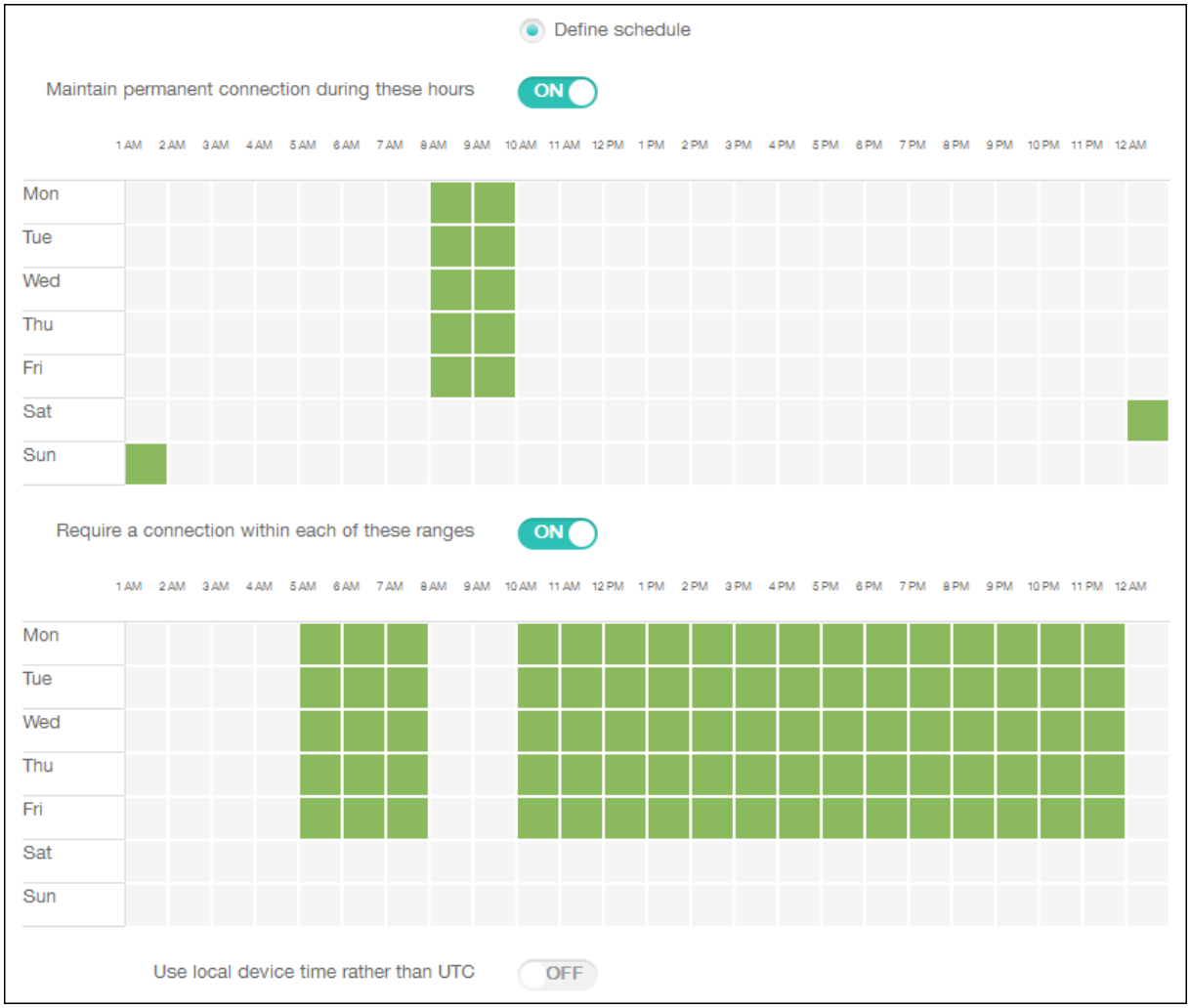
- デバイスに接続を要求： このスケジュールに対して設定するオプションをクリックします。
  - 常に： 接続のオンライン状態を永続的に維持します。ユーザーのデバイス上の XenMobile は、ネットワーク接続が失われた後、XenMobile サーバーへの再接続を試行し、一定の間隔でコントロールパケットを送信することによって接続を監視します。最適化されたセキュリティについては、このオプションをお勧めします。［常に］ を選択する場合は、デバイスでトンネルポリシーの ［接続のタイムアウトを定義］ 設定も使用して、接続によりバッテリーが切れないようにします。接続のオンライン状態を維持することにより、ワイプやロックなどのセキュリティコマンドを必要に応じてデバイスにプッシュできます。デバイスに展開された各ポリシーで、［展開スケジュール］ の ［常時接続に対する展開］ オプションを選択する必要もあります。
  - しない： 手動で接続します。ユーザーがデバイス上の XenMobile から接続を開始する必要があります。デバイスにセキュリティポリシーを展開できず、新しいアプリやポリシーを受信しなくなるため、実稼働環境ではこのオプションはおすすめしません。
  - 毎： 指定された間隔で接続します。このオプションが有効な状態でロックやワイプなどのセキュリティポリシーを送信すると、この操作は次回デバイスが接続されたときに処理されます。このオプションを選択すると、［**N** 分ごとに接続］ フィールドが表示されます。このフィールドに、デバイスが再接続されるまでの分数を入力する必要があります。デフォルトは **20** です。
  - スケジュールを定義： 有効にすると、ユーザーのデバイス上の XenMobile は、ネットワーク接続が失われた後に XenMobile サーバーへの再接続を試行し、定義した期間中、一定の間隔でコントロールパケットを送信することによって接続を監視します。接続期間の定義方法については、「接続期間の定義」を参照してください。
    * この時間帯は永続的な接続を維持： 定義した期間中、ユーザーのデバイスが接続されている必要があります。
    * これらの各範囲内で接続を要求： 定義した期間内に 1 回以上、ユーザーのデバイスが接続される必要があります。
    * **UTC** ではなくローカルデバイスの時間を使用： 定義した期間を、UTC（Coordinated Universal Time：協定世界時）ではなくローカルデバイスの時間に同期させます。

接続期間の定義

以下のオプションを有効にすると時間軸が表示されます。これを使用して必要な期間を定義できます。特定の時間内に永続的な接続を必要とするオプション、または特定の期間内に 1 回の接続を必要とするオプションのいずれか、ま

たはその両方を有効にできます。時間軸の各四角は 30 分間であるため、毎平日の 8:00 AM ～ 9:00 AM に接続が必要な場合は、時間軸で毎平日の［8 AM］と［9 AM］の間の 2 つの四角をクリックします。

たとえば、次の図の 2 つの時間軸では、毎平日の 8:00 AM ～ 9:00 AM に永続的な接続、土曜日の 12:00 AM ～日曜日の 1:00 AM に永続的な接続、毎平日の 5:00 AM ～ 8:00 AM または 10:00 AM ～ 11:00 PM に 1 回以上の接続が必要です。



連絡先（**CardDAV**）デバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、iOS 連絡先（CardDAV）アカウントをユーザーの iOS デバイスまたは macOS デバイスに追加し、CardDAV をサポートするサーバーとそのデバイスの連絡先データを同期することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明: アカウントの説明を入力します。このフィールドは必須です。
- ホスト名: CardDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート: CardDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**: ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名: ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード: 任意で、ユーザーのパスワードを入力します。
- **SSL** を使用: CardDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］ です。

macOS 設定

- アカウントの説明: アカウントの説明を入力します。このフィールドは必須です。
- ホスト名: CardDAV サーバーのアドレスを入力します。このフィールドは必須です。
- ポート: CardDAV サーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは **8443** です。
- プリンシパル **URL**: ユーザーのカレンダーに対するベース URL を入力します。
- ユーザー名: ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード: 任意で、ユーザーのパスワードを入力します。
- **SSL** を使用: CardDAV サーバーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オン］ です。

OS 更新の制御デバイスポリシー

January 10, 2020

OS 更新の制御デバイスポリシーを使用すると、以下を展開できます。

- 監視対象の iOS デバイスへの最新の OS 更新プログラムの展開。

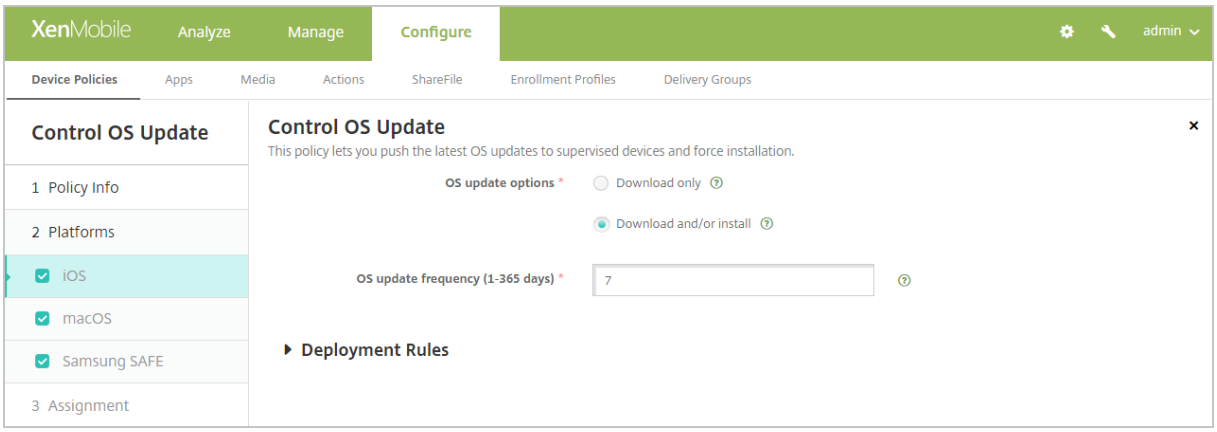
  iOS 10.3 以降を実行しているデバイスの場合、OS 更新の制御ポリシーは監視対象デバイスで機能します。iOS 10.3 より前のバージョンを実行している場合、OS 更新の制御ポリシーは監視対象デバイスおよび DEP に登録済みデバイスの両方で機能します。

- macOS 10.11.5 以降を実行している DEP 登録済み macOS デバイスへの、最新の OS とアプリの更新プログラムの展開。
- 監視対象の Samsung SAFE デバイスへの最新の OS 更新プログラムの展開。

  Samsung SAFE デバイスの場合、XenMobile は OS 更新の制御ポリシーを Secure Hub に送信し、Secure Hub がポリシーをデバイスに適用します。［管理］**>**［デバイス］ ページには、XenMobile Server がポリシーを送信するタイミングと、デバイスがポリシーを受信するタイミングが表示されます。

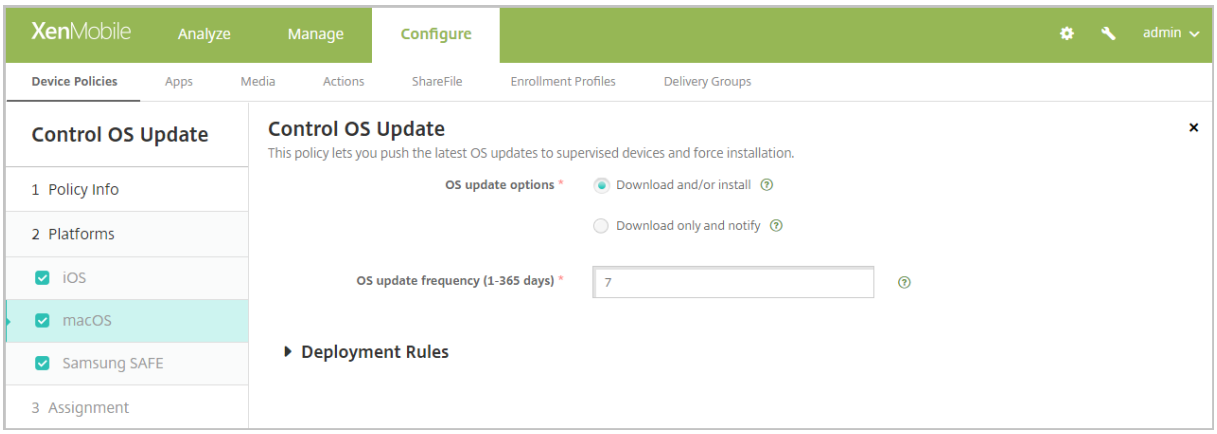
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **OS** の更新オプション: いずれのオプションでも［**OS** の更新頻度］ に従って、最新の OS 更新プログラムが監視対象デバイスにダウンロードされます。デバイスにより、更新プログラムのインストールが促されます。ユーザーがデバイスのロックを解除すると、プロンプトが表示されます。
- **OS** の更新頻度: XenMobile がデバイスの OS をチェックして更新する頻度を決定します。デフォルトは **7** 日です。

macOS 設定



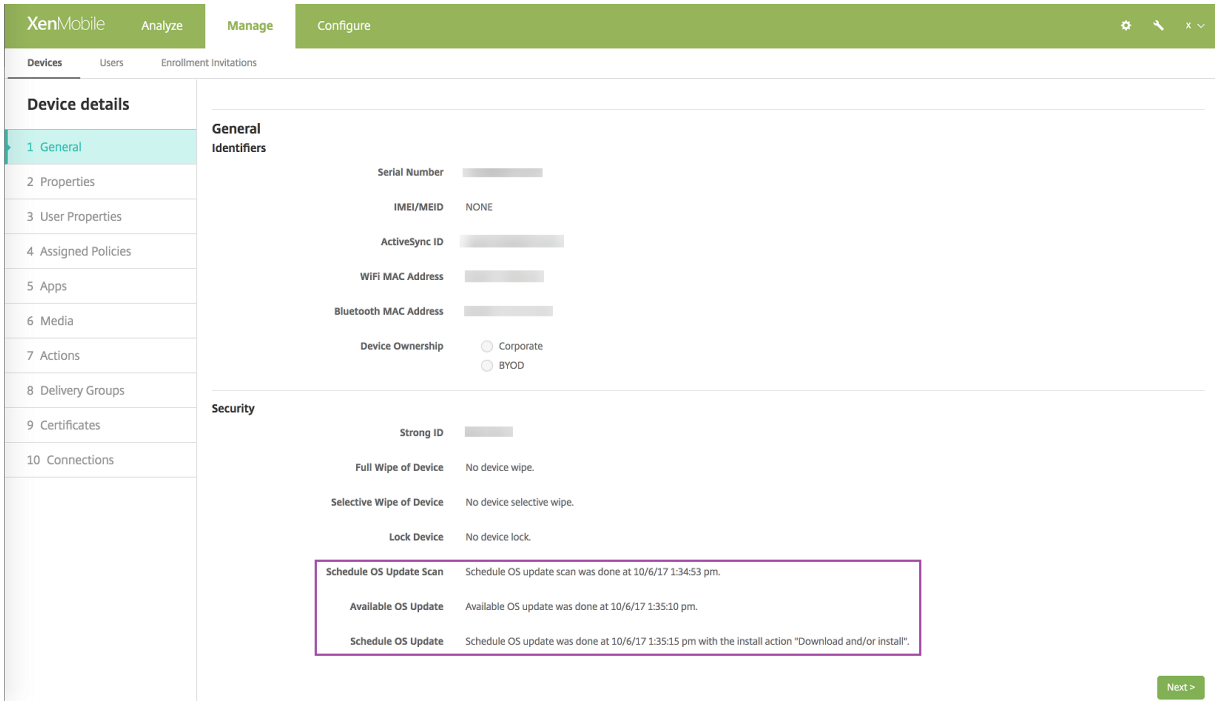
- **OS** の更新オプション： いずれのオプションでも［**OS** の更新頻度］ に従って、最新の macOS 更新プログラムがダウンロードされます。更新プログラムをインストールするか、更新プログラムが利用可能であることを App Store 経由でユーザーに通知するかを選択できます。
- **OS** の更新頻度： XenMobile がデバイスの OS をチェックして更新する頻度を決定します。デフォルトは **7** 日です。

iOS と macOS の更新操作のステータス取得

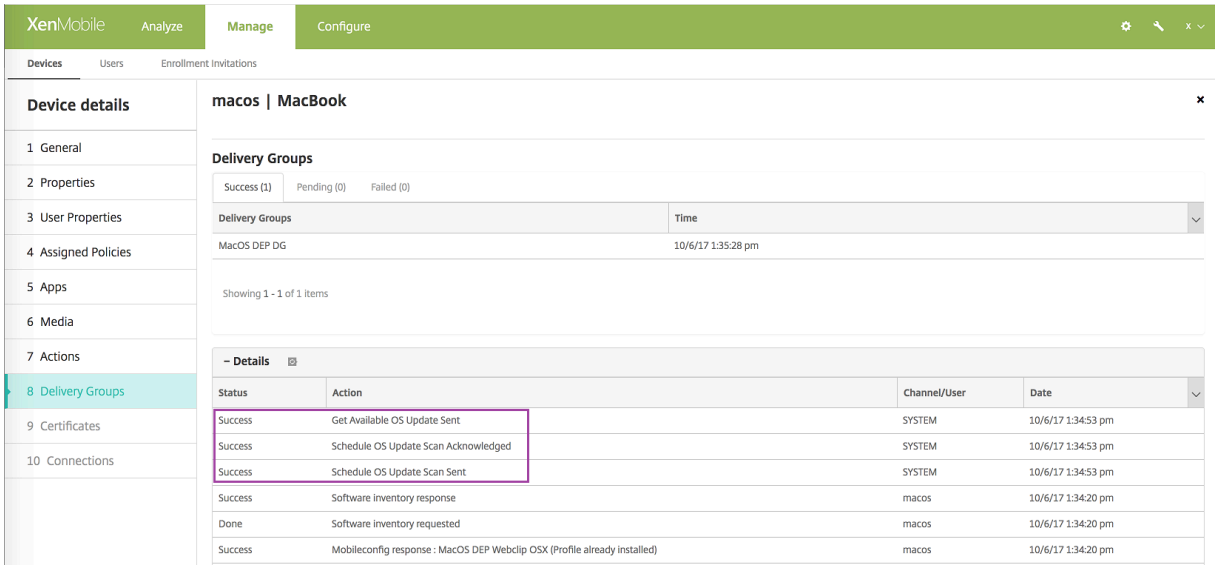
iOS と macOS の場合、XenMobile は OS 更新の制御ポリシーをデバイスに展開しません。代わりに、XenMobile はこのポリシーを使用して、次の MDM コマンドをデバイスに送信します。

- OS 更新プログラムのスキャンスケジュール：デバイスが OS 更新プログラムのバックグラウンドスキャンを実行するように要求します。（iOS ではオプション）
- 利用可能な OS 更新プログラム：利用可能な OS 更新プログラムの一覧をデバイスに問い合わせます。
- OS 更新プログラムのスケジュール：デバイスが macOS の更新プログラム、アプリの更新プログラム、またはその両方を実行するように要求します。したがって、デバイス OS は、OS およびアプリの更新プログラムをダウンロードまたはインストールするタイミングを決定します。

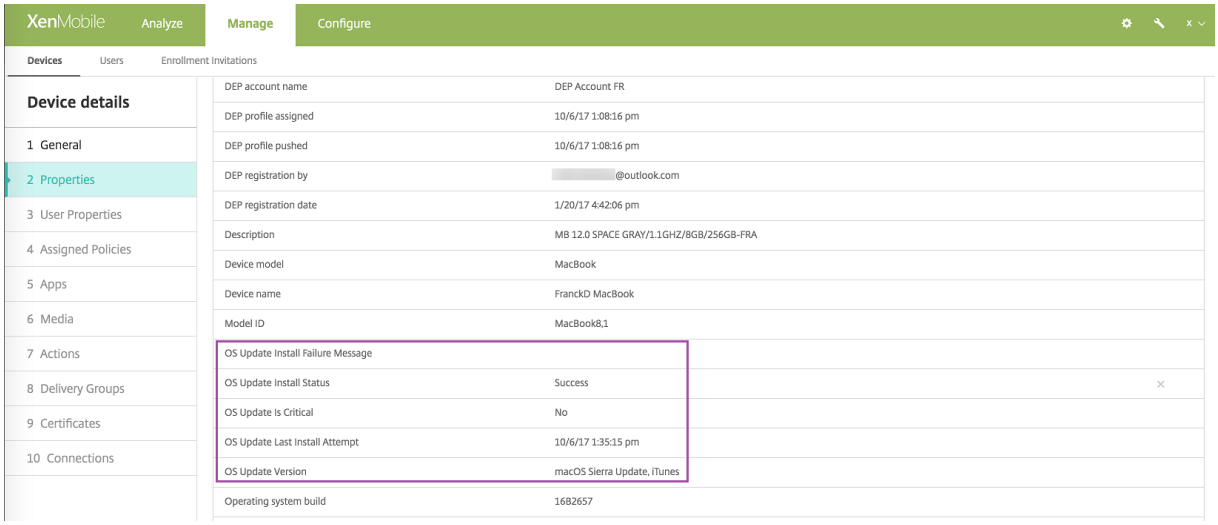
［管理］ **>** ［デバイス］ **>** ［デバイス詳細（全般）］ ページには、スケジュールされた使用可能な OS 更新プログラムスキャンのステータスと、スケジュールされた macOS とアプリの更新プログラムが表示されます。

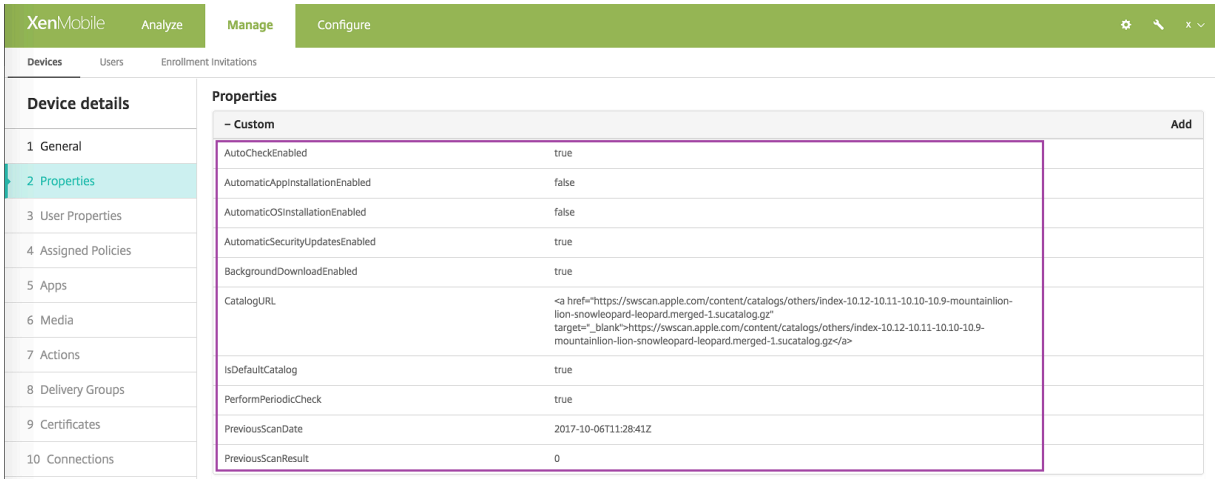


更新操作のステータスの詳細については、［管理］**>**［デバイス］**>**［デバイス詳細（デリバリーグループ）］ページを参照してください。



利用可能な OS 更新プログラムの一覧や最後のインストールの試行などの詳細については、［管理］**>**［デバイス］**>**［デバイス詳細（プロパティ）］ページを参照してください。

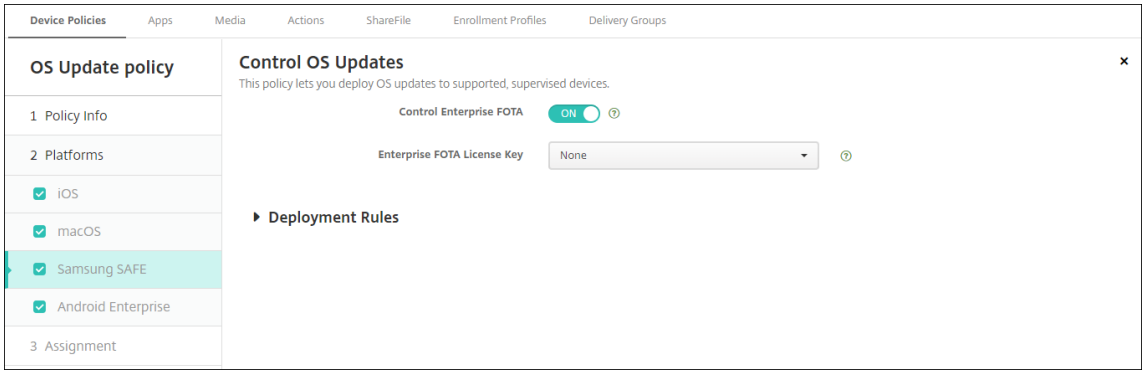




Samsung SAFE の設定

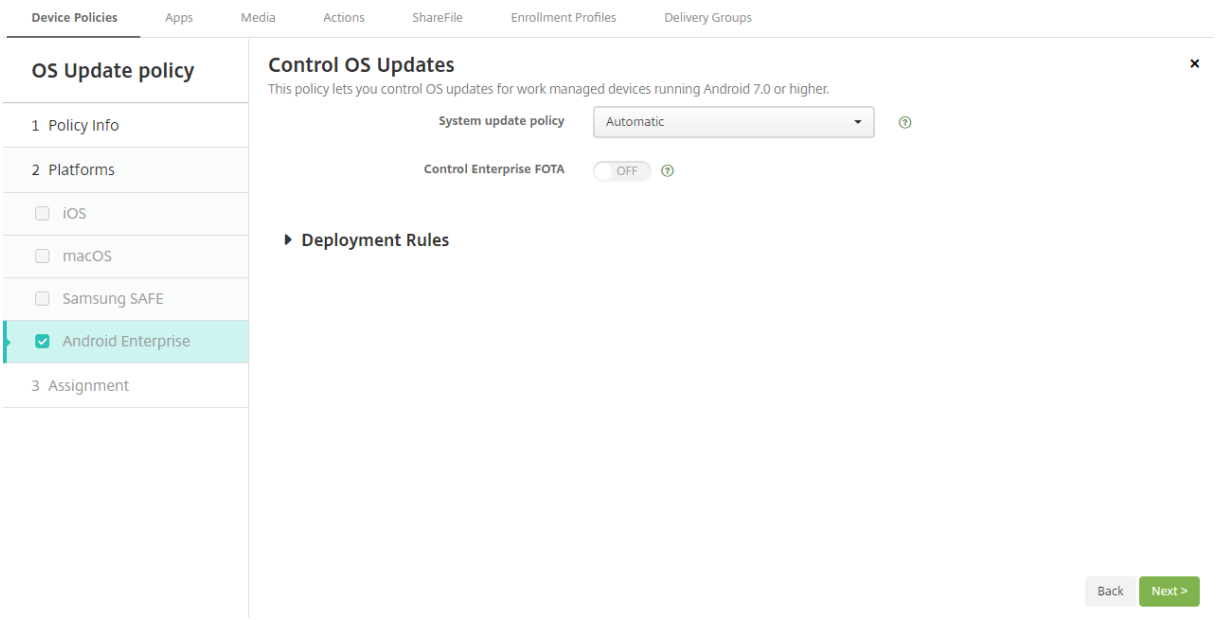
Samsung Enterprise FOTA（E-FOTA）では、デバイスの更新時期や使用するファームウェアのバージョンを決定できます。E-FOTA を使用するには:

1. Samsung から受け取ったキーとライセンス情報で Samsung MDM ライセンスキーデバイスポリシーを作成します。詳しくは、「Samsung MDM ライセンスキーデバイスポリシー」を参照してください。
2. Enterprise FOTA を有効にして OS 更新の制御デバイスポリシーを作成します。



- **Enterprise FOTA** の有効化: ［オン］ に設定します。
- **Enterprise FOTA** ライセンスキー: Samsung MDM ライセンスキーデバイスポリシーの名前を選択します。

Android Enterprise の設定



- システム更新ポリシー。システムの更新を行うタイミングを指定します。［自動］ では、更新プログラムが利用可能になるとインストールされます。［ウィンドウ］ では、［開始時間］と ［終了時間］ で指定した毎日のメンテナンスウィンドウ内に更新プログラムが自動でインストールされます。［延期］ に設定すると、ユーザーは最大 30 日間更新を延期できるようなります。
  - 開始日時。メンテナンスウィンドウの開始時間（分単位。**0** ～ **1440**）。デバイスのローカル時間の午前 0 時を基準とします。デフォルト値は **0** です。
  - 終了時間。メンテナンスウィンドウの終了時間（分単位。**0** ～ **1440**）。デバイスのローカル時間の午前 0 時を基準とします。デフォルトは **120** です。
- **Enterprise FOTA** の制御。Samsung Enterprise Firmware-Over-The-Air（E-FOTA）サービスを使用した

Samsung デバイスの更新を監理できます。Samsung Knox 3.0 以降を実行している Android Enterprise デバイスで有効です。デフォルトは ［オフ］ です。

- **Enterprise FOTA** ライセンスキー。［**Enterprise FOTA** の制御］ が ［オン］ の場合、［**Enterprise FOTA** ライセンスキー］ で Samsung FOTA の更新に使用するライセンスキーを指定できます。Samsung Knox 3.0 以降を実行している Android Enterprise デバイスで有効です。デフォルトは ［なし］ です。このキーは、［**Samsung MDM** ライセンスキー］ デバイスポリシーを使用して設定できます。Samsung MDM ライセンスキーデバイスポリシーを参照してください。

Samsung コンテナへのアプリのコピーデバイスポリシー

August 22, 2019

デバイスに既にインストールされているアプリが、サポートされている Samsung デバイス上の SEAMS コンテナまたは KNOX コンテナにコピーされるように指定できます。サポートされるデバイスの詳細については、Samsung の記事「Devices built on Knox」を参照してください。

SEAMS コンテナにコピーされたアプリは、ユーザーのホーム画面で使用できます。KNOX コンテナにコピーされたアプリは、ユーザーが KNOX コンテナにサインインした場合のみ使用できます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提条件

- XenMobile でのデバイスの登録
- Samsung MDM キー（ELM と KLM）を展開します。方法については、「Samsung MDM ライセンスキーデバイスポリシー」を参照してください。
- デバイスにアプリをインストールします。
- デバイスで KNOX を初期化して、アプリを KNOX コンテナにコピーします。

プラットフォーム設定

- 新規アプリ： 一覧に追加するアプリごとに、［追加］ をクリックして以下の操作を行います：
  - パッケージ ID を入力します。たとえば、LacingArt アプリの場合は com.mobiwolf.lacingart。
  - ［保存］ または ［キャンセル］ をクリックします。

資格情報デバイスポリシー

October 25, 2019

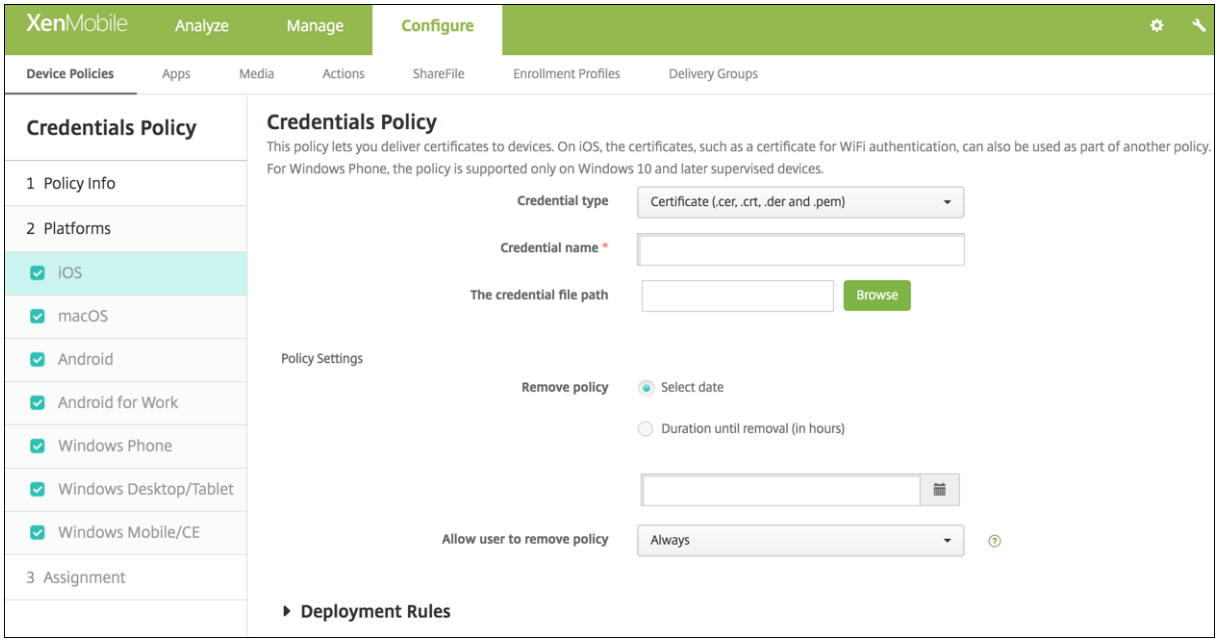
XenMobile で資格情報デバイスポリシーを作成し、XenMobile の PKI 構成（PKI エンティティ、キーストア、資格情報プロバイダー、サーバー証明書など）を使用した統合認証を有効にすることができます。資格情報について詳しくは、「証明書と認証」を参照してください。

資格情報ポリシーは、iOS、macOS、Android、Android Enterprise、Windows デスクトップ/タブレット、Windows Mobile/CE、Windows Phone デバイスに対して作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

> 注:
>
> このポリシーを作成するには、各プラットフォームで使用する予定の資格情報と、証明書およびパスワードが必要です。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

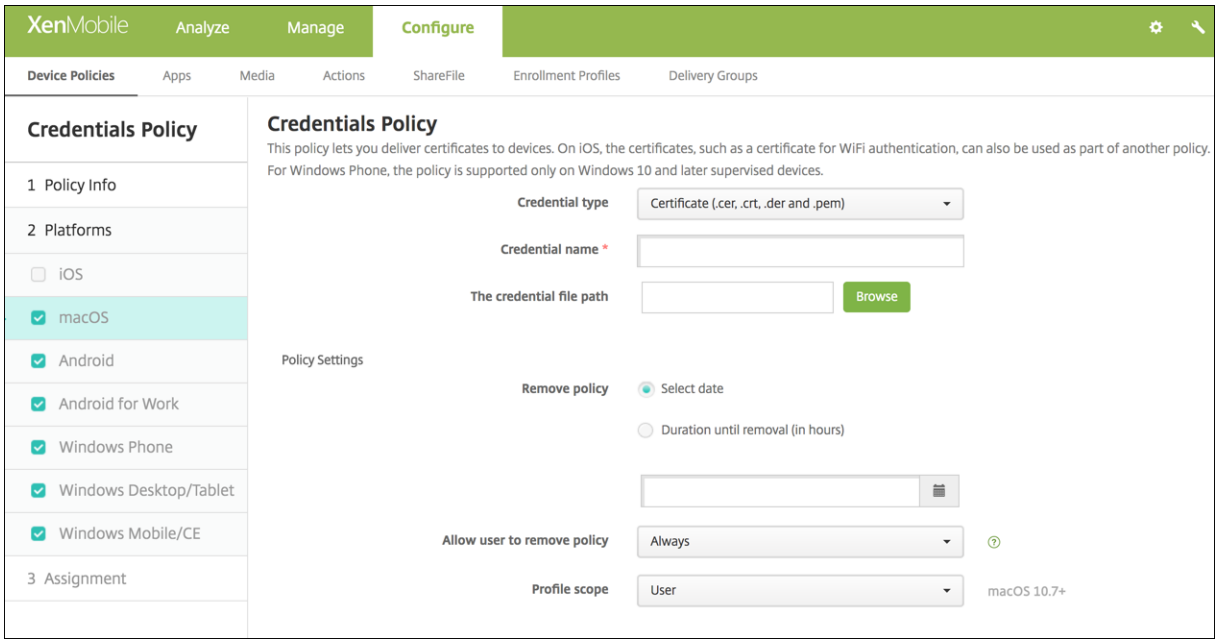


次の設定を構成します:

- 資格情報の種類: 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - 証明書

    * 資格情報の名前: 資格情報の固有の名前を入力します。
    * 資格情報ファイルのパス: ［ブラウザー］をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
  - キーストア
    * 資格情報の名前: 資格情報の固有の名前を入力します。
    * 資格情報ファイルのパス: ［ブラウザー］をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
    * パスワード: 資格情報のキーストアパスワードを入力します。
  - サーバー証明書
    * サーバー証明書: ボックスの一覧で、使用する証明書を選択します。
  - 資格情報プロバイダー
    * 資格情報プロバイダー: ボックスの一覧で、資格情報プロバイダーの名前を選択します。

macOS 設定

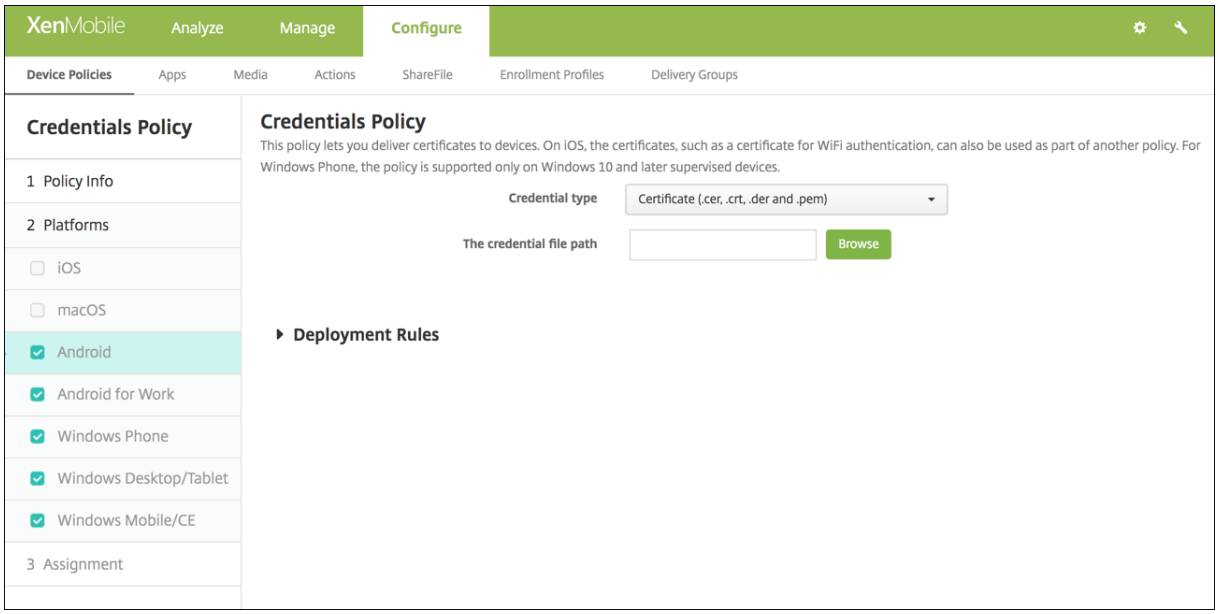


次の設定を構成します:

- 資格情報の種類: 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - 証明書
    * 資格情報の名前: 資格情報の固有の名前を入力します。
    * 資格情報ファイルのパス: ［参照］をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
  - キーストア
    * 資格情報の名前: 資格情報の固有の名前を入力します。

    * 資格情報ファイルのパス: ［参照］ をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
    * パスワード: 資格情報のキーストアパスワードを入力します。
  - サーバー証明書
    * サーバー証明書: ボックスの一覧で、使用する証明書を選択します。
  - 資格情報プロバイダー
    * 資格情報プロバイダー: ボックスの一覧で、資格情報プロバイダーの名前を選択します。

Android および **Android Enterprise** の設定

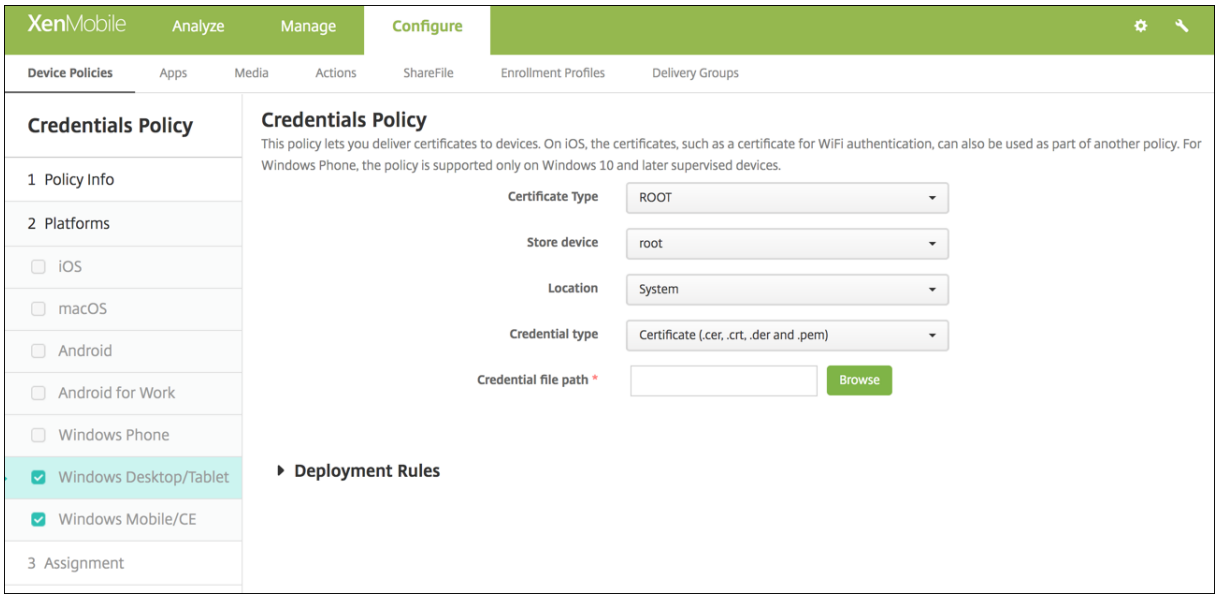


次の設定を構成します:

- 資格情報の種類: 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - 証明書
    * 資格情報の名前: 資格情報の固有の名前を入力します。
    * 資格情報ファイルのパス: ［参照］をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
  - キーストア
    * 資格情報の名前: 資格情報の固有の名前を入力します。
    * 資格情報ファイルのパス: ［参照］ をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。
    * パスワード: 資格情報のキーストアパスワードを入力します。
  - サーバー証明書
    * サーバー証明書: ボックスの一覧で、使用する証明書を選択します。

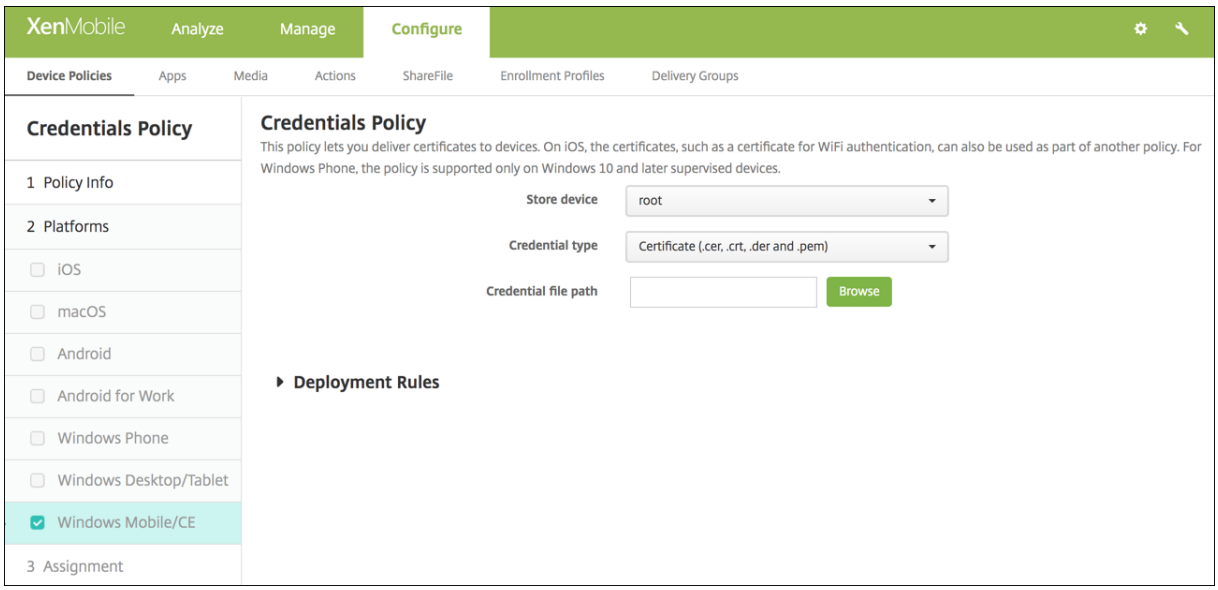
- 資格情報プロバイダー
  - 資格情報プロバイダー： ボックスの一覧で、資格情報プロバイダーの名前を選択します。

Windows デスクトップ/タブレットの設定



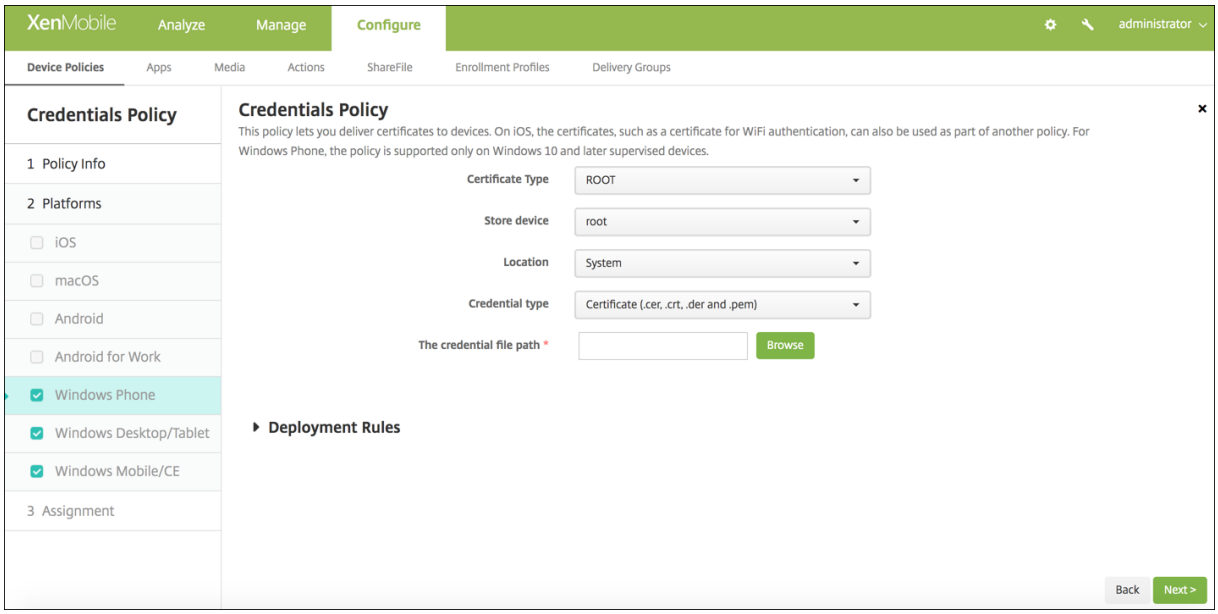
- 証明書の種類： 一覧から、［**ROOT**］ または ［**CLIENT**］ を選択します。
- ［**ROOT**］ を選択した場合は、次の設定を構成します。
  - ストアデバイス：資格情報の証明書ストアの場所に応じて、ボックスの一覧で［**root**］、［**My**］、［**CA**］のいずれかを選択します。［**My**］ を選択すると、証明書はユーザーの証明書ストアに保存されます。
  - 場所： Windows 10 タブレットの場合、場所は ［システム］ のみです。
  - 資格情報の種類： Windows 10 タブレットの場合、資格情報の種類は 証明書のみです。
  - 資格情報ファイルのパス： ［参照］ をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
- ［**CLIENT**］ を選択した場合は、次の設定を構成します。
- 場所： Windows 10 タブレットの場合、場所は ［システム］ のみです。
- 資格情報の種類： Windows 10 タブレットの場合、資格情報の種類はキーストアのみです。
- 資格情報の名前： 資格情報の名前を入力します。このフィールドは必須です。
- 資格情報ファイルのパス： ［参照］ をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
- パスワード： 資格情報に関連付けられたパスワードを入力します。このフィールドは必須です。

Windows Mobile/CE の設定



- ストアデバイス: ボックスの一覧から、資格情報の証明書ストアの場所を選択します。デフォルトは ［**root**］です。次のオプションがあります:
  - 特権のある実行信頼証明機関: このストアに属する証明書で署名されたアプリケーションが、特権信頼レベルで実行されます。
  - 特権のない実行信頼証明機関: このストアに属する証明書で署名されたアプリケーションが、標準信頼レベルで実行されます。
  - **SPC**（ソフトウェア発行者の証明書）: .cab ファイルの署名にソフトウェア発行元証明書（SPC）が使用されます。
  - **root**: ルート証明書を含む証明書ストア。
  - **CA**: 暗号化情報を含む証明書ストア（中間証明機関を含む）。
  - **MY**: エンドユーザーの個人証明書を含む証明書ストア。
- 資格情報の種類: Windows Mobile/CE デバイスの場合、資格情報の種類は証明書のみです。
- 資格情報ファイルのパス: ［参照］ をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。

Windows Phone の設定



- 証明書の種類: 一覧から、［**ROOT**］ または ［**CLIENT**］ を選択します。
- ［**ROOT**］ を選択した場合は、次の設定を構成します。
  - ストアデバイス: 資格情報の証明書ストアの場所に応じて、ボックスの一覧で［**root**］、［**My**］、［**CA**］のいずれかを選択します。［**My**］ を選択すると、証明書はユーザーの証明書ストアに保存されます。
  - 場所: Windows Phone の場合、場所は［システム］のみです。
  - 資格情報の種類: Windows Phone の場合、資格情報の種類は証明書のみです。
  - 資格情報ファイルのパス: ［参照］ をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
- ［**CLIENT**］ を選択した場合は、次の設定を構成します。
  - 場所: Windows Phone の場合、場所は ［システム］ のみです。
  - 資格情報の種類: Windows Phone の場合、資格情報の種類は キーストアのみです。
  - 資格情報の名前: 資格情報の名前を入力します。このフィールドは必須です。
  - 資格情報ファイルのパス: ［参照］ をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
  - パスワード: 資格情報に関連付けられたパスワードを入力します。このフィールドは必須です。

カスタム XML デバイスポリシー

August 22, 2019

XenMobile でカスタム XML ポリシーを作成して、サポートされる Windows、Zebra Android、および Android Enterprise デバイスの次の機能をカスタマイズできます:

- プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。
- デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。
- ソフトウェアのアップグレード。アプリやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。
- 障害管理。デバイスからのエラーおよび状態レポートの受信などです。

Windows デバイスの場合、Windows で Open Mobile Alliance Device Management（OMA DM）API を使用して、カスタム XML 構成を作成します。OMA DM API を使用したカスタム XML の作成については、このトピックでは扱いません。OMA DM API の使用について詳しくは、Microsoft Developer Network サイトの「OMA Device Management」を参照してください。

Zebra Android および Android Enterprise デバイスの場合、MX Management System（MXMS）を使用してカスタム XML 構成を作成します。MXMS API を使用したカスタム XML の作成については、この記事では扱いません。MXMS の使用について詳しくは、Zebra のサイトの「About MX」を参照してください。

> 注：
>
> Windows 10 RS2 Phone：Internet Explorer を無効にするカスタム XML ポリシーまたは制限ポリシーをスマートフォンに展開しても、Internet Explorer が有効なままです。この問題を解決するには、スマートフォンを再起動します。これはサードパーティ製品の問題です。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Phone、**Windows** デスクトップ/タブレット、**Zebra Android**、**Android Enterprise** の設定

- **XML** コンテンツ： ポリシーに追加するカスタム XML コードを入力するか、コピーして貼り付けます。

  ［次へ］ をクリックすると、XenMobile で XML コンテンツの構文がチェックされます。構文エラーがある場合、コンテンツボックスの下に表示されます。続行するにはエラーを修正してください。

  構文エラーがない場合は、［カスタム **XML** ポリシー］ 割り当てページが開きます。

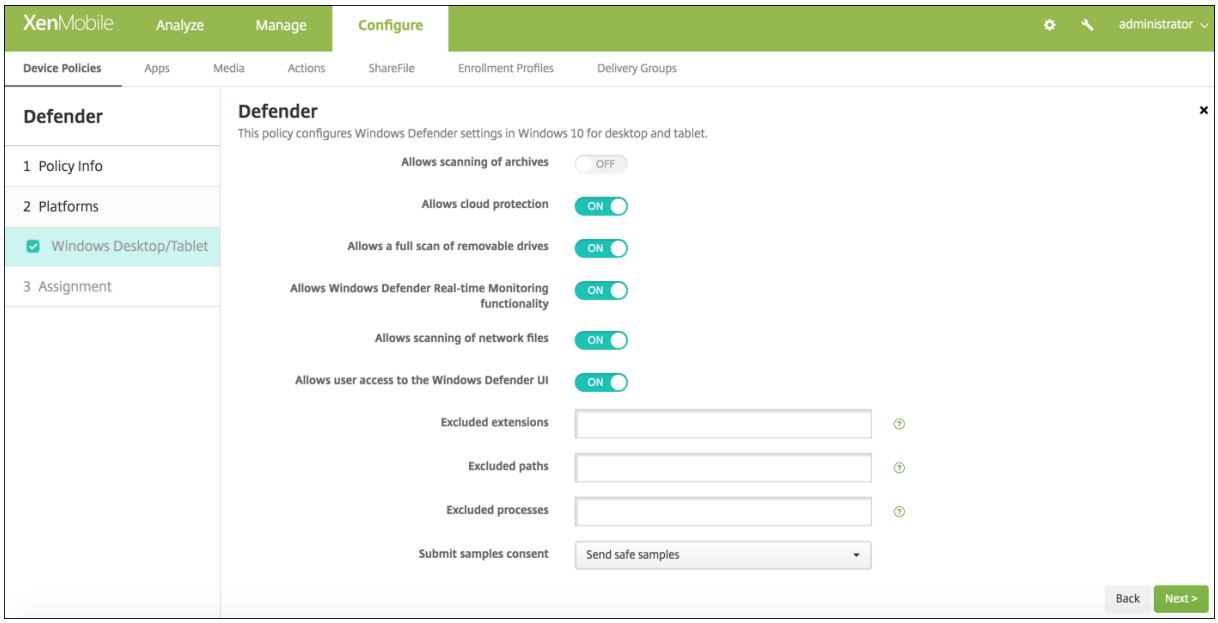
Defender デバイスポリシー

August 22, 2019

Windows Defender は、Windows 10 に搭載されたマルウェア対策ソフトです。XenMobile デバイスポリシー［Defender］を使用して、デスクトップおよびタブレットの Windows 10 の Microsoft Defender ポリシーを構成できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows デスクトップとタブレットの設定



- アーカイブのスキャンを許可する: Defender がアーカイブファイルをスキャンすることを許可または禁止します。デフォルトは、［オフ］ です。
- クラウド保護を許可する: Defender がマルウェアの活動について Microsoft に情報を送信することを許可または禁止します。デフォルトは、［オン］ です。
- リムーバブルドライブのスキャンを許可する: Defender が USB スティックなどのリムーバブルドライブをスキャンすることを許可または禁止します。デフォルトは、［オン］ です。
- **Windows Defender** のリアルタイム監視機能を許可する: デフォルトは ［オン］ です。
- ネットワークファイルのスキャンを許可する: Defender がネットワークファイルをスキャンすることを許可または禁止します。デフォルトは、［オン］ です。
- ユーザーに **Windows Defender** の **UI** へのアクセスを許可する: ユーザーが Windows Defender ユーザーインターフェイスにアクセスできるかどうかを指定します。この設定は、次にユーザーデバイスが起動するときに有効になります。この設定が ［オフ］ の場合、ユーザーは Windows Defender の通知を受け取りません。デフォルトは、［オン］ です。
- 除外された拡張子: リアルタイムまたは定時スキャンから除外する拡張子。拡張子を区切るには、|文字を使用します。たとえば、「lib|obj」と入力します。
- 除外されたパス: リアルタイムまたは定時スキャンから除外するパス。パスを区切るには、|文字を使用します。たとえば、「C:\Example|C:\Example1」と入力します。
- 除外された処理: リアルタイムまたは定時スキャンから除外する処理。処理を区切るには、|文字を使用します。たとえば、「C:\Example.exe|C:\Example1.exe」と入力します。
- サンプルの提出に同意する: 悪意があるかどうかを判断するために、さらに分析が必要なファイルを Microsoft に送信するかどうかを制御します。オプション: ［常に確認する］、［安全なサンプルを送信する］、［送信しない］、［すべてのサンプルを送信する］。デフォルトは、［安全なサンプルを送信する］ です。

ファイルおよびフォルダーの削除デバイスポリシー

August 22, 2019

XenMobile でポリシーを作成して、Windows Mobile/CE デバイスから特定のファイルまたはフォルダーを削除できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Mobile/CE の設定

- フォルダーファイルの削除: 削除するファイルまたはフォルダーごとに、［追加］をクリックして以下の操作を行います:
  - パス: ファイルまたはフォルダーまでのパスを入力します。
  - 種類: 一覧から、［ファイル］または［フォルダー］を選択します。デフォルトは［ファイル］です。
  - ［保存］ をクリックしてファイルまたはフォルダーを保存するか、［キャンセル］をクリックして操作を取り消します。

レジストリキーおよび値デバイスポリシーの削除

August 22, 2019

XenMobile でポリシーを作成して、Windows Mobile/CE デバイスから特定のレジストリキーおよび値を削除することができます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Mobile/CE の設定

- 削除するレジストリキーおよび値: 削除するレジストリキーおよび値ごとに、［追加］ をクリックして以下の操作を行います:
  - キー: レジストリキーのパスを入力します。これは必須フィールドです。レジストリキーのパスは、HKEY_CLASSES_ROOT\、HKEY_CURRENT_USER\、HKEY_LOCAL_MACHINE\、または HKEY_USERS\で始まる必要があります。
  - 値: 削除する値の名前を入力します。または、レジストリキー全体を削除する場合は、このフィールドを空白のままにします。
  - ［保存］ をクリックしてキーおよび値を保存するか、［キャンセル］ をクリックして操作を取り消します。

デバイス正常性構成証明デバイスポリシー

January 10, 2020

XenMobile では、分析目的で特定のデータおよびランタイム情報を Health Attestation Service（HAS）に送信させ、Windows 10 デバイスに正常性状態を報告させることができます。HAS は、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスから XenMobile に送信されます。XenMobile は正常性構成証明書を受信すると、その内容に基づいて、管理者が以前に設定した自動アクションを展開します。

HAS によって検証されるデータは以下のとおりです。

- AIK の有無
- BitLocker の状態
- ブートデバッグが有効化されているかどうか
- ブートマネージャー Rev リストバージョン
- コードの整合性チェックが有効化されているかどうか
- コードの整合性 Rev リストバージョン
- DEP ポリシー
- ELAM ドライバーが起動されているかどうか
- 発行時刻
- カーネルのデバッグが有効化されているかどうか
- PCR
- リセット回数
- 再起動回数
- セーフモードが有効化されているかどうか
- SBCP ハッシュ
- セキュアブートが有効化されているかどうか
- テスト署名が有効化されているかどうか
- VSM が有効であること。
- WinPE が有効であること。

詳しくは、Microsoft の「HealthAttestation CSP」ページを参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Microsoft Cloud を使用して **DHA** を構成するには

デバイス正常性構成証明ポリシーを追加し、選択した各プラットフォームに対してこの設定を構成します。

- デバイス正常性構成証明を有効にする： デバイス正常性構成証明を必須とするかどうかを選択します。デフォルトは ［オフ］ です。

オンプレミスの **Windows DHA** サーバーを使用して **DHA** を構成するには

オンプレミスで DHA を有効にするには、まず DHA サーバーを構成します。次に、XenMobile Server ポリシーを作成してオンプレミスの DHA サービスを有効にします。

1. DHA サーバーを構成するには、Windows Server 2016 Technical Preview 5 以降を実行するマシンで DHA サーバーの役割をインストールします。手順については、「オンプレミスのデバイス正常性構成証明（DHA）サーバーの構成」を参照してください。
2. デバイス正常性構成証明ポリシーを追加し、次の設定を構成します。
   - デバイス正常性構成証明を有効にする: ［オン］ にします。
   - 社内のデバイス正常性構成証明サービス（**DHA**）の構成: ［オン］ にします。
   - 社内の **DHA** サービスの **FQDN**: セットアップした DHA サーバーの完全修飾ドメイン名を入力します。
   - 社内の **DHA** の **API** バージョン: DHA サーバーにインストールする DHA サービスのバージョンを選択します。

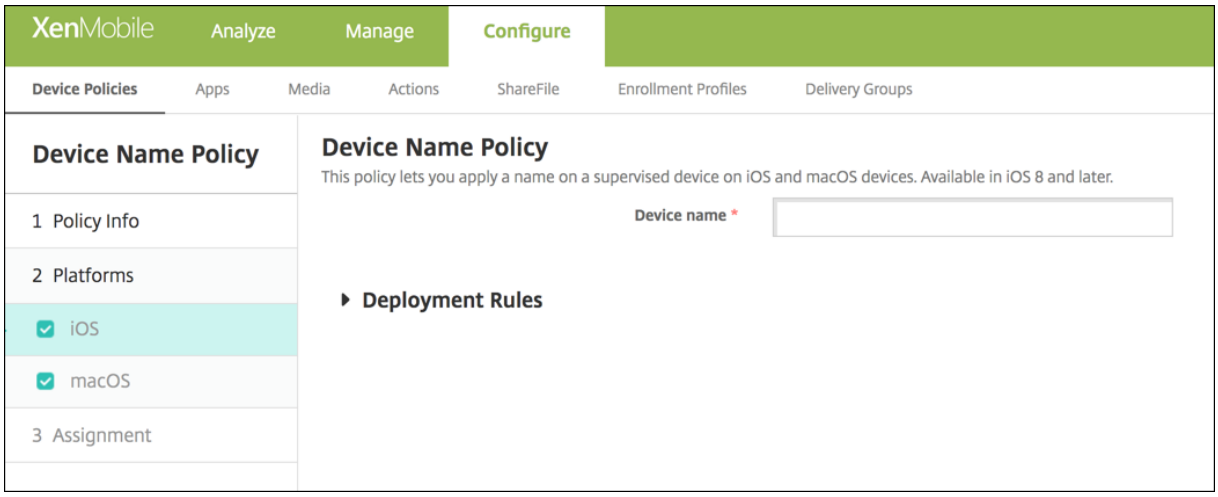
デバイス名デバイスポリシー

August 22, 2019

デバイスを特定しやすくするために、監視対象 iOS デバイスおよび macOS デバイスに名前を設定できます。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。たとえば、デバイス名をデバイスのシリアル番号として設定するには、${device.serialnumber} を使用します。デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.com を使用します。マクロについて詳しくは、「XenMobile のマクロ」を参照してください。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および macOS の設定



- デバイス名: マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。たとえば、デバイス名を各デバイスのシリアル番号に設定するには、${device.serialnumber} を使用します。デバイス名にユーザーの名前を含めるには、${device.serialnumber} ${ user.username} を使用します。

Education の構成デバイスポリシー

August 22, 2019

Education の構成デバイスポリシーでは、以下について定義します:

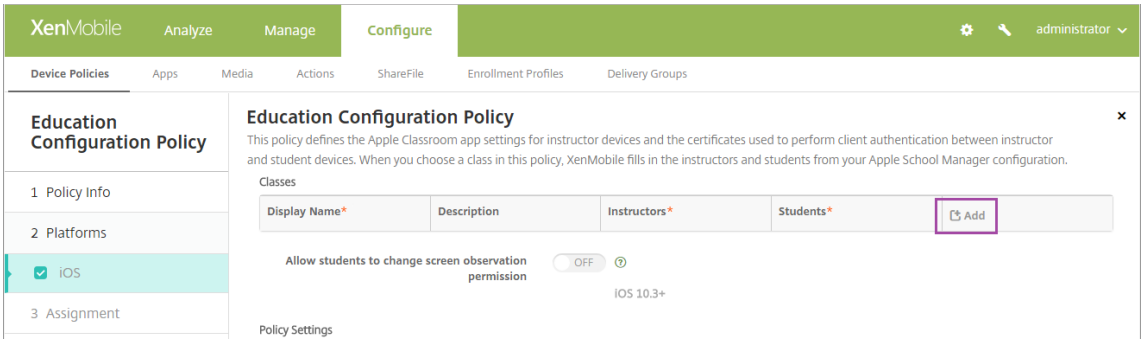
- 講師用デバイスの Apple クラスルームアプリの設定。
- 講師用デバイスと生徒用デバイス間でクライアント認証を実行するために使用する証明書。

このポリシーでクラスを選択すると、XenMobile コンソールで Apple School Manager の構成から講師と生徒が記入されます。このポリシーの Apple クラスルームアプリの設定がすべてのクラスで同じ場合は、ポリシーを 1 つ作成します。

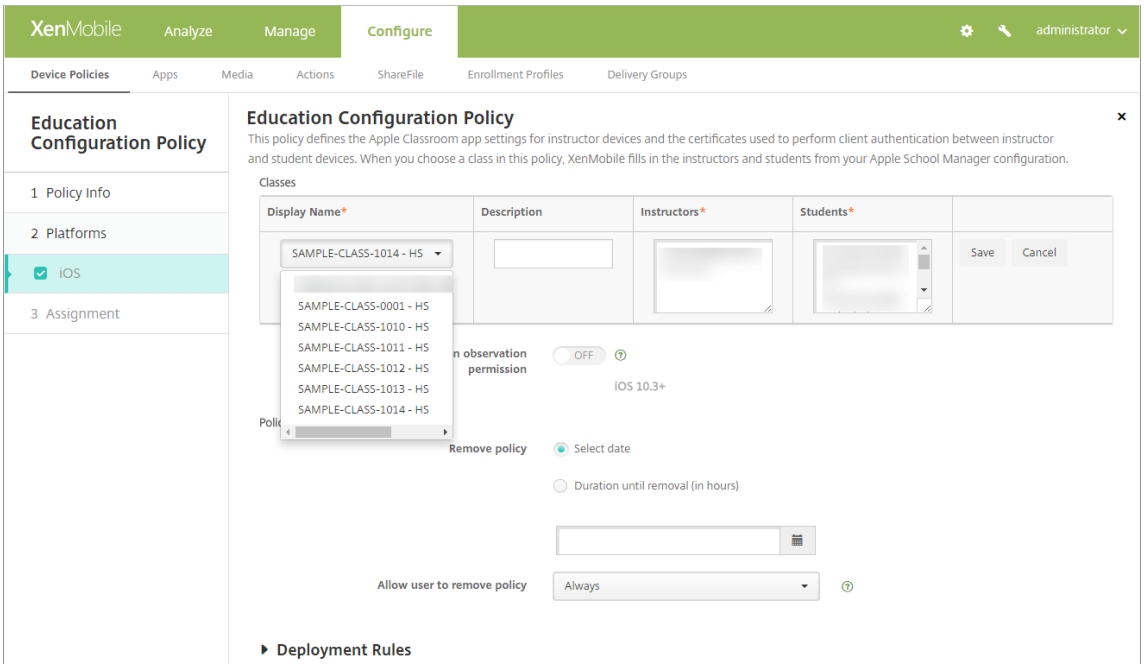
このポリシーを追加または構成するには、［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

ポリシーを構成するには

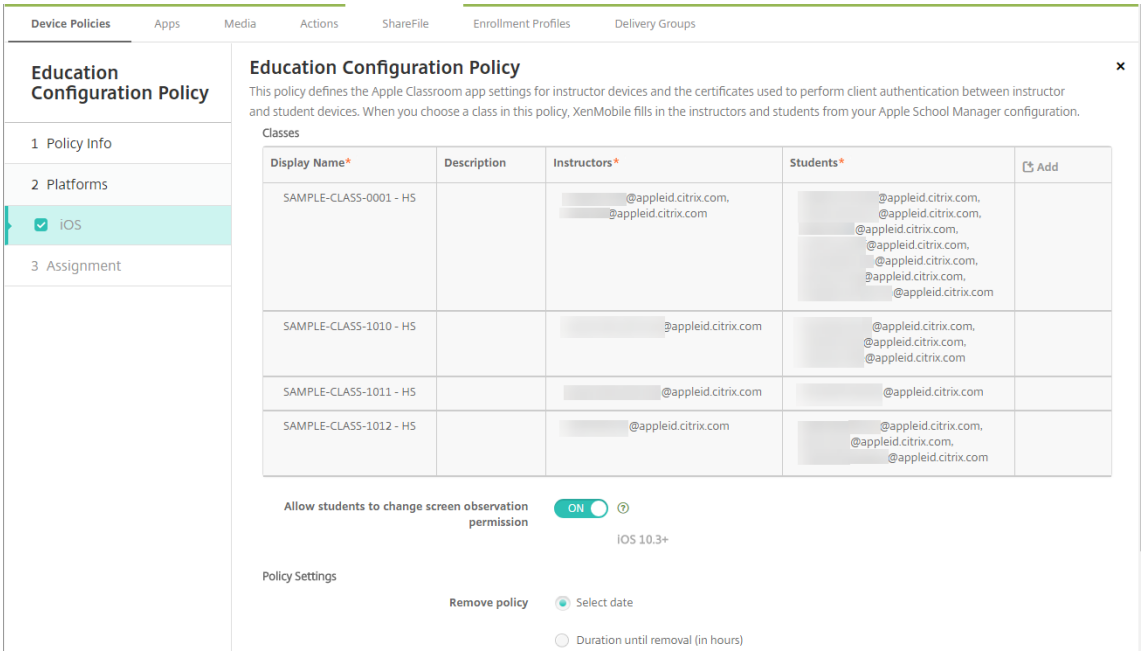
1. 教育の構成ポリシーを追加して、［追加］ をクリックします。



2. [表示名] 一覧をクリックします。接続した Apple School Manager アカウントから取得したクラスの一覧が表示されます。



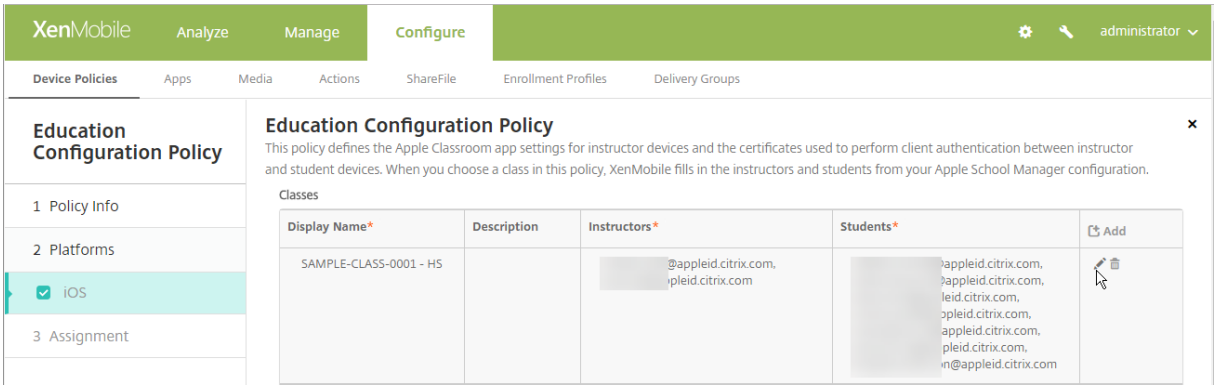
[表示名] からクラスを選択すると、XenMobile によって講師と生徒が入力されます。引き続きクラスを追加します。



ポリシーのクラス情報を編集するには

クラスに説明を加えることができます（クラスルームアプリの「表示名」）。また、講師や生徒を追加したり削除したりすることもできます。XenMobile Server では、このような変更は Apple School Manager アカウントに保存されません。詳しくは、「Apple Education 機能との統合」の「講師、生徒、クラスのデータ管理」を参照してください。

編集するクラスの ［追加］ 列の上にマウスポインターを置き、鉛筆アイコンをクリックします。



ポリシーからクラスを削除するには、削除するクラスの ［追加］ 列の上にマウスポインタ ― を置き、ごみ箱アイコンをクリックします。

エンタープライズハブデバイスポリシー

October 25, 2019

Windows Phone のエンタープライズハブデバイスポリシーでは、エンタープライズハブの業務用ストアを通じてアプリを配布できます。

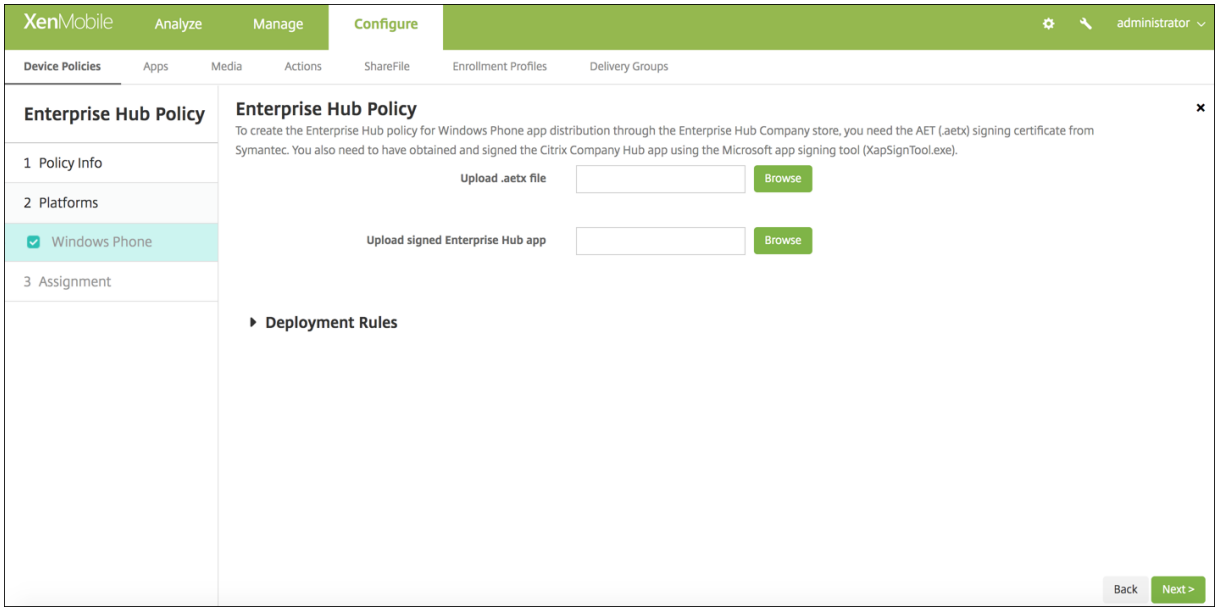
このポリシーを作成するには以下が必要です。

- DigiCert からの AET（.aetx）署名証明書
- Microsoft のアプリ署名ツール（XapSignTool.exe）を使用して署名された Citrix Company Hub アプリ

> 注：
>
> XenMobile では、Windows Phone Secure Hub の 1 つのモードについて、1 つの Enterprise Hub ポリシーだけがサポートされています。たとえば、Windows Phone Secure Hub for XenMobile Enterprise Edition をアップロードするために、複数の Enterprise Hub ポリシーをさまざまなバージョンの Work Home for XenMobile Enterprise Edition 用に作成する必要はありません。デバイスの登録中に最初のエンタープライズハブポリシーを展開するだけです。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Phone の設定



- **.aetx** ファイルのアップロード： ［参照］ をクリックして.aetx ファイルの場所に移動し、そのファイルを選択します。
- 署名済みエンタープライズハブアプリをアップロード： ［参照］ をクリックしてエンタープライズハブアプリの場所へ移動し、そのアプリを選択します。

Exchange デバイスポリシー

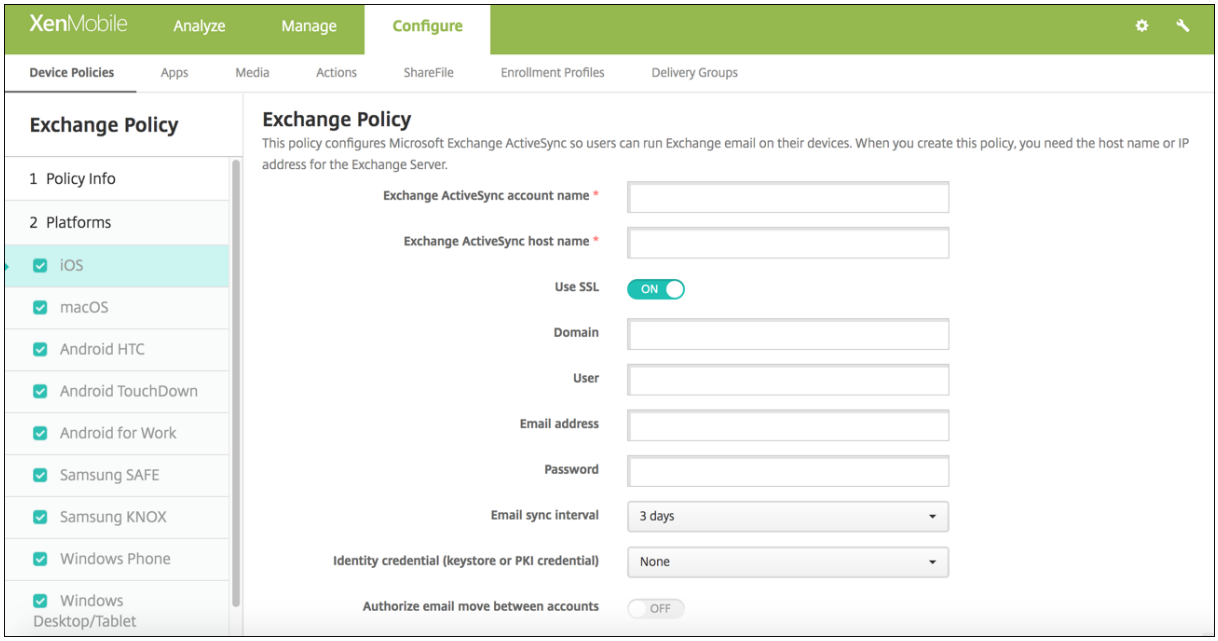
January 10, 2020

Exchange ActiveSync デバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchange でホストされている会社のメールにアクセスできるようにすることができます。iOS、macOS、Android HTC、Android TouchDown、Android Enterprise、Samsung SAFE、Samsung KNOX、Windows Phone、Windows タブレットに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、以下のセクションで説明しています。

このポリシーを作成するには、Exchange Server のホスト名または IP アドレスが必要です。ActiveSync の設定について詳しくは、Microsoft 社の記事「ActiveSync CSP」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

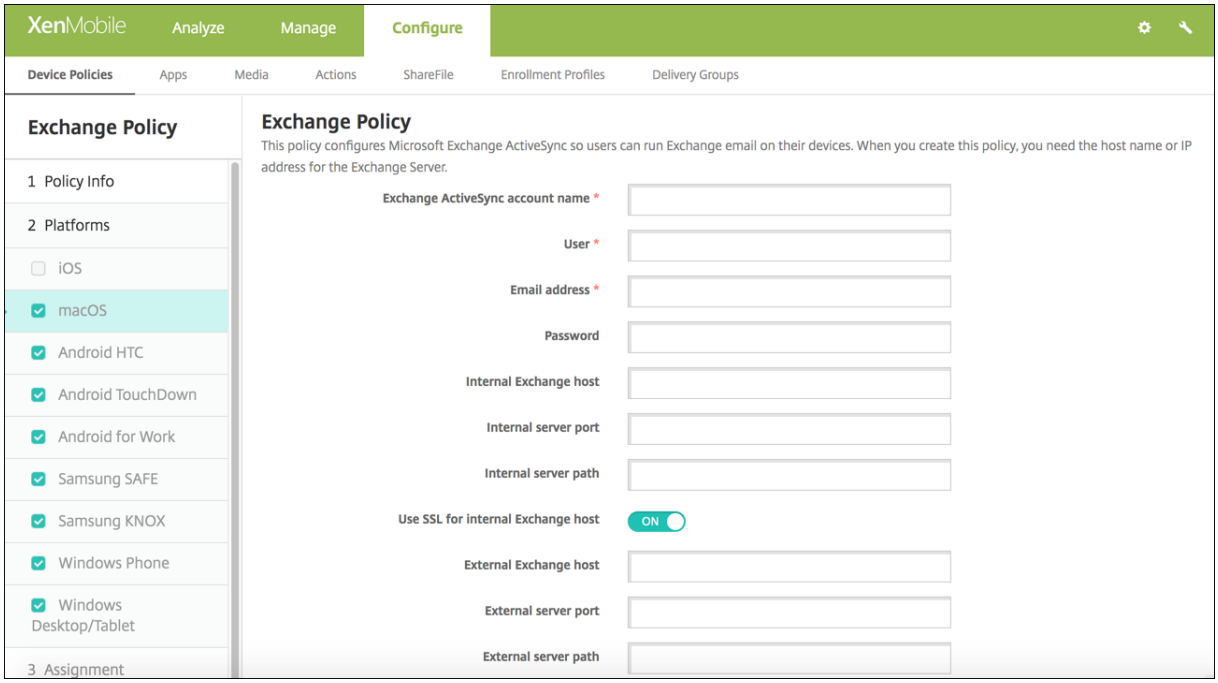


- **Exchange ActiveSync** のアカウント名： ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **Exchange ActiveSync** のホスト名： メールサーバーのアドレスを入力します。
- **SSL** を使用： ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］ です。
- ドメイン： Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。

- ユーザー: Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス: 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **OAuth** を使用: ［オン］ に設定すると、接続の認証で OAuth が使用されます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
- パスワード: 任意で、Exchange ユーザーアカウントのパスワードを入力します。この設定は、［**OAuth** を使用］ が ［オン］ の場合には表示されません。
- メールの同期間隔: 一覧から、メールを Exchange Server と同期する頻度を選択します。デフォルトは ［**3** 日］ です。
- **ID** 資格情報（キーストアまたは **PKI**）: XenMobile の ID プロバイダーを構成している場合、オプションとして、ボックスの一覧で ID 資格情報を選択します。このフィールドは、Exchange でクライアント証明書認証が必要な場合にのみ必要です。デフォルトは ［なし］ です。
- アカウント間でのメールの移動を承認: ユーザーが電子メールをこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。デフォルトは ［オフ］ です。
- メールアプリからのみメールを送信: ユーザーの電子メールの送信を iOS メールからのみに制限するかどうかを選択します。デフォルトは ［オフ］ です。
- メールの最近の同期を無効化: ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは ［オフ］ です。このオプションは iOS 6.0 以降にのみ適用されます。
- **S/MIME** 署名の有効化: アカウントで S/MIME 署名をサポートするかどうかを指定します。デフォルトは ［オン］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - 署名 **ID** 資格情報: 使用する署名資格情報を選択します。
  - ユーザーに **S/MIME** 署名設定の上書きを許可: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - ユーザーに **S/MIME** 署名証明書 **UUID** の上書きを許可: ［オン］ に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
- **S/MIME** 暗号化の有効化: このアカウントで S/MIME 暗号化をサポートするかどうかを選択します。デフォルトは ［オフ］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - 暗号化 **ID** 資格情報: 使用する暗号化資格情報を選択します。
  - メッセージごとの **S/MIME** 切り替えの有効化: ［オン］ に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］ です。
  - ユーザーに **S/MIME** 暗号化のデフォルト設定の上書きを許可: ［オン］ に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - ユーザーに **S/MIME** 暗号化証明書 **UUID** の上書きを許可: ［オン］ に設定した場合、ユーザーはデバ

イスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。

macOS 設定

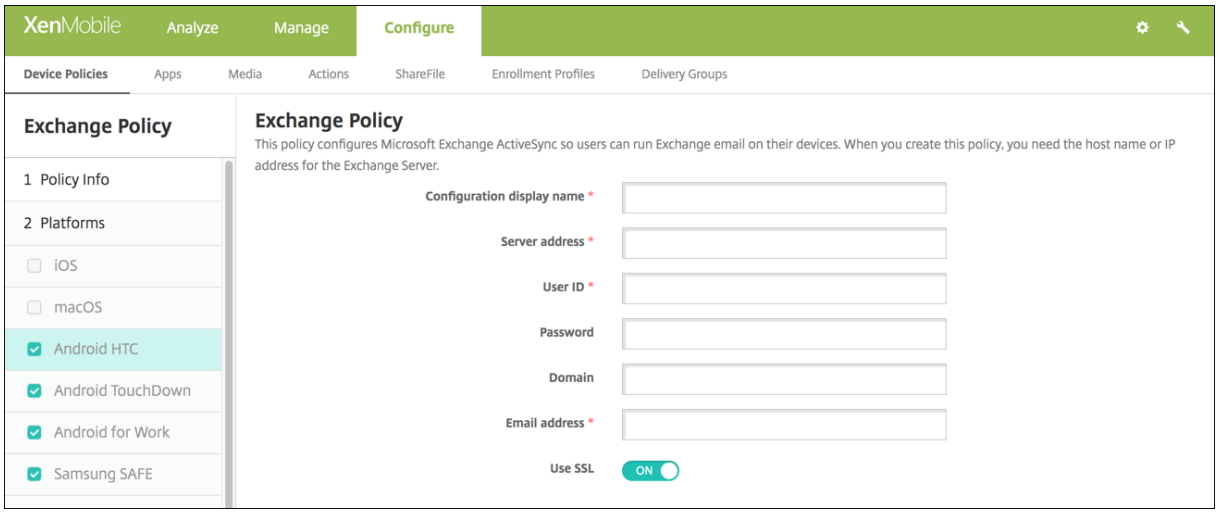


- **Exchange ActiveSync** のアカウント名： ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- ユーザー： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス： 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **OAuth** を使用： ［オン］ に設定すると、接続の認証で OAuth が使用されます。デフォルトは ［オフ］ です。このオプションは macOS 10.14 以降に適用されます。
- **OAuth** サインイン **URL**： AutoDiscovery サービスを使用しない場合に OAuth 認証用に Web ビューで読み込むサインイン URL を指定します。このフィールドは、［**OAuth** を使用］ を ［オン］ に設定すると表示されます。
- パスワード： 任意で、Exchange ユーザーアカウントのパスワードを入力します。この設定は、［**OAuth** を使用］ が ［オン］ の場合には表示されません。
- 内部 **Exchange** ホスト：Exchange のホスト名を内部と外部で別のものにする場合、任意で内部の Exchange ホスト名を入力します。
- 内部サーバーポート： Exchange のサーバーポートを内部と外部で別のものにする場合、任意で内部の Exchange サーバーのポート番号を入力します。
- 内部サーバーパス：Exchange のサーバーパスを内部と外部で別のものにする場合、任意で内部の Exchange

サーバーパスを入力します。

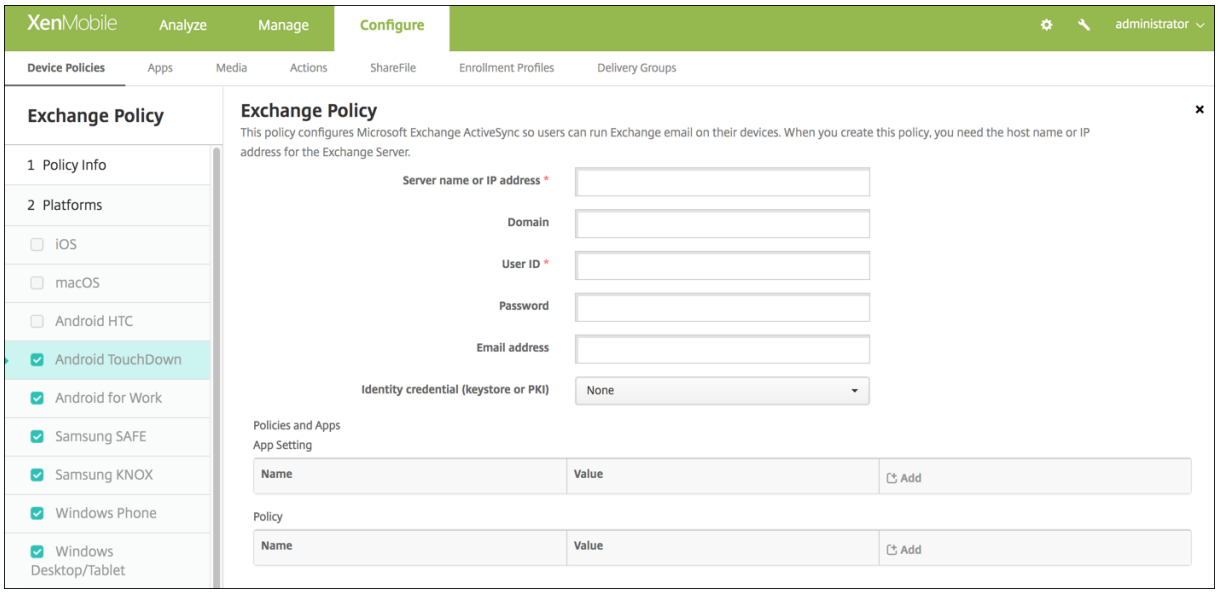
- 内部 **Exchange** ホストに **SSL** を使用： ユーザーのデバイスと内部の Exchange ホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］ です。
- 外部 **Exchange** ホスト：Exchange のホスト名を内部と外部で別のものにする場合、任意で外部の Exchange ホスト名を入力します。
- 外部サーバーポート： Exchange のサーバーポートを内部と外部で別のものにする場合、任意で外部の Exchange サーバーのポート番号を入力します。
- 外部サーバーパス：Exchange のサーバーパスを内部と外部で別のものにする場合、任意で外部の Exchange サーバーパスを入力します。
- 外部 **Exchange** ホストに **SSL** を使用： ユーザーのデバイスと外部の Exchange ホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］ です。
- メールドロップを許可：ユーザーが 2 台の Mac 間で、既存のネットワークに接続することなくワイヤレスでファイルを共有できるようにするかどうかを選択します。デフォルトは ［オフ］ です。

Android HTC の設定



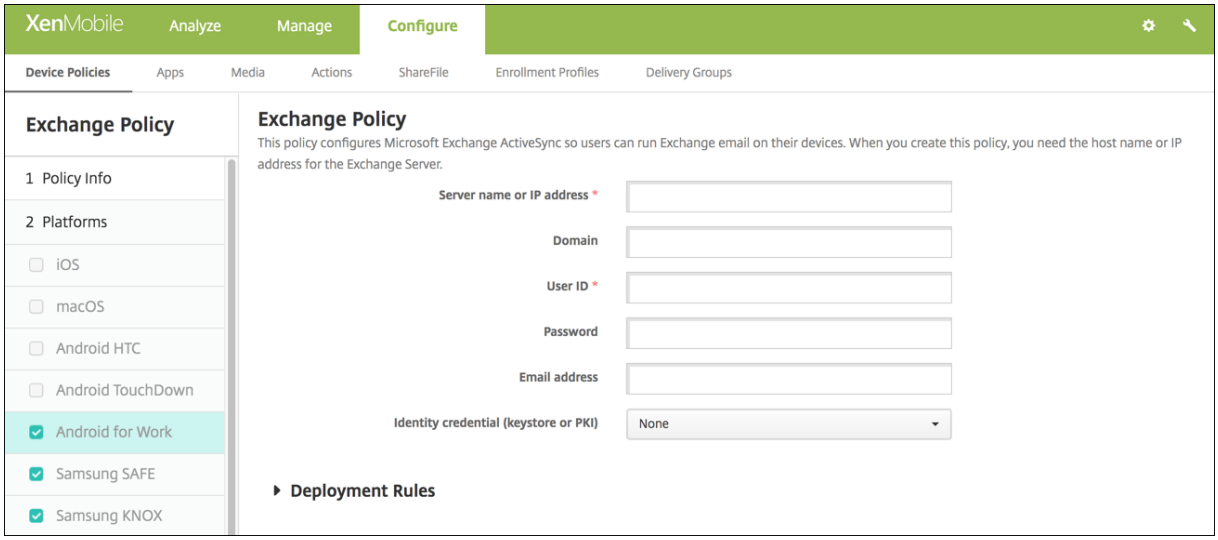
- 構成表示名： ユーザーのデバイスで表示される、このポリシーの名前を入力します。
- サーバーアドレス： Exchange Server のホスト名または IP アドレスを入力します。
- ユーザー **ID**： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- パスワード： 任意で、Exchange ユーザーアカウントのパスワードを入力します。
- ドメイン： Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。
- メールアドレス： 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **SSL** を使用： ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］ です。

Android TouchDown の設定



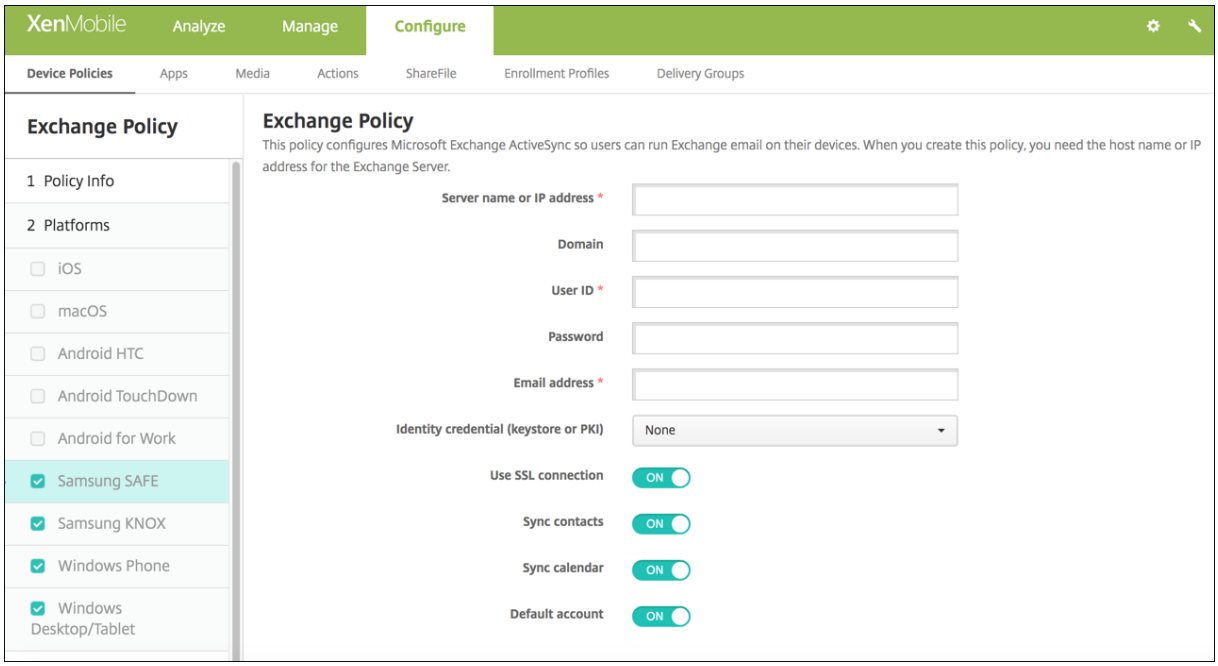
- サーバー名または **IP** アドレス： Exchange Server のホスト名または IP アドレスを入力します。
- ドメイン： Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー **ID**： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- パスワード： 任意で、Exchange ユーザーアカウントのパスワードを入力します。
- メールアドレス： 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **ID** 資格情報（キーストアまたは **PKI**）： XenMobile の ID プロバイダーを構成している場合、オプションとして、ボックスの一覧で ID 資格情報を選択します。このフィールドは、Exchange でクライアント証明書認証が必要な場合にのみ必要です。デフォルトは ［なし］ です。
- アプリ設定： オプションで、このポリシーの TouchDown アプリ設定を追加します。
- ポリシー： オプションで、このポリシーの TouchDown ポリシーを追加します。

Android Enterprise



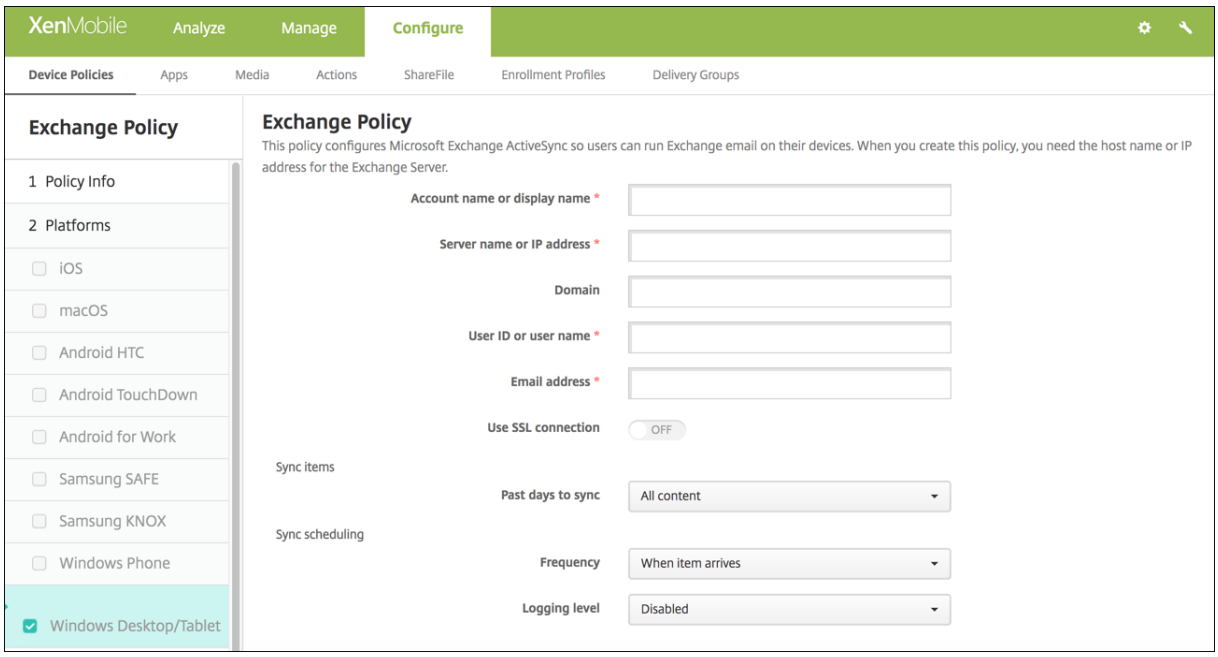
- サーバー名または **IP** アドレス： Exchange Server のホスト名または IP アドレスを入力します。
- ドメイン： Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー **ID**： Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- パスワード： 任意で、Exchange ユーザーアカウントのパスワードを入力します。
- メールアドレス： 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **ID** 資格情報（キーストアまたは **PKI**）： XenMobile の ID プロバイダーを構成している場合、オプションとして、ボックスの一覧で ID 資格情報を選択します。このフィールドは、Exchange でクライアント証明書認証が必要な場合にのみ必要です。デフォルトは ［なし］ です。

Samsung SAFE および Samsung KNOX の設定



- サーバー名または **IP** アドレス: Exchange Server のホスト名または IP アドレスを入力します。
- ドメイン: Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー **ID**: Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- パスワード: 任意で、Exchange ユーザーアカウントのパスワードを入力します。
- メールアドレス: 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **ID** 資格情報（キーストアまたは **PKI**）: XenMobile の ID プロバイダーを構成している場合、オプションとして、ボックスの一覧で ID 資格情報を選択します。このフィールドは、Exchange でクライアント証明書認証が必要な場合にのみ必要です。
- **SSL** 接続を使用: ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは ［オン］ です。
- 連絡先を同期: デバイスと Exchange Server の間でユーザーのアドレス帳を同期できるようにするかどうかを選択します。デフォルトは ［オン］ です。
- カレンダーを同期: デバイスと Exchange Server の間でユーザーのカレンダーを同期できるようにするかどうかを選択します。デフォルトは ［オン］ です。
- 優先アカウントにする: ユーザーの Exchange アカウントをデバイスから送信するメールのデフォルトにするかどうかを選択します。デフォルトは ［オン］ です。

Windows Phone および **Windows** デスクトップ/タブレットの設定



> 注:
>
> このポリシーを使ってユーザーパスワードを設定することはできません。ユーザーはポリシーがプッシュされた後に、デバイスでパラメーターを設定する必要があります。

- アカウント名または表示名: Exchange ActiveSync アカウント名を入力します。
- サーバー名または **IP** アドレス: Exchange Server のホスト名または IP アドレスを入力します。
- ドメイン: Exchange Server があるドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用して、ユーザーのドメイン名を自動的に検索することができます。
- ユーザー **ID** またはユーザー名: Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用して、ユーザーの名前を自動的に検索することができます。
- メールアドレス: 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **SSL** 接続を使用: ユーザーのデバイスと Exchange Server 間の接続をセキュリティで保護するかどうかを選択します。デフォルトは [オフ] です。
- 同期する期間: ボックスの一覧で、デバイス上のすべての内容を Exchange Server と過去にさかのぼって同期する日数を選択します。デフォルトは [すべての内容] です。
- 頻度: ボックスの一覧で、Exchange Server からデバイスへ送信されるデータの同期に使用するスケジュールを選択します。デフォルトは [受信したとき] です。
- ログレベル: ボックスの一覧で、[無効]、[基本]、または [詳細] を選択して、Exchange のアクティビティをログ記録する詳細レベルを指定します。デフォルトは [無効] です。

ファイルデバイスポリシー

August 22, 2019

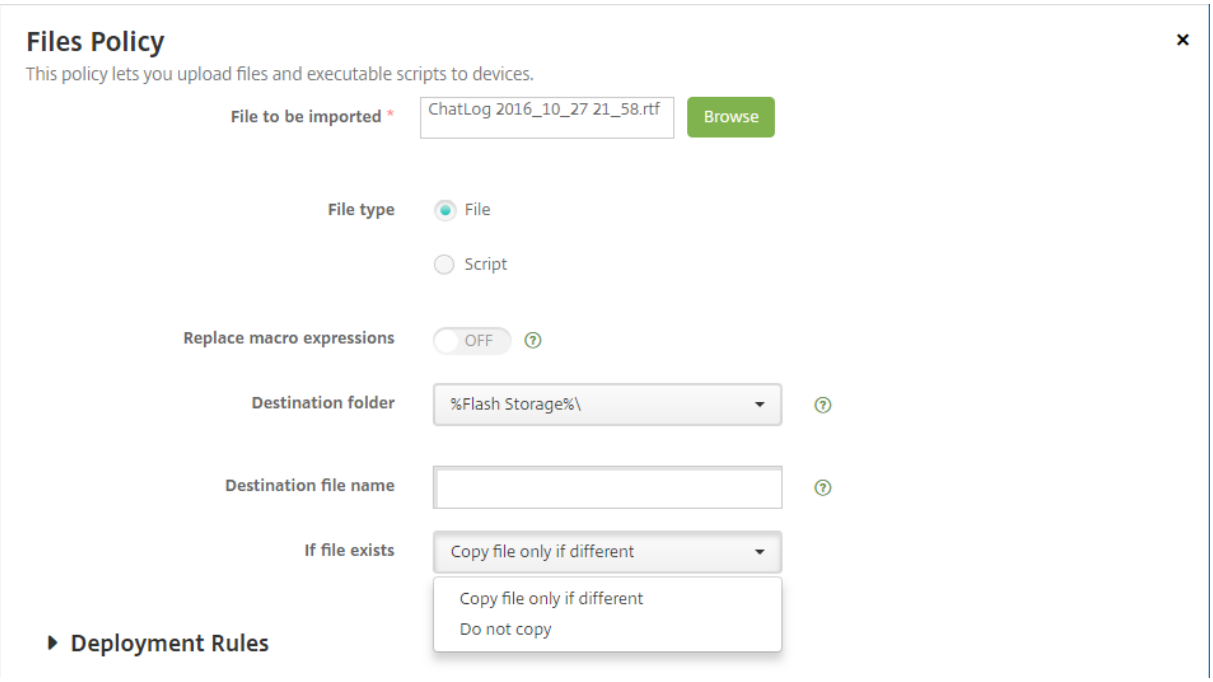
ユーザーに対して特定の機能を実行するスクリプトファイル、または Android デバイスユーザーがデバイスでアクセスできるドキュメントファイルを、XenMobile に追加できます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。たとえば、Android ユーザーが会社のドキュメントまたは.pdf ファイルを受け取るようにする場合は、ファイルをデバイスに展開し、ユーザーにファイルがある場所を知らせます。

このポリシーで追加できるファイルの種類は次のとおりです。

- テキストベースのファイル（.xml、.html、.py など）
- ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル
- Windows Mobile および Windows CE のみ: MortScript で作成されたスクリプトファイル

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android Enterprise の設定



- インポートするファイル: インポートするファイルを選択するには、［参照］をクリックしてインポートするファイルの場所へ移動します。
- ファイルタイプ: ［ファイル］ または ［スクリプト］ を選択します。［スクリプト］ を選択すると、［今すぐに実行］ が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。［今すぐに実行］ のデフォルトは ［オフ］ です。

- マクロ表現を置換: スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。マクロ構文については、「マクロ」を参照してください。デフォルトは ［オフ］です。
- ターゲットフォルダー: 一覧からアップロードしたファイルを格納する場所を選択するか、［新規追加］をクリックして、一覧にない場所を選択します。任意のパス識別子の始まりとしてマクロ%XenMobile Folder%\または%Flash Storage%\を使用することができます。
- 保存先ファイル名: 任意です。デバイスに展開する前にファイル名を変更する必要がある場合は、ファイル名を入力します。
- ファイルが存在する場合: 一覧で、既存のファイルをコピーするかどうかを選択します。デフォルトは、［異なる場合にのみファイルをコピーする］です。

Android の設定

- インポートするファイル: ［参照］ をクリックしてインポートするファイルの場所へ移動し、対象のファイルを選択します。
- ファイルタイプ: ［ファイル］ または ［スクリプト］ を選択します。［スクリプト］ を選択すると、［今すぐに実行］ が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは ［オフ］ です。
- マクロ表現を置換: スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは ［オフ］ です。
- ターゲットフォルダー: 一覧からアップロードしたファイルを格納する場所を選択するか、［新規追加］をクリックして、一覧にない場所を選択します。また、パス識別子の先頭に%XenMobile Folder%\または%Flash Storage%\というマクロを使用することもできます。
- ターゲットファイル名: オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- 異なる場合にのみファイルをコピーする: 一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。

Windows Mobile/CE の設定

- インポートするファイル: ［参照］をクリックしてインポートするファイルの場所へ移動し、対象のファイルを選択します。
- ファイルタイプ: ［ファイル］ または ［スクリプト］ を選択します。［スクリプト］ を選択すると、［今すぐに実行］ が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは ［オフ］ です。
- マクロ表現を置換: スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは ［オフ］ です。

- ターゲットフォルダー: 一覧からアップロードしたファイルを格納する場所を選択するか、［新規追加］ をクリックして、一覧にない場所を選択します。また、パス識別の先頭に以下のマクロを使用することもできます。
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- ターゲットファイル名: オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- 異なる場合にのみファイルをコピーする: 一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。
- 読み取り専用ファイル: ファイルを読み取り専用にするかどうかを選択します。デフォルトは ［オフ］ です。
- 非表示のファイル: ファイルをファイル一覧で非表示にするかどうかを選択します。デフォルトは［オフ］です。

FileVault デバイスポリシー

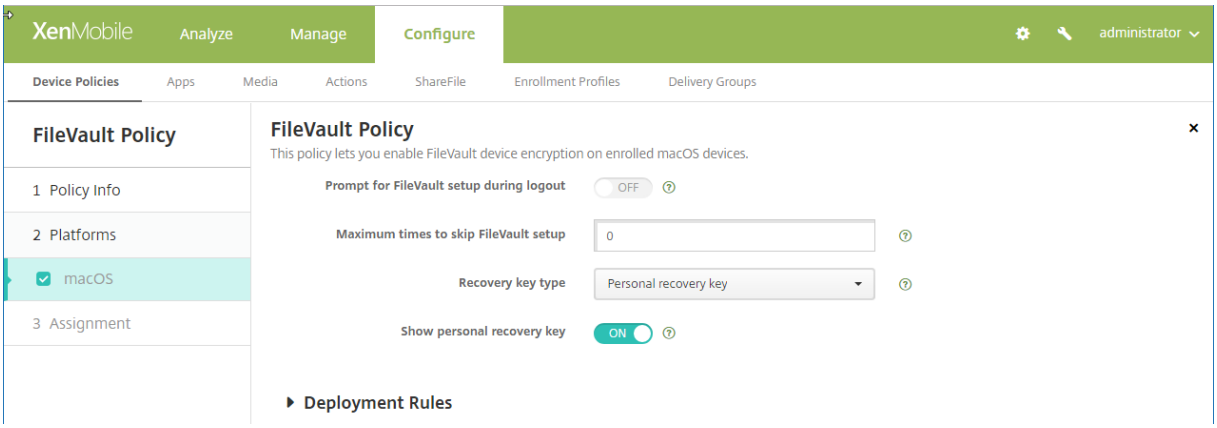
January 10, 2020

macOS の FileVault ディスク暗号化機能を使用すると、コンテンツを暗号化することでシステムボリュームを保護できます。MacOS デバイスで FileVault が有効になっていると、ユーザーはデバイスが起動するたびにアカウントパスワードでログインします。ユーザーがパスワードをなくした場合は、復元キーを使用すると、ディスクのロックを解除してパスワードをリセットできます。

XenMobile デバイスポリシー［FileVault］では、FileVault のユーザー設定画面を有効にし、復元キーなどの設定を構成します。FileVault について詳しくは、Apple のサポートサイト（https://support.apple.com）を参照してください。

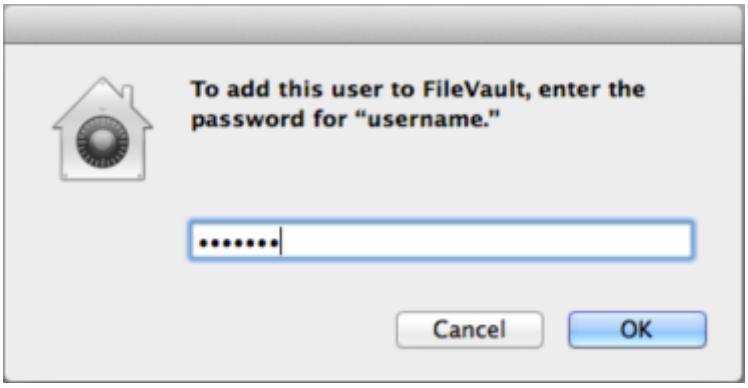
FileVault ポリシーを追加するには、［構成］**>**［デバイスポリシー］ の順に選択します。

macOS 設定

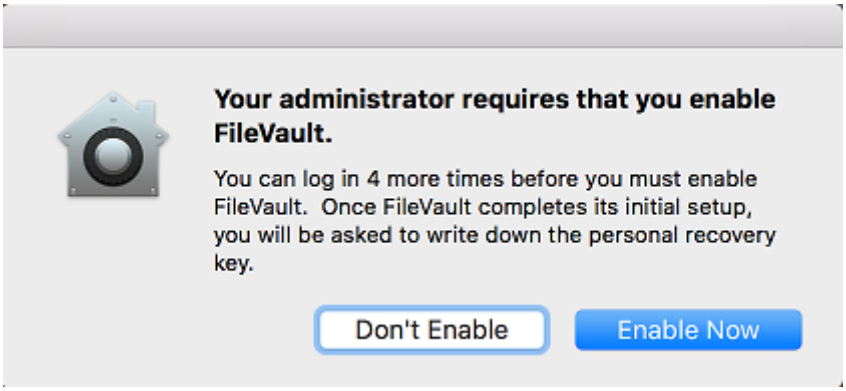


- ログオン時に **FileVault** のセットアップを要求: ［オン］ の場合、［**FileVault** のセットアップをスキップする最大回数］ で指定されている次の N 回目のログアウト時に、FileVault を有効にするようユーザーにメッセージが表示されます。［オフ］ の場合、FileVault のパスワードプロンプトは表示されません。

この設定を［オン］にして FileVault ポリシーを展開すると、ユーザーがデバイスからサインオフしたときに、次の画面が表示されます。画面には、サインオフする前に FileVault を有効にするオプションが表示されます。

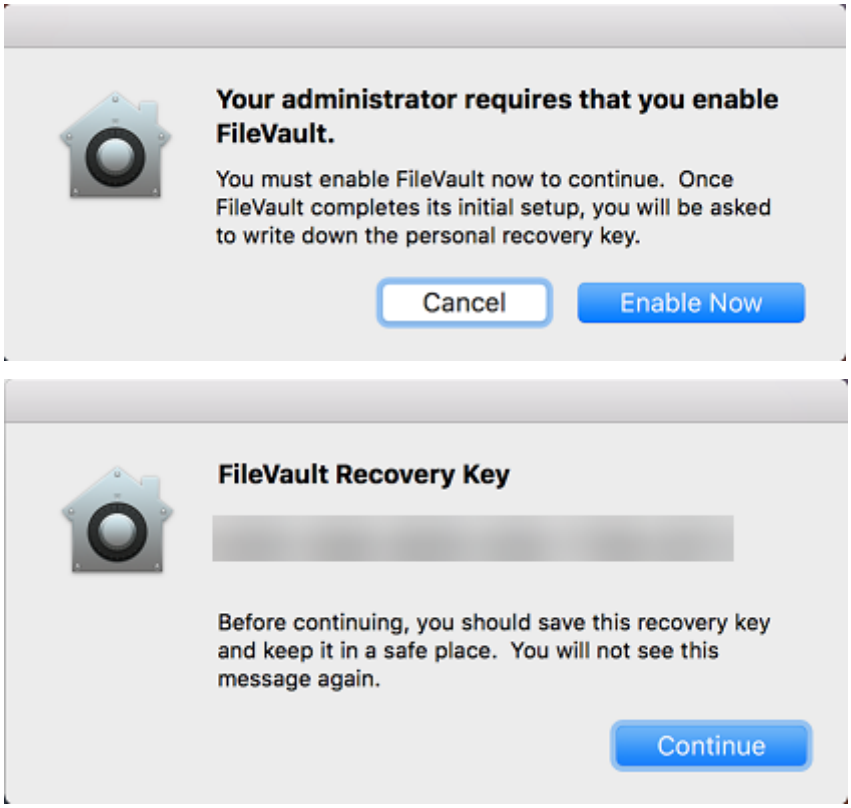


［**FileVault** のセットアップをスキップする最大回数］ の値が 0 以外の場合、この設定をオフにして FileVault ポリシーを展開すると、ユーザーがサインオンした時に、次の画面が表示されます。



［**FileVault** のセットアップをスキップする最大回数］ の値が 0 の場合、またはユーザーがセットアップを最大回数

スキップした場合は、次の画面が表示されます。



フォントデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、追加フォントを iOS デバイスおよび macOS デバイスに追加することができます。フォントは TrueType（.ttf）または OpenType（.oft）である必要があります。フォントコレクション（.ttc または.otc）はサポートされません。

iOS の場合、このポリシーは iOS 7.0 以降にのみ適用されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- ユーザーに表示される名前： ユーザーのフォント一覧に表示される名前を入力します。
- フォントファイル： ［参照］ をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、対象のファイルを選択します。

macOS 設定

- ユーザーに表示される名前: ユーザーのフォント一覧に表示される名前を入力します。
- フォントファイル: ［参照］ をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、対象のファイルを選択します。

ホーム画面のレイアウトに関するデバイスポリシー

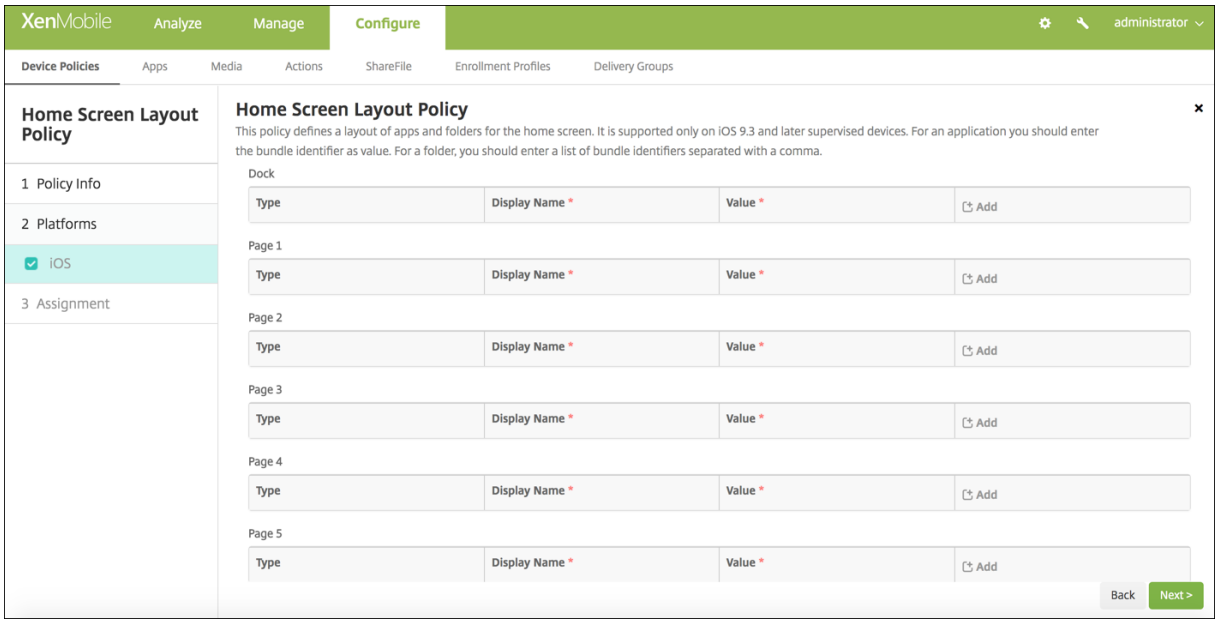
January 10, 2020

iOS のホーム画面のアプリやフォルダーのレイアウトを指定できます。ホーム画面のレイアウトに関するデバイスポリシーは、iOS 9.3 以降の管理対象デバイス用です。

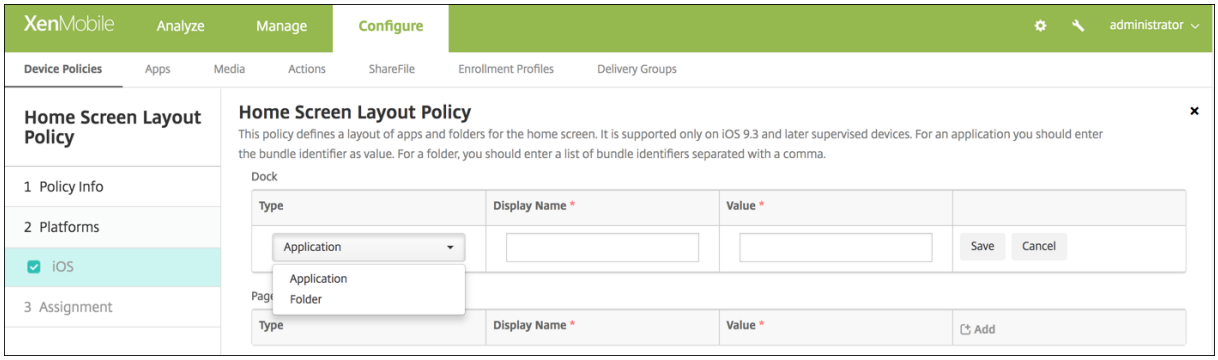
> 重要:
>
> 複数のホーム画面のレイアウトに関するポリシーを 1 台のデバイスに展開すると、デバイスで iOS エラーが発生します。この制限は、この XenMobile ポリシーまたは Apple Configurator を使用してホーム画面を定義するかどうかに関係なく適用されます。

このポリシーを追加または構成するには、［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- 構成する各画面の領域（ドックやページ **1** など）で、 ［追加］ をクリックします。
- **Type**: ［**Application**］ または ［**Folder**］ のいずれかを選択します。



- 表示名： アプリまたはフォルダーのホーム画面に表示される名前。
- 値： アプリの場合は、バンドル識別子。フォルダの場合は、コンマで区切られたバンドル識別子のリスト。

iOS および macOS プロファイルのインポートデバイスポリシー

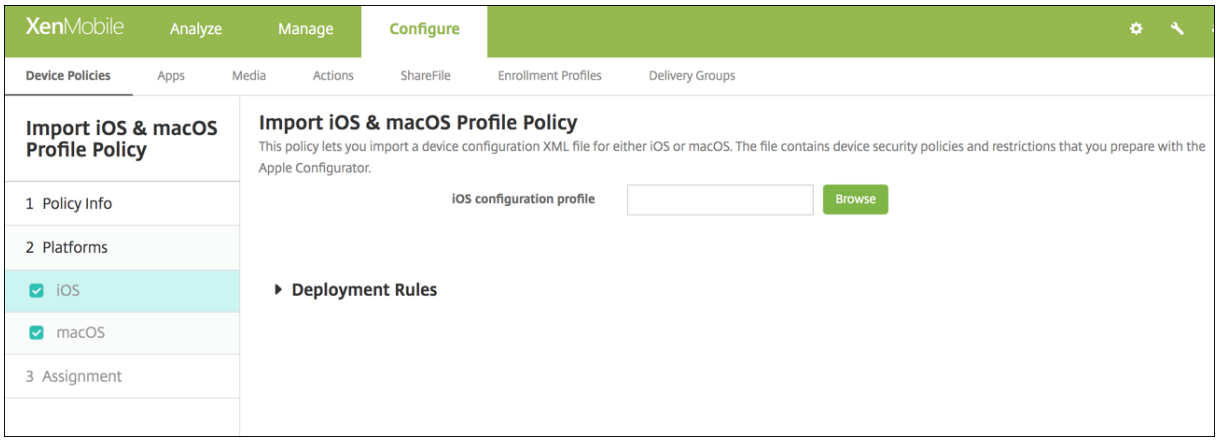
August 22, 2019

iOS および macOS デバイス用のデバイス構成 XML ファイルを XenMobile にインポートできます。XML ファイルには、Apple Configurator を使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。

この記事で説明するように、Apple Configurator を使用して iOS デバイスを Supervised モードにできます。Apple Configurator の使用による構成ファイルの作成について詳しくは、Apple の「Configurator サポート」を参照してください。

このポリシーを追加または構成するには、［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および macOS の設定



- **iOS** 構成プロファイルまたは **macOS** 構成プロファイル： ［参照］ をクリックしてインポートする構成ファイルの場所へ移動し、対象ファイルを選択します。

Apple Configurator を使用して **iOS** デバイスを **Supervised** モードにする

Apple Configurator を使用するには、Apple コンピューターで macOS 10.7.2 以降を実行している必要があります。

> 重要:
>
> デバイスを Supervised モードにすると、特定のバージョンの iOS がデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリがデバイスから完全に消去されます。

1. iTunes から Apple Configurator をインストールします。
2. iOS デバイスを Apple コンピューターに接続します。
3. Apple Configurator を起動します。監視の準備が整っているデバイスがあることが Configurator に表示されます。
4. デバイスの監視の準備を行うには:
   a) ［監視］ コントロールを ［オン］ に切り替えます。構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。
   b) 必要に応じてデバイスの名前を指定します。
   c) 最新バージョンの iOS をインストールする場合、［iOS］ボックスの一覧で ［最新］ を選択します。
5. デバイスの監視の準備が整ったら、［準備］ をクリックします。

キオスクデバイスポリシー

September 24, 2019

キオスクポリシーでは、次のように、実行可能なアプリを制限することで、デバイスをキオスクモードに制限できます。

- Samsung SAFE デバイスの場合: 特定のアプリのみを使用するように指定できます。このポリシーは、特定の種類またはクラスのアプリのみを実行するように設計されているコーポレートデバイスで役立ちます。また、このポリシーを使用して、デバイスがキオスクモードのときのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。
- Android Enterprise 専用デバイス（特定業務専用コーポレート所有（COSU）デバイスとも呼ばれる）の場合: アプリをホワイトリストに追加し、ロックタスクモードを設定できます。デフォルトでは、Secure Hub と Google Play サービスはホワイトリストに登録されています。

XenMobile が、キオスクモードでデバイスのどの部分がロックされるかを制御することはありません。ポリシーを展開した後、デバイスはキオスクモード設定を管理します。このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung SAFE デバイスをキオスクモードにするには

1. 「Samsung MDM ライセンスキーデバイスポリシー」の説明に従って、モバイルデバイス上で Samsung SAFE API キーを有効にします。この手順で、Samsung SAFE デバイス上でポリシーを有効にします。
2. 「Firebase Cloud Messaging」の説明に従って、Android デバイスで Firebase Cloud Messaging を有効にします。この手順で、Android デバイスを XenMobile に接続し直すことができます。
3. 次のセクションの説明に従って、キオスクデバイスポリシーを追加します。
4. 適切なデリバリーグループに、それら 3 つのデバイスポリシーを割り当てます。他のポリシー（たとえばアプリインベントリ）をデリバリーグループに含めるかどうかを検討します。

   キオスクモードからデバイスを削除するには、［キオスクモード］ を ［無効化］ に設定したキオスクデバイスポリシーを作成します。デリバリーグループを更新して、キオスクモードを有効にしたキオスクポリシーを削除し、キオスクモードを無効にするキオスクポリシーを追加します。

キオスクデバイスポリシーを追加するには

キオスクモード用に指定したすべてのアプリが、ユーザーのデバイスに既にインストールされている必要があります。

一部のオプションは、Samsung モバイルデバイス管理（MDM）API 4.0 以降にのみ適用されます。

Samsung SAFE の設定

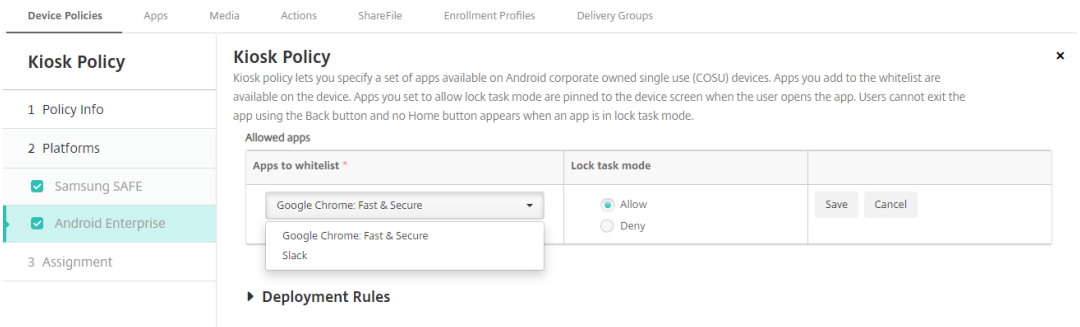
- キオスクモード: ［有効化］ または ［無効化］ を選択します。デフォルトは ［有効化］ です。［無効化］ をクリックすると、以下のオプションはすべて表示されなくなります。
- **Launcher** パッケージ: ユーザーがキオスクアプリを起動できる社内用ランチャーを開発した場合を除き、このフィールドは空白のままにしておくことをお勧めします。社内用ランチャーを使用する場合、ランチャーアプリケーションパッケージの完全な名前を入力します。
- 緊急電話番号: オプションで電話番号を入力します。紛失したデバイスの発見者が会社に連絡するときに、この番号を使用できます。MDM 4.0 以降にのみ適用されます。
- ナビゲーションバーを許可: キオスクモードのときに、ユーザーにナビゲーションバーを表示して使用できるようにするかどうかを選択します。MDM 4.0 以降にのみ適用されます。デフォルトは ［オン］ です。
- マルチウィンドウモードを許可: キオスクモードのときに、ユーザーが複数のウィンドウを使用できるようにするかどうかを選択します。MDM 4.0 以降にのみ適用されます。デフォルトは ［オン］ です。
- ステータスバーを許可: キオスクモードのときに、ユーザーにステータスバーを表示するかどうかを選択します。MDM 4.0 以降にのみ適用されます。デフォルトは ［オン］ です。
- システムバーを許可: キオスクモードのときに、ユーザーにシステムバーを表示するかどうかを選択します。デフォルトは ［オン］ です。
- タスクマネージャーを許可: キオスクモードのときに、ユーザーにタスクマネージャーを表示して使用できるようにするかどうかを選択します。デフォルトは ［オン］ です。

- 共通の **SAFE** パスコードの変更: この設定は［共通の SAFE パスコード］フィールドが不用意に変更されることを防ぐのに役立ちます。この設定が ［オフ］ の場合は、［共通の SAFE パスコード］フィールドを変更できません。デフォルトは ［オフ］ です。
- 共通の **SAFE** パスコード: すべての Samsung SAFE デバイスを対象とする汎用パスコードポリシーを設定した場合、オプションとして、このフィールドにパスコードを入力します。
- 壁紙
  - ホーム画面の壁紙を定義: キオスクモードのときに、ホーム画面でカスタムイメージを使用するかどうかを選択します。デフォルトは ［オフ］ です。
    * ホーム画面の画像: ［ホーム画面の壁紙を定義］ を有効にした場合、［参照］ をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
  - ロック画面の壁紙を定義: キオスクモードのときに、ロック画面でカスタムイメージを使用するかどうかを選択します。デフォルトは ［オフ］ です。MDM 4.0 以降にのみ適用されます。
    * ロック画面の画像: ［ロック画面の壁紙を定義］を有効にした場合、［参照］ をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
- アプリ: キオスクモードに追加するアプリごとに、［追加］ をクリックして以下の操作を行います:
  - 追加する新規アプリ: 追加するアプリの完全な名前を入力します。たとえば、「com.android.calendar」を入力すると、ユーザーが Android のカレンダーアプリを使用できます。
  - ［保存］ をクリックしてアプリを追加するか、［キャンセル］ をクリックしてアプリの追加を取り消します。

Android Enterprise の設定

アプリをホワイトリストに追加するには、［追加］ をクリックします。複数のアプリをホワイトリストに追加することができます。詳しくは、「Android Enterprise」を参照してください。

- ホワイトリストに追加するアプリ: ホワイトリストに追加するアプリのパッケージ名を入力するか、リストからアプリを選択します。
  - ［新規追加］ をクリックして、リストに表示することが承認されたアプリのパッケージ名を入力します。
  - リストから既存のアプリを選択します。このリストには、XenMobile にアップロードされているアプリが表示されます。デフォルトでは、Secure Hub と Google Play サービスはホワイトリストに登録されています。



- ロックタスクモード: ユーザーがアプリを起動した時にアプリをデバイス画面に固定するには、［許可］ を選

択します。アプリをデバイス画面に固定しない場合は、［禁止］ を選択します。デフォルトは ［許可］ です。

アプリがロックタスクモードになると、ユーザーがアプリを開いた時にデバイス画面にアプリが固定されます。［ホーム］ボタンは表示されず、［戻る］ボタンは無効になります。ユーザーは、サインアウトなど、アプリでプログラムされた操作を使用してアプリを終了します。

Android のランチャー構成デバイスポリシー

August 22, 2019

Citrix Launcher を使用すると、XenMobile によって展開された Android デバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix Launcher とランチャー構成デバイスポリシーは、Android Enterprise と互換性がありません。

Launcher 構成ポリシーを追加すると、次の Citrix Launcher 機能を制御できます。

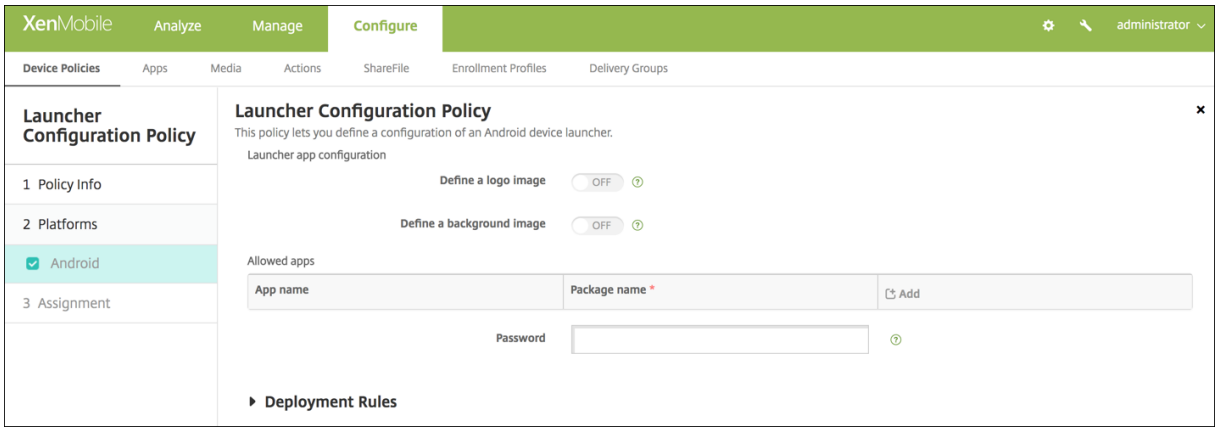
- ユーザーは管理者が指定したアプリにのみアクセスできるように Android デバイスを管理する。
- Citrix Launcher アイコンのカスタムロゴ画像と、Citrix Launcher のカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

Citrix Launcher を使用するとそれらのデバイスレベルの制約を適用できますが、ランチャーは、デバイス設定（たとえば、WiFi 設定、Bluetooth 設定、およびデバイスパスコード設定）への組み込みのアクセスを介して、必要な操作上の柔軟性をユーザーに付与します。Citrix Launcher は、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Citrix Launcher を展開すると、XenMobile がそれをインストールし、デフォルトの Android ランチャーを置換します。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android の設定



- ロゴ画像を定義: Citrix Launcher アイコンにカスタムロゴ画像を使用するかどうかを選択します。デフォルトは［オフ］です。
- ロゴ画像: ［ロゴ画像を定義］を有効にした場合、［参照］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、および GIF です。
- 背景画像を定義: Citrix Launcher の背景にカスタム画像を使用するかどうかを選択します。デフォルトは［オフ］です。
- 背景画像: ［背景画像を定義］を有効にした場合、［参照］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、および GIF です。
- 許可するアプリ: Citrix Launcher で許可するアプリごとに、［追加］をクリックして以下の操作を行います:
  - 追加する新規アプリ: 追加するアプリの完全な名前を入力します。たとえば、Android のカレンダーアプリの場合は「com.android.calendar」です。
  - ［保存］をクリックしてアプリを追加するか、［キャンセル］をクリックしてアプリの追加を取り消します。
- パスワード: Citrix Launcher を終了するために入力する必要があるパスワード。

LDAP デバイスポリシー

January 10, 2020

XenMobile で iOS デバイスの LDAP ポリシーを作成して、必要なアカウント情報など、使用する LDAP サーバーに関する情報を指定できます。また、LDAP サーバーの照会に使用する LDAP 検索ポリシーのセットが提供されます。

このポリシーを構成するには、LDAP ホスト名が必要です。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウントの説明: オプションで、アカウントの説明を入力します。
- アカウントユーザー名: オプションで、ユーザー名を入力します。
- アカウントパスワード: オプションで、パスワードを入力します。このフィールドは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP** ホスト名: LDAP サーバーのホスト名を入力します。このフィールドは必須です。
- **SSL** を使用: LDAP サーバーに対して SSL（Secure Socket Layer）接続を使用するかどうかを選択します。デフォルトは ［オン］ です。
- 検索設定: LDAP サーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも 1 つ入力してください。［追加］ をクリックして、以下の操作を行います。
  - 説明: 検索設定の説明を入力します。このフィールドは必須です。
  - スコープ: ［ベース］、［**1** レベル］、［サブツリー］ のいずれかを選択して、LDAP ツリーをどの深さまで検索するかを定義します。デフォルトは ［ベース］ です。
    * ［ベース］ を選択すると、［検索ベース］で参照されているノードを検索します。
    * ［**1** レベル］ を選択すると、［ベース］を選択した場合の検索対象ノードとその 1 つ下のレベルを検索します。
    * ［サブツリー］ を選択すると、［ベース］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - 検索ベース: 検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」です。このフィールドは必須です。
  - ［保存］ をクリックして検索設定を追加するか、［キャンセル］ をクリックして検索設定の追加を取り消します。
  - 追加する検索設定ごとに上記の手順を繰り返します。

macOS 設定

- アカウントの説明: オプションで、アカウントの説明を入力します。
- アカウントユーザー名: オプションで、ユーザー名を入力します。
- アカウントパスワード: オプションで、パスワードを入力します。このフィールドは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP** ホスト名: LDAP サーバーのホスト名を入力します。このフィールドは必須です。
- **SSL** を使用: LDAP サーバーに対して SSL（Secure Socket Layer）接続を使用するかどうかを選択します。デフォルトは ［オン］ です。
- 検索設定: LDAP サーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも 1 つ入力してください。［追加］ をクリックして、以下の操作を行います。
  - 説明: 検索設定の説明を入力します。このフィールドは必須です。

- スコープ: ［ベース］、［**1** レベル］、［サブツリー］ のいずれかを選択して、LDAP ツリーをどの深さまで検索するかを定義します。デフォルトは ［ベース］ です。
  - ［ベース］ を選択すると、［検索ベース］で参照されているノードを検索します。
  - ［**1** レベル］ を選択すると、［ベース］を選択した場合の検索対象ノードとその 1 つ下のレベルを検索します。
  - ［サブツリー］ を選択すると、［ベース］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
- 検索ベース: 検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」です。このフィールドは必須です。
- ［保存］ をクリックして検索設定を追加するか、［キャンセル］ をクリックして検索設定の追加を取り消します。
- 追加する検索設定ごとに上記の手順を繰り返します。

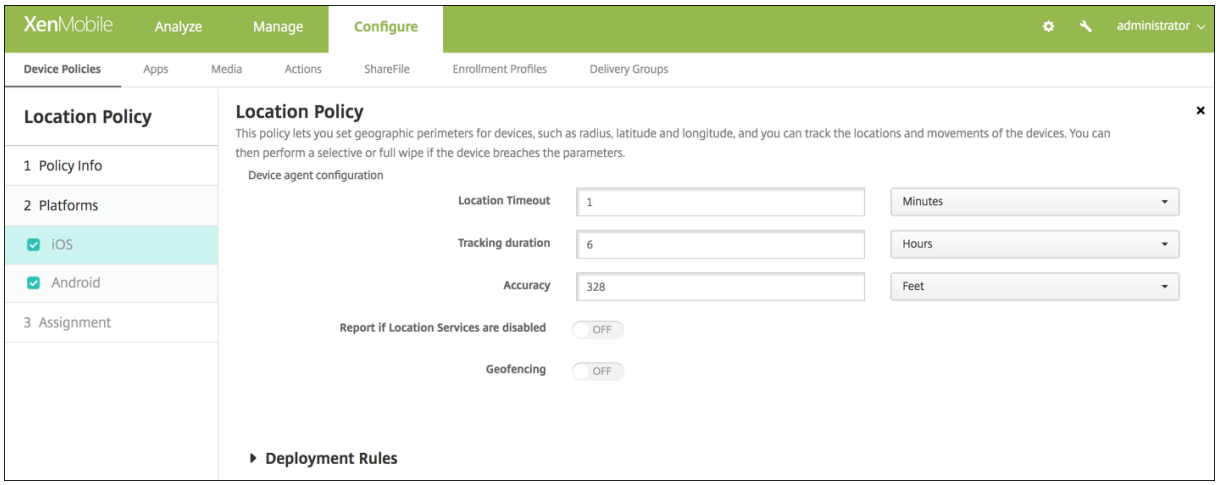
位置情報デバイスポリシー

January 10, 2020

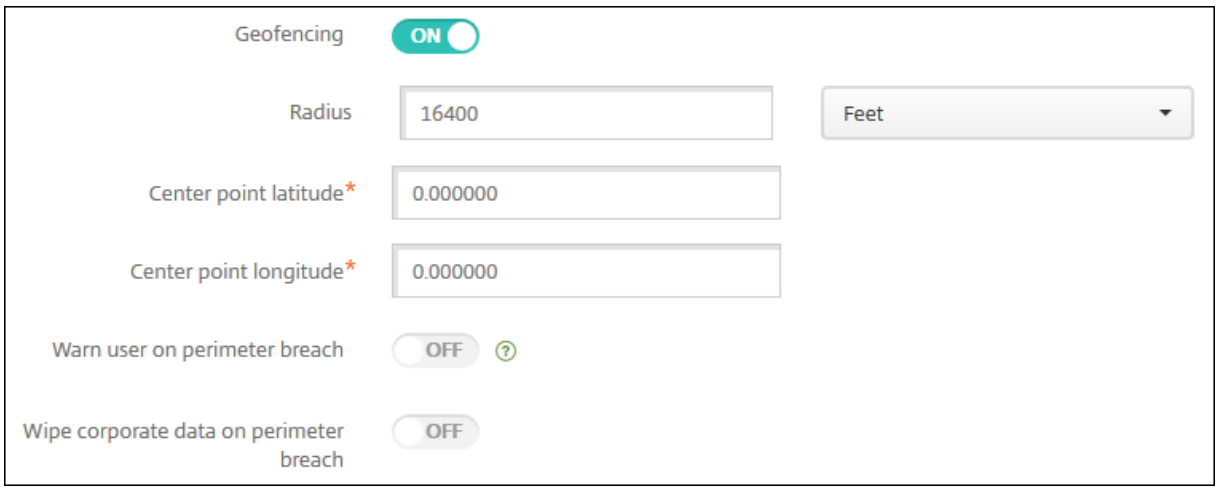
XenMobile で位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。定義された境界（ジオフェンスとも呼ばれます）の外にユーザーが出た場合、XenMobile では特定のアクションを実行できます。たとえば、定義された境界の外にユーザーが出た場合に、警告メッセージを表示するようにポリシーを構成できます。また、境界違反時にユーザーの企業データを即時または一定の時間が経過してからワイプするように構成することもできます。デバイスの追跡と検索の有効化などのセキュリティ操作について詳しくは、「セキュリティ操作」を参照してください。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- 位置タイムアウト： 数値を入力して、ボックスの一覧で ［秒］ または ［分］ を選択し、XenMobile がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、60 ～ 900 秒または 1 ～ 15 分です。デフォルトは 1 分です。
- 追跡期間： 数値を入力して、ボックスの一覧で ［時間］ または ［分］ を選択し、XenMobile がデバイスを追跡する時間を設定します。有効な値は、1 ～ 6 時間または 10 ～ 360 分です。デフォルトは 6 時間です。
- 精度： 数値を入力して、ボックスの一覧で ［メートル］、［フィート］、［ヤード］ のいずれかを選択し、XenMobile がデバイスを追跡する精度を設定します。有効な値は、10 ～ 5000 ヤード、10 ～ 5000m、または 30 ～ 15000 フィートです。デフォルトは 328 フィートです。
- 位置情報サービスが無効の場合は報告： GPS が無効になっている場合に、デバイスから XenMobile にレポートを送信するかどうかを選択します。デフォルトは ［オフ］ です。
- ジオフェンシング

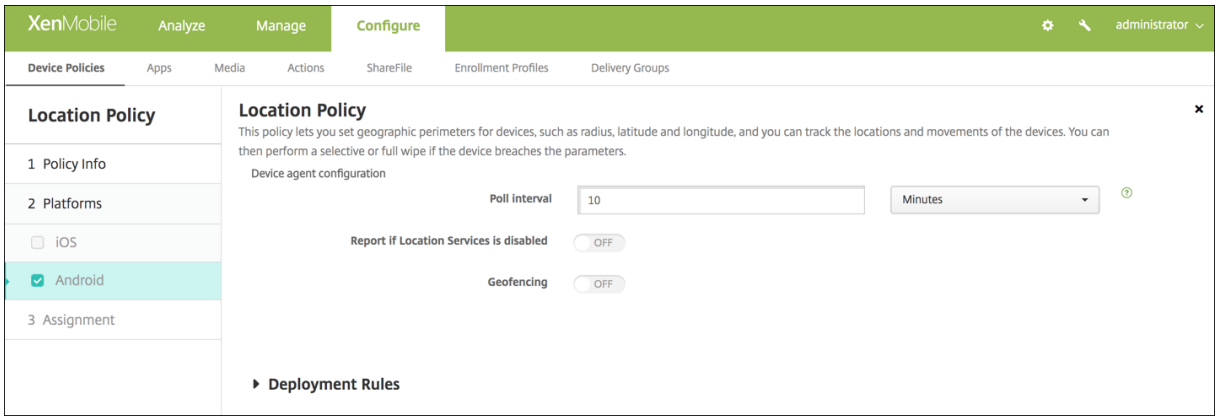


［ジオフェンシング］ を選択した場合は、次の設定を構成します。

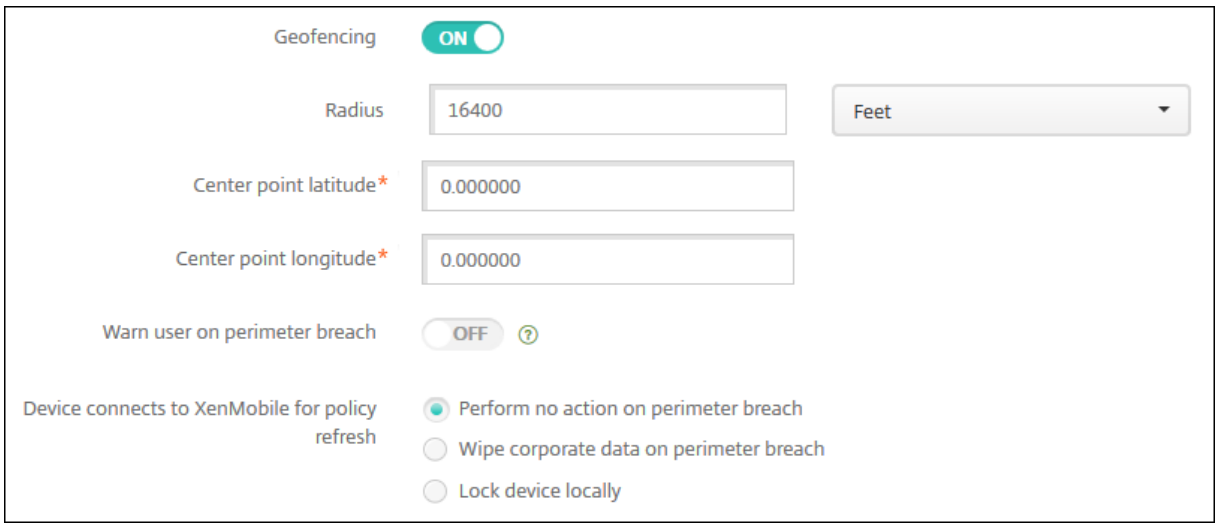
- 半径： 数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは 16,400 フィートです。有効な半径の値は次のとおりです。

  - 164 ～ 164000 フィート
  - 50 ～ 50000m
  - 54 ～ 54680 ヤード
  - 1 ～ 31 マイル
- 中心点の緯度： 緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。
- 中心点の経度： 経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告： 定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは ［オフ］ です。警告メッセージの表示に XenMobile への接続は必要ありません。
- 境界違反時に企業データをワイプ： ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にすると、［ローカルワイプを延期］ フィールドが表示されます。
  - 数値を入力し、一覧から ［秒］ または ［分］ を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが XenMobile によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは 0 秒です。

Android の設定



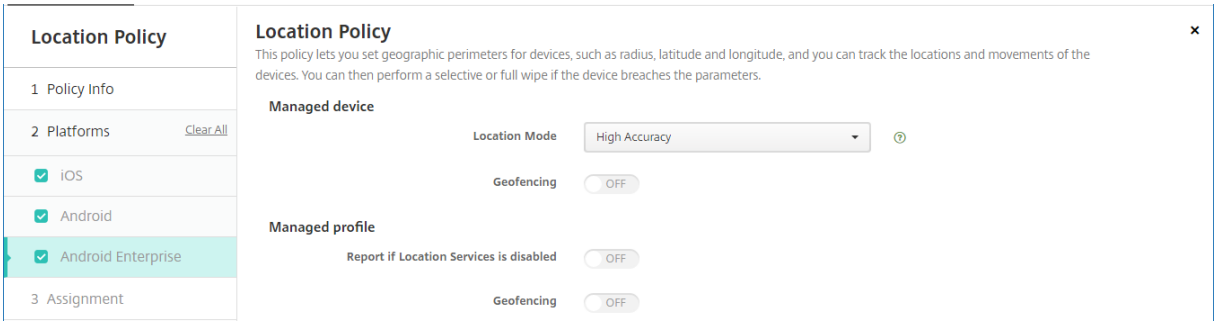
- ポーリング間隔：数値を入力して、ボックスの一覧で［分］、［時間］、［日］のいずれかを選択し、XenMobile がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1 ～ 1440 分、1 ～ 24 時間、または任意の日数です。デフォルトは 10 分です。この値を 10 分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- 位置情報サービスが無効の場合は報告： GPS が無効になっている場合に、デバイスから XenMobile にレポートを送信するかどうかを選択します。デフォルトは ［オフ］ です。
- ジオフェンシング



［ジオフェンシング］を選択した場合は、次の設定を構成します。

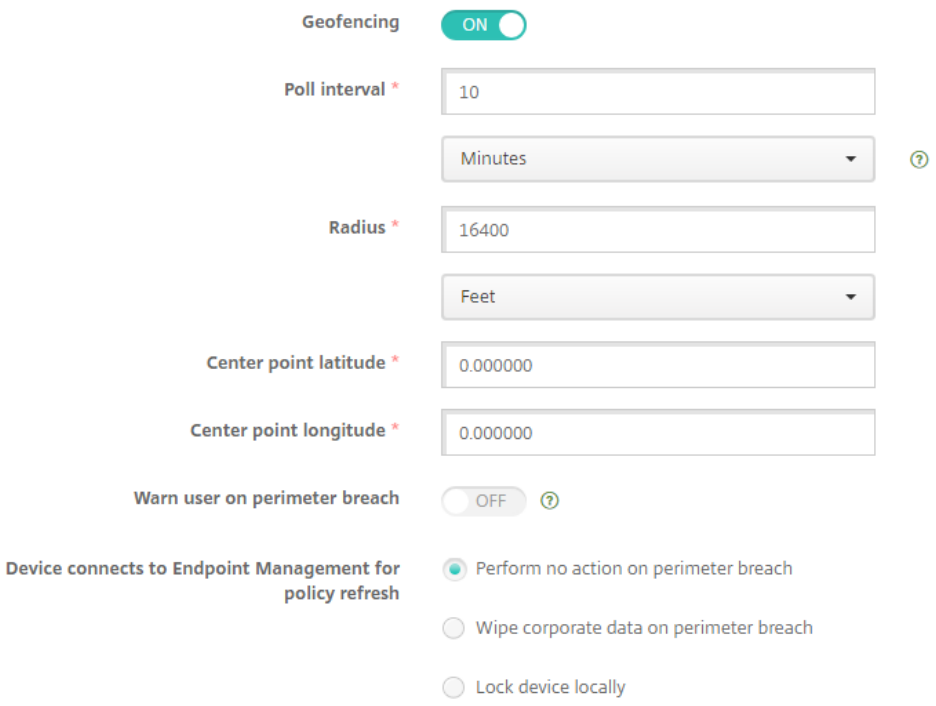
- 半径： 数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは 16,400 フィートです。有効な半径の値は次のとおりです。
  - 164 ～ 164000 フィート
  - 1 ～ 50km
  - 50 ～ 50000m
  - 54 ～ 54680 ヤード
  - 1 ～ 31 マイル
- 中心点の緯度： 緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。
- 中心点の経度： 経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告： 定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは ［オフ］ です。警告メッセージの表示に XenMobile への接続は必要ありません。
- ポリシー更新のためデバイスを **XenMobile** に接続： ユーザーが境界の外に出た場合のオプションを以下から選択します。
  - 境界違反時に何も実行しない： 何もしません。これがデフォルトの設定です。
  - 境界違反時に企業データをワイプ： 指定時間後に企業データをワイプします。このオプションを有効にすると、［ローカルワイプを延期］ フィールドが表示されます。
    * 数値を入力し、一覧から［秒］または［分］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが XenMobile によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは 0 秒です。
  - ロックを延期： 指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、［ロックを延期］ フィールドが表示されます。
    * 数値を入力し、一覧から［秒］または［分］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスが XenMobile によってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは 0 秒です。

Android Enterprise の設定



管理対象デバイス

- 位置情報モード： 有効にする位置情報検出のレベルを指定します。位置情報モードが［高精度］または［バッテリー節約］に設定されている場合のみ、検索セキュリティアクションを使用できます。デフォルトは［高精度］です。
  - 高精度： GPS、ネットワーク、その他のセンサーなど、すべての位置検出方法を有効にします。
  - センサーのみ： GPS およびその他のセンサーのみを有効にします。
  - バッテリー節約： ネットワーク位置情報プロバイダーのみを有効にします。
  - オフ： 位置の検出を無効にします。
- ジオフェンシング：



［ジオフェンシング］を選択した場合は、次の設定を構成します。

- ポーリング間隔: 数値を入力して、［分］、［時間］、［日］ のいずれかを選択し、XenMobile Server がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1 ～ 1440 分、1 ～ 24 時間、または任意の日数です。デフォルトは **10** 分です。この値を 10 分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- 半径: 数値を入力して、半径の測定に使用する単位を選択します。デフォルトは **16400** フィート（**5000m**）です。有効な半径の値は次のとおりです。
  - 164 ～ 164000 フィート
  - 1 ～ 50km
  - 50 ～ 50000m
  - 54 ～ 54680 ヤード
  - 1 ～ 31 マイル
- 中心点の緯度: 緯度（37.787454 など）を入力して、ジオフェンスの中心点の緯度を定義します。値を検索するには、［管理］**>**［デバイス］ の順に移動し、デバイスを選択して ［セキュリティ］、［検索］ の順にクリックします。デバイスの検出後、XenMobile Server は ［セキュリティ］ のデバイス ［詳細］**>**［一般］ ページでデバイスの位置情報を報告します。
- 中心点の経度: 経度（122.402952 など）を入力して、ジオフェンスの中心点の経度を定義します。
- 境界違反についてユーザーに警告: 定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは ［オフ］ です。警告メッセージの表示に XenMobile Server への接続は必要ありません。
- ポリシー更新のためデバイスを **XenMobile Server** に接続: ユーザーが境界の外に出た場合のオプションを以下から選択します:
  - 境界違反時に何も実行しない: 何もしません。この設定がデフォルトです。
  - 境界違反時に企業データをワイプ: 指定時間後に企業データをワイプします。このオプションを有効にすると、［ローカルワイプを延期］ フィールドが表示されます。
    * 数値を入力し、［秒］ または ［分］ を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスが XenMobile Server によって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。
  - デバイスをローカルにロック: 指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、［ロックを延期］ フィールドが表示されます。
    * 数値を入力し、［秒］ または ［分］ を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスが XenMobile Server によってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは **0** 秒です。

管理対象プロファイル

- 位置情報サービスが無効の場合は報告： GPS を無効にした場合に、デバイスから XenMobile Server にレポートを送信するかどうかを選択します。デフォルトは ［オフ］ です。
- ジオフェンシング： 前述の「管理対象デバイス」の設定を参照してください。

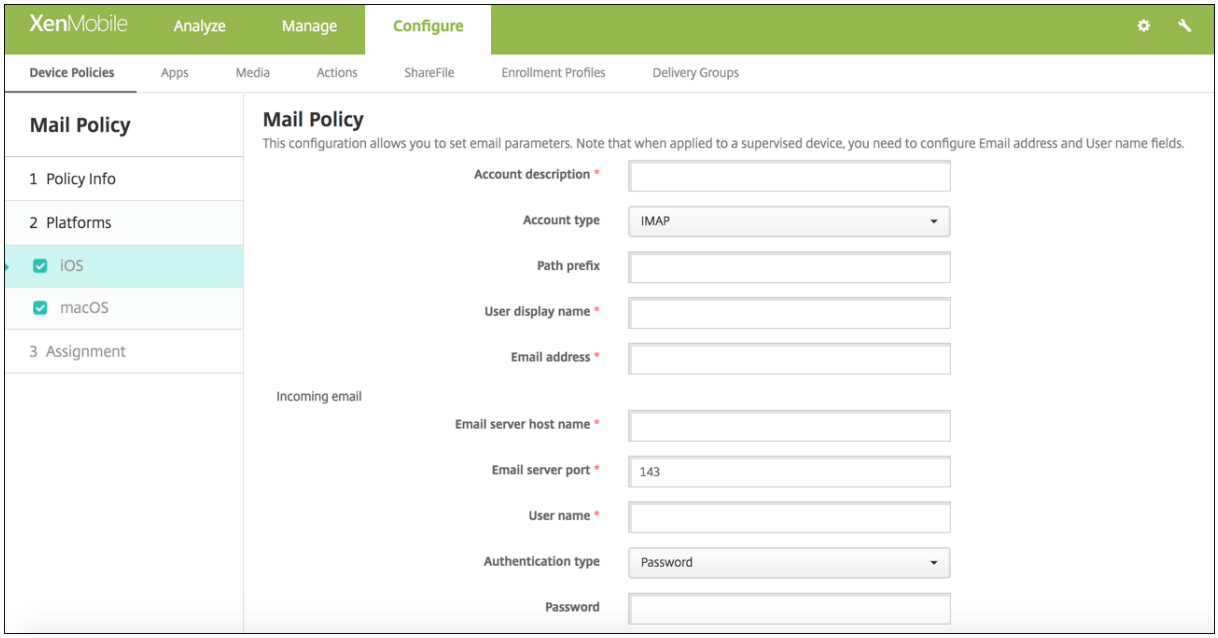
メールデバイスポリシー

January 10, 2020

XenMobile でメールデバイスポリシーを追加して、iOS または macOS デバイスのメールアカウントを構成することができます。

このポリシーを追加または構成するには、 ［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および macOS の設定



- アカウントの説明： メールおよび設定アプリに表示される、アカウントの説明を入力します。このフィールドは必須です。
- アカウントの種類： ［**IMAP**］ または ［**POP**］ を選択し、ユーザーアカウントで使用するプロトコルを選択します。デフォルトは［**IMAP**］です。［**POP**］ を選択した場合、以下の ［パスのプレフィックス］ オプションは表示されなくなります。

- パスのプレフィックス: 「**INBOX**」と入力するか、IMAP メールアカウントのパスのプレフィックスを入力します。このフィールドは必須です。
- ユーザー表示名: メッセージやその他の目的で使用する完全なユーザー名を入力します。このフィールドは必須です。
- メールアドレス: アカウントの完全なメールアドレスを入力します。このフィールドは必須です。
- 受信メール設定
  - メールサーバーのホスト名: 受信メールサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
  - メールサーバーのポート: 受信メールサーバーのポート番号を入力します。デフォルトは **143** です。このフィールドは必須です。
  - ユーザー名: メールアカウントのユーザー名を入力します。この名前は一般的に、メールアドレスの @ 記号より前の部分と同じです。このフィールドは必須です。
  - 認証の種類: 使用する認証の種類を選択します。デフォルトは ［パスワード］ です。［なし］ を選択した場合、以下の ［パスワード］ フィールドは表示されなくなります。
  - パスワード: 任意で、受信メールサーバーのパスワードを入力します。
  - **SSL** を使用: 受信メールサーバーで SSL（Secure Socket Layer）認証を使用するかどうかを選択します。デフォルトは ［オフ］ です。
- 送信メール設定
  - メールサーバーのホスト名: 送信メールサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
  - メールサーバーのポート: 送信メールサーバーのポート番号を入力します。ポート番号を入力しなかった場合、指定されたプロトコルのデフォルトポートが使用されます。
  - ユーザー名: メールアカウントのユーザー名を入力します。この名前は一般的に、メールアドレスの @ 記号より前の部分と同じです。このフィールドは必須です。
  - 認証の種類: 使用する認証の種類を選択します。デフォルトは ［パスワード］ です。
  - パスワード: 任意で、送信メールサーバーのパスワードを入力します。
  - 送信と受信に同じパスワードを使用: 受信パスワードと送信パスワードが同じであるかどうかを選択します。デフォルトは ［オフ］ で、パスワードが異なることを意味します。
  - **SSL** を使用: 送信メールサーバーで SSL（Secure Socket Layer）認証を使用するかどうかを選択します。デフォルトは ［オフ］ です。
- ポリシー
  - アカウント間でのメールの移動を承認: ユーザーが電子メールをこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - メールアプリからのみメールを送信: ユーザーの電子メールの送信を iOS メールアプリからのみに制限するかどうかを選択します。
  - メールの最近の同期を無効化: ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは ［オフ］ です。このオプションは iOS 6.0 以降にのみ適用されます。
  - メールドロップを許可: iOS 9.2 以降を実行するデバイスに対して Apple Mail Drop の使用を許可す

るかどうかを選択します。デフォルトは ［オフ］ です。

- **S/MIME** 署名の有効化: アカウントで S/MIME 署名をサポートするかどうかを指定します。デフォルトは ［オン］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - 署名 **ID** 資格情報: 使用する署名資格情報を選択します。
  - ユーザーに **S/MIME** 署名設定の上書きを許可: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 署名の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - ユーザーに **S/MIME** 署名証明書 **UUID** の上書きを許可: ［オン］ に設定した場合、ユーザーは使用する署名資格情報をデバイスの設定で選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
- **S/MIME** 暗号化の有効化: このアカウントで S/MIME 暗号化をサポートするかどうかを選択します。デフォルトは ［オフ］ です。［オン］ に設定した場合、以下の 2 つのフィールドが表示されます:
  - 暗号化 **ID** 資格情報: 使用する暗号化資格情報を選択します。
  - メッセージごとの **S/MIME** 切り替えの有効化: ［オン］ に設定すると、ユーザーがメッセージを作成するたびに S/MIME 暗号化のオンとオフを切り替えるオプションが表示されます。デフォルトは ［オフ］ です。
  - ユーザーに **S/MIME** 暗号化のデフォルト設定の上書きを許可: ［オン］ に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトで有効にするかどうかを選択できます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。
  - ユーザーに **S/MIME** 暗号化証明書 **UUID** の上書きを許可: ［オン］ に設定した場合、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化の有効化と無効化を切り替えられます。デフォルトは ［オフ］ です。このオプションは iOS 12.0 以降に適用されます。

- ポリシー設定
  - ポリシーの削除: 後でポリシーを削除するには、［日付を選択］ または ［削除までの期間（時間）を指定］ でポリシーを削除するようこの設定を構成できます。
  - ユーザーにポリシーの削除を許可: ユーザーが常にメールポリシーを削除できるか、削除するためにパスコードが必要か、ユーザーによるポリシーの削除を許可しないのかを選択できます。
  - プロファイルの対象: macOS のみ。ポリシーをユーザーレベルで適用するか、システム全体で適用するかを選択します。

管理対象ドメインデバイスポリシー

January 10, 2020

メールおよび Safari ブラウザーに適用する管理対象ドメインを定義できます。管理対象ドメインを使用すると、Safari を使用してドメインからダウンロードしたドキュメントを開くことができるアプリを制御して、会社のデータを保護することができます。

iOS8 以降の管理対象デバイスでは、URL またはサブドメインを使用して、ユーザーがドキュメント、添付ファイル

など、ブラウザーからダウンロードしたものを開く方法を制御します。iOS 9.3 以降の監視対象デバイスでは、URL を指定することで、ユーザーが Safari でその URL でのパスワードを保存できます。

iOS デバイスを Supervised モードに設定する手順について詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。

ドキュメント、添付ファイル、ダウンロードファイルなどのアイテムの場合: ユーザーが Safari を使用して、管理対象 Web ドメイン一覧に含まれている Web ドメインから取得したアイテムを開くと、適切な社内アプリによってアイテムが開かれます。アイテムが管理対象 Web ドメイン一覧にある Web ドメインから取得されたものでない場合、ユーザーは社内アプリでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリを使用する必要があります。

管理対象デバイスの場合（Safari パスワード自動入力ドメインを指定しない場合でも）: デバイスがエフェメラルマルチユーザーとして構成されている場合、ユーザーはパスワードを保存できません。ただし、デバイスがエフェメラルマルチユーザーとして構成されていない場合、ユーザーはすべてのパスワードを保存できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

ドメインの指定方法

形式	説明
`example.com`	`example.com`のすべてのパスを管理対象として扱いますが、`site.example.com/`は管理対象として扱いません。
`foo.example.com`	`foo.example.com`のすべてのパスを管理対象として扱いますが、`example.com/`と`bar.example.com/`は管理対象として扱いません。
`\*.example.com`	`foo.example.com`または`bar.example.com`のすべてのパスを管理対象として扱いますが、`example.com/`は管理対象として扱いません。
`example.com/sub`	`example.com/sub`とそのすべてのパスを管理対象として扱いますが、`example.com/`は管理対象として扱いません。

形式	説明
foo.example.com/sub	foo.example.com/subのすべてのパスを管理対象として扱いますが、example.com、example.com/sub、foo.example.com/、bar.example.com/subは管理対象として扱いません。
*.example.com/sub	foo.example.com/subまたはbar.example.com/subのすべてのパスを管理対象として扱いますが、example.comおよびfoo.example.com/は管理対象として扱いません。

規則

- ドメインの比較時に URL の前半部の「www.」および末尾のスラッシュは無視されます。
- エントリにポート番号が含まれる場合は、そのポート番号を指定しているアドレスのみが管理対象と見なされます。ポート番号が含まれない場合は、標準のポートが管理対象と見なされます（http の場合はポート 80、https の場合はポート 443）。たとえば、*.example.com:8080というパターンはhttps://site.example.com:8080/page.htmlと一致しますが、https://site.example.com/page.htmlとは一致しません。これに対して、*.example.comというパターンは、https://site.example.com/page.htmlとhttps://site.example.com/page.htmlとは一致しますが、https://site.example.com:8080/page.htmlとは一致しません。
- 管理対象の Safari Web ドメインの定義は蓄積されます。URL リクエストとの照合には、すべての管理対象 Safari Web ドメインのペイロードで定義されたパターンが使用されます。

設定:

- 管理対象ドメイン
  - マークされていないメールドメイン: 一覧に含めるメールドメインごとに、［追加］ をクリックして以下の操作を行います。
    - 管理対象のメールドメイン: メールドメインを入力します。
    - ［保存］ をクリックしてメールドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - 管理対象の **Safari Web** ドメイン: 一覧に含める Web ドメインごとに、［追加］ をクリックして以下の操作を行います。
    - 管理対象の **Web** ドメイン: Web ドメインを入力します。
    - ［保存］ をクリックして Web ドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **Safari** のパスワードオートフィルドメイン: 一覧に含める自動入力ドメインごとに、［追加］をクリックして以下の操作を行います。

* **Safari** のパスワードオートフィルドメイン: 自動入力ドメインを入力します。
* ［保存］ をクリックして自動入力ドメインを保存するか、［キャンセル］ をクリックして自動入力ドメインを取り消します。

MDM オプションデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを作成して、監視対象の iOS 7.0 以降のモバイルデバイスで［iPhone/iPad を探す］の［アクティベーションロック］を管理することができます。iOS デバイスを Supervised モードに設定する手順について詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

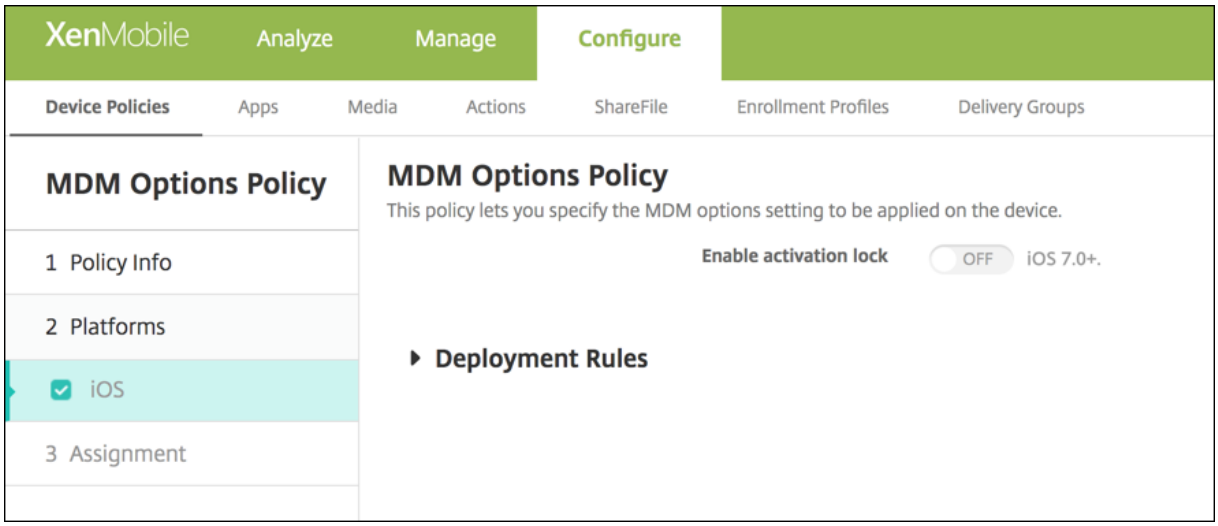
アクティベーションロックは、紛失したり盗まれたりした管理対象デバイスが再アクティブ化されないようにすることを目的とした［iPhone/iPad を探す］の機能です。アクティベーションロックでは、ユーザーの Apple ID とパスワードを入力してからでないと、［iPhone/iPad を探す］をオフにしたり、デバイスを消去したり、デバイスを再アクティブ化したりすることはできません。組織所有のデバイスの場合は、デバイスのリセットや再割り当てなどを行う際にアクティベーションロックをバイパスする必要があります。

アクティベーションロックを有効にするには、XenMobile MDM オプションのデバイスポリシーを設定して展開します。その後はユーザーの Apple 資格情報なしで、XenMobile コンソールからデバイスを管理することができます。アクティベーションロックで必要な Apple 資格情報の入力をバイパスするには、XenMobile コンソールから［アクティベーションロックバイパス］のセキュリティ操作を発行します。

たとえば、紛失した iPhone がユーザーによって返却されたり、フルワイプの前または後にデバイスを設定したりする場合、iPhone で iTunes アカウントの資格情報を入力するよう求められた際に、XenMobile コンソールから［アクティベーションロックバイパス］のセキュリティ操作を発行することでこの手順をバイパスすることができます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- アクティベーションロックを有効化: このポリシーを展開するデバイスでアクティベーションロックを有効にするかどうかを選択します。デフォルトは ［オフ］ です。

MDM オプションデバイスポリシーを展開してアクティベーションロックを有効にした後: ［管理］ > ［デバイス］ ページで該当するデバイスを選択し、 ［セキュリティ］ をクリックすると、セキュリティ操作の ［アクティベーションロックバイパス］ が表示されます。アクティベーションロックバイパスを使用すると、デバイスユーザーの Apple ID とパスワードがわからなくても、デバイスをアクティブ化する前に管理対象デバイスからアクティベーションロックを削除することができます。フルワイプの前または後に、デバイスにアクティベーションロックバイパスを送信できます。詳細については、「セキュリティ操作」の記事の「iOS アクティベーションロックのバイパス」を参照してください。

組織情報デバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、XenMobile から iOS デバイスにプッシュされるアラートメッセージ用の組織情報を指定できます。このオプションは iOS 7 以降のデバイスで使用できます。

このポリシーを追加または構成するには、 ［構成］ > ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 名前: XenMobile を実行している組織の名前を入力します。
- 住所: 組織の住所を入力します。

- 電話： 組織のサポート電話番号を入力します。
- メール： サポートメールアドレスを入力します。
- マジック： 組織が管理しているサービスについて説明する語句を入力します。

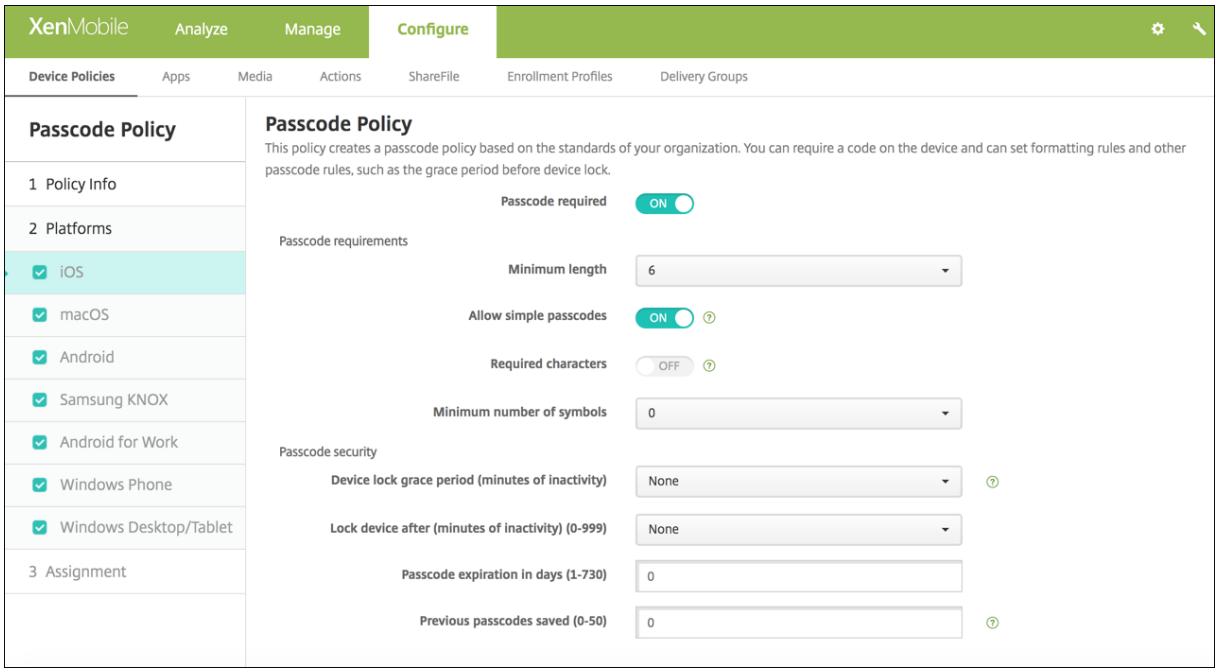
パスコードデバイスポリシー

January 10, 2020

組織の基準に基づいて、XenMobile でパスコードポリシーを作成します。ユーザーのデバイスでパスコードを要求し、さまざまな形式およびパスコード規則を設定することができます。iOS、macOS、Android、Samsung KNOX、Android Enterprise、Windows Phone、および Windows デスクトップ/タブレットに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

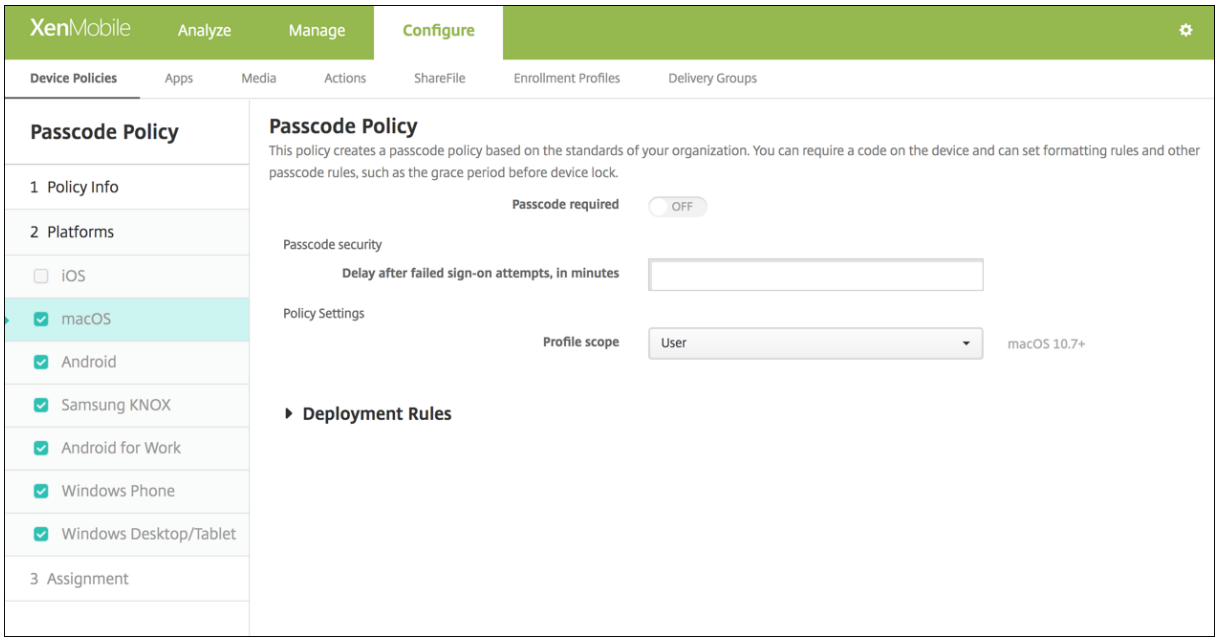
iOS の設定



- パスコードを要求： このオプションをオンにするとパスコードが必須になり、iOS のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、ポリシー設定を構成できます。
- パスコード要件
  - 最小の長さ： 一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。

  - 単純なパスコードを許可: 簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。デフォルトは ［オン］ です。
  - 必須文字: パスコードに文字を 1 つ以上含める必要があるかどうかを選択します。デフォルトは ［オフ］ です。
  - 記号の最小数: 一覧から、パスコードに含める必要がある記号の数を選択します。デフォルトは **0** です。
- パスコードセキュリティ
  - デバイスロックの猶予期間（分単位のアイドル時間）: 一覧から、ユーザーがパスコードを入力してデバイスのロックを解除することが必要になるまでの時間を選択します。デフォルトは ［なし］ です。
  - デバイスをロックするまでの期間（分単位のアイドル時間）: 一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは ［なし］ です。
  - パスコードの有効期限（**1-730** 日）: パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）: 保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - サインオン失敗回数の上限: 一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。デフォルトは ［未定義］ です。
- ポリシー設定
  - ［ポリシーの削除］ の横にある ［日付を選択］ または ［削除までの期間（時）を指定］ をクリックします。
  - ［日付を選択］ をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［ユーザーにポリシーの削除を許可］ の一覧で、［常に］、［パスワードが必要］、［しない］ のいずれかを選択します。
  - ［パスワードが必要］ を選択した場合、［パスワードを削除］ の横に求めるパスワードを入力します。

macOS 設定

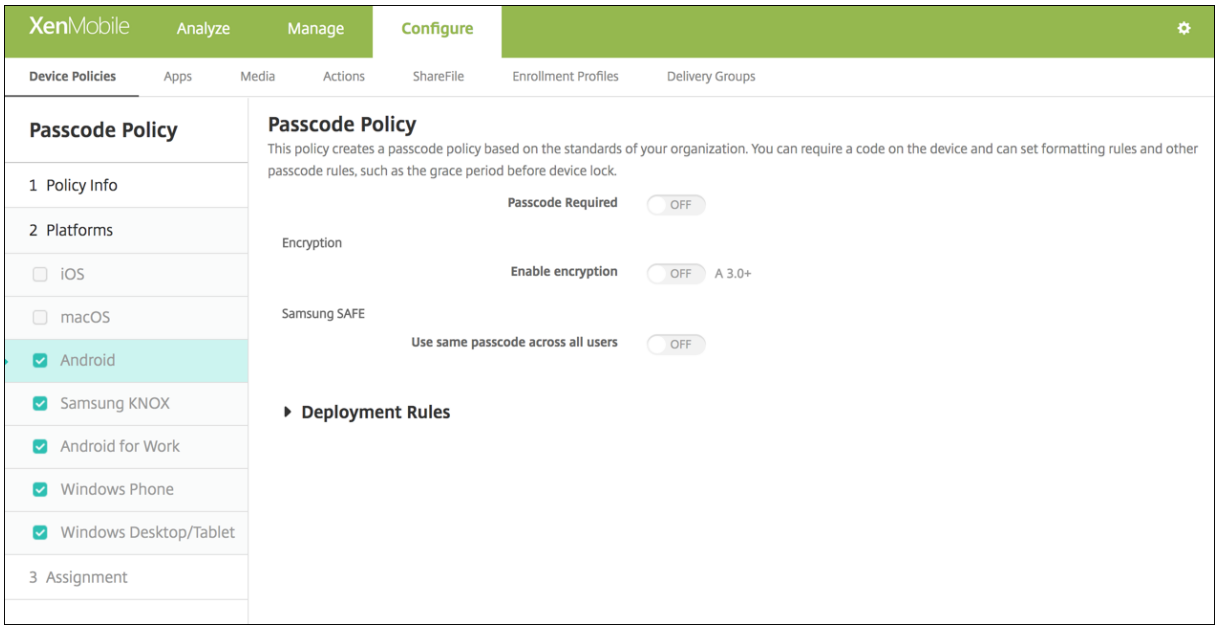


- パスコードを要求: このオプションをオンにするとパスコードが必須になり、iOS のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、ポリシー設定を構成できます。
- [パスコードを要求] を有効にしない場合は、[サインオン試行失敗後の待機時間 (分)] の横で、ユーザーがパスコードを再入力できるようになるまでの待機時間を分単位で入力します。
- [パスコードを要求] を有効にした場合は、次の設定を構成します:
- パスコード要件
  - 最小の長さ: 一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。
  - 単純なパスコードを許可: 簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。デフォルトは [オン] です。
  - 必須文字: パスコードに文字を 1 つ以上含める必要があるかどうかを選択します。デフォルトは [オフ] です。
  - 記号の最小数: 一覧から、パスコードに含める必要がある記号の数を選択します。デフォルトは **0** です。
- パスコードセキュリティ
  - デバイスロックの猶予期間 (分単位のアイドル時間): 一覧から、ユーザーがパスコードを入力してデバイスのロックを解除することが必要になるまでの時間を選択します。デフォルトは [なし] です。
  - デバイスをロックするまでの期間 (分単位のアイドル時間): 一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは [なし] です。
  - パスコードの有効期限 (**1-730** 日): パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数 (**0 - 50**): 保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーが

パスワードを再使用できることを意味します。
- サインオン失敗回数の上限: 一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはロックされます。デフォルトは ［未定義］ です。
- サインオン試行失敗後の待機時間（分）: ユーザーがパスコードを再入力できるようになるまでの待機時間を分単位で入力します。

- ポリシー設定
  - ［ポリシーの削除］ の横にある ［日付を選択］ または ［削除までの期間（時）を指定］ をクリックします。
  - ［日付を選択］ をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［ユーザーにポリシーの削除を許可］ の一覧で、 ［常に］、 ［パスワードが必要］、 ［しない］ のいずれかを選択します。
  - ［パスワードが必要］ を選択した場合、 ［パスワードを削除］ の横に求めるパスワードを入力します。
  - ［プロファイルの対象］ の横にある、 ［ユーザー］ または ［システム］ を選択します。デフォルトは ［ユーザー］ です。このオプションは macOS 10.7 以降でのみ使用できます。

Android の設定



> 注:
>
> Android のデフォルト設定は ［オフ］ です。

- パスコードを要求: このオプションをオンにするとパスコードが必須になり、Android のパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、暗号化、Samsung SAFE の設定を構成できます。
- パスコード要件
  - 最小の長さ: 一覧から、パスコードの最小文字数を選択します。デフォルトは 6 です。

- バイオメトリック認識： 生体認証を有効にするかどうかを選択します。このオプションを有効にした場合、［必須文字］フィールドは非表示になります。デフォルトは ［オフ］ です。
- 必須文字： 一覧から［制限なし］、［数字と文字の両方］、［数字のみ］、［文字のみ］のいずれかを選択して、パスコードの作成方法を構成します。デフォルトは［制限なし］です。
- 詳細な規則： 詳細なパスコード規則を適用するかどうかを選択します。このオプションは Android 3.0 以降で使用できます。デフォルトは ［オフ］ です。
- ［詳細な規則］ を有効にした場合、以下のボックスの一覧のそれぞれで、パスコードに含める必要がある文字、記号、または数字の数を、種類ごとに選択します。
  - 記号： 記号の最小使用数
  - 文字： 文字の最小使用数
  - 小文字： 小文字の最小使用数
  - 大文字： 大文字の最小使用数
  - 数字または記号： 数字または記号の最小使用数
  - 数字： 数字の最小使用数

- パスコードセキュリティ
  - デバイスをロックするまでの期間（分単位のアイドル時間）： 一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは［なし］ です。
  - パスコードの有効期限（**1-730** 日）： パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）： 保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - サインオン失敗回数の上限： 一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。デフォルトは ［未定義］ です。

- 暗号化
  - 暗号化を有効化： 暗号化を有効にするかどうかを選択します。このオプションは Android 3.0 以降で使用できます。このオプションは、［パスコードを要求］ 設定にかかわらず使用できます。

    デバイスを暗号化するには、ユーザーはまず充電済みのバッテリーを用意し、暗号化にかかる時間またはそれ以上の時間にわたってデバイスをコンセントに接続したままにする必要があります。暗号化処理を中断すると、デバイス上のデータの一部またはすべてが失われる可能性があります。デバイスを暗号化した後は、出荷時の設定へのリセットを実行してデバイス上のすべてのデータを消去しない限り、元に戻すことはできません。

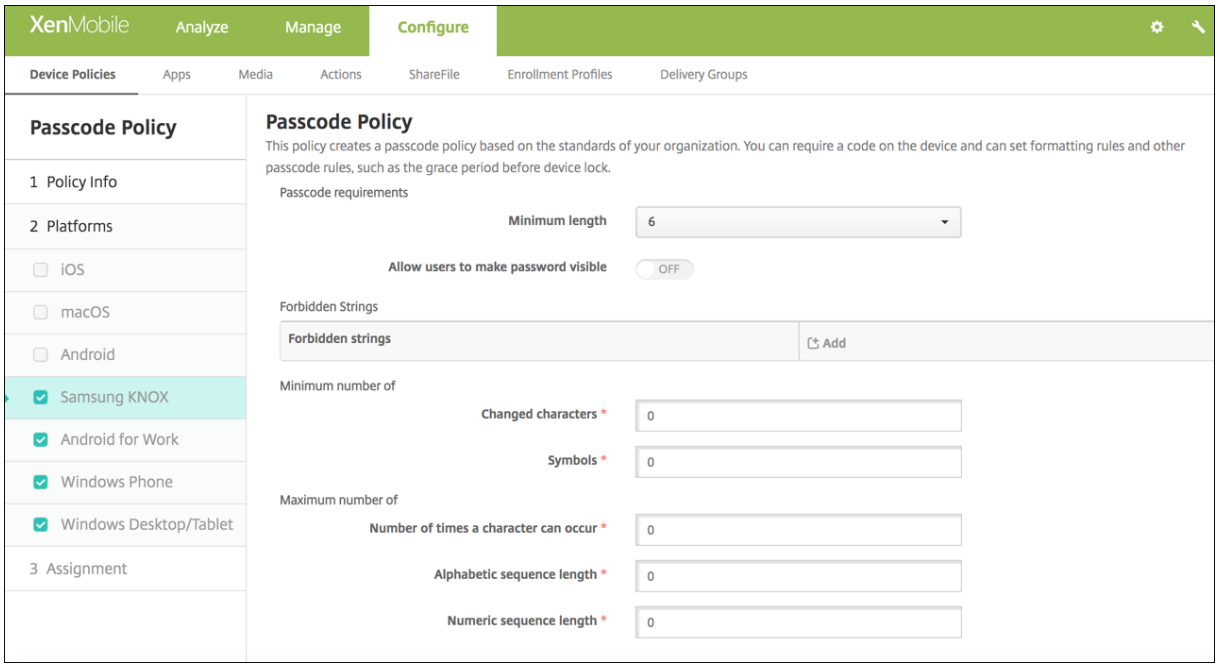
- **Samsung SAFE**

> 注:
>
> Samsung SAFE デバイスの顔認識および虹彩認識を無効にするための回避策：Samsung SAFE の制

> 限デバイスポリシーを作成します。制限ポリシーで、［アプリケーションを無効にする］ をオンにして、`com.samsung.android.bio.face.service`または`com.samsung.android.server.iris`をテーブルに追加します。その後、制限ポリシーを展開します。

- すべてのユーザーに同じパスコードを使用: すべてのユーザーに対して同じパスコードを使用するかどうかを選択します。デフォルトは ［オフ］ です。この設定は Samsung SAFE デバイスにのみ適用され、［パスコードを要求］ 設定にかかわらず使用できます。
- ［すべてのユーザーに同じパスコードを使用］ を有効にした場合は、［パスコード］ フィールドにすべてのユーザーが使用するパスコードを入力します。
- ［パスコードを要求］ を有効にした場合は、次の Samsung SAFE の設定を構成します:
  * 変更する文字数: ユーザーが前のパスコードから変更する必要がある文字数を入力します。デフォルトは **0** です。
  * 同一文字の最大使用数: パスコード内に 1 つの文字を繰り返し使用できる最大回数を入力します。デフォルトは **0** です。
  * アルファベットの最大連続数: パスコードに含まれる、連続するアルファベットの最大文字数を入力します。デフォルトは **0** です。
  * 数字の最大連続数: パスコードに含まれる、連続する数字の最大文字数を入力します。デフォルトは **0** です。
  * パスワードの表示をユーザーに許可: ユーザーがパスコードを表示できるようにするかどうかを選択します。デフォルトは ［オン］ です。
  * 生体認証の構成。生体認証を有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オン］ に設定すると、次のオプションを設定できます。
    - 指紋を許可。ユーザーが指紋による認証を許可する場合に選択します。
    - 虹彩を許可。ユーザーが虹彩による認証を許可する場合に選択します。
  * 禁止文字列: 禁止文字列を作成して、「password」、「pwd」、「welcome」、「123456」、「111111」などの類推しやすく安全ではない文字列をユーザーが使用できないようにします。拒否する文字列ごとに ［追加］ をクリックして、以下の操作を行います:
    - 禁止文字列: ユーザーに使用できないようにする文字列を入力します。
    - ［保存］ をクリックして文字列を追加するか、［キャンセル］ をクリックして文字列の追加を取り消します。

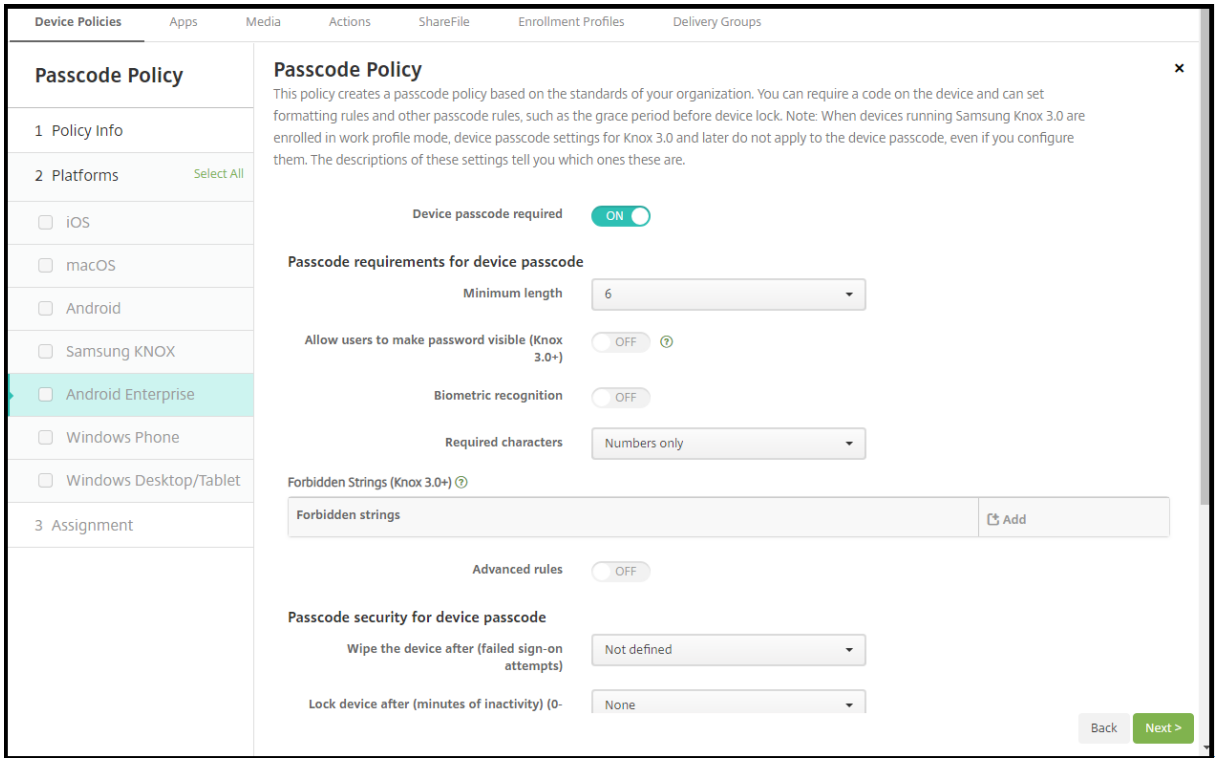
Samsung KNOX の設定



- パスコード要件
  - 最小の長さ： 一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。
  - パスワードの表示をユーザーに許可： ユーザーがパスワードを表示できるようにするかどうかを選択します。
  - 禁止文字列： 禁止文字列を作成して、「password」、「pwd」、「welcome」、「123456」、「111111」などの類推しやすく安全ではない文字列をユーザーが使用できないようにします。拒否する文字列ごとに［追加］をクリックして、以下の操作を行います：
    * 禁止文字列： ユーザーに使用できないようにする文字列を入力します。
    * ［保存］ をクリックして文字列を追加するか、 ［キャンセル］ をクリックして文字列の追加を取り消します。
- 最小数：
  - 変更する文字数： ユーザーが前のパスコードから変更する必要がある文字数を入力します。デフォルトは **0** です。
  - 記号： パスコードに含める必要がある記号の最小数を入力します。デフォルトは **0** です。
- 最大数：
  - 同一文字の最大使用数： パスコード内に 1 つの文字を繰り返し使用できる最大回数を入力します。デフォルトは **0** です。
  - アルファベットの最大連続数： パスコードに含まれる、連続するアルファベットの最大文字数を入力します。デフォルトは **0** です。
  - 数字の最大連続数： パスコードに含まれる、連続する数字の最大文字数を入力します。デフォルトは **0** です。
- パスコードセキュリティ

- デバイスをロックするまでの期間（分単位のアイドル時間）: 一覧から、デバイスを非アクティブにしておくことができる秒数を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは［なし］ です。
- パスコードの有効期限（**1-730** 日）: パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
- 使用済みパスワードの保存数（**0 - 50**）: 保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
- サインオン失敗回数の上限を超えると、デバイスがロックされます: 一覧から、ユーザーが正常なサインオンの前に失敗できる回数を選択します。この回数を超えると、デバイスはロックされます。デフォルトは ［未定義］ です。
- サインオン失敗回数の上限を超えると、デバイスがワイプされます: 一覧から、ユーザーが正常なサインオンの前に失敗できる回数をクリックします。この回数を超えると、KNOX コンテナ（および KNOX データ）がデバイスからワイプされます。ユーザーは、ワイプが発生した後、KNOX コンテナを再度初期化する必要があります。デフォルトは ［未定義］ です。

Android Enterprise の設定



Android Enterprise デバイスの場合は、デバイスのパスコードか Android Enterprise の仕事用プロファイルのセキュリティ確認、またはその両方を必須条件にできます。

Android 8.0 以降および Samsung Knox 3.0 以降を実行しているデバイスの場合は、［**Android Enterprise**］ペ

ージで Samsung Knox の設定を行います。それ以前のバージョンの Android または Samsung Knox を実行しているデバイスの場合は、［**Samsung Knox**］ ページで設定します。

> 注:
>
> Samsung Knox 3.0 を実行しているデバイスが仕事用プロファイルデバイスとして登録されている場合、Knox 3.0 以降のデバイスパスコード設定を構成していても、デバイスのパスコードには適用されません。

- デバイスのパスコードを要求: デバイスにパスコードが必要です。この設定が ［オン］ の場合は、［デバイスのパスコードのパスコード要件］ と ［デバイスのパスコードのパスコードセキュリティ］ を設定します。デフォルトは ［オフ］ です。
- デバイスのパスコードのパスコード要件:
  - 最小の長さ: パスコードの最小文字数を選択します。デフォルトは 6 です。
  - パスワードの表示をユーザーに許可: 有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス専用の設定で、仕事用プロファイルデバイスとして登録されているデバイスには適用されません。この設定をオンにすると、ユーザーはパスワードを表示できるようになります。デフォルトは ［オフ］ です。
  - バイオメトリック認識: 生体認証を有効にします。この設定が ［オン］ の場合、［必須文字］フィールドは非表示になります。デフォルトは ［オフ］ です。
  - 必須文字: パスコードに必要な文字の種類を指定します。一覧の中から、［制限なし］、［数字と文字の両方］、［数字のみ］、または ［文字のみ］ を選択します。［制限なし］ は、Android 7.0 を実行しているデバイスにのみ使用します。Android 7.1 以降では、［制限なし］設定は適用されません。デフォルトは ［数字と文字の両方］ です。
  - 禁止文字列: 有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス専用の設定で、仕事用プロファイルデバイスとして登録されているデバイスには適用されません。ユーザーがパスコードに使用できない文字列を指定します。禁止文字列を作成して、「password」、「pwd」、「welcome」、「123456」、「111111」などの類推しやすく安全ではない文字列をユーザーが使用できないようにします。拒否する文字列ごとに以下の操作を行います: ［追加］をクリックして、ユーザーに使用させない文字列を入力します。文字列を追加するには ［保存］ を、取り消すには ［キャンセル］ をクリックします。
  - 詳細な規則: パスコードに使用できる文字の種類を、規則で詳しく設定します。この設定が ［オン］ の場合は、［最小数］および ［最大数］ を設定します。この設定は、Android 5.0 より前の Android デバイスでは使用できません。デフォルトは ［オフ］ です。
  - 最小数:
    * 記号: 記号の最小使用数を指定します。デフォルト値は **0** です。
    * 文字: 文字の最小使用数を指定します。デフォルト値は **0** です。
    * 小文字: 小文字の最小使用数を指定します。デフォルト値は **0** です。
    * 大文字: 大文字の最小使用数を指定します。デフォルト値は **0** です。
    * 数字または記号: 数字または記号の最小使用数を指定します。デフォルト値は **0** です。
    * 数字: 数字の最小使用数を指定します。デフォルト値は **0** です。
    * 変更する文字数: 有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実

行しているデバイスで使用します。完全に管理されているデバイス専用の設定で、仕事用プロファイルデバイスとして登録されているデバイスには適用されません。ユーザーが前のパスコードから変更する必要がある文字数を指定します。デフォルトは **0** です。

  - 最大数： 有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス専用の設定で、仕事用プロファイルデバイスとして登録されているデバイスには適用されません。
    * 同一文字の最大使用数： パスコード内に 1 つの文字を繰り返し使用できる最大回数を指定します。デフォルトは **0** で、制限がないことを意味します。
    * アルファベットの最大連続数： パスコードに含まれる、連続するアルファベットの最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。
    * 数字の最大連続数： パスコードに含まれる、連続する数字の最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。

- デバイスのパスコードのパスコードセキュリティ：
  - デバイスをワイプ（サインオンの失敗回数が次を超えた場合）： ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、デバイスは完全にワイプされます。デフォルトは ［未定義］ です。
  - デバイスロックの猶予期間（分単位のアイドル時間）（**0-999**）： デバイスを非アクティブにしておくことができる分数を指定します。この時間が過ぎると、デバイスはロックされます。デフォルトは ［なし］ です。
  - パスコードの有効期限（**1-730** 日）： パスコードを有効期限切れにするまでの日数を指定します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
  - 使用済みパスワードの保存数（**0 - 50**）： 保存する使用済みパスワードの数を指定します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
  - デバイスをロック（サインオンの失敗回数が次を超えた場合） 有効な Knox ライセンスキーが設定されている Samsung Knox 3.0 以降を実行しているデバイスで使用します。完全に管理されているデバイス専用の設定で、仕事用プロファイルデバイスとして登録されているデバイスには適用されません。ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、デバイスがロックされます。デフォルトは ［未定義］ です。
- 仕事用プロファイルのセキュリティ確認： Android Enterprise の仕事用プロファイル内で実行されるアプリへのアクセスに対して、ユーザーにセキュリティの確認を求めます。Android 7.0 以降を実行するデバイス向けです。この設定が ［オン］ の場合は、［仕事用プロファイルのセキュリティ確認用のパスコード要件］と［仕事用プロファイルのセキュリティ確認用のパスコードセキュリティ］ を設定します。デフォルトは ［オフ］ です。
- 仕事用プロファイルのセキュリティ確認用のパスコード要件：
  - 最小の長さ： パスコードの最小文字数を選択します。デフォルトは 6 です。
  - パスワードの表示をユーザーに許可： 有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。この設定をオンにすると、ユーザーはパスワードを表示できるようになります。デフォルトは ［オフ］ です。
  - バイオメトリック認識： 生体認証を有効にします。この設定が ［オン］ の場合、［必須文字］フィール

ドは非表示になります。デフォルトは ［オフ］ です。

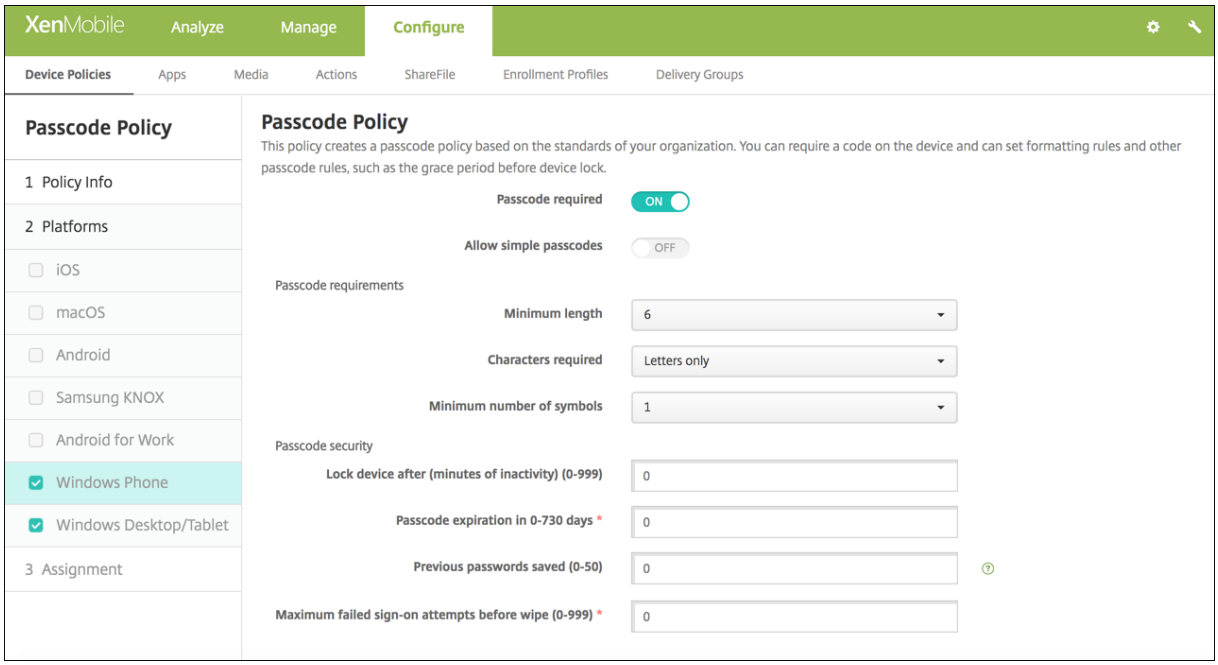
- 必須文字: パスコードに必要な文字の種類を指定します。一覧の中から、［制限なし］、［数字と文字の両方］、［数字のみ］、または ［文字のみ］ を選択します。［制限なし］ は、Android 7.0 を実行しているデバイスにのみ使用します。Android 7.1 以降では、［制限なし］設定は適用されません。デフォルトは ［数字と文字の両方］ です。
- 禁止文字列: 有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。ユーザーがパスコードに使用できない文字列を指定します。禁止文字列を作成して、「password」、「pwd」、「welcome」、「123456」、「111111」などの類推しやすく安全ではない文字列をユーザーが使用できないようにします。拒否する文字列ごとに以下の操作を行います: ［追加］をクリックして、ユーザーに使用させない文字列を入力します。文字列を追加するには ［保存］ を、取り消すには ［キャンセル］ をクリックします。
- 詳細な規則: パスコードに使用できる文字の種類を、規則で詳しく設定します。この設定が ［オン］ の場合は、［最小数］および ［最大数］ を設定します。この設定は、Android 5.0 より前の Android デバイスでは使用できません。デフォルトは ［オフ］ です。
- 最小数:
  - 記号: 記号の最小使用数を指定します。デフォルト値は **0** です。
  - 文字: 文字の最小使用数を指定します。デフォルト値は **0** です。
  - 小文字: 小文字の最小使用数を指定します。デフォルト値は **0** です。
  - 大文字: 大文字の最小使用数を指定します。デフォルト値は **0** です。
  - 数字または記号: 数字または記号の最小使用数を指定します。デフォルト値は **0** です。
  - 数字: 数字の最小使用数を指定します。デフォルト値は **0** です。
  - 変更する文字数: 有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。ユーザーが前のパスコードから変更する必要がある文字数を指定します。デフォルトは **0** です。
- 最大数: 有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。
  - 同一文字の最大使用数: パスコード内に 1 つの文字を繰り返し使用できる最大回数を指定します。デフォルトは **0** で、制限がないことを意味します。
  - アルファベットの最大連続数: パスコードに含まれる、連続するアルファベットの最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。
  - 数字の最大連続数: パスコードに含まれる、連続する数字の最大文字数を指定します。デフォルトは **0** で、制限がないことを意味します。

- 仕事用プロファイルのセキュリティ確認用のパスコードセキュリティ
  - コンテナをワイプ（サインオンの失敗回数が次を超えた場合）: ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、仕事用プロファイルとそのデータがデバイスからワイプされます。ユーザーは、ワイプが発生した後、仕事用プロファイルを再度初期化する必要があります。デフォルトは ［未定義］ です。
  - コンテナをロックするまでの期間（分単位のアイドル時間）: デバイスを非アクティブにしておくことができる分数を指定します。この時間が過ぎると、仕事用プロファイルはロックされます。デフォルト

は ［なし］ です。

- パスコードの有効期限（**1-730** 日）: パスコードを有効期限切れにするまでの日数を指定します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
- 使用済みパスワードの保存数（**0 - 50**）: 保存する使用済みパスワードの数を指定します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
- コンテナをロック（サインオンの失敗回数が次を超えた場合） 有効な Knox ライセンスキーが設定されている Knox 3.0 以降を実行しているデバイスで使用します。ユーザーがサインオンに失敗できる回数を指定します。この回数を超えると、デバイスがロックされます。デフォルトは ［未定義］ です。

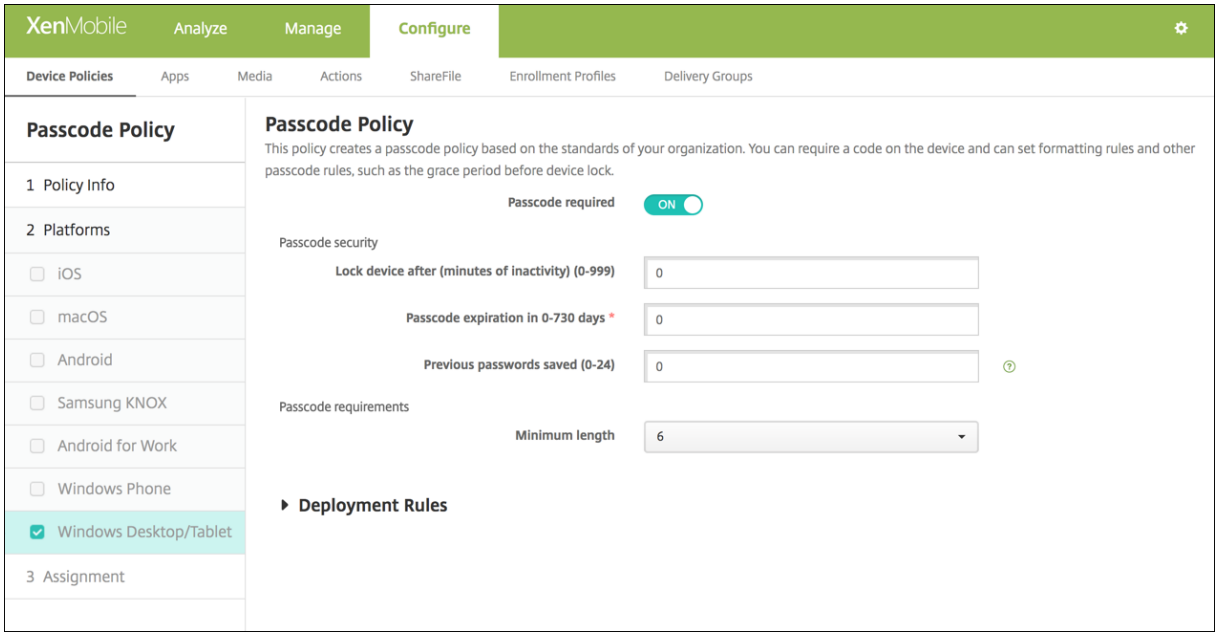
Windows Phone の設定



- パスコードを要求: Windows Phone デバイスでパスコードを要求しない場合、このオプションを選択します。デフォルト設定は ［オン］ で、パスコードを要求します。この設定を無効にすると、ページが折りたたまれ、以下のオプションは表示されなくなります。
- 単純なパスコードを許可: 簡単なパスコードを許可するかどうかを選択します。簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。デフォルトは［オフ］です。
- パスコード要件
  - 最小の長さ: 一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。
  - 必須文字: 一覧から ［数字または英数字］、［文字のみ］、［数字のみ］ のいずれかを選択して、パスワードの作成方法を構成します。デフォルトは ［数字のみ］ です。
  - 記号の最小数: 一覧から、パスコードに含める必要がある記号の数を選択します。デフォルトは **1** です。
- パスコードセキュリティ

- デバイスロックの猶予期間（分単位のアイドル時間）: デバイスを非アクティブにしておくことができる分数を入力します。この時間が過ぎると、デバイスはロックされます。デフォルトは **0** です。
- パスコードの有効期限（**0 - 730** 日）: パスコードを有効期限切れにするまでの日数を入力します。有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
- 使用済みパスワードの保存数（**0 - 50**）: 保存する使用済みパスワードの数を入力します。ユーザーはこの一覧にあるパスワードを使用できません。有効な値は 0 ～ 50 です。デフォルトは **0** で、ユーザーがパスワードを再使用できることを意味します。
- ワイプ前のサインオン失敗回数の上限（**0 - 999**）: ユーザーが正常なサインオンの前に失敗できる回数を入力します。この回数を超えると、企業データがデバイスからワイプされます。デフォルトは **0** です。

Windows デスクトップ/タブレットの設定



- 便利なログオンを許可しない: ユーザーがピクチャーパスワードまたは生体認証ログオンを使用してデバイスにアクセスできるようにするかどうかを選択します。デフォルトは ［オフ］ です。
- 最小パスコード長: 一覧から、パスコードの最小文字数を選択します。デフォルトは **6** です。
- ワイプ前のパスコード入力試行回数の上限: ユーザーが正常なサインオンの前に失敗できる回数を入力します。この回数を超えると、企業データがデバイスからワイプされます。デフォルトは **4** です。
- パスコードの有効期限（**0** ～ **730** 日）: パスコードを有効期限切れにするまでの日数を入力します有効な値は 1 ～ 730 です。デフォルトは **0** で、パスコードの有効期限がないことを意味します。
- パスコード履歴:（**1-24**）: 保存する使用済みパスコードの数を入力します。ユーザーはこの一覧にあるパスコードを使用できません。有効な値は 1 ～ 24 です。このフィールドには 1 ～ 24 の数値を入力する必要があります。デフォルトは **0** です。
- デバイスロックまでの最大アイドル時間（**1 - 999** 分）: デバイスを非アクティブにしておくことができる分数を入力します。この時間が過ぎると、デバイスはロックされます。有効な値は 1 ～ 999 です。このフィール

ドには 1 ～ 999 の数値を入力する必要があります。デフォルトは **0** です。

個人用ホットスポットデバイスポリシー

January 10, 2020

iOS デバイスの個人用ホットスポット機能を介して携帯データネットワーク接続を使用することにより、ユーザーが WiFi ネットワーク圏外にいてもインターネットに接続できるようにすることができます。iOS 7.0 以降で利用できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- パーソナルホットスポットを無効化: ユーザーのデバイスで個人用ホットスポット機能を無効にするかどうかを選択します。デフォルトは ［オフ］ で、ユーザーのデバイスで個人用ホットスポットは無効になっています。このポリシーでは機能は無効になりません。ユーザーは、引き続きデバイスで個人用ホットスポットを使用できますが、ポリシーが展開されると、デフォルトでオンのままにならないように、個人用ホットスポットがオフになります。

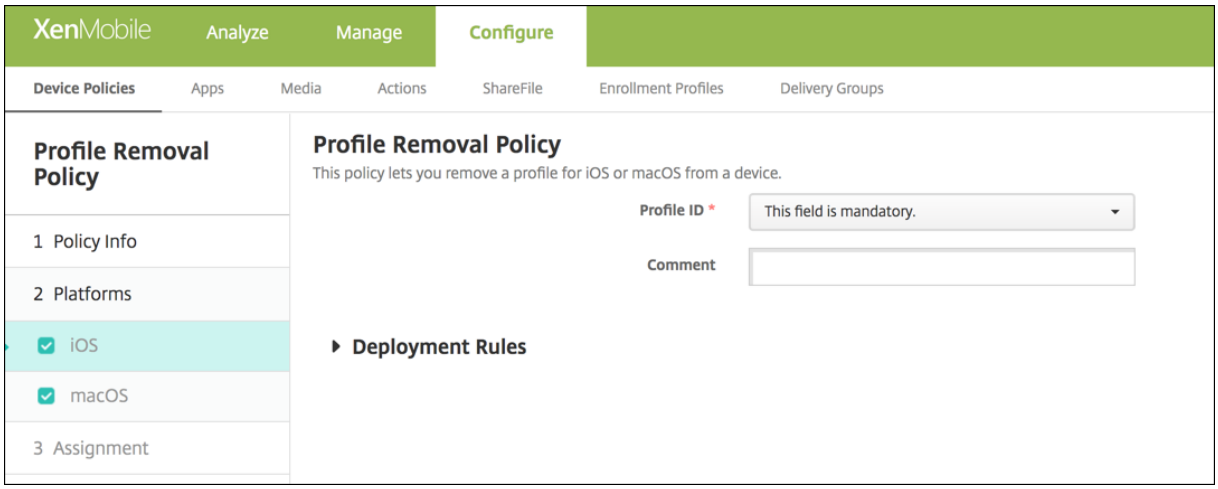
プロファイル削除デバイスポリシー

January 10, 2020

XenMobile で、アプリケーションプロファイル削除デバイスポリシーを作成することができます。ポリシーを展開すると、ユーザーの iOS デバイスまたは macOS デバイスからアプリプロファイルが削除されます。

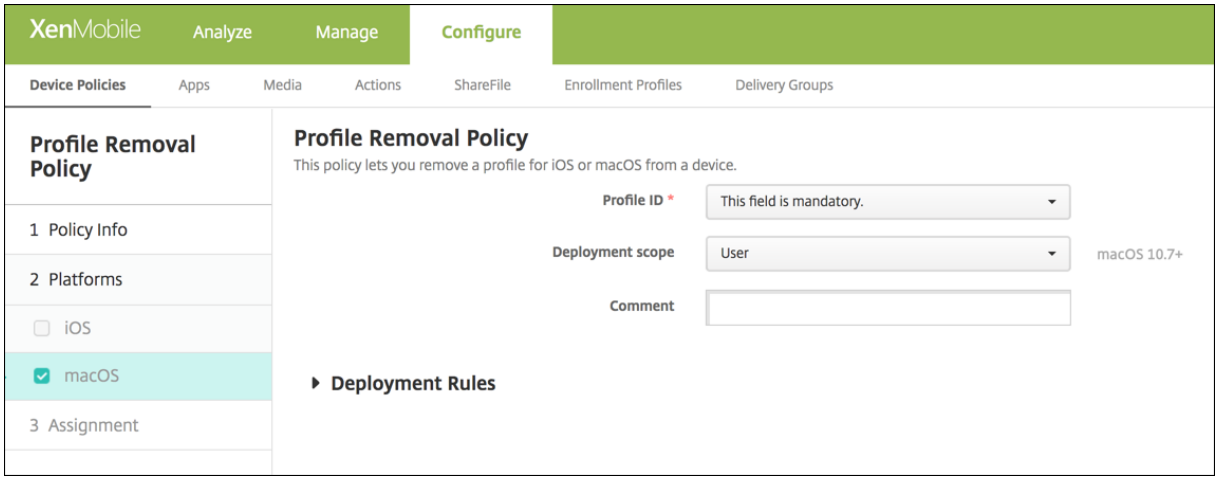
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- プロファイル **ID**: 一覧から、アプリプロファイル ID を選択します。このフィールドは必須です。
- コメント: 任意でコメントを入力します。

macOS 設定



- プロファイル **ID**: 一覧から、アプリプロファイル ID を選択します。このフィールドは必須です。
- 展開範囲: 一覧から、［ユーザー］または ［システム］ を選択します。デフォルトは ［ユーザー］ です。このオプションは macOS 10.7 以降でのみ使用できます。
- コメント: 任意でコメントを入力します。

プロビジョニングプロファイルデバイスポリシー

January 10, 2020

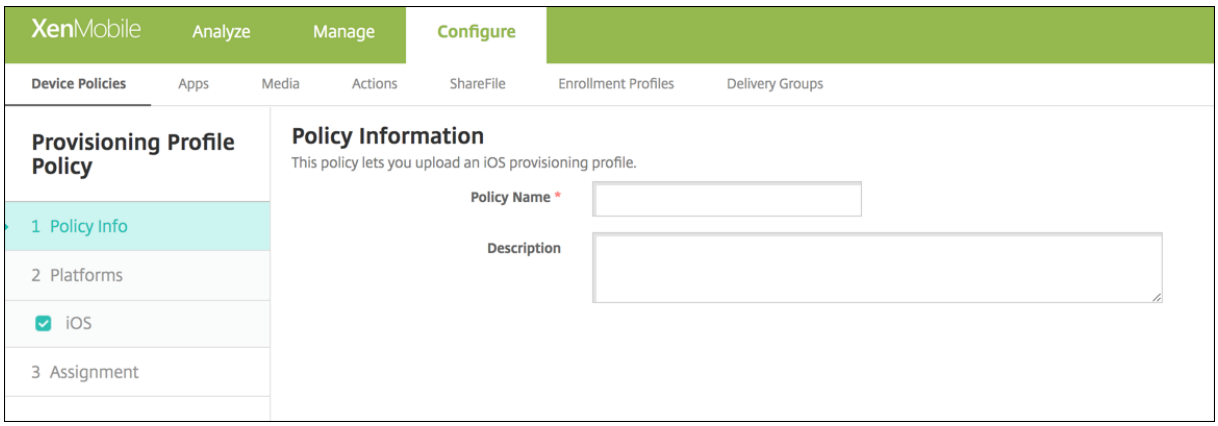
iOS エンタープライズアプリを開発しコード署名するときは、通常は、iOS デバイスで実行するアプリに Apple が求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。

プロビジョニングプロファイルの主な問題は、Apple Developer Portal で生成されてから 1 年で期限が切れるので、ユーザーによって登録されたすべての iOS デバイス上のすべてのプロビジョニングファイルの期限を追跡する必要があることです。期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信する、プロビジョニングプロファイルを Web ポータルに置いてダウンロードとインストールを可能にする、という 2 つの方法があります。これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Web ポータルにアクセスして適切なプロファイルをダウンロードしインストールすることを求めたりするので、エラーが発生する傾向があります。

このプロセスをユーザーが意識しないで済むように、XenMobile ではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。

プロビジョニングプロファイルポリシーを作成するには、プロビジョニングプロファイルのファイルを作成する必要があります。詳しくは、Apple Developer サイトの「開発プロビジョニングプロファイルを作成する」を参照してください。

iOS の設定



- **iOS** プロビジョニングプロファイル：［参照］ をクリックしてインポートするプロビジョニングプロファイルファイルの場所へ移動し、そのファイルを選択します。

プロビジョニングプロファイル削除デバイスポリシー

January 10, 2020

デバイスポリシーを使用して iOS プロビジョニングプロファイルを削除できます。プロビジョニングプロファイルについて詳しくは、「プロビジョニングプロファイルデバイスポリシー」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- **iOS** プロビジョニングプロファイル: 一覧から削除するプロビジョニングプロファイルを選択します。
- コメント: 必要に応じてコメントを追加します。

プロキシデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、Windows Mobile/CE および iOS 6.0 以降を実行しているデバイスのグローバル HTTP プロキシ設定を指定できます。グローバル HTTP プロキシポリシーはデバイスごとに 1 つのみ展開できます。

> 注:
>
> このポリシーを展開する前に、グローバル HTTP プロキシを設定するすべての iOS デバイスを必ず監視モードに設定してください。詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- プロキシ構成: ユーザーのデバイスでのプロキシの構成方法に関して、一覧から ［手動］ または ［自動］ を選択します。
  - ［手動］ を選択した場合は、次の設定を構成します。
    - プロキシサーバーのホスト名または **IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
    - プロキシサーバーのポート: プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - ユーザー名: 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - パスワード: 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［自動］ を選択した場合は、次の設定を構成します。

    * プロキシ **PAC URL**: プロキシ構成を定義する PAC ファイルの URL を入力します。
    * **PAC** に到達不能である場合は直接接続を許可: PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは［オン］です。このオプションは iOS 7.0 以降でのみ使用できます。
- キャプティブネットワークへのアクセスのためにプロキシのバイパスを許可: プロキシを使用せずにキャプティブネットワークにアクセスできるようにするかどうかを選択します。デフォルトは［オフ］です。
- ポリシー設定
  - ［ポリシーの削除］の横にある［日付を選択］または［削除までの期間（時）を指定］をクリックします。
  - ［日付を選択］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［ユーザーにポリシーの削除を許可］の一覧で、［常に］、［パスワードが必要］、［許可しない］のいずれかを選択します。
  - ［パスワードが必要］を選択した場合、［パスワードを削除］の横に必要なパスワードを入力します。

Windows Mobile/CE の設定

- ネットワーク: 一覧から、使用するネットワークの種類を選択します。デフォルトは［組み込みのオフィス］です。選択できるオプションは以下のとおりです:
  - ユーザー定義のオフィス
  - ユーザー定義のインターネット
  - 組み込みのオフィス
  - 組み込みのインターネット
- ネットワーク: 一覧から、使用するネットワーク接続プロトコルを選択します。デフォルトは［**HTTP**］です。選択できるオプションは以下のとおりです:
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- プロキシサーバーのホスト名または **IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
- プロキシサーバーのポート: プロキシサーバーのポート番号を入力します。このフィールドは必須です。デフォルトは **80** です。
- ユーザー名: 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
- パスワード: 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
- ドメイン名: 任意で、ユーザー名を入力します。
- 有効化: プロキシを有効にするかどうかを選択します。デフォルトは［オン］です。

レジストリデバイスポリシー

August 22, 2019

Windows Mobile/CE のレジストリには、アプリ、ドライバー、ユーザー設定、および構成設定に関するデータが格納されています。XenMobile では、Windows Mobile/CE デバイスを管理するためのレジストリキーおよび値を定義できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows Mobile/CE の設定

追加するレジストリキーまたはレジストリキーと値のペアごとに、［追加］ をクリックして以下の操作を行います：

- レジストリキーのパス: レジストリキーのフルパスを入力します。たとえば、「**HKEY_LOCAL_MACHINE\Software\Micro**
  と入力して、HKEY_LOCAL_MACHINE ルートキーから Windows キーまでのルートを指定します。
- レジストリ値の名前： レジストリキー値の名前を入力します。たとえば、「**ProgramFilesDir**」と入力して、レジストリキーのパス HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion に値の名前を追加します。このフィールドを空白のままにすると、レジストリキーと値のペアではなく、レジストリキーを追加することになります。
- 種類： 一覧から、値のデータの種類を選択します。デフォルトは ［**DWORD**］ です。選択できるオプションは以下のとおりです。
  - **DWORD**： 32 ビットの未署名の整数
  - 文字列： あらゆる文字列
  - 拡張文字列： %TEMP% や%USERPROFILE% のような環境変数を含めることができる文字列値
  - バイナリ： あらゆる任意のバイナリデータ
- 値： ［レジストリ値の名前］に関連付ける値を入力します。たとえば、ProgramFilesDir の値を指定するには、「**C:\Program Files**」と入力します。
- レジストリキー情報を保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。

リモートサポートデバイスポリシー

August 22, 2019

> 注：
>
> XenMobile Server のオンプレミス展開の場合：リモートサポートを使用すると、ヘルプデスクの担当者は

> 管理対象の Windows CE および Android モバイルデバイスをリモートで制御できます。画面のキャストは Samsung KNOX でのみサポートされています。
>
> リモートサポートはクラスター化されたオンプレミスの XenMobile Server 展開ではサポートされていません。
>
> 詳しくは、「サポートオプションとリモートサポート」を参照してください。

XenMobile でリモートサポートポリシーを作成して、サポート対象の Windows および Android デバイスへのリモートアクセスを行うことができます。次の 2 種類のサポートを構成できます。

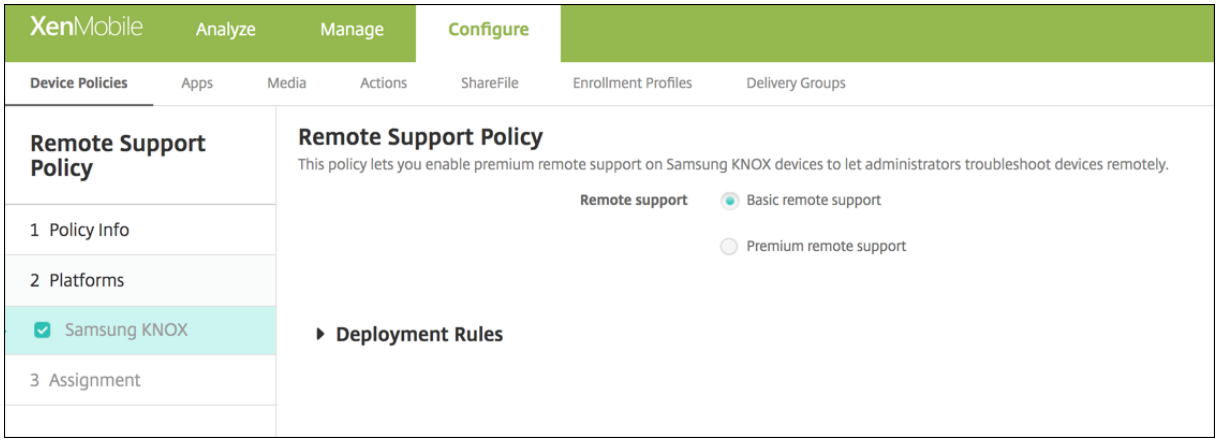
- [**Basic**] は、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率と CPU 使用率）、インストールされているソフトウェアフォルダーの内容など、デバイスに関する診断情報を表示できます。
- プレミアム: デバイスの画面をリモートで制御できます。次のような操作が可能です。
  - 色の制御（メインウィンドウまたは別の浮動ウィンドウ）
  - ヘルプデスクとユーザー間のボイスオーバー IP セッション（VoIP）の確立
  - 設定の構成
  - ヘルプデスクとユーザー間のチャットセッションの確立

このポリシーを実装するには、次の手順を実行する必要があります。

- XenMobile Remote Support アプリケーションを環境にインストールします。
- リモートサポートアプリトンネルを構成します。詳しくは、「アプリケーショントンネリングデバイスポリシー」を参照してください。
- このトピックの説明に従って Samsung KNOX のリモートサポートデバイスポリシーを構成します。
- アプリトンネルリモートサポートポリシーと、Samsung KNOX のリモートサポートポリシーの両方をユーザーのデバイスに展開します。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android と **Windows CE** の設定



- リモートサポート：［基本リモートサポート］ または ［プレミアムリモートサポート］をクリックします。デフォルトは ［基本リモートサポート］ です。

制限デバイスポリシー

October 25, 2019

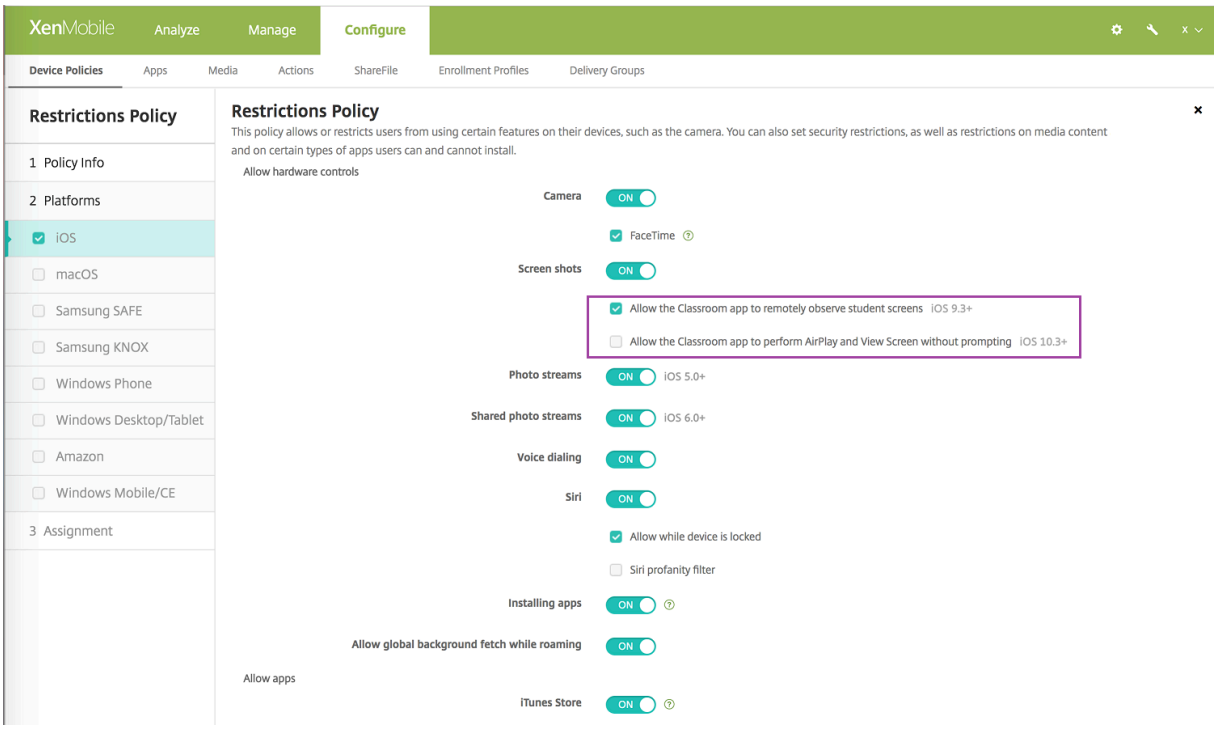
制限デバイスポリシーでは、ユーザーデバイスの特定の機能（カメラなど）を許可または制限します。また、セキュリティ制限、メディアコンテンツの制限、ユーザーがインストールできる（できない）アプリの種類の制限を設定できます。ほとんどの制限設定は、デフォルトでは ［オン］（許可） に設定されています。例外は、iOS セキュリティの強制機能とすべての Windows タブレット機能です。デフォルトで ［オフ］（制限） に設定されています。

Windows 10 RS2 Phone：Internet Explorer を無効にするカスタム XML ポリシーまたは制限ポリシーをスマートフォンに展開しても、Internet Explorer が有効なままです。この問題を解決するには、スマートフォンを再起動します。これはサードパーティ製品の問題です。

> ヒント：
>
> オプションで ［オン］ を選択した場合、ユーザーが該当する操作を実行、または該当する機能を使用できるようになります。次に例を示します：
>
> カメラ。［オン］ の場合、ユーザーはデバイスでカメラを使用できます。［オフ］ の場合、ユーザーはデバイスでカメラを使用できません。
>
> スクリーンショット。オンの場合、ユーザーはデバイスでスクリーンショットを取得できます。オフの場合、ユーザーはデバイスでスクリーンショットを取得できません。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



一部の iOS 制限ポリシー設定は、こちらおよび XenMobile Server コンソールの［制限ポリシー］ページで説明されているように、特定の iOS バージョンにのみ適用されます。

デバイスが Supervised モードで登録されると、すべての iOS 制限ポリシー設定が適用されます。iOS デバイスの Supervised モードへの設定については、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

一部の iOS 制限ポリシー設定は、デバイスがユーザー登録モードまたは監視対象外（完全 MDM）モードで登録されている場合にも適用されます。次の表は、iOS 13 以降を実行しているデバイスの設定が、ユーザー登録モードおよび監視対象外モードで使用できるかを示しています。

設定	ユーザー登録	監視対象外	監視
ハードウェアの制御を許可			
カメラ	いいえ	はい	はい
FaceTime	いいえ	いいえ（iOS 13 の新機能）	はい
スクリーンショット	はい	いいえ	はい
クラスルームアプリが生徒の画面をリモートで監視することを許可する	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視
プロンプトを表示せずにクラスルームアプリが AirPlay と画面表示を実行できるようにする	いいえ	いいえ	はい
フォトストリーム	いいえ	はい	はい
フォトストリームを共有	いいえ	はい	はい
音声ダイヤル	いいえ	はい	はい
Siri	はい	はい	はい
デバイスのロック中に許可	はい	はい	はい
Siri の不適切な単語フィルター	いいえ	いいえ	はい
アプリのインストール	いいえ	いいえ（iOS 13 の新機能）	はい
ローミング中にグローバルバックグラウンドフェッチを許可する	いいえ	はい	はい
アプリを許可			
iTunes ストア	いいえ	いいえ（iOS 13 の新機能）	はい
アプリ内課金	いいえ	はい	はい
購入時に iTunes パスワードを要求	いいえ	はい	はい
Safari	いいえ	いいえ（iOS 13 の新機能）	はい
オートフィル	いいえ	いいえ（iOS 13 の新機能）	はい
不正な Web サイトに対する警告を表示	はい	はい	はい
Javascript を有効化	いいえ	はい	はい
ポップアップをブロック	いいえ	はい	はい
Cookie を受け入れる	いいえ	はい	はい

設定	ユーザー登録	監視対象外	監視
ネットワーク **- iCloud** の操作を許可			
iCloud ドキュメントおよびデータ	いいえ	いいえ（iOS 13 の新機能）	はい
iCloud バックアップ	いいえ	はい	はい
iCloud フォトキーチェーン	いいえ	はい	はい
iCloud のフォトライブラリ	いいえ	はい	はい
セキュリティ **-** 強制			
バックアップを暗号化	はい	はい	はい
追跡型広告を制限	いいえ	はい	はい
最初の AirPlay ペアリングでパスコードを要求	はい	はい	はい
手首検出を使用するためのペアリングされた Apple Watch	はい	はい	はい
AirDrop を使用して管理対象のドキュメントを共有します	はい	はい	はい
セキュリティ **-** 許可			
信頼されていない SSL 証明書の受け入れ	いいえ	はい	はい
証明書信頼設定の自動更新	いいえ	はい	はい
管理対象アプリから非管理対象アプリへのドキュメントの移動	はい	はい	はい
非管理対象アプリによる管理対象アカウント連絡先の読み取り	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視
管理対象アプリによる非管理対象アカウント連絡先への書き込み	いいえ	いいえ	はい
非管理対象アプリから管理対象アプリへのドキュメントの移動	はい	はい	はい
診断データを Apple に送信	はい	はい	はい
Touch ID によるデバイスのロック解除	いいえ	はい	はい
ロック時に Passbook 通知を表示	いいえ	はい	はい
Handoff	いいえ	はい	はい
管理対象アプリの iCloud 同期	はい	はい	はい
エンタープライズブックのバックアップ	はい	はい	はい
エンタープライズブックのメモとハイライトの同期	はい	はい	はい
Spotlight でインターネット検索結果を表示	いいえ	はい	はい
エンタープライズアプリケーションを信頼する	いいえ	はい	はい
監視対象のみの設定 - 許可			
すべてのコンテンツと設定を消去	いいえ	いいえ	はい
制限の構成	いいえ	いいえ	はい
ポッドキャスト	いいえ	いいえ	はい
構成プロファイルのインストール	いいえ	いいえ	はい
フィンガープリントの変更	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視
デバイスからアプリをインストールします	いいえ	いいえ	はい
キーボードショートカット	いいえ	いいえ	はい
ペアリングされた Apple Watch	いいえ	いいえ	はい
パスコードの変更	いいえ	いいえ	はい
デバイス名の変更	いいえ	いいえ	はい
壁紙の変更	いいえ	いいえ	はい
自動的にアプリをダウンロードします	いいえ	いいえ	はい
AirDrop	いいえ	いいえ	はい
iMessage	いいえ	いいえ	はい
Siri にユーザー生成コンテンツを表示	いいえ	いいえ	はい
iBooks	いいえ	いいえ	はい
アプリの削除	いいえ	はい	はい
ゲームセンター	いいえ	いいえ（iOS 13 の新機能）	はい
友達を追加	いいえ	いいえ	はい
マルチプレーヤーゲーム	いいえ	いいえ（iOS 13 の新機能）	はい
アカウント設定の変更	いいえ	いいえ	はい
アプリの携帯ネットワークデータ設定の変更	いいえ	いいえ	はい
アプリの携帯ネットワークデータ設定の変更	いいえ	いいえ	はい
［友達を探す］設定の変更	いいえ	いいえ	はい
Configurator 以外のホストとのペアリング	いいえ	いいえ	はい
予測キーボード	いいえ	いいえ	はい
キーボード自動修正	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視
キーボードスペルチェック	いいえ	いいえ	はい
定義参照	いいえ	いいえ	はい
単一のアプリバンドル **ID**			
ニュース	いいえ	いいえ	はい
Apple Music サービス	いいえ	いいえ	はい
iTunes ラジオ	いいえ	いいえ	はい
通知の変更	いいえ	いいえ	はい
アプリ使用の制限	いいえ	いいえ	はい
診断データの送信の変更	いいえ	いいえ	はい
Bluetooth の変更	いいえ	いいえ	はい
ディクテーションを許可	いいえ	いいえ	はい
WiFi ポリシーでインストールされた WiFi ネットワークのみに参加する	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリが AirPlay と画面表示を実行できるようにする	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリがアプリとデバイスをロックできるようにする	いいえ	いいえ	はい
プロンプトを表示せずにクラスルームアプリのクラスに自動的に参加する	いいえ	いいえ	はい
AirPrint を許可	いいえ	いいえ	はい
AirPrint 資格情報のキーチェーンへの保存を許可する	いいえ	いいえ	はい
iBeacon を使用した AirPrint プリンターの検出を許可する	いいえ	いいえ	はい

設定	ユーザー登録	監視対象外	監視
信頼された証明書がある出力先に対してのみ AirPrint を許可する	いいえ	いいえ	はい
VPN 構成の追加	いいえ	いいえ	はい
携帯の通信プラン設定の変更	いいえ	いいえ	はい
システムアプリの削除	いいえ	いいえ	はい
近くの新しいデバイスをセットアップ	いいえ	いいえ	はい
USB 制限モードを許可	いいえ	いいえ	はい
ソフトウェア更新の延期を強制する	いいえ	いいえ	はい
ソフトウェア更新の強制延期	いいえ	いいえ	はい
クラスを離れる時の許可の要求を強制する	いいえ	いいえ	はい
自動的な日付と時刻を強制	いいえ	いいえ	はい
パスワードの自動入力	いいえ	いいえ	はい
パスワード近接要求	いいえ	いいえ	はい
パスワード共有	いいえ	いいえ	はい
セキュリティ - ロック画面に表示			
コントロールセンター	はい	はい	はい
通知	はい	はい	はい
今日ビュー	はい	はい	はい
メディアコンテンツ - 許可			
不適切な音楽、Podcast、iTunes U コンテンツ	いいえ	いいえ（iOS 13 の新機能）	はい
iBooks の不適切な性的コンテンツ	いいえ	はい	はい

設定	ユーザー登録	監視対象外	監視
レーティング地域	いいえ	はい	はい
ムービー	いいえ	はい	はい
テレビ番組	いいえ	はい	はい
アプリ	いいえ	はい	はい

- ハードウェアの制御を許可
  - カメラ: ユーザーがデバイスでカメラを使用できるようにします。
    - **FaceTime**: ユーザーがデバイスで FaceTime を使用できるようにします。監視対象の iOS デバイス向けです。
  - スクリーンショット: ユーザーがデバイスでスクリーンショットを撮れるようにします。
    - クラスルームアプリが生徒の画面をリモートで監視することを許可する: この制限が選択されていない場合、講師はクラスルームアプリを使用してリモートで生徒の画面を監視することはできません。デフォルト設定が選択されている場合、講師はクラスルームアプリを使用して生徒の画面を監視できます。［プロンプトを表示せずにクラスルームアプリが **AirPlay** と画面表示を実行できるようにする］ の設定では、講師に権限を与えるためのプロンプトを生徒に表示するかどうかを決めます。監視対象の iOS デバイス向けです。
    - プロンプトを表示せずにクラスルームアプリが **AirPlay** と画面表示を実行できるようにする: この制限が選択されている場合、講師は生徒のデバイスで AirPlay と画面表示を実行でき、権限を求めるプロンプトは表示されません。デフォルト設定では、選択解除されています。監視対象の iOS デバイス向けです。
  - フォトストリーム: MyPhotoStream を使い、iCloud を介してすべての iOS デバイスでユーザーが写真を共有できるようにします。
  - フォトストリームを共有: iCloud Photo Sharing を使い、仕事仲間、友人、および家族とユーザーが写真を共有できるようにします。
  - 音声ダイヤル: ユーザーデバイスで音声ダイヤルを可能にします。
  - **Siri**: ユーザーが Siri を使用できるようにします。
    - デバイスのロック中に許可: デバイスがロックされている間にユーザーが Siri を使用できるようにします。
    - **Siri** の不適切な単語フィルター: Siri の不適切な単語フィルターを有効にします。デフォルトではこの機能は制限されており、不適切な言葉はフィルタリングされません。
      Siri とセキュリティについて詳しくは、「Siri とディクテーションのポリシー」を参照してください。
  - アプリのインストール: ユーザーがアプリをインストールできるようにします。監視対象の iOS デバイス向けです。
  - ローミング中にグローバルバックグラウンドフェッチを許可する: デバイスのローミング中に iCloud とのメールアカウントの自動同期を許可するかを設定します。［オフ］ の場合、iOS スマートフォンの

ローミング中はグローバルバックグラウンドフェッチが無効になります。デフォルトは ［オン］ です。

- アプリを許可
  - **iTunes Store**: ユーザーが iTunes Store へアクセスできるようにします。監視対象の iOS デバイス向けです。
  - アプリ内課金: ユーザーがアプリ内課金で購入できるようにします。
    * 購入時に **iTunes** パスワードを要求: アプリ内購入時にパスワードを求めます。デフォルトではこの機能は制限されており、アプリ内での購入ではパスワードは必要ありません。
  - **Safari**: ユーザーが Safari にアクセスできるようにします。監視対象の iOS デバイス向けです。
    * オートフィル: ユーザーが Safari でユーザー名とパスワードの自動入力をセットアップできるようにします。
    * 不正な **Web** サイトに対する警告を表示: この設定が有効で、ユーザーがフィッシング詐欺の疑いのある Web サイトにアクセスした場合、Safari はユーザーに警告します。デフォルトではこの機能は制限されており、警告が発せられません。
    * **Javascript** を有効化: JavaScript を Safari で実行できます。
    * ポップアップをブロック: Web サイトの閲覧中にポップアップをブロックします。デフォルトではこの機能は制限されており、ポップアップはブロックされません。
  - **Cookie** を受け入れる: 許可する cookie を設定します。一覧で、cookie を許可または制限するオプションを選択します。デフォルトのオプションは ［常時］ で、Safari ですべての Web サイトの cookie の保存を許可します。ほかには、［現在の **Web** サイトのみ］、［許可しない］、および ［訪問したサイトからのみ］ というオプションがあります。
- ネットワーク **- iCloud** の操作を許可
  - **iCloud** ドキュメントおよびデータ: ユーザーがドキュメントとデータを iCloud へ同期できるようにします。監視対象の iOS デバイス向けです。
  - **iCloud** バックアップ: ユーザーが iCloud へデバイスをバックアップできるようにします。
  - **iCloud** キーチェーン: ユーザーが、iCloud キーチェーンにパスワード、Wi-Fi ネットワーク、クレジットカードなどの情報を保存できるようにします。
  - **iCloud** のフォトライブラリ: ユーザーが iCloud の写真ライブラリにアクセスできるようにします。
- セキュリティ **-** 強制

  デフォルトでは次の機能が制限され、有効になっているセキュリティ機能はありません。
  - バックアップを暗号化: 暗号化のため iCloud に強制的にバックアップします。
  - 追跡型広告を制限: ターゲティング広告の追跡をブロックします。
  - 最初の **AirPlay** ペアリングでパスコードを要求: AirPlay 対応デバイスで AirPlay を使用する前に、ワンタイムオンスクリーンコードで検証するように求めます。
  - 手首検出を使用するためのペアリングされた **Apple Watch**: 手首検出を使用するために Apple Watch のペアリングを求めます。
  - **AirDrop** を使用して管理対象のドキュメントを共有します: AirDrop アクセスは、管理対象オプションです。このオプションを ［オン］ に設定すると、監視対象デバイスが AirDrop を使用して近くの iOS

デバイスとデータおよびメディアを共有できるようになります。

- セキュリティ - 許可
  - 信頼されていない **SSL** 証明書の受け入れ: Web サイトの信頼されていない SSL 証明書をユーザーが承認できるようにします。
  - 証明書信頼設定の自動更新: 信頼された機関からの証明書を自動的に更新できます。
  - 管理対象アプリから非管理対象アプリへのドキュメントの移動: ユーザーが、管理されている（企業）アプリから管理されていない（個人）アプリへのデータを移動できるようにします。
  - 非管理対象アプリから管理対象アプリへのドキュメントの移動: ユーザーが管理されていない（個人）アプリから管理されている（企業）アプリへデータを移動できるようにします。
  - 診断データを **Apple** に送信: ユーザーのデバイスに関する匿名診断データの Apple への送信を許可します。
  - **Touch ID** によるデバイスのロック解除: ユーザーがフィンガープリントを使ってデバイスのロックを解除できるようにします。
  - ロック時に **Passbook** 通知を表示: ロック画面での Passbook 通知の表示を許可します。
  - **Handoff**: ユーザーが、ある iOS デバイスから近くにある別の iOS デバイスへアクティビティを転送できるようにします。
  - 管理対象アプリの **iCloud** 同期: ユーザーが、管理されているアプリを iCloud と同期できるようにします。
  - エンタープライズブックのバックアップ: エンタープライズブックの iCloud へのバックアップを許可します。
  - エンタープライズブックのメモとハイライトの同期: ユーザーがエンタープライズブックに追加したメモやハイライトを iCloud と同期できるようにします。
  - **Spotlight** でインターネット検索結果を表示: Spotlight で、デバイス同様にインターネットから検索結果を表示できるようにします。
  - エンタープライズアプリを信頼する: エンタープライズアプリケーションを信頼できるようにします。
  - 非管理対象アプリによる管理対象アカウント連絡先の読み取り: オプション。［管理対象アプリから非管理対象アプリへのドキュメントの移動］ が無効になっている場合にのみ利用できます。このポリシーを有効にすると、非管理対象アプリが管理対象アカウントの連絡先からデータを読み取ることができるようになります。デフォルトは ［オフ］ です。iOS 12 以降で利用できます。
  - 管理対象アプリによる非管理対象アカウント連絡先への書き込み: オプション。有効にすると、管理対象アプリによる非管理対象アカウントの連絡先への書き込みを許可します。［管理対象アプリから非管理対象アプリへのドキュメントの移動］ を有効にすると、この制限は有効になりません。デフォルトは［オフ］ です。iOS 12 以降で利用できます。
- 監視対象のみの設定 - 許可

  これらの設定は、監視対象のデバイスにのみ適用されます。iOS デバイスを Supervised モードに設定する手順について詳しくは、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。
  - すべてのコンテンツと設定を消去: ユーザーがデバイスからすべてのコンテンツと設定を消去できるよ

うにします。

- 制限の構成: ユーザーがデバイスで保護者による制限を構成できるようにします。
- ポッドキャスト: ユーザーがポッドキャストをダウンロードおよび同期できるようにします。
- 構成プロファイルのインストール: 管理者が展開した構成プロファイル以外の構成プロファイルを、ユーザーがインストールできるようにします。
- フィンガープリントの変更: ユーザーが Touch ID フィンガープリントを変更または削除できるようにします。
- デバイスからアプリをインストールします: ユーザーがアプリをインストールできるようにします。
- キーボードショートカット: ユーザーが使用頻度の高い単語やフレーズのカスタムキーボードショートカットを作成できるようにします。
- ペアリングされた **Apple Watch**: ユーザーが Apple Watch と監視対象デバイスをペアリングできるようにします。
- パスコードの変更: ユーザーが監視対象デバイスでパスコードを変更できるようにします。
- デバイス名の変更: ユーザーがデバイスの名前を変更できるようにします。
- 壁紙の変更: ユーザーがデバイスの壁紙を変更できるようにします。
- 自動的にアプリをダウンロードします: アプリのダウンロードを許可します。
- **AirDrop**: ユーザーが写真、ビデオ、Web サイト、場所、およびそれ以外のものを近くの iOS デバイスで共有できるようにします。
- **iMessage**: ユーザーが Wi-Fi を使って iMessage を送信できるようにします。
- **Siri** にユーザー生成コンテンツを表示: Web のユーザー生成コンテンツを Siri でクエリできるようにします。ユーザー生成コンテンツは、従来のジャーナリストではなく、一般のユーザーが作成したものです。たとえば、Twitter や Facebook に見られるコンテンツは、ユーザー生成コンテンツです。
- **iBooks**: ユーザーが iBooks アプリを使用できるようにします。
- アプリの削除: ユーザーがデバイスからアプリを削除できるようにします。
- **Game Center**: ユーザーがデバイスの Game Center を介してオンラインゲームをプレイできるようにします。
  * 友達を追加: ユーザーが友人に通知を送信してゲームをプレイできるようにします。
  * マルチプレーヤーゲーム: ユーザーがデバイス上でマルチプレーヤーゲームを起動できるようにします。
- アカウント設定の変更: ユーザーがデバイスのアカウント設定を変更できるようにします。
- アプリの携帯データネットワーク設定の変更: 携帯データネットワークをアプリがどのように使用するのか、ユーザーが変更できるようにします。

- ［友達を探す］設定の変更： 友達を探す設定をユーザーが変更できるようにします。
- **Configurator** 以外のホストとのペアリング： ユーザーデバイスがペアリングできるデバイスを管理者が制御できるようにします。この設定を無効にすると、Apple Configurator を実行している監視中のホスト以外とは、ペアリングできなくなります。監視中のホストの証明書が構成されていない場合は、すべてのペアリングが無効です。
- 予測キーボード： ユーザーデバイスで、キーボードからの入力時に候補となる単語を予測変換できるようにします。ユーザーに候補の単語を表示しない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- キーボード自動修正： ユーザーデバイスでキーボードの自動修正を使用できるようにします。ユーザーに自動修正を適用しない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- キーボードスペルチェック： ユーザーデバイスで入力中にスペルチェックを使用できるようにします。ユーザーにスペルチェッカーへアクセスさせない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- 定義参照： ユーザーデバイスで入力中に定義の検索を使用できるようにします。ユーザーに入力時での定義の検索をできるようにしない、管理のための標準化されたテストといった状況では、このオプションを無効にします。
- 単一のアプリバンドル **ID**： デバイス上のコントロールを維持し、ほかのアプリや機能との相互作用を防ぐことができるアプリの一覧を作成します。
  アプリを追加するには、［追加］ をクリックし、アプリ名を入力して ［保存］ をクリックします。追加するアプリごとにこの手順を繰り返します。
- **News**： ユーザーが News アプリを使用できるようにします。
- **Apple Music** サービス：ユーザーが Apple Music サービスを使用できるようにします。Apple Music サービスを許可しない場合、Music アプリはクラシックモードで動作します。
- **iTunes Radio**： ユーザーが iTunes Radio を使用できるようにします。
- 通知の変更： ユーザーが通知設定を変更できるようにします。
- パスワードの自動入力： オプション。無効にすると、ユーザーはパスワードの自動入力または自動強力パスワード機能を使用できません。デフォルトは ［オン］ です。iOS 12 以降で利用できます。
- パスワード近接要求： オプション。無効にすると、ユーザーのデバイスは近くのデバイスにパスワードを要求しません。デフォルトは ［オン］ です。iOS 12 以降で利用できます。
- パスワード共有： オプション。無効にすると、ユーザーは Airdrop パスワード機能を使用してパスワードを共有できません。デフォルトは ［オン］ です。iOS 12 以降で利用できます。
- アプリ使用の制限： 指定したバンドル ID に基づいて、ユーザーにすべてのアプリの使用を許可するか、またはアプリの使用を個別に許可または禁止できます。監視対象のデバイスにのみ適用されます。

> 注:
>
> iOS 11 以降、アプリの制限で利用できるポリシーが変更されました。適切な iOS アプリケーションバンドルを制限することで、設定アプリと電話アプリへのアクセスを削除することができなくなりました。

いくつかのアプリをブロックするように制限デバイスポリシーを構成して展開した後で、これらのアプリの一部またはすべてを許可する必要が生じた場合、制限デバイスポリシーを変更して展開しても制限は変更されません。これは、iOS では変更内容が iOS プロファイルに適用されないためです。変更内容を適用するには、プロファイルの削除ポリシーを使用して該当する iOS プロファイルを削除してから、更新した制限デバイスポリシーを展開します。

この設定を ［一部のアプリのみ許可］ に変更する場合: このポリシーを展開する前に、Apple DEP を使用して登録したデバイスのユーザーに、セットアップアシスタントから Apple アカウントにサインインするよう指示してください。それ以外の場合、ユーザーが Apple アカウントにサインインして許可されたアプリにアクセスするには、各自のデバイスで 2 要素認証を無効にする必要があります。

- 診断データの送信の変更: ユーザーが ［設定］**>**［診断と使用状況］ ペインで診断データの送信とアプリ分析に関する設定を変更できるようにします。
- **Bluetooth** の変更: ユーザーが Bluetooth の設定を変更できるようにします。
- ディクテーションを許可: 監視のみ。この制限が ［オフ］ に設定されている場合、ディクテーションを使用した入力は許可されません。デフォルトでは ［オン］ になっています。
- **Wi-Fi** ポリシーでインストールされた **Wi-Fi** ネットワークのみに参加する: オプション。監視のみ。この制限が ［オン］ に設定されている場合、構成プロファイルを使用して設定されたデバイスのみが Wi-Fi ネットワークに接続できます。デフォルトでは ［オフ］ になっています。
- プロンプトを表示せずにクラスルームアプリがアプリとデバイスをロックできるようにする: この制限が ［オン］ に設定されている場合、クラスルームアプリはユーザープロンプトを表示せず自動的に、アプリに対してユーザーデバイスをロックし、ユーザーデバイスをロックします。デフォルトでは ［オフ］ になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- プロンプトを表示せずにクラスルームアプリのクラスに自動的に参加する: この制限が ［オン］ に設定されている場合、クラスルームアプリはユーザーにプロンプトを表示せずに自動的にクラスに参加します。デフォルトでは ［オフ］ になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- **AirPrint** を許可: この制限が ［オフ］ に設定されている場合、ユーザーは AirPrint で印刷できません。デフォルトでは ［オン］ になっています。この制限が ［オン］ の場合、さらに次の制限が表示されます。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
  - **AirPrint** 資格情報のキーチェーンへの保存を許可する: この制限が選択されていない場合、AirPrint のユーザー名とパスワードはキーチェーンに保存されません。デフォルト設定では選択されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。

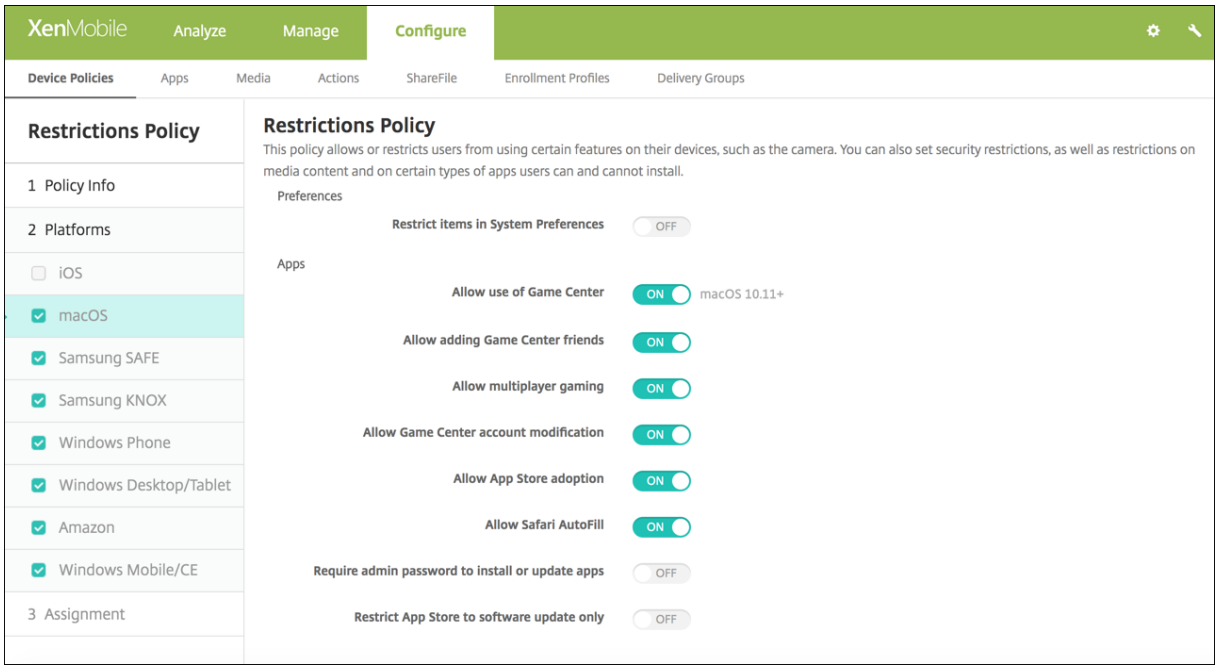
    * **iBeacons** を使用した **AirPrint** プリンターの検出を許可する: この制限が選択されていない場合、AirPrint プリンターの iBeacon 検出は無効になります。これにより、偽の AirPrint Bluetooth ビーコンのネットワークトラフィックがフィッシングされるのを防止します。デフォルト設定では選択されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
    * 信頼された証明書がある出力先に対してのみ **AirPrint** を許可する: この制限が選択されている場合、ユーザーは、信頼された機関からの証明書がある出力先にのみ AirPrint を使用して印刷できます。デフォルト設定では、選択解除されています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。

- **VPN** 構成の追加: この制限が ［オフ］ に設定されている場合、ユーザーは VPN 構成を作成できません。デフォルトでは ［オン］ になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- 携帯の通信プラン設定の変更: この制限が ［オフ］ に設定されている場合、ユーザーは携帯の通信プラン設定を変更できません。デフォルトでは ［オン］ になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- 日時の自動設定を強制する: 監視対象デバイスの日時を自動で設定できます。［オン］ の場合、デバイスユーザーは ［全般］ **>** ［日付と時刻］ で ［自動的に設定］ をオフにできません。デバイスのタイムゾーンは、デバイスが現在位置を特定できる場合にのみ更新されます。つまり、デバイスが移動体通信ネットワークまたは Wi-Fi に接続しており、位置情報サービスが有効になっている場合のみです。デフォルトは ［オフ］ です。iOS 12 以降の監視対象デバイスでのみ利用できます。
- システムアプリの削除: この制限が ［オフ］ に設定されている場合、ユーザーはデバイスからシステムアプリを削除できません。デフォルトでは ［オン］ になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- 近くの新しいデバイスをセットアップ: この制限が［オフ］に設定されている場合、ユーザーは近くの新しいデバイスを設定できません。デフォルトでは［オン］になっています。iOS 11（最小バージョン）を実行している監視対象デバイスの場合。
- **USB** 制限モードを許可:［オフ］ の場合、デバイスはロックされた状態でも常に USB アクセサリーに接続できます。デフォルトは ［オン］ です。iOS 11.3 以降の監視対象デバイスでのみ利用できます。
- ソフトウェア更新の延期を強制する: ［オン］ の場合、ソフトウェアの更新がユーザーに表示される時期が延期されます。この制限が設定されている場合、ソフトウェアの更新がリリースされてから指定された日数が経過するまで、ソフトウェアの更新は表示されません。デフォルトは ［オフ］ です。iOS 11.3 および macOS 10.13.4 以降で利用できます。
- ソフトウェア更新の強制延期期間（日）: デバイス上でソフトウェアの更新を遅らせる日数を指定できます。最大延期日数は **90** 日です。デフォルトは **30** 日です。iOS 11.3 および macOS 10.13.4 以降で利用できます。
- クラスルームを離れるときの許可の要求を強制する: ［オン］ の場合、クラスルームの管理対象外コー

スに登録した学生は、コースを離れるときに教師の許可を求める必要があります。デフォルトは ［オフ］ です。iOS 11.3 以降で利用できます。

- セキュリティ **-** ロック画面に表示
  - コントロールセンター: ロック画面のコントロールセンターへアクセスできるようにします。コントロールセンターでは、機内モード、Wi-Fi、Bluetooth、おやすみモード、画面の向きをロックといった設定をユーザーが簡単に変更できます。
  - 通知: ロック画面上へ通知できるようにします。
  - 今日ビュー: 天気や当日の予定といった情報を表示する今日の表示をロック画面上で有効にします。
- メディアコンテンツ **-** 許可
  - 不適切な音楽、**Podcast**、**iTunes U** コンテンツ: ユーザーのデバイスで成人向けのコンテンツを許可します。
  - **iBooks** の不適切な性的コンテンツ: iBooks から成人向けのコンテンツをダウンロードできるようにします。
  - レーティング地域: ペアレンタルコントロールのレートを取得する地域を設定します。一覧では、国をクリックするとレート地域が設定されます。デフォルトは ［米国］ です。
  - ムービー: ユーザーのデバイスでムービーを操作できるかどうかを設定します。ムービーの操作が許可される場合は、オプションでムービーのレートレベルを設定します。一覧で、デバイスでムービーを許可または制限するオプションをクリックします。デフォルトは［すべてのムービーを許可］です。
  - テレビ番組: ユーザーのデバイスでテレビ番組を操作できるかどうかを設定します。テレビ番組の操作が許可される場合は、オプションでテレビ番組のレートレベルを設定します。一覧で、デバイスでテレビ番組を許可または制限するオプションをクリックします。デフォルトは［すべてのテレビ番組を許可］です。
  - アプリ: ユーザーのデバイスでアプリを操作できるかどうかを設定します。アプリの操作が許可される場合は、オプションでムービーのレートレベルを設定します。一覧で、デバイスでアプリを許可または制限するオプションをクリックします。デフォルトは［すべてのアプリを許可］です。
- ポリシー設定
  - ポリシーの削除: このポリシーをデバイスから削除するタイミングを選択できます。［日付を選択］ を選択すると、日付ピッカーを使用してポリシーを削除するタイミングを選択できます。［削除までの期間（時間）を指定］ を選択すると、ポリシーが削除されるまでの時間数を入力できます。
  - ユーザーにポリシーの削除を許可: ユーザーが制限ポリシーを削除できるようにします。オプションは、［常に］、［パスコードを要求］、または ［なし］ です。
  - プロファイルの対象: 制限ポリシーを システムまたは ユーザーに適用できます。

macOS 設定



- 基本設定
  - システム環境設定のアイテムの制限： システム環境設定へのユーザーのアクセスを許可または制限します。デフォルトは ［オフ］ で、ユーザーにはシステム環境設定へのフルアクセス権が付与されます。有効にした場合は、次の設定を構成します。
    * システム環境設定ペイン： 選択した設定を有効にするのか、無効にするのかを選択します。デフォルトではすべての設定が有効になるように、すなわち ［オン］ に設定されています。
      - ユーザーおよびグループ
      - 一般
      - アクセシビリティ
      - App Store
      - ソフトウェアの更新
      - Bluetooth
      - CD と DVD
      - 日時
      - デスクトップとスクリーンセーバー
      - ディスプレイ
      - ドック
      - エネルギーセーバー
      - 拡張機能
      - ファイバーチャネル
      - iCloud
      - インク

- インターネットアカウント
- キーボード
- 言語とテキスト
- Mission Control
- マウス
- ネットワーク
- 通知
- ペアレンタルコントロール
- プリンターとスキャナー
- プロファイル
- セキュリティとプライバシー
- 共有
- サウンド
- ディクテーションと音声入力
- Spotlight
- 起動ディスク
- Time Machine
- トラックパッド
- Xsan

- アプリ
  - **Game Center** の使用を許可： ユーザーが Game Center を介してオンラインゲームをプレイできるようにします。デフォルトは ［オン］ です。
  - **Game Center** の友達の追加を許可： ユーザーが友人に通知を送信してゲームをプレイできるようにします。デフォルトは ［オン］ です。
  - マルチプレーヤーゲームを許可： ユーザーがマルチプレーヤーゲームを開始できるようにします。デフォルトは ［オン］ です。
  - **Game Center** のアカウント変更を許可： ユーザーが各自の Game Center アカウント設定を変更できるようにします。デフォルトは ［オン］ です。
  - **App Store** の採用を許可： OS X に既に存在するアプリの App Store への登録を許可または制限します。デフォルトは ［オン］ です。
  - **Safari** の自動入力を許可： Safari に保存されているパスワード、アドレス、およびその他の基本情報が自動的に Web サイトのフィールドに入力されるようにします。デフォルトは ［オン］ です。
  - アプリのインストールまたはアップデートで管理者パスワードを必須にする： アプリをインストールまたは更新するときに管理者のパスワードを必須にします。デフォルトは ［オフ］ で、管理者のパスワードが不要であることを意味します。
  - **App Store** をソフトウェアの更新のみに制限： App Store を更新のみに制限します。つまり、［アップデート］以外の App Store のタブはすべて無効になります。デフォルトは ［オフ］ で、App Store へのフルアクセスが許可されます。
  - 開くのを許可するアプリ制限ポリシー： ユーザーが使用できるアプリを制限または許可します。デフォ

ルトは［オフ］で、すべてのアプリの使用が許可されます。有効にした場合は、次の設定を構成します:

  * 許可するアプリ:［追加］ をクリックして、起動を許可するアプリの名前およびバンドル ID を入力し、［保存］ をクリックします。起動を許可するアプリごとに、この手順を繰り返します。
  * 許可しないフォルダー:［追加］ をクリックして、ユーザーアクセスを制限するフォルダーまでのファイルパス（例: /Applications/Utilities）を入力し、［保存］ をクリックします。ユーザーにアクセスできないようにするすべてのフォルダーについて、この手順を繰り返します。
  * 許可するフォルダー:［追加］ をクリックして、ユーザーアクセスを許可するフォルダーまでのファイルパスを入力し、［保存］ をクリックします。ユーザーにアクセスできるようにするすべてのフォルダーについて、この手順を繰り返します。

- ウィジェット
  - 以下のダッシュボードウィジェットのみ実行を許可: ユーザーが実行できるダッシュボードウィジェット（世界時計、計算機など）を許可または制限します。デフォルトは ［オフ］ で、ユーザーはすべてのウィジェットを実行できます。有効にした場合は、次の設定を構成します:
    * 許可するウィジェット:［追加］ をクリックして、実行を許可するウィジェットの名前および ID を入力し、［保存］ をクリックします。ダッシュボードでの実行を許可するウィジェットごとに、この手順を繰り返します。
- メディア
  - **AirDrop** を許可: ユーザーが写真、ビデオ、Web サイト、場所、およびそれ以外のものを近くの iOS デバイスで共有できるようにします。
- 共有
  - 新しい共有サービスを自動で有効にする: 共有サービスを自動的に有効にするかどうかを選択します。
  - メール: 共有メールボックスを許可するかどうかを選択します。
  - **Facebook**: 共有 Facebook アカウントを許可するかどうかを選択します。
  - ビデオサービス **- Flickr**、**Vimeo**、**Tudou**、**Youku**: 共有ビデオサービスを許可するかどうかを選択します。
  - **Aperture** に追加: Aperture への追加を行う共有機能を許可するかどうかを選択します。
  - **Sina Weibo**: 共有 Sina Weibo 投稿アカウントを許可するかどうかを選択します。
  - **Twitter**: 共有 Twitter アカウントを許可するかどうかを選択します。
  - メッセージ: メッセージへの共有アクセスを許可するかどうかを選択します。
  - **iPhoto** に追加: iPhoto への追加を行う共有機能を許可するかどうかを選択します。
  - リーディングリストに追加: リーディングリストへの追加を行う共有機能を許可するかどうかを選択します。
  - **AirDrop**: 共有 AirDrop アカウントを許可するかどうかを選択します。
- 機能
  - デスクトップ画像をロック: ユーザーがデスクトップの画像を変更できるかどうかを選択します。デフォルトは ［オフ］ で、ユーザーがデスクトップの画像を変更できることを意味します。
  - カメラの使用を許可: ユーザーが Mac でカメラを使用できるかどうかを選択します。デフォルトは［オフ］ で、ユーザーがカメラを使用できないことを意味します。
  - **Apple Music** を許可する: ユーザーが Apple Music サービスを使用できるようにします（macOS

10.12 以降)。Apple Music サービスを許可しない場合、Music アプリはクラシックモードで動作します。監視対象のデバイスにのみ適用されます。デフォルトは ［オン］ です。

- **Spotlight** の検索候補を許可: ユーザーが［Spotlight の検索候補］を使用して Mac を検索したり、［Spotlight の検索候補］にインターネット、iTunes、App Store の項目を表示したりできるかどうかを選択します。デフォルトは ［オフ］ で、ユーザーは［Spotlight の検索候補］を使用できません。
- 検索を許可: ユーザーがコンテキストメニューまたは Spotlight 検索メニューで単語の定義を検索できるかどうかを選択します。デフォルトは［オフ］で、ユーザーは Mac で検索機能を使用できません。
- ローカルアカウントでの **iCloud** パスワードの使用を許可: ユーザーが各自の Apple ID および iCloud パスワードを使用して Mac にサインオンできるかどうかを選択します。これを有効にすることは、ユーザーが Mac のすべてのログイン画面で同じ ID およびパスワードを使用することを意味します。デフォルトは ［オン］ で、ユーザーは各自の Apple ID および iCloud パスワードを使用して Mac にアクセスすることができます。
- **iCloud** ドキュメントおよびデータを許可: ユーザーが Mac から iCloud に保存されているドキュメントおよびデータにアクセスするのを許可するかどうかを選択します。デフォルトは ［オフ］ で、ユーザーは Mac から iCloud に保存されているドキュメントおよびデータを使用できないようになっています。
  * **iCloud** で”デスクトップ”と”書類”を許可する: （macOS 10.12.4 以降）デフォルトは［オン］です。
- **iCloud** キーチェーンの同期を許可する: iCloud キーチェーンの同期を許可します（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”メール”を許可する: ユーザーが iCloud メールを使用できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”連絡先”を許可する: ユーザーが iCloud の連絡先を使用できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”カレンダー”を許可する: ユーザーが iCloud のカレンダーを使用できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”リマインダー”を許可する: ユーザーが iCloud のリマインダーを使用できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** ブックマークを許可する: ユーザーが iCloud のブックマークと同期できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”メモ”を許可する: ユーザーが iCloud のメモを使用できるようにします（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **iCloud** で”写真”を許可する: この設定を ［オフ］ に変更すると、iCloud のフォトライブラリから完全にダウンロードされていない写真はすべてデバイスのローカルストレージから削除されます（macOS 10.12 以降)。デフォルトは ［オン］ です。
- 自動ロックの解除を許可する: このオプションと Apple Watch について詳しくは、https://www.imore.com/auto-unlockを参照してください（macOS 10.12 以降)。デフォルトは ［オン］ です。
- **Mac** のロック解除に **Touch ID** を許可する: （macOS 10.12.4 以降）デフォルトは ［オン］ です。
- ソフトウェア更新の延期を強制する:［オン］ の場合、ソフトウェアの更新がユーザーに表示されるまで

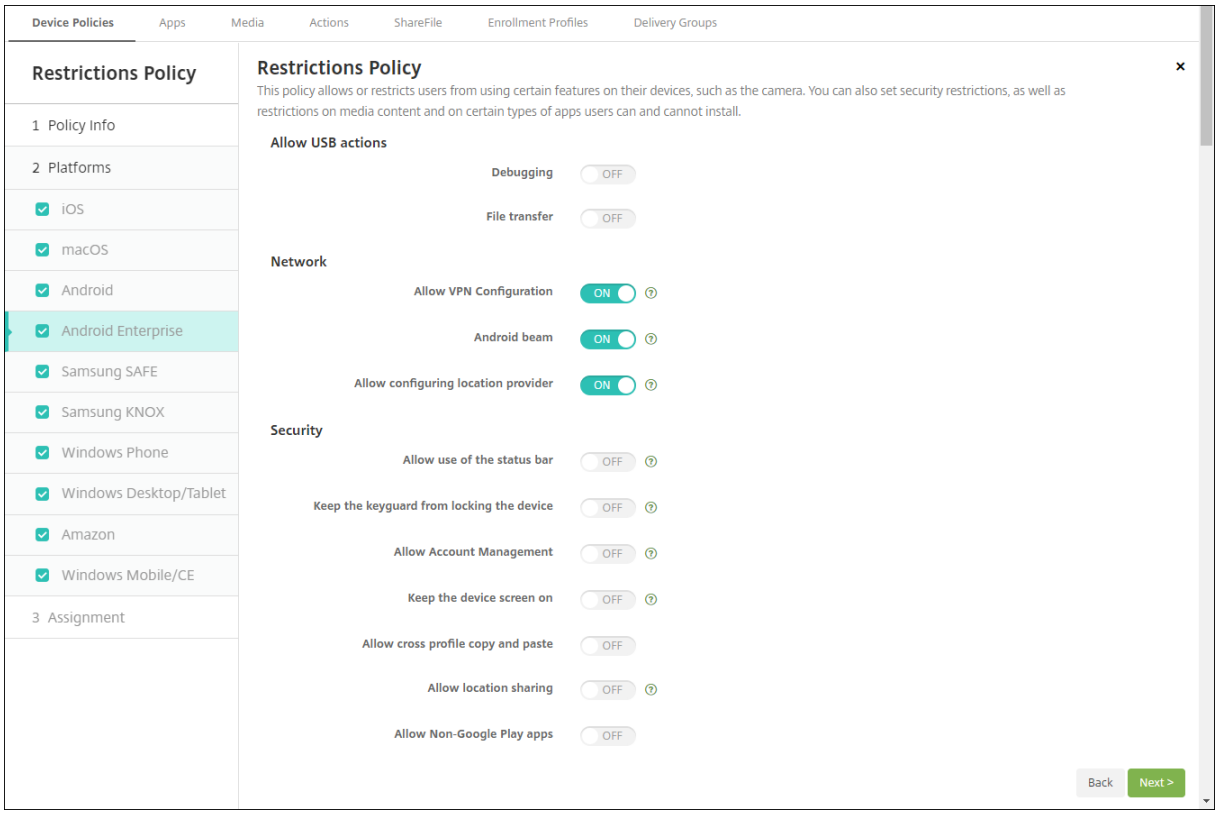
の時間が延期されます。ソフトウェアの更新がリリースされてから指定の日数が経過するまで、ユーザーにソフトウェアの更新は表示されません。デフォルトは ［オフ］ です。macOS 10.13.4 以降を実行する管理対象デバイスでのみ利用できます。

- ソフトウェア更新の強制延期期間（日）: デバイス上でソフトウェアの更新を延期する日数を指定します。日数の上限は 90 日です。デフォルトは **30** です。macOS 10.13.4 以降を実行する管理対象デバイスでのみ利用できます。
- パスワードの自動入力: オプション。無効にすると、ユーザーはパスワードの自動入力または自動強力パスワード機能を使用できません。デフォルトは ［オン］ です。macOS 10.14 以降で利用できます。
- パスワード近接要求: オプション。無効にすると、ユーザーのデバイスは近くのデバイスにパスワードを要求しません。デフォルトは ［オン］ です。macOS 10.14 以降で利用できます。
- パスワード共有: オプション。無効にすると、ユーザーは Airdrop パスワード機能を使用してパスワードを共有できません。デフォルトは ［オン］ です。macOS 10.14 以降で利用できます。

Android の設定

- カメラ: ユーザーがデバイスでカメラを使用できるようにします。［オフ］ の場合、カメラは無効になります。デフォルトは、［オン］ です。

Android Enterprise の設定



デバイスが Android Enterprise の仕事用プロファイルモードで登録されている場合、デフォルトでは **USB** デバッグおよび不明なソース設定は無効になっています。

Android 8.0 以降および Samsung Knox 3.0 以降を実行しているデバイスの場合は、［**Android Enterprise**］ページで Samsung Knox と Samsung SAFE の設定を行います。それよりも前のバージョンの Android または Samsung KNOX を実行しているデバイスの場合は、［**Samsung Knox**］と［**Samsung SAFE**］ページで設定します。

- **USB** 操作を許可
  - デバッグ。USB 経由のデバッグを可能にします。デフォルトは ［オフ］ です。
  - ファイル転送。USB 経由のファイル転送を可能にします。デフォルトは ［オフ］ です。
- ネットワーク
  - **VPN** 構成を許可。ユーザーが VPN 構成を作成できるようにします。Android 6 以降を実行する仕事用プロファイルデバイスおよび完全に管理されているデバイス向けです。デフォルトは ［オン］ です。
  - **Android Beam**。近距離無線通信（Near Field Communication：NFC）を使用して、ユーザーが手元のデバイスから他のデバイスに Web ページ、写真、ビデオなどのコンテンツを送信できるようにします。MDM 4.0 以降で使用します。デフォルトは ［オフ］ です。
  - 位置情報プロバイダーの構成を許可。ユーザーがデバイスで GPS をオンにできるようにします。Android API 28 以降で使用します。デフォルトは ［オン］ です。
- セキュリティ
  - ステータスバーの使用を許可。［オン］ に設定すると、管理対象デバイスおよび専用デバイス（COSU デバイス）上でステータスバーが有効になります。これにより、通知、クイック設定、その他の画面オーバーレイで全画面モードから移動することができなくなります。ユーザーはシステム設定に移動して通知を表示できます。Android 6.0 以降の場合、デフォルトは ［オフ］ です。
  - **Keyguard** がデバイスをロックしないようにする。［オン］の場合、この設定が管理対象デバイスおよび専用デバイス（COSU デバイス）のロック画面で Keyguard を無効にします。デフォルトは ［オフ］です。
  - アカウント管理を許可。仕事用プロファイルおよび管理対象デバイスでアカウントを追加できるようにします。デフォルトは ［オフ］ です。
  - デバイス画面を有効なまま維持する。この設定を ［オン］ に設定すると、デバイスを接続してもデバイス画面はオンのままです。デフォルトは ［オフ］ です。
  - プロファイル間でコピーと貼り付けを許可。Android Enterprise プロファイルのアプリとパーソナルエリアのアプリ間で、クリップボードを使用してコピーと貼り付けができるかどうかを指定します。デフォルトは ［オフ］ です。
  - 位置情報の共有を許可。位置情報の共有を可能にします。管理対象プロファイルの場合、デバイス所有者は設定を上書きできます。デフォルトは ［オフ］ です。
  - **Google Play** 非対応アプリを許可。Google Play 以外のストアからアプリをインストールできるようにします。デフォルトは ［オフ］ です。
  - スクリーンショットを許可。ユーザーがデバイス画面のスクリーンショットを取得できるかどうかを指定します。デフォルトは ［オフ］ です。
  - カメラの使用を許可。ユーザーがデバイスのカメラで写真やビデオを撮ることができます。デフォルト

は ［オフ］ です。

- ユーザーにアプリケーション設定の制御を許可。ユーザーがアプリのアンインストール、アプリの無効化、キャッシュやデータの消去、アプリの強制停止、デフォルト値のクリアをできるようにします。デフォルトは ［オフ］ です。
- ホーム画面で仕事用プロファイルアプリのウィジェットを許可。この設定が ［オン］ の場合、ユーザーは仕事用プロフィールアプリウィジェットを端末のホーム画面に配置できます。この設定が ［オフ］ の場合、ユーザーは仕事用プロフィールアプリウィジェットを端末のホーム画面に配置できません。デフォルトは ［オフ］ です。
  * ウィジェットを許可するアプリ。ホーム画面で許可するアプリの一覧。［ホーム画面で仕事用プロファイルアプリのウィジェットを許可］ を ［オン］ に設定して対象のアプリを追加します。［追加］をクリックし、一覧からホーム画面で許可するアプリを選択します。［保存］ をクリックします。この手順を繰り返して、ほかのアプリウィジェットも許可します。
- デバイスの連絡先で仕事用プロファイルの連絡先を許可。着信時に、管理対象の Android Enterprise プロファイルの連絡先を親プロファイルに表示します（Android 7.0 以降）。デフォルトは［オフ］です。
- システムアプリを有効にします。事前インストールされたデバイスアプリの実行をユーザーに許可します。デフォルトは ［オフ］ です。特定のアプリを有効にするには、システムアプリ一覧の表で［追加］をクリックします。
  * システムアプリ一覧。デバイスで有効にするシステムアプリの一覧。[システムアプリを有効にする]を[オン]に設定して、アプリのパッケージ名を追加します。システムアプリのパッケージ名を検索するには、Android Debug Bridge（adb）を使用して Android パッケージマネージャー（pm）コマンドを呼び出します。例えば `adb shell "pm list packages -f name"` で、ここで「名前」はパッケージ名の一部です。詳しくは、「https://developer.android.com/studio/command-line/adb」を参照してください。Android Enterprise デバイスの場合、Android Enterprise 管理対象の構成ポリシーポリシーを使用してアプリの権限を制限できます。
- アプリケーションを無効化。指定したアプリのリストがデバイス上で実行されるのをブロックします。デフォルトは ［オフ］ です。インストールされているアプリを無効にするには、設定を ［オン］ に変更し、［アプリケーション一覧］ 表で ［追加］ をクリックしてから、アプリのパッケージ名を入力します。
  * アプリケーション一覧。ブロックするアプリのリストです。［アプリケーションを無効にする］ を［オン］ に設定してアプリを追加し、アプリのパッケージ名を入力します。アプリ一覧を変更して展開すると、以前のアプリ一覧が上書きされます。たとえば、com.example1 と com.example2 を無効にしてから、後で一覧を com.example1 と com.example3 に変更すると、XenMobile により com.example.2 が有効化されます。
- アプリの検証を有効化。OS がアプリをスキャンして悪意のある動作を検出できるようにします。デフォルトは ［オン］ です。
- **Google Apps** を有効化。ユーザーが Google モバイルサービスからデバイスにアプリをダウンロードできるようにします。デフォルトは ［オン］ です。

- 完全に管理されているデバイス
  - 複数ユーザーを許可。複数のユーザーがデバイスを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。

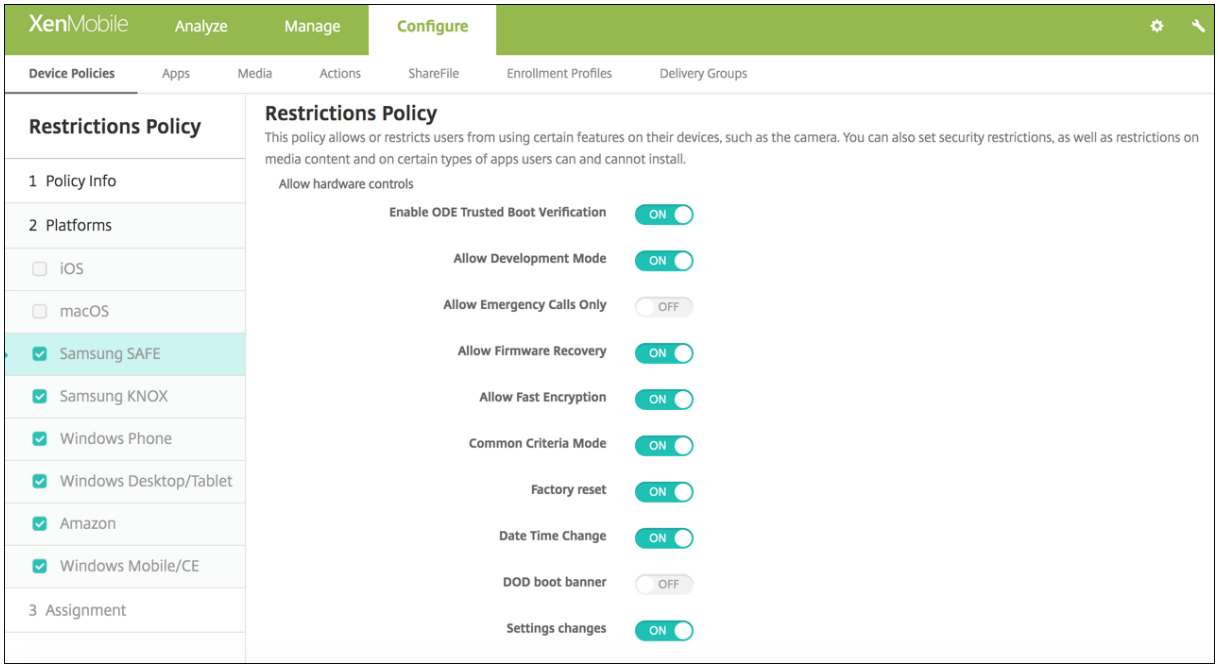
- ローミングを許可。ユーザーがローミング中に携帯データネットワークを使用できるようにします。デフォルトは［オフ］で、ユーザーのデバイスでローミングが無効になっています。デフォルトは ［オフ］です。
- **SMS** を許可。ユーザーが SMS メッセージを送受信できるようにします。デフォルトは ［オフ］ です。
- バックアップ。ユーザーがデバイス上にアプリケーションやシステムデータをバックアップできるようにします。デフォルトは ［オン］ です。
- **Bluetooth**。ユーザーが Bluetooth を使用できるようにします。デフォルトは ［オン］ です。
- 携帯データネットワーク。ユーザーがデータ用の携帯ネットワーク接続を使用できるようにします。デフォルトは ［オン］ です。
- 日単位で制限（**MB**）。ユーザーが 1 日に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 週単位で制限（**MB**）。ユーザーが 1 週間に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 月単位で制限（**MB**）。ユーザーが 1 か月に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- 日付**/**時刻の変更。ユーザーがデバイスの日付と時刻を変更できるようにします。デフォルトは ［オン］です。
- 工場出荷時リセット。ユーザーがデバイスを出荷時の設定に戻すことができるようにします。デフォルトは ［オン］ です。
- ホストストレージ。USB デバイスがユーザーのデバイスに接続された時、ユーザーのデバイスが USB ホストとして機能するようにできます。これにより、ユーザーのデバイスが USB デバイスに電源を供給します。デフォルトは ［オン］ です。
- 大容量ストレージ。USB 接続上で、ユーザーのデバイスとコンピューター間で大容量のデータファイルを転送できるようにします。デフォルトは ［オン］ です。
- マイク。ユーザーがデバイスでマイクを使用できるようにします。デフォルトは ［オン］ です。
- テザリング。ユーザーがポータブルホットスポットおよびテザリングデータを構成できるようにします。デフォルトは ［オフ］ です。この設定をオンにすると、Samsung デバイスで以下の設定を使用できます:
  * **USB**。ユーザーが、USB 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。
  * **Bluetooth**。ユーザーが、Bluetooth 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。
  * **Wi-Fi**。ユーザーが、Wi-Fi 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。
- **Wi-Fi**。ユーザーが Wi-Fi ネットワークに接続できるようにします。デフォルトは ［オン］ です。この設定をオンにすると、以下の設定を使用できます:
  * 直接。ユーザーが Wi-Fi 接続を介して、ほかのデバイスに直接接続できるようにします。Samsung デバイスの場合のみ使用します（MDM 4.0 以降）。
  * 状態の変更。アプリで Wi-Fi 接続の状態を変更できるようにします。

- **Samsung SAFE**：ハードウェアの制御を許可
  - **ODE** 信頼済み起動検証を有効化。ODE 信頼済み起動検証を使って、ブートローダーからシステムイメージへの信頼のチェーンを確立します。デフォルトは ［オン］ です。
  - 緊急電話のみ許可。ユーザーがデバイスで緊急電話のみモードを有効にできるようにします。デフォルトは ［オフ］ です。
  - ファームウェアリカバリを許可。ユーザーがデバイスでファームウェアを復元できるようにします。デフォルトは ［オン］ です。
  - 高速暗号化を許可。使用済みのメモリ領域のみ暗号化を許可します。これは、設定、アプリケーションデータ、ダウンロードしたファイルおよびアプリケーション、メディア、およびその他のファイルを含め、すべてのデータを暗号化するフルディスク暗号化とは対照的な方法です。デフォルトは ［オン］ です。
  - 情報セキュリティ国際評価基準（**Common Criteria**）モード。デバイスを情報セキュリティ国際評価基準モードにします。Common Criteria 構成は、厳重なセキュリティプロセスを遂行します。デフォルトは ［オン］ です。
  - **DOD** 起動バナー。ユーザーのデバイスが再起動された時に DoD 承認システム使用通知メッセージまたはバナーを表示します。デフォルトは ［オフ］ です。
  - 設定の変更。ユーザーが完全に管理されているデバイスの設定を変更できるようにします。デフォルトは ［オン］ です。
  - 無線アップグレード： ユーザーのデバイスでソフトウェアの更新プログラムをワイヤレスで受信できるようにします（MDM 3.0 以降）。デフォルトは ［オン］ です。
  - バックグラウンドデータ。アプリがバックグラウンドでデータを同期できるようにします。完全に管理されているデバイス向けの設定です。デフォルトは ［オン］ です。
  - クリップボード。ユーザーがデバイスでデータをクリップボードにコピーできるようにします。
    * クリップボード共有。ユーザーが自分のデバイスとコンピューター間でクリップボードのコンテンツを共有できるようにします（MDM 4.0 以降）。
  - ホームキー。ユーザーがデバイスで **Home** キーを使用できるようにします。デフォルトは ［オン］ です。
  - 疑似ロケーション。ユーザーが GPS の場所を偽装できるようにします。完全に管理されているデバイス用の設定です。デフォルトは ［オン］ です。
  - **NFC**。ユーザーが完全に管理されたデバイス（MDM 3.0 以降）で NFC を使用できるようにします。デフォルトは ［オン］ です。
  - 電源オフ。ユーザーが完全に管理されているデバイスの電源を切れるようにします（MDM 3.0 以降）。デフォルトは ［オン］ です。
  - **SD** カード。ユーザーが、可能な場合にはデバイスで SD カードを使用できるようにします。デフォルトは ［オン］ です。
  - 音声ダイヤラー。ユーザーがデバイスで音声ダイヤラーを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
  - **SBeam**。ユーザーが NFC や Wi-Fi Direct を使ってほかのユーザーとコンテンツを共有できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
  - **SVoice**。ユーザーがデバイスでインテリジェントパーソナルアシスタントおよびナレッジナビゲータ

ーを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。

- **Samsung SAFE**: アプリを許可
  - 顔認識: ユーザーが顔認識アプリを使用できるようにします。デフォルトは ［オン］ です。
  - ブラウザー。ユーザーが Web ブラウザーを使用できるようにします。デフォルトは ［オン］ です。
  - **Youtube**。ユーザーが YouTube へアクセスできるようにします。デフォルトは ［オン］ です。
  - **Google Play/Marketplace**。ユーザーが Google Play や Google Apps Marketplace にアクセスできるようにします。デフォルトは ［オン］ です。
  - システムアプリを停止。ユーザーが事前にインストール済みのシステムアプリを無効にできるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
- **Samsung SAFE**: ネットワーク
  - 受信 **MMS**。ユーザーが MMS メッセージを受信できるようにします。デフォルトは ［オン］ です。
  - 送信 **MMS**。ユーザーが MMS メッセージを送信できるようにします。デフォルトは ［オン］ です。
  - セキュリティで保護された接続のみ。ユーザーがセキュリティで保護された接続のみを使用できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
  - オーディオの録音。ユーザーがデバイスでオーディオを録音できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
  - ビデオの録画。ユーザーがデバイスでビデオを録画できるようにします（MDM 4.0 以降）。デフォルトは ［オン］ です。
- **Samsung Knox**
  - 失効チェックを有効にする。失効している証明書のチェックを有効にします。デフォルトは ［オン］ です。
  - コンテナにアプリを移動。ユーザーが、Knox コンテナとデバイス上の個人的領域間でアプリを移動できるようにします。デフォルトは ［オン］ です。
  - 多要素認証を強制。ユーザーはデバイスを開くため、指紋に加えてパスワードや PIN などもう 1 つ別の認証方式を使用する必要があります。デフォルトは ［オン］ です。
  - **TIMA** キーストアを有効化。TIMA KeyStore は、対称キーの TrustZone ベースのセキュアなキーストレージを提供します。RSA キーペアと証明書は、ストレージのデフォルトのキーストアプロバイダーを経由します。デフォルトは ［オン］ です。
  - コンテナ認証を強制。別個の異なる認証を使用して、デバイスのロック解除に使用されたものから Knox コンテナを開きます。デフォルトは ［オン］ です。
  - 共有一覧。ユーザーが Share Via の一覧のアプリ間でコンテンツを共有できるようにします。デフォルトは ［オン］ です。
  - 監査ログを有効化。デバイスのフォレンジクス解析用イベント監査ログの作成を有効にします。デフォルトは ［オン］ です。
  - セキュリティで保護されたキーパッドを使用。Knox コンテナ内部のセキュアなキーボードを強制的にユーザーに使用させます。デフォルトは ［オン］ です。
  - 認証スマートカードブラウザー。スマートカードリーダーが装備されているデバイスでブラウザー認証を有効にします。

Samsung SAFE の設定



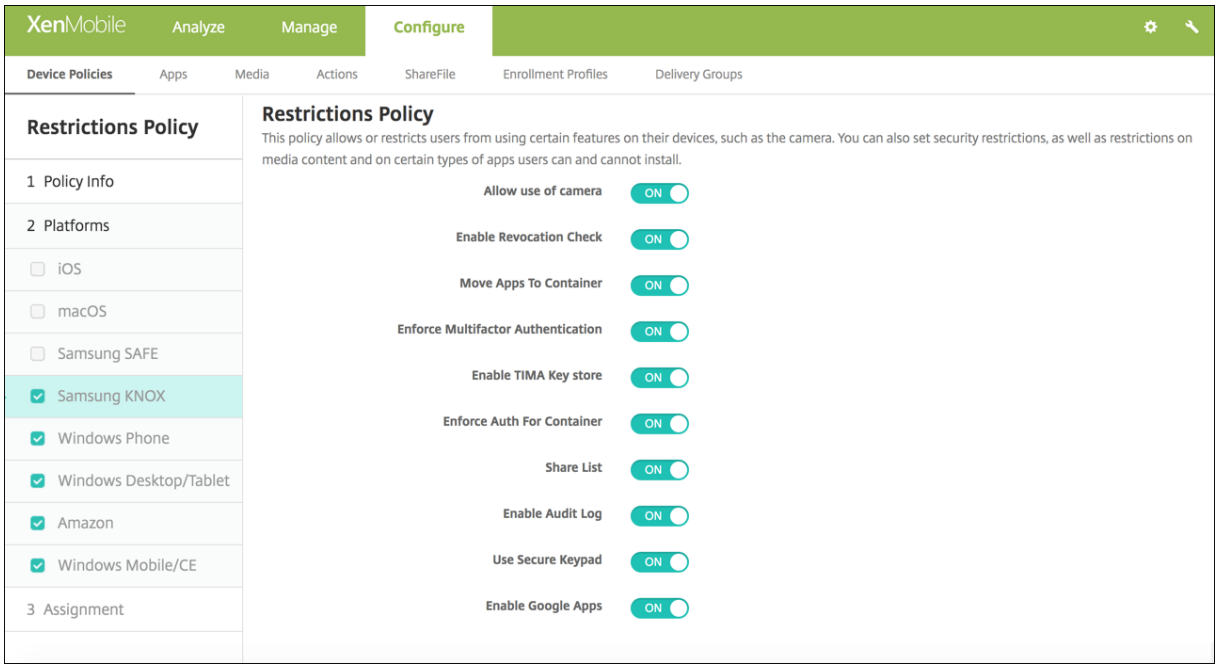
一部のオプションについては、特定の Samsung Mobile Device Management API の元でのみ使用できます。該当するオプションには、関連するバージョン情報が記されています。

- ハードウェアの制御を許可
  - **ODE** 信頼済み起動検証を有効化: ODE 信頼済みブート検証を使って、ブートローダーからシステムイメージへの信頼のチェーンを確立します。
  - 開発モードを許可: ユーザーがデバイスで開発者設定を有効にできるようにします。
  - 緊急電話のみ許可: ユーザーがデバイスで緊急電話のみモードを有効にできるようにします。
  - ファームウェアリカバリを許可: ユーザーがデバイスでファームウェアを復元できるようにします。
  - 高速暗号化を許可: 使用済みのメモリ領域のみ暗号化を許可します。これは、設定、アプリケーションデータ、ダウンロードしたファイルおよびアプリケーション、メディア、およびその他のファイルを含め、すべてのデータを暗号化するフルディスク暗号化とは対照的な方法です。
  - **Common Criteria Mode**: デバイスを Common Criteria モードにします。Common Criteria 構成は、厳重なセキュリティプロセスを遂行します。
  - 工場出荷時リセット: ユーザーがデバイスを出荷時の設定に戻すことができるようにします。
  - 日付/時刻の変更: ユーザーがデバイスの日付と時刻を変更できるようにします。
  - **DOD** 再起動バナー: ユーザーのデバイスが再起動された時に DoD 承認システム使用通知メッセージまたはバナーを表示します。
  - 設定の変更: デバイスでユーザーが設定を変更できるようにします。
  - バックアップ: ユーザーがデバイス上にアプリケーションやシステムデータをバックアップできるようにします。
  - 無線アップグレード: ユーザーのデバイスでソフトウェアの更新プログラムをワイヤレスで受信できるようにします（MDM 3.0 以降）。

  - バックグラウンドデータ: アプリがバックグラウンドでデータを同期できるようにします。
  - カメラ: ユーザーがデバイスでカメラを使用できるようにします。
  - クリップボード: ユーザーがデバイスでデータをクリップボードにコピーできるようにします。
    * クリップボード共有: ユーザーが自分のデバイスとコンピューター間でクリップボードのコンテンツを共有できるようにします（MDM 4.0 以降）。
  - ホームキー: ユーザーがデバイスで Home キーを使用できるようにします。
  - マイク: ユーザーがデバイスでマイクを使用できるようにします。
  - 疑似ロケーション: ユーザーが GPS の場所を偽装できるようにします。
  - **NFC**: ユーザーがデバイスで NFC (Near Field Communication) を使用できるようにします (MDM 3.0 以降)。
  - 電源オフ: ユーザーがデバイスの電源を切れるようにします（MDM 3.0 以降）。
  - スクリーンショット: ユーザーがデバイスでスクリーンショットを撮れるようにします。
  - **SD** カード: ユーザーが、可能な場合にはデバイスで SD カードを使用できるようにします。
  - 音声ダイヤラー: ユーザーがデバイスで音声ダイヤラを使用できるようにします（MDM 4.0 以降）。
  - **SBeam**: ユーザーが NFC や Wi-Fi Direct を使ってほかのユーザーとコンテンツを共有できるようにします（MDM 4.0 以降）。
  - **SVoice**: ユーザーがデバイスでインテリジェントパーソナルアシスタントおよびナレッジナビゲーターを使用できるようにします（MDM 4.0 以降）。
  - 複数ユーザーを許可: 複数のユーザーがデバイスを使用できるようにします（MDM 4.0 以降）。デフォルトは、［オフ］ です。
- アプリを許可
  - ブラウザー: ユーザーが Web ブラウザーを使用できるようにします。
  - **YouTube**: ユーザーが YouTube へアクセスできるようにします。
  - **Google Play/Marketplace**: ユーザーが Google Play や Google Apps Marketplace にアクセスできるようにします。
  - **Google Play** 非対応アプリを許可: ユーザーが Google Play や Google Apps Marketplace 以外のサイトからアプリをダウンロードできるようにします。［オン］ の場合、ユーザーはデバイスのセキュリティ設定を使用して、不明な情報源からのアプリを信頼できます。
  - システムアプリを停止: ユーザーが事前にインストール済みのシステムアプリを無効にできるようにします（MDM 4.0 以降）。
  - アプリケーションを無効化:［オン］ の場合、指定した一覧のアプリが Samsung SAFE デバイスで実行されないようにブロックされます。
- ネットワーク
  - 受信 **MMS**: ユーザーが MMS メッセージを受信できるようにします。
  - 受信 **SMS**: ユーザーが SMS メッセージを受信できるようにします。
  - 送信 **MMS**: ユーザーが MMS メッセージを送信できるようにします。
  - 送信 **SMS**: ユーザーが SMS メッセージを送信できるようにします。
  - ユーザーによるプロファイルの追加 **- VPN**:
  - **Bluetooth**: ユーザーが Bluetooth を使用できるようにします。

        * テザリング: ユーザーが、Bluetooth 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。
    - **Wi-Fi**: ユーザーが Wi-Fi ネットワークに接続できるようにします。
        * テザリング: ユーザーが、Wi-Fi 接続を使ってモバイルデータ接続をほかのデバイスと共有できるようにします。
        * 直接: ユーザーが Wi-Fi 接続を介して、ほかのデバイスに直接接続できるようにします（MDM 4.0 以降）。
        * 状態の変更: アプリで Wi-Fi 接続の状態を変更できるようにします。
        * ユーザーによるポリシーの変更: ユーザーが Wi-Fi ポリシーを変更できるようにします。オフの場合、ユーザーは Wi-Fi のユーザー名とパスワードのみを変更できます。オンにした場合、ユーザーはすべての Wi-Fi ポリシーを変更することができます。
    - テザリング: ユーザーが、モバイルデータ接続をほかのデバイスと共有できるようにします。
    - 携帯データネットワーク: ユーザーがデータ用の携帯ネットワーク接続を使用できるようにします。
    - ローミングを許可: ユーザーがローミング中に携帯ネットワークデータを使用できるようにします。デフォルトは［オフ］で、ユーザーのデバイスでローミングが無効になっています。
    - セキュリティで保護された接続のみ: ユーザーがセキュリティで保護された接続のみを使用できるようにします（MDM 4.0 以降）。
    - **Android** ビーム: NFC を使用して、ユーザーが手元のデバイスから他のデバイスに Web ページ、写真、ビデオなどのコンテンツを送信できるようにします（MDM 4.0 以降）。
    - オーディオの録音: ユーザーがデバイスでオーディオを録音できるようにします（MDM 4.0 以降）。
    - ビデオの録画: ユーザーがデバイスでビデオを録画できるようにします（MDM 4.0 以降）。
    - 位置情報サービス: ユーザーがデバイスで GPS をオンにできるようにします。
    - 日単位で制限（**MB**）: ユーザーが一日に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
    - 週単位で制限（**MB**）: ユーザーが一週間に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
    - 月単位で制限（**MB**）: ユーザーが 1 か月に使用できるモバイルデータの MB 数を入力します。デフォルトは 0 で、この機能が無効になっています（MDM 4.0 以降）。
- **USB** 操作を許可: ユーザーのデバイスとコンピューター間で USB 接続を可能にします。
    - デバッグ: USB 上でのデバッグを可能にします。
    - ホストストレージ: USB デバイスがユーザーのデバイスに接続された時、ユーザーのデバイスが USB ホストとして機能するようにできます。これにより、ユーザーのデバイスが USB デバイスに電源を供給します。
    - 大容量ストレージ: USB 接続上で、ユーザーのデバイスとコンピューター間で大容量のデータファイルを転送できるようにします。
    - **Kies** メディアプレーヤー: ユーザーが Samsung Kies ツールを使って、デバイスとコンピューター間でファイルを同期できるようにします。
    - テザリング: ユーザーが、USB 接続を介してモバイルデータ接続をほかのデバイスと共有できるようにします。

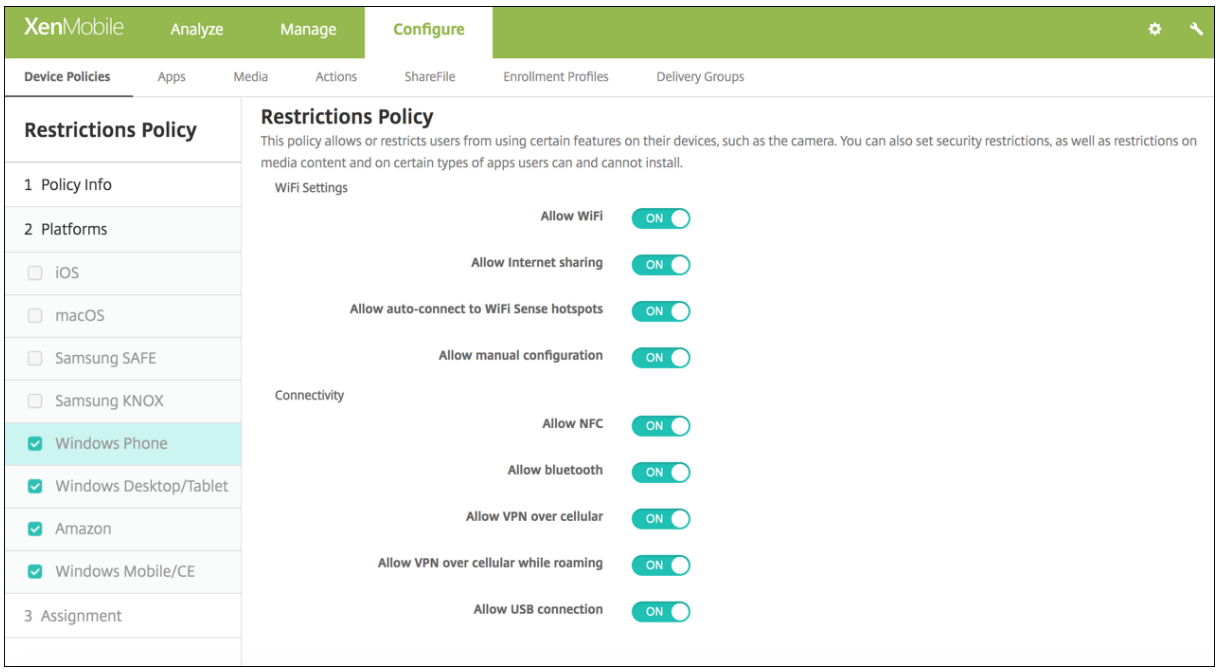
Samsung KNOX の設定



これらのオプションは、Samsung KNOX Premium（KNOX 2.0）でのみ使用できます。

- カメラの使用を許可： ユーザーがデバイスでカメラを使用できるようにします。
- 失効チェックを許可： 失効した証明書のチェックを有効にします。
- コンテナにアプリを移動： ユーザーに、KNOX コンテナとデバイス上の個人的領域間でアプリを移動できるようにします。
- 多要素認証を強制： ユーザーはデバイスを開くため、指紋に加えてパスワードや PIN などもう 1 つ別の認証方式を使用する必要があります。
- **TIMA** キーストアを有効化： TIMA KeyStore は、対称キーの TrustZone ベースのセキュアなキーストレージを提供します。RSA キーペアと証明書は、ストレージのデフォルトのキーストアプロバイダーを経由します。
- コンテナ認証を強制： 別個の異なる認証を使用して、デバイスのロック解除に使用されたものから KNOX コンテナを開きます。
- 共有一覧： ユーザーが Share Via の一覧のアプリ間でコンテンツを共有できるようにします。
- 監査ログを有効化： デバイスのフォレンジクス解析用イベント監査ログの作成を有効にします。
- セキュリティで保護されたキーパッドを使用： KNOX コンテナ内部のセキュアなキーボードを強制的にユーザーに使用させます。
- **Google Apps** を有効化： ユーザーが Google Mobile Services から KNOX コンテナにアプリをダウンロードできるようにします。
- 認証スマートカードブラウザー： スマートカードリーダーが装備されているデバイスでブラウザー認証を有効にします。

Windows Phone および **Windows** デスクトップ/タブレットの設定

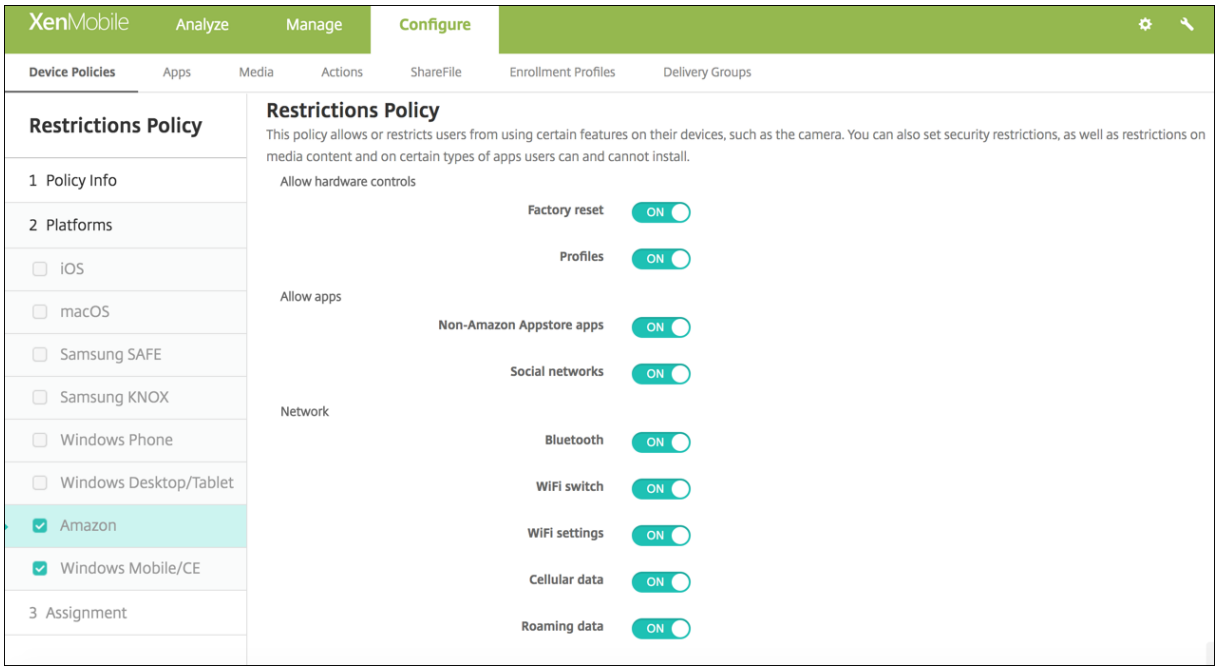


- **Wi-Fi** 設定
  - **Wi-Fi** を許可： デバイスを Wi-Fi ネットワークに接続できるようにします。Windows Phone のみ。
  - インターネット共有を許可： Wi-Fi ホットスポットに切り替えてデバイスがインターネット接続をほかのデバイスと共有できるようにします。
  - **Wi-Fi** センサーホットスポットへの自動接続を許可： デバイスが Wi-Fi センサーホットスポットに自動で接続できるようにします。このオプションを実行するには、位置情報サービスを有効にする必要があります。Wi-Fi Sense について詳しくは、Windows Phone のWi-Fi Sense FAQを参照してください。
  - 手動構成を許可： ユーザーが Wi-Fi 接続を手動で構成できるようにします。Windows Phone のみ。
- 接続
  - **NFC** を許可： デバイスが NFC タグまたはほかの NFC 対応送信デバイスと通信できるようにします。Windows Phone のみ。
  - **Bluetooth** を許可： デバイスが Bluetooth を介して接続できるようにします。Windows Phone のみ。
  - 携帯ネットワーク経由の **VPN** を許可： デバイスが VPN 上で携帯ネットワークと接続できるようにします。
  - ローミング時の携帯ネットワーク経由の **VPN** を許可： デバイスが携帯ネットワーク上をローミングしたら、デバイスが VPN 上で接続できるようにします。
  - **USB** 接続を許可： デスクトップが USB 接続を介してデバイスのストレージにアクセスできるようにします。Windows Phone のみ。
  - 携帯ネットワークデータのローミングを許可： ローミングの間にユーザーが携帯データネットワークを使えるようにします。
- アカウント

  - **Microsoft** アカウントの接続を許可: デバイスが、非メール関連の接続認証とサービスに Microsoft アカウントを使用できるようにします。
  - **Microsoft** 以外のメールを許可: ユーザーが Microsoft 以外のメールアカウントを追加できるようにします。
- 検索: Windows Phone のみ。
  - 場所を使用する検索を許可: 検索で、デバイスの位置情報サービスを使用できるようにします。
  - アダルトコンテンツをフィルター: アダルトコンテンツを許可します。デフォルトは ［オフ］ で、アダルトコンテンツはフィルターされません。
  - **Bing Vision** でイメージの格納を許可: Bing Vision 検索を実行するときに、Bing Vision がキャプチャされたイメージを格納できるようにします。
- システム
  - ストレージカードを許可: デバイスでストレージカードの使用を許可します。
  - テレメトリ: 一覧で、デバイスによる利用統計情報の送信を許可または制限するオプションをクリックします。デフォルトは ［許可］ です。そのほかのオプションには、［許可しない］ および ［許可（セカンダリデータ要求を除く）］ があります。
  - 位置情報サービスを許可: 位置情報サービスを有効にします。
  - 内部ビルドのプレビューを許可: ユーザーが Microsoft 内部ビルドをプレビューできるようにします。
- カメラ: Windows デスクトップ/タブレットのみ
  - カメラの使用を許可: ユーザーがデバイスのカメラを使用できるようにします。
- **Bluetooth**: Windows デスクトップ/タブレットのみ
  - 検出可能モードを許可: Bluetooth デバイスがローカルデバイスを検出できるようにします。
  - ローカルデバイス名: ローカルデバイスの名前。
- セキュリティ: Windows Phone のみ
  - ルート証明書の手動インストールを許可: ユーザーがルート証明書を手動でインストールできるようにします。
  - デバイスの暗号化を必須とする: デバイス暗号化を求めます。デバイスで暗号化が有効になった後は、それは無効にすることはできません。デフォルトは ［オフ］ です。
  - コピーと貼り付けを許可: ユーザーがデバイスでデータをコピーおよび貼り付けできるようにします。
  - スクリーンキャプチャを許可: ユーザーがデバイスで画面キャプチャを作成できるようにします。
  - 音声の録音を許可: ユーザーがデバイスで音声録音を使用できるようにします。
  - **Office** ファイルの［名前を付けて保存］を許可: ユーザーが Office ファイルを［名前を付けて保存］を使用して保存できるようにします。
  - アクションセンターの通知を許可: デバイスのロック画面で、アクションセンターの通知を有効にします。
  - **Cortana** を許可: ユーザーが Cortana のインテリジェントパーソナルアシスタントおよびナレッジナビゲーターにアクセスできるようにします。
  - デバイス設定の同期を許可: ユーザーがローミング時に Windows Phone 8.1 デバイス間で設定を同期できるようにします。
- 操作性: Windows デスクトップ/タブレットのみ

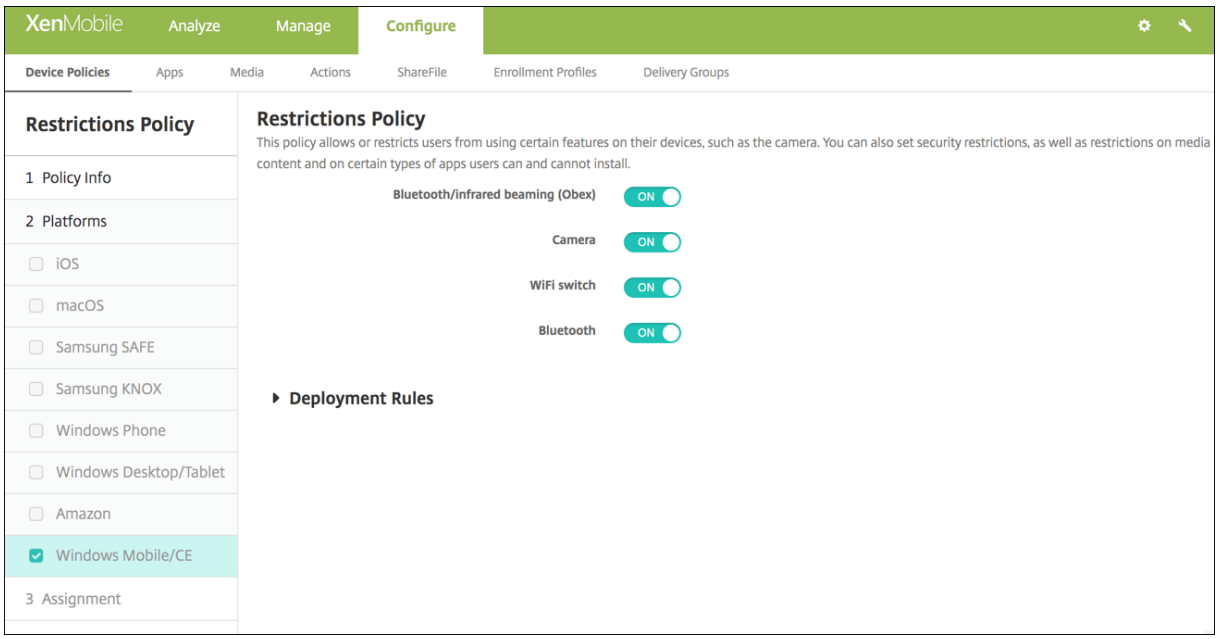
  - **Cortana** を許可: ユーザーが Cortana のインテリジェントパーソナルアシスタントおよびナレッジナビゲーターにアクセスできるようにします。
  - デバイスの検出を許可: デバイスのネットワーク検出を有効にします。
  - 手動の **MDM** 登録解除を許可: ユーザーが XenMobile MDM から手動でデバイスの登録を解除できるようにします。
  - デバイス設定の同期を許可: ユーザーがローミング時に Windows 10 デバイス間で設定を同期できるようにします。
- ロック例外: Windows デスクトップ/タブレットのみ
  - トーストを許可: ロック画面でトースト通知を許可します。Windows デスクトップ/タブレットのみ
- アプリ
  - ストアへのアクセスを許可: ユーザーが Microsoft ストアにアクセスできるようにします。Windows Phone のみ。
  - 開発者によるデバイスのロック解除を許可: ユーザーが Microsoft にデバイスを登録し、Windows Phone アプリストアにはないアプリケーションを開発またはインストールできるようにします。Windows Phone のみ。
  - **Web** ブラウザーアクセスを許可: デバイス上で Internet Explorer を使用できるようにします。Windows Phone のみ。
  - **Appstore** の自動更新を許可: アプリストアによるアプリの自動更新を許可します。Windows デスクトップ/タブレットのみ。
- プライバシー: Windows デスクトップ/タブレットのみ
  - 入力の個人設定を許可: 入力の個人設定を許可します。ペンやタッチキーボードなどでユーザーが入力した内容をベースに、予測変換の精度を向上します。
- 設定: Windows デスクトップ/タブレットのみ。
  - 自動再生を許可: ユーザーが自動再生設定を変更できるようにします。
  - データセンターを許可: ユーザーがデータセンサー設定を変更できるようにします。
  - 日付/時刻を許可: ユーザーが日付/時刻設定を変更できるようにします。
  - 言語を許可: ユーザーが言語設定を変更できるようにします。
  - 電源スリープを許可: ユーザーが電源設定およびスリープ設定を変更できるようにします。
  - リージョンを許可: ユーザーがリージョン設定を変更できるようにします。
  - サインインオプションを許可: ユーザーがサインイン設定を変更できるようにします。
  - ワークプレースを許可: ユーザーがワークプレース設定を変更できるようにします。
  - アカウントを許可: ユーザーがアカウント設定を変更できるようにします。

Amazon の設定



- ハードウェアの制御を許可
  - 工場出荷時リセット: ユーザーがデバイスを出荷時の設定に戻すことができるようにします。
  - プロファイル: ユーザーがデバイスでハードウェアプロファイルを変更できるようにします。
- アプリを許可
  - **Amazon** アプリストア非対応アプリを許可: ユーザーが Amazon アプリストアに対応していないアプリをデバイスにインストールできるようにします。
  - ソーシャルネットワーク: ユーザーがデバイスからソーシャルネットワークにアクセスできるようにします。
- ネットワーク
  - **Bluetooth**: ユーザーが Bluetooth を使用できるようにします。
  - **Wi-Fi** スイッチ: アプリで Wi-Fi 接続の状態を変更できるようにします。
  - **Wi-Fi** 設定: ユーザーが Wi-Fi 設定を変更できるようにします。
  - 携帯データネットワーク: ユーザーがデータ用の携帯ネットワーク接続を使用できるようにします。
  - ローミングデータ: ローミングの間にユーザーが携帯データネットワークを使えるようにします。
  - 位置情報サービス: ユーザーが GPS を使用できるようにします。
- **USB** 操作:
  - デバッグ: デバッグのためユーザーのデバイスが USB を介してコンピューターに接続できるようにします。

Windows Mobile/CE の設定



- **Bluetooth/**赤外線ビーム（**OBEX**）: Bluetooth または赤外線を介して OBEX（オブジェクト交換プロトコル）を有効にして、デバイス間でデータを交換します。
- カメラ: ユーザーのデバイスでカメラを有効にします。
- **WiFi** スイッチ: ユーザーが WiFi ネットワークを切り替えられるようにします。
- **Bluetooth**: ユーザーのデバイスで Bluetooth を有効にします。

ローミングデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、ユーザーの iOS デバイスおよび Windows Mobile/CE デバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。iOS の場合、このポリシーは iOS 5.0 以降のデバイスでのみ使用できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 音声ローミングを無効化: 音声通話ローミングを無効にするかどうかを選択します。このオプションを有効にした場合、データローミングは自動的に無効になります。デフォルトは ［オフ］ で、音声通話ローミングを許

可します。

- データローミングを無効化： データローミングを無効にするかどうかを選択します。このオプションは、音声通話ローミングが有効になっている場合にのみ使用できます。デフォルトは ［オフ］ で、データローミングを許可します。

Windows Mobile/CE の設定

- ローミング中
  - オンデマンド接続のみ使用： ユーザーがデバイスで接続を手動でトリガーする場合、またはモバイルアプリが強制接続を要求する場合のみ（Exchange Server に相応の設定があらかじめされている場合のプッシュ型のメール要求など）、デバイスは XenMobile に接続します。このオプションにより、デフォルトデバイス接続スケジュールポリシーは一時的に無効化される点に注意してください。
  - **XenMobile** で管理されないすべての携帯ネットワーク接続をブロック： XenMobile アプリケーショントンネルまたはそのほかの XenMobile デバイス管理タスクで公式に宣言されているデータトラフィックを除き、ほかのデータはデバイスによって送受信されません。たとえば、このオプションではデバイスの Web ブラウザーを使用したインターネットへの接続がすべて無効化されます。
  - **XenMobile** で管理されるすべての携帯ネットワーク接続をブロック： XenMobile トンネルを使用して転送されるすべてのアプリケーションデータ（XenMobile Remote Support を含む）がブロックされます。ただし、純粋なデバイス管理に関連するデータトラフィックはブロックされません。
  - **XenMobile** に対するすべての携帯ネットワーク接続をブロック： この場合、USB、Wi-Fi、またはデフォルトのモバイル事業者のモバイルネットワークを通じてデバイスが再接続されるまで、デバイスと XenMobile 間のトラフィックの転送は発生しません。
- 国内ローミング中
  - 国内ローミングを無視： ユーザーが国内でローミングしている間はデータがブロックされません。

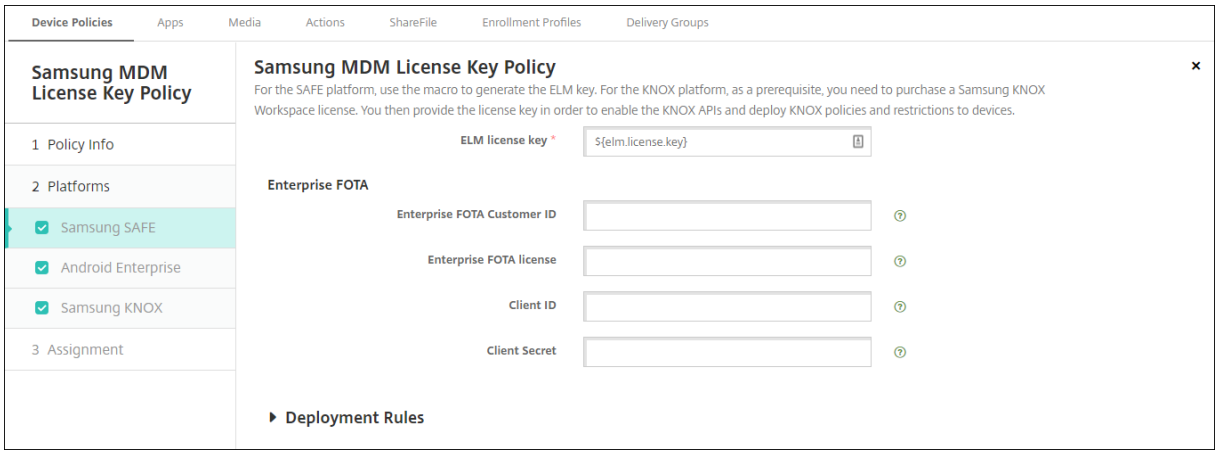
Samsung MDM ライセンスキーデバイスポリシー

September 24, 2019

SAFE のポリシーおよび制限を展開する前に、デバイスに展開する必要がある組み込みの Samsung Enterprise License Management（ELM）キーを指定します。XenMobile は、Samsung Enterprise Firmware-Over-The-Air (E-FOTA) サービスもサポートしています。XenMobile は Samsung for Enterprise (SAFE) および Samsung KNOX ポリシーの両方をサポートし、拡張しています。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung SAFE の設定



- **ELM** ライセンスキー: このフィールドには、ELM ライセンスキーを生成するマクロがあらかじめ入力されています。このフィールドが空白の場合は、「${elm.license.key}」というマクロを入力します。

Samsung E-FOTA の設定の構成

E-FOTA ポリシーを構成するには:

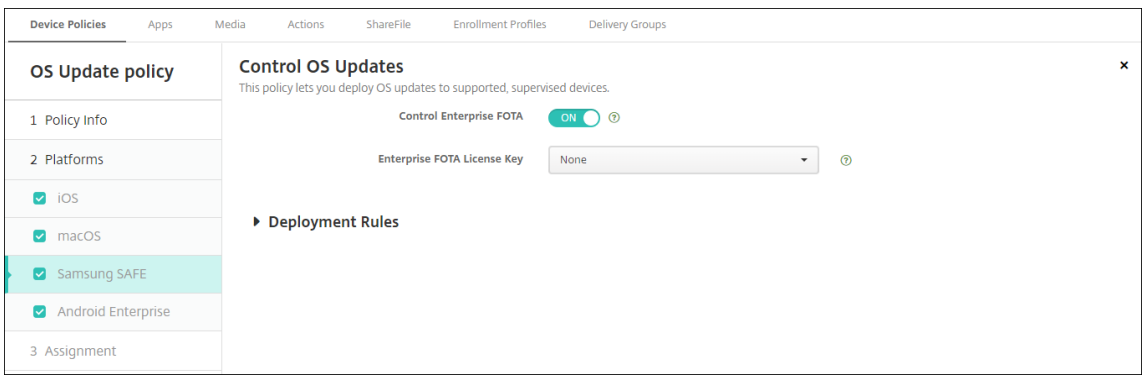
1. Samsung から受け取ったキーとライセンス情報で Samsung MDM ライセンスキーデバイスポリシーを作成します。XenMobile Server は、その後、その情報を検証して登録します。

   [**ELM** ライセンスキー] を入力します。このフィールドは、ELM ライセンスキーを生成するマクロがあらかじめ入力されています。このフィールドが空白の場合は、「${elm.license.key}」というマクロを入力します。

   E-FOTA パッケージを購入したときに Samsung から提供された、以下の情報を入力してください。

   - **Enterprise FOTA** 顧客 **ID**
   - **Enterprise FOTA** ライセンス
   - クライアント **ID**
   - クライアントシークレット

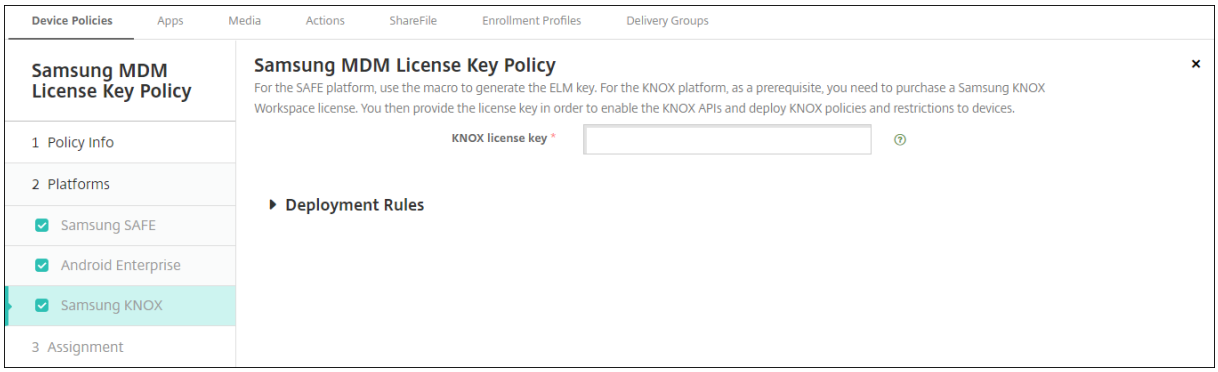
2. 必要に応じて、OS 更新の制御デバイスポリシーを作成します。



- **Enable Enterprise FOTA**: [オン] に設定します。
- **Enterprise FOTA** ライセンスキー: 手順 1 で作成した Samsung MDM ライセンスキーポリシーの名前を選択します。

3. OS 更新の制御ポリシーを Secure Hub に展開します。

Android Enterprise と **Samsung KNOX** の設定



- **KNOX** ライセンスキー: Samsung から取得した KNOX ライセンスキーを入力します。

Samsung SAFE のファイアウォールデバイスポリシー

August 22, 2019

このポリシーにより、Samsung デバイスのファイアウォール設定を構成できます。許可または禁止する IP アドレス、ポート、ホスト名を入力します。プロキシおよびプロキシ再ルーティングの設定を構成することもできます。

このポリシーを追加または構成するには、[構成] > [デバイスポリシー] の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Samsung SAFE の設定

- ホストの許可/拒否: アクセスを許可または拒否するホストごとに、[追加] をクリックして以下を構成します。
  - ホスト名/**IP** アドレスの範囲: ポリシーを適用するサイトのホスト名または IP アドレスの範囲を入力します。
  - ポート/ポートの範囲: ポートまたはポートの範囲。
  - 規則フィルターを許可/禁止: サイトへのアクセスを許可する場合は [ホワイトリスト] を選択し、サイトへのアクセスを拒否する場合は [ブラックリスト] を選択します。
- 再ルーティング構成: 構成するプロキシごとに、[追加] をクリックして以下を構成します。

  - ホスト名/**IP** アドレスの範囲: プロキシ再ルーティングのホスト名または IP アドレスの範囲。
  - ポート/ポートの範囲: プロキシ再ルーティングのポートまたはポートの範囲。
  - プロキシ **IP**: プロキシ再ルーティングのプロキシ IP アドレス。
  - プロキシポート: プロキシ再ルーティングのプロキシポート。
- プロキシ構成
  - プロキシ **IP**: プロキシサーバーの IP アドレス。
  - ポート: プロキシサーバーのポート。

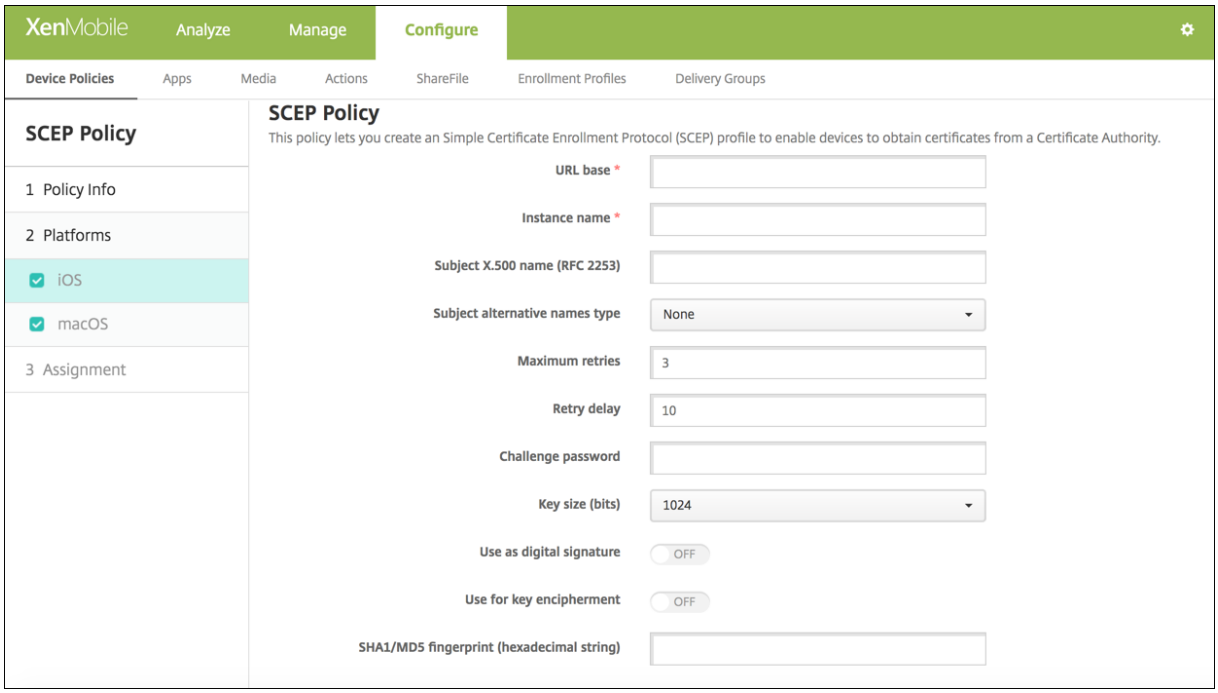
SCEP デバイスポリシー

January 10, 2020

このポリシーで iOS デバイスと macOS デバイスを構成し、SCEP（Simple Certificate Enrollment Protocol）を使用して外部 SCEP サーバーから証明書を取得することができます。XenMobile に接続されている PKI から SCEP を使用してデバイスに証明書を配布する場合は、PKI エンティティと PKI プロバイダーを分散モードで作成する必要があります。詳しくは、「PKI エンティティ」を参照してください。

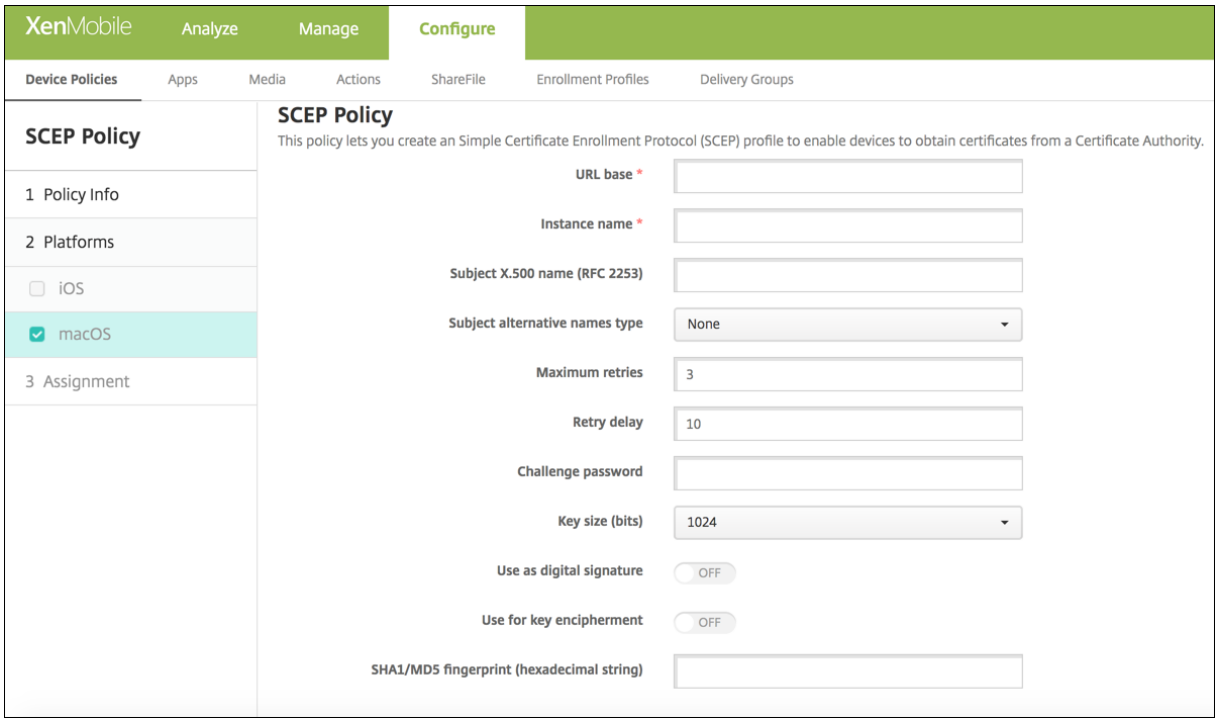
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **URL** ベース： HTTP または HTTPS を介した SCEP 要求の送信先を定義する SCEP サーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するために HTTPS を使用してください。これは必須の手順です。
- インスタンス名： SCEP サーバーで認識される文字列を入力します。たとえば、example.org のようなドメイン名です。CA に複数の CA 証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **X.500** サブジェクト名（**RFC 2253**）： オブジェクト識別子（OID）と値の配列として示される X.500 の名前の表現を入力します。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]」のように解釈されます。OID はドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
- [サブジェクトの別名の種類]： 一覧から、代替名の種類を選択します。SCEP ポリシーは、CA が証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。［なし］、［**RFC 822** 名］、［**DNS** 名］、［**URI**］ のいずれかを指定できます。
- 最大再試行回数： SCEP サーバーが PENDING 応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは、**3** です。
- 再試行の延期： 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは **10** です。
- チャレンジパスワード： 事前共有シークレットを入力します。
- キーサイズ（ビット）： 一覧から、**1024** または **2048** のいずれかのキーサイズ（ビット）を選択します。デフォルトは **1024** です。
- デジタル署名として使用： デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合（証明書が CA によって発行されたかどうかを確認する場合など）、公開キーを使ってハッシュを復号化する前に、SCEP サーバーではデジタル署名に証明書を使用できるかどうかが確認されます。
- キーの暗号化に使用： キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかが最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5** 指紋（**16** 進数の文字列）： CA で HTTP が使われている場合、このフィールドを使って、CA 証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CA の応答の信頼性を確認するためにデバイスで使われます。SHA1 または MD5 のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。

macOS 設定



- **URL** ベース： HTTP または HTTPS を介した SCEP 要求の送信先を定義する SCEP サーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するために HTTPS を使用してください。これは必須の手順です。
- インスタンス名： SCEP サーバーで認識される文字列を入力します。たとえば、example.org のようなドメイン名です。CA に複数の CA 証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **X.500** サブジェクト名（**RFC 2253**）： オブジェクト識別子（OID）と値の配列として示される X.500 の名前の表現を入力します。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[[“C”, “US”]], [[“O”, “Apple Inc.”]], …, [[“1.2.5.3”, “bar”]]]」のように解釈されます。OID はドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
- [サブジェクトの別名の種類]： 一覧から、代替名の種類を選択します。SCEP ポリシーは、CA が証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。［なし］、［**RFC 822** 名］、［**DNS** 名］、［**URI**］ のいずれかを指定できます。
- 最大再試行回数： SCEP サーバーが PENDING 応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは、**3** です。
- 再試行の延期： 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは **10** です。
- チャレンジパスワード： 事前共有シークレットを入力します。
- キーサイズ（ビット）： 一覧から、**1024** または **2048** のいずれかのキーサイズ（ビット）を選択します。デフ

ォルトは **1024** です。

- デジタル署名として使用: デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合（証明書が CA によって発行されたかどうかを確認する場合など）、公開キーを使ってハッシュを復号化する前に、SCEP サーバーではデジタル署名に証明書を使用できるかどうかが確認されます。
- キーの暗号化に使用: キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかが最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5** 指紋（**16** 進数の文字列）: CA で HTTP が使われている場合、このフィールドを使って、CA 証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CA の応答の信頼性を確認するためにデバイスで使われます。SHA1 または MD5 のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。

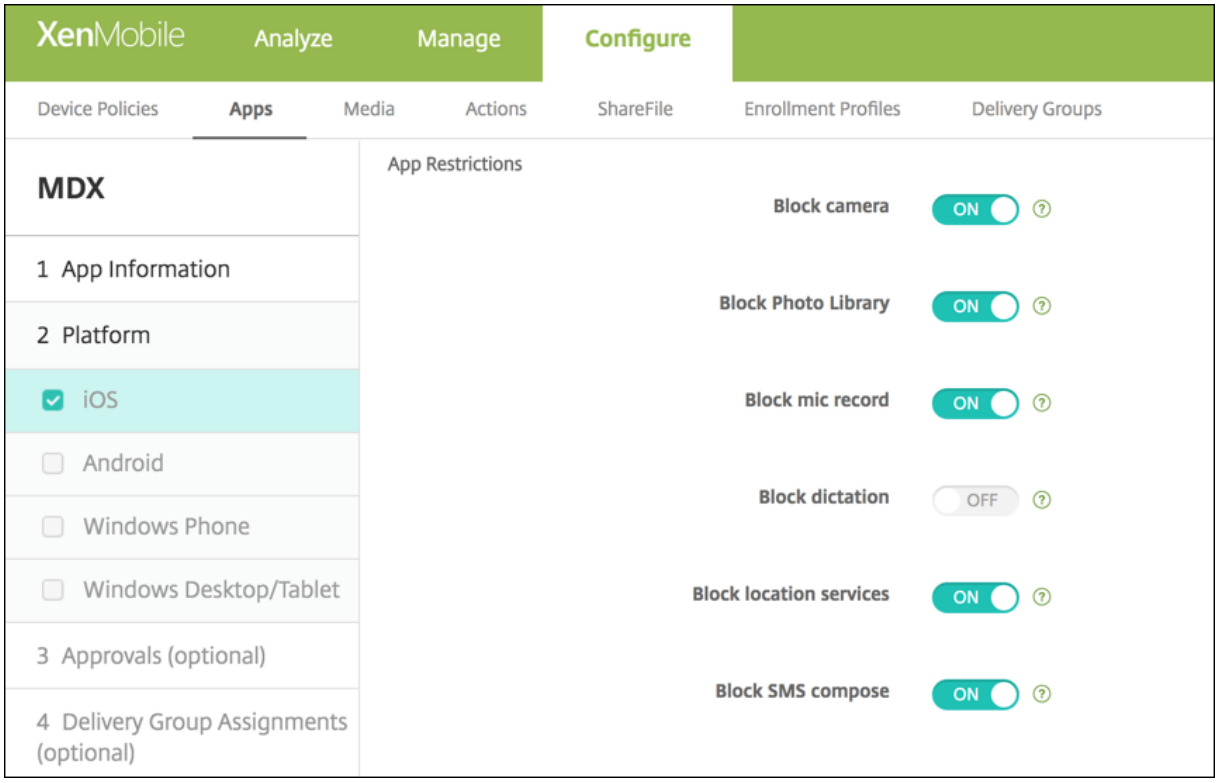
Siri とディクテーションのポリシー

August 22, 2019

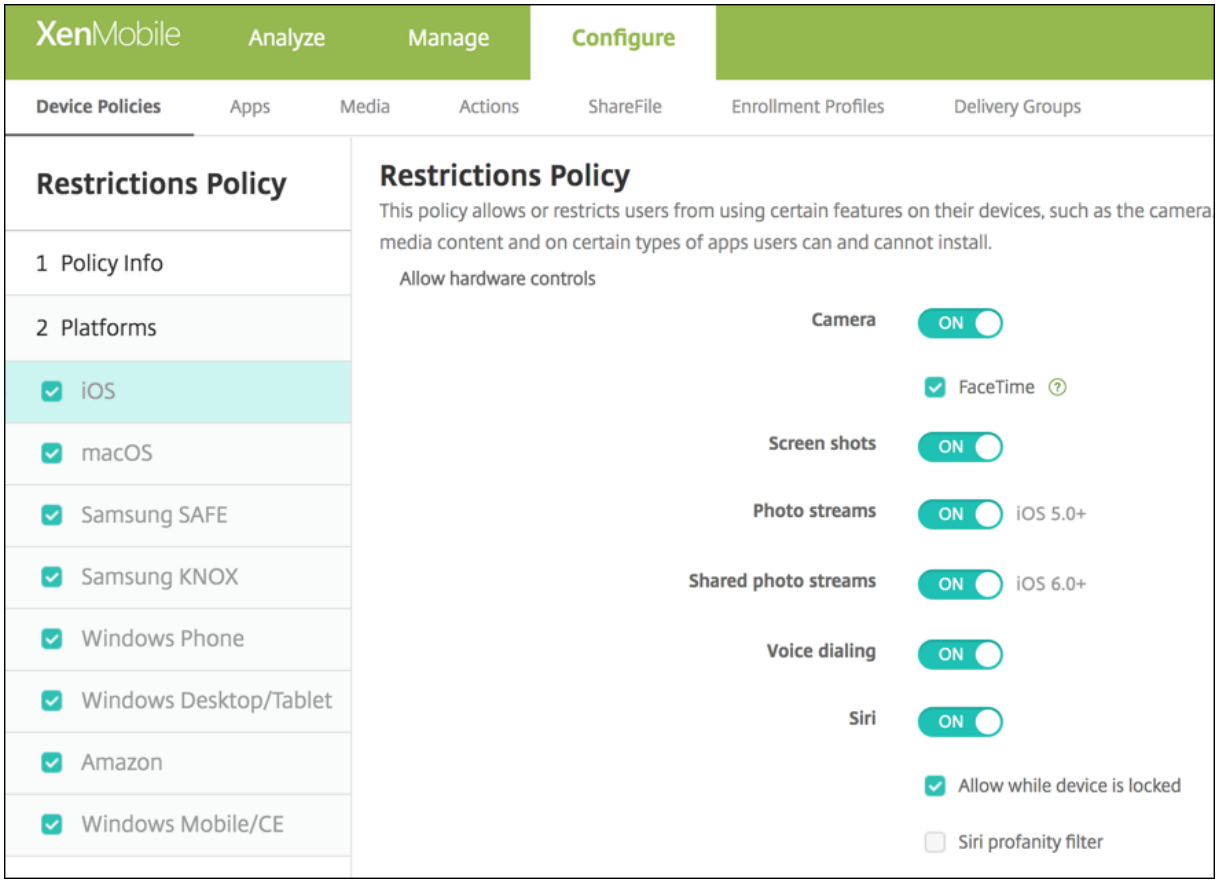
管理された iOS デバイス上でユーザーが Siri に何かを求めるか、テキストを口述する場合、Apple は Siri の改善のために音声データを収集します。音声データは Apple のクラウドベースのサービスを通過し、したがって、セキュアな XenMobile コンテナの外側に存在します。ただし、ディクテーションの結果として生じたテキストは、コンテナ内に残ります。

XenMobile では、セキュリティのニーズの要件に応じて、Siri およびディクテーションサービスをブロックできます。

MAM 展開では、各アプリのディクテーションブロックポリシーはデフォルトで ［オン］ であり、デバイスのマイクは無効になります。ディクテーションを許可する場合、［オフ］ に設定します。XenMobile コンソールの ［構成］**>** ［アプリ］ で、ポリシーを検出できます。アプリを選択し、［編集］ をクリックしてから ［**iOS**］ をクリックします。



MDM 展開では、［構成］>［デバイスポリシー］ で、Siri ポリシーとともに Siri を無効にすることもできます。Siri の使用は、デフォルトで許可されています。



Siri およびディクテーションを許可するかどうか決定するときの留意事項:

- Apple が公開した情報によると、Apple は Siri およびディクテーション音声クリップデータを最大で 2 年間保持します。データにはユーザーを表す乱数が割り当てられ、音声ファイルはこの乱数に関連付けられます。詳しくは、Wired の記事「Apple reveals how long Siri keeps your data」を参照してください。
- iOS デバイスで ［設定］ > ［一般］ > ［キーボード］ と移動して、［音声入力］ の下のリンクをタップすると、Apple のプライバシーポリシーを確認できます。

SSO アカウントデバイスポリシー

January 10, 2020

XenMobile でシングルサインオン（SSO）アカウントを作成して、ユーザーが 1 回サインオンするだけで、さまざまなアプリケーションから XenMobile および社内リソースにアクセスすることができるようにします。デバイスに資格情報を保存する必要はありません。SSO アカウントエンタープライズユーザーの資格情報は、App Store からのアプリを含む複数のアプリで使用されます。このポリシーは、Kerberos 認証バックエンドで動作するように設計されています。

このポリシーは iOS 7.0 以降にのみ適用されます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- アカウント名: ユーザーのデバイスで表示される Kerberos SSO アカウント名を入力します。このフィールドは必須です。
- **Kerberos** プリンシパル名: Kerberos プリンシパル名を入力します。このフィールドは必須です。
- **ID** 資格情報（キーストアまたは **PKI** 資格情報）: 一覧から、オプションとして、ID 資格情報を選択します。これを使用して、Kerberos 資格情報をユーザー操作なしで更新できます。
- **Kerberos** 領域: このポリシーの Kerberos レルムを入力します。これは通常、ドメイン名をすべて大文字にしたものです（例: EXAMPLE.COM）。このフィールドは必須です。
- 許可されている **URL**: シングルサインオンを要求する URL ごとに、［追加］ をクリックして以下の操作を行います。
  - 許可されている **URL**: ユーザーが iOS デバイスからアクセスしたときに SSO を要求する URL を入力します。
    たとえば、ユーザーがサイトを参照しようとし、Web サイトが Kerberos チャレンジを開始した場合、そのサイトが URL 一覧にないと、iOS デバイスでは、前の Kerberos ログオンでデバイスにキャッシュされた可能性がある Kerberos トークンを提供した SSO は試行されません。URL は、ホスト部分が正確に一致する必要があります。たとえば、`https://shopping.apple.com`は有効ですが、`https://*.apple.com`は有効ではありません。
    また、Kerberos がホストの一致に基づいてアクティブ化されない場合でも、URL は標準の HTTP 呼び出しにフォールバックします。これは、URL に Kerberos を使用する SSO だけが構成されている場合であっても、標準パスワードチャレンジや HTTP エラーなどを含むほとんどすべてのことを意味する可能性があります。
  - ［追加］をクリックして URL を追加するか、［キャンセル］をクリックして URL の追加を取り消します。
- アプリ識別子: このログインを許可するアプリごとに、［追加］ をクリックして以下の操作を行います。
  - アプリ識別子: このログインを使用できるアプリのアプリ ID を入力します。アプリ ID を追加しなかった場合、このログインはすべてのアプリ ID に一致します。
  - ［追加］ をクリックしてアプリ ID を追加するか、［キャンセル］ をクリックしてアプリ ID の追加を取り消します。

ストレージ暗号化デバイスポリシー

August 22, 2019

XenMobile でストレージ暗号化デバイスポリシーを作成して、内部ストレージと外部ストレージを暗号化したり、デバイスによっては、ユーザーがデバイスでストレージカードを使用できないようにしたりします。

Samsung SAFE、Windows Phone、Android Sony デバイスに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提条件

Samsung SAFE デバイスの場合は、次の要件が満たされていることを確認します。

- ユーザーのデバイスで画面のロックオプションを設定します。
- ユーザーのデバイスを接続し、少なくとも 80%充電します。
- デバイスパスワードには、数字と文字（または記号）のが両方が含まれている必要があります。

Samsung SAFE の設定の構成

- 内部ストレージを暗号化： ユーザーのデバイスの内部ストレージを暗号化するかどうかを選択します。内部ストレージには、デバイスのメモリと内部ストレージが含まれます。デフォルトは ［オン］ です。
- 外部ストレージを暗号化： ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。デフォルトは ［オン］ です。

Windows Phone の設定

- デバイスの暗号化を要求： ユーザーのデバイスを暗号化するかどうかを選択します。デフォルトは ［オフ］ です。
- ストレージカードを無効化： ユーザーがデバイスでストレージカードを使用できないようにするかどうかを選択します。デフォルトは ［オフ］ です。

Android Sony の設定の構成

- 外部ストレージを暗号化： ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。デフォルトは ［オン］ です。

ストアデバイスポリシー

August 22, 2019

XenMobile でポリシーを作成して、iOS、Android、または Windows タブレットデバイスのホーム画面で XenMobile Store の Web クリップを表示するかどうかを指定できます。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

プラットフォーム設定

構成するプラットフォームごとに、ユーザーデバイスに XenMobile Store Web クリップを表示するかどうかを選択します。デフォルトは ［オン］ です。

サブスクライブされたカレンダーデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加して、サブスクライブされたカレンダーを iOS デバイスのカレンダー一覧に追加することができます。サブスクライブできる公開カレンダーの一覧は、www.apple.com/downloads/macosx/calendarsにあります。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

前提要件

デバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みである必要があります。

iOS の設定

- 説明: カレンダーの説明を入力します。このフィールドは必須です。
- **URL**: カレンダーの URL を入力します。iCalendar ファイル（.ics）への`webcal://`URL または`https://`リンクを入力できます。このフィールドは必須です。
- ユーザー名: ユーザーのログオン名を入力します。このフィールドは必須です。
- パスワード: 任意で、ユーザーのパスワードを入力します。
- **SSL** を使用: カレンダーに対して Secure Socket Layer 接続を使用するかどうかを選択します。デフォルトは ［オフ］ です。

契約条件デバイスポリシー

August 22, 2019

社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、XenMobile で契約条件デバイスポリシーを作成します。ユーザーが XenMobile にデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。

社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。Android デバイスおよび iOS デバイスの場合は、PDF ファイルを提供する必要があります。Windows デバイスの場合は、テキスト（TXT）ファイルと付属のイメージファイルを提供する必要があります。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS および **Android** の設定

- インポートするファイル: ［参照］ をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。
- デフォルトの契約条件: このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは ［オフ］ です。

Windows Phone および **Windows** タブレットの設定

- インポートするファイル:［参照］ をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。
- イメージ:［参照］ をクリックしてインポートするイメージファイルの場所へ移動し、そのファイルを選択します。
- デフォルトの契約条件: このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは ［オフ］ です。

VPN デバイスポリシー

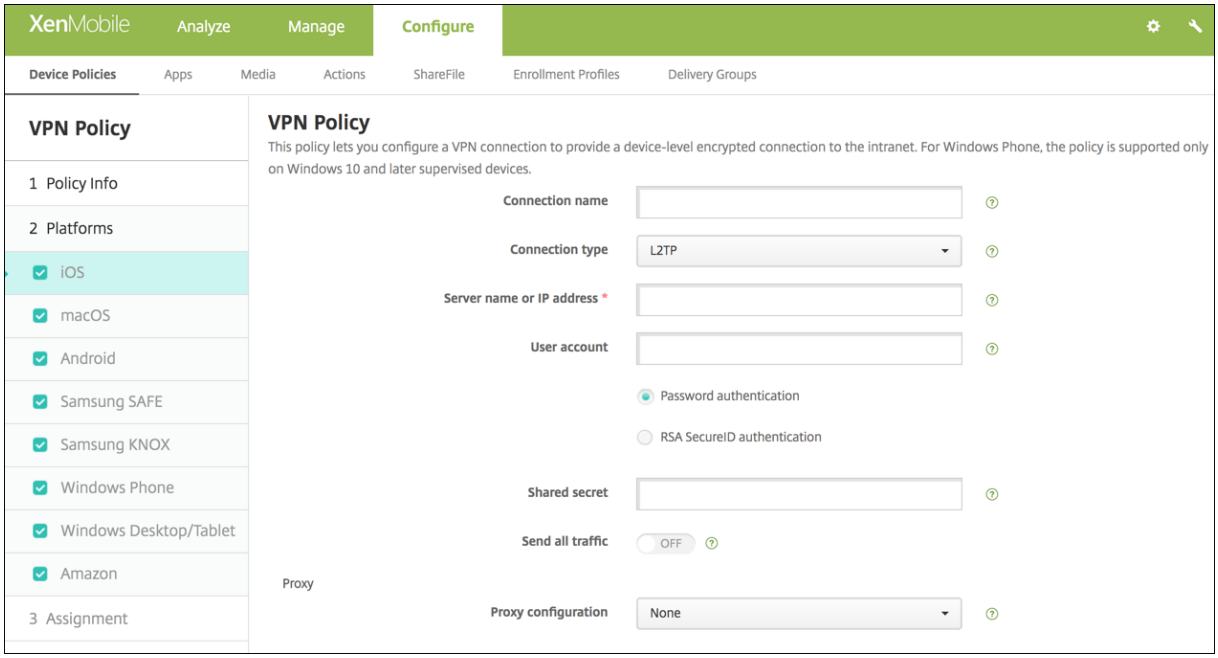
January 10, 2020

VPN デバイスポリシーでは、VPN（Virtual Private Network: 仮想プライベートネットワーク）の設定を構成し、ユーザーデバイスが社内リソースに安全に接続できるようにすることができます。次のプラットフォームで VPN デバイスポリシーを構成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、この記事で説明しています。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

> **iOS 12** へのデバイスアップグレードの準備：
>
> iOS 用の VPN デバイスポリシーの Citrix VPN 接続タイプは、iOS 12 をサポートしていません。VPN デバイスポリシーを削除し、Citrix SSO 接続の種類で VPN デバイスポリシーを作成するには、以下の手順に従います：
>
> 1. iOS の VPN デバイスポリシーを削除します。
> 2. iOS の VPN デバイスポリシーを追加します。重要な設定：
>   - 接続の種類 = **Citrix SSO**
>   - **Per-App VPN** を有効化 = オン
>   - プロバイダーの種類 = パケットトンネル
> 3. iOS のアプリ属性デバイスポリシーを追加します。［**Per-App VPN** 識別子］ で **iOS_VPN** を選択します。



- 接続名： 接続名を入力します。
- 接続の種類： 一覧から、この接続において使用するプロトコルを選択します。デフォルトは ［**L2TP**］ です。
  - **L2TP**： レイヤー 2 トンネリングプロトコルと事前共有キー認証。
  - **PPTP**： Point-to-Point トンネリング。
  - **IPSec**： 社内 VPN 接続。
  - **Cisco Legacy AnyConnect**： この接続の種類では、従来の Cisco AnyConnect VPN クライアントがユーザーデバイスにインストールされている必要があります。Cisco は、廃止された VPN フレームワークに基づいていた従来の Cisco AnyConnect クライアントを段階的に廃止しています。詳しくは、サポートの記事（https://support.citrix.com/article/CTX227708）を参照してください。
    現在の Cisco AnyConnect クライアントを使用するには、接続の種類はカスタム **SSL** を使用します。必要な設定については、このセクションの「カスタム SSL プロトコルの構成」を参照してください。

- **Juniper SSL**： Juniper Networks SSL VPN クライアント
- **F5 SSL**： F5 Networks SSL VPN クライアント
- **SonicWALL Mobile Connect**： iOS 用 Dell 統合 VPN クライアント
- **Ariba VIA**： Aruba Networks 仮想インターネットアクセスクライアント
- **IKEv2**（**iOS only**）： iOS 専用インターネットキー交換バージョン 2
- **AlwaysOn IKEv2**： IKEv2 を使用した常時アクセス。
- **AlwaysOn IKEv2** デュアル構成： IKEv2 デュアル構成を使用した常時アクセス。
- **Citrix SSO**： iOS 12 以降の Citrix SSO クライアント。
- カスタム **SSL**： カスタム SSL（Secure Socket Layer）この接続の種類は、バンドル ID が **com.cisco.anyconnect** の Cisco AnyConnect クライアントに必要です。**Cisco AnyConnect** の接続名を指定します。また、VPN ポリシーを展開して、iOS デバイス用のネットワークアクセス制御（NAC）フィルターを有効にすることもできます。このフィルターで、非準拠のアプリがインストールされているデバイスの VPN 接続をブロックできます。この構成では、iOS VPN ポリシーの特定の設定が必要です（下記の iOS セクションを参照）。NAC フィルターを有効にするために必要なその他の設定の詳細については、「ネットワークアクセス制御」を参照してください。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

iOS 向け **L2TP** プロトコルの設定

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- ［パスワード認証］ または ［**RSA SecurID** 認証］ をクリックします。
- 共有シークレット： IPsec 共有シークレットキーを入力します。
- すべてのトラフィックを送信： VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］ です。

iOS 向け **PPTP** プロトコルの設定

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- ［パスワード認証］ または ［**RSA SecurID** 認証］ をクリックします。
- 暗号化レベル： 一覧から、暗号化レベルを選択します。デフォルトは ［なし］ です。
  - なし： 暗号化を使用しません。
  - 自動： サーバーでサポートされている最も強力な暗号化レベルを使用します。
  - 最大（**128** ビット）： 常に 128 ビットの暗号化を使用します。
- すべてのトラフィックを送信： VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは ［オフ］ です。

iOS 向け **IPsec** プロトコルの構成

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧から、この接続の認証の種類として、［共有シークレット］ または ［証明書］ を選択します。デフォルトは ［共有シークレット］ です。
- ［共有シークレット］ を有効にした場合は、次の設定を構成します:
  - グループ名: 任意で、グループ名を入力します。
  - 共有シークレット: 任意で、共有シークレットキーを入力します。
  - ハイブリッド認証を使用: ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対する認証を行い、次にクライアントがサーバーに対する認証を行います。デフォルトは ［オフ］ です。
  - パスワードの入力を要求: ネットワークへの接続時にユーザーにパスワードの入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
- ［証明書］ を有効にした場合は、次の設定を構成します:
  - **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］ です。
  - 接続時に **PIN** を要求: ネットワークへの接続時にユーザーによる PIN の入力を必須とするかどうかを選択します。デフォルトは ［オフ］ です。
  - オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。
- オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
- **Safari** ドメイン:［追加］ をクリックして、Safari ドメイン名を追加します。

従来の **iOS** 向け **Cisco AnyConnect** プロトコルの構成

従来の Cisco AnyConnect クライアントから新しい Cisco AnyConnect クライアントに移行するには、カスタム SSL プロトコルを使用します。

- プロバイダーのバンドル識別子: 従来の AnyConnect クライアントの場合、バンドル ID は com.cisco.anyconnect.gui です。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- グループ: 任意で、グループ名を入力します。

- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求： ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - プロバイダーの種類： Per-App VPN が ［アプリプロキシ］ で提供されるか、［パケットトンネル］ で提供されるかを選択します。デフォルトは ［アプリプロキシ］ です。
  - **Safari** ドメイン： アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います：
    * ドメイン： 追加するドメインを入力します。
    * ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

iOS 向け **Juniper SSL** プロトコルの構成

- プロバイダーのバンドル識別子： Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- 領域： オプションの領域名を入力します。
- 役割： オプションの役割名を入力します。
- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。

    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
  - オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - プロバイダーの種類: Per-App VPN が ［アプリプロキシ］ で提供されるか、［パケットトンネル］ で提供されるかを選択します。デフォルトは ［アプリプロキシ］ です。
  - **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
    * ドメイン: 追加するドメインを入力します。
    *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

iOS 向け **F5 SSL** プロトコルの構成

- プロバイダーのバンドル識別子: Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  -［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  -［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:

- オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
- プロバイダーの種類: Per-App VPN が［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは［アプリプロキシ］です。
- **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います:
  * ドメイン: 追加するドメインを入力します。
  *［保存］をクリックしてドメインを保存するか、［キャンセル］をクリックして操作を取り消します。

iOS 向け **SonicWALL** プロトコルの構成

- プロバイダーのバンドル識別子: Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- ログオングループまたはドメイン: 任意で、ログオングループまたはドメインを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に［パスワード］か［証明書］のどちらを使用するかを選択します。デフォルトは［パスワード］です。
  -［パスワード］を有効にした場合は、［認証パスワード］フィールドに任意の認証パスワードを入力します。
  -［証明書］を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは［オフ］です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは［オフ］です。［オンデマンドに **VPN** を有効化］が［オン］であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは［オフ］です。このオプションを［オン］に設定した場合は、次の設定を構成します:
  - オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  - プロバイダーの種類: Per-App VPN が［アプリプロキシ］で提供されるか、［パケットトンネル］で提供されるかを選択します。デフォルトは［アプリプロキシ］です。
  - **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］をクリックして以下の操作を行います:

        * ドメイン: 追加するドメインを入力します。
        *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

iOS 向け **Ariba VIA** プロトコルの構成

- プロバイダーのバンドル識別子: Per-App VPN プロファイルに同じ種類の複数の VPN プロバイダーがあるアプリのバンドル識別子が含まれている場合、使用するプロバイダーをこのフィールドで指定します。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  –［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  –［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
  – オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  – **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
    * ドメイン: 追加するドメインを入力します。
    *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

iOS 向け **IKEv2** プロトコルの構成

このセクションには、IKEv2、AlwaysOn IKEv2、AlwaysOn IKEv2 のデュアル構成プロトコルで使用する設定が含まれます。AlwaysOn IKEv2 デュアル構成プロトコルの場合は、携帯電話ネットワークと Wi-Fi ネットワークの両方でこれらの設定をすべて構成します。

- 自動接続の無効化をユーザーに許可： AlwaysOn プロトコルが対象です。デバイスでネットワークへの自動接続をオフにすることをユーザーに許可するかどうかを選択します。デフォルトは ［オフ］ です。
- サーバーのホスト名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ローカル識別子： IKEv2 クライアントの FQDN または IP アドレスを入力します。このフィールドは必須です。
- リモート識別子： VPN サーバーの FQDN または IP アドレスを入力します。このフィールドは必須です。
- マシン認証： この接続の認証の種類として、［共有シークレット］ または ［証明書］ を選択します。デフォルトは ［共有シークレット］ です。
  - 共有シークレット： 任意で、共有シークレットキーを入力します。
  - ［証明書］ を選択した場合は、［**ID** 資格情報］ の使用を選択します。デフォルトは ［なし］ です。
- 拡張認証が有効： 拡張認証プロトコル（EAP）を有効にするかどうかを選択します。［オン］ を選択した場合は、ユーザーアカウントと認証パスワードを入力します。
- 停止ピア検出間隔： ピアデバイスが到達可能であるかを確認するための問い合わせ頻度を選択します。デフォルトは ［なし］ です。次のオプションがあります：
  - なし： 使用不能なピアの検出を無効にします。
  - 低： 30 分ごとにピアに問い合わせます。
  - 中： 10 分ごとにピアに問い合わせます。
  - 高： 1 分ごとにピアに問い合わせます。
- モビリティおよびマルチホーミングを無効化： この機能を無効にするかどうかを選択します。
- **IPv4/IPv6** 内部サブネット属性の使用： この機能を有効にするかどうかを選択します。
- リダイレクトを無効化： リダイレクトを無効にするかどうかを選択します。
- デバイスのスリープ中 **NAT** キープアライブを有効化： AlwaysOn プロトコルが対象です。キープアライブパケットは IKEv2 接続の NAT マッピングを維持するために使用されます。このパケットは、デバイスがオンになっているとチップによって定期的な間隔で送信されます。設定を［オン］にすると、デバイスがスリープ中でもキープアライブパケットはチップで送信されます。デフォルト間隔は、Wi-Fi 経由で 20 秒、携帯経由で 110 秒です。この間隔は、NAT キープアライブ間隔のパラメーターを使用して変更できます。
- **NAT** キープアライブ間隔（秒）： デフォルトでは 20 秒です。
- **Perfect Forward Secrecy** を有効化： この機能を有効にするかどうかを選択します。
- **DNS** サーバーの **IP** アドレス： オプション。DNS サーバーの IP アドレス文字列の一覧です。これらの IP アドレスには、IPv4 アドレスと IPv6 アドレスを混在させることができます。［追加］ をクリックしてアドレスを入力します。
- ドメイン名： オプション。トンネルのプライマリドメインです。

- 検索ドメイン: オプション。単一ラベルホスト名の完全修飾に使用されるドメインの一覧です。
- 補足マッチドメインをリゾルバー一覧に追加する: オプション。補足マッチドメイン一覧を、リゾルバーの検索ドメイン一覧に追加するかどうかを決定します。デフォルトは ［オン］ です。
- 補足マッチドメイン: オプション。どの DNS クエリが DNS サーバーアドレスに含まれる DNS リゾルバー設定を使用するかを判別するドメイン文字列の一覧です。このキーは、特定のドメインのホストのみがトンネルの DNS リゾルバーを使用して解決される、分割 DNS 設定を作成するために使用されます。この一覧のドメインにないホストは、システムのデフォルトのリゾルバーを使用して解決されます。

このパラメーターに空の文字列が含まれる場合は、この文字列がデフォルトのドメインです。これにより、分割トンネルの設定によって、すべての DNS クエリをプライマリ DNS サーバーの前にまず VPN DNS サーバーに振り分けることができます。VPN トンネルがネットワークのデフォルトルートである場合、一覧に追加された DNS サーバーはデフォルトのリゾルバーになります。この場合、補足マッチドメインの一覧は無視されます。

- **IKE SA** パラメーターおよび子 **SA** パラメーター: Security Association（SA）パラメーターオプションごとに、次の設定を構成します:
  - 暗号化アルゴリズム: 一覧から、使用する IKE 暗号化アルゴリズムを選択します。デフォルトは **3DES** です。
  - 整合性アルゴリズム: 一覧から、使用する整合性アルゴリズムを選択します。デフォルトは **SHA1-96** です。
  - **Diffie Hellman** グループ: 一覧から、Diffie Hellman グループ番号を選択します。デフォルトは **2** です。
  - **ike** 有効期間（分）: SA の有効期間（キー更新間隔）を表す 10 ～ 1440 の整数を入力します。デフォルトは **1440** 分です。
- サービスの例外: AlwaysOn プロトコルが対象です。サービスの例外とは、Always On VPN から除外されたシステムサービスです。次のサービス例外設定を構成します
  - ボイスメール: 一覧から、ボイスメールの例外を処理する方法を選択します。デフォルトは ［トンネル経由のトラフィックを許可］ です。
  - **AirPrint**: 一覧から、AirPrint の例外を処理する方法を選択します。デフォルトは ［トンネル経由のトラフィックを許可］ です。
  - **VPN** トンネル外のキャプティブ **Web** シートからのトラフィックを許可: ユーザーが VPN トンネルの外側にある公衆ホットスポットに接続するのを許可するかどうかを選択します。デフォルトは ［オフ］ です。
  - **VPN** トンネル外のすべてのキャプティブネットワークアプリからのトラフィックを許可: VPN トンネルの外側にあるすべてのホットスポットネットワーキングアプリを許可するかどうかを選択します。デフォルトは ［オフ］ です。
  - キャプティブネットワークアプリのバンドル **ID**: ユーザーによるアクセスが許可されているホットスポットネットワーキングのアプリバンドル ID ごとに、［追加］ をクリックしてホットスポットネットワ

ーキングのアプリバンドル **ID** を入力します。［保存］ をクリックしてアプリバンドル ID を保存します。

- アプリ単位の **VPN**。次の設定を IKEv2 の接続の種類用に構成します。
  - **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。
  - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - **Safari** ドメイン：［追加］ をクリックして、Safari ドメイン名を追加します。
- プロキシ構成： プロキシサーバー経由での VPN 接続のルーティング方法を選択します。デフォルトは ［なし］ です。

iOS 向け **Citrix SSO** プロトコルの構成

Citrix SSO クライアントは、Apple Store（https://apps.apple.com/us/app/citrix-sso/id1333396910）で入手することができます。

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求： ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを［オン］に設定した場合は、次の設定を構成します：
  - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
  - プロバイダーの種類： Per-App VPN が ［アプリプロキシ］ で提供されるか、［パケットトンネル］ で提供されるかを選択します。デフォルトは ［アプリプロキシ］ です。
  - プロバイダーの種類： ［パケットトンネル］ に設定します。

  - **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
    * ドメイン: 追加するドメインを入力します。
    * ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
- カスタム **XML**: 追加するカスタム XML パラメーターごとに、［追加］ をクリックしてキーと値のペアを指定します。使用できるパラメーターは次のとおりです:
  - **disableL3**: システムレベルの VPN を無効化します。アプリごとの VPN のみ許容します。値は不要です。
  - **useragent**: このデバイスポリシーに、VPN プラグインクライアントを対象とする任意の Citrix Gateway ポリシーを関連付けます。このキーの値は、プラグインによって開始される要求に対応して、VPN プラグインに自動的に追加されます。

iOS 向けカスタム **SSL** プロトコルの構成

従来の Cisco AnyConnect クライアントから Cisco AnyConnect クライアントに移行するには:

1. カスタム SSL プロトコルを使用して VPN デバイスポリシーを構成します。iOS デバイスにポリシーを展開します。
2. Cisco AnyConnect クライアントをhttps://apps.apple.com/us/app/cisco-anyconnect/id1135064690からアップロードし、このアプリを XenMobile に追加してから iOS デバイスに展開します。
3. iOS デバイスから古い VPN デバイスポリシーを削除します。

設定:

- カスタム **SSL** 識別子（リバース **DNS** 形式）: バンドル ID に設定します。Cisco AnyConnect クライアントの場合は、**com.cisco.anyconnect** を使用します。
- プロバイダーのバンドル識別子:［カスタム **SSL** 識別子］ で指定したアプリに同じ種類（アプリプロキシまたはパケットトンネル）の VPN プロバイダーが複数設定されている場合、このバンドル ID を指定します。Cisco AnyConnect クライアントの場合は、**com.cisco.anyconnect** を使用します。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。

        * オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「iOS 向け［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを［オン］に設定した場合は、次の設定を構成します：
    - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
    - プロバイダーの種類： プロバイダーの種類では、プロバイダーが VPN サービスとプロキシサービスのどちらであるかを指定します。VPN サービスの場合は ［パケットトンネル］ を選択します。プロキシサービスの場合は ［アプリプロキシ］ を選択します。Cisco AnyConnect クライアントの場合は、［パケットトンネル］ を選択します。
    - **Safari** ドメイン： アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います：
        * ドメイン： 追加するドメインを入力します。
        *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
- カスタム **XML**：追加するカスタム XML パラメーターごとに、［追加］をクリックして以下の操作を行います。
    - パラメーター名： 追加するパラメーターの名前を入力します。
    - 値：［パラメーター名］ に関連付ける値を入力します。
    -［保存］をクリックしてパラメーターを保存するか、［キャンセル］をクリックして操作を取り消します。

NAC をサポートするように **VPN** デバイスポリシーを設定するには

1. NAC フィルターを設定するには、カスタム **SSL** の接続の種類が必要です。
2. **VPN** の ［接続名］ を指定します。
3.［カスタム **SSL** 識別子］に、「**com.citrix.NetScalerGateway.ios.app**」と入力します。
4.［プロバイダーのバンドル識別子］ に、「**com.citrix.NetScalerGateway.ios.app.vpnplugin**」と入力します。

手順 3 と手順 4 の値は、NAC のフィルタリングに必要な Citrix SSO インストールの値です。認証パスワードは設定しないでください。NAC 機能の使用の詳細については、「ネットワークアクセス制御」を参照してください。

iOS 向け［オンデマンドに **VPN** を有効化］オプションの構成

- オンデマンドドメイン： ドメインごと、およびユーザーがドメインに接続したときに実行される関連アクションごとに、［追加］ をクリックして以下の操作を行います：
- ドメイン： 追加するドメインを入力します。
- アクション： 一覧から、提供されているアクションのいずれかを選択します：

- 常に確立: ドメインは常に VPN 接続をトリガーします。
- 確立しない: ドメインは VPN 接続をトリガーしません。
- 必要な場合確立: ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
- ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

• オンデマンドルール
  - アクション: 一覧から、実行するアクションを選択します。デフォルトは ［**EvaluateConnection**］ です。選択できるアクションは以下のとおりです:
    * 許可: トリガーされたときに VPN オンデマンドで接続できるようにします。
    * 接続: 無条件で VPN 接続を開始します。
    * 切断: VPN 接続を解除し、規則と一致しない限りオンデマンドの再接続を行いません。
    * **EvaluateConnection**: 接続ごとに、［ActionParameters］アレイを評価します。
    * 無視: 既存の VPN 接続を動作中のままにします。ただし、規則と一致しない限りオンデマンドの再接続を行いません。
  - **DNSDomainMatch**: デバイスの検索ドメイン一覧と一致する可能性のある、追加するドメインごとに、［追加］ をクリックして以下の操作を行います:
    * **DNS** ドメイン: ドメイン名を入力します。ワイルドカード文字「*」をプレフィックスに使用すると、複数のドメインと一致させることができます。たとえば、*.example.com は、mydomain.example.com、yourdomain.example.com、herdomain.example.com と一致します。
    *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **DNSServerAddressMatch**: ネットワークの指定された DNS サーバーと一致する可能性のある、追加する IP アドレスごとに、［追加］ をクリックして以下の操作を行います。
    * **DNS** サーバーアドレス: 追加する DNS サーバーアドレスを入力します。ワイルドカード文字「」をサフィックスに使用すると、複数の *DNS* サーバーと一致させることができます。たとえば、*17.* はクラス A サブネットのすべての DNS サーバーと一致します。
    *［保存］ をクリックして DNS サーバーアドレスを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **InterfaceTypeMatch**: 一覧から、使用中のプライマリネットワークインターフェイスハードウェアの種類を選択します。デフォルトは ［未指定］ です。使用できる値は以下のとおりです:
    * 未指定: あらゆるネットワークインターフェイスハードウェアと一致します。このオプションがデフォルトです。
    * イーサネット: イーサネットネットワークインターフェイスハードウェアのみと一致します。
    * **Wi-Fi**: Wi-Fi ネットワークインターフェイスハードウェアのみと一致します。
    * 携帯ネットワーク: 携帯ネットワークインターフェイスハードウェアのみと一致します。
  - **SSIDMatch**: 現在のネットワークと照合する、追加する SSID ごとに、［追加］ をクリックして以下の操作を行います。

        * **SSID**: 追加する SSID を入力します。ネットワークが Wi-Fi ネットワークでない場合、または SSID が表示されない場合は照合できません。すべての SSID と一致させるには、この一覧を空白のままにします。
        * ［保存］ をクリックして SSID を保存するか、［キャンセル］ をクリックして操作を取り消します。
    - **URLStringProbe**: フェッチする URL を入力します。この URL がリダイレクトされず正常にフェッチされた場合は、この規則に一致しています。
    - **ActionParameters**: **Domains**: EvaluateConnection のチェック対象となる、追加するドメインごとに、［追加］ をクリックして以下の操作を実行します:
        * ドメイン: 追加するドメインを入力します。
        * ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
    - **ActionParameters : DomainAction**: 一覧から、［**ActionParameters : Domains**］ で指定したドメインに対する **VPN** の動作を選択します。デフォルトは ［**ConnectIfNeeded**］ です。選択できるアクションは以下のとおりです:
        * **ConnectIfNeeded**: ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
        * **NeverConnect**: ドメインは VPN 接続をトリガーしません。
    - **Action Parameters**: **RequiredDNSServers**: 指定したドメインの解決に使用する DNS サーバーの IP アドレスごとに、［追加］ をクリックして以下の操作を行います:
        * **DNS** サーバー: ［**ActionParameters** :**DomainAction**］が ［**ConnectIfNeeded**］ の場合にのみ有効です。追加する DNS サーバーを入力します。このサーバーは、デバイスの現在のネットワーク構成に含まれている必要はありません。この DNS サーバーに到達できない場合、対応として VPN 接続が確立されます。この DNS サーバーは、内部 DNS サーバーまたは信頼できる外部 DNS サーバーである必要があります。
        * ［保存］ をクリックして DNS サーバーを保存するか、［キャンセル］ をクリックして操作を取り消します。
    - **ActionParameters : RequiredURLStringProbe**: 任意で、プローブする HTTP または HTTPS（推奨）の URL を、GET リクエストを使用して入力します。URL のホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、対応として VPN 接続が確立されます。［**ActionParameters** : **DomainAction**］ が ［**ConnectIfNeeded**］ の場合にのみ有効です。
    - **OnDemandRules : XML content**: XML 構成オンデマンド規則を入力するか、コピーして貼り付けます。
        * ［ディクショナリをチェック］ をクリックし、XML コードを検証します。XML が有効な場合は、［**XML** コンテンツ］ テキストボックスの下に緑色の文字で「有効な XML」と表示されます。XML が有効でない場合は、エラーを説明するエラーメッセージがオレンジ色の文字で表示されます。
- プロキシ
    - プロキシ構成: 一覧から、VPN 接続のプロキシサーバーのルーティング方法を選択します。デフォルトは ［なし］ です。

    * ［手動］ を有効にした場合は、次の設定を構成します:
        - プロキシサーバーのホスト名または **IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
        - プロキシサーバーのポート: プロキシサーバーのポート番号を入力します。このフィールドは必須です。
        - ユーザー名: 任意で、プロキシサーバーのユーザー名を入力します。
        - パスワード: 任意で、プロキシサーバーのパスワードを入力します。
    * ［自動］ を選択した場合は、次の設定を構成します:
        - プロキシサーバー **URL**: プロキシサーバーの URL を入力します。このフィールドは必須です。

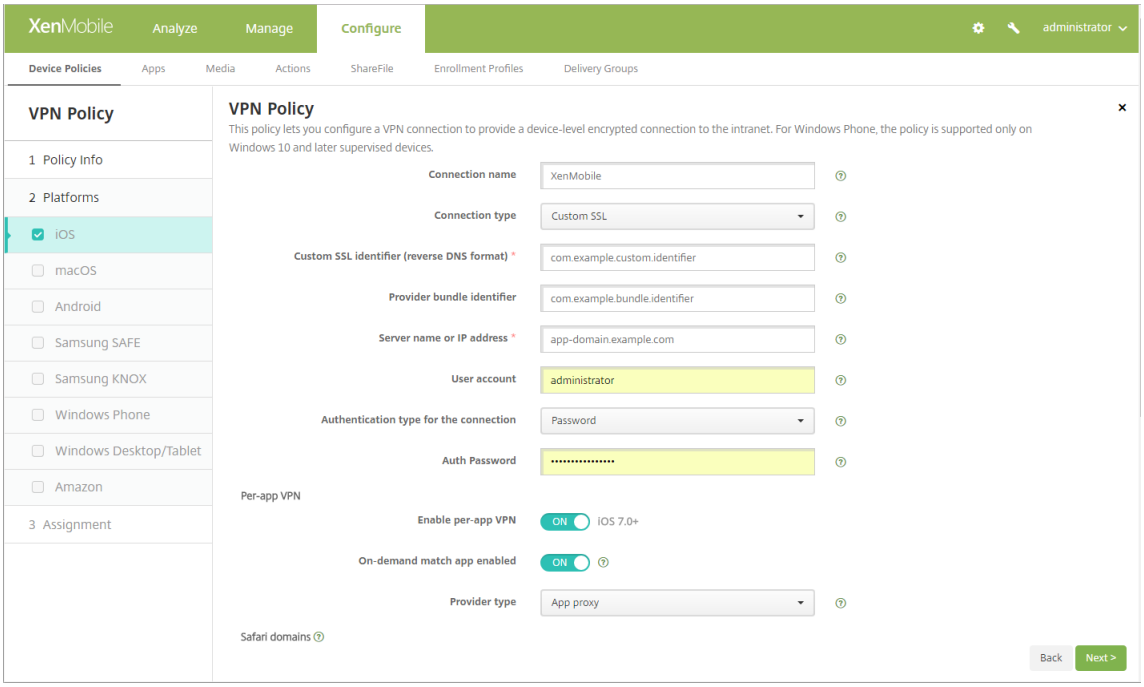
- ポリシー設定
  - ［ポリシー設定］ の下の ［ポリシーの削除］ の横にある、［日付を選択］ または ［削除までの期間（日）を指定］ をクリックします。
  - ［日付を選択］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［ユーザーにポリシーの削除を許可］ の一覧で、［常に］、［パスワードが必要］、［しない］ のいずれかを選択します。
  - ［パスワードが必要］ を選択した場合、［パスワードを削除］ の横に必要なパスワードを入力します。

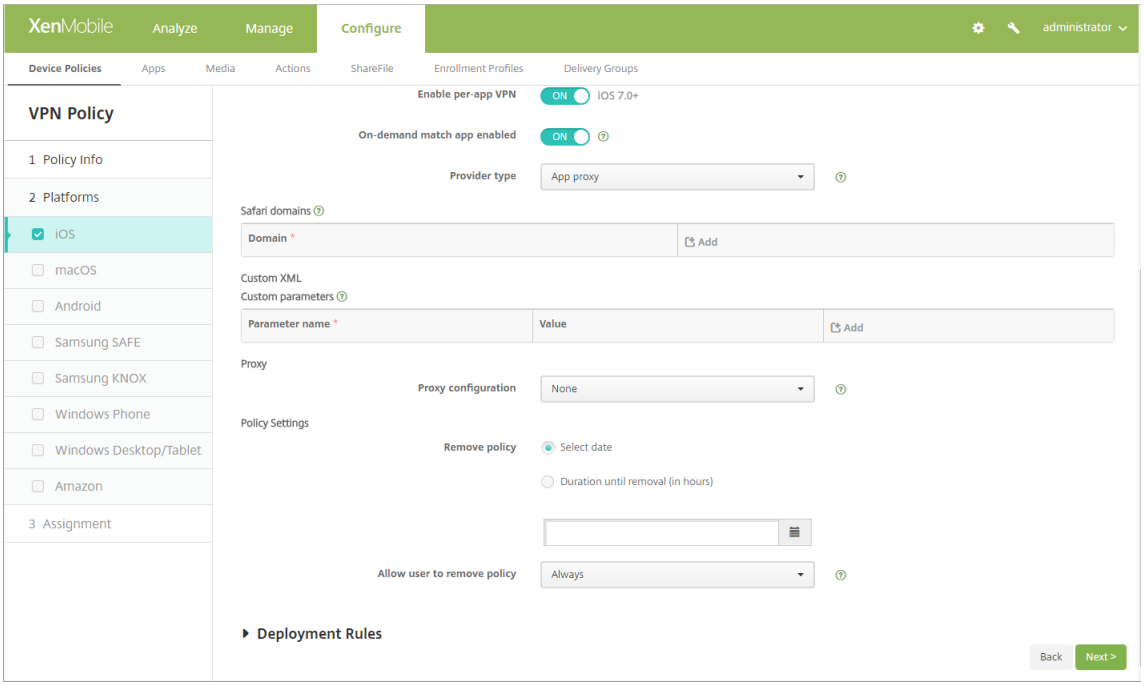
Per-App VPN の構成

iOS 向けの Per-App VPN オプションは、Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO、およびカスタム SSL の接続の種類で使用できます。

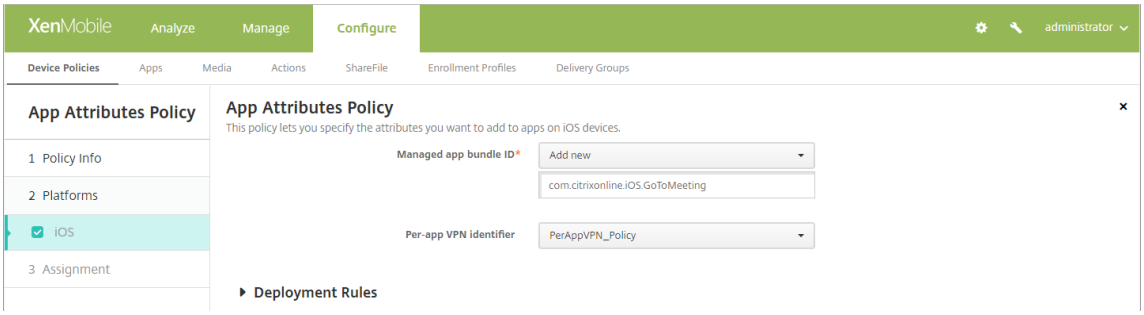
Per-App VPN を構成するには次の手順に従います。

1. ［構成］ **>** ［デバイスポリシー］ で、VPN ポリシーを作成します。次に例を示します:

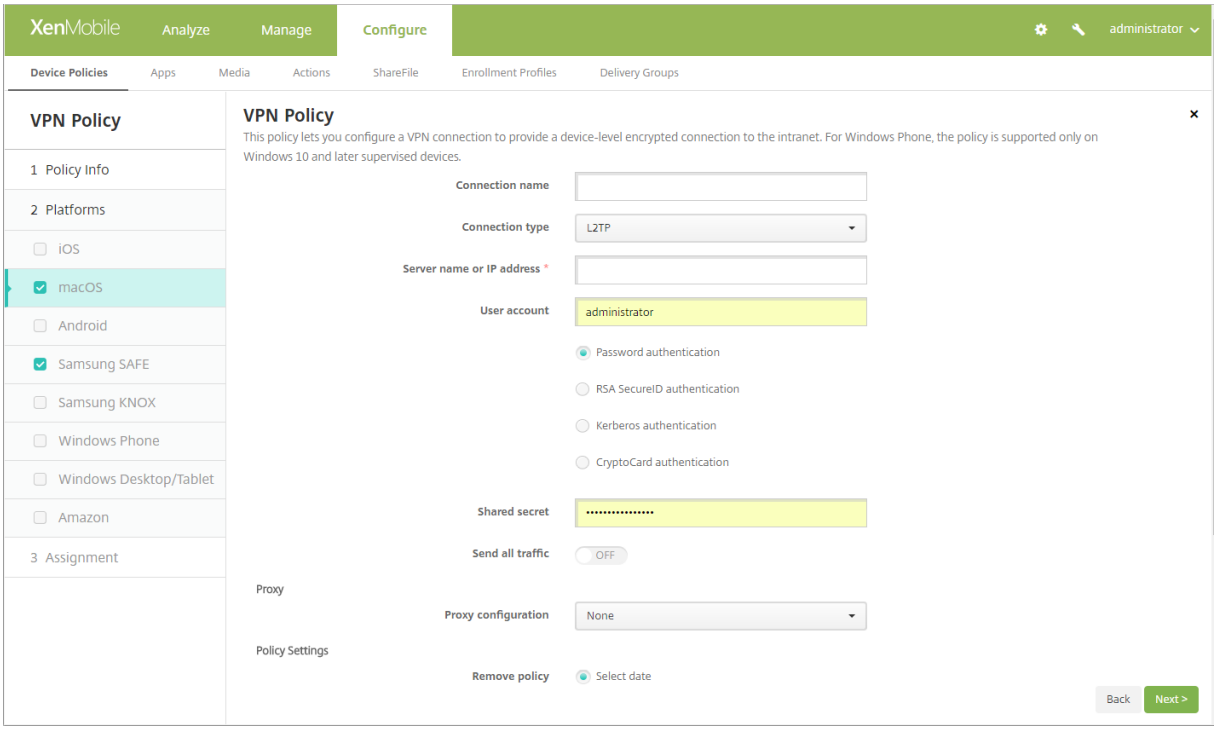




2. [構成] > [デバイスポリシー] でアプリ属性ポリシーを作成し、アプリをこの Per-App VPN ポリシーに関連付けます。 [**Per-app VPN** 識別子] では、手順 1 で作成した VPN ポリシーの名前を選択します。 [管理対象アプリのバンドル **ID**] は、アプリ一覧から選択するか、アプリバンドル ID を入力します（iOS アプリインベントリポリシーを展開している場合は、アプリ一覧にアプリが含まれます）。



macOS 設定



- 接続名： 接続名を入力します。
- 接続の種類： 一覧から、この接続において使用するプロトコルを選択します。デフォルトは［L2TP］です。
  - **L2TP**： レイヤー 2 トンネリングプロトコルと事前共有キー認証。
  - **PPTP**： Point-to-Point トンネリング。
  - **IPSec**： 社内 VPN 接続
  - **Cisco AnyConnect**： Cisco AnyConnect VPN クライアント
  - **Juniper SSL**： Juniper Networks SSL VPN クライアント
  - **F5 SSL**： F5 Networks SSL VPN クライアント
  - **SonicWALL Mobile Connect**： iOS 用 Dell 統合 VPN クライアント
  - **Ariba VIA**： Aruba Networks 仮想インターネットアクセスクライアント
  - **Citrix VPN**： Citrix VPN クライアント
  - カスタム **SSL**： カスタム SSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

macOS 向け **L2TP** プロトコルの設定

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- [パスワード認証]、[**RSA SecurID** 認証]、[**Kerberos** 認証]、[**CryptoCard** 認証] のいずれかを選択します。デフォルトは [パスワード認証] です。
- 共有シークレット: IPsec 共有シークレットキーを入力します。
- すべてのトラフィックを送信: VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは [オフ] です。

macOS 向け **PPTP** プロトコルの設定

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- [パスワード認証]、[**RSA SecurID** 認証]、[**Kerberos** 認証]、[**CryptoCard** 認証] のいずれかを選択します。デフォルトは [パスワード認証] です。
- 暗号化レベル: 必要な暗号化レベルを選択します。デフォルトは [なし] です。
  - なし: 暗号化を使用しません。
  - 自動: サーバーでサポートされている最も強力な暗号化レベルを使用します。
  - **Maximum (128-bit)**: 常に 128 ビットの暗号化を使用します。
- すべてのトラフィックを送信: VPN 経由ですべてのトラフィックを送信するかどうかを選択します。デフォルトは [オフ] です。

macOS 向け **IPsec** プロトコルの構成

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧から、この接続の認証の種類として、[共有シークレット] または [証明書] を選択します。デフォルトは [共有シークレット] です。
  - [共有シークレット] 認証を有効にした場合は、次の設定を構成します。
    * グループ名: 任意で、グループ名を入力します。
    * 共有シークレット: 任意で、共有シークレットキーを入力します。
    * ハイブリッド認証を使用: ハイブリッド認証を使用するかどうかを選択します。ハイブリッド認証では、まずサーバーがクライアントに対する認証を行い、次にクライアントがサーバーに対する認証を行います。デフォルトは [オフ] です。
    * パスワードの入力を要求: ネットワークへの接続時にユーザーにパスワードの入力を求めるかどうかを選択します。デフォルトは [オフ] です。

- ［証明書］ 認証を有効にした場合は、次の設定を構成します。
  - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
  - 接続時に **PIN** を要求： ネットワークへの接続時にユーザーによる PIN の入力を必須とするかどうかを選択します。デフォルトは ［オフ］ です。
  - オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［Enable VPN on demand］オプションの構成」を参照してください。

macOS 向け **Cisco AnyConnect** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- グループ： 任意で、グループ名を入力します。
- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します:
    - **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    - 接続時に **PIN** を要求： ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    - オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［Enable VPN on demand］オプションの構成」を参照してください。
  - **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
    - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
    - **Safari** ドメイン： アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
      - ドメイン： 追加するドメインを入力します。
      - ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

macOS 向け **Juniper SSL** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- 領域： オプションの領域名を入力します。
- 役割： オプションの役割名を入力します。
- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求： ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化： ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化： アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します。
  - オンデマンドマッチアプリが有効： アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - **Safari** ドメイン： アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います：
    * ドメイン： 追加するドメインを入力します。
    *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

macOS 向け **F5 SSL** プロトコルの構成

- サーバー名または **IP** アドレス： VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント： 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類： 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します：
    * **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。

    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
  - オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  - **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
    * ドメイン: 追加するドメインを入力します。
    * ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

macOS 向け **SonicWALL Mobile Connect** プロトコルの構成

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- ログオングループまたはドメイン: 任意で、ログオングループまたはドメインを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
  - オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。

- **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
  * ドメイン: 追加するドメインを入力します。
  *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

macOS 向け **Ariba VIA** プロトコルの構成

- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。
- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
- 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  –［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  –［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは［オフ］です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］設定の構成」を参照してください。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは［オフ］です。このオプションを有効にした場合は、次の設定を構成します:
  – オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。デフォルトは ［オフ］ です。
  – **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
    * ドメイン: 追加するドメインを入力します。
    *［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

macOS 向けカスタム **SSL** プロトコルの構成

- カスタム **SSL** 識別子（リバース **DNS** 形式）: SSL 識別子を逆引き DNS 形式で入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス: VPN サーバーのサーバー名または IP アドレスを入力します。このフィールドは必須です。

- ユーザーアカウント: 任意で、ユーザーアカウントを入力します。
  - 接続の認証の種類: 一覧で、この接続の認証の種類に ［パスワード］ か ［証明書］ のどちらを使用するかを選択します。デフォルトは ［パスワード］ です。
  - ［パスワード］ を有効にした場合は、［認証パスワード］ フィールドに任意の認証パスワードを入力します。
  - ［証明書］ を有効にした場合は、次の設定を構成します:
    * **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
    * 接続時に **PIN** を要求: ネットワークへの接続時にユーザーに PIN の入力を求めるかどうかを選択します。デフォルトは ［オフ］ です。
    * オンデマンドに **VPN** を有効化: ネットワークに接続する時に、VPN 接続のトリガーを有効にするかどうかを選択します。デフォルトは ［オフ］ です。［オンデマンドに **VPN** を有効化］ が ［オン］ であるときの設定の構成について詳しくは、「［オンデマンドに VPN を有効化］設定の構成」を参照してください。
  - **Per-app VPN**: アプリごとの VPN を有効にするかどうかを選択します。デフォルトは ［オフ］ です。このオプションを有効にした場合は、次の設定を構成します:
    * オンデマンドマッチアプリが有効: アプリごとの VPN サービスにリンクされているアプリがネットワーク通信を開始したときに、アプリごとの VPN 接続が自動的にトリガーされるようにするかどうかを選択します。
    * **Safari** ドメイン: アプリごとの VPN 接続をトリガーできる、追加する Safari ドメインごとに、［追加］ をクリックして以下の操作を行います:
      - ドメイン: 追加するドメインを入力します。
      - ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
- カスタム **XML**: 追加するカスタム XML パラメーターごとに、［追加］をクリックして以下の操作を行います。
  - パラメーター名: 追加するパラメーターの名前を入力します。
  - 値:［パラメーター名］ に関連付ける値を入力します。
  - ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

［オンデマンドに **VPN** を有効化］オプションの構成

- オンデマンドドメイン: 追加するドメインおよびユーザーがドメインに接続したときに実行される関連アクションごとに、［追加］ をクリックして以下の操作を行います:
  - ドメイン: 追加するドメインを入力します。
  - アクション: 一覧から、提供されているアクションのいずれかを選択します:
    * 常に確立: ドメインは常に VPN 接続をトリガーします。
    * 確立しない: ドメインは VPN 接続をトリガーしません。
    * 必要な場合確立: ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。

- ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。

- オンデマンドルール
  - アクション: 一覧から、実行するアクションを選択します。デフォルトは ［**EvaluateConnection**］ です。選択できるアクションは以下のとおりです:
    - 許可: トリガーされたときに VPN オンデマンドで接続できるようにします。
    - 接続: 無条件で VPN 接続を開始します。
    - 切断: VPN 接続を解除し、規則と一致しない限りオンデマンドの再接続を行いません。
    - **EvaluateConnection**: 接続ごとに、［**ActionParameters**］ アレイを評価します。
    - 無視: 既存の VPN 接続を動作中のままにします。ただし、規則と一致しない限りオンデマンドの再接続を行いません。
  - **DNSDomainMatch**: ユーザーデバイスの検索ドメイン一覧と一致する可能性のある、追加するドメインごとに、［追加］ をクリックして以下の操作を行います。
    - **DNS** ドメイン: ドメイン名を入力します。ワイルドカード文字「*」をプレフィックスに使用すると、複数のドメインと一致させることができます。たとえば、*.example.com は、mydomain.example.com、yourdomain.example.com、herdomain.example.com と一致します。
    - ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **DNSServerAddressMatch**: ネットワークの指定された DNS サーバーと一致する可能性のある、追加する IP アドレスごとに、［追加］ をクリックして以下の操作を行います。
    - **DNS** サーバーアドレス: 追加する DNS サーバーアドレスを入力します。ワイルドカード文字「」をサフィックスに使用すると、複数の *DNS* サーバーと一致させることができます。たとえば、*17.* はクラス A サブネットのすべての DNS サーバーと一致します。
    - ［保存］ をクリックして DNS サーバーアドレスを保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **InterfaceTypeMatch**: 一覧から、使用中のプライマリネットワークインターフェイスハードウェアの種類を選択します。デフォルトは ［未指定］ です。使用できる値は以下のとおりです:
    - 未指定: あらゆるネットワークインターフェイスハードウェアと一致します。このオプションがデフォルトです。
    - イーサネット: イーサネットネットワークインターフェイスハードウェアのみと一致します。
    - **Wi-Fi**: Wi-Fi ネットワークインターフェイスハードウェアのみと一致します。
    - 携帯ネットワーク: 携帯ネットワークインターフェイスハードウェアのみと一致します。
  - **SSIDMatch**: 現在のネットワークと照合する、追加する SSID ごとに、［追加］ をクリックして以下の操作を行います。
    - **SSID**: 追加する SSID を入力します。ネットワークが Wi-Fi ネットワークでない場合、または SSID が表示されない場合は照合できません。すべての SSID と一致させるには、この一覧を空白のままにします。
    - ［保存］ をクリックして SSID を保存するか、［キャンセル］ をクリックして操作を取り消します。
  - **URLStringProbe**: フェッチする URL を入力します。この URL がリダイレクトされず正常にフェッ

チされた場合は、この規則に一致しています。

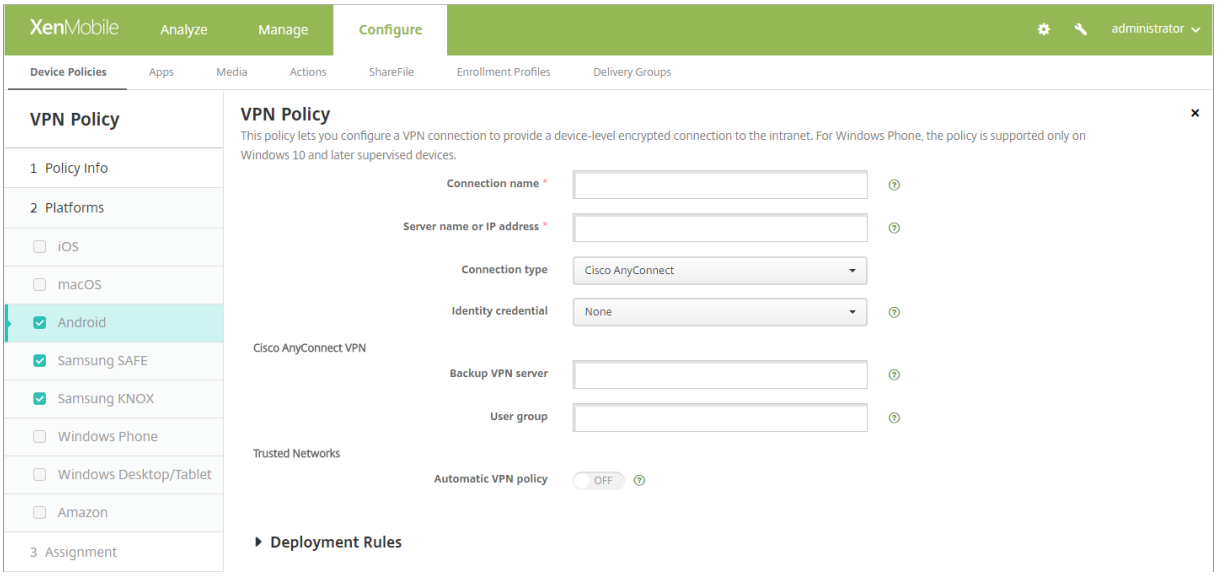
- **ActionParameters**: **Domains**: EvaluateConnection のチェック対象となる、追加するドメインごとに、［追加］ をクリックして以下の操作を実行します:
  - ドメイン: 追加するドメインを入力します。
  - ［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
- **ActionParameters : DomainAction**: 一覧から、［**ActionParameters : Domains**］で指定したドメインに対する **VPN** の動作を選択します。デフォルトは ［**ConnectIfNeeded**］ です。選択できるアクションは以下のとおりです:
  - **ConnectIfNeeded**: ドメイン名解決に失敗した場合、ドメインは VPN 接続試行をトリガーします。ドメイン名解決に失敗するのは、DNS サーバーがドメインを解決できない、別のサーバーにリダイレクトする、またはタイムアウトした場合です。
  - **NeverConnect**: ドメインは VPN 接続をトリガーしません。
- **Action Parameters**: **RequiredDNSServers**: 指定したドメインの解決に使用する DNS サーバーの IP アドレスごとに、［追加］ をクリックして以下の操作を行います:
  - **DNS** サーバー: ［**ActionParameters** :**DomainAction**］が ［**ConnectIfNeeded**］ の場合にのみ有効です。追加する DNS サーバーを入力します。このサーバーは、デバイスの現在のネットワーク構成に含まれている必要はありません。この DNS サーバーに到達できない場合、対応として VPN 接続が確立されます。この DNS サーバーは、内部 DNS サーバーまたは信頼できる外部 DNS サーバーである必要があります。
  - ［保存］ をクリックして DNS サーバーを保存するか、［キャンセル］ をクリックして操作を取り消します。
- **ActionParameters : RequiredURLStringProbe**: 任意で、プローブする HTTP または HTTPS（推奨）の URL を、GET リクエストを使用して入力します。URL のホスト名を解決できない場合、サーバーに到達できない場合、またはサーバーが応答しない場合、対応として VPN 接続が確立されます。［**ActionParameters** : **DomainAction**］ が ［**ConnectIfNeeded**］ の場合にのみ有効です。
- **OnDemandRules : XML content**: XML 構成オンデマンド規則を入力するか、コピーして貼り付けます。
  - ［ディクショナリをチェック］ をクリックし、XML コードを検証します。XML が有効な場合は、［**XML** コンテンツ］ テキストボックスの下に緑色の文字で「有効な XML」と表示されます。XML が有効でない場合は、エラーを説明するエラーメッセージがオレンジ色の文字で表示されます。

- プロキシ
  - プロキシ構成: 一覧から、VPN 接続のプロキシサーバーのルーティング方法を選択します。デフォルトは ［なし］ です。
    - ［手動］ を有効にした場合は、次の設定を構成します:
      - プロキシサーバーのホスト名または **IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。このフィールドは必須です。
      - プロキシサーバーのポート: プロキシサーバーのポート番号を入力します。このフィールドは必須です。

・ユーザー名: 任意で、プロキシサーバーのユーザー名を入力します。
・パスワード: 任意で、プロキシサーバーのパスワードを入力します。

* [自動] を選択した場合は、次の設定を構成します:
・プロキシサーバー **URL**: プロキシサーバーの URL を入力します。このフィールドは必須です。

Android の設定



Android 向け **Cisco AnyConnect VPN** プロトコルの構成

- 接続名: Cisco AnyConnect VPN 接続の名前を入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス: VPN サーバーの名前または IP アドレスを入力します。このフィールドは必須です。
- **ID** 資格情報: 一覧から、ID 資格情報を選択します。
- バックアップ **VPN** サーバー: バックアップ VPN サーバー情報を入力します。
- ユーザーグループ: ユーザーグループ情報を入力します。
- 信頼されたネットワーク
  - 自動 **VPN** ポリシー: このオプションをオンまたはオフにして、信頼できるネットワークおよび信頼できないネットワークに対する VPN の動作方法を設定します。有効にした場合は、次の設定を構成します。
    * 信頼されたネットワークポリシー: 一覧から、目的のポリシーを選択します。デフォルトは [切断] です。選択できるオプションは以下のとおりです:
      ・切断: クライアントにより、信頼できるネットワーク圏内の VPN 接続が終了されます。この設定がデフォルトです。
      ・接続: クライアントにより、信頼できるネットワーク圏内の VPN 接続が開始されます。

・何もしない: クライアントによるアクションはありません。
・一時停止: 信頼できるネットワーク圏外で VPN セッションが確立された後、信頼済みとして構成されたネットワークにユーザーがアクセスすると、VPN セッションが一時停止されます。ユーザーが信頼できるネットワークから離れると、セッションが再開されます。この設定により、信頼できるネットワークを離れた後に新しい VPN セッションを確立する手間が省かれます。

* 信頼されていないネットワークポリシー: 一覧から、目的のポリシーを選択します。デフォルトは［接続］ です。選択できるオプションは以下のとおりです:
・接続: クライアントにより、信頼できないネットワーク圏内で VPN 接続が開始されます。
・何もしない: クライアントにより、信頼できないネットワーク圏内で VPN 接続が開始されます。このオプションにより、［常時 VPN に接続］が無効化されます。

– 信頼されたドメイン: クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるドメインサフィックスごとに、［追加］ をクリックして以下の操作を行います:
* ドメイン: 追加するドメインを入力します。
*［保存］ をクリックしてドメインを保存するか、［キャンセル］ をクリックして操作を取り消します。
– 信頼されたサーバー: クライアントが信頼できるネットワーク圏内にある場合、ネットワークインターフェイスに設定することができるサーバーアドレスごとに、［追加］ をクリックして以下の操作を行います。
* サーバー: 追加するサーバーを入力します。
*［保存］ をクリックしてサーバーを保存するか、［キャンセル］ をクリックして操作を取り消します。

Android 向け **Citrix SSO** プロトコルの構成

- 接続名: VPN 接続名を入力します。このフィールドは必須です。
- サーバー名または **IP** アドレス: Citrix Gateway の FQDN または IP アドレスを入力します。
- 接続の認証の種類: 認証の種類を選択し、選択した種類に応じて表示される次のフィールドに入力します。
  –［ユーザー名］ と ［パスワード］: 認証の種類で ［パスワード］ または ［パスワードおよび証明書］ を選択した場合に、VPN 資格情報を入力します。オプションです。VPN 資格情報を入力しない場合は、Citrix VPN アプリによってユーザー名とパスワードの入力が求められます。
  – **ID** 資格情報: 認証の種類が ［証明書］ または ［パスワードおよび証明書］ の場合に表示されます。一覧で、ID 資格情報を選択します。
- **Per-App VPN** の有効化: アプリごとの VPN を有効にするかどうかを選択します。Per-App VPN を有効にしない場合は、すべてのトラフィックが Citrix VPN トンネルを経由します。Per-App VPN を有効にした場合は、次の設定を指定します。デフォルトは ［オフ］ です。

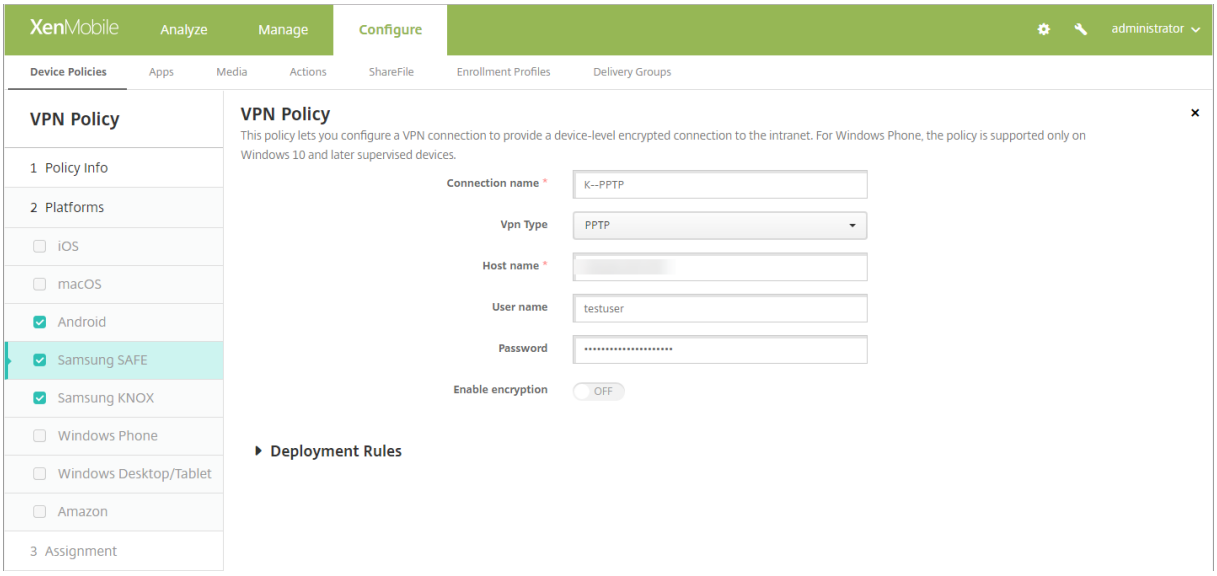
  - ホワイトリストまたはブラックリスト: ［ホワイトリスト］ の場合は、ホワイトリストに登録されたすべてのアプリがこの VPN を経由します。［ブラックリスト］ の場合は、ブラックリストに登録されたアプリ以外のすべてのアプリがこの VPN を経由します。
  - アプリケーション一覧: ホワイトリストまたはブラックリストに登録するアプリを指定します。［追加］をクリックし、アプリのパッケージ名のコンマ区切りの一覧を入力します。

- カスタム **XML**:［追加］ をクリックし、カスタムパラメーターを入力します。XenMobile では、Citrix VPN について次のパラメーターがサポートされます。
  - **DisableUserProfiles**: オプションです。このパラメーターを有効にするには、［値］ に「**Yes**」と入力します。有効にした場合、ユーザーが追加した VPN 接続が XenMobile に表示されなくなり、ユーザーは接続を追加できなくなります。この設定はグローバルな制限で、すべての VPN プロファイルに適用されます。
  - **userAgent**: 文字列値です。各 HTTP 要求で送信する任意のユーザーエージェント文字列を指定できます。指定したユーザーエージェント文字列は、Citrix VPN の既存のユーザーエージェントの末尾に追加されます。

Android Enterprise に対する **VPN** の構成

Android Enterprise デバイスに対して VPN を構成するには、Citrix SSO に対する Android Enterprise 管理対象の構成デバイスポリシーを作成します。「Android Enterprise に対する VPN プロファイルの構成」を参照してください。

Samsung SAFE の設定



- 接続名: 接続名を入力します。

- **VPN** の種類: 一覧から、この接続において使用するプロトコルを選択します。デフォルトは **L2TP with pre-shared key** です。選択できるオプションは以下のとおりです:
  - 事前共有キーを使用する **L2TP**: レイヤー 2 トンネリングプロトコルと事前共有キー認証。この設定がデフォルトです。
  - 証明書を使用する **L2TP**: レイヤー 2 トンネリングプロトコルと証明書。
  - **PPTP**: Point-to-Point トンネリング。
  - エンタープライズ: 社内 VPN 接続。Version 2.0 よりも前の SAFE バージョンに適用されます。
  - 汎用: 一般的な VPN 接続。Version 2.0 以降の SAFE バージョンに適用されます。

Samsung SAFE 向け［事前共有キーを使用する **L2TP**］プロトコルの構成

- ホスト名: VPN ホストの名前を入力します。このオプションは必須です。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- 事前共有キー: 事前共有キーを入力します。このオプションは必須です。

Samsung SAFE 向け証明書プロトコルによる **L2TP** の設定

- ホスト名: VPN ホストの名前を入力します。このオプションは必須です。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは ［なし］ です。

Samsung SAFE 向け **PPTP** プロトコルの設定

- ホスト名: VPN ホストの名前を入力します。このオプションは必須です。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- 暗号化を有効化: VPN 接続で暗号化を有効にするかどうかを選択します。

Samsung SAFE 向けエンタープライズプロトコルの構成

- ホスト名: VPN ホストの名前を入力します。このオプションは必須です。
- バックアップサーバーを有効化: バックアップ VPN サーバーを有効にするかどうかを選択します。有効にした場合は、［バックアップ **VPN** サーバー］ ボックスに、バックアップ VPN サーバーの FQDN または IP アドレスを入力します。
- ユーザー認証を有効化: ユーザー認証を必須とするかどうかを選択します。有効にした場合は、次の設定を構成します:
  - ユーザー名: ユーザー名を入力します。

  - パスワード: ユーザーパスワードを入力します。
- グループ名: 任意で、グループ名を入力します。
- 認証方法: 一覧から、使用する認証方法を選択します。選択できるオプションは以下のとおりです:
  - 証明書: 証明書認証を使用します。この設定がデフォルトです。このオプションを選択した場合は、[**ID** 資格情報] ボックスの一覧から、使用する資格情報を選択します。デフォルトは [なし] です。
  - 事前共有キー: 事前共有キーを使用します。このオプションを選択した場合は、[事前共有キー] フィールドに、共有シークレットキーを入力します。
  - ハイブリッド **RSA**: RSA 証明書を使用するハイブリッド認証を使用します。
  - **EAP MD5**: EAP ピアから EAP サーバーまでの認証を行います。ただし、相互認証は行いません。
  - **EAP MSCHAPv2**: 相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。
- **CA** 証明書: 一覧から、使用する証明書を選択します。デフォルトは [なし] です。
- デフォルトルートを有効化: VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。デフォルトは [オフ] です。
- スマートカード認証を有効化: ユーザーにスマートカードを使用した認証を許可するかどうかを選択します。デフォルトは [オフ] です。
- モバイルオプションを有効化: モバイルオプションを有効にするかどうかを選択します。デフォルトは [オフ] です。
- **Diffie-Hellman** グループ値（キーの強度）: 一覧から、使用するキー強度を選択します。デフォルトは 0 です。
- 分割トンネルの種類: 一覧から、使用する分割トンネリングの種類を選択します。デフォルトは [自動] です。選択できるオプションは以下のとおりです:
  - 自動: 分割トンネリングが自動的に使用されます。
  - 手動: 分割トンネリングが VPN サーバーで指定した IP アドレスおよびポートを介して使用されます。
  - 無効: 分割トンネリングは使用されません。
- **SuiteB** の種類: 一覧から、使用する NSA Suite B 暗号化のレベルを選択します。デフォルトは [**GCM-128**] です。選択できるオプションは以下のとおりです:
  - **GCM-128**: 128 ビットの AES-GCM 暗号化を使用します。
  - **GCM-256**: 256 ビットの AES-GCM 暗号化を使用します。
  - **GMAC-128**: 128 ビットの AES-GMAC 暗号化を使用します。
  - **GMAC-256**: 256 ビットの AES-GMAC 暗号化を使用します。
  - なし: 暗号化を使用しません。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、[追加] をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - [保存] をクリックしてルートを保存するか、[キャンセル] をクリックして操作を取り消します。

Samsung SAFE 向け汎用プロトコルの設定

- ホスト名: VPN ホストの名前を入力します。このオプションは必須です。

- ユーザー認証を有効化：ユーザー認証を必須とするかどうかを選択します。有効にした場合は、［パスワード］ボックスにユーザーパスワードを入力します。
- ユーザー名：ユーザー名を入力します。
- パッケージ名エージェント **VPN**：デバイスにインストールされた VPN のパッケージ名または ID です（例：Mocana または Pulse Secure）。
- **VPN** 接続の種類：一覧から、使用する接続の種類として［**IPSEC**］または［**SSL**］を選択します。デフォルトは［**IPSEC**］です。次のセクションでは、接続の種類ごとに、構成設定について説明します。

Samsung SAFE 向け［**IPSEC**］接続の種類の設定の構成

- **ID**：任意で、この構成の ID を入力します。
- **IPsec** グループ **ID** の種類：一覧から、使用する IPsec グループ ID の種類を選択します。デフォルトは［デフォルト］です。選択できるオプションは以下のとおりです：
  - デフォルト
  - **IPv4** アドレス
  - 完全修飾ドメイン名（**FQDN**）
  - ユーザー **FQDN**
  - **IKE** キー **ID**
- **IKE** のバージョン：一覧から、使用するインターネットキー交換バージョンを選択します。デフォルトは［**IKEv1**］です。
- 認証方法：一覧から、使用する認証方法を選択します。デフォルトは［証明書］です。選択できるオプションは以下のとおりです：
  - 証明書：証明書認証を使用します。このオプションを選択した場合は、［**ID** 資格情報］ボックスの一覧から、使用する資格情報を選択します。デフォルトは［なし］です。
  - 事前共有キー：事前共有キーを使用します。このオプションを選択した場合は、［事前共有キー］フィールドに、共有シークレットキーを入力します。
  - ハイブリッド **RSA**：RSA 証明書を使用するハイブリッド認証を使用します。
  - **EAP MD5**：EAP ピアから EAP サーバーまでの認証を行います。ただし、相互認証は行いません。
  - **EAP MSCHAPv2**：相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。
  - **CAC** ベースの認証：認証に Common Access Card（CAC）を使用します。
- **ID** 資格情報：ボックスの一覧で、使用する ID 資格情報を選択します。デフォルトは［なし］です。
- **CA** 証明書：一覧から、使用する証明書を選択します。
- 停止ピア検出を有効化：ピアが有効であるか確認するためにピアに問い合わせるかどうかを選択します。デフォルトは［オフ］です。
- デフォルトルートを有効化：VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。
- モバイルオプションを有効化：モバイルオプションを有効にするかどうかを選択します。
- **ike** 有効期間（分）：VPN 接続が再確立されるまでの時間を分単位で入力します。デフォルトは 1440 分（24 時間）です。
- **ipsec** 有効期間（分）：VPN 接続が再確立されるまでの時間を分単位で入力します。デフォルトは 1440 分

（24 時間）です。

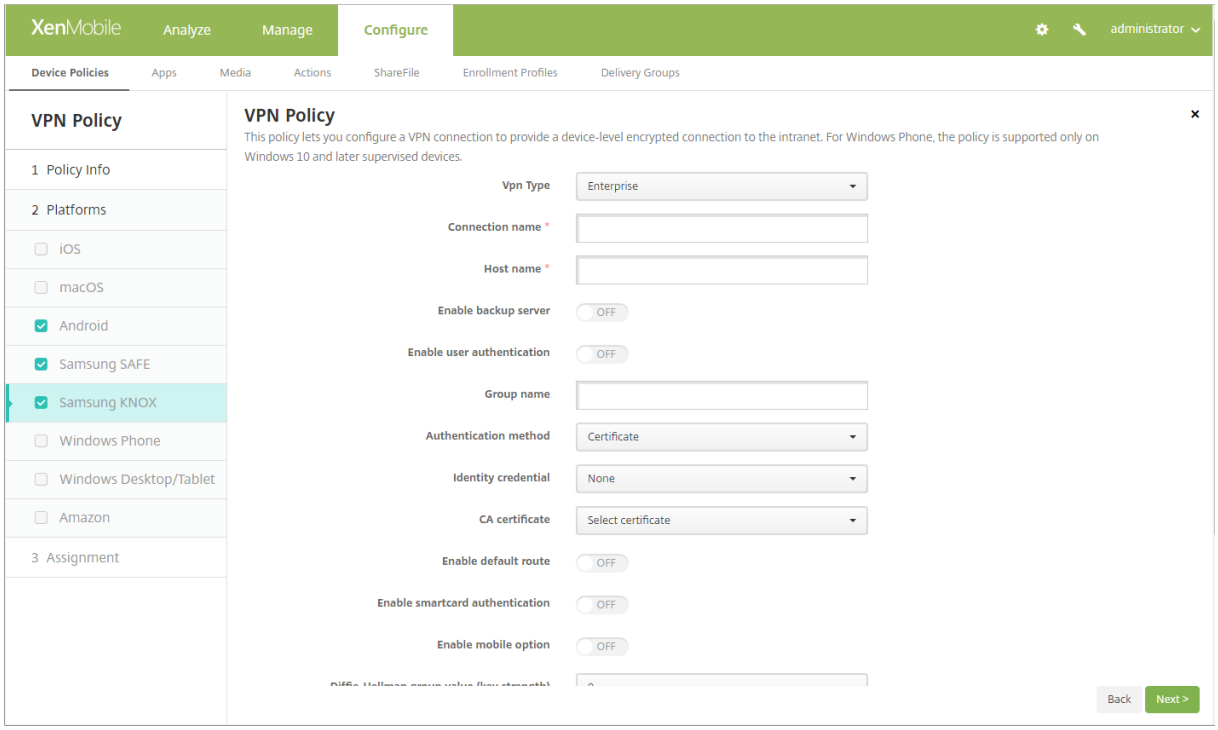
- **Diffie-Hellman** グループ値（キーの強度）： 一覧から、使用するキー強度を選択します。デフォルトは **0** です。
- **IKE** フェーズ **1** のキー交換モード： IKE フェーズ 1 のネゴシエーションモードとして、［メイン］ または ［アグレッシブ］ を選択します。デフォルトは ［メイン］ です。
  - メイン： ネゴシエーション時に情報が潜在的な攻撃者にさらされることはありませんが、［アグレッシブ］ モードより低速です。
  - アグレッシブ： ネゴシエーション時に一部の情報（ネゴシエーションを行うピアの ID など）が潜在的な攻撃者にさらされますが、［メイン］ モードより高速です。
- **Perfect Forward Secrecy**（**PFS**）値： 接続の再ネゴシエーションに新しいキー交換を必要とする PFS を使用するかどうかを選択します。
- 分割トンネルの種類： 一覧から、使用する分割トンネリングの種類を選択します。選択できるオプションは以下のとおりです：
  - 自動： 分割トンネリングが自動的に使用されます。
  - 手動： 分割トンネリングが VPN サーバーで指定した IP アドレスおよびポートを介して使用されます。
  - 無効： 分割トンネリングは使用されません。
- **IPSEC** 暗号化アルゴリズム： IPsec プロトコルが使用する VPN 構成です。
- **IKE** 暗号化アルゴリズム： IPsec プロトコルが使用する VPN 構成です。
- **IKE** 整合性アルゴリズム： IPsec プロトコルが使用する VPN 構成です。
- ベンダー： Knox API と通信する汎用エージェントの個人用プロファイルです。
- 転送ルート： 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］ をクリックして以下の操作を行います。
  - 転送ルート： 転送ルートの IP アドレスを入力します。
  - ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。
- **Per-App VPN**： 追加する各アプリごとの VPN について、［追加］ をクリックして以下の操作を行います：
  - **Per-App VPN**： アプリが通信に使用する VPN 構成です。
  - ［保存］ をクリックしてアプリごとの VPN を保存するか、［キャンセル］ をクリックして操作を取り消します。

Samsung SAFE 向け **SSL** 接続の種類の設定の構成

- 認証方法： 一覧から、使用する認証方法を選択します。デフォルトは ［該当なし］ です。選択できるオプションは以下のとおりです：
  - 該当なし
  - 証明書： 証明書認証を使用します。このオプションを選択した場合は、［**ID** 資格情報］ ボックスの一覧から、使用する資格情報を選択します。デフォルトは ［なし］ です。
  - **CAC** ベースの認証： 認証に Common Access Card（CAC）を使用します。
- **CA** 証明書： 一覧から、使用する証明書を選択します。
- デフォルトルートを有効化： VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。

- モバイルオプションを有効化: モバイルオプションを有効にするかどうかを選択します。
- 分割トンネルの種類: 一覧から、使用する分割トンネリングの種類を選択します。選択できるオプションは以下のとおりです:
  - 自動: 分割トンネリングが自動的に使用されます。
  - 手動: 分割トンネリングが VPN サーバーで指定した IP アドレスおよびポートを介して使用されます。
  - 無効: 分割トンネリングは使用されません。
- **SSL** アルゴリズム: クライアントとサーバー間のネゴシエーションに使用する SSL アルゴリズムを入力します。
- ベンダー: Knox API と通信する汎用エージェントの個人用プロファイルです。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。
- **Per-App VPN**: 追加する各アプリごとの VPN について、［追加］をクリックして以下の操作を行います:
  - **Per-App VPN**: アプリが通信に使用する VPN 構成です。
  - ［保存］をクリックしてアプリごとの VPN を保存するか、［キャンセル］をクリックして操作を取り消します。

Samsung Knox の設定



Samsung Knox のポリシーを構成した場合、ポリシーは Samsung Knox コンテナにのみ適用されます。

- **VPN** の種類: 一覧で、構成する VPN 接続の種類を選択します。接続は［エンタープライズ］（バージョン

2.0 より前の Knox バージョンに適用）または ［汎用］（バージョン 2.0 以降の Knox に適用）のいずれかを使用できます。デフォルトは ［エンタープライズ］ です。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

Samsung Knox 向けエンタープライズプロトコルの構成

- 接続名： 接続名を入力します。このフィールドは必須です。
- ホスト名： VPN ホストの名前を入力します。このオプションは必須です。
- バックアップサーバーを有効化： バックアップ VPN サーバーを有効にするかどうかを選択します。有効にした場合は、［バックアップ **VPN** サーバー］ ボックスに、バックアップ VPN サーバーの FQDN または IP アドレスを入力します。
- ユーザー認証を有効化： ユーザー認証を必須とするかどうかを選択します。有効にした場合は、次の設定を構成します：
  - ユーザー名： ユーザー名を入力します。
  - パスワード： ユーザーパスワードを入力します。
- グループ名： 任意で、グループ名を入力します。
- 認証方法： 一覧から、使用する認証方法を選択します。選択できるオプションは以下のとおりです：
  - 証明書： 証明書認証を使用します。証明書認証を使用するには、［**ID** 資格情報］ ボックスの一覧から、使用する資格情報も選択します。
  - 事前共有キー： 事前共有キーを使用します。このオプションを選択した場合は、［事前共有キー］ フィールドに、共有シークレットキーを入力します。
  - ハイブリッド **RSA**： RSA 証明書を使用するハイブリッド認証を使用します。
  - **EAP MD5**： EAP ピアから EAP サーバーまでの認証を行います。ただし、相互認証は行いません。
  - **EAP MSCHAPv2**： 相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。
- **CA** 証明書： 一覧から、使用する証明書を選択します。
- デフォルトルートを有効化： VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。
- スマートカード認証を有効化： ユーザーにスマートカードを使用した認証を許可するかどうかを選択します。デフォルトは ［オフ］ です。
- モバイルオプションを有効化： モバイルオプションを有効にするかどうかを選択します。
- **Diffie-Hellman** グループ値（キーの強度）： 一覧から、使用するキー強度を選択します。デフォルトは **0** です。
- 分割トンネルの種類： 一覧から、使用する分割トンネリングの種類を選択します。選択できるオプションは以下のとおりです：
  - 自動： 分割トンネリングが自動的に使用されます。
  - 手動： 分割トンネリングが VPN サーバーで指定した IP アドレスおよびポートを介して使用されます。
  - 無効： 分割トンネリングは使用されません。
- **SuiteB** の種類： 一覧から、使用する NSA Suite B 暗号化のレベルを選択します。選択できるオプションは以下のとおりです：
  - **GCM-128**： 128 ビットの AES-GCM 暗号化を使用します。これがデフォルトの設定です。

  - **GCM-256**： 256 ビットの AES-GCM 暗号化を使用します。
  - **GMAC-128**： 128 ビットの AES-GMAC 暗号化を使用します。
  - **GMAC-256**： 256 ビットの AES-GMAC 暗号化を使用します。
  - なし： 暗号化を使用しません。
- 転送ルート： 社内 VPN サーバーが複数のルートテーブルをサポートしている場合は、［追加］ をクリックし、任意で転送ルートを追加します。

Samsung Knox 向け汎用プロトコルの設定

- 接続名： 接続名を入力します。このフィールドは必須です。
- パッケージ名エージェント **VPN**： デバイスにインストールされた VPN のパッケージ名または ID です（例: Mocana または Pulse Secure)。
- ホスト名： VPN ホストの名前を入力します。このオプションは必須です。
- ユーザー認証を有効化： ユーザー認証を必須とするかどうかを選択します。有効にした場合は、次の設定を構成します:
  - ユーザー名： ユーザー名を入力します。
  - パスワード： ユーザーパスワードを入力します。
- **ID**： 任意で、この構成の ID を入力します。［**VPN** 接続の種類］ が［IPSEC］の場合にのみ適用されます。
- **VPN** 接続の種類： 一覧から、使用する接続の種類として［**IPSEC**］ または［**SSL**］ を選択します。デフォルトは ［**IPSEC**］ です。次のセクションでは、接続の種類ごとに、構成設定について説明します。
- ［**IPSEC**］接続の設定の構成
  - **IPsec** グループ **ID** の種類： 一覧から、使用する IPsec グループ ID の種類を選択します。デフォルトは ［デフォルト］ です。選択できるオプションは以下のとおりです:
    * デフォルト
    * **IPv4** アドレス
    * 完全修飾ドメイン名（**FQDN**）
    * ユーザー **FQDN**
    * **IKE** キー **ID**
  - **IKE** のバージョン： 一覧から、使用するインターネットキー交換バージョンを選択します。デフォルトは ［**IKEv1**］ です。
  - 認証方法： 一覧から、使用する認証方法を選択します。デフォルトは ［証明書］ です。選択できるオプションは以下のとおりです:
    * 証明書： 証明書認証を使用します。このオプションを選択した場合は、［**ID** 資格情報］ ボックスの一覧から、使用する資格情報を選択します。デフォルトは ［なし］ です。
    * 事前共有キー： 事前共有キーを使用します。このオプションを選択した場合は、［事前共有キー］ フィールドに、共有シークレットキーを入力します。
    * ハイブリッド **RSA**： RSA 証明書を使用するハイブリッド認証を使用します。
    * **EAP MD5**： EAP ピアから EAP サーバーまでの認証を行います。ただし、相互認証は行いません。
    * **EAP MSCHAPv2**： 相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。

    * **CAC** ベースの認証: 認証に Common Access Card（CAC）を使用します。
- **CA** 証明書: 一覧から、使用する証明書を選択します。
- 停止ピア検出を有効化: ピアが有効であるか確認するためにピアに問い合わせるかどうかを選択します。デフォルトは ［オフ］ です。
- デフォルトルートを有効化: VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。
- モバイルオプションを有効化: モバイルオプションを有効にするかどうかを選択します。
- **ike** 有効期間（分）: VPN 接続が再確立されるまでの時間を分単位で入力します。デフォルトは 1440 分（24 時間）です。
- **ipsec** 有効期間（分）: VPN 接続が再確立されるまでの時間を分単位で入力します。デフォルトは 1440 分（24 時間）です。
- **Diffie-Hellman** グループ値（キーの強度）: 一覧から、使用するキー強度を選択します。デフォルトは **0** です。
- **IKE** フェーズ **1** のキー交換モード: IKE フェーズ 1 のネゴシエーションモードとして、［メイン］ または ［アグレッシブ］ を選択します。デフォルトは ［メイン］ です。
    * メイン: ネゴシエーション時に情報が潜在的な攻撃者にさらされることはありませんが、［アグレッシブ］ モードより低速です。
    * アグレッシブ: ネゴシエーション時に一部の情報（ネゴシエーションを行うピアの ID など）が潜在的な攻撃者にさらされますが、［メイン］ モードより高速です。
- **Perfect Forward Secrecy**（**PFS**）値: 接続の再ネゴシエーションに新しいキー交換を必要とする PFS を使用するかどうかを選択します。
- 分割トンネルの種類: 一覧から、使用する分割トンネリングの種類を選択します。選択できるオプションは以下のとおりです:
    * 自動: 分割トンネリングが自動的に使用されます。
    * 手動: 分割トンネリングが VPN サーバーで指定した IP アドレスおよびポートを介して使用されます。
    * 無効: 分割トンネリングは使用されません。
- **SuiteB** の種類: 一覧から、使用する NSA Suite B 暗号化のレベルを選択します。デフォルトは［**GCM-128**］ です。選択できるオプションは以下のとおりです:
    * **GCM-128**: 128 ビットの AES-GCM 暗号化を使用します。
    * **GCM-256**: 256 ビットの AES-GCM 暗号化を使用します。
    * **GMAC-128**: 128 ビットの AES-GMAC 暗号化を使用します。
    * **GMAC-256**: 256 ビットの AES-GMAC 暗号化を使用します。
    * なし: 暗号化を使用しません。
- **IPSEC** 暗号化アルゴリズム: IPsec プロトコルが使用する VPN 構成です。
- **IKE** 暗号化アルゴリズム: IPsec プロトコルが使用する VPN 構成です。
- **IKE** 整合性アルゴリズム: IPsec プロトコルが使用する VPN 構成です。
- **Knox**: Samsung Knox のみの構成です。
- ベンダー: Knox API と通信する汎用エージェントの個人用プロファイルです。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、

［追加］ をクリックして以下の操作を行います。

* 転送ルート： 転送ルートの IP アドレスを入力します。
* ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。

– **Per-App VPN**： 追加する各アプリごとの VPN について、［追加］ をクリックして以下の操作を行います：

* **Per-App VPN**： アプリが通信に使用する VPN 構成です。
* ［保存］ をクリックしてアプリごとの VPN を保存するか、［キャンセル］ をクリックして操作を取り消します。

• ［**SSL**］接続の設定の構成

– 認証方法： 一覧から、使用する認証方法を選択します。選択できるオプションは以下のとおりです：

* 適用できません： 認証方法は適用されません。この設定がデフォルトです。
* 証明書： 証明書認証を使用します。この設定がデフォルトです。このオプションを選択した場合は、［ID 資格情報］ボックスの一覧から、使用する資格情報を選択します。デフォルトは［なし］です。
* **CAC** ベースの認証： 認証に Common Access Card（CAC）を使用します。

– **CA** 証明書： 一覧から、使用する証明書を選択します。
– デフォルトルートを有効化： VPN サーバーへのデフォルトルートを有効にするかどうかを選択します。
– モバイルオプションを有効化： モバイルオプションを有効にするかどうかを選択します。
– 分割トンネルの種類： 一覧から、使用する分割トンネリングの種類を選択します。選択できるオプションは以下のとおりです：

* 自動： 分割トンネリングが自動的に使用されます。
* 手動： 分割トンネリングが指定した IP アドレスおよびポートを介して使用されます。
* 無効： 分割トンネリングは使用されません。

– **SuiteB** の種類： 一覧から、使用する NSA Suite B 暗号化のレベルを選択します。デフォルトは［GCM-128］です。選択できるオプションは以下のとおりです：

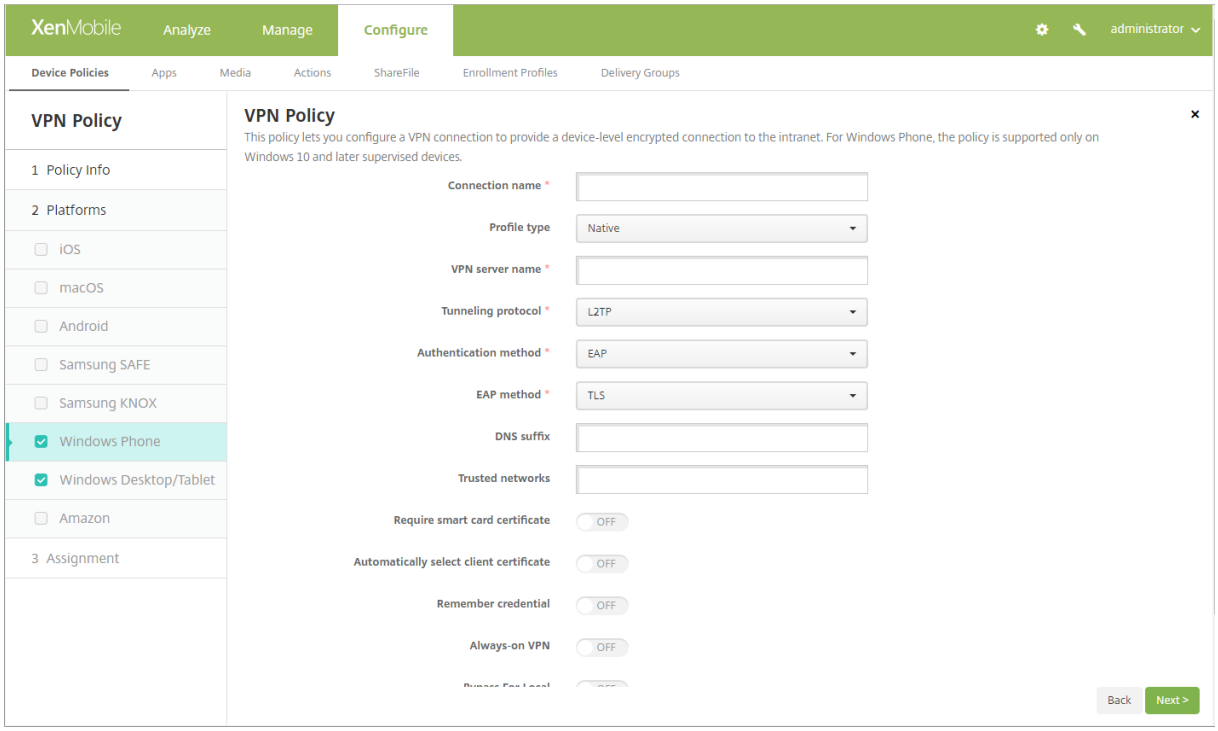
* **GCM-128**： 128 ビットの AES-GCM 暗号化を使用します。
* **GCM-256**： 256 ビットの AES-GCM 暗号化を使用します。
* **GMAC-128**： 128 ビットの AES-GMAC 暗号化を使用します。
* **GMAC-256**： 256 ビットの AES-GMAC 暗号化を使用します。
* なし：暗号化を使用しません： クライアントとサーバー間のネゴシエーションに使用する SSL アルゴリズムを入力します。

– **SSL** アルゴリズム： クライアントとサーバー間のネゴシエーションに使用する SSL アルゴリズムを入力します。
– **Knox**： Samsung Knox のみの構成です。
– ベンダー： Knox API と通信する汎用エージェントの個人用プロファイルです。
– 転送ルート： 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］ をクリックして以下の操作を行います。

* 転送ルート： 転送ルートの IP アドレスを入力します。
* ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。

- **Per-App VPN**： 追加する各アプリごとの VPN について、［追加］ をクリックして以下の操作を行います：
  - **Per-App VPN**： アプリが通信に使用する VPN 構成です。
  - ［保存］ をクリックしてアプリごとの VPN を保存するか、［キャンセル］ をクリックして操作を取り消します。

Windows Phone の設定



これらの設定は、Windows 10 以降の監視対象 Windows Phone でのみサポートされます。

- 接続名： 接続名を入力します。このフィールドは必須です。
- プロファイルの種類： 一覧から、［ネイティブ］ または ［プラグイン］ を選択します。デフォルトは ［ネイティブ］ です。次のセクションでは、各オプションの設定について説明します。
- ネイティブプロファイルタイプ設定の構成： 以下の設定は、ユーザーの Windows Phone に組み込まれている VPN に適用されます。
  - **VPN** サーバー名： VPN サーバーの FQDN または IP アドレスを入力します。このフィールドは必須です。
  - トンネリングプロトコル： 一覧から、使用する VPN トンネルの種類を選択します。デフォルトは［**L2TP**］ です。選択できるオプションは以下のとおりです：
    - **L2TP**： レイヤー 2 トンネリングプロトコルと事前共有キー認証。
    - **PPTP**： Point-to-Point トンネリング。
    - **IKEv2**： インターネットキー交換バージョン 2

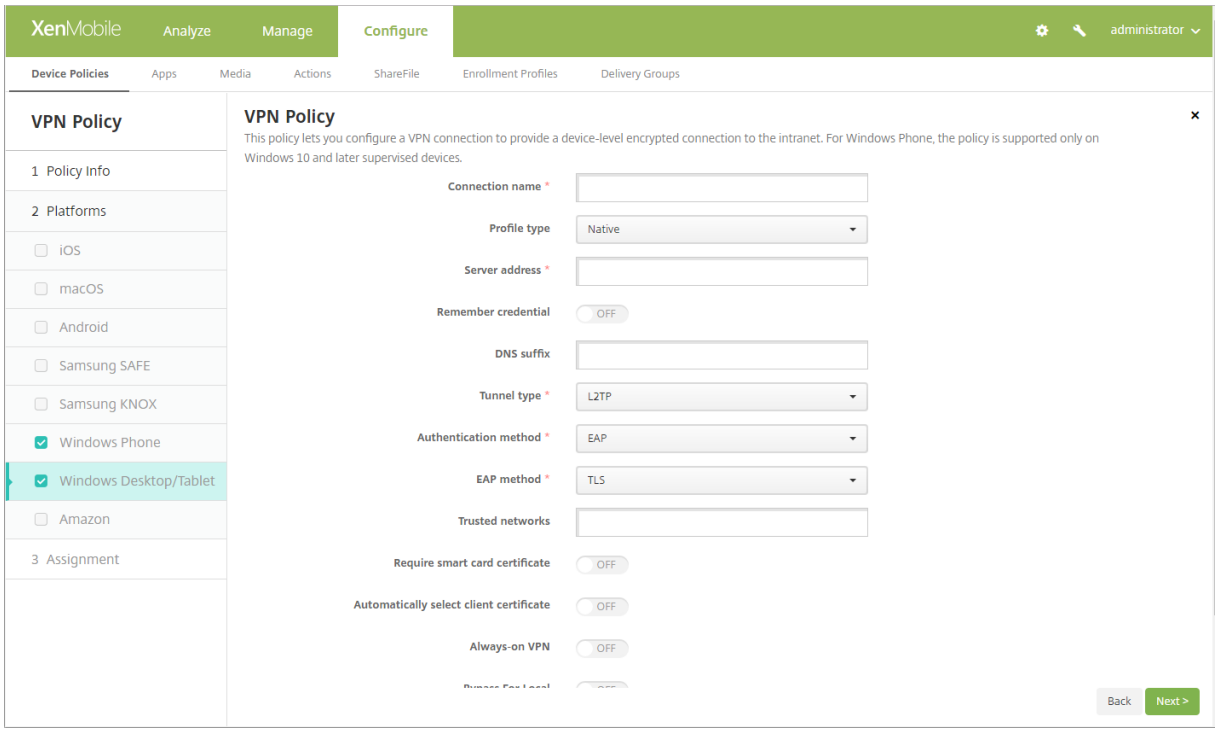
- 認証方法： 一覧から、使用する認証方法を選択します。デフォルトは ［**EAP**］ です。選択できるオプションは以下のとおりです：
  - **EAP**： 拡張認証プロトコル。
  - **MSChapV2**： 相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。トンネルの種類に［IKEv2］を選択した場合、このオプションは使用できません。［MSChapV2］を選択すると、［**Windows** 資格情報を自動的に使用］ オプションが表示されます。デフォルトは ［オフ］ です。
- **EAP** メソッド：一覧から、使用する EAP 方法を選択します。デフォルトは［**TLS**］です。[MSChapV2] 認証が有効になっている場合、このフィールドは使用できません。選択できるオプションは以下のとおりです：
  - **TLS**： Transport Layer Security
  - **PEAP**： 保護された拡張認証プロトコル
- **DNS** サフィックス： DNS サフィックスを入力します。
- 信頼されたネットワーク： アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- スマートカード証明書を要求： スマートカード証明書を必須とするかどうかを選択します。デフォルトは［オフ］です。
- クライアント証明書を自動的に選択： 認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。デフォルトは［オフ］です。［スマートカード証明書を要求］が有効になっている場合、このオプションは使用できません。
- 資格情報を保存： 資格情報をキャッシュするかどうかを選択します。デフォルトは［オフ］です。有効にすると、可能な場合に資格情報がキャッシュされます。
- 常時 **VPN** に接続： VPN を常にオンにするかどうかを選択します。デフォルトは［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
- ローカル用バイパス： ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

• プラグインプロトコルタイプの構成： 以下の設定は、Windows Store から取得し、ユーザーのデバイスにインストールした VPN プラグインに適用されます。
  - サーバーアドレス： VPN サーバーの IP アドレスを入力します。
  - クライアントアプリ **ID**： VPN プラグインのパッケージファミリ名を入力します。
  - プラグインプロファイル **XML**： 使用するカスタム VPN プラグインプロファイルの場所に ［参照］ をクリックして移動し、ファイルを選択します。形式などについて詳しくは、プラグインプロバイダーにお問い合わせください。
  - **DNS** サフィックス： DNS サフィックスを入力します。
  - 信頼されたネットワーク： アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - 資格情報を保存： 資格情報をキャッシュするかどうかを選択します。デフォルトは［オフ］です。有効

にすると、可能な場合に資格情報がキャッシュされます。

- 常時 **VPN** に接続： VPN を常にオンにするかどうかを選択します。デフォルトは［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
- ローカル用バイパス： ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

Windows デスクトップ/タブレットの設定

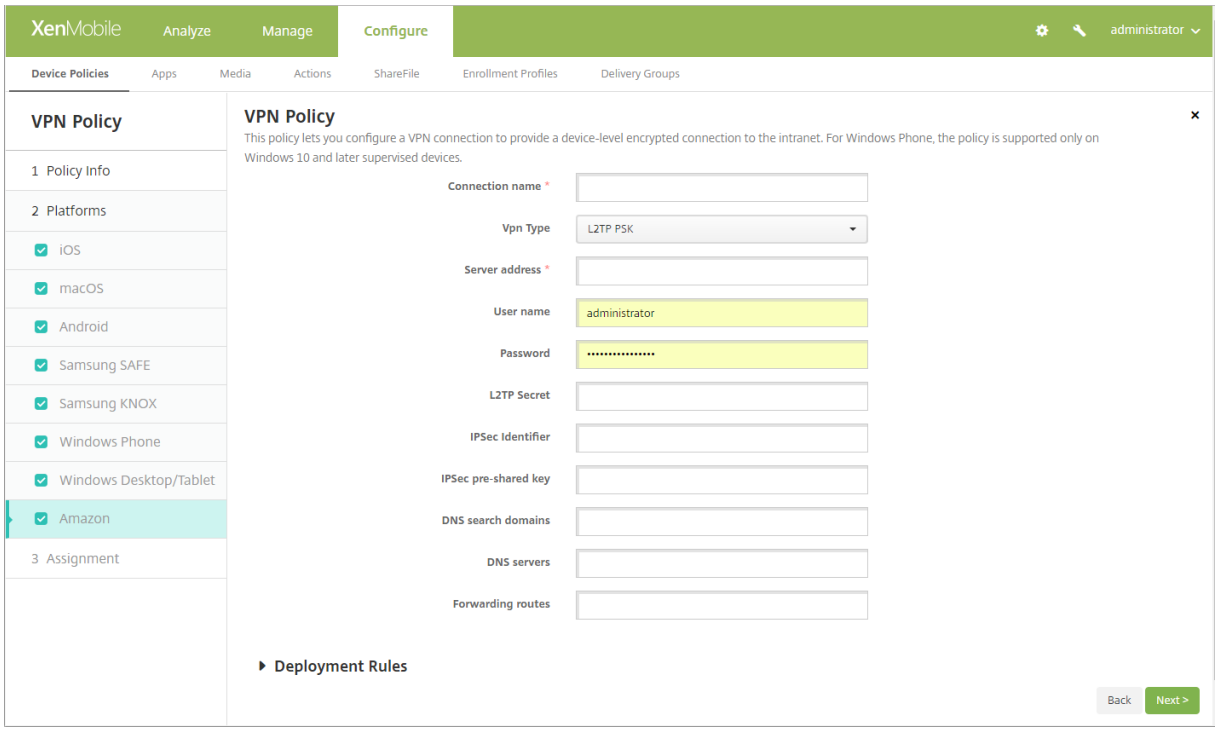


- 接続名： 接続名を入力します。このフィールドは必須です。
- プロファイルの種類： 一覧から、［ネイティブ］ または ［プラグイン］ を選択します。デフォルトは ［ネイティブ］ です。
- ネイティブプロファイルタイプの構成： 以下の設定は、ユーザーの Windows デバイスに組み込まれている VPN に適用されます。
  - サーバーアドレス： VPN サーバーの IP アドレスを入力します。このフィールドは必須です。
  - 資格情報を保存： 資格情報をキャッシュするかどうかを選択します。デフォルトは ［オフ］ です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **DNS** サフィックス： DNS サフィックスを入力します。
  - トンネルタイプ： 一覧から、使用する VPN トンネルの種類を選択します。デフォルトは ［**L2TP**］ です。選択できるオプションは以下のとおりです：
    * **L2TP**： レイヤー 2 トンネリングプロトコルと事前共有キー認証。
    * **PPTP**： Point-to-Point トンネリング。
    * **IKEv2**： インターネットキー交換バージョン 2

- 認証方法： 一覧から、使用する認証方法を選択します。デフォルトは ［**EAP**］ です。選択できるオプションは以下のとおりです：
  - **EAP**： 拡張認証プロトコル。
  - **MSChapV2**： 相互認証に Microsoft のチャレンジハンドシェイク認証を使用します。トンネルの種類に ［**IKEv2**］ を選択した場合、このオプションは使用できません。
- **EAP** メソッド：一覧から、使用する EAP 方法を選択します。デフォルトは［**TLS**］です。[MSChapV2] 認証が有効になっている場合、このフィールドは使用できません。選択できるオプションは以下のとおりです：
  - **TLS**： Transport Layer Security
  - **PEAP**： 保護された拡張認証プロトコル
- 信頼できるネットワーク： アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- スマートカード証明書を要求： スマートカード証明書を必須とするかどうかを選択します。デフォルトは ［オフ］ です。
- クライアント証明書を自動的に選択： 認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。デフォルトは ［オフ］ です。［スマートカード証明書を要求］ が有効な場合、このオプションは使用できません。
- 常時 **VPN** に接続： VPN を常にオンにするかどうかを選択します。デフォルトは ［オフ］ です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
- ローカル用バイパス： ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

- プラグインプロファイルタイプの構成： 以下の設定は、Windows Store から取得し、ユーザーのデバイスにインストールした VPN プラグインに適用されます。
  - サーバーアドレス： VPN サーバーの IP アドレスを入力します。このフィールドは必須です。
  - 資格情報を保存： 資格情報をキャッシュするかどうかを選択します。デフォルトは ［オフ］ です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **DNS** サフィックス： DNS サフィックスを入力します。
  - クライアントアプリ **ID**： VPN プラグインのパッケージファミリ名を入力します。
  - プラグインプロファイル **XML**： 使用するカスタム VPN プラグインプロファイルの場所に ［参照］ をクリックして移動し、ファイルを選択します。形式などについて詳しくは、プラグインプロバイダーにお問い合わせください。
  - 信頼されたネットワーク： アクセスに VPN 接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - 常時 **VPN** に接続： VPN を常にオンにするかどうかを選択します。デフォルトは ［オフ］ です。有効にすると、ユーザーが手動で切断するまで、VPN 接続はオンのままです。
  - ローカル用バイパス： ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

Amazon の設定



- 接続名： 接続名を入力します。
- **VPN** の種類： 一覧から、接続の種類を選択します。選択できるオプションは以下のとおりです：
  - **L2TP PSK**： レイヤー 2 トンネリングプロトコルと事前共有キー認証。この設定がデフォルトです。
  - **L2TP RSA**： レイヤー 2 トンネリングプロトコルと RSA 認証。
  - **IPSEC** 拡張認証 **PSK**： インターネットプロトコルセキュリティと事前共有キーおよび拡張認証。
  - **IPSEC** ハイブリッド **RSA**： インターネットプロトコルセキュリティとハイブリッド RSA 認証。
  - **PPTP**： Point-to-Point トンネリング。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

Amazon 向け L2TP PSK の設定の構成

- サーバーアドレス： VPN サーバーの IP アドレスを入力します。
- ユーザー名： 任意で、ユーザー名を入力します。
- パスワード： 任意で、パスワードを入力します。
- **L2TP** シークレット： 共有シークレットキーを入力します。
- **IPSec** 識別子： 接続時にユーザーのデバイスに表示される VPN 接続の名前を入力します。
- **IPSec** 事前共有キー： 秘密キーを入力します。
- **DNS** 検索ドメイン： ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー： 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。

- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］ をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。

Amazon 向け **L2TP RSA** の設定の構成

- サーバーアドレス: VPN サーバーの IP アドレスを入力します。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- **L2TP** シークレット: 共有シークレットキーを入力します。
- **DNS** 検索ドメイン: ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー: 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書: 一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書: 一覧から、使用する CA 証明書を選択します。
- **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］ をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。

Amazon 向け **IPSEC XAUTH PSK** の設定の構成

- サーバーアドレス: VPN サーバーの IP アドレスを入力します。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- **IPSec** 識別子: 接続時にユーザーのデバイスに表示される VPN 接続の名前を入力します。
- **IPSec** 事前共有キー: 共有シークレットキーを入力します。
- **DNS** 検索ドメイン: ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー: 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］ をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］ をクリックしてルートを保存するか、［キャンセル］ をクリックして操作を取り消します。

Amazon 向け **IPSEC AUTH RSA** の設定の構成

- サーバーアドレス: VPN サーバーの IP アドレスを入力します。
- ユーザー名: 任意で、ユーザー名を入力します。

- パスワード: 任意で、パスワードを入力します。
- **DNS** 検索ドメイン: ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー: 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書: 一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書: 一覧から、使用する CA 証明書を選択します。
- **ID** 資格情報: ボックスの一覧で、使用する ID 資格情報を選択します。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

Amazon 向け **IPSEC HYBRID RSA** の設定の構成

- サーバーアドレス: VPN サーバーの IP アドレスを入力します。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- **DNS** 検索ドメイン: ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー: 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- サーバー証明書: 一覧から、使用するサーバー証明書を選択します。
- **CA** 証明書: 一覧から、使用する CA 証明書を選択します。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

Amazon 向け **LPPTP** の設定の構成

- サーバーアドレス: VPN サーバーの IP アドレスを入力します。
- ユーザー名: 任意で、ユーザー名を入力します。
- パスワード: 任意で、パスワードを入力します。
- **DNS** 検索ドメイン: ユーザーデバイスの検索ドメインの一覧と照合可能なドメインを入力します。
- **DNS** サーバー: 指定したドメインの解決に使用する DNS サーバーの IP アドレスを入力します。
- **PPP** 暗号化（**MPPE**）: Microsoft Point-to-Point 暗号化（MPPE）によるデータの暗号化を有効にするかどうかを選択します。デフォルトは［オフ］です。
- 転送ルート: 社内 VPN サーバーが転送ルートをサポートしている場合は、使用する転送ルートごとに、［追加］をクリックして以下の操作を行います。
  - 転送ルート: 転送ルートの IP アドレスを入力します。
  - ［保存］をクリックしてルートを保存するか、［キャンセル］をクリックして操作を取り消します。

壁紙デバイスポリシー

January 10, 2020

.png ファイルまたは.jpg ファイル追加して、iOS デバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。iOS 7.1.2 以降で使用できます。iPad および iPhone で異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。

次の表に、Apple 社が iOS デバイス用に推奨しているイメージサイズを示します。

デバイス	イメージサイズ（ピクセル）
iPhone 5、5c、5s	640×1136
iPhone 6,6s	750×1334
iPhone 6 Plus	1080×1920
iPad Air、2	1536×2048
iPad 4、3	1536×2048
iPad Mini 2、3	1536×2048

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- 適用先: 一覧から、［画面をロック］、［ホーム（アイコン一覧）画面］、［ロック画面およびホーム画面］ のいずれかを選択して、壁紙を表示する場所を設定します。
- 壁紙ファイル:［参照］ をクリックして壁紙ファイルの場所に移動し、ファイルを選択します。

Web コンテンツフィルターデバイスポリシー

January 10, 2020

XenMobile でデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトと Apple のオートフィルター機能を組み合わせて使用して、iOS デバイスで Web コンテンツをフィルタリングできます。このポリシーは iOS 7.0 以降の Supervised モードのデバイスでのみ使用できます。iOS デバイスを Supervised モードにする方法については、「Apple Configurator を使用して iOS デバイスを Supervised モードにするには」を参照してください。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- フィルターの種類: 一覧から ［組み込み］ または ［プラグイン］ を選択し、選択したオプションに応じた手順を実行します。デフォルトは ［組み込み］ です。

組み込みフィルターの種類

- **Web** コンテンツフィルター
  - 自動フィルターが有効: Apple のオートフィルター機能を使用して、Web サイトに不適切なコンテンツがないかを分析するか否か。デフォルトは ［オフ］ です。
  - 許可されている **URL**: この一覧は、［自動フィルターが有効］ が ［オフ］ に設定されている場合は無視されます。［自動フィルターが有効］ が ［オン］ に設定されている場合、この一覧に含まれる項目は、オートフィルターがアクセスを許可しているかどうかにかかわらず常にアクセスできます。ホワイトリストに追加する URL ごとに、［追加］ をクリックして以下の操作を行います。
    * 許可する Web サイトの URL を入力します。Web アドレスの前には、`http://`または`https://`を付ける必要があります。
    * Web サイトをホワイトリストに保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。
  - ブラックリストに登録されている **URL**: この一覧に含まれる項目は常にブロックされます。ブラックリストに追加する URL ごとに、［追加］ をクリックして以下の操作を行います。
    * ブロックする Web サイトの URL を入力します。Web アドレスの前には、`http://`または`https://`を付ける必要があります。
    * Web サイトをブラックリストに保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。
- ホワイトリストのブックマーク
  - ホワイトリストのブックマーク: ユーザーがアクセスできるサイトを指定します。Web サイトへのアクセスを有効にするには、Web サイトの URL を追加します。
    * **URL**: ユーザーがアクセスできる各 Web サイトの URL。たとえば、Secure Hub ストアにアクセスできるようにするには、URL リストに XenMobile Server の **URL** を追加します。Web アドレスの前には、`http://`または`https://`を付ける必要があります。このフィールドは必須です。
    * フォルダーのブックマーク: 任意で、ブックマークフォルダー名を入力します。このフィールドを空白のままにすると、ブックマークはデフォルトのブックマークディレクトリに追加されます。
    * タイトル: Web サイトの説明的なタイトルを入力します。たとえば、`https://google.com`という URL に対して「Google」と入力します。

* Web サイトをホワイトリストに保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。

プラグインフィルターの種類

- フィルター名: フィルターの固有の名前を入力します。
- 識別子: フィルタリングサービスを提供するプラグインのバンドル ID を入力します。
- サービスアドレス: 任意で、サーバーアドレスを入力します。有効な形式は、IP アドレス、ホスト名、または URL です。
- ユーザー名: 任意で、サービスのユーザー名を入力します。
- パスワード: 任意で、デバイスのパスワードを入力します。
- 証明書: 一覧から、任意で、サービスでユーザーを認証するために使用する ID 証明書を選択します。デフォルトは ［なし］ です。
- **WebKit** のトラフィックをフィルター: WebKit トラフィックをフィルタリングするかどうかを選択します。
- ソケットトラフィックをフィルター: ソケットトラフィックをフィルタリングするかどうかを選択します。
- カスタムデータ: Web フィルターに追加するカスタムキーごとに、［追加］ をクリックして以下の操作を行います。
  - キー: カスタムキーを入力します。
  - 値: カスタムキーの値を入力します。
  - カスタムキーを保存する場合は ［保存］ をクリックし、保存しない場合は ［キャンセル］ をクリックします。

Web クリップデバイスポリシー

January 10, 2020

ショートカットや Web クリップを Web サイトに配置してユーザーデバイスのアプリと一緒に表示できます。iOS、macOS、Android デバイスの Web クリップを表す独自のアイコンを指定できます。Windows タブレットのみ、ラベルおよび URL が必要になります。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定

- ラベル: Web クリップと共に表示するラベルを入力します。
- **URL**: Web クリップに関連付ける URL を入力します。URL はプロトコル（例: `https://server`）で始まる必要があります。

- 削除可能: ユーザーが Web クリップを削除できるかどうかを選択します。デフォルトは ［オフ］ です。
- 更新するアイコン:［参照］ をクリックしてファイルの場所に移動し、Web クリップに使用するアイコンを選択します。
- 画像処理済みアイコン: アイコンにエフェクト（角丸、影付き、反射光）を適用するかどうかを選択します。デフォルトは ［オフ］ で、エフェクトが追加されます。
- 全画面: リンクされている Web ページを全画面モードで開くかどうかを選択します。デフォルトは ［オフ］ です。

macOS 設定

- ラベル: Web クリップと共に表示するラベルを入力します。
- **URL**: Web クリップに関連付ける URL を入力します。URL はプロトコル（例: `https://server`）で始まる必要があります。
- 更新するアイコン: ［参照］をクリックしてファイルの場所に移動し、Web クリップに使用するアイコンを選択します。

Android の設定

- 規則: このポリシーで Web クリップを追加または削除するかどうかを選択します。デフォルトは［**Add**］です。
- ラベル: Web クリップと共に表示するラベルを入力します。
- **URL**: Web クリップに関連付ける URL を入力します。
- アイコンを定義: アイコンファイルを使用するかどうかを選択します。デフォルトは ［オフ］ です。
- アイコンファイル:［アイコンを定義］ が ［オン］ の場合は、［参照］ をクリックしてアイコンファイルの場所に移動し、ファイルを選択します。

Windows デスクトップ**/**タブレットの設定

- 名前: Web クリップと共に表示するラベルを入力します。
- **URL**: Web クリップに関連付ける URL を入力します。

Wi-Fi デバイスポリシー

October 25, 2019

［構成］ **>**［デバイスポリシー］ ページを使用して、XenMobile で新しい Wi-Fi デバイスポリシーを作成するか、既存の Wi-Fi デバイスポリシーを編集します。Wi-Fi ポリシーを使用すると、次の項目を定義して、ユーザーがデバイスを Wi-Fi ネットワークに接続する方法を管理できます。

- ネットワーク名と種類
- 認証およびセキュリティポリシー
- プロキシサーバーの使用
- その他の Wi-Fi 関連の詳細

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

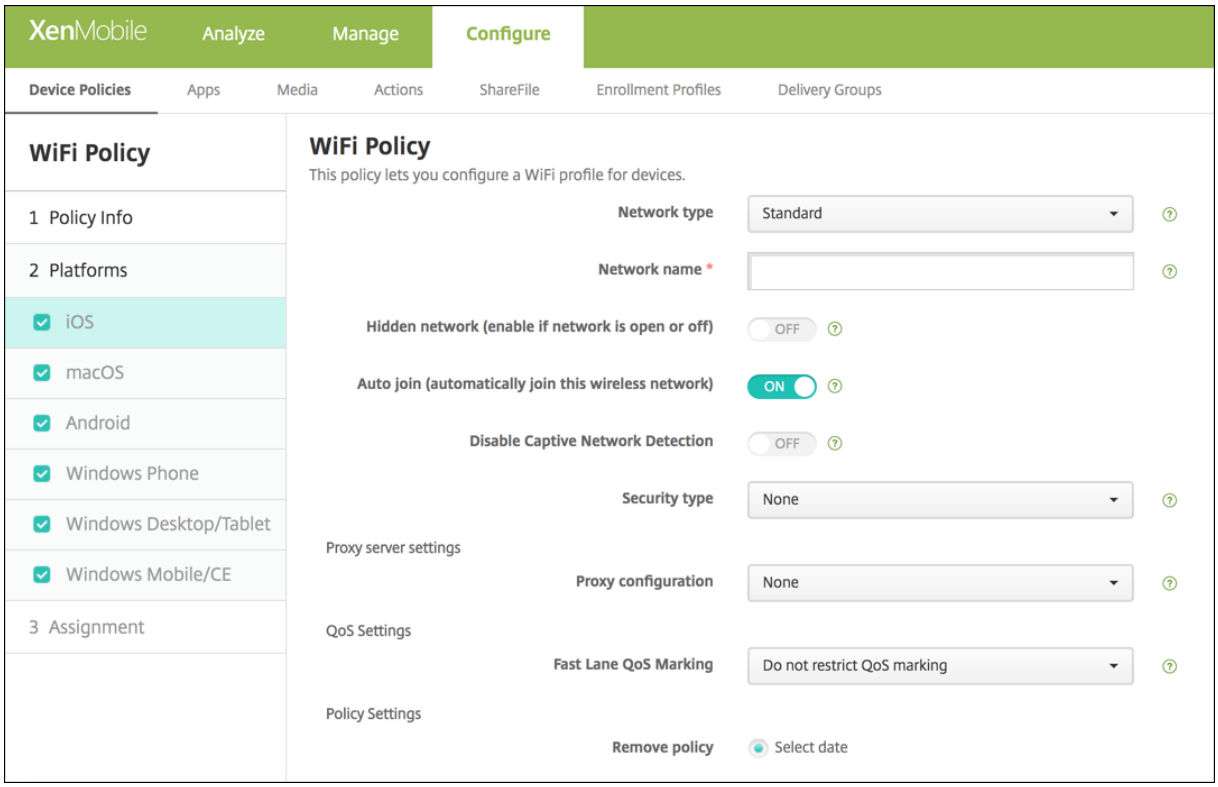
前提条件

ポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定のデリバリーグループを作成します。
- ネットワークの名前と種類を確認します。
- 使用する予定の認証またはセキュリティの種類を確認します。
- 必要な場合、プロキシサーバーの情報を確認します。
- 必要な CA 証明書をインストールします。
- 必要な共有キーを取得します。
- 証明書に基づいた認証のために PKI エンティティを作成します。
- 資格情報プロバイダーを構成します。

詳しくは、「認証」とそのサブ記事を参照してください。

iOS の設定



- ネットワークの種類: 一覧で、［標準］、［従来のホットスポット］、または ［**Hotspot 2.0**］ を選択して、使用するネットワークの種類を設定する必要があります。
- ネットワーク名: デバイスで使用可能なネットワークの一覧に表示される SSID を入力します。**Hotspot 2.0** には適用されません。
- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）: ネットワークを隠しネットワークにするかどうかを選択します。
- 自動参加（このワイヤレスネットワークに自動的に参加）: ネットワークに自動的に参加するかどうかを選択します。iOS デバイスがすでに別のネットワークに接続されている場合は、このネットワークに参加しません。ユーザーは、デバイスが自動的に接続する前に、以前のネットワークから切断する必要があります。デフォルトは ［オン］ です。
- セキュリティの種類: 一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0** には適用されません。
  - なし - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2 パーソナル
  - 任意（パーソナル）
  - WEP エンタープライズ
  - WPA/WPA2 エンタープライズ: Windows 10 の最新リリースでは、WPA-2 エンタープライズを使用するには SCEP を構成する必要があります。SCEP を構成すると、XenMobile から証明書をデバイス

に送信して Wi-Fi サーバーを認証することができます。SCEP を構成するには、［設定］**>**［資格情報プロバイダー］ の［ディストリビューション］ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

- 任意（エンタープライズ）

以下では、上記の接続の種類ごとに、構成するオプションを示します。

iOS の **WPA**、**WPA** パーソナル、任意（パーソナル）の設定

パスワード: 任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。

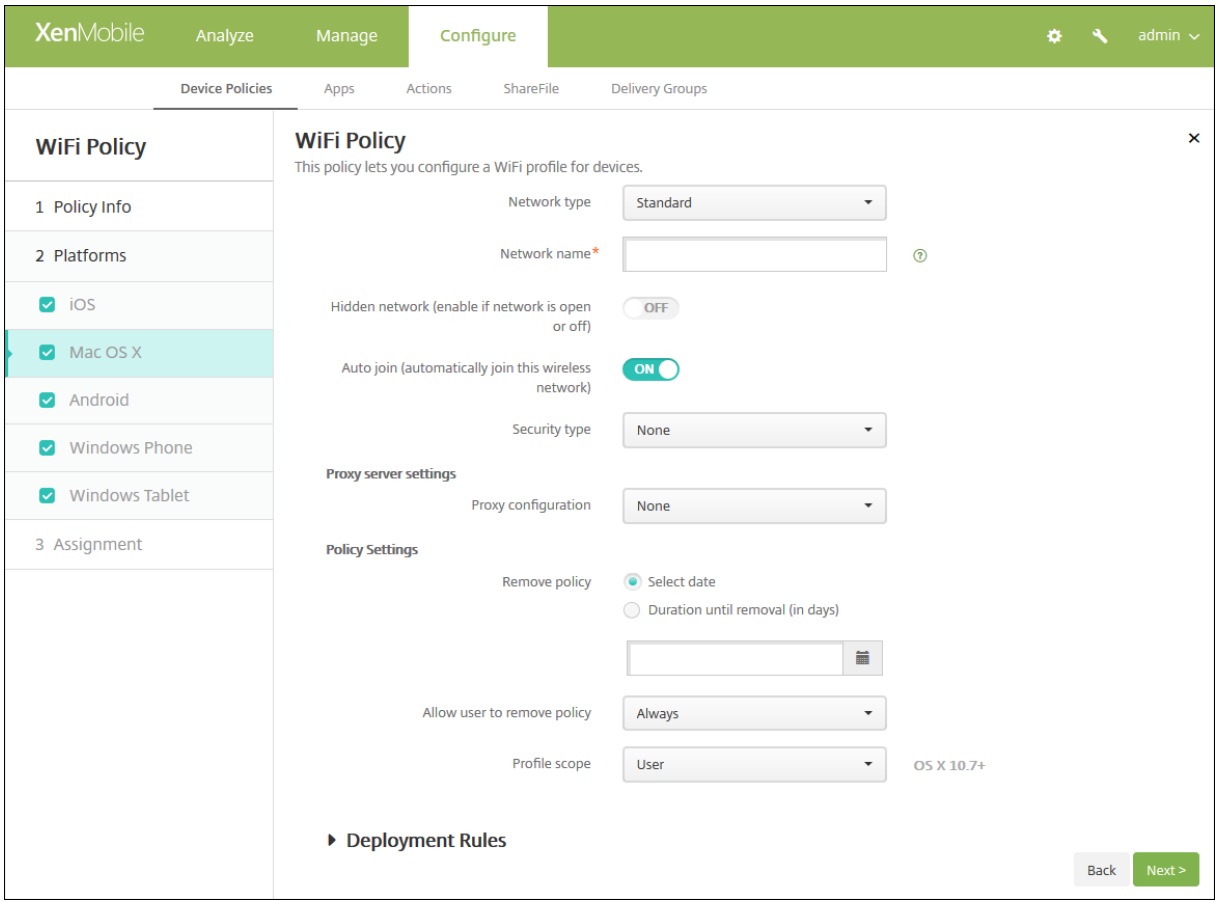
iOS の **WEP** エンタープライズ、**WPA** エンタープライズ、**WPA2** エンタープライズ、任意（エンタープライズ）の設定

これらの設定を選択すると、それぞれの設定項目が ［プロキシサーバーの設定］ の後に表示されます。

- プロトコル、許容される **EAP** の種類: サポートする EAP の種類を有効にして、関連する設定を構成します。使用できる各 EAP の種類のデフォルトは ［オフ］ です。
- 内部認証 **(TTLS)**: *TTLS* を有効にする場合にのみ必要です。一覧から、使用する内部認証方法を選択します。オプションは、［**PAP**］、［**CHAP**］、［**MSCHAP**］、または ［**MSCHAPv2**］ です。デフォルトは［**MSCHAPv2**］ です。
- プロトコル、**EAP-FAST**: 保護されたアクセス資格情報（PAC）を使用するかどうかを選択します。
  - ［**PAC** を使用］ を選択した場合は、プロビジョニング PAC を使用するかどうかを選択します。
    - ［**PAC** をプロビジョニング］ を選択した場合は、エンドユーザーのクライアントと XenMobile の間で匿名 TLS ハンドシェイクを許可するかどうかを選択します。
      - 匿名で **PAC** をプロビジョニング
- 認証:
  - ユーザー名: ユーザー名を入力します。
  - 接続ごとのパスワード: ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
  - パスワード: 任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。
  - **ID** 資格情報（キーストアまたは **PKI** 資格情報）: 一覧から、ID 資格情報の種類を選択します。デフォルトは ［なし］ です。
  - 外部 **ID**:［**PEAP**］、［**TTLS**］、または［**EAP-FAST**］ を有効にした場合にのみ必要です。画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」などの汎用的な用語を入力して、セキュリティを高めることができます。
  - **TLS** 証明書を要求: TLS 証明書を必須とするかどうかを選択します。
- 信頼
  - 信頼された証明書: 信頼された機関からの証明書を追加するには、［追加］ をクリックして、追加する証明書ごとに以下の操作を行います。

        * アプリケーション: 一覧から、追加するアプリケーションを選択します。
        *［保存］ をクリックして証明書を保存するか、［キャンセル］ をクリックします。
    - 信頼されたサーバー証明書の名前: 信頼されたサーバー証明書の一般名を追加するには、［追加］ をクリックして、追加する名前ごとに以下の操作を行います。
        * 証明書: サーバー証明書の名前を入力します。ワイルドカード文字を使用して、名前を「wpa.*.example.com」のように指定することができます。
        *［保存］ をクリックして証明書名を保存するか、［キャンセル］ をクリックします。
- 信頼の例外を許可: 証明書が信頼できないときに、デバイスに証明書信頼ダイアログを表示するかどうかを選択します。デフォルトは ［オン］ です。
- プロキシサーバーの設定
    - プロキシの構成: 一覧から、［なし］、［手動］、または ［自動］ を選択して VPN 接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルトは ［なし］ で、そのほかの構成は不要です。
    -［手動］ を選択した場合は、次の設定を構成します:
        * ホスト名**/IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。
        * ポート: プロキシサーバーのポート番号を入力します。
        * ユーザー名: 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
        * パスワード: 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
    -［自動］ を選択した場合は、次の設定を構成します:
        * サーバー **URL**: プロキシ構成を定義する PAC ファイルの URL を入力します。
        * **PAC** に到達不能である場合は直接接続を許可: PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは ［オン］ です。このオプションは iOS 7.0 以降でのみ使用できます。

macOS 設定



- ネットワークの種類: 一覧で、［標準］、［従来のホットスポット］、または ［**Hotspot 2.0**］ を選択して、使用するネットワークの種類を設定する必要があります。
- ネットワーク名: デバイスで使用可能なネットワークの一覧に表示される SSID を入力します。**Hotspot 2.0** には適用されません。
- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）: ネットワークを隠しネットワークにするかどうかを選択します。
- 自動参加（このワイヤレスネットワークに自動的に参加）: ネットワークに自動的に参加するかどうかを選択します。デバイスがすでに別のネットワークに接続されている場合は、このネットワークに参加しません。ユーザーは、デバイスが自動的に接続する前に、以前のネットワークから切断する必要があります。デフォルトは ［オン］ です。
- セキュリティの種類: 一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0** には適用されません。
  - なし - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2 パーソナル
  - 任意（パーソナル）
  - WEP エンタープライズ

- WPA/WPA2 エンタープライズ
- 任意（エンタープライズ）

以下では、上記の接続の種類ごとに、構成するオプションを示します。

macOS の **WPA**、**WPA** パーソナル、**WPA 2** パーソナル、任意（パーソナル）の設定

- パスワード: 任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。

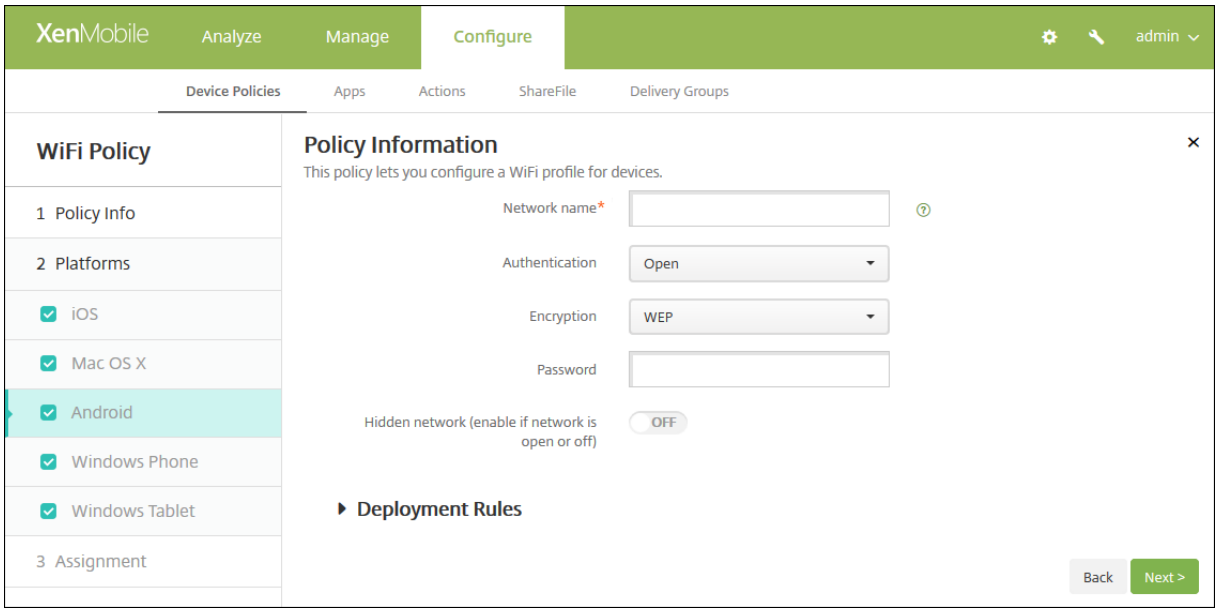
macOS の **WEP** エンタープライズ、**WPA** エンタープライズ、**WPA2** エンタープライズ、任意（エンタープライズ）の設定

これらの設定を選択すると、それぞれの設定項目が ［プロキシサーバーの設定］ の後に表示されます。

- プロトコル、許容される **EAP** の種類: サポートする EAP の種類を有効にして、関連する設定を構成します。使用できる各 EAP の種類のデフォルトは ［オフ］ です。
- 内部認証 **(TTLS)**: *TTLS* を有効にする場合にのみ必要です。一覧から、使用する内部認証方法を選択します。オプションは、［**PAP**］、［**CHAP**］、［**MSCHAP**］、または ［**MSCHAPv2**］ です。デフォルトは［**MSCHAPv2**］ です。
- プロトコル、**EAP-FAST**: 保護されたアクセス資格情報（PAC）を使用するかどうかを選択します。
  - ［**PAC** を使用］ を選択した場合は、プロビジョニング PAC を使用するかどうかを選択します。
    - ［**PAC** をプロビジョニング］ を選択した場合は、エンドユーザーのクライアントと XenMobile の間で匿名 TLS ハンドシェイクを許可するかどうかを選択します。
      - 匿名で **PAC** をプロビジョニング
- 認証:
  - ユーザー名: ユーザー名を入力します。
  - 接続ごとのパスワード: ユーザーがログオンするたびにパスワードを要求するかどうかを選択します。
  - パスワード: 任意で、パスワードを入力します。このフィールドを空白のままにすると、ユーザーがログオン時にパスワードの入力を求められることがあります。
  - **ID** 資格情報（キーストアまたは **PKI** 資格情報）: 一覧から、ID 資格情報の種類を選択します。デフォルトは ［なし］ です。
  - 外部 **ID**:［**PEAP**］、［**TTLS**］、または［**EAP-FAST**］ を有効にした場合にのみ必要です。画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
  - **TLS** 証明書を要求: TLS 証明書を必須とするかどうかを選択します。
- 信頼
  - 信頼された証明書: 信頼された機関からの証明書を追加するには、［追加］ をクリックして、追加する証明書ごとに以下の操作を行います。
    - アプリケーション: 一覧から、追加するアプリケーションを選択します。

    * ［保存］ をクリックして証明書を保存するか、［キャンセル］ をクリックします。
  - 信頼されたサーバー証明書の名前: 信頼されたサーバー証明書の一般名を追加するには、［追加］ をクリックして、追加する名前ごとに以下の操作を行います。
    * 証明書: 追加するサーバー証明書の名前を入力します。ワイルドカード文字を使用して、名前を「wpa.*.example.com」のように指定することができます。
    * ［保存］ をクリックして証明書名を保存するか、［キャンセル］ をクリックします。
- 信頼の例外を許可: 証明書が信頼できないときに、ユーザーデバイスに証明書信頼ダイアログを表示するかどうかを選択します。デフォルトは ［オン］ です。
- ログインウィンドウ構成として使用: ユーザーの認証に、ログインウィンドウで入力したものと同じ資格情報を使用するかどうかを選択します。
- プロキシサーバーの設定
  - プロキシの構成: 一覧から、［なし］、［手動］、または ［自動］ を選択して VPN 接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルトは ［なし］ で、そのほかの構成は不要です。
  - ［手動］ を選択した場合は、次の設定を構成します:
    * ホスト名**/IP** アドレス: プロキシサーバーのホスト名または IP アドレスを入力します。
    * ポート: プロキシサーバーのポート番号を入力します。
    * ユーザー名: 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    * パスワード: 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［自動］ を選択した場合は、次の設定を構成します:
    * サーバー **URL**: プロキシ構成を定義する PAC ファイルの URL を入力します。
    * **PAC** に到達不能である場合は直接接続を許可: PAC ファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは ［オン］ です。このオプションは iOS 7.0 以降でのみ使用できます。

Android の設定



- ネットワーク名: ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- 認証: 一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Android のオープン、共有設定

- 暗号化: 一覧から、［無効］ または ［**WEP**］ を選択します。デフォルトは ［**WEP**］ です。
- パスワード: 任意で、パスワードを入力します。

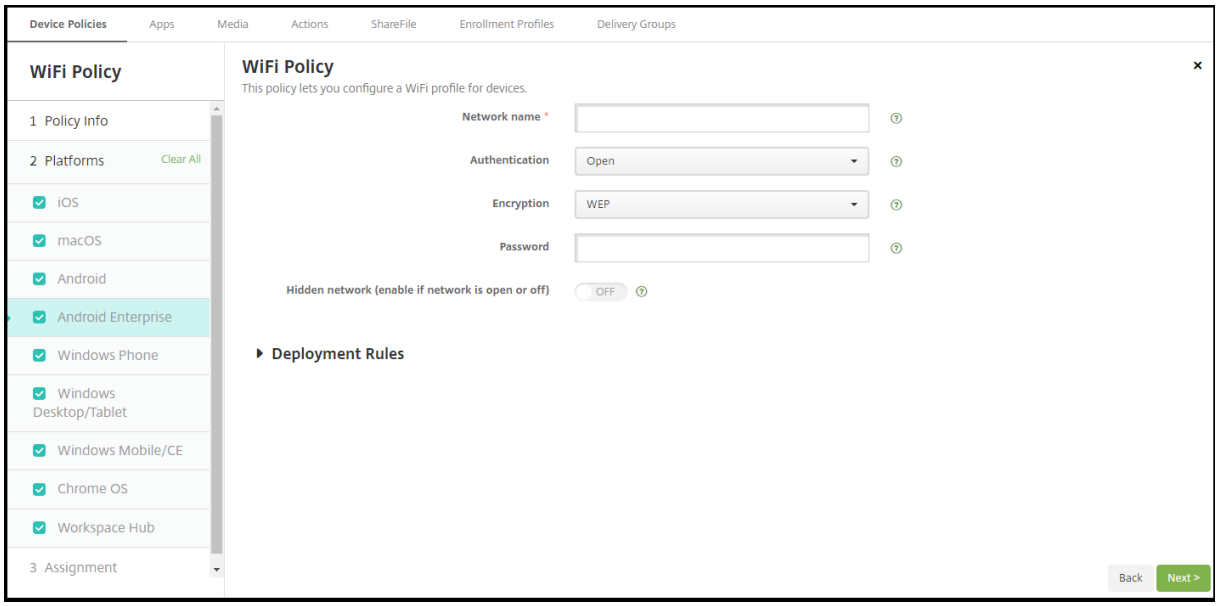
Android の WPA、WPA-PSK、WPA2、WPA2-PSK 設定

- 暗号化: 一覧から、［**TKIP**］ または ［**AES**］ を選択します。デフォルトは ［**TKIP**］ です。
- パスワード: 任意で、パスワードを入力します。

Android の 802.1x 設定

- **EAP** タイプ: 一覧から、[**PEAP**]、[**TLS**]、または [**TTLS**] を選択します。デフォルトは [**PEAP**] です。
- パスワード: 任意で、パスワードを入力します。
- 認証フェーズ **2**: 一覧から、[なし]、[**PAP**]、[**MSCHAP**]、[**MSCHAPPv2**]、または [**GTC**] を選択します。デフォルトは [**PAP**] です。
- **ID**: オプションのユーザー名およびドメインを入力します。
- 匿名: 任意で、画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
- **CA** 証明書: 一覧から、使用する証明書を選択します。
- **ID** 資格情報: 一覧から、使用する ID 資格情報を選択します。デフォルトは [なし] です。
- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）: ネットワークを隠しネットワークにするかどうかを選択します。

Android Enterprise の設定



- ネットワーク名: ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- 認証: 一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Android のオープン、共有設定

- 暗号化: 一覧から、［無効］ または ［**WEP**］ を選択します。デフォルトは ［**WEP**］ です。
- パスワード: 任意で、パスワードを入力します。

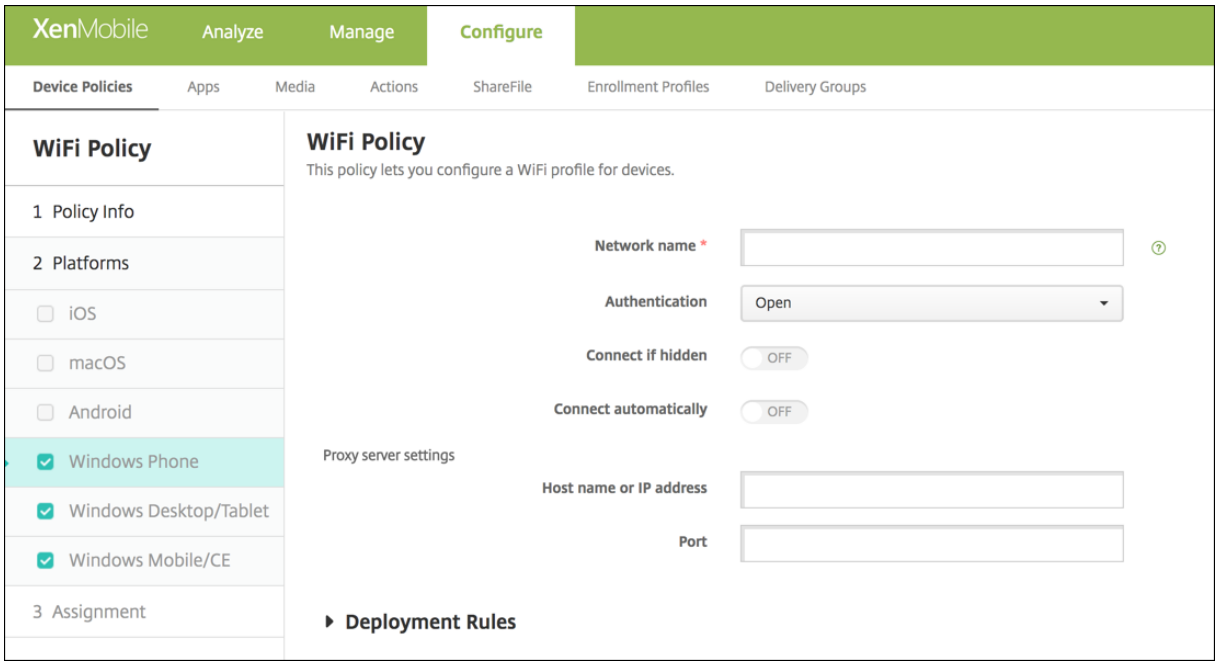
Android の **WPA**、**WPA-PSK**、**WPA2**、**WPA2-PSK** 設定

- 暗号化: 一覧から、［TKIP］または［AES］を選択します。デフォルトは［TKIP］です。
- パスワード: 任意で、パスワードを入力します。

Android の **802.1x** 設定

- **EAP** タイプ: 一覧から、［**PEAP**］、［**TLS**］、または［**TTLS**］を選択します。デフォルトは［**PEAP**］です。
- パスワード: 任意で、パスワードを入力します。
- 認証フェーズ **2**: 一覧から、［なし］、［**PAP**］、［**MSCHAP**］、［**MSCHAPPv2**］、または［**GTC**］を選択します。デフォルトは ［**PAP**］ です。
- **ID**: オプションのユーザー名およびドメインを入力します。
- 匿名: 任意で、画面に表示されるユーザー名を入力します。ユーザーの名前がわからないように「anonymous」のような汎用的な用語を入力して、セキュリティを高めることができます。
- **CA** 証明書: 一覧から、使用する証明書を選択します。
- **ID** 資格情報: 一覧から、使用する ID 資格情報を選択します。デフォルトは ［なし］ です。
- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）: ネットワークを隠しネットワークにするかどうかを選択します。

Windows Phone の設定



- ネットワーク名： ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- 認証： 一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPA パーソナル
  - WPA-2 パーソナル
  - WPA-2 エンタープライズ：Windows 10 の最新リリースでは、WPA-2 エンタープライズを使用するには SCEP を構成する必要があります。SCEP を構成すると、XenMobile から証明書をデバイスに送信して Wi-Fi サーバーを認証することができます。SCEP を構成するには、［設定］>［資格情報プロバイダー］ の ［ディストリビューション］ ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Windows Phone のオープン設定

- 非表示の場合は接続： ネットワークが隠しネットワークの場合に接続するかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

Windows Phone の WPA パーソナル、WPA-2 パーソナル設定

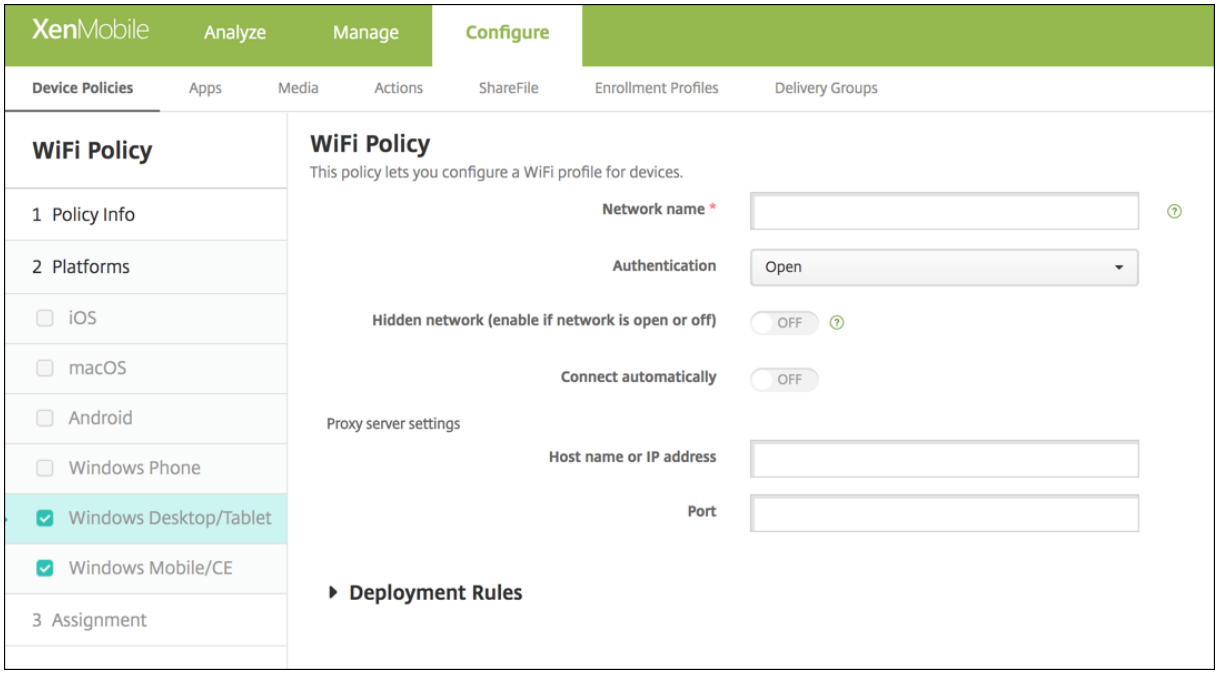
- 暗号化： 一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。

- 非表示の場合は接続： ネットワークが隠しネットワークの場合に接続するかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

Windows Phone の WPA-2 エンタープライズ設定

- 暗号化：一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。
- **EAP** タイプ：一覧から、［**PEAP-MSCHAPv2**］ または ［**TLS**］ を選択して、EAP の種類を設定します。デフォルトは ［**PEAP-MSCHAPv2**］ です。
- 非表示の場合は接続： ネットワークが隠しネットワークの場合に接続するかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。
- **SCEP** 経由で証明書をプッシュ： Simple Certificate Enrollment Protocol（SCEP）を介して証明書をユーザーデバイスにプッシュするかどうかを選択します。
- **SCEP** の資格情報プロバイダー： 一覧から、SCEP 資格情報プロバイダーを選択します。デフォルトは ［なし］ です。
- プロキシサーバーの設定
  - ホスト名または **IP** アドレス： プロキシサーバーの名前または IP アドレスを入力します。
  - ポート： プロキシサーバーのポート番号を入力します。

Windows 10 の設定



- 認証： 一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン

  - WPA パーソナル
  - WPA-2 パーソナル
  - WPA エンタープライズ
  - WPA-2 エンタープライズ：Windows 10 の最新リリースでは、WPA-2 エンタープライズを使用するには SCEP を構成する必要があります。SCEP を構成すると、XenMobile から証明書をデバイスに送信して Wi-Fi サーバーを認証することができます。SCEP を構成するには、［設定］**>**［資格情報プロバイダー］ の ［ディストリビューション］ ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Windows 10 のオープン設定

- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

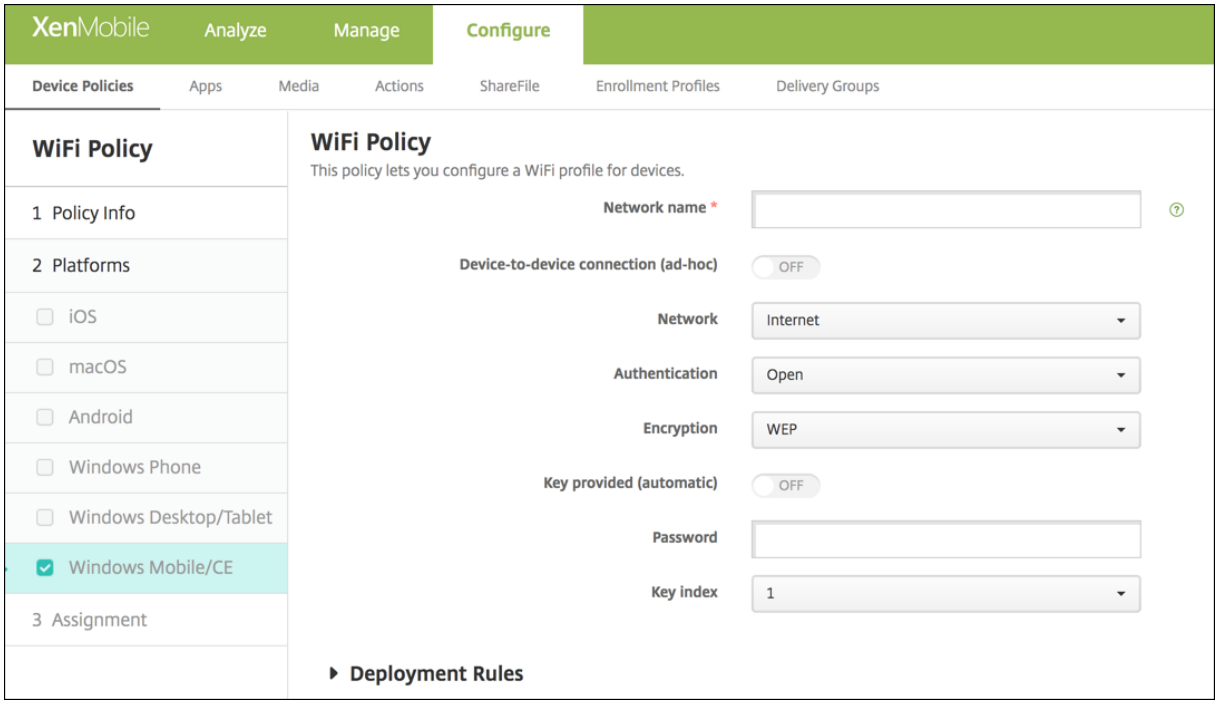
Windows 10 の **WPA** パーソナル、**WPA-2** パーソナル設定

- 暗号化：一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。
- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

Windows 10 の **WPA-2** エンタープライズ設定

- 暗号化：一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。
- **EAP** タイプ：一覧から、［**PEAP-MSCHAPv2**］ または ［**TLS**］ を選択して、EAP の種類を設定します。デフォルトは ［**PEAP-MSCHAPv2**］ です。
- 非表示の場合は接続： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。
- **SCEP** 経由で証明書をプッシュ： Simple Certificate Enrollment Protocol（SCEP）を使用して証明書をユーザーデバイスにプッシュするかどうかを選択します。
- **SCEP** の資格情報プロバイダー： ボックスの一覧で、SCEP 資格情報プロバイダーを選択します。デフォルトは ［なし］ です。

Windows Mobile/CE の設定



- ネットワーク名： ユーザーデバイスで使用可能なネットワークの一覧に表示される SSID を入力します。
- デバイス間接続（アドホック）： 2 つのデバイスを直接接続できます。デフォルトは ［オフ］ です。
- ネットワーク： デバイスを外部インターネットソースに接続するか、オフィスのイントラネットに接続するかを選択します。
- 認証： 一覧から、この Wi-Fi 接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPA パーソナル
  - WPA-2 パーソナル
  - WPA-2 エンタープライズ

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Windows Mobile/CE の設定を開く

- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

Windows Mobile/CE の WPA パーソナル、WPA-2 パーソナル設定

- 暗号化： 一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。

- 隠しネットワーク（ネットワークが開いているか、オフの場合は有効）： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。

Windows Mobile/CE の **WPA-2** エンタープライズ設定

- 暗号化： 一覧から、［**AES**］ または ［**TKIP**］ を選択して、暗号化の種類を設定します。デフォルトは ［**AES**］ です。
- **EAP** タイプ： 一覧から、［**PEAP-MSCHAPv2**］ または ［**TLS**］ を選択して、EAP の種類を設定します。デフォルトは ［**PEAP-MSCHAPv2**］ です。
- 非表示の場合は接続： ネットワークを隠しネットワークにするかどうかを選択します。
- 自動的に接続： ネットワークに自動的に接続するかどうかを選択します。
- **SCEP** 経由で証明書をプッシュ： Simple Certificate Enrollment Protocol（SCEP）を使用して証明書をユーザーデバイスにプッシュするかどうかを選択します。
- **SCEP** の資格情報プロバイダー： ボックスの一覧で、SCEP 資格情報プロバイダーを選択します。デフォルトは ［なし］ です。
- 入力されたキー（自動）： キーが自動的に指定されるかどうかを選択します。デフォルトは ［オフ］ です。
- パスワード： このフィールドにパスワードを入力します。
- キーインデックス：キーインデックスを選択します。使用可能なオプションは、［**1**］、［**2**］、［**3**］、［**4**］です。

Windows CE 証明書デバイスポリシー

August 22, 2019

XenMobile では、外部の PKI を基に Windows Mobile/CE 証明書を作成し、ユーザーのデバイスに配布するデバイスポリシーを作成できます。証明書および PKI エンティティについて詳しくは、「証明書」を参照してください。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows CE の設定

- 資格情報プロバイダー：ボックスの一覧で、資格情報プロバイダーを選択します。デフォルトは［なし］です。
- 生成された **PKCS#12** のパスワード： 資格情報の暗号化に使用するパスワードを入力します。
- ターゲットフォルダー： 一覧から資格情報の宛先フォルダーを選択するか、［新規追加］ をクリックして、一覧に表示されていないフォルダーを追加します。事前定義済みのオプションは以下のとおりです：
  - %Flash Storage%\
  - %XenMobile Folder%\

  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- ターゲットファイル名: 資格情報ファイルの名前を入力します。

Windows Information Protection のデバイスポリシー

August 22, 2019

Windows Information Protection(WIP、旧称エンタープライズデータ保護(EDP: Enterprise Data Protection))は、企業データの漏洩を防ぐ Windows のテクノロジーです。データ漏洩は、企業データを企業で保護されていないアプリで共有したり、アプリ間、または組織のネットワーク外で共有することによって起こります。詳しくは、Microsoft TechNet の「Windows 情報保護（WIP）を使用した企業データの保護」を参照してください。

XenMobile でデバイスポリシーを作成して、設定した適用レベルの Windows Information Protection が求められるアプリを指定できます。Windows Information Protection のポリシーは、Windows 10 バージョン 1607 以降の監視対象の携帯電話、タブレット、デスクトップに適用されます。

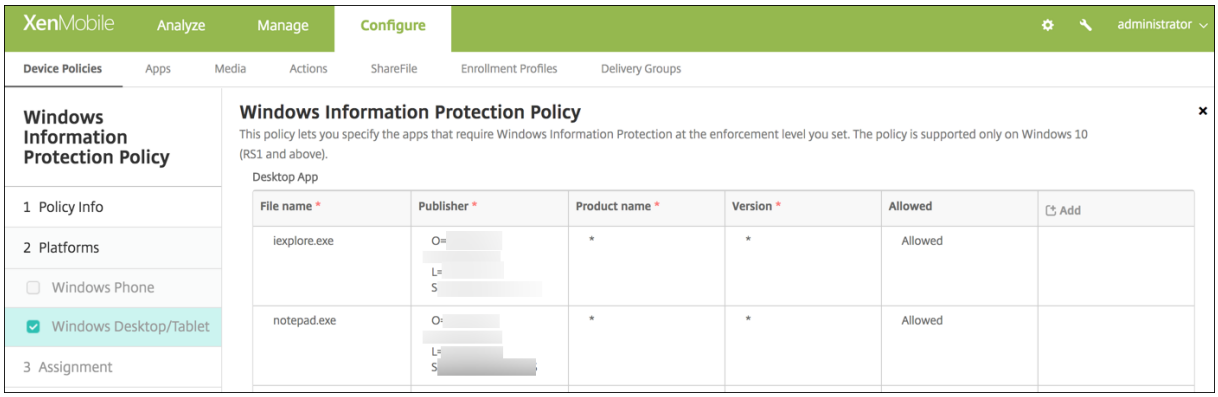
XenMobile に一般的なアプリがいくつか含まれていますが、別のアプリを追加することもできます。このポリシーでは、ユーザーエクスペリエンスに影響を及ぼす適用レベルを指定します。例えば、次の作業を行えます。

- 不適切なデータ共有をすべてブロックする。
- 不適切なデータ共有について警告するが、ユーザーによるポリシーの無視を許可する。
- 不適切なデータ共有を記録しながら許可し、サイレントで WIP を実行する。

Windows Information Protection からアプリを除外するには、Microsoft AppLocker の XML ファイルで除外するアプリを定義し、このファイルを XenMobile にインポートします。

このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Windows 10 の設定



- [デスクトップアプリ] (Windows 10 タブレット)、[ストアアプリ] (Windows 10 のスマートフォンおよびタブレット): 上の例に示されているように、XenMobile には一般的なアプリがいくつか含まれています。必要に応じてこれらのアプリを編集または削除できます。

  別のアプリを追加するには、[デスクトップアプリ] テーブルまたは [ストアアプリ] テーブルで [追加] をクリックし、追加するアプリの情報を入力します。

  [許可] に設定されたアプリでは、企業データの読み取り、作成、更新を行うことができます。[禁止] に設定されたアプリは、企業データにアクセスできません。[免除] に設定されたアプリでは、企業データを読み取ることはできますが、作成または変更することはできません。

  - **AppLocker XML**: Microsoft から、WIP との互換性に問題があることがわかっている Microsoft アプリのリストが提供されています。これらのアプリを WIP から除外するには、[参照] をクリックし、提供されているリストをアップロードします。XenMobile では、デバイスへ送信するポリシー内で、アップロード済みの AppLocker XML と構成済みのデスクトップアプリおよびストアアプリが組み合わされます。詳しくは、「Recommended deny list for Windows Information Protection」を参照してください。
  - 適用レベル: Windows Information Protection でのデータ共有の保護および管理方法を指定するオプションを選択します。デフォルトは、[オフ] です。
    * **0-**オフ: WIP は無効化され、データの保護と監査は行われません。
    * **1-**サイレント: WIP はサイレントに実行され、ブロックを行うことなく不適切なデータ共有をログに記録します。このログには、レポート CSPからアクセスできます。
    * **2-**上書き: WIP が、安全ではない可能性があるデータ共有についてユーザーに警告します。ユーザーはこの警告を無視してデータを共有することができます。このモードでは、ユーザーによる無視を含む操作が監査ログに記録されます。
    * **3-**ブロック: WIP により、安全ではない可能性があるデータ共有が禁止されます。
  - 保護対象ドメイン名: 企業のユーザー ID に使用するドメインを指定します。この管理対象 ID ドメインの一覧とプライマリドメインを合わせて、管理対象企業の ID が作成されます。一覧の先頭のドメインに

は、Windows UI で使用するプライマリ企業 ID を指定します。項目を区切るには「|」を使用します。次に例を示します: domain1.com | domain2.com

- データ回復証明書: [参照] をクリックして、暗号化ファイルのデータ回復に使用する回復証明書を選択します。この証明書は、ファイル暗号化システム（EFS: Encrypting File System）のデータ回復エージェント（DRA: Data Recovery Agent）の証明書と同じものであり、グループポリシーではなく MDM のみにより配信されます。利用できる回復証明書がない場合は作成してください。詳しくは、次の「データ回復証明書の作成」セクションを参照してください。
- ネットワークドメイン名: 企業の境界を構成するドメインの一覧を指定します。この一覧に含まれる完全修飾ドメインに対するすべてのトラフィックが、WIP により保護されます。この設定と [**IP** の範囲] 設定により、ネットワークエンドポイントがプライベートネットワーク上の企業のものであるか、個人のものであるかが検出されます。項目を区切るにはコンマを使用します。例えば、「corp.example.com,region.example.com」のように入力します。
- **IP** の範囲: 企業ネットワークに含まれるコンピューターを定義する、企業の IPv4 または IPv6 の範囲の一覧を指定します。これらの場所が、WIP で企業での安全なデータ共有先とみなされます。項目を区切るにはコンマを使用します。次に例を示します:

  10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff

- **IP** アドレス範囲の一覧は優先されます: Windows による IP 範囲の自動検出を無効化するには、この設定を [オン] に変更します。デフォルトは、[オフ] です。
- プロキシサーバー: 企業で社内リソース用に使用できるプロキシサーバーの一覧を指定します。この設定は、ネットワーク内でプロキシを使用する場合のみ必須です。プロキシサーバーを使用しないと、クライアントがプロキシの背後にある場合に社内リソースを利用できなくなる可能性があります。例えば、ホテルやレストランの特定の Wi-Fi ホットスポットでリソースを利用できないことがあります。項目を区切るにはコンマを使用します。次に例を示します:

  proxy.example.com:80;157.54.11.118:443

- 内部プロキシサーバー: デバイスがクラウドリソースへ到達するために経由するプロキシサーバーの一覧を指定します。このサーバーの種類を使用して、接続先のクラウドリソースが社内リソースであることを示します。この一覧には、[プロキシサーバー] 設定で指定したサーバーを含めないでください。これらのサーバーは、WIP で保護されないトラフィックに使用されます。項目を区切るにはコンマを使用します。次に例を示します:

  example.internalproxy1.com;10.147.80.50

- クラウドリソース: WIP の保護対象となるクラウドリソースの一覧を指定します。オプションでクラウドリソースごとに、クラウドリソースへのトラフィックをルーティングするプロキシサーバーを [プロキシサーバー] の一覧から指定できます。プロキシサーバー経由でルーティングされたトラフィックはすべて、社内トラフィックとして処理されます。項目を区切るにはコンマを使用します。次に例を示します:


```
domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.
domain2.com
```

- ロックに必要な保護を設定: Windows 10 スマートフォンのみ。［オン］ にすると、パスコードデバイスポリシーも必須になります。このポリシーがない場合、Windows Information Protection ポリシーの展開は失敗します。また、このポリシーを ［オン］ にすると、［ロック時に保護が必要です］ が表示されます。デフォルトは ［オフ］ です。
- ロック時に保護が必要です: Windows 10 スマートフォンのみ。ロック済みデバイスの企業データを、従業員の PIN により保護されるキーを使用して暗号化するかどうかを指定します。デバイスがロックされると、そのデバイスの社内データをアプリで読み取れなくなります。デフォルトは、［オン］ です。
- 登録解除時に **WIP** 証明書を失効: Windows Information Protection からユーザーデバイスの登録が解除された場合に、そのデバイスのローカルの暗号化キーを失効させるかどうかを指定します。暗号化キーが失効すると、ユーザーは暗号化された社内データにアクセスできなくなります。［オフ］ にすると登録解除後もキーは失効せず、ユーザーは保護対象ファイルに引き続きアクセスできます。デフォルトは、［オン］ です。
- オーバーレイアイコンを表示: エクスプローラーに Windows Information Protection アイコンのオーバーレイを表示し、［スタート］メニューに企業専用アプリのタイルを表示するかどうかを指定します。デフォルトは、［オフ］ です。

データ回復証明書の作成

Windows Information Protection ポリシーを有効化するには、データ回復証明書が必要です。

1. XenMobile Server でコマンドプロンプトを開き、証明書を作成する（Windows\System32 以外の）フォルダーに移動します。
2. 次のコマンドを実行します。

   ```
   cipher /r:ESFDRA
   ```

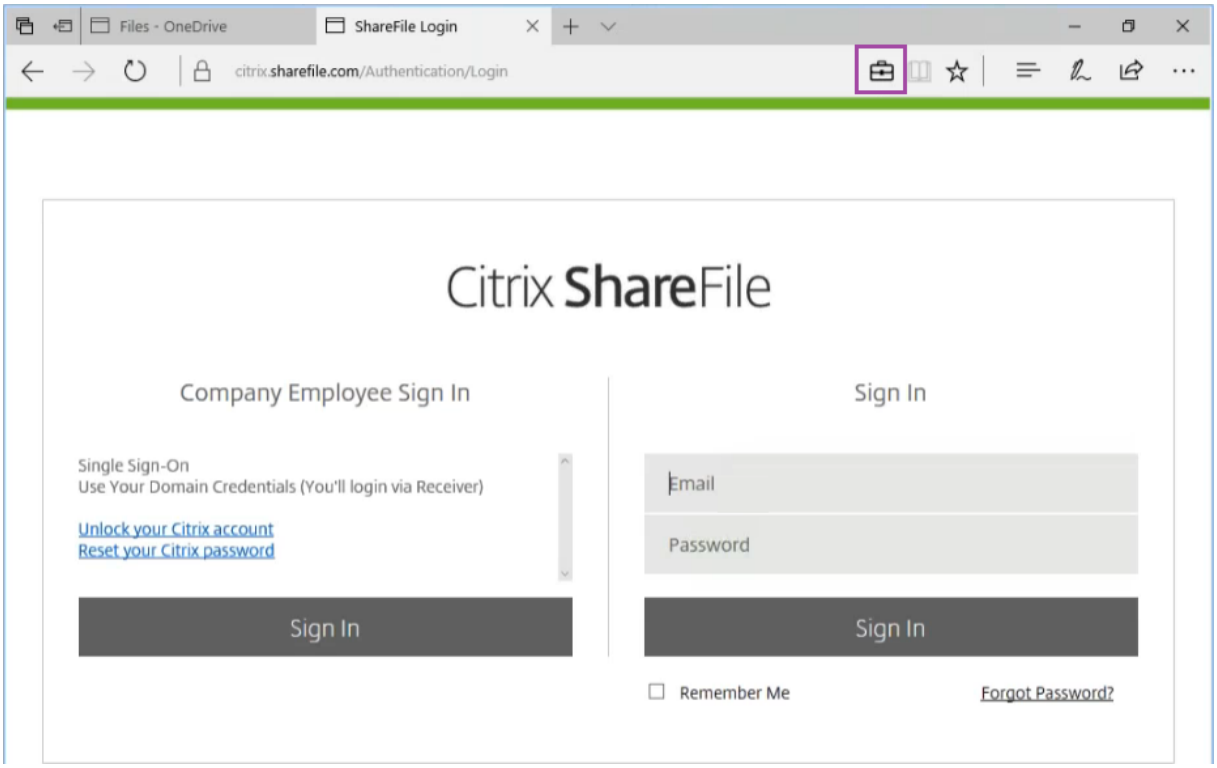
3. メッセージが表示されたら、秘密キーファイルを保護するパスワードを入力します。

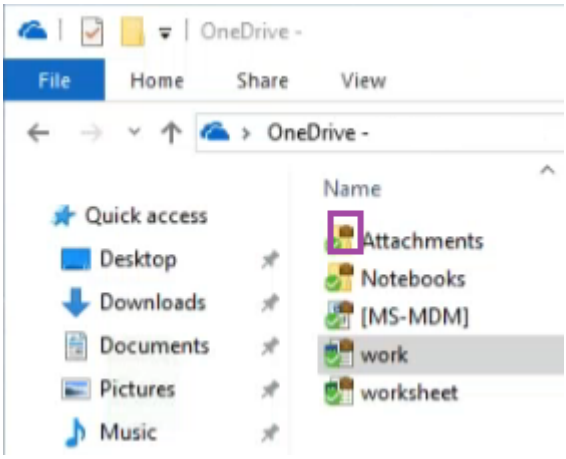
   この cipher コマンドにより、.cer ファイルと.pfx ファイルが作成されます。

4. XenMobile コンソールで ［設定］ **>** ［証明書］ の順に移動し、作成された.cer ファイルをインポートします。このファイルは Windows 10 のタブレットとスマートフォンの両方に適用されます。

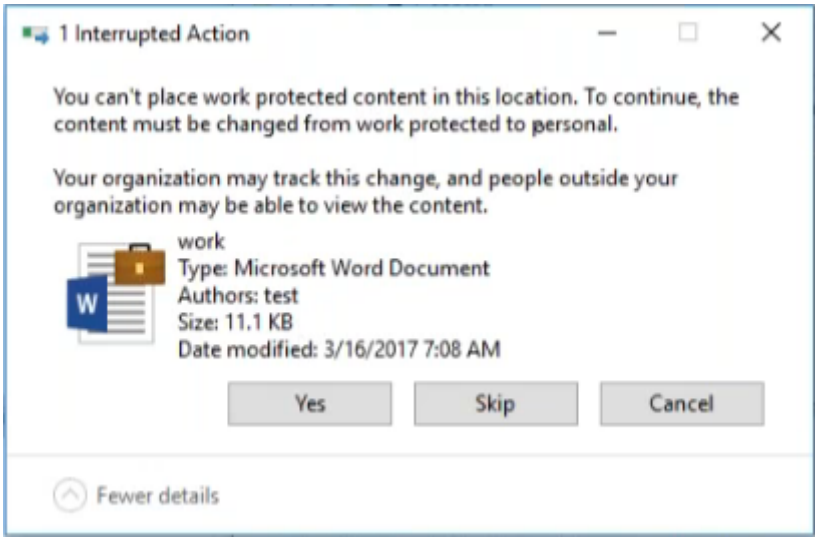
ユーザーエクスペリエンス

Windows Information Protection が有効な場合、アプリとファイルで次のアイコンが表示されます。





構成した適用レベルによっては、ユーザーが保護対象ファイルを保護されていない場所へコピーまたは保存しようとすると次の通知が表示されます。



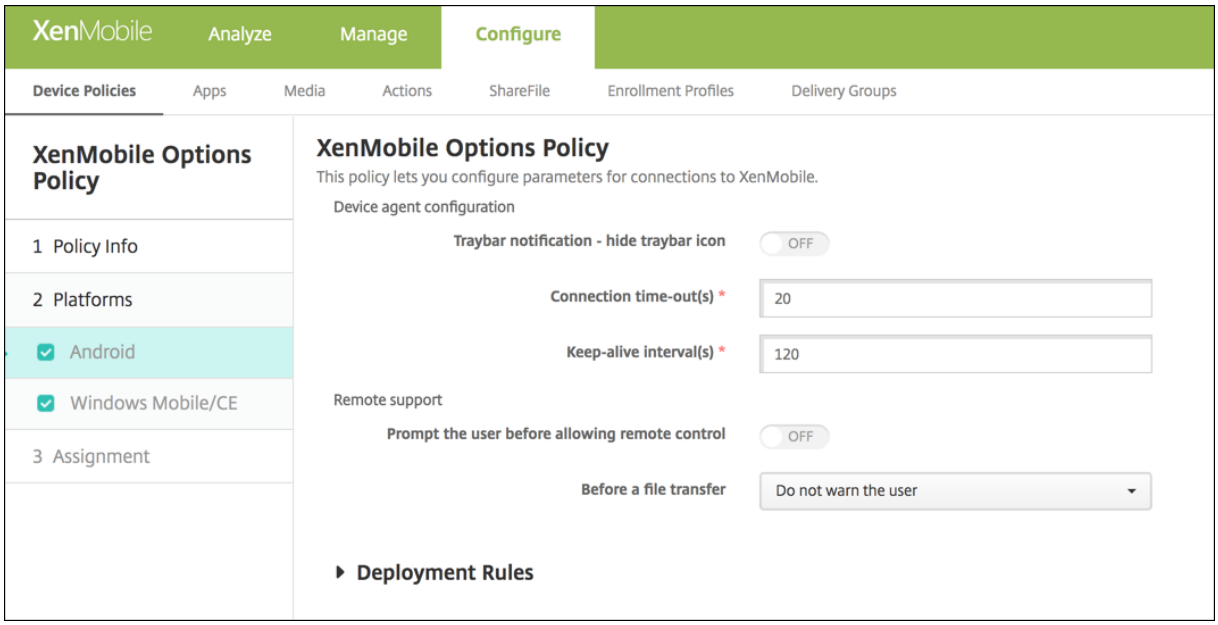
XenMobile オプションデバイスポリシー

August 22, 2019

XenMobile オプションポリシーを追加して、Android デバイスおよび Windows Mobile/CE デバイスから XenMobile に接続するときの Secure Hub の動作を構成します。

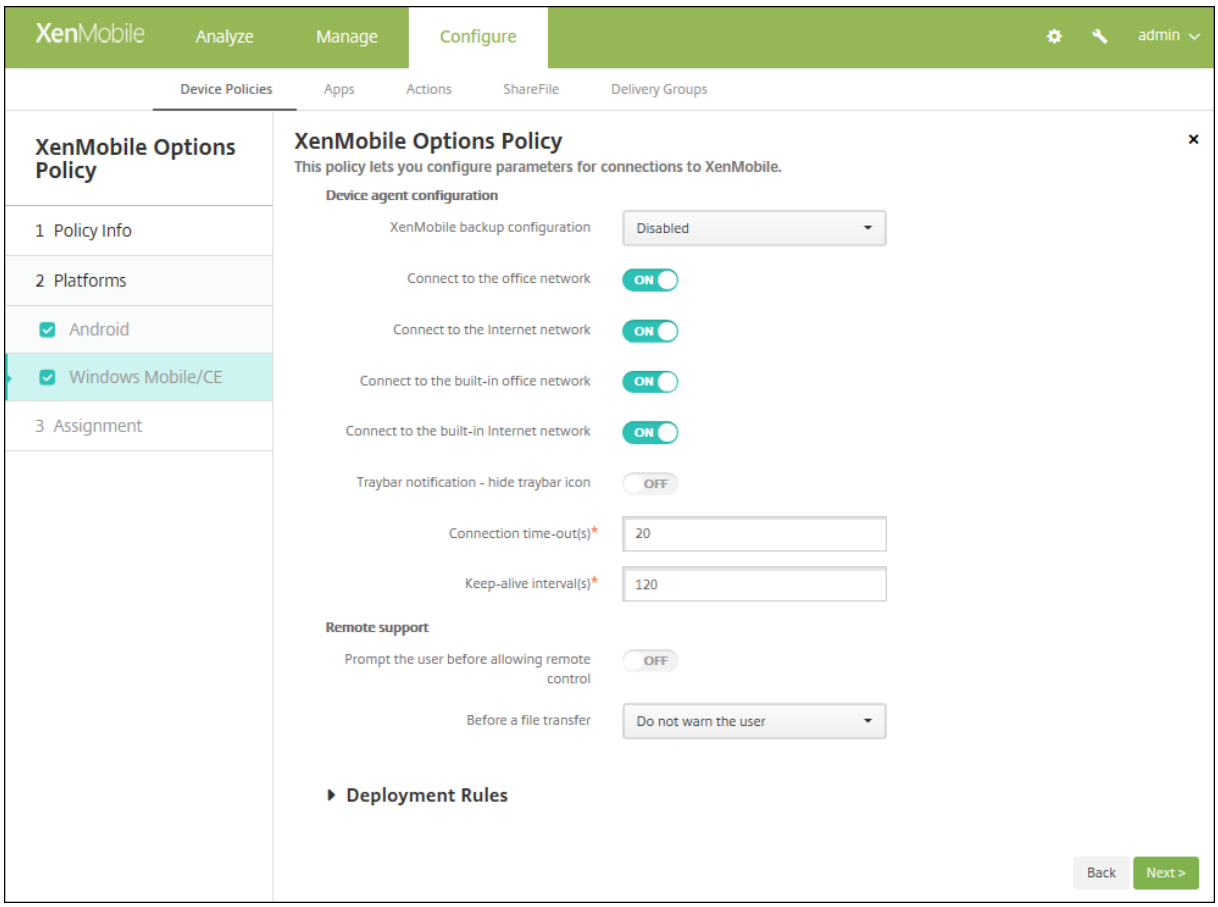
このポリシーを追加または構成するには、［構成］**>**［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android の設定



- トレイバー通知 - トレイバーアイコンを隠す： トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは ［オフ］ です。
- 接続タイムアウト： 接続のアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、接続はタイムアウトになります。デフォルトは 20 秒です。
- **Keep-alive** 間隔： 接続を開いたままにする時間（秒）を入力します。デフォルトは 120 秒です。
- リモート制御を許可する前にユーザーに確認メッセージを表示： リモートサポートの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは ［オフ］ です。
- ファイル転送の前： 一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。使用可能な値は、［ユーザーに警告しない］、［ユーザーに警告］、および ［ユーザーの許可を求める］ です。デフォルトは ［ユーザーに警告しない］ です。

Windows Mobile/CE の設定



- デバイスエージェント構成
  - **XenMobile** バックアップ構成： 一覧から、ユーザーのデバイスに XenMobile の構成をバックアップするためのオプションを選択します。デフォルトは ［無効］ です。選択できるオプションは以下のとおりです:
    * 無効
    * XenMobile インストール後の初回接続時
    * 各デバイスの再起動後の最初の接続時
  - オフィスネットワークに接続
  - インターネットネットワークに接続
  - 組み込みのオフィスネットワークに接続:［オン］ に設定した場合、XenMobile によりネットワークが自動的に検出されます。
  - 組み込みのインターネットネットワークに接続:［オン］ に設定した場合、XenMobile によりネットワークが自動的に検出されます。
  - トレイバー通知 - トレイバーアイコンを隠す： トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは ［オフ］ です。
  - 接続タイムアウト： 接続のアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、

接続はタイムアウトになります。デフォルトは 20 秒です。
  - **Keep-alive** 間隔： 接続を開いたままにする時間（秒）を入力します。デフォルトは 120 秒です。
- リモートサポート
  - リモート制御を許可する前にユーザーに確認メッセージを表示： リモートサポートの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは ［オフ］ です。
  - ファイル転送の前： 一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。使用可能な値は、［ユーザーに警告しない］、［ユーザーに警告］、および ［ユーザーの許可を求める］ です。デフォルトは ［ユーザーに警告しない］ です。

XenMobile アンインストールデバイスポリシー

August 22, 2019

XenMobile でデバイスポリシーを追加して、XenMobile を Android デバイスおよび Windows Mobile/CE デバイスからアンインストールすることができます。このポリシーを展開すると、展開グループ内のすべてのデバイスから XenMobile が削除されます。

このポリシーを追加または構成するには、［構成］ **>** ［デバイスポリシー］ の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android および **Windows Mobile/CE** の設定の構成

- **XenMobile** をデバイスからアンインストール： このポリシーを展開するすべてのデバイスから XenMobile をアンインストールするかどうかを選択します。デフォルトは ［オフ］ です。

アプリの追加

January 10, 2020

アプリケーションを XenMobile に追加して管理します。アプリケーションは XenMobile コンソールに追加します。このコンソールでは、アプリケーションをカテゴリ別に分類し、ユーザーに展開することができます。

以下の種類のアプリケーションを XenMobile に追加できます：

- **MDX**。MDX Toolkit でラップされたアプリケーションです。内部ストアおよび公開ストアから取得した MDX アプリを展開します。
- パブリックアプリストア。これらのアプリには、iTunes や Google Play などのパブリックアプリストアで無料または有料で提供されているアプリが含まれます。たとえば、GoToMeeting です。

- **Web** および **SaaS**。これらのアプリには、内部ネットワークからアクセスされるアプリ（Web アプリ）やパブリックネットワーク経由でアクセスされるアプリ（SaaS）が含まれます。独自のアプリを作成するか、一連のアプリコネクタの中から選択して、既存の Web アプリのシングルサインオン認証に使用することができます。たとえば、GoogleApps_SAML です。
- エンタープライズ。これらのアプリケーションは、MDX Toolkit でラップされておらず、MDX アプリに関連付けられたポリシーを含んでいない、ネイティブアプリです。
- **Web** リンク。これらのアプリは、パブリックサイトやプライベートサイト、またはシングルサインオンを必要としない Web アプリの Web アドレス（URL）です。

サイレントインストールについて

iOS および Samsung Android アプリのサイレントインストールがサポートされます。サイレントインストールとは、ユーザーはデバイスに展開するアプリのインストールを求められないことを意味します。アプリは、バックグラウンドで自動的にインストールされます。

サイレントインストールを実装する前提条件

- iOS アプリの場合、管理されている iOS デバイスを監視モードにします。詳しくは、「iOS および macOS プロファイルのインポートデバイスポリシー」を参照してください。
- Android アプリの場合、Samsung for Enterprise（SAFE）または KNOX ポリシーをデバイスで有効にします。

  このためには、Samsung MDM ライセンスキーデバイスポリシーを設定して、Samsung ELM および KNOX ライセンスキーを生成します。詳しくは、「Samsung MDM ライセンスキーデバイスポリシー」を参照してください。

モバイルおよび **MDX** アプリのしくみ

XenMobile では、Secure Hub、Secure Mail、Secure Web などの業務用モバイルアプリを含む iOS および Android アプリケーションと、MDX ポリシーの使用がサポートされます。XenMobile コンソールを使用し、アプリケーションをアップロードしてユーザーデバイスに配信できます。業務用モバイルアプリに加えて、次の種類のアプリを追加できます:

- 自社開発のカスタムアプリ。
- MDX ポリシーを使ってデバイスの機能を許可または制限するアプリ。

業務用モバイルアプリを配信するには、以下の一般的な手順に従います:

1. https://www.citrix.com/downloads/citrix-endpoint-management/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.htmlからパブリックストアの MDX ファイルをダウンロードします。
2. 必要に応じて MDX ポリシーを更新し、その MDX ファイルを XenMobile コンソールにアップロードします（［構成］**>**［アプリ］）。

3. MDX ファイルをパブリックアプリストアにアップロードします。詳しくは、この記事の「MDX アプリの追加」を参照してください。

   MDX Toolkit は、Citrix のロジックおよびポリシーで iOS および Android デバイス用のアプリをラップします。このツールは、組織内で作成されたアプリまたは社外で作成されたアプリに安全に対処できます。

必須のアプリとオプションのアプリについて

デリバリーグループにアプリを追加するときに、アプリがオプションか必須かを選択します。必要とマーク付けされたアプリについては、次のような場合に、ユーザーは速やかに更新プログラムを受信できます：

- アップロードした新しいアプリを必要なアプリとしてマーク付けした場合。
- 既存のアプリを必要なアプリとしてマーク付けした場合。
- 必要なアプリをユーザーが削除した場合。
- Secure Hub の更新が利用可能な場合。

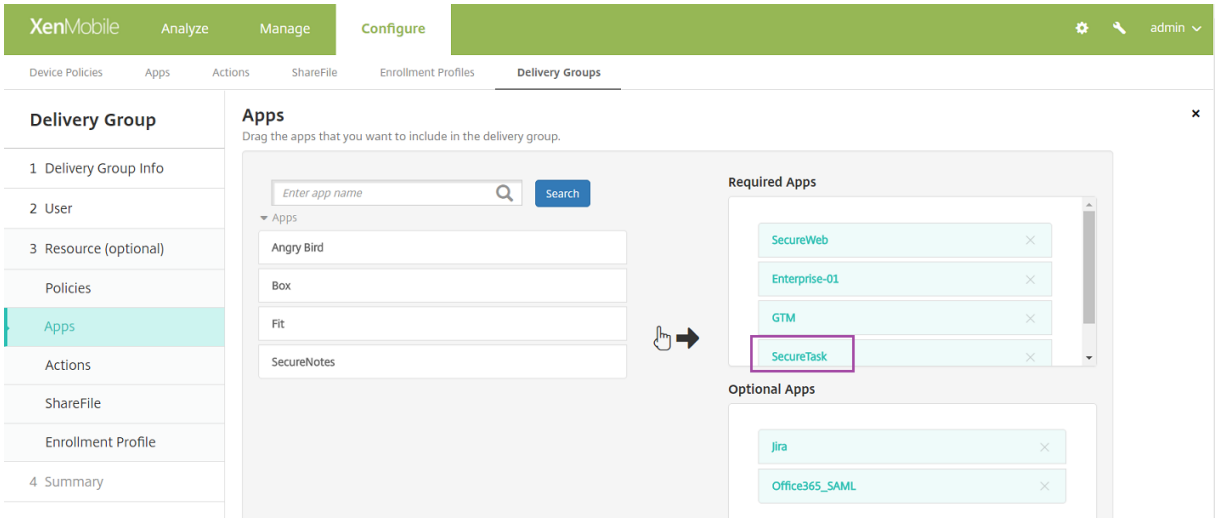
必須のアプリを強制展開するための要件

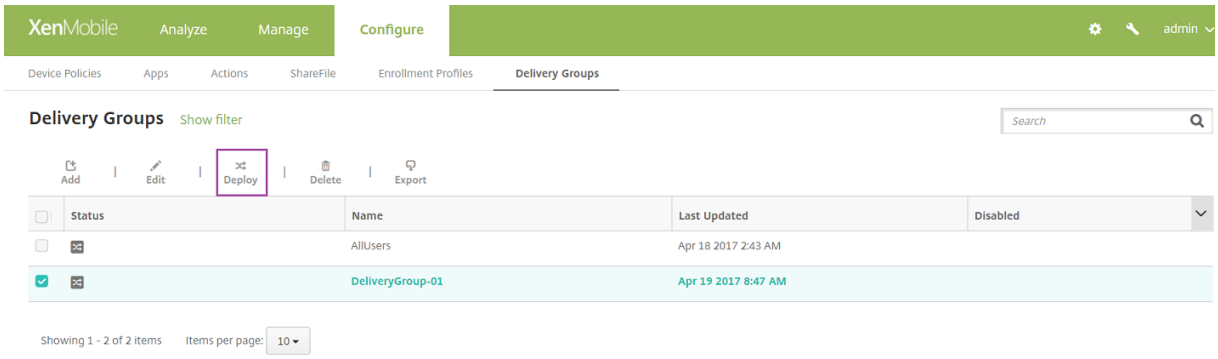
- XenMobile Server 10.6（最小バージョン）
- Secure Hub：iOS で 10.5.15、Android で 10.5.20（最小バージョン）
- MDX Toolkit 10.6（最小バージョン）
- カスタムサーバープロパティ、force.server.push.required.apps

  必須アプリの強制展開は、デフォルトでは無効になっています。この機能を有効にするには、カスタムキーのサーバープロパティを作成します。キーと表示名を **force.server.push.required.apps** に設定し、値を **true** に設定します。
- XenMobile Server と Secure Hub のアップグレード後：登録デバイスを使用するユーザーは Secure Hub をいったんサインオフしてから再びサインオンして、必要なアプリの展開の更新プログラムを取得する必要があります。

例

次の例で Secure Tasks アプリをデリバリーグループに追加し、そのデリバリーグループを展開する流れを示します。





サンプルアプリである Secure Tasks をユーザーデバイスに展開すると、Secure Hub によってアプリのインストールを求めるプロンプトがユーザーに表示されます。

> 重要:
>
> エンタープライズアプリやパブリックアプリストアのアプリなど、MDX 対応の必須アプリは、アプリ更新猶予期間が MDX ポリシーで構成され、ユーザーがアプリを後からアップグレードすることを選択した場合でも、すぐにアップグレードされます。

iOS 必須アプリのワークフロー（エンタープライズアプリおよびパブリックストアアプリの場合）

1. 初回登録時に XenMobile アプリを展開します。必須アプリがデバイスにインストールされます。
2. XenMobile コンソールのアプリを更新します。
3. XenMobile コンソールを使用して必須アプリを展開します。
4. ホーム画面のアプリが更新されます。また、パブリックストアアプリの場合は、アップグレードが自動的に開始されます。ユーザーに更新のメッセージは表示されません。
5. ユーザーはホーム画面からアプリを開きます。アプリ更新の猶予期間が設定済みで、後でアプリをアップグレードするようにユーザーが選択した場合でも、アプリはただちにアップグレードされます。

Android 必須アプリのワークフロー（エンタープライズアプリの場合）

1. 初回登録時に XenMobile アプリを展開します。必須アプリがデバイスにインストールされます。
2. XenMobile コンソールを使用して必須アプリを展開します。
3. アプリがアップグレードします。（Nexus デバイスでは更新プログラムのインストールを求めるメッセージが表示されますが、Samsung デバイスではサイレントインストールが行われます。）
4. ユーザーはホーム画面からアプリを開きます。アプリ更新の猶予期間が設定済みで、後でアプリをアップグレードするようにユーザーが選択した場合でも、アプリはただちにアップグレードされます。（Samsung デバイスではサイレントインストールが行われます。）

Android 必須アプリのワークフロー（パブリックストアアプリの場合）

1. 初回登録時に XenMobile アプリを展開します。必須アプリがデバイスにインストールされます。
2. XenMobile コンソールのアプリを更新します。
3. XenMobile コンソールを使用して必須アプリを展開します。または、デバイス上で Secure Hub ストアを開きます。アップデートアイコンがストアに表示されます。
4. 自動的にアプリのアップグレードが始まります。（Nexus デバイスにより、更新プログラムのインストールがユーザーに促されます。）
5. ホーム画面でアプリを開きます。アプリがアップグレードします。猶予期間に関するメッセージはユーザーに表示されません。（Samsung デバイスではサイレントインストールが行われます。）

Web および **SaaS** アプリのしくみ

XenMobile には、一連のアプリケーションコネクタが用意されています。これらは、Web アプリおよび SaaS アプリケーションのシングルサインオンを構成するためのテンプレートです。ユーザーアカウントの作成や管理用のテンプレートを構成することもできます。XenMobile には、Security Assertion Markup Language（SAML）コネクタが含まれています。SAML コネクタは、SSO およびユーザーアカウント管理用の SAML プロトコルをサポートする Web アプリで使用されます。XenMobile は、SAML 1.1 および SAML 2.0 をサポートします。

また、独自のエンタープライズ SAML コネクタを構築することもできます。

エンタープライズアプリのしくみ

エンタープライズアプリは、通常は内部ネットワークに存在します。ユーザーは Secure Hub を使ってそのアプリに接続できます。エンタープライズアプリを追加すると、XenMobile はそのアプリケーションコネクタを作成します。

パブリックアプリストアのしくみ

Apple App Store および Google Play からアプリの名前と説明を取得するための設定を構成できます。ストアからアプリ情報を取得すると、XenMobile により既存の名前と説明が上書きされます。

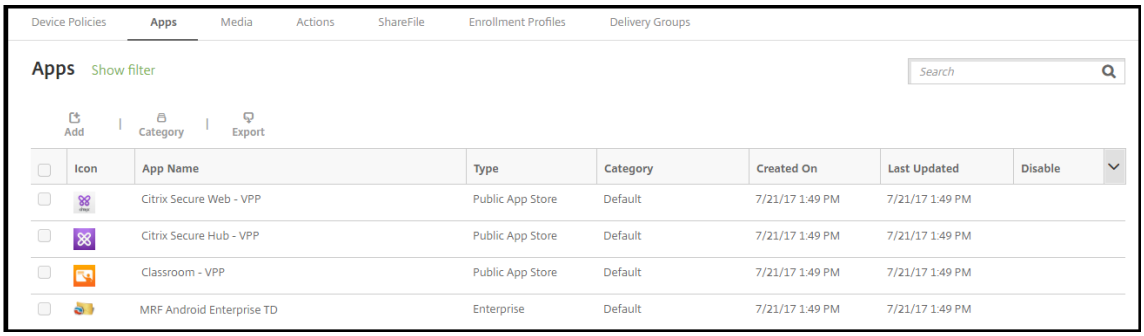
Web リンクのしくみ

Web リンクはインターネットサイトまたはイントラネットサイトの Web アドレスです。Web リンクは、SSO を必要としない Web アプリも参照できます。Web リンクの構成が完了すると、リンクは XenMobile Store にアイコンとして表示されます。ユーザーが Secure Hub を使ってログオンすると、リンクは使用可能なアプリおよびデスクトップの一覧と共に表示されます。

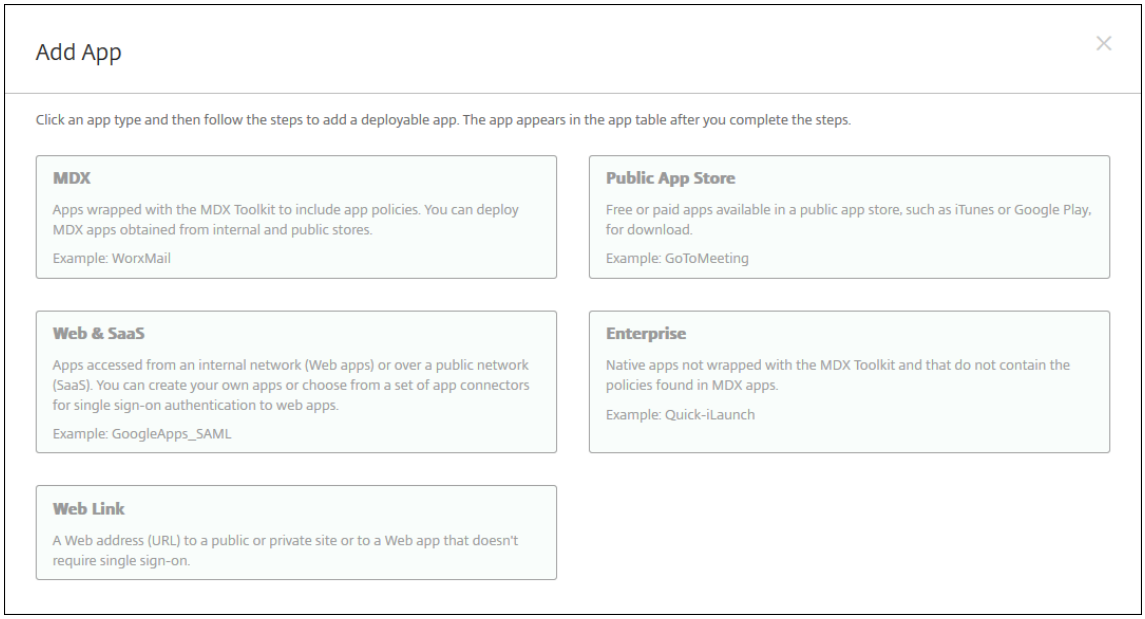
MDX アプリの追加

iOS または Android デバイス用のラップされた MDX モバイルアプリを取得したら、そのアプリを XenMobile にアップロードできます。アプリをアップロードした後、アプリの詳細とポリシー設定を構成できます。各デバイスプラットフォームの種類で使用できるアプリケーションポリシーについて詳しくは、「MDX ポリシーの概要」を参照してください。このトピックでは、ポリシーの詳細についても説明しています。

1. XenMobile コンソールで、［構成］ > ［アプリ］ をクリックします。［アプリ］ ページが開きます。



2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3. ［**MDX**］ をクリックします。［アプリ情報］ ページが開きます。

4. ［アプリ情報］ ペインで、以下の情報を入力します:

    - 名前: アプリの説明的な名前を入力します。その名前は、［アプリ］ の表の ［アプリ名］ の下に表示されます。
    - 説明: 任意で、アプリの説明を入力します。
    - アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリカテゴリの作成」を参照してください。

5. ［次へ］ をクリックします。アプリのプラットフォームページが開きます。

6. ［プラットフォーム］ で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

    1 つのプラットフォームの設定の構成が完了したら、手順 11 を参照してプラットフォームの展開規則を設定します。

7. ［アップロード］をクリックしてアップロードする MDX ファイルの場所へ移動し、そのファイルを選択します。

    - iOS VPP B2B アプリを追加する場合は、［お使いのアプリケーションは **VPP B2B** アプリケーションですか**?**］ をクリックして、一覧から使用する B2B VPP アカウントを選択します。

8. ［次へ］ をクリックします。［アプリケーション詳細］ ページが開きます。

9. 次の設定を構成します。

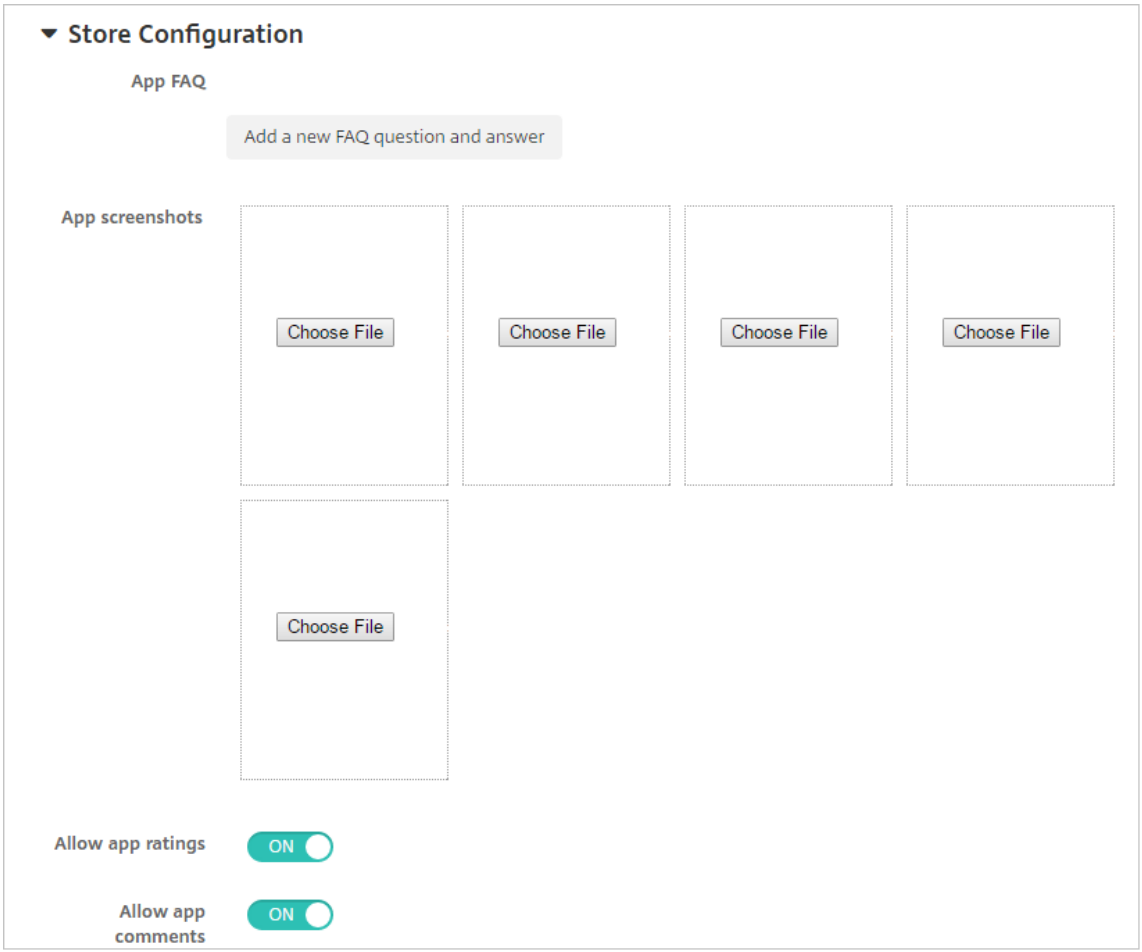
    - ファイル名: アプリに関連付けられているファイル名を入力します。
    - アプリの説明: アプリの説明を入力します。
    - アプリのバージョン: 任意で、アプリのバージョン番号を入力します。
    - 最小 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
    - 最大 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
    - 除外するデバイス: 任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
    - **MDM** プロファイルが削除されたらアプリを削除します: MDM プロファイルが削除された場合にデバイスからアプリを削除するかどうかを選択します。デフォルトは ［オン］ です。
    - アプリデータのバックアップを阻止します: ユーザーがアプリデータをバックアップできないようにするかどうかを選択します。デフォルトは ［オン］ です。
    - 管理されるアプリ: アプリが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリの管理を許可するように求めるかどうかを選択します。デフォルトは ［オン］ です。iOS 9.0 以降で利用できます。
    - **VPP** 経由で展開されたアプリ: VPP を使用してアプリを展開するかどうかを選択します。これが ［オン］ で、MDX バージョンのアプリを展開し、アプリの展開に VPP を使用する場合、Secure Hub では VPP インスタンスのみが表示されます。デフォルトは ［オフ］ です。

10. **MDX** ポリシーを構成します。MDX ポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、暗号化、アプリ相互作用、アプリ制限などのポリシー領域で適用するオプションが含まれます。

XenMobile コンソールでは、ポリシーごとに、ポリシーを説明するヒントが提供されます。

MDX アプリのアプリポリシーについて詳しくは、「MDX ポリシーの概要」を参照してください。その説明には各プラットフォームに適用するポリシーを示す表が含まれています。

11. 展開規則を構成します。詳しくは、「リソースの展開」を参照してください。
12. [**XenMobile Store** 構成] を展開します。

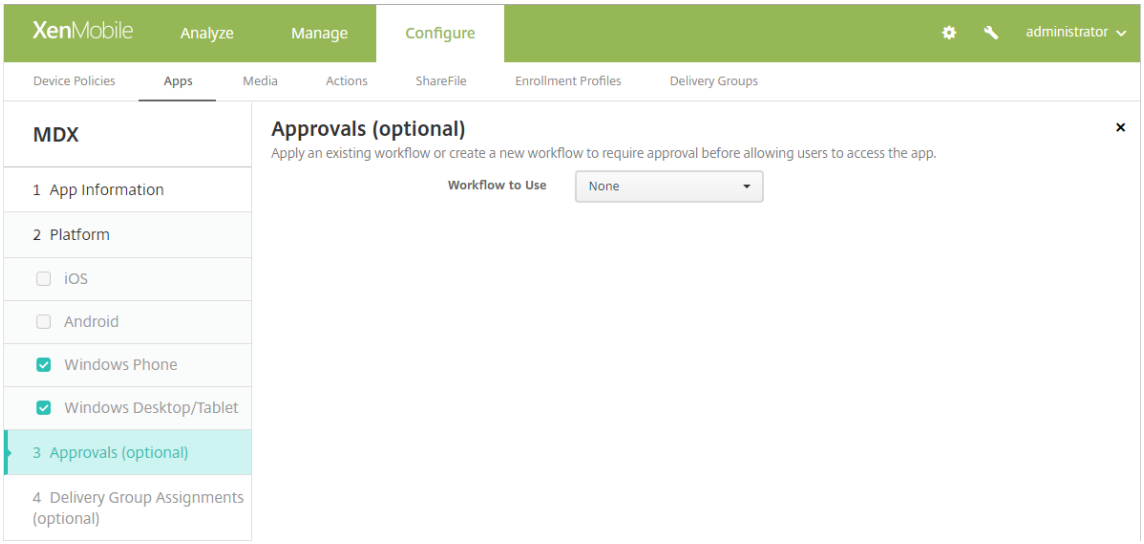


任意で、アプリに関する FAQ や、XenMobile Store に表示される画面キャプチャを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - アプリの **FAQ**: アプリに関する FAQ の質問および回答を追加します。
  - アプリスクリーンショット: アプリを XenMobile Store で分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックは PNG である必要があります。GIF イメージや JPEG イメージはアップロードできません。
  - アプリ評価を許可: ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは [オン] です。

    アプリコメントを許可: 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [オン] です。

13.［次へ］ をクリックします。［承認］ ページが開きます。



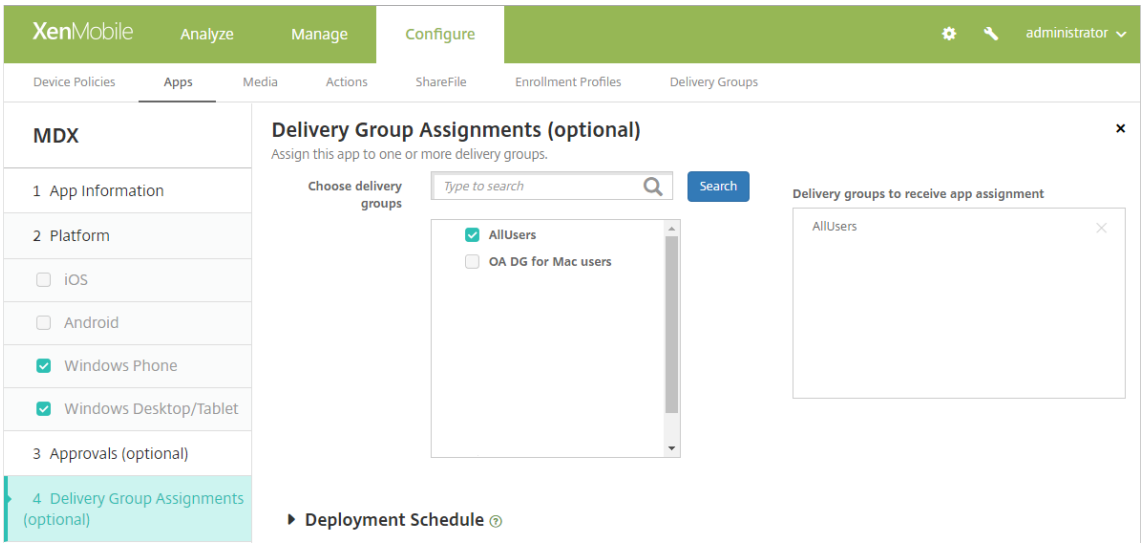
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順 15 に進みます。

ワークフローを割り当てるか作成するには、次の設定を構成します：

- 使用するワークフロー： 一覧から既存のワークフローを選択するか、［新しいワークフローの作成］ をクリックします。デフォルトは ［なし］ です。
- ［新しいワークフローの作成］ を選択した場合は、次の設定を構成します。詳しくは、「ワークフローの作成および管理」を参照してください。
- 名前： ワークフローの固有の名前を入力します。
- 説明： 任意で、ワークフローの説明を入力します。
- メール承認テンプレート： 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
- マネージャー承認のレベル： 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［1 つのレベル］です。選択できるオプションは以下のとおりです：
  - 不必要
  - 1 つのレベル
  - 2 つのレベル
  - 3 つのレベル
- **Active Directory** ドメインの選択： 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
- 追加の必須承認者を検索： 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
  - ［選択した追加の必須承認者］ の一覧からユーザーを削除するには、次のいずれかを行います：

* ［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
* 名前の全体または一部を検索ボックスに入力して ［検索］ をクリックし、検索結果を絞り込みます。
* ［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

14. ［次へ］ をクリックします。［デリバリーグループ割り当て］ ページが開きます。



15. ［デリバリーグループを選択］ の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。

16. ［展開スケジュール］ を展開して以下の設定を構成します:

- ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。
- ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
- ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリックします。デフォルトのオプションは、［接続するたび］ です。
- ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

> 注:
>
> このオプションは、［設定］ > ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
>
> 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォーム

> に変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。

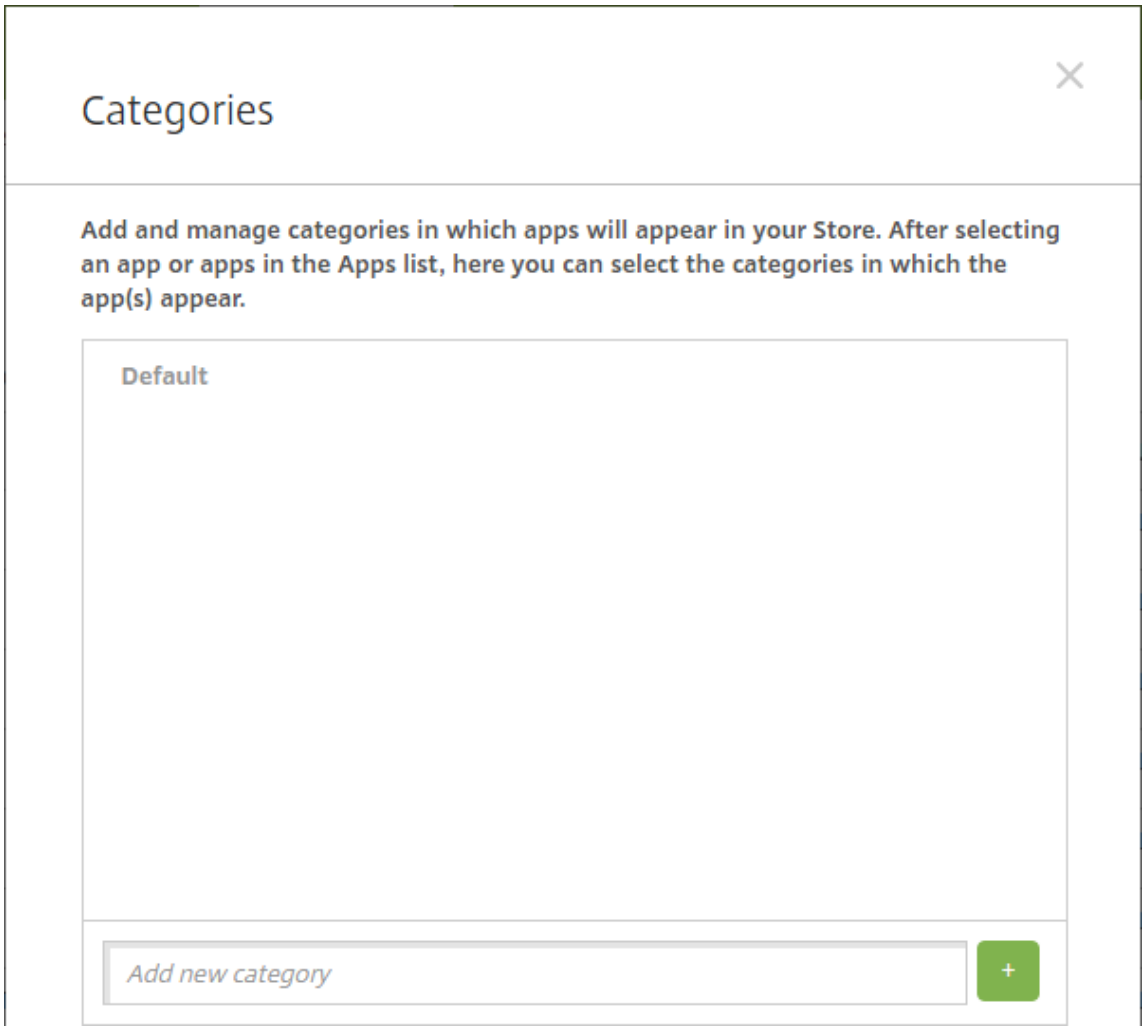
17. ［保存］ をクリックします。

アプリカテゴリの作成

ユーザーが Secure Hub にログオンすると、XenMobile で設定したアプリケーション、Web リンク、ストアの一覧が表示されます。管理者がアプリカテゴリを使用することにより、ユーザーは指定されたアプリ、ストア、または Web リンクだけにアクセスできます。たとえば、「Finance」カテゴリを作成して財務関連のアプリを追加したり、「Sales」カテゴリを構成して営業関連のアプリを追加したりすることができます。

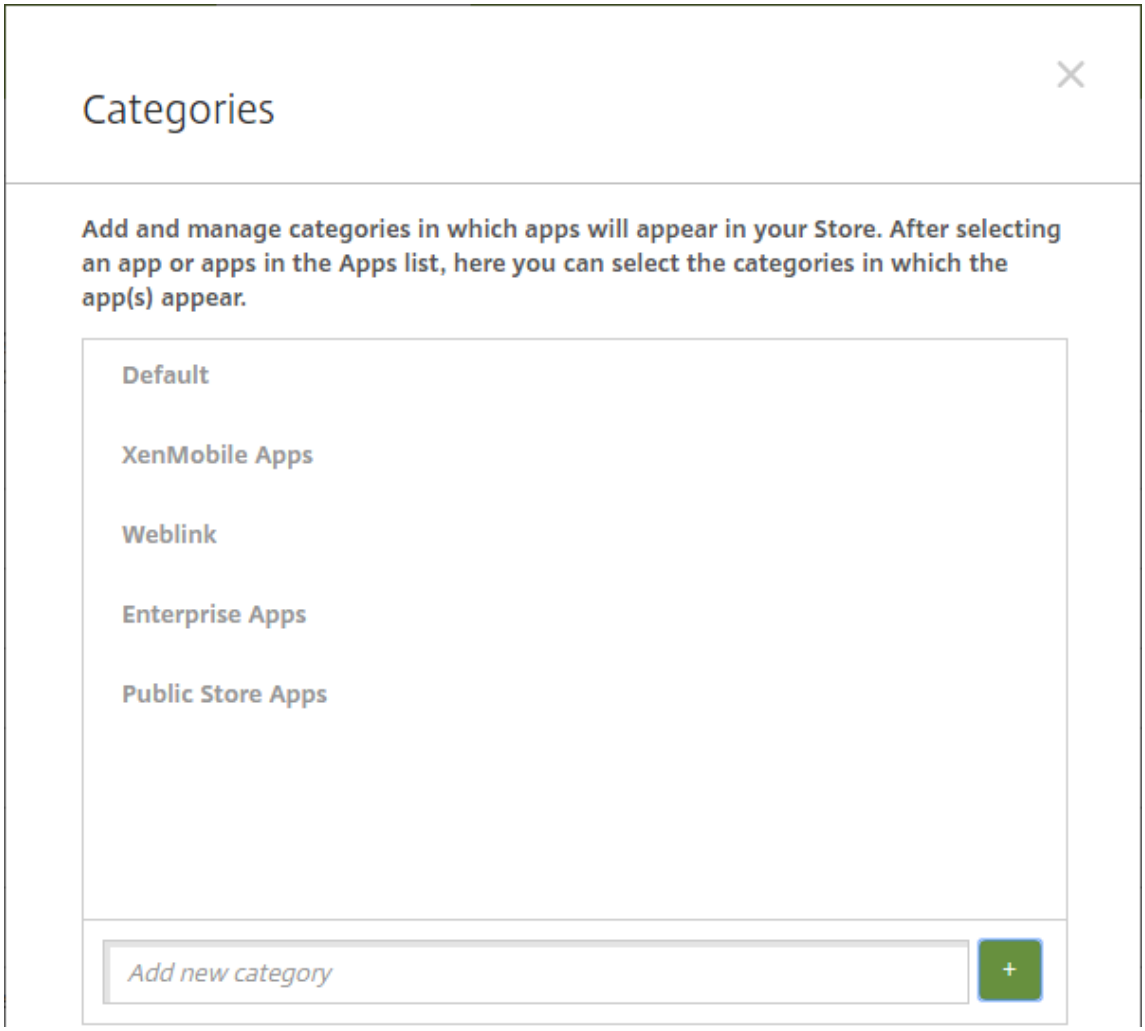
XenMobile コンソールの ［アプリ］ ページで、カテゴリを構成します。次に、アプリ、Web リンク、ストアを追加または編集するとき、構成した 1 つまたは複数のカテゴリにアプリを追加できます。

1. XenMobile コンソールで、［構成］ **>** ［アプリ］ をクリックします。［アプリ］ ページが開きます。
2. ［カテゴリ］ をクリックします。［カテゴリ］ ダイアログボックスが開きます。



3. 追加するカテゴリごとに、以下の操作を行います:

- ダイアログボックス下部にある ［新しいカテゴリの追加］ フィールドに、追加するカテゴリの名前を入力します。たとえば、「Enterprise Apps」と入力して、エンタープライズアプリのカテゴリを作成することができます。
- プラス記号（+）をクリックしてカテゴリを追加します。新しく作成したカテゴリが追加され、［カテゴリ］ ダイアログボックスに表示されます。



4. カテゴリの追加が終了したら、［カテゴリ］ ダイアログボックスを閉じます。
5. ［アプリ］ ページで、既存のアプリを新しいカテゴリに分類できます。
   - 分類するアプリを選択します。
   - ［編集］ をクリックします。［アプリ情報］ ページが開きます。
   - ［アプリカテゴリ］ の一覧で、新しいカテゴリのチェックボックスをオンにしてカテゴリを適用します。既存のカテゴリでアプリに適用しないものについては、チェックボックスをオフにします。
   - ［デリバリーグループ割り当て］ タブをクリックするか、後続の各ページで ［次へ］ をクリックして、残りのアプリセットアップページに示される手順に従います。
   - ［デリバリーグループ割り当て］ のページの ［保存］ をクリックして新しいカテゴリを適用します。新しいカテゴリがアプリに適用され、［アプリ］ の表に表示されます。

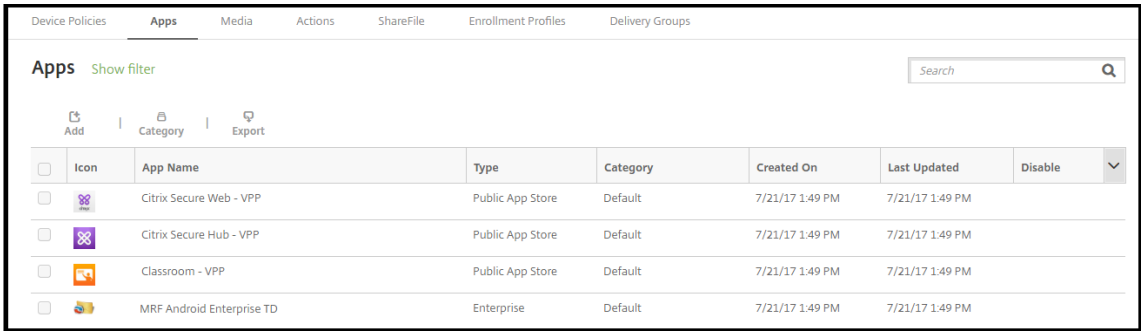
パブリックアプリストアのアプリの追加

iTunes や Google Play などのパブリックアプリケーションストアで入手できる無料または有料のアプリケーションを XenMobile に追加できます。

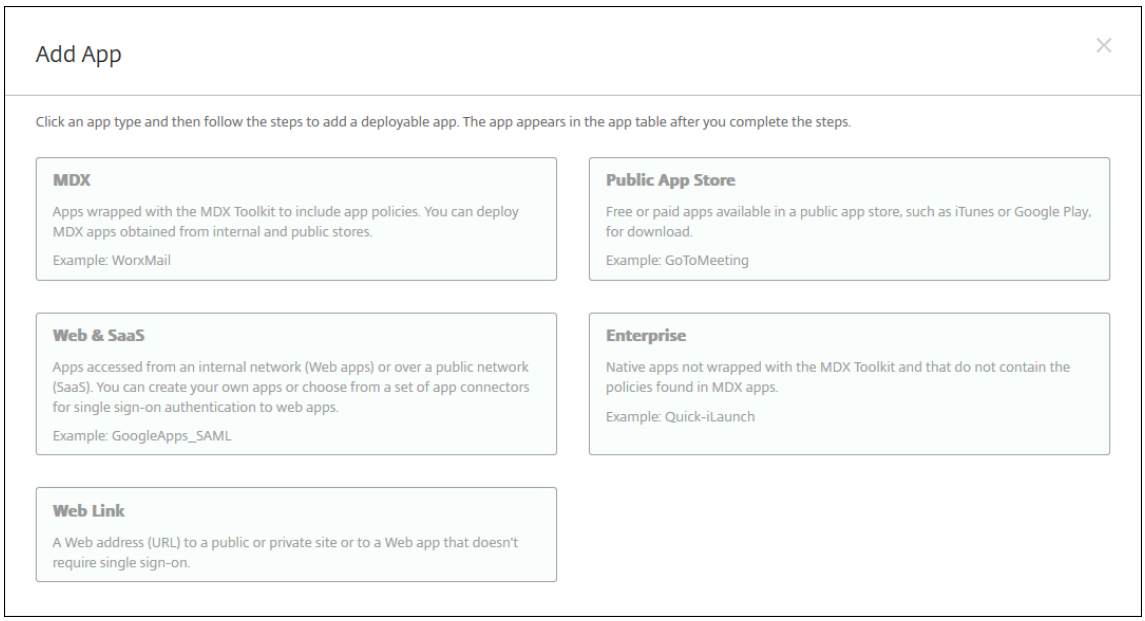
Android Enterprise 用のパブリックアプリストアの有料アプリを追加する場合、一括購入ライセンスの状態を確認できます。状態に含まれる情報は、使用できる合計ライセンス数、使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレスです。Android Enterprise の一括購入プランを利用すると、組織のアプリやその他のデータの検索、購入、配布の処理が簡単になります。

アプリ情報を構成し、アプリを配信するプラットフォームを選択します:

1. XenMobile コンソールで、［構成］ > ［アプリ］ をクリックします。［アプリ］ ページが開きます。



2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3. ［パブリックアプリストア］ をクリックします。［アプリ情報］ ページが開きます。
4. ［アプリ情報］ ペインで、以下の情報を入力します:
   - 名前: アプリの説明的な名前を入力します。この名前は、［アプリ］ の表の ［アプリ名］ の下に表示されます。

- 説明: 任意で、アプリの説明を入力します。
- アプリカテゴリ: 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリカテゴリの作成」を参照してください。

5. [次へ] をクリックします。アプリのプラットフォームページが開きます。
6. [プラットフォーム] で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

   次に、各プラットフォームのアプリ設定を構成します。1 つのプラットフォームの設定の構成が完了したら、プラットフォームの展開規則とストア構成を設定します。

次に、各プラットフォームのアプリ設定を構成します。1 つのプラットフォームの設定の構成が完了したら、プラットフォームの展開規則とストア構成を設定します。

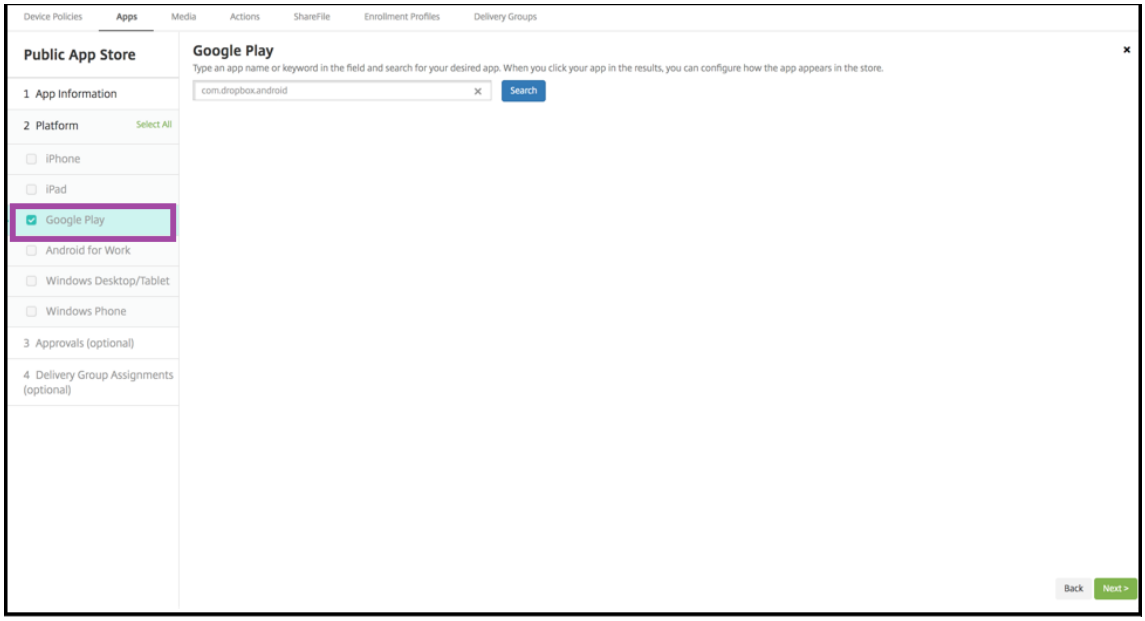
> 重要: Google Play ストアのアプリ設定を構成するには、他のプラットフォームのアプリとは異なる手順が必要です。Google Play ストアのアプリ情報は手動で構成する必要があります。

Google Play アプリのアプリ設定を構成する

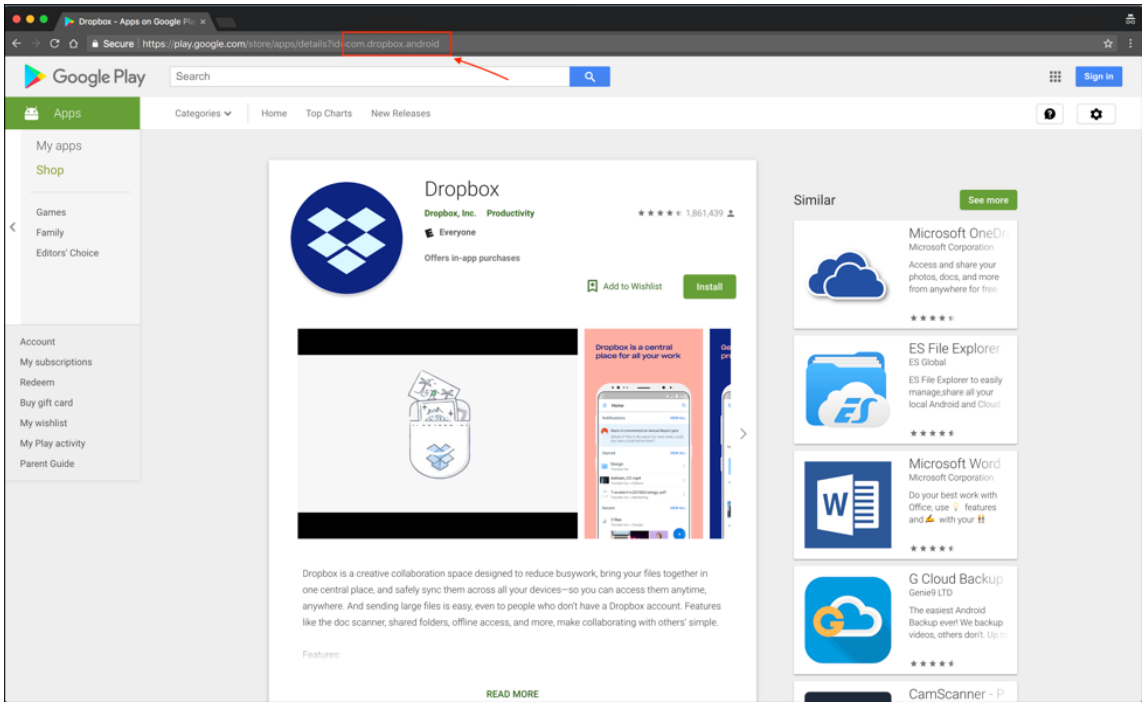
> 注:
>
> Google Play ストアのすべてのアプリに managed Google Play からアクセスできるようにするには、XenMobile のサーバープロパティ **Access all apps in the managed Google Play store** を使用します。サーバープロパティを参照してください。このプロパティを **true** に設定すると、すべての Android Enterprise ユーザー向けのパブリック Google Play ストアアプリがホワイトリストに登録されます。制限デバイスポリシーを使用してこれらのアプリへのアクセスを制御できます。

Google Play ストアのアプリ設定を構成するには、他のプラットフォームのアプリとは異なる手順が必要です。Google Play ストアのアプリ情報は手動で構成する必要があります。

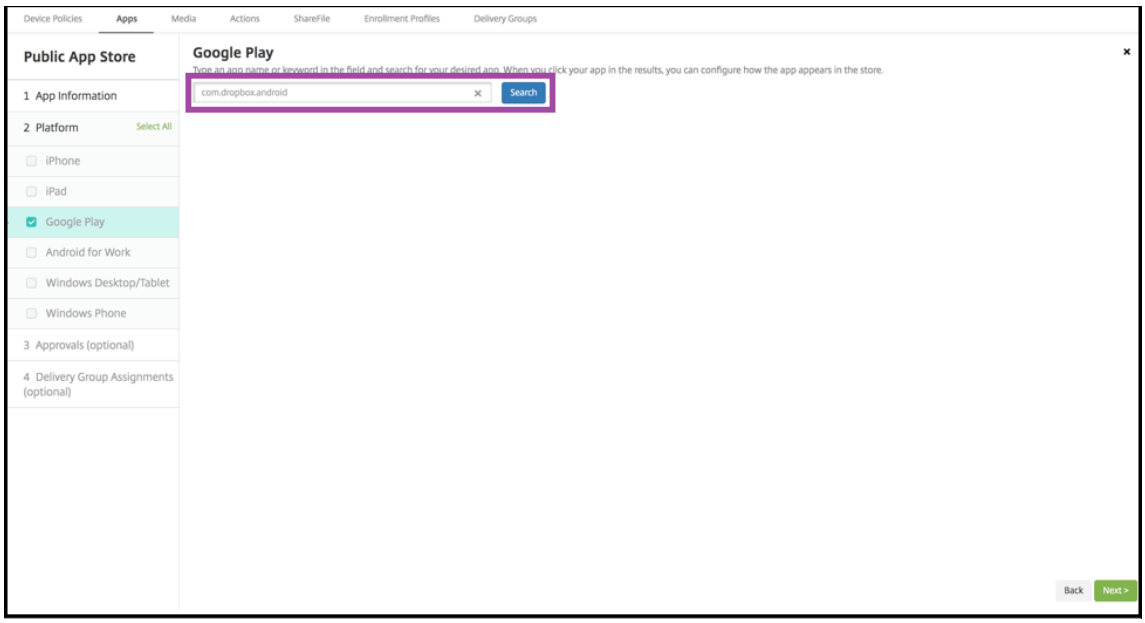
1. [プラットフォーム] で [**Google Play**] が選択されていることを確認します。



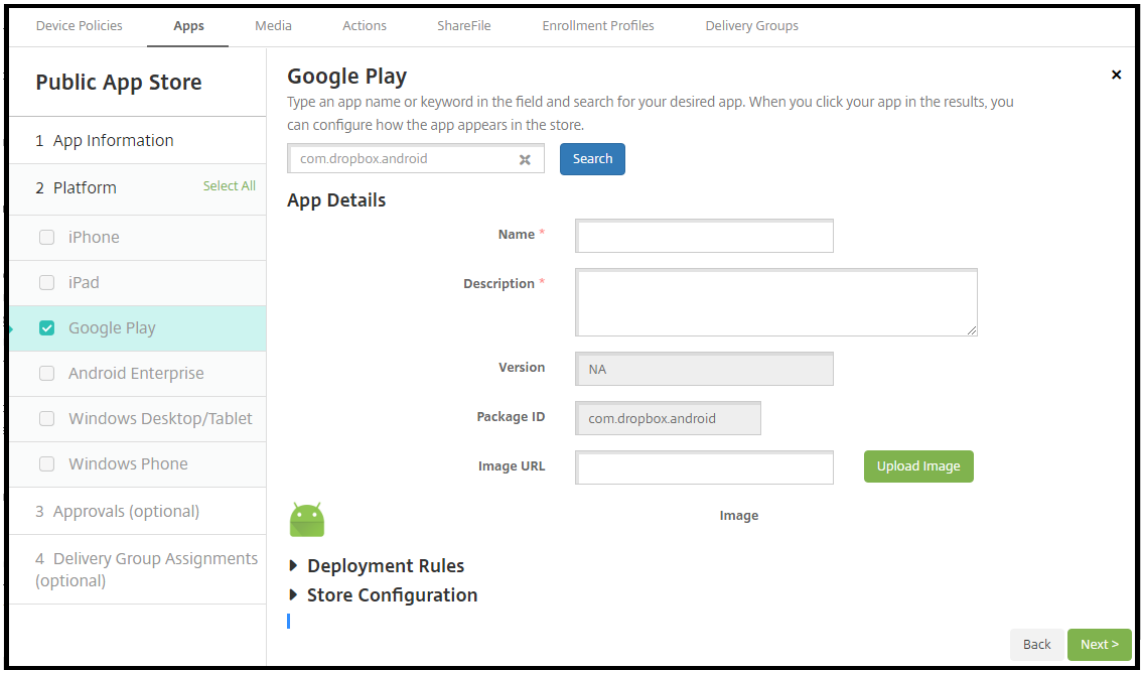
2. Google Play ストアに移動します。Google Play ストアからパッケージ ID をコピーします。この ID はアプリの URL に含まれています。



3. パブリックストアのアプリを XenMobile Server コンソールに追加する際に、検索バーに含まれるパッケージ ID を貼り付けます。［検索］ をクリックします。



4. パッケージ ID が有効な場合は、アプリの詳細を入力できる UI が表示されます。



5. ストアのアプリと共に表示する画像の URL を構成できます。Google Play ストアの画像を使用するには:

   a) Google Play ストアに移動します。アプリの画像を右クリックし、画像のアドレスをコピーします。

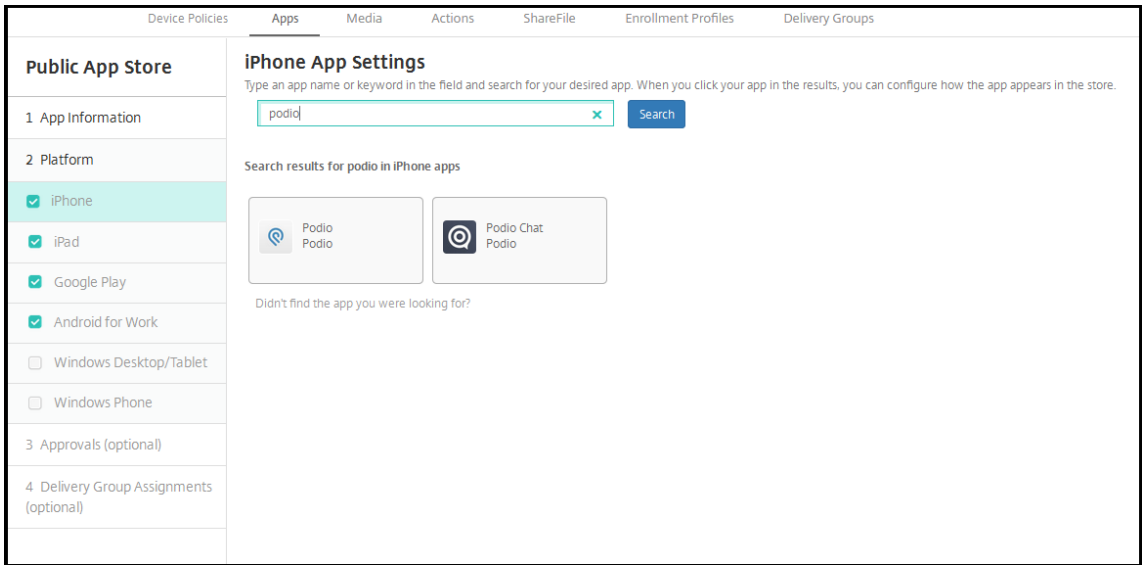
   b) アドレスを ［画像 **URL**］ フィールドに貼り付けます。

   c)［画像のアップロード］ をクリックします。画像が ［イメージ］ の横に表示されます。

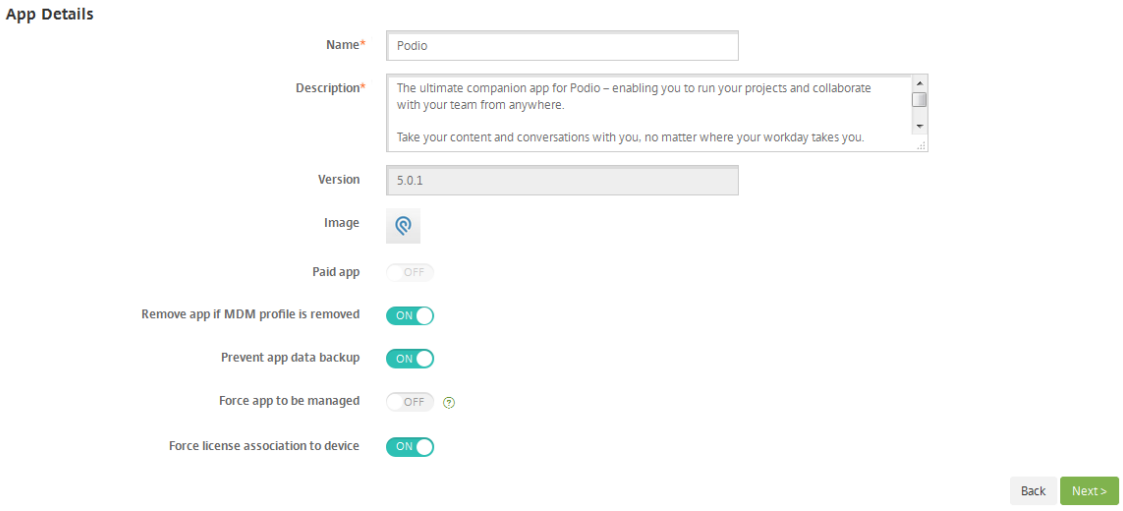
画像を構成しない場合は、Android の一般的な画像がアプリに表示されます。

Google Play 以外のプラットフォームのアプリ設定を構成する

1. 追加するアプリの名前を検索ボックスに入力し、［検索］ をクリックして、アプリを選択します。検索条件に一致するアプリが表示されます。次の図は、iPhone アプリでの「**podio**」の検索結果を示しています。



2. 追加するアプリをクリックします。［アプリケーションの詳細］ フィールドに、選択したアプリケーションに関連する情報（名前、説明、バージョン番号、関連付けられたイメージなど）を設定します。



3. 次の設定を構成します。

   - 必要に応じて、アプリの名前と説明を変更します。
   - 有料アプリ： このフィールドは事前に構成されており、変更できません。
   - **MDM** プロファイルが削除されたらアプリを削除します： MDM プロファイルが削除された場合にアプリを削除するかどうかを選択します。デフォルトは ［オン］ です。
   - アプリデータのバックアップを阻止します： アプリのデータをバックアップできないようにするかどうかを選択します。デフォルトは ［オン］ です。

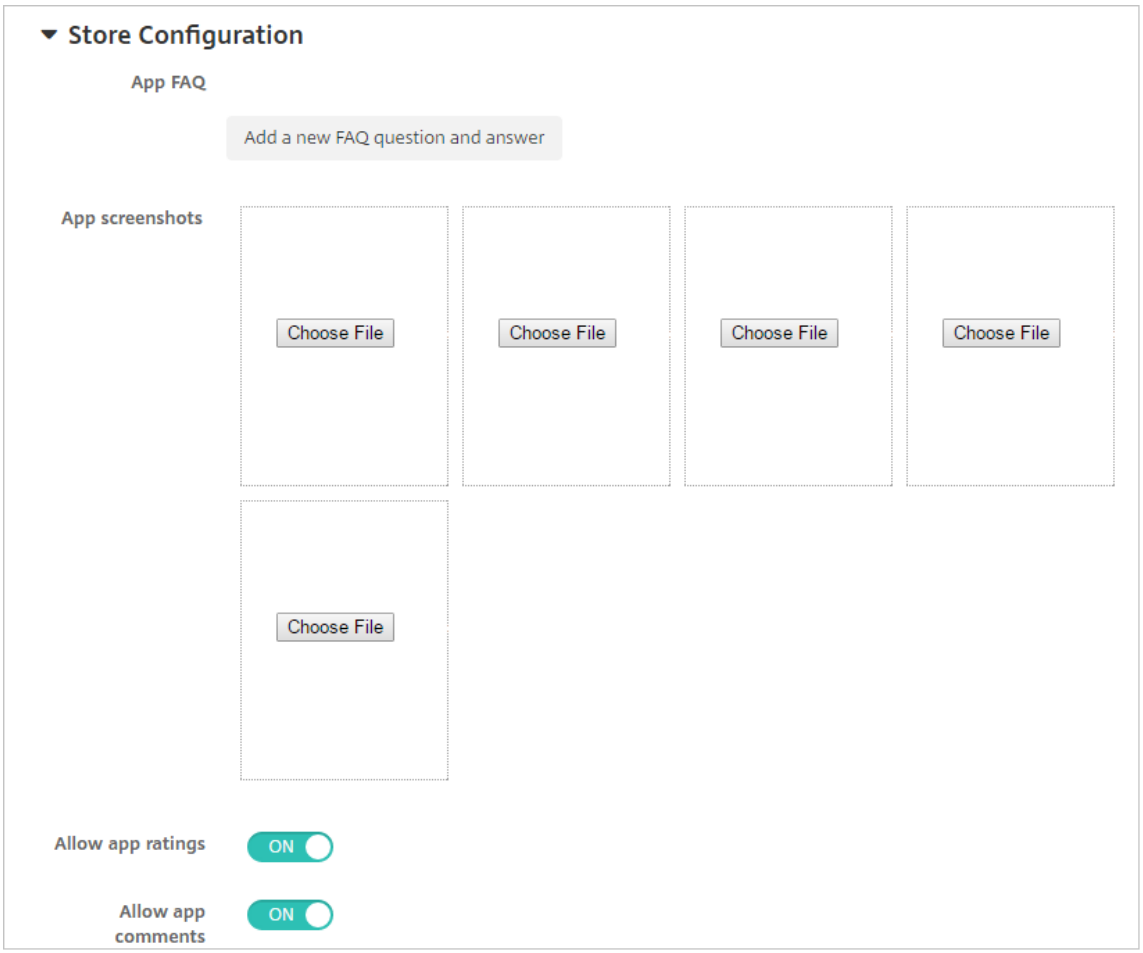
- 管理されるアプリ： アプリが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリの管理を許可するように求めるかどうかを選択します。デフォルトは ［オフ］ です。iOS 9.0 以降で利用できます。
- デバイスへの強制ライセンス割り当て： デバイスの関連付けを有効にして開発されたアプリを、ユーザーではなくデバイスに関連付けるかどうかを選択します。iOS 9 以降で利用できます。選択したアプリがデバイスへの割り当てをサポートしていない場合、このフィールドは変更できません。

展開規則を構成する

詳しくは、「リソースの展開」を参照してください。

ストア構成をセットアップする

1. ［**XenMobile Store** 構成］ を展開します。



任意で、アプリに関する FAQ や、XenMobile Store に表示される画面キャプチャを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - アプリの **FAQ**： アプリに関する FAQ の質問および回答を追加します。
  - アプリスクリーンショット： アプリを XenMobile Store で分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックは PNG である必要があります。GIF イメージや JPEG イメージはアップロードできません。
  - アプリ評価を許可： ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは［オン］です。
  - アプリコメントを許可： 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。

2. ［**Volume Purchase Program**（**VPP**）］ を展開するか、Android Enterprise の場合は ［一括購入］ を展開します。

   この Volume Purchase Program について、次の手順に従います。

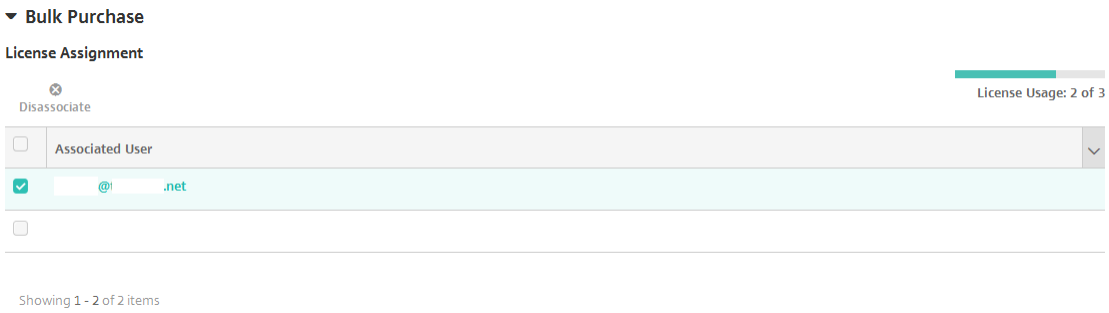
   a) XenMobile でアプリケーションの VPP ライセンスを適用できるようにする場合は、 ［**VPP** ライセンス］ の一覧から、 ［**VPP** ライセンスファイルをアップロードする］ を選択します。

   b) ダイアログボックスが開いたら、ライセンスをインポートします。

   Android Enterprise の一括購入の場合は、 ［一括購入］ セクションを展開します。

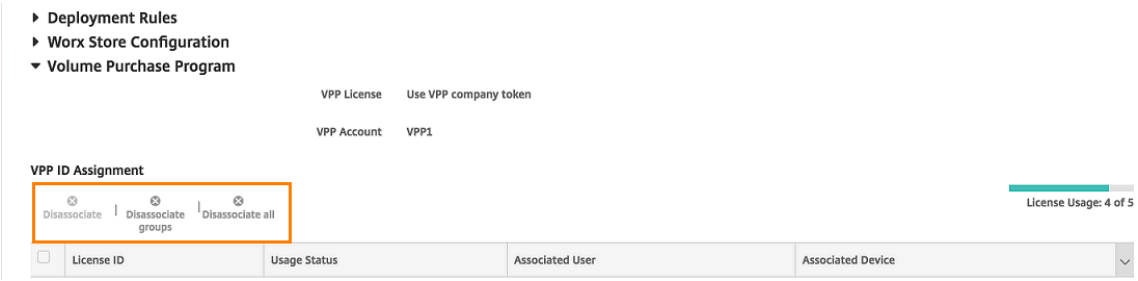
   ライセンス割り当て表によって、そのアプリの利用可能な全ライセンスの中で使用中のライセンスの数が分かります。

   Android Enterprise については、ユーザーを選択して ［割り当て解除］ をクリックすると、そのユーザーへのライセンスの割り当てが終了し、別のユーザー向けにライセンスを空けることができます。ただし、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。

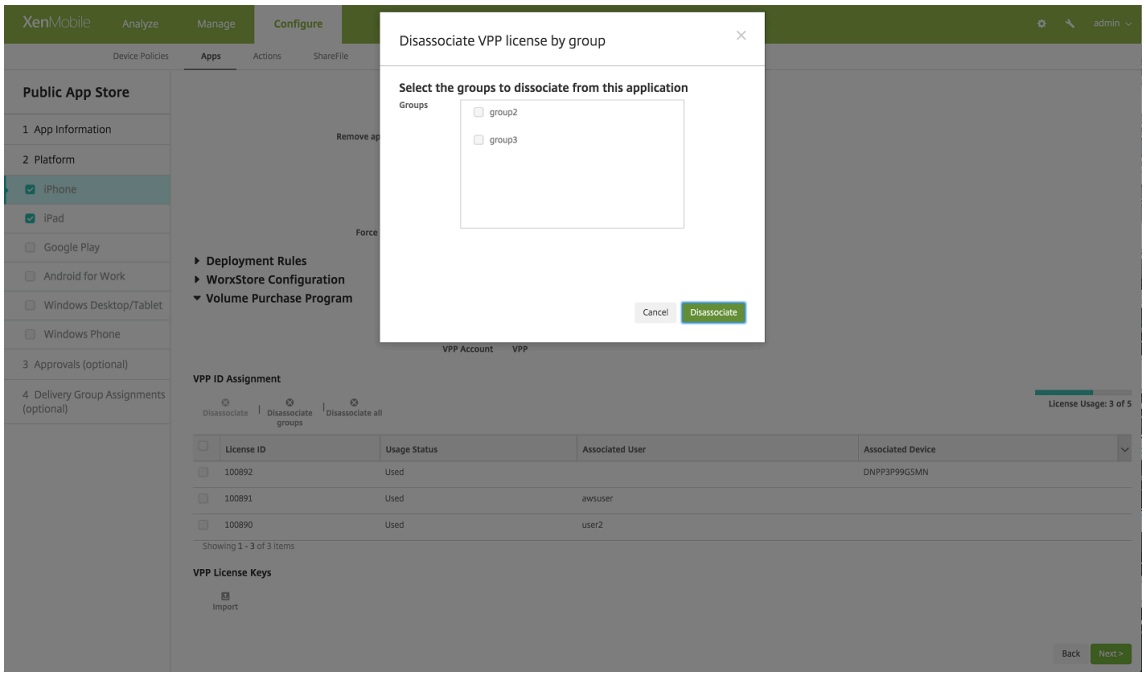


   Android Enterprise については、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。

   iOS については、個人ユーザー、ユーザーグループ、または割り当て全体の Volume Purchase Program ライセンスを解除することができます。それによってライセンスの割り当てが終了し、ライセンスを空けることができます。



［グループの割り当て解除］ をクリックすると、グループを選択するダイアログボックスが開きます。



3. ［**Volume Purchase Program**（**VPP**）］ または ［一括購入］ 設定が完了したら、［次へ］ をクリックします。［承認］ ページが開きます。

   ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、次の手順に進みます。

   ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します：

   - 使用するワークフロー： 一覧から既存のワークフローを選択するか、［新しいワークフローの作成］ をクリックします。デフォルトは ［なし］ です。
   - ［新しいワークフローの作成］ を選択した場合は、次の設定を構成します：
     - 名前： ワークフローの固有の名前を入力します。
     - 説明： 任意で、ワークフローの説明を入力します。
     - メール承認テンプレート： 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
     - マネージャー承認のレベル： 一覧から、このワークフローで必要なマネージャー承認のレベル数を

選択します。デフォルトは ［**1** つのレベル］ です。選択できるオプションは以下のとおりです:

* 不必要
* 1 つのレベル
* 2 つのレベル
* 3 つのレベル

– **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
– 追加の必須承認者を検索: 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
– ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
  * ［選択した追加の必須承認者］ の一覧からユーザーを削除するには、次のいずれかを行います:
  * ［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
  * 名前の全体または一部を検索ボックスに入力して ［検索］ をクリックし、検索結果を絞り込みます。
  * ［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

4. ［次へ］ をクリックします。［デリバリーグループ割り当て］ ページが開きます。
5. ［デリバリーグループを選択］ の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。
6. ［展開スケジュール］ を展開して以下の設定を構成します:

- ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。
- ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
- ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリックします。デフォルトのオプションは、［接続するたび］ です。
- ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

> 注:
>
> このオプションは、［設定］ **>** ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
>
> 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。

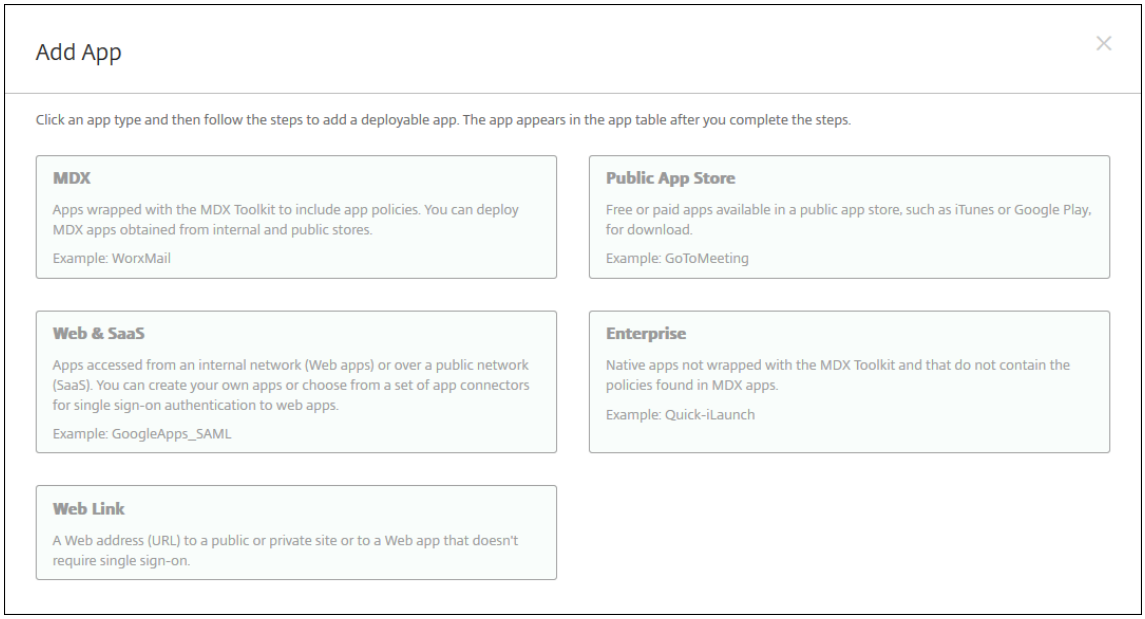
7. ［保存］ をクリックします。

Web または **SaaS** アプリの追加

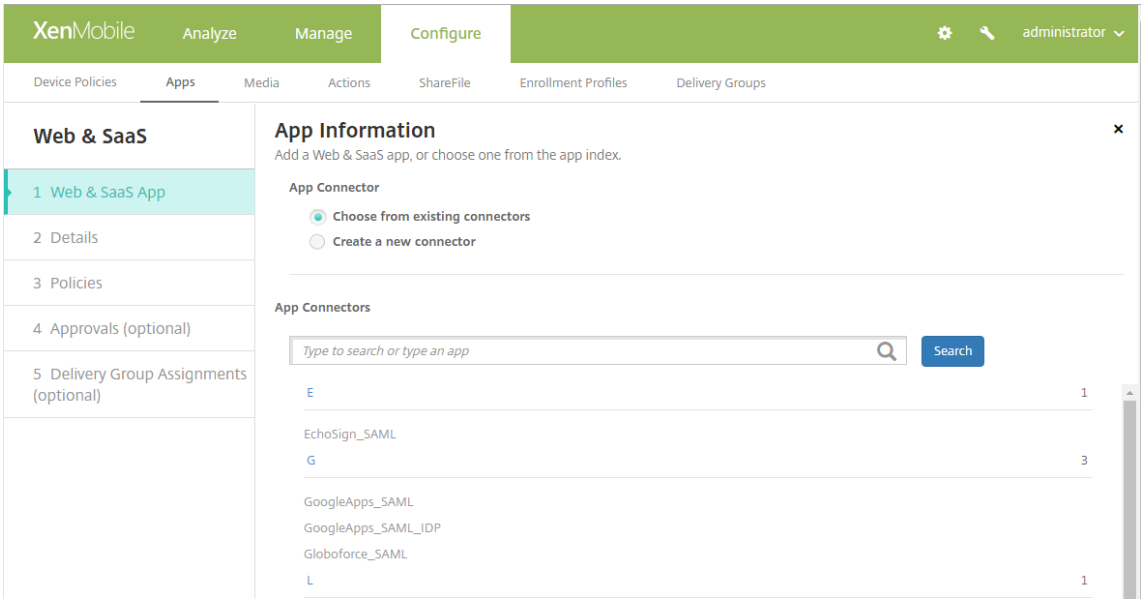
XenMobile コンソールを使用して、モバイル、エンタープライズ、Web、SaaS（Software as a Service）アプリケーションへの SSO（Single Sign-On：シングルサインオン）認証をユーザーに提供できます。アプリの SSO は、アプリケーションコネクタのテンプレートを使用して有効にできます。XenMobile で使用できるコネクタの種類の一覧については、「アプリケーションコネクタの種類」を参照してください。Web アプリまたは SaaS アプリを追加すると、XenMobile で独自のコネクタを構築することもできます。

アプリケーションが SSO のみに対応している場合に、その設定を保存すると、アプリケーションが XenMobile コンソールの ［アプリ］ タブに表示されます。

1. XenMobile コンソールで、［構成］ **>** ［アプリ］ をクリックします。［アプリ］ ページが開きます。
2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3. ［**Web** および **SaaS**］ を選択します。［アプリ情報］ ページが開きます。



4. 既存のまたは新しいアプリコネクタは、以下のように構成します。

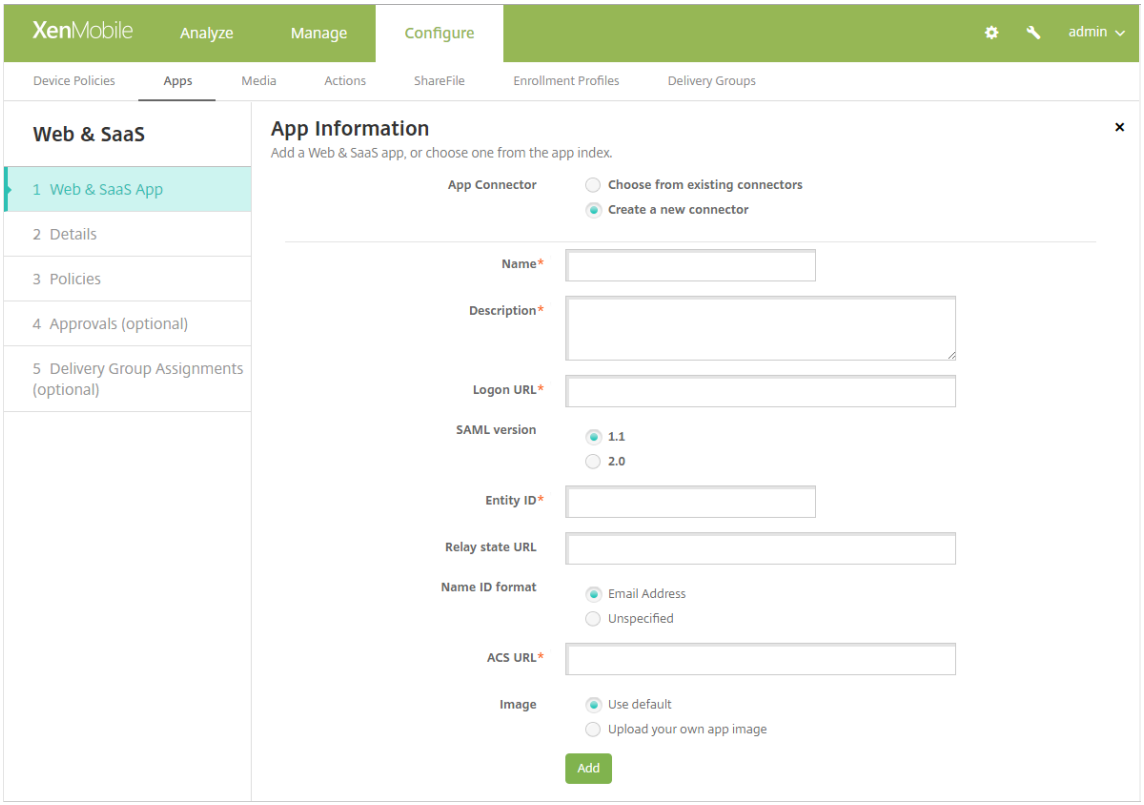
既存のアプリコネクタを構成するには

1. ［アプリ情報］ のページで、上のように ［既存のコネクタから選択します］ が既に選択されています。［アプリコネクタ］ 一覧で、使用するコネクタを選択します。アプリコネクタの情報が表示されます。
2. 次の設定を構成します。
   - アプリ名： 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
   - アプリの説明： 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
   - **URL**： 事前に入力されている URL をそのまま使用するか、アプリの Web アドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
   - ドメイン名： 該当する場合、アプリのドメイン名を入力します。
   - アプリケーションは内部ネットワークでホストされます： 内部ネットワークのサーバーでアプリを実行するかどうかを選択します。ユーザーがリモートから内部アプリに接続する場合は、NetScaler Gateway を介して接続する必要があります。このオプションを［オン］に設定すると、VPN キーワードがアプリに追加され、NetScaler Gateway を介して接続できるようになります。デフォルトは ［オフ］ です。
   - アプリカテゴリ： 一覧から、アプリに適用する任意のカテゴリを選択します。
   - ユーザーアカウントのプロビジョニング： アプリケーションのユーザーアカウントを作成するかどうかを選択します。Globalforce_SAML コネクタを使用している場合は、このオプションを有効にして、シームレスな SSO 統合が行われるようにする必要があります。
   - ［ユーザーアカウントのプロビジョニング］ を有効にした場合は、次の設定を構成します：
     - サービスアカウント

        * ユーザー名: アプリ管理者の名前を入力します。このフィールドは必須です。
        * パスワード: アプリ管理者のパスワードを入力します。このフィールドは必須です。
    - ユーザーアカウント
        * ユーザー権利の終了時: 一覧から、ユーザーがアプリへのアクセスを許可されなくなった場合に実行するアクションを選択します。デフォルトは ［アカウントの無効化］ です。
    - ユーザー名規則
        * 追加するユーザー名の規則ごとに、以下の操作を行います:
            - ユーザー属性: 一覧から、規則に追加するユーザー属性を選択します。
            - 長さ（文字）: 一覧から、ユーザー名の規則で使用するユーザー属性の文字数を選択します。デフォルトは ［すべて］ です。
            - 規則: 追加した各ユーザー属性が、ユーザー名の規則に自動的に追加されます。
- パスワード要件
    - 長さ: ユーザーパスワードの最小文字数を入力します。デフォルトは **8** です。
- パスワードの有効期限
    - 有効期間（日）: パスワードの有効期間（日数）を入力します。有効な値は **0** ～ **90** です。デフォルトは 90 です。
    - 有効期限が切れた後にパスワードを自動的にリセット: 有効期限が切れたときにパスワードを自動的にリセットするかどうかを選択します。デフォルトは ［オフ］ です。このフィールドを有効にしないと、ユーザーパスワードの有効期限が切れたときにアプリを開くことができなくなります。

新しいアプリコネクタを構成するには

1. ［アプリ情報］ のページで、［新しいコネクタの作成］ を選択します。アプリコネクタのフィールドが表示されます。

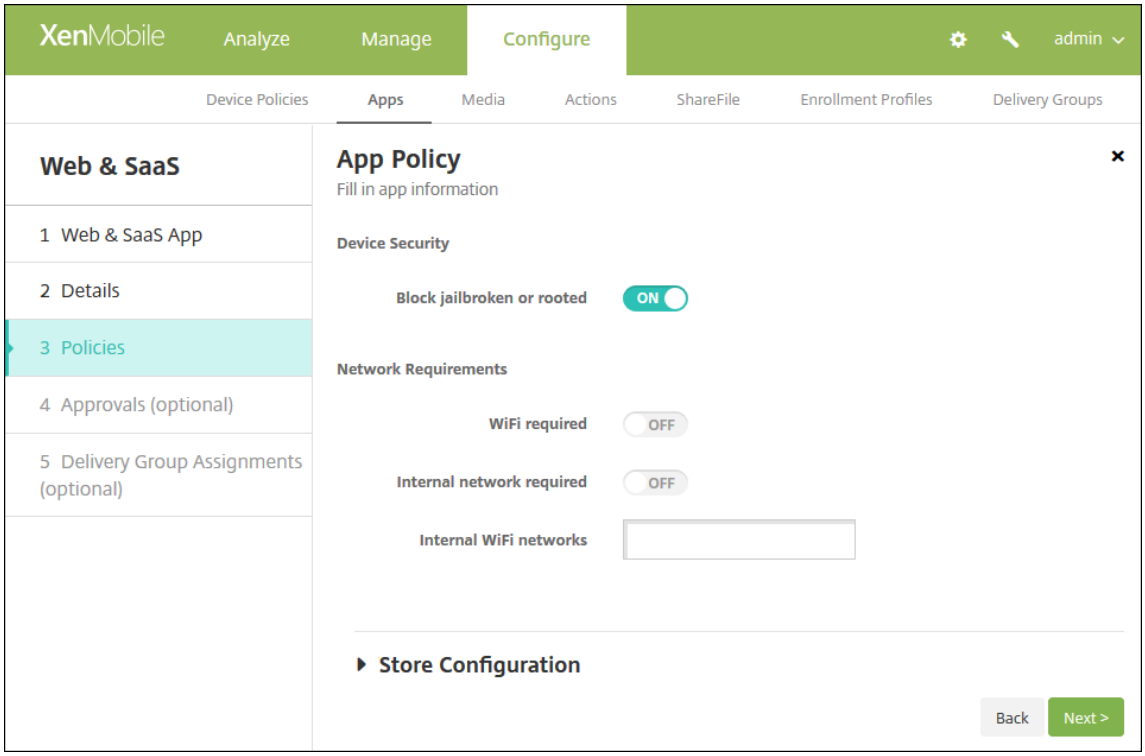


2. 次の設定を構成します。

- 名前： コネクタの名前を入力します。このフィールドは必須です。
- 説明： コネクタの説明を入力します。このフィールドは必須です。
- ログオン **URL**： ユーザーがサイトにログオンするときに使用する URL を入力するか、コピーして貼り付けます。たとえば、追加するアプリにログオンページがある場合、Web ブラウザーを開いてアプリのログオンページに移動します。「`https://www.example.com/logon`」などです。このフィールドは必須です。
- **SAML** のバージョン： ［**1.1**］ または ［**2.0**］ を選択します。デフォルトは ［**1.1**］ です。
- エンティティ **ID**： SAML アプリの ID を入力します。
- リレー状態 **URL**： SAML アプリの Web アドレスを入力します。リレーステート URL はアプリからの応答 URL です。
- 名前 **ID** 形式： ［メールアドレス］ または ［未指定］ を選択します。デフォルトは ［メールアドレス］ です。
- **ACS URL**： ID プロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービス URL（ACS URL）を入力します。ACS URL では、ユーザーがシングルサインオン機能を使用できます。
- イメージ： デフォルトの Citrix イメージを使用するのか、独自のアプリイメージをアップロードするのかを選択します。デフォルトは［デフォルトを使用］です。
  - 独自のイメージをアップロードする場合は、［参照］ をクリックしてアップロードするファイルの場所に移動します。そのファイルは、.PNG ファイルである必要があります。JPEG ファイルや GIF ファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフ

ィックを変更することはできません。

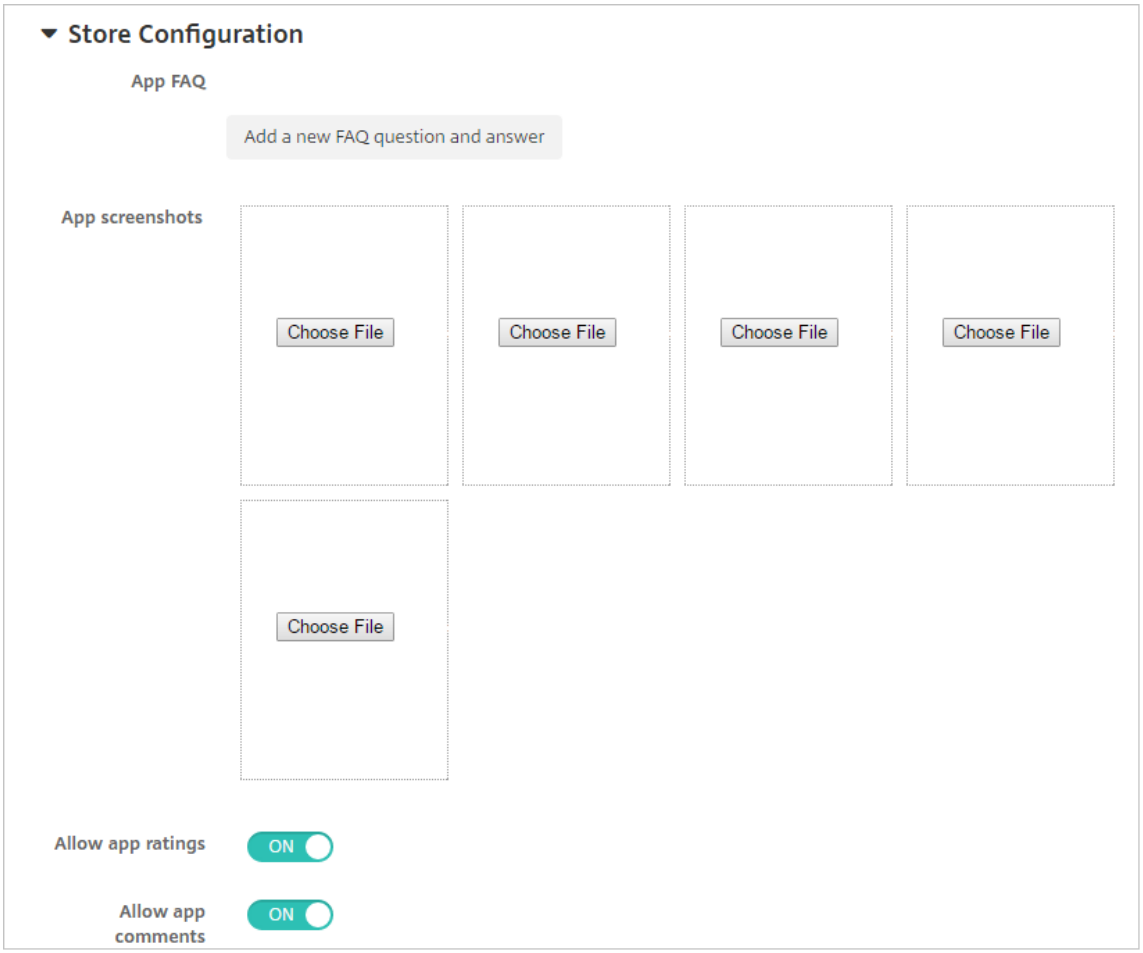
3. 完了したら、［追加］をクリックします。［詳細］ のページが開きます。
4. ［次へ］ をクリックします。［アプリのポリシー］ ページが開きます。



5. 次の設定を構成します。

- デバイスのセキュリティ
- ジェイルブレイクまたは **Root** 化をブロックします: ジェイルブレイク済みまたはルート化済みのデバイスによるアプリへのアクセスをブロックするかどうかを選択します。デフォルトは ［オン］ です。
- ネットワーク要件
- **WiFi** が必要です: アプリの実行に WiFi 接続が必要であるかどうかを選択します。デフォルトは ［オフ］ です。
- 内部ネットワークが必要です: アプリの実行に内部ネットワークが必要であるかどうかを選択します。デフォルトは ［オフ］ です。
- 内部 **WiFi** ネットワーク: ［WiFi が必要です］を有効にした場合は、使用する内部 WiFi ネットワークを入力します。

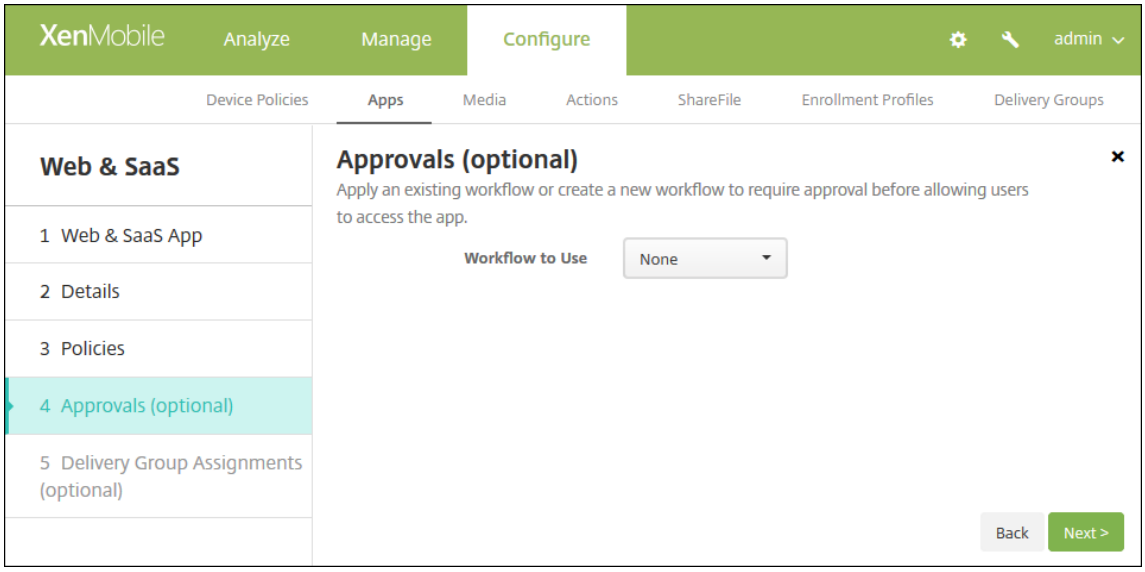
6. ［ストア構成］ を展開します。



任意で、アプリに関する FAQ や、XenMobile Store に表示される画面キャプチャを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - アプリの **FAQ**: アプリに関する FAQ の質問および回答を追加します。
  - アプリスクリーンショット: アプリを XenMobile Store で分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックは PNG である必要があります。GIF イメージや JPEG イメージはアップロードできません。
  - アプリ評価を許可: ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは［オン］です。
  - アプリコメントを許可: 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは［オン］です。

7. ［次へ］をクリックします。［承認］ページが開きます。



ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順 8 に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します:

- 使用するワークフロー: 一覧から既存のワークフローを選択するか、［新しいワークフローの作成］ をクリックします。デフォルトは ［なし］ です。
- ［新しいワークフローの作成］ を選択した場合は、次の設定を構成します:
  - 名前: ワークフローの固有の名前を入力します。
  - 説明: 任意で、ワークフローの説明を入力します。
  - メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
- マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは ［**1** つのレベル］ です。選択できるオプションは以下のとおりです:
  - 不必要
  - 1 つのレベル
  - 2 つのレベル
  - 3 つのレベル
- **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
- 追加の必須承認者を検索: 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
  - ［選択した追加の必須承認者］ の一覧からユーザーを削除するには、次のいずれかを行います:
    * ［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。

* 名前の全体または一部を検索ボックスに入力して ［検索］ をクリックし、検索結果を絞り込みます。
* ［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

8. ［次へ］ をクリックします。［デリバリーグループ割り当て］ ページが開きます。
9. ［デリバリーグループを選択］ の横に、デリバリーグループを入力して検索するか、1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。
10. ［展開スケジュール］ を展開して以下の設定を構成します:
    - ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。
    - ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
    - ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    - ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリックします。デフォルトのオプションは、［接続するたび］ です。
    - ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

    > 注:
    >
    > このオプションは、［設定］ > ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
    >
    > 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。
11. ［保存］ をクリックします。

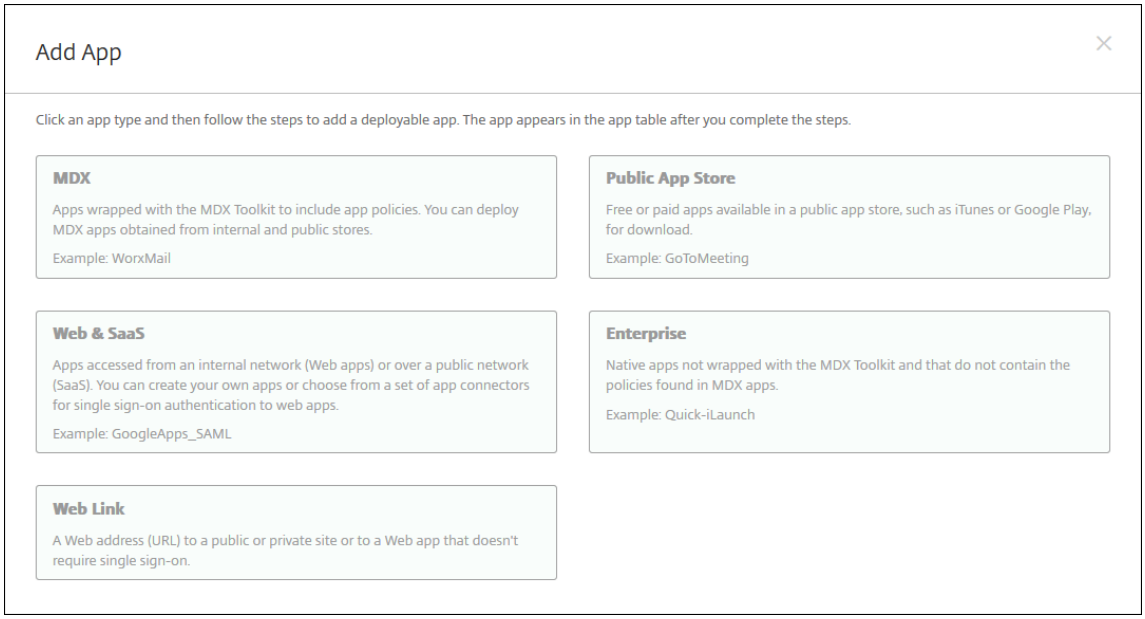
エンタープライズアプリの追加

XenMobile のエンタープライズアプリとは、MDX Toolkit でラップされておらず、MDX アプリに関連付けられたポリシーを含んでいない、ネイティブアプリを意味します。エンタープライズアプリのアップロードは、XenMobile コンソールの ［アプリ］ タブで行うことができます。エンタープライズアプリは、以下のプラットフォーム（および対応するファイルの種類）をサポートします:

- iOS（.ipa ファイル）
- Android（.apk ファイル）
- Samsung KNOX（.apk ファイル）
- Android Enterprise（.apk ファイル）

> 注：
>
> Google Play ストアからダウンロードしたアプリをエンタープライズアプリとして追加することはサポートされていません。代わりに、パブリックアプリストアのアプリとして Google Play ストアから入手したアプリを追加します。パブリックアプリストアのアプリの追加を参照してください。

1. XenMobile コンソールで、［構成］ > ［アプリ］ をクリックします。［アプリ］ ページが開きます。
2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3. ［エンタープライズ］ をクリックします。［アプリ情報］ ページが開きます。
4. ［アプリ情報］ ペインで、以下の情報を入力します：
   - 名前： アプリの説明的な名前を入力します。この名前は、［アプリ］ の表の［アプリ名］ の下に表示されます。
   - 説明： 任意で、アプリの説明を入力します。
   - アプリカテゴリ： 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリカテゴリについて詳しくは、「アプリカテゴリの作成」を参照してください。
5. ［次へ］ をクリックします。アプリのプラットフォームページが開きます。
6. ［プラットフォーム］ で、追加するプラットフォームをオンにします。1 つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

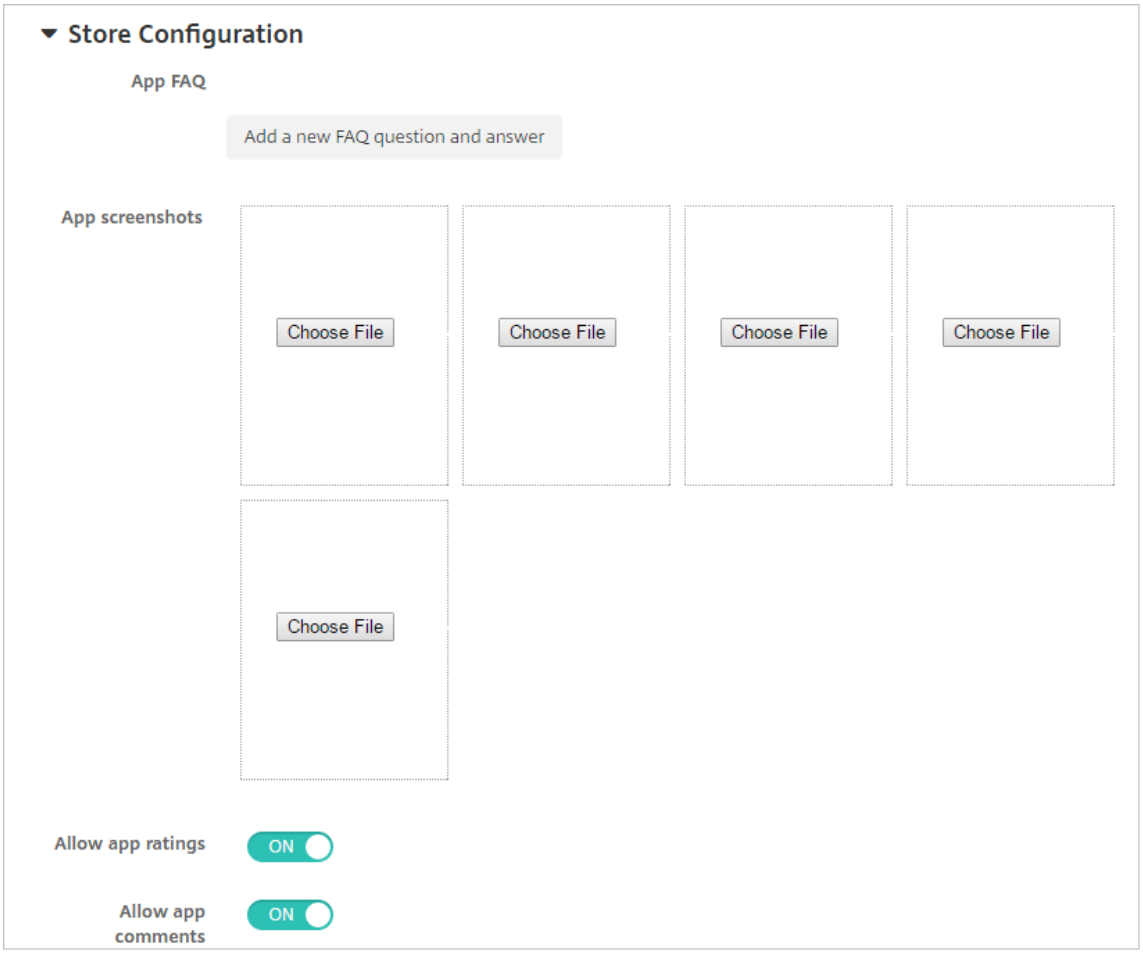
   1 つのプラットフォームの設定の構成が完了したら、手順 10 を参照してプラットフォームの展開規則を設定します。
7. 選択したプラットフォームごとに、［参照］ をクリックしてアップロードするファイルの場所に移動し、そのファイルを選択します。
8. ［次へ］ をクリックします。プラットフォームのアプリ情報ページが開きます。

9. プラットフォームの種類について、以下の設定を構成します:

   - ファイル名: 任意で、アプリの名前を新たに入力します。
   - アプリの説明: 任意で、アプリの説明を新たに入力します。
   - アプリのバージョン: このフィールドは変更できません。
   - 最小 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
   - 最大 **OS** バージョン: 任意で、アプリを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
   - 除外するデバイス: 任意で、アプリを実行できないデバイスの製造元またはモデルを入力します。
   - **MDM** プロファイルが削除されたらアプリを削除します: MDM プロファイルが削除された場合にデバイスからアプリを削除するかどうかを選択します。デフォルトは [オン] です。
   - アプリデータのバックアップを阻止します: アプリのデータをバックアップできないようにするかどうかを選択します。デフォルトは [オン] です。
   - 管理されるアプリ: 非管理対象のアプリをインストールして、監視対象デバイスのユーザーにアプリの管理を許可するよう求める場合は、[オン] を選択します。この設定は、iOS 9.x デバイスに適用されます。

10. 展開規則を構成します。詳しくは、「リソースの展開」を参照してください。

11. [**XenMobile Store** 構成] を展開します。



任意で、アプリに関する FAQ や、XenMobile Store に表示される画面キャプチャを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

次の設定を構成します。

- アプリの **FAQ**: アプリに関する FAQ の質問および回答を追加します。
- アプリスクリーンショット: アプリを XenMobile Store で分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックは PNG である必要があります。GIF イメージや JPEG イメージはアップロードできません。
- アプリ評価を許可: ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは ［オン］ です。
- アプリコメントを許可: 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは ［オン］ です。

12. ［次へ］ をクリックします。［承認］ ページが開きます。

ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順 13 に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します:

- 使用するワークフロー: 一覧から既存のワークフローを選択するか、［新しいワークフローの作成］ をクリックします。デフォルトは ［なし］ です。
- ［新しいワークフローの作成］ を選択した場合は、次の設定を構成します:
  - 名前: ワークフローの固有の名前を入力します。
  - 説明: 任意で、ワークフローの説明を入力します。
  - メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは ［**1** つのレベル］ です。選択できるオプションは以下のとおりです:
    * 不必要
    * 1 つのレベル
    * 2 つのレベル
    * 3 つのレベル
  - **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
  - 追加の必須承認者を検索: 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
    * ［選択した追加の必須承認者］ の一覧からユーザーを削除するには、次のいずれかを行います:
      ・［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      ・ 名前の全体または一部を検索ボックスに入力して ［検索］ をクリックし、検索結果を絞り込みます。
      ・［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

13. ［次へ］ をクリックします。［デリバリーグループ割り当て］ ページが開きます。
14. ［デリバリーグループを選択］ の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。
15. ［展開スケジュール］ を展開して以下の設定を構成します:

- ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。
- ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
- ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリッ

クします。デフォルトのオプションは、［接続するたび］ です。

- ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

> 注:
>
> このオプションは、［設定］ **>** ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
>
> 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。

16. ［保存］ をクリックします。

Web リンクの追加

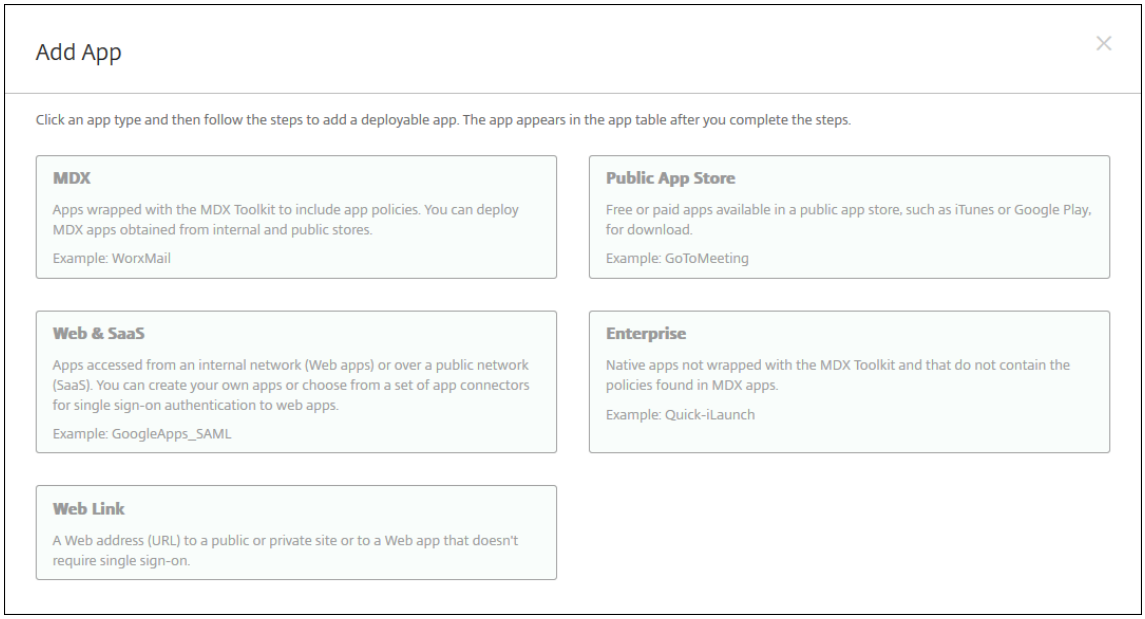
XenMobile で、パブリックサイトやプライベートサイト、またはシングルサインオン（SSO）を必要としない Web アプリの Web アドレス（URL）を設置できます。

Web リンクの構成は、XenMobile コンソールの ［アプリ］ タブで行うことができます。Web リンクの構成が完了すると、リンクは ［アプリ］ の表にある一覧にリンクアイコンとして表示されます。ユーザーが Secure Hub を使ってログオンすると、リンクは使用可能なアプリおよびデスクトップの一覧と共に表示されます。

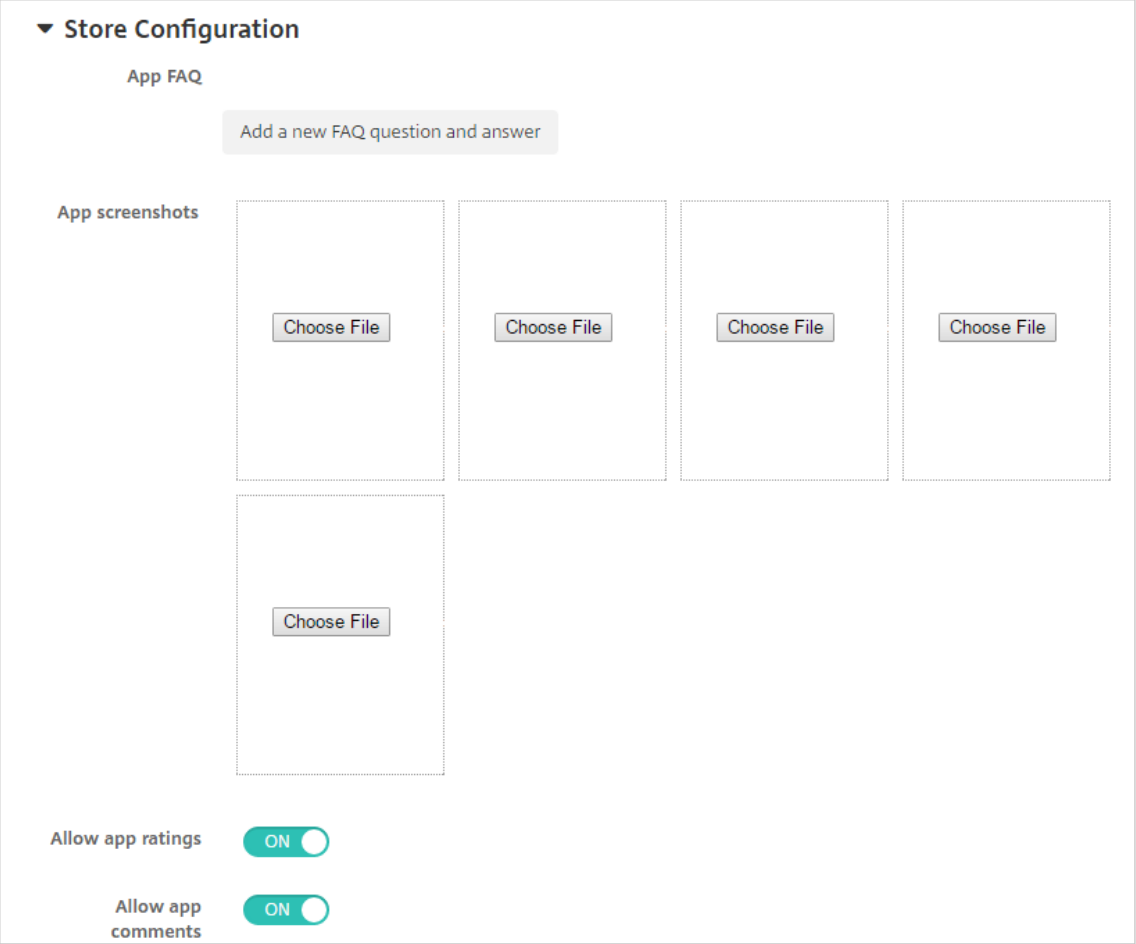
リンクを追加するには、次の情報を指定します:

- リンクの名前
- リンクの説明
- Web アドレス（URL）
- カテゴリ
- 役割
- .png 形式の画像（オプション）

1. XenMobile コンソールで、［構成］ **>** ［アプリ］ をクリックします。［アプリ］ ページが開きます。
2. ［追加］ をクリックします。［アプリの追加］ ダイアログボックスが開きます。



3. [**Web** リンク] をクリックします。[アプリ情報] ページが開きます。
4. 次の設定を構成します。
   - アプリ名: 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
   - アプリの説明: 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
   - **URL**: 事前に入力されている URL をそのまま使用するか、アプリの Web アドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
   - アプリは内部ネットワークでホストされます: 内部ネットワークのサーバーでアプリを実行するかどうかを選択します。ユーザーがリモートから内部アプリに接続する場合は、NetScaler Gateway を介して接続する必要があります。このオプションを [オン] に設定すると、VPN キーワードがアプリに追加され、NetScaler Gateway を介して接続できるようになります。デフォルトは [オフ] です。
   - アプリカテゴリ: 一覧から、アプリに適用する任意のカテゴリを選択します。
   - イメージ: デフォルトの Citrix イメージを使用するのか、独自のアプリイメージをアップロードするのかを選択します。デフォルトは [デフォルトを使用] です。
     - 独自のイメージをアップロードする場合は、[参照] をクリックしてアップロードするファイルの場所に移動します。そのファイルは、.PNG ファイルである必要があります。JPEG ファイルや GIF ファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。
5. [**XenMobile Store** 構成] を展開します。



任意で、アプリに関する FAQ や、XenMobile Store に表示される画面キャプチャを追加できます。また、ユーザーにアプリの評価やアプリについてのコメントを許可するかどうかも設定できます。

次の設定を構成します。

- アプリの **FAQ**: アプリに関する FAQ の質問および回答を追加します。
- アプリスクリーンショット: アプリを XenMobile Store で分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックは PNG である必要があります。GIF イメージや JPEG イメージはアップロードできません。
- アプリ評価を許可: ユーザーにアプリの評価を許可するかどうかを選択します。デフォルトは ［オン］ です。
- アプリコメントを許可: 選択したアプリについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは ［オン］ です。

6. ［次へ］ をクリックします。［デリバリーグループ割り当て］ ページが開きます。
7. ［デリバリーグループを選択］ の横にデリバリーグループを入力して検索するか、一覧で 1 つまたは複数のグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。

8. [展開スケジュール] を展開して以下の設定を構成します:
   - [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。
   - [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
   - [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
   - [展開状態] の横の [接続するたび] をクリックするか、[以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、[接続するたび] です。
   - [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

   > 注:
   >
   > このオプションは、[設定] > [サーバープロパティ] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。
   >
   > 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、[常時接続に対する展開] は適用されません。

9. [保存] をクリックします。

Microsoft 365 アプリの有効化

MDX コンテナを開いて、Secure Mail、Secure Web、および ShareFile が Microsoft Office 365 アプリにドキュメントやデータを転送するようにできます。詳しくは、「Office 365 アプリとのセキュアな対話式操作の許可」を参照してください。

ワークフローの作成および管理

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

XenMobile を初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

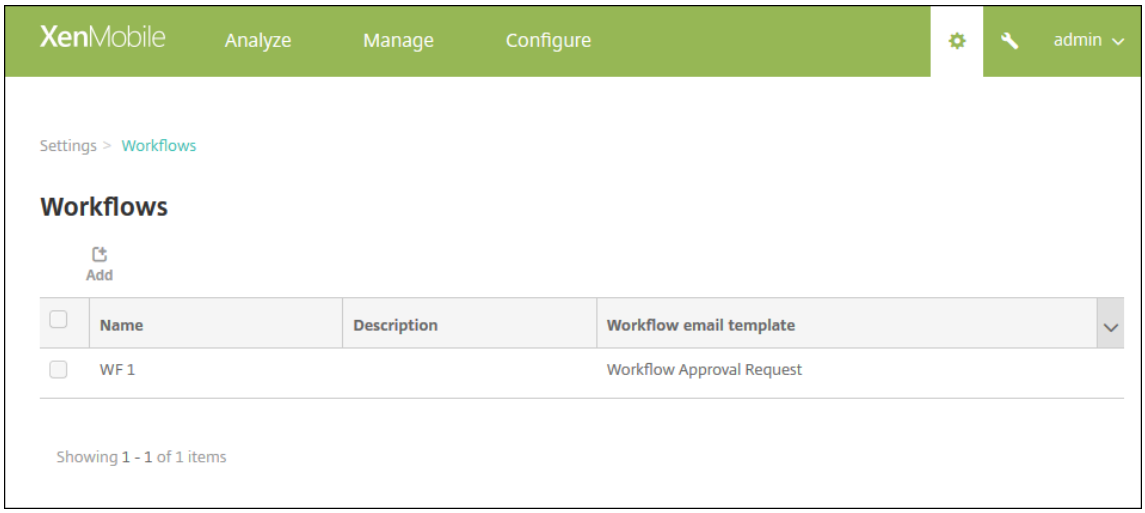
XenMobile の次の 2 つの方法でワークフローを構成できます:

- XenMobile コンソールの [ワークフロー] ページ。[ワークフロー] ページでは、アプリの構成で使用する複数のワークフローを構成できます。[ワークフロー] ページでワークフローを構成するとき、アプリを構成するときのワークフローを選択できます。

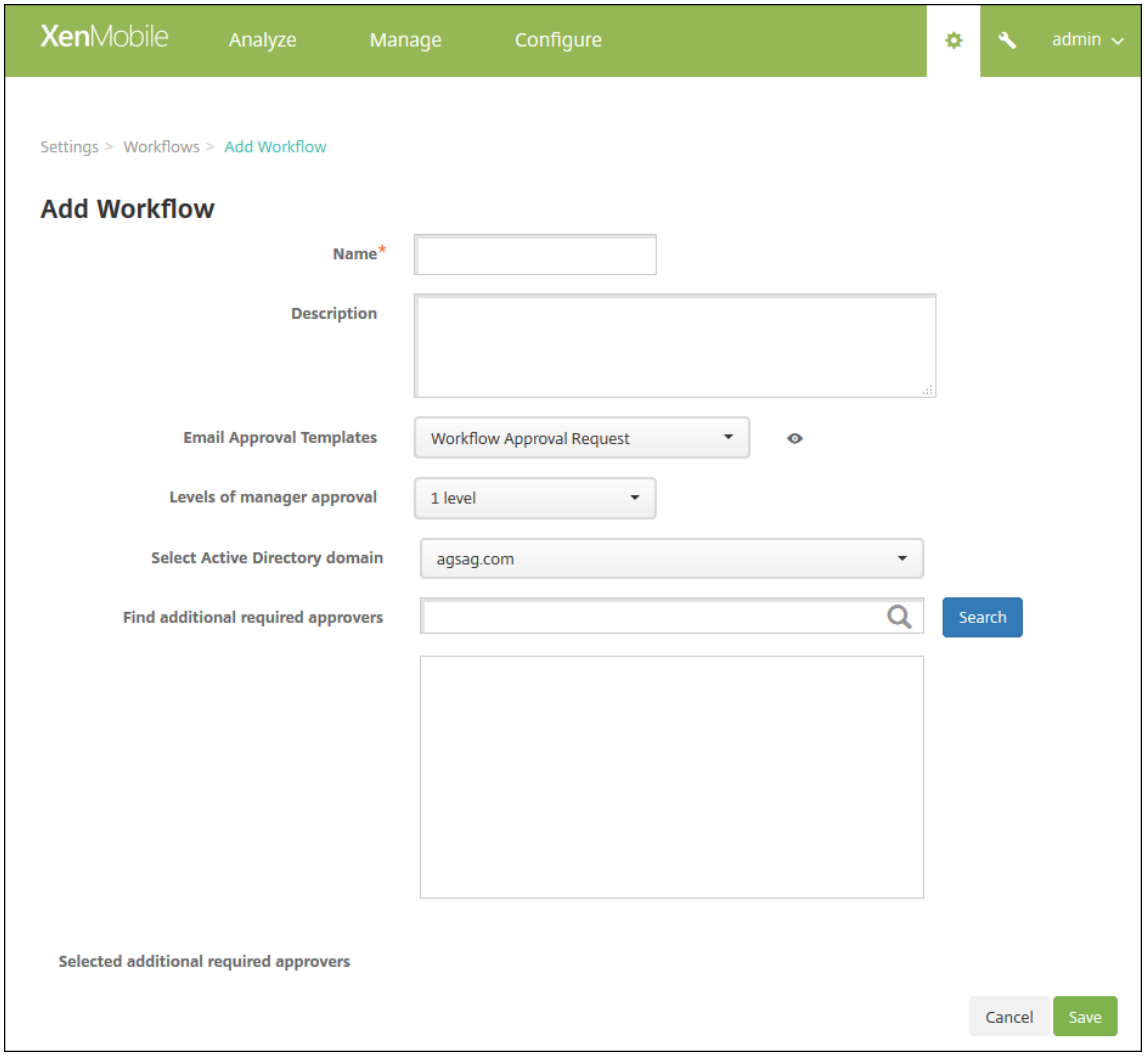
- アプリケーションコネクタを構成するとき、アプリで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。

ユーザーアカウントの管理者承認を最大 3 レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、名前またはメールアドレスでユーザーを検索し、選択することができます。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［ワークフロー］ をクリックします。［ワークフロー］ ページが開きます。

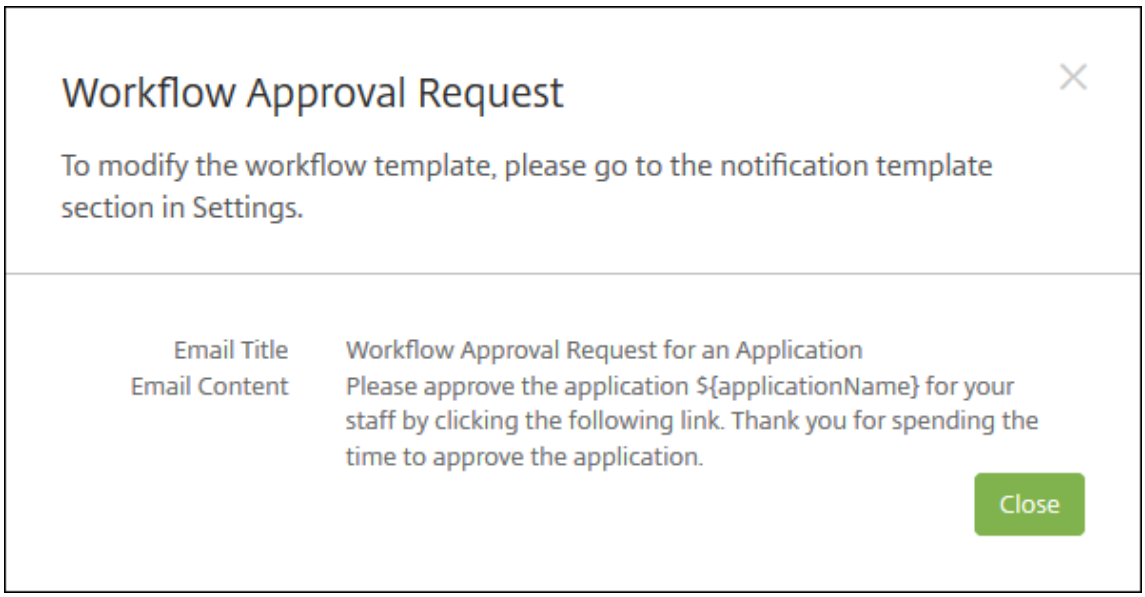


3. ［追加］ をクリックします。［ワークフローの追加］ ページが開きます。



4. 次の設定を構成します。

   - 名前: ワークフローの固有の名前を入力します。
   - 説明: 任意で、ワークフローの説明を入力します。
   - メール承認テンプレート: 一覧から、割り当てる電子メール承認テンプレートを選択します。電子メールテンプレートの作成は、XenMobile コンソールの［設定］の［通知テンプレート］セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、以下のダイアログボックスが表示されます。



- マネージャー承認のレベル: 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［1 つのレベル］です。選択できるオプションは以下のとおりです:
  - 不必要
  - 1 つのレベル
  - 2 つのレベル
  - 3 つのレベル
- **Active Directory** ドメインの選択: 一覧から、ワークフローで使用する適切な Active Directory ドメインを選択します。
- 追加の必須承認者を検索: 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］ をクリックします。名前は Active Directory で取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが ［選択した追加の必須承認者］ の一覧に表示されます。
- ［選択した追加の必須承認者］ の一覧からユーザーを削除するには、次のいずれかを行います:
  - ［検索］ をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
  - 名前の全体または一部を検索ボックスに入力して［検索］をクリックし、検索結果を絞り込みます。
  - ［選択した追加の必須承認者］ の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

5. ［保存］ をクリックします。作成したワークフローが ［ワークフロー］ ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリを表示したり、ワークフローを削除したりできます。ワークフローを作成した後でワークフローを編集することはできません。承認レベルまたは承認者が異なるワークフローが必要な場合は、別のワークフローを作成する必要があります。

ワークフローの詳細の表示および削除を行うには

1. ［ワークフロー］ ページで、表の行をクリックするかワークフローの横にあるチェックボックスをオンにして、ワークフローを選択します。
2. ワークフローを削除するには、［削除］ をクリックします。確認ダイアログボックスが開きます。もう一度［削除］ をクリックします。

> 重要:
>
> この操作を元に戻すことはできません。

アプリストアおよび **Citrix Secure Hub** のブランド設定

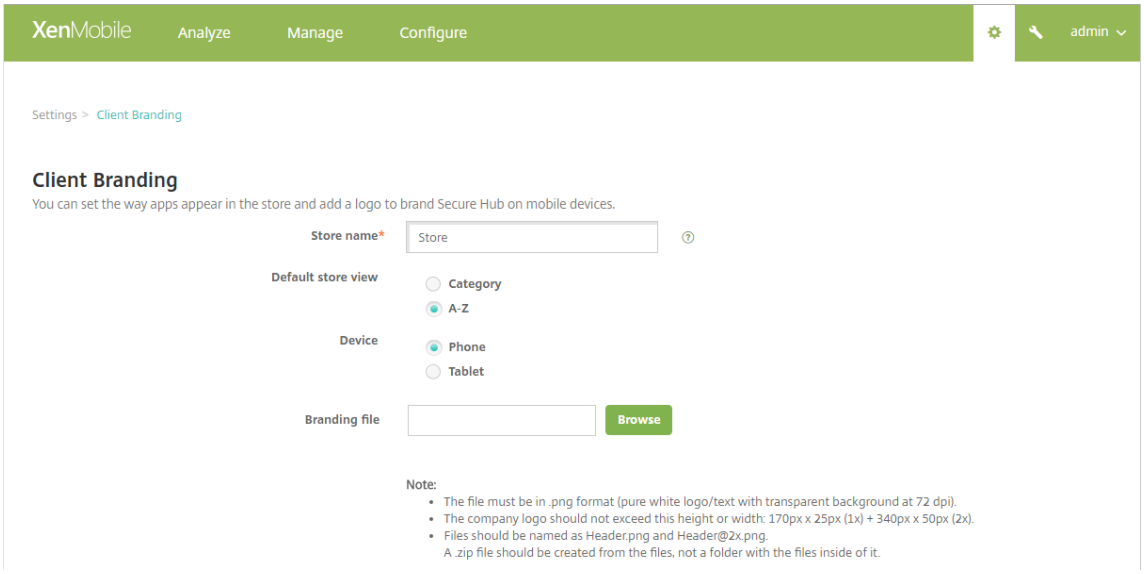
ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、Secure Hub およびアプリストアをブランド化することができます。このブランド設定機能は、iOS および Android デバイスでのみ利用できます。

> 注:
>
> 始める前に、カスタム画像を準備してアクセスできるようにしてください。

カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png 形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および 340px×50px（2x）を超過しないようにする必要があります。
- ファイルの名前は Header.png および Header@2x.png にします。
- ファイルを含むフォルダーではなく、ファイルから.zip ファイルを作成します。

1. XenMobile Server コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［クライアント］ で ［クライアントブランド化］ をクリックします。［クライアントブランド化］ ページが開きます。



次の設定を構成します:

- ストア名: ユーザーのアカウント情報にストア名が表示されます。この名前を変更すると、ストアサービスへのアクセスに使用される URL も変更されます。通常、デフォルトの名前をそのまま使用します。

  > 重要:
  >
  > ストア名に使用できるのは英数字のみです。

- デフォルトストアビュー: ［カテゴリ］ または ［**A** ～ **Z**］ を選択します。デフォルトは ［**A** ～ **Z**］ です。
- デバイスのオプション: ［電話］ または ［タブレット］ を選択します。デフォルトは ［電話］ です。
- ブランド化するファイル: ［参照］ をクリックしてブランド設定に使用するイメージまたはイメージの.zip ファイルの場所に移動し、ファイルを選択します。

3. ［保存］ をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、展開します。

アプリコネクタの種類

January 10, 2020

次の表に、Web アプリまたは SaaS アプリを追加する場合に XenMobile 内で使用できるコネクタとコネクタの種類を示します。Web または SaaS アプリを追加すると、新しいコネクタを追加することもできます。

この表は、各コネクタがユーザーアカウント管理をサポートするかどうかについて示します。ユーザーアカウント管理がサポートされる場合、管理者は新しいアカウントを自動的に作成したり、ワークフローを使って作成したりできます。

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
EchoSign_SAML	☒	☒
Globoforce_SAML		注： このコネクタを使用する場合は、プロビジョニングのユーザー管理を有効にして、シームレスな SSO 統合が行われるようにする必要があります。
GoogleApps_SAML	☒	☒
GoogleApps_SAML_IDP	☒	☒
Lynda_SAML	☒	☒
Office365_SAML	☒	☒
Salesforce_SAML	☒	☒
Salesforce_SAML_SP	☒	☒
SandBox_SAML	☒	
SuccessFactors_SAML	☒	
ShareFile_SAML	☒	
ShareFile_SAML_SP	☒	
WebEx_SAML_SP	☒	☒

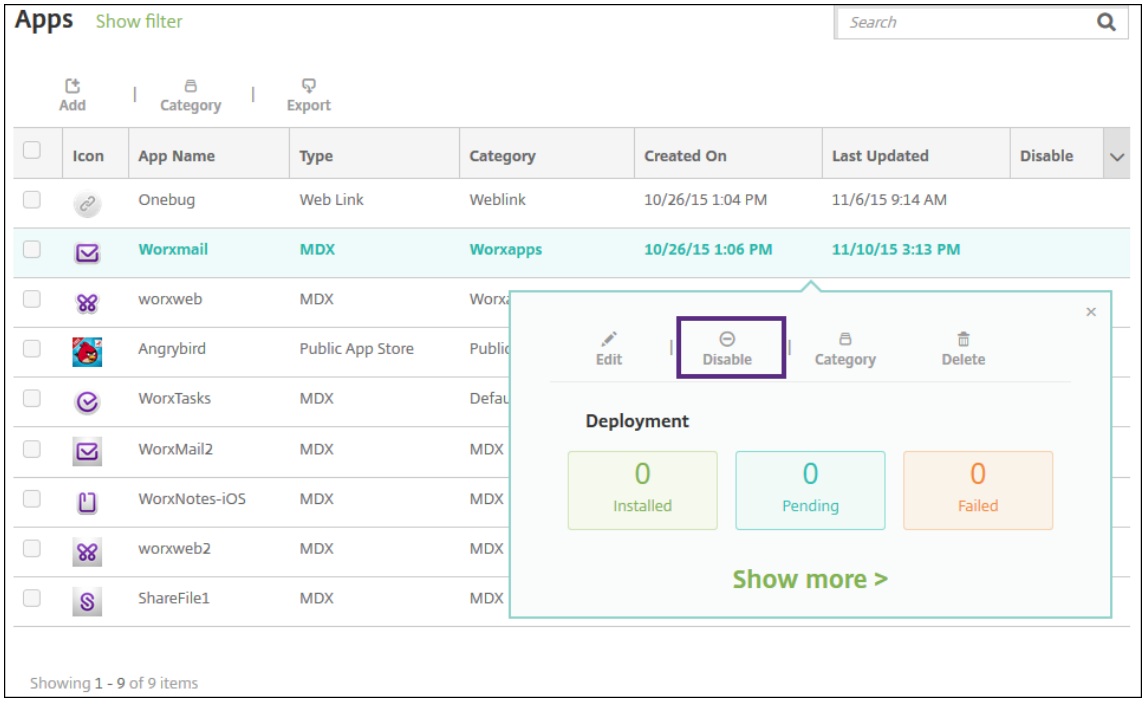
MDX またはエンタープライズアプリのアップグレード

August 22, 2019

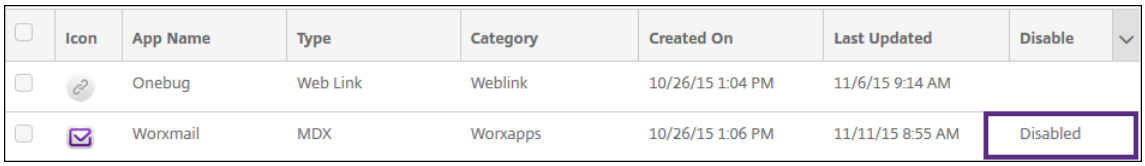
XenMobile で MDX またはエンタープライズアプリケーションをアップグレードするには、XenMobile コンソールでアプリケーションを無効にしてから、アプリケーションの新しいバージョンをアップロードします。

1. XenMobile コンソールで、［構成］**>**［アプリ］ をクリックします。［アプリ］ ページが開きます。
2. 管理対象デバイス（モバイルデバイス管理で XenMobile に登録されたデバイス）の場合は、スキップして手順 3 に進みます。非管理対象デバイス（エンタープライズアプリケーション管理の目的のみで XenMobile に登録されたデバイス）の場合は、次の手順に従います。
    - ［アプリ］ の表で、アプリの横のチェックボックスをオンにするか、更新するアプリを含む行をクリックします。

- 表示されるメニューで、［無効にする］ をクリックします。



- 確認のダイアログボックスで ［無効］ をクリックします。アプリの ［無効にする］ 列に「無効」と表示されます。



> 注:
>
> アプリを無効にすると、アプリが保守モードになります。アプリが無効になっている場合、ユーザーはログオフ後にそのアプリに再接続することはできません。アプリの無効化は任意の設定ですが、アプリの機能の問題を避けるために、アプリを無効にすることをお勧めします。ポリシーを更新する場合や、XenMobile にアプリケーションをアップロードするのと同時にユーザーがダウンロードを要求する場合などに問題が発生することがあります。

3. ［アプリ］ の表で、アプリの横のチェックボックスをオンにするか、更新するアプリを含む行をクリックします。
4. 表示されるメニューで、［編集］ をクリックします。アプリに対して最初に選択したプラットフォームが選択された状態で、［アプリ情報］ ページが開きます。
5. 次の設定を構成します。

- 名前: 任意で、アプリ名を変更します。
- 説明: 任意で、アプリの説明を変更します。
- アプリカテゴリ: 任意で、アプリのカテゴリを変更します。

6. ［次へ］ をクリックします。最初に選択したプラットフォームのページが開きます。選択したプラットフォームごとに、以下の操作を行います。
   - ［アップロード］ をクリックしてアップロードするファイルの場所に移動し、置き換えるファイルを選択します。アプリケーションが XenMobile にアップロードされます。
   - 任意で、プラットフォームのアプリの詳細とポリシー設定を変更します。
   - 任意で、展開規則の構成および XenMobile Store の構成を行います。詳しくは、「アプリの追加」の「MDX アプリの追加」を参照してください。
7. ［保存］ をクリックします。［アプリ］ ページが開きます。
8. 手順 2 でアプリを無効にした場合は、次の手順に従います。
   - ［アプリ］ の表で更新したアプリをクリックして選択し、表示されるメニューで ［有効にする］ をクリックします。
   - 確認ダイアログボックスが表示されたら、［有効にする］ をクリックします。これで、ユーザーがアプリにアクセスでき、アプリのアップグレードを求める通知を受信できるようになりました。

MDX アプリケーションポリシーの概要

October 15, 2018

制限事項と Citrix の推奨事項が注に記載された、iOS と Android の MDX アプリケーションポリシーの一覧については、MDX Toolkit のドキュメントの「MDX アプリケーションポリシーの概要」を参照してください。

XenMobile Store および Citrix Secure Hub のブランド設定

August 22, 2019

ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、Secure Hub および XenMobile Store をブランド化することができます。このブランド設定機能は、iOS および Android デバイスでのみ利用できます。

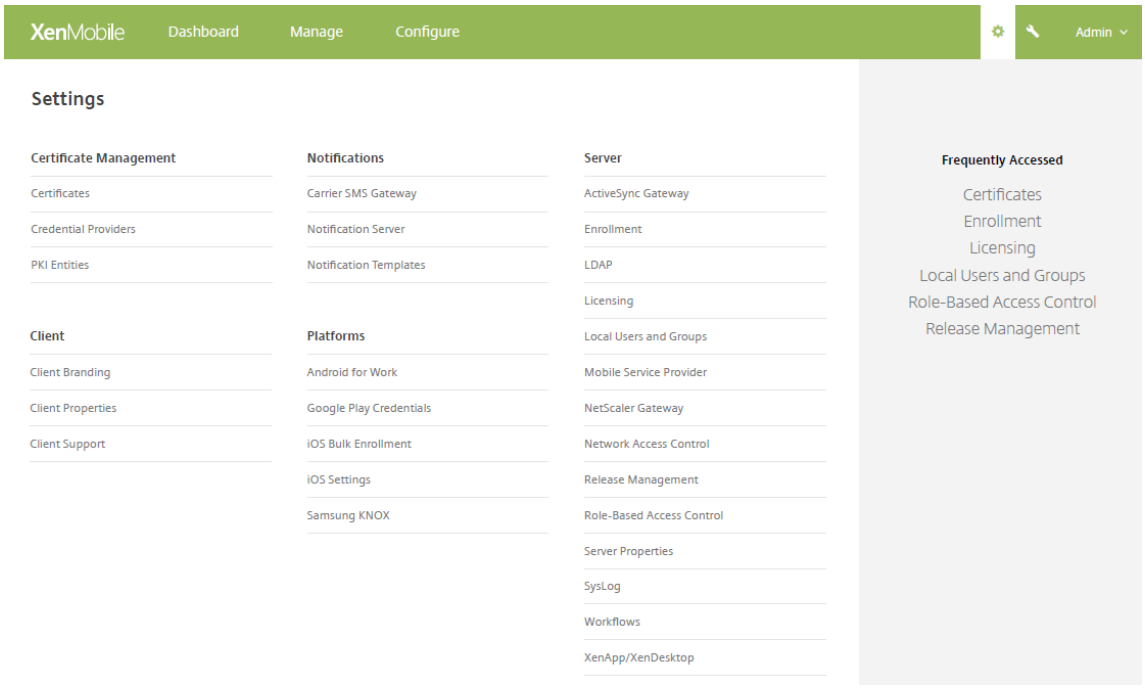
> 注:
>
> 始める前に、カスタム画像を準備してアクセスできるようにしてください。

カスタムイメージは、以下の要件を満たす必要があります。

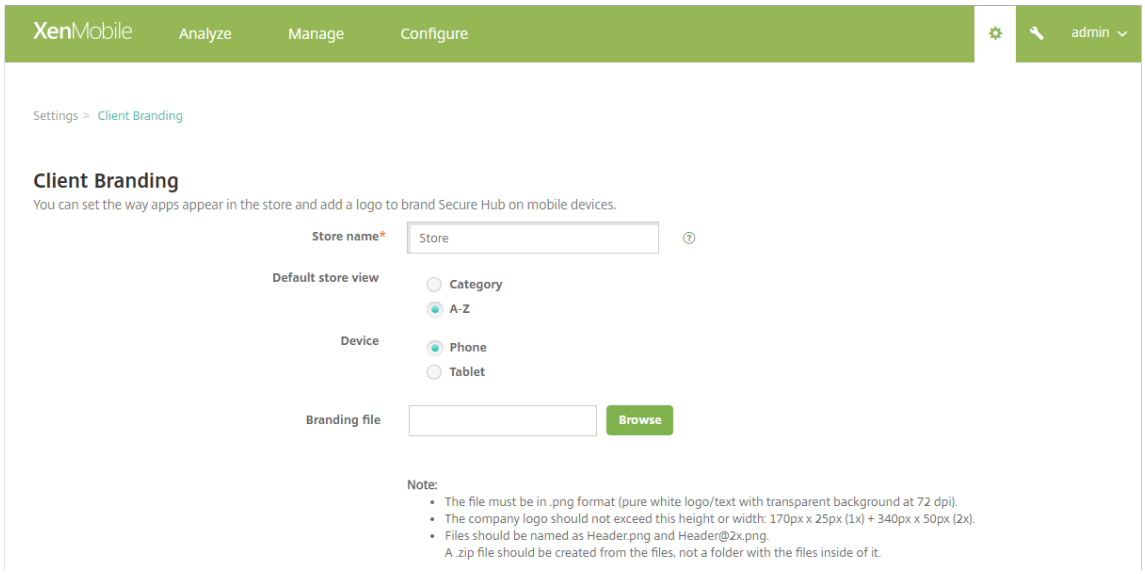
- ファイルは.png 形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および 340px×50px（2x）を超過しないようにする必要があります。

- ファイルの名前は Header.png および Header@2x.png にします。
- ファイルを含むフォルダーではなく、ファイルから.zip ファイルを作成します。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。



2. ［クライアント］ で ［クライアントブランド化］ をクリックします。［クライアントブランド化］ ページが開きます。



次の設定を構成します：

- ストア名： ユーザーのアカウント情報に含まれるストア名が表示されます。この名前を変更すると、ストアサービスへのアクセスに使用される URL も変更されます。通常、デフォルトの名前をそのまま使用します。

> 重要：
>
> ストア名に使用できるのは英数字のみです。

- デフォルトストアビュー：［カテゴリ］または［**A** ～ **Z**］を選択します。デフォルトは［**A** ～ **Z**］です。
- デバイスのオプション：［電話］または［タブレット］を選択します。デフォルトは［電話］です。
- ブランド化するファイル：［参照］をクリックしてブランド設定に使用するイメージまたはイメージの.zip ファイルの場所に移動し、ファイルを選択します。

3. ［保存］をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、展開します。

Citrix Launcher

August 22, 2019

Citrix Launcher を使用すると、XenMobile によって展開された Android デバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix Launcher の Secure Hub 管理でサポートされる Android の最小バージョンは、Android 4.0.3 です。Citrix Launcher とランチャー構成デバイスポリシーは、Android Enterprise と互換性がありません。

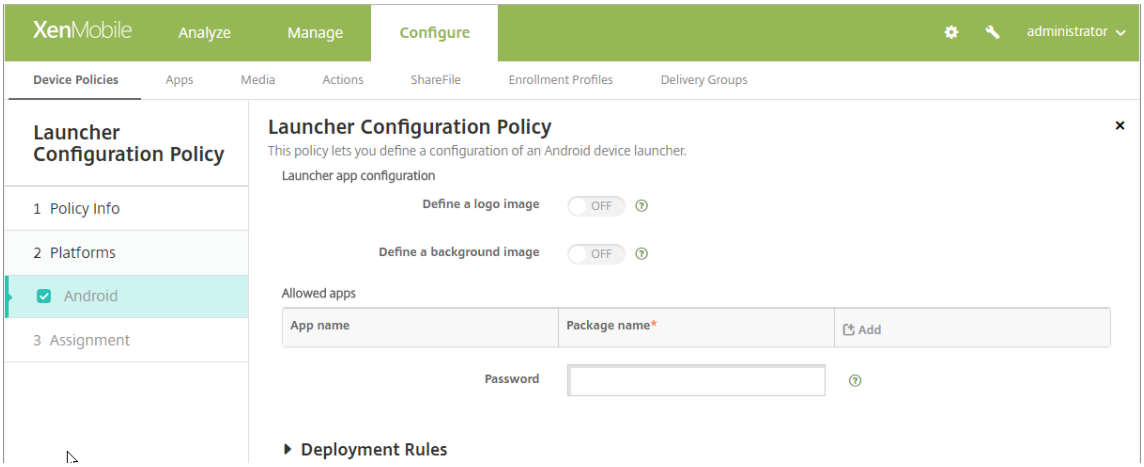
Launcher Configuration ポリシーを追加すると、次の Citrix Launcher 機能を制御できます。

- ユーザーは管理者が指定したアプリにのみアクセスできるように Android デバイスを管理する。
- Citrix Launcher アイコンのカスタムロゴ画像と、Citrix Launcher のカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

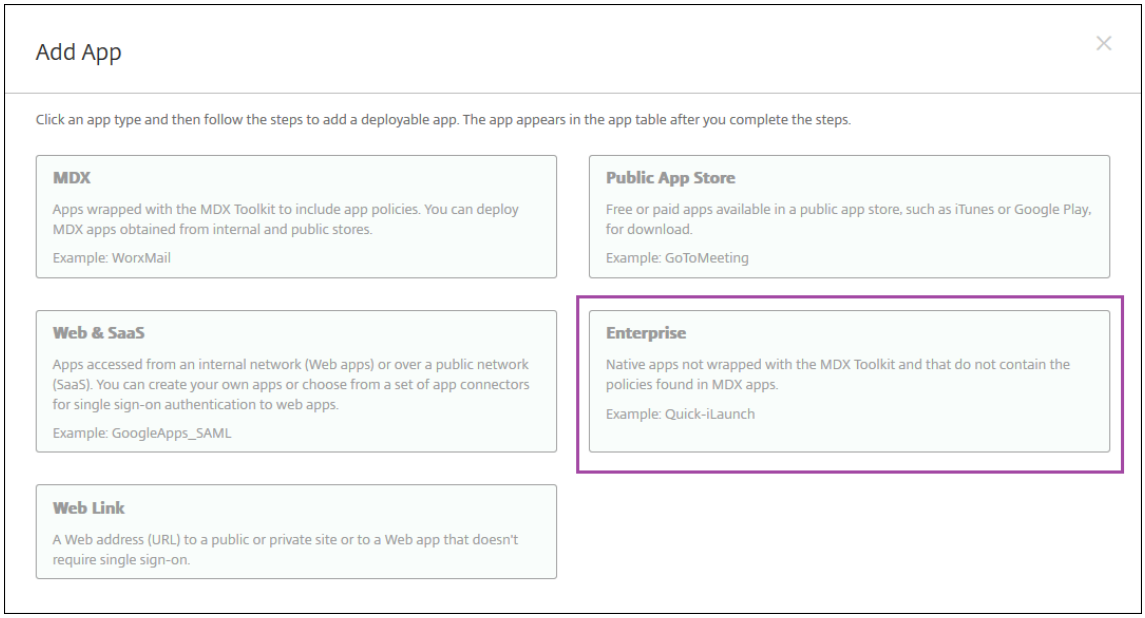
Citrix Launcher を使用するとそれらのデバイスレベルの制約を適用できますが、ランチャーは、Wi-Fi 設定、Bluetooth 設定、およびデバイスパスコード設定などのデバイス設定への組み込みのアクセス権をユーザーに付与します。Citrix Launcher は、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Citrix Launcher を Android デバイスに提供するには、次の一般的な手順に従います。

1. Citrix Launcher アプリを XenMobile エディションのCitrix XenMobile ダウンロードページからダウンロードします。ファイル名は CitrixLauncher.apk です。ファイルはすぐに XenMobile にアップロードできる状態で、ラッピングを必要としません。
2. デバイスポリシーに［**Launcher** 構成ポリシー］を追加します。［構成］**>**［デバイスポリシー］の順にクリックして、［追加］をクリックし、［新しいポリシーの追加］ダイアログボックスに「**Launcher**」と入力します。詳しくは、「Launcher 構成ポリシー」を参照してください。

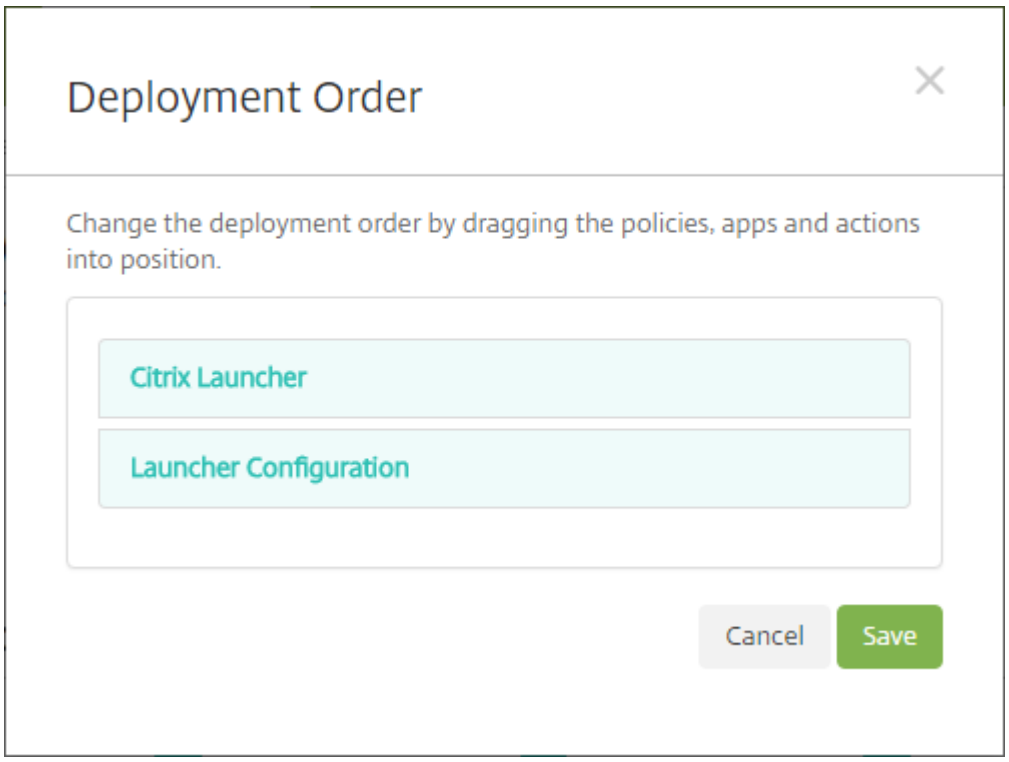


3. Citrix Launcher アプリをエンタープライズアプリケーションとして XenMobile に追加します。［構成］**>** ［アプリ］ で、［追加］、［エンタープライズ］ の順にクリックします。詳しくは、「エンタープライズアプリの追加」を参照してください。



4. ［構成］**>** ［デリバリーグループ］ で次のように構成して、Citrix Launcher のデリバリーグループを作成します。

   - ［ポリシー］ ページで、［**Launcher** 構成ポリシー］ を追加します。
   - ［アプリ］ ページで、**Citrix Launcher** を ［必須アプリ］ にドラッグします。
   - ［概要］ ページで ［展開順］ をクリックして、**Citrix Launcher** アプリが **Launcher** 構成ポリシーよりも先であることを確認します。



詳しくは、「リソースの展開」を参照してください。

iOS Volume Purchase Program

January 10, 2020

Apple の iOS Volume Purchase Program（VPP）を使用すると、iOS アプリのライセンスを管理することができます。VPP ソリューションを利用すると、組織のアプリケーションやそのほかの大量なデータの検索、購入、配布の処理が簡単になります。

VPP では XenMobile を使用してパブリックアプリケーションストアのアプリを配布することができます。VPP は、業務用モバイルアプリ、または MDX Toolkit を使用してラップしたアプリではサポートされていません。VPP ではパブリックストアから入手した XenMobile アプリを配布することはできますが、展開は最適化されません。この制約に対処するには、XenMobile Server と Secure Hub ストアをさらに強化する必要があります。VPP 経由の XenMobile パブリックストアアプリの展開に関する既知の問題と想定される解決策の一覧は、Citrix knowledge Centerのこちらのトピックを参照してください。

VPP によって、適用可能なアプリをデバイスに直接配布できます。また、引き換え可能なコードを使用してユーザーにコンテンツを割り当てることができます。XenMobile で、iOS VPP に固有の設定を構成できます。

XenMobile は、VPP ライセンスを Apple から定期的に再インポートしてライセンスにすべての変更を反映させています。このような変更には、インポートしたアプリを VPP から手動で削除する場合も含まれます。デフォルトで、

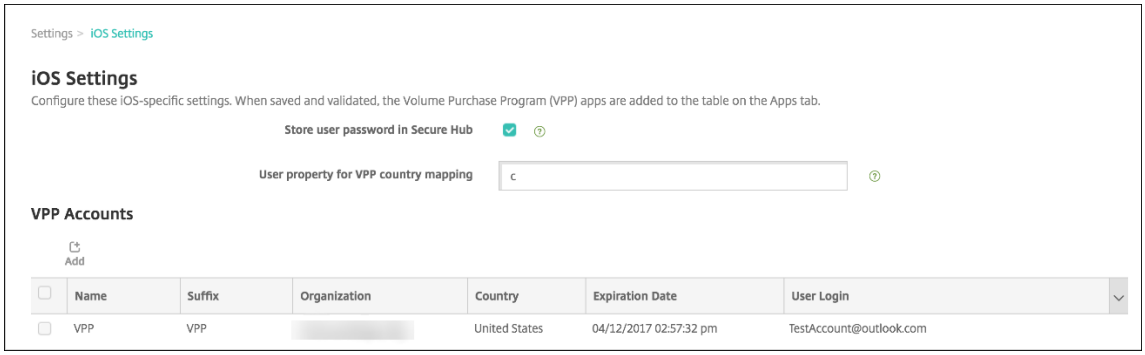
XenMobile は VPP ライセンスベースラインを最小で 720 分ごとに更新します。このベースライン間隔をサーバープロパティの［VPP ベースライン間隔］（vpp.baseline）で変更することができます。詳しくは、「サーバープロパティ」を参照してください。

このトピックは、管理されたライセンスで VPP を使用して、XenMobile でアプリを配布できるようにする方法について説明します。引き換えコードを使用して、管理対象の配布に変更する場合は、Apple 社のサポートドキュメントの「Migrate from redemption codes to managed distribution with the Volume Purchase Program」を参照してください。

iOS VPP について詳しくは、https://vpp.itunes.apple.com/us/storeを参照してください。VPP に登録するには、https://deploy.apple.com/qforms/open/register/check/avsにアクセスします。iTunes で VPP ストアにアクセスするには、https://vpp.itunes.apple.com/?l=enに移動します。

XenMobile で iOS VPP 設定を保存すると、購入したアプリケーションが XenMobile コンソールの ［構成］**>**［アプリ］ ページに表示されます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［プラットフォーム］ で ［**iOS** 設定］ をクリックします。［**iOS** 設定］ 構成ページが開きます。

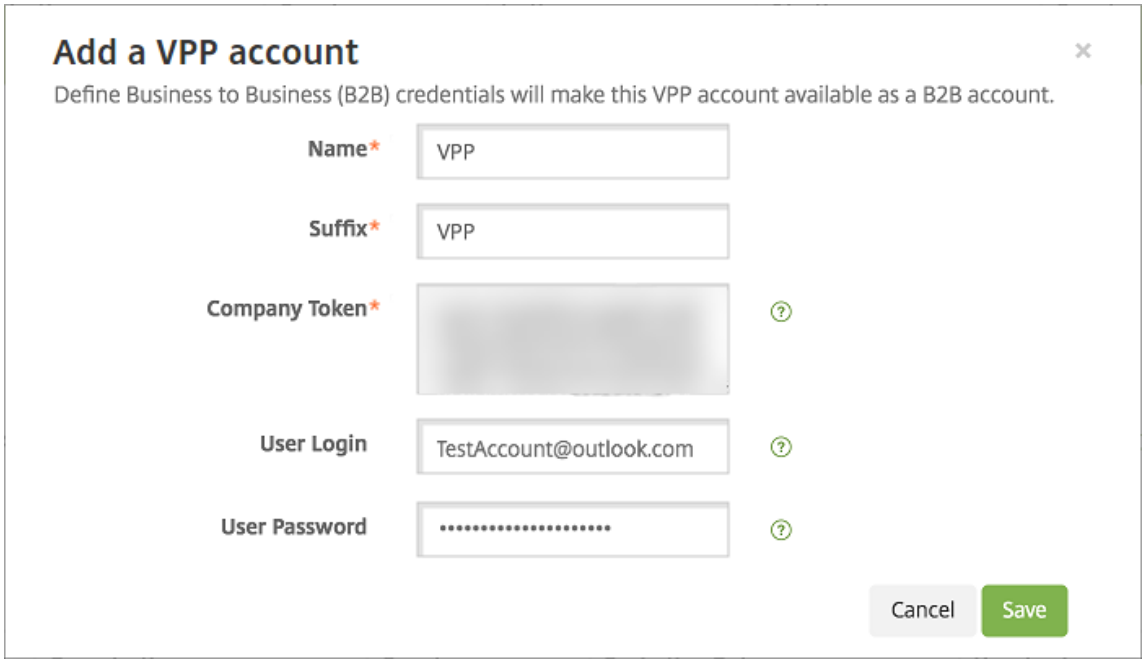


3. 次の設定を構成します。

   - **Secure Hub** のユーザーパスワードを保存する： XenMobile 認証用のユーザー名とパスワードを Secure Hub に保存するかどうかを選択します。デフォルトでは、この安全な方法で情報を保存します。
   - **VPP** 国マッピングのユーザープロパティ： ユーザーが国固有のアプリストアからアプリをダウンロードできるようにするコードを入力します。

   このマッピングは VPP のプロパティプールの選択に使用されます。たとえば、ユーザープロパティが米国で、アプリの VPP コードが日本用の場合、そのユーザーはそのアプリをダウンロードすることはできません。国マッピングコードについて詳しくは、VPP プラン管理者に問い合わせてください。

4. 追加する VPP アカウントごとに、［追加］ をクリックします。［**VPP** アカウントの追加］ ダイアログボックスが開きます。



5. 追加するアカウントごとに、次の設定を構成します。

> 注:
>
> Apple Configurator 1 を使用している場合、次の手順でライセンスファイルをアップロードします。［構成］**>**［アプリ］、プラットフォームページの順に移動し、［**Volume Purchase Program**］を展開します。

   - 名前: VPP アカウント名を入力します。
   - サフィックス: VPP アカウントを介して取得したアプリに表示されるサフィックスを入力します。たとえば、**VPP** を入力すると、Secure Mail アプリはアプリ一覧に［**Secure Mail - VPP**］として表示されます。
   - 会社トークン: Apple から取得した VPP サービストークンを入力するか、コピーして貼り付けます。トークンを取得するには、Apple VPP ポータルの［**Account Summary**］ページで［**Download**］をクリックし、VPP ファイルを生成してダウンロードします。このファイルには、サービストークンのほかに、国コードや有効期限などの他の情報も含まれます。ファイルを安全な場所に保存します。
   - ユーザーログイン: 任意で、カスタム B2B アプリのインポートに使用する、認証済み VPP アカウントの管理者名を入力します。
   - ユーザーパスワード: VPP アカウントの管理者パスワードを入力します。

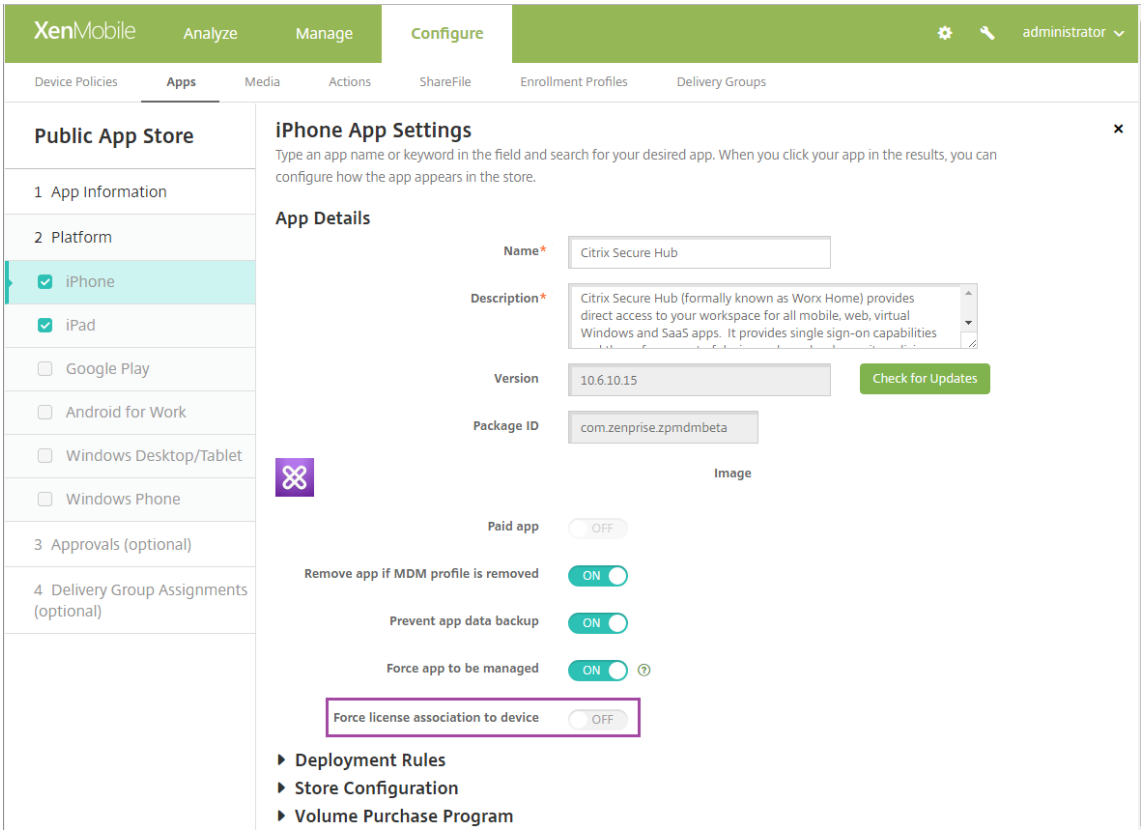
6. ［保存］をクリックしてダイアログボックスを閉じます。
7. ［保存］をクリックして iOS 設定を保存します。

   アプリを［構成］**>**［アプリ］ページの一覧に追加することを伝えるメッセージが表示されます。このページで、VPP アカウントのアプリ名に前述の構成で指定したサフィックスが含まれていることを確認してください。

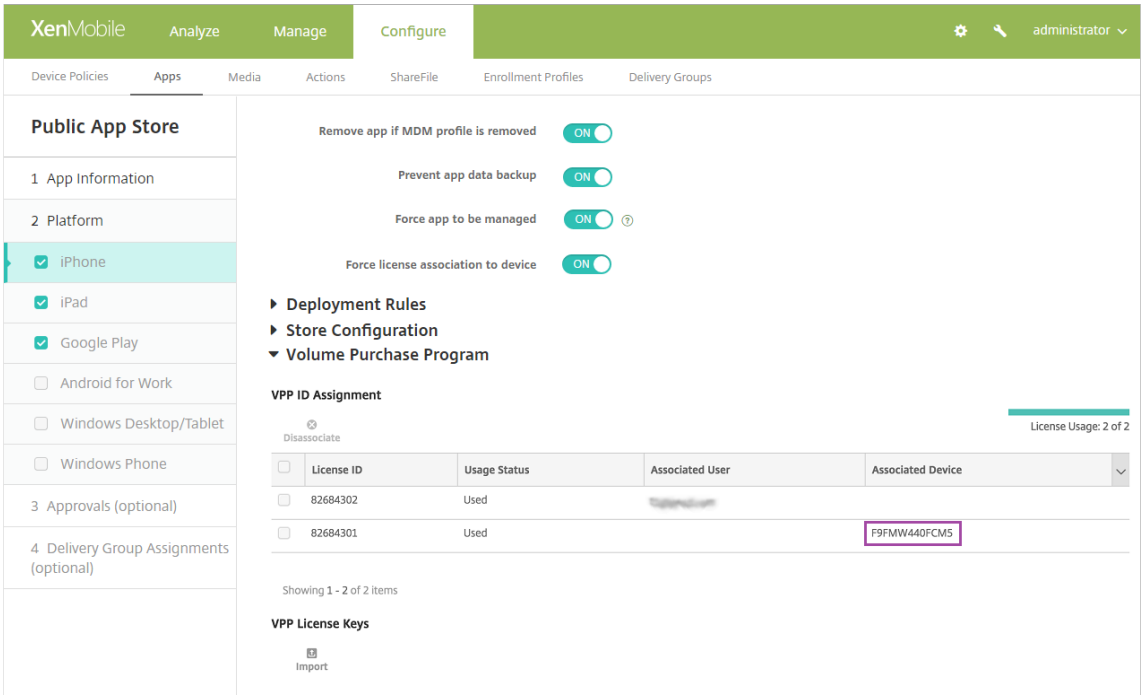
VPP アプリ設定を構成し、VPP アプリのデリバリーグループおよびデリバリーポリシー設定を調整できるようにな

りました。この構成を完了すると、ユーザーはデバイスを登録できるようになります。以下は、この手順で検討する事項です。

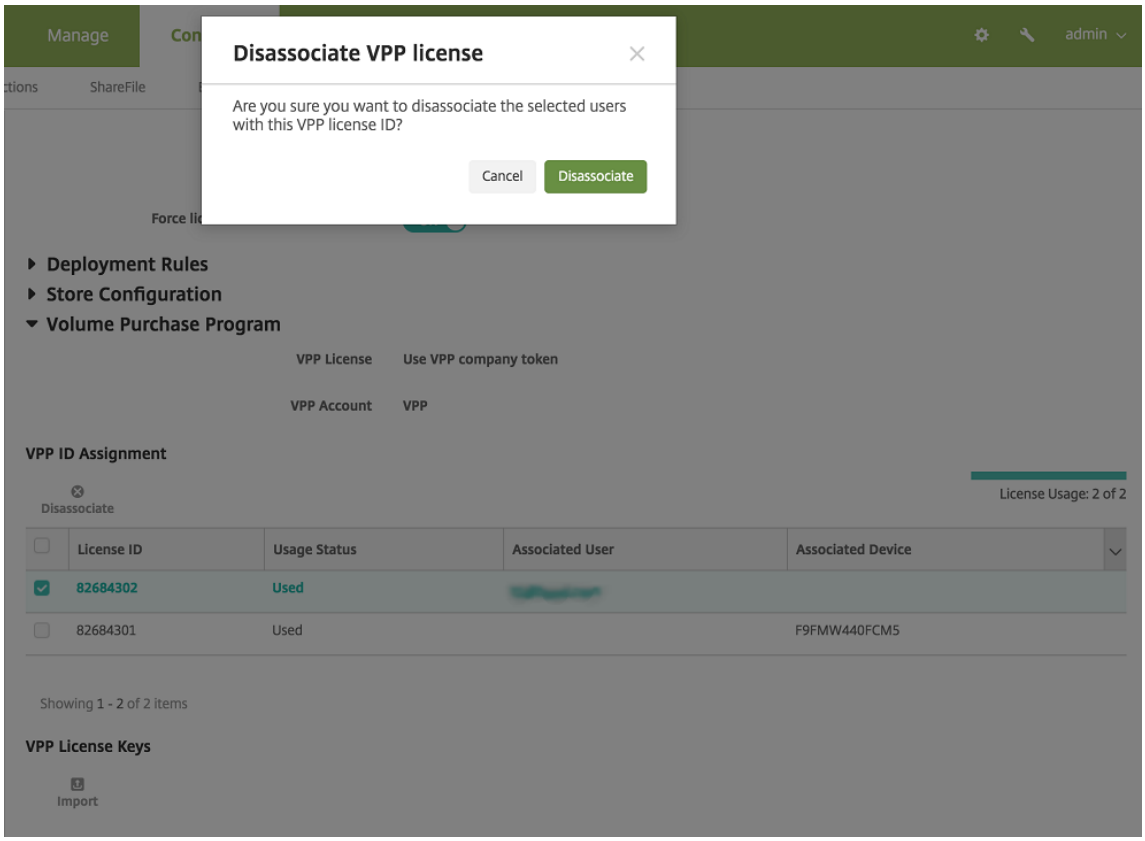
- VPP アプリ設定（［構成］**>**［アプリ］）を構成すると、［デバイスへの強制ライセンス割り当て］が有効になります。監視対象デバイスで Apple VPP および DEP を使用する利点は、XenMobile がアプリをデバイスレベル（ユーザーレベルではなく）で割り当てることができるようになることです。このため、Apple ID デバイスを使用する必要がありません。また、VPP プログラム参加の招待状がユーザーに送信されることもありません。ユーザーは各自の iTunes アカウントにサインインせずにアプリをダウンロードできます。



アプリの VPP 情報を表示するには、［**Volume Purchase Program**］を展開します。［**VPP ID** 割り当て］の表で、ライセンスがデバイスに関連付けられていることにご注意ください。デバイスのシリアル番号は［割り当てられたデバイス］列に表示されます。ユーザーがトークンを削除して再度インポートすると、シリアル番号ではなく「非表示」と表示されます。これは Apple 社のプライバシー制限によるものです。

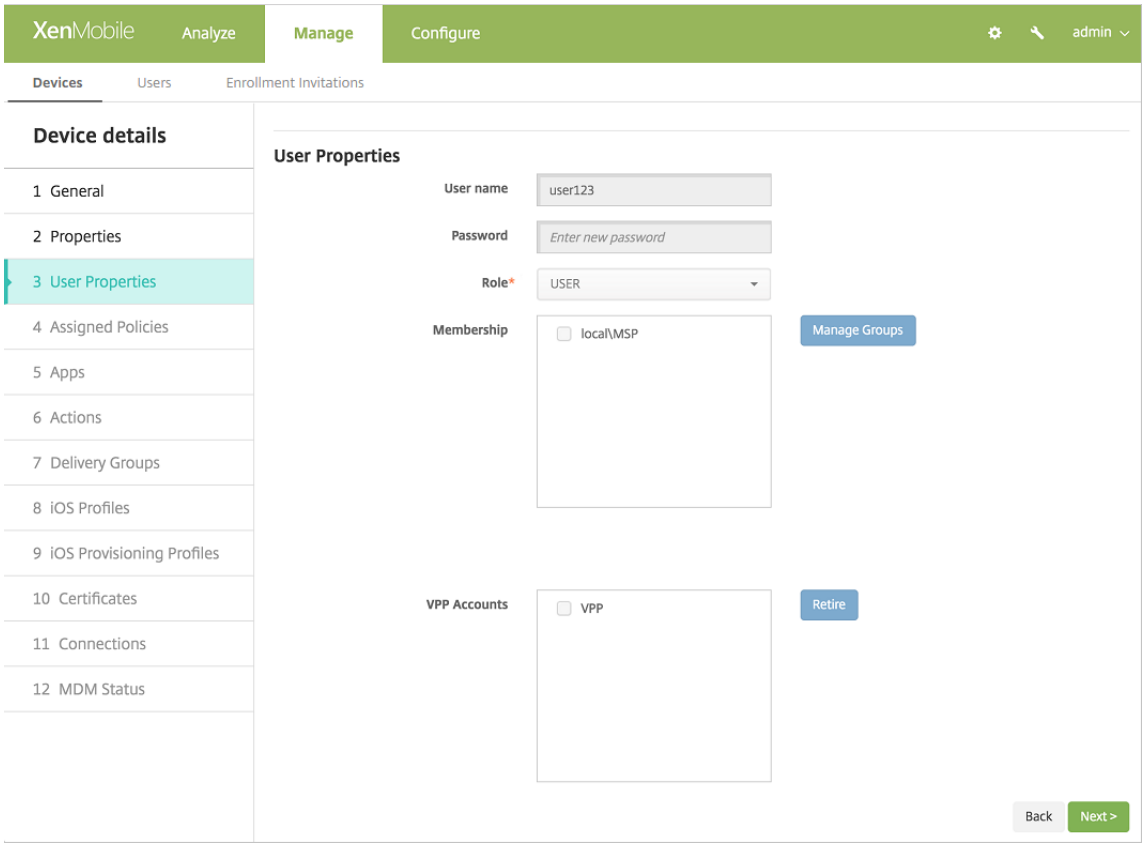


ライセンスの関連付けを解除するには、該当ライセンスの行を選択して ［割り当て解除］ をクリックします。

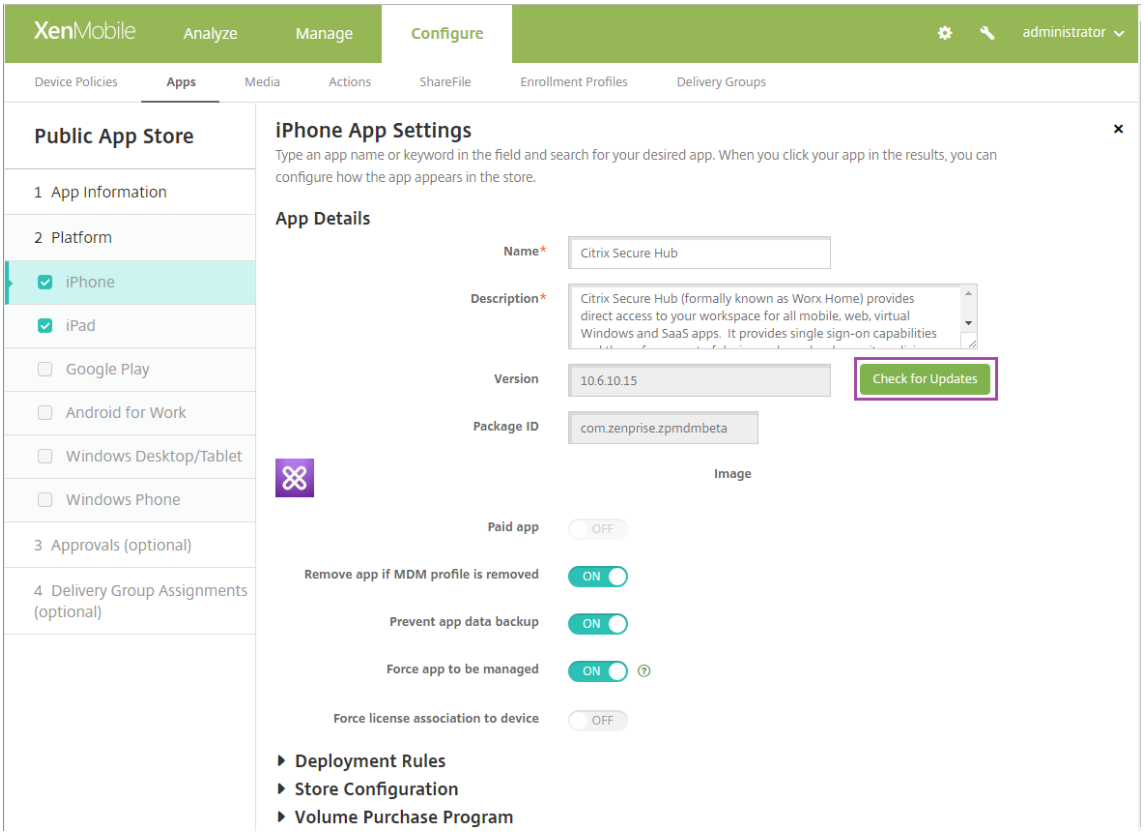


VPP ライセンスをユーザーに関連付けると、XenMobile はユーザーを VPP アカウントに統合し、ユーザーの iTunes ID を VPP アカウントに関連付けます。ユーザーの iTunes ID がユーザーの会社や XenMobile

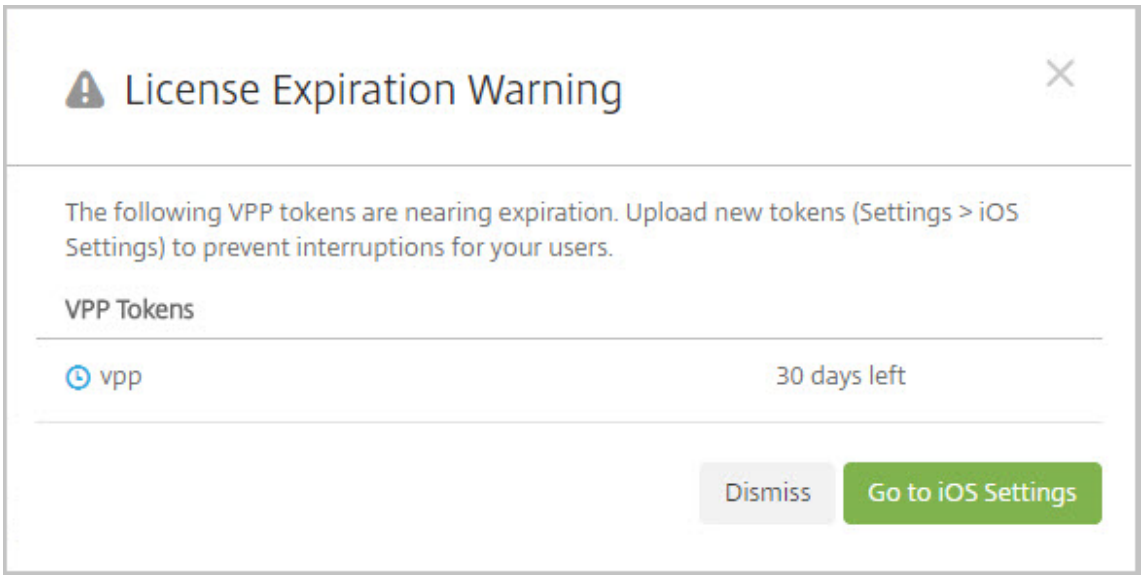
Server に表示されることはありません。Apple 社はユーザーのプライバシーを確保するために、透過的に関連付けを作成します。ユーザーアカウントからすべてのライセンスの関連付けを解除することで、VPP プログラムからユーザーを削除できます。ユーザーを削除するには、［管理］**>**［デバイス］ にアクセスします。



- アプリをデリバリーグループに割り当てると、XenMobile はデフォルトでアプリを任意アプリとして認識します。XenMobile で確実にアプリがデバイスに展開されるようにするには、［構成］**>**［デリバリーグループ］に移動します。［アプリ］ ページでアプリを ［必須アプリ］ 一覧に移動します。
- パブリックアプリケーションストアのアプリの更新が使用可能で、アプリが VPP 経由でプッシュされる場合、ユーザーが更新をチェックして適用するまで、このアプリは自動的にデバイスで更新されません。Secure Hub（ユーザーではなくデバイスに割り当てられている場合）の更新をプッシュするには、次の手順を実行します。プラットフォームページの ［構成］**>**［アプリ］ で、［更新プログラムのチェック］ をクリックして更新を適用します。



XenMobile は、Apple VPP トークンの有効期限が近づいているか、期限が切れている場合、ライセンス有効期限切れ警告を表示します。



Citrix Secure Hub を介した Virtual Apps and Desktops

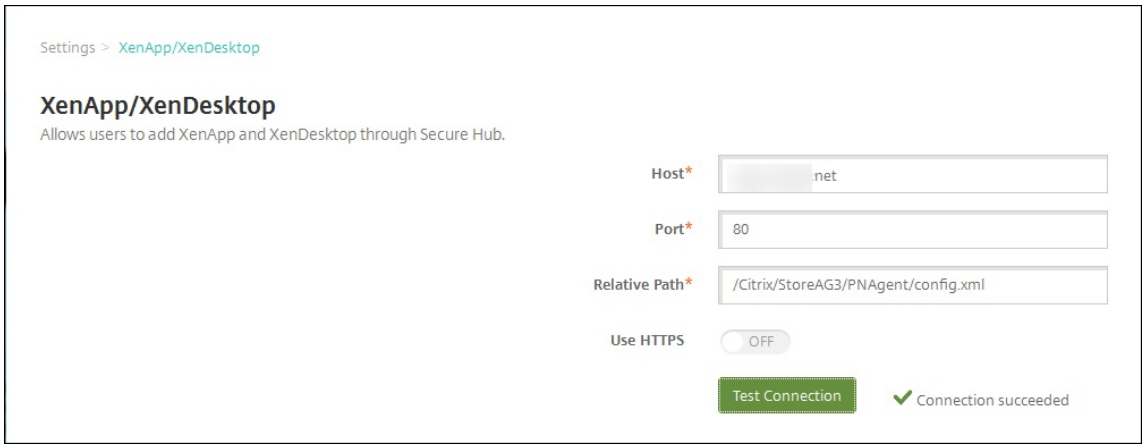
September 24, 2019

> 注：
>
> Citrix XenApp および XenDesktop は、Citrix Virtual Apps and Desktops に名前が変更されます。まだ名前の変更が反映されていないドキュメントやインターフェイスも一部あります。

XenMobile では、Virtual Apps and Desktops からアプリを収集して、XenMobile Store でモバイルデバイスユーザーがそのアプリを使用できるようにすることができます。ユーザーは、XenMobile Store 内から直接アプリケーションをサブスクライブして、Secure Hub から起動します。アプリケーションを起動するために、Citrix Receiver をユーザーのデバイスにインストールする必要があります。ただし、構成する必要はありません。

この設定を構成するには、Web Interface サイトまたは StoreFront の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）または IP アドレスと、ポート番号が必要です。

1. XenMobile Web コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［**XenApp/XenDesktop**］ をクリックします。［**XenApp/XenDesktop**］ ページが開きます。



3. 次の設定を構成します。
   - ホスト： Web Interface サイトまたは StoreFront の完全修飾ドメイン名（FQDN）または IP アドレスを入力します。
   - ポート：Web Interface サイトまたは StoreFront のポート番号を入力します。デフォルトは 80 です。
   - 相対パス： パスを入力します。たとえば、「/Citrix/PNAgent/config.xml」と入力します。
   - **HTTPS** の使用： Web Interface サイトまたは StoreFront とクライアントデバイスの間で安全な認証を有効にするかどうかを選択します。デフォルトは ［オフ］ です。
4. ［接続のテスト］ をクリックして XenMobile が特定の Virtual Apps and Desktops サーバーに接続可能なことを検証します。
5. ［保存］ をクリックします。

ShareFile を XenMobile と使用する

January 10, 2020

XenMobile には、ShareFile と統合するために次の 2 つのオプションがあります。ShareFile Enterprise と StorageZone コネクタです。ShareFile Enterprise または StorageZone コネクタとの統合には、XenMobile Enterprise Edition が必要です。

ShareFile Enterprise

XenMobile Enterprise Edition をお持ちの場合、ShareFile Enterprise アカウントへのアクセスを提供するように XenMobile を構成できます。この構成により以下の機能が実現します:

- モバイルユーザーに、ファイル共有、ファイル同期、StorageZone コネクタなどの ShareFile の完全な機能セットへのアクセス権を与えることができます。
- XenMobile Apps ユーザーのシングルサインオン認証、Active Directory ベースのユーザーアカウントプロビジョニング、および包括的なアクセス制御ポリシーを ShareFile で使用できます。
- XenMobile コンソールから ShareFile の構成、サービスレベルの監視、およびライセンスの使用状況の監視を行えます。

ShareFile Enterprise のための XenMobile の構成について詳しくは、「ShareFile での SAML によるシングルサインオン」を参照してください。

StorageZone コネクタ

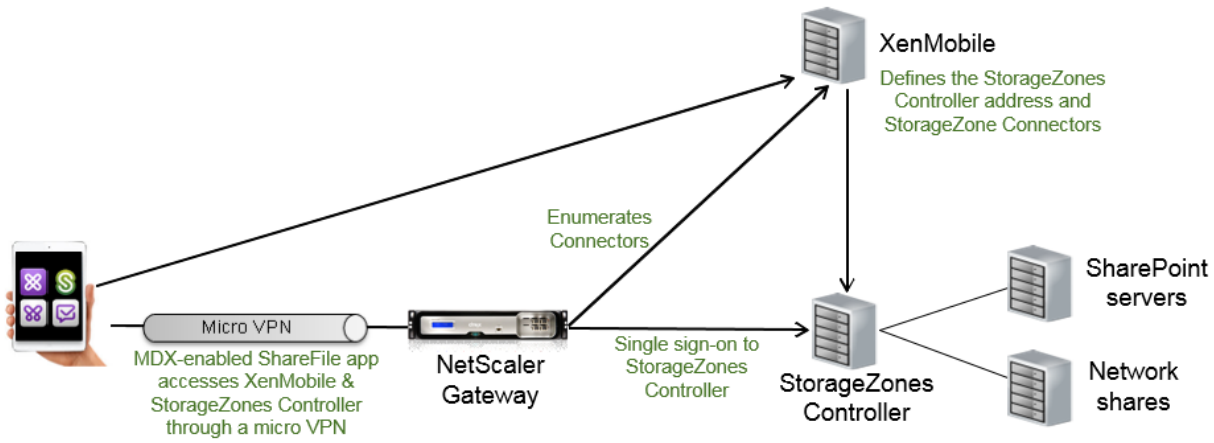
XenMobile を、XenMobile コンソールで作成した StorageZone コネクタだけにアクセスできるように構成することも可能です。この構成により以下の機能が実現します:

- SharePoint サイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。
- ShareFile サブドメインの設定や ShareFile に対するユーザーのプロビジョニング、ShareFile データのホストが不要になります。
- iOS および Android 用の業務用モバイルアプリでデータにモバイルアクセスできます。Microsoft Office ドキュメントを編集できます。モバイルデバイスから Adobe PDF ファイルのプレビューおよび注釈もできます
- 社内ネットワーク外へのユーザー情報漏洩に対するセキュリティ規制に準拠します。
- XenMobile コンソールから StorageZone コネクタを簡単にセットアップできます。後で XenMobile で完全な ShareFile 機能を使用することにした場合は、XenMobile コンソールで構成を変更できます。
- XenMobile Enterprise Edition が必要です。

XenMobile と StorageZone コネクタのみとの統合の場合、次のようになります:

- ShareFile は、NetScaler Gateway へのシングルサインオン構成を使用して StorageZone Controller に対する認証を行います。
- ShareFile コントロールプレーンが使用されないため、XenMobile での SAML 経由での認証は行われません。

次の図は、XenMobile と StorageZone コネクタを組み合わせて使う高度なアーキテクチャを示しています。



要件

- 各コンポーネントの最小バージョンは次のとおりです:
  - XenMobile Server 10.5（オンプレミス）
  - ShareFile for iOS（MDX）5.3
  - ShareFile for Android（MDX）5.3
  - ShareFile StorageZones Controller 5.0

    この記事では、ShareFile StorageZones Controller 5.0 の構成方法を説明します。
- StorageZone Controller を実行するサーバーがシステム要件を満たしていることを確認してください。要件について詳しくは、「システム要件」を参照してください。

StorageZone for ShareFile Data および Restricted StorageZone に関する要件は、XenMobile と StorageZone コネクタのみとの統合には適用されません。

XenMobile では、Documentum コネクタはサポートされません。

- PowerShell スクリプトを実行するには:
  - スクリプトは、32 ビット（x86）バージョンの PowerShell で実行します。

インストール作業

StorageZone Controller のインストールと設定を行うには、次の作業を記載順に実行します。これらの手順は、XenMobile と StorageZone コネクタのみとの統合に固有のものです。以下の記事の一部は、StorageZone Controller のドキュメントのものです。

1. StorageZone Controller 用の NetScaler の構成

   NetScaler を StorageZone Controller の DMZ プロキシとして使用できます。

2. SSL 証明書のインストール

   StorageZone Controller で標準ゾーンをホストする場合、SSL 証明書が必要になります。StorageZone Controller で制限付きゾーンをホストし内部アドレスを使用する場合は、SSL 証明書は必要ありません。

3. サーバーの準備

   StorageZone コネクタに対して IIS と ASP.NET を設定する必要があります。

4. StorageZone Controller のインストール

5. StorageZone コネクタのみで使用する StorageZone Controller の準備

6. StorageZone のプロキシサーバーの指定

   StorageZone Controller のコンソールで、StorageZone Controller のプロキシサーバーを指定できます。プロキシサーバーは他の方法で指定することもできます。

7. 委任のために StorageZone Controller を信頼するようにドメインコントローラーを構成する

   ネットワーク共有上または SharePoint サイト上の NTLM か Kerberos 認証をサポートするようにドメインコントローラーを構成します。

8. StorageZone へのセカンダリ StorageZone Controller の追加

   高可用性を実現するように StorageZone を構成するには、2 つ以上の StorageZone Controller を StorageZone に接続します。

StorageZone Controller のインストール

1. StorageZone Controller ソフトウェアをダウンロードしてインストールします：

   a) ShareFile のダウンロードページ（https://www.citrix.com/downloads/sharefile.html）でログオンして、最新の StorageZone Controller インストーラーをダウンロードします。

   b) StorageZone Controller をインストールすると、サーバーのデフォルトの Web サイトが StorageZone Controller のインストールパスに変更されます。デフォルトの Web サイトで匿名認証を有効にします。

2. StorageZone Controller をインストールするサーバー上で StorageCenter.msi を実行します。

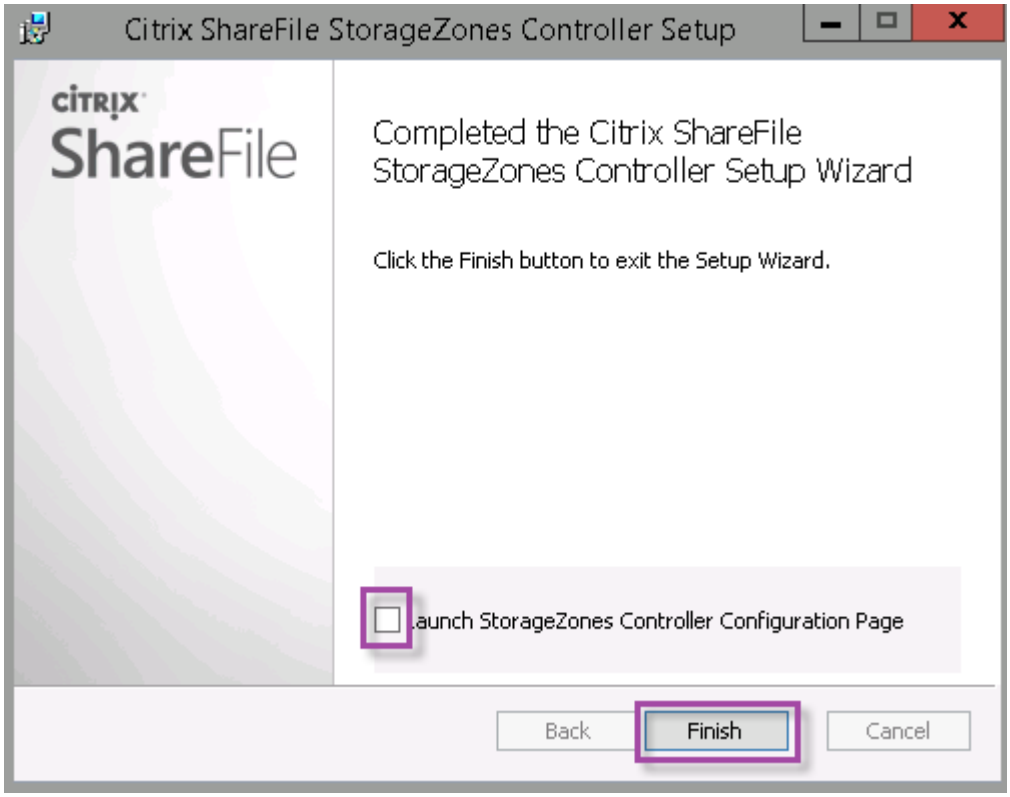
   ShareFile StorageZone Controller Setup ウィザードが起動します。

3. プロンプトに従ってインストールを進めます。

   - インターネットインフォメーションサービス（IIS：Internet Information Services）がデフォルトの場所にインストールされている場合、［ターゲットフォルダー］ ページの設定はデフォルトのままにし

ます。IIS がデフォルトの場所以外にインストールされている場合は、IIS のインストール先を指定します。

- インストールが完了したら、［**StorageZone Controller** の構成ページを起動］ チェックボックスをオフにして ［完了］ をクリックします。



4. メッセージが表示されたら、StorageZone Controller を再起動します。
5. インストールが成功したかテストするために、`https://localhost/`にアクセスします。インストールが成功している場合、ShareFile のロゴが表示されます。

   ShareFile のロゴが表示されない場合は、ブラウザーのキャッシュを削除してもう一度アクセスしてください。

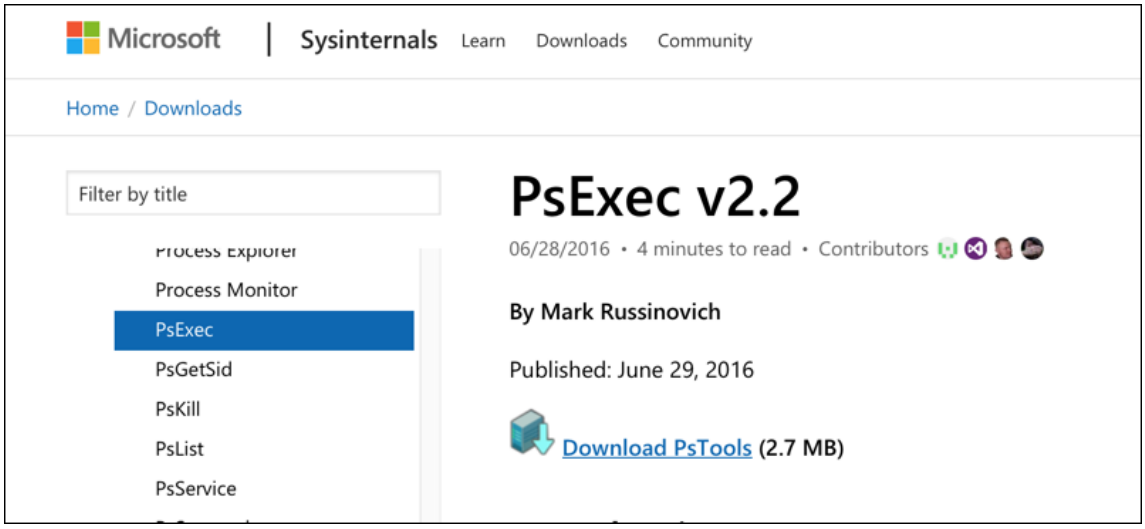
   > 重要:
   >
   > StorageZones Controller を複製する予定がある場合は、StorageZones Controller の構成に進む前にディスクイメージをキャプチャします。

StorageZone コネクタのみで使用する **StorageZone Controller** の準備

StorageZone コネクタのみと統合する場合、StorageZone Controller の管理コンソールは使用しません。これは、管理コンソールではこのソリューションに必要ない ShareFile の管理者アカウントが求められるためです。このため、PowerShell スクリプトを実行して、使用する StorageZone Controller の準備を ShareFile コントロールプレーンを用いずに行います。このスクリプトでは次の操作が行われます。

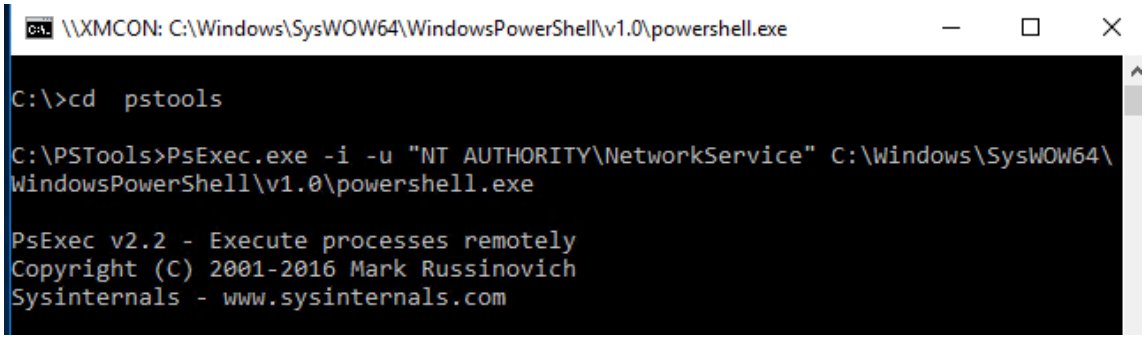
- プライマリ StorageZone Controller としての現在の StorageZone Controller の登録。後で、このプライマリ StorageZone Controller にセカンダリ StorageZone Controller を追加できます。
- ゾーンの作成およびゾーンのパスフレーズの設定

1. StorageZone Controller サーバーでの PsExec ツールのダウンロード: Microsoft Windows Sysinternalsにアクセスして ［**PsTools** のダウンロード］ をクリックします。ダウンロードしたツールを C ドライブのルートに展開します。

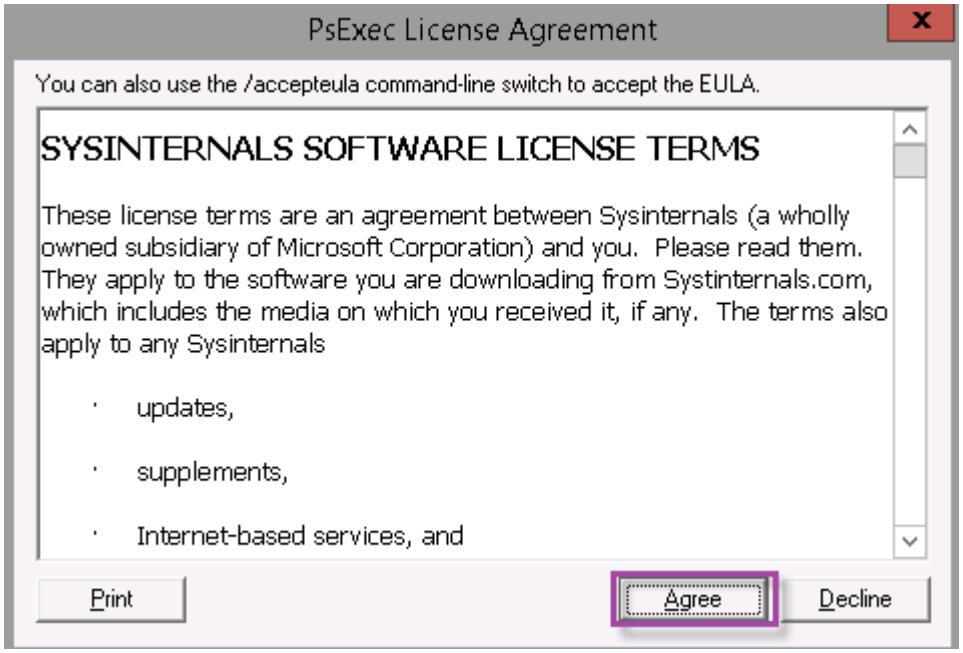


2. PsExec ツールの実行: 管理者ユーザーとしてコマンドプロンプトを開き、次のように入力します。

```
cd c:\pstools
PsExec.exe -i -u ”NT AUTHORITY\NetworkService” C:\Windows\SysWOW64
    \WindowsPowerShell\v1.0\powershell.exe
```



3. メッセージが表示されたら、 ［同意］ をクリックして Sysinternals ツールを実行します。



PowerShell ウィンドウが開きます。

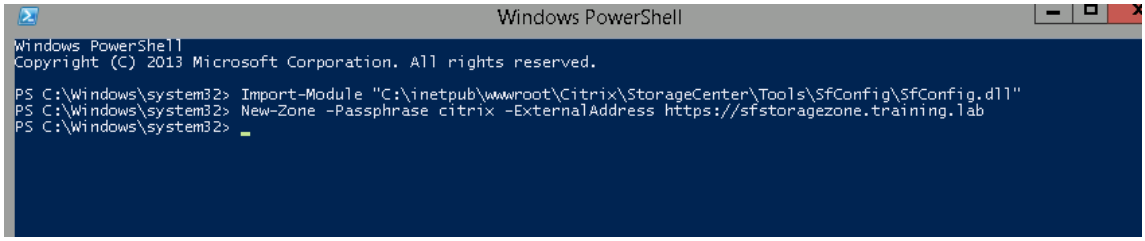
4. PowerShell ウィンドウで次のよう入力します。

```
Import-Module ”C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll”
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

各項目の意味は次の通りです:

Passphrase: サイトに割り当てるパスフレーズを指定します。このパスフレーズはメモしておいてください。Storagezone Controller でパスフレーズを回復することはできません。パスフレーズを失くすと、StorageZone の再インストール、StorageZone への StorageZone Controller の追加、サーバー障害時の StorageZone の復旧を行えなくなります。

ExternalAddress: StorageZone Controller サーバーの外部完全修飾ドメイン名を指定します。



これで、プライマリ StorageZone Controller の準備ができました。

該当する場合は、XenMobile にログインして StorageZone コネクタを作成する前に以下の構成を行います。

StorageZone のプロキシサーバーの指定

委任のために StorageZone Controller を信頼するようにドメインコントローラーを構成する

StorageZone へのセカンダリ StorageZone Controller の追加

StorageZone コネクタを作成する場合は、「XenMobile で StorageZones Controller 接続を定義する」を参照してください。

StorageZone へのセカンダリ StorageZone Controller の追加

高可用性を実現するように StorageZone を構成するには、2 つ以上の StorageZone Controller を StorageZone に接続します。ゾーンにセカンダリ StorageZone Controller を追加するには、2 台目のサーバーに StorageZone Controller をインストールします。その後、インストールした StorageZone Controller を、プライマリ StorageZone Controller のゾーンに追加します。

1. プライマリサーバーに追加する StorageZone Controller サーバーで、PowerShell ウィンドウを開きます。
2. PowerShell ウィンドウで次のよう入力します。

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

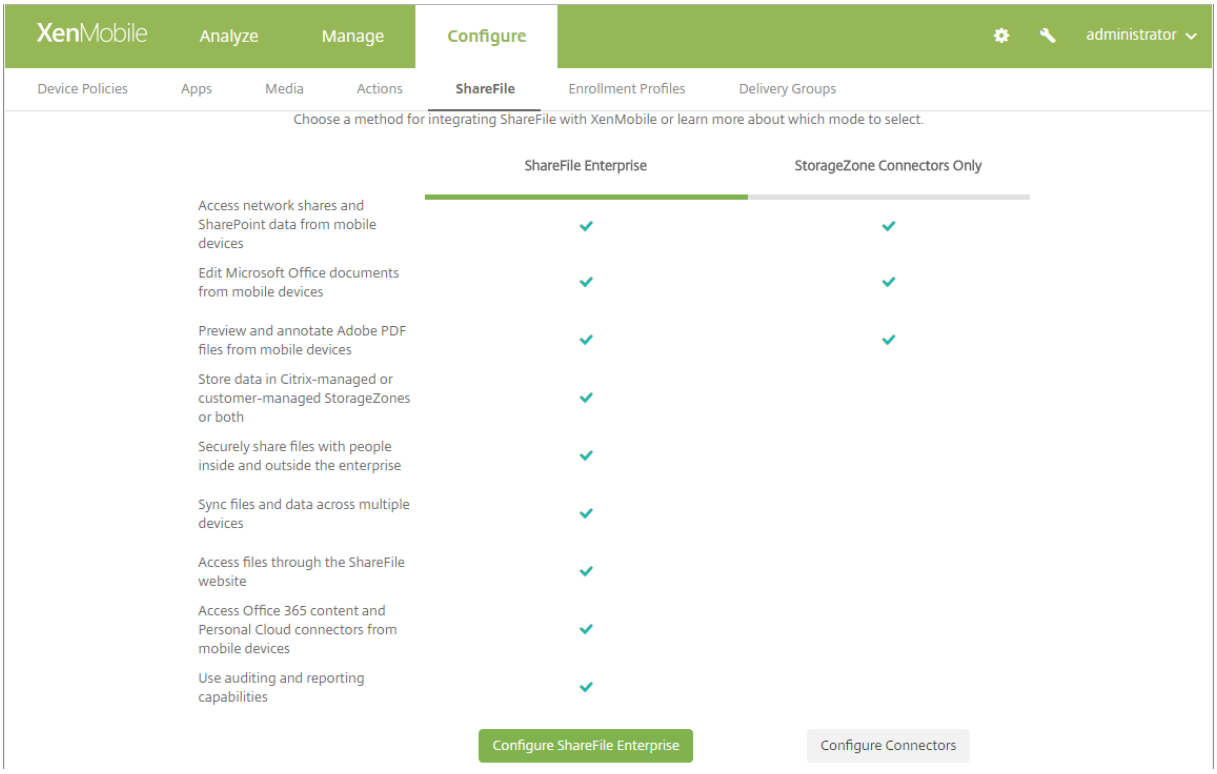
   次に例を示します:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

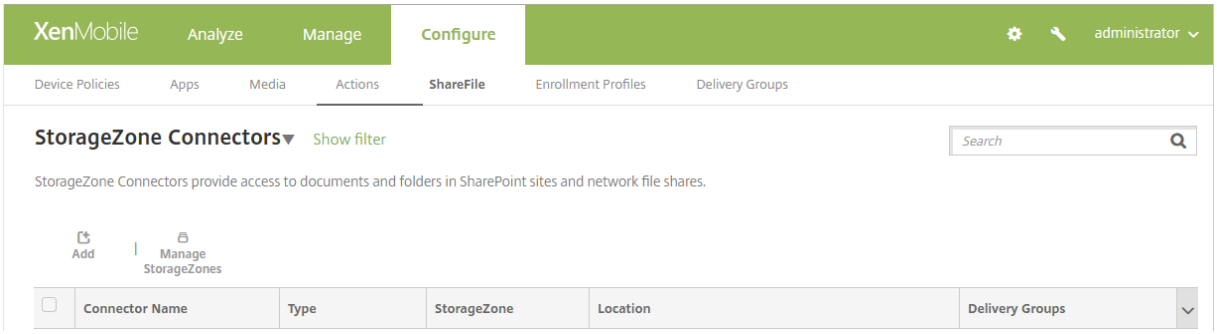
XenMobile で StorageZones Controller 接続を定義する

StorageZone コネクタを追加する前に、StorageZone コネクタに対応する各 StorageZone Controller の接続情報を構成します。このセクションの説明通りに StorageZones Controller を定義してください。つまり、コネクタを追加する場合の手順は以下の通りです。

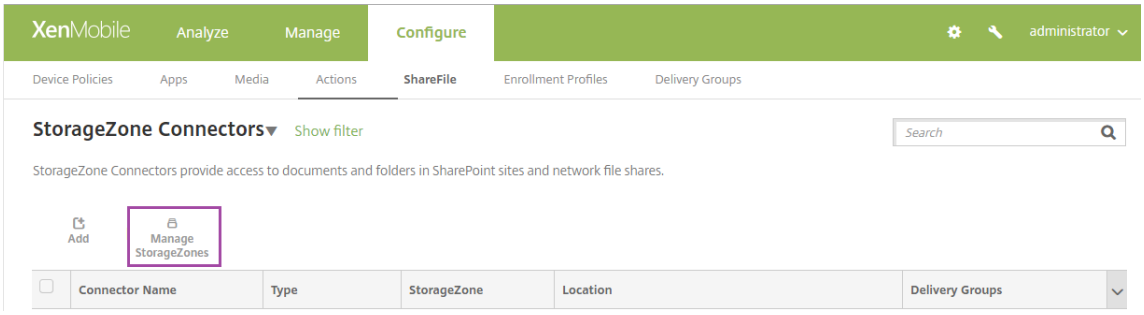
初めて ［構成］**>** ［**ShareFile**］ の順にアクセスすると、XenMobile を ShareFile Enterprise と組み合わせた場合と StorageZone コネクタと組み合わせた場合との差異の要約が表示されます。



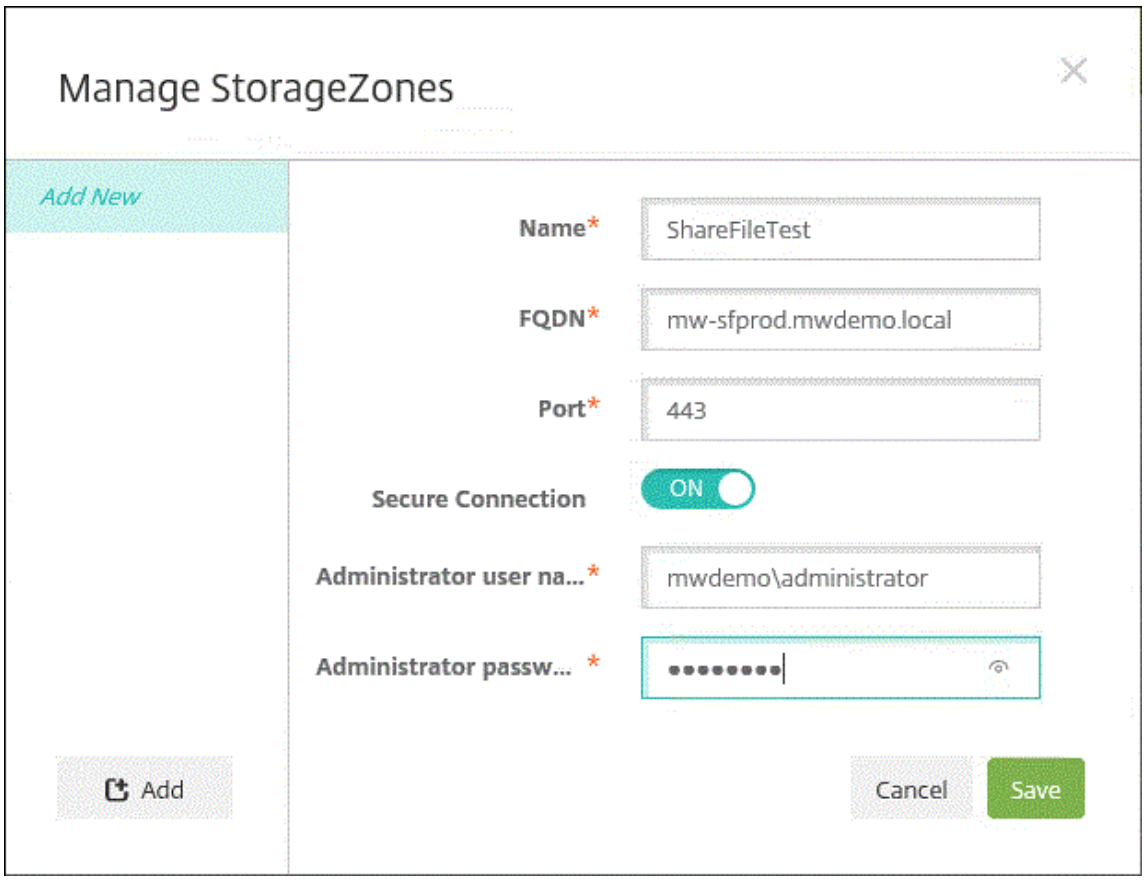
［コネクタの構成］ をクリックしてこの記事の構成手順を進めます。



1. ［構成］ > ［**ShareFile**］ で、 ［**StorageZone** の管理］ をクリックします。



2. ［**StorageZone** の管理］ で、接続情報を追加します。



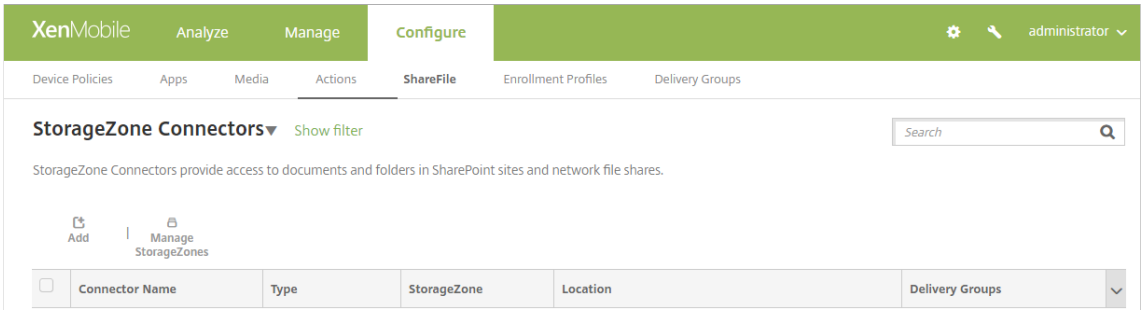
- 名前: StorageZone の説明的な名前で、XenMobile で StorageZone を識別するのに使用されます。名前に空白や特殊文字は含めないでください。
- [**FQDN**] および [ポート]: XenMobile サーバーからアクセス可能な StorageZone Controller の完全修飾ドメイン名（FQDN）とポート番号。
- セキュリティで保護された接続: StorageZone Controller との接続に SSL を使用する場合は、デフォルト設定の [オン] を使用します。接続に SSL を使用しないのであれば、この設定を [オフ] に変更します。
- [管理者ユーザー名] と [管理者パスワード]: 管理者サービスアカウントのユーザー名 (domain\admin 形式) とパスワード。または、StorageZone Controller の読み取り権限と書き込み権限を持つユーザーアカウントを指定します。

3. [保存] をクリックします。
4. 接続をテストするために、XenMobile Server がポート 443 で StorageZone Controller の完全修飾ドメイン名に接続できることを確認します。
5. 別の StorageZones Controller 接続を設定するには、[**StorageZone** の管理] の [追加] ボタンをクリックします。

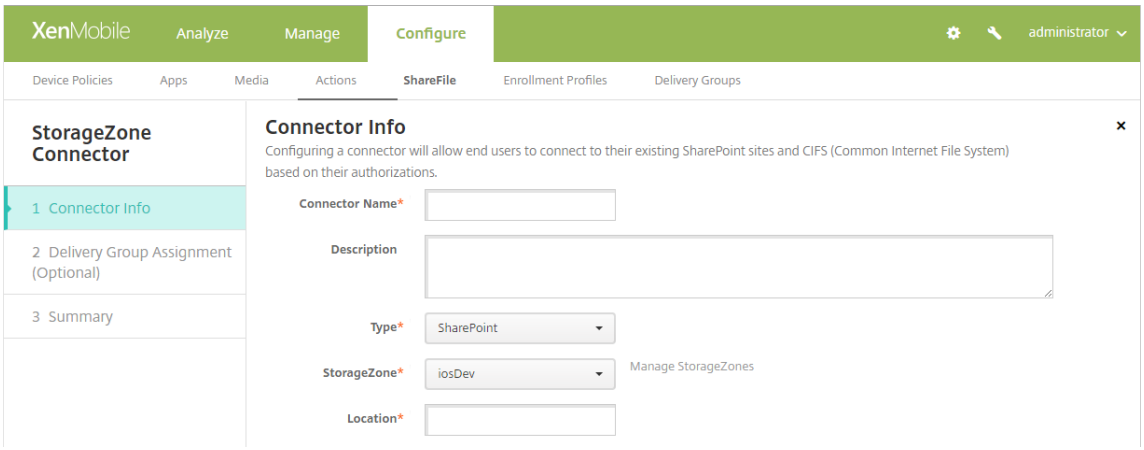
   StorageZones Controller の接続情報を編集したり、削除するには、[**StorageZones** の管理] で接続名を選択します。続いて、[編集] または [削除] をクリックします。

XenMobile に StorageZone コネクタを追加する

1. [構成] > [**ShareFile**] に移動し、 [追加] をクリックします。

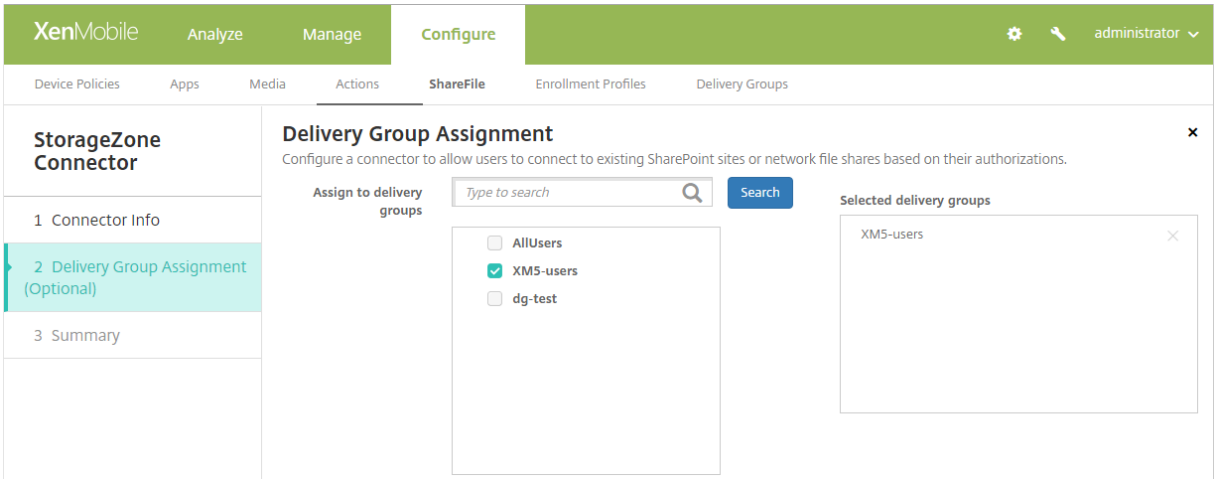


2. [コネクタ情報] ページで、次の設定を行います。



- コネクタ名: XenMobile で StorageZone コネクタを識別する名前。
- 説明: このコネクタに関するオプションのメモ。
- 種類: [**SharePoint**] または [ネットワーク] のいずれかを選択します。
- **StorageZone**: コネクタに関連付けられた StorageZone を選択します。StorageZone が表示されない場合は、 [**StorageZone** の管理] をクリックして、StorageZone Controller を定義します。
- 場所: SharePoint の場合は、SharePoint ルートレベルのサイト、サイトコレクション、またはドキュメントライブラリの URL を`https://sharepoint.company.com`の形式で指定します。ネットワーク共有の場合は、UNC（Uniform Naming Convention）パスの完全修飾ドメイン名を\\server\share の形式で指定します。

3. [デリバリーグループ割り当て] ページで、オプションでコネクタをデリバリーグループに割り当てます。コネクタのデリバリーグループへの関連付けには、 [構成] > [デリバリーグループ] を使うこともできます。



1. ［概要］ ページで、構成したオプションを確認できます。構成を調整するには、［戻る］ をクリックします。
2. ［保存］ をクリックしてコネクタを保存します。
3. コネクタをテストします:

    a) ShareFile クライアントをラップする場合は、次の操作を行います:

    - ネットワークアクセスポリシーを ［内部ネットワークへトンネル］ に設定します。

    この操作モードでは、ShareFile クライアントからのネットワークトラフィックがすべて XenMobile MDX フレームワークによりインターセプトされます。インターセプトされたトラフィックは、アプリ固有の Micro VPN により NetScaler Gateway 経由でリダイレクトされます。

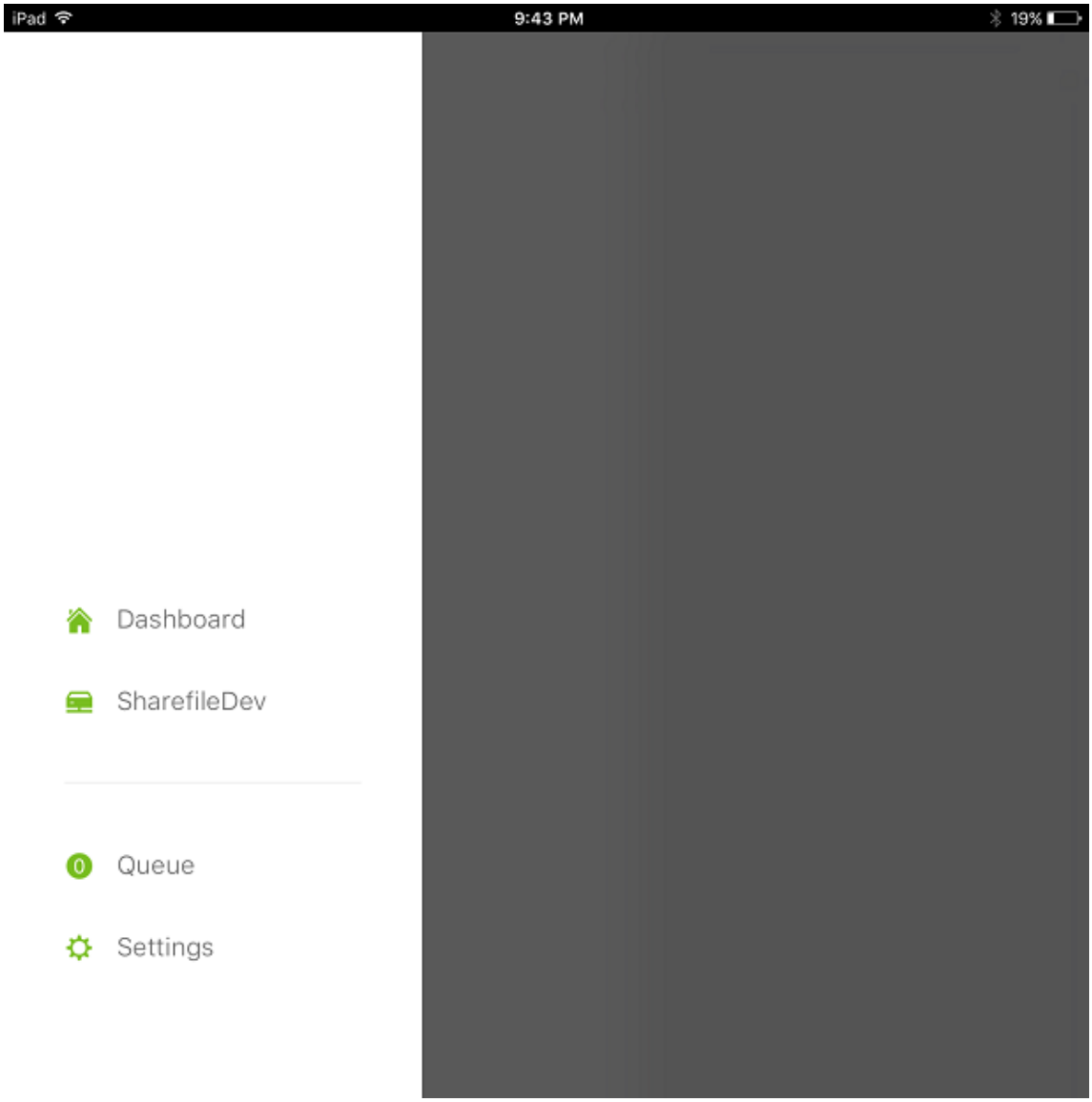
    - ［優先 VPN モード］ポリシーを ［トンネル**-Web SSO**］ に設定します。

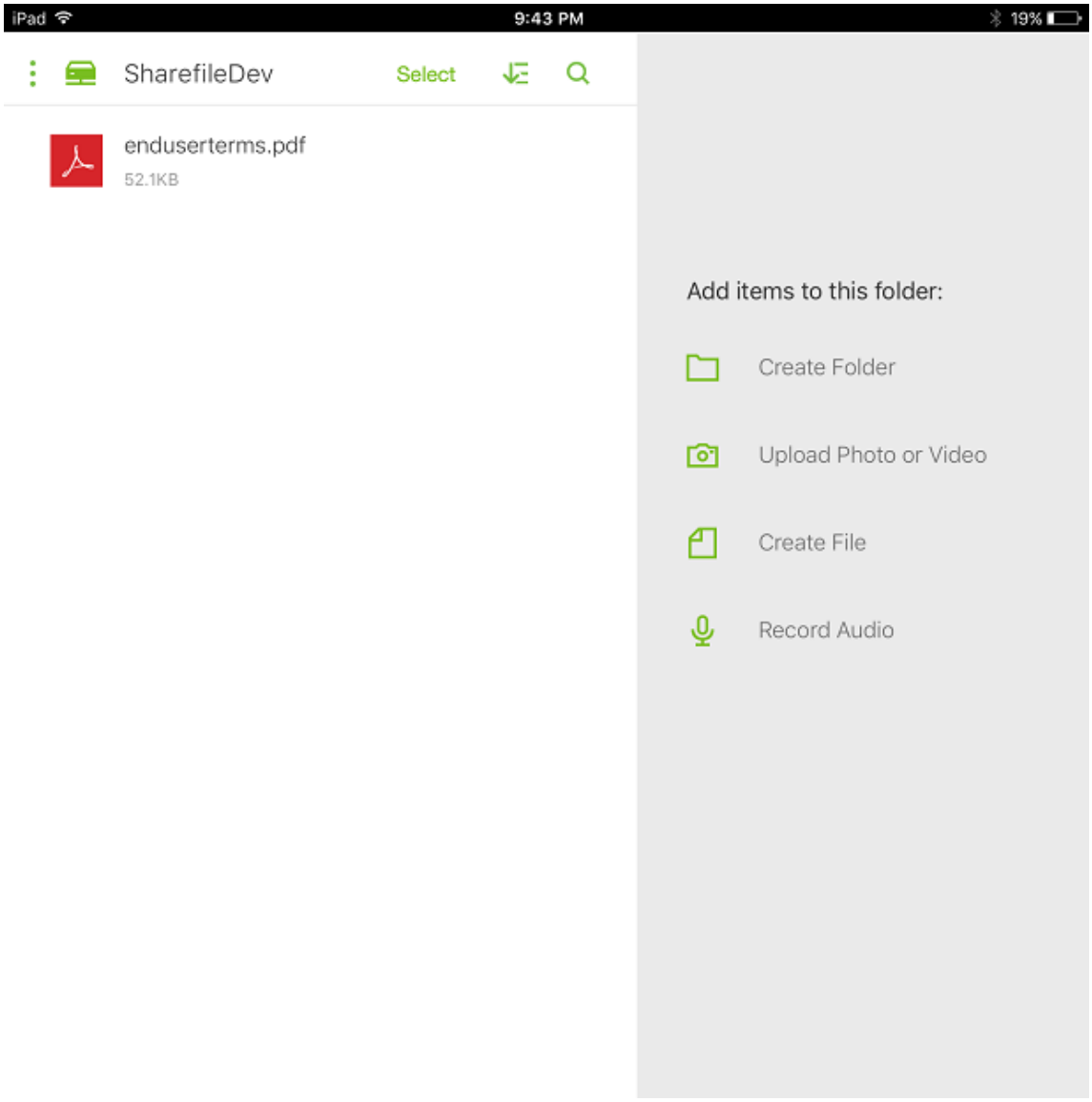
    このトンネルモードでは、MDX アプリからの SSL/HTTP トラフィックが MDX フレームワークによって終了されます。その後、ユーザーに代わって MDX により内部接続に対する新しい接続が開始されます。このポリシー設定では、MDX フレームワークが、Web サーバーから発行された認証チャレンジを検出してそれに応答できます。

    b) ShareFile クライアントを XenMobile に追加します。詳しくは、「Citrix Files for Endpoint Management クライアントの統合と提供」を参照してください。

    c) サポート対象のデバイスで、ShareFile およびコネクタへのシングルサインオンを確認します。

次の例の SharefileDev はコネクタの名前です。

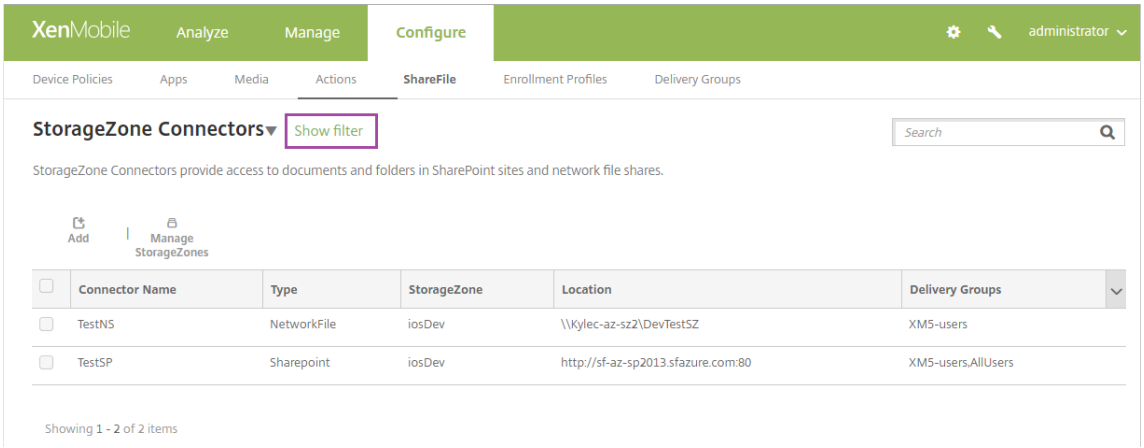




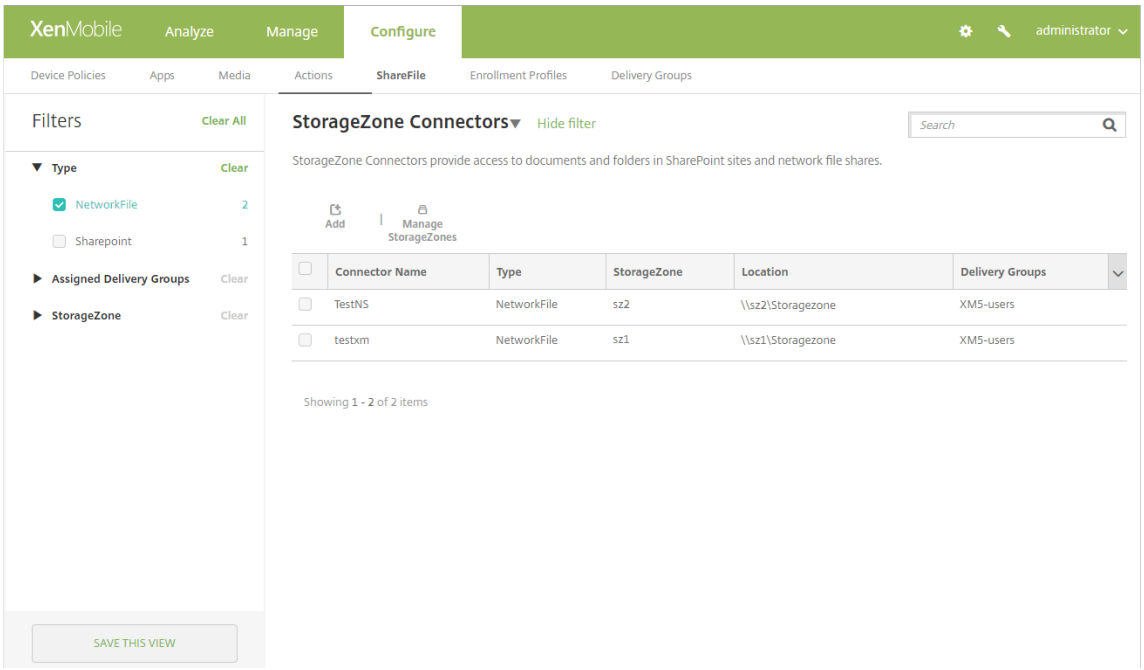
StorageZone コネクター一覧をフィルターする

StorageZone コネクタの一覧は、コネクタタイプ、割り当てられているデリバリーグループ、および StorageZone でフィルタリングできます。

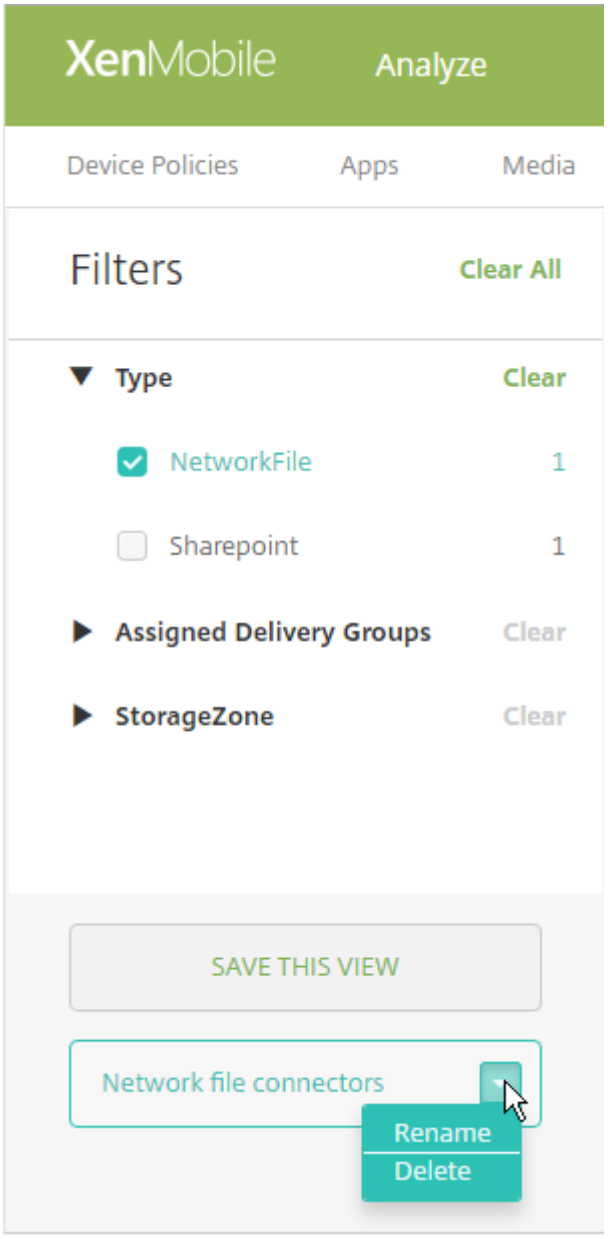
1. ［構成］ **>** ［**ShareFile**］ に移動し、［フィルターを表示］ をクリックします。



2. フィルターの見出しを展開して選択します。フィルターを保存するには、［このビューを保存］ をクリックし、フィルター名を入力して ［保存］ をクリックします。



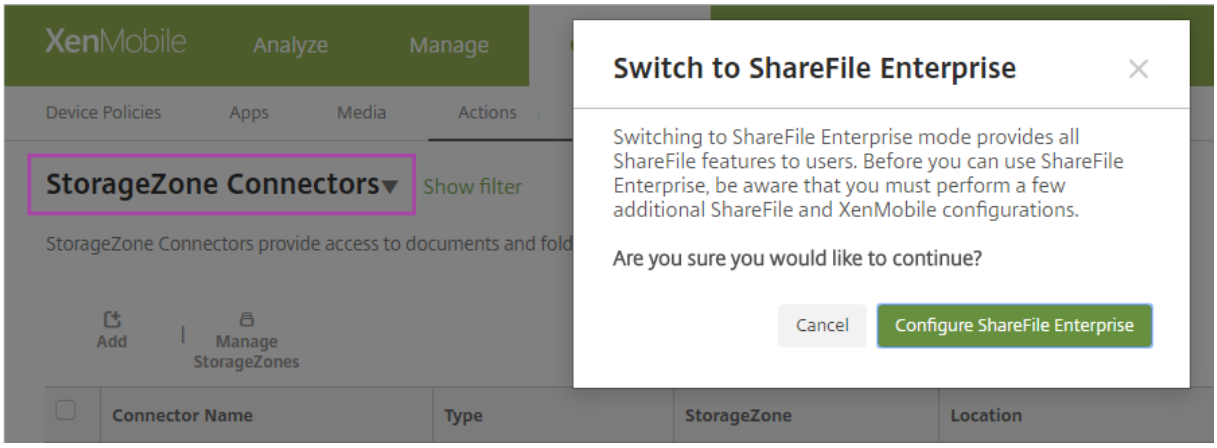
3. フィルターの名前を変更または削除するには、フィルター名の横にある矢印アイコンをクリックします。



ShareFile Enterprise に切り替え

StorageZone コネクタを XenMobile と統合した後にも、ShareFile Enterprise の全機能セットに切り替えることができます。ShareFile Enterprise の機能セットを使用するには、XenMobile Enterprise Edition が必要です。XenMobile では、既存の StorageZone コネクタの統合設定が保持されます。

［構成］**>**［**ShareFile**］ に移動し、［**StorageZone** コネクタ］ ボックスの一覧をクリックし、［**ShareFile Enterprise** の構成］ をクリックします。



ShareFile Enterprise の構成については、「ShareFile での SAML によるシングルサインオン」を参照してください。

HDX アプリ向け SmartAccess

October 25, 2019

この機能により、デバイスプロパティ、デバイスのユーザープロパティ、デバイスにインストールされたアプリケーションに基づいて HDX アプリへのアクセスを制御できます。この機能を使用するには、デバイスをコンプライアンス違反に指定してアクセスを拒否する、自動化された操作を設定します。この機能を使用する HDX アプリを Virtual Apps and Desktops で構成するには、コンプライアンス違反のデバイスへのアクセスを拒否する SmartAccess ポリシーを使用します。XenMobile は、署名された暗号化タグを使って、StoreFront にデバイスの状態を伝えます。すると StoreFront は、アプリのアクセス制御ポリシーに基づいてアクセスを許可または拒否します。

この機能を使用するには、次の環境が必要です。

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 または 3.8
- StoreFront サーバーから HDX アプリを集計するように構成された XenMobile Server
- タグの署名と暗号化に使用する SAML 証明書が構成された XenMobile Server。秘密キーのない同じ証明書が StoreFront サーバーにアップロードされます。

この機能を使い始めるには:

- XenMobile Server 証明書を StoreFront ストアに構成します。
- 必要な SmartAccess ポリシーを使用して、少なくとも 1 つの Virtual Apps and Desktops デリバリーグループを構成します。
- XenMobile で自動化された操作を設定します。

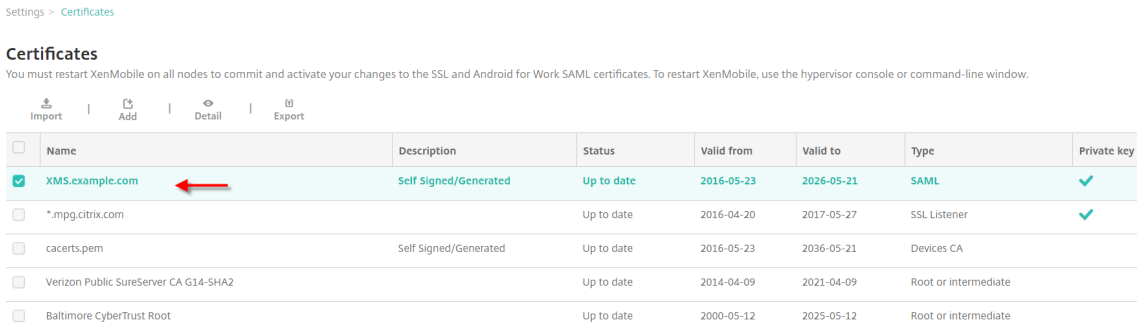
XenMobile Server 証明書のエクスポートと構成、および **StoreFront** ストアへのアップロード

SmartAccess は、署名された暗号化タグを使用して、XenMobile サーバーと StoreFront サーバー間で通信します。この通信を有効にするには、XenMobile のサーバー証明書を StoreFront ストアに追加します。

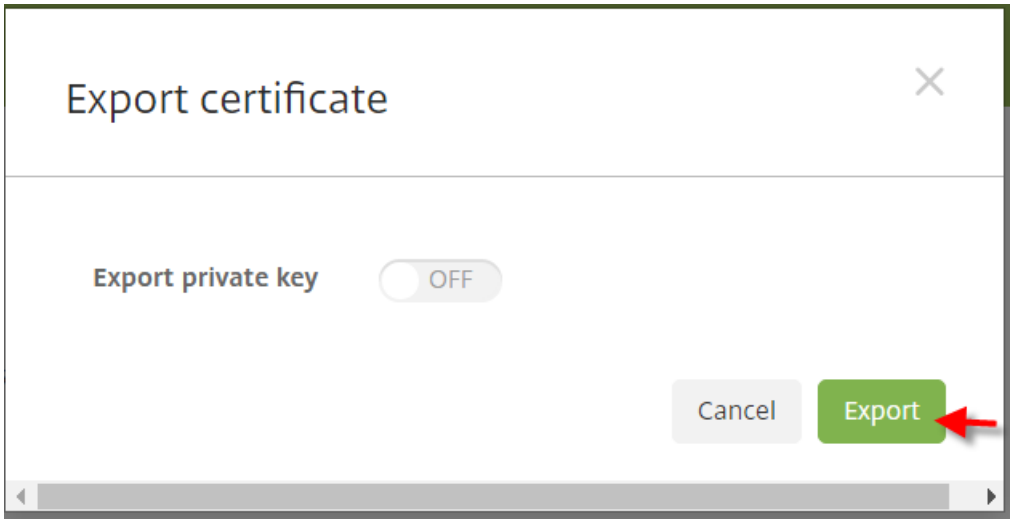
XenMobile がドメインおよび証明書ベースの認証で有効な場合に StoreFront と XenMobile を統合する方法について詳しくは、Support Knowledge Centerを参照してください。

SAML 証明書を **XenMobile Server** からエクスポートする

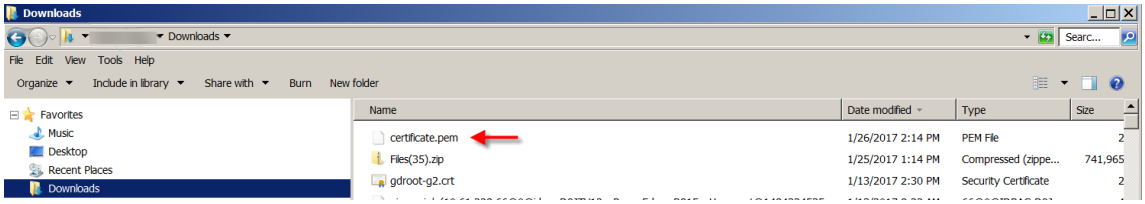
1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ページが開きます。［証明書］をクリックします。
2. XenMobile Server の SAML 証明書を検索します。



3. ［機密キーをエクスポート］が［オフ］に設定されていることを確認します。［エクスポート］をクリックして、証明書をダウンロードディレクトリにエクスポートします。

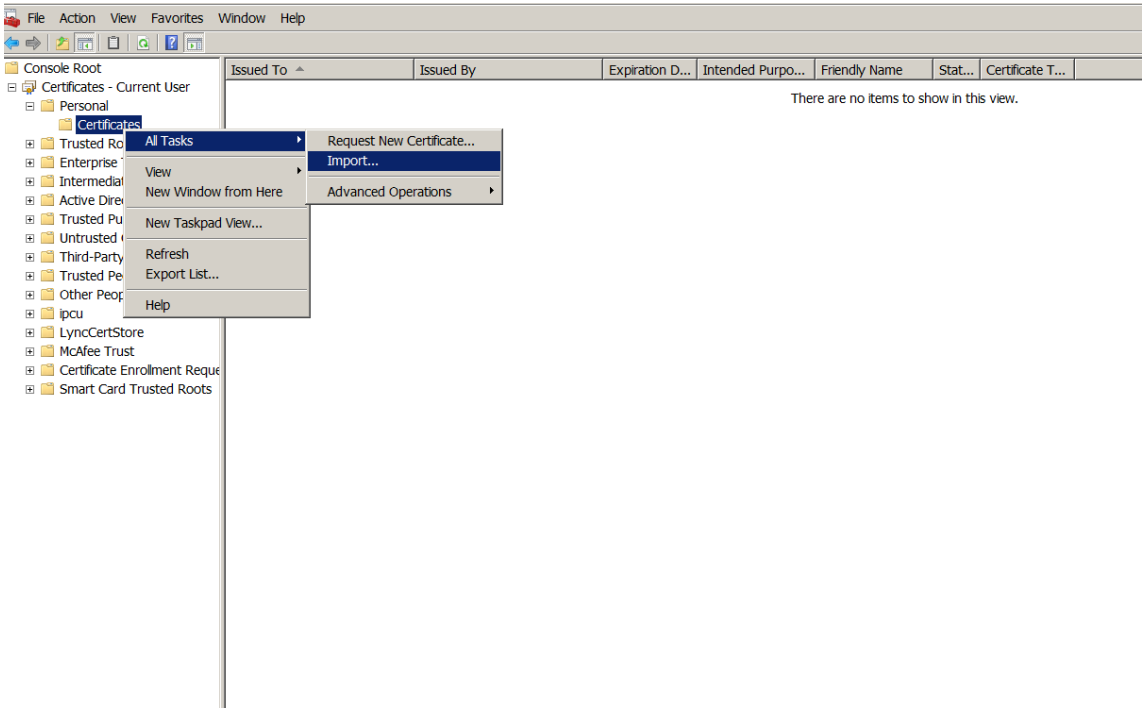


4. ダウンロードディレクトリで証明書を検索します。証明書は PEM 形式です。

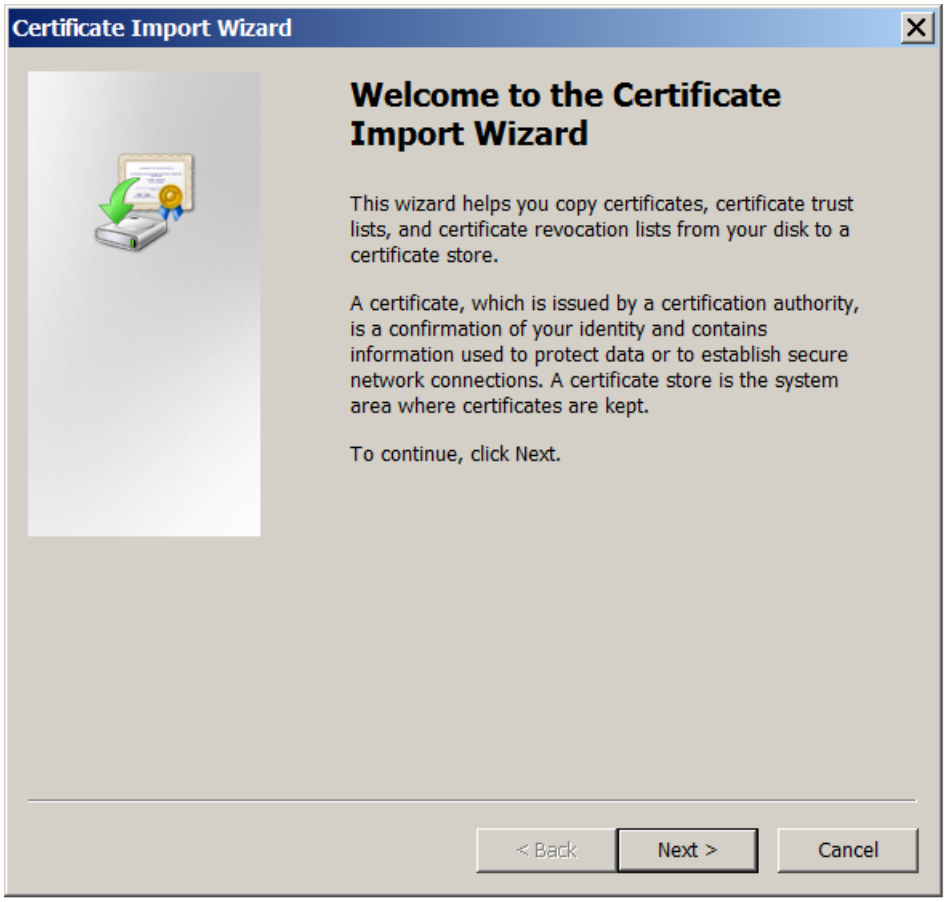


証明書を **PEM** から **CER** に変換する

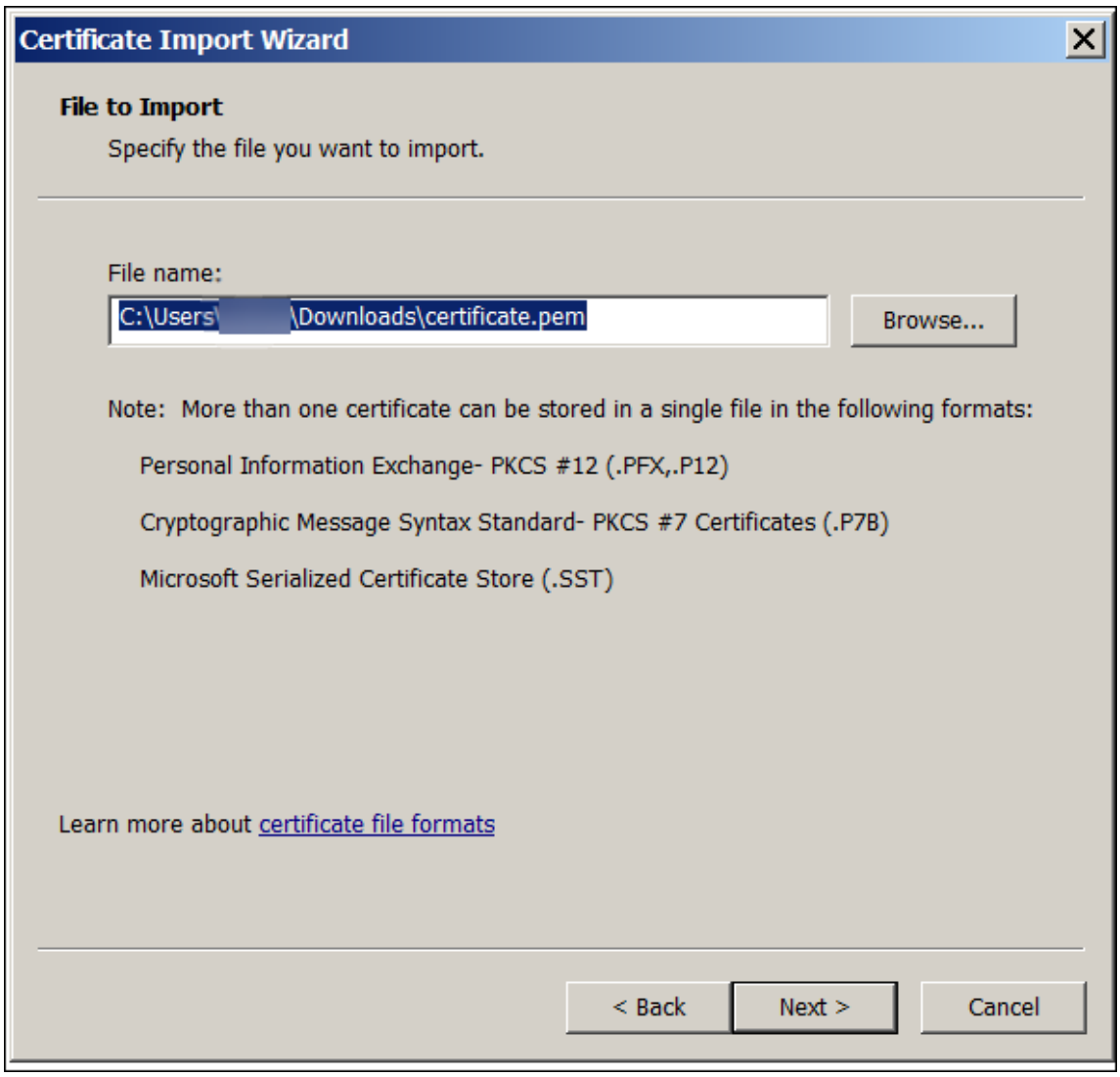
1. Microsoft 管理コンソール（MMC）を開き、［証明書］**>**［すべてのタスク］**>**［インポート］ を右クリックします。



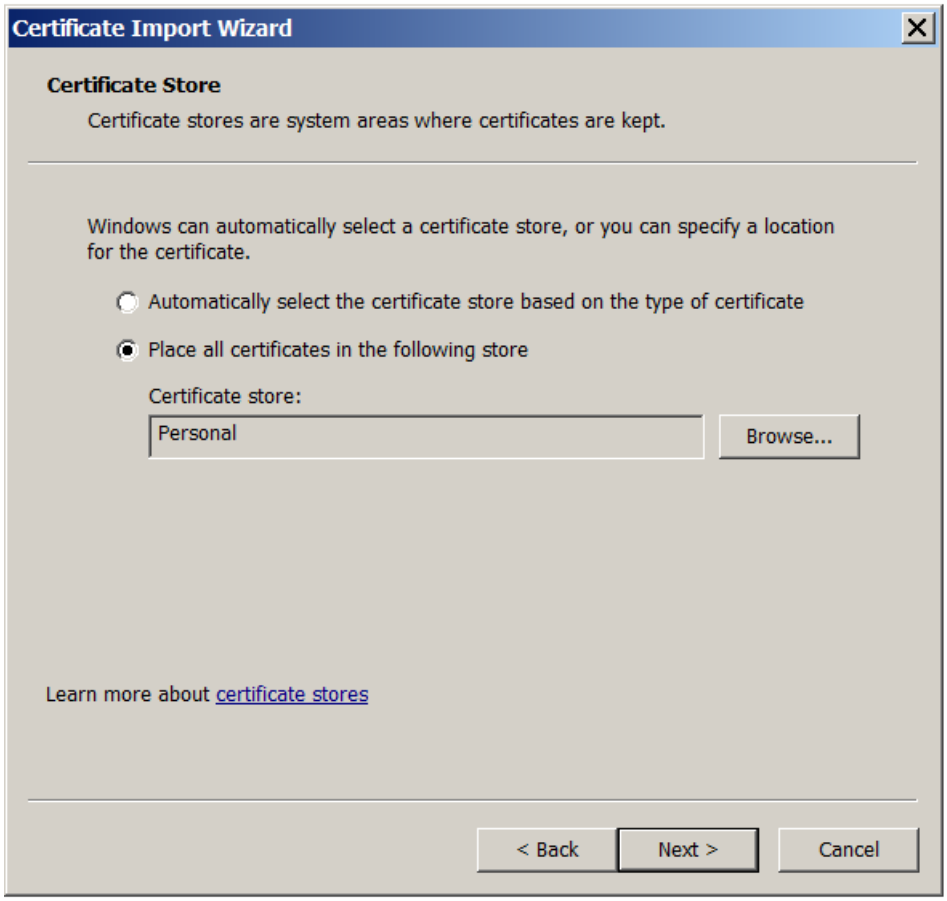
2. 証明書のインポートウィザードが表示されたら、［次へ］ をクリックします。



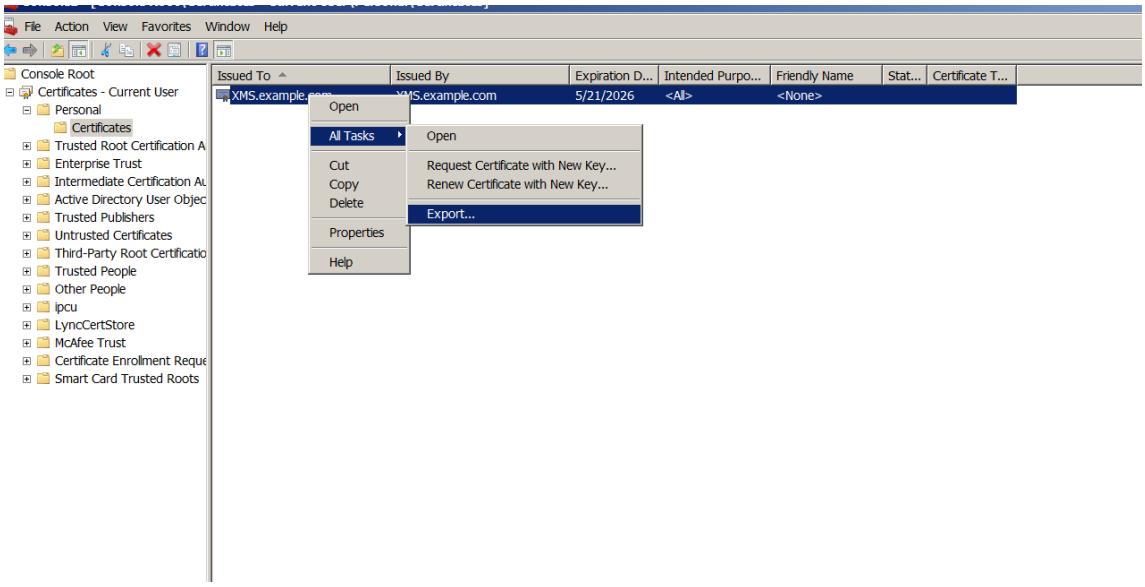
3. ダウンロードディレクトリで証明書を参照します。



4. [証明書をすべて次のストアに配置する] をクリックし、証明書ストアとして [個人] を選択します。[次へ] をクリックします。

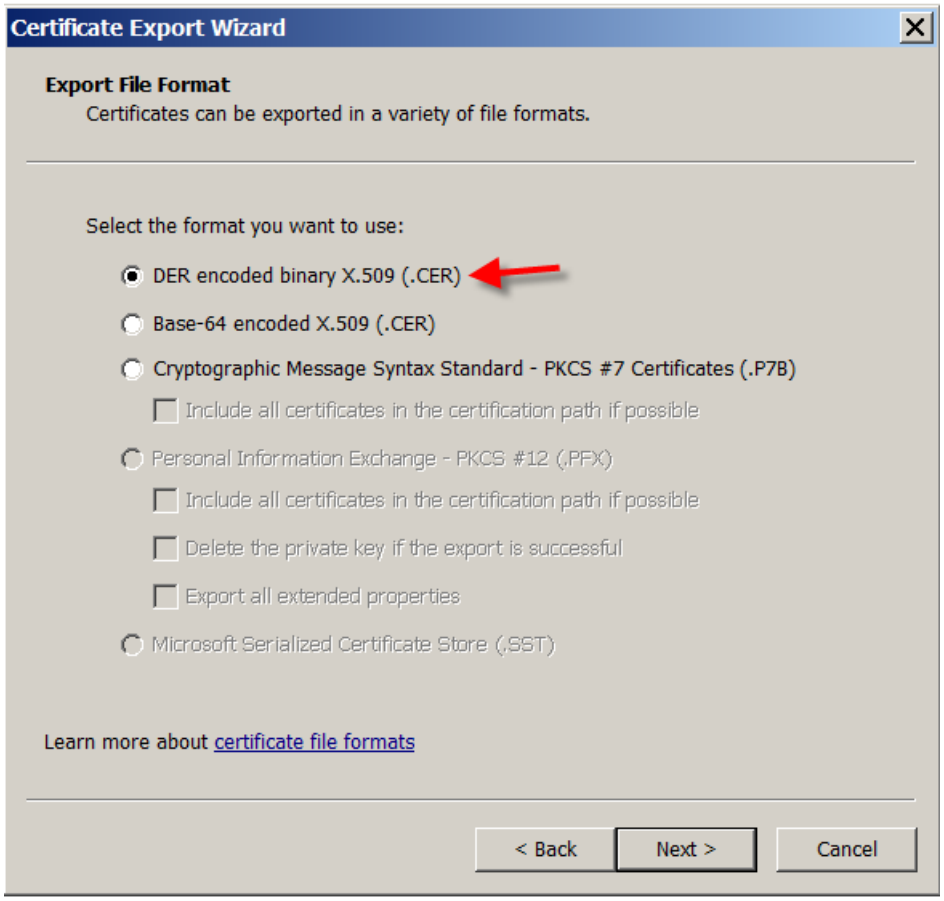


5. 選択した内容を確認し、［完了］ をクリックします。［**OK**］ をクリックして確認ウィンドウを閉じます。
6. MMC で証明書を右クリックし、［すべてのタスク］、［エクスポート］ の順に選択します。

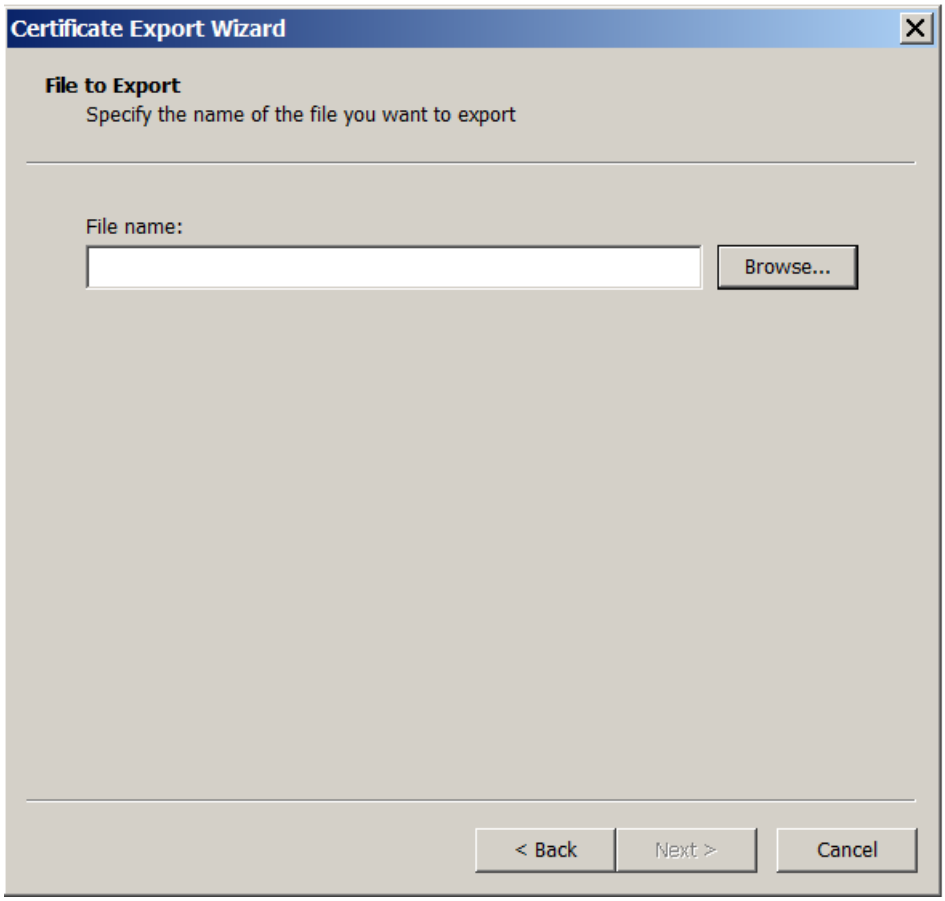


7. 証明書のエクスポートウィザードが表示されたら、［次へ］ をクリックします。

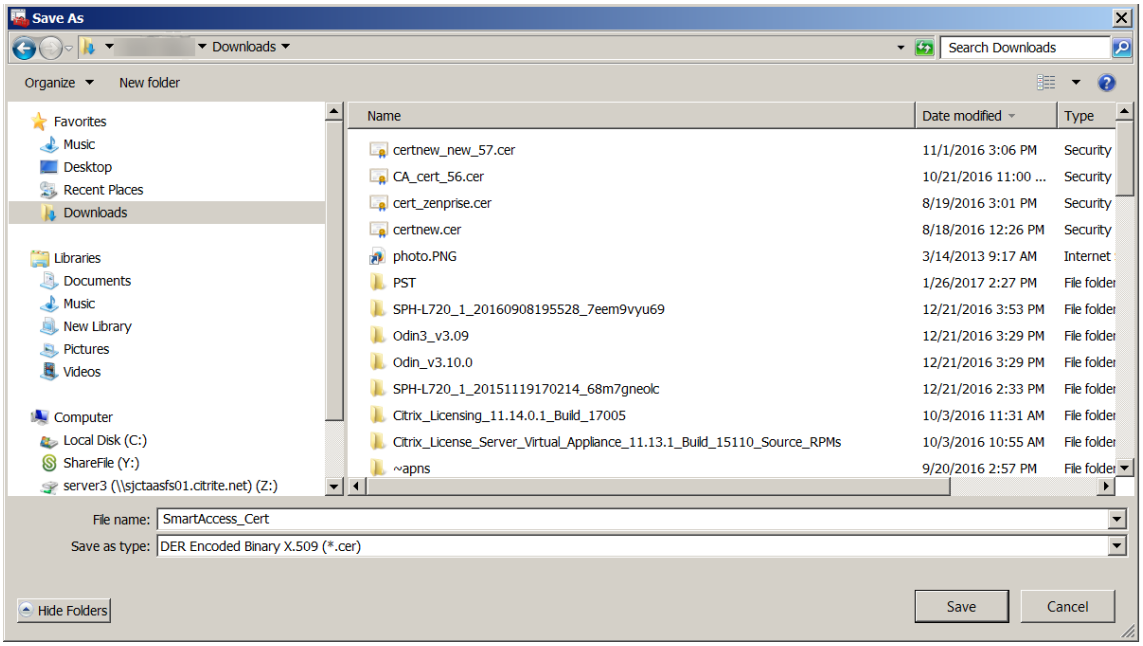
8. [**DER encoded binary X.509 (.CER)**] の形式を選択します。［次へ］ をクリックします。



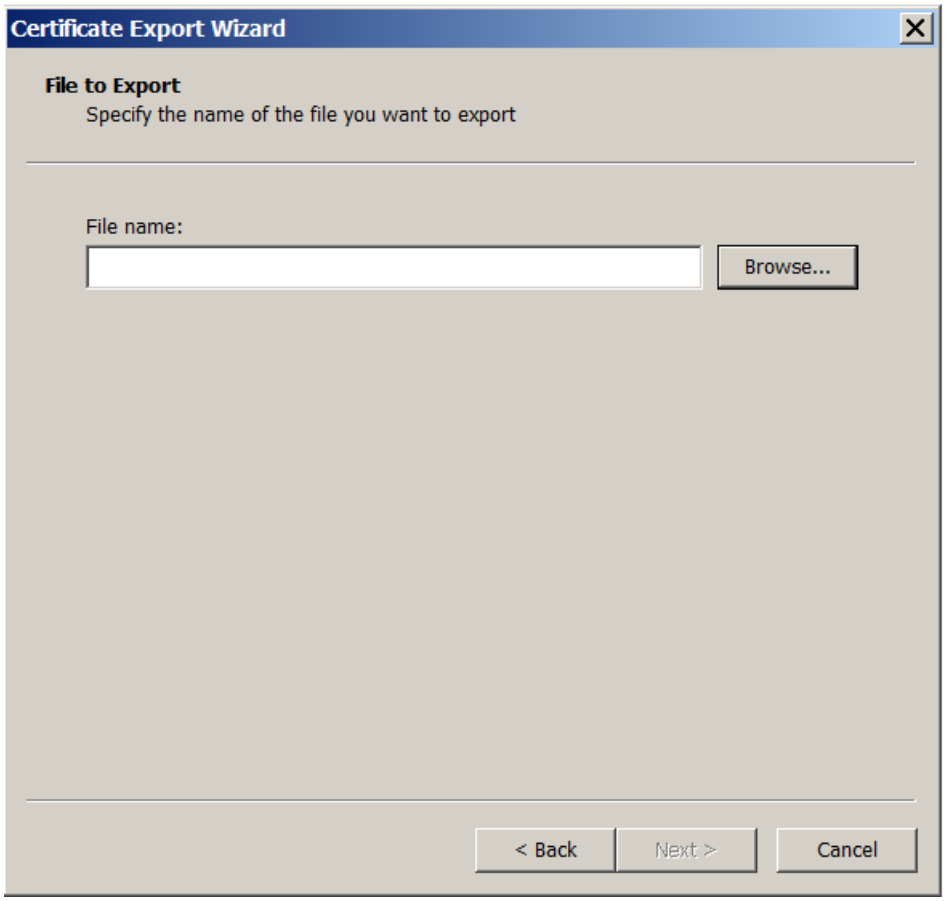
9. 証明書を参照します。証明書の名前を入力し、［次へ］をクリックします。



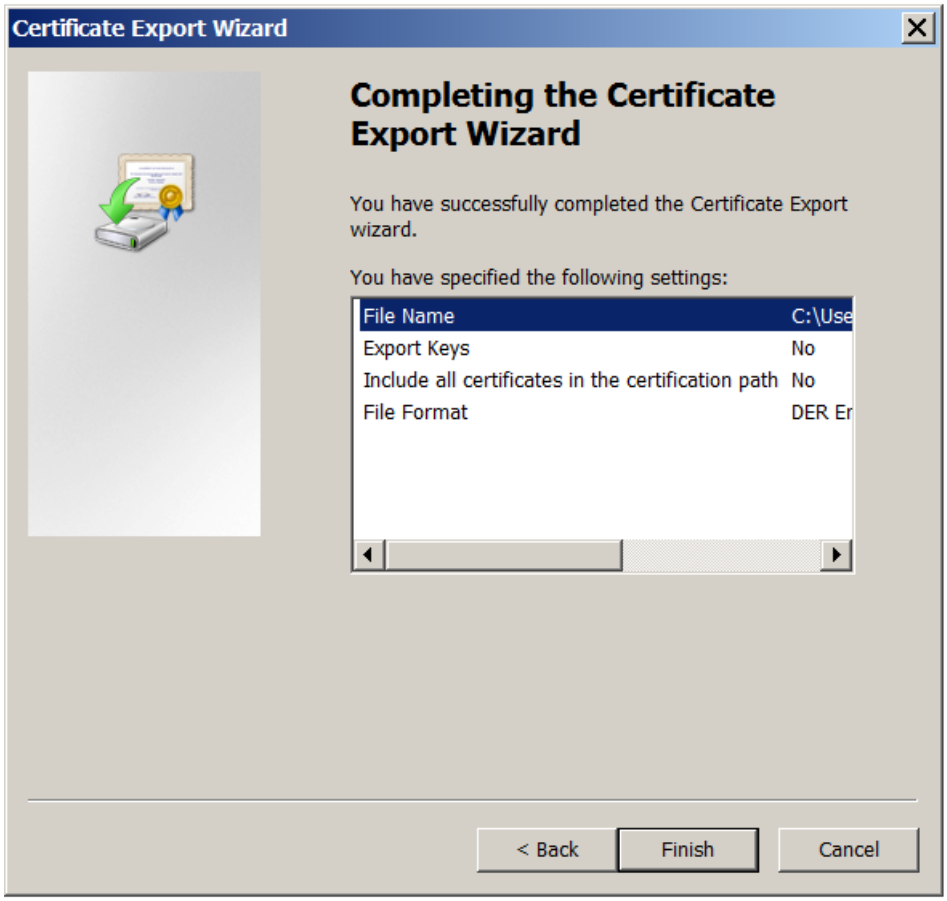
10. 証明書を保存します。



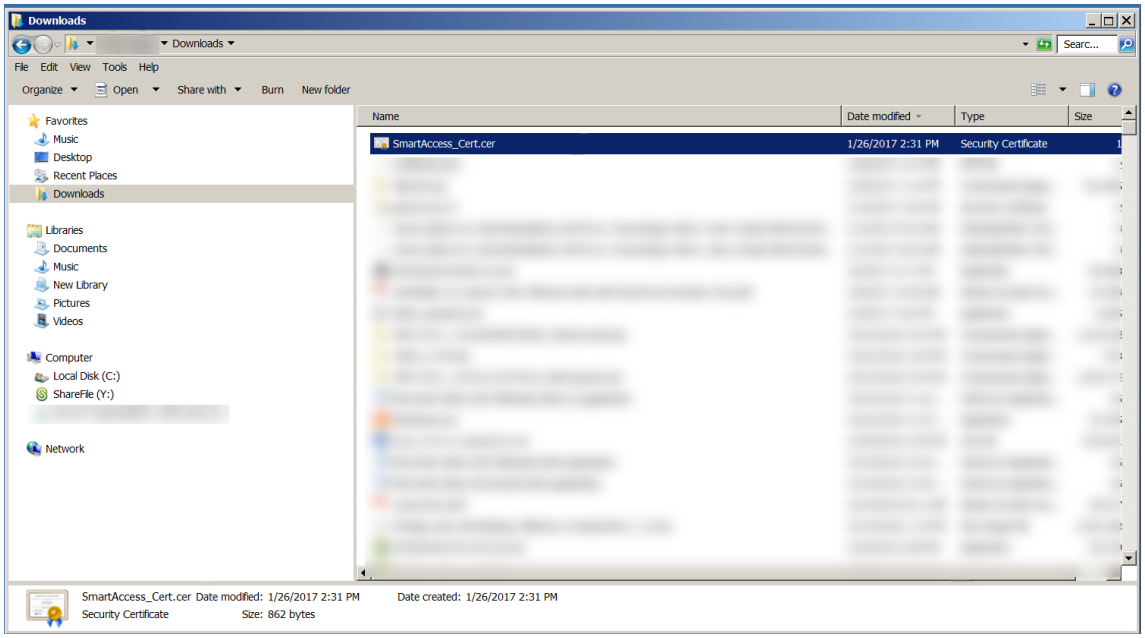
11. 証明書を参照し、［次へ］をクリックします。



12. 選択した内容を確認し、［完了］ をクリックします。［**OK**］ をクリックして確認ウィンドウを閉じます。

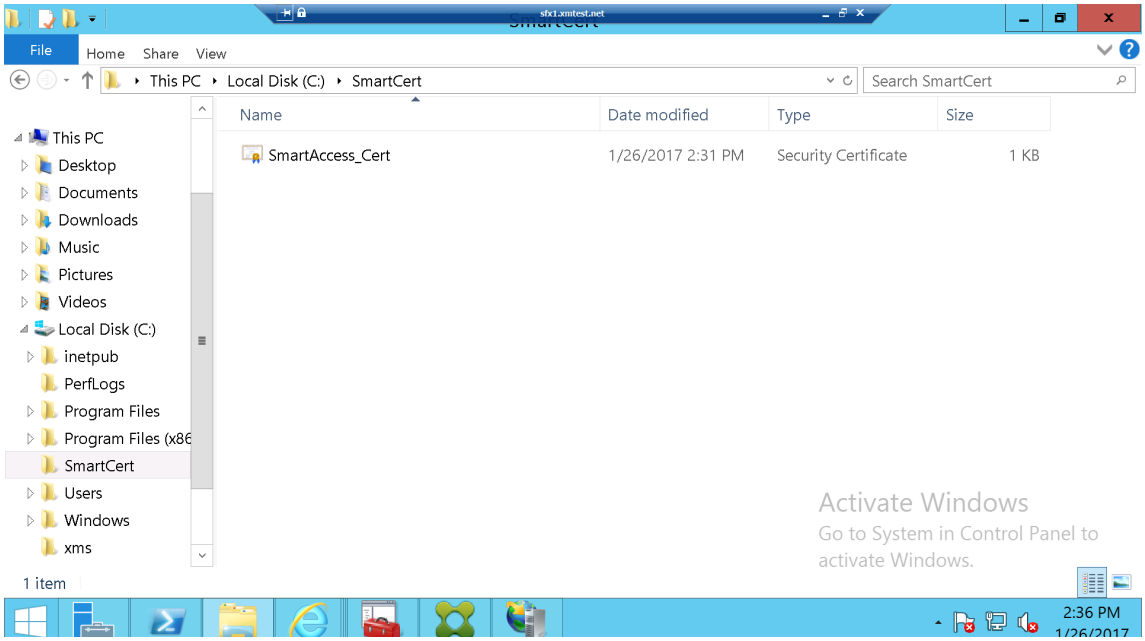


13. ダウンロードディレクトリで証明書を検索します。証明書は CER 形式であることに注意してください。



証明書を **StoreFront** サーバーにコピーする

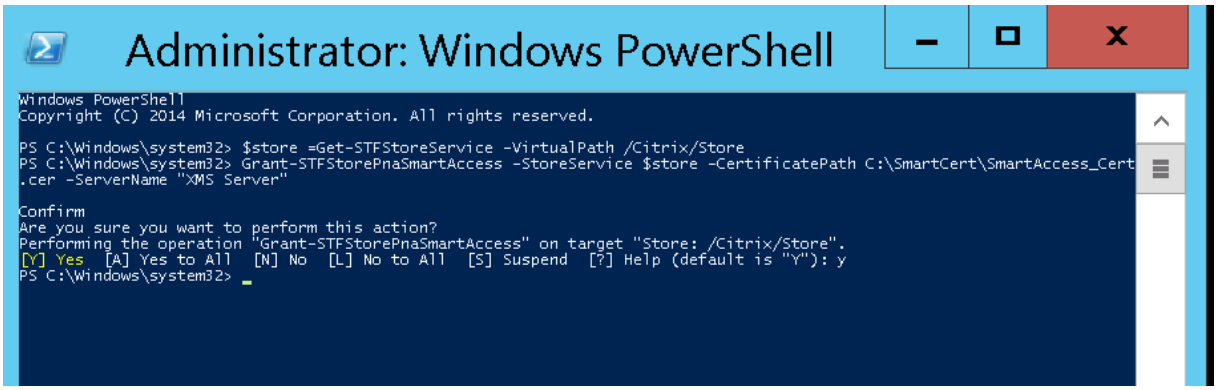
1. StoreFront サーバーで、**SmartCert** という名前のフォルダーを作成します。
2. 証明書を **SmartCert** フォルダーにコピーします。



StoreFront ストアで証明書を構成する

StoreFront サーバーで、次のとおり PowerShell コマンドを実行し、変換された XenMobile Server 証明書をストアに設定します。

```
Grant-STFStorePnaSmartAccess -StoreService $store -CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
```



StoreFront ストアに既存の証明書が存在する場合は、次の PowerShell コマンドを実行して証明書を無効にします。

```
Revoke-STFStorePnaSmartAccess -StoreService $store -All
```

あるいは、StoreFront サーバー上で次の PowerShell コマンドのいずれかを実行して、StoreFront ストア上の既存の証明書を取り消すこともできます。

- 名前で取り消す:

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess -StoreService $store -ServerName "My XM Server"
```

- 拇印で取り消す:

```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess -StoreService $store -CertificateThumbprint "ReplaceWithThumbprint"
```

- サーバーオブジェクトで取り消す:

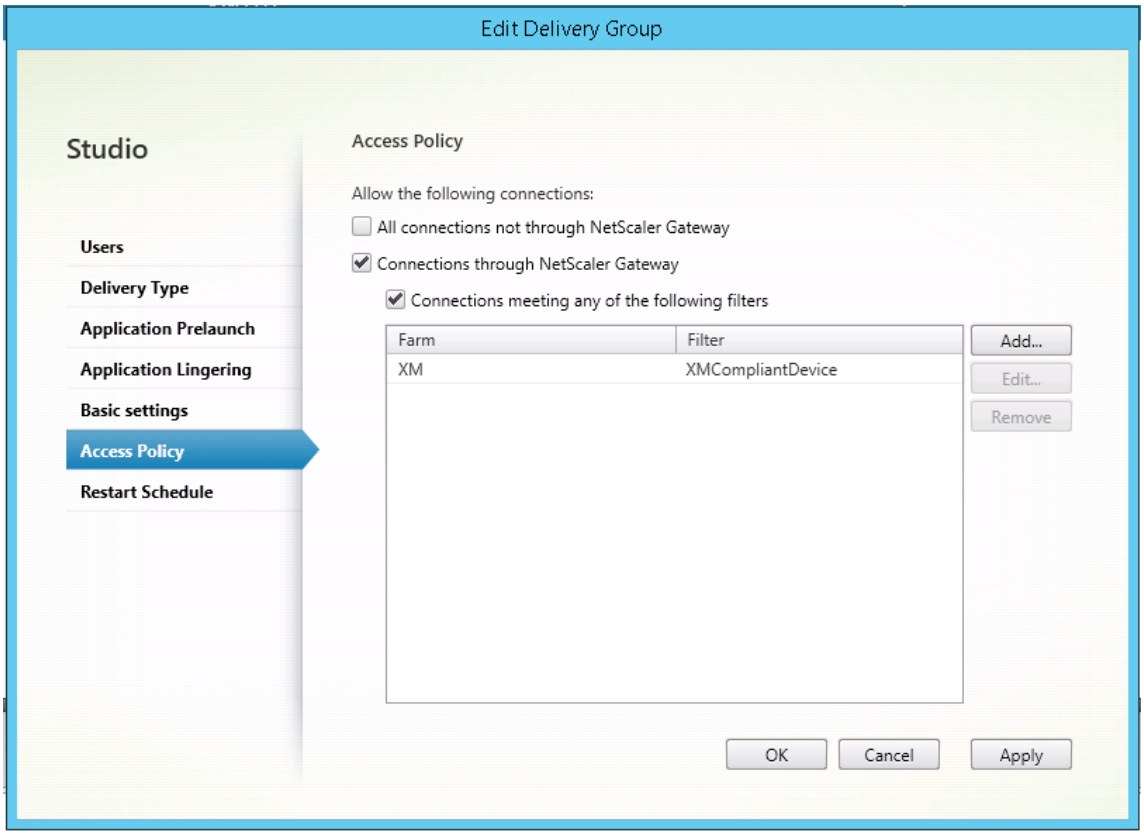
```
$store = Get-STFStoreService -VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess -StoreService $store

Revoke-STFStorePnaSmartAccess -StoreService $store -SmartAccess $access.AccessConditionsTrusts[0]
```

Virtual Apps and Desktops での SmartAccess ポリシーの構成

HDX アプリを配信するデリバリーグループに必要な SmartAccess ポリシーを追加するには、次の手順を行います。

1. Virtual Apps and Desktops サーバーで、Citrix Studio を開きます。
2. Studio のナビゲーションペインで ［デリバリーグループ］ を選択します。
3. アプリを配信するグループまたはアクセスを制御するアプリを選択します。［操作］ ペインの ［デリバリーグループの編集］ を選択します。
4. ［アクセスポリシー］ ページで、 ［**NetScaler Gateway** を経由する接続］ と ［次のいずれかに一致する接続］ を選択します。
5. ［追加］ をクリックします。

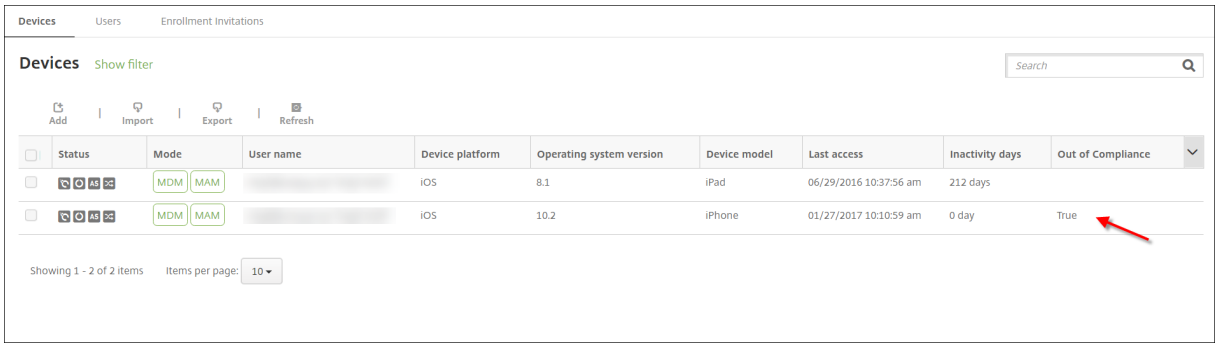
6. ［ファーム］ が「**XM**」で、［フィルター］ が「**XMCompliantDevice**」のアクセスポリシーを追加します。



7. ［適用］ をクリックして行った変更を適用しウィンドウを開いたままにするか、［**OK**］をクリックして変更を適用しウィンドウを閉じます。

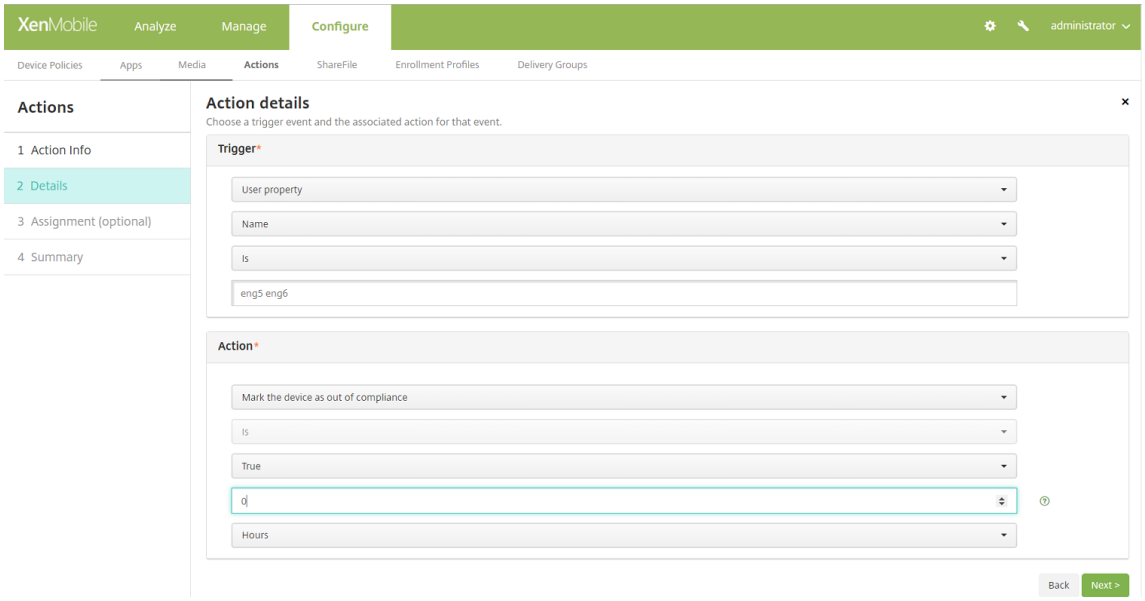
XenMobile で自動化された操作を設定する

HDX アプリのデリバリーグループに設定した SmartAccess ポリシーは、デバイスがコンプライアンス違反である場合にそのデバイスへのアクセスを拒否します。自動化された操作を使用して、そのデバイスをコンプライアンス違反としてマークします。



1. XenMobile コンソールで、［構成］の［操作］ をクリックします。［アクション］ ページが開きます。

2. [追加] をクリックして操作を追加します。[アクション情報] ページが開きます。
3. [アクション情報] ページで、操作の名前と説明を入力します。
4. [次へ] をクリックします。[アクションの詳細] ページが開きます。次の例では、ユーザープロパティ名が **eng5** または **eng6** の場合に、デバイスをただちにコンプライアンス違反と指定するトリガーを作成します。



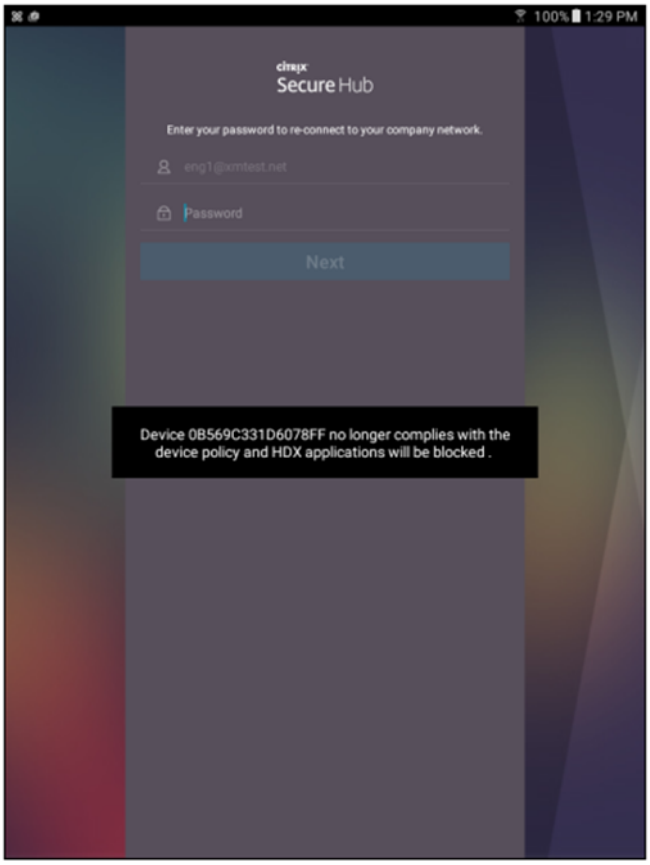
5. [トリガー] 一覧で、[デバイスプロパティ]、[ユーザープロパティ]、または [インストール済みアプリ名] を選択します。SmartAccess はイベントトリガーをサポートしていません。
6. [アクション] 一覧で、以下を実行します。
   - [コンプライアンス違反としてデバイスをマーク] を選択します。
   - [=] を選択します。
   - [真] を選択します。
   - トリガー条件が満たされたときに、ただちにデバイスをコンプライアンス違反としてマークされるように操作を設定するには、時間枠を **0** に設定します。
7. XenMobile デリバリーグループまたはこの操作を適用するグループを選択します。
8. 操作の概要を確認します。
9. [次へ] をクリックし、[保存] をクリックします。

デバイスがコンプライアンス違反としてマークされると、HDX アプリは Secure Hub ストアに表示されなくなります。ユーザーはアプリにサブスクライブされなくなります。デバイスに通知は送信されず、Secure Hub ストアでは HDX アプリが以前は利用可能であったことは示されません。

デバイスがコンプライアンス違反としてマークされたときにユーザーに通知する場合は、通知を作成し、その通知を送信する自動化された操作を作成します。

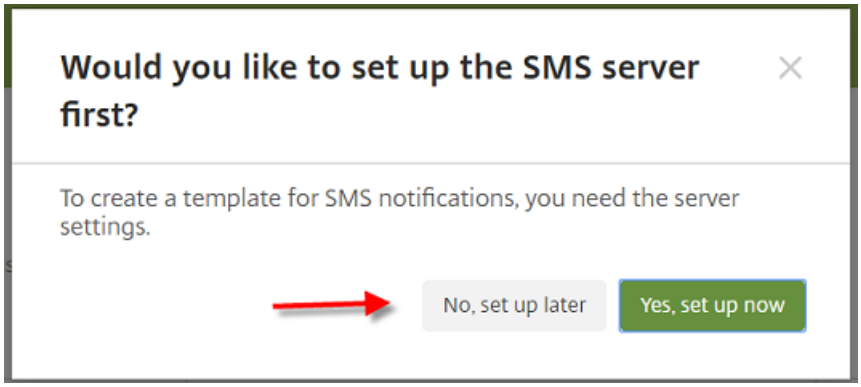
この例では、デバイスがコンプライアンス違反としてマークされたときに「Device serial number or telephone

number no longer complies with the device policy and HDX applications will be blocked.」という通知を作成して送信します。



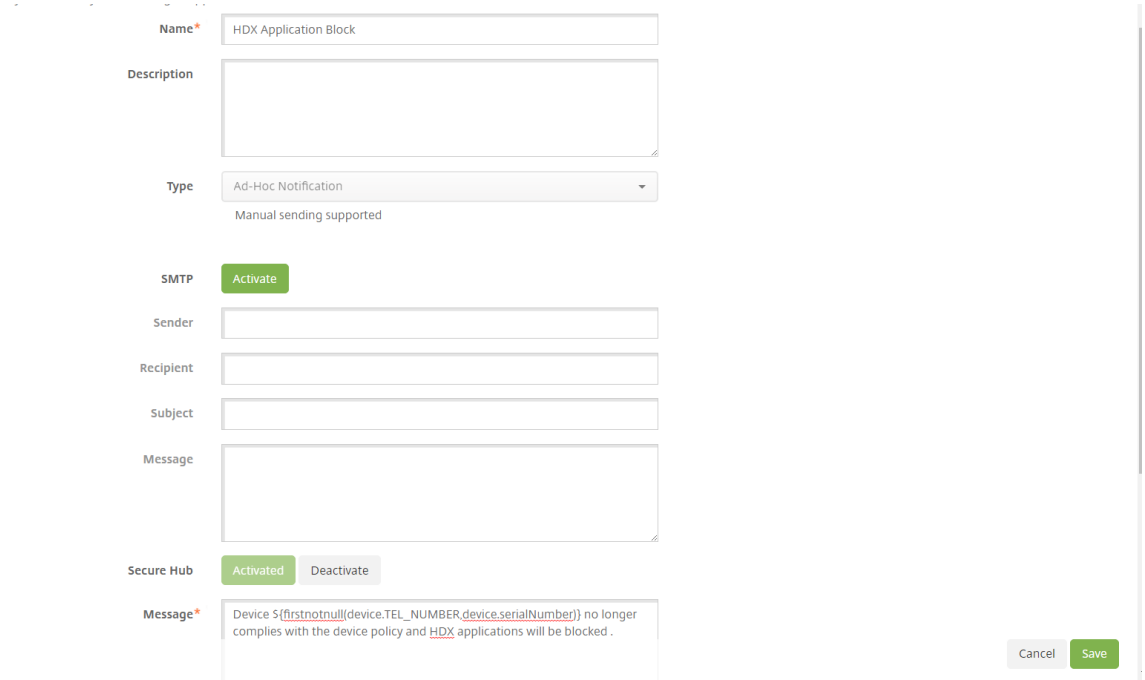
デバイスがコンプライアンス違反としてマークされたときにユーザーに表示される通知を作成する

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［通知テンプレート］ をクリックします。［通知テンプレート］ ページが開きます。
3. ［通知テンプレート］ ページで ［追加］ をクリックして追加します。
4. 最初に SMS サーバーを設定するように求められたときは、［いいえ、あとでセットアップする］ をクリックします。



5. 次の設定を構成します。

   - 名前: HDX アプリケーションブロック
   - 説明: デバイスがコンプライアンス違反である場合のエージェント通知
   - 種類: アドホック通知
   - **Secure Hub**: アクティブ
   - メッセージ: Device ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

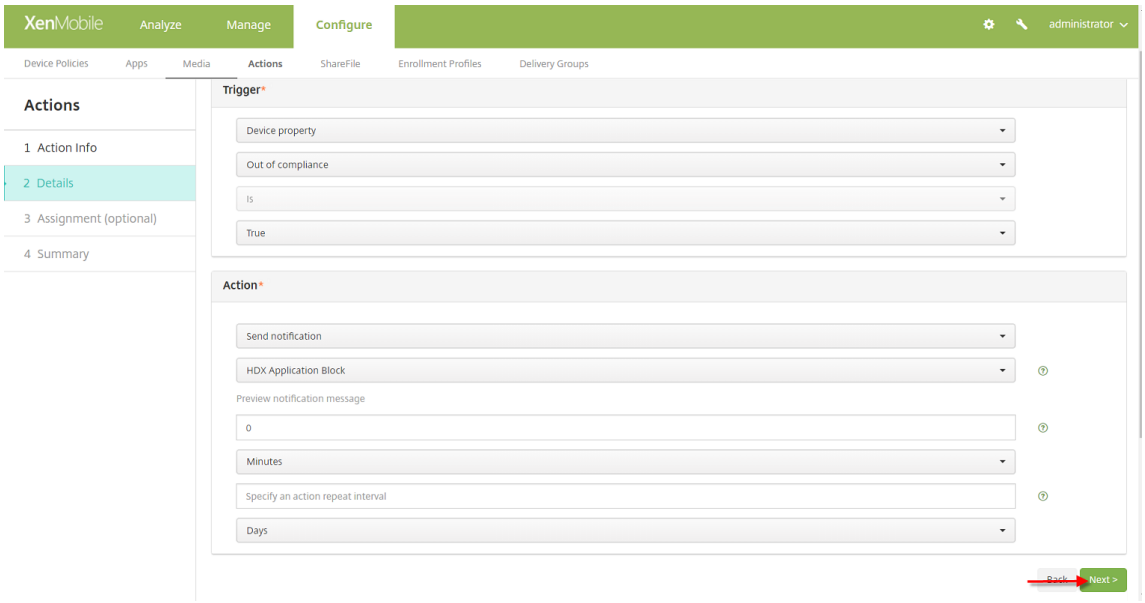


6. [保存] をクリックします。

デバイスがコンプライアンス違反としてマークされたときに通知を送信する操作を作成する

1. XenMobile コンソールで、[構成] の [操作] をクリックします。[アクション] ページが開きます。
2. [追加] をクリックして操作を追加します。[アクション情報] ページが開きます。

3. [アクション情報] ページで、操作の名前と説明を入力します。
   - 名前: HDX ブロック通知
   - 説明: デバイスがコンプライアンス違反である場合の HDX ブロック通知
4. [次へ] をクリックします。[アクションの詳細] ページが開きます。
5. [トリガー] 一覧で、以下を実行します。
   - [デバイスプロパティ] を選択します。
   - [コンプライアンス違反] を選択します。
   - [=] を選択します。
   - [真] を選択します。



6. [操作] 一覧で、トリガーが満たされたときに実行される操作を指定します。
   - [通知を送信] を選択します。
   - 作成した通知である [**HDX Application Block**] を選択します。
   - **0** を選択します。この値を 0 に設定すると、トリガー条件が満たされるとすぐに通知が送信されます。
7. XenMobile デリバリーグループまたはこの操作を適用するグループを選択します。この例では、[**AllUsers**] を選択します。
8. 操作の概要を確認します。
9. [次へ] をクリックし、[保存] をクリックします。

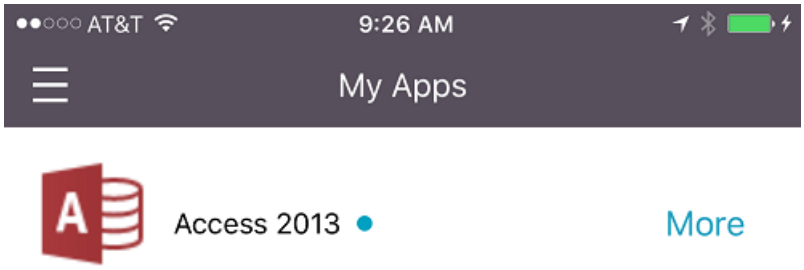
自動化された操作の設定について詳しくは、「自動化された操作」を参照してください。

ユーザーが **HDX** アプリに再度アクセスする方法

デバイスがコンプライアンスを再び満たすようになると、ユーザーは HDX アプリに再びアクセスできます。

1. デバイスで、Secure Hub ストアにアクセスして、ストア内のアプリを更新します。
2. 対象のアプリに移動して ［追加］ をタップします。

アプリが追加されると、［マイアプリ］の横に青い点を付けて表示され、新しくインストールされたアプリであることを示します。



メディアの追加

August 22, 2019

XenMobile にメディアを追加して、ユーザーデバイスにそのメディアを展開できます。XenMobile を使用して、Apple Volume Purchase Program（VPP）を介して取得した iBooks を展開することができます。

XenMobile で VPP アカウントを構成すると、購入済みブックや無料ブックが ［構成］ **>** ［メディア］ に表示されます。［メディア］ ページでデリバリーグループを選択し、展開規則を指定して、iOS デバイスに展開する iBooks を構成します。

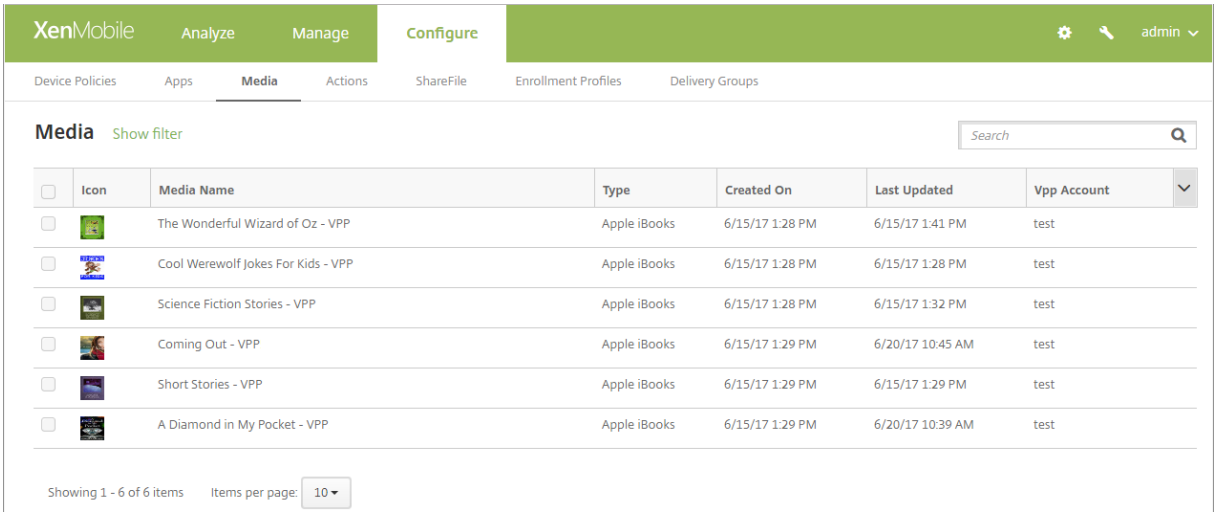
ユーザーが初めて iBook を受信し、VPP ライセンス契約に同意したときに、展開されたブックがデバイスにインストールされます。ブックは Apple iBook アプリに表示されます。ユーザーからブックライセンスの割り当てを解除したり、デバイスからブックを削除することはできません。XenMobile では、iBooks は必須メディアとしてインストールされます。インストールされたブックがユーザーによってデバイスから削除されても、そのブックは iBook アプリ内に保持されて、いつでもダウンロードできます。

前提条件

- iOS デバイス（最小バージョン iOS 8）
- 「iOS Volume Purchase Plan の設定」の説明に従って、XenMobile で iOS VPP を構成します。

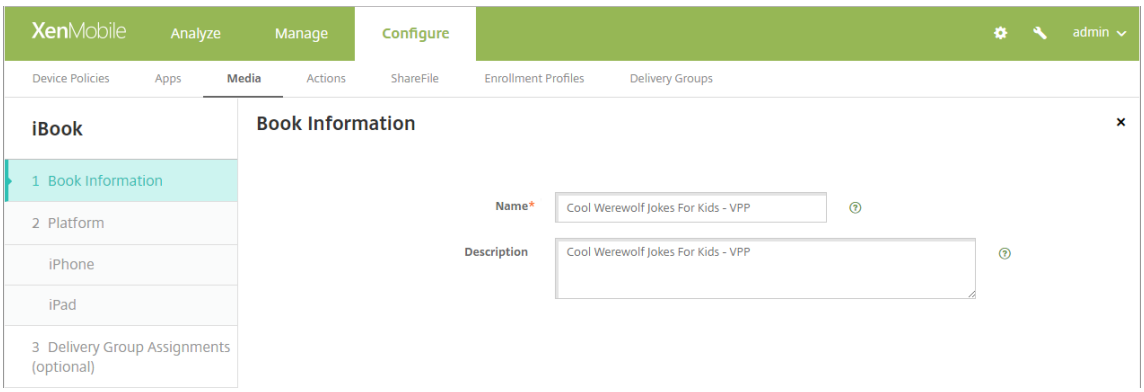
iBooks の構成

VPP を介して取得した iBooks は、［構成］>［メディア］ ページに表示されます。



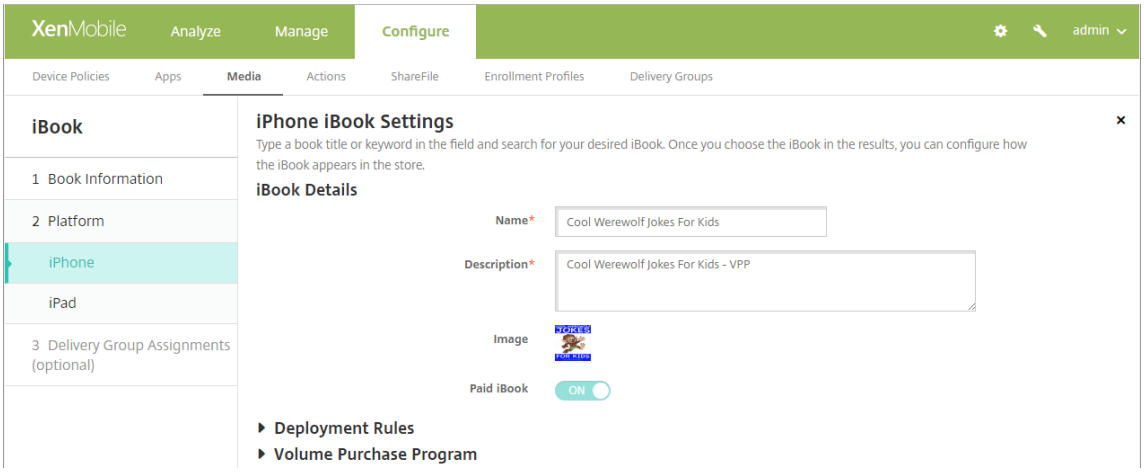
展開する **iBooks** を構成するには、次の手順を実行します

1. ［構成］>［メディア］ の順に選択し、iBooks を選択して ［編集］ をクリックします。［ブック情報］ ページが開きます。

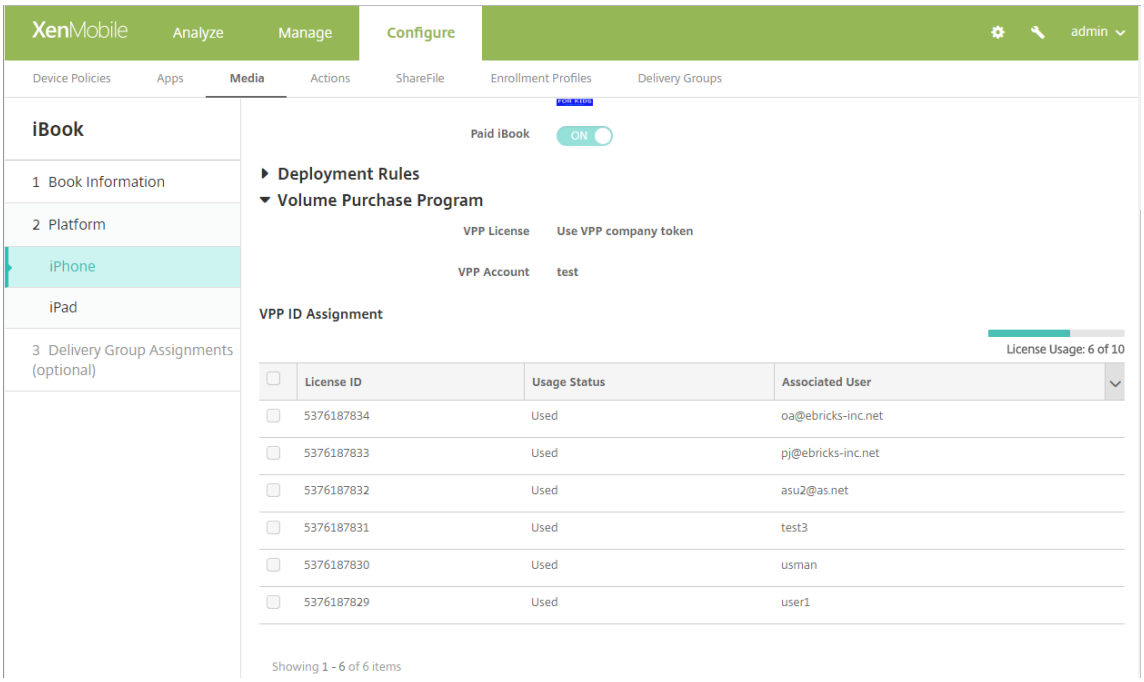


   名前と説明は、XenMobile コンソールとログにのみ表示されます。

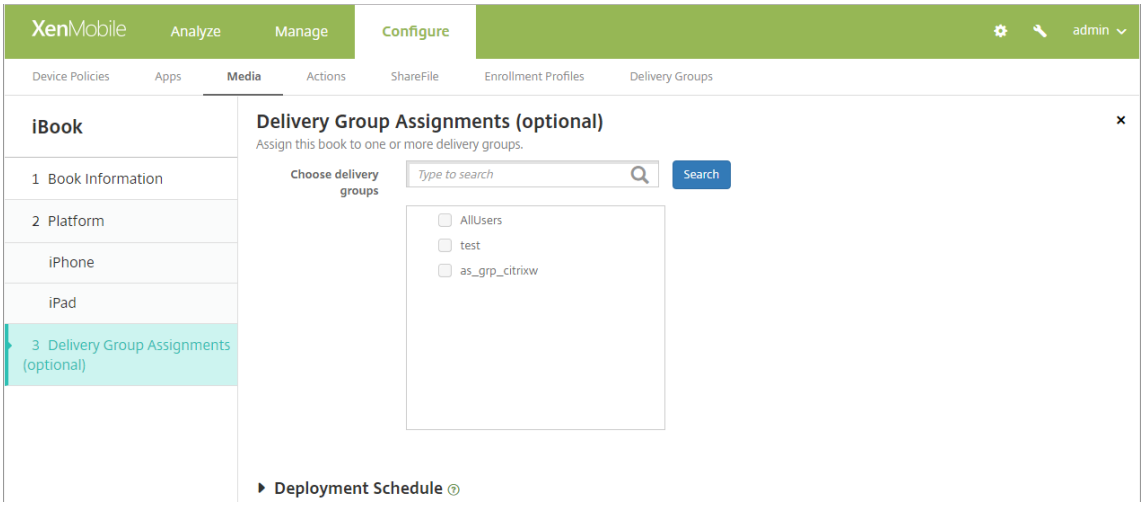
2. ［**iPhone iBook** の設定］ ページと ［**iPad iBook** の設定］ ページで、iBook の名前と説明は任意に変更できますが、これらの設定は変更しないことをお勧めします。画像は参考用であり、編集することはできません。［購入済み **iBook**］ には、VPP を介して購入した iBook であることが表示されます。



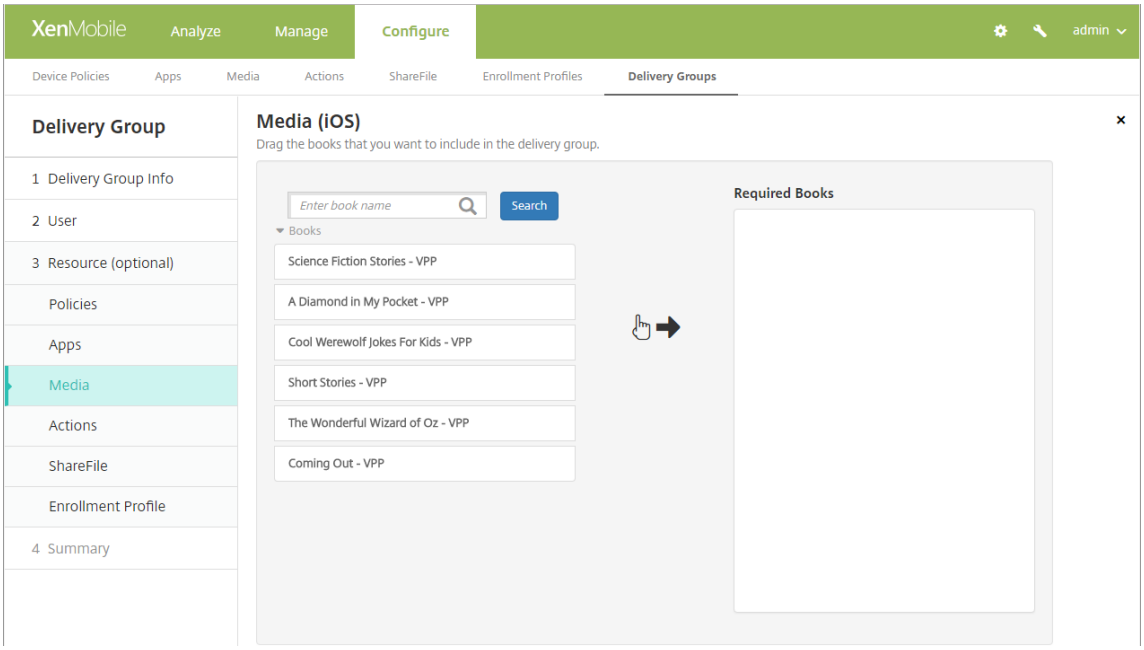
展開規則を指定したり、VPP 情報を表示したりすることもできます。



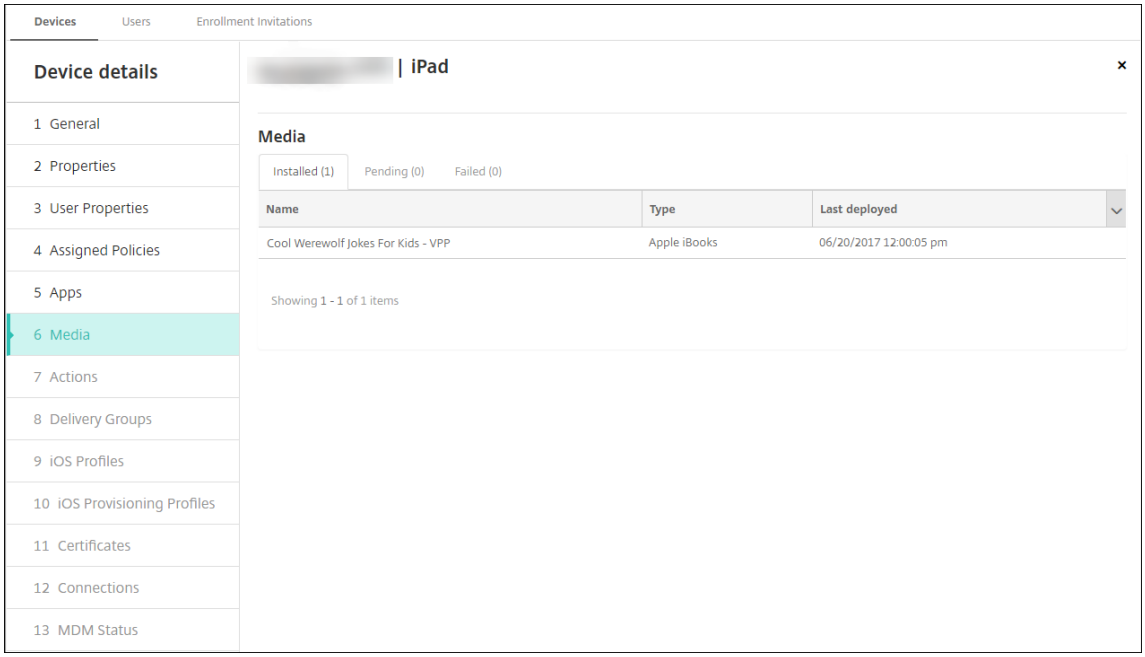
3. オプションで、iBook をデリバリーグループに割り当てて、展開スケジュールを設定することもできます。



また、［構成］>［デリバリーグループ］ の順に選択し、［メディア］ タブでデリバリーグループに iBooks を割り当てることもできます。XenMobile では必須ブックの展開のみがサポートされます。

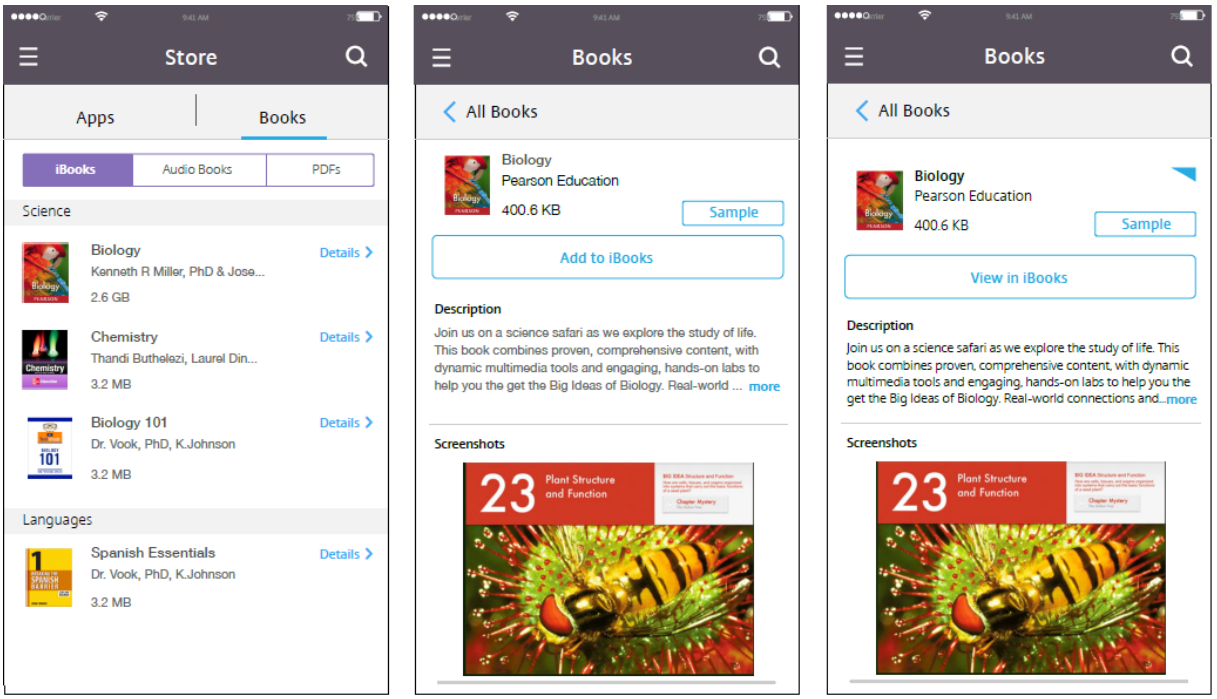


4.［管理］>［デバイス］ の順に選択し、［メディア］ タブを使用して展開状況を表示します。



> 注:
>
> [構成] > [メディア] ページで、ブックを選択して [削除] をクリックすると、XenMobile ではそのブックが一覧から削除されます。ただし、VPP から削除されない限り、XenMobile が次に VPP と同期するときに、そのブックは再び一覧に表示されます。ブックを一覧から削除しても、デバイスからは削除されません。

iBooks は、次の例のようにユーザーデバイスに表示されます。



リソースの展開

January 24, 2020

デバイスの構成および管理は、通常 XenMobile コンソールでリソース（ポリシー、アプリ、メディア）および操作を作成し、デリバリーグループを使用してそれらをパッケージ化します。XenMobile がリソースおよび操作をデリバリーグループでデバイスにプッシュする順番は、展開順と呼ばれます。ここでは以下の方法について説明します:

- デリバリーグループを追加、管理、および展開するには
- デリバリーグループ内でリソースと操作の展開順序を変更するには
- ユーザーが複数のデリバリーグループに属していて、そのデリバリーグループにポリシーの重複または矛盾があるときには、XenMobile が展開順序を決定します。

デリバリーグループによって、ポリシー、アプリ、メディア、アクションを組み合わせて展開する対象となるデバイスのユーザーのカテゴリを指定します。通常、デリバリーグループへの追加は、ユーザーの会社、国、部門、オフィスの住所、役職などの特性に基づいて行われます。デリバリーグループを使用することにより、どのユーザーがどのリソースをいつ取得するかを詳細に管理できます。デリバリーグループは、全員に展開することや、より絞り込んで定義したユーザーグループに展開することができます

デリバリーグループへの展開とは、サポート対象の iOS デバイスおよび Windows デバイスを持つすべてのユーザーにプッシュ通知を送信することを意味します。そのユーザーは XenMobile に再接続するデリバリーグループに属している必要があります。デバイスを再評価し、デリバリーグループの一部であるポリシー、アプリ、メディア、アクションを展開できるようにします。

Android デバイスを持つユーザーについては、既に接続済みであればすぐにそのリソースを受信します。接続していない場合は、スケジューリングポリシーに基づいて、次に接続するときにリソースを受信します。

デフォルトの AllUsers デリバリーグループは、XenMobile をインストールして構成するときに作成されます。このグループには、すべてのローカルユーザーと Active Directory ユーザーが含まれます。AllUsers グループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

展開順の作成

展開順は XenMobile がリソースをデバイスにプッシュする順番です。展開順は XenMobile の MDM モードでのみサポートされます。

展開順を判断する際、XenMobile はポリシー、アプリ、メディア、操作、デリバリーグループにフィルターを適用して条件（展開規則、展開スケジュール）を制御します。デリバリーグループを追加する前に、展開の目的に合わせてこのセクションの情報を参照してください。

以下は、展開順に関する主な概念の要約です。

- 展開順： XenMobile がリソース（ポリシー、アプリ、メディア）および操作をデバイスにプッシュする順序です。契約条件やソフトウェアインベントリのような一部のポリシーの展開順は、ほかのリソースに影響を与

えません。アクションが展開される順序はほかのリソースに影響を与えません。したがって、XenMobile でリソースが展開されるとき、リソースの位置は無視されます。

- 展開規則： XenMobile は、デバイスプロパティで指定された展開規則を使って、ポリシー、アプリ、メディア、操作、デリバリーグループをフィルターします。たとえば、ドメイン名が特定の値に一致した場合、展開規則が展開パッケージをプッシュするよう指定できます。
- 展開スケジュール： XenMobile では、ポリシー、アプリ、メディア、操作に対して指定する展開スケジュールを使用して、これらのアイテムの展開を制御できます。展開が即座に実行されるか、特定の日時に実行されるか、展開条件に従って実行されるかを指定できます。

次の表は、各種オブジェクトとリソースのフィルターと制御条件を示しています。展開規則はデバイスプロパティに基づきます。

オブジェクト/リソース	デバイスプラットフォーム	展開規則	展開スケジュール	ユーザー/グループ
デバイスポリシー	☒	☒	☒	-
アプリ	☒	☒	☒	-
メディア	☒	☒	☒	-
操作（アクション）	-	☒	☒	-
デリバリーグループ	-	☒	-	☒

通常の環境では、複数のデリバリーグループが単一ユーザーに割り当てられ、次のような状況が発生する可能性があります：

- デリバリーグループ内に重複したオブジェクトが存在する。
- 1 つ以上のデリバリーグループが単一ユーザーに割り当てられることによって、特定のポリシーに異なる構成が存在する。

このような状況が発生した場合、XenMobile は、デバイスに配布し実行するすべてのオブジェクトの展開順を計算します。計算の手順はデバイスプラットフォームに共通です。

計算の手順：

1. ユーザーやグループのフィルターおよび展開規則に基づいて、特定のユーザーが存在するすべてのデリバリーグループを判断します。
2. 選択したデリバリーグループ内のすべてのリソース（ポリシー、アプリ、メディア、操作）の順序付き一覧を作成します。その一覧は、デバイスプラットフォーム、展開規則、および展開スケジュールのフィルターに基づいています。順序のアルゴリズムは、次のとおりです：

    a) ユーザー定義の展開順があるデリバリーグループのリソースを、展開順がないデリバリーグループのリソースの前に配置します。この配置の理由は、これらの手順の後に説明します。

b) 同じ条件のデリバリーグループの中から、デリバリーグループ名に従ってリソースを順序付けします。たとえば、デリバリーグループ A のリソースをデリバリーグループ B のリソースの前に配置します。

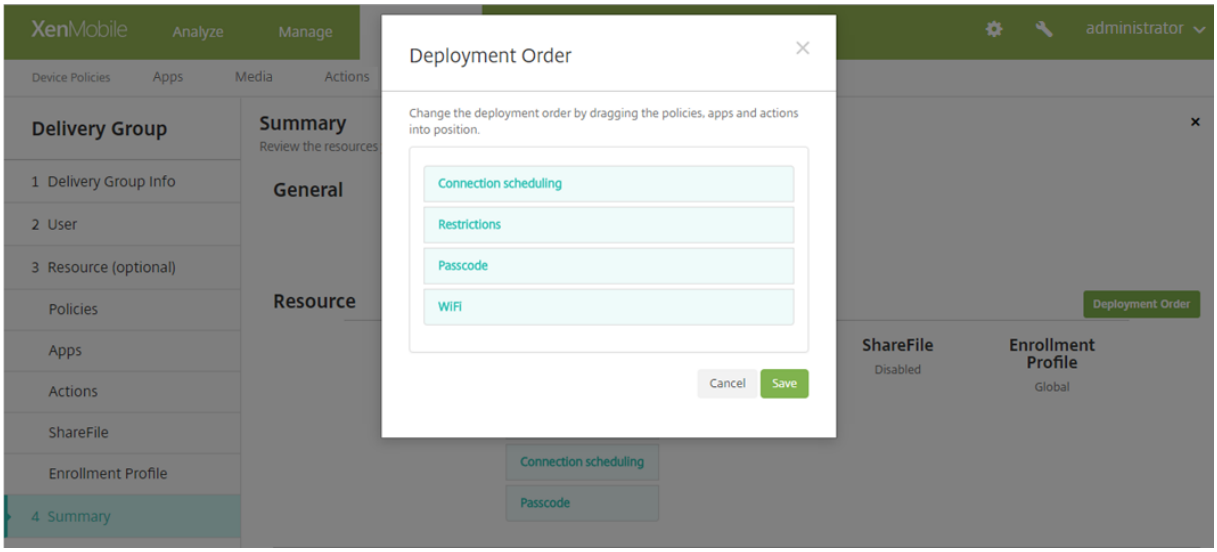
c) 並べ替え中、デリバリーグループのリソースにユーザー定義の展開順が指定されている場合、その順序を保持します。そうでない場合は、デリバリーグループ内でリソースをリソース名で並べ替えることができます。

d) 同じリソースが複数回表示される場合、重複するリソースを削除します。

リソースに関連したユーザー定義の順序を持つリソースを、ユーザー定義の順序のないリソースの前に展開します。リソースは、ユーザーに割り当てられた複数のデリバリーグループに存在する可能性があります。上記の手順で示されたように、計算のアルゴリズムは余分なリソースを削除し、この一覧の最初のリソースのみを配布します。この方法で重複するリソースを削除することによって、XenMobile 管理者が定義する順序を XenMobile に適用します。

たとえば、次のような 2 つのデリバリーグループがあるとします：

- デリバリーグループ、Account Manager1：リソースの順序が未指定です。**WiFi** ポリシーおよびパスコードポリシーを含みます。
- デリバリーグループ、Account Manager2：リソースの順序が指定です。接続スケジュールポリシー、制限ポリシー、パスコードポリシー、および **WiFi** ポリシーを含みます。この事例では、**WiFi** ポリシーの前にパスコードポリシーを配信するように指定されます。



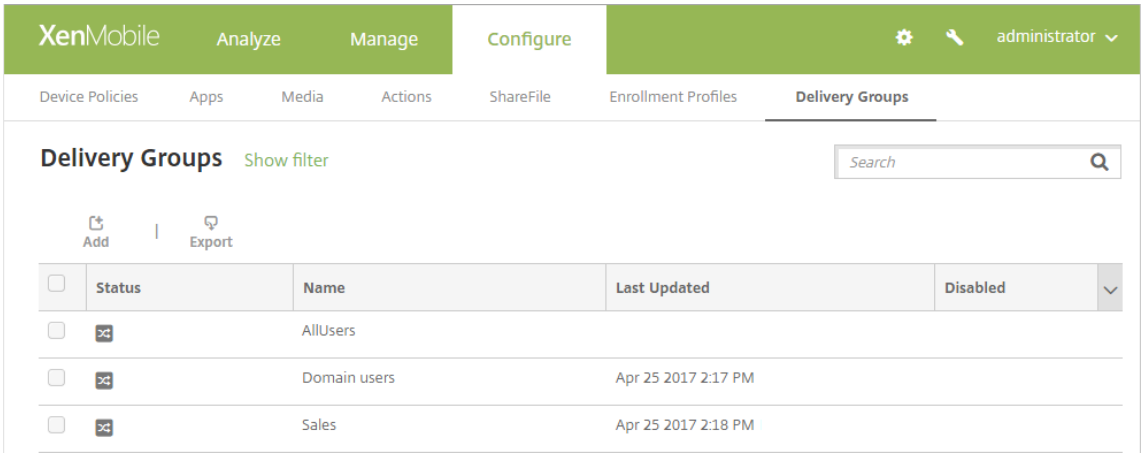
計算アルゴリズムが名前のみを基準に展開グループを順序づけた場合、XenMobile はデリバリーグループ Account Manager 1 から開始して、次の順序で展開を実行します：**WiFi**、**Passcode**、**Connection scheduling** および **Restrictions**。XenMobile は、Account Manager 2 デリバリーグループの重複する **Passcode** および **WiFi** を無視します。

ただし、Account Managers 2 グループには、管理者指定の展開順序があります。したがって、計算アルゴリズムによって、Account Managers 2 デリバリーグループのリソースが、その他のデリバリーグループのリソースより、一覧のより上位に配置されます。その結果、XenMobile はこの順序でポリシーをデプロイします：**Connection scheduling**、**Restrictions**、**Passcode**、および **WiFi**。XenMobile は、Account Manager 1 デリバリーグルー

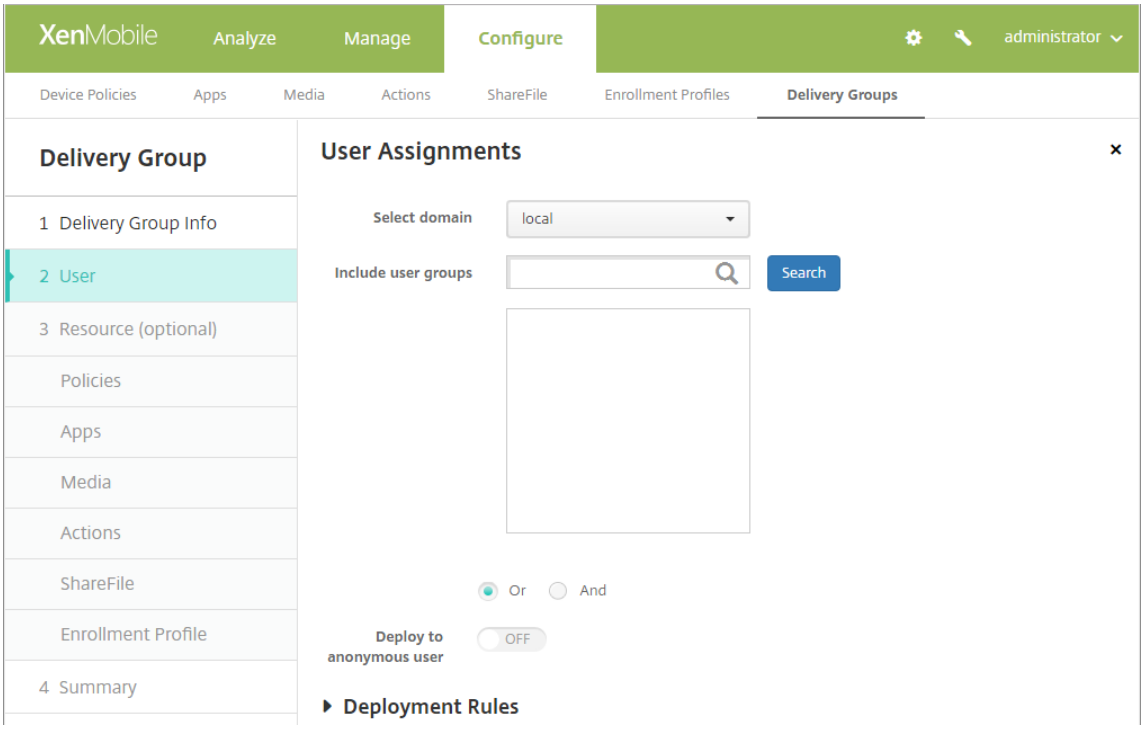
プからのポリシー **WiFi** および **Passcode** を無視します。重複しているためです。このアルゴリズムは、XenMobile 管理者によって指定された順序を優先します。

デリバリーグループを追加するには

1. XenMobile コンソールで、［構成］の［デリバリーグループ］をクリックします。［デリバリーグループ］ページが開きます。



2. ［デリバリーグループ］ページで、［追加］をクリックします。［デリバリーグループ情報］ページが表示されたら、以下の情報を入力します。
   - 名前: デリバリーグループの説明的な名前を入力します。
   - 説明: 任意で、デリバリーグループの説明を入力します。
3. ［次へ］をクリックします。［ユーザー割り当て］ページが開きます。次の設定を構成します。



- ドメインを選択: 一覧から、ユーザーを選択するドメインを選択します。
- ユーザーグループを含める: 次のいずれかを行います:
  - ユーザーグループの一覧で、追加するグループを選択します。選択したグループが ［選択したユーザーグループ］ 一覧に表示されます。
  - ［検索］ をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - グループ名の全体または一部を検索ボックスに入力して ［検索］ をクリックし、ユーザーグループの一覧を絞り込みます。

  ［選択したユーザーグループ］ の一覧からユーザーグループを削除するには、次のいずれかを行います:

  - ［選択したユーザーグループ］ の一覧で、削除する各グループの横にある ［**X**］ をクリックします。
  - ［検索］ をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
  - グループ名の全体または一部を検索ボックスに入力して ［検索］ をクリックし、ユーザーグループの一覧を絞り込みます。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
- **Or/And**: リソースが展開されるユーザーがいずれかのグループに属していればよいか（[Or]）、すべてのグループに属している必要があるか（[And]）を選択します。
- 匿名ユーザーに展開: デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。

  認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスを XenMobile に接続することを許可したユーザーを指します。

4. 展開規則を構成します。

5. ［展開規則］ を展開して以下の設定を構成します。デフォルトでは ［基本］ タブが表示されます。

    - 一覧から、ポリシーをいつ展開するかを指定するオプションを選択します。すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは ［すべて］ です。
    - ［新しい規則］ をクリックして条件を定義します。
    - 一覧で、ユーザーログオン名やドメイン名などの条件をクリックします。
    - 条件をさらに追加するには、［新しい規則］ をもう一度クリックします。

6. ［詳細］ タブをクリックし、ブール値オプションを使用して規則を組み合わせます。［基本］ タブで選択した条件が表示されます。
7. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。

    - ［**AND**］、［**OR**］、または［**NOT**］をクリックします。
    - 規則に条件を追加するには、一覧で規則に追加する条件を選択して右側のプラス記号（＋）をクリックします。

      いつでも、条件をクリックして選択し、［編集］ をクリックして条件を変更したり、［削除］ をクリックして条件を削除したりすることができます。
    - 条件を追加する場合は、［新しい規則］ をもう一度クリックします。

8. ［次へ］ をクリックします。［デリバリーグループのリソース］ ページが開きます。オプションとして、このページでデリバリーグループのポリシー、アプリ、アクションを追加します。この手順をスキップするには、［デリバリーグループ］の ［概要］ をクリックしてデリバリーグループ構成の概要情報を表示します。

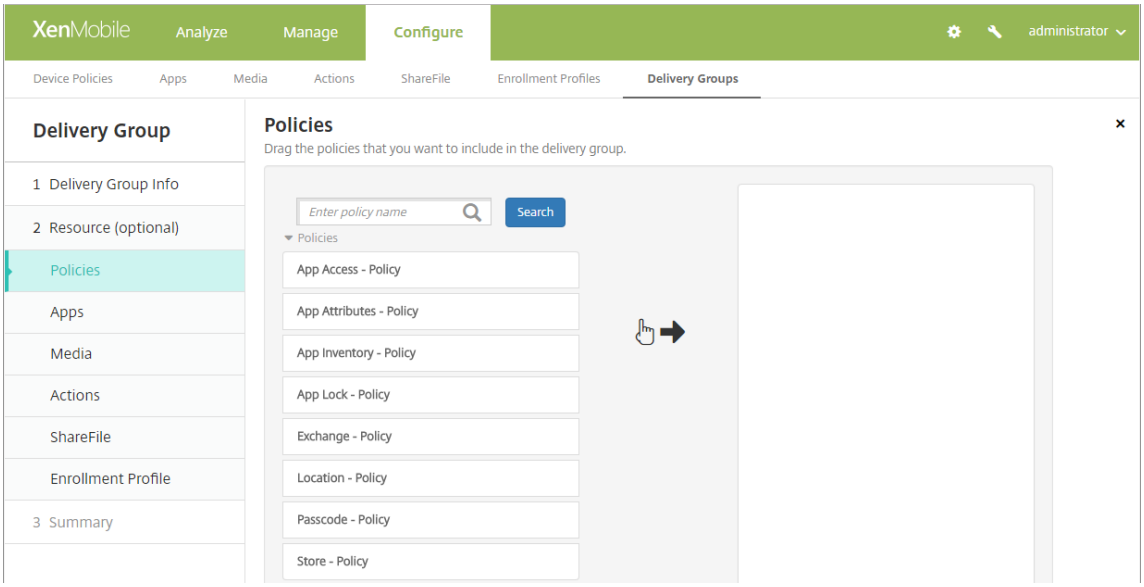
   リソースをスキップするには、［リソース（任意）］で追加するリソースをクリックし、そのリソースの手順に従います。

ポリシーを追加するには

1. 追加するポリシーごとに、以下の操作を行います:

    - 使用可能なポリシーの一覧をスクロールして、追加するポリシーを見つけます。
    - または、ポリシーの一覧を絞り込むため、検索ボックスにポリシー名の全体または一部を入力して ［検索］ をクリックします。
    - 追加するポリシーをクリックして、右側のボックス内へドラッグします。

   ポリシーを削除するには、右側のボックス内のポリシー名の横にある ［**X**］ をクリックします。



2. ［次へ］ をクリックします。［アプリ］ ページが開きます。

アプリを追加するには

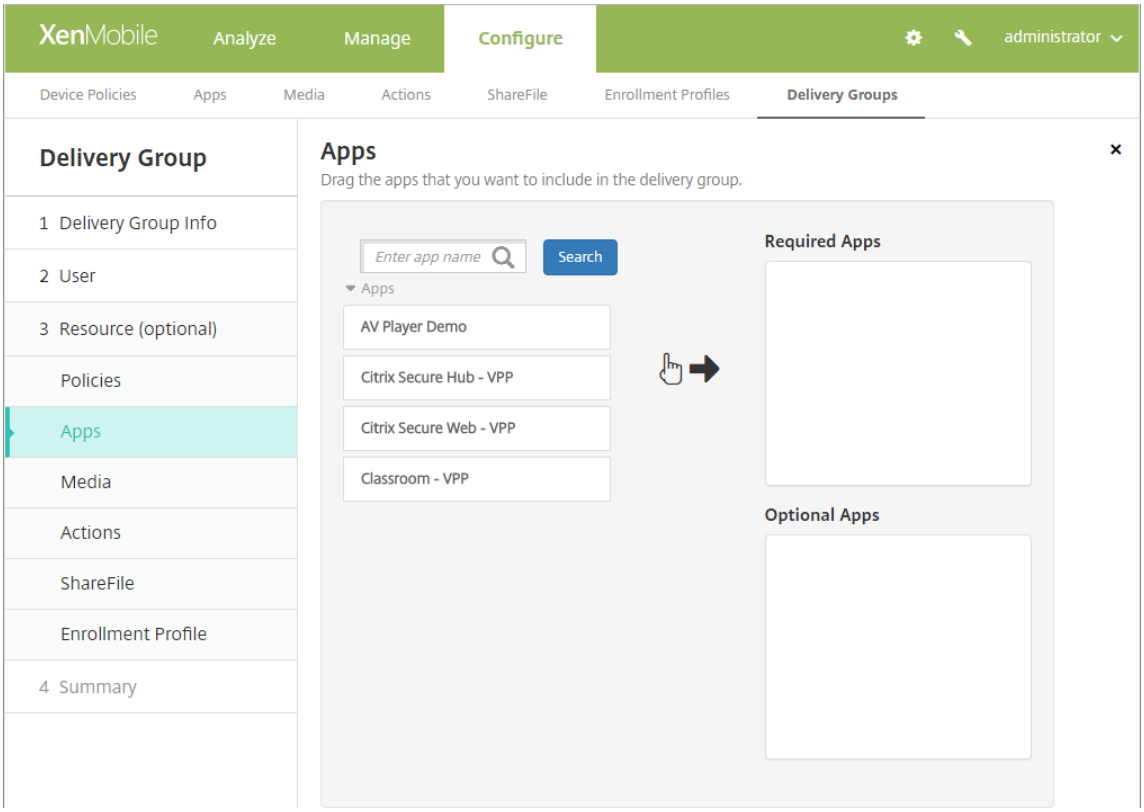
1. 追加するアプリごとに、以下の操作を行います:

   - 使用可能なアプリの一覧をスクロールして、追加するアプリを見つけます。
   - または、アプリの一覧を絞り込むため、検索ボックスにアプリ名の全体または一部を入力して ［検索］ をクリックします。
   - 追加するアプリをクリックして、［必須アプリ］ボックス内または ［任意アプリ］ ボックス内へドラッグします。

   必要とマーク付けされたアプリについては、次のような場合に、ユーザーは速やかに更新プログラムを受信できます:

   - アップロードした新しいアプリを必要なアプリとしてマーク付けした場合。
   - 既存のアプリを必要なアプリとしてマーク付けした場合。
   - 必要なアプリをユーザーが削除した場合。
   - Secure Hub の更新が利用可能な場合。

   この機能を有効にする方法を含む、必須アプリの強制展開については、「必須のアプリとオプションのアプリについて」をご覧ください。

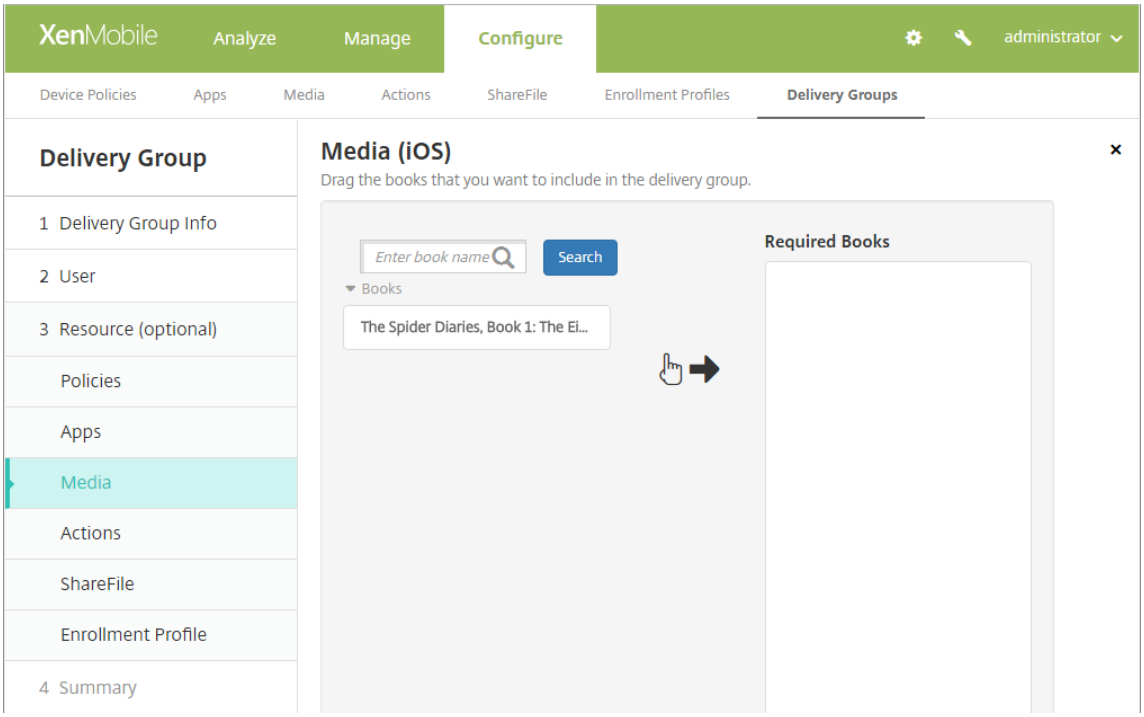


アプリを削除するには、右側のボックス内のアプリ名の横にある ［**X**］ をクリックします。

2. ［次へ］ をクリックします。［メディア］ ページが開きます。

メディアを追加するには

1. 追加する各ブックで、次の手順を実行します。
   - 使用可能なブックの一覧をスクロールして、追加するブックを見つけます。
   - または、ブックの一覧を絞り込むため、検索ボックスにブック名の全体または一部を入力して ［検索］ をクリックします。
   - 追加するブックをクリックして、［必須ブック］ ボックス内へドラッグします。



必要とマーク付けされたブックについては、次のような場合に、ユーザーは速やかに更新プログラムを受信します。

- アップロードした新しいブックを必要なブックとしてマーク付けした場合。
- 既存のブックを必要なブックとしてマーク付けした場合。
- 必要なブックをユーザーが削除した場合。
- Secure Hub の更新が利用可能な場合。

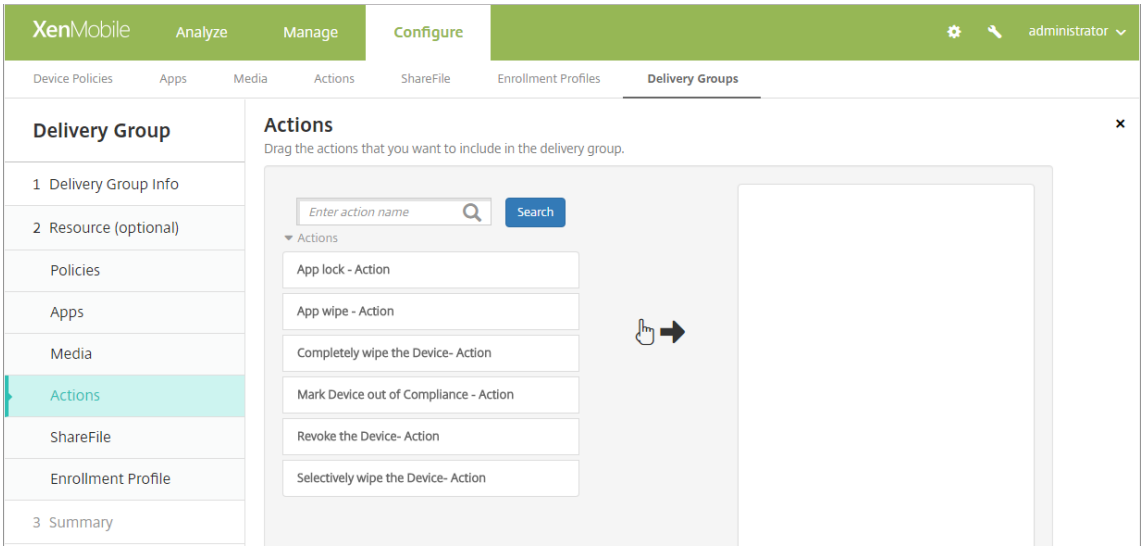
ブックを削除するには、右側のボックス内のブック名の横にある ［**X**］ をクリックします。

2. ［次へ］ をクリックします。 ［操作］ ページが開きます。

アクションを追加するには

1. 追加するアクションごとに、以下の操作を行います:
   - 使用可能なポリシーの一覧をスクロールして、追加するアクションを見つけます。
   - または、操作の一覧を絞り込むため、検索ボックスに操作名の全体または一部を入力して ［検索］ をクリックします。
   - 追加するアクションをクリックして、右側のボックス内へドラッグします。

   操作を削除するには、右側のボックス内の操作名の横にある ［**X**］ をクリックします。

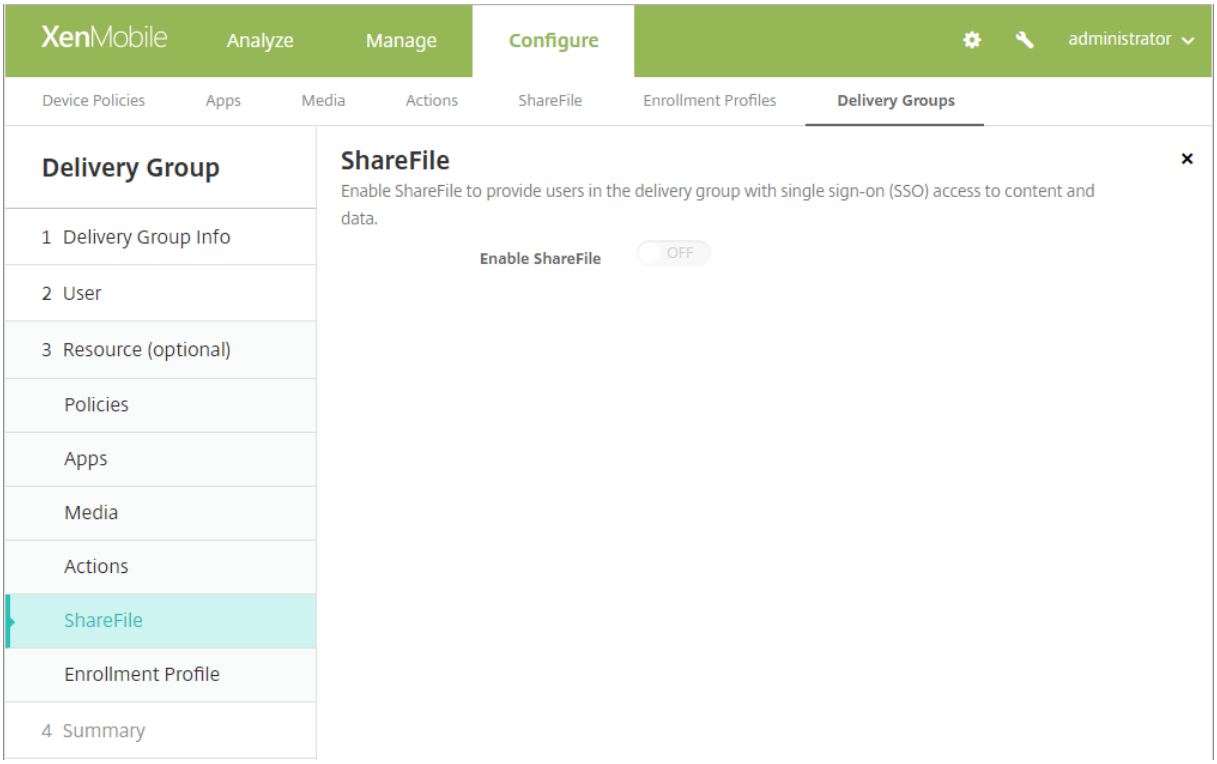


2. [次へ] をクリックします。 [**ShareFile**] ページが開きます。

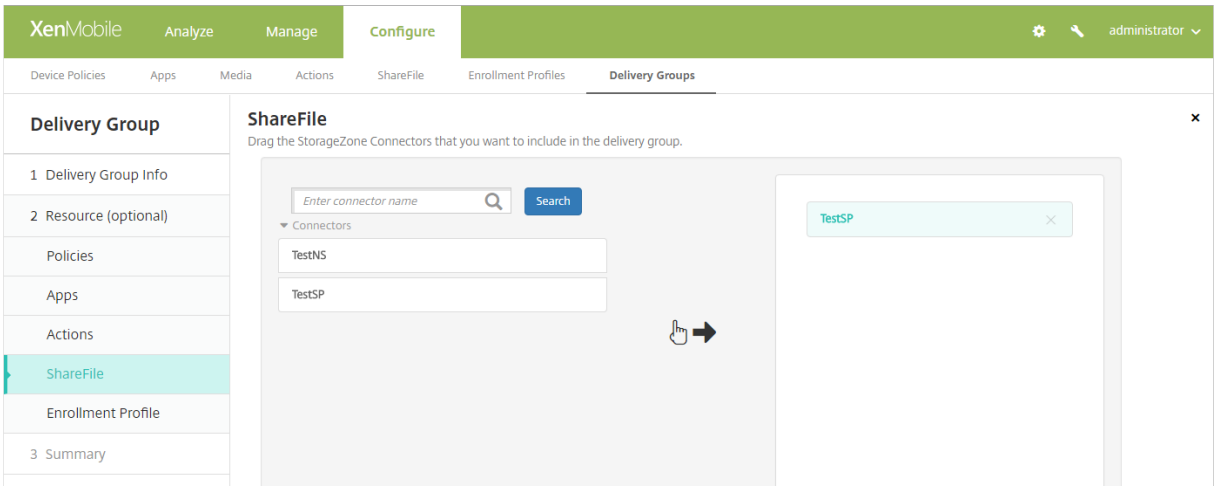
ShareFile 構成を適用するには

ShareFile ページの表示は、XenMobile（ [構成] **>** [**ShareFile**] ）を ShareFile Enterprise 用に構成したか、StorageZone コネクタ用に構成したかによって異なります。

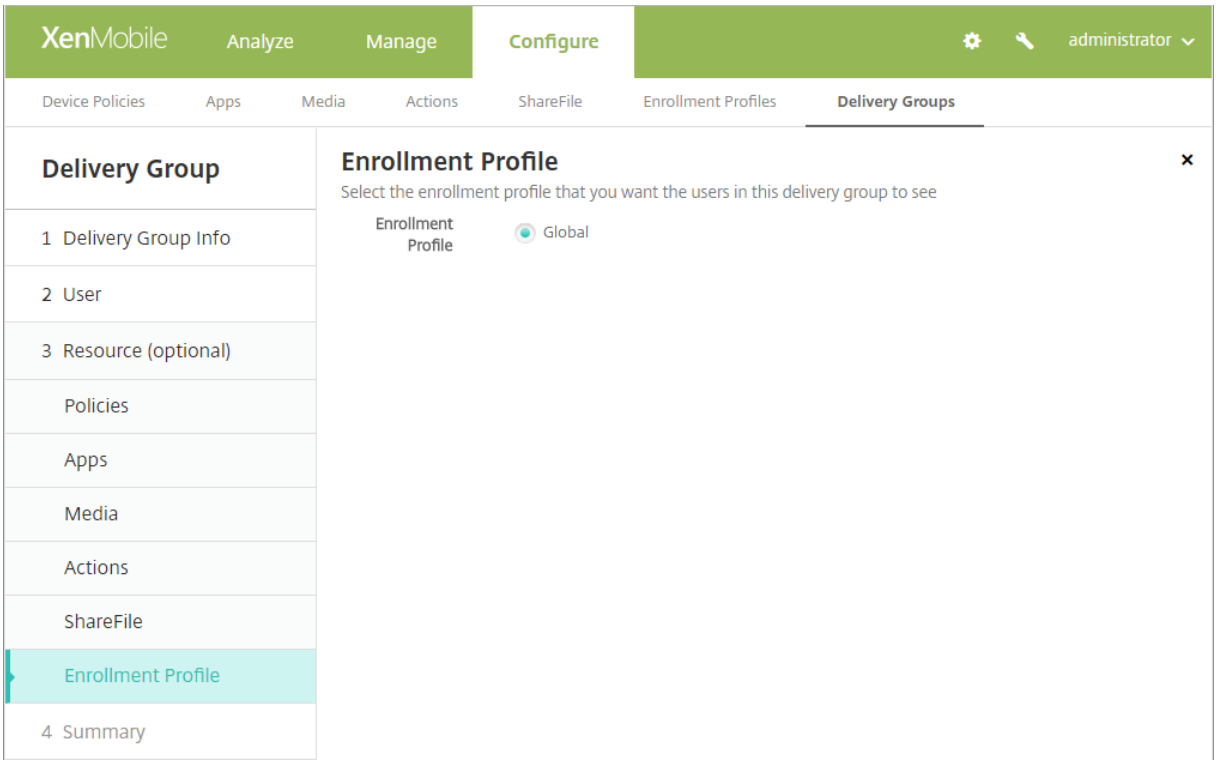
ShareFile Enterprise を XenMobile と組み合わせて使用するように構成した場合、 [**ShareFile** の有効化] を [オン] に設定して、デリバリーグループが ShareFile のコンテンツとデータにシングルサインオンでアクセスできるようにします。



StorageZone コネクタを XenMobile と組み合わせて使用するように構成した場合、StorageZone コネクタを選択してデリバリーグループに含めます。

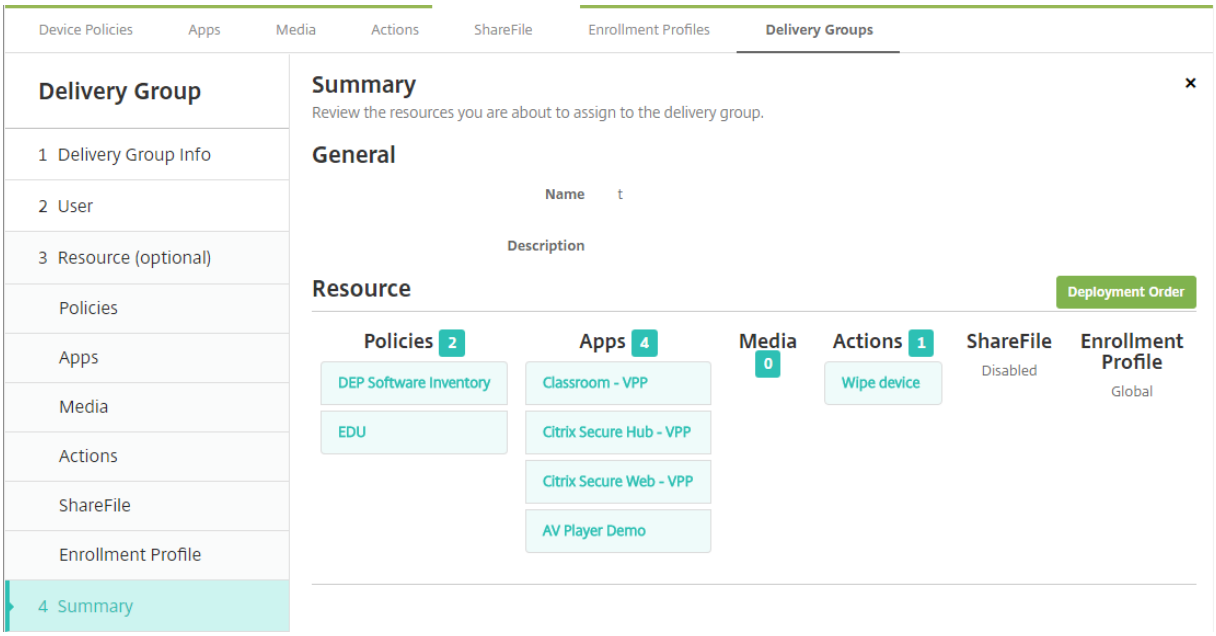


登録プロファイルを選択するには



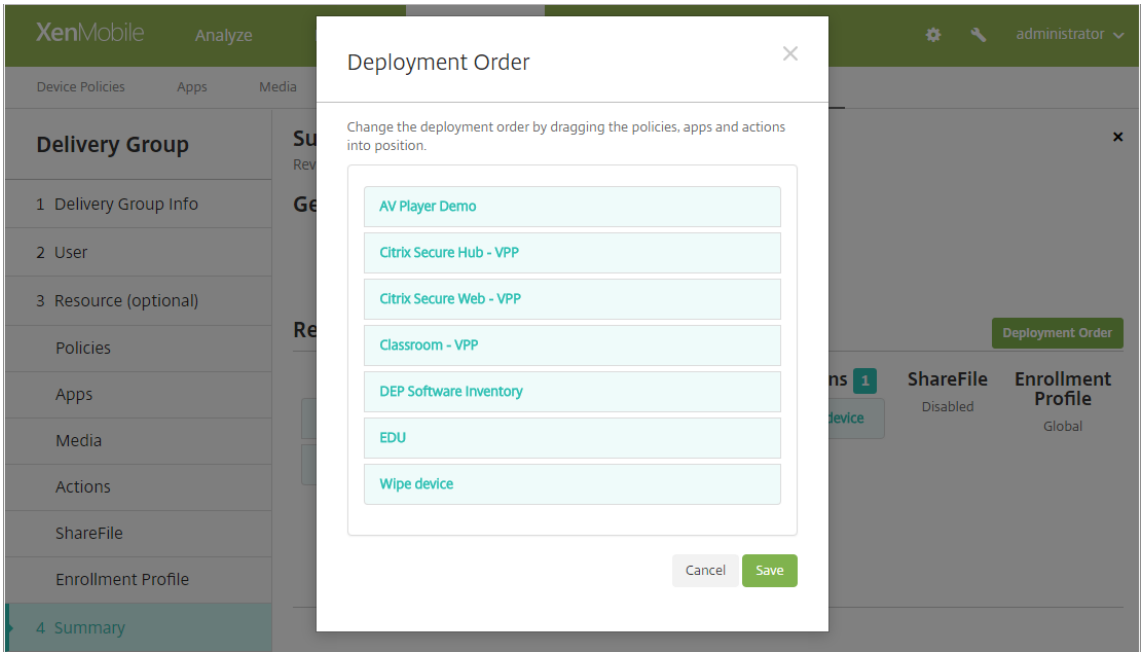
- 登録プロファイル: 登録プロファイルを選択します。登録プロファイルを作成するには、「デバイス登録の制限」を参照してください。
- [次へ] をクリックします。 [概要] ページが開きます。

構成したオプションの確認および展開順序の変更を行うには



[概要] ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。[概要] ページには、リソースがカテゴリ別に表示されます。[概要] ページは、展開順序を反映してはいません。

1. 構成の調整が必要な場合は、 [戻る] をクリックして前のページに戻ります。
2. 展開順序を表示するか、展開順序を並べ替えるには、 [展開順] をクリックします。 [展開順] ダイアログボックスが開きます。



3. リソースをクリックして展開する場所にドラッグします。展開順序を変更すると、一覧の上から下への順にリソースが展開されます。

4. ［保存］ をクリックして、展開順序を保存します。
5. ［保存］ をクリックして、デリバリーグループを保存します。

デリバリーグループを編集するには

既存のデリバリーグループの名前は変更できません。他の設定を更新するには、［構成］**>**［デリバリーグループ］ の順に選択し、編集するグループを選択して、［編集］ をクリックします。

AllUsers デリバリーグループを有効化および無効化するには

AllUsers は、有効化または無効化することができる唯一のデリバリーグループです。

［デリバリーグループ］ ページで、［**AllUsers**］の横にあるチェックボックスをオンにするか、［AllUsers］を含む行をクリックして、AllUsers デリバリーグループを選択します。次に、以下のいずれかを行います。

- AllUsers デリバリーグループを無効化するには、［無効］をクリックします。このコマンドは、［AllUsers］が有効（デフォルト）になっている場合にのみ使用できます。デリバリーグループの表の ［無効］ の見出しの下に、［無効］が表示されます。
- AllUsers デリバリーグループを有効化するには、［有効］をクリックします。このコマンドは、［AllUsers］が無効になっている場合にのみ使用できます。デリバリーグループの表の ［無効］ の見出しの下の ［無効］ の表示が消えます。

デリバリーグループに展開するには

デリバリーグループへの展開とは、iOS、Windows Phone、Windows タブレットデバイスを持つすべてのユーザーにプッシュ通知を送信することを意味します。そのユーザーは XenMobile に再接続するデリバリーグループに属している必要があります。それによってデバイスを再評価し、アプリ、ポリシー、アクションを展開できるようにします。

その他のプラットフォームのデバイスを持つユーザーについては、デバイスが既に XenMobile に接続済みであれば、すぐにそのリソースを受信します。接続していない場合は、スケジューリングポリシーに基づいて、次に接続するときにリソースを受信します。

Android デバイスで、XenMobile Store の［更新可能］の一覧に更新されたアプリが表示されるようにするには、最初にアプリインベントリポリシーをユーザーのデバイスに展開します。

1. ［デリバリーグループ］ ページで、次のいずれかを行います:
    - 複数のデリバリーグループに同時に展開するには、展開するグループの横にあるチェックボックスをオンにします。
    - 1 つのデリバリーグループに展開するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

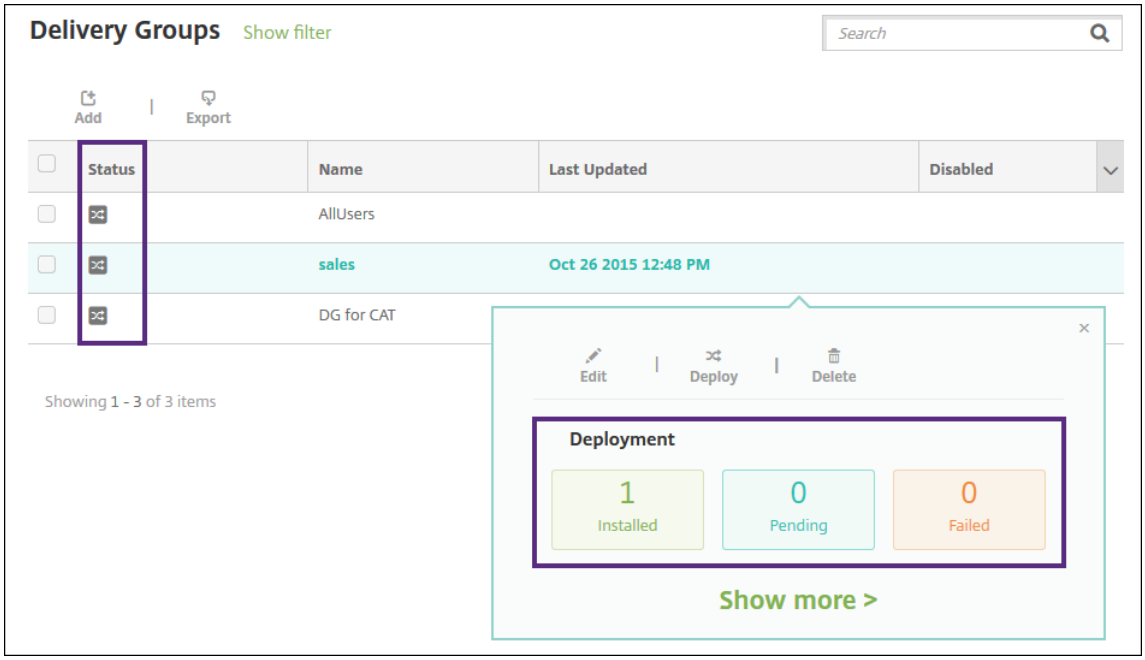
2. ［展開］ をクリックします。

   1 つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に ［展開］ コマンドが表示されます。

   アプリ、ポリシー、アクションを展開するグループが一覧にあることを確認して、［展開］をクリックします。デバイスプラットフォームとスケジュール設定ポリシーに基づいて、選択したグループにアプリ、ポリシー、アクションが展開されます。

   ［デリバリーグループ］ ページで、次のいずれかの方法により展開ステータスを確認できます。

   - デリバリーグループの ［状態］ の見出しの下で、展開エラーを示す展開アイコンを確認します。
   - デリバリーグループを含む行をクリックし、［インストール済み］、［保留中］、［失敗］の展開を示すオーバーレイを表示します。



デリバリーグループを削除するには

AllUsers デリバリーグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

1. ［デリバリーグループ］ ページで、次のいずれかを行います:

   - 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。
   - 1 つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

2. ［削除］ をクリックします。［削除］ ダイアログボックスが開きます。

1 つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に ［削除］ コマンドが表示されます。

> 重要:
>
> 削除を元に戻すことはできません。

3. ［削除］ をクリックします。

［デリバリーグループ］の表をエクスポートするには

1. ［デリバリーグループ］ の表の上にある ［エクスポート］ をクリックします。XenMobile によって ［デリバリーグループ］ の表の情報が抽出され、.csv ファイルに変換されます。
2. ブラウザーの通常の手順に従って、.csv ファイルをオープンまたは保存します。操作を取り消すこともできます。

マクロ

January 10, 2020

XenMobile では、次の項目のテキストフィールド内にユーザーまたはデバイスのプロパティデータを設定する方法としてマクロが提供されています。

- ポリシー
- 通知
- 登録テンプレート
- 自動化された操作
- 資格情報プロバイダー証明書署名要求

XenMobile では、対応するユーザーまたはシステムの値でマクロが置換されます。たとえば、何千人ものユーザーがいる 1 つの Exchange プロファイルに、ユーザーのメールボックスの値を事前に設定できます。

マクロの構文

マクロの形式は次のとおりです。

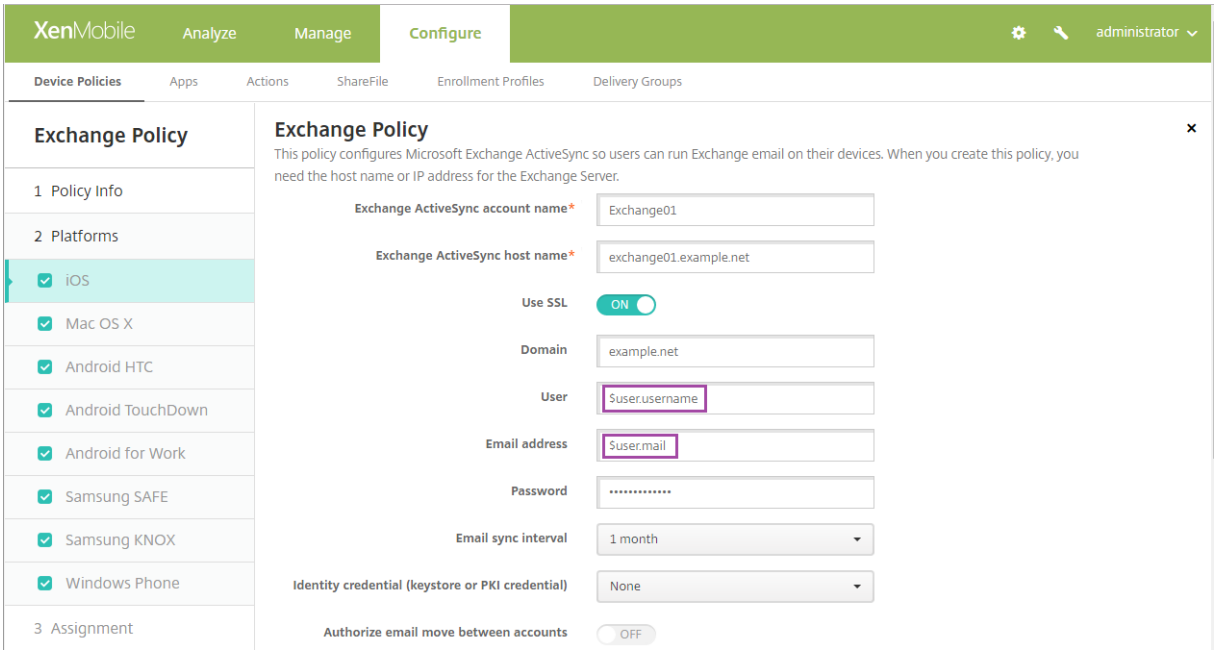
- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)] ] }`

ドル記号（$）に続くすべての構文は中かっこ（{ }）で囲みます。

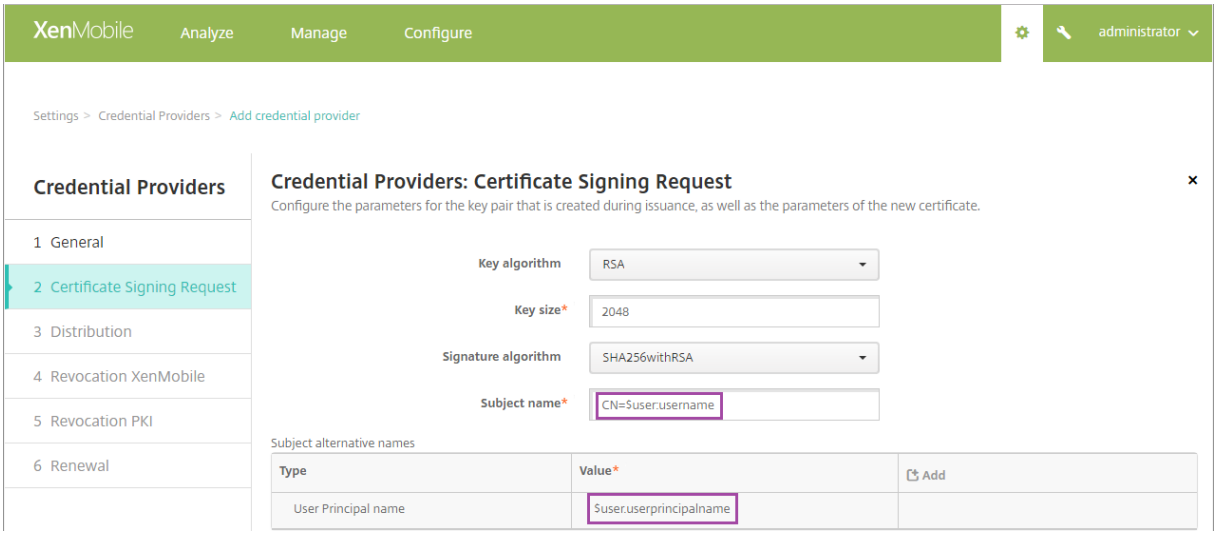
- 修飾されたプロパティ名は、ユーザープロパティ、デバイスプロパティ、またはカスタムプロパティを示します。
- 修飾されたプロパティ名は、プレフィックスと実際のプロパティ名で構成されます。
- ユーザープロパティの形式は次のとおりです。`${ user.[PROPERTYNAME] (prefix="user.")}`
- デバイスプロパティの形式は次のとおりです。`${ device.[PROPERTYNAME] (prefix="device.")}`
- プロパティ名の大文字と小文字は区別されます。
- 関数を定義するサードパーティの参照に対して、関数の一覧またはリンクを制限できます。通知メッセージの次のマクロには、関数 **firstnotnull** が含まれます。

  デバイス`${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` がブロックされました...
- カスタムマクロ（ユーザーが定義するプロパティ）の場合、プレフィックスは`${ custom }` です。プレフィックスは省略できます。

以下は、ポリシーのテキストフィールドにユーザー名の値を設定する、一般的なマクロ`${ user.username }` の例です。このマクロは、複数のユーザーが使用する Exchange ActiveSync プロファイルおよびそのほかのプロファイルを構成するのに便利です。次の例は、Exchange ポリシーでのマクロの使用方法を示しています。ユーザーのマクロは**`${ user.username }`** です。電子メールアドレスのマクロは**`${ user.mail }`** です。

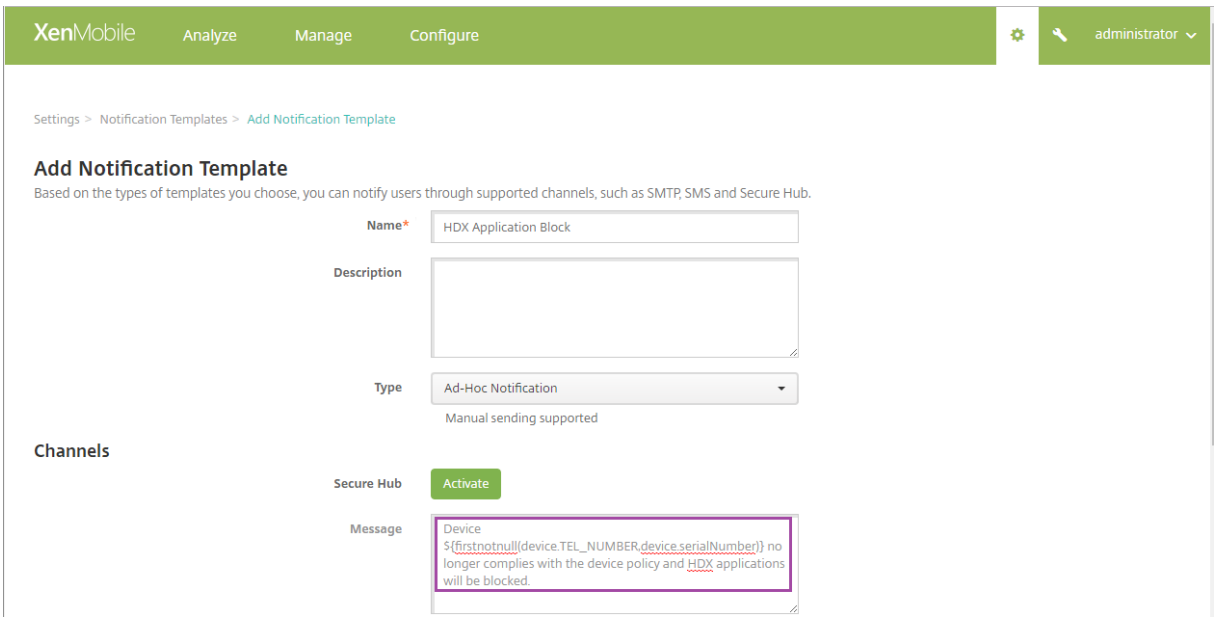


次の例は、証明書署名要求でのマクロの使用方法を示しています。サブジェクト名のマクロは**`CN=$user.username`**です。サブジェクトの別名の 値のマクロは**`$user.userprincipalname`**です。



次の例は、通知テンプレートでのマクロの使用方法を示しています。このテンプレート例では、デバイスが非準拠のため HDX アプリケーションがブロックされた場合にユーザーに送信されるメッセージを定義します。［メッセージ］のマクロは次のとおりです。

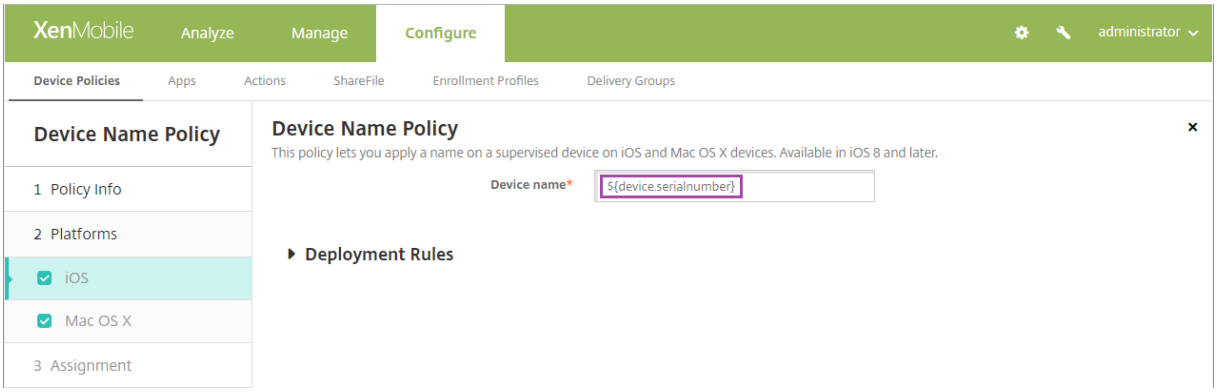
デバイス`${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` がデバイスポリシーに準拠しなくなりましたので、HDX アプリケーションがブロックされます。



通知で使用されるマクロの例については、［設定］**>**［通知テンプレート］の順に移動し、事前定義されたテンプレートを選択して、［編集］をクリックします。

次の例は、デバイス名デバイスポリシーのマクロを示しています。マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。たとえば、デバイス名を各デバイスのシリアル番号に設定するには、`${ device.serialnumber }` を使用します。デバイス名にユーザー名を含めるには、`${ device.serialnumber } ${ user.username }` を使用します。デバイス名デバイスポリ

シーは、監視対象の iOS デバイスおよび macOS デバイスで機能します。



デフォルトの通知テンプレートのマクロ

デフォルトの通知テンプレートで次のマクロを使用できます。

- ${ account.SUPPORT_EMAIL }
- ${ applicationName }
- ${ enrollment.andriod.agent.download.url }
- ${ enrollment.ios.agent.download.url }
- ${ enrollment.pin }
- ${ enrollment.url }
- ${ enrollment.urls }
- ${ enrollment.ios.url }
- ${ enrollment.macos.url }
- ${ enrollment.android.url }
- ${ enrollment.ios.platform }
- ${ enrollment.macos.platform }
- ${ enrollment.android.platform }
- ${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}
- ${ firstnotnull(device.TEL_NUMBER,user.mobile)}
- ${ outofcompliance.reason(smg_block)}
- ${ outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${ vpp.account }
- ${ vpp.appname }
- ${ vpp.url }
- ${ zdmserver.hostPath } /enroll

特定のポリシーのマクロ

デバイス名デバイスポリシー（iOS と macOS 用）では、デバイス名に次のマクロを使用できます:

- ${ device.serialnumber }
- ${ user.username } @example.com
- ${ device.serialnumber }
- ${ device.serialnumber }
- ${ user.username }
- ${ enrollment.pin }
- ${ user.dnsroot }

webclip デバイスポリシーの場合は、**URL** で次のマクロを使用できます:

- ${ webeas-url }

Samsung MDM ライセンスキーのデバイスポリシーについては、このマクロを **ELM** ライセンスキーに使用できます:

- ${ elm.license.key }

組み込みのデバイスプロパティを取得するためのマクロ

表示名	マクロ
デバイス ID	$device.id
デバイスの IMEI	$device.imei
OS ファミリ	$device.OSFamily
シリアル番号	$device.serialNumber

すべてのデバイスプロパティ向けのマクロ

以下は、表示名、Web 要素、マクロの一覧です。

アカウントを一時停止しますか?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- ${device.GOOGLE_AW_DIRECTORY_SUSPENDED

アクティベーションロックバイパスコード

- ACTIVATION_LOCK_BYPASS_CODE
- ${device.ACTIVATION_LOCK_BYPASS_CODE

アクティベーションロックが有効になっています

- ACTIVATION_LOCK_ENABLED
- ${device.ACTIVATION_LOCK_ENABLED

アクティブな iTunes アカウント

- ACTIVE_ITUNES
- ${device.ACTIVE_ITUNES}

MSP により認知された ActiveSync デバイス

- AS_DEVICE_KNOWN_BY_ZMSP
- ${device.AS_DEVICE_KNOWN_BY_ZMSP

ActiveSync ID

- EXCHANGE_ACTIVESYNC_ID
- ${device.EXCHANGE_ACTIVESYNC_ID

管理者が無効になっています

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED

AIK は存在しますか?

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT

Amazon MDM API 実行可能

- AMAZON_MDM
- ${device.AMAZON_MDM

Android Enterprise デバイス ID

- GOOGLE_AW_DEVICE_ID
- ${device.GOOGLE_AW_DEVICE_ID

Android Enterprise 対応デバイスですか?

- GOOGLE_AW_ENABLED_DEVICE
- ${device.GOOGLE_AW_ENABLED_DEVICE

Android Enterprise インストールの種類

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE

スパイウェア対策の署名の状態

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS

スパイウェア対策の状態

- ANTI_SPYWARE_STATUS

- ${device.ANTI_SPYWARE_STATUS

ウイルス対策の署名の状態

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS

ウイルス対策の状態

- ANTI_VIRUS_STATUS
- ${device.ANTI_VIRUS_STATUS

ASM DEP アクティベーションロックバイパスコード

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- ${device.DEP_ACTIVATION_LOCK_BYPASS_CODE

ASM DEP エスクローキー

- DEP_ESCROW_KEY
- ${device.DEP_ESCROW_KEY

アセットタグ

- ASSET_TAG
- ${device.ASSET_TAG

ソフトウェアの更新を自動確認

- AutoCheckEnabled
- ${device.AutoCheckEnabled

ソフトウェアの更新をバックグラウンドで自動ダウンロード

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled

アプリの更新を自動インストール

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled

OS の更新を自動インストール

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled

セキュリティの更新を自動インストール

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled

自動更新の状態

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS

使用できる RAM

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE

使用可能なソフトウェアの更新

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE

使用できるストレージ領域

- FREEDISK
- ${device.FREEDISK

バックアップバッテリー

- BACKUP_BATTERY_PERCENT
- ${device.BACKUP_BATTERY_PERCENT

ベースバンドファームウェアのバージョン

- MODEM_FIRMWARE_VERSION
- ${device.MODEM_FIRMWARE_VERSION

バッテリー充電中

- BATTERY_CHARGING_STATUS
- ${device.BATTERY_CHARGING_STATUS

バッテリー充電

- BATTERY_CHARGING
- ${device.BATTERY_CHARGING

バッテリー残量

- BATTERY_ESTIMATED_CHARGE_REMAINING
- ${device.BATTERY_ESTIMATED_CHARGE_REMAINING

バッテリー駆動中

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME

バッテリー状態

- BATTERY_STATUS
- ${device.BATTERY_STATUS

MS によって認知されている BES デバイス

- BES_DEVICE_KNOWN_BY_ZMSP
- ${device.BES_DEVICE_KNOWN_BY_ZMSP

BES PIN

- BES_PIN
- ${device.BES_PIN

BES サーバーエージェント ID

- AGENT_ID
- ${device.AGENT_ID

BES サーバー名

- BES_SERVER
- ${device.BES_SERVER

BES サーバーのバージョン

- BES_VERSION
- ${device.BES_VERSION

BIOS 情報

- BIOS_INFO
- ${device.BIOS_INFO

BitLocker の状態

- WINDOWS_HAS_BIT_LOCKER_STATUS
- ${device.WINDOWS_HAS_BIT_LOCKER_STATUS

Bluetooth MAC アドレス

- BLUETOOTH_MAC
- ${device.BLUETOOTH_MAC

ブートデバッグは有効ですか?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED

ブートマネージャー Rev リストバージョン

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- ${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION

キャリアコード

- CARRIER_CODE

- ${device.CARRIER_CODE

キャリア設定バージョン

- CARRIER_SETTINGS_VERSION
- ${device.CARRIER_SETTINGS_VERSION

カタログの URL

- CatalogURL
- ${device.CatalogURL

携帯ネットワークの高度

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR

携帯ネットワークのコース

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR

携帯ネットワークの水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR

携帯ネットワーク緯度

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR

携帯ネットワーク経度

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR

携帯ネットワークの速度

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR

携帯ネットワークテクノロジ

- CELLULAR_TECHNOLOGY
- ${device.CELLULAR_TECHNOLOGY

携帯ネットワークタイムスタンプ

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR

携帯ネットワークの垂直精度

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

次回のログイン時にパスワードを変更しますか?

- GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN
- ${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

クライアントデバイス ID

- CLIENT_DEVICE_ID
- ${device.CLIENT_DEVICE_ID

クラウドバックアップが有効になりました

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED

コードの整合性は有効ですか?

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED

コードの整合性 Rev リストバージョン

- INDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION
- ${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION

色

- COLOR
- ${device.COLOR

CPU クロック速度

- CPU_CLOCK_SPEED
- ${device.CPU_CLOCK_SPEED

CPU の種類

- CPU_TYPE
- ${device.CPU_TYPE}

作成時刻

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME

重要なソフトウェアの更新

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- ${device.AVAILABLE_OS_UPDATE_IS_CRITICAL

現在のキャリアネットワーク

- CARRIER
- ${device.CARRIER

現在のモバイル国コード

- CURRENT_MCC
- ${device.CURRENT_MCC

現在のモバイルネットワークコード

- CURRENT_MNC
- ${device.CURRENT_MNC

データローミングが許可されました

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED

最新の iCloud バックアップ日

- LAST_CLOUD_BACKUP_DATE
- ${device.LAST_CLOUD_BACKUP_DATE}

デフォルトカタログ

- IsDefaultCatalog
- ${device.IsDefaultCatalog

DEP アカウント名

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- ${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME

DEP ポリシー

- WINDOWS_HAS_DEP_POLICY
- ${device.WINDOWS_HAS_DEP_POLICY

割り当てられた DEP プロファイル

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME

プッシュされた DEP プロファイル

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME

削除された DEP プロファイル

- PROFILE_REMOVE_TIME

- ${device.PROFILE_REMOVE_TIME

DEP 登録者

- DEVICE_ASSIGNED_BY
- ${device.DEVICE_ASSIGNED_BY

DEP 登録日

- DEVICE_ASSIGNED_DATE
- ${device.DEVICE_ASSIGNED_DATE

説明

- 説明
- ${device.DESCRIPTION

デバイスのモデル

- SYSTEM_OEM
- ${device.SYSTEM_OEM

デバイス名

- DEVICE_NAME
- ${device.DEVICE_NAME

デバイスの種類

- DEVICE_TYPE
- ${device.DEVICE_TYPE

ボイスメールへ自動転送がアクティブになりました

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB

ELAM ドライバーは読み込まれていますか?

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED

暗号化のコンプライアンス

- ENCRYPTION_COMPLIANCE
- ${device.ENCRYPTION_COMPLIANCE

ENROLLMENT_KEY_GENERATION_DATE

- ENROLLMENT_KEY_GENERATION_DATE
- ${device.ENROLLMENT_KEY_GENERATION_DATE

エンタープライズ ID

- ENTERPRISEID
- ${device.ENTERPRISEID

外部ストレージ 1: 使用可能領域

- EXTERNAL_STORAGE1_FREE_SPACE
- ${device.EXTERNAL_STORAGE1_FREE_SPACE

外部ストレージ 1: 名前

- EXTERNAL_STORAGE1_NAME
- ${device.EXTERNAL_STORAGE1_NAME

外部ストレージ 1: 総領域

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE

外部ストレージ 2: 使用可能領域

- EXTERNAL_STORAGE2_FREE_SPACE
- ${device.EXTERNAL_STORAGE2_FREE_SPACE

外部ストレージ 2: 名前

- EXTERNAL_STORAGE2_NAME
- ${device.EXTERNAL_STORAGE2_NAME

外部ストレージ 2: 総領域

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE

外部ストレージが暗号化されました

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION

FileVault が有効です

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED

ファイアウォールの状態

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS

ファイアウォールの状態

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS

ファームウェアのバージョン

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION

最初の同期

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC

Google ディレクトリのエイリアス

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS

Google ディレクトリのファミリ名

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME

Google ディレクトリ名

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google ディレクトリのプライマリメール

- GOOGLE_AW_DIRECTORY_PRIMARY
- ${device.GOOGLE_AW_DIRECTORY_PRIMARY}

Google ディレクトリユーザー ID

- GOOGLE_AW_DIRECTORY_USER_ID
- ${device.GOOGLE_AW_DIRECTORY_USER_ID}

GPS 高度

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS

GPS のコース

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS

GPS の水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS

GPS 緯度

- GPS_LATITUDE_FROM_GPS

- ${device.GPS_LATITUDE_FROM_GPS

GPS 経度

- GPS_LONGITUDE_FROM_GPS
- ${device.GPS_LONGITUDE_FROM_GPS

GPS の速度

- GPS_SPEED_FROM_GPS
- ${device.GPS_SPEED_FROM_GPS

GPS タイムスタンプ

- GPS_TIMESTAMP_FROM_GPS
- ${device.GPS_TIMESTAMP_FROM_GPS

GPS の垂直精度

- GPS_VERTICAL_ACCURACY_FROM_GPS
- ${device.GPS_VERTICAL_ACCURACY_FROM_GPS

ハードウェアデバイス ID

- HW_DEVICE_ID
- ${device.HW_DEVICE_ID

ハードウェア暗号化機能

- HARDWARE_ENCRYPTION_CAPS
- ${device.HARDWARE_ENCRYPTION_CAPS

HAS_CONTAINER

- HAS_CONTAINER
- ${device.HAS_CONTAINER

現在ログオンしている iTunes ストアアカウントのハッシュ

- ITUNES_STORE_ACCOUNT_HASH
- ${device.ITUNES_STORE_ACCOUNT_HASH

ホームキャリアネットワーク

- SIM_CARRIER_NETWORK
- ${device.SIM_CARRIER_NETWORK

ホームモバイル国コード

- SIM_MCC
- ${device.SIM_MCC

ホームモバイルネットワークコード

- SIM_MNC
- ${device.SIM_MNC

HTC API バージョン

- HTC_MDM_VERSION
- ${device.HTC_MDM_VERSION

HTC MDM API 実行可能

- HTC_MDM
- ${device.HTC_MDM

ICCID

- ICCID
- ${device.ICCID

Identit

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY

IMEI/MEID 番号

- IMEI
- ${device.IMEI

IMSI

- SIM_ID
- ${device.SIM_ID

内部ストレージが暗号化されました

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION

IP の場所

- IP_LOCATION
- ${device.IP_LOCATION

IPv4 アドレス

- IP_ADDRESSV4
- ${device.IP_ADDRESSV4

IPv6 アドレス

- IP_ADDRESSV6
- ${device.IP_ADDRESSV6

発行時刻

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT

ジェイルブレイク済み/ルート指定済み

- ROOT_ACCESS
- ${device.ROOT_ACCESS

カーネルデバッグは有効ですか?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- ${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED

キオスクモード

- IS_KIOSK
- ${device.IS_KIOSK

前回認知した IP アドレス

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR

前回のポリシー更新時間

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME

前回のスキャン日

- PreviousScanDate
- ${device.PreviousScanDate

前回のスキャン結果

- PreviousScanResult
- ${device.PreviousScanResult

前回スケジュールされたソフトウェアの更新

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME

前回スケジュールされたソフトウェアの更新の失敗メッセージ

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG

前回スケジュールされたソフトウェアの更新の状態

- AVAILABLE_OS_UPDATE_INSTALL_STATUS

- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS

前回の同期

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC

ロケーターサービスが有効になっています

- DEVICE_LOCATOR
- ${device.DEVICE_LOCATOR

MAC アドレス

- MAC_ADDRESS
- ${device.MAC_ADDRESS

MAC アドレスネットワーク接続

- MAC_NETWORK_CONNECTION
- ${device.MAC_NETWORK_CONNECTION

MAC アドレスの種類

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE

メールボックスセットアップ

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- ${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP

メインバッテリー

- MAIN_BATTERY_PERCENT
- ${device.MAIN_BATTERY_PERCENT

MDM の紛失モードが有効になっています

- IS_MDM_LOST_MODE_ENABLED
- ${device.IS_MDM_LOST_MODE_ENABLED

MDX_SHARED_ENCRYPTION_KEY

- MDX_SHARED_ENCRYPTION_KEY
- ${device.MDX_SHARED_ENCRYPTION_KEY

MEID

- MEID
- ${device.MEID

携帯電話番号

- TEL_NUMBER
- ${device.TEL_NUMBER

モデル ID

- MODEL_ID
- ${device.MODEL_ID}

モデル番号

- MODEL_NUMBER
- ${device.MODEL_NUMBER

ネットワークアダプターの種類

- NETWORK_ADAPTER_TYPE
- ${device.NETWORK_ADAPTER_TYPE

NitroDesk TouchDown がインストールされました

- TOUCHDOWN_FIND
- ${device.TOUCHDOWN_FIND

NitroDesk TouchDown ライセンスが MDM を介して割り当てられました

- TOUCHDOWN_LICENSED_VIA_MDM
- ${device.TOUCHDOWN_LICENSED_VIA_MDM

オペレーティングシステムビルド

- SYSTEM_OS_BUILD
- ${device.SYSTEM_OS_BUILD

オペレーティングシステムのエディション

- OS_EDITION
- ${device.OS_EDITION

オペレーティングシステム言語（ロケール）

- SYSTEM_LANGUAGE
- ${device.SYSTEM_LANGUAGE

オペレーティングシステムバージョン

- SYSTEM_OS_VERSION
- ${device.SYSTEM_OS_VERSION

組織の住所

- ORGANIZATION_ADDRESS
- ${device.ORGANIZATION_ADDRESS

組織のメール

- ORGANIZATION_EMAIL
- ${device.ORGANIZATION_EMAIL

組織のマジック

- ORGANIZATION_MAGIC
- ${device.ORGANIZATION_MAGIC

組織名

- ORGANIZATION_NAME
- ${device.ORGANIZATION_NAME

組織の電話番号

- ORGANIZATION_PHONE
- ${device.ORGANIZATION_PHONE

コンプライアンス違反

- OUT_OF_COMPLIANCE
- ${device.OUT_OF_COMPLIANCE

所有者

- CORPORATE_OWNED
- ${device.CORPORATE_OWNED

パスコード準拠

- PASSCODE_IS_COMPLIANT
- ${device.PASSCODE_IS_COMPLIANT

構成に準拠したパスコード

- PASSCODE_IS_COMPLIANT_WITH_CFG
- ${device.PASSCODE_IS_COMPLIANT_WITH_CFG

現在のパスコード

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0

境界違反

- GPS_PERIMETER_BREACH

- ${device.GPS_PERIMETER_BREACH

定期的な確認

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck

パーソナルホットスポットがアクティブになりました

- PERSONAL_HOTSPOT_ENABLED
- ${device.PERSONAL_HOTSPOT_ENABLED

ジオフェンスの PIN コード

- PIN_CODE_FOR_GEO_FENCE
- ${device.PIN_CODE_FOR_GEO_FENCE

プラットフォーム

- SYSTEM_PLATFORM
- ${device.SYSTEM_PLATFORM}

プラットフォーム API レベル

- API_LEVEL
- ${device.API_LEVEL

ポリシー名

- POLICY_NAME
- ${device.POLICY_NAME

プライマリ電話番号

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER

プライマリ SIM の通信事業者

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR

プライマリ SIM ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID

プライマリ SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI

プライマリ SIM IMSI

- IDENTITY1_IMSI
- ${device.IDENTITY1_IMSI

プライマリ SIM ローミング

- IDENTITY1_ROAMING
- ${device.IDENTITY1_ROAMING

プライマリ SIM ローミングのコンプライアンス

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE

製品名

- PRODUCT_NAME
- ${device.PRODUCT_NAME

発行元デバイス ID

- PUBLISHER_DEVICE_ID
- ${device.PUBLISHER_DEVICE_ID

リセット回数

- WINDOWS_HAS_RESET_COUNT
- ${device.WINDOWS_HAS_RESET_COUNT

再起動回数

- WINDOWS_HAS_RESTART_COUNT
- ${device.WINDOWS_HAS_RESTART_COUNT

セーフモードは有効になっていますか?

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE

Samsung KNOX API 実行可能

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX

Samsung KNOX API バージョン

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION

Samsung KNOX 構成証明

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED

Samsung KNOX 構成証明更新日

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME

Samsung SAFE API 実行可能

- SAMSUNG_MDM
- ${device.SAMSUNG_MDM

Samsung SAFE API バージョン

- SAMSUNG_MDM_VERSION
- ${device.SAMSUNG_MDM_VERSION

SBCP ハッシュ

- WINDOWS_HAS_SBCP_HASH
- ${device.WINDOWS_HAS_SBCP_HASH

画面: 高さ

- SCREEN_HEIGHT
- ${device.SCREEN_HEIGHT

画面: 色数

- SCREEN_NB_COLORS
- ${device.SCREEN_NB_COLORS

画面: サイズ

- SCREEN_SIZE
- ${device.SCREEN_SIZE

画面: 幅

- SCREEN_WIDTH
- ${device.SCREEN_WIDTH

画面: X 軸解像度

- SCREEN_XDPI
- ${device.SCREEN_XDPI

画面: Y 軸解像度

- SCREEN_YDPI
- ${device.SCREEN_YDPI

セカンダリ電話番号

- IDENTITY2_PHONENUMBER

- ${device.IDENTITY2_PHONENUMBER

セカンダリ SIM の通信事業者

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY2_CARRIER_NETWORK_OPERATOR

セカンダリ SIM ICCID

- IDENTITY2_ICCID
- ${device.IDENTITY2_ICCID

セカンダリ SIM IMEI

- IDENTITY2_IMEI
- ${device.IDENTITY2_IMEI

セカンダリ SIM IMSI

- IDENTITY2_IMSI
- ${device.IDENTITY2_IMSI

セカンダリ SIM ローミング

- IDENTITY2_ROAMING
- ${device.IDENTITY2_ROAMING

セカンダリ SIM ローミングのコンプライアンス

- IDENTITY2_ROAMING_COMPLIANCE
- ${device.IDENTITY2_ROAMING_COMPLIANCE

セキュアブートは有効ですか?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- ${device.WINDOWS_HAS_SECURE_BOOT_ENABLED

セキュアブートの状態

- SECURE_BOOT_STATE
- ${device.SECURE_BOOT_STATE

SecureContainer 有効

- DLP_ACTIVE
- ${device.DLP_ACTIVE

セキュリティパッチレベル

- SYSTEM_SECURITY_PATCH_LEVEL
- ${device.SYSTEM_SECURITY_PATCH_LEVEL

シリアル番号

- SERIAL_NUMBER
- ${device.SERIAL_NUMBER

SMS 可

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE

Sony Enterprise API 実行可能

- SONY_MDM
- ${device.SONY_MDM

Sony Enterprise API バージョン

- SONY_MDM_VERSION
- ${device.SONY_MDM_VERSION

監視

- SUPERVISED
- ${device.SUPERVISED

一時停止理由

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON

改ざん状態

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS

使用条件

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS

条件および契約を承認しますか?

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS

テスト署名は有効になっていますか?

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED

RAM 合計

- MEMORY
- ${device.MEMORY

総ストレージ領域

- TOTAL_DISK_SPACE
- ${device.TOTAL_DISK_SPACE

TPM バージョン

- TPM_VERSION
- ${device.TPM_VERSION

UDID

- UDID
- ${device.UDID}

ユーザーアカウント制御の状態

- UAC_STATUS
- ${device.UAC_STATUS

ユーザーエージェント

- USER_AGENT
- ${device.USER_AGENT

ユーザー定義 #1

- USER_DEFINED_1
- ${device.USER_DEFINED_1

ユーザー定義 #2

- USER_DEFINED_2
- ${device.USER_DEFINED_2

ユーザー定義 #3

- USER_DEFINED_3
- ${device.USER_DEFINED_3

ユーザー言語（ロケール）

- USER_LANGUAGE
- ${device.USER_LANGUAGE

ベンダー

- VENDOR
- ${device.VENDOR

音声可

- IS_VOICE_CAPABLE

- ${device.IS_VOICE_CAPABLE

音声ローミングが許可されました

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED

VSM は有効になっていますか?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED

Wi-Fi MAC アドレス

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- ${device.WINDOWS_ENROLLMENT_KEY

WinPE は有効になっていますか?

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE

WNS 通知の状態

- PROPERTY_WNS_PUSH_STATUS
- ${device.PROPERTY_WNS_PUSH_STATUS

WNS 通知 URL

- PROPERTY_WNS_PUSH_URL
- ${device.PROPERTY_WNS_PUSH_URL

WNS 通知 URL 有効期限

- PROPERTY_WNS_PUSH_URL_EXPIRY
- ${device.PROPERTY_WNS_PUSH_URL_EXPIRY

XenMobile エージェント ID

- ENROLLMENT_AGENT_ID
- ${device.ENROLLMENT_AGENT_ID

XenMobile エージェントリビジョン

- EW_REVISION
- ${device.EW_REVISION

XenMobile エージェントバージョン

- EW_VERSION
- ${device.EW_VERSION

Zebra API 実行可能

- ZEBRA_MDM
- ${device.ZEBRA_MDM

Zebra MXMF バージョン

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION

Zebra Patch バージョン

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

組み込みのデバイスプロパティを取得するためのマクロ

表示名	マクロ
domainname（ドメイン名（デフォルトドメイン））	`${ user.domainname }`
loginname（ユーザー名とドメイン名）	`${ user.loginname }`
username（loginname からドメイン名を除去したもの（ある場合））	`${ user.username }`

すべてのデバイスプロパティ向けのマクロ

表示名	**Web** 要素	マクロ
Active Directory へのサインインに失敗しました	badpwdcount	`${ user.badpwdcount }`
ActiveSync ユーザーメール	asuseremail	`${ user.asuseremail }`
ASM のデータソース	asmpersonsource	`${ user.asmpersonsource }`
ASM DEP アカウント名	asmdepaccount	`${ user.asmdepaccount }`
ASM の管理対象 Apple ID	asmpersonmanagedappleid	`${ user.asmpersonmanagedappleid }`

表示名	**Web** 要素	マクロ
ASM のパスコードの種類	asmpersonpasscodetype	${ user.asmpersonpasscodetype }
ASM の個人 ID	asmpersonid	${ user.asmpersonid }
ASM の個人の状態	asmpersonstatus	${ user.asmpersonstatus }
ASM の個人の役職	asmpersontitle	${ user.asmpersontitle }
ASM の一意の個人 ID	asmpersonuniqueid	${ user.asmpersonuniqueid }
ASM のソースシステム ID	asmpersonsourcesystemid	${ user.asmpersonsourcesystemid }
ASM の生徒の学年	asmpersongrade	${ user.asmpersongrade }
BES ユーザーメール	besuseremail	${ user.besuseremail }
会社	会社	${ user.company }
会社名	companyname	${ user.companyname }
国	c	${ user.c }
部署	department	${ user.department }
説明	description	${ user.description }
無効なユーザー	disableduser	${ user.disableduser }
表示名	displayname	${ user.displayname }
識別名	distinguishedname	${ user.distinguishedname }
ドメイン名	domainname	${ user.domainname }
メール	mail	${ user.mail }
名	givenname	${ user.givenname }
自宅の住所	homestreetaddress	${ user.homestreetaddress }

表示名	**Web** 要素	マクロ
自宅の市区町村	homecity	${ user.homecity }
自宅の国	homecountry	${ user.homecountry }
自宅のファックス	homefax	${ user.homefax }
自宅の電話	homephone	${ user.homephone }
自宅の都道府県	homestate	${ user.homestate }
自宅の郵便番号	homezip	${ user.homezip }
IP 電話	ipphone	${ user.ipphone }
ミドルネーム、イニシャル	middleinitial	${ user.middleinitial }
ミドルネーム	middlename	${ user.middlename }
モバイル	モバイル	${ user.mobile }
名前	cn	${ user.cn }
会社の住所	physicaldeliveryofficename	${ user.physicaldeliveryofficename }
会社の市区町村	l	${ user.l }
会社のファックス番号	facsimiletelephonenumber	${ user.facsimiletelephonenumber }
会社の都道府県	st	${ user.st }
会社の番地	officestreetaddress	${ user.officestreetaddress }
会社の電話番号	telephonenumber	${ user.telephonenumber }
会社の郵便番号	postalcode	${ user.postalcode }
私書箱	postofficebox	${ user.postofficebox }
ポケベル	pager	${ user.pager }
プライマリグループ ID	primarygroupid	${ user.primarygroupid }
SAM アカウント	samaccountname	${ user.samaccountname }

表示名	**Web** 要素	マクロ
番地	streetaddress	`${ user.streetaddress }`
姓	sn	`${ user.sn }`
役職	タイトル	`${ user.title }`
ユーザーログオン名	userprincipalname	`${ user.userprincipalname }`

自動化された操作

January 10, 2020

XenMobile で自動化された操作を作成して、イベント、ユーザー、デバイスプロパティ、またはユーザーデバイスでのアプリの存在に対する対応をプログラミングします。自動化された操作を作成する場合は、操作に対して定義したトリガーによって、ユーザーのデバイスが XenMobile に接続したときにそのデバイス上で何が起きるかが決まります。イベントがトリガーされたときに、より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信できます。

たとえば、以前にブラックリストに追加したアプリ（例：Words with Friends）を検出するとします。ユーザーのデバイス上で「Words with Friends」が検出された場合に、そのデバイスをコンプライアンス違反に設定するトリガーを指定できます。この操作では次に、そのアプリを削除して、デバイスが再度コンプライアンス遵守状態に戻す必要があることがユーザーに通知されます。ユーザーが遵守するのを待つ時間を設定することもできます。その期限が過ぎると、デバイスの選択的なワイプなどの定義された操作が実行されます。

ユーザーのデバイスがコンプライアンス不遵守状態になった後で、ユーザーがデバイスを修正した場合：デバイスをコンプライアンス遵守状態にリセットするパッケージを展開するようポリシーを構成する必要があります。

自動的に発生する効果は、次の範囲から設定します：

- デバイスに選択的ワイプまたは完全なワイプを実行する。
- デバイスをコンプライアンス違反に設定する。
- デバイスを取り消す。
- より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信する。

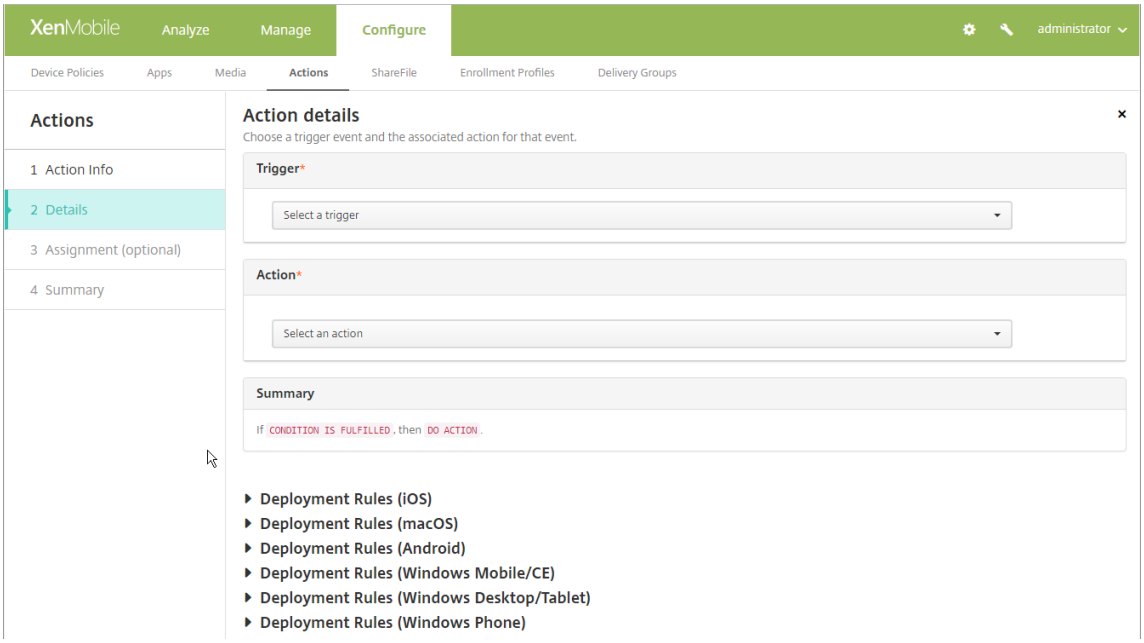
この記事では、自動化された操作の追加、編集、フィルターの方法、およびアプリロックおよびアプリワイプ操作を MAM-only モード用に構成する方法について説明します。

> 注：
>
> ユーザーに通知するには、XenMobile がメッセージを送信できるように、XenMobile の設定で通知サーバー

> (SMTP および SMS) を構成している必要があります。詳しくは、「通知」を参照してください。また、続行する前に使用予定の通知テンプレートを設定します。詳しくは、「通知テンプレートの作成および更新」を参照してください。

1. XenMobile コンソールで、［構成］の［操作］ をクリックします。［アクション］ ページが開きます。
2. ［アクション］ ページで、次のいずれかを行います:
   - ［追加］ をクリックして操作を追加します。
   - 編集または削除する既存の操作を選択します。使用するオプションをクリックします。
3. ［アクション情報］ ページが開きます。
4. ［アクション情報］ ページで、次の情報を入力または変更します:
   - 名前: 操作を識別する名前を入力します。このフィールドは必須です。
   - 説明: 操作の意図する内容を説明します。
5. ［次へ］ をクリックします。［アクションの詳細］ ページが開きます。

   次の例はイベントトリガーの設定方法を示しています。別のトリガーを選択した場合、この図で示されているものとは異なるオプションになります。



6. ［アクションの詳細］ ページで、次の情報を入力または変更します:

   ［トリガー］ 一覧で、この操作に対するイベントトリガーの種類をクリックします。各トリガーの意味は次のとおりです:

   - イベント: 定義済みのイベントに対応します。
   - デバイスプロパティ: MDM モードで収集されたデバイスのデバイス属性を確認して、それに対応します。詳しくは、「デバイスのプロパティ名と値」を参照してください。
   - ユーザープロパティ: ユーザー属性（通常、Active Directory からの属性）に対応します。

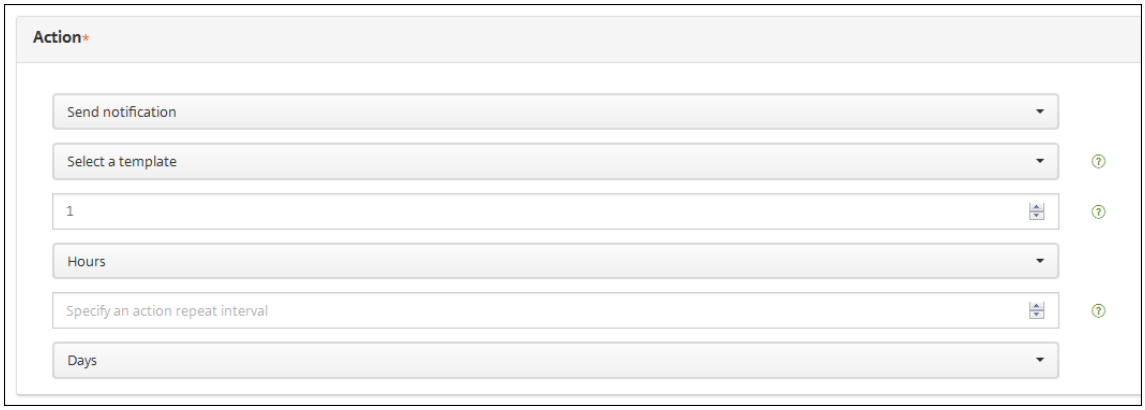
- インストールされているアプリ名: インストール中のアプリに対応します。MAM-only モードには適用されません。デバイスでアプリインベントリポリシーを有効にする必要があります。デフォルトでは、アプリインベントリポリシーはすべてのプラットフォームで有効です。詳しくは、「アプリインベントリデバイスポリシー」を参照してください。

7. 次の一覧で、トリガーに対する応答をクリックします。
8. [アクション] の一覧で、トリガーの条件が満たされたときに実行される操作をクリックします。[通知を送信] 以外では、トリガーの原因となった問題をユーザーが解決できる期間を選択します。その期間内に問題が解決されない場合は、選択した操作が実行されます。操作の定義については、「セキュリティ操作」を参照してください。

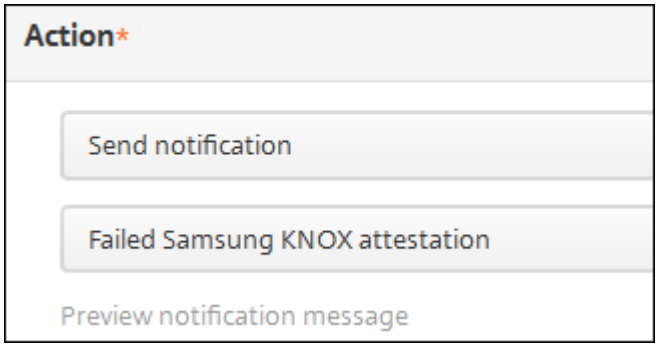
   [通知を送信] を選択した場合は、次の手順を実行して通知を送信します。

9. 次の一覧で、通知に使用するテンプレートを選択します。選択したイベントに関連した通知テンプレートが表示されます（通知の種類に既にテンプレートが存在する場合）。テンプレートがない場合、テンプレートの構成を促す次のメッセージが表示されます: このイベントの種類用のテンプレートはありません。[設定] の通知テンプレートを使用してテンプレートを作成します。

   ユーザーに通知するには、XenMobile がメッセージを送信できるように、[設定] で通知サーバー（SMTP および SMS）を構成している必要があります。次を参照してください。通知 また、続行する前に使用予定の通知テンプレートを設定します。通知テンプレートの設定について詳しくは、「通知テンプレートの作成および更新」を参照してください。



テンプレートを選択した後、[通知メッセージをプレビュー] をクリックして通知をプレビュー表示できます。



10. 次のフィールドでは、操作を実行するまでの遅延を日、時間、または分単位で設定します。ユーザーがトリガーの問題に対処するまで、操作が繰り返される間隔を設定します。

11. ［概要］ で、意図したとおりに、自動化された操作を作成したことを確認します。

12. 操作の詳細を構成したら、プラットフォームごとに個別に展開規則を構成できます。これを行うには、選択した各プラットフォームに対して、手順 13 を実行します。

13. 展開規則を構成します展開規則の構成に関する一般情報については、「リソースの展開」を参照してください。

    この例の場合:

    - デバイスの所有権は **BYOD** でなければなりません。
    - デバイスのローカル暗号化は **True** でなければなりません。
    - デバイスはパスコードに準拠している必要があります。
    - デバイスのモバイル国コードを Andorra のみにすることはできません。

14. 操作のプラットフォームの展開規則の構成が完了したら、［次へ］ をクリックします。アクション割り当てのページが開きます。ここで操作をデリバリーグループに割り当てます。この手順はオプションです。

15. ［デリバリーグループを選択］ の横にデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが ［アプリ割り当てを受信するためのデリバリーグループ］ 一覧に表示されます。

16. ［展開スケジュール］を展開して以下の設定を構成します:

    - ［展開］ の横の ［オン］ をクリックすると展開がスケジュールされ、［オフ］ をクリックすると展開が行われません。デフォルトのオプションは ［オン］ です。［オフ］ を選択した場合、そのほかのオプションは必要はありません。
    - ［展開スケジュール］ の横の ［すぐに］ または ［あとで］ をクリックします。デフォルトのオプションは ［すぐに］ です。
    - ［あとで］ をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    - ［展開状態］ の横の ［接続するたび］ をクリックするか、［以前の展開が失敗した場合のみ］ をクリックします。デフォルトのオプションは、［接続するたび］ です。

- ［常時接続に対する展開］ の横の ［オン］ または ［オフ］ をクリックします。デフォルトのオプションは ［オフ］ です。

  このオプションは、［設定］ **>** ［サーバープロパティ］ において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOS デバイスでは使用できません。

構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただし iOS には、［常時接続に対する展開］ は適用されません。

17. ［次へ］ をクリックします。［概要］ ページが開きます。ここで操作の構成を確認できます。
18. ［保存］ をクリックして変更を保存します。

MAM-only モードでのアプリロックとアプリワイプ操作

XenMobile コンソールに一覧表示されたトリガーの 4 種類のカテゴリすべてに応じて、デバイスでアプリをワイプまたはロックできます：トリガーの種類は、「イベント」、「デバイスプロパティ」、「ユーザープロパティ」、「インストール済みアプリ名」です。

自動でアプリのワイプまたはロックを構成するには

1. XenMobile コンソールで、［構成］の［アクション］ をクリックします。
2. ［アクション］ ページで、［追加］ をクリックします。
3. ［アクション情報］ ページで、アクションの名前および任意で説明を入力します。
4. ［アクションの詳細］ ページで、目的のトリガーを選択します。
5. ［アクション］ でアクションを選択します。

   この段階で、以下の条件に注意してください：

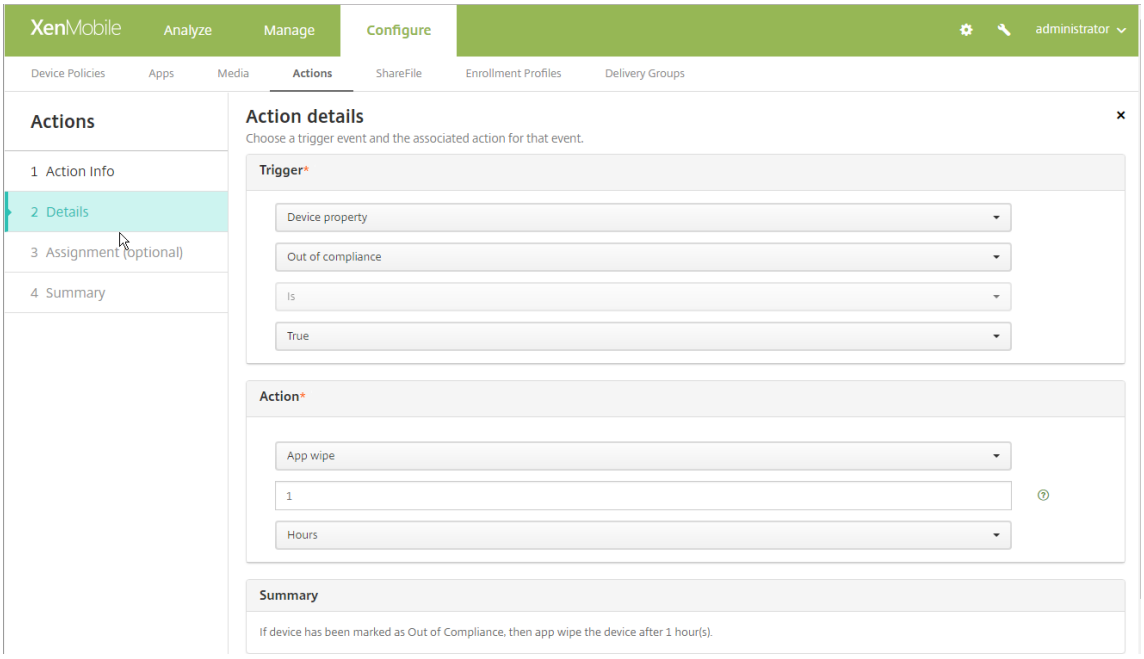
   トリガーの種類が ［イベント］ で値が ［**Active Directory** 無効ユーザー］ ではない場合、［アプリのワイプ］ および ［アプリのロック］ アクションは表示されません。

   トリガーの種類が ［デバイスプロパティ］ で値が ［**MDM** の紛失モードが有効になっています］ である場合、次のアクションは表示されません：

   - デバイスを選択的にワイプ
   - デバイスを完全にワイプ
   - デバイスを取り消す

   各オプションでは、自動で 1 時間の遅延が設定されていますが、遅延の期間は分単位、時間単位、日数単位を選択できます。遅延の目的は、アクションが発生する前に問題を修正する時間をユーザーに与えることです。［アプリのワイプ］ および［アプリのロック］ アクションの詳細については、「セキュリティ操作」を参照してください。

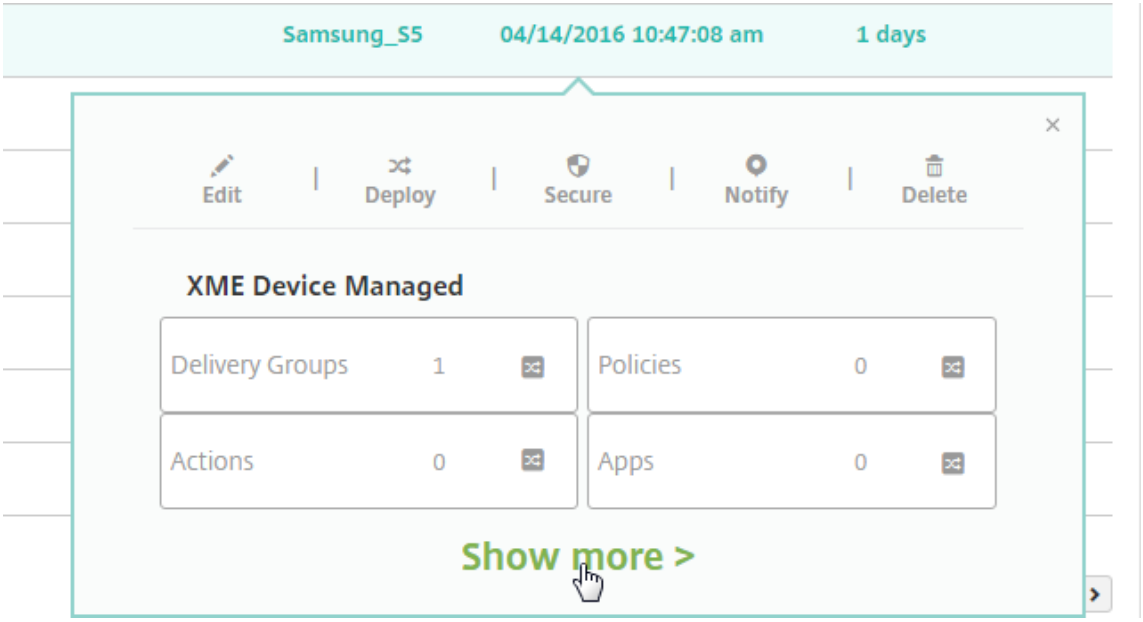
> 注:
>
> トリガーを ［イベント］ に設定すると、繰り返し間隔は自動的に最小 1 時間となります。通知を生成するには、デバイスはポリシーの更新を実行して、サーバーと同期する必要があります。通常、ユーザーのサインオン時、または Secure Hub でポリシーを手動で更新すると、デバイスはサーバーと同期します。
>
> Active Directory データベースと XenMobile との同期を許可するアクションが実行される前に、さらに約 1 時間、遅延を追加できます。



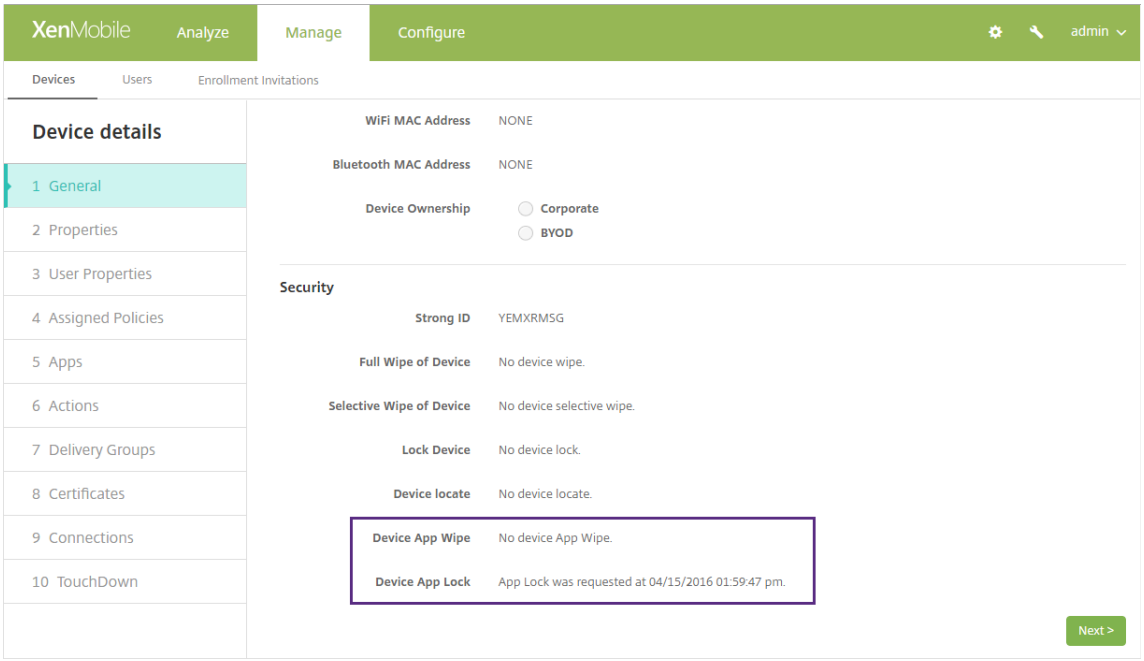
6. 展開規則を構成して、［次へ］ をクリックします。
7. デリバリーグループの割り当てと展開スケジュールを構成して、［次へ］ をクリックします。
8. ［保存］ をクリックします。

アプリロックとアプリワイプの状態を確認するには

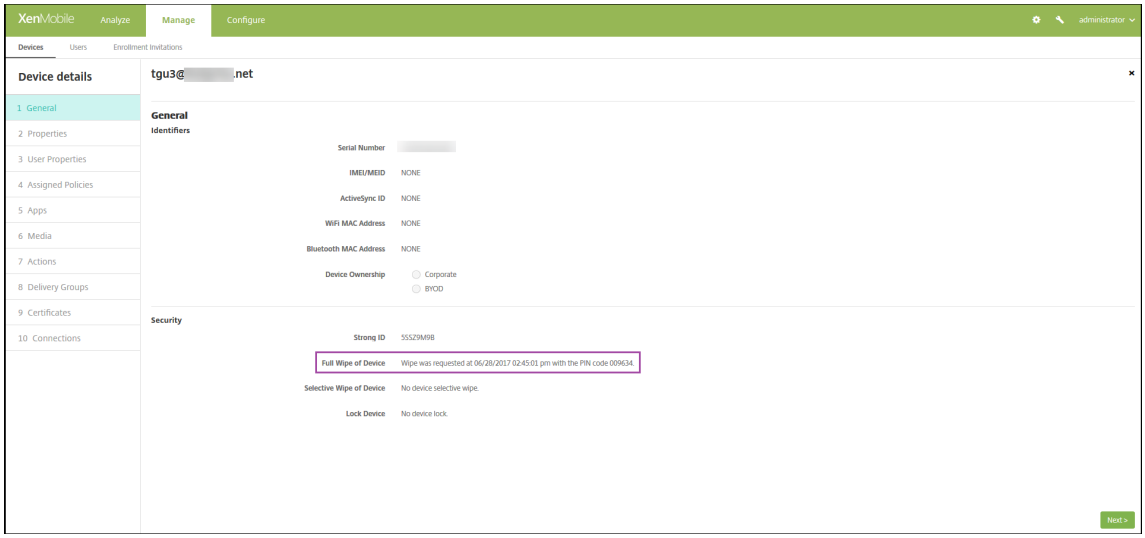
1. ［管理］ > ［デバイス］ に移動し、デバイスをクリックしてから ［詳細表示］ をクリックします。



2. [デバイスのアプリのワイプ] および [デバイスのアプリのロック] までスクロールします。



デバイスがワイプされると、PIN コードの入力を要求するメッセージがユーザーに表示されます。ユーザーがコードを忘れた場合は、[デバイス詳細] で確認できます。



モニターとサポート

January 10, 2020

XenMobile ダッシュボードと XenMobile サポートページを使用して、XenMobile Server の監視およびトラブルシューティングができます。XenMobile サポートページを使用して、サポートに関連する情報とツールにアクセスします。

オンプレミスの XenMobile Server の場合は、XenMobile CLI から操作を実行することもできます。詳しくは、「コマンドラインインターフェイスオプション」を参照してください。

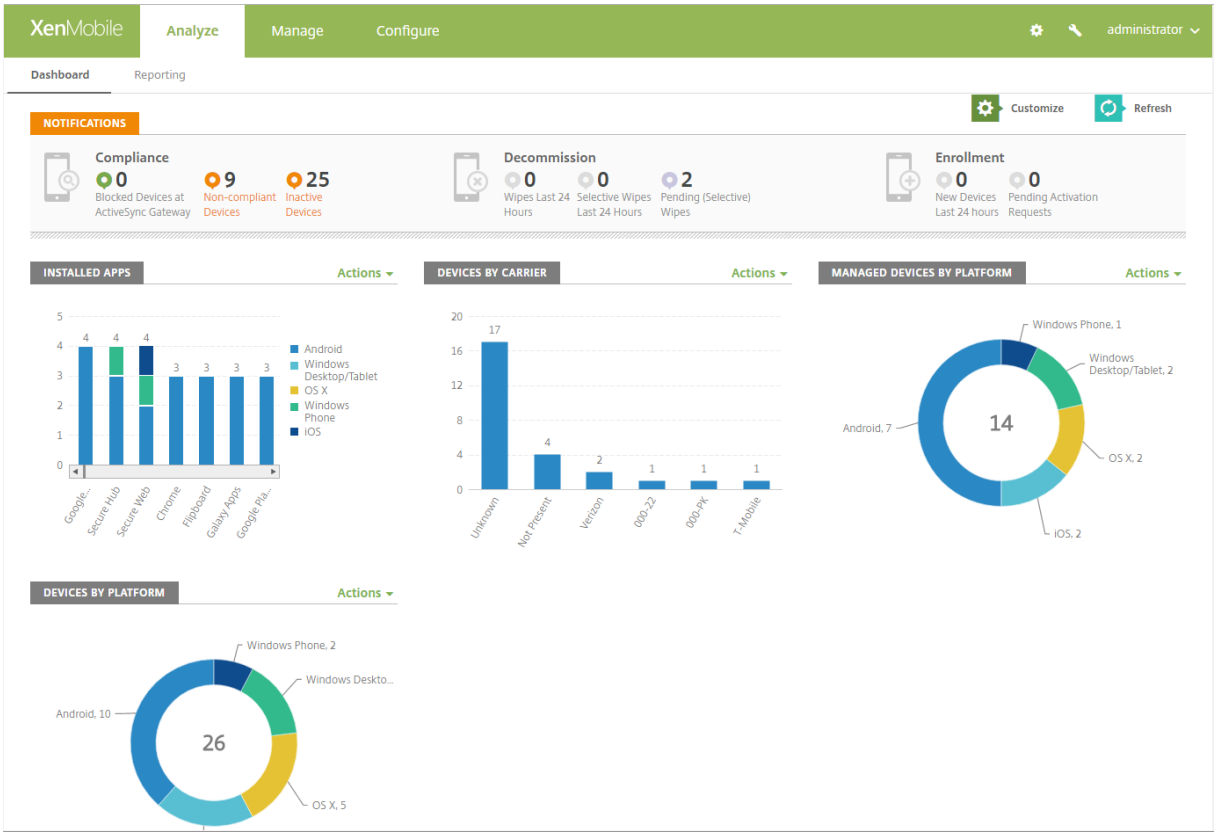
XenMobile コンソールで、右上のレンチアイコンをクリックします。

[トラブルシューティングとサポート] ページが開きます。

[サポート] ページを使用して以下を行います。

- 診断へのアクセス
- サポートバンドルの作成（オンプレミスインストールのみ）
- Citrix 製品ドキュメントおよび Knowledge Center へのリンクへのアクセス
- ログ操作へのアクセス
- 高度な構成オプションの使用
- 一連のツールおよびユーティリティへのアクセス

XenMobile コンソールのダッシュボードにアクセスして、情報を一目で確認することもできます。この情報を使用して、ウィジェットで問題や成功を速やかに確認できます。



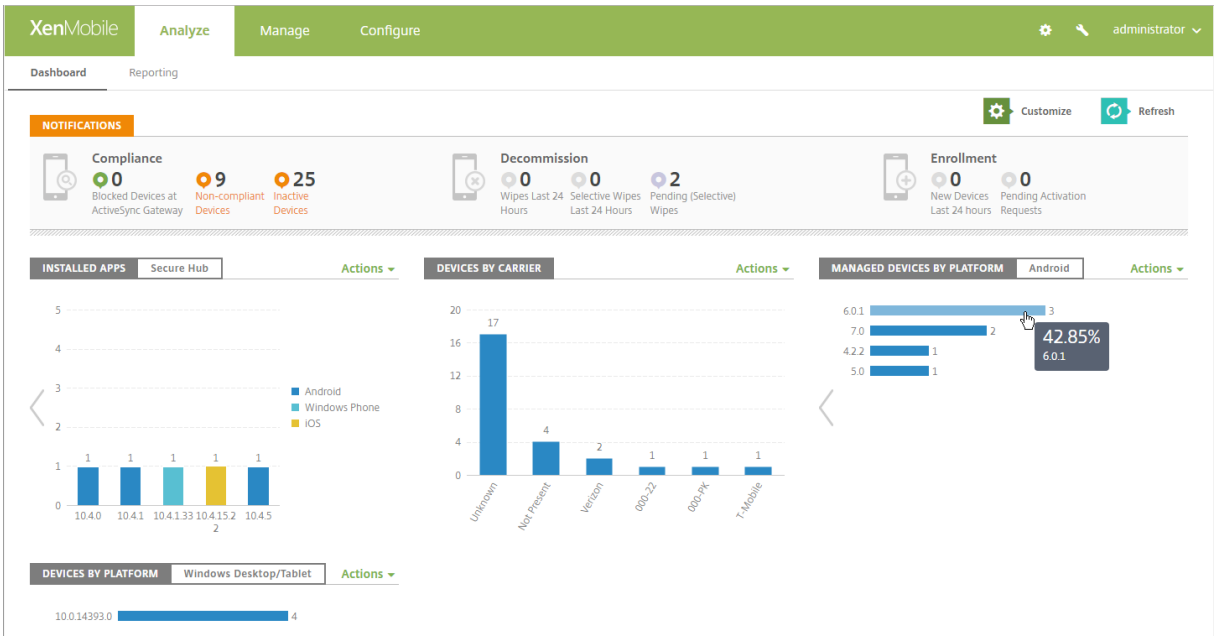
ダッシュボードは、XenMobile コンソールにサインオンすると最初に表示されるページです。コンソールの別の場所からダッシュボードにアクセスするには、［分析］ をクリックします。ページのレイアウトを編集したり表示されるウィジェットを編集するには、ダッシュボードの ［カスタマイズ］ をクリックします。

- マイダッシュボード： 最大 4 つのダッシュボードを保存できます。ダッシュボードを個別に編集し、保存したダッシュボードを選択してそれぞれを表示することができます。
- レイアウトスタイル： この行では、ダッシュボードに表示するウィジェットの数とレイアウトを選択することができます。
- ウィジェット選択： ダッシュボードに表示する情報を選択することができます。
  - 通知： 左側の数字の上のチェックボックスをオンにして、ウィジェットの上に通知バーを追加します。このバーには、準拠デバイス数、非アクティブデバイス数、24 時間以内にワイプまたは登録されたデバイス数が表示されます。
  - プラットフォームごとのデバイス： プラットフォームごとの管理対象デバイス数と管理対象外デバイス数が表示されます。
  - キャリアごとのデバイス： キャリアごとの管理対象デバイス数と管理対象外デバイス数が表示されます。各バーをクリックすると、プラットフォームごとの内訳が表示されます。
  - プラットフォームにより管理されているデバイス： プラットフォームごとの管理対象デバイス数が表示されます。
  - プラットフォームにより管理されていないデバイス： プラットフォームごとの管理対象外デバイス数が表示されます。このグラフに表示されるデバイスにはエージェントがインストールされている場合があ

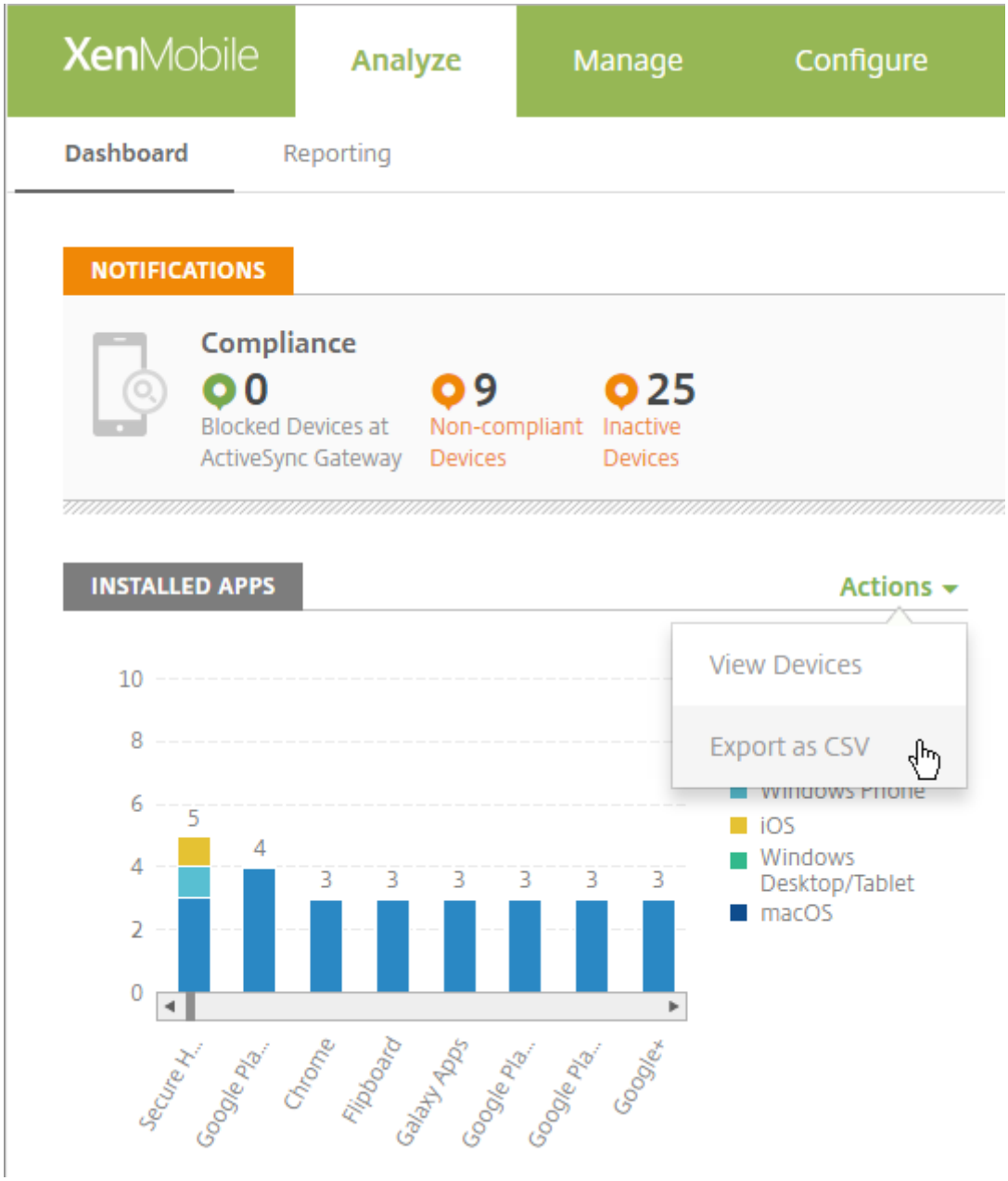
りますが、特権が失効またはワイプされています。

- **ActiveSync** ゲートウェイ状態ごとのデバイス: ActiveSync ゲートウェイの状態ごとにグループ化されたデバイス数が表示されます。この情報では拒否、許可、または不明の状態が表示されます。各バーをクリックするとプラットフォームごとの内訳が表示されます。
- 所有権ごとのデバイス: 所有権の状態ごとにグループ化されたデバイス数が表示されます。この情報ではコーポレート所有、従業員所有、または不明の所有権状態が表示されます。
- **Android TouchDown** ライセンス状態: TouchDown ライセンスがあるデバイス数が表示されます。
- 失敗したデリバリーグループ展開: 失敗した展開の合計数がパッケージごとに表示されます。展開に失敗したパッケージのみが表示されます。
- ブロックされた理由ごとのデバイス: ActiveSync でブロックされたデバイス数が表示されます。
- インストール済みアプリ: アプリ名を入力すると、アプリ情報のグラフが表示されます。
- **VPP** アプリライセンス使用状況: Apple Volume Purchase Program アプリのライセンス使用状況に関する統計データが表示されます。

各ウィジェットでは個々の部分をクリックして、さらに情報をドリルダウンできます。



[操作] のドロップダウンをクリックして、情報を.csv ファイルとしてエクスポートすることもできます。



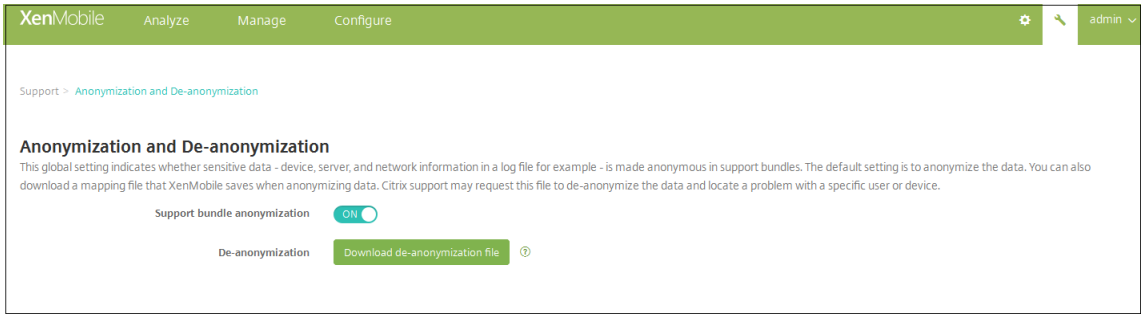
サポートバンドルのデータの匿名化

August 22, 2019

XenMobile でサポートバンドルを作成する場合、デフォルトでは、機密性の高いユーザー、サーバー、ネットワークのデータは匿名化されます。この動作は、[Anonymization and De-anonymization] ページで変更することができます。また、XenMobile がデータの匿名化時に保存したマッピングファイルをダウンロードすることもできます。データの匿名化を解除したり、ユーザーまたはデバイスで発生した問題を特定したりする目的で、Citrix のサポート

からこのファイルを要求される場合があります。

1. XenMobile コンソールで、右上のレンチアイコンをクリックします。［サポート］ ページが開きます。
2. ［サポート］ ページで、［上級］ の下の ［匿名化および匿名化解除］ をクリックします。［匿名化および匿名化解除］ ページが開きます。



3. ［サポートバンドルの匿名化］ で、データを匿名化するかどうかを選択します。デフォルトは ［オン］ です。
4. Citrix のサポートで問題の診断に特定のデバイスまたはユーザーの情報が必要な場合にサポートに送信するマッピングファイルを、［匿名化解除］ の横の ［匿名化解除ファイルのダウンロード］ をクリックしてダウンロードします。

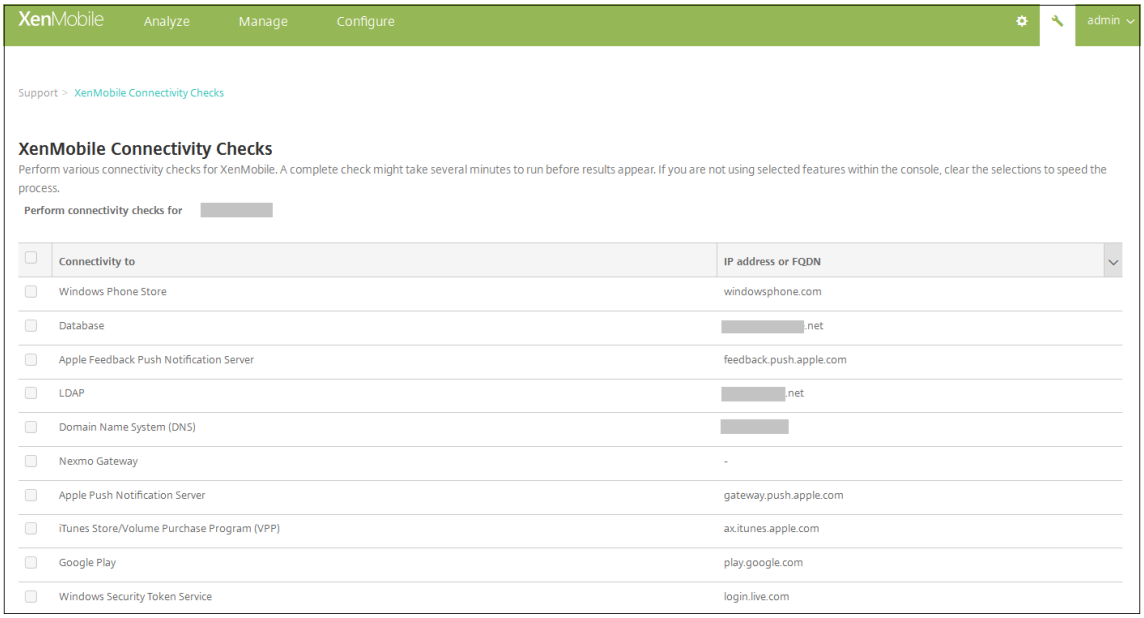
接続確認

August 22, 2019

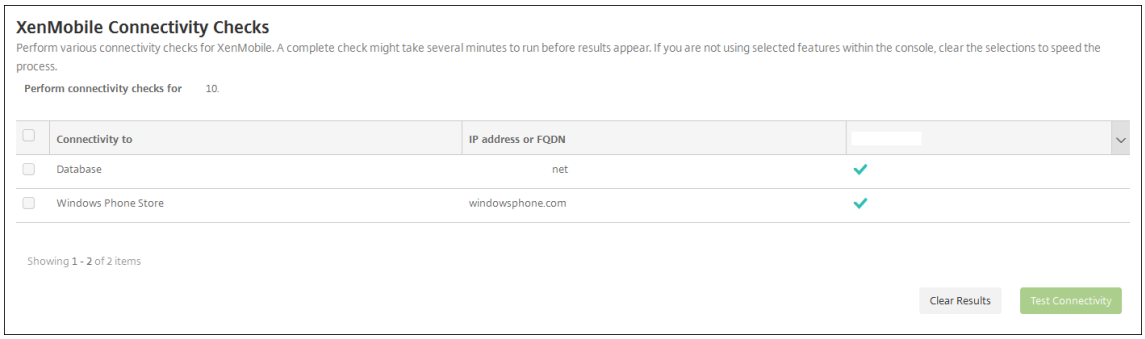
XenMobile の ［サポート］ ページで、NetScaler Gateway およびそのほかのサーバーや場所への XenMobile の接続を確認できます。

XenMobile の接続確認の実行

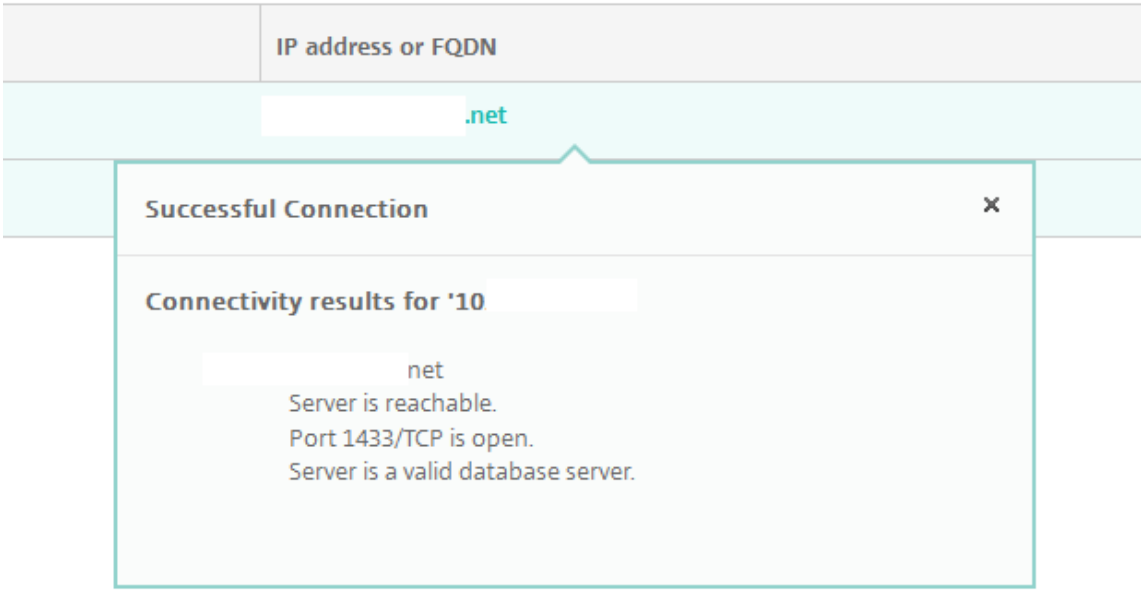
1. XenMobile コンソールで、右上のレンチアイコンをクリックします。［サポート］ ページが開きます。
2. ［診断］ の下の ［**XenMobile** 接続性チェック］ をクリックします。［**XenMobile** 接続性チェック］ ページが開きます。XenMobile 環境内にクラスターノードがある場合は、すべてのノードが表示されます。



3. 接続テストに含めるサーバーをオンにして、［接続性をテスト］をクリックします。［テスト結果］ページが開きます。

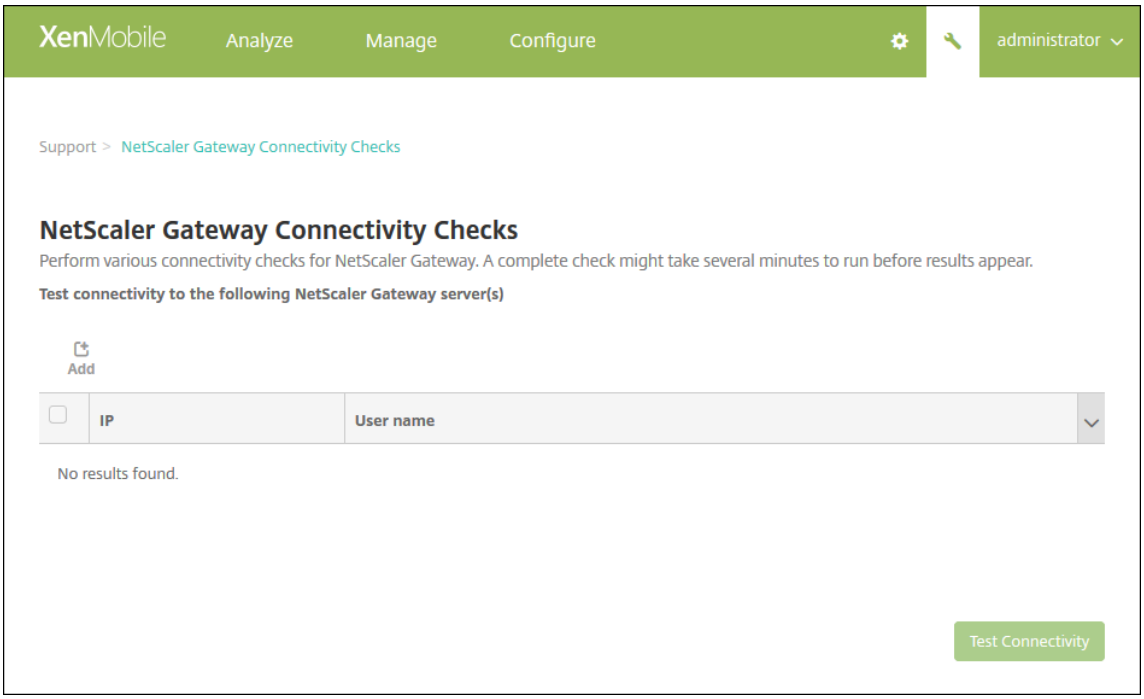


4. ［テスト結果］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

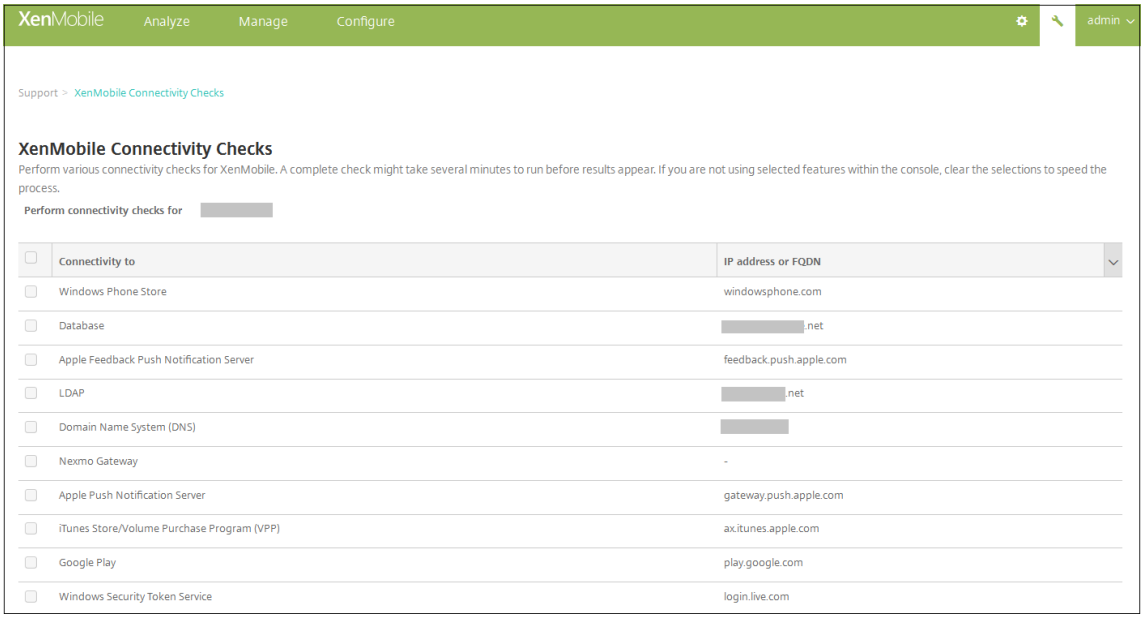


NetScaler Gateway の接続確認の実行

1. [サポート] ページで、[診断] の下の [**NetScaler Gateway** 接続性チェック] をクリックします。[**NetScaler Gateway** 接続性チェック] ページが開きます。NetScaler Gateway サーバーが追加されていない場合、表は空白です。



2. [追加] をクリックします。[**NetScaler Gateway** サーバーの追加] ダイアログボックスが開きます。



3. [**NetScaler Gateway** 管理 **IP**] ボックスに、テストする NetScaler Gateway を実行しているサーバーの管理 IP アドレスを入力します。

   > 注:
   >
   > 既に追加されている NetScaler Gateway サーバーの接続確認を実行する場合、IP アドレスは入力されています。

4. この NetScaler Gateway の管理者資格情報を入力します。

   > 注:
   >
   > 既に追加されている NetScaler Gateway サーバーの接続確認を実行する場合、ユーザー名は入力されています。

5. [追加] をクリックします。NetScaler Gateway が、[**NetScaler Gateway** 接続性チェック] ページの表に追加されます。
6. NetScaler Gateway サーバーを選択して、[接続性をテスト] をクリックします。[テスト結果] の表に結果が表示されます。
7. [テスト結果] の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

カスタマーエクスペリエンス向上プログラム

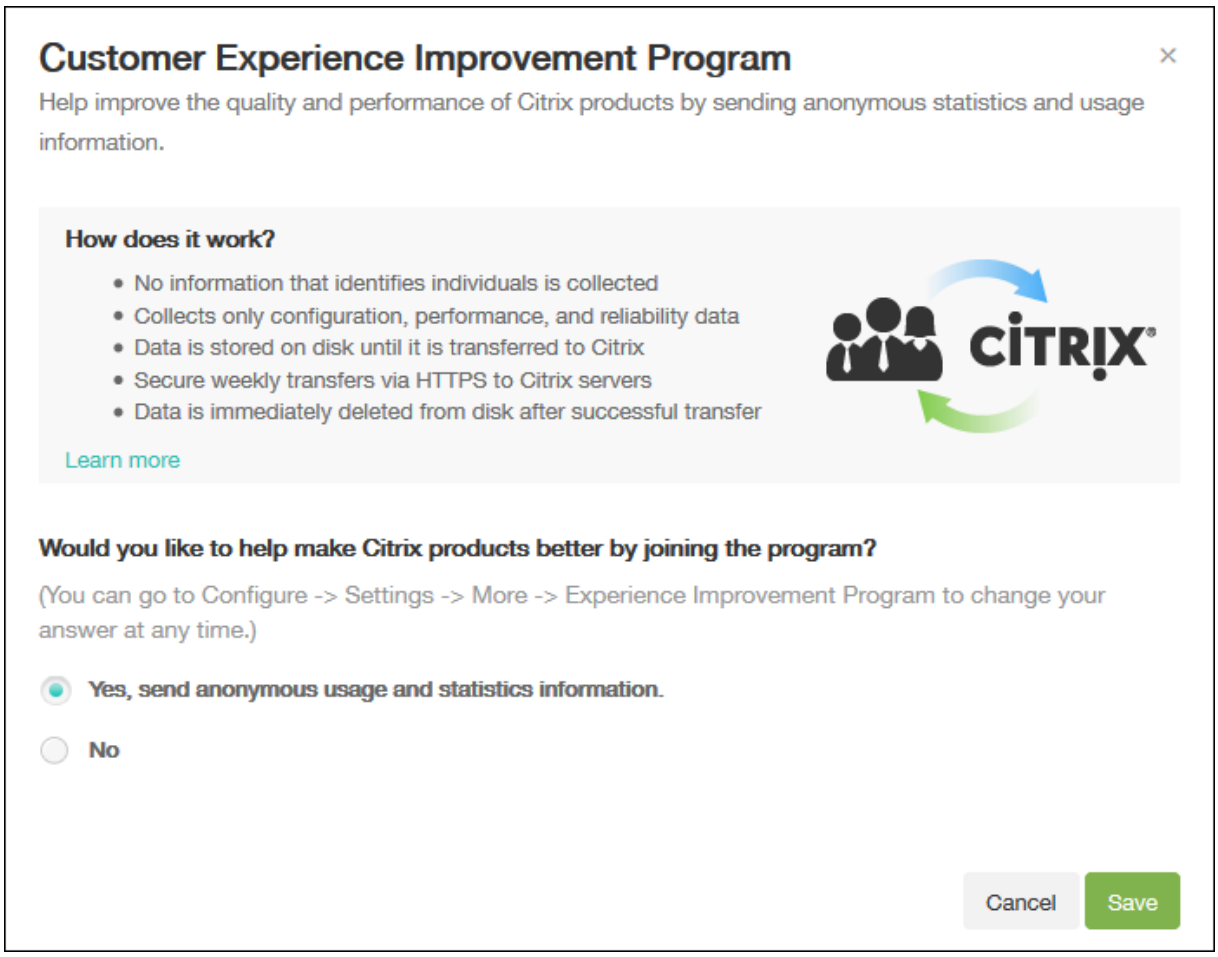
August 22, 2019

Ctrix カスタマーエクスペリエンス向上プログラム（CEIP）では、XenMobile の構成および使用に関するデータが匿名で収集され、そのデータが Citrix に自動的に送信されます。このデータは、XenMobile の品質、信頼性、およ

びパフォーマンスを向上させる目的で使用させていただきます。CEIP へのご参加は任意です。XenMobile の初回インストール時、または更新のインストール時に、CEIP への参加が可能です。選択した場合、データは通常週単位で、パフォーマンスおよび使用に関するデータは時間単位で収集されます。これらのデータはディスク上に格納され、1 週間ごとに HTTPS により安全にシトリックスに送信されます。CEIP に参加するかどうかは、XenMobile コンソールで変更できます。CEIP について詳しくは、「カスタマーエクスペリエンス向上プログラム（CEIP）について」を参照してください。

CEIP で参加を選択する

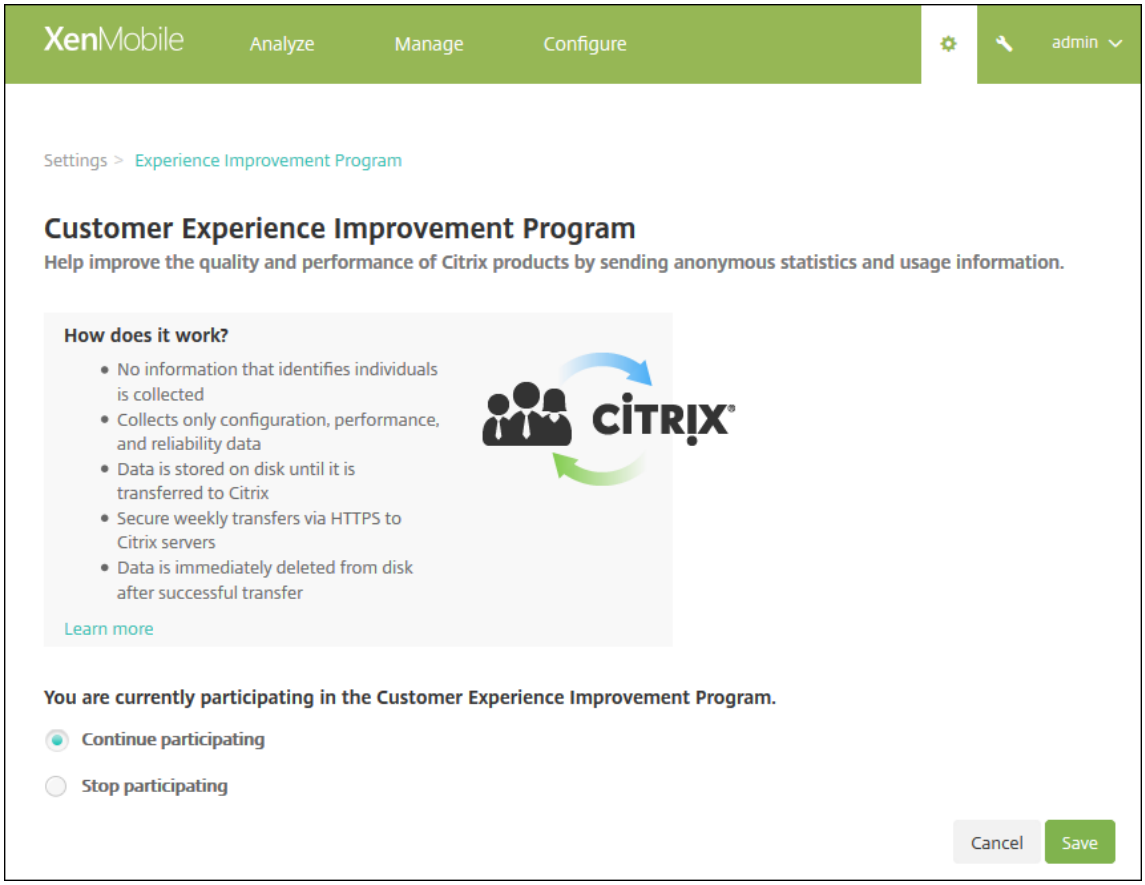
XenMobile の初回インストール時、または更新時に、参加を促す以下のダイアログボックスが開きます。



CEIP 参加設定の変更

1. CEIP 参加設定を変更するには、XenMobile コンソールで右上の歯車アイコンをクリックして ［設定］ ページを開きます。
2. ［サーバー］ の下で ［エクスペリエンス向上プログラム］ をクリックします。［カスタマーエクスペリエンス

向上プログラム] ページが開きます。表示される実際のページは、現在 CEIP に参加しているかどうかによって異なります。



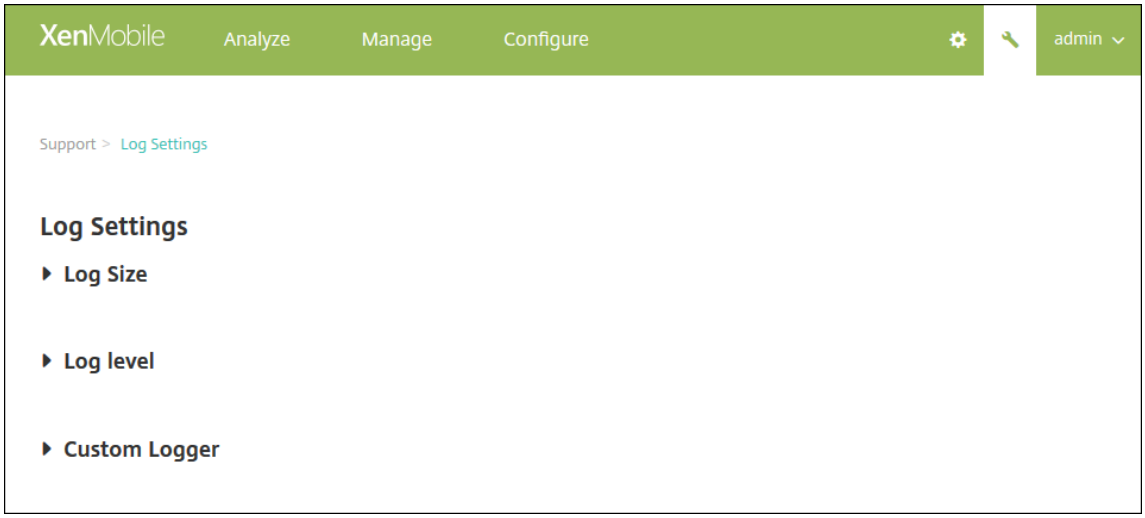
3. 現在 CEIP に参加していて、中止を希望する場合、［参加停止］ をクリックします。
4. 現在 CEIP に参加していなくて、開始を希望する場合、［参加開始］ をクリックします。
5. ［保存］ をクリックします。

ログ

January 10, 2020

ログ設定を構成して、XenMobile で生成されるログの出力をカスタマイズすることができます。XenMobile サーバーをクラスター化している場合は、XenMobile コンソールでログ設定を構成すると、その設定はクラスター内のほかのすべてのサーバーと共有されます。

1. XenMobile コンソールで、右上のレンチアイコンをクリックします。［サポート］ ページが開きます。
2. ［ログの操作］ の下の ［ログ設定］ をクリックします。［ログ設定］ ページが開きます。

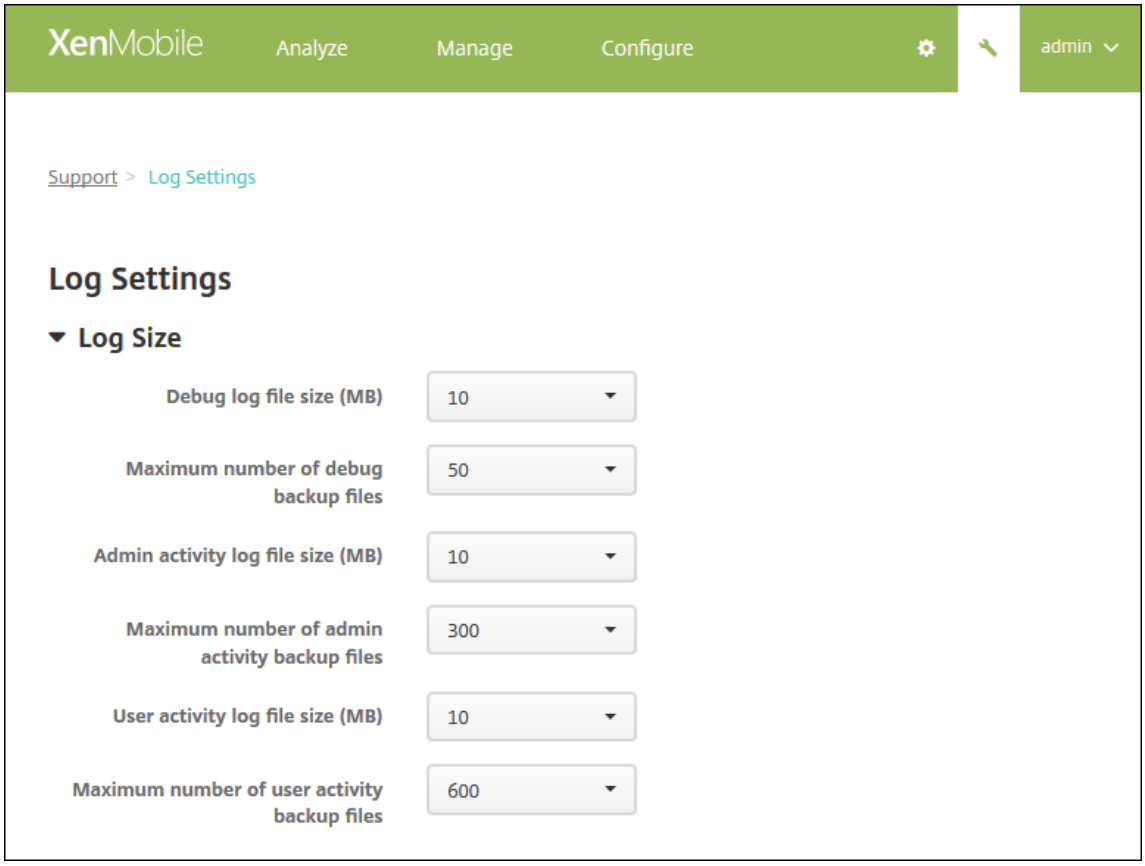


［ログ設定］ ページでは、以下のオプションにアクセスできます。

- ログサイズ。このオプションを使用して、ログファイルのサイズと、データベースで保持されるログのバックアップファイルの最大数を制御します。ログのサイズは、XenMobile でサポートされる各ログ（デバッグログ、管理者アクティビティログ、およびユーザーアクティビティログ）に適用されます。
- ログレベル。このオプションを使用して、ログレベルを変更したり、設定を永続的にしたりします。
- カスタムロガー。このオプションを使用して、カスタムロガーを作成します。カスタムログには、クラス名とログレベルが必要です。

［ログサイズ］のオプションを構成するには

1. ［ログ設定］ ページで ［ログサイズ］ を展開します。



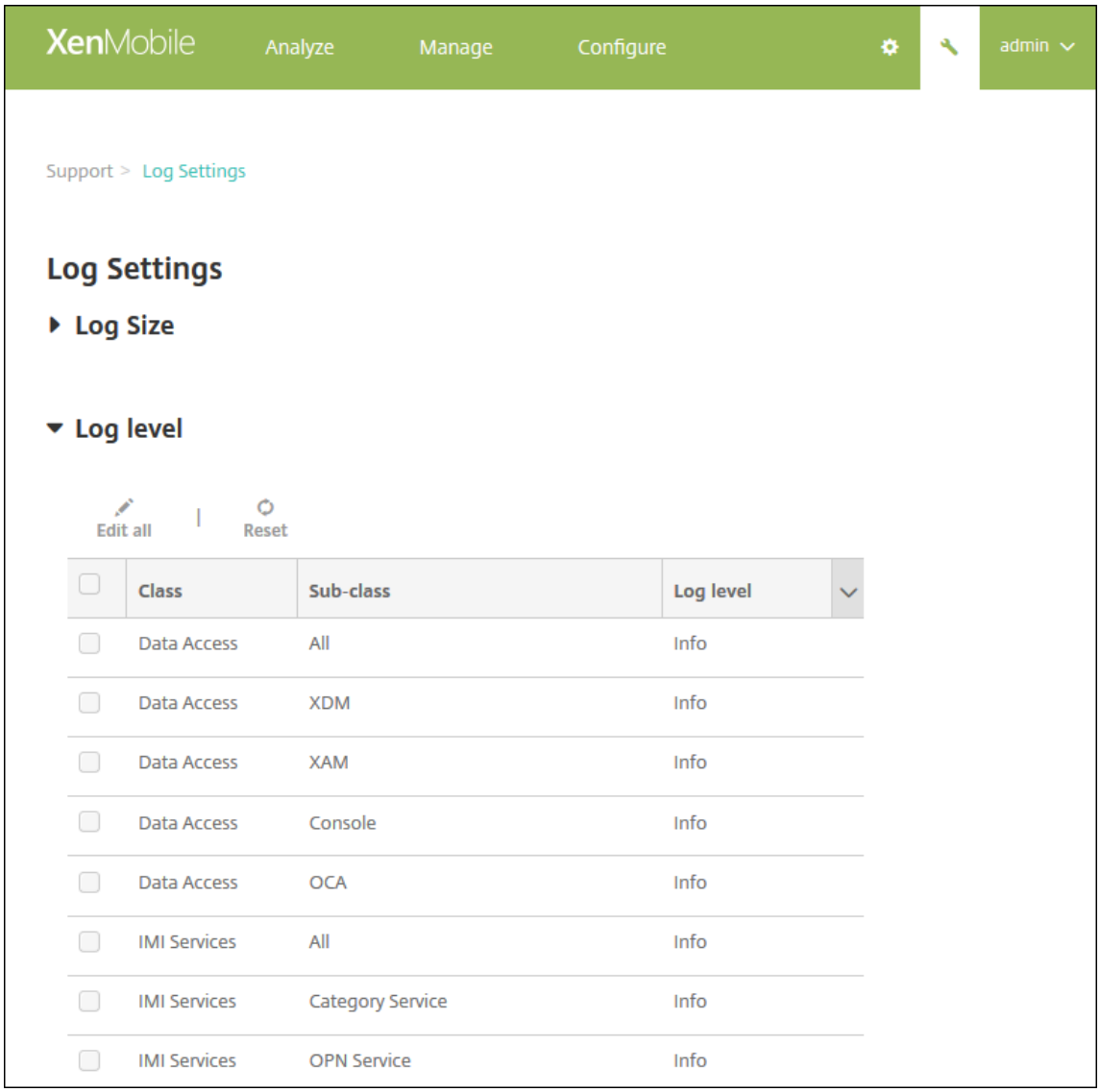
2. 次の設定を構成します。

   - デバッグログのファイルサイズ（**MB**）： 一覧からサイズ（5 ～ 20MB）を選択して、デバッグファイルの最大サイズを変更します。デフォルトのファイルサイズは **10 MB** です。
   - デバッグバックアップファイルの最大数： サーバーにより保持されるデバッグファイルの最大数をクリックします。デフォルトでは、サーバーに 50 件のバックアップファイルが保持されます。
   - 管理者アクティビティログのファイルサイズ（**MB**）： 一覧からサイズ（5 ～ 20MB）を選択して、管理者アクティビティファイルの最大サイズを変更します。デフォルトのファイルサイズは **10 MB** です。
   - 管理者アクティビティバックアップファイルの最大数： サーバーにより保持される管理者アクティビティファイルの最大数をクリックします。デフォルトでは、サーバーに 300 件のバックアップファイルが保持されます。
   - ユーザーアクティビティログのファイルサイズ（**MB**）：一覧からサイズ（5 ～ 20MB）を選択して、ユーザーアクティビティファイルの最大サイズを変更します。デフォルトのファイルサイズは **10 MB** です。
   - ユーザーアクティビティバックアップファイルの最大数： サーバーにより保持されるユーザーアクティビティファイルの最大数をクリックします。デフォルトでは、サーバーに 300 件のバックアップファイルが保持されます。

［ログレベル］のオプションを構成するには

ログレベルを設定することにより、XenMobile でログに収集される情報の種類を指定できます。すべてのクラスに同じレベルを設定することも、個別のクラスに特定のレベルを設定することもできます。

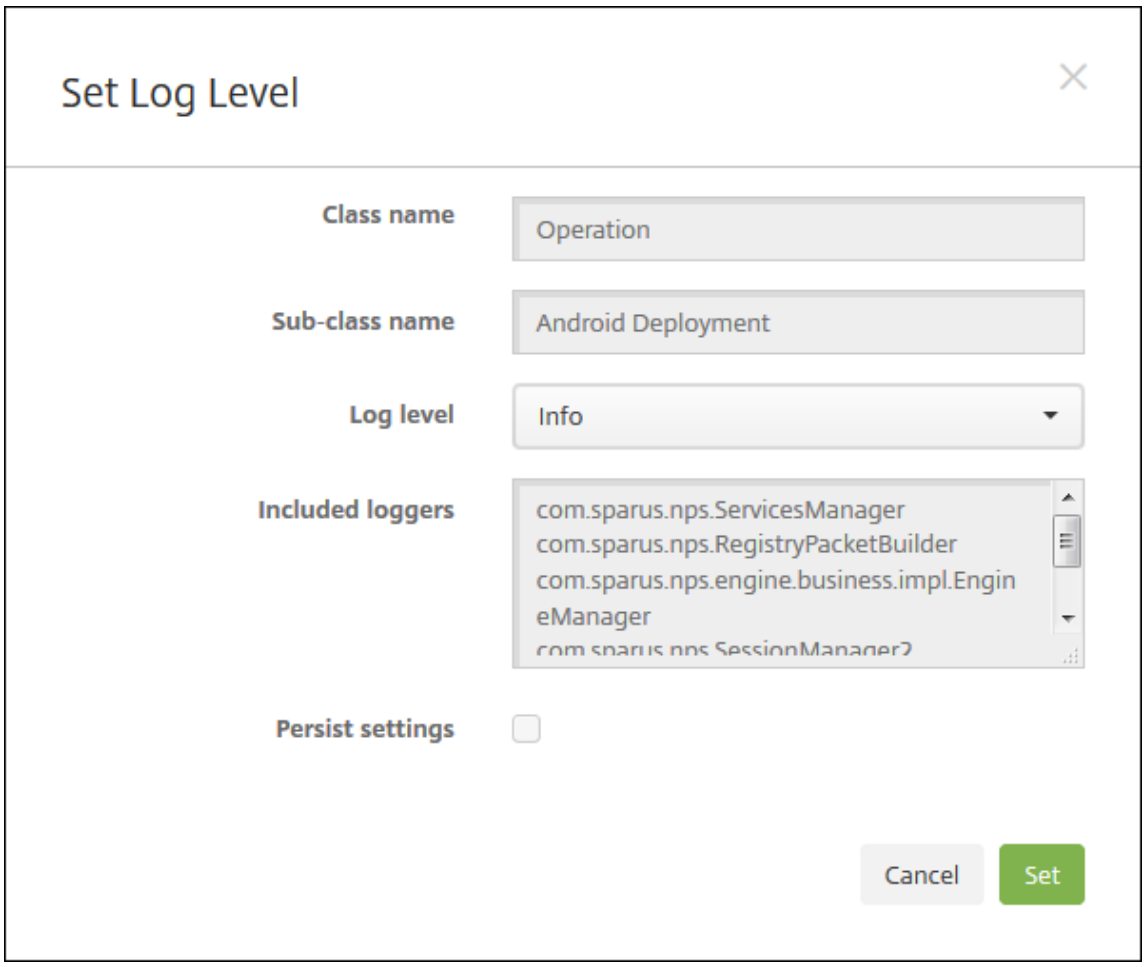
1. ［ログ設定］ ページで ［ログレベル］ を展開します。すべてのログクラスの表が表示されます。



2. 次のいずれかを行います:

   - 1 つのクラスの横のチェックボックスをクリックして ［レベルを設定］ をクリックし、そのクラスのログレベルのみを変更します。
   - ［すべて編集］ をクリックしてログレベルの変更を表内のすべてのクラスに適用します。

   ［ログレベルの設定］ ダイアログボックスが表示され、そこでログレベルを設定し、XenMobile サーバーを再起動したときにログレベル設定を維持するかどうかを選択できます。

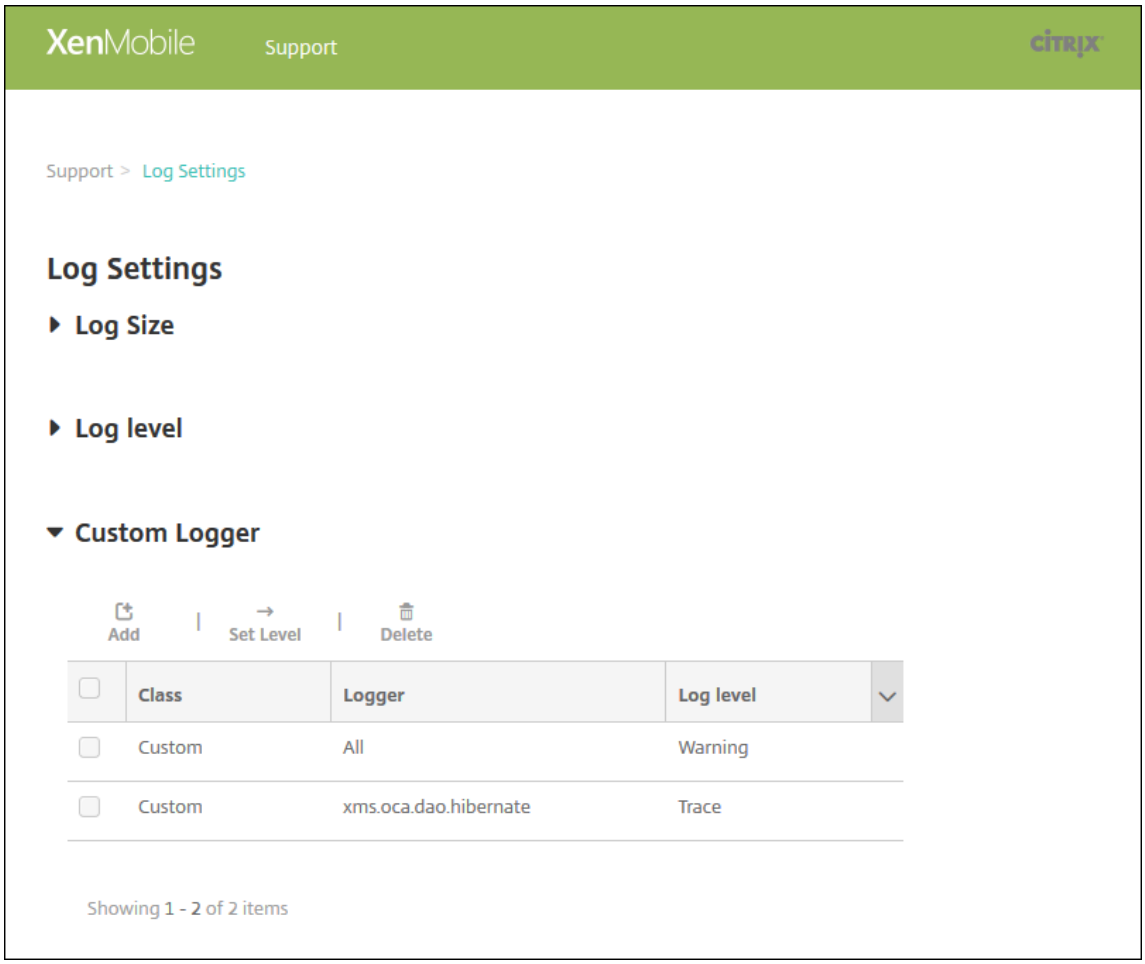


- クラス名： すべてのクラスのログレベルを変更する場合はこのフィールドに［すべて］と表示されます。そうでない場合は個別のクラス名が表示されます。編集できません。
- サブクラス名： すべてのクラスのログレベルを変更する場合はこのフィールドに［すべて］と表示されます。そうでない場合は個別のクラスのサブクラス名が表示されます。編集できません。
- ログレベル： 一覧でログレベルをクリックします。サポートされるログレベルは以下のとおりです。
  - 重大
  - エラー
  - 警告
  - 情報
  - デバッグ
  - トレース
  - 無効
- 含まれるロガー： すべてのクラスのログレベルを変更する場合はこのフィールドは空白です。そうでない場合は個別のクラスに対して現在構成されているロガーが表示されます。編集できません。
- 永続設定： サーバーを再起動してもログレベルの設定を維持する場合はこのチェックボックスをオンにします。このチェックボックスがオフの場合は、サーバーを再起動するとログレベル設定がデフォルト設定に戻ります。

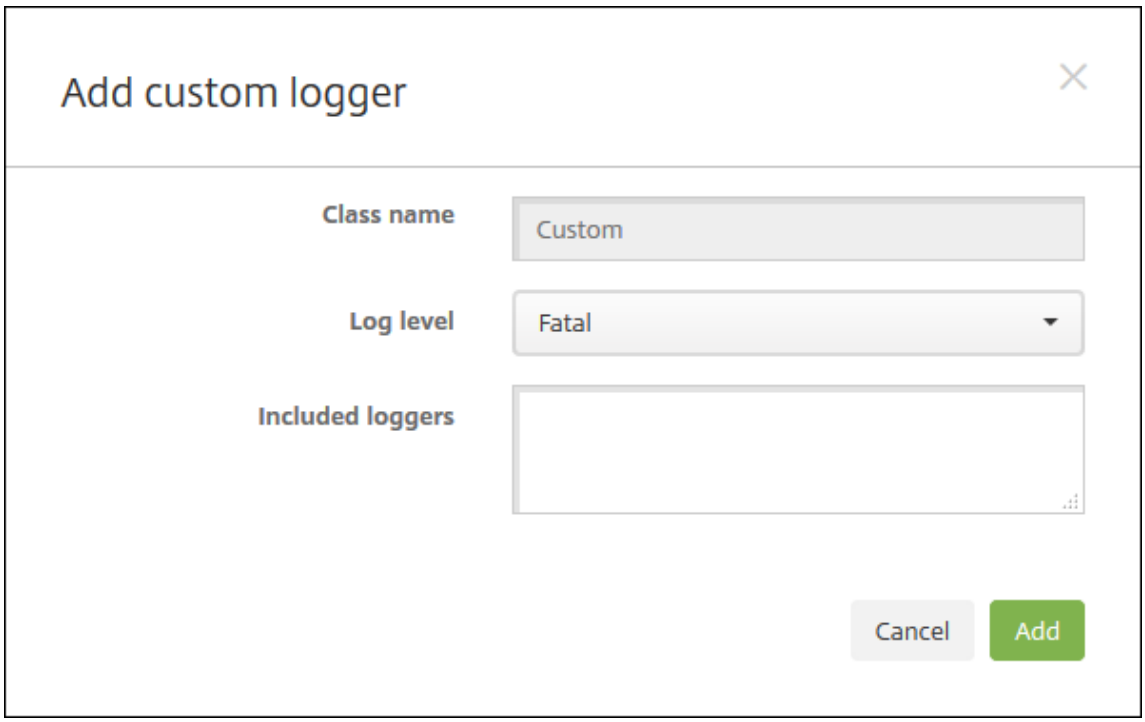
3. ［設定］ をクリックして変更を確定します。

カスタムロガーを追加するには

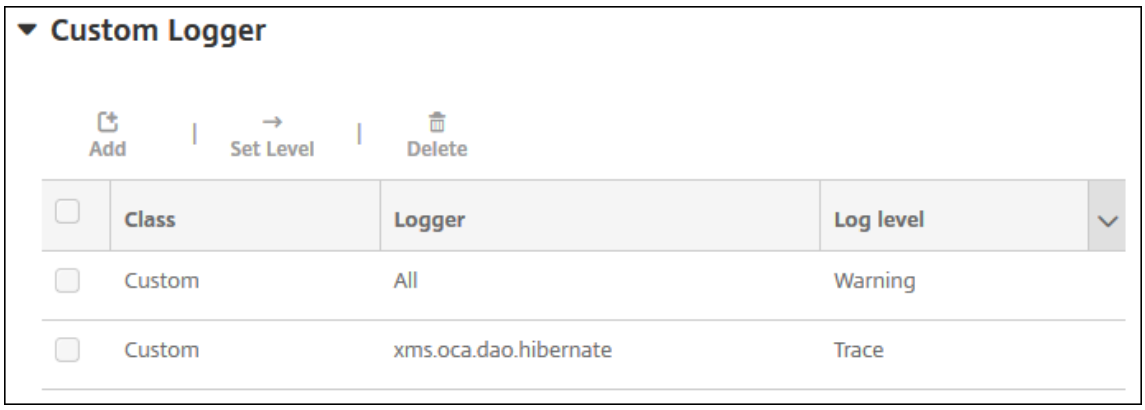
1. ［ログ設定］ ページで ［カスタムロガー］ を展開します。［カスタムロガー］ の表が表示されます。カスタムロガーがまだ追加されていない場合、最初はこの表が空白の状態で表示されます。



2. ［追加］ をクリックします。［カスタムロガーの追加］ ダイアログボックスが開きます。



3. 次の設定を構成します。
   - クラス名: このフィールドには ［カスタム］ と表示されます。編集できません。
   - ログレベル: 一覧でログレベルをクリックします。サポートされるログレベルは以下のとおりです。
     - 重大
     - エラー
     - 警告
     - 情報
     - デバッグ
     - トレース
     - 無効
   - 含まれるロガー: カスタムロガーに含める特定のロガーを入力するか、このフィールドを空白にしてすべてのロガーが含まれるようにします。
4. ［追加］ をクリックします。カスタムロガーが ［カスタムロガー］ の表に追加されます。



カスタムロガーを削除するには

1. [ログ設定] ページで [カスタムロガー] を展開します。
2. 削除するカスタムロガーを選択します。
3. [削除] をクリックします。カスタムロガーを削除するかどうかを確認するダイアログボックスが開きます。[**OK**] をクリックします。

   > 重要:
   >
   > この操作を元に戻すことはできません。

モバイルサービスプロバイダー

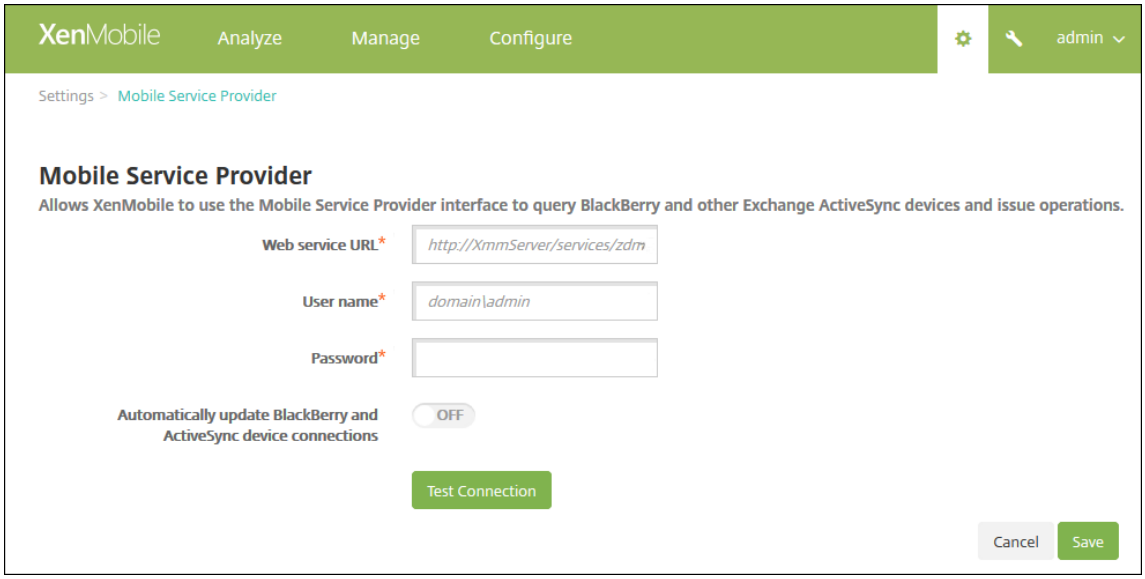
August 22, 2019

XenMobile でモバイルサービスプロバイダーインターフェイスの使用を有効にして、BlackBerry や Exchange ActiveSync デバイスに対してクエリを実行したり、操作を発行したりできます。

たとえば、組織に 1,000 ユーザーが存在し、各ユーザーが 1 つまたは複数のデバイスを使用するとします。すべてのユーザーに対して、管理のためにデバイスを XenMobile に登録する必要があることを通知した後、XenMobile コンソールはユーザーが登録したデバイスの数を表示します。この設定を構成することで、Exchange Server に接続しているデバイスの数を判断できます。これによって、次の操作を実行できます。

- ほかにデバイスを登録する必要のあるユーザーがいるかどうかを確認する。
- Exchange Server に接続するユーザーデバイスにコマンド（データワイプなど）を発行する。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。[設定] ページが開きます。
2. [サーバー] の下の [モバイルサービスプロバイダー] をクリックします。[モバイルサービスプロバイダー] ページが開きます。



3. 次の設定を構成します。
   - **Web サービス URL**: Web サービスの URL（`https://<XmmServer>/services/xdmservice`など）を入力します。
   - ユーザー名: domain\admin の形式でユーザー名を入力します。
   - パスワード: パスワードを入力します。
   - **BlackBerry** および **ActiveSync** デバイス接続を自動的に更新: デバイス接続を自動的に更新するかどうかを選択します。デフォルトは ［オフ］ です。
   - ［接続のテスト］ をクリックして、接続を検証します。
4. ［保存］ をクリックします。

レポート

August 22, 2019

XenMobile には、以下の事前定義されたレポートが用意されており、アプリケーションおよびデバイスの展開を分析できます。各レポートは表とグラフで表示されます。表は、列を基準にして並び替えとフィルターを行うことができます。グラフ内の要素を選択すると詳細を確認できます。

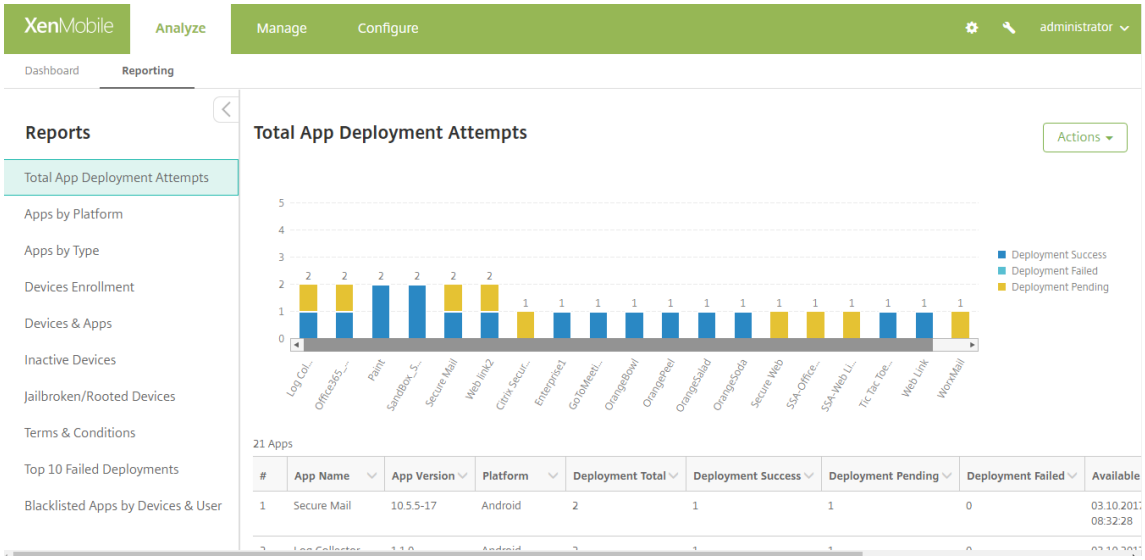
- アプリ展開の合計試行回数: ユーザーがデバイスへのインストールを試みた展開済みのアプリを一覧表示します。
- プラットフォームを基準とするアプリ: アプリとアプリバージョンを、デバイスプラットフォーム別およびバージョン別に一覧表示します。
- 種類別アプリ: アプリをバージョン別、種類別、およびカテゴリ別に一覧表示します。
- デバイス登録: すべての登録済みデバイスを一覧表示します。

- デバイスおよびアプリ: 管理対象アプリを実行しているデバイスを一覧表示します。
- 非アクティブデバイス: XenMobile サーバーのプロパティ device.inactivity.days.threshold で指定された日数にわたりアクティビティがないデバイスを一覧表示します。
- ジェイルブレイク/**Root** 化されたデバイス: ジェイルブレイクされた iOS デバイスと Root 化された Android デバイスを一覧表示します。
- 使用条件: 使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。グラフの各領域を選択すると詳細を確認できます。
- 上位 **10** のアプリ: 失敗した展開 - 展開に失敗したアプリを最大で 10 個まで一覧表示します。
- ユーザーがデバイスごとにブラックリストに登録したアプリ: ユーザーのデバイスに存在し、ブラックリストに登録されているアプリを一覧表示します。

各表のデータを、Microsoft Excel などのプログラムで開くことが可能な.csv 形式でエクスポートできます。各レポートのグラフは PDF 形式でエクスポートできます。

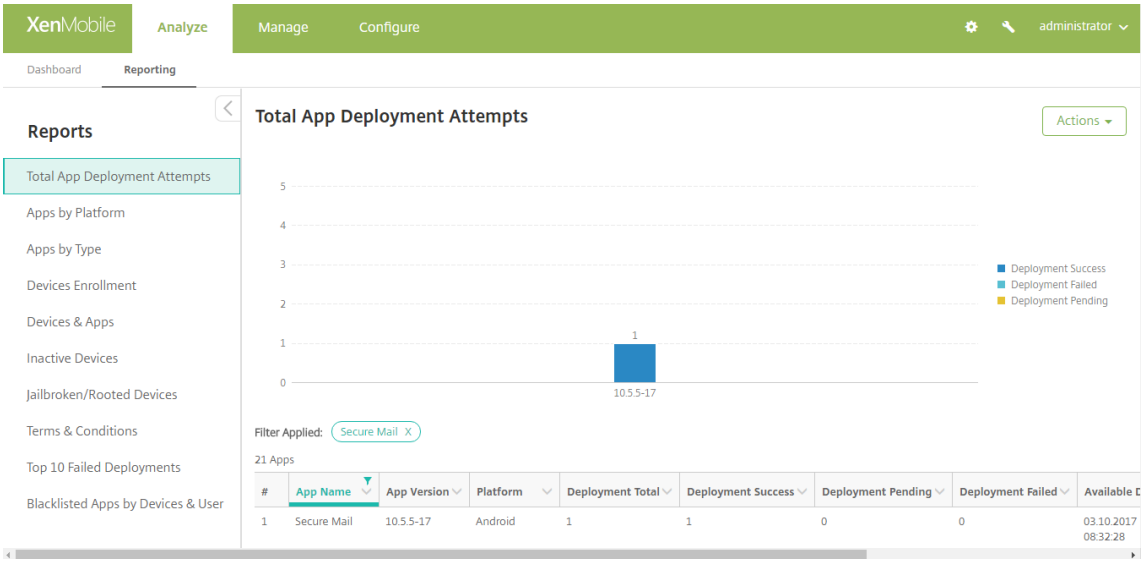
レポートを作成するには

1. XenMobile コンソールで ［分析］ **>** ［レポート］ の順にクリックします。［レポート］ ページが開きます。
2. 作成するレポートをクリックします。

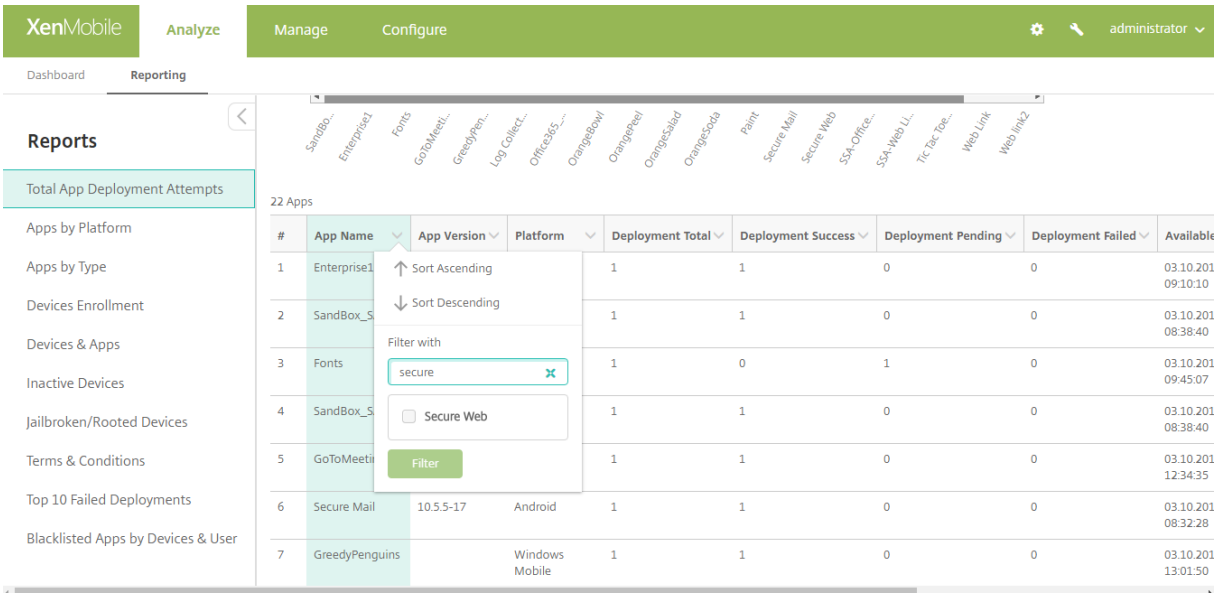


レポートの詳細を確認するには

1. グラフの各領域をクリックしてドリルダウンすると、詳細が表示されます。

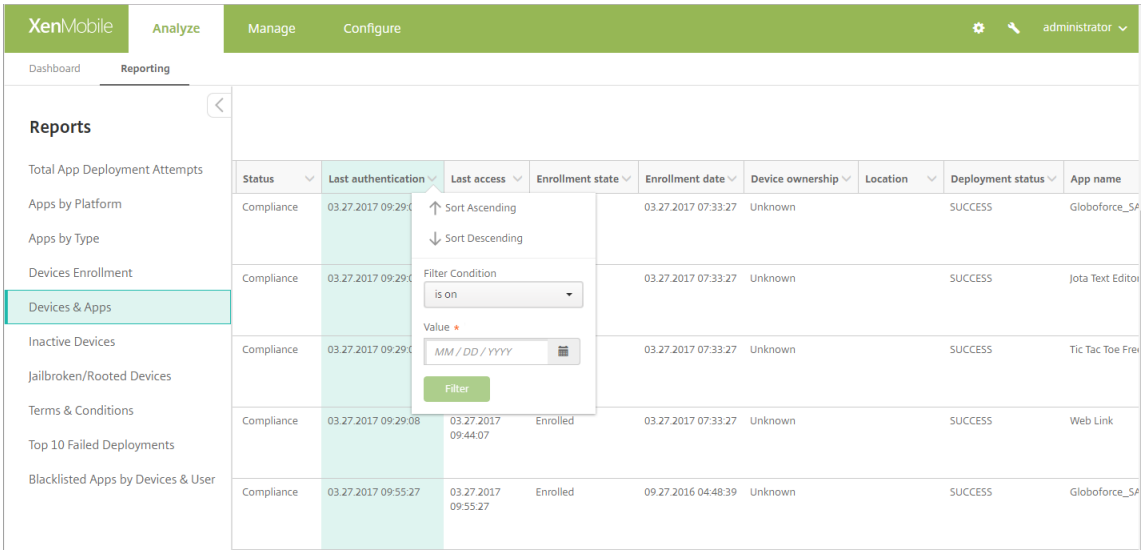


表の列を並び替え、フィルター、または検索するには、列の見出しをクリックします

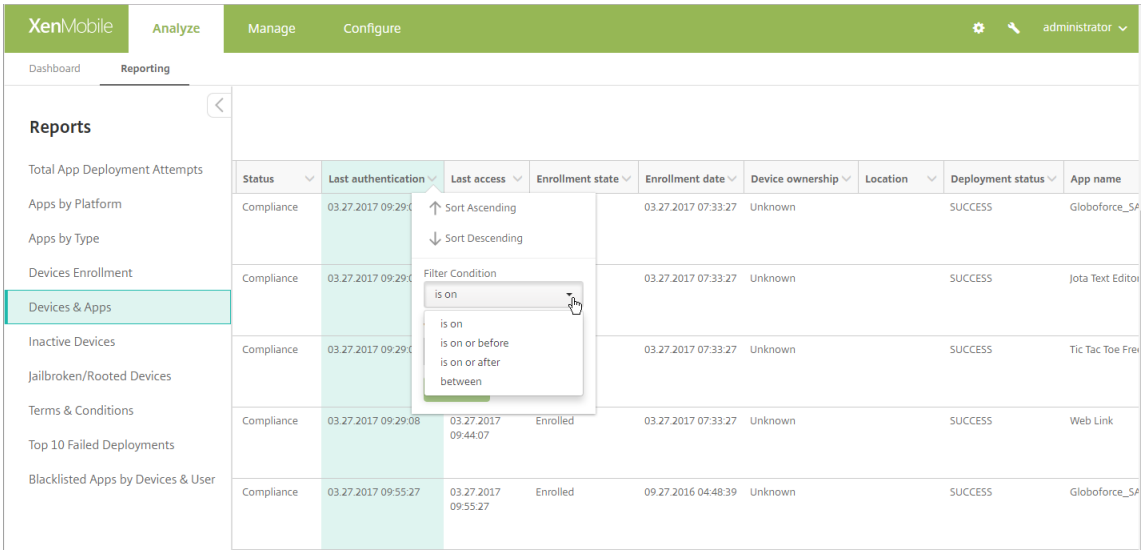


レポートを日付でフィルターするには

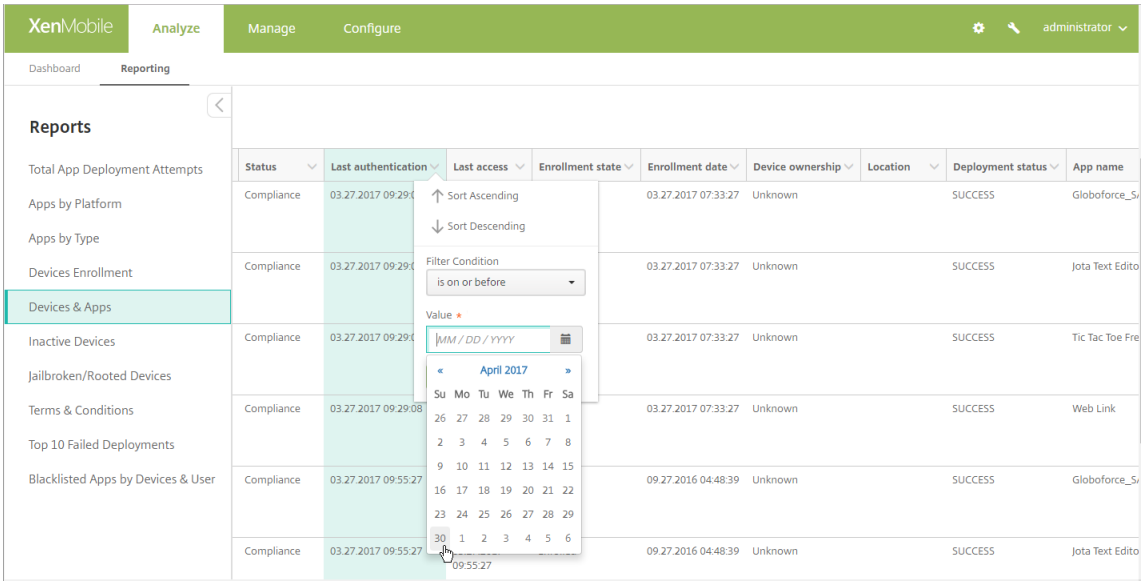
1. 列の見出しをクリックして、フィルター設定を表示します。



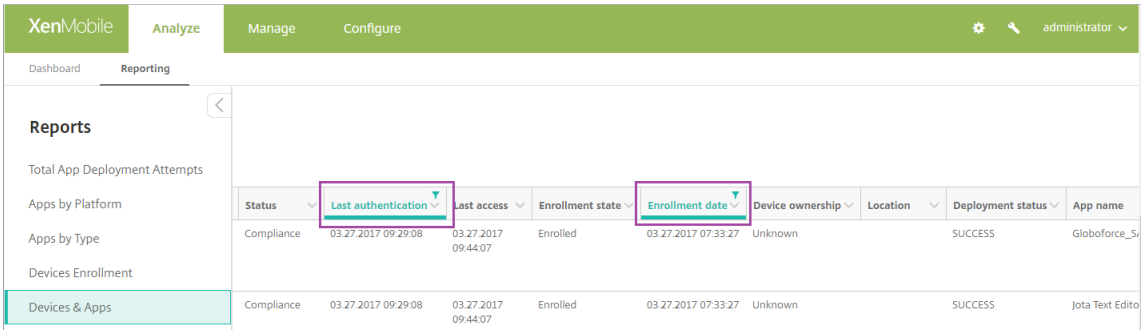
2. [フィルター条件] で、レポート対象期間を絞り込む方法を選択します。



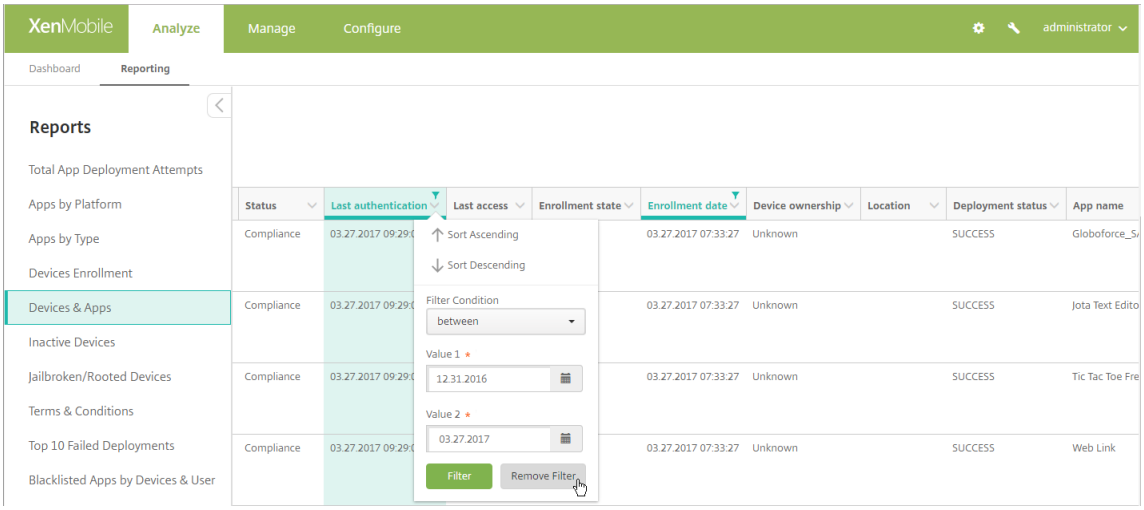
3. カレンダーを使用して日付を指定します。



4. 次の例のように、日付フィルターの付いた列が表示されます。

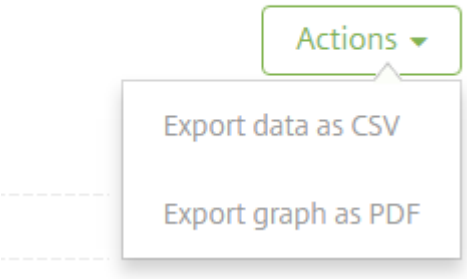


5. フィルターを削除するには、列の見出しをクリックして ［フィルターの削除］ をクリックします。



グラフまたは表をエクスポートするには

- グラフを PDF 形式でエクスポートするには、［操作］>［**PDF** でグラフをエクスポート］ の順にクリックします。
- 表のデータを CSV 形式でエクスポートするには、［操作］>［**CSV** でデータをエクスポート］ の順にクリックします。



> 重要:
>
> カスタムレポートの作成に SQL Server を使用することは可能ですが、お勧めしません。シトリックスではスキーマを公開していません。また通知なしにスキーマを変更することができます。このレポート作成方法を実行する場合は、SQL クエリが読み取り専用アカウントで実行されるようにしてください。複数の JOIN を使用するクエリは実行に時間がかかるため、クエリの実行時に XenMobile Server のパフォーマンスに影響を与える場合があることに注意してください。

SNMP の監視

September 24, 2019

XenMobile Server で SNMP 監視を有効にすると、監視システムが XenMobile ノードの情報をクエリして情報を取得できるようになります。クエリでは、プロセッサ負荷、負荷平均、メモリ使用状況、接続性などのパラメーターを使用します。認証および暗号化の仕様など、SNMP v3 について詳しくは、RFC 3414の公式の SNMP ドキュメントを参照してください。

> 注:
>
> SNMP v3 の監視は、XenMobile Server 10.8 以降でサポートされています。

SCOM（System Center Operations Manager）などの SNMP 監視をサポートするさまざまな監視アプリケーションを使用できます。SCOM の設定について詳しくは、このCitrix Support Knowledge Center の記事を参照してください。

前提条件

次の TCP ポートを構成します。

- ポート **161**（**UDP**）: UDP プロトコルを使用する SNMP トラフィックに使用されます。接続元は SNMP マネージャーで、接続先は XenMobile です。
- ポート **162**（**UDP**）: XenMobile から SNMP マネージャーに SNMP トラップ通知を送信するために使用されます。接続元は XenMobile で、接続先は SNMP マネージャーです。

XenMobile のポート構成について詳しくは、「ポート要件」を参照してください。

SNMP を含むオンプレミスの XenMobile 環境のアーキテクチャ図については、「オンプレミス環境のリファレンスアーキテクチャ」を参照してください。

SNMP を設定する一般的な手順は次のとおりです。

1. ユーザーの追加: ユーザーは、トラップの受信と XenMobile Server の監視権限を継承します。
2. **SNMP** マネージャーを追加してトラップを受信: トラップとは、XenMobile ノードがユーザー定義の最大しきい値を超えたときに XenMobile によって生成される通知です。
3. **XenMobile** と対話するように **SNMP** マネージャを設定: XenMobile Server は特定の管理情報ベース（MIB）を使用して処理を実行します。MIB は、XenMobile コンソールの［設定］**>**［**SNMP** の構成］ページからダウンロードします。次に MIB インポーターを使用して、MIB を SNMP マネージャーにインポートします。

   > 注:
   >
   > すべての SNMP マネージャーには、固有の MIB インポーターがあります。

4. トラップの有効化: XenMobile コンソールでトラップを有効にし、環境に応じて間隔としきい値を定義します。
5. サードパーティの **SNMP** マネージャ内のトラップを表示する: トラップを表示するには、SNMP マネージャを確認します。一部のマネージャーでは、マネージャーの外部で通知を有効にする設定が可能です。電子メールなどに通知が表示されるように構成できます。

XenMobile から次のトラップを生成できます。

トラップ名: プロセッサ負荷

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.2.1.25.3.3.1.2
- 説明: ユーザー定義の間隔でシステムの CPU 負荷を監視します。負荷がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: 1 分間の負荷平均

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.2021.10.1.5.1
- 説明: ユーザー定義の間隔で 1 分間の平均システム負荷を監視します。負荷平均がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: 5 分間の負荷平均

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.2021.10.1.5.2
- 説明: ユーザー定義の間隔で 5 分間の平均システム負荷を監視します。負荷平均がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: 15 分間の負荷平均

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.2021.10.1.5.3
- 説明: ユーザー定義の間隔で 15 分間の平均システム負荷を監視します。負荷平均がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: 使用可能なメモリの合計

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.2021.4.11
- 説明: ユーザー定義の間隔で使用可能なメモリを監視します。平均メモリがカスタムしきい値を下回る場合、XenMobile は SNMP トラップを生成します。注: 使用可能なメモリの合計には、RAM メモリとスワップメモリ（仮想メモリ）の両方が含まれます。スワップメモリの合計を取得するには、SNMP OID .1.3.6.1.4.1.2021.4.3 を使用してクエリできます。使用可能なスワップメモリを取得するには、SNMP OID .1.3.6.1.4.1.2021.4.4 を使用してクエリできます。

トラップ名: 使用ディスクストレージ合計

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.2021.9.1.9.1
- 説明: ユーザー定義の間隔でシステムディスク記憶域を監視します。ディスク記憶域がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: Java ヒープメモリ使用状況

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.2.4.0
- 説明: ユーザー定義の間隔で XenMobile の Java 仮想マシン（JVM）のヒープメモリの使用状況を監視します。使用量がカスタムしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: Java メタスペース使用状況

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.2.5.0
- 説明: ユーザー定義の間隔で XenMobile の Java メタスペースの使用状況を監視します。使用量がしきい値を超える場合、XenMobile は SNMP トラップを生成します。

トラップ名: LDAP の接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.1.0
- 説明: ユーザー定義の間隔で LDAP サーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: DNS の接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.2.0
- 説明: ユーザー定義の間隔で DNS サーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Google ストアサーバーの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.3.0
- 説明： ユーザー定義の間隔で Google ストアサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Windows Phone ストアの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.4.0
- 説明： ユーザー定義の間隔で Windows Phone ストアサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Windows タブレットストアの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.5.0
- 説明： ユーザー定義の間隔で Windows タブレットストアサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

説明： Windows セキュリティトークンサーバーの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.6.0
- 説明： ユーザー定義の間隔で Windows セキュリティトークンストアサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Windows 通知サーバーの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.7.0
- 説明： ユーザー定義の間隔で Windows 通知サーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Apple プッシュ通知サーバー（APNs）の接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.8.0
- 説明： ユーザー定義の間隔で APNs と XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Apple フィードバックサーバーの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.9.0
- 説明： ユーザー定義の間隔で Apple フィードバックサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： Apple Store サーバーの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.10.0
- 説明： ユーザー定義の間隔で Apple Store サーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名： XenMobile データベースの接続性

- 監視オブジェクト **ID**（**OID**）： .1.3.6.1.4.1.3845.5.1.1.18.11.0

- 説明: ユーザー定義の間隔で XenMobile データベースと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: Firebase Cloud Messaging サーバーの接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.12.0
- 説明: ユーザー定義の間隔で Firebase Cloud Messaging サーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: Citrix ライセンスサーバーの接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.13.0
- 説明: ユーザー定義の間隔で Citrix ライセンスサーバーと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: NetScaler Gateway の接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.15.0
- 説明: ユーザー定義の間隔で NetScaler Gateway と XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: XenMobile ノード間の接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.16.0
- 説明: ユーザー定義の間隔で XenMobile クラスターノード間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

トラップ名: XenMobile Tomcat ノードサービスの接続性

- 監視オブジェクト **ID**（**OID**）: .1.3.6.1.4.1.3845.5.1.1.18.17.0
- 説明: ユーザー定義の間隔で XenMobile Tomcat ノードサービスと XenMobile ノードとの間の接続を監視します。接続に失敗すると、XenMobile は SNMP トラップを生成します。

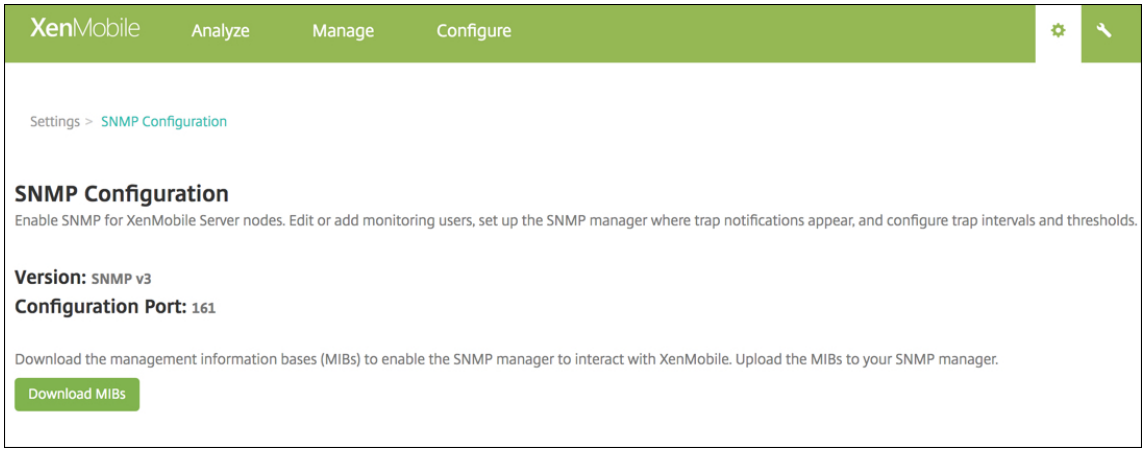
サーバーのパフォーマンスを最大にするために SNMP のしきい値を設定するときは、次の点に注意してください。

- 呼び出しの頻度
- 収集されるトラップデータとしきい値のチェック
- ノード間通信のメカニズム
- 接続チェックの頻度
- チェック中に失敗した場合のタイムアウト

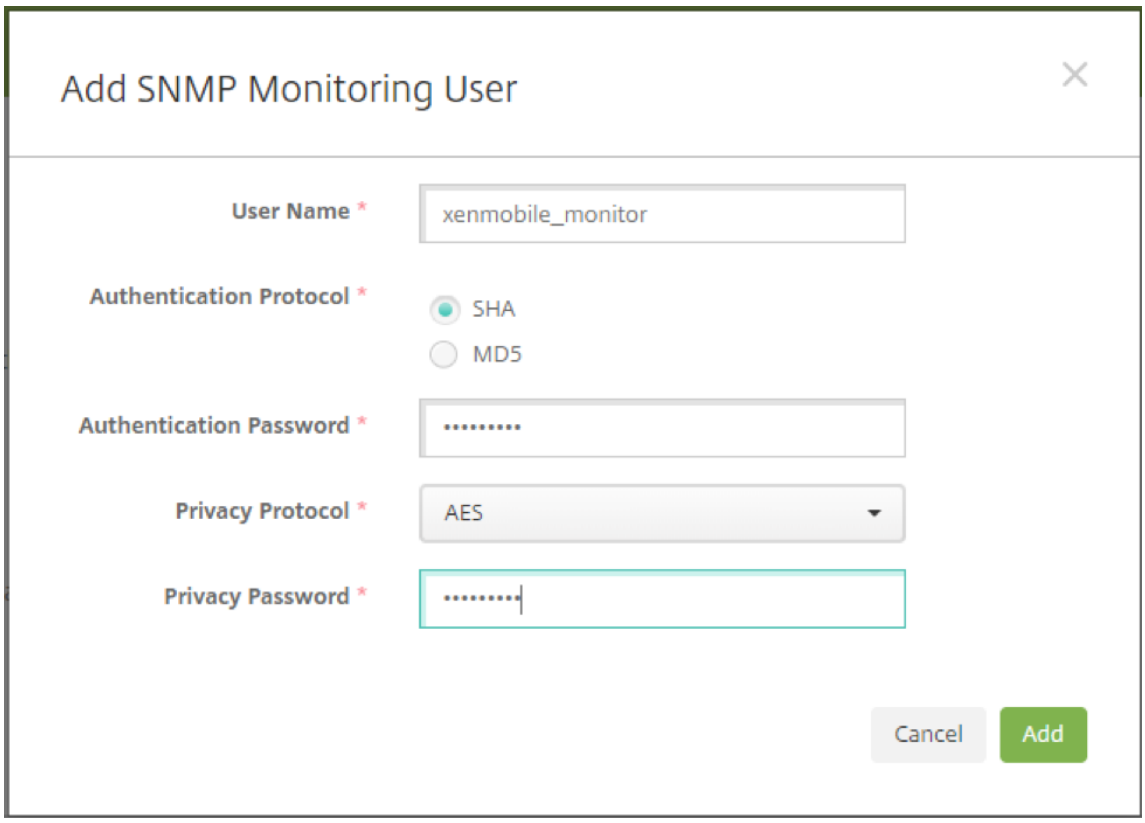
SNMP ユーザーを追加するには

SNMP ユーザーは SNMP マネージャーとやり取りし、トラップを受信します。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［監視］ の下の ［**SNMP** の構成］ をクリックします。［**SNMP** の構成］ ページが開きます。



3. [**SNMP** 監視ユーザー] の下の [追加] をクリックします。
4. [**SNMP** 監視ユーザーの追加] ダイアログボックスで、次の設定を構成します。



ユーザー名: SNMP マネージャーへのログオンに使用するユーザー名。英数字、アンダースコア、ハイフンは使用できますが、ユーザー名にスペースやその他の特殊文字は使用できません。

> 注:
>
> ユーザー名「xmsmonitor」を追加することはできません。これは、XenMobile が内部で使用するために予約されているからです。

認証プロトコル:

- **SHA**（推奨）
- **MD5**

認証パスワード： 8 ～ 18 文字のパスワードを入力します。英数字と特殊文字を含めることができます。

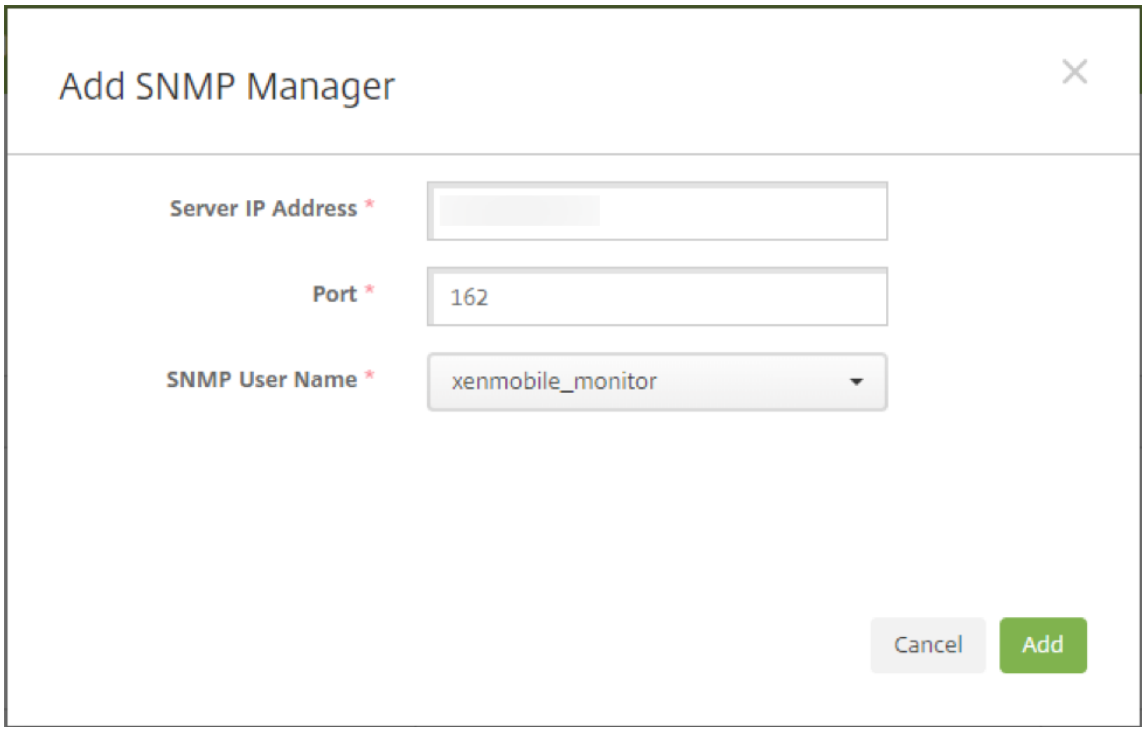
プライバシープロトコル：

- **DES**
- **AES 128**（推奨）

プライバシーパスワード： 8 ～ 18 文字のパスワードを入力します。英数字と特殊文字を含めることができます。

SNMP マネージャーを追加するには

1. ［**SNMP** マネージャー］ の下の ［追加］ をクリックします。
2. ［**SNMP** マネージャーの追加］ ダイアログボックスで、次の設定を構成します。



サーバー **IP** アドレス： SNMP マネージャーの IP アドレスを入力します。

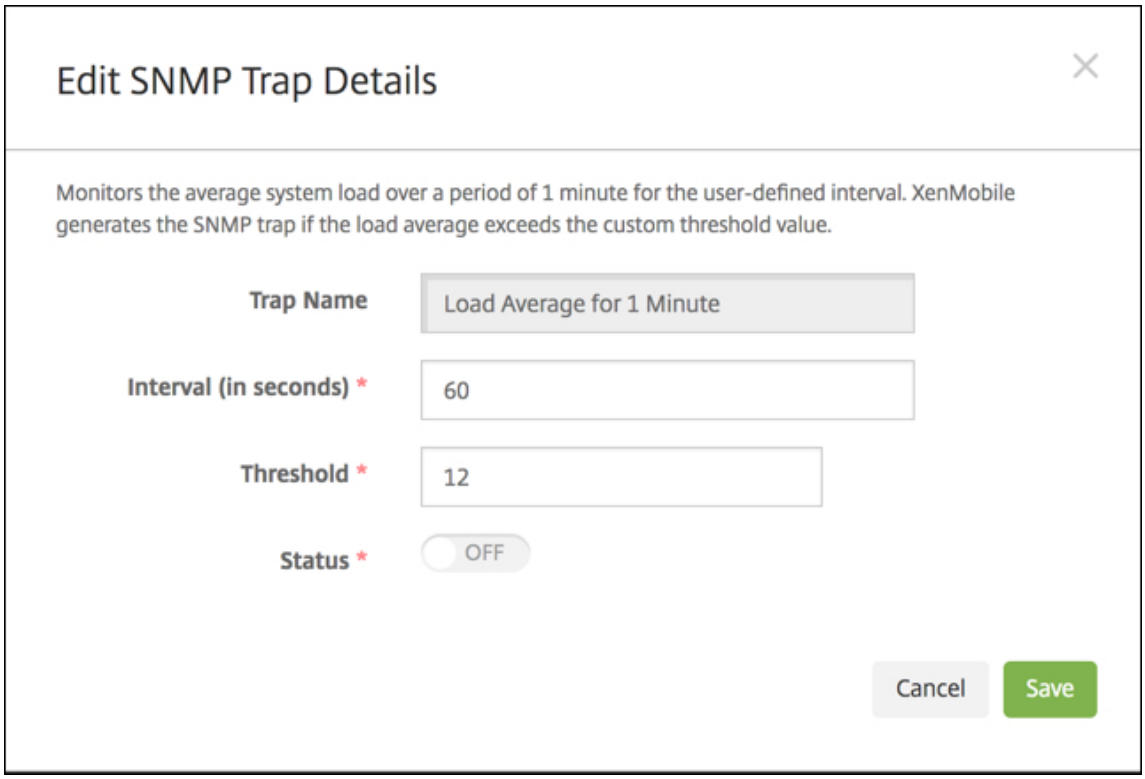
ポート： 必要に応じてポート番号を変更します。デフォルトは 162 です。

SNMP ユーザー名： マネージャーにアクセスできるユーザーの名前を選択します。

SNMP トラップを有効にして構成するには

環境に適したトラップ設定を決定するには、「スケーラビリティとパフォーマンス」を参照してください。たとえば、XenMobile の負荷平均を 1 分間監視するには、［1 分間の負荷平均］を有効にして、しきい値を指定します。XenMobile Server の 1 分間の負荷平均が、指定したしきい値を超えた場合、構成済みの SNMP マネージャーでトラップを受信します。

1. 個々のトラップを有効にするには、次のいずれかを実行します。
   - パラメーターの横にあるチェックボックスをオンにし、［有効化］ をクリックします。
   - 一覧のすべてのトラップを有効にするには、上部のチェックボックスをオンにして、［有効化］ をクリックします。
2. トラップを編集するには、パラメーターを選択して、［編集］ をクリックします。
3. ［**SNMP** トラップの詳細の編集］ ダイアログボックスでは、個々のトラップのしきい値を編集できます。



トラップ名： トラップの名前。このフィールドは編集できません。

間隔（秒）： 許容範囲は 60 ～ 86400（24 時間）です。

しきい値： 次のトラップのしきい値のみを変更できます。

- プロセッサ負荷
- 1 分間の負荷平均
- 5 分間の負荷平均
- 15 分間の負荷平均

- 使用可能なメモリの合計
- 使用ディスクストレージ合計
- Java ヒープメモリ使用状況
- Java メタスペース使用状況

状態:［オン］ を選択すると、トラップの SNMP 監視が有効になります。［オフ］ を選択すると、監視が無効になります。

SNMP を使用して XenMobile を監視する方法の詳細については、このブログ記事を参照してください。

サポートバンドル

August 22, 2019

問題を Citrix に報告するか、問題のトラブルシューティングを行うには、サポートバンドルを作成します。その後で、Citrix Insight Services（CIS）にサポートバンドルをアップロードします。

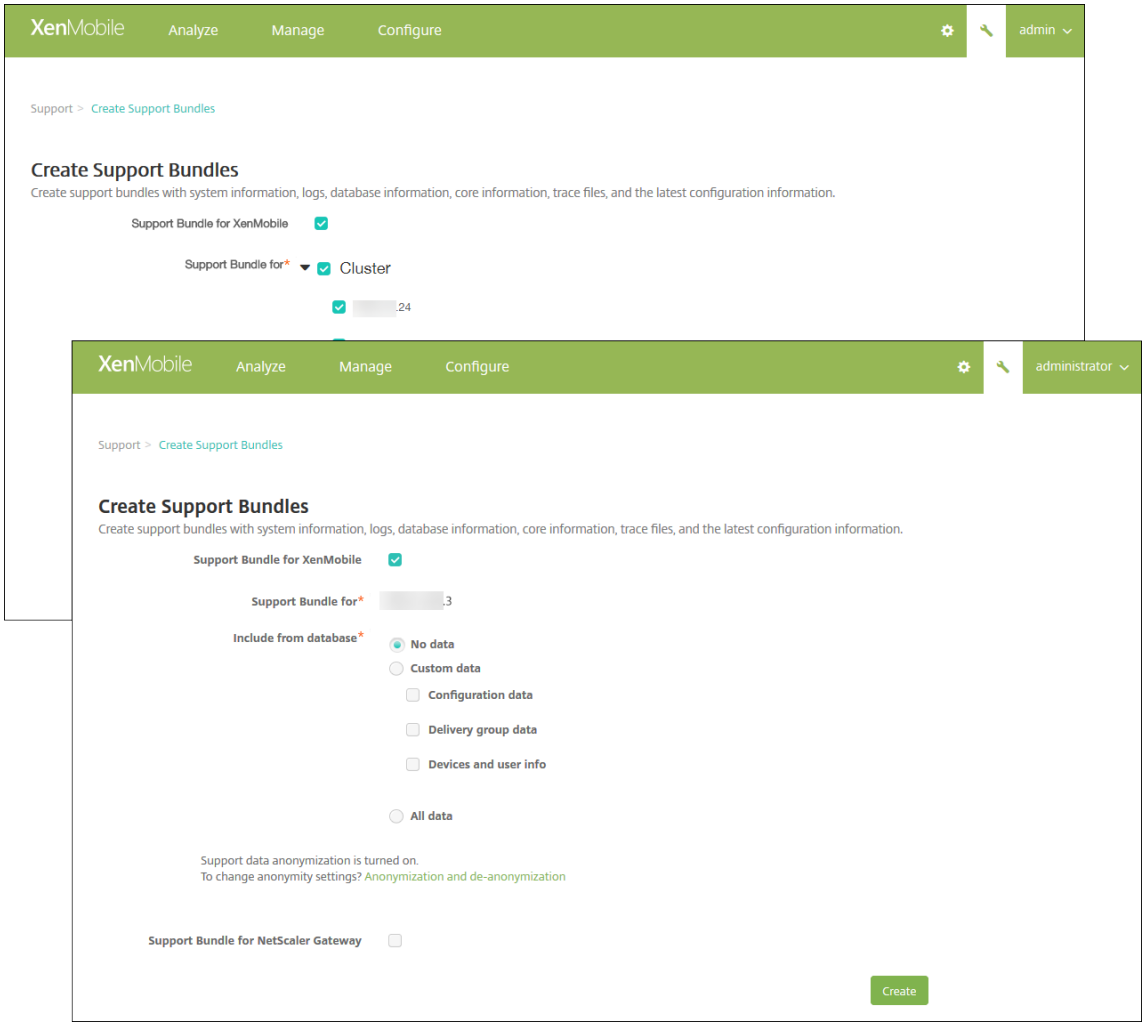
デフォルトでは、サポートバンドルには次のファイルのバックアップアーカイブが最大 100 個含まれます。デフォルトのファイルサイズは 10MB です。

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

サポートバンドルにこれらのカテゴリごとに 100 個のログアーカイブファイルが含まれている場合、ログファイルはロールオーバーされます。ログファイルの最大数を少なく設定すると、XenMobile はそのノードの不要なログファイルを直ちに削除します。ログファイルの数を設定するには、［トラブルシューティングとサポート］ > ［ログ設定］ の順に進みます。

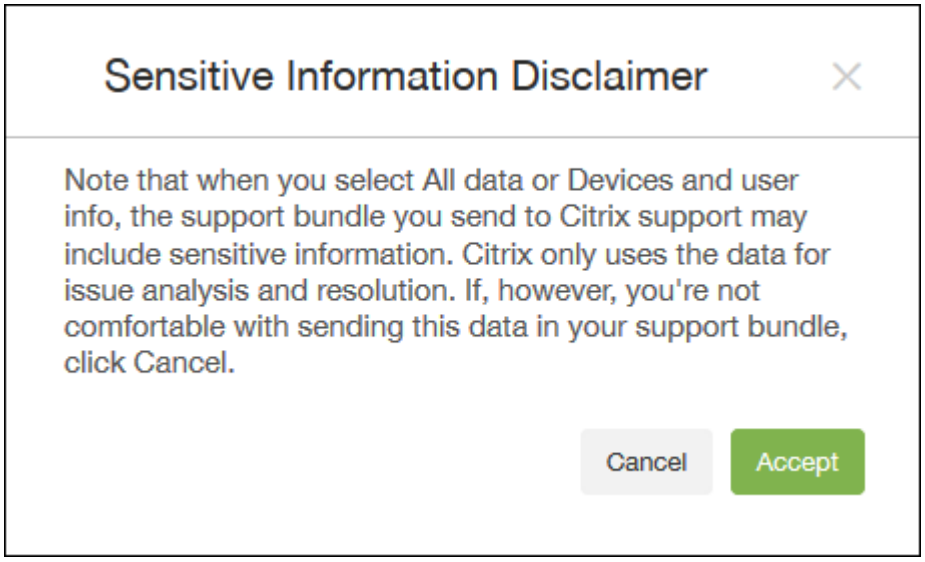
サポートバンドルを作成するには:

1. XenMobile コンソールで、右上のレンチアイコンをクリックします。［サポート］ ページが開きます。
2. ［サポート］ ページで、［サポートバンドルの作成］ をクリックします。［サポートバンドルの作成］ ページが開きます。XenMobile 環境内にクラスターノードがある場合は、すべてのノードが表示されます。



3. [**XenMobile** のサポートバンドル] チェックボックスがオンになっていることを確認します。
4. XenMobile 環境内にクラスターノードがある場合は、[サポートバンドルの対象] ですべてのノードを選択するか、データの取得先にするノードの組み合わせを選択できます。
5. [データベースから包含] で、次のいずれかを実行します。
   - [データなし] をクリックします。
   - [カスタムデータ] をクリックします。デフォルトでは、これらのオプションがすべて選択されています。
     - 構成データ： 証明書構成とデバイスマネージャーポリシーを含めます。
     - デリバリーグループデータ： アプリの種類やアプリデリバリーポリシー詳細など、アプリのデリバリーグループの情報を含めます。
     - デバイスおよびユーザー情報： デバイスポリシー、アプリ、アクション、デリバリーグループを含めます。
   - [すべてのデータ] をクリックします。

> 注:
>
> ［デバイスおよびユーザー情報］ または ［すべてのデータ］を選択し、かつこれが初めて作成するサポートバンドルである場合は、［機密情報に関する免責事項］ ダイアログボックスが開きます。免責事項を読み、［承諾］ または ［キャンセル］ をクリックします。［キャンセル］ をクリックした場合は、サポートバンドルを Citrix にアップロードできません。［承諾］ をクリックした場合は、サポートバンドルを Citrix にアップロードでき、次回デバイスやユーザーデータを含むサポートバンドルを作成するときに免責事項が表示されなくなります。

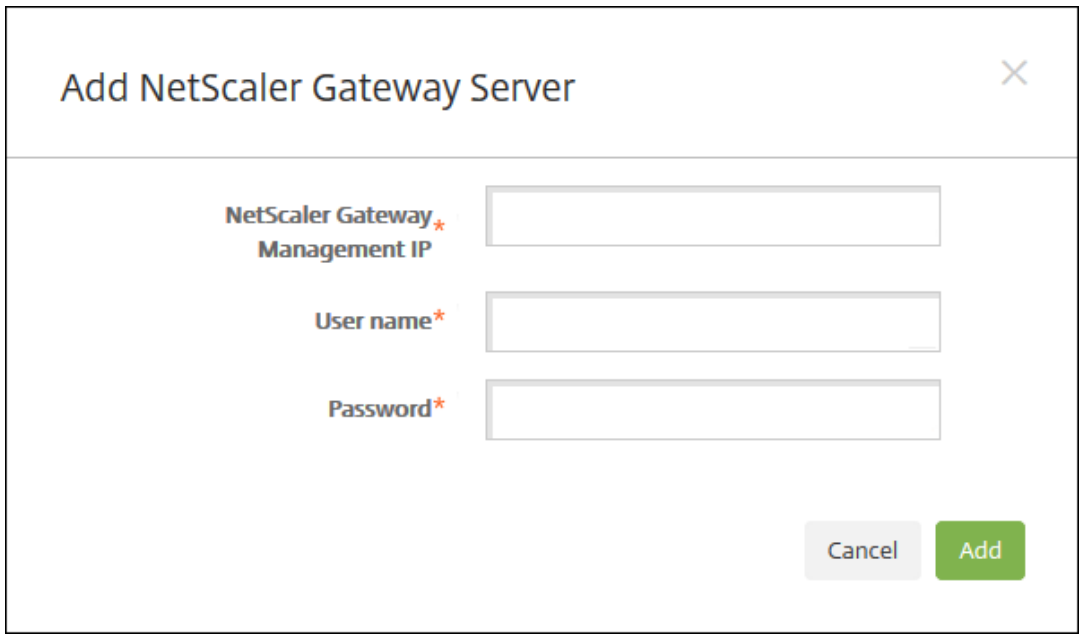


6. ［サポートデータ匿名化が有効です］ オプションは、デフォルトの設定でデータの匿名化を指定していることを示します。データの匿名化とは、機密性が高いユーザー、サーバー、およびネットワークデータがサポートバンドルで匿名化されることを意味します。

   この設定を変更するには、［匿名化および匿名化解除］ リンクをクリックします。データの匿名化について詳しくは、「サポートバンドルのデータの匿名化」を参照してください。

7. NetScaler Gateway からのサポートバンドルを含めるには: ［**NetScaler Gateway** のサポートバンドル］チェックボックスをオンにして以下を行います。

   a) ［追加］ をクリックします。［**NetScaler Gateway** サーバーの追加］ ダイアログボックスが開きます。



b) [**NetScaler Gateway** 管理 **IP**] ボックスに、サポートバンドルの取得先にする NetScaler Gateway の NetScaler 管理 IP アドレスを入力します。

> 注:
>
> 既に追加されている NetScaler Gateway サーバーからバンドルを作成する場合、IP アドレスは入力されています。

c) [ユーザー名] ボックスと [パスワード] ボックスに、NetScaler Gateway を実行しているサーバーへのアクセスに必要なユーザーの資格情報を入力します。

> 注:
>
> 既に追加されている NetScaler Gateway サーバーからバンドルを作成する場合、ユーザー名は入力されています。

8. [追加] をクリックします。新しい NetScaler Gateway サポートバンドルが表に追加されます。
9. 手順 7 を繰り返し、ほかの NetScaler Gateway サポートバンドルを追加します。
10. [作成] をクリックします。サポートバンドルが作成され、[**CIS** へアップロード] と [クライアントへダウンロード] の 2 つの新しいボタンが表示されます。

Citrix Insight Services へのサポートバンドルのアップロード

サポートバンドルを作成した後、Citrix Insight Services（CIS）にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。

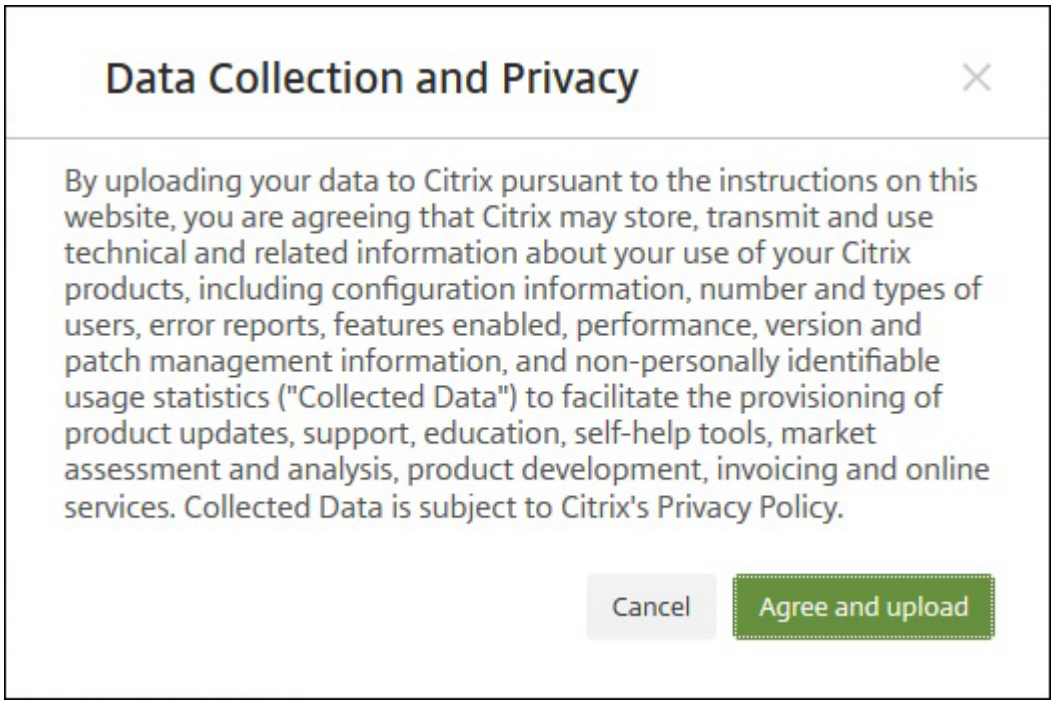
XenMobile から CIS へのアップロードには、SSL 送信接続を使用します。CIS サーバーの IP アドレス（52.88.24.76、52.88.118.220、52.11.72.119）に対してポート 443 を開きます。HTTPS トラフィックのプロキシがある場合は、プ

ロキシが CIS サーバーの IP アドレスに到達できることを確認します。

以下の手順は、CIS にバンドルをアップロードする方法を示しています。CIS にアップロードするには、My Citrix の ID およびパスワードが必要です。

1. ［サポートバンドルの作成］ページで、［**CIS** へアップロード］をクリックします。［**Citrix Insight Services (CIS)** へのアップロード］ ダイアログボックスが開きます。
2. ［ユーザー名］ ボックスに My Citrix ID を入力します。
3. ［パスワード］ ボックスに My Citrix パスワードを入力します。
4. このバンドルを既存のサービスリクエスト番号に関連付ける場合は、［**SR#** に割り当て］ チェックボックスをオンにし、新たに表示される 2 つのフィールドで以下を実行します。
   - ［**SR#**］ ボックスに、このバンドルを関連付けるサービスリクエスト番号（8 桁）を入力します。
   - ［**SR** 説明］ ボックスに、SR の説明を入力します。
5. ［アップロード］をクリックします。

   CIS にサポートバンドルをアップロードするのはこれが初めてであり、ほかの製品を介して CIS のアカウントを作成したことがなく、かつデータの収集とプライバシーについての契約に同意していない場合は、以下のダイアログボックスが表示されます。アップロードを開始する前にこの契約に同意する必要があります。CIS のアカウントを作成済みで、以前に契約に同意している場合は、サポートバンドルが直ちにアップロードされます。



6. 契約を読み、［同意してアップロード］ をクリックします。サポートバンドルがアップロードされます。

コンピューターへのサポートバンドルのダウンロード

サポートバンドルを作成した後、CIS にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。問題のトラブルシューティングを自分で行う場合は、サポートバンドルをコンピューターにダウンロードします。

［サポートバンドルの作成］ページで、［クライアントへのダウンロード］をクリックします。バンドルがコンピューターにダウンロードされます。

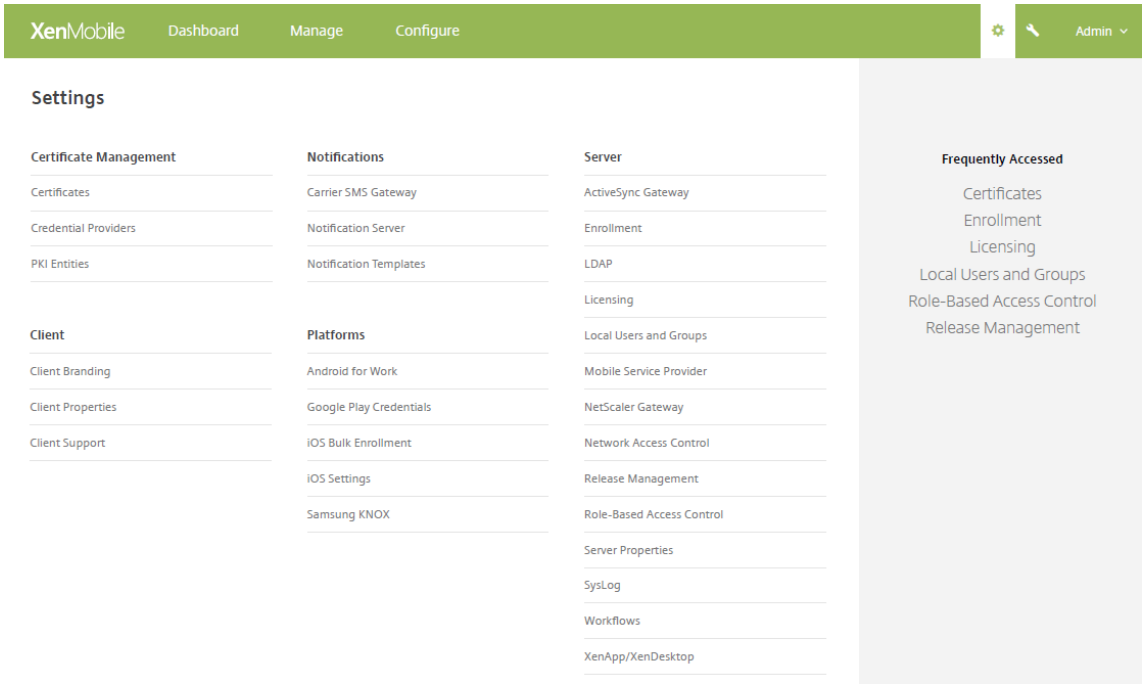
サポートオプションとリモートサポート

January 10, 2020

サポートスタッフへの問い合わせ用のメールアドレスをユーザーに提供できます。ユーザーがデバイスからサポートを要求すると、このメールアドレスが表示されます。

ユーザーがデバイスからヘルプデスクにログを送信する方法も構成できます。ログは直接またはメールで送信するように構成できます。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。



2. ［クライアント］ の下の ［クライアントサポート］ をクリックします。［クライアントサポート］ ページが開きます。
3. 次の設定を構成します:

- サポート用メール（**IT** ヘルプデスク）: IT ヘルプデスク担当者のメールアドレスを入力します。
- **IT** ヘルプデスクにデバイスログを送信: デバイスログの送信方法として ［直接］ または ［メールにより］ を選択します。デフォルトは ［メールにより］ です。
  - ［直接］ を有効にすると、［ShareFile にログを保存］の設定が表示されます。［ShareFile にログを保存］を有効にすると、ログは ShareFile に直接送信されます。それ以外の場合は、ログは XenMobile に送信され、ヘルプデスクにメールで送信されます。さらに、［直接送信に失敗したら、メールを使用］ オプションが表示されます。このオプションはデフォルトで有効化されています。サーバーの問題に関するログの送信にクライアントのメールを使用しない場合は、このオプションを無効にすることができます。ただし、このオプションを無効にすると、サーバーに問題があってもログが送信されません。
  - ［メールにより］ を有効にすると、ログの送信では常にクライアントのメールが使用されます。

4. ［保存］ をクリックします。

リモートサポート

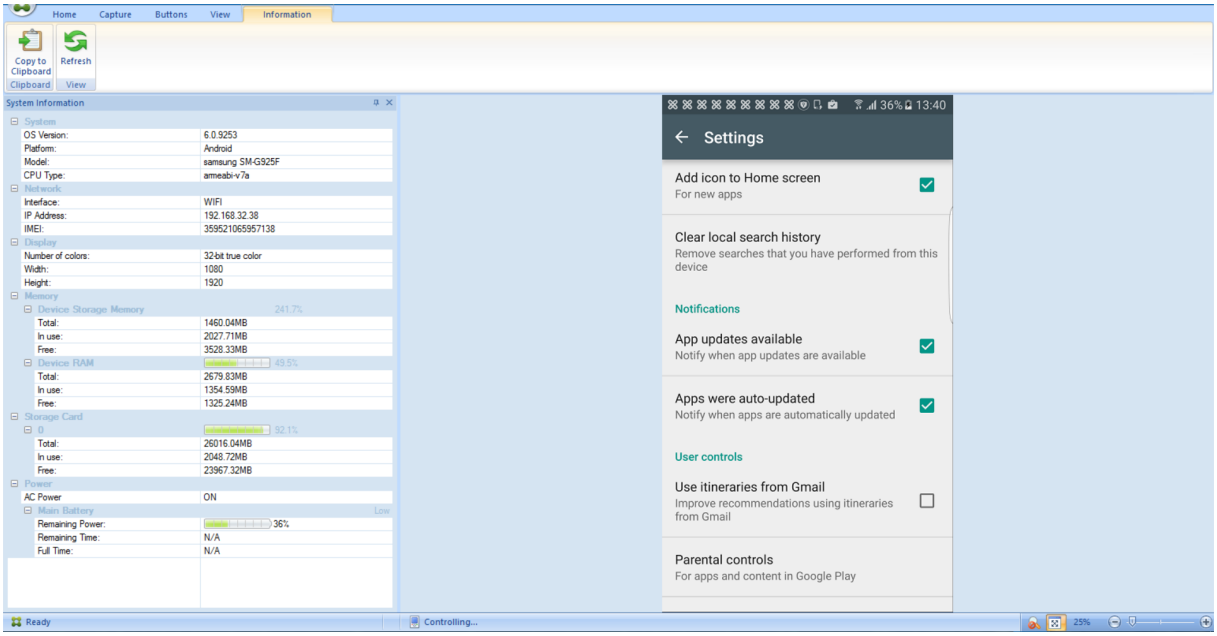
> 注:
>
> 2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。

XenMobile Server のオンプレミス展開の場合: リモートサポートを使用すると、ヘルプデスクの担当者は管理対象の Windows CE および Android モバイルデバイスをリモートで制御できます。画面のキャストは Samsung KNOX でのみサポートされています。

XenMobile サービスのお客様はリモートサポートを利用できません。またリモートサポートはクラスター化されたオンプレミスの XenMobile Server 展開ではサポートされていません。

リモート制御セッション時の動作は次のようになります。

- ユーザーのモバイルデバイスには、リモート制御セッションがアクティブであることを示すアイコンが表示されます。
- Remote Support アプリケーションウィンドウが開いて、［Remote Contorol］ウィンドウに制御対象デバイスが表示されます。



Remote Support で、次のことを実行できます。

- ユーザーデバイスにリモートでサインオンし、デバイスの画面を制御する。ユーザーはヘルプデスク担当者による画面の移動を確認できるため、ユーザーのトレーニングとしても役に立つことがあります。
- リアルタイムでリモートデバイス内を移動して修復する。構成の変更、オペレーティングシステムの問題のトラブルシューティング、問題があるアプリケーションやプロセスの無効化または終了を行うことができます。
- ネットワークアクセスの無効化、不正プロセスの停止、アプリまたはマルウェアの削除をリモートに実行することで、ほかのモバイルデバイスに脅威が広がる前に、その脅威を隔離して封じこめる。
- ユーザーがデバイスを見つけられるように、デバイスの着信音や電話の発信をリモートで有効にする。デバイスを見つけることができなかった場合は、重要なデータが侵害されないように、デバイスにワイプを実行できます。

Remote Support では、サポート担当者に次の機能も提供されます。

- 1 つまたは複数の XenMobile インスタンスについて、接続しているすべてのデバイスの一覧を表示する。
- デバイスのモデル、オペレーティングシステムのレベル、IMEI (International Mobile Station Equipment Identity: 国際移動体装置識別番号)、シリアル番号、メモリおよびバッテリーの状態、接続状態などのシステム情報を表示する。
- XenMobile のユーザーおよびグループを表示する。
- アクティブなプロセスの表示や停止、およびモバイルデバイスの再起動を行うためのデバイスタスクマネージャーを実行する。
- モバイルデバイスと中央ファイルサーバー間の双方向のリモートファイル転送を実行する。
- 1 つまたは複数のモバイルデバイスに対するソフトウェアプログラムの一括ダウンロードおよびインストール。
- デバイスのレジストリキーのリモートからの構成。
- モバイルネットワークによる狭帯域幅接続でのレスポンスを最適化するリアルタイムのデバイス画面リモート制御。

- さまざまなモバイルデバイスブランドおよびモデルのデバイススキンを表示する。スキンエディターを表示して、新規デバイスモデルの追加および物理キーのマッピングを行うことができます。
- デバイス画面の取り込み、記録、再生により、デバイスでの一連のビデオ AVI ファイル作成操作を記録できるようにする。
- 共有ホワイトボード、VoIP ベースの音声通信、およびチャットによるモバイルユーザーとサポート担当者間の Live Meeting。

Remote Support のシステム要件

Remote Support ソフトウェアは、以下の要件を満たす Windows ベースのコンピューターにインストールします。ポートの要件については、「ポート要件」を参照してください。

サポートされるプラットフォームは、以下のとおりです。

- Intel Xeon/Pentium 4-1GHz 以上のワークステーションクラス
- 512MB 以上の RAM
- 100MB 以上の空きディスクスペース

以下のオペレーティングシステムがサポートされています:

- Microsoft Windows 2003 Server Standard Edition または Enterprise Edition SP1 以降
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 以降
- Microsoft Windows Vista SP1 以降
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Remote Support ソフトウェアをインストールするには

1. Remote Support インストーラをダウンロードするには、XenMobile 10 のダウンロードページに移動し、アカウントにログオンします。
2. [**Tools**] を展開し、XenMobile Remote Support v9 をダウンロードします。
   Remote Support のファイル名は XenMobileRemoteSupport-9.0.0.35265.exe です。
3. Remote Support インストーラーをダブルクリックし、表示されるインストールウィザードの指示に従います。

コマンドラインから **Remote Support** をインストールするには

次のコマンドを実行します。

```
\*RemoteSupport\*.exe /S
```


RemoteSupport にはインストールプログラムの名称を指定します。次に例を示します:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

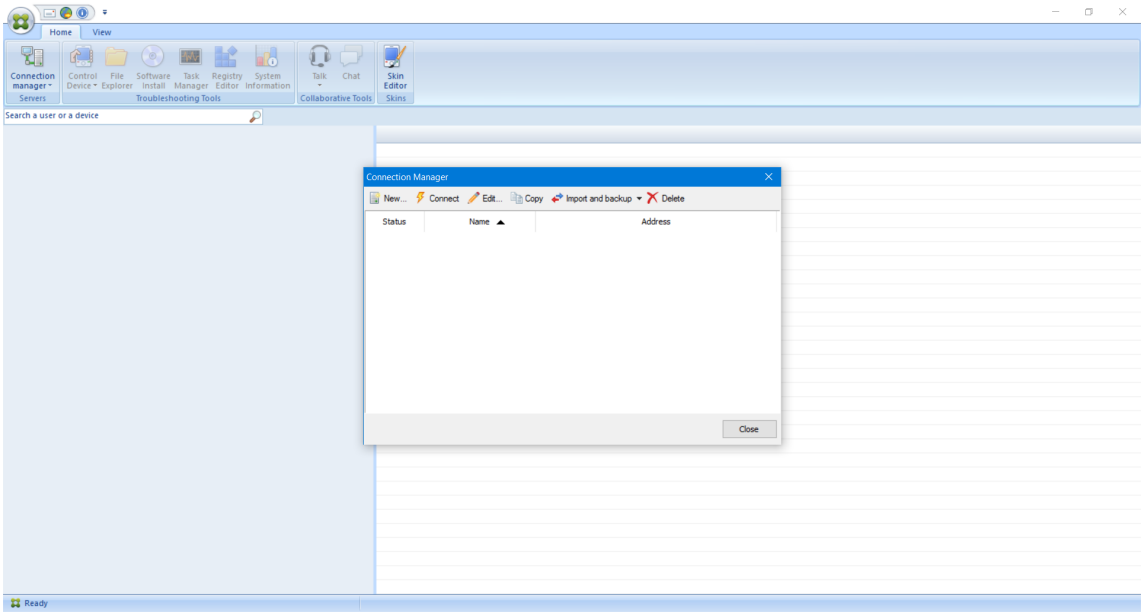
Remote Support ソフトウェアのインストール時には、次の変数を使用できます。

- /S: デフォルトのパラメーターを使用して Remote Support ソフトウェアをサイレントでインストールします。
- /D=dir:。カスタムのインストールディレクトリを指定します。

Remote Support を **XenMobile** に接続するには

管理対象デバイスへのリモートサポート接続を確立するには、Remote Support からの接続を、該当のデバイスを管理する 1 つまたは複数の XenMobile Server に追加する必要があります。この接続は、Android および Windows Mobile/CE デバイス向けのデバイスポリシーであるトンネル MDM ポリシーで定義したアプリトンネル上で実行されます。Remote Support を XenMobile に接続するには、アプリトンネルを定義します詳しくは、「アプリケーショントンネリングデバイスポリシー」を参照してください。

1. Remote Support ソフトウェアを起動し、XenMobile の資格情報を使用してサインオンします。
2. [**Connection Manager**] で、 [**New**] をクリックします。



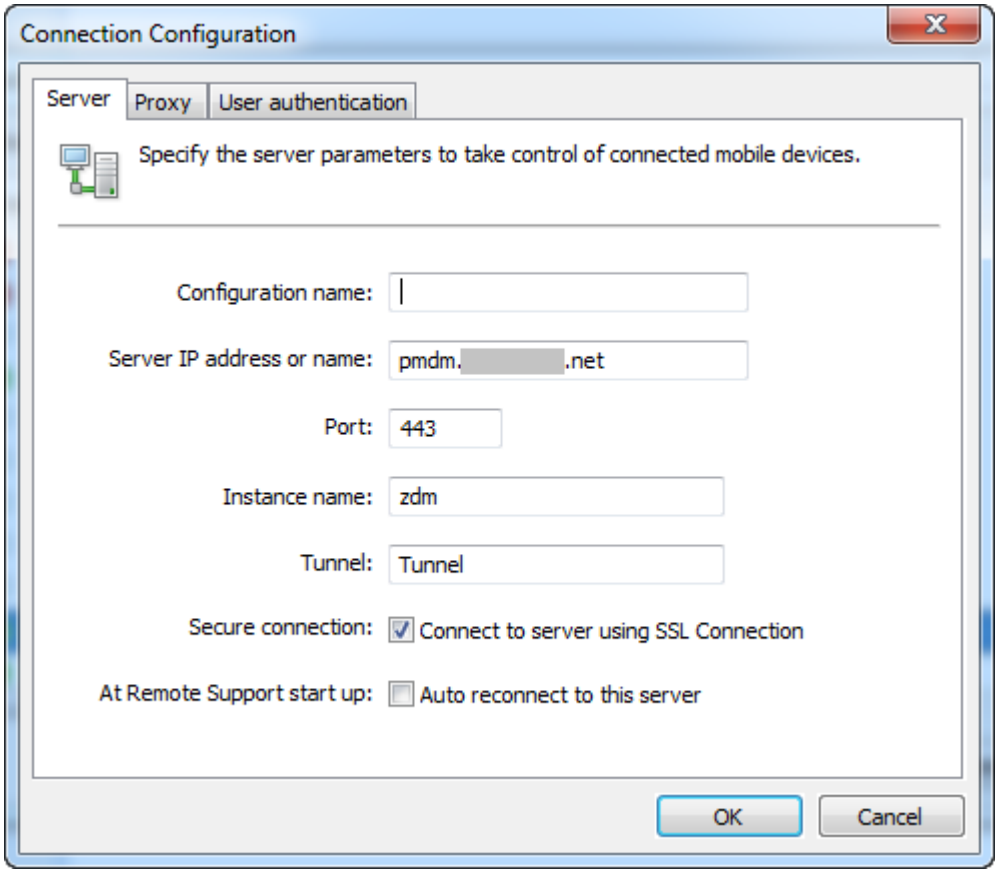
3. [**Connection Configuration**] ダイアログボックスの [**Server**] タブで、次の値を入力します。
   a) [**Configuration name**] に構成エントリの名前を入力します。
   b) [**Server IP address or name**] に XenMobile サーバーの IP アドレスまたは DNS 名を入力します。
   c) [**Port**] に、XenMobile Server 構成で定義されている TCP ポート番号を入力します。

d) XenMobile がマルチテナント環境に含まれている場合は、［**Instance name**］ にインスタンス名を入力します。

e) ［**Tunnel**］ にトンネルポリシーの名前を入力します。

f) ［**Connect to server using SSL Connection**］ チェックボックスをオンにします。

g) Remote Support アプリケーションが起動するたびに、構成した XenMobile Server に接続するには、［**Auto reconnect to this server**］ チェックボックスをオンにします。



4. ［**Proxy**］ タブで、［**Use a http proxy server**］ を選択して次の情報を入力します。

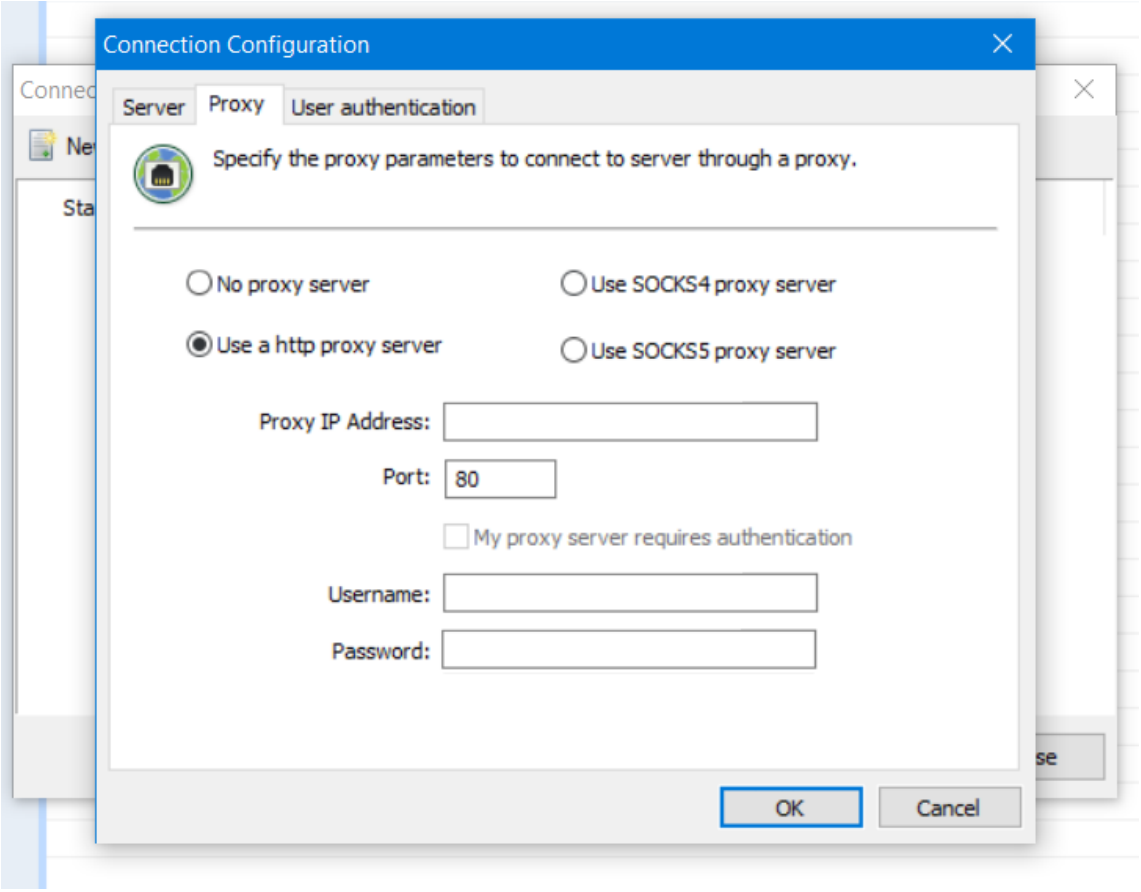
a) ［**Proxy IP Address**］ の横に、プロキシサーバーの IP アドレスを入力します。

b) ［**Port**］ に、プロキシで使用する TCP ポート番号を入力します。

c) プロキシサーバーでトラフィックの許可に認証が必要な場合は、［**My proxy server requires authentication**］ チェックボックスをオンにします。

d) ［**Username**］ に、プロキシサーバーで認証するユーザー名を入力します。

e) ［**Password**］ に、プロキシサーバーで認証するパスワードを入力します。



5. [**User Authentication**] タブで、 [**Remember my login and password**] チェックボックスをオンにして資格情報を入力します。
6. [**OK**] をクリックします。

XenMobile に接続するには、作成した接続をダブルクリックし、この接続用に構成したユーザー名とパスワードを入力します。

Samsung KNOX デバイスでリモートサポートを有効にするには

XenMobile で Remote Support ポリシーを作成して、Samsung KNOX デバイスへのリモートアクセスを行うことができます。次の 2 種類のサポートを構成できます。

- 基本: デバイスに関する診断情報を表示できます。たとえば、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率と CPU 使用率）、およびインストールされているソフトウェアフォルダーの内容などです。
- プレミアム: デバイスの画面をリモートで制御できます。たとえば、ウィンドウの色の制御、ヘルプデスクとユーザー間での VoIP セッションの確立、ヘルプデスクとユーザー間でのチャットセッションの確立などを行うことができます。

プレミアムサポートでは、XenMobile コンソールで Samsung MDM ライセンスキーのデバイスポリシーを構成する必要があります。このポリシーを構成する場合は、**Samsung KNOX** プラットフォームのみを選択してください。Samsung SAFE プラットフォームについては、XenMobile への登録時に ELM キーが自動で Samsung デバイスに展開されます。このため、このポリシーで Samsung SAFE プラットフォームは選択しないでください。詳しくは、「Samsung MDM ライセンスキー」を参照してください。

リモートサポートポリシーの設定の詳細については、「リモートサポートデバイスポリシー」を参照してください。

リモートサポートセッションを使用するには

Remote Support を起動すると、Remote Support アプリケーションウィンドウの左側に、XenMobile コンソールで定義した XenMobile ユーザーグループが表示されます。デフォルトでは、現在接続されているユーザーが含まれているグループのみが表示されます。ユーザーエントリの横に、各ユーザーのデバイスが表示されます。

1. すべてのユーザーを表示するには、左側の列の各グループを展開します。
   XenMobile Server に現在接続されているユーザーは、緑のアイコンで表示されます。
2. すべてのユーザー（現在接続されていないユーザーを含む）を表示するには、［**View**］ をクリックし、［**Non-connected devices**］ を選択します。
   接続されていないユーザーは、緑のアイコンなしで表示されます。

XenMobile Server に接続されているもののユーザーに割り当てられていないデバイスは、匿名モードで表示されます（一覧に「**Anonymous**」と表示されます）。これらのデバイスを、ログインユーザーのデバイスと同じように制御できます。

デバイスを制御するには、デバイスの行をクリックしてデバイスを選択してから、［**Control Device**］ をクリックします。デバイスが［Remote Control］ウィンドウに表示されます。制御対象デバイスは次の方式で操作できます。

- デバイス画面のメインウィンドウまたは別の浮動ウィンドウを制御する（色の制御を含む）。
- ヘルプデスクとユーザー間のボイスオーバー IP（VoIP）セッションを確立する。VoIP 設定を構成します。
- ユーザーとのチャットセッションを確立する。
- デバイスのタスクマネージャーにアクセスして、メモリの使用率、CPU の使用率、実行中のアプリケーションなどのアイテムを管理する。
- モバイルデバイスのローカルディレクトリを探索する。ファイルを転送する。
- Windows Mobile デバイス上のデバイスレジストリを編集する。
- デバイスシステム情報およびインストールされているすべてのソフトウェアを表示する。
- XenMobile Server とモバイルデバイスの接続状態を更新する。

Syslog

August 22, 2019

XenMobile Server（オンプレミスのみ）を構成して、ログファイルをシステムログ（syslog）サーバーに送信できます。サーバーのホスト名または IP アドレスが必要です。

Syslog は、監査モジュール（アプライアンス上で実行）とサーバー（リモートシステムで実行可能）の 2 つのコンポーネントを使用する、標準ロギングプロトコルです。Syslog プロトコルでは、データ転送でユーザーデータプロトコル（UDP）を使用します。管理者イベントとユーザーイベントが記録されます。

サーバーを構成して、以下の種類の情報を収集できます。

- XenMobile で実行されたアクションの記録が含まれるシステムログ
- XenMobile のシステムアクティビティの時系列の記録が含まれる監査ログ

syslog サーバーがアプライアンスから収集したログ情報は、メッセージ形式でログファイルに保存されます。通常、これらのメッセージには次の情報が含まれています。

- ログメッセージを生成したアプライアンスの IP アドレス
- タイムスタンプ
- メッセージの種類
- イベントに関連付けられたログレベル（重要、エラー、通知、警告、情報、デバッグ、アラート、または緊急）
- メッセージの情報

XenMobile は、log4j syslog アペンダーを使用して、RFC5424 形式の syslog メッセージを送信します。syslog メッセージ内のメッセージデータはプレーンテキストであり、特定の形式はありません。

この情報を使用してアラートの原因を分析したり、必要に応じて修正作業を行ったりすることができます。

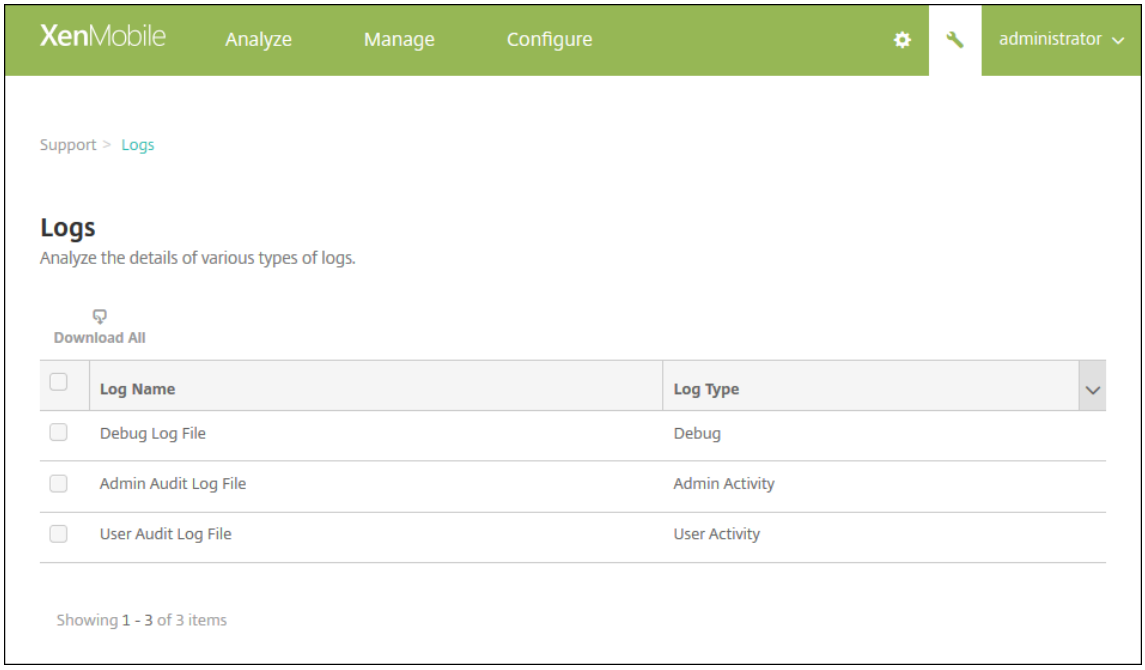
1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［**Syslog**］ をクリックします。［**Syslog**］ ページが開きます。
3. 次の設定を構成します。
    - サーバー： syslog サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。
    - ポート： ポート番号を入力します。デフォルトのポートは、514 です。
    - ログを記録する情報：［システムログ］ チェックボックスおよび ［監査］ チェックボックスをオンまたはオフにします。
        - システムログには、XenMobile で実行されたアクションが含まれます。
        - 監査ログには、XenMobile のシステムアクティビティの時系列の記録が含まれます。
        - XenMobile のログをデバッグします。
4. ［保存］ をクリックします。

XenMobile でのログファイルの表示

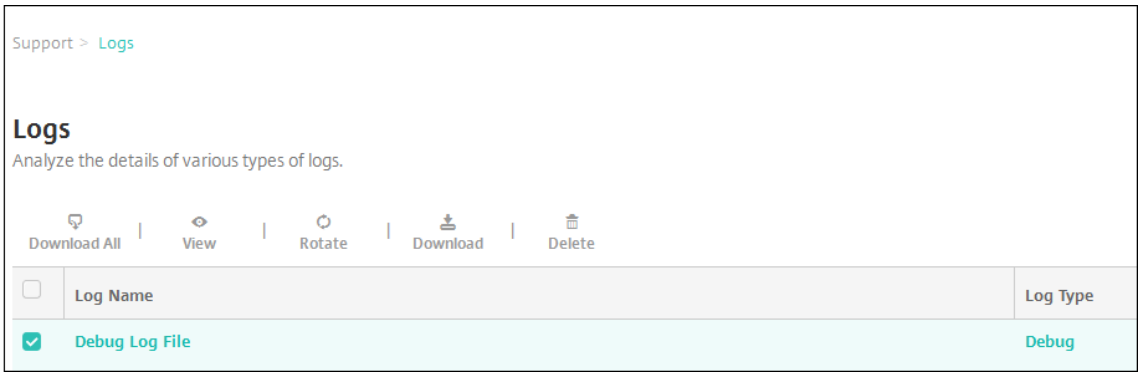
January 10, 2020

ログを表示、操作、およびダウンロードして、XenMobile での管理に役立てることができます。

1. XenMobile コンソールで、右上のレンチアイコンをクリックします。［サポート］ ページが開きます。
2. ［ログの操作］ の ［ログ］ をクリックします。［ログ］ ページが開きます。表に個別のログが表示されます。



3. 表示するログをオンにします。
   - デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrix のサポート担当者向けの有用な情報が含まれています。
   - 管理監査ログファイルには、XenMobile コンソール上の活動についての監査情報が含まれています。
   - ユーザー監査ログファイルには構成済みユーザーに関連する情報が含まれています。
4. 表の上にあるアクションを使用して、すべてダウンロード、表示、交換、単一ログのダウンロード、選択したログの削除を行います。

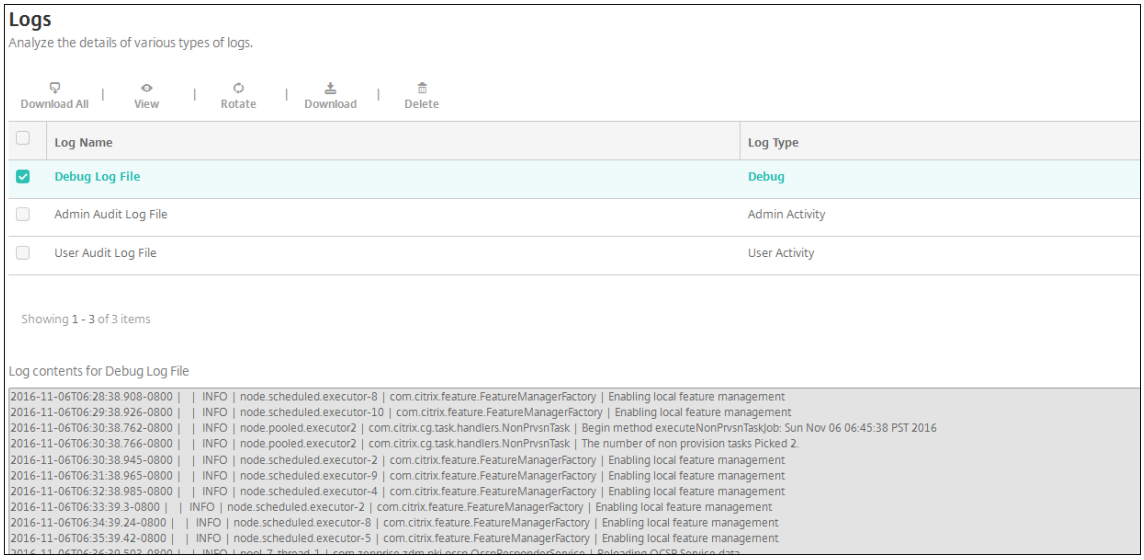


> 注:
>
> - 複数のログファイルを選択した場合は、［すべてダウンロード］ と ［交換］ のみを使用できます。

> • XenMobile サーバーをクラスター化している場合は、接続しているサーバーのログのみを表示できます。ほかのサーバーのログを表示するには、ダウンロードオプションのいずれかを使用します。

5. 次のいずれかを行います:

- すべてをダウンロード: システム上に存在するすべてのログ（デバッグ、管理監査、ユーザー監査、サーバーのログなど）をダウンロードします。
- 表示: 表の下に選択したログの内容を表示します。
- 交換: 現在のログファイルをアーカイブし、ログエントリを取得するための新しいファイルを作成します。ログファイルをアーカイブ化するときに、ダイアログボックスが開きます。[交換] をクリックして続行します。
- ダウンロード: 選択されている単一の種類のログファイルのみをダウンロードします。アーカイブ済みの同じ種類のログもダウンロードされます。
- 削除: 選択したログファイルを完全に削除します。



XenMobile Analyzer ツール

January 10, 2020

XenMobile Analyzer は、構成やその他の機能についての XenMobile に関連する問題の診断とトラブルシューティングを行うことができる、クラウドベースのツールです。このツールにより、XenMobile 環境内でのデバイスまたはユーザーの登録と認証の問題がチェックされます。

XenMobile サーバーをポイントするようにこのツールを構成するとともに、サーバーの展開の種類、モバイルプラットフォーム、認証の種類、ユーザーの資格情報などの情報の入力を行います。設定が完了するとツールはサーバーに接続し、構成の問題をチェックするために環境をスキャンします。XenMobile Analyzer で問題が検出されると、ツールにより問題を修正するための推奨事項が示されます。

主な機能

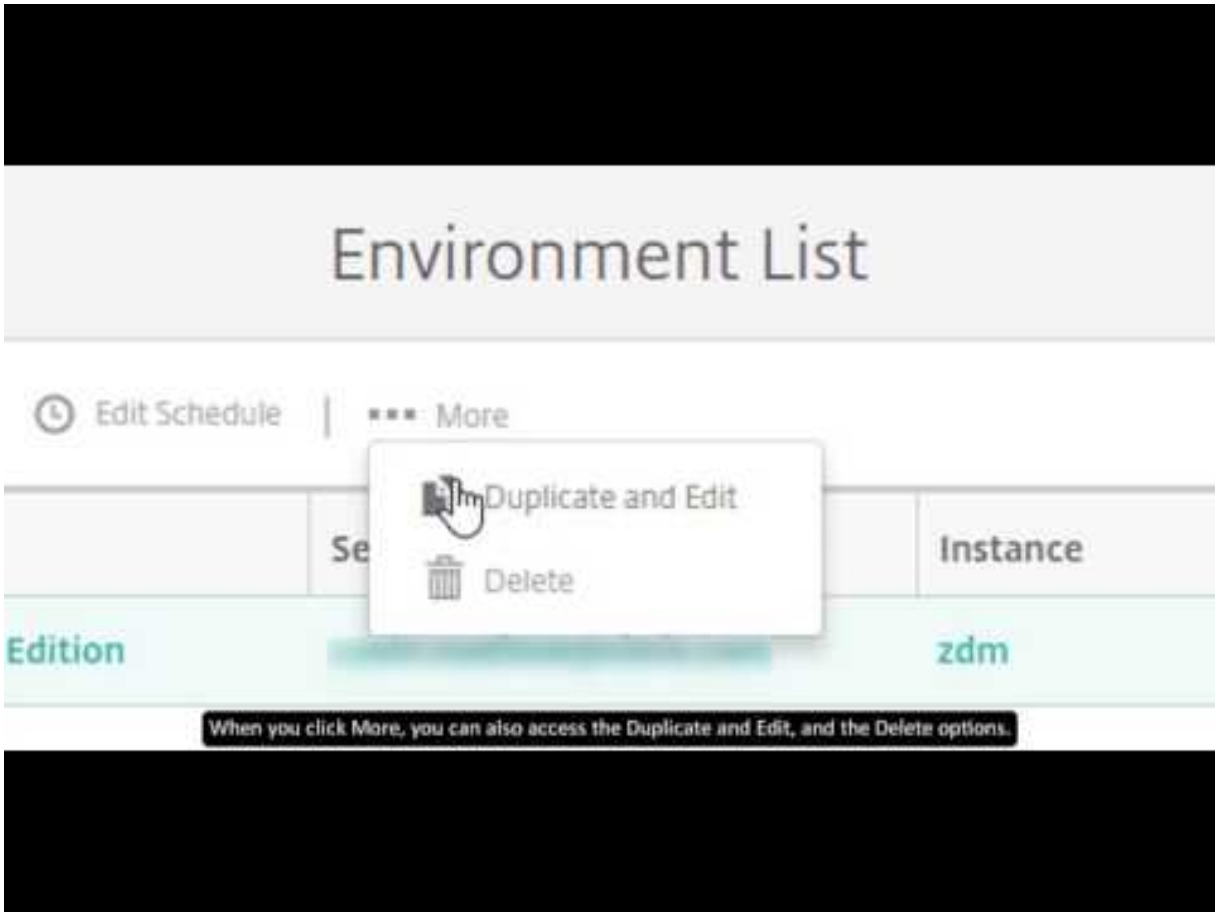
- 安全なクラウドベースのマイクロサービスにより XenMobile 関連の問題すべてのトラブルシューティングを行うことができます。
- 正確な推奨事項により XenMobile の構成に関する問題を解決できます。
- サポートへの問い合わせ件数を低減し XenMobile 環境のトラブルシューティングを迅速化します。
- XenMobile サーバーの各種リリースに対してゼロデイのサポートを行います。
- ヘルスチェックのスケジュールを毎日または週ごとで設定できます。
- NetScaler の構成をチェックします。
- イントラネットサイトへの Secure Web の到達可能性をテストします。
- Secure Mail Autodiscovery サービスのチェックを行います。
- ShareFile へのシングルサインオン（SSO）をチェックします。

新機能

- NetScaler 構成レポートに、推奨事項の数を示すバッジ通知が表示されるようになりました。推奨事項は、特定の NetScaler Gateway に対する必須構成チェックに基づいて作成されます。
- ユーザーエクスペリエンスの向上のため、［Test Environment List］ページのグローバルナビゲーションバーに含まれるアイコンの順序が調整されました。

次のビデオでは、ユーザーインターフェイスのナビゲーションの変更点について概要をお伝えします。

Citrix XenMobile Analyzer: 新しい環境リストの **UI**



> 注:
>
> このビデオには音声が含まれていません。全画面モードでご覧になることをお勧めします。

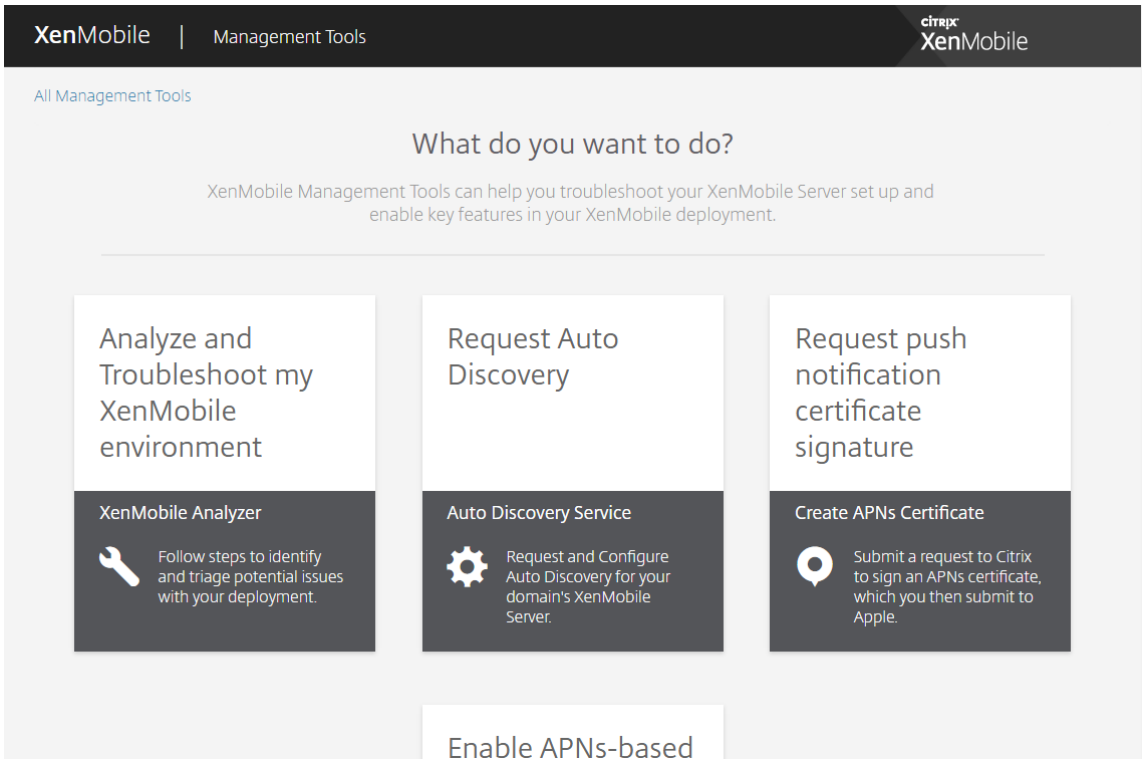
XenMobile Analyzer へのアクセスと起動

前提条件

製品	サポートされるバージョン
XenMobile Server	10.1.0 以降
NetScaler Gateway	10.5 以降
クライアント登録シミュレーション	iOS または Android

XenMobile Analyzer へのアクセスは、次のいずれかの方法で行います。

- XenMobile コンソールの右上にあるレンチアイコンをクリックして、［トラブルシューティングとサポート］ページを開きます。
- My Citrix 資格情報を使用してhttps://xenmobiletools.citrix.comからツールへアクセスします。表示された［XenMobile Management Tools］ページで、［**Analyze and Troubleshoot my XenMobile Environment**］ をクリックして XenMobile Analyzer を起動します。



XenMobile Analyzer には、トリアージプロセスを実行しサポートチケットを削減するための 5 つのオプションがあります。これらのオプションにより、すべてのユーザーの負担を減らすことができます。

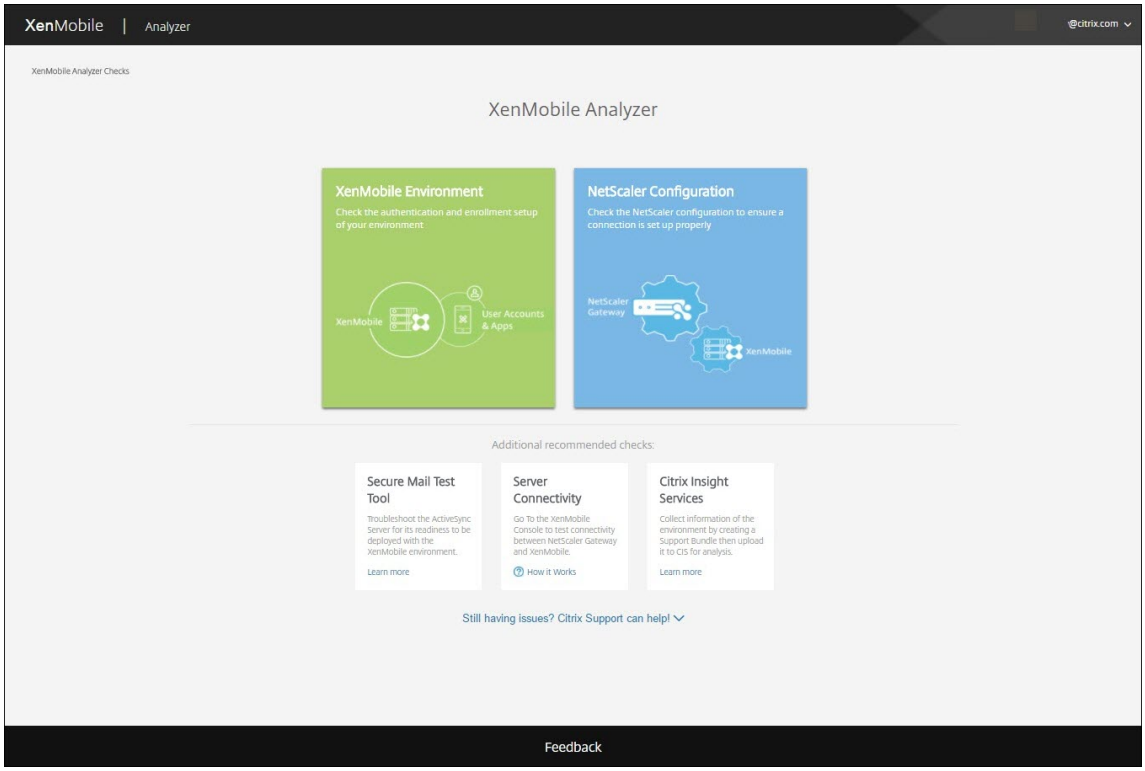
使用できるオプションは、次のとおりです。

- 環境チェック： この手順では、設定に問題がないかどうかをチェックするテストを設定します。また、デバイス、ユーザー登録、および認証に関する問題についての推奨事項も示されます。
- **NetScaler** チェック： この手順では、XenMobile 展開向けの NetScaler の構成が準備できているかをチェックします。
- 詳細診断： この手順では、環境チェックで見逃された可能性のある問題を Citrix Insight Services を使用して見つけるための情報が提供されます。
- サーバー接続チェック： この手順では、サーバーの接続性をテストする方法が示されます。
- **Citrix** サポートへの問い合わせ： この手順では、依然として問題が発生する場合に Citrix サポートケースを登録するためのサイトのリンクが表示されます。

以下のセクションで、これらのオプションについてより詳しく説明します。

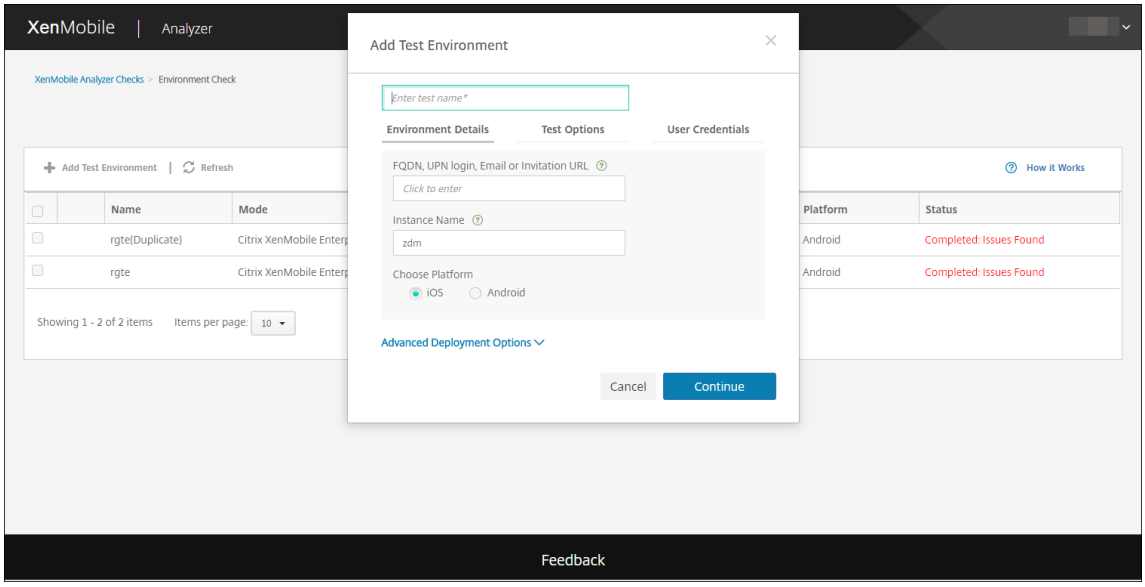
環境チェックの実行

1. XenMobile Analyzer にログオンし、［**XenMobile Environment**］ をクリックします。



2. ［**Add Test Environment**］ をクリックします。

3. 新しい ［**Add Test Environment**］ ダイアログボックスで、以下の操作を行います。



a) 今後テストを特定できるように、テストの一意の名前を入力します。

b) ［**FQDN, UPN login, Email or URL Invitation**］ に、サーバーへのアクセスに使用する情報を入力します。

c) カスタムインスタンスを使用している場合は、［**Instance Name**］ にその値を入力します。

d) ［**Choose Platform**］ で、テスト用のプラットフォームとして **iOS** または **Android** を選択します。

e) ［**Advanced Deployment Options**］ を展開すると、［**Deployment Mode**］ ボックスの一覧で、使用する XenMobile 展開モードを選択できます。使用できるオプションは ［**Enterprise**（**MDM + MAM**）］、［**App Management**（**MAM**）］、［**Device Managment**（**MDM**）］ です。

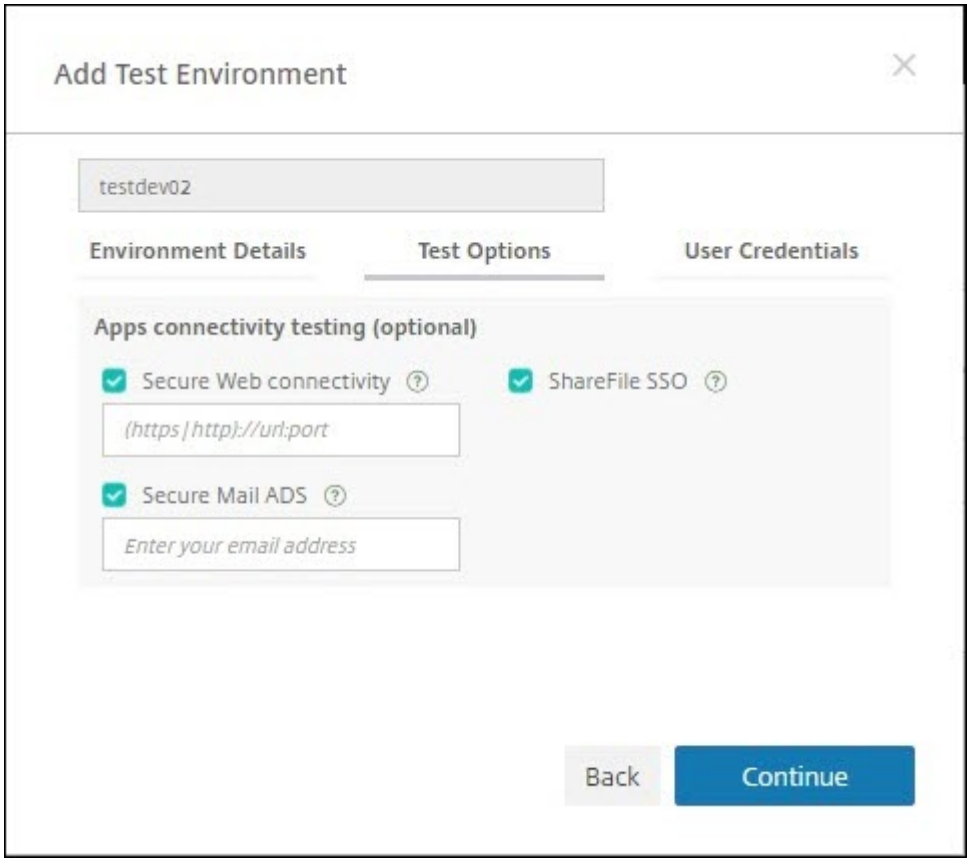
f) ［続行］ をクリックします。

4. ［**Test Options**］ タブで次のテストを 1 つまたは複数選択して、［**Continue**］ をクリックします。

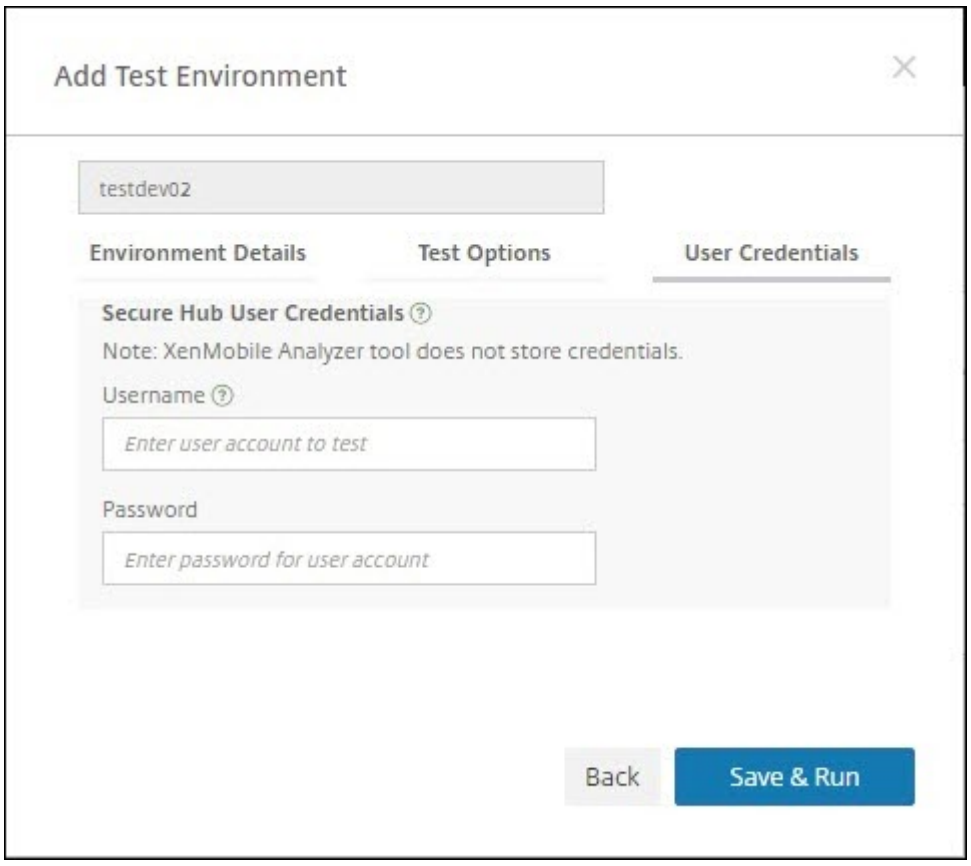
a) **Secure Web Connectivity**。イントラネットの URL を指定します。ツールにより、入力した URL への到達可能性がテストされます。このテストでは、イントラネットの URL への接続時に Secure Web アプリで生じる可能性のある、接続に関する問題が検出されます。

b) **Secure Mail ADS**。ユーザーの電子メール ID を指定します。この ID を使用して、XenMobile 環境にある Microsoft Exchange Server の自動検出機能がテストされます。Secure Mail Auto Discovery 関連の問題があるかどうかが検出されます。

c) **ShareFile SSO**。このオプションをオンにすると、ShareFile の DNS 解決が正常に行われるかどうかがテストされます。また、指定したユーザー資格情報で ShareFile のシングルサインオン（SSO）を実行できるかどうかもチェックされます。



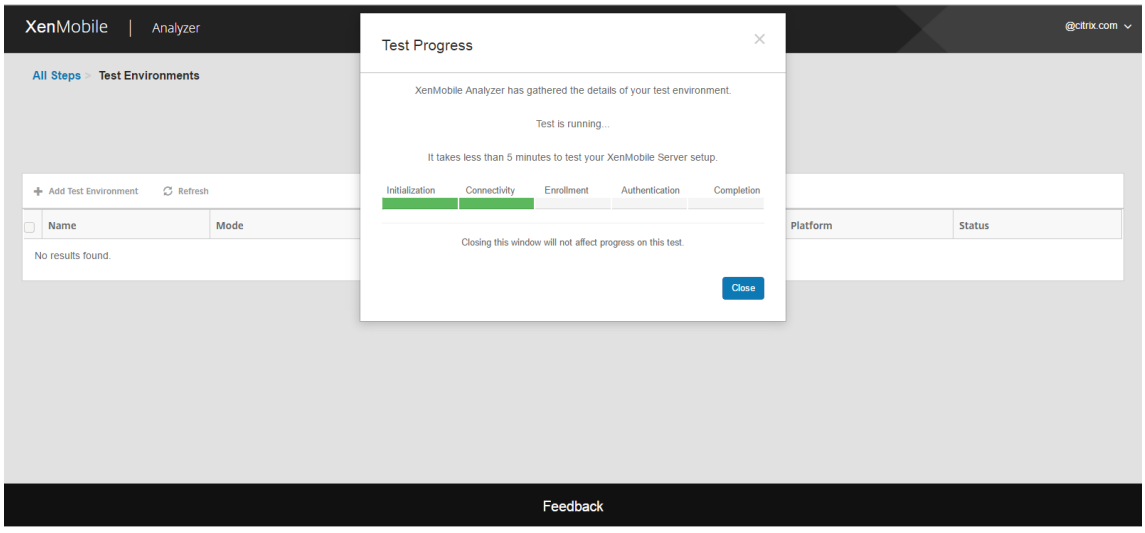
5. サーバーの設定によっては、［**User Credentials**］ タブに表示されるフィールドが異なる場合があります。［**Username**］、［**Username**］と［**Password**］、または［**Username**］、［**Password**］、［**Enrollment PIN**］ が表示される可能性があります。



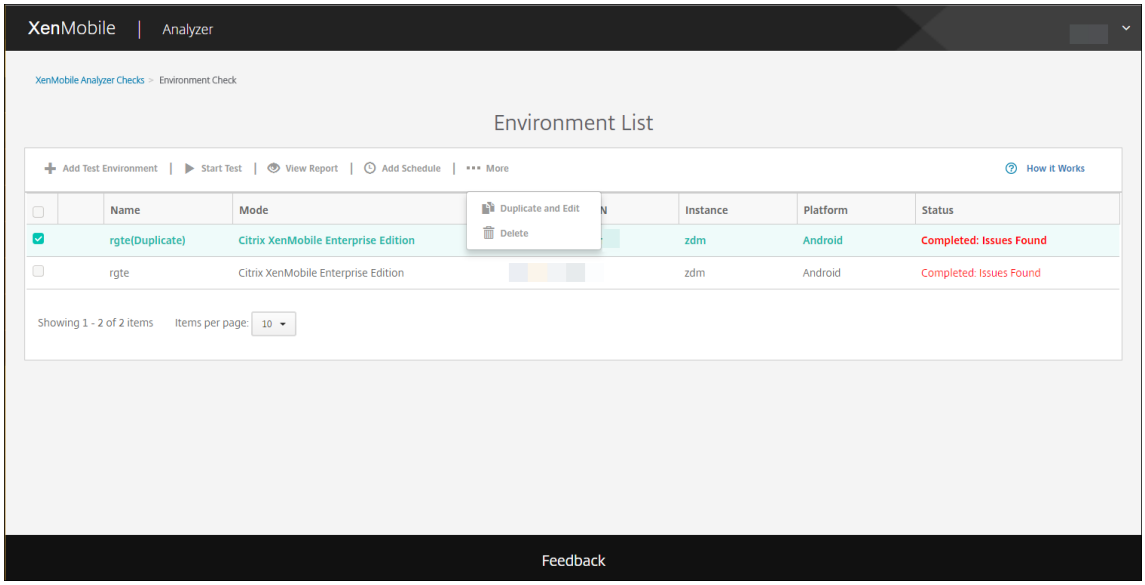
6. [**Save & Run**] をクリックしてテストを開始します。

   進行状況が表示されます。この進行状況を示すダイアログボックスは開いたままにしても、閉じても構いません。どちらの場合でもテストは続行されます。

   問題なく完了したテストは緑色で表示されます。失敗したテストは赤色で表示されます。



   進捗状況ダイアログボックスを閉じると、 [**Environments List**] ページに戻ります。



［**Results**］ ページには、テストの詳細、推奨事項、結果が表示されます。

7. ［**View Report**］ アイコンをクリックすると、テストの結果が表示されます。

   推奨事項に Citrix Knowledge Base の記事が関連している場合は、該当の記事がこのページに一覧表示されます。

8. ［**Results**］ タブをクリックすると、個別のカテゴリーとツールにより実行されたテストが、結果とともに表示されます。

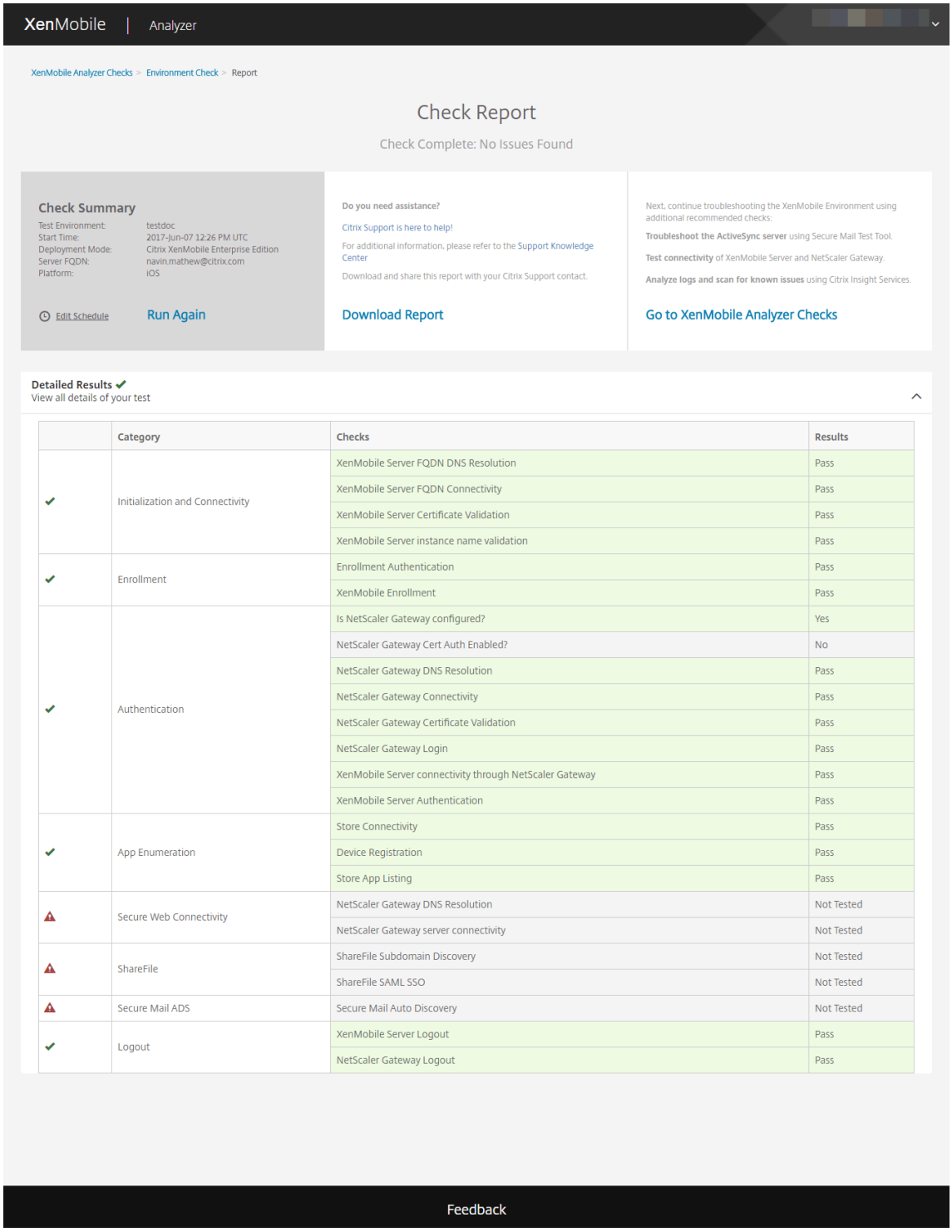
   a) レポートをダウンロードするには、［**Download Report**］ をクリックします。

   b) テスト環境の一覧に戻るには、［**Environment Check**］ をクリックします。

   c) 同じテストをもう一度実行するには、［**Run Again**］ をクリックします。

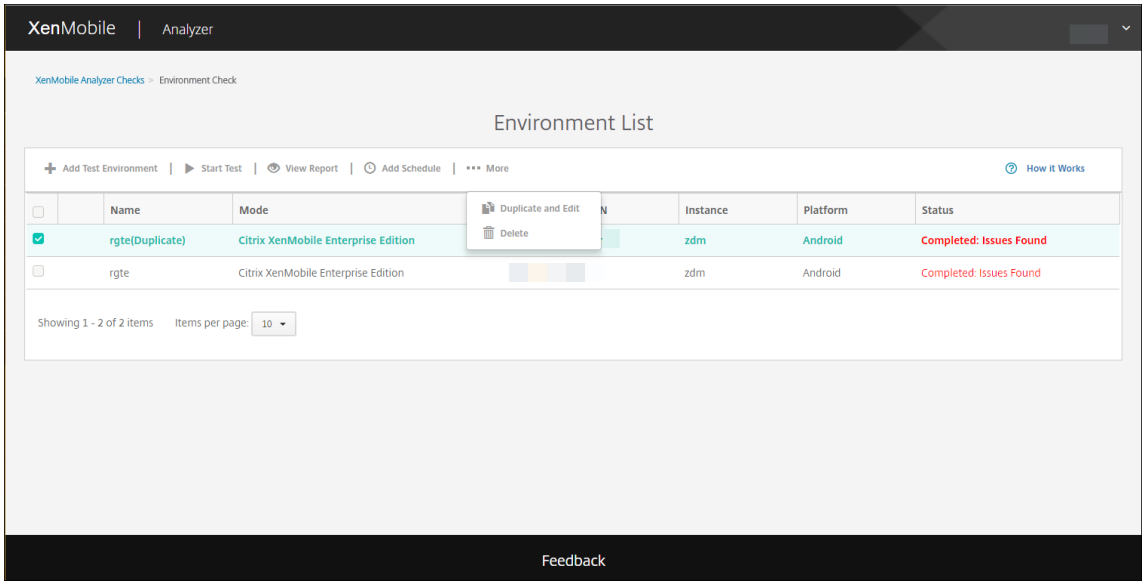
   d) 別のテストをもう一度実行するには、［**Test Environments**］ に戻って再実行するテストを選択し、［**Start Test**］ をクリックします。

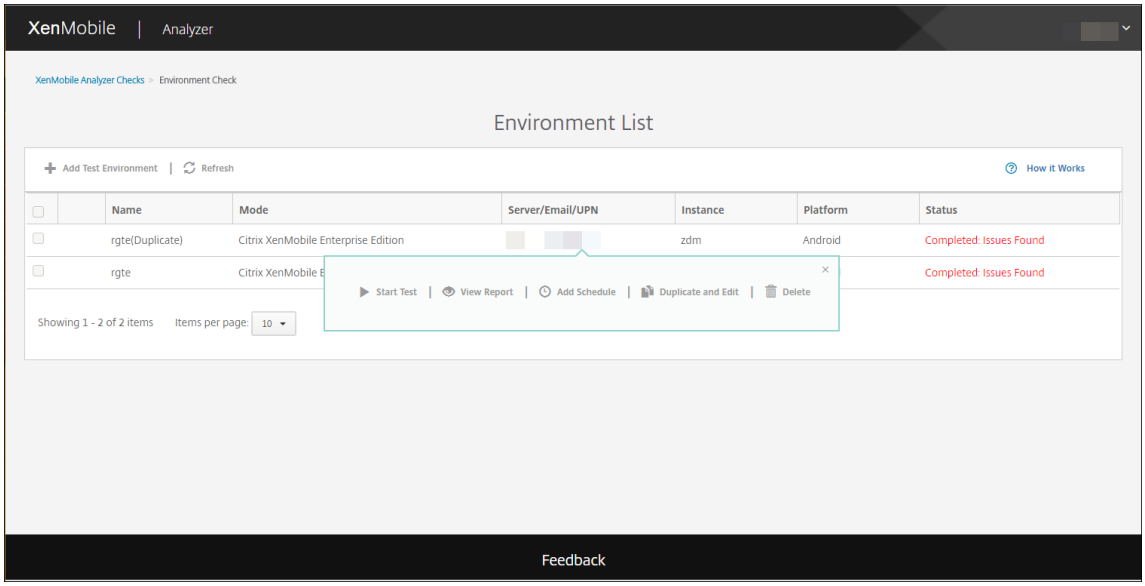
   e) XenMobile Analyzer の別のオプションを選択するには、［**Go To XenMobile Analyzer Checks**］ をクリックします。

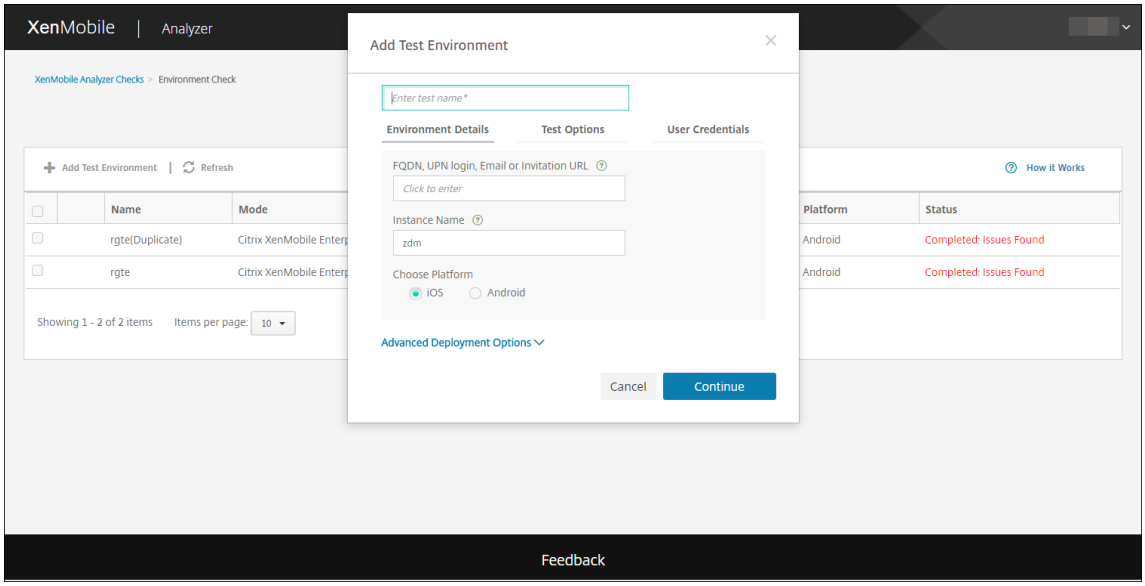


9. [Test Environments] ページで、テストをコピーし、編集できます。このためには、テストを選択して [**More**] をクリックし、 [**Duplicate and Edit**] を選択します。

   選択したテストのコピーが作成され、[Add Test Environment] ダイアログが開いて新しいテストを変更できるようになります。



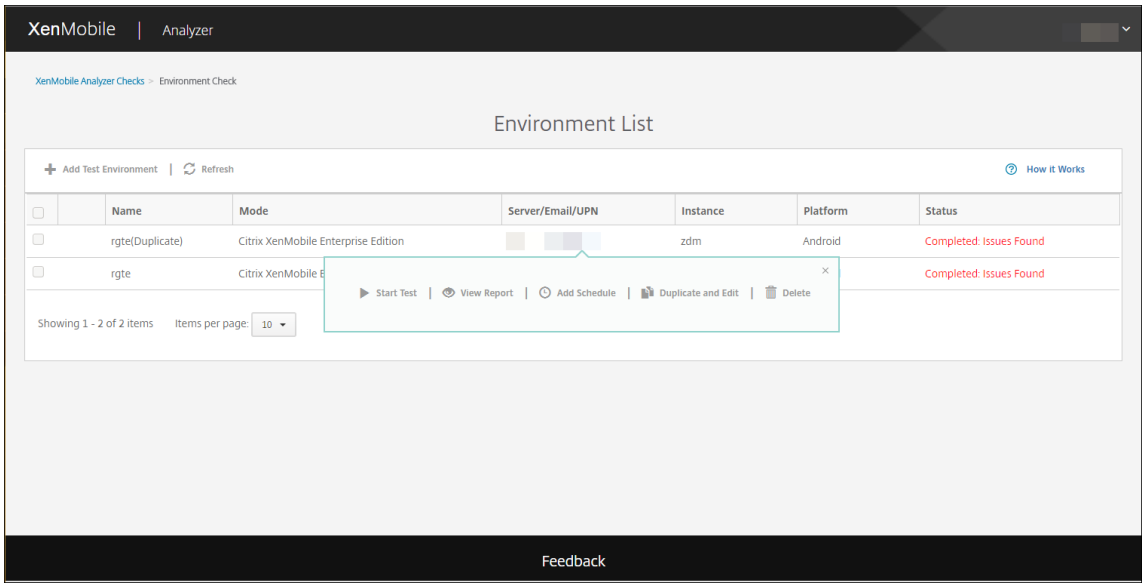




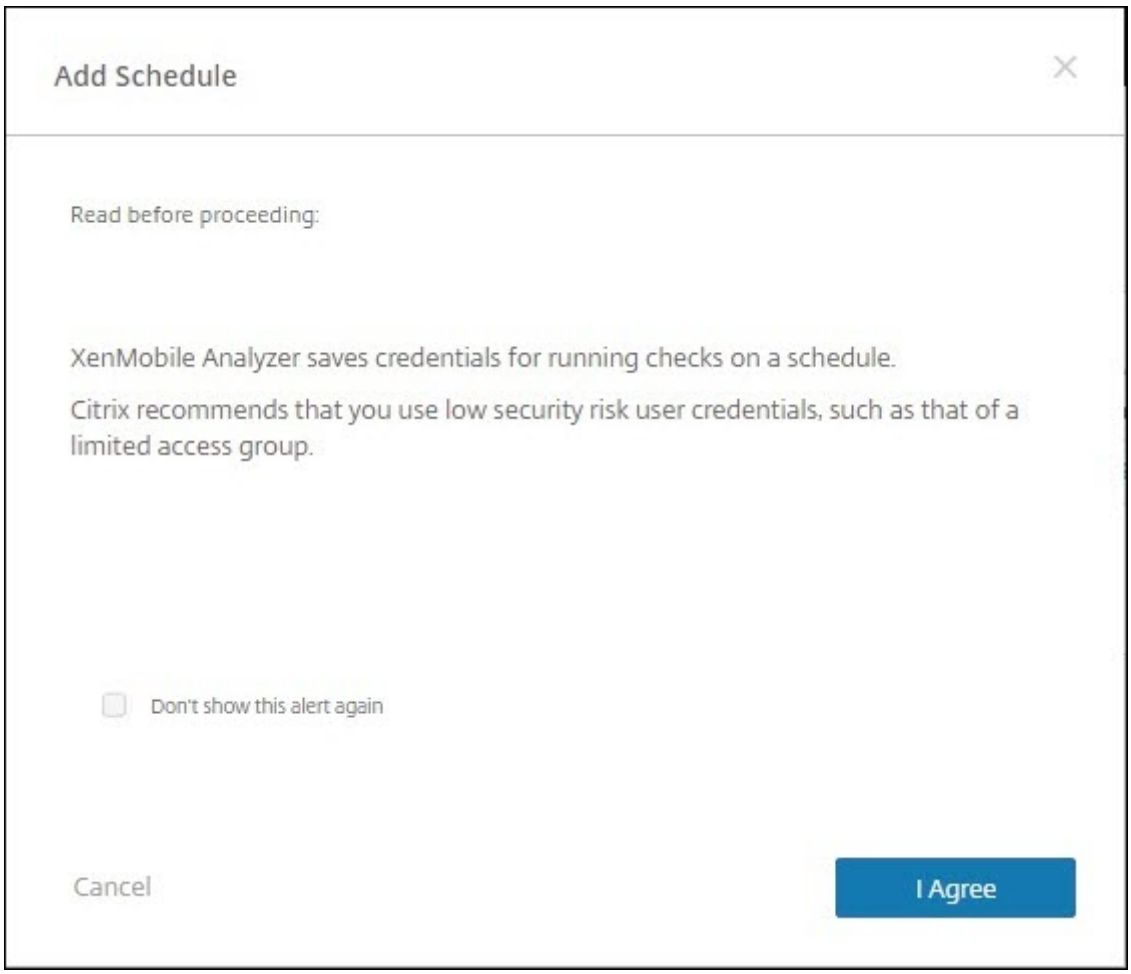
環境チェックのスケジュールの追加

テストは、スケジュールに基づいて自動で実行し、構成した一覧のユーザーに結果を送信するように構成できます。

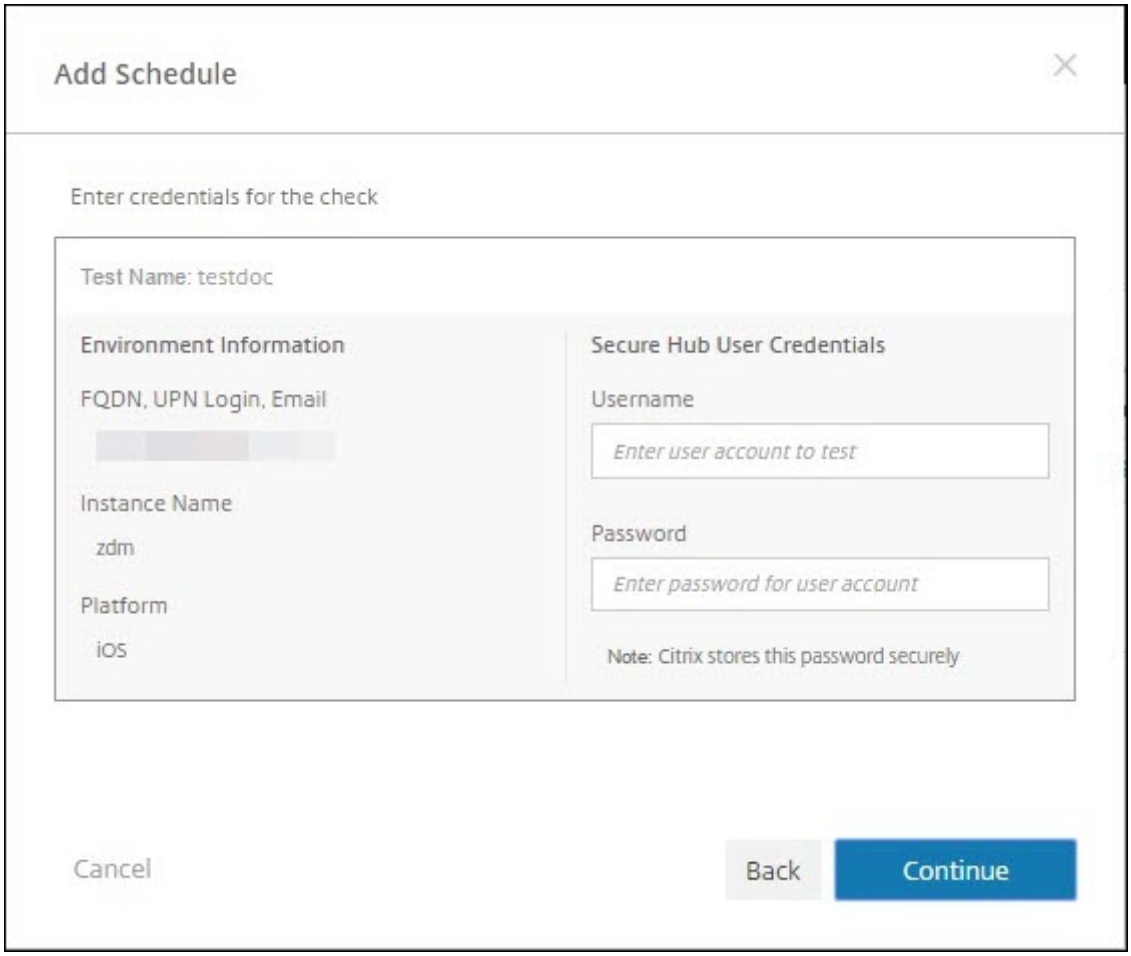
1. [**Environment List**] ページでスケジュールを設定する環境を選択し、[**Add Schedule**] をクリックします。



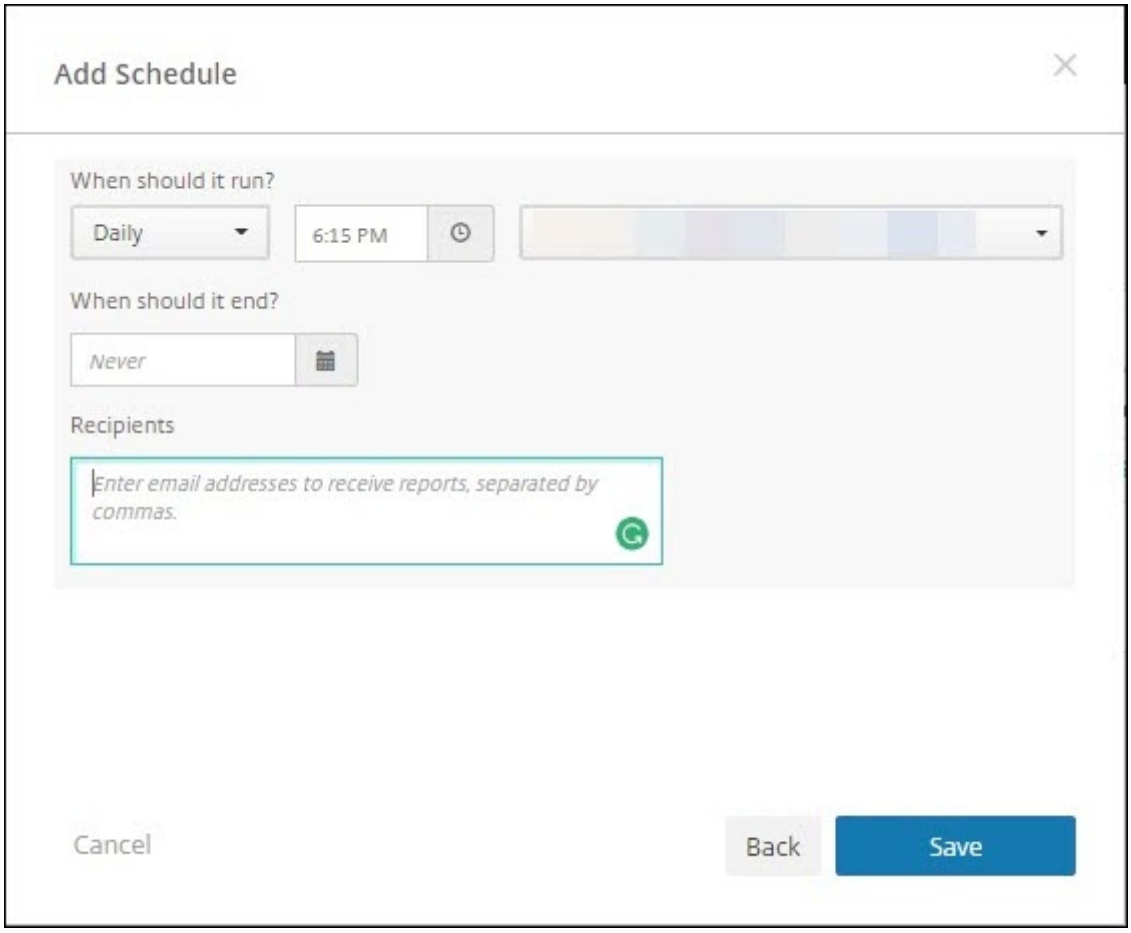
2. [**Add Schedule**] ウィンドウに、スケジュールに基づいてテストを実行するために XenMobile Analyzer に資格情報が保存されることを警告するメッセージが表示されます。スケジュールによるテストの実行には、アクセスが制限されたアカウントを使用することをお勧めします。[**I Agree**] をクリックして続行します。



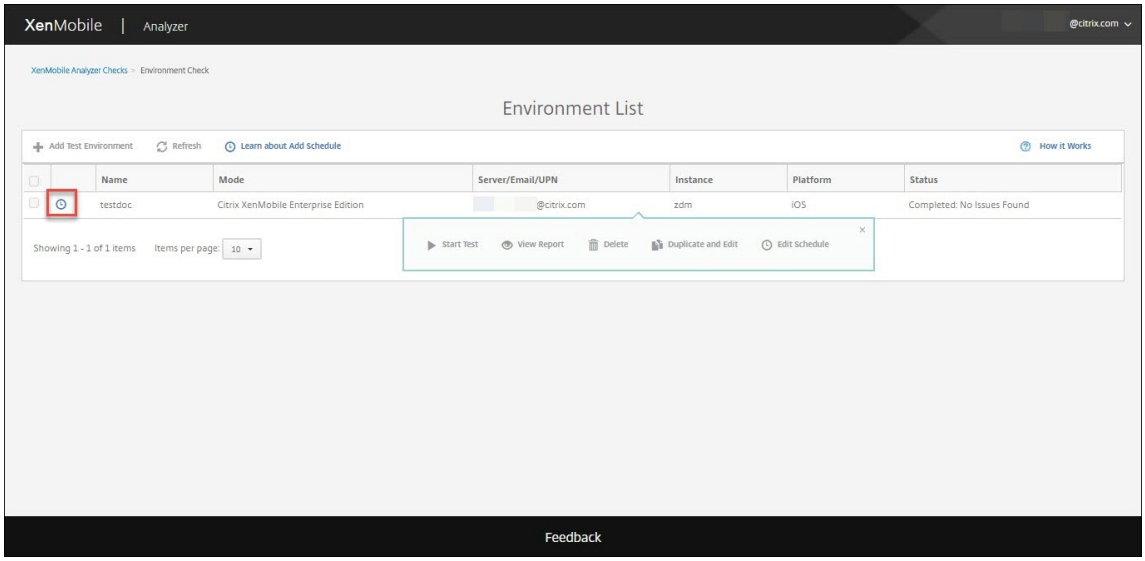
3. テストを実行するユーザー名とパスワードを入力します。



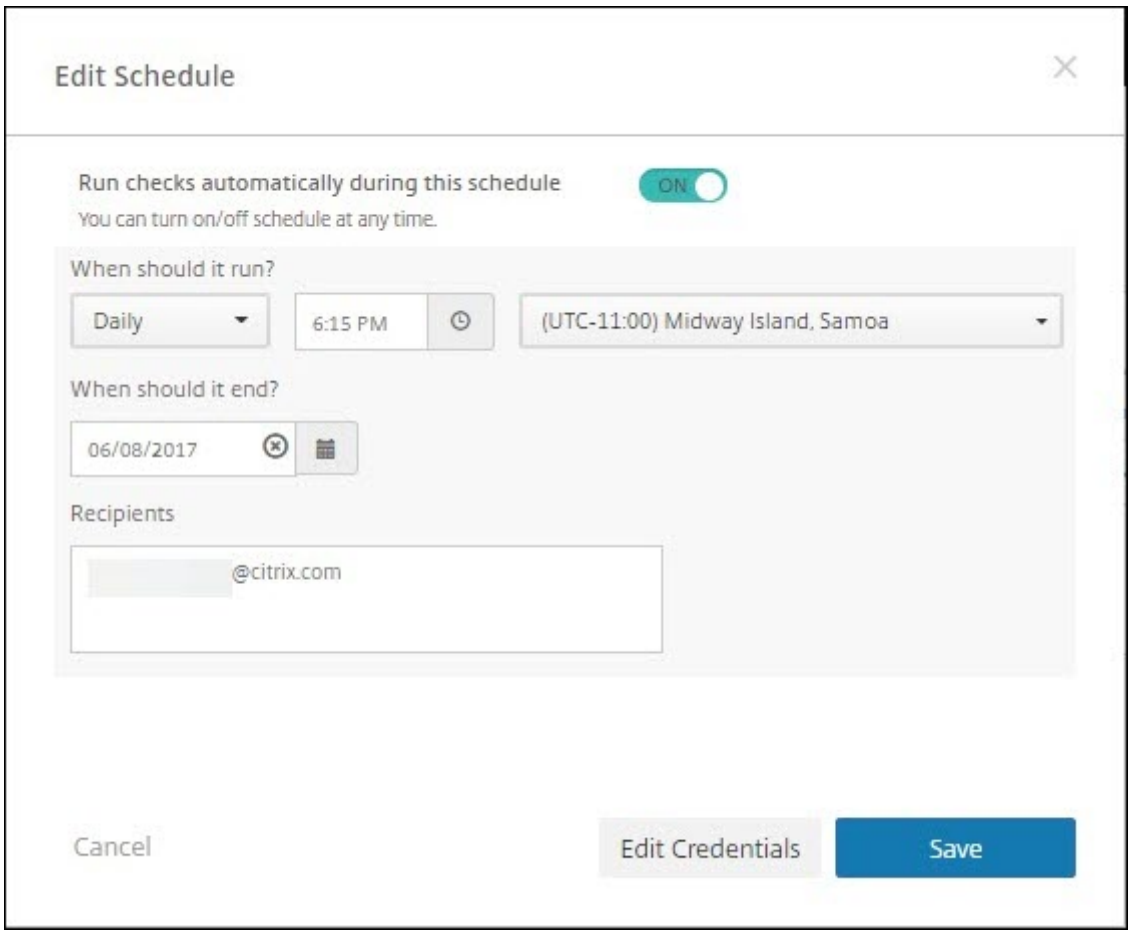
4. テストを実行するスケジュールを構成します。ドロップダウンから［**Daily**］ または ［**Weekly**］ を選択します。テストを実行する時刻とタイムゾーンを選択します。カレンダーを使用して、スケジュールしたテストの実行を停止する日付を選択します。テストを無期限に実行する場合は空白のままにします。レポートを送信するメールアドレスの一覧を、コンマで区切って入力します。［保存］ をクリックします。



5. テストの左側に、スケジュールが構成されていることを示す時計アイコンが表示されます。テストの実行タイミングを変更するには、テストを選択して ［**Edit Schedule**］ をクリックします。

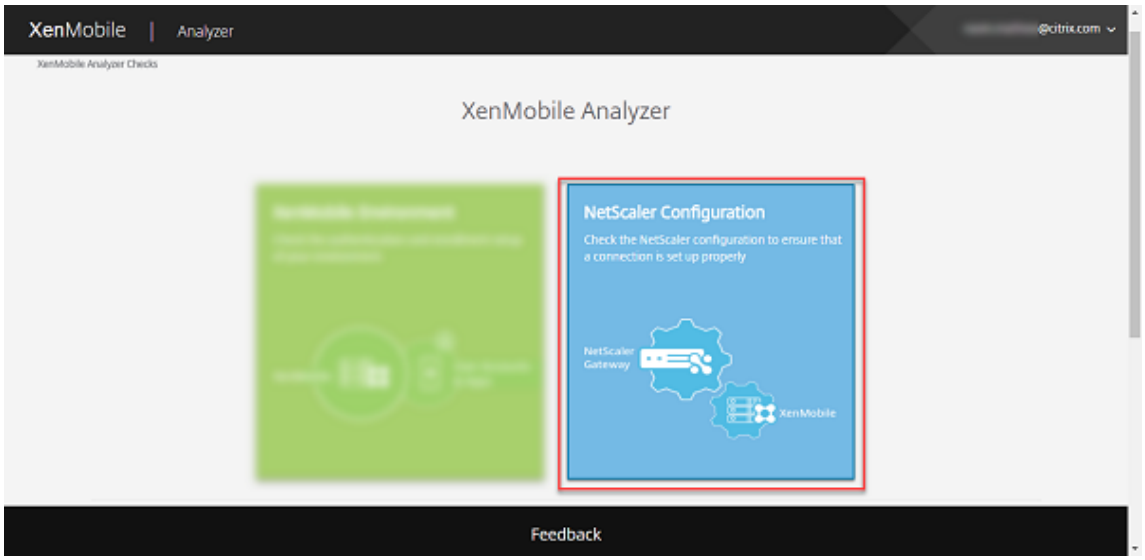


6. 表示されたウィンドウで、テストの実行タイミングを変更できます。最上部にあるスイッチをクリックして、テストを無効にすることもできます。変更が完了したら ［**Save**］ をクリックします。

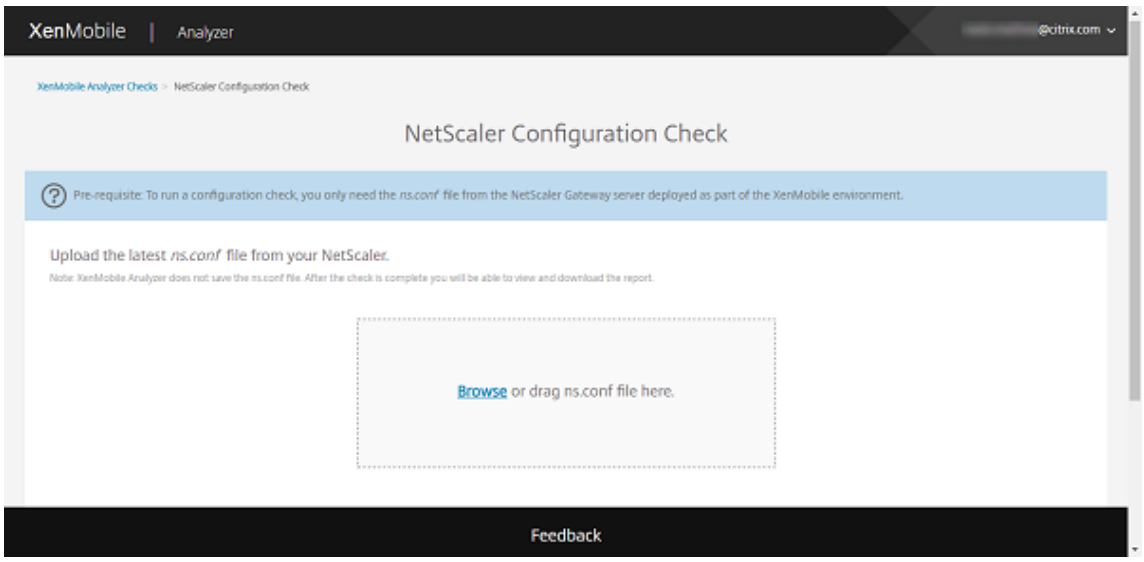


NetScaler チェックの実行

1. XenMobile Analyzer にログオンして ［**NetScaler Configuration**］ をクリックします。

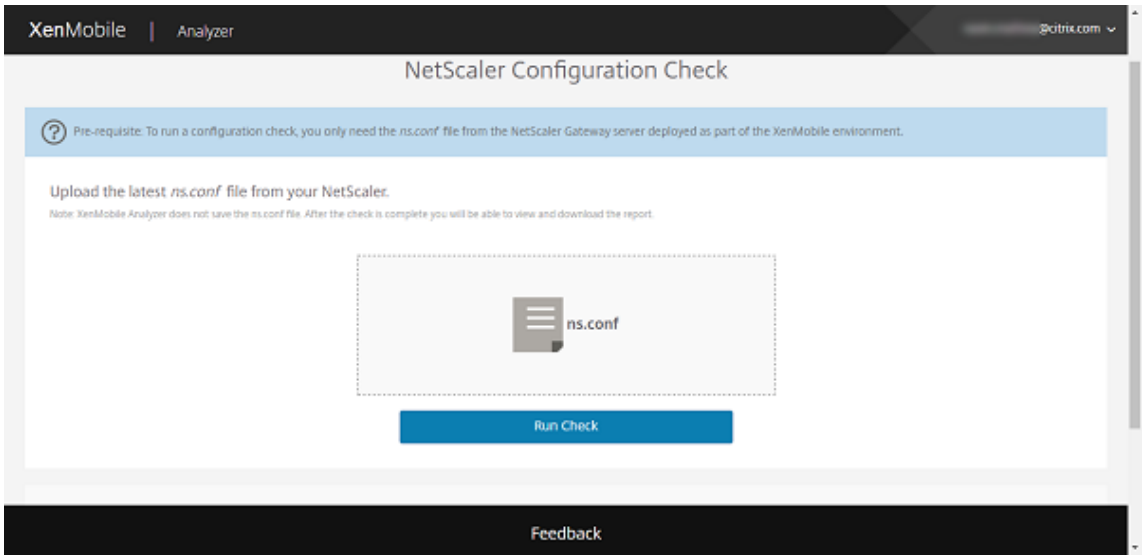


2. NetScaler インスタンスの最新の ns.conf ファイルをアップロードします。アップロードは、ns.conf ファイルをアップロードボックスにドラッグするか、［**Browse**］ をクリックしてファイルを追加することにより行います。最新の ns.conf ファイルのダウンロード方法について詳しくは、Support Knowledge Centerを参照してください。



> 注:
>
> XenMobile Analyzer に ns.conf ファイルは保存されません。チェックが完了すると、レポートを表示およびダウンロードできるようになります。

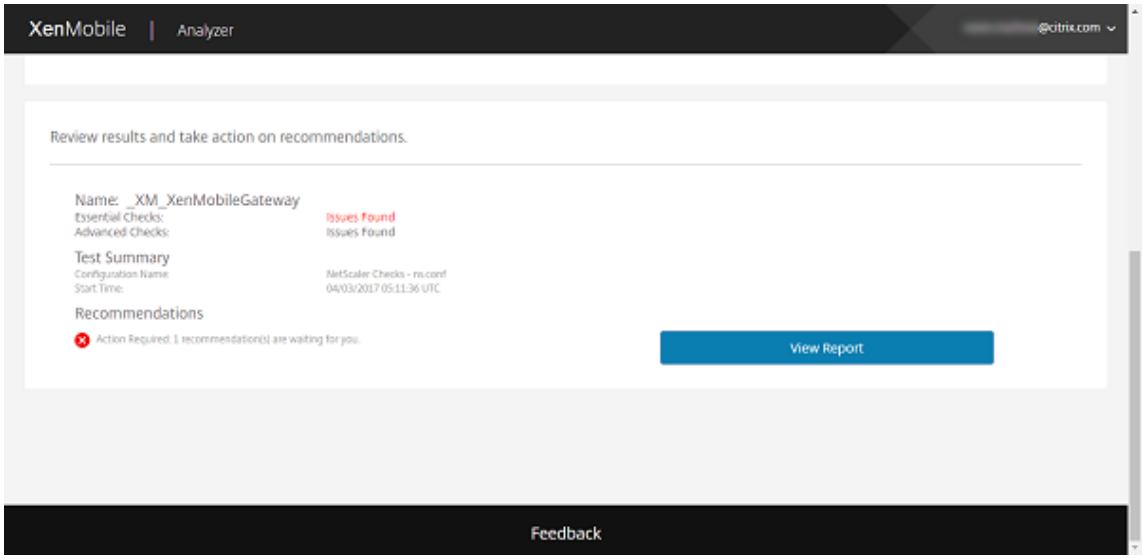
3. ［**Run Check**］ をクリックします。



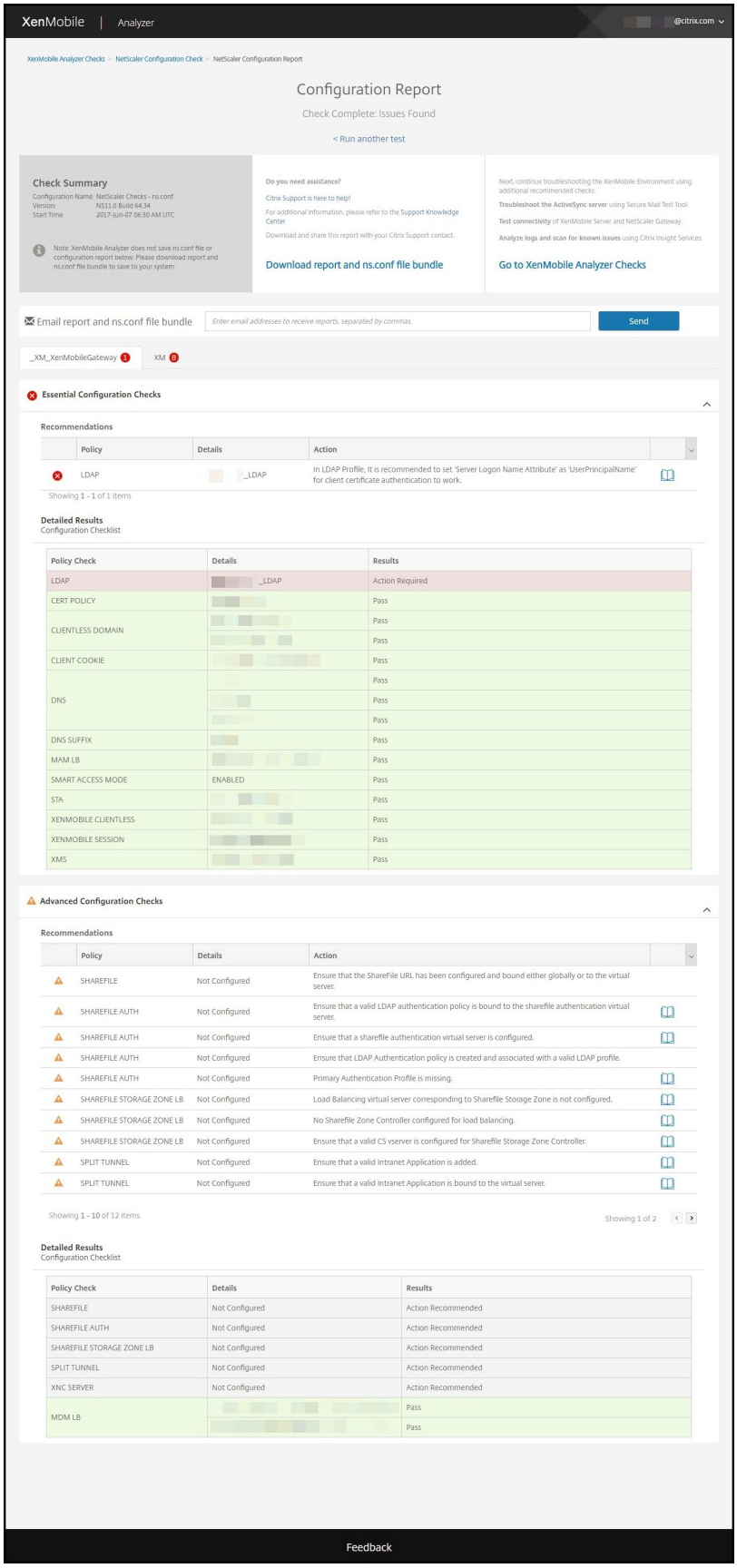
2 種類の構成チェックが実行されます。

- 必須チェックでは、XenMobile を正常に展開するために不可欠なコンポーネントを確認します。
- 詳細チェックでは、必須ではないものの XenMobile の展開を補助するコンポーネントを確認します。

4. NetScaler の必須チェックおよび詳細チェックに基づく推奨事項を確認するには、［**View Report**］ をクリックします。



［**Configuration Report**］ ページが開きます。



> 注：
>
> XenMobile Analyzer では、NetScaler ウィザードを使用して構成されたゲートウェイサーバーがサポートされます。NetScaler Gateway インスタンスのタイトルにはすべて、「_XM_* 展開時にユーザーが指定した名前」という名前が付けられます。

必須構成チェックに合格すると、全体の状態が［成功］になります。

必須構成チェックに失敗すると、［Recommendations］テーブルにポリシー、詳細、結果（必要なアクション）が一覧表示されます。

詳細構成チェックに失敗すると、［Recommendations］テーブルにポリシー、詳細、結果（推奨されるアクション）が一覧表示されます。

構成レポートの通知バッジに、NetScaler ウィザードを使用して構成されたゲートウェイサーバーおよびユーザーが構成したゲートウェイに関する必須構成チェックの推奨事項の件数が表示されます。

［**Configuration Report**］ ページには次のオプションが用意されています。

a) 詳細を表示するには、［**Essential Configuration Checks**］または［**Advanced Configuration Checks**］（または展開アイコン）をクリックします。

b) 別の NetScaler 構成チェックを実行するには、［**Run another test**］ をクリックします。

c) トラブルシューティングツールおよび分析ツールを表示するには、［**Go to XenMobile Analyzer Checks**］ をクリックします。

d) 結果のレポートをダウンロードするには ［**Download report**］ と ［**ns.conf file bundle**］ をクリックします。または、［**Email report and ns.conf bundle**］ にメールアドレスを入力して、［送信］ をクリックします。

その他の有益なチェックの実行

XenMobile Analyzer の環境チェック手順では直接操作してテストを実行しますが、その他のオプションでは役立つ情報が提供されます。これらの各オプションでは、XenMobile 環境を正しく設定するために使用できる他のツールの情報が提供されます。

- 詳細診断： 環境に関する情報を収集して、Citrix Insight Services にアップロードします。このツールによってデータが分析され、環境に合ったレポートが推奨される解決方法とともに提供されます。
- **Secure Mail** の用意： XenMobile Exchange ActiveSync Test アプリケーションをダウンロードして実行します。このアプリケーションでは、XenMobile 環境への展開についての ActiveSync サーバーのトラブルシューティングを行います。アプリケーションを実行した後に、レポートを確認したり他のユーザーと共有したりできます。
- サーバー接続チェック： XenMobile サーバー、認証サーバー、および ShareFile サーバーへの接続を確認するための手順が示されます。

- **Citrix** サポートへの問い合わせ： 他のすべての手順が失敗した場合に、Citrix サポートでサポートチケットを作成できます。

既知の問題

Citrix Endpoint Management アナライザーに関する既知の問題は次のとおりです。

- Secure Web の接続チェックを実行する場合、テキストボックスに複数の URL を入力することはできません。
- Secure Hub の共有デバイス認証機能は使用できません。
- Secure Web テストは入力された URL への接続をチェックするだけで、関連サイトへの認証はチェックしません。

解決された問題

以下の XenMobile Analyzer の問題は解決されました。

- 登録招待を使用してチェックを実行すると、テストは成功しますが登録招待は受理されません。

REST API

January 10, 2020

> 注:
>
> この記事では、XenMobile Server の REST API について説明します。Endpoint Management 用の REST API については、「REST API」を参照してください。

XenMobile REST API により、XenMobile コンソールで公開されるサービスを呼び出すことができます。REST クライアントを使用して、REST サービスを呼び出すことができます。API について、サービスを呼び出すために XenMobile コンソールにサインオンする必要はありません。

現在使用できる API の全一覧については、『Public API for REST Services』（PDF）をダウンロードしてください。

REST API へのアクセスに必要な権限

REST API へのアクセスには、以下の権限のうち 1 つが必要です。

- 役割ベースのアクセス構成の一部として設定されたパブリック API アクセス権限詳しくは、「RBAC を使用した役割の構成」を参照してください。
- スーパーユーザー権限

REST API サービスを呼び出すには

REST クライアントまたは CURL コマンドを使用して、REST API サービスを呼び出すことができます。以下の例では、Advanced REST client for Chrome を使用します。

> 注：
>
> 以下の例のホスト名とポート番号は、自分の環境に合わせて変更してください。

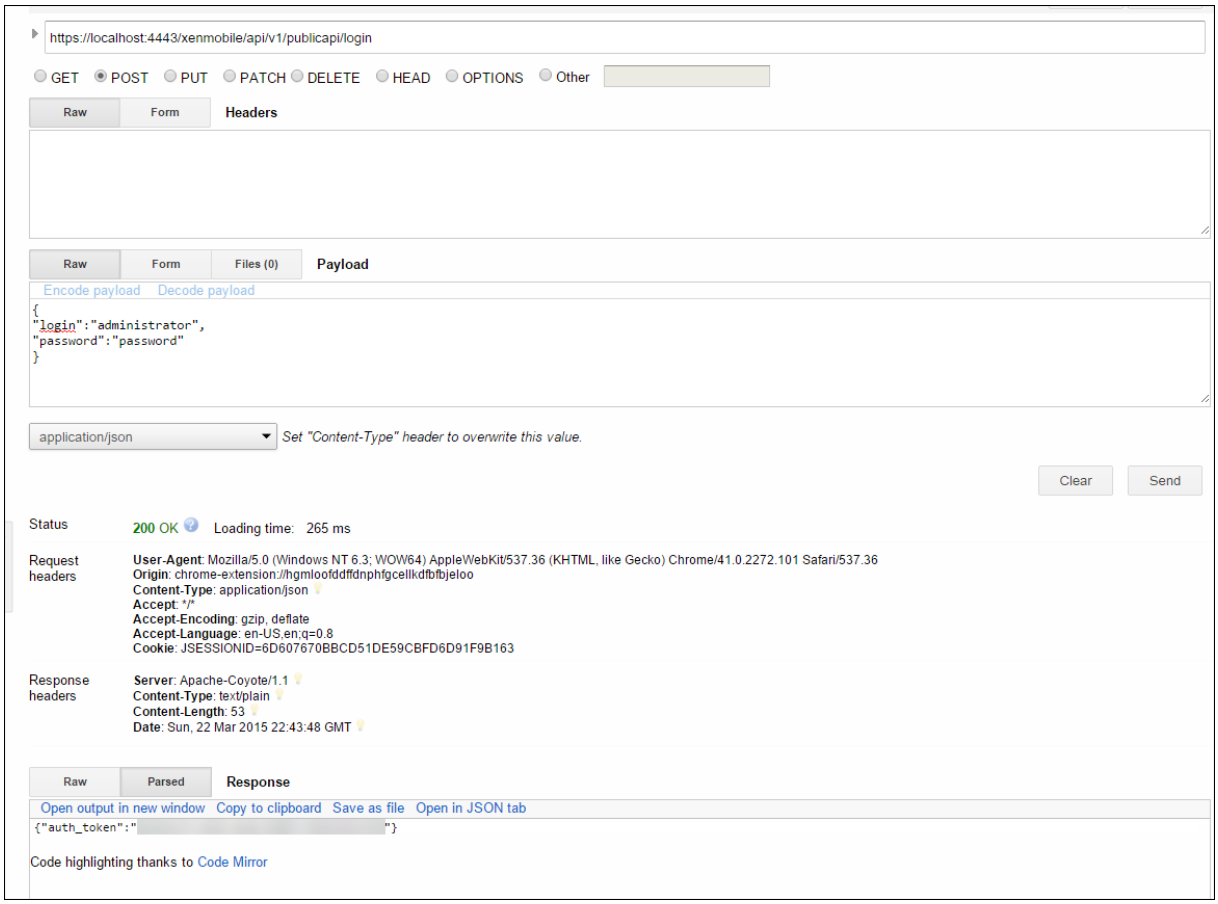
ログイン

URL：`https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

要求：`{ "login":"administrator", "password":"password"}`

メソッドの種類：POST

コンテンツの種類：application/json



関連情報

- XenMobile REST API

Endpoint Management コネクタ：Exchange ActiveSync 用

October 25, 2019

XenMobile Mail Manager は「Endpoint Management コネクタ：Exchange ActiveSync 用」になりました。シトリックス統合製品ラインについて詳しくは、シトリックス製品名ガイドを参照してください。

コネクタは、以下の方法で XenMobile の機能を拡張します：

- Exchange ActiveSync（EAS）デバイスに対するダイナミックアクセス制御。EAS デバイスの Exchange サービスに対するアクセスを自動的に許可または禁止できます。
- Exchange が提供する EAS デバイスパートナーシップ情報にアクセスする、XenMobile の機能。
- モバイルデバイスで EAS ワイプを実行する XenMobile の機能。
- Blackberry デバイスに関する情報にアクセスしたり、ワイプやパスワードリセットなどの制御操作を実行したりする XenMobile の機能。

「Endpoint Management コネクタ：Exchange ActiveSync 用」をダウンロードするには、Citrix.comの XenMobile 10 サーバーのサーバーコンポーネントセクションに移動します。

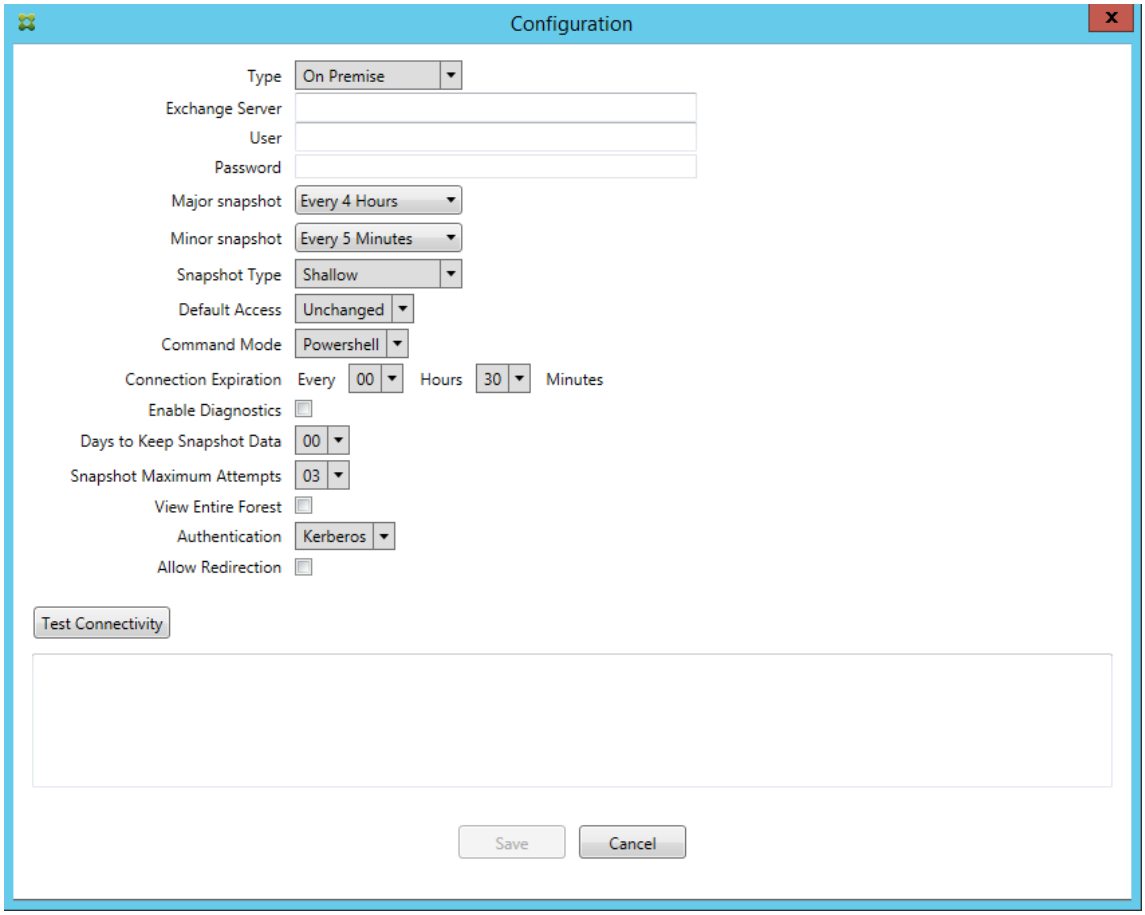
新機能

以下のセクションでは、「Endpoint Management コネクタ：Exchange ActiveSync 用」（旧称：XenMobile Mail Manager）の新機能を示します。

バージョン **10.1.10** の新機能

バージョン 10.1.10 では、次の問題が解決されています。

- ネットワークの問題が頻繁に発生している場合、以前の 3 回の試行では、スナップショットを完了できない場合があります。このリリースでは、管理者は最大試行数（1 ～ 10）を設定できます。この修正により、スナップショットの通信が複数回中断されても、スナップショット処理を完全に放棄する必要がなくなりました。[CXM-70837]



- 以前のバージョンでは、Exchange 構成の一覧にスナップショットの種類が表示されませんでしたが、スナップショットの種類が表示されるようになりました。[CXM-70846]
- PowerShell によって報告された PSRemotingTransport の例外は、Exchange へのセッションが実行可能ではなくなったことを示しています。この状態は、デフォルトで構成ファイルの［重大なエラー］の一覧に追加されます。これにより、PSRemotingTransportException が検出されると、この接続は後で廃棄のために［エラー］としてマークされます。次の通信では、有効な接続を使用するか、新しい接続を作成します。[XMHELP-2184, CXM-70836]
- 構成の変更を保存すると、新しい構成を読み込む前に、以前に構成された内部コンポーネントの一部が適切に廃棄されない可能性があります。この問題により、予期しない動作が発生する可能性があります。動作は、特定の変更によって、また変更が以前の構成と競合しているかどうかによって異なります。このリリースでは、新しい構成が読み込まれる前に、すべての内部コンポーネントが破棄されます。[XMHELP-2259, CXM-71388]

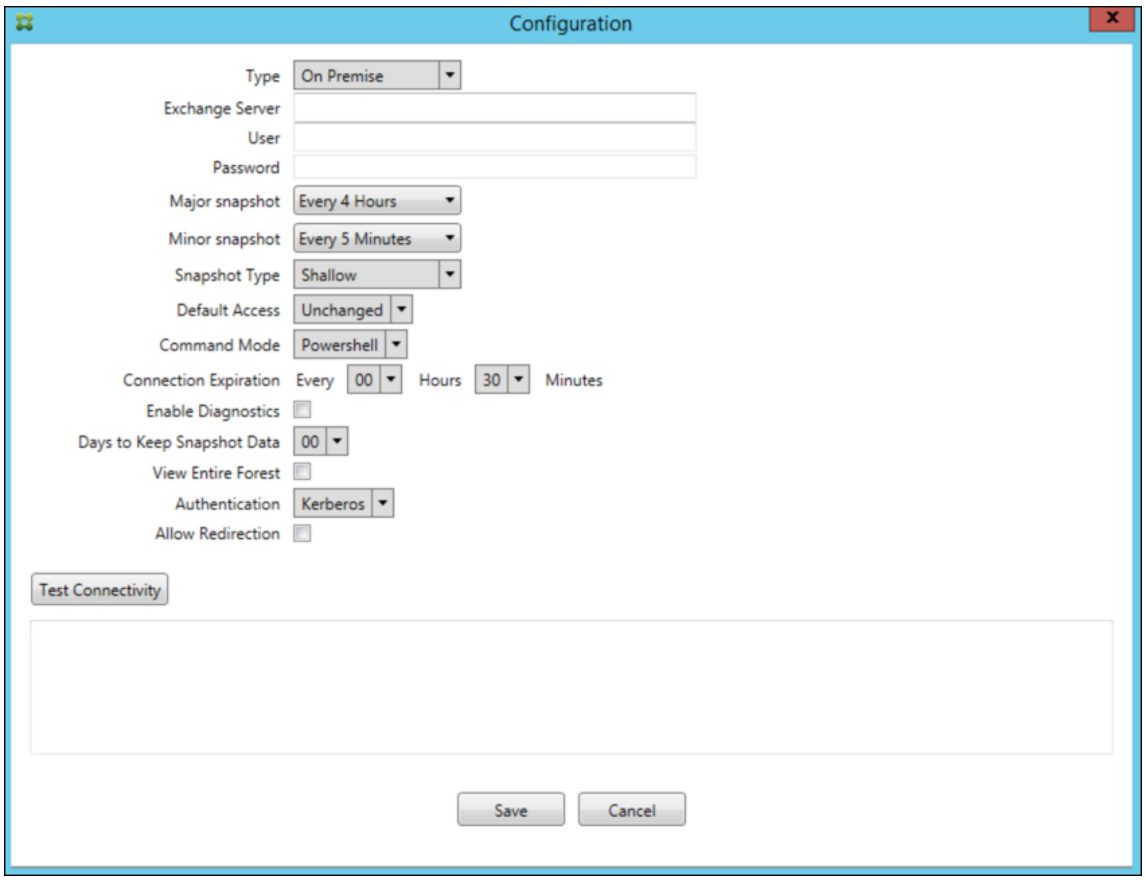
以前のバージョンの新機能

次のセクションでは、Endpoint Management コネクタ: Exchange ActiveSync 用の機能と、以前のバージョンから解決された問題の一覧を示します。

バージョン **10.1.9** の新機能

バージョン 10.1.9 では、次の問題が解決されています。

- 構成の変更は、より一貫性のある方法で処理されるようになりました。サービスが構成の変更を検出すると、各内部サブシステムが停止します。その結果、アクティブな処理またはスケジュールされた処理が中断されます。次に、新しい構成が読み込まれ、サブシステムが再起動します。つまり、すべてのスケジュールと他の内部インフラストラクチャが新しい設定で再確立されます。これによって、バージョン 10.1.8 の既知の問題が修正されます。[CXM-47709, CXM-61330]
- アップグレード中に、既存のデータベース構成が新しい構成ファイルにマージされませんでしたが、アップグレードされた構成ファイルにデータベース構成がマージされるようになりました。[CXM-49326]
- スナップショット関連の診断ファイルで、列見出しが見つかりませんでした。この見出しは復元されます。[CXM-62680]
- 以前のバージョンからアップグレードする場合、構成ファイルのデフォルトのセクションは、使用中の構成ファイルの類似セクションによって上書きされていました。この問題により、アップグレード後にサービスによって読み込まれるデフォルトのセクションに対する追加や機能向上が無視されていました。このバージョンでは、デフォルトのセクションには常に最新の構成が反映されます。[CXM-62681]
- 管理者は、アプリケーションの実行時に Shift キーを押すことで特定のオプションにアクセスできなくなります。これらのオプションは、以前は Citrix 権限で使用できました。[Allow Redirection] などの一部のオプションは完全に使用できるようになり、[Hang Detection] や [Count Correction] などの他のオプションは廃止されました。[CXM-62767]



バージョン **10.1.8** の新機能

バージョン 10.1.8 では、次の問題が解決されています。

- Citrix Endpoint Management コネクタ: Exchange ActiveSync サービス用が頻繁にコマンドを発行しないように、Exchange が調整することがあります。これは、Office 365 への接続でよくあることです。この結果、次のコマンドの送信前にサービスが一定期間停止する必要があります。構成コンソールで、停止の残り時間が表示されるようになりました。[CXM-48044]
- 構成ファイル（config.xml）の「Watchdog」セクションや「SpecialistsDefaults」セクションが変更されても、アップグレード後の構成ファイルに変更が反映されませんでした。このリリースでは、新しい構成ファイルに変更が正しく反映されます。[CXM-52523]
- Google Analytics に送信される分析内容（特にスナップショット関連）にさらに詳細が追加されました。[CXM-56691]
- Exchange の接続性テスト機能が接続を開始しようとするのは 1 回だけです。Office 365 の接続は調整されることがあるため、調整時に接続性テストが失敗したように見えることがあります。Citrix Endpoint Management コネクタ: Exchange ActiveSync 用では、接続の開始を最大 3 回試行するようになりました。[CXM-58180]
- Exchange でポリシーを有効にするには、Citrix Endpoint Management コネクタ: Exchange ActiveSync 用が **Set-CASMailbox** コマンドを実行して、各メールボックスですべての関連デバイスを次の 2 つの一覧に

登録する必要があります: 許可およびブロック。デバイスがどちらの一覧にも含まれていない場合、Exchange はデフォルトのアクセス状態にフォールバックします。このデフォルトのアクセス状態がデバイスの必要な状態とは異なる場合、デバイスはコンプライアンス違反になります。したがって、許可が必要な Exchange のデフォルトのアクセス状態がブロックである場合、ユーザーはメールにアクセスできなくなる可能性があります。または、メールへのアクセスをブロックする必要があるユーザーにアクセス権が付与される場合もあります。Citrix Endpoint Management コネクタ: Exchange ActiveSync 用によって、必要な状態を有効にしたすべてのデバイスが各 **Set-CasMailbox** コマンドに含まれるようになりました。[CXM-61251]

バージョン 10.1.8 では、次の既知の問題が確認されています。

サービスがスナップショットやポリシー評価のような長期間の操作を実行しているときに構成データを変更する構成アプリケーションで管理者が変更を加えると、サービスが不確定の状態になることがあります。その結果、ポリシーの変更が処理されない、またはスナップショットが開始されないなどの現象が発生することがあります。サービスを稼働状態に戻すには、サービスを再起動する必要があります。サービスを開始する前に、Windows サービスマネージャーでサービスプロセスの終了が必要な場合があります。[CXM-61330]

バージョン **10.1.7** の新機能

- XenMobile Mail Manager は「Endpoint Management コネクタ: Exchange ActiveSync 用」になりました。
- [Exchange の構成] ダイアログボックスの [パイプライン処理を無効にする] オプションは廃止されました。同じ機能を実現するには、config.xml ファイルの各コマンドに複数の手順を設定します。[CXM-54593]

バージョン 10.1.7 では、次の問題が解決されています。

- [スナップショット履歴] ウィンドウでは、エラーメッセージにコンテキストがほとんど表示されないことがあります。エラーメッセージに、発生した場所のコンテキストが接頭辞に付くようになりました。[CXM-49157]
- XmmGoogleAnalytics .dll には、リリースに対応するファイルバージョンがありませんでした。[CXM-52518]
- 診断を改善するために、最近、メールボックスの許可/ブロック状態を設定するために使用するデバイス ID のリストの文字列形式を変更しました。ただし、デバイスが多すぎたため、仕様が最大文字列サイズを超えました。そのため内部配列データ構造を採用しました。この構造にサイズの制限はなく、データを診断の目的に適した形式にフォーマットします。[CXM-52610]
- Exchange に同期されていないデバイスポリシーが検出された場合、このデバイスポリシーのコマンドの対象には、関連するメールボックスに属していないデバイスが含まれる可能性がありました。「Endpoint Management コネクタ: Exchange ActiveSync 用」では、Exchange へのコマンドが各メールボックスに属するデバイスのみを対象とするようになりました。[CXM-54842]
- 一部の環境では、Microsoft アセンブリは使用できません。必要なアセンブリがアプリケーションとともに明示的にインストールされるようになりました。[CXM-55439]
- デバイスまたはメールボックスの識別名で、属性名と等号の間にスペース、または等号の後にスペースが含まれている場合、「Endpoint Management コネクタ: Exchange ActiveSync 用」がデバイスをそのメール

ボックスに（またはその逆）正しく一致させないことがあります。その結果、スナップショットの調停時に一部のデバイスやメールボックスが拒否される可能性があります。[CXM-56088]

> 注:
>
> 以下のセクションでは、「Endpoint Management コネクタ: Exchange ActiveSync 用」を旧称の XenMobile Mail Manager で呼びます。名前はバージョン 10.1.7 から変更されました。

バージョン **10.1.6.20** の更新点

10.1.6 に対する更新プログラムには、10.1.6.20 で追加された以下の修正が含まれています:

- Exchange に同期されていないデバイスポリシーが検出された場合、このデバイスポリシーのコマンドの対象には、関連するメールボックスに属していないデバイスが含まれる可能性がありました。XenMobile Mail Manager では、Exchange へのコマンドで各メールボックスに属するデバイスのみを対象とするようになりました。[CXM-54842]

バージョン **10.1.6** の新機能

XenMobile Mail Manager バージョン 10.1.6 では、次の問題の修正と機能の強化が行われました。

- [スナップショット履歴] ウィンドウが時々更新されなくなることがありました。このウィンドウの更新メカニズムが改善され、更新がより確実に行われるようになりました。[CXM-47983]
- パーティション化済みのスナップショットとパーティション化されていないスナップショットに、別々のモードおよびコードパスが使用されていました。パーティション化されていないスナップショットは、単一の「*」パーティションを用いた構成でパーティション化したスナップショットと同じであったため、パーティション化なしのスナップショットモードは削除されました。デフォルトのスナップショットモードは、36 個のパーティション（0 ～ 9、A ～ Z）でパーティション化されたスナップショットになりました。[CXM-49093]
- [スナップショット履歴] ウィンドウで、エラーメッセージが状態メッセージにより上書きされていました。このバージョンより、状態とエラーを同時に確認できるよう、XenMobile Mail Manager に 2 つの別々のフィールドが表示されるようになりました。[CXM-51942]
- Exchange Online（Office 365）に接続するときに、スナップショット関連のクエリによってデータセットの切り捨てが行われることがありました。この問題は、XenMobile Mail Manager で複数のコマンドをパイプラインでつないだスクリプトを実行すると発生していました。上流のコマンドから下流のコマンドへデータを渡す速度が十分ではなかったため、作業が途中で終了し、結果としてデータが不完全になっていました。このバージョンより、XenMobile Mail Manager でパイプラインそのものを再現できるようになったため、上流のコマンドが完了するまで待機してから、下流のコマンドが呼び出されるようになりました。この変更により、すべてのデータが処理され、記録されるようになります。[CXM-52280]
- Exchange に対するポリシー更新コマンドで解決不能なエラーが発生した場合、そのコマンドが長時間にわたって繰り返し作業キューへ返されていました。このため、Exchange に何度も同じコマンドが送信されていました。このバージョンの XenMobile Mail Manager では、エラーが生じたコマンドは、限られた回数だけ作業キューへ返されるようになりました。[CXM-52633]

- 特定のメールボックスのポリシー更新で全デバイスの許可またはブロックを行った場合：空のリストが **NULL** ではなく空の文字列に変換されていたため、発行した **Set-CASMailbox** コマンドが失敗していました。このバージョンより、適切なデータが送信されるようになりました。[CXM-53759]
- 新しいデバイスを処理する場合、Exchange では一定時間（通常 15 分）にわたり、「DeviceDiscovery」という状態が返されることがあります。XenMobile Mail Manager では、この状態を特に処理していませんでした。このバージョンより、XenMobile Mail Manager は、この状態を処理するようになりました。UI の［モニター］タブで、この状態にあるデバイスをフィルターできるようになりました。[CXM-53840]
- XenMobile Mail Manager では、XenMobile Mail Manager データベースへの書き込みが可能かどうかのチェックを行っていませんでした。そのため、権限に制限があると、動作を予測できていませんでした。このバージョンより、XenMobile Mail Manager は、データベースで必要な権限を取得、検証するようになりました。XenMobile Mail Manager で、接続のテスト中（表示メッセージ）、またはメインの［構成］ウィンドウ下部のデータベースインジケーター（マウスカーソルを重ねるとメッセージを表示）に、権限が足りないことが示されるようになりました。[CXM-54219]
- 実行中のワークロードによっては、XenMobile Mail Manager サービスに命令を出してもすぐに止まらないことがありました。このため、サービスは応答なし状態のようになっていました。改善により実施中のタスクを中断できるようになり、シャットダウンが正常に行われるようになりました。[CXM-54282]

バージョン **10.1.5** の新機能

XenMobile Mail Manager バージョン 10.1.5 では、次の問題が修正されています。

- Exchange が XenMobile Mail Manager のアクティビティを制限している場合でも、制限が行われていることがログ以外に示されていませんでした。このリリースでは、アクティブなスナップショットにマウスカーソルを重ねると、「制限中」状態が表示されるようになりました。また、XenMobile Mail Manager が制限を受けている場合、Exchange で制限が解除されるまでメジャースナップショットを開始できなくなりました。[CXM-49617]
- メジャースナップショット中に Exchange により XenMobile Mail Manager が制限されている場合：十分な時間が経過する前に、次のスナップショットが試行されることがありました。この問題により、さらに制限が行われ、スナップショットは失敗していました。このバージョンより、XenMobile Mail Manager は、各スナップショット試行の間に Exchange で指定された最小時間だけ待機するようになりました。[CXM-49618]
- 診断を有効にすると、コマンドファイルに、各プロパティ名の前にハイフンがついていない **Set-CasMailbox** コマンドが表示されていました。この問題は診断ファイルの書式内でのみ発生し、Exchange への実際のコマンドでは発生しません。ハイフンが不足しているため、コマンドを切り取って直接 PowerShell プロンプトに貼り付けて、テストや検証を行うことができませんでした。このバージョンより、ハイフンが追加されました。[CXM-52520]
- メールボックス ID の形式が「姓, 名」の場合、Exchange では、クエリのデータを返すときにコンマの前にバックスラッシュが追加されます。XenMobile Mail Manager でこの ID を使用してさらにデータのクエリを行う場合、このバックスラッシュは削除する必要があります。[CXM-52635]

既知の制限事項

> 注：
>
> バージョン 10.1.6 では次の制限が解決されています。

XenMobile Mail Manager には、Exchange に対するコマンドの失敗の原因となる可能性がある既知の問題が存在しています。ポリシーの変更を Exchange に適用する場合、XenMobile Mail Manager により **Set_CASMailbox** コマンドが発行されます。このコマンドでは、許可リストと禁止リストの 2 つのデバイスリストを取ることができます。コマンドは、メールボックスのパートナーに設定されているデバイスに適用されます。

これらの各リストの文字数は、Microsoft の API により 256 文字までに制限されています。どちらかのリストの文字数がこの制限を超えると、コマンド全体が失敗し、指定したメールボックスのデバイスにはいずれのポリシーも設定されません。エラーは次のような形で、XenMobile Mail Manager ログに表示されます。禁止リストの場合の例を次に示します。

“メッセージ：‘パラメーター ‘ActiveSyncBlockedDeviceIDs’ をターゲットにバインドできません。例外設定 “ActiveSyncBlockedDeviceIDs”：” プロパティが長すぎます。文字数の上限は 256 文字であり、指定された値の長さは…”

デバイス ID の長さはさまざまですが、通常 10 台以上のデバイスを一度に許可または禁止しようとするとこの制限を超える可能性があります。あまり行われませんが、多数のデバイスを特定のメールボックスに関連付けることは可能です。XenMobile Mail Manager が改善されこのようなシナリオに対処できるようになるまでは、ユーザーおよびメールボックスに関連付けるデバイスの数は 10 台以下に制限することをお勧めします。[CXM-52633]

バージョン **10.1.4** の新機能

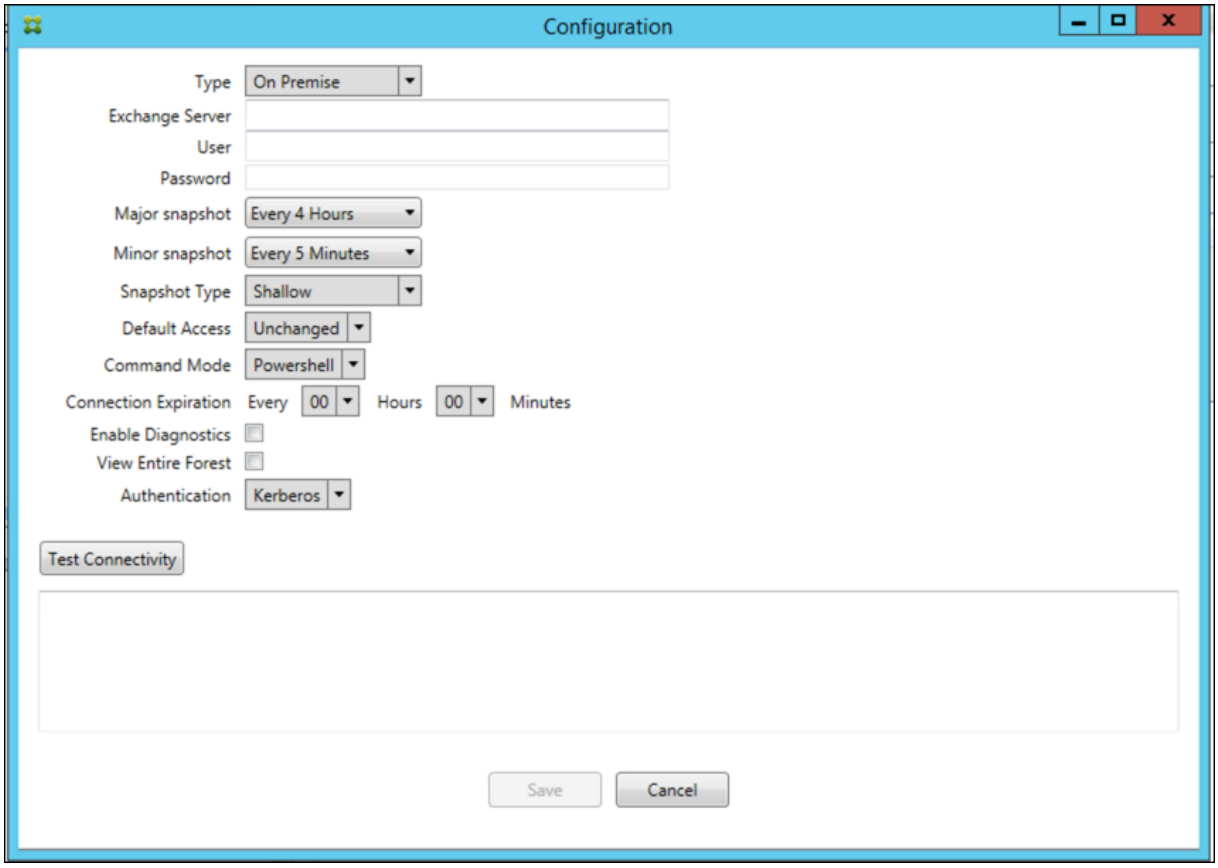
XenMobile Mail Manager バージョン 10.1.4 では、次の問題が修正されています。

- セキュリティの弱化のため、TLS 1.0 は PCI 評議会の推奨でなくなりました。XenMobile Mail Manager に TLS 1.1 および 1.2 のサポートが追加されました。[CXM-38573、CXM-32560]
- XenMobile Mail Manager に新しい診断ファイルが追加されました。Exchange の仕様で ［診断を有効にする］ を選択すると、新しいスナップショット履歴ファイルが生成されます。スナップショットを試行するたびに、スナップショットの結果を含む行がファイルに追加されます。[CXM-49631]
- コマンド診断ファイルで、**Set-CASMailbox** コマンドで許可された、またはブロックされたデバイスの一覧が表示されませんでした。代わりに、関連する引数のファイルに内部クラス名が表示されていました。XenMobile Mail Manager で、deviceID の一覧がコンマ区切り一覧として表示されるようになりました。[CXM-50693]
- 不適切な仕様のために Exchange への接続の確立が失敗した場合：エラーメッセージが、「すべての接続が使用中です」という不適切なメッセージで上書きされます。「すべての接続が動作不能」、「接続プールが空です」、「すべての接続が抑制されている」、「使用可能な接続がありません」などのよりわかりやすいメッセージが表示されるようになりました。[CXM-50783]
- 一部のケースで、XenMobile Mail Manager の内部キャッシュに、Allow、Block、または Wipe コマンドが複数回キューイングされることがあります。この問題により、Exchange に送信されるコマンドの遅延が発

生します。XenMobile Mail Manager は、各コマンドで 1 つのインスタンスのみをキューイングするようになりました。[CXM-51524]

バージョン **10.1.3** の新機能

- **Google Analytics** のサポート: 製品の改善可能な箇所に集中できるように、私たちはユーザーの皆様が XenMobile Mail Manager をどのように使用しているかについて知りたいと考えています。
- 診断を有効にするための設定: ［診断を有効にする］ チェックボックスが、［設定］ ダイアログボックスの設定コンソールに表示されます。



Version 10.1.3 で解決された問題

- ［スナップショット履歴］ ウィンドウで、スナップショットの現在の状態を示すツールチップに実際の状態が反映されません。[CXM-5570]
  XenMobile Mail Manager がコマンド診断ファイルに書き込めないことがありました。これが発生すると、コマンド履歴全体が記録されません。[CXM-49217]
- 接続でエラーが発生した場合に、接続が「エラー」とマークされないことがあります。その結果、後続のコマンドが接続を使用しようとして、別のエラーを引き起こす可能性があります。[CXM-49495]

- Exchange Server からの調整が発生すると、ヘルスチェックルーチンで例外がスローされる場合があります。その結果、エラーが発生した、または期限切れになった接続が削除されないことがあります。また、XenMobile Mail Manager は調整時間の期限が切れるまで接続を作成しないことがあります。[CXM-49794]。
- Exchange の最大セッション数を超えた場合に XenMobile Mail Manager から「デバイスのキャプチャに失敗した」というエラーが報告されますが、このメッセージは正確でありません。このメッセージではなく、XenMobile Mail Manager が通常 Exchange 通信に使用する 2 つのセッションが使用中であることを示すメッセージを表示する必要があります。[CXM-49994]

バージョン **10.1.2** の新機能

- **Exchange** との接続の改善：XenMobile Mail Manager は PowerShell セッションを使用して Exchange と通信します。PowerShell セッション（特に Office 365 を扱う場合）は、しばらくすると不安定になり、その後のコマンドが正常に機能しなくなる可能性があります。XenMobile Mail Manager で接続の有効期限を設定できるようになりました。接続が有効期限に達すると、XenMobile Mail Manager は PowerShell セッションを即時シャットダウンしてセッションを作成します。これにより、PowerShell セッションが不安定になる可能性が低くなり、スナップショットの失敗の可能性が大幅に減少します。
- スナップショットのワークフローの改善： 大半のスナップショットは、プロセスを集中的に使用する時間のかかる操作です。スナップショット中にエラーが発生した場合に、XenMobile Mail Manager がスナップショットの完了を複数回（最大 3 回）試行するようになりました。その後の試行では最初からは開始されません。中断した場所から続行します。この機能拡張により、スナップショットの進行中に一時的なエラーが発生するのを許容することで、スナップショットの成功率が向上します。
- 診断の改善： スナップショット中に 3 つの新しい診断ファイルが生成されるようになり（オプション）、スナップショット操作のトラブルシューティングが簡単になりました。これらのファイルは、PowerShell コマンドの問題、情報が欠落しているメールボックス、およびメールボックスに関連付けできないデバイスを識別するのに役立ちます。管理者はこれらのファイルを使用して、Exchange 内の不適切なデータを識別できます。
- メモリ使用率の向上：XenMobile Mail Manager のメモリ使用効率が向上しました。管理者は、XenMobile Mail Manager を自動的に再起動し、システムにクリーンスレートが提供されるようにスケジュールできます。
- **Microsoft .NET Framework 4.6** の前提条件： Microsoft .NET Framework の前提条件がバージョン 4.6 になりました。

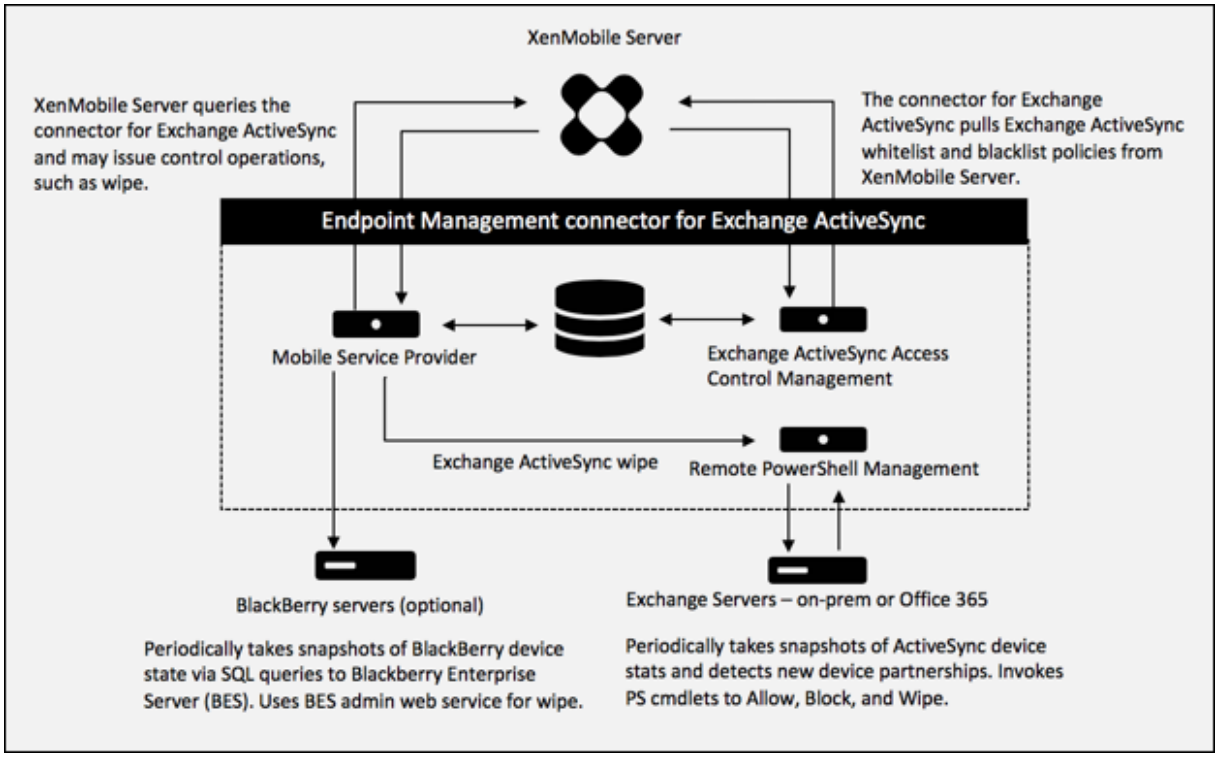
解決された問題

- 資格情報の要求エラー：Office 365 のセッションが不安定なために、このエラーが発生することがよくありました。Exchange への接続を改善する機能強化により、この問題に対応しています。（XMHELP-293、XMHELP-311、XMHELP-801）
- メールボックスとデバイスの数が不正確：XenMobile Mail Manager で、メールボックスとデバイスの関連付けアルゴリズムが改善されました。診断機能の改善により、XenMobile Mail Manager が責任範囲外と判断したメールボックスとデバイスを識別できるようになりました。(XMHELP-623)

- Allow、Block、Wipe コマンドが認識されない：XenMobile Mail Manager の Allow、Block、Wipe コマンドが認識されないことがあるバグが修正されました。(XMHELP-489)
- メモリ管理：メモリ管理とメモリ緩和が改善されました。(XMHELP-419)

アーキテクチャ

次の図は「Endpoint Management コネクタ：Exchange ActiveSync 用」の主要コンポーネントを示しています。詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。



次の 3 つの主要コンポーネントがあります：

- **Exchange ActiveSync** アクセス制御管理： XenMobile と通信して、XenMobile から Exchange ActiveSync ポリシーを取得します。さらに、このポリシーをローカルに定義されているポリシーと統合して、Exchange へのアクセスを許可または拒否する Exchange ActiveSync デバイスを決定します。ローカルポリシーにより、Active Directory のグループ、ユーザー、デバイスの種類、またはデバイスのユーザーエージェント（一般的にはモバイルプラットフォームのバージョン）によってアクセス制御できるように、ポリシー規則を拡張できます。
- リモート **PowerShell** 管理： リモートの PowerShell コマンドのスケジュール設定と呼び出しを処理して、Exchange ActiveSync アクセス制御管理によって作成されたポリシーを有効にします。定期的に Exchange ActiveSync データベースのスナップショットを取得し、新規の、または変更された Exchange ActiveSync デバイスを検出します。
- モバイルサービスプロバイダー： XenMobile で Exchange ActiveSync デバイスや BlackBerry デバイスに対してクエリを実行したり、Wipe などの制御操作を発行したりできるように、Web サービスインターフェ

イスを提供します。

システム要件および前提条件

Endpoint Management コネクタ: Exchange ActiveSync 用を使用するには、次の最小システム要件が必要です:

- Windows Server 2016、Windows Server 2012 R2 または Windows Server 2008 R2 Service Pack 1。英語ベースのサーバーが必要です。Windows Server 2008 R2 Service Pack 1 のサポートは、2020 年 1 月 14 日に終了します。
- Microsoft SQL Server 2016 Service Pack 2、SQL Server 2014 Service Pack 3 または SQL Server 2012 Service Pack 4。
- Microsoft .NET Framework 4.6。
- Blackberry Enterprise Service バージョン 5（オプション）。

Microsoft Exchange Server のサポートされる最小バージョン:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3（サポートは 2020 年 1 月 14 日に終了します）

前提条件

- Windows Management Framework がインストールされていること。
  - PowerShell V5、V4、V3
- PowerShell 実行ポリシーが Set-ExecutionPolicy RemoteSigned によって RemoteSigned に設定されていること。
- Endpoint Management コネクタ: Exchange ActiveSync 用を実行しているコンピューターとリモートの Exchange Server の間で、TCP ポート 80 が開いていること。
- デバイスのメールクライアント: すべてのメールクライアントが、デバイスに関して一貫して同じ ActiveSync ID を返すわけではありません。Endpoint Management コネクタ: Exchange ActiveSync 用は、各デバイスに対して一意の ActiveSync ID を前提とするため、デバイスごとに一意の同じ ActiveSync ID を一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントはテスト済みで、エラーなく実行できます:
  - HTC のネイティブメールクライアント
  - Samsung のネイティブメールクライアント
  - iOS のネイティブメールクライアント
  - TouchDown for Smartphones

- **Exchange**: Exchange を実行しているオンプレミスコンピューターの要件は以下のとおりです:

  Exchange の構成 UI で指定される資格情報を使用して Exchange Server に接続でき、次の Exchange 固有の PowerShell コマンドレットを実行するためのフルアクセスが付与される必要があります。

  - **Exchange Server 2010 SP2** の場合:
    * Get-CASMailbox
    * Set-CASMailbox
    * Get-Mailbox
    * Get-ActiveSyncDevice
    * Get-ActiveSyncDeviceStatistics
    * Clear-ActiveSyncDevice
    * Get-ExchangeServer
    * Get-ManagementRole
    * Get-ManagementRoleAssignment
  - **Exchange Server 2013** および **Exchange Server 2016** の場合:
    * Get-CASMailbox
    * Set-CASMailbox
    * Get-Mailbox
    * Get MobileDevice
    * Get MobileDeviceStatistics
    * Clear-MobileDevice
    * Get-ExchangeServer
    * Get-ManagementRole
    * Get-ManagementRoleAssignment
  - Endpoint Management コネクタ: Exchange ActiveSync 用がフォレスト全体を表示するように構成されている場合は、**Set-AdServerSettings -ViewEntireForest $true** を実行するための権限が付与されている必要があります。
  - 指定された資格情報には、リモートシェルを介して、Exchange Server に接続する権限が与えられている必要があります。デフォルトでは、Exchange をインストールしたユーザーがこの権限を持ちます。
  - Microsoft TechNet サポート技術情報「about_Remote_Requirements」によれば、リモート接続を確立してリモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。Set-PSSessionConfiguration を使用して管理要件を排除できますが、このコマンドの説明はこのドキュメントの範囲外です。詳細については、ブログ記事「You Don't Have to Be An Administrator to Run Remote PowerShell Commands」を参照してください。
  - Exchange Server は、HTTP を介してリモート PowerShell 要求をサポートするように構成されている必要があります。通常、Exchange Server で次の PowerShell コマンドを実行する管理者にとって必要なのは、WinRM QuickConfig だけです。
  - Exchange には多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可される PowerShell の同時接続数が制御されます。Exchange 2010 の場合、1 人のユーザーに許可されている同時接続数のデフォルトは 18 です。接続数の上限に達すると、Endpoint Management

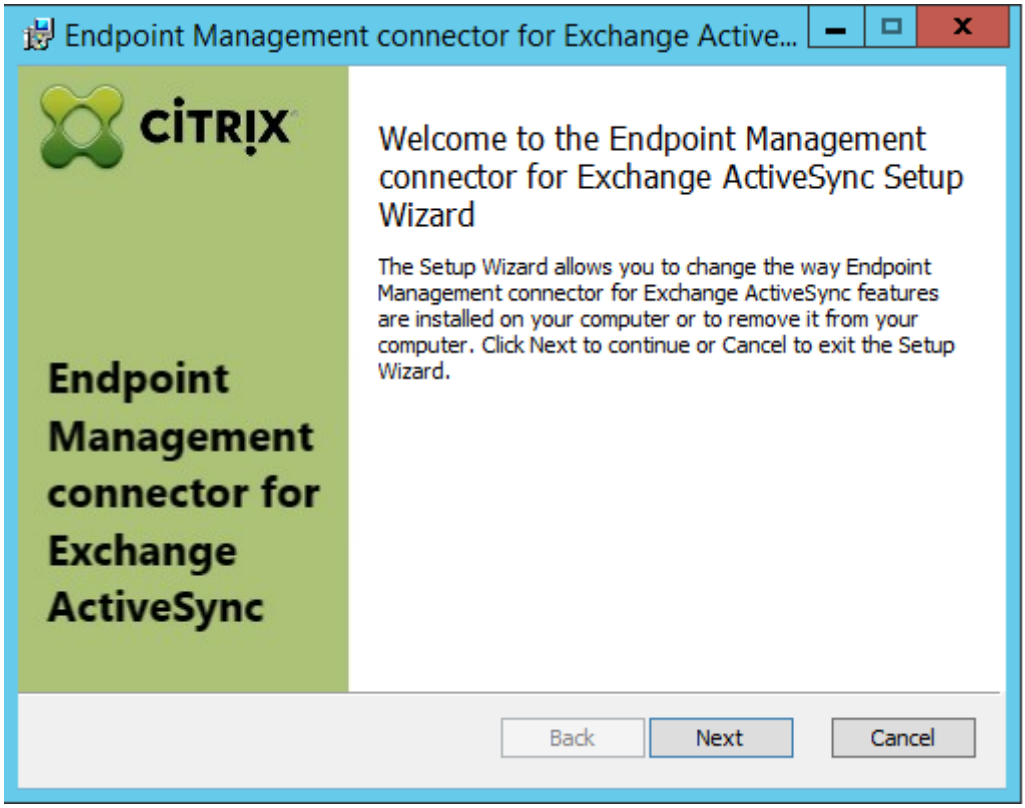
コネクタ: Exchange ActiveSync 用は Exchange Server に接続できなくなります。PowerShell の同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShell によるリモート管理に関連する、Exchange の調整ポリシーについて調べてください。

Office 365 Exchange の要件

- 権限: Exchange の構成 UI で指定される資格情報を使用して Office 365 に接続でき、次の Exchange 固有の PowerShell コマンドレットを実行するためのフルアクセスが付与される必要があります:
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get MobileDevice
  - Get MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 特権: 指定された資格情報には、リモートシェルを介して、Office 365 サーバーに接続する権限が与えられている必要があります。デフォルトでは、Office 365 のオンライン管理者には、必要な権限が備えられています。
- 調整ポリシー: Exchange には多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可される PowerShell の同時接続数が制御されます。Office 365 の場合、1 人のユーザーに許可されている同時接続数のデフォルトは 3 です。接続数の上限に達すると、Endpoint Management コネクタ: Exchange ActiveSync 用は Exchange Server に接続できなくなります。PowerShell の同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShell によるリモート管理に関連する、Exchange の調整ポリシーについて調べてください。

インストールと構成

1. XmmSetup.msi ファイルをクリックして、インストーラーのプロンプトに従い、Endpoint Management コネクタ: Exchange ActiveSync 用をインストールします。
2. セットアップウィザードの最後の画面で、［構成ユーティリティの起動］ をオンのままにしておきます。または、［スタート］ メニューから、Endpoint Management コネクタ: Exchange ActiveSync 用を開きます。



3. 次のデータベースプロパティを構成します:

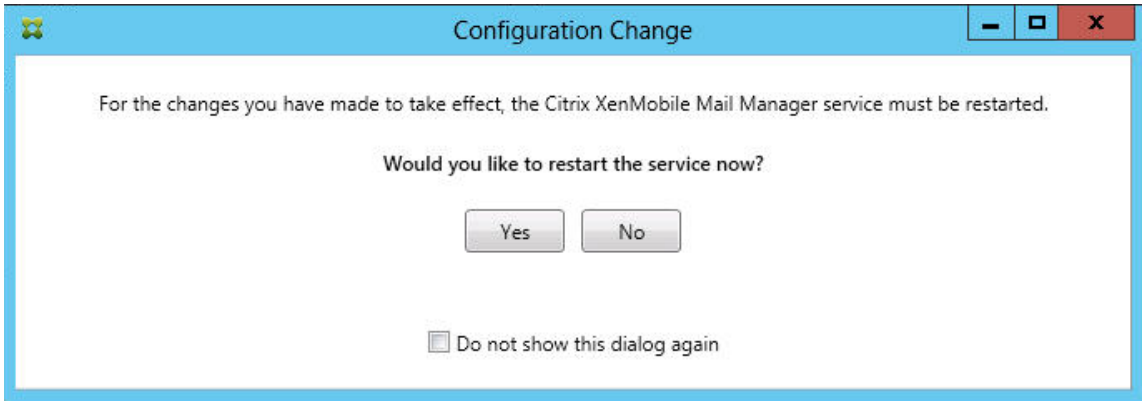
   - [**Configure**] > [**Database**] タブをクリックします。
   - SQL Server の名前（デフォルトは localhost）を入力します。
   - データベースはデフォルトの **CitrixXmm** のままにします。

4. SQL に使用される次のいずれかの認証モードを選択します:

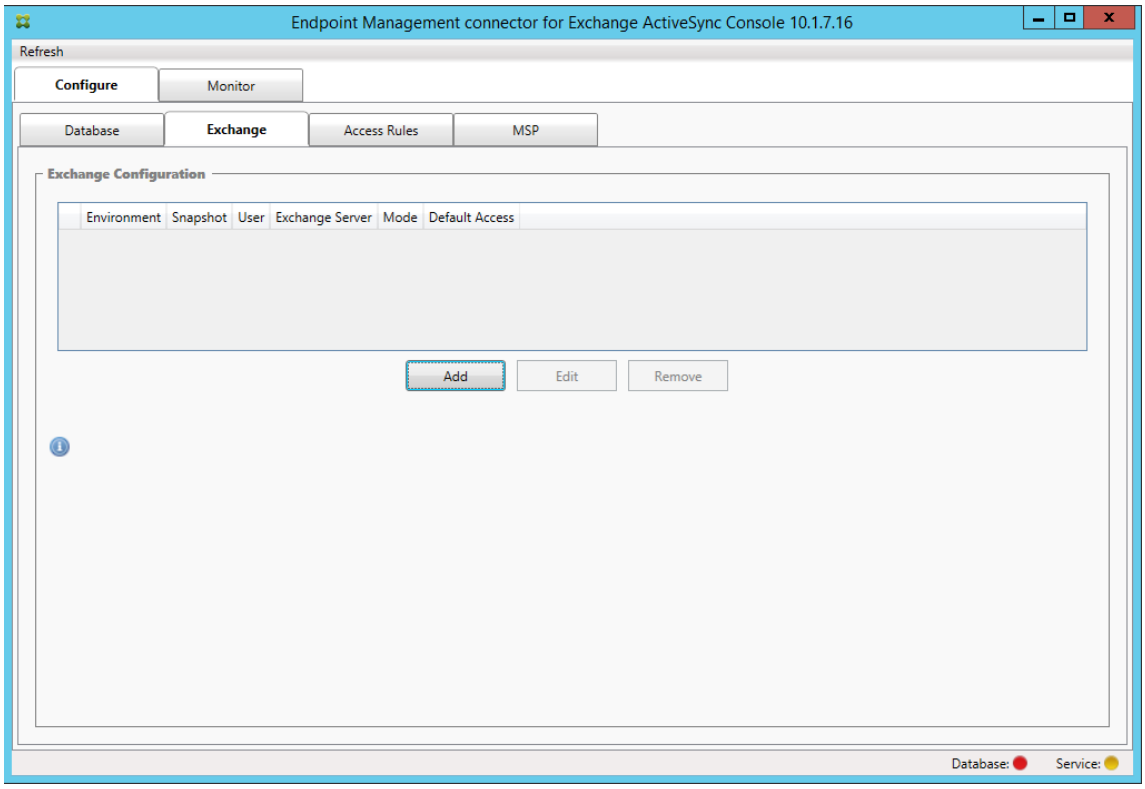
   - **SQL**: 有効な SQL ユーザーのユーザー名とパスワードを入力します。
   - **Windows** 統合: このオプションを選択した場合、Endpoint Management コネクタ: Exchange ActiveSync 用サービスのログオン資格情報を、SQL Server にアクセスするための権限を持つ Windows アカウントに変更する必要があります。これを行うには、[コントロールパネル]、[管理ツール]、[サービス] の順に選択し、Endpoint Management コネクタ: Exchange ActiveSync 用サービスエントリを右クリックし、[ログオン] タブをクリックします。

   BlackBerry データベース接続に対しても「Windows 統合」を選択している場合は、ここで指定されている Windows アカウントに BlackBerry データベースへのアクセスも付与する必要があります。

5. [接続性をテスト] をクリックして SQL Server に接続できることを確認し、[保存] をクリックします。
6. サービスの再起動を求めるメッセージが表示されます。[はい] をクリックします。



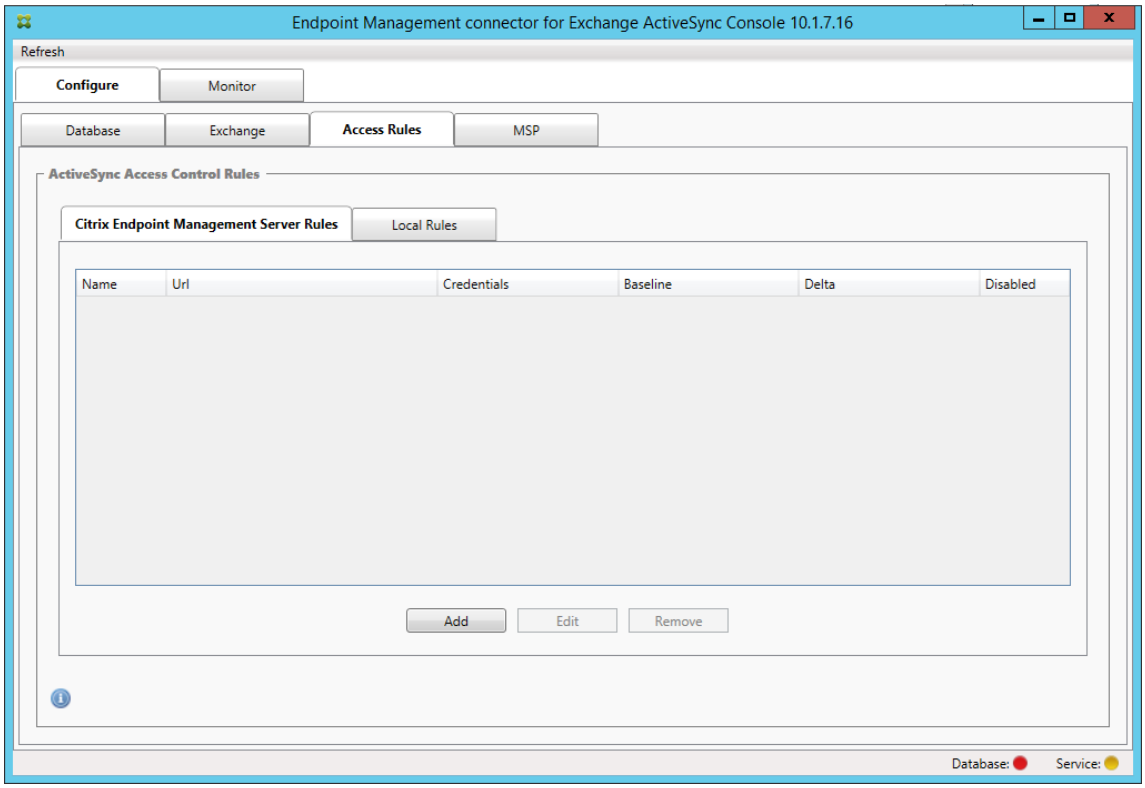
7. 1 つまたは複数の Exchange Server を構成します。
   - 単一の Exchange 環境を管理している場合は、サーバーを 1 つのみ指定します。複数の Exchange 環境を管理している場合は、Exchange 環境ごとに 1 つの Exchange Server を指定する必要があります。
   - [**Configure**] > [**Exchange**] タブをクリックし、 [**Add**] をクリックします。



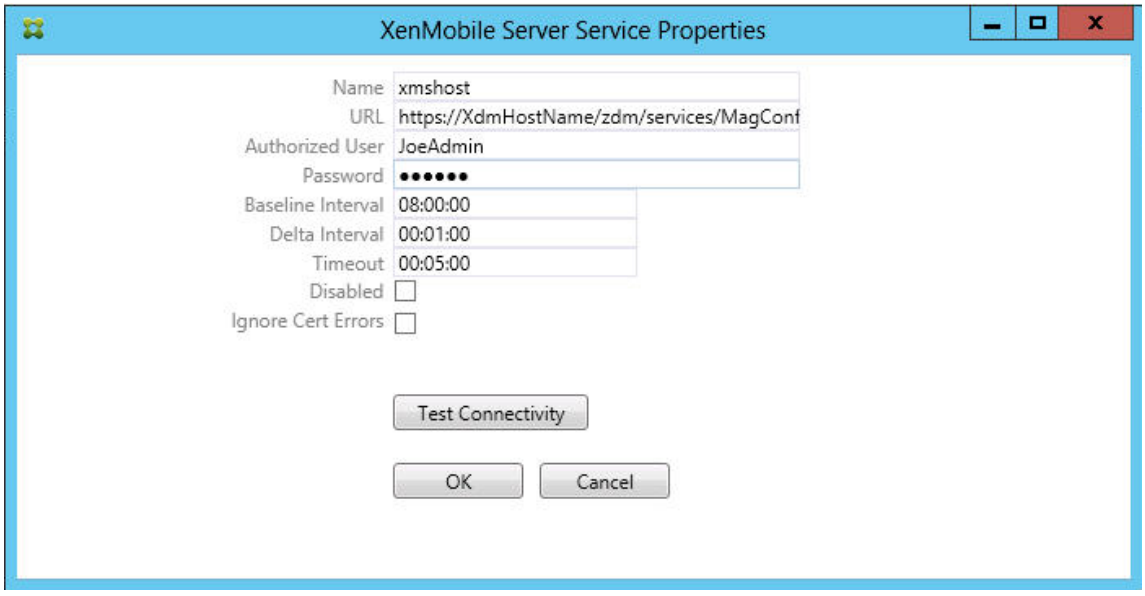
8. Exchange Server 環境の種類として [**On Premise**] または [**Office 365**] を選択します。
   - [**On Premise**] を選択した場合は、リモート PowerShell コマンドで使用する Exchange Server の名前を入力します。
   - 要件セクションに指定された、Exchange Server に対する適切な権限を持つ Windows ID のユーザー名を入力し、その後そのユーザーのパスワードを入力します。
   - メジャースナップショットを実行するスケジュールを選択します。メジャースナップショットにより、

すべての Exchange ActiveSync パートナーシップが検出されます。
- マイナースナップショットを実行するスケジュールを選択します。マイナースナップショットにより、新しく作成された Exchange ActiveSync パートナーシップが検出されます。
- スナップショットの種類として、[**Deep**] または [**Shallow**] を選択します。通常、簡易スナップショットははるかに高速で、Endpoint Management コネクタ: Exchange ActiveSync 用の Exchange ActiveSync アクセス制御機能をすべて実行するには十分です。詳細スナップショットは、処理にかかる時間が長くなることがあり、モバイルサービスプロバイダーが ActiveSync に対して有効にされている場合にのみ必要です。このオプションを使用すると、XenMobile は非管理デバイスを照会できます。
- [Default Access] で、[**Allow**]、[**Block**]、または [**Unchanged**] を選択します。この設定により、明示的な XenMobile またはローカル規則で特定されたものを除くすべてのデバイスの処理方法が制御されます。[**Allow**] を選択すると、そのようなすべてのデバイスへの ActiveSync アクセスが許可されます。[**Block**] を選択すると、アクセスは拒否されます。[**Unchanged**] を選択すると、変更は行われません。
- [ActiveSync Command Mode] で、[**PowerShell**] または [**Simulation**] を選択します。
- [**PowerShell**] モードでは、Endpoint Management コネクタ: Exchange ActiveSync 用は PowerShell コマンドを発行し、必要なアクセス制御を有効にします。[Simulation] モードでは、Endpoint Management コネクタ: Exchange ActiveSync 用は PowerShell コマンドを発行しませんが、想定しているコマンドと結果をデータベースに記録します。[Simulation] モードでは、PowerShell モードを有効にした場合の結果を [**Monitor**] タブを使って確認できます。
- [**Connection Expiration**] で、接続の有効期間を分単位で設定します。接続が指定された経過時間に達すると、その接続は期限切れとマークされ、接続が再度使用されることはありません。期限切れの接続が使用されなくなると、Endpoint Management コネクタ: Exchange ActiveSync 用は接続を即時シャットダウンします。再接続が必要な場合は、使用可能なものがなければ、新しい接続が初期化されます。何も指定しないと、デフォルトの 30 分が使用されます。
- Exchange 環境で Active Directory フォレスト全体を表示するように Endpoint Management コネクタ: Exchange ActiveSync 用を構成するには、[**View Entire Forest**] を選択します。
- 認証プロトコルとして [**Kerberos**] または [**Basic**] を選択します。Endpoint Management コネクタ: Exchange ActiveSync 用は、オンプレミス展開の基本認証をサポートします。これにより、Endpoint Management コネクタ: Exchange ActiveSync 用サーバーが Exchange Server が存在するドメインのメンバーでなくても、使用できるようになります。
- [**Test Connectivity**] をクリックして SQL Server に接続できることを確認し、[**Save**] をクリックします。
- サービスの再起動を求めるメッセージが表示されます。[はい] をクリックします。

9. アクセス規則を構成します: [**Configure**] **>** [**Access Rules**] タブの順に選択し、[**XMS Rules**] タブをクリックして、[**Add**] をクリックします。



10. [**XenMobile server Service Properties**] ページで、XenMobile Server を指すように URL 文字列を変更します。たとえば、インスタンス名が **zdm** の場合は、`https://<XdmHostName>/zdm/services/MagConfigService`と入力します。この例では、**XdmHostName** を XenMobile Server の IP アドレスまたは DNS アドレスに置き換えます。



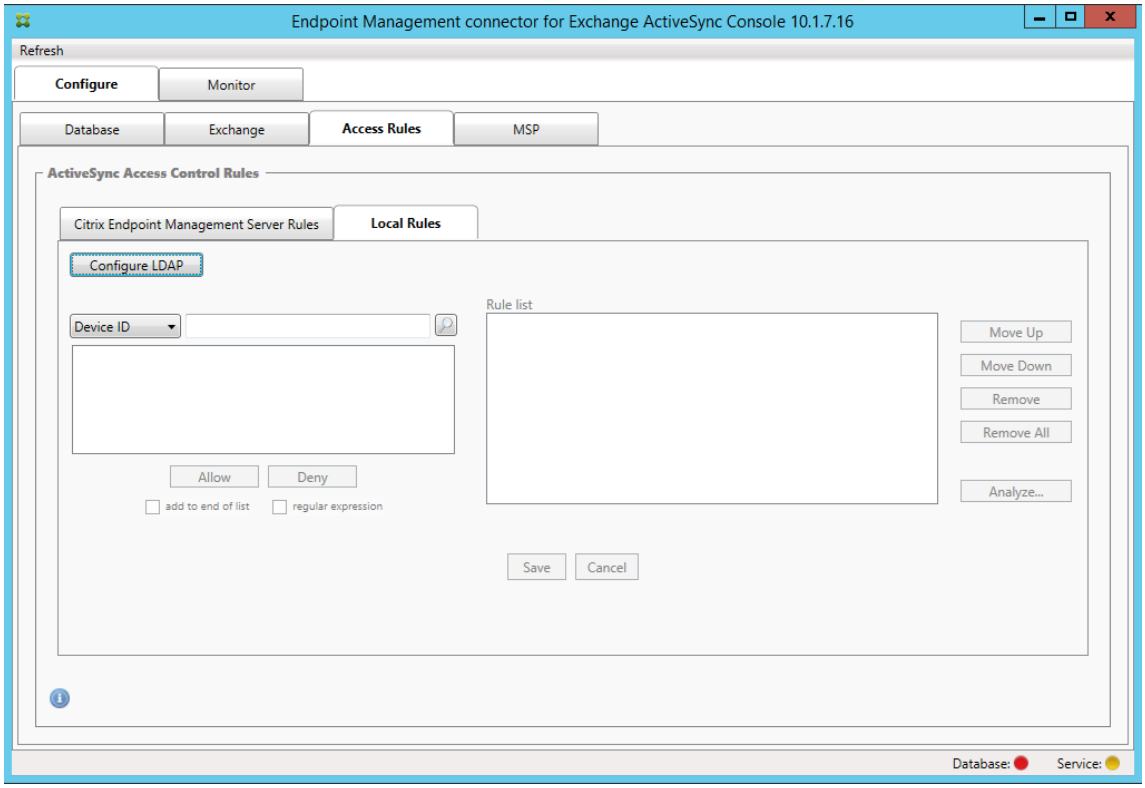
- サーバーで認証されているユーザーを入力します。
- そのユーザーのパスワードを入力します。
- [**Baseline Interval**]、[**Delta Interval**]、および [**Timeout**] の値をデフォルト値のままにし

ます。

- [**Test Connectivity**] をクリックして、サーバーへの接続を確認し、 [**OK**] をクリックします。

[**Disabled**] チェックボックスがオンの場合は、XenMobile Mail サービスで XenMobile からポリシーが収集されません。

11. [**Local Rules**] タブをクリックします。

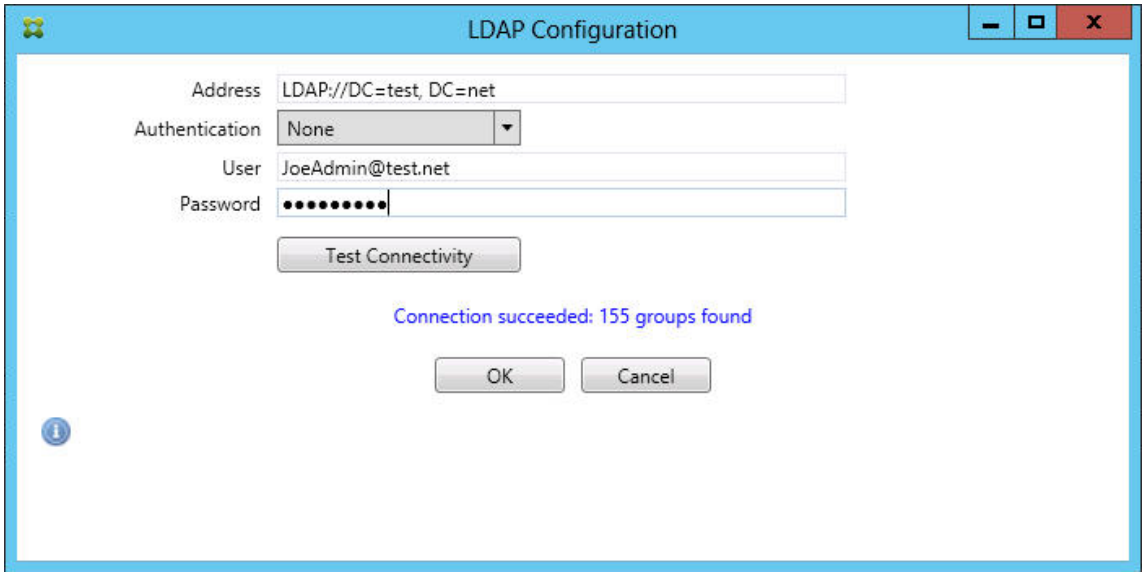


- [ActiveSync Device ID]、[Device Type]、[AD Group]、[User]、またはデバイスの [UserAgent] に基づいてローカル規則を追加できます。一覧で、適切な種類を選択します。
- テキストボックスにテキストまたはテキストフラグメントを入力します。必要に応じて、クエリボタンをクリックしてフラグメントに一致するエンティティを表示します。

[Group] 以外のすべての種類の場合、システムはスナップショットで見つかったデバイスに依存します。したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。

- テキスト値を選択し、 [**Allow**] または [**Deny**] をクリックして右側の [**Rule List**] ペインに追加します。 [**Rule List**] ペインの右側にあるボタンを使用して、規則の順序を変更したり、規則を削除したりすることができます。順序は重要です。なぜなら、指定したユーザーおよびデバイスに対して規則が表示順に評価され、上位の規則（より上部に近い規則）に一致すると以降の規則が無効になるためです。たとえば、すべての iPad デバイスを許可する規則とユーザー「Matt」をブロックする下位の規則がある場合、Matt の iPad は許可されます。この理由は、「iPad」規則の効果の優先度が「Matt」規則よりも高いからです。
- 規則一覧内の規則の分析を実行して、上書き、競合、または補足構造の可能性を検出する場合は、[**Analyze**] 、 [**Save**] の順にクリックします。

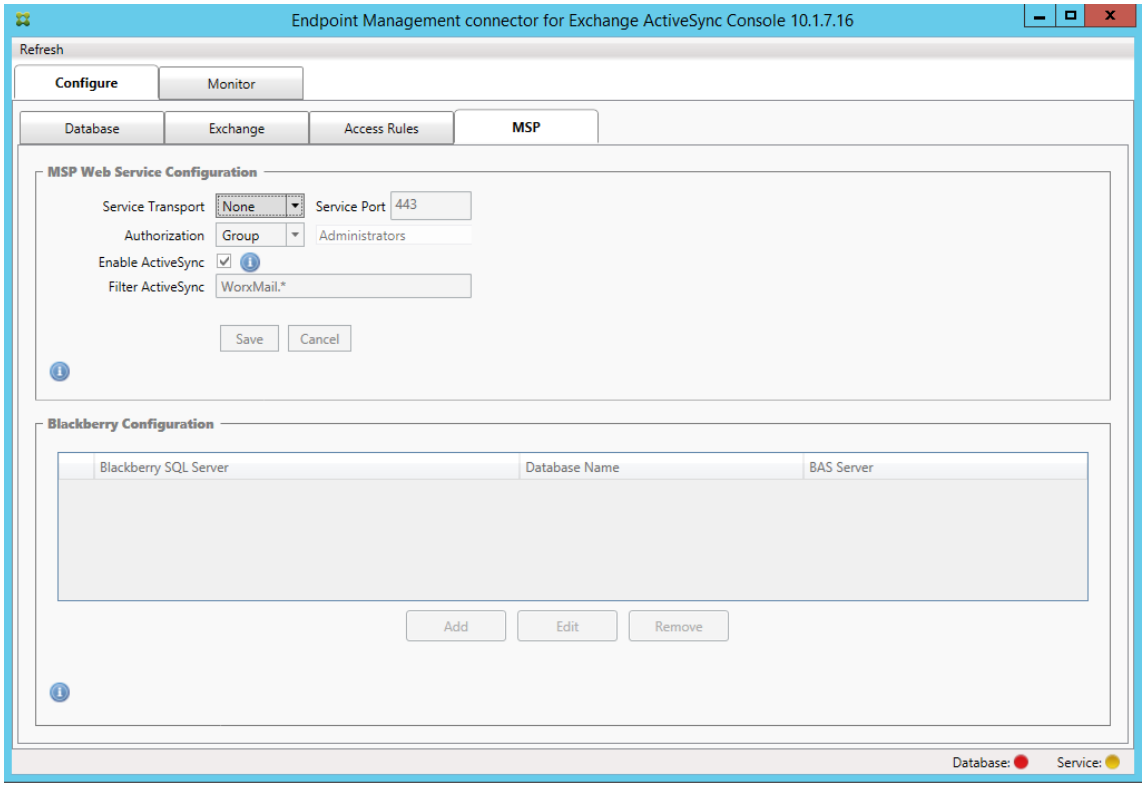
12. Active Directory のグループに対して使用するローカル規則を作成する場合は、［**Configure LDAP**］をクリックし、LDAP 接続プロパティを構成します。



13. モバイルサービスプロバイダーを構成します。

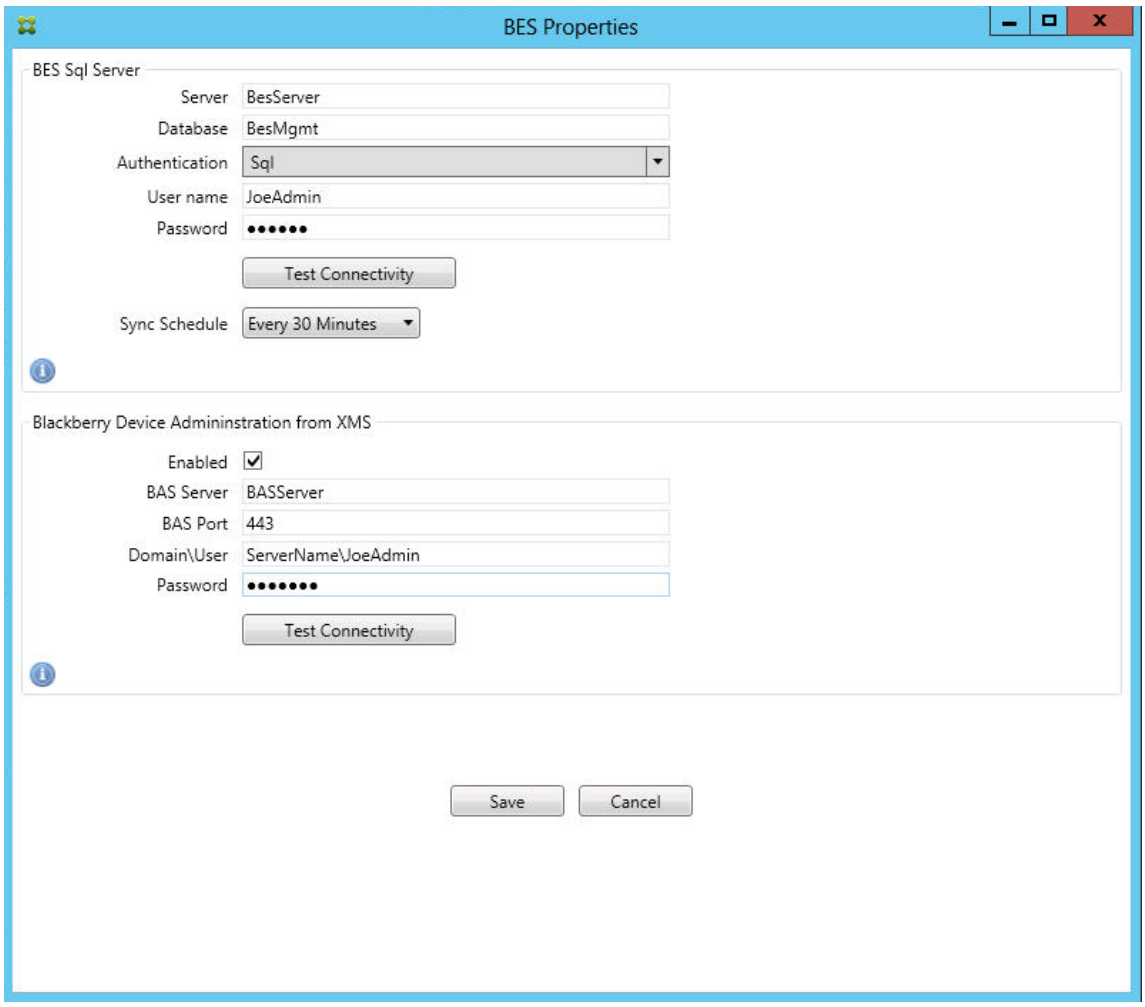
    モバイルサービスプロバイダーはオプションです。この設定は、モバイルサービスプロバイダーインターフェイスを使用して非管理対象デバイスを照会するように XenMobile が構成されている場合にのみ必要です。

    - ［**Configure**］**>** ［**MSP**］ の順にタブをクリックします。



- モバイルサービスプロバイダーサービスのサービストランスポートの種類（**HTTP** または **HTTPS**）を設定します。
- モバイルサービスプロバイダーサービスのサービスポート（通常、80 または 443）を設定します。ポート 443 を使用する場合は、IIS のこのポートにバインドされた SSL 証明書が必要です。
- ［**Authorization Group**］ または ［**User**］ を設定します。これにより、XenMobile からモバイルサービスプロバイダーサービス接続できるユーザーまたは一連のユーザーが設定されます。
- ActiveSync クエリを有効または無効に設定します。XenMobile サーバーで ActiveSync クエリが有効の場合は、Exchange Server（1 つまたは複数）のスナップショットの種類を ［**Deep**］ に設定する必要があります。この設定により、スナップショットの取得に相当なパフォーマンスコストがかかる場合があります。
- デフォルトでは、正規表現 WorxMail.* に一致する ActiveSync デバイスは、XenMobile に送信されません。この動作を変更するには、必要に応じて ［**Filter ActiveSync**］ フィールドを変更します。空白は、すべてのデバイスが XenMobile に転送されることを意味します。
- ［保存］ をクリックします。

14. 必要に応じて、BlackBerry Enterprise Server（BES）のインスタンスを 1 つ以上構成します：［**Add**］ をクリックし、BES SQL Server のサーバー名を入力します

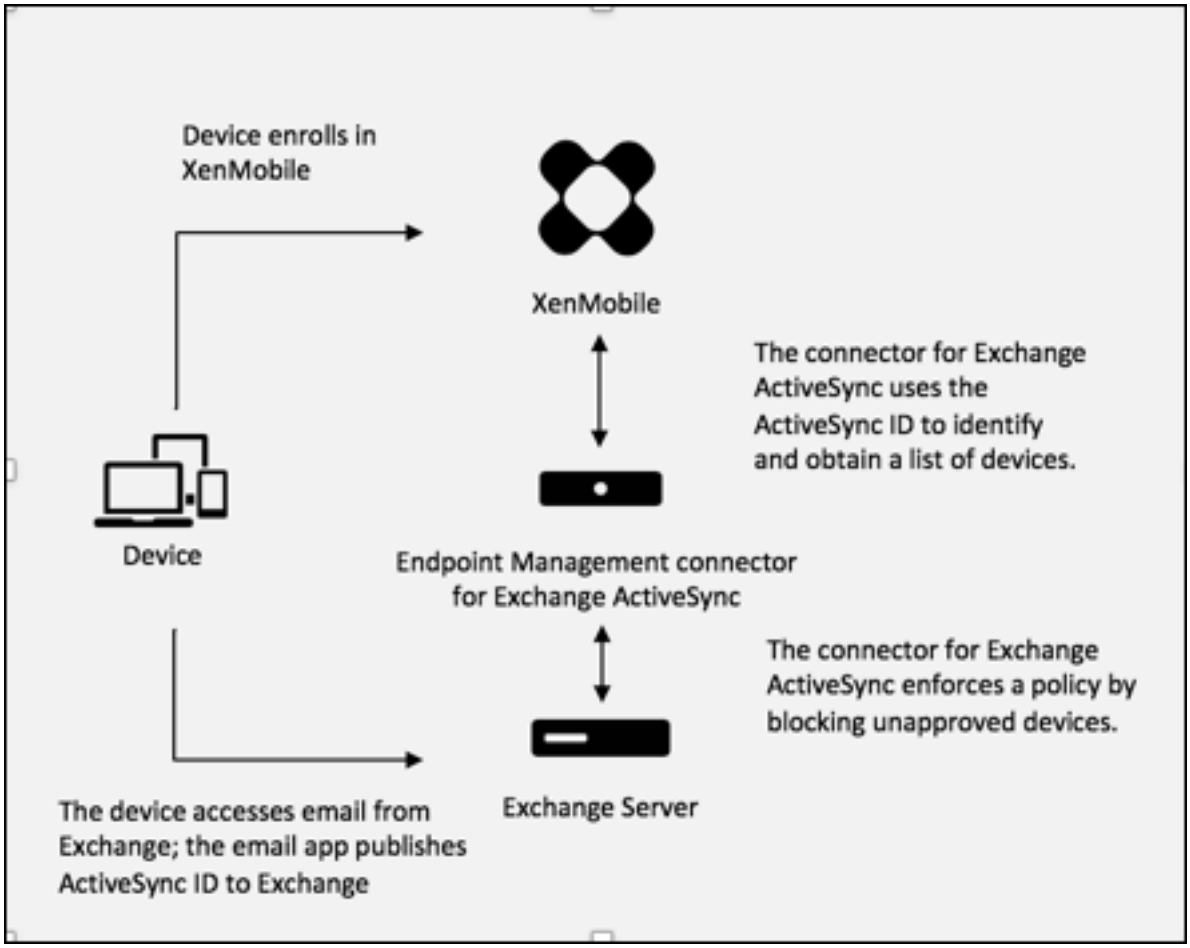


- BES 管理データベースのデータベース名を入力します。
- 認証モードを選択します。統合 Windows 認証を選択すると、Endpoint Management コネクタ：Exchange ActiveSync 用サービスのユーザーアカウントが、BES SQL Server への接続に使用するアカウントになります。Endpoint Management コネクタ：Exchange ActiveSync 用のデータベース接続に［Windows Integrated］を選択する場合は、ここで指定した Windows アカウントに、Endpoint Management コネクタ：Exchange ActiveSync 用データベースへのアクセス権も付与する必要があります。
- **SQL** 認証を選択する場合、ユーザー名とパスワードを入力します。
- ［**Sync Schedule**］ を設定します。これは、BES SQL Server への接続とデバイス更新のチェックに使用するスケジュールです。
- ［**Test Connectivity**］をクリックして、SQL Server への接続を確認します。［Windows Integrated］を選択している場合、このテストでは、Endpoint Management コネクタ：Exchange ActiveSync 用サービスのユーザーではなく、現在ログオンしているユーザーが使用されるため、SQL 認証が正確にテストされません。
- XenMobile からの BlackBerry デバイスのリモートワイプや ResetPassword をサポートする場合は、［有効］ チェックボックスをオンにします。
- BES の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を入力します。
- 管理者 Web サービスで使用する BES ポートを入力します。
- BES サービスに必要な完全修飾ユーザー名とパスワードを入力します。
- ［**Test Connectivity**］をクリックして、BES への接続をテストします。
- ［保存］ をクリックします。

ActiveSync ID によるメールポリシーの適用

企業のメールポリシーによっては、特定のデバイスで企業メールを使用することが認められない場合があります。このポリシーに従うには、そのようなデバイスから従業員が企業メールにアクセスできないようにする必要があります。Endpoint Management コネクタ：Exchange ActiveSync 用と XenMobile を連携させ、こうしたメールポリシーを適用することができます。XenMobile は企業の電子メールアクセスのポリシーを設定し、承認されていないデバイスが XenMobile に登録すると、Endpoint Management コネクタ：Exchange ActiveSync 用がポリシーを適用します。

デバイス上のメールクライアントはデバイス ID を使用して Exchange Server（または Office 365）にクライアントの存在を通知します。この ID は ActiveSync ID としても知られており、デバイスを識別するために使用されます。Secure Hub では同様の識別子を取得し、デバイスが登録されると XenMobile にこの識別子を送信します。Endpoint Management コネクタ：Exchange ActiveSync 用で 2 つのデバイス ID を比較することによって、特定のデバイスに企業メールへのアクセスを許可するかどうかが判定されます。次の図は、この概念を示しています：



デバイスが Exchange に公開した ID と異なる ActiveSync ID が XenMobile から Endpoint Management コネクタ: Exchange ActiveSync 用に送信されると、Endpoint Management コネクタ: Exchange ActiveSync 用から Exchange に対してそのデバイスに対する処理を指示できません。

ほとんどのプラットフォームで、ActiveSync ID は確実に一致します。ただし、一部の Android の実装では、デバイスが送信する ActiveSync ID とメールクライアントが Exchange に通知する ID が異なることが判明しています。この問題を緩和するため、次のことを実行できます:

- Samsung SAFE プラットフォームでは、デバイスの ActiveSync 構成を XenMobile からプッシュします。
- ほかのすべての Android プラットフォームでは、XenMobile から Touchdown アプリと Touchdown ActiveSync 構成の両方を XenMobile からプッシュします。

ただし、これにより従業員が Android デバイスに Touchdown 以外のメールクライアントをインストールできなくなるわけではありません。企業メールアクセスポリシーの適切な適用を保証するために、セキュリティについて防御的なスタンスをとり、静的なポリシーを［Deny by default］に設定することで Endpoint Management コネクタ: Exchange ActiveSync 用でメールを禁止するように構成することができます。これは、従業員が Android デバイスに TouchDown 以外のメールクライアントを構成し、ActiveSync ID の検出が適切に動作しない場合は、従業員は企業メールへのアクセスを拒否されるということを意味します。

アクセス制御規則

Endpoint Management コネクタ：Exchange ActiveSync 用では、Exchange ActiveSync デバイスのアクセス制御を動的に構成するための、規則に基づく手法が提供されます。Endpoint Management コネクタ：Exchange ActiveSync 用のアクセス制御規則は、一致式と目的のアクセス状態（許可またはブロック）の 2 つで構成されます。特定の Exchange ActiveSync デバイスに対して規則を評価して、その規則がデバイスに適用されるかどうか、またはデバイスと一致するかどうかを判別できます。一致式にはいくつかの種類があります。たとえば、規則は、特定のデバイスの種類のすべてのデバイス、特定の Exchange ActiveSync デバイス ID、特定のユーザーのすべてのデバイスと一致するなどの条件を指定できます。

規則一覧の規則を追加、削除、および並べ替えているときに［**Cancel**］をクリックすると、規則一覧が最初に開いたときの状態に戻ります。［**Save**］をクリックしない限り、構成ツールを閉じるとこのウィンドウに対して加えた変更が失われます。

Endpoint Management コネクタ：Exchange ActiveSync 用には、ローカル規則、XenMobile Server 規則（XDM 規則とも呼ばれます）、およびデフォルトのアクセス規則の 3 種類の規則があります。

ローカル規則： ローカル規則が最も優先されます：デバイスがローカル規則と一致すると、規則の評価は停止します。XenMobile Server 規則とデフォルトのアクセス規則は参照されません。ローカル規則は、［**Configure**］**>**［**Access Rules**］**>**［**Local Rules**］タブから、Endpoint Management コネクタ：Exchange ActiveSync 用に対してローカルに構成します。サポート一致は、特定の Active Directory グループ内のユーザーのメンバーシップに基づきます。サポート一致は、次のフィールドの正規表現に基づいています：

- Active Sync デバイス ID
- ActiveSync デバイスの種類
- ユーザープリンシパル名 (UPN)
- ActiveSync ユーザーエージェント（通常、デバイスプラットフォームまたはメールクライアント）

メジャースナップショットが完了し、デバイスが検出されている限り、通常の規則または正規表現の規則のいずれかを追加できます。メジャースナップショットが完了していない場合、正規表現の規則のみを追加できます。

XenMobile Server 規則： 管理対象デバイスに関する規則を提供する外部 XenMobile Server への参照です。XenMobile Server は、デバイスがジェイルブレイク済みかどうかや、デバイスに禁止アプリが含まれるかどうかなど、XenMobile が認識しているプロパティに基づいてデバイスが許可されるか、ブロックされるかを識別する独自の高レベルの規則を使用して構成できます。XenMobile では、高レベルの規則が評価され、許可またはブロックする一連の ActiveSync デバイス ID が生成されて、これらが Endpoint Management コネクタ：Exchange ActiveSync 用に配信されます。

デフォルトのアクセス規則： デフォルトのアクセス規則は、すべてのデバイスと一致する可能性があり、常に最後に評価されるという点で独特です。この規則は、あらゆる状況に対応できる規則です。つまり、特定のデバイスがローカル規則と XenMobile Server 規則のいずれにも一致しない場合は、デフォルトのアクセス規則での目的のアクセス状態によってデバイスにおける目的のアクセス状態が決まります。

- デフォルトのアクセス **–** 許可： ローカル規則と XenMoble Server 規則のいずれにも一致しないすべてのデバイスが許可されます。

- デフォルトのアクセス – ブロック: ローカル規則と XenMoble Server 規則のいずれにも一致しないすべてのデバイスがブロックされます。
- デフォルトのアクセス – 変更なし: ローカル規則と XenMobile Server 規則のいずれにも一致しないすべてのデバイスのアクセス状態は、Endpoint Management コネクタ: Exchange ActiveSync 用によって変更されません。Exchange によってデバイスが Quarantine モードになっている場合、アクションは実行されません。たとえば、Quarantine モードからデバイスを削除する方法は、ローカル規則または XDM 規則で隔離を明示的に上書きすることのみです。

規則の評価について

Exchange から Endpoint Management コネクタ: Exchange ActiveSync 用に報告されるデバイスごとに、次のように優先度の高い順に規則が評価されます:

- ローカル規則
- XenMobile Server 規則
- デフォルトのアクセス規則

一致が検出されると、評価は停止します。たとえば、ローカル規則が特定のデバイスと一致すると、そのデバイスは XenMobile Server 規則またはデフォルトのアクセス規則に対して評価されません。このことは、特定の種類の規則内でも当てはまります。たとえば、ローカル規則一覧で、特定のデバイスに対して複数の一致がある場合、最初の一致が見つかるとすぐに評価は停止します。

デバイスプロパティが変更されたとき、デバイスが追加または削除されたとき、または規則自体が変更されたときは、現在定義されている一連の規則が Endpoint Management コネクタ: Exchange ActiveSync 用によって再評価されます。メジャースナップショットにより、構成可能な間隔でデバイスのプロパティ変更または削除が確認されます。マイナースナップショットにより、構成可能な間隔で新しいデバイスが確認されます。

Exchange ActiveSync にも、アクセスを管理する規則があります。これらの規則が Endpoint Management コネクタ: Exchange ActiveSync 用でどのように機能するかを理解することが重要です。Exchange は、個人の適用除外、デバイスの規則、組織の設定という 3 つのレベルの規則で構成できます。Endpoint Management コネクタ: Exchange ActiveSync 用では、リモート PowerShell 要求をプログラムで発行して個人の適用除外一覧に反映させることで、アクセス制御を自動化します。これらは、特定のメールボックスに関連する、許可またはブロックする Exchange ActiveSync デバイス ID の一覧です。展開すると、Endpoint Management コネクタ: Exchange ActiveSync 用は Exchange 内の適用除外一覧の管理機能を効果的に引き継ぎます。詳細については、このMicrosoft の技術文書を参照してください。

分析は、同じフィールドに対して複数の規則が定義されている場合に特に便利です。規則間の関係をトラブルシューティングできます。規則フィールドの観点から分析を実行します。たとえば、ActiveSync デバイス ID、ActiveSync デバイスの種類、ユーザー、ユーザーエージェントなどの照合されるフィールドに基づくグループで規則が分析されます。

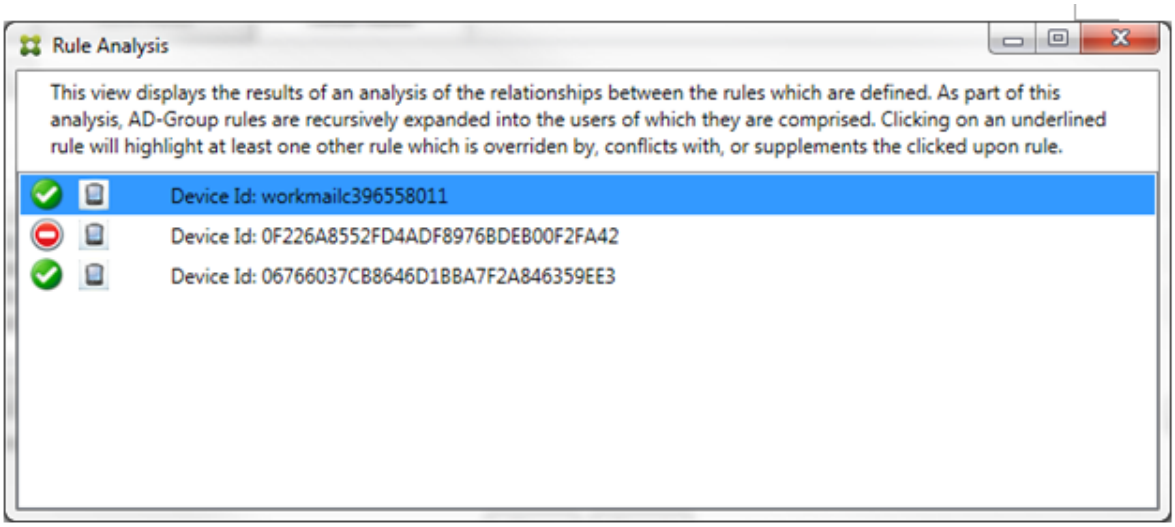
規則の用語

- 上書き規則： 同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- 競合規則： 同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- 補足規則： 正規表現の規則が複数あるので、2 つ（またはそれ以上）の正規表現を 1 つの正規表現の規則に結合できるか、またはそれらの機能が重複していないようにする必要がある場合に補足が発生します。補足規則もアクセス（許可/ブロック）で競合する場合があります。
- プライマリ規則： プライマリ規則は、ダイアログボックス内でクリックされた規則です。この規則は、実線の罫線で囲まれて示されます。この規則には、上方向または下方向を指す 1 つまたは 2 つの緑色の矢印も示されます。矢印が上方向を指している場合は、プライマリ規則よりも優先される補助規則があることを示しています。矢印が下方向を指している場合は、プライマリ規則よりも優先度の低い補助規則があることを示しています。アクティブにできるプライマリ規則は、常に 1 つのみです。
- 補助規則： 補助規則は、上書き、競合、または補足の関係のいずれかで、プライマリ規則と何らかの関係を持ちます。この規則は、破線の罫線で囲まれて示されます。各プライマリ規則に対して、1 対多の補助規則を指定できます。下線付きのエントリをクリックしたときに強調表示される補助規則は、常にプライマリ規則の観点から示されます。たとえば、補助規則がプライマリ規則によって上書きされたり、プライマリ規則とアクセスで競合したり、プライマリ規則を補足したりします。

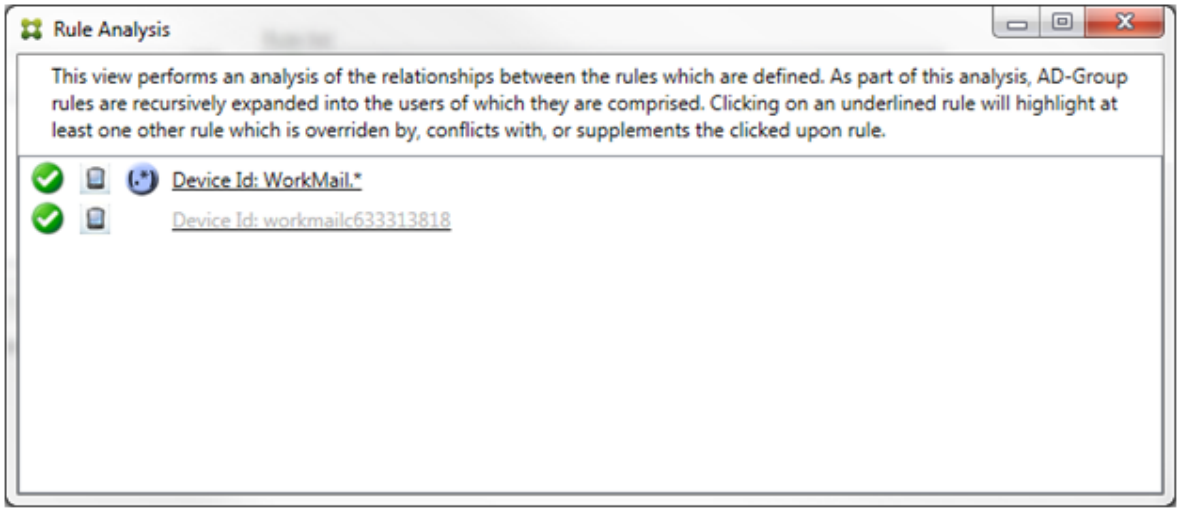
［**Rule Analysis**］ダイアログボックスに表示する規則の種類の外観

競合、上書き、または補足がない場合、［Rule Analysis］ダイアログボックスに下線付きのエントリは表示されません。どのアイテムをクリックしても影響はありません。通常の選択済みアイテムの表示になります。

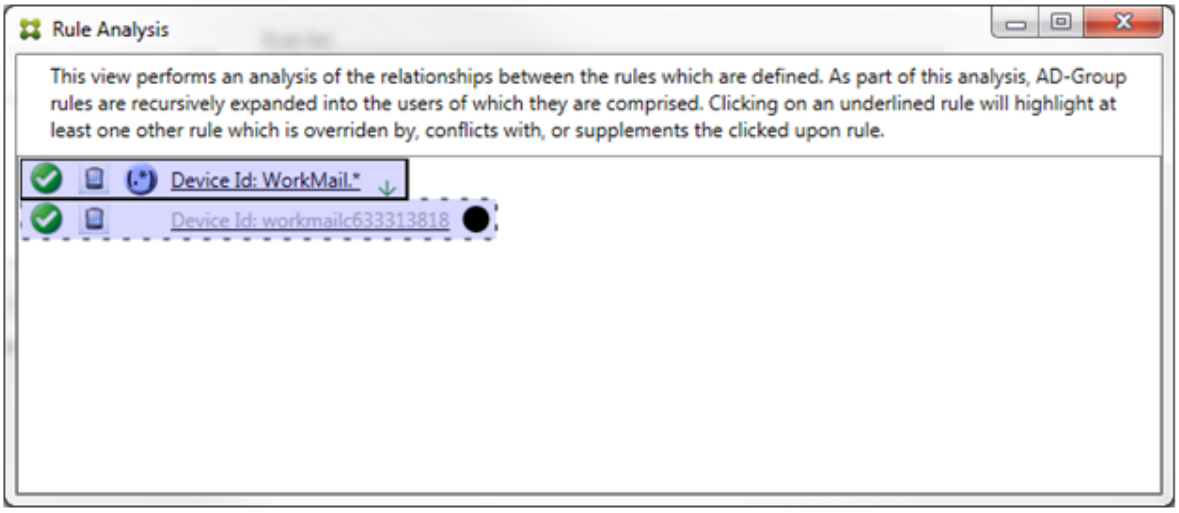
［Rule Analysis］ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。



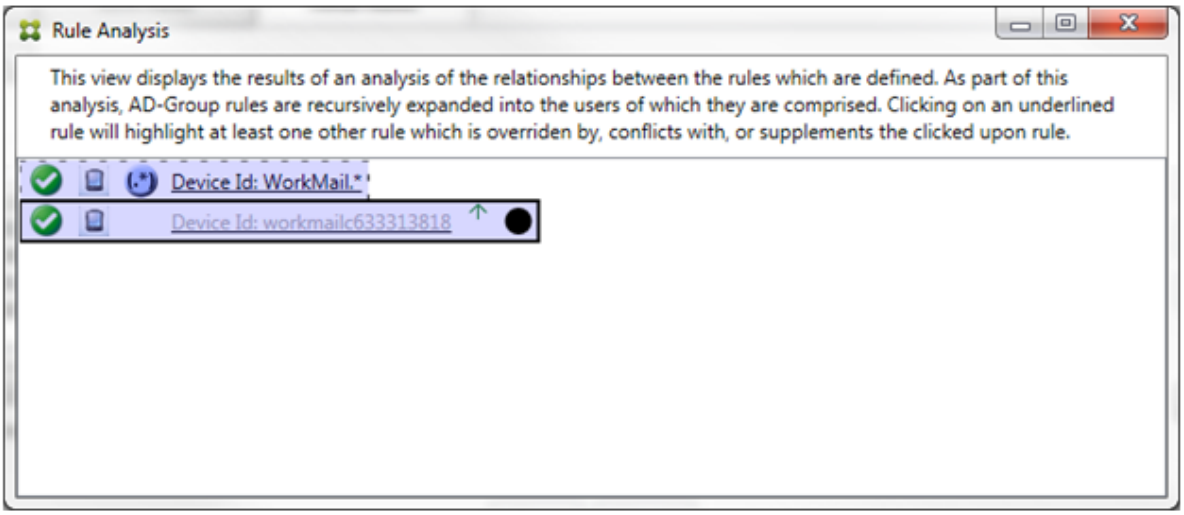
上書きが発生した場合、2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。1 つ以上の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。上書きされた規則をクリックして、その規則を上書きした規則を確認できます。規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます:



最も優先度の高い規則をクリックすると、ダイアログボックスの表示は次のようになります:

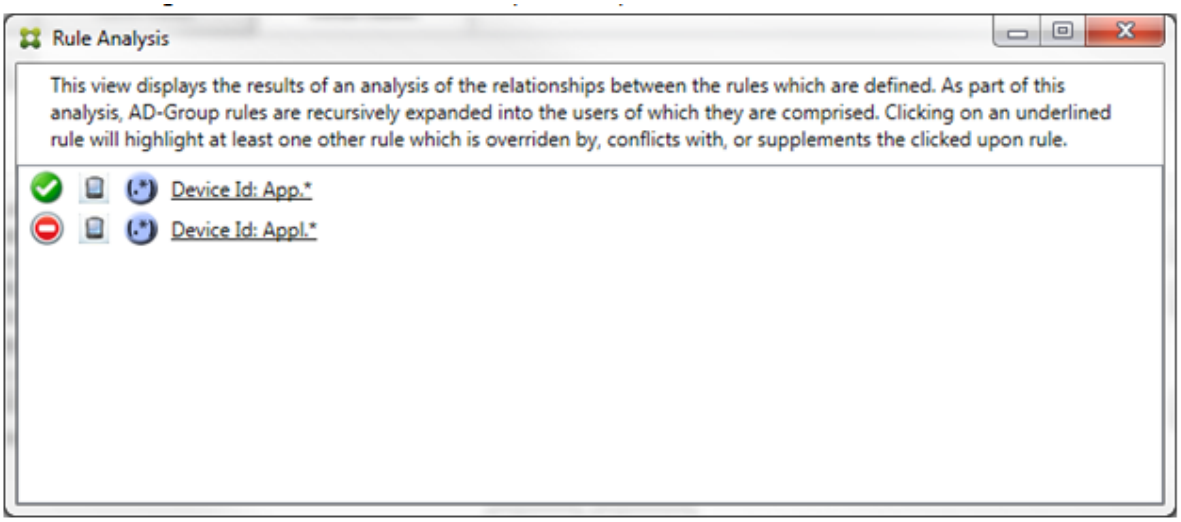


この例では、正規表現の規則`WorkMail.*`がプライマリ規則（実線の罫線で表示）で、通常の規則`workmailc633313818`が補助規則（破線の罫線で表示）です。補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります:

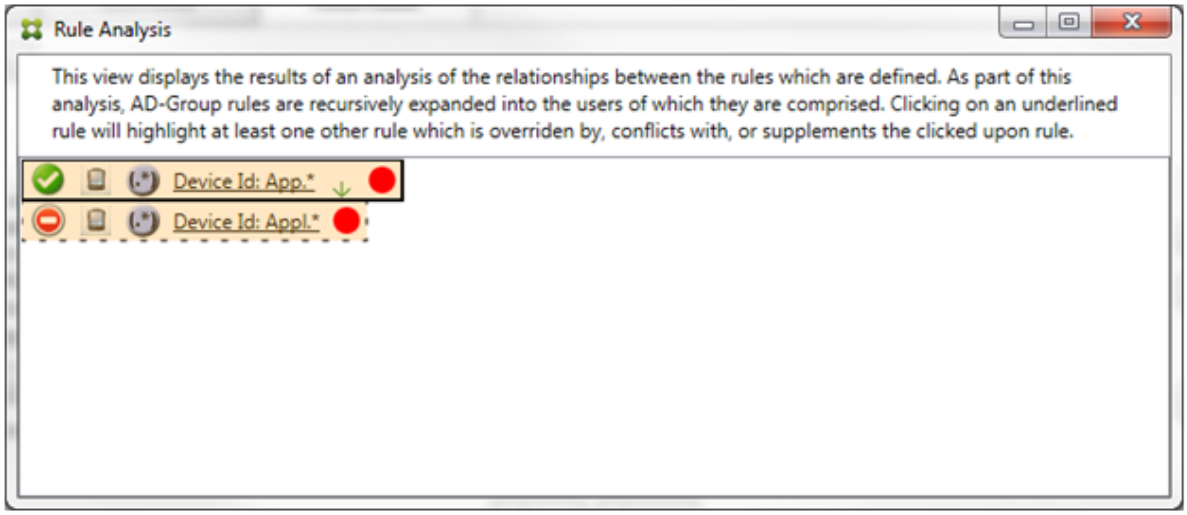


上記の例では、正規表現の規則`WorkMail.*`が補助規則(破線の罫線で表示)で、通常の規則`workmailc633313818`がプライマリ規則（実線の罫線で表示）です。このシンプルな例では、大きな違いはありません。より複雑な例については、このトピックで後述する複雑な式の例を参照してください。多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

競合が発生した場合、2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。競合している規則は赤色の点で示されます。相互に競合のみが発生している規則は、2 つ以上の正規表現の規則が定義されている場合に限り発生します。ほかのすべての競合のシナリオでは、競合のみではなく、上書きも発生します。シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます:

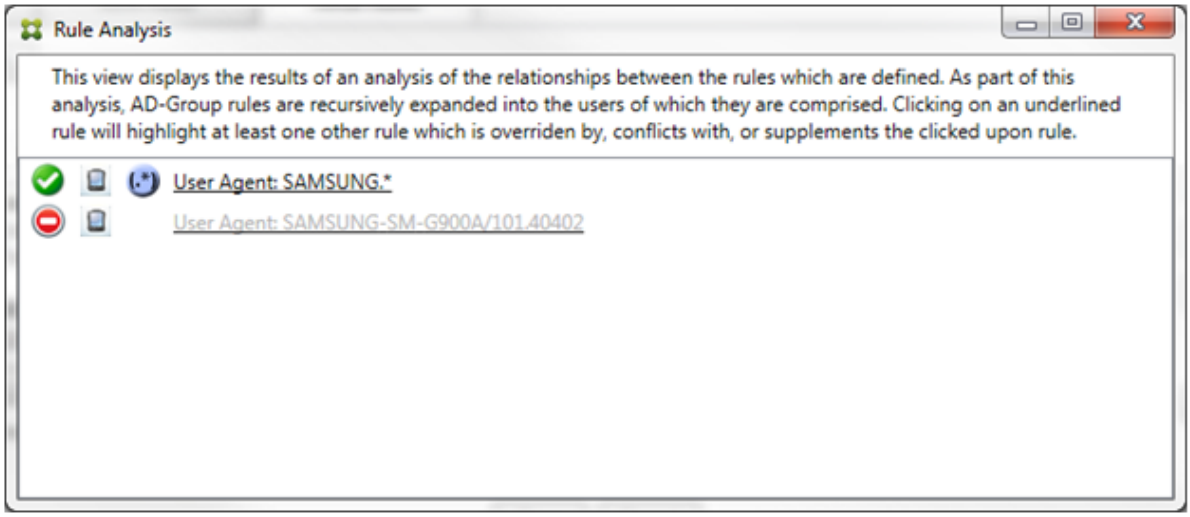


2 つの正規表現の規則を確認すると、最初の規則で「App」がデバイス ID に含まれるすべてのデバイスを許可し、2 つ目の規則で「Appl」がデバイス ID に含まれるすべてのデバイスを拒否することがわかります。さらに、2 つ目の規則で「Appl」がデバイス ID に含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは決して拒否されません。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります:



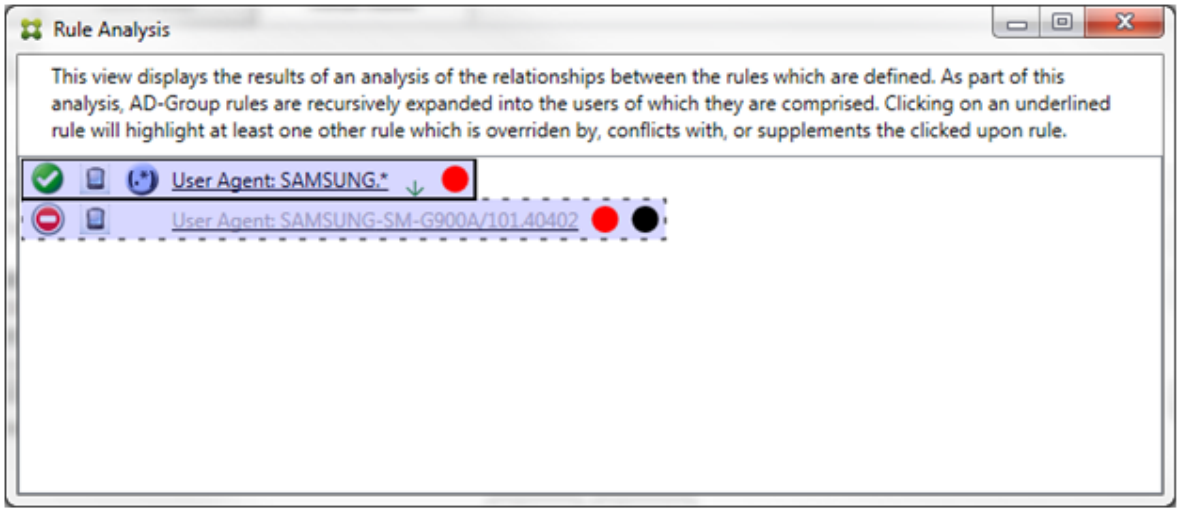
前述のシナリオでは、プライマリ規則（正規表現の規則`App.*`）と補助規則（正規表現の規則`Appl.*`）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

競合と上書きの両方を含むシナリオでは、プライマリ規則（正規表現の規則`App.*`）と補助規則（正規表現の規則`Appl.*`）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。



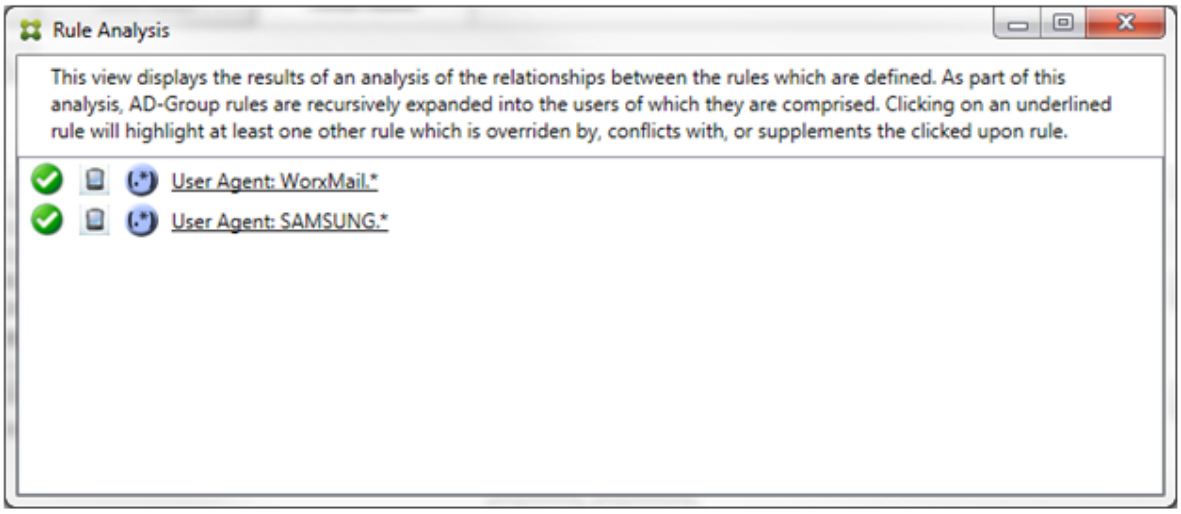
上記の例では、最初の規則（正規表現の規則SAMSUNG.*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2 つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。2 つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

正規表現の規則をクリックすると、ダイアログボックスの表示は次のようになります:

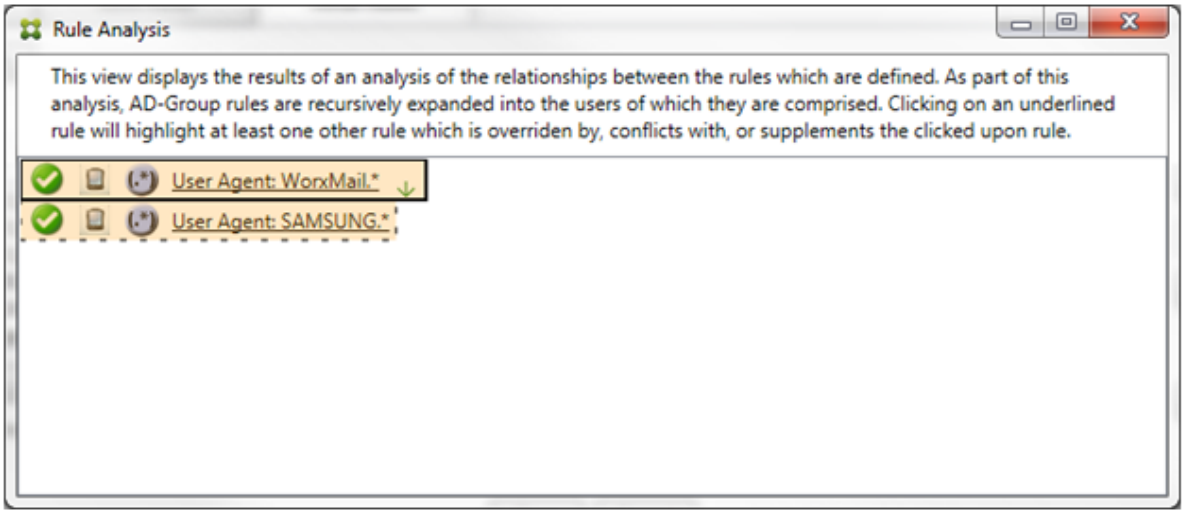


プライマリ規則（正規表現の規則SAMSUNG.*）の末尾には赤色の点が付けられて、アクセス状態が 1 つまたは複数の補助規則と競合していることが示されます。補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には赤色の点が付けられて、アクセス状態がプライマリ規則と競合していることが示されます。この規則の末尾には黒色の点が付けられて、上書きされたために非アクティブであることが示されます。

2 つ以上の規則（プライマリ規則と、1 つまたは複数の補助規則）に下線が付けられます。相互に補足のみが発生している規則には、正規表現の規則のみが定義されています。相互に補足が発生している規則は、黄色のオーバーレイで示されます。シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます:



目視で確認すると、両方の規則が正規表現の規則で、両方とも Endpoint Management コネクタ: Exchange ActiveSync 用の［ActiveSync device ID］フィールドに適用されていることが容易にわかります。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります:

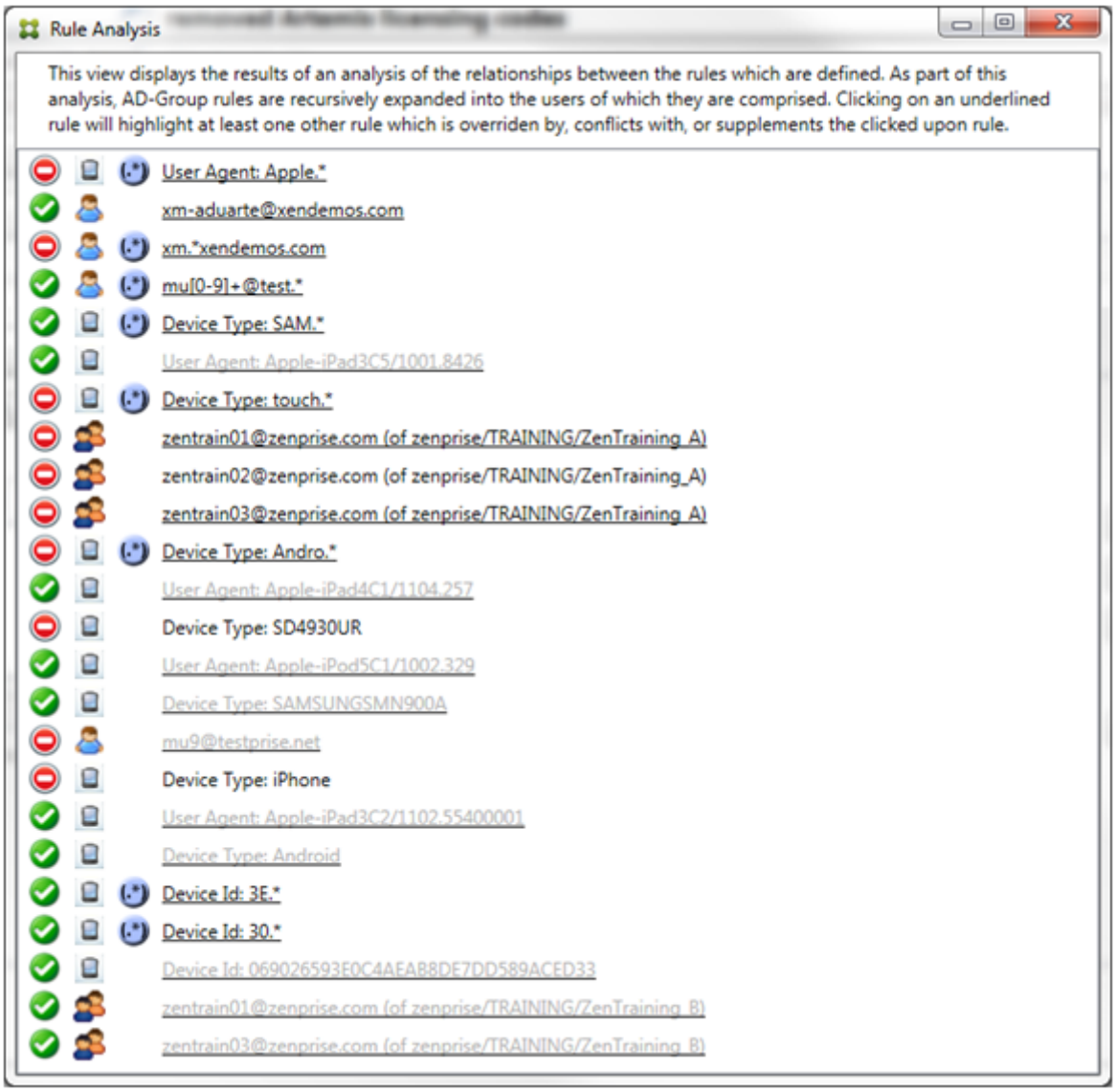


プライマリ規則（正規表現の規則`WorkMail.*`）が黄色のオーバーレイで強調表示され、正規表現の補助規則がほかに 1 つ以上存在することが示されます。補助規則（正規表現の規則`SAMSUNG.*`）が黄色のオーバーレイで強調表示され、この規則とプライマリ規則の両方が、Endpoint Management コネクタ: Exchange ActiveSync 用内の同じフィールドに適用されている正規表現の規則であることが示されます。この場合、そのフィールドは ActiveSync デバイス ID です。正規表現は重複する場合としない場合があります。正規表現が適切に作成されているかどうかの判断は、ユーザーに委ねられます。

複雑な式の例

発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。次の

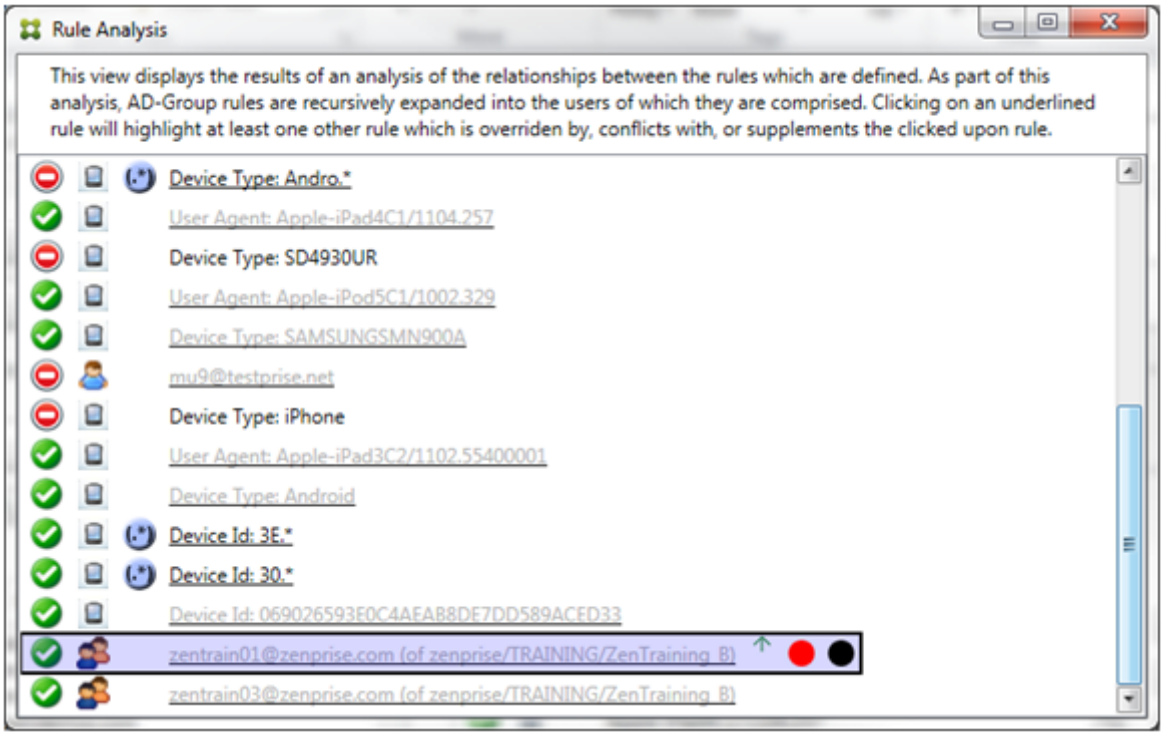
図では、ほとんどのアイテムに下線が付けられています。多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。同様に、  アイコンで示される多数の正規表現の規則も一覧に含まれています。



上書きの分析方法

特定の規則を上書きした規則を確認するには、その規則をクリックします。

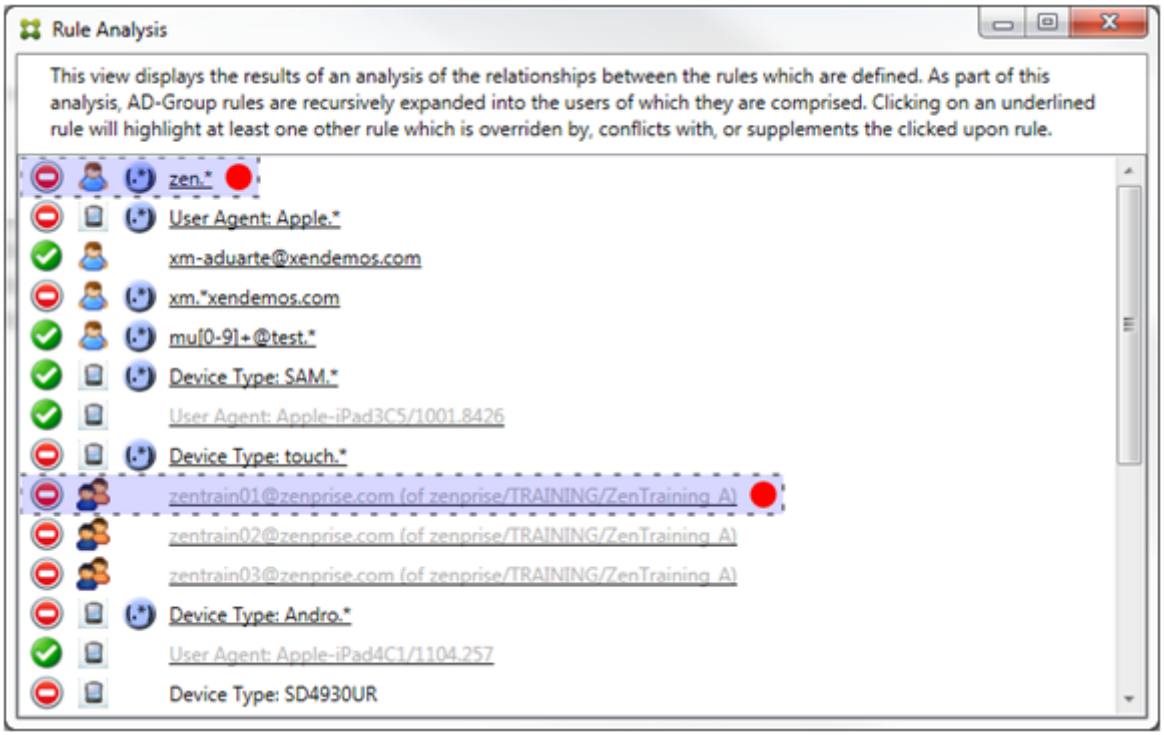
例 **1**: この例では、`zentrain01@zenprise.com`が上書きされた理由を調べます。



プライマリ規則（zentrain01@zenprise.comがメンバーとして属する AD グループ規則zenprise/TRAINING/ZenTraining B）には、次の特性があります:

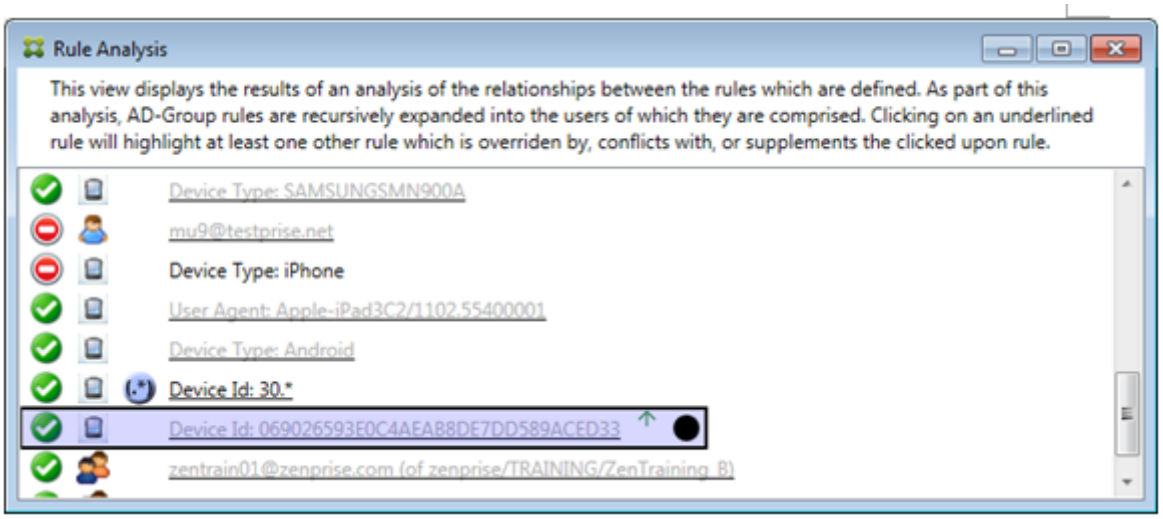
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（すべての補助規則がこの規則より上に表示されていることを示します)。
- 末尾に、1 つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます:



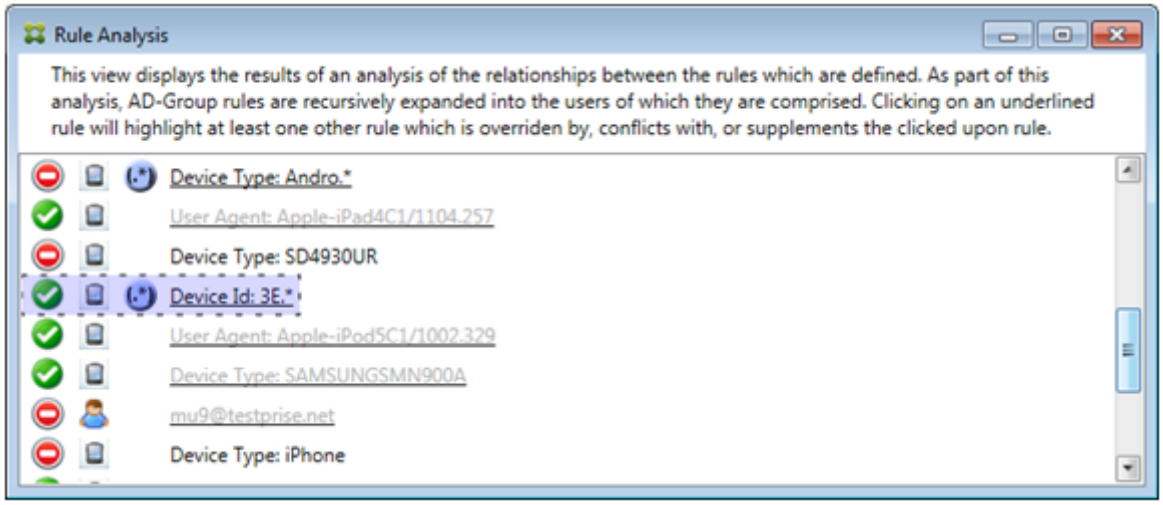
この場合、プライマリ規則を上書きする 2 つの補助規則があります: 正規表現の規則`zen.*`と通常の規則`zentrain01@zenprise.com`（`zenprise`/`TRAINING`/`ZenTraining A`の規則）です。後者の補助規則の場合、Active Directory グループ規則`ZenTraining A`にユーザー`zentrain01@zenprise.com`が含まれる一方、Active Directory グループ規則`ZenTraining B`にもユーザー`zentrain01@zenprise.com`が含まれることになります。ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、プライマリ規則は上書きされています。プライマリ規則のアクセスが許可で、両方の補助規則のアクセスがブロックであるので、これらすべての末尾に赤色の点が付けられて、アクセスが競合していることも示されています。

例 **2**: 次の例は、ActiveSync デバイス ID が`069026593E0C4AEAB8DE7DD589ACED33`であるデバイスが上書きされた理由を示しています:



このプライマリ規則（通常のデバイス ID の規則069026593E0C4AEAB8DE7DD589ACED33）には、次の特性があります:

- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、補助規則がそのプライマリ規則を上書きして、非アクティブであることを示す黒色の円が付けられている。



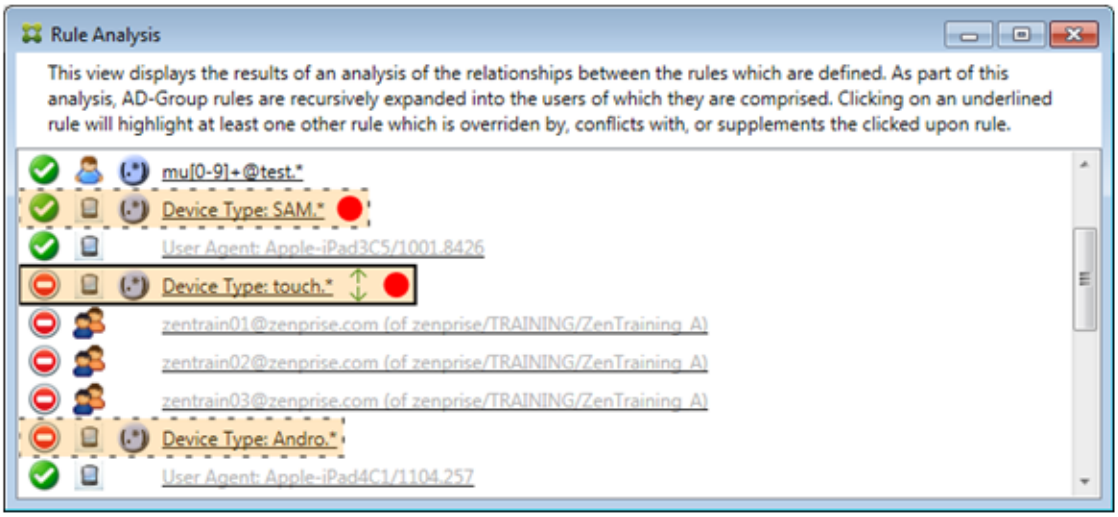
この場合、単一の補助規則（正規表現の ActiveSync デバイス ID の規則3E.*）がプライマリ規則を上書きします: 正規表現3E.*が069026593E0C4AEAB8DE7DD589ACED33に一致するため、プライマリ規則は評価されません。

補足および競合の分析方法

この場合、プライマリ規則は正規表現の ActiveSync デバイスの種類の規則touch.*です。特性は次のとおりです:

- 実線の罫線で囲まれ、特定の規則フィールド（この場合は、ActiveSync デバイスの種類）に対して複数の正規表現の規則が使用されているという警告として、黄色のオーバーレイが適用されている。
- 上方向および下方向をそれぞれ指す 2 つの矢印が付けられ、より優先度の高い 1 つ以上の補助規則とより優先度の低い 1 つ以上の補助規則が存在することが示されている。
- 横に赤色の円が付けられ、1 つ以上の補助規則のアクセスが許可に設定されて、プライマリ規則のアクセス状態のブロックと競合することが示されている。
- 2 つの補助規則: 正規表現の ActiveSync デバイスの種類の規則SAM.*と正規表現の ActiveSync デバイスの種類の規則Andro.*が存在する。
- 両方の補助規則が破線の罫線で囲まれ、補助規則であることが示されている。
- 両方の補助規則に黄色のオーバーレイが適用され、ActiveSync デバイスの種類の規則フィールドにこれらが適用されていることが示されている。

- このようなシナリオでは、正規表現の規則が冗長でないようにする必要がある。



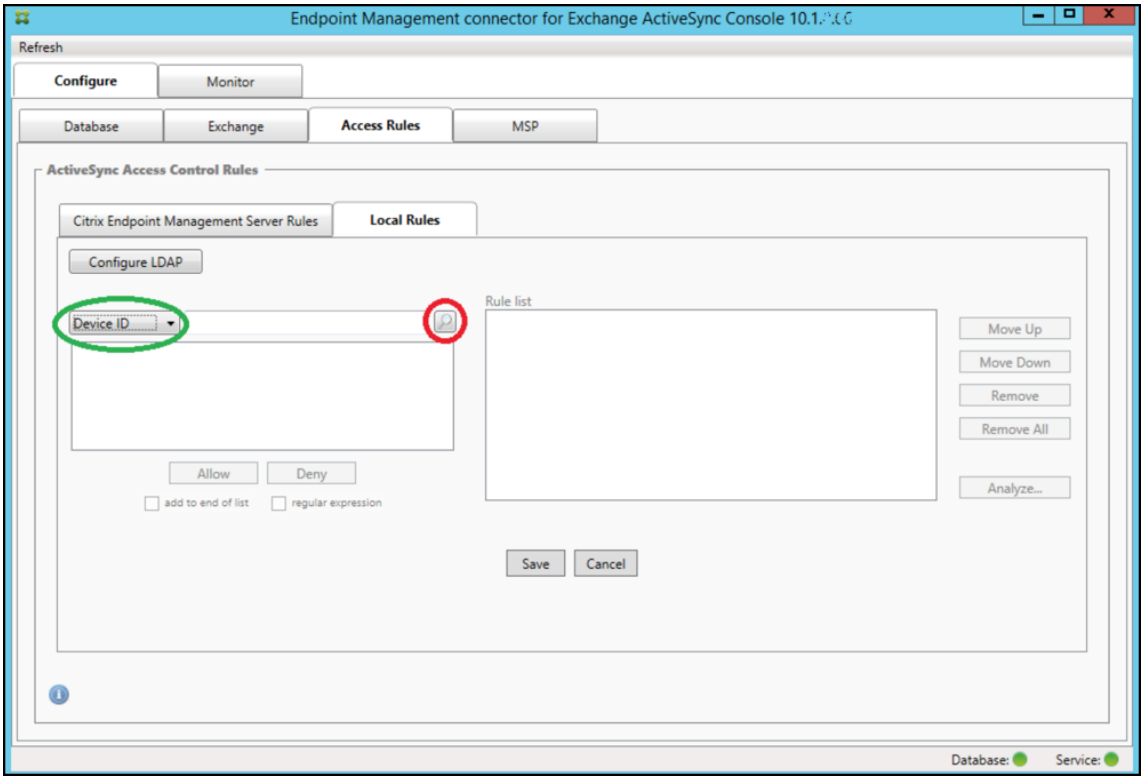
規則の高度な分析方法

次の例では、規則の関係が常にプライマリ規則の観点から示されるしくみを確認します。上記の例では、値が`touch.*`のデバイスの種類の規則フィールドに適用される正規表現規則をクリックする方法を示しました。補助規則`Andro.*`をクリックすると、さまざまな一連の補助規則が強調表示されます。

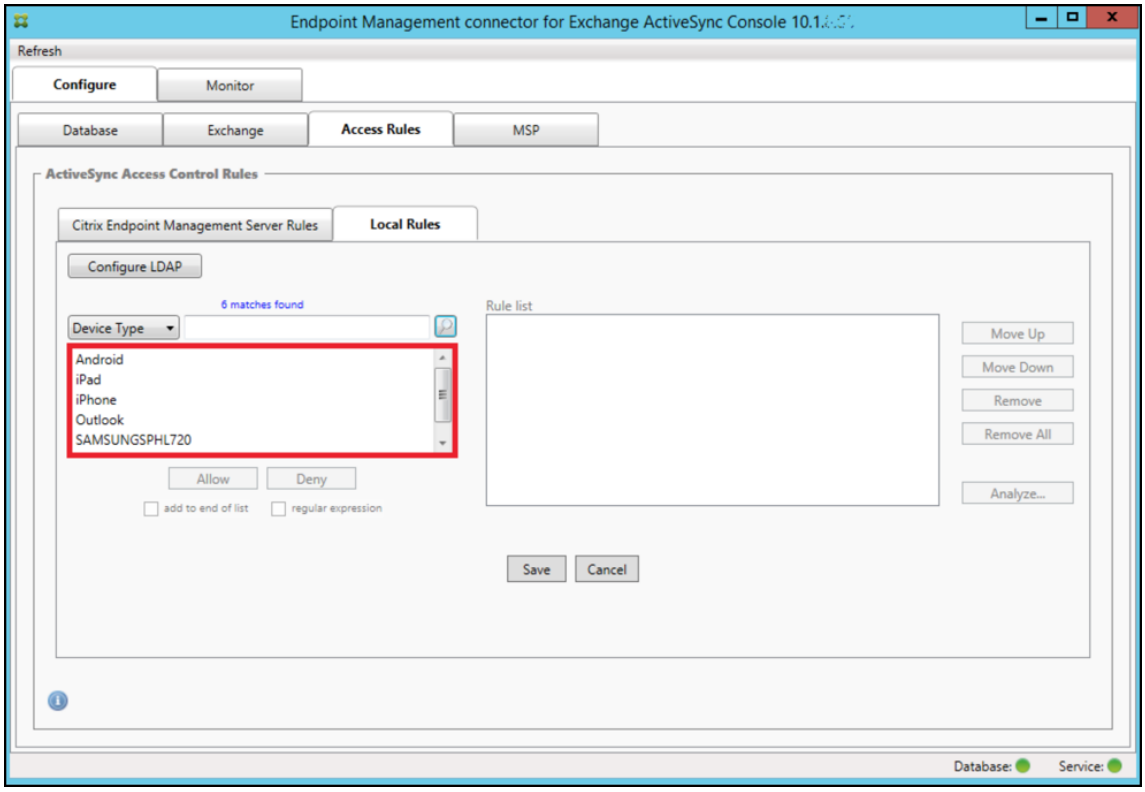
この例では、規則の関係に含まれる上書きされた規則が示されています。この規則は、通常の ActiveSync デバイスの種類の規則`Android`です。この規則は上書きされている（淡色のフォントで示され、横に黒点が付けられています）と同時に、プライマリ規則（正規表現の ActiveSync デバイスの種類の規則`Andro.*`）のアクセスと競合しています。この規則は、クリックされる前は補助規則でした。前述の例では、その時点でのプライマリ規則（正規表現の ActiveSync デバイスの種類の規則`touch.*`）の観点からは関係しなかったため、通常の ActiveSync デバイスの種類の規則`Android`は補助規則として表示されていませんでした。

通常の式のローカル規則を構成するには

1. [**Access Rules**] タブをクリックします。



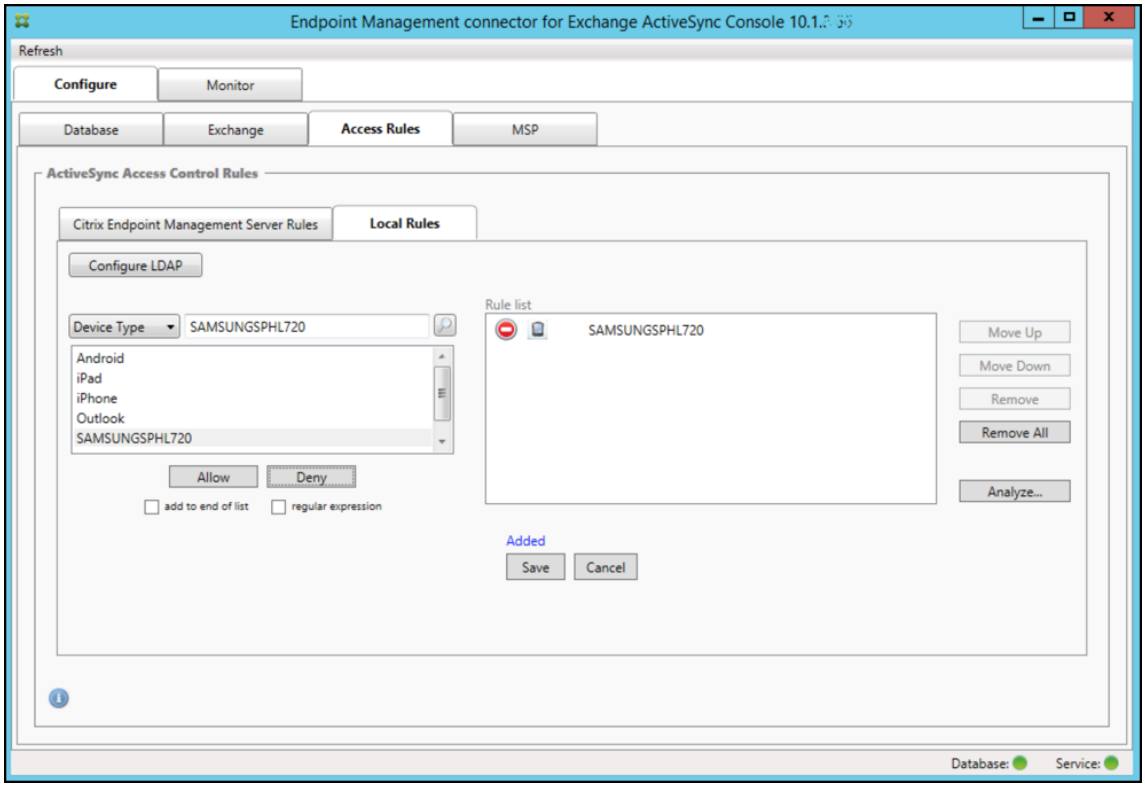
2. [**Device ID**] 一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[**Device Type**] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 表示されたリストボックスでいずれかのアイテムをクリックして、次のいずれかのオプションをクリックします:

   - **Allow**: すべての一致するデバイスに対して、ActiveSync トラフィックを許可するように Exchange が構成されます。
   - **Deny**: すべての一致するデバイスに対して、ActiveSync トラフィックを拒否するように Exchange が構成されます。

   この例では、デバイスの種類が SamsungSPhl720 であるすべてのデバイスのアクセスが拒否されます。



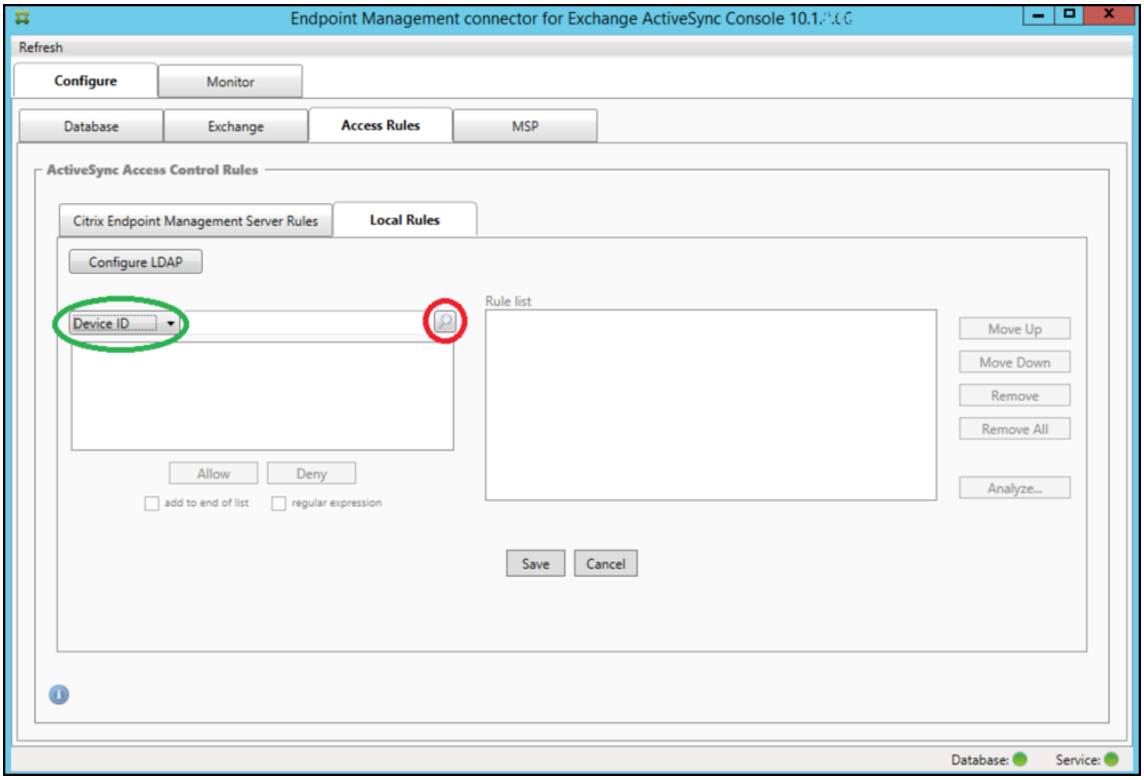
正規表現を追加するには

正規表現のローカル規則は、横に表示されるアイコン（  ）で識別できます。

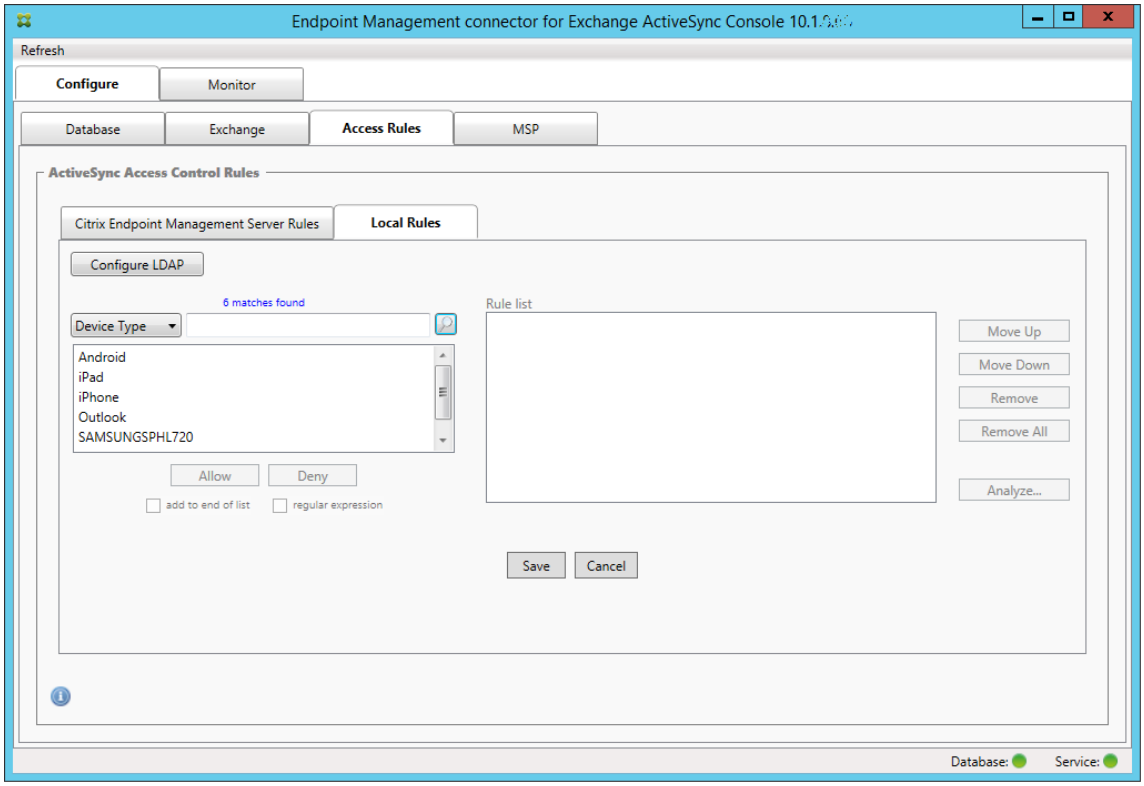
正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

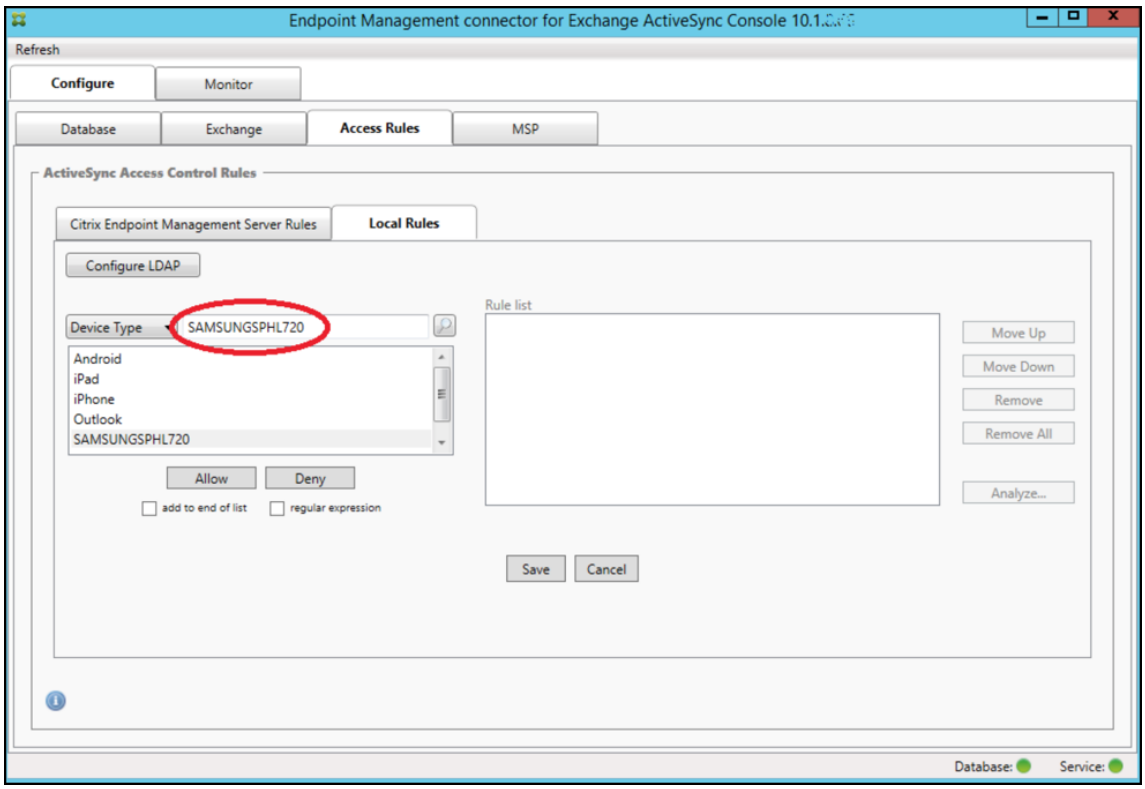
1. [**Access Rules**] タブをクリックします。



2. [**Device ID**] 一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[**Device Type**] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 結果一覧でいずれかのアイテムをクリックします。この例では、**SAMSUNGSPHL720** が選択され、それが［**Device Type**］ に隣接するテキストボックスに表示されています。



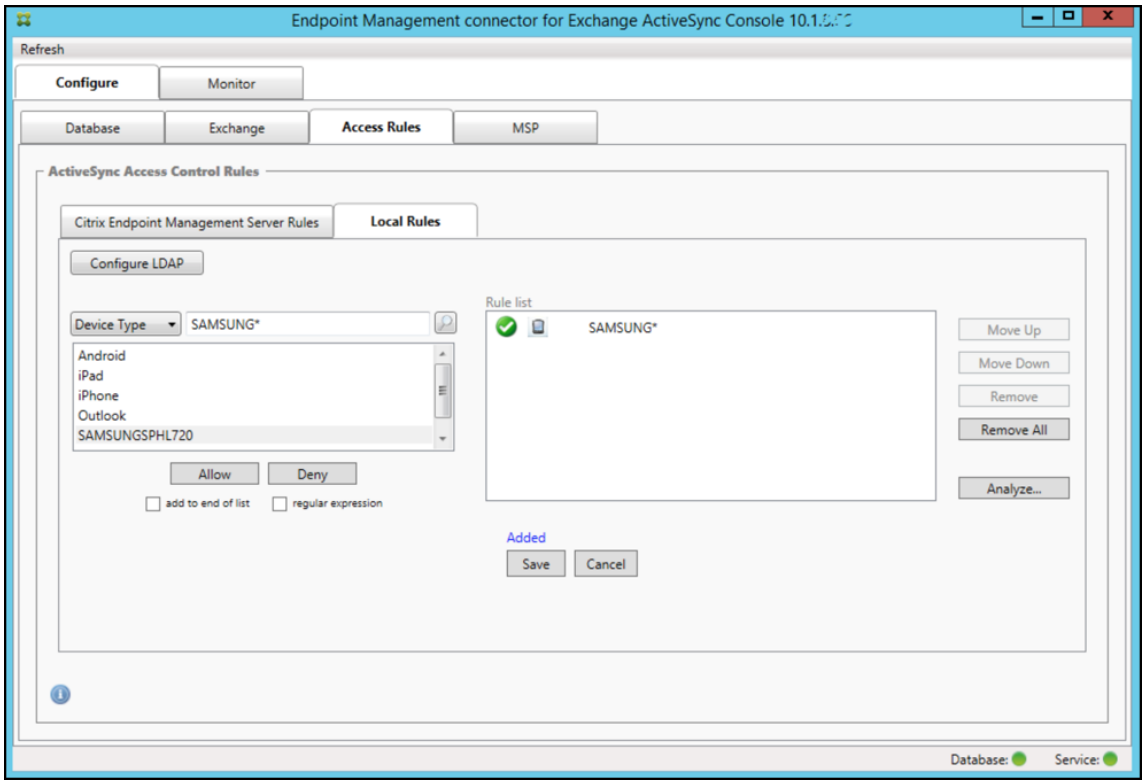
5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。

   a) 選択済みアイテムのテキストボックス内をクリックします。

   b) **SAMSUNGSPHL720** から **SAMSUNG.*** にテキストを変更します。

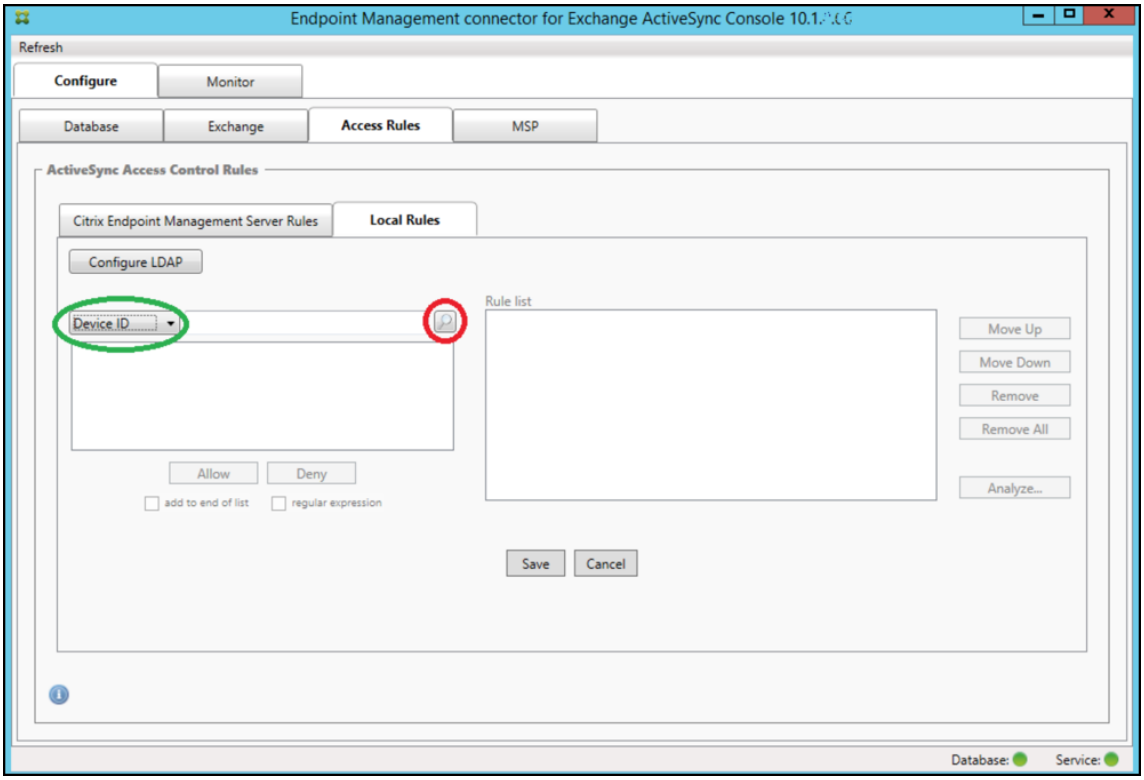
   c) [regular expression] チェックボックスをオンにします。

   d) [**Allow**] をクリックします。

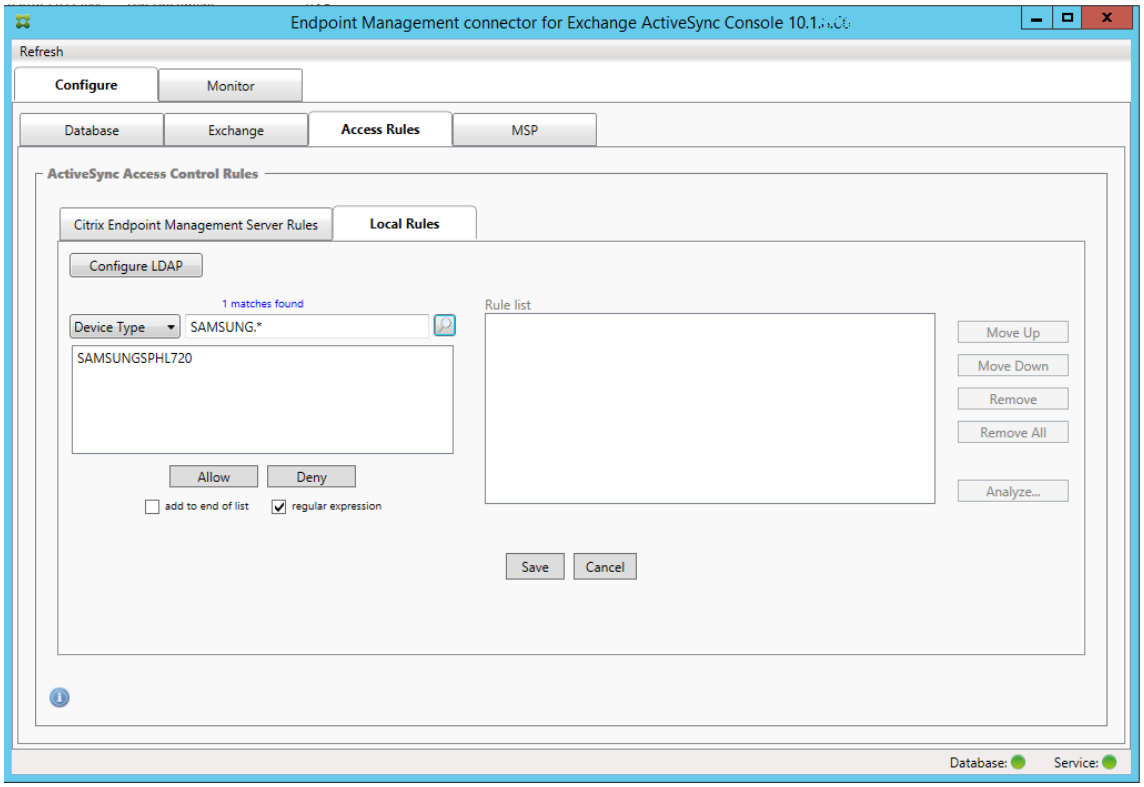


アクセス規則を作成するには

1. [**Local Rules**] タブをクリックします。
2. 正規表現を入力するには、[Device ID] 一覧と選択済みアイテムのテキストボックスの両方を使用する必要があります。



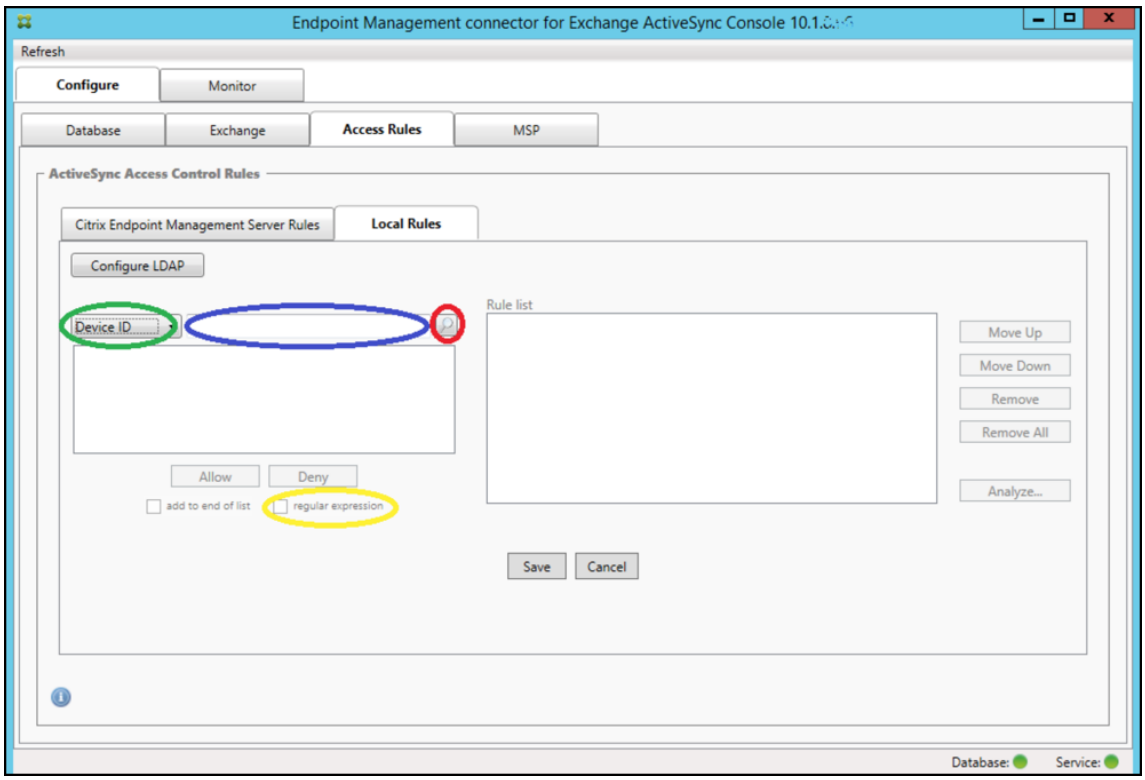
3. 照合するフィールドを選択します。この例では［Device Type］を使用します。
4. 正規表現を入力します。この例では次の文字列を使用します：`samsung.*`
5. ［regular expression］チェックボックスをオンにして、［**Allow**］または［**Deny**］をクリックします。この例では、［**Allow**］が選択されています。最終的な結果は次のとおりです：



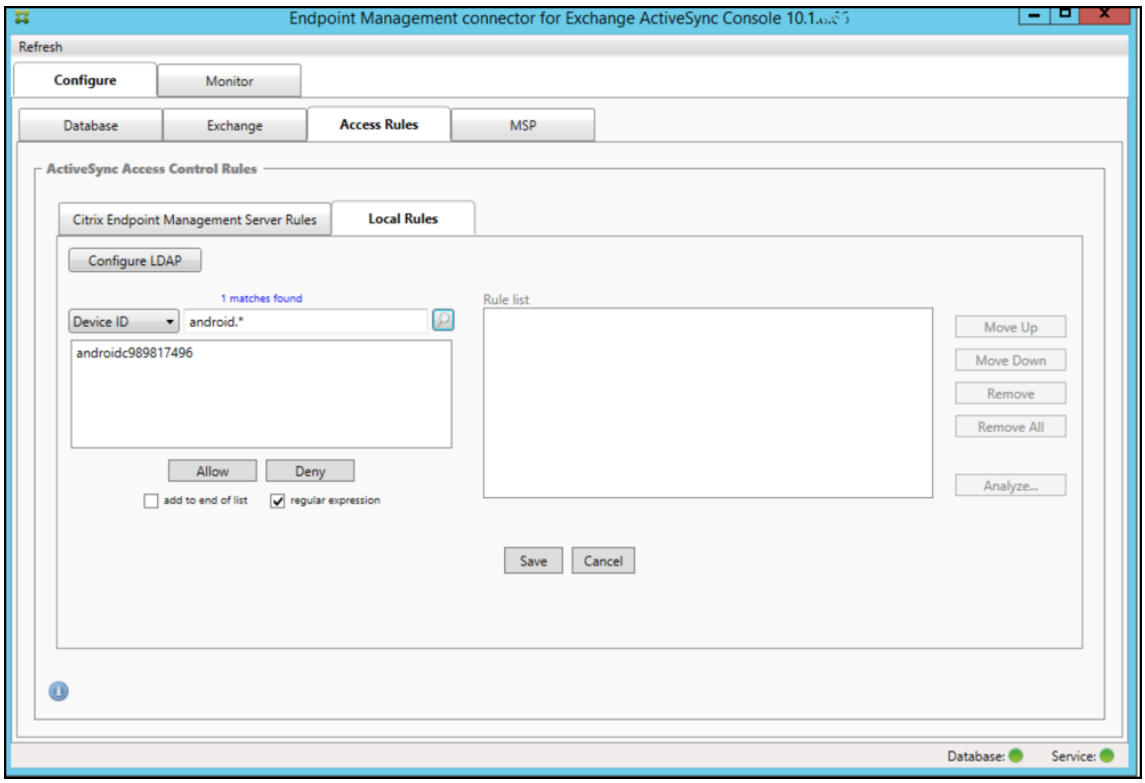
デバイスを検出するには

[regular expression] チェックボックスをオンにして、特定の式に一致する特定のデバイスの検索を実行できます。この機能は、メジャースナップショットが正常に完了している場合にのみ利用できます。正規表現の規則を使用しない場合でも、この機能を使用できます。たとえば、ActiveSync デバイス ID にテキスト「workmail」が含まれるすべてのデバイスを検出するとします。これを行うには、以下の手順に従います。

1. [**Access Rules**] タブをクリックします。
2. デバイスの照合フィールドセレクターが [Device ID]（デフォルト）に設定されていることを確認します。



3. 選択済みアイテムのテキストボックス内（上記の図に青色で示されています）をクリックし、「**workmail.***」と入力します。
4. ［regular expression］チェックボックスをオンにして、虫眼鏡アイコンをクリックし、次の図に示すように一致を表示します。

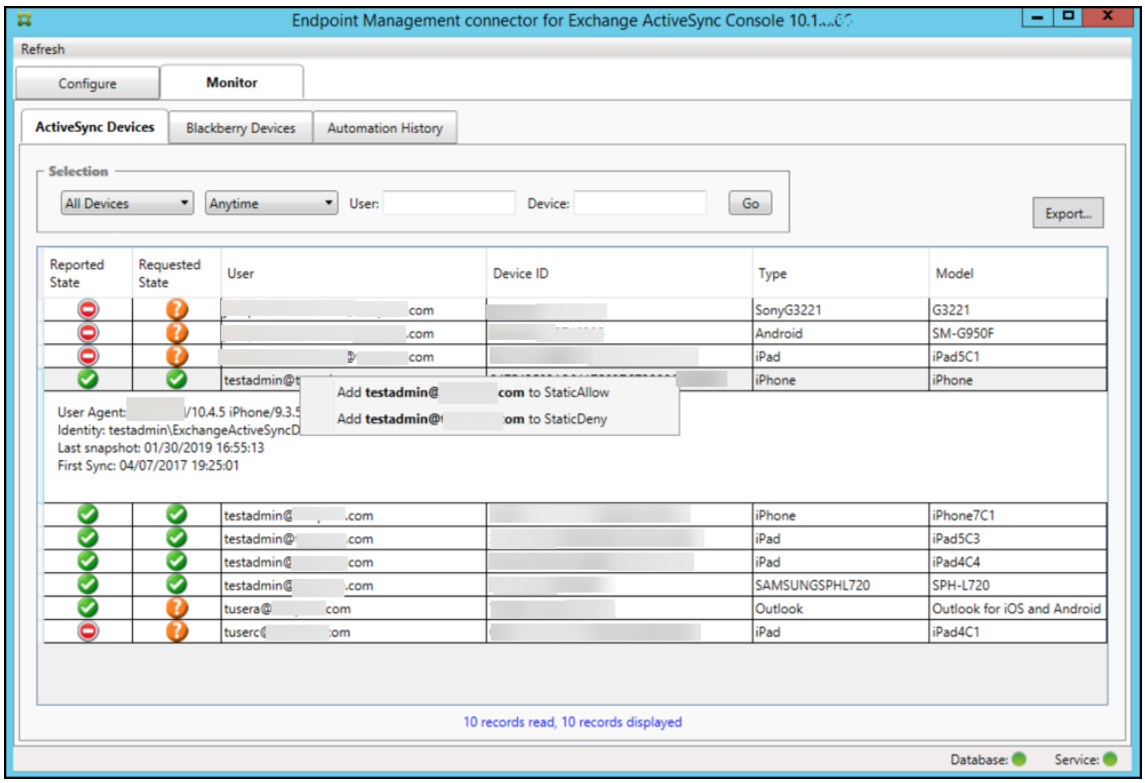


個々のユーザー、デバイス、またはデバイスの種類を静的規則に追加するには

[ActiveSync Devices] タブで、ユーザー、デバイス ID、またはデバイスの種類に基づく静的規則を追加できます。

1. [**ActiveSync Devices**] タブをクリックします。
2. 一覧で、ユーザー、デバイス、またはデバイスの種類を右クリックして、選択内容を許可するか、または拒否するかを選択します。

   次の図は、user1 を選択したときの許可/拒否オプションを示しています。



デバイス監視

Endpoint Management コネクタ：Exchange ActiveSync 用の［**Monitor**］タブでは、検出された Exchange ActiveSync デバイスおよび BlackBerry デバイスと、これまで自動で発行された PowerShell コマンドの履歴を参照できます。［**Monitor**］タブには、次の 3 つのタブがあります。

- **ActiveSync Devices**:
  - ［**Export**］をクリックして、表示されている ActiveSync デバイスパートナーシップをエクスポートできます。
  - ［**User**］、［**Device ID**］、または［**Type**］列を右クリックし、許可またはブロックから適切な規則の種類を選択して、ローカル（静的）規則を追加できます。
  - 展開した行を折りたたむには、Ctrl キーを押しながらその行をクリックします。
- **Blackberry Devices**
- **Automation History**

［**Configure**］タブにはすべてのスナップショットの履歴が表示されます。スナップショットの履歴には、スナップショットの作成時刻、作成にかかった時間、検出されたデバイス数、発生したすべてのエラーが表示されます。

- ［**Exchange**］タブで、目的の Exchange Server の情報アイコンをクリックします。
- ［**MSP**］タブで、目的の BlackBerry Server の情報アイコンをクリックします。

トラブルシューティングおよび診断

Endpoint Management コネクタ: Exchange ActiveSync 用では、エラーなどの動作情報が以下のログファイルに記録されます: *Install Folder*\log\XmmWindowsService.log Endpoint Management コネクタ: Exchange ActiveSync 用は、重要なイベントを Windows イベントログにも記録します。

ログレベルを変更するには

Endpoint Management コネクタ: Exchange ActiveSync 用には［エラー］、［情報］、［警告］、［デバッグ］、［トレース］というログレベルがあります。

> 注:
>
> 各レベルで生成される情報は、この順に詳しく（データが多く）なっていきます。たとえば、［エラー］レベルは最も情報量が少なく、［トレース］レベルは最も情報量が多くなります。

ログレベルを変更するには、次の手順を実行します:

1. C:\Program Files\Citrix\Citrix Endpoint Management connector にある nlog.config ファイルを開きます。
2. ファイル内の<rules>セクションで、*minilevel* パラメータを任意のログレベルに変更します。次に例を示します:

```
1     <rules>
2
3     <logger name="*" writeTo="file" minlevel="Debug" />
4
5     </rules>
```

3. ファイルを保存します。

   変更内容は直ちに有効になるため、Exchange ActiveSync 用コネクタを再起動する必要はありません。

一般的なエラー

一般的なエラーを以下に示します:

- Endpoint Management コネクタ: Exchange ActiveSync 用サービスが開始されない

  ログファイルと Windows イベントログでエラーを確認します。一般的な原因は次のとおりです:

  - Endpoint Management コネクタ: Exchange ActiveSync 用サービスが、SQL Server にアクセスできません。これは、次の問題が原因である可能性があります:
    * SQL Server サービスが実行されていない。
    * 認証エラー。

統合 Windows 認証が構成されている場合、Endpoint Management コネクタ: Exchange ActiveSync 用サービスのユーザーアカウントは、許可された SQL ログオンでなければなりません。Endpoint Management コネクタ: Exchange ActiveSync 用サービスのアカウントは、デフォルトではローカルシステムですが、ローカルの管理者権限を持つ任意のアカウントに変更できます。SQL 認証が構成されている場合、SQL ログオンが SQL で適切に構成されている必要があります。

- Mobile Service Provider（MSP）に対して構成されたポートが使用できない。システムのほかのプロセスで使用されていないリッスンポートを選択する必要があります。

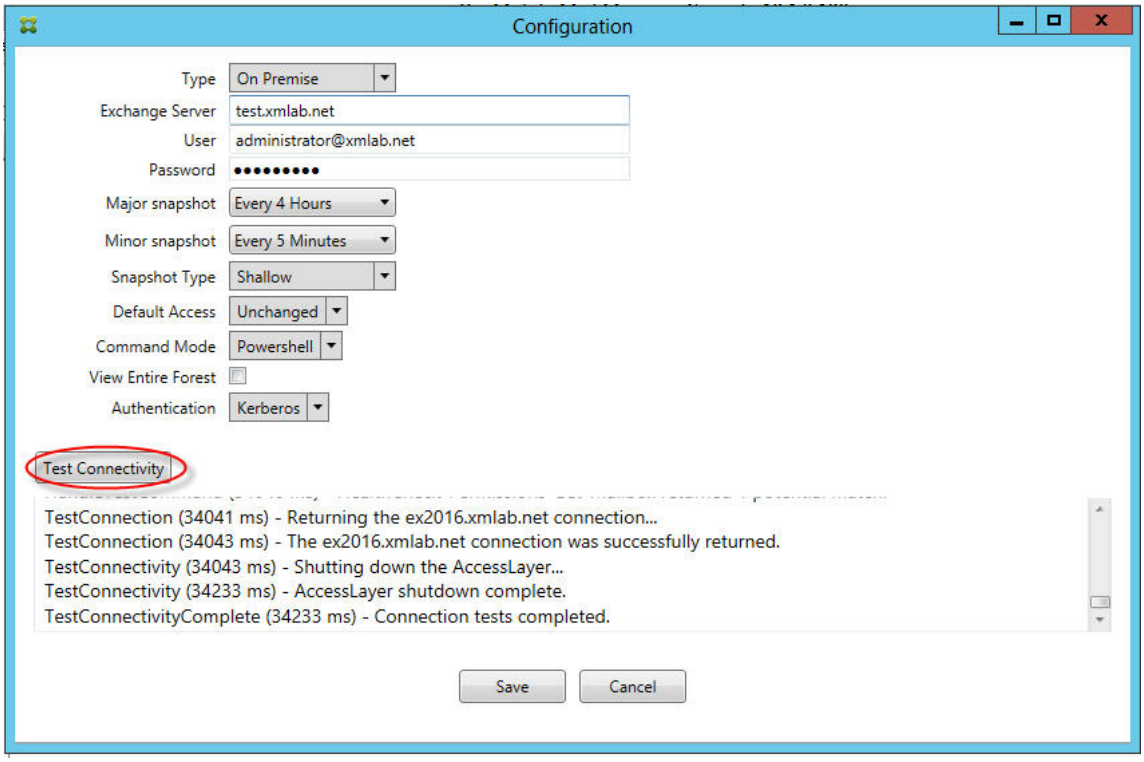
- XenMobile が MSP に接続できない

  Endpoint Management コネクタ: Exchange ActiveSync 用コンソールの［**Configure**］**>**［**MSP**］タブで、MSP サービスポートとトランスポートが適切に構成されていることを確認します。承認グループまたはユーザーが適切に設定されていることを確認します。

  HTTPS が構成されている場合は、有効な SSL サーバー証明書がインストールされている必要があります。IIS がインストールされている場合は、証明書のインストールに IIS マネージャーを使用できます。IIS がインストールされていない場合、How to configure a porty with an SSL certificateで証明書のインストールの詳細を参照してください。

  Endpoint Management コネクタ: Exchange ActiveSync 用には、MSP サービスへの接続をテストするためのユーティリティプログラムが含まれています。*InstallFolder*\MspTestServiceClient.exe プログラムを実行して、URL と資格情報を XenMobile で構成される URL と資格情報に設定して、［**Test Connectivity**］をクリックします。これにより、XenMobile Server が発行する Web サービス要求がシミュレートされます。HTTPS が構成されている場合は、サーバーの実際のホスト名（SSL 証明書で指定された名前）を指定する必要があります。

  ［**Test Connectivity**］ をクリックするときは、少なくとも 1 つ ActiveSyncDevice レコードがあることを確認してください。レコードがないとテストが失敗する可能性があります。



トラブルシューティングツール

Support\PowerShell フォルダーに、トラブルシューティング用の PowerShell ユーティリティー式が用意されています。

トラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細 RBAC 分析を行います。すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

Citrix Gateway コネクタ：Exchange ActiveSync 用

September 24, 2019

XenMobile NetScaler Connector は Exchange ActiveSync 用の Citrix Gateway コネクタになりました。シトリックス統合製品ラインについて詳しくは、シトリックス製品名ガイドを参照してください。

Exchange ActiveSync のコネクタでは、Exchange ActiveSync プロトコルのリバースプロキシとして動作する NetScaler に、ActiveSync クライアントのデバイスレベルの認証サービスを提供します。認証は、XenMobile 内で定義されているポリシーの組み合わせと、Citrix Gateway コネクタ：Exchange ActiveSync 用によりローカルで定義されているルールによって制御されます。

詳しくは、「ActiveSync ゲートウェイ」を参照してください。

詳細なリファレンスアーキテクチャ図については、「アーキテクチャ」を参照してください。

Exchange ActiveSync 用の Citrix Gateway コネクタの現在のリリースは、バージョン 8.5.2 です。

新機能

以下のセクションでは、Citrix Gateway コネクタ：Exchange ActiveSync 用（旧称：XenMobile NetScaler Connector）の最新および以前のバージョンの新機能を示します。

バージョン **8.5.3** の新機能

- このリリースでは、ActiveSync プロトコル 16.0 および 16.1 のサポートが追加されています。
- Google Analytics に送信される分析内容（特にスナップショット関連）にさらに詳細が追加されました。[CXM-52261]

バージョン **8.5.2** の新機能

- XenMobile NetScaler Connector は Exchange ActiveSync 用の Citrix Gateway コネクタになりました。

このリリースでは、以下の問題が解決されています。

- ポリシー規則の定義に複数の基準が使用され、条件の 1 つにユーザー ID が含まれている場合、次の問題が発生する可能性があります。ユーザーに別名がある場合、ルール適用時に別名もチェックされません。[CXM-55355]

> 注：
>
> 以下の新機能セクションでは、「Citrix Gateway コネクタ：Exchange ActiveSync 用」を旧称の XenMobile NetScaler Connector で呼びます。名前はバージョン 8.5.2 から変更されました。

バージョン **8.5.1.11** の新機能

- システム要件の変更： 現在のバージョンの NetScaler Connector では、Microsoft .NET Framework 4.5 が必要です。
- **Google Analytics** のサポート： 製品の改善可能な箇所に集中できるように、私たちはユーザーの皆様が XenMobile NetScaler Connector をどのように使用しているかについて知りたいと考えています。
- **TLS 1.1** および **1.2** のサポート： セキュリティの弱化のため、TLS 1.0 は PCI 評議会の推奨でなくなりました。XenMobile NetScaler Connector に TLS 1.1 および 1.2 のサポートが追加されました。

Citrix Gateway コネクタ: Exchange ActiveSync 用の監視

Citrix Gateway コネクタ: Exchange ActiveSync 用構成ユーティリティでは、Secure Mobile Gateway によって許可またはブロックされる、Exchange Server 経由のすべてのトラフィックを表示するために使用できる詳細なログが提供されます。

認証のために NetScaler によって Exchange ActiveSync 用コネクタに転送される ActiveSync 要求の履歴を確認するには、［**Log**］ タブを使用します。

また、Citrix Gateway コネクタ: Exchange ActiveSync 用 Web サービスが実行されていることを確認するには、コネクタサーバー上のブラウザーに URL（`https://<host:port>/services/ActiveSync/Version`）をロードします。この URL をロードした結果、製品バージョンが文字列で返される場合は、Web サービスが応答しています。

Citrix Gateway コネクタ: Exchange ActiveSync 用で ActiveSync トラフィックをシミュレートするには

Citrix Gateway コネクタ: Exchange ActiveSync 用を使用して、ポリシーとともに ActiveSync トラフィックがどのようになるかシミュレートすることができます。コネクタ構成ユーティリティで、［**Simulator**］ タブをクリックします。構成した規則にしたがってポリシーがどのように適用されるかが表示されます。

Citrix Gateway コネクタ: Exchange ActiveSync 用のフィルタの選択

Citrix Gateway コネクタ: Exchange ActiveSync 用のフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。デバイスが条件に合致すると、デバイスは［Device List］に置かれます。この［Device List］は、許可一覧およびブロック一覧のどちらでもありません。これは、定義された条件に合ったデバイスの一覧です。XenMobile 内では、Citrix Gateway コネクタ: Exchange ActiveSync 用で次のフィルターを使用できます。各フィルターの 2 つのオプションは、［**Allow**］ または ［**Deny**］ です。

- 匿名デバイス: XenMobile に登録されているが、ユーザーの ID が不明なデバイスが許可または拒否されます。たとえばこのユーザーは、登録されているが Active Directory パスワードの有効期限が切れている、または不明な資格情報を使って登録されている場合があります。
- **Samsung KNOX** 構成証明に失敗しました: Samsung デバイスは、セキュリティと診断の機能を備えています。このフィルターは、デバイスが KNOX 用に設定されているかどうかを確認します。詳しくは、「Samsung KNOX」を参照してください。
- 禁止アプリ: ブラックリストポリシーによって定義されたデバイスの一覧およびブラックリスト内のアプリの存在に基づいて、デバイスが許可または拒否されます。
- 暗黙的な許可/拒否: そのほかのフィルタールール条件に合致しないすべてのデバイスの一覧が作成され、この一覧に基づいてデバイスが許可または拒否されます。［暗黙的な許可/拒否］オプションを使用すると、［デバイス］タブにある Citrix Gateway コネクタ: Exchange ActiveSync 用の状態が確実に有効化され、デバイスのコネクタの状態が表示されます。また、［暗黙的な許可/拒否］オプションにより、選択されていないほか

のすべてのコネクタのフィルターが制御されます。たとえば、［Blacklists Apps］は、コネクタによって拒否（ブロック）されます。その一方で、［暗黙的な許可/拒否］オプションが ［許可］ に設定されているので、ほかのすべてのフィルターは許可されます。

- 非アクティブデバイス： XenMobile との通信が特定の期間に行われていないデバイスの一覧が作成されます。これらのデバイスは非アクティブだと見なされます。これに従って、フィルターはデバイスを許可または拒否します。
- 不足必須アプリ： ユーザーが登録すると、インストールする必要のある必須アプリの一覧がこのユーザーに送信されます。［不足必須アプリ］のフィルターは、ユーザーが 1 つまたは複数のアプリを削除するなどして、必須アプリのうち 1 つまたは複数のアプリが不足していることを示します。
- 非推奨アプリ： ユーザーが登録すると、インストールする必要のあるアプリの一覧がこのユーザーに送信されます。［非推奨アプリ］のフィルターは、この一覧に含まれていないアプリがデバイスにインストールされていないかをチェックします。
- 非準拠パスワード： デバイスでパスコードが設定されていないすべてのデバイスの一覧が作成されます。
- コンプライアンス外デバイス： 独自の内部 IT コンプライアンス条件に合致するデバイスが拒否または許可されます。コンプライアンスは、Out of Compliance という名前のデバイスプロパティによって定義される任意の設定であり、**True** または **False** のいずれかになるブール型のフラグです（このプロパティを手動で作成して値を設定するか、デバイスが特定の条件に合致する場合、または合致しない場合は、自動化された操作を使用してデバイス上でこのプロパティを作成できます）。
  - **Out of Compliance = True**。デバイスが、IT 部門によって設定されたコンプライアンス基準およびポリシー定義に合致しない場合、デバイスはコンプライアンス違反になります。
  - **Out of Compliance = False**。デバイスが、IT 部門によって設定されたコンプライアンス基準およびポリシー定義に合致する場合、デバイスはコンプライアンスに準拠しています。
- 失効状態： 取り消されたすべてのデバイスの一覧が作成され、取り消された状態に基づいてデバイスが許可または拒否されます。
- **Root** 化済み **Android** デバイス/ジェイルブレイクされた **iOS** デバイス。ルートされていることを示すフラグが付けられたすべてのデバイスの一覧が作成され、ルートされた状態に基づいてデバイスが許可または拒否されます。
- 非管理デバイス。XenMobile データベース内のすべてのデバイスの一覧が作成されます。Mobile Application Gateway は、ブロックモードで展開する必要があります。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用への接続を構成するには

Citrix Gateway コネクタ：Exchange ActiveSync 用は、セキュアな Web サービスを通じて XenMobile およびその他のリモート設定プロバイダと通信します。

1. コネクタの構成ユーティリティで、［**Config Providers**］ タブをクリックし、［**Add**］ をクリックします。
2. ［**Config Providers**］ ダイアログボックスの ［**Name**］ に、XenMobile Server での HTTP 基本認証に使用する、管理者権限を持つユーザー名を入力します。
3. ［**Url**］に、XenMobile GCS の Web アドレス（通常は`https://<FQDN>/<instanceName>/services/<MagConfigService>`という形式）を入力します。*MagConfigService* の名前は大文字と小文字が区

別されます。

4. [**Password**] に、XenMobile Server での HTTP 基本認証に使用するパスワードを入力します。
5. [**Managing Host**] に、コネクタのサーバー名を入力します。
6. [**Baseline Interval**] で、新しく更新された動的規則のセットが Device Manager から取得される期間を指定します。
7. [**Delta interval**] で、動的規則の更新が取得される期間を指定します。
8. [**Request Timeout**] で、サーバー要求のタイムアウト間隔を指定します。
9. [**Config Provider**] で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
10. [**Events Enabled**] で、デバイスがブロックされたときにコネクタから XenMobile に通知する場合はこのオプションを有効にします。XenMobile の自動化された操作でコネクタ規則を使用する場合、このオプションが必要です。
11. [**Save**] をクリックし、[**Test Connectivity**] をクリックして、ゲートウェイから構成プロバイダーへの接続をテストします。接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い合わせてください。
12. 接続が成功した場合、[**Disabled**] チェックボックスをオフにし、[**Save**] をクリックします。

新しい設定プロバイダを追加すると、Citrix Gateway コネクタ: Exchange ActiveSync 用によって、プロバイダに関連付けられた 1 つ以上のポリシーが自動的に作成されます。これらのポリシーは、config\policyTemplates.xml の NewPolicyTemplate セクションに含まれているテンプレート定義によって定義されます。このセクション内で定義される各ポリシー要素に対して、新しいポリシーが作成されます。

以下が当てはまる場合は、演算子を使用して、ポリシー要素を追加、削除、または変更できます。ポリシー要素がスキーマ定義に適合しており、標準の置換文字列（中かっこで囲まれている）が変更されていない場合。次に、プロバイダーの新しいグループを追加し、ポリシーを更新してこの新しいグループを含めます。

XenMobile からポリシーをインポートするには

1. Citrix Gateway コネクタ: Exchange ActiveSync 用構成ユーティリティで、[**Config Providers**] タブをクリックし、[**Add**] をクリックします。
2. [構成プロバイダー] ダイアログボックスの [名前] に、XenMobile Server での HTTP 基本認証に使用する、管理者権限を持つユーザー名を入力します。
3. [**Url**] に、XenMobile Gateway Configuration Service（GCS）の Web アドレス（通常は`https://<xdmHost>/xdm/services/<MagConfigService>`という形式）を入力します。MagConfigService の名前は大文字と小文字が区別されます。
4. [**Password**] に、XenMobile Server での HTTP 基本認証に使用するパスワードを入力します。
5. [**Test Connectivity**] をクリックし、ゲートウェイから構成プロバイダーへの接続をテストします。接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い合わせてください。

6. 接続が成功した場合、［**Disabled**］チェックボックスをオフにし、［**Save**］をクリックします。
7. ［**Managing Host**］ で、ローカルホストコンピューターの DNS 名をデフォルトのままにします。1 つのアレイ内で複数の Forefront Threat Management Gateway（TMG）が構成されている場合、この設定を使用して、XenMobile との通信を調整します。

   設定を保存してから、GCS を開きます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用ポリシーモードの構成

Citrix Gateway コネクタ：Exchange ActiveSync 用は、次の 6 つのモードで実行できます。

- **Allow All**。このポリシーモードでは、コネクタを経由するすべてのトラフィックのアクセスが許可されます。そのほかのフィルター規則は使用されません。
- **Deny All**。このポリシーモードでは、コネクタを経由するすべてのトラフィックのアクセスがブロックされます。そのほかのフィルター規則は使用されません。
- **Static Rules: Block Mode**。このポリシーモードでは、最後に暗黙的な拒否ステートメントまたはブロックステートメントを使って静的規則が実行されます。ほかのフィルター規則によって許可または許容されないデバイスは、コネクタでブロックされます。
- **Static Rules: Permit Mode**。このポリシーモードでは、最後に暗黙的な許容ステートメントまたは許可ステートメントを使って静的規則が実行されます。ほかのフィルター規則によってブロックまたは拒否されないデバイスは、コネクタで許可されます。
- **Static + ZDM Rules**： Block Mode。このポリシーモードでは、最初に静的規則が実行され、最後に暗黙的な拒否ステートメントまたはブロックステートメントを使って XenMobile から動的規則が実行されます。デバイスは、定義済みのフィルターおよび Device Manager の規則に基づいて許容または拒否されます。定義済みのフィルターおよび規則に一致しないデバイスはブロックされます。
- **Static + ZDM Rules**： Permit Mode。このポリシーモードでは、最初に静的規則が実行され、最後に暗黙的な許容ステートメントまたは許可ステートメントを使って XenMobile から動的規則が実行されます。デバイスは、定義済みのフィルターおよび XenMobile の規則に基づいて許容または拒否されます。定義済みのフィルターおよび規則に一致しないデバイスは許可されます。

Citrix Gateway コネクタ：Exchange ActiveSync 用の処理によって、XenMobile から受け取った iOS モバイルデバイスおよび Windows ベースのモバイルデバイス用の一意の ActiveSync ID に基づいて、動的規則が許容またはブロックされます。Android デバイスの場合、製造元によって動作が異なり、一部の Android デバイスでは、一意の ActiveSync ID が直ちに提供されません。代わりに、XenMobile により Android デバイスのユーザー ID 情報が送信され、許容するかブロックするかを決定します。その結果、ユーザーが 1 台の Android デバイスしか持っていない場合でも、許容およびブロック機能が正常に動作します。ユーザーが複数の Android デバイスを持っている場合は、Android デバイスを区別できないため、すべてのデバイスが許可されます。これらのデバイスが既知の場合は、ActiveSyncID で静的にブロックするようにゲートウェイを構成できます。また、デバイスの種類またはユーザーエージェントに基づいてブロックするようにゲートウェイを構成することもできます。

ポリシーモードを指定するには、SMG Controller Configuration ユーティリティで次の操作を実行します。

1. ［**Path Filters**］タブをクリックし、［**Add**］をクリックします。
2. ［**Path Properties**］ ダイアログボックスの ［**Policy**］ リストからポリシーモードを選択し、［**Save**］ をクリックします。

［**Policies**］タブで規則を確認できます。この規則は、Citrix Gateway コネクタ：Exchange ActiveSync 用で上から順に処理されます。［Allow］が設定されたポリシーは緑のチェックマークで示されます。［Deny］が設定されたポリシーは中央に線が入った赤い丸で示されます。画面を更新して、最近更新された規則を表示するには、［**Refresh**］をクリックします。config.xml ファイル内の規則の順序を変更することもできます。

規則をテストするには、［**Simulator**］タブをクリックします。フィールドに値を指定します。これらの値をログから取得することもできます。［Allow］または［Block］が指定された結果メッセージが表示されます。

静的規則を構成するには

ActiveSync 接続の HTTP 要求の ISAPI フィルターによって読み取られる値を使用して静的規則を入力します。静的規則を使用すると、Citrix Gateway コネクタ：Exchange ActiveSync 用で次の条件に基づいてトラフィックを許可またはブロックすることができます。

- **User**。Citrix Gateway コネクタ：Exchange ActiveSync 用は、デバイスの登録時に取得された許可されたユーザーの値と名前の構造を使用します。これは通常、LDAP 経由で Active Directory に接続された XenMobile を実行しているサーバーによって参照される domain\username に示されています。コネクタ構成ユーティリティ内の ［**Log**］ タブには、コネクタを経由して渡される値が表示されます。値の構造を決定する必要がある場合、または値の構造が異なる場合に、値が渡されます。
- **Deviceid (ActiveSyncID)**。接続されたデバイスの ActiveSyncID とも呼ばれます。この値は、通常、XenMobile コンソールの特定のデバイスプロパティページ内にあります。また、コネクタ構成ユーティリティの［Log］タブから、この値を確認できます。
- **DeviceType**。コネクタでは、デバイスが iPhone、iPad、またはそのほかの種類のデバイスかどうかを特定し、その条件に基づいてデバイスを許可またはブロックできます。ほかの値の場合と同じように、コネクタ構成ユーティリティを使用して、ActiveSync 接続のために処理中の接続済みデバイスの種類をすべて表示できます。
- **UserAgent**。使用する ActiveSync クライアントの情報が含まれます。ほとんどの場合、指定された値は、モバイルデバイスプラットフォームのオペレーティングシステムの特定のビルドおよびバージョンに対応します。

サーバーで実行中のコネクタ構成ユーティリティによって、静的規則は常に管理されます。

1. SMG Controller Configuration ユーティリティで、［**Static Rules**］ タブをクリックし、［**Add**］ をクリックします。
2. ［**Static Rule Properties**］ダイアログボックスで、条件として使用する値を指定します。たとえば、ユーザー名（たとえば、「AllowedUser」）を入力して、アクセスを許可するユーザーを指定し、［**Disabled**］ チェックボックスをオフにします。
3. ［保存］ をクリックします。

これで、静的規則が有効になりました。また、正規表現を使用して値を定義できますが、config.xml ファイルで規則処理モードを有効化する必要があります。

動的な規則を構成するには

XenMobile のデバイスポリシーおよびプロパティは動的な規則を定義し、Citrix Gateway コネクタ: Exchange ActiveSync 用の動的フィルターをトリガーできます。トリガーは、ポリシー違反またはプロパティ設定の有無に基づいています。コネクタのフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。デバイスが条件に合致すると、デバイスは［Device List］に置かれます。この［Device List］は、許可一覧およびブロック一覧のどちらでもありません。これは、定義した条件に合致するデバイスの一覧です。次の構成オプションでは、コネクタを使用して［Device List］のデバイスを許可または拒否するかどうかを定義できます。

> 注:
>
> 動的規則を構成するには、XenMobile コンソールを使用する必要があります。

1. XenMobile コンソールで、右上の歯車アイコンをクリックします。［設定］ ページが開きます。
2. ［サーバー］ の下の ［**ActiveSync** ゲートウェイ］ をクリックします。ActiveSync ゲートウェイのページが開きます。
3. ［次の規則をアクティブ化］ で、有効にするルールを 1 つまたは複数オンにします。
4. ［Android のみ］の ［**Android** ドメインユーザーを **ActiveSync** ゲートウェイに送信］ で ［はい］ をクリックし、XenMobile によって Android デバイスの情報が Secure Mobile Gateway に送信されるようにします。

   このオプションを有効にすると、Android デバイスユーザーの ActiveSync 識別子が XenMobile にない場合でも、XenMobile によって Android デバイスの情報が Citrix Gateway コネクタ: Exchange ActiveSync 用に送信されます。

Citrix Gateway コネクタ: **Exchange ActiveSync** 用の **XML** ファイルを編集してカスタムポリシーを構成するには

Citrix Gateway コネクタ: Exchange ActiveSync 用構成ユーティリティの ［**Policies**］ タブで、デフォルトの構成の基本ポリシーを確認できます。カスタムポリシーを作成する場合、コネクタの XML 構成ファイル (config\config.xml) を編集できます。

1. ファイル内の **PolicyList** セクションに移動し、新しい **Policy** 要素を追加します。
2. 別の静的グループや別の GCP をサポートするグループなどの新しいグループも必要な場合は、新しい **Group** 要素を **GroupList** セクションに追加します。
3. 必要に応じて、**GroupRef** 要素を並べ替えることにより、既存のポリシー内のグループの順序を変更できます。

Citrix Gateway コネクタ: **Exchange ActiveSync** 用の **XML** ファイルの構成

Citrix Gateway コネクタ: Exchange ActiveSync 用では、XML 構成ファイルを使用して、コネクタのアクションが指示されます。このファイルにより、ほかのエントリと同様に、グループファイルと、HTTP 要求を評価するときにフィルターにより実行される関連アクションが指定されます。デフォルトでは、このファイルには config.xml という名前が付けられ、次の場所に配置されます: ..\Program Files\Citrix\XenMobile NetScaler Connector\config\

GroupRef ノード

GroupRef ノードにより、論理的なグループ名が定義されます。デフォルトでは、AllowGroup と DenyGroup です。

> 注:
>
> GroupRefList ノードに表示される GroupRef ノードの順序は重要です。

GroupRef ノードの ID 値により、特定のユーザーアカウントまたはデバイスを一致させるために使用するメンバーの論理的なコンテナまたはコレクションが特定されます。アクションの属性により、コレクション内の規則に一致するメンバーをフィルターで処理する方法が指定されます。たとえば、AllowGroup セット内の規則に一致するユーザーアカウントまたはデバイスは「合格」します。合格すると、Exchange CAS へのアクセスが許可されます。DenyGroup セット内の規則に一致するユーザーアカウントまたはデバイスは「拒否」されます。拒否されると、Exchange CAS へのアクセスが許可されません。

特定のユーザーアカウント/デバイスまたはその組み合わせが両方のグループの規則に一致する場合、優先する規則を使用して要求の結果が指定されます。優先順位は、config.xml ファイルの GroupRef ノードの最上位から最下位へと至る順序で表されています。GroupRef ノードは優先度によりランク付けされています。許可グループの特定条件の規則は、拒否グループの同じ条件の規則よりも常に優先されます。

グループノード

さらに、config.xml により、グループノードが定義されます。これらのノードによって、論理的なコンテナ、つまり AllowGroup および DenyGroup が外部 XML ファイルとリンクされます。外部ファイルに格納されたエントリは、フィルター規則の基礎を形成します。

> 注:
>
> このリリースでは、外部 XML ファイルのみがサポートされています。

デフォルトのインストールでは、構成に 2 つの XML ファイル（allow.xml と deny.xml）が実装されます。

Citrix Gateway コネクタ: **Exchange ActiveSync** 用の構成

[**Active Sync Service ID**]、[**Device type**]、[**User Agent**]（デバイスのオペレーティングシステム）、[**Authorized user**]、[**ActiveSync Command**] といったプロパティに基づいて、ActiveSync 要求を選択的

にブロックまたは許可するように Citrix Gateway コネクタ：Exchange ActiveSync 用を構成できます。

デフォルトの構成では、静的グループと動的グループの組み合わせがサポートされています。静的グループは、SMG Controller Configuration ユーティリティを使用して保守します。静的グループは、特定のユーザーエージェントを使用するすべてのデバイスなど、デバイスの既知のカテゴリで構成される場合があります。

動的グループは、ゲートウェイ構成プロバイダーと呼ばれる外部ソースによって保守されます。グループは Citrix Gateway コネクタ：Exchange ActiveSync 用によって定期的に接続されます。XenMobile を使用して、許可されたデバイスとユーザーおよびブロックされたデバイスとユーザーのグループをコネクタにエクスポートできます。

動的グループは、ゲートウェイ構成プロバイダーと呼ばれる外部ソースによって保守され、XCitrix Gateway コネクタ：Exchange ActiveSync 用によって定期的に収集されます。XenMobile を使用して、許可されたデバイスとユーザーおよびブロックされたデバイスとユーザーのグループをコネクタにエクスポートできます。

ポリシーとは、アクション（許可またはブロック）が関連付けられた各グループの順序指定された一覧と、グループメンバーの一覧のことです。ポリシーには、任意の数のグループを含めることができます。ポリシー内のグループの順序は重要です。これは、1 つの一致が見つかると、グループのアクションが実行され、以降のグループは評価されないからです。

メンバーにより、要求のプロパティに一致する方法が定義されます。デバイス ID などの単一のプロパティ、またはデバイスの種類およびユーザーエージェントなどの複数のプロパティに一致することが可能です。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のセキュリティモデルの選択

あらゆる規模の組織にとって、モバイルデバイスを適切に展開するには、セキュリティモデルの確立が不可欠です。保護または隔離されたネットワーク制御を使用して、ユーザー、コンピューター、またはデバイスへのアクセスをデフォルトで許可することは一般的ですが、これは必ずしも望ましい方法ではありません。IT セキュリティを管理する各組織では、モバイルデバイスのセキュリティに対して多少異なったアプローチまたは組織に合わせたアプローチをとっている場合があります。

モバイルデバイスのセキュリティについても、同じことが言えます。多くのモバイルデバイスおよびその種類、ユーザーごとのモバイルデバイス数、利用できるオペレーティングシステムプラットフォームおよびアプリを考慮すると、許可モデルの使用はお勧めできません。多くの組織では、制限モデルの使用が最適な選択となります。

Citrix Gateway コネクタ：Exchange ActiveSync 用と XenMobile の統合で許可される構成シナリオは次のとおりです。

許可モデル（[**Permit Mode**]）

許可セキュリティモデルは、デフォルトでアクセスがすべて許可または付与されているという前提で動作します。規則およびフィルターの使用時のみ、ブロックされたり、制限が適用されたりします。許可セキュリティモデルは、モバイルデバイスに対するセキュリティ上の懸念が比較的少ない組織に適しています。このモデルでは、アクセスを拒否するのが適切な場合（ポリシー規則が失敗した場合）にのみ、制限コントロールが適用されます。

制限モデル（[**Block Mode**]）

制限セキュリティモデルは、デフォルトでアクセスが許可または付与されていないという前提に基づきます。セキュリティチェックポイントを通過するすべてのデータがフィルターおよび検査され、アクセスを許可する規則をパスしない限り、アクセスが拒否されます。制限セキュリティモデルは、モバイルデバイスに対するセキュリティ上の条件が比較的に厳しい組織に適しています。このモードでは、アクセスを許可するすべての規則をパスした場合にのみ、ネットワークサービスの使用と機能へのアクセスが許可されます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用の管理

Citrix Gateway コネクタ：Exchange ActiveSync 用を使用してアクセス制御規則を作成できます。この規則は、管理対象デバイスからの ActiveSync 接続要求へのアクセスを許可またはブロックします。アクセスは、デバイスのステータス、アプリのブラックリストまたはホワイトリスト、およびその他のコンプライアンス設定状況に基づきます。

Citrix Gateway コネクタ：Exchange ActiveSync 用構成ユーティリティを使用して、社内のメールポリシーを適用する動的および静的規則を作成し、コンプライアンス基準に違反しているユーザーをブロックすることができます。また、Exchange Server を経由して管理対象デバイスに送信されるすべての添付ファイルを暗号化して、管理対象デバイスで権限のあるユーザーのみが添付ファイルを表示できるようにメールの添付ファイル暗号化をセットアップすることができます。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用をアンインストールするには

1. 管理者アカウントで XncInstaller.exe を実行します。
2. 画面の指示に従って、アンインストールを完了します。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用をインストール、アップグレード、またはアンインストールするには

1. 管理者アカウントで XncInstaller.exe を実行してコネクタをインストールするか、既存のコネクタをアップグレードまたは削除できます。
2. 画面の指示に従って、インストール、アップグレード、またはアンインストールを完了します。

コネクタをインストールした後、XenMobile の構成サービスおよび通知サービスを手動で再起動する必要があります。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用のインストール

Citrix Gateway コネクタ：Exchange ActiveSync 用を専用の Windows Server にインストールします。

コネクタがサーバーに与える CPU 負荷は、管理対象デバイスの数によって異なります。多数のデバイス（50,000 個以上）がある場合に、クラスター環境がないときは、追加のコアが必要になることがあります。コネクタのメモリサイズは、追加メモリを保証するのに十分ではありません。

Citrix Gateway コネクタ：Exchange ActiveSync 用のシステム要件

Citrix Gateway コネクタ：Exchange ActiveSync 用では、NetScaler アプライアンスで構成された SSL ブリッジを介して NetScaler との通信が行われます。SSL ブリッジを使用すると、アプライアンスですべてのセキュアなトラフィックを XenMobile に直接ブリッジすることができます。コネクタの最小構成要件は、以下のとおりです：

コンポーネント	条件
コンピューターとプロセッサ	Pentium III 733MHz 以上のプロセッサ。Pentium III 2.0GHz 以上のプロセッサ（推奨）
NetScaler	ソフトウェアバージョン 10 を備えた NetScaler アプライアンス
メモリ	1GB
ハードディスク	150MB のハードディスクスペースがある、NTFS でフォーマットしたローカルパーティション
オペレーティングシステム	Windows Server 2016、Windows Server 2012 R2 または Windows Server 2008 R2 Service Pack 1。英語ベースのサーバーが必要です。Windows Server 2008 R2 Service Pack 1 のサポートは、2020 年 1 月 14 日に終了します。
そのほかのデバイス	ホストオペレーティングシステムと互換性があるネットワークアダプター（内部ネットワークとの通信用）
Microsoft .NET Framework。	バージョン 8.5.1.11 では、Microsoft .NET Framework 4.5 が必要です。
表示	VGA 以上の解像度のモニター

Citrix Gateway コネクタ：Exchange ActiveSync 用のホストコンピューターには、次の最小ハードディスクスペースが必要です：

- アプリケーション： 10 ～ 15MB（推奨値は 100MB）
- ログ： 1GB（推奨値は 20GB）

Citrix Gateway コネクタ：Exchange ActiveSync 用のプラットフォームのサポートについて詳しくは、「サポートされるデバイスオペレーティングシステム」を参照してください。

デバイスのメールクライアント

すべてのメールクライアントが、デバイスに関して一貫して同じ ActiveSync ID を返すわけではありません。Citrix Gateway コネクタ: Exchange ActiveSync 用は、各デバイスに対して一意の ActiveSync ID を前提とするため、デバイスごとに一意の同じ ActiveSync ID を一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントはテスト済みで、エラーなく実行できます。

- HTC のネイティブメールクライアント
- Samsung のネイティブメールクライアント
- iOS のネイティブメールクライアント
- TouchDown

Citrix Gateway コネクタ: **Exchange ActiveSync** 用の展開

Citrix Gateway コネクタ: Exchange ActiveSync 用では、NetScaler を使用して、XenMobile による管理対象デバイスと XenMobile Server 間の通信をプロキシ接続したり、負荷分散したりできます。コネクタと XenMobile 間の通信は定期的に行われ、ポリシーが同期されます。コネクタと XenMobile をまとめて、または別々にクラスター化したり、NetScaler によって負荷を分散したりできます。

Citrix Gateway コネクタ: **Exchange ActiveSync** 用のコンポーネント

- **Citrix Gateway** コネクタ: **Exchange ActiveSync** 用サービス: このサービスでは、NetScaler によって呼び出される REST Web サービスのインターフェイスが提供され、デバイスからの ActiveSync 要求が承認されるかどうかが決定されます。
- **XenMobile** 構成サービス: このサービスでは、XenMobile との通信が行われ、XenMobile ポリシーの変更がコネクタと同期されます。
- **XenMobile** 通知サービス: このサービスでは、XenMobile への承認されていないデバイスのアクセスが通知されます。これにより XenMobile では、デバイスがブロックされた理由をユーザーに通知するなどの適切な処置を施すことができます。
- **Citrix Gateway** コネクタ: **Exchange ActiveSync** 用構成ユーティリティ: このアプリケーションにより、管理者はコネクタを構成および監視できます。

Citrix Gateway コネクタ: **Exchange ActiveSync** 用のリッスンアドレスをセットアップするには

Citrix Gateway コネクタ: Exchange ActiveSync 用が NetScaler から要求を受信して ActiveSync トラフィックを承認できるようにするには、次の手順を実行します。コネクタが NetScaler Web サービス呼び出しをリッスンするポートを指定します。

1. [スタート] ボタンをクリックして、Citrix Gateway コネクタ: Exchange ActiveSync 用構成ユーティリティを選択します。

2. [**Web Service**] タブをクリックし、XenMobile NetScaler Connector Web サービスのリッスンアドレスを入力します。**HTTP** と **HTTPS** のいずれかまたは両方を選択できます。コネクタが XenMobile と共存している場合（同じサーバーにインストールされている場合）、XenMobile と競合しないポート値を選択します。
3. この値を構成した後、［**Save**］をクリックして、［**Start Service**］をクリックし、Web サービスを起動します。

Citrix Gateway コネクタ：**Exchange ActiveSync** 用でデバイスのアクセス制御ポリシーを構成するには

管理対象デバイスに適用するアクセス制御ポリシーを構成するには、次の操作を実行します。

1. Citrix Gateway コネクタ：Exchange ActiveSync 用構成ユーティリティで［**Path Filters**］タブをクリックします。
2. 最初の行の［**Microsoft-Server-ActiveSync is for ActiveSync**］を選択し、［**Edit**］をクリックします。
3. ［**Policy**］の一覧から、目的のポリシーを選択します。XenMobile ポリシーが含まれるポリシーの場合、［**Static + ZDM: Permit Mode**］または［**Static + ZDM: Block Mode**］を選択します。これらのポリシーでは、ローカル（または、静的）規則と XenMobile の規則が組み合わされます。［Permit Mode］では、規則によって明示的に特定されないすべてのデバイスが ActiveSync へのアクセスを許可されます。［Block Mode］では、そのようなデバイスがブロックされます。
4. ポリシーを設定したら、［**Save**］をクリックします。

XenMobile との通信を構成するには

Citrix Gateway コネクタ：Exchange ActiveSync 用および NetScaler で使用する XenMobile Server（構成プロバイダーともいいます）の名前およびプロパティを指定します。

> 注：
>
> このタスクでは、XenMobile がインストールされていて、構成済みであることを前提としています。

1. Citrix Gateway コネクタ：Exchange ActiveSync 用構成ユーティリティで、［**Config Providers**］タブをクリックし、［**Add**］をクリックします。
2. この展開で使用する XenMobile Server の名前および URL を入力します。マルチテナント展開で複数の XenMobile Server がある場合は、この名前は各サーバーインスタンスで固有である必要があります。たとえば、［**Name**］に「**XMS**」を入力します。
3. ［**Url**］に、XenMobile GlobalConfig Provider（GCP）の Web アドレス（通常は`https://<FQDN>/<instanceName>/services/<MagConfigService>`という形式）を入力します。*MagConfigService* の名前は大文字と小文字が区別されます。
4. ［**Password**］に、XenMobile Web サーバーでの HTTP 基本認証に使用するパスワードを入力します。
5. ［**Managing Host**］に、Citrix Gateway コネクタ：Exchange ActiveSync 用をインストールしたサーバー名を入力します。

6. ［**Baseline Interval**］ で、新しく更新された動的規則のセットが XenMobile から取得される期間を指定します。
7. ［**Request Timeout**］ で、サーバー要求のタイムアウト間隔を指定します。
8. ［**Config Provider**］ で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
9. ［**Events Enabled**］ で、デバイスがブロックされたときに Secure Mobile Gateway から XenMobile に通知する場合はこのオプションを有効にします。Device Manager の自動化された操作で Secure Mobile Gateway の規則を使用する場合、このオプションが必要です。
10. サーバーを構成したら、［**Test Connectivity**］ をクリックして、XenMobile への接続をチェックします。
11. 接続が確立したら、［**Save**］ をクリックします。

冗長性とスケーラビリティのための **Citrix Gateway** コネクタ：**Exchange ActiveSync** 用の展開

Citrix Gateway コネクタ：Exchange ActiveSync 用および XenMobile 展開のスケーラビリティを向上させるには、コネクタのインスタンスを複数の Windows サーバーにインストールして同じ XenMobile インスタンスを参照させ、NetScaler を使用してこれらのサーバーの負荷を分散します。

Citrix Gateway コネクタ：Exchange ActiveSync 用の構成には、次の 2 種類のモードがあります：

- 非共有モードでは、Citrix Gateway コネクタ：Exchange ActiveSync 用の各インスタンスが XenMobile Server と通信し、結果として生成されるポリシーの独自のプライベートコピーを保持します。たとえば、XenMobile Server のクラスターがある場合、コネクタインスタンスを各 XenMobile Server で実行すると、コネクタにより、ローカル XenMobile からポリシーが取得されます。
- 共有モードでは、コネクタの 1 つのノードがプライマリノードに指定され、このノードと XenMobile との通信が行われます。Windows ネットワーク共有または Windows（または、サードパーティの）レプリケーションによって、結果として生成される構成がほかのノード間で共有されます。

コネクタの構成全体は、単一のフォルダー（数個の XML ファイルから構成されます）にあります。コネクタの処理によって、このフォルダー内のファイルに加えられた変更が検出され、構成が自動的に再ロードされます。共有モードのプライマリノードに対するフェイルオーバーはありません。ただし、システムでは、前回の正常な構成がコネクタの処理にキャッシュされるため、プライマリサーバーが数分間停止（たとえば、再起動のために）しても許容されます。

高度な設定

August 22, 2019

> 注：
>
> この記事では、XenMobile Server の高度な概念について説明します。エンドポイント管理の詳細については、「高度な概念」を参照してください。

XenMobile の高度な設定の記事では、XenMobile の製品ドキュメントをさらに詳しく紹介しています。その目的は専門家の技術を使用して開発期間の短縮を支援することです。その記事では、コンテンツを作成した 1 人または複数の技術者に言及する場合もあります。

エンドツーエンド XenMobile 環境の決定ポイント、推奨事項、よくある質問、およびユースケースについては、このセクションの「XenMobile 環境ハンドブック」を参照してください。

XenMobile のコミュニティサポートフォーラムについては、Citrix Discussionsを参照してください。

オンプレミス **XenMobile** の **Active Directory** とのやり取り

January 10, 2020

寄稿者：Siddartha Vuppala

この記事では、XenMobile サーバーと Active Directory のやり取りについて説明します。XenMobile サーバーと Active Directory のやり取りは、インラインとバックグラウンドの両方で行われます。以下のセクションでは、Active Directory とのやり取りを伴うインライン操作およびバックグラウンド操作の詳細について説明します。

> 注：
>
> この記事ではやり取りの概要のみを示し、細かい詳細については扱いません。XenMobile コンソールで Active Directory と LDAP を設定する方法について詳しくは、「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。

インラインでのやり取り

XenMobile サーバーは、管理者が構成する LDAP 設定を使用して Active Directory との通信を行います。この設定により、ユーザーとグループに関する情報が取得されます。XenMobile サーバーと Active Directory 間のやり取りが生じる操作を次に示します。

1. **LDAP** 構成。Active Directory 自体を構成するため、Active Directory とのやり取りが行われます。XenMobile サーバーは Active Directory で構成情報の認証を行うことで、構成情報の検証を試みます。この認証は、インターネットプロトコル、ポート、および指定のサービスアカウントの資格情報を使用して行われます。バインドが成功すれば、接続は適切に構成されています。
2. グループベースの対話。
    a) 役割ベースのアクセス制御（RBAC）時およびデリバリーグループの定義の作成時における 1 つ以上のグループの検索。XenMobile サーバーの管理者が、XenMobile コンソールで検索テキストを入力します。XenMobile サーバーにより、指定した文字列の一部が含まれるすべてのグループについて選択したドメインが検索されます。次に、XenMobile サーバーは検索で見つかったグループの objectGUID 属性、sAMAccountName 属性、識別名属性を取得します。

> 注：
>
> この情報は、XenMobile サーバーのデータベースには格納されません。

b) RBAC および展開グループの定義の追加または更新。XenMobile サーバーの管理者が上記の検索結果に基づいて目的の Active Directory グループを選択し、展開グループの定義に追加します。XenMobile サーバーにより、Active Directory 内で指定したグループが一度に 1 つずつ検索されます。XenMobile サーバーは objectGUID 属性を検索し、メンバーシップ情報を含む選択した属性を取得します。グループのメンバーシップ情報により、取得したグループと XenMobile サーバーデータベースの既存のユーザーまたはグループ間のメンバーシップが特定されます。グループのメンバーシップを変更すると、影響を受けるユーザーメンバーに関わる RBAC および展開グループが確認され、ユーザーの権利割り当てが行われます。

> 注：
>
> 展開グループの定義を変更すると、影響を受けるユーザーのアプリまたはポリシーの使用権が変更される場合があります。

c) ワンタイム **PIN**（**OTP**）招待状。XenMobile サーバー管理者が、XenMobile サーバーデータベースに存在する Active Directory グループの一覧からグループを選択します。このグループのすべてのユーザーが、直接的および間接的に Active Directory から取得されます。前の手順で特定されたユーザーに対して、OTP 招待状が送られます。

> 注：
>
> 上記 3 つのやり取りは、XenMobile サーバーの構成変更によりグループベースのやり取りが開始されることを示しています。構成に変更がない場合、これらのやり取りでは Active Directory との通信は行われません。また、定期的にバックグラウンドジョブでグループ側の変更を取得する必要もありません。

3. ユーザーベースの対話。

a) ユーザー認証。ユーザー認証のワークフローでは、Active Directory と 2 種類のやり取りが行われます。

- 指定した資格情報によるユーザーの認証
- XenMobile サーバーデータベースへの選択したユーザー属性（objectGUID、識別名、sAMAccountName、グループのダイレクトメンバーシップなど）の追加または更新。グループのメンバーシップを変更すると、アプリ、ポリシー、アクセス資格の再評価が行われます。

ユーザーは、デバイスと XenMobile サーバーコンソールのどちらからでも認証を行うことができます。どちらの場合でも、Active Directory とのやり取りの動作は同じです。

b) App Store へのアクセスおよび更新。ストアを更新すると、ダイレクトグループメンバーシップを含むユーザー属性が更新されます。この処理により、ユーザー資格の再評価が可能になります。

c) デバイスのチェックイン。管理者は、定期的に XenMobile コンソールでデバイスのチェックインを構成します。デバイスのチェックインが行われるたびに、ダイレクトグループメンバーシップを含む対応

するユーザー属性が更新されます。こうしたチェックインにより、ユーザー資格の再評価が可能になります。

d) グループ単位での OTP による招待。XenMobile サーバー管理者が、XenMobile サーバーデータベースに存在する Active Directory グループの一覧からグループを選択します。ユーザーメンバーが直接的および間接的（入れ子構造の場合）に Active Directory から取得され、XenMobile サーバーデータベースに保存されます。前の手順で特定されたユーザーメンバーに対して、OTP 招待状が送られます。

e) ユーザー単位での OTP による招待。管理者が、XenMobile コンソールで検索テキストを入力します。XenMobile サーバーにより Active Directory に対する紹介が行われ、入力したテキストに一致するユーザーレコードが返されます。次に、管理者が OTP 招待状の送信先となるユーザーを選択します。ユーザーへの招待状の送信前に、XenMobile サーバーが Active Directory からユーザーの詳細を取得してデータベースの該当する情報を更新します。

バックグラウンドでのやり取り

Active Directory とのインライン通信で 1 つわかることは、XenMobile サーバーの構成が変更されるとグループベースのやり取りが行われるということです。構成に変更がない場合、グループについて Active Directory との通信は行われません。

こうしたやり取りではバックグラウンドジョブにより、Active Directory と定期的に同期して変更内容を対象のグループに反映する必要があります。

Active Directory をのやり取りを行うバックグラウンドジョブを次に示します。

1. グループ同期ジョブ。このジョブの目的は、対象のグループについて一度に 1 グループずつ Active Directory に照会し、識別名属性または sAMAccountName 属性の変更がないか確認することです。この Active Directory に対する検索クエリでは、対象グループの objectGUID を使用して識別名属性と sAMAccountName 属性の現在の値を取得します。対象グループの識別名または sAMAccountName の値の変更結果で、データベースが更新されます。

   > 注:
   >
   > このジョブでは、ユーザーのグループメンバーシップ情報は更新されません。

2. ネストされたグループ同期ジョブ。このジョブでは、対象グループの入れ子構造の変更内容が反映されます。XenMobile サーバーでは、対象グループの直接メンバーと間接メンバーの両方が資格を得ることができます。ユーザーのダイレクトメンバーシップは、ユーザーベースのインラインでのやり取りの際に更新されます。このジョブはバックグラウンドで実行され、間接メンバーシップを追跡します。間接メンバーシップとは、対象グループのメンバーであるグループにユーザーが属している状態を指します。

   このジョブでは、XenMobile サーバーデータベースから Active Directory グループのリストを取得します。Active Directory のグループは、展開グループか RBAC 定義のどちらかに含まれます。このリストの各グループについて、XenMobile サーバーがグループのメンバーを取得します。グループのメンバーは、ユーザーとグループの両方を表す識別名をリスト化したものです。XenMobile サーバーは Active Directory に対し

て別のクエリを実行し、対象グループのユーザーメンバーのみを取得します。これら 2 つのリストの差を取ると、対象グループのグループメンバーのみが残ります。メンバーグループへの変更結果がデータベースに反映されます。階層内のすべてのグループについて、同じ手順が繰り返されます。

入れ子構造を変更すると、影響を受けるユーザーに対して資格の変更処理が行われます。

3. 無効なユーザーのチェック。このジョブは、XenMobile 管理者が無効なユーザーをチェックする操作を作成した場合のみ実行されます。このジョブはグループ同期ジョブの範囲内で実行されます。このジョブでは、Active Directory に対してクエリを実行し、対象ユーザーの無効化状態を一度に 1 ユーザーずつ確認します。

よくある質問

デフォルトでは、バックグラウンドジョブの実行頻度はどのようになっていますか?

- グループ同期ジョブはローカル時間の 02:00 から 5 時間ごとに実行されます。
- 入れ子グループの同期ジョブは 1 日に 1 回、ローカル時間の深夜に実行されます。

なぜグループ同期ジョブが必要なのですか?

- Active Directory のユーザーレコードの memberOf 属性から、ユーザーが直接メンバーとなっているグループのリストが得られます。組織単位間でグループが移動された場合、memberOf 属性には識別名の最新の値が反映されます。また、XenMobile サーバーデータベースには最後に更新された値が保持されます。グループの識別名が一致しない場合、ユーザーは展開グループにアクセスできなくなります。同時に、展開グループに関連付けられているアプリやポリシーにもアクセスできなくなります。
- バックグラウンドジョブにより、XenMobile サーバーデータベースのグループの識別名属性が最新の状態に保たれるため、ユーザーは使用権へのアクセスを確保できます。
- Active Directory でのグループが変更される頻度は高くないと考えられるため、同期ジョブは 5 時間間隔でスケジュールされています。

グループ同期ジョブは無効化できますか?

- 組織単位間で対象グループが変更されないことがわかっている場合は、ジョブを無効化できます。

なぜ入れ子グループによる処理中のバックグラウンドジョブが必要なのですか?

- Active Directory 内のグループの入れ子構造の変更は、毎日発生するわけではありません。対象グループの入れ子構造を変更すると、影響を受けるユーザーの使用権が変更されます。階層にグループを追加すると、そのメンバーユーザーに各役割の使用権が付与されます。グループが入れ子構造から外されると、そのグループのメンバーユーザーはこうした役割ベースの使用権にアクセスできなくなる場合があります。
- 入れ子構造の変更内容は、ユーザーによる更新時には取得されません。入れ子構造の変更をオンデマンドで行うことはできないため、変更内容はバックグラウンドジョブにより取得されます。
- 入れ子構造の変更はあまり行われないものと考えられるため、このバックグラウンドジョブは 1 日に 1 回実行され、変更の有無を確認します。

入れ子グループによる処理中のジョブは無効化できますか?

- 該当するグループに入れ子構造の変更が発生していないことがわかっている場合は、ジョブを無効化できます。

XenMobile の展開

July 5, 2019

XenMobile の展開を計画する際には、考慮すべき点がたくさんあります。どんなデバイスを選ぶか。それらをどのように管理するか。良好なユーザーエクスペリエンスを実現しながらネットワークを安全に保つにはどうすればよいか。どんなハードウェアを用意し、そのトラブルシューティングをどのように行うか。このハンドブックは、これらの質問などに答えることを目的としています。展開の問題や、想定外の質問に関連したユースケースや推奨事項を取り上げています。

ガイドラインや推奨事項は、すべての環境やユースケースに適用されるわけではないことに注意してください。XenMobile の展開を開始する前に、テスト環境を設定してください。

このハンドブックには、次の 3 つの主要セクションがあります:

- 評価: 展開を計画する際に考慮すべき共通のユースケースと質問
- 設計と構成: 環境の設計と構成に関する推奨事項
- 動作と監視: 実行環境の円滑な動作の確保

評価

どの環境でも、ニーズを評価することが最優先事項です。XenMobile に対する一番のニーズは何ですか。環境内のすべてのデバイスを管理する必要があるのか、それともアプリだけ管理すればよいのか。もしかすると両方を管理する必要があるかもしれません。XenMobile 環境にはどの程度の安全性が必要ですか。展開を計画する際に考慮すべき共通のユースケースと質問を見ていきましょう。

- 管理モード
- デバイスの要件
- セキュリティとユーザーエクスペリエンス
- アプリ
- ユーザーコミュニティ
- メール戦略
- XenMobile 統合
- 複数サイトの要件

設計と構成

展開ニーズの評価が完了したら、環境の設計と構成に関する意思決定を下すことができます。以下は、検討が必要な項目の例です:

- サーバー用のハードウェアの選定
- アプリおよびデバイスのポリシーの設定

- ユーザーの登録

このセクションには、これらのシナリオやその他のユースケースと推奨事項が含まれています。

- NetScaler と NetScaler Gateway の統合
- MDX アプリの SSO とプロキシの考慮事項
- 認証
- オンプレミス環境のリファレンスアーキテクチャ
- サーバープロパティ
- デバイスポリシーとアプリポリシー
- ユーザー登録オプション
- XenMobile の動作の調整

動作と監視

XenMobile 環境が稼働したら、スムーズに動作するように監視を行います。「監視」セクションでは、XenMobile とそのコンポーネントが生成するさまざまなログとメッセージの格納場所と、それらのログの見方について説明します。また、このセクションでは、カスタマーサポートのフィードバックにかかる時間を短縮できる一般的なトラブルシューティングの手順も紹介します。

- アプリのプロビジョニングとプロビジョニング解除
- ダッシュボードベースの操作
- 役割ベースのアクセス制御と XenMobile のサポート
- システムの監視
- 障害回復
- Citrix のサポートプロセス

管理モード

August 22, 2019

各 XenMobile インスタンス（単一のサーバーまたはノードのクラスター）に対し、デバイス、アプリ、またはその両方を管理するかどうかを選択できます。XenMobile は、デバイス管理モードとアプリケーション管理モード（展開モードと呼ばれる場合もあります）で次の用語を使用します。

- モバイルデバイス管理（MDM）モード
- モバイルアプリケーション管理（MAM）モード
- MDM + MAM（企業）モード

モバイルデバイス管理（**MDM**）モード

> 重要：
>
> MDM モードに構成し、後で ENT モードに変更する場合は、必ず同じ（Active Directory）認証を使用してください。XenMobile では、ユーザー登録後の認証モードの変更をサポートしていません。詳しくは、「アップグレード」を参照してください。

MDM を使用すると、モバイルデバイスを設定、保護、およびサポートできます。MDM では、システムレベルでデバイス上のデバイスとデータを保護できます。ポリシー、アクション、およびセキュリティ機能を設定できます。たとえば、デバイスが紛失や盗難にあったり、コンプライアンス違反となった場合に、デバイスを選択的にワイプできます。アプリ管理は MDM モードでは利用できませんが、このモードではパブリックアプリストアやエンタープライズアプリなどのモバイルアプリを配信できます。以下は、MDM モードの一般的なユースケースです。

- MDM は、完全なワイプ、選択的なワイプ、またはジオロケーションなどのデバイスレベルの管理ポリシーや制約が必要な企業所有デバイスが考慮されています。
- 顧客が実際のデバイスの管理を必要としながら、アプリのコンテナ化、アプリデータの共有の制御、マイクロ VPN などの MDX ポリシーを必要としない場合。
- ユーザーはモバイルデバイス上のネイティブメールクライアントへのメールの配信のみが必要で、Exchange ActiveSync やクライアントアクセスサーバーにはすでに外部からアクセス可能な場合。このユースケースでは、MDM を使用してメールの配信を設定できます。
- ネイティブエンタープライズアプリ（非 MDX）、パブリックアプリストアアプリ、またはパブリックストアから配信された MDX アプリを展開する場合。MDM ソリューションだけでは、デバイス上のアプリ間の機密情報の漏洩を防止できない可能性があることを考慮してください。データ漏洩は、Office 365 アプリでのコピー＆ペースト操作や名前を付けて保存操作で発生する可能性があります。

モバイルアプリケーション管理（**MAM**）モード

MAM はアプリデータを保護し、アプリデータ共有を制御できるようにします。また、個人データとは別に企業のデータやリソースの管理も可能です。XenMobile を MAM モードに設定すると、MDX 対応のモバイルアプリを使用して、アプリごとのコンテナ化と制御を提供できます。MAM モードは、MAM-only モードとも呼ばれます。この用語は、このモードを従来の MAM モードと区別するものです。

MDX ポリシーを活用することにより、XenMobile はネットワークアクセス（マイクロ VPN など）、アプリとデバイスのやり取り、データの暗号化、およびアプリへのアクセスをアプリレベルで制御します。

デバイスは管理されませんが企業データの保護は維持されるため、多くの場合 MAM モードは持ち込みデバイス（BYO）に適しています。MDX には 50 以上の MAM 専用のポリシーがあり、MDM 制御なしで、デバイスパスコードによる暗号化に頼らずに設定できます。

MAM モードでは、業務用モバイルアプリもサポートされます。このサポートには、Citrix Secure Mail へのメールの安全な配信、保護対象の業務用モバイルアプリ間でのデータ共有、および ShareFile の安全なデータストレージが含まれます。詳しくは、「業務用モバイルアプリ」を参照してください。

多くの場合、MAM は次の例に適しています。

- アプリレベルで管理されている MDX アプリなどのモバイルアプリを配信する。
- システムレベルでデバイスを管理する必要がない。

MDM + MAM（企業）モード

MDM + MAM はハイブリッドモードで、エンタープライズモードとも呼ばれ、XenMobile Enterprise Mobility Management（EMM）ソリューションで利用できるすべての機能セットを使用できます。XenMobile を MDM + MAM モードで構成すると、MDM と MAM の両方の機能が有効になります。

XenMobile では、ユーザーがデバイス管理をオプトアウトできるか、またはデバイス管理が必要かどうかを指定できます。この柔軟性は、複数のユースケースが混在する環境で役立ちます。これらの環境では、MAM リソースへのアクセスで、MDM ポリシーに基づいたデバイスの管理が必要な場合とそうでない場合があります。

多くの場合、MDM + MAM は次の例に適しています。

- MDM と MAM の両方が必要なユースケースが 1 つだけある。MAM リソースにアクセスするために MDM が必要である。
- MDM が必要なユースケースもあるが、そうでないユースケースもある。
- MAM が必要なユースケースもあるが、そうでないユースケースもある。

XenMobile Server の管理モードは、サーバーモードプロパティで指定します。XenMobile コンソールでこの設定を構成できます。サーバーモードは、MDM、MAM、または ENT（MDM + MAM）です。

次の表に示すとおり、ライセンスを保有する XenMobile エディションによって使用可能な管理モードとその他の機能が決まります。

XenMobile MDM Edition	**XenMobile Advanced Edition**	**XenMobile Enterprise Edition**
MDM の機能	MDM の機能	MDM の機能
-	MAM の機能	MAM の機能
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	Secure Tasks	Secure Tasks
-	-	ShareConnect
-	-	Secure Notes

-	-	ShareFile Enterprise Edition

デバイス管理と **MDM** 登録

XenMobile Enterprise 環境には、MAM リソースへのアクセスを許可する MDM ポリシーによるデバイス管理が必要なユースケースが混在している場合があります。業務用モバイルアプリをユーザーに展開する前に、ユースケースを十分に評価し、MDM 登録を必須にするかどうかを決定してください。MDM 登録の必要性を後で変更すると、ユーザーがデバイスを再登録しなければならない場合もあります。

> 注:
>
> ユーザーが MDM に登録する必要があるかどうかを指定するには、XenMobile コンソールの XenMobile Server プロパティ ［登録が必要］ を使用します（［設定］ **>** ［サーバープロパティ］）。そのグローバルサーバープロパティは、XenMobile インスタンスのすべてのユーザーとデバイスに適用されます。このプロパティは、XenMobile Server モードが ENT の場合にのみ適用されます。

次に、XenMobile Enterprise モードでの展開において MDM 登録を必要とする場合のメリットとデメリットを（緩和策とともに）示します。

MDM 登録をオプションとする場合

長所:

- ユーザーはデバイスを MDM 管理下に置くことなく、MAM リソースにアクセスできる。このオプションは、ユーザーへの導入を増やすことができます。
- MAM リソースへのアクセスを保護し、企業データを保護できる。
- アプリのパスコードなどの MDX ポリシーで、各 MDX アプリのアプリアクセスを制御できる。
- NetScaler、XenMobile Server、およびアプリケーションごとのタイムアウトを Citrix PIN で構成すると、保護が強化される。
- MDM アクションはデバイスには適用されませんが、一部の MDX ポリシーを MAM アクセスを拒否するのに使用できます。この拒否は、ジェイルブレイクデバイスまたは Root 化済みデバイスなどのシステム設定に基づいて行なわれます。
- ユーザーは初回使用時に、MDM を使用してデバイスを登録するかどうかを選択できます。

短所:

- MAM リソースを MDM に登録されていないデバイスで使用できる。
- MDM のポリシーとアクションを、MDM に登録されているデバイスでしか使用できない。

緩和オプション:

- コンプライアンスに違反した場合はユーザーが責任を負うという企業の契約条件に対して、本人の同意を得ます。管理者に「管理されないデバイス」を監視させます。
- アプリケーションタイマーを使用して、アプリケーションアクセスとセキュリティを管理します。タイムアウト値を小さくするとセキュリティは向上しますが、ユーザーエクスペリエンスに影響する場合があります。
- MDM 登録が必要な 2 番目の XenMobile 環境はオプションです。このオプションを検討する場合には、2 つの環境を管理するためにオーバーヘッドが増え、追加のリソースが必要となることに留意してください。

MDM 登録を必要とする場合

長所:

- MAM リソースへのアクセスを MDM が管理するデバイスのみに制限できる。
- MDM のポリシーとアクションを、必要に応じて環境内のすべてのデバイスに適用できる。
- ユーザーがデバイス登録をオプトアウトすることはできない。

短所:

- すべてのユーザーを MDM に登録する必要がある。
- 個人用デバイスの企業管理に反対するユーザーへの導入が減る可能性がある。

緩和オプション:

- XenMobile が実際にデバイス上の何を管理するか、管理者がどの情報にアクセスできるかについてユーザーを教育します。
- MDM 管理が不要なデバイスで、MAM のサーバーモード（MAM-only モードとも呼ばれます）にした 2 番目の XenMobile 環境を使用できます。このオプションを検討する場合には、2 つの環境を管理するためにオーバーヘッドが増え、追加のリソースが必要となることに留意してください。

MAM と従来の **MAM** モードについて

XenMobile 10.3.5 では、新しい MAM-only サーバーモードが導入されます。以前の MAM モードと新しい MAM モードを区別するために、このドキュメントでは次の用語を使用します。新しいモードを MAM-only または MA とし、以前の MAM モードを従来の MAM モードとします。

XenMobile のサーバーモードプロパティが MAM の場合、MAM-only モードが有効になります。デバイスは MAM モードで登録します。

従来の MAM 機能は、XenMobile サーバーモードプロパティが ENT であり、ユーザーがデバイス管理を行わないことを選択した場合に有効になります。その場合、デバイスは MAM モードで登録します。MDM 管理を行わないユーザーは、従来の MAM 機能を引き続き使用できます。

> 注:

> 以前は、サーバーモードプロパティを MAM に設定すると、ENT に設定するのと同じ効果がありました。MDM 管理を行わないユーザーは従来の MAM 機能を使用できました。

次の表は、特定のライセンスの種類および機能のデバイスモードで使用するサーバーモードの概要を示しています。

現在のエディションのライセンス	デバイスを登録するモード	必要なサーバーモードプロパティの設定
Enterprise/ Advanced/MDM	MDM モード	MDM
Enterprise/Advanced	MAM モード（MAM-only モードとも呼ばれます）	MAM
Enterprise/Advanced	MDM+MAM モード	ENT（デバイス管理を行わないユーザーは従来の MAM モードで操作します）

MAM-only モードでは、以前は ENT でのみ使用可能だった以下の機能がサポートされています。これらの機能は、Windows Phone では利用できません。

- 証明書ベースの認証： MAM-only モードでは、証明書ベースの認証がサポートされます。Active Directory のパスワードの有効期限が切れても、ユーザーは引き続きアプリにアクセスできます。MAM デバイスに証明書ベースの認証を使用する場合は、NetScaler Gateway を構成する必要があります。デフォルトでは、[**XenMobile** 設定] **>** [**NetScaler Gateway**] の［認証用のユーザー証明書を配信］は［オフ］であり、これはユーザー名とパスワードによる認証が使用されていることを意味します。その設定を［オン］に変更すると証明書による認証が有効になります。
- **Self Help Portal**： ユーザーは独自のアプリロックとアプリワイプを実行できます。これらの操作は、デバイス上のすべてのアプリに適用されます。アプリロックとアプリワイプのアクションは、［設定］**>**［アクション］で設定できます。
- 全登録モード：［高セキュリティ］、［招待 URL］、［2 要素］が含まれます。［管理］**>**［登録］で設定します。
- **Android** と **iOS** デバイスのデバイス登録制限： サーバープロパティ ［ユーザーごとのデバイスの数］ は［構成］**>**［登録プロファイル］ に移動し、すべてのサーバーモードに適用されるようになりました。
- **MAM-only API**：MAM-only デバイスでは、REST クライアントと XenMobile REST API を使用して REST サービスを呼び出し、XenMobile コンソールで公開されているサービスを呼び出します。
- MAM-only API を使用すると、次のことが可能になります。
  - 招待 URL とワンタイム PIN を送信する。
  - デバイスでアプリロックとアプリワイプを発行する。

次の表は、従来の MAM と MAM-only との機能の違いをまとめたものです。

登録シナリオおよびその他の機能	従来の **MAM**（サーバーモード **ENT**）	**MAM-only** モード（サーバーモード **MAM**）
証明書認証	サポートされません。	サポートされます。証明書認証を使用するには、NetScaler Gateway が必要です。
展開要件	XenMobile サーバーは、デバイスから直接アクセスできるようにする必要はありません。	XenMobile サーバーは、デバイスから直接アクセスできるようにする必要はありません。
登録オプション	NetScaler Gateway FQDN を使用するか、MDM FQDN を使用する場合は登録しないことを選択してください。	XenMobile Server FQDN を使用してください。
登録方法 *	ユーザー名およびパスワード	[User name + Password]、[High Security]、[Invitation URL]、[Invitation URL + PIN]、[Invitation URL + Password]、[Two Factor]、[User name + PIN]
アプリロックおよびアプリワイプ	サポートされます。	サポートされます。
アプリロックおよびアプリワイプの Self Help Portal オプション	サポートされません。	サポートされます。
アプリワイプの動作	アプリはデバイス上に残りますが、使うことはできません。XenMobile は、クライアント上のアカウントのみを削除します。	アプリはデバイス上に残りますが、使うことはできません。XenMobile は、クライアント上のアカウントのみを削除します。
MAM-only ユーザー向けの自動化された操作	イベント、デバイスプロパティ、ユーザープロパティ操作がサポートされます。インストールされたアプリベースの自動化された操作はサポートされません。	イベント、デバイスプロパティ、ユーザープロパティ、アプリワイプやアプリロックなどの一部のアプリベースの操作がサポートされます。
Active Directory ユーザーが削除された場合の組み込み操作	アプリワイプがサポートされます。	アプリワイプがサポートされます。
登録の制限	サポートされます。登録プロファイル経由で設定されます。	サポートされます。登録プロファイル経由で設定されます。

ソフトウェアインベントリ	サポートされます。XenMobile は、デバイスにインストールされているアプリの一覧を作成します。	サポートされません。

* 通知について： SMTP は、登録招待状の送信でサポートされる唯一の方法です。

> 重要：
>
> MAM-only モードでは、以前に登録したユーザーはデバイスを再登録する必要があります。登録に必要な XenMobile Server の FQDN をユーザーに提供してください。MAM-only モードでは、ENT モードと同様、デバイスの登録に XenMobile Server の FQDN を使用します。（従来の MAM モードでは、デバイスの登録に NetScaler Gateway の FQDN を使用します。）

デバイスの要件

January 10, 2020

展開で検討すべき重要なポイントは、展開を計画するデバイスです。iOS、Android、および Windows プラットフォームでは、多くの選択肢があります。XenMobile でサポートされるデバイスについて詳しくは、「サポート対象のデバイスプラットフォーム」を参照してください。

独自のデバイス（Bring Your Own Devive：BYOD）環境では、サポート対象のプラットフォームを混在させることができます。ただし、登録可能なデバイスについてユーザーに通知するときは、サポート対象のデバイスプラットフォームの記事に記載されている制限事項を考慮してください。ご使用の環境で 1 台または 2 台のデバイスだけを許可する場合でも、XenMobile は iOS、Android、および Windows デバイスで機能が若干異なります。各プラットフォームで異なる機能セットを使用できます。

また、すべてのアプリが、タブレットとスマートフォン両方のフォームファクタを対象とした設計になっているわけではありません。広範囲に変更を加える前にアプリをテストして、アプリを展開するデバイスの画面に合わせるようにしてください。

登録要素を検討することもできます。Apple と Google ではエンタープライズ登録プログラムを提供しています。Apple デバイス登録プログラム（DEP）およびGoogle Android Enterpriseを通して、従業員が使用する準備が整った事前設定済みデバイスを購入できます。これらのプログラムを使用しない場合でも、SMS 経由でユーザーに招待リンクを送信するかどうかを検討してください。タブレットで SMS を使用することはできません。

登録について詳しくは、「ユーザー登録オプション」を参照してください。

セキュリティとユーザーエクスペリエンス

January 10, 2020

すべての組織にとってセキュリティは重要ですが、その一方でセキュリティとユーザーエクスペリエンスのバランスをとる必要があります。安全性は高いものの、ユーザーにとって使いにくい環境もあれば、ユーザーにとって使いやすいものの、アクセス制御が厳しくない環境もあります。この仮想ハンドブックの他のセクションではセキュリティ機能について詳しく説明していますが、この記事は、利用できるセキュリティオプションの概要を説明し、XenMobile で一般的なセキュリティ上の問題についてユーザーに考えてもらうことを目的とします。

各ユースケースで留意する重要な考慮事項は次のとおりです:

- 特定のアプリ、デバイス全体、またはその両方を保護しますか。
- どのような方法でユーザーの ID が認証されるようにしますか。LDAP、証明書ベースの認証、またはこの 2 つの組み合わせを使用しますか。
- ユーザーのセッションがタイムアウトするまでにどれくらいの時間が経過する必要がありますか。バックグラウンドサービス、NetScaler、およびオフラインでのアプリへのアクセスでは、タイムアウト値が異なることに留意してください。
- ユーザーがデバイスレベルのパスコードやアプリレベルのパスコードを設定するようにしますか。ユーザーに許容されるログオン試行回数は何回ですか。MAM で実装できるアプリごとの追加の認証要件と、ユーザーによってこれがどのように受け止められるかに留意してください。
- ユーザーに対して、他にどのような制限を加えますか。Siri などのクラウドサービスにユーザーがアクセスできるようにする必要がありますか。使用できるそれぞれのアプリで、ユーザーができること、およびできないことは何ですか。オフィススペース内にいるときに携帯データ通信プランが消費されるのを防ぐために、企業の WiFi ポリシーを導入する必要がありますか。

アプリとデバイス

最初に、特定のアプリだけを保護すればいいのか（モバイルアプリケーション管理（MAM））、またはデバイス全体を管理する必要があるのか（モバイルデバイス管理（MDM））について考える必要があります。一般に、デバイスレベルの制御が不要な場合は、モバイルアプリを管理すれば十分です。これは特に、BYOD（Bring Your Own Device）がサポートされている組織に当てはまります。

MAM-only の環境では、ユーザーは利用可能なリソースにアクセスできます。MAM ポリシーは、アプリそのものを保護および管理します。

一方 MDM では、デバイス上のすべてのソフトウェアのインベントリを取得したり、ジェイルブレイクまたは Root 化されたデバイス、または安全でないソフトウェアがインストールされたデバイスの登録を防止したりして、デバイス全体を保護することができます。ただし、このレベルで制御すると、ユーザーは自分が使用する個人用デバイスに対してこのような権限を許可することに慎重になり、登録率が低下する可能性があります。

MDM は一部のデバイスには必要でも、他のデバイスには不要な場合があります。ただし、この選択をすると 2 つの専用の環境を設定し、追加のリソースと保守が必要になる点に留意する必要があります。

認証

認証は、ユーザーエクスペリエンスの重要な部分を占めています。既に Active Directory を実行している組織では、Active Directory を使用することが、ユーザーをシステムにアクセスさせる最も簡単な方法です。

そのほかに、認証におけるユーザーエクスペリエンスで重要な要素となるのがタイムアウトです。高度なセキュリティ環境では、ユーザーがシステムにアクセスするたびにログオンさせる場合がありますが、このオプションはすべての組織にとって最適とは言えません。たとえば、メールにアクセスするたびに資格情報を入力しなければならないことはユーザーにとって煩雑であり、不要かもしれません。

ユーザーエントロピー

セキュリティを強化するために、ユーザーエントロピーと呼ばれる機能を有効にすることができます。Citrix Secure Hub や他のアプリでは、パスワード、PIN、および証明書などの共通データを共有することで、すべてが適正に機能するようになっています。この情報は、Secure Hub 内の汎用コンテナに保存されます。シークレットの暗号化オプションでユーザーエントロピーを有効にすると、XenMobile は UserEntropy という名前の新しいコンテナを作成し、汎用コンテナからこの新しいコンテナに情報を移動させます。Secure Hub や他のアプリがこのデータにアクセスするには、ユーザーはパスワードまたは PIN を入力する必要があります。

ユーザーエントロピーを有効にすると、複数の場所で認証が強化されます。ただし、UserEntropy コンテナに格納された共有データ（パスワード、PIN、証明書など）にアプリがアクセスする必要があるたびに、ユーザーはパスワードまたは PIN を入力する必要があります。

ユーザーエントロピーについては、「MDX Toolkit について」を参照してください。ユーザーエントロピーをオンにする場合は、関連する設定項目を［クライアントプロパティ］で見つけることができます。

ポリシー

MDX ポリシーと MDM ポリシーは、組織に大きな柔軟性をもたらす一方で、ユーザーが制限される場合もあります。状況によってはこれが必要な場合もありますが、ポリシーによってシステムが使用できなくなることもあります。たとえば、送信されたくない場所に機密データが送信される可能性のある、Siri や iCloud などのクラウドアプリケーションへのアクセスを禁止する必要がある場合、これらのサービスへのアクセスを禁止するポリシーを設定できますが、このようなポリシーによって意図しない結果がもたらされる可能性があることに注意してください。iOS のキーボード上のマイクもクラウドアクセスに依存しているため、この機能へのアクセスも禁止されることになります。

アプリ

エンタープライズモビリティ管理（EMM：Enterprise Mobility Management）は、モバイルデバイス管理（MDM：Mobile Device Management）とモバイルアプリケーション管理（MAM：Mobile Application Management）に分けられます。MDM を利用するとモバイルデバイスを保護し、制御できる一方、MAM ではアプリケーションの配信と管理を簡単に行えます。BYOD（Bring Your Own Device）の導入率が増加した場合、一般的には、アプリケーション配信、ソフトウェアライセンス、構成、アプリケーションライフサイクル管理を支援するため、XenMobile などの MAM ソリューションを実装します。

XenMobile を使用すると、データの漏洩などのセキュリティ上の脅威を防ぐように特定の MAM ポリシーと VPN 設定を構成し、こうしたアプリの保護をさらに強化できます。XenMobile は柔軟性に優れており、MAM 専用環境または MDM 専用環境としてソリューションを展開したり、同一のプラットフォーム内で MDM と MAM の両方の機能を提供する統合 XenMobile Enterprise 環境として XenMobile を実装したりすることができます。

XenMobile は、モバイルデバイスへのアプリ配信機能に加えて、MDX テクノロジーによるアプリのコンテナ化機能も備えています。MDX では、デバイスレベルの暗号化とは別の暗号化によってアプリを保護します。アプリはワイプまたはロック可能であり、ポリシーベースで詳細に制御することができます。独立系ソフトウェアベンダー（ISV：Independent Software Vendor）では、Worx App SDK を使用してこうした制御を行うことができます。

企業の環境では、ユーザーは職務の助けとしてさまざまなモバイルアプリを利用しています。こうしたアプリには、パブリックアプリストアのアプリや社内アプリ、場合によってはネイティブアプリも含まれます。XenMobile では、これらのアプリは次のように分類されます：

パブリックアプリ： これらのアプリには、iTunes や Google Play など、パブリックアプリストアで無料または有料で提供されているアプリが含まれます。組織外のベンダーの多くは、パブリックアプリストアで自社のアプリを公開しています。こうすることで、ベンダーの顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズによっては、組織内でパブリックアプリが数多く使用される場合があります。こうしたアプリには、GoToMeeting、Salesforce、EpicCare などがあります。

Citrix では、パブリックアプリストアからアプリバイナリを直接ダウンロードすることおよび、こうしたバイナリを社内配布用に MDX Toolkit でラップすることはサポートしていません。サードパーティのアプリケーションをラップする必要がある場合は、そのアプリのベンダーと協力して、MDX Toolkit でラップ可能なアプリのバイナリを入手します。

社内アプリ： 多くの組織には社内開発者がおり、特定の機能を備え、組織内で独自に開発および配布されるアプリを作成しています。組織によっては、ISV から提供されるアプリを導入している場合もあります。こうしたアプリは、ネイティブアプリとして展開するか、XenMobile などの MAM ソリューションを使用してコンテナ化できます。たとえば、医療機関で、モバイルデバイスで医師が患者の情報を確認できる社内アプリを作成したとします。さらに MDX Toolkit を使用してこのアプリをラップすることで、患者の情報を保護するとともに、バックエンドの患者データベースサーバーへの VPN アクセスを有効化できます。

Web アプリおよび **SaaS** アプリ： これらのアプリには、内部ネットワークからアクセスするアプリ（Web アプリ）やパブリックネットワーク経由でアクセスするアプリ（SaaS）が含まれます。XenMobile では、さまざまなアプリコネクタを使用して、カスタムの Web アプリおよび SaaS アプリを作成することもできます。これらのアプリコネ

クタを利用することで、既存の Web アプリへのシングルサインオン（SSO：Single Sign-On）を簡単に行えます。詳しくは、「アプリコネクタの種類」を参照してください。たとえば、Google Apps 向けのセキュリティアサーションマークアップランゲージ（SAML：Security Assertion Markup Language）を基にした、SSO 用の Google Apps SAML を使用できます。

業務用モバイルアプリ： Citrix が開発したアプリであり、XenMobile ライセンスに含まれています。詳しくは、「業務用モバイルアプリについて」を参照してください。Citrix では、ISV が Worx App SDK を使用して開発したビジネス対応アプリも提供しています。

HDX アプリ： StoreFront で公開される、Windows でホストされたアプリです。Citrix Virtual Apps and Desktops 環境を使用している場合、こうしたアプリを XenMobile に統合し、登録済みユーザーに公開することができます。

基になる構成およびアーキテクチャは、XenMobile で展開および管理するモバイルアプリの種類によって異なります。たとえば、1 つのアプリを権限レベルの異なる複数のユーザーグループが使用する場合、別々のデリバリーグループを作成して、このアプリを 2 つのバージョンで展開する必要があります。さらに、ユーザーデバイスでのポリシーの不一致を避けるため、ユーザーグループのメンバーシップが相互に排他的であることを確認する必要もあります。

iOS アプリケーションのライセンスは、Apple の Volume Purchase Program（VPP）を使用して管理することもできます。この方法を使用するには、XenMobile コンソールで VPP プログラムを登録し、VPP ライセンスでアプリを配信するように XenMobile の VPP 設定を構成する必要があります。このようにユースケースは多様であるため、XenMobile 環境を実装する前に、MAM 戦略を評価し計画することが重要です。MAM 戦略の計画は、次の事柄を定義することから始めることをお勧めします。

アプリの種類： パブリックアプリ、ネイティブアプリ、業務用モバイルアプリ、Web アプリ、社内アプリ、ISV アプリなど、サポート予定のアプリの種類をリストアップして分類します。また、iOS や Android などのデバイスプラットフォームごとにもアプリを分類します。このように分類することで、アプリの種類ごとに必要な XenMobile 設定を調整しやすくなります。たとえば、一部のアプリをラップの対象から除外する場合や、いくつかのアプリでほかのアプリとのやりとりを行うために、Worx App SDK を使用して特殊な API を有効化する必要のある場合があります。

ネットワーク要件： アプリには、適切に設定した明確なネットワークアクセス要件を構成する必要があります。たとえば、VPN 経由で内部ネットワークにアクセスする必要のあるアプリもあれば、DMZ 経由でアクセスをルーティングするためにインターネットアクセスが必要なアプリもあります。こうしたアプリが必要なネットワークに接続できるようにするには、さまざまな設定を適切に構成しなければなりません。アプリごとのネットワーク要件を定義することで、アーキテクチャに関する決定事項を早期に確定し、実装プロセス全体の効率を高めることができます。

セキュリティ要件： 個々またはすべてのアプリに適用されるセキュリティ要件を定義することは、XenMobile サーバーのインストール時に確実に適切な構成を作成するために重要です。MDX ポリシーなどの設定は個々のアプリに適用されますが、セッションと認証の設定はすべてのアプリに適用されます。また、アプリによっては、展開を簡単に行うため、暗号化、コンテナ化、ラップ化、認証、ジオフェンシング、パスコード、あるいはデータ共有に関する特定の要件を事前に定める必要があります。

展開の要件： 公開したアプリを適合したユーザーのみがダウンロードできるように、ポリシーベースの展開を使用する必要のある場合があります。たとえば、特定のアプリについて、デバイスの暗号化が有効であるかデバイスが管理対象であること、またはデバイスがオペレーティングシステムの最小バージョンを満たしていることを必須にできま

す。また、特定のアプリをコーポレートユーザーだけに利用可能にする必要のある場合もあります。適切な展開ルールまたはアクションを構成できるように、こうした要件の概要を事前に定める必要があります。

ライセンス要件： アプリ関連のライセンス要件を記録することをお勧めします。こうした記録により、ライセンスの使用状況を効率的に管理できるとともに、XenMobile でライセンス管理を容易にする特定の機能を構成する必要があるかを判断できます。たとえば、iOS アプリを展開した場合、そのアプリが無料か有料かにかかわらず、Apple によりユーザーに iTunes アカウントへのサインインが求められ、アプリにライセンス要件が適用されます。こうしたアプリは、Apple VPP に登録することで、XenMobile 経由で配信および管理できます。VPP を利用することで、ユーザーは各自の iTunes アカウントにサインインすることなくアプリをダウンロードできるようになります。さらに、Samsung SAFE や Samsung KNOX などのツールには、機能を展開する前に履行する必要のある特殊なライセンス要件が備わっています。

ブラックリスト/ホワイトリストの要件： ユーザーにインストールや使用を禁止する必要のあるアプリも存在します。ブラックリストを作成すると、コンプライアンス違反イベントを定義できます。その後、コンプライアンス違反が起きた場合にトリガーされるようにポリシーを設定できます。一方で、使用が容認されるアプリが、なんらかの理由でブラックリストに該当する可能性もあります。このような場合には、ホワイトリストにそのアプリを追加し、アプリは使用してもよいが必須ではないと示すことができます。また、新しいデバイスにあらかじめインストールされているアプリの中には、オペレーティングシステムには含まれていないものの一般的に使用されているアプリもあります。こうしたアプリは、ブラックリスト化の方針に抵触する可能性があります。

アプリの使用例

ある医療機関が、同機関のモバイルアプリ向けの MAM ソリューションとして XenMobile を導入する予定を立てました。モバイルアプリは、コーポレートユーザーおよび BYOD ユーザーに配信されます。IT 部門は、次のアプリを配信および管理することを決定しました。

- 業務用モバイルアプリ： Citrix が提供する iOS アプリおよび Android アプリ。
- **Secure Mail**： メール、カレンダー、連絡先アプリ。
- **Secure Web**： インターネットとイントラネットサイトへのアクセスを提供するセキュアな Web ブラウザー。
- **Secure Notes**： メールとカレンダーが統合されたセキュアなノート作成アプリ。
- **ShareFile**： 共有データにアクセスし、ファイルを共有、同期、編集するためのアプリ。

パブリックアプリストア

- **Secure Hub**： すべてのモバイルデバイスで XenMobile との通信に使用するクライアント。IT 部門では、Secure Hub クライアントを経由してセキュリティ設定、構成、およびモバイルアプリをモバイルデバイスにプッシュします。Android デバイスおよび iOS デバイスは、Secure Hub 経由で XenMobile に登録されます。
- **Citrix Receiver**： Virtual Apps and Desktops でホストされているアプリケーションをユーザーがモバイルデバイス上で開くことができるモバイルアプリ。

- **GoToMeeting**: ほかのコンピューターユーザー、顧客、クライアント、同僚とインターネット経由でリアルタイムに話し合うことができる、オンライン会議、デスクトップ共有、ビデオ会議用クライアント。
- **SalesForce1**: モバイルデバイスから Salesforce へのアクセスを可能にし、あらゆる Salesforce ユーザーが統一されたエクスペリエンスで Chatter、CRM、カスタムアプリ、およびビジネスプロセスを利用できるようにするモバイルアプリ。
- **RSA SecurID**: 2 要素認証用のソフトウェアベーストークン。
- **EpicCare** アプリ: 医療従事者がモバイルデバイスで患者のカルテおよびリスト、スケジュールに安全にアクセスし、メッセージを通信できるようにするアプリ。
  - **Haiku**: iPhone および Android スマートフォン向けのモバイルアプリ。
  - **Canto**: iPad 用モバイルアプリ
  - **Rover**: iPhone および iPad 用のモバイルアプリ。

HDX: これらのアプリは、Citrix Virtual Apps and Desktops 経由で配信されます。

- **Epic Hyperspace**: 電子カルテ管理用の Epic のクライアントアプリケーション。

ISV

- **Vocera**: iPhone や Android スマートフォンで時間や場所を問わず Vocera 音声技術を利用できるようにする、HIPAA に準拠したボイスオーバー IP およびメッセージ用モバイルアプリ。

社内アプリ

- **HCMail**: 暗号化されたメッセージを作成し、内部メールサーバー上のアドレス帳を検索して、暗号化されたメッセージをメールクライアントで連絡先へ送信できるアプリ。

社内 **Web** アプリ

- **PatientRounding**: 複数の部署で患者の健康情報の記録に使用する Web アプリケーション。
- **Outlook Web Access**: Web ブラウザー経由でメールにアクセスできるようになります。
- **SharePoint**: 組織全体でのファイルおよびデータの共有に使用します。

次の表に、MAM の構成に必要な基本情報を示します。

アプリ名	アプリの種類	**MDX** によるラップ	**iOS**	**Android**
Secure Mail	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
Secure Web	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい

Secure Notes	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
ShareFile	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
Secure Hub	パブリックアプリ	-	はい	はい
Citrix Receiver	パブリックアプリ	-	はい	はい
GoToMeeting	パブリックアプリ	-	はい	はい
SalesForce1	パブリックアプリ	-	はい	はい
RSA SecurID	パブリックアプリ	-	はい	はい
Epic Haiku	パブリックアプリ	-	はい	はい
Epic Canto	パブリックアプリ	-	はい	いいえ
Epic Rover	パブリックアプリ	-	はい	いいえ
Epic Hyperspace	HDX アプリ	-	はい	はい
Vocera	ISV アプリ	はい	はい	はい
HCMail	社内アプリ	はい	はい	はい
PatientRounding	Web アプリ	-	はい	はい
Outlook Web Access	Web アプリ	-	はい	はい
SharePoint	Web アプリ	-	はい	はい

次の表に、XenMobile での MAM ポリシーの構成の参考要件を示します。

アプリ名

VPN の要否

相互作用

相互作用

デバイスの暗号化

（コンテナ外のアプリに対して）

（コンテナ外のアプリから）

Secure Mail

Secure Web

Secure Notes

ShareFile

Secure Hub

-

-

-

Citrix Receiver

-

-

-

GoToMeeting

×

-

-

-

SalesForce1

×

-

-

-

RSA SecurID

×

-

-

-

Epic Haiku

-

-

-

Epic Canto

-

-

-

Epic Rover

-

-

-

Epic Hyperspace

☒

-

-

-

Vocera

☒

禁止

禁止

不要

HCMail

☒

禁止

禁止

必須

PatientRounding

☒

-

-

必須

Outlook Web Access

☒

-

-

不要

SharePoint

-

-

不要

アプリ名	プロキシのフィルタリング	ライセンス	ジオフェンシング	**Worx App SDK**	オペレーティングシステムの最小バージョン
Secure Mail	必須	-	選択的に必須化	-	適用する
Secure Web	必須	-	不要	-	適用する
Secure Notes	必須	-	不要	-	適用する
ShareFile	必須	-	不要	-	適用する
Secure Hub	不要	VPP	不要	-	適用しない
Citrix Receiver	不要	VPP	不要	-	適用しない
GoToMeeting	不要	VPP	不要	-	適用しない
SalesForce1	不要	VPP	不要	-	適用しない
RSA SecurID	不要	VPP	不要	-	適用しない
Epic Haiku	不要	VPP	不要	-	適用しない
Epic Canto	不要	VPP	不要	-	適用しない
Epic Rover	不要	VPP	不要	-	適用しない
Epic Hyperspace	不要	-	不要	-	適用しない
Vocera	必須	-	必須	必須	適用する
HCMail	必須	-	必須	必須	適用する
PatientRounding	必須	-	不要	-	適用しない
Outlook Web Access	必須	-	不要	-	適用しない
SharePoint	必須	-	不要	-	適用しない

ユーザーコミュニティ

すべての組織は、異なる機能的役割を持つ多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーのモバイルデバイスを通して提供されるさまざまなリソースを使用して、さまざまなタスクを実行しオフィス機能を果たします。ユーザーは、支給されたモバイルデバイス、または特定のセキュリティコンプライアンスルールの対象となるツールへのアクセスが許可された個人のモバイルデバイスを使用して、自宅やリモートオフィスで作業することができます。

職務を簡素化したり助けとするためにモバイルデバイスを使用するユーザーコミュニティが増えるにつれ、データ漏洩を防止し、組織のセキュリティ制限を実施するために、エンタープライズモビリティ管理（EMM）が非常に重要になります。効率的で高度なモバイルデバイス管理を実現するために、ユーザーコミュニティを分類することができます。そうすることにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーを適切なユーザーに適用できます。

次の例は、医療機関のユーザーコミュニティにおける EMM 向けの分類方法を示したものです。

ユーザーコミュニティの使用例

この医療機関の例では、ネットワークやアフィリエイトの従業員、ボランティアなどの複数のユーザーに技術リソースやアクセスを提供します。この組織は EMM ソリューションを非幹部ユーザーのみに展開することを選択しました。

この医療機関のユーザー役割と機能は、医療、医療以外、契約社員などのサブグループに分けられます。指定されたグループのユーザーが企業のモバイルデバイスを受け取ります。その他のユーザーは個人のデバイスから限られた企業リソースにアクセスできます。適切なレベルのセキュリティ制限を実施し、データ漏洩を防止するために、この組織では、登録された各デバイス（企業所有のデバイスと BYOD（Bring Your Own Device））を企業の IT 部門が管理することに決定しました。また、ユーザーが登録できるデバイスは 1 台のみです。

以下のセクションでは、各サブグループの役割と機能の概要について説明します。

医療

- 看護師
- 医師（医師、外科医など）
- スペシャリスト（栄養士、採血師、麻酔医、放射線科医、心臓病専門医、がん専門医など）
- 外部の医師（外来の医師とリモートオフィスで作業するオフィスワーカー）
- 在宅医療サービス（患者の往診で医療サービスを行うオフィスワーカーとモバイルワーカー）
- 研究スペシャリスト（医薬における問題解決のための臨床研究を行う 6 つの研究機関のナレッジワーカーとパワーユーザー）
- 教育と訓練（教育と訓練に従事する看護師、医師、スペシャリスト）

医療以外

- 共通サービス（人事、給与、財務、サプライチェーンサービスなどのさまざまなバックオフィス機能を果たすオフィスワーカー）
- 医療サービス（管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、総合的健康管理、患者アクセスソリューション、収益サイクルソリューションなどの、さまざまな医療管理、管理サービス、ビジネスプロセスソリューションをプロバイダーに提供するオフィスワーカー）
- サポートサービス（福利厚生管理、医療の統合、コミュニケーション、報酬および業績管理、施設および土地サービス、ヒューマンリソーステックシステム、情報サービス、内部監査およびプロセス改善など、医療以外のさまざまな機能を果たすオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するさまざまな機能を果たすオフィスワーカーとモバイルワーカー）

契約社員

- メーカーやベンダーのパートナー（オンサイト、またはサイト間 VPN 経由でリモート接続された、医療以外のさまざまなサポート機能を提供する人々）

上記の情報に基づいて、この医療機関では以下のエンティティを作成しました。XenMobile のデリバリーグループの詳細については、「リソースの展開」を参照してください。

Active Directory 組織単位（**OU**）とグループ

OU **=** XenMobile リソース:

- OU = 医療; グループ =
  - XM-看護師
  - XM-医師
  - XM-スペシャリスト
  - XM-外部の医師
  - XM-在宅医療サービス
  - XM-研究スペシャリスト
  - XM-教育と訓練
- OU = 医療以外; グループ =
  - XM-共通サービス
  - XM-医療サービス
  - XM-サポートサービス
  - XM-慈善プログラム

XenMobile のローカルユーザーとグループ

グループ = 契約社員、ユーザー =

- ベンダー 1
- ベンダー 2

- ベンダー 3
- …ベンダー 10

XenMobile デリバリーグループ

- 医療-看護師
- 医療-医師
- 医療-スペシャリスト
- 医療-外部の医師
- 医療-在宅医療サービス
- 医療-研究スペシャリスト
- 医療-教育と訓練
- 医療以外-共通サービス
- 医療以外-医療サービス
- 医療以外-サポートサービス
- 医療以外-慈善プログラム

デリバリーグループとユーザーグループのマッピング

Active Directory グループ	**XenMobile** デリバリーグループ
XM-看護師	医療-看護師
XM-医師	医療-医師
XM-スペシャリスト	医療-スペシャリスト
XM-外部の医師	医療-外部の医師
XM-在宅医療サービス	医療-在宅医療サービス
XM-研究スペシャリスト	医療-研究スペシャリスト
XM-教育と訓練	医療-教育と訓練
XM-共通サービス	医療以外-共通サービス
XM-医療サービス	医療以外-医療サービス
XM-サポートサービス	医療以外-サポートサービス
XM-慈善プログラム	医療以外-慈善プログラム

デリバリーグループとリソースのマッピング

次の表は、この使用例で各デリバリーグループに割り当てられたリソースを示しています。最初の表はモバイルアプリの割り当てを示しています。2 番目の表はパブリックアプリ、HDX アプリ、デバイス管理リソースを示しています。

XenMobile デリバリーグループ	**Citrix** モバイルアプリ	パブリックモバイルアプリ	**HDX** モバイルアプリ
医療-看護師	☒		
医療-医師			
医療-スペシャリスト			
医療-外部の医師	☒		
医療-在宅医療サービス	☒		
医療-研究スペシャリスト	☒		
医療-教育と訓練		☒	☒
医療以外-共通サービス		☒	☒
医療以外-医療サービス		☒	☒
医療以外-サポートサービス	☒	☒	☒
医療以外-慈善プログラム	☒	☒	☒
契約社員	☒	☒	☒

XenMobile デリバリーグループ	パブリックアプリ: **RSA SecurID**	パブリックアプリ: **EpicCare Haiku**	**HDX** アプリ: **Epic Hyper-space**	パスコードポリシー	デバイスの制限	自動化された操作	**Wi-Fi** ポリシー
医療-看護師							☒
医療-医師					☒		
医療-スペシャリスト							
医療-外部の医師							

医療-在宅医療サービス			
医療-研究スペシャリスト			
医療-教育と訓練	☒	☒	
医療以外-共通サービス	☒	☒	
医療以外-医療サービス	☒	☒	
医療以外-サポートサービス	☒	☒	

注意事項と考慮事項

- XenMobile は初期構成時に「すべてのユーザー」というデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしないと、すべての Active Directory ユーザーに XenMobile への登録権限が付与されます。
- XenMobile は、LDAP サーバーとの動的接続により Active Directory のユーザーとグループをオンデマンドで同期します。
- ユーザーが XenMobile にマップされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが複数のグループのメンバーである場合、XenMobile はユーザーを XenMobile にマップされているグループにのみ分類します。
- MDM の登録を必須にするには、XenMobile コンソールで［サーバープロパティ］の［登録が必要］オプションを［はい］に設定する必要があります。詳しくは、「サーバープロパティ」を参照してください。
- XenMobile デリバリーグループからユーザーグループを削除するには、dbo.userlistgrps 内にある SQL Server データベースのエントリを削除します。
  注意： この操作を実行する前に、XenMobile とデータベースのバックアップを作成してください。

XenMobile のデバイスの所有権について

ユーザーデバイスの所有者に応じてユーザーをグループ化できます。デバイスの所有権には、企業所有のデバイスと、BYOD（Bring Your Own Device）とも呼ばれるユーザー所有のデバイスがあります。XenMobile コンソールの 2 つの場所（［設定］ページの［展開規則］と XenMobile Server プロパティ）で、BYOD デバイスをネットワークに接続する方法を制御できます。展開規則の詳細については、XenMobile のドキュメントの「展開規則の構成」を参照してください。詳しくは、「サーバープロパティ」を参照してください。

サーバープロパティを設定することで、すべての BYOD ユーザーに対して企業によるデバイス管理を受け入れてからアプリにアクセスするように要求したり、ユーザーのデバイスを管理せずに、ユーザーに企業アプリへのアクセス権を付与したりすることができます。

サーバー設定 **wsapi.mdm.required.flag** を **true** に設定すると、XenMobile がすべての BYOD デバイスを管理し、登録を拒否したユーザーはアプリへのアクセスが拒否されます。XenMobile にユーザーのデバイスが登録されることによって実現する高いセキュリティと優れたユーザーエクスペリエンスを企業の IT チームが必要とする環境では、**wsapi.mdm.required.flag** を **true** に設定することを検討してください。

wsapi.mdm.required.flag をデフォルト設定の **false** のままにした場合、ユーザーは登録を拒否できますが、引き続き XenMobile Store を通じてデバイス上のアプリにアクセスできます。プライバシー、法律、または規制上の制約によりデバイスの管理が不要で、エンタープライズアプリの管理のみが必要な環境では、**wsapi.mdm.required.flag** を **false** に設定することを検討してください。

XenMobile が管理しないデバイスを持つユーザーは、XenMobile Store からアプリをインストールできます。選択的ワイプや完全なワイプなどのデバイスレベルの制御ではなく、アプリポリシーに従ってアプリへのアクセスを制御します。ポリシーでは、設定した値に応じて、デバイスが XenMobile サーバーを定期的にチェックして、アプリの実行が引き続き許可されていることを確認する必要があります。

セキュリティ要件

XenMobile 環境を展開する場合は、セキュリティ上のさまざまな点を考慮する必要が生じてきます。さまざまな部分や設定が連動しているため、許容できる保護レベルを確保するためにどこから始めたらいいのか、または何を選択すべきかがわからない場合があります。これらの選択を簡単にするために、次の表では、「高」、「より高い」、および「最高」のセキュリティの推奨事項を示しています。

セキュリティの問題だけでは、選択する展開モードが決まらないことに注意してください。展開モードを選択する前に、ユースケースの要件を確認して、セキュリティの問題を軽減できるかどうかを判断することが重要です。

高： この設定を使用すると、ほとんどの組織で許容可能な基本レベルのセキュリティを維持しながら、最適なユーザーエクスペリエンスを実現できます。

より高い： この設定では、セキュリティとユーザービリティ間でよりバランスがとれています。

最高： この推奨事項に従うと、非常に高いレベルのセキュリティが実現しますが、ユーザービリティとユーザーへの導入が犠牲になります。

展開モードのセキュリティに関する考慮事項

次の表は、各セキュリティレベルでの展開モードを示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
MAM および/または MDM	MDM + MAM	MDM + MAM、プラス FIPS

注:

- 使用例によっては、MDM-only または MAM-only の展開でセキュリティ要件を満たし、優れたユーザーエクスペリエンスを提供できる場合もあります。
- アプリのコンテナ化、マイクロ VPN、またはアプリ固有のポリシーが不要な場合は、デバイスの管理と保護に MDM を使用すれば十分です。
- アプリのコンテナ化のみでビジネスとセキュリティ上のすべての要件が満たされる BYOD のような使用例では、MAM-only モードをお勧めします。
- 高セキュリティ環境（および企業がデバイスを支給）の場合、利用可能なすべてのセキュリティ機能を利用するために MDM + MAM をお勧めします。XenMobile コンソールのサーバープロパティを使用して MDM 登録を適用する必要があります。
- FIPS は、連邦政府などの、最高水準のセキュリティが求められる環境向けのオプションです。

FIPS モードを有効にする場合は、SQL トラフィックを暗号化するように SQL Server を構成する必要があります。

NetScaler および **NetScaler Gateway** のセキュリティに関する考慮事項

次の表は、各セキュリティレベルでの NetScaler および NetScaler Gateway の推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
NetScaler をお勧めします。MAM と ENT には NetScaler Gateway が必須。MDM に推奨	XenMobile が DMZ 内にある場合は、SSL ブリッジを使用した標準の NetScaler for XenMobile ウィザード構成。XenMobile サーバーが内部ネットワークに配置されている場合にセキュリティ基準を満たすには SSL オフロードが必要です。	エンドツーエンド暗号化による SSL オフロード

注:

- XenMobile サーバーを NAT や既存のサードパーティ製プロキシ、またはロードバランサー経由で公開することは、SSL トラフィックが XenMobile サーバー上で終端する限りは MDM のオプションとなります。ただしこの選択には潜在的なセキュリティリスクがあります。
- 高度なセキュリティ環境を実現するには、NetScaler とデフォルトの XenMobile 構成の組み合わせがセキュリティ要件を満たしているか、それ以上の条件を備えている必要があります。
- 最高水準のセキュリティが求められる MDM 環境を実現するには、SSL の終端を NetScaler にすることで、エンドツーエンドの SSL 暗号化を維持しながら境界でトラフィックを検査できます。
- SSL/TLS 暗号を定義するオプション。
- SSL FIPS NetScaler ハードウェアも利用できます。
- 詳しくは、「NetScaler Gateway および NetScaler の統合」を参照してください。

登録のセキュリティに関する考慮事項

次の表は、各セキュリティレベルでの NetScaler および NetScaler Gateway の推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。	招待のみの登録モード。Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。	デバイス ID に関連付けられた登録モード。Active Directory グループメンバーシップのみ。すべてのユーザーデリバリーグループが無効になっています。

注:

- 事前定義された Active Directory グループ内のユーザーのみに登録を制限することをお勧めします。そのためには、組み込みのすべてのユーザーデリバリーグループを無効にする必要があります。
- 登録招待状を使用すると、招待状を持つユーザーだけが登録できるように制限できます。
- 2 段階認証としてワンタイム PIN（OTP）による登録招待状を使用し、ユーザーが登録できるデバイス数を制御できます。
- 環境のセキュリティ要件が非常に厳しい場合は、SN、UD、または EMEI を使用して登録招待状とデバイスを関連付けることができます。Active Directory のパスワードと OTP を求める 2 段階オプションも用意されています（OTP は現在 Windows デバイスのオプションではないことに注意してください）。

デバイスの **PIN** のセキュリティに関する注意事項

次の表は、各セキュリティレベルでのデバイスの PIN の推奨事項を示しています。

高セキュリティ	より高いセキュリティ	最高のセキュリティ
推奨。デバイスレベルの暗号化には高いセキュリティが必要です。MDM で適用できます。MDX ポリシーを使用して、MAM-only で必要な設定にできます。	MDM および/または MDX ポリシーを使用して適用されます。	MDM および MDX ポリシーを使用して適用されます。MDM の複雑なパスコードポリシー。

注:

- デバイスの PIN を使用することをお勧めします。
- MDM ポリシーを使用してデバイスの PIN を適用できます。
- MDX ポリシーを使用して、管理対象アプリの使用にデバイスの PIN を必須にすることができます（BYOD の使用例など）。
- MDM + MAM 環境では、セキュリティを強化するために MDM と MDX のポリシーオプションを組み合わせることをお勧めします。
- セキュリティ要件が最も高い環境では、複雑なパスコードポリシーを構成し、MDM でこのポリシーを適用できます。デバイスがパスコードポリシーに準拠していない場合は、管理者に通知したり、デバイスの選択的またはフルワイプを発行したりする自動アクションを構成できます。

アプリ

January 10, 2020

エンタープライズモビリティ管理（EMM: Enterprise Mobility Management）は、モバイルデバイス管理（MDM: Mobile Device Management）とモバイルアプリケーション管理（MAM: Mobile Application Management）に分けられます。MDM を利用するとモバイルデバイスを保護し、制御できる一方、MAM ではアプリケーションの配信と管理を簡単に行えます。BYOD（Bring Your Own Device）の導入率が増加した場合、一般的には、アプリケーション配信、ソフトウェアライセンス、構成、アプリケーションライフサイクル管理を支援するため、XenMobile などの MAM ソリューションを実装します。

XenMobile を使用すると、データの漏洩などのセキュリティ上の脅威を防ぐように特定の MAM ポリシーと VPN 設定を構成し、こうしたアプリの保護をさらに強化できます。XenMobile は柔軟性に優れており、MAM 専用環境または MDM 専用環境としてソリューションを展開したり、同一のプラットフォーム内で MDM と MAM の両方の機能を提供する統合 XenMobile Enterprise 環境として XenMobile を実装したりすることができます。

XenMobile は、モバイルデバイスへのアプリ配信機能に加えて、MDX テクノロジーによるアプリのコンテナ化機能も備えています。MDX では、デバイスレベルの暗号化とは別の暗号化によってアプリを保護します。アプリはワイ

プまたはロック可能であり、ポリシーベースで詳細に制御することができます。独立系ソフトウェアベンダー（ISV: Independent Software Vendor）では、Worx App SDK を使用してこうした制御を行うことができます。

企業の環境では、ユーザーは職務の助けとしてさまざまなモバイルアプリを利用しています。こうしたアプリには、パブリックアプリストアのアプリや社内アプリ、場合によってはネイティブアプリも含まれます。XenMobile では、これらのアプリは次のように分類されます：

- パブリックアプリ： これらのアプリには、iTunes や Google Play など、パブリックアプリストアで無料または有料で提供されているアプリが含まれます。組織外のベンダーの多くは、パブリックアプリストアで自社のアプリを公開しています。こうすることで、ベンダーの顧客はインターネットから直接アプリをダウンロードできます。ユーザーのニーズによっては、組織内でパブリックアプリが数多く使用される場合があります。こうしたアプリには、GoToMeeting、Salesforce、EpicCare などがあります。

  Citrix では、パブリックアプリストアからアプリバイナリを直接ダウンロードすることおよび、こうしたバイナリを社内配布用に MDX Toolkit でラップすることはサポートしていません。サードパーティのアプリケーションをラップする必要がある場合は、そのアプリのベンダーと協力して、MDX Toolkit でラップ可能なアプリのバイナリを入手します。

- 社内アプリ： 多くの組織には社内開発者がおり、特定の機能を備え、組織内で独自に開発および配布されるアプリを作成しています。組織によっては、ISV から提供されるアプリを導入している場合もあります。こうしたアプリは、ネイティブアプリとして展開するか、XenMobile などの MAM ソリューションを使用してコンテナ化できます。たとえば、医療機関で、モバイルデバイスで医師が患者の情報を確認できる社内アプリを作成したとします。さらに MDX Toolkit を使用してこのアプリをラップすることで、患者の情報を保護するとともに、バックエンドの患者データベースサーバーへの VPN アクセスを有効化できます。

- **Web** アプリおよび **SaaS** アプリ： これらのアプリには、内部ネットワークからアクセスするアプリ（Web アプリ）やパブリックネットワーク経由でアクセスするアプリ（SaaS）が含まれます。XenMobile では、さまざまなアプリコネクタを使用して、カスタムの Web アプリおよび SaaS アプリを作成することもできます。これらのアプリコネクタを利用することで、既存の Web アプリへのシングルサインオン（SSO：Single Sign-On）を簡単に行えます。詳しくは、「アプリコネクタの種類」を参照してください。たとえば、Google Apps 向けのセキュリティアサーションマークアップランゲージ（SAML：Security Assertion Markup Language）を基にした、SSO 用の Google Apps SAML を使用できます。

- **Citrix** 業務用モバイルアプリ： シトリックスが開発したアプリであり、XenMobile ライセンスに含まれています。詳しくは、「業務用モバイルアプリについて」を参照してください。Citrix では、ISV が Worx App SDK を使用して開発したビジネス対応アプリも提供しています。

- **HDX** アプリ： StoreFront で公開される、Windows でホストされたアプリです。Citrix Virtual Apps and Desktops 環境を使用している場合、こうしたアプリを XenMobile に統合し、登録済みユーザーに公開することができます。

基になる構成およびアーキテクチャは、XenMobile で展開および管理するモバイルアプリの種類によって異なります。たとえば、1 つのアプリを権限レベルの異なる複数のユーザーグループが使用する場合、別々のデリバリーグループを作成して、このアプリを 2 つのバージョンで展開する必要があります。さらに、ユーザーデバイスでのポリシーの不一致を避けるため、ユーザーグループのメンバーシップが相互に排他的であることを確認する必要もあります。

iOS アプリケーションのライセンスは、Apple の Volume Purchase Program（VPP）を使用して管理することもできます。この方法を使用するには、XenMobile コンソールで VPP プログラムを登録し、VPP ライセンスでアプリを配信するように XenMobile の VPP 設定を構成する必要があります。このようにユースケースは多様であるため、XenMobile 環境を実装する前に、MAM 戦略を評価し計画することが重要です。MAM 戦略の計画は、次の事柄を定義することから始めることをお勧めします:

- アプリの種類 - パブリックアプリ、ネイティブアプリ、Worx アプリ、Web アプリ、社内アプリ、ISV アプリなど、サポート予定のアプリの種類をリストアップして分類します。また、iOS や Android などのデバイスプラットフォームごとにもアプリを分類します。このように分類することで、アプリの種類ごとに必要な XenMobile 設定を調整しやすくなります。たとえば、一部のアプリをラップの対象から除外する場合や、いくつかのアプリでほかのアプリとのやりとりを行うために、Worx App SDK を使用して特殊な API を有効化する必要のある場合があります。
- ネットワーク要件 - アプリには、適切に設定した明確なネットワークアクセス要件を構成する必要があります。たとえば、VPN 経由で内部ネットワークにアクセスする必要のあるアプリもあれば、DMZ 経由でアクセスをルーティングするためにインターネットアクセスが必要なアプリもあります。こうしたアプリが必要なネットワークに接続できるようにするには、さまざまな設定を適切に構成しなければなりません。アプリごとのネットワーク要件を定義することで、アーキテクチャに関する決定事項を早期に確定し、実装プロセス全体の効率を高めることができます。
- セキュリティ要件 - 個々またはすべてのアプリに適用されるセキュリティ要件を定義することは、XenMobile サーバーのインストール時に確実に適切な構成を作成するために重要です。MDX ポリシーなどの設定は個々のアプリに適用されますが、セッションと認証の設定はすべてのアプリに適用されます。また、アプリによっては、展開を簡単に行うため、暗号化、コンテナ化、ラップ化、認証、ジオフェンシング、パスコード、あるいはデータ共有に関する特定の要件を事前に定める必要があります。XenMobile のセキュリティの詳細については、「セキュリティとユーザーエクスペリエンス」を参照してください。
- 展開の要件 - 公開したアプリを適合したユーザーのみがダウンロードできるように、ポリシーベースの展開を使用する必要のある場合があります。たとえば、特定のアプリについて、デバイスの暗号化が有効であるかデバイスが管理対象であること、またはデバイスがオペレーティングシステムの最小バージョンを満たしていることを必須にできます。また、特定のアプリをコーポレートユーザーだけに利用可能にする必要のある場合もあります。適切な展開ルールまたはアクションを構成できるように、こうした要件の概要を事前に定める必要があります。
- ライセンス要件 - アプリ関連のライセンス要件を記録することをお勧めします。こうした記録により、ライセンスの使用状況を効率的に管理できるとともに、XenMobile でライセンス管理を容易にする特定の機能を構成する必要があるかを判断できます。たとえば、iOS アプリを展開した場合、そのアプリが無料か有料かにかかわらず、Apple によりユーザーに iTunes アカウントへのサインインが求められ、アプリにライセンス要件が適用されます。こうしたアプリは、Apple VPP に登録することで、XenMobile 経由で配信および管理できます。VPP を利用することで、ユーザーは各自の iTunes アカウントにサインインすることなくアプリをダウンロードできるようになります。さらに、Samsung SAFE や Samsung KNOX などのツールには、機能を展開する前に履行する必要のある特殊なライセンス要件が備わっています。
- ブラックリスト/ホワイトリストの要件 - ユーザーにインストールや使用を禁止する必要のあるアプリも存在します。ブラックリストを作成すると、コンプライアンス違反イベントを定義できます。その後、コンプライ

アンス違反が起きた場合にトリガーされるようにポリシーを設定できます。一方で、使用が容認されるアプリが、なんらかの理由でブラックリストに該当する可能性もあります。このような場合には、ホワイトリストにそのアプリを追加し、アプリは使用してもよいが必須ではないと示すことができます。また、新しいデバイスにあらかじめインストールされているアプリの中には、オペレーティングシステムには含まれていないものの一般的に使用されているアプリもあります。こうしたアプリは、ブラックリスト化の方針に抵触する可能性があります。

使用例

ある医療機関が、同機関のモバイルアプリ向けの MAM ソリューションとして XenMobile を導入する予定を立てました。モバイルアプリは、コーポレートユーザーおよび BYOD ユーザーに配信されます。IT 部門は、次のアプリを配信および管理することを決定しました。

業務用モバイルアプリ: シトリックスが提供する iOS アプリおよび Android アプリ。詳しくは、「業務用モバイルアプリ」を参照してください。

Citrix Secure Hub: すべてのモバイルデバイスで XenMobile との通信に使用するクライアント。IT 部門では、Secure Hub を経由してセキュリティ設定、構成、およびモバイルアプリをモバイルデバイスにプッシュします。Android デバイスおよび iOS デバイスは、Secure Hub 経由で XenMobile に登録されます。

Citrix Receiver: モバイルデバイスユーザーが Citrix Virtual Apps でホストされているアプリケーションを開くことができるモバイルアプリ。

GoToMeeting: ほかのコンピューターユーザー、顧客、クライアント、同僚とインターネット経由でリアルタイムに話し合うことができる、オンライン会議、デスクトップ共有、ビデオ会議用クライアント。

SalesForce1: モバイルデバイスから Salesforce へのアクセスを可能にし、あらゆる Salesforce ユーザーが統一されたエクスペリエンスで Chatter、CRM、カスタムアプリ、およびビジネスプロセスを利用できるようにするモバイルアプリ。

RSA SecurID: 2 要素認証用のソフトウェアベーストークン。

EpicCare アプリ: 医療従事者がモバイルデバイスで患者のカルテおよびリスト、スケジュールに安全にアクセスし、メッセージを通信できるようにするアプリ。

Haiku: iPhone および Android スマートフォン向けのモバイルアプリ。

Canto: iPad 用モバイルアプリ

Rover: iPhone および iPad 用のモバイルアプリ。

HDX: これらのアプリは、Citrix Virtual Apps 経由で配信されます。

- **Epic Hyperspace**: 電子カルテ管理用の Epic のクライアントアプリケーション。

ISV:

- **Vocera**: iPhone や Android スマートフォンで時間や場所を問わず Vocera 音声技術を利用できるようにする、HIPAA に準拠したボイスオーバー IP およびメッセージ用モバイルアプリ。

社内アプリ:

- **HCMail**: 暗号化されたメッセージを作成し、内部メールサーバー上のアドレス帳を検索して、暗号化されたメッセージをメールクライアントで連絡先へ送信できるアプリ。

社内 **Web** アプリ:

- **PatientRounding**: 複数の部署で患者の健康情報の記録に使用する Web アプリケーション。
- **Outlook Web Access**: Web ブラウザー経由でメールにアクセスできるようになります。
- **SharePoint**: 組織全体でのファイルおよびデータの共有に使用します。

次の表に、MAM の構成に必要な基本情報を示します。

アプリ名	アプリの種類	**MDX** によるラップ	**iOS**	**Android**
Secure Mail	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
Secure Web	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
Secure Notes	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
ShareFile	XenMobile アプリ	バージョン 10.4.1 以降では ×	はい	はい
Secure Hub	パブリックアプリ	-	はい	はい
Citrix Receiver	パブリックアプリ	-	はい	はい
GoToMeeting	パブリックアプリ	-	はい	はい
SalesForce1	パブリックアプリ	-	はい	はい
RSA SecurID	パブリックアプリ	-	はい	はい
Epic Haiku	パブリックアプリ	-	はい	はい
Epic Canto	パブリックアプリ	-	はい	いいえ
Epic Rover	パブリックアプリ	-	はい	いいえ
Epic Hyperspace	HDX アプリ	-	はい	はい
Vocera	ISV アプリ	はい	はい	はい
HCMail	社内アプリ	はい	はい	はい
PatientRounding	Web アプリ	-	はい	はい
Outlook Web Access	Web アプリ	-	はい	はい

SharePoint	Web アプリ	-	はい	はい

次の表に、XenMobile での MAM ポリシーの構成の参考要件を示します。

アプリ名	**VPN** の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	デバイスの暗号化	プロキシのフィルタリング	ライセンス	ジオフェンシング	**Worx App SDK**	オペレーティングシステムの最小バージョン
Secure Mail	☒	選択的に許可	許可	不要	必須	-	選択的に必須化	-	適用する
Secure Web	☒	許可	許可	不要	必須	-	不要	-	適用する
Secure Notes	☒	許可	許可	不要	必須	-	不要	-	適用する
ShareFile	☒	許可	許可	不要	必須	-	不要	-	適用する
Secure Hub	☒	-	-	-	不要	VPP	不要	-	適用しない
Citrix Re-ceiver	☒	-	-	-	不要	VPP	不要	-	適用しない
GoToMe	×	-	-	-	不要	VPP	不要	-	適用しない
SalesForce	☒1	-	-	-	不要	VPP	不要	-	適用しない
RSA Se-curID	×	-	-	-	不要	VPP	不要	-	適用しない
Epic Haiku	☒	-	-	-	不要	VPP	不要	-	適用しない

アプリ名	**VPN** の要否	通信（コンテナ外のアプリに対して）	通信（コンテナ外のアプリから）	デバイスの暗号化	プロキシのフィルタリング	ライセンス	ジオフェンシング	**Worx App SDK**	オペレーティングシステムの最小バージョン
Epic Canto		-	-	-	不要	VPP	不要	-	適用しない
Epic Rover		-	-	-	不要	VPP	不要	-	適用しない
Epic Hyper-space		-	-	-	不要	-	不要	-	適用しない
Vocera		禁止	禁止	不要	必須	-	必須	必須	適用する
HCMail		禁止	禁止	必須	必須	-	必須	必須	適用する
PatientRounding		-	-	必須	必須	-	不要	-	適用しない
Outlook Web Access		-	-	不要	必須	-	不要	-	適用しない
SharePoint		-	-	不要	必須	-	不要	-	適用しない

ユーザーコミュニティ

July 5, 2019

すべての組織は、異なる機能的役割を持つ多様なユーザーコミュニティで構成されています。これらのユーザーコミュニティは、ユーザーのモバイルデバイスを通して提供されるさまざまなリソースを使用して、さまざまなタスクを実行しオフィス機能を果たします。ユーザーは、提供されたモバイルデバイスを使用して、自宅やリモートオフィスで作業する場合もあります。また、特定のセキュリティコンプライアンスルールの対象となるツールへのアクセスが許可された個人のモバイルデバイスを使用する場合もあります。

モバイルデバイスを使用するユーザーコミュニティが増えるにつれ、データ漏洩を防止し、組織のセキュリティ制限を実施するために、エンタープライズモビリティ管理（EMM）が非常に重要になります。効率的で高度なモバイルデバイス管理を実現するために、ユーザーコミュニティを分類することができます。そうすることにより、ユーザーとリソースのマッピングが簡素化され、適切なセキュリティポリシーを適切なユーザーに適用できます。

ユーザーコミュニティを分類するには、次のコンポーネントを使用できます。

- Active Directory 組織単位（OU）とグループ

  特定の Active Directory セキュリティグループに追加されたユーザーは、ポリシーと、アプリなどのリソースを受け取ることができます。Active Directory セキュリティグループからユーザーを削除すると、以前に許可された XenMobile リソースへのアクセスが削除されます。

- XenMobile のローカルユーザーとグループ

  Active Directory にアカウントを持たないユーザーの場合は、ローカルの XenMobile ユーザーとしてユーザーを作成できます。ローカルユーザーをデリバリーグループに追加し、Active Directory ユーザーと同じ方法でリソースをプロビジョニングできます。

- XenMobile デリバリーグループ

  権限レベルの異なるユーザーからなる複数のグループが 1 つのアプリを使用する場合は、個別のデリバリーグループの作成が必要になる場合があります。個別のデリバリーグループを使用すると、同じアプリの 2 つの異なるバージョンを展開できます。

- デリバリーグループとユーザーグループのマッピング

  デリバリーグループと Active Directory グループのマッピングは、1 対 1 または 1 対多のいずれでもかまいません。基本のポリシーとアプリを 1 対多のデリバリーグループマッピングに割り当てます。機能に固有のポリシーとアプリを 1 対 1 のデリバリーグループマッピングに割り当てます。

- アプリのデリバリーグループとリソースのマッピング

  特定のアプリを各デリバリーグループに割り当てます。

- MDM リソースのデリバリーグループとリソースのマッピング

  アプリと特定のデバイス管理リソースを各デリバリーグループに割り当てます。たとえば、アプリの種類（パブリック、HDX など）、アプリの種類別の特定のアプリ、リソース（デバイスポリシーや自動アクションなど）を任意に組み合わせてデリバリーグループを設定します。

次の例は、医療機関のユーザーコミュニティにおける EMM 向けの分類方法を示したものです。

使用例

この医療機関の例では、ネットワークやアフィリエイトの従業員、ボランティアなどの複数のユーザーに技術リソースやアクセスを提供します。この組織は EMM ソリューションを非幹部ユーザーのみに展開することを選択しました。

この医療機関のユーザー役割と機能は、医療、医療以外、契約社員などのサブグループに分けられます。指定されたグループのユーザーが企業のモバイルデバイスを受け取ります。その他のユーザーは個人のデバイス（BYOD）から限られた企業リソースにアクセスできます。適切なレベルのセキュリティ制限を実施し、データ漏洩を防止するために、この組織では、登録された各デバイスを企業の IT 部門が管理することに決定しました。また、ユーザーが登録できるデバイスは 1 台のみです。

以下のセクションでは、各サブグループの役割と機能の概要について説明します。

臨床

- 看護師
- 医師（医師、外科医など）
- スペシャリスト（栄養士、採血師、麻酔医、放射線科医、心臓病専門医、がん専門医など）
- 外部の医師（外来の医師とリモートオフィスで作業するオフィスワーカー）
- 在宅医療サービス（患者の往診で医療サービスを行うオフィスワーカーとモバイルワーカー）
- 研究スペシャリスト（医薬における問題解決のための臨床研究を行う 6 つの研究機関のナレッジワーカーとパワーユーザー）
- 教育と訓練（教育と訓練に従事する看護師、医師、スペシャリスト）

医療以外

- 共通サービス（人事、給与、財務、サプライチェーンサービスなどのさまざまなバックオフィス機能を果たすオフィスワーカー）
- 医療サービス（管理サービス、分析およびビジネスインテリジェンス、ビジネスシステム、クライアントサービス、財務、総合的健康管理、患者アクセスソリューション、収益サイクルソリューションなどの、さまざまな医療管理、管理サービス、ビジネスプロセスソリューションをプロバイダーに提供するオフィスワーカー）
- サポートサービス（福利厚生管理、医療の統合、コミュニケーション、報酬および業績管理、施設および土地サービス、ヒューマンリソーステックシステム、情報サービス、内部監査およびプロセス改善など、医療以外のさまざまな機能を果たすオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するさまざまな機能を果たすオフィスワーカーとモバイルワーカー）

契約社員

- メーカーやベンダーのパートナー（オンサイト、またはサイト間 VPN 経由でリモート接続された、医療以外のさまざまなサポート機能を提供する人々）

上記の情報に基づいて、この医療機関では以下のエンティティを作成しました。XenMobile のデリバリーグループの詳細については、XenMobile 製品ドキュメントの「リソースの展開」を参照してください。

Active Directory 組織単位（**OU**）とグループ

OU = XenMobile リソース

- OU = 医療; グループ =
  - XM-看護師
  - XM-医師
  - XM-スペシャリスト
  - XM-外部の医師
  - XM-在宅医療サービス
  - XM-研究スペシャリスト
  - XM-教育と訓練
- OU = 医療以外; グループ =
  - XM-共通サービス
  - XM-医療サービス
  - XM-サポートサービス
  - XM-慈善プログラム

XenMobile のローカルユーザーとグループ

グループ = 契約社員、ユーザー =

- ベンダー 1
- ベンダー 2
- ベンダー 3
- …ベンダー 10

XenMobile デリバリーグループ

- 医療-看護師
- 医療-医師
- 医療-スペシャリスト
- 医療-外部の医師
- 医療-在宅医療サービス
- 医療-研究スペシャリスト
- 医療-教育と訓練
- 医療以外-共通サービス
- 医療以外-医療サービス
- 医療以外-サポートサービス
- 医療以外-慈善プログラム

デリバリーグループとユーザーグループのマッピング

Active Directory グループ	**XenMobile** デリバリーグループ
XM-看護師	医療-看護師
XM-医師	医療-医師
XM-スペシャリスト	医療-スペシャリスト
XM-外部の医師	医療-外部の医師
XM-在宅医療サービス	医療-在宅医療サービス
XM-研究スペシャリスト	医療-研究スペシャリスト
XM-教育と訓練	医療-教育と訓練
XM-共通サービス	医療以外-共通サービス
XM-医療サービス	医療以外-医療サービス
XM-サポートサービス	医療以外-サポートサービス
XM-慈善プログラム	医療以外-慈善プログラム

アプリのデリバリーグループとリソースのマッピング

	Secure Mail	**Secure Web**	**Secure Notes**	**ShareFil**	**Receive**	**SalesFo**	**RSA Se-curID**	**EpicCar Haiku**	**Epic Hy-per-space**
医療-看護師	☒	☒	☒	☒					
医療-医師									
医療-スペシャリスト									
医療-外部の医師	☒		☒	☒					

医療-在宅医療サービス	☒		☒	☒				
医療-研究スペシャリスト	☒		☒	☒				
医療-教育と訓練							☒	☒
医療以外-共通サービス							☒	☒
医療以外-医療サービス							☒	☒
医療以外-サポートサービス	☒		☒	☒			☒	☒
医療以外-慈善プログラム	☒		☒	☒			☒	☒
契約社員	☒		☒	☒	☒	☒	☒	☒

MDM リソースのデリバリーグループとリソースのマッピング

	MDM: パスコードポリシー	**MDM**: デバイスの制限事項	**MDM**: 自動化された操作	**MDM**: **Wi-Fi** ポリシー

医療-看護師		☒
医療-医師	☒	
医療-スペシャリスト		
医療-外部の医師		
医療-在宅医療サービス		
医療-研究スペシャリスト		
医療-教育と訓練		
医療以外-共通サービス		
医療以外-医療サービス		
医療以外-サポートサービス		
医療以外-慈善プログラム		
契約社員		☒

注意事項と考慮事項

- XenMobile は初期構成時に「すべてのユーザー」というデフォルトのデリバリーグループを作成します。このデリバリーグループを無効にしないと、すべての Active Directory ユーザーに XenMobile への登録権限が付与されます。
- XenMobile は、LDAP サーバーとの動的接続により Active Directory のユーザーとグループをオンデマンドで同期します。
- ユーザーが XenMobile にマップされていないグループに属している場合、そのユーザーは登録できません。同様に、ユーザーが複数のグループのメンバーである場合、XenMobile はユーザーを XenMobile にマップされているグループにのみ分類します。
- MDM の登録を必須にするには、XenMobile コンソールで ［サーバープロパティ］ の ［登録が必要］ オプションを ［はい］ に設定します。詳しくは、「サーバープロパティ」を参照してください。
- XenMobile デリバリーグループからユーザーグループを削除するには、dbo.userlistgrps 内にある SQL

Server データベースのエントリを削除します。

> 注意：
>
> この操作を実行する前に、XenMobile とデータベースのバックアップを作成してください。

XenMobile のデバイスの所有権について

ユーザーデバイスの所有者に応じてユーザーをグループ化できます。デバイスの所有権には、企業所有のデバイスと、BYOD（Bring Your Own Device）とも呼ばれるユーザー所有のデバイスがあります。XenMobile コンソールの 2 つの場所（［設定］ページの［展開規則］と XenMobile Server プロパティ）で、BYOD デバイスをネットワークに接続する方法を制御できます。展開規則の詳細については、XenMobile のドキュメントの「リソースの展開」を参照してください。サーバープロパティの詳細については、このハンドブックの「サーバープロパティ」を参照してください。

サーバープロパティを設定することで、すべての BYOD ユーザーに対して企業によるデバイス管理を受け入れてからアプリにアクセスするように要求できます。または、ユーザーのデバイスを管理せずに、ユーザーに企業アプリへのアクセス権を付与することもできます。

サーバープロパティ **wsapi.mdm.required.flag** を **true** に設定すると、XenMobile がすべての BYOD デバイスを管理し、登録を拒否したユーザーはアプリへのアクセスが拒否されます。企業の IT チームが登録中に高いセキュリティと優れたユーザーエクスペリエンスを必要とする環境では、**wsapi.mdm.required.flag** を **true** に設定することを検討してください。

wsapi.mdm.required.flag をデフォルト設定の **false** にしておくと、ユーザーは登録を拒否できます。ただし、ユーザーは XenMobile Store からデバイス上のアプリにアクセスできます。プライバシー、法律、または規制上の制約によりデバイスの管理が不要で、エンタープライズアプリの管理のみが必要な環境では、**wsapi.mdm.required.flag** を **false** に設定することを検討してください。

XenMobile が管理しないデバイスを持つユーザーは、XenMobile Store からアプリをインストールできます。選択的ワイプや完全なワイプなどのデバイスレベルの制御ではなく、アプリポリシーに従ってアプリへのアクセスを制御します。一部のポリシー設定では、デバイスが XenMobile Server を定期的にチェックして、アプリの実行が引き続き許可されていることを確認する必要があります。

メール戦略

May 21, 2019

モバイルデバイスからメールに安全にアクセスできるようにすることは、組織のモビリティ管理の取り組みを推進するうえで主要な要因の 1 つです。適切なメール戦略を決定することは、XenMobile 設計の鍵となる要素です。XenMobile では、セキュリティ、ユーザーエクスペリエンス、および統合の要件に基づいて、さまざまなユースケー

スに対応するためのオプションを提供しています。この記事では、クライアントの選択からメールのトラフィックフローまで、最適なソリューションを選択するための典型的な設計決定プロセスと考慮事項について説明します。

メールクライアントの選択

通常、クライアントの選択は、メール戦略の設計全体において最初に実行すべき項目です。Citrix Secure Mail、特定のモバイルプラットフォームのオペレーティングシステムに含まれるネイティブメール、またはパブリックアプリストアを通じて利用できる他のサードパーティクライアントから選択できます。必要に応じて、単一の（標準）クライアントを使用したり、クライアントの組み合わせを使用したりして、ユーザーコミュニティをサポートできます。

次の表に、使用可能なさまざまなクライアントオプションで設計上考慮すべき事項を示します。

トピック	**Secure Mail**	ネイティブ（**iOS Mail** など）	サードパーティのメール（**TouchDown** など）
XenMobile の最小エディション	詳細設定	MDM	MDM
構成	MDX ポリシーによって構成された Exchange アカウントプロファイル。	MDM ポリシーによって構成された Exchange アカウントプロファイル。Android のサポートは次に限定されます: SAFE/KNOX、HTC、および Android Enterprise。他のすべてのクライアントはサードパーティのクライアントと見なされます。	一般に、ユーザーが手動で構成する必要があります。TouchDown のみ、MDM ポリシーを介した Exchange アカウントプロファイルの構成。
セキュリティ	これ自体がセキュアに設計されており、最高のセキュリティを提供します。データ暗号化レベルが強化された MDX ポリシーを使用します。Secure Mail は、MDX ポリシーによって完全に管理されているアプリです。Citrix PIN により、認証が強化されています。	ベンダーおよびアプリの機能セットに基づきます。より高いセキュリティを提供します。デバイスの暗号化設定を使用します（MDX ポリシーによるセキュリティなし）。アプリへのアクセスでデバイスレベルの認証に依存します。	ベンダーおよびアプリの機能セットに基づきます。高いセキュリティを提供します。

統合	デフォルトで管理対象（MDX）アプリの操作を許可します。Citrix Secure Web で Web URL を開きます。ShareFile にファイルを保存し、ShareFile からファイルを添付します。GoToMeeting への直接参加およびダイヤルイン。	デフォルトでは、他の非管理対象（非 MDX）アプリのみ操作できます。	デフォルトでは、他の非管理対象（非 MDX）アプリのみ操作できます。
展開/ライセンス	MDM を通じて、パブリックアプリストアから直接 Secure Mail をプッシュできます。XenMobile の Advanced および Enterprise Edition のライセンスに含まれています。	クライアントアプリは、プラットフォームのオペレーティングシステムに含まれています。追加のライセンス要件はありません。	エンタープライズアプリとして MDM 経由で、またはパブリックアプリストアから直接、プッシュできます。アプリベンダーに基づき、関連ライセンスモデル/コスト。
サポート	クライアントおよび EMM ソリューションを提供する単一ベンダーのサポート（Citrix）。Secure Hub/アプリのデバッグログ機能にサポートの連絡先情報が埋め込まれています。サポートするクライアントは 1 つです。	ベンダーによって定義されたサポート（Apple/Google）。デバイスのプラットフォームに基づいて異なるクライアントをサポートする必要がある場合があります。	ベンダーによって定義されたサポート。サードパーティのクライアントがすべての管理対象デバイスプラットフォームでサポートされていることを前提に、1 つのクライアントをサポートします。

メールのトラフィックフローとフィルタリングに関する考慮事項

ここでは、XenMobile のコンテキストでのメール（ActiveSync）のトラフィックフローに関する 3 つの主要なシナリオと設計上の考慮事項について説明します。

シナリオ **1**: インターネットに接続された **Exchange**

外部クライアントをサポートする環境では、通常、Exchange ActiveSync サービスがインターネットに接続されています。モバイルの ActiveSync クライアントは、この外部に対するパスを通じて、リバースプロキシ（NetScaler など）またはエッジサーバーを介して接続します。このオプションは、ネイティブまたはサードパーティのメールクライアントを使用する場合に必要です。このため、このシナリオではこれらのクライアントが一般的な選択になります。また、一般的な方法ではありませんが、このシナリオで Secure Mail クライアントを使用することもできます。これにより、MDX ポリシーの使用とアプリの管理によって提供されるセキュリティ機能のメリットが得られます。

シナリオ **2**: **NetScaler** 経由のトンネリング（マイクロ **VPN** および **STA**）

Secure Mail の Micro VPN 機能により、Secure Mail クライアントを使用する場合はこのシナリオがデフォルトになります。この場合、Secure Mail クライアントは、NetScaler Gateway 経由で ActiveSync へのセキュリティで保護された接続を確立します。本質的に、Secure Mail は、内部ネットワークから ActiveSync に直接接続するクライアントと考えることができます。通常 Citrix のお客様は、最適なモバイル ActiveSync クライアントとして Secure Mail を標準に決定します。この決定は、1 つ目のシナリオで説明したように、インターネットに接続された Exchange Server 上で、ActiveSync サービスがインターネットに接続されないようにする取り組みの一部です。

管理対象（MDX でラップされた）アプリのみが Micro VPN 機能を使用できます。したがって、このシナリオはネイティブクライアントには適用されません。MDX Toolkit を使用してサードパーティのクライアントをラップすることは可能ですが、この方法は一般的ではありません。ネイティブまたはサードパーティのクライアントにトンネルを介したアクセスを許可するためにデバイスレベルの VPN クライアントを使用することは煩雑であり、実行可能なソリューションではないことが実証されています。

シナリオ **3**: クラウドでホストされた **Exchange** サービス

クラウドでホストされた Exchange サービス（Microsoft Office 365 など）の普及が進んでいます。ActiveSync サービスもインターネットに接続しているため、XenMobile のコンテキストでは、このシナリオは 1 つ目のシナリオと同じように扱うことができます。この場合、クラウドサービスプロバイダーの要件によってクライアントの選択が決まります。一般的にこの選択には、Secure Mail や他のネイティブクライアントまたはサードパーティクライアントなど、ほとんどの ActiveSync クライアントのサポートが含まれます。

このシナリオでは、XenMobile は次の 3 つの領域で価値を付加できます:

- MDX ポリシーによるクライアントのラッピングと Secure Mail によるアプリの管理
- サポートされているクライアント（TouchDown などのネイティブ）での MDM ポリシーを使用したクライアント構成
- Endpoint Management コネクタ: Exchange ActiveSync 用を使用した ActiveSync のフィルターオプション

メールトラフィックのフィルタリングに関する考慮事項

インターネットに接続している大半のサービスと同様に、パスを保護し、承認されたアクセスに対してフィルターを提供する必要があります。XenMobile ソリューションには、ネイティブクライアントとサードパーティクライアントに ActiveSync のフィルタリング機能を提供するために特別に設計された 2 つのコンポーネントである、Citrix Gateway コネクタ：Exchange ActiveSync 用、Endpoint Management コネクタ：Exchange ActiveSync 用が含まれています。

Citrix Gateway コネクタ：Exchange ActiveSync 用

Citrix Gateway コネクタ：Exchange ActiveSync 用は、ActiveSync トラフィックのプロキシとして NetScaler を使用して、境界で ActiveSync フィルタリングを提供します。その結果、フィルタリングコンポーネントはメールトラフィックフローのパスの一部として、メールが環境に出入りする時にインターセプトします。Citrix Gateway コネクタ：Exchange ActiveSync 用は、NetScaler と XenMobile Server 間の仲介役を果たします。デバイスが NetScaler 上の ActiveSync 仮想サーバーを介して Exchange と通信する場合、NetScaler は Exchange ActiveSync サービス用コネクタに対して HTTP コールアウトを実行します。このサービスは、XenMobile を使用してデバイスの状態を確認します。Exchange ActiveSync 用コネクタは NetScaler に応答し、デバイスの状態に基づいて接続を許可または拒否します。また、ユーザー、エージェント、デバイスの種類や ID に基づいてアクセスをフィルターするように静的規則を構成することもできます。

この設定では、不正なアクセスを防ぐためにセキュリティレイヤーを追加して、Exchange ActiveSync サービスのインターネットへの接続を許可します。設計上の考慮事項は次のとおりです：

- Windows Server：Exchange ActiveSync 用コネクタコンポーネントには Windows Server が必要です。
- フィルター規則のセット：Exchange ActiveSync 用コネクタは、ユーザー情報ではなくデバイスの状態と情報に基づいてフィルターするように設計されています。ユーザー ID でフィルターするように静的規則を構成することもできますが、たとえば Active Directory グループのメンバーシップに基づいてフィルターするオプションはありません。Active Directory グループのフィルターが必要な場合は、代わりに Endpoint Management コネクタ：Exchange ActiveSync 用を使用できます。
- NetScaler のスケーラビリティ：NetScaler を介した ActiveSync トラフィックのプロキシ要件を考慮すると、すべての ActiveSync SSL 接続によって追加されたワークロードをサポートするには、NetScaler インスタンスの適切なサイズ設定が不可欠です。
- NetScaler 統合キャッシュ：NetScaler 上の Exchange ActiveSync 用コネクタの構成では、統合キャッシュ機能を使用して Exchange ActiveSync 用コネクタからの応答をキャッシュします。この構成により、NetScaler では、特定のセッション内のすべての ActiveSync トランザクションに対して Citrix Gateway コネクタ：Exchange ActiveSync 用に要求を発行する必要がありません。適切なパフォーマンスとスケーラビリティを実現するにはこの構成も不可欠です。統合キャッシュは、NetScaler Platinum Edition で使用できます。また、Enterprise Edition では個別に機能のライセンスを取得できます。
- カスタムのフィルターポリシー：カスタムの NetScaler ポリシーを作成して、特定の ActiveSync クライアントを標準のネイティブモバイルクライアント以外に制限する必要がある場合があります。この構成では、ActiveSync HTTP 要求と NetScaler のレスポンダーポリシーの作成に関する知識が必要です。

- Secure Mail クライアント: Secure Mail には Micro VPN 機能があるため、境界でのフィルターが不要になります。一般に、Secure Mail クライアントは、NetScaler Gateway を介して接続されている場合、内部の（信頼できる）ActiveSync クライアントとして扱われます。ネイティブおよびサードパーティクライアント（Exchange ActiveSync 用コネクタを使用）、および Secure Mail クライアントのサポートが必要な場合: Secure Mail のトラフィックが、Exchange ActiveSync 用コネクタで使用される NetScaler 仮想サーバー経由でフローしないようにすることをお勧めします。これを実行するには、トラフィックが DNS 経由でフローし、Exchange ActiveSync 用コネクタポリシーが Secure Mail クライアントに影響を与えないようにします。

XenMobile 展開の Citrix Gateway コネクタ: Exchange ActiveSync 用の図については、「オンプレミス環境のリファレンスアーキテクチャ」を参照してください。

Endpoint Management コネクタ: Exchange ActiveSync 用

Endpoint Management コネクタ: Exchange ActiveSync 用は、Exchange サービスレベルで ActiveSync フィルタを提供する XenMobile コンポーネントです。つまり、メールが XenMobile 環境に到達した時ではなく、Exchange サービスに到達した後にのみフィルタリングが行われます。Mail Manager は、PowerShell を使用して Exchange ActiveSync にデバイスパートナーシップ情報のクエリを実行し、デバイスの隔離操作を通じてアクセスを制御します。これらのアクションは、Endpoint Management コネクタ: Exchange ActiveSync 用の規則条件に基づいて、デバイスを検疫に出し入れします。Citrix Gateway コネクタ: Exchange ActiveSync 用と同様に、Endpoint Management コネクタ: Exchange ActiveSync 用では XenMobile を使用してデバイスの状態を確認し、デバイスのコンプライアンスに基づいてアクセスをフィルターします。また、デバイスの種類や ID、エージェントのバージョン、Active Directory グループのメンバーシップに基づいてアクセスをフィルターするように静的規則を構成することもできます。

このソリューションでは、NetScaler を使用する必要はありません。既存の ActiveSync トラフィックのルーティングに変更を加えることなく、Endpoint Management コネクタ: Exchange ActiveSync 用を展開できます。設計上の考慮事項は次のとおりです:

- Windows Server: Endpoint Management コネクタ: Exchange ActiveSync 用には Windows Server の展開が必要です。
- フィルター規則のセット: Citrix Gateway コネクタ: Exchange ActiveSync 用と同様に、Endpoint Management コネクタ: Exchange ActiveSync 用には、デバイスの状態を評価するためのフィルター規則が含まれています。さらに、Endpoint Management コネクタ: Exchange ActiveSync 用は、Active Directory グループのメンバーシップに基づいてフィルターする静的規則をサポートしています。
- Exchange の統合: Endpoint Management コネクタ: Exchange ActiveSync 用では、ActiveSync の役割をホストしている Exchange クライアントアクセスサーバー（CAS）に直接アクセスし、デバイスの隔離操作を制御する必要があります。環境アーキテクチャとセキュリティ状況によっては、この要件により課題がもたらされる可能性があります。この技術要件を前もって評価することが重要です。
- 他の ActiveSync クライアント: Endpoint Management コネクタ: Exchange ActiveSync 用は ActiveSync サービスレベルでフィルターするため、XenMobile 環境外の他の ActiveSync クライアントにつ

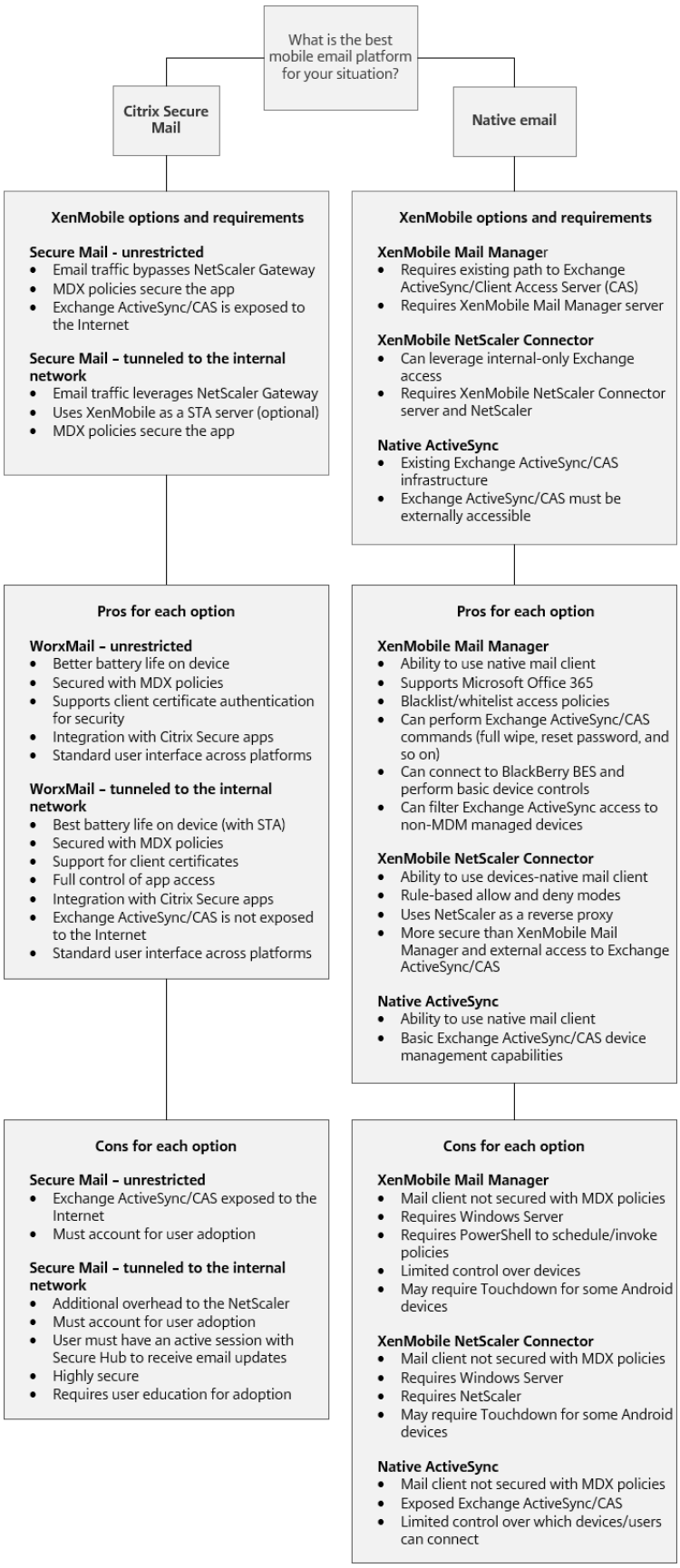
いて考慮します。Endpoint Management コネクタ: Exchange ActiveSync 用の静的規則を構成して、他の ActiveSync クライアントへの意図しない影響を防ぐことができます。

- 拡張された Exchange 機能: Exchange ActiveSync との直接統合により、Endpoint Management コネクタ: Exchange ActiveSync 用は、モバイルデバイス上で Exchange ActiveSync のワイプを実行する機能を XenMobile に提供します。また Endpoint Management コネクタ: Exchange ActiveSync 用では、XenMobile が Blackberry デバイスに関する情報にアクセスしたり、その他の制御操作を実行することを許可します。

XenMobile 展開の Endpoint Management コネクタ: Exchange ActiveSync 用の図については、「オンプレミス環境のリファレンスアーキテクチャ」を参照してください。

電子メールプラットフォーム決定木

次の図は、XenMobile の展開でネイティブメールまたは Secure Mail のソリューションを使用する場合のメリットとデメリットを理解するのに役立ちます。選択ごとに、サーバー、ネットワーク、およびデータベースにアクセスするための XenMobile の関連オプションと要件がまとめられています。メリットとデメリットには、セキュリティ、ポリシー、およびユーザーインターフェイスの考慮事項に関する詳細が含まれています。



XenMobile 統合

October 25, 2019

この記事では、XenMobile を既存のネットワークおよびソリューションと統合する方法を計画するときに考慮すべき点について説明します。たとえば、Virtual Apps and Desktops 用の NetScaler を既に使用している場合は、次の点を考慮します：

- 既存の NetScaler インスタンス、または専用の新しいインスタンスを使用する必要がありますか。
- StoreFront を使用して公開されている HDX アプリを XenMobile と統合しますか。
- XenMobile で ShareFile を使用する予定ですか。
- XenMobile に統合するネットワークアクセス制御のソリューションがありますか。
- ネットワークからのすべてのアウトバウンドトラフィックに対して Web プロキシを展開していますか。

NetScaler および NetScaler Gateway

NetScaler Gateway は、XenMobile の ENT モードと MAM モードで必須です。NetScaler Gateway は、すべての企業リソースにアクセスするためのマイクロ VPN パスを提供し、強力な多要素認証をサポートします。次の場合、すべての XenMobile サーバーデバイスモードで NetScaler の負荷分散が必要です：

- XenMobile Server が複数ある場合。
- または、XenMobile Server が DMZ または内部ネットワーク内にある場合（つまり、デバイスから NetScaler、XenMobile の順にトラフィックが流れる場合）

既存の NetScaler インスタンスを使用することも、XenMobile 用に新しいインスタンスを設定することもできます。以下のセクションでは、既存、または新規の専用の NetScaler インスタンスを使用するメリットとデメリットについて説明します。

XenMobile 用に作成された NetScaler Gateway VIP を使用した共有 NetScaler MPX

長所：

- Citrix のすべてのリモート接続：Citrix Virtual Apps and Desktops、完全 VPN、およびクライアントレス VPN に共通の NetScaler インスタンスを使用します。
- 証明書の認証や DNS、LDAP、NTP などのサービスへのアクセスに、NetScaler の既存の構成を使用します。
- 単一の NetScaler プラットフォームライセンスを使用します。

短所：

- 同じ NetScaler で 2 つの大きく異なるユースケースを処理する場合は、スケールの計画が難しくなります。
- Citrix Virtual Apps and Desktops のユースケースに特定のバージョンの NetScaler が必要になる場合があります。この特定のバージョンで、XenMobile の既知の問題がある場合があります。または、XenMobile に、NetScaler のこのバージョンに関する既知の問題がある場合があります。

- NetScaler Gateway がある場合は、XenMobile 用の NetScaler 構成を作成するために、NetScaler for XenMobile ウィザードを再度実行することはできません。
- Platinum ライセンスが NetScaler Gateway 11.1 以降で使用されている場合を除き、NetScaler にインストールされ、VPN 接続に必要なユーザーアクセスライセンスはプールされます。これらのライセンスはすべての NetScaler 仮想サーバーで使用可能であるため、XenMobile 以外のサービスによってライセンスが消費される可能性があります。

専用の **NetScaler VPX/MPX** インスタンス

長所:

専用の NetScaler インスタンスを使用することをお勧めします。

- スケールの計画が容易になるほか、既にリソースの制約がある可能性のある NetScaler インスタンスから XenMobile のトラフィックが分離されます。
- XenMobile と Citrix Virtual Apps and Desktops で必要な NetScaler ソフトウェアのバージョンが異なる事態を回避できます。通常、XenMobile と互換性のある最新の NetScaler バージョンおよびビルドを使用することをお勧めします。
- 組み込みの NetScaler for XenMobile ウィザードを使用して、XenMobile 用に NetScaler を構成できます。
- サービスの仮想的および物理的な分離。
- NetScaler Gateway 11.1 以降で Platinum ライセンスが使用されている場合を除きます: XenMobile に必要なユーザーアクセスライセンスは、NetScaler 上の XenMobile サービスでのみ使用できます。

短所:

- XenMobile の構成をサポートするために、NetScaler で追加のサービスを設定する必要があります。
- 別の NetScaler プラットフォームライセンスが必要です。NetScaler Gateway の NetScaler インスタンスごとにライセンスを取得します。

XenMobile サーバーの各モードで NetScaler と NetScaler Gateway を統合するときに考慮すべき点については、「NetScaler と NetScaler Gateway の統合」を参照してください。

StoreFront

Citrix Virtual Apps and Desktops 環境の場合は、StoreFront を使用して HDX アプリケーションを XenMobile と統合できます。HDX アプリを XenMobile と統合すると:

- XenMobile に登録されているユーザーがこのアプリを利用できます。
- このアプリが、XenMobile Store で他のモバイルアプリと共に表示されます。
- XenMobile は、StoreFront の従来の PNAgent（サービス）サイトを使用します。
- Citrix Receiver がデバイスにインストールされると、HDX アプリはこの Citrix Receiver の使用を開始します。

StoreFront には、StoreFront インスタンスごとに 1 つのサービスサイトの制限があります。複数のストアがあり、他の実稼働環境での使用から分離する必要があるとします。その場合は、通常、XenMobile 用の新しい StoreFront インスタンスとサービスサイトを検討することをお勧めします。

考慮事項は次のとおりです:

- StoreFront では認証要件が異なりますか。StoreFront サービスサイトでは、ログオンに Active Directory 資格情報が必要です。証明書ベースの認証のみを使用するユーザーは、同じ NetScaler Gateway を使用して XenMobile 経由でアプリケーションを列挙することはできません。
- 同じストアを使用しますか。それとも新しいストアを作成しますか。
- 同じ StoreFront サーバーを使用しますか。それとも別の StoreFront サーバーを使用しますか。

以下のセクションでは、Citrix Receiver と業務用モバイルアプリで StoreFront を個別に使用する場合と組み合わせて使用する場合のメリットとデメリットについて説明します。

既存の **StoreFront** インスタンスを **XenMobile** サーバーと統合する

長所:

- 同じストア: HDX アクセスに同じ NetScaler VIP を使用する場合、XenMobile では StoreFront の追加の構成が不要です。同じストアを使用する選択をし、Citrix Receiver が新しい NetScaler VIP にアクセスするように指示する必要があるとします。その場合は、StoreFront に適切な NetScaler Gateway 構成を追加します。
- 同じ StoreFront サーバー: StoreFront の既存のインストールと構成を使用します。

短所:

- 同じストア: Virtual Apps and Desktops のワークロードをサポートするように StoreFront を再構成すると、XenMobile にも悪影響が及ぶ可能性があります。
- 同じ StoreFront サーバー: 大規模な環境では、XenMobile がアプリの列挙と起動で PNAgent を使用することにより、追加の負荷がかかる点を考慮する必要があります。

XenMobile サーバーとの統合に新しい専用の **StoreFront** インスタンスを使用する

長所:

- 新しいストア: XenMobile で使用する StoreFront ストアの構成を変更しても、Virtual Apps and Desktops の既存のワークロードには影響しません。
- 新しい StoreFront サーバー: サーバー構成の変更は、Virtual Apps and Desktops のワークフローに影響しません。さらに、XenMobile がアプリの列挙と起動で PNAgent を使用する以外の負荷は、スケーラビリティに影響しません。

短所:

- 新しいストア: StoreFront ストアの構成。

- 新しい StoreFront サーバー: StoreFront の新規のインストールと構成が必要です。

詳しくは、XenMobile のドキュメントの「Citrix Secure Hub を介した Virtual Apps and Desktops」を参照してください。

ShareFile

ShareFile を使用すると、ユーザーは任意のデバイスからすべてのデータにアクセスして同期することができます。ShareFile を使用すると、ユーザーは組織内外のユーザーとデータを安全に共有できます。ShareFile を XenMobile Advanced Edition または Enterprise Edition と統合すると、XenMobile によって ShareFile に以下が提供されます:

- XenMobile Apps ユーザーのシングルサインオン認証。
- Active Directory ベースのユーザーアカウントのプロビジョニング。
- 包括的なアクセス制御ポリシー。

モバイルユーザーに完全な ShareFile Enterprise 機能セットのメリットをもたらすことができます。

または、StorageZone コネクタとのみ統合するように XenMobile を構成することもできます。StorageZone コネクタを介して、ShareFile は以下へのアクセスを提供します:

- ドキュメントとフォルダー
- ネットワークファイル共有
- SharePoint サイトの場合: サイトコレクションとドキュメントライブラリ。

接続したファイル共有には、Citrix Virtual Apps and Desktops 環境で使用されるのと同じネットワークのホームドライブを含めることができます。XenMobile コンソールを使用して、ShareFile Enterprise または StorageZone コネクタとの統合を構成します。詳しくは、「ShareFile を XenMobile と使用する」を参照してください。

次のセクションでは、ShareFile の設計を決定するときに確認すべき質問項目について説明します。

ShareFile Enterprise または **StorageZone** コネクタのみとの統合

確認すべき質問項目:

- Citrix 管理の StorageZone にデータを保存する必要がありますか。
- ユーザーにファイルの共有および同期の機能を提供しますか。
- ShareFile Web サイト上のファイルにユーザーがアクセスできるようにしますか。またはモバイルデバイスから Office 365 のコンテンツおよび個人向けクラウドコネクタにアクセスできるようにしますか。

設計の決定:

- 上記の質問のいずれかの回答が「はい」の場合は、ShareFile Enterprise と統合します。
- StorageZone コネクタのみと統合すると、iOS ユーザーは、SharePoint サイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。この構成では、

ShareFile サブドメインの設定や ShareFile に対するユーザーのプロビジョニング、ShareFile データのホストが不要になります。XenMobile で StorageZone コネクタを使用すると、社内ネットワーク外へのユーザー情報漏洩に対するセキュリティ規制に準拠します。

ShareFile StorageZone コントローラーサーバーの場所

確認すべき質問項目:

- オンプレミスのストレージや機能（StorageZone コネクタなど）が必要ですか。
- ShareFile のオンプレミス機能を使用する場合、ShareFile StorageZone コントローラーはネットワーク内のどこに配置されますか。

設計の決定:

- ShareFile クラウド、オンプレミスの単一テナントストレージシステム、またはサポートされているサードパーティのクラウドストレージに、StorageZone コントローラーサーバーを配置するかどうかを決定します。
- StorageZone コントローラーは、Citrix ShareFile コントロールプレーンと通信するためにインターネットアクセスが必要です。直接アクセス、NAT および PAT の設定、プロキシ設定など、いくつかの方法で接続できます。

StorageZone コネクタ

確認すべき質問項目:

- CIFS 共有パスは何ですか。
- SharePoint の URL は何ですか。

設計の決定:

- オンプレミスの StorageZone コントローラーがこれらの場所にアクセスする必要があるかどうかを判断します。
- StorageZone コネクタは、ファイルリポジトリ、CIFS 共有、SharePoint などの内部リソースと通信するため、StorageZone コントローラーは、DMZ ファイアウォールの内側にあり、NetScaler が前に置かれた内部ネットワークに配置することをお勧めします。

SAML と **XenMobile Enterprise** の統合

確認すべき質問項目:

- ShareFile に Active Directory 認証が必要ですか。
- XenMobile で ShareFile アプリを初めて使用するときに SSO が必要ですか。
- 現在の環境に標準の IdP はありますか。
- いくつのドメインで SAML を使用する必要がありますか。

- Active Directory ユーザーに複数のメールエイリアスがありますか。
- Active Directory ドメインの移行が進行中、または近日中に予定されていますか。

設計の決定：

XenMobile Enterprise 環境では、ShareFile の認証メカニズムとして SAML の使用を選択できます。認証オプションは次のとおりです：

- SAML の ID プロバイダー（IdP）として XenMobile Server を使用します。

このオプションは、優れたユーザーエクスペリエンスを提供し、ShareFile アカウントの作成を自動化するだけでなく、モバイルアプリの SSO 機能を有効にすることができます。

- XenMobile Server はこのプロセスのために強化されています：そのため、Active Directory の同期は不要です。
- ユーザープロビジョニングに ShareFile User Management Tool を使用します。
- サポートされているサードパーティベンダーを SAML の IdP として使用します。

既存のサポートされている IdP があり、モバイルアプリの SSO 機能が不要な場合は、このオプションが最適です。また、このオプションでは、アカウントのプロビジョニングに ShareFile User Management Tool を使用する必要があります。

サードパーティの IdP ソリューション（ADFS など）を使用すると、Windows クライアント側にも SSO 機能が提供される場合があります。ShareFile の SAML IdP を選択する前に、ユースケースを評価するようにします。

さらに、両方のユースケースを満たすために、ADFS と XenMobile をデュアル IDP として構成できます。

モバイルアプリ

確認すべき質問項目：

- どの ShareFile モバイルアプリ（パブリック、MDM、MDX）を使用する予定ですか。

設計の決定：

- 業務用モバイルアプリは Apple App Store や Google Play ストアから配信できます。パブリックアプリストアからの配信では、Citrix ダウンロードページからラップされたアプリを入手します。
- セキュリティレベルが低くコンテナ化が不要の場合、パブリックの ShareFile アプリケーションは適切でない可能性があります。MDM-only 環境では、XenMobile を MDM モードで使用して、ShareFile アプリの MDM バージョンを配信できます。
- 詳しくは、「アプリ」および「Citrix ShareFile for XenMobile」を参照してください。

セキュリティ、ポリシー、およびアクセス制御

確認すべき質問項目：

- デスクトップ、Web、およびモバイルユーザーにはどのような制限が必要ですか。

- ユーザーに対する標準的なアクセス制御をどのような設定にしますか。
- どのようなファイル保持ポリシーを使用する予定ですか。

設計の決定:

- ShareFile を使用すると、従業員の権限とデバイスのセキュリティを管理できます。詳しくは、「従業員の権限」および「デバイスとアプリの管理」を参照してください。
- 一部の ShareFile のデバイスセキュリティ設定と MDX ポリシーは、同じ機能を制御します。そのような場合は XenMobile のポリシーが優先され、次に ShareFile のデバイスセキュリティ設定が適用されます。例: 外部アプリを ShareFile で無効にし、XenMobile では有効にすると、ShareFile ではこの外部アプリが無効になります。XenMobile では PIN とパスコードが不要、ShareFile アプリでは PIN とパスコードが必要なようにアプリを構成できます。

標準 **StorageZone** と制限付き **StorageZone**

確認すべき質問項目:

- 制限付き StorageZone が必要ですか。

設計の決定:

- 標準 StorageZone は機密性の低いデータを対象としており、従業員は非従業員とデータを共有できます。このオプションは、ドメイン外でデータを共有するワークフローをサポートします。
- 制限付き StorageZone では機密データが保護され、認証されたドメインユーザーのみが、ゾーンに格納されたデータにアクセスできます。

Web プロキシ

XenMobile トラフィックを HTTP(S)/SOCKS プロキシ経由でルーティングする、最もありがちなシナリオは、次のとおりです: XenMobile サーバーが存在するサブネットに、必要な Apple、Google、または Microsoft IP アドレスへの送信方向のインターネットアクセスがない場合。XenMobile でプロキシサーバーの設定を指定すると、すべてのインターネットトラフィックをプロキシサーバーにルーティングできます。詳しくは、「プロキシサーバーの有効化」を参照してください。

次の表に、XenMobile で使用される最も一般的なプロキシの長所と短所を示します。

オプション	長所	短所

XenMobile サーバーで HTTP(S)/SOCKS プロキシを使用します。	ポリシーにより、XenMobile サーバーのサブネットからの送信インターネット接続が許可されない場合：インターネット接続を提供するように HTTP(S) または SOCKS プロキシを構成できます。	プロキシサーバーに障害が発生すると、APNs（iOS）または Firebase Cloud Messaging（Android）の接続が切断されます。その結果、すべての iOS 端末と Android 端末でデバイスの通知が失敗します。
Secure Web で HTTP（S）プロキシを使用してください。	HTTP/HTTPS トラフィックを監視して、インターネット活動が組織の標準に準拠していることを確認できます。	この構成では、すべての Secure Web Internet トラフィックを企業ネットワークにトンネリングしてからインターネットに送り返す必要があります。インターネット接続でブラウズが制限されている場合：この設定はインターネットブラウジングのパフォーマンスに影響する可能性があります。

分割トンネリングの NetScaler セッションプロファイル設定は、次のようにトラフィックに影響します。

NetScaler 分割トンネリングが［**Off**］ の場合：

- MDX ネットワークアクセスポリシーが ［内部ネットワークへトンネル］の場合： すべてのトラフィックは、Microsoft VPN またはクライアントレス VPN（cVPN）トンネルを使用して NetScaler Gateway に強制的に戻されます。
- プロキシサーバーの NetScaler トラフィックポリシー/プロファイルを設定し、それらを NetScaler Gateway VIP にバインドします。

> 重要：
>
> 必ず Secure Hub cVPN トラフィックをプロキシから除外してください。

- 詳しくは、「XenMobile Secure Hub Traffic Through Proxy Server in Secure BrowseMode」を参照してください。

NetScaler 分割トンネリングが ［**On**］ の場合：

- アプリが MDX ネットワークアクセスポリシーで ［内部ネットワークへトンネル］ に設定されている場合：アプリケーションは、まず Web リソースを直接取得しようとします。Web リソースが公開されていない場合、それらのアプリケーションは NetScaler Gateway にフォールバックします。
- プロキシサーバーの NetScaler トラフィックポリシーとプロファイルを設定します。次に、これらのポリシーとプロファイルを NetScaler Gateway VIP にバインドします。

> 重要：
>
> 必ず Secure Hub cVPN トラフィックをプロキシから除外してください。

［分割 **DNS**］ の NetScaler セッションプロファイル設定（［クライアントエクスペリエンス］配下）は、分割トンネリングと同様に機能します。

［分割 **DNS**］ が ［両方］ に設定されている場合：

- クライアントはまず FQDN をローカルで解決し、障害発生時には NetScaler にフォールバックして DNS を解決しようとします。

［分割 **DNS** ］ が ［リモート］ に設定されている場合：

- DNS 解決は NetScaler でのみ発生します。

［分割 **DNS**］ が ［ローカル］ に設定されている場合：

- クライアントは FQDN をローカルに解決しようとします。DNS 解決に NetScaler は使用されません。

アクセス制御

企業は、ネットワーク内外のモバイルデバイスを管理できるようになりました。XenMobile などのエンタープライズモビリティ管理ソリューションは、場所に関係なくモバイルデバイスのセキュリティと制御を提供することに優れていますが、ネットワークアクセス制御（NAC）ソリューションと組み合わせると、ネットワーク内のデバイスに対して QoS とより詳細な制御を加えることができます。この組み合わせにより、NAC ソリューションを通じて XenMobile のデバイスセキュリティ評価を強化できます。NAC ソリューションは XenMobile のセキュリティ評価を使用して、認証の決定を効率的に処理することができます。Citrix では、XenMobile と Cisco Identity Services Engine（ISE）または ForeScout の NAC 統合を確認しています。他の NAC ソリューションとの統合は保証されていません。

XenMobile との NAC ソリューション統合の利点は次のとおりです：

- 社内ネットワーク上のすべてのエンドポイントのセキュリティ、コンプライアンス、制御の強化。
- NAC ソリューションでは、次のことが可能です：
  - ネットワークに接続しようとするデバイスを瞬時に検出します。
  - XenMobile にデバイス属性を照会します。
  - 次にこの情報を使用して、デバイスを許可、禁止、制限、またはリダイレクトするかどうかを決定します。これらの決定は、適用されるセキュリティポリシーによって異なります。
- NAC ソリューションでは、IT 管理者に非管理デバイスと非準拠デバイスのビューを提供します。

XenMobile でサポートされている NAC 準拠フィルターについては、「ネットワークアクセス制御」を参照してください。

複数サイトの要件

August 22, 2019

複数サイトの高可用性と障害回復を含めた XenMobile 展開環境を構築し、構成できます。この記事では、XenMobile の展開で使用される高可用性および障害回復モデルの概要を説明します。

高可用性

- XenMobile クラスタノードの場合、NetScaler は負荷分散を処理します。詳しくは、「クラスタリングの構成」を参照してください。
- XenMobile サーバーノードは、アクティブ/アクティブ構成で動作します。
- 容量が必要な場合は、追加の XenMobile サーバーノードが高可用性クラスタに追加されます。1 つのノードで最大約 8,500 のユーザーデバイスを処理できます（詳細については「スケーラビリティとパフォーマンス」を参照）。
- Citrix では、「n + 1」台の XenMobile サーバーを構成することを推奨しています：つまり、8,500 個のユーザーデバイスごとに 1 台のサーバーと、冗長性のために 1 台のサーバーを追加します。
- 可能であれば、すべての NetScaler インスタンスに高可用性を設定して、設定を 2 番目の NetScaler と同期させることをお勧めします。
- 標準の NetScaler 高可用性ペアは、アクティブ/パッシブ構成で動作します。

一般的な高可用性 XenMobile 環境には次のものが含まれます：

- 2 つの NetScaler インスタンス（VPX または MPX）。NetScaler SDX プラットフォームを使用する場合は、高可用性も考慮する必要があります。
- 同じデータベース設定で構成された 2 台以上の XenMobile サーバー。

障害回復

1 つのアクティブデータセンターと 1 つのパッシブデータセンターを持つ 2 つのデータセンターにまたがって XenMobile を障害回復用に構成できます。NetScaler と GSLB（Global Server Load Balancing）を使用してアクティブ/アクティブデータパスを作成し、ユーザーエクスペリエンスがアクティブ/アクティブセットアップのエクスペリエンスになるようにします。

障害回復の場合、XenMobile 環境には次のものが含まれます：

- 2 つのデータセンター。それぞれに 1 つ以上の NetScaler インスタンス、XenMobile サーバー、および SQL Server データベースが含まれています。
- データセンターにトラフィックを誘導する GSLB サーバー。GSLB サーバーは、サイトへの XenMobile 登録 URL と NetScaler Gateway URL の両方のトラフィックを処理するように設定されています。

- NetScaler for XenMobile ウィザードを使用して NetScaler Gateway を設定した場合、デフォルトでは GSRB は、MAM 負荷分散サーバーへの途上で XenMobile 登録サーバーへのトラフィックと NetScaler Gateway へのトラフィックを解決できるようになっていません。その結果、追加のステップが必要になります。これらの手順の準備と実装の詳細については、「障害回復」を参照してください。
- Always On 可用性グループのクラスタ化 SQL サーバー
- XenMobile サーバーと SQL Server の間の遅延は、5 ミリ秒未満でなければなりません。

> 注：
>
> このハンドブックで説明されている障害回復方法は、アクセスレイヤーの自動障害回復のみを提供します。デバイスが XenMobile サーバーに接続するには、フェールオーバーサイトですべての XenMobile サーバーノードと SQL Server データベースを手動で起動する必要があります。

NetScaler Gateway および NetScaler の統合

September 24, 2019

XenMobile と統合すると、NetScaler Gateway を経由して MAM（Mobile Application Management：モバイルアプリケーション管理）デバイス用の内部ネットワークにアクセスできる認証メカニズムを、リモートデバイスで利用できるようになります。この統合を利用すると、業務用モバイルアプリはモバイルデバイス上のアプリで作成した NetScaler Gateway へのマイクロ VPN を介して、イントラネット内にある社内サーバーにアクセスすることができます。

XenMobile サーバーが複数ある場合、または XenMobile サーバーが DMZ または内部ネットワーク内にある場合（つまり、デバイスから NetScaler へのトラフィックが XenMobile に流れる場合）は、NetScaler の負荷分散が必要です。

XenMobile Server モードの統合要件

NetScaler Gateway と NetScaler の統合要件は、XenMobile Server モード（MAM、MDM（Mobile Device Management：モバイルデバイス管理）、ENT）に応じて異なります。

MAM

XenMobile Server を MAM モードで使用する場合：

- **NetScaler Gateway** は必須です。NetScaler Gateway は、すべての企業リソースにアクセスするためのマイクロ VPN パスを提供し、強力な多要素認証をサポートします。
- 負荷分散には **NetScaler** をお勧めします。

XenMobile を高可用性構成で展開することをお勧めしています。高可用性構成では、XenMobile の前にロードバランサーが必要です。詳しくは、「MAM と従来の MAM モードについて」を参照してください。

MDM

XenMobile Server を MDM モードで使用する場合：

- NetScaler Gateway は不要です。MDM の展開では、モバイルデバイス VPN として NetScaler Gateway をお勧めします。
- セキュリティと負荷分散のために NetScaler をお勧めします。

  セキュリティと負荷分散のために、XenMobile サーバーの前に NetScaler アプライアンスを配置することをお勧めします。DMZ 内に XenMobile サーバーを標準展開する場合は、NetScaler for XenMobile ウィザードを使用し、SSL ブリッジモードでの XenMobile サーバーの負荷分散をお勧めします。また、XenMobile サーバーが DMZ ではなく内部ネットワーク上にある環境や、セキュリティ上そのような構成が必要な環境の場合は、SSL オフロードを検討することもできます。

  XenMobile サーバーを NAT や既存のサードパーティ製プロキシ、または MDM 用のロードバランサー経由で公開することを検討する場合、SSL トラフィックが XenMobile サーバー（SSL Bridge）上で終端すると潜在的なセキュリティリスクがあるため、お勧めしません。

  高度なセキュリティ環境を実現するには、NetScaler とデフォルトの XenMobile 構成の組み合わせがセキュリティ要件を満たしているか、それ以上の条件を備えている必要があります。

  最高水準のセキュリティが求められる MDM 環境を実現するには、SSL の終端を NetScaler にすることで、エンドツーエンドの SSL 暗号化を維持しながら境界でトラフィックを検査できます。詳しくは、「セキュリティ要件」を参照してください。NetScaler ではオプションとして SSL/TLS 暗号と SSL FIPS NetScaler ハードウェアを定義できます。

ENT（MAM + MDM）

XenMobile Server を ENT モードで使用する場合：

- NetScaler Gateway は必須です。NetScaler Gateway は、すべての企業リソースにアクセスするためのマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

  XenMobile サーバーモードが ENT の場合にユーザーが MDM 登録をオプトアウトすると、デバイスは従来の MAM モードで動作します。従来の MAM モードでは、デバイスの登録に NetScaler Gateway の完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を使用します。詳しくは、「MAM と従来の MAM モードについて」を参照してください。
- 負荷分散には NetScaler をお勧めします。詳細については、上記「MDM」の NetScaler の箇所を参照してください。

> 重要：
>
> 初回の登録では、負荷分散用仮想サーバーを SSL オフロードまたは SSL ブリッジのいずれで構成する場合でも、ユーザーデバイスからのトラフィックは XenMobile サーバー上で認証されることに注意してください。

設計の決定

以下のセクションでは、NetScaler Gateway と XenMobile との統合を計画するときに検討すべき、多くの設計上の決定についてまとめています。

ライセンスとエディション

決定する事項の詳細：

- NetScaler のどのエディションを使用するか
- NetScaler にプラットフォームライセンスを適用しているか
- MAM の機能が必要な場合は、NetScaler ユニバーサルアクセスライセンスを適用しているか

設計ガイド：

NetScaler Gateway に適切なライセンスを適用するようにしてください。Citrix Gateway コネクタ：Exchange ActiveSync 用を使用している場合、統合キャッシュが必要な場合があります。そのため、適切な NetScaler のエディションを使用していることを確認する必要があります。

NetScaler の機能を有効にするためのライセンス要件は次のとおりです。

- XenMobile MDM の負荷分散では、NetScaler の標準プラットフォームライセンスが最低限必要となります。
- StorageZones Controller を使用した ShareFile の負荷分散には、NetScaler の標準プラットフォームライセンスが最低限必要となります。
- XenMobile Enterprise Edition には、MAM に必要な NetScaler Gateway Universal ライセンスが含まれています。
- Exchange の負荷分散には、NetScaler Platinum プラットフォームライセンスまたは NetScaler Enterprise プラットフォームライセンスに、Integrated Caching ライセンスを追加する必要があります。

XenMobile 用の **NetScaler** のバージョン

決定する事項の詳細：

- XenMobile 環境で実行されている NetScaler のバージョンは何か
- 別のインスタンスが必要か

設計ガイド：

NetScaler Gateway 仮想サーバーに専用の NetScaler インスタンスを使用することをお勧めします。最低限必要となる NetScaler のバージョンおよびビルドを、XenMobile 環境で使用していることを確認してください。通

常、XenMobile と互換性のある最新の NetScaler バージョンおよびビルドを使用するのが最適です。NetScaler Gateway のアップグレードが既存の環境に影響する場合は、XenMobile の 2 つ目の専用インスタンスが適切な場合があります。

VPN 接続を使用する XenMobile およびその他のアプリ用に NetScaler インスタンスを共有する場合は、両方で使用する VPN ライセンスの数が足りていることを確認してください。XenMobile のテスト環境および実稼働環境では、NetScaler インスタンスを共有できないことに留意してください。

証明書

決定する事項の詳細:

- 登録や XenMobile 環境へのアクセスに高度なセキュリティが必要か
- LDAP は選択しないか

設計ガイド:

XenMobile のデフォルト構成は、ユーザー名とパスワードによる認証です。登録および XenMobile 環境へのアクセスのセキュリティを強化するには、証明書ベースの認証の使用を考慮してください。LDAP で 2 要素認証の証明書を使用すると、RSA サーバーを必要とせずに高度なセキュリティを提供できます。

LDAP やスマートカードの使用または同様の方法を許可しない場合、証明書を構成すると XenMobile にスマートカードを提示できます。ユーザーはそれにより、XenMobile が生成する一意の PIN を使用して登録できます。ユーザーがアクセス権を獲得すると、XenMobile は、それ以降 XenMobile 環境に認証するために使用される証明書を作成して展開します。

XenMobile は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートします。Microsoft CA が構成されている場合、XenMobile は NetScaler を使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、Citrix Gateway 証明書失効一覧（CRL）設定（［**Enable CRL Auto Refresh**］）を構成する必要があるかどうか検討します。この手順を使用すると、MAM-only モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証することができなくなります。ユーザー証明書が失効してもユーザーによる生成が制限されるわけではないので、XenMobile は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

ネットワークトポロジ

決定する事項の詳細:

- どのような NetScaler トポロジが必要か

設計ガイド:

XenMobile には NetScaler インスタンスを使用することをお勧めします。ただし、内部ネットワークから DMZ にトラフィックが流れないようにするには、NetScaler インスタンスを 1 つ追加して、内部ユーザー用と外部ユーザー用に 1 つずつ NetScaler インスタンスを使用することを検討してください。ユーザーが内部ネットワークと外部ネ

ットワークを切り替えると、DNS レコードのキャッシュによって Secure Hub のログオンプロンプトの回数が増える場合があることに注意してください。

XenMobile は、NetScaler Gateway のダブルホップをサポートしていません。

専用または共有の **NetScaler Gateway VIP** アドレス

決定する事項の詳細:

- 現在、Virtual Apps and Desktops 用の NetScaler Gateway を使用しているか
- Virtual Apps and Desktops と同じ NetScaler Gateway を XenMobile で利用するか
- 両方のトラフィックフローの認証要件は何か

設計ガイド:

Citrix 環境に XenMobile と、Virtual Apps and Desktops が含まれている場合は、両方で同じ NetScaler インスタンスと NetScaler Gateway 仮想サーバーを使用できます。バージョンによる競合が起きたり環境が孤立したりする可能性があるため、NetScaler インスタンスと NetScaler Gateway は、それぞれの XenMobile 環境専用にすることをお勧めします。ただし、専用の NetScaler インスタンスを選択しない場合は、XenMobile と Virtual Apps and Desktops との間で共有される vServer ではなく、専用の NetScaler Gateway vServer を使用して、Secure Hub のトラフィックフローを分離することをお勧めします。

LDAP 認証を使用する場合、Citrix Receiver と Secure Hub は問題なく同じ NetScaler Gateway と認証できます。証明書ベースの認証を使用する場合、XenMobile は MDX コンテナ内の証明書をプッシュし、Secure Hub はその証明書を使用して NetScaler Gateway で認証します。Citrix Receiver は Secure Hub とは異なり、Secure Hub と同じ証明書を使用して同じ NetScaler Gateway と認証することはできません。

2 台の NetScaler Gateway VIP で同じ FQDN を使用できる、以下の回避策を検討することもできます。同じ IP アドレスを持つ 2 つの NetScaler Gateway VIP を作成できますが、Secure Hub 用の IP には標準の 443 ポートを使用し、(Citrix Receiver を展開する) Virtual Apps and Desktops 用の IP にはポート 444 を使用します。こうすることで、1 つの FQDN が同じ IP アドレスに解決されます。この方法ではデフォルトのポート 443 ではなく、ポート 444 に ICA ファイルを返すよう StoreFront を構成する必要がある場合があります。この回避策では、ユーザーはポート番号を入力する必要はありません。

NetScaler Gateway のタイムアウト

決定する事項の詳細:

- XenMobile のトラフィックに対する NetScaler Gateway のタイムアウトをどのように構成するか

設計ガイド:

NetScaler Gateway には、セッションタイムアウトと強制タイムアウトの設定があります。詳しくは、「推奨構成」を参照してください。バックグラウンドサービス、NetScaler、およびオフラインでのアプリケーションへのアクセスでは、タイムアウト値が異なることに留意してください。

MAM 用の **XenMobile** ロードバランサー **IP** アドレス

決定する事項の詳細:

- VIP アドレスに内部 IP アドレスまたは外部 IP アドレスを使用しているか

設計ガイド:

NetScaler Gateway の VIP アドレスにパブリック IP アドレスを使用できる環境では、その方法で XenMobile の負荷分散 VIP アドレスを割り当てると、登録のエラーにつながります。

そのシナリオでは負荷分散 VIP アドレスに内部 IP を使用し、登録のエラーが起こらないようにしてください。この VIP アドレスは、RFC 1918 標準のプライベート IP アドレスに準拠する必要があります。この仮想サーバーに非プライベート IP アドレスを使用すると、NetScaler は認証プロセスで XenMobile サーバーに正常に接続できなくなります。詳しくは、「https://support.citrix.com/article/CTX200430」を参照してください。

MDM の負荷分散の仕組み

決定する事項の詳細:

- NetScaler Gateway でどのように XenMobile サーバーの負荷分散を行うか

設計ガイド:

XenMobile が DMZ 内にある場合は、SSL ブリッジを使用します。XenMobile サーバーが内部ネットワークにあり、セキュリティの標準を満たす必要がある場合には、SSL オフロードを使用します。

- NetScalerVIP アドレスを設定した XenMobile サーバーを SSL ブリッジモードで負荷分散すると、インターネットのトラフィックは接続が終端する XenMobile サーバーに直接流れます。SSL ブリッジモードはセットアップとトラブルシューティングが最も簡単なモードです。
- NetScalerVIP アドレスを設定した XenMobile サーバーを SSL オフロードモードで負荷分散すると、インターネットのトラフィックは接続が終端する NetScaler に直接流れます。その場合 NetScaler は、XenMobile サーバーに対して新しいセッションを確立します。SSL オフロードモードでのセットアップとトラブルシューティングはさらに複雑です。

SSL オフロードを使用する **MDM** 負荷分散用のサービスポート

決定する事項の詳細:

- 負荷分散に SSL オフロードモードを使用する場合、バックエンドサービスはどのポートを使用するか

設計ガイド:

SSL オフロードでは、次のようにポート 80 またはポート 8443 を選択します。

- オフロードの効果を得るには、XenMobile サーバーへのポートとしてポート 80 を利用します。

- エンドツーエンドの暗号化、つまりトラフィックの再暗号化はサポートされていません。詳細については、Citrix のサポート記事「NetScaler と XenMobile Server 間でサポートされているアーキテクチャ」を参照してください。

登録 **FQDN**

決定する事項の詳細:

- 登録用の FQDN と XenMobile インスタンスまたは負荷分散 VIP アドレス用の FQDN はどのようになるか

設計ガイド:

クラスター内の最初の XenMobile サーバーの初期設定では、XenMobile サーバーの FQDN を入力する必要があります。その FQDN は、MDM の VIP アドレス URL と内部 MAM の負荷分散 VIP アドレス URL と一致する必要があります。(NetScaler の内部アドレスレコードにより、MAM 負荷分散 VIP アドレスが解決されます)。詳細については、この記事の後半の「展開タイプごとの登録 FQDN」を参照してください。

また、XenMobile SSL リスナー証明書、MAM 用の内部負荷分散 VIP アドレス証明書、および MDM 用の VIP アドレス証明書(MDM 用の VIP アドレスに SSL オフロードを使用する場合)と同じ証明書を使用する必要があります。

> 重要:
>
> 登録 FQDN を構成すると、変更はできません。新しい登録 FQDN を使用するには、新しい SQL Server データベースと XenMobile サーバーの再構築が必要です。

Secure Web のトラフィック

決定する事項の詳細:

- Secure Web を内部の Web ブラウジングのみに制限するか
- 内部と外部両方の Web ブラウジングで Secure Web を有効にするか

設計ガイド:

Secure Web を内部の Web ブラウジング専用で使用する場合で、Secure Web がデフォルトですべての内部サイトに到達できる場合には、NetScaler Gateway の設定は簡単です。つまりファイアウォールとプロキシサーバーの構成が必要になる場合があります。

内部および外部のブラウジングに Secure Web を使用する場合は、サブネット IP アドレスに送信方向のインターネットアクセスを許可する必要があります。一般的に、IT は登録済みデバイス(MDX コンテナを使用)を社内ネットワークの延長として見ているため、Secure Web 接続は NetScaler に戻り、プロキシサーバーを経由してインターネットに接続する必要があります。デフォルトでは、Secure Web アクセスは内部ネットワークにトンネルされます。つまり、Secure Web ではすべてのネットワークアクセスにおいて、アプリケーションごとの VPN トンネルを使用して内部ネットワークに戻ってくるということであり、NetScaler では分割トンネリング設定を使用します。

Secure Web 接続の詳細については、「ユーザー接続の構成」を参照してください。

Secure Mail のプッシュ通知

決定する事項の詳細:

- プッシュ通知を使用するか

iOS 向け設計ガイド:

NetScaler Gateway 構成に Secure Ticket Authority（STA）が含まれていて、分割トンネリングがオフの場合、NetScaler Gateway は Secure Mail から、iOS 向け Secure Mail にプッシュ通知で指定されている Citrix リスナーサービス URL へのトラフィックを許可する必要があります。

Android 向け設計ガイド:

アクティブなポーリング周期 MDX ポリシーの代わりに Firebase Cloud Messaging（FCM）を使用して、Android デバイスが XenMobile に接続するタイミングと方法を制御することもできます。FCM 構成では、セキュリティアクションや展開コマンドによって、ユーザーに XenMobile サーバーへの再接続を求めるプッシュ通知が Secure Hub に送信されます。

HDX の STA

決定する事項の詳細:

- HDX アプリケーションのアクセスを統合する場合にどんな STA を使用するか

設計ガイド:

HDX の STA は StoreFront の STA と一致する必要があり、Virtual Apps and Desktops ファームで有効である必要があります。

ShareFile

決定する事項の詳細:

- 利用環境で ShareFile StorageZone Controller を使用するか
- どの ShareFile VIP アドレス URL を使用するか

設計ガイド:

利用環境に ShareFile StorageZone Controller を含める場合、ShareFile Content Switch VIP アドレス（ShareFile コントロールプレーンが StorageZones Controller サーバーとの通信に使用）、ShareFile 負荷分散 VIP アドレス、および必要なすべてのポリシーとプロファイルが正しく構成されていることを確認してください。詳細については、Citrix ShareFile StorageZones Controller ドキュメントを参照してください。

SAML ID プロバイダー

決定する事項の詳細:

- ShareFile に SAML が必要な場合、XenMobile を SAML ID プロバイダーとして使用するか

設計ガイド:

ベストプラクティスとして、ShareFile を Citrix XenMobile Advanced Edition または XenMobile Enterprise Edition と統合することをお勧めします。この方法は、SAML ベースのフェデレーションを構成するより簡単です。ShareFile を XenMobile の上記エディションと組み合わせることで、業務用モバイルアプリユーザーのシングルサインオン認証、Active Directory に基づくユーザーアカウントのプロビジョニング、および包括的なアクセス制御ポリシーを ShareFile で使用できるようになります。XenMobile コンソールを使用して ShareFile を構成したり、サービスレベルやライセンスの使用状況を監視したりできます。

ShareFile for XenMobile クライアント（別名、ラップされた ShareFile）と ShareFile モバイル（別名、ラップされていない ShareFile）の 2 種類の ShareFile クライアントがあります。違いを理解するには、「[ShareFile for XenMobile クライアントと ShareFile モバイルクライアントの相違点]」（/ja-jp/mobile-productivity-apps/sharefile.html#how-citrix-files-for-endpoint-management-clients-differ-from-citrix-files-mobile-clients）を参照してください。

XenMobile と ShareFile を構成し、SAML を使用することで、MDX Toolkit でラップされた ShareFile Mobile アプリはもちろん、Web サイト、Outlook プラグイン、同期クライアントなどのラップされていない ShareFile クライアントへのシングルサインオンアクセスを提供することができます。

XenMobile を ShareFile 用の SAML ID プロバイダーとして使用する場合は、設定が適切であることを確認してください。詳しくは、「ShareFile での SAML による SSO」を参照してください。

ShareConnect での直接接続

決定する事項の詳細:

- ユーザーが直接接続を利用して、ShareConnect が動作するコンピューターまたはモバイルデバイスからホストコンピューターにアクセスするか

設計ガイド:

ShareConnect を使用すると、ユーザーは iPad、Android タブレット、Android スマートフォンから自分のコンピューターに安全に接続して、ファイルやアプリケーションにアクセスできます。直接接続の場合、XenMobile は NetScaler Gateway を使ってローカルネットワークの外にあるリソースへの安全なアクセスを提供します。構成の詳細については、「ShareConnect」を参照してください。

展開の種類ごとの登録 **FQDN**

展開の種類	登録 **FQDN**
エンタープライズ（MDM ＋ MAM）と必須の MDM 登録	XenMobile Server の FQDN
エンタープライズ（MDM ＋ MAM）とオプションの MDM 登録	XenMobile サーバーの FQDN または NetScaler Gateway の FQDN
MDM のみ	XenMobile サーバーの FQDN
MAM のみ（レガシー）	NetScaler Gateway の FQDN
MAM のみ	XenMobile サーバーの FQDN

環境のまとめ

NetScaler for XenMobile ウィザードを使用して適切な設定を行うことをお勧めしています。ウィザードを使用できるのは 1 度限りです。テスト環境、開発環境、および実稼働環境などの複数の XenMobile インスタンスがある場合は、追加の環境用に手動で NetScaler を構成する必要があります。作業環境がある場合は、XenMobile 用に手動で NetScaler を構成する前に、設定を書き留めておいてください。

ウィザードの使用時に決定する事項の中で重要となるのは、XenMobile サーバーとの通信に HTTPS を使用するか、あるいは HTTP を使用するかという点です。HTTPS の場合は NetScaler と XenMobile との間のトラフィックが暗号化されるため、安全なバックエンド通信が可能ですが、再暗号化は XenMobile サーバーのパフォーマンスに影響します。HTTP の場合は XenMobile サーバーのパフォーマンスは向上しますが、NetScaler と XenMobile との間のトラフィックは暗号化されません。以下の表に、NetScaler および XenMobile サーバーの HTTP および HTTPS ポートの要件を示します。

HTTPS

Citrix では通常、NetScaler MDM 仮想サーバー構成用の SSL ブリッジをお勧めしています。MDM 仮想サーバーで NetScaler SSL オフロードを使用する場合、XenMobile はバックエンドサービスとしてポート 80 のみをサポートします。

展開の種類	**NetScaler** の負荷分散手法	**SSL** 再暗号化	**XenMobile** サーバーポート
MDM	SSL ブリッジ	-	443、8443
MAM	SSL オフロード	有効	8443
Enterprise	MDM：SSL ブリッジ	-	443、8443

Enterprise	MAM：SSL オフロード	有効	8443

HTTP

展開の種類	**NetScaler** の負荷分散手法	**SSL** 再暗号化	**XenMobile** サーバーポート
MDM	SSL オフロード	未サポート	80
MAM	SSL オフロード	有効	8443
Enterprise	MDM：SSL オフロード	未サポート	80
Enterprise	MAM：SSL オフロード	有効	8443

XenMobile 環境での NetScaler Gateway の図については、「オンプレミス環境のリファレンスアーキテクチャ」を参照してください。

MDX アプリの SSO とプロキシの考慮事項

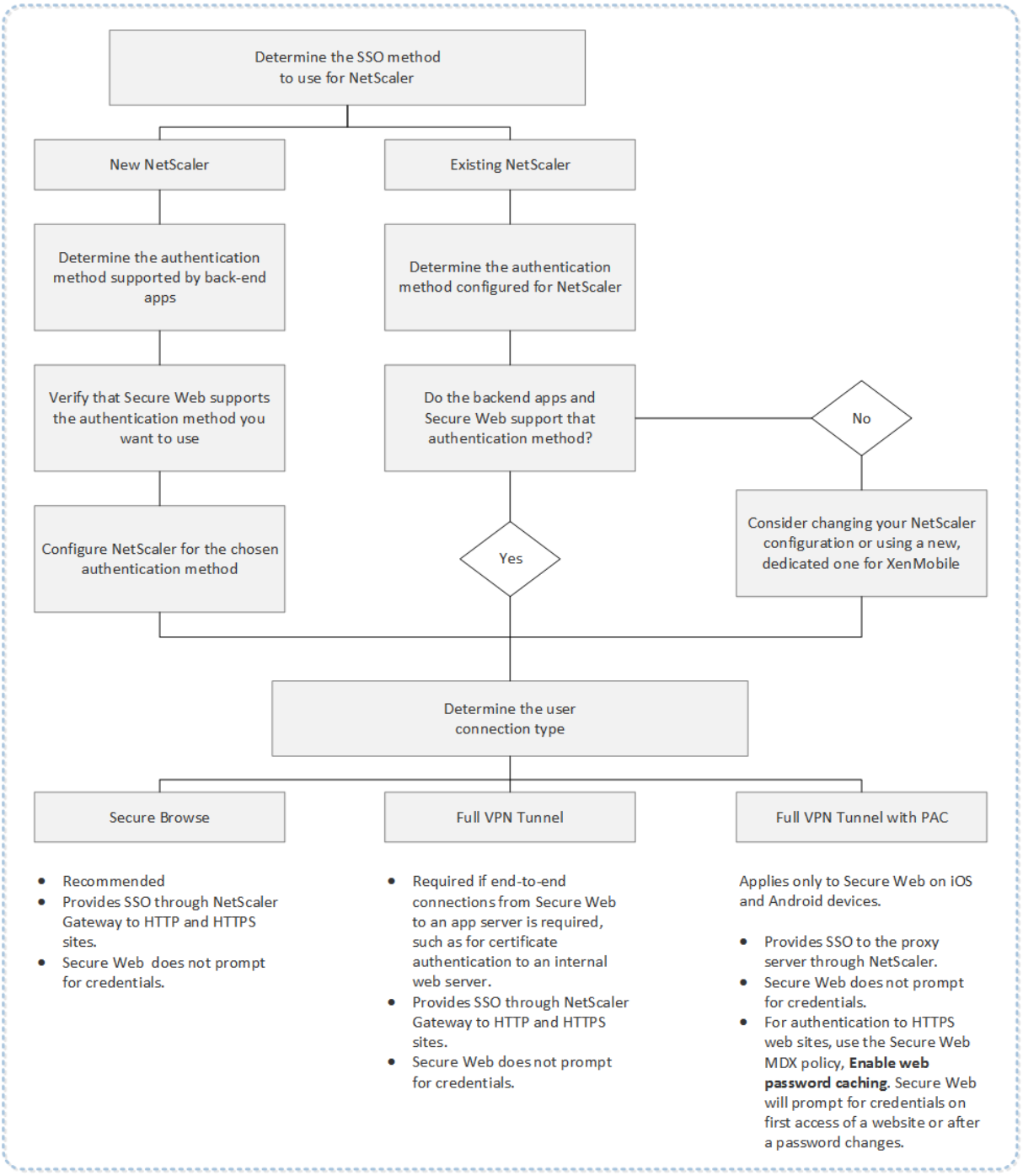
August 22, 2019

XenMobile と NetScaler の統合により、ユーザーにバックエンドのすべての HTTP/HTTPS リソースへのシングルサインオン（SSO）を提供することができます。SSO 認証の要件に応じて、MDX アプリへのユーザー接続を、次のいずれかのオプションを使用するように構成できます。

- クライアントレス VPN の一種であるセキュアブラウズ
- 完全 VPN トンネル

お客様の環境において SSO を提供する最善の方法が NetScaler でない場合は、ポリシーベースのローカルパスワードキャッシュを使用して MDX アプリをセットアップできます。この記事では、Secure Web に焦点を当てて、さまざまな SSO とプロキシのオプションについて説明します。この概念は他の MDX アプリにも適用されます。

次のフローチャートは、SSO とユーザー接続の決定フローをまとめたものです。



NetScaler 認証方法

ここでは、NetScaler でサポートされる認証方法について一般的な情報を説明します。

SAML 認証

SAML（Security Assertion Markup Language）を使用するように NetScaler を構成すると、ユーザーはシングルサインオンの SAML プロトコルをサポートする Web アプリに接続できます。NetScaler Gateway では、SAML Web アプリに対して ID プロバイダー（IdP）を使用したシングルサインオンがサポートされます。

必要な構成：

- NetScaler のトラフィックプロファイルで SAML SSO を構成します。
- 要求されたサービスの SAML Idp を構成します。

NTLM 認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler は NTLM 認証を自動的に実行します。

必要な構成：

- NetScaler のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

Kerberos 偽装

XenMobile では、Secure Web についてのみ Kerberos をサポートします。Kerberos SSO を使用するように NetScaler を構成すると、NetScaler ではユーザーパスワードを使用できる場合に偽装が使用されます。偽装とは、NetScaler がユーザーの資格情報を使用して、Secure Web などのサービスにアクセスするために必要なチケットを取得することです。

必要な構成：

- NetScaler の「Worx」セッションポリシーを構成して、接続から Kerberos レルムを識別できるようにします。
- NetScaler で Kerberos 制約付き委任（KCD）アカウントを構成します。このアカウントをパスワードなしで構成し、XenMobile ゲートウェイのトラフィックポリシーにバインドします。
- 上記およびその他の構成の詳細については、Citrix ブログ：WorxWeb and Kerberos Impersonation SSOを参照してください。

Kerberos 制約付き委任

XenMobile では、Secure Web についてのみ Kerberos をサポートします。Kerberos SSO を使用するように NetScaler を構成すると、NetScaler ではユーザーパスワードを使用できない場合に制約付き委任が使用されます。

制約付き委任では、NetScaler は指定された管理者アカウントを使用して、ユーザーとサービスに代わってチケットを取得します。

必要な構成：

- 必要な権限と NetScaler の KCD アカウントを使用して、Active Directory に KCD アカウントを構成します。
- NetScaler のトラフィックプロファイルで SSO を有効にします。
- Kerberos 認証用のバックエンド Web サイトを構成します。
- 上記およびその他の構成の詳細については、Citrix ブログ「Configuring Kerberos Single Sign-on for WorxWeb」を参照してください。

フォーム入力認証

フォームベースのシングルサインオンを使用するように NetScaler を構成すると、ユーザーは一度ログオンするだけで、ネットワーク内の保護されたすべてのアプリにアクセスできます。この認証方法は、セキュアブラウズモードまたは完全 VPN モードを使用するアプリに適用されます。

必要な構成:

- NetScaler のトラフィックプロファイルでフォームベースの SSO を構成します。

ダイジェスト **HTTP** 認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler はダイジェスト HTTP 認証を自動的に実行します。この認証方法は、セキュアブラウズモードまたは完全 VPN モードを使用するアプリに適用されます。

必要な構成:

- NetScaler のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

HTTP 基本認証

セッションプロファイルで Web アプリへの SSO が有効になっている場合、NetScaler は HTTP 基本認証を自動的に実行します。この認証方法は、セキュアブラウズモードまたは完全 VPN モードを使用するアプリに適用されます。

必要な構成:

- NetScaler のセッションプロファイルまたはトラフィックプロファイルで SSO を有効にします。

セキュアブラウズ、完全 **VPN** トンネル、または **PAC** がある完全 **VPN** トンネル

以下のセクションでは、Secure Web のユーザー接続の種類について説明します。詳しくは、Citrix ドキュメント「Secure Web」の記事の「ユーザー接続の構成」を参照してください。

完全 **VPN** トンネル

内部ネットワークへトンネルする接続では完全 VPN トンネルを使用できます。完全 VPN トンネルを構成するには、Secure Web の［優先 VPN モード］ポリシーを使用します。内部ネットワークのリソースにクライアント証明書またはエンドツーエンドの SSL を使用する接続に対しては、［完全 VPN トンネル］を推奨します。完全 VPN トンネルは、TCP 上のあらゆるプロトコルを処理します。Windows、Mac、iOS、および Android デバイスで完全 VPN トンネルを使用できます。

完全 VPN トンネルモードにすると、NetScaler では HTTPS セッション内の状態が表示されなくなります。

セキュアブラウズ

内部ネットワークをトンネルする接続は、さまざまなクライアントレス VPN を使用できます。これはセキュアブラウズと呼ばれています。セキュアブラウズは、Secure Web の［優先 **VPN** モード］ポリシーに指定されるデフォルトの構成です。シングルサインオン（SSO）を必要とする接続に対しては、セキュアブラウズが推薦されます。

セキュアブラウズモードの場合、NetScaler は HTTPS セッションを次の 2 つの部分に分割します：

- クライアントから NetScaler まで
- NetScaler からバックエンドリソースサーバーまで。

このようにして、クライアントとサーバー間のすべてのトランザクションを把握することにより、NetScaler で SSO が提供できるようになります。

また、セキュアブラウズモードで使用される場合に Secure Web に対してプロキシサーバーを構成できます。詳しくは、ブログ「XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode」を参照してください。

PAC がある完全 **VPN** トンネル

iOS および Android デバイスの Secure Web に対して、Proxy Automatic Configuration（PAC）ファイルを完全 VPN トンネル展開で使用できます。XenMobile は NetScaler が指定するプロキシ認証をサポートします。PAC ファイルには、指定の URL にアクセスするために Web ブラウザーがどのようにプロキシを選択するかを定義する規則が含まれます。PAC ファイル規則は、内部および外部の両サイトの処理を指定できます。Secure Web は PAC ファイル規則を解析し、プロキシサーバー情報を NetScaler Gateway に送信します。NetScaler Gateway は PAC ファイルまたはプロキシサーバーを認識しません。

HTTPS Web サイトへの認証の場合：Secure Web の MDX ポリシーである［**Web** パスワードのキャッシュを有効化］により、MDX を介するプロキシサーバーへの SSO を Secure Web が認証して提供するようにできます。

NetScaler 分割トンネリング

SSO とプロキシの構成を計画するときは、NetScaler 分割トンネリングを使用するかどうかも決める必要があります。NetScaler 分割トンネリングは、必要な場合にのみ使用することをお勧めします。ここでは、分割トンネリングのしくみの概要を説明します: NetScaler では、ルーティングテーブルに基づいてトラフィックパスが決定されます。NetScaler 分割トンネリングがオンの場合、Secure Hub は内部（保護された）ネットワークのトラフィックとインターネットのトラフィックを区別します。Secure Hub は、DNS サフィックスとイントラネットアプリケーションに基づいてこの決定を行います。次に Secure Hub は、VPN トンネルを使用して内部ネットワークのトラフィックのみをトンネル処理します。NetScaler 分割トンネリングがオフの場合、すべてのトラフィックが VPN トンネルを経由します。

- セキュリティ上の理由からすべてのトラフィックを監視する必要がある場合は、NetScaler 分割トンネリングをオフにします。これにより、すべてのトラフィックが VPN トンネルを経由します。
- PAC がある完全 VPN トンネルを使用する場合は、NetScaler Gateway の分割トンネリングを無効にする必要があります。分割トンネリングが有効で PAC ファイルが構成されていると、PAC ファイル規則により NetScaler 分割トンネリング規則は無効になります。トラフィックポリシーで構成されたプロキシサーバーは、NetScaler 分割トンネリング規則を上書きしません。

Secure Web では、［ネットワークアクセス］ ポリシーはデフォルトで ［内部ネットワークへトンネル］ に設定されています。この構成では、MDX アプリは NetScaler 分割トンネル設定を使用します。［ネットワークアクセス］ポリシーのデフォルト設定は、業務用モバイルアプリによって異なる場合があります。

また NetScaler Gateway には、マイクロ VPN を使用したリバース分割トンネルモードもあります。この構成では、NetScaler にトンネル処理されない、除外対象の IP アドレス一覧がサポートされます。これらのアドレスは、代わりにデバイスのインターネット接続を使用して送信されます。リバース分割トンネリングについて詳しくは、NetScaler Gateway のドキュメントを参照してください。

XenMobile には、リバース分割トンネルの除外対象一覧が含まれています。特定の Web サイトを NetScaler Gateway 経由でトンネリングしない場合: 代わりにローカルエリアネットワーク（LAN）を使用して接続する完全修飾ドメイン名（FQDN）または DNS サフィックスのコンマ区切りの一覧を追加します。この一覧は、NetScaler Gateway がリバース分割トンネリング用に構成された、セキュアブラウズモードにのみ適用されます。

認証

January 10, 2020

XenMobile 環境で認証の構成方法を決定する場合、いくつかの点を考慮する必要があります。このセクションでは、認証に影響するさまざまな要素を理解できるよう、以下の項目について説明します:

- 認証に関係する主な MDX ポリシー、XenMobile クライアントプロパティ、NetScaler Gateway の設定。
- これらのポリシー、クライアントプロパティ、および設定の関連性。
- それぞれの選択肢の代償。

また、セキュリティを強化する上で推奨される 3 つの構成例も紹介します。

大まかに言えば、セキュリティを強化するほどユーザーはより頻繁に認証を行わなければならなくなるため、最適なユーザーエクスペリエンスから遠ざかることになります。こうした問題のバランスをとる方法は、組織のニーズと優先事項によって異なります。3 つの推奨構成を検討することで、利用可能な認証手段の関係と、お客様に合った XenMobile 環境の最適な展開方法についてより深く理解できます。

認証モード

オンライン認証： ユーザーは XenMobile ネットワークに接続できます。インターネット接続が必要になります。

オフライン認証： デバイスで認証を行います。ユーザーは、セキュリティで保護された資格情報コンテナのロックを解除して、ダウンロード済みのメール、キャッシュされた Web サイト、メモなどにオフラインでアクセスできます。

認証方法

単一要素

LDAP： XenMobile では、LDAP（Lightweight Directory Access Protocol）に準拠している 1 つ以上のディレクトリ（Active Directory など）への接続を構成することができます。この方法は、企業環境でシングルサインオン（SSO：Single Sign-On）を実現するためによく使用されています。Active Directory のパスワードのキャッシュ化で Citrix PIN を選択すると、LDAP によりユーザーエクスペリエンスを向上させながら、登録時に複雑なパスワードを要求し、パスワードの有効期限およびアカウントのロックアウトを設定してセキュリティを確保できます。

詳しくは、「ドメインまたはドメイン +STA」を参照してください。

クライアント証明書： XenMobile を業界標準の証明機関と統合し、証明書を唯一のオンライン認証方法として使用できます。XenMobile では、ワンタイムパスワード、招待 URL、LDAP 資格情報のいずれかが要求されるユーザー登録を行った後に、この証明書が提供されます。クライアント証明書をプライマリ認証方法とする場合、クライアント証明書のみの環境では、デバイスで証明書を保護するために Citrix PIN が必要になります。

XenMobile は、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートします。Microsoft CA が構成されている場合、XenMobile は NetScaler を使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、Citrix Gateway 証明書失効一覧（CRL）設定（[Enable CRL Auto Refresh]）を構成する必要があるかどうか検討します。この手順を使用すると、MAM-only モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証することができなくなります。ユーザー証明書が失効してもユーザーによる生成が制限されるわけではないので、XenMobile は新しい証明書を再発行します。この設定は、CRL が期限切れの PKI エンティティを確認する場合、PKI エンティティのセキュリティを強化します。

ユーザー向けに証明書ベースの認証を使用する場合、またはデバイスの証明書の発行でエンタープライズ証明機関（CA：Certificate Authority）を利用する必要がある場合に必要な展開環境を示した図については、「オンプレミス環境のリファレンスアーキテクチャ」を参照してください。

2 要素

LDAP ＋クライアント証明書: XenMobile 環境において、この構成では最適な SSO 機能と NetScaler の 2 要素認証で提供されるセキュリティが結びつけられており、セキュリティおよびユーザーエクスペリエンスについて最高の組み合わせとなります。LDAP とクライアント証明書の両方を使用することで、ユーザーの知識（Active Directory パスワード）と所有物（デバイス上のクライアント証明書）の両方によるセキュリティを実現します。Exchange クライアントアクセスサーバーの環境が適切に構成されていれば、Secure Mail（および他のいくつかの業務用モバイルアプリ）では、初回アクセス時にクライアント証明書認証を自動で構成し、シームレスなユーザーエクスペリエンスを提供できます。ユーザービリティを最適にするために、このオプションを Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。

LDAP ＋トークン: この構成では、RADIUS プロトコルを使用して、従来の LDAP 資格情報の構成とワンタイムパスワードを組み合わせることができます。ユーザービリティを最適にするために、このオプションを Citrix PIN や Active Directory のパスワードキャッシュと組み合わせることができます。

認証に関係する重要なポリシー、設定、およびクライアントプロパティ

後に示す 3 つの推奨構成では、次のポリシー、設定、およびクライアントプロパティを利用します。

MDX ポリシー

アプリのパスコード:［オン］ の場合、アプリを起動する時、または一定期間操作を行わなかった後で再開する時に、アプリのロック解除のために Citrix PIN またはパスコードが求められます。デフォルトは ［オン］ です。

すべてのアプリに対して無操作タイマーを構成するには、XenMobile コンソールの ［設定］ タブの ［クライアントプロパティ］ で、INACTIVITY_TIMER 値を分単位で設定します。デフォルトは 15 分です。無通信タイマーを無効にして、PIN またはパスコードを要求するプロンプトがアプリの起動時のみに表示されるようにするには、この値をゼロに設定します。

> 注:
>
> ［暗号キー］ポリシーでオフラインのセキュリティ保護を選択した場合、このポリシーは自動的に有効になります。

オンラインセッションを必須とする:［オン］ の場合、デバイス上のアプリにアクセスするために、エンタープライズネットワークおよびアクティブなセッションへ接続する必要があります。［オフ］ の場合、デバイス上のアプリにアクセスするために、アクティブなセッションに接続する必要はありません。デフォルトは ［オフ］ です。

最大オフライン期間（時間）: XenMobile からアプリ使用権の再確認とポリシーの更新を求められることなくアプリを実行できる最大期間を定義します。最大オフライン期間が設定されており、iOS 向け Secure Hub に有効な NetScaler Gateway トークンがある場合、アプリはユーザーの操作を中断することなく、XenMobile から MDX アプリの新しいポリシーを取得します。Secure Hub に有効な NetScaler トークンがない場合、アプリポリシーを更新するにはユーザーが Secure Hub で認証する必要があります。非アクティブな NetScaler 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、NetScaler 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。

期間が終了する 30 分前、15 分前、5 分前に、サインオンするようユーザーに警告メッセージが表示されます。期間終了後は、ユーザーがサインインするまでアプリはロックされます。デフォルトは **72** 時間（**3** 日）です。最短の期間は 1 時間です。

> 注：
>
> ユーザーの移動が頻繁であり国際ローミングを使用する可能性があるシナリオでは、デフォルトの 72 時間（3 日）では時間が足りない場合があることに注意してください。

バックグラウンドサービスチケットの有効期間： バックグラウンドネットワークサービスチケットの有効状態が維持される期間。NetScaler Gateway を介して Secure Mail が ActiveSync を実行する Exchange Server に接続する場合、XenMobile は内部 Exchange Server への接続に Secure Mail が使用するトークンを発行します。このプロパティ設定により、認証のために新しいトークンおよび Exchange Server への接続を要求することなく Secure Mail がトークンを使用できる期間が決まります。有効期限が切れた場合は、ユーザーは再度ログオンして新しいトークンを生成する必要があります。デフォルトは **168** 時間（**7** 日間） です。この有効期間が切れると、メール通知は行われなくなります。

オンラインセッションを必須とするまでの猶予期間： ［オンラインセッションを必須とする］ポリシーにより使用を停止されるまで（オンラインセッションが検証されるまで）に、オフラインでアプリを使用できる分数を指定します。デフォルトは 0（猶予期間なし）です。

MDX Toolkit 認証ポリシーの詳細について詳しくは、「iOS の XenMobile MDX ポリシー」および「Android の XenMobile MDX ポリシー」を参照してください。

XenMobile クライアントプロパティ

> 注：
>
> クライアントプロパティは、XenMobile に接続するすべてのデバイスに適用されるグローバル設定です。

Citrix PIN： サインインを簡略化する場合は、Citrix PIN を有効にします。PIN を使用する場合、ユーザーは他の資格情報（Active Directory のユーザー名やパスワードなど）を繰り返し入力する必要はありません。Citrix PIN は単独のスタンドアロンのオフライン認証として設定できるほか、Active Directory のパスワードキャッシュと組み合わせて認証を効率化し、ユーザビリティを最適化することもできます。Citrix PIN の構成は、XenMobile コンソールの ［設定］**>**［クライアント］**>**［クライアントプロパティ］ で行うことができます。

以下に、いくつかの重要なプロパティの概要を示します。詳しくは、「クライアントプロパティ」を参照してください。

ENABLE_PASSCODE_AUTH

表示名： Enable Citrix PIN Authentication

このキーを使用すると、Citrix PIN 機能を有効にできます。ユーザーは、Citrix PIN またはパスコードにより、Active Directory パスワードの代わりに使用する PIN を定義するように求められます。**ENABLE_PASSWORD_CACHING** を有効にしているか、XenMobile で証明書認証を使用している場合は、この設定を有効にする必要があります。

設定可能な値: **true** または **false**

デフォルト値: **false**

ENABLE_PASSWORD_CACHING

表示名: Enable User Password Caching

このキーを使用すると、ユーザーの Active Directory パスワードをモバイルデバイス上でローカルにキャッシュできます。このキーを true に設定すると、ユーザーは Citrix PIN またはパスコードを設定するように求められます。このキーを **true** に設定する場合は、ENABLE_PASSCODE_AUTH キーを true に設定する必要があります。

設定可能な値: **true** または **false**

デフォルト値: **false**

PASSCODE_STRENGTH

表示名: PIN Strength Requirement

このキーでは、Citrix PIN またはパスコードの強度を定義します。この設定を変更すると、ユーザーは次回認証を求められたときに、新しい Citrix PIN またはパスコードを設定するように求められます。

設定可能な値: **Low**、**Medium**、または **Strong**

デフォルト値: **Medium**

INACTIVITY_TIMER

表示名: Inactivity Timer

このキーでは、ユーザーがデバイスの操作を行わなくなってから、Citrix PIN またはパスコードの入力を求められずにアプリにアクセスできる時間（分単位）を定義します。MDX アプリでこの設定を有効にするには、［アプリのパスコード］設定を ［オン］ にする必要があります。［アプリのパスコード］設定を ［オフ］ に設定すると、ユーザーは完全認証を実行するよう Secure Hub にリダイレクトされます。この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。デフォルトは 15 分です。

ENABLE_TOUCH_ID_AUTH

表示名: Enable Touch ID Authentication

オフライン認証での指紋リーダー（iOS のみ搭載）の使用を許可します。オンライン認証では、この設定によらずプライマリ認証方法が求められます。

ENCRYPT_SECRETS_USING_PASSCODE

表示名: Encrypt secrets using Passcode

このキーでは、機密データをプラットフォームベースのネイティブな格納場所（iOS キーチェーンなど）ではなく、モバイルデバイスの Secret Vault に格納できます。この構成キーにより、重要な成果物を強力に暗号化できますが、ユーザーエントロピー（ユーザーだけが知る、ユーザーが生成したランダムな PIN コード）も追加されます。

設定可能な値: **true** または **false**

デフォルト値: **false**

NetScaler の設定

Session time-out: この設定を有効にすると、指定期間にわたって NetScaler でネットワークアクティビティが検出されない場合、NetScaler Gateway によりセッションが切断されます。この設定は、NetScaler Gateway Plug-in、Citrix Receiver、Secure Hub、または Web ブラウザーを使用して接続するユーザーに適用されます。デフォルトは **1440** 分です。値を 0 にすると、設定は無効になります。

Forced time-out: この設定を有効にした場合、タイムアウト時間が経過すると、ユーザーの操作内容にかかわらず NetScaler Gateway によりセッションが切断されます。タイムアウト時間が経過した場合、ユーザーが切断を中止することはできません。この設定は、NetScaler Gateway Plug-in、Citrix Receiver、Secure Hub、または Web ブラウザーを使用して接続するユーザーに適用されます。Secure Mail で STA（特別な NetScaler モード）を使用している場合、この設定は Secure Mail のセッションには適用されません。デフォルトは **1440** 分です。この値を空白にすると、設定は無効になります。

NetScaler Gateway のタイムアウト設定について詳しくは、NetScaler のドキュメントを参照してください。

ユーザーにデバイスで資格情報を入力して XenMobile の認証を行うように求めるシナリオについては、「認証を求められるシナリオ」を参照してください。

デフォルトの構成設定

NetScaler for XenMobile ウィザード、MDX Toolkit、および XenMobile コンソールのデフォルト設定を以下に示します。

設定	設定を見つける場所	デフォルト設定
セッションのタイムアウト	NetScaler Gateway	1,440 分
Forced time-out	NetScaler Gateway	1,440 分
最大オフライン期間	MDX ポリシー	72 時間
バックグラウンドサービスチケットの有効期間	MDX ポリシー	168 時間（7 日）
オンラインセッションを必須とする	MDX ポリシー	無効
オンラインセッションを必須とするまでの猶予期間	MDX ポリシー	0
アプリのパスコード	MDX ポリシー	有効
Encrypt secrets using passcode	XenMobile クライアントプロパティ	false
Enable Citrix PIN Authentication	XenMobile クライアントプロパティ	false

設定	設定を見つける場所	デフォルト設定
PIN Strength Requirement	XenMobile クライアントプロパティ	中
PIN の種類	XenMobile クライアントプロパティ	Numeric
Enable User Password Caching	XenMobile クライアントプロパティ	false
Inactivity Timer	XenMobile クライアントプロパティ	15
Enable Touch ID Authentication	XenMobile クライアントプロパティ	false

推奨構成

このセクションでは、セキュリティが最も弱く最適なユーザーエクスペリエンスが得られる構成から、セキュリティが最高レベルでユーザーに操作が求められる頻度が最も多い構成まで、3 種類の XenMobile の構成例を示します。お客様自身の構成配置のスケールを決定する際は、これらの例を参考にしてください。これらの設定を変更する場合、他の設定の変更も必要になる可能性があります。たとえば、最大オフライン期間は、セッションのタイムアウト期間よりも短くする必要があります。

最高のセキュリティ

この構成ではセキュリティのレベルは最高になりますが、ユーザビリティが大きく損なわれます。

設定	設定を見つける場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	1440	ユーザーは、オンライン認証が求められた時（24 時間ごと）にのみ、Secure Hub の資格情報を入力します。

Forced time-out	NetScaler Gateway	1440	24 時間ごとにオンライン認証を厳格に要求します。アクティビティによりセッションの有効期間が延長されることはありません。
最大オフライン期間	MDX ポリシー	23	毎日ポリシーを更新するように求めます。
バックグラウンドサービスチケットの有効期間	MDX ポリシー	72 時間	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Secure Mail では、STA のタイムアウト期限をセッションのタイムアウト期限よりも長くすると、ユーザーがセッションの期限切れまでにアプリを開かなかった場合に、ユーザーに確認を求めることなくメール通知が停止されてしまう事態を回避できます。
オンラインセッションを必須とする	MDX ポリシー	無効	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを必須にします。
オンラインセッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[オンラインセッションを必須とする］を有効にする場合）。
アプリのパスコード	MDX ポリシー	有効	アプリケーションのパスコードを求めます。

Encrypt secrets using passcode	XenMobile クライアントプロパティ	true	ユーザーエントロピーで設定されたキーにより資格情報コンテナを保護します。
Enable Citrix PIN Authentication	XenMobile クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。
PIN Strength Requirement	XenMobile クライアントプロパティ	強	パスワードの複雑さに関する高レベルの要件を適用します。
PIN の種類	XenMobile クライアントプロパティ	Alphanumeric	PIN は英数字の文字列になります。
Enable Password Caching	XenMobile クライアントプロパティ	false	Active Directory のパスワードはキャッシュされず、Citrix PIN を使用してオフライン認証を行います。
Inactivity Timer	XenMobile クライアントプロパティ	15	ユーザーがこの期間にわたり MDX アプリまたは Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	XenMobile クライアントプロパティ	false	iOS でのオフライン認証のユースケースで、Touch ID を無効にします。

より高いセキュリティ

この構成は中間的なアプローチであり、ユーザーに認証を求める頻度を増やし（7 日ごとではなく最長で 3 日ごと）、セキュリティを強化しています。認証回数を増やしたことでコンテナはより頻繁にロックされるようになり、デバイスが使用されていない時のデータのセキュリティを確保できます。

設定	設定を見つける場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	4320	ユーザーは、オンライン認証が求められた時（3日ごと）にのみ、Secure Hub の資格情報を入力します。
Forced time-out	NetScaler Gateway	値なし	アクティビティが行われれば、セッションは延長されます。
最大オフライン期間	MDX ポリシー	71	3 日ごとにポリシーを更新するように求めます。1時間短くしているのは、セッションタイムアウトより前に更新を行わせるようにするためです。
バックグラウンドサービスチケットの有効期間	MDX ポリシー	168 時間	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Secure Mail では、STA のタイムアウト期限をセッションのタイムアウト期限よりも長くすると、ユーザーがセッションの期限切れまでにアプリを開かなかった場合に、ユーザーに確認を求めることなくメール通知が停止されてしまう事態を回避できます。
オンラインセッションを必須とする	MDX ポリシー	無効	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを必須にします。

オンラインセッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[オンラインセッションを必須とする］を有効にする場合）。
アプリのパスコード	MDX ポリシー	有効	アプリケーションのパスコードを求めます。
Encrypt secrets using passcode	XenMobile クライアントプロパティ	false	ユーザーエントロピーを要求せずに、資格情報コンテナを暗号化します。
Enable Citrix PIN Authentication	XenMobile クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。
PIN Strength Requirement	XenMobile クライアントプロパティ	中	中レベルのパスワードの複雑さ規則を適用します。
PIN の種類	XenMobile クライアントプロパティ	Numeric	PIN は数列になります。
Enable Password Caching	XenMobile クライアントプロパティ	true	ユーザー PIN により、Active Directory のパスワードをキャッシュ化して保護します。
Inactivity Timer	XenMobile クライアントプロパティ	30	ユーザーがこの期間にわたり MDX アプリまたは Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	XenMobile クライアントプロパティ	true	iOS でのオフライン認証のユースケース向けに、Touch ID を有効にします。

高セキュリティ

この構成はユーザーが最も使いやすいものであり、セキュリティは基本レベルになります。

設定	設定を見つける場所	推奨設定	動作への影響
セッションのタイムアウト	NetScaler Gateway	10080	ユーザーは、オンライン認証が求められた時（7日ごと）にのみ、Secure Hub の資格情報を入力します。
Forced time-out	NetScaler Gateway	値なし	アクティビティが行われれば、セッションは延長されます。
最大オフライン期間	MDX ポリシー	167	毎週（7 日ごと）にポリシーを更新するように求めます。1 時間短くしているのは、セッションタイムアウトより前に更新を行わせるようにするためです。
バックグラウンドサービスチケットの有効期間	MDX ポリシー	240	NetScaler Gateway のセッショントークンなしでセッションを長時間継続できるようにする、STA のタイムアウト期限です。Secure Mail では、STA のタイムアウト期限をセッションのタイムアウト期限よりも長くすると、ユーザーがセッションの期限切れまでにアプリを開かなかった場合に、ユーザーに確認を求めることなくメール通知が停止されてしまう事態を回避できます。

オンラインセッションを必須とする	MDX ポリシー	無効	アプリを使用する場合に、有効なネットワーク接続と NetScaler Gateway セッションを必須にします。
オンラインセッションを必須とするまでの猶予期間	MDX ポリシー	0	猶予期間なし（[オンラインセッションを必須とする] を有効にする場合）。
アプリのパスコード	MDX ポリシー	有効	アプリケーションのパスコードを求めます。
Encrypt secrets using passcode	XenMobile クライアントプロパティ	false	ユーザーエントロピーを要求せずに、資格情報コンテナを暗号化します。
Enable Citrix PIN Authentication	XenMobile クライアントプロパティ	true	認証工程の簡略化のため、Citrix PIN を有効化します。
PIN Strength Requirement	XenMobile クライアントプロパティ	低	パスワードの複雑さに関する要件を適用しません。
PIN の種類	XenMobile クライアントプロパティ	Numeric	PIN は数列になります。
Enable Password Caching	XenMobile クライアントプロパティ	true	ユーザー PIN により、Active Directory のパスワードをキャッシュ化して保護します。
Inactivity Timer	XenMobile クライアントプロパティ	90	ユーザーがこの期間にわたり MDX アプリまたは Secure Hub を使用しない場合、オフライン認証を求めるメッセージが表示されます。
Enable Touch ID Authentication	XenMobile クライアントプロパティ	true	iOS でのオフライン認証のユースケース向けに、Touch ID を有効にします。

高レベルな認証を使用する

アプリによっては、高度な認証（トークンや短い間隔のセッションタイムアウトといった 2 番目の認証要素など）が必要になる場合があります。こうした認証方法は、MDX ポリシーで制御します。この方法では、認証方法を制御するために別個の（同一または別の NetScaler アプライアンス上の）仮想サーバーも必要になります。

設定	設定を見つける場所	推奨設定	動作への影響
代替 NetScaler Gateway	MDX ポリシー	セカンダリ NetScaler アプライアンスの FQDN とポートを必須にする。	セカンダリ NetScaler アプライアンスの認証ポリシーおよびセッションポリシーによって制御する、より強固な認証が可能になります。

代替 NetScaler Gateway インスタンスにログオンするアプリをユーザーが開くと、他のすべてのアプリは、内部ネットワークとの通信にその NetScaler Gateway インスタンスを使用するようになります。セキュリティが強化された NetScaler Gateway インスタンスのセッションがタイムアウトした場合、セキュリティの弱い NetScaler Gateway インスタンスに切り替わるだけです。

［オンラインセッションを必須とする］を使用する

Secure Web などの特定のアプリケーションでは、ユーザーが認証されたセッションを開いておりデバイスがネットワークに接続されている間のみ、ユーザーがアプリを実行できるようにしたほうが良い場合があります。このポリシーではこうした設定を適用し、ユーザーが作業を完了できるように猶予期間を設けます。

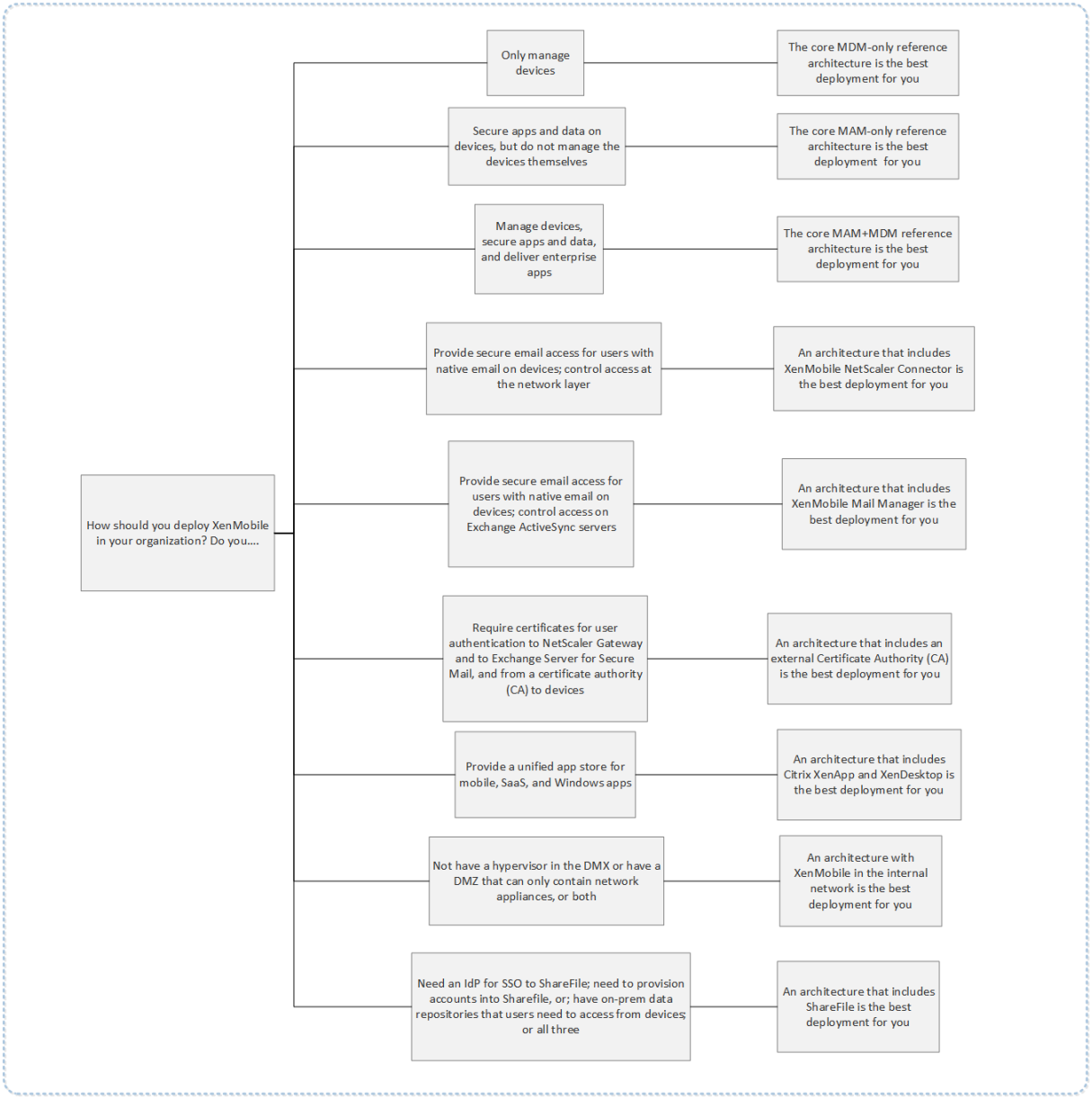
設定	設定を見つける場所	推奨設定	動作への影響
オンラインセッションを必須とする	MDX ポリシー	有効	デバイスがオンラインで、有効な認証トークンを持っていることを必須にします。
オンラインセッションを必須とするまでの猶予期間	MDX ポリシー	15	ユーザーがアプリを使用できなくなるまでに 15 分間の猶予期間を設けます。

オンプレミス環境のリファレンスアーキテクチャ

September 24, 2019

この記事の図は、オンプレミス XenMobile 展開のリファレンスアーキテクチャを示しています。展開シナリオには、コアアーキテクチャとして MDM-only、MAM-only、MDM+MAM のほか、SNMP マネージャー、Citrix Gateway コネクタ: Exchange ActiveSync 用、Endpoint Management コネクタ: Exchange ActiveSync 用、Virtual Apps and Desktops などのコンポーネントを含むシナリオが含まれます。図は、XenMobile に必要な最小限のコンポーネントを示しています。

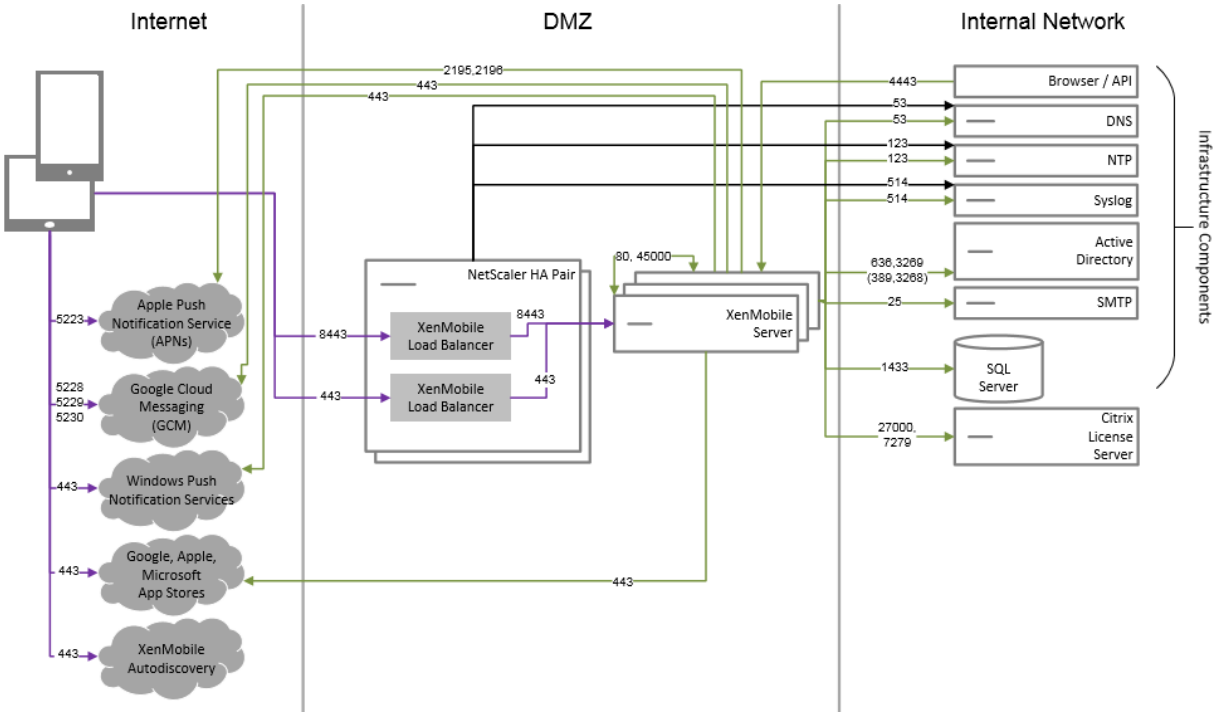
このチャートは、展開の決定に関する一般的なガイドとして使用してください。



この図のコネクタの番号は、コンポーネント間の接続を許可するために開く必要があるポートを表しています。ポートの完全なリストについては、XenMobile のドキュメントの「ポート要件」を参照してください。

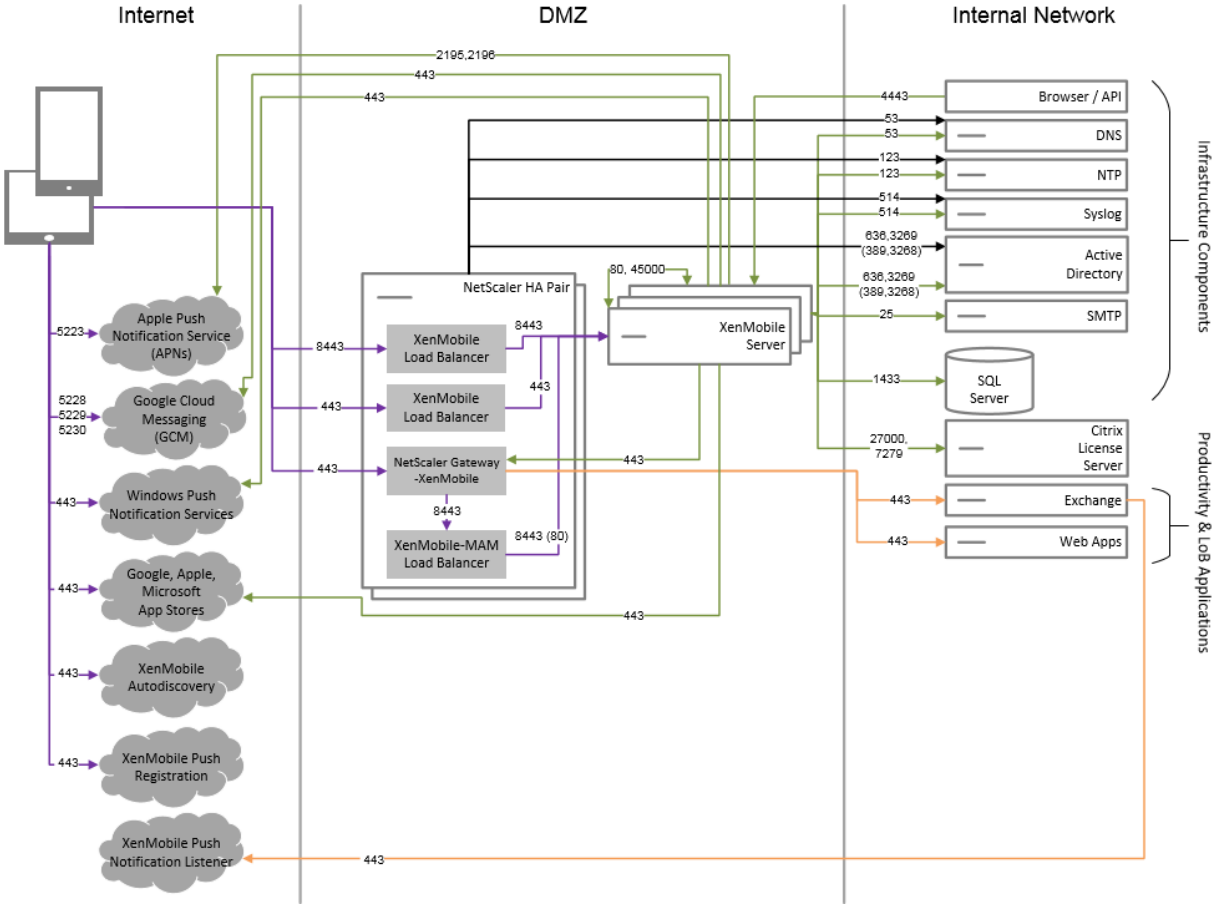
コア **MDM-Only** リファレンスアーキテクチャ

XenMobile の MDM 機能のみを使用する場合は、このアーキテクチャを展開してください。たとえば、コーポレート発行のデバイスを MDM で管理して、デバイスポリシーやアプリを展開し、アセットインベントリを取得して、デバイスワイプなどのアクションをデバイスで実行できるようにする必要がある場合などです。



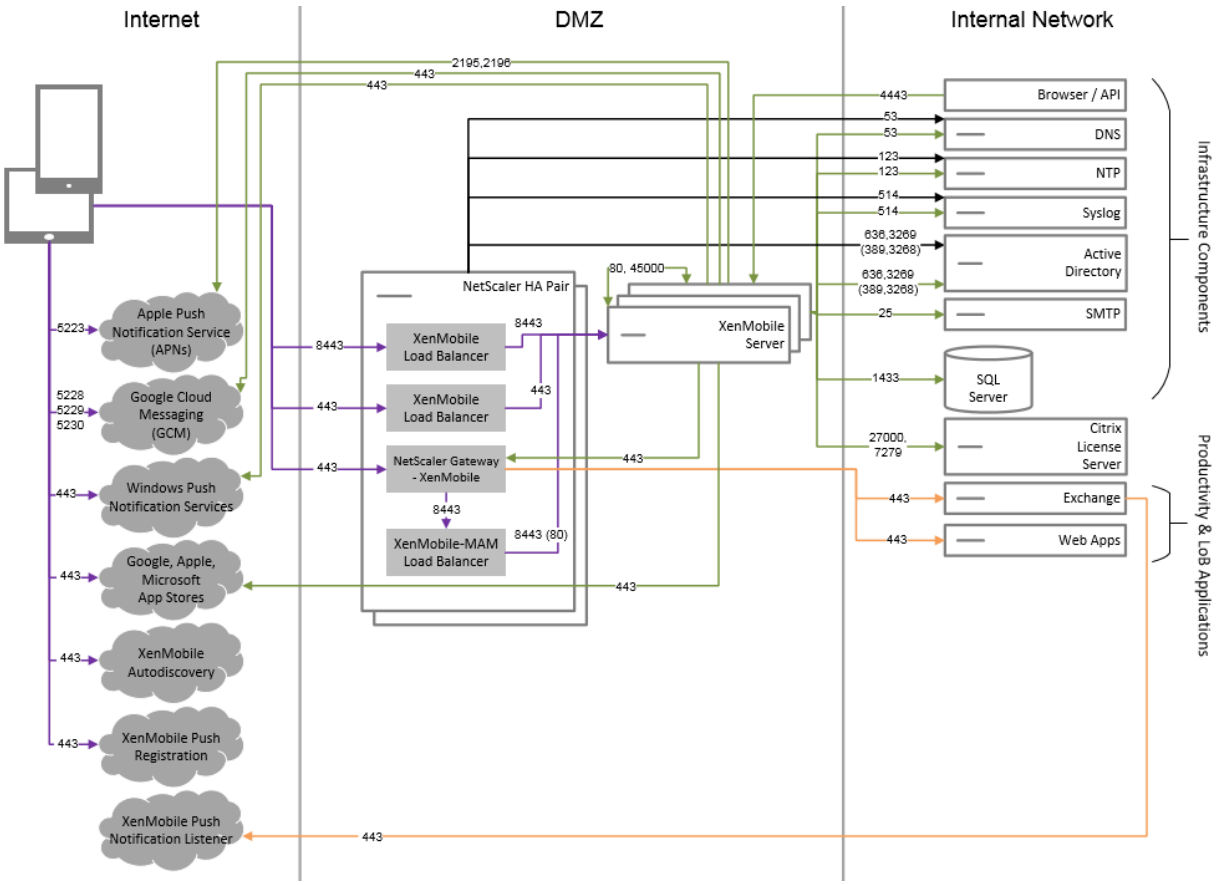
コア **MAM-Only** リファレンスアーキテクチャ

デバイスを MDM に登録せずに XenMobile の MAM 機能のみを使用する場合は、このアーキテクチャを展開してください。たとえば、BYO モバイルデバイスのアプリとデータをセキュリティ保護する必要がある場合や、エンタープライズモバイルアプリを配信して、アプリのロックおよびデータのワイプを実行できるようにする必要がある場合などです。デバイスを MDM に登録することはできません。



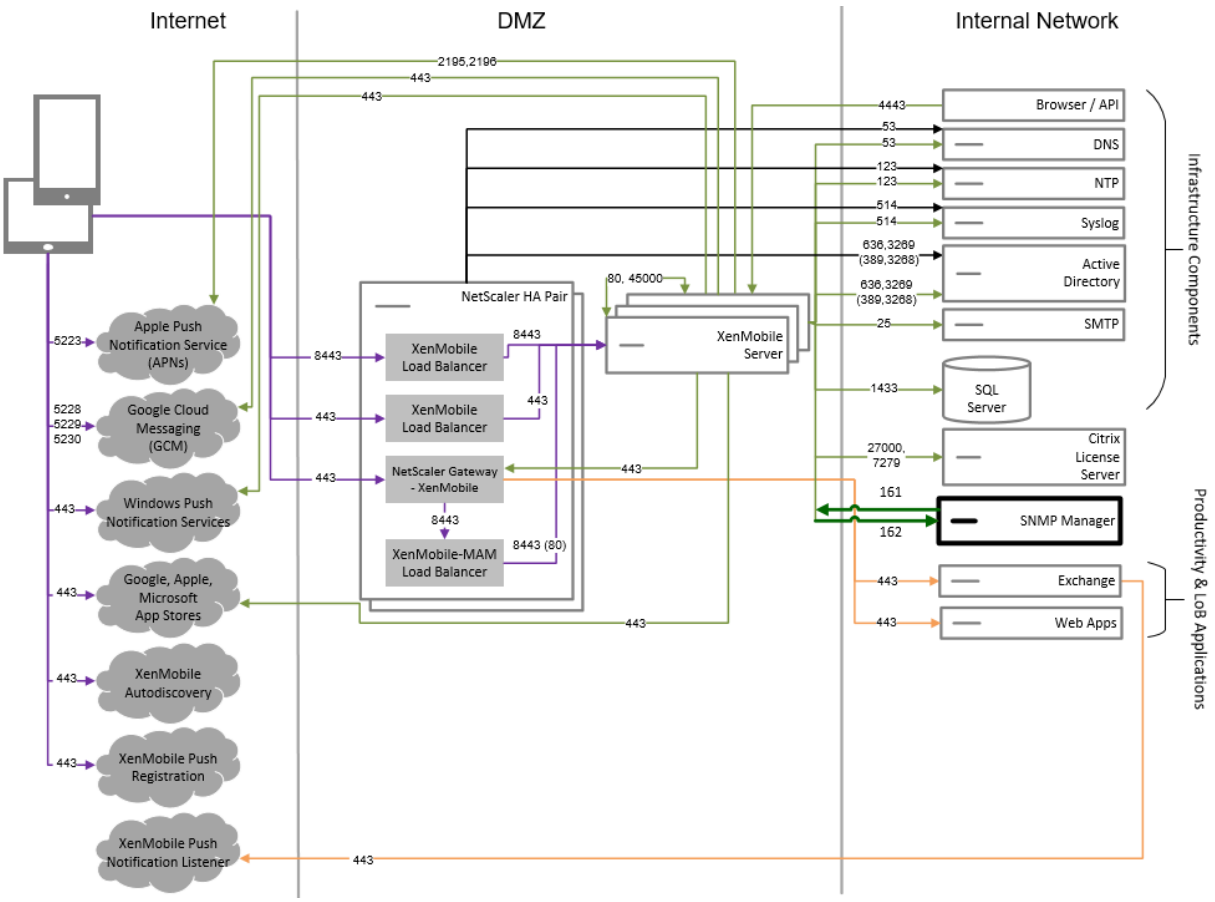
コア **MAM+MDM** リファレンスアーキテクチャ

XenMobile の MDM+MAM 機能を使用する場合は、このアーキテクチャを展開してください。たとえば、コーポレート発行のデバイスを MDM で管理する必要がある場合や、デバイスポリシーやアプリを展開し、アセットインベントリを取得して、デバイスをワイプできるようにする必要がある場合です。さらに、エンタープライズモバイルアプリを配信し、アプリのロックとデバイスのデータのワイプを実行できるようにする必要がある場合もあります。



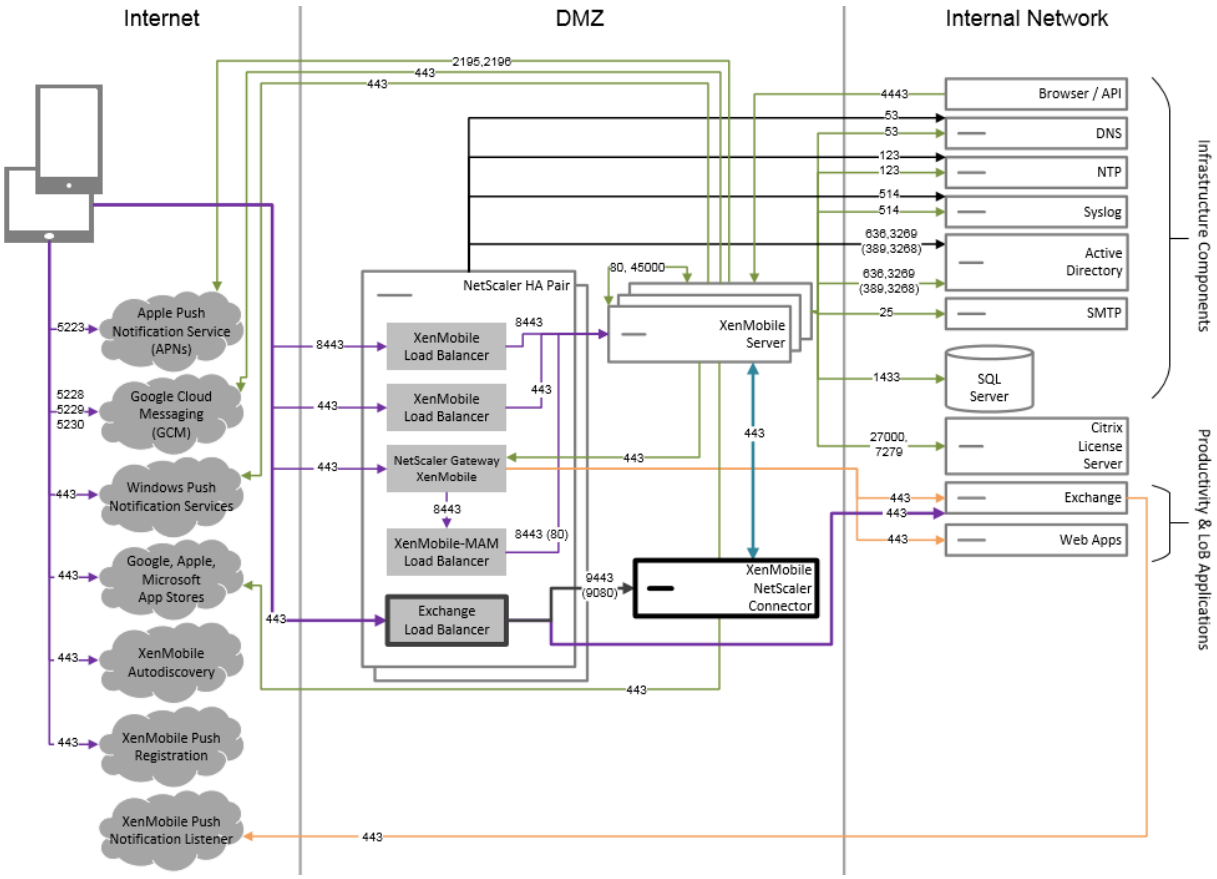
SNMP を使用するリファレンスアーキテクチャ

XenMobile で SNMP の監視を有効にする場合は、このアーキテクチャを展開します。たとえば、監視システムが XenMobile ノードの情報をクエリして情報を取得できるようにしたい場合です。詳しくは、「SNMP の監視」を参照してください。



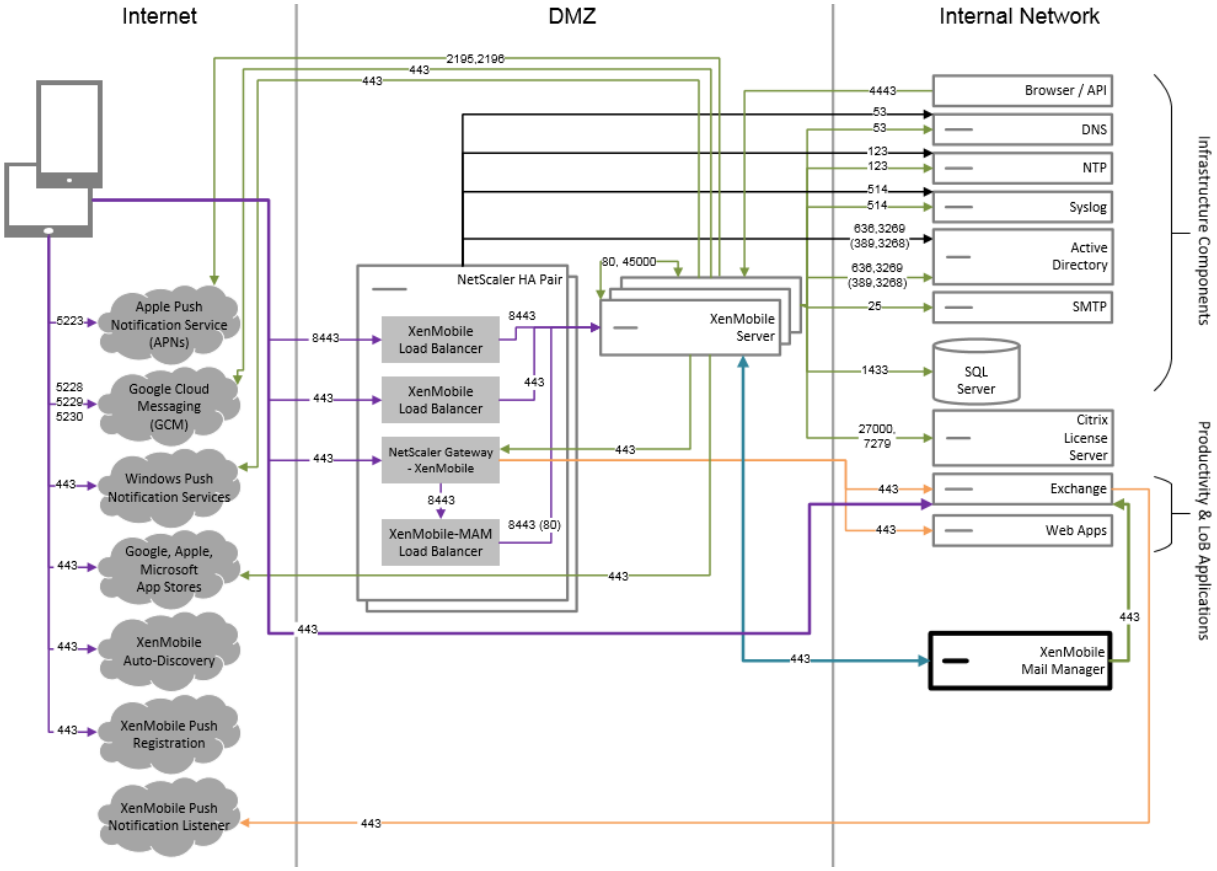
Citrix Gateway コネクタ: **Exchange ActiveSyn** 用を含む参照アーキテクチャ

XenMobile で Citrix Gateway コネクタ: Exchange ActiveSyn 用を使用する場合は、このアーキテクチャを展開します。たとえば、ネイティブモバイル電子メールアプリを使用するユーザーには安全な電子メールアクセスを提供する必要があります。これらのユーザーは、引き続きネイティブアプリを使用して電子メールにアクセスしますが、時間をかけて Citrix Secure Mail に移行させることも可能です。トラフィックが Exchange Active Sync サーバーに到達する前に、ネットワーク層でアクセス制御を行う必要があります。この図には、MDM および MAM アーキテクチャに展開された Exchange ActiveSync 用コネクタが示されていますが、同様に MDM-only アーキテクチャの一部として Exchange ActiveSync 用コネクタを展開することもできます。



Endpoint Management コネクタ：**Exchange ActiveSyn** 用を含む参照アーキテクチャ

XenMobile で Endpoint Management コネクタ：Exchange ActiveSyn 用を使用する場合は、このアーキテクチャを展開します。たとえば、ネイティブモバイル電子メールアプリを使用するユーザーには安全な電子メールアクセスを提供したい場合もあります。これらのユーザーは、引き続きネイティブアプリを使用して電子メールにアクセスしますが、時間をかけて Secure Mail に移行させることも可能です。Exchange ActiveSync サーバーのアクセス制御を実現できます。この図は、MDM および MAM アーキテクチャに展開された Endpoint Management コネクタ：Exchange ActiveSync 用を示していますが、MDM 専用アーキテクチャの一部と同じ方法で Endpoint Management コネクタ：Exchange ActiveSync 用を展開することもできます。

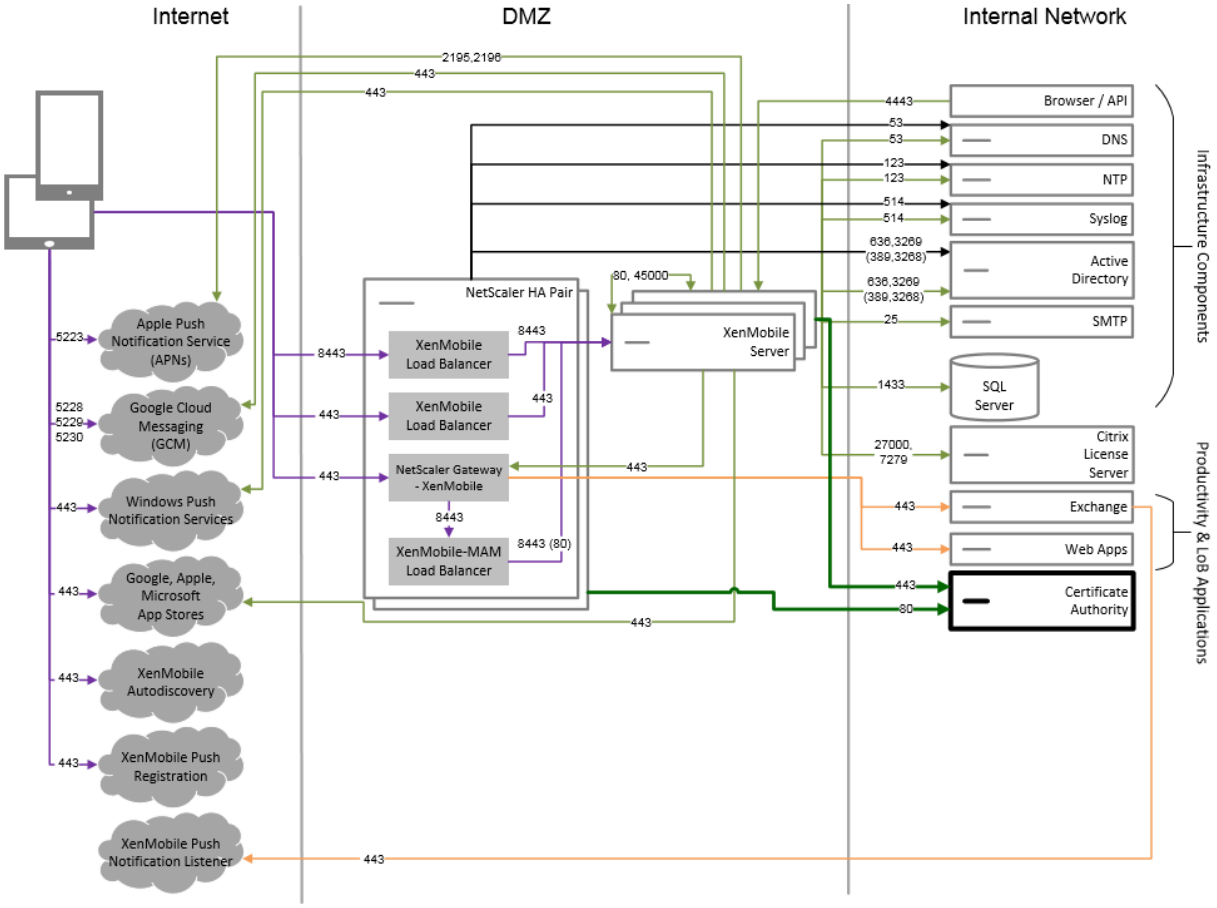


外部証明機関を含むリファレンスアーキテクチャ

外部認証期間を含む環境により次の要件の 1 つ以上を満たすことが推奨されます:

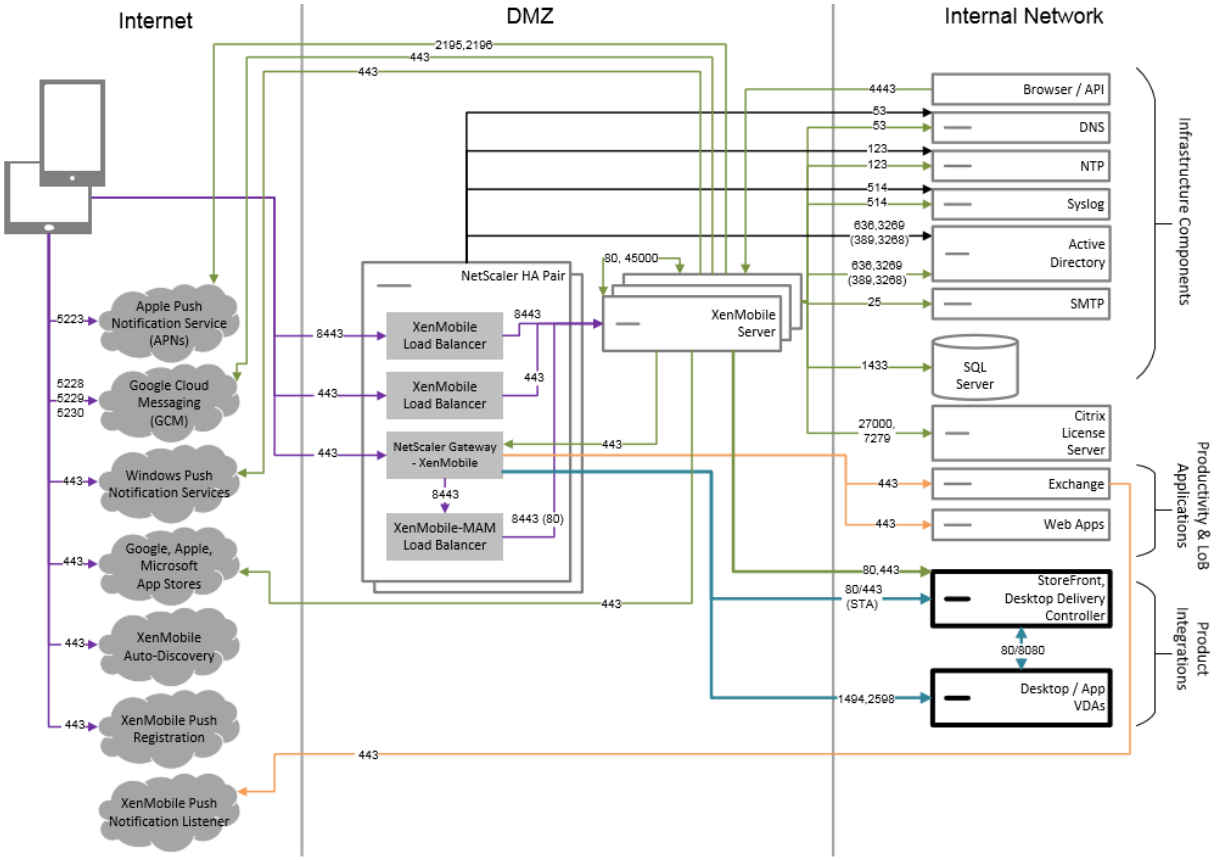
- NetScaler Gateway でのユーザー認証にユーザー証明書を要求する（イントラネットアクセス用）。
- Secure Mail ユーザーには、Exchange Server の認証にユーザー証明書を要求する。
- たとえば、企業の証明機関が発行した証明書をモバイルデバイスにプッシュして、WiFi アクセスできるようにする必要があります。

この図は MDM+MAM アーキテクチャに展開された外部証明機関を示していますが、同様に MDM-only または MAM-only アーキテクチャの一部として外部証明機関を展開することもできます。



Virtual Apps and Desktops を含むリファレンスアーキテクチャ

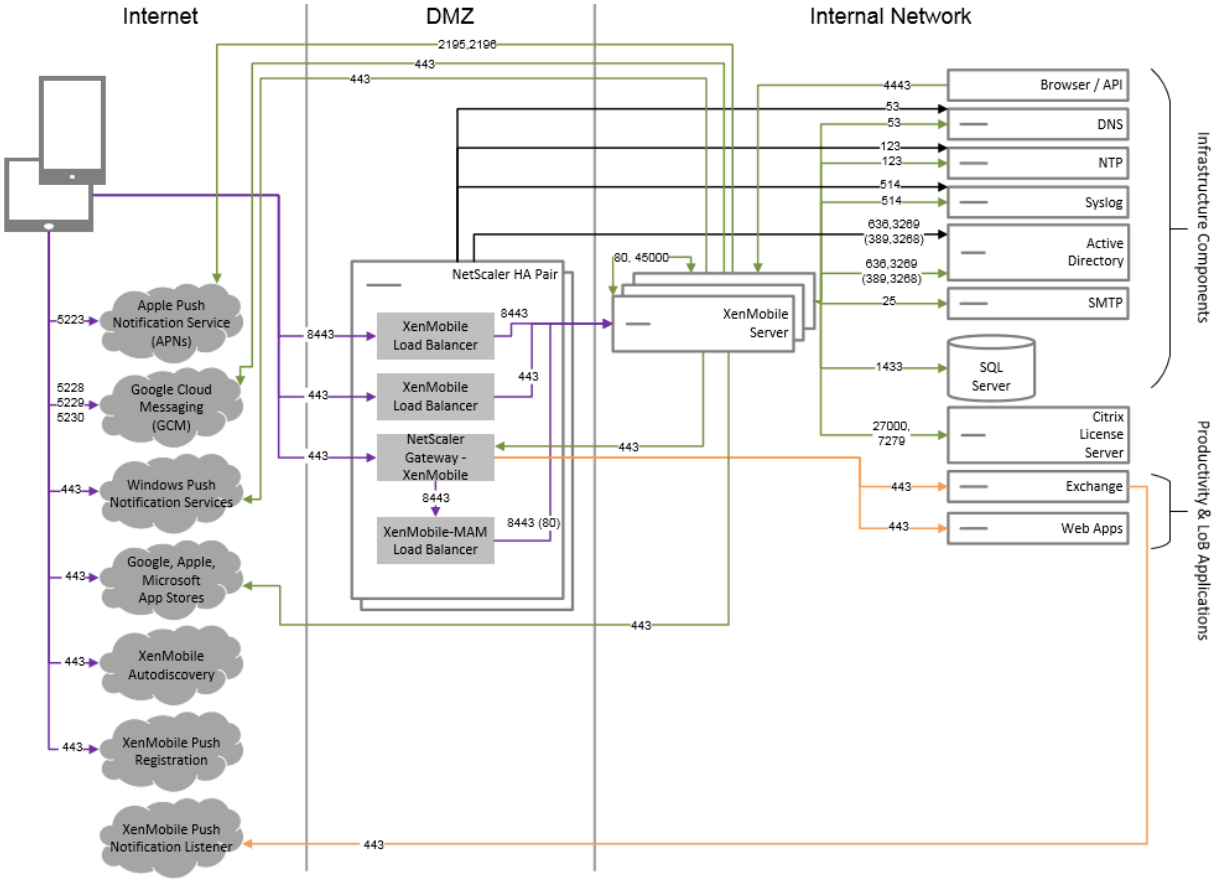
Virtual Apps and Desktops を XenMobile に統合する場合は、このアーキテクチャを展開します。たとえば、すべてのタイプのアプリケーション（モバイル、SaaS、Windows）のモバイルユーザーに統一されたアプリストアを提供する必要がある場合です。図には、MDM および MAM アーキテクチャに展開された Virtual Desktops が示されていますが、同様に MAM-only アーキテクチャの一部として Virtual Desktops を展開することもできます。



内部ネットワークにおける **XenMobile** を使用したリファレンスアーキテクチャ

XenMobile では、次の 1 つ以上の要件に対応するために、アーキテクチャを内部ネットワーク内に展開できます:

- DMZ にハイパーバイザーがないか、許可されていない。
- DMZ にはネットワークアプライアンスしか含めることができない。
- セキュリティ要件のため、SSL オフロードを使用する必要がある。



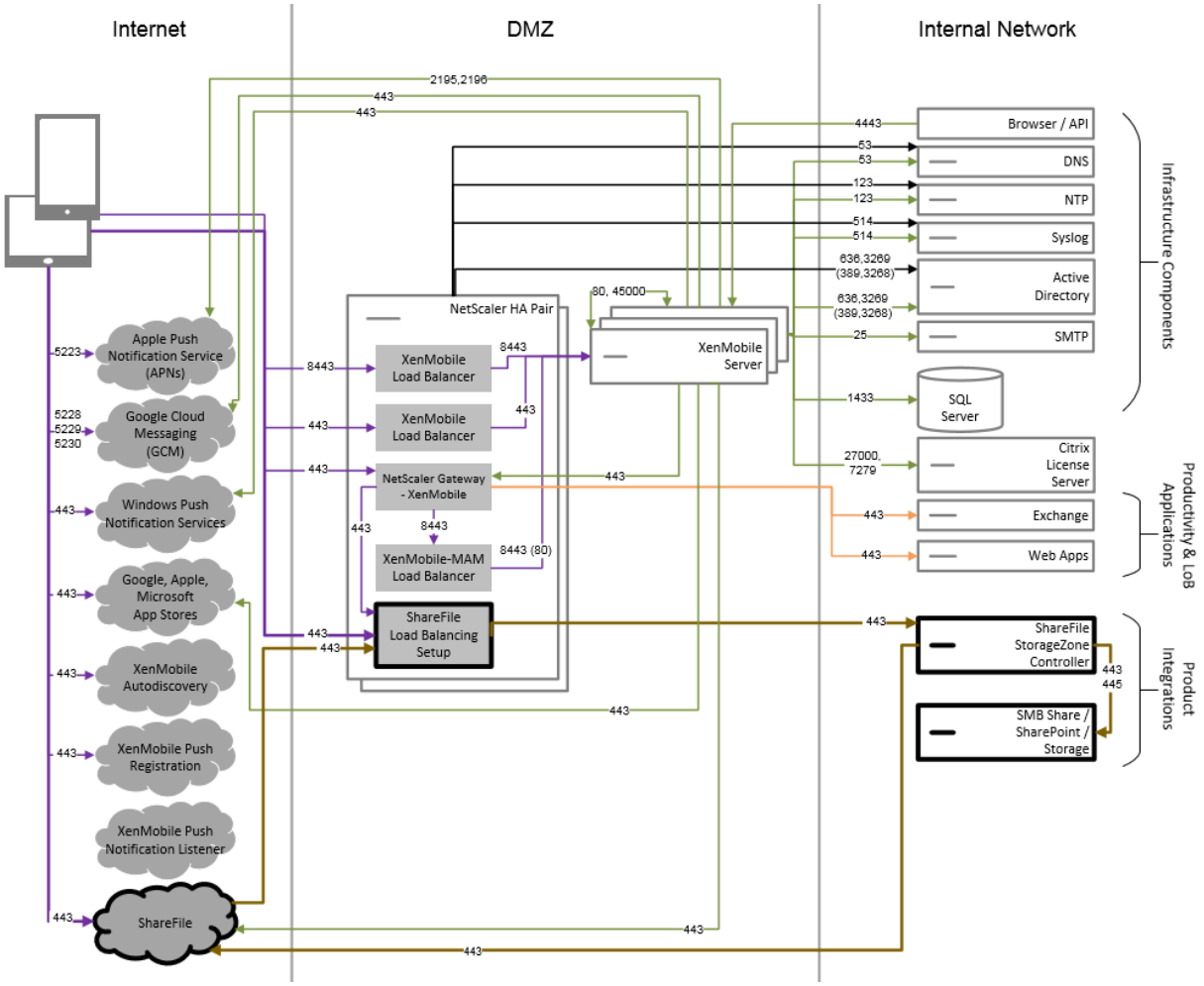
ShareFile を使用するリファレンスアーキテクチャ

XenMobile に ShareFile Enterprise または StorageZone Connectors のみを統合する場合は、このアーキテクチャを展開します。ShareFile Enterprise 統合により、次の要件の 1 つ以上を満たすことができます：

- ShareFile.com にユーザーにシングルサインオン（SSO）を設定するには、IDP が必要である。
- ShareFile.com にアカウントをプロビジョニングする方法が必要である。
- モバイルデバイスからアクセスする必要があるオンプレミスのデータリポジトリがある。

StorageZone コネクタのみと統合すると、ユーザーは、SharePoint サイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。この構成では、ShareFile サブドメインの設定や ShareFile に対するユーザーのプロビジョニング、ShareFile データのホストが不要になります。

図には、MDM+MAM アーキテクチャに展開された ShareFile が示されていますが、同様に MAM-only アーキテクチャの一部として ShareFile を展開することもできます。



サーバープロパティ

September 24, 2019

サーバープロパティは、XenMobile インスタンス全体の動作、ユーザー、およびデバイスに適用されるグローバルプロパティです。使用する環境で、この記事で取り上げたサーバープロパティを評価していただくことをお勧めします。他のサーバーのプロパティを変更する前には、シトリックスにご相談ください。

一部のサーバープロパティを変更すると、XenMobile Server の各ノードの再起動が必要になります。再起動が必要な時に XenMobile によって通知されます。

一部のサーバープロパティは、パフォーマンスと安定性を向上させます。詳しくは、「XenMobile の動作の調整」を参照してください。

Access all apps in the managed Google Play storetrue の場合、XenMobile によってパブリック Google Play ストアのすべてのアプリに managed Google Play ストアからアクセスできるようになります。このプロパテ

ィを **true** に設定すると、すべての Android Enterprise ユーザー向けのパブリック Google Play ストアアプリがホワイトリストに登録されます。管理者は、制限デバイスポリシーを使用してこれらのアプリへのアクセスを制御できます。デフォルトは **false** です。

ルート化された **Android** とジェイルブレイクされた **iOS** デバイスの登録をブロック: このプロパティが **True** の場合、XenMobile はルート化された Android デバイスおよびジェイルブレイクされた iOS デバイスの登録をブロックします。デフォルト値は **true** です。推奨の設定は、すべてのセキュリティレベルに対して **True** です。

登録が必要: このプロパティは、XenMobile サーバーのモードが ENT の場合にのみ適用され、ユーザーが MDM に登録する必要があるかどうかを指定します。このプロパティは、XenMobile インスタンスのすべてのユーザーとデバイスに適用されます。登録を必要とすることで、より高度なセキュリティを提供します。ただし、その決定は MDM が必要かどうかにより異なります。デフォルトでは、登録は必要ありません。

このプロパティが **False** の場合、ユーザーは登録を拒否できますが、引き続き XenMobile Store を通してデバイス上のアプリにアクセスできます。このプロパティが **True** の場合、登録を拒否するユーザーはアプリへのアクセスが拒否されます。

ユーザーが登録した後にこのプロパティを変更すると、ユーザーを再登録する必要があります。

MDM 登録が必要かどうかについて詳しくは、「デバイス管理と MDM 登録」を参照してください。

XenMobile MDM Self Help Portal コンソールの最大非アクティブ間隔 **(**分**)**: このプロパティ名には、古い XenMobile のバージョンが反映されています。このプロパティは、XenMobile コンソールの最大非アクティブ間隔を制御します。この間隔は、非アクティブなユーザーが XenMobile コンソールからログアウトされるまでの分数です。タイムアウトが 0 の場合、非アクティブなユーザーはログインしたままになります。デフォルトは **30** です。

無操作状態によるタイムアウト **(**分**)**: XenMobile の公開 API を使用して XenMobile コンソールやサードパーティ製アプリにアクセスする非アクティブなユーザーがログアウトされるまでの分数。タイムアウト値が **0** の場合、非アクティブなユーザーはログインしたままになります。API にアクセスするサードパーティのアプリは、通常はログインしたままにする必要があります。デフォルトは **5** です。

iOS デバイス管理登録: 必要な場合ルート **CA** をインストールする: Apple の最新の登録ワークフローでは、ユーザーが手動で MDM プロファイルをインストールする必要があります。このワークフローは、Apple Business Manager または Apple School Manager で割り当てられたサーバーへの MDM 登録には適用されません。ただし、MDM に手動で登録する場合、iOS デバイスのユーザーには MDM デバイス証明書のプロンプトのみが表示されます。

手動登録時のユーザーエクスペリエンスを向上させるには、サーバープロパティ`ios.mdm.enrollment.installRootCaIfRequired`を**`false`**に変更することをお勧めします。デフォルト値は**`true`**です。その結果、MDM 登録中に Safari ウィンドウが開き、ユーザーのプロファイルのインストールが簡素化されます。

最小 **VPP** 基準間隔: 最小 **VPP** 基準間隔は XenMobile が VPP ライセンスを Apple から再インポートする最小間隔を設定します。ライセンス情報を更新することにより、XenMobile にすべての変更が反映されます（インポートされたアプリを VPP から手動で削除した場合など）。デフォルトで、XenMobile は VPP ライセンスベースラインを最低 **720** 分ごとに更新します。

多数の VPP ライセンスをインストールしている場合（たとえば、50,000 個以上）、ベースライン間隔を広げてライセンスをインポートする頻度とオーバーヘッドを減らすことをお勧めします。Apple からの頻繁な VPP ライセンス

変更が予想される場合は、変更に対して XenMobile が最新状態を維持できるよう、この値を下げることをお勧めします。2 つのベースライン間の最小間隔は 60 分です。cron ジョブはバックグラウンドで 60 分ごとに実行されるため、VPP ベースライン間隔が 60 分の場合、ベースライン間の間隔は最大 119 分開く可能性があります。

デバイスポリシーおよびアプリポリシーの展開

January 10, 2020

XenMobile にデバイスポリシーとアプリポリシーを適用すると、次のような要素間のバランスを最適化できます。

- 企業セキュリティ
- 企業データおよび資産の保護
- ユーザーのプライバシー
- 生産的で好ましいユーザーエクスペリエンス

これらの要素間の最適なバランスはさまざまです。たとえば、金融などの高度に規制されている組織では、ユーザーの生産性が重視される教育や小売りなどの業界よりも厳格なセキュリティ管理が求められます。

ユーザーの ID、デバイス、場所、および接続タイプに基づいてポリシーを集中的に管理および構成し、企業コンテンツが悪用されるのを抑制できます。デバイスを紛失または盗まれた場合、ビジネスアプリとデータをリモートで無効にしたり、ロックやワイプを行ったりできます。総合的に見ると、従業員の満足度と生産性を向上させると同時に、セキュリティと管理者によるコントロールを保証するソリューションということになります。

この記事ではセキュリティに関連する多くのデバイスポリシーとアプリポリシーに焦点を当てます。

セキュリティリスクに対処するポリシー

XenMobile のデバイスポリシーとアプリポリシーは、次のようなセキュリティリスクを引き起こす可能性のある、様々な状況に対応しています。

- 信頼できないデバイスや予期しない場所からアプリやデータにアクセスしようとした場合。
- デバイス間でデータを移動させる場合。
- 権限のないユーザーがデータにアクセスしようとした場合。
- 退社したユーザーが独自のデバイス（Bring Your Own Device：BYOD）を使用した場合。
- デバイスを紛失した場合。
- 常時安全にネットワークにアクセスする必要がある場合。
- ユーザーが自分でデバイスを管理していて、仕事用のデータと個人用のデータを分ける必要がある場合。
- デバイスがアイドル状態で、ユーザーの資格情報の検証が再度必要な場合。
- 機微なコンテンツをコピーして、保護されていないメールシステムに貼り付ける場合。
- 個人用アカウントと企業アカウントの両方があり、機微なデータが保存されているデバイスで電子メールの添付ファイルまたは Web リンクを受信した場合。

企業データの保護においては、こうした事態が懸念される場面は主に 2 つあります。具体的にはデータが次のような状態にあるときです。

- 保存されている
- 転送している

XenMobile による保存データの保護

モバイルデバイスに格納されているデータは、保存データと呼ばれます。XenMobile のモバイルアプリケーション管理（MAM）機能を利用すると、業務用モバイルアプリ、MDX 対応アプリ、およびそれらに関連付けられたデータに対する完全な管理、セキュリティ、および制御を実現できます。XenMobile 環境でアプリを有効にする Worx App SDK は、Citrix MDX アプリコンテナ技術を利用して、ユーザーのモバイルデバイス上にある企業のアプリとデータを、個人のアプリとデータから分離します。これにより、包括的なポリシーベースの制御に基づいて、カスタムで開発されたモバイルアプリやサードパーティ製のモバイルアプリ、BYO モバイルアプリをすべて保護することができます。

豊富な MDX ポリシーライブラリに加えて、XenMobile はアプリレベルでの暗号化も備えています。XenMobile はデバイスの PIN コードを必要とせずに、MDX 対応アプリ内に保存されたデータを単独で暗号化します。ポリシーを適用するためにデバイスを管理する必要もありません。

ポリシーと Worx App SDK を使用すると次のことを実現できます。

- ビジネス用と個人用それぞれのアプリおよびデータをセキュリティで保護されたモバイルコンテナ内で分離。
- 暗号化やその他のモバイルデータ損失防止（Data Loss Prevention：DLP）技術でアプリを保護。

MDX ポリシーは多くの操作を制御できるため、すべての通信を制御しながら、MDX でラップされたアプリ間のシームレスな統合を実現できます。このようにして、MDX 対応アプリでのみデータにアクセスできるようにするなどのポリシーを適用することができます。

デバイスポリシーとアプリポリシーの管理以外では、暗号化が保存データを安全に保護する方法としては最適です。XenMobile は MDX 対応のアプリケーションに保存されたデータに暗号化レイヤーを追加することで、パブリックファイル暗号化、プライベートファイル暗号化、暗号化の除外などの機能をポリシーで制御できます。Worx App SDK では、保護された Citrix Secret Vault に保存されているキーを用いて、FIPS 140-2 準拠の AES 256 ビット暗号化を行います。

XenMobile による転送データの保護

ユーザーのモバイルデバイスと内部ネットワークとの間を移動するデータは、転送データと呼ばれます。MDX アプリコンテナ技術は、内部ネットワークに対するアプリケーション専用の VPN アクセスを、NetScaler Gateway を介して提供します。

従業員が、モバイルデバイスからセキュアなエンタープライズネットワークに存在するリソース（企業メールサーバー、企業イントラネット上にホストされている SSL 対応の Web アプリケーション、ファイルサーバーや Microsoft SharePoint に保存されているドキュメントなど）にアクセスする場合を考えてみます。MDX を使用すると、アプリ

ケーション専用のマイクロ VPN を介して、モバイルデバイスからこれらすべての企業リソースにアクセスできます。各デバイスに専用のマイクロ VPN トンネルが用意されます。

Micro VPN 機能により、信頼できないモバイルデバイスのセキュリティを脅かす可能性がある、デバイス全体での VPN は不要になります。そのため、内部ネットワークがマルウェアや企業システム全体に感染する可能性のある攻撃にさらされることはありません。企業のモバイルアプリと個人用のモバイルアプリを、1 つのデバイス上で共存させることができます。

セキュリティレベルをさらに強化するには、代替 NetScaler Gateway ポリシーを使用して MDX 対応アプリを構成することができます。これは認証およびアプリとのマイクロ VPN セッションに使用します。代替 NetScaler Gateway をオンラインセッション必須ポリシーと組み合わせて使用し、アプリを指定のゲートウェイで再認証するようにできます。通常、このようなゲートウェイには、別の（確実性の高い）認証要件およびトラフィック管理ポリシーが割り当てられています。

マイクロ VPN はセキュリティ機能に加えて、最小限のデータだけを転送する圧縮アルゴリズムなどのデータ最適化技術を提供し、転送が最短時間で実行されるようにします。それによってモバイルのプロジェクトを成功させる要素として重要な、ユーザーエクスペリエンスが向上します。

次のような場合は、デバイスポリシーを定期的に再評価する必要があります。

- デバイスのオペレーティングシステムのアップデートがリリースされたことで、XenMobile の新しいバージョンに新しいポリシーまたは更新されたポリシーが含まれる場合。
- 新しいデバイスタイプを追加する場合。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、iOS、Android、Windows デバイスの間で異なるほか、Android を実行するデバイスの製造元によっても違いがある場合があります。
- XenMobile の運用を、企業の新しいセキュリティポリシーやコンプライアンス規制など、企業や業界の変化に対して継続的に同期させる。
- 新しいバージョンの MDX Toolkit に新しいポリシーまたは更新されたポリシーが含まれている場合。
- アプリを追加または更新する場合。
- アプリや要件が新しくなった結果、ユーザー用に新しいワークフローを統合する必要がある場合。

アプリポリシーとユースケースのシナリオ

Secure Hub で利用可能なアプリを選択できますが、それらのアプリが XenMobile とやり取りする方法を定義しなくてはならない場合もあります。特定の期間が経過した後にユーザーを認証させたい場合、またはユーザーが情報にオフラインでアクセスできるようにする場合は、アプリポリシーを使用します。以下の一覧ではポリシーの一部と、その使用方法について説明します。プラットフォームごとの MDX ポリシーの一覧については、「MDX ポリシーの概要」を参照してください。

認証ポリシー

- デバイスのパスコード

このポリシーを使用する理由: デバイスのパスコードポリシーを有効にして、デバイスのデバイス PIN が有効になっている場合にのみ、ユーザーが MDX アプリにアクセスできるようにします。iOS 9 デバイスでは、この機能によってデバイスレベルおよび MDX コンテナでの iOS 暗号化が保証されます。

ユーザーの例: このポリシーを有効にすると、iOS デバイスで PIN コードを設定しない限りは、MDX アプリにアクセスできないようになります。

- アプリのパスコード

  このポリシーを使用する理由: アプリのパスコードポリシーを有効にすると、Secure Hub で管理対象アプリを認証しない限りは、アプリを開いてデータにアクセスできないようになります。XenMobile Server 設定のクライアントのプロパティで構成する内容に応じて、ユーザーは Active Directory のパスワード、Citrix PIN、または iOS TouchID で認証できます。クライアントのプロパティで非アクティブタイマーを設定すると、継続的に使用している限りは、タイマーが切れるまでの間に Secure Hub が管理対象アプリの認証をユーザーに再度求めないようにすることができます。

  アプリのパスコードはデバイスのパスコードとは次の点で異なります。デバイスのパスコードポリシーをデバイスにプッシュすると、Secure Hub はパスコードまたは PIN を設定するようにユーザーに求めます。これにより、デバイスの電源を入れたとき、または非アクティブタイマーが時間切れになったときに、デバイスのロックを解除しない限りはデバイスにアクセスできなくなります。詳しくは、「XenMobile での認証」を参照してください。

  ユーザーの例: デバイス上で Citrix Secure Web アプリケーションを開くときに非アクティブ期間が過ぎていると、Citrix PIN を入力しない限りは Web サイトを参照できなくなります。

- オンラインセッションを必須とする

  このポリシーを使用する理由: アプリケーションを実行するために Web アプリケーション（Web サービス）へのアクセスが必要である場合は、このポリシーを有効にすることで、企業ネットワークに接続するかアクティブなセッションを確立してからアプリケーションを使用するように、XenMobile からユーザーに対して求めるようにできます。

  ユーザーの例: オンラインセッションを必須とするポリシーが有効になっている MDX アプリをユーザーが開こうとすると、携帯電話または Wi-Fi サービスを使用してネットワークに接続しない限り、アプリを使用できなくなります。

- 最大オフライン期間

  このポリシーを使用する理由: このポリシーを追加のセキュリティオプションとして使用すると、XenMobile でアプリの資格の再確認および最新のポリシーの更新を行わずに、長期間アプリをオフラインで実行することはできなくなります。

  ユーザーの例: 最大オフライン期間を適用した MDX アプリを構成すると、オフラインタイマー期間が終了するまでの間、ユーザーはオフラインでアプリを開いて使用できます。期間が終了した時点で、ユーザーは携帯電話または Wi-Fi サービス経由でネットワークに接続し、プロンプトが表示されたら再認証する必要があります。

その他のアクセスポリシー

- アプリ更新猶予期間（時間）

  このポリシーを使用する理由： アプリ更新猶予期間とは、XenMobile Store にリリースされている新しいバージョンのアプリを更新するまでの間、ユーザーが利用できる時間です。猶予期間が終了した時点で、ユーザーはアプリを更新しない限り、アプリ内のデータにアクセスできなくなります。この値を設定する場合には、モバイルワーカーのニーズ、特に海外旅行で長期間オフラインの状態になる可能性があるユーザーのニーズを考慮してください。

  ユーザーの例：XenMobile Store に新しいバージョンの Secure Mail をロードしてから、アプリ更新猶予期間を 6 時間に設定します。Secure Mail のすべてのユーザーには、6 時間が経過するまで、Secure Mail アプリの更新を求めるメッセージが表示されます。6 時間が経過すると、Secure Hub はユーザーを XenMobile Store にルーティングします。

- アクティブなポーリング周期（分）

  このポリシーを使用する理由：アクティブなポーリング周期とは、XenMobile がアプリの App Lock や App Wipe などのセキュリティアクションを実行するタイミングをチェックする間隔のことです。

  ユーザーの例： アクティブなポーリング期間ポリシーを 60 分に設定した場合、XenMobile からデバイスに App Lock コマンドを送信すると、最後のポーリングが行われてから 60 分以内にロックが発生します。

暗号化ポリシー

これらのポリシーを使用する理由： XenMobile には強力な暗号化レイヤーを備えた Secret Vault が搭載されており、これにより Secure Hub や他の業務用モバイルアプリがパスワードや暗号キーなどの機微なデータを、プラットフォームのネイティブキーストアに依存することなくデバイスに保存できます。そのため、デバイスが何らかの形で侵害された場合、企業データは MDX コンテナ内で暗号化された状態が維持され、このデータはコンテナの外に転送される前に XenMobile によって難読化されます。

ユーザーの例： デバイスの所有者がデバイスの PIN を設定しなかった場合、またはデバイスの PIN が侵害された場合、Secure Hub コンテナ内の企業データはセキュリティで保護された状態が維持されます。

アプリ相互作用ポリシー

これらのポリシーを使用する理由： アプリ相互作用ポリシーを使用して、MDX アプリからデバイス上の他のアプリへのドキュメントおよびデータの流れを制御します。たとえば、ユーザーがコンテナの外部にある個人アプリにデータを移動したり、コンテナの外部からコンテナ化されたアプリにデータを貼り付けたりすることを防止できます。

ユーザーの例： アプリ相互作用ポリシーを［制限］に設定すると、ユーザーは Secure Mail から Secure Web にテキストをコピーできますが、コンテナの外にある個人の Safari や Chrome ブラウザーにそのデータをコピーすることはできません。また、ユーザーは Secure Mail の添付ファイルを ShareFile または Quick Edit で開くことはできますが、添付ファイルをコンテナの外にある個人のファイル閲覧アプリで開くことはできません。

アプリ制限ポリシー

これらのポリシーを使用する理由: アプリ制限ポリシーは、MDX アプリが開いている間にユーザーがアプリからアクセスできる機能を制御するために使用します。これにより、アプリの実行中に悪意のある行為が発生しないようにすることができます。アプリ制限ポリシーは、iOS と Android でわずかに異なります。たとえば iOS では、MDX アプリの実行中に iCloud へのアクセスをブロックできます。Android では、MDX アプリの実行中に近距離無線通信（NFC）の使用を停止できます。

ユーザーの例: アプリ制限ポリシーを有効にして MDX アプリでの iOS の音声入力をブロックすると、ユーザーは MDX アプリの実行中に、iOS キーボードの音声入力機能を使用できなくなります。そのため、ユーザーの音声入力データが、セキュリティで保護されていないサードパーティのクラウド音声入力サービスに渡されることはありません。ユーザーがコンテナの外で個人のアプリを開いた場合、ユーザーが個人的な通信手段として使用する音声入力のオプションは、変わらず利用できます。

アプリのネットワークアクセスポリシー

これらのポリシーを使用する理由: アプリのネットワークアクセスポリシーは、デバイスのコンテナ内の MDX アプリから社内ネットワークにあるデータへのアクセスを提供するために使用します。ネットワークアクセスポリシーでは、［内部ネットワークへトンネル］オプションを設定して、MDX アプリから NetScaler 経由での、バックエンドの Web サービスまたはデータストアへのマイクロ VPN を自動化します。

ユーザーの例: トンネリングが有効になっている Secure Web などの MDX アプリをユーザーが開くと、Web ブラウザーが開いてイントラネットサイトが起動します。ユーザーが VPN を開始する必要はありません。Secure Web アプリは、マイクロ VPN 技術を使用して内部サイトに自動的にアクセスします。

アプリの地理位置情報およびジオフェンシングポリシー

これらのポリシーを使用する理由: アプリの地理位置情報およびジオフェンシングを制御するポリシーには、中心点経度、中心点緯度、および半径が含まれます。これらのポリシーの対象には、特定の地理的領域にある MDX アプリのデータに対するアクセスが含まれます。このポリシーでは緯度および経度座標の半径によって地理的エリアを定義します。定義された半径外にあるアプリをユーザーが使用しようとしても、アプリはロックされたままで、アプリデータにはアクセスできません。

ユーザーの例: ユーザーが自分の職場がある場所にいる間は M&A のデータにアクセスできますが、オフィスの外に移動すると、この機微なデータにアクセスできなくなります。

Secure Mail アプリポリシー

- バックグラウンドネットワークサービス

  このポリシーを使用する理由: Secure Mail のバックグラウンドネットワークサービスは、Secure Ticket Authority（STA）を利用します。これは、事実上 NetScaler Gateway 経由で接続する SOCKS5 プロキシ

です。STA は長時間の接続をサポートしており、マイクロ VPN に比べてバッテリー寿命が長くなります。そのため、STA は常に接続しておくメールに最適です。Secure Mail ではこれらの設定を構成することをお勧めします。NetScaler for XenMobile ウィザードでは、Secure Mail の STA が自動的に設定されます。

ユーザーの例： STA が有効になっていないときに Android ユーザーが Secure Mail を開くと、VPN を開くように求められ、デバイス上で開かれたまま維持されます。STA が有効になっているときに Android ユーザーが Secure Mail を開くと、Secure Mail は VPN を必要とせずシームレスに接続されます。

- デフォルトの同期間隔

  このポリシーを使用する理由： この設定では、ユーザーが Secure Mail に初めてアクセスしたときに、メールが Secure Mail と同期する既定の日数を指定します。2 週間分のメールの同期には 3 日以上の時間がかかり、ユーザーのセットアッププロセスが長くなることに注意してください。

  ユーザーの例： ユーザーが最初に Secure Mail を設定したときのデフォルトの同期間隔が 3 日に設定されている場合、現在から過去 3 日間に受信した受信トレイ内のメールがすべて表示されます。4 日以上経過したメールを見たい場合は、検索することができます。そうすることでサーバーに保存されている古いメールが Secure Mail に表示されます。Secure Mail のインストール後に、ユーザーはそれぞれのニーズに合わせてこの設定を変更できます。

デバイスポリシーとユースケースの動作

XenMobile がデバイスでどのように動作するかは、デバイスポリシー（MDM ポリシーとも呼ばれます）によって決まります。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。以下の一覧ではデバイスポリシーの一部と、その使用方法について説明します。すべてのデバイスポリシーの一覧については、「デバイスポリシー」を参照してください。

- アプリインベントリポリシー

  このポリシーを使用する理由： ユーザーがインストールしたアプリを表示する必要がある場合は、アプリインベントリポリシーをデバイスに展開します。アプリインベントリポリシーを展開しない場合、ユーザーが XenMobile Store からインストールしたアプリのみが表示され、個人的にインストールしたアプリケーションは表示されません。特定のアプリが企業デバイスで実行されないようにブラックリストに追加するには、このポリシーを使用する必要があります。

  ユーザーの例： MDM 管理デバイスを使用するユーザーがこの機能を無効にすることはできません。ユーザーが個人的にインストールしたアプリケーションは、XenMobile 管理者に表示されます。

- アプリのロックポリシー

  このポリシーを使用する理由： Android 用のアプリのロックポリシーを使用すると、アプリをブラックリストまたはホワイトリストに追加できます。たとえば、アプリをホワイトリストに追加するとキオスクデバイスを構成できます。ユーザーがインストールできるアプリが制限されるため、通常は企業所有のデバイスにのみアプリのロックポリシーを展開します。上書きパスワードを設定すると、ブロックされているアプリにユーザーがアクセスできます。

ユーザー例： Angry Birds アプリをブロックするというアプリのロックポリシーを展開するとします。ユーザーは Google Play から Angry Birds アプリをインストールできますが、アプリを開くと管理者がアプリをブロックした旨のメッセージが表示されます。

- 接続のスケジューリングポリシー

  このポリシーを使用する理由： Windows Mobile デバイスが MDM 管理、アプリのプッシュ、およびポリシーの展開を行うために XenMobile Server に接続するには、接続のスケジューリングポリシーを使用する必要があります。Android、Android Enterprise、および Chrome OS デバイスの場合、このポリシーの代わりに Google の Firebase Cloud Messaging（FCM）を使用して、XenMobile Server への接続を制御します。スケジューリングオプションは次のとおりです：

  - 常に： 接続のオンライン状態を永続的に維持します。最適化されたセキュリティについては、このオプションをお勧めします。［常に］ を選択する場合は、接続タイマーポリシーも使用して、接続によるバッテリー切れが起こらないようにします。接続のオンライン状態を維持することにより、ワイプやロックなどのセキュリティコマンドを必要に応じてデバイスにプッシュできます。デバイスに展開した各ポリシーで、［展開スケジュール］オプションの ［常時接続に対する展開］ を選択することも必要です。
  - しない： 手動で接続します。デバイスにセキュリティポリシーを展開できず、新しいアプリやポリシーを受信しなくなるため、実稼働環境での ［しない］ オプションはお勧めしません。
  - 毎： 指定された間隔で接続します。このオプションが有効な状態でロックやワイプなどのセキュリティポリシーを送信すると、このポリシーは次回デバイスが接続されたときに XenMobile によって処理されます。
  - スケジュールを定義 - 有効にすると、XenMobile はネットワーク接続が失われた後に、ユーザーのデバイスを XenMobile サーバーに再接続するよう試行し、定義した期間中、一定の間隔でコントロールパケットを送信することによって接続を監視します。

  ユーザーの例： 登録されたデバイスにパスコードポリシーを展開する場合。スケジューリングポリシーを利用することで、デバイスは一定の間隔でサーバーに接続し、新しいポリシーを収集できます。

- 資格情報ポリシー

  このポリシーを使用する理由： 多くは Wi-Fi ポリシーと連携して使用されますが、この資格情報ポリシーを利用することで、証明書による認証が必要な内部リソースの認証に使用する証明書を展開できます。

  ユーザーの例： デバイスにワイヤレスネットワークを構成する Wi-Fi ポリシーを展開します。Wi-Fi ネットワークには認証用の証明書が必要です。資格情報ポリシーが証明書を展開すると、証明書はオペレーティングシステムのキーストアに格納されます。それによりユーザーは、内部リソースに接続したときに証明書を選択できます。

  - **Exchange** ポリシー

  このポリシーを使用する理由： XenMobile には、Microsoft Exchange ActiveSync のメールを配信する 2 つのオプションがあります。

- **Secure Mail** アプリ: パブリックアプリケーションストアまたは XenMobile Store から配布する Secure Mail アプリを使用してメールを配信します。
- ネイティブメールアプリ: Exchange ポリシーを使用して、デバイス上のネイティブメールクライアントで ActiveSync メールを有効にできます。ネイティブメールで Exchange ポリシーを使用すると、Active Directory 属性からマクロでユーザーデータを取得して入力できます。${user.username} ならユーザー名、${user.domain} ならユーザードメインのように、ユーザーデータを入力できます。

ユーザーの例: Exchange ポリシーをプッシュすると、Exchange Server の詳細がデバイスに送信されます。次に Secure Hub はユーザーに認証を求め、メールの同期を開始します。

- 場所ポリシー

  このポリシーを使用する理由: 場所ポリシーでは、デバイスの GPS が Secure Hub で有効になっている場合に、地図上でそのデバイスの場所を検出できます。このポリシーを展開し、XenMobile サーバーから locate コマンドを送信すると、デバイスは場所の座標を返します。

  ユーザーの例: 場所ポリシーが展開され、GPS がデバイスで有効になっている場合にユーザーがデバイスを紛失したときは、XenMobile Self Help Portal にログオンして［検索］オプションを選択すると、デバイスの場所を地図上に表示できます。Secure Hub で位置情報サービスの使用を許可することについては、ユーザーに選択権があることに注意してください。ユーザーがデバイスを自分で登録した場合に、位置情報サービスの使用を強制することはできません。このポリシーを使用するときにもう 1 つ考慮すべき事項は、バッテリー寿命への影響です。

- パスコードポリシー

  このポリシーを使用する理由: パスコードポリシーを使用すると、管理対象デバイスに PIN コードまたはパスワードを適用できます。このパスコードポリシーでは、デバイス上でパスコードの複雑さやタイムアウトを設定できます。

  ユーザーの例: パスコードポリシーを管理対象デバイスに展開すると、Secure Hub はパスコードまたは PIN を構成するようにユーザーに求めます。これにより、デバイスの電源を入れたとき、または非アクティブタイマーが時間切れになったときに、デバイスのロックを解除しない限りデバイスにアクセスできなくなります。

- プロファイル削除ポリシー

  このポリシーを使用する理由: ユーザーのグループにポリシーを展開した後で、そのポリシーをユーザーのサブセットから削除する必要があるとします。選択したユーザーのポリシーを削除するには、プロファイル削除ポリシーを作成し、展開規則を使用して、プロファイル削除ポリシーを指定されたユーザー名にのみ展開します。

  ユーザーの例: プロファイル削除ポリシーをユーザーデバイスに展開すると、ユーザーは変更に気付かない可能性があります。たとえば、デバイスカメラを無効にする制限がプロファイル削除ポリシーによって削除された場合、ユーザーにはカメラの使用が許可されていることは分かりません。ユーザーエクスペリエンスに影響を及ぼす変更については、ユーザーに通知することを検討してください。

- 制限ポリシー

このポリシーを使用する理由: 制限ポリシーによって、管理対象デバイスの機能をロックダウンおよび制御するさまざまなオプションを使用できます。対応デバイスでは数百の制限オプションを利用して、デバイスのカメラやマイクを無効にしたり、ローミング規則の適用やアプリストアのようなサードパーティサービスへのアクセスなどを制限したりできます。

ユーザーの例: iOS デバイスに制限を展開すると、ユーザーは iCloud または iTunes ストアにアクセスできなくなることがあります。

- 契約条件ポリシー

  このポリシーを使用する理由: デバイスを管理することの法的な意味を、ユーザーに知らせる必要がある場合があります。また、企業データをデバイスにプッシュするときの、セキュリティ上のリスクをユーザーに認識させる必要がある場合もあります。カスタムの契約条件文書では、ユーザー登録の前に規則および通知を公開できます。

  ユーザーの例: 登録処理中に契約条件の情報をユーザーに表示します。指定された条件の受け入れを拒否した場合、登録処理は終了し、ユーザーは企業データにアクセスすることはできません。レポートを生成して HR/法務/コンプライアンスチームに提供し、条件を了承または拒否した対象者を確認できます。

- **VPN** ポリシー

  このポリシーを使用する理由: VPN ポリシーは、古い VPN ゲートウェイ技術を使用するバックエンドシステムへのアクセスを提供するために使用します。このポリシーではさまざまな VPN プロバイダー（Citrix VPN に加えて Cisco AnyConnect、Juniper など）がサポートされています。また、このポリシーを CA にリンクして、オンデマンドで VPN を有効にできます（VPN ゲートウェイがこのオプションをサポートしている場合）。

  ユーザーの例: VPN ポリシーを有効にすると、ユーザーのデバイスは、ユーザーが内部ドメインにアクセスしたときに VPN 接続を開きます。

- **Web** クリップポリシー

  このポリシーを使用する理由: Web クリップポリシーは、Web サイトが直接開かれるアイコンをデバイスにプッシュする場合に使用します。Web クリップには Web サイトへのリンクが含まれており、カスタムアイコンを加えることができます。デバイス上では、Web クリップはアプリのアイコンのように見えます。

  ユーザーの例: ユーザーが Web クリップアイコンをクリックしてインターネットのサイトを開くことで、アクセスが必要なサービスを利用できます。Web リンクを使用する方が、Web ブラウザーアプリを開いてリンクアドレスを入力するよりも便利です。

- **Wi-Fi** ポリシー

  このポリシーを使用する理由: Wi-Fi ポリシーを使用すると、SSID、認証データ、および設定データなどの Wi-Fi ネットワークの詳細を管理対象デバイスに展開できます。

  ユーザーの例: Wi-Fi ポリシーを展開すると、デバイスが自動的に Wi-Fi ネットワークに接続してユーザー認証を行なうことで、ユーザーがネットワークにアクセスできるようになります。

- **Windows Information Protection** のポリシー

  このポリシーを使用する理由： Windows Information Protection（WIP）ポリシーは、企業データの潜在的な漏洩を防止するために使用します。設定した適用レベルの Windows Information Protection が求められるアプリを指定できます。たとえば、不適切なデータ共有のブロックや警告を行ったり、ユーザーにポリシーの上書きを許可したりすることができます。不適切なデータ共有を記録しながら許可し、サイレントで WIP を実行できます

  ユーザーの例： 不適切なデータ共有をブロックするように WIP ポリシーを構成するとします。ユーザーが保護されたファイルを、保護されていない場所にコピーまたは保存すると、この場所に保護された作業コンテンツを置くことはできない、という旨のメッセージが表示されます。

- **XenMobile Store** ポリシー

  このポリシーを使用する理由： XenMobile Store は、ユーザーが必要とするすべての企業アプリとデータリソースを、管理者が公開できる一元化されたアプリストアです。Citrix StoreFront で公開された Web アプリ、SaaS アプリ、MDX ラップされたアプリ、Citrix の生産性向上アプリ、.ipa や.apk ファイルなどのネイティブモバイルアプリ、iTunes と Google Play アプリ、Web リンク、Virtual Apps and Desktops アプリを追加できます。

  ユーザーの例： デバイスを XenMobile に登録すると、ユーザーは Citrix Secure Hub アプリを通じて XenMobile Store にアクセスし、利用できるすべての企業アプリとサービスを表示できます。ユーザーはアプリをクリックすると、インストール、データへのアクセス、アプリの評価とレビュー、XenMobile Store からのアプリの更新プログラムのダウンロードを行えます。

ユーザー登録オプション

January 10, 2020

ユーザーが iOS デバイスを XenMobile に追加できるようにする方法は数多くあります。詳細を検討する前に、環境内のデバイスをエンタープライズモード（MDM + MAM）、MDM モード、または MAM モード（MAM-only モードとも呼ばれます）のどれで登録するかを決定する必要があります。管理モードの詳細については、「管理モード」を参照してください。

最も高いレベルには、次の 4 つの登録オプションがあります。

- 登録招待状： ユーザーに登録招待状や招待リンクを送信します。
- **Self Help Portal**： ユーザーがアクセスするポータルを設定します。このポータルでは Secure Hub をダウンロードしてデバイスを登録したり、自分に登録招待状を送信したりすることができます。
- 手動登録： システムが起動していて登録可能であることをユーザーに知らせるメール、ハンドブック、その他の通信を送信します。ユーザーは Secure Hub をダウンロードし、デバイスを手動で登録します。
- エンタープライズ： デバイス登録のもう 1 つの選択肢は、Apple Device Enrollment Program（DEP）と Google Android Enterprise による登録です。これらの各プログラムを通して、従業員が使用する準備が整

った事前設定済みデバイスを購入できます。詳しくは、「Apple デバイス登録プログラム（DEP）」および「Google Android Enterprise」を参照してください。

登録招待状

iOS、macOS、または Android デバイスを使用するユーザーに登録招待状メールを送信できます。また、iOS、macOS、Android、Windows デバイスを使用するユーザーに、SMTP または SMS を使用してインストールリンクを送信することもできます。詳しくは、「デバイスの登録」を参照してください。

登録招待状による方法を選択した場合：最大 7 つの登録モード（プラットフォームによって異なります）から選択可能で、モードを任意に組み合わせて使用できます。XenMobile の設定ページからモードを有効にしたり無効にしたりできます。ユーザー名およびパスワード、2 要素、ユーザー名および PIN からデフォルトを選択できます。各登録モードについては、「登録モードを構成するには」を参照してください。

証明書ベースを選択した場合は、許可されるオプションからユーザー名およびパスワードによる従来の認証を除外することを検討してください。このモードは利用環境のオンボーディング面での手薄さをさらすことになり、強制されたセキュリティ品質を無効にする可能性があります。

招待状は多くの目的にかないます。招待状の最も一般的な使用方法は、システムが利用でき、登録可能であることをユーザーに通知することです。招待 URL は一意的なものです。ユーザーが招待 URL を使用すると、その URL は 2 度と使用できなくなります。このプロパティを使用して、システムに登録するユーザーやデバイスを制限できます。

次のいずれかの方法で、iOS ユーザーが登録時に資格情報を提供できるように XenMobile を設定できます。

- ユーザーが登録時に資格情報を入力する。
- ユーザーが派生資格情報プロバイダーのスマートカードをデスクトップに接続されたリーダーに挿入する。派生資格情報について詳しくは、「派生資格情報」を参照してください。

XenMobile コンソールでは、登録プロファイルのオプションを選択することもできます。これを使用すると、特定のユーザーが登録できるデバイスの数を Active Directory のグループに基づいて制御できます。たとえば、財務部門でユーザーごとに 1 つのデバイスしか許可しない場合には、登録プロファイルを使用してそのシナリオを構成できます。

特定の登録オプションを選ぶことで発生する追加コストや潜在的な危険に注意してください。SMS を使用して招待状を送信する場合は、追加のインフラストラクチャを設定する必要があります。詳しくは、「通知」を参照してください。

また、招待状をメールで送信しようとしている場合は、ユーザーが Secure Hub 以外のメールにアクセスする方法があることを確認してください。MDM 登録用の Active Directory パスワードの代わりに、ワンタイムパスワード（OTP）登録モードを使用できます。

Self Help Portal

ユーザーは Self Help Portal から登録招待状を要求できます。デフォルトモードはユーザー名およびパスワードですが、その要件を 2 要素やユーザー名および PIN に変更することもできます。Self Help Portal の設定について詳しくは、「登録モードを構成するには」を参照してください。

手動登録

手動登録では、ユーザーは Autodiscovery またはサーバー情報の入力によって XenMobile に接続します。Autodiscovery を利用する場合、ユーザーはメールアドレス、またはユーザープリンシパル名形式の Active Directory 資格情報のみを使用してサーバーにログオンします。Autodiscovery を利用しない場合、サーバーアドレスと Active Directory の資格情報を入力する必要があります。Autodiscovery の設定の詳細については、「XenMobile AutoDiscovery サービス」を参照してください。

手動登録は、さまざまな方法で簡単に行うことができます。ガイドを作成してユーザーに配布し、自身で登録してもらうことができます。IT 部門に依頼して、特定の時間枠でユーザーのグループを手動で登録してもらうこともできます。または、ユーザーが資格情報やサーバー情報を入力する必要がある同様の方法を利用することもできます。

ユーザーオンボーディング

環境を設定したら、どのようにしてユーザーを環境に取り込むかを決定する必要があります。この記事の前のセクションで、ユーザー登録モードの詳細について説明しています。このセクションでは、ユーザーにアプローチする方法について説明します。

オープン登録と選択的招待

ユーザーのオンボーディング時には、次の 2 つの基本的な方法で登録を許可できます。デフォルトでは、LDAP 資格情報と XenMobile 環境の情報を持つユーザーが登録できるオープン登録を許可できます。または、招待状を持つユーザーのみが登録できるようにして、ユーザー数を制限できます。さらに、Active Directory グループごとにオープン登録を制限することもできます。

招待状による方法を使用すると、ユーザーが登録できるデバイスの数を制限することもできます。ほとんどの場合、オープン登録を適用できますが、考慮すべき点がいくつかあります。

- MAM 環境を展開している場合、Active Directory グループメンバーシップを通して簡単に登録を制限できます。
- MDM 環境では、登録を制限する唯一の方法は、Active Directory グループメンバーシップに基づいて登録できるデバイスの数を制限することです。環境内で企業デバイスのみを許可する場合は、これは問題ではありません。ただし、環境内のデバイス数を制限する BYOD ワークプレースでは、この方法を検討することをお勧めします。
- ユーザーライセンスまたはデバイスライセンスがあるかどうかも念頭に置いてください。ユーザーライセンスでは、各ユーザーは複数のデバイスを所有できますが、使用するのは 1 つのライセンスのみです。デバイスライセンスでは、登録されたデバイスごとに 1 つのライセンスを使用します。

選択的招待は通常、必要な作業がオープン登録よりも少し多いため、オープン登録ほど頻繁に行なわれません。ユーザーが自分のデバイスを環境に登録するには、各ユーザーに固有の招待状を送信する必要があります。登録招待状を送信する方法については、「登録招待状の送信」を参照してください。

環境に登録するユーザーまたはグループごとに招待状を送信する必要があるため、組織の規模によっては時間がかかることがあります。Active Directory グループを使用して一括して招待状を作成することも可能ですが、この方法は間をおいて何度も行う必要があります。

ユーザーとの最初の連絡

オープン登録を使用するか選択的招待を使用するかを決定し、それらの環境を設定したら、ユーザーに登録オプションを知らせる必要があります。

選択的招待の方法を使用する場合は、メールと SMS メッセージが対応に含まれます。オープン登録の場合も、XenMobile コンソールからメールを送信できます。詳しくは、「登録招待状の送信」を参照してください。

どちらの場合も、メール用の SMTP サーバーが必要となります。テキストメッセージの場合は、SMS サーバーが必要です。これらは、決定の際に追加費用として考慮すべき場合があります。また、方法を選択する前に、新しいユーザーがメールなどの情報にアクセスする方法を検討してください。すべてのユーザーが XenMobile からメールにアクセスする場合には、招待メールの送信が問題になります。

また、オープン登録環境の場合、ユーザーが Secure Hub アプリを入手できる場所や登録に使用する方法などのすべての関連情報が含まれていれば、XenMobile 以外の別の方法で通信を送信することもできます。Autodiscovery を無効にしている場合は、XenMobile サーバーのアドレスも伝える必要があります。Autodiscovery の詳細については、「XenMobile AutoDiscovery サービス」を参照してください。

XenMobile の動作の調整

September 24, 2019

XenMobile の動作のパフォーマンスと安定性には XenMobile 全体にわたる多くの設定が関連しており、NetScaler と SQL Server データベースの構成によっても異なります。この記事では、XenMobile の調整と最適化に関連した代表的な構成を管理する設定に注目します。XenMobile を展開する前に、この記事の各設定を評価することをお勧めします。

> 重要:
>
> これらのガイドラインでは、デバイス数に対して XenMobile Server の CPU と RAM が適切であることを想定しています。スケーラビリティの詳細については、「スケーラビリティとパフォーマンス」を参照してください。

次のサーバープロパティは、XenMobile インスタンス全体の動作、ユーザー、およびデバイスにグローバルに適用されます。一部のサーバープロパティを変更すると、XenMobile Server の各ノードの再起動が必要になります。再起動が必要な時に XenMobile によって通知されます。

これらの調整のガイドラインは、クラスタ環境と非クラスタ環境の両方に適用されます。

hibernate.c3p0.idle_test_period

このカスタムキーという XenMobile サーバープロパティでは、接続が自動的に検証されるまでのアイドル時間を秒単位で指定します。このキーは次のように構成します。デフォルトは **30** です。

- キー：カスタムキー
- キー：**hibernate.c3p0. idle_test_period**
- 値：**120**
- 表示名：**hibernate.c3p0. idle_test_period**
- 説明：**Hibernate idle test period**

hibernate.c3p0.max_size

このカスタムキーでは、XenMobile で SQL Server データベースに対して開くことのできる最大接続数を指定します。XenMobile では、このカスタムキーに指定した値が上限として使用されます。接続は必要な場合のみ開かれます。値は、データベースサーバーの処理能力に合わせて設定します。

クラスター構成では、次の式に注意してください。c3p0 接続にノード数を掛けた値は、XenMobile が SQL Server データベースに対して開くことができる実際の最大接続数と等しくなります。

クラスター構成と非クラスター化構成では、小型の SQL Server に対してこの設定値が大きすぎると、ピーク負荷時に SQL 側でリソースの問題が発生する場合があります。設定値が小さすぎると、使用可能な SQL リソースを利用できなくなる場合があります。

このキーは次のように構成します。デフォルト値は **1000** です。

- キー：**hibernate.c3p0.max_size**
- 値：**1000**
- 表示名：**hibernate.c3p0.max_size**
- 説明：DB connections to SQL

hibernate.c3p0.min_size

このカスタムキーでは、XenMobile が SQL Server データベースに対して開く最小接続数を指定します。このキーは次のように構成します。デフォルトは **100** です。

- キー：**hibernate.c3p0.min_size**
- 値：**100**
- 表示名：**hibernate.c3p0.min_size**
- 説明：DB connections to SQL

hibernate.c3p0.timeout

このカスタムキーでは、アイドル状態のタイムアウトを指定します。データベースクラスターフェールオーバーを使用する場合は、このカスタムキーを追加し、アイドルタイムアウトの時間が短くなるように設定することをお勧めします。デフォルトは **120** です。

- キー：カスタムキー
- キー：**hibernate.c3p0.timeout**
- 値：**120**
- 表示名：**hibernate.c3p0.timeout**
- 説明：データベースのアイドルタイムアウト

プッシュサービスのハートビート間隔

この設定では、APNs（Apple プッシュ通知サービス）通知が一時的に配信されない場合に、iOS デバイスでチェックする頻度を指定します。APNs のハートビートの頻度を増やすと、データベース通信が最適化される場合があります。値が大きすぎると、不必要な負荷が加わる場合があります。この設定は、iOS にのみ適用されます。デフォルトは **20** 時間です。

ご使用の環境に多数の iOS デバイスがある場合、ハートビートの間隔により必要以上に負荷が高くなる場合があります。選択的なワイプ、ロック、完全なワイプなどのセキュリティ操作はこのハートビートに依存しません。これらの操作が実行されると、APNs 通知がデバイスに送信されるためです。この値は、Active Directory グループのメンバーシップが変更された後、ポリシーをどれだけ早く更新するかを管理します。そのため、多くの場合、負荷を軽減するにはこの値を 12 ～ 20 時間に増やすのが適しています。

iOS MDM APNS 接続プールのサイズ

APNs 接続プールが小さすぎると、100 を超えるデバイスを使用する場合、APNs アクティビティのパフォーマンスに悪影響を及ぼすことがあります。パフォーマンスの問題としては、アプリやポリシーのデバイスへの展開が遅くなったり、デバイスの登録が遅くなったりするといった問題があります。デフォルトは **1** です。デバイスが約 400 台が追加されるごとに、この値を 1 増やすことをお勧めします（最大 **15**）。

auth.ldap.connect.timeout

LDAP の反応が遅い場合に対処するには、次のカスタムキーのサーバープロパティを追加することをお勧めします。

- キー：カスタムキー
- キー：**auth.ldap.connect.timeout**
- 値：**60000**
- 表示名：**auth.ldap.connect.timeout**
- 説明：**LDAP** 接続のタイムアウト

auth.ldap.read.timeout

LDAP の反応が遅い場合に対処するには、次のカスタムキーのサーバープロパティを追加することをお勧めします。

- キー：カスタムキー
- キー：**auth.ldap.read.timeout**
- 値：**60000**
- 表示名：**auth.ldap.read.timeout**
- 説明：**LDAP** 読み取りのタイムアウト

その他のサーバーの最適化

サーバープロパティ	デフォルト設定	この設定を変更する理由
バックグラウンド展開	1,440 分	バックグラウンドポリシーの展開の頻度（分）。Android デバイスの常時接続にのみ適用されます。ポリシー展開の頻度を増やすと、サーバーの負荷が軽減されます。推奨の設定値は **1440**（24 時間）です。
バックグラウンドハードウェアインベントリ	1,440 分	バックグラウンドハードウェアインベントリの頻度（分）。Android デバイスの常時接続にのみ適用されます。ハードウェアインベントリの頻度を増やすと、サーバーの負荷が軽減されます。推奨の設定値は **1440**（24 時間）です。
削除された **Active Directory** ユーザーのチェック間隔	15 分	Active Directory の標準同期時間は **15** 分です。値 **0** を指定すると、XenMobile は削除された Active Directory ユーザーをチェックしません。推奨の設定値は **15** 分です。

MaxNumberOfWorker	3	多数の VPP ライセンスをインポートする時に使用するスレッド数です。デフォルトは **3** です。さらに最適化が必要な場合は、スレッド数を増やすことができます。ただし、スレッド数を大きくする（6 など）と、VPP ライセンスのインポートにより CPU 使用率が高くなる点に注意してください。

Android デバイスの展開スケジュールの最適化

Google Firebase Cloud Messaging（FCM）を使用して、Android デバイスの展開をスケジュールできます。

XenMobile 環境で FCM を有効にすると、iOS デバイスの APNS と同様に、Android デバイスにほぼリアルタイムで通知できます。FCM が構成されている場合で、XenMobile がポリシーのアップデートや選択的ワイプなどでデバイスに接続する必要がある場合、XenMobile Server はクライアントデバイスに要求を転送するように FCM サーバーに通知メッセージを送信します。デバイスが FCM から通知を受信すると、デバイスは XenMobile に接続して以降の手順を実行します。この方法は、サードパーティ製のサーバー（Google）に依存しているため、IT 部門または Citrix サポートの管理外でサービスが中断される場合があります。

FCM サービスへの登録方法については、「XenMobile and Firebase Cloud Messaging (FCM) Configuration（XenMobile および Firebase Cloud Messaging（FCM）の構成）」を参照してください。

Android で FCM を使用する場合、次の XenMobile Server プロパティに注意してください。

- **FCM API** キー： Google Developers Console で作成されたキー。
- **FCM** 送信者 **ID**： Google Developers Console のプロジェクト番号。
- **FCM** 登録 **ID TTL**： デバイスの FCM 登録 ID が更新されるまでの待ち時間（日）。デフォルトは **10** です。
- **FCM** ハートビート間隔： デフォルトは **20** 時間です。

SQL DB 内のデッドロックをチェックし、履歴データを削除する方法

デッドロックが発生したら、次のクエリを実行してデッドロックを確認してください。その後、データベース管理者または Microsoft SQL チームがその情報を確認できます。

SQL クエリ


```
SELECT

db.name DB_Service,

tl.request_session_id,

wt.blocking_session_id,

OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,

tl.resource_type,

h1.TEXT AS RequestingText,

h2.TEXT AS BlockingTest,

tl.request_mode

FROM sys.dm_tran_locks AS tl

INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id

INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address

INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id

INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id

INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id

CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1

CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2

GO
```

データベースのクリーンアップ

> 重要:
>
> テーブルに変更を加える前にデータベースをバックアップしてください。

1. 次のクエリを実行して履歴データを確認します。

```
select COUNT(\*) as total_record from dbo.EWDEPLOY_HISTO;
select COUNT(\*) as total_record from dbo.EWSESS;
select COUNT(*) as total_record from dbo.EWAUDIT;
```

2. 上記の 3 つのテーブルからデータを削除します。

> 注:
>
> 履歴データがテーブルに表示されないことがあります。その場合は、その特定のテーブルでの TRUNCATE クエリの実行をスキップします。

```
truncate TABLE dbo.EWDEPLOY_HISTO;
truncate TABLE dbo.EWSESS;
truncate TABLE dbo.EWAUDIT;
```

3. デッドロックが発生したためにブロックされた SELECT クエリのブロックを解除します。この手順ではさらに、そのほかのデッドロックも処理されます。

```
ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT
    ON WITH ROLLBACK IMMEDIATE
```

4. デフォルトのデータベースクリーンアップ設定では、セッションおよび監査ログの保持データは 7 日間保持されます。これは、多くのユーザーにとって長すぎます。そのため、クリーンアップ値を 1 日または 2 日に変更します。サーバープロパティで、次の変更を行います:

```
zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
zdm.dbcleanup.auditRetentionTimeInDays=1 day
```

KEYSTORE テーブルの孤立したファイルのクリーンアップ

XenMobile ノードのパフォーマンスが低い場合は、KEYSTORE テーブルが大きすぎないかを確認します。XenMobile は、登録証明書を ENROLLMENT_CERTIFICATE テーブルおよび KEYSTORE テーブルに保存します。デバイスを削除または再登録すると、証明書が ENROLLMENT_CERTIFICATE テーブルから削除されます。一方、KEYSTORE テーブルのエントリは保持され、パフォーマンスの問題を引き起こす可能性があります。次の手順を実行して、KEYSTORE テーブルの孤立したファイルをクリーンアップします。

> 重要:
>
> テーブルに変更を加える前にデータベースをバックアップしてください。

1. 次のクエリを実行して履歴データを確認します。

```
select COUNT(*) from KEYSTORE
```

2. 次のクエリを使用して、KEYSTORE テーブル内で孤立したファイルを確認します。

```
WITH cte(KEYSTORE_ID)
AS (SELECT KEYSTORE_ID
    FROM ENROLLMENT_CERTIFICATE
    UNION
    SELECT CA_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT CLIENT_KEYSTORE_ID
    FROM LDAP_CONFIG
    UNION
    SELECT KEYSTORE_ID
    FROM SAML_SERVICE_PROVIDER
    UNION
    SELECT KEYSTORE_ID
    FROM SERVER_CERTIFICATE)
SELECT keystore.id
FROM keystore
    LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
WHERE KEYSTORE_ID IS NULL;
```

3. 次のクエリを使用して、孤立したファイルをクリアします。

```
WITH cte(KEYSTORE_ID)
    AS (SELECT KEYSTORE_ID
        FROM ENROLLMENT_CERTIFICATE
        UNION
        SELECT CA_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT CLIENT_KEYSTORE_ID
        FROM LDAP_CONFIG
        UNION
        SELECT KEYSTORE_ID
        FROM SAML_SERVICE_PROVIDER
        UNION
        SELECT KEYSTORE_ID
```

```
15          FROM SERVER_CERTIFICATE)
16      DELETE FROM keystore
17      WHERE id IN
18      (
19          SELECT keystore.id
20          FROM keystore
21              LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
22          WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
23      );
```

4. 検索効率が向上するように、KEYSTORE テーブルにインデックスを追加します。

```
1 DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
2 ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;
3 CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
    ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
    DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
```

アプリのプロビジョニングとプロビジョニング解除

January 10, 2020

アプリケーションのプロビジョニングの中心は、モバイルアプリのライフサイクル管理であり、主として XenMobile 環境内でのモバイルアプリのラップ、構成、配信、管理を行います。場合によっては、プロビジョニングプロセスの一環としてアプリケーションコードの開発や変更も行います。XenMobile には、アプリのプロビジョニングに使用できるさまざまなツールとプロセスが用意されています。

アプリのプロビジョニングに関するこの記事を読む前に、アプリおよびユーザーコミュニティに関する各記事を読むことをお勧めします。組織でユーザーに提供する予定のアプリの種類を確定したら、アプリをライフサイクル全体にわたって管理するプロセスの概要を策定できるようになります。

アプリのプロビジョニングプロセスを定める際には、次の点を考慮してください。

- アプリのプロファイリング： 最初はアプリの数も限られているかもしれませんが、ユーザーへの普及率が増加し環境が拡大するにつれて、管理するアプリの数が急増する可能性があります。アプリのプロビジョニングを簡単に管理できるように、初めからアプリのプロファイルを明確に定義する必要があります。アプリのプロファイリングを行うことにより、非技術的な観点から、アプリを論理的なグループに分類できます。たとえば、次の要素に基づいてアプリのプロファイルを作成します。
  - バージョン：追跡用のアプリのバージョン
  - インスタンス：ユーザー集団別に、異なるアクセスレベルなどを設定してインスタンスを複数展開
  - プラットフォーム：iOS、Android、または Windows
  - 対象ユーザー：標準ユーザー、部署、経営幹部

- 所有権：アプリを所有する部門
- 種類：MDX、パブリック、Web および SaaS、または Web リンク
- アップグレードサイクル：アプリをアップグレードする頻度
- ライセンス：ライセンス要件と所有権
- MDX ポリシー：MDX セキュリティポリシーでラップするかどうか
- ネットワークアクセス：アクセスの種類（セキュアブラウズや完全 VPN など）

> 注：
> ［トンネル-Web SSO］は、MDX 設定において［セキュアブラウズ］に相当する名前です。動作は同じです。

例：

要素	Secure Mail	メール	社内	Epic Rover
バージョン	10.1	10.1	X.x	X.x
インスタンス	VIP	医師	臨床	臨床
プラットフォーム	iOS	iOS	iOS	iOS
対象ユーザー	VIP ユーザー	医師	臨床ユーザー	臨床ユーザー
所有権	IT 部門	IT 部門	IT 部門	IT 部門
種類	MDX	MDX	ネイティブ	パブリック
アップグレードサイクル	四半期単位	四半期単位	年単位	-
ライセンス	-	-	-	VPP
MDX ポリシー	はい	はい	はい	いいえ
ネットワークアクセス	VPN	VPN	VPN	パブリック

- アプリのバージョン管理： アプリのバージョンの管理および追跡は、プロビジョニングプロセスの重要な要素です。通常、ユーザーがバージョン管理を意識することはありません。ユーザーは、アプリの新しいバージョンがダウンロード可能になったときに通知を受け取るだけです。管理者の観点では、作成現場に影響を与えないために、作成担当者以外がアプリの各バージョンのレビューおよびテストを行うことも重要です。

  また、特定のアップグレードが本当に必要かどうかを評価することも重要です。アプリのアップグレードには、通常 2 つのタイプがあります。1 つは特定のバグの修正などのマイナーアップグレードであり、もう 1 つは、アプリに大幅な変更や改善をもたらすメジャーリリースです。どちらの場合でも、アップグレードが必要かどうか評価するために、アプリのリリースノートを慎重に確認する必要があります。

- アプリの署名およびラップ： XenMobile では、管理対象のアプリに MDX ポリシーを設定して、アプリをラップすることで企業データを保護できます。MDX Toolkit のアプリラッピングの詳細については、XenMobile

のドキュメントの「MDX Toolkit」を参照してください。ラップされたアプリのアプリプロビジョニングプロセスは、標準的なラップされていないアプリのプロビジョニングプロセスとは大きく異なります。

- アプリのセキュリティ： プロビジョニングプロセスの一環として、個々のアプリまたはアプリプロファイルのセキュリティ要件を定義します。アプリを展開する前に、セキュリティ要件を特定の MDM ポリシーまたは MAM ポリシーにマップすると、アプリの展開を大幅に簡略化し、迅速に行えるようになります。特定のアプリを異なる方法で展開する場合や、アプリで必要とされるセキュリティコンプライアンスの種類に応じて、XenMobile 環境のアーキテクチャの変更が必要になる場合があります。たとえば、重要なビジネスインテリジェンスアプリの使用を許可するためにデバイスを暗号化したり、特定のアプリでエンドツーエンドの SSL 暗号化やジオフェンシングを必須にしたりすることなどが考えられます。
- アプリの配信： XenMobile では、アプリを MDM アプリまたは MAM アプリとして配信できます。MDM アプリは XenMobile ストアに表示されます。このストアを利用することで、デバイスレベルの制限以外はアプリの制御を行うことなく、パブリックアプリまたはネイティブアプリをユーザーへ簡単に配信できます。一方、MAM モードでのアプリの配信では、アプリの配信およびアプリ自体を完全に制御できます。オンプレミスの XenMobile 環境に MDM と合わせてアプリ管理の要件も設けられている場合、通常は MAM モードでのアプリの配信が最適です。MAM モードでアプリを配信する場合は、モバイルデバイスを XME（MDM + MAM）モードまたは MAM-only モードに登録する必要があります。
- アプリケーションのメンテナンス：
  - 初期監査の実施：実稼働環境に存在するアプリのバージョン、および最新のアップグレードサイクルを常に把握しておく必要があります。アップグレードが必要になった特定の機能やバグの修正を記録します。
  - ベースラインの確立：アプリごとに、最新の安定リリースのリストを維持する必要があります。アップグレード後に予期しない問題が発生した場合、そのアプリのバージョンを戻す必要があります。また、ロールバックの計画を作成する必要もあります。アプリのアップグレードは、実稼働環境へ導入する前にテスト環境でテストする必要があります。可能であれば、まず実稼働環境の一部のユーザーにアップグレードを展開してから、次にユーザーベース全体に展開することをお勧めします。
  - Citrix のソフトウェアのアップデート通知およびサードパーティソフトウェアベンダの通知の購読：これは、アプリの最新リリースに関する最新の情報を常に把握するために重要です。早期アクセスリリース（EAR）ビルドを事前に入手し、テストできる場合もあります。
  - ユーザーへの通知の方針の作成：アプリのアップグレードが利用可能になった場合のユーザーへの通知方法を定める必要があります。展開前に、ユーザーにトレーニングを提供してください。アプリの更新前に、複数の通知を送信できます。アプリによっては、メール通知やウェブサイトで通知を行うことが最適な場合もあります。

アプリライフサイクル管理は、アプリの初期展開から廃止に至るまでのライフサイクル全体に相当します。アプリのライフサイクルは、次の 5 つの段階に分けられます。

1. 仕様要件：ビジネスケースとユーザー要件から着手します。
2. 開発：アプリがビジネスニーズを満たしていることを検証します。
3. テスト：テストユーザー、問題、バグを特定します。
4. 展開：実稼働環境のユーザーにアプリを展開します。

5. メンテナンス：アプリのバージョンを更新します。実稼働環境でアプリを更新する前に、テスト環境にアプリを展開します。

Secure Mail によるアプリケーションライフサイクルの例

1. 仕様要件：セキュリティ要件として、コンテナ化されており、MDX セキュリティポリシーをサポートするメールアプリが必要です。
2. 開発：アプリがビジネスニーズを満たしていることを検証します。MDX ポリシーコントロールをアプリに適用できる必要があります。
3. テスト：テストユーザーグループに Secure Mail を割り当て、対応する MDX ファイルを XenMobile Server から展開します。テストユーザーが、メールを問題なく送受信できること、およびカレンダーと連絡先にアクセスできることを検証します。また、問題の報告とバグの特定も行います。テストユーザーのフィードバックに基づいて、実稼働環境での使用向けに Secure Mail の設定を最適化します。
4. 展開：テスト段階が完了したら、実稼働環境ユーザーに Secure Mail を割り当て、XenMobile Server から対応する MDX ファイルを展開します。
5. メンテナンス：Secure Mail の新しい更新プログラムが利用可能になります。シトリックスのダウンロードページから新しい MDX ファイルをダウンロードし、XenMobile Server 上の既存の MDX ファイルと置き換えます。ユーザーに更新を実行するように指示します。注：アプリを XenMobile の実稼働環境へアップロードしてユーザーへ展開する前に、テスト環境でこのプロセスを実行してテストすることをお勧めします。

詳しくは、「iOS モバイルアプリのラッピング」および「Android モバイルアプリのラッピング」を参照してください。

ダッシュボードベースの操作

January 10, 2020

XenMobile コンソールのダッシュボードにアクセスすると、情報を一目で確認することができます。この情報を使用して、ウィジェットで問題や成功を速やかに確認できます。

ダッシュボードとは、XenMobile コンソールに最初にサインインすると表示される画面です。コンソールの別の場所からダッシュボードにアクセスするには、［分析］ をクリックします。ページのレイアウトを編集したり表示されるウィジェットを編集するには、ダッシュボードの ［カスタマイズ］ をクリックします。

- マイダッシュボード： 最大 4 つのダッシュボードを保存できます。ダッシュボードを個別に編集し、保存したダッシュボードを選択してそれぞれを表示することができます。
- レイアウトスタイル： この行では、ダッシュボードに表示するウィジェットの数とレイアウトを選択することができます。
- ウィジェット選択： ダッシュボードに表示する情報を選択することができます。

- 通知: 左側の数字の上のチェックボックスをオンにして、ウィジェットの上に通知バーを追加します。このバーには、準拠デバイス数、非アクティブデバイス数、24 時間以内にワイプまたは登録されたデバイス数が表示されます。
- プラットフォームごとのデバイス: プラットフォームごとの管理対象デバイス数と管理対象外デバイス数が表示されます。
- キャリアごとのデバイス: キャリアごとの管理対象デバイス数と管理対象外デバイス数が表示されます。各バーをクリックすると、プラットフォームごとの内訳が表示されます。
- プラットフォームにより管理されているデバイス: プラットフォームごとの管理対象デバイス数が表示されます。
- プラットフォームにより管理されていないデバイス: プラットフォームごとの管理対象外デバイス数が表示されます。このグラフに表示されるデバイスにはエージェントがインストールされている場合がありますが、特権が失効またはワイプされています。
- **ActiveSync** ゲートウェイ状態ごとのデバイス: ActiveSync ゲートウェイの状態ごとにグループ化されたデバイス数が表示されます。この情報では拒否、許可、または不明の状態が表示されます。各バーをクリックするとプラットフォームごとの内訳が表示されます。
- 所有権ごとのデバイス: 所有権の状態ごとにグループ化されたデバイス数が表示されます。この情報ではコーポレート所有、従業員所有、または不明の所有権状態が表示されます。
- **Android TouchDown** ライセンス状態: TouchDown ライセンスがあるデバイス数が表示されます。
- 失敗したデリバリーグループ展開: 失敗した展開の合計数がパッケージごとに表示されます。展開に失敗したパッケージのみが表示されます。
- ブロックされた理由ごとのデバイス: ActiveSync でブロックされたデバイス数が表示されます。
- インストール済みアプリ: このウィジェットを使用して、アプリ名を入力すると、グラフにはそのアプリに関する情報が表示されます。
- **VPP** アプリライセンス使用状況: Apple Volume Purchase Program アプリのライセンス使用状況に関する統計データが表示されます。

使用例

環境の監視におけるダッシュボードウィジェットの多彩な活用法の一例を次に示します。

- 業務用モバイルアプリを展開したところ、業務用モバイルアプリをデバイスにインストールできないというサポートチケットを受け取りました。［コンプライアンス外デバイス］ ウィジェットおよび ［インストール済みアプリ］ウィジェットを使用して、業務用モバイルアプリがインストールされていないデバイスを確認します。
- 非アクティブなデバイスを環境から削除してライセンスを解放できるように、こうしたデバイスを監視するとします。こうした統計情報を把握するには、［非アクティブデバイス］ウィジェットを使用します。
- データが正しく同期されないというサポートチケットを受け取りました。［**ActiveSync** ゲートウェイ状態ごとのデバイス］ ウィジェットおよび ［ブロックされた理由ごとのデバイス］ ウィジェットを使用すると、この問題に ActiveSync が関連しているかどうかを特定できます。

レポート

環境のセットアップおよびユーザーの登録後、レポートを実行すると環境に関する情報を確認できます。XenMobile には、実際の環境でのデバイスの動作状況を把握するためのレポートが多数組み込まれています。詳しくは、「レポート」を参照してください。

> 重要：
>
> カスタムレポートの作成に SQL Server を使用することは可能ですが、お勧めしません。この方法で SQL Server データベースを使用すると、お使いの XenMobile 環境で予期しない結果が生じることがあります。このレポート作成方法を実行する場合は、SQL クエリが読み取り専用アカウントで実行されるようにしてください。

役割ベースのアクセス制御と **XenMobile** のサポート

July 5, 2019

XenMobile では、役割ベースのアクセス制御（RBAC）を使用して、XenMobile コンソール、Self Help Portal、Remote Support、パブリック API などの XenMobile システム機能へのユーザーアクセスとグループアクセスを制限します。この記事では、XenMobile に組み込まれた役割について説明し、RBAC を活用した XenMobile のサポートモデルを決定するための考慮事項について説明します。

> 注：
>
> 2019 年 1 月 1 日以降の新規のお客様は、リモートサポートをご利用いただくことはできません。既存のお客様は引き続きこの製品を使用できますが、機能強化や修正プログラムは提供されません。

組み込みの役割

次の組み込みの役割に付与されたアクセス権を変更したり、役割を追加したりできます。各役割とそのデフォルト設定に関連したすべてのアクセス権と機能権限については、XenMobile のドキュメントから『Role-Based Access Control Defaults』をダウンロードしてください。各機能の定義については、XenMobile のドキュメントの「RBAC を使用した役割の構成」を参照してください。

Admin の役割

付与されるデフォルトのアクセス権：

- システムへのフルアクセス。ただし、Self Help Portal と Remote Support は除きます。
- デフォルトでは、管理者は接続の確認やサポートバンドルの作成などの一部のサポートタスクを実行できます。

注意事項：

- 管理者の一部または全員が Self Help Portal や Remote Support にアクセスする必要がありますか？その場合は、管理者の役割を編集するか、管理者の役割を追加できます。
- 一部の管理者または管理者グループのアクセスをさらに制限するには、管理者テンプレートに基づいて役割を追加し、権限を編集します。

デバイスプロビジョニング

付与されるデフォルトのアクセス権：

- Windows CE デバイスの基本的な管理を行うための XenMobile コンソールへのアクセス権。デバイスの追加、変更、および削除を行うことができます。［設定］ページを使用します。

注意事項：

- Windows CE デバイスにのみ適用されます。

サポート

付与されるデフォルトのアクセス権：

- Remote Support へのアクセス権。

注意事項：

- XenMobile Server のオンプレミス展開の場合：リモートサポートを使用すると、ヘルプデスクの担当者は管理対象の Windows CE および Android モバイルデバイスをリモートで制御できます。画面のキャストは Samsung KNOX でのみサポートされています。
- XenMobile サービスのお客様はリモートサポートを利用できません。またリモートサポートはクラスター化されたオンプレミスの XenMobile Server 展開ではサポートされていません。

ユーザー

付与されるデフォルトのアクセス権：

- Self Help Portal へのアクセス権。認証済みユーザーは登録リンクを生成できます。これらのリンクを使用して、デバイスを登録したり、登録招待状を自己送信したりできます。
- XenMobile コンソールへの制限付きアクセス権：デバイス機能（デバイスのワイプやロック/ロック解除、コンテナのロック/ロック解除、場所の参照と地理的制限の設定、デバイスの呼び出し、コンテナパスワードのリセットなど）、登録招待状の追加、削除、送信を行うことができます。

注意事項：

- ユーザー役割を使用すると、ユーザーは自分のことは自分自身でできるようになります。
- 共有デバイスをサポートするには、共有デバイス登録用のユーザー役割を作成します。

XenMobile サポートモデルに関する考慮事項

採用可能なサポートモデルは多様で、レベル 1 とレベル 2 のサポートをサードパーティが担当し、レベル 3 とレベル 4 のサポートは従業員が担当するような場合があります。サポート負荷をどのように分散させるかに関わらず、このセクションで説明する考慮事項で、ご利用の XenMobile 環境とユーザーベースに固有の点に留意してください。

ユーザーは企業所有のデバイスを持っていますか、**BYO** デバイスを持っていますか?
サポートに影響する第一の問題は、XenMobile 環境でユーザーデバイスを所有しているのが誰なのかということです。ユーザーが企業所有のデバイスを持っている場合は、デバイスをロックダウンする方法として、サポートのレベルを下げることが考えられます。その場合、デバイスの問題と使用方法に関してユーザーを支援するヘルプデスクを提供することができます。サポートが必要なデバイスのタイプに応じて、ヘルプデスクの RBAC デバイスプロビジョニングとサポートの役割をどのようにするかを検討してください。

ユーザーが BYO デバイスを持っている場合、組織ではデバイスサポートの独自の情報源をユーザー自身が探すよう期待することが考えられます。そのような場合、組織が提供するサポートは、XenMobile 固有の問題に対応する管理者の役割のようなものになります。

デスクトップのサポートモデルはどのようなものですか?
デスクトップのサポートモデルが他の企業所有デバイスに適しているかどうかを検討します。同じサポート組織を利用できますか? どのような追加トレーニングが必要ですか?

XenMobile Self Help Portal へのアクセス権をユーザーに付与しますか?
XenMobile へのアクセス権をユーザーに付与するのは好ましくないとする組織もありますが、ユーザーに自己サポートの能力を与えると、サポート組織の負荷を軽減できます。RBAC のデフォルトのユーザー役割に、付与したくない権限が含まれる場合、付与したい権限のみを含む新しい役割を作成することを検討してください。要件を満たすのに必要な数の役割を作成できます。

システムの監視

January 10, 2020

アプリケーションのアクセスと接続の最適な動作時間を確保するには、XenMobile 環境で以下のコアコンポーネントを監視する必要があります。

XenMobile サーバー

XenMobile Server はローカルストレージ上にログを生成して格納するため、システムログ（syslogs）サーバーにもエクスポートできます。サイズ制限、ログレベルを指定してログ設定を構成することも、カスタムロガーを作成して特定のイベントをフィルターすることもできます。XenMobile Server のログは、XenMobile コンソールからいつでも参照できます。また、ログ内の情報を syslog サーバー経由で、実稼働 Splunk ログサーバーにエクスポートすることもできます。

次のリストに、XenMobile で使用できるさまざまなタイプのログファイルを示します。

デバッグログファイル: エラーメッセージやサーバー関連のアクションなど、XenMobile のコア Web サービスに関するデバッグレベルの情報が含まれています。

メッセージ形式:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>
```

- <id>は、sessionID のような一意の識別子です。
- <log message>は、アプリケーションによって提供されるメッセージです。

管理監査ログファイル: XenMobile コンソール上のアクティビティについての監査情報が含まれます。

> 注:
>
> 監理監査ログとユーザー監査ログの両方で同じ形式が使用されます。

メッセージ形式:

必須の Date や Timestamp の値を除き、他のすべての属性はオプションです。オプションのフィールドは、メッセージ内では”“で表します。

```
<date> <timestamp> ”<username/id>””<sessionid>””<deviceid>””<clientip>””<action>””<status>””<application name>””<app user id>””<user agent>””<details>”
```

次の表に、使用可能な管理監査ログのイベントを示します。

イベントの管理監査ログメッセージ	ステータス
ログオン	成功/失敗
ログアウト	成功/失敗
管理者の取得	成功/失敗
管理者の更新	成功/失敗
アプリケーションの取得	成功/失敗
アプリケーションの追加	成功/失敗
アプリケーションの更新	成功/失敗
アプリケーションの削除	成功/失敗
アプリケーションのバインド	成功/失敗
アプリケーションのバインド解除	成功/失敗
アプリケーションの無効化	成功/失敗
アプリケーションの有効化	成功/失敗

イベントの管理監査ログメッセージ	ステータス
カテゴリの取得	成功/失敗
カテゴリの追加	成功/失敗
カテゴリの更新	成功/失敗
カテゴリの削除	成功/失敗
証明書の追加	成功/失敗
証明書の削除	成功/失敗
有効な証明書	成功/失敗
CSR 証明書	成功/失敗
証明書のエクスポート	成功/失敗
証明書チェーンの削除	成功/失敗
証明書チェーンの追加	成功/失敗
コネクタの取得	成功/失敗
コネクタの追加	成功/失敗
コネクタの削除	成功/失敗
コネクタの更新	成功/失敗
デバイスの取得	成功/失敗
デバイスのロック	成功/失敗
デバイスのロック解除	成功/失敗
デバイスのワイプ	成功/失敗
デバイスのワイプ解除	成功/失敗
デバイスの削除	成功/失敗
役割の取得	成功/失敗
役割の追加	成功/失敗
役割の更新	成功/失敗
役割の削除	成功/失敗
役割のバインド	成功/失敗
役割のバインド解除	成功/失敗
構成設定の更新	成功/失敗
ワークフローメールの更新	成功/失敗

イベントの管理監査ログメッセージ	ステータス
ワークフローの追加	成功/失敗
ワークフローの削除	成功/失敗
Active Directory の追加	成功/失敗
Active Directory の更新	成功/失敗
マスターユーザーリストの追加	成功/失敗
マスターユーザーリストの更新	成功/失敗
DNS の更新	成功/失敗
ネットワークの更新	成功/失敗
ログサーバーの更新	成功/失敗
ログサーバーからのログの転送	成功/失敗
syslog の更新	成功/失敗
Receiver の更新	成功/失敗
タイムサーバーの更新	成功/失敗
信頼の更新	成功/失敗
サービスレコードの追加	成功/失敗
サービスレコードの更新	成功/失敗
Receiver メールの更新	成功/失敗
パッチのアップロード	成功/失敗
スナップショットのインポート	成功/失敗
アプリストアアプリの詳細の取得	成功/失敗
MDM の更新	成功/失敗
MDM の削除	成功/失敗
HDX の追加	成功/失敗
HDX の更新	成功/失敗
HDX の削除	成功/失敗
ブランド設定の追加	成功/失敗
ブランド設定の削除	成功/失敗
SSL オフロードの更新	成功/失敗
アカウントプロパティの追加	成功/失敗

イベントの管理監査ログメッセージ	ステータス
アカウントプロパティの削除	成功/失敗
アカウントプロパティの更新	成功/失敗
ビーコンの追加	成功/失敗

ユーザー監査ログファイル： 登録されたデバイスのユーザーアクティビティに関連する情報が保存されます。

> 注:
>
> ユーザー監査ログと管理監査ログの両方で同じ形式が使用されます。

メッセージ形式:

必須の Date や Timestamp の値を除き、他のすべての属性はオプションです。オプションのフィールドは、メッセージ内では”“で表します。例:

```
<date> <timestamp> ”<username/id>””<sessionid>””<deviceid>””<clientip>”
”<action>””<status>””<application name>””<app user id>””<user agent>””<
details>”
```

次の表に、使用可能なユーザー監査ログのイベントを示します。

イベントのユーザー監査ログメッセージ	ステータス
ログオン	成功/失敗
セッションのタイムアウト	成功/失敗
サブスクライブ	成功/失敗
サブスクリプション解除	成功/失敗
事前起動	成功/失敗
AGEE SSO	成功/失敗
ShareFile 用の SAML トークン	成功/失敗
デバイス登録	成功/失敗
デバイスチェック	ロック/ワイプ
デバイス更新	成功/失敗
トークンリフレッシュ	成功/失敗
シークレット保存済	成功/失敗
シークレット取得済	成功/失敗
ユーザーによるパスワードの変更	成功/失敗

イベントのユーザー監査ログメッセージ	ステータス
モバイルクライアントのダウンロード	成功/失敗
ログアウト	成功/失敗
検出サービス	成功/失敗
エンドポイントサービス	成功/失敗

MDM 機能	ステータス
REGHIVE	成功/失敗
CAB インベントリ	成功/失敗
CAB	成功/失敗
CAB 自動インストール	成功/失敗
CAB シェルインストール	成功/失敗
CAB 作成フォルダー	成功/失敗
CAB ファイル取得	成功/失敗
ファイル作成フォルダー	成功/失敗
ファイル取得	成功/失敗
ファイル送信	成功/失敗
スクリプト作成フォルダー	成功/失敗
スクリプト取得	成功/失敗
スクリプト送信	成功/失敗
スクリプトシェル実行	成功/失敗
スクリプト自動実行	成功/失敗
APK インベントリ	成功/失敗
APK	成功/失敗
APK シェルインストール	成功/失敗
APK 自動インストール	成功/失敗
APK 作成フォルダー	成功/失敗
APK ファイル取得	成功/失敗
APK アプリ	成功/失敗

MDM 機能	ステータス
EXT アプリ	成功/失敗
リスト取得	成功/失敗
リスト送信	成功/失敗
デバイスの場所の確認	成功/失敗
CFG	成功/失敗
ロック解除	成功/失敗
SharePoint ワイプ	成功/失敗
SharePoint 構成	成功/失敗
プロファイルの削除	成功/失敗
アプリケーションの削除	成功/失敗
非管理アプリケーションの削除	成功/失敗
非管理プロファイルの削除	成功/失敗
IPA アプリ	成功/失敗
EXT アプリ	成功/失敗
引き換えコードの適用	成功/失敗
設定の適用	成功/失敗
デバイス追跡の有効化	成功/失敗
アプリ管理ポリシー	成功/失敗
SD カードワイプ	成功/失敗
暗号化されたメール添付ファイル	成功/失敗
ブランド設定	成功/失敗
Secure Browser	成功/失敗
コンテナブラウザー	成功/失敗
コンテナのロック解除	成功/失敗
コンテナのパスワードリセット	成功/失敗
AG クライアントの認証クレジット	成功/失敗

NetScaler は XenMobile Web サービスの状態も監視します。インテリジェントな監視プローブで構成され、各 XenMobile サーバークラスターノードへの HTTP 要求をシミュレートします。このプローブは、サービスがオ

ンラインであるかどうかを判別し、受信した応答に基づいて応答します。ノードが想定どおりに応答しない場合、NetScaler はサーバーを停止状態としてマークします。さらに、NetScaler はノードを負荷分散プールから取り出し、NetScaler の監視ソリューションを介してアラートを生成するのに使用するイベントを記録します。

また、標準のハイパーバイザー監視ツールを使用して、XenMobile 仮想マシンを監視したり、CPU、メモリ、およびストレージ使用率メトリックに関連するアラートを出したりすることもできます。

SQL Server とデータベース

SQL Server とデータベースのパフォーマンスは、XenMobile サービスに直接影響します。XenMobile インスタンスは、データベースへの常時アクセスが必要で、SQL インフラストラクチャが停止した場合にはオフラインになります（たとえば、応答を停止するなど）。XenMobile コンソールは、SQL Server にディスクスペースの問題が発生した後も、しばらくの間は機能し続けることがあります。データベースの稼働時間を最大限に保ち、XenMobile ワークロードの適切なパフォーマンスを確保するには、Microsoft が推奨する内容に従って SQL Server の状態を積極的に監視する必要があります。また、XenMobile 環境の拡大に合わせて、CPU、メモリ、ストレージのリソース割り当てを調整し、サービスレベルアグリーメントを保証する必要があります。

NetScaler

NetScaler には、内部ストレージにメトリックを記録したり、ログを外部ログサーバーに送信する機能があります。NetScaler ログを実稼働環境用の Splunk ログサーバーにエクスポートするように syslog サーバーを構成できます。NetScaler では、次のログレベルが利用できます。

- 緊急
- アラート
- 重大
- エラー
- 警告
- 情報

ログファイルは、/var/log/ns.log ディレクトリ内の NetScaler ストレージにも格納され、newnslog という名前が付けられます。NetScaler は GZIP アルゴリズムを使用してファイルをロールオーバーし、圧縮します。ログファイル名は newnslog.xx.gz です（xx は連番を表します）。

NetScaler は、監視オプションとして SNMP トラップおよびアラートもサポートしています。SNMP トラップのリストについて詳しくは、「SNMP の監視」を参照してください。

障害回復

August 22, 2019

アクティブ/パッシブフェイルオーバー戦略を使用して複数サイトの障害回復を含めた XenMobile 展開環境を構築し、構成できます。

この記事で説明する推奨障害回復戦略は次のとおりです:

- 地理的に 1 つの場所のデータセンターにある単一のアクティブな XenMobile サイト。すべての企業ユーザーにグローバルに提供され、プライマリサイトと呼ばれます。
- 第 2 の地理的な場所のデータセンターにある第 2 の XenMobile サイト。障害回復サイトと呼ばれます。この障害回復サイトは、プライマリサイトでサイト全体のデータセンターの障害が発生した場合にアクティブ/パッシブサイトフェールオーバーを提供します。プライマリサイトには、XenMobile、SQL データベース、NetScaler インフラストラクチャが含まれており、フェールオーバーを容易にし、プライマリサイトへの接続に失敗した場合に XenMobile へのアクセスをユーザーに提供します。

障害回復サイトの XenMobile サーバーは、通常の運用中はオフラインのままで、プライマリサイトから障害回復サイトへの完全なサイトフェールオーバーが必要な障害回復シナリオのみでオンラインになります。障害回復サイトの SQL Server は、アクティブで、障害回復サイトで XenMobile サーバーを起動する前に接続を処理する準備ができている必要があります。

この障害回復戦略は、停止時に MDM および MAM 接続を障害回復サイトにルーティングするための DNS 変更による NetScaler アクセス層の手動フェールオーバーに依存しています。

> 注:
>
> このアーキテクチャを使用するには、データベースの非同期バックアップと SQL インフラストラクチャの高可用性を確保するためのプロセスが必要です。

障害回復フェールオーバープロセス

1. 障害回復フェールオーバープロセスをテストする場合は、プライマリサイトの XenMobile サーバーをシャットダウンしてサイトの障害をシミュレートします。
2. 障害回復サイトの外部 IP アドレスを参照するように、XenMobile サーバーの公開 DNS レコードを変更します。
3. 障害回復サイトの SQL Server IP アドレスを参照するように、SQL Server の内部 DNS レコードを変更します。
4. 障害回復サイトで XenMobile SQL データベースをオンラインにします。SQL Server とデータベースがアクティブで、サイトのローカル XenMobile サーバーからの接続を処理できる状態になっていることを確認します。
5. 障害回復サイトの XenMobile サーバーの電源を入れます。

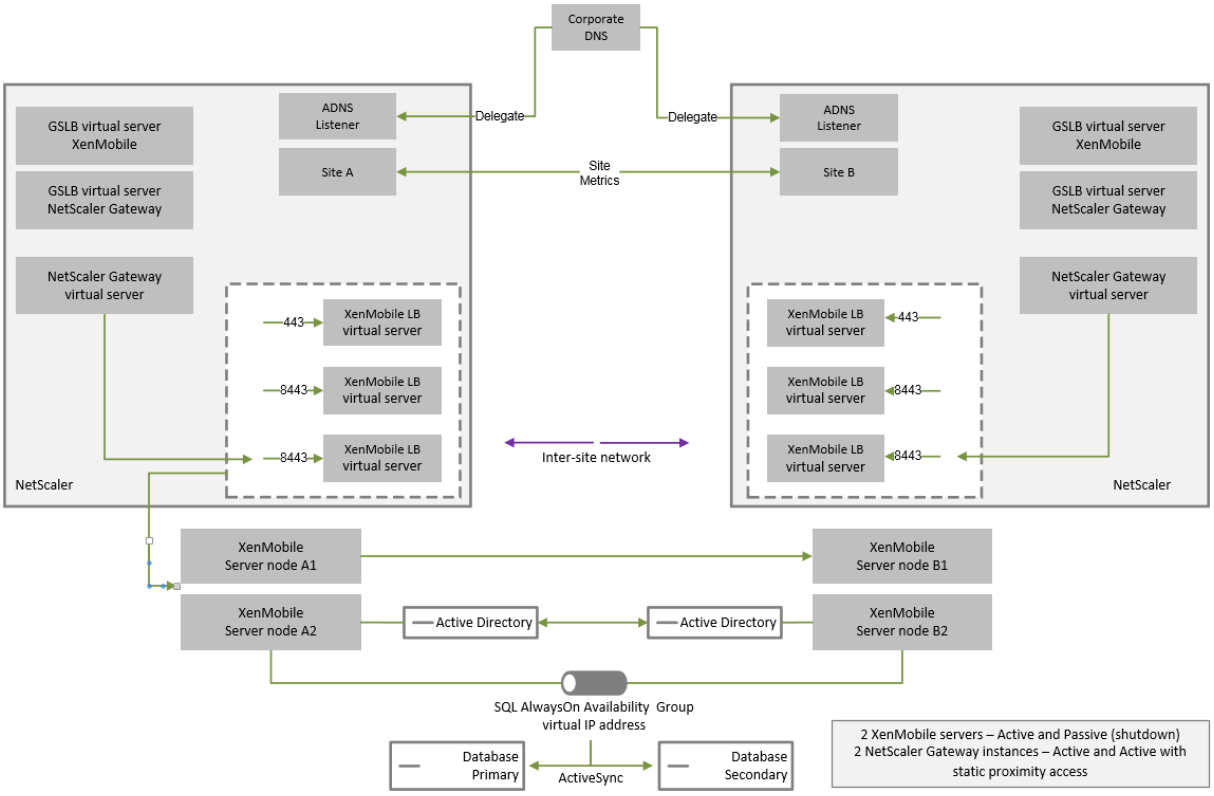
XenMobile サーバー更新プロセス

プライマリサーバーと障害回復サーバーのコードを統一するために、XenMobile をパッチおよびリリースで更新するたびに、次の手順を実行します。

1. プライマリサイトの XenMobile サーバーがパッチ適用またはアップグレードされていることを確認します。
2. SQL Server の DNS レコードがプライマリサイトのアクティブな SQL Server データベースに解決されていることを確認します。
3. 障害回復サイトの XenMobile サーバーをオンラインにします。サーバーは、アップグレード処理時にのみ WAN を介してプライマリサイトのデータベースに接続します。
4. すべての障害回復サイトの XenMobile サーバーに必要なパッチおよびアップデートを適用します。
5. XenMobile サーバーを再起動し、パッチまたはアップグレードが成功したことを確認します。

障害回復リファレンスアーキテクチャの図

次の図は、XenMobile の障害回復環境のハイレベルアーキテクチャを示しています。



障害回復の **GSLB**

このアーキテクチャの重要な要素は、GSLB（Global Server Load Balancing）を使用してトラフィックを正しいデータセンターに誘導することです。

デフォルトでは、NetScaler for XenMobile ウィザードは、障害回復に GSLB を使用できないように NetScaler Gateway を設定します。したがって、追加の手順を実行する必要があります。

GSLB のしくみ

GSLB は DNS の中核部にあります。参加する NetScaler アプライアンスは権限のある DNS サーバーとして機能し、DNS レコードを正しい IP アドレス（通常はトラフィックを受信するはずの VIP）に解決します。NetScaler アプライアンスは、そのシステムへのトラフィックを誘導する DNS クエリに応答する前に、システムの健全性をチェックします。

レコードが解決されると、トラフィックを解決する GSLB の役割は完了です。クライアントは、ターゲット仮想 IP (VIP）アドレスと直接通信します。DNS クライアントの動作は、レコードがいつどのように期限切れになるかに重要な役割を果たします。これは大部分 NetScaler システムの範囲外です。そのため、GSLB には DNS 名前解決と同じ制限があります。クライアントは応答をキャッシュします。したがって、このような負荷分散には、従来の負荷分散ほどのリアルタイム性はありません。

サイト、サービス、およびモニターなど、NetScaler の GSLB 設定は、正しい DNS 名前解決を提供するために存在します。

サーバーを公開するための実際の設定（このシナリオでは、NetScaler for XenMobile ウィザードが作成する設定）は、GSLB の影響を受けません。GSLB は NetScaler 上の別個のサービスです。

GSLB を XenMobile で使用する場合のドメイン委任の課題

NetScaler for XenMobile ウィザードは、NetScaler Gateway for XenMobile を設定します。このウィザードは、3 つの負荷分散仮想サーバーと NetScaler Gateway 仮想サーバーを生成します。

負荷分散仮想サーバーのうち 2 つは、ポート 443 と 8443 で MDM トラフィックを処理します。NetScaler Gateway はポート 8443 で MAM トラフィックを受信し、第 3 のサーバーである MAM 負荷分散仮想サーバに転送します。MAM 負荷分散仮想サーバーへのトラフィックはすべて NetScaler Gateway を通過します。

MAM 負荷分散仮想サーバーには XenMobile サーバーと同じ SSL 証明書が必要で、デバイスの登録に使用されたものと同じ FQDN が使用されます。MAM 負荷分散サーバーは、MDM 負荷分散サーバーの 1 つと同じポート（8443）も使用します。トラフィックを解決するには、NetScaler for XenMobile ウィザードを使用して、NetScaler Gateway にローカル DNS レコードを作成します。DNS レコードは、デバイスの登録に使用された FQDN と一致します。

この設定は、XenMobile サーバーの URL が GSLB ドメインサーバーの URL でない場合に有効です。障害回復には GSLB ドメインの URL を XenMobile サーバーの URL として使用することが必要ですが、その場合、ローカル DNS レコードが、NetScaler Gateway による MDM 負荷分散サーバーへのトラフィック解決を妨げます。

GSLB 障害回復での CNAME メソッドの使用

NetScaler for XenMobile ウィザードで作成されたデフォルト設定の問題を解決するには、親ドメイン（company.com）に XenMobile サーバーの FQDN に対応する CNAME レコードを作成し、NetScaler が認証されている委任済みサブゾーン（gslb.company.com）のレコードを参照します。これにより、トラフィックを解決するために必要な MAM 負荷分散 VIP アドレス用の静的 DNS A レコードを作成できます。

1. 外部 DNS で、NetScaler GSLB 上の GSLB ドメイン FQDN を参照する XenMobile サーバー FQDN の CNAME を作成します。次の 2 つの GSLB ドメインが必要です: 1 つは MDM トラフィック用、もう 1 つは MAM（NetScaler Gateway）トラフィック用。

   例:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. 各サイトの NetScaler Gateway インスタンスで、CNAME レコードが参照する FQDN を持つ GSLB 仮想サーバーを作成します。

   例:

   ```
   bind gslb vserver xms-gslb -domainName xms.gslb.company.com
   ```

   NetScaler for XenMobile ウィザードを使用して NetScaler Gateway を展開する場合は、MAM 負荷分散サーバーを設定するときに XenMobile サーバーの URL を使用します。これにより、XenMobile サーバーの URL に対応する静的 DNS A レコードが作成されます。

3. XenMobile サーバー URL（`xms.company.com`）を使用して、Secure Hub に登録しているクライアントでテストします。

   この例では、次の FQDN を使用します:

   - `xms.company.com`は MDM トラフィックによって使用される URL で、登録されているデバイスで使用されます。この例では、NetScaler for XenMobile ウィザードを使用して設定されています。
   - `xms.gslb.company.com`は XenMobile サーバーの GSLB ドメイン FQDN です。

Citrix のサポートプロセス

September 24, 2019

シトリックス製品に関する問題の解決には、Citrix Technical Support Services を利用できます。このサポートグループでは、回避策と解決策を提示しているほか、開発チームと連携してソリューションの提供も行っています。

Citrix Consulting Services と Citrix Education Services では、製品のトレーニング、製品の使用や構成、インストール、環境設計およびアーキテクチャに関連する支援をそれぞれご用意しています。

Citrix Consulting Services では、概念実証、経済効果の評価、インフラストラクチャの状態検査、設計要件の分析、アーキテクチャ設計の検証、統合、運用プロセスの開発など、シトリックス製品に関連するプロジェクトのサポートを行っています。

Citrix Education Services では、シトリックスの仮想化、クラウド、ネットワーキング技術に関する最高レベルの IT トレーニングと認定試験を提供しています。

サポートケースを作成する前に、シトリックスのセルフヘルプリソースと推奨事項を十分に活用することをお勧めします。たとえば、シトリックスの技術専門家が作成した記事や掲示板にアクセスしたり、シトリックスのソリューシ

ョンおよびテクノロジに関する製品ドキュメントを参照したり、シトリックスの役員、製品チーム、技術専門家からの率直な意見を読んだりすることができます。Knowledge Center、製品ドキュメント、およびブログの各ページをそれぞれ参照してください。

よりインタラクティブな支援が必要な場合には、各種ディスカッションフォーラムに参加してください。他のユーザーに質問をして実世界に即した答えを得たり、ユーザーグループや対象グループ内でアイデア、意見、技術情報、ベストプラクティスを共有したりすることができます。また、シトリックスサポートのソーシャルネットワーキングサイトをチェックしているシトリックスサポートのエンジニアと対話することもできます。サポートフォーラム、Citrix コミュニティ、およびTwitter の Citrix サポートの各ページをそれぞれ参照してください。

また、トレーニングおよび認定コースを受けて、スキルを磨くことも可能です。Citrix Educationを参照してください。

Citrix Insight Services では、Citrix 環境向けにシンプルなトラブルシューティングプラットフォームとヘルスチェッカーをオンラインで提供しています。XenMobile、Citrix Virtual Apps and Desktops、Citrix Hypervisor、Citrix Gateway で利用できます。分析ツールを参照してください。

テクニカルサポートを受けるには、電話か Web 経由でサポートケースを作成します。重要度が低および中程度の問題には Web で、重要度の高い問題の場合は電話でご連絡ください。XenMobile の問題に対するサポートを受ける方法について詳しくは、「How to Contact Support（サポートへの連絡方法）」を参照してください。

Citrix Services には、Citrix ソリューションを長年にわたり提供してきた経験を持ち、高度なトレーニングを受けた総合担当者として、テクニカルリレーションシップマネージャーも在籍しています。Citrix Services の提供サービスとメリットについて詳しくは、『Citrix Worldwide Services』を参照してください。

XenMobile でのグループ登録招待状の送信

May 21, 2019

寄稿者：John Bartel III

XenMobile でグループに登録招待状を送信できます。ネストされたグループにも招待状を送信できます。グループ招待状を設定するときは、1 つまたは複数のデバイスプラットフォームを指定できます。企業所有のデバイスと従業員が所有するデバイスを区別できるように、デバイスにタグを付けることもできます。次に、ユーザーデバイスの認証の種類を設定します。

> 注：
>
> カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「通知テンプレートの作成および更新」を参照してください。

ユーザーアカウント、役割、および登録モードと招待状の基本的な構成の詳細については、「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。

一般的な手順

1. XenMobile コンソールで、［管理］**>**［登録招待］ に移動します。
2. 画面の左上にある ［追加］ をクリックし、［招待の追加］ をクリックします。
3. ［宛先］ メニューの ［グループ］ をクリックします。

   このステップでは、1 つまたは複数のプラットフォームを選択できます。社内に異なるオペレーティングシステムプラットフォームが混在している場合は、すべてのプラットフォームを選択します。特定のプラットフォームを使用するユーザーがいないことがわかっている場合は、そのプラットフォームの選択をオフにします。
4. 招待プロセス中にデバイスにタグを付けるように選択できます。［コーポレート］ または ［従業員］ を選択します。

   タグ付けにより、企業所有のデバイスと従業員所有のデバイスを簡単に区別することができます。
5. ［ドメイン］ 一覧で、グループが存在するドメインを選択します。
6. ［グループ］ 一覧で、招待状を送信する Active Directory グループを選択します。
7. ［登録モード］ では、ユーザーに対する認証の種類を設定できます。

   - ユーザー名およびパスワード
   - 高セキュリティ
   - 招待 URL
   - 招待 URL および PIN
   - 招待 URL およびパスワード
   - 2 要素
   - ユーザー名および PIN
8. エージェントダウンロード、登録用 **URL**、登録 **PIN**、および 登録確認用テンプレートでは、過去に作成したカスタムの通知テンプレートを選択します。または、一覧に記載されているデフォルトを選択します。

   カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「通知」を参照してください。

   これらの通知テンプレートでは、XenMobile 内で構成した SMTP サーバー設定を使用します。続行する前にまず SMTP 情報を設定してください。

   > 注:
   >
   > ［有効期限］ および ［最大試行数］ のオプションは、選択した ［登録モード］ オプションに基づいて変更されます。ユーザーはこれらのオプションを変更できません。
9. ［招待状を送信］ で［オン］を選択し、［保存］および［送信］ をクリックしてプロセスを完了します。

ネストされたグループのサポート

ネストされたグループを使用して招待状を送信できます。通常、ネストされたグループは、同じ権限を持つグループが互いにバインドされている大規模な環境で使用されます。

［設定］**>**［**LDAP**］ に移動し、**[**ネストされたグループをサポートする］ オプションを有効にします。

トラブルシューティングと既知の制限事項

問題： Active Directory グループから削除したユーザーにも招待状が送信されます。

解決策： Active Directory 環境の規模によっては、変更がすべてのサーバーに反映されるまでに最大 6 時間かかることがあります。ユーザーまたはネストされたグループが最近削除された場合、XenMobile では引き続きこのユーザーがグループの一部と見なされる可能性があります。

このため、グループに別のグループへの招待状を送信する前に、最大 6 時間待つことをお勧めします。

オンプレミスのデバイス正常性構成証明（**DHA**）サーバーの構成

August 22, 2019

寄稿者：Sanket Mishra

オンプレミスの Windows サーバーから、Windows 10 モバイルデバイスのデバイス正常性構成証明（DHA）を有効化できます。オンプレミスで DHA を有効にするには、まず DHA サーバーを構成します。

DHA サーバーを構成したら、XenMobile Server ポリシーを作成してオンプレミスの DHA サービスを有効にします。このポリシーの作成については、「デバイス正常性構成証明デバイスポリシー」を参照してください。

DHA サーバーの前提条件

- Windows Server の Technical Preview 5 以降が［デスクトップエクスペリエンス］のインストールオプションを使用してインストールされ、実行されているサーバー。
- 1 台以上の Windows 10 クライアントデバイス。これらのデバイスには、最新バージョンの Windows を実行する TPM 1.2 または 2.0 が搭載されている必要があります。
- 以下の証明書：
  - **DHA SSL** 証明書。エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 SSL 証明書です。この証明書により、サーバー間（DHA サービスと MDM サーバー）およびサーバーとクライアント間（DHA サービスと Windows 10 デバイス）を含めて、DHA のデータ通信が保護されます。

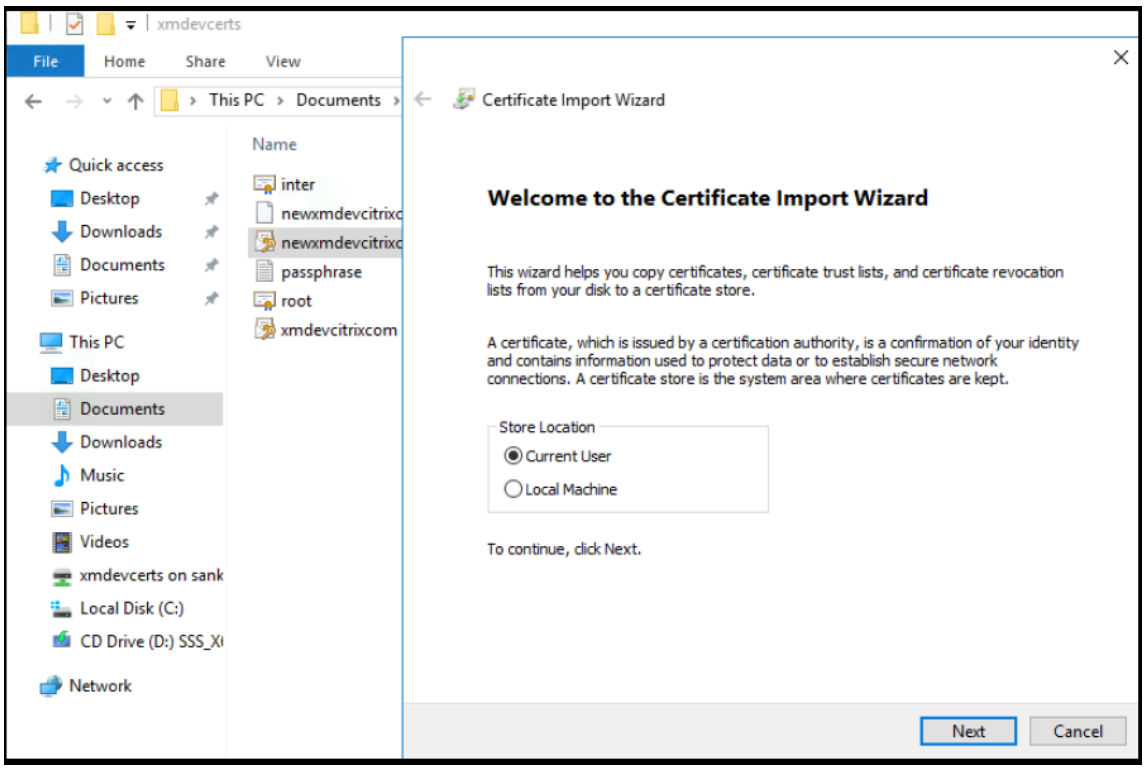
  - **DHA** 署名証明書。エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 証明書です。DHA サービスでは、この証明書を使用してデジタル署名を行います。
  - **DHA** 暗号化証明書。エクスポート可能な秘密キーを使用して、エンタープライズの信頼されたルートにチェーンされている x.509 証明書です。DHA サービスでは、この証明書を暗号化にも使用します。
- 次のいずれかの証明書検証モードを選択します。
  - **EKCert**。EKCert 検証モードは、インターネットに接続されていない組織のデバイス向けに最適化されています。EKCert 検証モードで実行されている DHA サービスに接続する場合、デバイスはインターネットに直接アクセスすることはありません。
  - **AIKCert**。AIKCert 検証モードは、インターネットにアクセス可能な運用環境向けに最適化されています。AIKCert 検証モードで実行されている DHA サービスに接続する場合、デバイスはインターネットに直接アクセスする必要があり、Microsoft から AIK 証明書を取得できます。

Windows サーバーに **DHA** サーバーの役割を追加する

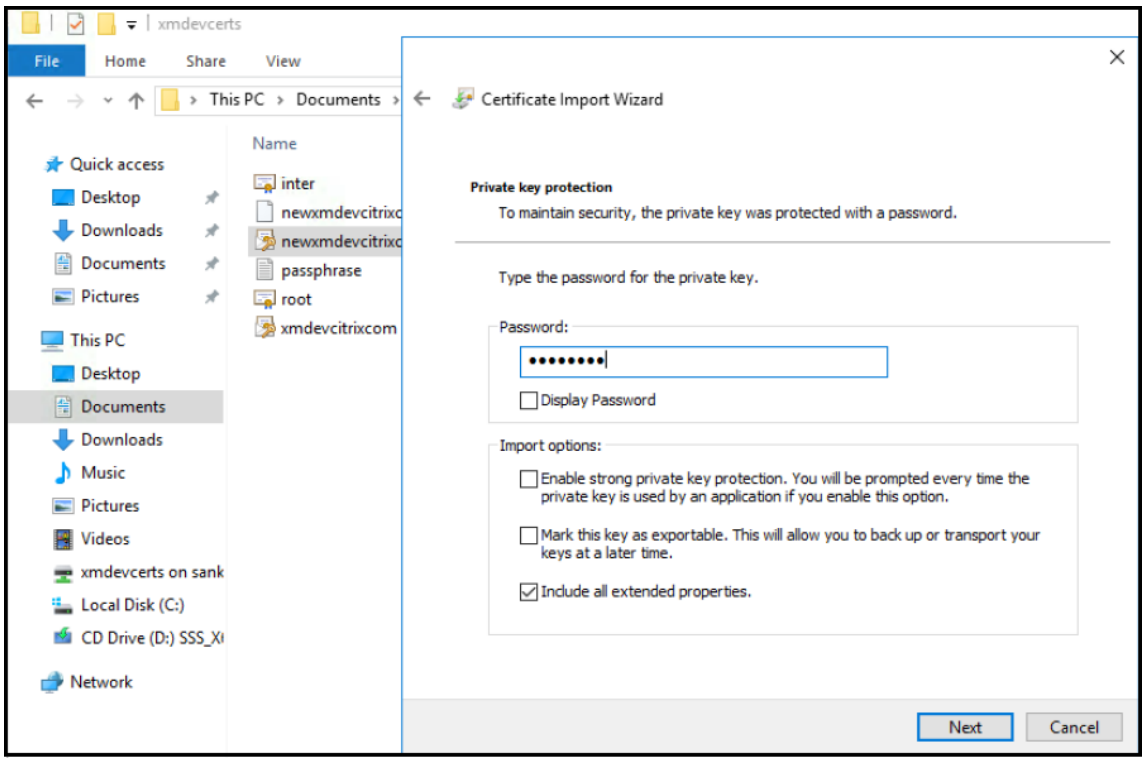
1. Windows サーバーで、サーバーマネージャーがまだ開かれていない場合は、［スタート］、［サーバーマネージャー］ の順にクリックします。
2. ［役割と機能の追加］ をクリックします。
3. ［始める前に］ ページで ［次へ］ をクリックします。
4. ［インストールの種類の選択］ ページで、［役割ベースまたは機能ベースのインストール］ をクリックして、［次へ］ をクリックします。
5. ［対象サーバーの選択］ ページで、［サーバープールからサーバーを選択］ をクリックして、［次へ］ をクリックします。
6. ［サーバーの役割の選択］ ページで、［デバイス正常性構成証明］ チェックボックスをオンにします。
7. オプション: ［機能の追加］ をクリックして、その他の必要な役割サービスと機能をインストールします。
8. ［次へ］ をクリックします。
9. ［機能の選択］ ページで、［次へ］ をクリックします。
10. ［**Web** サーバーの役割（**IIS**）］ ページで、［次へ］ をクリックします。
11. ［役割サービスの選択］ ページで、［次へ］ をクリックします。
12. ［デバイス正常性構成証明サービス］ ページで、［次へ］ をクリックします。
13. ［インストールオプションの確認］ ページで、［インストール］ をクリックします。
14. インストールが完了したら、［閉じる］ をクリックします。

サーバーの証明書ストアに **SSL** 証明書を追加する

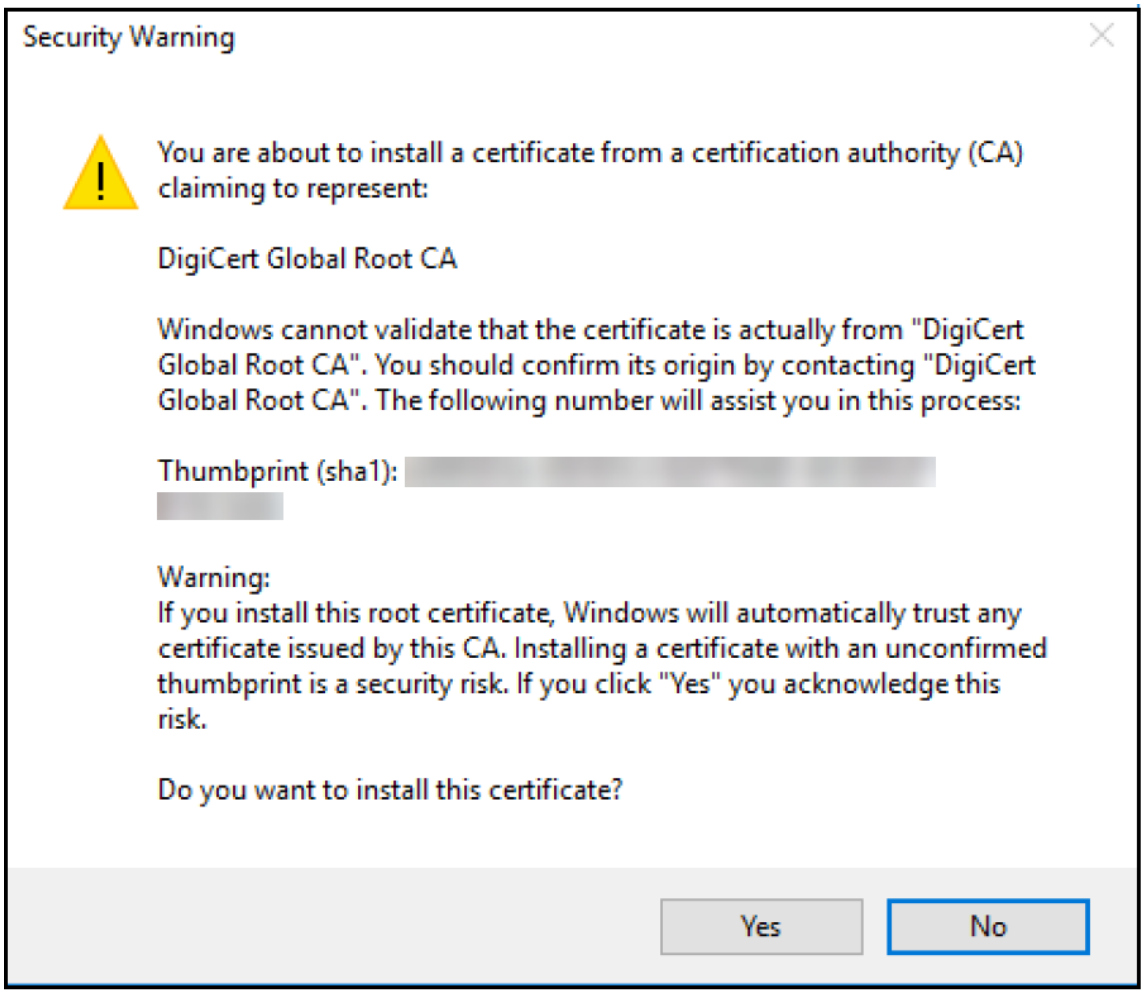
1. SSL 証明書ファイルの場所に移動して選択します。
2. ストアの保存場所として ［現在のユーザー］ を選択し、［次へ］ をクリックします。



3. 秘密キーのパスワードを入力します。
4. ［すべての拡張プロパティを含める］ インポートオプションが選択されていることを確認します。［次へ］ をクリックします。



5. 以下のウィンドウが表示されたら、［はい］ をクリックします。



6. 証明書がインストールされたことを確認します。

   a) ［コマンドプロンプト］ウィンドウを開きます。

   b) 「**mmc**」と入力して Enter キーを押します。ローカルマシンのストア内の証明書を表示するには、管理者の役割に属している必要があります。

   c) ［ファイル］メニューで、［スナップインの追加と削除］ をクリックします。

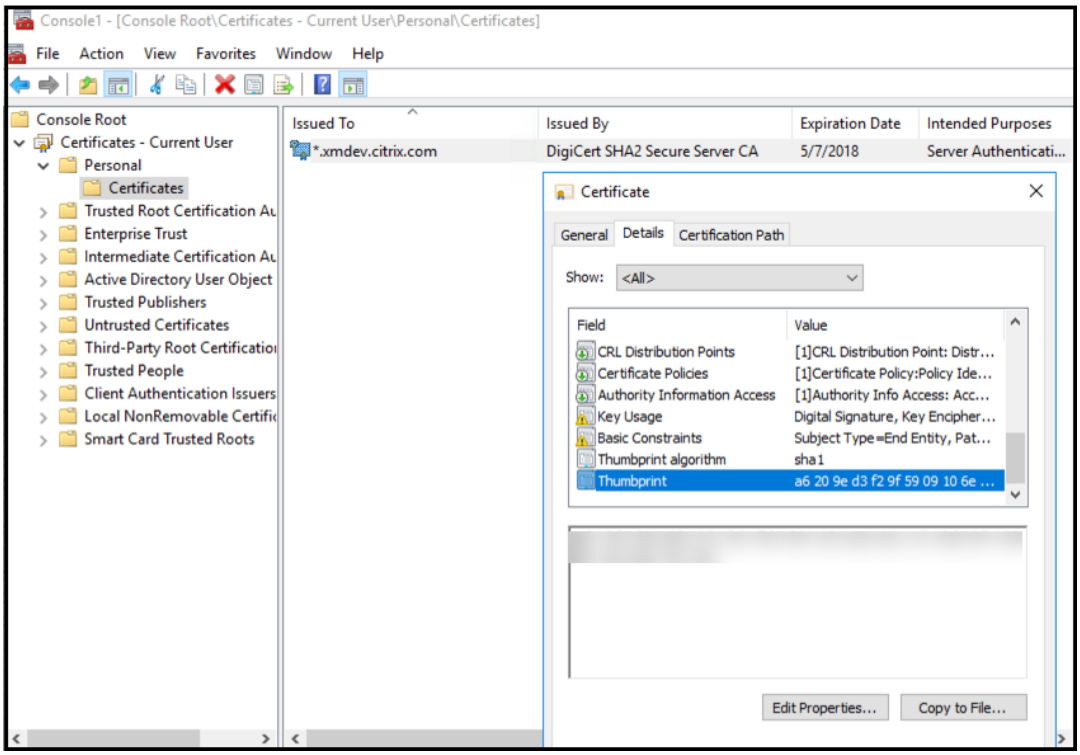
   d) ［追加］ をクリックします。

   e) ［スタンドアロンスナップインの追加］ダイアログボックスで、［証明書］ を選択します。

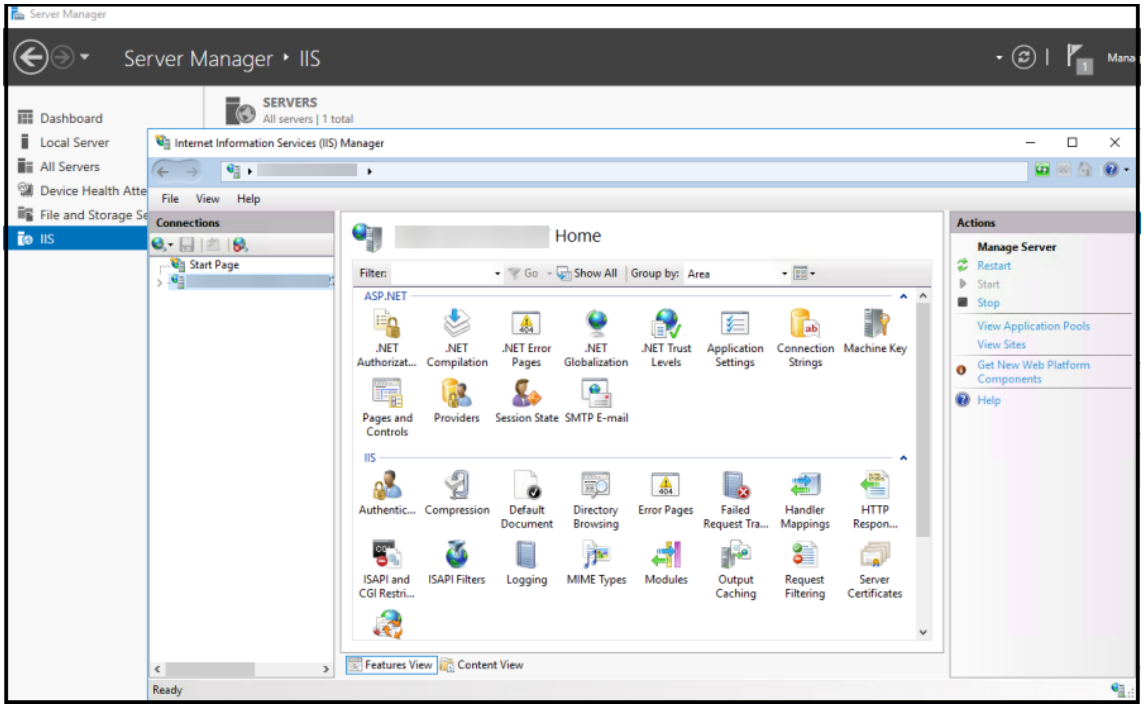
   f) ［追加］ をクリックします。

   g) ［証明書スナップイン］ダイアログボックスで、［ユーザーアカウント］ を選択します（サービスアカウント所有者としてログインしている場合は、［サービスアカウント］ を選択します）。

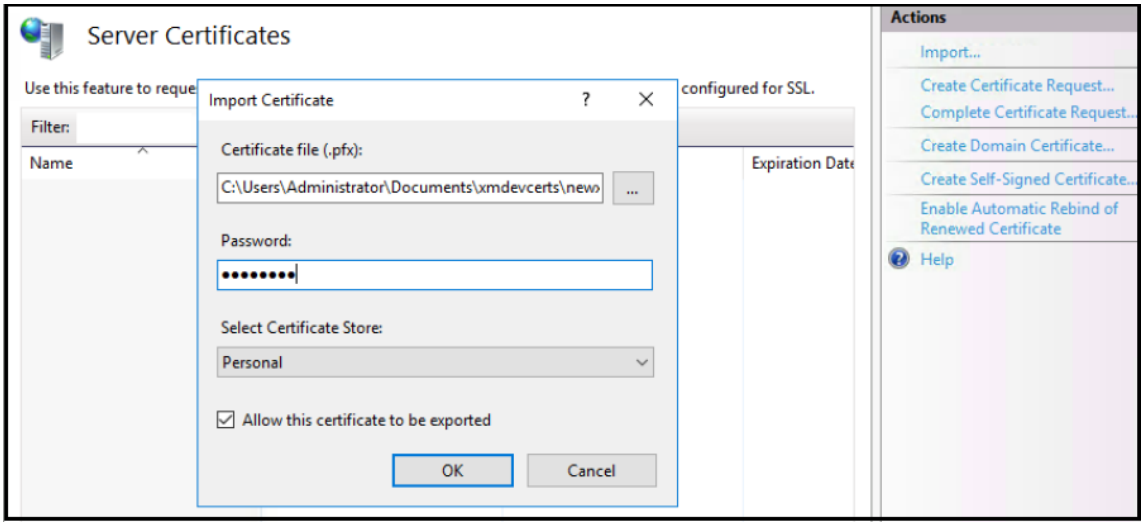
   h) ［コンピュータの選択］ダイアログボックスで、［完了］をクリックします。



7. [サーバーマネージャ] > [**IIS**] の順に選択し、アイコンの一覧で [サーバー証明書] を選択します。

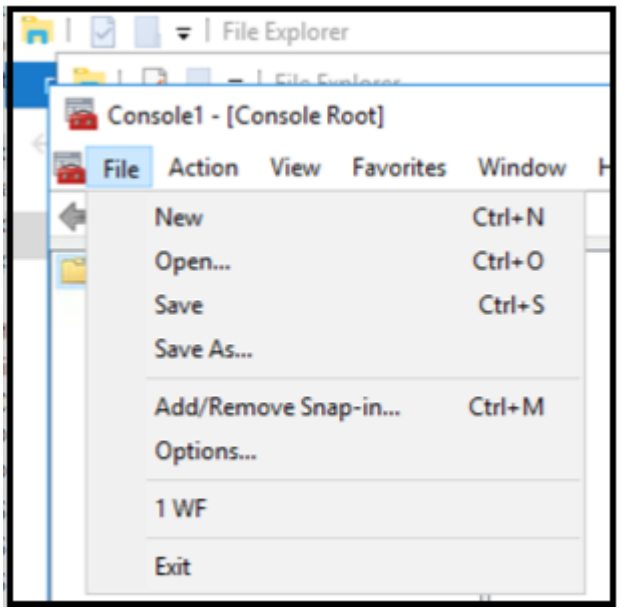


8. [アクション] メニューで [インポート**...**] を選択して、SSL 証明書をインポートします。

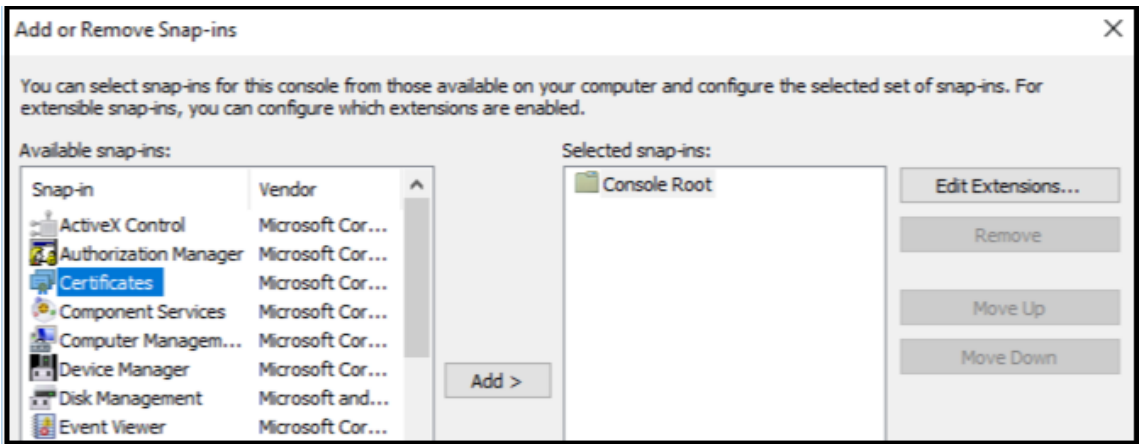


証明書の拇印を取得して保存する

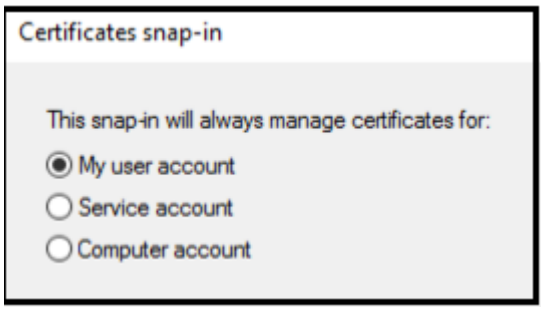
1. ファイルエクスプローラーの検索バーに「**mmc**」と入力します。
2. ［コンソールルート］ウィンドウで、［ファイル］**>**［スナップインの追加と削除］ の順にクリックします。



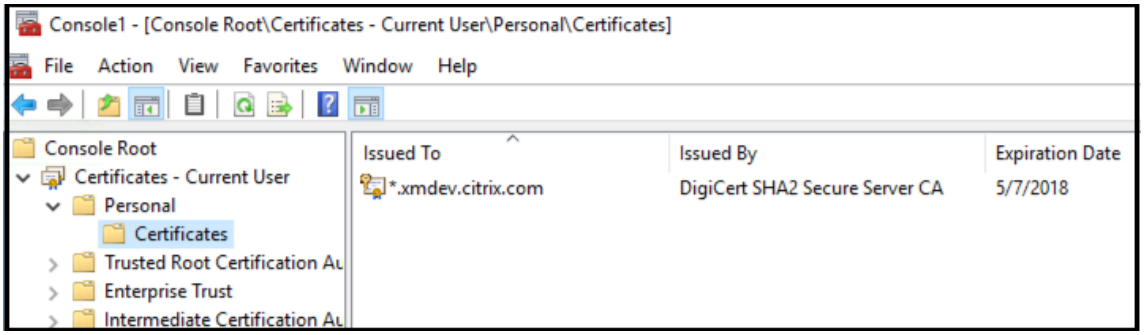
3. ［利用できるスナップイン］で［証明書］を選択し、［選択されたスナップイン］に追加します。



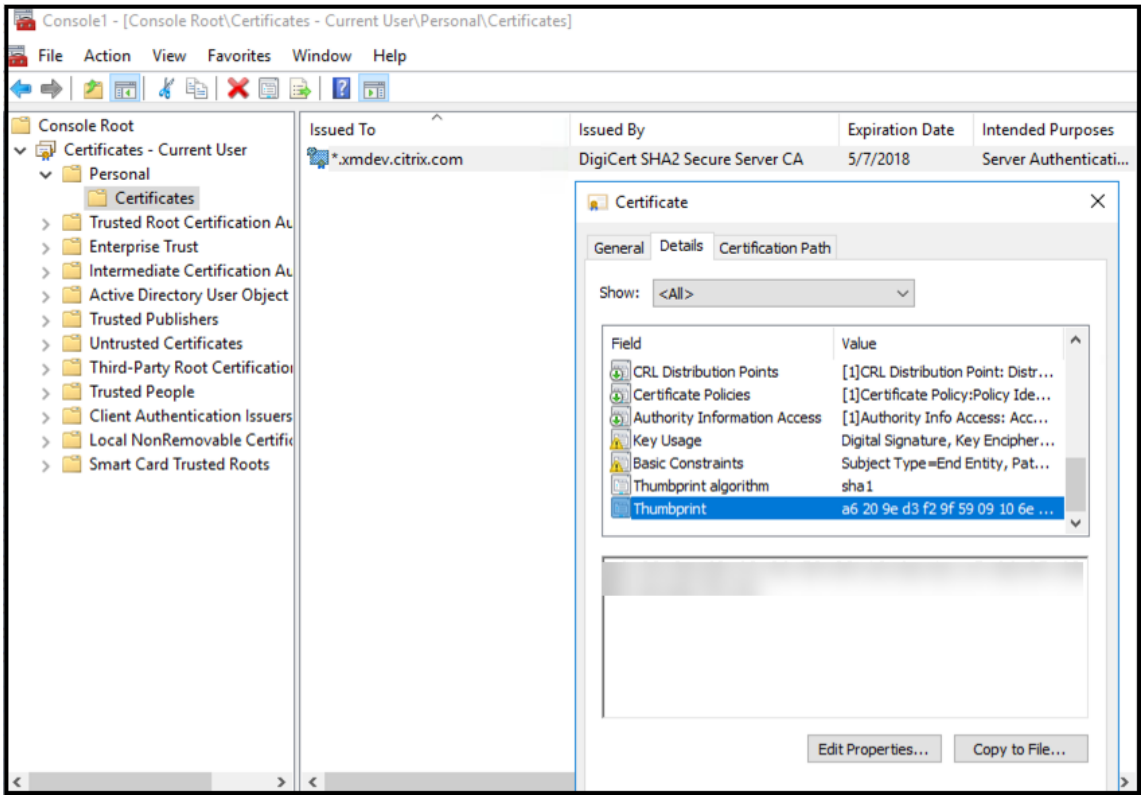
4. [ユーザーアカウント] を選択します。



5. 証明書を選択し、 [**OK**] をクリックします。



6. 証明書をダブルクリックして、 [詳細] タブをクリックします。下方向にスクロールして、証明書の拇印を表示します。



7. 拇印をファイルにコピーします。PowerShell コマンドで拇印を使用する場合は、スペースを削除します。

署名証明書と暗号化証明書をインストールする

以下の PowerShell コマンドを Windows サーバーで実行して、署名証明書と暗号化証明書をインストールします。

プレースホルダー ReplaceWithThumbprint を置き換えて、下に示すように二重引用符で囲みます。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
 $_.Thumbprint -like ”ReplaceWithThumbprint” }


$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + ”\Microsoft\Crypto\RSA\MachineKeys” +
   $keyname icacls $keypath /grant IIS_IUSRS‘:R
```

TPM ルート証明書を抽出し、信頼できる証明書パッケージをインストールする

以下のコマンドを Windows サーバーで実行します。

```
mkdir .\TrustedTpm
```



```
2
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
```

DHA サービスを構成する

Windows サーバー上で次のコマンドを実行して、DHA サービスを構成します。

プレースホルダー ReplaceWithThumbprint を置き換えます。

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
     ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
     ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
```

以下のコマンドを Windows サーバーで実行して、DHA サービスの証明書チェーンポリシーを設定します。

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

以下のようにプロンプトに回答します。

```
1   Confirm
2
3     Are you sure you want to perform this action?
4
5     Performing the operation "Install-DeviceHealthAttestation" on
         target "WIN-N27D1FKCEBT".
6
7     [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?]
         Help (default is "Y"): A
8
9     Adding SSL binding to website 'Default Web Site'.
```



```
10
11      Add SSL binding?
12
13      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15      Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17      Add application pool?
18
19      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21      Adding web application 'DeviceHealthAttestation' to website '
           Default Web Site'.
22
23      Add web application?
24
25      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27      Adding firewall rule 'Device Health Attestation Service' to allow
           inbound connections on port(s) '443'.
28
29      Add firewall rule?
30
31      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33      Setting initial configuration for Device Health Attestation Service
           .
34
35      Set initial configuration?
36
37      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39      Registering User Access Logging.
40
41      Register User Access Logging?
42
43      [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

構成を確認する

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーで次のコマンドを実行します。

```
Get-DHASActiveSigningCertificate
```


証明書がアクティブな場合、証明書の種類（署名）と拇印が表示されます。

DHASActiveSigningCertificate がアクティブであるかどうかを確認するには、サーバーで次のコマンドを実行します。

プレースホルダー ReplaceWithThumbprint を置き換えて、下に示すように二重引用符で囲みます。

```
Set-DHASActiveEncryptionCertificate -Thumbprint ”ReplaceWithThumbprint”
    -Force

Get-DHASActiveEncryptionCertificate
```

証明書がアクティブな場合、拇印が表示されます。

最終チェックを行うには、次の URL にアクセスします。

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

DHA サービスが実行されている場合は、「メソッドは許可されていません」と表示されます。

Secure Mail のプッシュ通知用に EWS で証明書ベースの認証を構成する

May 21, 2019

寄稿者: Vijay Kumar Kunchakuri

Secure Mail のプッシュ通知が確実に動作するようにするには、証明書ベースの認証用に Exchange Server を構成する必要があります。証明書ベースの認証で Secure Hub を XenMobile に登録する場合には、この要件が特に必要です。

Exchange メールサーバーの Active Sync および Exchange Web サービス（EWS）仮想ディレクトリで、証明書ベースの認証を構成する必要があります。

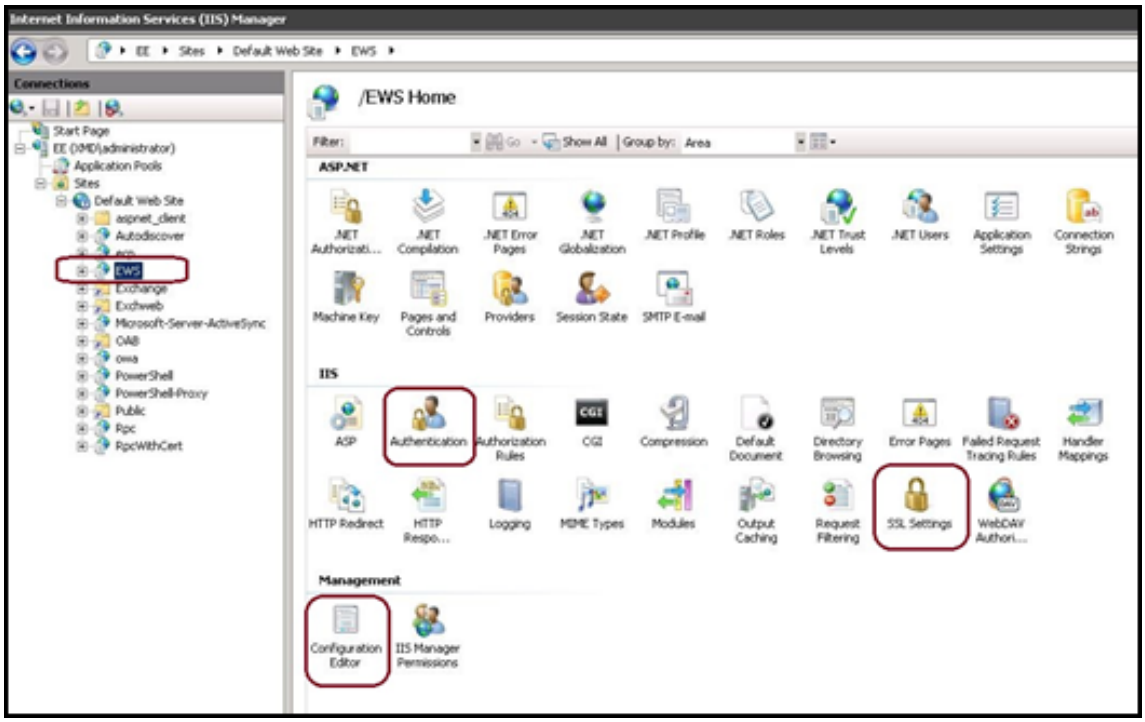
これらの構成を完了しないと、Secure Mail のプッシュ通知へのサブスクリプションが失敗するほか、Secure Mail でバッジの更新が行われません。

この記事では、証明書ベースの認証を構成する手順について説明します。この構成は、特に Exchange Server の EWS 仮想ディレクトリに対するものです。

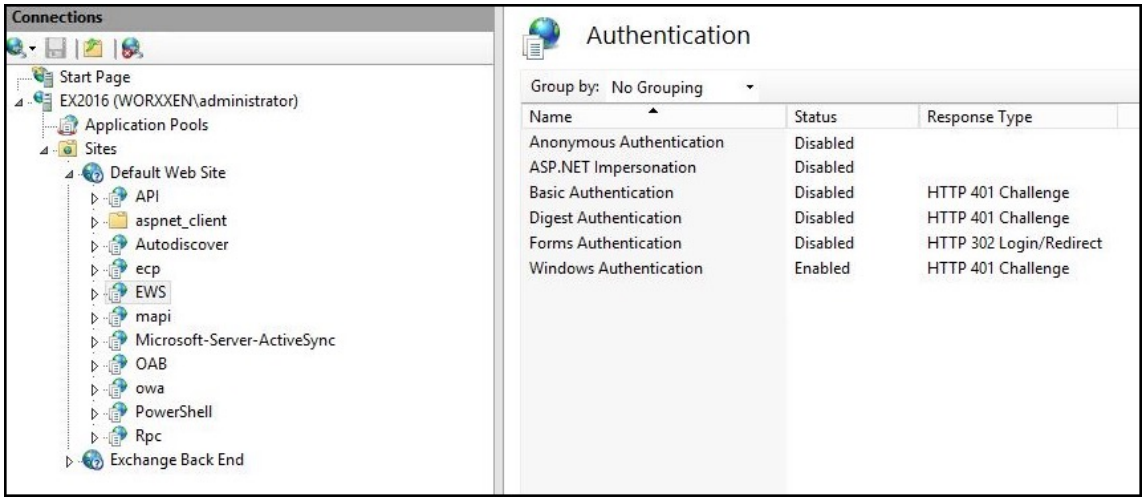
構成を開始するには、次の手順を実行します:

1. EWS 仮想ディレクトリがインストールされているサーバーにログオンします。
2. IIS マネージャーコンソールを開きます。
3. [既定の **Web** サイト] で、[EWS 仮想ディレクトリ] をクリックします。

   認証、SSL、構成エディターのスナップインは、IIS マネージャーコンソールの右側にあります



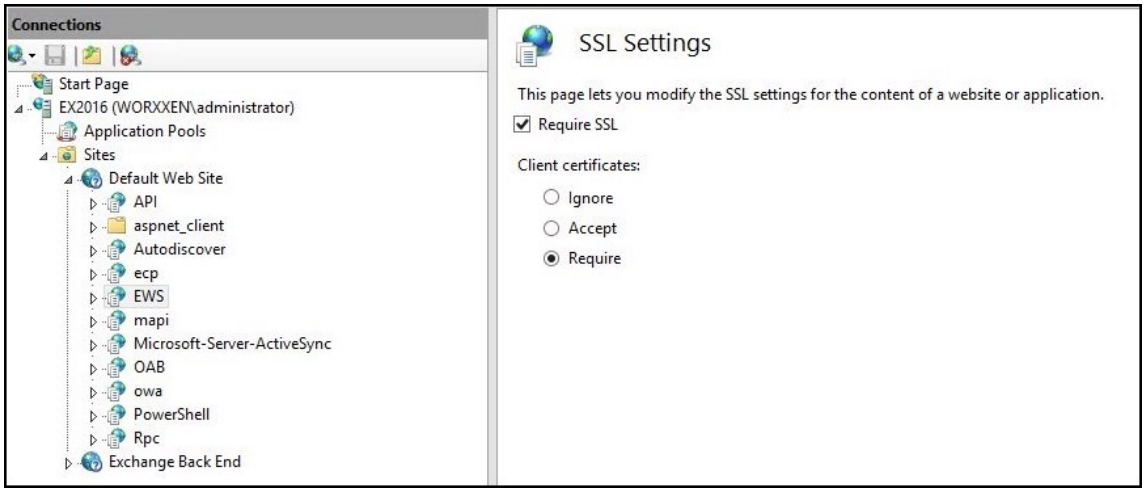
4. 次の図に示すように、EWS の 認証設定が構成されていることを確認します。



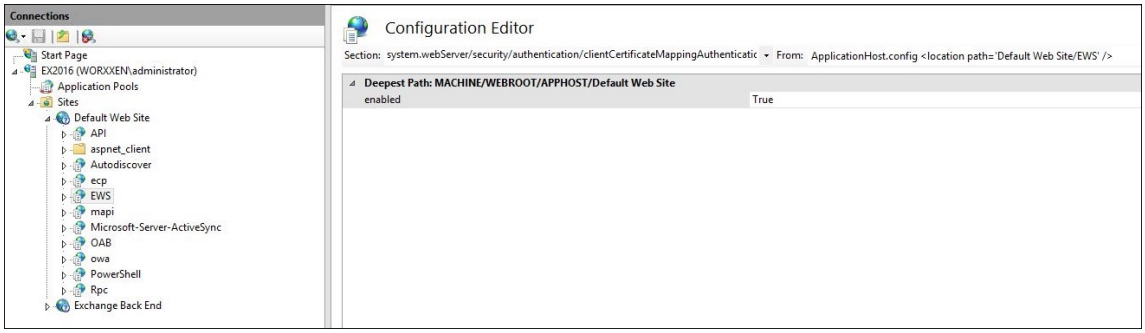
5. EWS 仮想ディレクトリの **SSL** 設定を構成します。

   a) [**SSL** を必要とする] チェックボックスをオンにします。

b) ［クライアント証明書］ で、［必須］ をクリックします。他の EWS メールクライアントが、認証と Exchange Server への接続のための資格情報としてユーザー名とパスワードを使用する場合は、このオプションを ［承認］ に設定できます。



6. ［構成エディター］ をクリックし、［セクション］ ドロップダウンリストで次のセクションに移動します：
   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. ［有効］ の値を **True** に設定します。



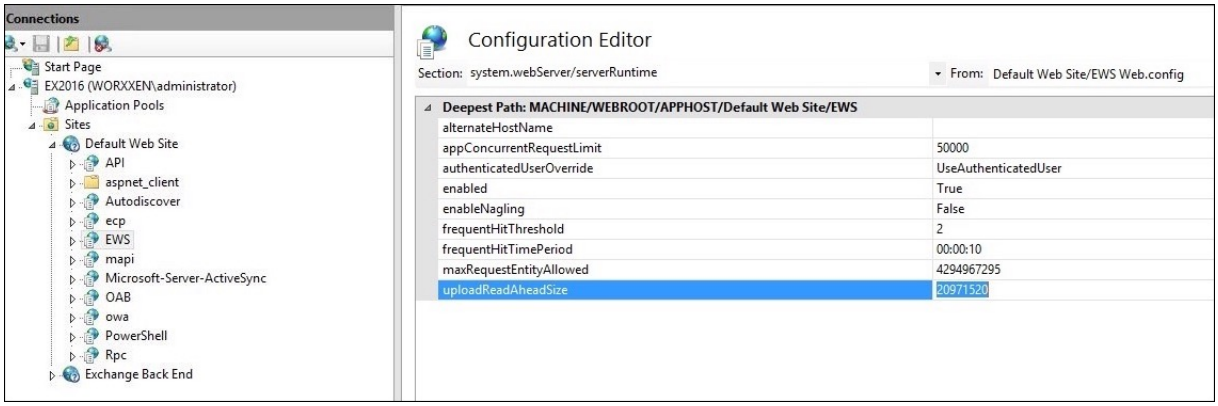
8. ［構成エディター］ をクリックし、［セクション］ ドロップダウンリストで次のセクションに移動します：
   - **system.webServer/serverRuntime**
9. ［**uploadReadAheadSize**］ の値を **10485760**（10 MB）または **20971520**（20 MB）に設定するか、組織で必要な値に設定します。

   > 重要：
   >
   > この値が正しく設定されないと、EWS プッシュ通知のサブスクライブ時に証明書ベースの認証が失敗し、エラーコード 413 が発生する可能性があります。
   >
   > この値を **0** に設定しないでください。

詳しくは、次のサードパーティリソースを参照してください：

- Microsoft IIS サーバーランタイム

- Butsch クライアント管理ブログ



iOS のプッシュ通知に関連した Secure Mail の問題のトラブルシューティングについては、Citrix Support Knowledge Centerの記事を参照してください。

関連情報

Secure Mail for iOS のプッシュ通知

XenMobile モバイルデバイス管理（MDM）の Cisco Identity Services Engine（ISE）との統合

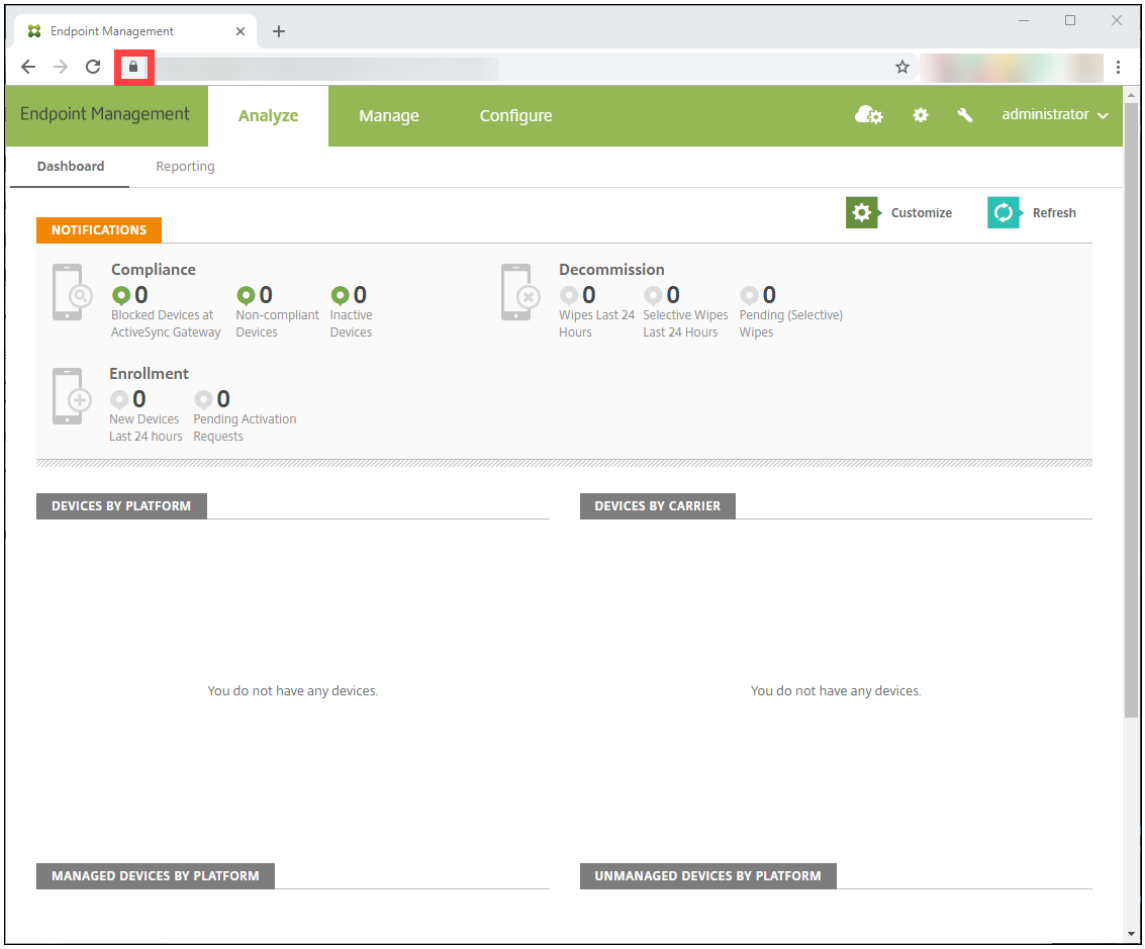
January 24, 2020

寄稿者：John Bartel III

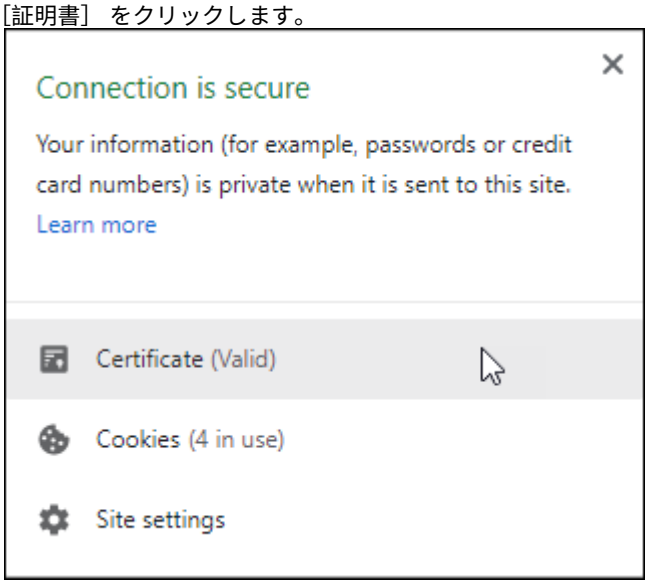
Cisco ISE は、社内でのモバイルデバイスの展開、セキュリティ保護、監視、統合、および管理に使用されます。モバイルデバイスにダウンロードされたソフトウェアが、エンドポイント上のアプリケーションとパッチの配布、制御データ、構成を制御します。XenMobile を Cisco ISE と統合して、Cisco ISE コンソール上の非準拠デバイスや管理対象外デバイスを管理できます。XenMobile では、企業サービスへのアクセスを選択的に許可、拒否、または検疫することもできます。

XenMobile との統合を設定するには、管理者 RBAC の役割が割り当てられた XenMobile Server 上にローカルのサービスアカウントを作成します。この役割により、Cisco ISE は XenMobile API にアクセスできます。ISE は XenMobile 証明書を信頼する必要があります。この証明書をダウンロードするには、Web ブラウザーを開き、サーバーの URL に移動してログインします。

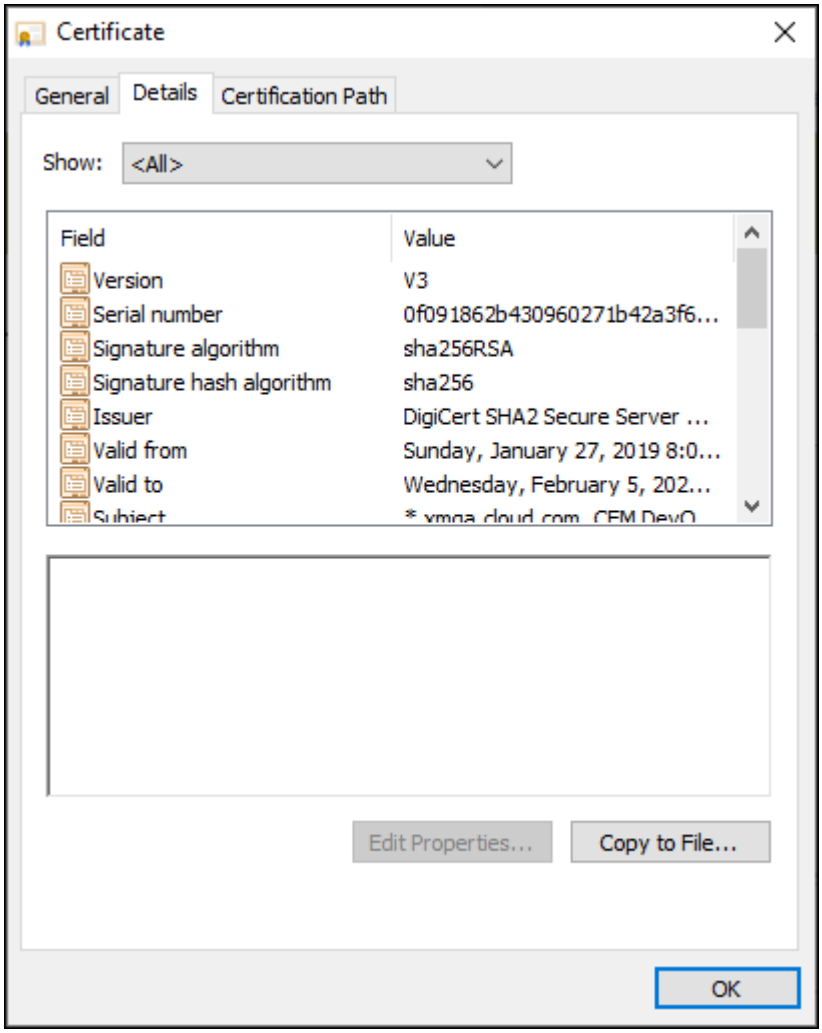
1. ログインした後、アドレスバーの URL の横にあるロックをクリックします。



2. [証明書] をクリックします。



3. [詳細] タブを選択して、[ファイルへコピー] をクリックします。



4. ウィザードに従って、証明書をローカルに保存します。
5. Cisco ISE コンソールにログインし、以前にダウンロードした XenMobile 証明書をインポートします。この証明書は、Cisco ISE の信頼された証明書ストアにインポートします。Cisco ISE が XenMobile Server との通信を信頼するためには、このインポートが必要です。
   a) ［管理］ **>** ［システム］ **>** ［証明書］ **>** ［証明書管理］ **>** ［信頼された証明書］ に移動します。［インポート］ をクリックします。
   b) 証明書に名前を付け、［**ISE** 内の認証用に信頼する］ および ［シスコサービスの認証用に信頼する］ ボックスをオンにします。
6. XenMobile を Cisco ISE 内の外部 MDM として追加します。
   a) ［管理］ **>** ［ネットワークリソース］ **>** ［外部 **MDM**］ に移動します。［追加］ をクリックして、以下を記入します:
      - サーバーホスト: XenMobile FQDN
      - ポート: 443
      - インスタンス名: XenMobile Server のインスタンス名。ほとんどの展開では、インスタンス名はデフォルトで「zdm」です。

- ユーザー名: このタスク用に作成したユーザーの名前を入力します。ユーザーは、元の管理者 RBAC グループのローカルの管理者アカウントとする必要があります。
- パスワード: さきほど追加したユーザーのパスワードです。
- [有効] となっている箇所を確認してください。

7. テストが成功したら、[送信] をクリックします。

Cisco ISE の詳細については、「Cisco ドキュメント」を参照してください。

